Міністерство освіти і науки України

Національна академія наук України

Національний центр «Мала академія наук України»

С. Б. МОГИЛЬНИЙ

ІНФОРМАЦІЙНА БЕЗПЕКА ПРИ РОБОТІ В ІНТЕРНЕТІ

Навчально-методичний посібник

Київ 2018

Міністерство освіти і науки України
Національна академія наук України
Національний центр «Мала академія наук України»

С. Б. МОГИЛЬНИЙ

ІНФОРМАЦІЙНА БЕЗПЕКА ПРИ РОБОТІ В ІНТЕРНЕТІ

Навчально-методичний посібник

Київ
2018

Рекомендовано науково-методичною радою
Національного центру «Мала академія наук України»
(протокол №1 від 18.01.2018)

Могильний С. Б.

Інформаційна безпека при роботі в Інтернеті : навч.-метод. посіб. / за ред. О. В. Лісового та ін. – К., 2018. – 105 с.

Посібник адресований як слухачам Всеукраїнських наукових профільних шкіл – дослідникам-початківцям, так і тим, хто проводить серйозні наукові дослідження.

ЗМІСТ

ВСТУП

Хто, як і навіщо стежить за вами через Інтернет

Безпека комп'ютерних даних і наша, користувацька, вимірюється відсутністю вірусів – троянів, черв'яків та інших гидких шкідливих програмок, розрахованих на те, щоб злегка або серйозно зіпсувати життя нам з вами. Однак…[1]

Однак останні пару років свідчать, що віруси минулого, та й сьогодення, – дитячий 8-бітний писк на галявині Super Mario у порівнянні з тим, що дійсно загрожує кожному з нас.

Ну що, справді, може зробити вірус? Змусити власника комп'ютера скачати, розлучившись із кровно зароблениими п'ятдесятьма доларами, ліцензійний антивірус? Перевстановити операційну систему? Поміняти паролі у Facebook? Залатати діру у Wi-Fi? Побігати по конторах, що відновлюють дані? Налякали! Усе це можна вирішити і не страшно.

Набагато страшніше, що вся та, здавалося б, нешкідлива інформація, якою ми щодня ділимося з цікавими друзями, хвалькуватими колегами і набридливими родичами, в будь-який момент може опинитися у зловмисників. Хто, як і навіщо стежить за нами безперервно і як запобігти цьому мерзенному факту – ось про що йтиметься далі.

Не бажаєте печива?

Смартфони можуть заносити в системні поля фотофайлів координати точки, в якій зроблений знімок. При публікації знімка в соціальних мережах онлайн-ресурси можуть автоматично зіставити координати і видати точну адресу місця зйомки.

Facebook і електронна пошта стали для багатьох невід'ємною частиною кожного ранку. Проте задумайтеся на хвилинку! Адже ми з вами постійно відправляємо у Всесвітню мережу стільки інтимних деталей власного життя, що ніякий шпигун і не потрібний. Досить 24 години на добу записувати дії, які ми виконуємо за нашими девайсами: в якому клубі і з ким Світлана п'ятий раз за ніч побувала у Facebook; туфлі якого розміру і за скільки купив Олексій; коли Ірина збирається на конференцію в Польщу; в якій дитячий клуб Сергій відвів свого сина; на якій станції метро вийшла Катя; яким координатам GPS Андрій присвоїв тег home sweet home.

І хто ж буде записувати всю цю начебто нікому не потрібну нісенітницю, запитаєте ви. Є такий Джеймс Бонд, і на вашому комп'ютері він теж встановлений. Це – наша власна безпечність, що ховається під милою назвою «печеньки», або cookies.

«C is for cookie and it's good enough for me», – співав симпатичний синій плюшевий Монстр Пряник у навчальній програмі «Вулиця Сезам», навіть не підозрюючи, що послужить ідейним натхненником для творців перших «печеньок», компанії Netscape Communications. Старі гики, можливо, пам'ятають, що до Google Chrome, Internet Explorer, Opera і, звичайно, до Safari був такий браузер як Netscape Navigator, «дідусь» сучасного Mozilla Firefox, і був він найпоширенішим аж до середини 90-х років XX століття.

[1] http://isearch.kiev.ua/uk/news/security/1509

Саме в Netscape вперше і з'явилася підтримка cookies. Їх придумали для того, щоб збирати інформацію про відвідувачів і зберігати її не на переповнених серверах компанії, а на жорстких дисках самих відвідувачів. Для початку «печеньки» реєстрували базову інформацію: перевірялося, був уже відвідувач на сайті Netscape чи зайшов уперше. Пізніше програмісти зрозуміли, що cookies можна навчити записувати практично будь-які відомості про користувача, які він сам захоче залишити в Інтернеті. Збиралися вони, зрозуміло, без відома мирних відвідувачів.

Непомітно впроваджені в Netscape Navigator у 1994-му, а в Internet Explorer у 1995-му, «печеньки» залишалися безвісними трудівниками аж до 1996 року, коли про них, завдяки журналістському розслідуванню, дізналася вся поважна інтернет-публіка, – і вибухнув міжнародний скандал. Громадськість була в шоці: брат, поки не дуже великий, але все ж брат, виявляється, стежив за всіма діями щохвилини і, більш того, все записував. Твердження творців про те, що всі дані зберігаються в безпеці (а саме – на власному комп'ютері кожного користувача) і не можуть бути використані зловмисниками, заспокоювали слабко. А незабаром стало ясно, що ці твердження не є достовірними.

Як з'ясувалося, при великому бажанні зловмисник може перехопити файл-«печеньку», відправлений на сайт, який створив цей витвір комп'ютерно-кулінарного мистецтва, і, прикинувшись користувачем, діяти на сайті на власний розсуд. Так зламують поштові скриньки, акаунти в інтернет-магазинах, банках тощо. Однак зізнаємося, зробити це не так просто.

Більше того, незважаючи на заявлену анонімність cookies, навіть самі маркетологи визнають, що класифікація користувачів, тобто нас із вами, дійшла до досконалості. Потрібні всі володарі Safari 25–35 річного віку, чоловічої статі, з карткою в Citibank, які закінчили МАІ, неодружені, що страждають короткозорістю, що носять довге волосся, фанати серіалу Star Wars і групи Nickelback, з річним доходом $50–100 тисяч, часті відвідувачі клубу Rolling Stone, що проживають біля метро «Політехнічний інститут»? Будь ласка, ось ці три людини.

Хто купує цю інформацію? Як він захоче нею скористатися? Наша параноя налила собі склянку чогось з апельсиновим соком і відмовляється відповідати на ці питання. Масовість же явища давно вийшла за будь-які прийнятні межі.

Експеримент, проведений Wall Street Journal ще в 2010 році, засвідчив: 50 найпопулярніших сайтів Америки встановили від свого імені на тестовий комп'ютер 3180 файлів-шпигунів (уже згадані нами «печеньки» і їх молодші просунуті брати «Бікон», або «маячки»), що записують за безтурботними користувачами в буквальному сенсі все. Лише менше третини файлів стосувалися роботи власне сайтів – фіксували паролі, запам'ятовували бажаний розділ, щоб з нього почати наступного разу, і т. ін. Решта існували лише для того, щоб більше дізнатися про конкретного відвідувача і подорожче продати зібрані про нього відомості. Єдиним сайтом, який не встановив жодної неприємної програмки, виявилася «Вікіпедія».

Як діє цей алгоритм? Дуже просто. Сайт, на який ви зайшли, щоб прочитати ранкову пошту, присвоює вам унікальний код, наприклад 76buj7btimlglrs98vv549vvvvv3v46un9r8, надсилає цей код вам як текстовий файл, зберігає на вашому комп'ютері і починає разом з вами читати вашу дорогоцінну пошту під сімома замками і багатобітним паролем. І що ж там пишуть? Друзі покликали вас у кіно! «Печеньки», не гаючи часу, записали, на який фільм, у якому кінотеатрі і в який день. З банку надійшов лист? «Печеньки» змальовують назву банку, а може, й суми з виписки, а також магазини, в яких ви витрачали гроші. Лист від авіакомпанії зі звітом щодо миль? «Печеньки» відзначать, куди ви літали. Запрошення

приєднатися до папки на DropBox? «Печеньки» відзначать, що він у вас встановлений, і автоматично зарахують вас у гики. Реклама бренду ноутбуків на найближчі три місяці на цьому сайті вам забезпечена. Далі – більше.

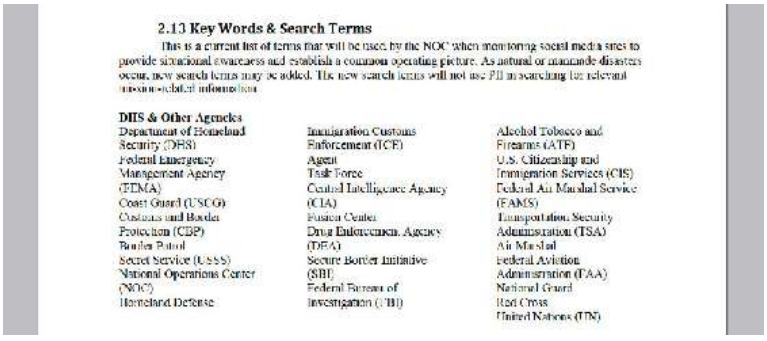
Крім cookies, як уже зазначалося вище, є ще «маячки». Вони не надсилають самі себе користувачам, а розміщуються прямо на сайті як невелика картинка або піксель. «Бікон» здатні запам'ятовувати введені з клавіатури дані, розпізнавати місце розташування курсору миші і ще багато чого. Зіставивши їх разом з «печеньками», отримуємо картину, гідну гнізда параноїка.

Якщо ви не вірите, спробуйте набрати назву будь-якого популярного товару в Google. Ваш інтерес до цієї речі миттєво запишуть «печеньки», а ділки рекламного світу тут же продадуть його ненаситному рекламодавцю. Будьте впевнені, «вранці в газеті – ввечері в куплеті»: в найближчий же час ви побачите рекламу цього товару на власній сторінці у Facebook. Натиснете «Мені подобається»?

Для чого можна використовувати таку інформацію

Нині значна частина інформації, що використовується, на перший погляд, нешкідлива. У дівчаток, які публікують котиків у соціальних мережах, з'являються оголошення про нові види котячого корму; хлопчикам, які обговорюють девайси, пропонують купити новий смартфон; модним хіпстерам рекомендують фотокамери Leica; татам, які вболівають за «Динамо», показують нові кросівки; а мам, які запитували поради зі сповивання юного нащадка, завалюють рекламою підгузників. Бабусі з другого під'їзду можуть запропонувати віагру і поховальні послуги недорого. Не дуже гуманно, чим вкрай незадоволені американські та англійські асоціації з захисту прав людини, але поки що законодавчо cookies на міжнародному рівні ніяк не обмежені, а навіть, навпаки, виділені у пріоритетну групу із «зеленим світлом».

Компаній, що діють на цьому небідному ринку витягання вигоди з наших з вами хвастощів і цікавості (а грошовий еквівалент всесвітнього ринку інтернет-реклами вже впритул підібрався до сотні мільярдів доларів), превелика безліч. І дійсно, кому потрібний просто банер, якщо є шанс повісити рекламу, тісно пов'язану з інтересами і способом життя користувача. У цьому випадку шанс, що наївний користувач клацне на строкатий квадратик, який кричить «купи мене!», буде набагато вищим. Тому і вартість таких оголошень у кілька разів вище, ніж зазвичай, адже рекламодавці, що йдуть на преміумну покупку, наївно хочуть бути впевнені в тому, що їх ролики і товари будуть затребувані споживачем.



2.13 Key Words & Search Terms

This is a current list of terms that will be used by the NOC when monitoring social media sites to provide situational awareness and establish a common operating picture. As natural or manmade disasters occur, new search terms may be added. The new search terms will not use PII in searching for relevant open-source information

DHS & Other Agencies

Department of Homeland Security (DHS)
Federal Emergency Management Agency (FEMA)
Coast Guard (USCG)
Customs and Border Protection (CBP)
Border Patrol
Secret Service (USSS)
National Operations Center (NOC)
Homeland Defense
Immigration Customs Enforcement (ICE)
Agent
Task Force
Central Intelligence Agency (CIA)
Fusion Center
Drug Enforcement Agency (DEA)
Secure Border Initiative (SBI)
Federal Bureau of Investigation (FBI)
Alcohol Tobacco and Firearms (ATF)
U.S. Citizenship and Immigration Services (CIS)
Federal Air Marshal Service (FAMS)
Transportation Security Administration (TSA)
Air Marshal
Federal Aviation Administration (FAA)
National Guard
Red Cross
United Nations (UN)

Затверджений список слів, фраз і висловів, уживання яких може спричинити підвищену увагу до ваших дій у Глобальній мережі

Розвідник Марк Цукерберг

Якщо ви думаєте, що за інформацією, залишеною вами в Мережі, стежать тільки милі рекламні шпигуни, поспішаємо переконати вас у протилежному. Охочих пізнати ваші секрети набагато більше. Деякі з них ставлять начебто і благородні цілі – мир у всьому світі, всесвітнє панування і процвітання. Втім, викресліть всесвітнє панування – ми цього не писали. Отже, наступним у нашому списку довгоносих буратін буде всього лише Міністерство внутрішньої безпеки США.

Американська громадськість, на відміну від нашої, не дрімає і, пронюхавши, що МВБ веде запекле стеження за простими людьми, створила противагу цій організації зі скромною назвою EPIC. В одному зі своїх контррозслідувань співробітникам EPIC вдалося з'ясувати, що МВБ розробило якийсь список слів-активаторів стеження. Забиваєте ви, скажімо, в Google невинне словосполучення «Гвадалахара, Мексика». А МВБ тут же заносить вас у список потенційних Бін Ладенів і починає фіксувати, про всяк випадок, усі ваші дії в Інтернеті. Раптом вирішите щось підірвати, мало чого...

Повний список вкрай дивних слів, багато з яких ми з вами вживаємо в інтернет-спілкуванні кожен день, можна подивитися за цим посиланням на сторінках 20–23[2].

До того ж, як з'ясували в EPIC, абсолютна більшість хоч скількись значущих доменів, на зразок Facebook, Twitter, новинних поштових сайтів, співпрацюють з усіма відомими службами безпеки, надаючи їм доступ до листування, особистих даних, місця перебування і навіть зовнішнього вигляду користувачів, не маючи на те постанови суду. За заявою одного із співробітників МВБ, на одного реального підозрюваного доводиться десяток підозрюваних абсолютно необґрунтовано. Незрозуміло, як відбувається в такій ситуації передача даних, наскільки вона безпечна і як утилізується отримана інформація в разі непотрібності.

Ще один кричущий факт упровадження в комп'ютери Джонсонів, Петерсонів і Сідорсонів під егідою боротьби з піратством був оприлюднений у США в липні нинішнього року. Справа в тому, що Асоціація звукозапису та кінематографії США розробила проект, за яким провайдери будуть автоматично повідомляти про випадки медіа-піратства. Ми, звичайно ж, проти піратства, проте така ініціатива означає стеження за користувачами. Особливо дивними здаються заходи покарання: від спасенних бесід і обмеження швидкості інтернет-каналу до заборони доступу до двохста основних сайтів світу.

Навіть якщо у вас є окремий комп'ютер для роботи, з якого ви, як пристойний параноїк, ніколи не виходите у Всесвітню павутину, поспішаємо вас засмутити. Є способи стежити за ним навіть в обхід «печеньок», «маячків», слів із терористичного списку тощо. Адже ви все одно регулярно оновлюєте антивірус? А що за сигнатури надсилають на ваш комп'ютер? Зацікавлений (вже урядом чи третіми особами) творець антивірусу може завдяки своїй програмі шукати на вашому жорсткому диску все, що завгодно. Достатньо лише оголосити це новим вірусом.

Та що там антивірус – ваш GPS, ваш смартфон, який ось-ось обзаведеться датчиком відбитків пальців, Google Street View, програми для розпізнаванню осіб на фотографіях – межі впровадження незнайомців, що не мають на те права, в наше повсякденне життя просто немає. Ваш куратор у ФБР або MI-6 у курсі, йому вже передали.

[2] https://epic.org/foia/epic-v-dhs-media-monitoring/Analyst-Desktop-Binder-REDACTED.pdf

Танці зі свинями

Але хто передав? Передали ми з вами. Подивіться, як ми ставимося до власної інформації! Подивіться налаштування Facebook: скільком додаткам сторонніх розробників ви дозволили користуватися своїми даними? Спробуйте встановити нову програмку з Google Play Store в Android і для різноманітності прочитайте, які повноваження ви їй обіцяєте (Доступ до телефонної книги? Користування Інтернетом за потребою? Здійснення дзвінків вашої бабусі?) Подивіться на угоду користувача Instagram: підписавшись, ви передали всі свої фотографії в повну власність Facebook! Заведіть акаунт у хмарі Amazon і поцікавтеся, на що ви погодилися: Amazon має право змінювати, видаляти завантажену вами інформацію на свій розсуд, а також припиняти ваш доступ на сайт.

Гуру інформатики, професор Прінстонського університету Едвард Фелт влучно охрестив те, що відбувається, «синдромом танцюючої свині». Якщо друг надіслав вам посилання на програмку з танцюючими свинями, ви напевно встановите її, навіть якщо в ліцензійній угоді буде написано про можливість втрати всіх даних, почуття гумору, провини, совісті, розуму і середнього достатку.

Що ж робити?

Ось декілька абсолютно легальних рекомендацій, дотримуючись яких, ви злегка обмежите присутність всевидющого ока у вашому комп'ютері:

1. Переконайтеся, що ваш домашній Wi-Fi добре запаролений і ніколи не користуйтеся підозрілим інтернет-з'єднанням.
2. Змінюйте паролі частіше, робіть їх довшими і складнішими. Ми, як і раніше, скептично ставимося до програм управління паролями і розривамося між страхом забути свій двадцятитрьохзначний цифро-буквений пароль, страхом злому пошти, Facebook, Twitter та інших миленьких сайтів і страхом того, що хтось запише наші паролі, якщо вести їх облік у спеціалізованій програмі. Як кажуть, ось вам отрута на вибір. Якщо ви обираєте останню опцію, наша параноя рекомендує вам RoboForm і Last Pass.
3. Установіть програмку CCleaner і не забувайте нею користуватися (в ідеалі – щодня).
4. Установіть антитрекінгові плагіни у ваш браузер. У Google Chrome, наприклад, нам подобається Keep my opt-outs Plugin. Він прибирає дані про вас більш ніж із 230 сайтів. Після цього встановіть Do not track plus – цей плагін не дає «печенькам» знову надсилати інформацію про вас. У Chrome, до речі, рекомендуємо користуватися функцією Incognito. У такому режимі за вами можна підглядати тільки із-за спини, так що не забувайте озиратися або повісьте дзеркало позаду комп'ютера. Жарт.
5. Використовуйте анонімну VPN. Хороша і швидка може коштувати невеликих грошей, але сервіс зазвичай того вартий. З безкоштовних нам подобається HotSpot Shield.
6. Відключіть історію в Google. Для цього наберіть google.com/history і, використовуючи свій акаунт на gmail.com, видаліть усе, що Google записав про вас. Після цієї операції Google перестане записувати (напевно), якщо ви самі не попросите про зворотне.
7. Також можна перейти і на популярний нині браузер з TOR, який застосовує волонтерську мережу комп'ютерів для досягнення максимальної анонімності переданих зашифрованих даних.
8. Якщо вам необхідно спілкуватися з друзями та колегами каналом, який не переглядається, встановіть програму анонімного файл-шерінга типу GNUnet, Freenet

або скористайтеся мережею I2P. У цьому ж випадку рекомендуємо регулярно робити резервні копії даних і зберігати їх на різних хмарах, звертаючись до них через анонімну VPN.

9. І, найголовніше, читайте користувальницькі угоди встановлюваних програм. Перед тим як встановлювати чергових котиків, добре подумайте, чи потрібна вам ця програмка, якщо вона зобов'язується в будь-який час, як теща, користуватися від вашого імені Інтернетом, телефоном, перевіряти, хто вам дзвонив, дізнаватися, де ви перебуваєте, оплачувати покупки вашою кредитною картою і міняти мелодію вашого дзвінка.

Як реалізувати наведені вище рекомендації, в тому числі з застосуванням мікрокомп'ютера Raspberry Pi, буде розглянуто в наступних розділах посібника.

1. Захист паролів та даних

1.1. Криптографічні алгоритми шифрування

Під терміном сучасної криптографії мають на увазі етап розвитку алгоритмів шифрування інформації, який відбувався після становлення шенноновської математичної криптографії, з середини 70-х років XX століття. У цей час зародився і почав інтенсивно розвиватися новий напрям прикладної криптографії – використання шифрування у мережевих протоколах і сервісах[3]. Криптографія охоплює багато різних напрямів, таких як шифрування, електронний цифровий підпис, хешування тощо. Розглянуто лише напрям шифрування інформації – видозмінення вхідних даних з метою приховування інформаційної складової від сторонніх осіб при передачі незахищеним каналом.

Розрізняють два напрями шифрування:

- шифрування закритим ключем, або симетричне шифрування;
- шифрування кодом з відкритим ключем, або асиметричне шифрування.

Алгоритм шифрування, в якому для кодування і декодування використовується один і той самий криптографічний ключ, називається симетричним. Ключ алгоритму вибирається до початка обміну, відомий обом сторонам і є секретним, він не передається через канал обміну. Це історично перший алгоритм шифрування, оскільки технічно порівняно простий у реалізації. Найпростішим методом симетричного шифрування є перестановка символів за певним законом, відомим двом сторонам.

Ідея асиметричного шифрування різниться тим, що існує два типи ключів – відкритий ключ, що передається незахищеним каналом, і таємний ключ, що використовується для підтвердження аутентифікації і декодування інформації.

Системи шифрування з відкритим ключем набули значної популярності з інтенсивним розвитком мережі Інтернет і віртуальних сервісів.

Принципи шифрування даних з використанням відкритого ключа використані в сучасних мережевих протоколах. Ідея алгоритмів шифрування з відкритим ключем полягає у використанні принципу односторонньої функції: маючи відому функцію f(x), можемо легко знайти результат опрацювання відкритого ключа z – f(z), але, знаючи z, знайти функцію f(x) майже неможливо.

[3] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1276-evolution-of-cryptographic-algorithms-for-encryption

Прикладом такого алгоритму шифрування «з життя» є використання певної книжки як таємного ключа. В даному випадку відкритим ключем, що передається по незахищеному каналу є послідовність даних, що містить номера сторінки, рядку і слова закодованого повідомлення. Навіть отримавши повну послідовність даних відкритого ключа, розшифрувати повідомлення не вдасться, не знаючи таємної книги.

Сучасні алгоритми шифрування передбачають, що стороннім особам може бути відомий як сам алгоритм, так і частини розшифрованого відкритого коду. Єдине, що не знає «викрадач інформації», – це секретний ключ, що не дозволяє розшифрувати дані. Єдиним методом відкриття секретного ключа є послідовний перебір усіх можливих варіантів. Вважається, що довжина секретного коду, який використовується в сучасних алгоритмах шифрування даних, не дає змоги розкодувати дані за прийнятний час. До алгоритмів шифрування також ставлять вимоги відносної стійкості криптографічному аналізу.

Починаючи з 70-х років, Агентство національної безпеки США почало проводити конкурс на криптографічний алгоритм шифрування даних, що мав би відповідати вимогам щодо високої надійності. Перші спроби завершилися невдачею, а в результаті третього конкурсу був прийнятий криптографічний алгоритм шифрування DES, який невдовзі став першим міжнародним криптографічним стандартом.

DES (Data Encryption Standard) — симетричний блочний алгоритм шифрування, розроблений фірмою IBM і затверджений у США в 1977 році як офіційний стандарт (FIPS 46-3). DES має блоки по 64 біти і 16-циклічну структуру мережі Фейстеля, для шифрування використовується ключ довжиною 56 біт. Алгоритм застосовує комбінацію нелінійних (S-блоки) і лінійних (перестановки E, IP, IP-1) перетворень. Алгоритм DES у своєму складі містить засекречені елементи, що із самого початку його використання породило велику кількість побоювань, оскільки вони могли давати Агентству національної безпеки США можливість неправомірного контролю.

Як вже було зазначено вище, DES – блочний алгоритм шифрування, вхідними даними коду є блок розміром n біт і k-бітний ключ. На виході, після застосування шифруючого перетворення, отримаємо n-бітний блок, при чому навіть незначна зміна вхідних даних приводить до істотних змін зашифрованого блоку. Блочні алгоритми шифрування реалізують методом багаторазового застосування до блоків вхідних даних деяких базових перетворень.

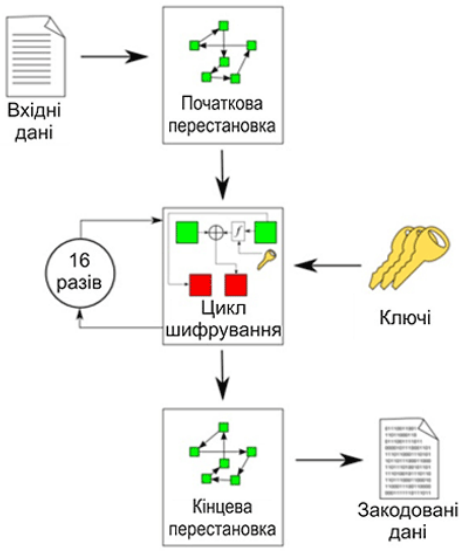


Рис. 1.1. DES – блочний алгоритм шифрування

Схема шифрування алгоритмом DES

Першим етапом опрацювання вхідних даних є вхідна перестановка (рис. 1.1). Таке опрацювання класифікується як просте перетворення над частинами одного блоку. Проста перестановка без ключа – один із найпростіших алгоритмів шифрування. Символи вхідних даних перемішуються за певним попередньо домовленим законом, що не розголошується.

Наступним етапом шифрування є основний цикл опрацювання даних – 16-циклічне перетворення мережею Фейстеля з використанням секретного ключа – що класифікується як складне перетворення над локальною частиною у блоці. Мережа Фейстеля – криптографічне перетворення над блоками, що являють собою ліву і праву половини регістру зсуву. Аргументами функції шифрування є 32-бітний вектор вхідної послідовності Ri – 1 і 48-бітний ключ, що є результатом попереднього опрацювання 56-бітного заданого ключа. На останньому етапі зашифровані дані знову перемішуються вихідною перестановкою.

В алгоритмі шифрування DES використовується пряме перетворення мережею Фейстеля при кодуванні і зворотне при декодуванні.

Алгоритм шифрування DES критикували за малу довжину ключа, що, врешті, не завадило йому стати загальноприйнятим стандартом. За історію свого існування алгоритм шифрування DES пережив декілька публічних криптографічних атак, що довели його невисоку надійність. Уперше код було розшифровано за допомогою використання мережі, що налічувала десятки тисяч комп'ютерів і на декодування знадобилося 39 днів. Пізніше, у 1998 році в рамках досліджень DES Challenge II, що проводила RSA Laboratory, алгоритм шифрування був зламано за допомогою суперкомп'ютера за 3 дні, що викликало значні побоювання щодо достатньої надійності міжнародного криптографічного стандарту шифрування. Остаточним доказом ненадійності DES стало публічне дешифрування коду у 1999 році, що зайняло лише 22 години 15 хвилин.

На сьогодні алгоритм шифрування DES вважається ненадійним переважно через малу довжину ключа – 56 біт та розмір блоку – 64 біти. Вважається, що алгоритм шифрування достатньо надійний для застосування у модифікації.

3-DES є простим методом усунення недоліків DES – недостатньої криптостійкості. По суті, ця модифікація шифрування є послідовним трьохциклічним DES з використанням 112- або 168-бітного ключа. Швидкість роботи такого алгоритму шифрування в три рази нижча, ніж у DES, але криптостійкість набагато краща, час, необхідний для криптоаналізу 3-DES, теоретично може в мільярд разів перевищити час злому попередника.

Хоча існують розроблені теоретичні атаки, про здійснені розшифрування алгоритму 3-DES не відомо. Однак низька швидкість та наслідування усіх інших недоліків алгоритму шифрування DES (наприклад, незручності для програмної реалізації, оскільки із самого початку алгоритм шифрування був розроблений для апаратної реалізації) зумовлюють неконкурентоспроможність алгоритму 3-DES порівняно з алгоритмом шифрування AES. Алгоритми DES та 3-DES поступово витісняються алгоритмом шифрування AES, що з 2002 року є стандартом США.

AES (Advanced Encryption Standard), також відомий під назвою Rijndael, – симетричний алгоритм блочного шифрування з розміром блока 128 біт і ключем 128/192/256 біт. У результаті жорстокого відбору в рамках конкурсу AES, що проводився урядом США починаючи з 1997 року, був визнаний найкращим і прийнятий як державний стандарт шифрування Сполучених Штатів у 2001 році (FIPS 197). Розроблений Вінсентом Рейменом і Йоаном Дейменом алгоритм шифрування Рейндол найкраще відповідав запропонованим умовам конкурсу.

По суті, алгоритм шифрування, запропонований авторами, і AES не є одне і те саме. Алгоритм шифрування Рейндол підтримує широкий діапазон розміру блоку та ключа. Алгоритм AES має фіксовану довжину у 128 біт, а розмір ключа може приймати значення 128, 192 або 256 біт, у той час як алгоритм Рейндол підтримує розмірність блоку та ключа із кроком 32 біт у діапазоні від 128 до 256. Через фіксований розмір блоку алгоритм шифрування AES оперує з масивом 4×4 байт, який називається станом (версії алгоритму з більшим розміром блоку мають додаткові колонки) (рис. 1.2):

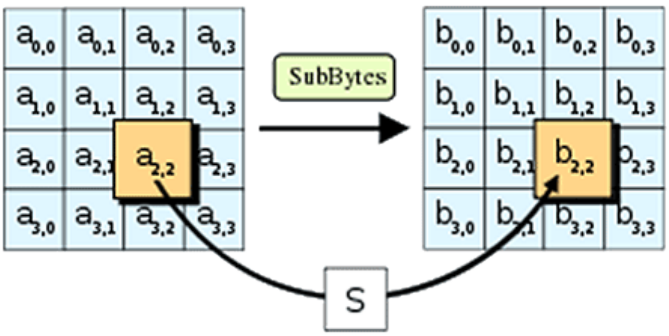


Рис. 1.2. Блок алгоритму шифрування AES

За принципом роботи алгоритм шифрування AES – підстановочно-перестановочна мережа. Особливістю криптографічного алгоритму AES є проста і доступна програмна реалізація, що розповсюджується у вигляді бібліотеки функцій. У складі бібліотеки – основна функція шифрування та 8 допоміжних, а також оголошуються масиви змінних. У процесі шифрування алгоритмом AES вхідні дані і ключ вносяться у таблиці (квадратні масиви) – стани і трансформуються за допомогою перестановок, зсувань та взаємних перенесень за певними визначеними законами в декілька кроків (раундів).

Незважаючи на відкритість коду, специфіка алгоритму шифрування AES не дозволяє декодувати секретні дані за прийнятний час. У червні 2003 року Агентство національної безпеки США постановило, що алгоритм AES з довжиною ключа 128 біт є достатньо надійним, щоб використовувати його для захисту інформації, що становить державну таємницю, а для найвищого рівня TOP SECRET – AES із ключем 192/256 біт.

На відміну від більшості інших алгоритмів шифрування AES має досить простий математичний опис. Це спричинило досить негативні відгуки у наукових колах. Багато вчених висловлювали побоювання щодо безпечності алгоритму шифрування AES, що ґрунтується на неперевіреному стверджуванні про складність розв’язання певних видів рівнянь, на яких базується код. Гіпотези і навіть їх доведення декілька разів публікувалися в наукових журналах. Так, наприклад, у роботі Ніколя Картуа і Йозефа Пепшика у 2002 році була описана теоретична процедура під назвою XSL-атака, що могла б уможливити злам алгоритму шифрування AES. Тим не менше, ці дані не були підтверджені на практиці, тому не викликали значного резонансу. Через декілька років іншими дослідниками було доведено, що в описаному вигляді XSL-атака на алгоритм AES не може бути здійснена.

Значний удар по репутації стійкості алгоритму шифрування AES завдали так звані атаки по сторонніх каналах. Це процедури зламу коду, що не ґрунтуються на недоліках у його математичній моделі, а використовують специфіку реалізації захищеного протоколу. У 2005 році Даніель Бернштейн опублікував роботу з описом атаки, що використовує для зламу інформацію про час виконання кожної операції шифрування. Для здійснення вдалої атаки знадобилося понад 200 мільйонів вибраних шифрованих текстів. У тому самому році Даг Арне Освік, Аді Шамір і Еран Трумер представили роботу з описом декількох

аналогічних методик, одна з яких добирала ключ лише за 800 циклів шифрування. Пізніше, у 2009 році були оприлюднені результати роботи з використання диференціального аналізу помилок, що дало змогу отримати ключ усього за 232 операції шифрування.

Станом на сьогодні AES є одним з найпоширеніших алгоритмів симетричного шифрування. Підтримка криптографічного алгоритму AES на апаратному рівні впроваджена фірмою Intel у новітнє сімейство високопродуктивних процесорів сімейства Sandy Bridge. Алгоритм шифрування використовується в сучасних захищених мережевих протоколах і платних сервісах.

1.2. Хешування для захисту паролів

Хешування (англ. hashing) – перетворення вхідного масиву даних довільної довжини у вихідну бітову послідовність фіксованої довжини, яку можна використати для порівняння даних[4].

Такі перетворення також називаються хеш-функціями, або функціями згортки, а їх результати називають хешем, хеш-кодом або дайджестом повідомлення (англ. message digest – MD).

Розрахувати значення хеш-функції або спробувати знайти пароль за значенням хеш-функції можна, наприклад, за допомогою ресурсу hashcrack.com[5] (рис. 1.3):

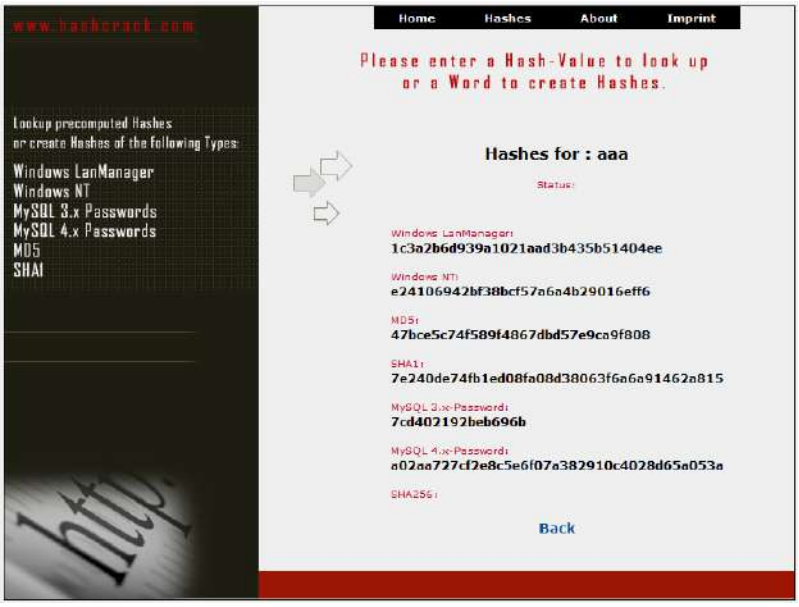


Рис. 1.3. Розрахунок значення хеш-функції онлайн

Хешування застосовується для порівняння даних: якщо у двох масивах хеш-коди різні, масиви гарантовано різняться; якщо однакові – масиви, швидше за все, однакові. У загальному випадку однозначної відповідності між вихідними даними і хеш-кодом немає в силу того, що кількість значень хеш-функцій менше, ніж варіантів вхідного масиву; існує безліч масивів, які дають однакові хеш-коди – так звані колізії. Ймовірність виникнення колізій відіграє важливу роль в оцінюванні якості хеш-функцій.

[4] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/837-hashing-message-digest
[5] http://hashcrack.com/index.php

Існує безліч алгоритмів хешування з різними характеристиками (розрядність, обчислювальна складність, крипостійкість тощо). Вибір тієї чи іншої хеш-функції визначається специфікою розв'язуваної задачі. Найпростішими прикладами хеш-функцій може слугувати контрольна сума або CRC.

Контрольні суми

Нескладні, вкрай швидкі й легко реалізовані апаратні алгоритми, використовувані для захисту від ненавмисних спотворень, у тому числі помилок апаратури. За швидкістю обчислення в десятки і сотні разів швидші, ніж криптографічні хеш-функції, і значно простіші в апаратній реалізації.

Платою за таку високу швидкість є відсутність криптостійкості – легка можливість підігнати повідомлення під заздалегідь відому суму. Також зазвичай розрядність контрольних сум (типове число: 32 біти) нижче, ніж криптографічних хешей (типові числа: 128, 160 і 256 біт), що означає можливість виникнення ненавмисних колізій.

Найпростішим випадком такого алгоритму є розподіл повідомлення на 32- або 16-бітні слова і їх підсумовування, що застосовується, наприклад, у TCP/IP.

Як правило, до такого алгоритму ставлять вимоги відстеження типових апаратних помилок, таких як кілька поспіль помилкових біт до заданої довжини. Сімейство алгоритмів та інші «Циклічні надлишкові коди» задовольняють цим вимогам. До них належить, наприклад, CRC32, застосовуваний в апаратурі Ethernet і у форматі упакованих файлів ZIP.

Криптографічні хеш-функції

Серед безлічі сучасних хеш-функцій прийнято виокремлювати криптографічно стійкі, які застосовуються в криптографії. Для того, щоб хеш-функція H вважалася криптографічно стійкою, вона має задовольняти трьом основним вимогам, на яких засновано більшість застосувань хеш-функцій у криптографії:

1. Незворотність: для заданого значення хеш-функції m має бути обчислювально нездійсненно знайти блок даних X, для якого H (X) = m.
2. Стійкість до колізій першого роду: для заданого повідомлення M має бути обчислювально нездійсненно дібрати інше повідомлення N, для якого H (N) = H (M).
3. Стійкість до колізій другого роду: має бути обчислювально нездійсненно дібрати пару повідомлень (M, M'), що мають однаковий хеш.

Ці вимоги не є незалежними:

1. Зворотна функція нестійка до колізій першого і другого роду.
2. Функція, нестійка до колізій першого роду, нестійка до колізій другого роду; зворотне неправильно.

Варто зазначити, що не доведено існування необоротних хеш-функцій, для яких обчислення будь-якого прообразу заданого значення хеш-функції теоретично неможливо. Зазвичай знаходження зворотного значення є лише обчислювально складним завданням.

Атака «днів народження» дає змогу знаходити колізії для хеш-функції з довжиною значень n бітів у середньому за приблизно $2^{n/2}$ обчислень хеш-функції. Тому n-бітова хеш-функція вважається криптостійкою, якщо обчислювальна складність перебування колізій для неї близька до $2^{n/2}$.

Для криптографічних хеш-функцій також важливо, щоб при найменшій зміні аргументу значення функції сильно змінювалося (лавинний ефект). Зокрема, значення хешу не має давати витоку інформації навіть для окремих бітів аргументу. Ця вимога є запорукою

криптостійкості алгоритмів хешування, які хешують пароль користувача для отримання ключа.

Застосування хеш-функцій

Хеш-функції також використовуються в деяких структурах даних – хеш-таблицях, фільтрах Блума і декартових деревах. Вимоги до хеш-функції в цьому разі інші:

- хороша перемішуваність даних;
- швидкий алгоритм обчислення.

Перевірка даних

У загальному випадку це застосування можна описати, як перевірка деякою інформацією на ідентичність оригіналу, без використання оригіналу. Для звірки використовується хеш-значення перевіреній інформації. Розрізняють два основні напрями цього застосування:

- ***Перевірка на наявність помилок***

Наприклад, контрольна сума може бути передана каналом зв'язку разом з основним текстом. На приймальному кінці контрольна сума може бути розрахована наново і її можна порівняти з переданим значенням. Якщо буде виявлена розбіжність, то це означає, що при передачі виникли спотворення і можна запросити повтор.

Побутовим аналогом хешування в такому разі може слугувати прийом, коли при переїздах у пам'яті тримають кількість місць багажу. Тоді для перевірки не потрібно згадувати про кожну валізу, а досить їх порахувати. Збіг буде означати, що жодної валізи не втрачено. Такий метод використовується у пірингових мережах для перевірки скачаного файлу на помилки (рис. 1.4):

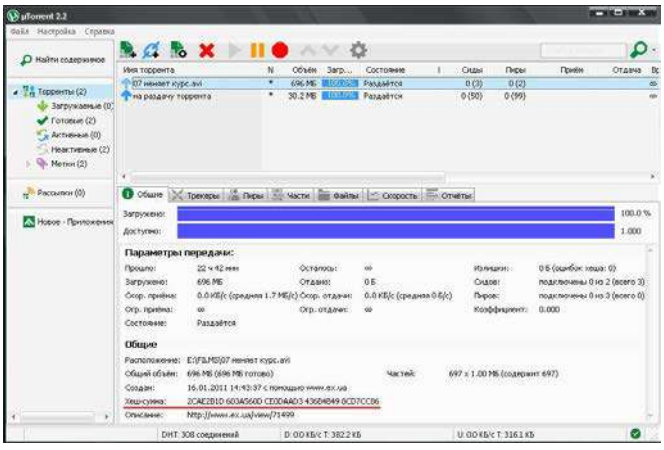


Рис. 1.4. Перевірка скачаного файлу на помилки

Цей метод легко доповнити до захисту від фальсифікації переданої інформації (метод MAC). У цьому випадку хешування проводиться криптостійкою функцією над повідомленням, об'єднаним із секретним ключем, відомим тільки відправнику й одержувачу повідомлення. Таким чином, криптоаналітик не зможе відновити код за перехоплених повідомлень і значення хеш-функції, тобто не зможе підробити повідомлення.

- ***Прискорення пошуку даних***

Наприклад, під час запису текстових полів у базі даних може розраховуватися їх хеш-код і дані можуть міститися в розділі, що відповідає цій хеш-функції. Тоді при пошуку даних необхідно буде спочатку обчислити хеш-код тексту і відразу стане відомо, в якому розділі його потрібно шукати, тобто шукати треба буде не серед усієї бази, а лише в одному її розділі (це сильно прискорює пошук).

Побутовим аналогом хешування в цьому випадку може слугувати розміщення слів у словнику за алфавітом. Перша літера слова є його хеш-кодом і при пошуку ми переглядаємо не весь словник, а тільки потрібну літеру.

Місцезнаходження хешів

На вашому комп'ютері містяться хеші паролів доступу до системи всіх користувачів. У системі Windows XP їх можна подивитися в такому файлі:

`C:\windows\system32\config\SAM`

Цей файл шифрується утилітою syskey для покращення захисту паролів. Інформація для розшифрування паролів міститься у папці:

`C:\windows\system\config\`

Ці папки недоступні жодному з користувачів. Доступ до них має тільки операційна система під час роботи, але переглянути їх можна за допомогою деяких програм (які вміють робити копії файлів – так звані «дампи») або в тому випадку, коли на комп'ютері завантажена інша операційна система.

Злом хешів

Нині для зберігання паролів практично в усіх операційних системах та інших програмних продуктах і інтернет-ресурсах використовуються хеш. Найпоширеніші алгоритми хешування в таких системах: LM, NTLM, MD5, SHA1, MYSQLSHA1, HALFLMCHALL, NTLMCHALL, ORACLE-SYSTEM, MD5-HALF. Перші два наведених алгоритми використовуються операційною системою Windows для зберігання паролів користувача. MD5, SHA1 на сьогодні є найстійкішими криптографічними хешами і можуть використовуватися в різноманітних системах доступу. Сфера застосування інших алгоритмів зрозуміла з їх назви.

У Мережі можна відшукати досить багато онлайн-сервісів, що дають змогу зламувати хеші. Одним з них є вже згаданий сервіс відновлення паролів passcracking.ru.

Спробуємо відкрити наш нещодавно вирахований хеш MD5 (рис. 1.3) для слова «ааа» і отримуємо (рис. 1.5):

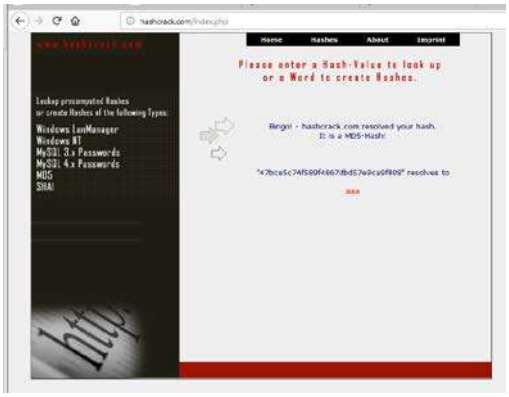


Рис. 1.5. Знаходження слова за хешем MD5

Список найбільш популярних on-line-ресурсів для злому хешів:

- crackstation.net[6];
- crackfor.me[7];

[6] https://crackstation.net/
[7] http://crackfor.me/

- md5.rednoize.com[8];
- md5.crysm.net[9];
- onlinehashcrack.com[10].

Отже, ми бачимо, що злом хешів є чи не найголовнішою задачею для злому систем.

Для цього хакери використовують 3 основні підходи:

A. Метод грубої сили (від. англ. Brute-force). Під цим методом розуміють послідовний перебір усіх можливих комбінацій біт, поки не буде знайдена потрібна. Цей підхід, теоретично, дає змогу відшукати пароль будь-якої складності, але він має один значний недолік – час. Наприклад, для злому пароля, який складається лише з малих латинських літер та цифр, при швидкості перебору 100 000 паролей за секунду буде потрібно:

Кількість знаків	Кількість варіантів	Час перебору
1	36	менше секунди
2	1296	менше секунди
3	46 656	менше секунди
4	1 679 616	17 секунд
5	60 466 176	10 хвилин
6	2 176 782 336	6 годин
7	78 364 164 096	9 днів
8	$2{,}821\ 109\ 9 \times 10^{12}$	11 місяців
9	$1{,}015\ 599\ 5 \times 10^{14}$	32 роки
10	$3{,}656\ 158\ 4 \times 10^{15}$	1162 роки
11	$1{,}316\ 217\ 0 \times 10^{17}$	41 823 роки
12	$4{,}738\ 381\ 3 \times 10^{18}$	1 505 615 років

Цей метод отримав новий приплив прихильників після появи так званих ботнетів – хакерських розподілених систем обчислення. Якщо в такому ботнеті буде 10 комп'ютерів, що одночасно зламують один і той самий пароль – то і час відповідно скоротиться в 10 разів! Очевидно, що цей екстенсивний метод усе одно прийнятний лише для паролів довжиною до 12 символів.

B. Метод перебору за словником. Нині це найпоширеніший метод взлому. Метод, як і попередній, послідовно перебирає паролі, але робить це не всліпу (всі можливі комбінації), а за списком можливих комбінацій – словником. Найчастіше захиститися від такого методу можна використовуючи паролі, що не мають відповідності з словами будь-якої мови. Крім того, не підходить для створення пароля і такий підхід, як набір слова на іншій розкладці клавіатури чи стандартна транслітерація. Ці підходи на сьогодні досить відомі і в найкращому випадку лише затримають зловмисника, але не зупинять.

C. Метод Reinbow (офіційний сайт project-rainbowcrack.com[11]). Цей метод є різновидом методу грубої сили. Під час злому пароля не просто перебираються всі можливі комбінації, а й зберігаються паролі, які не підходять, у файл. Таке архівування паролів дозволяє досить швидко відшукати потрібний пароль, якщо він хоча б один раз був згенерований системою злому.

Проте такий метод, крім досить значного часу, вимагає ще й гігабайтів пам'яті для зберігання паролів, але надає можливість використати витрачений машинний час неодноразово (рис. 1.6).

[8] http://hashtoolkit.com
[9] http://ww31.md5.crysm.net/
[10] https://www.onlinehashcrack.com/
[11] http://project-rainbowcrack.com/index.htm

Користуючись можливістю, хочемо дати такі поради:

- Завжди використовуйте стійкі паролі довжиною не менше 8 символів різного регістру, спеціальні символи та цифри. Це значно затримає злом і захистить вашу інформацію.
- Досить корисно буде використати як першу літеру символ із середини алфавіту – це затримає злом методом грубої сили, оскільки пароль типу 00000000 зламується миттєво будь яким методом, бо він перший! Наприклад, надійним паролем буде щось на зразок «**к%гЦ4Р*у!Й**».
- Не забувайте змінювати свої паролі хоча б раз на місяць і не використовувати однакові паролі для доступу в різні системи.

Rainbow Tables

LM Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
lm_ascii-32-65-123-4#1-7	ascii-32-65-123-4	1 to 7	7,555,858,447,479	99.9 %	27 GB 32 GB	Perfect Non-perfect	Perfect Non-perfect

NTLM Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
ntlm_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	52 GB 64 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	460 GB 576 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	127 GB 160 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	690 GB 864 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	65 GB 80 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	316 GB 396 GB	Perfect Non-perfect	Perfect Non-perfect

Рис. 1.6. Частина таблиць методу Reinbow для завантаження

1.3. Створення пароля, який легко запам’ятати

Про важливість створення надійних і різних паролів нині стверджувти не доводиться. У кожного сучасного користувача Інтернету існують декілька поштових скриньок, акаунти в соціальних мережах, на форумах та інших різноманітних ресурсах.

І хоча паролі тепер зазвичай ніде не зберігаються у відкритому вигляді, а використовується їх хешування – це ще не гарантія повної безпеки їх зберігання.

Одне з найголовніших правил – використовувати скрізь різні паролі і не використовувати як пароль імена знайомих, дітей та дати народжень (у сучасному світі їх можна досить нескладно дізнатися, використовуючи соціальні мережі або методи соціальної інженерії), прості слова (можуть бути дібрані за словником), комбінації типу «12345» тощо (рис. 1.7).

Існує багато рекомендацій щодо створення, зберігання, запам’ятовування паролів. Хтось використовує хмарні сервіси типу LastPass і KeePas (але все одно потрібно створювати один майстер-пароль), хтось користується генераторами паролів і просто вивчає їх, хтось іде своїм шляхом.

Розглянемо кілька методик для створенню пароля, який легко запам’ятовується.[12]

Придумайте фразу, яку ви точно не забудете, наприклад «Я живу на планеті Земля» (для прикладу обрано не дуже довге речення, на практиці рекомендується вибирати більш довге, наприклад, куплет з вашої улюбленої пісні). Вибравши по першій (можна й останній) букві з кожного слова, можна отримати «яжнпз». Міняючи регістр через букву вже отримаємо «ЯжНпЗ». Замінюючи букви на цифри, додаючи спецзнаки можна отримати «ЯжНп3!». Останній крок – переведення в транслітна англійську, тому що бажано все-таки використовувати англійські паролі (раптом колись виникне необхідність ввести пароль і не буде доступу до кириличної розкладки).

Рис. 1.7. Паролі, які прості, але не завжди надійні

У результаті отримаємо ось такий пароль – «YAzhNp3!». Такий пароль на перший погляд складний, але, знаючи методику його створення, дуже легко запам’ятати.

Проаналізувавши багато рекомендацій, були зроблені такі узагальнення для створення стійких паролів, які легко запам’ятовуються:

- Використовуйте в паролі антоніми, синоніми і омоніми тощо в різних комбінаціях з розділовими знаками і цифрами («молодийдідусь18років», «svitlo! Темний», «собака = @»);
- Використовуйте формули і вирази («12!=12.1», «@die('hard')», «echo$string»).
- Використовуйте несправжні адреси електронної пошти («Ya.Krevedko@ya.ya»).
- Використовуйте рими в паролі («google'shmugl», «HABRa_kadabra»);
- Повторення («http://http://double_pass», «zloe_zlo»);
- Візуалізація («Зомбі_виїли_мені_мо3г», «КуКла.Даша.плачет»);
- Перебільшення («25_годин_ранку», «Кличк’аВмери!», «ПочухайМЕНІшлунок»).
- Один з найнадійніших способів запам’ятати пароль – багаторазово набрати його на клавіатурі

[12] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1234-samples-vhdl-create-a-password-that-is-easy-to-remember-practical-advice

Ще одним варіантом створення пароля, що легко запам'ятовується, може бути банальне словосполучення з 3 різних слів, нічим не пов'язаних між з собою. Підібрати такий пароль перебором практично неможливо (займе дуже багато часу). Приклад такого пароля – «let's do our hometask kgb». Якщо використовувати пробіли в паролі заборонено, то його можна замінити на «_» або іншим будь-яким знаком/цифрою. У статті The Usability of Passwords[13] наводиться така ілюстрація по стійкості паролів (рис. 1.8) (у статті передбачається, що використовується підбір пароля на веб-сервісах, на яких у будь-якому випадку існують обмеження щодо частоти введення пароля й існують паузи між спробами введення паролів):

Type	Password	Method	Time	Security level
6 random characters	jskerv	Brute-force	1 month	risky
6 random characters with numbers	ergs43	Brute-force	8 months	Low risk
6 random characters with mixed case, symbols and numbers	J4fS<2	Brute-force	219 years	Secure for life
6 character common word	orange	Common words	3 minutes	useless
6 character uncommon word	woosaa	dictionary	1 hour 22 minutes	useless

Type	Password	Method	Time	Security level
2 common word password	alpine fun	Common word	2 months	Low risk
3 common word password	this is fun	Common word	2,537 years	Secure forever

Рис. 1.8. Стійкість паролів до злому

Дуже популярним на пострадянському просторі є набір речення російською при латинській розкладці, коли «всім привіт як справи» виглядає як «dcsv ghbdsn zr cghfdb». Це теж хороший спосіб створення пароля, який легко запам'ятовується, але може виявитися летальним, якщо Ви забудете розташування символів на російській розкладці, коли її не виявиться під рукою. Також незручно вводити з телефону і багато програм підбору паролів цей спосіб вже враховують.

Ще один із способів, коли доведеться досить легко запам'ятати пароль – скористатися генераторами паролів, які враховують властивість пам'яті людини.

Не забувайте, що за рекомендаціями фахівців інформаційної безпеки, паролі потрібно змінювати раз в 3-4 місяці. Але також варто пам'ятати, що зайва параноя теж не приводить до добра. Звичайно для найважливіших і критичних даних (основна пошта, доступ в інтернет-банкінг) варто використовувати самі надійні паролі, а на сайтах, де ви реєструєтеся один раз і навряд чи туди будете часто повертатися – можна вводити і більш прості паролі.

Якщо паролі для сайтів складні, то можливо використовувати майстер-паролів (Firefox, Opera), щоб кожного разу не вводити паролі повністю. Проте, розробники Google Chrome вважають, що майстер-пароль створює оманливе враження про свою безпеку і такої функції в Google Chrome на даний момент немає. Виправити дану ситуацію можна, скориставшись розширенням LastPass[14], яке крім автоматизації створення складних паролів на будь-яких веб-ресурсах, має функцію майстер-пароля.

Також деякі сучасні браузери (Google Chrome, Firefox, Opera) підтримують синхронізацію паролів між різними ПК, використання сервісу LastPass і йому подібних дозволяє синхронізувати свої паролі не тільки на різних комп'ютерах, але і в різних браузерах і навіть мобільних пристроях.

[13] https://www.baekdal.com/insights/password-security-usability
[14] https://chrome.google.com/webstore/detail/lastpass-free-password-ma/hdokiejnpimakedhajhdlcegeplioahd?hl=uk

А щоб паролі ніхто «не витягнув» є ще один цікавий спосіб: запам’ятовувати при використанні майстер-паролів пароль не повністю, а залишити 3-4 символи для «додруковування» вручну в кінці пароля при його автоматичному введенні. І запам’ятати ці символи легко, і ніде ваш пароль не буде зберігатися в повному вигляді.

1.4. Гра в хованки або стеганографія для захисту інформації

Сьогодення неможливо уявити без обміну інформацією. Ми відсилаємо повідомлення електронною поштою, через телефон, спілкуємося на фейсбуці, твітерим останні новини, постійно залишаючись відкритими для оточуючих.

У всьому цьому хаосі легко простежити за Вашим життям, створити психологічний портрет та навіть пізнати таємниці особистого життя. Що ж робити тим, хто хоче сховатися від контролю?

Безумовно, всі майже відразу згадують про шифрування, але сам факт шифрування насторожує і привертає увагу зловмисника. Тут нам на допомогу приходить метод стеганографії.[15] В контексті захисту інформації – це можливість пограти в хованки таким чином, щоб сховати сам факт існування прихованої інформації.

Які ж головні допущення та принципи побудови стеганосистеми?

- противник має повне уявлення про стеганографічну систему і деталі її реалізації. Єдиною інформацією, яка залишається невідомою потенційному супротивникові, є ключ, за допомогою якого тільки його власник може встановити факт присутності і зміст прихованого повідомлення;
- якщо противник якимось чином дізнається про факт існування прихованого повідомлення – це не повинно дозволити йому отримати подібні повідомлення з інших даних доти, поки ключ зберігається в таємниці;
- потенційний противник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

Будь-яка стеганосистема повинна відповідати наступним вимогам:

- Властивості контейнера – носія інформації повинні бути модифіковані, щоб зміни було неможливо виявити при візуальному контролі. Ця вимога визначає якість приховування впроваджуваного повідомлення: для забезпечення безперешкодного проходження стегоповідомлення через каналу зв’язк, воно жодним чином не повинно привернути увагу атакуючого.
- Стеганоповідомлення має бути стійким до спотворень, в тому числі і зловмисних. В процесі передачі зображення (звуку або іншої інформації) можуть відбуватися різні трансформації: зменшуватися або збільшуватися, перетворюватися в інший формат і т. д. Крім того, воно може бути стисненим, в тому числі і з використанням алгоритмів стиснення з втратою даних.
- Для збереження цілісності вбудованого повідомлення необхідне використання коду з виправленням помилки.
- Для підвищення надійності вбудовуване повідомлення має бути продубльоване.

Найпоширенішими контейнерами для методів стеганографії на сьогодні є файли зображень та відеофайли. А програми для практичної реалізації данного методу захисту інформації можна знайти в Інтернеті.

Найбільш наглядними є програми, які дозволяють приховати деяке повідомлення всередині зображення.

Найрозповсюдженішим методом, який дозволяє приховувати повідомлення в графічних файлах, є метод НЗБ (найменшого значущого біта). Чому саме він? Тому що це один з

[15] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1283-the-game-of-hide-and-seek-or-steganography-in-modern-life

найпростіших методів цифрової стеганографії, який дозволяє створити прихований канал з досить великою пропускною здатністю без суттєвої втрати якості контейнера.

Цей метод приховування даних із спотворенням контейнера базується на особливостях людського сприйняття. Конкретніше, ідея методу полягає ось у чому: якщо взяти картинку у форматі BMP, найкраще TrueColor, в 24-х бітному форматі та змінити молодші значущі біти кольору, то на око це не буде помітно. Чому 24 біта? Існує такий важливий фактор, як обсяг контейнера – скільки всього можна вставити в картинку, поки це не стане явним. Логічно припустити, що чим більший контейнер, тим більше можна і втиснути, а поширені на сьогодні 24-х бітні BMP – насприятливіші для цього.

До того ж 24 біта є зручним форматом зберігання інформації про зображення. При такому поданні за один канал кольору відповідає один байт, цим усі і користуються.

Здійснити перетворення можна так:

- Беремо повідомлення і попередньо готуємо його: шифруємо і пакуємо. Цим досягається відразу дві мети – підвищення ККД та збільшення стійкості системи. Перед усім, для зручності можна записати сигнатуру методу, що не є таємницею, зате просто.
- Беремо контейнер і впроваджуємо підготовлене повідомлення в молодші біти контейнера будь-яким зручним для нас способом. Наприклад:
    - розкладаємо упаковане повідомлення в бітову послідовність;
    - замінюємо надлишкові біти (НЗБ) контейнера бітами повідомлення.

Надійність такого втиснення прямо пропорційна відповідності характеру розподілу НЗБ в контейнері і повідомленні. А ці розподіли в переважній більшості випадків збігатися й не будуть. Хоча в деяких випадках це буде візуально помітно на картинці, побудованій з одних тільки молодших бітів контейнера

Назва програми	**Можливості**	**Переваги**	**Недоліки**	**ОС**
OutGuess (ver. 0.2)	Приховування даних в JPEG зображеннях.	Можливість контролю, «внесення статистичних спотворень», більша стійкість до атак.		UNIX
JSTEG			Нестійкість до атак пасивних противників, можливість автоматичного детектування наявності прихованого повідомлення.	MS-DOS UNIX Windows
JPHS (ver. 0.5)				
Gifshuffle (ver. 2.0)	Приховування даних в графічних файлах в форматі GIF.	Можливість попереднього стискання чи шифруваня повідомлення, що шифрується.	Невеликий об’єм повідомлення, яке приховується. Залежить від розміру контейнера.	UNIX Windows
Hide-and-Seek		Використовуючи алгоритм шифрування “Blowfish”, виконує випадковий вибір точок збереження.		MS-DOS Windows
Steganos	Приховування даних в графічних файлах BMP, DIB.	Заповнення невикористаного простору контейнера шумоподібним сигналом.	Використання застарілих форматів контейнерів.	
Steghide (ver. 0.5.1)	Приховування даних в графічних BMP.	Можливість попереднього шифрування повідомлення, що приховується.		MS-DOS Linux Windows

Steganography 1.8.1	Приховування даних в графічних файлах.		Відсутність розподілення інформації, що приховується по контейнеру, відсутність попереднього аналізу контейнера на придатність.	Windows
Fox Secret 1.0		Можливість попереднього шифрування повідомлення, що приховується.		

Використання методу стеганографії продемонструємо на прикладі програми Fox Secret 1.0[16].

За допомогою цієї невеликої програми, яка орієнтована для використання з операційною системою Windows, спробуємо показати зміни, які відбудуться з зображенням після втиснення в нього повідомлення. Завантажити дану програму можна за посиланням, наведеним внизу сторінки.

Після запуску програма має аскетичний вигляд (рис. 1.9):

Рис. 1.9. Запуск програми Fox Secret 1.0

Спробуємо щось приховати. Обираємо меню *Секрет/Новий*. Відкривається вікно (рис. 1.10):

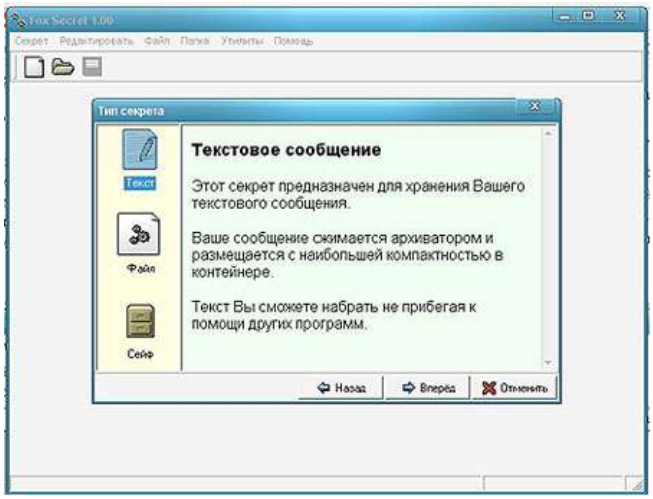


Рис. 1.10. Запуск процесу шифрування

Спробуємо приховати текст. Для цього обираємо *Текст* і тиснемо кнопку *Вперёд* (рис. 1.11).

[16] http://www.softportal.com/software-4962-fox-secret.html

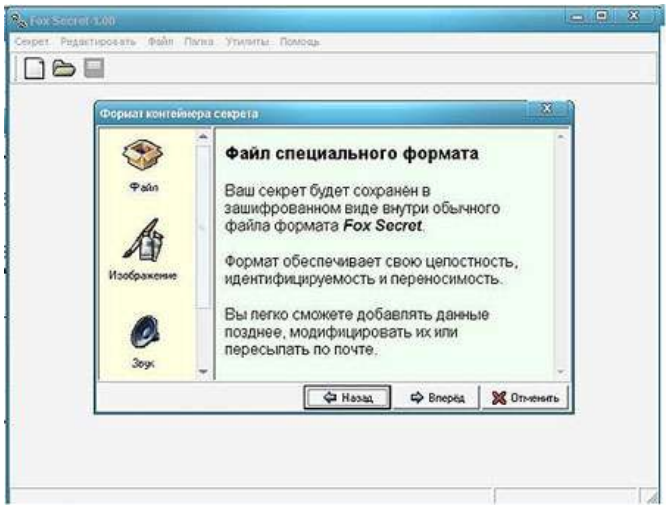


Рис. 1.11. Приховування тексту

Обираємо *Изображение* і натискаємо *Вперёд*. Обираємо зображення для контейнера і натискаємо *Сохранить* (рис. 1.12):

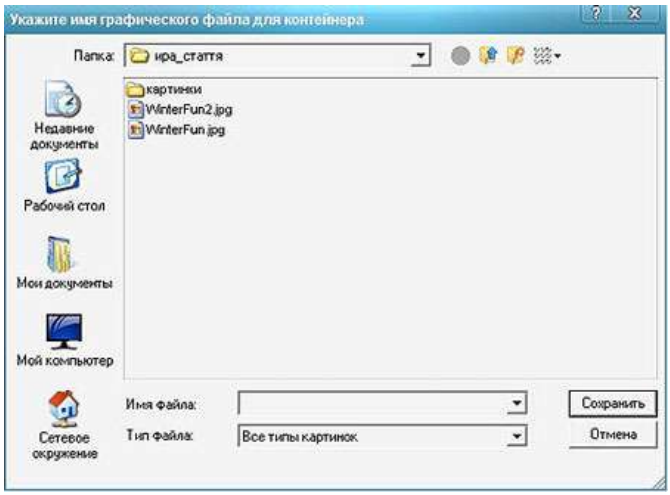


Рис. 1.12. Вибір зображення для контейнера

Нам дозволяють зашифрувать приховані дані. Зверніть увагу на місткість контейнера. Вона вказує, що дані будуть приховуватися або в коментарі файла JPEG, або в кінці шляхом дописування.

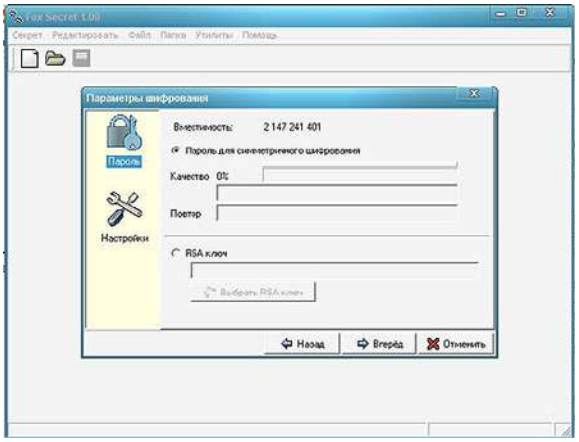


Рис. 1.13. Додавання парольного захисту повідомлення

Вводимо пароль і натискуємо *Вперёд* (рис. 1.13). Після цього в вікні, що відкрилося, вводимо текст, який хочемо приховати (рис. 1.14), натискаємо *Сохранить*.

Рис. 1.14. Введення тексту, який приховуємо

Картинка, в якій схований файл, і оригінал мають наступний вигляд (рис. 1.15):

А)  Б) 

Рис. 1.15. Зображення з повідомленням (А) і оригінал зображення (Б)

Зміни неозброєним оком безумовно не помітні. Тепер спробуємо дістати інформацію, яка прихована в нашому зображенні. Для цього натискаємо *Секрет>Открыть*. Обираємо картинку, в якій ми приховали файл, і вводимо пароль. Натискаємо *Впёред* (рис. 1. 16).

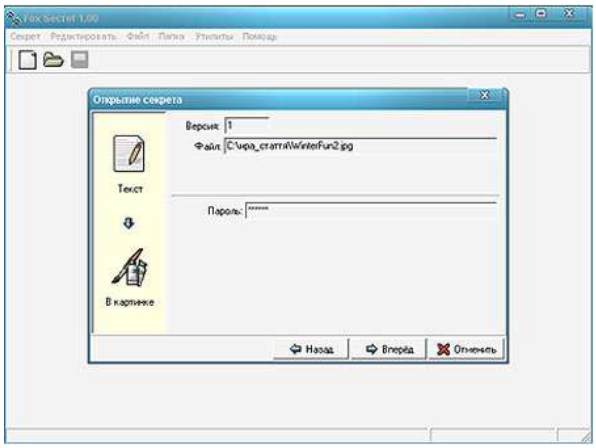


Рис. 1.16. Дістаємо повідомлення з контейнера

В результаті відкривається прихований нами текст (рис. 1.17):

Рис. 1.17. Отримуємо прихований текст

Отож навіть за допомогою такої простої в користуванні програми, як Fox Secret 1.0 ви можете приховати важливі для вас дані. І ніхто навіть не запідозрить сам факт присутності повідомлення! А тепер зверніть увагу, що на Фейсбук щодня додається понад 350 млн. нових фотографій…

1.5. Зберігаємо таємниці в хмарах

Dropbox – для файлів, Google – для пошти, iCloud, ну ... для всього іншого!

Середньостатистичний громадянин має всі можливі варіанти для зберігання своєї інформації в «хмарі». Тепер, і шпигуни хочуть того ж. Скоро, всі секрети країни зможуть зберігатися в «досить хмарній» формі.[17]

In-Q-Tel, інвестиційний відділ ЦРУ і американське співтовариство розвідки, з недавнього часу почав «затоплювати» гроші в компанію хмарного зберігання даних, що називається Cleversafe. Як заявлено в ЦРУ, платформа ідеально підходить для зберігання критично важливих даних, звертаючись до основних принципів конфіденційності, цілісності та доступності даних. (До речі, про ці принципи так само заявляло ЦРУ).

І це лише одна з безлічі нових державних ініціатив по використанню «хмарних сервісів». Починаючи з минулого року, адміністрація США прийняла політику «cloud first» (дослівно, «спочатку хмари»), яка заохочує рішення на основі хмарних технологій, «всякий раз, коли існує безпечний, надійний та економічно-ефективний хмарний варіант». Пентагон вже планує переходити на хмарні технології, а очікуваний протягом декількох тижнів «Акт переходу на хмарні обчислення 2011» («2011 Cloud Computing Act») може породити ще більше стимулів для інвестування коштів у хмарні технології.

Але цей рух «вгору» приносить с собою всі види проблем безпеки, особливо для ЦРУ, яке все ще страждає від недавнього злому їх публічного веб-сайту. У той час як ішли гучні дебати з безпеки хмарних методів зберігання інформації проти більш традиційних форм зберігання, в Cleversafe були впевнені, що дані з ними будуть у безпеці. І це добре, тому що уряд хотів би запобігти «чергового Бредлі Меннінга», який зливає всі їхні таємниці в WikiLeaks.

Генеральний директор Cleversafe, Кріс Гледвін (Chris Gladwin), розробник програмного забезпечення з ухилом на криптографію з Чикаго, каже, що безпечний метод хмарного зберігання даних вже був відомий протягом тривалого часу. Вперше написаний на папері 1979-го року метод «Як розподілити секрети» («How to Share a Secret») досить простий: «Візьміть якусь інформацію, потім пропустіть її через певні математичні алгоритми, що розділяють її на купи шматочків вихідних даних, нічого не значущих поодинці».

Аналогічна цьому методу технологія «розосередження інформації» і використовується: Cleversafe бере масивні обсяги даних, нарізає їх на частини і потім розподіляє зберігання з різних розташуванням, або «версія сайтів зберігання». Хоча дані можуть перебувати в чотирьох різних дата центрах по всій країні, вони можуть бути доступні в реальному часі з «окремих хмар». І на відміну від традиційних методів зберігання, немає ніякої необхідності, робити кілька копій вихідних даних, що заощаджує місце і кошти.

За заявою Кріса Гледвін, є ще кілька переваг даного виду зберігання даних. По перше – це конфіденційність: окремі шматочки даних не можуть бути розшифровані самі по собі, навіть якщо стороння особа отримало декілька таких частин. По друге – це надійно: навіть якщо який-небудь з дисків, на яких лежить один зі шматочків, був пошкоджений, випав в

[17] http://isearch.kiev.ua/uk/news/internet/1066-spycloud-cleversafe

offline, або просто загубився, є чимала ймовірність відновлення всього файлу з наявних частин. Малоймовірно, щоб 10 серверів або дисків відмовили одночасно.

In-Q-Tel впевнені, що Cleversafe «дасть нашим клієнтам у розвідувальному співтоваристві потужні засоби розподіленого зберігання даних, які забезпечать рівні неперевершеної надійності, які вони вимагають».

З тих пір, як виділений в США державний бюджет на IT склав небагато-немало 20 мільярдів доларів на розвиток хмарних технологій, варто чекати, що незабаром й інші структури, ймовірно, підуть в цьому ж напрямку.

Найчастіше сервіси, які надають місце для зберігання даних (DropBox, Google Drive, Microsoft SkyDrive, iCloud), мають можливість не тільки зберігати дані, а й мають розширений функціонал, який дозволяє редагувати файли всередині хмари, контролювати зміну файлів, давати загальний доступ до файлів і т. д.

Однак, в багатьох сервісах не вказано наскільки добре захищені ваші дані. В наш час інформація коштує грошей, і найчастіше – чималих.

Одним з сервісів, який позиціонує себе як найбільш захищене хмарне сховище даних є SpiderOak.[18]

У SpiderOak[19], як в захищеному хмарному сховище даних використовується комбінування 2048 біт RSA з 256 біт AES. Ключі зовнішнього рівня зберігаються не у відкритому, а в зашифрованому 256 бітним AES-ключем, який був виведений алгоритмом PBKDF2, використовуючи 16384 цикли і 32 байт випадкової інформації. Даний метод запобігає злому пароля методом брутфорс. Без пароля дані, що знаходяться на сервері, прочитати неможливо.

Для економії місця в історії зміни файлів використовується метод дельта – кодування, при якому записуються тільки ті частини файлу, які були змінені

Головна сторінка проекту захищеного хмарного сховища не проти гучних слів, що не применшують його переваг (рис. 1.18).

На головній сторінці можна прочитати наступні слова: «*Наша політика конфіденційності «Нульове знання» гарантує, що ми ніколи не зможемо побачити Ваші дані. Ні наші співробітники. Ні уряд. Ніхто …*»

Також сказано: «*ВОНИ (інші файлові сховища) можуть бачити ВСІ Ваші дані. Ми бачимо НУЛЬ*»

Рис. 1.18. Головна сторінка проекту

Сайт одразу пропонує зареєструватися, що займає менше хвилини (рис. 1.19). Після того, як всі поля заповнені, почнеться завантаження клієнта SpiderOak.

[18] http://isearch.kiev.ua/uk/news/programs/tools-sec/1596-spideroak-secure-cloud-storage-data
[19] https://spideroak.com/

Рис. 1.19. Вікно реєстрації

Установка проста і зрозуміла. Після установки програма запропонує перезавантажити комп'ютер.

Після перезавантаження запускаємо SpiderOak. Вводимо логін, пароль. Є можливість зайти в програму, використовуючи проксі, що також підвищує анонімність та безпеку. Далі, програма просить ввести ім'я комп'ютера, на якому вона запущена.

При першому запуску програма пропонує зробити резервне копіювання робочого столу, документів, фільмів, музики і картинок зі стандартними шляхами.

У вікні програми видно декілька вкладок: STATUS, BACK UP, VIEW, SYNC, SHARE. Розглянемо кожну з них.

STATUS (рис. 1.20)

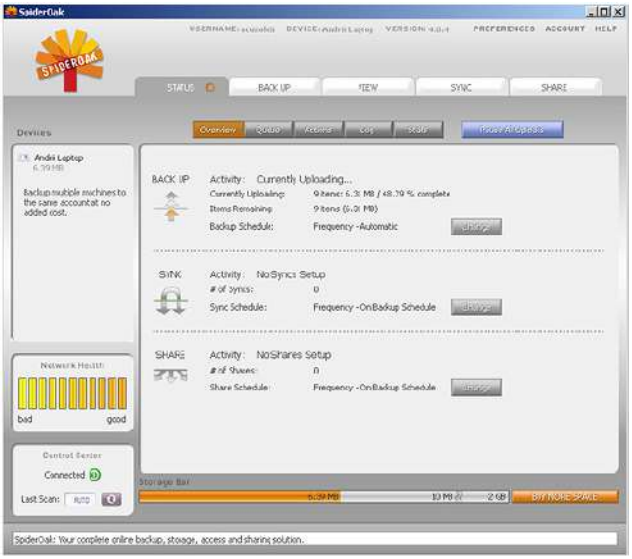


Рис. 1.20. Вкладка STATUS

На цій вкладці в підвкладці Overview можна спостерігати за станом резервного копіювання, синхронізації або роздачі даних.

Кожну з цих функцій можна налаштувати на певний час роботи, натиснувши на кнопку Change (змінити).

Також в цій вкладці є такі підвкладки, як:

- Queue (черга) – показана чергу файлів, які очікують виконання дій,
- Actions (Дії) – відображення подій, які виконуються у Вашому акаунті,

- Log – журнал,
- Stats – статистика.

BACK UP

Вкладка дозволяє вибрати теки і файли, для яких буде виконуватися резервне копіювання (рис. 1.21). При натисканні на кнопку Advanced можна вибрати шляхи, відмінні від стандартних.

Рис. 1.21. Вкладка BACK UP

VIEW

У цій вкладці можна переглядати дерево даних, завантажених в SpiderOak, а так само завантажувати файли використовуючи менеджер завантажень.

SYNC

Виберіть дві папки, які ви хочете синхронізувати. Можна створити кілька правил для синхронізації.

SHARE

Дуже цікава і корисна функція SpiderOak, якщо Ви хочете поділитися деякими своїми файлами. Просто виберіть файли і введіть назву, яка буде в URL. Програма сама згенерує адресу, яка буде виглядати наступним чином:
`https://spideroak.com/browse/share/загальне_ім'я_вашої_шари/ім'я_для конкретного_правила.`

Ви можете створити кілька правил, додаючи різні папки, так що різним людям може бути даний доступ до різних файлів.

Жодне захищене хмарне сховище не може дати 100% гарантію безпеки і захищеності. Тому, наприклад, співробітникам компанії IBM заборонено використовувати хмарні сховища для корпоративних цілей. Але можна постаратися звести ризик до мінімуму, використовуючи такі безпечні хмарні сховища, як SpiderOak.

1.6. Захист поштових сервісів

Якщо Ви віддаєте перевагу використанню веб-інтерфейсів, які передбачені в Gmail, Hotmail або Yahoo!, то, мабуть, знаєте, що не можна реально захистити свої дані при безпосередньому їх використанні.

Більшість популярних сервісів веб-пошти не підтримують шифрування електронної пошти, яке, наприклад, захищатиме зміст повідомлень від читання автоматизованими засобами і будь-ким іншим, хто отримає доступ.

Mailvelope[20] – безкоштовне розширення для браузерів Google Chrome і Mozilla Firefox, яке вводить шифрування OpenPGP для сервісів веб-пошти, якими ви можете користуватися.[21] Розширення поставляється з підтримкою за замовчуванням Gmail, Yahoo! Mail, Outlook і GMX, а також варіантами для інтеграції інших веб-постачальників послуг електронної пошти.

Встановлення трохи складніше, особливо якщо ви раніше ніколи не працювали з PGP. Після встановлення розширення у браузері треба вибрати: створити новий ключ шифрування чи імпортувати існуючий.

OpenPGP для послуг електронної пошти

Якщо вам необхідно створити новий ключ, то буде запропоновано ввести своє ім’я, адресу електронної пошти та пароль, який використовуватиметься для шифрування і розшифровування повідомлень. Якщо хочете, то також можете змінити алгоритм і розмір ключа (за замовчуванням 1024 і можна збільшити до 4096), та встановити термін придатності (рис. 1.22).

Вам потрібно імпортувати відкриті ключі співрозмовникам зі списку контактів, щоб ви могли шифрувати повідомлення для них.

Дозвольте пояснити, як працює процес шифрування. PGP використовує парну систему секретного і відкритого ключів. Коли ви створюєте новий набір ключів, то генеруєте приватний ключ і відкритий ключ. Інші використовуватимуть відкритий ключ для шифрування повідомлень для вас, які зможете розшифрувати тільки ви за допомогою свого секретного ключа.

Автор рекомендує вам перевірити налаштування, перш ніж запустити сервіс веб-пошти з вибором початку шифрування електронної пошти.

Деякі наступні цікаві варіанти, які у вас є:

1. Вибрати, хочете використовувати сформоване вікно сервісу веб-пошти чи окремий редактор.
2. Вибрати, хочете ви розшифровувати повідомлення на сторінці постачальника пошти чи в окремому вікні.
3. Встановити, чи хочете, щоб первинний ключ вибирався автоматично.

Тут ви також можете додати в список підтримуваних сервісів інші системи електронної пошти.

[20] https://www.mailvelope.com/de
[21] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1740-mailvelope-apply-openpgp-encryption-for-gmail-yahoo-hotmail-and-other-email-services

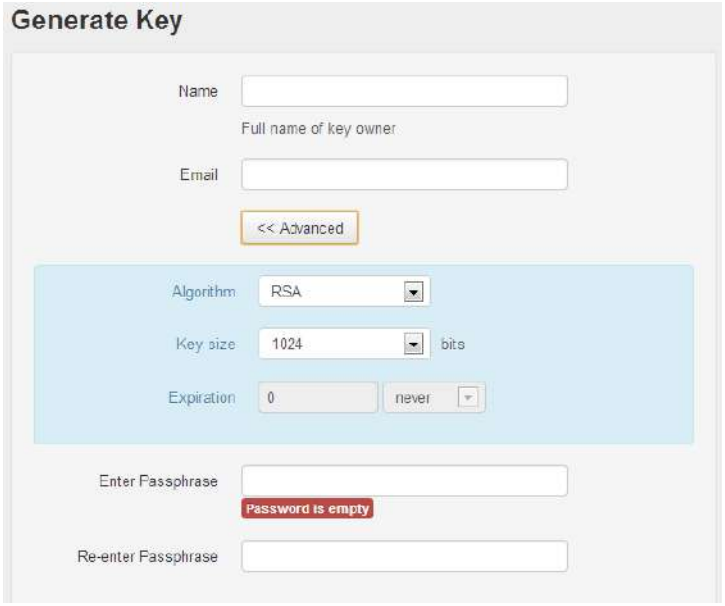


Рис. 1.22. Початкові налаштування OpenPGP

Новий значок буде відображатися у вікні створення повідомлення, як тільки ви додали хоча б один ключ для підтримуваної адреси електронної пошти. При натисканні на нього, з'являється нове вікно, яке дозволяє ввести повідомлення (рис. 1.23).

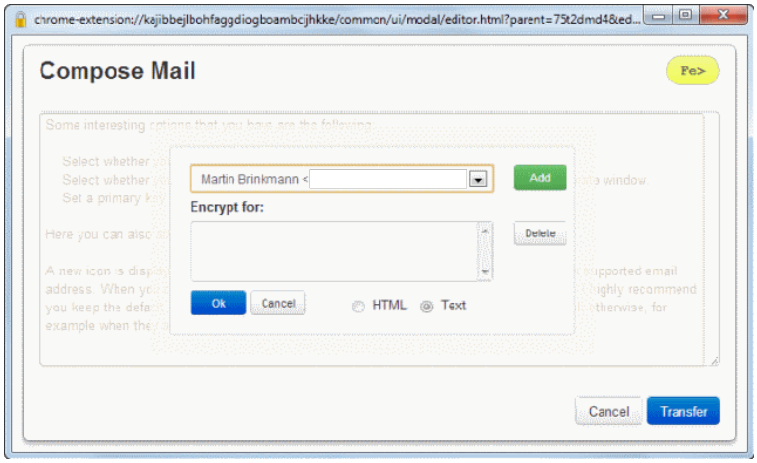


Рис. 1.23. Вікно введення повідомлення

Автор настійно рекомендує вам залишити вибір за замовчуванням введення листів в окремому вікні, бо в іншому випадку може відбутися витік, наприклад, коли листи автоматично зберігаються.

Після того, як ви натиснули на значок шифрування, можна вводити своє повідомлення. вам потрібно натиснути на значок **Fe>**, як тільки будете готові почати процес шифрування.

Що вам потрібно зробити – це вибрати одержувачів електронної пошти. Можна додавати тільки одержувачів, яким раніше були імпортовані відкриті ключі в додаток.

Після цього натиснути кнопку передачі, щоб відправити повідомлення всім вибраним одержувачам. Ви також можете додати себе в список і тоді зможете читати повідомлення у своїй папці відправки (і вхідних).

Зашифровані повідомлення з'являється в поштовій скриньці, як звичайні повідомлення. Вони мають звичайний текст заголовка, але тіло зашифроване. При відкритті зашифрованої електронної пошти, ви побачите випадкові символи і значок замка в середині.

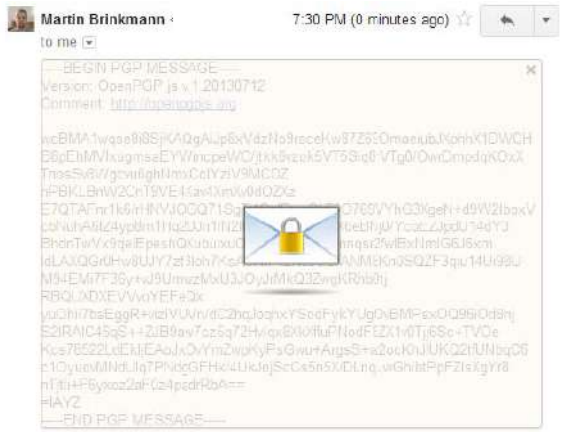


Рис. 1.24. Зашифрована PGP електронна пошта

Клацнувши на іконку, відкриєте вікно введення паролю. Ви повинні ввести правильний пароль, який ви обрали під час створення ключа. Електронна пошти буде відображатися у вигляді звичайного тексту, коли зробите це, щоб можна було лист прочитати.

Mailvelope додає дуже корисну функцію для послуг веб-пошти, але є кілька умов.

По-перше, треба, щоб ваші контакти почали використовувати PGP, тільки тоді ви зможете використовувати його ефективно.

По-друге, ви покладаєтеся на розширення Chrome або Firefox, а це означає, що ви не зможете отримати доступ до своєї електронної пошти в будь-який час. Наприклад, у випадку, якщо перевіряєте пошту в публічній бібліотеці або з чужого комп'ютера.

Також поточна реалізація не підтримує підписання повідомлень.

Хороша новина, однак, в тому що рішення повністю сумісне з існуючими шифруваннями пошти, що використовують OpenPGP.

В поштових сервісах та соціальних мережах можуть читати ваші повідомлення, якщо вони будуть в результатах внутрішнього пошуку. Особливо гостро дане питання постає при використанні корпоративних мереж та поштових скриньок.

Тому, якщо ви не бажаєте, щоб ваші колеги або інші сторонні особи стали свідками вашої переписки, необхідно повідомлення шифрувати. Для цього існує безліч таких програм, як Crypt&DeCrypt, fSekrit та безліч інших[22]. Недоліком всіх їх є те, що вони функціонують як окрема утиліта і тому дуже часто користуватися ними незручно. Хотілося, щоб даний шифратор знаходився безпосередньо в браузері.

І тут на допомогу може прийти дуже корисний букмарклет Encipher.it.[23] Представляє він собою звичайний Javascript.

Encipher.it буде шифрувати і захищати паролем ваші текстові повідомлення за допомогою симетричного шифрування, що використовує AES256 і PDBKF2 (Password-Based Key Derivation Function) для генерації ключів. Сам сайт використовує цифровий сертифікат SSL для захисту від атак MITM (Man In The Middle).

[22] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1270-safely-correspondence-its-easy
[23] https://encipher.it/

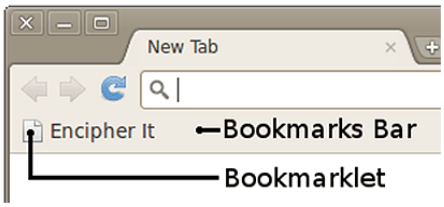


Рис. 1.25. Encipher.it на панелі

Встановлюється він елементарно – просто зберігаємо його в «Закладках», виносимо на головну панель браузера (рис. 1.25) і все, він готовий до використання.

Наприклад, для того щоб зашифрувати якесь повідомлення – просто необхідно його виділити та натиснути на іконку «Encipher.it», яка з'явилася на панелі браузера (рис. 1.26). У новому вікні, що з'явилось, вводимо ключ і повідомлення відразу ж зашифровується.

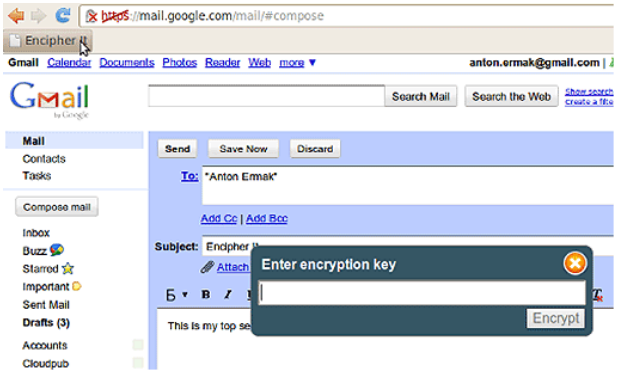


Рис. 1.26. Процес шифрування

Дешифрування відбувається аналогічно – виділяємо зашифрований текст, натискаємо на букмарклет, вводимо пароль і повідомлення розшифровується (рис. 1.27).

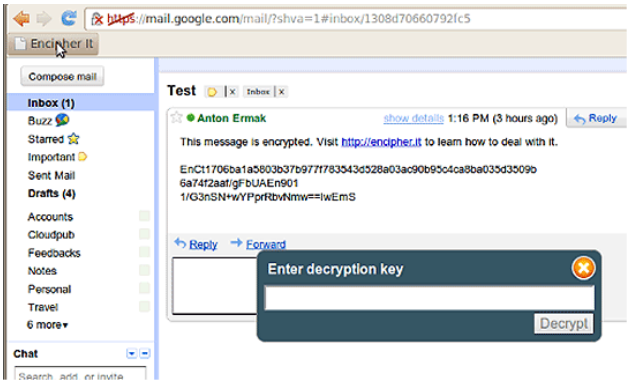


Рис. 1.27. Розшифровуємо повідомлення

Залишається лише домовитись з тим, з ким переписуєтесь, про спільний ключ. Звичайно, що для передачі ключа необхідно використовувати інший канал зв'язку, відмінний від того, в якому відбуватиметься переписка.

Шифрування і дешифрування відбувається повність на стороні клієнта.

Для користувачів Firefox дуже корисним може стати плагін LockTheText[24].

Принцип, за яким він працює, аналогічний. Для того щоб зашифрувати текст достатньо його виділити, після чого за допомогою правої кнопки миші визвати контекстне меню, де необхідно вибрати Lock The Text/Lock (рис. 1.28):

[24] https://www.hosoft.ru/plugins/firefox/lock-the-text-0.27

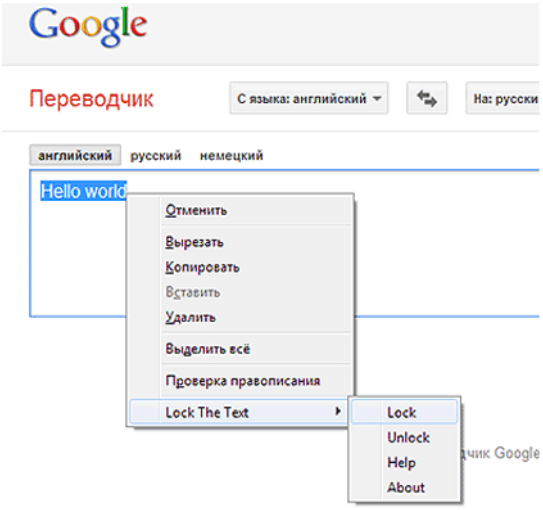


Рис. 1.28. Шифрування з LockTheText

У вікні, що з'явилось, вводимо ключ. Таким чином, ми отримуємо зашифроване повідомлення. Дешифрування відбувається аналогічно.

Однак найбезпечнішим методом переписки є перехід у невидимий Інтернет I2P, в якому можна скористатись послугою I2P-Mail.

При встановлені необхідного програмного забезпечення треба перейти у так званий «невидимий інтернет» I2P. Даний ресурс пропонує власного поштового клієнта або, як його ще називають, I2P-Mail, хоча різниці зі звичайною поштою ви не помітите.

Іншим поштовим сервісом в I2P є I2P-Bote.

Анонімна розподілена пошта – I2P-Bote значно відрізняється за своєю суттю від простої пошти, за архітектурою більш схожа на торренти, ніж на поштову систему звичайного Інтернету. Замість адреси e-mail використовуються хеші. Після відправлення, повідомлення розбивається на частини, шифрується і розподіляється серед інших версій сайту I2P-Bote. Як тільки одержувач з'явиться в мережі він отримає адреси (хеші) частин свого повідомлення і завантажить їх на комп'ютер. Так само, як і всі інші дані в I2P, повідомлення також будуть проходити ланцюжками тунелів. Використовувати поштові клієнти для роботи з I2P-Bote, зрозуміло, не можна – він вбудовується як плагін у веб-інтерфейс I2P-маршрутизатора. Саме така архітектура передачі даних робить переписку безпечною.

I2P-Bote на сьогодні, мабуть, самий зручний і безпечний спосіб обміну повідомленнями, якщо швидкість доставки повідомлення не важлива або треба відправити повідомлення одержувачу, якого наразі немає в Мережі.

Детальніше про мережу I2P в останньому розділі даного методичного посібника.

1.7. 5 речей, які потрібно знати про безпеку додатків Google

Як було розглянуто вище, користувачі все частіше переміщають свої дані в «хмарні» сховища, тому не буде зайвим подбати про безпеку цих даних.[25]

Звичайно, є й очевидні переваги зберігання документів онлайн: зниження витрат, миттєвий доступ, спільна робота і зростання популярності Google Docs... Але, незважаючи на все це, необхідно ставитися до даних, що зберігаються в хмарі, інакше, ніж до їх «фізичних побратимів».

«Руформатор» пропонує переклад п'яти порад з безпеки зберігання даних у «хмарі». Поради дає Гіл Циммерман (Gil Zimmermann), генеральний

[25] http://isearch.kiev.ua/uk/news/security/1058-5-things-to-know-about-the-safety-of-google-applications

директор «хмарної» компанії CloudLock, що забезпечує захист корпоративних даних, які зберігаються в Google Docs.

Контроль доступу тепер в руках користувача

Кінцеві користувачі отримують набагато більший контроль над такими даними заради спрощеної спільної роботи: модель Google Docs перекладає відповідальність за дані на самих користувачів. На користувачів, а не на IT-персонал, який зазвичай розпоряджається тим, які дані можна використовувати спільно. Тому, теоретично, інформація може бути випадково або навмисно надана як не тим людям всередині компанії, так і чужинцям за межами домену або в Інтернеті.

Розташування даних

У Google Apps інформація створюється користувачами і знаходиться в їхніх особистих облікових записах (на відміну від центрального сервера у Вашій компанії). Крім того, якщо обліковий запис вилучений, то видаляються і всі дані цього користувача. Вже немає поняття «центральний загальний файл-сервер», який знаходиться у віданні IT-департаменту. Компанії, які використовують Google Docs, повинні розуміти, які взагалі дані є у користувачів, перш ніж приймати рішення про видалення будь-яких акаунтів.

Розмежування доступу

Тим, хто використовує Google Docs, необхідно знати, хто ще має доступ до конфіденційних даних. Це необхідно не тільки для безпеки даних в середовищі спільної роботи, а й щоб контролювати, хто що робить, ну і за дотриманням регламенту теж. Моніторинг користувачів, які отримують доступ і використовують інформацію, стає критично важливим моментом у справі захисту даних від зловживань.

Витік даних

Ті, хто використовує Google Docs, повинні мати можливість періодичної перевірки своїх даних і отримання повідомлень тоді, коли необхідні якісь дії. Припустимо, що у компанії є надсекретний проект під назвою «Проект Monkeyfeet», і до нього повинен мати доступ тільки строго певний персонал. Компанія повинна бути попереджена будь-коли про доступ до проекта сторонніх і повинна мати можливість негайної зміни привілеїв користувачів. Це допомагає захистити дані від внутрішніх і зовнішніх загроз.

Втрата даних

Додатково до простого захисту своїх даних, користувачі повинні бути в змозі зберегти всі записи, перенести дані в міру необхідності і зробити резервні копії, не втрачаючи при цьому ні байта. Так як контроль за даними знаходиться в руках користувачів, компаніям необхідно захистити себе і користувачів від випадкових і зловмисних вилучень – тобто від людського фактора. Існує набагато більший ризик, що співробітник випадково видалить документ або адміністратор видалить користувача (разом з усіма даними, які у нього є), ніж «впаде» сама система Google Docs.

Але навіть у тих компаніях, які перейшли на Google Docs, системні адміністратори мають більше привілеїв, ніж раніше. У Google всі користувачі і їх дані сконцентровані в єдиній віртуальної локації: це великий смітник неструктурованих даних, які розповзлися по сотні мережних пристроїв. Крім того, ця інформація може бути отримана за допомогою звичайного доступу або за допомогою керуючого API. Деякі компанії можуть написати свої власні програми для інтеграції даних, що зберігаються в Google Docs, з іншими внутрішніми процесами й додатками.

Крім того, Google Apps Marketplace є справжньою кондитерською для IT-адміністраторів. Цей онлайн-магазин пропонує сотні сторонніх додатків, які дозволяють розвивати та налаштовувати функції Google Apps.

Google робить відмінну роботу у справі забезпечення безпеки даних в «хмарному» сховищі. Стороннім практично неможливо отримати доступ до даних без дозволу. Це і є те, про що варто турбуватися і де варто проявляти обережність. Коли ви зрозумієте, як використовують дані та обмінюються ними, викличте на допомогу високі технології і рішення, щоб повністю захистити свою інформацію в «хмарах».

1.8. Фізична та логічна руйнації даних: відновлення інформації

Майже кожен користиувач комп'ютера в своєму житті стикався з втратою важливої інформації на різних носіях. Трапитися це може з різних причин: починаючи від банального випадкового видалення, закінчуючи несправністю жорсткого диска або іншого накопичувача. [26]

Інколи дешевше купити новий фізичний носій та скачати необхідну інформацію з Інтернету. Але бувають випадки, коли даної інформації в Інтернеті не знайдеш: сімейні фото, курсова робота, робочий звіт за певний період. В сучасному світі інформація може бути актуальною досить короткий проміжок часу. Тому відновлення втрачених даних – завжди актуальна проблема.

Існує фізична та логічна руйнації даних.

Фізичне руйнування – ваша флешка чи вінчестер згоріли від неправильного живлення чи їх випадково переїхав асфальтоукладач (рис. 1.29).

Логічне руйнування – внутрішні помилки файлових систем різних типів.

Рис. 1.29. Фізичне руйнування

При втраті інформації внаслідок фізичного виходу з ладу певного функціонального вузла накопичувача даних, зазвичай, необхідно провести «хірургічну операцію», а точніше – радіотехнічну: перепаяти неробочий елемент чи плату, замінивши на ідентичну або аналогічну (якщо це можливо). Це дуже тендітна робота і вона проводиться виключно фахівцями в даній області з використанням спеціальної апаратури.

Для відновлення інформації при логічній руйнації необхідно фізичний носій підключити до робочої машини, де встановлено необхідне програмне забезпечення. Можна відновлювати як певні файли, так і дискові масиви (RAID). Хоча існує дуже багато утиліт для відновлення втраченої чи видаленої інформації, дійсно дієвих – незначна кількість.

Розглянемо деякі найпопулярніші:

1. AOMEI Backupper[27]

Безкоштовний і надійний продукт для відновлення і резервного копіювання розділів дисків і дисків в цілому, з можливістю розбиття копії на частини. Основною особливістю програми є те, що вона підтримує не тільки декстопні ОС, а й серверні. Дане ПЗ також дозволяє робити відновлення системи. AOMEI Backupper має дуже широкий вибір додаткових можливостей: створення завантажувальних носіїв, підтримка стиснення і

[26] http://isearch.kiev.ua/uk/news/programs/tools-sec/1785-physical-and-logical-destruction-of-data-data-recovery-at-home
[27] https://www.aomeitech.com/

шифрування інформації. Як недолік можна назвати те, що на Windows 8 копії займають більший розмір ніж початкові файли.

2. Power Data Recovery

Дане ПЗ непогано зарекомендувало себе не тільки при відновленні файлів з вінчестерів, а й з карт пам'яті, USB-накопичувачів, а також з пошкоджених CD/DVD дисків. Power Data Recovery працює доволі швидко і немає потреби чекати декілька годин поки просканується ваш носій інформації. Слід зазначити, що флешки відформатовані в системі exFAT, програма Power Data Recovery не бачить.

3. Ontrack EasyRecovery Professional[28]

Даний софт включає в себе можливості програм, які були описані раніше, з дуже потужним пакетом додаткових інструментів: відновленням даних з електронної пошти, діагностикою пошкоджених і збережених секторів, SMART-аналізом і безпосередньо працює з RAID-масивами. Вбудована утиліта Hex Viewer дозволяє вручну шукати дані, відкривши диск в шістнадцятковому редакторі.

4. GetDataBack[29] для FAT|NTFS

Допоможе відновити дані, навіть якщо завантажувальний сектор і таблиця розділів пошкоджені. Використовується безпечна для файлів система відновлення, яка працює в режимі "тільки читання-копіювання" і може налаштовуватись індивідуально користувачем. В будь-який момент можна зупинити процес сканування та зберегти файли. GetDataBack розроблена окремо для FAT і NTFS. Програма може також відновлювати інформацію на інших комп'ютерах локальної мережі.

5. Zero Assumption Recovery[30]

ZAR підтримує різні мови, дуже довгі назви в файлах та NTFS-компресію, а також добре працює з RAID0 або RAID5. Програма дуже повільна, але дуже ретельно сканує диск і реанімує цифрову інформацію. ZAR має режим відновлення цифрових фото. Файлова система ext2 (Linux) підтримується частково.

6. МанСофт[31]

У вас є файл, але він «не відкривається» чи «заглючив»? Безкоштовний онлайн-сервіс відновлення файлів – детальніше в статті[32].

7. Hetman Partition Recovery[33]

Розроблений компанією Hetman Software софт допоможе відновити необхідні дані з пошкоджених чи недоступних розділів жорсткого диску, флешок, mp3-плеєрів, SSD-накопичувачів, «лікує» файлову систему від помилок. Якщо вірус заблокував, змінив чи пошкодив важливий файл – Hetman Partition Recovery допоможе.

8. R-Studio[34]

Це комплекс програм від компанії R-Tools Technology Inc. Саме він вважається найпотужнішим і найкориснішим інструментом серед аналогів. Хоча R-Studio спочатку розроблялася для компаній, що професіонально займаються відновленням цінної інформації, рядовий користувач може без проблем нею скористатися завдяки детальним інструкціям, які розміщені на сайті-виробнику.

---

[28] https://www.krollontrack.com/
[29] http://www.runtime.org/
[30] http://www.z-a-recovery.com/
[31] http://onlinerecovery.munsoft.com/ru/
[32] http://isearch.kiev.ua/ru/-news-ru/-security-ru/1553-the-fastest-way-to-free-repair-damaged-files
[33] https://hetmanrecovery.com/
[34] http://www.r-studio.com/

Розглянемо детальніше як працювати з вищезгаданим софтом.

R-Studio включає в себе широкий арсенал програм, який дозволяє відновлювати файли конкретного розширення, архіви файлів, великі групи файлів як локально, так і через мережу.

Так, як відновлення інформації – це ціла бізнес-індустрія, то даний софт не є повністю безкоштовним. За найпотужніші утиліти, які мають фактично необмежений спектр функцій для відновлення, доведеться заплатити. Але є й безкоштовні програми, які дозволять рядовому юзеру швидко й зручно повернути втрачені дані. Такою програмою є R-Undelete Home.

Якщо вашому вінчестеру з кожним днем «стає все гірше і гірше», версія R-Undelete Home створить файл-образ пошкодженого розділу, що дозволить працювати над відновленням інформації в зручний для вас час в зручному місці. Причому, можна розбити образ на частини для зручного транспортування файлів, так як образ займає місце, рівне за об’ємом пошкодженому розділу.

Для початку, завантажуємо інсталятор програми[35] (рис. 1.30).

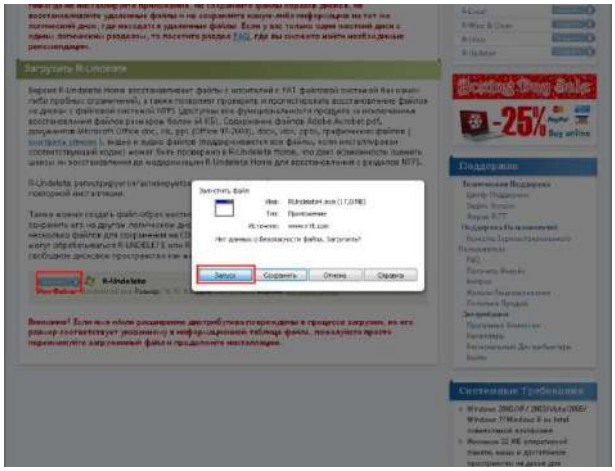


Рис. 1.30. Завантаження інсталятора програми

Всі подібні програми розроблялися першочергово для професіоналів в даній області, але розробники максимально адаптували свій софт під користувачів, які зіштовхуються з проблемою відновлення даних вперше:

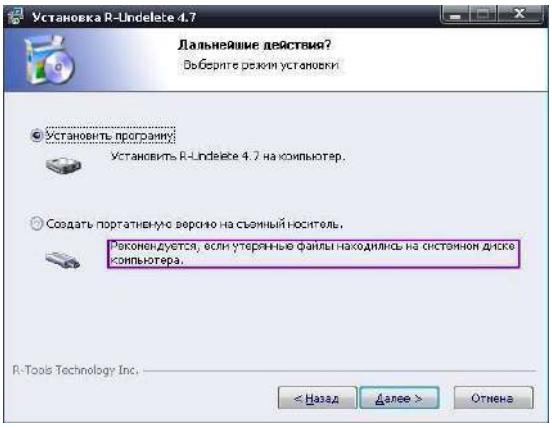


Рис. 1.31. Встановлення програми

Якщо необхідні файли знаходилися на системному розділі вашого носія, є великий ризик «запороти» систему. Все це враховано.

[35] http://www.r-undelete.com/ru/Download.shtml

Після встановлення програмного забезпечення (рис. 1.31), можна відразу приступати до роботи. R-Undelete Home детально, крок за кроком підкаже що робити (рис. 1.32):

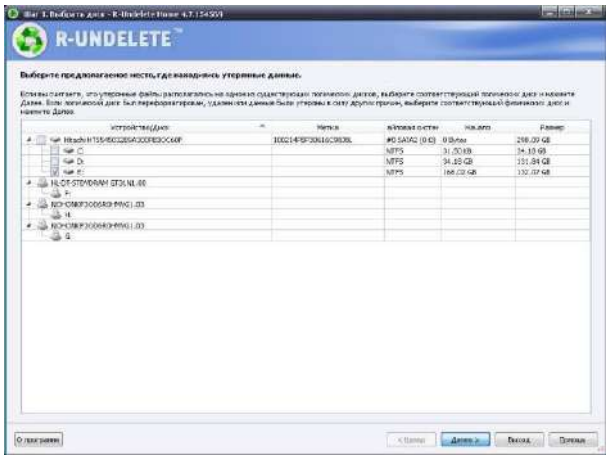


Рис. 1.32. Підказка для роботи

Відновлення займає дуже багато часу, тому чим більше ви знаєте інформації про необхідний файл (назва, розмір, точне розміщення, дата створення чи існування) – тим менше часу у вас займе ця процедура.

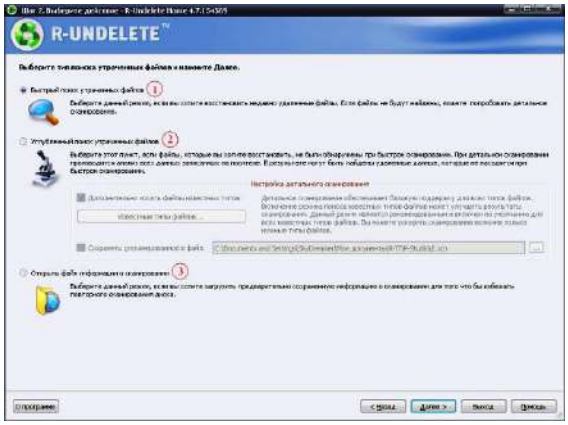


Рис. 1.33. Початкова інформація про втрачені файли

Якщо файли були втрачені не дуже давно – обирайте швидкий пошук [**1**] (рис. 1.33). При невдачі – поглиблений [**2**]. Для заощадження часу можна використати попередній звіт сканування програми [**3**]. Обираєте необхідний пункт, чекаєте відповідний час та переглядаєте отриманий звіт. Червоним хрестиком позначені знайдені втрачені файли (рис. 1.34):

Рис. 1.34. Інформація про знайдені файли

Побачили необхідне – ставите галочку та продовжуєте роботу (рис. 1.35):

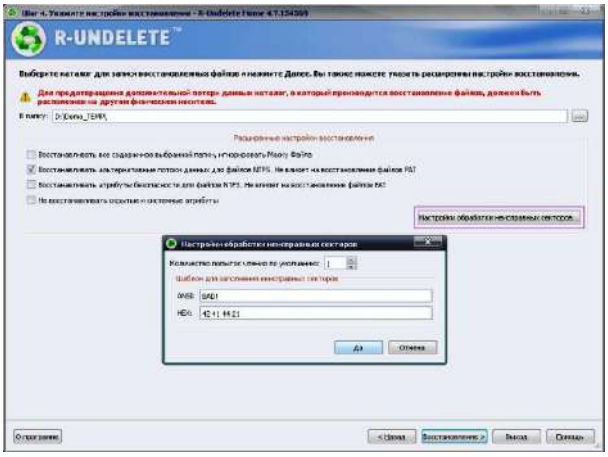


Рис. 1.35. Вибір режиму відновлення файлів

При відновленні дуже важливо не затерти назовсім відновлюваний файл, тому зберігати його необхідно на іншому фізичному носієві, чи хоча б обрати інший розділ жорсткого диску. Про це попереджає програма. Запускаємо відновлення (рис. 1.36):

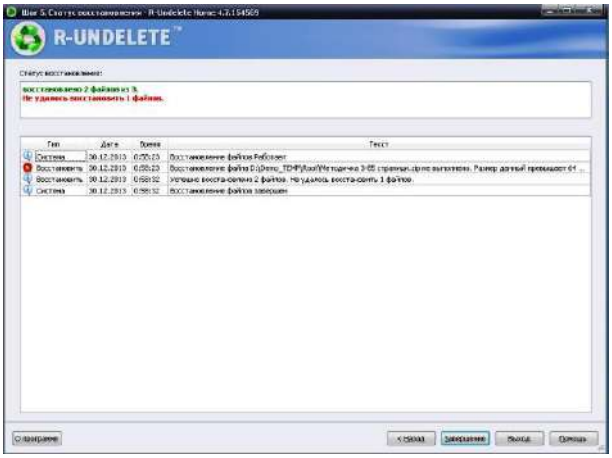


Рис. 1.36. Запуск відновлення

Бачимо, що не всі файли були відновлені (демоверсія, все таки). Але відновлені файли працюють досить коректно. Отже, втратили важливу інформацію – не впадайте у відчай, трохи терпіння – і все на своїх місцях!

1.9. Поради, які допоможуть зберегти вашу конфіденційну інформацію

Від соціальних мереж до онлайн-банкінгу, Інтернет дійсно проник у наше життя, як ніколи раніше. Сьогодні крім швидких настільних комп'ютерів та ноутбуків, ми також підключаємо до Інтернету смартфони, планшети і багато інших портативних пристроїв. Саме тому дуже важливо знати якомога більше про безпеку в Інтернеті.[36]

Необхідні знайти правильні способи захисту нашого приватного життя, коли ми онлайн.

Деякі з нас думають, що безпека в Інтернеті – це ілюзія. Тому що, веб-сайти збирають конфіденційну інформацію так тонко, що ми навіть не знаємо що саме їм відомо. Це,

[36] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1777-online-safety-tips-to-help-keep-your-sensitive-information

можливо, вірно, але ця невпевненість – ще одна причина, щоб зберегти свою анонімність та уникнути витоку даних в Інтернет[37].

Чи є щось, що ми можемо зробити, щоб залишатись у безпеці, поки займаємось серфінгом, крім того, що не показувати свої паролі, або не надавати багато особистої інформації? Ось кілька хороших способів, які можна використовувати для збереження вашої особистої інформації.

Ввімкніть приватний перегляд

Багато інтернет-сайтів використовують такі технології, як cookie, щоб захопити IP-адреси конкретних комп'ютерів перед збиранням інформації про діяльність в Інтернеті.

Окрім використання цих даних, щоб допомогти їм забезпечити оптимізовані і персоналізовані послуги користувачам і краще зрозуміти поведінку відвідувачів на своїх сайтах, вони також можуть продавати такі "цифрові профілі» для зацікавлених сторін для їх власного маркетингового дослідження, без нашої попередньої згоди.

Аби вирішити зростаюче занепокоєння з приводу того, що наше приватне життя під загрозою із-за таких дій, основні веб-браузери, такі як Internet Explorer, Google Chrome і Mozilla Firefox мають функцію "приватний перегляд" в налаштуваннях своїх останніх релізів для забезпечення online безпеки.

Іншими словами, ви можете запобігти зберігання cookie (а також інших деталей, таких як перегляд історії і тимчасові інтернет-файли) на своїх комп'ютерах, і тим самим зменшити ймовірність несанкціонованого збору інформації про те, як ви подорожуєте в Мережі.

Така функція безпеки була надана в Safari 2.0 з 2005 року, Mozilla Firefox 3.1 і Google Chrome 1.0 в 2008 році та Internet Explorer 8 з 2009 року. Ввімкніть приватний перегляд в браузері (навіть на смартфоні) і це буде першою лінією оборони online безпеки.

Приховайте свою IP-адресу

У певному сенсі, ваша IP-адреса як найчіткіший відбиток пальця в онлайн всесвіті. Для того, щоб скрити вашу IP-адресу є сенс розглянути питання про використання веб-проксі, наприклад, таких сервісів як HideMyAss[38] або відкритого інтернет-браузера Tor[39]. Ці сервіси приховують інформацію, щоб ви не залишали жодних слідів, незалежно від того, які сайти відвідуєте. Але треба мати на увазі, що деякі з таких веб-проксі мають сумнівну політику online безпеки і можуть самі мати доступ до даних, які ви намагаєтесь приховати. Зробіть власне дослідження перед їх використанням.

Бонусом веб-проксі або Tor є те, що ви можете відвідувати сайти, які заблоковані вашим інтернет-провайдером.

Не забувайте виходити

Ось тривожний факт про Facebook, яким хочемо поділитися з вами. Як пише Business Insider, Facebook може відстежувати онлайн-активність користувачів, які залишаються авторизованими у своєму обліковому записі Facebook. Це означає, що якщо ви закрили вкладку Facebook, не натиснувши кнопку «вийти», і продивляєтесь інші сайти, які містять кнопку «like», то ці сайти можуть відстежувати і обробляти дані про вашу діяльність (навіть якщо ви не натискуєте на неї).

---

[37] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1148-how-to-avoid-data-leaks-on-the-internet
[38] https://www.hidemyass.com/index
[39] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1742-how-to-safely-continue-using-tor-on-windows

Також, інтернет-активність може контролюватися на різних платформах, так як на ваш обліковий запис Facebook можна увійти за допомогою будь-якого пристрою, підключеного до Інтернету.

Такі інтернет-гіганти, як Facebook, Amazon і Google мають великі прибутки від реклами та інформації про нас, яку вони захопили. Це ще одна причина бути обережним, так як вони можуть тонко відняти у нас наше приватне життя і використовувати це для своєї вигоди.

Отже, не забувайте виходити[40] зі своїх аккаунів у соціальних мережах, поштових клієнтах та іншого.

Остерігайтеся відкритих Wi-Fi точок доступу

Якщо ви знайшли відкриту Wi-Fi точку, ми не радимо швидко підключатися до неї. За замовчуванням, відкриті джерела Wi-Fi в зонах загального користування не мають шифрування, а це означає, що будь-хто поруч з вашим місцем розташування, може записувати такі дані, які ви передаєте онлайн, як ваші паролі, банківські рахунки та електронні листи.

Захистіть себе! Є деякі основні запобіжні заходи які можна вжити, якщо ви не готові відмовитися від зручності цих безкоштовних з'єднань Wi-Fi:

1. Вимкніть обмін файлами на пристрої або комп'ютері
2. Уникайте сайтів, де вам потрібно вводити персональні дані, щоб увійти в свій обліковий запис (сайти, наприклад, соціальних мереж, електронної пошти або онлайн-банкінгу)
3. Якщо вам необхідно використовувати електронну пошту, шифруйте її з SSL (Secure Sockets Layer) або TSL (Transport Layer Security)
4. Переконайтеся в тому, що ви підключені до захищених каналів (адреси, що починаються з "HTTPS"[41]).
5. Щоб отримати максимальну безпеку в Інтернеті, створіть VPN (віртуальну приватну мережу)[42]

Не забувайте, що лише весь комплекс цих нескладних рекомендацій допоможе вам залишатися в безпеці. В наступних розділах розглядається реалізація запропонованих методів захисту.

[40] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/748
[41] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1134
[42] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/712

2. Raspberry Pi як інструмент пентестера

2.1. Налаштування автономної платформи пентестера на Raspberry Pi з Kali Linux

Raspberry Pi – комп'ютер розміром з кредитну карту, який може зламати Wi-Fi, зробити копію ключа карти, увірватися в ноутбуки і навіть клонувати існуючу мережу Wi-Fi, щоб обдурити користувачів, з'єднавши їх з RPi замість мережі[43].

Він може блокувати Wi-Fi, робити трек стільникових телефонів, прослуховувати поліцейські сканери, транслювати сигнал FM-радіо і, мабуть, навіть направити ракету в гелікоптер.

Ключем до такої потужності є масове співтовариство розробників та виробників, які вносять тисячі нововведень для платформ Kali Linux і Raspberry Pi. За ціни, меншої від ціни балону з газом, купуючи Raspberry Pi 3, ви отримуєте недорогу, гнучку кіберзброю.

Пам'ятайте, що використання цих знань, щоб увірватися в захищені мережі, швидше за все, призведе до вашого арешту і звинувачення в кримінальному злочині, адже можливе порушення закону про комп'ютерну безпеку. Ви повинні використовувати ці знання тільки на благо, для власного навчання, і застосовувати лише з мережами, які контролюєте.

Не у всіх є доступ до суперкомп'ютера, але, на щастя, він і не потрібний, щоб мати міцну платформу Kali Linux.

Вже з більш ніж 12 мільйонів проданих одиниць, Raspberry Pi можна придбати всього за $35, щоб заощадити. Це робить більш важким визначення, хто стоїть за атакою, запущеною з Raspberry Pi, бо з однаковою ймовірністю це може бути спонсорована державою атака літака з радаром або гіперактивного підлітка з навичками кодування на рівні середньої школи.

Думай як зловмисник

Raspberry Pi має кілька унікальних особливостей, які роблять його потужним і легко доступним комплектом інструментів тестера вразливостей. Зокрема, RPi дешевий. Крім того, Raspberry Pi компактний. А завдяки ОС Kali Linux (рис. 2.1), він отримує можливість запуску широкого спектру інструментів злому від клонованих значків до скриптів крекінгу Wi-Fi. Замінивши SD-карту, або додавши чи видаливши компоненти з таких торгових майданчиків, як Adafruit, можна налаштувати Raspberry Pi відповідно до будь-якої ситуації.

Raspberry Pi в наступі

По-перше, дуже важливо розуміти, що Raspberry Pi не суперкомп'ютер і не має величезної обчислювальної потужності. Тому, не дуже добре підходить для завдань з такими інтенсивними процесами, як злом перебором паролів WPA, або організація мережевих атак, бо з'єднання є занадто повільним. Але, RPi ідеально підходить для багатьох середовищ атаки. Ми просто перекладаємо перераховані завдання на великі комп'ютери, а RPi використовуємо для збору даних.

[43] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1940-setting-up-an-autonomous-platform-pentestera-on-raspberry-pi-with-kali-linux

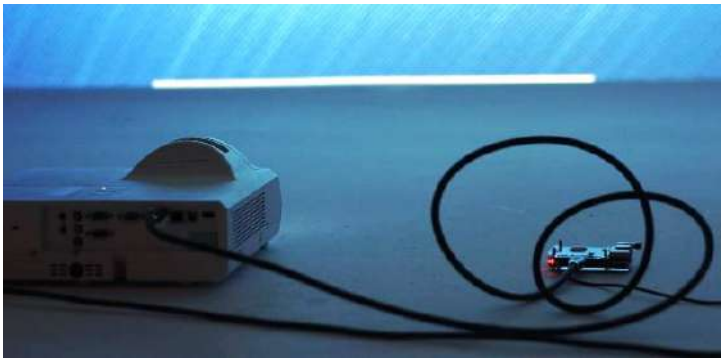


Рис. 2.1. Raspberry Pi + проектор = Kali на величезному екрані

З досвіду багатьох, Raspberry Pi працює виключно чудова платформа для атаки Wi-Fi (рис. 2.2). Завдяки своєму невеликому розміру і великій бібліотеці інструментів атаки на базі Kali Linux, він ідеально підходить для розвідки і атак мереж Wi-Fi. Наша збірка Kali Linux для наступу буде спрямована на анонімний польовий аудит дротових і бездротових мереж.

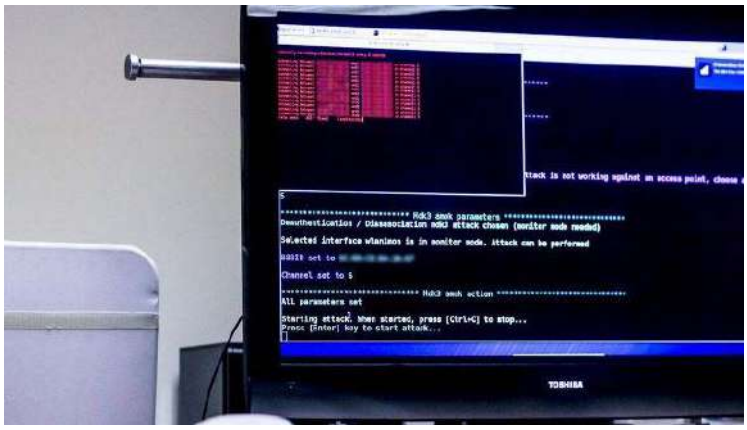


Рис. 2.2. Активний Raspberry Pi з налаштуванням блокування Wi-Fi

Основні компоненти нашої системи

Основні компоненти, необхідні для побудови системи атаки з нашим RPi, і чому вони нам потрібні.

- *Raspberry Pi*: Raspberry Pi 3 (рис. 2.3) є платформою пропонованих збірок, координує і управляє всіма іншими компонентами. Низьке енергоспоживання і гнучкі можливості RPi дозволяють отримати платформу для запуску інших операційних систем на базі Linux, крім Kali.
-

Рис. 2.3. Raspberry Pi 3

- *Бездротова карта управління та контролю (C2)*: Метою бездротової карти C2 є автоматичне підключення RPi до керуючої AP (access point – точки доступу), такої як телефонна точка доступу або домашня мережа. Це дозволяє здійснювати дистанційне керування RPi приховано або з великої відстані за допомогою SSH (Secure Shell) чи через VNC (Virtual Network Computing). На щастя для нас, Raspberry Pi 3 має вбудовану карту Wi-Fi, але адаптер бездротової мережі може також бути доданий до Raspberry Pi 2.
- *Бездротова карта для атаки*: Нашою бездротовою картою для атаки буде сумісний з Kali Linux Wi-Fi адаптер (рис. 2.4), здатний виконувати ін'єкції пакетів. Це буде наша площина атаки і може бути з дальнім або коротким радіусом дії, чи зі спрямованою антеною, в залежності від вимог атаки. Для вибору ви можете переглянути чудовий посібник *Вибір бездротового адаптера для злому*[44].

Chipset	Supported by airodump for Windows	Supported by airodump for Linux	Supported by aireplay for Linux
Atheros	CardBus: YES PCI: NO (see CommView)	PCI, PCI-E: YES Cardbus/PCMCIA/Expresscard:YES USB: YES(b/g/n)	New mac80211 Atheros drivers have native injection and monitoring support
Atmel	UNTESTED	802.11b YES 802.11g UNTESTED	UNTESTED
Broadcom bcm43xx	Old models only (BRCM driver)	YES	MOSTLY (Forum thread) No fragmentation attack support. Recommend to use b43, see below.
Broadcom b43	NO	Yes (1.0-beta2 and up, check here)	Yes, check here
Centrino b	NO	PARTIAL (ipw2100 driver doesn't discard corrupted packets)	NO
Centrino b/g	NO	YES	NO (firmware drops most packets) ipw2200inject No fragmentation attack support
Centrino a/b/g	NO	YES	YES (use ipwraw or iwl3945)
Centrino a/g/n (4965)	NO	YES	MOSTLY, see iwlagn. Fakeauth is currently broken.
Centrino a/g/n (5xxx)	NO	YES	YES
Cisco Aironet	YES?	Yes, but very problematic	NO (firmware issue)
Hermes I	YES	Only with airodump not airodump-ng and only with a specific firmware	NO (firmware corrupts the MAC header)

Рис. 2.4. Параметри Wi-Fi адаптерів для підтримки команд Kali Linux

Карти з записаними ОС: Хости ОС і мозок комп'ютера на мікроSD-карті можуть бути точно налаштовані для будь-якого бажаного середовища. Створивши налаштовані карти, можна швидко змінювати конфігурацію і функції Raspberry Pi простою заміною карти і компонентів.

- Комп'ютер: Вам також знадобиться комп'ютер, щоб завантажити прошивку та записати її на мікроSD-карту.
- *Електроживлення*: Raspberry Pi використовує стандартний блок живлення Micro-USB і майже будь-який зарядний пристрій для телефону Андроїд або акумуляторна батарея будуть придатні для живлення RPi. Це дозволяє мати різні конфігурацій акумуляторів відповідно до довготривалої розвідки або операцій з тривалим живлення.
- *Ethernet-кабель (додатково)*: Кабель Ethernet дозволяє обійти бездротову аутентифікацію шляхом прямої взаємодії з локальними мережами, до яких у вас є фізичний доступ. Такі спеціалізовані атаки, як PoisonTap також можуть скористатися інтерфейсом Ethernet для проникнення в комп'ютери.

[44] https://null-byte.wonderhowto.com/how-to/hack-wi-fi-choosing-wireless-adapter-for-hacking-0157057/

- Bluetooth клавіатура (опціонально): Клавіатура Bluetooth корисна для взаємодії, коли у вас є підключення HDMI.
- Корпус (за бажанням): корпус потрібний кожному RPi, щоб захистити його.

Міркування з побудови

Будуть розглянуті два основні режими, в яких будемо працювати на Raspberry Pi. У відкритій конфігурації RPi підключається до дисплея через кабель HDMI, а також приєднується бездротова миша і клавіатура (рис. 2.5). У тактичній конфігурації будемо використовувати ноутбук або смартфон, щоб отримати віддалений доступ до Raspberry Pi через SSH (рис. 2.6). При підключенні RPi до точки доступу на своєму телефоні або до сусідньої дружньої AP, ми зможемо отримати доступ до Raspberry Pi, залишаючись в змозі використовувати передані в полі дані.

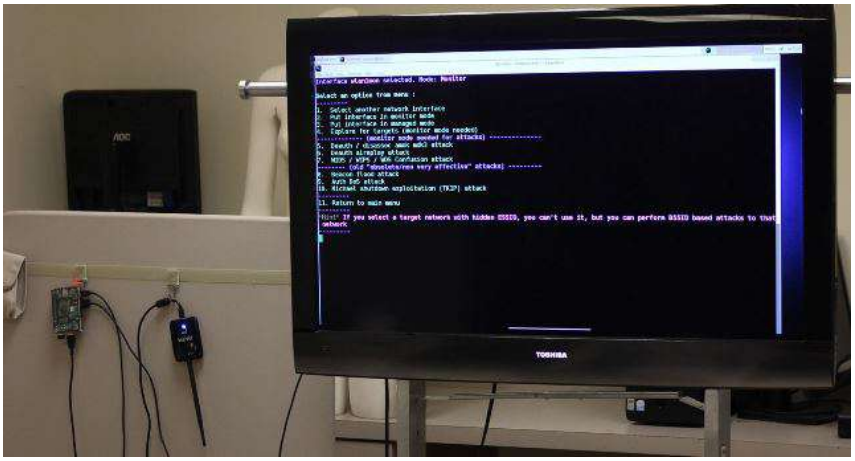


Рис. 2.5. Відкрита конфігурації виходу і входу

Рис. 2.6. Тактична конфігурація: Kali Linux через SSH

Як все налаштувати

Далі покажемо кроки, необхідні для налаштування Raspberry Pi 3 як основної платформи з Kali Linux. Розглянемо, як вибрати збірку для встановлення, записати образ диска на карту мікроSD, і які кроки для першого запуску RPi після встановлення. Ми оновимо Kali Linux до останньої версії, щоб переконатися, що все працює правильно,

змінимо ключ SSH за замовчуванням, і потурбуємося про деякі домашні налаштування, наприклад, змінимо пароль адміністратора.

Зауважимо, що існує багато способів налаштувати Kali на Raspberry Pi 3. Деякі включають сенсорний екран, деякі зовсім «без голови» (доступ через мережеві з'єднання без клавіатури або дисплея), а інші використовують вбудовану карту Wi-Fi, щоб створити точку доступу для дистанційного керування RPi. При виборі даної збірки ми відкинули будь-які конструкції, які включали енергозатратний та тендітний сенсорний екран або додаткові апаратні засоби, і залишили версію, оптимізовану для наших двох різних сценаріїв C2.

Крок 1. **Завантаження образу Kali Linux для Raspberry Pi**

Перейдіть на Offensive Security[45] і завантажте останню версію образу Kali Linux для Raspberry Pi. Сьогодні це "RaspberryPi 2/3" версії 2017.3 (рис. 2.7).

Рис. 2.7. Сторінка завантаження останньої версії образу Kali Linux для Raspberry Pi

Крок 2. **Запис образу на MicroSD карту**

Можете використати такий інструмент, як ApplePiBaker for Mac[46] або Etcher[47], щоб завантажити образ Kali на свою SD-карту, але іноді це може призвести до помилок. Щоб не допустити цього, ми розглянемо, як записати образ на Mac за допомогою Terminal. Якщо використовуєте Windows, то можете завантажити Win32 Disk Imager[48], щоб розмістити образ на SD -карті.

На Mac, перш ніж підключитися до своєї SD-карти, виконайте наступну команду в терміналі:

```
df -h
```

Буде відображений список всіх дисків, підключених до системи (рис. 2.8). Вставте карту SD і знову виконайте команду і зверніть увагу на ім'я файлової системи своєї SD-карти (це те, чого раніше не було). Воно повинно виглядати як `/dev/disk2s1`, і ви повинні бути дуже обережні, щоб не сплутати його на наступних кроках, оскільки можете переписати свій жорсткий диск.

```
/dev/disk2 (internal, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:     FDisk_partition_scheme                        *15.9 GB    disk2
   1:             Windows_FAT_32 NO NAME                 64.0 MB    disk2s1
   2:                      Linux                         7.3 GB     disk2s2
```

Рис. 2.8. Доступні диски

[45] https://www.offensive-security.com/kali-linux-arm-images/
[46] https://www.tweaking4all.com/software/macosx-software/macosx-apple-pi-baker/
[47] https://etcher.io/
[48] https://sourceforge.net/projects/win32diskimager/

Тепер використаємо команду `dd`, щоб завантажити образ Kali на карту. Для отримання інформації про параметри команди `dd` скористайтесь командою `man` (рис. 2.9).

```
DD(1)                    BSD General Commands Manual                    DD(1)

NAME
     dd -- convert and copy a file

SYNOPSIS
     dd [operands ...]

DESCRIPTION
     The dd utility copies the standard input to the standard output.  Input
     data is read and written in 512-byte blocks.  If input reads are short,
     input from multiple reads are aggregated to form the output block.  When
     finished, dd displays the number of complete and partial input and output
     blocks and truncated input records to the standard error output.

     The following operands are available:

     bs=n      Set both input and output block size to n bytes, superseding the
               ibs and obs operands.  If no conversion values other than
               noerror, notrunc or sync are specified, then each input block is
               copied to the output as a single block without any aggregation
               of short blocks.
```

Рис. 2.9. Скористайтеся `man dd`, щоб побачити інші операнди для `dd`

По-перше, давайте демонтуємо розділ, щоб ви могли написати на нього, за допомогою наступної команди, де `X` повинно бути правильним номером диска:

```
sudo diskutil unmount /dev/diskX
```

Тепер ми готові до завантаження Kali. Наберіть, але не виконуйте команду, `sudo dd bs=1m if=`, бо треба ввести розташування образу Kali Linux, який хочете записати на карту. Ви можете перетягнути образ диска у вікно, щоб показати шлях до файлу. Після цього, введіть пробіл, потім `of=/dev/rdisk` і номер диска, отриманий раніше.

Якщо є `s` після початкового номера диска (як `rdisk2s1`), не включайте в команду `s` і наступний номер. Так, "`rdisk2s1`" повинен виглядати як "`rdisk2`". Тому, команда в цілому повинна виглядати десь так:

```
sudo dd bs=1m if=LocationOfKaliImage of=/dev/rdiskX
```

Натисніть **Enter**, щоб почати процес, і зауважимо, що `dd` не надає інформації на екрані, якщо немає помилки або він не закінчив. Щоб побачити хід виконання під час передачі, можете набрати **Ctrl+T**. Дочекайтеся завершення процесу. Ви будете знати, що процес завершений, коли побачите зчитані байти, передані за час виконання процесу.

Це буде виглядати як на скріншоті (рис. 2.10) (якщо натиснути **Ctrl+T** кілька разів під час передачі) при завершенні.

```
/dev/disk2 (internal, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:                                                    *15.9 GB    disk2
0:~          $ sudo dd bs=1m if=/Users/                          \ DATA/kali-2.1.2-rpi2.img  of=/dev/rdisk2
load: 1.93  cmd: dd 12479 uninterruptible 0.00u 0.13s
146+0 records in
145+0 records out
152043520 bytes transferred in 19.731557 secs (7705602 bytes/sec)
load: 1.79  cmd: dd 12479 uninterruptible 0.00u 0.28s
298+0 records in
297+0 records out
311427072 bytes transferred in 48.662200 secs (6399774 bytes/sec)
7000+0 records in
7000+0 records out
7340032000 bytes transferred in 1131.140905 secs (6489052 bytes/sec)
0:~          $
```

Рис. 2.10. Статус: зайнято 1,131 секунд для передачі

Крок 3. **Завантаження в Kali Linux**

Коли закінчите, ваша карта мікроSD буде готова для використання. Вставте мікроSD-карту в RPi, підключіть HDMI, а також клавіатуру Bluetooth (рис. 2.11). Підключіть джерело живлення, щоб вперше завантажитися в Kali Linux. Для того, щоб дістатися до робочого столу, вашим логіном за замовчуванням є `root`, а паролем `toor` (рис. 2.12).

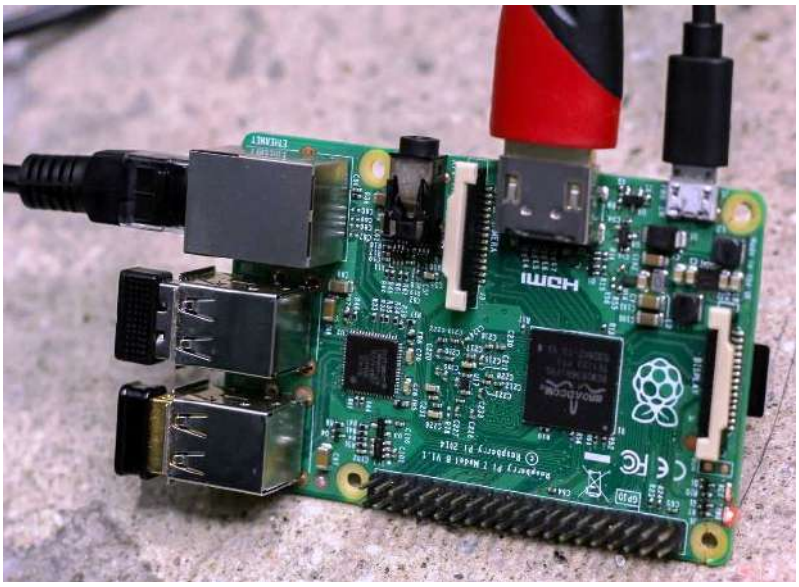


Рис. 2.11. Kali Pi з Ethernet, Bluetooth-приймачем і додатковим адаптером Wi-Fi

Процес залогінення є проблемою для автономного управління і нам треба буде його пізніше відключити. Це дозволить нам увімкнути RPi і відразу віддалено підключитися до нього без екрану.

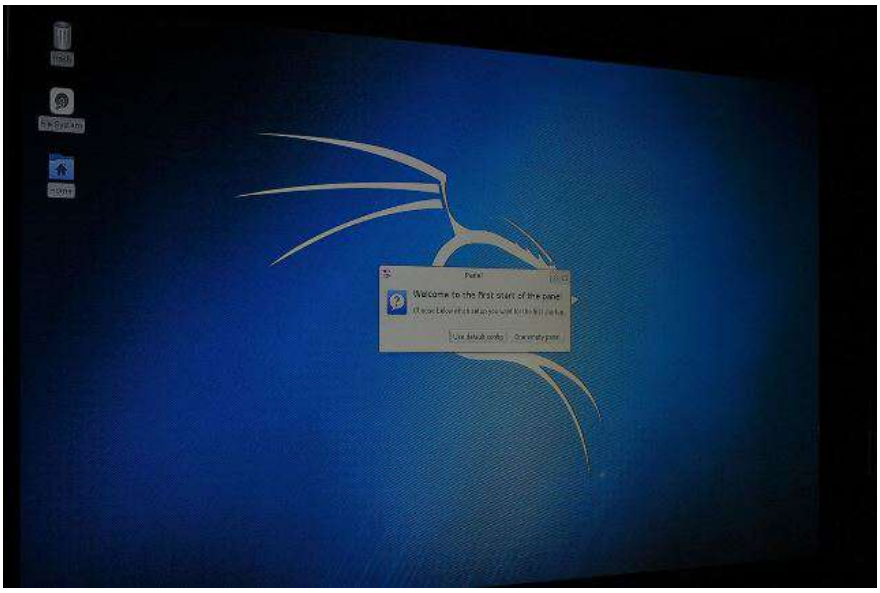


Рис. 2.12. Перше завантаження Kali Linux

Крок 4. **Вмикання Wi-Fi карти**

Тепер прийшов час, щоб увійти і увімкнути Wi-Fi-карту, щоб ви могли використовувати інструменти в Kali Linux. RPi автоматично розпізнає вашу карту Wi-Fi, але ви все одно повинні увійти в мережу. Найперше, ми повинні запустити графічний користувальницький інтерфейс Kali Linux і переконатися, що все працює:

1. Ви побачите запрошення на введення ім’я користувача та паролю з рядка терміналу на своєму RPi. Введіть ім’я користувача `root` та пароль `toor` (ми змінимо пароль пізніше).

2. Введіть команду `startx` та натисніть клавішу **Enter** для завантаження графічного інтерфейсу для Kali. Це може зайняти деякий час, щоб завантажити на RPi.
3. Тепер можете переміщатися по RPi з сенсорним екраном і клавіатури. Натисніть невеликий значок терміналу в нижній частині, щоб відкрити командний рядок.
4. Щоб встановити карту Wi-Fi, введіть `nano /etc/network/interfaces` з рядка термінала та натисніть Enter, щоб завантажити файл конфігурації для налаштування Wi-Fi.
5. Додайте наступні рядки в текстовий файл, який тільки що відкрився, підставляючи інформацію про свою мережу:

```
auto wlan0
iface wlan0 inet dhcp
wpa-ssid “ім’я вашої мережі”
wpa-psk “пароль доступу до мережі”
```

Коли закінчите, натисніть **Ctrl+X**, щоб зберегти і вийти. Ваша карта Wi-Fi тепер повинна працювати (хоча, можливо, доведеться спочатку перезавантажитися).

Крок 5. **Оновлення Kali Linux**

Kali Linux – це особлива версія Debian Linux, призначена для тестування на проникнення. Вона сумісна з деякими з кращих і найсучасніших інструментів, доступних для бездротового хакерства і достатньо гнучка, щоб підтримувати велику кількість хакерських розробок. Вона підтримується Offensive Security і вам необхідно оновити її до останньої версії, щоб переконатися, що всі інструменти працюють належним чином.

Перш, ніж запустити, маєте чудовий час, щоб розширити свою установку до розміру розділу. Для цього виконайте такі дії:

```
resize2fs /dev/mmcblk0p2
```

У правому верхньому куті робочого столу побачите можливість підключення до сусідньої бездротової мережі. Підключіться до точки доступу свого телефону або дружньої AP, щоб отримати оновлення. Виконайте оновлення, відкривши вікно терміналу і ввівши наступні команду:

```
apt-get update
apt-get dist-upgrade
reboot
```

Ваш Kali встановиться зараз в актуальний стан. Змініть кореневий пароль до чогось більш безпечного, ніж "`toor`", набравши:

```
passwd root
```

Потім введіть новий пароль для своєї системи Kali Linux.

Крок 6. **Установка сервера OpenSSH**

Для того, щоб спілкуватися зі своїм Raspberry Pi з комп’ютера або телефону, ми повинні мати можливість увійти в систему. Для цього можемо використати SSH для підключення через будь-яке з’єднання з Wi-Fi, яке ділимо з RPi. SSH, або Secure Shell – мережевий протокол, який дозволяє виконувати команди на віддаленому пристрої. Це означає, що нам не потрібно підключати екран, щоб взаємодіяти з нашим RPi.

У терміналі, виконайте наступні дії для встановлення серверу OpenSSH і оновлення рівнів запуску, щоб дозволити запуск SSH при завантаженні:

```
apt-get install openssh-server
update-rc.d -f ssh remove
```

```
update-rc.d -f ssh defaults
```

Ключі за замовчуванням представляють величезну вразливість, так як будь-яка людина може вгадати їх. Давайте негайно змінимо їх, виконавши наступні команди:

```
cd /etc/ssh/
mkdir insecure_old
mv ssh_host* insecure_original_default_kali_keys/
dpkg-reconfigure openssh-server
```

Будуть створені резервні копії старих ключів SSH в іншій папці і згенеруються нові ключі. Проблема вирішена! Тепер давайте переконаємося, що можемо увійти через корінь ввівши:

```
sudo nano /etc/ssh/sshd_config
```

Ми відкрили для редагування папку конфігурації SSH. Змініть рядок:

```
PermitRootLogin without-password
```

щоб він виглядав як:

```
PermitRootLogin yes
```

Натисніть **Ctrl+O**, щоб зберегти зміни. Якщо все зроблено правильно, то вам не потрібно вже нічого змінювати (рис. 2.13).

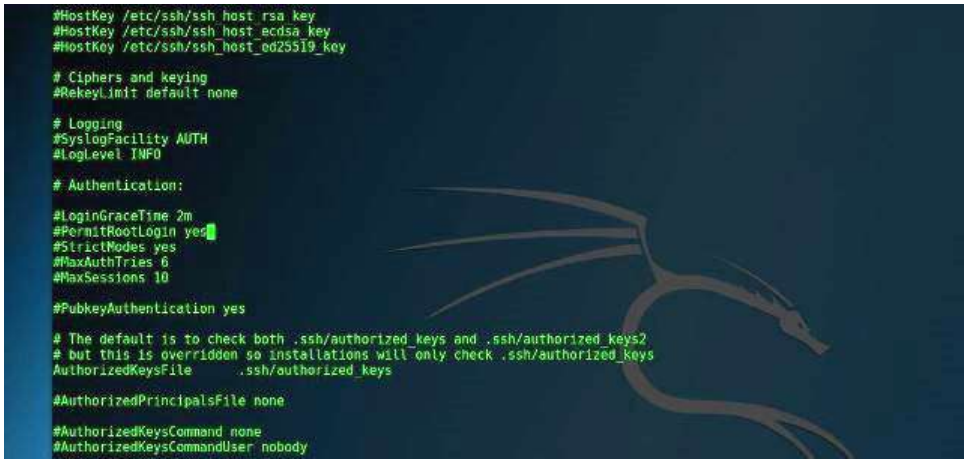


Рис. 2.13. Налаштування `sshd config`

Відмінно! Давайте перезапустимо службу SSH, ввівши команди:

```
sudo service ssh restart
update-rc.d -f ssh enable 2 3 4 5
```

І, нарешті, перевіримо, що SSH працює, за допомогою наступних дій, щоб побачити, чи запущена SSH в даний час.

```
sudo service ssh status
```

Ми повинні побачити щось подібне, якщо все успішно (рис. 2.14).

Рис. 2.14. Перевірка SSH

Якщо не так, запустіть команду, щоб отримати працюючу службу:

```
sudo service ssh start
```

Якщо виявили, що SSH не працює, то можете використати `raspi-config` як обхідний шлях. Команда призначено для Jessie, але буде працювати і на Kali також. Для того, щоб використовувати її, клонуйте з GitHub[49], наберіть `sudo mount /dev/mmcblk0p1/boot` для монтування завантажувального розділу, перейдіть в директорію через `cd` і запустіть `sudo bash raspi-config`.

Крок 7. **Створення налаштовуваного MOTD**

Вас може зустріти після успішного входу в систему чудове повідомлення банера дня (MOTD).Створіть своє власне, набравши:

```
sudo nano /etc/motd
```

Видаліть вміст і вставте все, що хочете, щоб воно показувалось щоразу при вході в систему. Збережіть і вийдіть з `nano`, натиснувши **Ctrl+O**, а потім **Ctrl+X** (рис. 2.15).

Рис. 2.15.

Крок 8. **Тестування входу за допомогою SSH**

Давайте спробуємо увійти в систему з вашого домашнього комп'ютера або ноутбука. Підключіть RPi до тієї ж бездротової домашньої мережі або до робочої, до якої підключений комп'ютер. Виконайте команду ifconfig на своєму RPi в терміналі, щоб дізнатися свою IP-адресу (рис. 2.16):

```
ifconfig
```

Рис. 2.16. В прикладі наш IP виглядає як 10.11.1.144

[49] https://github.com/asb/raspi-config

На своєму персональному комп’ютері введіть:

```
ssh root@(ваша IP-адреса)
```

Ви повинні побачити екран MOTD (рис. 2.17).

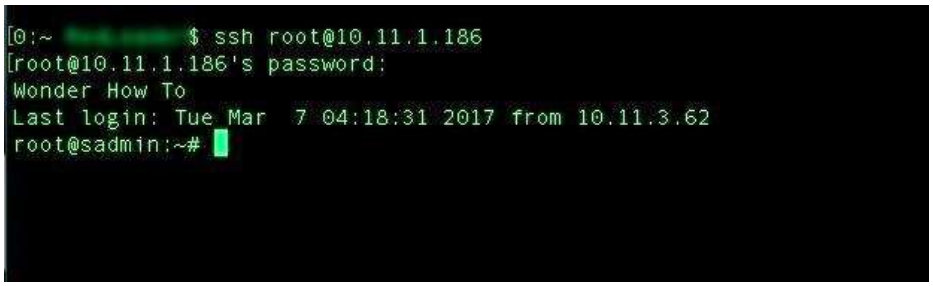


Рис. 2.17. Простий MOTD при успішному SSH-вході в систему

Якщо немає, то можете запустити arp-scan[50] на Mac, щоб побачити список усіх доступних пристроїв в мережі, якщо необхідно знайти IP-адресу свого RPi з персонального комп’ютера.

Крок 9. **Налаштування автологіну для віддаленого доступу**

Іноді, ми хочемо мати можливість увійти в інший обліковий запис, ніж кореневий. Давайте створимо нового користувача з ім’ям WHT (або будь-яким іншим) з кореневим дозволом командою:

```
useradd -m WHT -G sudo -s /bin/bash
```

Змініть для WHT (або для того, як ви назвали) пароль до чогось більш безпечного, ніж `toor`:

```
passwd WHT
```

Відмінно! Тепер давайте відключимо цей вхід до того, поки ми зможемо завантажуватися безпосередньо в Kali, і наші бездротові карти запустяться і підключаться, щоб дозволити нам дистанційне керування. Для цього введіть наступну команду:

```
sudo nano /etc/lightdm/lightdm.conf
```

Видаліть # перед наступними рядками (рис. 2.18):

```
autologin-user=root
autologin-user-timeout=0
```

Рис. 2.18. Налаштування автологіну

Збережіть і вийдіть за допомогою **Ctrl+X**. Далі введіть:

```
sudo nano /etc/pam.d/lightdm-autologin
```

Вам треба змінити запуск в рядку 11:

[50] http://macappstore.org/arp-scan/

```
# Allow access without authentication

auth required pam_succeed_if.so user != root quiet_success
auth required pam_permit.so
```

на цей (рис. 2.19):

```
# Allow access without authentication
###auth required pam_succeed_if.so user != root quiet_success
auth required pam_permit.so
```

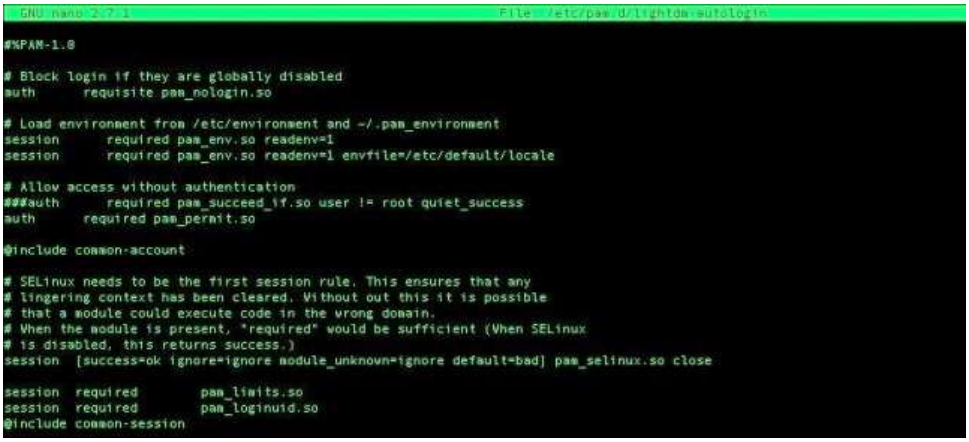


Рис. 2.19.

Збережіть і вийдіть. Введіть `reboot` в терміналі, щоб перезапустити RPi.

Перевірка вашої збірки з контрольним списком

Для того, щоб розглядати все готовим, пристрій повинен виконати цей контрольний список:

1. Пристрій запускається, входите в систему без запиту пароля і запускається SSH при завантаженні, щоб дозволити віддалений доступ.
2. Пристрій підключається до команди AP, щоб включити дистанційне керування (робить це за замовчуванням після підключення вперше).
3. RPi може бути виключена без руйнування даних на мікро SD-карті (нормально завантажується після виключення).

Пройшли всі вимоги? Тоді ваш Raspberry Pi готовий продовжити роботу (рис. 2.20).

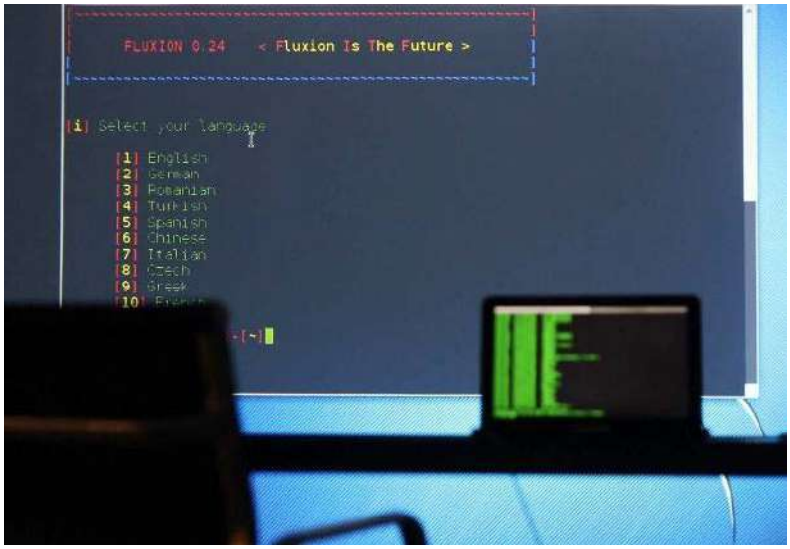


Рис. 2.20. Використання Fluxion з Raspberry Pi і проектором

З цього моменту, ви можете працювати зі своєю маленькою портативною станцією пентестера. Для базової навігації можна використовувати сенсорний екран на RPi і запустити будь-яку програму в Kali Linux. Якщо не знаєте, з чого почати, кілька ідей в наступних підрозділах підручника.

2.2. Як тестувати власну мережу та посилити свою безпеку з Kali Linux

Kali Linux – операційна система, орієнтована на безпеку, яку ви можете запустити з компакт-диска, USB-накопичувача, або навіть на мікрокомп'ютері Raspberry Pi, в будь-якому місці.

За допомогою інструментарію безпеки Kali Linux можна зламати паролі Wi-Fi, створити підроблені мережі та перевірити інші вразливості. Розглянемо, як його використовувати, щоб зробити техогляд безпеки своєї власної мережі[51].

Kali Linux упакований з тонною програмного забезпечення для тестування вразливостей вашої мережі. Його занадто багато, щоб перерахувати тут, тому виберемо кілька улюблених інструментів, щоб показати, як вони працюють: Aircrack, Airbase і Arpspoof. Ми покажемо вам, як зламати пароль Wi-Fi за допомогою методів грубої сили, створити підроблений маршрутизатор, щоб обдурити машини при реєстрації на ньому, а також виконати атаку «людина в центрі», щоб підслухати мережеві комунікації.

Пам'ятайте: використовувати ці повноваження можна лише для блага, а не для зла. Знаючи, як зробити ці речі, ви можете допомогти собі дізнатися, як зробити безпечною свою власну мережу, але робити їх ще з кимсь ми не рекомендуємо.

2.2.1. Тестування паролю WPA Wi-Fi з Aircrack

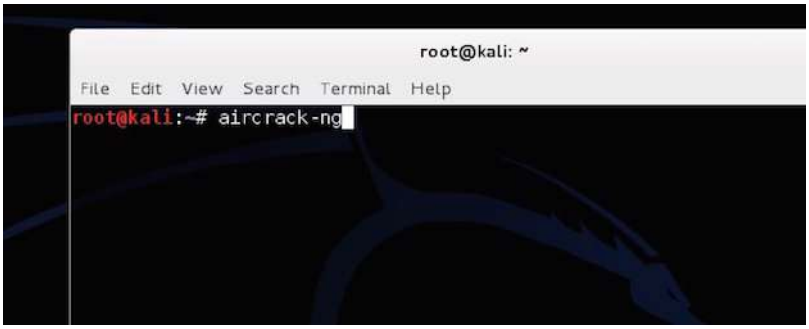


Рис. 2.21. Запуск Aircrack

[51] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1864-how-to-hack-your-own-network-and-beef-up-its-security-with-kali-linux

Kali Linux поставляється з цілим набором додатків для злому Wi-Fi мереж, в тому числі Aircrack[52] і Reaver[53] – які придатні для злому WEP і WPA паролів, відповідно.

Проте, WEP паролі вже більше не такі популярні (бо їх легко зламати), і Reaver працює тільки якщо мережа дозволяє WPS. Ми збираємося ще раз поглянути на Aircrack і використати його для нашого шляху в мережу WPA методом грубої сили (за допомогою списку паролів).

Крок 1. **Конфігурування бездротової карти**

Рис. 2.22.

Насамперед: відключіться від всіх бездротових мереж. Тепер відкрийте термінал. Для того, щоб використовувати Aircrack, вам знадобиться адаптер бездротового зв'язку, який підтримує ін'єкції. Введіть наведене нижче в терміналі, щоб переконатися, що ваша карта їх підтримує:

```
airmon-ng
```

Отримаєте список всіх бездротових адаптерів, що підтримують цей злом. Якщо ваша карта не підтримує ін'єкції, вона не буде тут відображатися. Ви, швидше за все, перераховані під інтерфейсом `wlan0`, але це може залежати від вашої машини.

Далі введіть:

```
airmon-ng start wlan0
```

Замініть `wlan0` адресою інтерфейсу своєї Wi-Fi картки. Ви повинні отримати повідомлення у відповідь, яке скаже, що режим монітора включений.

Крок 2. **Монітор мережі**

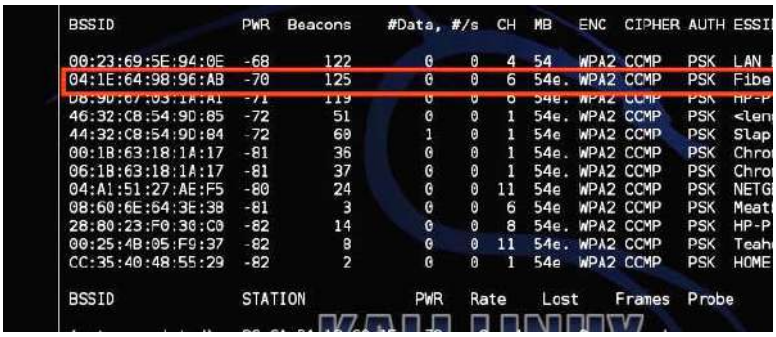


Рис. 2.23. Список мереж

Далі, збираємося отримати список всіх мереж в вашому оточенні і моніторити їх.

Введіть:

```
airodump-ng mon0
```

[52] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1749-how-to-crack-wi-fi-evil-wpa2-psk-passwords-using-dictionary-attacks-via

[53] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1293-how-to-crack-password-wpa-wi-fi-network-by-reaver

Ви побачите всі мережі у вашому оточенні (рис. 2.23). Знайдіть свою мережу у списку і скопіюйте BSSID, занотувавши, на якому вона каналі. Натисніть **Ctrl+C**, щоб зупинити процес.

Потім введіть команду нижче, замінивши інформацію в дужках інформацією, яку ви зібрали вище:

```
airodump-ng -c (channel) --bssid (bssid) -w /root/Desktop/
(monitor interface)
```

Побачите щось на зразок цього:

```
airodump-ng -c 6 --bssid 04:1E:64:98:96:AB -w /root/Desktop/ mon0
```

Тепер, будете моніторити свою мережу. Ви повинні побачити спливаючі на робочому столі чотири файли. Не турбуйтеся про них зараз; ви повинні будете повернутися до одного з них пізніше. Наступний крок є чимось на зразок гри в очікування, бо будете сидіти і чекати підключення пристрою до мережі. В нашому випадку, просто відкрийте пристрій, яким володієте і підключайтеся до свого Wi-Fi. Ви повинні побачити спливаюче вікно як для нової станція. Запишіть номер станції, тому що він потрібний на наступному етапі.

Крок 3. **Захоплення рукостискання**

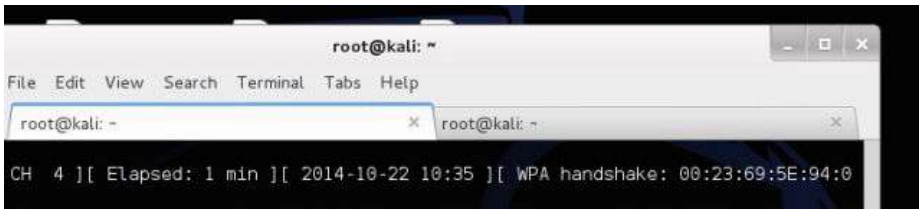


Рис. 2.24. WPA рукостискання

Тепер ви збираєтеся змусити перепідключитися, щоб мати змогу захопити рукостискання між комп'ютером і маршрутизатором. Залиште Airodump запущеним і відкрийте нову вкладку в терміналі. В ній введіть:

```
aireplay-ng -0 2 -a (router bssid) -c (client station number) mon0
```

Це має виглядати приблизно так:

```
aireplay-ng -0 2 -a 04:1E:64:98:96:AB -c 54:4E:85:46:78:EA mon0
```

Побачите, як Aireplay посилає пакети на ваш комп'ютер, щоб змусити перепідключитися. Поверніться назад на вкладку Airodump і побачите нове число, вказане після WPA-рукостискання. Якщо воно є, то ви успішно схопили рукостискання і можете почати злом пароля.

Крок 4. **Злом пароля**

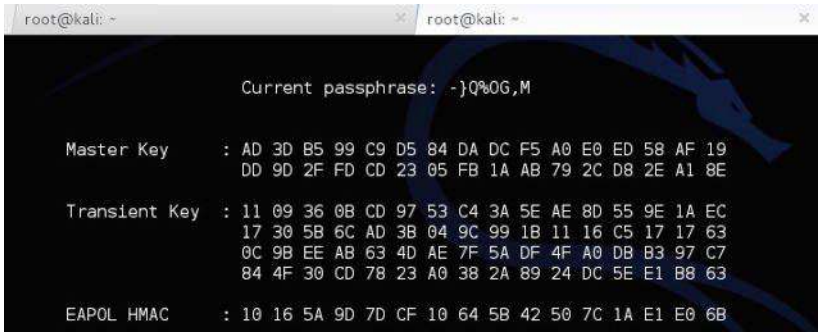


Рис. 2.25. Злом пароля

Тепер у вас є пароль маршрутизатора в зашифрованому вигляді, але вам все ще потрібно з'ясувати, який він насправді. Щоб зробити це, використаємо список паролів, щоб спробувати методом грубої сили почати свій шлях в мережу. Ви можете знайти ці списки в Інтернеті, але Kali Linux включає в себе кілька невеликих списків, щоб ви стартували, в каталозі /usr/share/wordlists, так що ми зараз використаємо один з них. Для початку злому пароля введіть:

```
aircrack-ng -a2 -b (router bssid) -w (path to wordlist)
/Root/Desktop/*.cap
```

Так, продовжуючи наш приклад вище і за допомогою одного з вбудованих списків слів, введене повинне читатися як щось на кшталт:

```
aircrack-ng -a2 -b 04:1E:64:98:96:AB -w /usr/share/wordlists/fern-
wifi/common.txt /Root/Desktop/*.cap
```

Тепер, Aircrack спробує всі ці паролі, щоб побачити, чи не підходить один з них. Якщо вдало, то ви отримаєте повідомлення про те, що був знайдений ключ з паролем. Якщо ні, то спробуйте ще один список з перерахованими паролями, поки не знайдете той, який працює. Чим більший список паролів, тим більше часу займе цей процес, але тим більше у вас шансів на успіх.

Як використовувати дану інформацію, щоб захистити себе

Таким чином, ви простим методом грубої сили прокладаєте свій шлях у своїй мережі. Залежно від того, наскільки хороший ваш пароль, це триватиме п'ять хвилин чи п'ять годин. Якщо в ролі пароля щось типу, як "password123", то є ймовірність того, що один з невеликих словників доможе зламати його досить швидко. Якби пароль буде більш складним, то, ймовірно, треба буде багато часу, або ніколи його не зламаєте взагалі (якщо так, то це добре для вас!).

Найкращим захистом є хороший, сильний пароль на маршрутизаторі. Чим довший, більш дивний і складніший він, тим краще. Точно так же, переконайтеся, що використовуєте протокол безпеки WPA2 і що не включено WPS.

2.2.2. Створення фейкової мережі з Airbase

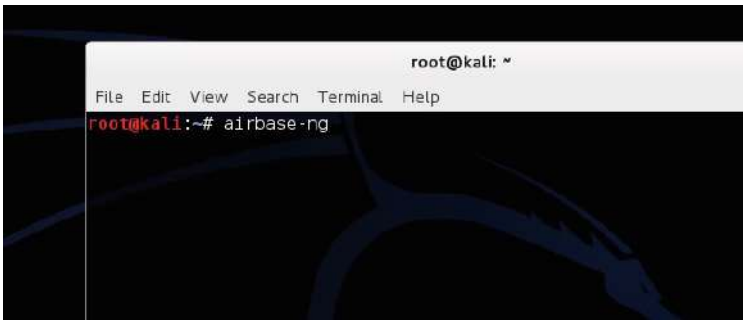


Рис. 2.26. Запуск Airbase

Тепер давайте поглянемо на те, як ви можете підробити мережеву адресу, щоб обдурити людей, підключивши їх до неправильної мережі, так щоб можня було побачити, що вони роблять. Хакери можуть так зробити, і ви підключаєтесь до фальшивої мережі, думаючи, що це ваша справжня, потім отримуєте атаку «людина в центрі» (докладніше про це в наступному розділі), щоб зібрати інформацію про вас з вашого трафіку. Це на диво легко зробити за допомогою інструменту Kali Linux під назвою Airbase.

По суті, ви перетворите свій Wi-Fi адаптер в точку доступу на Kali Linux з тим же ім'ям, що й інша мережі. Для того щоб це зробити, будемо слідувати тій же лінії досліджень, як робили вище, але кінцівка трохи відрізняється.

***Крок 1.* Конфігурування бездротової карти**

Так само, як і минулого разу, ви повинні налаштувати бездротову карту для моніторингу трафіку. Відкрийте термінал і введіть:

```
airmon-ng
```

Отримаєте список всіх бездротових адаптерів, що підтримують цей злом. Ваш, швидше за все, перерахований під інтерфейсом wlan0.

Потім введіть:

```
airmon-ng start wlan0
```

Тепер ви в режимі монітора. Пора знайти мережу, яку підробити.

***Крок 2.* Знаходимо Wi-Fi мережу для обману**

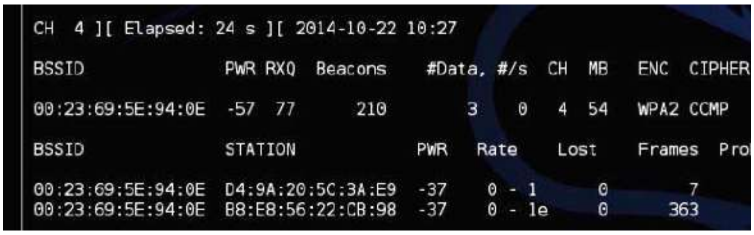


Рис. 2.27.

Для того, щоб обманювати маршрутизатор, вам знадобиться інформація про нього. Введіть:

```
airodump-ng mon0
```

Ви побачите всі мережі свого оточення. Знайдіть свою мережу у списку і скопіюйте BSSID, занотувавши її ім'я і на якому вона каналі. Це той маршрутизатор, який ви збираєтеся обманювати. Натисніть **Ctrl+C**, щоб зупинити процес.

***Крок 3.* Створюємо фейкову мережу**

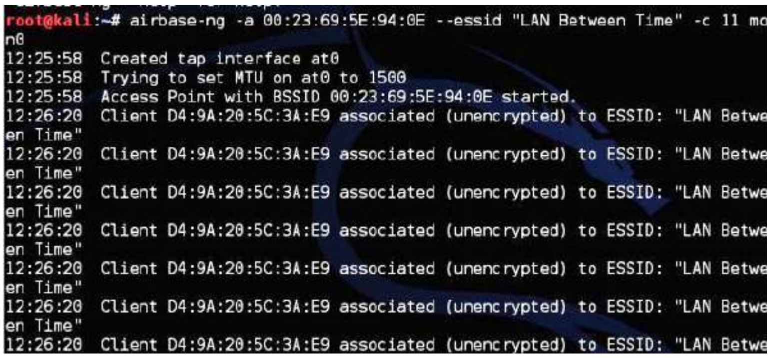


Рис. 2.28. Запуск Airbase

Тепер, ви збираєтеся створити підроблену мережу за допомогою Airbase. Вкажіть її, замінивши в дужках на інформацію, яку ви зібрали на останньому етапі:

```
airbase-ng -a (router BSSID) --essid "(network name)" -c (channel)
mon0
```

Наприклад, тепер повинні читати щось на кшталт:

```
airbase-ng -a 04:1E:64:98:96:AB --essid "MyNetwork" -c 11 mon0
```

Це так. Ви зараз підробили маршрутизатор і створили клон з таким же ім'ям, каналом, і номером SSID, тому не відрізняєтеся від оригіналу. На жаль, комп'ютери цієї мережі завжди будуть підключатися автоматично до найпотужніших маршрутизатором з таким же ім'ям, тому вам потрібно збільшити потужність своєї підробленої мережі. Введіть:

```
iwconfig wlan0 txpower 27
```

Це піднімає потужність вашої підробленої мережі до максимально прийнятої межі, так що можна сподіватися, що коли користувачі увійдуть наступного разу, то підключаються до вас автоматично. Це не повинно як-небудь пошкодити карту доти, поки ви не пішли вище, ніж 27. Після того, як користувач ввійде в мережу, це буде так само, як ви обоє в одній і тій же мережі. А це означає, що можете досить легко отримати доступ до всього, що він роблять.

Як використовувати дану інформацію, щоб захистити себе

Підміну мережі виявити важко, але можете виявити її, коли мережевий трафік сповільнився, або якщо він раптом не вимагає парольної аутентифікації. Якщо ви дійсно параноїк, що хтось підмінив маршрутизатор, то можете відключити можливість автоматичного підключення до Wi-Fi, так що у вас принаймні буде час, щоб подивитися на маршрутизатор, до якого під'єднуєтесь.

2.2.3. Перехоплення трафіку іншого пристрою за допомогою атаки «людина в центрі» з підміною ARP

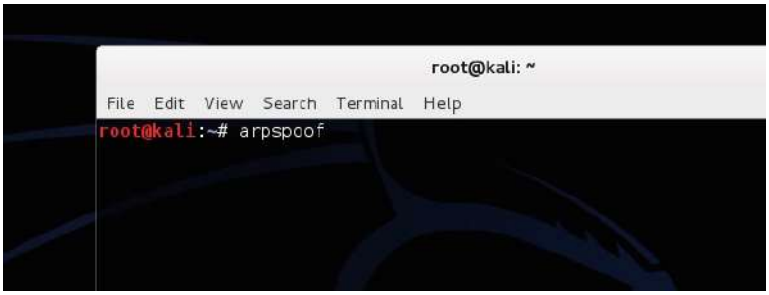


Рис. 2.29.

Атака «людина в центрі» по суті є підслуховуванням в вашій мережі. Тут ви перехоплюєте мережеві сигналів між комп'ютером і маршрутизатором без комп'ютера для реалізації. Ми показали вам, як зробити перехоплення пакетів і зараз будемо використовувати ARP-спуфинг, щоб зібрати цю інформацію. І спуфинг, і сніффінг подібні, бо підслуховують розмови, але вони працюють трохи по-різному. Сніффінг захоплює трафік під час моніторингу мережі, а спуфинг прикидається мережею. Ці типи атак часто використовуються, щоб захопити паролі, зображення, і в значній мірі що-небудь ще, що ви відправляєте мережею.

Крок 1. **Вмикання маршрутизації пакетів**

Насамперед, ви повинні зробити свою машину Kali Linux, щоб вона перенаправляла будь-який трафік, який отримує, так, щоб цільовий комп'ютер міг отримати доступ в Інтернет. Введіть в командному рядку:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Це гарантуватиме, що вся інформація передається вперед після перехоплення. Таким чином, Інтернет і будь-які інші зв'язки між маршрутизатором і цільовим комп'ютером продовжуватимуть працювати.

Крок 2. **Вмикання підміни ARP**

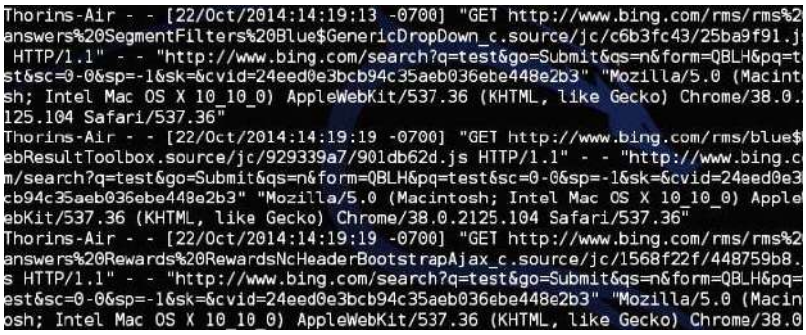


Рис. 2.30.

Тепер вам потрібно увімкнути ARP-спуфинг. Це обманює комп'ютер і маршрутизатор, заставляючи думати, що ваш Wi-Fi адаптер є мостом. Коли обман буде успішним, ви зможете контролювати весь трафік між пристроями. Ви будете робити це двічі, щоб змогли захопити трафік, який проходить через ваш комп'ютер від маршрутизатора і з комп'ютера до маршрутизатора.

Для запису трафіку від вашого маршрутизатора введіть наведене нижче, замінивши дужки інформацією вашої мережі:

```
arpspoof -i wlan0 -t (router address) (target computer
address)
```

Ви побачите виведення купи чисел, які показують, що все працює. Залиште це запущеним, і відкрийте іншу вкладку в терміналі та зробіть навпаки:

```
arpspoof -i wlan -t (target computer address) (router address)
```

Обидва рядки повинні виглядати приблизно так:

```
arpspoof -i wlan0 -t 192.168.1.1 192.168.1.105
arpspoof -i wlan0 -t 192.168.1.105 192.168.1.1
```

Тепер, весь трафік між цими двома машинами буде збиратися в Kali Linux. Є тонна інструментів, щоб захопити цю інформацію, але давайте просто подивимося на пару з них.

Щоб відстежувати будь-які URL-адрес для візитів комп'ютера, відкрийте іншу вкладку Terminal і введіть:

```
urlsnarf -i wlan0
```

Це покаже веб-сайти відвідувань комп'ютера.

Якщо ви більше зацікавлені в зображеннях, то такожожете захопити будь-який трафік зображень. Введіть:

```
driftnet -i wlan0
```

З'явиться вікно і відображатиме будь-які зображення, які завантажуються і передаються мережею. В принципі, якщо є будь-яка незашифрована інформація, яка пересилається між маршрутизатором і комп'ютером, то ви побачите, що станеться.

Як використовувати дану інформацію, щоб захистити себе

Кращий спосіб, щоб захистити користувачів від ARP-спуфинга мережі, є захист мережі за допомогою надійного пароля і переконатися, що вона та, в першу чергу. Проте, включення брандмауера на вашому комп'ютері також допомагає. Крім того, переконайтеся, що завжди користуєтесь HTTPS, коли він доступний. Коли включений HTTPS, спуфер ARP

не зможе нічого захопити, що ви робите. Це особливо важливо, коли використовуєте громадський Wi-Fi і не можете контролювати мережеву безпеку.

2.3. 5 кроків, щоб промацати свою мережу та побачити все, що відбувається в ній

Ваша домашня мережа є вашою фортецею. Усередині лежать тонни цінної інформації – незашифровані файли, особисті, приватні дані і, можливо, найголовніше те, що все це може бути викрадене з комп'ютерів і використане для будь-яких цілей.

Давайте поговоримо про те, як ви можете дослідити свою домашню мережу, щоб переконатися, що не маєте в ній яких-небудь непроханих гостей[54].

Покажемо, як спланувати мережу, «заглянути під ковдру», щоб побачити, хто розмовляє і про що, та як розкрити пристрої чи процеси, які можуть зменшувати пропускну здатність. Коротше кажучи, ви будете в змозі визначити ознаки того, що щось у вашій мережі перебуває під загрозою. Припускаємо, що ви знайомі з деякими такими основами мереж, як знаходження списку пристроїв на своєму маршрутизаторі і що таке MAC-адреса.

Хоча, перш ніж іти далі, ми повинні видати попередження:

Використовуйте ці повноваження для хороших справ і запускайте дані інструменти та команди тільки на обладнанні або в мережі, якими володієте чи керуєте. Мета нашої наших занять навчити вас, як це робиться, щоб ви змогли робити це самостійно і захистити себе, а не зламувати інших.

Крок 1. **Зробіть карту мережі**

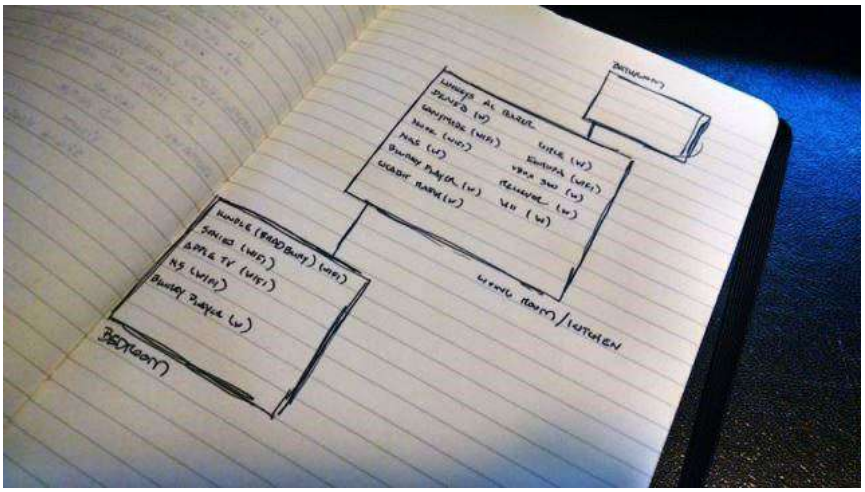


Рис. 2.31.

Перш ніж увійти навіть в свій комп'ютер, запишіть те, що ви думаєте, що знаєте. Візьміть аркуш паперу і запишіть всі свої підключені пристрої. Вони включають такі речі, як смарт-телевізори, телевізійні приставки, ноутбуки і комп'ютерів, планшети і телефони, або будь-які інші пристрої, які можуть бути підключені до мережі. Якщо це допоможе, намалюйте карту свого будинку, разом з кімнатами. Потім запишіть кожен пристрій і де він

[54] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1917-5-steps-to-touch-its-network-and-see-everything-that-happens-in-it

знаходиться. Ви можливо здивуєтесь, скільки саме пристроїв під'єднано до Інтернету одночасно.

Мережеві адміністратори та інженери визнають, що цей крок є першим кроком у вивченні будь-якої мережі, з якою не знайомі. Через інвентаризацію пристроїв в ній визначте їх, а потім подивіться, чи співпадає реальність з тим, що очікували. Якщо (або коли) це не так, ви зможете швидко відділити те, що знаєте, від того, що не знаєте. Ви можете увійти до маршрутизатора і подивитися на його сторінці стану, щоб побачити те, що підключено, але ще не працює. Якщо не можете визначити всі пристрої у своїй мережі за їх IP-адресами та MAC, то просто отримаєте великий список речей, який може включати будь-яких зловмисників або нахлібників. Зробіть спочатку фізичну інвентаризацію, а потім перейдіть до цифрової.

Крок 2. **Перевірте мережу, щоб переглянути, хто в ній**

Якщо у вас є фізична карта мережі і список всіх ваших довірених пристроїв, прийшов час, щоб покопатися. Увійдіть у свій маршрутизатор і перевірте список підключених до нього пристроїв. Це дасть вам основний список імен, IP і MAC-адрес. Пам'ятайте, список пристроїв вашого маршрутизатора може або не може показати все. Він повинен показати, однак деякі маршрутизатори покажуть лише пристрої, що використовують маршрутизатор для отримання своєї IP-адреси. У кожному разі, отримати даний список – це добре, але ми хочемо більше інформації.

Далі, звернемося до Nmap[55]. Nmap є крос-платформним інструмент сканування мережі з відкритим вихідним кодом, який може знайти пристрої в мережі, поряд з тонною докладної інформації про ці пристрої. Ви можете побачити відкриті порти, операційну систему, яка використовується, IP і MAC-адреси, навіть служби. Завантажте Nmap[56], прочитайте дану інструкцію з його установки[57], і дотримуйтесь цих вказівок[58] для виявлення вузлів у домашній мережі.

Рис. 2.32.

У нашому випадку, встановимо і запустимо його з командного рядка (якщо хочете графічний інтерфейс, то Zenmap[59] зазвичай доступний з інсталятором), потім задамо Nmap діапазон IP-адрес для сканування, які використовуються для домашньої мережі. Знайдені більшість активних пристроїв в домашній мережі, за винятком небагатьох, на яких є деякі

[55] https://nmap.org/
[56] https://nmap.org/download.html
[57] https://nmap.org/book/install.html
[58] https://nmap.org/book/man-host-discovery.html
[59] https://nmap.org/zenmap/

розширені функції безпеки (хоча їх теж можна виявити з деякими командами Nmap, які можете знайти за посиланнями вище).

Порівняйте список Nmap зі списком свого маршрутизатора. Ви повинні побачити ті ж самі речі (якщо те, що ви записали раніше, і досі не вимкнено). Якщо бачите щось на маршрутизаторі, що відсутнє в Nmap, спробуйте використати Nmap безпосередньо проти цієї IP-адреси. Потім, на підставі того, що ви знаєте, подивіться на інформацію про пристрій, знайдену Nmap. Якщо вона стверджує, що це Apple TV, то, ймовірно, не повинна мати служби, які використовують HTTP, наприклад. Якщо це виглядає дивно, досліджуйте його спеціально для отримання більш докладної інформації, як це зроблено на скріншоті вище. Автор помітив, що одна з його машин відкидає запити ping, які робив Nmap, пропускаючи їх. Автор задав Nmap просто зондувати його в будь-якому випадку, і переконатися, що пристрій відповів достатньо.

Nmap є надзвичайно потужним інструментом, але він не найпростіший у використанні. Є й інші варіанти. Angry IP Scanner[60] – ще одна крос-платформна утиліта, яка має красивий і простий у використанні інтерфейс, який дасть вам багато тієї ж інформації. Утиліта Who Is On My Wi-Fi[61] пропонує подібні функції і може бути налаштована на сканування у фоновому режимі у разі, якщо хтось заходить в Інтернет, коли ви не дивитеся. Wireless Network Watcher[62], знову для Windows, є ще однією утилітою з красивим інтерфейсом, яка, незважаючи на свою назву, не обмежується лише бездротовими мережами.

Крок 2. **Сніферіть навколо, щоб подивитися, хто і з ким розмовляє**

На даний час, ви повинні мати список пристроїв, які знаєте і довіряєте, та список пристроїв, які знайшли підключеними до мережі. Якщо пощастить, то на цьому закінчите, бо все або збігається або зрозуміле (наприклад, телевізор в даний час вимкнений). Тим не менше, якщо ви побачите будь-які не визначені актори, запущені служби, які не відповідають пристрою (чому ваш Roku запустив postgresql?), або відчуваєте щось ще не так, прийшов час, щоб зробити трохи підслуховування. Для цього є пакет сніфера.

Коли два комп'ютери спілкуються в мережі або через Інтернет, вони посилають один до одного біти інформації під назвою "пакети". Всі ці пакети разом створюють складні потоки даних, які складають відео, яке спостерігаємо, або документи, які завантажуємо. Сніфер пакетів є процесом збору і вивчення цих бітів інформації, щоб побачити, куди вони йдуть і що вони містять. Щоб зробити це, нам буде потрібний Wireshark[63]. Це крос-платформний інструмент моніторингу мережі, який дозволить зробити трохи перехоплення пакетів для сніферу паролів і куків. Але наша ціль не захопити що-небудь конкретне, а просто контролювати, які типи трафіку є в мережі. Щоб зробити це, потрібно запустити Wireshark через Wi-Fi в "promiscuous mode". Це означає, що він не просто шукає пакети, відправлені з/до комп'ютера, а збирає всі пакети, які можна побачити у нашій мережі.

Після установки, відкрийте Wireshark і виберіть Wi-Fi адаптер. Натисніть "options" поруч з ним, і, як ви бачите у відео вище, можете вибрати "promiscuous mode" для цього адаптера. Після того, як ви зробили це, можете почати захоплення пакетів. Коли починаєте захоплення, то збираєтеся отримати багато інформації (рис. 2.33). На щастя, Wireshark очікує цього і робить результати легкими для фільтрування.

[60] http://angryip.org/
[61] https://whoisonmywifi.com/
[62] http://www.nirsoft.net/utils/wireless_network_watcher.html
[63] https://www.wireshark.org/

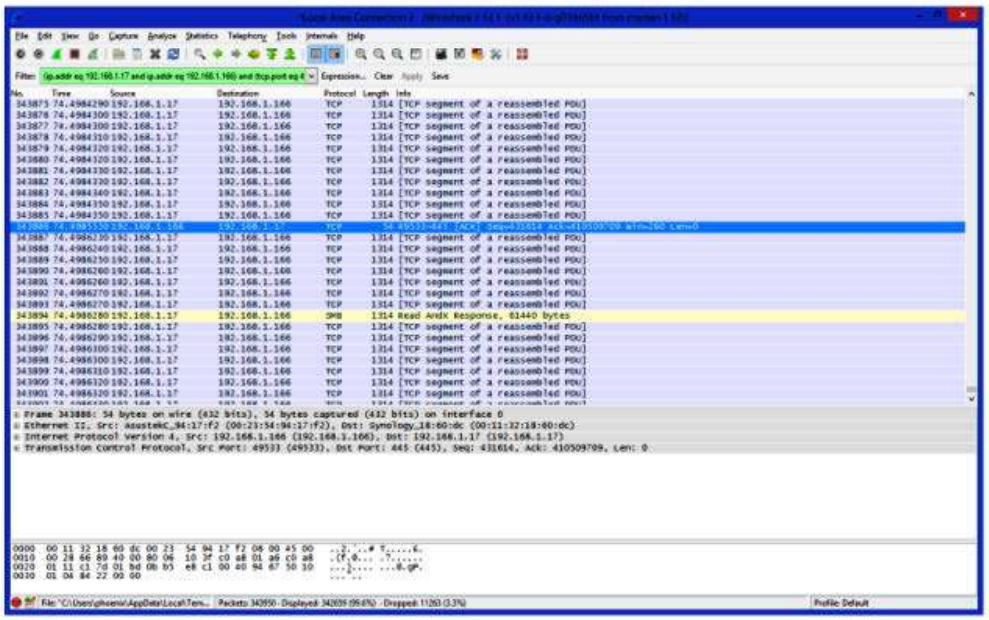


Рис. 2.33. Wireshark

Оскільки ми просто переглядаємо, щоб побачити, що роблять в мережі підозрілі суб'єкти, переконайтеся, що досліджувана система в Інтернеті. Ідіть вперед і захопіть для початку декілька хвилин цінного трафіку. Потім ви зможете фільтрувати цей трафік на основі IP-адреси цього пристрою, використовуючи вбудовані фільтри Wireshark. Виконання описаного дає швидкий погляд на те, яка IP-адреса відправника і яка інформація, яку він відправляє туди і назад. Ви можете натиснути правою кнопкою миші на будь-який з цих пакетів, щоб оглянути його, стежити за розмовою між обома кінцями та фільтрувати все захоплення IP або бесіди. Для більш детального вивчення, How-To Geek має докладний посібник з фільтрації Wireshark[64]. Ви можете не знати, на що дивитися, але це трохи стеження за тим, звідки входить.

Якщо побачите, що підозрілий комп'ютер щось надсилає до чужої IP-адреси, використайте команду nslookup[65] (в командному рядку в Windows, або в терміналі в OS X чи Linux), щоб отримати ім'я хоста. Це може багато сказати про місце і тип мережі, до якої комп'ютер підключений. Wireshark також повідомляє, які порти використовуються, тому введіть в Google номер порту і подивіться, які додатки використовують його. Якщо, наприклад, у вас є комп'ютер з підключенням до дивного імені хоста через порти, які часто використовуються для IRC або передачі файлів, то, можливо, виявили зловмисника. Звичайно, якщо знайдете пристрій, що підключається до авторитетних служб з широко використовуваниими портами для таких речей, як електронна пошта або HTTP/HTTPS, то можете лише знайти, що наткнулися на планшет свого сусіда, який ніколи не говорив, що він належить йому, або хтось поруч краде Wi-Fi. У будь-якому випадку, ви отримаєте дані, необхідні, щоб зрозуміти, що це не ваша власність.

Крок 4. **Відстежуйте довго і протоколюйте захоплені вами трофеї**

Звичайно, не кожен поганий актор в мережі буде в Інтернеті і скачувати тоді, коли ви шукаєте його. До цього моменту, ми навчив вас, як перевірити підключені пристрої, сканувати їх, щоб визначити, чим вони є насправді, а потім сніферити трохи їх трафік, щоб

[64] https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/
[65] https://en.wikipedia.org/wiki/Nslookup

переконатися, що все відповідає їх ролі. Тим не менш, що робити, якщо підозрілий комп'ютер робить свою чорну справу вночі, коли ви спите, або хтось використовує ваш Wi-Fi, коли ви весь день знаходитесь на роботі, а не поруч, щоб перевірити?

Є кілька шляхів вирішення цього. Перш за все, додаток Who's On My Wi-Fi, який може працювати у фоновому режимі на вашому комп'ютері з Windows, і бачити, що хтось підключився і коли (рис. 2.34).

Рис. 2.34. Додаток Who's On My Wi-Fi

Він може повідомити вас, коли ви не дивитеся за ним, щоб знали, коли хтось підключиться до мережі. Ви можете залишити його працювати на комп'ютері у себе вдома, а потім, коли прокидаєтеся, або повернулися додому з роботи, подивитися, що трапилося, поки ви не дивились.

Ваш наступний варіант, це перевірити можливості реєстрації свого маршрутизатора. Як правило, захована у глибині параметрів про виправлення неполадок або безпеку вашого маршрутизатора, вкладка присвячена реєстрації. Як багато можете зберегти і яку інформацію, змінюється залежно від маршрутизатора, але можете побачити на скріншоті (рис. 2.35), можна зберігати вхідний IP, номер порту призначення, вихідний IP або URL, що фільтрується згідно пристрою у вашій мережі, внутрішню IP-адресу та MAC адресу пристроїв, і які пристрої у вашій мережі перевірені в маршрутизаторі за допомогою DHCP для отримання своєї IP-адреси (і, за проксі, яке не мають). Це досить надійно, і чим довше ви залишили журнали запущеними, тим більше інформації можете захопити.

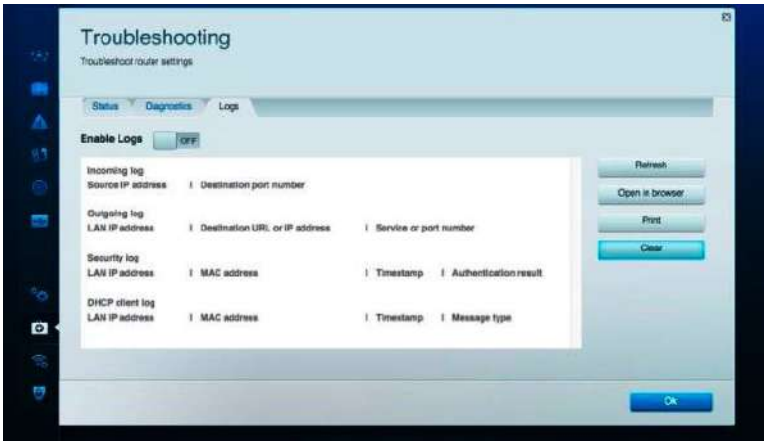


Рис. 2.35. Журнал маршрутизатора

Такі користувальницькі прошивки, як DD-WRT і Tomato дозволяють відстежувати і реєструвати пропускну здатності і підключення пристроїв доти, поки ви хочете, і навіть

може скинути цю інформацію в текстовий файл, який можна просіяти пізніше. Залежно від того, як ви налаштували свій маршрутизатор, він може навіть відправляти вам файл регулярно або помістити його на зовнішній жорсткий диск чи NAS. У будь-якому випадку, використовувати часто ігноровані функції реєстрації свого маршрутизатора – це відмінний спосіб побачити, що, наприклад, після півночі, коли всі пішли спати, ваш ігровий ПК раптом починає працювати і передавати багато вихідних даних, або у вас є регулярні п'явку, що люблять стрибати на ваш бездротовий доступ в Інтернет і починати завантаження торрентів протягом годин.

Ваш останній варіант, і це ядерний варіант: просто дайте Wireshark захоплювати протягом декількох годин або днів. Це не нечувано, і багато мережевих адміністраторів робить саме так, коли дійсно аналізують дивну поведінку в мережі. Це відмінний спосіб придавити поганих акторів чи балакучі пристрої. Тим не менш, варіант вимагає залишати комп'ютер протягом тривалого часу, постійно сніферити пакети в мережі, захоплюючи все, що відбувається в ній, і ці журнали можуть забрати чималий обсяг на вінчестері. Ви можете обрізати дещо за допомогою фільтрації IP захоплень або типу трафіку, але якщо не впевнені, що саме шукаєте, то отримаєте багато даних, які треба просіяти, коли переглядаєте захоплене протягом навіть кількох годин. Тим не менш, це, безумовно, розповість вам все, що потрібно знати.

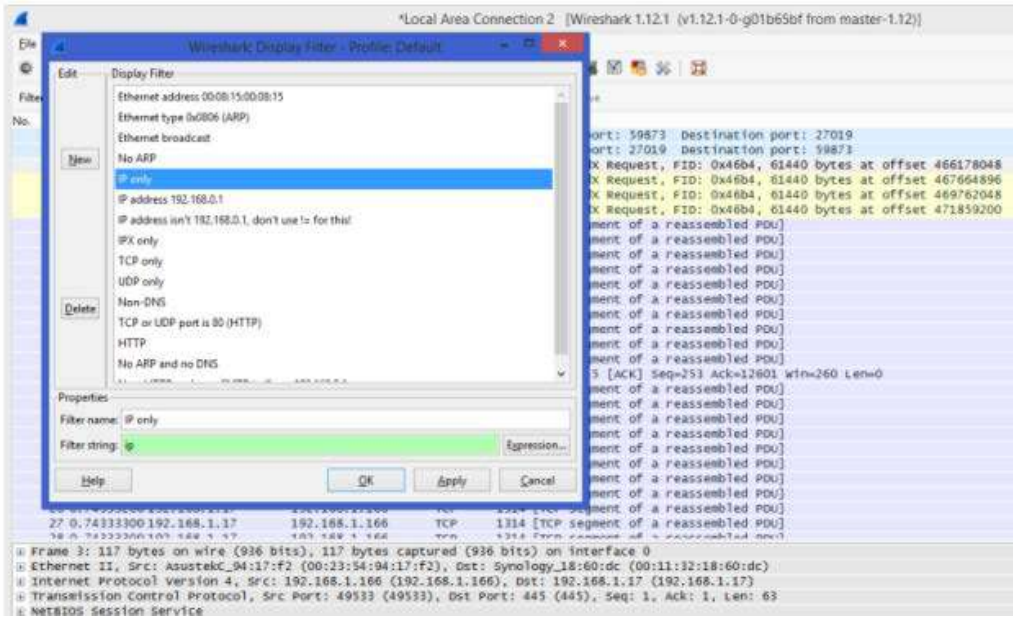


Рис. 2.36.

У всіх цих випадках, коли є достатньо даних в журналі, ви можете дізнатися, хто використовує вашу мережу, коли, і чи знайдені пристрої збігаються з картою мережі, яку ви зробили раніше

Крок 5. **Блокування своєї мережі від напасників**

Якщо ви все зробили разом з нами до цього місця, то вже визначили пристрої, які повинні мати можливість підключитися до домашньої мережі, і ті, які насправді підключені, визначені відмінності і, сподіваємося, розібралися, чи є які-небудь погані актори, несподівані пристрої, або стирчать п'явки. Тепер все, що вам потрібно зробити, це боротися з ними, і, що дивно, це найпростіша частина.

Wi-Fi п’явки будуть робити спроби завантаження, як тільки ви заблокуєте свій маршрутизатор. Перш, ніж зробити ще щось, змініть пароль маршрутизатора і вимкніть WPS, якщо він включений. Якщо комусь вдалося увійти безпосередньо до маршрутизатора, то ви ж не хочете змінити одні речі і залишити те, через що вони увійшли і отримали доступ. Переконайтеся, що використовуєте хороший, сильний, пароль, який складно зламати методом грубої сили. Потім перевірте оновлення прошивки. Якщо п’явка використала експлойта або уразливості в прошивці маршрутизатора, це утримає їх, припускаючи, що вразливість була виправлена, звичайно. Нарешті, переконайтеся, що режим безпеки бездротової мережі встановлений на WPA2 (тому, що WPA і WEP дуже легко зламати) і змініть свій Wi-Fi пароль на інший хороший, довгий пароль, який не може бути грубо підібраний. Тоді, тільки для пристроїв, які повинні бути в змозі перепід’єднатися, дайте новий пароль.

Це повинно захистити від тих, хто качав через ваш Wi-Fi і робив все своє завантаження в мережі. Також це допомагає з безпекою проводового підключення. Якщо можете, то повинні зробити ще кілька додаткових кроків для бездротової безпеки: відключення віддаленого адміністрування, відключення UPnP і, звичайно, подивитися, чи ваш маршрутизатор підтримує Tomato або DD-WRT.

Ви повинні дещо зробити для поганих акторів на своїх дротових комп’ютерах. Якщо це насправді фізичний пристрій, то він повинен мати пряме підключення до маршрутизатора. Почніть з відстеження кабелів і поговоріть з сусідами по кімнаті або сім’єю, щоб побачити що до чого приєднано. У гіршому випадку, ви завжди можете знову увійти на маршрутизатор і повністю блокувати підозрілу IP-адресу. Власник працюючої телеприставки або спокійно підключеного комп’ютера прибіжить досить швидко, коли вони перестануть працювати.

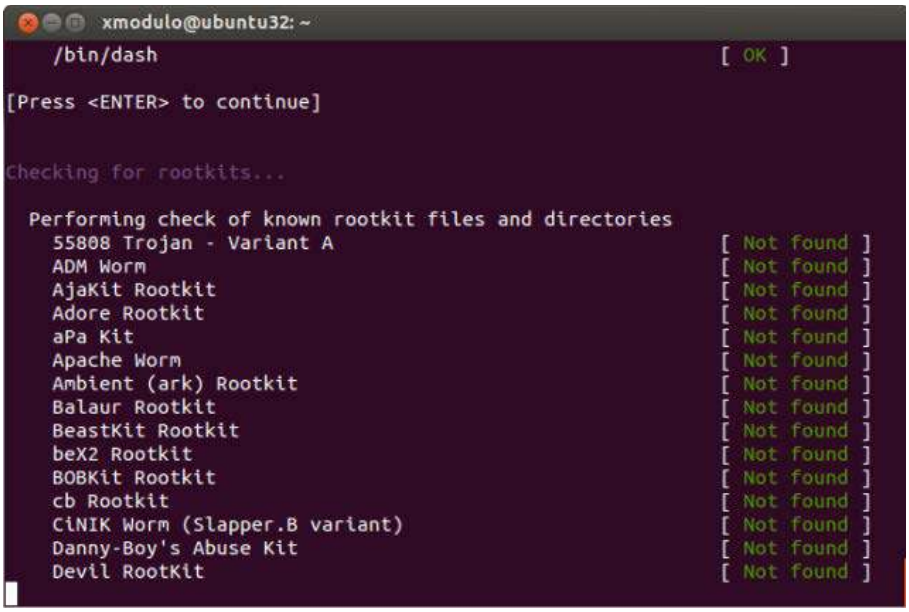


Рис. 2.37. Перевірка на наявність руткітів

Найбільше занепокоєння викликають компроментовані комп’ютери. Настільний комп’ютер, який був викрадений і приєднаний до бот-мережі для видобутку Bitcoin, наприклад, або машина, заражена шкідливими програмами, яка називається вами і посилає вашу особисту інформацію, хто-зна куди, може бути поганим. Після того, як ви звузити пошук конкретних комп’ютерів, прийшов час, щоб викорінити проблеми на кожній машині. Якщо дійсно стурбовані, прийміть підхід до проблеми як інженер з безпеки: після того, як

ваші машини змінили власника, вони більше не заслуговують довіри. Заберіть їх геть, перевстановіть або відновіть систему з резервних копій. (У вас є резервні копії своїх даних, чи не так?) Просто переконайтеся, що тримаєте контроль над ПК після всього – ви ж не хочете відновити з зараженої резервної копії і починати процес знову і знову.

Якщо готові засукати рукави, то можете захопити потужну антивірусну утиліту і серйозний сканер шкідливих програм (так, вам потрібно, обоє), та спробувати очистити комп'ютер, який під питанням. Якщо побачили трафік для певного типу додатків, подивіться, чи це не шкідливі програми або просто хтось щось встановив погане для себе. Продовжуйте сканування доти, поки не буде все чистим, і продовжуйте перевірку трафіку з цього комп'ютера, щоб переконатися, що все в порядку.

Ми дійсно тільки подряпали поверхню, коли справа дійшла до моніторингу та безпеки мережі. Є тони спеціальних інструментів і методів, які фахівці використовують для захисту своїх мереж, але наведені кроки будуть корисними для вас, якщо ви адмін мережі свого дому та сім'ї.

Викорінення підозрілих пристроїв або п'явок у мережі може бути тривалим процесом, який вимагає стеження і пильності. Тим не менш, ми не намагаємося робити вас параноїками. Є шанси, що ви не знайдете чогось надзвичайного, і повільні завантаження або паскудні швидкості Wi-Fi є чимось зовсім іншим. Тим не менш, це добре, знати, як досліджувати мережу і що робити, якщо знайшли щось незнайоме.

Тільки не забудьте завжди використовувати свої повноваження, не виходячи за їх рамки.

2.4. Перехоплення паролів WPA користувачів за допомогою атаки Fluxion

Залишається все менше життєздатних варіантів для тестів на проникнення за допомогою таких інструментів, як Reaver, бо інтернет-провайдери замінити вразливі маршрутизатори. Якщо у вас немає часу, щоб зламати пароль WPA, або він незвично сильний, то вам важко вибрати свій наступний крок.

На щастя, майже всі системи мають одну загальну вразливість, на яку ви можете розраховувати, – це користувачі!

Соціальна інженерія виходить за рамки апаратних засобів і атакує найбільш вразливу частину будь-якої системи, і одним з інструментів, який робить це супер просто, є Fluxion. Навіть самий антисоціальним хакер може ховатися за добре продуманою сторінкою входу в систему, а Fluxion автоматизує процес створення підробленої точки доступу для захоплення паролів WPA.

Вибір найбільш слабких ланок для нападу

Користувачі майже завжди є найслабшою ланкою системи, і тому напади на них часто є кращими, оскільки вони дешевші і ефективніші. Апаратні проблеми часто можуть бути проігноровані, якщо користувачі досить недосвідчені в технологіях атак соціальної інженерії. У той час як атаки соціальної інженерії можуть підняти прапори проти більш технічно підкованих організацій, атаки фішингу та спуфингу на користувачів є інструментом першого вибору як для держав, так і для кримінальних хакерів.

Одними з найбільш уразливих цілей такого роду атак є дрібний та середній бізнес, орієнтований на виробництво, а не на технології. Ці підприємства, як правило, мають багато вразливих або незакритих систем з обліковими даними за замовчуванням, які легко використовувати для бездротових мереж, бо вони не знають, як виглядає атака.

Як працює магія Fluxion

Fluxion – це майбутнє поєднання технічних і соціальних систем автоматизації, що змушує користувача передавати пароль Wi-Fi протягом декількох натискань клавіш. Зокрема, воно основане на соціальній інженерії з використання підробленої точки доступу (AP) «evil twin», інтегрованого блокування і функції захоплення рукостискання, ігноруючи апаратні засоби, а зосереджуючись на " wetware". Такі інструменти, як Wifiphisher[66], виконують подібні атаки, але в комплекті поставки не мають можливості перевіряти паролі WPA.

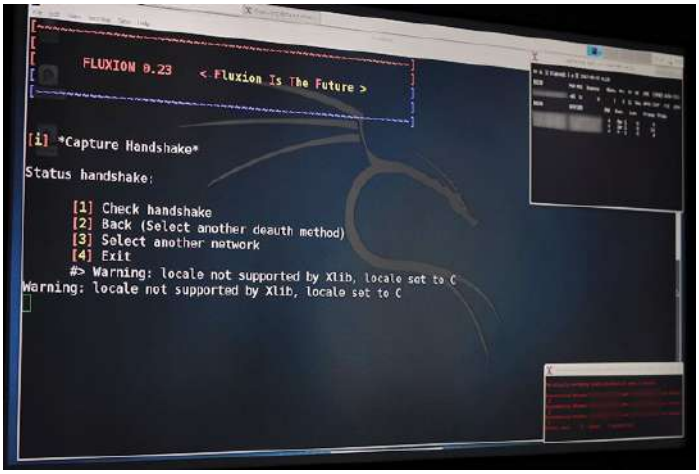


Рис. 2.38. Меню Fluxion

Fluxion еволюціонувала від просунутої атаки соціальної інженерії з назвою Lindset, в якій оригінальний інструмент був написаний в основному на іспанському і страждав від цілого ряду помилок. Fluxion є переписаною атакою, щоб обдурити недосвідчених користувачів і заставити розголосити паролі/ідентифікаційні фрази мережі.

Fluxion є унікальним інструментом при використанні для рукостискання WPA, коли можна не тільки контролювати поведінку сторінки входу в систему, але і поведінку всього сценарію. Створюється «клема» вихідної мережі і будується клон з таким же ім'ям, спокушаючи відключеного користувача приєднатися. Це будуть підроблені сторінки входу з зазначенням маршрутизатора, якого необхідно перезапустити або замінити прошивку і запитується мережевий пароль, щоб продовжити. Дуже просто.

Інструмент використовує захоплене рукостискання, щоб перевірити введений пароль і продовжує глушити цільову AP, поки не буде введений правильний пароль. Fluxion використовує розглянутий вище Aircrack-ng, щоб перевірити результати введенням паролю, і успішний результат означає, що пароль наш (рис. 2.39).

Рис. 2.39. Перевірка захоплення пароля WPA підтвердженням через Aircrack-ng

[66] https://null-byte.wonderhowto.com/how-to/hack-wi-fi-get-anyones-wi-fi-password-without-cracking-using-wifiphisher-0165154/

Тактично, ця атака добре працює тільки тоді, коли на екрані є підроблений вхід в систему. Багато з таких входів були додані до Fluxion під час створення, і можна створити інші екрани після деяких досліджень. Загалом, запуск цього нападу з екраном входу в систему за замовчуванням негайно зверне на себе увагу більш досвідчених користувачів або технічно підкованих в організації. Дана атака є найбільш ефективною, коли вона націлена проти того, хто є найстарішим або найменш технічно підкованим в організації. Чутливі точки доступу можна виявити за допомогою систем виявлення вторгнень і спробувати захиститися від цієї атаки, блокуючи ваш IP у відповідь на комплексне блокування.

Сумісність системи і вимоги

Fluxion працює на Kali Linux. Просто переконайтеся, що ви повністю оновлені, або що запустили Kali Rolling, щоб оновити систему і залежності до актуального стану. Ви можете запустити програму на спеціальному встановленій віртуальній машині Kali, або навіть на Raspberry Pi, якщо хочете мати невеликий портативний варіант (рис. 2.40).

Рис. 2.40. Запуск Fluxion

Цей інструмент не буде працювати через SSH, оскільки він спирається на відкриття інших вікон. Atheros AR9271 або інші сумісні з Kali бездротові мережеві адаптери повинні бути здатні переходити в режим моніторингу, а знайти його можете, прочитавши попередні матеріали про вибів Wi-Fi адаптера. Переконайтеся, що ваш бездротової адаптер здатний підключатися в режим моніторингу і розпізнається в Kali. Це можна зробити через команду `iwconfig` або `ifconfig`.

Як захопити паролі WPA з Fluxion

Нашою метою буде приєднатися до мережі підприємства через його Wi-Fi з шифруванням WPA. Ми почнемо атаку проти користувачів, підключених до точки доступу "Probe", захопленням рукостискання, потім створимо клоновану (evil twin) AP, заблокуємо цільову AP, створимо підроблену сторінку входу в систему і підтвердимо захоплений через рукостискання пароль.

Крок 1. **Встановлення Fluxion**

Щоб отримати Fluxion, запущений в нашій системі Linux Kali, клонуємо сховище Git з: `git clone https://github.com/wi-fi-analyzer/fluxion` (рис. 2.41).

```
root@Cine:~# git clone https://github.com/deltaxflux/fluxion.git
Cloning into 'fluxion'...
remote: Counting objects: 2326, done.
remote: Compressing objects: 100% (33/33), done.
Receiving objects: 100% (2326/2326), 26.51 MiB | 317.00 KiB/s, done.
remote: Total 2326 (delta 13), reused 0 (delta 0), pack-reused 2293
Resolving deltas: 100% (1290/1290), done.
root@Cine:~#
```

Рис. 2.41. Встановлення Fluxion через клонування

Тепер давайте перевіримо чи немає відсутніх залежностей, перейшовши в папку і запустивши Fluxion вперше (рис. 2.42):

```
cd fluxion
sudo ./fluxion
```

Рис. 2.42. Перший запуск Fluxion

Швидше за все, ви побачите наступне (рис. 2.43), де буде вказано на необхідність отримати деякі залежності:

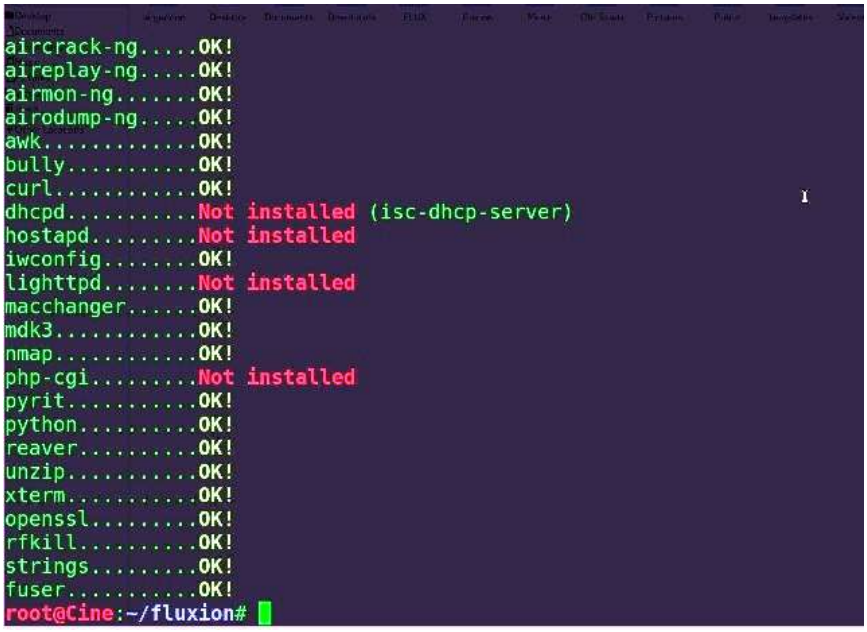


Рис. 2.43. Інформація про відсутні пакети

Запустіть програму установки для вилучення залежностей:

```
sudo ./Installer.sh
```

Відкриється вікно для обробки установки відсутніх пакетів (рис. 2.44). Будьте терплячі і дозвольте завершити установку залежностей.

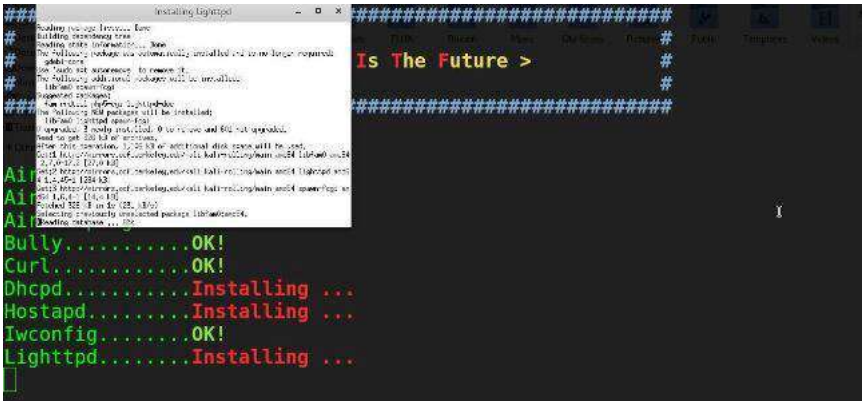


Рис. 2.44. Обробка установки відсутніх пакетів

Після того, як всі залежності будуть встановлені і наша плата зелена, можемо перейти до інтерфейсу атаки. Виконайте знову команду Fluxion з `sudo ./fluxion`, щоб запустити оновлений Fluxion (рис. 2.45).

Рис. 2.45. Оновлена програма Fluxion

Крок 2. **Сканування гарячих точок Wi-Fi**

Спочатку треба вибрати мову. Виберіть мову, ввівши номер поруч з нею, і натисніть клавішу **Enter**, щоб перейти до стадії ідентифікації цілі. Тепер, якщо канал мережі, який хочете атакувати, відомий, можете ввести 2, щоб звузити сканування лише на потрібний канал (рис. 2.46). В іншому випадку, виберіть 1, щоб сканувати всі канали, і продовжуйте сканування для збору даних бездротової передачі протягом не менше 20 секунд.

Рис. 2.46. Вибір або сканування каналів

Відкриється вікно, коли це відбувається. Натисніть **CTRL+C**, щоб зупинити процес захоплення щоразу, коли побачите бездротову мережу, яку хочете. Важливо дозволити виконання атаки протягом не менше 30 секунд, що буде достатньо для перевірки, чи клієнт підключений до мережі.

Крок 3. **Вибір вашої цільової AP**

Виберіть для атаки ціль з активними клієнтами, щоб запустити її, ввівши номер поруч з нею (рис. 2.47). Якщо не маєте наміру чекати, поки клієнт підключиться (можливо, протягом тривалого часу), то знайте, що атака не буде працювати в мережі без будь-яких клієнтів. Якщо немає нікого підключеного до мережі, то кого можемо обманним шляхом заставити дати нам пароль?

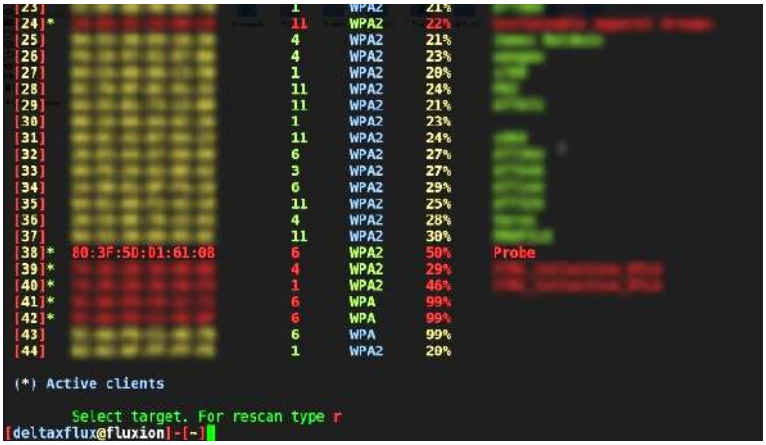


Рис. 2.47. Вибір клієнта для атаки

Крок 4. **Вибір атаки**

Після того, як ви ввели номер цільової мережі, натисніть клавішу введення, щоб завантажити профіль мережі в селектор атаки. Для наших цілей ми будемо використовувати варіант 1 (рис. 2.48), щоб зробити "FakeAP" за допомогою Hostapd. Це дозволить створити підроблену точку доступу за допомогою зібраної інформації, щоб клонувати цільову точку доступу. Введіть 1 і натисніть клавішу **Enter**.

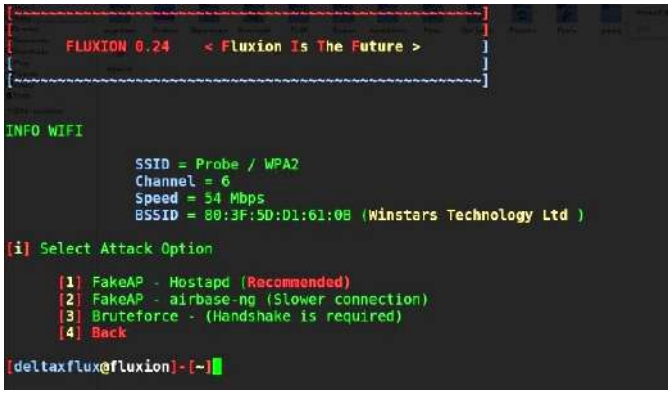


Рис. 2.48. Вибір типу атаки

Крок 5. **Отримання рукостискання**

Для того, щоб переконатися, що ми отримали працюючий пароль, перевіримо його проти захопленого рукостискання. Якщо у нас є рукостискання, то можемо ввести його на наступному екрані. Якщо немає, то можемо натиснути Enter, щоб змусити мережу виконати рукостискання в наступному кроці.

Використовуючи метод Aircrack-ng, вибравши варіант 1 ("aircrack-ng"), Fluxion пошле пакети деаутентифікації до цільової точки доступу як клієнт і прослухає отримане рукостискання WPA. Коли побачите, що рукостискання з’явилося, як це показано в правому верхньому куті екрану (рис. 2.49), то ви захопили рукостискання. Введіть 1 ("Check handshake") і натисніть Enter, щоб завантажити рукостискання в конфігурацію нашої атаки.

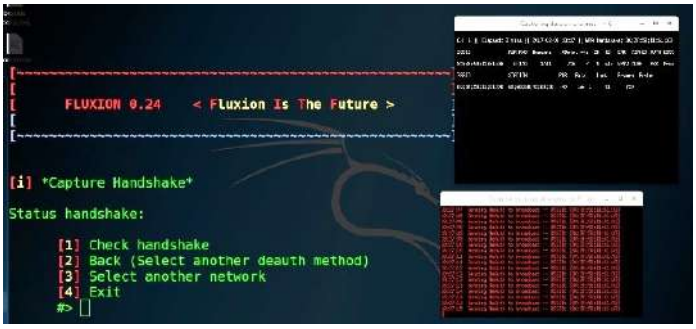


Рис. 2.49. Інформація про рукостискання

Крок 6. **Створення підробленої сторінки входу в систему**

Виберіть варіант 1 "Web Interface" (рис. 2.50) для використання інструменту соціальної інженерії.

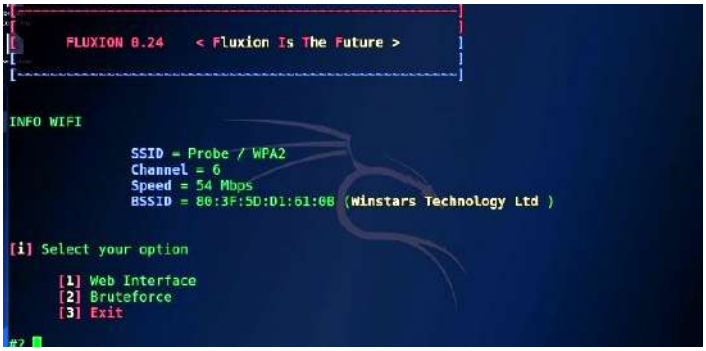


Рис. 2.50. Вибір інструменту Fluxion

Вам буде представлено меню різних підроблених сторінок входу, які ви можете надати користувачеві. Вони налаштовуються за допомогою деякої роботи, але мають відповідати пристрою і мові. Значення за замовчуванням повинні бути перевірені перед використанням, бо деякі з них не дуже переконливі.

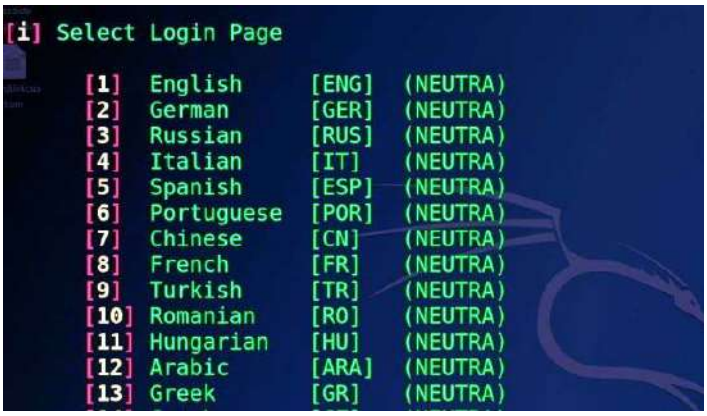


Рис. 2.51. Вибір мови

Виберемо, наприклад, напад англійської мови Netgear (рис.2.51). Це останній крок, щоб озброїти атаку. На даний момент, ви вже готові до «пострілу», тому натисніть клавішу **Enter**, щоб почати атаку (рис. 2.52). Атака породжує кілька вікон, щоб створити клоновану версію своєї бездротової мережі, одночасно заблокувати нормальну точку доступу, заманюючи користувача приєднатися до мережа з ідентичною назвою, але в незашифрованому вигляді.

Рис. 2.52. Процес атаки

Крок 7. **Захоплення пароля**

Користувач направляється на підроблену сторінку входу в систему (рис. 2.53), яка переконлива чи ні, в залежності від того, яку ви обрали.

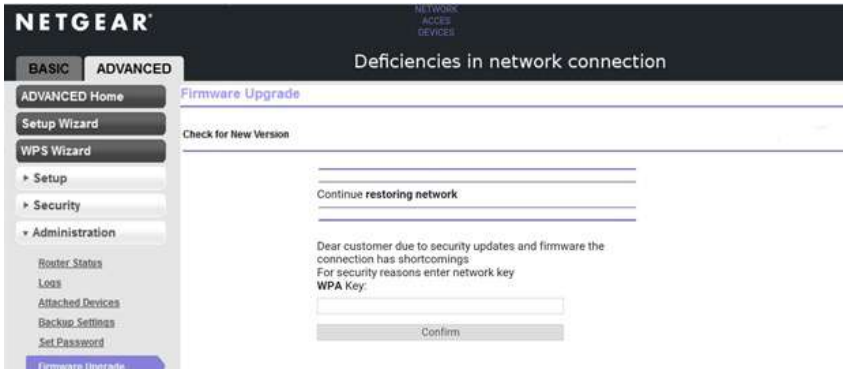


Рис. 2.53. Підроблена сторінка входу в систему

Можливо, це не самий витончений обман, але всі файли можна налаштовувати.

Через введення неправильного пароля відбудеться збій перевірки рукостискання і користувачеві буде запропоновано спробувати ще раз. Після введення правильного пароля, Aircrack-ng перевіряє і зберігає пароль у текстовий файл, який відображається на екрані.

Користувач перенаправляється на екран "thank you", глушіння припиняється і вимикається підроблена точка доступу.

Ви можете перевірити, чи досягли успіху, шляхом перевірки зчитування екрану Aircrack-ng.

Рис. 2.54. Ключ захопили і перевірили

Вітаємо, ви досягли успіху в отриманні та перевірці паролю, що поставляється з прицілом на "Wetware." Ми обдурили користувача з введенням паролю, не покладаючись на раніше існуючі вади з безпекою.

Увага: Використання даної техніки без дозволу може бути незаконним.

З юридичної точки зору Fluxion поєднує в собі сканування, клонування, створення підробленої AP, створення фішингового екрану входу в систему та використання сценарію Aircrack-ng для отримання і злому рукостискань WPA. Таким чином, залишається запис в логах маршрутизатора, які узгоджуються з допомогою цих методів. Більшість з цих методів є незаконними і небажаними для будь-якої системи, якщо у вас немає дозволу на проведення аудиту.

2.5. Як зламують WPA/WPA2-Enterprise

WPA Enterprise широко використовується у великих корпораціях, бо з ним пропонується індивідуальне та централізоване управління через сервер, який визначає автентичність користувачів (RADIUS-сервер).

Розглянемо, як зламують бар'єр і отримують реєстраційні дані.

Як це працює?

Давайте кинемо швидкий погляд на те, що обговорюємо.

Рис. 2.55. Аутентифікація з використанням сервера RADIUS

RADIUS є абревіатурою від Remote Authentication Dial-In User Service – служба аутентифікації віддалених користувачів через комутовані канали зв'язку. Коли користувач

запитує підключення до мережі за допомогою вірчих сертифікатів, запит перенаправляється на сервер RADIUS (рис. 2.55). Він перевіряє інформацію і, якщо правильна, призначає клієнту мережеві ресурси, такі як конкретна IP-адреса.

У деяких випадках облікові дані, які використовуються для підключення до мережі компанії, такі ж, які використовують користувачі для доступу до послуг компанії. Це означає, що якщо ви отримали ці дані, то зможете їх ввести в обліковий запис електронної пошти користувача, наприклад. Цікаво? Думаю, що так.

У великих компаніях точки доступу (AP) до мережі, як правило, розподілені з метою забезпечення хорошого сигналу Wi-Fi для всіх користувачів. У нашому випадку, ми будемо діяти як точка доступу мережі і запити користувача будуть перенаправлятися на наш сервер RADIUS!

Крок 1. **Передумови**

Те, з чого ми повинні почати:

- Kali Linux (версія 1)
- зовнішній мережевий адаптер (з мікросхемою від Atheros)

Перш за все, ми збираємося налаштувати сервер RADIUS на машині атакуючого, щоб слухати користувачів, які підключаються до мережі. Щоб зробити це, ми використаємо сценарій, який спрощує весь процес, щоб зробити все набагато простіше. Це сценарій easy-creds і ви можете завантажити його з сайту[67].

Відкрийте термінал і перейдіть до папки, куди ви розмістили архівний файл (зазвичай, папка *Завантаження*). Введіть:

```
tar -xzvf easy-creds-3.8-DEV.tar.gz
```

Змініть каталог на `easy-creds` і введіть:

```
./installer.sh
```

Ми використовуємо Kali, який зібраний на основі Debian, тому оберіть варіант 1. Вам буде запропоновано ввести шлях, куди ви хочете встановити easy-creds, автор вказав `/opt/`.

Тепер будуть встановлені всі необхідні компоненти. Даний сценарій може робити й інші такі речі, як створити Evil Twin, але ми охоплюємо тільки FreeRADIUS Attack.

Крок 2. **Захоплюємо хеші**

Тепер, коли ми закінчили установку, давайте запустимо AP і сервер RADIUS.
У терміналі введіть:

```
easy-creds
```

Коли ви будете на екрані вибору (рис.2.56), виберіть опцію 3: FakeAP Attacks.

Тепер, виберіть опцію 4: FreeRadius Attack (рис. 2.57) (*Примітка:* Ця атака працює тільки на мікросхемах Atheros, ми використовували TP-LINK TL-WN722N, який коштує близько 12$ і працює бездоганно).

Вам буде запропоновано ввести розшарений ключ, ви можете вказати тут будь-що, в нашому випадку "sharedsecret". Виберіть інтерфейс, який хочете використовувати (щось на зразок `wlanX`). Введіть ESSID мережі підприємства (наприклад, якщо ім'я мережі є "CompanyNetwork", то необхідно ввести це ім'я). Виберіть канал і ... запустіть захоплення (рис. 2.58)!

[67] https://sourceforge.net/projects/easy-creds/

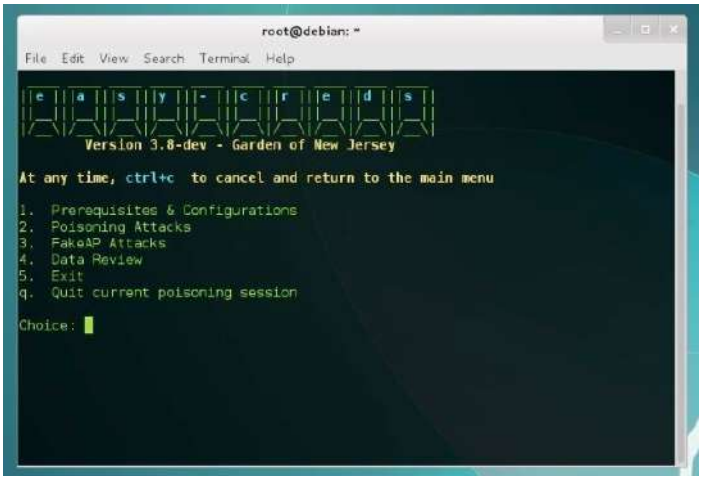


Рис. 2.56. Вибір FakeAP Attacks (опція 3)

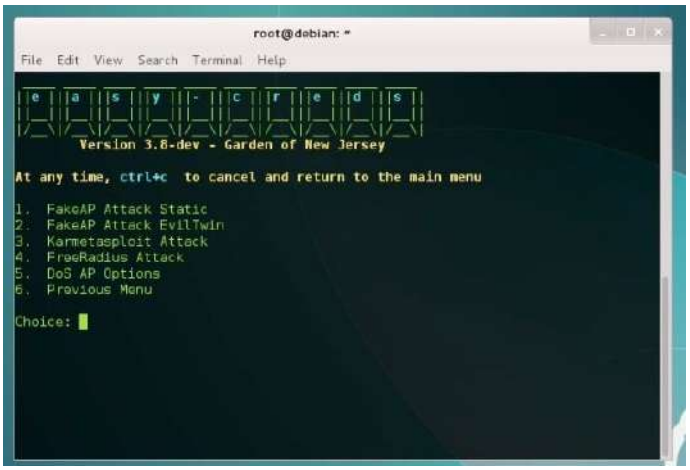


Рис. 2.57. Вибір FreeRadius Attack (опція 4)

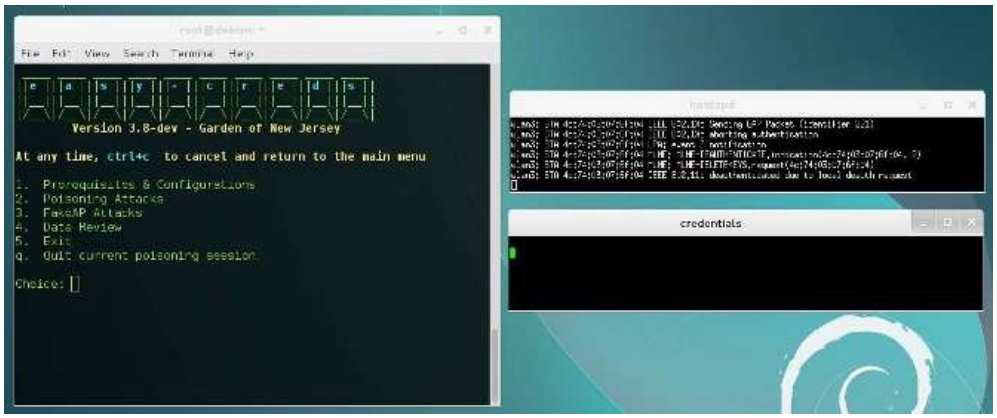


Рис. 2.58. Процес захоплення паролів

Коли користувачі підключаються до нашої AP, хеші будуть з’являтися в екрані облікових записів у форматі запит/відповідь. Аутентифікація типу виклик/відповідь є сімейством протоколів, в яких одна сторона задає питання (виклик), а інша сторона повинна дати обґрунтовану відповідь (відгук) для проходження авторизації. У цьому випадку наш RADIUS запитує пароль (виклик), і користувач відповідає з інформацією про нього (відгук).

Наш локальний сервер RADIUS використовує PEAP (Protected Extensible Authentication Protocol) для перевірки автентичності, який заснований на дайджесті MSCHAPv2 з NetNTLMv1. Знати це дуже важливо, тому що далі використаємо цю інформацію, щоб отримати паролі.

Коли ви закінчите захоплення, введіть 5 (рис. 2.58) і натисніть **Enter**, щоб вийти з easy-creds. Захоплені дані були збережені у папці з датою захоплення, в нашій домашній директорії (ми використовуємо Kali, тому наша домашня директорія `/root/`). Усередині цієї директорії є файл з ім'ям `FreeRADIUS-credsXXXXXXXX.txt`, з якого ми повинні отримати паролі у вигляді простого тексту.

Крок 3. **Зламуємо хеші**

Після того, як у нас є хеші паролів, ми можемо зламати їх за допомогою деяких інструментів, типу John the Ripper або Hashcat, про що буде далі.

Тепер ми збираємося зламати хеши, які захопили раніше. Пояснимо, як це зробити з потужним John the Ripper. Він поставляється з Kali за замовчуванням, тому немає необхідності в установці.

Використовуємо John the Ripper

Якщо ви нічого не знаєте про цей інструмент, то можете перечитати статтю у Вікіпедії[68].

По-перше, ми повинні надати для John хеші паролів в зручному форматі. Щоб зробити це, використаємо простий сценарій, що конвертує наш файл FreeRADIUS-credsXXXXX.txt у формат John, який можете завантажити з сайту[69].

Відвідайте вказане посилання, скопіюйте текст сценарію в буфер обміну і відкрийте термінал.

Введіть: `sudo nano radiustojohn.py`

Вставте текст з буфера обміну і натисніть **Ctrl+O**, щоб зберегти зміни, а потім **Ctrl+X** для виходу. Змініть права доступу до файлу за допомогою команди:

chmod +x radiustojohn.py

Тепер виконайте сценарій з вказаним як параметр файлом `FreeRADIUS-credsXXXXXXX.txt`:

```
./radiustojohn.py <path to the freeradius-creds file>
```

Ми згенерували файл `freeradius.john`, який John може зрозуміти. Введіть (рис. 2.59):

```
john --format=netntlm freeradius.john
```

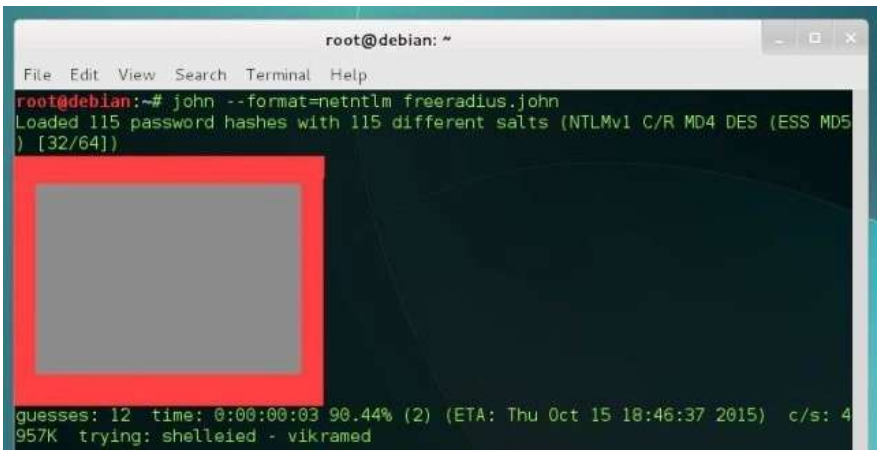


Рис. 2.59. Запуск John

[68] https://en.wikipedia.org/wiki/John_the_Ripper
[69] https://pastebin.com/RJwgbwNh

У будь-який момент ви можете натиснути будь-яку клавішу, щоб побачити статус. Як ви можете побачити, ми за приблизно 3 секунди знайшли 12 паролів. Чим слабкіший пароль, тим швидше його зламати. Щоб зламати сильні паролі можна затратити зайняти роки, звичайно, ви можете скористатися налаштованим списком слів:

```
john --format=netntlm --wordlist=<шлях до вашого файлу словника> freeradius.john
```

Якщо ви знаєте щось про пароль, наприклад, його довжину, ви можете змінити файл конфігурації John для того, щоб спробувати тільки паролі даної довжини. Файл конфігурації знаходиться в `/etc/john/john.conf`, але давайте спочатку зробимо резервну копію цього файлу:

```
cd /etc/john/
cp john.conf john.conf.old
```

Тепер, коли ми зробили резервну копію оригінального файлу, давайте змінювати:

```
leafpad john.conf
```

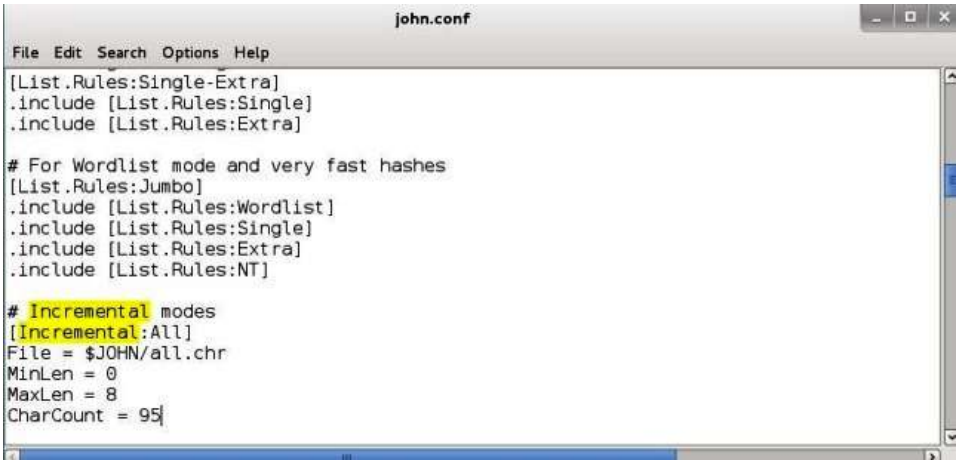


Рис. 2.60. Введення початкових параметрів для паролю

Тепер у файл, змініть `MinLen` і `MaxLen` для довжини пароля. Уявіть собі, що ви знаєте, що довжина пароля саме 8 символів, тому ви повинні поставити 8 в MinLen і 8 в MaxLen (рис. 2.60). Збережіть зміни і запустіть John:

```
john --format=netntlm --incremental=All freeradius.john
```

John також підтримує OpenCL для роботи з GPU, що допоможе зламати набагато швидше.

2.6. Як захистити себе від програм, які роблять злом Wi-Fi простим

Це не параноя: громадські або відкриті Wi-Fi мережі, не привертаючі увагу до безпеки, є поганою ідеєю.

Вам навіть не доведеться зламувати паролі мережі, щоб захопити тонни даних у нічого не підозрюючих користувачів мережі. Вище ми показали, як це зробити, і що треба зробити, щоб цього не сталося з вами. Тепер, BetterCAP[70], інструмент безпеки, який робить процес настільки простим, що будь-хто зможе це зробити.

Подивимось, як він працює і як захистити себе.

[70] https://www.bettercap.org/

Що таке BetterCAP?

BetterCAP – потужний, гнучкий та портативний інструмент, створений для виконання різних типів атак MITM на мережу, маніпулювання HTTP, HTTPS та TCP трафіком у режимі реального часу, витягування облікових даних та багато іншого. BetterCAP насправді є набором засобів безпеки, об'єднаних в одному додатку. Це відмінна утиліта, якщо ви фахівець з безпеки або інший, хто насолоджується плюсами і мінусами мережевої безпеки, зломом і тестування на проникнення. Ми хочемо внести ясність, що не відносимо цей інструмент до лиходійників.

На відміну від таких додатків, як Firesheep, Faceniff і Droidsheep, BetterCAP не робився з єдиною метою злому мереж або викрадення сесій користувача. Він, безумовно, може винюхувати паролі, які передаються у вигляді звичайного тексту на відкритій мережі, і він може зламати погано захищену Wi-Fi мережу. Він також може сканувати мережі на наявність вразливостей, зламувати ключі на загальних маршрутизаторах і, звичайно, блокувати браузери, веб-сайти, або сесії соціальних мереж і триматися за них. Ви можете побачити на сайті повний список можливостей інструменту.

Для фахівців з безпеки, любителів пошуку доступних способів дізнатися більше про мережеву безпеку (або тих, на чий офіс покладена безпека Wi-Fi, але які не можуть дозволити собі професійних пентестерів), або для тих, хто шукає, як захистити свої власні мережі, BetterCAP може бути цінним ресурсом. Він також може бути цінним для тих, хто хоче вкрасти ваші дані. Ось чому ми збираємося поговорити про те, як він працює і як ви можете захистити свої паролі та особисті дані від будь-кого за допомогою цього набору.

Як працює BetterCAP (та інші подібні програми)

BetterCAP дозволяє легко робити дві речі: винюхувати паролі під час передавання в незашифрованому вигляді і викрадати активні сесії браузера, а тому може маскуватися під когось, хто вже увійшов на сайт, або на сервіс. В обох випадках, дійсно потрібно тільки один дотик для операції, якщо додаток вже у вас встановлений. Перше зробити легко. Якщо хтось заходить на сайт, або входить в сервіс, не використовуючи HTTPS або SSL, то пароль, швидше за все, направляє у вигляді відкритого тексту. Будь-хто може сніферити пакети в мережі і може захопити їх без необхідності робити будь-який реальний тип інспекції пакетів, і як тільки їх отримає, спробує їх на кількох сайтах і сервісах, що можна побачити, як використовувати їх для інших облікових записів.

Друге – трохи складніше. Якщо ви не знайомі з захопленням сеансу, то це процес захоплення куків для використання дійсно активного сеансу інших користувачів з безпечного сервісу для того, щоб видати себе за іншого користувача. Оскільки ніяких важливих даних, як ім'я користувача або пароль, не передається в куках, вони, зазвичай, передаються у відкритому вигляді і, в більшості випадків, використовуються на веб-сайтах і в соціальних мережах як спосіб ідентифікації користувача в поточній сесії, щоб сайт щоразу при завантаженні не забував, хто ви. Це найбільш поширені атаки на додатки, які винюхують паролі та сесії за допомогою Wi-Fi. Нижче ми покажемо вам, як працювати з Disconnect[71], одним з наших улюблених розширень браузера для захисту конфіденційності.

BetterCAP виконує захоплення сеансу аналогічним чином, як і інші інструменти групи, про які ми вже згадували в основному тому, що це добре працює. Багато веб-сайтів просто шифрують ваші ім'я користувача та пароль, і як тільки зроблена ця передача

[71] https://chrome.google.com/webstore/detail/disconnect/jeoacafpbcihiomhlakheieifhpjdfeo?hl=uk

обслуговування – все інше передається в незашифрованому вигляді. Хоча чимало сайтів перейшли на HTTPS, більшість з них вимагають активації параметру HTTPS. Багато ж інших сайтів взагалі.не турбуються про переїзд на HTTPS.

З появою соціальних мереж, однак, все більше і більше приватної інформації передається через веб-сайти без будь-якого рівня захисту. Хоча цілком можливо, посиливши свою приватність, зробивши профіль приватним, ваші дані все ще будуть передаватися в незашифрованому вигляді і, таким чином, можуть бути легко перехоплені. Твіттер і Facebook відреагували і запропонували додатково захищене з'єднання, тобто HTTPS.

Що означає HTTPS?

HTTPS означає HyperText Transfer Protocol Secure. Щоб розібратися в цій загадковій назві, давайте розіб'ємо її на складові частини.

HyperText описує вміст веб-сайту, який не вимагає скрипти або плагіни, тобто текст, таблиці або зображення. Слово також знаходиться в акронімі HTML, що означає мову розмітки гіпертексту.

HTTP є мережевим протоколом, який виконує передачу даних між клієнтами, наприклад, браузером і сервером, яким зазвичай є комп'ютер хостингу веб-сайту.

Безпечні з'єднання представляють собою комбінацію з двох протоколів: HTTP та SSL/TLS. Останні є криптографічними протоколами, які шифрують з'єднання мережі. Скорочення перекладаються як протоколи Secure Sockets Layer і Transport Layer Security. Окрім перегляду веб-сторінок, ці протоколи використовуються для шифрування передачі даних в повідомленнях електронної пошти, онлайн-факсів, миттєвих повідомлені і голосу поверх IP.

Взяті разом протоколи утворюють HTTPS, який означає, що зв'язок "звичайного тексту" веб-сайту зашифрований для підвищення безпеки.

Який реальний ризик?

Реальний ризик від подібних інструментів різний. Шанси, що ви зіткнетеся в місцевому кафе з кимось, хто працює з BetterCAP, Firesheep, або будь-яким іншим додатком, який захоплює для них паролі і викрадає сесії, досить малі, але, як ми вже згадували, що досить всього однієї людини, щоб зіпсувати вам день.

Хтось міг би просто захопити настільки багато сесій Facebook або Twitter, наскільки вони зможуть (після чого вони можуть змінити пароль користувача і зберегти обліковий запис Facebook для себе), викрасти торгові сесії Amazon і захопити адресу і дані кредитної карти, читати електронну пошту та чати, тощо. Ризик зростає, бо все більше і більше інструментів, які прості для використання будь-ким, а також збільшується кількість людей, які просто не захищають себе шифруванням своїх даних.

Як можна захистити себе?

Захистити себе від цих інструментів насправді на диво легко, якщо ви докладете зусиль, щоб дійсно це зробити:

- Включіть HTTPS для кожного сайту, який дозволяє підключатися через нього, і встановіть HTTPS Everywhere[72]. Це дозволить переконатися, що ви використовуєте

[72] https://www.eff.org/https-everywhere

HTTPS завжди, коли це можливо, і жоден трафік вашого веб-серфінгу не передається в незашифрованому вигляді.

- Отримайте розширення браузера для захист конфіденційності, типу Disconnect, який також захищає від злому віджета або бічного викрадення. Disconnect є нашим улюбленим, але він не повинен бути єдиним інструментом у вашому інструментарії.
- Використовуйте VPN при перегляді в громадських місцях, безкоштовних, або в інших відкритих мережах. Використання VPN є кращим способом, щоб переконатися, що всі ваші дані зашифровані і захищені від будь-кого в тій же мережі, будь то провідна або бездротова, державна чи приватна.
- Використовуйте свою голову і дотримуйтесь гігієни Інтернету. Відточіть свої навички та виявлення афер фішингу, переключіть ваш BS Detecter в максимум. Ніхто не повинен захопити ваш сеанс або паролі, щоб дістатися до вас, – вони так само легко замінять сайт, на якому ви знаходитесь на інший, що виглядатиме подібно, але наполягатиме, щоб ви надали йому тонну даних. Будьте розумними.

Не займе багато часу використовувати HTTPS скрізь, де можна, запустіть VPN, якщо ви збираєтеся працювати з бібліотеки, або просто не використовуйте громадський Wi-Fi і почекайте, поки ви не повернетеся додому, або замість цього скористайтеся мобільним Інтернетом зі свого телефону (що завжди є іншим варіантом). Проте, ми застерігаємо тих, хто хоче недобросовісного використання цих інструментів, що можете мати проблеми, а інструменти тільки для тих, хто потребує їх використання для захисту. Тим не менш, поки вони настільки ефективні, то має сенс прийняти необхідні заходи, щоб захистити себе.

В наступному розділі ми навчимося, як користуватися запрпонованими інструментами безпеки.

3. Анонімність в Інтернеті

3.1. Вимкніть блоки відстеження даних, соціальні віджети та інше в Chrome і Firefox

Ви можете думати про Інтернет як кращий винахід після колеса, але цей винахід за багато років перетворився на досить «пиляючий екран» через масу «дрібниць»

Це постійно спливаючі вікна реклами, куки, які відстежують ваші дані в маркетингових цілях, повільна швидкість завантаження, викликана соціальними віджетами, шкідливі та шпигунські програми, нав’язливі повідомлення та ще багато чого.

Люди схильні використовувати кілька розширень браузера, щоб позбутися усіх, пов’язаних з браузером, неприємностей, але якби ви могли позбутися їх усіх і насолоджуватися приватною, безпечною і швидкою роботою в Інтернеті, чого заслуговуєте, використовуючи тільки одне розширення мережі? Disconnect – розширення з відкритим вихідним кодом для Mozilla Firefox[73] і Google Chrome[74], яке дозволяє назавжди блокувати такі неприємності. Веб-розширення призначене для фільтрації небажаних інструментів відстеження та віджетів, які просто уповільнюють швидкість роботи вашого браузера.

[73] https://addons.mozilla.org/uk/firefox/addon/disconnect/
[74] https://chrome.google.com/webstore/detail/disconnect/jeoacafpbcihiomhlakheieifhpjdfeo?hl=uk

Для початку, просто завантажте розширення Disconnect для будь-якого з підтримуваних веб-браузерів (рис. 3.1).

Рис. 3.1. Сторінка сайту з Disconnect

Зайдіть на сторінку Disconnect і натисніть велику зелену кнопка Get Disconnect (рис.3.2). Сервіс автоматично розпізнає ваш веб-браузер і підкаже відповідне розширення, так що далі досить дотримуватися деяких інструкції на екрані, щоб отримати розширення.

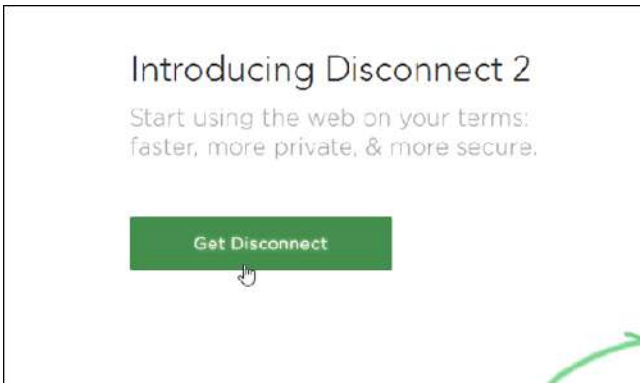


Рис. 3.2. Сторінка завантаження Disconnect

Хоча це безкоштовний у використанні додаток, ви можете пожертвувати розробникам, заплативши їм, скільки ви вважаєте Disconnect вартий, щоб зберегти проект працюючим. Гроші від пожертвувань також можна поділити між командою Disconnect і благодійністю. Ви можете сплатити за допомогою кредитної карти або з вашого рахунку PayPal. Тим не менше, якщо хочете пропустити цей крок, просто виберіть заплатити $0 (рис. 3.3).

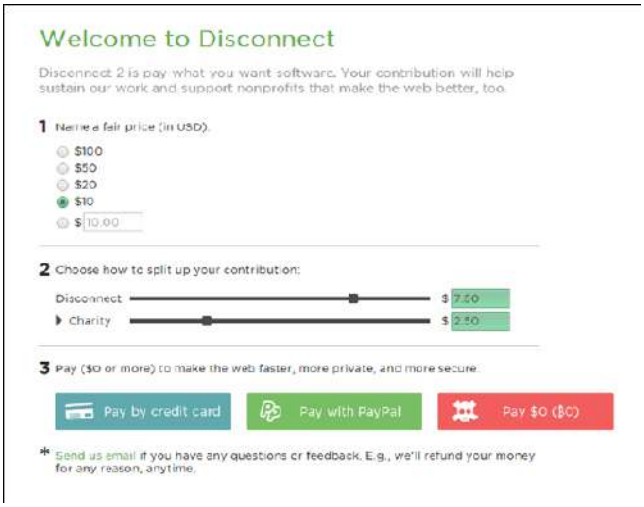


Рис. 3.3. Вибір параметрів

Розширення додає кнопку панелі інструментів Disconnect до веб-браузера. При відвідування веб-сайту, ви можете натиснути цю кнопку, щоб побачити, які відстеження інформації будуть заблоковані на ньому, наприклад, дані, що надходять із соціальних віджетів, типу, Facebook, Twitter і Google+, куки відстеження, Google Analytics, соціальні запити і так далі (рис. 3.4). Інтерфейс виглядає яскравим, чистим і простим, і досить інтуїтивний для орієнтації.

Кнопки автоматично змінюють свій колір між зеленим і сірим, де зеленим позначені заблоковані запити, в той час як сірі показують розблоковані запити. Ви можете натиснути будь-який значок, щоб на льоту включити або відключити блокування для даного запиту. Розширення навіть надає внизу статистичну діаграму, представляючи збережений час і трафік, і безпечні запити.

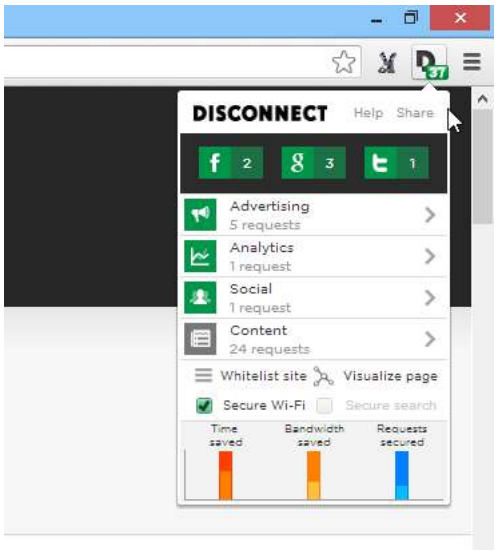


Рис. 3.4. Кнопки для блокування

Крім вертикально відображеної в стислій формі інформації, ви також можете звернутися до функції "Сторінка візуалізації" (рис. 3.5), яка перемикає вигляд списку за замовчуванням до ретельнішого подання з використанням візуального графіка. Це також дає вам уявлення про те, як веб-сайти пов'язані з іншими сервісами та сайтами, а наведення курсору миші на кожне коло розкриває їх назву.

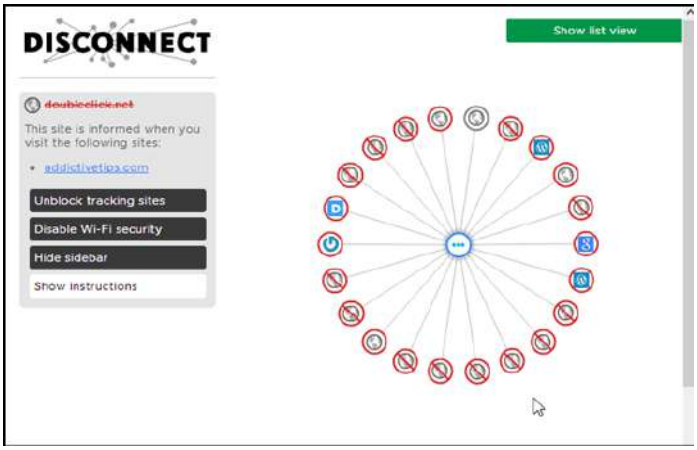


Рис. 3.5. Сторінка візуалізації

У двох словах, це досить хороший додаток, який надає швидкий і безпечний перегляд веб-сторінок, не використовуючи купу різних інструментів для цієї мети. Випробування проводилися на Google Chrome при роботі на Windows 8 Pro 64-біт.

3.2. Як змінити «відбитки пальців» вашого браузера так, щоб він більше не був унікальним

Відстеження є тим, чому інтернет-користувачі піддаються незалежно від того, куди вони йдуть[75].

Веб-сайти використовують програмне забезпечення аналітики, щоб їх відстежувати, рекламні компанії використовують відстеження, щоб заробити більше грошей через цільові оголошення, і соціальних мережі теж майже завжди можуть знати, де ви були, тому що кнопки і скрипти встановлені на більшості веб-сайтів.

Є й менш очевидні способи та можливості відстеження користувачів, і один з них використовується у вигляді «відбитків пальців» браузера. При підключенні до веб-сайту інформація про вашу систему і браузер доступна серверу, до якого ви підключаєтеся. Ця інформація використовується для отримання «відбитків пальців» браузера, що працює дуже добре, враховуючи, що віддалений сервер має доступ до такої інформації, як агент браузера, заголовки, часовий пояс, розмір екрану і глибина кольору, плагіни, шрифти і ряд інших точок даних.

Створений Panopticlick[76] був для того, щоб надати користувачам Інтернету засіб подивитися, наскільки насправді унікальний їх браузер (рис. 3.6). Щоб з'ясувати це, просто завантажте веб-сайт і запустіть на ньому тест. В кінцевому підсумку отримаєте звіт, який покаже вам, наскільки ваш браузер є унікальним серед інших, які були протестовані до нього, або він має ті ж «відбитки пальців», що й інші.

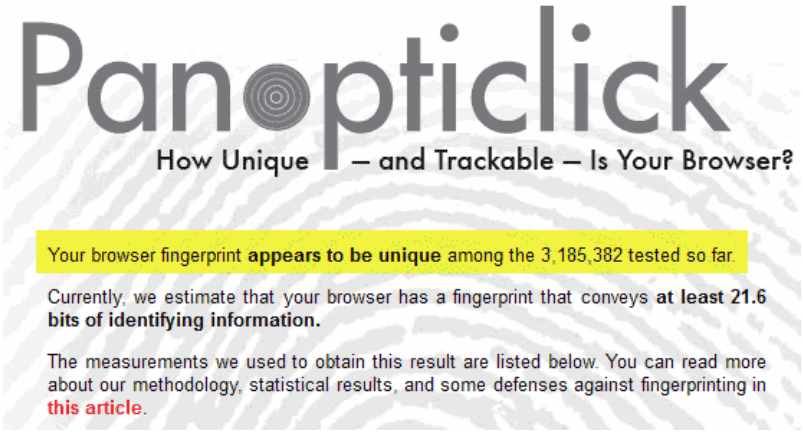


Рис. 3.6. Повідомлення про унікальність браузера

Унікальний – в цьому тесті це погано, бо це означає, що ніякий інший випробуваний браузер не мав всі характеристики однакові з вашим. При тому, що «відбитки пальців» створені, теоретично через них можна ідентифікувати вас на веб-сайтах, які відвідуєте, за умови, що ваш браузер унікальний.

*Примітка:*В той час, як Panopticlick відображає за допомогою тесту браузер як унікальний, то це не обов'язково означає, що він дійсно унікальний, враховуючи, що більшість інтернет-користувачів не перевіряли свій браузер на даному сайті.

[75] http://isearch.kiev.ua/uk/news/programs/tools-sec/1738-how-to-change-the-qfingerprintq-of-your-browser-so-that-it-was-no-longer-unique
[76] https://panopticlick.eff.org/

Налаштування Вашого браузера

Якщо вам не подобається те, що ваш браузер унікальний, ви можете зацікавитись програмами тонкого налаштування для зменшення виявлення бітів інформації, які показує браузер, коли підключається до веб-сайтів (рис. 3.7).

Це може здатися простим, на перший погляд, але насправді це не так. Деяка інформація не може бути відключена, так як вона завжди передається незалежно від того, що ви робите. Відключення певних функцій, таких як модулі, також може бути використане для дактилоскопії. Якщо ви запускаєте браузер без плагінів, то це ознака того, що веб-сайти також можуть використовувати це для зняття «відбитків пальців».

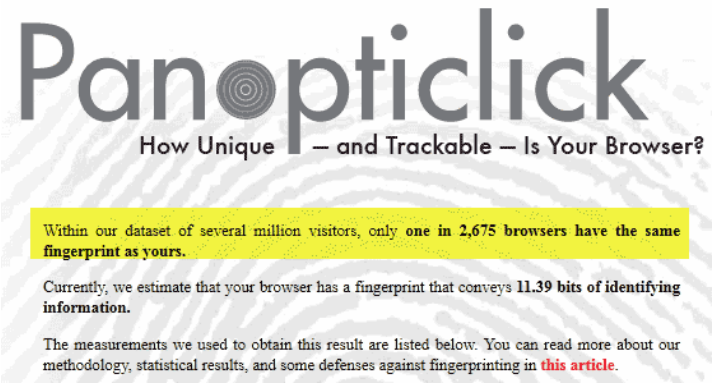


Рис. 3.7. Інформація про браузери

Отже, як отримати ваш браузер без наявності унікального «відбитка пальця», щоб його відбитки співпадали з «відбитками пальців» інших браузерів?

Ідея полягає в тому, щоб змінити такі параметри, як агент користувача або розмір екрану і глибину кольору, щоб вони відповідали найбільшому відсотку браузерів. Замість того щоб використовувати агента користувача FirefoxNightly, наприклад, ви можете використовувати агента користувача, який використовується найчастіше.

3.3. Як зробити серфінг в Інтернеті анонімним з Tor на Raspberry Pi

Якщо ви думали про Tor, щоб анонімізувати весь свій веб-серфінг, то можете просто The Tor Browser, але набагато більше задоволення зробити свій власний портативний проксі, до якого можете легко підключитися інтуїтивно. Додайте Raspberry Pi[77].

Tor є одним з найпростіших способів для анонімного перегляду в Інтернеті, хоча при цьому дійсно втрачаємо швидкість. Насправді, це досить повільно, що важко використовувати для основного перегляду в Інтернеті. Але це не означає, що це не корисно для інших речей, і так як ви, ймовірно, не хочете використовувати його весь час, то швидкий спосіб перемикання між Tor і регулярним Інтернетом є зручним.

Може допомогти Raspberry Pi. Перш за все, необхідно, зробити з Raspberry Pi точку доступу, так само, як точки доступу Wi-Fi, а потім встановити Tor на неї, щоб весь трафік, який проходить через цю точку доступу, був анонімний.

Якщо хочете використовувати Tor, то просто підключіться до мережі Wi-Fi через Raspberry Pi. Коли ви цього не робите, то можете підключитися до будь-якої мережі, яку

[77] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1942-how-to-surf-the-internet-anonymously-with-tor-on-raspberry-pi

використовуєте зазвичай. Завжди варіантом є The Tor Browser[78], але, можливо, вам не хочеться встановлювати програмне забезпечення на всіх своїх пристроях.

Що потрібно

Нічого особливого не потрібно, щоб зробити RPi-проксі з Tor:

• Raspberry Pi 3
• Живлення через Micro USB 5 В
• Кабель Ethernet
• MicroSD карта не менше 8 Гб
• Доступ до вашого роутера
• Миша/клавіатура/настільний комп'ютер для початкового налаштування процесу

Ви хочете продовжити і налаштувати свою SD-карту з Raspbian та встановити також SSH? Ви можете використовувати або стандартну версію Raspbian або версію Lite, якщо будете використовувати тільки командний рядок для даного керівництва. Після того, як ви зібрали все разом, переконайтеся, що Raspberry Pi підключений безпосередньо до маршрутизатора за допомогою мережевого кабелю, а потім йдемо далі і підключимо його.

Крок 1. Встановіть необхідне програмне забезпечення

Перше, що нам потрібно зробити, це зробити Raspberry Pi з Wi-Fi точкою доступу. Так ви отримаєте можливість підключитися до нього з головного комп'ютера, так само, як і ло будь-якої бездротової мережі. Ми будемо робити все це з командного рядка Raspberry Pi:

1. Введіть `sudo apt-get update` та натисніть **Enter**.
2. Введіть `sudo apt-get install iptables-persistent git`
3. Виберіть **Yes** і натисніть **Enter** двічі, коли буде запропоновано.

Тепер, коли все завантажено і встановлено, прийшов час, щоб все встановити.

Крок 2. Перетворіть свій Raspberry Pi на точку доступу

Рис. 3.8. Процес установки точки доступу

Процес перетворення Raspberry Pi в точку доступу трохи складніший, але, на щастя, користувач harryallerston виклав на GitHub сценарій, який автоматизує весь процес.

1. Введіть `git clone https://github.com/unixabg/RPI-Wireless-Hotspot.git` і натисніть **Enter**.

[78] https://www.torproject.org/projects/torbrowser.html.en

2. Введіть `cd RPI-Wireless-Hotspot` і натисніть **Enter**.

3. Введіть `sudo ./install` і натисніть **Enter**. Запускається процес установки (рис. 3.8).

4. Натисніть кнопку **Y**, щоб погодитися з умовами, **Y**, щоб використовувати попередньо налаштований DNS-сервер, **N** для використання Unblock-Us серверів, **Y** для використання OpenDNS і N для значень за замовчуванням для Wi-Fi.

5. У відповідь на запит після питання за замовчуванням, введіть новий пароль. Це пароль для підключення мережі на RPi.

6. У відповідь на запит введіть новий SSID – це назва вашої мережі.

7. Введіть номер каналу. 6 буде добре, якщо не знаєте, що потрібно щось інше.

8. Введіть **N** для інших питань.

Після завершення, ваш Raspberry Pi буде перезавантажений і тепер повинен працювати як точка доступу. Ви можете перевірити це, перейшовши на інший комп'ютер або телефон, вибравши свій Raspberry Pi зі списку мережі Wi-Fi і переконатися, що Інтернет працює. Якщо з якоїсь причини це не так, Adafruit має керівництво[79], щоб зробити все це вручну. В іншому випадку, продовжіть і встановіть програмне забезпечення Tor-проксі (рис. 3.9).

Крок 3. Встановіть TOR

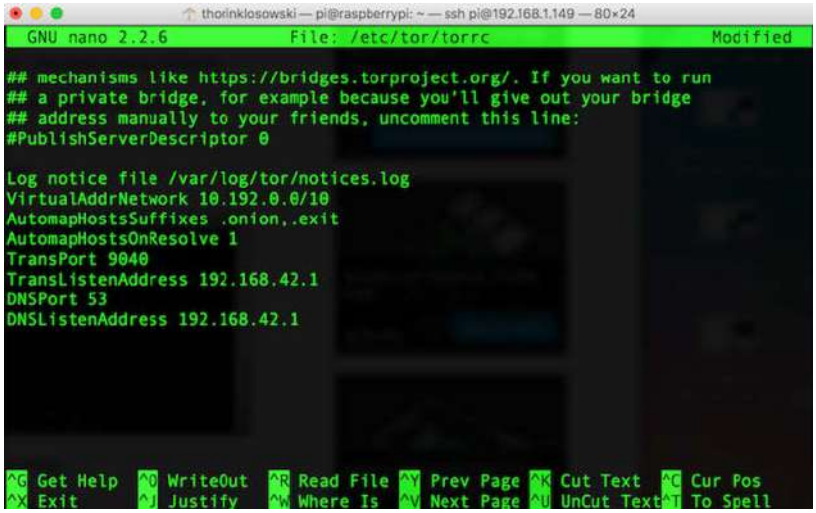


Рис. 3.9. Встановлення Tor

Tor має досить прямолінійний процес налаштування, але вам все одно доведеться налаштувати кілька речей, щоб змусити його працювати.

1. Введіть `sudo apt-get install tor` і натисніть **Enter**.

2. Введіть `sudo nano /etc/tor/torrc` і натисніть **Enter**.

Перегорніть весь шлях до нижньої частини документа і додайте текст, наведений нижче, в текстовий файл. Коли закінчите, натисніть **Ctrl+X**, щоб зберегти і продовжити:

```
Log notice file /var/log/tor/notices.log
VirtualAddrNetwork 10.192.0.0/10
AutomapHostsSuffixes .onion,.exit
AutomapHostsOnResolve 1
TransPort 9040
```

[79] https://learn.adafruit.com/setting-up-a-raspberry-pi-as-a-wifi-access-point/overview

```
TransListenAddress 192.168.42.1
DNSPort 53
DNSListenAddress 192.168.42.1
```

Далі, вам потрібно вказати інтерфейс Wi-Fi для відправки інтернет-трафіка через програмне забезпечення Tor. Це відбувається з декількома командами:

1. Введіть `sudo iptables -F` і натисніть **Enter**.
2. Введіть `sudo iptables -t nat -F` і натисніть **Enter**.
3. Введіть `sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 22 -j REDIRECT --to-ports 22` і натиснути кнопку **ENTER**.
4. Введіть `sudo iptables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to-ports 53` і натисніть клавішу **Enter**.
5. Введіть `sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --syn -j REDIRECT --to-ports 9040` і натисніть **Enter**.
6. Введіть `sudo sh -c “iptables-save > /etc/iptables.ipv4.nat”` і натисніть **Enter**.

Тепер прийшов час, щоб, нарешті, запустити Tor. Введіть `sudo service tor start` і натисніть **Enter**. Потім введіть `sudo service tor status`, щоб переконатися, що він працює правильно. Якщо не бачите ніяких кодів помилок, то він працює. Ви можете налаштувати його для автоматичного запуску при старті, набравши `sudo update-rc.d tor enable` і натиснути клавішу **Enter**.

Коли закінчиться, йдіть вперед і перезавантажитеся ще раз. Введіть `sudo reboot` і натисніть **Enter**. Ваш Raspberry Pi повинен тепер запустити все автоматично при запуску.

Крок 4. Підключіться та переглядайте з вашим новим TOR-Proxy

Рис. 3.10. Привітання зі встановленням Tor

Рис. 3.11. Перевірка роботи Tor

Щоб переконатися, що проксі-сервер працює, відвідайте сайт типу http://www.ipchicken.com, який показуватиме вашу IP-адресу, як він її бачить, а також відповідне доменне ім'я, якщо воно доступне (рис. 3.11). IP-адреса повинна бути не вашого інтернет-провайдера – насправді, якщо ви перезавантажите сторінку, то вона повинна змінитися!

Трафік Вашого веб-браузера тепер анонімний!

ПЕРЕД ПОЧАТКОМ ВИКОРИСТАННЯ ПРОКСІ – пам'ятаєте, що є багато способів ідентифікувати вас, навіть якщо ваші IP-адреси «рандомізовані». Видаляючи і блокуючи кеш браузера, історію і куки – деякі браузери дозволяють «анонімні сесії». Не заходьте на існуючі облікові записи з особистою інформацією (якщо не впевнені, що це те, що ви хочете зробити). Використовуйте SSL, при його наявності, кінець-в-кінців, шифруйте своє спілкування. І читайте https://www.torproject.org/, де набагато більше інформації про те, як використовувати Tor в розумний і безпечний спосіб.

Тепер все, що потрібно зробити, це підключити будь-який пристрій, з яким хочете мати анонімний серфінг, до нової мережі Wi-Fi на Raspberry Pi. І ваш звичайний Wi-Fi, і ця нова мережа будуть існувати разом, тому можна вибрати будь-яку мережу Wi-Fi. Насолоджуйтесь повільним, але анонімним доступом в Інтернет!

3.4. Як встановити VPN на Raspberry Pi

Віртуальна приватна мережа, або VPN (Virtual Private Network), є важливою частиною онлайн-безпеки та конфіденційності. Якщо коротко, то коли ви вже не працюєте поруч зі своїми звичайними засобами безпеки, то повинен бути VPN.

Віртуальні приватні мережі доступні для Windows, Linux і MacOS, а також Android і IOS. А якщо ви використовуєте Raspberry Pi (рис. 3.12)?

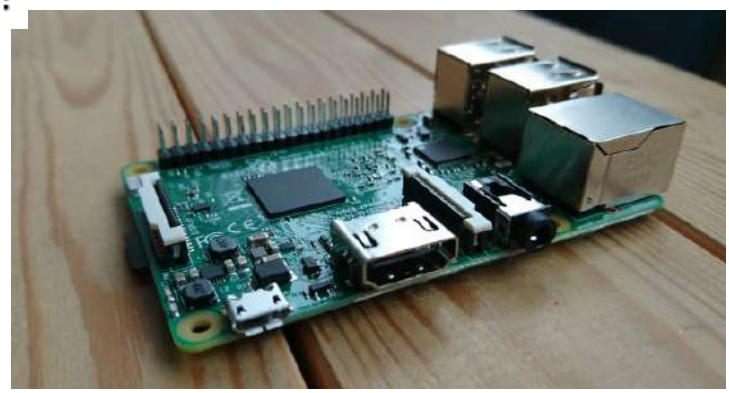


Рис. 3.12. Мікрокомп'ютер Raspberry Pi 3

Більшість операційних систем для RPi засновані на Linux; На жаль, провайдери VPN не пропонує спеціальне програмне забезпечення RPi. Якщо вам потрібно налаштувати VPN для Pi, то необхідно зробити деякі налаштування власноруч.

Подивитися, як встановити VPN[80]. Наступні кроки будуть працювати з усіма такими дистрибутивами на основі Debian, як Raspbian Jessie та Kodi (як OpenElec і OSMC).

[80] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1946-how-to-set-up-a-vpn-on-raspberry-pi

Навіщо використовувати VPN?

Є багато чудових причин для використання VPN, всі з яких в кінцевому підсумку опускаються до конфіденційності користувачів. Якщо коротко, то клієнт VPN шифрує дані з вашого комп'ютера або мобільного і відправляє його через VPN-сервер (рис. 3.13). З точки зору анонімності, онлайн активність прихована.

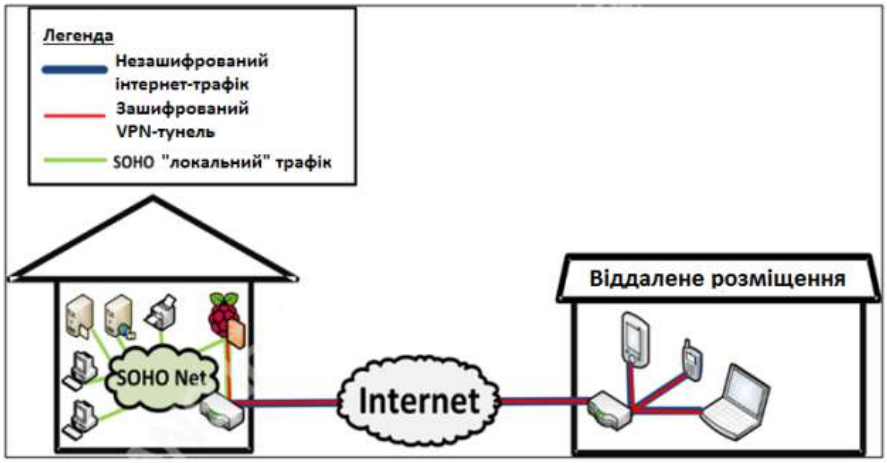


Рис. 3.13. Архітектура VPN на Raspberry Pi

Як це може бути корисно? Ну, якщо ви використовуєте свій Raspberry Pi як настільний комп'ютер і проживаєте в регіоні, де в Інтернеті рясніє цензура (рис. 3.14), то VPN зможе допомогти обійти такі обмеження. Ця ж технологія може допомогти, якщо ви просто хочете завантажити програмне забезпечення для RPi, але живете під репресивним режимом.

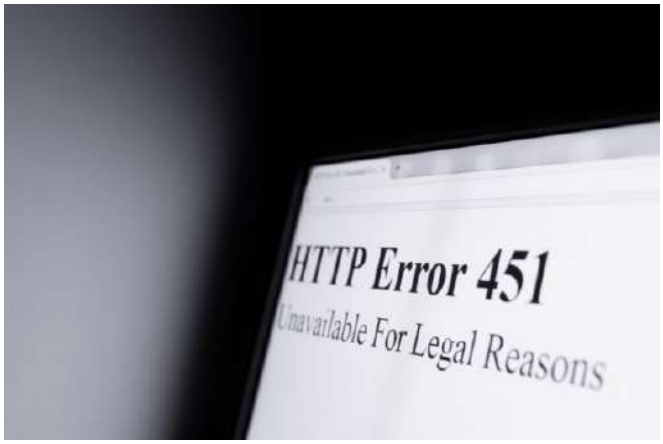


Рис. 3.14. Блокування доступу до сайту

Для медіа-центр Kodi VPN допоможе обійти регіональне блокування, цензуру, або інше, що ще блокує доступ до засобів масової інформації.

Наприклад, якщо ви хочете отримати доступ до BBC iPlayer із США, то VPN-може допомогти. При підключенні до VPN у Великобританії, наприклад, ви будете мати можливість транслювати своє улюблене ТВ-шоу. Однак, ви повинні бути впевнені, що законно користуєтеся медіа-центром, який вибрали.

Посібник 10 причин, чому ви повинні використовувати VPN[81], повинен пояснити більше. У той же час, якщо хочете більше зосередитися на шифруванні, безпеці і на тому, як працює VPN, перегляньте приклад VPN[82].

[81] https://www.makeuseof.com/tag/reasons-to-use-vpn/

Як вже зазначалося, існують й інші способи використання VPN. Наприклад, ви хотіли б запустити VPN на настільному комп'ютері або створити якусь універсальний захист шляхом створення облікового запису VPN на маршрутизаторі. У будь-якому випадку, ви повинні скористатися ним.

Як вибрати VPN

Якщо ви просто переглядаєте веб-сторінки і хочете робити це приватно, то повинен бути обраний стандартний VPN[83] (серед тих, які пропонують мінімальні логи).

Проте, якщо хочете обійти регіональне блокування або використовувати додаток потокового відео в Kodi, то вам треба знайти VPN, який пропонує необмежену пропускну здатність для передачі потокового відео. Він також повинен бути дружнім до P2P, так як багато доповнень використовують P2P-мережі для потокового контенту.

Також переконайтеся, що використовуєте сервіс VPN, який заслуговує на довіру.

Вимоги до VPN на Raspberry Pi

Щоб використовувати VPN на Raspberry Pi, знадобляться наступні речі:

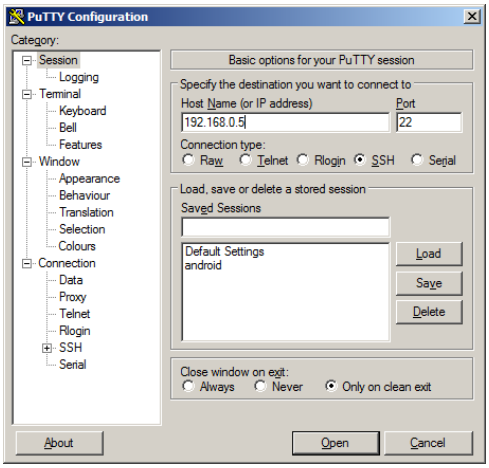


Рис. 3.15. Вікно запуску PuTTY

- Raspberry Pi 2 або пізніша версія. Більш ранні моделі будуть боротися з шифруванням.
- Обліковий запис VPN, який підтримує OpenVPN. Наш улюблений ExpressVPN, але є й інші:
  - обліковий запис проплачених VPN найбільш прийнятний, якщо бажаєте мати потокове відео;
  - доступні також безкоштовні VPN[84], але вони менше підходять для потокової передачі.
- Програмне забезпечення SSH на вашому комп'ютері.
  - користувачам Windows слід використовувати PuTTY (рис. 3.15);
  - Linux і Mac мають вже функціональність SSH через термінал.
- Потрібно включити SSH на RPi. Один із способів, це підключити його до монітора і змінити налаштування SSH за замовчуванням в raspi-config. Якщо ви не в змозі зробити це, вставте карту MicroSD RPi в свій комп'ютер, перейдіть в каталог

[82] https://www.makeuseof.com/tag/virtual-private-network-work-technology-explained/
[83] https://www.top10bestvpn.com/reviews
[84] https://www.makeuseof.com/tag/5-great-free-vpn-services-compared-which-is-fastest/

завантаження (в корінь) і створіть порожній текстовий файл з ім'ям SSH (без розширення файлу). Після того, як витягнете диск з ПК, вставите його в RPi і перезавантажитесь, SSH буде включений.

OpenVPN[85] є додатком з відкритим вихідним кодом VPN, що дозволяє використовувати конфігурації, які надаються сервісами VPN з використанням OpenSSL для шифрування. Якщо коротко, то можете налаштувати VPN на Raspberry Pi без виділеного додатка. Іншим варіантом безкоштовного VPN є використання LogMeIn Hatachi[86].

Є два варіанти для створення VPN. Перший – встановити OpenVPN в Raspbian (або обраної OS для Raspberry Pi). Крім того, можете налаштувати VPN в межах обраного образу Kodi.

Налаштування VPN на Raspberry Pi

З різними образами, доступними для RPi, це може бути трохи незручно.

На щастя, доти, поки використовуєте образ на основі Debian, це рішення буде працювати. Це простий спосіб для запуску VPN на вашому Raspberry Pi, незалежно від операційної системи або образу диска.

Спосіб встановлення перевірений з використанням OSMC на Kodi, який, як і Raspbian, заснований на Debian. Тим не менш, все також повинно працювати на OpenElec.

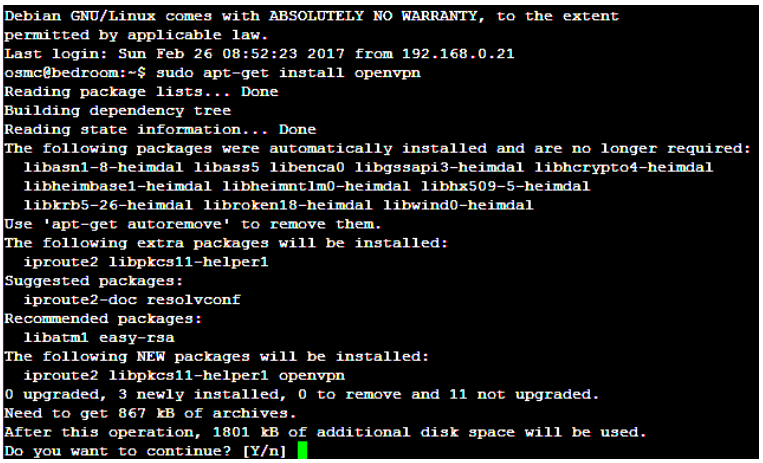


Рис. 3.16. Встановлення VPN

Почнемо з підключенням до Raspberry Pi через SSH, використовуючи правильні облікові дані для вашого образу, і установки OpenVPN (рис. 3.16):

```
sudo apt-get install openvpn
```

Після завершення виконайте команду перезавантаження:

```
sudo reboot
```

Коли RPi перезапуститься, вам необхідно завантажити файли OpenVPN від постачальника VPN. Переважна більшість сервісів пропонує підтримку OpenVPN.

Найбільш доцільний спосіб зробити це – завантажити файли на комп'ютер, розархівувати їх (це, як правило, ZIP-файли), а потім відправити їх на Raspberry Pi через SFTP або WinSCP[87] (рис. 3.17). Створіть нову папку для їх розміщення, назвавши її `openvpn-config`. Це повинно бути всередині `/home/`.

[85] https://openvpn.net/
[86] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1792-use-the-raspberry-pi-for-personal-vpn-to-securely-from-anywhere-on-the-internet
[87] http://mikrotik.kpi.ua/index.php/courses-list/category-raspberry/69-remote-work-with-files-on-raspberry-pi-session-4

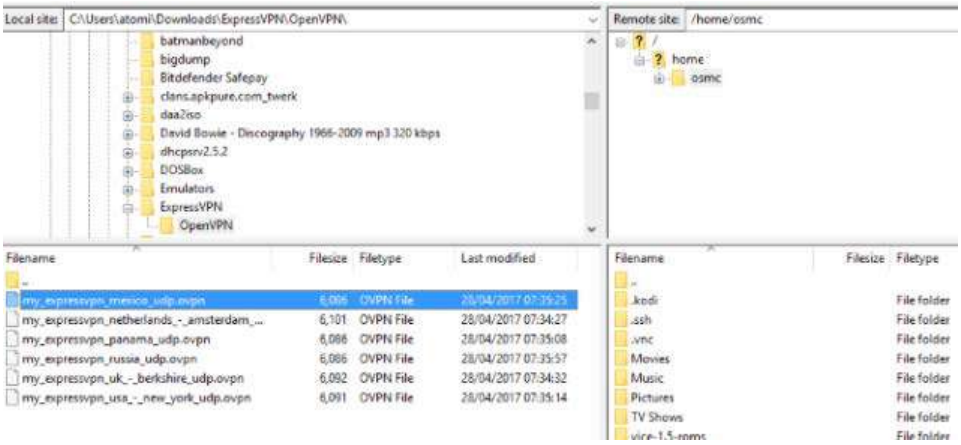


Рис. 3.17. Використання WinSCP

Після того, як файли будуть скопійовані, використайте SSH для видачі команди запуску:

```
sudo openvpn your_ovpn_configuration_file.ovpn
```

Вам буде запропоновано ввести ім’я користувача і пароль свого VPN (рис. 3.18), тому введіть їх.

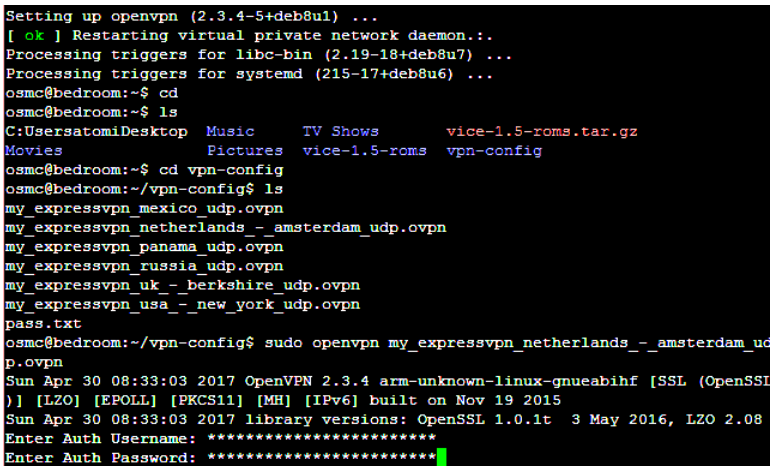


Рис. 3.18. Введення паролю

Через мить має бути встановлено з’єднання VPN і ви зможете насолоджуватися повністю приватним використанням Raspberry Pi.

Зверніть увагу, що якщо використовуєте Kodi на іншому пристрої або платформі, то вам треба буде встановити VPN через спеціальний додаток.

Відключення і зміна VPN

Якщо хочете відключити VPN, то треба натиснути **Ctrl+C**, щоб завершити сеанс. Для того, щоб підключитися до іншого сервера, просто повторіть попередню команду, але з іншим файлом конфігурації. Кожне з’єднання вимагає імені користувача та пароль.

3.5. Перші кроки в I2P – анонімному зашифрованому Інтернеті

Мережа I2P являє собою одну з реалізацій проекту невидимого інтернету (invisible internet project). Мережа забезпечує стійку анонімність, як клієнтам, так і серверам, що дозволяє приховувати не лише факт доступу до сайтів, але й самі сайти в цій мережі таким чином, що правоохоронні органи будуть не в змозі визначити точне місцезнаходження сервера.

Скандально-відомий сайт RusLeaks (російський аналог проекту WikiLeaks) був переміщений саме в мережу I2P[88], як тільки з'явився тиск з боку влади. Сама по собі мережа є розподіленою і зашифрованою, функціонує незалежно від Інтернету (можна «розвернути» дану мережу всередині локальної мережі без доступа в Інтернет, але крім академічного інтересу це не має ніякої практичної цінності). Мережа I2P працює поверх транспортного рівня моделі OSI, що трохи порушує ідеологію OSI, але задумка такою і є: з точки зору стороннього спостерігача видно лише зашифрований трафік (схожий на випадкове сміття і який має високий ступінь ентропії) з різними вузлами.

Поряд з ПЗ (програмним забезпеченням) Tor, для анонімізації використовується ланцюжок вузлів. Відмінність I2P від Tor полягає в тому, що в останньому використовується ланцюжок проксі серверів, які передають клієнтові свої публічні ключі для шифрування, а клієнт шифрує повідомлення таким чином, що перший проксі розшифрувавши це повідомлення знає про другий проксі, другий знає про наступний, а самий останній знає вихідне, незашифроване повідомлення, але не має інформації про те, хто відправив це повідомлення. Це називається цибульною (Onion) маршрутизацією.

У мережі I2P для кожного піра будується кілька так званих тунелів (аналогічно ланцюжку проксі в Tor), такі тунелі бувають двох типів: вхідні і вихідні. Для організації з'єднання між вузлами спочатку проходить пошук вхідного тунелю цільового вузла, а потім відбувається приєднання до нього свого вихідного тунелю. Причому тунелі в даній мережі недовговічні і існують не довше десятка хвилин. Безпосередньо один з одним піри не спілкуються за винятком побудови тих самих тунелів і опитування про вхідні тунелі цільового вузла у якихось посередників (рис. 3.19–3.21).

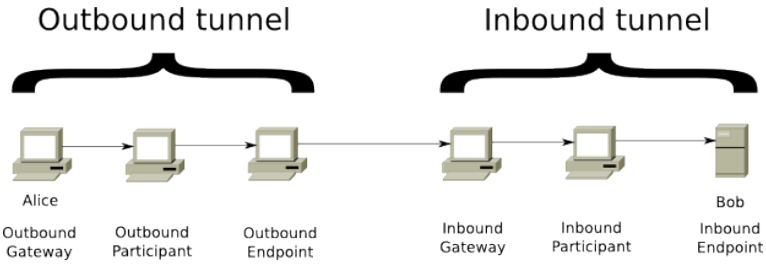


Рис. 3.19. Тунелі для зв'язку між двома вузлами

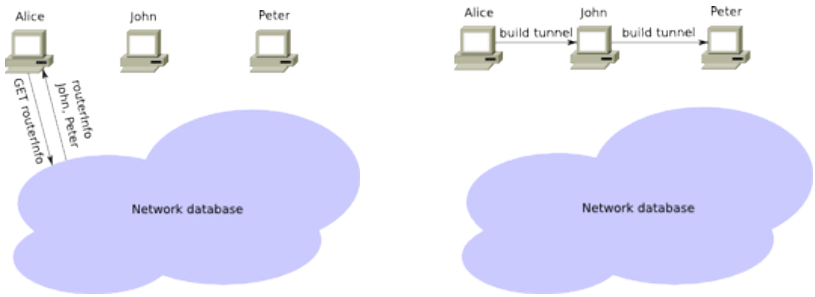


Рис. 3.20. Побудова тунелю (отримання інформації про маршрутизаторах з NetDB)

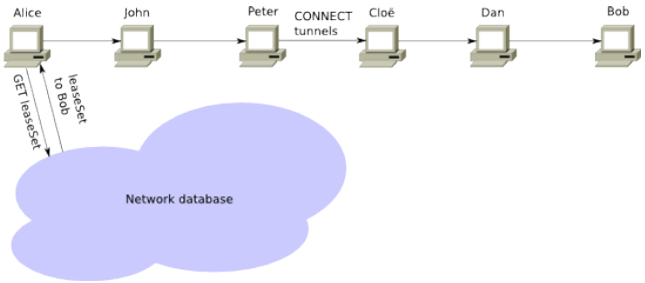


Рис. 3.21. Установка зв'язку з вузлом (одержання з NetDB інформації про вхідні тунелі) цільового вузла

[88] http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1291-the-first-steps-in-i2p-an-anonymous-encrypted-internet

Для входу в мережу I2P необхідно встановити ПЗ, яке є на офіціальному сайті проекта[89]. ПЗ поширюється вільно (у т.ч. і безкоштовно), а також з відкритим вихідним кодом. Останнє дуже корисно програмістам тому що дозволяє їм поліпшити ПЗ або використовувати його в своїх цілях, наприклад, існує модифікація клієнта eMule, так звана iMule, яка дозволяє отримати доступ до мереж eDonkey, використовуючи мережу I2P.

Встановлене ПЗ являє собою, так званий маршрутизатор, який при включенні починає інтеграцію в мережу I2P. Оскільки сама мережа I2P заснована на розподіленій хеш-таблиці (DHT) Kademila, у кожного піра (користувача) є власний унікальний ідентифікатор, який і використовується для пошуку цього піра в мережі. Поступова інтеграція в мережу нає на увазі накопичення бази даних існуючих пірів. Найбільш інтегровані в мережу піри, які мають широкий канал доступу, називаються високоємними і використовуються як мережеві бази даних NetDB (насправді в якості NetDB можна використовувати будь-який інший пір, можна не використовувати NetDB взагалі, але тоді робота в мережі стане настільки повільною, що користуватися мережею буде неможливо). Існує думка, що для повної інтеграції в мережу необхідна присутність в мережі не менше доби, але за великим рахунком це залежить від багатьох факторів і триває від декількох годин до декількох тижнів.

Щоб дозволити існуючим програмам використовувати мережу I2P без їх модифікації (аналогічно iMule) ПЗ маршрутизатора надає стандартний інтерфейс: відкривається локальний (на Вашому комп'ютері) проксі. Якщо вказати даний проксі в налаштуваннях веб-браузера, чат-клієнта або інших програм, вони почнуть працювати всередині мережі I2P. Сама по собі, I2P не є тим "зовнішнім" Інтернетом, який існує за її межами. Всередині цієї мережі всі сайти знаходяться в доменній зоні i2p., А для доступу до сайтів "зовнішнього" Інтернету (зон com., Org. тощо) використовуються вихідні точки. В налаштуваннях за замовчуванням вказана точка false.i2p, яка фізично знаходиться десь в Німеччині. У черговому порівнянні з Tor, I2P має розвинену інфраструктуру всередині самої мережі і часто вихід в зовнішній Інтернет не тільки є не потрібним, а й стає небезпечним через можливість випадкової деанонімізація.

I2P – відкрите програмне забезпечення, створене для організації анонімної, оверлейної, зашифрованої мережі і призначене для веб-серфінгу, анонімного хостингу, систем обміну миттєвими повідомленнями, ведення блогів, а також для файлообміну, електронної пошти, VoIP тощо.

Анонімна зашифрована мережа I2P була представлена в 2003 співтовариством розробників, які виступають за безпеку і анонімність в Мережі.

У мережі I2P всі пакети зашифровуються на стороні відправника і розшифровуються тільки на стороні одержувача.

Анонімність і захищеність забезпечується тим, що до загального Інтернету не йдуть незашифровані дані, а з того, що йде в мережу, дуже складно зрозуміти – чи ви ініціювали цей трафік, чи це просто через ваш комп'ютер проходить транзитний трафік інших клієнтів. Тобто довести будь-яку причетність конкретної особи до тієї чи іншої мережевої діяльності/активності дуже складно.

При цьому ніхто з проміжних учасників обміну не має можливості перехопити розшифровані дані.

Кожен клієнт мережі з'єднується з іншими клієнтами і утворює тунелі, через які ведеться транзит трафіку (не нагадує Skype?).

Підтримується 4 види шифрування: наскрізне шифрування, тунельне шифрування, транспортне шифрування, "часникове" шифрування, але більш докладно на сайті[90].

[89] https://geti2p.net/en/download
[90] https://geti2p.net/en/

Всередині мережі I2P працює власний каталог сайтів, електронні бібліотеки, а також торрент-трекери.

Щоб потрапити в мережу I2P, потрібно всього лише встановити на своєму комп'ютері програму-маршрутизатор – програму, що працює в режимі проксі-сервера, яка буде розшифровувати/зашифровувати весь трафік і перенаправляти його в мережу I2P.

Як це зробити?

Йдемо на сайт i2p2.de. У розділі "Установка з нуля" завантажуємо і встановлюємо I2P 0.9.32 – поточну версію I2P, запускаємо. Настроювати програму-маршрутизатор в більшості випадків не потрібно – вона вже за замовчуванням налаштована оптимальним чином. Інтерфейс повністю переведений російською мовою. У браузері треба поставити проксі на HTTP і HTTPS: IP: 127.0.0.1, Port: 4444. Ну, взагалі то, і все. Проксі встановлений і запущений. Тепер у вашому браузері відкривайте адресу http://127.0.0.1:7657/index.jsp або натискуєте відповідну піктограму в меню програм – і ви побачите консоль маршрутизатора (рис. 3.22):

Рис. 3.22. Консоль маршрутизатора

Тут відображається статус Вашої мережі, активність Вашого вузла, кількість активних тунелів та інше.

Оскільки в I2P немає звичних IP-адрес, то для збережень посилань на сайти рекомендується скористайтесь адресною книгою (рис.3.23):

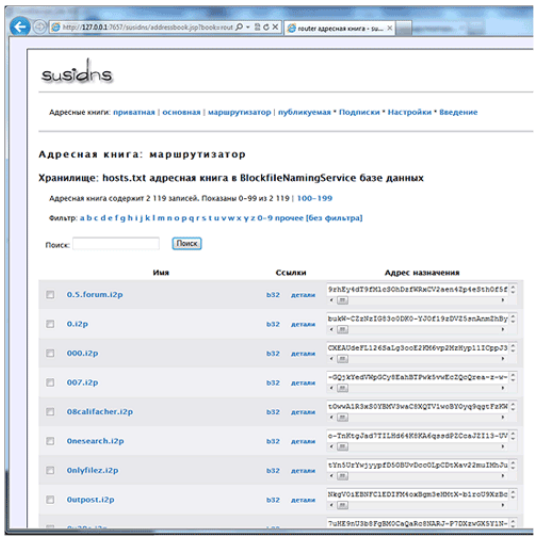


Рис. 3.23. Адресна книга

Для виходу в пірингову мережу є вбудований клієнт (рис.3.24), який дозволяє як завантажувати файли, так і розміщувати торенти на трекері:

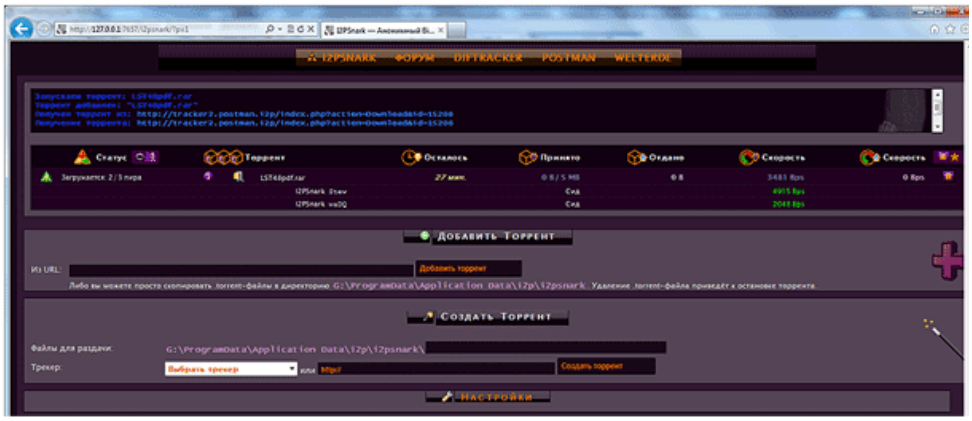


Рис. 3.24. Клієнт для торентів

До речі, головні трекери мережі I2P, підтримують RSS стрічки новин, що дозволяє відстежувати оновлення на трекері в реальному часі.

До послуг користувача також анонімна зашифрована пошта (рис. 3.25):

Рис. 3.25. Анонімна зашифрована пошта

Хоча є шлюз пересилання електронних листів у звичайний Інтернет і навпаки, але для більшої захищеності рекомендується налагодити листування лише всередині мережі I2P.

Які ж недоліки такої мережі?

У доступній для огляду області I2P мережі дуже мало кириличних сайтів. Також система не підходить людям, у яких платний трафік, тому що за ідеологією I2P потрібно ділитися своїм трафіком з іншими людьми.

3.6. Проксі-сервер на Raspberry Pi для доступу в I2P

I2P є тим програмним забезпеченням, яке краще залишити працюючим вічно. Raspberry Pi – одна з платформи, яка чудово підходить для такого завдання[91].

Думаю, що ви могли б залишити свій Raspberry Pi працюючим "за лінією фронту", і змогли б отримувати до нього доступ через даркнет I2P.

Підготовка

Перше, що ми зробимо, це оновимо операційну систему, так як в образі може бути далеко не остання версія різних пакетів та іншого:

[91] http://isearch.kiev.ua/uk/searchpractice/methodsinstruments/1841-proxy-server-on-raspberry-pi-to-access-i2p

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get dist-upgrade
sudo apt-get install default-jre-headless
```

Нам потрібно буде створити каталог для установки. Це можна зробити за допомогою декількох простих команд, і буде працювати під управлінням користувача pi. Якщо ви використовуєте інший обліковий запис, то відповідно змініть шлях. Нагадуємо, що ~ просто умовне позначенням поточного домашньому каталогу користувача.

```
cd ~
mkdir i2pbin
cd i2pbin
```

Знайдіть URL, щоб завантажити I2P, перейшовши в http://www.i2p2.de/download, але адреса з часом змінюється, бо з'являються нові версії. На момент написання цієї статті маємо працюючим наступне (рис. 3.26):

```
wget
https://download.i2p2.de/releases/0.9.32/i2pinstall_0.9.32.jar
```

або

```
wget
http://download.i2p2.no/releases/0.9.32/i2pinstall_0.9.32.jar
```

Рис. 3.26. Сторінку сайту для завантаження інсталятора i2p

Встановлюємо Java

Зверніть увагу: не треба ставити стандартну JRE з пакетів! Вона гальмує! Ми будемо ставити Java, спеціально скомпільовану для процесора ARM.

Тепер доступний Oracle JDK8 для ARM як видання Developer Preview! Розглянемо детально, як встановити Oracle Java SE 8 (з JavaFX) Developer Preview для ARM на Raspberry Pi.

Насамперед, завантажимо Java SE 8 for ARM[92] для Raspberry Pi.

Переносимо Oracle JDK на Raspberry Pi

Після завантаження Oracle JDK до настільного комп'ютера, ми повинні перенести його на на Raspberry Pi. Будемо використовувати SCP для передачі файлів мережею. Якщо ви працюєте на десктопному Windows, то завантажте і встановіть WinSCP[93].

Якщо використовуєте Mac OSX, то можете завантажити і встановити Cyberduck. Екрани будуть виглядати по-різному, але суть одна і та ж.

Створіть нову сесію в WinSCP за допомогою IP-адреси свого Raspberry Pi (рис. 3.27). Повноваження аутентифікації за замовчуванням для образу є ім'я користувача **pi** і пароль

[92] http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html
[93] https://winscp.net/download/WinSCP-5.11.3-Setup.exe

raspberry. Збережіть сесію, а потім увійдіть в систему. Вам може бути запропоновано прийняти відбиток SSH, виберіть "Yes", щоб прийняти і продовжити.

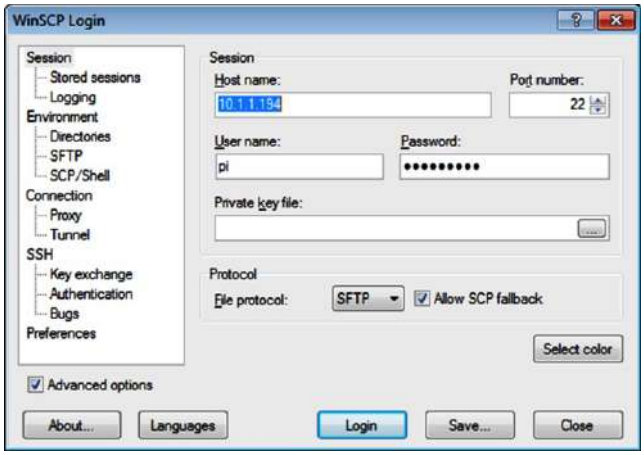


Рис. 3.27. Нова сесія в WinSCP

Після успішного встановлення з'єднання, виберіть диск і папку в лівій панелі, куди ви завантажити файл Oracle JDK на свою локальну машину. На правій панелі відображена файлова система на Raspberry Pi, ми залишимо її в положенні за замовчуванням в домашньому каталозі користувача "pi". Перетягніть файл Oracle JDK з лівої панелі на праву панель (рис. 3.28) і WinSCP почне процес передачі файлів. Вам буде запропонований діалог передачі – просто натисніть кнопку "Copy", щоб почати передачу.

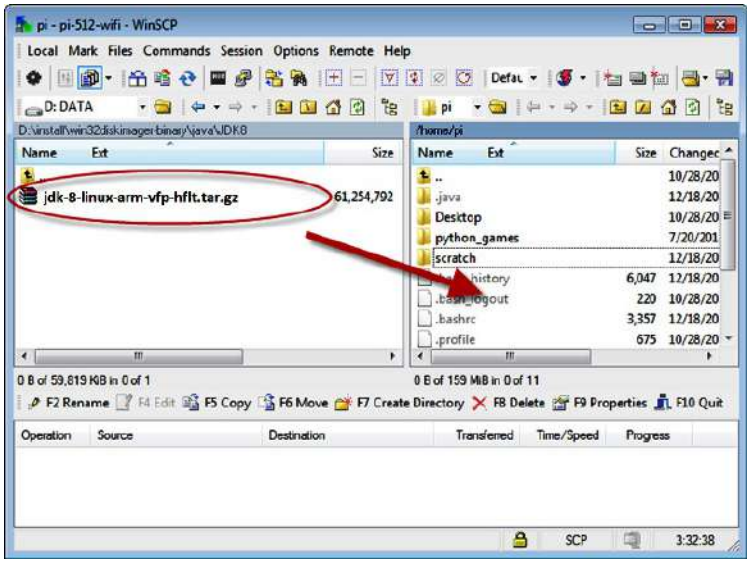


Рис. 3.28. Передача файлів в WinSCP

Коли завершення передачі файлу, можете закрити WinSCP (або Cyberduck).

Процедура встановлення на Raspberry Pi

Решта кроків мають бути виконані безпосередньо на консолі Raspberry Pi або з використанням з'єднання через термінал SSH з доступом до оболонки. На останньому етапі, ми передали файл Oracle JDK в домашній каталог користувача «pi». Ми повинні увійти в систему, як користувач «pi» і відразу будемо в домашньому каталозі користувача.

Давайте створимо новий каталог, до якого будуть встановлені файли JDK:

```
sudo mkdir -p -v /opt/java
```

Далі, розпакуємо файл .gz Oracle JDK за допомогою команди:

```
tar xvzf ~/ jdk-8-linux-arm-vfp-hflt.tar.gz
```

Процес розпакування займе кілька секунд. Буде розпакований весь вміст файлу .gz Oracle JDK в новий каталог з ім'ям `jdk1.8.0`, розташований в домашньому каталозі користувача.

Після завершення розпакування настав час перенести новий розпакований каталог в місце розташування встановленої Java, створене нами раніше як `opt/java`.

```
sudo mv -v ~/jdk1.8.0 /opt/java
```

Ми можемо також видалити оригінал файлу .gz, який нам більше не потрібний:

```
rm ~/jdk-8-linux-arm-vfp-hflt.tar.gz
```

Для завершення установки JDK нам потрібно, щоб система знала, що є нова JVM встановлена і де вона знаходиться. Використайте наступну команду, щоб виконати це завдання (рис. 3.29):

```
sudo update-alternatives --install "/usr/bin/java" "java"
"/opt/java/jdk1.8.0/bin/java" 1
```

І, нарешті , ми також повинні повідомити системі, що хочемо, щоб цей JDK бути для системи Java Runtime за замовчуванням. Наступна команда виконає цю дію:

```
sudo update-alternatives --set java /opt/java/jdk1.8.0/bin/java
```

Рис. 3.29. Інформація про місцезнаходження JVM

Тепер встановлений Java. Для перевірки і підтвердження ми можемо виконати команду перевірки версії Java за допомогою:

```
java -version
```

Ви повинні отримати таку відповідь (рис. 3.30):

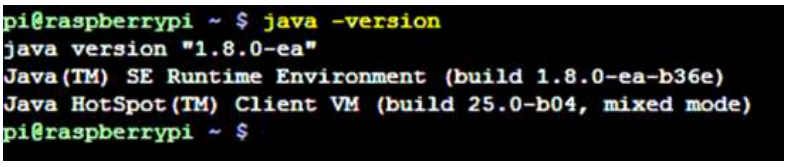


Рис. 3.30. Підтвердження встановлення Oracle JDK

Це підтверджує, що Oracle JDK встановлений і готовий до використання.

Додавання змінної середовища JAVA_HOME

Деякі програми Java вимагають наявність налаштованої в системі змінної JAVA_HOME. Додайте наступний рядок до вашого "/etc/environment", використовуючи улюблений текстовий редактор:

```
JAVA_HOME="/opt/java/jdk1.8.0"
```

Крім того, відредагуйте файл "~/.bashrc" за допомогою цієї команди:

```
sudo nano ~/.bashrc
```

додавши наступні два рядки в кінець файлу, та збережіть його:

```
export JAVA_HOME="/opt/java/jdk1.8.0"
export PATH=$PATH:$JAVA_HOME/bin
```

Перезавантажтеся або повторно увійдіть в систему, щоб застосувати експорт у своє середовище.

Встановлення I2P-маршрутизатора

Вводимо:

```
java -jar i2pinstall_0.9.32.jar -console
```

Замість `i2pinstall_0.9.32.jar` підставляєте назву свого файлу установника маршрутизатора, бо версія може змінитися. Шлях для встановлення: `/home/pi/i2p/`

Ось і все! I2P-маршрутизатор встановлений!

Налаштування маршрутизатора

Хоча маршрутизатор встановлений, але працювати з ним ще рано. Він вас просто не "почує", тому що чекає команд з 127.0.0.1, а зовсім не з вашого комп'ютера. Виправимо:

```
cd ~/i2pbin
sudo ./runplain.sh
kill -9 `cat /tmp/router.pid
cd..
cd ~/i2pbin
sudo nano ~/.i2p/clients.config
```

Ми дозволяємо вперше запуск `runplain.sh`, а потім вбиваємо його для того, щоб створити профіль I2P для наступного редагуванняю.

Якщо хочете, то можете скористатися RDP для підключення до Raspberry Pi і просто використовувати I2P звідти. Автор хоче зробити Pi воротами в I2P для всієї своєї локальної мережі, тому давайте зробимо це так, щоб ми могли потрапити в веб-консоль з будь ПК, а не тільки з локальний хоста. Відкриваємо в редакторі `~/.i2p/clients.config` і знаходимо рядок, який виглядає як:

```
clientApp.0.args=7657 ::1,127.0.0.1 ./webapps/
```

Коментуємо його з # і розкоментуємо рядок, який виглядає як:

```
#clientApp.0.args=7657 0.0.0.0 ./webapps/
```

в:

```
clientApp.0.args=7657 0.0.0.0 ./webapps/
```

Якщо ми зробимо цей крок, але не довіряємо всім хостам в нашій локальній мережі, це, ймовірно, хороша ідея, зробити пароль для маршрутизатора. Просто редагуємо `clients.config` далі, додавши рядок:

```
consolePassword=SomePassword
```

Очевидно замінивши "`SomePassword`" паролем, який хочете використовувати. Ім'я для входу – `admin`. Переконайтеся, що маєте тепер доступ до консолі I2P, щоб мати можливість дістатися до проксі. Для цього ми повинні встановити проксі на портах 4444 і 4445 для прослуховування 0.0.0.0.

Тепер продовжимо з редагування файлу `i2ptunnel.config`:

```
sudo nano ~/.i2p/i2ptunnel.config
```

Знайдіть рядки, які виглядають як :

```
tunnel.0.interface=127.0.0.1
tunnel.6.interface=127.0.0.1
```

і змініть їх на:

```
tunnel.0.interface=0.0.0.0
```

```
tunnel.6.interface=0.0.0.0
```

Тепер можемо запустити I2P:

```
cd /home/pi/i2p
./runplain.sh
```

але, якщо хочете запускати при завантаженні і бути впевненим, що все працює будь-коли, навіть після аварії, скористайтесь наведеним нижче рішенням. Вводимо:

```
crontab –e
```

Цим ми запускаємо редактор, щоб додати заплановані завдання. Додайте наступні рядки:

```
0 * * * * /home/pi/i2pbin/runplain.sh
reboot /home/pi/i2pbin/runplain.sh
```

Потім `exit` для завершення роботи.

Дані рядки повинні запускати I2P при завантаженні і робити спроби завантажити його щогодини. Приводом для кожного щогодинного рядка для перезапуску I2P є випадок, що він зламався. Якщо I2P вважає, що він вже запущений, то це повинно витончено закритись.

Ми тепер повинні мати піднятий і працюючий I2P, залишилось конфігурувати свій браузер для вказівки на порти 4444 і 4445 для HTTP і HTTPS проксі, відповідно.

Базові налаштування i2p

Багато користувачів віддають перевагу веб-інтерфейсу, а не файлам конфігурації.

Спочатку доступ до вебінтерфейсу дозволений тільки з локального комп'ютера. Так що будемо робити першу «дірку в безпеці» – відкривати доступ до адмінки з будь-якої адреси . Але для початку треба хоч якось до неї достукатися . Беремо ssh і робимо тунель з порту 7657 хостингу на порт 7657 нашого комп'ютера.

```
C:\>ssh user@ваш_сервер-L7657:127.0.0.1:7657
user@ваш_сервер's password:
Linux ваш_сервер3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64
You have mail.
Last login: Tue Dec 24 06:18:58 2013
ваш_сервер:~>
```

Якщо бачимо запрошення шелла, то за посиланням `http://127.0.0.1:7657/` стає доступна сторінка адміністрування i2p-маршрутизатора.

Рис. 3.31. Закладка вибору мови

По-перше, на закладці UI ставимо англійську мову (рис. 3.31). Тому що, якщо щось знадобиться знайти, то простіше шукати за англійськими назвами термінів. Наприклад, так відразу не здогадаєшся, що «транзитний трафік» – це «share bandwidth».

Закладка Bandwidth (рис. 3.32) – виставлено IN - 512 , OUT - 256 і 50% Share (той самий транзитний трафік через ваш сервер).

Звичайно, при 50% страждає анонімність і, потенційно, швидкість. Хочеться анонімності – приближайтесь до 100%. А швидкість треба налаштовувати залежно від каналу вашого сервера і ваших потреб.

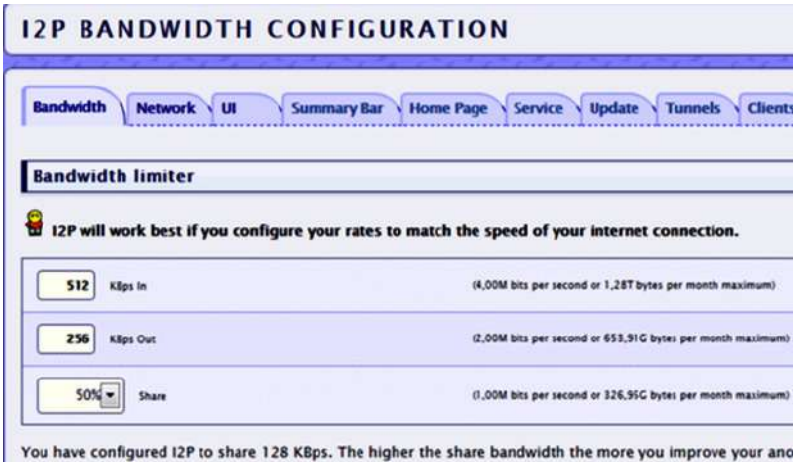


Рис. 3.32. Закладка Bandwidth

Далі налаштовуємо адресну книгу. Справа в тому, що мережа I2P не має звичних нам DNS-серверів. Тому SusiDNS звертається до вже відомих ресурсів для поповнення так званої «Адресної книги».

Заходимо в браузері на `http://<IP Raspberry Pi>:7657/susidns/subscriptions` і додаємо:

```
http://www.i2p2.i2p/hosts.txt
http://i2host.i2p/cgi-bin/i2hostetag
http://stats.i2p/cgi-bin/newhosts.txt
http://tino.i2p/hosts.txt
http://inr.i2p/export/alive-hosts.txt
```

Основні налаштування зроблені, тому можна почати освоєння «невидимого» Інтернету.

Висновки

Незважаючи на те, що в 2017 році кількість користувачів Інтернету в Україні дещо зменшилась, він залишається сьогодні основним інформаційним джерелом для соціальних медіа, навчальних і наукових ресурсів. Тому залишається актуальним питання доступу до наданих ресурсів при збереженні приватності, захисту від шкідливих програм та шахраїв.

Використані джерела

Матеріали сайтів isearch.kiev.ua та mikrotik.kpi.ua.