I.J. Wireless and Microwave Technologies, **2025, 4, 1-18**
Published Online on August 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2025.04.01

Evaluating the Effectiveness of WPA3 Protocol against Advanced Hacking Attacks

Asmaa A. Ghanim*
Department of Electrical Engineering, University of Mosul, Mosul, Iraq
E-mail: asmaa.22enp38@student.uomosul.edu.iq
ORCID iD: https://orcid.org/0009-0002-3563-6642
*Corresponding Author

Mohammed Y. Thanoun
Department of Electrical Engineering, University of Mosul, Mosul, Iraq
E-mail: myounisth@uomosul.edu.iq
ORCID iD: https://orcid.org/0000-0002-2852-3917

Received: 28 September, 2024; Revised: 20 November, 2024; Accepted: 03 June, 2025; Published: 08 August, 2025

Abstract: Personal Mode Home Wi-Fi networks are an integral part of our daily lives, providing convenience and ease of access to the Internet. However, many people believe that modern encryption protocols such as Wi-Fi Protected Access3 (WPA3) provide sufficiently strong protection. This research aims to evaluate the effectiveness of encryption protocols used in home Wi-Fi networks, focusing on the currently most widely used Wi-Fi Protected Access2 (WPA2) protocol and the newer and more secure WPA3 protocol, and the effectiveness of the Protected Management Frames (PMF) against deauthentication attacks. A penetration test was conducted in a controlled, secure environment using a set of specialized tools such as Aircrack-ng, Fluxion, Bettercap, and Wireshark to assess the vulnerability of these networks to various attacks. The research results showed that home Wi-Fi networks using WPA2 protocol and WPA3 protocol (who support transitional mode) are vulnerable to hacking. deauthentication attacks and dictionary attacks were successful in hacking networks, especially when the passwords were weak or could be guessed. In addition, evil twin attacks using the captive portal approach have been proven effective in penetrating networks that use WPA2 and WPA3 (even when they do not support transitional mode) by exploiting weaknesses in user behavior. The results also show that deauthentication attacks are still effective before establishing a 4-way handshake. This paper proposes some countermeasures to reduce the risk of home network penetration.

Index Terms: Wi-Fi Security, WPA2, WPA3, deauthentication attack, dictionary attack, evil twin attack, Penetration testing

1. Introduction

With the rapid development of the digital age, wireless communication, especially the wireless local area network Wireless Fidelity (Wi-Fi) has become very important in various institutions. Wireless access to local areas provides the advantage of mobility, as users can connect to the network while roaming freely without using physical wires [1]. The Media Access Control (MAC) address is a unique identifier assigned to a network adapter within a router. The group of devices that communicate with each other within an 802.11 network is called the Basic Service Set (BSS), while the MAC address used by the wireless interface of an access point is called the Basic Service Set Identifier (BSSID). The network name assigned by network administrators, such as " home network ", is called the Service Set Identifier (SSID). When a Wi-Fi-enabled device is in range of a network, it can discover the network by name and attempt to connect to it [2,3]. This research paper presents an assessment of the security of wireless networks through penetration testing, which is a comprehensive method for identifying vulnerabilities in the system. It can also be defined as a mechanism for penetration without damaging or destroying the network. Penetration testing is also known as red team, white hat hacker, or ethical hacking [4,5].

2. Related Works

In 2018, C. P. Kohlios and T. Hayajneh, presented a systematic and comprehensive theoretical study of possible attacks on the latest Wi-Fi security standards. it has been concluded that WPA3 is not affected by the following attacks: deauthentication attack, dictionary attack, and Pairwise Master Key Identifier (PMKID) Dictionary attack. Ident, and Key Reinstallation Attacks (KRACK), while the Evil Twin attack is still possible, one of the interesting findings in this paper is that after penetrating local networks that support WPA3, The network still lacks addressing all the problems found in Wi-Fi Protected Access2 (WPA2). The most prominent of these problems are Man In the Middle (MITM) attacks [6].

In 2022, D. Schepers, A. Ranganathan, and M. Vanhoef, examined the robustness and protection of Management Frame Protection (MFP) in the latest WPA3 and Wi-Fi 6 standards. While analyzing the 802.11 MFP rules, they found inconsistent rules for handling strong management frames, and insecure rules that lead to denial of service vulnerabilities. They were able to prevent a client from joining the network or disconnect any client despite the forced use of Management Frame Protection (MFP). As a result, they concluded that the use of MFP is insufficient to protect against deauthentication attacks. The research also suggested some recommendations for countermeasures [7].

In 2022, L. R, A. Sharma, B. S, C. B, and M. G M, studied different Wi-Fi protocols with their features, weaknesses, key generation methods, encryption processes, and how the weaknesses can be mitigated through improvements. The study concluded that Wired Equivalent Privacy (WEP) is the most vulnerable and fragile protocol and was replaced by WPA, and WPA2 is the most widely implemented and robust encryption protocol. WPA3 is the latest protocol that aims to provide a second line of defense in communications involving weak passwords because it has strong encryption that is difficult to crack [8].

In 2023, J. Cathcart and T. Khan Mohd, presented a study analyzing five password cracking tools in Kali Linux. The attacks included in this experiment are dictionary-based. Each application is examined through 5 attributes: speed, efficiency, complexity, design, and versatility. It was concluded from practical experiments that (hydra), (Fern WiFi cracker), and (hashcat) are less efficient compared to (aircrack-ng) and (wifite), as they gave a complete analysis of attacks. This still does not diminish the potential of these first three tools if used successfully [9].

In 2023, L. Wang, C. Chin Ta, and T. Chih Ming, conducted a penetration test of a Wi-Fi network using WPA2 encryption, This paper proposes to attack the wireless network using penetration testing tools from Kali Linux. The (aircrack-ng) toolkit is used to crack the Wi-Fi password, which is based on the bit code form of the password. After trying several passwords of 26 uppercase and lowercase letters using computers and password dictionaries, the Wi-Fi password can be quickly obtained through a high-speed laptop, bringing the benefits of simplicity, speed and stability. In addition, some tips are proposed to improve the security level of the wireless network [10].

Among the studies reviewed, some research papers examined and analyzed WLAN security standards, while others simulated penetration testing of these standards to assess security levels and detect vulnerabilities. Most penetration testing research was conducted on the currently most common standard, WPA2, while research on WPA3 was mostly analytical and theoretical, lacking practical testing. WPA3 is still rarely used worldwide, and there are no dedicated tools for penetrating by advanced attacks against this protocol, such as side-channel attack. Therefore, this paper will test the WPA3 penetration and robustness against common cyberattacks (such as deauthentication attacks, evil twin attacks, and dictionary attacks) using the same tools used to crack WPA2. Additionally, it will test the effectiveness of MFP against deauthentication attacks and the effectiveness of social engineering techniques used to obtain personal data.

3. Theoretical background

3.1 Wi-Fi Security Standards

The IEEE 802.11 standard specifies four strong security protocols (WEP, WPA, WPA2, WPA3) to secure information exchange at the MAC layer. These protocols were developed by the Wi-Fi Alliance [11].

Wired Equivalent Privacy (WEP) was introduced in 1997 to provide wireless security equivalent to wired LANs by using Rivest Cipher 4 (RC4) encryption with a 64-bit encryption key, which is a simple encryption that can be cracked as different cryptanalysis methods can decrypt the data. For this reason, the Wi-Fi Alliance officially abandoned WEP in 2004 [12,13].

The Wi-Fi Protected Access (WPA) protocol was officially introduced in 2003, with the aim of solving the security weaknesses of the WEP standard. This fix was necessary because WEP had become obsolete and left Wi-Fi networks without security at the MAC layer [14]. It is worth noting that WPA has two modes of operation: Pre-Shared Key (WPA-PSK) mode, known as WPA-Personal mode, and Enterprise mode (WPA-Enterprise) [15]. The IEEE 802.11 Task Force and the Wi-Fi Alliance created WPA, which uses Temporal Key Integrity Protocol (TKIP) encryption and a 128-bit Pairwise Transient Key (PTK) encryption key to replace WEP without the need to replace older hardware by upgrading wireless network interface cards and using TKIP [16]. Although WPA has many advantages over the previous WEP standard, it is not considered strong enough and has many vulnerabilities and was

deprecated in 2012 [17].

The second version of Wi-Fi Protected Access (WPA2) was introduced in 2004, one year after WPA. The WPA2 security standard was developed for two reasons: first, to solve all the flaws and security problems that WPA had. Second, to replace the first security standard WEP with a more advanced and long-lasting standard [18]. WPA2 uses the Cipher Block Chaining Message Authentication Code Protocol (CCMP), which uses the Advanced Encryption Standard (AES) algorithm. The use of WPA2 requires new devices that support AES. WPA2 continues to incorporate TKIP to maintain compatibility with other existing devices [12]. CCMP encryption is primarily based on the AES algorithm, which is an encryption algorithm that supports keys with a length of 128 bits. CCMP encryption uses a pairwise transitional key (PTK) if the message is unicast, and a group temporary key (GTK) if the message is broadcast [6]. To generate a key in WPA2, a 4-way handshake is required to obtain a pairwise transitional key (PTK) and a group temporary key (GTK). In the 4-way handshake protocol, both the user and the access point need a pairwise master key (PMK) generated from the authentication process to derive a pairwise transitional key (PTK), which is then used to derive a Message Integrity Code (MIC) to ensure data integrity and avoid cross-site spoofing attacks [6]. WPA-AES encryption has become the most popular in both home and business settings because it is more resistant to network attacks and has two modes of operation (WPA-Personal and WPA-Enterprise). Although the WPA2 security standard has been in use for nearly 20 years, it has several vulnerabilities.

In 2018, the Wi-Fi Alliance announced the third version of Wi-Fi Protected Access (WPA3) and in 2020, WPA3 became mandatory for certified wireless applications. The adoption rate of WPA3 was expected to grow rapidly, but statistics have shown otherwise [19]. The enhancement of the security of the WPA2-PSK handshake was the main motivation for the development of WPA3. Like its predecessor, WPA3 also has two operating modes: WPA3-Personal and WPA3-Enterprise [20]. WPA3-Personal uses Simultaneous Authentication of Equals (SAE) also known as Dragonfly handshake for authentication and key management, which is a secure key exchange protocol designed for authentication purposes. Authentication is performed based on the shared password (PSK) between all parties to the handshake. WPA3-SAE authentication produces a paired master key (PMK), which will be used as input for the 4-way handshake to create a 192-bit PTK, which is better than WPA2's 128-bit key length. SAE is therefore stronger than the PSK used in WPA2 and protects against dictionary and brute force attacks [21]. Protected Management Frames (MFP) are mandatory with WPA3-SAE to prevent deauthentication attacks where attackers force users to disconnect from the access point (AP). Not all devices Current 802.11 protocols are capable of supporting either MFP or SAE, so WPA3 provides a transition mode that supports both WPA2 and WPA3 simultaneously, where non-WPA3 devices will connect using a 4-way handshake without MFP, and WPA3 devices will connect using an SAE handshake with MFP. WPA3-Enterprise is essentially unchanged from WPA2, but instead focuses on adding improvements and increasing resistance to abuse [22].

The adoption of new standards and the prompt phasing out of outdated and dangerous protocols remain crucial to safeguarding Wi-Fi networks, even if the Wi-Fi Alliance announced WPA3 as a replacement for WPA2, giving enhanced security and minimizing vulnerabilities caused by bad password choices. Devices that use older standards (like Apple's operating systems) now display a warning to promote the adoption of current standards. In a similar vein, the Wi-Fi Alliance suggests using user interface symbols to show which standards the network is compatible with [23]. A late 2021 survey of one million access points found that 2.22% of encrypted networks offered PMF, These results are surprising, given that IEEE 802.11w was released more than fifteen years ago, 0.06% offered WPA3 with transitional mode, and 0% of networks mandated WPA3 only [24].

3.2 Management Frames

This section introduces the basic management frames, as they are important during the establishment of the connection. Some attacks that we will discuss later rely on them. Management frames can be divided into two main types, the first is unprotected management frames, and the second is protected management frames.

3.2.1 Unprotected management frames:

- Bacon: of alert neighboring Wi-Fi-capable devices of the network's existence, the access point broadcasts "bacon frames." They are provided on a regular basis and include details about the capabilities and setup of the network, including encryption and frequency information.
- Probe Request and Probe Response: A user can send a probe request to get information from all nearby access points or from a particular network.
- Authentication Request and Authentication Response: Authentication Request and Authentication Response: Using their security credentials, the user sends out an Authentication Request to the appropriate network following receipt of the Probe Response.
- Association Request and Association Response: Following his selection of the desired access point, the user sends an Association Request to that access point.
- Deauthentication and Disassociation: To disconnect from the network, the user must send an access point a Disassociation Frame. He must submit a Deauthentication Frame instead if he wants to discontinue the authentication relationship. There is only one field in both frames, and that is the explanation for ending the relationship [25].

3.2.2 Protected Management Frames (PMF):

Also called the Management Frames Protection (MFP). As an advancement of the 2003-issued (IEEE 802.11) standard, the Wi-Fi Alliance introduced (IEEE 802.11w) in 2009 to boost the security of Management Frames [7], A feature PMF guards against numerous attacks related to management frames while also providing data confidentiality, integrity, and authentication. This functionality authenticates and encrypts disassociation and deauthentication frames. It hinders denial-of-service (DoS) assaults and makes it harder for an adversary to remove users' authenticated accounts from the network. Since Protected Management Frames (PMF) rely on already-in-place security measures, frames transmitted prior to the transmission key (PTK) cannot be secured. In other words, probes (requests and responses) and beacons cannot be secured [26]. Since not all users support IEEE 802.11w, the Wi-Fi Alliance has made it optional for WPA and WPA2 and required for WPA3. As a result, usage is discussed between the user and the access point [27].

3.3 De-authentication Attack

De-authentication Attack: The de-authentication attack has been around since the early days of Wi-Fi, where an adversary aims to disconnect a user from the network in order to disrupt service or cause a sustained denial of service (DoS) attack, rendering the network useless to one or more users [7][28]. In such an attack, the address of the access point responsible for sending the deauthentication frames is spoofed, and then fake deauthentication frames are injected to force users to leave the network [29]. The goal of PMF is to prevent an adversary from spoofing deauthentication frames and forcibly disconnecting the user from the wireless network. Unfortunately, this prevention is done after the four-way handshake (after the PTK key is installed). However, an attacker can still spoof the deauthentication packet before this handshake and can cause a service outage for a user trying to connect to the network. In addition, an attacker can spoof a Beacon Frame and advertise unsupported configurations in Information Elements (IEs), for example, an invalid bandwidth configuration, which causes the user to force a deauthentication process, resulting in a disconnection. From the above, it is clear why PMF is not sufficient to prevent deauthentication attacks [7,30].

3.4 Dictionary Attack

It is the process of guessing the password by attackers to breach the privacy of users. Dictionary Attack is classified into active dictionary attack and passive dictionary attack, also known as offline dictionary attack [31]. The WPA/WPA2 PSK protocol is vulnerable to offline dictionary attacks. The way the WPA/WPA2 PSK protocol works is that it derives a session-by-session key called the Pairwise Transitional Key (PTK) from the random numbers exchanged in the 4-way handshake, which will be different in each session, making the PTK renewable in each session as shown in Fig.1.

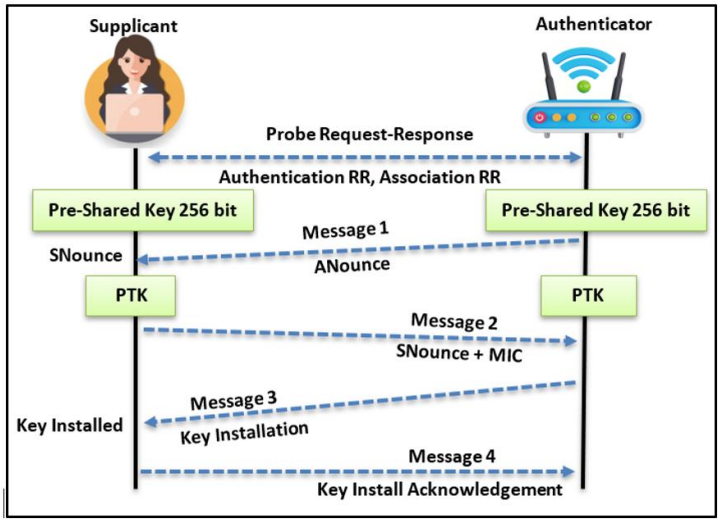

Fig. 1. 4-way handshake [32].

The pairwise transition key (PTK) is derived from the pre-shared key (PSK) and five pieces of information exchanged between the user and the access point during the 4-way handshake, namely the network name (SSID), the authenticator Nounce (ANounce), the supplicant Nounce (SNounce), the user's MAC address, and the access point's MAC address. All of this information is transmitted as plain text without encryption during the handshake except for the PSK [32].

The PTK is used to encrypt all data between the access point and the user. An attacker, eavesdropping on the conversation between the user and the access point, can obtain all five pieces of information mentioned in the previous paragraph. The only thing that cannot be obtained is the pre-shared key (PSK). The PSK is derived from the password (WPA-PSK) and the network name (SSID). This information is fed into the Password-Based Key Derivation Function 2 (PBDKF2), which produces the 256-bit PSK [6], Fig.2 illustrates an offline dictionary attack.

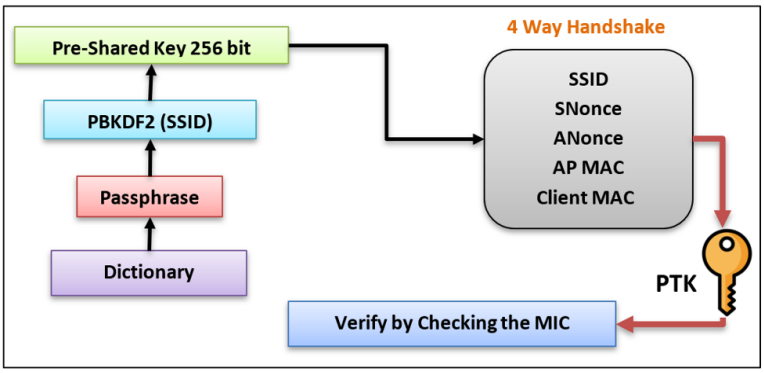

Fig. 2. Offline Dictionary Attack [32].

In a typical WPA/WPA2 PSK dictionary attack, the attacker uses a large dictionary of possible passphrases using an attack tool. The tool extracts the 256-bit pre-shared key (PSK) from each passphrase and uses it, along with the other information described earlier, to create a PTK. The PTK will be used to verify the Message Integrity Check (MIC) in one of the handshake packets. If it matches, the guessed passphrase from the dictionary was correct; if it doesn't, it's incorrect. Finally, if the valid network passphrase is in the dictionary, it is recognized. This is how the WPA/WPA2 PSK protocol is cracked [6,33].

In an active dictionary attack, the attacker continuously changes his MAC address so that the attack is not detected. Multiple virtual wireless clients (VWCs) are created using a single WLAN interface card. Each VWC will simulate an independent wireless user to the access point. To speed up the process, we can use multiple virtual machines that act as separate users to the access point. All VWCs start guessing the passphrase in parallel. As long as the wireless session is active, the VWC will continue guessing the passphrase repeatedly until a deauthentication frame is received from the access point [31,34]. Active dictionary attacks can be used to recover the WPA2-PSK passphrase when the attacker cannot capture the 4-way handshake frames between the access point and the authenticated user [38]. WPA3 was introduced to combat offline dictionary attacks using the SAE protocol, where the attacker will not be able to see the word list and calculate the PSK. Which comes from dragonfly handshake to test MIC of PTK without internet connection and without interacting with the authenticator. However, through downgrade attack, it became possible to perform passive dictionary attack on WPA3-SAE protocol, and WPA3 is still vulnerable to active dictionary attack [31,35].

3.5 Evil Twin Attack

An evil twin attack is when a hacker creates a spoof network with the target network's MAC, BSSID, and SSID in an effort to fool people or devices into joining to it. The attacker functions as a man-in-the-middle (MITM) and can decrypt, view, and control the traffic that a user transmits and receives from their device when their device connects to the evil twin network. An MITM attack is categorized as an evil twin assault. Deauthentication signals must be sent by the attacker to remove the user's authentication from the legitimate access point. The user's device will reconnect after disconnecting and begin its connection search anew. Most devices will typically select the network with the stronger signal, as shown in Fig.3, when given a choice between two access points with the same SSID. Networks that are open to the public, require authentication before users can connect, and have passwords that are unknown are all susceptible to an evil twin assault. The user may be tricked by an enemy by opening a captive portal-style Attack of the Evil Twins [6,36].

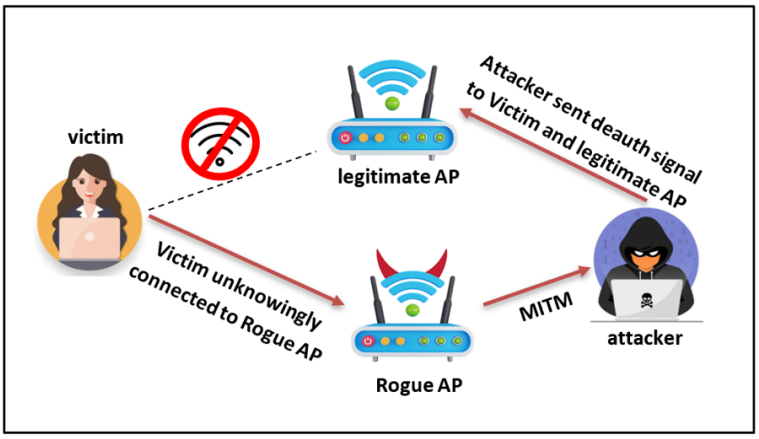

Fig. 3. Evil Twin Attack [37].

4. Methodology

The proposed methodology is a penetration test for a home network that supports personal mode, the tools needed to set up a secure penetration lab, and a plan to execute a set of attacks on the network.

Laboratory Setup: A wireless laboratory is established in this research to conduct practical penetration experiments, and to ensure a safe and controlled environment.

4.1 Hardware requirements we need to set up the penetration lab:

1. Access point: A mobile phone (realme, V3.0) that supports the standards (WPA2, WPA2/3, WPA3) was used as an access point, where the mobile phone was used instead of a router for the ease of portability of the lab and also because it supports the latest standard (WPA3).
2. In this lab there are three devices, the first (User1) works as a victim which is a laptop (Lenovo, DESKTOP-I6BOT1Q) that does not support the (WPA3) protocol, the second device (User2) works as a victim which is a mobile phone (Galaxy A04s) that supports the (WPA3) protocol. The third device is a laptop (Razer, DESKTOP-MJS8ORR, RAM=16GB) that works as an attacker.
3. Wi-Fi adapter: Inside the attacker's laptop, there is a Wi-Fi adapter, but it does not support Monitor mode and packet injection. Therefore, an external Wi-Fi adapter (ALFA, AWUS036NH, USB Adapter) was used for this purpose.

4.2 Software Requirements:

1. VMware is a software that allows the creation of virtual machines inside a real computer. It was used to install the operating system (Kali Linux 2023.2) that plays the role of the attacker.
2. Kali Linux: The version used in this research is (Kali Linux 2023.2). To conduct penetration tests, we need to download and install the following tools on the (Kali Linux) system: Aircrack-ng, Airodump-ng, Aireplay-ng, Wireshark, Bettercap, Fluxion. These tools were selected after extensive review and testing of a variety of available wireless network penetration testing tools. They demonstrated the best performance and effectiveness within the context of our methodology, making them the most suitable choice for achieving our research objectives and providing accurate and reliable results.

4.3 Proposed Penetration Test Model:

The penetration test aims to evaluate the security level of a home wireless network that supports (WPA2/WPA3) encryption and supports personal mode. Fig.4 shows the structure of the home network. there are four hypotheses:

1. If the protocol used in encryption is WPA2, the steps to crack the encryption are shown in Fig.5.
2. If the protocol used in encryption is WPA3, that supports the transitional mode, the steps to crack the encryption are shown in Fig.6.
3. If the protocol used in encryption is WPA2, the steps to implement the evil twin attack are shown in Fig.7.
4. If the protocol used in encryption is WPA3, the steps to implement the evil twin attack are shown in Fig.8.

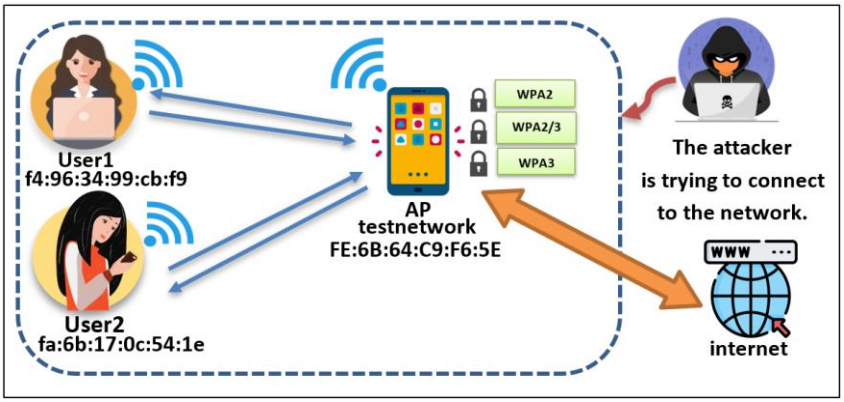

Fig. 4. Home network structure

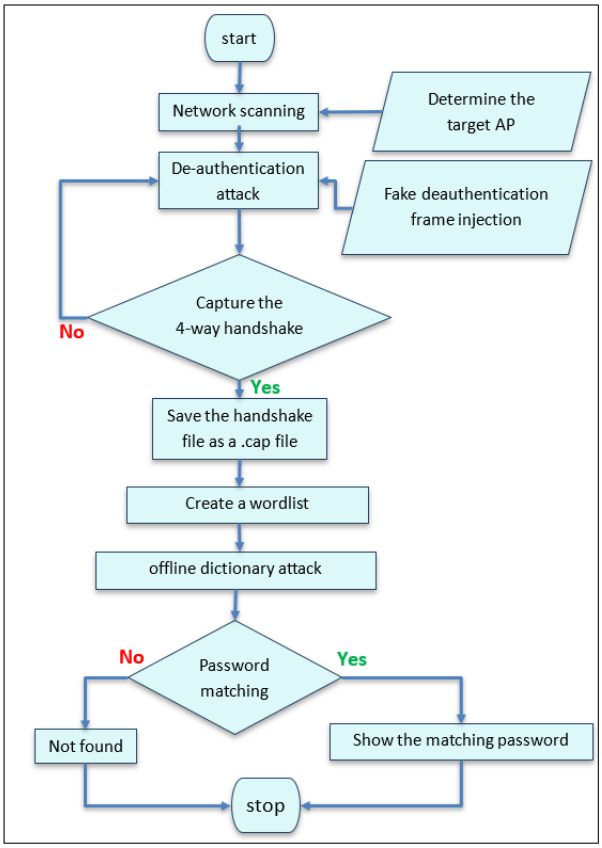

Fig. 5. WPA2 encryption cracking test

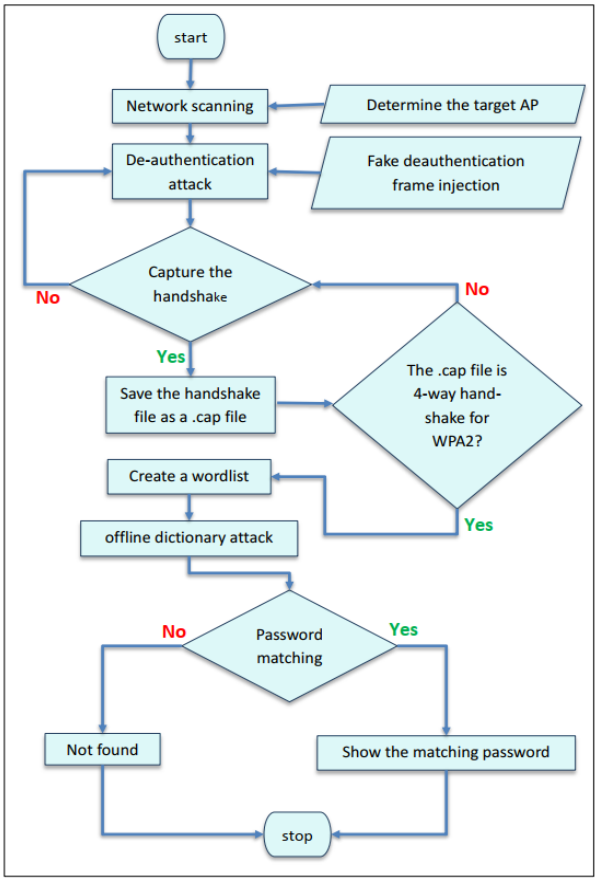

Fig. 6. WPA3 protocol hacking supports transitional mode

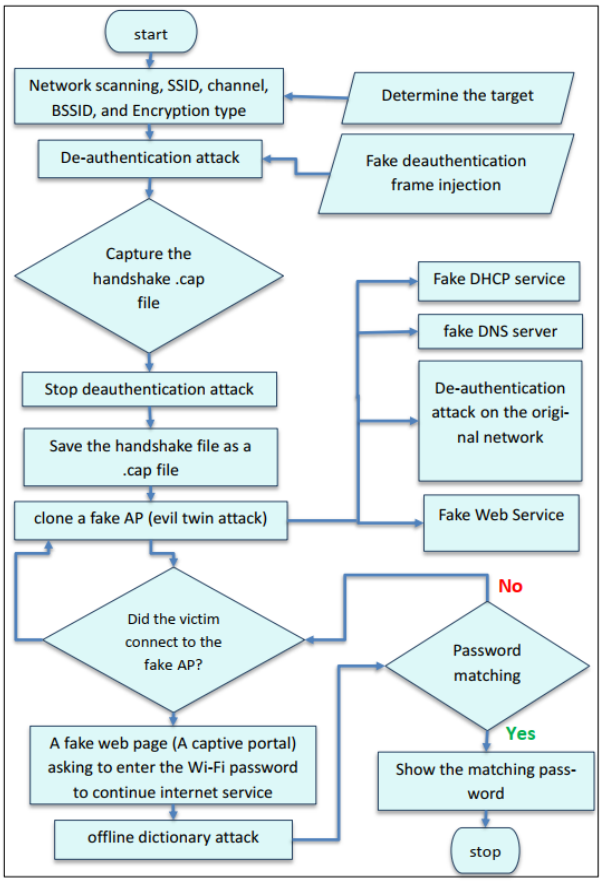

Fig. 7. Evil Twin Attack on WPA2 Protocol

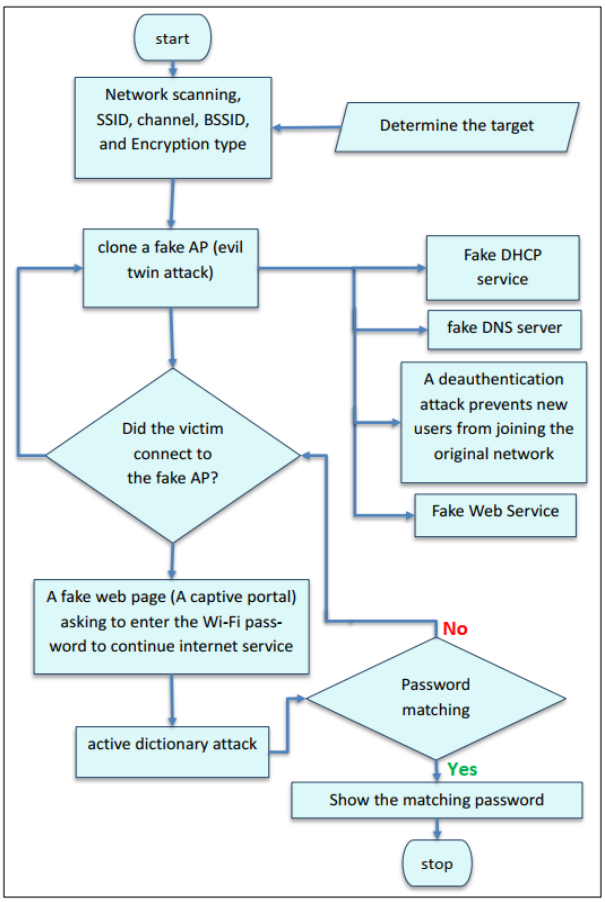

Fig. 8. Evil Twin Attack on WPA3 Protocol

5. Practical Steps and Results

1-WPA2 protocol encryption cracking test: A scan of access points is performed, or what is called passive eavesdropping or packet sniffing using the "airodump-ng" guides. Fig.9 displays the information table obtained as a result of the passive eavesdropping process, and includes information about the wireless access points within the range of the wireless adapter, including the network name (SSID), the channel allocated for broadcasting (CH), the type of encryption used (ENC), the (MAC) address of the access points (BSSID), and the (MAC) addresses of the users (STATTION) connected to each access point.

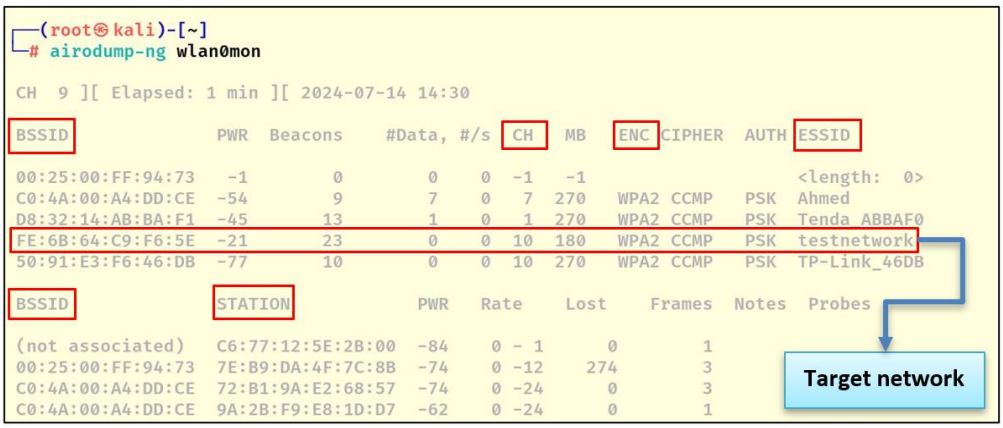

Fig. 9. Scans for nearby access points

The access point (testnetwork) is selected to be hacked, (SSID=testnetwork, BSSID=FE:6B:64:C9:F6:5E, CH=10, Encryption protocol=WPA2). The purpose of monitoring the network is to obtain the handshake file (4-way handshake) to perform an offline dictionary attack, to focus on the target network and hide the rest of the networks and to capture more packets, the network information (testnetwork) is added to the "airodum-ng" command and also a file with the extension (WPA2.cap) to store the handshake packets (4-way handshake) as shown in the Fig.10.

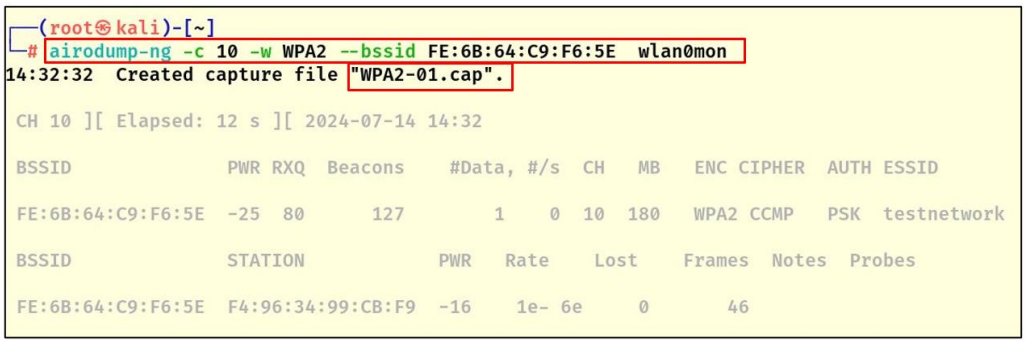

Fig. 10. Monitor the target network and wait for the handshake file to be captured

Handshake packets can only be retrieved when a user joins the network, which can take a long time. To speed up the process, a deauthentication attack is applied to force users to leave the network and reconnect. Using the “airreplay-ng” tool, as shown in Fig.11, the network MAC address is spoofed and fake deauthentication frames are injected. Users are forced to leave the network and try to reconnect, enabling the 4-way handshake to be captured.

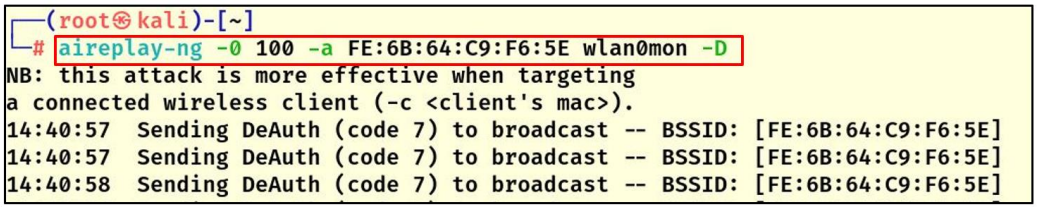

Fig. 11. deauthentication attack

After successfully capturing the handshake packets that will appear on the “airodump” eavesdropping station, they are stored in the file “WPA2-1.cap” as shown in the Fig.12. The first line displays the current channel, the time taken to

capture the handshake, and the current date/time.

After that, the tools "airodump-ng" and "aireplay-ng" are stopped. With the availability of both the handshake file "WPA2-1.cap" and the default wordlist file "wordlist-probable.txt" in Kali which contains (203814) commonly used passwords, the dictionary attack becomes possible, using the tool "aircrack-ng" the encryption (WPA2-PSK) was successfully cracked and the password is "abcdefgh" as shown in the Fig.13.

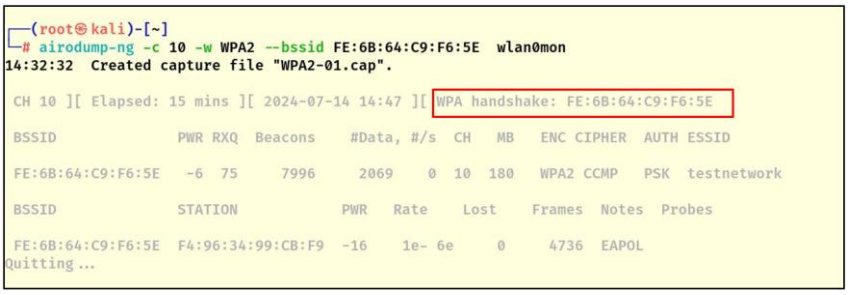

Fig. 12. Capture handshake file

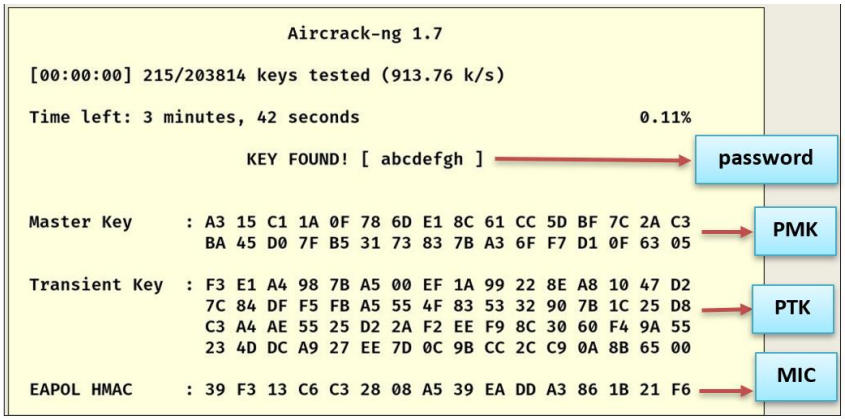

Fig. 13. Dictionary attack

2 - WPA3 protocol encryption cracking test supports transitional mode: Passive eavesdropping was applied to capture available networks using the tool "airodump-ng" as shown in Fig.14. Fig.15 shows the selection of the target network (SSID=testnetwork, BSSID=FE:6B:64:C9:F6:5E, CH=10, Encryption protocol=WPA2/3), and the preparation of a file to capture the handshake (WPA2,3.cap).

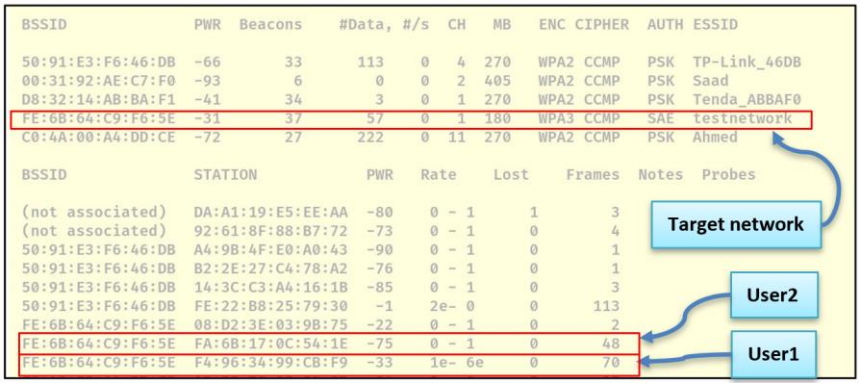

Fig. 14. Scanning access points within the wireless adapter

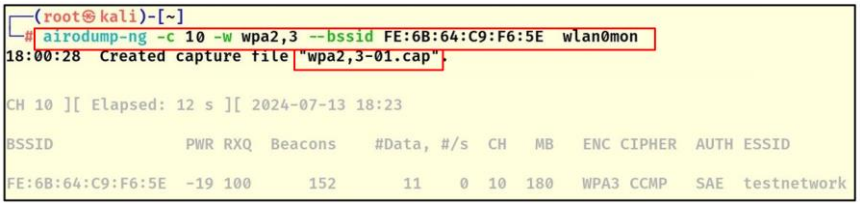

Fig. 15. Eavesdropping on the target network and creating a file to capture the handshake

In this part of the penetration test, there are two users on the network, the first (User1=f4:96:34:99:cb:f9) supports the WPA2 protocol that uses PMF optionally, and the second (User2=fa:6b:17:0c:54:1e) supports the WPA3 protocol that uses PMF mandatory. A deauthentication attack is performed. To verify the effect of this attack on the users, the packets are analyzed in the “Wireshark” program as shown in the Fig.16. Despite sending deauthentication frames, there is no response from the users, and the fake frames were unable to disconnect the users from the network.

However, when users leave the network, they cannot rejoin the network while the deauthentication attack is being carried out, i.e. the attack is still active with PMF. As shown in Fig.17, the attack blocks connection attempts and prevents the 4-way handshake.

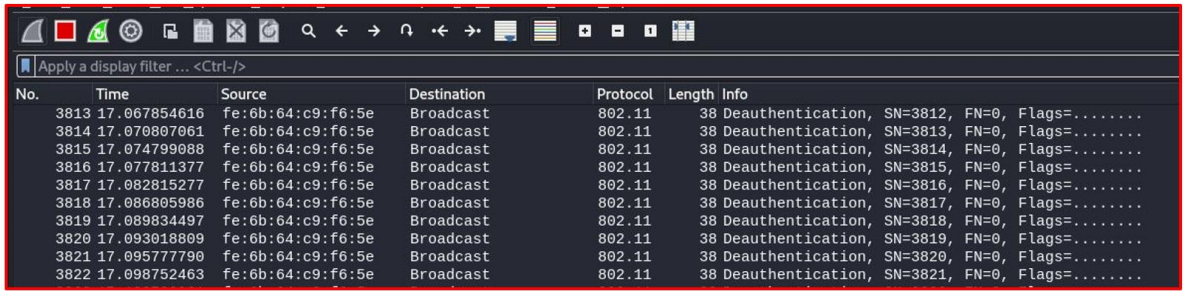

Fig. 16. Failed deauthentication attack

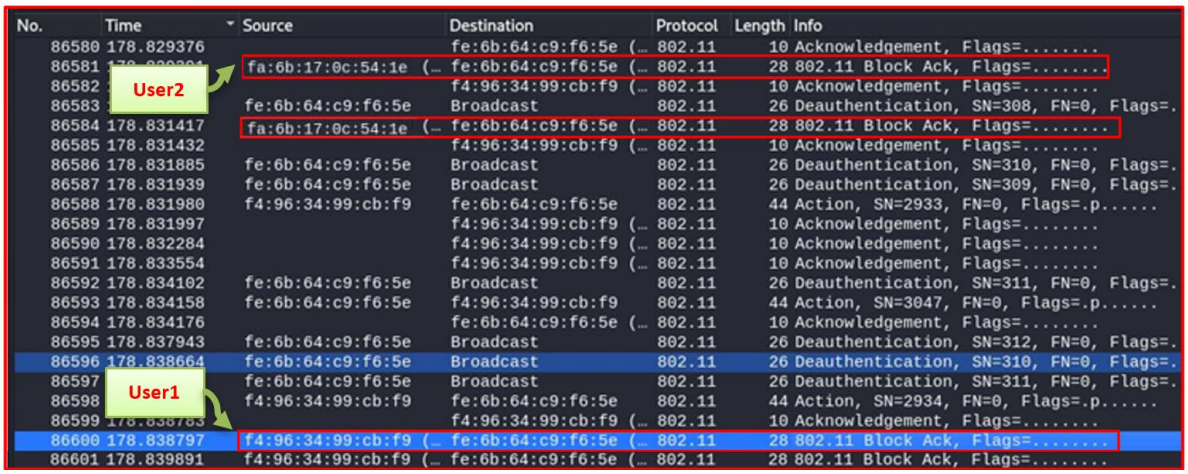

Fig. 17. Preventing the user from connecting to the network before the 4-way handshake

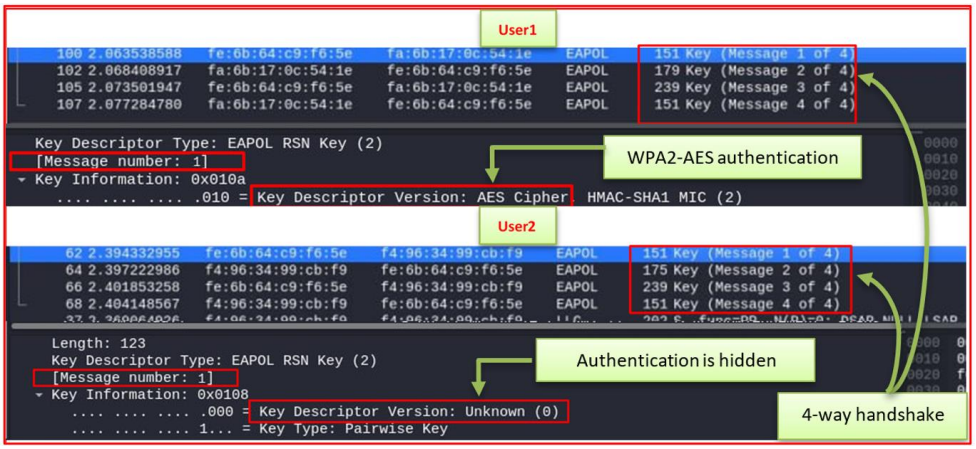

Fig. 18. Enables users to perform a 4-way handshake and join the network

Once the deauthentication attack is stopped, users (User1) and (User2) can connect to the network as shown in Fig.18. At the same time, the tool "airodum-ng" was able to capture the handshake files (WPA2,3-01.cap) and (WPA2,3-02.cap). A dictionary attack was performed on each of the captured handshake files using the tool "aircrak-ng". Fig.19 shows the success of the attack, indicating the use of the (WPA2) protocol, and Fig.20 shows the failure of the dictionary attack because the protocol used is (WPA3). In practice, most (Wi-Fi) networks are connected to many users, so it is preferable to search for a user connecting using the (WPA2) protocol to the network to avoid repeating the unnecessary dictionary attack. The user connected via the (WPA2) protocol can be identified by the type of

authentication negotiated in the first message of the handshake (4-way handshake) as in Fig.18. In WPA3, the authentication type is encrypted.

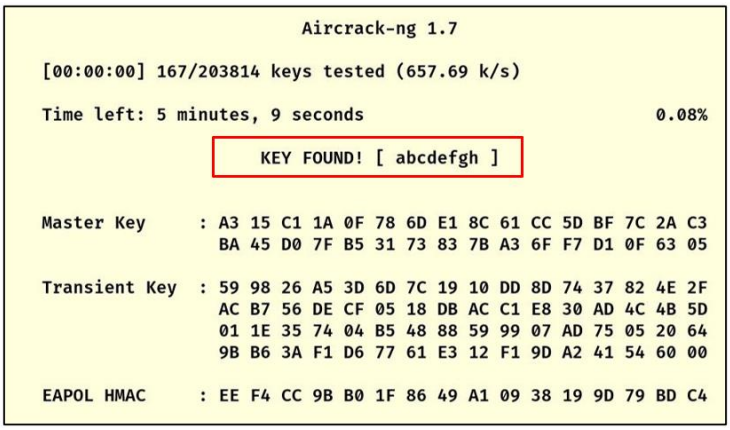

Fig. 19. Dictionary attack success on WPA2 protocol

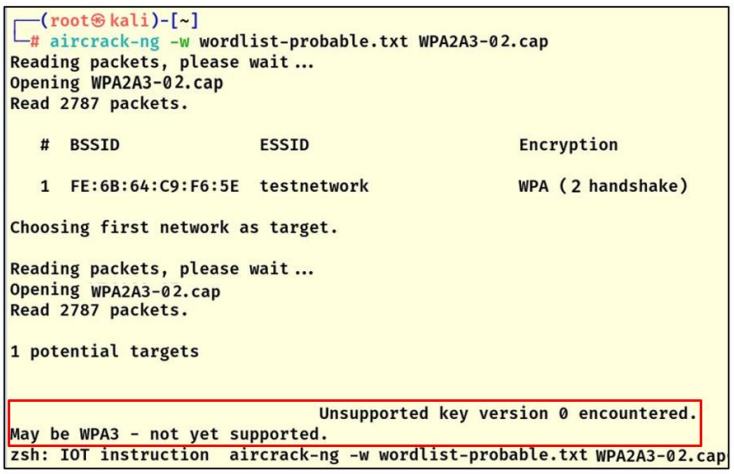

Fig. 20. Dictionary attack on WPA3 protocol failed

3- Evil Twin Attack on WPA2 Protocol: The password of the targeted access point is recovered by a Captive portal-style Evil Twin Attack, and a social engineering attack (phishing) using the "Fluxion" tool, where a legitimate access point is cloned and users are tricked into connecting to it. To clone a network, all we need is the network name, MAC address, used channel, speed, and signal strength as shown in the Fig.21, this information is easily obtained by sniffing the management packets (Bacon frame) broadcast by the access point as plain text and captured by (Kali Linux) when monitoring mode is enabled, and the information of the available networks is extracted by the "airodump" tool, which is activated by "Fluxion" when the command "scan all channels" is given. The next step is to select the target network by giving the command "select target".

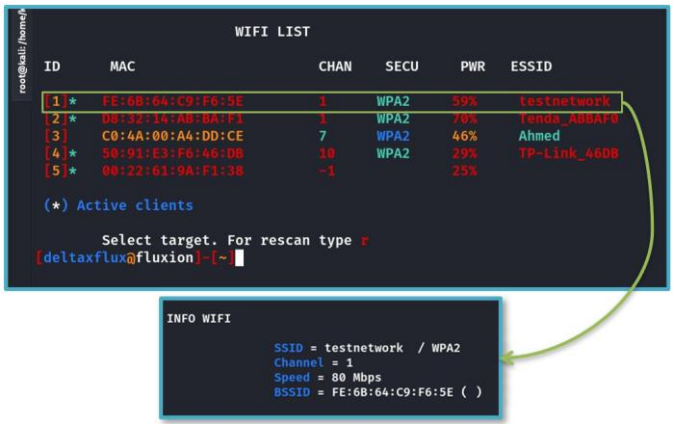

Fig. 21. Specify target network information

After selecting the target network and determining the type of attack that will be carried out, “Fluxion” lists a set of attacks to choose from. A fake network access point can be cloned using the “Hostapd” or “Airbase-ng” tool, or a dictionary attack can be used to crack the network password using the “Aircrack-ng” tool. The fake access point cloning attack is selected by giving the command (FakeAP – Hostapd). "fluxion" provides several ways to capture the handshake file. The "pyrit" tool was used to capture the 4-way handshake file, and the "airpelay-ng" tool was used to initiate a deauthentication attack and speed up the process of obtaining the handshake file, which is later used to verify the validity of the password. As shown in Fig.22, the handshake file was captured successfully. Once the handshake file is captured, the deauthentication attack is terminated.

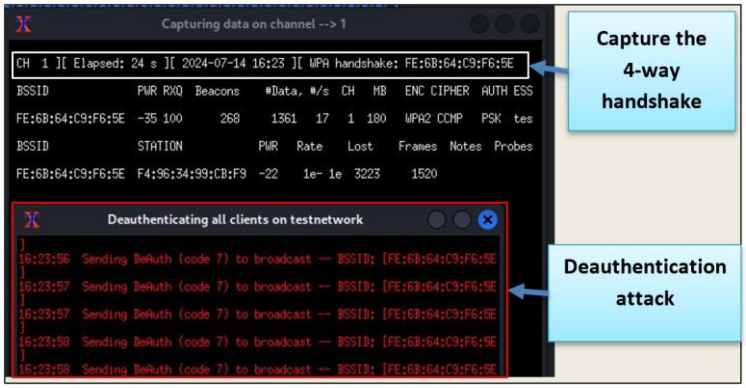

Fig. 22. performs a deauthentication attack and captures the handshake file

The captive portal that is displayed to the victim when connecting to the fake access point is then configured, where "fluxion" provides several examples of password entry pages that are displayed on the "Lighttpd" web server inside "fluxion".

The fake access point is then created that mimics the original access point, by activating five windows at the same time as shown in the Fig.23, below is an explanation of the function of each window:

- The first window (Wi-Fi Information): This window records SSID, MAC and other information about the fake network that is transferred to the victim's device. It also displays a list of victims connected to the fake network, and displays the attempts to enter the password by the victims and the result of checking whether the password is correct or incorrect using the "Aircrack-ng" tool.
- The second window (Deauth all [mdk3] testnetwork): It carries out the deauthentication attack for the different devices connected to the targeted access point, where the MAC address of the targeted access point is impersonated and fake deauthentication frames are sent using the "mdk3" tool to prevent devices from connecting to the legitimate access point and force them to connect to the fake access point.
- The third window (AP): It is responsible for receiving and sending the management frames, so that users can connect to the fake network.
- The fourth window (DHCP): It is a fake DHCP-server to respond to DHCP requests and give the victim an IP address when joining the fake network. It is activated using the "dhcpd" tool found in the "fluxion" toolkit.
- The fifth window (FAKE DNS): It is a fake DNS-server that redirects all DNS requests to a login page (captive portal) that requests the network password to obtain Internet service. The fake access point is not connected to the internet so the victim will not be able to browse websites when connected to it, and all DNS queries generated from the victim's device will be answered by this service.

What happens on the victim's screen is that the original network is disconnected and unable to connect to it, and at the same time there is a matching open network (without encryption protocol) once connected to it the victim is redirected to the fake captive gateway, where he is asked to enter the correct Wi-Fi password to reconnect to the network. If he enters an incorrect password, "Aircrack-ng" will detect that this is not the correct password and ask the victim to re-enter the password, where the offline dictionary attack is performed on the handshake captured before creating the fake network with the password that the victim entered in the captive gateway. Once the correct Wi-Fi password is entered, the message "Your connection will be restored in a few moments" appears as shown in Fig.24, "Fluxion" will stop the rogue access point, allowing the victim to reconnect to the real access point. "Aircrack-ng" then displays the Wi-Fi password on the first window as shown in Fig.25.

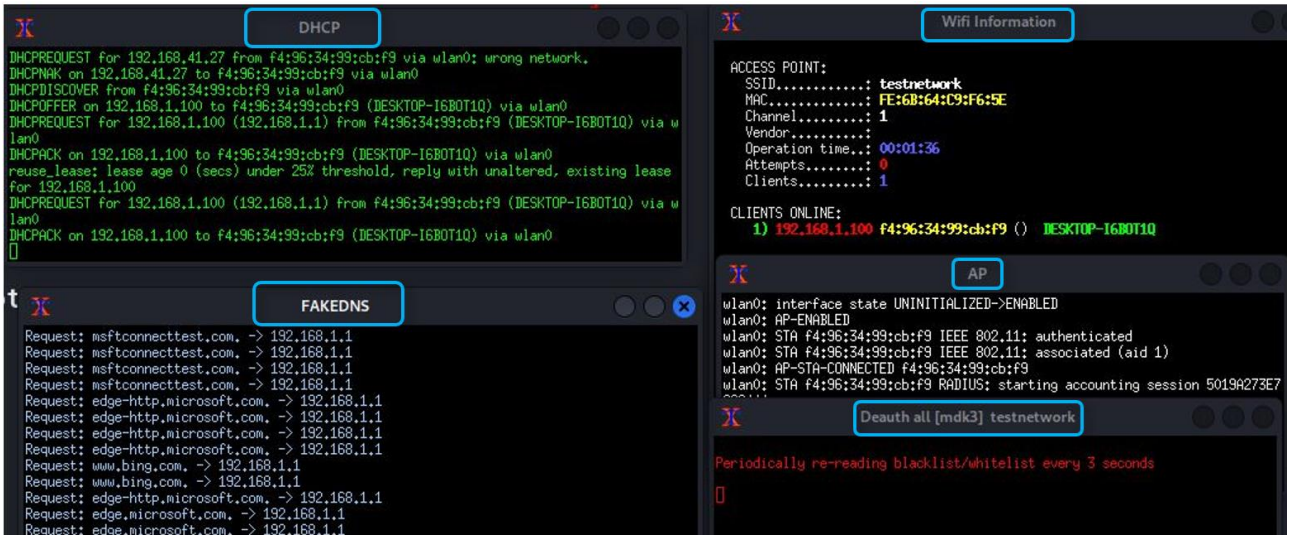

Fig. 23. Create a fake access point

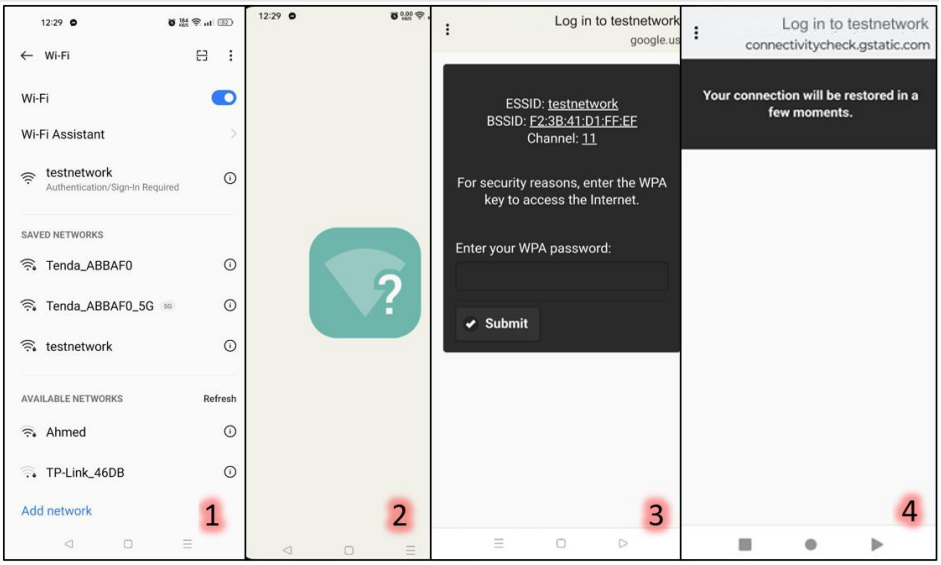

Fig. 24. What happens on the victim's screen during the attack

Fig. 25. Gets the correct password and displays it on the first window

4- Evil Twin Attack on WPA3 Protocol: Hacking the WPA3 protocol using the evil twin attack using the captive portal method will be similar to hacking WPA2 with some differences.

Using passive eavesdropping, the target network and the information we need to create a fake network are identified as shown in Fig.26, we do not need to capture the handshake file because offline dictionary attacks are not possible with WPA3, the captive portal is directly configured and the fake access point is created as explained previously by activating five windows as shown in Fig.27.

The only difference between the five windows and the previous experiment will be that the first window was unable to verify whether the passwords entered by the victims were correct or incorrect, and therefore no password was displayed on the first window, but only the information that is transmitted to the victims, as the "Fluxion" tool is designed to hack the WPA1/2 protocol and to display the password on the first window if it is correct or incorrect after performing the offline dictionary attack on it. Therefore, a sixth window must be created to capture everything that the victims enter into the restricted gateway. Since the restricted gateway uses the (HTTP) protocol to transfer data, the data is transferred as plain text without encryption. Using the "Bettercap" tool, the packets transferred within the fake network that contain attempts to enter the password are sniffed through passive eavesdropping. Since the protocol used is WPA3 which prevents deauthentication attacks after performing the 4-way handshake, this has led to the inability to disconnect users from the original network, but it is still possible to prevent users who try to join the original network. Once a victim connects to the fake network, the Captive portal is displayed asking for the password as shown in Fig.24. The passwords that the victim enters will appear on the sixth gateway that was created as shown in Fig.28. The correctness of the password can be verified by logging into the original network or what is known as an active dictionary attack. If the password is correct, the fake network is stopped, otherwise the fake network remains active to force the victim to re-enter the correct password. Table 1 shows a summary of the penetration test results obtained.

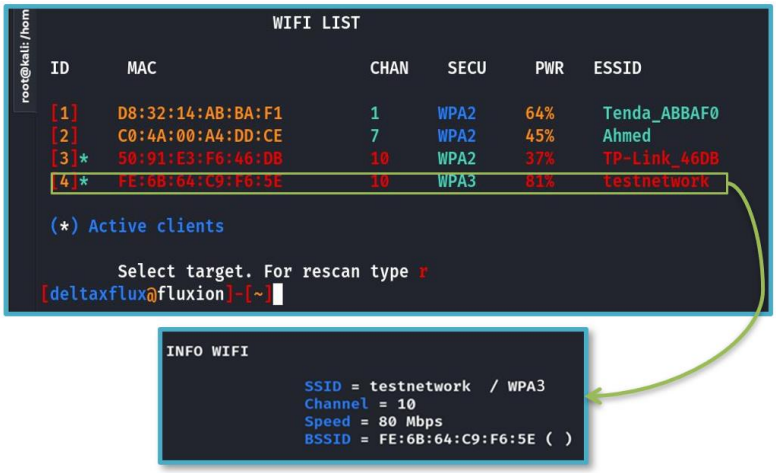

Fig. 26. Define the target network

Fig. 27. The five windows of the fake network

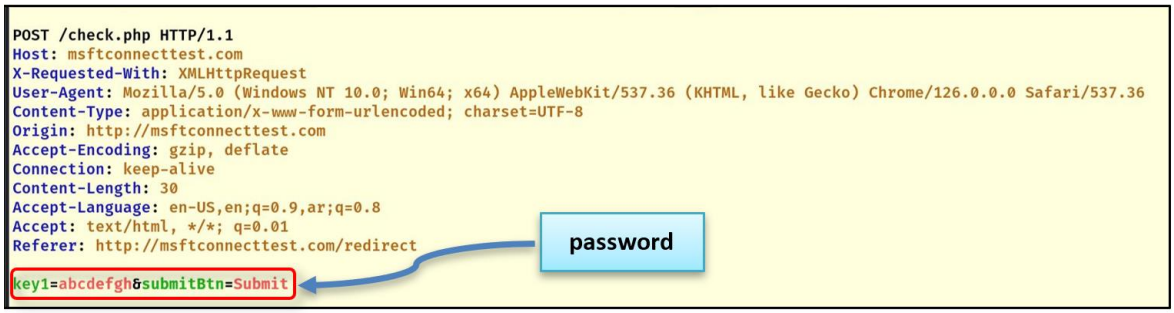

Fig. 28. The sixth window to capture the password from the captive portal.

Table 1. Comparison of penetration test results for WPA2 and WPA3 protocols.

attack	WPA2	WPA2/3 (transition mode)	WPA3
De-authentication attack	Easy to spoof MAC addresses and inject fake deauthentication frames due to the optional use of PMF.	It is possible to spoof MAC addresses and inject fake deauthentication frames before the 4-way handshake (less likely) due to the mandatory use of PMF.	It is possible to spoof MAC addresses and inject fake deauthentication frames before the 4-way handshake (less likely) due to the mandatory use of PMF.
Capture handshake file	successful	successful	successful
dictionary attack	successful	It is possible if one of the user devices does not support WPA3 and connects via WPA2.	Not possible
Evil Twin Attack	successful	The attack was successful but more complex.	The attack was successful but more complex.
social engineering attack	successful	successful	successful

6. Countermeasures

Based on the result of the Wi-Fi penetration test, the study suggests the following practices:

- Continuously updating the access point, adopting the latest encryption standards, and immediately stopping old and weak protocols is the main key to securing wireless networks, and setting a password of no less than 8 characters, preferably a combination of symbols, numbers, and letters, and it should be strong and not hacked, and it should not include general information that people may know about the person, such as the person's name and birth date in the password, because it is easy for social engineers to discover, and also regularly updating passwords is one of the methods of securing local networks.
- It is very necessary to reset the default settings of the access point, including (SSID), channel, and default passwords. The default setting of the network name (SSID) can reveal the device model, manufacturer, and weak and known default password, and provide the attacker with all the information necessary to launch an attack on the wireless network.
- Steer clear of public Wi-Fi networks where users are required to provide personal information like their name, phone number, email address, etc. as these are potential points of attack for hackers.
- There are several approaches we might take to the problem of thwarting evil twin attacks. From the client's perspective, there exist many tactics that they might utilize to lessen their vulnerability. A few examples include forgetting networks once connected, shutting off wireless interfaces while the device is not actively connected to the network, and disabling automated connections. This helps stop the device from connecting to an Evil Twin, which is a fake network that looks and acts like the actual network.
- Activate the mandatory use of PMF protected management frames.
- Despite WPA3's security capabilities and its difficulty in hacking, its adoption remains limited. It is essential to raise awareness of the security risks associated with using protocols such as WPA2 and WEP. Potential vulnerabilities and their impact on data privacy should be highlighted, emphasizing the importance of upgrading to WPA3.
- Operating systems and devices should display clear and direct warnings to users when connecting to networks that use older security standards. These warnings should be accompanied by instructions on how to strengthen the connection's security.
- While hiding the network name does not deter sophisticated attackers, it is an additional precaution that complicates the process of randomly targeting networks. This feature should be used in conjunction with WPA3 and a strong password, and should not be relied upon as a substitute for basic security measures.

7. Conclusions and Discussion

Penetration tests have revealed weaknesses in the WPA2 and WPA3 protocols. For WPA2, a penetration test revealed a significant weakness in the management frames, where the MAC address of the access point can be easily spoofed and users are denied service, forcing them to resubmit a 4-way handshake. This weakness makes networks vulnerable to dictionary attacks using open source tools, especially when weak passwords are used. A WPA3 penetration test showed that a deauthentication attack is still possible before the 4-way handshake occurs, and that WPA3 does not provide complete protection against dictionary attacks in transition mode. Although dictionary attacks failed with a user connected directly via WPA3, a single user connected to WPA2 makes the entire network vulnerable to this type of attack.

Evil twin attacks on both WPA2 and WPA3 have proven highly effective in penetrating networks. Using social engineering and captive portal techniques, attackers can trick victims into obtaining Wi-Fi passwords if a dictionary attack fails. The success of these attacks is not limited to a specific protocol; they can be implemented on both protocols, but are more complex when using WPA3. Finally, some recommendations have been proposed to mitigate the potential for hacking into local networks, most notably the adoption of modern standards, the need to continuously update access points, and abandoning old and weak protocols.

References

[1] A. Efe and M. B. Kaplan, "Wi-fi security analysis for E&M-Government applications," *Int. J. Multidiscip. Stud. Innov. Technol.*, vol. 3, no. 2, pp. 86–98, 2019.

[2] S. Xie, X. Zhu, and J. Shen, "Method and system for automatically adapting to Wi-Fi network with hidden SSID," Oct. 30, 2018, *Google Patents*.

[3] M. Z. Masoud, Y. Jaradat, and M. Alia, "IEEE802. 11 Access Point's Service Set Identifier (SSID) for Localization and Tracking.," *Comput. Mater. Contin.*, vol. 71, no. 3, 2022.

[4] S. Perumal, M. Tabassum, G. Narayana Samy, S. Ponnan, A. K. Ramamoorthy, and K. J. Sasikala, "Cybercrime issues in smart cities networks and prevention using ethical hacking," in *Data-Driven Mining, Learning and Analytics for Secured Smart Cities: Trends and Advances*, Springer, 2021, pp. 333–358.

[5] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," in *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*, IEEE, 2014, pp. 237–242.

[6] C. P. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for Wi-Fi and WPA3," *Electronics*, vol. 7, no. 11, p. 284, 2018.

[7] D. Schepers, A. Ranganathan, and M. Vanhoef, "On the robustness of Wi-Fi deauthentication countermeasures," in *Proceedings of the 15th ACM conference on security and privacy in wireless and mobile networks*, 2022, pp. 245–256.

[8] R. Lakshmi, A. Sharma, S. Bhuvan, B. Chinmay, and G. M. Megha, "Comparative Analysis of Security and Privacy Protocols in Wireless Communication".

[9] J. Cathcart and T. Khan Mohd, "Password Hacking Analysis of Kali Linux Applications," in *International Conference on Intelligent Sustainable Systems*, Springer, 2023, pp. 815–828.

[10] L. Wang, C. T. Chen, and C. M. Tsai, "Research on cracking WIFI wireless network using Kali-Linux penetration testing software," in *Third International Conference on Digital Signal and Computer Communications (DSCC 2023)*, SPIE, 2023, pp. 378–382.

[11] M. A. C. Aung and K. P. Thant, "Detection and mitigation of wireless link layer attacks," in *2017 IEEE 15th international conference on software engineering research, management and applications (SERA)*, IEEE, 2017, pp. 173–178.

[12] A. Sari and M. Karay, "Comparative Analysis of Wireless Security Protocols: WEP vs WPA," *Int. J. Commun. Netw. Syst. Sci.*, vol. 08, no. 12, pp. 483–491, 2015, doi: 10.4236/ijcns.2015.812043.

[13] I. S. Al-Mejibli and N. R. Alharbe, "Analyzing and evaluating the security standards in wireless network: A review study," *Iraqi J. Comput. Informatics*, vol. 46, no. 1, pp. 32–39, 2020.

[14] G. Mironov, "Challenges of Wireless Security in the Healthcare Field: A study on the WPA3 standard," 2020.

[15] A. Halbouni, L.-Y. Ong, and M.-C. Leow, "Wireless Security Protocols WPA3: A Systematic Literature Review," *IEEE Access*, 2023.

[16] M. K. Kissi and M. Asante, "Penetration testing of IEEE 802.11 encryption protocols using Kali Linux hacking tools," *Int. J. Comput. Appl.*, vol. 975, p. 8887, 2020.

[17] A. H. Adnan *et al.*, "A comparative study of WLAN security protocols: WPA, WPA2," in *2015 International Conference on Advances in Electrical Engineering (ICAEE)*, IEEE, 2015, pp. 165–169.

[18] A. Sari and M. Karay, "Comparative analysis of wireless security protocols: WEP vs WPA," *Int. J. Commun. Netw. Syst. Sci.*, vol. 8, no. 12, p. 483, 2015.

[19] E. Lamers, R. Dijksman, A. Van Der Vegt, M. Sarode, and C. De Laat, "Securing home Wi-Fi with WPA3 personal," in *2021 IEEE 18th Annual Consumer Communications and Networking Conference, CCNC 2021*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021. doi: 10.1109/CCNC49032.2021.9369629.

[20] B. Scheuermann, "Model based fuzzing of the WPA3 Dragonfly handshake," 2019, *MS thesis, Humboldt-Universität zu Berlin, Germany*.

[21] I. Despotopoulos, "Wireless local area network security and modern cryptographic protocols: WEP & WPA1/2/3," 2024.

[22] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," in *Proceedings - IEEE Symposium on Security and Privacy*, Institute of Electrical and Electronics Engineers Inc., May 2020, pp. 517–533. doi: 10.1109/SP40000.2020.00031.
[23] W.-F. Alliance, "Generational Wi-Fi User Guide," *URL https//www. wi-fi. org/download. php*, 2020.
[24] D. Schepers, A. Ranganathan, and M. Vanhoef, "Let numbers tell the tale: measuring security trends in wi-fi networks and best practices," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021, pp. 100–105.
[25] M. Vink, E. Poll, and A. Verbiest, "A comprehensive taxonomy of wi-fi attacks," 2020, *Radboud University Nijmegen Nijmegen, The Netherlands*.
[26] M. Vanhoef, N. Bhandaru, T. Derham, I. Ouzieli, and F. Piessens, "Operating channel validation: Preventing multi-channel man-in-the-middle attacks against protected wi-fi networks," in *WiSec 2018 - Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Association for Computing Machinery, Inc, Jun. 2018, pp. 34–39. doi: 10.1145/3212480.3212493.
[27] K. Lounis, S. H. H. Ding, and M. Zulkernine, "Cut It: Deauthentication attacks on protected management frames in WPA2 and WPA3," in *International symposium on foundations and practice of security*, Springer, 2021, pp. 235–252.
[28] J. Bellardo and S. Savage, "802.11 {Denial-of-Service} attacks: Real vulnerabilities and practical solutions," in *12th USENIX Security Symposium (USENIX Security 03)*, 2003.
[29] R. A. C. Ferreira, "A probability problem arising from the security of the temporal key hash of wpa," *Wirel. Pers. Commun.*, vol. 70, pp. 1235–1241, 2013.
[30] M. Dandotiya, "A Secure Detection Framework for ARP, DHCP, and DoS Attacks on Kali Linux," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 7, pp. 3044–3053, Jul. 2022, doi: 10.22214/ijraset.2022.42176.
[31] M. Patel, P. P. Amritha, and R. Sam Jasper, "Active dictionary attack on WPA3-SAE," in *Advances in Computing and Network Communications: Proceedings of CoCoNet 2020, Volume 1*, Springer, 2021, pp. 633–641.
[32] V. Ramachandran and C. Buchanan, *Kali Linux Wireless Penetration Testing Beginner ' s Guide*. 2015. [Online]. Available: https://www.programmer-books.com/kali-linux-wireless-penetration-testing-beginners-guide/
[33] V. Manjunath Honnamma, "SPECIFICATION-BASED INTRUSION DETECTION SYSTEM FOR 802.11 NETWORKS USING INCREMENTAL DECISION TREE CLASSIFIER," 2018.
[34] O. Nakhila, A. Attiah, Y. Jin, and C. Zou, "Parallel active dictionary attack on WPA2-PSK Wi-Fi networks," in *MILCOM 2015-2015 IEEE Military Communications Conference*, IEEE, 2015, pp. 665–670.
[35] N. MM, V. Kothamasu, and N. Kenchaiah, "Method to support iPSK for WPA3 clients as well as reduce Online Dictionary Attacks," 2022.
[36] A. Wakhloo, "Client-side Evil-Twin access point detection using beacon-frame delay and wireless network parameter deviation," 2023.
[37] P. Cisar and R. Pinter, "Some ethical hacking possibilities in Kali Linux environment," *J. Appl. Tech. Educ. Sci. jATES*, vol. 9, no. 4, pp. 129–149, 2019, [Online]. Available: http://doi.org/10.24368/jates.v9i4.139http://jates.org

Authors' Profiles

Asmaa Akram Ghanim completed the B.S. in electrical engineering/ electronic and communication from the University of Mosul, Iraq, in 2020 and received the M.Sc. degree in electronic and communication in 2025. She is interested in the field of computer networks and communication and cybersecurity.

Mohammed Younis Thanoun completed the B.S. in electrical engineering/ electronic and communication from the University of Mosul, Iraq, in 1991 and received the M.Sc. degree in electronic and communication in 2000 and Ph.D. in 2011 from Mosul University. He is interested in the field of computer networks and communication and he has published research papers in Deep Learning, SDN, machine learning algorithms and cybersecurity engineering He has been working as an assistant professor at the University of Mosul since 2021. He is a member of the computer networks lab in the Electrical Dept / Engineering College.

How to cite this paper: Asmaa A. Ghanim, Mohammed Y. Thanoun, "Evaluating the Effectiveness of WPA3 Protocol against Advanced Hacking Attacks", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.15, No.4, pp. 1-18, 2025. DOI:10.5815/ijwmt.2025.04.01