Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіті другий (магістерський)

Дослідження вразливостей безпровідних мереж шляхом реалізації тестового проникнення
(тема)

Виконав:
здобувач 2 року навчання,
групи ІМІм-23-1
Курочкін О.О.
(прізвище, ініціали)

Спеціальність 172 Електронні комунікації та радіотехніка
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник: проф. Безрук В.М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Безрук В.М.
(підпис) (прізвище, ініціали)

2025 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ / Курочкін О.О. /
(підпис) (прізвище та ініціали)

Керівник _____ / Безрук В.М. /
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій

Кафедра Інформаційно-мережної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 172 Електронні комунікації та радіотехніка

(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Інформаційно-мережна інженерія

(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
« 28 » жовтня 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Курочкіну Олександру Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження вразливостей безпровідних мереж шляхом реалізації тестового проникнення

затверджена наказом по університету від« 28» жовтня 2025 р. № 1148 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 21 січня 2025 р.

3. Вхідні дані до роботи Дослідити фактори, які містять у собі потенційні ризики безпеки бездротових мереж; виконати аналіз типів атак, які може бути реалізовано потенційним зловмисником відносно мереж WiFi; виконати дослідження специфіки підготовчих дій до проведення типових атак; дослідити процеси тестового проникнення до мережі WiFi за різними сценаріями; розробити рекомендації, спрямовані на збільшення захищеності мереж WiFi.

4. Перелік питань, що потрібно опрацювати у роботі Вступ

1. Мережі WiFi як, одна з компонент інформаційного середовища

2. Засоби реалізації атак на мережі WiFi

3. Реалізація тестового проникнення до WiFi мережі

4. Реалізація тестового зламу точки доступу WiFi з використанням засобу Airgeddon

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) слайди презентації в форматі Power Point (назва та мета роботи, чинники розповсюдженості мереж WiFi, поширені механізми зламу мереж WiFi, тестове проникнення до мережі з використанням Aircrack-ng, тестове проникнення до мережі з використанням Airgeddon, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Вступ	30.10.2024	виконано
2	Мережі WiFi як, одна з компонент інформаційного середовища	05.11.2024	виконано
3	Засоби реалізації атак на мережі WiFi	20.11.2024	виконано
4	Реалізація тестового проникнення до WiFi мережі	07.12.2024	виконано
5	Реалізація тестового зламу точки доступу WiFi	25.12.2024	виконано
6	Висновки	06.01.2025	виконано
7	Оформлення пояснювальної записки	07.01.2025	виконано

Дата видачі завдання 28 жовтня 2024 р.

здобувач Курочкін О.О.
(підпис)

Керівник роботи _____ проф. Безрук В.М.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 74 с., 29 рис., 23 джерела, 2 додатки.

Об'єкт дослідження – методи та засоби зламу бездротових мереж.

Мета роботи – дослідити можливості та порядок застосування інструментів та засобів реалізації тестового зламу бездротової мережі.

Виконується огляд вразливостей бездротових мереж та чинників, які зумовлюють їх появу. Розглядаються типові схеми та сценарії атак. Досліджуються інструменти реалізації атак на бездротові мережі за сценаріями Pixie Dust та Evil Twin з використанням спеціалізованих утиліт. Розробляються рекомендації зі збільшення захищеності мереж WiFi.

WIFI, KALI LINUX, PIXIE DUST, EVIL TWIN, HANDSHAKE, WPA/WPA2, SSID, ТОЧКА ДОСТУПУ, БЕЗДРОТОВИЙ СЕГМЕНТ.

THE ABSTRACT

Explanatory note: 7472 p., 29 fig., 23 sources, 2 app.

The object of research is Methods and means of hacking wireless networks.

The purpose of the work is to investigate the possibilities and procedure for applying tools and tools for implementing a test hacking of a wireless network.

An overview of wireless network vulnerabilities and factors that cause them to appear is performed. Typical attack schemes and scenarios are considered. Tools for implementing attacks on basedrot networks based on Pixie Dust and Evil Twin scenarios using specialized utilities are studied. Recommendations are being developed to increase the security of WiFi networks.

WIFI, KALI LINUX, PIXIE DUST, EVIL TWIN, HANDSHAKE, WPA/WPA2, SSID, ACCESS POINT, WIRELESS SEGMENT.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 9
ВСТУП 10
1 МЕРЕЖІ WIFI ЯК, ОДНА З КОМПОНЕНТ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА 12
1.1 Місце та роль бездротових мереж WiFi як складової мережевої інфраструктури 12
1.2 Тенденція щодо розширення частки бездротових комунікацій 14
1.3 Поширені механізми зламу мереж WiFi 16
1.3.1 Підходи до реалізації атак на Wi-Fi-мережі 16
1.3.2 Підбір WEP-ключа 16
1.3.3 Соціальна інженерія 17
1.3.4 Brootforce-атака 20
1.3.5 Метод підбору паролю зі спеціалізованих баз 21
1.3.6 Метод рукопотискань 22
2 ЗАСОБИ РЕАЛІЗАЦІЇ АТАК НА МЕРЕЖІ WiFi 24
2.1 Aircrack-ng 24
2.2 Засіб CoWPAtty 25
2.3 Утиліта Void11 25
2.4 Типізовані рішення на базі скриптів 27
2.5 Airgeddon 28
2.6 Попередні висновки 29
3 РЕАЛІЗАЦІЯ ТЕСТОВОГО ПРОНИКНЕННЯ ДО WI-FI МЕРЕЖІ 30
3.1 Загальна стратегія реалізації зламу мережі 30
3.2 Апаратні засоби, необхідні для зламу мережі 30
3.3 Реалізація тестового зламу точки доступу Wi-Fi з використанням Aircrack-ng 31
3.3.1 Налаштування бездротового адаптеру 31
4 РЕАЛІЗАЦІЯ ТЕСТОВОГО ЗЛАМУ ТОЧКИ ДОСТУПУ WIFI З ВИКОРИСТАННЯМ ЗАСОБУ AIRGEDDON 37
4.1 Апаратні засоби, необхідні для використання Airgeddon 37
4.2 Ініціалізація бездротового адаптеру 38
4.3 Інтеграція словника 38

4.4 Клонування головного модулю Airgeddon 38
4.5 Запуск Airgeddon 39
4.6 Реалізація атак на WiFi-мережі 40
4.6.1 Атака на WEP 40
4.6.2 Атака на WPS 45
4.6.3 Атака на мережі WPA/WPA2 48
4.7 Заходи з підвищення безпеки бездротових мереж WiFi за результатами реалізації тестових зламів 53
ВИСНОВКИ 55
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 57
ДОДАТОК А СЛАЙДИ ПРЕЗЕНТАЦІЇ 59
ДОДАТОК Б ТЕЗИ КОНФЕРЕНЦІЇ 66

ПЕРЕЛІК СКОРОЧЕНЬ

WiFi – технологія бездротових локальних мереж з пристроями на базі стандартів IEEE 802.11;

IIoT – (Industrial Internet of Things) – промислова версія IoT;

IMT2020/5G – високошвидкісна телекомунікаційна технологія покоління 5G;

WiMax – високошвидкісна телекомунікаційна технологія, що забезпечує універсальний бездротовий зв'язок на великі відстані;

LTE, LTE-A – (Long-Term Evolution) – стандарти високошвидкісного бездротового зв’язку, які належать поколінням 3,5G та 4G;

HSPA, HSPA+ – (High Speed Packet Access) – технології високошвидкісного бездротового зв’язку, надбудова над WCDMA/UMTS;

UMTS – (Universal Mobile Telecommunications System) – технологія мобільного обміну даними третього покоління;

DoS – (Denial-of-service) – атака «відмова у обслуговуванні»;

WEP – (Wired Equivalent Privacy) – протокол безпеки Wi-Fi;

AP – (Access Point) – точка доступу;

WPA/WPA2 – (Wi-Fi Protected Access) – базова та оновлена версії протоколу безпеки Wi-Fi;

GPU – (Graphics Processing Unit) – графічний процесор;

CUDA – (Compute Unified Device Architecture) – програмно-апаратна архітектура паралельних обчислень;

WPA-PSK – спрощений механізм аутентифікації у стандарті WPA;

WPS – (Wi-Fi Protected Setup) – стандарт (та однойменний протокол) напівавтоматичного створення мережі Wi-Fi.

ВСТУП

Мережеву інфраструктуру будь-якого підприємства, установи чи приватного домоволодіння сьогодні важко уявити без існування бездротових сегментів. Їхня роль сьогодні не обмежується лише забезпеченням доступу до Всесвітньої мережі для мобільних терміналів, розповсюджуючись також на:

– забезпечення середовища для бездротового підключення стаціонарних ПК та оргтехніки для заощадження часу розгортання мережі або в умовах, коли побудову СКС з тих чи інших причин ускладнено;

– надання спрощеної взаємодії з рядом специфічних пристроїв, таких, як WiFi-камери, принтери і т.д.

Безумовна зручність та простота розгортання мереж WiFi, прийнятні показники обміну даними та майже повна сумісність між собою пристроїв різних виробників та різних стандартів зумовила широку розповсюдженість WiFi-пристроїв.

Так, суттєвий відсоток роутерів Consumer-сегменту оснащується WiFi-модулем, який є активованим за замовчуванням, при цьому сьогодні майже неможливо знайти мобільний термінал, який не має підтримки WiFi. Більш того, розгортання бездротового сегменту зазвичай зводиться до включення точки доступу до мережі та внесення паролю на клієнтських пристроях.

З іншого боку, така ситуація я потенційно небезпечною, як така, що створює передумови до ймовірного зламу мережі зловмисником, так як [1, 2]:

– користувачами ігноруються додаткові заходи з безпеки, які напряму не відносяться до процесу налаштування зв’язку з точкою доступу;

– нерідко як під час першого запуску точки доступу, так і далі, користувач застосовує стандартний ключ, надрукований на корпусі пристрою.

Окрім зазначеного, слід брати до уваги те, що на сьогодні фактично для усіх протоколів безпеки WiFi (включаючи механізми шифрування даних) виявлено недоліки, експлуатація яких дає зловмиснику потенційні можливості успішної реалізації кібератак [3].

Типів атак, які спрямовані саме на мережі WiFi, та які сьогодні можна вважати результативними, існує дуже велика кількість. Це може свідчити як про привабливість даних мереж для зловмисника, так і про існування високого рівня небезпеки для даних мереж та необхідність їх захисту а також аудиту

захищеності для того, щоб виявити і надалі – усунути уразливості у рамках тієї чи іншої мережі на рівні окремих точок доступу.

Одним з підходів до реалізації аудиту мережі WiFi є виконання її тестового зламу. Отже, усе зазначене вище свідчить щодо актуальності теми роботи.

1 МЕРЕЖІ WIFI ЯК, ОДНА З КОМПОНЕНТ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

1.1 Місце та роль бездротових мереж WiFi як складової мережевої інфраструктури

Використання бездротового способу підключення до мережі має ряд переваг порівняно з випадком фіксованого способу доступу, серед яких наступні:

– мобільність клієнтських терміналів у межах усієї зони стійкого прийому сигналу;

– відсутність необхідності використання кабелів на ділянці клієнт-мережевий пристрій і, як наслідок – заощадження коштів та відсутність необхідності слідкувати за фізичним станом кабелів;

– легкість підключення нових клієнтів до мережі – за великим рахунком, для цього користувачеві достатньо знати ім’я мережі та пароль доступу.

Серед технологій бездротового доступу найширшого розповсюдження набуло сімейство WiFi (перелік стандартів 802.11), на базі яких сьогодні забезпечується підключення до мережі (рис.1.1):

– АРМ користувачів, таких, як планшети та ноутбуки;

– смартфонів;

– елементів IoT на кшталт автоматизованих вузлів, датчиків, фото- та відеокамер і т.д.;

– мобільних платіжних терміналів.

Окрім, власне, забезпечення доступу до мережі, на базі бездротових технологій реалізовано велику кількість додаткових можливостей, як-то, наприклад, друк документів зі смартфона прямим доступом до WiFi-принтерів, багатофункціональних пристроїв тощо.

У сутності, мережі WiFi сьогодні є окремим сегментом мережевої інфраструктури, що характеризується зручністю користування та спрощеним порядком клієнтських підключень.

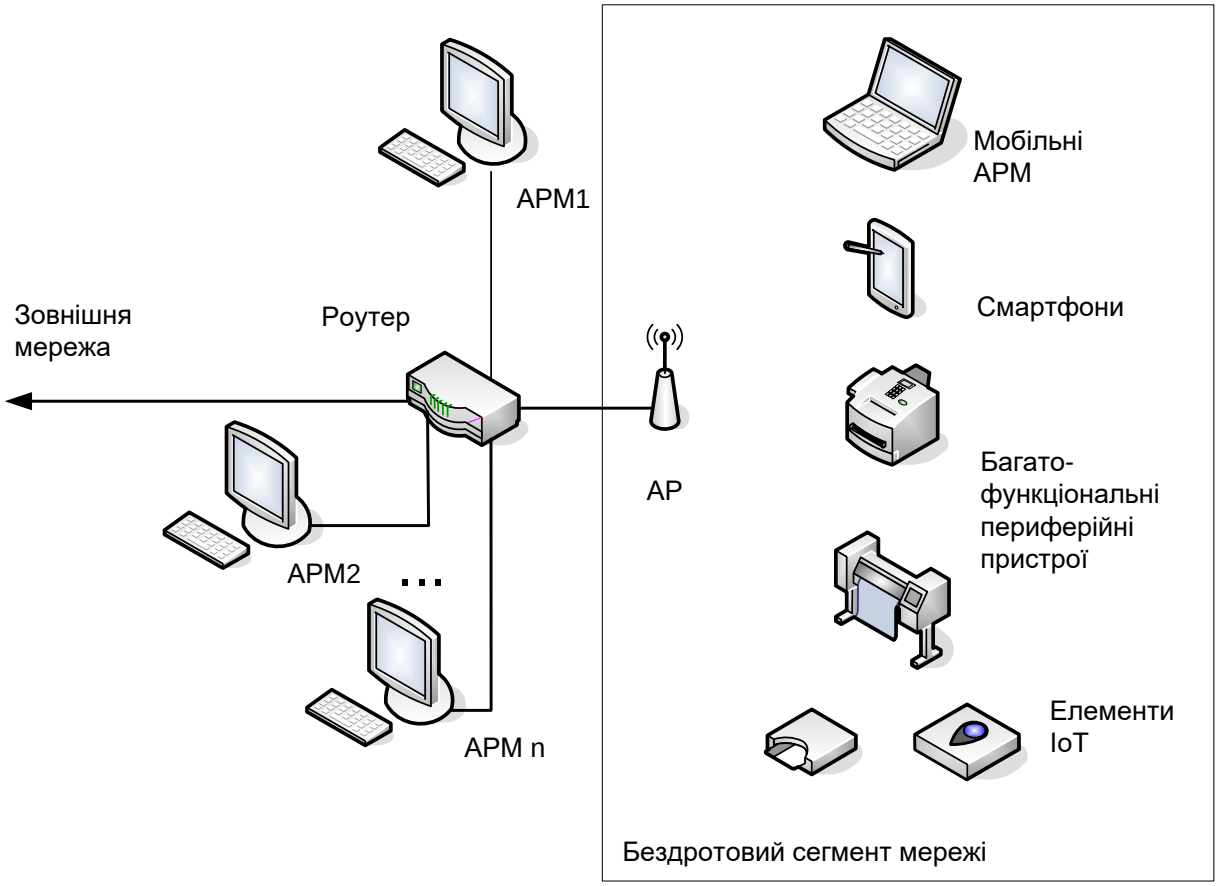

Рисунок 1.1 – Типові клієнти бездротового сегменту мережі

У свою чергу, поширеності саме технологій сімейства WiFi з-поміж інших технологій бездротового доступу сприяли такі фактори, як [4]:

– суттєво вищі швидкісні показники порівняно з бездротовими технологіями IIoT;

– можливість налагодити локальну стійку зону прийому рівня будівлі, поверху чи окремого офісу (з радіусом 30-100 м);

– відсутність необхідності передавачів високої потужності та складного конфігурування активного обладнання, а також на кілька порядків менша собівартість, порівняно з випадками IMT2020/5G, WiMax, LTE, LTE-A, HSPA, HSPA+ та UMTS;

– незначна ймовірність виникнення колапсів навіть для випадків одного зі старіших стандартів - 802.11b;

– легкість підключення та налаштування бездротових точок доступу без необхідності мати спеціалізовані навички.

1.2 Тенденція щодо розширення частки бездротових комунікацій

Останні роки намітилася чітка тенденція щодо зміни технологічної парадигми стосовно способів підключення кінцевих пристроїв до мережевих ресурсів.

При цьому, може бути виокремлено 3 окремих стадії перебігу даних змін [3].

Так, традиційно комунікація клієнтських терміналів з мережевим середовищем здійснювалася з використанням однієї з технологій мереж доступу фіксованого типу (Ethernet-сімейство, Token Ring тощо). Тобто, виробником за замовчуванням на фізичному рівні було передбачено наявність хоча б одного порту, який давав змогу з'єднувати кінцевий вузол з мережевим комунікаційним пристроєм. Також існувала можливість бездротового з'єднання, для чого використовувалися зовнішні мережеві адаптери.

Згодом, синхронно з розвитком стандартів WiFi, переважна більшість виробників почала додатково оснащувати клієнтські пристрої інтегрованими бездротовими адаптерами. Спочатку – для ноутбуків а пізніше – навіть для стаціонарних ПК, тим самим даючи змогу користувачеві самостійного вибору зі способу підключення.

Зараз же, наприклад, хоча для стаціонарних ПК ситуація, у цілому, не змінилася, проте значна частина виробників відмовилася від оснащення ноутбуків Consumer-сегменту портами RG-45. Це пояснюється, по-перше, впливом тренду на забезпечення компактності подібних пристроїв а по-друге – тим міркуванням, що середня кількість бездротових точок доступу поступово стає співрозмірною кількості клієнтських мереж. Тобто, ймовірність того, що користувацький ноутбук чи смартфон може під'єднатися до довільної WiFi-мережі, наближається до 1.

Водночас, можливість підключення до мережі на базі технології фіксованого доступу залишається за умови використання конверторів інтерфейсу USB/RJ-45. Проте, на сьогодні такий спосіб інтеграції з мережевим середовищем не отримав значного поширення з досить банальної причини, а саме – брак вільних USB-портів. Справа у тім, що consumer-пристрої, за невеликими виключеннями, не мають більш 3-х USB-портів, з яких щонайменше 1 задіяно для бездротового підключення маніпулятору «миша» а інший – для підключення зовнішнього накопичувача. Тому в умовах, коли 3-й порт

відноситься до стандарту USB 2.0, на його базі отримати швидкісний обмін даними неможливо.

У підсумку, складаються умови, що, за винятком фіксованих кінцевих пристроїв, переважна більшість мобільних терміналів є клієнтами WiFi-мережі.

На тлі цього, орієнтований сумарний обсяг точок доступу WiFi у масштабі світу сьогодні становить не менш, ніж 11x106 одиниць. У свою чергу, загальний трафік мереж WiFi дорівнює величині близько 115x1018 Байт/місяць [4, 5].

Не в останню чергу означена тенденція було спричинена швидкісними показниками технологій, які, поряд з іншими ключовими показниками кожного зі стандартів, наведено у таблиці 1.1 [3].

Таблиця 1.1 – Головні параметри технологій сімейства WiFi

Стандарт	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
Рік	1997	1999	1999	2003	2009	2014	2017-2019
Частота	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz	2,4 GHz/ 5 GHz	5 GHz	2,4 GHz/ 5 GHz
Частотні канали	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160 MHz
Пікова канальна швидкість	2 Mbit/s	11 Mbit/s	108 Mbit/s	54 Mbit/s	150-600 Mbit/s	0,433-6,77 Gbit/s	0,433-10 Gbit/s
Пікова реальна швидкість	Близько 1 Mbit/s	5 Mbit/s	40 Mbit/s	24 Mbit/s	220 Mbit/s	від 200 Mbit/s	Від 400 Mbit/s
Тип модуляції	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM	OFDM, OFDMA
Тип кодування	DQPSK	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	1024-QAM, 5/6
Макс. кількість тонів OFDM	-	-	64	64	128	512	2048
Рознесення субтонів	-	-	312,5 КГц	312,5 КГц	312,5 КГц	312,5 КГц	78,125 КГц

Також, стосовно додаткових чинників розповсюдженості мереж WiFi обов’язково слід зазначити, такі, як:

– прагнення з боку компаній надати можливість використання достатньо стабільного та продуктивного зв’язку як співробітникам, так і потенційним (відвідувачам) та реальним клієнтам;

– надання безкоштовного бездротового доступу до Всесвітньої мережі на базі WiFi на території розважальних закладів, торгівельних центрів та закладів громадського харчування, що є нічим іншим, як вдалим маркетинговим ходом з боку їх власників.

1.3 Поширені механізми зламу мереж WiFi

1.3.1 Підходи до реалізації атак на Wi-Fi-мережі

За характером впливу та метою проведення атаки на бездротові мережі Wi-Fi можна поділити на дві головні категорії, а саме [6-8]:

– атаки, спрямовані на перешкоджання функціонування мережі (DoS-атаки);

– атаки, головним завданням яких є проникнення до атакованої мережі.

При цьому, беручи до уваги те, що переважна більшість атак [8] відноситься саме до другої категорії, дослідження методів та механізмів, які можуть бути задіяними у даному випадку, становлять суттєвий науковий та практичний інтерес.

Аналізуючи базу статистики успішно реалізованих атак на мережі WiFi, можемо зазначити, що найбільш часто застосовуваними та найбільш результативними можна вважати такі методи, як: [9-12]:

– handshake-метод, або метод рукопотискань;

– brootforce-атака, тобто, підбір паролю повним перебором;

– підбір WEP-ключа;

– підбір паролю зі спеціалізованих баз;

– соціальна інженерія;

– пошук паролю у режимі ручного підбору.

Далі проаналізуємо перелічені методи для того, щоб виявити найбільш ефективні з них для подальшого використання у ході реалізації тестового зламу бездротової мережі.

1.3.2 Підбір WEP-ключа

Як зазначалося раніше у розділі 1, останніми роками склалася тенденція до спрощення процесу використання мережевих пристроїв. Це привело до того, що переважна більшість виробників як бездротових Wi-Fi-роутерів, так і точок доступу, передбачають можливість швидкого підключення користувачів до мережі на базі WEP-ключа за замовчуванням, який нерідко розміщується на корпусі пристрою. Більшою мірою це справедливо для пристроїв Consumer-категорії, хоча відсоток відсоток пристроїв категорії Enterprise, для яких справедливе усе, зазначене вище, також є значним [10].

Сам процес підключення до точки доступу на базі WEP потребує виключно введення ПІН-коду, для якого справедливими є наступні твердження [13, 14]:

– довжина 8 символів;

– може бути однаковим для багатьох пристроїв одного виробника у межах однієї серії одного модельного ряду.

Звідси виходить, що у зазначених умовах пошук WEP-ключа може бути побудовано за рахунок повного перебору простору паролів. Ураховуючи його обмеженість, це може бути реалізовано за невеликий проміжок часу.

Разом з тим, у ході ранніх досліджень зі стійкості WEP було виявлено кореляцію між символами та вихідною шифрограмою. Це, у свою чергу, дозволяє побудувати процес пошуку паролю попарно. Тобто, спершу виконується підбір перших 4 символів, після чого - інших 4-х.

Отже, очевидним є те, що за цих умов час зламу додатково значно скорочується.

Інший варіант реалізації даної атаки передбачає пошук паролю серед тих, які надаються виробником за замовчуванням, замість сканування усього 8-розрядного простору можливих значень ключа.

Ураховуючи повторюваність ключа виробником, та ігнорування необхідності його зміни після первинного підключення, атака на WEP може потребувати зовсім незначних часових ресурсів.

1.3.3 Соціальна інженерія

Як специфічний, та один з найбільш продуктивних підходів до реалізації зловмисних атак на інформаційні системи, соціальна інженерія базується на використанні уразливостей не технічного, а організаційного характеру, а також людських вад та рис, притаманних людині взагалі – звичок, лінностей, неуважності чи, навпаки, надмірної уваги до тих чи інших деталей, підсвідомих симпатій та антипатій тощо [9].

Результативність зламів паролю до мережі Wi-Fi на базі соціальної інженерії є дуже високою, так, понад 90% спроб зламу є успішними.

У рамках даного підходу атаки може бути реалізовано за багатьма сценаріями. за рядом сценаріїв. Одними з найбільш широко застосовуваними серед них сьогодні є, зокрема [9]:

1. Атака на базі нової точки доступу.

Даний тип атаки передбачає створення зловмисником нової АР яка, при цьому, повинна мати таке саме ім’я, як і точка доступу, на яку планується атака. Головна умова для можливості реалізації цієї атаки – розташування фальшивої АР у зоні стійкого прийому атакованої точки доступу.

При цьому, рівень сигналу фальшивої АО має бути достатньо високим для користувачів реальної мережі – таким, щоб, за потреби, забезпечити сталий прийом.

Основою методу є твердження про високу ймовірність того, що хоча б один користувач атакованої мережі врешті решт виконає спробу підключення до фальшивої АР, вводячи при цьому пароль реальної точки доступу. Цьому сприяють такі фактори, як:

– знаходження у зоні прийому користувача реальної мережі АР зі «знайомим» ім’ям;

– високий рівень сигналу фальшивої АР, що опосередковано надає їй ознак реальної;

– ігнорування користувачем перегляну повного списку доступних мереж (частково цьому сприяє перенасиченість ефіру сигналами від сусідніх АР).

Розглянутий метод є достатньо ефективним, але лише у довготривалій перспективі. При цьому, гарантія захоплення паролю у зазначений спосіб протягом короткого терміну відсутня: атака може тривати як кілька хвилин, так і кілька днів. Це і є головним недоліком методу.

2. Використання спливаючих вікон у браузері.

У рамках реалізації даного методу застосовуються механізми завантаження спливаючих вікон у користувацький браузер. Зміст таких вікон, на перший погляд, не є підозрілим. Частіше за все користувач отримує інформацію про необхідність оновлення самого браузеру або його окремих компонент, чи прикладного ПЗ. Для цього пропонується ввести пароль до Wi-Fi точки доступу у розташованому у самому вікні полі. Приклад такого вікна зображено на рисунку 1.2.

Ефективність даного методу, у загальному випадку, не може вважатися високою за ряду причин, серед яких головними є те, що:

– технічна реалізація методу є досить складною;

– попередньо необхідно визначити множину потенційних клієнтів атакованої мережі

– ймовірність успішної реалізації атаки відсутня, як наслідок обізнаності користувачів з елементарних питань безпеки.

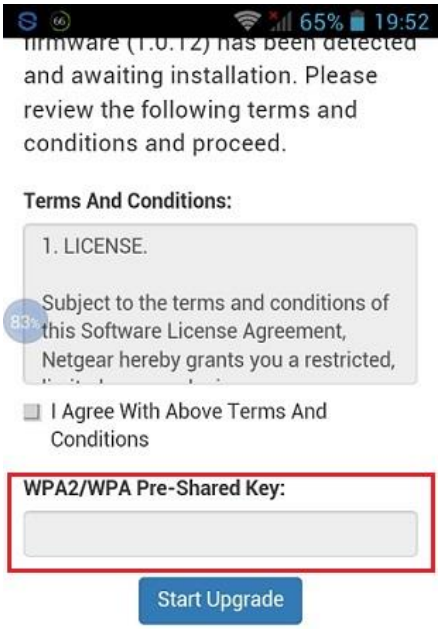

Рисунок 1.2 – Типова спливаюча сторінка, яка містить запит щодо введення паролю для оновлення мобільного браузеру

3. Використання фальшивої AP з примусовим відключенням.

У сутності, даний метод являє собою розвиток методу на базі нової точки доступу.

На відміну від базового методу, зловмисник додатково використовує спеціалізоване ПЗ, а також 2 бездротових мережевих адаптера.

Виконаємо огляд одного зі способів реалізації даного методу з використанням утиліти Wifiphisher.

У даному разі зловмисник має виконувати наступну послідовність дій:

– вибір об’єкту атаки (цільової AP) з наступним копіюванням її загальних параметрів конфігурації (її ім’я, канал тощо);

– клонування атакованої AP. Тобто, як і у базовому варіанті, зовні така точка доступу повністю схожа з оригіналом. Виключенням є те, що підключення до неї потребує введення паролю;

– примусова деаутентифікація одного або кількох користувачів атакованої AP (у сутності, це відключення користувачів від справжньої AP);

– реалізація довготривалого пригнічення радіоканалу атакованої АР, для чого використовується друга точка доступу WiFi;

– спонукання користувача ввести ключ доступу до WiFi після того, як користувач виконає спробу з'єднання з клонованою АР (додатково тут може бути використано механізм спливаючих вікон, які інформуватимуть користувача, наприклад, про необхідність оновлення того чи іншого ПЗ);

– зчитування паролю, введеного користувачем.

Зазначимо, що додаткові механізми спонукання введення паролю використовувати не обов'язково. Частіше за все користувач самостійно вводить відомий йому пароль після кількох невдалих спроб з'єднання.

Розглянутий метод є досить продуктивним, не потребує специфічних навичок та легкий у реалізації.

При цьому, у випадку даного методу говорити про гарантований злам також недоцільно (хоча ймовірність успіху досить висока), так як результат так чи інакше залежить від впливу людського фактору.

1.3.4 Brootforce-атака

Підхід на базі простого підбору паролю є ефективним для WEP-мереж, а також мереж WPA/WPA2 у випадку, коли не передбачено використання додаткових механізмів захисту. Інакше метод перетворюється на один з найменш результативних.

Це зумовлено тим, що [8,15]:

– WPA/WPA2-ключі не обмежені 8-ма символами, як для випадку WEP;

– brootforce-атаку як для WEP, так і для WPA/WPA2-мереж може бути виявлено та блоковано запити бездротового адаптеру зловмисника на рівні апаратного ідентифікатору а відтак – результативність її не гарантовано.

Зазвичай brootforce-атака блокується інструментами захисту WiFi-мереж, які забезпечують можливість встановлення обмежень на допустиму кількість запитів щодо введення паролю протягом деякого часового відрізку.

Отже, усе зазначене потенційно створює такі ймовірні сценарії реалізації атаки, як:

– значне падіння швидкості процесу перевірки паролів, на тлі чого дана атака буде позбавлена сенсу;

– результативне завершення атаки (коли пароль було підібрано);

– блокування AP зловмисника за MAC-адресою, що тягне за собою необхідність застосування нової точки доступу для подальшого розвитку та завершення атаки.

1.3.5 Метод підбору паролю зі спеціалізованих баз

Даний метод належить до т.з. атак словникового типу [9, 16]. Цей метод базується на існуючих статистичних даних, згідно з якими ряд слів, висловів, цифрово-літерних комбінацій та невеликих словосполучень досить часто використовуються як паролі, як показує рисунок 1.3.

1	123456	6	1234567890	11	qwertyuiop	16	7777777	21	google
2	123456789	7	1234567	12	mynoob	17	1q2w3e4r	22	1q2w3e4r5t
3	qwerty	8	password	13	123321	18	654321	23	123qwe
4	12345678	9	123123	14	666666	19	555555	24	zxcvbnm
5	111111	10	987654321	15	18atcskd2w	20	3rjs1la7qe	25	1q2w3e

Рисунок 1.3 – Перелік з 25 паролів, що найчастіше використовувалися у мережах на базі WEP

Так, роль паролів нерідко відіграють:

– ім’я та/або ініціали, поєднані з іншими даними користувача;

– дата народження;

– цитати та відомі вислови різними мовами, встановлені з пробілами та іншими розділовими знаками, або суцільним текстом;

– власні імена відомих осіб та персонажів, географічні назви, назви об’єктів та предметів;

– специфічні комбінації цифр та літер;

– окремі слова, терміни та назви, які у повсякденному лексиконі з тих чи інших причин (специфічність, застарілість тощо) не мають широкого вжитку (Канченджанґа, амікошонство та ін.).

Попри усе зазначене слід розуміти, що досить велика частка користувачів для налаштування AP Wi-Fi може використовувати той самий пароль, який встановлено для електронної пошти, входу до ПК чи месенджеру.

Водночас, у мережах з WEP-захистом, де ключ обмежено 8 символами, часто знаходяться паролі на кшталт «QWERTY», «parol», «12345» та інші схожі.

Окрім зазначеного, бази паролів містять у собі суттєву частку паролів, які раніше було скомпрометовано (які попередньо зазнали зламу).

У свою чергу, даний тип атаки, у сутності, являє собою особливий різновид атаки brootforce. Різниця полягає лише у тому, що під час словникової атаки виконується не повний перебір паролів у певному діапазоні величин, а виключно перебір паролів з деякої множини, що є апріорі обмеженою. Дані можуть братися як з одного, так і кількох словників.

Розглянутий тип атаки здатен забезпечити високу ймовірність успіху для випадків WEP-мереж, або для мереж будь-якого типу захисту, але лише тоді, коли питаннями безпеки займаються особи, що не мають достатньо досвіду або відповідного рівня кваліфікації.

Таким чином, даний метод злам WiFi-мережі також не надає гарантії результативності.

1.3.6 Метод рукопотискань

Рукопотискання, або handshake, являє собою процедуру обміну даними між AP бездротової мережі та клієнтом при його підключенні.

При цьому, сама процедура handshake є стандартизованою. Для обміну даними під час її перебігу послідовно виконується ряд технологічних стадій [17].

Дані, якими між собою обмінюються клієнт та AP також отримали назву handshake. В основі методу знаходяться наступні твердження:

1. Захоплення handshake може виконуватися під час спроб підключення до AP клієнтів, що мають валідний пароль.

2. Деякий обсяг handshake може містити об’єм даних, якого достатньо для розшифрування паролю до бездротової мережі.

Процес виокремлення паролю на базі зібраної handshake-інформації зводиться до повного перебору ймовірних варіантів, що зовні робить його подібним до підходу на базі brootforce.

У той же час, метод handshake суттєвим чином відрізняється від brootforce, оскільки:

– у ході реалізації «класичного» brootforce, виконуються спроби підключення до точки доступу, кожен раз – з новим паролем;

– у випадку методу «хендшейк» виконується захоплення даних, попередньо шифрованих з використанням реального паролю. Процес підбору виконується у offline-режимі.

Для підбору паролю може бути використано або процесорна потужність, або зовнішні сервіси, або можливості GPU, використовуючи CUDA.

При цьому, на відміну від brootforce, кожного ражу не здійснюється звернення до точки доступу. Наслідком цього є:

– суттєве заощадження часу за рахунок відсутності необхідності підключення для перевірки кожного чергового паролю;

– мінімізація, або повна відсутність ймовірності блокування точки доступу системою безпеки атакованої мережі.

Водночас, як свідчить статистика [10], за умови перехоплення достатньої кількості векторів ініціалізації, WiFi-мережу на базі WPA/WPA2 може бути гарантовано зламано.

Отже, розглянувши найбільш поширені методи зламу паролів у мережах WiFi, можемо зробити попередній висновок про те, що:

– гарантований злам WiFi-мережі серед розглянутих - забезпечують виключно хендшейк-методи;

– результативність методів фішингу та таких, що орієнтуються на підбір паролів, суттєвим чином залежить від «якості» пароля атакованої точки доступу;

– у випадку мультизвернень до точки доступу, можливе або тимчасове, або повне блокування адаптеру зловмисника на рівні MAC-адреси, що вимагає або за діяння нового апаратного пристрою, або маскування існуючого MAC.

Таким чином, ураховуючи вищезазначене, найбільш результативним методом для зламу паролів WiFi є метод handshake.

Виконаємо дослідження засобів, що дозволяють реалізувати метод handshake для зламу паролів WiFi.

2 ЗАСОБИ РЕАЛІЗАЦІЇ АТАК НА МЕРЕЖІ WIFI

На сьогоднішній час для зламу паролів WiFi на базі handshake існує велика кількість програмних засобів. Це є прямим наслідком того, що уразливості як WEP, так і WPA, є широковідомими. Розглянемо деякі з них.

2.1 Aircrack-ng

Утиліту Aircrack-ng може бути використано як у середовищі Windows, так у Linux-оточенні [19].

Даний засіб застосовується для реалізації зламу паролів WEP та WPA/WPA2 мереж WiFi.

На базі використання Aircrack-ng може бути побудовано атаки за сценаріями Pychkine-Tews-Weinmann а також KoreK. Кожен з зазначених сценаріїв ґрунтується на пошуку статистичних закономірностей прийнятих handshake та забезпечує при цьому вищу ефективність у порівнянні ефективними з атакою FMS, яка зараз вже вважається класичною.

До складу утиліти Aircrack-ng входить декілька компонент, серед яких наступні:

– Airmon-ng, яка застосовується для того, щоб налаштовувати бездротовий мережевий адаптер. При цьому, коректне функціонування утиліти вимагає використання мережевих адаптерів Wi-Fi, які можуть підтримувати режиму моніторингу (Monitor mode);

– Airodump-ng, яка виконує процедуру захоплення кадрів. Дана компонента вирішує завдання з прийому та наступної обробки усіх перехоплених пакетів, фіксує дані відносно параметрів атакованих мереж та зберігає дані, які далі буде використано на етапі підбору ключів;

– Aireplay-ng, завданням якої є генерування трафіку;

– компонента Aircrack-ng (однойменна з утилітою), що застосовується безпосередньо для зламу, який реалізується з використанням даних, що було попередньо зібрано компонентою airodump-ng;

– airdecap-ng, завданням якої є дешифрування перехоплених пакетів.

Отже, у сутності, Aircrack-ng являє собою пакет програмних засобів.

2.2 Засіб CoWPAtty

Утиліта CoWPAtty може використовуватися як у оточенні Windows, так і у Linux-середовищі, Android та Mac OS [8].

Засіб грунтується на використанні механізмів автоматизація атаки за словником для WPA-PSK.

При цьому, за аналогією з Aircrack-ng, запуск та управління роботою утиліти застосовується командний рядок. Водночас, роль головного параметру, необхідного для успішної реалізації атаки, відіграє перелік слів, на базі якого забезпечується ймовірність реконструювання паролю.

До переваг даного засобу слід віднести його відносно високу продуктивність.

З іншого боку, головними недоліками можна вважати довгий процес інсталяції та налаштування, а також складність для розуміння деяких його функцій.

2.3 Утиліта Void11

Засіб Void11, фактично, не може вважатися окремим інструментарієм зламу. Дана утиліта є допоміжним засобом, який застосовується паралельно з іншими інструментами, які, у свою чергу, реалізують функціонал підбору паролю [16, 19].

Отже, припустимо, що виконується атака на бездротову АР з використанням Airodump-ng (рис.2.1).

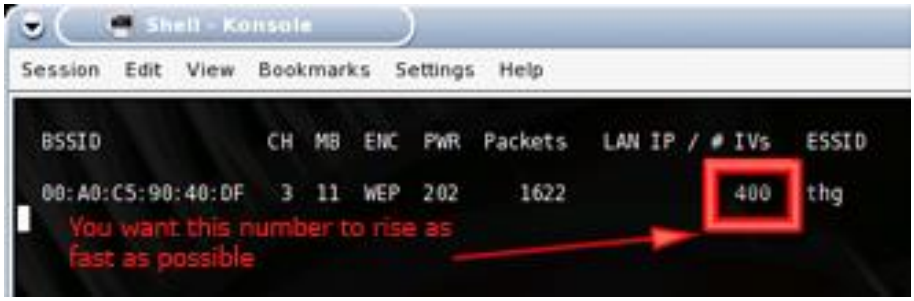

Рисунок 2.1 – Перебіг процесу перехоплення пакетів бездротової мережі з використанням утиліти Airodump-ng

Завданням Void11 є забезпечення деаутентифікації користувачів мережі бездротового доступу, так само, як це дозволяє робити Wifiphisher а також ряд аналогічних засобів. Для того, щоб обґрунтувати доцільність застосування Void11, розглянемо наступний приклад [16].

Як видно на рисунку 2.1, у лівій колонці консолі розміщено MAC-адресу бездротової AP, на яку здійснюється атака, а також заголовок BSSID.

При цьому, у ході атаки постійно збільшується як кількість перехоплених пакетів (Packet count), так і векторів ініціалізації (IV count). У свою чергу, дана залежність буде справедливою навіть тоді, коли атакована мережа буде незавантаженою, або завантаженою незначно.

Водночас, для успішної реалізації атаки важливим є лише швидкість зростання показника IV count (зміна величини Packet count може бути наслідком процесів, які жодним чином не мають відношення до атаки).

Наприклад, дану залежність може бути пояснено тією обставиною, що що суттєвий обсяг пакетів являє собою не що інше, дані об’яв бездротової AP, які за замовчуванням мають надсилатися щосекунди з частотою 10 пакетів/с.

Разом з цим, за інформацією, яку відображує лічильник IV, можна опосередковано робити висновки щодо перебігу атаки.

За існуючими статистичними даними вважається, що забезпечити гарантований злам мережі, де використовується протокол WEP та ключ, що має довжину 64 біта, можна в умовах, якщо було зібрано від 50000 до 200000 векторів ініціалізації. У свою чергу, для зламу ключа WEP довжиною 128 біт потрібно зібрати від 200000 до 700000 IV [19].

Разом з тим, під час реальної атаки при невисокій інтенсивності трафіку усередині бездротової мережі процес росту значення IV до необхідного рівня може зайняти досить тривалий час, як від декількох годин, так і навіть кількох днів.

Очевидно, що швидкість збору IV напряму впливає на тривалість усієї атаки у цілому. У такому випадку для збору достатньої кількості векторів ініціалізації може знадобитися суттєвий проміжок часу – від кількох годин, до кількох діб.

У свою чергу, для того, щоб суттєвим чином сприяти прискоренню швидкості збільшення кількості зібраних IV, необхідно додатково завантажити бездротову мережу, на яку здійснюється атака.

Так як зловмисник, перебуваючи за межами сегменту фіксованого доступу атакованої мережі не може забезпечити, наприклад, пересилання між кількома вузлами значного обсягу файлів (чи розсилання ECHO-запитів), мережу може бути завантажено з використанням Void11 за бездротовим каналом.

Щоб скористатися засобом Void11, необхідно додатково задіяти ще один ПК, який оснащено WiFi-адаптером. Після запуску Void11 починає виконуватися сценарій деаутентифікації активних клієнтів атакованої мережі. Даний процес може бути проілюстровано наступним переліком команд [16]:

```
switch-to-hostap
cardctl eject
cardctl insert
iwconfig wlan0 channel [номер каналу мережі, що
атакується]
iwpriv wlan0 hostapd 1
iwconfig wlan0 mode master
void11_penetration -D -s [MAC-адреса клієнта] -B [MAC-
адреса точки доступу] wlan0
```

Сам процес деаутентифікування клієнтів бездротового доступу відносно AP є, у сутності, їх примусовим від’єднанням від AP.

Далі, після кожного випадку деаутентифікування, клієнт атакованої WiFi-мережі в автоматичному режимі буде виконувати спроби повторного підключення до AP.

Відтак є очевидним, що у ході кожної наступної спроби клієнта буде генеруватися трафік. Це, у свою чергу, створюватиме додаткове навантаження мережі.

Клас атак, подібних розглянутій, отримали загальну назву атак відключення, атак деаутентифікування або «deauth attack».

2.4 Типізовані рішення на базі скриптів

Сьогодні відома значна кількість командних сценаріїв, які дають змогу зловмисникові успішно реалізувати злам мережа WiFi, які використовують WEP та WPA-шифрування.

Серед даного класу інструментів сьогодні одним з найчастіше використовуваних є Wifite [20].

Використовуючи Wifite та схожі інструменти, процедуру зламу паролів мережі WiFi може бути реалізовано у спосіб, який є у цілому аналогічним до попередньо розглянутого.

У свою чергу, результативність використання зазначеного інструментарію у цілому може бути аналогічною до тієї, яку забезпечують Aircrack-ag та схожі засоби.

Водночас. слід зазначити, що типізованим рішенням на базі скриптів властивий ряд недоліків, а саме:

– значна частка рішень з загального обсягу не є уніфікованими – вони є ефективними лише для певного алгоритму шифрування мережі WiFi або для певних умов зламу;

– ефективне застосування того чи іншого рішення вимагає від користувача досить глибоко вивчити склад та логіку функціонування пакету скриптів а також зрозуміти особливості їх застосування.

2.5 Airgeddon

Даний засіб можна вважати розвитком Aircrack-ag. У сутності, Airgeddon також поєднує у собі ряд окремих засобів, що реалізують функції моніторингу ефіру, збору IV та їх подальшої обробки, деаутентифікації користувачів цільової мережі тощо [21].

Засіб продемонстрував свою високу результативність атак на WEP та WPS-ключі. На відміну від Aircrack-ag є повністю автоматизованим і дозволяє зловмиснику виконати вдалу атаку навіть без достатніх знань ідеології WiFi та супутніх питань.

Єдиним недоліком Airgeddon можна вважати те, що він працює з мережевими бездротовими адаптерами не усіх виробників. Проте, розробники, зі свого боку, надають рекомендований моделей адаптерів.

2.6 Попередні висновки

Ураховуючи особливості розглянутого інструментарію, для того, щоб дослідити можливість реалізації тестового зламу мережі WiFi за найбільш ефективними сценаріями, може бути використано такі засоби, як Aircrack-ng разом з утилітою Void11, а також Airgeddon.

Вибір саме цих засобів пояснюється тим, що:

– порядок застосування та необхідний перелік дій під час реалізації атак з Aircrack-ng та Void11, а також Airgeddon, чітко визначено розробниками та вказано у довідках до зазначених інструментів. Тобто, користувачеві достатньо слідувати вказівкам без необхідності вивчення специфіки функціонування кожного з засобів;

– інструменти, обрані для дослідження процесу зламу, мають суттєву підтримку інформаційної спільноти та досить розгорнуті довідкові системи, що дозволяє усунути більшість проблем, що можуть виникати у ході інсталяції та налаштувань засобів, а також під час безпосередньо використання;

– кожен з засобів багаторазово продемонстрував свою високу результативність.

3 РЕАЛІЗАЦІЯ ТЕСТОВОГО ПРОНИКНЕННЯ ДО WI-FI МЕРЕЖІ

3.1 Загальна стратегія реалізації зламу мережі

Розглянемо сценарій виконання аудиту захищеності мережі Wi-Fi, який передбачає здійснення тестового зламу.

Бездротові мережі Wi-Fi для захисту даних застосовують ряд різних протоколів безпеки та шифрів. При цьому, атака на кожен з ним може здійснюватися різними способами. Інакше кажучи, можемо говорити про існування багатьох різних векторів атаки.

Як вже зазначалося раніше, ряд використовуваних для захисту мережі Wi-Fi шифрів та протоколів не можуть забезпечити достатнього рівня стійкості.

Відтак, загальна стратегія зламу мережі зводиться до реалізації ряду поступових атак. При цьому, першими об’єктами атаки мають бути найбільш слабкі протоколи безпеки. За рахунок цього збільшується ймовірність успіху, а також може значно скорочуватися загальний час, який витрачається для зламу.

У даному розділі тестове проникнення виконується з використанням Aircrack-ng.

При цьому, буде задіяно атаку, яка отримала назву «злий близнюк» (Evil Twin).

3.2 Апаратні засоби, необхідні для зламу мережі

У загальному випадку, вимоги для ПК, на базі якого виконується тестове проникнення з Aircrack-ng, жорстко не регламентуються. Головна вимога у даному випадку – можливість підтримки Kali Linux.

Водночас, процесорні ресурси та обсяг оперативної пам’яті розробниками вищеозначених засобів не віднесено до критичних параметрів, хоча очевидно, що від їхніх номіналів напряму залежатиме час відновлення паролю [18].

3.3 Реалізація тестового зламу точки доступу Wi-Fi з використанням Aircrack-ng

3.3.1 Налаштування бездротового адаптеру

Як вже було зазначено вище, робочим середовищем є Kali Linux. Дану операційну систему попередньо розгорнуто на базі віртуального середовища VMware.

Після завантаження ОС необхідно виконати під'єднання бездротової АР до USB-порту, а далі – здійснити процедуру ініціалізації під'єднаного WiFi-адаптеру [21].

Сама процедура ініціалізації не виконується системою автоматично, а відтак - вимагає виконання ряду послідовних дій (`VM →RemovableDevices→Ralink 802.11n USB WirelessLanCard→Connect`), як це зазначено на рисунку 3.1.

Рисунок 3.1 – Перелік дій, необхідний для ініціалізації бездротового адаптеру у системі

Наступним кроком, після ініціалізації мережевого адаптеру, необхідно виконати перевірку готовності підключеного пристрою до наступного застосування.

У цьому випадку достатнім виконати запит інформації щодо інтерфейсів, доступних у системі.

Для того, щоб мати змогу реалізувати такий запит, достатньо виконати у терміналі команду звернення до однієї з утиліт з пакету Aircrack [18]. Наприклад:

```
airmon-ng
```

Якщо означений запит було виконано успішно, при цьому, AP є активною у системі, отримаємо відповідь від Airmon-ng у вигляді, як показано рисунком 3.2.

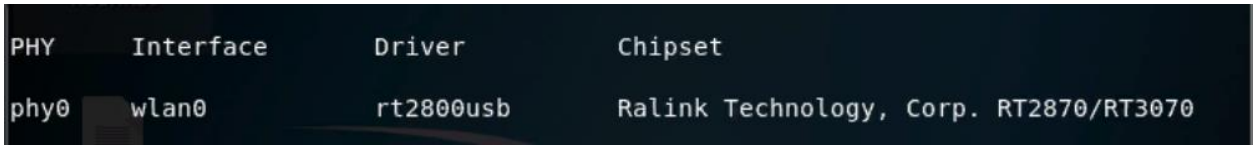

Рисунок 3.2 – Виведення інформації відносно активних WiFi-адаптерів у системі

Як можна бачити з рисунку 3.2, бездротовий адаптер Ralink 802.11n USB WirelessLanCard є активним у системі, при цьому, його асоційовано з інтерфейсом wlan0.

На наступному підготовчому кроці реалізації атаки, скориставшись отриманими даними відносно інтерфейсу, асоційованого з бездротовим адаптером, виконується переведення вже самого пристрою у режим моніторингу.

Для здійснення даної процедури достатньо виконати команду, що має синтаксис airmon-ngstart [ідентифікатор інтерфейсу].

Відтак, для нашого випадку команда переведення у режим моніторингу прийме вигляд, як зазначено далі:

```
airmon-ngstart wlan0
```

Для виконання будь-яких подальших дій попередньо слід упевнитись у тому, що у поточний час бездротову точку доступу успішно переведено до режим моніторингу.

У свою чергу, для цього достатньо у терміналі виконати перегляд відомостей, які виведено за результатом виконання вищенаведеної команди, як це видно з рисунку 3.3.

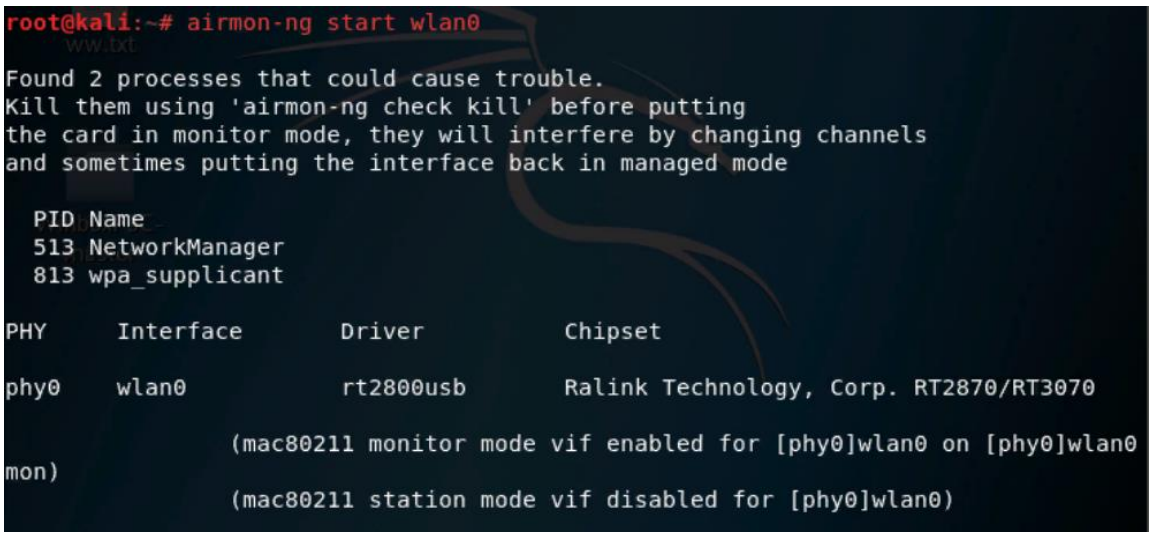

Рисунок 3.3 – Перегляд даних щодо поточного режиму функціонування адаптеру

Далі, коли АР переведено до режиму моніторингу, може бути одержано інформацію щодо присутності мереж WiFi у межах зони досяжності. Отримати вказану інформацію можемо, виконавши команду [18, 19]:

```
airodump-ng wlan0 mon
```

Результат виконання даної команди подано на рисунку 3.4.

Судячи за цим, під час виконання моніторингу оточення було виявлено досить значну кількість мереж Wi-Fi у зоні досяжності.

Для кожної з них також при цьому отримано:

– дані щодо ідентифікатору мережі (BSSID). У даному випадку це MAC-– адреси мережевих адаптерів або точок доступу;

– відомості про імена виявлених точок доступу;

– інформацію щодо застосованих протоколів безпеки (WPA2);

– дані про використані алгоритми шифрування (CCMP);

– відомості про алгоритми аутентифікації (PSK).

Отже, можна зазначити, що усі виявлені у зоні достяжності мережі потенційно є уразливими [9, 21].

Після цього виконується конфігурування утиліти для того, щоб мати змогу прослухувати одну зі знайдених мереж.

Це може бути виконано командою, що має загальний вигляд: `airodump-ng -c [номер цільового каналу] –bssid [цільовий BSSID] -w /root/Desktop/ [інтерфейс моніторингу]`.

Для подальшого дослідження процедури тестового зламу обирається BSSID 4C:ED:FB:8A:4F:C0. Приймаючи це до уваги, команда буде наступною (рис.3.5):

```
airodump-ng -c 6 –bssid 4C:ED:FB:8A:4F:C0 -w /root/Desktop/ wlan0 mon
```

Результатом виконання вищенаведеної команди буде початок моніторингу утилітою airodump цільової бездротової мережі, у ході чого будуть очікуватися під’єднання до цієї мережі легітимних користувачів.

Рисунок 3.4 – Дані щодо бездротових WiFi мереж, виявлених у зоні прийому адаптеру

Рисунок 3.5 – Виконання команди моніторингу обраної мережі

Далі, якщо у процесі моніторингу хоча б одного користувача буде під’єднано до цільової мережі, ініціюється процес збору handshake-даних.

У свою чергу, файли, що містять дані рукостискань, як і зазначено у команді вище, зберігатися у локації /root/Desktop.

Перебіг процесу моніторингу бездротової мережі з використанням засобу airodump, включаючи операції захопленням пакетів з наступним утворенням handshake-файлів демонструється на рисунку 3.6.

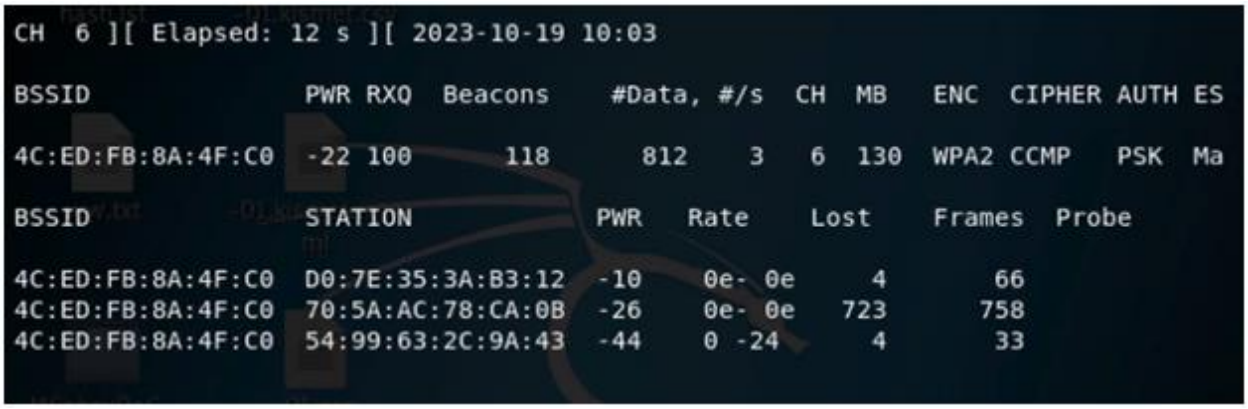

Рисунок 3.6 – Перебіг процес збору пакетів handshake

Наступним етапом атаки, який слідує за збором handshake, є аналіз захоплених пакетів рукостискань [19].

Даний етап починається тоді, коли зібрано обсяг handshake-файлів, якого може бути достатньо для того, щоб виокремити ключ WiFi-мережі.

При цьому, процес збору рукостискань у нашому випадку виконувався близько 3,5 годин. Це, у свою чергу, могло бути наслідком того, що:

– у межах цільової мережі знаходиться незначна кількість користувачів;

– інтенсивність обміну даними між користувачами цільової мережі є досить низькою.

Для того, щоб за допомогою aircrack-ng розпочати процес аналізу зібраних handshake, необхідно виконати команду вигляду `aircrack-ng -a2 -b [router bssid] -w [path to wordlist] /root/Desktop/*.cap`. Стосовно нашого випадку уточнена команда буде наступною:

```
aircrack-ng -a2 -b 4C:ED:FB:8A:4F:C0 -w /root/Desktop/ww.txt
                        /root/Desktop/*.cap
```

Результуючі дані, які було одержано у наслідок аналізу попередньо зібраних рукостискань, а також відновлений ключ мережі WiFi демонструються на рис. 3.7.

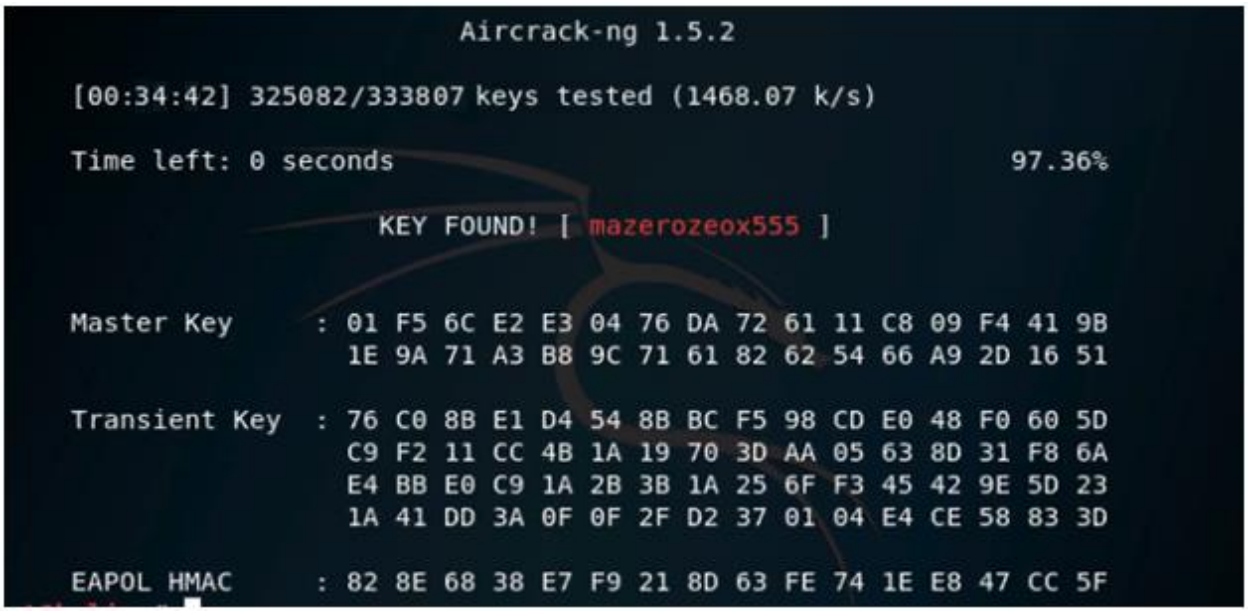

Рисунок 3.7 – Результуючі дані, які було одержано у наслідок аналізу попередньо зібраних рукостискань, а також відновлений ключ мережі WiFi

4 РЕАЛІЗАЦІЯ ТЕСТОВОГО ЗЛАМУ ТОЧКИ ДОСТУПУ WIFI З ВИКОРИСТАННЯМ ЗАСОБУ AIRGEDDON

4.1 Апаратні засоби, необхідні для використання Airgeddon

Вимоги щодо апаратного базису для успішного використання Airgeddon є аналогічними тим, що висувалися до Aircrack-ng. Разом з тим, для критичними є вимоги до безпровідного адаптеру [22].

Так, частіше за все вибір того чи іншого адаптеру залежить від ряду факторів – зокрема, можливості підтримки того чи іншого типу атак, наявності драйверів Linux тощо.

У нашому випадку вибір адаптеру виконаємо з огляду на необхідність тестування мережі на захищеність шляхом спроб зламу WEP та WPS.

Так, для першого випадку може бути використано адаптери Alfa AWUS052NH чи Panda Wireless PAU09 N600 [21].

Кожен з цих пристроїв є дводіапазонним, може функціонувати у діапазонах частот 2.4GHz та 5GHz. Оснащені двома антенами з підсиленням 5dBi для забезпечення покращення сигналу. Разом з тим, для атаки на WPS їх використовувати недоцільно.

У свою чергу, для реалізації брутфорс-атаки відносно WPS ПІНу (що, у разі успіху, дозволить відновити WPA/WPA2 пароль), пропонується скористатися адаптером Alfa AWUS036NHA, як рекомендують розробники Airgeddon [21].

Також для підсилення сигналу рекомендується комбінувати обрані раніше адаптери з антенами наступних моделей:

– Alfa ARS-N19 (Wi-Fi RP-SMA всенаправлена антена, підсилення 9 dbi);

– Alfa APA-M04 (Wi-Fi RP-SMA направлена антена одного діапазону, підсилення 7 dBi);

– Alfa APA-M25 (Wi-Fi RP-SMA направлена дводіапазонна антена для приміщень, підсилення 10 dBi).

Водночас, для Aircrack-ng обмеження та рекомендації з вибору моделей AP відсутні. Відтак, можемо скористатися поширеною моделлю Ralink 802.11n USB WirelessLanCard.

4.2 Ініціалізація бездротового адаптеру

Для випадку Airgeddon ініціалізації бездротового адаптеру виконується аналогічно тому, як це було виконано для Aircrack-ng. Різниця полягає лише у використанні іншого обладнання, як зазначалося у п. 3.2.

4.3 Інтеграція словника

Для реалізації ряду атак на мережу Wi-Fi може знадобитися словник. Це може бути будь-який словник – або свій власний, або попередньо завантажений з того чи іншого мережевого ресурсу [23].

У випадку повної відсутності словника може бути використано внутрішній словник, який відпочатку присутній у Kali Linux.

Для підготовки даного словника для використання виконаємо ряд дій, які ілюструє наступний лістинг:

```
cp /usr/share/wordlists/rockyou.txt.gz ~/
gunzip ~/rockyou.txt.gz
cat ~/rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > ~/newrockyou.txt
rm ~/rockyou.txt
```

У результаті цього отримуємо словник для зламу паролю Wi-Fi. Він знаходиться у файлі /root/newrockyou.txt.

4.4 Клонування головного модулю Airgeddon

Хоча увесь набір інструментарію, який є необхідним для функціонування Airgeddon (та залежності між усіма інструментами) початково присутній у Kali Linux, проте необхідно також завантажити сам головний модуль засобу. За великим рахунком, достатньо виконати клонування Airgeddon з GitHub. Дану процедуру може бути виконано за допомогою наступної команди [22, 23]:

```
git clone https://github.com/v1s1t0r1sh3r3/airgeddon
```

Для подальших дій змінюємо поточну локацію на ту, у яку завантажено Airgeddon:

```
cd airgeddon/
```

У випадку, коли планується реалізувати не лише хендшейк-механізм зламу мережі, але також атаки, що використовують механізми інших типів, попередньо додатково виконується завантаження відповідних програмних модулів (наприклад, для фішингових атак та/або сніффінгу). Водночас, у нашому разі вони є не актуальними.

4.5 Запуск Airgeddon

Безпосередньо самому запуску Airgeddon мають передувати такі дії, як:

– підключення мережевого адаптеру до USB-порту;

– вивантаження Network Manager.

За великим рахунком, деактивація Network Manager не є обов’язковою процедурою, якою може бути знехтувано. Разом з тим, слід пам’ятати, що у деяких випадках Network Manager може чинити вплив на процеси, які виконуються під час роботи з Airgeddon.

Для зупинки NetworkManager виконується команда [23]:

```
sudo systemctl stop NetworkManager
sudo airmon-ng check kill
```

Далі виконується скрипт запуску Airgeddon:

```
sudo bash airgeddon.sh
```

Після виконання зазначеного скрипта необхідно обрати бездротовий інтерфейс, який буде надалі використовуватися за замовчуванням. У нашому випадку це wlan0mon (рис.4.1).

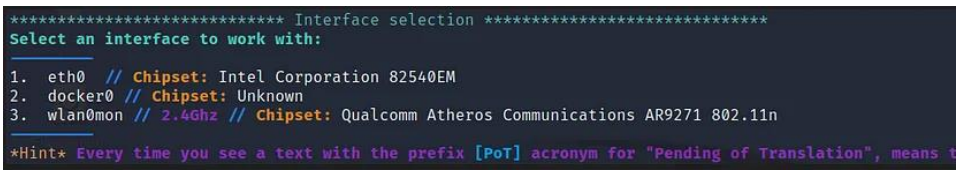

Рисунок 4.1 – Вибір мережевого адаптеру

4.6 Реалізація атак на WiFi-мережі

4.6.1 Атака на WEP

Як зазначалося раніше, WiFi мережі використовують ряд шифрів та протоколів [15, 21].

Найбільш слабким з них є WEP.

Фактично, беручи до уваги особливості WEP, його злам може бути реалізовано протягом невеликого проміжку часу – до кількох хвилин, якщо попередньо було згенеровано достатню кількість трафіку.

На першому кроці виконаємо перевірку наявності мереж у зоні прийому адаптеру, які використовують WEP.

Для цього обирається пункт меню 9 «Атака на WEP все в одному» (рисунок 4.2).

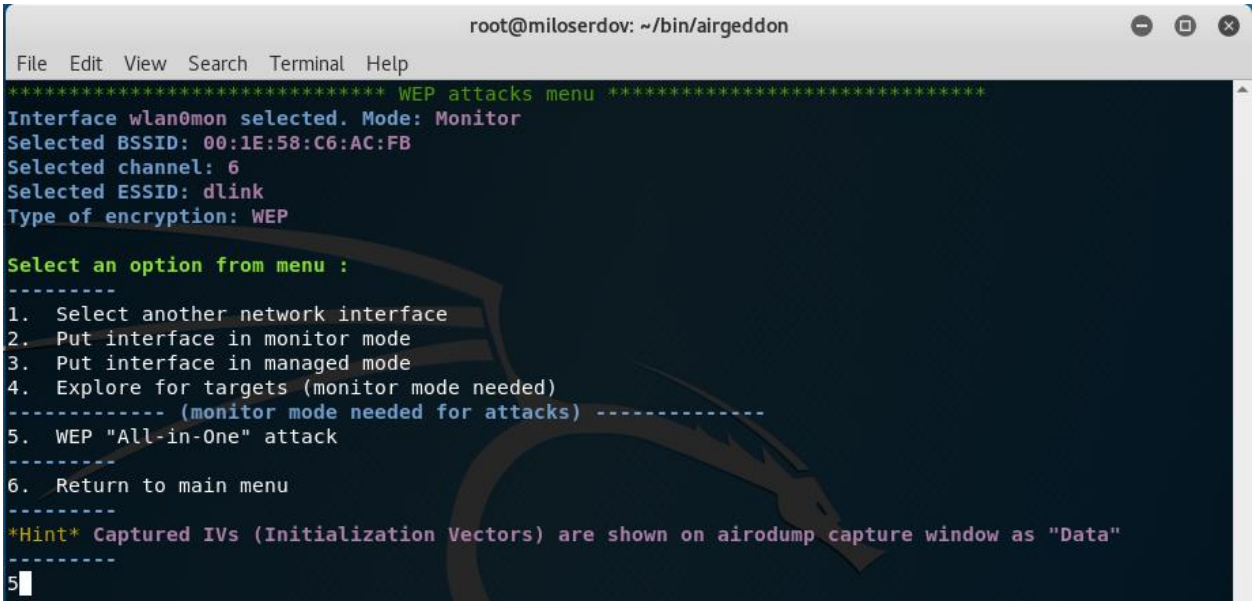

Рисунок 4.2 – Вибір режиму атаки WEP

Далі обирається пункт 4 «Пошук цілей (необхідний режим монітору)» для того, щоб мати змогу виявити усі доступні мережі Wi-Fi, що використовують WEP (рисунок 4.3) [23].

Як можна бачити на даному рисунку, ще на початку сканування попередньо було виявлено мережі, які використовують протокол WEP. Сканування усього доступного простору бездротових мереж зупиняється після знаходження необхідної мережі.

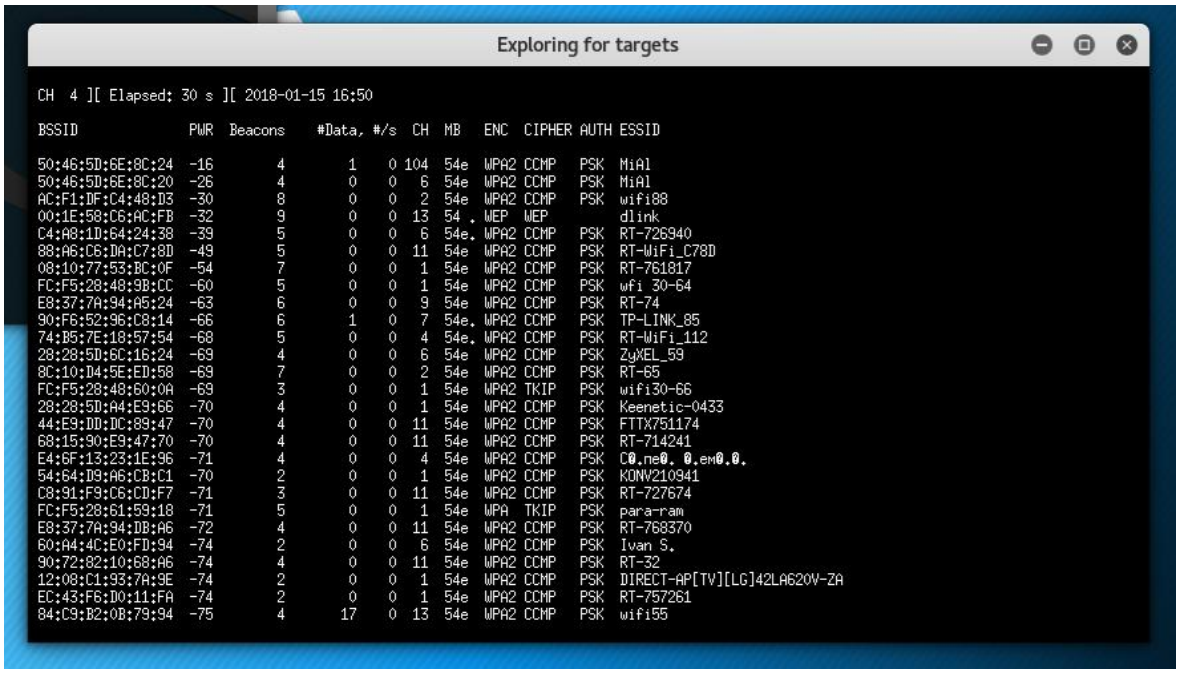

Рисунок 4.3 – Процес пошуку WEP-мереж

У підсумку, у межах досяжності було виявлено виключно одну мережу, що використовує WEP з параметрами, поданими рис.4.4.

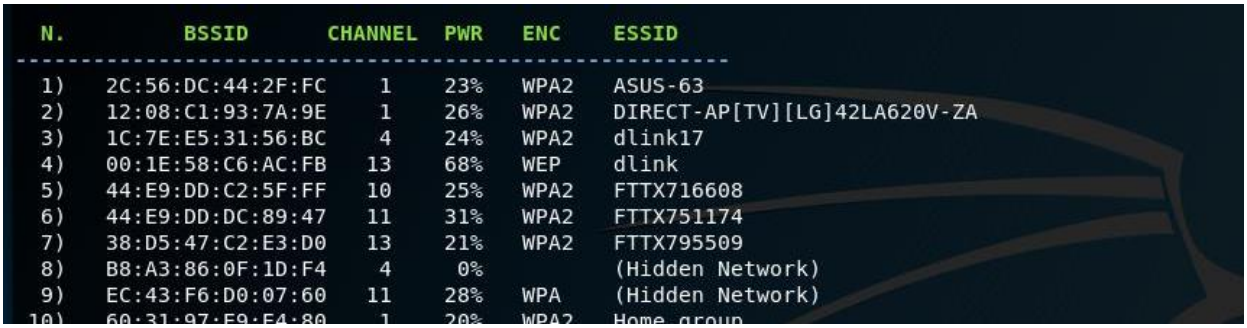

Рисунок 4.4 – Результати пошуку бездротових мереж Wi-Fi, які використовують WEP

Знайдена цільова мережа йде 4-ю у загальному переліку, відтак для усіх наступних операцій з нею, де необхідний її ідентифікатор, буде вказуватися саме цей номер (рис. 4.5).

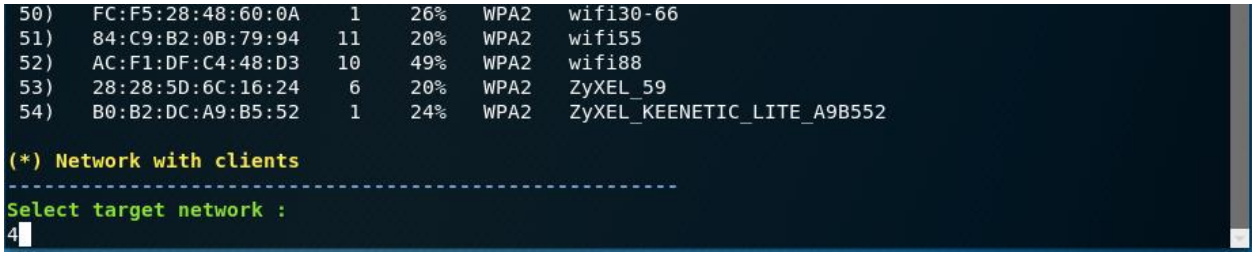

Рисунок 4.5 – Вибір цільової мережі для подальших дій

Далі можна розпочинати процедуру атаки на мережу, лише треба обрати її необхідний тип. У нашому випадку це – «Атака на WEP все в одному» (рис. 4.6).

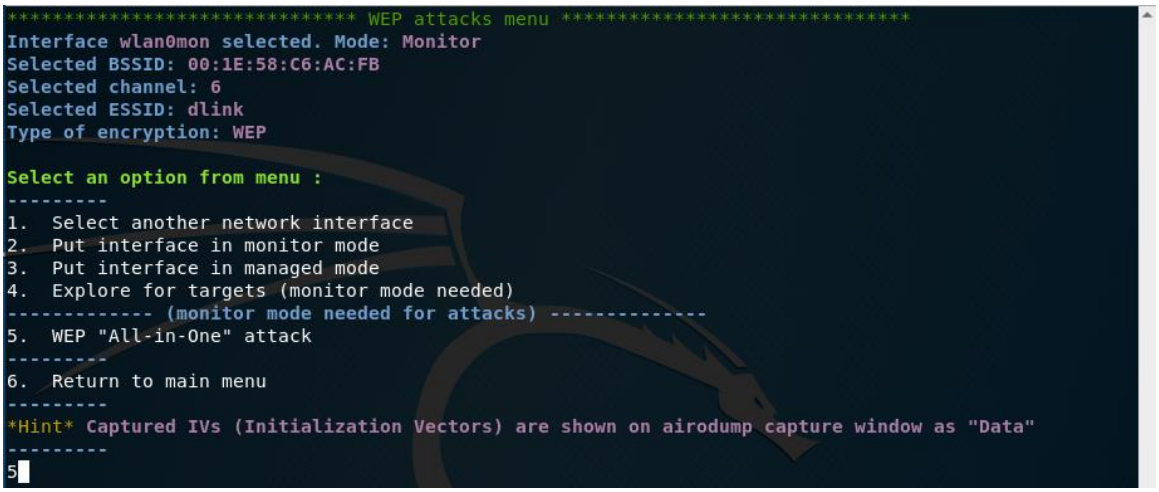

Рисунок 4.6 – Вибір режиму «Атака на WEP все в одному»

У свою чергу, атака на WEP «все в одному» включає у себе ряд різних методів генерування трафіку в об’ємі, достатнього для того, щоб виконати відновлення ключа (методи Chop-Chop, Caffe Latte, Hirte, Replay, Фальшиві асоціації, Дроблення тощо) [23].

Далі система генерує сповіщення про те, що мережу, яка є підходячою для подальшої реалізації атаки, знайдено, та сформує запит на продовження операції:

```
1) You have a valid WEP target network selected. Script can continue...
2) Press [Enter] key to continue...
```

Після цього скрипт інформує користувача про те, що коли протягом виконання атаки на WEP «Все в одному» було знайдено пароль, необхідно вказати шлях для його збереження. Тут у консолі необхідно вказати необхідну локацію для розміщення файлу зі знайденим паролем, як показано на рисунку 4.7.

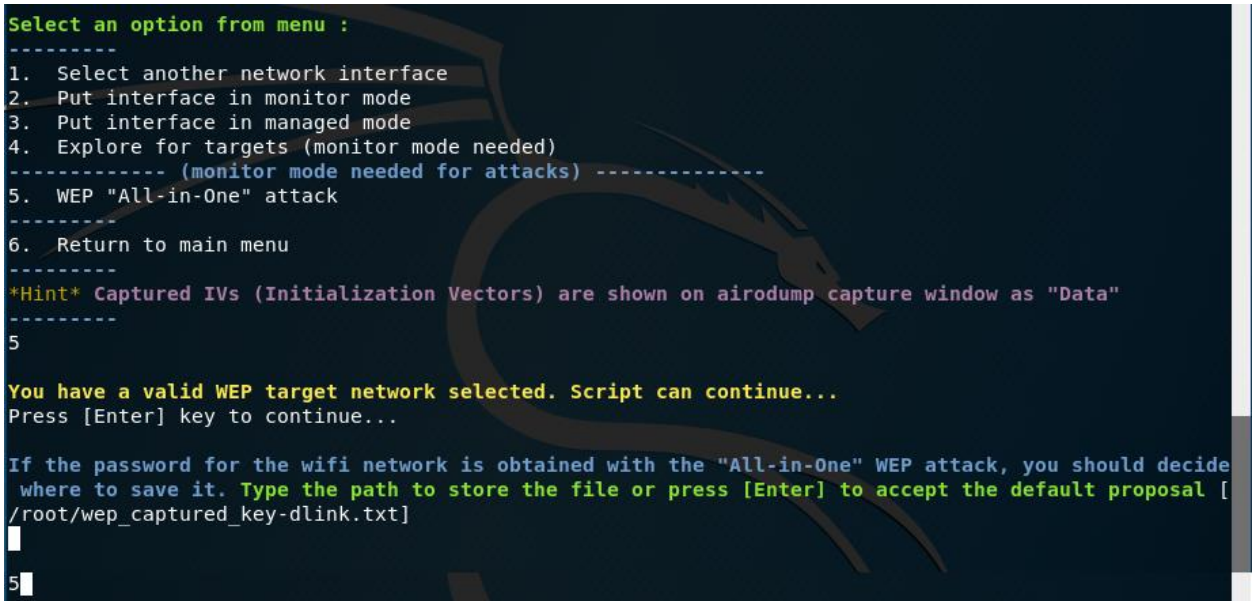

Рисунок 4.7 – Встановлення шляху для збереження файлу з паролем

Система виконує перевірку заданого шляху і якщо визнає його коректним, далі видає сповіщення про те, що шлях існує і атаку може бути розпочато [21-23]:

```
The path is valid and you have write permissions. Script can
continue...
Press [Enter] key to continue...

All parameters and requirements are set. The attack is going to
start. Multiple windows will be opened, don't close anyone. When you
want to stop the attack press [Enter] on this window and the script
will automatically close them all
Press [Enter] key to continue...
```

Процес виконання атаки на WEP за обраним сценарієм показано рисунком 4.8.

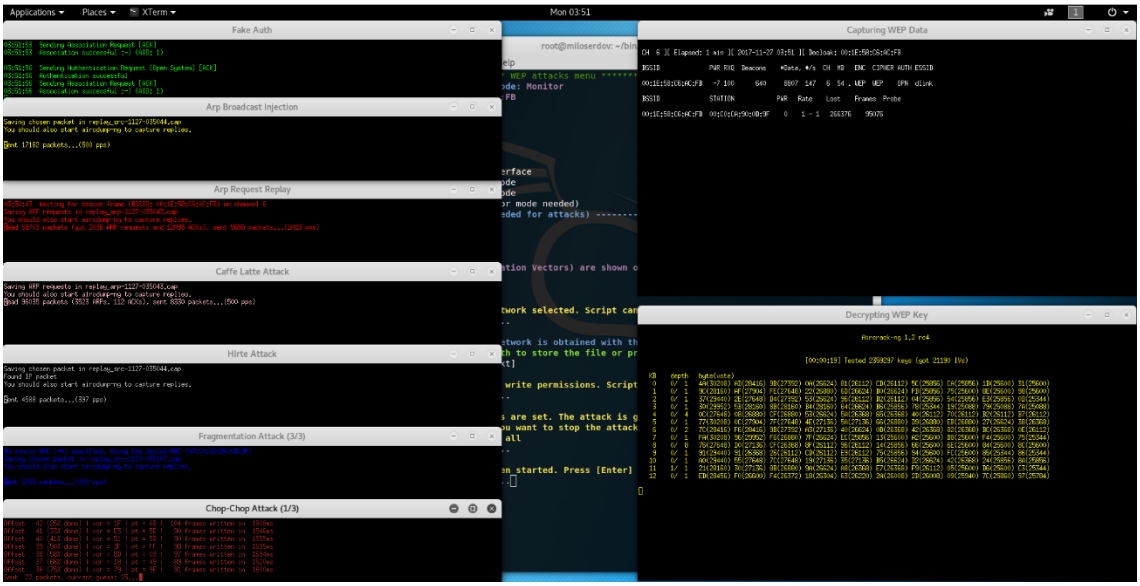

Рисунок 4.8 – Перебіг атаки на WEP «Все в одному»

Як бачимо з даного рисунку, у ході даної атаки виконується збір даних для аналізу, одночасно застосовано ряд механізмів зламу та виконуються спроби підбору паролю [22, 23].

Знайдений пароль WEP відображається у окремому вікні як ASCII- рядок, поданий у шістнадцятеричному форматі (рис.4.9).

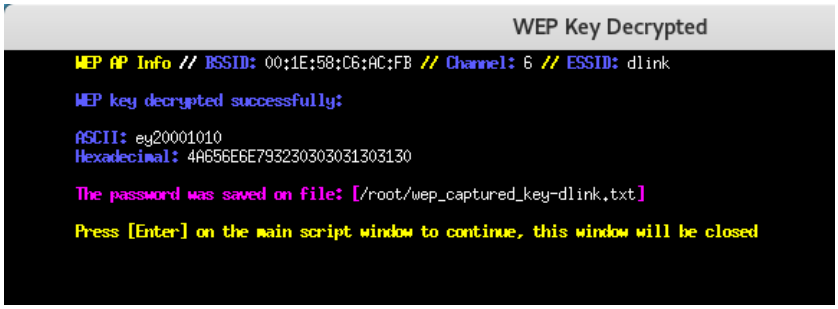

Рисунок 4.9 – Знайдений пароль WEP

Також пароль може бути записано до файлу /root/wep_captured_key-dlink.txt.

Разом з тим, у нашому випадку рядок ASCII не є тотожнім рядку у шістнадцятеричному форматі. Тому для того, щоб перевести шістнадцятеричний запис на рядок ASCII, додатково виконуємо команду конвертації [23]:

```
echo 4A656E6E793230303031303130 | xxd -r -p
Jenny20001010
```

4.6.2 Атака на WPS

Значна частка бездротових мереж WiFi, що використовують захист на базі WPS, мають уразливості до WPS-атак.

Слід також зазначити, що для ряду бездротових AP, які, у свою чергу, використовують драйвер rt2800usb, сьогодні виявлено ряд проблем, що обмежують повноцінну роботу з WPS зараз виявлено [21, 23].

Це, зокрема, є справедливим для точок доступу, що працюють під управлінням контролерів RT3070, RT3272, RT3570, RT3572 і подібних. Саме з цієї причини можливість повноцінного використання даних бездротових адаптерів разом з Airgeddon під час атак на WPS поки що відсутня. Відтак, зазначені раніше AP, такі, як Alfa AWUS052NH а також Panda Wireless PAU09 N600 у цьому разі не може бути використано. Тому для атаки на WPS необхідно використовувати бездротовий адаптер, який використовує інший драйвер та працює під управлінням чіпсету іншого типу. Наприклад, це може бути Alfa AWUS036NHA.

Для того, щоб після налаштування відповідної AP далі розпочати атаку на WPS, у головному меню Airgeddon необхідно обрати пункт «8. Меню атак на WPS», зміст якого показано на рисунку 4.10.

При цьому, для зламу WPS-мережі Airgeddon дає можливість використати такі типи атак, як:

– відновлення паролю за відомим PIN;

– Pixie Dust;

– злам з використанням бази даних вже відомих PIN’ів;

– атака з використанням повного перебору PIN’ів.

Розглянемо приклад реалізації атаки на базі Pixie Dust [23].

В основі даної атаки знаходяться відомості про те, що ряд бездротових AP використовують для WPS надмірно низький рівень ентропії. Так, один з етапів роботи WPS передбачає генерування простих чисел (E-S1 и E-S2) на роутерах. Якщо при цьому зловмисник зможе отримати дані числа, він отримує змогу реконструювати WPS PIN, оскільки саме ці числа використовуються криптографічною функцією для захисту від атак brootforce для отримання WPS PIN.

Роутер повертає хеш-значення, яке розраховується з використанням WPS PIN та чисел E-S1 і E-S2 чисел, для того, щоб довести, що PIN йому також

відомий. У свою чергу, це необхідно для захисту від підключення до зловмисної AP, яка б мала змогу просто прийняти пароль та прослуховувати трафік.

Самі числа E-S1 и E-S2 необхідні для генерування E-Hash1 та E-Hash2, котрі, у свою чергу, отримуємо від роутеру у повідомленні M3.

При цьому, порівняно з багатьма атаками, що вже можуть вважатися класичними (наприклад – brooteforce атака на PIN, що входить до складу таких інструментів, як Bully чи Reaver), час, необхідний відновлення PIN'а, складає не декілька годин, а щонайбільше кілька хвилин, залежно від конкретних умов. Слід також розуміти, що досліджуваний зламу метод буде ефективним виключно лише тоді, коли атакована мережа матиме вразливість до атаки даного типу.

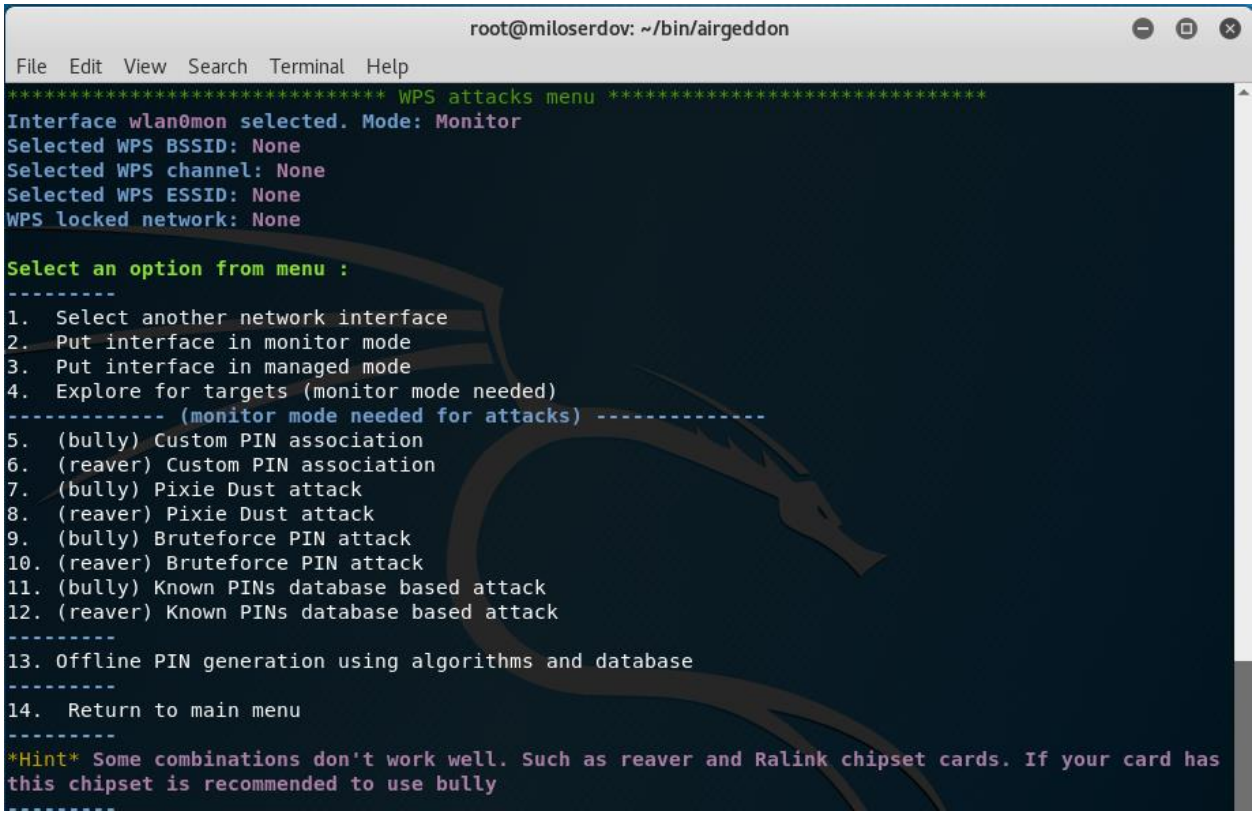

Рисунок 4.10 – Меню атак на WPS

При цьому, будь-яка атака на WPS, як і інші типи атак на WiFi мережу, які може бути реалізовано реалізовано за допомогою Airgeddon, починається з вибору пункту «4. Пошук цілей (вимагає режиму монітору)».

Після вибору даної операції і запуску сканування середовища, з підсумкового переліку виявлених мереж може бути обрано ті з них, які не є

блокованими (усі крім тих, які відмічені червоним шрифтом), як показує рисунок 4.11.

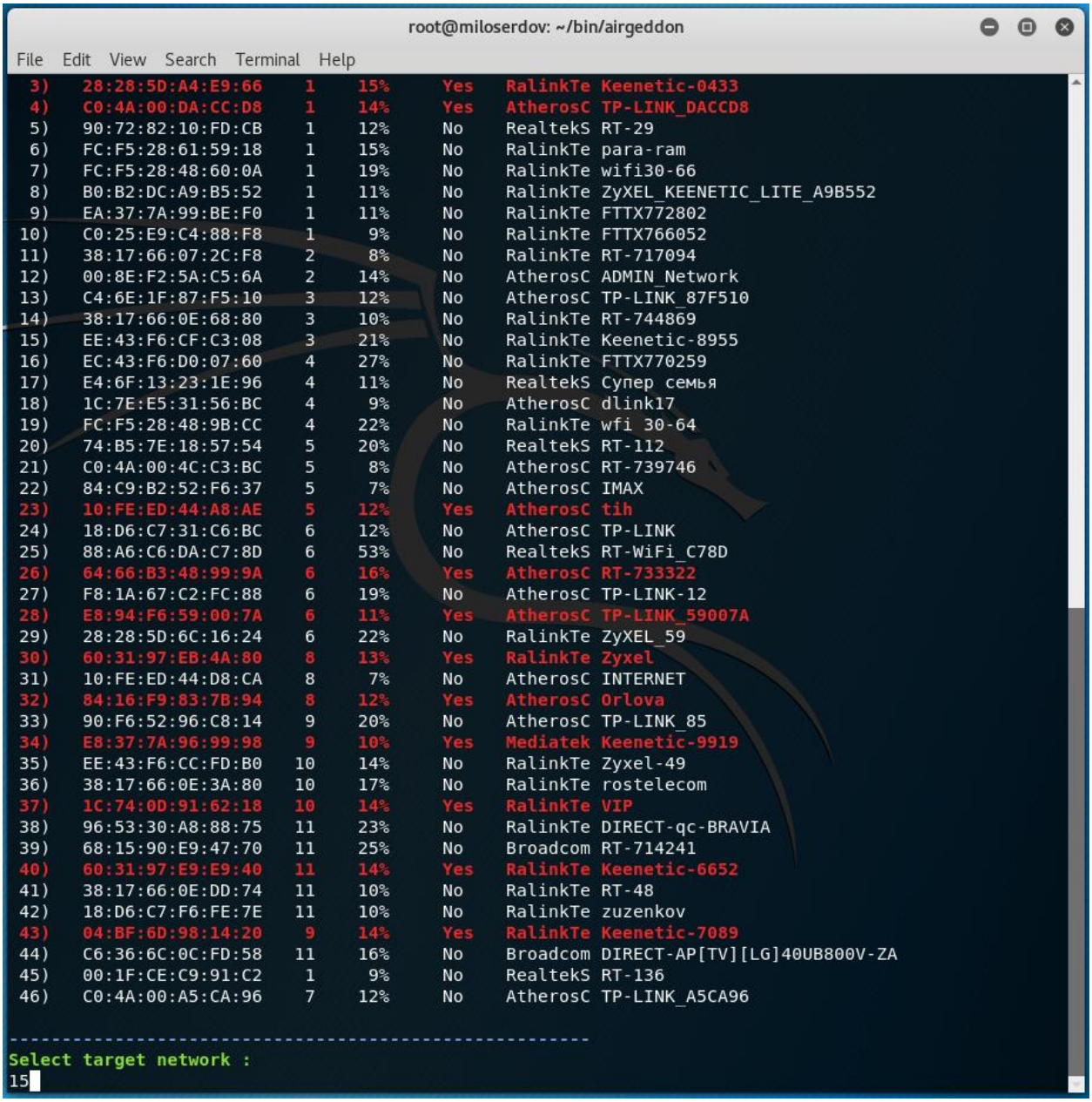

Рисунок 4.11 – Вибір мережі для реалізації атаки Pixie Dust

Після цього з меню Airgeddon обирається пункт «8. (reaver) Атака Pixie Dust». Для налаштування даної атаки необхідно вказати необхідну тривалість тайм-ауту у секундах, з діапазону від 25-2400 сек. При цьому для того, щоб збільшити ймовірність вдалої атаки, рекомендується встановлювати значення тайм-ауту не меншим, ніж 300 секунд.

Перебіг атаки, звіт за результатами її виконання а також знайдений ключ WPS, показано на рисунку 4.12.

Рисунок 4.12 – Перебіг атаки, звіт за результатами її виконання а також знайдений ключ WPS

4.6.3 Атака на мережі WPA/WPA2

На той випадок, коли атакована точка доступу не використовує WPS або тоді, коли спроби атак на WPS не були успішними, далі доцільно застосувати підхід, у рамках якого виконується перехоплення пакетів підтвердження зв'язку

(кадрів, якими AP та клієнт обмінюються під час з'єднання) – тобто, як і у випадку Aircrack-ng, handshake-кадрів з їх подальшим розшифруванням [19, 23].

Для цього спочатку у головному меню Airgeddon обирається пункт «5. Capture Handshake» (рис. 4.13).

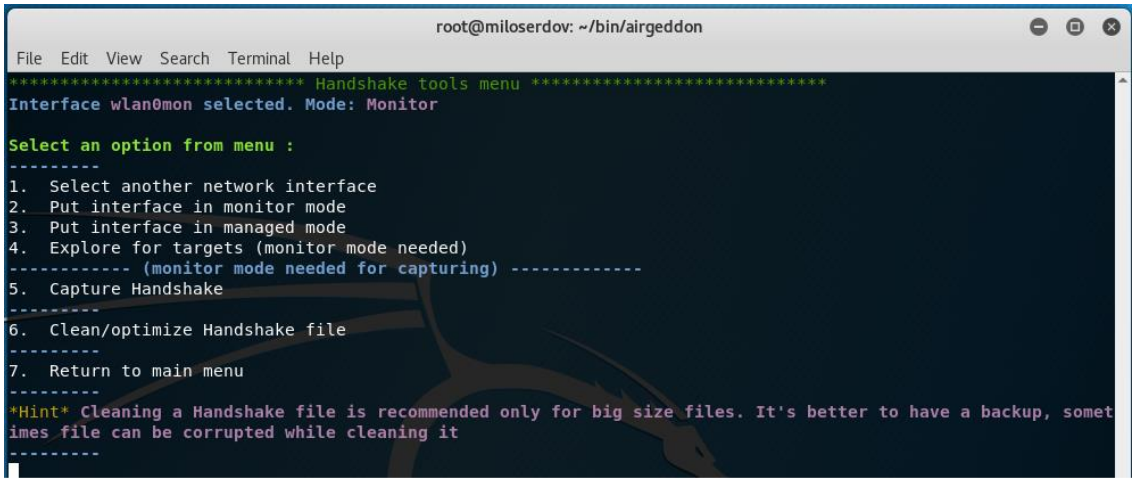

Рисунок 4.13 – Вибір меню перехоплення рукостискань у головному меню

Далі обирається пункт «4. Explore for targets (monitor mode needed)», після цього починається сканування доступних мереж (рис.4.14).

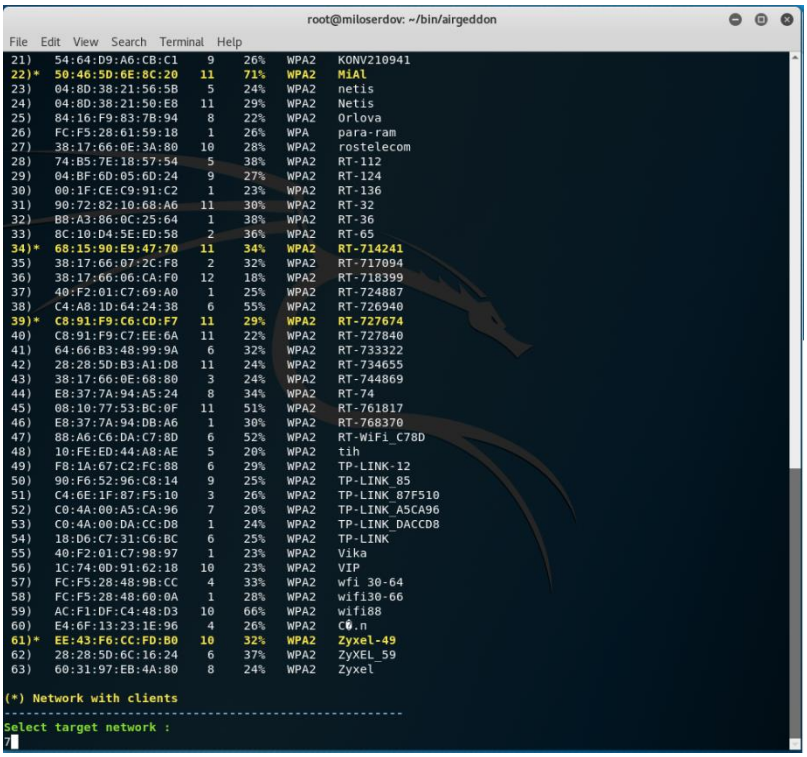

Рисунок 4.14 – Процес сканування доступних мереж

При цьому, найбільш потенційно уразливими є мережі, які мають велику кількість клієнтів а також потужний сигнал передавача. Після вибору цільової AP, знову звертаємося до пункту «5. Capture Handshake», де може бути обрано один з трьох режимів перебігу атаки (рис.4.15).

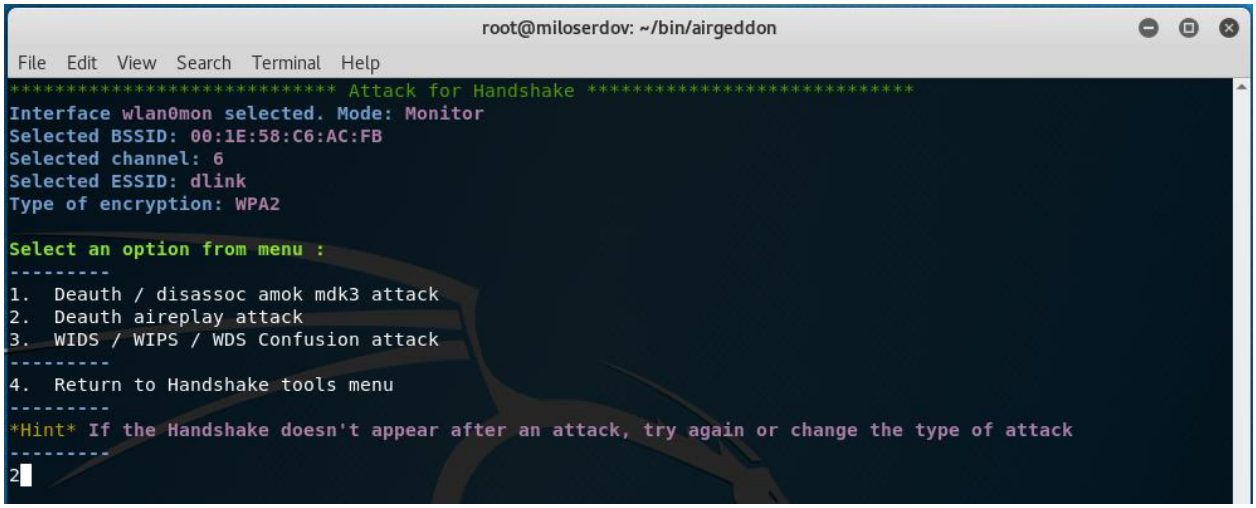

Рисунок 4.15 – Режими роботи атаки перехоплення Handshake

Тут може бути використано одну з наступних атак:

– атака деаутентифікації/роз'єднання amok mdk3;

– атака деаутентифікації aireplay;

– атака змішування WIDS/WIPS/WDS.

Тут може бути обрано будь-який режим, наприклад, починаючи з першого. Далі, якщо перша атака не буде ефективною, може бути задіяно наступні.

У першому режимі активуються вікна, де відображено процес захоплення рукостискань, а також - атака примусового переключення бездротових клієнтів. Атака виконується в автоматичному режимі. При цьому, частіше за все через 20-30 секунд стає відомо щодо успішності її перебігу.

Так, скрипт надає запит [23]:

```
Did you get the Handshake? (Look at the top right corner of the capture window) [y/n]
```

У нашому випадку handshake було отримано (рисунок 4.16).

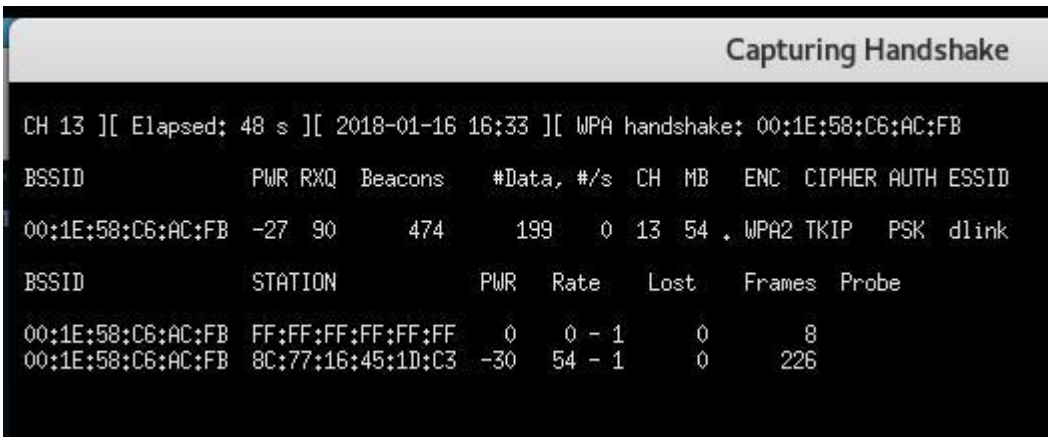

Рисунок 4.16 – Результат перехоплення handshake

Далі система згенерує запит щодо місця збереження файлу handshake. У цьому випадку може бути обрано локацію за замовчуванням, або вказати нову. Після цього слід повернутися до головного меню режиму, та обрати пункт «6. Offline WPA/WPA2 decrypt menu» для подальшого розшифрування handshake у офлайн-режимі (рис.4.17).

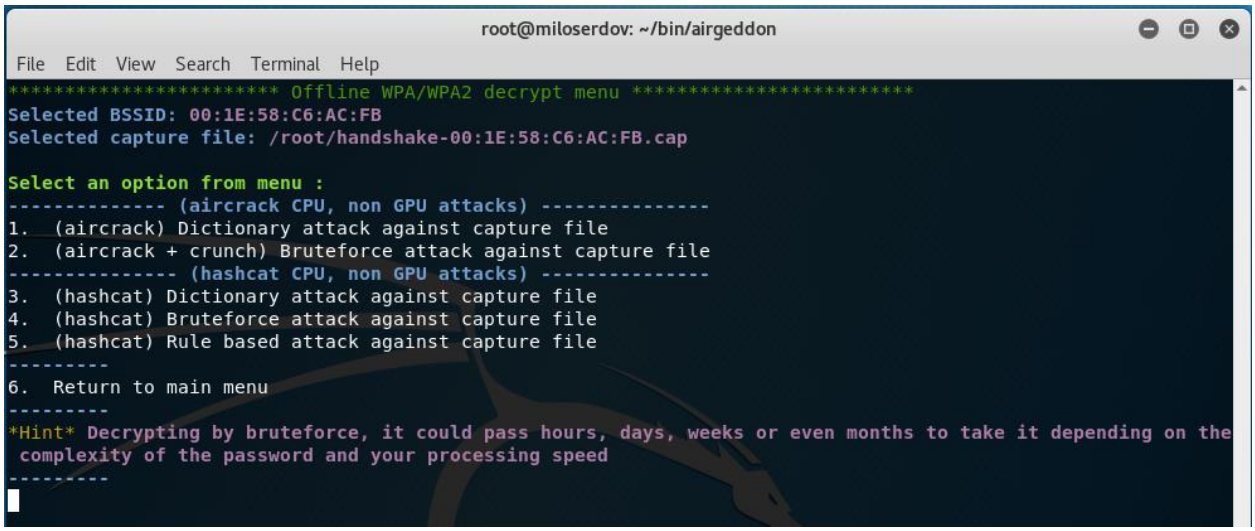

Рисунок 4.17 – Вибір режиму розшифрування handshake

Далі, для прикладу, у першу чергу використаємо атаку за словником, для вибору цього режиму обираємо пункт меню «1. (aircrack) Dictionary attack against capture file».

Після цього отримаємо повідомлення від скрипту про те, що файл під час поточної сесії вже захоплено і необхідно або використати даний файл, або обрати інший [19, 23]:

```
    You already have selected a capture file during this
session [/root/handshake-00:1E:58:C6:AC:FB.cap]

    Do you want to use this already selected capture file?
[Y/n]
     You already have selected a BSSID during this session
and is present in capture file [00:1E:58:C6:AC:FB]
    Do you want to use this already selected BSSID? [Y/n]
```

У нашому випадку обираємо варіант за замовчуванням, тобто, той самий файл, після цього у якості словника встановлюємо раніше вже зазначений файл /root/newrockyou.txt. Далі виконуємо атаку за словником (рис. 4.18).

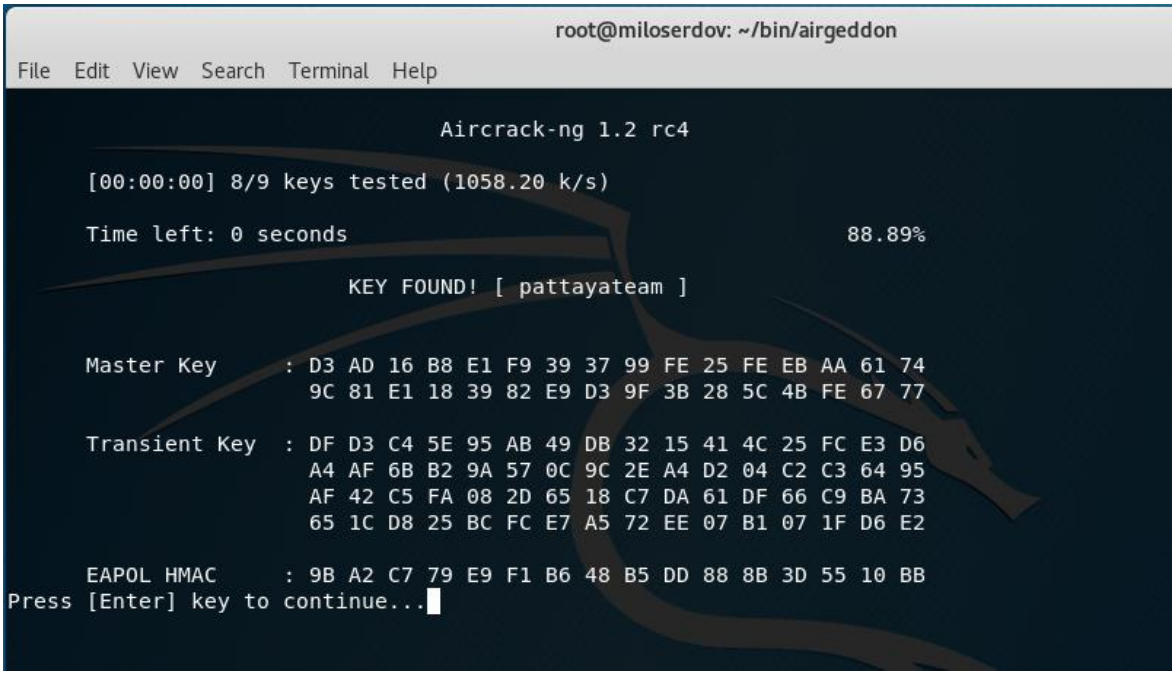

Рисунок 4.18 – Результати розшифрування handshake-матеріалу

Як видно з рисунку 4.18, пароль знайдено. Далі скрипт виконає запит щодо локації для збереження файлу, що містить знайдений пароль.

При цьому, якщо результат виконання атаки за словником виявився незадовільним, далі може бути використано або інший словник, або атаку «2. (aircrack + crunch) Bruteforce attack against capture file» - тобто, атаку за методом bruteforce стосовно перехопленого файлу.

Зі свого боку, розробники ідеології даного підходу рекомендують у цьому випадку використовувати паролі довжиною або 8, або 12 елементів. Так, у першому випадку мається на увазі дні народження (19990210) а у другому – номери мобільних телефонів (380507436858).

4.7 Заходи з підвищення безпеки бездротових мереж WiFi за результатами реалізації тестових зламів

Вектор захисту мереж WiFi рекомендується реалізовувати на базі наступних підходів [9, 10, 23]:

– на рівні SSID, а саме - конфігурування бездротових клієнтів та точок доступу на використання виключно єдиного SSID, значення якого, при цьому, обирається відмінним від встановленого за замовчуванням;

– на рівні довірених MAC-адрес, у рамках чого передбачається AP надавати дозволи на взаємодію виключно з клієнтами, MAC-адреси яких належать до довіреного переліку, який відомий точці доступу;

– на рівні механізмів аутентифікації та шифрування, а саме - конфігурувати клієнтів на аутентифікацію в AP та криптографічного захисту трафіку.

Разом з тим слід відмітити, що зараз більшість точок доступу конфігуруються таким чином, що дозволяється взаємодія з SSID, встановленими за замовчуванням. При цьому, перелік довірених MAC-адрес клієнтів не використовується. Окрім цього, для аутентифікації та шифрування нерідко використовується відомий загальний ключем, а у ряді випадків дані технологічні процедури взагалі ігноруються, як і той факт, що означені відомості можуть не лише друкуватися у супровідній документації та на корпусі пристроїв, але також на у відповідних розділах Web-ресурсів виробника.

Отже, складаються суперечливі умови, коли навіть пересічний користувач без відповідних знань та досвіду здатен забезпечити оперативне розгортання бездротової мережі та баз будь-яких суттєвих труднощів.

Проте, з іншого боку, у таких умовах, коли не забезпечується коректне налаштування AP та клієнтів, а також ігнорується ряд інструментів безпеки, суттєво зменшується захищеність мережі та зростає ймовірність її зламу. На додачу до цього, стан безпеки мережі значно погіршується за рахунок налаштування великої частини вузлів доступу на використання широкомовного

транслювання SSID. За рахунок цього потенційний зловмисних може виявити уразливі мережі на базі стандартних SSID.

Отже, заміна значення SSID вузла доступу може розглядатися як первинний захід з забезпечення захищеності мережі WiFi. При цьому, ідентифікатор SSID також підлягає зміні на клієнтах для того, щоб гарантувати можливість комунікації з AP. Тут рекомендується встановлювати такі SSID, що будуть тією чи іншою мірою зрозумілими для легальних користувачів бездротової мережі, водночас ніяк не ідентифікуючи мережу з-поміж сукупностей сторонніх SSID, які зловмисник може перехопити у той чи інший спосіб.

Далі, після безпечного призначення SSID, логічним продовженням налаштування додаткових заходів з безпеки бездротової мережі є блокування широкомовного розсилання SSID усім вузлам, що знаходяться у зоні доступу. Це є необхідним для того, щоб сприяти затрудненню (хоча ця можливість може не усуватися повністю) виявити активну мережу WiFi та SSID зловмисником.

Водночас, для певної кількості моделей точок доступу різних виробників така можливість відсутня. Тому у цьому разі доцільним є зміна інтервалів широкомовної передачі у бік їх максимального розширення. Попри це, комунікація з деякою кількістю бездротових клієнтів може забезпечуватися виключно з використанням широкомовної трансляції ідентифікатору SSID вузлом доступу. У такому випадку адміністратор безпеки імперичним шляхом виявляє ширину інтервалу, яка буде оптимальною.

Також, якщо є можливість вибору різних протоколів безпеки мереж WiFi, у тому числі з сімейства WPA, рекомендується скористатися саме ними - WPA або WPA2 чи WPA-PSK. При цьому, вибір між WPA чи WPA2, та WPA-PSK залежить від можливості розгортання адміністратором безпеки інфраструктури, яка використовується WPA, а також WPA2 для реалізації процедури аутентифікування користувачів. Зокрема WPA та WPA2 вимагають попереднього розгортання серверів RADIUS. Окрім цього, за деякими виключеннями, додатково необхідно розгортнути PKI (PublicKeyInfrastructure).

У свою чергу функціонування WPA-PSK, як і у випадку протоколу WEP, вимагає використання загального ключа, який є відомими точці доступу та клієнту. При цьому, для WPA-PSK застосовується загальний ключ, на базі якого функціонують процеси як шифрування, так і аутентифікації, оскільки зазначений протокол позбавлений характерних недоліків протоколу WEP.

ВИСНОВКИ

Згідно з умовами технічного завдання, у ході виконання кваліфікаційної роботи було здійснено:

– огляд чинників, що сприяли широкій розповсюдженості бездротових мереж WiFi;

– дослідження факторів, які містять у собі потенційні ризики безпеки бездротових мереж;

– аналіз типів атак, які може бути реалізовано потенційним зловмисником відносно мереж WiFi;

– дослідження специфіки підготовчих дій (у т.ч. налаштування програмного середовища та апаратних засобів), необхідних для реалізації тестового зламу бездротової мережі на базі ряду поширених атак;

– тестове проникнення до мережі WiFi;

– розробку рекомендацій, спрямованих на збільшення захищеності мереж WiFi.

Зокрема, було виявлено, що більшість успішних атак на бездротові мережі є наслідком некоректного налаштування як точок доступу, так і бездротових клієнтів користувачами.

При цьому, окремо слід відмітити те, що за можливості включення у склад фіксованої мережі некоректно налаштованої AP легальним користувачем, повністю нівелюються будь-які захисні засоби та механізми, реалізовані у базовій мережі. Це зумовлено тим, що зловмисник може використати таку AP як точку входу.

У рамках дослідження засобів зламу мереж WiFi було проаналізовано можливості та порядок роботи пакетів спеціалізованих утиліт Aircrack-ng та Airgeddon. Дані засоби входять до складу стандартних складових Kali Linux та призначені саме для реалізації тестових зламів.

У свою чергу, на базі Aircrack-ng було досліджено реалізацію тестового зламу мережі на базі атаки Evil Twin, використовуючи при цьому механізми захоплення та аналізу handshake-пакетів. Виявлено, що залежно від типу шифрування, довжини паролю та кількості захоплених пакетів handshake час відновлення ключа може варіюватися від кількох хвилин до кількох годин.

Розглядаючи можливості реалізації тестових зламів з використанням Airgeddon, який, у сутності, можна вважати подальшим розвитком проекту Aircrack-ng, було досліджено особливості планування та виконання атак на WEP, WPS, WPA/WPA2 мережі. У цьому випадку також використовувалася атака Evil Twin, яку було реалізовано за handshake-сценарієм та сценарієм Pixie Dust.

Отже усі завдання до кваліфікаційної роботи у повній мірі виконано

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Microsoft security report [Електронний ресурс] – Режим доступу: https://microsoft.com/securityinsights.
2. Antivirus and Cybersecurity Statistics & Facts 2021 [Електронний ресурс] – Режим доступу: https://wethegeek.com/antivirus-statistics-facts/.
3. Understanding Wi-Fi 4/5/6/6E/7(802.11 n/ac/ax/be) [Електронний ресурс] – Режим доступу: https://www.duckware.com/tech/wifi-in-the-us.html
4. VNI Service Adoption Forecast [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/dam/assets/sol/sp/vni/sa_tools/vnisa-graphing-tool/vnisa-graphing-tool.html
5. Wifi to carry 60 pc of mobile data traffic by 2019 [Електронний ресурс] – Режим доступу: http://www.juniperresearch.com/press/press-releases/wifi-to-carry-60pc-of-mobile-data-traffic-by-2019.
6. Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems (2 ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6.
7. Шаньгін В.Ф. Захист інформації в розподілених корпоративних мережах і системах [Текст]: підручник / В.Ф. Шаньгин, А.В. Соколов. – М.: ДМК Пресс, 2002. – 656 с.
8. Colon S. Wireless Networks and Communications. Wiiford Press, 2019. – 229 p.
9. Bejtlich R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response / Richard Bejtlich. – San Francisco: Search Press Inc, 2013. – 341p.
10. Coleman David D., Westcott David A. CWNA Certified Wireless Network Administrator Study Guide: Exam CWNA-107, 5th Edition. D. Coleman. – Wiley, 2018. – 1024 p. ISBN: 978-1-119-42578-6.
11. Coleman David D., Westcott David A., Bryan Harkins E. CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205, 2nd Edition. D. Coleman. – Wiley, 2016. – 696 p. ISBN: 978-1-119-21109-9.
12. Coleman David D., Westcott David A., Miller B., Mackenzie P. CWAP Certified Wireless Analysis Professional Official Study Guide: Exam PW0-270. D. Coleman. – Wiley, 2011. – 696 p. ISBN: 978-1-118-07523-4.

13. Matthew Gast S. 802.11ac: A Survival Guide. O'Reilly Media, Inc, 2003. – 152 p. ISBN: 9781449343149.
14. WEP Crack Method in Wireless Networks [Електронний ресурс] – Режим доступу: IEEE 802.11-2016 [Електронний ресурс] – Режим доступу: https://standards.ieee.org/ieee/802.11/5536/
15. IEEE 802.11-2016 [Електронний ресурс] – Режим доступу: https://standards.ieee.org/ieee/802.11/5536/
16. 10 bestwi-fi hacking tools 2018 [Електронний ресурс] – Режим доступу: https://www.techworm.net/2018/01/10-best-wi-fi-hacking-tools-2018.html
17. Handshaking [Електронний ресурс] – Режим доступу: https://networkencyclopedia.com/handshaking/
18. Aircrack-ng [Електронний ресурс] – Режим доступу: https://aircrackng.com/doku.php?id=main
19. How to Hack WPA/WPA2 WiFi Using Kali Linux? [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/how-to-hack-wpa-wpa2-wifi-using-kali-linux/
20. Github - ParrotSec / wifite [Електронний ресурс] – Режим доступу: https://github.com/ParrotSec/wifite
21. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution [Електронний ресурс] – Режим доступу: https://www.kali.org/
22. Airgeddon | Kali Linux Tools [Електронний ресурс] – Режим доступу: https://www.kali.org/tools/airgeddon/
23. The easiest and fastest ways to hack Wi-Fi (using airgeddon) [Електронний ресурс] – Режим доступу: https://miloserdov.org/?p=459&ysclid=m4o7xvp9jt510454219