МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

(назва факультету, інституту)

Систем інформаційного та кібернетичного захисту

(назва кафедри)

"На правах рукопису"

«До захисту допущено»

Завідувач кафедри

Шуклін Г. В.

(підпис) (ініціали, прізвище)

“____” _____ 2021р.

# МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 Кібербезпека

(код та назва спеціальності)

на тему: Дослідження шляхів та вироблення рекомендацій щодо побудови та оптимізації комплексу засобів захисту домашніх Wi-Fi інформаційно-комунікаційних радіомереж

Студент групи СЗДМ – 61 Гуренко Микола Вікторович _____

(шифр групи) (прізвище, ім’я, по батькові) (підпис)

**Керівник** к.т.н., Пепа Юрій Володимирович _____

(вчені ступінь та звання, прізвище, ініціали) (підпис)

**Нормоконтроль**: Гребенніков А.Б. _____

(вчені ступінь та звання, прізвище, ініціали) (підпис)

Київ – 2021

ЗАТВЕРДЖУЮ»

Завідувач кафедри

Шуклін Г. В.

(підпис) (ініціали, прізвище)

“__” _____ 2021р.

# ЗАВДАННЯ

**на атестаційну роботу магістра**

студенту Гуренко Миколі Вікторовичу

(прізвище, ім’я, по батькові)

**1. Тема роботи:** Дослідження шляхів та вироблення рекомендацій щодо побудови та оптимізації комплексу засобів захисту домашніх Wi-Fi інформаційно-комунікаційних радіомереж

Затверджена наказом по університету від “__” _ 2021_р. №_____

**2. Термін здачі** студентом оформленої роботи “____” Січень 2021_р.

**3. Об’єкт дослідження:** бездротові технології стандарту IEEE 802.11.

**4. Предмет дослідження:** алгоритми та протоколи забезпечення безпеки бездротових мереж.

**5. Мета роботи:** Аналіз уразливостей бездротових комп'ютерних мереж, а також шляхи та методи їх усунення.

**6. Перелік питань, які мають бути розроблені:**

**7. Перелік публікацій:** Ахрамович В.М., Гуренко М. В.- Оцінка показника захисту інформації в засобах персонального використання та локальній мережі

**8. Перелік ілюстративного матеріалу:**

**9. Дата видачі завдання** “__” _____ 2021 р.

**Керівник** _____ Пепа Ю. В.

(підпис) (ініціали, прізвище)

**Завдання прийняв до виконання** _____ Гуренко М.В.

(підпис) (ініціали, прізвище)

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів дипломної роботи | Строк виконання етапів роботи | **Примітка** |
|---|---|---|---|
| 1 | Підбір науково-технічної літератури | 05.10.2021 | Вик. |
| 2 | Обґрунтування актуальності теми роботи | 17.10.2021 | Вик. |
| 3 | Написання першого розділу роботи | 22.10.2021 | Вик. |
| 4 | Написання другого розділу роботи | 28.10.2021 | Вик. |
| 5 | Написання третього розділу роботи | 03.11.2021 | Вик. |
| 6 | Написання висновків по роботі | 18.11.2021 | Вик. |
| 8 | Підготовка демонстраційних матеріалів | 25.11.2021 | Вик. |
| 9 | Підготовка доповіді | 05.12.2021 | Вик. |
| 10 | Захист в ДЕК | 18.01.2022 | |

Студент _____ Гуренко М.В.

( підпис ) ( ініціали, прізвище)

Керівник роботи _____ Пепа Ю. В.

( підпис ) (ініціали, прізвище)

# РЕФЕРАТ

**Мета випускної кваліфікаційної роботи:**

Аналіз уразливостей бездротових комп'ютерних мереж, а також шляхи та методи їх усунення.

**Завдання випускної кваліфікаційної роботи:**

1. Виявлення уразливостей бездротових комп'ютерних мереж;
2. Вироблення засобів захисту уразливих місць мережі;
3. Розроблення практичних рекомендацій щодо забезпечення безпеки бездротової мережі;
4. Розробка автоматизованої системи для аналізу уразливостей та впливу на них.

**Об'єктом дослідження випускної кваліфікаційної роботи** є бездротові технології стандарту IEEE 802.11.

**Предметом дослідження випускної кваліфікаційної роботи** є алгоритми та протоколи забезпечення безпеки бездротових мереж.

**Гіпотеза випускної кваліфікаційної роботи:**

Розвиток інформаційних технологій та стандартів забезпечення інформаційної безпеки дозволяє захистити мережі на належному рівні, але найчастіше людський фактор, в особі адміністратора мережі, упускає низку особливостей, які дозволяють злодіям проникати в дані мережі. Розроблені рекомендації після проведення аналізу зможуть дозволити закрити доступ до уразливостей, які найчастіше використовують зловмисники і цим забезпечити надійне підключення до бездротової мережі, без побоювання за крадіжку або зміна інформації, що передається.

**Методи дослідження:** Методологічною основною при написанні роботи є наукові методи, що ґрунтуються на вимогах об'єктивного та всебічного аналізу бездротових технологій. Дослідження проведені із застосуванням сукупності методів та способів наукового пізнання. Абстрактно-логічний метод дозволив розкрити теоретичні аспекти протоколів забезпечення безпеки підключення, визначити основні алгоритми, що використовуються. Метод класифікації дозволив розділити протоколи та способи на них. Порівняльний метод дозволив знайти найоптимальніший спосіб проведення тестування на проникнення.

Практична значимість методів злому та захисту бездротових мереж полягає у застосуванні розроблених рекомендацій для забезпечення безпеки бездротової мережі та використання алгоритму тестування на проникнення для перевірки бездротових мереж, що експлуатуються в даний момент.

**Короткий опис структури:**

Структура випускної кваліфікаційної роботи обумовлена предметом, метою та завданнями дослідження. Робота складається з вступу, чотирьох розділів та висновків.

Введення розкриває актуальність, визначає об'єкт, предмет, мету, завдання та методи дослідження. Розкриває теоретичну та практичну значущість роботи.

У першому розділі розглядаються бездротові технології, проводиться аналіз вибору об'єкта дослідження. Вивчаються стандарти функціонування.

В іншому розділі розглядається тестування проникнення бездротових точок доступу з налаштованими різними протоколами забезпечення безпеки.

Третій розділ присвячений розробці автоматизованої системи тестування на проникнення, порядок її використання, спосіб управління та рознесення виконання розрахунків.

У висновку підбиваються підсумки роботи, формуються залишкові висновки.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

WLAN (Wireless Local Area Network) – бездротова локальна мережа

SSID (Service Set Identifier) – ідентифікатор бездротової мережі

WEP – Wired Equivalent Privacy

WPA – Wi-Fi Protected Access

WPAN - WirelessPersonalAreaNetworks

WLAN – WirelessLocalAreaNetworks

WWAN - WirelessWideAreaNetwork

MIMO – Multiple Input Multiple Output

ОС – операційна система

Ki – Key Identification

ІС – інформаційна система

# ЗМІСТ

# ВСТУП

Актуальність теми випускної кваліфікаційної роботи

Бездротові мережі стають все більш важливим ресурсом в умовах розвитку корпоративних та домашніх технологій. Однією з основних потреб їх використання є розширення існуючих провідних мереж з мінімальними витратами у найкоротші терміни.

З збільшенням числа мобільних користувачів виникає потреба у найкоротші терміни створення комунікаційних мереж між ними: для обміну даними, отримання інформації у максимально низькі терміни. Тому природно відбувається швидке розвиток бездротових технологій. Звідси виникла гостра необхідність захисту таких мереж, забезпечення їх інформаційної цілісності та безпеки.

Незважаючи на те, що тема безпеки бездротових мереж піднімається рік у рік, адміністратори цих мереж дуже часто забувають або нехтують найпростішими заходами безпеки, і більшість пристроїв досі надають великі можливості для зловмисників.

Зі зростанням обчислювальної потужності обладнання протоколи безпеки, розроблені кілька років тому, втрачають свою актуальність досить швидко.

Крім того, питання фізичної безпеки у бездротових технологіях виходити на новий рівень. Через відсутність кабелів неможливо чітко описати периметр мережі, яку потрібно захистити. Отже, складніше організувати розмежування доступу авторизованих та несанкціонованих користувачів.

Зі збільшенням популярності бездротових мереж та ідей розумного будинку для підвищення ступеня комфортності та об'єднання всіх систем в єдину мережу з

єдиним центром управління часто використовуються бездротові технології, і одним з перших постає питання забезпечення безпеки таких мереж, адже від цього починає залежати життя та здоров'я людини. а не лише безпека даних.

Таким чином, аспекти безпеки є актуальними навіть для бездротових мереж, що не мають виходу в Інтернет, але передають особисті дані або інформацію, що становить комерційну таємницю.

# РОЗДІЛ 1. БЕЗДРОТОВІ МЕРЕЖІ

## 1.1. Бездротові мережі

Бездротові технології - це підклас інформаційних технологій, які служать для передачі інформації на відстані між двома точками або декількома, не вимагаючи зв'язку за допомогою проводів. Для передачі інформації можуть використовуватися різні середовища та типи випромінювань, найчастіше використовуються радіохвилі, а також інфрачервоне, оптичне або лазерне випромінювання.

Існує багато бездротових технологій, найчастіше відомих за назвами компаній, які просували цей тип технологій, таких як Wi-Fi, WiMAX, Bluetooth. Кожна технологія має певні характеристики, що впливають на сферу застосування. І тому класифікуємо їх.

Існують різні підходи до класифікації бездротових технологій.

За дальністю дії:

Бездротові персональні мережі (WPAN - WirelessPersonalAreaNetworks). Приклади технологій – Bluetooth.

Бездротові локальні мережі (WLAN – WirelessLocalAreaNetworks).

Приклади технологій – Wi-Fi.

Бездротові мережі масштабу міста (WMAN - WirelessMetropolitanAreaNetworks). Приклади технологій – WiMAX.

Бездротові глобальні мережі (WWAN - WirelessWideAreaNetwork).

Приклад технології – CSD, GPRS, EDGE, EV-DO, HSPA. За топологією:

"Точка-точка".

«Точка-багатоточка». По області застосування:

Корпоративні (відомчі) бездротові мережі — створені компаніями для потреб.

Операторські бездротові мережі — створювані операторами зв'язку для надання послуг.»[1]

На даний момент існує два найбільш застосовувані напрямки бездротових комп'ютерних мереж:

1. Робота у замкнутому обсязі (офіс, виставковий зал тощо);

2. З'єднання віддалених один від одного локальних мереж (або віддалених на відстані сегментів локальної мережі).

Таблиця 1 – порівняння стандартів бездротового зв'язку

| Технологія | Стандарт | Використання | Пропускна здатність | Радіус дії | Частоти |
|---|---|---|---|---|---|
| Wi-Fi | 802.11a | WLAN | до 54 Мбіт/с | до 300 метрів | 5,0 ГГц |
| Wi-Fi | 802.11b | WLAN | до 11 Мбіт/с | до 300 метрів | 2,4 ГГц |
| Wi-Fi | 802.11g | WLAN | до 54 Мбіт/с | до 300 метрів | 2,4 ГГц |
| Wi-Fi | 802.11n | WLAN | до 300 Мбит/с (в перспективі до 600 Мбит/с) | до 300 метрів | 2,4 — 2,5 або 5,0 ГГц |
| WiMax | 802.16d | WMAN | до 75 Мбіт/с | 25-80 км | 1,5-11 ГГц |

| | | | | | |
|---|---|---|---|---|---|
| WiMax | 802.16e | Mobile WMAN | до 40 Мбіт/с | 1-5 км | 2,3-13,6 ГГц |
| WiMax 2 | 802.16m | WMAN, Mobile WMAN | до 1 Гбіт/с Мбіт/с | 120-150 км (стандарт в розробці) | До 11 ГГц |
| Bluetooth v. 1.1 | 802.15.1 | WPAN | до 1 Мбіт/с | до 10 метрів | 2,4 ГГц |
| Bluetooth v. 2.0 | 802.15.3 | WPAN | до 2,1 Мбіт/с | до 100 метрів | 2,4 ГГц |
| Bluetooth v. 3.0 | 802.11 | WPAN | Від 3 Мбіт/с до 24 Мбіт/с | до 100 метрів | 2,4 ГГц |
| ZigBee | 802.15.4 | WPAN | Від 20 до 250кбіт/с | 1-100 м | 2,4 ГГц (16 каналів), 915 МГц (10 каналів), 868МГц (один канал) |
| Інфрачервона лінія зв’язку | IrDa | WPAN | Від 15 Мбіт/с | від 5 до 50 сантиметрів, односторонній зв'язок - до 10 метрів | Інфрачервоне випромінювання |

## 1.2. Група протоколів ieee 802.11

Зробимо акцент на корпоративних бездротових мережах для роботи в замкнутому обсязі, які в наш час дуже активно використовуються для швидкого доступу до локальних та глобальних ресурсів. Найчастіше вони будуються з використанням бездротової технології, більш відомої під назвою: Wi-Fi. Для організації бездротових мереж у замкнутому просторі використовуються всеспрямовані антени передавача. Використовуються розроблені стандарти зв'язку для комунікації в бездротовій локальній мережі частотних діапазонів, що не ліцензуються, 0,9, 2,4, 3,6 та 5 ГГц – IEEE

802.11. Спочатку стандарт IEEE 802.11 передбачав передачу даних по радіоканалу на швидкості близько 1 Мбіт/с і як опцію на швидкості порядку 2 Мбіт/с. Один із перших високошвидкісних стандартів бездротових мереж – IEEE 802.11a – визначає швидкість передачі на швидкості до 54 Мбіт/с. Як робочий діапазон, використовується 5 ГГц.

В ідеальних умовах стандарт IEEE 802.11a регламентує швидкість передачі до 54 Мб/с. У менш ідеальних умовах (або при чистому сигналі) пристрої можуть вести зв'язок зі швидкістю<54 Мбіт/с і кратно 6, зазвичай це: 48 Мбіт/с, 36 Мбіт/с, 24 Мбіт/с, 18 Мбіт/с, 12 Мбіт/с та 6 Мбіт/с.

Сумісність стандарту IEEE 802.11a із 802.11b або 802.11g відсутня.

Незважаючи на свою назва, стандарт IEEE 802.11b, прийнятий у 1999 році, не є продовженням стандарту 802.11a, оскільки використовуються різні технології: метод прямої послідовності для розширення спектру (DSSS), а якщо бути точніше, то його покращена версія високошвидкісний метод прямої послідовності для розширення спектру (HR-DSSS) 802.11b проти мультиплексування з ортогональним частотним поділом каналів (OFDM)

802.11a. Стандарт 802.11b передбачає використання діапазону частот, що не ліцензується, 2,4 ГГц. Швидкість передачі – до 11 Мбіт/с.

У жовтні 2002 року було затверджено проект стандарту IEEE 802.11g, який передбачає використання діапазону частот 2,4 ГГЦ, тим самим забезпечуючи швидкість з'єднання близько 54 Мбіт/с в ідеальних умовах, ніж перевершивши стандарт IEEE 802.11b, який дозволяв працювати на швидкостях до 11 Мбіт/с. Крім того, стандарт 802.11g забезпечує сумісність з 802.11b. Сумісність може бути реалізована в режимі модуляції прямої послідовності для розширення спектра, і тоді швидкість з'єднання обмежується в 11 Мбіт/с, а якщо в режимі модуляції мультиплексування з ортогональним частотним поділом каналів, то 54 Мбіт/с. Тому цей стандарт рекомендується і є прийнятним при побудові бездротових комп'ютерних Wi-Fi мереж.

«Стандарт 802.11n підвищує швидкість передачі даних практично вче -тверо порівняно з пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мбіт/с) за умови використання в режимі 802.11n з іншими пристроями 802.11n. Теоретично 802.11n здатний забезпечити швидкість передачі даних до 600 Мбіт/с брутто, застосовуючи передачу даних відразу за чотирма антенами. За однією антеною – до 150 Мбіт/с. Пристрої 802.11n працюють у діапазонах 2,4-2,5 або 5,0 ГГц. Крім того, пристрої 802.11n можуть працювати у трьох режимах:

1. спадкованому (Legacy), у якому забезпечується підтримка пристроїв 802.11b/g та 802.11a;

2. змішаному (Mixed), у якому підтримуються пристрої 802.11b/g, 802.11a та 802.11n;

3. "чистому" режимі - 802.11n (саме в цьому режимі можна скористатися перевагами підвищеної швидкості та збільшеною дальністю передачі даних, що забезпечуються стандартом 802.11n).

Чорну версію стандарту 802.11n (DRAFT 2.0) підтримують багато сучасних мережевих пристроїв. Підсумкова версія стандарту (DRAFT 11.0), прийнята 11 вересня 2009 року, забезпечує швидкість до 300

Мб/с, Багатоканальний вхід/вихід, відомий як MIMO, та більше покриття.»[3]

Стандарт 802.11n вводити важливе нововведення - MIMO (MultipleInput, MultipleOutput - «багато входів, багато виходів»), за допомогою якого здійснюється просторове мультиплексування: одночасна передача декількох інформаційних потоків по одному каналу, а також використання для доставки сигналу багатопроменевого поширення, яке мінімізує вплив перешкод та втрат даних, але потребує наявності кількох антен. Саме можливість одночасної передачі та прийому даних робить пропускну здатність пристроїв 802.11n більш високою.

На початок 2016 року більшість точок доступу, що пропонуються виробниками, підтримує MIMO 2×2 або 1×1, тобто SISO (одне потокове передавання). Вбудовані в мобільні пристрої Wi-Fi-адаптери зазвичай підтримують режим SISO.»[4]

1. Ad-hoc, тобто точка-точка – це найпростіша бездротова мережа, де зв'язок між клієнтами (станціями) встановлюється безпосередньо без використання третіх пристроїв, таких як точка доступу.

2. Клієнт – сервер – бездротова мережа складається, як мінімум, з однієї точки доступу, що є сервером, підключеною до провідної мережі та деякого набору бездротових клієнтських станцій, які називаються клієнтами.

У зв'язку з тим, що в більшості бездротових мереж необхідно забезпечувати доступ до різних серверів прикладних завдань, принтерів та будь-яких інших пристроїв, підключених за допомогою дротової локальної мережі, зазвичай використовують режим з використанням точки доступу, тобто клієнт-сервер. Без підключення додаткових антен зв'язок для обладнання, що працює в стандарті IEEE 802.11b, досягається приблизно на таких відстанях:,

1.Вільний відкритий простір – близько 500 м

2.Кімната, розділена перегородками з матеріалу, що не має у своїй основі великої кількості металу - 100 м

3.Офісне приміщення з кількох кімнат – 30 м.

-Слід мати на увазі, що через залізобетонні стіни (частіше несучі, тому що в них багато арматури) радіохвилі діапазону 2,4 ГГц можуть взагалі не проходити, тому в розділених такою стіною приміщеннях доведеться ставити свої точки доступу, частіше об'єднані загальною провідною мережею .

Також група протоколів IEEE 802.11 регулює інші сторони мережі та обладнання для їх побудови. Список протоколів з коротким описом їх застосування уявлень нижче:

802.11 - початковий 1 Мбіт/с та 2 Мбіт/с, 2,4 ГГц та ІЧ стандарт (1997).

– 802.11a – 54 Мбіт/с, 5 ГГц стандарт (1999, вихід продуктів у 2001).

- 802.11b – покращення до 802.11 для підтримки 5,5 та 11 Мбіт/с (1999).

- 802.11c – процедури операцій з мостами; включено до стандарту IEEE 802.1D (2001).

- 802.11d – міжнародні роумінгові розширення (2001).

- 802.11e - покращення: QoS, пакетний режим (packetbursting) (2005).

- 802.11F – Inter-Access Point Protocol (2003).

- 802.11g – 54 Мбіт/с, 2,4 ГГц стандарт (зворотна сумісність з b) (2003).

- 802.11h – розподіл за спектром 802.11a (5 GHz) для сумісності в Європі (2004).

- 802.11i – покращена безпека (2004).

- 802.11j – розширення для Японії (2004).

- 802.11k - покращення вимірювання радіоресурсів.

- 802.1m – поправки та виправлення для всієї групи стандартів 802.11n – збільшення швидкості передачі (600 Мбіт/с). 2,4-2,5 чи 5 ГГц. Зворотна сумісність із 802.11a/b/g (вересень 2009).

- 802.11p - WAVE - Wireless Access for the Vehicular Environment (бездротовий доступ до середовища транспортного засобу).

- 802.11q - зарезервування, іноді його плутають з 802.1Q.

- 802.11r – швидкий роумінг.

- 802.11s - ESS Wireless mesh network [en] (Extended Service Set - розширений набір служб; Mesh Network - багатозв'язкова мережа).

- 802.11T - WirelessPerformancePrediction (WPP, передбачення продуктивності бездротового обладнання) - методи тестів та вимірювань.

- 802.11u - взаємодія з не-802 мережами (наприклад, стільниковими).

- 802.11v - управління бездротовими мережами.

- 802.11w - Protected Management Frames

- 802.11x - зарезервування і не буде використовуватися. Не слід плутати зі стандартом контролю доступу IEEE 802.1X.

- 802.11y – додатковий стандарт зв'язку, який працює на частотах 3,65-3,70 ГГц. Забезпечує швидкість до 54 Мбіт/с на відстані до 5000 м на відкритому просторі.

- 802.11ac – новий стандарт IEEE. Швидкість передачі даних – до 6,77 Гбіт/с для пристроїв, що мають 8 антен. Затверджено у січні 2014 року.

- 802.11ad — новий стандарт із додатковим діапазоном 60 ГГц (частота не потребує ліцензування). Швидкість передачі – до 7 Гбіт/с. вимагає ліцензування). Швидкість передачі даних – до 7 Гбіт/с.

Зі всього вищезазначеного списку можна назвати два найменування: 802.11F і 802.11T, які є рекомендаціями, а чи не стандартами, тому застосовуються великі літери в тому назва.»[2]

## 1.3. Переваги і недоліки безпровідних мереж

Мережі 802.11 дозволяють підвищувати мобільність пересональних користувачів та співробітників в офісних та виробничих приміщеннях, допомагають позбутися витрат на монтаж та обслуговування провідних мереж, особливо якщо ремонт вже закінчено, а кабелі спочатку не були прокладені. «Бездротові локальні мережі Wi-Fi мають сенс використовувати в умовах дому або ж на підприємствах з невеликим кількістю робочих місць або коли використовується досить велика кількість бездротових пристроїв (планшетів, ноутбуків, смартфонів, комунікаторів тощо). Найчастіше логічним методом побудови мережі є використання обох типів мереж одночасно: провідних та бездротових мереж Wi-Fi.

Основні переваги полягають у наступному:

- Простота та швидкість розгортання мережі;
- Низька вартість розгортання;
- Відсутність проводів на робочому місці або в житловому приміщенні (хоча б частини проводів).»[5]

А основні недоліки:

- Швидкість передачі даних ділиться між пристроями, підключеними до бездротової мережі Wi-Fi у межах однієї і тієї ж точки доступу, що їх обслуговує. Це означає, що якщо роутер надає нам швидкість передачі даних близько 220 мбіт/с і до неї буде одночасно підключено, наприклад, 2 планшети, 2 смартфони та ноутбук, то швидкість передачі даних для кожного пристрою складає 220/5 = 44мбіт/с. А насправді буде ще менше, бо потрібна ще передача

службової інформації, яка може зайняти від 30 до 40 відсотків. В результаті швидкість передачі становить приблизно 26 мбіт/с на один пристрій;

- Вплив предметів навколо таких, як дерева, стіни будівель, навіть побутових пристроїв, таких як холодильник;
- Досить низька надійність у зв'язку з тим, що все «передається повітрям» і будь-який злодій може атакувати цю точку доступу в межах її доступності;
- Низька стійкість до зла при неправильному настроюванні.

Мінуси частично можна перекрити якіснішим та безпечнішим обладнанням, а також об'єднанням кількох рознесених по приміщеннях точок доступу до однієї провідної мережі.

При розгортанні бездротової мережі будинку, для підключення пари ноутбуків, комп'ютера та кількох будь-яких гаджетів бездротова мережа Wi-Fi буде ідеальним варіантом за швидкістю розгортання та економічною складовою. Також легко розширює вже створену провідну мережу у поміщенні.

«Для з'єднання віддалених локальних мереж (або віддалених сегментів локальної мережі) використовується обладнання із направленими антенами, що дозволяє збільшити дальність зв'язку до 20 км, (а при використанні спеціальних підсилювачів та великої висоті розміщення антен – до 50 км). Причому як подібне обладнання можуть виступати і пристрої Wi-Fi, потрібно лише додати до них спеціальні антени (звичайно якщо це допускається конструкцією). Комплекси для об'єднання локальних мереж із топології поділяються на точку-точку та зірку. При топології «точка-точка» (режим Ad-hoc в IEEE 802.11) організується радіоміст між двома віддаленими сегментами мережі. При топології «зірка» одна зі станцій є центральною та взаємодіє з іншими віддаленими станціями. У цьому центральна станція має всеспрямовану антену, інші віддалені станції - односпрямовані антени. Застосування всеспрямованої

антени на центральній станції обмежує дальність зв'язку дистанцією приблизно 7 км. Тому, якщо потрібно з'єднати між собою сегменти локальної мережі, віддалені один від одного на відстань понад 7 км, доводиться з'єднувати їх за принципом «точка-точка». У цьому організується бездротова мережа з кільцевою чи іншою, складнішою топологією.»[6].

## 1.4. Способи взлому wi-fi мережі

Вищі викладені методи безпеки використовуються для захисту від загроз порушення інформаційної безпеки, ці загрози умовно можна розділити на два класи:

Прямі — загрози інформаційної безпеки, що виникають при інформаційному обміні бездротовою локальною мережею Wi-Fi;

Непрямі – загрози, пов'язані з великою кількістю точок доступу Wi-FI

Прямі загрози

Радіоканал у межах доступності Wi-FI роутера, за допомогою якого здійснюється передача даних, схильний до легкого втручання з метою отримання несанкціонованого доступу до ресурсів та інформації.

У стандартах, що регламентують роботу Wi-Fi, передбачені як автентифікація, так і шифрування, але ці елементи захисту мають свої вади та слабкі місця.

Шифрування впливає на швидкість передачі даних, і часто воно відключається адміністратором для оптимізації трафіку в бездротовій мережі. Перший стандарт шифрування Wired Equivalent Privacy був дискредитований знаходженням уразливостей в алгоритмі розподілу ключів RC4. Це трохи загальмувало розвиток ринку бездротових Wi-Fi мереж і викликало створення інститутом інженерів електротехніки та електроніки (IEEE) групи 802.11i для розробки нового стандарту безпеки, що враховує відомі вразливості WEP, що забезпечує 128-бітове шифрування AES та автентифікацію для захисту даних, що передаються. Альянс Wi-Fi у 2003 представивши своє бачення цього стандарту, так званий проміжний варіант цього стандарту Wi-FiProtectedAccess (WPA). Wi-FiProtectedAccess використовує протокол цілісності тимчасових

ключів TemporalKeyIntegrityProtocol (TKIP). Також у ньому почали використовувати метод підрахунку контрольної суми: MIC (MessageIntegrityCode), яка стала дозволяти перевіряти цілісність переданих пакетів. У 2004 альянс Wi-Fi

випустили новий, що набрав великої популярності на сьогоднішній день, стандарт WPA2, який є покращенням стандарту WPA. Основна різниця між стандартами WPA та WPA2 полягає у технології шифрування: WPA – TKIP та WPA2 – AES. Стандарт WPA2 дозволяє забезпечити більш високий рівень захисту бездротової мережі, оскільки TKIP дозволяє створювати ключі завдовжки лише до 128 біт, а AES – вже до 256 біт.

Загроза блокування інформації у бездротовому каналі Wi-Fi залишена практично без уваги при розробці технології бездротових мереж. Блокування каналу не є небезпечним, тому що зазвичай бездротові Wi-Fi мережі є допоміжними для провідних мереж, незважаючи на те, що блокування може бути підготовчим етапом для проведення атаки «людина посередині», коли між роутером та клієнтським пристроєм впроваджується третій пристрій, що перенаправляє. . трафік між роутером та клієнтом через себе. Дане використання дозволяє видаляти, по-різному видозмінювати інформацію, а також «підсовувати» неправдиву інформацію.

**Чужаки**

Чужаками (RogueDevices, Rogues) називають периферійні пристрої та комп'ютери, що дають можливість несанкціонованого доступу до корпоративної мережі, зазвичай, обминаючи захисні механізми, визначені політикою безпеки. Заборона на будь-яке використання пристроїв бездротового зв'язку не зможе захистити від бездротових мережевих атак, якщо в мережі, навмисне або ненавмисно, з'явиться чужинець. У ролі пристрою чужинця може виступати все,

що завгодно, у чого є провідний і бездротовий інтерфейси: роутери (включаючи програмні), проектори, сканери, ноутбуки з обома включеними інтерфейсами і т.д.

**Нефіксована природа зв'язку**

Бездротові wi-fi пристрої можуть легко змінювати точки підключення до мережі прямо в процесі роботи і навіть непомітно для користувача. Наприклад, можуть відбуватися «випадкові асоціації», коли ноутбук з Windows XP (налаштовані на довірчі відносини до всіх бездротових мереж) або просто неправильно настроєний клієнт бездротової мережі автоматично асоціюється і підключає користувача до найближчої бездротової wi-fi мережі. Таким чином, злодій може перемикати на свою підставну точку доступу для подальшого сканування вразливостей, фішингу або атак «людина посередині». А якщо пристрій при цьому підключено і до провідної локальної мережі, то він стає точкою входу, так званим чужинцем. На додаток до цього багато користувачів, підключені до внутрішньої локальної мережі, використовуючи Wi-Fi інтерфейс, зазвичай незадоволені якістю та політикою роботи мережі, перемикаються на найближчу доступну точку доступу (або недбало налаштована операційна система робить це автоматично при відмові проводової мережі). При цьому весь побудований захист мережі зазнає краху.

Є ще одна проблема – мережі точка-точка, за допомогою яких зручно передавати файли між колегами або друкувати на принтері, який підтримує Wi-Fi. Але така організація бездротових мереж не підтримує багато методів забезпечення безпеки, що робить їх легко доступною здобиччю для злодія. А нові технології VirtualWiFi і Wi-FiDirect, що прийшли, тільки погіршили ситуацію в плані безпеки.

**Вразливості мереж та пристроїв**

Некоректно налаштовані мережеві пристрої, пристрої зі слабкими та недостатньо довгими ключами шифрування, що використовують скомпрометовані методи автентифікації – саме ці пристрої зазнають атак у першу чергу. «Згідно зі звітами аналітиків, більшість успішних зломів відбувається саме через неправильні налаштування точок доступу та програмного забезпечення клієнта.»[7]

**Некоректно налаштовані точки доступу**

Варто підключити некоректно налаштовану точку доступу до мережі для злої останньої. Заводські налаштування, так звані "за замовчуванням", зазвичай не включають шифрування та автентифікацію, або використовують ключі, прописані в посібниках користувача, і тому вони є всіма відомими навіть на офіційних форумах виробника.

Малоймовірно, що користувачі досить серйозно спантеличуються налаштуванням пристроїв, націлених на безпеку. Саме такі точки доступу до бездротової мережі і створюють основні загрози захищеним мережам.

**Неправильно налаштовані бездротові клієнти**

Неправильно настроєні клієнтські пристрої — загроза значно небезпечніша, ніж неправильно настроєні точки доступу. Це клієнтські пристрої, які не конфігуруються спеціально для безпеки внутрішньої мережі підприємства. До того ж, зазвичай вони знаходяться за межами периметра контрольованої зони або всередині периметра, що може дозволити зловмиснику проводити всілякі атаки, наприклад, поширювати вирусне програмне забезпечення або просто забезпечувати легкодоступну та зручну точку входу.

**Злом шифрування**

Про захищеність скомпрометованого алгоритму забезпечення безпеки WEP і не йдеться. Інтернет має у своєму розпорядженні у вільному доступі спеціальним та зручним у використанні програмним забезпеченням для зламування цього стандарту, яке здійснює збір статистики трафіку доти, доки не стане достатньо для відновлення ключа шифрування. Стандарти WPA та WPA2 також мають кілька уразливостей різного ступеня опасности, що дозволяють здійснити їх злом, але поки що немає інформації про успішні атаки на WPA2-Enterprise (802.1x).

**Імперсонація та IdentityTheft**

Імперсонація (видача собі за іншу людину) авторизованого користувача — серйозна загроза для будь-якої комп'ютерної мережі, що стосується не лише бездротової. Однак у бездротовій мережі визначення справжності користувача відбувається складніше. Існують SSID і можна робити спроби фільтрувати за MAC-адресами, але, і ті, і інші передається в ефірі у відкритому вигляді, і їх нескладно підробити, а коли підробивши - можна, як мінімум, знизити пропускну здатність мережі, вставляючи неправильні frame, а трохи розібравшись в алгоритмах шифрування, влаштовувати тестування на проникнення у цілу структуру мережі (наприклад, використовувати атаки типу ARP-spoofing). Імперсонація користувача можлива не тільки в разі заміни MAC адреси за умови встановлення MAC-автентифікації або використання статичних ключів. Схеми будівництва мереж на основі 802.1x (WPA2 Enterprise) не є абсолютно безпечними. Деякі механізми (LEAP) мають складність зла, схожу зі зломом WEP. Інші механізми, EAP-FAST або PEAP-MSCHAPv2, хоч і надійніше, але не гарантують стійкості до проведеної зловмисником комплексної атаки.

**Відмови в обслуговуванні**

DoS атаки спрямовані на порушення якості функціонування сервісу бездротової мережі або на абсолютне припинення доступу користувачів та відмови обладнання до перезавантаження. У разі Wi-Fi мережі відстежити джерело, що завалює мережу, специфічним для цього типу атаки, «сміттєвими» пакетами, дуже складно – його розташування обмежується лише зоною покриття. До того ж є апаратний варіант цієї атаки — встановлення досить сильного джерела перешкод у частотному діапазоні точки доступу, що працюють, так звані «глушилки».

## 1.5. Особливості функціонування безпровідних мереж

У бездротових мереж є деякі специфічні особливості, які у провідних мережах відсутні. Дані особливості в цілому впливають на загальну продуктивність, доступність, безпеку та ціну обслуговування бездротової мережі. Їх доводиться враховувати, хоча вони не привносять будь-якого внеску до шифрування чи автентифікації. Для вирішення таких питань потрібний спеціальний інструментарій та налагоджені механізми адміністрування та моніторингу мережі.

### Активність у неробочу годину

Логічним буде рішення обмежити політикою безпеки доступ до мережі поза робочою годиною (аж до фізичного відключення електроживлення точки доступу), активність у бездротовій мережі в неробочу годину має моніторитися, вважатися як підозріла та піддаватися розслідуванню.

### Інтерференція

Якість роботи бездротової Wi-Fi мережі як радіоефіру залежить від багатьох факторів. Один з них — інтерференція радіосигналів, яка може дуже знизити пропускну здатність і омежити кількість користувачів, аж до повної неможливості використання мережі. Як джерело може виступати будь-яке пристрій, наприклад, роутер із занадто сильним випромінювачем, не дозволеним у вільному продажі, що випромінює на тій же частоті сигнал достатньої потужності. Це можуть бути як сусідні точки доступу, так і мікрохвильові печі. Цю особливість цілком можуть також використовувати атакуючі як атака відмови в обслуговуванні або для підготовки атаки «людина посередині», заглушаючи безпечні точки доступу і залишаючи свою з таким же SSID (підмінна при атакі людина «посередині»).

**Зв'язок**

Існують інші специфічні особливості бездротових мереж, крім інтерференції сигналу. Неправильно налаштований термінал клієнта або антена, що дають збої, можуть значно знижувати якість обслуговування решти користувачів. Або питання стабільності зв'язку, що логічно виникає. Не тільки сигнал роутера повинен досягти клієнта, а сигнал клієнта повинен досягти назад роутера. Зазвичай роутери в кілька разів потужніші, і щоб досягти симетрії, можливо, доведеться знизити потужність сигналу на роутері. Для 5 ГГц слід пам'ятати, що надійно працюють лише 4 канали: 36/40/44/48 (для Європи, для США є ще 5). На інших включено режим співіснування з радарами (DFS). В результаті, зв'язок роутера та клієнтського пристрою може досить часто пропадати.

## 1.6. Технології захисту безпровідних wi-fi мереж

Для захисту Wi-Fi мереж використовується кілька широко відомих способів, таких як метод обмеження доступу та метод аутентифікації. Розглянемо методи трохи докладніше.

Методи обмеження доступу:

- Фільтрування MAC-адреса:

До стандарту IEEE 802.11 такий метод не входить. Але є три способи фільтрації:

Роутер дозволяє підключатися клієнтам з будь-якою MAC-адресою;

Роутер дозволяє підключатися клієнтам, чиї MAC'і знаходяться у білому списку;

Роутер забороняє підключатися клієнтам, чиї MAC

"чорному списку";

З точки зору безпеки найнадійнішим може бути інший варіант, але він не розрахований на заміну MAC-адреси, чим легко може скористатися злодій.

- Режим приховування ідентифікатора точки доступу SSID (англ.

ServiceSetIDentifier):

Для свого виявлення точка доступу періодично здійснює розсилку beaconframes (у перекладі кадрів-маяків). Такий кадр містить певну службову інформацію для підключення, а також містить у собі SSID (ідентифікатор бездротової мережі). У разі режиму приховання SSID

це поле порожнє, тобто стає неможливим виявити вашу бездротову мережу та підключитися до неї, не знаючи значення самого SSID. Але всі клієнти, підключені до мережі, знають SSID і під час підключення, коли розсилають ProbeRequest (у перекладі спроба на підключення), вказують идентифікатори цих мереж, збережені в їх профілях підключень. Прослуховуючи робочий трафік даних клієнтів, можна легко отримати значення SSID точки доступу, необхідної для підключення до бажаного роутера.

**Методи аутентифікації**

**1. OpenAuthentication (укр.Відкрита автентифікація):**

Клієнт робить запит аутентифікації, в якому присутній лише свій MAC-адреси. Роутер відповідає або відмовою, або підтвердженням автентифікації. Рішення приймається на основі фільтрації за списком MAC-адрес, тобто це спосіб захисту бездротової локальної Wi-Fi мережі на основі списку доступу.

**2.Використання для автентифікації шифру:**

без шифрування.SharedKeyAuthentication (укр. Аутентифікація із загальним ключем). Потрібне налаштування незмінного - статичного ключа шифрування алгоритму WEP (WiredEquivalentPrivacy). Клієнт робить запит у точки доступу на автентифікацію, на що отримує підтвердження, яке містить

128 байт випадкової інформації. Станція шифрує отримані дані алгоритмом WEP (проводиться побітове додавання за модулем 2 даних повідомлення з послідовністю ключа) та відправляє зашифрований текст разом із запитом на асоціацію. Точка доступу розшифровує текст та порівнює з вихідними даними. У разі збігу надсилається підтвердження асоціації, і клієнт вважається підключеним до мережі.

Схема автентифікації із загальним ключем уразлива до атак

«Maninthemiddle (людина посередині)». Алгоритм шифрування WEP – це простий XOR ключової послідовності з корисною інформацією, отже, прослухавши трафік між станцією та точкою доступу, можна відновити частину ключа.

Шифри, що використовуються: без шифрування, динамічний WEP, CKIP.

**3.Аутентифікація за MAC-адресою:**

«Цей метод не передбачений у IEEE 802.11, але підтримується більшістю виробників обладнання, наприклад D-Link та Cisco. Відбувається порівняння MAC-адреси клієнта з таблицею дозволених MAC-адрес, що зберігається на точці доступу, або використовується зовнішній сервер аутентифікації. Використовується як додатковий захід захисту.

IEEE розпочав розробки нового стандарту IEEE 802.11i, але через труднощі затвердження, організація WECA (англ. Wi-FiAlliance) спільно з IEEE анонсували стандарт WPA (англ. Wi-FiProtectedAccess). У WPA використовують TKIP (англ. TemporalKeyIntegrityProtocol, протокол перевірки цілісності ключа), який використовує удосконалений спосіб управління ключами та покадрову зміну ключа.»[6]

**4.Wi-Fi Protected Access (WPA)**

Після перших успішних атак на WEP було прийнято розробити новий стандарт 801.11i. Але до нього був випущений проміжний стандарт WPA, який включав нову систему аутентифікації на базі 801.1x і новий метод шифрування TKIP. Існують два варіанти аутентифікації: за допомогою RADIUS сервера (WPA-Enterprise) та за допомогою попередньо встановленого ключа (WPA-PSK)

Використані шифри: TKIP (стандарт), AES-CCMP (розширення), WEP (як зворотної сумісності).»[8]

### 5.WI-FI Protected Access2 (WPA2, 801.11I)

“WPA2 або стандарт 801.11i – це фінальний варіант стандарту безпеки бездротових мереж. Як основний шифр був обраний стійкий блоковий шифр AES. Система аутентифікації порівняно з WPA зазнала мінімальних змін. Також як і в WPA, WPA2 є два варіанти аутентифікації WPA2-Enterprise з автентифікацією на сервері RADIUS і WPA2-PSK з установленим ключем.

Використані шифри: AES-CCMP (стандарт), TKIP (як зворотної сумісності).»[9]

### 6. Cisco Centralized Key Management (CCKM)

Варіант аутентифікації від фірми CISCO. Підтримує роумінг між точками доступу. Клієнт один раз проходить автентифікацію на сервері RADIUS, після чого може перемикатися між точками доступу.

Використані шифри: WEP, CKIP, TKIP, AES-CCMP»[10]

# РОЗДІЛ 2. ЗЛОМ БЕЗПРОВІДНИХ МЕРЕЖ НА ПРАКТИЦІ

## 2.1. Обладнання для злому (тестування на проникнення)

- Для того, щоб почати займатися тестуванням на проникнення, нам знадобиться персональний комп'ютер на x86, x64 або ARM архітектурі з установленою операційною системою Linux з ядром версії не менше 2.6.22. Я використовував ноутбук HPPavilionDV6 3056er із встановленою ОС KaliLinux 2016.2 та встановленими всіма останніми оновленнями.

- Wi-Fiадаптер, драйвери якого, під операційною Linux, підтримують режими моніторингу та ін'єкцій. Список таких адаптерів можна легко знайти в інтернеті, наприклад, на сайті: https://wikidevi.com/wiki/Category:Linux_driver/802dot11.

- Комплект ПЗ aircrack-ng (версія під Linux), який включає наступні пакети: aircrack-ng

- Взламує ключі WEP та WPA (Перебір за словником).

- airdecap-ng Розшифровує перехоплення трафік за відомого ключа.

- airmon-ngВиставляє мережеву картку в режим моніторингу.

- aireplay-ngПакетний інжектор.

- airodump-ng Аналізатор трафіку: Поміщає трафік у файли PCAP або IVS та показує інформацію про мережі.

- airtun-ng Створює віртуальний інтерфейс тунелювання.

- packetforge-ng Створює шифровані пакети для ін'єкції.

- Ivstools Інструменти для злиття та конвертування.

- airbase-ng Надає техніку для атаки клієнта.

- airdecloak-ng Забирає WEP-маскування з файлів pcap.

- airolib-ng Зберігає та керує списками ESSID та паролів, обчислює парні майстер-ключі.

- airserv-ng Відкриває доступ до бездротової мережі з інших комп'ютерів.

- buddy-ng Сервер-помічник для easside-ng, запущений на віддаленому комп'ютері.

- easside-ng Інструмент для комунікації з точкою доступу без наявності WEP-ключа.

- tkiptun-ngАтака WPA/TKIP.

- wesside-ng Автоматичний інструмент для відновлення WEP-ключа.

У моєму варіанті дане ПЗ йшло у складі ОС.

Бездротова точка доступу, яку ми будемо налаштовувати під конкретне шифрування і використовувати її як атаковану. Я для своєї роботи використав D-linkDIR-615.

Для спрощення та покращення якості тестування на проникнення краще використовувати KaliLinux останньої стабільної версії, її можна безкоштовно отримати для некомерційного використання на офіційному сайті розробників: https://www.kali.org/, до неї включені всі пакети для тестування на проникнення.

## 2.2. Злом на практиці wi-fi мережі з wep шифруванням

Перейдемо до тестування на проникнення в мережу, організовану бездротовою точкою доступу із встановленим на ній для авторизації WEP шифруванням.

Для цього нам потрібна бездротова точка доступу. Я налаштував із зазначенням наступних параметрів:

назва – mntl

пароль – дізнаєтесь наприкінці

тип шифрування – WEP Початок:

Для початку нам потрібно залогінитись під обліковим записом root. Або будь-який інший, але тоді перед кожною командою потрібно вводити sudo.

Відкриваємо термінал (ctrl + alt + t) та для визначення драйвера вводимо команду:

airmon-ng


Рисунок 1 – Виведення результату виконання команди airmon-ng

В результаті виконання програми інтерфейс називається "wlan0",

—Chipset" має статус "Unknown", але драйвер визначився. Якщо подібний висновок або "Chipset" визначився, значить, можемо переходити далі, інакше потрібно налагодити драйвер або використовувати інший wi-fi адаптер.

Наступним кроком потрібно перевести карту в режим роботи - моніторинг, для цього ввести в терміналі команду:

airmon-ngstart wlan0


Рисунок 2 – Виконання команди airmon-ngstartwlan0

В результаті виконання команди в передостанньому рядку терміналу бачимо текст: "monitormodeenabledonmon0", що означає, що ми можемо для моніторингу використовувати включений інтерфейс mon0.

Наступним кроком буде увімкнення режиму прослуховування для визначення доступних Wi-Fi мереж, для цього виконаємо команду:

airodump-ng mon0

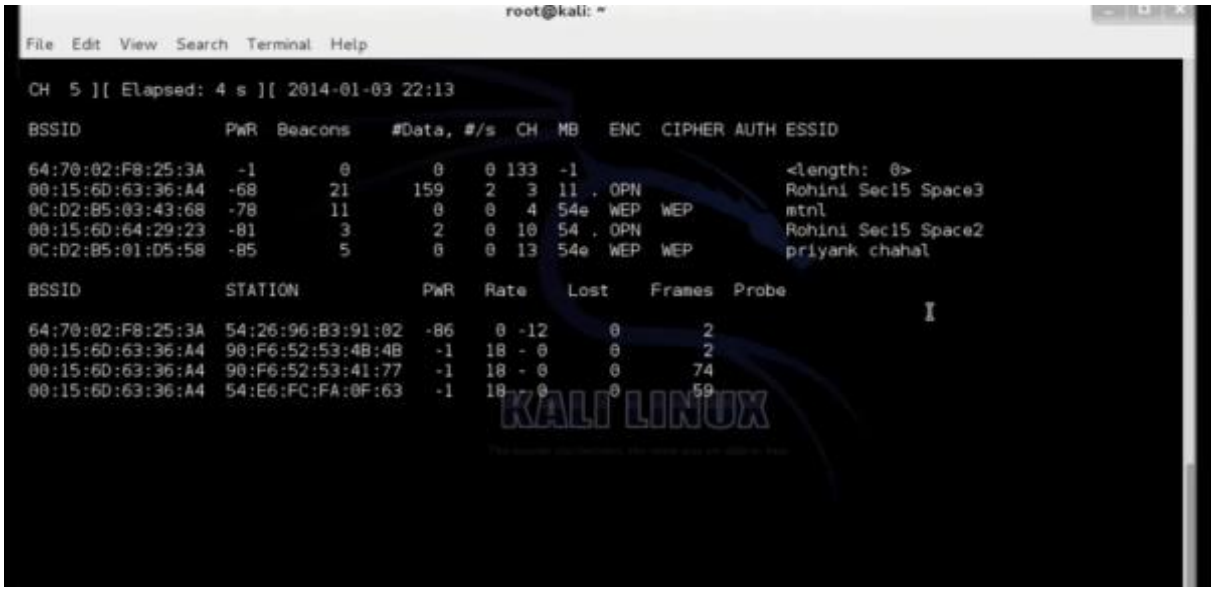


Рисунок 3 – Список доступних мереж

В результаті виконання команди ми можемо спостерігати список бездротових мереж у радіусі дії нашого Wi-Fi адаптера. Можемо

спостерігати, що створена нами спочатку мережа, названа mtnl, має такі важливі для нас характеристики: використовуване шифрування WEP, 4 канал, bssid

– фізична адреса точки доступу для відповідної мережі - 0C:D2:B5:03:43:68.

Тепер, знаючи потрібну нам інформацію, почнемо захоплювати пакети, в яких, можливо, отримаємо зашифрований пароль, зробити це можна ввівши таку команду:

airodump-ng –w mtnl-org –c 4 –bssid 0C:D2:B5:03:43:68 mon0

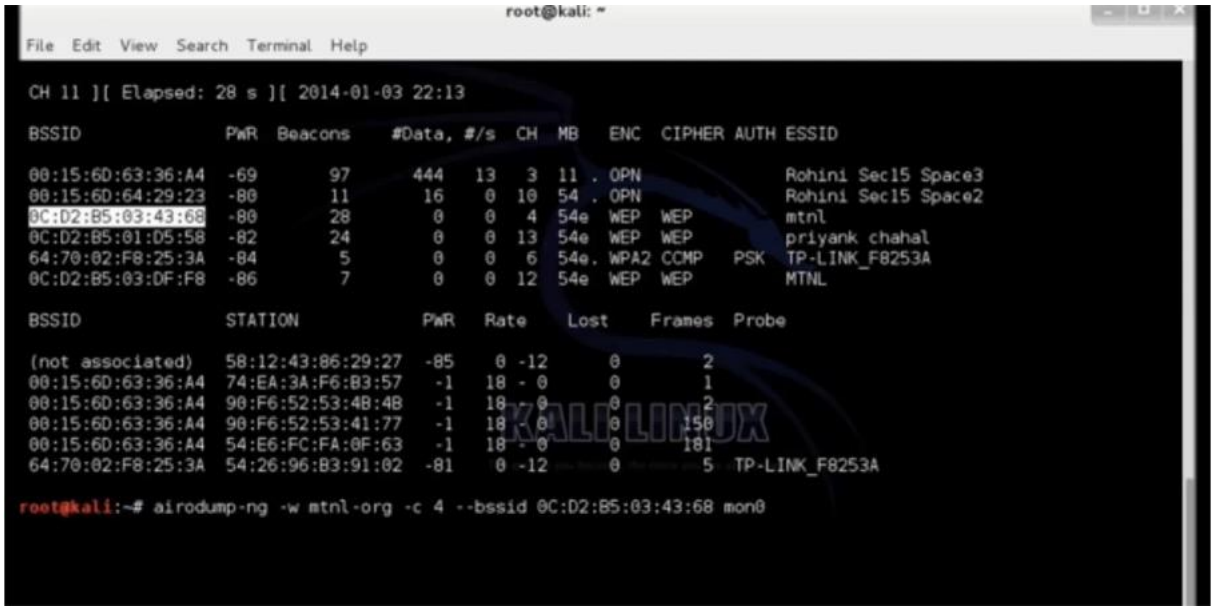


Рисунок 4 – Процес захоплення пакетів

Де –wmtnl записати перехоплені пакети у файл mtnl (файл буде автоматично створено у вигляді: l-org-X.cap, де X номер файлу з перехопленими пакетами змінюватиметься, якщо атака переривалася, і ми починали заново, не видаляючи старий файл), я вибрав як і назву мережі, щоби не плутатися; -з 4 вказівку каналу, на якому працює бездротова мережа під назвою mtnl; - bssid фізична адреса точки доступу; mon0 – вибір інтерфейсу, у якому виконати захоплення пакетів.

Після виконання команди чекаємо орієнтовно 10-15 хвилин, щоб захопити близько 15000 IVS пакетів (пакетів, що містять вектор ініціалізації). Тривалість очікування залежить від активності мережі. Якщо до точки доступу ніхто не підключений, час може затягнутися. Відстань до точки доступу не така важлива, як активність у мережі. Якщо

активність маленька, і збирання пакетів йде повільно, то спробуємо

«розтрусити» точку доступу, для цього відкриваємо ще один термінал - дуже важливо залишити термінал, що використовується раніше активним, просто згортаємо його в трей і використовуємо команду

aireplay-ng -0 0 -a 0C:D2:B5:03:43:68 mon0

де -0 0 зробити атаку деаутентифікація(-0), доки вона не буде зупинена вручну (0).

-a фізична адреса точки доступу

mon0 інтерфейс, який використовується для атаки.

Коли закінчили збір приблизно 15000 пакетів, відкриваємо новий термінал, у ньому починаємо розшифровувати пакет, для цього скористаємося командою

aircrack-ng mtnl-org-01.cap

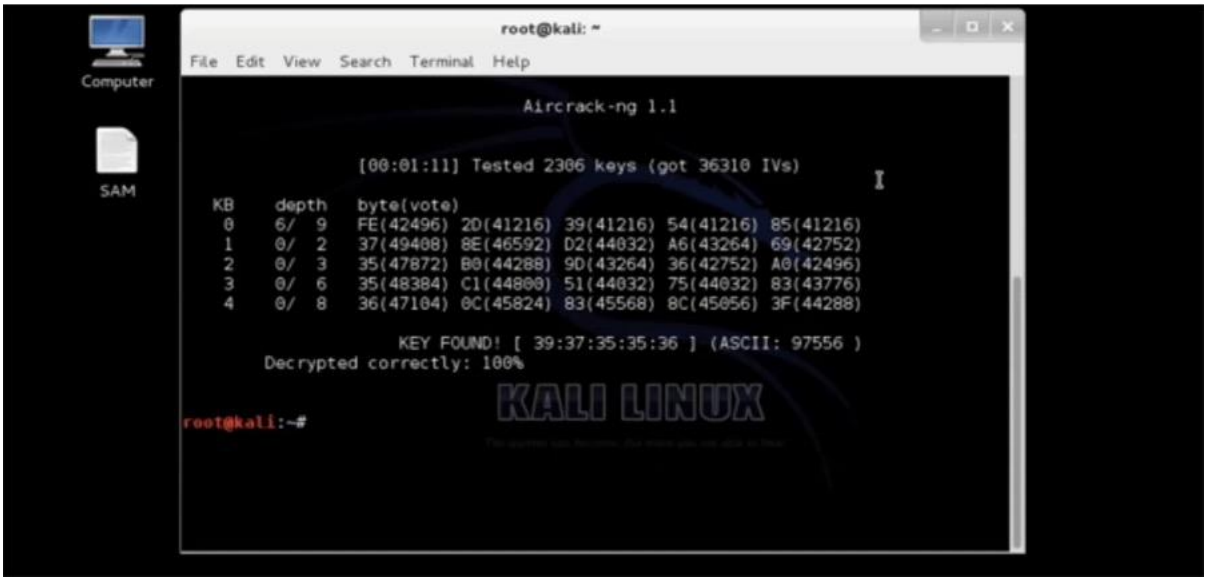


Рисунок 5 – Розшифровка пакетів

Після закінчення процесу дешифрування ми побачимо, що пароль 100% розшифровано коректно. Тепер можемо підключитися до точки доступу mtnl, використовуючи пароль: 3937353536. Якщо цього повідомлення не побачили

або побачили, що не на 100%, повторіть захоплення пакетів і зберіть в 2-5 разів більше пакетів. І повторіть процес дешифрування. Кількість пакетів, що захоплюються, може вимагатися більше або менше, залежно від складності і довжини пароля.

## 2.3. Злом на практиці wi-fi мережі з wpa/wpa2 personal шифруванням

Перейдемо до тестування на проникнення в мережу, організовану бездротовою точкою доступу із встановленим на ній для авторизації WPA/WPA2 Personal шифруванням.

Для цього нам потрібна бездротова точка доступу. Я налаштував із зазначенням наступних параметрів:

назва – pentest_router

пароль – дізнаєтесь наприкінці

тип шифрування – WPA

Приступимо до дій:

Для початку нам потрібно залогінитись під обліковим записом root. Або будь-який інший, але тоді перед кожною командою потрібно вводити sudo.

Відкриваємо термінал (ctrl + alt + t) та для визначення драйвера вводимо команду:

airmon-ng


Рисунок 6 – Перегляд драйвера мережевої карти

Виведення команди показує список бездротових карт, які підтримують режим монитора. Якщо жодні карти не вказані, потрібно перепідключити адаптер і

переконатися, що він підтримує режим мониторингу. Якщо використовується вбудований адаптер, він не підтримує режим дисплея, тоді потрібно використовувати зовнішній за допомогою режиму дисплея. У виведенні команди можна переконатися, що моя карта підтримує моніторинг і називається wlan0

Далі нам потрібно перевести нашу картку в режим моніторингу, для цього виконаємо команди:

airmon-ng start wlan0

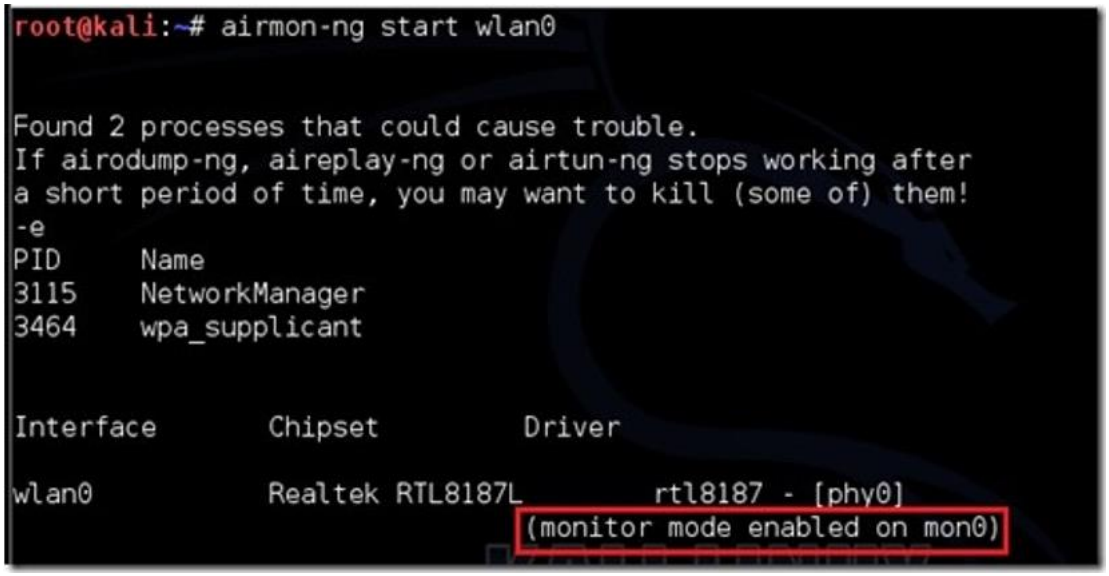


Рисунок 7 – Переведення мережевої картки в режим моніторингу

Червоним виділено виведення команди, що означає, що режим мониторингу увімкнено та інтерфейс називається mon0.

Наступним кроком буде увімкнення режиму прослуховування для визначення доступних Wi-Fi мереж, для цього виконаємо команду:

airodump-ng mon0

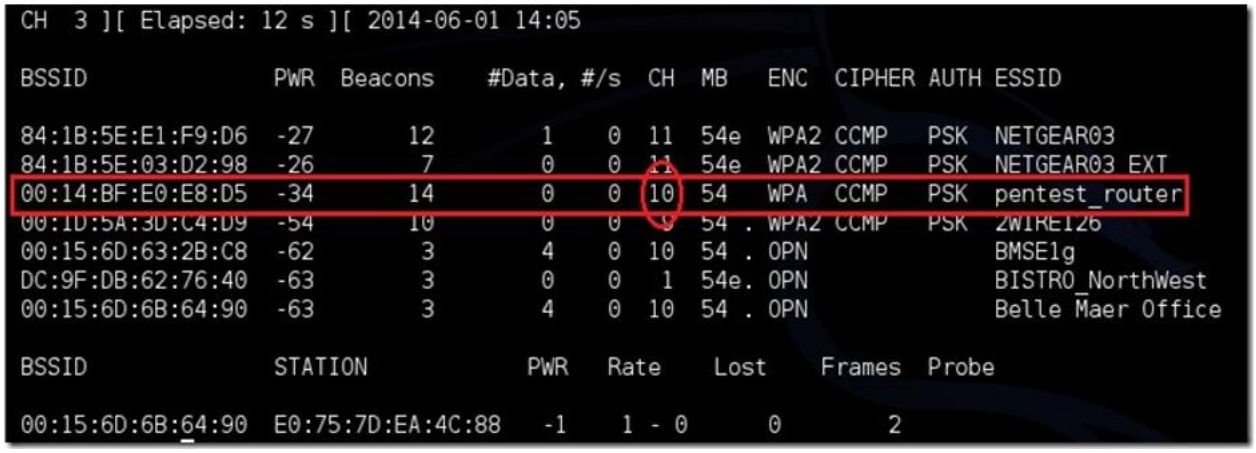


Рисунок 8 – Список бездротових мереж

На рисунку виділено мережу, яку ми створили та використовуємо для тестування атаки.

Далі нам потрібно використати команду

airodump-ng -c 10 --bssid 00:14:BF:E0:E8:D5 -w /root/Desktop/ mon0, де-c – номер каналу

--bssid – фізична адреса точки доступу

-w шлях, куди записуватимемо перехоплений початковий обмін пакетами, так званий handshake.

Для того щоб перехопити handshake нам потрібно після запуску виконання вищезгаданої команди дочекатися поки хтось підключиться до мережі, або, при наявному вже підключеному клієнті, потрібно зробити деавторизацію клієнта, що підключеного в даний момент. Для виконання цього кроку може знадобитися багато часу, якщо активні підключення будуть відсутні. Ми підключимо будь-який інший пристрій до відомої мережі, емулюючи активність.


Рисунок 9 – Перегляд підключених клієнтів

На рисунку 9 бачимо підключеного клієнта, де виділення червоним, меншим за розміром – фізична адреса клієнта

Для виконання деавторизації клієнта нам потрібно, не закриваючи термінал, відкрити другий і виконати команду:

aireplay-ng –0 2 –a 00:14:BF:E0:E8:D5 –c 4C:EB:42:59:DE:31 mon0, де

-0 – ключ для проведення деавторизації

2 – кількість пакетів деавторизації

-a – фізична адреса точки доступу

-c – фізична адреса клієнта

mon0 – наш інтерфейс, який використовується для атаки

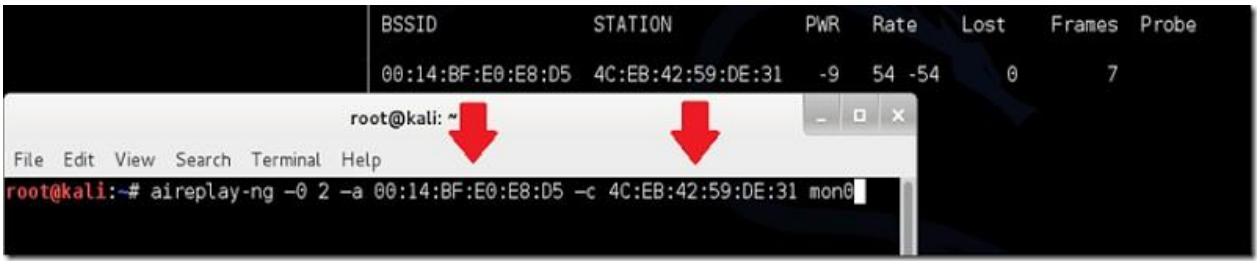


Рисунок 10 – Виконання деавторизації клієнта

Якщо все пройшло успішно, побачимо повідомлення в термінал, де виконували попередню команду:


Рисунок 11- Перехоплення handshake

Потрібне нам повідомлення:


Рисунок 12 – Перехоплений handshake

Отримавши це повідомлення можемо переходити до наступного кроку, інакше повторювати попередню команду доти, доки не отримаємо у виведенні повідомлення про отримання handshake'a. перехоплення handshake

Тепер ми можемо натиснути клавіші ctrl+c в терміналі, в якому виконується aireplay. Не варто одразу закривати термінал.

Після цього ми можемо переходити до злому - використовуватимемо спосіб перебору. Для цього нам знадобиться словник паролів. Його можна легко знайти на просторах інтернету або створити свій, дотримуючись лише кількох правил синтаксису: один пароль = один рядок і жодних пробілів перед і після і розширення файлу —.txt‖.

Приступимо до методу перебору пароля, для цього потрібно виконати команду

aircrack-ng –a2 –b 00:14:BF:E0:E8:D5 –w /root/wpa.txt root/Desktop/*.cap

```
aircrack-ng -a2 -b 00:14:BF:E0:E8:D5 -w /root/wpa.txt /root/Desktop/*.cap
```

Рисунок 13 – Запуск перебору паролів

-a- це метод атаки з використанням наявного рукостискання (handshake'a),

2 - WPA

-b – фізична адреса атакованої точки доступу

-w – шлях до словника з розширенням —.txt‖

/root/Desktop/*.cap – директорія для збереження cap файлу, що містить пароль.

```
Opening /root/Desktop/-01.cap
Reading packets, please wait...

                                Aircrack-ng 1.2 beta3

                  [00:00:00] 192 keys tested (1409.45 k/s)

                           KEY FOUND! [ notsecure ]


      Master Key     : 42 28 5E 5A 73 33 90 E9 34 CC A6 C3 B1 CE 97 CA
                       06 10 96 05 CC 13 FC 53 B0 61 5C 19 45 9A CE 63

      Transient Key  : 86 D0 43 C9 AA 47 F8 03 2F 71 3F 53 D6 65 F3 F3
                       86 36 52 0F 48 1E 57 4A 10 F8 B6 A0 78 30 22 1E
                       4E 77 F0 5E 1F FC 73 69 CA 35 5B 54 4D B0 EC 1A
                       90 FE D0 B9 33 06 60 F9 33 4B CF 30 B4 A8 AE 3A

      EAPOL HMAC     : 8E 52 1B 51 E8 F2 7E ED 95 F4 CF D2 C6 D0 F0 68
root@kali:~#
```

Рисунок 14 – Результат перебору паролів

На рисунку вище після перебору 192 комбінацій у словарі ми знайшли наш пароль. Цей метод не є оптимальним, т.к. якщо словарь на кілька тисяч комбінацій, перебір виходить дуже довгим і часто трапляється, що пароля, встановленого на роутері, немає у нашому словарі. Такий спосіб зручний для перебору найпопулярніших комбінацій, таких як: 12345678, qwertyui і т.д. У разі складних паролів цей спосіб може мати жодного успіху. Але ми просто так не

здамося, спробуємо розглянути ще один випадок. Наприклад, наша точка доступу також налаштована на WPS підключення (підключення за пін-кодом або натискання клавіші на самому роутері).

Для цього ми виконаємо дії, що і з методом перебору, до кроку визначення точки доступу та її каналу (дії ідентичні). Повторю результат, який нам потрібний:

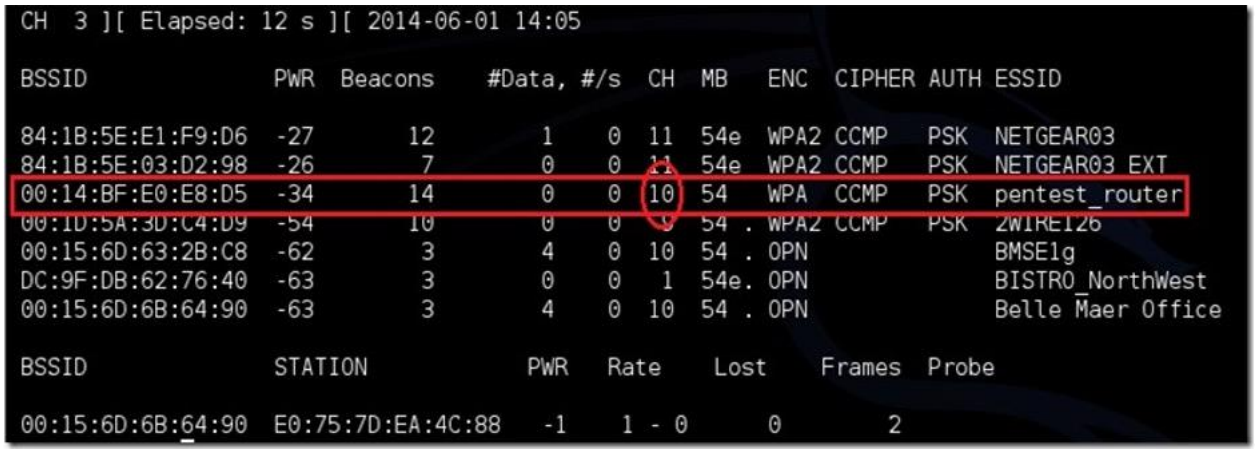


Рисунок 15 – Перевірка WPS

Превіряємо, чи WPS на точці доступу командою

wash -i mon0

Якщо точки доступу немає у списку, то пробуємо іншу. Наше є, т.к. ми налаштували WPS для тестування даного методу.

Далі починаємо перебір пін-кодів командою reaver -i mon0 -b 1C:BD:B9:B5:C6:B9 -a -vv

де mon0 - інтерфейс з якого виконуємо атаку

-b – фізична адреса точки доступу

-a – автоматичне визначення параметрів злому

-vv – діагностичні повідомлення В результаті пішов перебір пінів:

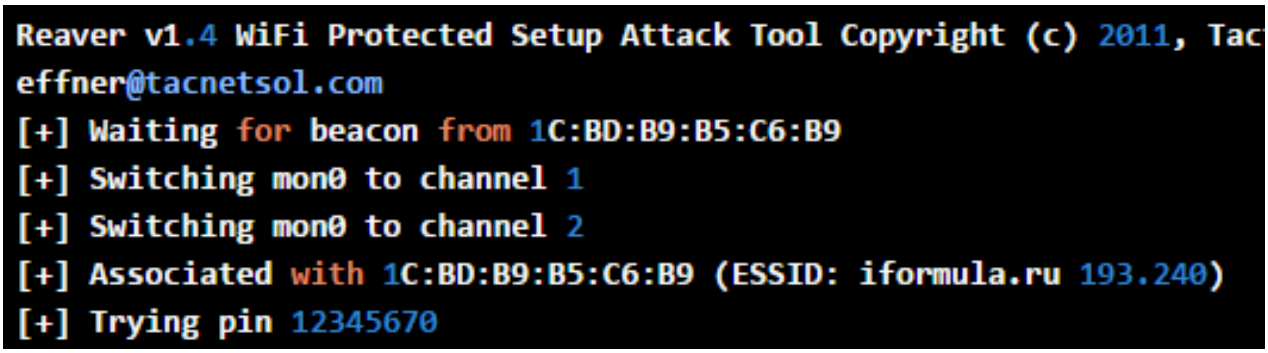


Рисунок 16 – Старт перебору пін кодів Приблизно через 10-12 годин ми отримуємо:

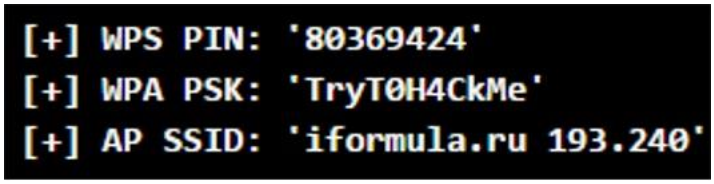


Рисунок 17 – Знайдений пін код

Ось таким теж довгим, але найвірогіднішим способом можемо отримати і WPSпін і WPAkey.

Різними ключами, доступними за командою reaver –h, можна прискорити процес не більше ніж удвічі, або вказати будь-які специфічні параметри для зламування конкретної точки доступу.

Вишезазначені способи є не найоптимальнішими, адже може статися так, що WPS вимкнено, пароль встановлений досить великою довжиною, т.к. встановлювати можна від 8 до 63 символів, і тоді перебір може закінчитися за кілька років, але це неактуально.

Про це, проаналізувавши загальнодоступну інформацію, дізнаємось про райдужні таблиці.

«В результаті SQL-ін'єкції на сайті RockYou хакерам вдалося затягнути 32 мільйони паролів відкритим текстом. З того моменту і розпочалася нова епоха.

Гігантська база даних дозволила розробникам ПЗ на зло паролів повністю переробити словари, якими здійснюється брутфорс. Замість «теоретичних» слівників вони з'явилися справжніми словниками з реальними паролями. База RockYou досі залишається унікальним, найкращим ресурсом для зла.

Після кожного нового витоку хешів дедалі більшу частку з них вдавалося підібрати за словарем, а ресурси виділялися на аналіз складних паролів, які потім також додавалися до словника. Наприклад, в наш час пароль на зразок Sup3rThinkers вважається легким для зла, тому що він підбирається за словарем з кількома замінами, для яких існують відповідні правила. Для прискорення пошуку за словарями з десятків гігабайт застосовуються райдужні таблиці.»[16]


Рисунок 18 – Райдужні таблиці

Тому скористаємося інструментом, що є у вільному доступі, і проведемо атаку на мережу з використанням «райдужних таблиць».

На моєму ноутбуку встановлено відеокарту від AMD. Для проведення атаки потрібно встановити пропрієтарний fglrx драйвер, для цього послідовно виконаємо команди:

Оновлення системи: apt-get update

apt-getdist-upgrade

встановлення хедерів Linux та рекомендованих програм apt-get install firmware-linux-nonfree

apt-get install amd-opencl-icd

apt-get install linux-headers-$(uname -r)

Установлення драйверів fglrx та контрольної панелі

apt-get install fglrx-atieventsdfglrx-driver fglrx-control fglrx-modules-dkms –y

Тестування установки

fglrxinfo fgl_glxgears

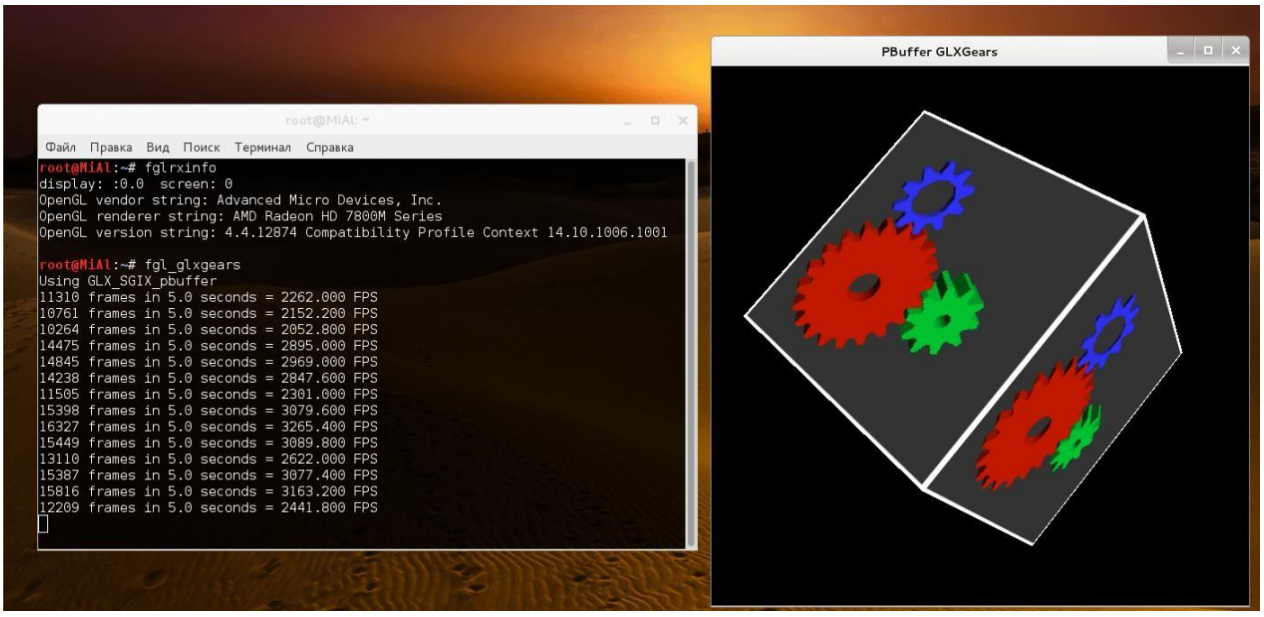


Рисунок 19 –Тестування коректності встановлення драйвера

Тепер нам необхідно згенерувати xorg.conf

aticonfig --initial -f

файл xorg.conf буде розміщено у каталозі /etc/X11.

Далі нам потрібно оновити файл grub.cfg та перезавантажити ноутбук, для цього відкриваємо grub.cfg командою:

leafpad /boot/grub/grub.cfg знаходимо секцію:

```
### BEGIN /etc/grub.d/10_linux ###
menuentry 'Kali GNU/Linux, с Linux 3.18.0-kali3-amd64' --class kali --class gnu-linux --class gnu --class os {
load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='(hd0,msdos1)'
search --no-floppy --fs-uuid --set=root 4b5ccc43-ae6f-4cca-bf7d-0344af8644c6
echo 'Загружается Linux 3.18.0-kali3-amd64 ...'
linux /boot/vmlinuz-3.18.0-kali3-amd64 root=UUID=4b5ccc43-ae6f-4cca-bf7d-0344af8644c6 ro initrd=/install/gtk/initrd.gz quiet
echo 'Загружается начальный ramdisk ...'
initrd /boot/initrd.img-3.18.0-kali3-amd64
}
```

Рисунок 20 – Сегмент конфігураційного файлу grub.cfg I на кінець наступного рядка додаємо

radeon.modeset=0, тобто. має вийти так:

```
linux /boot/vmlinuz-3.18.0-kali3-amd64 root=UUID=4b5ccc43-ae6f-4cca-bf7d-0344af8644c6 ro initrd=/install/gtk/initrd.gz quiet r
adeon.modeset=0
```

Рисунок 21 – Потрібний рядок

Зверніть увагу: значення UUID, яке в моєму випадку 4b5ccc43-ae6f-4cca-bf7d-0344af8644c6, може бути різним на кожному ПК. Чи не перезаписуйте ваше значення моїм.

Зберігаємо файл і перезавантажуємо ноутбук командою:

Reboot

Після перезавантаження нам потрібно перевірити, чи встановлено модуль fglrx, командою

lsmod | grepfglrx

В результаті має бути висновок приблизно наступного змісту

```
fglrx 8679112 140
button 12988 1 fglrx
```

Рисунок 22 – Перевірка коректності установки модуля fglrx

Далі нам потрібно встановити AMDAPPSDK 3.0 Beta, для встановлення спочатку скачем зі сторінки завантаження архівів AMD, доступне за посиланням http://developer.amd.com/tools-and-sdks/opencl-zone/amd-accelerated-parallel- pro-cessing-app-sdk/

Переходимо до установки SDK, виконаємо наступні команди: mkdiramdappsdk – створюємо папку

mv/root/Downloads/AMD-APP-SDK-v3.0-0.113.50-Beta-linux64.tar.bz2 amdappsdk/ - копіюємо завантажений архів у створену папку cdamdappsdk – переходимо до створеної папки

tarxvjfAMD-APP-SDK-v3.0-0.113.50-Beta-linux64.tar.bz2 – розпаковуємо архів shAMD-APP-SDK-v3.0-0.113.50-Beta-linux64.sh – запускаємо установник

Дотримуючись інтерактивної інструкції проходимо установку до кінця і найголовніше, коли програма запитає шлях установки, натискаємо Enter, щоб встановити в папку за замовчуванням, а саме /opt - що нам і потрібно

Далі нам потрібно відредагувати файл /root/.bashrc, виконаємо команду leafpad /root/.bashrc

і в кінець файлу допишемо

```
# AMD APP SDK
export AMDAPPSDKROOT=/opt/AMDAPPSDK-3.0-0-Beta/
export AMDAPPSDKSAMPLESROOT=/opt/AMDAPPSDK-3.0-0-Beta/
export LD_LIBRARY_PATH=${AMDAPPSDKROOT}lib/x86_64:${LD_LIBRARY_PATH}
export ATISTREAMSDKROOT=$AMDAPPSDKROOT
```

Рисунок 23 – Необхідний конфігураційний файл Зберігаємо зміни та потім у терміналі виконуємо команду:

source ~/.bashrc

Перевірити успішність установки та початкового налаштування можемо командою:

env | grep -i amd

висновок має бути приблизно наступного виду:

```
AMDAPPSDKSAMPLESROOT=/opt/AMDAPPSDK-3.0-0-Beta/
LD_LIBRARY_PATH=/opt/AMDAPPSDK-3.0-0-Beta/lib/x86_64:
ATISTREAMSDKROOT=/opt/AMDAPPSDK-3.0-0-Beta/
AMDAPPSDKROOT=/opt/AMDAPPSDK-3.0-0-Beta/
```

Рисунок 24 – Виведення команди env | grep -Iamd

Далі нам потрібно встановити CAL++

Тепер нам потрібно підготуватися для наступного кроку, виконаємо команди:

svncheckouthttps://github.com/clockfort/amd-app-sdk-fixes/trunk/include/CAL;

$AMDAPPSDKROOT/include/CAL apt-get install cmakelibboost-all-dev

Шукаємо сам CAL++ за посиланням:
https://sourceforge.net/projects/calpp/files/calpp-0.90/calpp-0.90.tar.gz/download

Встановлюємо CAL++ cd ~/Downloads

tar-xvfcalpp-0.90.tar.gz cd calpp-0.90/

Нам потрібно відредагувати файл CMakeLists.txt, для цього виконаємо команду:

leafpad CMakeLists.txt

Знаходимо рядки, що починаються з FIND_LIBRARY та FIND_PATH та поміняємо їх на:

```
FIND_LIBRARY( LIB_ATICALCL aticalcl PATHS "$ENV{ATISTREAMSDKROOT}" )
FIND_LIBRARY( LIB_ATICALRT aticalrt PATHS "$ENV{ATISTREAMSDKROOT}" )
FIND_PATH( LIB_ATICAL_INCLUDE NAMES cal.h calcl.h PATHS "$ENV{ATISTREAMSDKROOT}/include/CAL" )
```

Рисунок 25 – Результат зміни файлу Зберігаємо відредагований файл та закриваємо його. Далі для встановлення виконуємо команди:

cmake . –.Обов'язкова make

makeinstall

Заключним підготовчим етапом буде встановлення Pyrit Pyritдозволяє нам створювати масивні бази даних, попередньо
прораховувати частину фази аутентифікації IEEE 802.11 WPA/WPA2-PSK з компромісними витратами часу та місця. Використання обчислювальної потужності багатопроцесорних систем та інших платформ, у тому числі ATI-Stream, Nvidia CUDA, OpenCL та VIA Padlock, - це на даний момент найбільш потужний вектор атаки на протоколи безпеки, що найбільш використовуються.

Для встановлення виконаємо наступні команди:

- apt-getinstalllibpcap-dev – встановлюємо бібліотеку, що бракує,
- svncheckout http://pyrit.googlecode.com/svn/trunk/ pyrit_svn – завантажуємо pyrit
- cdpyrit_svn/pyrit/ -переходимо в папку
- ./setup.pybuildinstall – запускаємо установку

Установка плагіна CAL++

- Переходимо до папки командою: cd ../cpyrit_calpp/
- редагуємо файл setup.py, для цього введемо команду: leafpad setup.py
- знаходимо у файлі рядок:VERSION  = '0.4.0-dev' і наводимо її до вигляду: VERSION = '0.4.1-dev'
- знаходимо у файлі рядок: CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include')) і наводимо його до вигляду: CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include/CAL'))
- Зберігаємо внесені зміни та закриваємо редагування файлу.
- Далі вводимо команду: ./setup.py buildinstall

Буде кілька попереджень, але не повинно бути помилок.

Тестуємо pyrit командою pyritlist_cores

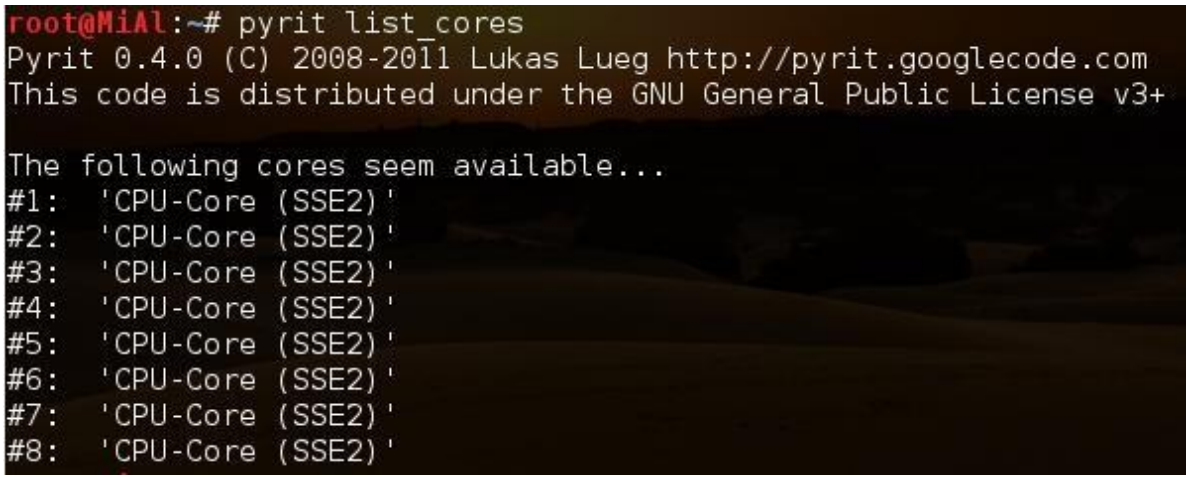


Рисунок 26 – Список ядер

Для наочності виконаної роботи наведу два приклади роботи

Перший без CAL++


Рисунок 27 –Швидкість перебору парольних фраз без CAL++

Бачимо 4037,9 PMKs/s

Другий із CAL++

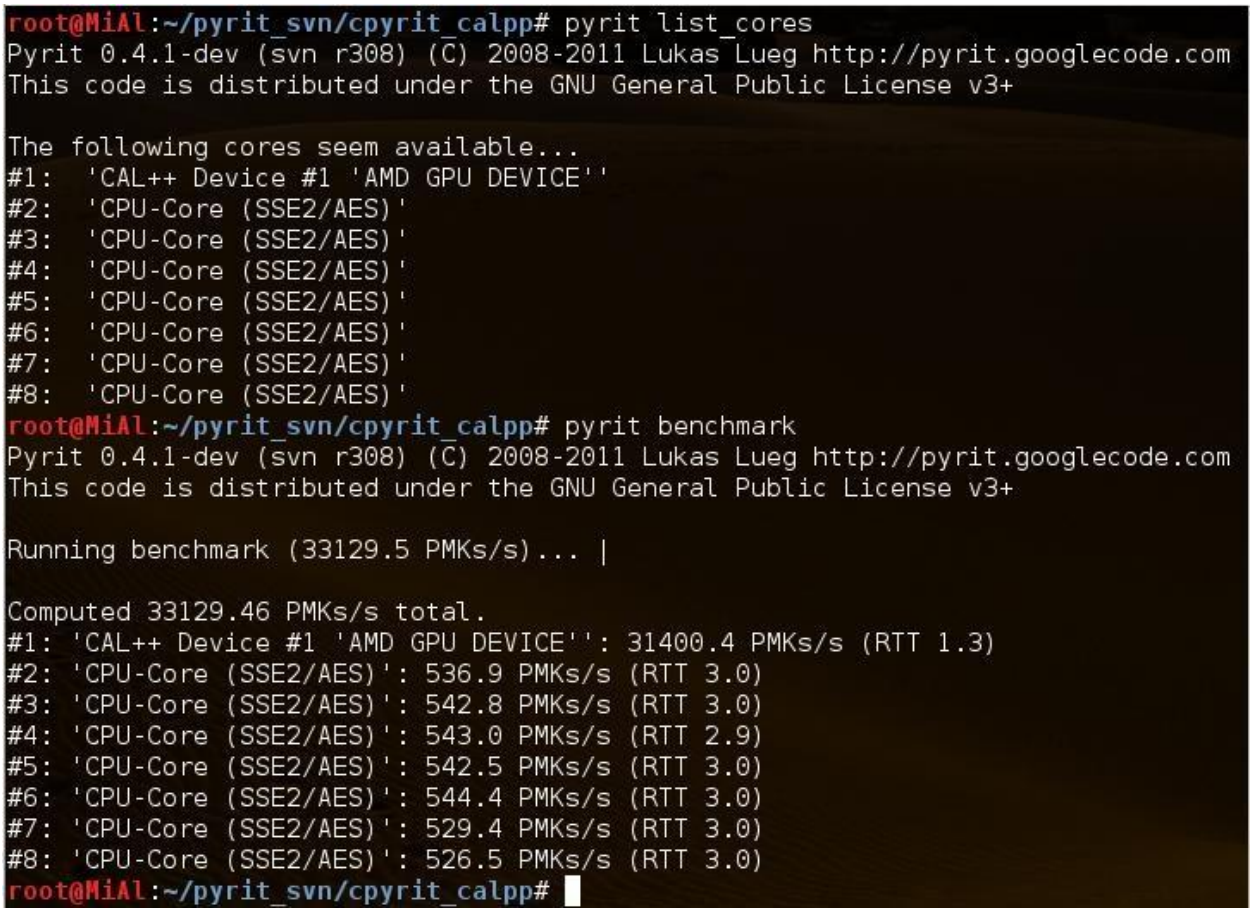


Рисунок 28 – Швидкість перебору парольних фраз із CAL++

Бачимо 33129,5 PMKs/s

У PMKs/s вимірюється швидкість, звана SpeedHashcat – що у перекладі російською означає швидкість перебору хешей(результату виконання підрахунку хеш функцій).

Тепер наш ноутбук готовий до атаки з використанням райдужних таблиць. Повторюся, оскільки використання райдужних таблиць має на увазі такий самий перебір, як і в першому випадку, і ми підготували наш ноутбук для прискореного перебору з використанням відеокарти та процесора. Відмінність полягає лише в тому, що перебір буде не безпосередньо кодової комбінації, а хеша з алгоритмом перестановки.

Нам потрібно захопити «рукостискання» він-же «handshake». Для початку переведемо мережевий адаптер в режим моніторингу

Для захоплення handshake можна скористатися утилітою, що автоматизує наші дії, яка називається wifite і йде за замовчуванням в KaliLinux.

Введемо команду - wifite

Ви можете як ключі вказати тип шифрування (WEP, WPA, WPA2), якщо ви хочете вивести бездротові мережі з конкретним типом шифрування.

Коли програма закінчить роботу, ми побачимо доступні точки доступу, а також запрошення для введення точок доступу, з яким ви хочете "handshake". Я вибравши 1 і 2, для цього ввівши без лапок «1,2» і натиснувши ENTER, якщо ви хочете вибрати все відразу, то потрібно замість «1,2» (без лапок) вписати "all" (без лапок). Після того, як натиснули Enter, звернемо увагу на висновок. Дуже довго на першій точці доступу нічого не відбувалося і щоб не гаяти годину я натиснув клавіші ctrl+c. Далі програма запитала

```
What do you want to do?
[c]ontinue attacking targets
[e]xit completely.
```

Рисунок 29 – Діалогове вікно

І тут виявилася зручна функція, так як у реченні було натиснути клавішу "c" для атаки на інші вібрані точки, або "e" для виходу. Я натиснувши "c" і через кілька секунд отримав "handshake", це "рукостискання" було збережено у файлі: /root/hs/BigPond_58-98-35-E9-2B-8D.cap. Після того, як захоплення відбулося, і точок доступу більше немає, програма автоматично завершить своє виконання, і ви отримаєте командну строчку.

Тепер, коли у нас є файл із захопленим «рукостисканням», ми можемо піти двома шляхами:

1. Використовувати атаку за словником
2. Використовувати атаку «грубою силою»

У зв'язку з тим, що за статистикою, кожна п'ята точка доступу матиме пароль зі словника rockyou, який поповнюється новими паролями після кожного витоку в інтернеті, розглянемо спочатку атаку за словником.

Завантажуємо актуальну версію словника за посиланням: https://wiki.skullsecurity.org/index.php?title=Passwords

Скопіюємо файл словника до каталогу root, виконавши команду: cp /usr/share/wordlists/rockyou.txt.gz

Розпакуємоархів, виконавши команду: gunziprockyou.txt.gz

Відповідно до IEEE 802.11 довжина пароля повинна бути не менше 8 символів і не більше 63, давайте очистимо наш словник і приберемо всі записи, які не задовольняють умову: 7 < кількість символів у записі < 64, виконаємо це наступною командою:

cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > newrockyou.txt де –m 8 – мінімальна довжина символів,

- - M 63 максимальна довжина символів
- sort - відсортувати
- uniq – тільки унікальні записи
- >newrockyou.txt – вихідний файл після сортування.

Тепер дізнаємось, скільки унікальних комбінацій залишилося, командою: wc –lnewrockyou.txt

Висновок команди нам видав 9605346 записів = паролів. Виконавши команду:

wc –lrockyou.txt

Висновок команди нам видав 14342346 записів = паролів.

Отже, ми зробили файл коротшим, що означає, що ми можемо протестувати наш словник у більш стислий термін, тепер перейменуємо наш

файл і зробимо його у вигляді: wpa2.lst, командою:

mv newrockyou.txt wpa.lst

Наступним кроком буде створення ESSID у базі даних Pyrit, для цього виконаємо команду:

pyrit -eBigPondcreate_essid, де BigPond назва нашої бездротової мережі. Якщо в назві бездротової мережі є пробіли, то найменування разом із пробілом (як є) пишеться в апострофах.

Наступним кроком нам потрібно імпортувати наш відсортований та перейменований словник у базу даних pyrit, для цього виконаємо команду: pyrit -i /root/wpa.lstimport_passwords

Створюємо наші "райдужні таблиці", використовуючи пакетний (batch) процес, для цього виконаємо команду:

pyritbatch

Увага, будьте обережні, на моєму ноутбуці процесор був задіяний на 100%, і температура на ядрах піднялася до 94 градусів Цельсія. Потрібно бути дуже обережним, і в залежності від того, наскільки великий файл словника та

наскільки гарячі процесор та відеокарта. Бажано наскільки можна використовувати додаткове охолодження.

Тепер сам процес злому. У нас є пара варіантів

1. Використовуючи Pyrit
2. Використовуючи Cowpatty

Використовуватимемо атаку на «рукостискання» з бази даних, використовуючи Pyrit, для цього введемо команду:

pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap attack_db, де hs/ - файл із захопленим handshake'ом,

attac_db – використовувана база даних

Час виконання кілька хвилин, щоб пройти по всій таблиці бази даних. Швидкість у виведенні команди сягала 159186.00 PMKs/s. І якщо встановлений пароль був у базі даних, він визначається за кілька хвилин. Очевидно, що це швидше за перші два способи.

Якщо не створювати базу даних, а звертатися безпосередньо до нашого словника (не імпортованого wpa2.lst), можна скористатися командою:

pyrit -rhs/BigPond_58-98-35-E9-2B-8D.cap -i /root/wpa.lstattack_passthrough, де -i /root/wpa.lst– шлях до словника attack_passthrough – атака по проходу (проходитиметься словник, комбінація за комбінацією)

За виконання цієї команди швидкість склала близько 8000 PMKs/s, що значно повільніше і неоптимально.

Продовжимо шукати найоптимальніший спосіб, для цього спробуємо скористатися cowpatty для проведення нашої атаки, введемо наступну команду:

pyrit -e BigPond -o cow.outexport_cowpatty Після запуску процесу перебору, командою:

cowpatty -d cow.out -s BigPond -r hs/BigPond_58-98-35-E9-2B-8D.cap

Після введення команди буде перевірено великий список паролів на відповідність хеш файлу. Це продовжуватиметься до перебору всіх паролів. Як тільки у файлі словника буде знайдено відповідний пароль, процес злому зупиниться, і вам буде виведено пароль. Швидкість у момент перебору склала 164 823 PMKs/s.

Цей спосіб я вважаю найефективнішим і найшвидшим. Дуже зручно за допомогою засобів автоматизації деяких процесів швидко перевіряти безпеку мережі.

# РОЗДІЛ 3. АВТОМАТИЗОВАНА СИСТЕМА ДЛЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ. РЕКОМЕНДАЦІЇ З КОНФІГУРУВАННЯ ТОЧОК ДОСТУПУ

## 3.1. Одноплатний комп'ютер

У ході виконання роботи ми дізналися, що потрібне мобільне пристрій на базі ОС Linux, за допомогою якого ми зможемо робити атаки, в той же час через досить тривалий процес нам потрібна хороша автономність. Крім хорошої автономності потрібний мінімальний розмір пристрою, для того щоб можна було його сховати в будь-якій сумці, без уваги. Виникає питання: для чого такі вимоги? Логічним буде висновок, що при зайнятті тестуванням на проникнення нам не потрібно великих габаритів, що цю функцію може виконати будь-яка людина, яка перебуває в радіусі роботи бездротової точки доступу. Тим самим було демонструючи потенційному замовнику чистоту процесу. Зробивши висновки з вищезгаданих обмежень та провівши аналіз ринку вільно доступних пристроїв, вибір впав на одноплатні комп'ютери на ARMархітектурі.

**Переваги перед ноутбуками та нетбуками:**

1.Низьке тепловиділення, що не вимагає активного охолодження і як наслідок безшумність пристрою;

2.Низьке енергоспоживання, що досягається достатня автономність;

3.Відсутність вбудованих пристроїв введення та виведення, таких як клавіатура та монитор, що зменшує розміри пристрою;

4. Багато програмного забезпечення у вільному доступі.

**Недоліки**

1.Відсутність вбудованих пристроїв введення та виведення, що потребує додаткових пристроїв для управління;

2.Низька обчислювальна потужність;

3.Слабкий контролер живлення.

Дивлячись на переваги та недоліки, виникає усвідомлене розуміння, що одноплатні комп'ютери задовольняють всі вимоги, крім обчислювальної потужності. Тому що пристроєм введення та виведення може бути будь-який смартфон або планшет. Наявність USB порту та великої кількості вільно доступного ПЗ дозволяє використовувати 3G/4G модем для підключення зовнішнього пристрою управління за протоколами ssh, telnet, VNC та інші.

У ході аналізу ринку одноплатних комп'ютерів було зроблено акцент на двох поширених моделях: RaspberryPi 3 model Bi та IntelEdisonKit.

Таблиця 2 – Порівняння двох популярних одноплатних комп'ютерів

| Найменування | Raspberry Pi 3 model B | Intel Edison Kit |
|---|---|---|
| Виробник | RaspberryPiFoundation | Intel |
| Графічний процесор | 2-х ядерний videocoreiv | відсутня |
| ОЗУ | 1 Гб | 1 Гб |
| Підтримувані ОС | Linux, Windows 10 | Linux,Windows embedded |

| | | |
|---|---|---|
| Тип процесора | bcm23874-х ядерний cortex-a53 | intelatom+intel quark |
| Встановлені інтерфейси | 4 xusb, hdmi, ethernet, micro-sd, audio, dsi, csi, i/o. | usb, i/o, wi-fi, bluetooth, Arduino |
| Частота процесора | 1.2 ГГц | 500 МГц |

З представленого порівняння за технічними характеристиками RaspberryPi3 modelB перевершує IntelEdisonKit. У зв'язку з цим для тестування на проникнення використовуватимемо RaspberryPi 3 modelB.

Рисунок 30 – Одноплатний комп’ютер  RaspberryPi 3 model B

## 3.2. Підготовка комп'ютера до тестування на проникнення в бездротові мережі

Одноплатний комп'ютер у базовій комплектації не дозволяє проводити атаки на бездротові мережі. Щоб з'явилася ця можливість, потрібно:

1. Оснастити USBWi-Fiадаптером з режимом проведення ін'єкцій;

2. Карта пам'яті MicroSD16Gb 10Class;

3. Дистрибутив KaliLinux для RaspberryPi, що включає необхідні пакети, такі як airmon, aircrack і т.д.;

4. Портативний аккумулятор із двома USB портами (2A, 5V, 16000 mAh);

5. USB хаб із зовнішнім живленням;

6. 3g/4g модем із "білою" ip адресою.

Для керування одноплатним комп'ютером за допомогою стороннього пристрою необхідно встановити та настроїти SSH сервер. Згодом для керування буде використовуватися SSH підключення із зазначенням наступних параметрів:

1. IP-адресою для підключення буде біла ip-адреса 3G/4G модему;
2. Логін та пароль будуть використані вказані під час встановлення ОС.

Подальшою дією буде тестування швидкості перебору парольних комбінацій, всі підготовчі дії проведено відповідно до пункту підготовки до проведення атаки на мережу з використанням «райдужних таблиць» (пункт 2.3)


Рисунок 31 – Швидкість перебору на одноплатному комп'ютері

Швидкість перебору 2037,9 парольних комбінацій за секунду, що не є достатнім результатом для швидкого проникнення.

У ситуації, що склалася, і наявної інформації в іншому розділі ми знаємо, що для злого WEP нам потрібні перехоплені пакети, записані у файл з розширенням .cap; для злого WPA/WPA2 нам потрібний так званий рукостискання (handshake) та словарь парольних фраз; Злом WPA/WPA2 за допомогою райдужних таблиць відрізняється від простого злому лише в методі перебору парольних фраз, де до обчислень залучаються ресурси графічного адаптера. Вирішили рознести процеси проведення атаки. За допомогою одноплатного комп'ютера робити захоплення необхідної інформації, а далі для її обробки передавати на віддалену машину, з великими обчислювальними потужностями, порівняно з одноплатним комп'ютером.

### 3.3. Комп'ютер для виконання ресурсомістких операцій

Для виконання ресурсомістких операцій, таких як пошук по райдужних таблицях, обчислення райдужних таблиць, потрібні великі потужності ЦП і відеокарти. Знаючи про те, що процес захоплення handshake і процес перебору парольних фраз можна рознести, вирішено використовувати стаційний персональний комп'ютер, який знаходиться вдома або в офісі, має вихід в інтернет і має наступні мінімальні характеристики:

1. Процесор не гірший за Corei7 5930K
2. Відеокарта не гірша за Radeon RX 480 G1
3. ОЗУ не менше 32 ГБ із тактовою частотою 3200 МГц і вище
4. SSD накопичувач

Вище вказані мінімальні характеристики комп'ютера дозволяють, здійснивши всі підготовчі дії, наведені в пункті підготовки до проведення атаки на мережу з використанням «райдужних таблиць» (пункт 2.3), продемонструвати на рисунку - 30 швидкість перебору в 95218,5 парольних комбінацій:

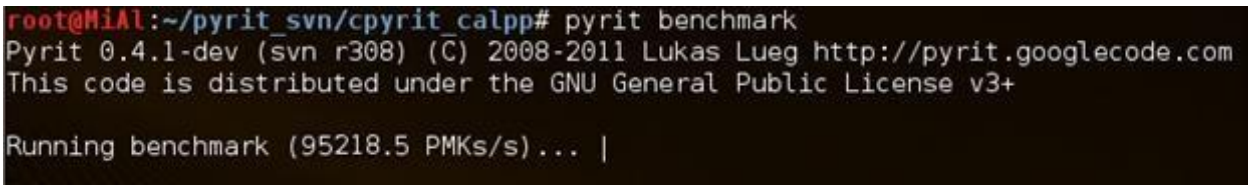


Рисунок 32 – Швидкість перебору на потужному комп'ютері

Зазначені вище мінімальні характеристики дозволяють отримати пароль SS367JYNbyeEJ285, маючи початкове значення виконання його хешування (8fae34ea751a81a7d41572d38eec54ea) приблизно за 11-12 секунд. Крім виконання операції перебору пароля є ще одна ресурсомістка операція, це операція створення райдужних таблиць, яку потрібно виконувати для кожної

точки доступу, що атакується. При перерахованих вище мінімальних характеристиках комп'ютера створення райдужних таблиць для парольної фрази довжиною від 8 до 63 символів займає близько 15-20 хвилин, що не буде критичним для проведення атаки на проникнення.

Зв'язок двох пристроїв

У ході виконання рознесеного тестування на проникнення з'ясувалося кілька складних нюансів. По-перше, шкірна точка доступу, на яку ми збираємося проводити атаку, має свій унікальний BSSID і в автоматичному режимі складно зробити вибір даної точки доступу, набагато швидше і точніше це робиться при виконанні вручну. По-друге, для отримання handshake потрібно переводити бездротовий інтерфейс у режим мониторингу, при виконанні даної функції скриптом інтерфейс не переводився в 25% випадках з 20 випробувань. По-третє, отримавши handshake і автоматично передаючи його на потужний комп'ютер, є ймовірність неправильної його передачі, для переконання у правильності передачі потрібно додатково передавати контрольну суму з подальшою перевіркою цілісності. Потрібна наявність «білої» ip-адреси на потужному комп'ютері ПК для встановлення сесії передачі від одноплатного на потужний комп'ютер, але це змушує до додаткових витрат. З усього вищесказаного був зроблений висновок, що весь процес рекомендовано відстежувати в реальному часі, і з'являється можливість вносити алгоритм тестування на проникнення.

Для управління процесом та передачі файлів між 2 пристроями будемо використовувати третій – керуючий пристрій, в якості якого буде використовуватися планшет або смартфон із підключеним мобільним інтернетом та встановленими:

1. TeamViewer
2. SSH клієнт

TeamViewer буде використовуватися для підключення до потужного комп'ютера та виконання на ньому операцій:

1. Передача з керуючого пристрою на потужний комп'ютер handshake'ів від точок доступу з налаштованим алгоритмом безпеки WPA/WPA2

2. Передача з керуючого пристрою на потужний комп'ютер захоплених пакетів від точки доступу з налаштованим алгоритмом безпеки WEP

3. Виконання команд для створення райдужних таблиць

4. Управління перебором парольних фраз.

SSH клієнт буде використовуватися для підключення до одноплатного комп'ютера RaspberryPi 3 modelBi виконання на ньому операцій:

1. Переведення безпроводового Wi-Fi інтерфейсу в режим мониторингу

2. Вибір точки доступу, що атакується.

3. Захоплення handshake'ів від точок доступу з налаштованим алгоритмом безпеки WPA/WPA2 та передача їх на керуючий пристрій

4. Захоплення пакетів від точок доступу з налаштованим алгоритмом безпеки WEP та передача їх одним файлом на керуючий пристрій

Вищезазначене програмне забезпечення даним функціоналом не обмежується, перераховані лише основні функції, що використовуються у даній роботі.

## 3.4. Покрокова структура виконання тестування на проникнення

1. Увімкнути потужний компютер із налаштованим автозапуском TeamViewer.

2. Створити словник (текстовий файл із парольними фразами), з наявного у вільному доступі rockyou.txt, вибравши всі парольні фрази завдовжки від 8 до 63 символів.

3. Підготувати одноплатний комп'ютер, підключивши USB Wi-Fi адаптер та 3G/4G модем із «білою» ip-адресою.

4. Опинитися в радіусі дії точки доступу, що атакується.

5. Увімкнути комп'ютер, вставивши кабель живлення в портативний акумулятор.

6. Дочекавшись залишкового завантаження одноплатного комп'ютера, (приблизно дві хвилини), підключитися до нього з керуючого пристрою за допомогою SSH клієнта.

7. Перевести бездротовий Wi-Fi-інтерфейс у режим моніторингу.

8. Вибрати точку доступу, що атакується.

9. Здійснити перехоплення handshake'у або пакетів (залежно від протоколу безпеки встановленого на точці доступу).

10. За допомогою команди scp скопіювати handshake або перехоплені пакети, записані у файл під час виконання п. 8.

11. Завершити сесію ssh.

12. Скопіюйте передані на керуючий пристрій файли у буфер обміну.

13. Запустити на керуючому пристрої Team Viewer та підключитись до потужного комп'ютера.

14. Виконати команду вставки (права кнопка миші>вставити) у потрібній директорії на потужному комп'ютері.

15. Якщо є точка доступу з налаштованим протоколом безпеки WEP, то виконавши команду: aircrack-ng «повний шлях до файлу без лапок», в результаті отримаємо пароль, який можна використовувати для підключення до атакованої бездротової мережі. Якщо налаштований алгоритм безпеки WPA/WPA2, слід пропустити цей пункт і перейти до п.16.

16. Створити ESSID в базу даних «pyrit» командою pyrit -e «назва атакованої атаки без лапок» create_essid.

17. Імпортувати в базу даних відсортований словарь, полученний під час виконання п.2 командою pyrit -i «повний шлях до файлу без лапок» import_passwords.

18. Створюємо "райдужні таблиці", використовуючи пакетний (batch) процес, виконавши команду: pyritbatch.

19. Активувати cowpatty для швидкого перебору командою: pyrit - e«назва точки доступу без лапок» -ocow.outexport_cowpatty

20. Запускаємо процес перебору парольних фраз командою cowpatty -dcow.out -sBigPond -rhs/"повний шлях до файлу з handshake'ом".

21. Очікуємо завершення виконання процесу перебору парольних фраз і в результаті отримуємо пароль, за допомогою якого можемо підключатися до бездротової мережі.

## 3.5 Захист мережі за допомоги wpa2-enterprise

Корпоративні мережі із шифруванням WPA2-Enterprise будуються на аутентифікації протоколу 802.1x через RADIUS-сервер. Протокол 802.1x (EAPOL) визначає методи відправлення та прийому запиту даних аутентифікації і зазвичай вбудований в операційні системи та спеціальні програмні пакети та передбачає три ролі в мережі:

Клієнт (supplicant) - клієнтський пристрій, якому потрібний доступ до мережі; сервер аутентифікації (зазвичай RADIUS);

аутентифікатор — роутер/комутатор, який з'єднує багато клієнтських пристроїв із сервером аутентифікації та відключає/підключає клієнтські пристрої.

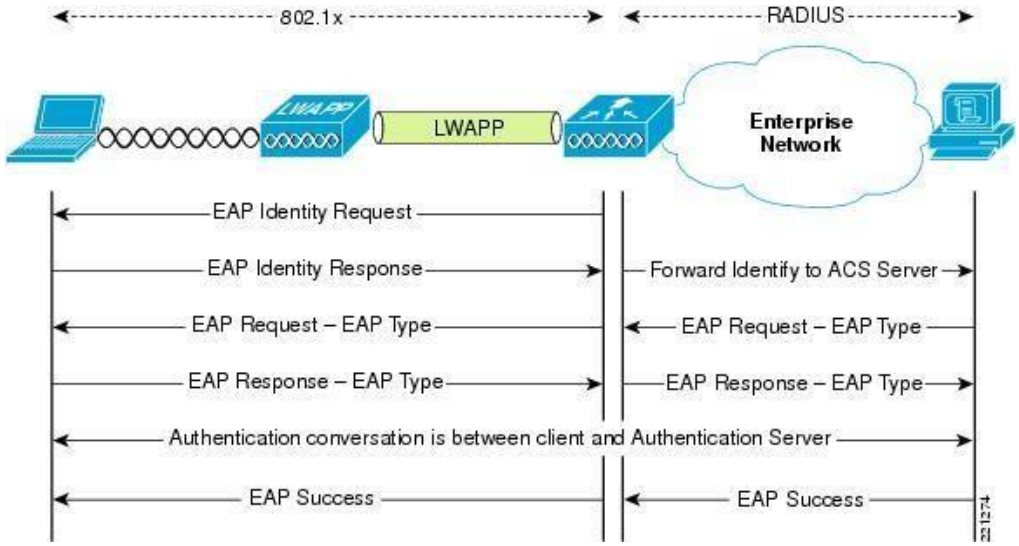


Рисунок 33 – Схема роботи

Є кілька режимів роботи 802.1x, але найпоширеніший і найнадійніший наступний:

Аутентифікатор передає EAP-запит на клієнтський пристрій, як тільки виявляє активне з'єднання.

Клієнт відправляє EAP-відповідь – пакет ідентифікації. Аутентифікатор пересилає цей пакет на сервер аутентифікації (RADIUS).

RADIUS перевіряє пакет і право доступу клієнтського пристрою за базою даних користувача або іншими ознаками, а потім відправляє на автентифікатор роздільну здатність або заборону підключення. Відповідно, автентифікатор дозволяє або забороняє доступ до мережі.

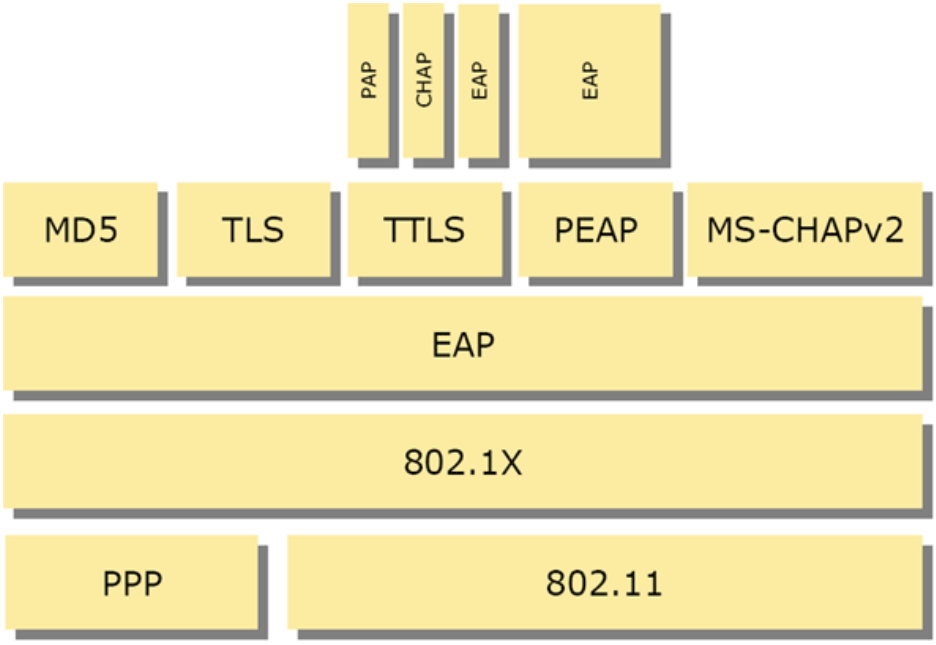


Рисунок 34 – Список використаних протоколів

Використання сервера RADIUS дозволяє відмовитися від PSK та генерувати індивідуальні ключі, валідні тільки для конкретної сесії підключення. Простіше кажучи, ключі шифрування неможливо витягти із клієнтського пристрою. Захист від перехоплення пакетів забезпечується за допомогою шифрування з різних внутрішніх протоколів EAP, кожен з яких має свої особливості. Так, протокол EAP-FAST дозволяє авторизуватися за логіном та паролем, а PEAP-GTC — за спеціальним токеном (карта доступу, картки з одноразовими

паролями, флешки тощо). Протоколи PEAP-MSCHAPv2 та EAP-TLS проводять авторизацію за клієнтськими сертифікатами.

Максимальний захист мережі Wi-Fi забезпечує лише WPA2-Enterprise та цифрові сертифікати безпеки в поєднанні з протоколом EAP-TLS або EAP-TTLS. Сертифікат – це заздалегідь згенеровані файли на сервері RADIUS та клієнтському пристрої. Клієнт та сервер аутентифікації взаємно перевіряють ці файли, тим самим гарантується захист від несанкціонованих підключень з чужих пристроїв та помилкових точок доступу. Протоколи EAP-TTL/TTLS входять до стандарту 802.1X та використовують

для обміну даними між клієнтом та RADIUS інфраструктурою відкритих ключів (PKI). PKI для авторизації використовує секретний ключ (знає користувач) та відкритий ключ (зберігається у сертифікаті, потенційно відомий усім). Поєднання цих ключів забезпечує надійну аутентифікацію.

Цифрові сертифікати слід робити для шкірного бездротового пристрою. Це трудомісткий процес, тому сертифікати зазвичай використовуються лише у Wi-Fi-мережах, що потребують максимальної захисту. У той же час можна легко відкликати сертифікат та заблокувати клієнта.

Сьогодні WPA2-Enterprise в поєднанні із сертифікатами безпеки забезпечує надійний захист корпоративних Wi-Fi мереж. При правильному настроюванні та використанні зламати такий захист практично неможливо "з вулиці", тобто без фізичного доступу до авторизованих клієнтських пристроїв. Тим не менш, адміністратори мереж іноді допускають помилки, які залишають злодійниками "лазівки" для проникнення в мережу. Проблема ускладнюється доступністю софту для зламування та покрокових інструкцій, якими можуть скористатися навіть дилетанти.

# ВИСНОВОК

У цій випускній кваліфікаційній роботі було розглянуто популярні технології для створення бездротових мереж, проведено їх порівняльний аналіз, виявлено та представлено вразливості та недоліки алгоритмів забезпечення безпеки бездротових мереж. Різними способами проведено тестування бездротових мереж щодо перевірки популярних алгоритмів для забезпечення їх безпеки.

У ході виконання роботи було визначено, що забезпечення безпеки бездротової корпоративної або домашньої мережі останнім часом найчастіше ставиться в пріоритетні завдання адміністраторам даного обладнання.

Виявлення уразливостей бездротових комп'ютерних мереж показало, що алгоритм забезпечення безпеки WEP давно скомпрометований і використання його обмеження доступу сторонніх осіб є недоцільним. При використанні алгоритму WEP отримати доступ до мережі можливо за кілька хвилин, якщо активний клієнт, підключений до цієї точки доступу.

З 90-92% безпровідних мереж, що залишилися, використовують алгоритм WPA/WPA2, який вважається криптостійким, але розвиток потужних апаратних засобів для особистого користування дозволяє здійснювати дуже швидкий перебір парольних фраз, а якщо для перебору використовуються райдужні таблиці, то для отримання пароля довжиною 63 символи з ймовірністю близько 75% потрібно кілька хвилин.

У ході розгляду алгоритмів забезпечення безпеки було виявлено, що алгоритм WPA2-Enterprise на сьогодні є найстійкішим проти зловмисників. Цей алгоритм підтримує дво- та більш факторну автентифікацію. Крім пароля для підключення до точки доступу є можливість задавати пару логін та пароль для конкретного

користувача, які будуть використовуватись при автентифікації на сервері Radius. Крім простої пари логін/пароль, можна настроїти Radius сервер таким чином, що потрібно підтвердження, отримане в смс або будь-яким іншим способом. Така аутентифікація дозволяє відкинути більшість зловмисників, тому що складно відстежити процес аутентифікації. Процес стає практично безглуздим.

У ході роботи, провівши аналіз всіх алгоритмів забезпечення безпеки та допоміжного програмного забезпечення, було розроблено рекомендації щодо конфігурування бездротової мережі:

Використання алгоритму забезпечення безпеки WPA2-Enterprise;

Використання Radius сервера, налаштованого на автентифікацію за допомогою пари логін-пароль;

Додаткове впровадження смс-сервісу для підтвердження своєї особи після введення пари логін-пароль на телефон, занесений заздалегідь адміністратором мережі до бази даних, надходити смс з кодом, який можна ввести не частіше, ніж 1 раз на 5 хвилин (підряд триразовий помилковий введення блокує можливість підключення на годину);

Вимкнення точки доступу в неробочу годину, щоб зловмисник не мав багато годин для проведення атак;

Щоденна зміна пароля для автентифікації на точці доступу;

Щоденна зміна пароля для аутентифікації на Radius сервері;

Видача паролів на початку кожного робочого дня в усній формі або демонстрація на моніторі для проходження аутентифікації;

При зміні паролів використовувати програмний генератор паролів, наприклад PasswordSafe.

Список рекомендацій із восьми пунктів зможе убезпечити вашу мережу в рази краще, ніж використання простих алгоритмів забезпечення безпеки, але він накладає деякі незручності та витрати на підприємство. Але ці витрати забезпечують цілісність і захищеність інформації. Особливо варто зазначити, що збитки, які може зазнати

компанія через незахищену мережу, що можуть в рази перевищувати витрати на обслуговування мережі, з урахуванням розроблених рекомендацій.

Під час розробки автоматизованої системи було виявлено досить велику кількість проблем, пов'язаних з керуванням одноплатного комп'ютера, для цього знадобився мобільний пристрій, який виступає як дисплей і клавіатура. Не можу не відзначити, що також за допомогою цього мобільного пристрою здійснювалася передача необхідної інформації між одноплатним та потужним комп'ютерами. Необхідність передачі даних між комп'ютерами звела нанівець недолік у вигляді відсутності клавіатури та монітора у одноплатного комп'ютера. Крім вищесказаного ми досягли меншої помітності через те, що зараз довге використання мобільного пристрою не привертає уваги в суспільстві.

Отже, в результаті проведеної роботи, гіпотеза випускної кваліфікаційної роботи виконана: на основі проведеного аналізу уразливостей бездротових мереж складено рекомендації, що дозволяють забезпечити надійне підключення до такої мережі, без побоювання за крадіжку або зміну інформації, що передається.

# СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

1. Бездротові технології // wikipedia URL: http://ru.wikipedia.org/wiki/Безпровідні технології.

2. IEEE 802.11 // wikipedia URL: https://ua.wikipedia.org/wiki/IEEE_802.11.

3. IEEE 802.11: Wireless LANs // IEEE-SA URL http://standards.ieee.org/about/get/802/802.11.html .

4. IEEE 802.11n // wikipediaURL: https://ua.wikipedia.org/wiki/IEEE_802.11n.

5. Рошан П., «Основи побудови бездротових локальних мереж стандарту 802.11. Практичний посібник з вивчення, розробки та використання бездротових ЛОМ стандарту 802.11» / П.Рошан, Д.Лієрі. - М: CiscoPress Переклад з англійської. Видавничий дім "Вільямс", 2009р.

6. Мауфер Т., "WLAN: практичне керівництво для адміністраторів та професійних користувачів" / Т.Мауфер. - М.: КУДИЦЬ-Образ, 2005р.

7. Хабракен Д., Домашні бездротові мережі/Д.Хабракен – М: НТ-Прес, 2009.

8. WPA // wikipedia URL: https://ua.wikipedia.org/wiki/WPA.

9.WPA2 на захисті бездротових мереж Wi-Fi // Техноріум URL: http://www.technorium.ua/cisco/wireless/wpa2.shtml.

10. Захист у мережах Wi-Fi // Wikipedia URL ua.wikipedia.org/wiki/Захист_в_мережах_Wi-Fi.

11. Колісниченко Д Бездротова мережа вдома та в офісі. - СПб.: БХВ-Петербург, 2009. - 480с.

12. Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи. Підручник - Санкт-Петербург, 2001р.

13. Бездротові технології від останньої милі до останнього дюйма / Немирівський, Бабін, Сартаков, Шорін та ін. – М.: ЕКО-ТРЕНДЗ, 2000.

14. Берлін А.Н. Телекомунікаційні мережі та пристрої: Навчальний посібник / А.М. Берлін - М.: Інтернет-Університет Інформаційних Технологій; БІНОМ. Лабораторія знань, 2008. - 319 с.

15. Гордійчик С.В., Дубровін В.В. Безпека бездротових мереж. - М: Інтуїт, 2007. - 177с.

16. Чому паролі ніколи не були такими слабкими, як зараз // "Хакер" URL: https://xakep.ru/2012/08/21/59192/.

17. Колісніченко, Д.М. Адміністрація Unix-сервера та Linux-станцій / Д.М. Колісніченко. - СПб.: Пітер, 2011. - 400 с.

18. manAirdrop-ng // aircrack-ng.org URL: https://www.aircrack-ng.org/doku.php?id=airdrop-ng.

19. manAireplay-ng // aircrack-ng.org URL: https://www.aircrack-ng.org/doku.php?id=aireplay-ng.

20. manAirmon-ng // aircrack-ng.org URL: http://www.aircrack-ng.org/doku.php?id=airmon-ng&DokuWiki=tf80pkvriakjf6gi3etnpvqab3.

21. manAircrack-ng // aircrack-ng.org URL: https://www.aircrack-ng.org/doku.php?id=aircrack-ng;

22. pyrit (1) A GPGPU-driven WPA/WPA2-PSK key cracker // manpages.org URL: http://manpages.org/pyrit

23. coWPAtty // KALITOOLS URL: http://tools.kali.org/wireless-attacks/cowpatty.

24. OpenSSH Manual Pages - https://www.openssh.com/manual.html.

25. TeamViewer 9 Посібник Віддалене управління // teamviewerURL: https://www.teamviewer.com/ru/res/pdf/TeamViewer9-Manual- RemoteControl-ru.pdf.

26. Kali Linux – Raspberry Pi // Kali Linux Official Documentation URL: http://docs.kali.org/kali-on-arm/install-kali-linux-arm-raspberry-pi.

27. Фленов, М.Є. Linux очима хакера. 4-те вид / М.Є. Фленів. - СПб.: БХВ-Петербург, 2016. - 432 с.

28. Бікманс Ж. LINUXс нуля / Ж. Бікманс, - М: ДМК Прес, 2014. - 428 с.

29. Сергєєв А.М. Основи локальних комп'ютерних мереж. Навчальний посібник/О.М. Сергєєв. - СПб.: Лань, 2016. - 184 с.