Chapter 16: Hacking Wireless Networks

Introduction

Wireless networks are more cost-effective and simpler to manage than wired ones. However, they can be highly vulnerable to attacks without adequate security protocols or network configuration. Since implementing advanced security measures for wireless networks can be costly, it is essential to identify critical assets, potential risks, and vulnerabilities within the network. Once these are assessed, the current security framework should be evaluated to ensure it can safeguard the network against all potential threats. If it falls short, enhancements to the security measures should be made.

This chapter covers the various types of wireless networks, their associated security protocols, potential threats, and strategies to mitigate them, ensuring the network remains secure. It also examines wireless encryption algorithms, highlighting their strengths and limitations. Additionally, the chapter explores methods used in wireless network attacks and provides counterstrategies to safeguard information systems.

By completing this chapter, you will gain the ability to:

- Understand wireless networking concepts
- Explain and compare wireless encryption algorithms
- Identify and analyze wireless threats
- Understand wireless hacking methodologies
- Use tools for wireless network penetration testing
- Implement countermeasures against wireless hacking
- Utilize various tools to enhance wireless security

Wireless Concepts

The evolution of network technology is entering a transformative phase driven by advancements in wireless communication. Wireless networking is reshaping how people interact, both professionally and recreationally. Eliminating the need for physical cables enables users to access and share data with greater mobility and flexibility. A wireless network is an open communication system that relies on radio-frequency signals to transmit data and connect devices. Electromagnetic waves allow seamless interaction between two points without requiring physical wiring. This section delves into the fundamental concepts of wireless networking.

Wireless Terminology

In a wireless network, data is transmitted using Electromagnetic (EM) waves, which carry signals along the communication path. Key terms associated with wireless networks include:

- **Global System for Mobile Communications (GSM):** This is a universal standard for transmitting mobile data, widely used in wireless networks worldwide.

- **Bandwidth:** Refers to the capacity for transmitting information over a connection. It is commonly expressed as the rate of data transfer, measured in Bits Per Second (bps).
- **Access Point (AP):** A device that connects wireless devices to a wired or wireless network. Using standards like Bluetooth and Wi-Fi, an AP bridges a wired LAN and a wireless network.
- **Basic Service Set Identifier (BSSID):** The Media Access Control (MAC) address of an Access Point (AP) or base station that establishes a Basic Service Set (BSS). While users are typically unaware of the specific BSS their device uses, the BSS may change as they move between access points without disrupting connectivity.
- **Industrial, Scientific, and Medical (ISM) Band:** International frequencies for industrial, scientific, and medical applications.
- **Hotspot:** A public area offering wireless network access, typically via Wi-Fi. Users can connect to the internet by enabling Wi-Fi on their devices in these zones.
- **Association:** The process by which a wireless device connects to an access point.
- **Service Set Identifier (SSID):** A unique 32-character alphanumeric identifier assigned to a Wireless Local Area Network (WLAN). Devices must use the same SSID to connect to the intended network.
- **Orthogonal Frequency-Division Multiplexing (OFDM):** It is a digital modulation technique that divides a signal into multiple orthogonal carrier frequencies. This method enhances data transmission by allowing higher bit rates and efficient bandwidth sharing.
- **Multiple Input, Multiple Output-Orthogonal Frequency-Division Multiplexing (MIMO-OFDM):** A technique that improves spectral efficiency in 4G and 5G networks. It minimizes interference and enhances the robustness of communication channels.
- **Direct-Sequence Spread Spectrum (DSSS):** A method that combines the original data signal with a pseudo-random noise-spreading code to protect signals from interference or jamming.
- **Frequency-Hopping Spread Spectrum (FHSS):** Also known as Frequency-Hopping Code-Division Multiple Access (FH-CDMA), this technique transmits signals by rapidly switching the carrier among various frequency channels. It reduces the risk of unauthorized interception or jamming using a pseudorandom frequency-hopping sequence shared between the transmitter and receiver.

Wireless Networks

Wireless networks rely on radio waves for data transmission and typically operate at the physical layer of the network infrastructure. As wireless communication revolutionizes global connectivity, data networking and telecommunications fields undergo significant transformations.

Wi-Fi, a type of Wireless Local Area Network (WLAN) based on the IEEE 802.11 standard, enables devices to connect to a network within the coverage area of an Access Point (AP). Widely adopted for wireless communication, Wi-Fi operates over radio frequencies and employs technologies such as Direct-Sequence Spread Spectrum (DSSS), Frequency-Hopping Spread Spectrum (FHSS), Infrared (IR), and Orthogonal Frequency-Division Multiplexing (OFDM) to establish reliable connections between transmitters and receivers. Common devices like personal computers, gaming

consoles, and smartphones use Wi-Fi to connect to the internet or other network resources via an AP.

Advantages of Wireless Networks:

- Quick and simple installation without running cables through walls or ceilings
- Facilitates connectivity in areas where laying cables is challenging
- Provides network access from anywhere within the AP's range
- Public spaces like airports, libraries, schools, and coffee shops offer constant internet access through WLANs

Disadvantages of Wireless Networks:

- Security may not always meet expectations
- Bandwidth can decrease as more devices connect to the network
- Upgrading Wi-Fi infrastructure may necessitate new wireless cards or access points
- Certain electronic devices may interfere with Wi-Fi signals

Types of Wireless Networks

Wireless networks come in various forms, each serving specific connectivity needs. Below is an overview of these types:

1. Extension to a Wired Network

A wired network can be extended by incorporating Access Points (APs) to facilitate connections with wireless devices. These APs can establish a wireless network through two main types:

- **Software APs (SAPs):** These run on computers with wireless Network Interface Cards (NICs) and can link directly to wired networks.
- **Hardware APs (HAPs):** Standalone devices offering advanced wireless features. HAPs serve as switches, connecting wireless devices with NICs to a wired LAN. This setup provides wireless access to network resources like file servers and internet connections.

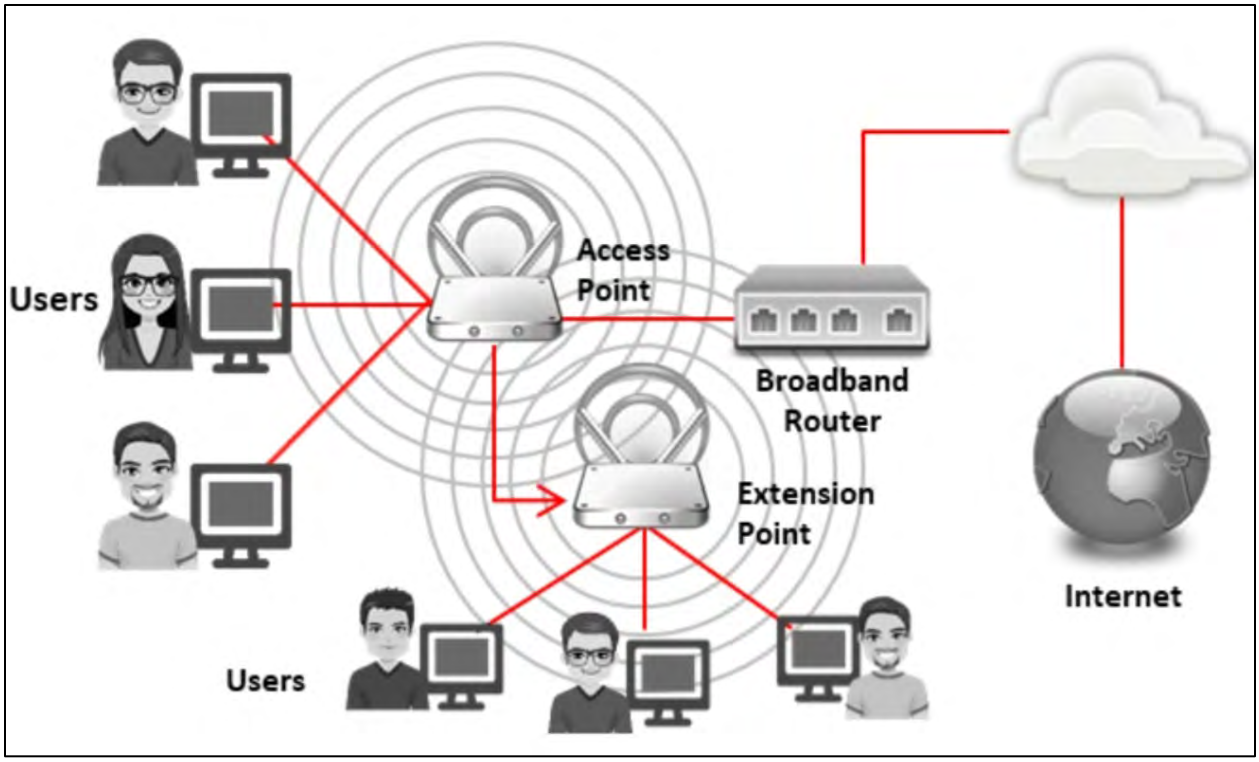


Figure 16-01: Extension to a Wired Network

2. Networks with Multiple Access Points

When a single AP cannot adequately cover an area, multiple APs or extension points can be deployed to ensure broader coverage.

- Overlapping wireless coverage areas enable seamless mobility using a feature known as roaming
- Some manufacturers offer extension points that act as wireless relays, extending the coverage of a central AP
- By connecting multiple extension points in sequence, wireless access can be provided to distant locations

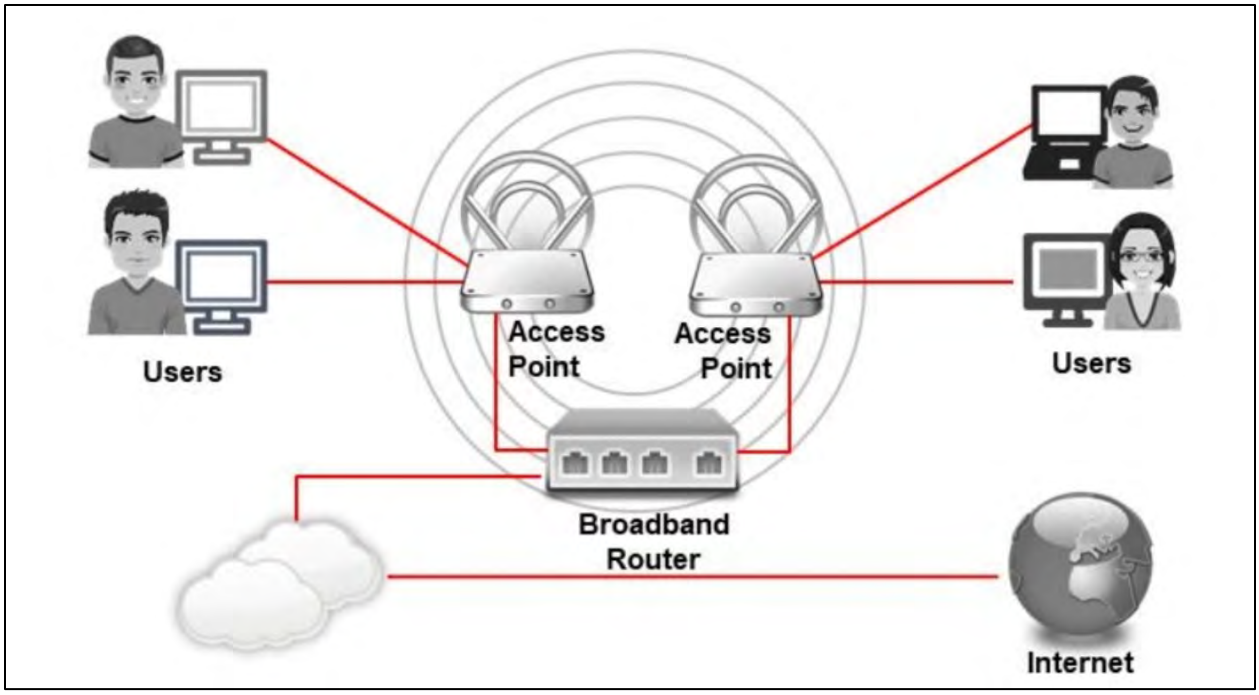


Figure 16-02: Networks with Multiple Access Points

3. LAN-to-LAN Wireless Networks

Access points can wirelessly connect local computers and enable communication between local networks. Hardware APs can interconnect with other hardware APs, though setting up wireless connections between LANs is complex.

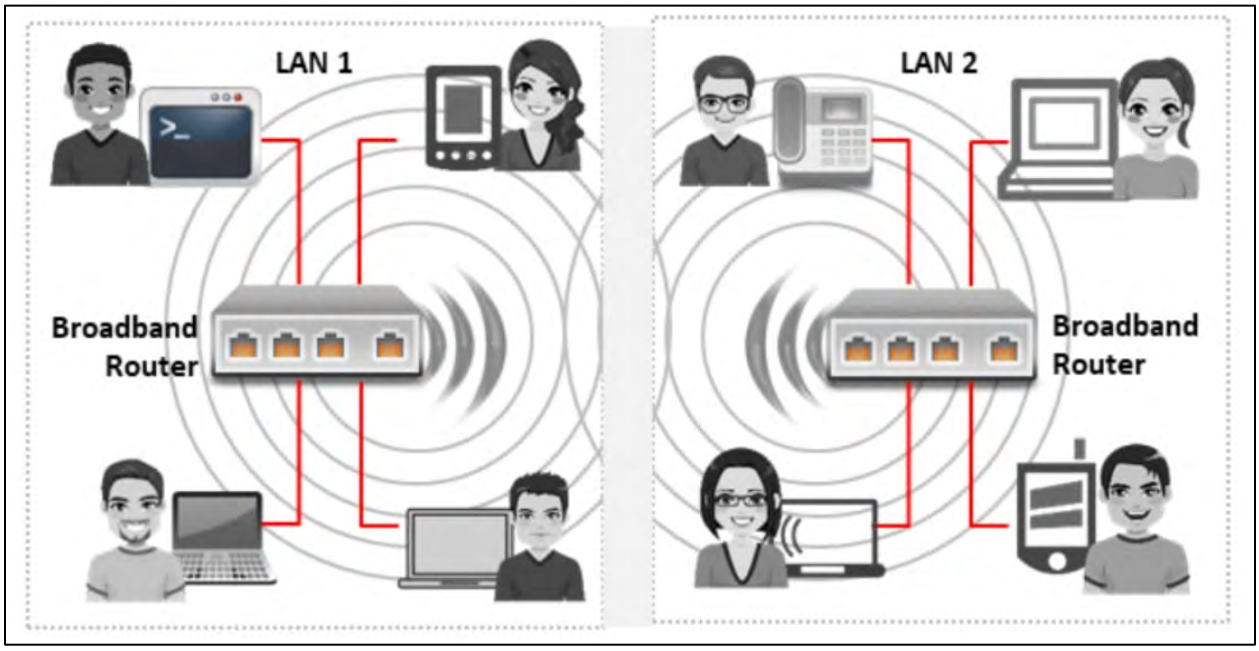


Figure 16-03: LAN-to-LAN Wireless Networks

4. 3G/4G/5G Hotspots

These wireless networks use cellular technology to provide Wi-Fi access to compatible devices, such as laptops, tablets, MP3 players, cameras, and PDAs. These hotspots enable on-the-go connectivity for Wi-Fi-enabled devices.

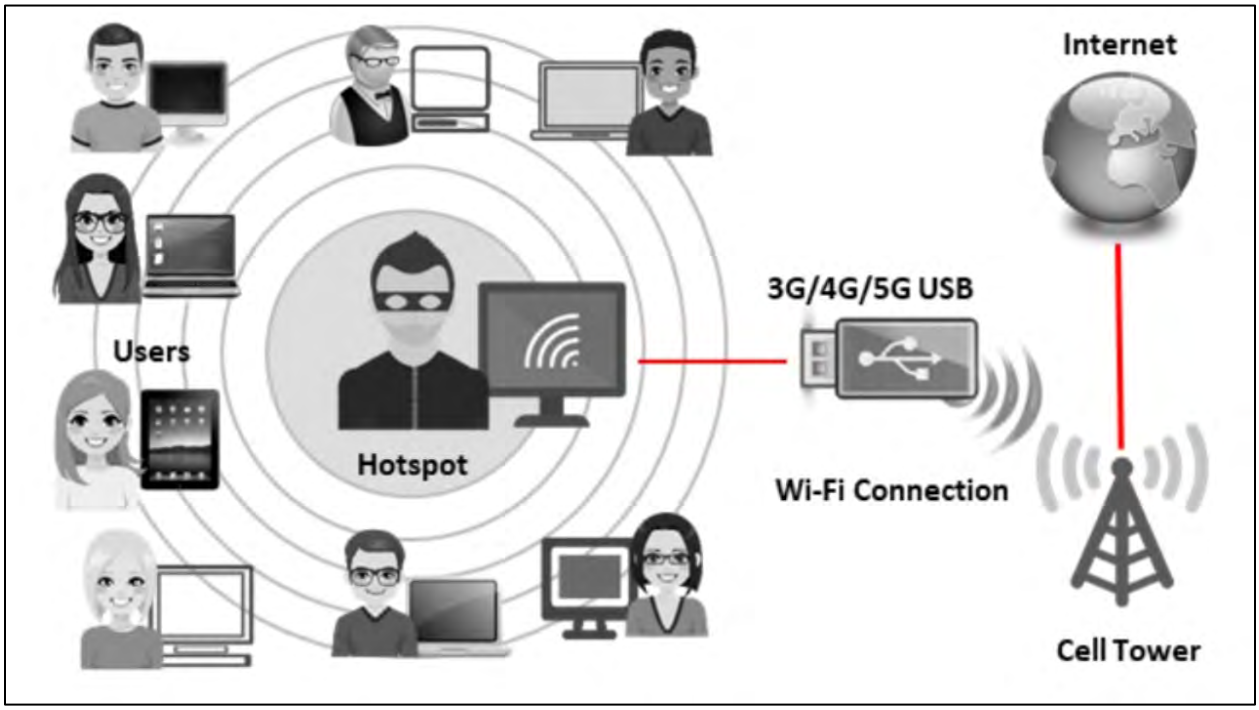


Figure 16-04: 3G/4G/5G Hotspots

Wireless Standards

The IEEE 802.11 standard has progressed significantly, evolving from a simple wireless extension of wired LANs to a robust protocol capable of supporting enterprise-grade authentication, advanced encryption methods, and Quality of Service (QoS). Initially introduced in 1997, the WLAN standard operated at 1 and 2 Mbps speeds, utilizing both infrared and the unlicensed 2.4-GHz Industrial, Scientific, and Medical (ISM) frequency band.

In its early implementation, 802.11 networks typically consisted of a few wireless-enabled PCs connected to an Ethernet (IEEE 802.3) LAN via a single Access Point (AP). Today, these networks function at much faster speeds and span multiple frequency bands. However, advancements have brought new challenges, including enhanced security requirements, seamless roaming across multiple APs, and maintaining QoS.

Updates to the 802.11 standard are developed by dedicated task groups and are identified by alphabetic suffixes, as detailed in Table 16-01.

Amendments	Frequency (GHz)	Modulation	Speed (Mbps)	Range (Meters)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20-100

802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35-100
	3.7			5000
802.11ax	2.4 to 5	1024-QAM	2400	240
802.11b	2.4	DSSS	1, 2, 5.5, 11	35- 140
802.11be	2.4, 5, 6	QAM	3000	120
802.11d	This improvement builds upon 802.11a and 802.11b, facilitating worldwide adaptability by accommodating differences in frequency ranges, power outputs, and bandwidth requirements.			
802.11e	It offers guidelines for prioritizing the transmission of data, voice, and video to ensure Quality of Service (QoS).			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38- 140
802.11i	A Wireless Local Area Networks (WLANs) standard that enhances encryption for networks operating on 802.11a, 802.11b, and 802.11g introduces WPA2-Enterprise and WPA2-Personal for Wi-Fi security.			
802.11n	2.4, 5	MIMO-OFDM	54- 600	70- 250
802.15.1 (Bluetooth)	2.4	GFSK, π/4-DPSK, 8DPSK	25- 50	10- 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1- 100
802.16 (WiMAX)	2- 11	SOFDMA	34- 1000	1609.34-9656.06 (1-6 miles)

Table 16-01: Wireless Standards

- **802.11**: The 802.11 (Wi-Fi) standard is designed for WLANs and employs Frequency-Hopping Spread Spectrum (FHSS) or Direct-Sequence Spread Spectrum (DSSS) for data transmission. It enables electronic devices to connect wirelessly within a network.
- **802.11a**: This was the first amendment to the original 802.11 standard. Operating in the 5 GHz frequency band, it supports up to 54 Mbps bandwidths through Orthogonal Frequency-Division Multiplexing (OFDM). While offering high speeds, it is more susceptible to interference from physical barriers like walls.
- **802.11ax (Wi-Fi 6)**: Known as Wi-Fi 6, this latest Wi-Fi standard builds upon 802.11ac (Wi-Fi 5). It speeds up to 9.6 Gbps, uses Orthogonal Frequency-Division Multiple Access (OFDMA) to manage simultaneous connections efficiently, and incorporates features like BSS Coloring and Target Wake Time (TWT) to optimize performance in crowded environments. It is well-suited for high-density areas such as stadiums, airports, and smart homes with numerous connected devices.
- **802.11b**: Introduced in 1999, this extension to the original 802.11 standard operates in the 2.4 GHz ISM band and supports data rates up to 11 Mbps using Direct-Sequence Spread Spectrum (DSSS) modulation.
- **802.11be (Wi-Fi 7)**: Wi-Fi 7, or 802.11be, is an upcoming standard designed to greatly enhance Wi-Fi 6/6E. It supports data rates up to 30 Gbps, utilizes Multilink Operation (MLO) to combine multiple channels across various bands, and reduces latency for real-time applications. Wi-Fi 7

is intended to support future high-speed internet, virtual reality, augmented reality, and advanced IoT technologies.

- **802.11d**: The 802.11d standard is an improvement over 802.11a and 802.11b, offering support for regulatory domains. It allows the configuration of these settings within the Media Access Control (MAC) layer.
- **IEEE 802.11e**: This standard is designed for real-time voice, VoIP, and video services. To prioritize these time-sensitive applications, 802.11e defines Quality of Service (QoS) mechanisms within layer 2 of the reference model, specifically the MAC layer.
- **802.11g**: An extension of the 802.11 standard, 802.11g offers a maximum bandwidth of 54 Mbps using OFDM technology. It operates on the same 2.4 GHz frequency as 802.11b. It is compatible with 802.11b devices, allowing seamless operation with 802.11b access points.
- **802.11i**: The 802.11i standard enhances WLAN security by incorporating new encryption methods, such as the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).
- **802.11n**: The 802.11n standard improves upon 802.11g by integrating Multiple-Input Multiple-Output (MIMO) antennas, supporting 2.4 GHz and 5 GHz bands. It is widely adopted as an IEEE industry standard for Wi-Fi, utilizing OFDM for Digital Audio Broadcasting (DAB) and WLAN.
- **802.11ah**: Known as Wi-Fi HaLow, this standard operates on 900 MHz bands and offers extended-range Wi-Fi networks. It supports Internet of Things (IoT) communication with better data rates and broader coverage than previous standards.
- **802.11ac**: Operating on the 5 GHz frequency, 802.11ac offers a high-throughput network, surpassing 802.11n in speed and reliability. It supports Gigabit networking for fast and efficient data transfer.
- **802.11ad**: The 802.11ad standard introduces a new physical layer for 802.11 networks, functioning on the 60 GHz spectrum. This standard delivers faster data propagation than those using the 2.4 GHz and 5 GHz bands, such as 802.11n.
- **802.12**: This standard uses a demand priority protocol for media utilization and has an Ethernet speed of 100 Mbps. It is compatible with 802.3 and 802.5 standards, enabling users to upgrade directly from those existing standards.
- **802.15**: This standard outlines the specifications for a Wireless Personal Area Network (WPAN) and details how wireless connectivity can be established with fixed and portable devices.
- **802.15.1 (Bluetooth)**: Bluetooth is primarily used for short-range data exchange between fixed or mobile devices operating on the 2.4 GHz frequency band.
- **802.15.4 (ZigBee)**: The 802.15.4 standard is designed for low data rates and minimal complexity. It is used with ZigBee to transmit data over long distances via a mesh network. With a data rate of 250 Kbps, it is ideal for applications prioritizing energy efficiency and extending battery life.
- **802.15.5**: This standard operates on a full-mesh or half-mesh topology and includes network initialization, addressing, and unicasting features.
- **802.16 (WiMax)**: The IEEE 802.16 standard, also known as WiMax, provides a range of Physical Layer (PHY) and Media Access Control (MAC) options. It uses a point-to-multipoint architecture for fixed broadband wireless Metropolitan Area Networks (MANs).

Service Set Identifier (SSID)

A Service Set Identifier (SSID) is a unique, case-sensitive, human-readable label used to identify a WLAN, consisting of up to 32 alphanumeric characters. It is a marker for locating and identifying 802.11 (Wi-Fi) networks. By default, it is included in the frame header of packets transmitted across the WLAN. It serves as a shared identifier between Access Points (APs) and clients. This enables users to find an AP to which they can attempt to authenticate and associate. Security risks arise when the default SSID values are not changed, as these networks can be easily compromised.

APs respond to probe requests with probe responses containing the SSID unless hidden. Since the SSID uniquely identifies a WLAN, all devices and APs in that network must share the same SSID. Any device wishing to join the WLAN must provide the correct SSID. Network administrators must update the SSID configuration on all client devices if the SSID is altered. A non-secure access mode allows clients to connect using the SSID, a blank SSID, or one configured as "any." However, SSID alone does not secure a WLAN, as it is easily retrievable in plaintext from packets. The default SSID is typically the manufacturer's name in many commercial devices. SSID confidentiality can only be maintained in closed networks with no activity, which can be inconvenient for legitimate users.

Wi-Fi Authentication Process

Pre-Shared Key (PSK) Mode

The Pre-Shared Key (PSK) authentication method, also called WPA-PSK or WPA2-PSK, is commonly used to secure wireless networks by employing a single shared password for device authentication. This method is especially favored in home and small office settings due to its straightforward setup process. In this mode, a shared password, or pre-shared key, is manually configured on the wireless router and the device attempting to connect. Its simplicity makes it a convenient option for smaller environments where ease of use is essential. However, the security of WPA/WPA2-Personal relies heavily on the strength and confidentiality of the pre-shared key.

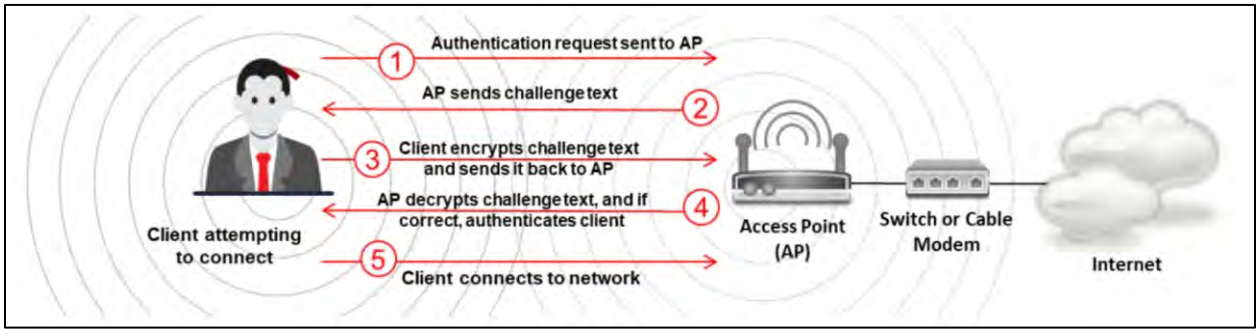


Figure 16-05: PSK Wi-Fi Authentication Process

Centralized Authentication Mode

In this mode, a centralized authentication server, often called Remote Authentication Dial-In User Service (RADIUS), is responsible for sending authentication keys to both the Access Point (AP) and the client that needs to authenticate with the AP. WPA/WPA2-Enterprise, or 802.1X mode, is a security protocol for large-scale networks and enterprises. Unlike WPA/WPA2-Personal, which

relies on a Pre-Shared Key (PSK) for authentication, WPA/WPA2-Enterprise uses a centralized authentication server, typically a RADIUS server, to manage individual user credentials. Users receive unique login details, such as a username and password or a digital certificate, to authenticate and authorize their network access. This method enhances security by verifying each user's credentials separately, making unauthorized access more difficult. WPA/WPA2-Enterprise is ideal for environments with high-security needs and a large user base, such as corporate offices, educational institutions, and government organizations.

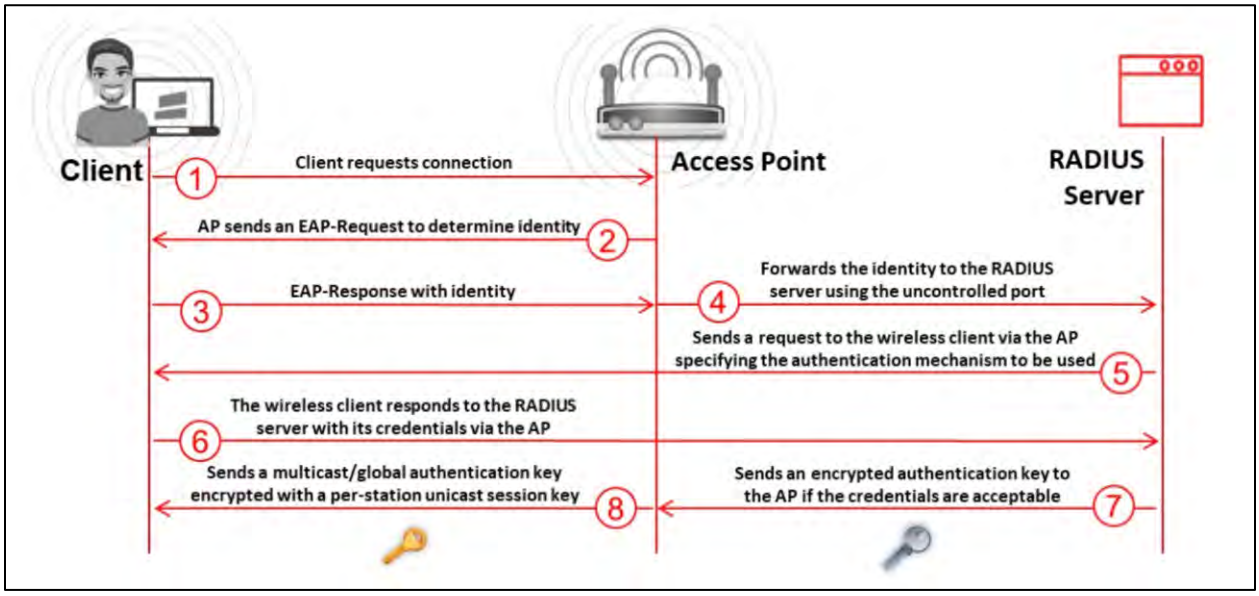


Figure 16-06: Centralized Authentication Process

Types of Wireless Antennas

Antennas are crucial components in Wi-Fi networks. They transmit and receive radio signals and convert electrical signals into radio waves and vice versa. The primary types of wireless antennas include:

- **Directional Antenna**: A directional antenna sends and receives radio signals from a specific direction. Its design optimizes transmission and reception in particular directions, enhancing performance and reducing interference.

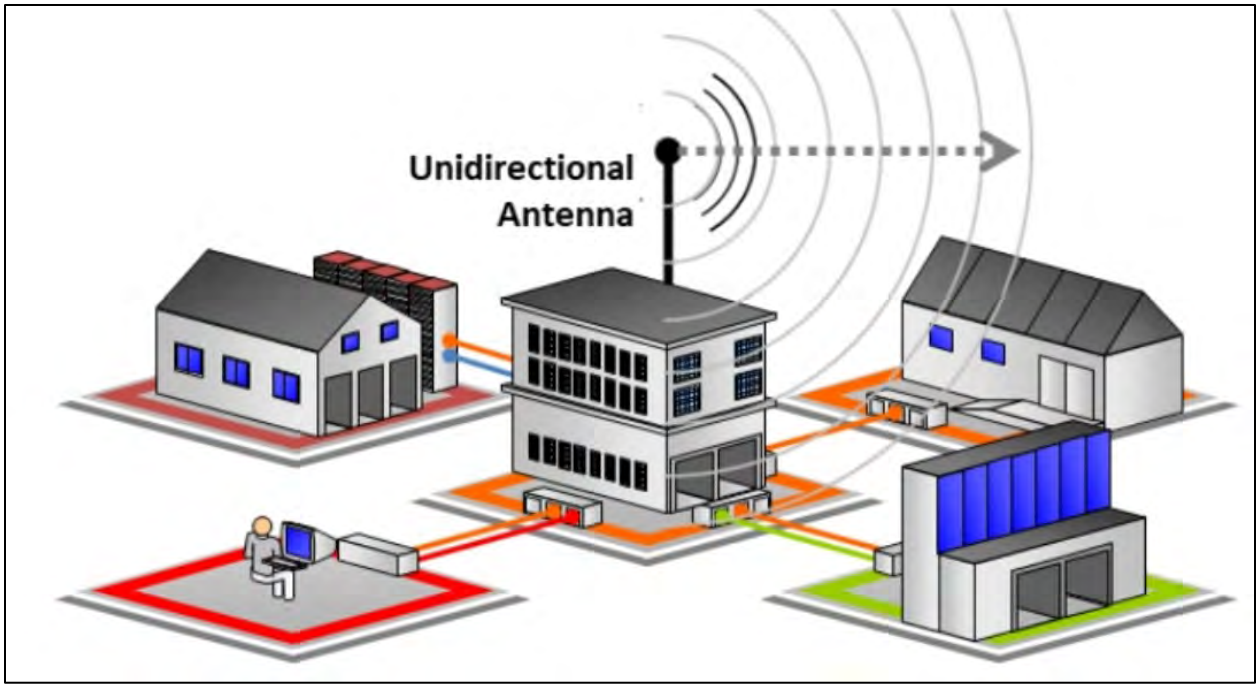


Figure 16-07: Directional Antenna

- **Omnidirectional Antenna**: Omnidirectional antennas emit electromagnetic energy in every direction, creating a 360° horizontal radiation pattern. While they provide strong, uniform waves in two dimensions, their strength is typically weaker in the third dimension. These antennas are ideal for environments where wireless devices use time-division multiple access technology. A common example is the antenna used by radio stations, which is effective for transmitting signals to moving receivers, ensuring the signal can be received from any location.

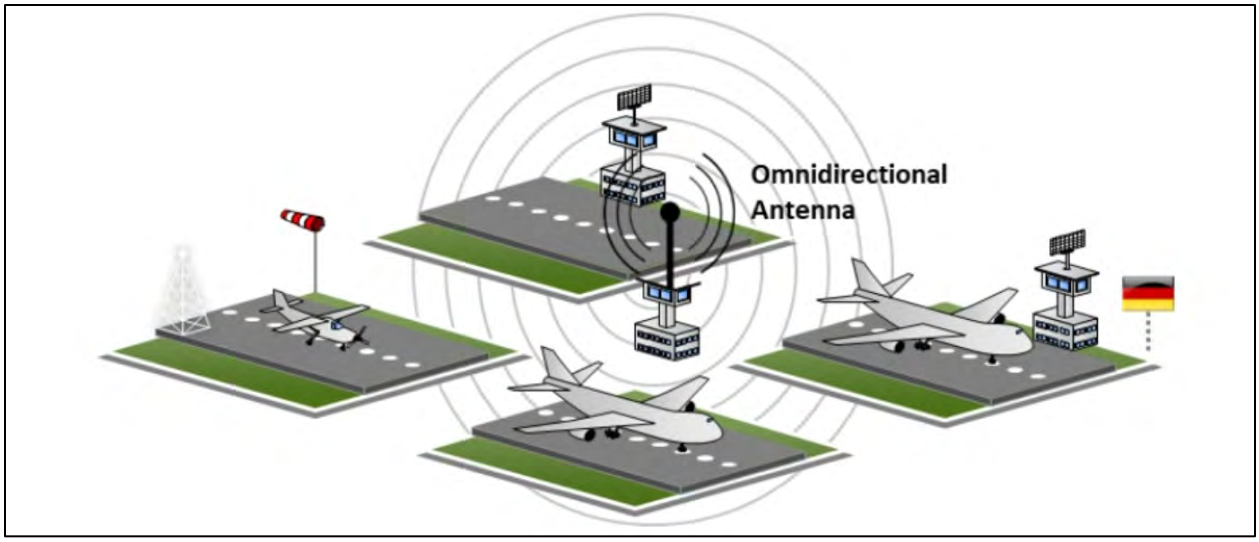
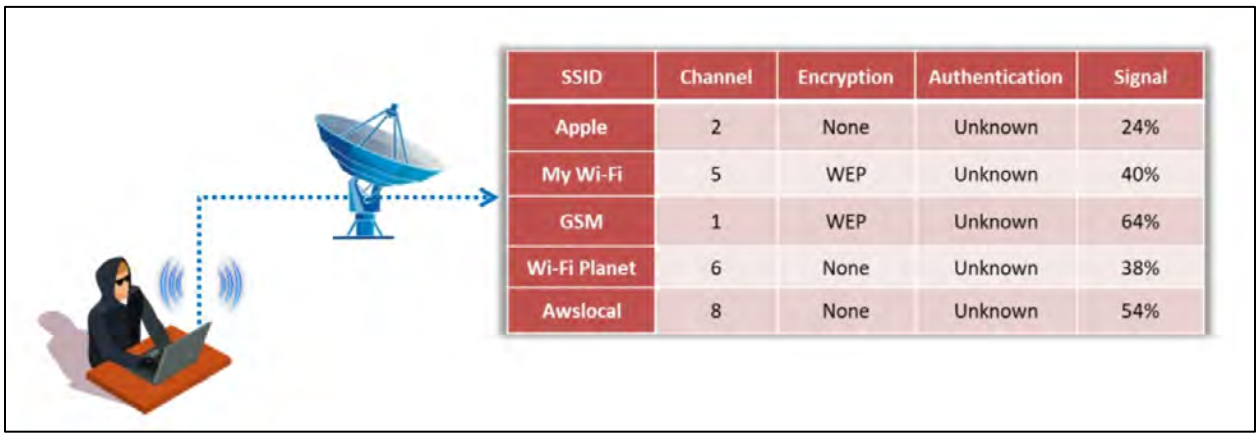


Figure 16-08: Omnidirectional Antenna

- **Parabolic Grid Antenna**: A parabolic grid antenna operates on the same principle as a satellite dish but lacks a solid dish structure. Instead, it features a semi-dish grid made of aluminum wires. This type of antenna can achieve long-range Wi-Fi transmissions by focusing radio

beams. Parabolic grid antennas are ideal for transmitting weak signals over distances of up to 10 miles. However, attackers can also exploit them, offering improved signal quality, increased data interception, more available bandwidth, and higher power output, facilitating layer-1 Denial-of-Service (DoS) and Man-In-The-Middle (MITM) attacks. Its design is lightweight and compact, capable of receiving both horizontally and vertically polarized Wi-Fi signals.



SSID	Channel	Encryption	Authentication	Signal
Apple	2	None	Unknown	24%
My Wi-Fi	5	WEP	Unknown	40%
GSM	1	WEP	Unknown	64%
Wi-Fi Planet	6	None	Unknown	38%
Awslocal	8	None	Unknown	54%

Figure 16-09: Parabolic Grid Antenna

- **Yagi Antenna**: The Yagi antenna, also known as the Yagi-Uda antenna, is a unidirectional antenna typically used for communication in the frequency range of 10 MHz to VHF and UHF. This antenna offers high gain and low Signal-to-Noise Ratio (SNR) for radio signals. It features a unidirectional radiation and response pattern, focusing the radiation in a specific direction. The antenna comprises a reflector, dipole, and several directors, creating an end-fire radiation pattern.
- **Dipole Antenna**: A dipole antenna consists of a straight conductor that is half the wavelength in length, with the feed line connected at the center. Also known as a doublet, this antenna is bilaterally symmetrical and naturally balanced. It operates using a balanced parallel-wire RF transmission line.
- **Reflector Antennas**: Reflector antennas are designed to focus Electromagnetic (EM) energy at a specific focal point for transmission or reception. Typically, the reflectors are parabolic in shape. When the surface is within specific tolerance limits, it can serve as a primary mirror for a broad range of frequencies, minimizing interference with other satellite communications. Larger reflector antennas, in terms of wavelength multiples, provide higher gain. However, reflector antennas tend to have a high manufacturing cost.

Wireless Encryption

Wireless encryption is a method to secure a wireless network from malicious actors who try to intercept sensitive data by exploiting RF traffic. This section explores different wireless encryption protocols, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WPA3, and the challenges associated with each of these standards.

Wireless Encryption

The rise in the use of wireless networks has led to an increase in attacks targeting these networks. One of the most effective methods to safeguard wireless networks from such attacks is encrypting the data before transmission. There are various wireless encryption algorithms, each with its own set of strengths and weaknesses. Here are some key wireless encryption protocols:

- **802.11i**: An IEEE amendment that outlines security mechanisms for 802.11 wireless networks.
- **WEP**: An older encryption algorithm for IEEE 802.11 wireless networks vulnerable to cracking.
- **EAP**: The Extensible Authentication Protocol supports multiple authentication methods, including token cards, Kerberos, and certificates.
- **LEAP**: A proprietary version of EAP created by Cisco.
- **WPA**: A more advanced encryption protocol that uses TKIP and Message Integrity Check (MIC) for strong encryption and authentication. It features a 48-bit Initialization Vector (IV), a 32-bit CRC, and TKIP encryption.
- **TKIP**: A security protocol used in WPA to replace WEP.
- **WPA2**: An improved version of WPA that uses AES and CCMP for encryption, offering stronger data protection.
- **AES**: A symmetric-key encryption algorithm used in WPA2 as a substitute for TKIP.
- **CCMP**: A protocol used in WPA2 for strong encryption and authentication.
- **WPA2 Enterprise**: Integrates EAP standards with WPA2 encryption for enterprise environments.
- **RADIUS**: A centralized system for managing authentication and authorization.
- **PEAP**: A protocol that wraps EAP within an encrypted TLS tunnel for secure authentication.
- **WPA3**: The latest Wi-Fi security protocol offers new personal and enterprise network features. It uses GCMP-256 for encryption and HMAC-SHA-384 for authentication with a 384-bit hash.

Wireless Encryption: Wired Equivalent Privacy (WEP)

WEP was an early security measure designed to safeguard wireless networks from unauthorized access. However, as technology advanced, it became clear that WEP-encrypted information was susceptible to attacks. Here, we explore WEP in detail.

What is WEP Encryption?

WEP is part of the IEEE 802.11 WLAN standards. It is primarily aimed at ensuring the confidentiality of data on wireless networks, providing security similar to that of wired LANs, which rely on physical barriers to prevent unauthorized access. Unlike wired networks, WLANs allow users or attackers to connect without physical access to the network. WEP uses encryption at the data link layer to address this to reduce unauthorized access. The encryption is implemented using the symmetric Rivest Cipher 4 (RC4) algorithm, a cryptographic technique designed to protect against threats.

Role of WEP in Wireless Communication

- WEP helps prevent eavesdropping on wireless transmissions
- It seeks to block unauthorized access to the wireless network

- It relies on a shared secret key between a mobile station and an Access Point (AP) to encrypt packets before they are sent
- An integrity check ensures that the packets remain unaltered during transmission WEP specifically encrypts the data exchanged between network clients

Main Advantages of WEP

- **Confidentiality**: Prevents eavesdropping at the link layer
- **Access Control**: Controls who can access the data
- **Data Integrity**: Safeguards against data modification by unauthorized third parties
- **Efficiency:** WEP provides relatively fast encryption and decryption processes, making it suitable for wireless networks with low overhead

Key Points

WEP was created without academic or public scrutiny, specifically lacking review by cryptologists during its development. As a result, it has major vulnerabilities and design flaws. WEP is a stream cipher using RC4 to generate a stream of XORed bytes with plaintext. The key lengths for WEP are as follows:

- 64-bit WEP uses a 40-bit key
- 128-bit WEP uses a 104-bit key
- 256-bit WEP uses a 232-bit key

How WEP Works

- A CRC-32 checksum calculates a 32-bit Integrity Check Value (ICV) for the data appended to the data frame
- A 24-bit random number, called the Initialization Vector (IV), is combined with the WEP key. Together, they form the WEP seed
- The WEP seed is used as input for the RC4 algorithm to create a keystream, which is XORed with both the data and the ICV to encrypt
- The IV field (IV + PAD + KID) is appended to the ciphertext to form a MAC frame

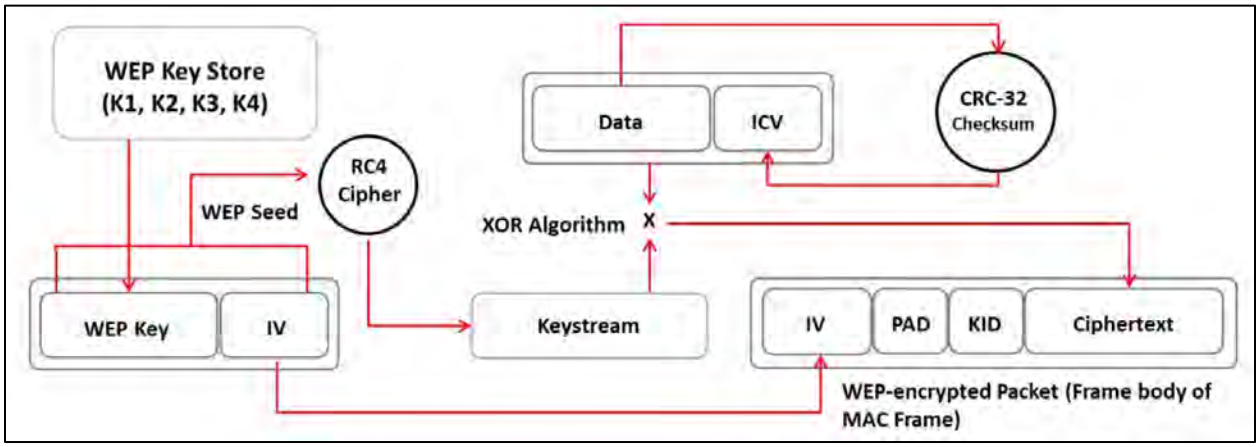


Figure 16-10: Operational Flow of WEP

Flaws of WEP

Several fundamental vulnerabilities weaken WEP's ability to defend against serious attacks:

- **Lack of a defined method for key distribution:**
  - Pre-Shared Keys (PSKs) are set during installation and are seldom updated
  - It is easy to deduce the number of plaintext messages encrypted using the same key
- **RC4's suitability issue:**
  - RC4 was intended for use in more randomized environments than WEP provides
  - Since the PSK remains unchanged for long periods, the same key is reused frequently
  - Attackers can observe network traffic and discover methods to exploit plaintext messages.
  - With ciphertext and plaintext, an attacker can compute the encryption key
- **Passive traffic analysis:**
  - Attackers can capture network traffic and use tools like Fern Wifi Cracker and WEP-key-break to crack the WEP key
- **Vulnerabilities in key scheduling algorithms:**
  - The key scheduling mechanism itself is susceptible to attacks

Wireless Encryption: Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is a security standard outlined by the 802.11i specification. Previously, WEP encryption was the primary security method used between wireless Access Points (APs) and clients. However, WEP had a significant flaw due to its reliance on a fixed encryption key, which made it vulnerable to attacks using publicly available tools. IEEE developed WPA as an enhancement to 802.11 protocols to improve security. It is now widely supported by almost all Wi-Fi device manufacturers.

WPA offers enhanced data encryption compared to WEP. It uses the Temporal Key Integrity Protocol (TKIP), which encrypts data with the RC4 stream cipher and 128-bit keys. Additionally, WPA ensures data integrity through a Message Integrity Check (MIC) and provides strong encryption and authentication. As part of the 802.11i standard, WPA incorporates features such as Pre-Shared Key (PSK) or Extensible Authentication Protocol (EAP) authentication methods. Unlike WEP, which uses a 40-bit or 104-bit key, WPA with TKIP utilizes 128-bit keys for each packet, and it includes features like per-packet mixing functions, extended Initialization Vectors (IVs), re-keying, and MICs. These measures prevent attackers from altering or replaying packets.

- **TKIP**

This encryption protocol uses a unique unicast encryption key that changes with every packet, thus improving security. The key change for each packet is automatically synchronized between the wireless client and the Access Point (AP). TKIP incorporates the Michael Integrity Check (MIC) algorithm and a MIC key to generate the MIC value. It also employs the RC4 stream cipher with

128-bit keys and a 64-bit MIC for data integrity. TKIP enhances security by expanding the Initialization Vector (IV) size and introducing mixing functions. With TKIP, the client starts with a 128-bit Temporal Key (TK), which is then combined with the client's MAC address and the IV to form a keystream that encrypts the data using RC4. It also uses a sequence counter to prevent replay attacks. TKIP improves upon WEP by introducing a rekeying mechanism, ensuring new encryption and integrity keys. The temporal keys are refreshed every 10,000 packets, increasing resistance to cryptanalytic attacks that exploit key reuse.

- **TKs**

Modern Wi-Fi devices use TKIP (for WPA) or AES (for WPA2) encryption to maintain WLAN security. In WEP encryption, the encryption keys (TKs) are derived from the Pairwise Master Key (PMK) established during the EAP authentication session. In contrast, WPA and WPA2 encryption protocols generate the encryption keys during a four-way handshake. After the EAP success message, the PMK is sent to the AP but not directly sent to the Wi-Fi client, as the client generates its own copy of the PMK.

Figure 16-11 illustrates the process for installing TKs.

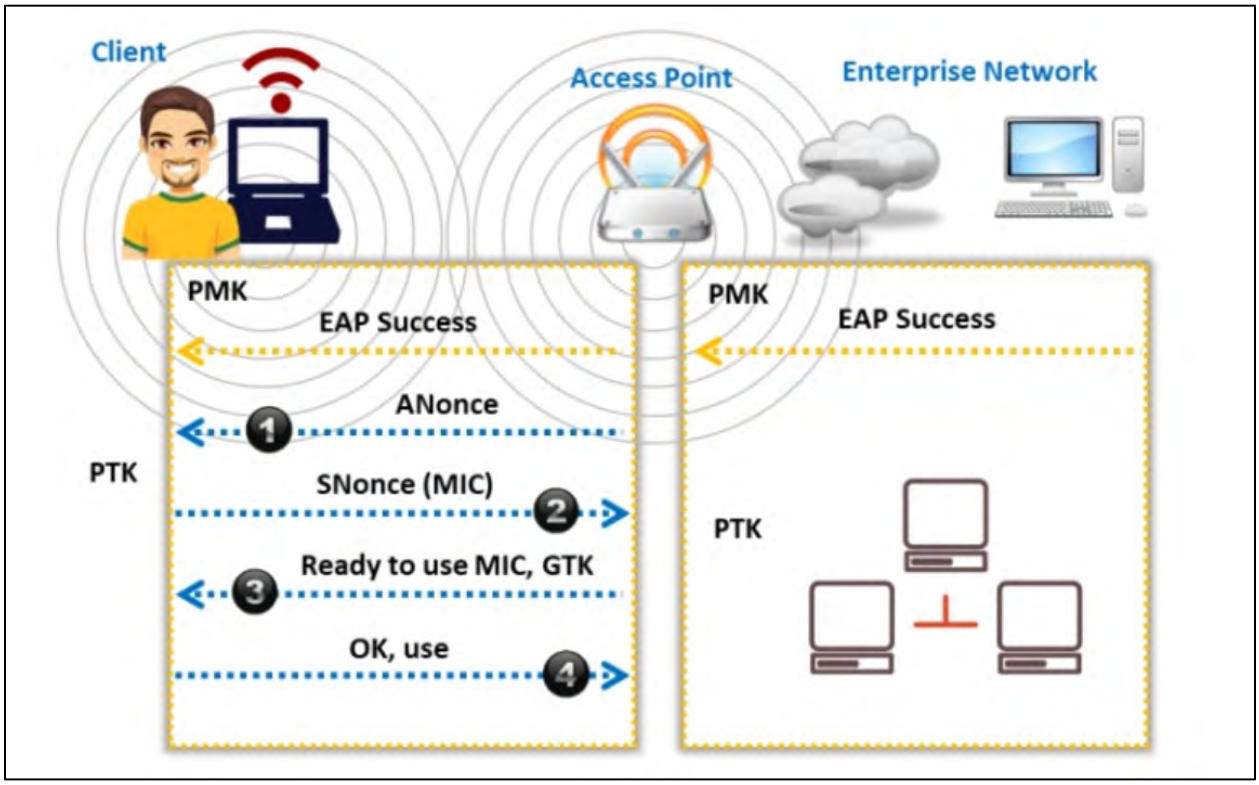


Figure 16-11: Operational Flow of Temporal Keys

- The AP sends an ANonce to the client, which then uses it to generate the Pairwise Transient Key (PTK)
- The client replies with its SNonce value and an MIC to the AP
- The AP sends the Group Temporal Key (GTK), a sequence number, and another MIC, which will be used for the upcoming broadcast frames

- The client verifies that the temporal keys have been successfully installed

How WPA Functions

- The RC4 algorithm uses the TK, transmit address, and TKIP Sequence Counter (TSC) as inputs to generate a keystream.
    - The IV or TK sequence, transmit address (or MAC destination address), and TK are mixed using a hash or mixing function to create a 128-bit or 104-bit key
    - This key is then processed with RC4 to generate a keystream that matches the length of the original message
- The MAC Service Data Unit (MSDU) and Message Integrity Check (MIC) are combined using the Michael algorithm
- The MSDU and MIC are fragmented to create the MAC Protocol Data Unit (MPDU)
- A 32-bit Integrity Check Value (ICV) is calculated for the MPDU
- The MPDU and ICV are XORed with the keystream to generate the encrypted data
- The IV is added to the encrypted data to create the MAC frame

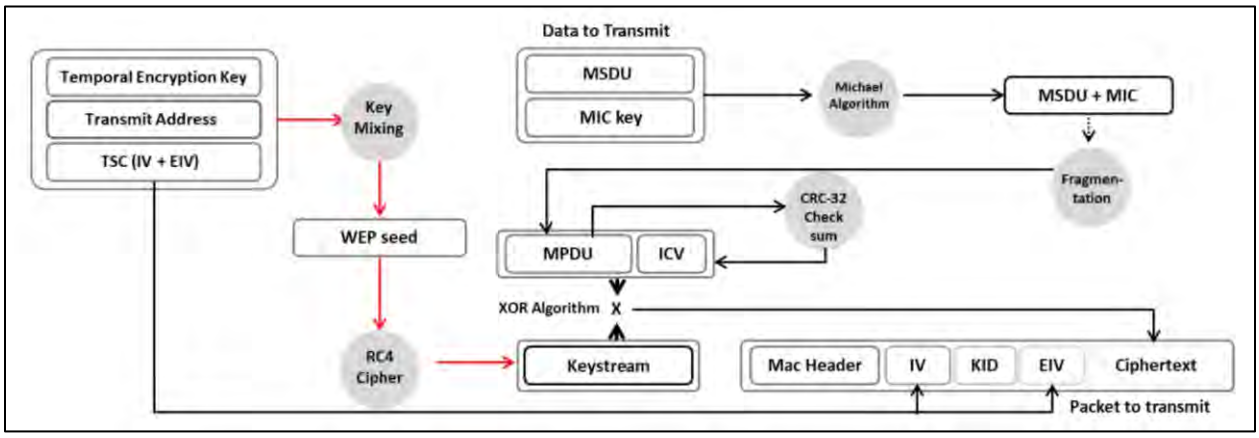


Figure 16-12: Operational Flow of WPA

Wireless Encryption: WPA2

Wi-Fi Protected Access 2 (WPA2) is a security protocol that protects wireless networks. Introduced in 2006, WPA2 replaced WPA and is aligned with the 802.11i standard. It offers several advanced security features not found in WPA. WPA2 incorporates the AES encryption algorithm, which complies with the National Institute of Standards and Technology (NIST) FIPS 140-2, providing robust encryption for wireless networks. Additionally, it utilizes the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), offering enhanced data protection and network access control. WPA2 ensures higher security for Wi-Fi connections, ensuring only authorized users can access the network.

Modes of Operation

WPA2 operates in two modes:

- **WPA2-Personal**: This mode utilizes a Pre-Shared Key (PSK) to prevent unauthorized access. A common 256-bit key is derived from a password and used by all wireless devices to authenticate with the Access Point (AP). Each device encrypts network traffic using a 128-bit key generated from an 8–63 character passphrase. The router combines the passphrase, network SSID, and TKIP to generate unique encryption keys for each device, which change periodically.
- **WPA2-Enterprise**: This mode leverages EAP or RADIUS for centralized authentication supporting methods like token cards, Kerberos, and certificates. It assigns a unique encrypted key to each device and keeps it hidden to prevent key sharing, enhancing security. A centralized server manages user login credentials, which must be provided when connecting to the network.

How WPA2 Works?

In WPA2, during the CCMP process, Additional Authentication Data (AAD) is created using the MAC header and incorporated into the encryption, which utilizes both AES and CCMP. This ensures that the unencrypted portion of the frame remains protected from modification. A sequenced Packet Number (PN) and part of the MAC header generate a Nonce for the encryption. The plaintext data, temporal keys, AAD, and Nonce are inputs for the encryption process with AES and CCMP algorithms.

A PN is included in the CCMP header to prevent replay attacks. The AES and CCMP encryption result in encrypted data and a MIC value. Finally, the MAC header, CCMP header, encrypted data, and encrypted MIC combine to form the WPA2 MAC frame.

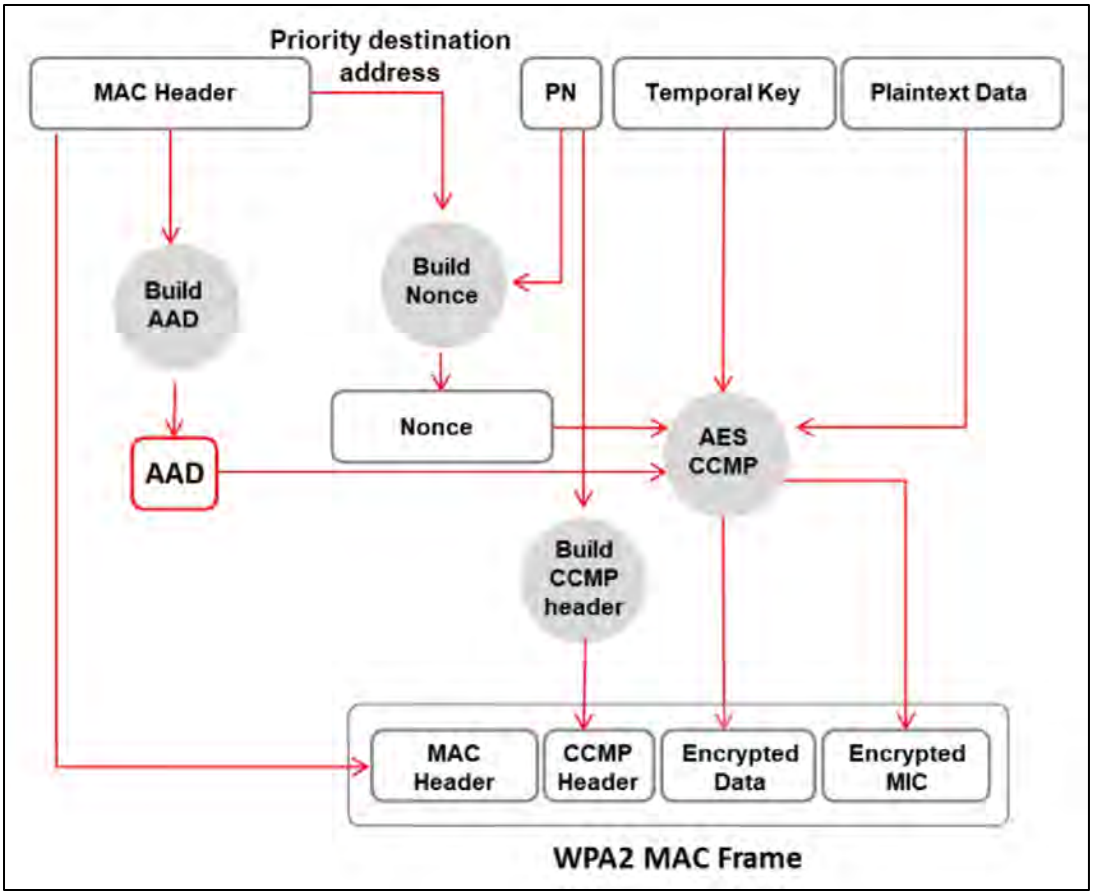


Figure 16-13: Operational Flow of WPA2

Wireless Encryption: WPA3

Wi-Fi Protected Access 3 (WPA3) was introduced by the Wi-Fi Alliance in January 2018 as an advanced version of WPA2, offering innovative protocols. Similar to WPA2, WPA3 has two versions: WPA3-Personal and WPA3-Enterprise.

WPA3 introduces state of the art features to enhance Wi-Fi security and cater to various network setups, from corporate environments to home networks. It ensures strong cryptographic protection by utilizing encryption algorithms like AES and TKIP to counteract network threats. Additionally, WPA3 strengthens network security with Protected Management Frames (PMF), offering robust defense against eavesdropping and spoofing attacks. WPA3 also eliminates support for outdated legacy protocols.

Modes of Operation

WPA3 provides two operational modes:

- **WPA3-Personal**: This mode focuses on password-based authentication and offers stronger resistance to attacks than WPA2. It employs a modern key exchange protocol called Simultaneous Authentication of Equals (SAE), or Dragonfly Key Exchange, replacing the PSK method from WPA2-Personal. Key features of WPA3-Personal include:

- **Protection against offline dictionary attacks**: It prevents passive attacks, like brute force password attempts
- **Prevention of key recovery**: Even if a password is compromised, session keys cannot be captured, maintaining the forward secrecy of network traffic
- **Support for easy-to-remember passwords**: Users can choose simple or commonly used phrases without sacrificing security
- **Improved accessibility**: WPA3 offers stronger security than WPA2 without requiring changes to the user's typical connection method

- **WPA3-Enterprise**: Building upon WPA2, this mode enhances network security and protects sensitive data through cryptographic techniques. WPA3-Enterprise incorporates the following protocols:
  - **Authenticated encryption**: Ensures data authenticity and confidentiality using the 256-bit Galois/Counter Mode Protocol (GCMP-256)
  - **Key derivation and validation**: It generates cryptographic keys from passwords or master keys using the 384-bit HMAC with the Secure Hash Algorithm (HMAC-SHA-384)
  - **Key establishment and verification**: It enables secure cryptographic key exchange through Elliptic Curve Diffie–Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) with a 384-bit elliptic curve
  - **Frame protection and robust administration**: WPA3 uses the 256-bit BIP-GMAC-256 to ensure the integrity of Broadcast/Multicast frames and robust management

Improvements in WPA3 Over WPA2

WPA3 introduces several enhancements to provide more comprehensive protection for Wi-Fi networks, enabling a multi-layered security approach. WPA3 also has a certification program that ensures products meet current standards, with the Dragonfly handshake/SAE protocol being a requirement for certification. Some of the key features of WPA3 include:

1. **Secure Handshake**: The Simultaneous Authentication of Equals (SAE) protocol, also known as the Dragonfly handshake, helps safeguard passwords against dictionary and brute-force attacks, preventing offline data decryption.
2. **Wi-Fi Easy Connect**: This feature streamlines the security setup process by managing multiple interface connections within a network through the Wi-Fi Device Provisioning Protocol (DPP). It allows secure connections for various smart devices via a QR code or password, aiding in setting IoT device connections.
3. **Unauthenticated Encryption**: WPA3 introduces Opportunistic Wireless Encryption (OWE), which improves protection when connecting to public hotspots or networks by replacing the 802.11 "open" authentication method with stronger encryption.

4. **Larger Session Keys**: WPA3-Enterprise employs cryptographic security that supports key sizes of 192 bits or more, making it more resistant to cracking and providing robust protection.

Comparison of WEP, WPA, WPA2 and WPA3

WEP offers basic data confidentiality for wireless networks but is vulnerable and fails to meet security standards. While WPA addresses many of WEP's issues, WPA2 provides near-wireless network security equivalent to wired networks. WPA2 supports authentication, ensuring that only authorized users can access the network. WEP and WPA should be replaced with WPA2 or WPA3 to secure a Wi-Fi network. Although WPA and WPA2 protect against forgery and replay attacks, WPA3 provides stronger password protection, secures IoT connections, and uses enhanced encryption. Table 16-02 compares WEP, WPA, WPA2, and WPA3 based on encryption algorithms, key size, Initialization Vector (IV), key management, and data integrity.

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24- bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48- bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48- bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length $1 - 2^{64}$	192-bits	ECDH and ECDSA	BIP-GMAC-256

Table 16-02: Comparison of WEP, WPA, WPA2, and WPA3

Issues with WEP, WPA, WPA2 and WPA3

Issues with WEP

- **CRC32 is inadequate for cryptographic integrity**: CRC32 fails to secure a packet's integrity fully. An attacker can capture two packets, alter a bit in the encrypted stream, and modify the checksum, ensuring the packet is still accepted.
- **IVs are limited to 24 bits**: The 24-bit IV is too small for secure encryption and is transmitted in cleartext within the message. When an Access Point (AP) sends 1500-byte packets at 11 Mbps, the IV space is exhausted within five hours.
- **Vulnerability to known plaintext attacks**: When an IV collision occurs, attackers can reconstruct the RC4 keystream using the IV and the decrypted packet payload, exposing the network to attacks.
- **Vulnerability to dictionary attacks**: WEP relies on passwords susceptible to password-cracking methods. The small IV space allows attackers to create a decryption table, making dictionary attacks feasible.

- **Vulnerable to DoS attacks**: WEP is exposed to Denial-of-Service (DoS) attacks because associate and disassociate messages are not authenticated.
- **Decryption table construction**: An attacker with approximately 24 GB of storage space can create a reconstructed keystream table, enabling real-time WEP packet decryption.
- **Lack of centralized key management**: The absence of centralized key management makes regular key changes difficult, which is a significant security flaw.
- **IV field is too small**: The 24-bit IV is inadequate for randomness and is transmitted in the cleartext portion of the message. A busy AP could use up all IV values within hours. Reusing IVs results in identical keystreams, which attackers can exploit to decrypt messages. Additionally, wireless devices from the same manufacturer might generate identical IV sequences, aiding attackers in keystream determination.
- **The IV field is not unique for each packet:** Vendors only utilize a small portion of the 24-bit IV range, undermining the mechanism's randomness. Attackers can determine the keystream, allowing them to decrypt additional messages.
- **RC4 was not designed for multiple message encryption**: RC4 was meant as a one-time cipher and is unsuitable for use with multiple messages, weakening its security when applied to WEP.
- **Shared keys across the network**: Since all users share the same key, changing it requires reconfiguring each device in the network, discouraging frequent key changes.
- **Lack of replay attack prevention**: WEP lacks a mechanism to stop replay attacks, allowing attackers to retransmit intercepted packets.
- **CRC-32 is not a cryptographic hash**: It is susceptible to bit-flipping attacks, in which attackers can modify the packet and adjust the checksum accordingly.
- **Insufficient key length**: Even with a 104-bit key, WEP fails to meet modern cryptographic standards, making brute-force attacks possible.
- **One-way authentication**: WEP only supports one-way authentication, in which the client authenticates the AP, but the AP does not authenticate the client.
- **FMS attack vulnerability**: The Fluhrer, Mantin, and Shamir (FMS) attack exploits RC4's key scheduling weakness. By reusing IVs, attackers can use statistical analysis to recover the WEP key, rendering WEP encryption insecure.

Many organizations configure their network clients and Access Points (APs) to use either the same shared key or one of four default keys, making the keystream's randomness heavily dependent on the uniqueness of the IV value. While combining the IV with a key is intended to produce a unique keystream for each packet, the key typically remains static, leaving the IV as the sole variable. This lack of variability undermines the encryption process, resulting in insufficient randomization.

A busy AP can exhaust all 224 possible IV values within hours, forcing the reuse of IVs. Such repetition in an encryption process that depends on randomness compromises security. The problem is further aggravated by the 802.11 standard, which does not mandate unique IV values for every packet—akin to claiming robust security while implementing inadequate measures.

In many cases, the IV only changes when the wireless NIC is reinitialized, such as during a reboot. While 24 bits theoretically allow many IV combinations, most implementations utilize only a fraction of this potential, failing to leverage the available security features fully.

The generation of weak IVs in WEP can be attributed to several factors:

- **Predictability in RC4's Key Scheduling Algorithm (KSA):** To generate different packets, RC4 uses a KSA that creates an IV and combines it with the base key, making the first few bytes of plaintext predictable
- **Non-unique IVs across devices:** Since IV values are not specific to the network, the same IV can be reused with the same secret key on multiple wireless devices, reducing randomness
- **Vulnerability to FMS Attacks:** Appending the IV to the security key exposes the network to Fluhrer–Mantin–Shamir (FMS) attacks. Attackers can exploit this by using scripts to analyze links and crack the secret key
- **Weak IVs reveal key information:** Many weak IVs depend on the WEP key and can reveal precise details about the key bytes from the first RC4 output byte and smaller clues from other bytes
- **Emulating key details from IVs:** Additional processing of recovered bytes enables attackers to simulate parts of the Pseudo-Random Generation Algorithm (PRGA) and extract key details from an IV
- **Ineffective message tampering detection:** While methods like checksum and ICV can verify message integrity, they have limitations. Secure MIC computations, as used in TKIP, often involve high overhead
- **No key update mechanism:** WEP uses the master key directly without a built-in process for key updates

This design flaw in RC4's implementation makes WEP vulnerable to weak IV generation, which attackers can exploit. Attackers can use WLAN sniffing tools to capture packets encrypted with the same key and employ software like aircrack-ng and Wifi-Cracker to decrypt weak IVs, ultimately exposing the base WEP key.

Issues with WPA

While WPA represents an improvement over WEP due to its use of TKIP for data encryption and secured data transfer, it still faces several security challenges:

- **Weak Passwords:** WPA PSK is susceptible to password-cracking attacks when users rely on weak passwords
- **Absence of Forward Secrecy:** If attackers gain access to the PSK, they can decrypt all packets encrypted with that key, including past and ongoing transmissions
- **Packet Spoofing and Decryption Risks:** WPA-TKIP devices are vulnerable to packet injection and decryption attacks, enabling attackers to hijack TCP connections
- **Predictable Group Temporal Key (GTK):** An insecure Random Number Generator (RNG) in WPA can expose the GTK created by the AP. This vulnerability allows attackers to inject malicious traffic and decrypt ongoing transmissions on the network

- **IP Address Guessing:** TKIP weaknesses enable attackers to deduce the subnet's IP address and inject small packets into the network, deteriorating network performance

Issues with WPA2

Although WPA2 provides stronger security than WPA, it is not without its vulnerabilities, as outlined below:

- **Weak Passwords:** When users rely on weak passwords, WPA2 PSK is susceptible to eavesdropping, dictionary attacks, and password cracking
- **Absence of Forward Secrecy:** If an attacker obtains the PSK, they can decrypt all past and ongoing packets encrypted with that key
- **Man-In-The-Middle (MITM) and Denial-of-Service (DoS) Vulnerabilities:** The Hole96 vulnerability in WPA2 enables attackers to exploit the shared Group Temporal Key (GTK) to conduct MITM and DoS attacks
- **Predictable Group Temporal Key (GTK):** A weak Random Number Generator (RNG) in WPA2 can expose the GTK generated by the Access Point (AP), allowing attackers to inject malicious traffic and decrypt ongoing transmissions
- **KRACK Vulnerabilities:** The Key Reinstallation Attack (KRACK) exploit in WPA2 can allow attackers to sniff packets, hijack connections, inject malware, and decrypt communications
- **Wireless DoS Attacks:** Attackers can misuse WPA2's replay attack detection feature by sending forged group-addressed data frames with a large Packet Number (PN) to carry out DoS attacks
- **Insecure WPS PIN Recovery:** When WPA2 and WPS are enabled, attackers can expose the WPA2 key by identifying the WPS Personal Identification Number (PIN) through straightforward methods. Disabling both WPA2 and WPS can be complex and time-consuming, providing further opportunities for attackers

Issues with WPA3

Although WPA3 provides enhanced security compared to WPA2, it still has certain vulnerabilities and challenges, as outlined below:

- **Implementation Challenges:** Transitioning from WPA2 to WPA3 can be problematic for older devices and networks. Many legacy devices lack WPA3 support unless updated via firmware, leading to compatibility issues
- **Slow Adoption:** The limited adoption of WPA3 remains a significant concern. Many networks and devices continue to use WPA2, undermining the widespread effectiveness of WPA3's security improvements
- **Resource Demands:** WPA3 employs more advanced encryption algorithms, requiring greater processing power. This can negatively impact the performance of older devices with limited computational capabilities
- **Configuration Errors:** Proper setup and implementation are critical to leveraging WPA3's security features. Misconfigurations, such as weak passwords or poor network setups, can leave networks susceptible to breaches despite WPA3's advanced protections

- **Timing Attacks:** WPA3 uses Simultaneous Authentication of Equals (SAE) to replace WPA2's Pre-Shared Key (PSK). However, some implementations of SAE are vulnerable to timing attacks, potentially enabling attackers to deduce the password
- **Cache-Based Side-Channel Attacks:** These attacks exploit cache access patterns to extract sensitive cryptographic information, potentially exposing secure data
- **Transition Mode Vulnerabilities:** To maintain compatibility with older devices, WPA3 includes a "transition mode" where both WPA3 and WPA2 are enabled. Attackers can exploit WPA2's vulnerabilities, such as KRACK, to compromise the network, weakening overall security in this mixed mode
- **Hardware Requirements:** WPA3 requires updated hardware to support its features fully. Many older devices are incompatible with WPA3 and cannot be upgraded, making hardware replacement costly for organizations and individuals

 **EXAM TIP:** Understand the different types of wireless encryption protocols (WEP, WPA, WPA2, WPA3) and their weaknesses. Focus on WPA3 as the most secure option and how it improves upon WPA2.

Wireless Threats

The earlier sections covered foundational wireless concepts and security mechanisms, including encryption algorithms to safeguard wireless network communications. Administrators must recognize potential vulnerabilities in these encryption algorithms to protect wireless networks that could attract attackers effectively. Wireless networks face various threats, such as access-control attacks, integrity breaches, confidentiality compromises, availability disruptions, and authentication challenges. This section explores wireless network security risks, threats, and attacks.

Access Control Attacks

Wireless access-control attacks target a network by bypassing WLAN access-control mechanisms, such as MAC address filtering on Access Points (APs) and Wi-Fi port access controls. Common types of these attacks include the following:

- **MAC Spoofing:** Attackers manipulate their device's MAC address to impersonate an authorized AP on a trusted network. Tools like SMAC are often employed for this purpose, allowing the attacker to deceive the network into granting access.
- **AP Misconfiguration:** Security vulnerabilities can arise when an AP is not configured correctly. Misconfigured APs, often due to errors in security settings, can expose an entire network to attacks. Since intrusion detection systems usually recognize these APs as legitimate devices, they fail to generate alerts, making detection challenging. Users may inadvertently change an AP's security settings, leading to misconfigurations compromising network integrity.

Misconfigured APs represent a significant security risk because attackers can exploit these devices to connect to a secured network unnoticed. These APs operate normally without triggering security alarms even after gaining unauthorized access. Many organizations struggle to maintain robust Wi-

Fi security policies, leaving these vulnerabilities unaddressed and their networks susceptible to attacks.

As organizational Wi-Fi networks expand to encompass more locations and devices, misconfigured APs pose an increasing threat. Key factors contributing to this vulnerability include:

- **SSID Broadcast:** Attackers may set APs to broadcast SSIDs to appear legitimate to authorized users. Most AP models come with default SSIDs, and those left in their default state are particularly susceptible to brute-force dictionary attacks. Even if WEP is enabled, an unencrypted SSID broadcasts the password in plaintext, making it easier for attackers to exploit.
- **Weak Passwords:** Some network administrators mistakenly use SSIDs as basic passwords to authenticate users. While SSIDs can help identify authorized wireless devices, relying on them as a security measure makes networks vulnerable to unauthorized access.
- **Configuration Errors:** These errors can arise during installation, in AP configuration policies, through human mistakes while troubleshooting, or from inconsistent implementation of security changes across the network. SSID broadcasting, a common configuration error, allows attackers to intercept the SSID. Once acquired, the attacker can trick the AP into recognizing their connection as legitimate.

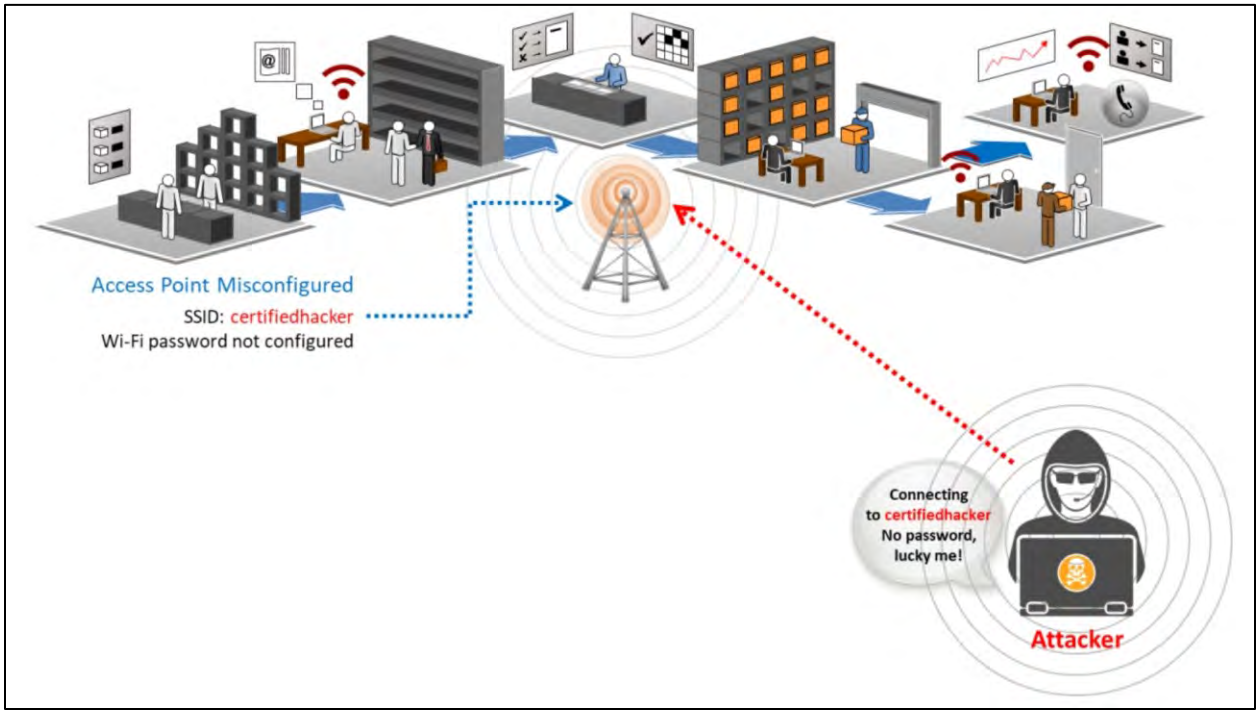


Figure 16-14: Misconfigured AP Attack

- **Ad Hoc Associations:** In ad hoc mode, Wi-Fi clients can connect directly to each other without relying on an AP to forward packets. This setup is popular among Wi-Fi users for its convenience in sharing data. However, security risks emerge when an attacker manipulates the network to activate ad hoc mode. Some resources are accessible exclusively through ad hoc

connections. However, this mode lacks robust authentication and encryption, making it inherently insecure. An attacker can easily exploit these weaknesses to connect to and compromise a client in ad hoc mode. Additionally, once inside the wireless network, the attacker can use the ad hoc connection to breach the security of the organization's wired LAN.

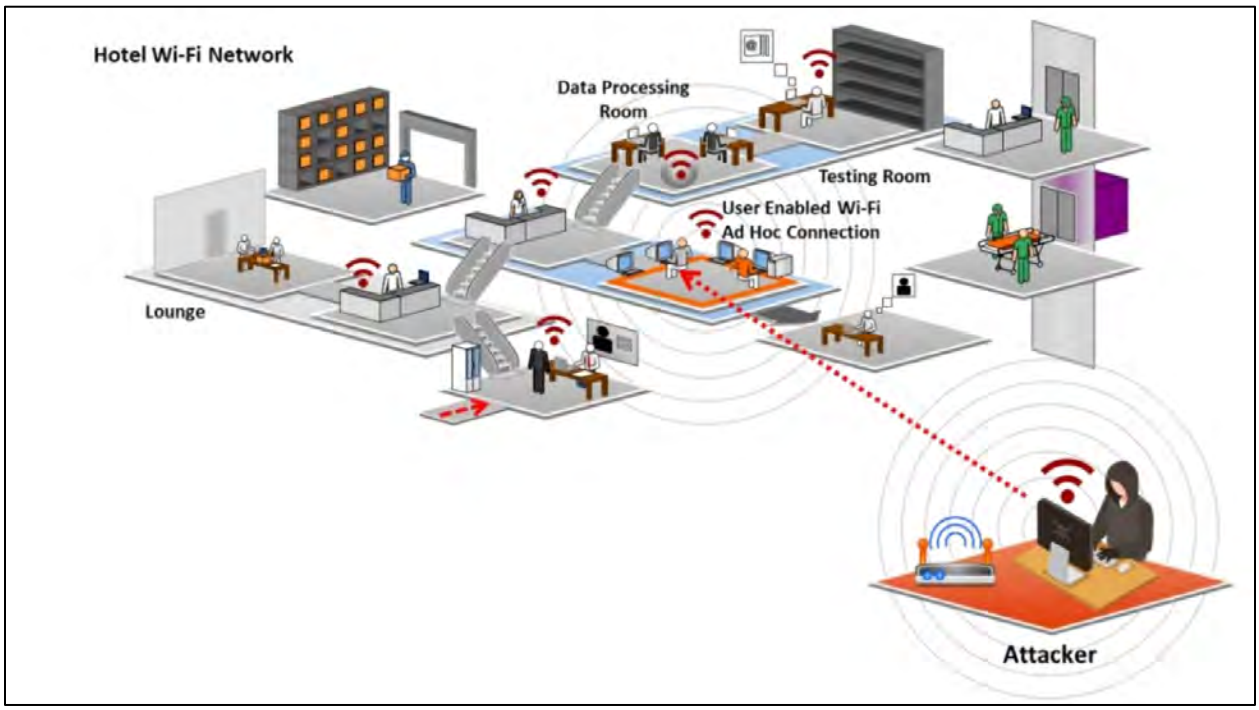


Figure 16-15: Ad Hoc Associations Attack

- **Promiscuous Client:** Attackers exploit the behavior of 802.11 wireless cards, which are designed to seek out the strongest available signal. By positioning an AP near the target network and assigning it a common SSID, the attacker creates a stronger, more appealing signal to lure clients away from legitimate networks. Once connected, the attacker can route network traffic through this fake AP. This method resembles the "evil twin" attack, where an attacker sets up an AP mimicking the legitimate network by broadcasting the same SSID, deceiving clients into connecting.
- **Client Mis-association:** Clients may intentionally or inadvertently connect to an unauthorized AP outside the intended network because WLAN signals travel through walls and other barriers. This mis-association introduces vulnerabilities to access-control attacks. Such connections may result from misconfigured devices, inadequate corporate Wi-Fi coverage, lack of clear Wi-Fi policies, restricted office internet access, unmanaged ad hoc connections, or enticing SSIDs. Mis-associations can happen with or without the client's knowledge and often involve rogue APs or neighboring networks.

  An attacker establishes a rogue AP outside the organization's boundary to conduct a client mis-association attack. After identifying the target network's SSID, the attacker uses a spoofed SSID to broadcast beacons, enticing clients to connect to the rogue AP. This rogue AP acts as a gateway to circumvent enterprise security measures. Once a client is connected, the attacker

can extract sensitive data, including usernames and passwords, by employing Man-In-The-Middle (MITM) attacks, EAP dictionary attacks, or leveraging tools like Metasploit to exploit the mis-association.

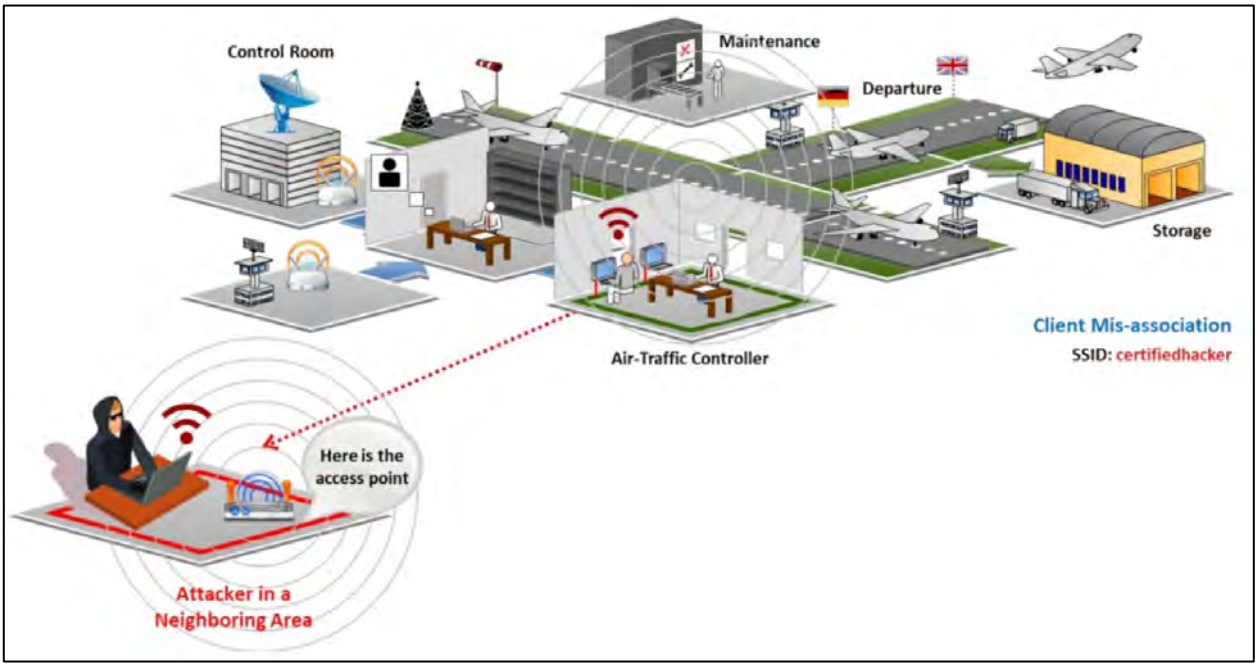


Figure 16-16: Client Mis-Association Attack

- **Unauthorized Association:** Wireless networks face significant risks from unauthorized associations, which can occur in two forms: malicious and accidental.
    - **Malicious Association:** An attacker uses a soft AP instead of a legitimate corporate AP to infiltrate a network. This is typically done by running software on a device like a laptop to make its Network Interface Card (NIC) appear as a valid AP. Tools for creating soft APs are often embedded in WLAN radios on some laptops, PDAs, or client cards, and attackers can activate them manually or through malware. The attacker can activate a soft AP to establish unauthorized connections to the enterprise network by infecting a victim's device. Once access is gained, the attacker may steal sensitive information, launch attacks on the wired network, or install malicious software like trojans.
    - **Accidental Association:** This occurs when a device unintentionally connects to a neighboring organization's overlapping network AP without the user's awareness, creating an unintentional security vulnerability.

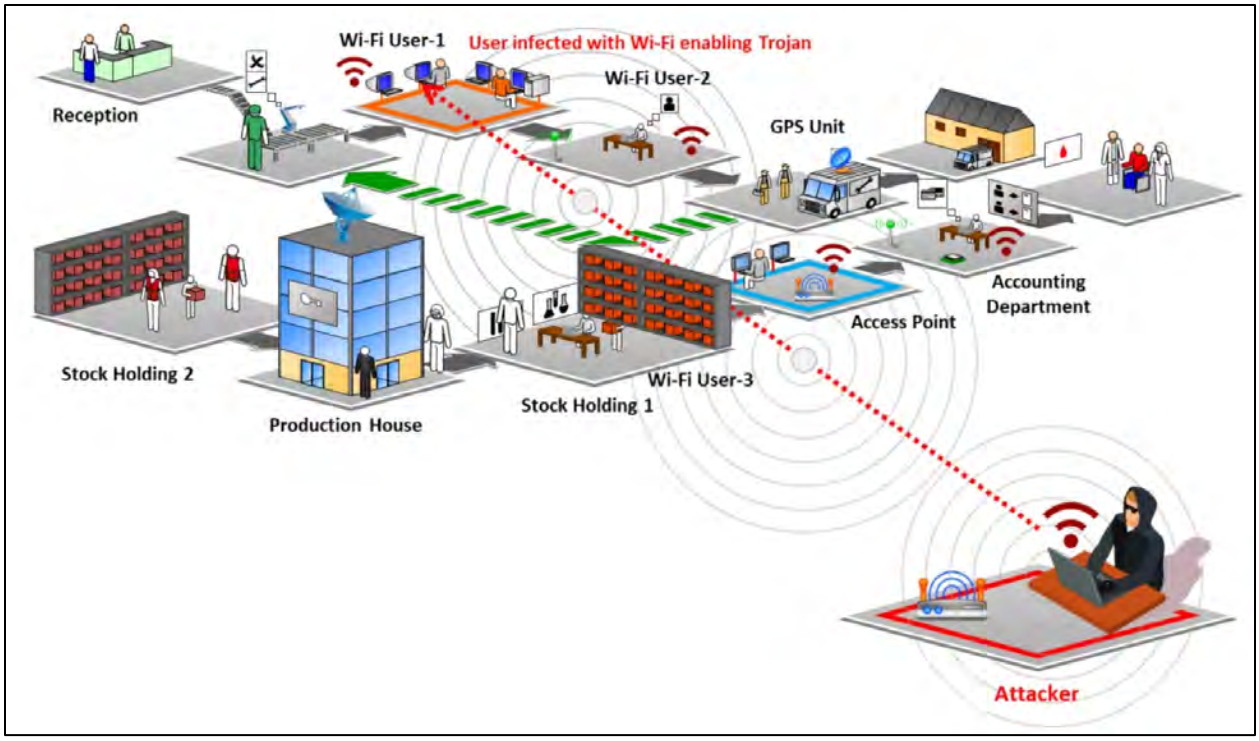


Figure 16-17: Unauthorized Association Attack

Integrity Attacks

An integrity attack occurs when data is tampered with or modified during transmission. In the context of wireless networks, attackers achieve this by transmitting falsified control, management, or data frames. These forged frames can mislead wireless devices and facilitate further attacks, such as Denial-of-Service (DoS) attacks. Table 16-03 provides an overview of various types of integrity attacks.

Type of Attack	Description	Method and Tools
Data-Frame Injection	Constructing and sending forged 802.11 frames.	Airpwn-ng, Wperf
WEP Injection	Constructing and sending forged WEP encryption keys.	WEP cracking + injection tools
Bit-Flipping Attacks	Capturing the frame, flipping random bits in the data payload, modifying the ICV, and sending it to the user.	
Extensible AP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, and Failure) for later replay.	Wireless capture + injection tools between client and AP
Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + injection tools

Initialization Vector Replay Attacks	Deriving the keystream by sending a plaintext message.	
RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay	Ethernet capture + injection tools between AP and authentication server
Wireless Network Viruses	Viruses have a great impact on wireless networks. They can provide an attacker with a simple method to compromise APs.	

Table 16-03: Integrity Attacks

Confidentiality Attacks

Confidentiality attacks aim to capture sensitive information transmitted over a wireless network, whether the data is sent in cleartext or encrypted. If encryption protocols such as WEP or WPA are used, attackers may attempt to decrypt the data. Table 16-04 outlines various types of confidentiality attacks on wireless networks.

Type of Attack	Description	Method and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	Wireshark, Ettercap, Kismet, commercial analyzers
Traffic Analysis	Inferring information from the observation of external traffic characteristics.	Wireshark, Ettercap, Snort
Cracking WEP Key	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	Aircrack-ng, WEPCrack
Evil Twin AP	Posing as an authorized AP by beaconing the WLAN's SSID to lure users.	Hostapd, EvilTwinFramework, Wifiphisher
Honeypot AP	Setting an AP's SSID to be the same as that of a legitimate AP	Manipulating SSID
Session Hijacking	Manipulating the network so that the attacker's host appears to be the desired destination.	Manipulating
Masquerading	Pretending to be an authorized user to gain access to a system.	Stealing login IDs and passwords, bypassing authentication mechanisms
MITM Attack	Running conventional MITM attack tools on an evil-twin AP to intercept TCP sessions or Secure Sockets Layer (SSL)/Secure Shell (SSH) tunnels.	dsniff, Ettercap, aLTEr attack

Table 16-04: Confidentiality Attacks

Availability Attacks

Availability attacks are designed to disrupt wireless services, preventing legitimate users from accessing or utilizing WLAN resources. These attacks compromise the accessibility of wireless network services by either overwhelming the resources or denying users access. Attackers employ various techniques to execute such attacks, hindering the functionality of wireless networks. Table 16-05 provides an overview of different types of availability attacks on wireless networks.

Type of Attack	Description	Method and Tools
Access Point Theft	Physically removing an AP from its installed location.	Stealth and/or speed
Disassociation Attacks	Destroying the connectivity between an AP and a client to make the target unavailable to other wireless devices	Destruction of connectivity
EAP-Failure	Observe a valid 802.1X EAP exchange and send the client a forged EAP-Failure message.	Airtool Pi
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it difficult for clients to find a legitimate AP.	
Denial-of-Service	Exploiting the Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) Clear Channel Assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports the CW Tx mode with a low-level utility to invoke continuous transmissions
De-authenticate Flood	Flooding client(s) with forged de-authenticates or disassociates to disconnect users from an AP.	AirJack
Routing Attacks	Distributing routing information within the network.	RIP protocol, exploiting Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols using wormhole and sinkhole attacks
Authenticate Flood	Sending forged authenticates or associates from random MACs to fill a target AP's association table.	AirJack
Address Resolution Protocol (ARP) Cache Poisoning Attacks	Creating many attack vectors.	
Power Saving Attacks	Transmitting a spoofed Traffic Indication Map (TIM) or delivery TIM (DTIM) to a	

	client in the power-saving mode makes the client vulnerable to a DoS attack.	
TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	

Table 16-05: Availability Attacks

Authentication Attacks

Authentication attacks aim to steal Wi-Fi clients' identities, including their personal information and login credentials, to gain unauthorized access to network resources. Table 16-06 outlines various types of authentication attacks on wireless networks.

Type of Attack	Description	Method and Tools
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool.	Cowpatty, Fern Wifi Cracker
LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Asleap, THC-LEAPcracker
VPN Login Cracking	Gaining user credentials (e.g., Point-to-Point Tunneling Protocol (PPTP) password or Internet Protocol Security (IPsec) pre-shared secret key) using brute-force attacks on Virtual Private Network (VPN) authentication protocols.	ike_scan and IKECrack (IPsec), Anger and THC-pptp-bruter (PPTP)
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes with a brute-force or dictionary-attack tool.	John the Ripper, LophtCrack, THC-Hydra
Key Reinstallation Attack	Exploiting the four-way handshake of the WPA2 protocol.	Nonce reuse technique
Identity Theft	Capturing user identities from cleartext 802.1X Identity Response packets.	Packet capturing tools
Shared Key Guessing	Attempting 802.11 shared key authentication with the vendor default or cracked WEP keys.	WEP cracking tools, Wifite
Password Speculation	Repeatedly attempting 802.1X authentication using a captured identity to guess the user's password.	Password dictionary
Application Login Theft	Capturing user credentials (e.g., email address and password) from cleartext application protocols.	Ace Password Sniffer, dsniff, Wi-Jacking Attack

Table 16-06: Authentication Attacks

Honeypot AP Attack

In areas with multiple WLANs, users can connect to any available network, making such locations susceptible to attacks. When a wireless client is powered on, it searches for a specific SSID nearby. Attackers exploit this behavior by setting up a rogue AP with a high-power antenna, broadcasting the same SSID as the target network. Users who frequently connect to various WLANs may inadvertently connect to this rogue AP, a "honeypot" AP. These APs emit a stronger beacon signal than legitimate ones, attracting wireless clients seeking the strongest available signal. Suppose an authorized user connects to a honeypot AP. In that case, it creates a security vulnerability, potentially exposing the attacker to sensitive information such as usernames, passwords, and identities.

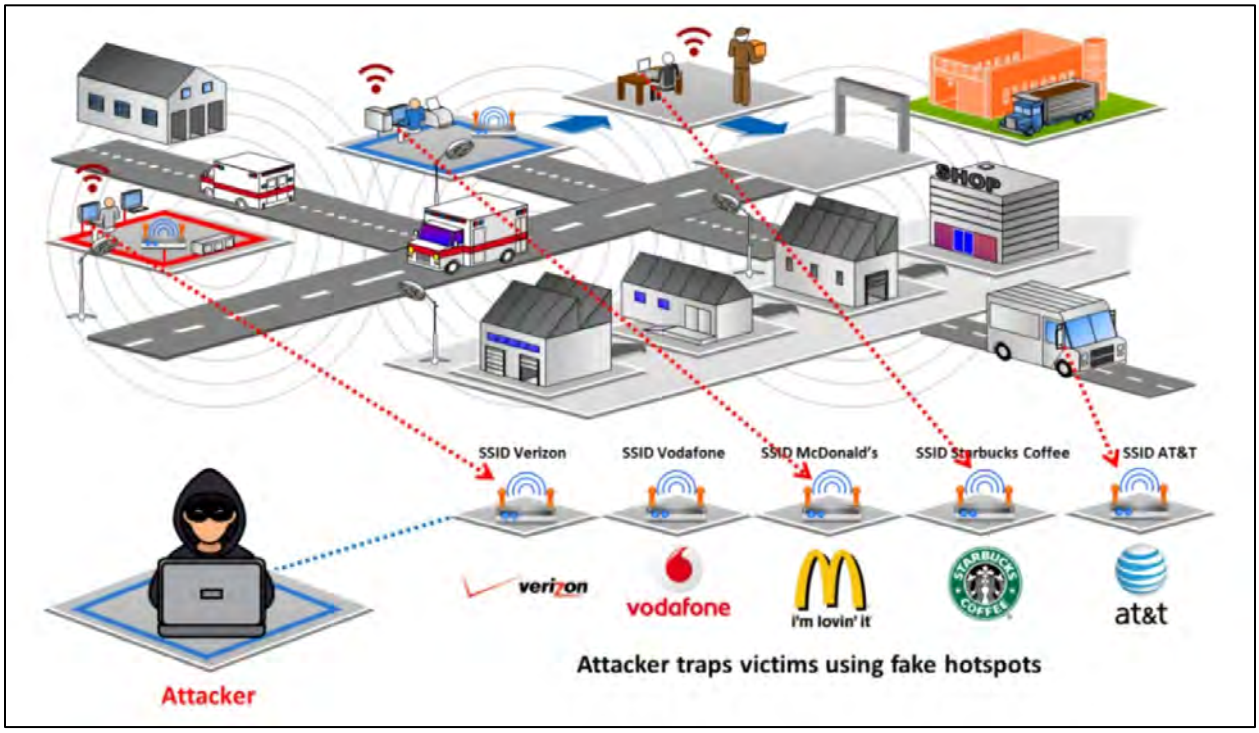


Figure 16-18: Honeypot AP Attack

Wormhole Attack

A wormhole attack targets dynamic routing protocols like Dynamic Source Routing (DSR) and Ad-Hoc On-Demand Distance Vector (AODV). In this type of attack, the attacker positions themselves within the target network to intercept and record ongoing wireless transmissions. From this location, the attacker claims that the malicious node offers the shortest path for data transmission to other network nodes. To facilitate this, the attacker establishes a tunnel to forward data between the source and destination nodes, enabling them to eavesdrop on the communication.

In wireless sensor networks, protocols like AODV and DSR rely on Route Request (RREQ) and Route Reply (RREP) messages to discover routes between source and destination nodes

dynamically. For example, when a source node (S) broadcasts an RREQ packet to the destination node (D), D responds by sending an RREP packet containing route information. This reply is a unicast message. Upon receiving the RREP, the source node stores the route information in its cache. It uses it to forward application data to the destination.

In a wormhole attack, the attacker attempts to create a tunnel between the source node (S) and destination node (D) by positioning a malicious node (M) within the transmission range of both S and D. The attacker monitors network traffic to capture RREQ messages. When S sends an RREQ to find a route to D, the attacker intercepts this message and forwards it directly to D before the original RREQ reaches D. Similarly, the attacker intercepts the RREP message from D and forwards it to S before the original RREP arrives at S, effectively establishing a fake direct link between S and D via M. Once the tunnel is in place, the attacker can control the data flow between S and D and potentially launch further attacks.

Wormhole attacks represent a significant risk to wireless sensor networks. Attackers can alter routing and application data in real-time, severely compromising network data's confidentiality, integrity, and availability.

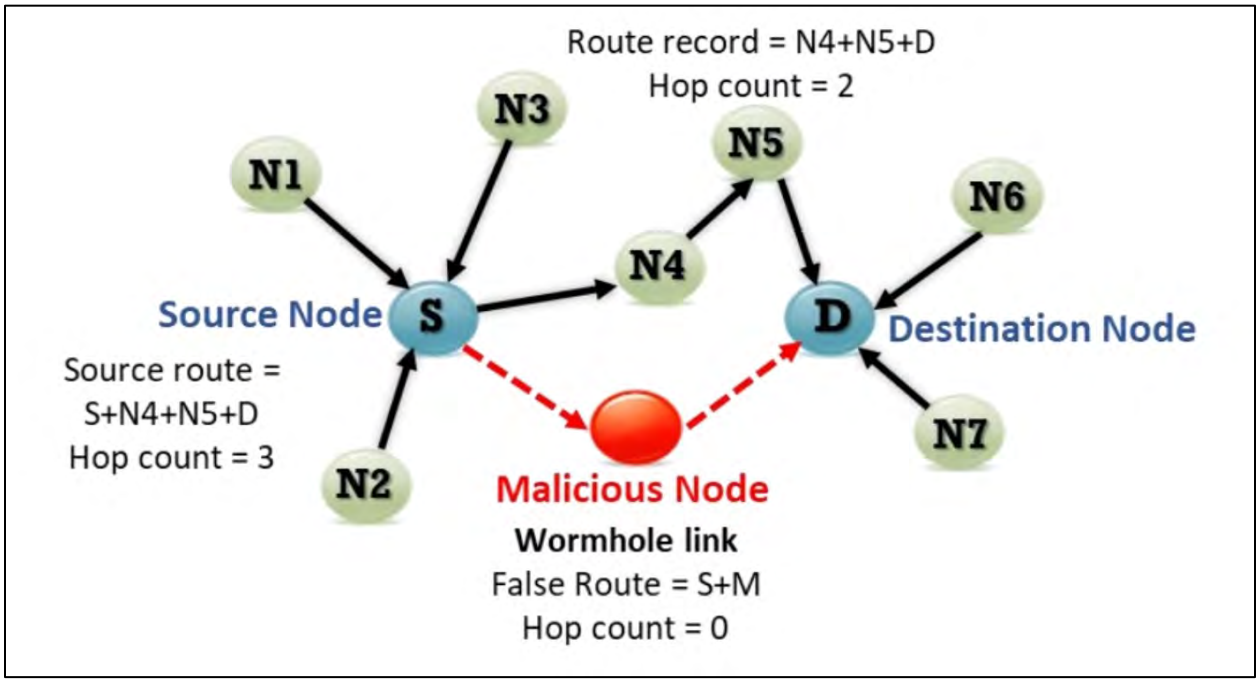


Figure 16-19: Wormhole Attack

Sinkhole Attack

A sinkhole attack is a type of selective forwarding attack where the attacker promotes a compromised or malicious node as the shortest route to the base station. The attacker places this malicious node close to the base station, luring neighboring nodes with false routing information, and then performs a data manipulation attack. The compromised node allows the attacker to intercept and alter network communications.

A sinkhole attack can be combined with a wormhole attack, where the malicious node captures all network traffic and uses tunneling to reach the base station more quickly than other nodes. Sinkhole attacks are difficult to detect and can harm higher-layer applications in the OSI model.

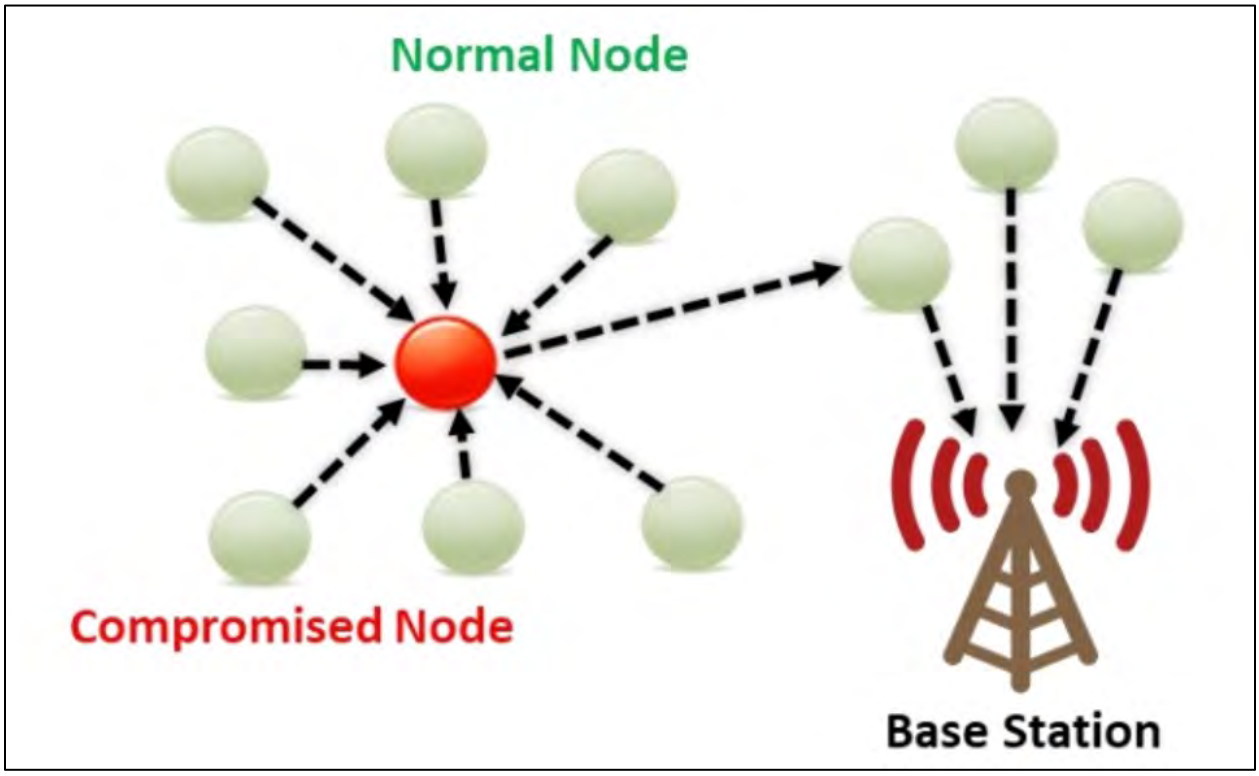


Figure 16-20: Sinkhole Attack

Inter-Chip Privilege Escalation/Wireless Co-Existence Attack

An inter-chip privilege escalation attack takes advantage of vulnerabilities in the wireless chips responsible for handling Bluetooth and Wi-Fi communications. Manufacturers typically design separate chips for Bluetooth and Wi-Fi or create a single combo chip to support both types of wireless communication. Attackers exploit these combo chips by using one chip to access data from another and move laterally to target other chips. For example, while sharing resources, a Bluetooth chip might capture sensitive information like credentials from the Wi-Fi chip or manipulate the traffic passing through it. This can lead to a wireless co-existence attack, which could result in privilege escalation at the chip boundaries.

EXAM TIP: Study the various wireless threats, such as man-in-the-middle attacks, eavesdropping, de-authentication attacks, and rogue APs. Understand how each threat works and how attackers exploit wireless networks.

Wireless Hacking Methodology

To compromise wireless networks, attackers use a structured hacking methodology comprising a series of systematic steps designed to target and infiltrate a wireless network. This section outlines

the process involved in this methodology. By following this approach, attackers aim to identify and exploit all potential entry points into the target network.

The primary goal of the wireless hacking methodology is to breach a Wi-Fi network and gain unauthorized access to its resources. The typical steps in this process include:

- Wi-Fi discovery
- Wireless traffic analysis
- Launch of wireless attacks
- Wi-Fi encryption cracking
- Compromising the Wi-Fi network

Wi-Fi Discovery

The initial step involves identifying a Wi-Fi network or device. Attackers conduct Wi-Fi discovery to detect potential target networks using tools like inSSIDer, NetSurveyor, etc. This process includes mapping nearby wireless networks and selecting a suitable target within range to initiate an attack.

Wireless Network Footprinting

An attack on a wireless network starts with its discovery and analysis. This process, known as footprinting, involves identifying and understanding the network. To accomplish this, attackers locate the Basic Service Set (BSS) associated with the Access Point (AP). They may also identify an Independent Basic Service Set (IBSS) by detecting the network's SSID. Determining the SSID is crucial, as it allows the attacker to connect with the AP, paving the way to compromise the network's security.

Attackers commonly use two methods to uncover a wireless network's SSID:

Passive Footprinting Method

This technique involves listening to wireless signals to capture packets transmitted over the airwaves. By analyzing these packets, the attacker can discover wireless devices, APs, and the SSID without actively connecting to any APs or wireless clients or injecting data packets into the network traffic.

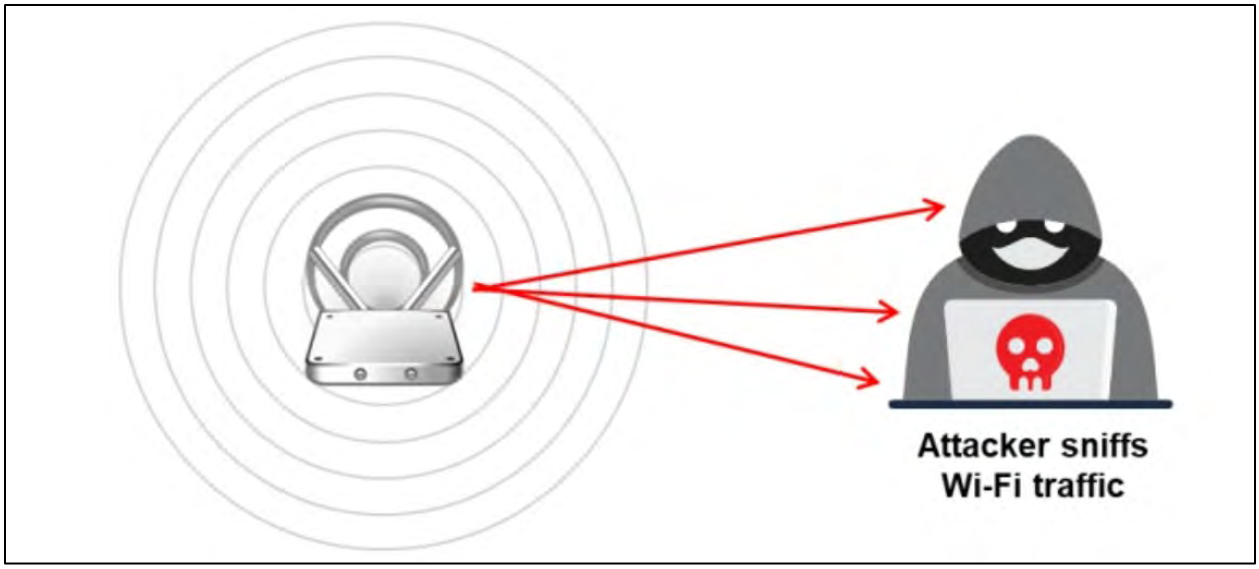


Figure 16-21: Passive Footprinting Method

Active Footprinting Method

In this approach, the attacker's device communicates with an Access Point (AP) by sending a probe request containing the SSID. The device can send a probe request with a blank SSID if the SSID is unknown. Most APs respond to such requests by including their SSID in the probe response packet, making empty SSIDs a valuable way to uncover the SSIDs of APs. Using this method, the attacker identifies the correct Basic Service Set (BSS) to target. Additionally, attackers may configure the AP to ignore probe requests with empty SSIDs to refine their attack strategy.

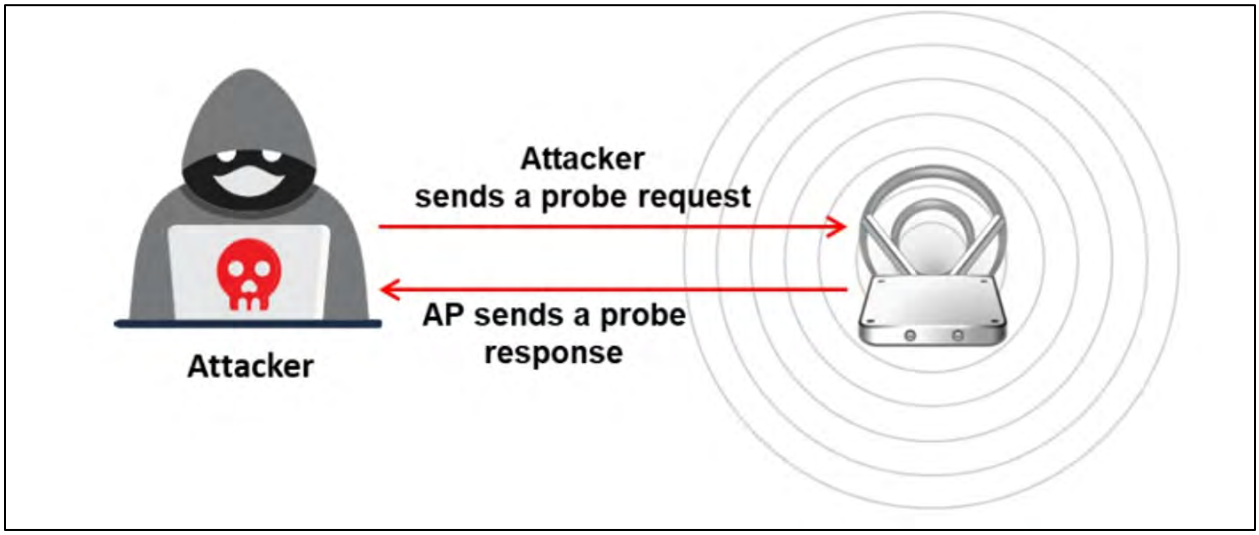


Figure 16-22: Active Footprinting Method

Attackers can use tools like NetSurveyor and Wi-Fi Scanner to scan for nearby Wi-Fi networks. The SSID is included in various types of wireless communication, such as beacons, probe requests and responses, and association and re-association requests. Through passive scanning, an attacker can capture the SSID without direct interaction. The attacker can switch to active scanning to reveal

the SSID if passive scanning is unsuccessful. Once the SSID is identified, the attacker can connect to the wireless network and carry out attacks. Wireless network scanning involves sniffing by adjusting to different radio channels used by devices.

Figure 16-23: Attackers Scanning for Wi-Fi Networks

Finding Wi-Fi Networks in Range to Attack

The initial step for an attacker targeting Wi-Fi networks is identifying potential networks within range and selecting the most suitable one for an attack. To locate target networks, attackers employ various Wi-Fi chalking methods, including:

- **WarWalking**: In this method, attackers walk through areas carrying Wi-Fi-enabled laptops equipped with wireless discovery tools to identify open networks.
- **WarChalking**: Attackers mark public spaces with symbols to indicate the presence of open Wi-Fi networks.
- **WarFlying**: Drones detect and map open wireless networks from the air.
- **WarDriving**: Attackers drive around in vehicles equipped with Wi-Fi-enabled laptops and wireless discovery tools to scan for open networks.

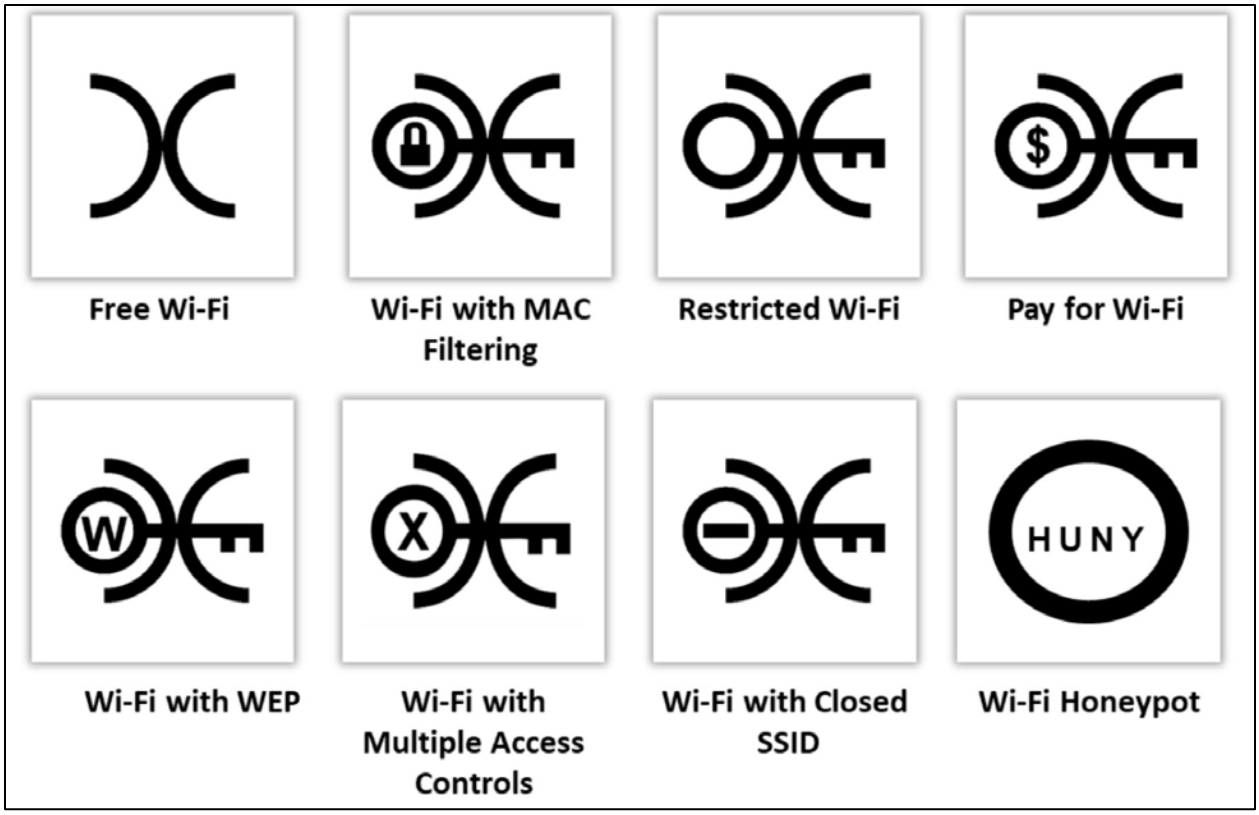


Figure 16-24: Wi-Fi Chalking Symbols

To identify Wi-Fi networks as potential targets for attacks, attackers utilize the following equipment and tools:

- A laptop equipped with a Wi-Fi card
- An external Wi-Fi antenna
- Network discovery software

Commonly used tools for detecting Wi-Fi networks within the range include inSSIDer, NetSurveyor, Wi-Fi Scanner, and Acrylic WiFi Heatmaps.

Wi-Fi Discovery Tools

inSSIDer

inSSIDer is a Wi-Fi troubleshooting and optimization tool that scans for wireless networks using the user's Wi-Fi adapter. It provides a visual representation of signal strengths, the channels each network operates on, and detailed information about the networks. Attackers often use inSSIDer to locate nearby Wi-Fi access points and devices.

Features:

- Analyzes WLANs and nearby networks to identify competing APs
- Monitors signal strength in dBm over time and filters APs based on specific criteria
- Highlights areas with a high concentration of Wi-Fi access points
- Exports Wi-Fi and GPS data as a KML file for visualization in Google Earth

- Displays overlapping Wi-Fi channels

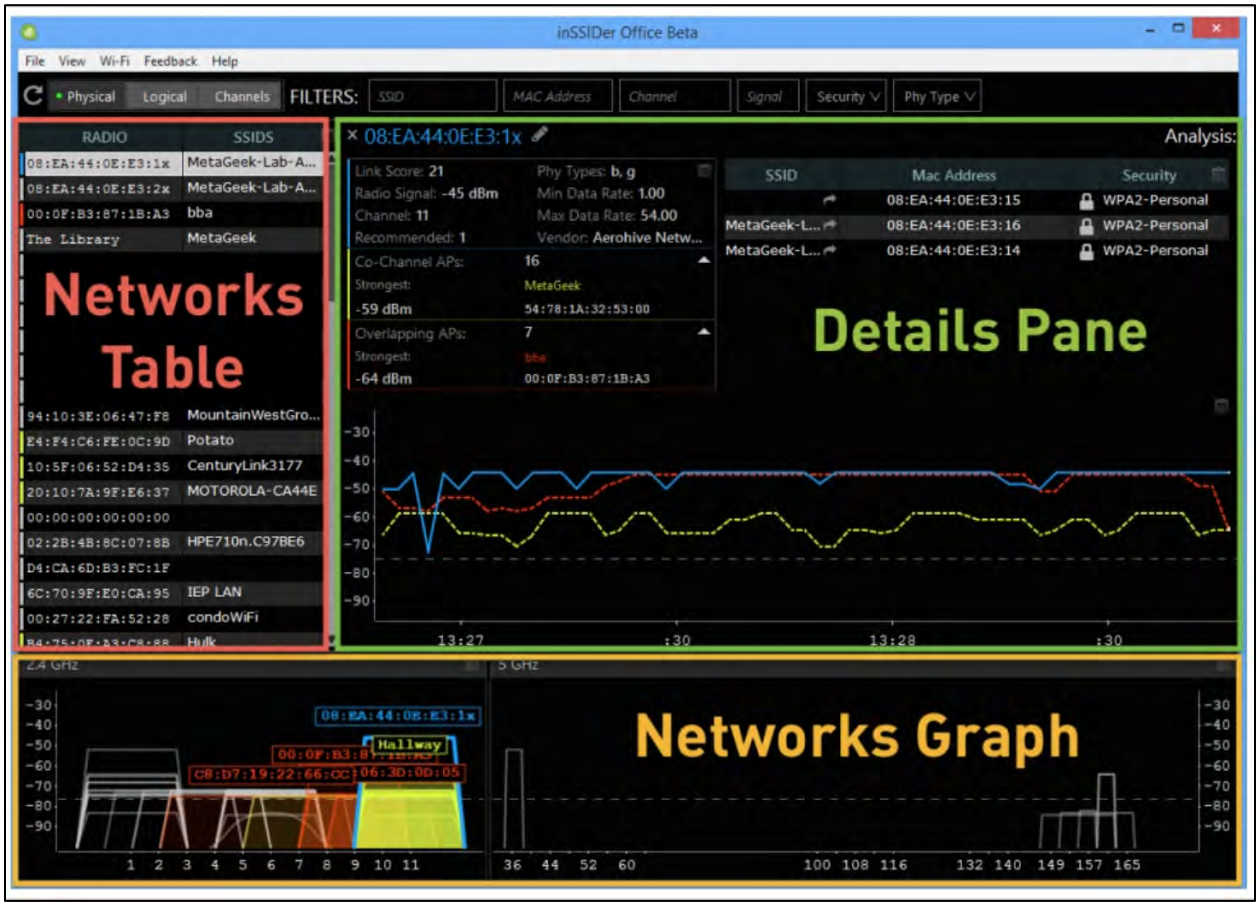


Figure 16-25: inSSIDer

Sparrow-WiFi

Sparrow-WiFi is a Graphical User Interface (GUI) based tool for comprehensive Wi-Fi spectral analysis across 2.4 GHz and 5 GHz frequencies. It enables attackers to integrate software-defined radio devices like HackRF, advanced Bluetooth tools such as Ubertooth, traditional GPS via gpsd, and drone or rover GPS using mavlink protocols. The tool facilitates the discovery of Wi-Fi access points, identification of SSIDs, source tracking, and spectrum analysis. Additionally, it supports importing and exporting data in CSV and JSON formats. It can generate Google Maps visualizations for identified devices.

Figure 16-26: Sparrow-WiFi

The following are some of the additional Wi-Fi discovery tools:

- Wi-Fi Scanner (https://lizardsystems.com)
- Acrylic WiFi Heatmaps (https://www.acrylicwifi.com)
- WirelessMon (https://www.passmark.com)
- Ekahau Wi-Fi Heatmaps (https://www.ekahau.com)
- NetSpot (https://www.netspotapp.com)
- AirMagnet® Survey PRO (https://www.netally.com)

Mobile-based Wi-Fi Discovery Tools

WiFi Analyzer

WiFi Analyzer is a tool designed to optimize Wi-Fi networks by analyzing nearby networks, assessing signal strengths, and identifying congested channels. Attackers utilize WiFi Analyzer to locate nearby Access Points (APs), visualize channel signal strengths through graphs, estimate distances to APs, and more.

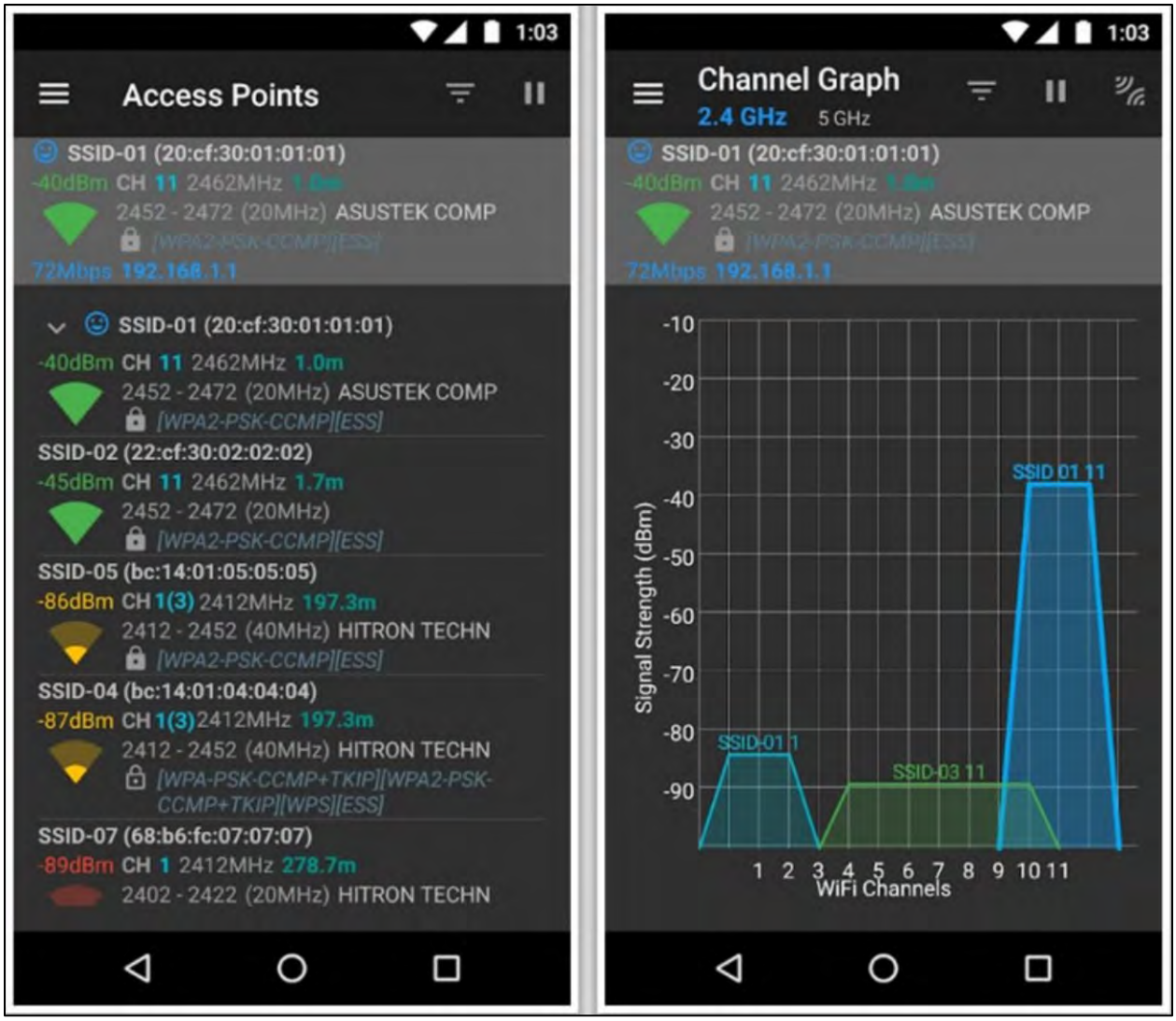


Figure 16-27: WiFi Analyzer

The following are some of the additional mobile-based Wi-Fi discovery tools:

- Opensignal (https://opensignal.com)
- Network Signal Info Pro (https://www.kaibits-software.com)
- Net Signal Pro:WiFi & 5G Meter (https://play.google.com)
- NetSpot WiFi Analyzer (https://apps.apple.com)
- WiFiman (https://play.google.com)

Finding WPS-Enabled Aps

Attackers utilize the Wash command-line tool to detect WPS-enabled Access Points (APs) within a target wireless network and verify whether the AP is locked. Typically, WPS-enabled routers become locked after more than five consecutive incorrect credential attempts and can only be unlocked manually through the router's administrator interface. The Wash command is compatible with the 5 GHz channel and can be installed using the Reaver package.

Below are some key arguments of the Wash command frequently used by attackers:

Commands	Description
-i, --interface=<iface>	specifies the interface to capture packets
-a, --all	displays all access points, including those with WPS disabled
-f, --file [FILE1 FILE2 FILE3 ...]	reads packets from captured files
-c, --channel=<num>	specifies the channel to listen [auto]
-o, --out-file=<file>	writes data to a file
-n, --probes=<num>	specifies the maximum number of probes to send to each AP in the scan mode
-D, --daemonize	Wash command
-5, --5ghz	command to use 5 GHz 802.11 channels
-s, --scan	command to run in the scan mode
-u, --survey	command to use the survey mode [default]

Table 16-07: Commands Description

Attackers execute the following command to identify the access point, Extended Service Set Identifier (ESSID), and BSSID of a device or router:

```
# sudo wash -i wlano
```

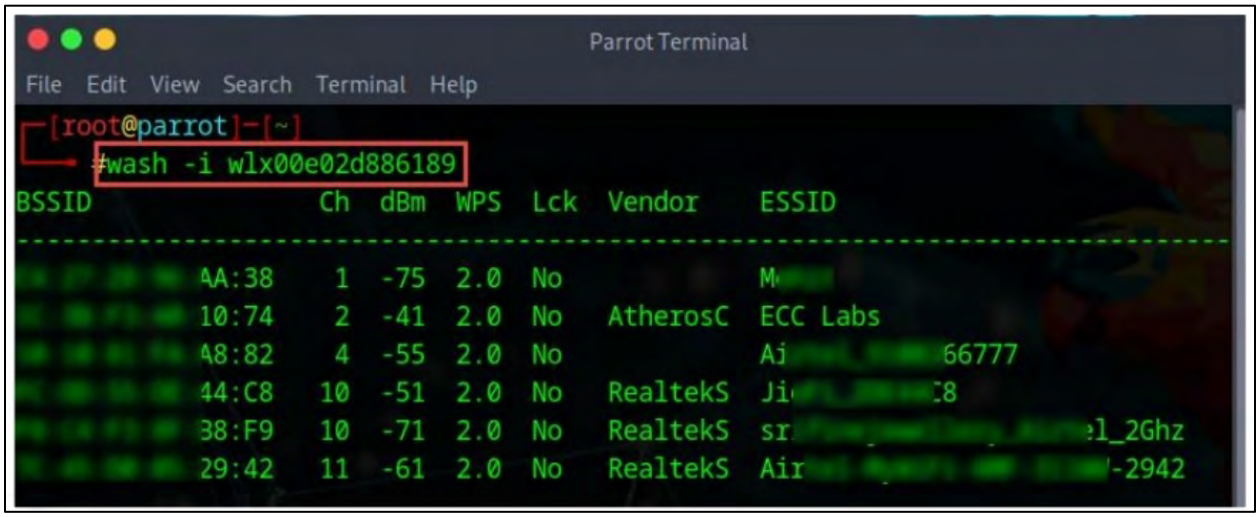


Figure 16-28: Output of the Wash Command

Wireless Traffic Analysis

The next phase in the wireless hacking process involves analyzing the traffic of the identified wireless network. Before carrying out any actual attacks, an attacker conducts a traffic analysis to assess the vulnerabilities and potential targets within the network and devise an effective attack strategy. The attacker employs a range of tools and methods to analyze the traffic of the target wireless network.

Wi-Fi protocols operate at layer 2, and because the traffic transmitted over the air is not serialized, it is relatively simple to intercept and examine wireless packets. Attackers analyze a wireless

network to gather information such as the broadcasted SSID, multiple APs, the potential for recovering SSIDs, the authentication method, and the WLAN encryption algorithms. To capture and analyze the traffic of a target wireless network, attackers use Wi-Fi packet sniffing tools like AirMagnetTM G3 Pro, Wireshark, Riverbed Packet Analyzer, OmniPeek, and CommView for Wi-Fi.

Sniffing is a form of eavesdropping where attackers intercept all active wireless communications. To conduct wireless sniffing, attackers tune their receiver to the target transmission frequency and identify the communication protocol. They then analyze the captured traffic to plan further attacks on the target network. Attackers must enable monitor mode on their Wi-Fi card to sniff wireless traffic.

Not all Wi-Fi cards are compatible with monitor mode in Windows. To check if a Wi-Fi card supports monitor mode, use the link: https://secwiki.org/w/Npcap/WiFi_adapters.

Attackers employ various tools to intercept wireless networks, such as Wireshark, Riverbed Packet Analyzer, OmniPeek Network Protocol Analyzer, CommView for Wi-Fi, and Kismet.

- **Wireshark**

Wireshark is a network protocol sniffer and analyzer that enables users to capture and interactively explore traffic within a target network. It can capture live data from various network types, including Ethernet, Token Ring, FDDI, PPP, SLIP, 802.11 wireless LAN, ATM connections (if supported by the ATM's OS), and any device supported by recent versions of libpcap on Linux. For comprehensive WLAN traffic analysis, Wireshark integrates with Npcap, which provides advanced visualization, drill-down capabilities, and reporting.

Attackers can capture wireless traffic by enabling monitor mode in Wireshark. This allows them to intercept various frames, including management, control, and data frames. This helps them analyze Radiotap header fields, which provide valuable information such as the protocols and encryption methods used, frame sizes, and MAC addresses.

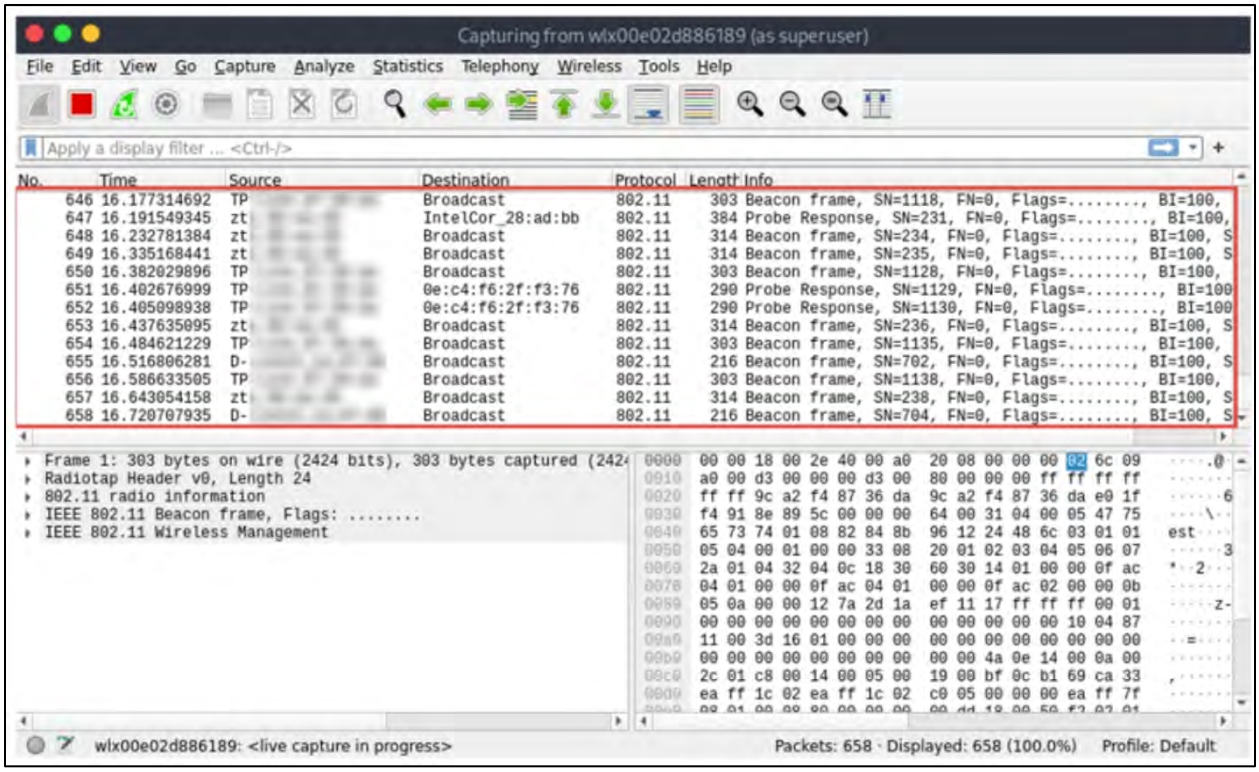


Figure 16-29: Wireshark Capturing Wireless Traffic

- **CommView for Wi-Fi**

CommView for Wi-Fi is a monitoring and analysis tool for 802.11 a/b/g/n networks. It captures wireless packets and provides key details such as lists of Access Points (APs) and stations, statistics for each node and channel, signal strength, packet and network connection information, and charts showing protocol distribution.

Users can decrypt packets using custom WPA-PSK keys and analyze them to the most basic layer. This network analyzer provides a detailed view of each captured packet, organizing the protocol layers and packet headers in an easy-to-understand tree-like structure.

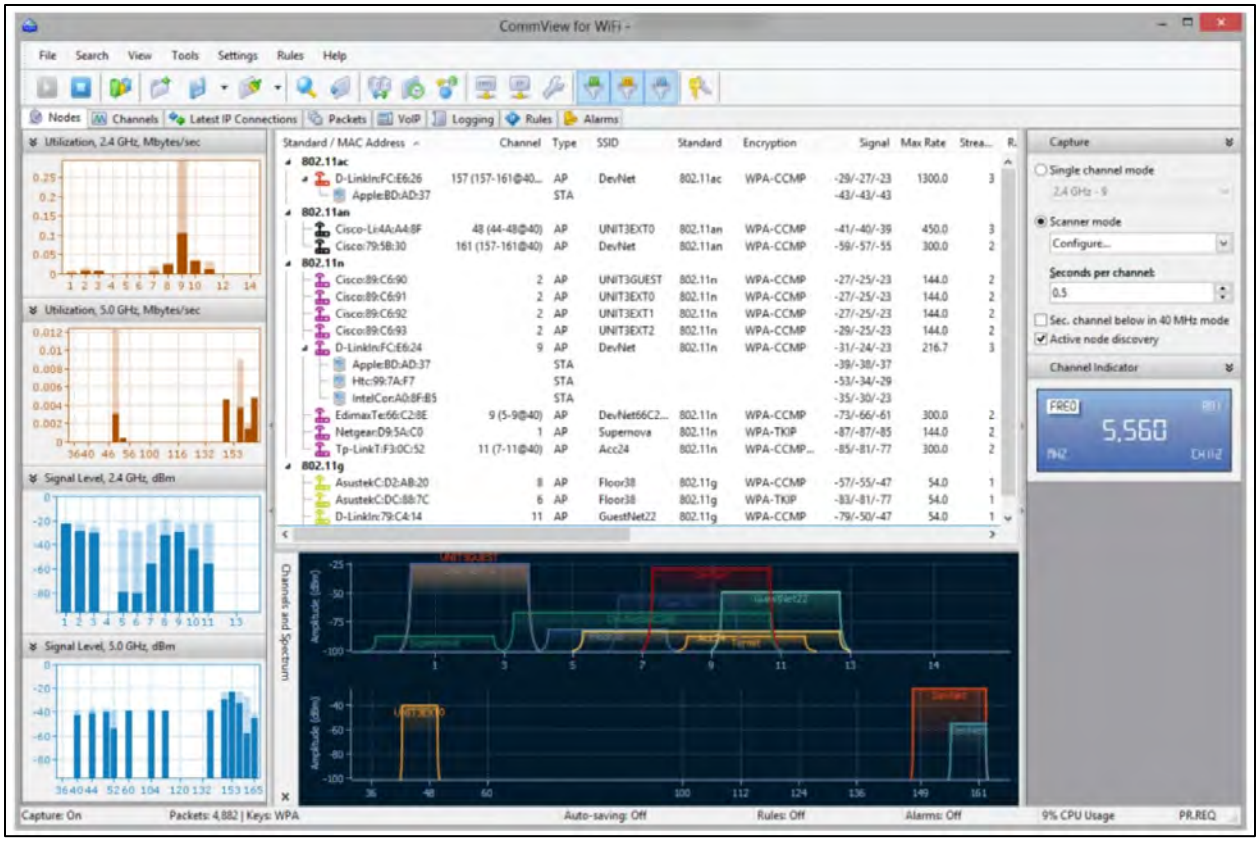


Figure 16-30: CommView for Wi-Fi

The following are some additional Wi-Fi Packet Sniffers:

- Omnipeek® Network Protocol Analyzer (https://www.liveaction.com)
- Kismet (https://www.kismetwireless.net)
- SolarWinds Network Performance Monitor (https://www.solarwinds.com)
- Acrylic Wi-Fi Analyzer (https://www.acrylicwifi.com)
- airgeddon (https://github.com)

Choosing the Optimal Wi-Fi Card

Selecting the right Wi-Fi card for Wi-Fi hacking involves choosing hardware that supports the necessary features for the task. This decision is crucial for attackers because tools like Aircrack-ng and NetSpot only work with specific wireless chipsets. When selecting the optimal Wi-Fi card, an attacker takes the following factors into account:

- **Understand the Wi-Fi requirements**: An attacker may need to either listen to wireless traffic or both listen to and inject packets. Windows systems can capture network traffic but not inject data packets, while Linux systems can perform both tasks. The attacker selects the Operating System (OS), hardware type (such as PCMCIA or USB), and capabilities like listening, injection, or both based on these needs.
- **Understand the capabilities of a wireless card**: Two key manufacturers to consider for Wi-Fi cards are the card brand and the chipset manufacturer. Knowing the brand and model alone

is not enough; understanding the chipset is essential. Though often not disclosed by card manufacturers, this information helps the attacker determine the supported OS, necessary drivers, and any limitations.

- **Identify the chipset of the Wi-Fi card**: An attacker can determine the chipset of a Wi-Fi card using several methods:
  - Searching online
  - Checking Windows driver filenames, which often indicate the chipset
  - Visiting the manufacturer's website
  - Examining the wireless chip on some cards, where the chipset number may be visible
  - Using the FCC ID Search to find detailed device information if the board includes an FCC ID number. Manufacturers may change the chipset while keeping the model number, sometimes labeling it as a "card revision" or "card version". This means the attacker must also check the version or revision. Compatibility information may be available at https://wireless.wiki.kernel.org/en/users/Drivers.
- **Verify the chipset capabilities**: Before finalizing the Wi-Fi card choice, the attacker must ensure that the chipset is compatible with the OS and meets all requirements.
- **Identify the required drivers and patches**: The attacker must determine which drivers are needed for the chipset and whether any OS patches are required.

Once these considerations are made, the attacker selects a Wi-Fi card that uses the desired chipset by referencing a compatible card list.

Perform Spectrum Analysis

Attackers can use spectrum analyzers to detect the presence of wireless networks. By analyzing the spectrum of wireless networks, an attacker can actively monitor spectrum usage in a specific area and identify the signal of the target network. This process also allows the attacker to measure the power of known and unknown signals. Spectrum analyzers use statistical methods to map spectrum usage, assess "air quality," and locate transmission sources. RF technicians utilize RF spectrum analyzers for the installation and maintenance of wireless networks, as well as to identify interference sources. Wi-Fi spectrum analysis is also valuable for detecting wireless attacks, such as DoS attacks, authentication/encryption attacks, and network penetration attacks.

Below are some automated tools attackers use to analyze a target wireless network spectrum.

RF Explorer

RF Explorer is a tool designed for RF spectrum analysis. It can function as a standalone, handheld RF spectrum analyzer or connect to a PC for more advanced data analysis. RF spectrum analyzers are essential for the initial detection and identification of RF interference sources and for monitoring a wireless system's overall health. RF Explorer is a basic tool that allows users to observe transmitted RF signals, visually representing the local RF environment. This view can assist in detecting the presence of RF transmissions that may be sources of interference.

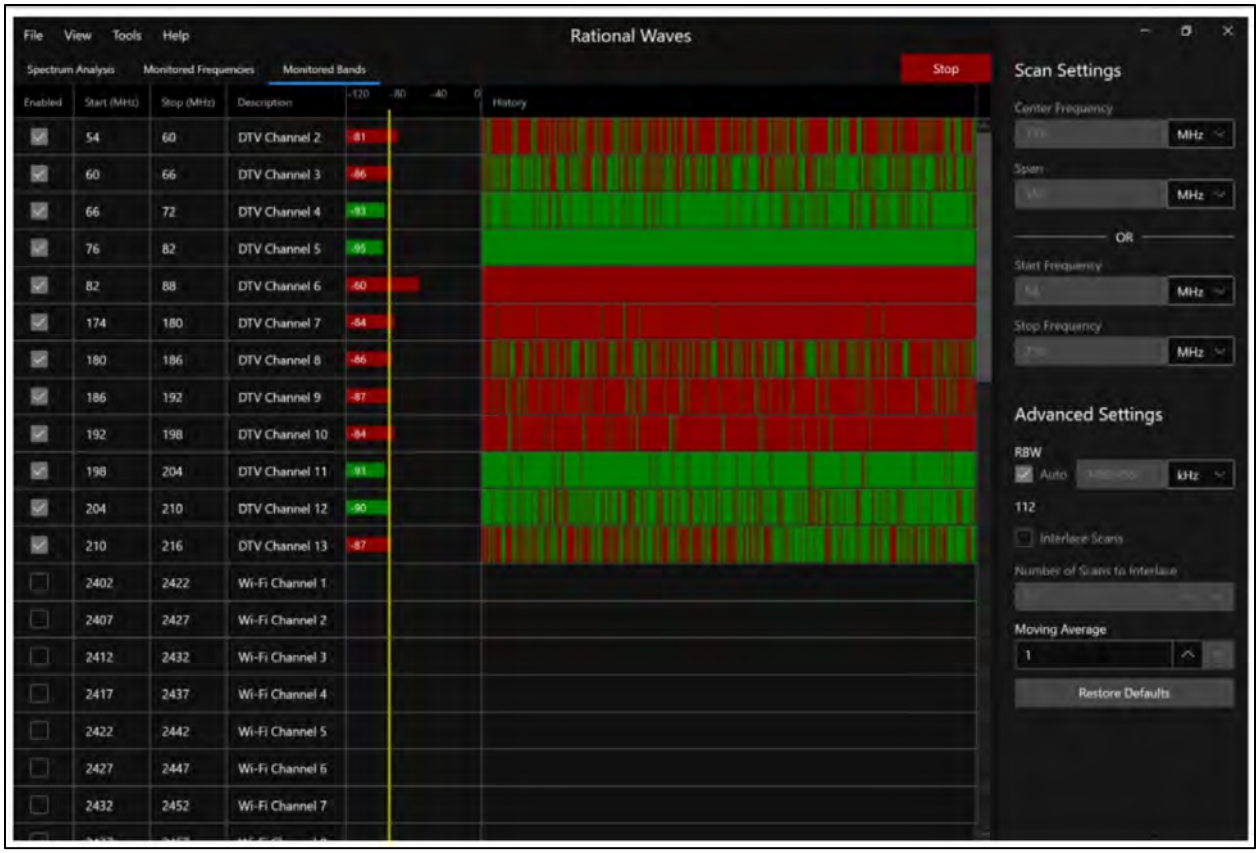


Figure 16-31: RF Explorer

The following are some RF monitoring and spectrum analyzing tools.

- Chanalyzer (https://www.metageek.com)
- AirCheck G3 Pro (https://www.netally.com)
- Spectraware S1000 (https://thinkrf.com)
- RSA306B USB Spectrum Analyzer (https://www.tek.com)
- RF Explorer 6G (https://j3.rf-explorer.com)
- RFXpert (https://www.dektec.com)
- Monics® 200 (https://www.kratosdefense.com)
- Monics® satID® (https://www.kratosdefense.com)
- Signal Hound (https://signalhound.com)
- FieldSENSE (https://www.fieldsense.com)

Launch of Wireless Attacks

Once the wireless network discovery, mapping, and analysis of the target network are complete, an attacker is ready to initiate an attack on the target wireless network. The attacker may carry out different attacks, including fragmentation attacks, MAC spoofing, DoS attacks, and ARP poisoning attacks. This section outlines the various wireless attacks and explains how they are executed.

Aircrack-ng Suite

Aircrack-ng is a network software suite for 802.11 wireless network detection, packet sniffing, and analysis. It includes tools for cracking WEP and WPA PSK (WPA 1 and 2) encryption and works on both Linux and Windows operating systems.

- **Airbase-ng**: Captures WPA/WPA2 handshakes and can be an ad-hoc Access Point (AP)
- **Aircrack-ng**: The primary tool for cracking WEP and WPA/WPA2 PSK encryption keys
- **Airdecap-ng**: Decrypts WEP/WPA/WPA2 encryption and removes wireless headers from Wi-Fi packets
- **Airdrop-ng**: Targets users for rule-based de-authentication
- **Aireplay-ng**: Effective for collecting Initialization Vectors (WEP IVs) and WPA handshakes for use with Aircrack-ng in further analysis and security testing
- **Airgraph-ng**: Creates a client-AP relationship and probe graph from an airodump file
- **Airmon-ng**: Switches wireless interfaces between managed mode and monitor mode
- **Airodump-ng**: Captures raw 802.11 frames and collects WEP IVs
- **Airolib-ng**: Manages and stores ESSID and password lists for WPA/WPA2 cracking
- **Airtun-ng**: Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network

Detection of Hidden SSIDs

Following the principle of security through obscurity, many organizations hide the SSID of their wireless networks to prevent it from being broadcast. This is a common security measure, as attackers might exploit the SSID to compromise the network. However, hiding the SSID does not enhance security. An attacker can uncover a hidden SSID using tools like the Aircrack-ng suite and mdk3 by following these steps:

- Start by running **airmon-ng** in monitor mode with the command:

```
airmon-ng start <Wireless interface>
```

If any processes interfere, use the following command to resolve the issue.

```
airmon-ng check kill
```

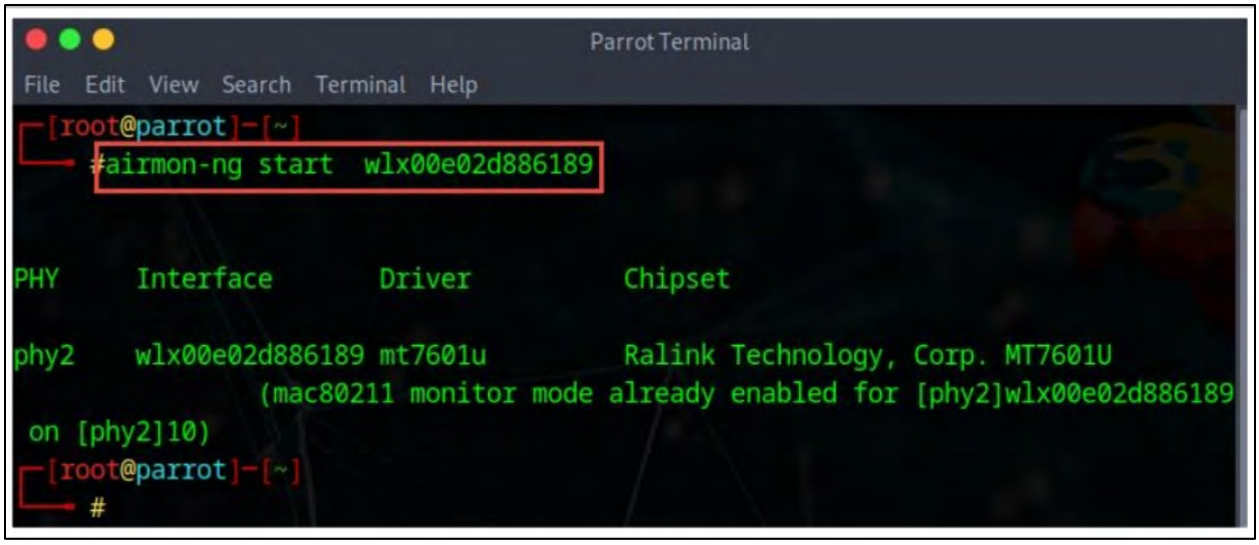


Figure 16-32: Execution of airmon-ng start

- Run **airodump-ng** to identify SSIDs on the interface.

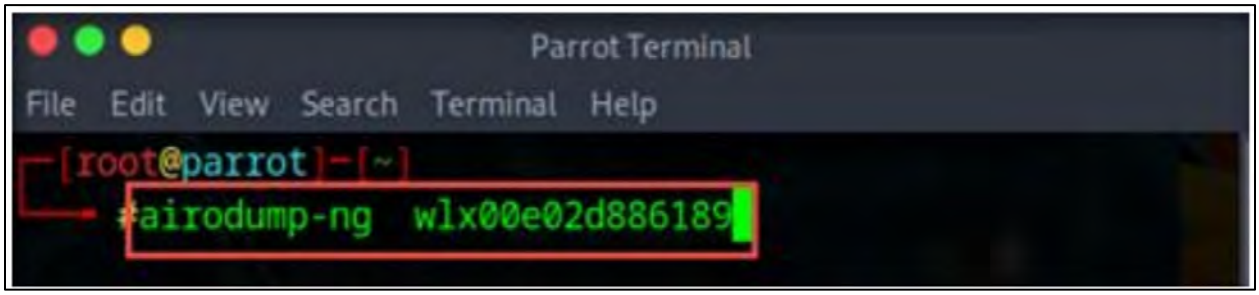


Figure 16-33: Execution of airodump-ng start

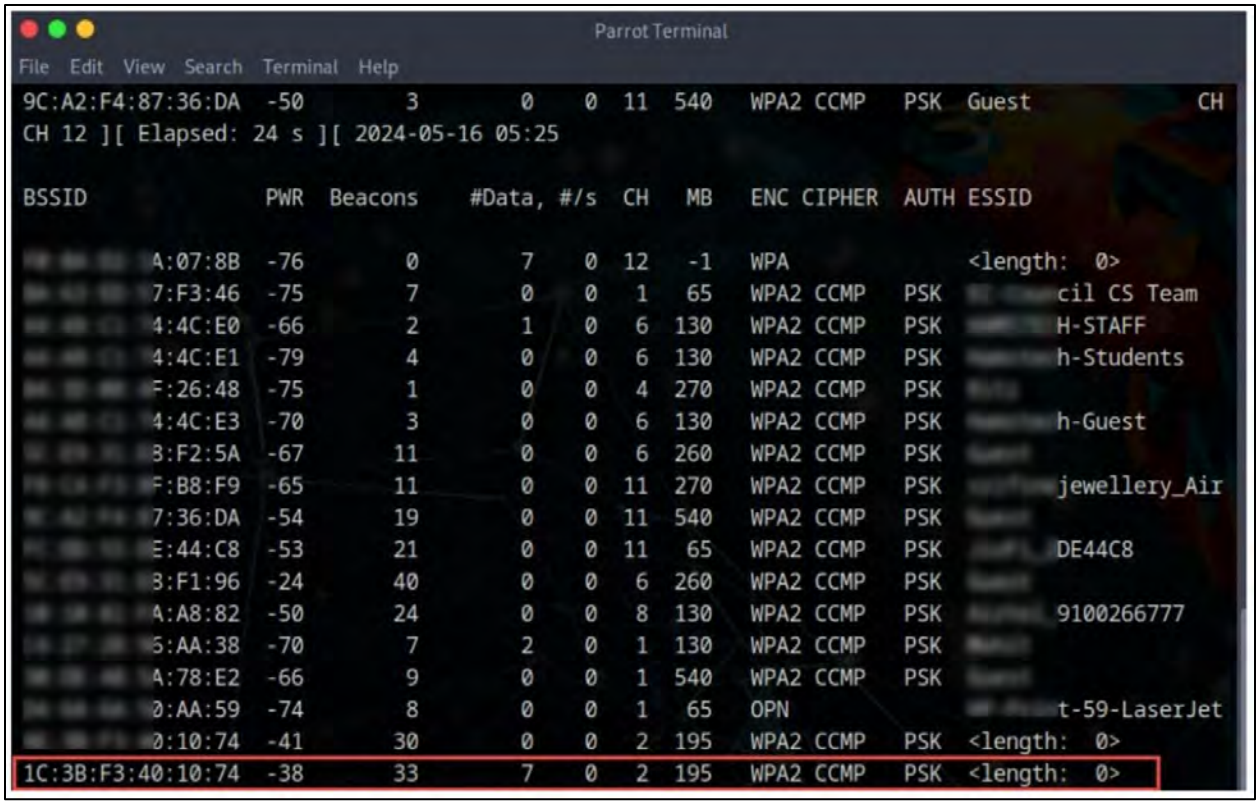


Figure 16-34: Execution of airodump-ng

The SSID of the targeted access point is concealed, as shown in Figure 16-34.

- Open a new terminal as root and execute the command **mdk3 <Wireless Interface> p -b 1 -c <Channel> -t <Target BSSID>** to perform a brute-force attack and uncover the hidden SSID.

Commands	Description
P	Enables basic probing and ESSID brute-force mode
-b	Activates beacon flood mode
1	Conducts an EAPOL logoff test
-c	Specifies the channel (in this case, 2)
-t	Indicates the target BSSID (for example, 1C:3B:F3:40:10:74)
wlx00e02d886189	Denotes the wireless interface

Table 16-08: Commands Description

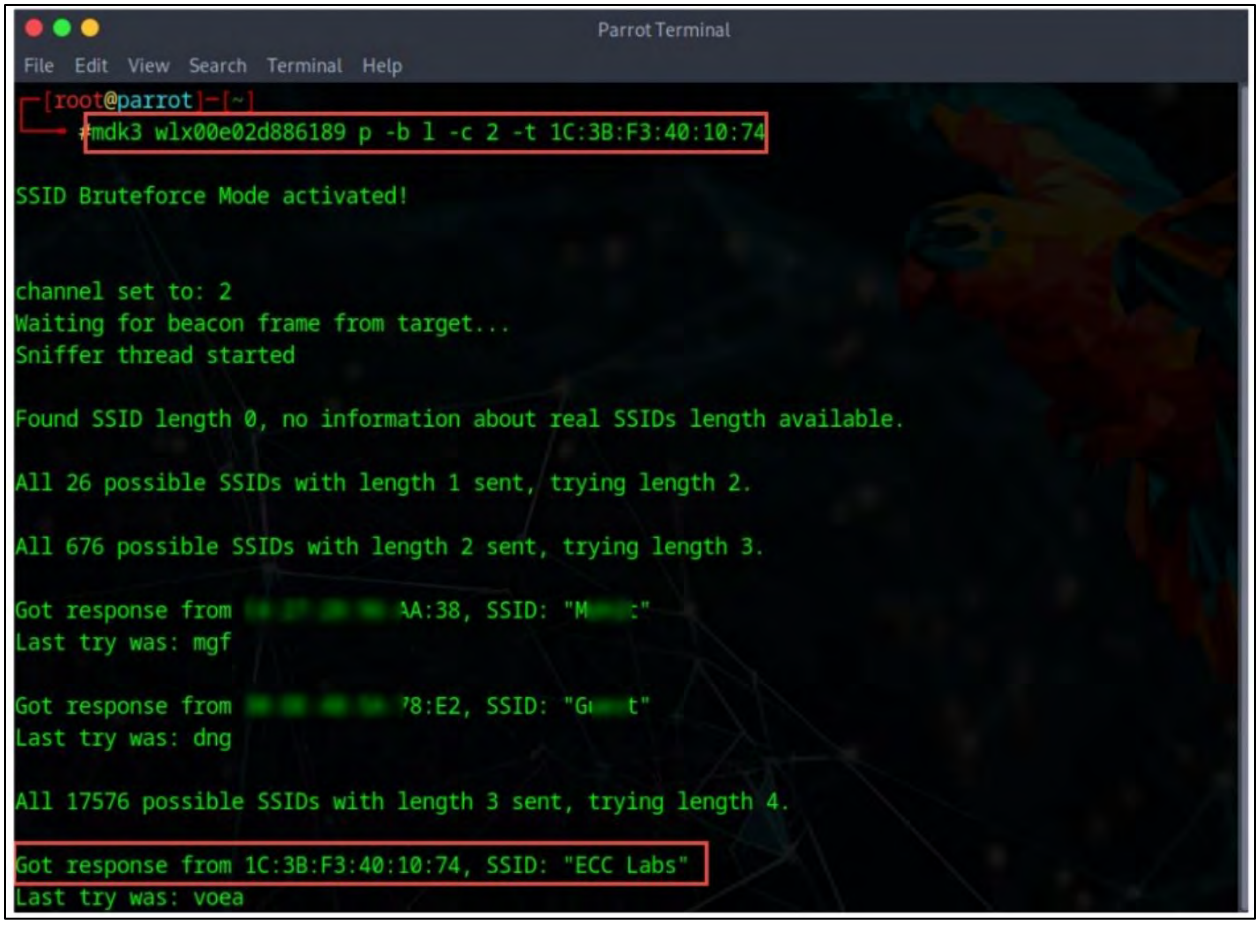


Figure 16-35: mdk3 Displaying Result in Revealing SSID

Denial-of-Service

Wireless networks are susceptible to DoS attacks due to the interdependencies between the physical, data link, and network layers. These networks operate in unlicensed frequency bands, transmitting data via radio signals. While the MAC protocol was designed for simplicity, it leaves the network vulnerable to DoS attacks. WLANs often support essential applications like VoIP, database access, project files, and internet connectivity. Disrupting these applications through a DoS attack can easily cause network downtime or a loss of productivity.

Wireless DoS attacks typically work by broadcasting de-authentication commands, forcing clients to disconnect from the access point.

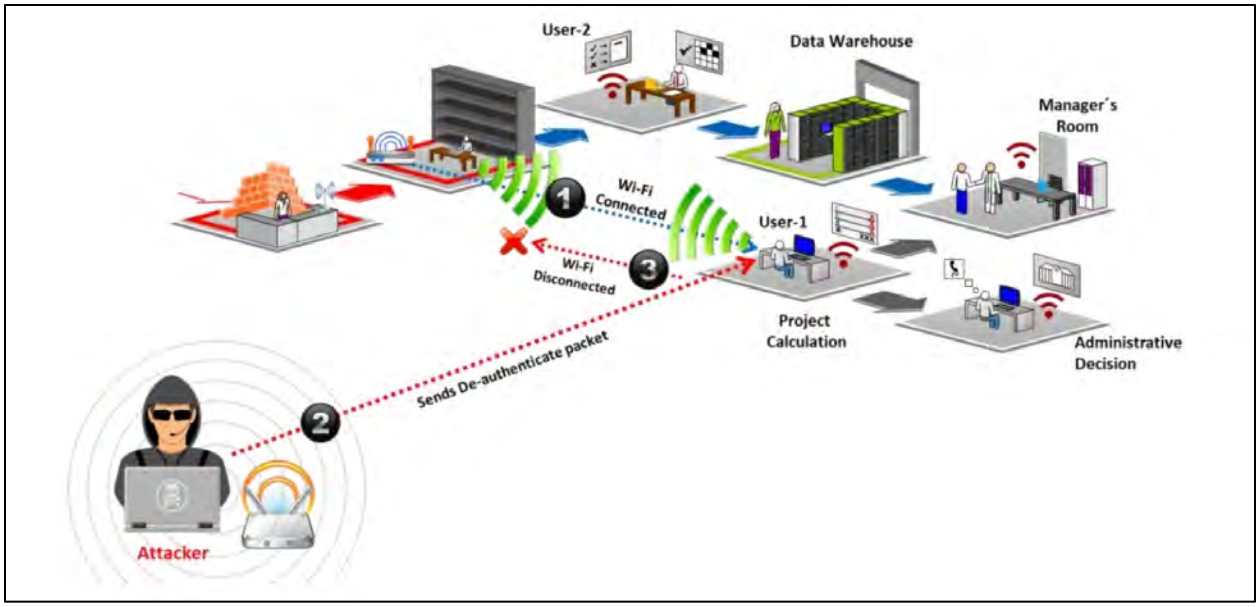


Figure 16-36: DoS Attack

Wireless DoS attacks comprise disassociation and de-authentication attacks.

- **Disassociation Attack**: In this attack, the attacker disrupts the connection between the access point and the client, rendering the victim unable to communicate with other wireless devices

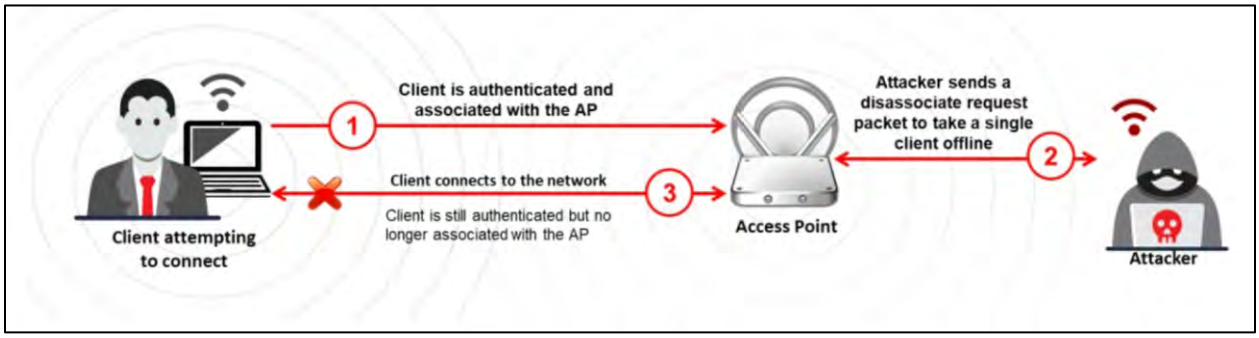


Figure 16-37: Disassociation Attack

- **De-authentication Attack**: This attack involves the attacker sending forged de-authentication or disassociation messages to stations, causing them to disconnect from the access point

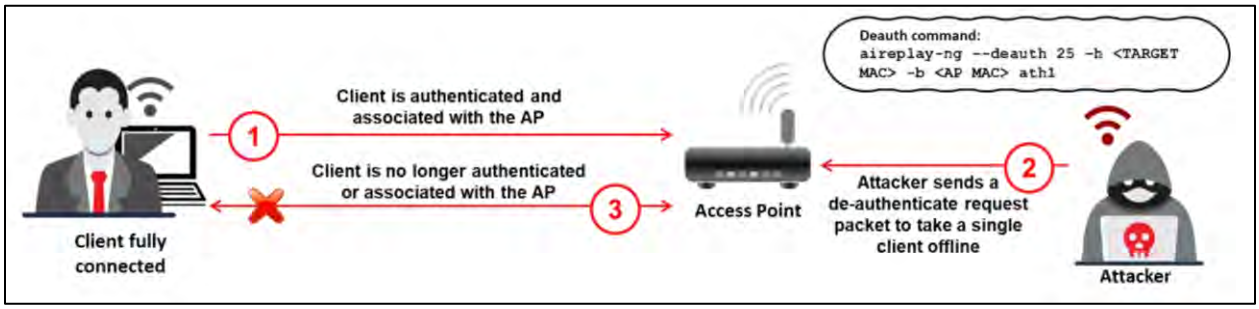


Figure 16-38: De-authentication Attack

Man-in-the-Middle Attack

A Man-In-The-Middle (MITM) attack is an active cyber-attack where the attacker intercepts, reads, or manipulates the communication between two computers. MITM attacks can affect both 802.11 WLANs and wired communication systems.

- **Eavesdropping**

Eavesdropping is relatively easy in wireless networks since no physical medium is required for communication. An attacker within range of the network can effortlessly capture radio waves transmitted over the network. Additionally, the attacker can analyze or save the entire data frame for later review.

To protect against this, multiple encryption layers should be applied. WEP or data link encryption can be used at one layer, while additional security protocols like IPsec, SSH, or SSL must be employed. Without these, the transmitted data may be exposed to attackers. However, as highlighted earlier, online tools can crack WEP encryption. Accessing emails through protocols like POP or IMAP is particularly vulnerable, as these protocols may transmit email data over a wireless network without additional encryption. A skilled hacker could log large amounts of WEP-encrypted traffic, later analyze it, and break the encryption.

- **Manipulation**: This goes a step further than eavesdropping. It happens when an attacker intercepts the victim's encrypted data, alters it, and returns the modified data to the victim. Additionally, the attacker can capture encrypted data packets and modify the destination address, redirecting these packets across the internet. In an MITM attack, the attacker follows these steps:
    - The attacker observes and gathers the victim's wireless parameters, such as the MAC address, ESSID/BSSID, and the number of channels in use

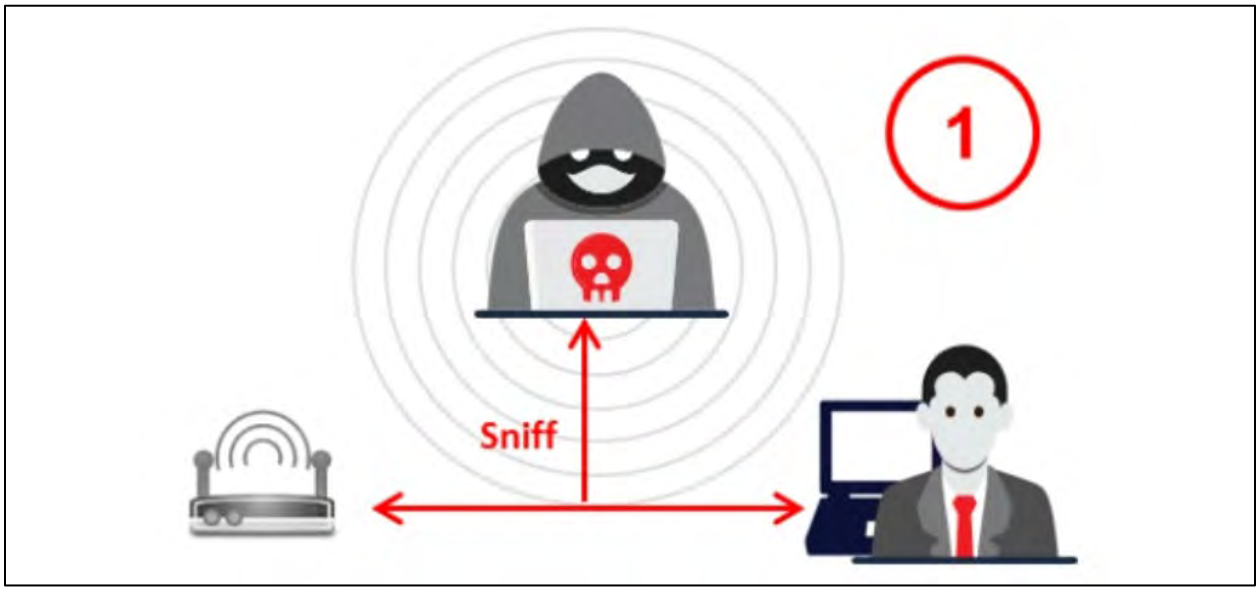


Figure 16-39: Sniffing of the Victim's Wireless Parameters

- The attacker sends a DEAUTH request to the victim, spoofing the source address to appear as the victim's AP

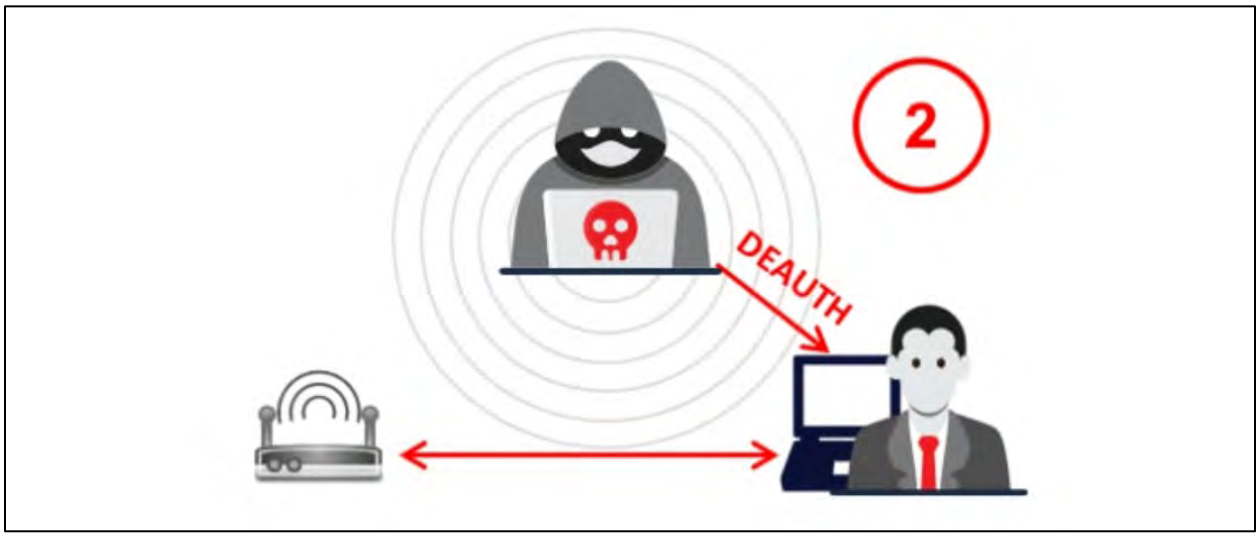


Figure 16-40: Sending a DEAUTH Request

- Upon receiving this request, the victim's device becomes de-authenticated, and all channels are searched for a new valid AP

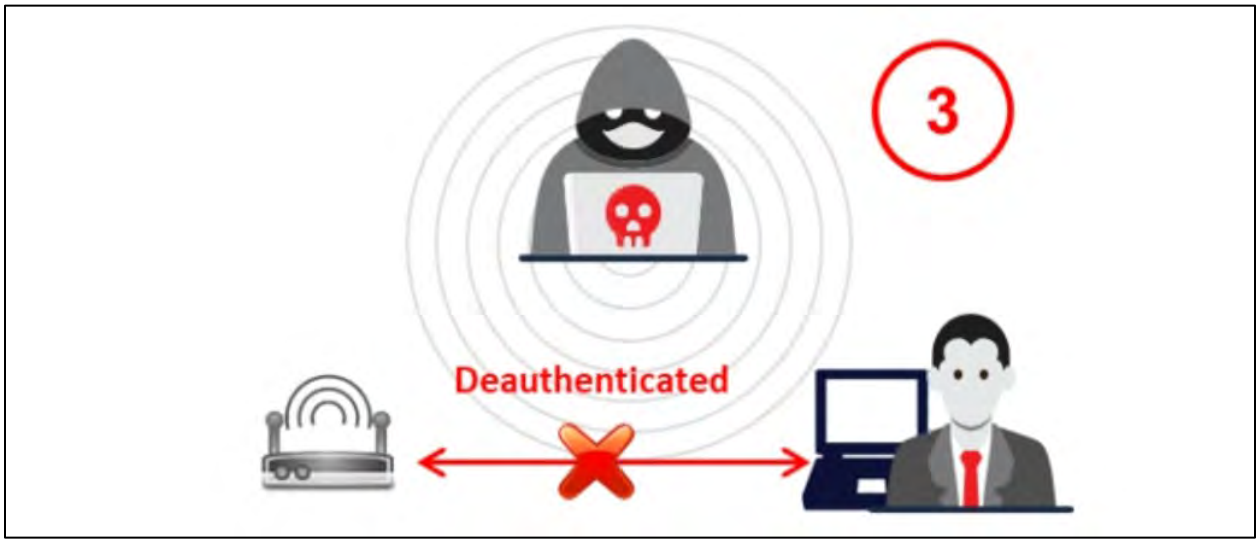


Figure 16-41: De-authentication of the Victim's Computer

- The attacker then creates a fake AP on a different channel, using the original MAC address (BSSID) and ESSID of the victim's AP, causing the victim to connect to the forged AP
- Once the victim connects to the fake AP, the attacker impersonates the victim to force a

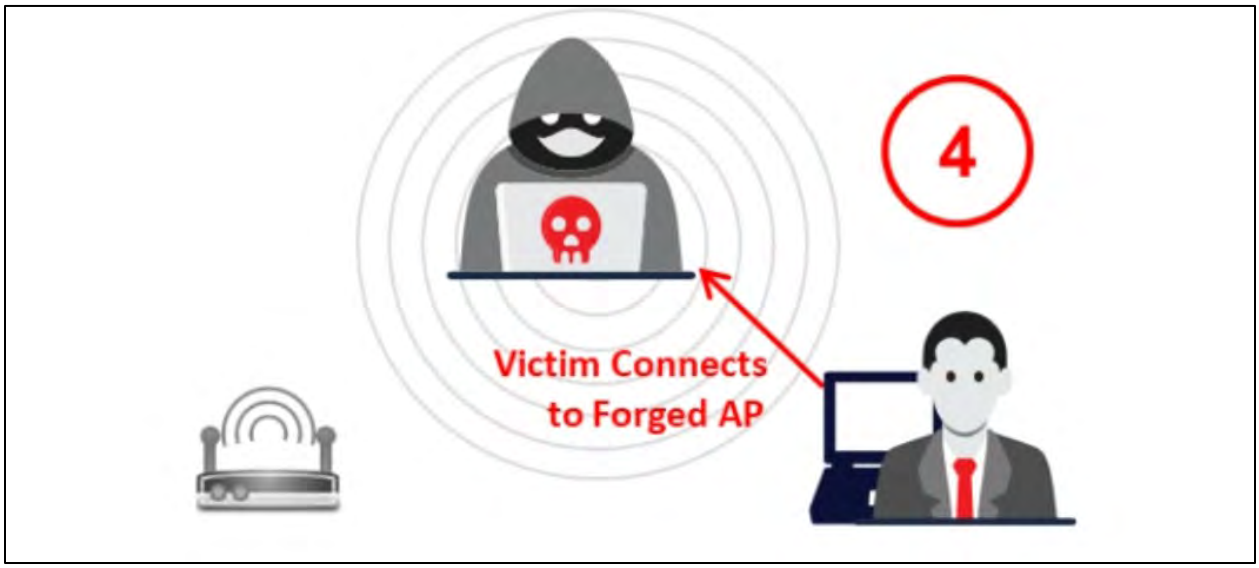


Figure 42: Connection of the Victim to the Forged AP

connection to the real AP

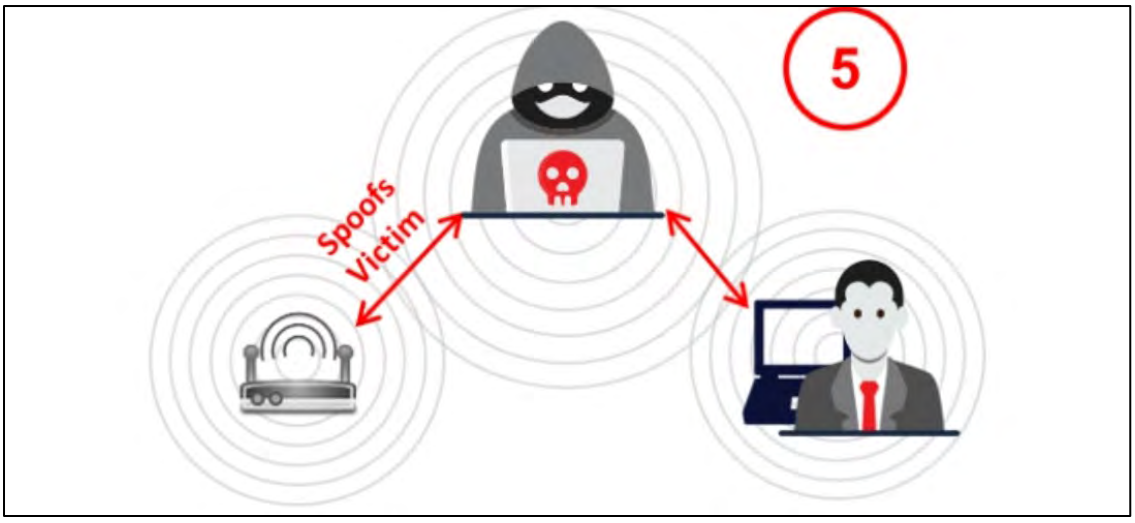


Figure 16-43: Spoofing the Victim

- The attacker then places themselves between the victim and the AP, intercepting all network traffic

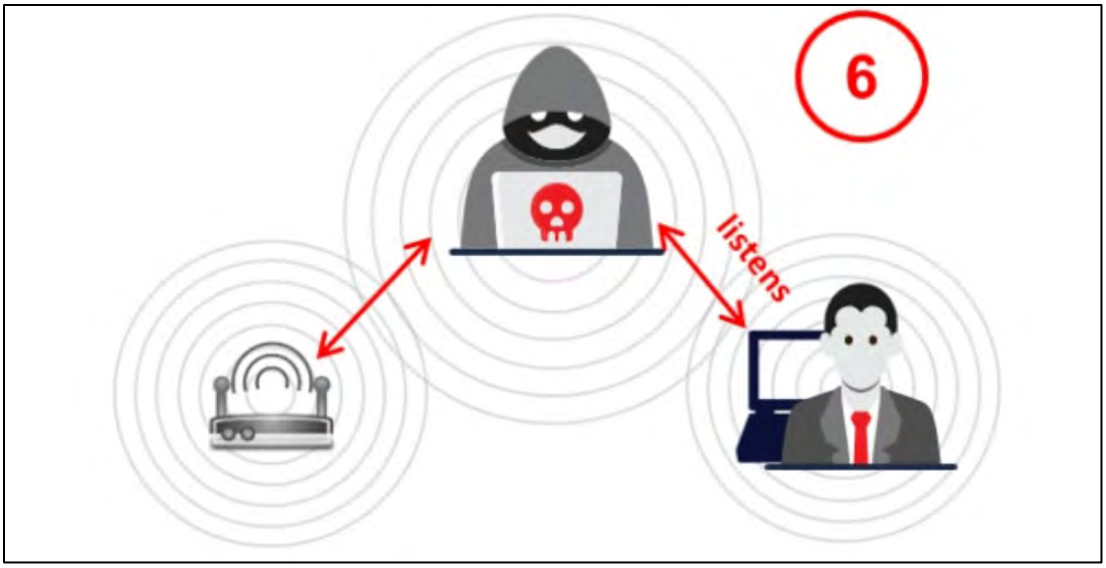


Figure 16-44: Listening to all the Traffic

MITM Attack Using Aircrack-ng

An attacker can execute an MITM attack using aircrack-ng by following these steps:

- Activate monitor mode with airmon-ng
- Use airodump to identify SSIDs on the interface

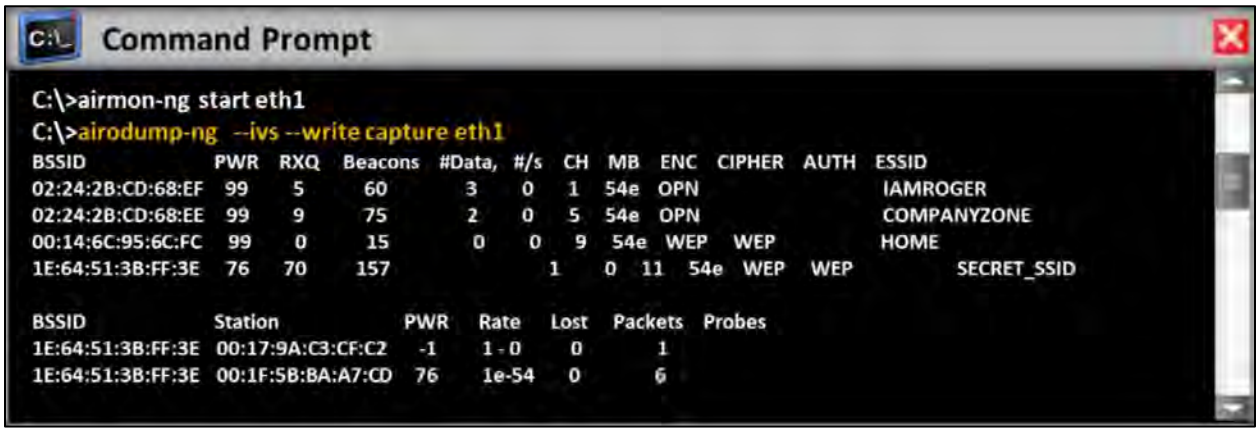


Figure 16-45: Execution of airmon-ng

- De-authenticate the client with aireplay-ng

Figure 16-46: Command to Launch aireplay-ng

- Perform a fake association with the target AP using aireplay-ng

Figure 16-47: Displaying the Result of Association

MAC Spoofing Attack

AP MAC Spoofing

In wireless networks, Access Points (APs) broadcast probe responses through beacons to signal their presence and availability. These responses include the AP's MAC address and the SSID of the network it supports. Nearby clients use this information to connect to the network. Various software tools and APs enable users to configure custom MAC addresses and SSIDs for AP devices.

AP MAC spoofing is a method where attackers mimic a legitimate wireless Access Point (AP) by altering their device's MAC address to match that of the trusted AP. The attacker begins by identifying the MAC address of the authentic AP, usually by monitoring network traffic or using a scanning tool. The attacker then configures their rogue access point to use the same MAC address, typically the same SSID as the legitimate AP. To force users off the legitimate AP, attackers may send deauthentication packets, causing users' devices to reconnect to the nearest AP, which is often the rogue AP. Once users connect to the rogue AP, attackers can intercept, modify, or redirect network traffic, allowing them to capture sensitive data or launch additional attacks.

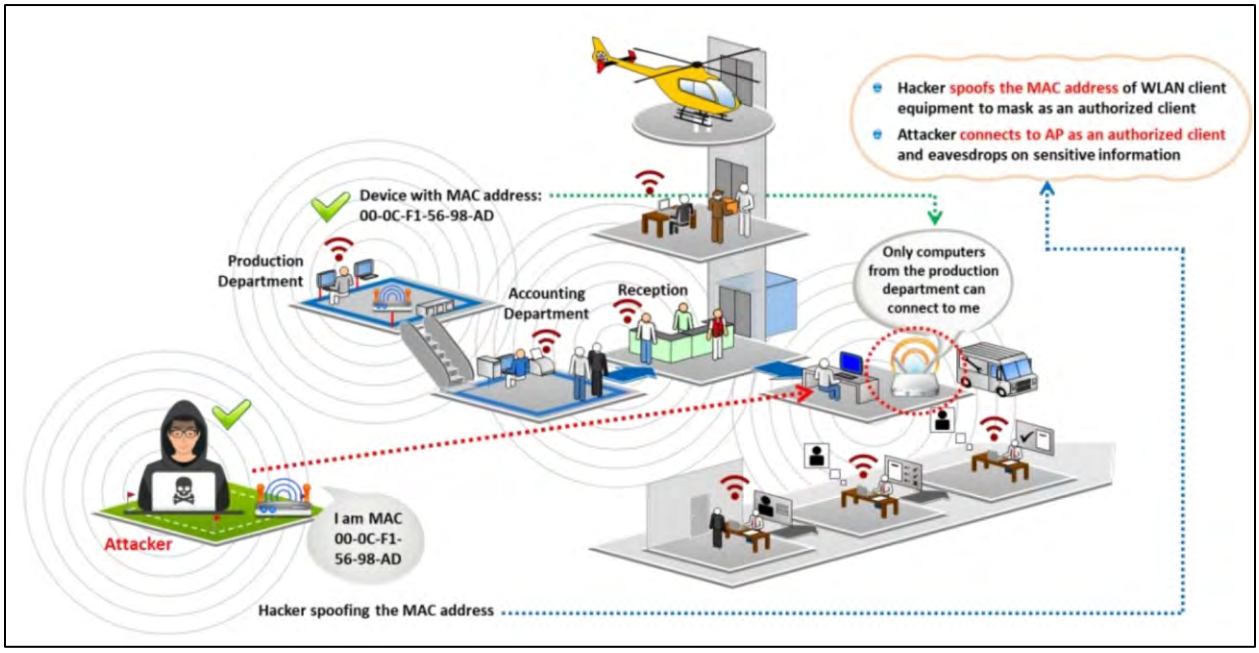


Figure 16-48: AP MAC Spoofing

MAC Spoofing Attack

A MAC address is a unique identifier embedded in a network card's circuitry by its manufacturer. Some networks use MAC address filtering as a security measure. In a MAC spoofing attack, an attacker alters their MAC address to match an authorized user's to bypass the MAC filtering set up on an Access Point (AP). To perform MAC spoofing, the attacker modifies the MAC address by changing the value returned by the ifconfig command to a different hexadecimal value, such as aa:bb:cc:dd:ee:ff. This modification is typically done using the sudo command, which requires root access. Attackers can also utilize tools like Technitium MAC Address Changer or LizardSystems Change MAC Address to spoof the MAC address.

Figure 16-49: MAC Address Spoofing in Linux and Windows

MAC Spoofing Tools

- **Technitium MAC Address Changer**

Technitium MAC Address Changer is a tool that enables users to quickly change (spoof) the MAC address of their Network Interface Card (NIC). It features an easy-to-use interface and displays detailed information about each NIC on the system. Windows drivers utilize the MAC address to connect to Ethernet LANs.

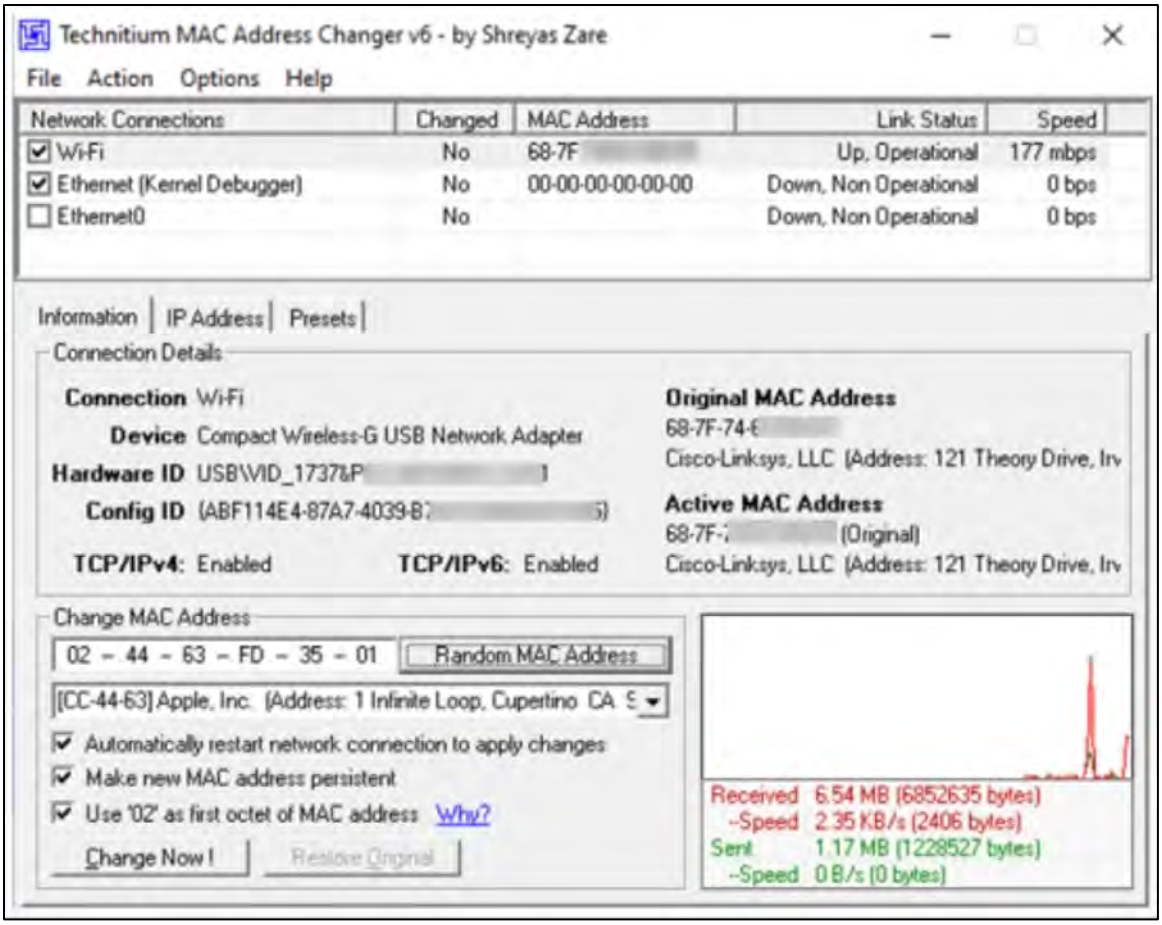


Figure 16-50: Technitium MAC Address Changer

Wireless ARP Poisoning Attack

ARP is responsible for resolving the MAC address of an Access Point (AP) when it knows the corresponding IP address. However, ARP lacks a mechanism to verify the authenticity of the responses it receives. ARP poisoning takes advantage of this vulnerability. In this attack, the operating system's ARP cache is polluted with incorrect MAC addresses. The attacker accomplishes this by sending an ARP reply packet containing a false MAC address.

An ARP poisoning attack affects all devices within a subnet. Since most Access Points (APs) function as transparent MAC-layer bridges, every device connected to a subnet targeted by ARP poisoning is at risk. Devices connected to a switch or hub are also vulnerable if the AP is directly linked to the switch or hub without any router or firewall in between. Figure 16-51 demonstrates how an ARP poisoning attack occurs.

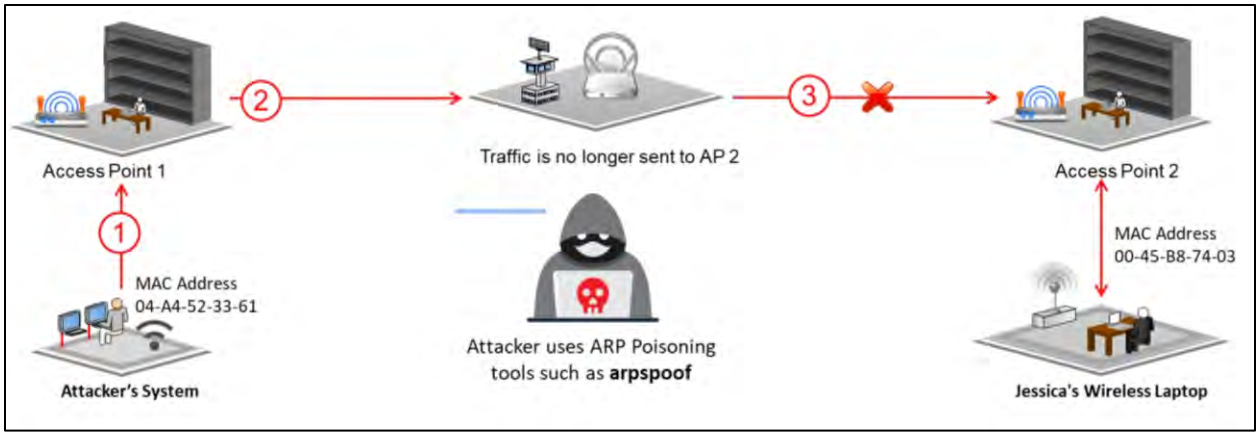


Figure 16-51: ARP Poisoning Attack

In the wireless ARP spoofing attack illustrated in Figure 16-51, the attacker first mimics the victim's MAC address and attempts to authenticate with Access Point 1 (AP1) using an ARP poisoning tool like arpspoof. AP1 then sends the updated MAC address details to the network routers and switches, prompting them to update their routing and switching tables. As a result, traffic intended for the victim's system is directed to AP1 instead of Access Point 2 (AP2).

ARP Poisoning Attack Using Ettercap

Attackers utilize Ettercap to identify the MAC addresses of clients and routers, enabling them to execute attacks like ARP poisoning, sniffing, and MITM attacks. This tool allows attackers to access detailed information about the victim's network traffic. The steps to perform an ARP poisoning attack using Ettercap are as follows:

- Open the Ettercap graphical interface and activate unified sniffing by selecting **Sniff → Unified Sniffing** from the menu bar. This bridges the connection and enables traffic sniffing across interfaces.
- In the **Ettercap Setup** pop-up window, configure the primary interface for sniffing and click **OK**. This action unlocks advanced menu options such as targets, hosts, MITM, and plugins.

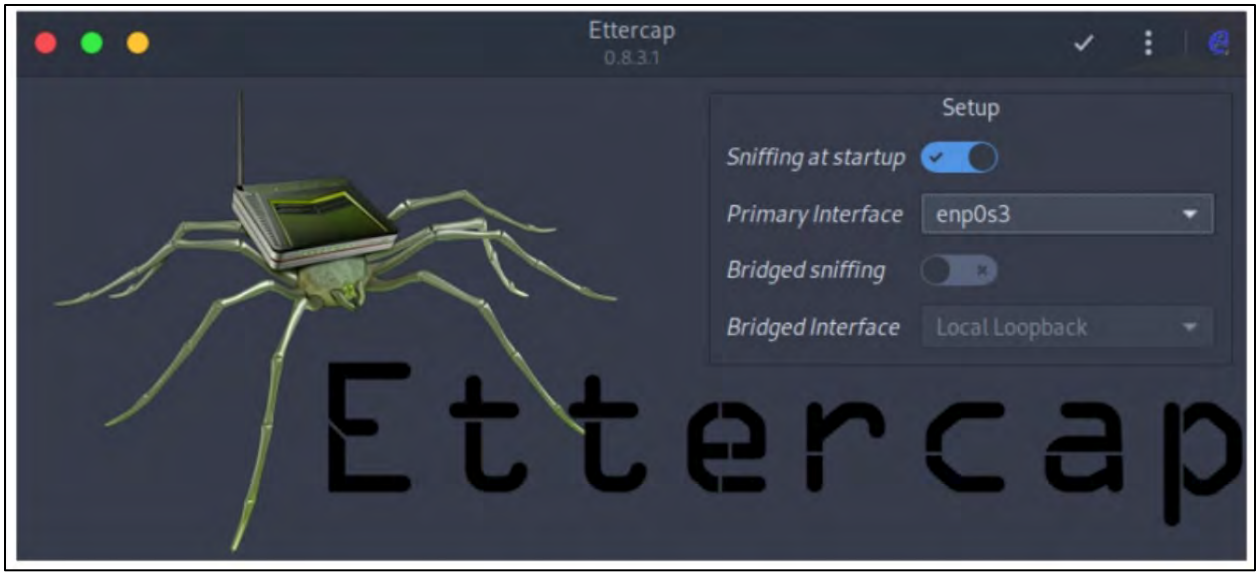


Figure 16-52: Ettercap Interface for Setting the Network Interface to Sniff

- To identify the target host within the network, navigate to **Hosts → Scan for Hosts**. Ettercap will scan for all active hosts on the network and generate a list of detected devices. Then, go to **Hosts → Hosts List** to view all the discovered hosts on the local network.

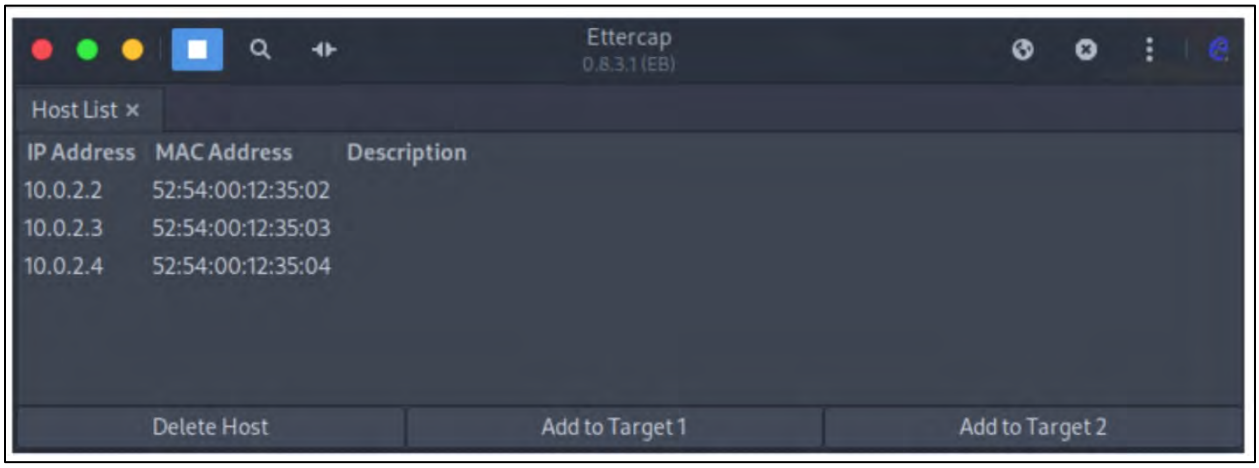


Figure 16-53: Ettercap Showing the Host List

- Navigate to **View → Connections** to begin monitoring the identified connections. Within the Connections view, you can filter connections based on criteria such as IP address, connection type, and status (open, closed, active, or terminated).

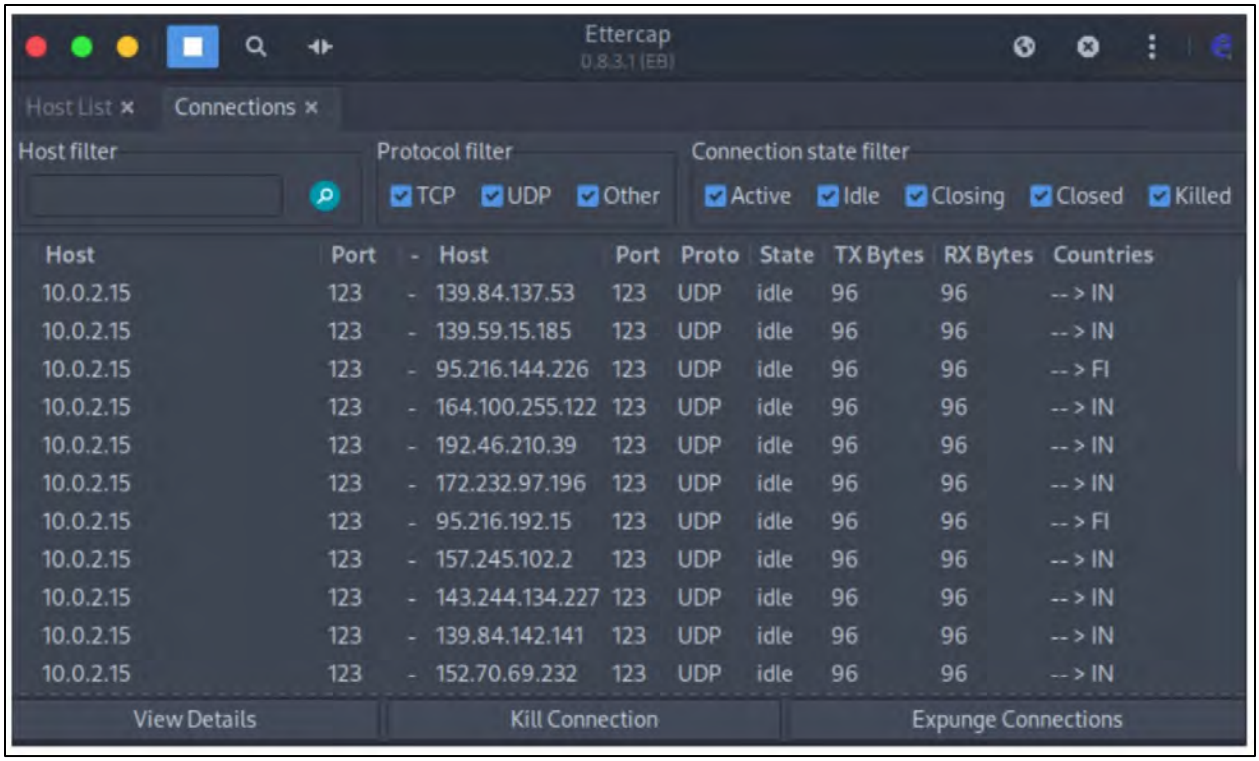


Figure 16-54: Ettercap Showing the Host List

- Choose the hosts for the ARP spoofing attack by navigating the **Hosts** window and selecting the target IP address. Then, go to **Targets → Current Targets** to compile a list of target hosts for the ARP spoofing operation.

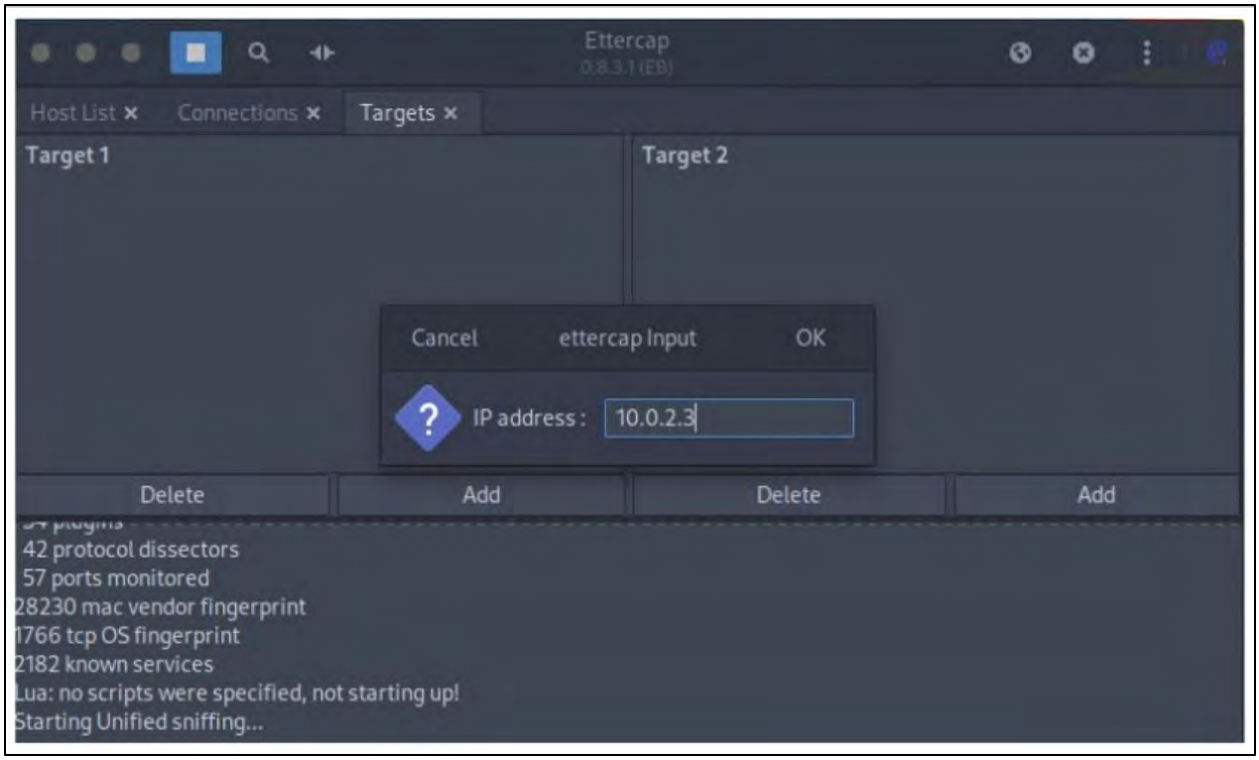


Figure 16-55: Ettercap Showing Targets

- Navigate to **MITM → ARP Poisoning**. Enable the Sniff remote connections option in the pop-up window and click **OK** to initiate the ARP poisoning attack on the selected target.

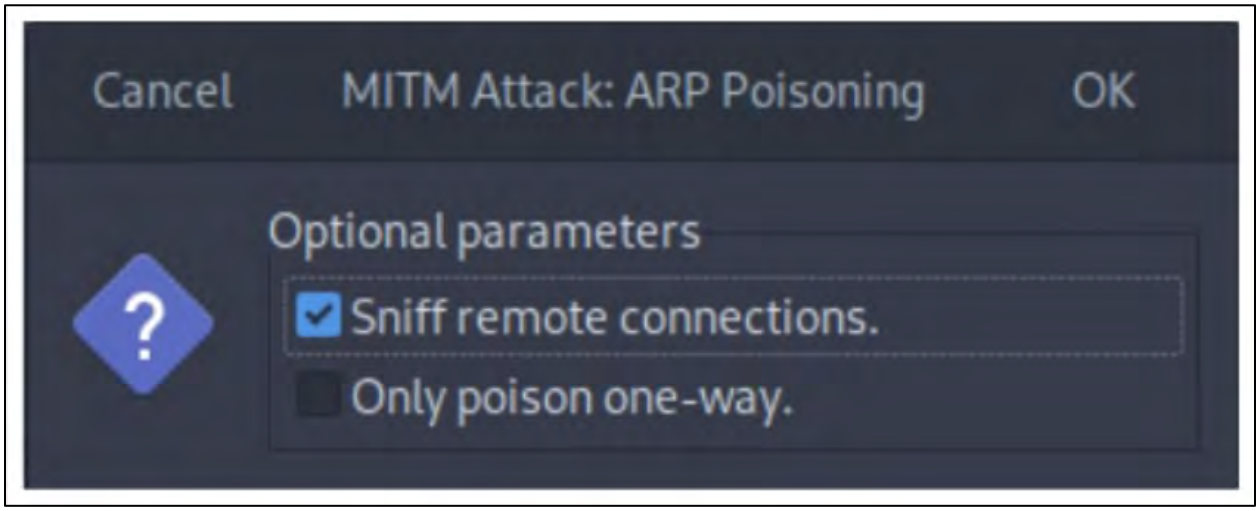


Figure 16-56: Optional Parameter Selection in Ettercap when Launching an ARP Poisoning Attack

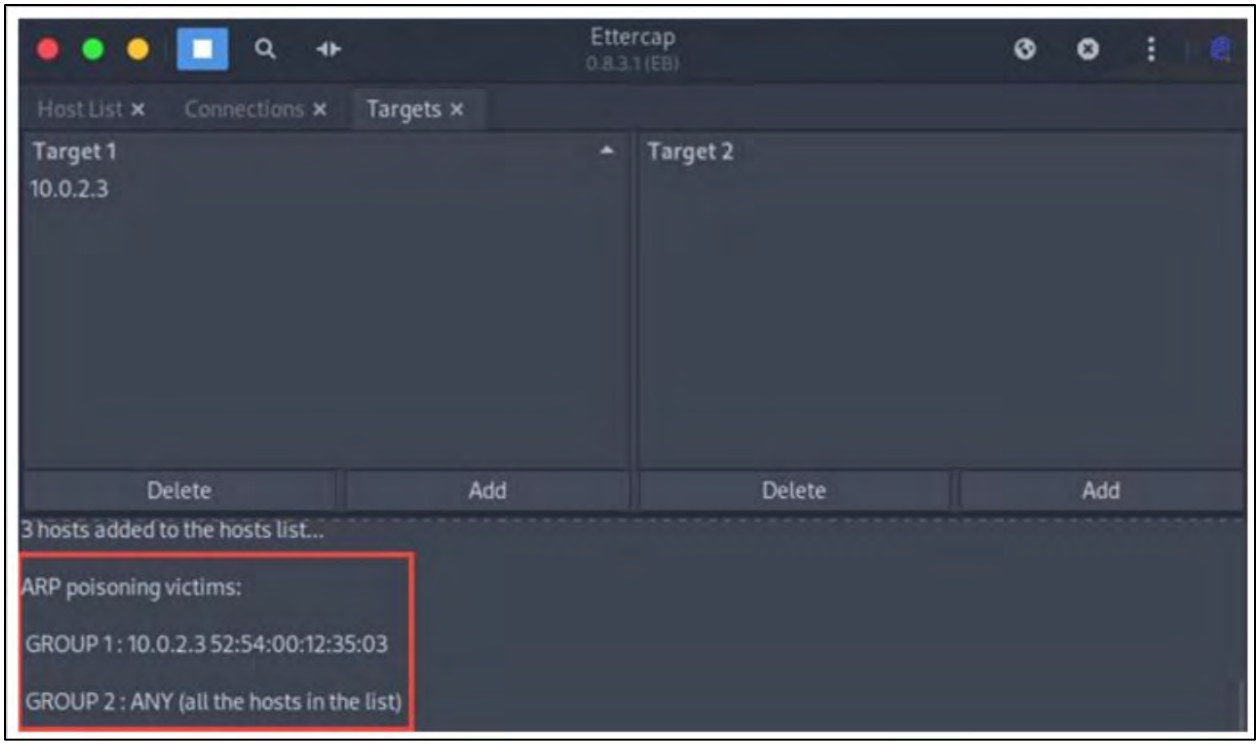


Figure 16-57: Ettercap Launching an ARP Poisoning Attack

Suppose the web traffic is not secured using Hypertext Transfer Protocol Secure (HTTPS) after the attack is initiated. In that case, the login credentials of the target host can be intercepted.

Rogue APs

Rogue AP Attack

Access Points (APs) establish connections with client Network Interface Cards (NICs) by authenticating through Service Set Identifiers (SSIDs). Unauthorized or rogue APs can enable any device with 802.11 capabilities to connect to a corporate network, potentially granting attackers access. Using wireless sniffing tools, attackers can gather details from APs, such as authorized MAC addresses, vendor information, and security configurations.

Attackers may compile a list of MAC addresses for authorized APs on the target network and compare it with the MAC addresses identified through sniffing. They can then deploy a rogue AP near the target corporate network. Rogue APs are used within an 802.11 network to hijack connections from legitimate users. When a user powers on their device, the rogue AP may prompt a connection with the user's NIC. By sending the SSID, the rogue AP tricks users into connecting, believing it to be legitimate.

Once connected, all user traffic is routed through the rogue AP, allowing the attacker to intercept and analyze packets. This traffic may include sensitive information such as usernames and passwords.

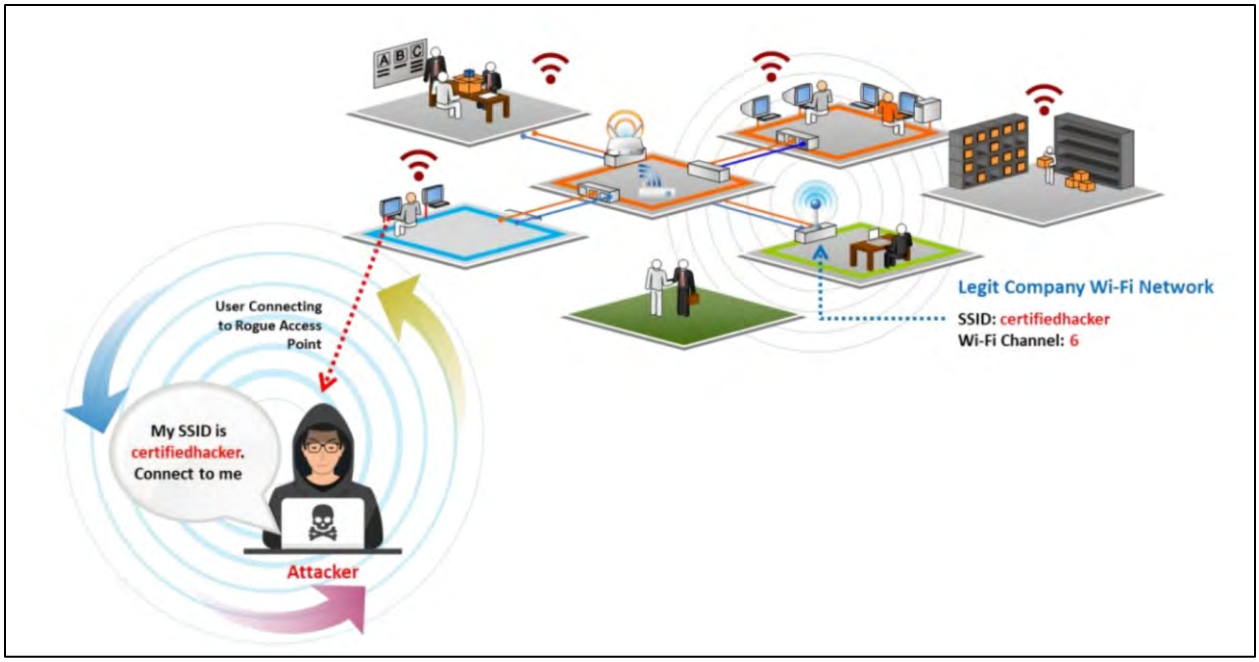


Figure 16-58: Rogue AP Attack

Rogue APs are unauthorized wireless access points installed by attackers on a network without the knowledge or control of the network administrator. Unlike authorized APs, rogue APs lack proper security configurations, making them a potential backdoor to the target network. Below are some common scenarios for setting up and installing rogue APs:

- **Compact Rogue APs Plugged into Ethernet Ports**: Attackers may use small, pocket-sized rogue APs that can be discreetly plugged into the target network's Ethernet ports. These devices are easily portable, require minimal power, and can be installed without drawing attention.
- **Rogue APs Connected via Wi-Fi Links**: A rogue AP can connect to the target network over a Wi-Fi link. This setup allows the AP to be hidden easily as it connects wirelessly, although it requires credentials for the target network.
- **USB-Based Rogue APs**: Attackers can plug USB-based rogue APs into Windows machines connected to the target network via wired or wireless connections. The software on the USB device shares the machine's network access with the rogue AP, eliminating the need for credentials or unused Ethernet ports.
- **Software-Based Rogue APs**: Instead of using separate hardware, attackers can configure software-based rogue APs on the Wi-Fi adapter of a networked Windows machine. This method utilizes the embedded or plugged Wi-Fi adapter to set up the rogue AP.

The steps to deploy a rogue Access Point (AP) are as follows:

- **Select a Strategic Location**: Identify an optimal spot to connect the rogue AP to ensure maximum network coverage from the connection point
- **Disable Visibility and Management Features**: Turn off SSID broadcasting (silent mode) and disable management settings to reduce the risk of detection

- **Position Behind a Firewall**: If feasible, place the rogue AP behind a firewall to evade detection by network scanning tools
- **Limit Deployment Time**: Operate the rogue AP for a short duration to minimize the chances of being discovered

Creation of a Rogue AP Using MANA Toolkit

The MANA Toolkit is a collection of tools used by attackers to create rogue access points, perform sniffing attacks, and execute Man-In-The-Middle (MITM) attacks. It is also effective in bypassing HTTPS and HTTP Strict Transport Security (HSTS) protections. Attackers can use the MANA Toolkit to set up a rogue AP by following these steps:

- **Modify Configuration File**: Use a text editor to edit the **hostapd-mana.conf** file to configure the rogue access point
- **Set Key Parameters**: Define the wireless interface (e.g., wlano) along with the MAC address (BSSID) or the desired SSID (e.g., **Free Internet**)

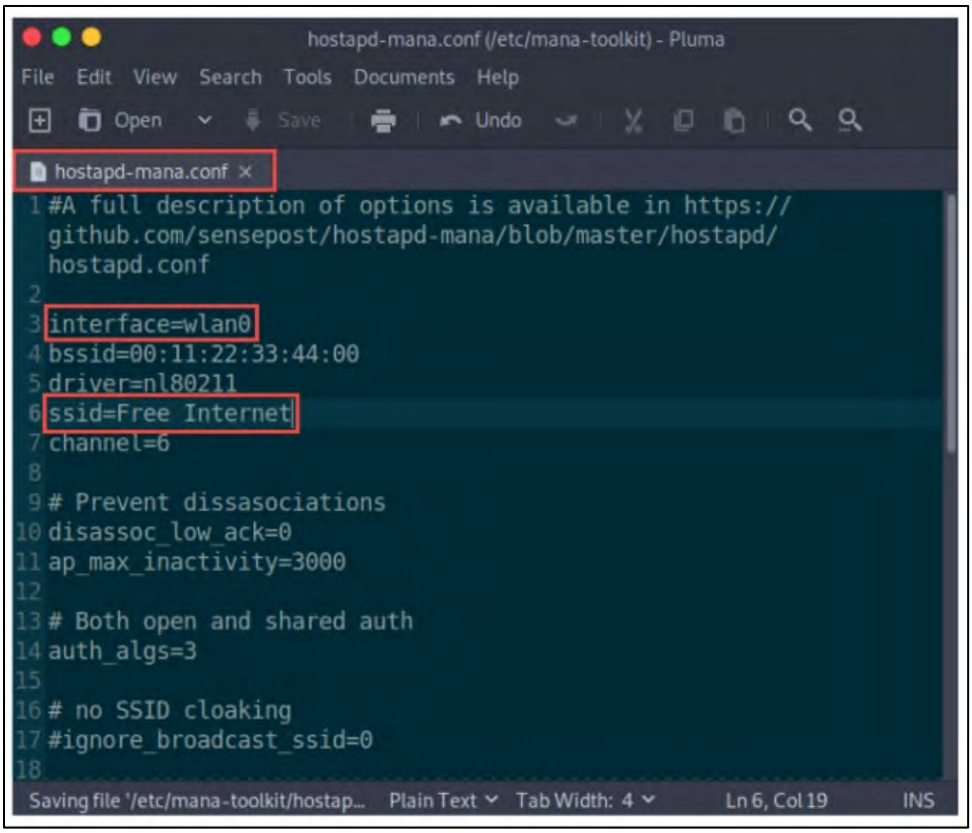


Figure 16-59: hostapd-mana.conf

- **Edit the Script File**: Modify the **start-nat-simple.sh** script to initiate the rogue access point. Set the wireless card parameter **phy** (e.g., wlano) and the **upstream** parameter (e.g., etho) to specify whether the card has an internet connection

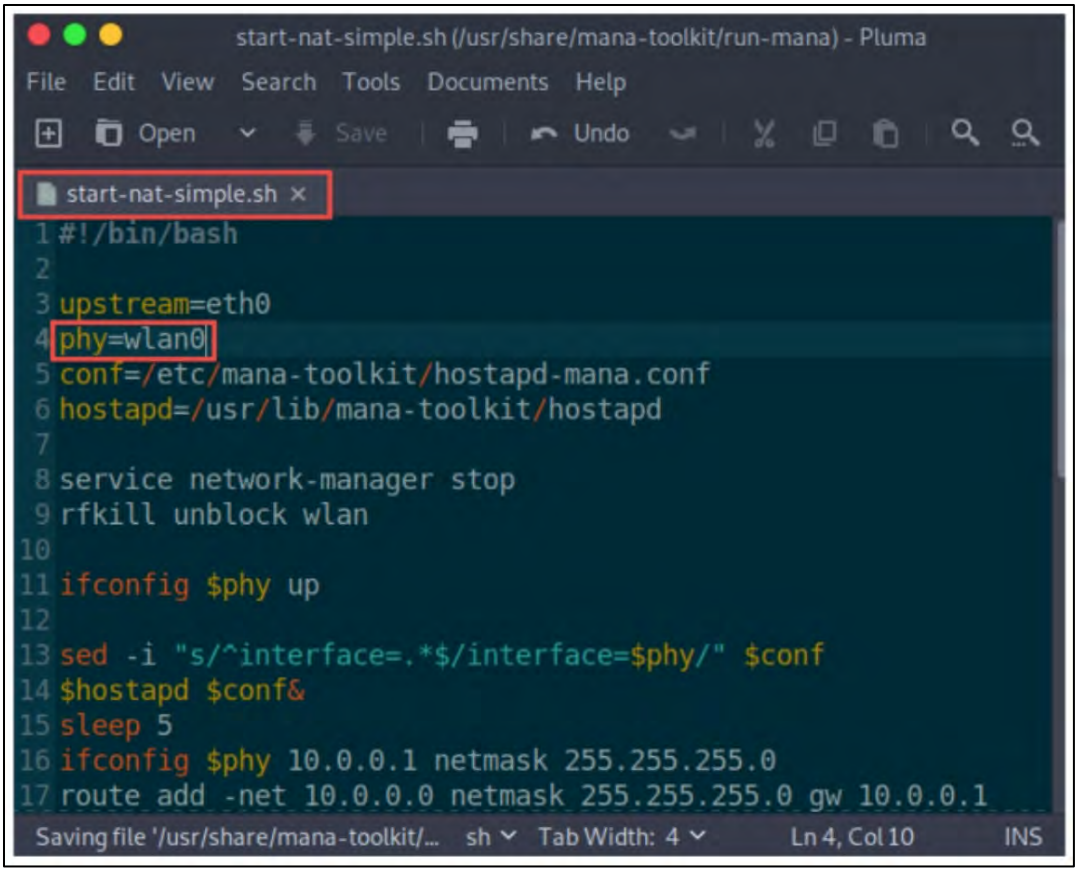


Figure 16-60: start-nat-simple.sh

- **Run the Script**: Execute the **start-nat-simple.sh** script using the bash command # **bash <Path to MANA>/mana-toolkit/run-mana/start-nat-simple.sh.** This will initiate the rogue access point

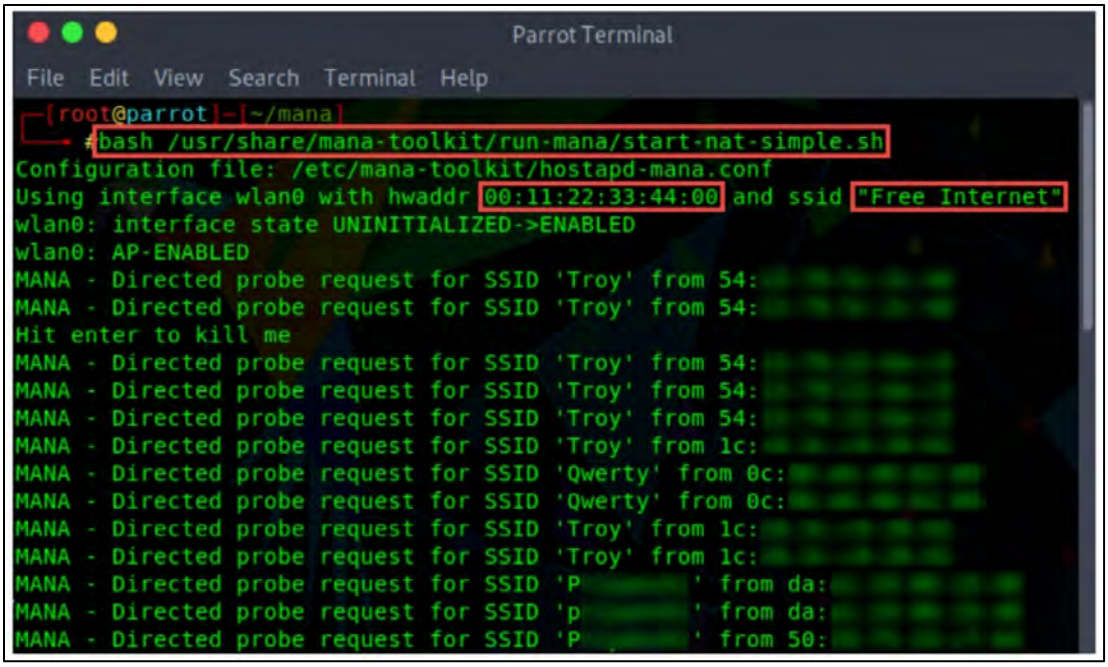


Figure 16-61: Displaying the Output of start-nat-simple.sh

- **Connect to the Rogue AP**: After the Rogue AP is up and running, use a Windows machine or mobile device with a different wireless card to connect to it
- **Search for the Connection**: On the Wi-Fi-enabled device, look for an unprotected internet connection (e.g., **Free Internet**) and connect to it

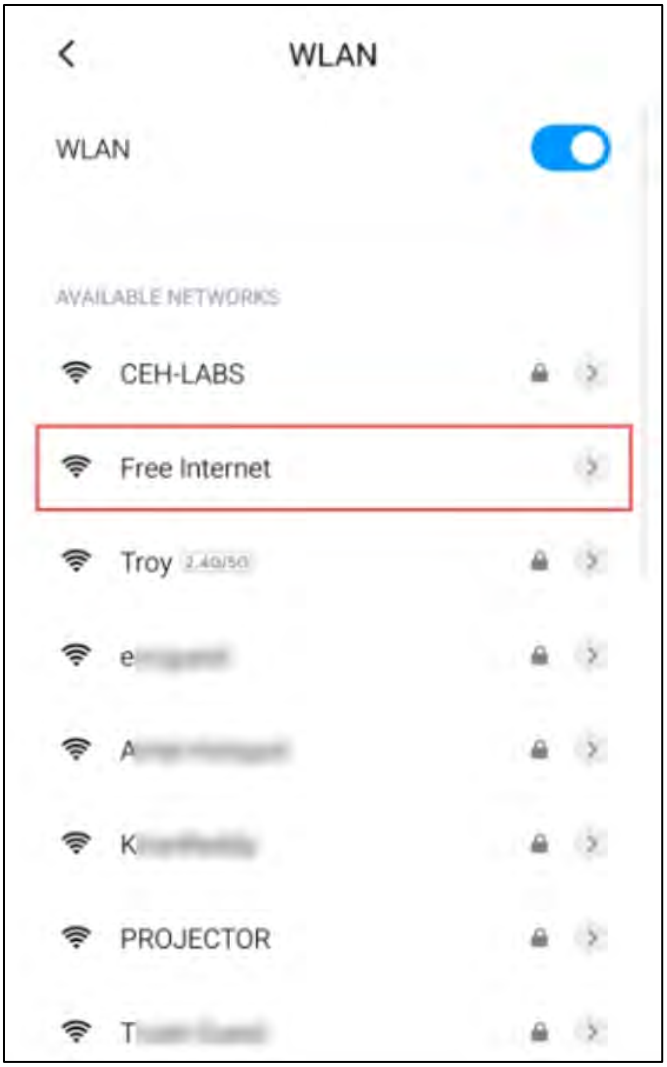


Figure 16-62: Displaying Available Networks in the Mobile Device

- **Packet Capture**: After connecting to the internet through the rogue AP, all data packets from the device pass through it. Tools like tcpdump and Wireshark can then be utilized to capture and analyze these packets

Evil Twin

An evil twin is a fraudulent wireless Access Point (AP) designed to mimic a legitimate AP by replicating its SSID. It poses a significant threat to users on both private and public WLANs. Attackers establish a rogue AP outside the network boundary to entice users to connect. Tools like KARMA are commonly used for this purpose, as they monitor station probes to craft an evil twin. KARMA passively listens to wireless probe request frames and adopts frequently used SSIDs to attract users. The attacker can set up an evil twin with SSIDs commonly associated with residential networks, public hotspots, or an organization's WLAN. If legitimate users are monitored, the attacker can also target APs that omit SSIDs in their probe requests.

An evil twin is a fraudulent wireless Access Point (AP) designed to mimic a legitimate AP by replicating its SSID. It poses a significant threat to users on both private and public WLANs. Attackers establish a rogue AP outside the network boundary to entice users to connect. Tools like KARMA are commonly used for this purpose, as they monitor station probes to craft an evil twin. KARMA passively listens to wireless probe request frames and adopts frequently used SSIDs to attract users. The attacker can set up an evil twin with SSIDs commonly associated with residential networks, public hotspots, or an organization's WLAN. If legitimate users are monitored, the attacker can also target APs that omit SSIDs in their probe requests.

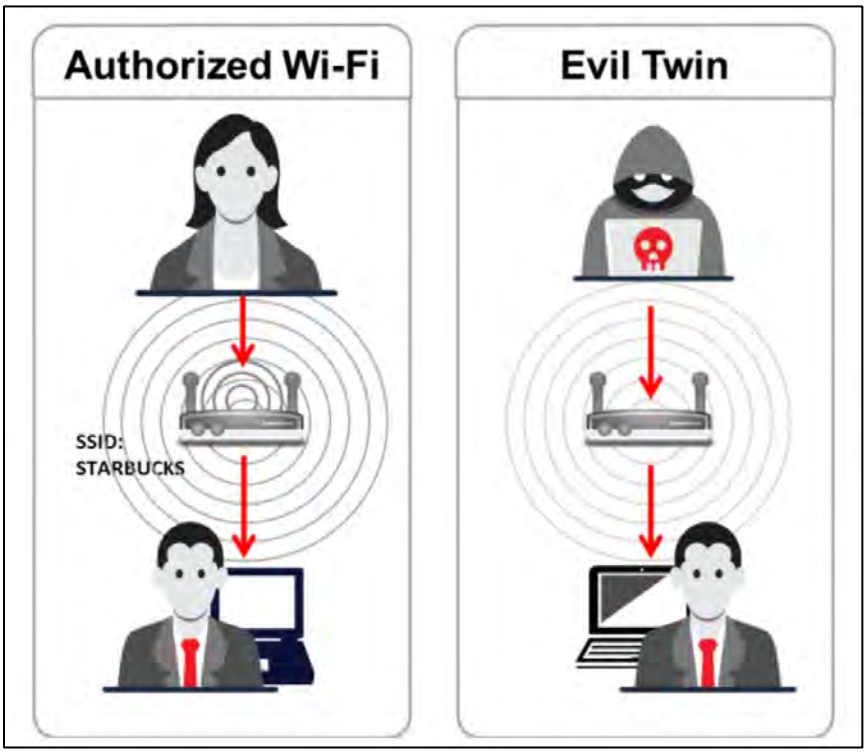


Figure 16-63: Evil Twin

Ensuring company data security becomes difficult when employees use their corporate laptops on public Wi-Fi networks at various establishments.

Setting Up a Fake Hotspot (Evil Twin)

Not all hotspots in an area are genuine, as attackers can deploy an evil twin to mimic a legitimate hotspot. Distinguishing between a legitimate hotspot and an evil twin can be challenging. For instance, a user attempting to connect may see two APs, one being genuine. Suppose the user inadvertently connects to the evil twin. In that case, the attacker can capture login credentials and potentially access the victim's device. Any login attempt by the user would fail, leading them to believe it was a random error. A fake hotspot can be created using a laptop with internet access (via 3G or a wired connection) and a mini AP through the following steps.

1. Activate **Internet Connection Sharing** on Windows or enable **Internet Sharing** on macOS.

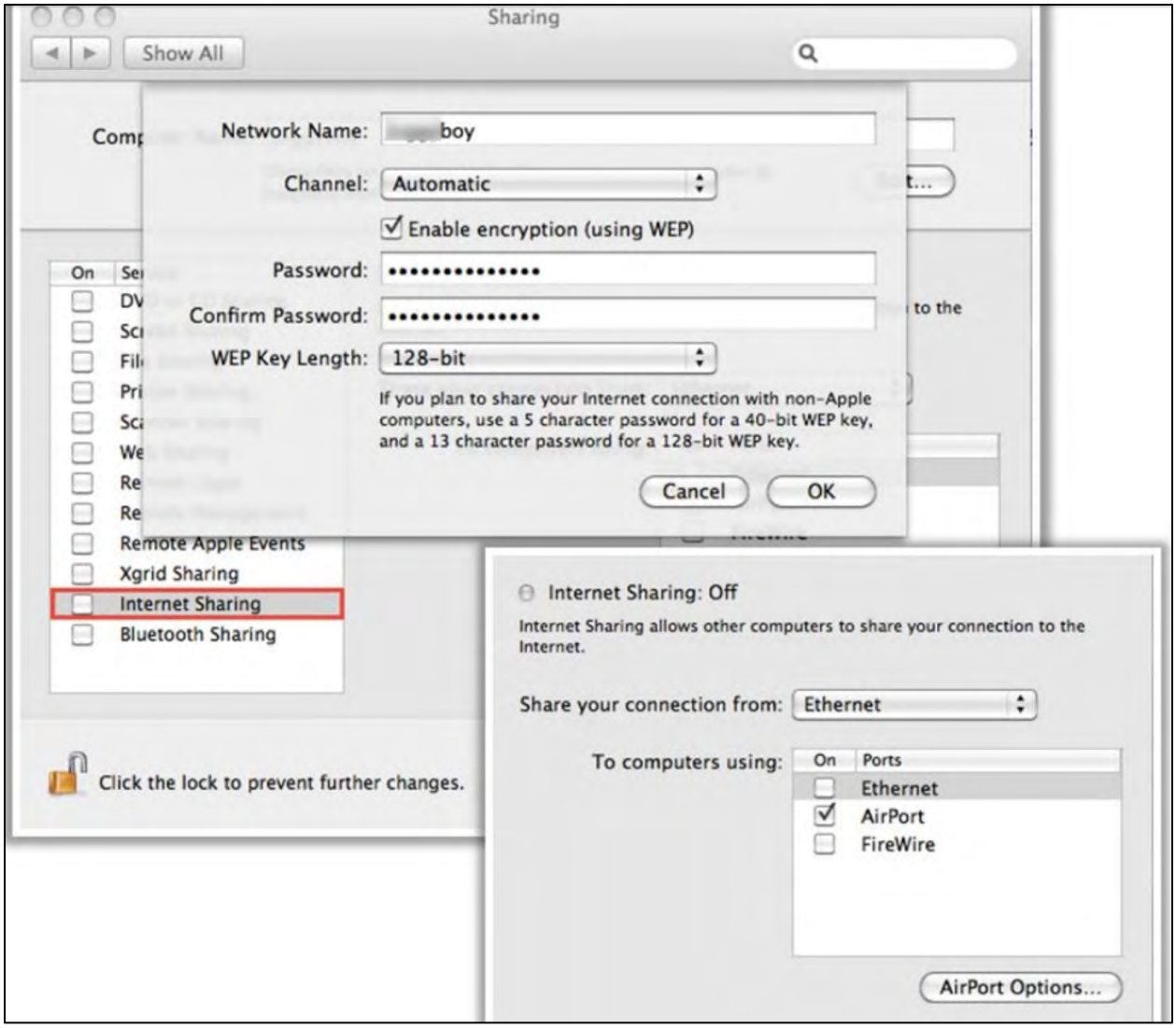


Figure 16-64: Internet Sharing Window in macOS

2. Share the Wi-Fi connection and use a network sniffer program to intercept and capture passwords.

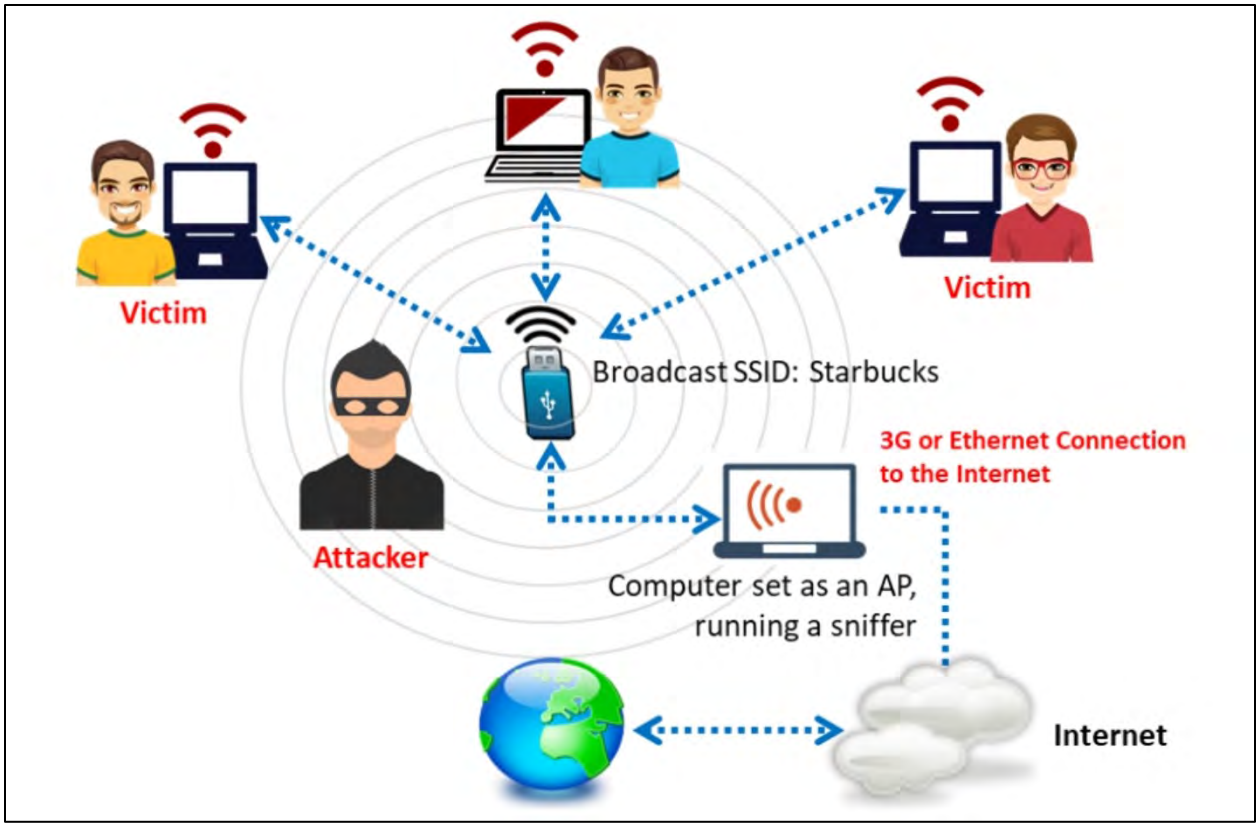


Figure 16-65: Set up of a Fake Hotspot

Key Reinstallation Attack (KRACK)

The Key Reinstallation Attack (KRACK) takes advantage of vulnerabilities in implementing the four-way handshake process in the WPA2 authentication protocol. This protocol establishes connections between devices and access points. Secure Wi-Fi networks rely on the four-way handshake to initiate connections and generate new encryption keys to secure network traffic.

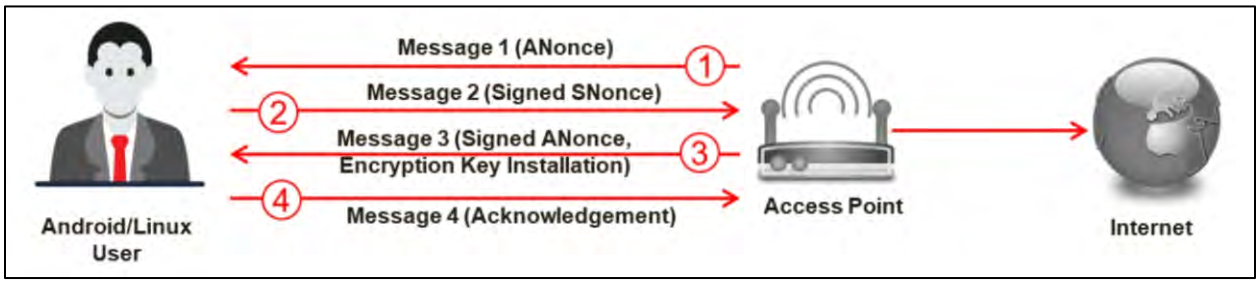


Figure 16-66: Four-way Handshake Process in WPA2

The attacker exploits the WPA2 protocol's four-way handshake by forcing the reuse of the Nonce value. During this attack, the attacker intercepts the victim's ANonce key, which is already used to manipulate and replay cryptographic handshake messages. This method is effective against all modern protected Wi-Fi networks, including WPA and WPA2, personal and enterprise networks, and ciphers such as WPA-TKIP, AES-CCMP, and GCMP. It enables the attacker to access sensitive information like credit card numbers, passwords, chat messages, emails, and photos. Devices

running Android, Linux, Windows, Apple, OpenBSD, or MediaTek are susceptible to some form of the KRACK attack.

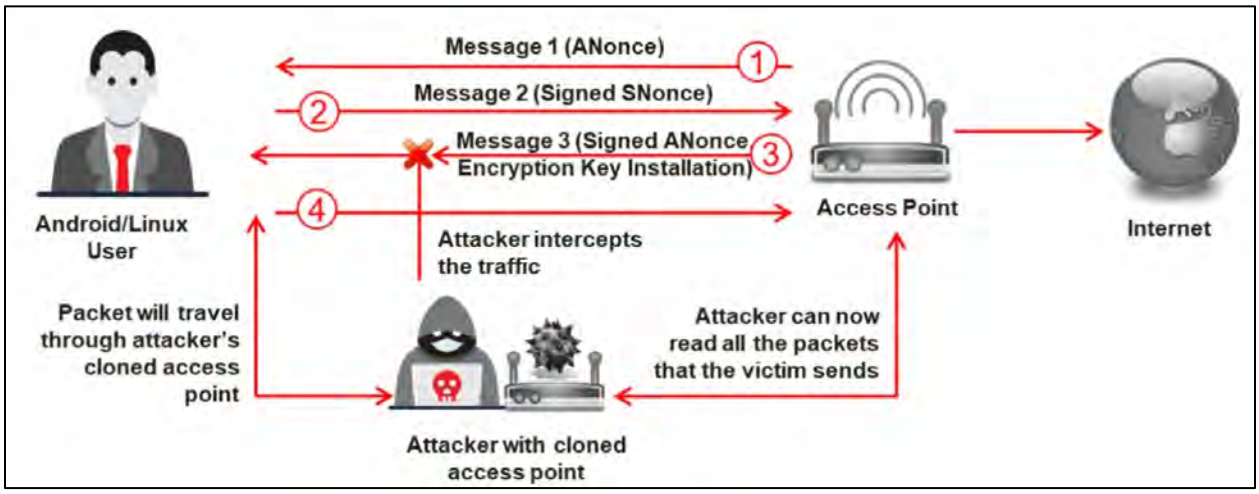


Figure 16-67: KRACK Attack Exploiting the Four-way Handshake Process in WPA2

Jamming Signal Attack

Jamming is a type of attack that targets wireless networks to disrupt their functionality. It involves flooding the network with excessive malicious traffic, causing a Denial-of-Service (DoS) for authorized users, and obstructing legitimate communication. All wireless networks are vulnerable to jamming; spectrum jamming attacks can often completely block all communications.

In this attack, the attacker utilizes specialized hardware to generate signals that appear as noise to devices on the wireless network. This causes the devices to delay their transmissions until the interference is cleared, leading to a Denial-of-Service (DoS). Jamming signal attacks are often difficult to detect. The process of executing a jamming signal attack is outlined as follows.

- The attacker positions themselves near the target area with a high-gain amplifier that overwhelms the legitimate access point's signal
- Users can either not connect or get disconnected due to the stronger nearby signal
- The jamming signal creates a Denial-of-Service (DoS) because the 802.11 protocol uses a CSMA/CA collision avoidance mechanism, which requires a quiet period before any transmission can occur.

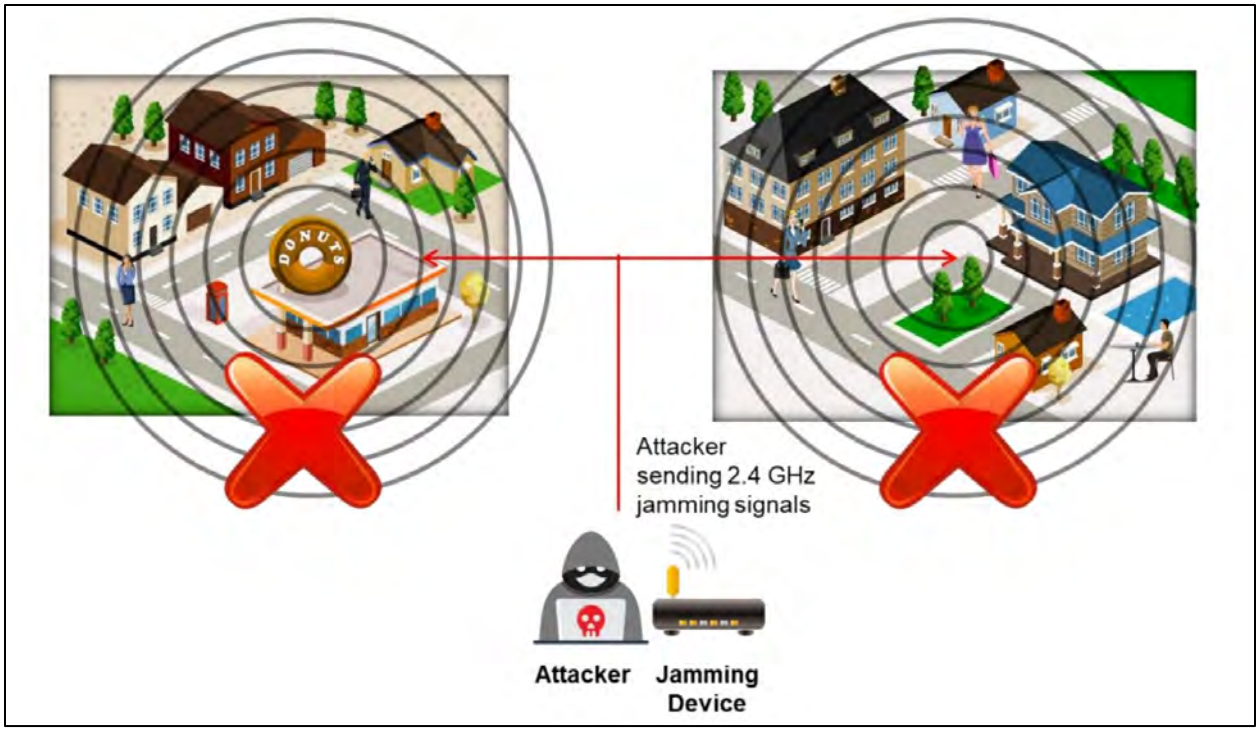


Figure 16-68: Jamming Signal Attack

Wi-Fi Jamming Devices

An attacker can disrupt a wireless network using a Wi-Fi jammer, which operates on the same frequency band as the legitimate network, causing interference and temporarily interrupting network services. An example of a Wi-Fi jamming device is:

- **PCB-4510 Jammer**
  - **Range:** 50–150 meters
  - **Antennas:** 10
  - **10 Frequency Bands Jammed:** GSM, 3G, UMTS, 4G LTE, Wi-Fi 11.b & g, GPS, 5G, Wi-Fi 11.a
  - **Operating Time:** 1-2 hours

Figure 16-69: PCB-4510 Jammer

- **CPB-2920 Jammer**
  - **Range:** 10–40 meters
  - **Antennas:** 20
  - **20 Frequency Bands Jammed:** CDMA, DCS, PCS, 3G, UMTS, 4G, Wi-Fi 11.b & g, 4G WiMAX Sprint, 5G, GPS, Lojack, VHF, Car Remote, UHF
  - **Operating Time:** No time limit

Figure 16-70: CPB-2920 Jammer

- **CPB-2612H-5G Jammer**
  - **Range:** 20–60 meters
  - **Antennas:** 12

- **12 Frequency Bands Jammed:** 5G, 4G, GSM, DCS, 3G, UMTS, Wi-Fi 11.b & g, Lojack Car Tracking, UHF, VHF
- **Operating Time:** No time limit

Figure 16-71: CPB-2612H-5G Jammer

- **CPB-2080-5G Jammer**
  - **Range:** 10–40 meters
  - **Antennas:** 8
  - **8 Frequency Bands Jammed:** 5G, 4G, GSM900, DCS, 3G, UMTS, Wi-Fi 11.b & g
  - **Operating Time:** No time limit

Figure 16-72: CPB-2080-5G Jammer

- **PCB-2112 Jammer**
  - **Range:** 20–50 meters

- **Antennas:** 12
- **12 Frequency Bands Jammed:** CDMA, DCS, 3G, Wi-Fi 11a, 4G, 5G, GPS, VHF, UHF
- **Operating Time:** 60–80 minutes

Figure 16-73: PCB-2112 Jammer

- **PCB-1016 Jammer**
  - **Range:** 10–30 meters
  - **Antennas:** 16
  - **16 Frequency Bands Jammed:** CDMA, DCS, PCS, 3G, UMTS, 4G, 5G, Wi-Fi 11.b & g, 4G WiMAX Sprint, GPS, UHF Remote Control, 5G LTE
  - **Operating Time:** 3 hours

Figure 16-74: PCB-1016 Jammer

aLTEr Attack

Long-Term Evolution (LTE), also known as 4G, is a wireless broadband communication standard developed to replace 3G. It aims to enhance the speed and security of mobile networks. It offers scalable bandwidth and is compatible with earlier technologies like the Global System for Mobile Communications (GSM; 2G) and Universal Mobile Telecommunications System (UMTS; 3G). While LTE is designed to address the limitations of previous wireless networks, it remains vulnerable to data hijacking attacks.

The aLTEr attack targets LTE devices that encrypt user data using the AES Counter (AES-CTR) mode, which lacks integrity protection. In this attack, the attacker sets up a virtual (fake) communication tower between two legitimate endpoints to deceive the victim. The attacker uses this virtual tower to interfere with the data transmission between the user and the real tower, attempting to hijack an active session. When the attacker receives the user's request, they manipulate the traffic through the virtual tower and redirect the victim to harmful websites.

This attack targets "layer 2," the data link layer, which handles the exchange of information over wireless networks using standard data encryption technologies. It also allows multiple users to access network resources and defines how data is transferred between nodes without interference. By exploiting vulnerabilities or design flaws in this layer, the attacker seeks to gain control of browsing data and alter user inputs using a spoofed DNS server, redirecting the user to malicious or unintended websites. The steps involved in an aLTEr attack are outlined as follows.

- The attacker sets up a fake tower that mimics a legitimate one
- The attacker identifies the user's location and sends a packet that seems like a valid request to the genuine tower
- The real tower sends the requested web link in response
- The attacker then redirects the user to malicious or undesired websites

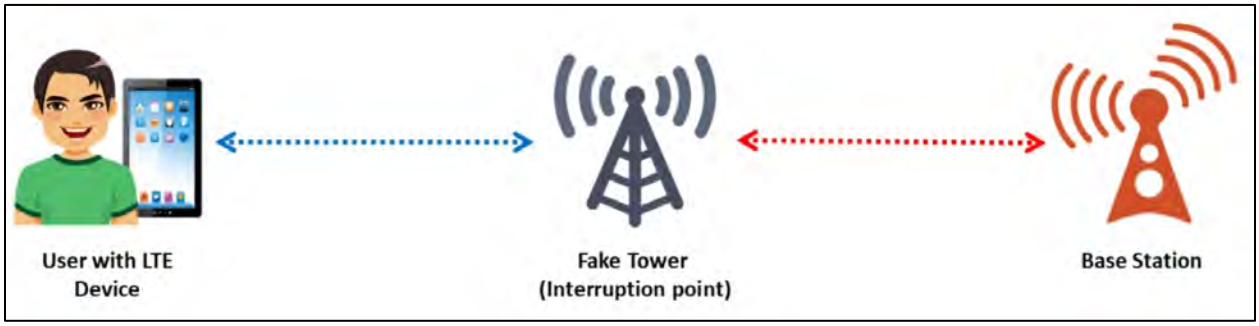


Figure 16-75: aLTEr Attack

An aLTEr attack consists of two phases:

- **Information gathering phase:** The attacker collects necessary information passively, using methods like identity mapping and website fingerprinting
- **Attack phase:** Using the gathered information, the attacker launches an active attack, often employing tactics like DNS spoofing

Information Gathering Phase

During this phase, attackers observe the websites users attempt to visit and track their frequency of visits. They only monitor the communication between the base station and the user without altering credentials or data. Attackers employ the following passive techniques to gather information:

- **Identity mapping:** The attacker maps the identity to identify the target device. Once the target is located, the attacker plans the next stages of the attack
- **Website fingerprinting:** The attacker tracks the volume of traffic accessed by the client, recording the user's online activity and associated metadata

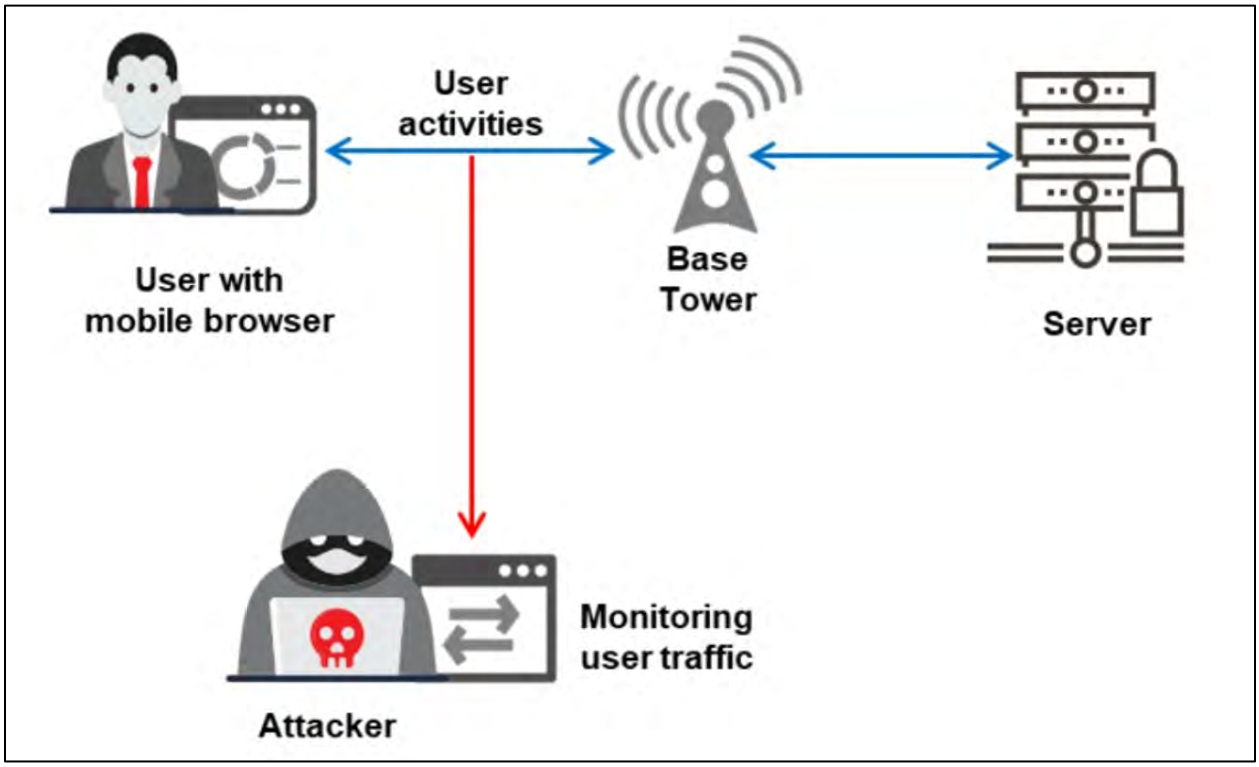


Figure 16-76: Information Gathering Phase

Attack Phase

After collecting information on the target users, the attacker initiates a Man-in-the-Middle (MITM) attack by deploying a fake tower that interferes with and manipulates the user data meant for the legitimate tower. The attacker employs DNS spoofing to redirect the victim to a malicious or chosen website, where they can capture sensitive information like usernames and passwords entered by the victim.

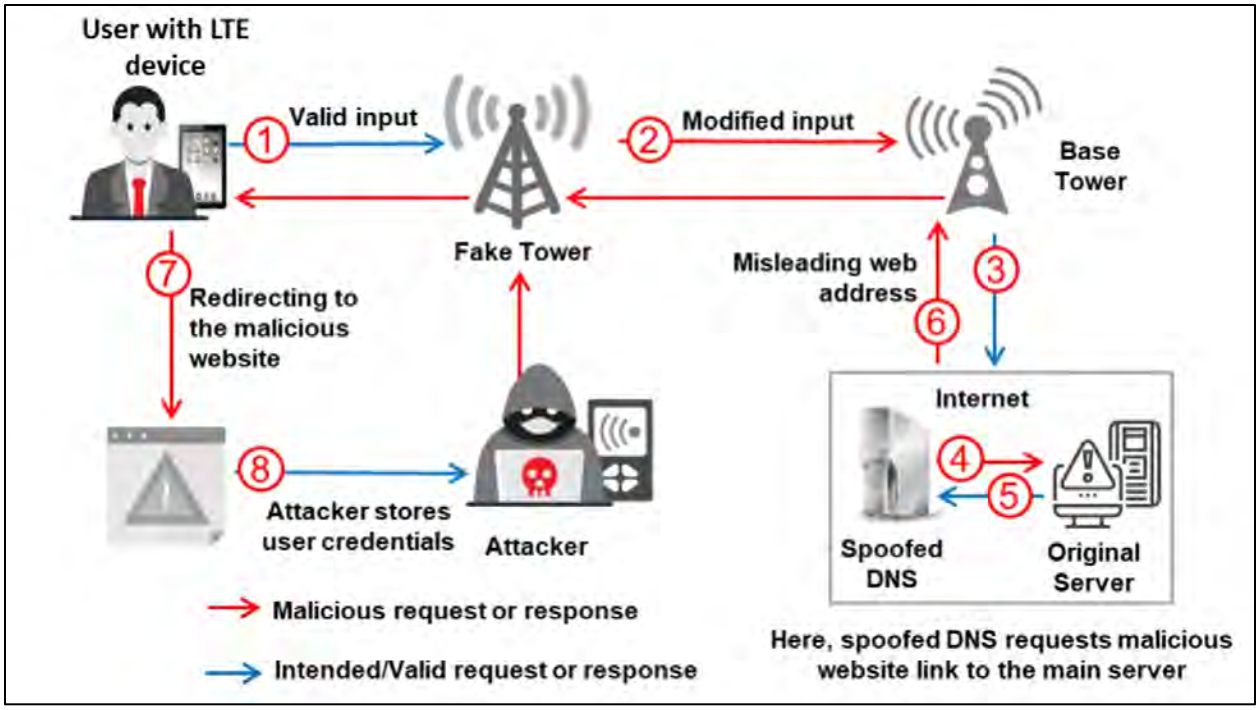


Figure 16-77: Attack Phase

Wi-Jacking Attack

Attackers utilize a Wi-Jacking attack to gain access to many wireless networks. In this type of attack, the Wi-Fi details of nearby victims can be retrieved without the need for cracking tools. This attack is effective when credentials are stored in the victim's browser, when the victim repeatedly visits the same website, or when the router's configuration interface is accessed over an unencrypted HTTP connection. Attackers exploit these vulnerabilities to breach WPA/WPA2 networks without performing a handshake. The following conditions must be met for a Wi-Jacking attack to occur.

- There must be at least one active client device connected to the target network.
- The client device must have previously connected to an open network and be set to reconnect automatically.
- The client device should be using a chromium-based web browser.
- The browser on the client device must have stored the router's admin interface credentials.
- The router of the target network must allow access to the configuration interface through an unencrypted HTTP connection.

Attackers carry out a Wi-Jacking attack by following these steps:

- Send de-authentication requests to the victim's device using aireplay-ng to disconnect them from their legitimate Wi-Fi network.

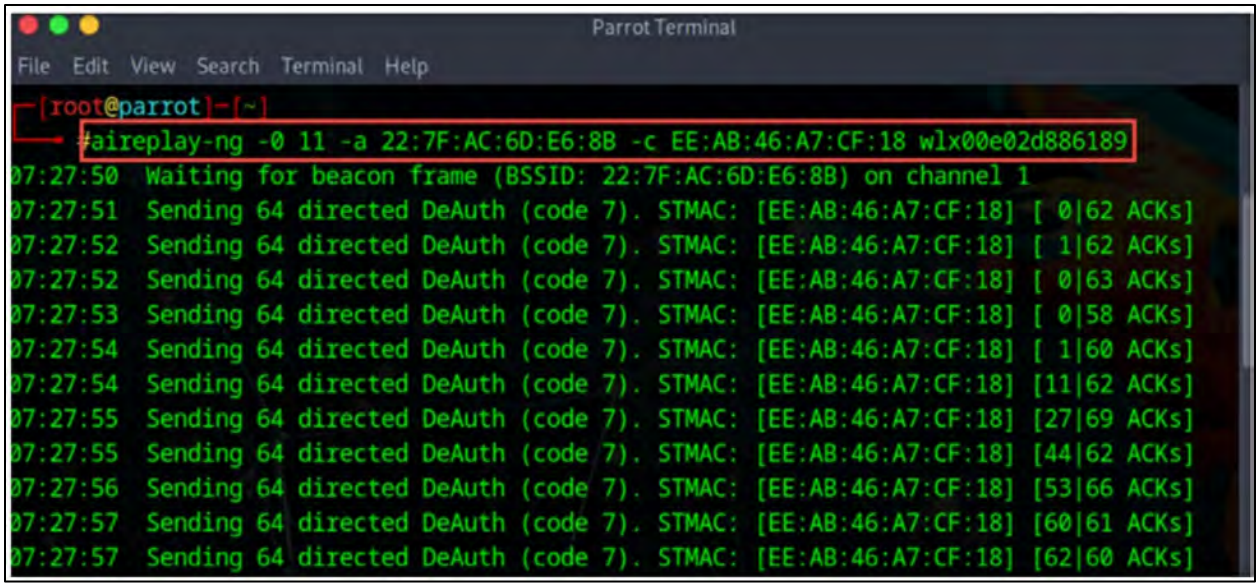


Figure 16-78: De-authentication Requests Sent via aireplay-ng

- Execute a KARMA attack with "hostapd-wpe" to trick the victim into connecting to a malicious Wi-Fi network.
- After successful de-authentication, use tools like "dnsmasq" and Python scripts to inject a harmful URL, causing the victim's browser to load it. The BSSID and ESSID determine the URL/page pair.
- Wait for the victim to visit the HTTP page, during which the router is updated and restarted automatically.

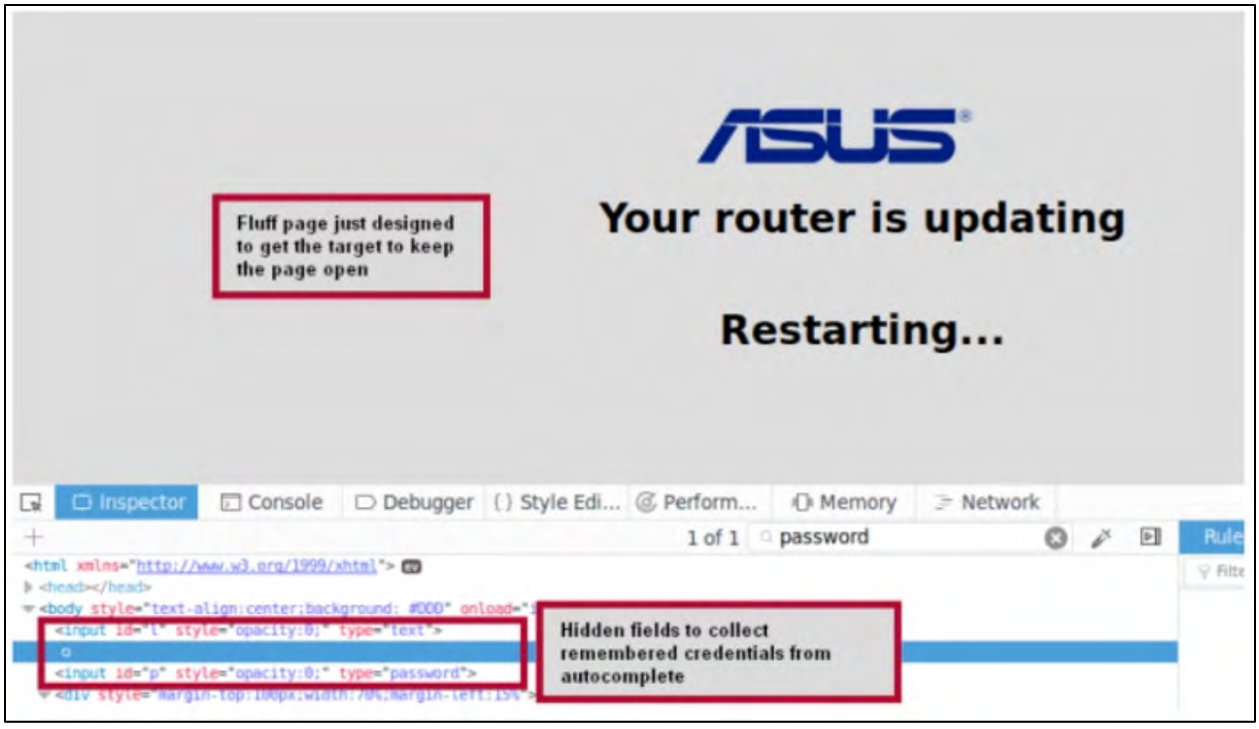


Figure 16-79: Update and Restarting of the Router

- When the victim accesses the malicious page, the browser checks these two conditions to load stored credentials:
    - Does the malicious URL and the router's admin interface share the same origin?
    - Do the input fields of the page match those of the router's admin interface?
- After obtaining the credentials, the victim is kept on the malicious page for a while. The KARMA attack is stopped, and the victim reconnects to their legitimate network. However, the router's admin interface and the stored admin credentials remain in the browser's JavaScript.
- Use XMLHttpRequest to log into the router and extract the victim's WPA2 PSK, making additional malicious changes as needed. With the PSK and other credentials, the attacker can compromise the victim's private network and manipulate sensitive data using the Wi-Jacking technique.

RFID Cloning Attack

RFID cloning involves copying the data from a genuine RFID tag and creating duplicates using a new chip. Essentially, the information from one RFID tag is transferred to another tag by altering the Tag ID (TID), while the form factor and data may remain the same. The cloned tag differs from the original and can be easily identified. Attackers often use tools like iCopy-X, RFIDler, Flipper Zero, and others to clone RFID tags.

iCopy-X

iCopy-X is a handheld RFID cloning tool used to duplicate RFID tags. It is a standalone device with an integrated screen and buttons, offering the same functionality as a Proxmark without requiring an external computer.

Figure 16-80: iCopy-X RFID Cloner

The following are some additional RFID cloning tools:

- RFIDler (https://github.com)
- RFID Mifare Cloner (https://github.com)
- Flipper Zero (https://flipperzero.one)
- Boscloner Pro (https://www.boscloner.com)

Wi-Fi Encryption Cracking

Once an attacker gains unauthorized access to a target network through techniques like wireless attacks, rogue access points, or evil twins, the next step is to bypass the security measures set up by the target's wireless network. Typically, Wi-Fi networks use WPA, WPA2, or WPA3 encryption to secure communications, and the attacker must break these encryption systems. This section explores how an attacker can decrypt these security protocols to compromise the network's security.

WPA/WPA2 Encryption Cracking

WPA encryption is more secure than WEP encryption. However, an attacker can still break WPA/WPA2 encryption by capturing the required packets. While this process can be carried out

offline, the attacker must be within range of the access point for a brief period. Below are some techniques used to crack WPA encryption.

- **WPA PSK**: WPA PSK utilizes a password defined by the user to initiate the four-way handshake. Although the password cannot be directly cracked, the encryption keys can be attacked through brute-force dictionary attacks, which can successfully crack most consumer passwords.
- **Offline Attack**: To carry out an offline attack, an attacker must be within range of the access point for a few seconds to capture the WPA/WPA2 authentication handshake. Once the necessary packets are captured, WPA encryption keys can be cracked offline. Since the WPA handshake does not transmit the password over the network (usually over insecure, plaintext channels), capturing a full authentication handshake between the client and AP allows the attacker to break the WPA/WPA2 encryption without injecting any packets.
- **De-authentication Attack**: In a de-authentication attack to crack WPA encryption, an attacker must first identify an actively connected client. The attacker then forces the client to disconnect from the Access Point (AP) and uses tools like aireplay to capture the authentication packet when the client tries to reconnect. The client typically re-authenticates with the AP within seconds. The authentication packet contains the Pairwise Master Key (PMK), which the attacker can crack using dictionary or brute-force attacks to obtain the WPA key.
- **Brute-Forcing WPA Keys**: Brute-force techniques effectively break WPA/WPA2 encryption keys. An attacker can attempt a brute-force attack on WPA encryption keys using a dictionary or tools like aircrack and aireplay. Brute-force attacks are computationally intensive and can significantly impact WPA encryption. Cracking WPA keys through brute-force methods may take hours, days, or even weeks.

Cracking WPA/WPA2 Using Aircrack-ng

Cracking WPA/WPA2 with aircrack-ng involves several steps to assess the security of Wi-Fi networks. The process starts by enabling monitor mode on a compatible Wi-Fi adapter to capture traffic. Airodump-ng is then used to capture a WPA/WPA2 handshake, often by sending de-authentication packets to prompt client reconnection. After capturing the handshake, aircrack-ng tries to crack the password by comparing it against a wordlist of possible passwords.

Here are the steps to crack WPA-PSK:

- Use airmon-ng to monitor wireless traffic with the command:

```
airmon-ng start <wireless interface>
```

Note: If you encounter an error indicating two processes that might cause issues, run the command:

```
airmon-ng check kill
```

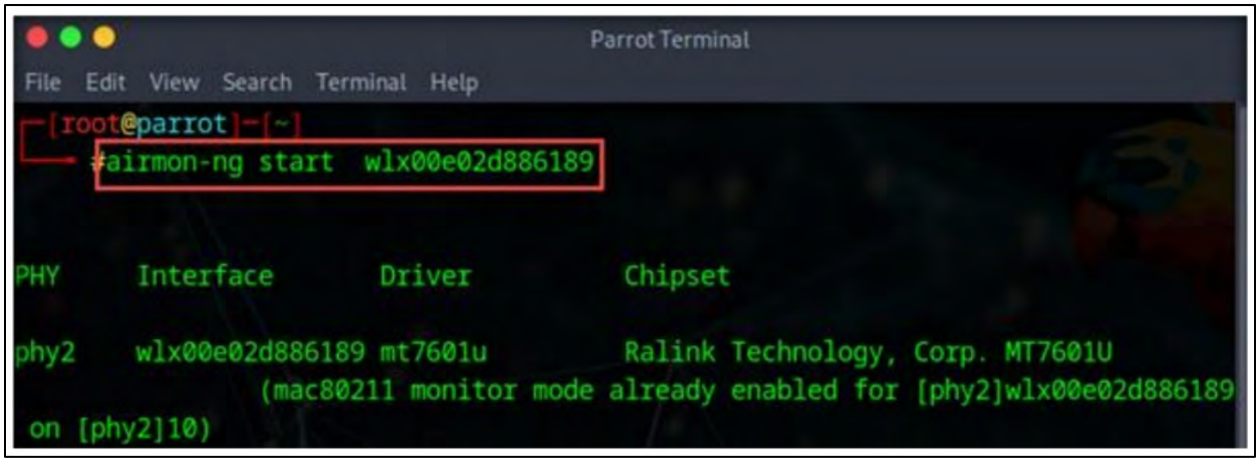


Figure 16-81: Execution of airmon-ng

- Use the airodump-ng command to display a list of detected access points and connected clients:

airodump-ng <Wireless Interface>

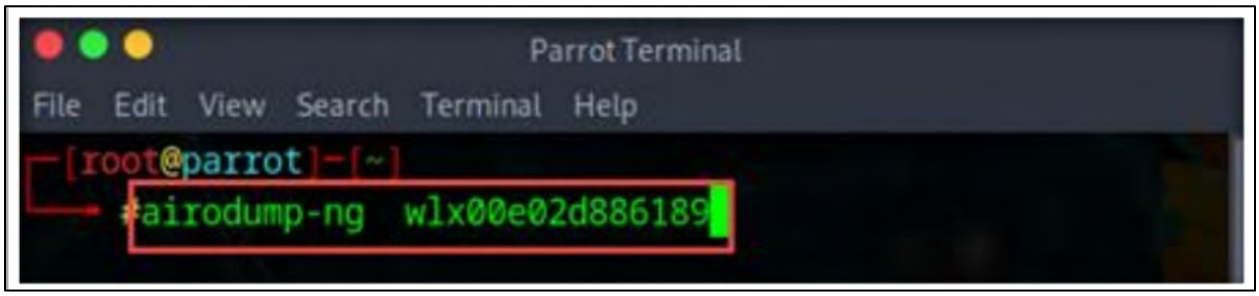


Figure 16-82: Execution of airodump-ng to Show Identified APs

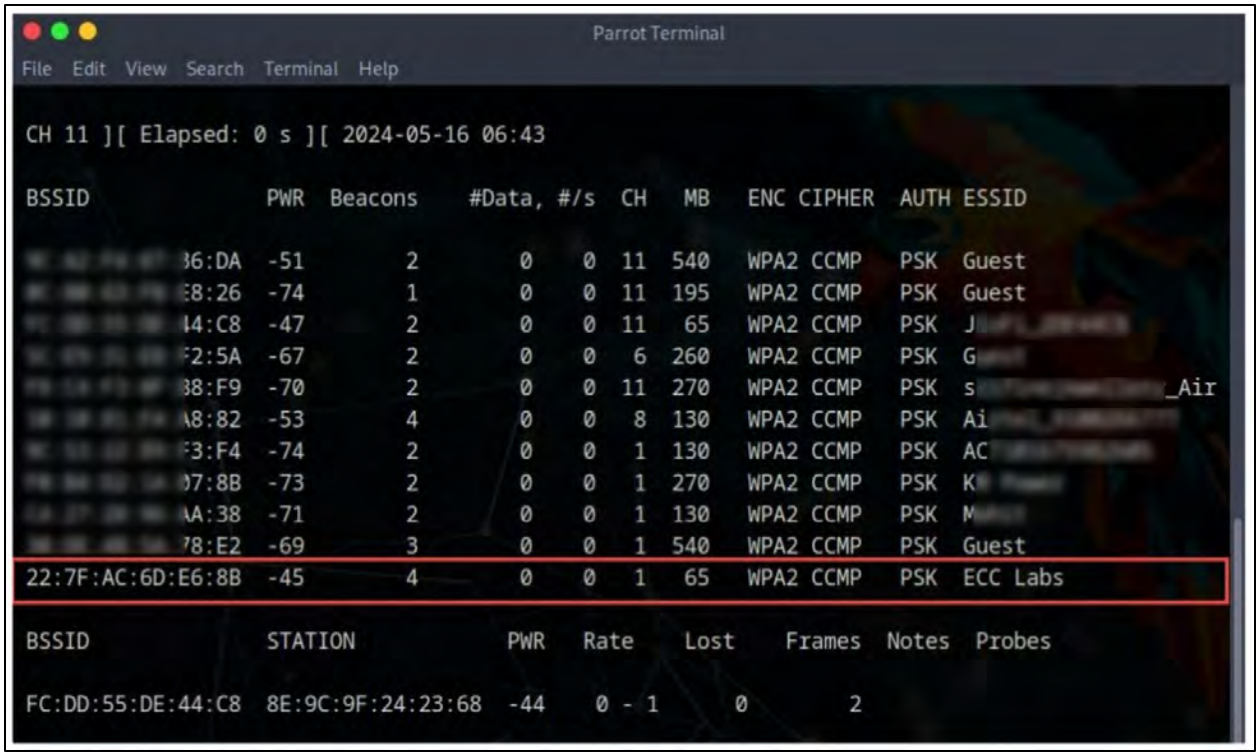


Figure 16-83: List of Detected Access Points

- In Figure 16-84, choose the target wireless access point.
- Open a new terminal and execute the following airodump-ng command to capture packets from the selected access point as the root user, then close the terminal:

airodump-ng --bssid <BSSID> -c 1 -w <ESSID> <Wireless interface>

Figure 16-85: Execution of airodump-ng to Capture Packets

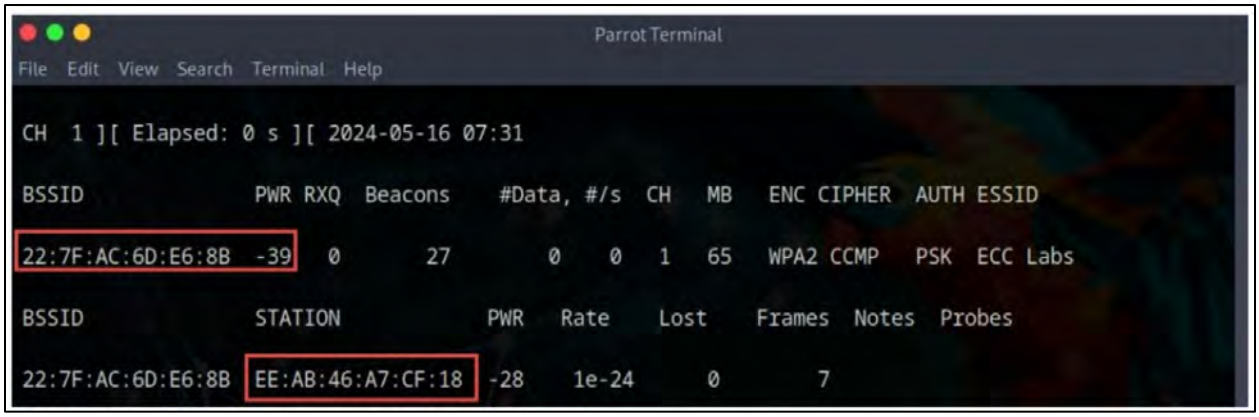


Figure 16-86: Result of airodump-ng

- Open a new terminal and execute the following aireplay-ng command repeatedly to send a significant number of de-authentication packets to the connected device:

aireplay-ng -0 11 -a <Access point MAC address/BSSID> -c <MAC address of connected device> <Wireless interface>

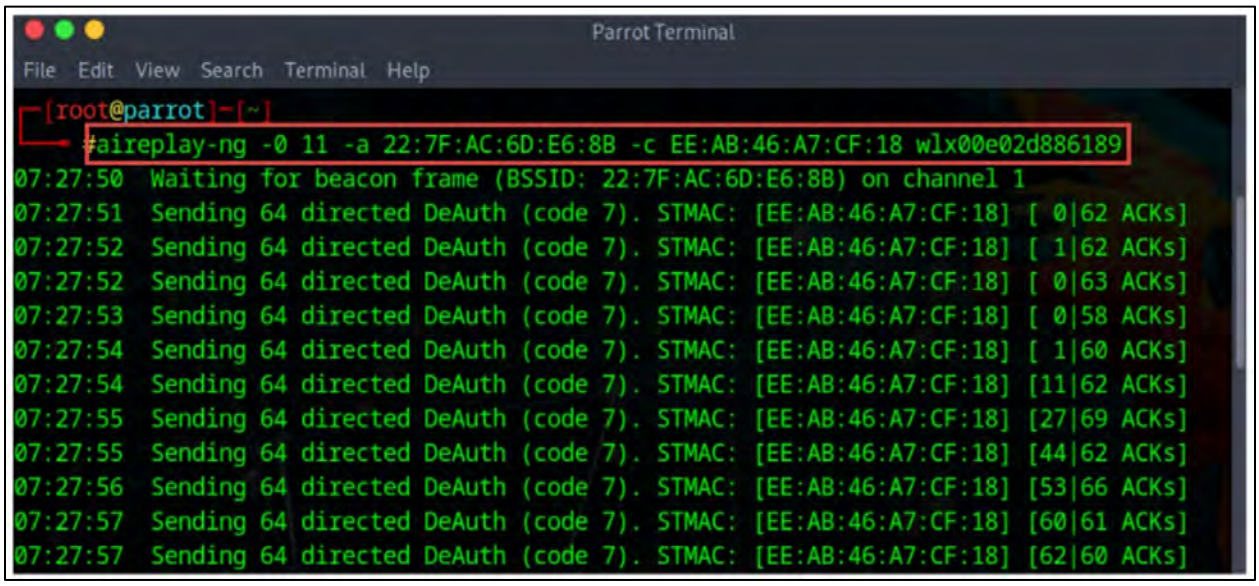


Figure 16-87: Execution of aireplay-ng to Transmit De-Authentication Packets

- Return to the airodump-ng terminal that was left running and continue capturing packets until the WPA handshake (22:7F:AC:6D:E6:8B) is received. The captured packets will be stored in a .cap file.
- In a different terminal, execute the following aircrack-ng command as the root user, using the password.txt file against the captured .cap file:

aircrack-ng -a2 <Access point MAC address/BSSID> -w password.txt <captured file name>.cap

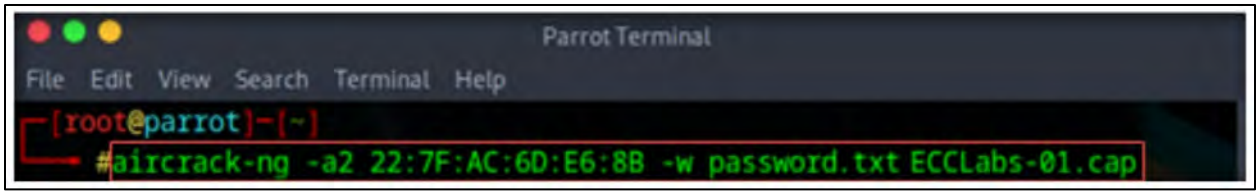


Figure 16-88: Execution of aircrack-ng to Crack WPA/WPA2 Password

- The output of the aircrack-ng command will display the cracked key with the message "KEY FOUND!". If the password is complex, the cracking process will take more time.

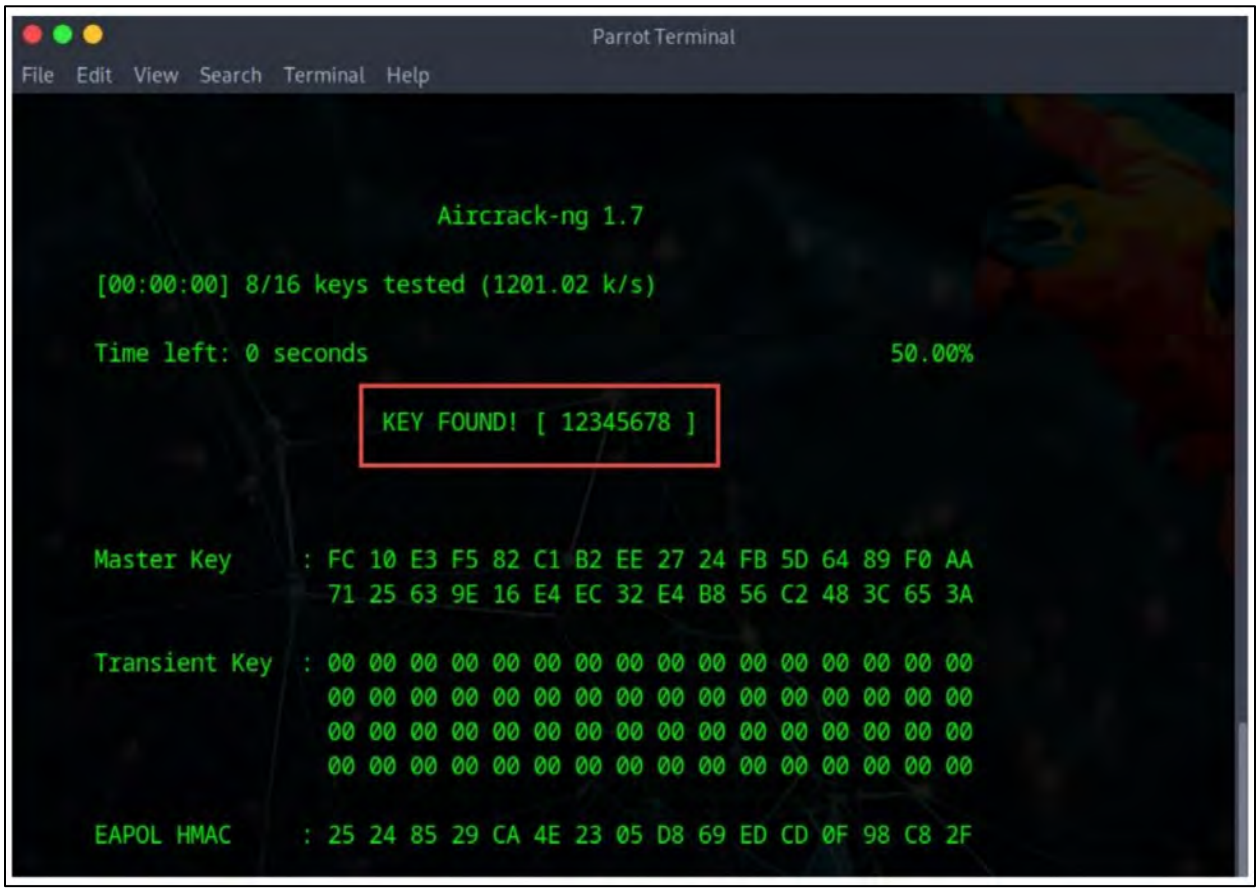


Figure 16-89: Result of aircrack-ng Cracking the WPA/WPA2 Password

The following are some of the additional WPA/WPA2 cracking tools:

- hashcat (https://hashcat.net)
- EAPHammer (https://github.com)
- Portable Penetrator (https://www.secpoint.com)
- WepCrackGui (https://sourceforge.net)
- Wifite (https://github.com)

WPA Brute Forcing Using Fern Wifi Cracker

Fern Wi-Fi Cracker is a wireless security auditing and attack tool developed in Python, utilizing the Python Qt Graphical User Interface (GUI) library. It can crack and recover WPA/WPS keys and carry out various network-based attacks on wireless and Ethernet networks.

Below are the steps to perform WPA brute-forcing:

- **Step 1**: Use the following command to launch the Fern WiFi Cracker tool:

```
sudo fern-wifi-cracker
```

- **Step 2**: Activate Monitor Mode by selecting the Wi-Fi adapter from the drop-down menu and clicking the **Monitor Mode** button.
- **Step 3**: Click the **Scan for Access Points** button to begin scanning for Wi-Fi networks, then select a target WPA/WPA2 network from the list of available networks.
- **Step 4**: Start a de-authentication attack by clicking the **Attack** button next to the target network. This will force a connected client to re-authenticate and allow the tool to capture the WPA handshake during the process.
- **Step 5**: The tool will notify you once it successfully captures the WPA handshake.
- **Step 6**: Select a wordlist file containing possible passwords to test against the captured handshake (e.g., rockyou.txt, located in /usr/share/wordlists/).
- **Step 7**: Click the **Start WPA Attack** button to test each password in the wordlist against the captured handshake. Once the correct password is identified, it will be displayed on the screen, as shown in Figure 16-90.

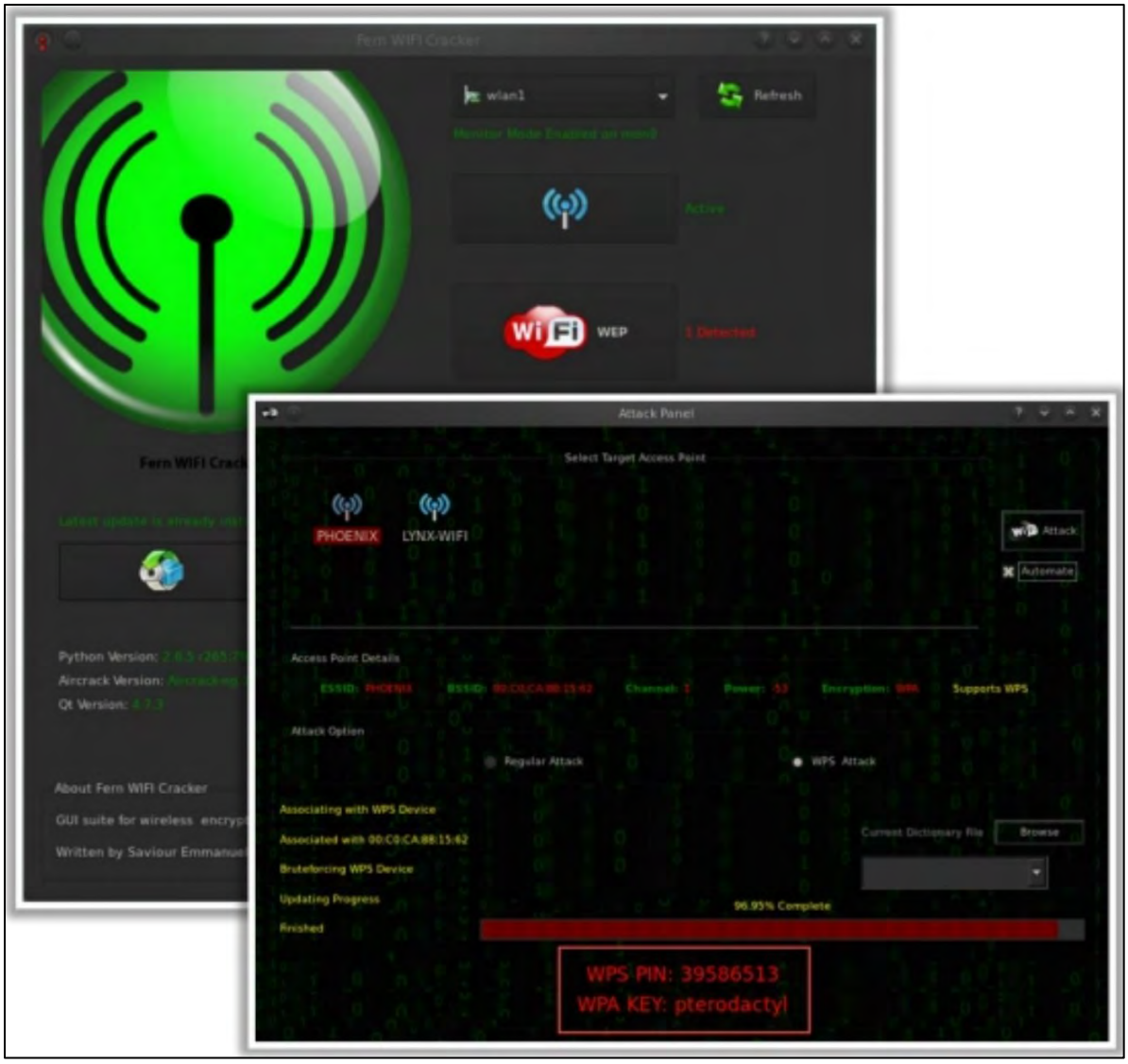


Figure 16-91: WPA2 cracking using Fern Wifi Cracker

WPA3 Encryption Cracking

The WPA3 Wi-Fi security standard replaces WPA2's four-way (PSK) handshake method with the Dragonfly (SAE) handshake to provide the most secure password-based authentication. However, it remains susceptible to password-cracking attacks. Dragonblood refers to a series of vulnerabilities within the WPA3 standard that enable attackers to recover keys, downgrade security measures, and execute various data theft attacks. Attackers can exploit these vulnerabilities using tools like Dragonslayer, Dragonforce, Dragondrain, and Dragontime to launch attacks on WPA3-enabled networks. Below are some techniques used to crack WPA3 encryption.

- **Downgrade Security Attacks**: For this attack to succeed, both the client and the access point must support WPA3 and WPA2 encryption methods. The attacker forces the user to connect to the network using the older WPA2 encryption method instead of WPA3. A downgrade security attack can be carried out in the following two ways.

- **Exploiting Backward Compatibility**: If the user and access point support WPA2 and WPA3, the attacker sets up a rogue AP that only supports WPA2. The attacker then forces the client to go through the WPA2 four-way handshake to establish a connection. Once connected, the attacker uses various attack tools to exploit or crack the WPA2 encryption.
- **Exploiting the Dragonfly Handshake**: In this method, the attacker impersonates a legitimate AP. When a user tries to exchange keys to access the internet via WPA3, the attacker informs the user that WPA3 is not supported. The attacker suggests using a weaker encryption method, such as WPA2, for internet access. Following this, the attacker can use different techniques to exploit or crack the WPA2 encryption.

- **Side-Channel Attacks (Information-Leaking Attack)**: Attackers focus on the protocols or encryption methods used by devices connecting to a network. During the key exchange process, they exploit any leaked information, which can then be used to perform brute-force or dictionary attacks to access the target user's data. A side-channel attack can be carried out in two ways:
  - **Timing-based Attack**: In this method, the attacker analyzes the time it takes for the Dragonfly handshake to encode a password authentication process. By studying the encoding iterations, the attacker can narrow down potential passwords. Once a list is formed, they attempt to access the target device using various techniques.
  - **Cache-based Attack**: The attacker injects malicious JavaScript or a web application into the target user's browser. This enables the attacker to control the browser and monitor memory access patterns to extract password information.

Cracking WPA3 Using Aircrack-ng and hashcat

The following steps outline how to crack WPA3 encryption using hcxtools to convert raw packets to hash format and hashcat to crack the handshake:

- **Step 1**: Set the wireless interface to monitor mode by running the command:

```
airmon-ng start <Wireless_Interface>
```

- **Step 2**: In another terminal, capture the handshake by running the command as the root user:

```
airodump-ng wlanomon
```

Alternatively, focus on a target network with the command:

```
airodump-ng --bssid <BSSID> --channel <CH> --write capture wlanomon
```

- **Step 3**: De-authenticate the client to capture the handshake by running:

```
aireplay-ng --deauth 10 -a <BSSID> -c <Client_MAC> wlanomon
```

This forces the client to reconnect, capturing the handshake in the process.

- **Step 4**: Convert the captured .cap file to .hccapx format using hcxtools by running:

```
hcxpcapngtool -o capture.hccapx <capture>.cap
```

- **Step 5**: Finally, crack the handshake using hashcat with a wordlist file by running:

```
hashcat -m 22000 capture.hccapx </path/to/wordlist.txt>
```

Cracking WPS Using Reaver

Reaver is a powerful and effective tool for attacking Wi-Fi Protected Setup (WPS) registrar PINs to recover WPA/WPA2 passphrases. It has been thoroughly tested against numerous Access Points (APs) and WPS implementations. The process to crack the WPS PIN using Reaver is as follows:

- Set up a wireless interface in monitoring mode using Airmon-ng with the following command:

```
airmon-ng <start|stop> <interface>
```

For instance, use

```
airmon-ng start wlano
```

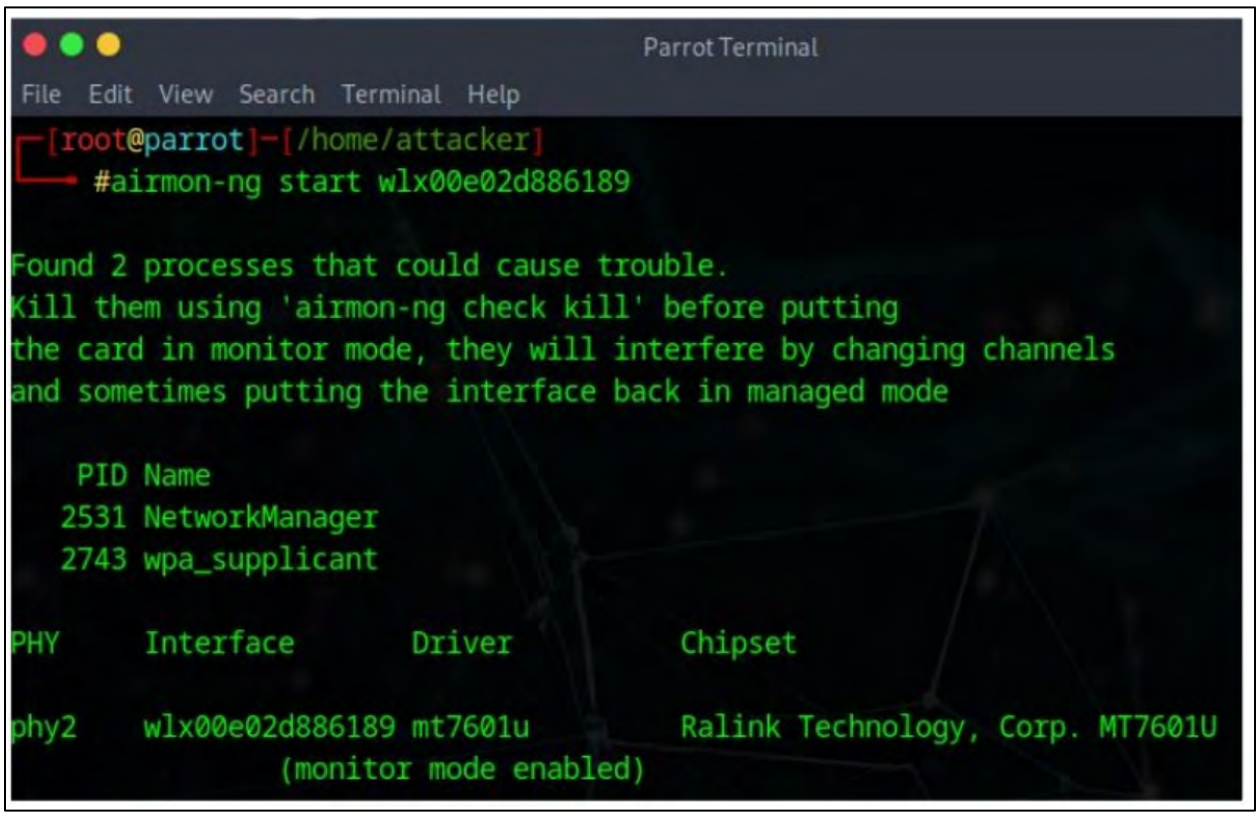


Figure 16-92: airmon-ng

- Use the Wash utility to identify WPS-enabled devices by running:

```
wash -i <interface>
```

For example:

```
wash -i mono
```

- If Wash fails to detect WPS-enabled devices, use Airodump-ng to find them with the command:

```
airodump-ng <interface>
```

For instance, if the device in monitor mode is wlanomon from the previous step, the command would be:

airodump-ng wlanomon

This will display all available BSSIDs (MAC addresses of APs).

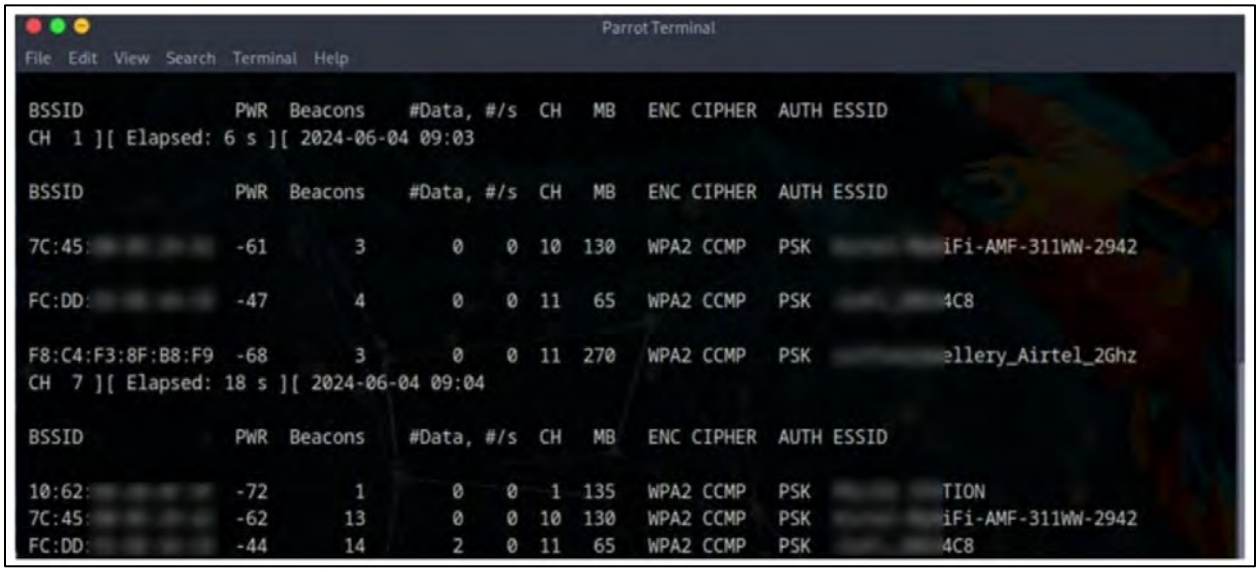


Figure 16-93: airodump-ng Showing BSSIDs

- Once you have identified the BSSID of the target device, initiate the WPS PIN cracking process with Reaver by running the following command:

reaver -i <monitor-mode interface> -b <target AP's BSSID> -vv

For example:

reaver -i wlanomon -b B4:75:0E:89:00:60 -vv

This command will scan through all available WPS PINs until it finds a matching one, after which it will begin the exploitation process.

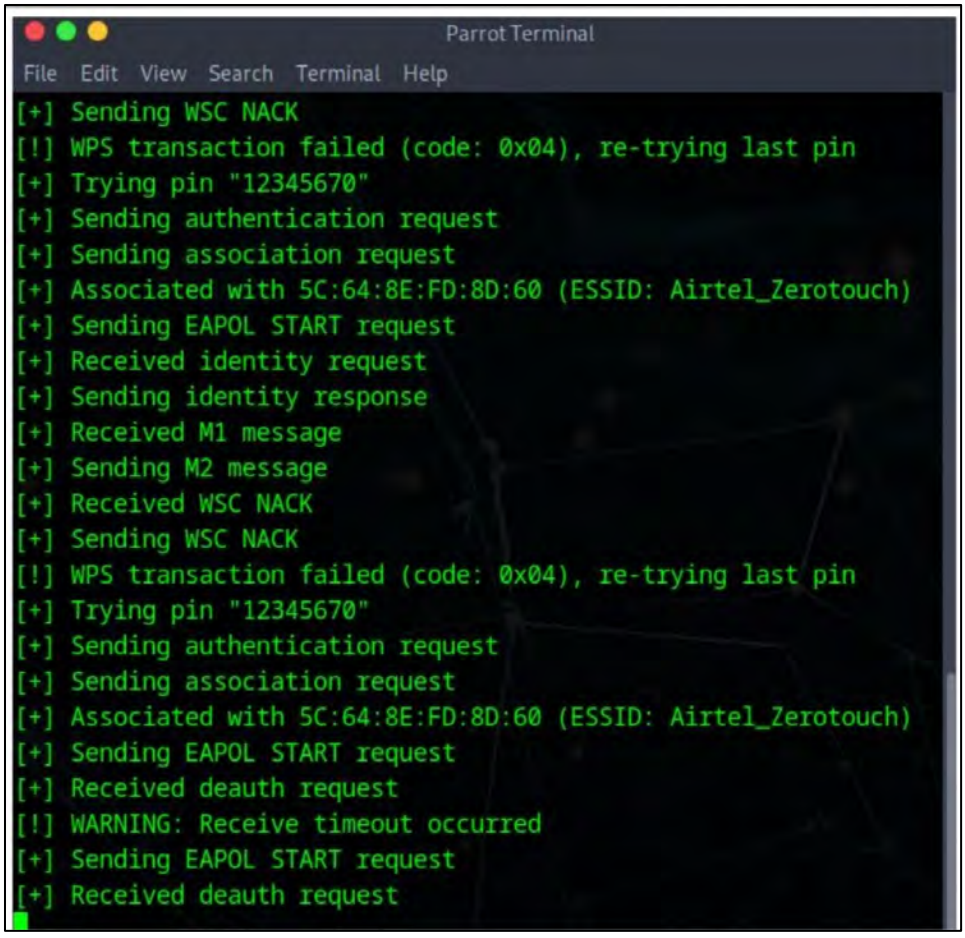


Figure 16-94: Reaver Displaying the Output

EXAM TIP: Learn the stages of wireless hacking, including Wi-Fi discovery, traffic analysis, attack launch, and encryption cracking. Understand how hackers scan for networks, capture traffic, and break weak encryptions (e.g., WEP and WPA cracking). Understand the hacking tools used (e.g., Aircrack-ng, Kismet, Wireshark) and the attack methods (e.g., dictionary attacks, brute force, etc.).

Wireless Attack Countermeasures

The earlier sections outlined how attackers compromise wireless networks to access sensitive information. Ethical hackers focus on enhancing the security of wireless networks. To safeguard a wireless network, it is crucial to implement effective countermeasures and follow recommended best practices. This section overviews these countermeasures and guidelines for ensuring wireless network security.

Wireless Security Layers

Wireless security operates through six distinct layers. This multi-layered strategy enhances the network's defenses against potential attacks. It improves the chances of detecting and apprehending an attacker. Figure 16-93 illustrates the framework of wireless security layers.

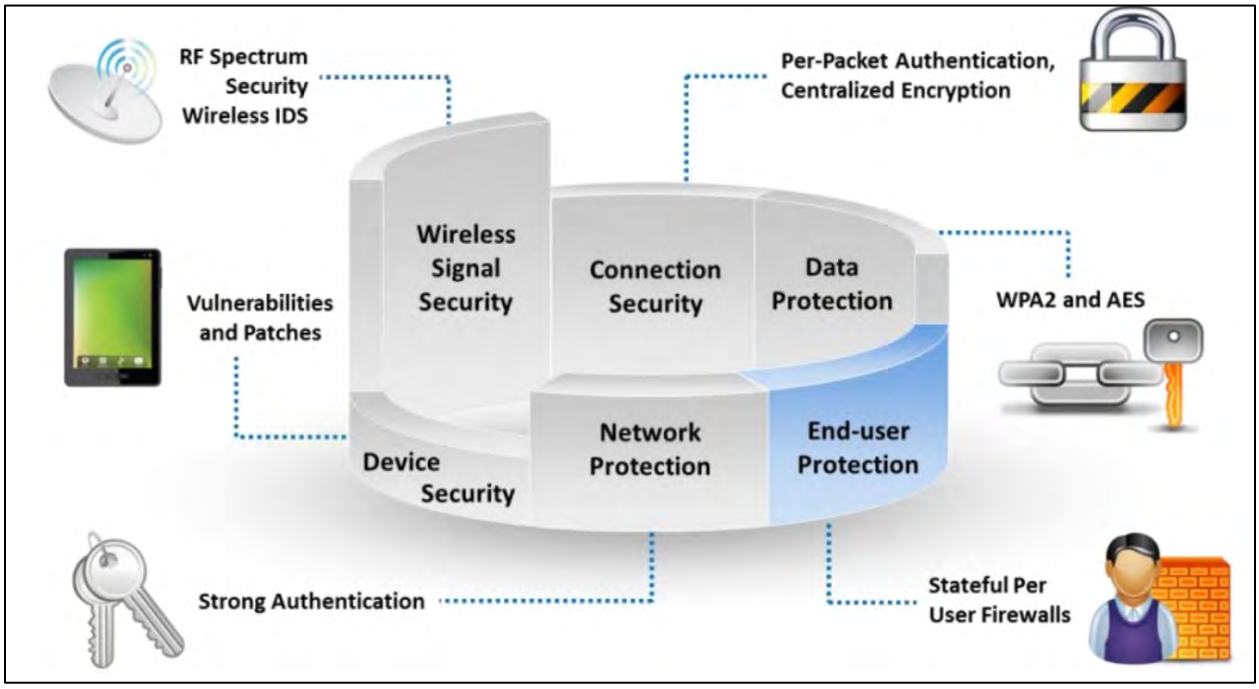


Figure 16-95: Structure of Wireless Security Layers

- **Wireless Signal Security:** In wireless networks, continuous monitoring and management of the network and RF spectrum within the environment are essential for identifying threats and enhancing awareness. A Wireless Intrusion Detection System (WIDS) analyzes and monitors the RF spectrum. It generates alerts to detect unauthorized wireless devices that breach network security policies. Signs such as increased bandwidth usage, RF interference, or rogue wireless access points can indicate a potential malicious intruder. Continuous network monitoring is crucial to prevent such attacks and ensure network security.
- **Connection Security:** Per-frame or per-packet authentication safeguards against Man-In-The-Middle (MITM) attacks. This method prevents attackers from intercepting data exchanged between legitimate users and securing communication.
- **Device Security:** Effective security infrastructure requires vulnerability and patch management to protect devices.
- **Data Protection:** Encryption protocols like WPA3, WPA2, and AES ensure the confidentiality and security of data.
- **Network Protection:** Robust authentication mechanisms ensure that only authorized users can access the network.
- **End-User Protection:** Personal firewalls installed on end-user devices in WLANs provide an additional layer of defense, preventing attackers from accessing files, even if they connect to access points.

Defense Against WPA/WPA2/WPA3 Cracking

- **Use Strong Passwords**
  - Ensure the Wi-Fi password (pre-shared key) is complex, strong, and hard to guess
  - Use a password with 12-16 characters, including uppercase and lowercase letters, numbers, and special characters
- **Client Settings**
  - Configure Wi-Fi to use WPA2 with AES/CCMP encryption exclusively
  - Set proper client configurations, such as validating the server, specifying the server address, and avoiding prompts for new servers
  - Generate new keys for each connection
- **Additional Controls**
  - Utilize VPN technologies like remote access VPN, extranet VPN, and intranet VPN
  - Implement secure communication protocols such as IPsec and SSL/TLS
  - Adopt Network Access Control (NAC) or Network Access Protection (NAP) solutions to enhance end-user connectivity controls
- **Disable TKIP**
  - Turn off TKIP in router settings and enable only AES encryption
- **MAC Address Filtering**
  - Restrict network access to devices with approved MAC addresses
- **Upgrade to WPA3**
  - Upgrade to WPA3 to prevent device exploitation and improve protection against brute-force attacks
- **Disable Remote Management**
  - Deactivate remote management features on routers to block external attacks
- **Disable WPS**
  - Turn off WPS in router settings to mitigate vulnerabilities that could lead to brute-force attacks on the WPS PIN
- **Regularly Update Router Firmware**
  - Keep router firmware up to date by patching known vulnerabilities. Check the manufacturer's website frequently for updates and apply them promptly
- **Reduce Signal Range**

- Limit Wi-Fi signal coverage to reduce unauthorized access from outside the premises. Adjust router transmission power and place it centrally within the target area

- **Monitor Network Activity**
  - Continuously monitor network activity for unusual patterns or unauthorized devices. Use network monitoring tools to identify and respond to suspicious activity
- **Enable WPA3-SAE**
  - Activate WPA3-SAE for improved security, protecting against offline dictionary attacks and providing forward secrecy. Enable it for all compatible devices
- **Disable Transition Mode**
  - Turn off WPA3's mixed WPA2/WPA3 mode if all devices support WPA3 to ensure optimal security

Defense Against KRACK Attacks

The following are some countermeasures to prevent KRACK attacks:

- Ensure all routers and Wi-Fi devices have the most recent security updates
- Activate automatic updates for all wireless devices and keep firmware patched
- Steer clear of using public Wi-Fi networks whenever possible
- Limit browsing to secure websites and avoid accessing sensitive resources on unsecured networks
- Review IoT devices and refrain from connecting them to unprotected Wi-Fi routers
- Keep the HTTPS Everywhere extension enabled at all times
- Implement two-factor authentication for additional security
- Use a VPN to encrypt data during transmission
- Opt for the WPA3 security protocol for wireless networks whenever feasible
- Turn off fast roaming and repeater mode in wireless devices to reduce susceptibility to KRACK attacks
- Utilize the EAPOL-key replay counter to ensure the access point accepts only the most recent counter value
- Switch to a wired Ethernet connection or mobile data as a backup if KRACK vulnerabilities are detected
- Replace ISP-provided routers with third-party alternatives if the former lacks adequate security updates
- Apply network segmentation to isolate critical network components from general access
- Disable the 802.11r protocol in wireless settings if seamless roaming is unnecessary, as it is vulnerable to KRACK attacks
- Use 802.1X authentication with a RADIUS server to enhance security in enterprise networks

Defense Against aLTEr Attacks

Encrypting DNS queries using appropriate security standards is the primary approach to safeguarding a network against aLTEr attacks. In partnership with Apple, Cisco has developed an

application called Cisco Security Connectors, which blocks clients from accessing unauthorized websites. This application encrypts DNS queries and processes them through the Cisco Umbrella (intelligence block) for validation. It ensures protection against hijacking at both the IP and DNS levels. Below are additional countermeasures to defend against aLTEr attacks.

- Encrypt DNS queries and rely on trusted DNS resolvers only
- Use the HTTPS protocol to resolve DNS queries
- Visit websites that exclusively use HTTPS connections
- Encrypt DNS traffic and ensure its integrity by using DNS over Transport Layer Security (TLS) or Datagram TLS (DTLS)
- Implement RFC 7858 or RFC 8310 to prevent DNS spoofing and enhance encryption and intelligent name resolution policies
- Incorporate Message Authentication Codes (MACs) into user plane packets
- Use the DNSCrypt protocol to authenticate communications between DNS clients and resolvers
- Employ tools like Zimperium on mobile devices to detect phishing and other attacks from malicious websites
- Configure HTTPS parameters, such as HTTP Strict Transport Security (HSTS), to avoid redirecting malicious sites
- Establish virtual network tunnels with endpoint authentication and integrity protection
- Upgrade to a 5G network for enhanced security
- Adopt eSIM technology to improve authentication and encryption mechanisms
- Use DNSSEC to secure DNS lookup processes and ensure the authenticity of response data
- Ensure that all LTE infrastructure components, including base stations and core network equipment, are updated with the latest firmware and software
- Regularly apply security patches provided by network equipment vendors to address known vulnerabilities
- Implement robust encryption for data transmitted over LTE networks, such as AES-256, and ensure end-to-end encryption
- Mutual authentication between User Equipment (UE) and the network is required to prevent unauthorized access
- Deploy secure SIM cards with advanced features, such as over-the-air updates and secure storage, to guard against cloning and unauthorized access
- Use location-based access controls to restrict sensitive network service access based on the geographical location of user equipment
- Protect physical network infrastructure with security measures such as surveillance, access control systems, and tamper-evident seals

Detection and Blocking of Rogue APs

Detection of Rogue APs

- **RF scanning**: Deploy APs re-purposed as RF sensors to perform packet capturing and analysis. These sensors are connected throughout the wired network to detect and alert WLAN administrators about any nearby wireless devices.

- **AP scanning**: Use APs with built-in scanning capabilities to scan neighboring APs. These devices can expose the detected data via their MIBs and web interfaces.
- **Wired-side detection**: Leverage network management software to identify rogue APs by scanning devices connected to the LAN. This involves using Telnet, SNMP, and Cisco Discovery Protocol (CDP).
- **Authorized AP comparison**: Maintain a list of authorized APs and regularly compare them with detected devices to pinpoint unauthorized APs. Tools such as the AirMagnet WiFi Analyzer can assist in this process by matching detected APs against the predefined list.
- **Signal strength analysis**: Evaluate the signal strength of detected APs to locate potentially unauthorized devices nearby. Tools like the Ekahau Survey for Wi-Fi planning and analysis effectively identify unexpected APs based on signal strength.
- **MAC address filtering**: Monitor the network for the MAC addresses of authorized APs and flag any unknown addresses. For enhanced security, use features provided by Cisco Wireless LAN Controllers, such as rogue AP detection and MAC address filtering.

Blocking of Rogue APs

- Prevent new clients from connecting to rogue APs by initiating a Denial-of-Service (DoS) attack against the unauthorized AP
- Disable the switch port to which the rogue AP is connected or physically locate and remove the unauthorized AP from the network
- Deploy Wireless Intrusion Prevention Systems (WIPS) to continuously scan the wireless spectrum for unauthorized devices and take automated actions to block them
- Use Access Control Lists (ACLs) to limit network access to approved MAC addresses only
- Enforce 802.1X authentication to ensure only verified users and devices can access the network
- Segment the network to separate critical resources from general wireless traffic
- Turn off open SSID broadcasting to minimize the chances of unauthorized connections
- Maintain a whitelist of approved MAC addresses and configure the wireless controller to block all other devices

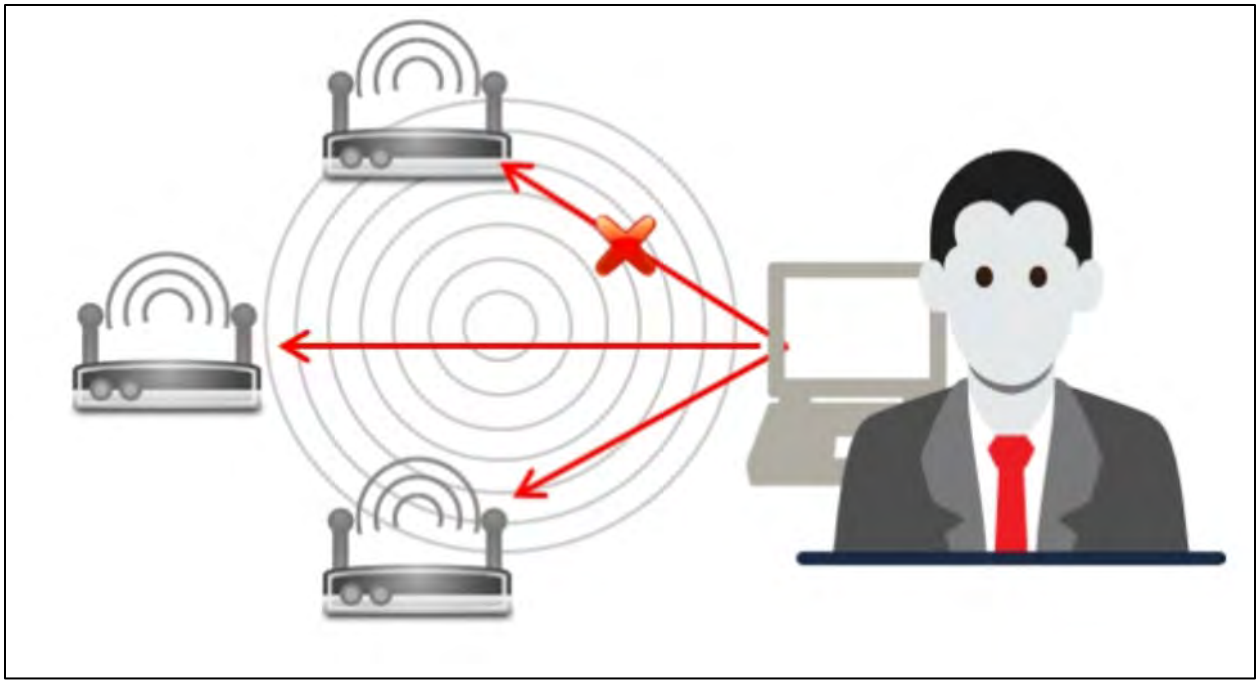


Figure 16-96: Blocking of Rogue APs

Defense Against Wireless Attacks

Best Practices for Configuration

- Change the default SSID once the WLAN setup is complete
- Set a strong router access password and enable firewall protection
- Turn off SSID broadcasting
- Disable remote router login and wireless administrative access
- Enable MAC address filtering on access points or routers
- Enable encryption on access points and update passphrases regularly
- Close any unused ports to prevent unauthorized access to access points
- Separate networks to ensure guests cannot access the private network
- Use closed networks and provide the SSID directly to employees instead of allowing them to select it from a broadcast list
- Disable Dynamic Host Configuration Protocol (DHCP) and use static IP addresses instead
- Disable Simple Network Management Protocol (SNMP), or configure it with the least privileges if necessary
- Change the router console's default IP address
- Always use WPA3 encryption when possible; if not available, use WPA2 with AES encryption
- Turn off Wi-Fi Protected Setup (WPS) on the router
- Use VLANs or separate SSIDs to isolate different types of traffic
- Adjust the router's transmission power to limit the Wi-Fi signal to the required area
- Disable unnecessary services and close unused ports
- Use the router's built-in firewall to filter both incoming and outgoing traffic
- Set up a separate guest network with limited access to the main network resources

Best Practices for SSID Settings

- Use SSID cloaking to prevent the default wireless messages from revealing the SSID to everyone
- Avoid using the SSID, company name, network name, or easily guessable strings in passphrases
- Place a firewall or packet filter between an access point and the corporate intranet
- Limit the wireless network's range to ensure it cannot be detected beyond the organization's premises
- Regularly check wireless devices for any configuration or setup issues
- Implement additional encryption techniques, such as IPsec over wireless, to protect traffic
- Modify the default SSID with unique characters and strings instead of using the manufacturer's default SSID
- Create a separate SSID for guest users to isolate them from the main network
- Divide the organizational network into multiple zones, each with its own SSID, to minimize the risk of exploitation during attacks
- Always keep the SSID broadcast for the organization's wireless devices hidden
- Ensure each SSID is secured with WPA3 encryption or at least WPA2 with AES encryption
- Periodically update SSIDs and their associated passwords

Best Practices for Authentication

- Activate WPA3 for optimal security, as it offers stronger encryption and better defense against attacks
- If WPA3 is unavailable, use WPA2 with AES encryption (avoid using WPA or TKIP)
- Implement 802.1X authentication with a RADIUS server for enterprise networks to provide unique credentials for each user
- Whenever possible, enable multifactor authentication to enhance security
- For 802.1X implementations, ensure effective digital certificate management, including strong encryption and regular certificate updates
- Disable the network when it is not in use
- Place wireless access points in secure locations
- Keep drivers for all wireless devices up to date
- Use a centralized authentication server
- Enable server verification on the client side with 802.1X authentication to prevent Man-In-The-Middle (MITM) attacks
- Activate two-factor authentication for an additional layer of protection
- Implement rogue access point detection or wireless intrusion prevention/detection systems to protect against wireless threats

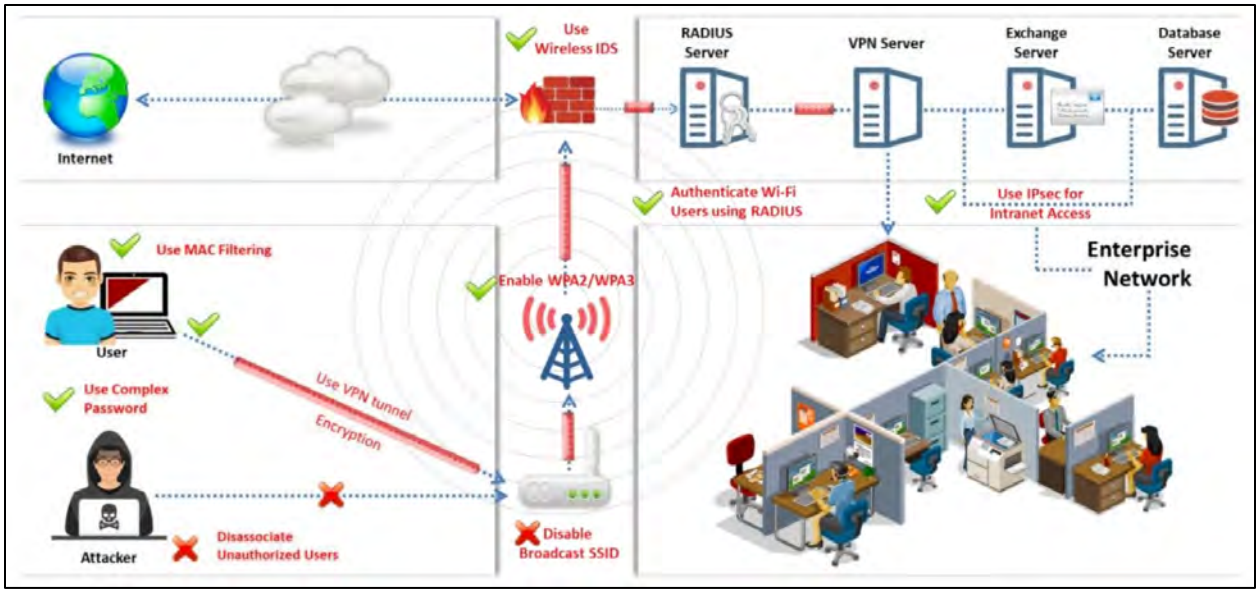


Figure 16-97: Defense Against Wireless Attacks

Wireless Intrusion Prevention Systems

A Wireless Intrusion Prevention System (WIPS) is a network device that observes the radio spectrum to identify unauthorized Access Points (APs) in nearby areas. It can also take automatic actions to counter these threats. WIPSs safeguard networks from wireless attacks and allow administrators to detect and prevent various network security issues.

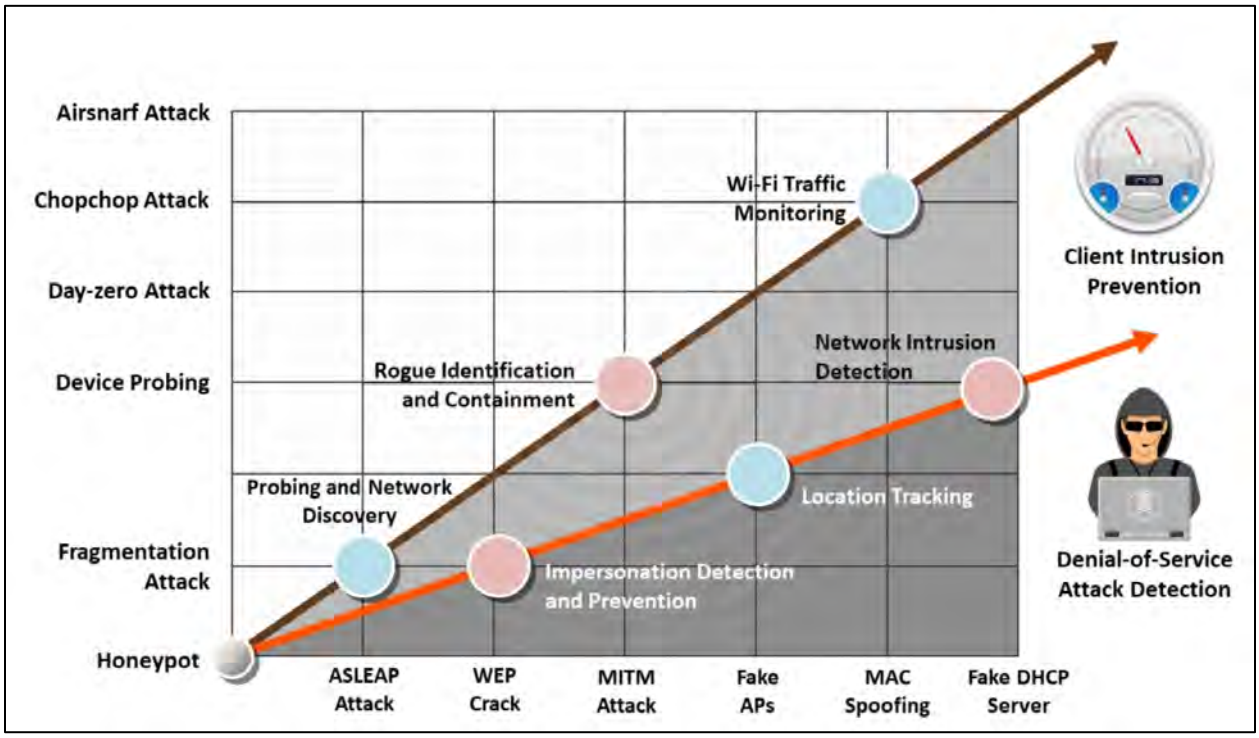


Figure 16-98: Wireless Attacks and Their Prevention Methods

WIPS Deployment

A WIPS comprises several components that collaborate to deliver comprehensive security monitoring. Cisco's WIPS setup includes the following key elements:

- **APs in monitor mode**: This mode continuously scans channels, detects attacks, and captures packets.
- **Mobility services engine (with a wireless IPS service)**: This is the central hub for aggregating alarms from controllers and wireless IPS monitor-mode APs. It stores alarm data and forensic files for later reference.
- **Local mode AP(s)**: These APs provide wireless connectivity to clients and perform rogue detection and location scanning on a time-sharing basis.
- **Wireless LAN controller(s)**: These controllers transmit attack data from wireless IPS monitor-mode APs to the MSE and distribute configuration settings to APs.
- **Wireless control system**: This system configures the wireless IPS service on the MSE, pushes configurations to the controller, and sets APs to wireless IPS monitor mode. It also provides access to wireless IPS alarms, forensics, reports, and the threat encyclopedia.

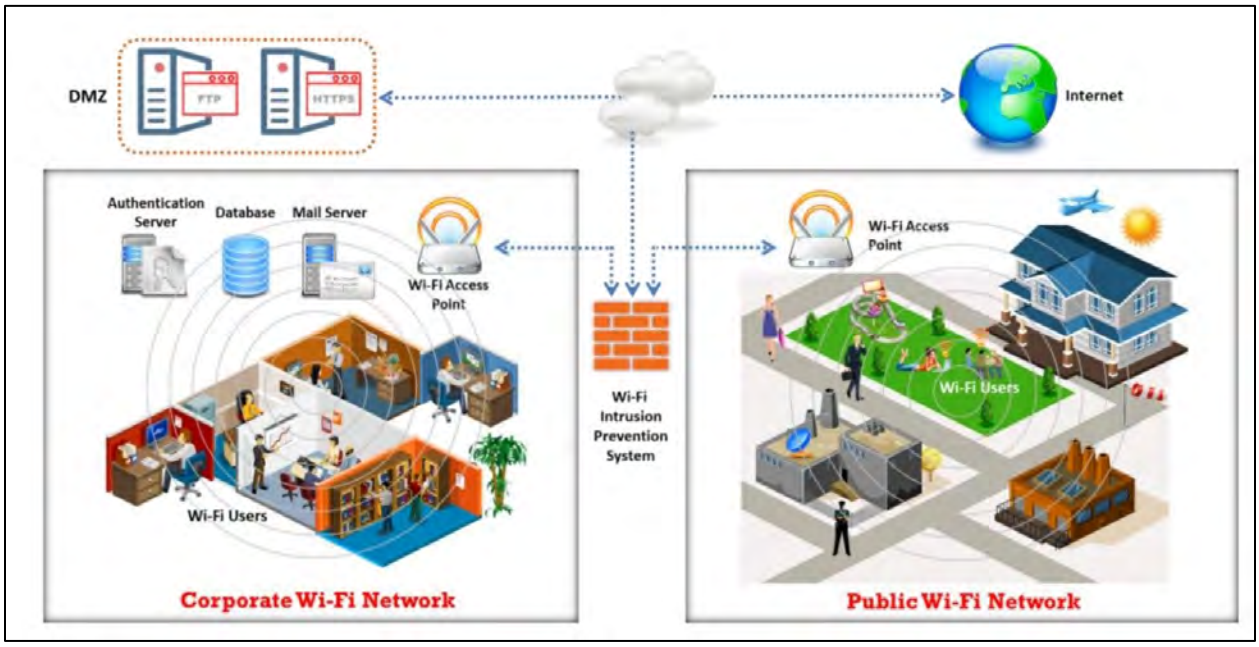


Figure 16-99: WIPS Deployment

Wi-Fi Security Auditing

Cisco Adaptive Wireless IPS

The Cisco Adaptive Wireless Intrusion Prevention System (IPS) provides advanced security for monitoring and detecting wireless network anomalies, unauthorized access, and RF attacks. Fully integrated with the Cisco Unified Wireless Network, this solution offers seamless visibility and control across the network, eliminating the need for separate solutions. Adaptive WIPS helps detect and mitigate wireless network threats, addressing malicious attacks and security vulnerabilities. It

also enables security professionals to effectively detect, analyze, and identify wireless security threats.

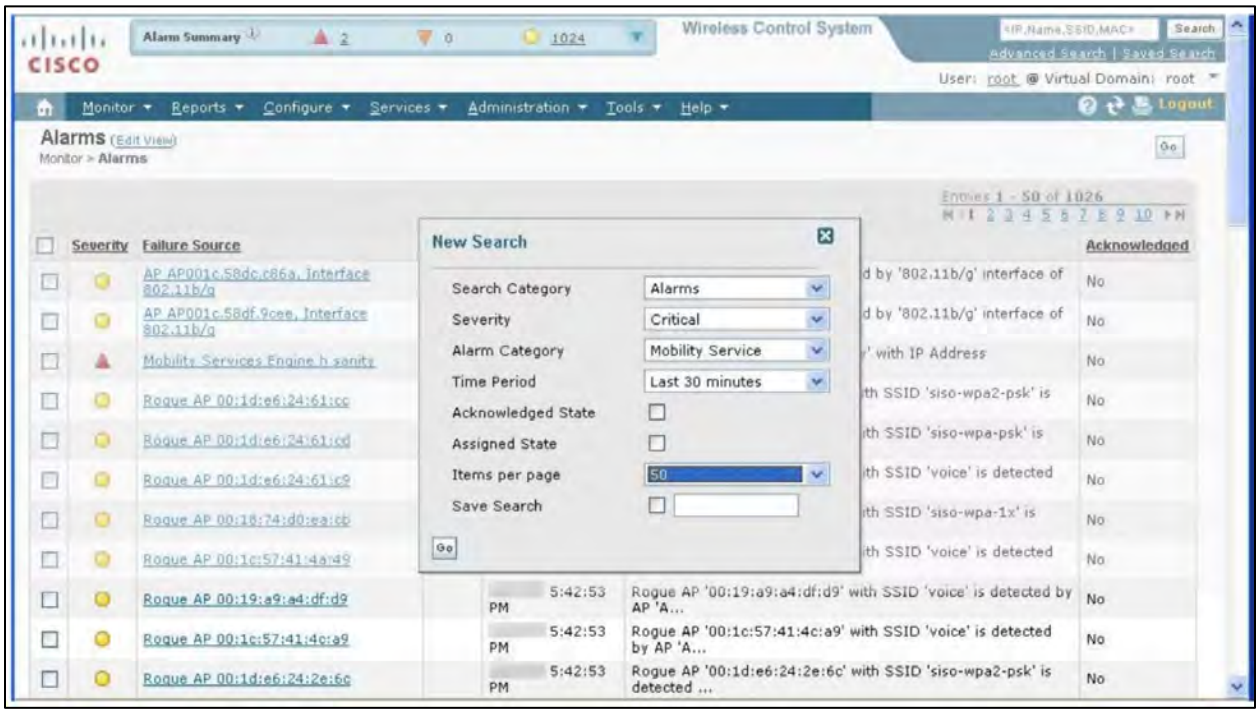


Figure 16-100: Cisco Adaptive Wireless IPS

The following are some additional Wi-Fi security auditing tools:

- RFProtect (https://www.arubanetworks.com)
- Fern Wifi Cracker (https://github.com)
- OSWA-Assistant (https://securitystartshere.org)
- BoopSuite (https://github.com)
- Wifite (https://github.com)

Wi-Fi IPSs

Wi-Fi Intrusion Prevention Systems (IPS) prevent wireless threats by automatically scanning, detecting, and categorizing unauthorized access and rogue traffic to the network. They also block skilled hackers or nearby users from gaining unauthorized access to Wi-Fi resources.

WatchGuard Wi-Fi Cloud WIPS

WatchGuard Wi-Fi Cloud WIPS protects against unauthorized devices and rogue access points, stops evil twin attacks, and defends against malicious attacks like DoS, all while maintaining high-performance wireless connectivity and minimizing false positives.

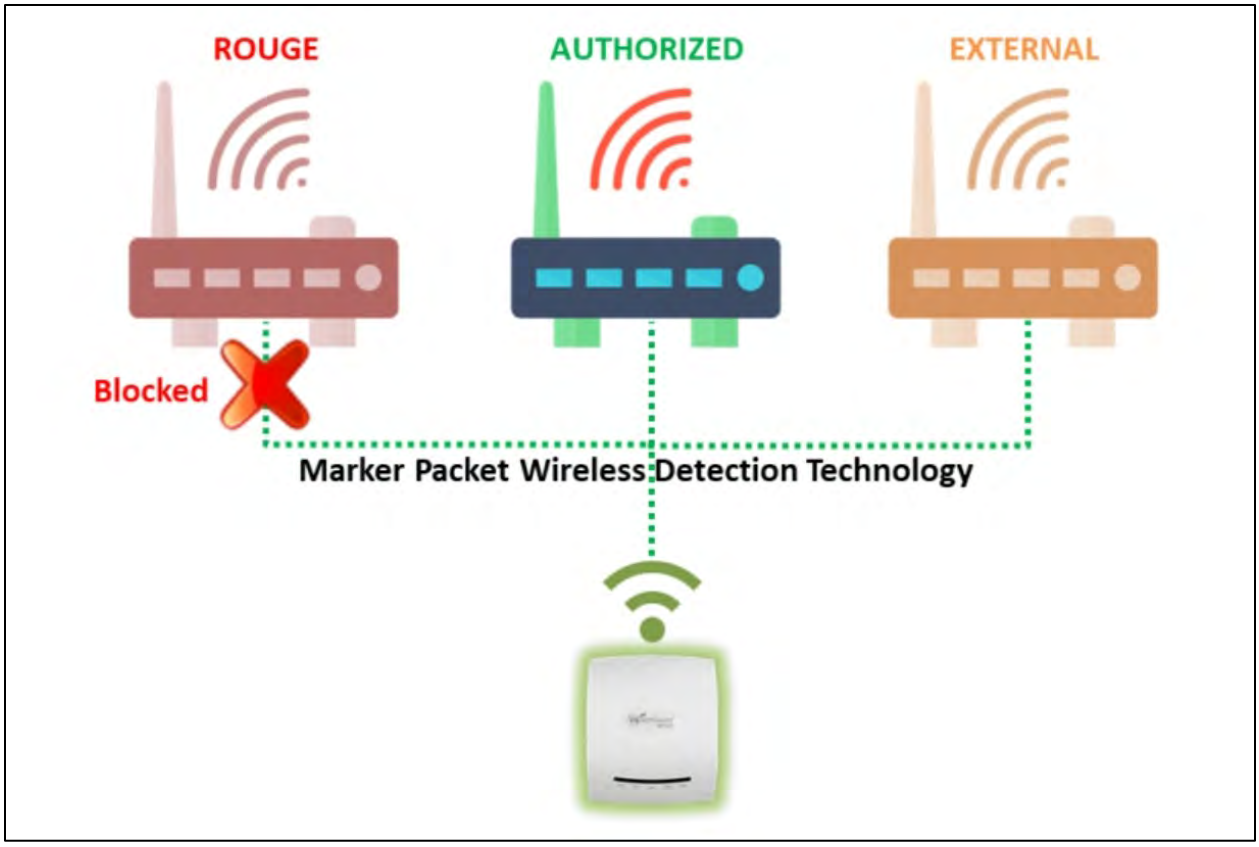


Figure 16-101: Conceptual Diagram of WatchGuard WIPS

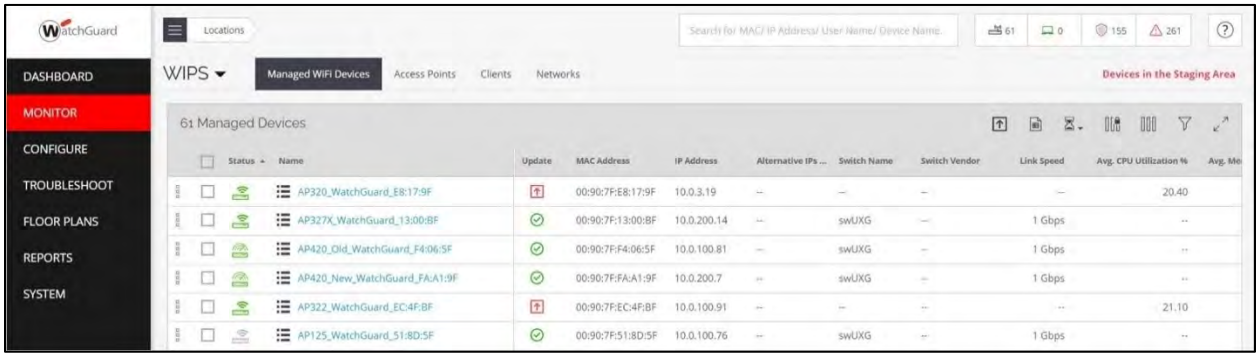


Figure 16-102: WatchGuard Wi-Fi Cloud WIPS

The following are some additional wireless intrusion prevention tools:

- Extreme AirDefense (https://www.extremenetworks.com)
- Arista WIPS (https://www.arista.com)
- SonicWall Wireless Network Manager (https://www.sonicwall.com)
- Cisco Meraki (https://www.cisco.com)
- FortiGate Next-Generation Firewall (NGFW) (https://www.fortinet.com)

EXAM TIP: Gain a clear understanding of the security layers in Wi-Fi networks. Review defense strategies to protect against WPA/WPA2/WPA3 cracking, such as using strong passwords

and adopting the latest security protocols. Familiarize yourself with attacks like KRACK and aLTEr and their corresponding mitigation techniques. Lastly, explore the role of Wireless Intrusion Prevention Systems (WIPS) and Wi-Fi Intrusion Prevention Systems (IPS) in detecting and blocking potential threats.

Summary

This chapter covered the fundamentals of wireless networks and explored various wireless encryption technologies. We also examined wireless threats and the methods used in wireless hacking, including Wi-Fi discovery, traffic analysis, attack execution, and encryption cracking. The chapter provided an overview of several wireless hacking tools and discussed countermeasures to protect wireless networks from potential attacks by threat actors. Lastly, we focused on securing wireless networks through wireless security tools.

Mind Map

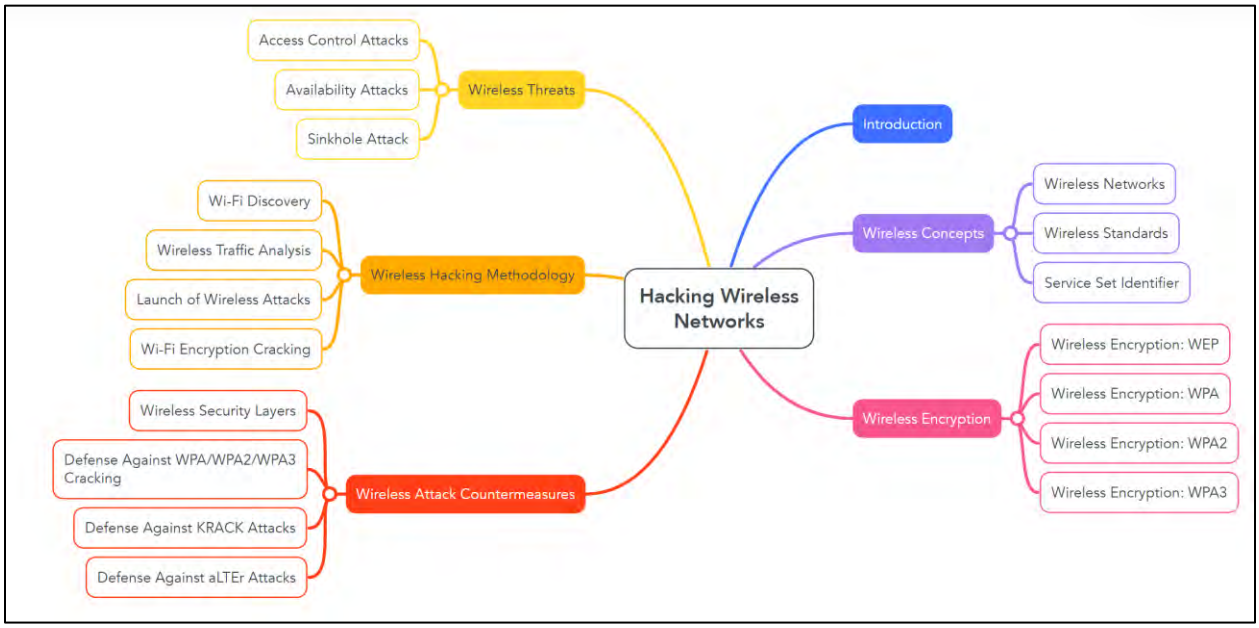


Figure 16-103: Mind Map

Practice Questions

1. Which of the following is a standard for mobile data transmission used worldwide in wireless networks?
A. Wi-Fi
B. GSM
C. Bluetooth
D. ZigBee

2. What is the primary function of an Access Point (AP) in a wireless network?
A. To amplify the signal of a router.

B. To connect wireless devices to a wired or wireless network.
C. To manage the bandwidth of the network.
D. To regulate the power output of a network.

3. What is the main advantage of using 802.11ax (Wi-Fi 6) over older Wi-Fi standards?
A. Faster speeds and better efficiency in high-density areas.
B. Enhanced security through WPA2 encryption.
C. Compatibility with older Wi-Fi standards.
D. Support for devices operating in the 2.4 GHz frequency band.

4. Which of the following wireless encryption protocols uses the RC4 stream cipher for encryption?
A. WEP
B. WPA2
C. WPA3
D. AES

5. What is the main difference between WPA/WPA2-Personal and WPA/WPA2-Enterprise?
A. WPA2-Enterprise uses a pre-shared key, while WPA/PWA-Personal does not.
B. WPA/WPA2-Personal uses a centralized RADIUS server, while WPA/WPA2-Enterprise does not.
C. WPA/WPA2-Enterprise uses a centralized RADIUS server for authentication, while WPA/WPA2-Personal relies on a pre-shared key.
D. WPA/WPA2-Personal supports multiple authentication methods, while WPA2-Enterprise uses just one.

6. Which type of antenna is best suited for transmitting weak Wi-Fi signals over long distances?
A. Directional Antenna
B. Omnidirectional Antenna
C. Parabolic Grid Antenna
D. Yagi Antenna

7. What encryption algorithm is used in WPA2 for wireless network security?
A. RC4
B. AES
C. DES
D. RSA

8. Which of the following is a key feature introduced by WPA3 that enhances security over WPA2?
A. Use of RC4 encryption
B. Simultaneous Authentication of Equals (SAE)
C. Support for legacy protocols
D. 40-bit encryption

9. What is a significant vulnerability of WEP encryption?
A. Limited IV size of 24 bits
B. AES-CCMP encryption

C. Use of RSA for key management
D. Protection against brute force attacks

10. What is the primary risk associated with MAC spoofing in wireless networks?
A. Unauthorized access due to weak passwords.
B. The attacker can impersonate a trusted AP and gain unauthorized access.
C. Exploiting AP misconfigurations to manipulate network traffic and gain access.
D. Data interception through promiscuous client attacks.

11. Which of the following is a common configuration error that increases security risks in wireless networks?
A. Disabling SSID broadcasts
B. Using strong encryption methods like WPA2
C. Broadcasting SSIDs and using weak passwords
D. Activating WPA3 encryption

12. What is a key characteristic of an "ad hoc mode" attack in wireless networks?
A. Attackers exploit misconfigured AP settings.
B. Attackers manipulate ad hoc connections to gain unauthorized access.
C. The attack uses strong encryption protocols to secure the connection.
D. Attackers use rogue APs to create a stronger signal to lure clients.

13. What is the main goal of an availability attack on wireless networks?
A. To capture login credentials from users.
B. To disrupt wireless services and prevent legitimate users from accessing resources.
C. To manipulate AP settings and exploit vulnerabilities to compromise network availability.
D. To eavesdrop on communication between nodes.

14. How does a honeypot AP attack work in wireless networks?
A. By setting up a rogue AP that emits a stronger beacon signal than legitimate ones, tricking users into connecting.
B. By exploiting weak encryption protocols to gain unauthorized access.
C. By manipulating network protocols to redirect user traffic through a malicious access point for interception.
D. By launching a denial-of-service attack on legitimate APs.

15. In a wormhole attack, what do attackers use as the primary method to compromise the wireless network?
A. Redirecting the communication through a malicious node to manipulate routing.
B. Using weak passwords to gain unauthorized access to networks.
C. Creating a fake AP to impersonate legitimate devices.
D. Overloading the network with traffic to prevent legitimate access.

16. Which tools are commonly used for detecting nearby Wi-Fi networks and visualizing their signal strengths?
A. Wireshark
B. inSSIDer
C. NetSpot

D. Riverbed Packet Analyzer

17. What is the primary difference between passive and active footprinting methods in wireless network attacks?
A. Passive footprinting involves connecting to the network, while active footprinting does not.
B. Passive footprinting captures packets without connecting to the network, while active footprinting requires sending probe requests to discover SSIDs.
C. Passive footprinting uses drones for detection, while active footprinting uses mobile devices.
D. Active footprinting requires physical proximity to the network, while passive footprinting does not.

18. Which of the following is a common tool used by attackers to perform sniffing and analyze wireless traffic?
A. Kismet
B. NetSurveyor
C. Acrylic WiFi Heatmaps
D. Sparrow-WiFi

19. What is the primary consideration when selecting a Wi-Fi card for Wi-Fi hacking?
A. The brand and model of the card.
B. The operating system used by the attacker.
C. The Wi-Fi card's chipset and its capabilities.
D. The size of the Wi-Fi card.

20. What is the primary function of tools like RF Explorer in Wi-Fi hacking?
A. To inject packets into a network.
B. To monitor and analyze RF spectrum usage.
C. To crack WEP and WPA encryption.
D. To identify hidden SSIDs.

21. What is the purpose of using mdk3 in uncovering a hidden SSID?
A. To scan for all available Wi-Fi networks.
B. To perform a brute-force attack on the hidden SSID.
C. To decode encrypted traffic.
D. To change the BSSID of the access point.

22. What is the primary goal of a Denial-of-Service (DoS) attack on wireless networks?
A. To intercept sensitive data
B. To disrupt network communication by disconnecting clients from the access point
C. To manipulate the destination address of data packets
D. To overwhelm the network with excessive traffic, making resources unavailable to legitimate users.

23. In a Man-in-the-Middle (MITM) attack, what does the attacker do once the victim connects to a fake access point?
A. Redirects the traffic to another network.
B. Forces the victim to disconnect from the network and attempt to reconnect to a rogue access point.

C. Intercepts and manipulates the network traffic between the victim and the real access point.
D. Encrypts the traffic to prevent detection.

24. What is the purpose of a MAC spoofing attack in wireless networks?
A. To decrypt encrypted network traffic.
B. To bypass MAC address filtering by impersonating an authorized device.
C. To intercept wireless traffic without detection.
D. To manipulate access control mechanisms and evade network security measures.

25. Which attack targets the WPA2 protocol's four-way handshake to access sensitive data like passwords and credit card numbers?
A. Wi-Jacking Attack
B. Evil Twin Attack
C. Key Reinstallation Attack (KRACK)
D. aLTEr Attack

Answers

1. Answer: B
Explanation: Global System for Mobile Communications (GSM) is a universal standard for transmitting mobile data and is widely used in wireless networks globally.

2. Answer: B
Explanation: An Access Point (AP) bridges the connection between wireless devices and a wired or wireless network, enabling devices to communicate with the network.

3. Answer: A
Explanation: 802.11ax, or Wi-Fi 6, improves upon previous standards by offering faster speeds (up to 9.6 Gbps) and efficiently managing multiple simultaneous connections, making it ideal for high-density areas like stadiums or airports.

4. Answer: A
Explanation: Wired Equivalent Privacy (WEP) uses the RC4 stream cipher for encryption, which has significant vulnerabilities that make it less secure than newer protocols like WPA2 and WPA3.

5. Answer: C
Explanation: WPA/WPA2-Enterprise (802.1X) uses a centralized RADIUS server for authentication, managing individual credentials for each user, while WPA/WPA2-Personal uses a shared pre-shared key for device authentication.

6. Answer: C
Explanation: The Parabolic Grid Antenna is designed to transmit Wi-Fi signals over long distances by focusing the radio beams. It is ideal for long-range communication (up to 10 miles), even though it is more susceptible to interference.

7. Answer: B

Explanation: WPA2 uses the AES encryption algorithm, which is compliant with NIST's FIPS 140-2 standard and provides robust encryption for wireless networks.

8. Answer: B
Explanation: WPA3 replaces WPA2's Pre-Shared Key (PSK) method with SAE, which provides stronger protection against offline dictionary attacks and ensures better security.

9. Answer: A
Explanation: WEP's 24-bit Initialization Vector (IV) is too small, leading to IV collisions, which attackers can exploit to reconstruct the encryption keystream and decrypt messages.

10. Answer: B
Explanation: In MAC spoofing, the attacker manipulates their device's MAC address to impersonate an authorized Access Point (AP), tricking the network into granting access.

11. Answer: C
Explanation: Broadcasting SSIDs and using weak passwords are common configuration errors that can make networks vulnerable to attacks, especially when default SSIDs are left unchanged, making them easy targets.

12. Answer: B
Explanation: Ad hoc mode allows direct client-to-client connections without an access point, which attackers can exploit to bypass security and gain unauthorized access to the network.

13. Answer: B
Explanation: Availability attacks aim to hinder the accessibility of wireless network services by overwhelming resources or denying users access, preventing legitimate use.

14. Answer: A
Explanation: In a honeypot AP attack, the attacker sets up a rogue access point with the same SSID as the target network and a stronger signal. Users unknowingly connect to it, exposing sensitive information.

15. Answer: A
Explanation: In a wormhole attack, the attacker creates a tunnel between two nodes, manipulating routing protocols to intercept and control the data flow between source and destination nodes, compromising network communication.

16. Answer: B
Explanation: inSSIDer is a tool designed for Wi-Fi troubleshooting and optimization. It scans for nearby wireless networks and provides detailed information, including signal strengths and channel usage, which is essential for attackers identifying potential targets for Wi-Fi attacks.

17. Answer: B
Explanation: In passive footprinting, the attacker listens to wireless signals and captures packets to gather network information without directly interacting with the network. In contrast, active footprinting requires sending requests to the access point to obtain SSIDs.

18. Answer: A
Explanation: Kismet is a popular wireless network detector and sniffer attacker that captures wireless traffic, including SSIDs, MAC addresses, and encryption types. It supports sniffing and analyzing network traffic to plan further attacks.

19. Answer: C
Explanation: The chipset is crucial for selecting the optimal Wi-Fi card because it determines the supported operating system, necessary drivers, and the card's capabilities, such as listening or packet injection, which are essential for Wi-Fi hacking.

20. Answer: B
Explanation: RF Explorer and similar tools monitor and analyze the RF spectrum, detect interference, and measure signal power, which is critical for identifying target networks and analyzing wireless systems.

21. Answer: B
Explanation: mdk3 performs a brute-force attack to uncover a hidden SSID by sending de-authentication packets to force the access point to reveal its SSID.

22. Answer: B
Explanation: A DoS attack typically involves broadcasting de-authentication or disassociation messages, forcing clients to disconnect from the access point, disrupting communication, and causing downtime.

23. Answer: C
Explanation: In an MITM attack, once the victim connects to the fake access point, the attacker places themselves between the victim and the real access point, intercepting and potentially manipulating the network traffic.

24. Answer: B
Explanation: In a MAC spoofing attack, the attacker changes their device's MAC address to match that of an authorized device, bypassing MAC address filtering and gaining unauthorized access to the network.

25. Answer: C
Explanation: KRACK exploits vulnerabilities in the WPA2 protocol's four-way handshake by forcing the reuse of the Nonce value, enabling attackers to manipulate cryptographic messages and access sensitive data.