ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія тестування безпеки безпроводових мереж за допомогою Kali Linux»

зі спеціальності 125 Кібербезпека та захист інформації
(код, найменування спеціальності)

освітньо-професійної програми Інформаційна та кібернетична безпека
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ілля ГОНЧАРУК
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
ГОНЧАРУК Ілля
(прізвище, ім'я)

Керівник к.т.н., доцент БОРСУКОВСЬКИЙ Юрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
"___" жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гончаруку Іллі Дмитровичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія тестування безпеки безпроводових мереж за допомогою Kali Linux»
керівник кваліфікаційної роботи БОРСУКОВСЬКИЙ Ю.В., **к.т.н., доцент**
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
оперативна система Kali Linux;
вбудовані засоби та інструменти ОС Kali;
експлуатаційна документація безпроводових мереж та стандартів Wi-Fi,
нормативні документи, наукова та технічна література, міжнародні стандарти щодо забезпечення безпеки безпроводових мереж.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми безпеки безпроводових мереж, основних загроз.
2. Методи та засоби забезпечення безпеки Wlan-мереж.
3. Огляд інструментів Kali Linux для тестування безпеки безпроводових мереж.

4. Оформлення рекомендацій щодо покращення безпеки безпроводових мереж на основі отриманих результатів.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми забезпечення безпеки безпроводових мереж.	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури щодо методів забезпечення безпеки безпроводових мереж та методів їх тестування за допомогою ОС Kali.	12.10.2024 р.	
3.	Аналіз інструментів та засобів оперативної системи Kali Linux.	27.10.2024 р.	
4.	Технологія тестування мереж та опис методів захисту від атак.	03.11.2024 р.	
5.	Розроблення рекомендацій щодо покращення безпеки Wi-Fi мереж.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Ілля ГОНЧАРУК
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ГОНЧАРУКА Іллі
на тему: «Технологія тестування безпеки безпроводових мереж за допомогою Kali Linux»

Актуальність даної роботи полягає у вирішенні критичної проблеми сучасних технологій: безпеки бездротових мереж, які є невід'ємною частиною як особистого, так і професійного середовища. Зосереджуючись на тестуванні безпеки Wi-Fi з використанням Kali Linux, кваліфікаційна робота підкреслює важливість розуміння векторів атак та інструментів, доступних для виявлення слабких місць. Це особливо актуально в сьогоднішніх умовах, коли кіберзагрози стають все більш витонченими і поширеними.

Позитивні сторони:

1. На основі проведеного дослідження в роботі встановлено зміст проблеми забезпечення безпеки Wi-Fi мереж.

2. Достатньо успішно викладено матеріали тестування безпеки Wi-Fi мережі на базі ОС Kali Linux.

3. Сформовано рекомендації щодо покращення безпеки бездротової мережі у цілому.

Недоліки:

1. Робота концентрується лише навколо безпеки мережі Wi-Fi.

2. У роботі не представлено схему реалізації використання Kali на підприємствах.

Висновок: враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «добре», а здобувач ГОНЧАРУК Ілля – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач ГОНЧАРУК Ілля до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія тестування безпеки безпроводових мереж за допомогою Kali Linux»
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(ім'я, прізвище) *(підпис)*

Висновок керівника кваліфікаційної роботи

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(ім'я, прізвище)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи містить: 69 сторінок, 31 рисунок, 1 таблиця, 29 джерел.

Об'єкт дослідження – безпека безпроводових мереж та їх стійкість до сучасних атак.

Предмет дослідження – технологія тестування безпеки безпроводових мереж за допомогою операційної системи Kali Linux.

Мета роботи - розробити технологію тестування безпеки безпроводових мереж з використанням Kali Linux для оцінки рівня захищеності та оформити рекомендації щодо удосконалення безпеки на основі отриманих результатів.

Методи дослідження – опрацювання літератури за даною тематикою, перевірка безпеки власної мережі за допомогою інструментів ОС Kali.

Тестування безпеки бездротових мереж надає значні переваги не тільки приватним особам, а й підприємствам та організаціям, забезпечуючи безпеку та надійність їхньої цифрової інфраструктури. Корисним інструментом у цьому процесі є Kali Linux, спеціалізована операційна система, призначена для тестування на проникнення та оцінки мережевої безпеки.

В роботі проаналізовано технологію тестування безпеки безпроводових мереж, визначено її мету та завдання. Проведено аналіз принципів роботи бездротових мереж та загроз, що існують в їх середовищі. Досліджено методи та засоби технології мережевого тестування за допомогою ОС Kali.

На основі досліджень, проведених в роботі, запропоновано порядок застосування технології тестування бездротової мережі для покращення її захисту від потенційних загроз. Розроблено рекомендації щодо застосування технології забезпечення безпеки Wi-Fi.

Галузь використання – може бути використано для захисту кінцевих точок доступу звичайних громадян, кібербезпека інформаційних ресурсів організацій.

БЕЗДРОТОВІ МЕРЕЖІ, WLAN, Wi-Fi, KALI LINUX, ТЕХНОЛОГІЯ ТЕСТУВАННЯ БЕЗПЕКИ БЕЗПРОВОДОВИХ МЕРЕЖ.

ABSTRACT

The text part of the qualification work contains: 69 pages, 31 figures, 1 table, 29 references.

Object of research - ensuring the security of wireless networks and testing their vulnerabilities to modern attacks.

Subject of research - methods and tools for testing the security of wireless networks based on the Kali Linux operating system

The aim of research - to develop a technology for testing the security of Wi-Fi networks using Kali Linux.

Research methods - studying the literature on this topic, checking the security of your own network using Kali OS tools.

Wireless network security testing provides significant benefits not only to individuals but also to businesses and organizations, ensuring the safety and reliability of their digital infrastructure. A useful tool in this process is Kali Linux, a specialized operating system designed for penetration testing and network security assessment.

The paper analyzes the technology of wireless network security testing, defines its purpose and objectives. The principles of wireless networks and the threats that exist in their environment are analyzed. The methods and means of network testing technology using the Kali OS are investigated. The purpose and main functions of Kali Linux are determined.

Based on the research carried out in the work, a procedure for applying wireless network testing technology to improve its protection against potential threats is proposed. Recommendations for the use of Wi-Fi security technology have been developed.

Field of application - can be used to protect the endpoints of ordinary citizens, cybersecurity of information resources of organizations.

WIRELESS NETWORKS, WLAN, Wi-Fi, KALI LINUX, WIRELESS NETWORKS SECURITY TESTING TECHNOLOGY.

Зміст

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES - Advanced Encryption Standard

AP - Access Point

ARM - Advanced RISC (Reduced Instruction Set Computer) Machine

BSS - Basic Service Set

CCMP - Counter Mode Cipher Block Chaining Message Authentication Code Protocol

DS - Distribution System

DoS (DDoS) - Denial of Service (Distributed Denial of Service)

ESS - Extended Service Set

FHSS - Frequency-Hopping Spread Spectrum

IEEE - Institute of Electrical and Electronics Engineers Standard

KRACK - Key Reinstallation Attack

LAN - Local Area Network

LLC - Logical Link Control

MAC - Media Access Control

MIMO, MU-MIMO - Multiple Input, Multiple Output; Multi-User Multiple Input, Multiple Output

MitM - Man-in-the-Middle

OFDM - Orthogonal Frequency-Division Multiplexing

PAN - Personal Area Network

SAE - Simultaneous Authentication of Equals

SSID - Service Set Identifier

TKIP - Temporal Key Integrity Protocol

VPN - Virtual Private Network

WEP -Wired Equivalent Privacy

WiMAX - Worldwide Interoperability for Microwave Access

WMAN - Wireless Metropolitan Area Network

WPA - Wi-Fi Protected Access

WPS - Wi-Fi Protected Setup

WWAN - Wireless Wide Area Network

ВСТУП

Актуальність дослідження. У сучасну цифрову епоху бездротові мережі відіграють вирішальну роль у забезпеченні зв'язку, обміну даними та комунікації в різних секторах - від персональних пристроїв до промислових систем управління. Поширеність бездротових мереж не тільки покращила та спростила людям життя, ставши невід'ємною частиною повсякденної діяльності, вони також стають першочерговими цілями для кібератак. Зловмисники часто використовують вразливості в протоколах безпеки бездротових мереж, отримуючи несанкціонований доступ до конфіденційних даних та порушуючи роботу цілих підприємств. Зростаюча залежність від бездротових технологій у поєднанні з постійною загрозою кібератак робить тему тестування безпеки бездротових мереж надзвичайно актуальною.

Серед доступних інструментів для оцінки та підвищення безпеки бездротових мереж операційна система Kali Linux виділяється завдяки своєму об’ємному набору утиліт, орієнтованих на тестування мережі, таких як Aircrack-ng, Wifite, WireShark тощо. Ці інструменти дозволяють фахівцям з безпеки виявляти слабкі місця в протоколах шифрування, таких як WEP, WPA і WPA2, проводити тести на проникнення і аналізувати вразливості мережі.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять аналіз існуючих типів бездротових мереж та проведення тестування безпеки безпроводової мережі за допомогою Kali Linux.

Об’єкт дослідження – безпека безпроводових мереж та їх стійкість до сучасних атак.

Предмет дослідження – технологія тестування безпеки безпроводових мереж за допомогою операційної системи Kali Linux.

Мета роботи - розробити технологію тестування безпеки безпроводових мереж з використанням Kali Linux для оцінки рівня захищеності.

Методи дослідження – опрацювання літератури за даною тематикою, перевірка безпеки власної мережі за допомогою інструментів ОС Kali.

Наукові завдання:

– дослідити сутність проблеми забезпечення безпечної роботи безпроводових мереж;

– проаналізувати сучасні методи забезпечення безпеки Wi-Fi мереж;

– проаналізувати інструменти ОС Kali Linux щодо тестування безпечності безпроводових мереж;

– реалізувати тестування на проникнення бездротової мережі;

– розробити рекомендації щодо покращення безпеки бездротової мережі на основі отриманих результатів.

Практичне значення одержаних результатів: запропоновано порядок застосування технології тестування безпеки безпроводової мережі, також розроблено рекомендації щодо її реалізації та покращення безпеки Wi-Fi в цілому.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БЕЗПРОВОДОВИХ МЕРЕЖ

1.1. Дослідження принципів роботи та стандартів безпроводових мереж

Бездротові мережі відіграють ключову роль у тому, як сучасний світ контактує та обмінюється інформацією сьогодні. На відміну від дротових мереж, Wi-Fi мережі використовують радіохвилі для передачі даних, що робить їх більш зручними та гнучкими, але водночас наражає їх на унікальні виклики, особливо з точки зору безпеки. Щоб зрозуміти ці виклики і працювати над покращенням безпеки бездротових мереж, важливо спочатку вивчити стандарти і принципи, які визначають, як ці мережі функціонують.

Загалом, бездротові мережі дозволяють мобільним та стаціонарним пристроям, оснащеними мережевою картою, підключатися до глобальної мережі інтернет і комунікувати між собою без необхідності використання фізичних кабелів. Наприклад, Wi-Fi мережа працює за допомогою радіохвиль для передачі даних між пристроями та бездротовою точкою доступу, яка є пристроєм, що підключається до Інтернету і виконує роль концентратора бездротової мережі. Бездротові мережі можна класифікувати на чотири конкретні групи відповідно до області застосування та діапазону сигналу:

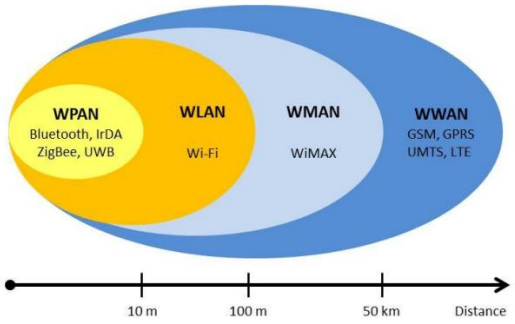

Рис. 1.1. Класифікація бездротових мереж [1]

Крім того, бездротові мережі також можна розділити на два великі сегменти: ближнього та дальнього радіусу дії. Бездротова мережа малого радіусу дії відноситься до мереж, які працюють в обмеженому радіусі. Це стосується локальних мереж (LAN), таких як корпоративні будівлі, школи та університети, виробничі підприємства або житлові будинки, а також до персональних мереж (PAN), де портативним пристроям, що знаходяться в безпосередній близькості, потрібно обмінюватися даними. Ці мережі зазвичай працюють в неліцензованому спектрі, зарезервованому для промислового, наукового та медичного використання [2]. Найпоширенішими є частотні діапазони 2,4 ГГц і 5 ГГц, які доступні на більшій частині земної кулі. Відсутність необхідності ліцензування сприяло поширенню мереж WLAN та WPAN [3].

У мережах далекого радіусу дії зв'язок, як правило, надається компаніями, які продають бездротовий зв'язок як послугу. Ці мережі охоплюють великі території, такі як мегаполіс (WMAN), область або цілу країну. Метою мереж великого радіусу дії - забезпечити бездротове покриття в усьому світі. Найпоширенішою мережею дальнього радіусу дії є бездротова глобальна мережа. Найбільше до глобального покриття наблизились супутникові мережі.

Бездротові глобальні мережі (WWAN) - забезпечують бездротовий зв'язок на великих географічних територіях, таких як міста, регіони або навіть цілі країни. Вони використовують такі технології як LTE, 5G і супутниковий зв'язок, щоб забезпечити доступ до інтернету для мобільних пристроїв, транспортних засобів і віддалених місць. Зона покриття в стільниковій системі поділяється на області, кожна з яких обслуговується передавачем, розташованим в її центрі. Кожна така область називається сотою. Передавач обслуговує свою область, забезпечуючи зв'язок для пристроїв у ній. Всі передавачі з'єднані з базовою станцією, а остання - з мобільним телекомунікаційним комутатором, який з'єднує стільникову та дротову телефонну мережу. Оператори мобільного зв'язку часто використовують глобальні мережі для забезпечення покриття для смартфонів, планшетів та пристроїв Інтернету речей [4].

Бездротовий зв'язок можна також надавати через супутник. Завдяки великій висоті над рівнем моря висоті, супутникові передачі можуть покривати велику площу над поверхнею землі. Це може бути дуже корисно для користувачів, які знаходяться у віддалених районах або на островах, де немає підводних кабелів.

Бездротові міські мережі (WMAN) забезпечують бездротове з'єднання в межах міста або мегаполісу. Мережі WMAN базуються на стандарті IEEE 802.16, який часто називають WiMAX (Worldwide Interoperability for Microwave Access). WiMAX схожий на Wi-Fi, але забезпечує покриття на більші відстані. WiMAX працює у двох частотних діапазонах (2-11 ГГц і 10-66 ГГц), що включає як ліцензовані, так і неліцензовані частоти [3].

WiMAX може забезпечити передачу даних до 70 Мбіт/с на відстані до 50 км, обслуговуючи тисячі користувачів з однієї базової станції. Завдяки можливості роботи на двох частотних діапазонах, WiMAX може функціонувати як у зоні прямої видимості, так і поза нею. Наприклад, в діапазоні 2-11 ГГц, він може працювати за межами прямої видимості, коли комп'ютер всередині будівлі зв'язується з вежею/антеною зовні. Короткочастотний діапазон сприяє передачі даних через фізичні перешкоди, тоді як високочастотний використовуються для зв'язку в межах прямої видимості, дозволяючи вежам і антенам взаємодіяти на більших відстанях.

Бездротові персональні мережі (WPAN) базуються на стандарті IEEE 802.15 і призначені для зв'язку на невеликих відстанях, як правило, в межах кількох метрів. Вони використовують такі технології, як Bluetooth, Zigbee та інфрачервоний (ІЧ) зв'язок для підключення таких пристроїв, як смартфони, переносні та периферійні пристрої (наприклад, клавіатура або навушники) [5]. WPAN-мережі зазвичай використовуються для особистих потреб, наприклад, для підключення пристроїв «розумного будинку» або обміну файлами між пристроями.

Бездротові локальні мережі (WLAN) - з'єднують пристрої в межах обмеженої географічної зони, наприклад, будинку, офісу або кампусу, за допомогою технології Wi-Fi (на основі стандартів IEEE 802.11). WLAN зазвичай складаються з точок доступу (AP), які транслюють бездротові сигнали і з'єднують такі пристрої, як ноутбуки, смартфони та принтери, з локальною мережею та Інтернетом [6].

WLAN широко використовуються завдяки простоті налаштування, масштабованості та економічній ефективності. Однак їхній радіус дії обмежений, і вони вразливі до загроз безпеці, якщо не налаштовані належним чином.

Таблиця 1.1

Специфікація типів бездротових мереж

	WWAN	WMAN	WLAN	WPAN
Зона покриття	Від 50 км	В межах міста (50 кілометрів)	100-300 метрів	від 1 до 10 метрів
Стандарти	AMPS, GSM, GPRS, UMTS, HSDPA, LTE, супутниковий DVB-S2	IEEE 802.16 (WiMAX)	IEEE 802.11 (Wi-Fi: 802.11a/b/g/n/ac/ax/be)	IEEE 802.15 (Bluetooth, Zigbee, ІЧ
Швидкість	LTE: 10–100 Мбіт/с; 5G: 1–10 Гбіт/с	30 Мбіт/с –1 Гбіт/с	Wi-Fi 5 (802.11ac): 433 Мбіт/с –6.9 Гбіт/с; Wi-Fi 6 (802.11ax): 1.2–9.6 Гбіт/с	Bluetooth 5.0: до 2 Мбіт/с; Zigbee: до 250 Кбіт/с
Діапазон частот	Стільникові діапазони: 700 МГц–2,6 ГГц, 24–100 ГГц	2-11 ГГц та10-66 ГГц	2,4 ГГц, 5 ГГц, 6 ГГц (Wi-Fi 6E та Wi-Fi 7)	Bluetooth: 2,4 ГГц; Zigbee: 868 -2,4 ГГц; ІЧ: видимий спектр
Засоби безпеки	Шифрування LTE, IPsec, аутентифікація на основі SIM-карти	Шифрування WPA2/WPA, VPN	Шифрування WPA/WPA2/WPA3	Bluetooth (SAFER+, AES-CCM), Zigbee AES-128

Незважаючи на широкий спектр застосовуваних технологій, різні призначення та стандарти, бездротові мережі впевнено зайняли свою нішу в світі технологій і з кожним роком набувають все більшої популярності. Бездротові мережі мають низку переваг в порівнянні з дротовими, зокрема:

Переваги:

Ефективність - покращена передача даних забезпечує швидший обмін інформацією всередині компаній та між партнерами та клієнтами.

Мобільність - відсутність дротів дозволяє змінювати місцезнаходження без втрати з'єднання.

Гнучкість - співробітники, які працюють у бездротових мережах, можуть працювати не лише з фіксованих комп'ютерів, але й залишатися продуктивними за межами офісу.

Економія - відсутність кабелів знижує витрати завдяки дешевизні бездротових маршрутизаторів і відсутності необхідності в прокладанні кабелів.

Адаптивність - швидка і проста інтеграція пристроїв у мережу, висока гнучкість при модифікації установки.

Недоліки:

Безпека - безпровідна передача даних більш уразлива до атак з боку несанкціонованих користувачів.

Середовище існування - перешкоди від інших бездротових технологій або радіосигналів можуть спричинити поганий зв'язок або втрату з'єднання.

Швидкість - безпровідна передача повільніша і має більші затримки порівняно з дротовими мережами.

Масштабованість – зі зростанням кількості пристроїв росте і необхідність збільшувати кількість точок доступу, оскільки підключення великої кількості пристроїв до однієї AP веде до падіння її продуктивності.

Підсумовуючи, можна сказати, що різноманітні типи бездротових мереж — WWAN, WLAN, WPAN і WMAN — служать широкому діапазону цілей, від зв’язку з персональним пристроєм до створення мережі по всьому місту. Незважаючи на різні зони покриття, швидкості та технології (Таб.1), усі бездротові мережі стикаються з загальними проблемами безпеки. В даній роботі увага буде приділена тестуванню безпеки WLAN, а конкретно способу її реалізації – Wi-Fi. Основною причиною є, насамперед, широке поширення пристроїв Wi-Fi, їх доступність, можливість неліцензійного використання (кожен пристрій використовує частоту 2,4

– 5 ГГц без необхідності отримувати дозвіл) і, як наслідок, великий інтерес від зловмисників і варіативність реалізацій їх атак.

За прогнозами International Data Corporation (IDC), до 2025 року у світі буде налічуватися приблизно 55,7 мільярдів пристроїв, 75% з яких складатимуть IoT-пристрої, підключені до інтернету. Також IDC зазначає, що обсяг даних, які генеруватимуть ці пристрої, досягне 73,1 зетабайтів у 2025 році, що значно більше, ніж 18,3 зетабайтів у 2019 році [7].

Однак такі пристрої можуть бути вразливими до атак зловмисників, які здатні використовувати недоліки та уразливості в системах захисту, зокрема в протоколах безпеки, таких як WEP або WPA, які мають кілька версій. Зафіксовано зростання частки атак на комп'ютери, сервери та мережеве обладнання: якщо у першому кварталі 2021 року цей показник складав 71%, то у другому кварталі він досяг 87% [8]. Подібні загрози можуть спричинити серйозні наслідки, такі як втрати зв’язку між пристроями, витоки конфіденційної інформації, захоплення управління точкою доступу та інші проблеми.

1.2. Аналіз стандарту безпроводового підключення IEEE 802.11

Технологія Wi-Fi (Wireless Fidelity) є реалізацією бездротового підключення LAN для комунікації різних пристроїв, що належить до набору стандартів IEEE 802.11 [3]. Wi-Fi використовує радіохвилі (так само, як Bluetooth і стільникові мережі) для комунікації пристроїв у малому масштабі, наприклад, у будинках, торгових центрах, на площах тощо. Wi-Fi - це найдешевший і найшвидший спосіб передавання даних на короткі відстані, включно з переглядом веб-сторінок, онлайн-іграми, відеостримінгом тощо. У 2019 році кількість поставлених Wi-Fi пристроїв перевищила 310 млн [9].

IEEE 802.11 — набір стандартів для комунікації в бездротовій локальній мережевій зоні частотних діапазонів 2.4 (2412-2472) і 5 (5160-5185) ГГц. Стандарт IEEE 802.11 визначає на канальному рівні специфікації для фізичного рівня і рівня

керування доступом до середовища передачі даних (MAC), які взаємодіють з рівнем керування логічним зв'язком (LLC), як зображено на рисунку 1.3.

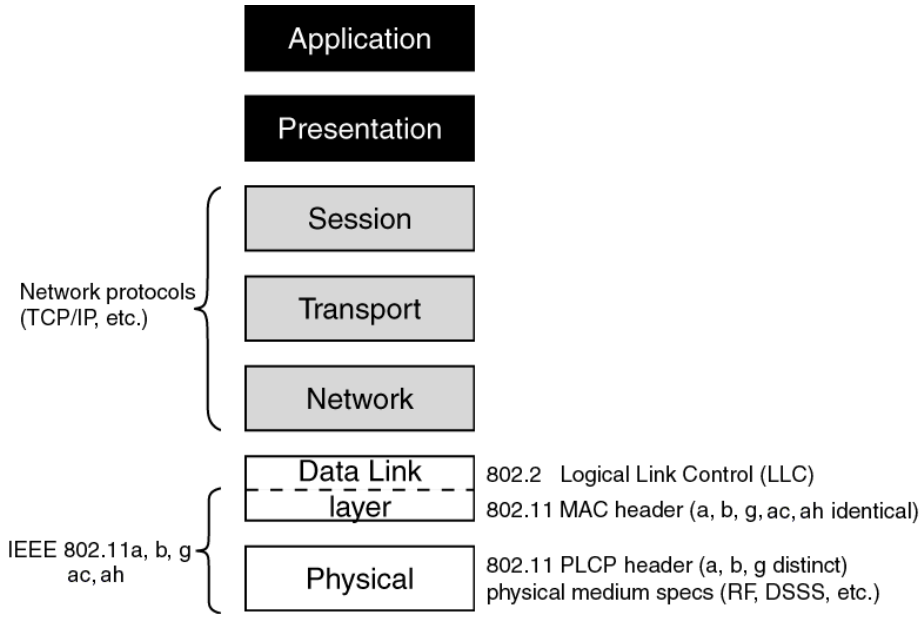

Рис. 1.2. Стандарт 802.11 в еталонній моделі OSI [10]

Всі компоненти в архітектурі 802.11 належать або до канального (Data Link Layer) або до фізичного рівня (Physical Layer). На канальному рівні стандарт займає два підрівні: підрівень логічного зв'язку LLC (Logical Link Control) і підрівень управління доступом до каналу (середовища) MAC (Medium Access Control). На фізичному рівні та рівні управління доступом до носія він визначає їхні специфікації, які взаємодіють з рівнем управління логічним зв'язком [3].

Підрівень MAC відповідає за розподіл спільного радіоканалу між користувачами, за виявлення (повторну передачу) помилково прийнятих пакетів даних. На MAC-рівні визначено принцип, за яким пристрої використовують (ділять) спільний канал, механізм аутентифікації користувача, механізм шифрування даних.

Згідно з Рис. 1.2, на фізичному рівні стандарт 802.11 визначає низку схем кодування і передавання для організації бездротового зв'язку, найпоширенішими є метод передавання за допомогою інфрачервоного випромінювання, метод стрибкоподібного (псевдовипадкового, перескоку) перебудови частоти (Frequency Hopping Spread Spectrum - FHSS), метод розширення спектра прямої послідовності

(Direct Sequence Spread Spectrum - DSSS) і метод ортогонального частотного мультиплексування (Orthogonal Frequency Division Multiplexing - OFDM).

Швидкість передачі даних у початковому стандарті IEEE 802.11 складає 2 Мбіт/с, працював в діапазоні частот від 2.4 до 2.5 ГГц. Усі пристрої в мережі WLAN мають відповідати однаковим специфікаціям 802.11 - пристрій із найстарішим набором поправок 802.11 буде найслабшою ланкою бездротової мережі. На даний момент існує більше 15 поколінь стандарту Wi-Fi, такі як [11]:

802.11a Введений у 1999 році, 802.11a працює в частотному діапазоні 5 ГГц, забезпечуючи максимальну теоретичну швидкість до 54 Мбіт/с. Використання вищої частоти 5 ГГц знижує перешкоди від пристроїв, що працюють у завантаженому діапазоні 2.4 ГГц. Однак його радіус дії відносно обмежений — приблизно 35 метрів у приміщенні і до 120 метрів на відкритому просторі. Цей стандарт впровадив ортогональне частотне мультиплексування (OFDM), яке покращило ефективність передачі даних і стало основою для майбутніх стандартів.

802.11b Також введений у 1999 році, 802.11b працює в діапазоні 2.4 ГГц, забезпечуючи максимальну швидкість 11 Мбіт/с. Хоча він повільніший за 802.11a, його популярність була вища завдяки більшій дальності дії (приблизно 40 метрів у приміщенні і 140 метрів на відкритому просторі) і сумісності з існуючими пристроями.

802.11g Випущений у 2003 році, 802.11g об'єднав найкращі характеристики 802.11a та 802.11b. Він працював у діапазоні 2.4 ГГц, як і 802.11b, але досягав швидкостей до 54 Мбіт/с завдяки використанню OFDM.

802.11n Введений у 2009 році, 802.11n став значним кроком вперед. Він працює у діапазонах 2.4 ГГц і 5 ГГц, досягаючи швидкостей до 600 Мбіт/с завдяки технології Multiple Input, Multiple Output (MIMO). MIMO дозволяє використовувати декілька антен для одночасної передачі і прийому даних, покращуючи швидкість і дальність дії. Цей стандарт став основою для сучасних Wi-Fi мереж.

802.11ac Випущений у 2013 році, 802.11ac, часто називається Wi-Fi 5. Працюючи виключно в діапазоні 5 ГГц, він підтримує швидкості до 6.9 Гбіт/с завдяки впровадженню Multi-User MIMO (MU-MIMO) і ширших каналів (до 160

МГц). Він також покращив модуляцію сигналу за допомогою 256-QAM, що значно підвищило ефективність передачі даних.

802.11ax Введений у 2019 році як Wi-Fi 6, 802.11ax працює у діапазонах 2.4 ГГц і 5 ГГц (а також у діапазоні 6 ГГц з Wi-Fi 6E). Він пропонує теоретичні швидкості до 9.6 Гбіт/с, зосереджуючись не тільки на швидкості, але й на ефективності у густонаселених середовищах.

802.11be Очікується, що цей стандарт з'явиться близько 2024 року під назвою Wi-Fi 7. Він буде використовувати діапазони 2.4 ГГц, 5 ГГц і 6 ГГц, обіцяючи швидкості до 46 Гбіт/с. Він впровадить ширину каналу 320 МГц, 4096-QAM та покращену технологію MIMO, забезпечуючи наднизьку затримку і високу продуктивність.

Архітектура 802.11 складається з кількох ключових компонентів, кожен з яких виконує свою роль у забезпеченні бездротового зв'язку:

Станція (STA) - це пристрій, який має можливість підключатися до бездротової мережі. Це може бути комп'ютер, ноутбук, телефон або інший пристрій з підтримкою Wi-Fi.

Точка бездротового доступу (AP) - іноді також називається базовою станцією (BS). Цей пристрій дозволяє станціям підключатися до дротової мережі, використовуючи стандарти Wi-Fi. AP функціонує як міст між бездротовими пристроями і дротовою мережею [6].

Способи організації бездротового підключення в Wi-Fi мережах різноманітні: з однією AP, з кількома точками доступу або без AP. Розглянемо особливості цих конфігурацій мереж.

Базовий набір послуг (BSS) - складається з точки доступу і всіх підключених до неї станцій (Рис.1.3). Точка доступу керує всіма станціями в межах цього BSS. Найпростіше схема такої топології включає одну точку доступу і одну станцію.

Кожна BSS має строкове ім'я, яке оголошується точкою доступу. Цей ідентифікатор називається ідентифікатором набору послуг (Service Set Identifier, SSID). SSID це символьна назва бездротової точки доступу, яка служить для ідентифікації її серед інших точок користувачами або пристроями, що

підключаються до мережі. SSID є рядком розміром до 32 байт, який передається широкомовно в ефір. Розташовані поруч із мережею пристрої приймають назву і якщо їм дозволено приєднатися до точки доступу, то з'єднуються з нею. SSID інколи називають «назвою мережі».

Але є ще один ідентифікатор, який використовується пристроями і повинен бути унікальним, оскільки він однозначно ідентифікує точку доступу. Це MAC-адреса точки доступу, яка називається BSSID (BSS ID).

У топології BSS точка доступу відіграє ключову роль. Щоб пристрій міг стати клієнтом цієї мережі, він спершу має отримати «дозвіл» від точки доступу. Для цього клієнт надсилає запит на підключення (асоціацію), а точка доступу або приймає його, або відхиляє. Якщо запит прийнятий, клієнт може користуватися мережею. Інакше – підключення неможливе.

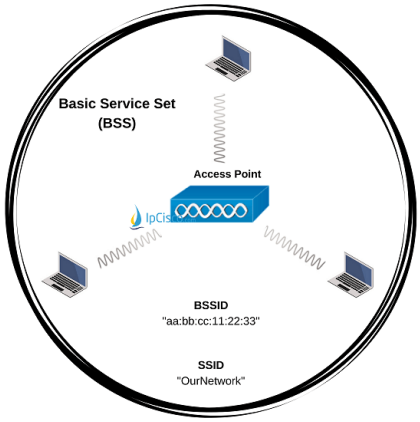

Рис. 1.3. Топологія BSS

Усередині BSS всі дані передаються через точку доступу. Це дозволяє централізовано контролювати трафік (Рис.1.3.) і забезпечує певний рівень безпеки. Однак, оскільки сигнали передаються через повітря, без додаткового шифрування вони залишаються вразливими. Саме тому використовуються різні методи захисту, типу вбудованих стандартів шифрування.

Клієнти в одній BSS можуть обмінюватися даними між собою. Для зв’язку з мережами поза зоною BSS використовується точка доступу, що підключена до DS.

Зазвичай, DS це Ethernet-з’єднання, що створює міст між клієнтами BSS і іншими мережами. Такий механізм інтеграції називається системою розподілу (Distribution System, DS), згідно зі стандартом 802.11.

Якщо площа мережі значно перевищує можливості однієї точки доступу, як це часто буває у великих компаніях, додаються додаткові AP. Ці точки підключаються через Ethernet-комутатор і створюють єдину мережу. З точки зору користувача, це виглядає як безперервне підключення: можна вільно переміщатися між зонами покриття без розриву з’єднання. Така мережа, що об’єднує кілька точок доступу, називається *розширеним набором послуг* (Extended Service Set, ESS).

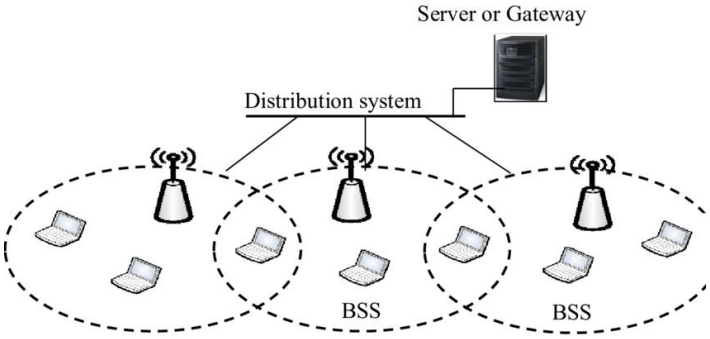

Рис. 1.4. Структурна схема ESS [6]

Для забезпечення стабільності всі точки доступу в ESS повинні мати однаковий SSID. При цьому BSSID (унікальний ідентифікатор кожної точки доступу) буде різним. Коли користувач переходить із зони покриття однієї точки доступу до іншої, це називається роумінгом. Його принцип схожий на роумінг у мобільних мережах. Клієнт автоматично шукає нову точку доступу і підключається до неї, якщо така є в зоні досяжності.

Незалежний базовий набір послуг (IBSS) або ad-hoc - це спеціальна мережа, що складається виключно з мобільних станцій без точки доступу.

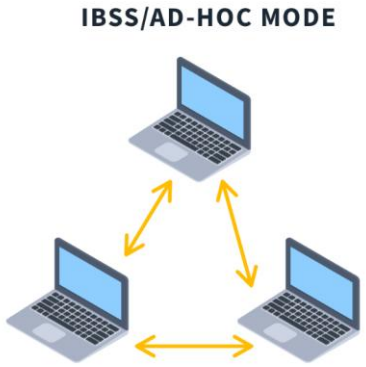

Рис. 1.5. Топологія ad-hoc [12]

В режимі ad-hoc станції комунікують лише між собою, без потреби в точці доступу. Режим ad-hoc найкраще підходить для невеликої групи пристроїв, і всі ці пристрої повинні бути фізично присутніми в безпосередній близькості один від одного. При цьому станції в цьому режимі не будуть мати доступу до глобальної мережі інтернет без встановлення спеціальних шлюзів. Проте Ad hoc є чудовим варіантом для створення бездротових мереж у невеликих середовищах, забезпечуючи простий і економічний спосіб організації зв'язку.

Незалежно від покоління чи типу підключення, стандарт є вразливим до кібератак або інших незаконних дій. Важливість забезпечення його безпеки гостро повстала з огляду на стрімке поширення технології Wi-Fi у світі. Задля забезпечення конфіденційності переданих повідомлень застосовують методи шифрування, що розглянуті у наступному розділі.

1.3. Технології та методи захисту Wi-Fi

Бездротові мережі зазвичай менш безпечні, ніж дротові. Дротові мережі передають дані між двома точками, A та B, які з'єднані кабелем. Бездротові мережі, натомість, передають дані в усі сторони, охоплюючи всі пристрої в межах досяжності. Дротова мережа може бути захищена обмеженням фізичного доступу та встановленням міжмережевих екранів. Але з такими самими заходами безпеки

бездротові мережі будуть залишатися вразливими, тому для забезпечення безпеки бездротових мереж потрібні більш цілеспрямовані зусилля.

Захист бездротових мереж створює послідовні «фронти» оборони за допомогою комбінації шифрування, автентифікації, контролю доступу, захисту пристроїв та виявлення вторгнень, щоб запобігти незаконному доступу та забезпечити безпеку мережі. Процес починається з активації методів шифрування мережі, таких як WPA або WPA2, для шифрування передачі даних. Це робить дані нерозбірливими для неавторизованих сторін, навіть якщо вони будуть перехоплені.

Користувачі або пристрої, які бажають підключитися до мережі, повинні підтвердити свою особу, зазвичай через введення пароля. Правила контролю доступу визначають, які користувачі або пристрої мають доступ до мережі і на якому рівні, залежно від ролі користувача, типу пристрою та явних прав доступу.

Процес продовжується забезпеченням захисту мережевих пристроїв за допомогою підтримки антивірусного програмного забезпечення, оновлення операційних систем та обмеження використання адміністраторських облікових записів для запобігання несанкціонованому доступу. Інтегровані системи виявлення та запобігання вторгненням (IDPS) та інші інструменти відстежують мережу на наявність незвичайної активності або порушень безпеки. Ці системи виявляють і реагують на спроби несанкціонованого доступу, зараження шкідливим програмним забезпеченням та інші загрози в режимі реального часу.

Як зазначено вище, перша лінія оборони починається з протоколів безпеки бездротової мережі. З кінця 1990-х років алгоритми безпеки Wi-Fi зазнали численних оновлень, що включали повну відмову від старих алгоритмів та суттєву ревізію новіших алгоритмів. WEP, WPA, WPA2 і найновіший WPA3 - це чотири типи протоколів безпеки бездротових мереж, кожен з яких забезпечує дедалі вищий рівень захисту [13]. WPA3, незважаючи на покращене шифрування та додаткові функції безпеки, все ще не так поширений як WPA2 через свою новизну. У хронологічному порядку вони розміщуються:

- WEP (Wired Equivalent Privacy) – 1997 р.;
- WPA (Wi-Fi Protected Access) – 2003 р.;

- WPA2 (Wi-Fi Protected Access, версія 2) – 2004 р.;
- WPA3 (Wi-Fi Protected Access, версія 3) – 2018 р.

WEP був затверджений як стандарт безпеки Wi-Fi у вересні 1999 року. Перші версії WEP були не дуже надійними навіть для свого часу, через обмеження США на експорт криптографічних технологій, що змусило виробників обмежити свої пристрої 40-бітним шифруванням RC4. Коли ці обмеження були зняті, шифрування збільшили до 104 біт [14].

Попри покращення алгоритму та збільшення розміру ключа, з часом в WEP виявили численні недоліки безпеки, і через зростання обчислювальних потужностей персональних комп’ютерів, зловмисникам стало легше їх експлуатувати. Вже в 2001 році з'явилися експлойти, що демонстрували можливість зламу, а в 2005 році ФБР провело публічну демонстрацію, зламавши WEP-паролі за кілька хвилин за допомогою доступного програмного забезпечення.

Незважаючи на різні вдосконалення та спроби зміцнити WEP, цей стандарт залишився дуже вразливим. Системи, які використовують WEP, повинні бути оновлені або замінені, якщо оновлення безпеки неможливе. Wi-Fi Alliance офіційно припинив обслуговування WEP у 2004 році.

Для вирішення вразливостей WEP торгова група Wi-Fi Alliance розробила WPA на початку 2003 року. Найпоширенішою конфігурацією WPA є WPA-PSK (Pre-Shared Key). Ключі WPA мають довжину 256 біт, що значно більше порівняно з 64- та 128-бітними ключами, які використовувались у WEP.

Однією з важливих змін, які були впроваджені в WPA, є перевірка цілісності повідомлень. Це дозволяє визначити, чи були пакети, що передаються між точкою доступу і клієнтом, перехоплені або змінені зловмисником. Ще однією значною зміною стало впровадження протоколу цілісності тимчасового ключа (TKIP), який використовує систему ключів для кожного пакета, що є набагато безпечнішим у порівнянні з фіксованим ключем, який використовувався у WEP. Пізніше TKIP був замінений на вдосконалений стандарт шифрування (AES) [14].

Попри значні покращення WPA порівняно з WEP, деякі вразливості залишилися. TKIP, основний компонент WPA, був створений таким чином, щоб

його можна було легко впровадити на існуючі пристрої з підтримкою WEP за допомогою оновлення прошивки. В результаті TKIP використовував деякі елементи, які також були вразливими у WEP.

Запроваджений як тимчасовий захід для усунення недоліків WEP, WPA мав на меті лише забезпечити тимчасове покращення шифрування та автентифікації, зберігаючи при цьому сумісність з існуючим обладнанням. Він покладався на протокол тимчасової цілісності ключа (TKIP), який сам по собі не був повноцінним алгоритмом шифрування, а лише обхідним шляхом, розробленим для застарілих систем .

З часом дослідники виявили вразливості в WPA, зокрема атаки типу Beck-Tews та Ohigashi-Morii [15], які могли розшифровувати частини даних за певних умов. Крім того, механізм перевірки цілісності, заснований на TKIP-MIC, і слабкі місця в таких функціях, як Wi-Fi Protected Setup (WPS) – спрощений метод налаштування мережі, зробили WPA неспроможним протистояти протистоянню новим загрозам. В результаті WPA був замінений на WPA2, який запровадив вдосконалений стандарт шифрування (AES) для посилення безпеки та усунув залежність від TKIP [16].

Однією з найбільш значних змін між WPA та WPA2 стало обов'язкове використання алгоритму AES та введення CCMP – базований на алгоритмі шифрування AES покращений протокол блокового кодування, що прийшов на заміну TKIP, який все ще зберігався у WPA2 як резервна система, а також для сумісності з WPA. На жаль, та ж сама вразливість, яка є найбільшою дірою в броні WPA, а саме вектор атаки через Wi-Fi Protected Setup (WPS), залишається і в сучасних точках доступу з підтримкою WPA2. Хоча проникнення в мережу, захищену WPA/WPA2 з використанням цієї вразливості вимагає від 2 до 14 годин безперервних зусиль на сучасному комп'ютері, це все ще є вірогідною проблемою безпеки. Методи ліквідації цього вектору атаки будуть описані в наступному розділі.

Стандарт WPA3, представлений Wi-Fi Alliance у 2018 році, був створений для усунення зростаючих вразливостей його попередника, WPA2. Розробка WPA3 була

зумовлена необхідністю посилити захист від сучасних загроз, таких як атаки грубої сили, атаки за допомогою райдужних таблиць [17] та атаки на переустановлення ключів (KRACK), які значно послаблювали WPA2. Він також мав на меті задовольнити зростаючий попит на надійний захист бездротових мереж в персональних, корпоративних та IoT-середовищах. Ключові особливості WPA3:

1. WPA3 представив одночасну автентифікацію рівних (SAE), яка замінила систему попередньо наданого ключа (PSK) в WPA2. SAE захищає мережі навіть тоді, коли користувачі обирають слабкі паролі, оскільки вона зменшує кількість спроб перебору, обмежуючи їх кількість [18].

2. WPA3-Enterprise підтримує 192-бітове шифрування, що забезпечує більшу стійкість для чутливих додатків, таких як урядові або фінансові мережі. Для звичайних користувачів в основному застосовується 128-бітове шифрування.

3. Додана підтримка PMF (Protected Management Frames) – використовується для контролю цілісності трафіка, забезпечує управління одноадресною та багатоадресною передачею і підвищує безпеку, захищаючи кадри управління бездротовою мережею, що заважає здійснити атаку на деаутентифікацію (коли зловмисник насильно від’єднує користувача від точки доступу).

Незважаючи на переваги WPA3, повномасштабне його розгортання ще не відбулося, що свідчить про повільний перехід від старих протоколів безпеки до цього сучасного стандарту. Однією з основних проблем є сумісність, адже багато застарілих пристроїв не можуть підтримувати WPA3. Це змушує мережі працювати в «перехідному режимі», який зберігає сумісність з WPA2, але створює додаткові вразливості.

Крім того, вартість модернізації обладнання для підтримки WPA3 часто є занадто високою для підприємств і споживачів, що стримує широке впровадження цього стандарту. Обмежена обізнаність багатьох користувачів і організацій про переваги WPA3 також сприяє продовженню використання WPA2.

Загальний рейтинг від найкращого до найгіршого серед сучасних методів захисту WiFi, доступних на сучасних (після 2006 року) роутерах:

– WPA3 + AES-CCMP;
– WPA2 + AES;
– WPA + AES;
– WPA + TKIP/AES (TKIP використовується як запасний метод);
– WPA + TKIP;
– WEP;
– відкрита мережа (взагалі без захисту).

Найкращий спосіб - вимкнути Wi-Fi Protected Setup (WPS) і налаштувати роутер на WPA3 + AES-CCMP/AES-GCMP. Чим нижче за списком, тим менше захисту отримує мережа [19].

Технологічні заходи, такі як WPA2 і WPA3, забезпечують необхідні рівні захисту бездротових мереж, але вони не можуть гарантувати повну безпеку. Мережі є складними системами, на які впливають як людські, так і технічні фактори, і зловмисники часто використовують вразливості, що виходять за рамки цих протоколів. Наприклад, людські помилки, такі як погане управління паролями або нездатність оновити прошивку, можуть зробити вразливими навіть найсучасніші системи. Аналогічно, атаки соціальної інженерії, такі як фішинг, націлені безпосередньо на користувачів, а не на технічну інфраструктуру, повністю оминаючи технології безпеки.

Крім того, деякі вразливості виникають через еволюцію кіберзагроз. Наприклад, розробка складних інструментів для зламу шифрування або використання недоліків у реалізації протоколів підкреслює, що жоден захід безпеки не є невразливим.

Зменшити ризик, що оминає технології безпеки можна за допомогою впровадження в мережу чотирьох додаткових засобів захисту: активних, пасивних, превентивних та комбінованих. Активні засоби керують трафіком, пасивні - виявляють загрози, превентивні - сканують слабкі місця, а комбіновані UTM-системи поєднують кілька видів безпеки для забезпечення повного захисту.

Активні засоби функціонують подібно до своїх дротових аналогів, але призначені для бездротових середовищ. До них відносяться брандмауери,

антивіруси і пристрої фільтрації контенту. Брандмауери фільтрують вхідний і вихідний бездротовий трафік, запобігають небажаному доступу і виявляють шкідливі пакети. Антивірусні сканери безперервно перевіряють бездротові з'єднання на наявність шкідливого програмного забезпечення. Пристрої фільтрації контенту обмежують доступ до певних веб-сайтів або контенту, забезпечуючи при цьому дотримання правил безпеки.

Пасивні засоби, такі як пристрої виявлення вторгнень, підвищують безпеку бездротової мережі, відстежуючи мережевий трафік на предмет підозрілої активності. Вони досліджують тенденції та аномалії даних, щоб виявити потенційні небезпеки, такі як спроби несанкціонованого доступу або передачу шкідливого програмного забезпечення. Виявляючи такі випадки та повідомляючи про них, ці пристрої надають важливу інформацію, яка дозволяє мережевим менеджерам вжити негайних заходів для зменшення ризиків безпеки та захисту мережі.

Профілактичні засоби, такі як інструменти для тестування на проникнення і прилади для оцінки вразливостей, підвищують безпеку бездротової мережі, активно шукаючи потенційні недоліки в системі безпеки. Ці пристрої проводять повну перевірку мережевої інфраструктури, виявляючи недоліки, якими можуть скористатися зловмисники. Превентивні пристрої захищають мережу від кіберзагроз, виявляючи та виправляючи дефекти безпеки до того, як вони будуть використані, зменшуючи ймовірність порушень безпеки.

Системи UTM захищають бездротові мережі, об'єднуючи багато функцій безпеки в одному апаратному пристрої. Ці пристрої, розташовані по периметру мережі, діють як шлюзи, забезпечуючи комплексний захист від шкідливого програмного забезпечення, незаконного проникнення та інших загроз безпеці. Пристрої UTM інтегрують багато служб безпеки, таких як брандмауер, захист від шкідливого програмного забезпечення та виявлення вторгнень, щоб спростити обслуговування та покращити загальний захист.

Бездротові мережі сьогодні є життєво важливою частиною повсякденного життя, з'єднуючи все - від персональних пристроїв до критично важливих систем на підприємствах і в промисловості - їх широке використання робить їх основною

мішенню для кібератак. Такі серйозні заходи щодо захисту мережі випливають з можливостей потенційних загроз, наслідки з втілення яких можуть бути катастрофічними як для простого громадянина, так і для великого підприємства.

1.4. Аналіз загроз безпеці Wi-Fi

У попередньому розділі було розглянуто методи і технології, призначені для захисту бездротових мереж. Незважаючи на їхню важливість, ці захисні заходи ефективні лише настільки, наскільки ефективні загрози, які вони покликані зменшити. Бездротові мережі мають численні вразливості, які можуть бути використані зловмисниками, починаючи від недоліків у протоколах шифрування і закінчуючи маніпулятивними тактиками, спрямованими на користувачів.

Цей розділ присвячений аналізу ключових загроз безпеці бездротових мереж. Розглядаючи найпоширеніші методи атак і вразливості, які вони використовують, можна сформувати стратегії для посилення захисту мережі. Розуміння цих загроз має важливе значення для розробки більш ефективних і комплексних рішень для забезпечення безпеки. Окреслимо найтиповіші з наявних уразливостей і загроз безпеці стандарту IEEE 802.11:

- критична вразливість KRACK у протоколі захисту WPA2;
- підроблена точка доступу (Roque AP);
- MITM-атаки;
- неправильно налаштована точка доступу;
- аналіз пакетів та прослуховування мережі;
- шахрайство;
- атака «відмова в обслуговуванні»;
- атаки на протоколи захисту мереж Wi-Fi.

Однією з найнебезпечніших загроз для Wi-Fi мереж є, насамперед, вразливість *KRACK*. Це пов’язано з тим, що стандарт WPA2 є досі широко поширеним, що більш детально описано в попередньому розділі. Атака KRACK, скорочено від Key Reinstallation Attack, є серйозною вразливістю в протоколі

безпеки Wi-Fi WPA2. Виявлена у 2017 році, ця вразливість використовує слабкі місця в чотиристоронньому рукостисканні, яке використовується для встановлення зашифрованих з'єднань між пристроями та точками доступу в мережах Wi-Fi.

KRACK націлений саме на третій етап рукостискання (підключення клієнту до точки доступу), на якому відбувається обмін ключами шифрування [20]. Перехоплюючи та маніпулюючи цим етапом, зловмисники можуть обманом змусити пристрої перевстановити ключ шифрування, який вже використовується. В результаті зловмисники можуть розшифрувати конфіденційні дані, що передаються мережею, такі як паролі, електронні листи та фінансова інформація. Вони також можуть впроваджувати в трафік жертви шкідливі дані, в тому числі програми-вимагачі або інше шкідливе програмне забезпечення.

Ця атака викликала особливе занепокоєння, оскільки впливала майже на всі пристрої, що підтримують WPA2, включаючи роутери, ноутбуки, смартфони та пристрої Інтернету речей (IoT). Однак атака KRACK вимагає фізичної близькості до цільової мережі, оскільки зловмисник повинен перебувати в зоні дії сигналу Wi-Fi.

Щоб зменшити вплив KRACK, виробники випустили виправлення програмного забезпечення для постраждалих пристроїв, але багато пристроїв Інтернету речей та старіші маршрутизатори залишаються вразливими через нечасті оновлення. Ця вразливість підкреслила необхідність прийняття більш безпечних стандартів, таких як WPA3, і застосування додаткових заходів захисту, таких як віртуальні приватні мережі (VPN) і шифрування HTTPS.

Підроблені або фальшиві точки доступу (Hidden or Rogue Access Points) представляють собою серйозну уразливість, пов'язану з SSID (Service Set Identifier) маршрутизаторів. Під час під'єднання до мережі пристрій з Wi-Fi модулем сканує радіоефір, шукаючи відомі та дозволені користувачем SSID. Якщо знаходить відповідні, то автоматично під'єднується.

Зловмисники можуть змінити SSID на своїх пристроях на популярні назви, наприклад, McDonalds_WiFi_Free, Coffee_Shop тощо. Пристрої жертв під'єднуються до цих мереж автоматично, якщо користувач дозволив підключення

до таких SSID. Це дає змогу зловмисникам здійснювати незаконні дії, такі як перехоплення трафіку, підміна даних або завантаження шкідливого програмного забезпечення. До цього виду загроз належать такі атаки, як Honeypot, Evil Twin Aps, MITM-атаки та інші.

Атака «*людина посередині*» (Man-in-the-Middle, MitM) - це кібератака, під час якої зловмисник таємно перехоплює і змінює комунікацію між двома сторонами, які вважають, що вони безпосередньо пов'язані між собою.

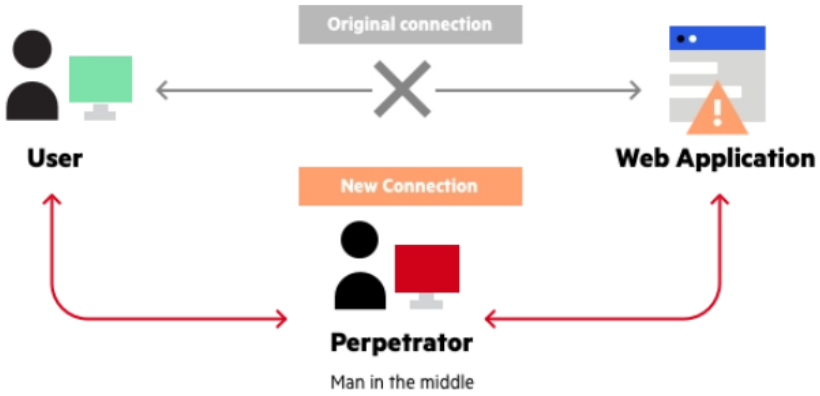

Рис. 1.6. Структурна схема принципу атаки «людина посередині»[21]

MitM-атаки часто полягають у перехопленні даних, якими обмінюються пристрої в скомпрометованій мережі. Зловмисник може підслуховувати комунікацію, перехоплювати облікові дані або впроваджувати шкідливі дані без відома сторін, що спілкуються. Це часто робиться шляхом використання вразливостей у публічних мережах Wi-Fi, DNS-серверах або за допомогою фішингових методів, щоб обманом змусити користувачів під'єднатися до несанкціонованої точки доступу, як описано вище.

Неправильно налаштована точка доступу (Misconfigured APs). Для реалізації загрози, користувач не налаштовує узагалі точку доступу Wi-Fi або не змінює заводських налаштувань: не змінює логінів і паролів, не вимикає широкомовні запити SSID, можливість віддаленого керування тощо. В Інтернеті можна знайти велику кількість баз даних із заводськими налаштуваннями найпоширеніших виробників роутерів (Asus, TP-Link, D-Link, Keenetic), використовуючи які зловмисники можуть під'єднатися до цих пристроїв і

реалізовувати незаконні дії, наприклад, перехопити керування, підмінити дані, завантажити стороннє ПЗ тощо.

Аналіз пакетів (сніфери пакетів, аналізатори протоколів) - це метод, який використовується для перехоплення даних, що передаються в незахищеному вигляді, під час підключення до точки доступу. Зловмисники можуть скористатися відкритим підключенням Wi-Fi і застосувати спеціалізоване програмне забезпечення (наприклад, Wireshark, tcpdump, Capsa, Snoop), щоб отримати доступ до трафіку, що проходить через точку доступу. Це дає змогу витягти корисні та конфіденційні дані.

Такі інструменти можуть використовуватися як на законних підставах (наприклад, адміністраторами мережі), так і незаконно. Вразливість особливо актуальна, якщо мережеві додатки передають дані в текстовому форматі (Telnet, FTP, SMTP, POP3) і без шифрування.

За своєю природою WLAN взагалі вразливі до *DoS-атак*. Всі користуються одними і тими ж неліцензійними частотами, що робить конкуренцію неминучою в населених пунктах Оскільки корпоративні мережі WLAN переходять на стандарт 802.11n, вони можуть використовувати канали в більшому, менш переповненому діапазоні 5 ГГц, що зменшує «випадковий DoS». Крім того, сучасні точки доступу (AP) можуть автоматично налаштовувати канали, щоб обійти перешкоди. Але все одно залишаються цілеспрямовані DoS-атаки: фальшиві повідомлення, що надсилаються з метою відключення користувачів, споживання ресурсів точки доступу та зашумлення каналів. Атака на відмову в обслуговуванні - це тип кібератаки, в якій зловмисник намагається зробити комп'ютер або інший пристрій недоступним для користувачів, перериваючи його нормальне функціонування. Для DoS-атаки характерним є використання одного комп'ютера для запуску атаки, що атакує ціль шкідливим трафіком або ресурсоємними запитами. Це перевантажує пропускну здатність системи, що призводить до її уповільнення або виходу з ладу. DoS-атаки часто використовують вразливості в мережевих протоколах або програмному забезпеченні, надсилаючи неправильно сформовані пакети або використовуючи методи посилення, щоб збільшити їхній вплив.

DDoS-атаки розвивають цю концепцію, використовуючи для виконання атаки кілька систем, часто частину ботнету. Ботнети - це мережі скомпрометованих пристроїв, контрольованих зловмисником, які одночасно надсилають величезні обсяги трафіку на ціль. Оскільки трафік надходить з багатьох джерел, його важче заблокувати, ніж DoS-атаку. DDoS-атаки часто використовують різні вектори, такі як переповнення мережевого рівня, запити на рівні додатків або специфічні для протоколу експлойти, що робить їх більш складними для ліквідації.

Поширеною та сумнозвісною є *загроза шахрайства (фішингу).* Їх існує така велика кількість, що описати всі варіації в одній роботі не є можливим. В цілому фішинг це загальний термін для різних видів атак, які зловмисники можуть здійснювати, вводячи жертву в оману [22]. Це може включати видачу себе за справжню точку доступу (Ewil Twins Aps), створення фальшивої бездротової мережі або використання методів соціальної інженерії щоб вивідати пароль, логін чи SSID тощо.

Атаки на протоколи захисту мереж Wi-Fi. В попередньому розділі було описано деякі способи захисту, що застосовуються в бездротових мережах, зокрема в мережах Wi-Fi. Загрозами для них може бути наступне: підбір паролів WEP, увімкнутий WPS, атака на зниження WPA (наприклад зловмисник змушує AP перейти з WPA3 на WPA2 і здійснити KRACK) , підміна дозволеної MAC-адреси або SSID маршрутизатора та інші. Ці загрози - це здебільшого атаки, які пов'язані з паролями або пін-кодами, їхньою довжиною і застосуванням сучасного ПЗ, яке дає змогу за відносно короткий проміжок часу підібрати потрібну послідовність символів, знаків і (або) цифр для отримання доступу до цільової точки доступу.

Висновки до розділу 1

Об’єднує вище перераховані вразливості те, що реалізація шляхом атак на них можуть бути зручно та централізовано реалізована за допомогою однієї конкретної операційної системи – Kali Linux. Завдяки архітектурі Лінукс, яка надає широкі можливості для модифікації та налаштування ядра системи, яке є відкритим

будь-якому спеціалісту, в цю ОС було імплементовано широкий набір інструментів для тестування та проникнення в різноманітні системи безпеки. Такі інструменти, як Aircrack-ng, Wireshark, nmap та ін., дозволяють користувачам ОС виявляти вразливості, перехоплювати трафік та використовувати слабкі місця в бездротових мережах.

Здатність платформи автоматизувати завдання і надавати детальні результати щодо тестувань робить його потужним інструментом не лише для етичних хакерів, які проводять аудит, але й для зловмисників, які експлуатують незахищені або слабко захищені мережі. Такий подвійний тип використання підкреслює потребу в впровадженні безпечних мережевих практик і передових захисних технологій для протидії типам атак, які стають можливими завдяки таким інструментам. Використовуючи їх для моделювання реальних сценаріїв атак, фахівці з безпеки можуть краще зрозуміти слабкі місця своєї мережевої інфраструктури. Такий підхід дозволяє покращити захист і вдосконалити протоколи безпеки.

Розуміння основних векторів атак, доступних в Kali Linux, дає фахівцям уявлення про тактику, яку використовують зловмисники. Ці знання не тільки допомагають зміцнити індивідуальну мережеву безпеку, але й сприяють підвищенню загальної стійкості бездротових систем. Етично використовуючи Kali Linux, системні адміністратори можуть випереджати нові загрози і забезпечувати надійний захист своїх мереж.

2 ДОСЛІДЖЕННЯ ОС KALI LINUX ТА ЇЇ ІНСТРУМЕНТІВ ДЛЯ ТЕСТУВАННЯ БЕЗПЕКИ WI-FI МЕРЕЖ

2.1. Аналіз призначення та можливостей операційної системи Kali Linux

Операційна система є комплексом програм, що забезпечують управління апаратними засобами комп’ютера, та організовують роботу з файлами (у тому числі запуск і управління виконанням програм), а також реалізують взаємодію з користувачем, тобто інтерпретацію команд, що ним вводяться, і виведенням результатів обробки цих команд [23].

Сьогодні найпопулярнішими операційними системами для комп’ютерів є сімейства Microsoft Windows, UNIX-подібних систем і власне Unix. Сімейство Windows бере свій початок з операційної системи MS-DOS, яка встановлювалася на перші персональні комп’ютери IBM. Операційна система UNIX була створена у 1969 році співробітниками Bell Labs під керівництвом Денніса Рітчі, Кена Томпсона та Браяна Кернігана. Однак, сучасне використання терміна "UNIX" частіше стосується не конкретної ОС, а групи UNIX-подібних систем. Вони базуються на концепціях UNIX, мають подібний функціонал, але використовують інше ядро.

Перша версія UNIX вийшла ще в 1969-у році і була написана на низькорівневій та складній мові Assembler, що не сприяло широкому поширенню такої ОС. Згодом, UNIX був повністю переписаний для новіших типів ПК на мові програмування С, що була створена якраз для цього. В результаті UNIX отримав широке поширення і прихильність серед користувачів, завдяки можливості повністю налаштувати та оптимізувати систему під себе – завдячуючи відкритому вихідному коду.

На підставі такої популярності створювалося безліч підверсій UNIX, які відрізнялися від оригіналу. Програмісти істотно доповнили систему новими можливостями і програмами, зробивши великий внесок в розвиток цієї операційної системи. Протягом тривалого часу системи UNIX не були стандартизовані. Часто

програми створювались конкретною людиною під свою версію ОС, що не дозволяло запустити її на іншій системі. Це намагалися виправити введенням стандартизації System V Interface Definition (SVID), який містив правила, яким необхідно було слідувати розробникам. Це підвищило сумісність різних версій ОС, але не ліквідувало проблему повністю. Під впливом від популярності UNIX та намагаючись вирішити її основні проблеми, згодом було створено два проекти – GNU (GNU's Not UNIX — «GNU — не Unix») та ядро Linux, який був написаний на мові С з використанням розширень GNU.

Головною причиною розробки Linux послугувала обмеженість ліцензії UNIX та Minix для використання тільки в рамках «навчальних цілей», що обмежувало їх комерційне використання. Ліцензія GNU GPL та відкритість коду дала можливість усім охочим брати участь у покращенні роботи ядра, що у свою чергу призвело до створення великої кількості UNIX-подібних операційних систем, які базуються на ядрі Linux.

Linux-системи реалізуються на модульних принципах, стандартах і угодах, закладених в Unix протягом 1970-х і 1980-х років. Така система використовує монолітне ядро, яке керує процесами, мережевими функціями, периферією і доступом до файлової системи. Драйвери пристроїв або інтегровані безпосередньо в ядро, або додані у вигляді модулів, які завантажуються під час роботи системи.

Окремі програми, взаємодіючи з ядром, забезпечують функції системи вищого рівня. Наприклад, призначені для користувача компоненти GNU є важливою частиною більшості Лінукс-систем, що містить найпоширеніші реалізації бібліотеки мови С, популярних оболонок операційної системи, та багатьох інших загальних інструментів UNIX, які виконують багато основних завдань операційної системи.

Відкритість ядра Linux дозволила розробляти операційних систем для вирішення різного типу задач: серверні ОС, ОС для мікрокомп’ютерів (Raspberri Pi), ОС для персонального комп’ютера і т. д. Усі подібні рішення прийнято називати – дистрибутивами Linux. Отже, встановлюючи операційну систему на комп’ютер користувач встановлює не Linux, а дистрибутив що базується на ядрі Linux. До

складу більшості дистрибутивів входить не лише ядро ОС, а й набір інструментів: GNU Tools, net-tools, x server і т. д. До кожного дистрибутиву входить різний набір додаткового програмного забезпечення [23].

Система, що розглядається в даній роботі, починає свою історію з 2013 року. Kali Linux, дистрибутив для тестування на проникнення та етичного хакінгу, був офіційно запущений як наступник BackTrack – ОС, призначеної для пен-тесту програм, мереж та систем, який також є відомим інструментом у спільноті безпеки. Створення Kali Linux було мотивоване потребою у більш спрощеній, надійній та керованій спільнотою платформі. Її розробку очолила компанія Offensive Security, використовуючи методи та навички, отримані з BackTrack.

До Kali BackTrack пройшов кілька ітерацій розвитку, починаючи з перших назв Whoppix і WHAX. Сам BackTrack спочатку базувався на Slackware – одному із самих ранніх UNIX-подібних дистрибутивів Linux, а пізніше перейшов на Ubuntu. Зі зростанням складності потреб у кібербезпеці та попиту на більш адаптований фреймворк, розробники вирішили створити Kali Linux на основі Debian. Це рішення забезпечило більшу гнучкість, часті оновлення, а також надійну підтримку ARM-архітектури та різноманітних середовищ [24].

Kali Linux була розроблена спеціально для тестувальників на проникнення і фахівців з безпеки, інтегруючи сотні попередньо встановлених інструментів для таких завдань, як оцінка вразливостей, моніторинг мережі та цифрова криміналістика. Доступність та багатомовна підтримка розширили його можливості використання для ширшого кола користувачів. Завдяки використанню стандартів Debian і зосередженню на автоматизації та масштабованості, Kali Linux швидко зарекомендувала себе як провідний інструмент у сфері кібербезпеки.

На момент створення, в інтернет-спільноті ходила велика кількість чуток, чому розробники обрали саме таке ім’я. Калі — індуїстська богиня вічної сили, часу і змін, смерті і знищення. Дехто припускав, що розроблений дистрибутив мав настільки потужні можливості, що в руках зловмисника і справді міг стати «богинею знищення». Хоча ця теорія мала сенс і подобалася користувачам системою, нещодавно розробники пояснили, чому вони обрали саме таке ім’я –

воно вже було частиною внутрішнього лексикону і коли хтось з команди запропонував назву Kali для нового дистрибутиву, вони одразу його прийняли [25].

Які ж можливості надає ця ОС користувачу, що її довгий час вважали «богинею знищення». Перш за все, це [26]:

1. Тестування безпеки та оцінка вразливостей - Kali Linux постачається з понад 600-а попередньо встановленими інструментами, призначеними для етичного злому, такими як Metasploit для розробки експлойтів, Nmap для виявлення мереж та Wireshark для аналізу пакетів. Ці інструменти дозволяють професіоналам імітувати реальні кібератаки та ефективно виявляти вразливості в системах.

2. Перевірка безпеки бездротової мережі - Kali Linux відмінно справляється з тестуванням безпеки бездротових мереж за допомогою таких інструментів, як Aircrack-ng, який підтримує ін'єкцію пакетів, відновлення ключів шифрування і моніторинг трафіку. Ці функції є критично важливими для оцінки надійності мереж Wi-Fi.

3. Адаптивність і гнучкість - платформа підтримує різні методи розгортання, включаючи встановлення на віртуальні машини та ARM-пристрої, такі як Raspberry Pi. Її модульна конструкція дозволяє користувачам адаптувати операційну систему та набори інструментів до своїх конкретних потреб, забезпечуючи значну гнучкість.

4. Цифрова криміналістика - Kali Linux також включає такі інструменти, як Autopsy та Sleuth Kit для криміналістичного аналізу. Вони життєво необхідні для таких завдань, як відновлення видалених файлів, аналіз дампів пам'яті та дослідження цифрових слідів.

5. Інтегроване середовище розробки - підтримує написання сценаріїв і розробку програмного забезпечення, дозволяючи користувачам створювати автоматизовані тести безпеки за допомогою таких мов, як Python, Ruby і Bash. Ця функція особливо корисна для написання користувацьких експлойтів або керування складними тестами на проникнення.

6. Глибокі навчальні можливості - Kali Linux відіграє ключову роль в освіті з кібербезпеки. Завдяки широкому набору інструментів та відкритому коду

він є чудовою платформою для навчання нових спеціалістів та проведення змагань або симуляцій з кібербезпеки.

7. Широкий інструментарій - централізуючи широкий спектр інструментів і надаючи впорядковане, орієнтоване на безпеку середовище, Kali Linux спрощує процес проведення комплексних аудитів безпеки. Він також забезпечує регулярне оновлення свого репозиторію інструментів, що дозволяє фахівцям використовувати найновіші технології кібербезпеки.

Підсумовуючи, такий набір інструментів Kali Linux робить її потужною та універсальною операційною системою для широкого спектру завдань кібербезпеки. Її попередньо встановлені інструменти охоплюють все - від сканування мережі та оцінки вразливостей до криміналістичного аналізу.

Ці особливості роблять Kali Linux найкращим вибором для професійних і навчальних целій, пов’язаних з кібербезпекою.

2.2. Дослідження інструментів для тестування безпеки безпроводових мереж

Як зазначалося вище, Kali містить більше шестисот засобів та інструментів, що слугують різним цілям [26]. Для тестування безпеки бездровотових мереж застосовуються зазвичай:

1. *Nmap (Network Mapper)* - це широко використовуваний інструмент для виявлення мереж та аудиту безпеки. Він дозволяє користувачам сканувати відкриті порти та служби, що обслуговуються в мережі. Nmap є інструментом розвідки, що дозволяє виявити можливі вразливості в системі та підготувати атаку.

2. *Aircrack-ng* - це набір інструментів, спеціально призначених для тестування безпеки бездротових мереж. Він підтримує такі завдання, як моніторинг мережевого трафіку, впровадження пакетів і злом ключів шифрування WEP/WPA/WPA2.

3. *Wireshark* - це аналізатор пакетів, який дозволяє користувачам перехоплювати і перевіряти мережевий трафік в режимі реального часу. Він має

вирішальне значення для діагностики мережевих проблем, аналізу протоколів і виявлення підозрілої активності в мережі.

4. Фреймворк Metasploit є одним з найбільш комплексних інструментів для тестування на проникнення та розробки експлойтів. Він включає в себе базу даних готових експлойтів та допоміжних модулів, які можуть бути спрямовані на різні вразливості в мережі.

5. *Ettercap* - це інструмент для проведення атак типу «людина посередині» (MitM) на локальні мережі. Він може перехоплювати і модифікувати мережевий трафік, що робить його корисним для тестування вразливостей, пов'язаних з перехопленням даних.

6. *Responder* це інструмент для атаки на мережеві протоколи шляхом перехоплення запитів на автентифікацію та збору облікових даних.

7. *Hydra* використовується для злому паролів за допомогою методів грубого перебору або словникових атак на різні мережеві протоколи, такі як FTP, HTTP, SSH та інші. Це універсальний інструмент для тестування надійності паролів.

8. *Burp Suite* - це просунутий сканер веб-вразливостей і проксі-інструмент. Він зазвичай використовується для тестування веб-додатків, розміщених в мережі, виявлення таких проблем, як SQL-ін'єкції або міжсайтовий скриптинг (XSS).

9. *Nikto* - це сканер веб-серверів, який виявляє вразливості, такі як застаріле серверне програмне забезпечення, неправильні конфігурації та потенційно небезпечні файли. Він необхідний для захисту веб-сервісів у мережі.

10. *DNSenum* автоматизує перерахування DNS, збираючи інформацію про DNS-сервери та пов'язані з ними зони. Це корисно для відображення структури цільової мережі.

11. *John the Ripper* - потужний і універсальний інструмент для злому паролів (шляхом перебору), який використовується для тестування на проникнення і аудиту безпеки. Отримав широку популярність через вміння швидко знаходити слабкі паролі в системах.

12. *Wifite* – автоматизований інструмент аудиту бездротових мереж, призначений для спрощення процесу тестування безпеки мереж Wi-Fi. Він поєднує

в собі різні методи та інструменти бездротових атак (такі як nmap, wireshark та інструменти брутфорсу) для автоматизованого та полегшеного взлому мережі.

Підсумовуючи перераховане, Kali надає широкий спектр інструментів для тестування мережевої безпеки. Комбінуючи використання цих інструментів, користувачам надається можливість виявляти вразливості, тестувати захист та ефективно проводити атаки. Консолідуючи всі ці інструменти в одному місці, Kali Linux полегшує тестування і вдосконалення мережевого захисту. Це важлива платформа для всіх, хто хоче виявити і виправити проблеми безпеки до того, як ними скористаються зловмисники.

2.3. Технологія встановлення та налаштування Kali Linux для тестування безпроводових мереж

У 1985 році Microsoft представила Windows 1.0, яка надавала графічний інтерфейс користувача (GUI) поверх MS-DOS. Хоча першій версії було далеко до ідеалу, наступні випуски, такі як Windows 3.0 і 3.1, враховували відгуки користувачів, покращуючи функції та продуктивність.

Стратегічно Microsoft зосередилася на широкій сумісності. На відміну від Apple, яка прив'язувала своє програмне забезпечення до пропрієтарного обладнання, Microsoft ліцензувала Windows для різних виробників обладнання. Такий підхід наповнив ринок доступними комп'ютерами під управлінням Windows, що сприяло її швидкому поширенню в усьому світі.

У 1990-х роках такі випуски, як Windows 95 та Windows XP, здійснили революцію в обчислювальній техніці завдяки таким функціям, як підтримка plug-and-play та інтуїтивно зрозумілий інтерфейс, що закріпило домінування Microsoft. Партнерство з виробниками обладнання та постійне вдосконалення програмного забезпечення ще більше зміцнили позиції Windows як стандартної операційної системи як для особистого, так і для професійного використання.

Таким чином, впевнена експансія Microsoft, ітеративний розвиток зручного графічного інтерфейсу, сумісність з різноманітним обладнанням та ефективне

партнерство зіграли вирішальну роль в становленні Windows як найпопулярнішу систему у світі.

Сьогодні складно уявити домашній ноутбук, шкільний чи робочий ПК без установленої Windows та її екосистеми. Постає питання – яким чином здійснити тестування бездротової мережі за допомогою іншої ОС без необхідності переустановлення наявної з неминучим видаленням важливих персональних файлів? На допомогу приходить віртуалізація - створення віртуального, тобто штучного, об'єкта чи середовища. В даній роботі буде використане віртуальна машина Oracle VM VirtualBox, яка дає можливість на одному ПК мати обмежену лише ресурсами самого комп’ютера кількість операційних систем.

Існує два способи встановлення Kali на віртуальну машину. Перший, класичний, мало відрізняється від звичайного встановлення Windows, звичайно, з поправками на те що система встановлюється «віртуально», тобто користувач має ще створити середовище виконання.

Для реалізації першого необхідно завантажити образ ISO з офіційного сайту – *kali-linux-2024.3-installer-amd64.iso*. В меню віртуальної машини тиснемо «Створити» і вибираємо образ.

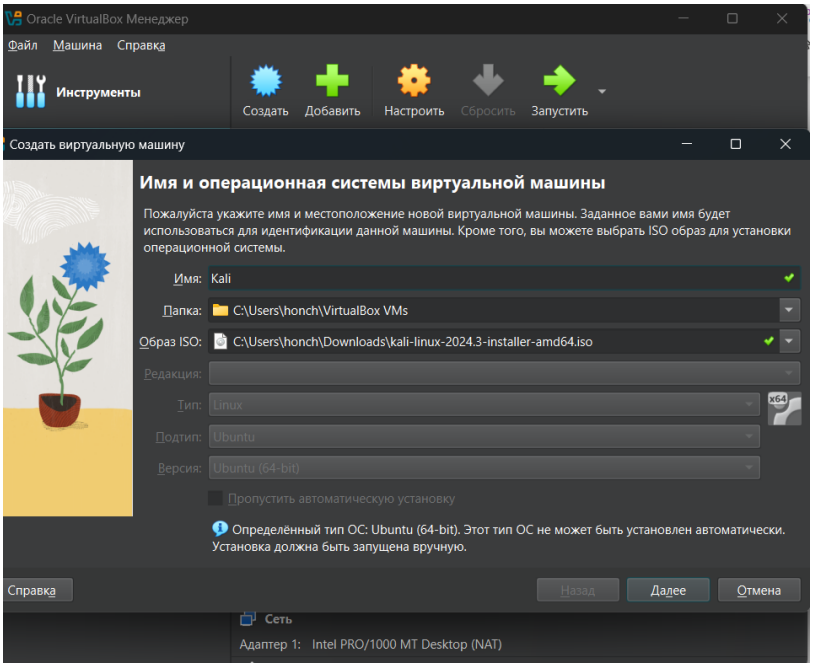

Рис. 2.1. Встановлення Kali

Далі необхідно створити саму систему на яку буде встановлено ОС. VirtualBox пропонує користувачу самому задати ресурси ПК, які він може виділити на віртуальну машину. Слід пам’ятати, що Калі необхідно не менш ніж 2 ядра ЦП, 2 гігібайти ОЗУ та 20 Гб вільного місця. Чим більше ресурсів буде виділено віртуальній системі, тим вище в неї буде продуктивність, і тим нижче продуктивність буде на основній системі, якщо обидві будуть працювати одночасно.

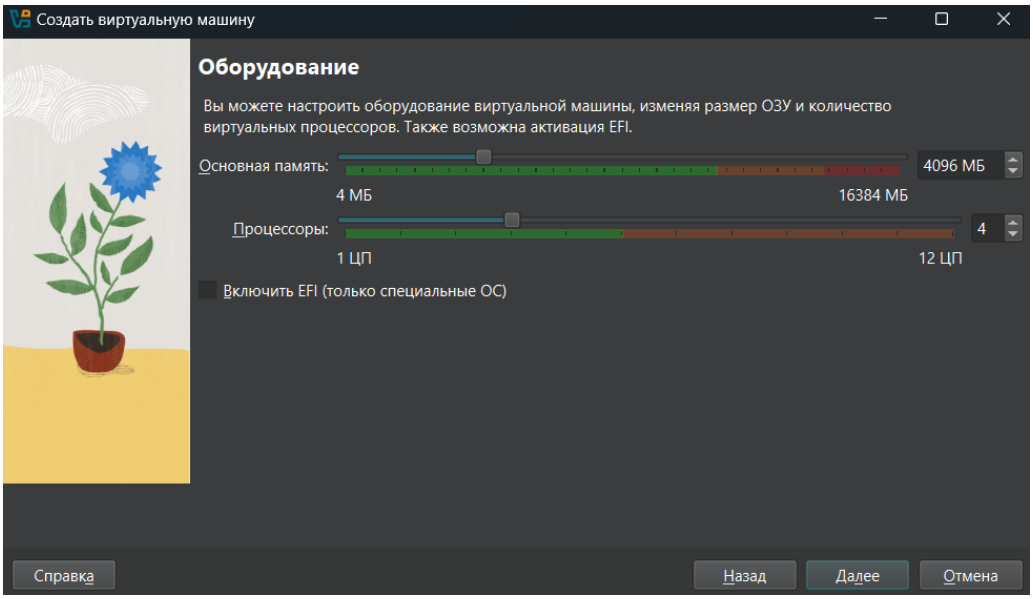

Рис. 2.2. Виділення ресурсів для віртуальної машини

Наступним кроком буде створення віртуального жорсткого диску. Рекомендується виділяти не менш ніш 20-25 гігабайт пам’яті для стабільної роботи. Окремо слід виділити можливість повного і неповного виділення місця. В першому випадку, якщо поставити галочку (виділено на Рис.2.3.), місце на жорсткому буде зарезервовано повністю, тобто від всього об’єму накопичувача буде відмінусовано 25 Гб, коли при другому варіанті (залишаючи за замовчуванням), місце на жорсткому диску зарезервується, але буде заповнюватись на фоні заповнення ОС на віртуальній машині. Це корисно, коли накопичувач має обмежений об’єм пам’яті, який доводиться заощаджувати.

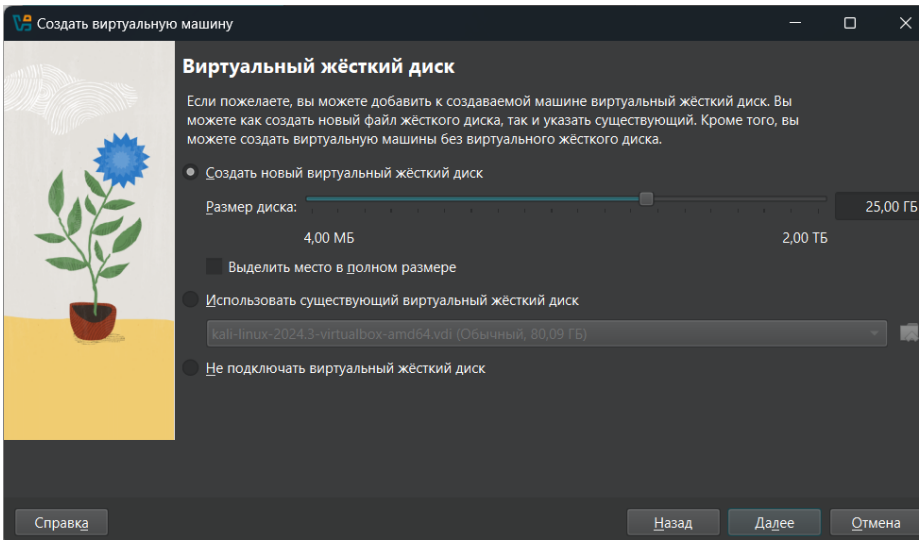

Рис. 2.3. Створення віртуального жорсткого диску

Після прооблених маніпуляцій в меню VirtualBox з’явиться нова віртуальна система. Натиснувши «Запустити» користувач ініціює звичайну установку нової ОС на ПК, яка схожа на установку Windows.

Рис. 2.4. Встановлення ОС на віртуальну машину

Після установлення системи вона повністю готова до роботи і буде імітувати поведінку як на звичайному десктопному комп’ютері. Завжди зберігається

можливість подальшого налаштування системи (додати чи зменшити обсяг залучених ядер процесора, кількості відеопам'яті, змінити тип мережевого адаптера тощо).

Другий варіант встановлення набагато простіше. Необхідно завантажити вже створений образ VirtualBox, який після запуску сам розвернеться на віртуальній машині. Із мінусів такого методу – в ньому вже задані основні характеристики ПК, які після встановлення системи можна змінити, але розмір виділеного жорсткого диску буде незмінним – 80 гігабайт з поступовим розширенням по мірі заповнення.

Після успішного встановлення тим чи іншим методом системи рекомендується установити всі доступні оновлення системи та її інструментів. Робиться це за допомогою команд sudo apt-get update (оновлює системні компоненти), sudo apt-get upgrade (оновлює інструменти) та sudo apt-get dist-upgrade (встановлює останню версію дистрибутиву).

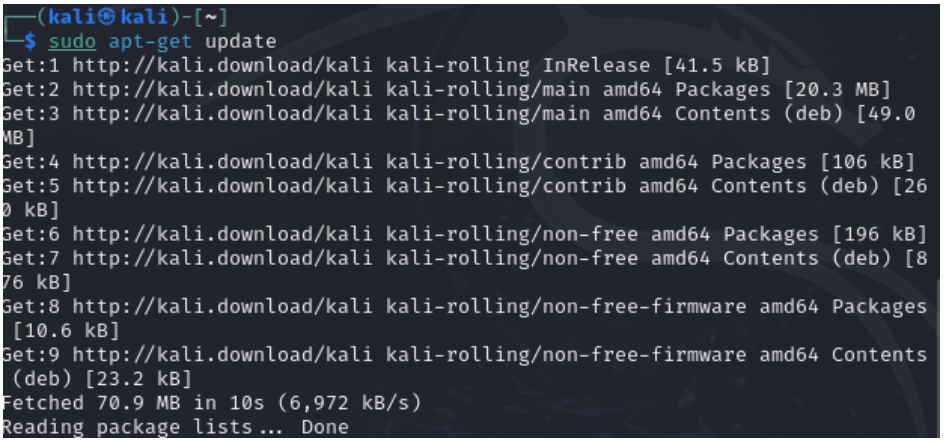

Рис. 2.5. Встановлення системних оновлень

Оновлення, особливо інструментів, виходять доволі часто, тому важливо постійно перевіряти їх наявність. Окрім того, в систему можна встановлювати додаткові інструменти та видаляти вже інстальовані за допомогою sudo apt-get «ім'я пакету» та sudo apt-get remove «ім'я пакету».

Висновки до розділу 2

Kali дає можливість користувачам встановити систему на будь-яку конфігурацію ПК, на Андроїд чи навість в хмару. Швидкий, Windows-подібний процес налаштування системи дозволяє навіть недосвідченим користувачам Linux оперативно розгорнути систему, встановити необхідні оновлення та почати виконувати свої задачі.

При цьому ОС є потужним інструментом щодо вирішення цілої низки задач – від тестувань на проникнення до навчання майбутніх спеціалістів з кібербезпеки. Інтегруючи Kali в освітній процес, навчальні заклади мають змогу зацікавити здобувачів освіти унікальним процесом тестування систем на проникнення, і при цьому в майбутньому підвищити безпеку підприємств, на роботу до яких влаштується випускник.

3 СТРАТЕГІЯ ПОКРАЩЕННЯ БЕЗПЕКИ НА ОСНОВІ ТЕСТУВАННЯ WI-FI МЕРЕЖІ

3.1 Технологія тестування Wi-Fi мережі

Для здійснення тестування мережі безпроводовий адаптер (БА) повинен підтримувати режим моніторингу. Зазвичай, це не є проблемою на десктопних персональних комп'ютерах або коли Kali є основною встановленою операційною системою, що не є даним випадком. У випадку, коли ОС встановлена на віртуальну машину (VirtualBox, VMware чи Hyper V) що базується на ноутбуці, доведеться використати сторонній Wi-Fi адаптер, оскільки вбудовані не підтримують режим моніторингу.

Для налаштування зовнішнього мережевого адаптеру в налаштуваннях ВМ Kali необхідно додати новий пристрій USB. Це дозволить віртуальній операційній системі бачити та керувати адаптером.

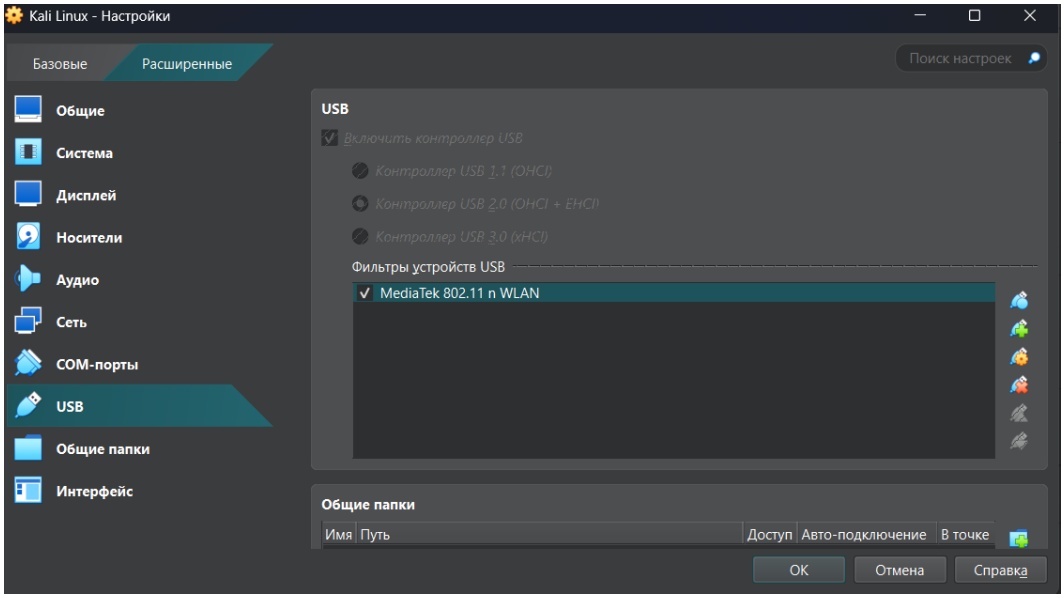

Рис.3.1. Додавання пристрою USB у віртуальну машину

Відбувається це таким чином – необхідно увімкнути контролер USB, виділити належний USB-порт та додати до нього підключений сторонній адаптер.

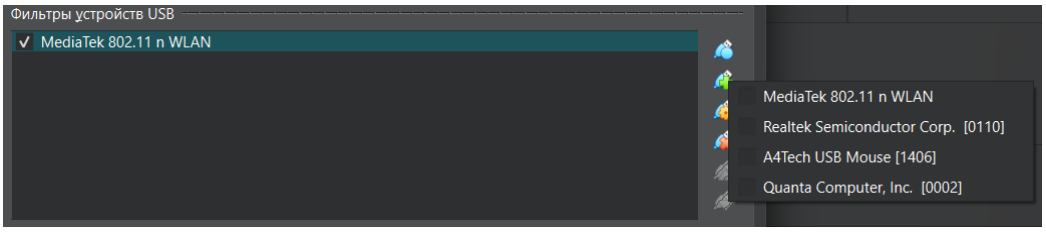

Рис.3.2. Додавання підключеної мережевої карти до USB-інтерфейсу

Якщо користувач не знає назву адаптеру, можна відключити його, переглянути доступні USB-пристрої, підключити адаптер знову і вибрати його при появі. Після пророблених дій БА має з'явитися як доступний пристрій USB при запущеній віртуальній машині.

Рекомендується від'єднатися і підключитися до пристрою після запуску ВМ, оскільки іноді без цього вона не бачить новий мережевий інтерфейс. Для перегляду доступних мережевих інтерфейсів використовуємо команду *ifconfig*.

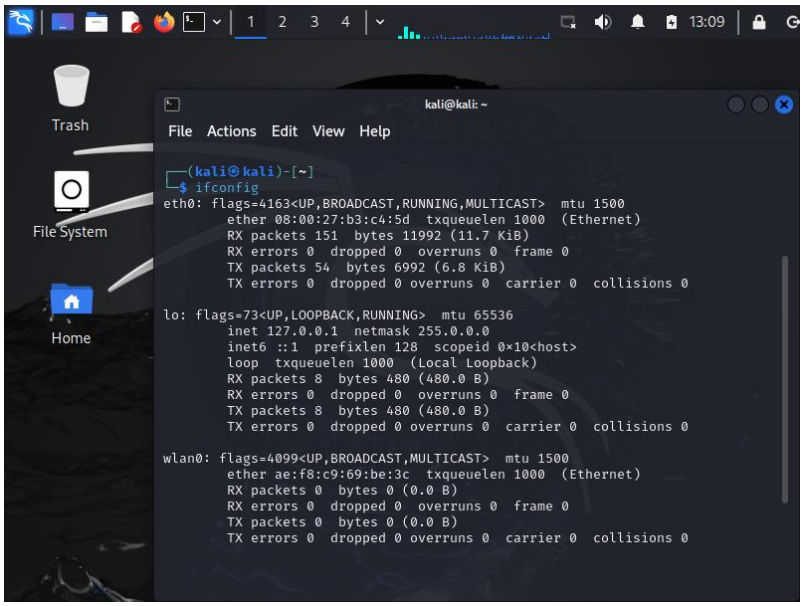

Рисунок 3.3. Відображення доступних мережевих інтерфейсів

Адаптер з доступним режимом мережевого моніторингу зазвичай має назву wlan0, що продемонстровано на Рисунку. Також доступність БА можна переглянути за допомогою *sudo airmon-ng* – вбудованої в комплект aircrack-ng утиліти для перегляду доступних карт у режимі моніторингу.

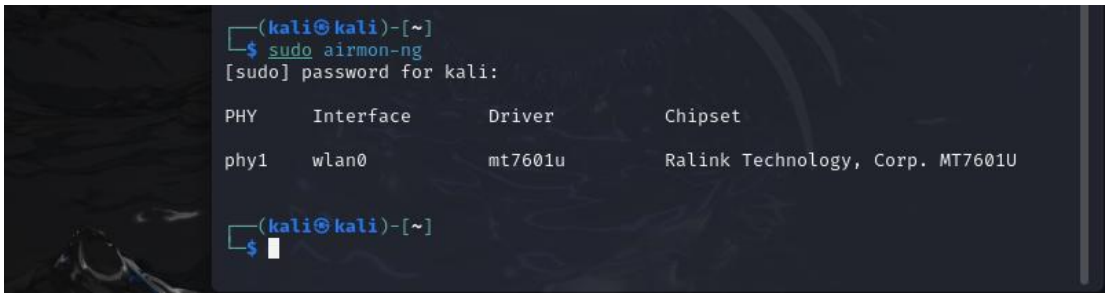

Рис.3.3. Відображення підтримуючих режим моніторингу мережевих карт

Airmon-ng дає більше інформації про доступні Це корисно коли на робочій станції наявно декілька мережевих адаптерів, і користувачу необхідно вибрати, яку з них перевести в режим моніторингу.

Для виявлення наявних мереж скористаємось утилітою Wifite, викликавши її командою *sudo wifite*. Даний інструмент дає змогу автоматизувати та значно прискорити процес тестування мережі, оскільки об’єднує цілу низку інструментів.

Після виклику команди вона автоматично переведе адаптер в режим моніторингу.

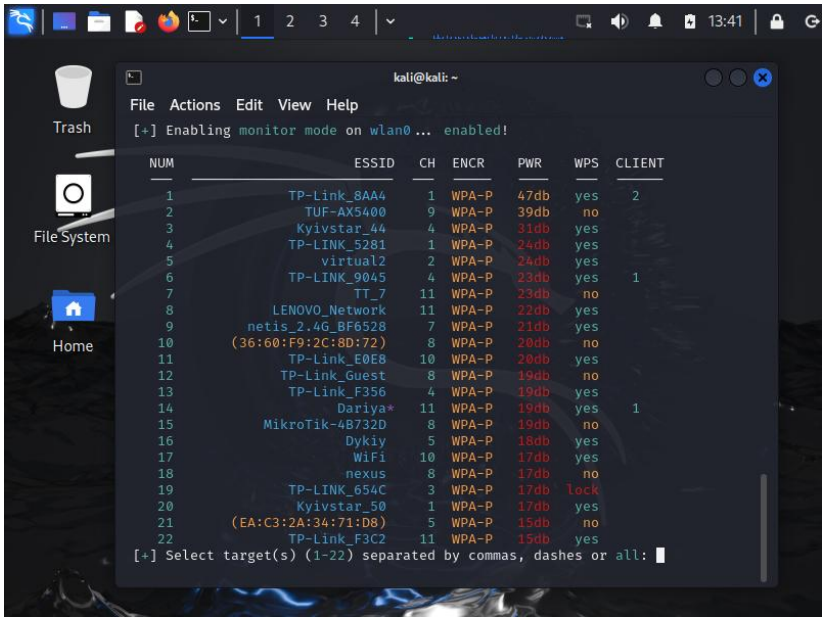

Рис.3.4. Відображення доступних WLAN-мереж

Утиліта відображає мережеві назви, робочий канал, тип шифрування, потужність сигналу, кількість підключених пристроїв та чи включений WPS. Останній є серйозною вразливістю, і його наявність на більш ніж половині з доступних мереж Wi-Fi свідчить про необізнаність користувачів з базисом мережевої безпеки.

Зручно відсортувати мережі з WPS можна командою *sudo wash -i wlan0*.

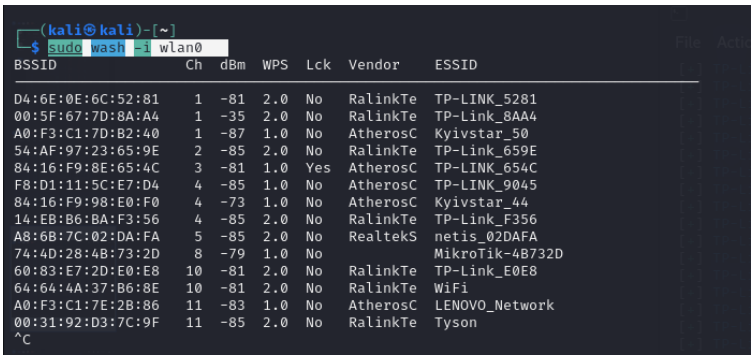

Рис.3.5. Мережі з WPS

Найпоширенішим інструментом для атаки таких мереж є утиліта Reaver. Для запуску атаки слід виконати команду *sudo reaver -i wlan0 -b 00:5F:67:7D:8A:A5 -c 6 -vv*, де -i: Reaver використовує інтерфейс wlan0; -b: атака спрямована на мережу з BSSID 00:5F:67:7D:8A:A5; -c: Reaver слухає трафік на каналі 1: -vv: показує детальну інформацію про процес.

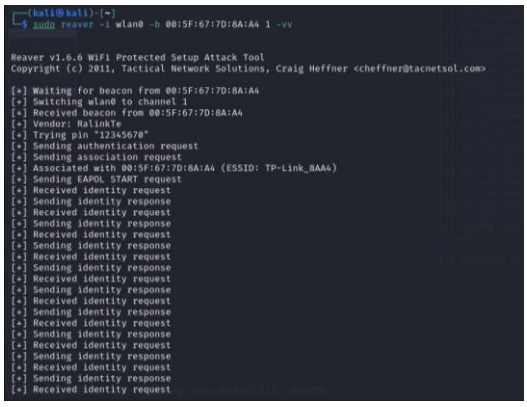

Рис.3.6. Атака на WPS утилітою Reaver

Слід зазначити, що процес такої атаки доволі повільний і може затягнутися до кількох годин. Окрім того, вразливість WPS відома вже доволі давно, тому

виробники точок доступу можуть забезпечити захист від таких атак. В даному випадку, AP зрозуміла і виявила численні запити від мережевого адаптеру і почала слати команди на від'єднання (*deauth request*). Проте, в деяких випадках ця вразливість є гарантованим способом отримати пароль, тому слід перевіряти спочатку цей метод.

Для запуску тестування Wifite необхідно обрати цифру, якій відповідає бажаній для атаки мережі. Допускається атака великої кількості мереж (для цього необхідно вибрати діапазон мереж, наприклад 1-3, або перерахувати їх через кому), навіть взагалі всіх, що є у списку. Звичайно, атака кількох мереж займе більше часу.

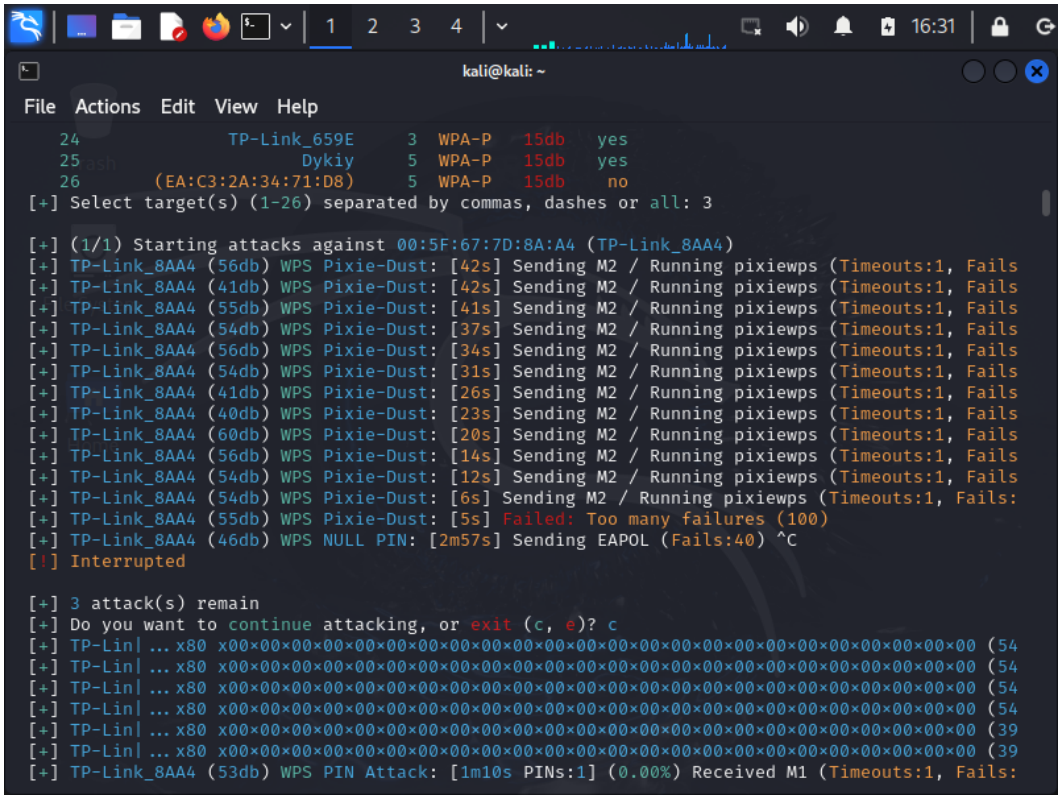

Рис.3.7. Процес атаки на обрану мережу

В процесі роботи програма буде перебирати декілька версій атак на мережу. Враховуючи що системи безпеки покращуються і виробники точок доступу зацікавлені в підтримці цього процесу, не всі атаки будуть успішними. В даному випадку атаки Pixie-Dust і атака на WPS не увінчались успіхом. Атака Pixie-Dust використовує вразливість у реалізації WPS, зокрема в автономному обчисленні PIN-

коду, який використовується під час під’єднання пристроїв. Це дозволяє відновити PIN-код, використовуючи передбачувану або слабку ентропію в обміні WPS, що дає можливість отримати доступ до мережі без перебору всього PIN-коду.

Атака на WPS PIN-код полягає в переборі 8-значного WPS PIN-коду для отримання ключової фрази мережі WPA/WPA2. Оскільки PIN-код часто розбивається на дві частини для перевірки, зловмисники можуть вгадати кожну частину окремо, що значно зменшує кількість необхідних спроб. Щоправда, такі атаки працюють не завжди.

В такому випадку, щоб не марнувати час, рекомендується зупинити атаку (за умовчуванням Ctrl+C) та перейти до наступної.

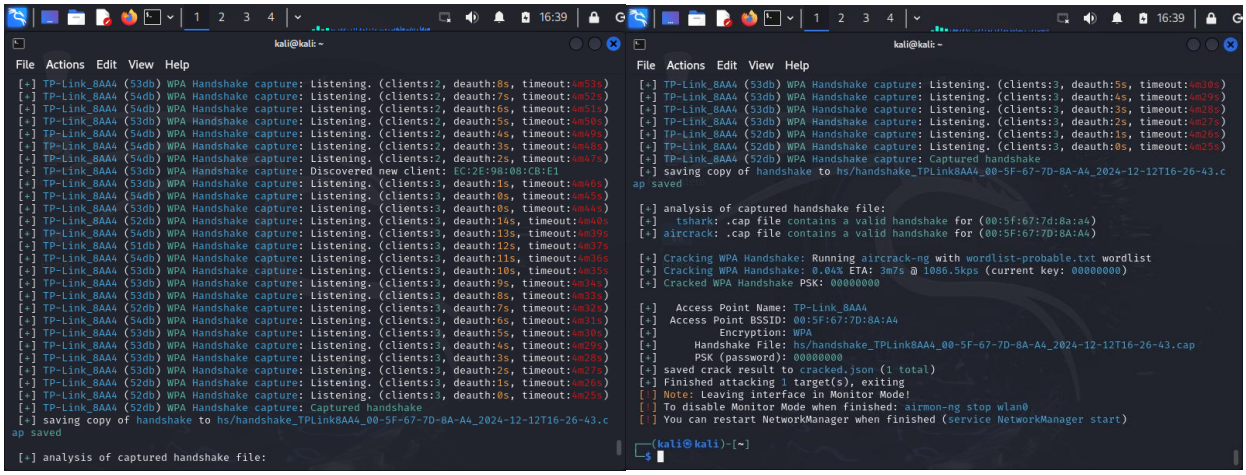

Рис.3.8. Успішне перехоплення рукостискання

Наступна атака була успішною. В процесі роботи програма від’єднала та відстежувала пристрої, що підключаються до мережі і перехопила handshake, зберігши його в директорію. Рукостискання - це зашифрований обмін, який відбувається, коли пристрій підключається до мережі Wi-Fi. Він включає в себе чотириетапний процес між клієнтом і точкою доступу, який гарантує, що обидві сторони мають правильні облікові дані перед встановленням безпечного з'єднання.

Під час перехоплення рукостискання тестувальник мережі або зловмисник використовує такі інструменти, як Aircrack-ng або Wireshark, щоб перехопити і записати цей обмін. Зазвичай для цього тестеру потрібно або дочекатися, поки клієнт підключиться до мережі природним чином, або змусити пристрій повторно

підключитися, виконавши атаку з деаутентифікацією, що змусить його повторно ініціювати рукостискання. Wifite реалізує дану атаку цілеспрямованим від'єднанням клієнта мережі.

Перехоплене рукостискання може бути проаналізовано або піддано атакам грубої сили або за словником для відновлення попередньо наданого ключа мережі (PSK). Хоча саме по собі перехоплення рукостискання не компрометує мережу, етап аналізу створює значні ризики, якщо PSK є слабким або погано підібраним.

Після цього утиліта автоматично застосувала *aircrack-ng* для дешифрування рукостискання атакою за словником (в утиліту *wifite* уже вбудований невеликий (4800) набір найпопулярніших шаблонів паролів).

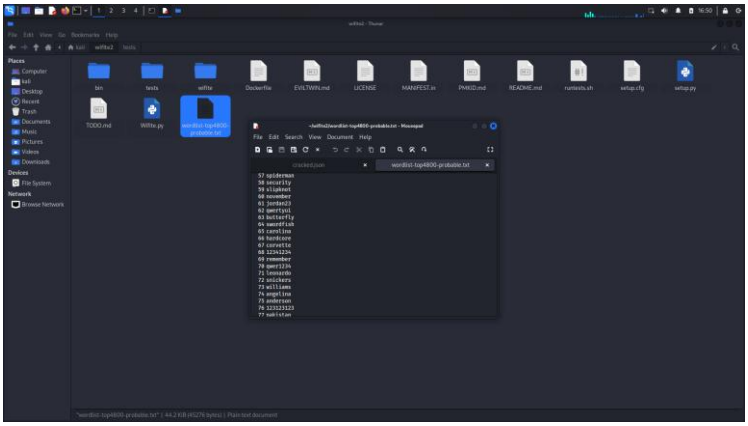

Рис.3.9. Вбудований словник wifite

Програма дозволяє використати свій набір, наприклад завантажений з інтернету чи DarkNet (постійно з'являються словники з мільйонами різних діючих паролів, завантаження таких файлів доступно і платно, і безкоштовно – тому так важливо змінювати стандартні паролі точок доступу). Для використання свого словника необхідно щоб він був у вигляді списку (як на Рис.3.9).

В результаті виконаної роботи було створено короткий звіт про атаку, який міститься під назвою «*cracked.json*».

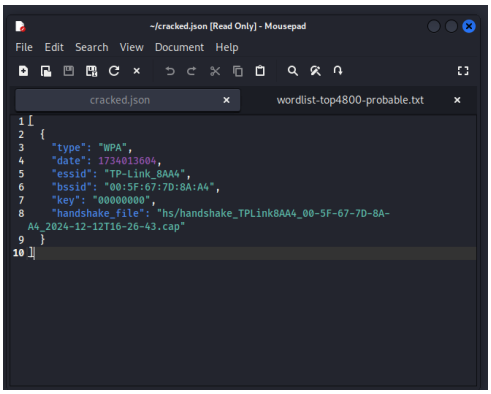

Рис.3.10. Звіт про атаку

В файлі міститься інформація про стандарт атакованої мережі (WPA), широкомовну назву мережі (TP-Link_8AA4), фізичну назву мережі (BSSID, або MAC), сам пароль та відомості про файл рукостискання. Всього, на атаку було затрачено 3 хвилини. Підбір пароля відбувся практично миттєво.

Які висновки можна зробити про атаковану мережу? Перш за все, це:

1. використання протоколу захисту WPA за умовчуванням;

2. робоча широкомовна назва мережі;

3. увімкнутий WPS;

4. простий для зламу пароль.

Після налаштування захисту мережі методикою, описаною в наступному пункті, маємо:

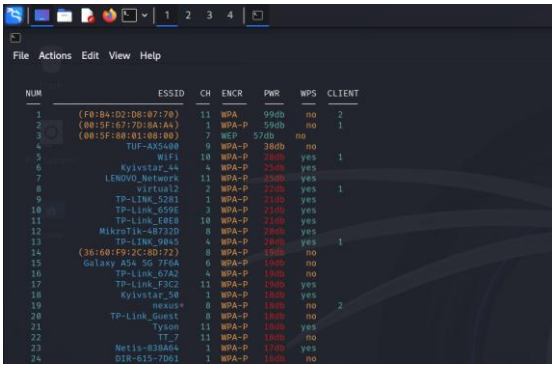

Рис.3.11. Відсутня ESSID мережі

Відключивши широкомовне оголошення SSID із корисної інформації зловмиснику тепер доступна лише сила сигналу та MAC-адреса (00:5F:67:7D:8A:A4). Пам’ятаючи MAC, запустимо атаку.

Рис.3.12. Результат атаки на мережу

Як видно на Рис.12, Wifite вдалось перехопити рукостискання навіть при умові переходу на покращений WPA2, але утиліта не змогла підібрати вірний пароль.

Спробуємо здійснити брутфорс-атаку на handshake за допомогою словника rockyou. Він містить близько 32-х мільйонів паролів, які вдалося витягнути завдяки SQL-ін’єкції ще в 2009-му році. Словник постійно поповнюється новими паролями і досі є актуальним інструментом для атак шляхом перебору [27].

Цей і інші словники вже вбудовані в Kali і знаходяться в usr/share/wordlists. Користувач може переглядати вже дискредитовані паролі і не використовувати їх в своїх системах.

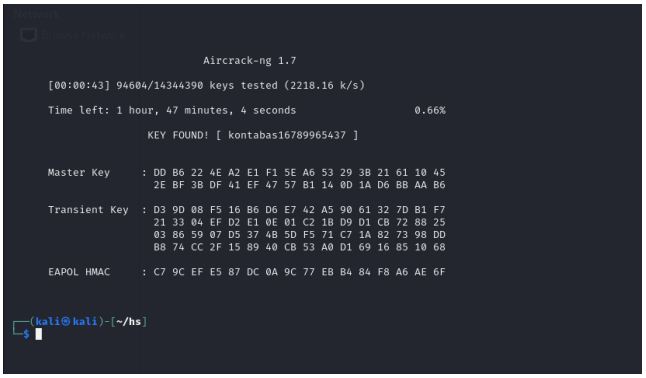

Рис.3.13. Атака за словником rockyou

На перебір всіх паролів словника використовуючи CPU (процессор) необхідно близько 2-х годин. Цей процес значно пришвидшиться за використанням GPU (відеокарти). Для залучення GPU необхідно конвертувати перехоплене рукостискання з формату *.cap* у формат *.hccapx*. Це робиться за допомогою утиліти hcxpcapngtool командою *hcxpcapngtool -o handshake.hccapx «імя рукостискання».cap.* Після конвертації маємо змогу запустити атаку утилітою *hashcat* при задіянні GPU.

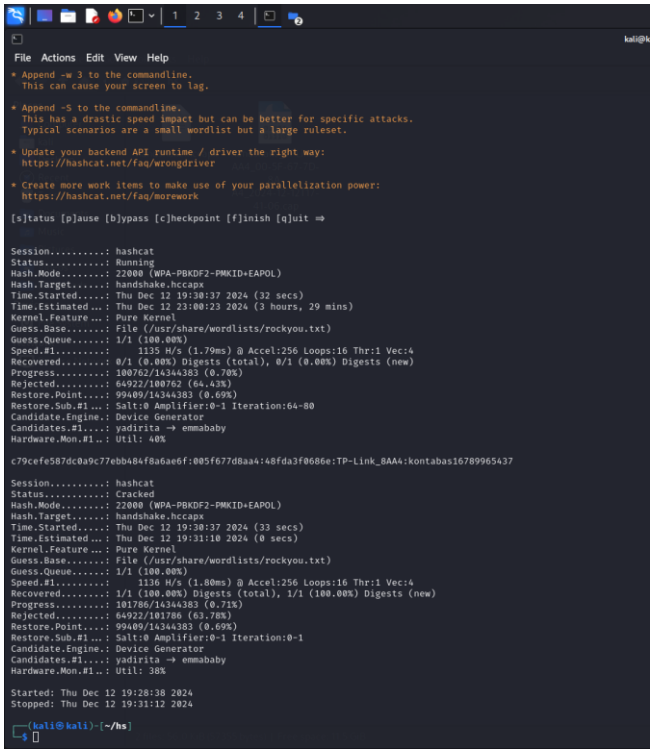

Рис.3.14. Словникова атака за допомогою *hashcat*

Пароль kontabas16789965437 був знайдений за 33 секунди. Якщо ж використовувати атаку не за словником, а методом брут-форсу, процес зламу розтягнеться на декілька годин для пароля з восьми символів і до декількох днів для чисельно-буквенних паролів від 12 символів (залежить від потужності відеокарти).

Для запуску брутфорс атаки (без словника) - *hashcat -m 22000 -a 3 handshake.hccapx ?a?a?a?a?a?a?a?a,* де:

1. -m 22000 - режим для хендшейків WPA/WPA2;
2. -a 3 - це режим брутфорс атаки (brute-force);

3. handshake.hccapx – файл рукостискання, з яким працюватиме Hashcat;

4. ?a - це маска, де ?a означає будь-який символ (букви, цифри, спеціальні символи). У цьому випадку, маска з 8 символів. Якщо пароль довший або коротший, потрібно змінити кількість символів у масці.

Для брутфорс атаки важливо спробувати вгадати кількість символів в паролі. Найкращим варіантом буде також вгадати чи наявні в паролі спеціальні символи, тощо. Це дасть змогу більш точно задати вектор атаки (?l - маленькі літери (a-z), ?u - великі літери (A-Z), ?d - цифри (0-9), ?s - спеціальні символи (наприклад, !, @, #, $, %).

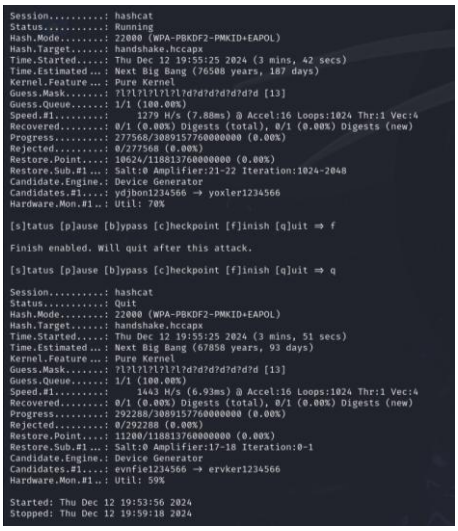

Рис.3.15. Проведення брутфорс атаки

Навіть при таких «ідеальних» умовах, коли умовою для старту утиліти було обрано максимально підходящу умову (8 букв, 11 чисел) в правильному порядку, програма іронічно оцінює термін закінчення операції «до наступного великого вибуху». Слід зазначити, що злам проводився на офісному ноутбуці з вбудованим чіпом GPU і 512 Мб відеопам'яті, з яких ВМ доступно лише 128 Мб. На більш потужних пристроях злам буде набагато швидшим, особливо якщо вдасться вгадати деякі специфікації пароля. Як зазначалося вище, для 8-бітних паролів це займе лічені години.

3.2. Принципи покращення мережевої безпеки

Атака на дротову мережу пов'язана з фізичним проникненням або знаходженням на досить близькій відстані (наприклад, за рахунок отримання доступу до комутаційної шафи бізнес-центру). Як варіант, можна використати інсайдера, щоб під'єднати до мережі портативний пристрій з метою перехоплення пакетів або прослуховування трафіку. В будь-якому разі, зловмиснику необхідно наблизитися або навіть проникнути за периметр безпеки.

Як видно з попереднього розділу, бездротові мережі є значно вразливішими до атак, особливо коли користувач залишає «заводські» налаштування точки доступу. Передвстановлений пароль, WPS, автоматичний режим шифрування, що використовує WPA замість WPA2 – все це суттєво знижує безпеку системи в цілому.

Як відомо, абсолютного захисту не існує. Основний принцип, на що має покладатися адміністратор безпеки це максимально укріпити систему безпеки, щоб затрачені зусилля перевищували імовірний зиск від атаки. Окрім того, використання декілька «шарів» захисту може дозволити виявити вторгнення і прийняти міри.

Перш за все, необхідно переконатися, що на точці доступу вимкнутий WPS. Це робиться в додаткових налаштуваннях точки доступу, в розділі з відповідною назвою.

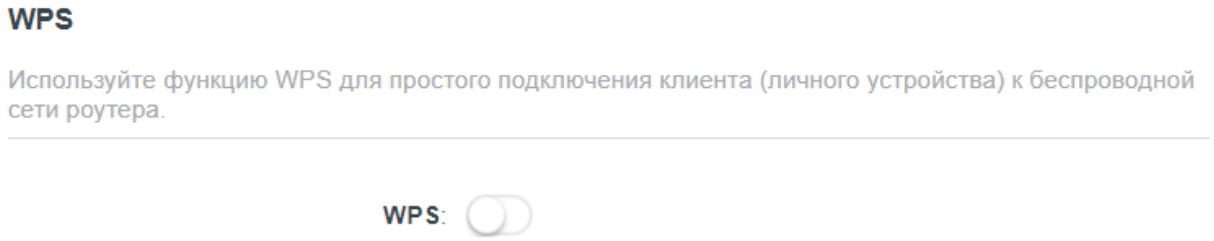

Рис.3.16. Вимкнення функції WPS

Залишаючись в налаштуваннях точки доступу, вибираємо найліпший з доступних методів захисту (згідно з пунктом 1.3.), для досліджуваної мережі це WPA/WPA2 Personal.

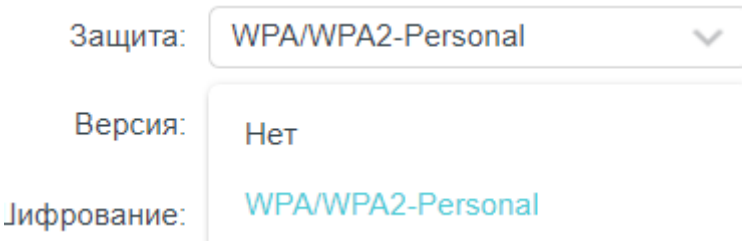

Рис.3.17. Вибір технології захисту

В меню нижче маємо змогу вибрати версію захисту, обираємо WPA2-PSK замість «Авто» з типом шифрування AES.

Рис.3.18. Налаштування специфікацій захисту

WPA2-PSK (pre-shared key) використовує єдиний ключ для всіх клієнтів мережі. В разі компрометації зловмисник отримує доступ до всієї мережі, такий ключ трудоємнісно міняти - потрібно переналаштувати всі клієнти. Проте через простоту реалізації та поширеністю точок доступу з таким метод захисту, він широко застосовується в домашніх мережах і малому бізнесі.

У випадку, коли точка доступу підтримує WPA3-Personal, слід вибирати його. В якості заміни Pre-Shared Key, про проблеми якого вже сказано вище, в WPA3 використовується метод аутентифікації SAE [18].

В основу роботи покладено принцип рівноправності пристроїв. На відміну від звичайного сценарію, коли один пристрій оголошується як такий, що надсилає запит (клієнт), а другий - як такий, що встановлює право на під'єднання (точка доступу або маршрутизатор) і вони обмінюються повідомленнями по черзі, у випадку з SAE кожна зі сторін може послати запит на з'єднання, після чого відбувається відправлення засвідчувальної інформації. Під час під'єднання та

ідентифікації використовується метод dragonfly handshake, із застосуванням криптографічного захисту для запобігання крадіжки пароля (що було продемонстровано в попередньому розділі).

SAE надає захист від атаки з перевстановленням ключа (Key Reinstallation Attacks, KRACK), а також від найпоширеніших атак за словником, коли комп'ютер перебирає безліч паролів, щоб підібрати підходящий для розшифровки інформації, отриманої під час PSK-з'єднань.

Одним з найважливіших пунктів є зміна передвстановленого паролю. Доступною довжиною паролю є символьно-чисельна комбінація від 8 до 63-ох знаків. Довгий та складний пароль нівелює загрозу атаки шляхом підбору.

Не менш важливим є приховування SSID. В цьому випадку точка доступу перестає відкрито сповіщати потенційних клієнтів про наявність мережі з цим ім'ям. За ідеєю, тепер під‘єднатися буде можливо тільки якщо знати ім'я мережі, тип шифрування і пароль.

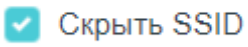

Рис.3.19. Зупинка широкомовної трансляції імені мережі

При прихованому SSID, у відкритий доступ все одно транслюється інший ідентифікатор - BSSID (Basic Service Set Identifie). Тому сканери мереж Wi-Fi можуть без особливих зусиль визначити потрібні параметри. Однак необхідність докласти додаткових зусиль для виявлення прихованих Wi-Fi мереж в рази знижує активність бажаючих протестувати точку доступу на проникнення.

Увімкнення фільтрації MAC-адрес. Створення таблиці (списку) дозволених пристроїв, що можуть підключитися до мережі, використовуючи їх MAC та IP-адреси.

Имя устройства	MAC-адрес	IP-адрес	Привязать	Изменить
---	48-FD-A3-F0-68-6E	192.168.0.100		
DESKTOP-268CC4O	EC-2E-98-08-CB-E1	192.168.0.101		
HONOR_8S-65150e89afd2966a	24-DA-33-98-DD-3D	192.168.0.103		
DESKTOP-268CC4O	EC-2E-98-08-CB-E1	192.168.0.105		

Рис.3.20. Список дозволених пристроїв для точки доступу

Слід зазначити, що в бездротових мережах для захисту від стеження за пристроями (щоб зловмисники не могли отримати точні дані про реальних клієнтів мережі) часто використовують підстановку MAC-адрес. Тому цей спосіб годиться тільки для внутрішнього периметра мережі і вимагає вимкнути функцію підстановки MAC на пристроях (необхідно прописати в налаштуваннях дозволені MAC-адресу та ім'я хоста). В такому випадку, для партнерів, клієнтів та інших відвідувачів офісу рекомендується створити гостьову мережу Wi-Fi, адже не внесені в таблицю доступу пристрої не зможуть підключитися до основної мережі.

Проведення постійного моніторингу мережі дозволяє своєчасно виявити атаку методом Roque AP і швидко змінити SSID для перешкоджання пристроям мережі випадково приєднатися до точки доступу зловмисника, що намагається таким чином перехопити паролі чи іншу конфіденційну інформацію.

Впровадження вищеназваних мір захисту дозволить підвищити рівень мережі простого користувача до такої ступені, коли зиск від злому буде набагато меншим за затрачені зусилля. Але для підприємств важливим є використання більш комплексних засобів захисту.

Для покращення безпеки в організації доцільно використовувати UTM-системи як засіб, що поєднує в собі функції антивіруса, брандмауера, систему

виявлення вторгнень тощо. Допускається також використання перерахованих вище засобів і поодинці, що теж має позитивний вплив на безпеку мережі.

Брандмауери слугують першою лінією захисту, відстежуючи і регулюючи трафік між захищеною внутрішньою мережею і зовнішніми мережами, такими як Інтернет. Вони забезпечують дотримання політик безпеки, блокуючи несанкціонований або шкідливий трафік, дозволяючи при цьому законний зв'язок, не даючи зловмисникам використовувати відкриті порти або отримувати доступ до чутливих систем.

IDS забезпечують додатковий захист, аналізуючи мережевий трафік на наявність аномалій, вторгнень або зловмисних дій в режимі реального часу. Ці системи не лише виявляють потенційні загрози, але й забезпечують автоматичне реагування, наприклад, блокують підозрілі IP-адреси або ізолюють скомпрометовані сегменти мережі, зводячи до мінімуму ризик пошкодження. Наприклад, в разі атаки на WPS вони можуть визначити, що невстановлений пристрій постійно намагається під’єднатися до мережі, раз за разом отримаючи команду деаутентифікації.

VPN забезпечують безпечну та конфіденційну передачу даних через Інтернет, шифруючи з'єднання між пристроями та мережею. Це особливо важливо для віддалених працівників або мобільних користувачів, які отримують доступ до корпоративних ресурсів, оскільки захищає конфіденційну інформацію від перехоплення або стеження. Тобто в разі злому мережі, зловмиснику доведеться ще й дешифрувати весь вихідний та вхідний трафік, що, за умови потужних алгоритмів шифрування мереж VPN, зводить нанівець ризик витоку даних.

Важливу роль у забезпеченні безпеки установи відіграють центри інформаційної безпеки (SOC). Їх головні задачі – моніторинг роботи засобів захисту інформації (СЗІ) та реагування на інциденти. SOC-центри можуть бути внутрішніми (як структурний підрозділ компанії) або зовнішніми (комерційні або аутсорсингові). Фахівці цих центрів постійно контролюють інформацію про стан безпеки, що надходять від засобів описаних вище, з метою оперативного усунення загроз [28].

Використовуючи ці технології поодинці чи в комплекті UTM, компанії можуть значно знизити ризик витоку даних, несанкціонованого доступу та інших кіберзагроз. Вищенаведені заходи не лише захищають цілісність і конфіденційність мережі, але й зміцнюють довіру до її надійності.

Висновки до розділу 3

Під час проведення тестування безпеки Wi-Fi мережі було використано інструменти Wifite, Reaver, HashCat та інші методи аналізу уразливостей. У результаті проведеної роботи вдалося виявити недоліки у захисті мережі, підсумувати їх і розробити рекомендації щодо покращення безпеки Wi-Fi.

ВИСНОВКИ

Безпека бездротових мереж є життєво важливим компонентом сучасних систем зв'язку, забезпечуючи цілісність і конфіденційність даних, що передаються між мільйонами різних пристроїв щосекундно. В процесі виконання роботи було досліджено фундаментальні аспекти функціонування бездротових мереж, розглянуто різні їх типи та їх відповідні стандарти. Особливу увагу було приділено стандарту IEEE 802.11, оскільки технологія його реалізації Wi-Fi грає важливу роль у функціонуванні нинішнього суспільства. Проведене дослідження підкреслює складність захисту бездротового зв'язку у взаємопов'язаному світі.

Розуміння систем безпеки бездротових мереж має важливе значення, оскільки зловмисники постійно вдосконалюють свої методи, намагаючись знайти слабкі місця навіть у найсучасніших системах. Тестування цих систем має вирішальне значення для виявлення вразливостей до того, як вони будуть використані. За допомогою змодельованих атак компанії та приватні особи можуть розробити сильніший захист і завчасно усунути прогалини в мережевій безпеці. Тестування дає практичний погляд на теоретичний захист, гарантуючи, що заходи безпеки не тільки добре розроблені, але й стійкі в реальних умовах.

Було проаналізовано та досліджено спеціалізовані інструменти та утиліти, доступні в Kali Linux, відомій своїм широким набором можливостей для тестування безпеки. Доступність, відкритий вихідний код і прозорість розробки забезпечують надійну платформу як для фахівців з безпеки, так і для початківців з криптозахисту. ОС об'єднує широкий спектр інструментів, що спрощує процес оцінки вразливостей і тестування на проникнення в мережу.

У практичній частині було використано вищенаведені інструменти ОС Kali для демонстрації реальних сценаріїв тестування, успішно отримуючи мережеві ключі. Ці вправи підкреслюють важливість розуміння інструментів і методології, що використовуються потенційними зловмисниками для посилення захисних заходів. Функції безпеки, розглянуті в третьому розділі, такі як протоколи

шифрування і механізми виявлення вторгнень, є життєво важливими для зменшення вразливостей і підвищення стійкості мережі.

Проведене дослідження підкреслює подвійну роль тестування безпеки: виявлення слабких місць у бездротових мережах і керівництво розробкою більш надійних систем безпеки. Комплексний захист вимагає як надійних протоколів безпеки, так і проактивного тестування. Оскільки мережі стають все більш складними і взаємопов'язаними, важливість ретельного тестування і постійного вдосконалення заходів безпеки неможливо переоцінити. Зрештою, захист бездротових мереж захищає не лише дані, але й довіру та надійність, від яких залежить сучасна цифрова взаємодія.

ПЕРЕЛІК ПОСИЛАНЬ

1. Пахомова В., Назарова Д. Organizing wireless network at marshalling yards using the bee method / Вісник Дніпропетровського національного університету залізничного транспорту. – 2020. – с. 60 -73.

2. ISM Bands Around the World [Електронний ресурс] / Altium Designer. – Режим доступу: https://resources.altium.com/p/ism-bands-around-world. – Дата звернення: 12.10.2024 р.

3. Salazar J. Wireless networks: 1st Edition / Prague: Czech Technical University of Prague, Faculty of Electrical Engineering, 2017. – 37 с.

4. Самойленко М.Ю. Принципи застосування технології Інтернет речей у сучасному світі техніки – Київ: Київський національний університет імені Тараса Шевченка, 2020. – 7 с.

5. 802.15 – Wireless Personal Area Network (WPAN) [Електронний ресурс] / Вікі ЦУСУ. – Режим доступу: https://wiki.cusu.edu.ua/index.php/802.15_–_*Wireless_Personal_Area_Network*(WPAN). – Дата звернення: 12.10.2024 р.

6. Harahap B.S.D., Silalahi J., Saragih A., Pandia R.E., Sitompul D. Wireless Networking: How Wi-Fi Works and the Different Types of Wireless Networks / Медан: Навчальна програма D3 «Інженерія інформатики», факультет професійної освіти, Університет Північної Суматри, січень 2023 р. – 7 с.

7. The Internet of Things and Big Data [Електронний ресурс] / Pure Storage. – Режим доступу: https://www.purestorage.com/uk/knowledge/big-data/internet-of-things-and-big-data.html. – Дата звернення: 15.10.2024 р.

8. Cyber Security Breaches Survey 2021 [Електронний ресурс] – Режим доступу: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021. – Дата звернення: 15.10.2024 р.

9. Wi-Fi [Електронний ресурс] – Режим доступу: https://www.tp-link.com/ru/wifi/. – Дата звернення: 17.10.2024 р.

10. Asad Abbas, Muhammad Taha Jilani1, Muhammad Khalid Khan Comparative Analysis of Wireless Technologies for Internet-of-Things Based Smart Farm / Karachi Institute of Economics and Technology, Karachi, Pakistan – лютий, 2017 р. – 6 с.

11. The Evolution of Wi-Fi Technology and Standards [Електронний ресурс] – Режим доступу: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/. – Дата звернення: 18.10.2024 р.

12. Ad-Hoc [Електронний ресурс] – Режим доступу: https://ru.nettech.ua/news/ad-hoc. – Дата звернення: 18.10.2024 р.

13. Wireless Network Security: WEP, WPA, WPA2 & WPA3 Explained – Режим доступу: https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks/. – Дата звернення: 19.10.2024 р.

14. Безпека WiFi: історія небезпеки WEP, WPA і WPA2 [Електронний ресурс] – Режим доступу: https://e-server.com.ua/uk/poradi/bezpeka-wifi-istoriia-nebezpeki-wep-wpa-i-wpa2?srsltid=AfmBOooy8Z2scP7LrOAXoowymwNLAt7q2-1-7NIZPtx6vUUQX83NY3Lw. – Дата звернення: 22.10.2024 р.

15. WPA тепер може бути зламаний за 1 хвилину WPA2 [Електронний ресурс] – Режим доступу: https://habr.com/ru/articles/68156/. – Дата звернення: 11.12.2024.

16. WiFi security: history of insecurities in WEP, WPA and WPA2 [Електронний ресурс] – Режим доступу: https://security.blogoverflow.com/2013/08/wifi-security-history-of-insecurities-in-wep-wpa-and-wpa2/. - Дата звернення: 22.10.2024 р.

17. Гуренко М.В., Круогла А.В. Дослідження захищеності wi-fi мережі з WPA/WPA2 Personal шифруванням – Київ, Державний університет телекомунікацій, 2022 р. – 10 с.

18. WPA3 покращена безпека мережі [Електронний ресурс] – Режим доступу: https://www.tp-link.com/ru/wpa3/. - Дата звернення: 26.10.2024 р.

19. Wireless Security Protocols: WEP, WPA, WPA2, and WPA3 [Електронний ресурс] – Режим доступу: https://www.netspotapp.com/blog/wifi-security/wifi-encryption-and-security.html?form=MG0AV3. – Дата звернення: 30.10.2024 р.

20. The KRACK Wi-Fi Vulnerability Explained in Plain Terms [Електронний ресурс] – Режим доступу: https://heimdalsecurity.com/blog/the-krack-wi-fi-vulnerability/. – Дата звернення: 03.11.2024 р.

21. Man in the Middle (MITM) Attack [Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/. – Дата звернення: 05.11.2024 р.

22. Kasowaki, L., Yusef, O. The Human Factor in Cybersecurity: Addressing Social Engineering and Insider Threats – 23 грудня, 2023 р. – 9 с.

23. Горбань Г. В. Операційна система Linux : навчальний посібник / Г. В. Горбань, І. О. Кандиба. – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2019. – 276 с.

24. The History of Kali Linux Distribution [Електронний ресурс] – Режим доступу: https://www.ubuntumint.com/kali-linux-history/. – Дата звернення: 15.11.2024.

25. 10th Anniversary & Kali's Story [Електронний ресурс] – Режим доступу: https://www.kali.org/blog/10-years/#kalis-name. – Дата звернення: 22.11.2024.

26. 25 Best Kali Linux Tools [Електронний ресурс] – Режим доступу: https://phoenixnap.com/kb/kali-linux-tools. – Дата звернення: 22.11.2024.

27. Understanding RockYou.txt: A Tool for Security and a Weapon for Hackers [Електронний ресурс] – Режим доступу: https://www.keepersecurity.com/blog/2023/08/04/understanding-rockyou-txt-a-tool-for-security-and-a-weapon-for-hackers/. - Дата звернення: 22.11.2024.

28. Гончарук, І. Д. Технічні системи захисту інформації / Державний університет телекомунікацій, Кафедра систем і технологій кібербезпеки. – Київ, 2024. – 2 с.