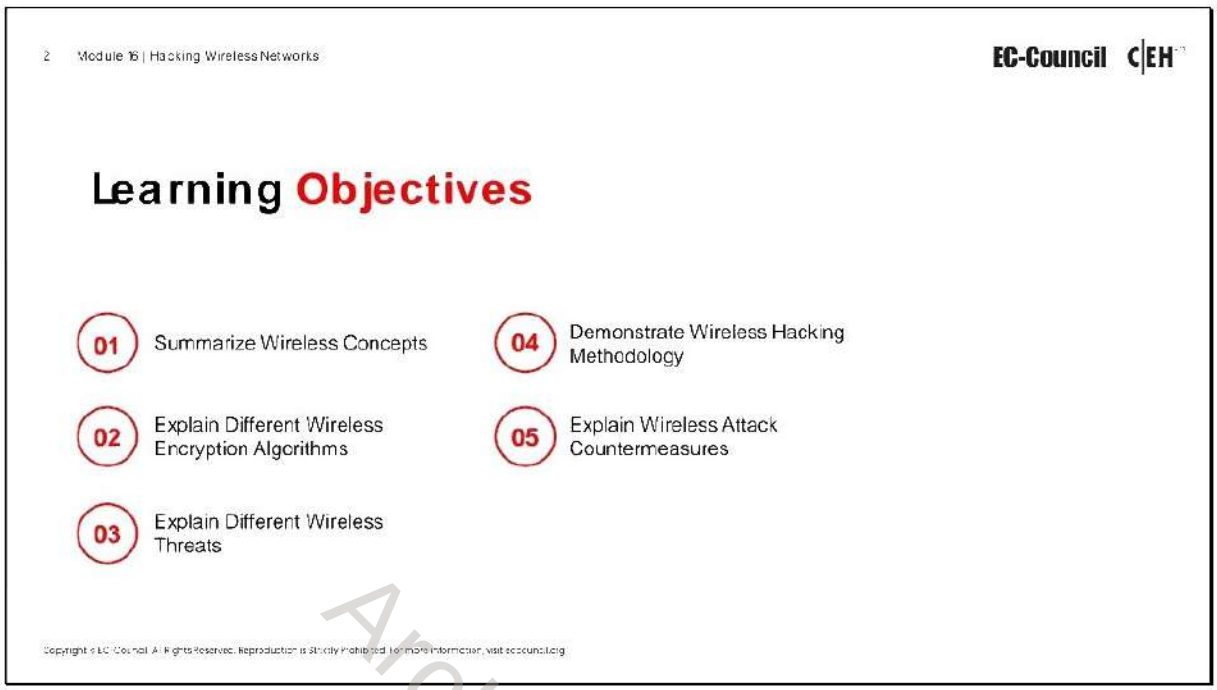
Module 16

Hacking Wireless Networks

EC-Council
Official Curricula

EC-Council C|EH™ Certified Ethical Hacker



Learning Objectives

Wireless networks are cheaper and easier to maintain than wired networks. An attacker can easily compromise a wireless network without proper security measures or an appropriate network configuration. Because high-security mechanisms for wireless networks may be expensive, it is advisable to determine critical sources, risks, or vulnerabilities associated with the network and then check whether the current security mechanism can protect the wireless network against all possible attacks. If not, the security mechanisms must be upgraded.

This module describes the types of wireless networks, their security mechanisms, threats, and measures to combat the threats to keep the network secure. Various wireless encryption algorithms are analyzed with their strengths and weakness. The module also analyzes wireless-network attack techniques and discusses countermeasures to protect information systems.

At the end of this module, you will be able to do the following:

- Describe wireless concepts
- Explain different wireless encryption algorithms
- Describe wireless threats
- Describe wireless hacking methodology
- Use different wireless hacking tools
- Apply wireless hacking countermeasures
- Use different wireless security tools

Wireless Concepts

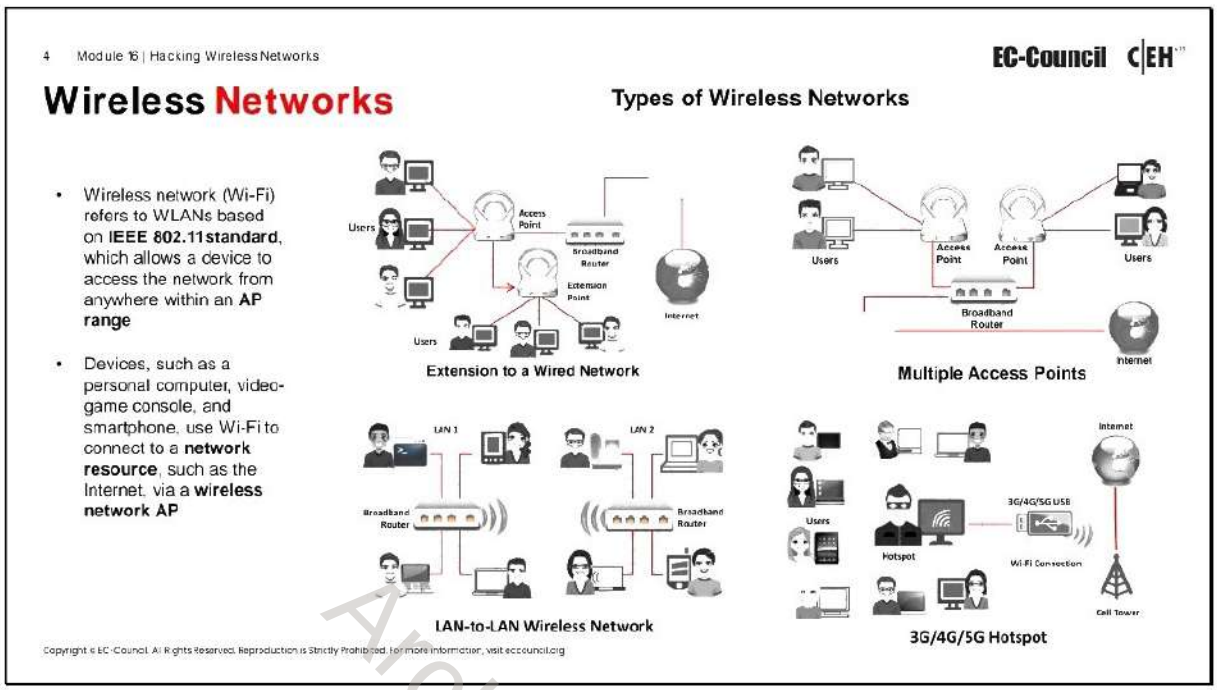
Network technology is heading toward a new era of technological evolution through wireless technologies. Wireless networking is revolutionizing the way people work and play. By removing physical connections or cables, individuals can use networks in new ways to make data portable, mobile, and accessible. A wireless network is an unbounded data communication system that uses radio-frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections using electromagnetic (EM) waves to interconnect two individual points without establishing any physical connection. This section will describe basic wireless concepts.

Wireless Terminology

In a wireless network, data are transmitted through EM waves that carry signals over the communication path. Terms associated with wireless networks include the following:

- **Global System for Mobile Communications (GSM)**: It is a universal system used for mobile data transmission in wireless networks worldwide.
- **Bandwidth**: It describes the amount of information that may be broadcast over a connection. Usually, bandwidth refers to the data transfer rate and is measured in bits (amount of data) per second (bps).
- **Access point (AP)**: An AP is used to connect wireless devices to a wireless/wired network. It allows wireless communication devices to connect to a wireless network through wireless standards such as Bluetooth and Wi-Fi. It serves as a switch or hub between a wired LAN and wireless network.

- **Basic service set identifier (BSSID)**: It is the media access control (MAC) address of an access point (AP) or base station that has set up a basic service set (BSS). Generally, users are unaware of the BSS to which they belong. When a user moves a device, the BSS used by the device could change because of a variation in the range covered by the AP, but this change may not affect the connectivity of the wireless device.
- **Industrial, scientific, and medical (ISM) band**: This band is a set of frequencies used by the international industrial, scientific, and medical communities.
- **Hotspot**: These are places where wireless networks are available for public use. Hotspots refer to areas with Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the Internet.
- **Association**: It refers to the process of connecting a wireless device to an AP.
- **Service set identifier (SSID)**: An SSID is a 32-alphanumeric-character unique identifier given to a wireless local area network (WLAN) that acts as a wireless identifier of the network. The SSID permits connections to the desired network among available independent networks. Devices connecting to the same WLAN should use the same SSID to establish connections.
- **Orthogonal frequency-division multiplexing (OFDM)**: An OFDM is a method of digital modulation of data in which a signal, at a chosen frequency, is split into multiple carrier frequencies that are orthogonal (occurring at right angles) to each other. OFDM maps information on the changes in the carrier phase, frequency, amplitude, or a combination of these and shares bandwidth with other independent channels. It produces a transmission scheme that supports higher bit rates than parallel channel operation. It is also a method of encoding digital data on multiple carrier frequencies.
- **Multiple input, multiple output-orthogonal frequency-division multiplexing (MIMO-OFDM)**: MIMO-OFDM influences the spectral efficiency of 4G and 5G wireless communication services. Adopting the MIMO-OFDM technique reduces interference and increases the channel robustness.
- **Direct-sequence spread spectrum (DSSS)**: DSSS is a spread spectrum technique that multiplies the original data signal with a pseudo-random noise-spreading code. Also referred to as a data transmission scheme or modulation scheme, the technique protects signals against interference or jamming.
- **Frequency-hopping spread spectrum (FHSS)**: FHSS, also known as frequency-hopping code-division multiple access (FH-CDMA), is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels. It decreases the efficiency of unauthorized interception or jamming of telecommunications. In FHSS, a transmitter hops between available frequencies using a specified algorithm in a pseudorandom sequence known to both the sender and receiver.



Wireless Networks

Wireless networks use radio-wave transmission, which usually occurs at the physical layer of the network structure. With the global wireless communication revolution, data networking and telecommunication are fundamentally changing. Wi-Fi refers to a WLAN based on the IEEE 802.11 standard, and it allows a device to access the network from anywhere within the range of an AP. Wi-Fi is a widely used technology in wireless communication across a radio channel. Wi-Fi utilizes numerous techniques such as DSSS, FHSS, infrared (IR), and OFDM to establish a connection between a transmitter and receiver. Devices such as personal computers, video-game consoles, and smartphones use Wi-Fi to connect to a network resource such as the Internet via a wireless network AP.

The following are some of the advantages and disadvantages of wireless networks:

- **Advantages**
  - Installation is fast and easy without the need for wiring through walls and ceilings
  - Easily provides connectivity in areas where it is difficult to lay cables
  - The network can be accessed from anywhere within the range of an AP
  - Public spaces such as airports, libraries, schools, and even coffee shops offer constant Internet connections through WLANs
- **Disadvantages**
  - Security may not meet expectations
  - The bandwidth suffers as the number of devices in the network increases
  - Wi-Fi upgrades may require new wireless cards and/or APs
  - Some electronic equipment can interfere with Wi-Fi networks

Types of Wireless Networks

The different types of wireless networks are described as follows.

- **Extension to a Wired Network**

  A user can extend a wired network by placing APs between a wired network and wireless devices. A wireless network can also be created using an AP.

  The types of APs include the following:

  - **Software APs (SAPs)**: SAPs can be connected to a wired network, and they run on a computer equipped with a wireless network interface card (NIC).
  - **Hardware APs (HAPs)**: HAPs support most wireless features.

  In this type of network, the AP acts as a switch, providing connectivity for computers that use a wireless NIC. The AP can connect wireless clients to a wired LAN, which allows wireless access to LAN resources such as file servers and Internet connections.

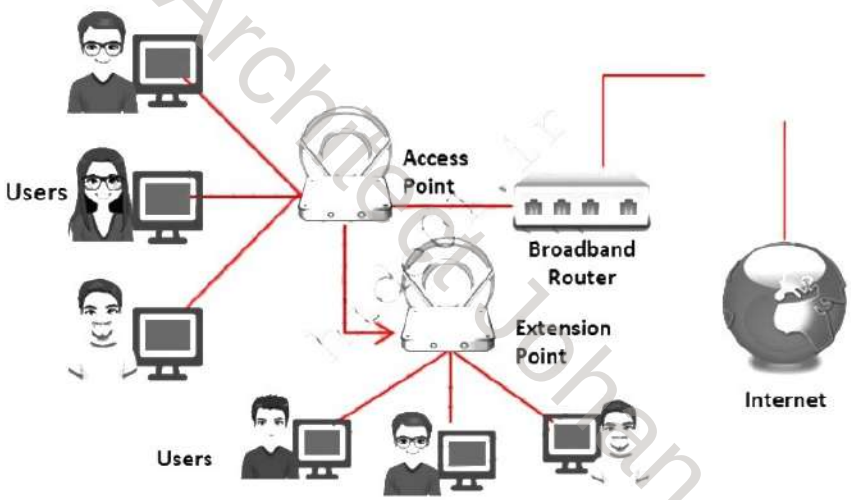


Figure 16.1: Extension to a wired network

- **Multiple Access Points**

  This type of network connects computers wirelessly using multiple APs. If a single AP cannot cover an area, multiple APs or extension points can be established.

  The wireless area of each AP must overlap its neighbor's area. This provides users the ability to move around seamlessly using a feature called roaming. Some manufacturers develop extension points that act as wireless relays, extending the range of a single AP. Multiple extension points can be strung together to provide wireless access to locations far from the central AP.

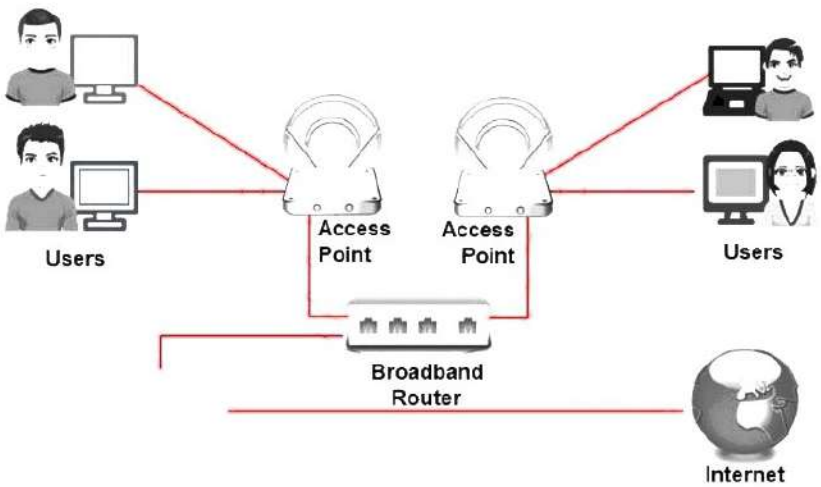


Figure 16.2: Multiple access points

- **LAN-to-LAN Wireless Network**

  APs provide wireless connectivity to local computers, and local computers on different networks can be interconnected. All hardware APs have the capability to interconnect with other hardware APs. However, interconnecting LANs over wireless connections is a complex task.

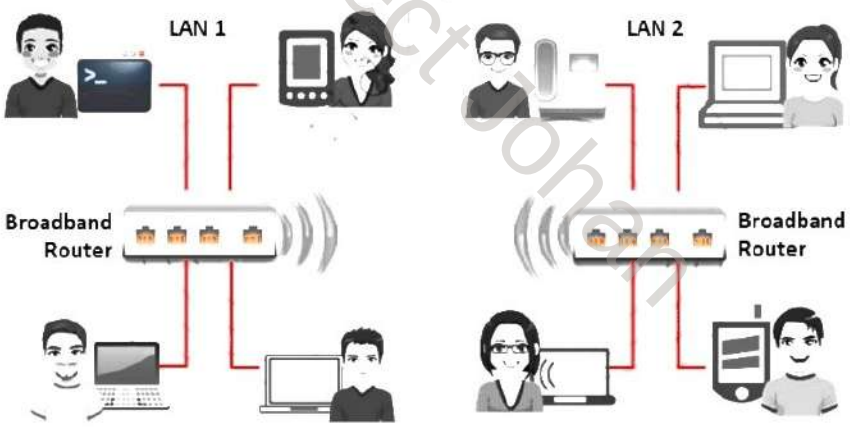


Figure 16.3: LAN-to-LAN wireless network

- **3G/4G/5G Hotspot**

  A 3G/4G/5G hotspot is a type of wireless network that provides Wi-Fi access to Wi-Fi-enabled devices, including MP3 players, notebooks, tablets, cameras, PDAs, netbooks, and more.

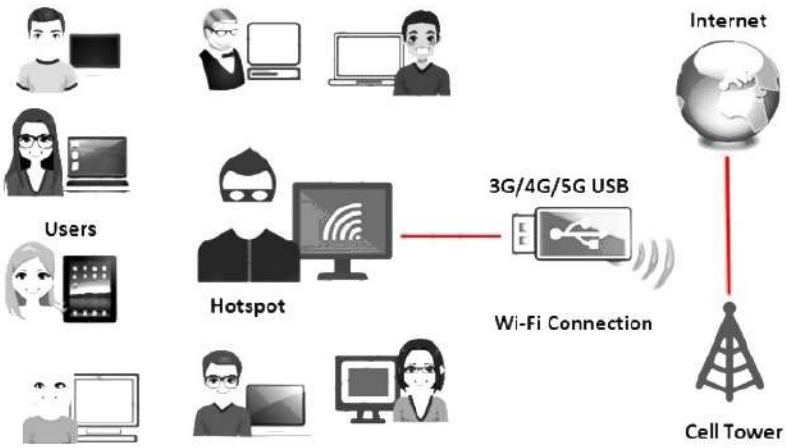
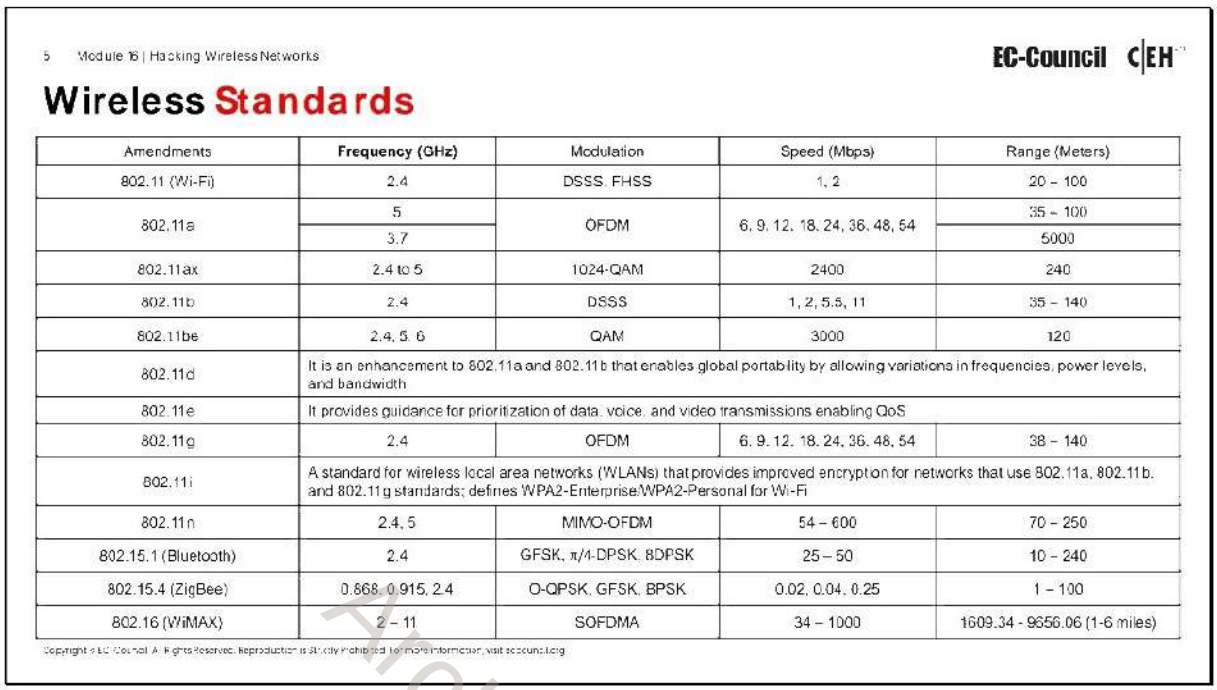


Figure 16.4: 3G/4G/5G hotspot



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	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			
802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
802.11i	A standard for wireless local area networks (WLANs) that provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
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)

Wireless Standards

IEEE Standard 802.11 has evolved from a standard for a basic wireless extension to wired LAN to a mature protocol that supports enterprise authentication, strong encryption, and quality of service. When introduced in 1997, the WLAN standard specified operation at 1 and 2 Mbps in the infrared range as well as in the license-exempt 2.4-GHz industrial, scientific, and medical (ISM) frequency band. In the early days, an 802.11 network had a few PCs with wireless capability connected to an Ethernet (IEEE 802.3) LAN through a single network AP. Now, 802.11 networks operate at substantially higher speeds and in additional bands. New issues have arisen, such as security, roaming among multiple APs, and quality of service. Amendments to the standard are indicated by letters of the alphabet derived from the 802.11 task groups that created them, as shown in the below table.

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	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			
802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
802.11i	A standard for wireless local area networks (WLANs) that provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
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 16.1: Wireless standards

- **802.11**: The 802.11 (Wi-Fi) standard applies to WLANs and uses FHSS or DSSS as the frequency-hopping spectrum. It allows an electronic device to establish a wireless connection in any network.
- **802.11a**: It is the first amendment to the original 802.11 standard. The 802.11 standard operates in the 5 GHz frequency band and supports bandwidths up to 54 Mbps using orthogonal frequency-division multiplexing (OFDM). It has a high maximum speed but is relatively more sensitive to walls and other obstacles.
- **802.11ax (Wi-Fi 6):** Wi-Fi 6, also known as 802.11ax, is the latest generation of Wi-Fi and enhances the foundation of 802.11ac (Wi-Fi 5). It supports speeds of up to 9.6 Gbps, uses orthogonal frequency-division multiple access (OFDMA) to efficiently manage multiple connections, and improves performance in crowded areas through features such as BSS Coloring and target wake time (TWT). Wi-Fi 6 is ideal for dense environments, such as stadiums, airports, and smart homes with many connected devices.
- **802.11b**: IEEE extended the 802.11 standard by creating the 802.11b specifications in 1999. This standard operates in the 2.4 GHz ISM band and supports bandwidths up to 11 Mbps using direct-sequence spread spectrum (DSSS) modulation.

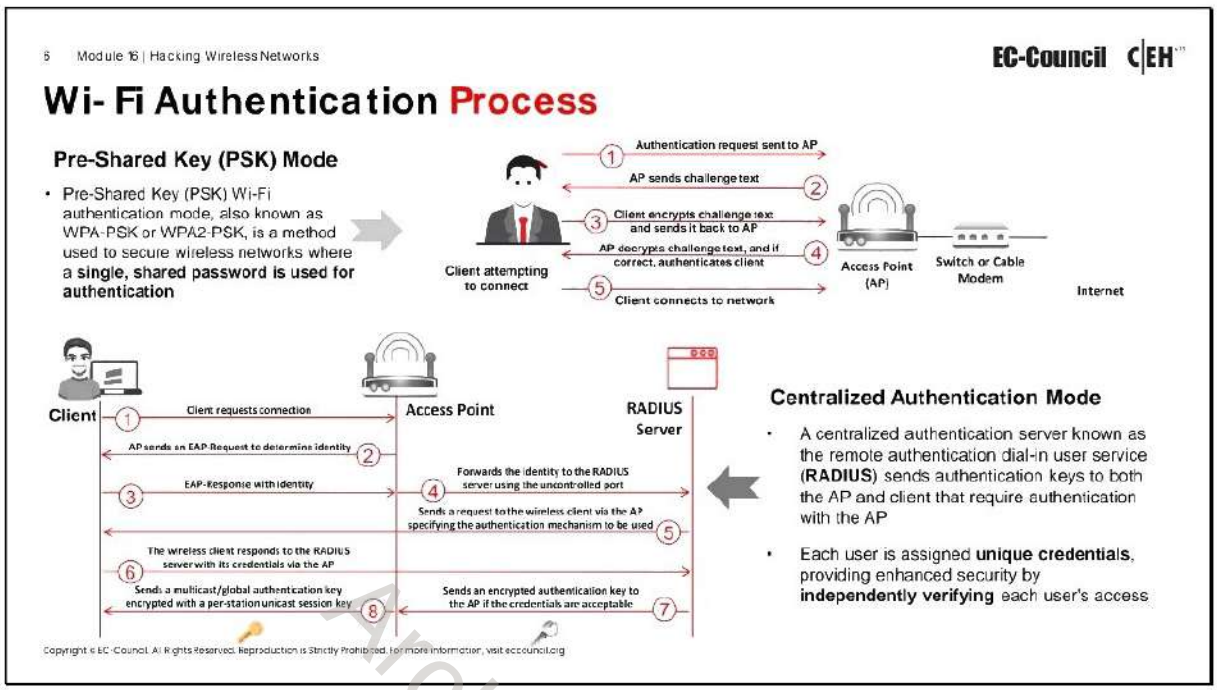
- **802.11be (Wi-Fi 7)**: Wi-Fi 7, also known as 802.11be, is an emerging standard that aims to significantly improve Wi-Fi 6/6E. It supports speeds of up to 30 Gbps, uses a multilink operation (MLO) to aggregate multiple channels across different bands, and reduces the latency for real-time applications. Wi-Fi 7 was designed for future-proof, ultrahigh-speed Internet, virtual reality, augmented reality, and advanced IoT applications.
- **802.11d**: The 802.11d standard is an enhanced version of 802.11a and 802.11b that supports regulatory domains. The specifications of this standard can be set in the media access control (MAC) layer.
- **IEEE 802.11e**: It is used for real-time applications such as voice, VoIP, and video. To ensure that these time-sensitive applications have the network resources they need, 802.11e defines mechanisms to ensure quality of service (QoS) to Layer 2 of the reference model, which is the MAC layer.
- **802.11g**: It is an extension of 802.11 and supports a maximum bandwidth of 54 Mbps using OFDM technology. It uses the same 2.4 GHz band as 802.11b. The IEEE 802.11g standard defines high-speed extensions to 802.11b and is compatible with the 802.11b standard, which means 802.11b devices can work directly with an 802.11g AP.
- **802.11i**: The IEEE 802.11i standard improves WLAN security by implementing new encryption protocols such as the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).
- **802.11n**: The IEEE 802.11n is a revision that enhances the 802.11g standard with multiple-input multiple-output (MIMO) antennas. It works in both the 2.4 GHz and 5 GHz bands. Furthermore, it is an IEEE industry standard for Wi-Fi wireless local network transportation. Digital Audio Broadcasting (DAB) and WLAN use OFDM.
- **802.11ah:** Also called Wi-Fi HaLow, uses 900 MHz bands for extended-range Wi-Fi networks and supports Internet of Things (IoT) communication with higher data rates and wider coverage range than the previous standards.
- **802.11ac**: It provides a high-throughput network at a frequency of 5 GHz. It is faster and more reliable than the 802.11n standard. Moreover, it involves Gigabit networking, which provides an instantaneous data-transfer experience.
- **802.11ad**: The 802.11ad standard includes a new physical layer for 802.11 networks and works on the 60 GHz spectrum. The data propagation speed in this standard is much higher from those of standards operating on the 2.4 GHz and 5 GHz bands, such as 802.11n.
- **802.12**: Media utilization is dominated by this standard because it works on the demand priority protocol. The Ethernet speed with this standard is 100 Mbps. Furthermore, it is compatible with the 802.3 and 802.5 standards. Users currently on those standards can directly upgrade to the 802.12 standard.

- **802.15**: It defines the standards for a wireless personal area network (WPAN) and describes the specifications for wireless connectivity with fixed or portable devices.
- **802.15.1 (Bluetooth)**: Bluetooth is mainly used for exchanging data over short distances on fixed or mobile devices. This standard works on the 2.4 GHz band.
- **802.15.4 (ZigBee)**: The 802.15.4 standard has a low data rate and complexity. The specification used in this standard is ZigBee, transmits long-distance data through a mesh network. The specification handles applications with a low data rate of 250 Kbps, but its use increases battery life.
- **802.15.5**: This standard deploys itself on a full-mesh or half-mesh topology. It includes network initialization, addressing, and unicasting.
- **802.16**: The IEEE 802.16 standard is a wireless communications standard designed to provide multiple physical layer (PHY) and MAC options. It is also known as WiMax. This standard is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture.

Service Set Identifier (SSID)

A service set identifier (SSID) is a case-sensitive, human-readable unique identifier of a WLAN that is 32 alphanumeric characters in length. SSID is a token used to identify and locate 802.11 (Wi-Fi) networks. By default, it is a part of the frame header of packets sent over a WLAN. It acts as a single shared identifier between APs and clients. This helps users locate an AP to which they can attempt a subsequent AUTH and ASSOC. Security concerns arise when the user does not change default values, because these units can be easily compromised.

SSID APs respond to probe requests with probe responses that also include the SSID itself, if it is not hidden. Because SSID is the unique identifier of a WLAN, all devices and APs in the WLAN must use the same SSID. Any device that attempts to join the WLAN must provide the SSID. As every user in the network needs to configure the SSID in their system's network settings, if the SSID of the network is changed, the network administrator needs to reconfigure the SSID on every client. A non-secure access mode allows clients to connect to the AP using the configured SSID, a blank SSID, or an SSID configured as "any." Unfortunately, SSID does not provide security to a WLAN, because it is easy to obtain the SSID as plaintext from packets. For many commercial products, the default SSID is the vendor's name. The SSID can be kept confidential only in closed networks with no activity, which is inconvenient to legitimate users.



Wi-Fi Authentication Process

- **Pre-Shared Key (PSK) Mode**

  The pre-shared key (PSK) Wi-Fi authentication mode, also known as WPA-PSK or WPA2-PSK, is used to secure wireless networks in which a single shared password is used for authentication. This mode is particularly popular in homes and small office environments owing to its simplicity and ease of setup. This mode leverages a shared password to authenticate devices that attempt to connect to a wireless network. The shared password, also known as the pre-shared key, is manually entered into both the wireless router and the device that wishes to connect. The simplicity of this setup makes it an ideal choice for environments in which ease of use is prioritized and the number of users is relatively small. Although convenient, the security of WPA/WPA2-Personal depends on the complexity and secrecy of the pre-shared key.

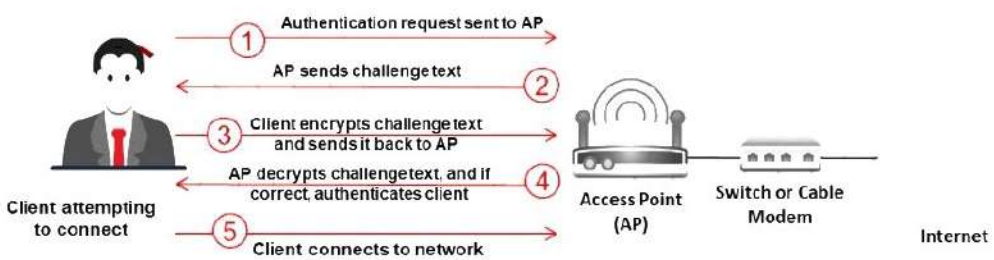


Figure 16.5: PSK Wi-Fi authentication process

- **Centralized Authentication Mode**

  A centralized authentication server, known as the remote authentication dial-in user service (RADIUS), sends authentication keys to both the AP and the client, which

requires authentication with the AP. WPA/WPA2-Enterprise mode, also known as the 802.1X mode, is a security protocol designed for enterprises and large-scale network environments. Unlike WPA/WPA2-Personal, which uses a pre-shared key (PSK) for authentication, WPA/WPA2-Enterprise utilizes a centralized authentication server, typically a RADIUS server, to manage individual user credentials. Each user is assigned unique credentials, such as a username and password or a digital certificate, which are used to authenticate and authorize network access. This mode offers enhanced security by ensuring that the credentials of each user are verified independently, thereby making it difficult for unauthorized users to gain access to the network. WPA/WPA2-Enterprise is particularly suited to environments with high security requirements and a large number of users, such as corporate offices, educational institutions, and government agencies.

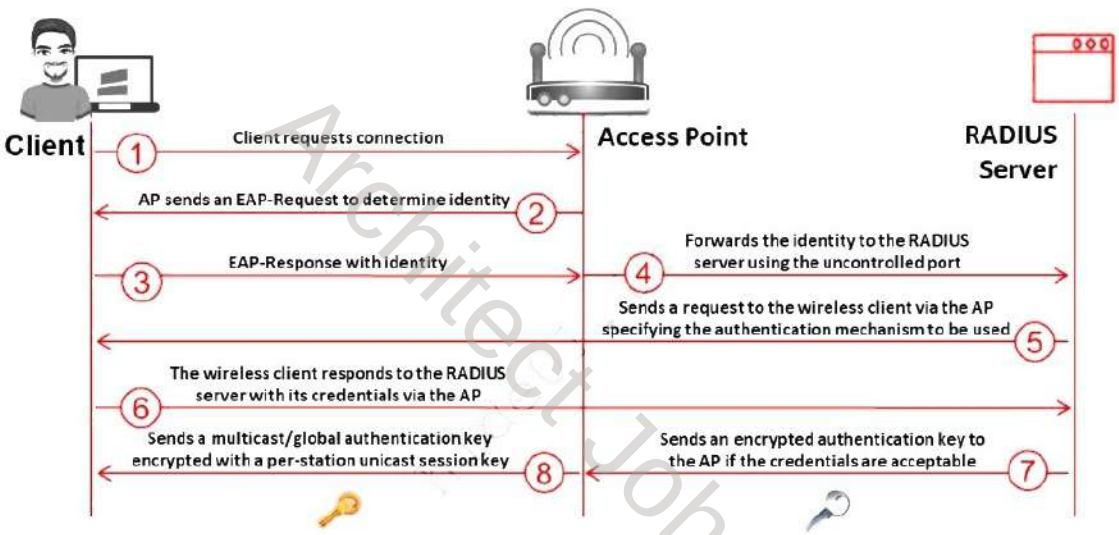


Figure 16.6: Centralized authentication process

Types of Wireless Antennas

Antennas are an integral part of Wi-Fi networks. In addition to sending and receiving radio signals, they convert electrical impulses into radio signals and vice versa.

The types of wireless antennas include the following:

- **Directional Antenna**

  A directional antenna can broadcast and receive radio waves from a single direction. In order to improve transmission and reception, the directional antenna's design allows it to work effectively in only a few directions. This also helps in reducing interference.

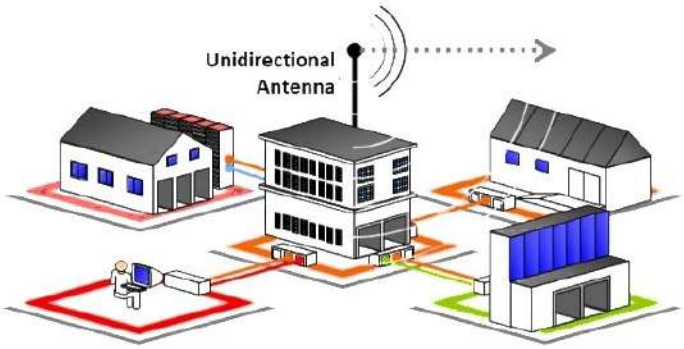


Figure 16.7: Directional antenna

- **Omnidirectional Antenna**

  Omnidirectional antennas radiate electromagnetic (EM) energy in all directions. It provides a 360° horizontal radiation pattern. They radiate strong waves uniformly in two dimensions, but the waves are usually not as strong in the third dimension. These antennas are efficient in areas where wireless stations use time-division multiple access technology. A good example for an omnidirectional antenna is the antenna used by radio stations. These antennas are effective for radio signal transmission because the receiver may not be stationary. Therefore, a radio can receive a signal regardless of its location.

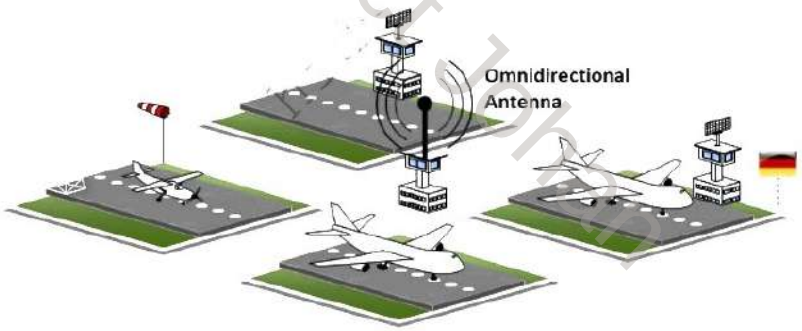
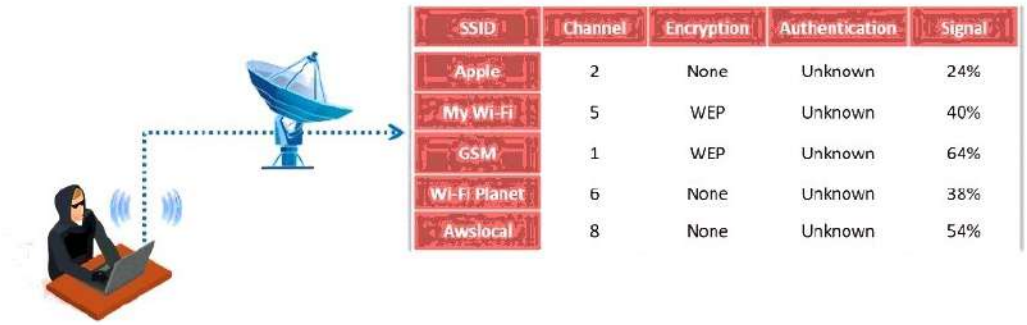


Figure 16.8: Omnidirectional antenna

- **Parabolic Grid Antenna**

  A parabolic grid antenna uses the same principle as a satellite dish, but it does not have a solid dish. It consists of a semi-dish in the form of a grid consisting of aluminum wires. Parabolic grid antennas can achieve very-long-distance Wi-Fi transmissions through highly focused radio beams. This type of antenna is useful for transmitting weak radio signals over very long distances on the order of 10 miles. This enables attackers to obtain a better signal quality, resulting in more data to eavesdrop on, more bandwidth to abuse, and a higher power output, which is essential in Layer-1 denial-of-service (DoS) and man-in-the-middle (MITM) attacks. The design of this antenna saves weight and space, and it can receive Wi-Fi signals that are either horizontally or vertically polarized.



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 16.9: Parabolic grid antenna

- **Yagi Antenna**

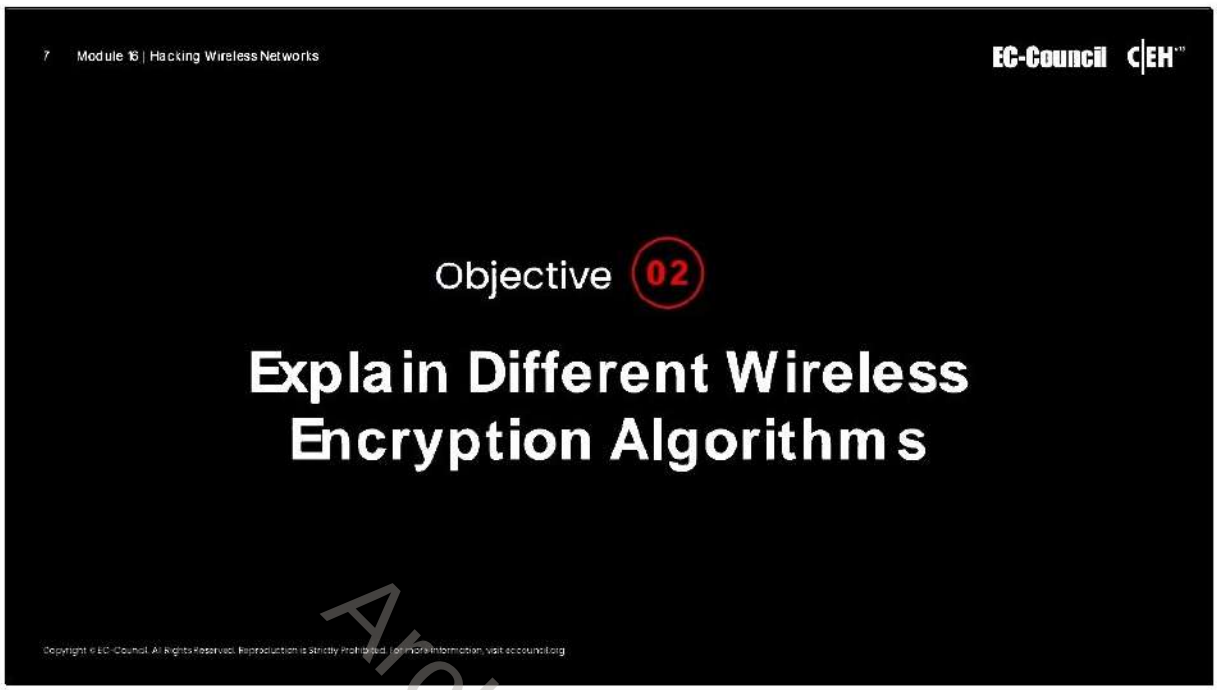
  A Yagi antenna, also called Yagi–Uda antenna, is a unidirectional antenna commonly used in communications at a frequency band of 10 MHz to VHF and UHF. This antenna has a high gain and low signal-to-noise (SNR) ratio for radio signals. Furthermore, it not only has a unidirectional radiation and response pattern, but also concentrates the radiation and response. It consists of a reflector, dipole, and many directors. This antenna develops an end-fire radiation pattern.

- **Dipole Antenna**

  A dipole antenna is a straight electrical conductor measuring half a wavelength from end to end, and it is connected at the center of the radio frequency (RF) feed line. Also called a doublet, the antenna is bilaterally symmetrical; therefore, it is inherently a balanced antenna. This kind of antenna feeds on a balanced parallel-wire RF transmission line.

- **Reflector Antennas**

  Reflector antennas are used to concentrate EM energy that is radiated or received at a focal point. These reflectors are generally parabolic. If the surface of the parabolic antenna is within a tolerance limit, it can be used as a primary mirror for all frequencies. This can prevent interference while communicating with other satellites. A larger antenna reflector in terms of wavelength multiples results in a higher gain. Reflector antennas reflect radio signals and has a high manufacturing cost.



Wireless Encryption

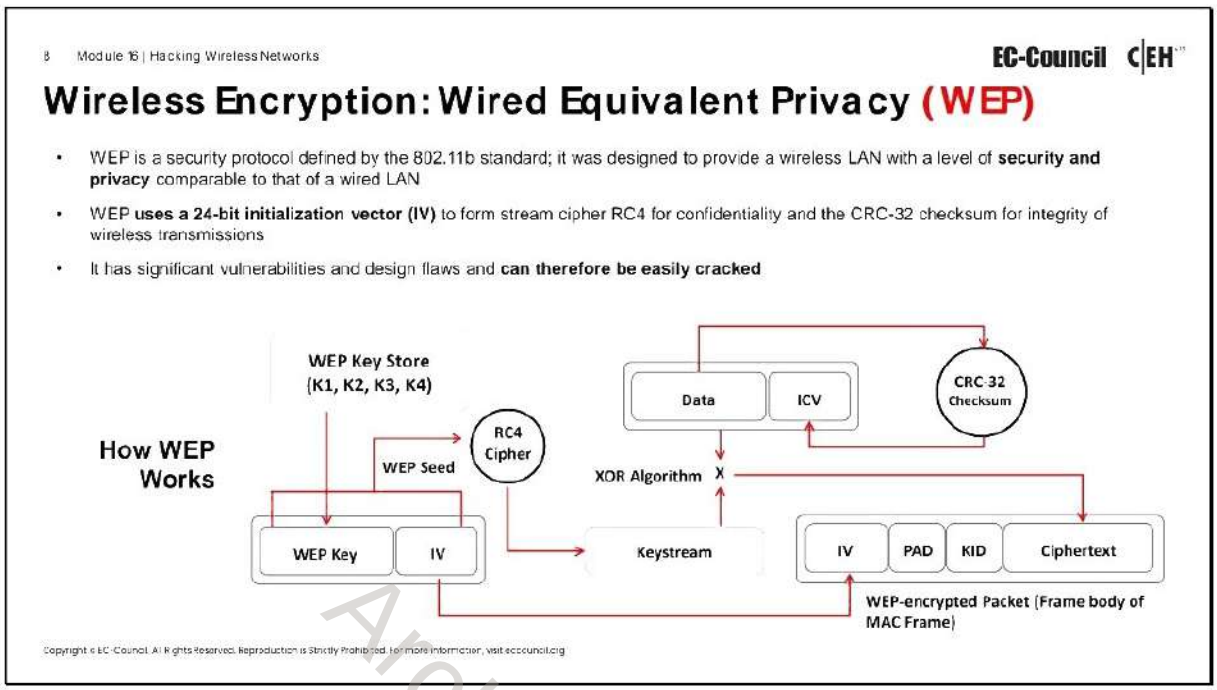
Wireless encryption is a process of protecting a wireless network from attackers who attempt to collect sensitive information by breaching the RF traffic. This section provides insight into various wireless encryption standards such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WPA3, in addition to issues in WEP, WPA, WPA2, and WPA3.

Wireless Encryption

Attacks on wireless networks are increasing daily with the increasing use of wireless networks. The encryption of information before it is transmitted on a wireless network is the most popular method of protecting wireless networks against attackers. There are several types of wireless encryption algorithms that can secure a wireless network. Each wireless encryption algorithm has advantages and disadvantages.

- **802.11i**: It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks.
- **WEP**: WEP is an encryption algorithm for IEEE 802.11 wireless networks. It is an old wireless security standard and can be cracked easily.
- **EAP**: The Extensible Authentication Protocol (EAP) supports multiple authentication methods, such as token cards, Kerberos, and certificates.
- **LEAP**: Lightweight EAP (LEAP) is a proprietary version of EAP developed by Cisco.
- **WPA**: It is an advanced wireless encryption protocol using TKIP and Message Integrity Check (MIC) to provide strong encryption and authentication. It uses a 48-bit initialization vector (IV), 32-bit cyclic redundancy check (CRC), and TKIP encryption for wireless security.

- **TKIP**: It is a security protocol used in WPA as a replacement for WEP.
- **WPA2**: It is an upgrade to WPA using AES and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) for wireless data encryption.
- **AES**: It is a symmetric-key encryption used in WPA2 as a replacement for TKIP.
- **CCMP**: It is an encryption protocol used in WPA2 for strong encryption and authentication.
- **WPA2 Enterprise**: It integrates EAP standards with WPA2 encryption.
- **RADIUS**: It is a centralized authentication and authorization management system.
- **PEAP**: It is a protocol that encapsulates the EAP within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
- **WPA3**: It is a third-generation Wi-Fi security protocol that provides new features for personal and enterprise usage. It uses Galois/Counter Mode-256 (GCMP-256) for encryption and the 384-bit hash message authentication code with the Secure Hash Algorithm (HMAC-SHA-384) for authentication.



Wireless Encryption: Wired Equivalent Privacy (WEP)

WEP was an early attempt to protect wireless networks from security breaches, but as technology improved, it became evident that information encrypted with WEP is vulnerable to attack. We discuss WEP in detail here.

What is WEP Encryption?

WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to ensure data confidentiality on wireless networks at a level equivalent to that of wired LANs, which can use physical security to stop unauthorized access to a network.

In a WLAN, a user or an attacker can access the network without physically connecting to the LAN. Therefore, WEP utilizes an encryption mechanism at the data link layer for minimizing unauthorized access to the WLAN. This is accomplished by encrypting data with the symmetric Rivest Cipher 4 (RC4) encryption algorithm, which is a cryptographic mechanism used to defend against threats.

Role of WEP in Wireless Communication

- WEP protects against eavesdropping on wireless communications.
- It attempts to prevent unauthorized access to a wireless network.
- It depends on a secret key shared by a mobile station and an AP. This key encrypts packets before transmission. Performing an integrity check ensures that packets are not altered during transmission. 802.11 WEP encrypts only the data between network clients.

Main Advantages of WEP

- **Confidentiality**: It prevents link-layer eavesdropping.
- **Access Control**: It determines who may access data.
- **Data Integrity**: It protects the change of data by a third party.
- **Efficiency**

Key Points

WEP was developed without any academic or public review. In particular, it was not reviewed by cryptologists during development. Therefore, it has significant vulnerabilities and design flaws.

WEP is a stream cipher that uses RC4 to produce a stream of bytes that are XORed with plaintext. The length of the WEP and secret key are as follows:

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

How WEP Works

- CRC-32 checksum is used to calculate a 32-bit integrity check value (ICV) for the data, which, in turn, is added to the data frame.
- A 24-bit arbitrary number known as the initialization vector (IV) is added to the WEP key; the WEP key and IV are together called the WEP seed.
- The WEP seed is used as the input to the RC4 algorithm to generate a keystream, which is bit-wise XORed with a combination of the data and ICV to produce the encrypted data.
- The IV field (IV + PAD + KID) is added to the ciphertext to generate a MAC frame.

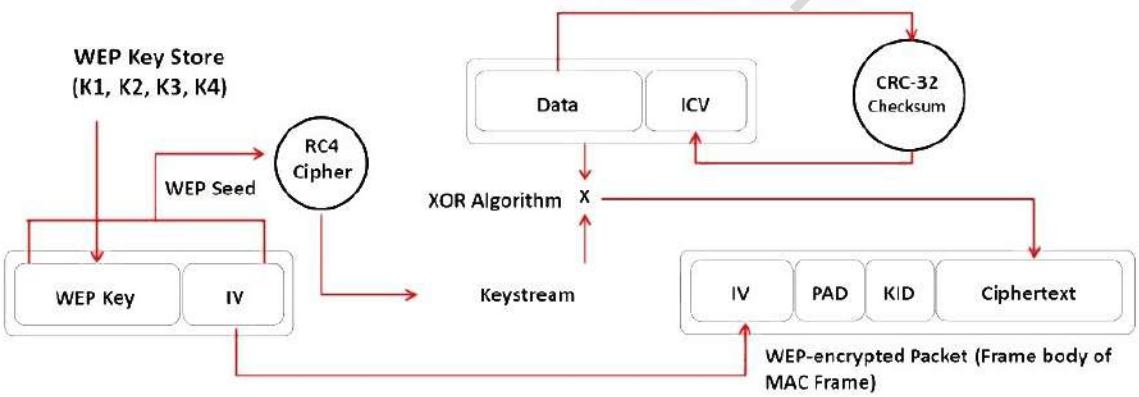
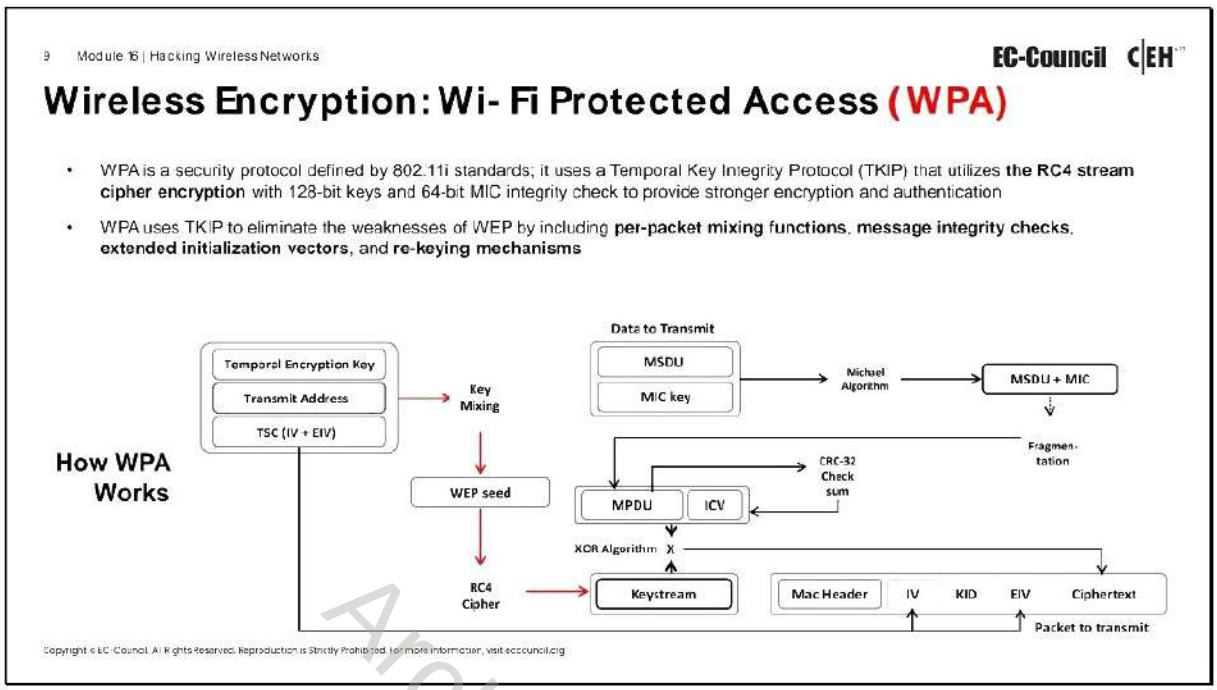


Figure 16.10: Operational flow of WEP

Flaws of WEP

The following basic flaws undermine WEP's ability to protect against a serious attack.

- No defined method for encryption key distribution:
  - Pre-shared keys (PSKs) are set once at installation and are rarely (if ever) changed.
  - It is easy to recover the number of plaintext messages encrypted with the same key.
- RC4 was designed to be used in a more randomized environment than that utilized by WEP:
  - As the PSK is rarely changed, the same key is used repeatedly.
  - An attacker monitors the traffic and finds different ways to work with the plaintext message.
  - With knowledge of the ciphertext and plaintext, an attacker can compute the key.
- Attackers analyze the traffic from passive data captures and crack WEP keys with the help of tools such as Fern Wifi Cracker and WEP-key-break.
- Key scheduling algorithms are also vulnerable to attack.



Wireless Encryption: Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is a security protocol defined by the 802.11i standard. In the past, the primary security mechanism used between wireless APs and wireless clients was WEP encryption, which has a major drawback in that it uses a static encryption key. An attacker can exploit this weakness using tools that are freely available on the Internet. IEEE defines WPA as "an expansion to the 802.11 protocols that can allow for increased security." Nearly every Wi-Fi manufacturer provides WPA.

WPA has better data encryption security than WEP because messages pass through a Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP), which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC to provide strong encryption and authentication. WPA is an example of how 802.11i provides stronger encryption and enables pre-shared key (PSK) or EAP authentication. WPA uses TKIP for data encryption, which eliminates the weaknesses of WEP by including per-packet mixing functions, MICs, extended IVs and re-keying mechanisms.

WEP normally uses a 40-bit or 104-bit encryption key, whereas TKIP uses 128-bit keys for each packet. The MIC for WPA prevents the attacker from changing or resending the packets.

- **TKIP**: It is used in a unicast encryption key that changes for every packet, thereby enhancing security. This change in the key for each packet is automatically coordinated between the wireless client and AP. TKIP uses a Michael Integrity Check algorithm with an MIC key to generate the MIC value. It utilizes the RC4 stream cipher encryption with 128-bit keys and a 64-bit MIC integrity check. It mitigates vulnerability by increasing the size of the IV and using mixing functions. Under TKIP, the client starts with a 128-bit temporal key (TK) that is then combined with the client's MAC address and with an IV to create a keystream that is used to encrypt data via RC4. It implements a sequence

counter to protect against replay attacks. TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. TKs are changed every 10,000 packets, which makes TKIP-protected networks more resistant to cryptanalytic attacks involving key reuse.

- **TKs**: All newly deployed Wi-Fi equipment uses either TKIP (for WPA) or AES (for WPA2) encryption to ensure WLAN security. In the WEP encryption mechanism, the protocol derives encryption keys (TKs) from the pairwise master key (PMK), which is created during the EAP authentication session, whereas in the WPA and WPA2 encryption mechanisms, the protocol obtains the encryption keys during a four-way handshake. In the EAP success message, the PMK is sent to the AP but is not directed to the Wi-Fi client because it has derived its own copy of the PMK.

  The below figure shows the installation procedure for TKs.

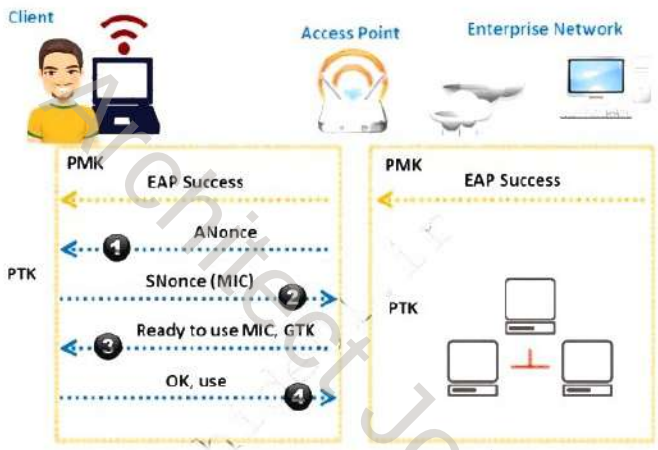


Figure 16.11: Operational flow of temporal keys

  - AP sends an ANonce to the client, which uses it to construct the pairwise transient key (PTK).
  - The client responds with its own Nonce value (SNonce) to the AP, together with an MIC.
  - The AP sends the group temporal key (GTK) and a sequence number, together with another MIC, which is used in the next broadcast frames.
  - The client confirms that the temporal keys are installed.

How WPA Works

- A TK, transmit address, and TKIP sequence counter (TSC) are used as input to the RC4 algorithm to generate a keystream.
  - The IV or TK sequence, transmit address or MAC destination address, and TK are combined with a hash function or mixing function to generate a 128-bit and 104-bit key.
  - This key is then combined with RC4 to produce the keystream, which should be of the same length as the original message.
- The MAC service data unit (MSDU) and message integrity check (MIC) are combined using the Michael algorithm.
- The combination of MSDU and MIC is fragmented to generate the MAC protocol data unit (MPDU).
- A 32-bit ICV is calculated for the MPDU.
- The combination of MPDU and ICV is bitwise XORed with the keystream to produce the encrypted data.
- The IV is added to the encrypted data to generate the MAC frame.

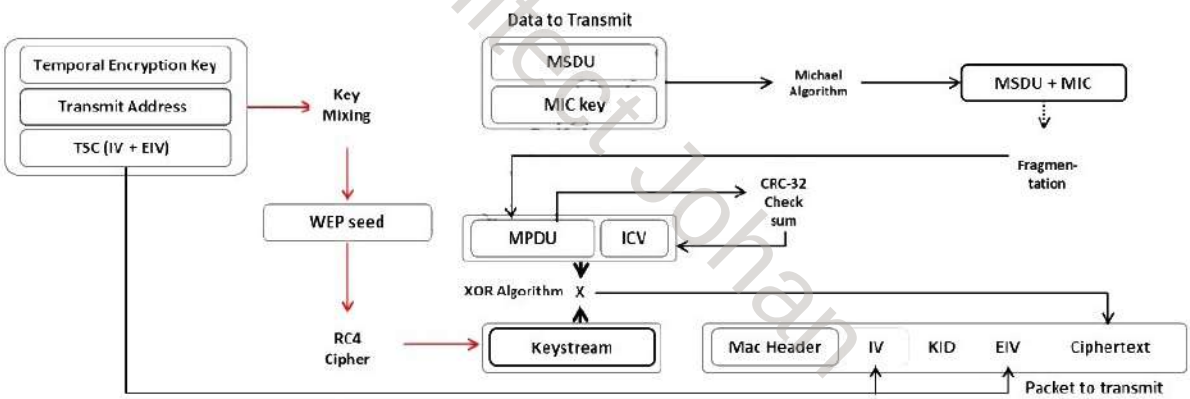
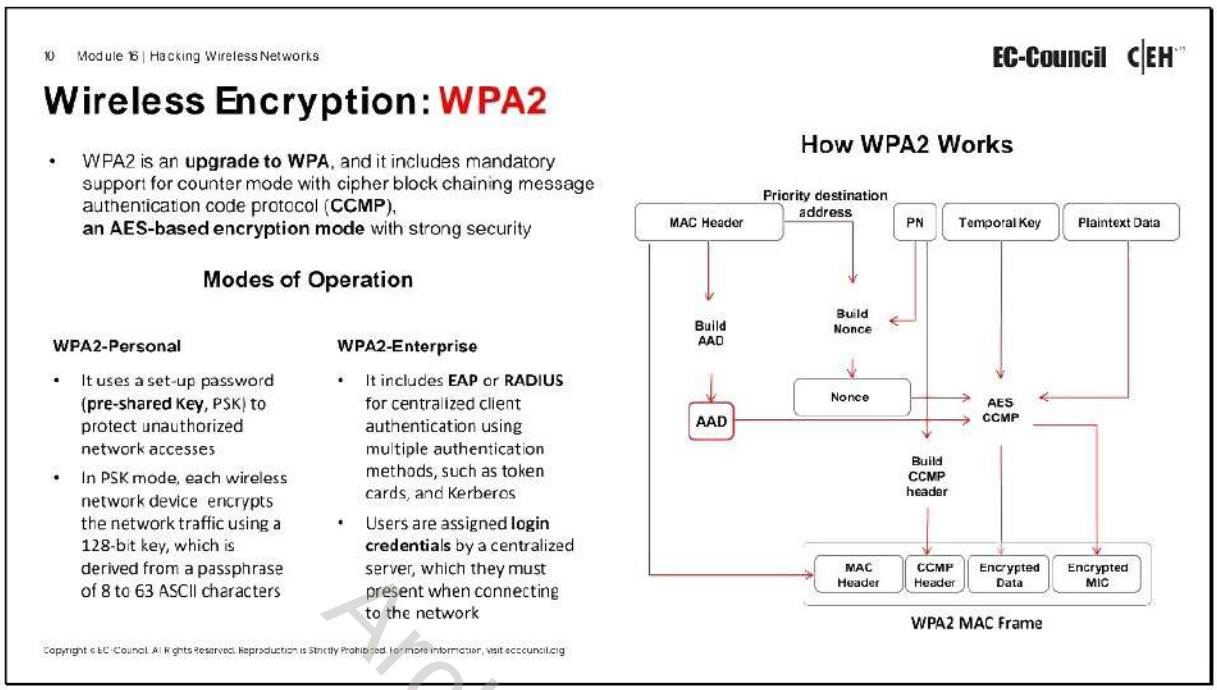


Figure 16.12: Operational flow of WPA



Wireless Encryption: WPA2

Wi-Fi Protected Access 2 (WPA2) is a security protocol used to safeguard wireless networks. WPA2 replaced WPA in 2006. It is compatible with the 802.11i standard and supports many security features that WPA does not. WPA2 introduces the use of the National Institute of Standards and Technology (NIST) FIPS 140-2-compliant AES encryption algorithm, which is a strong wireless encryption algorithm, and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). It provides stronger data protection and network access control than WPA. Furthermore, it gives a high level of security to Wi-Fi connections so that only authorized users can access the network.

Modes of Operation

WPA2 offers two modes of operation:

- **WPA2-Personal**: WPA2-Personal uses a password set in advance, called the pre-shared key (PSK), to protect unauthorized network access. Each wireless device uses the same 256-bit key generated from a password to authenticate with the AP. In the PSK mode, each wireless network device encrypts the network traffic using a 128-bit key derived from a passphrase of 8–63 ASCII characters. The router uses the combination of a passphrase, network SSID, and TKIP to generate a unique encryption key for each wireless client. These encryption keys change continually.
- **WPA2-Enterprise**: WPA2-Enterprise uses EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, and certificates. WPA-Enterprise assigns a unique ciphered key to every system and hides it from the user in order to provide additional security and to prevent the sharing of keys. Users are allocated login credentials by a centralized server, which they must present when connecting to the network.

How WPA2 Works

During CCMP implementation, additional authentication data (AAD) are generated using a MAC header and included in the encryption process that uses both AES and CCMP encryptions. Consequently, the non-encrypted portion of the frame is protected from any alteration or distortion. The protocol uses a sequenced packet number (PN) and a portion of the MAC header to generate a Nonce that it uses in the encryption process. The protocol gives plaintext data, and temporal keys, AAD, and Nonce are used as input for the data encryption process that uses both AES and CCMP algorithms.

A PN is included in the CCMP header for protection against replay attacks. The resultant data from the AES and CCMP algorithms produce encrypted text and an encrypted MIC value. Finally, the assembled MAC header, CCMP header, encrypted data, and encrypted MIC form the WPA2 MAC frame. The below figure shows the operational flow of WPA2.

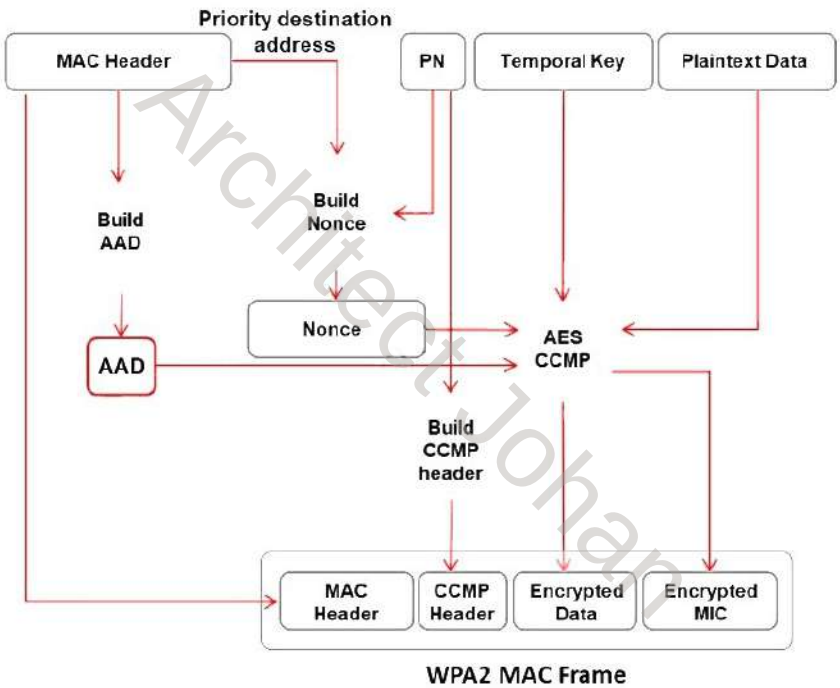
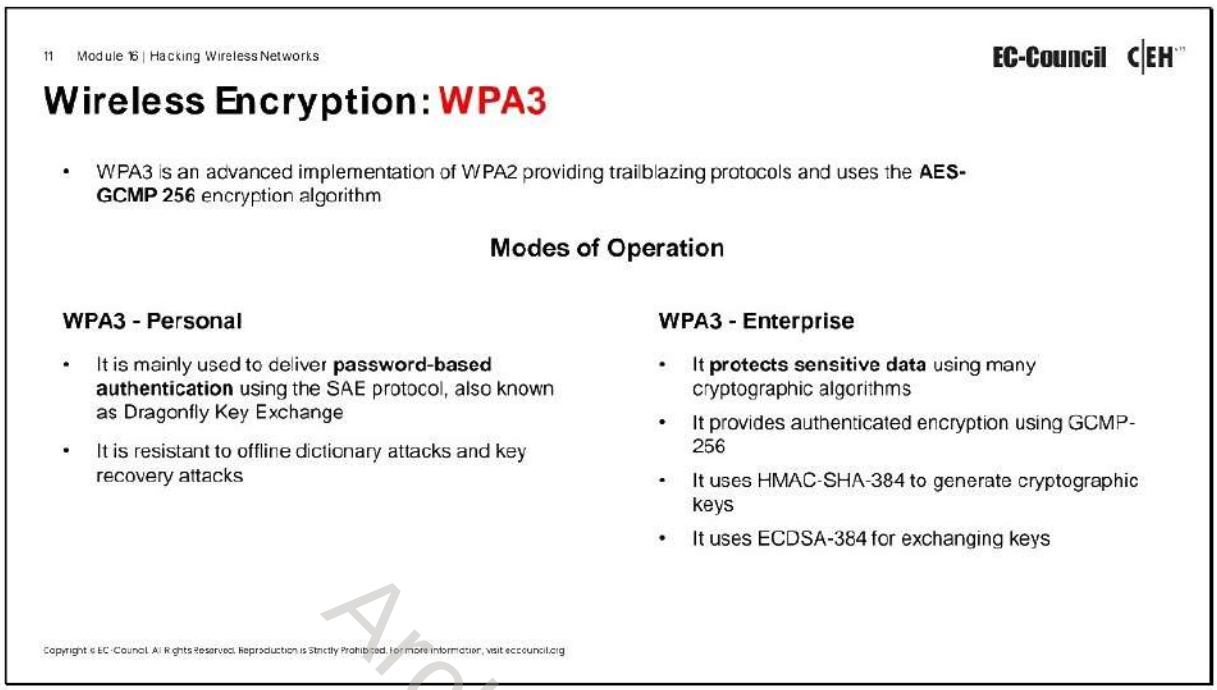


Figure 16.13: Operational flow of WPA2



Wireless Encryption: WPA3

Wi-Fi Protected Access 3 (WPA3) was announced by the Wi-Fi Alliance on January 2018 as an advanced implementation of WPA2 that provides trailblazing protocols. Like WPA2, the WPA3 protocol has two variants: WPA3-Personal and WPA3-Enterprise.

WPA3 provides cutting-edge features to simplify Wi-Fi security and provides the capabilities necessary to support different network deployments ranging from corporate networks to home networks. It also ensures cryptographic consistency using encryption algorithms such as AES and TKIP to defend against network attacks. Furthermore, it provides network resilience through Protected Management Frames (PMF) that deliver a high level of protection against eavesdropping and forging attacks. WPA3 also disallows outdated legacy protocols.

Modes of Operation

WPA3 offers two modes of operation:

- **WPA3-Personal**: This mode is mainly used to deliver password-based authentication. WPA3 is more rigid to attacks than WPA2 because it uses a modern key establishment protocol called the Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, which replaces the PSK concept used in WPA2-Personal. Some of the features of WPA3-Personal are described below.
  - **Resistance to offline dictionary attacks**: It prevents passive password attacks such as brute-forcing.
  - **Resistance to key recovery**: Even when a password is determined, it is impossible to capture and determine session keys while maintaining the forward secrecy of network traffic.

- **Natural password choice**: It allows users to choose weak or popular phrases as passwords, which are easy to remember.
- **Easy accessibility**: It can provide greater protection than WPA2 without changing the previous methods used by users for connecting to a network.

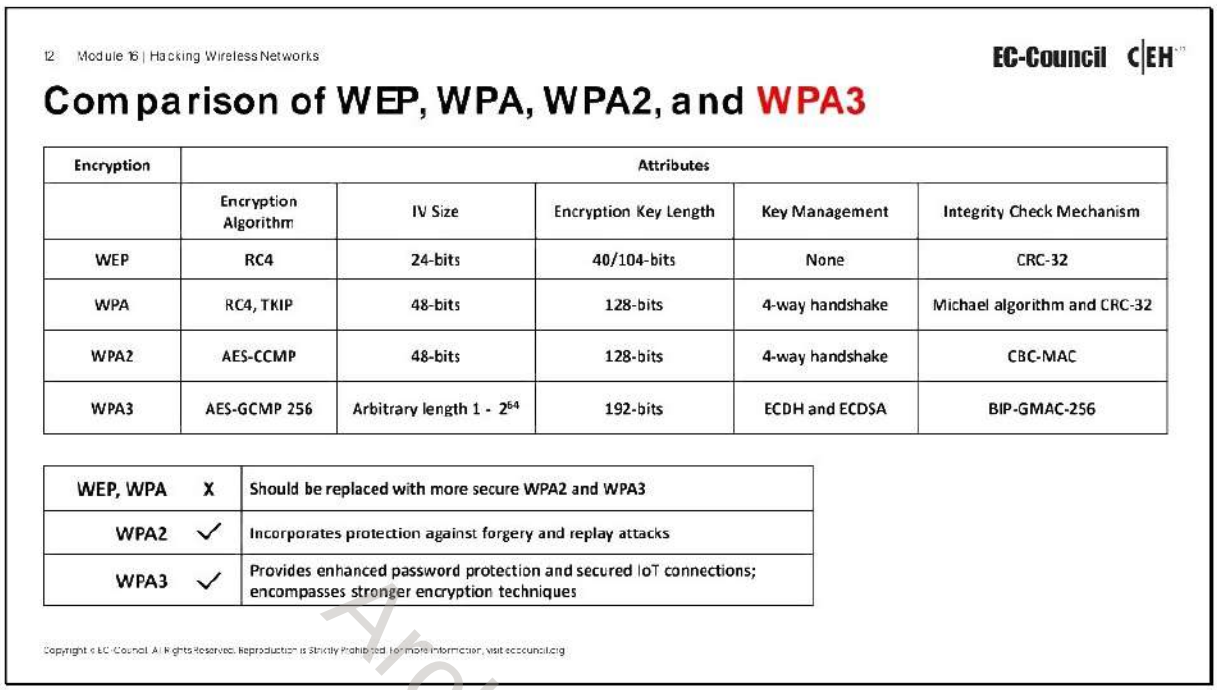
- **WPA3-Enterprise**: This mode is based on WPA2. It offers better security than WPA2 across the network and protects sensitive data using many cryptographic concepts and tools. Some of the security protocols used by WPA3-Enterprise are described below.
  - **Authenticated encryption**: It helps in maintaining the authenticity and confidentiality of data. For this purpose, WPA3 uses the 256-bit Galois/Counter Mode Protocol (GCMP-256).
  - **Key derivation and validation**: It helps in generating a cryptographic key from a password or master key. It uses the 384-bit hashed message authentication mode (HMAC) with the Secure Hash Algorithm, termed HMAC-SHA-384.
  - **Key establishment and verification**: It helps in exchanging cryptographic keys among two parties. For this purpose, WPA3 uses Elliptic Curve Diffie–Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve.
  - **Frame protection and robust administration**: WPA3 uses 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) for this purpose.

Enhancements in WPA3 with Respect to WPA2

WPA3 can be used to implement a layered security strategy that can protect all aspects of a Wi-Fi network. WPA3 has a certification program that specifies the prevailing standards the product must support. The Dragonfly handshake/SAE protocol is mandatory for WPA3 certification.

The important features of WPA3 are as follows.

1. **Secured handshake**: The Simultaneous Authentication of Equals (SAE) protocol, also known as the Dragonfly handshake, can be used to make a password resistant to dictionary and brute-force attacks, preventing the offline decryption of data.
2. **Wi-Fi Easy Connect**: This feature simplifies the security configuration process by managing different interface connections in a network with one interface using the Wi-Fi Device Provisioning Protocol (DPP). This can securely allow a plethora of smart devices in a network to connect to one device using a quick response (QR) code or password. It also helps set up a connection between different IoT devices.
3. **Unauthenticated encryption**: It uses a new feature called Opportunistic Wireless Encryption (OWE) that replaces the 802.11 "open" authentication by providing better protection when using public hotspots and public networks.
4. **Bigger session keys**: The cryptographic security process of WPA3-Enterprise supports key sizes of 192 bits or higher, which are difficult to crack, ensuring rigid protection.

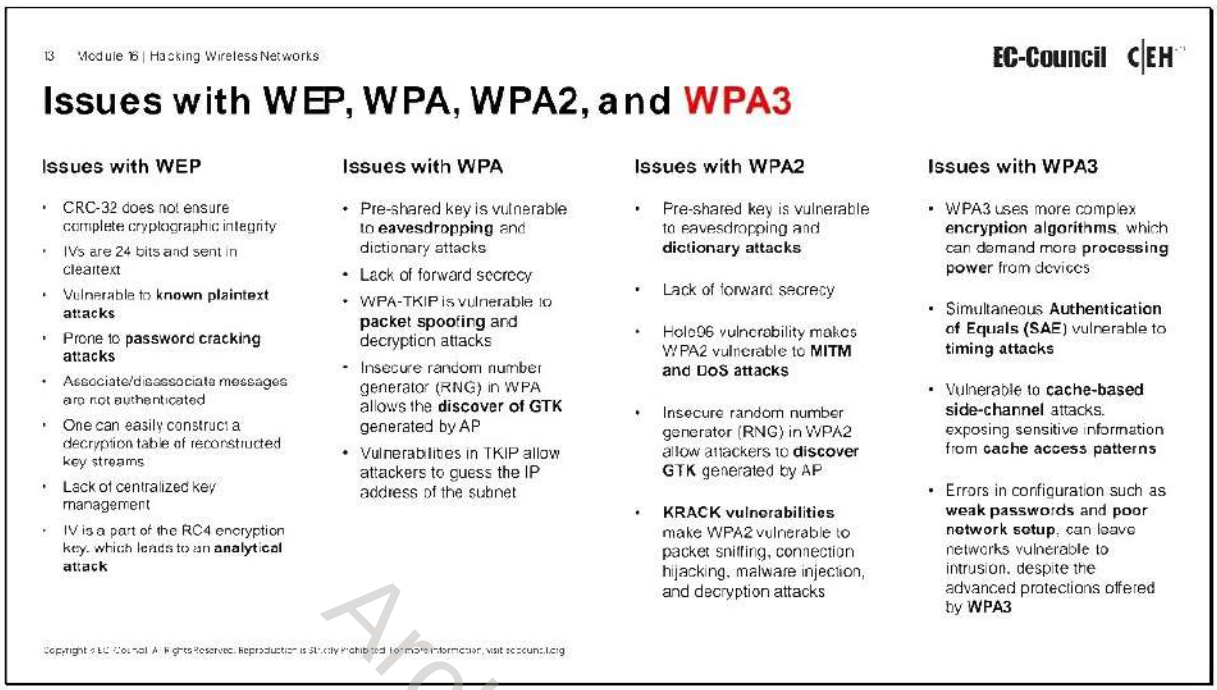


Comparison of WEP, WPA, WPA2, and WPA3

WEP provides data confidentiality on wireless networks, but it is weak and fails to meet any of its security goals. While WPA fixes most of WEP's problems, WPA2 makes wireless networks almost as secure as wired networks. Because WPA2 supports authentication, only authorized users can access the network. WEP and WPA should be replaced with either WPA2 or WPA3 to secure a Wi-Fi network. Though WPA and WPA2 incorporate protections against forgery and replay attacks, WPA3 can provide a more enhanced password-protection mechanism and secure IoT connections; further, it utilizes stronger encryption techniques. The below table compares WEP, WPA, WPA2, and WPA3 in terms of the encryption algorithm used, the encryption-key size, the initialization vector (IV) it produces, 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 16.2: Comparison of WEP, WPA, WPA2, and WPA3



Issues with WEP, WPA, WPA2, and WPA3

Issues with WEP

WEP encryption is insufficient to secure wireless networks because of certain issues and anomalies, which include the following.

- **CRC32 is insufficient to ensure the complete cryptographic integrity of a packet**: By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
- **IVs are of 24 bits**: The IV is a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. An AP broadcasting 1500-byte packets at 11 Mbps would exhaust the entire IV space in five hours.
- **WEP is vulnerable to known plaintext attacks**: When an IV collision occurs, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.
- **WEP is vulnerable to dictionary attacks**: Because WEP is based on a password, it is prone to password-cracking attacks. The small IV space allows the attacker to create a decryption table, which is a dictionary attack.
- **WEP is vulnerable to DoS attacks**: This is because associate and disassociate messages are not authenticated.
- **An attacker can eventually construct a decryption table of reconstructed keystreams**: With approximately 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.
- **A lack of centralized key management makes it difficult to change WEP keys regularly.**

- **IV is a value used to randomize the keystream value, and each packet has an IV value**: The standard IV allows only a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. All available IV values can be used up within hours at a busy AP. IV is a part of the RC4 encryption key and is vulnerable to an analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic. Identical keystreams are produced with the reuse of the IV for data protection because the short IV keystreams are repeated within a short time. Furthermore, wireless adapters from the same vendor may all generate the same IV sequence. This enables attackers to determine the keystream and decrypt the ciphertext.
- **The standard does not require each packet to have a unique IV:** Vendors use only a small part of the available 24-bit possibilities. Consequently, a mechanism that depends on randomness is not random at all, and attackers can easily determine the keystream and decrypt other messages.
- **The use of RC4 was designed to be a one-time cipher and not intended for use with multiple messages.**
- All users in the network share the same key, and changing the key requires reconfiguring every device on the network. This discourages frequent key modifications.
- WEP does not include a mechanism to prevent replay attacks, which allows attackers to retransmit captured packets.
- CRC-32 is not a cryptographic hash function and is vulnerable to bit-flipping attacks, in which attackers can modify the packet and adjust the checksum accordingly.
- Even a key length of 104 bits is insufficient according to modern cryptographic standards, making brute-force attacks feasible.
- WEP only supports one-way authentication, where the client authenticates the access point, but the access point is not authenticated to the client.
- The FMS attack exploits the weakness of RC4 key scheduling when the IVs are reused. This attack method can quickly recover the WEP key using statistical analysis, making WEP encryption easily breakable.

Because most organizations have configured their network clients and APs to use the same shared key or the four default keys, the randomness of the keystream relies on the uniqueness of the IV value. The use of IV and a key ensures that the keystream for each packet is different, but in most cases, the IV changes while the key remains constant. Since there are only two main components to this encryption process and one stays constant, the process has an unacceptable level of randomization. A busy AP can use all 224 available IV values within hours, necessitating the reuse of IV values. Such repetition in a process that relies on randomness leads to failure.

The IV issue is exacerbated by the fact that the 802.11 standard does not require each packet to have a different IV value, which is analogous to claiming stringent security while adopting weak measures. In many implementations, the IV value changes only when the wireless NIC reinitializes, usually during a reboot. Although 24 bits provide sufficient possible combinations of IV values, most implementations use only a handful of bits; thus, these implementations do not even utilize the security measures available to them.

The reasons for generating weak IVs in WEP include the following:

- To generate different packets in WEP, the RC4 algorithm uses a key scheduling algorithm (KSA) to create an IV and adds it to the base key, which makes the first few bytes of plaintext easily predictable.
- The IV value is not explicit to the network. Therefore, the same IV can be used with the same secret key on multiple wireless devices.
- The method of appending the IV to the beginning of the security key makes the network vulnerable to Fluhrer–Mantin–Shamir (FMS) attacks, which allow attackers to execute script tools to crack the secret key by examining a link.
- Most weak IVs depend on a WEP key and reveal accurate information about the key bytes from the first RC4 output byte, as well as smaller clues from other bytes.
- Through additional processing on recovered bytes, parts of a pseudo-random generation algorithm (PRGA) can be emulated to extract key information in the byte of an IV.
- Message tampering cannot be effectively detected. Although methods such as checksum and ICV can check message integrity, they have some drawbacks. Some secure methods for computing MIC have a high computational cost when introduced in TKIP.
- WEP directly uses the master key and has no built-in provision to update the keys.

A security flaw in the WEP implementation of RC4 results in the generation of weak IVs, which attackers can easily exploit to deduce the base WEP key. An attacker can use WLAN sniffing tools to capture packets encrypted with the same key and tools such as aircrack-ng and Wifi-Cracker to decrypt the weak IVs, thereby exposing the base WEP key.

Issues with WPA

WPA is an improvement over WEP in many ways because it uses TKIP for data encryption and helps in secured data transfer. However, WPA has many security issues as well.

Some of the security issues of WPA are as described follows.

- **Weak passwords:** If users depend on weak passwords, the WPA PSK is vulnerable to various password-cracking attacks.
- **Lack of forward secrecy**: If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to packet spoofing and decryption**: Clients using WPA-TKIP are vulnerable to packet-injection attacks and decryption attacks, which further allows attackers to hijack Transmission Control Protocol (TCP) connections.

- **Predictability of the group temporal key (GTK)**: An insecure random number generator (RNG) in WPA allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **Guessing of IP addresses**: TKIP vulnerabilities allow attackers to guess the IP address of the subnet and inject small packets into the network to downgrade the network performance.

Issues with WPA2

Although WPA2 is more secure than WPA, it also has some security issues, which are discussed below.

- **Weak passwords**: If users depend on weak passwords, the WPA2 PSK is vulnerable to various attacks such as eavesdropping, dictionary, and password-cracking attacks.
- **Lack of forward secrecy**: If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to man-in-the-middle (MITM) and denial-of-service (DoS) attacks**: The Hole96 vulnerability in WPA2 allows attackers to exploit a shared group temporal key (GTK) to perform MITM and DoS attacks.
- **Predictability of GTK**: An insecure random number generator (RNG) in WPA2 allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **KRACK vulnerabilities**: WPA2 has a significant vulnerability to an exploit known as key reinstallation attack (KRACK). This exploit may allow attackers to sniff packets, hijack connections, inject malware, and decrypt packets.
- **Vulnerability to wireless DoS attacks**: Attackers can exploit the WPA2 replay attack detection feature to send forged group-addressed data frames with a large PN to perform a DoS attack.
- **Insecure WPS PIN recovery**: In some cases, disabling WPA2 and WPS can be a time-consuming process, in which the attacker needs to control the WPA2 PSK used by the clients. When WPA2 and WPS are enabled, the attacker can disclose the WPA2 key by determining the WPS personal identification number (PIN) through simple steps.

Issues with WPA3

Although WPA3 is more secure than WPA2, it also has certain security issues, which are discussed below.

- **Implementation challenges:** Transition from WPA2 to WPA3 can be difficult for certain devices and networks. Older devices may not support WPA3, leading to compatibility issues unless firmware updates are provided.

- **Limited adoption**: The slow adoption rate of WPA3 is also a significant issue. Many devices and infrastructure components still use WPA2, which limits the overall effectiveness of the WPA3 security enhancement across networks.
- **Resource intensive**: WPA3 uses more complex encryption algorithms, which demand more processing power from devices. This can affect the performance of older devices with limited computational resources.
- **Configuration errors**: Proper implementation and configuration are crucial for maximizing the benefits of WPA3. Errors in configuration, such as weak passwords and poor network setup, can leave networks vulnerable to intrusion despite the advanced protection offered by WPA3.
- **Timing attacks**: WPA3 uses simultaneous authentication of equals (SAE), intended to replace the pre-shared key (PSK) of WPA2. However, certain implementations of SAE have been found to be vulnerable to timing attacks, allowing attackers to potentially recover the password.
- **Cache-based side-channel attacks**: These attacks involve extracting sensitive information from cache access patterns, which can reveal the details of cryptographic operations, potentially leading to the recovery of secure data.
- **Transition mode weakness**: WPA3 supports a "transition mode" to maintain compatibility with older devices that only support WPA2. In transition mode, both WPA3 and WPA2 are enabled, allowing clients to choose which to use. Attackers can exploit the less-secure WPA2 mode to attack the network because WPA2 is still vulnerable to attacks such as KRACK. The presence of WPA2 and WPA3 in transition mode can weaken the overall security posture of the network.
- **Hardware requirements:** WPA3 requires updated hardware to fully support its new features. Many older devices do not support WPA3 and cannot be upgraded for use. Upgrading new hardware that supports WPA3 can be costly for both organizations and individuals.

Objective 03

Explain Different Wireless Threats

Wireless Threats

Access Control Attacks

- Wireless access control attacks aim to penetrate a network by **evading WLAN access control measures**, such as AP MAC filters and Wi-Fi port access controls

- MAC Spoofing
- AP Misconfiguration
- Ad Hoc Associations
- Promiscuous Client
- Client Mis-association
- Unauthorized Association

Integrity Attacks

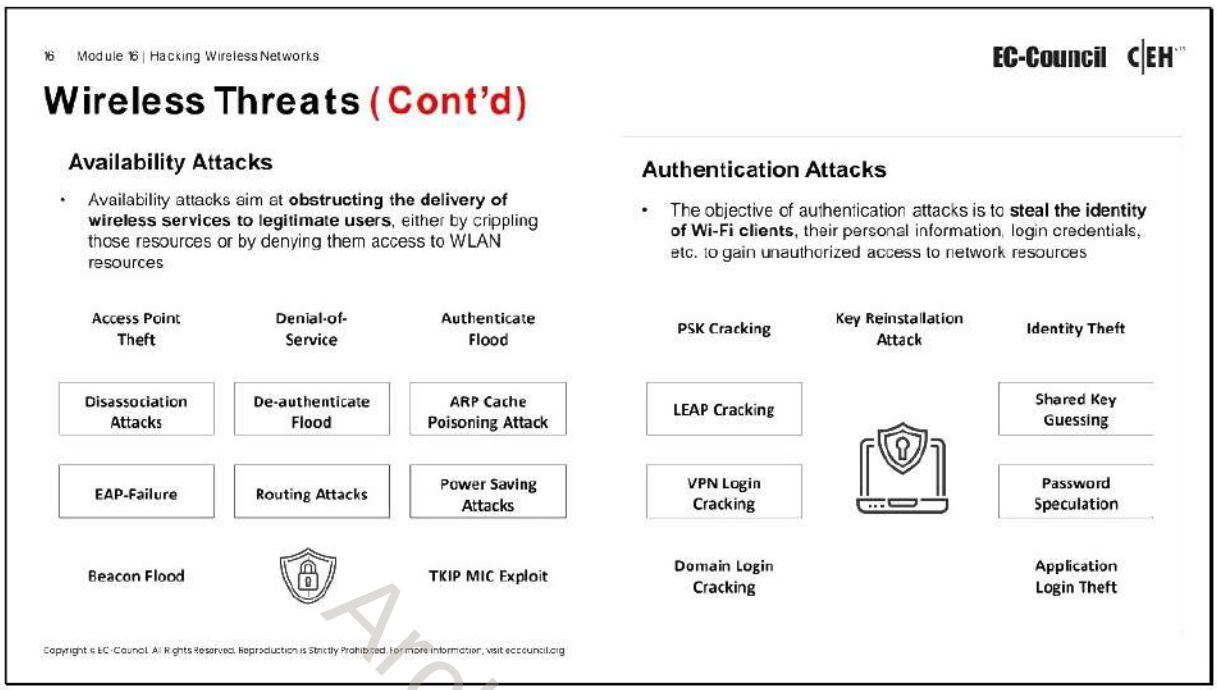
- In integrity attacks, attackers **send forged control, management, or data frames over a wireless network** to misdirect the wireless devices to perform another type of attacks (e.g., DoS)

- Data Frame Injection
- WEP Injection
- Bit-Flipping Attacks
- Extensible AP Replay
- Data Replay
- Initialization Vector Replay Attacks
- RADIUS Replay
- Wireless Network Viruses

Confidentiality Attacks

- These attacks attempt to **intercept confidential information sent over wireless associations**, regardless of whether they were sent in clear text or encrypted by Wi-Fi protocols

- Eavesdropping
- Traffic Analysis
- Cracking WEP Key
- Evil Twin AP
- Honeypot AP
- Session Hijacking
- Masquerading
- Man-in-the-Middle Attack



Wireless Threats

The previous sections discussed basic wireless concepts and wireless security mechanisms such as encryption algorithms that secure wireless network communications. To secure wireless networks, a network administrator needs to understand the various possible weaknesses of encryption algorithms, which may lure attackers. The wireless network can be at risk to various types of attacks, including access-control attacks, integrity attacks, confidentiality attacks, availability attacks, and authentication attacks. This section discusses different types of security risks, threats, and attacks associated with wireless networks.

Access Control Attacks

Wireless access-control attacks aim to penetrate a network by evading WLAN access-control measures, such as AP MAC filters and Wi-Fi port access controls.

There are several types of access-control attacks, including the following.

- **MAC spoofing**: Using the MAC spoofing technique, an attacker can reconfigure a MAC address to appear as an authorized AP to a host on a trusted network. The attacker may use tools such as SMAC to perform this kind of attack.
- **AP misconfiguration**: If a user improperly configures any of the critical security settings at any of the APs, the entire network could be exposed to vulnerabilities and attacks. The AP cannot trigger alerts in most intrusion-detection systems, because these systems recognize them as a legitimate device.

  Most organizations spend significant amounts of time defining and implementing Wi-Fi security policies, but it may be possible for a client of a wireless network to change the

security settings of an AP unintentionally. This, in turn, may lead to misconfigurations in APs. A misconfigured AP can expose an otherwise well-secured network to attacks.

It is difficult to detect a misconfigured AP because it is an authorized, legitimate device on the network. Attackers can easily connect to a secured network through misconfigured APs, which continue to function normally after an attacker connects because no alerts will be triggered even if the attacker uses the connection to compromise security. Many organizations fail to maintain Wi-Fi security policies and do not take proper measures to eliminate this flaw in security configurations.

As the Wi-Fi networks of organizations expand to more locations and more devices, misconfigured APs become increasingly dangerous. The key elements that play an important role in this kind of attack include the following:

- **SSID broadcast**: An attacker configures APs to broadcast SSIDs to authorized users. All AP models have their own default SSID, and APs with default configurations using default SSIDs are vulnerable to brute-force dictionary attacks. Even if users enable WEP, an unencrypted SSID broadcasts the password in plaintext.
- **Weak password**: Some network administrators incorrectly use SSIDs as basic passwords to verify authorized users. SSIDs act as rudimentary passwords and help network administrators recognize authorized wireless devices in the network.
- **Configuration error**: Configuration errors include errors made during installation, configuration policies on an AP, human errors made while troubleshooting WLAN problems, and security changes not implemented uniformly across an architecture. SSID broadcasting is a configuration error that assists attackers in stealing an SSID, which makes the AP assume that the attacker is attempting a legitimate connection.

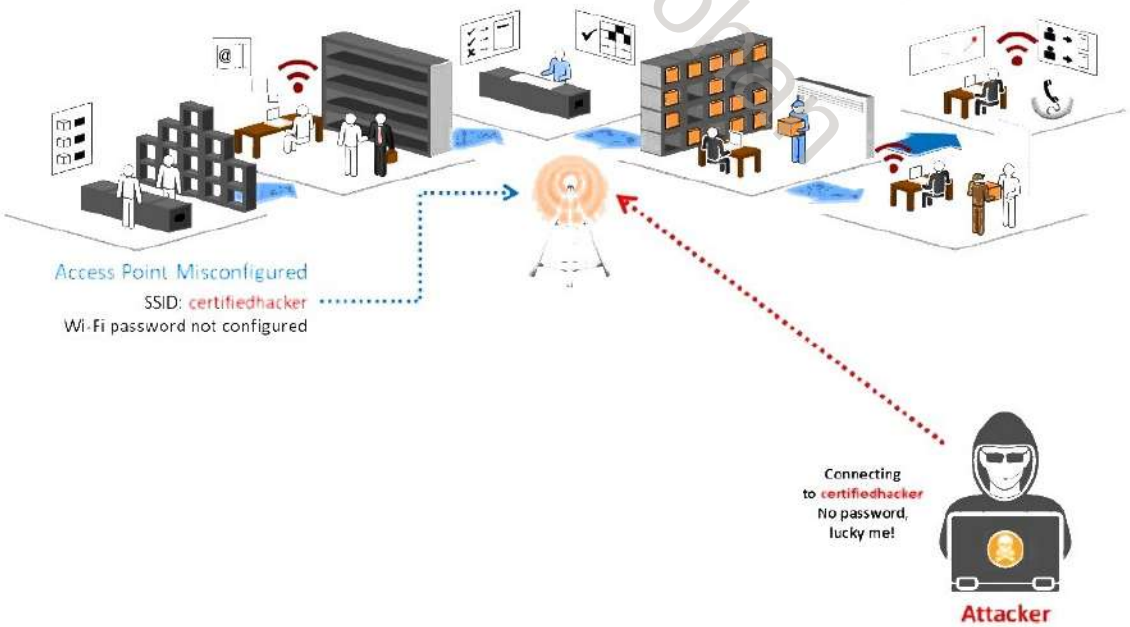


Figure 16.14: Misconfigured AP attack

- **Ad hoc associations**: Wi-Fi clients can communicate directly via an ad-hoc mode that does not require an AP to relay packets. Data can be conveniently shared among clients in ad-hoc networks, which are quite popular among Wi-Fi users. Security threats arise when an attacker forces a network to enable the ad-hoc mode. Some network resources are accessible only in the ad-hoc mode, but this mode is inherently insecure and does not provide strong authentication or encryption. Thus, an attacker can easily connect to and compromise a client operating in the ad-hoc mode. An attacker who penetrates a wireless network can also use an ad-hoc connection to compromise the security of the organization's wired LAN.

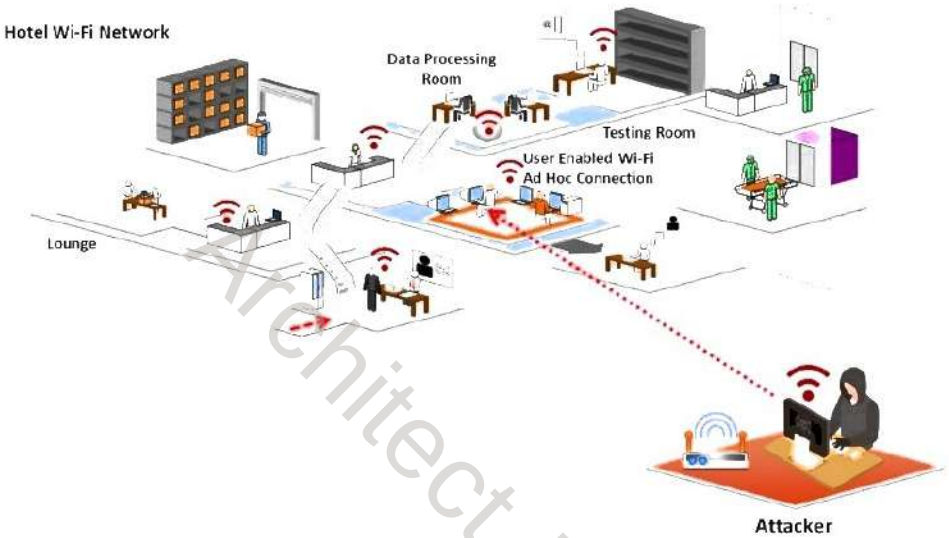


Figure 16.15: Ad-Hoc connection attack

- **Promiscuous client**: Using a promiscuous client, an attacker exploits the behavior of 802.11 wireless cards: they always attempt to find a stronger signal to connect. An attacker places an AP near the target Wi-Fi network and gives it a common SSID, offering an irresistibly stronger signal and higher speed than the target Wi-Fi network. The intent is to lure the client to connect to the attacker's AP, rather than a legitimate Wi-Fi network. Promiscuous clients allow an attacker to transmit target network traffic through a fake AP. It is very similar to the evil-twin threat on wireless networks, in which an attacker launches an AP that poses as an authorized AP by beaconing the WLAN's SSID.

- **Client mis-association**: The client may intentionally or accidentally connect or associate with an AP outside the legitimate network because the WLAN signals travel through the air, walls, and other obstructions. This kind of client mis-association can lead to access-control attacks.

  Mis-association is a security flaw that can occur when a network client connects with a neighboring AP. Client mis-associations can occur for various reasons such as misconfigured clients, insufficient coverage of corporate Wi-Fi, lack of a Wi-Fi policy, restrictions on the use of Internet in the office, ad-hoc connections that administrators

do not manage regularly, and attractive SSIDs. They can occur with or without the knowledge of the wireless client and rogue AP.

To perform a client mis-association attack, an attacker sets up a rogue AP outside the corporation's perimeter. The attacker first learns the SSID of the target wireless network. Using a spoofed SSID, the attacker may send beacons advertising the rogue AP in order to lure clients to connect. The attacker can use the rogue AP as a channel to bypass enterprise security policies. Once a client connects to the rogue AP, an attacker can retrieve sensitive information such as usernames and passwords by launching MITM, EAP dictionary, or Metasploit attacks to exploit client mis-association.

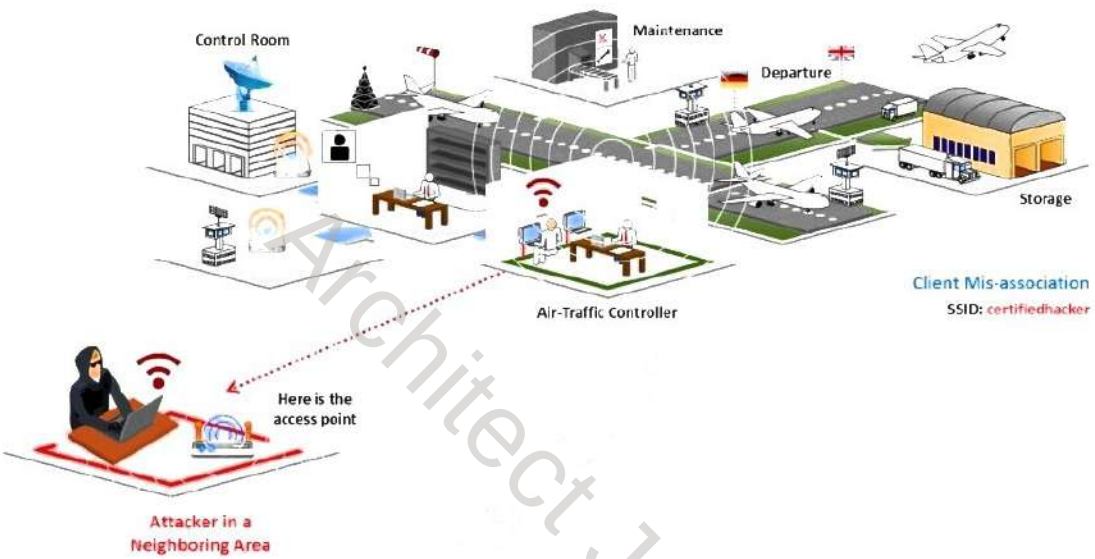


Figure 16.16: Client mis-association attack

- **Unauthorized association**: Unauthorized association is a major threat to wireless networks. It has two forms: accidental association and malicious association. An attacker performs malicious association with the help of soft APs instead of corporate APs. The attacker creates a soft AP, typically on a laptop, by running a tool that makes the laptop's NIC appear as a legitimate AP. The attacker then uses the soft AP to gain access to the target wireless network. Software APs are available on client cards or embedded WLAN radios in some PDAs and laptops; an attacker can launch these directly or through a virus program. The attacker infects the victim's machine and activates soft APs, allowing an unauthorized connection to the enterprise network. An attacker who gains access to the network using unauthorized association may steal passwords, launch attacks on a wired network, or plant Trojans. On the other hand, accidental association involves connecting to the target network's AP from a neighboring organization's overlapping network without the victim's knowledge.

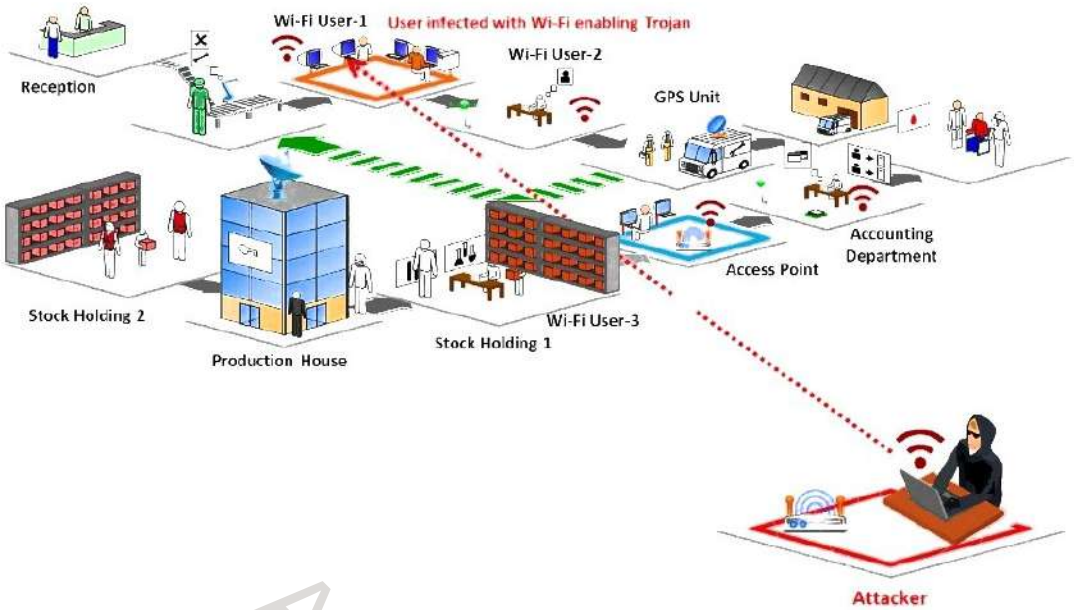


Figure 16.17: Unauthorized association attack

Integrity Attacks

An integrity attack involves changing or altering data during transmission. In wireless integrity attacks, attackers send forged control, management, or data frames over a wireless network to misdirect wireless devices and perform another type of attack such as a DoS attack. The below table summarizes different 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 and 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 16.3: Integrity attacks

Confidentiality Attacks

These attacks attempt to intercept confidential information sent over a wireless network, regardless of whether the system transmits data in cleartext or an encrypted format. If the system transmits data in an encrypted format (such as WEP or WPA), an attacker may attempt to break the encryption. The below table summarizes different 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 such 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 16.4: Confidentiality attacks

Availability Attacks

Availability attacks aim at obstructing the delivery of wireless services to legitimate users, either by crippling WLAN resources or by denying them access to these resources. This attack makes wireless network services unavailable to legitimate users. Attackers can perform availability attacks in various ways, obstructing the availability of wireless networks. The below table summarizes 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 client to make the target unavailable to other wireless devices.	Destruction of connectivity
EAP-Failure	Observing a valid 802.1X EAP exchange and then sending 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, making 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 16.5: Availability attacks

Authentication Attacks

The objective of authentication attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources. The below table summarizes different 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, L0phtCrack, 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 16.6: Authentication attacks

Honeypot AP Attack

If multiple WLANs co-exist in the same area, a user can connect to any available network. Such areas are vulnerable to attacks. Normally, when a wireless client is switched on, it probes a nearby wireless network for a specific SSID. An attacker takes advantage of this behavior of wireless clients by setting up an unauthorized wireless network using a rogue AP. This AP has high-power (high-gain) antennas and uses the same SSID as the target network. Users who regularly connect to multiple WLANs may connect to the rogue AP. Such APs mounted by attackers are called "honeypot" APs. They transmit a stronger beacon signal than legitimate APs so that NICs searching for the strongest available signal may connect to the rogue AP. If an authorized user connects to a honeypot AP, a security vulnerability is created and sensitive user information such as identity, username, and password may be revealed to the attacker.

Figure 16.18: Honeypot AP attack

Wormhole Attack

A wormhole attack exploits dynamic routing protocols such as Dynamic Source Routing (DSR) and the Ad-Hoc On-Demand Distance Vector (AODV). In this attack, an attacker locates themselves strategically in the target network to sniff and record ongoing wireless transmissions. From this location, the attacker advertises that the malicious node has the shortest route for transmitting data to other nodes in the network. To perform sniffing and to record the ongoing communication, the attacker creates a tunnel to forward the data between the source and destination node.

In wireless sensor networks, protocols such as AODV and DSR use route request (RREQ) and route reply (RREP) messages to discover the dynamic route between source and destination nodes. For example, a source node (S) sends an RREQ packet, which is a broadcast message to the destination node (D), and D responds by sending the RREP packet, which is a unicast message. RREP contains the route information to reach D. When S receives this message, it stores this information in its route cache and forwards all the application data to D using this route.

In a wormhole attack, the attacker attempts to build a tunnel between S and D using a malicious node (M) within the transmission range of S and D. The attacker listens to the network traffic waiting for RREQ messages. When S attempts to transmit some application data to D, it first sends an RREQ message to discover the route to D. The attacker sniffs this RREQ message from S and forwards the RREQ message directly to D before the original RREQ message reaches D. Similarly, the attacker sniffs the RREP message from D and forwards it to S before the original RREP message reaches S, thereby creating a fake direct link between S and D via M. After establishing a successful tunnel between S and D, the attacker starts controlling the data flow between the two nodes and may start performing other types of attacks.

Wormhole attacks pose a severe threat to wireless sensor networks because attackers using this attack may manipulate routing and application data in real time, severely impacting the confidentiality, integrity, and availability of network data.

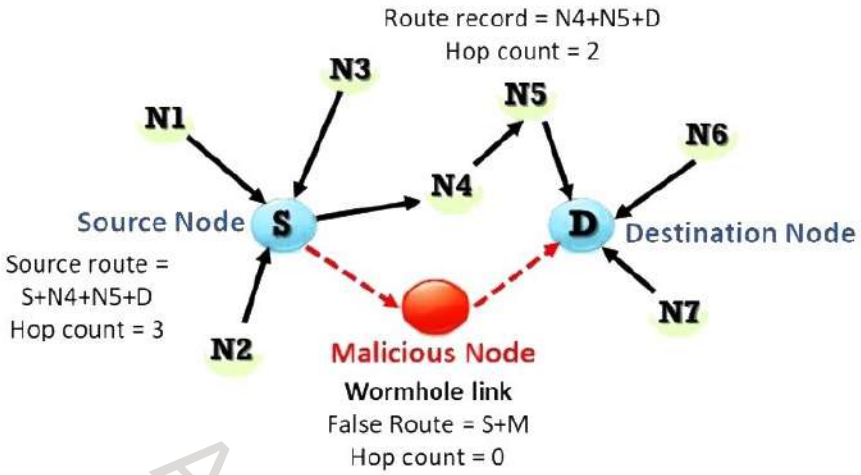


Figure 16.19: Wormhole attack

Sinkhole Attack

A sinkhole attack is a variant of the selective forwarding attack in which the attacker advertises a compromised or malicious node as the shortest possible route to the base station. The attacker places the malicious node near the base station and attracts all the neighboring nodes with fake routing path information and further performs a data forging attack. Attackers use the compromised node to sniff and manipulate all ongoing network transmissions.

A sinkhole attack can also be performed simultaneously with a wormhole attack, where the malicious node can occupy all the network traffic and use the tunneling technique to reach the base station faster than other nodes. A sinkhole attack is complex to detect, and it can adversely affect higher-layer applications in the Open Systems Interconnection (OSI) model.

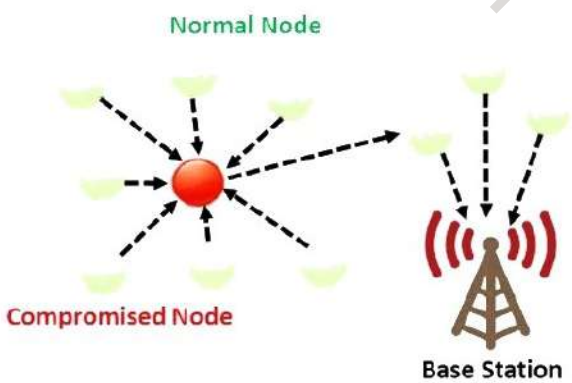
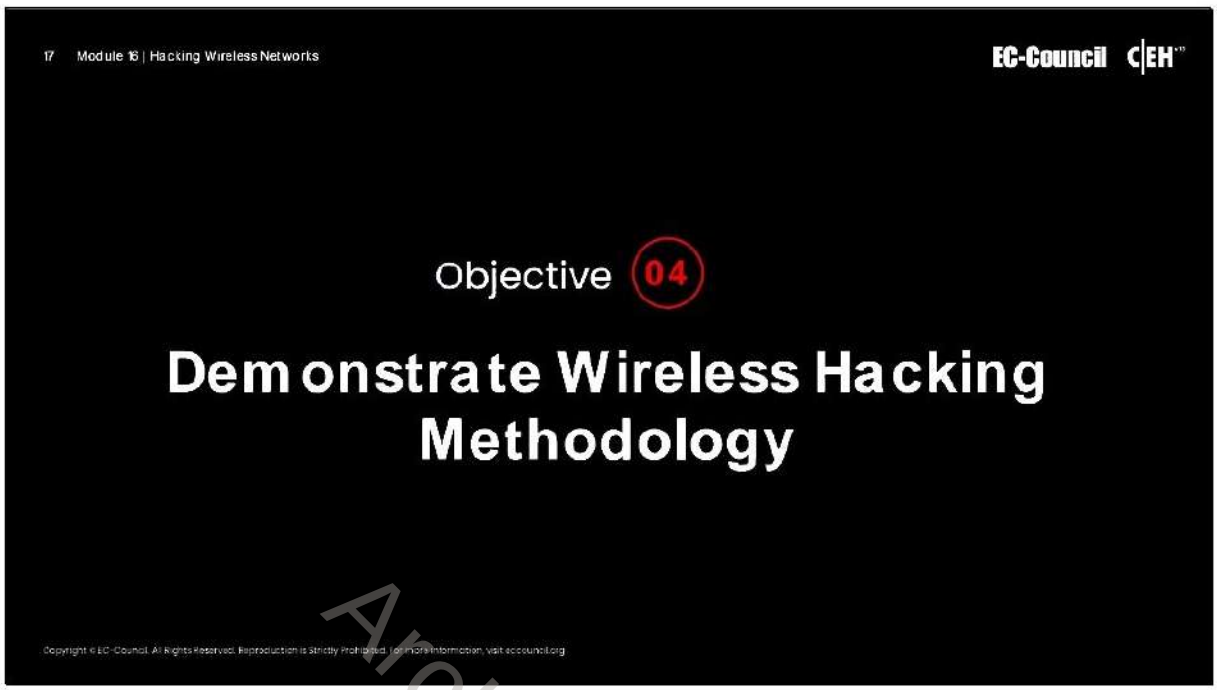
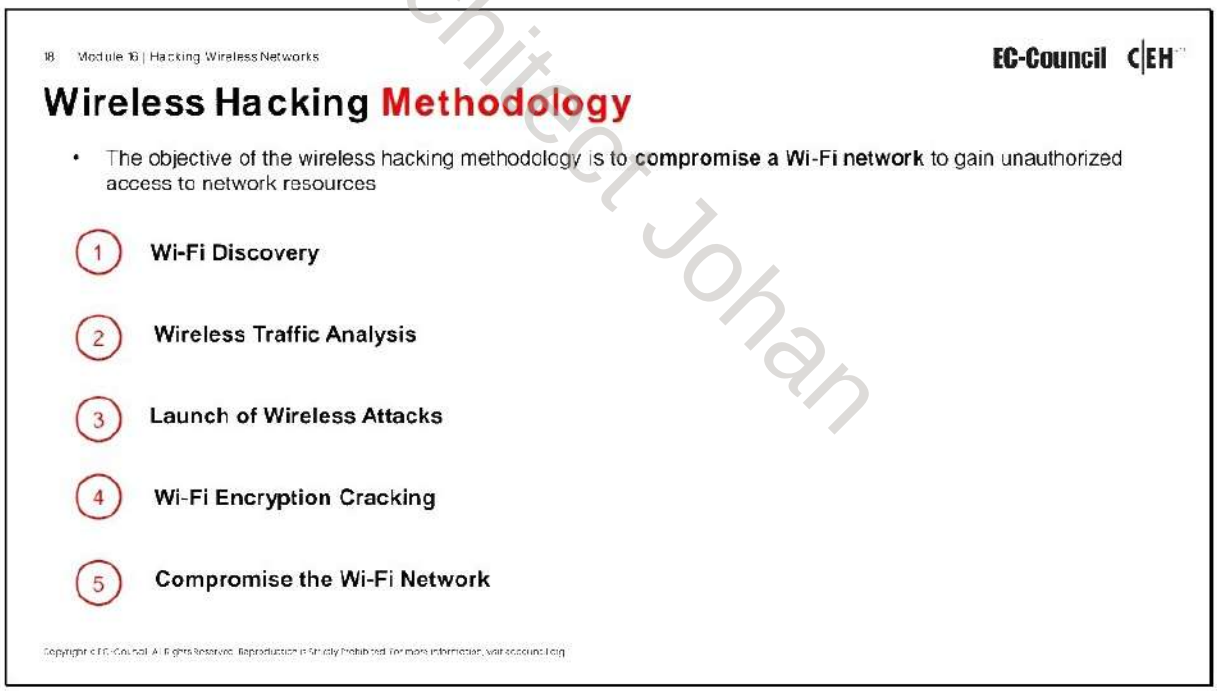


Figure 16.20: Sinkhole attack

Inter-Chip Privilege Escalation/Wireless Co-Existence Attack

An inter-chip privilege escalation attack exploits the underlying vulnerabilities in wireless chips that handle wireless communications such as Bluetooth and Wi-Fi. Manufacturers often design separate chips for Bluetooth and Wi-Fi. Alternatively, they design a combo chip for both types of wireless communications. Attackers leverage combo chips to exploit one chip to steal the data from another chip and make lateral moves to exploit other chips. For example, while sharing resources, a Bluetooth chip can directly capture credentials or other sensitive data from the Wi-Fi chip, or it can manipulate the traffic going through the Wi-Fi chip. This can cause a wireless co-existence attack, which may lead to privilege escalation at chip boundaries.





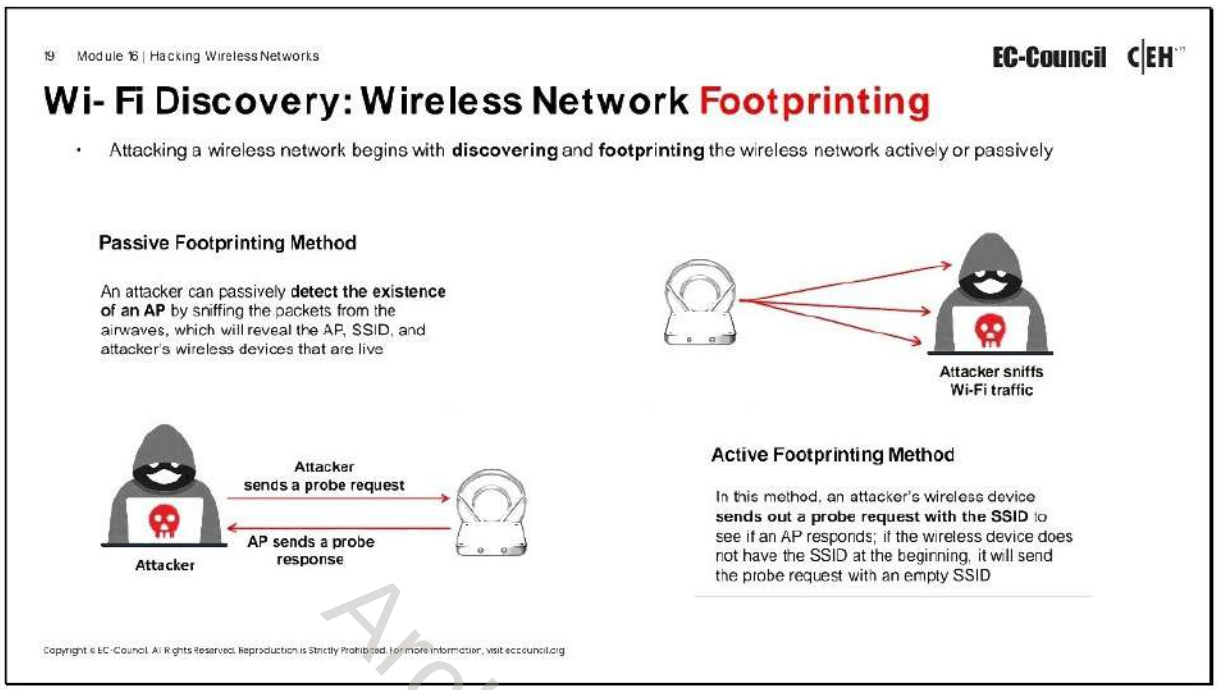
Wireless Hacking Methodology

To hack wireless networks, an attacker follows a hacking methodology involving systematic steps to perform a successful attack on a target wireless network. This section explains the steps of the wireless hacking methodology.

The wireless hacking methodology helps an attacker reach the goal of hacking a target wireless network. An attacker usually follows a hacking methodology to be sure of finding every single-entry point to break into the target network.

The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources. Attackers use the following steps to perform wireless hacking:

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



Wi-Fi Discovery

The first step is to find a Wi-Fi network or device. An attacker performs Wi-Fi discovery to locate a target wireless network using tools such as inSSIDer, NetSurveyor, etc. Wi-Fi discovery procedures include footprinting the wireless networks and finding the appropriate target network that is in range to launch an attack.

Wireless Network Footprinting

An attack on a wireless network begins with its discovery and footprinting. Footprinting involves locating and analyzing (or understanding) the network. To footprint a wireless network, an attacker needs to identify the BSS provided by the AP. An attacker may identify the BSS or independent BSS (IBSS) with the help of the SSID of the wireless network. Therefore, the attacker needs to determine the SSID of the target wireless network, which can be used to establish an association with an AP to compromise its security.

An attacker can use the following two footprinting methods to detect the SSID of a wireless network:

- **Passive Footprinting Method**

  Using the passive method, an attacker detects the existence of an AP by sniffing the packets from airwaves. This discloses wireless devices, APs, and the SSID. In the passive footprinting method, the attacker neither attempts to connect with any APs or wireless clients nor injects any data packet into the wireless traffic.

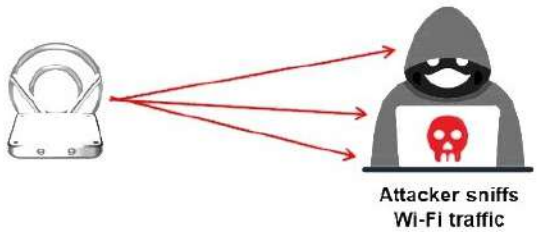


Figure 16.21: Passive footprinting method

- **Active Footprinting Method**

  In this method, the attacker's wireless device sends a probe request with the SSID to an AP and waits for a response. If the wireless device does not have the SSID in advance, it can send a probe request with an empty SSID. In the case of a probe request with an empty SSID, most APs respond with their own SSID in a probe response packet. Consequently, empty SSIDs are useful in learning the SSIDs of APs. In this method, the attacker knows the correct BSS to associate with and can configure the AP to ignore a probe request with an empty SSID.

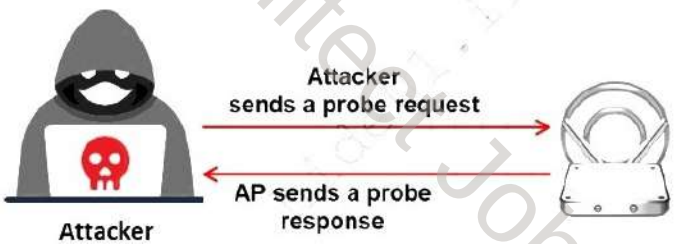


Figure 16.22: Active footprinting method

An attacker can scan for Wi-Fi networks with the help of wireless network scanning tools such as NetSurveyor and Wi-Fi Scanner. The SSID is present in beacons, probe requests, and responses, as well as association and re-association requests. An attacker can obtain the SSID of a network through passive scanning. An attacker who fails to obtain the SSID through passive scanning can detect it through active scanning. Subsequently, the attacker can connect to the wireless network and launch attacks. Wireless network scanning allows sniffing by tuning into various radio channels of the devices.

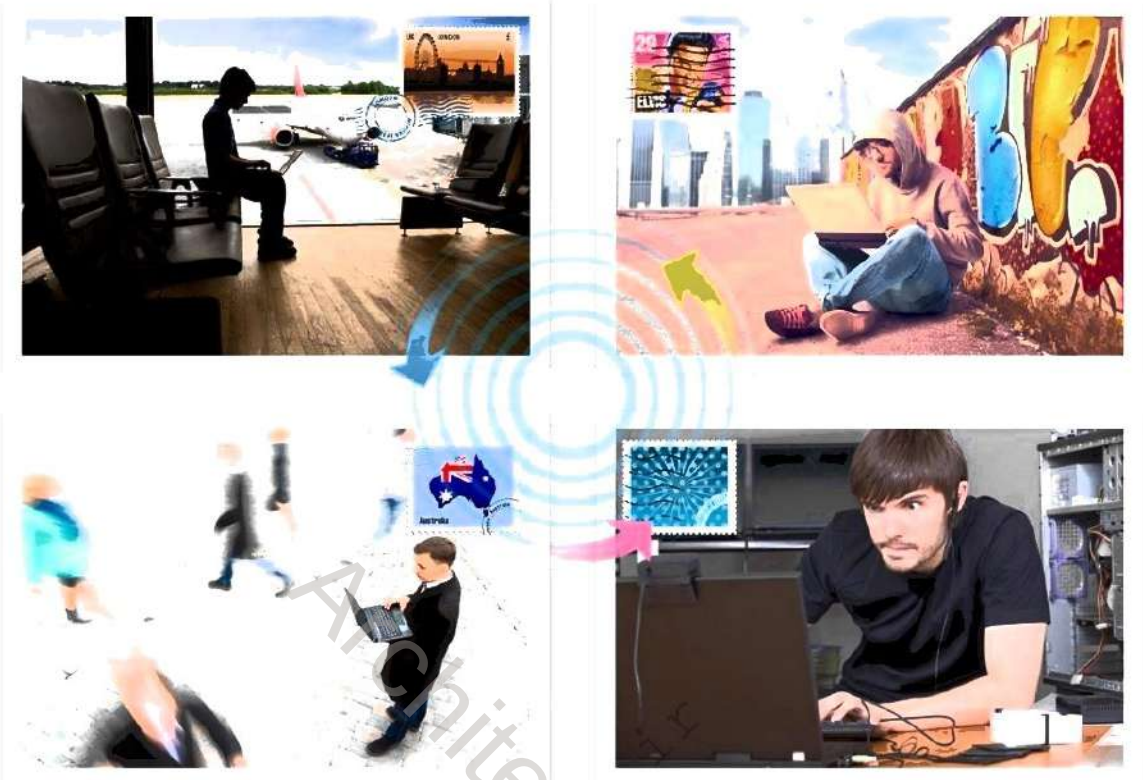
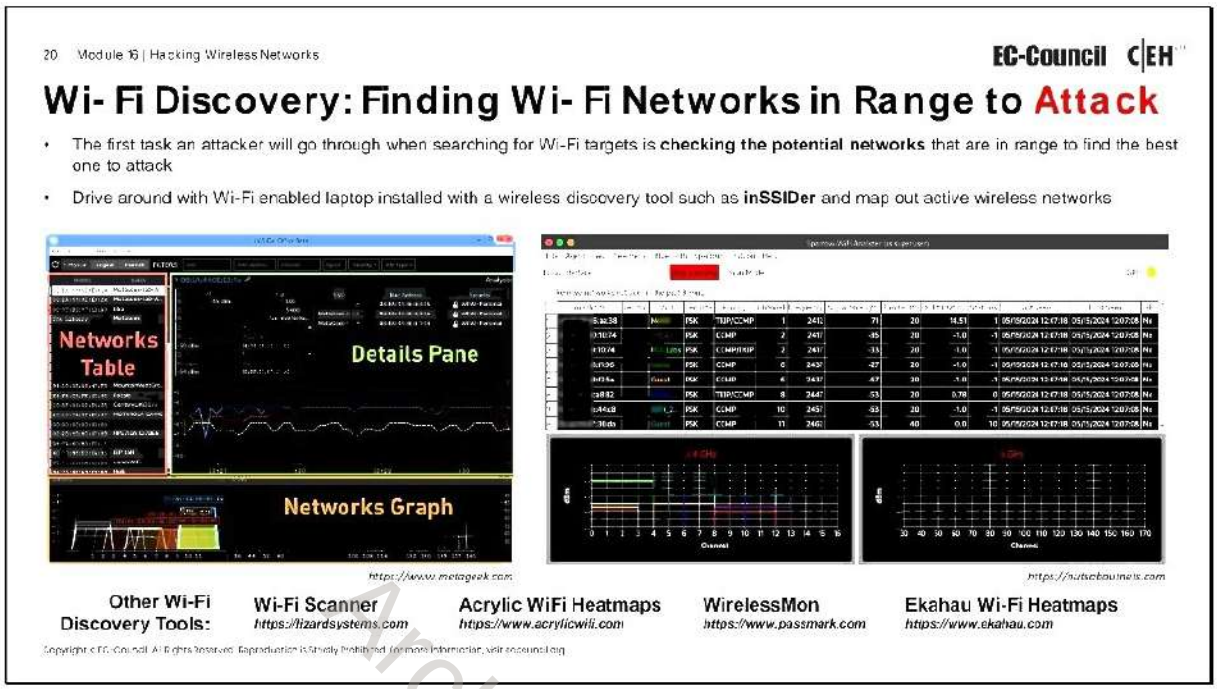


Figure 16.23: Attackers scanning for Wi-Fi networks



Finding Wi-Fi Networks in Range to Attack

The first task for an attacker searching for Wi-Fi targets is to check potential networks that are in range to find the best one to attack. Attackers use various Wi-Fi chalking techniques such as WarWalking, WarChalking, WarFlying, and WarDriving to find a target Wi-Fi network.

- **Wi-Fi Chalking Techniques**
  - **WarWalking**: Attackers walk around with Wi-Fi-enabled laptops installed with a wireless discovery tool to map out open wireless networks.
  - **WarChalking**: Symbols are drawn in public places to advertise open Wi-Fi networks.
  - **WarFlying**: Attackers use drones to detect open wireless networks.
  - **WarDriving**: Attackers drive around with Wi-Fi-enabled laptops installed with a wireless discovery tool to map out open wireless networks.

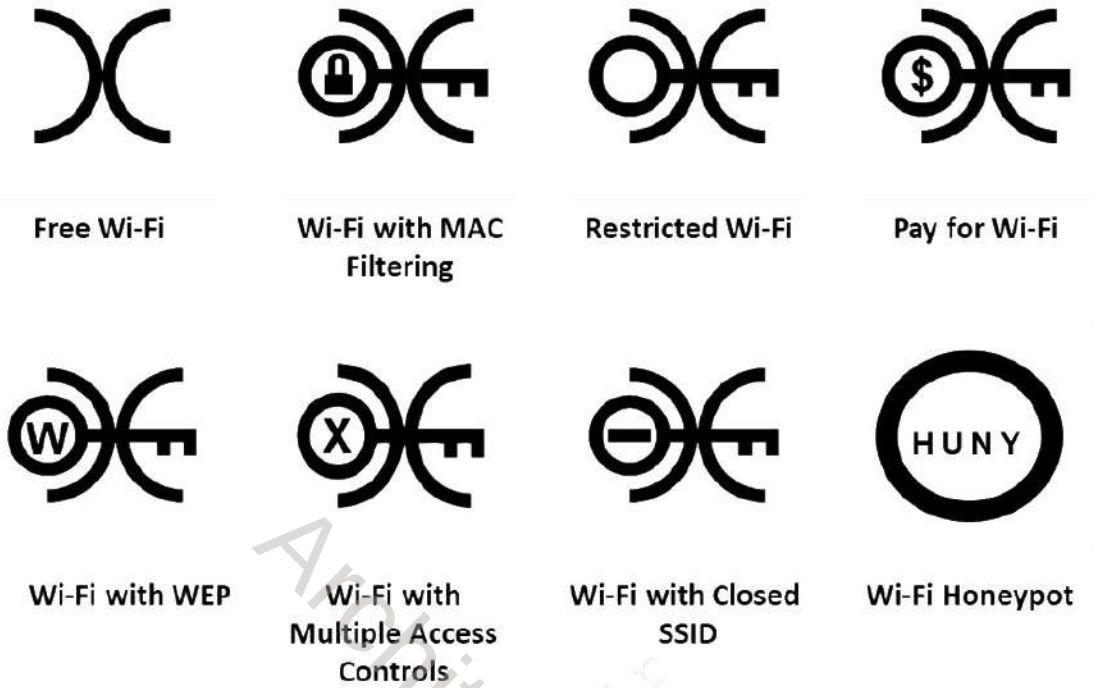


Figure 16.24: Wi-Fi chalking symbols

Attackers use the following tools to discover Wi-Fi networks for launching attacks:

- Laptop with a Wi-Fi card
- External Wi-Fi antenna
- Network discovery software

Some of the tools used to discover Wi-Fi networks in range to attack are inSSIDer, NetSurveyor, Wi-Fi Scanner, and Acrylic WiFi Heatmaps.

Wi-Fi Discovery Tools

- **inSSIDer**

  Source: *https://www.metageek.com*

  inSSIDer is a Wi-Fi optimization and troubleshooting tool that scans for wireless networks with the user's Wi-Fi adapter so that the user can visualize their signal strengths and the channels they are using. It also lists useful information about each network. Attackers use inSSIDer to discover Wi-Fi access points and devices in their vicinity.

  Features:

  - Inspects WLAN and surrounding networks to troubleshoot competing APs
  - Tracks the strength of a received signal in terms of dBm over time and filters APs
  - Highlights APs for areas with high Wi-Fi concentration

- Exports Wi-Fi and GPS data to a KML file to view in Google Earth
- Shows overlapping Wi-Fi network channels

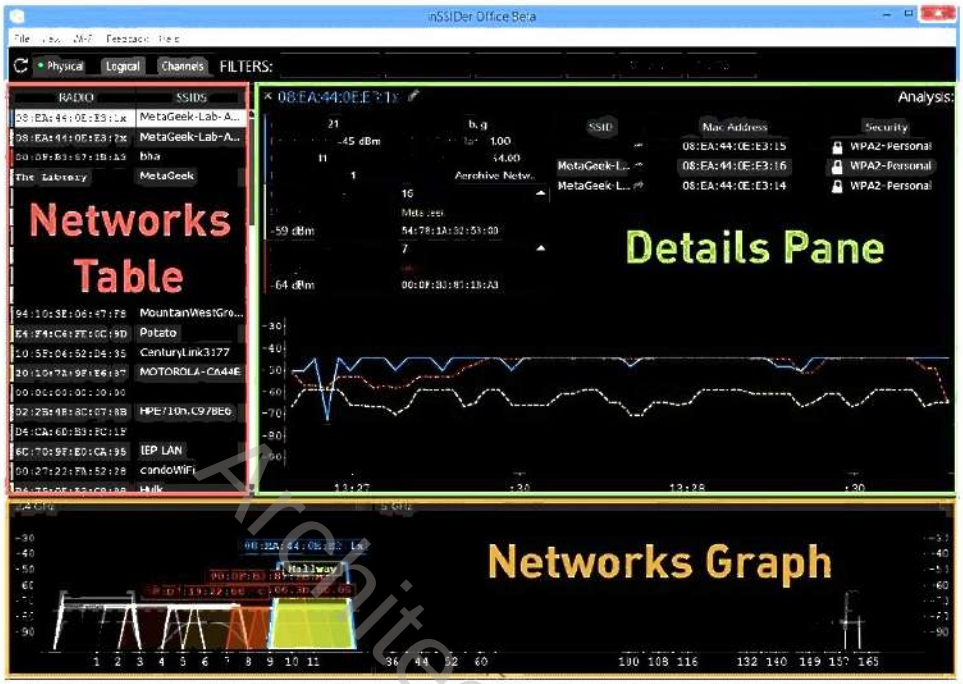


Figure 16.25: Screenshot of inSSIDer

- **Sparrow-wifi**

  Source: *https://github.com*

  Sparrow-Wi-Fi is a GUI-based comprehensive 2.4 GHz and 5 GHz Wi-Fi spectral awareness tool. It allows attackers to integrate software-defined radio (HackRF), advanced Bluetooth tools (Ubertooth), traditional GPS (via gpsd), and drone/rover GPS (via mavlink) to discover Wi-Fi access points, identify SSIDs, perform source hunting, and conduct spectrum analysis. It offers import/export capabilities for CSV and JSON, and can produce Google Maps for the discovered devices.

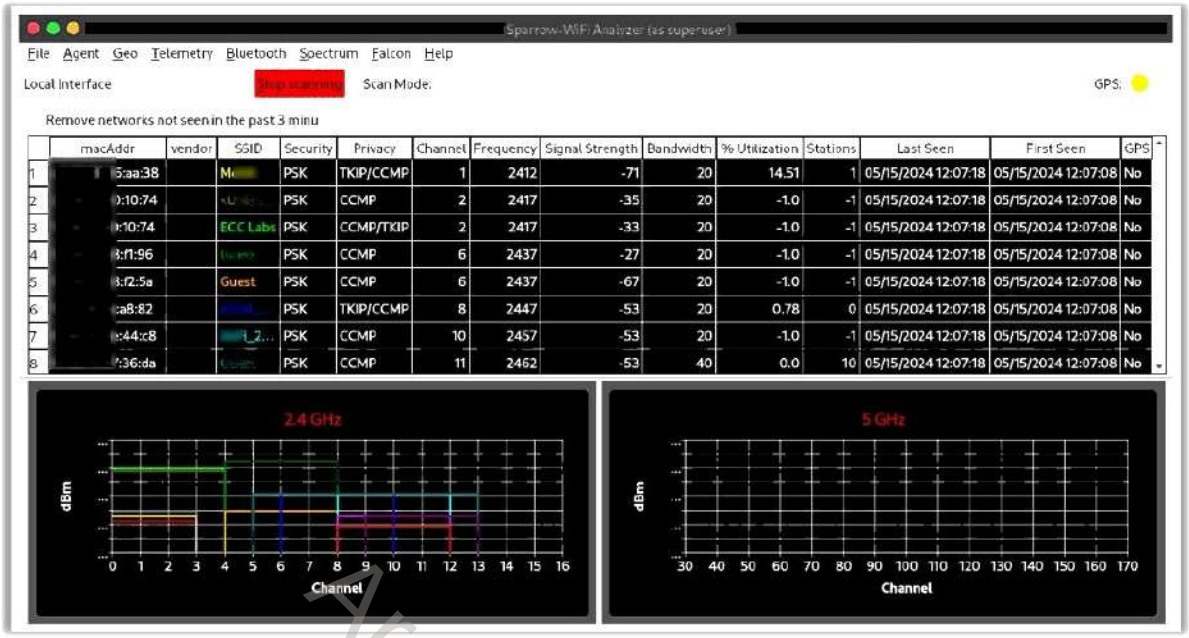


Figure 16.26: Screenshot of Sparrow-wifi

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**

  Source: *https://play.google.com*

  WiFi Analyzer is a Wi-Fi network optimization tool used to examine surrounding Wi-Fi networks, measure their signal strengths, and identify crowded channels. Attackers use WiFi Analyzer to detect nearby APs, graph the signal strengths of channels, estimate distances to APs, etc.

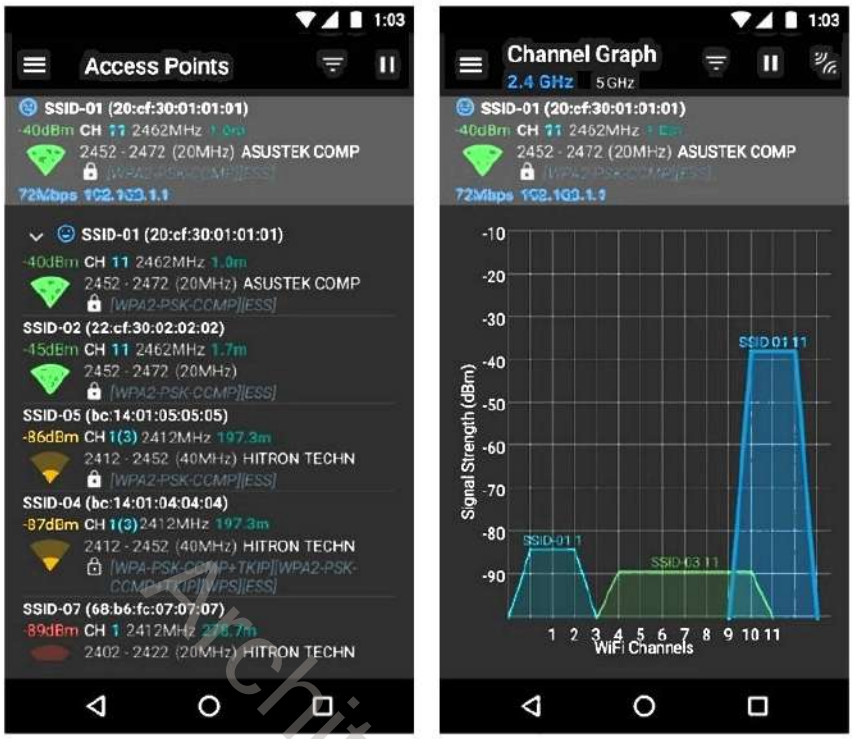
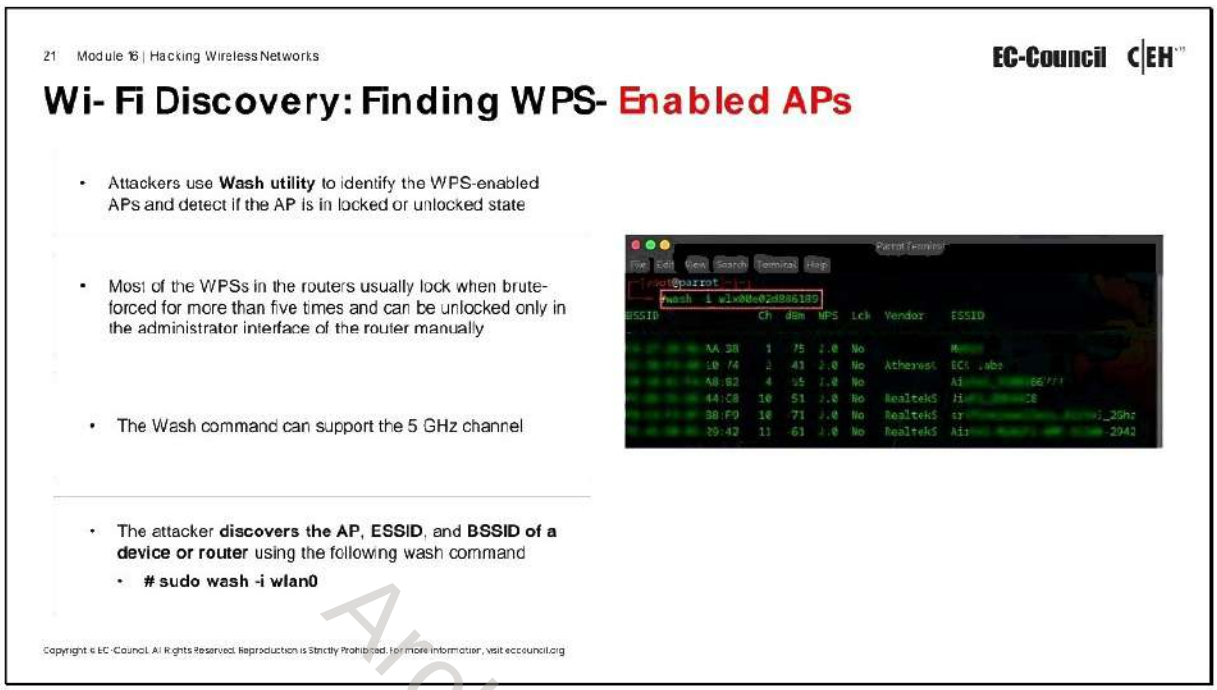


Figure 16.27: Screenshot of WiFi Analyzer

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 use the Wash command-line utility to identify WPS-enabled APs in the target wireless network. This utility also helps attackers check whether the AP is in a locked state. Most WPS-enabled routers are locked automatically when incorrect credentials are entered more than 5 times consecutively, and they can be unlocked only in the administrator interface of the router manually. The Wash command supports the 5 GHz channel and can be used by installing the Reaver package.

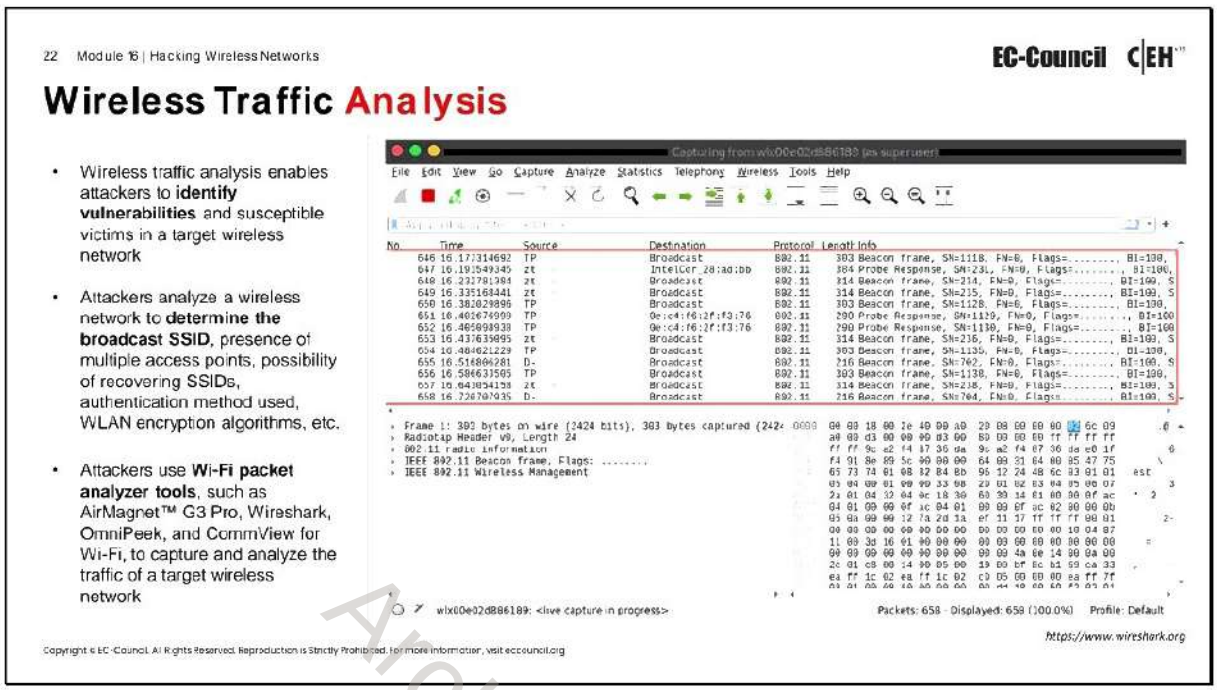
The following are some of the important arguments of the Wash command that are used by attackers:

- **-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 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])

Attackers use the following command to discover the access point, extended service set identifier (ESSID), and BSSID of a device or router:

```
# sudo wash -i wlan0
```

Figure 16.28: Screenshot showing the output of the Wash command



Wireless Traffic Analysis

The next step in the wireless hacking methodology is to analyze the traffic of the discovered wireless network. An attacker performs wireless traffic analysis before launching actual attacks on the wireless network. This analysis helps the attacker determine the vulnerabilities and susceptible victims in the target network as well as the appropriate strategy for a successful attack. The attacker uses various tools and techniques to analyze the traffic of the target wireless network.

Wi-Fi protocols are unique to Layer 2, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets. Attackers analyze a wireless network to determine the broadcasted SSID, presence of multiple APs, possibility of recovering SSIDs, authentication method used, WLAN encryption algorithms, etc. Attackers use Wi-Fi packet sniffing tools such as AirMagnet™ G3 Pro, Wireshark, Riverbed Packet Analyzer, OmniPeek, and CommView for Wi-Fi to capture and analyze the traffic of a target wireless network.

Sniffing is a type of eavesdropping in which attackers intercept all ongoing wireless communication. Attackers perform wireless sniffing by simply tuning a receiver to the target transmission frequency and identifying the target communication protocol used. Attackers analyze the captured traffic to perform further attacks on the target network. To sniff wireless traffic, an attacker needs to enable the monitor mode on their Wi-Fi card.

All Wi-Fi cards do not support the monitor mode in Windows. The following link can be used to check whether a Wi-Fi card supports the monitor mode: *https://secwiki.org/w/Npcap/WiFi_adapters*

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

- **Wireshark**

  Source: *https://www.wireshark.org*

  Wireshark is a network protocol sniffer and analyzer. It allows users to capture and interactively browse the traffic in a target network. Wireshark can read live data from Ethernet networks, Token Ring networks, FDDI networks, Point-to-Point Protocol (PPP) and Serial Line Internet Protocol (SLIP) networks, 802.11 wireless LAN, automated teller machine (ATM) connections (if the ATM's OS allows Wireshark to do so), and any device supported on Linux by recent versions of libpcap. Npcap is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

  Attackers capture wireless traffic by enabling the monitor mode in Wireshark. Wireshark allows attackers to capture a huge amount of management frames, control frames, data frames, etc. and further helps them analyze Radiotap header fields to gather critical information such as the protocols used, encryption techniques used, frame lengths, and MAC addresses.

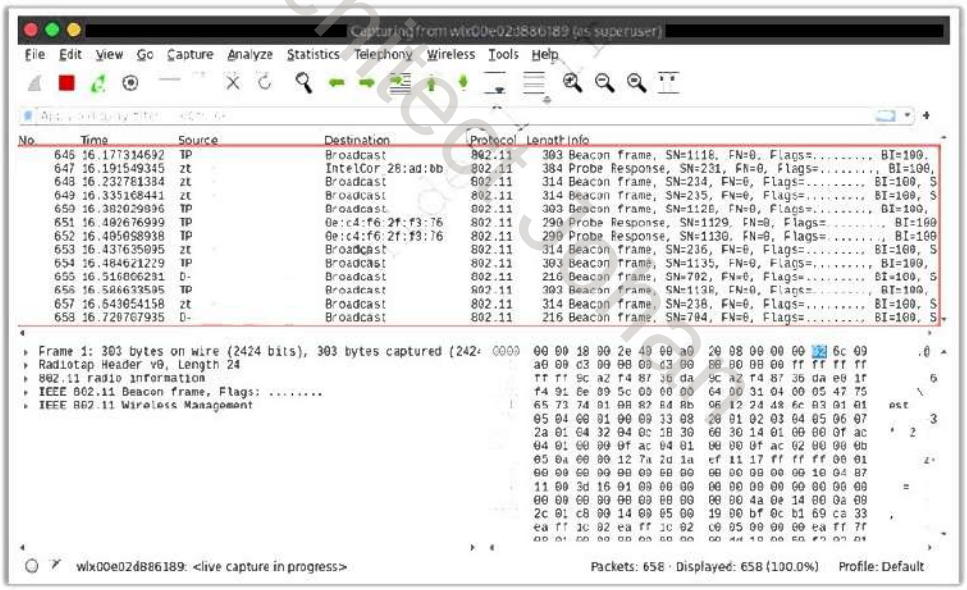


Figure 16.29: Screenshot showing Wireshark capturing wireless traffic

- **CommView for Wi-Fi**

  Source: *https://www.tamos.com*

  CommView for Wi-Fi is a wireless network monitor and analyzer for 802.11 a/b/g/n networks. It captures packets and displays important information such as the list of APs and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, and protocol distribution charts.

A user can decrypt the packets with user-defined WPA-PSK keys and decode them down to the lowest layer. This network analyzer reveals every detail of a captured packet using a convenient tree-like structure to display protocol layers and packet headers.

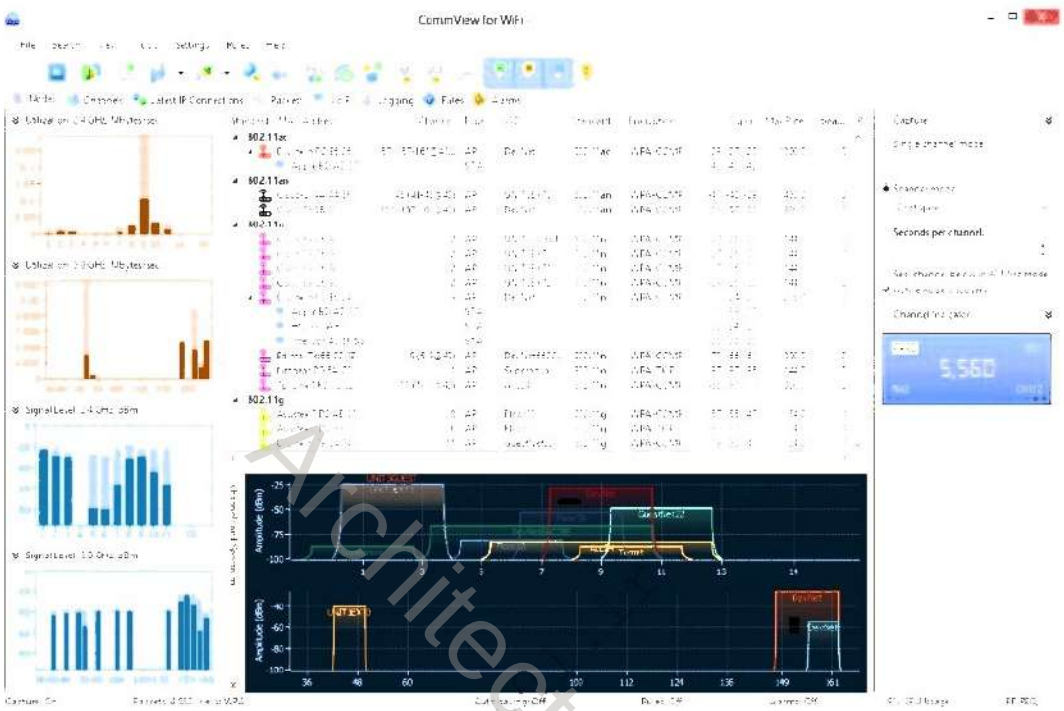
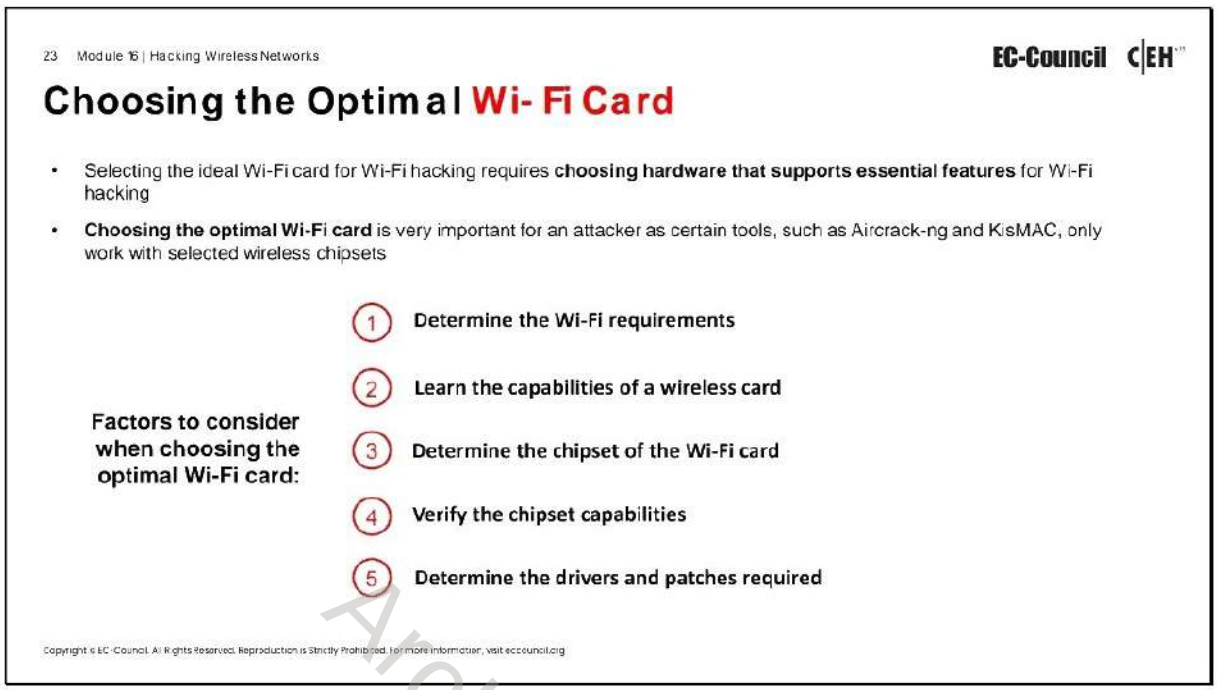


Figure 16.30: Screenshot of CommView for Wi-Fi

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 ideal Wi-Fi card for Wi-Fi hacking requires choosing hardware that supports essential features for Wi-Fi hacking. Choosing the optimal Wi-Fi card is very important for an attacker because tools such as Aircrack-ng and NetSpot work only with selected wireless chipsets. An attacker considers the following when choosing the optimal Wi-Fi card.

- **Determine the Wi-Fi requirements**: An attacker may want to listen to wireless network traffic or both listen to and inject packets. Windows systems can listen to network traffic but do not have the capability of injecting data packets, whereas Linux has the capability of both listening and injecting packets. Based on these issues, the attacker chooses the OS; hardware format, such as Personal Computer Memory Card International Association (PCMCIA) and USB; and features, such as listening, injection, or both.
- **Learn the capabilities of a wireless card**: Wireless cards have two manufacturers. One is the brand of the card, and the other is the chipset manufacturer. Knowing the card manufacturer and model is not sufficient to choose the Wi-Fi card. The attacker must also know about the chipset of the card. Most card manufacturers are reluctant to reveal the chipset used in their cards, but this information is critical for the attacker because it allows the attacker to determine the supported OS, the required software drivers, and limitations.
- **Determine the chipset of the Wi-Fi card**: An attacker can determine the chipset of a Wi-Fi card using the following techniques.
  - Search the Internet.
  - View Windows driver filenames, which often reveal the chipset name.
  - Check the manufacturer's page.

- The wireless chip can be directly viewed for some cards. Often, the chipset number can also be observed.
- The Federal Communications Commission (FCC) ID Search can be used to look up detailed information on the device if an FCC identification number is printed on the board. This search will return information on the manufacturer, model, and chipset.

Card manufacturers occasionally change the card chipset while retaining the model number. Manufacturers may call this a "card revision" or "card version." Therefore, an attacker's search must include the version or revision. The method to determine it may vary by OS. The site *https://wireless.wiki.kernel.org/en/users/Drivers* may provide compatibility information.

- **Verify the chipset capabilities**: Before choosing a Wi-Fi card, the attacker must verify that the chipset is compatible with the OS and that it meets all requirements.
- **Determine the drivers and patches required**: Attackers must determine the drivers required for the chipset and any patches required for the OS.

After considering all these aspects to choose a chipset, the attacker chooses a card that uses that specific chipset with the help of a compatible card list.

Perform Spectrum Analysis

An attacker can use spectrum analyzers to discover the presence of wireless networks. The spectrum analysis of wireless networks enables an attacker to actively monitor the spectrum usage in a particular area and detect the spectrum signal of the target network. It also helps the attacker measure the spectrum power of known and unknown signals. Spectrum analyzers employ statistical analysis to plot spectrum usage, quantify "**air quality,**" and isolate transmission sources. RF technicians use RF spectrum analyzers to install and maintain wireless networks and identify sources of interference. Wi-Fi spectrum analysis also helps in the detection of wireless attacks, including DoS attacks, authentication/encryption attacks, and network penetration attacks.

The following are some of the automated tools used by attackers for the spectrum analysis of a target wireless network.

- **RF Explorer**

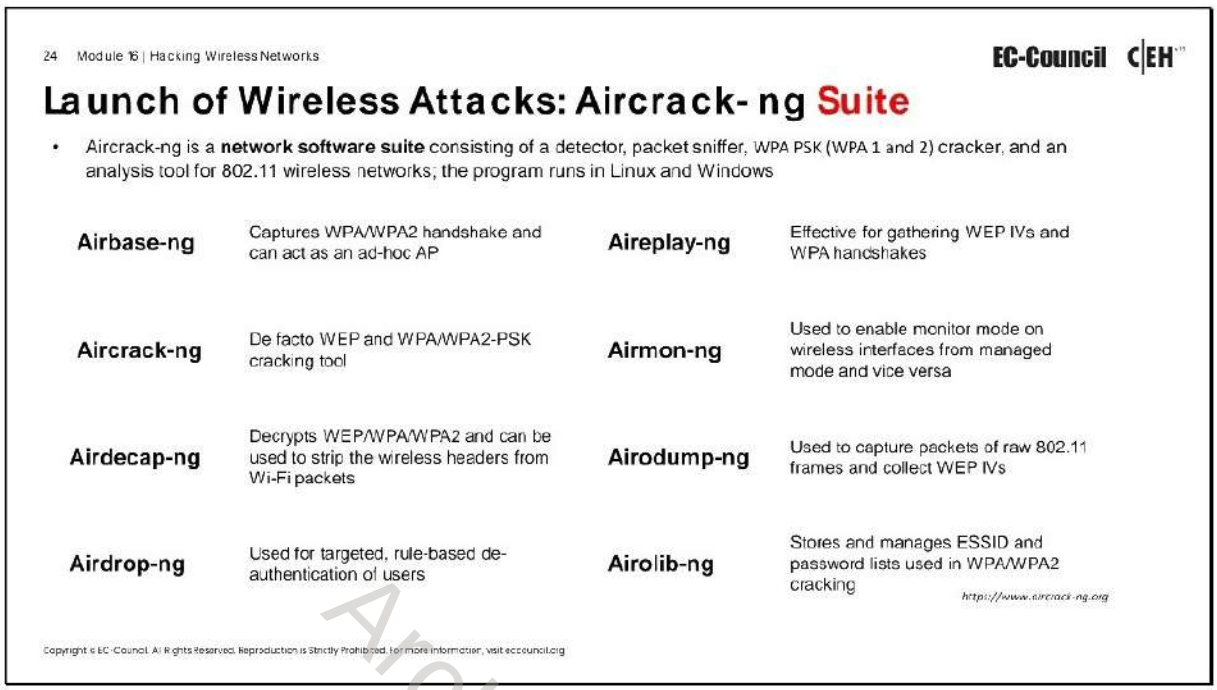
  Source: *https://rfexplorer.com*

  RF Explorer is an RF spectrum analysis tool. It can operate as a standalone, handheld RF spectrum analyzer or interface with a PC running more sophisticated data analysis software. An RF spectrum analyzer is the instrument of choice for the initial detection and identification of RF interference sources and the subsequent monitoring of the health of a wireless system. RF Explorer is a basic tool used for observing transmitted RF signals and aids the user by providing a view of the local RF environment. This RF view can be used to help detect the presence of RF transmissions that are interference source.

Figure 16.31: Screenshot of 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

After completing the wireless network discovery, mapping, and analysis of the target wireless network, an attacker will be in a position to launch an attack on the target wireless network. The attacker may launch various types of attacks such as fragmentation attacks, MAC spoofing attacks, DoS attacks, and Address Resolution Protocol (ARP) poisoning attacks. This section describes wireless attacks and how they are performed.

Aircrack-ng Suite

Source: *https://www.aircrack-ng.org*

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA PSK (WPA 1 and 2) cracker, and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.

- **Airbase-ng**: It captures the WPA/WPA2 handshake and can act as an ad-hoc AP.
- **Aircrack-ng**: This program is the de facto WEP and WPA/WPA2 PSK cracking tool.
- **Airdecap-ng**: It decrypts WEP/WPA/WPA2 and can be used to strip wireless headers from Wi-Fi packets.
- **Airdrop-ng**: This program is used for the targeted, rule-based de-authentication of users.
- **Aireplay-ng**: It is especially effective for gathering initialization vectors (WEP IVs) and WPA handshakes, which can then be utilized with aircrack-ng for further analysis and potential network security testing.

- **Airgraph-ng**: This program creates a client–AP relationship and common probe graph from an airodump file.
- **Airmon-ng**: It is used to switch from the managed mode to the monitor mode on wireless interfaces and vice versa.
- **Airodump-ng**: This program is used to capture packets of raw 802.11 frames and collect WEP IVs.
- **Airolib-ng**: This program stores and manages ESSID and password lists used in WPA/ WPA2 cracking.
- **Airtun-ng**: It creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network.

Detection of Hidden SSIDs

Based on the principle of security through obscurity, many organizations hide the SSID of their wireless networks without broadcasting them. This is part of the security policy of many organizations because an attacker may take advantage of the SSID to breach the security of their wireless networks. However, hiding SSIDs does not increase security. An attacker can reveal a hidden SSID using the aircrack-ng suite and mdk3 through the following steps.

- Run airmon-ng in the monitor mode using the command **`airmon-ng start <Wireless interface>`**. If any process causes trouble, first run **`airmon-ng check kill`** command.

Figure 16.32: Screenshot of the execution of airmon-ng start

- Start airodump-ng to discover SSIDs on the interface

Figure 16.33: Screenshot of the execution of airodump-ng start

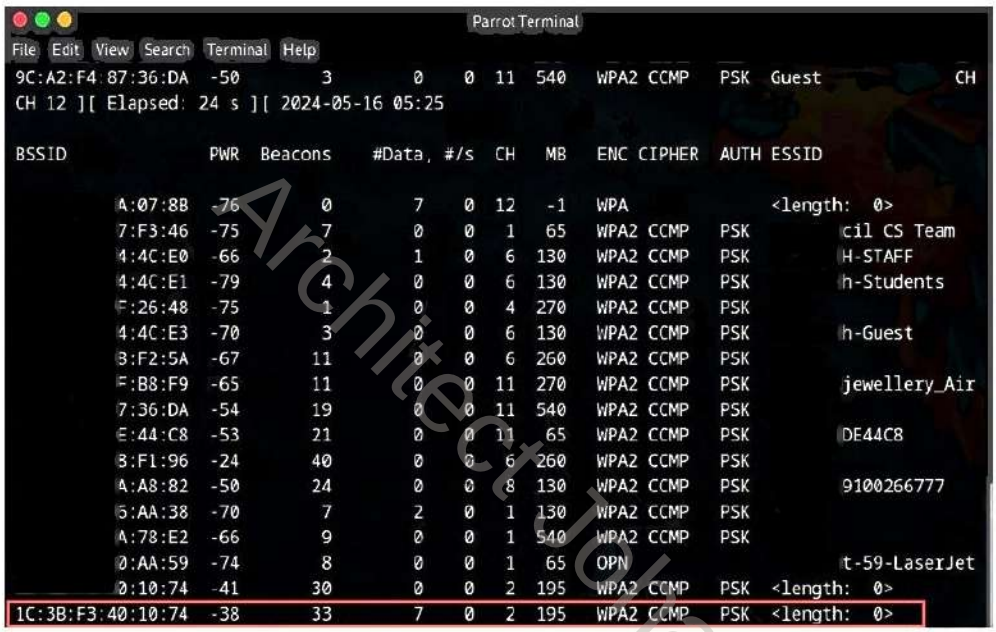


Figure 16.34: Screenshot of the execution of airodump-ng

The SSID of the targeted access point is hidden as shown in the above screenshot

- Open another terminal as root and run **`mdk3 <Wireless Interface> p -b 1 -c <Channel> -t < Target BSSID>`** command to brute force and retrieve the actual hidden SSID

  In the command,

  - p: Basic probing and ESSID Brute-force mode
  - -b: Beacon flood mode
  - 1: EAPOL logoff test
  - -c: Selection channel (here, 2)
  - -t: Target BSSID (here, 1C:3B:F3:40:10:74)
  - wlx00e02d886189: Wireless interface

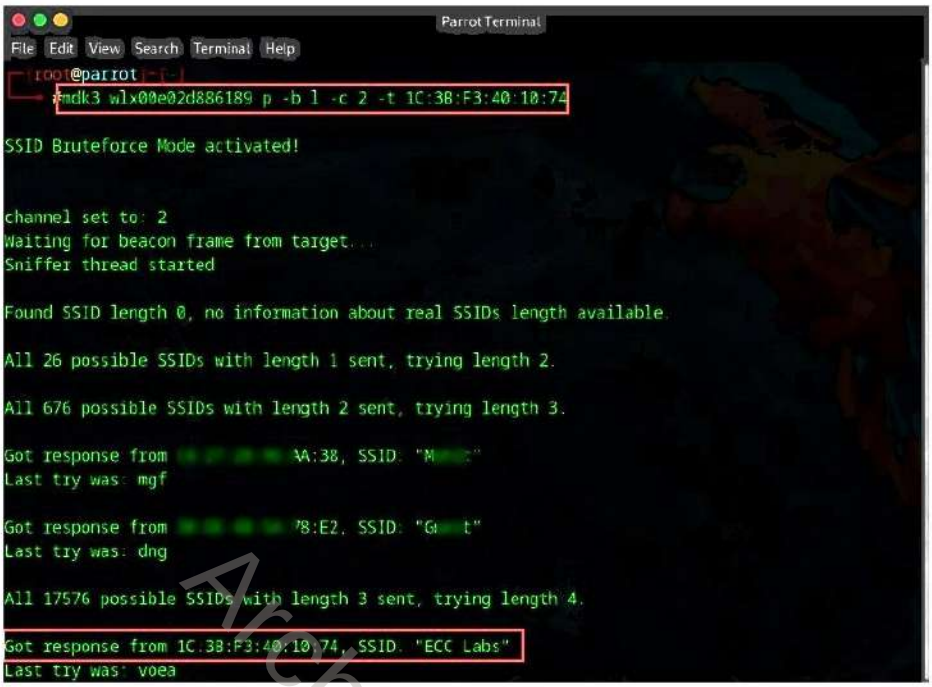
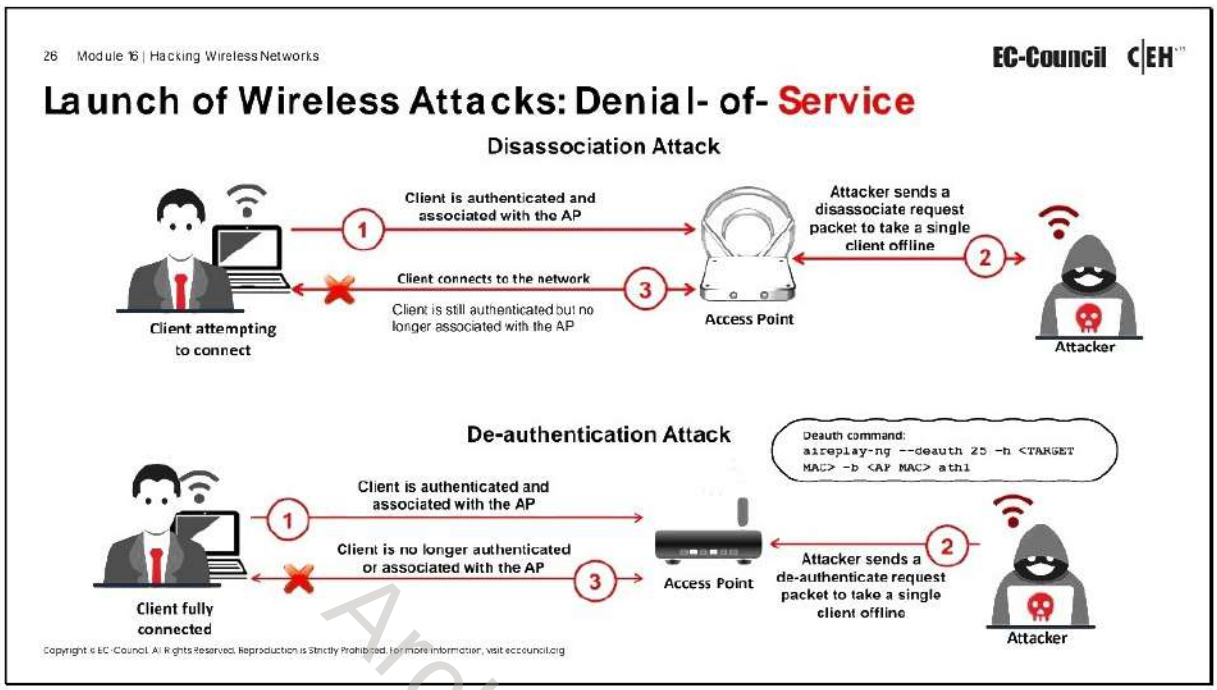


Figure 16.35: Screenshot of mdk3 displaying result in revealing SSID



Denial-of-Service

Wireless networks are vulnerable to DoS attacks because of the relationships among the physical, data-link, and network layers. These networks operate in unlicensed bands with data transmission in the form of radio signals. The designers of the MAC protocol aimed at simplicity, but it is vulnerable to DoS attacks. WLANs usually carry mission-critical applications such as VoIP, database access, project data files, and Internet access. Disrupting these applications on WLANs through a DoS attack is easy and can cause a loss of productivity or network downtime.

Wireless DoS attacks disrupt wireless network connections by broadcasting de-authenticate commands. The transmitted de-authentication forces the clients to disconnect from the AP.

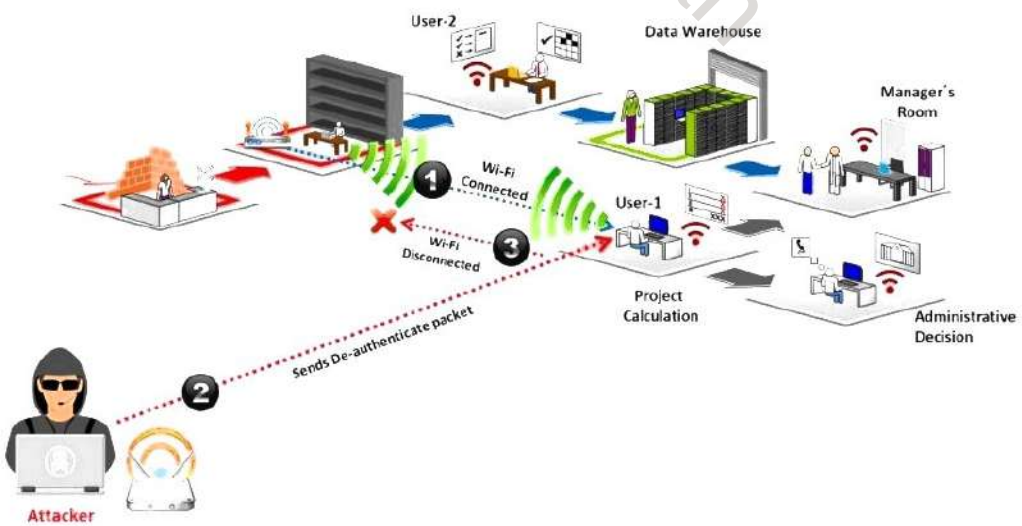


Figure 16.36: DoS attack

Wireless DoS attacks include disassociation attacks and de-authentication attacks.

- **Disassociation Attack**

  In a disassociation attack, the attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the AP and client.

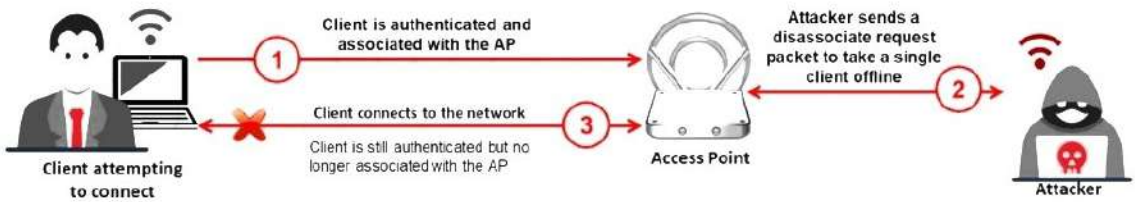


Figure 16.37: Disassociation attack

- **De-authentication Attack**

  In a de-authentication attack, the attacker floods station(s) with forged de-authenticates or disassociates to disconnect users from an AP.

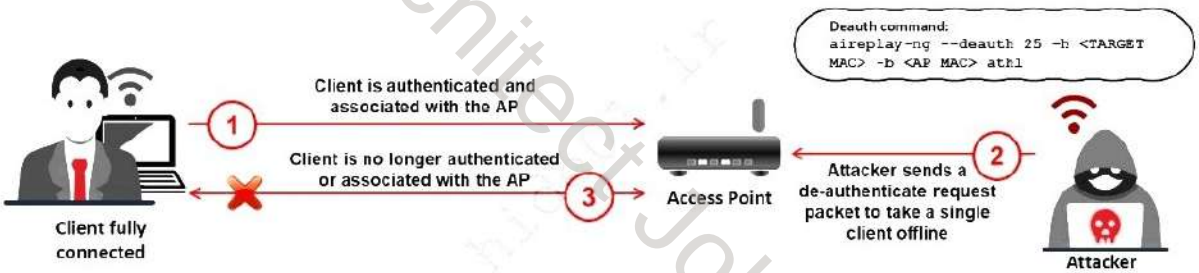
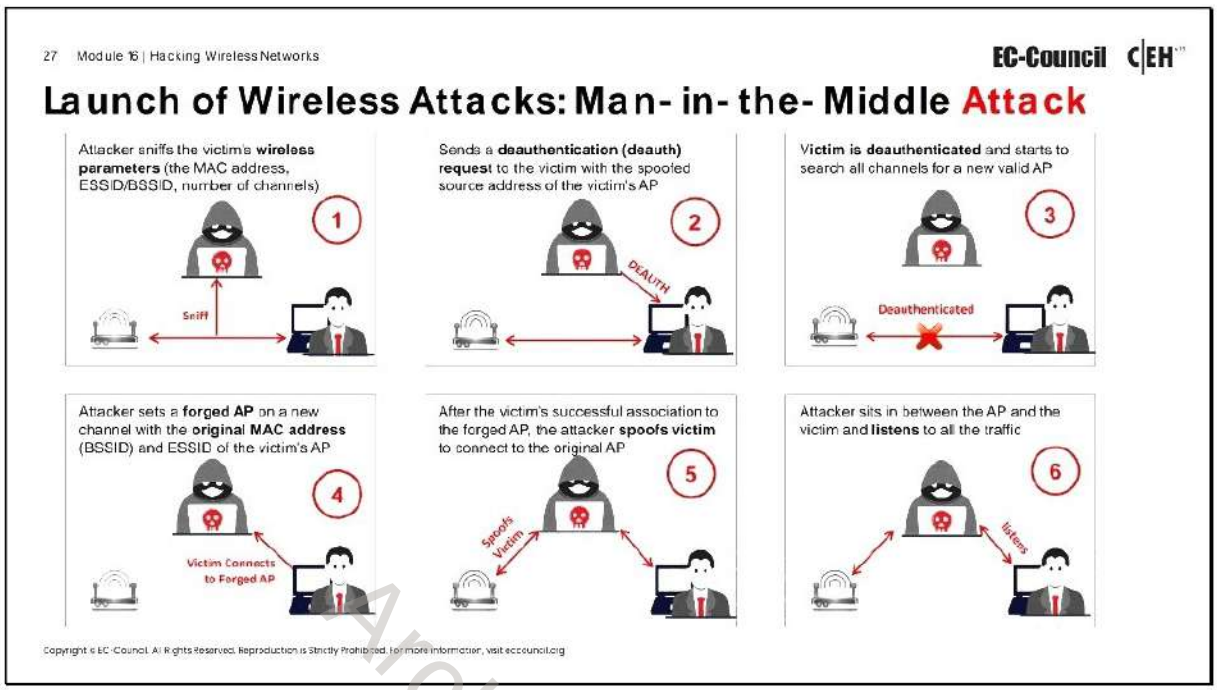


Figure 16.38: De-authentication attack



Man-in-the-Middle Attack

A man-in-the-middle (MITM) attack is an active Internet attack in which the attacker attempts to intercept, read, or alter information transmitted between two computers. MITM attacks are associated with 802.11 WLANs as well as wired communication systems.

- **Eavesdropping**

  Eavesdropping is easy in a wireless network because no physical medium is used for communication. An attacker in the vicinity of a wireless network can receive radio waves on the wireless network without much effort or equipment. Furthermore, the attacker can examine the entire data frame sent across the network or store it for later assessment.

  Several layers of encryption need to be implemented to prevent attackers from obtaining sensitive information. WEP or data-link encryption can be used in these layers. Further, a security mechanism such as IPsec, SSH, or SSL must be used, failing which sent data may be available to attackers.

  However, as demonstrated in a previous section, an attacker can crack WEP with tools freely available on the Internet. Accessing email using the Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) is risky because these protocols can send an email over a wireless network without any form of extra encryption. A skilled hacker can potentially log gigabytes of WEP-protected traffic, post-process the data, and break the encryption.

- **Manipulation**

  Manipulation is a level beyond eavesdropping. It occurs when an attacker receives the victim's encrypted data, manipulates it, and retransmits the manipulated data to the victim. In addition, an attacker can intercept packets with encrypted data and change the destination address to forward these packets across the Internet.

An attacker performs an MITM attack through the following steps.

- The attacker sniffs the victim's wireless parameters (MAC address, ESSID/BSSID, and number of channels).

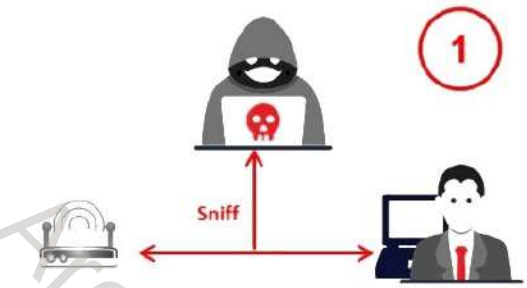


Figure 16.39: Sniffing of the victim's wireless parameters

- The attacker sends a DEAUTH request to the victim with a spoofed source address of the victim's AP.

Figure 16.40: Sending a DEAUTH request

- On receiving the request, the victim's computer is de-authenticated and starts to search all channels for a new valid AP.

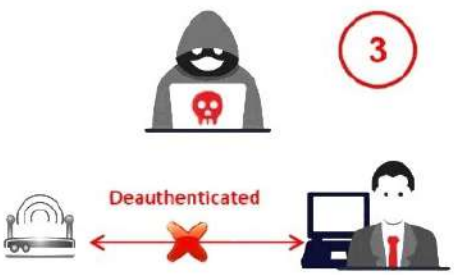


Figure 16.41: De-authentication of the victim's computer

- The attacker sets a forged AP on a new channel with the original MAC address (BSSID) and ESSID of the victim's AP, thereby connecting the victim to the forged AP.

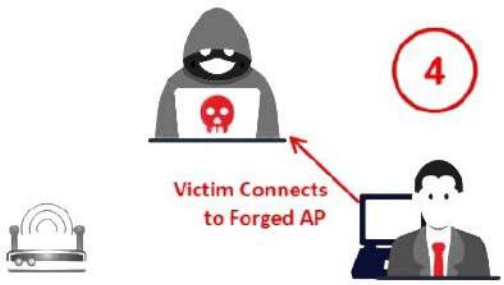


Figure 16.42: Connection of the victim to the forged AP

- After the victim's successful association to the forged AP, the attacker spoofs the victim to connect to the original AP.

Figure 16.43: Spoofing the victim

- The attacker positions themselves between the AP and victim, listening to all the traffic.

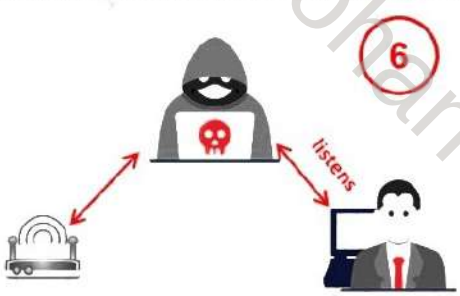
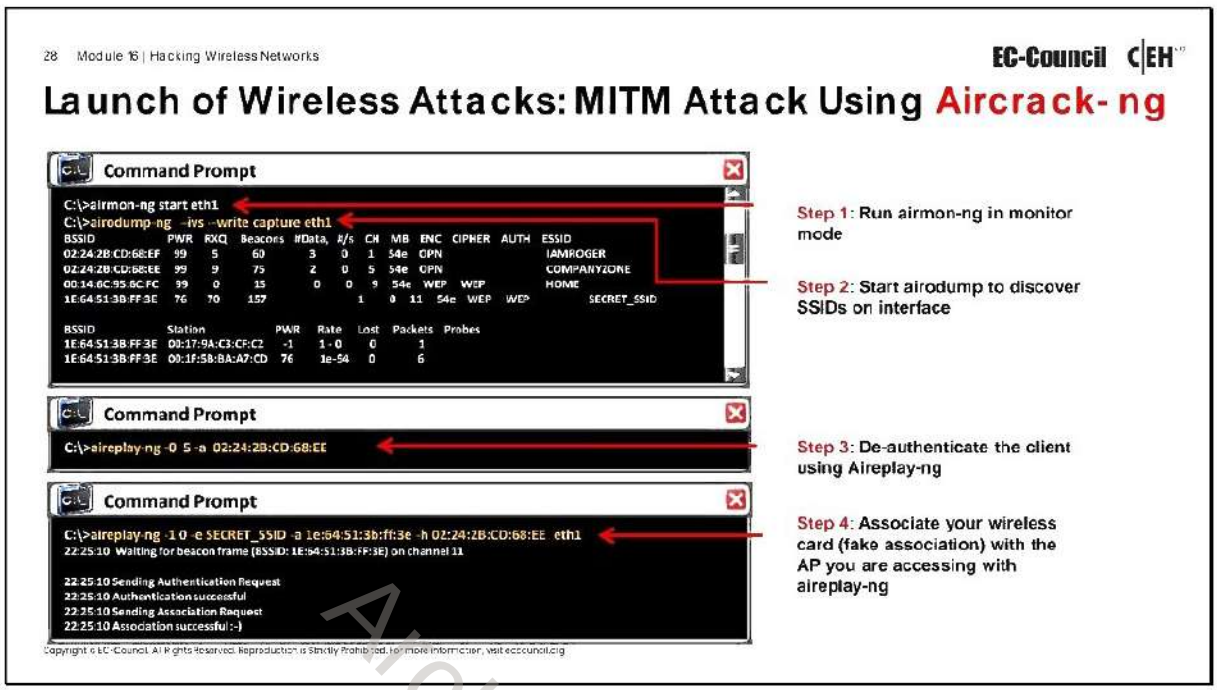


Figure 16.44: Listening to all the traffic



MITM Attack Using Aircrack-ng

An attacker can perform an MITM attack using aircrack-ng through the following steps.

- Run airmon-ng in the monitor mode.
- Start airodump to discover SSIDs on the interface.

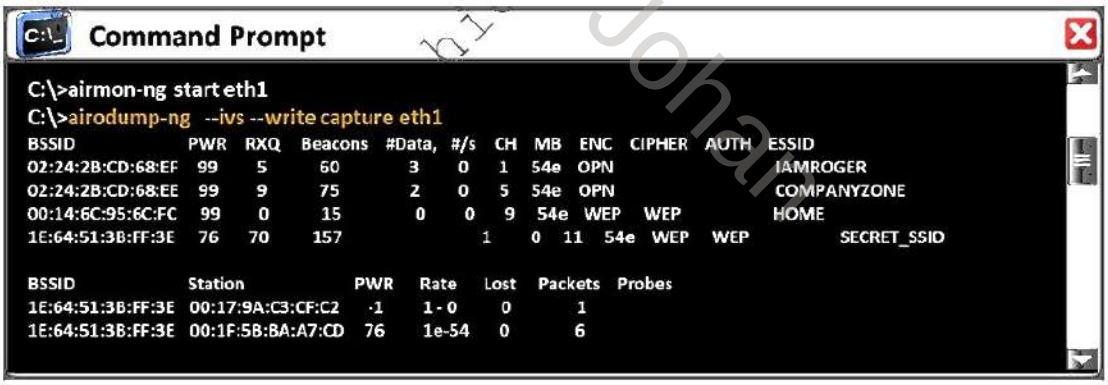


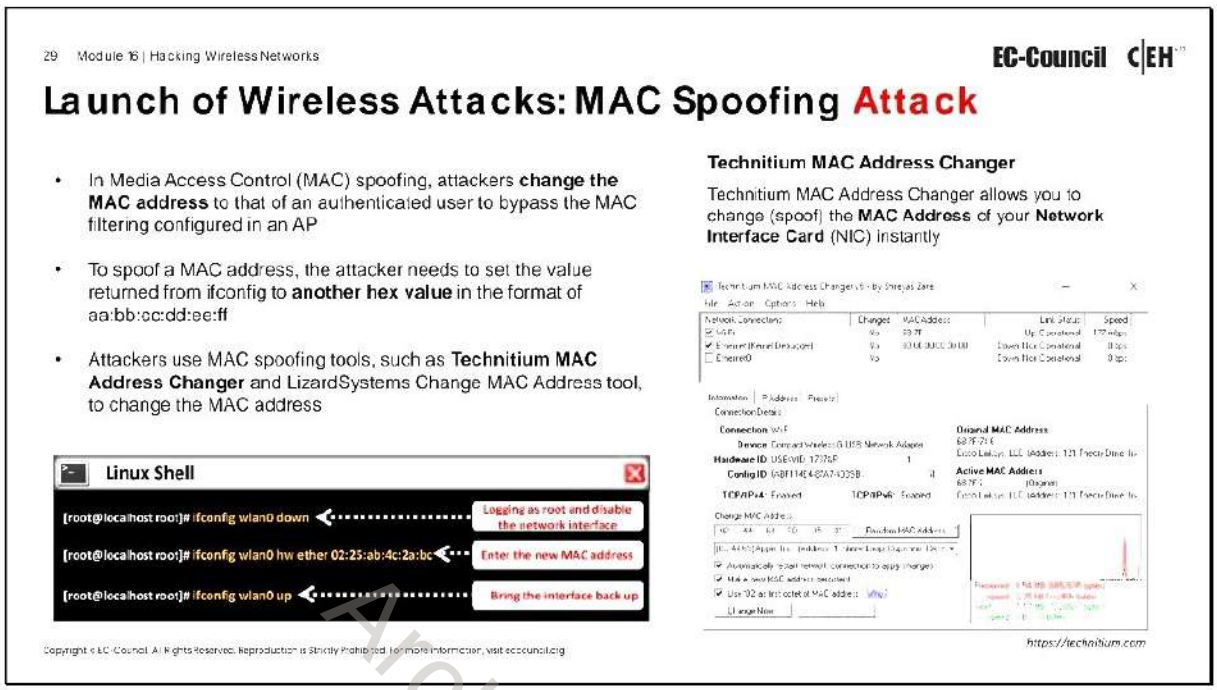
Figure 16.45: Screenshot showing the execution of airmon-ng

- De-authenticate (deauth) the client using aireplay-ng.

Figure 16.46: Screenshot showing the command to launch aireplay-ng

- Associate the wireless card (fake association) with the AP to be accessed with aireplay-ng.

Figure 16.47: Screenshot displaying the result of association



MAC Spoofing Attack

AP MAC Spoofing

In wireless networks, the transmit probes of APs respond through beacons to advertise presence and availability. The probe responses contain information on the AP identity (MAC address) and the identity of the network it supports (SSID). Clients in the vicinity connect to the network through these beacons based on the MAC address and the SSID it contains. Many software tools and APs allow setting user-defined values for the MAC addresses and SSIDs of AP devices.

AP MAC spoofing is a technique used by attackers to impersonate a legitimate wireless access point (AP) by changing the MAC address of the device to match that of the trusted AP. First, the attacker identifies the MAC address of a legitimate AP, typically by monitoring the network traffic or using a tool to scan available wireless networks. The attacker then configures its rogue access point with the same MAC address and, often, the same SSID as the legitimate AP. Attackers may use deauthentication packets to force users off a legitimate AP, prompting their devices to reconnect to the nearest AP with the same MAC address and SSID, often the rogue AP. Once users connect to a rogue AP, attackers can intercept, manipulate, or redirect the network traffic, enabling them to capture sensitive information or launch further attacks.

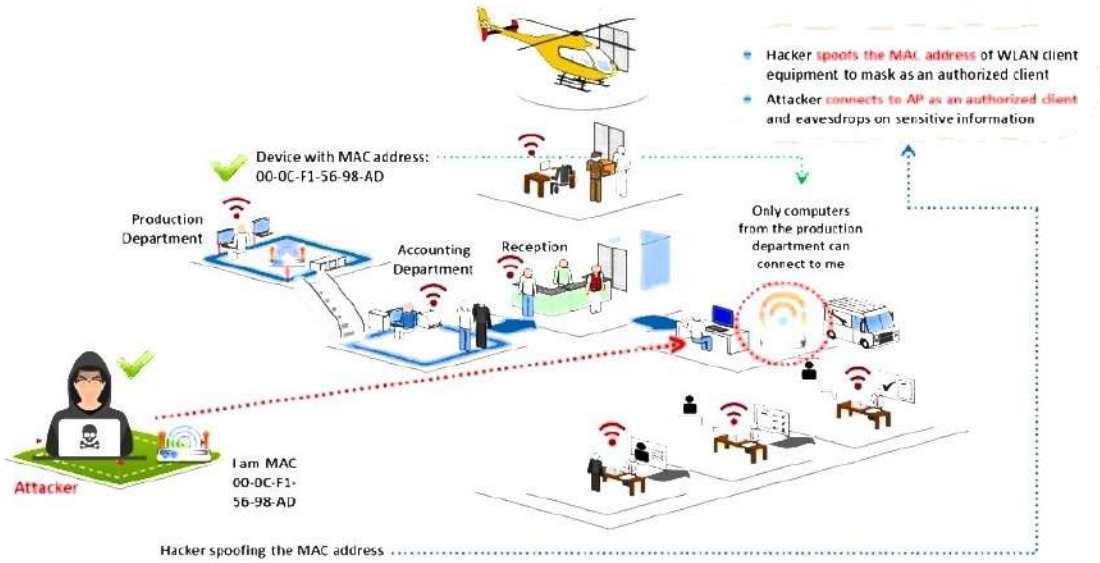


Figure 16.48: AP MAC spoofing

MAC Spoofing Attack

A MAC address is a unique identifier hard-coded in the circuit of a network card by its manufacturer. Some networks implement MAC address filtering as a security measure. In MAC spoofing, attackers change their MAC address to that of an authenticated user to bypass the MAC filtering configured in an AP. To spoof a MAC address, the attacker simply needs to set the value returned by ifconfig to another hex value in the format of aa:bb:cc:dd:ee:ff. This change is made through the sudo command, which requires the root password. Attackers use MAC spoofing tools such as Technitium MAC Address Changer and LizardSystems Change MAC Address tool to change the MAC address.

Figure 16.49: MAC address spoofing in Linux and Windows

MAC Spoofing Tools

- **Technitium MAC Address Changer**

  Source: *https://technitium.com*

  Technitium MAC Address Changer allows a user to change (spoof) the MAC address of their NIC instantly. It has a simple user interface and provides information regarding each NIC in the machine. The MAC address is used by Windows drivers to access Ethernet LANs.

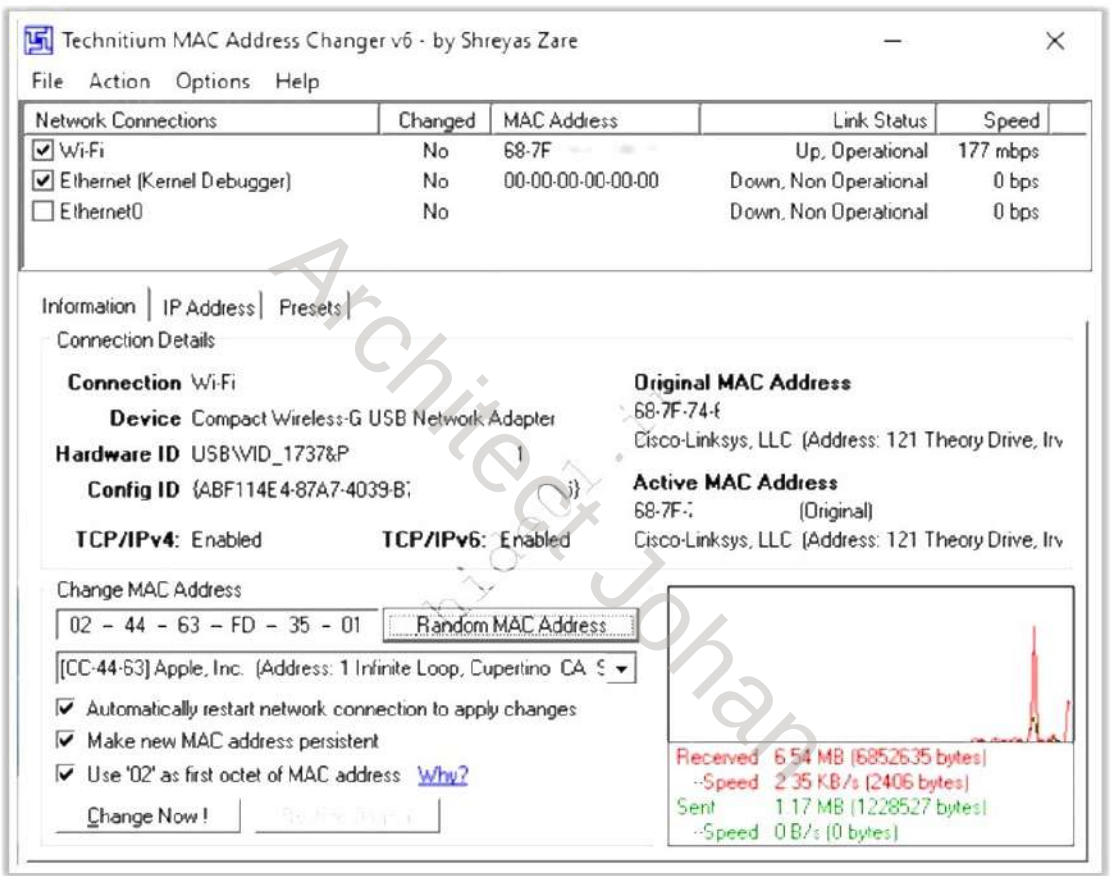
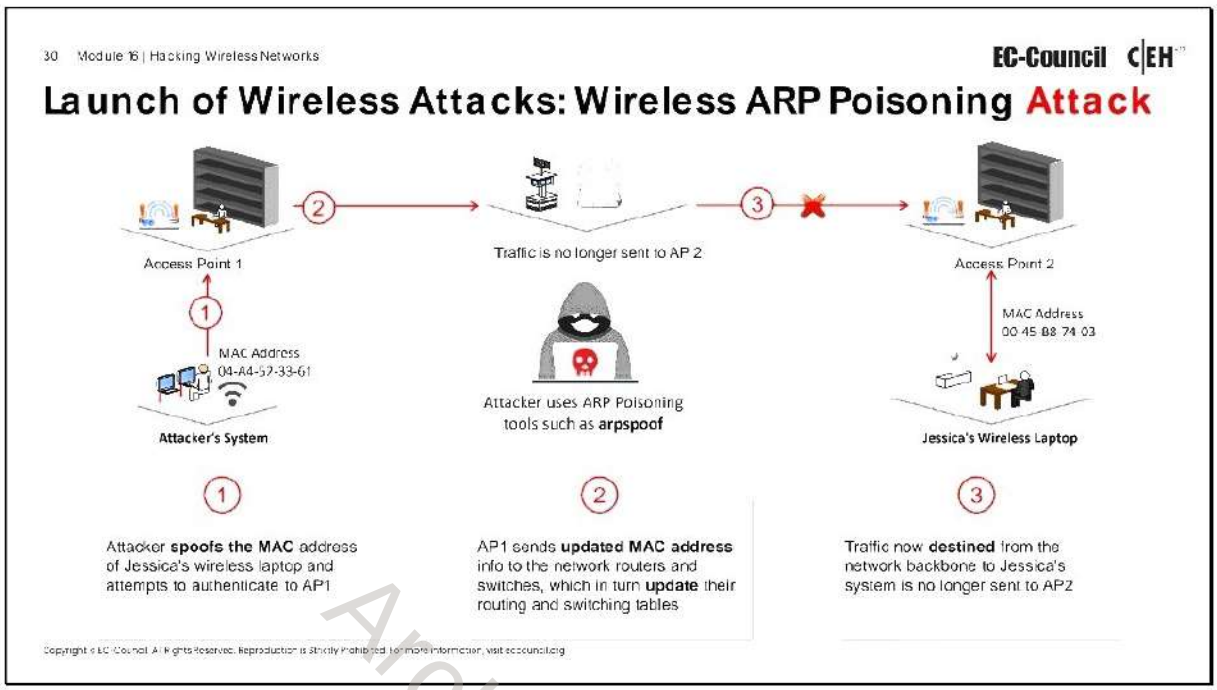


Figure 16.50: Screenshot of Technitium MAC Address Changer



Wireless ARP Poisoning Attack

ARP determines the MAC address of an AP if it already knows its IP address. Usually, ARP does not possess any feature to verify whether the responses are from valid hosts. ARP poisoning is an attack technique that exploits this lack of verification. In this technique, the ARP cache maintained by the OS is corrupted with wrong MAC addresses. An attacker achieves this by sending an ARP replay packet constructed with a wrong MAC address.

An ARP poisoning attack impacts all the hosts in a subnet. All stations associated with a subnet affected by an ARP poisoning attack are vulnerable because most APs act as transparent MAC-layer bridges. All hosts connected to a switch or hub are susceptible to ARP poisoning attacks if the AP is connected directly to that switch or hub without any router/firewall between them. The below figure illustrates the process of an ARP poisoning attack.

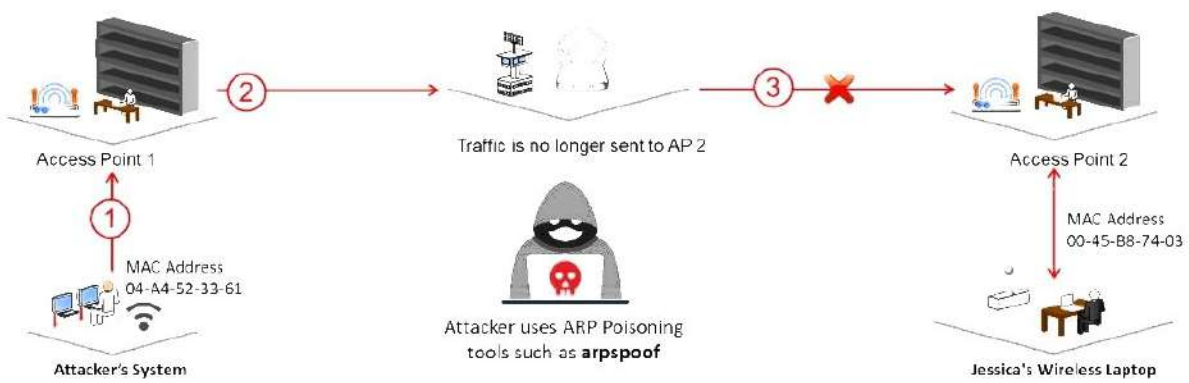
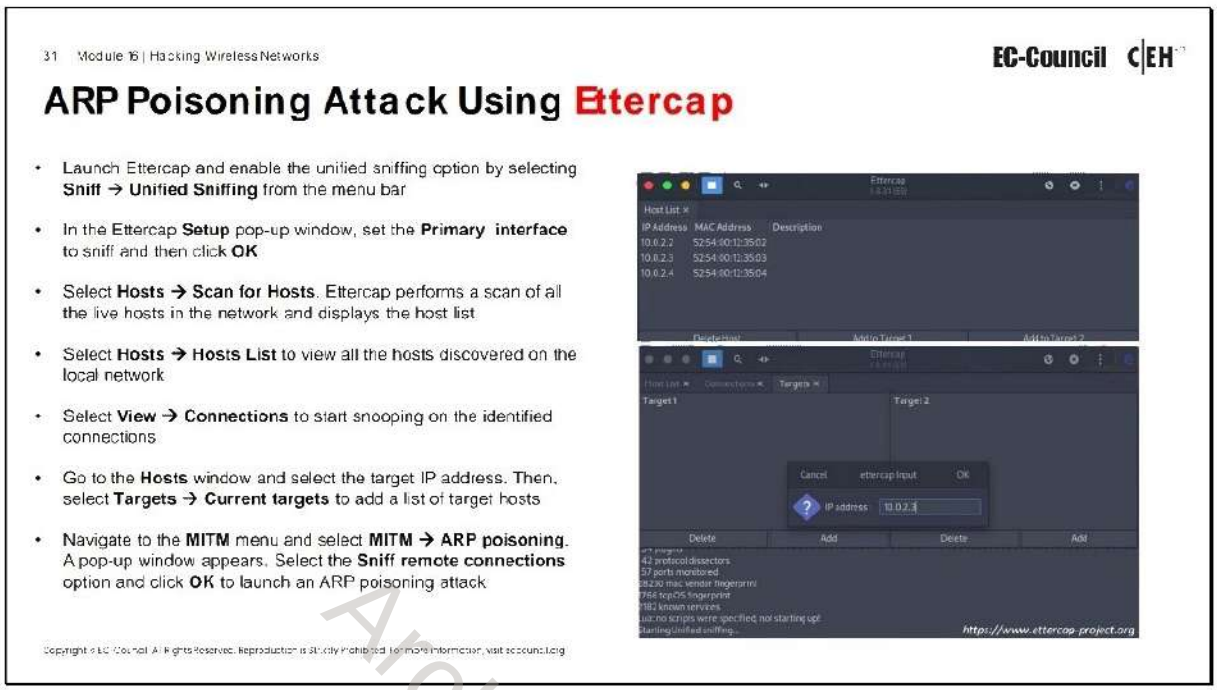


Figure 16.51: ARP poisoning attack

In the wireless ARP spoofing attack shown in the above figure, the attacker first spoofs the MAC address of the victim's system and attempts to authenticate to access point 1 (AP1) using an ARP poisoning tool such as arpspoof. AP1 sends the updated MAC address information to the network routers and switches, which in turn update their routing and switching tables. Consequently, the traffic from the network backbone to the victim's system is sent to AP1, rather than to access point 2 (AP2).



ARP Poisoning Attack Using Ettercap

Source: *https://www.ettercap-project.org*

Attackers use Ettercap to identify the MAC addresses of the clients and routers for performing various attacks such as ARP poisoning, sniffing, and MITM attacks. Using this tool, an attacker can obtain all the information about the network traffic of the victim. An attacker performs an ARP poisoning attack using Ettercap through the following steps.

- Launch the Ettercap graphical interface and enable the unified sniffing option by selecting **Sniff → Unified Sniffing** from the menu bar. This allows the attacker to bridge the connection and sniff the traffic crossing the interfaces.
- In the Ettercap **Setup** pop-up window, set the **Primary interface** to sniff and click on **OK**. This will show advanced menu options such as targets, hosts, MITM, and plugins.

Figure 16.52: Screenshot of the Ettercap interface for setting the network interface to sniff

- Identify the target host in the network by selecting **Hosts → Scan for Hosts**. Ettercap performs a scan of all live hosts in the network and displays a list of hosts. Next, select **Hosts → Hosts List** to view all the hosts discovered on the local network.

Figure 16.53: Screenshot of Ettercap showing the host list

- Select **View → Connections** to start snooping on the identified connections. The connections can be filtered in the **Connections** view based on the IP address, type of connection, and state of connection (open/closed/active/killed).

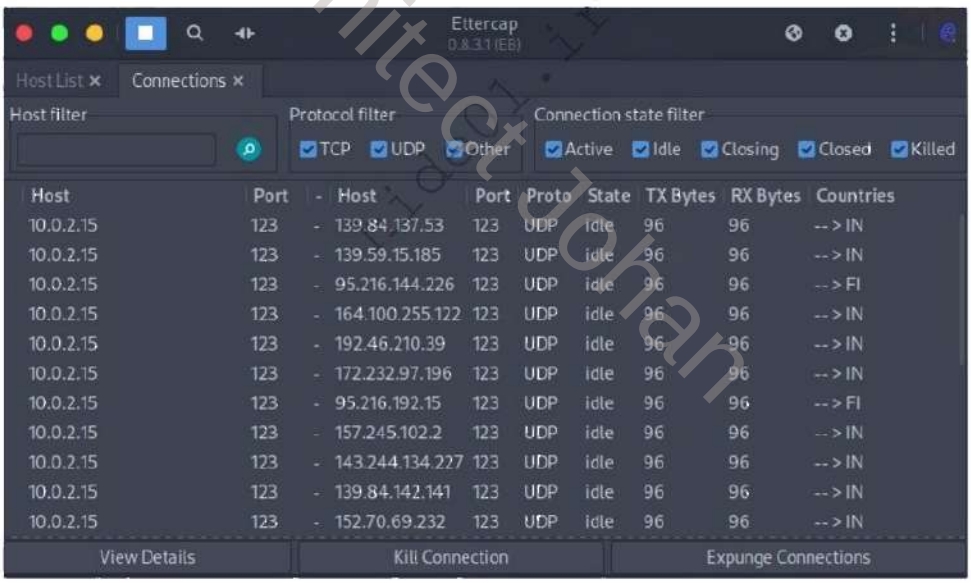


Figure 16.54: Screenshot of Ettercap showing the host list

- Select the hosts to perform an ARP spoofing attack. Go to the **Hosts** window and select the target IP address. Select **Targets → Current targets** to add a list of target hosts to use for ARP spoofing.

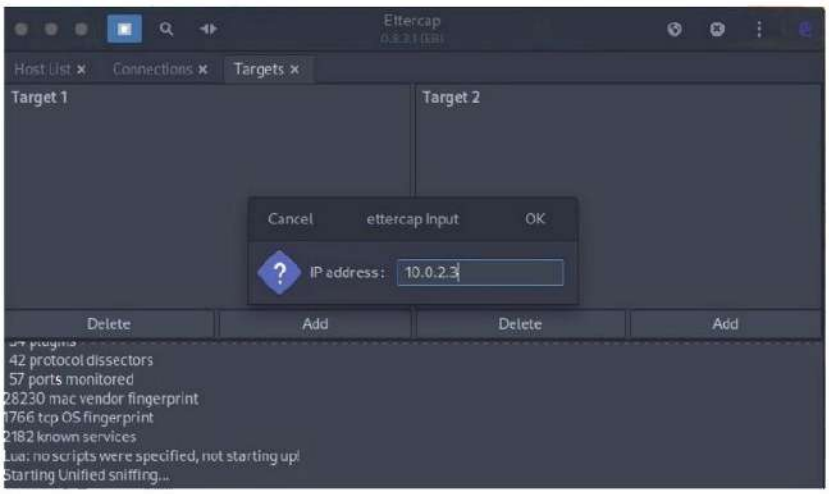


Figure 16.55: Screenshot of Ettercap showing targets

- Select **MITM → ARP poisoning**. In the pop-up window that appears, select **Sniff remote connections** and click on **OK** to launch an ARP poisoning attack on the target.

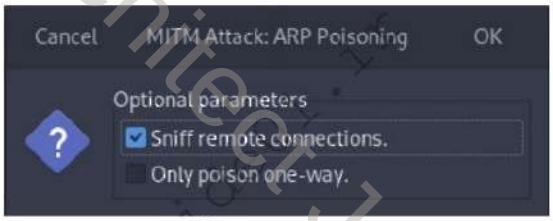


Figure 16.56: Screenshot of optional parameter selection in Ettercap when launching an ARP poisoning attack

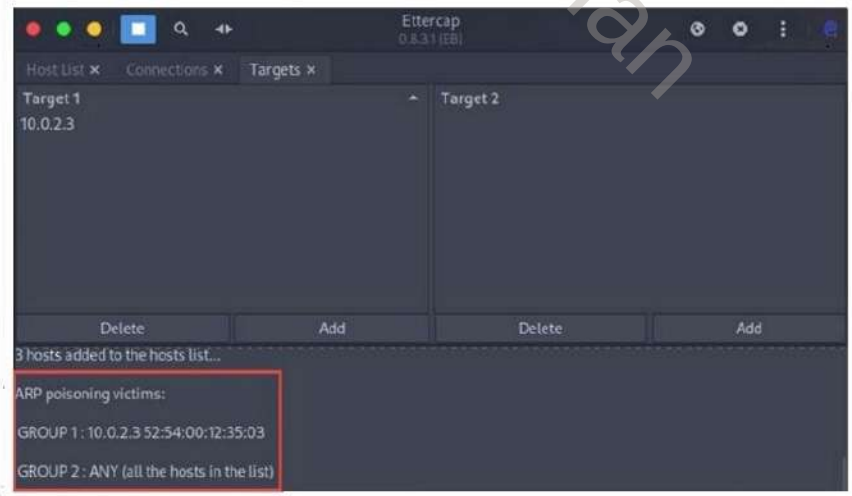
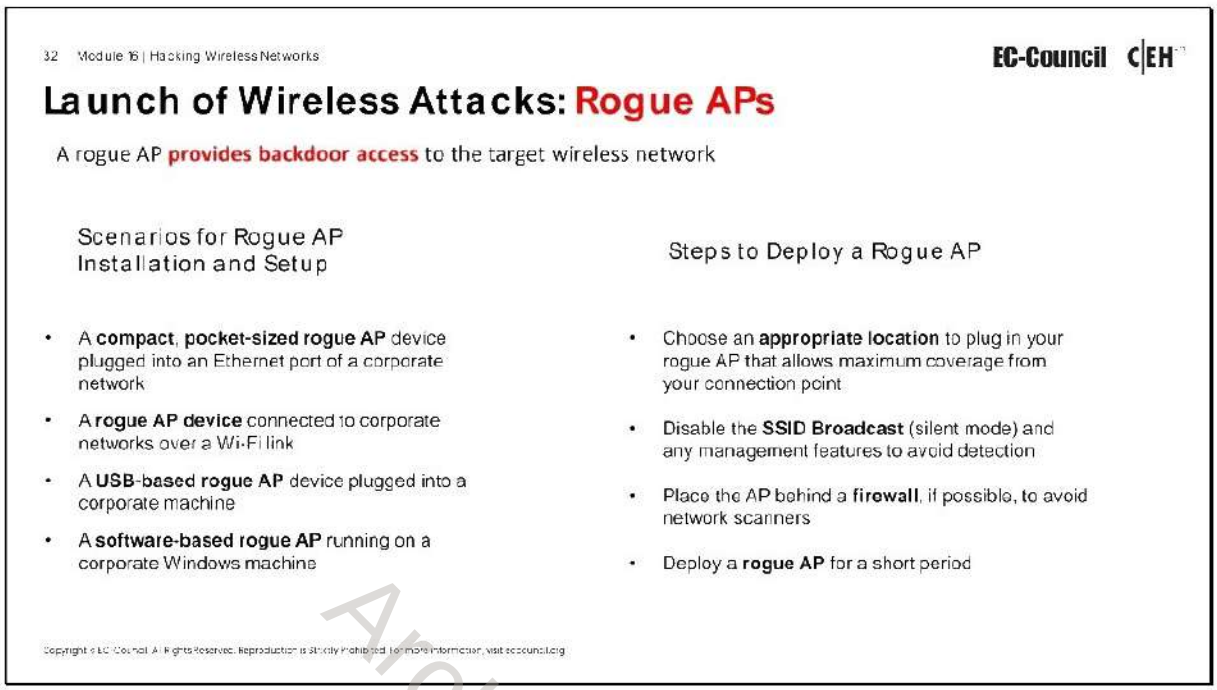


Figure 16.57: Screenshot of Ettercap launching an ARP poisoning attack

Once the attack is launched, the target host's login credentials can also be sniffed if the web traffic is not encrypted with Hypertext Transfer Protocol Secure (HTTPS).



Rogue APs

Rogue AP Attack

APs connect to client NICs by authenticating with the help of SSIDs. Unauthorized (or rogue) APs can allow anyone with an 802.11-equipped device to connect to a corporate network. An unauthorized AP can give an attacker access to the network.

With the help of wireless sniffing tools, the following can be determined from APs: authorized MAC addresses, the vendor name, and security configurations. An attacker can then create a list of MAC addresses of authorized APs on the target LAN and crosscheck this list with the list of MAC addresses found by sniffing. Subsequently, an attacker can create a rogue AP and place it near the target corporate network. Attackers use rogue APs placed in an 802.11 network to hijack the connections of legitimate network users. When a user turns on a computer, the rogue AP will offer to connect with the network user's NIC. The attacker lures the user to connect to the rogue AP by sending the SSID. If the user connects to the rogue AP under the impression that it is a legitimate AP, all the traffic from the user passes through the rogue AP, enabling a form of wireless packet sniffing. The sniffed packets may even contain usernames and passwords.

Figure 16.58: Rogue AP attack

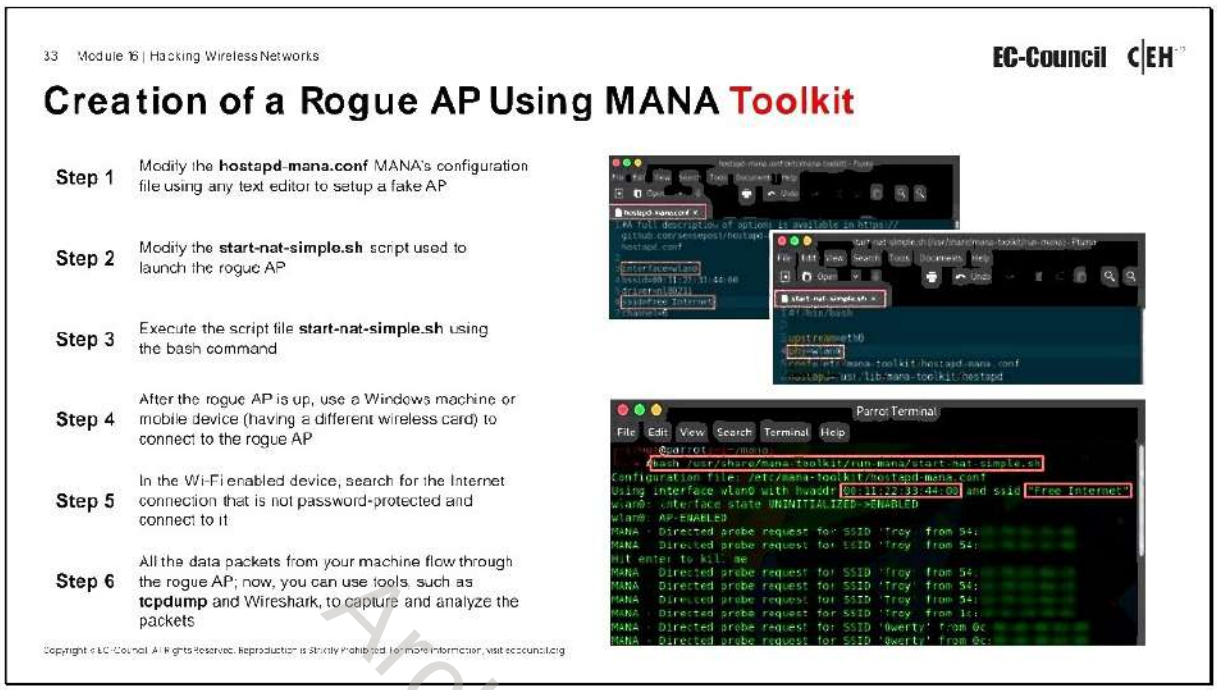
Rogue APs are wireless APs that an attacker installs on a network without authorization and are not under the management of the network administrator. These rogue APs are not configured for security, unlike the authorized APs on the target wireless network. Thus, this rogue AP can provide backdoor access to the target wireless network.

Interesting scenarios for rogue AP installation and setup include the following.

- **Compact, pocket-sized rogue AP plugged into an Ethernet port of the target network**: An attacker can use compact, pocket-sized rogue APs because they are easily available, can be stealthily brought onsite, and consume very little power.
- **Rogue AP connected to corporate networks over a Wi-Fi link**: An attacker connects a rogue AP to a Wi-Fi link of the target network. Because the rogue AP connects wirelessly to the authorized network, it is easily hidden. However, it requires the credentials of the target network to connect.
- **USB-based rogue AP plugged into a network machine**: An attacker can easily plug a USB-based rogue AP into any Windows machine on the target network that is connected through wired or wireless means. The USB AP's software shares the network access of the machine with the rogue AP. This eliminates the need for both an unused Ethernet port and the credentials of the target Wi-Fi, which are required in the above two scenarios to set up a rogue AP.
- **Software-based rogue AP running on a network Windows machine**: An attacker can set up a software-based rogue AP on the embedded/plugged Wi-Fi adapter of the target network, instead of a separate hardware device.

A rogue AP is deployed through the following steps.

- Choose an appropriate location to plug in the rogue AP for maximum coverage from the connection point
- Disable SSID broadcast (silent mode) and any management features to avoid detection.
- Place the AP behind a firewall, if possible, to avoid network scanners.
- Deploy the rogue AP for a short period.



Creation of a Rogue AP Using MANA Toolkit

MANA Toolkit comprises a set of tools that are used by the attackers for creating rogue APs and perform sniffing attacks and MITM attack. It is also used for bypassing HTTPS and HTTP Strict Transport Security (HSTS). Attackers use MANA Toolkit to create a rogue AP through the following steps.

- Modify MANA's configuration file **hostapd-mana.conf** using any text editor to set up a fake access point. Set the wireless interface (**wlan0** is used here) as well as the MAC address (BSSID) or SSID (the SSID **Free Internet** is used here).

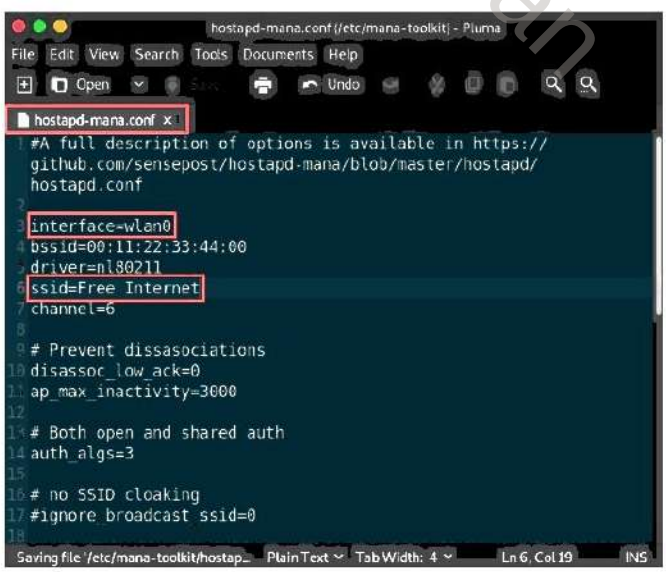


Figure 16.59: Screenshot showing hostapd-mana.conf

- Modify the script file **start-nat-simple.sh** used to launch the rogue AP. Set the wireless card parameter **phy** (**wlan0** is used here) and the **upstream** parameter (**eth0** is used here) that specifies the card as having an Internet connection.

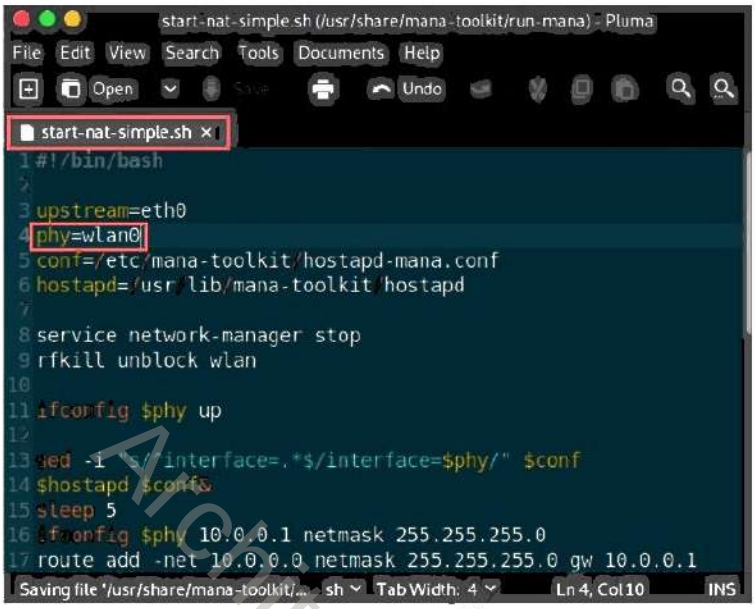


Figure 16.60: Screenshot showing start-nat-simple.sh

- Execute the script file **start-nat-simple.sh** using the bash command **# bash <Path to MANA>/mana-toolkit/run-mana/start-nat-simple.sh.** By executing this command, the rogue AP starts running.

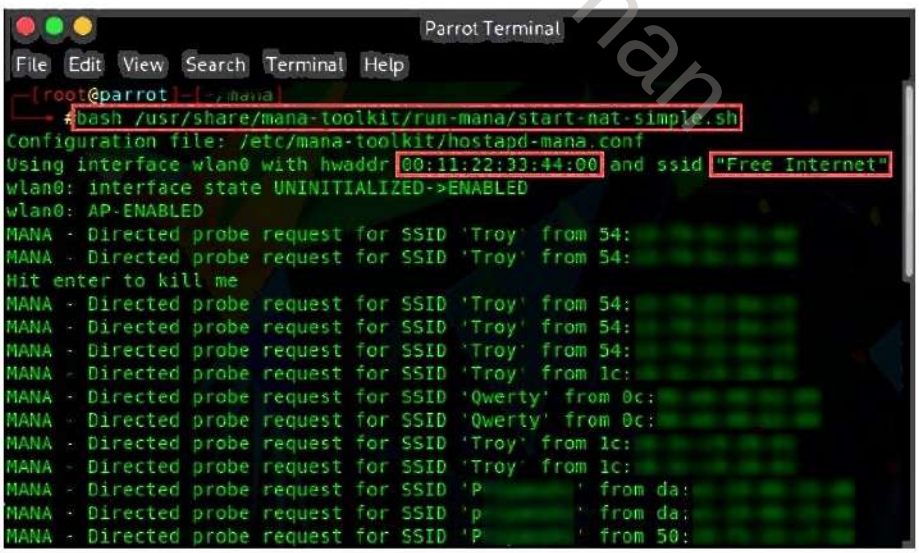
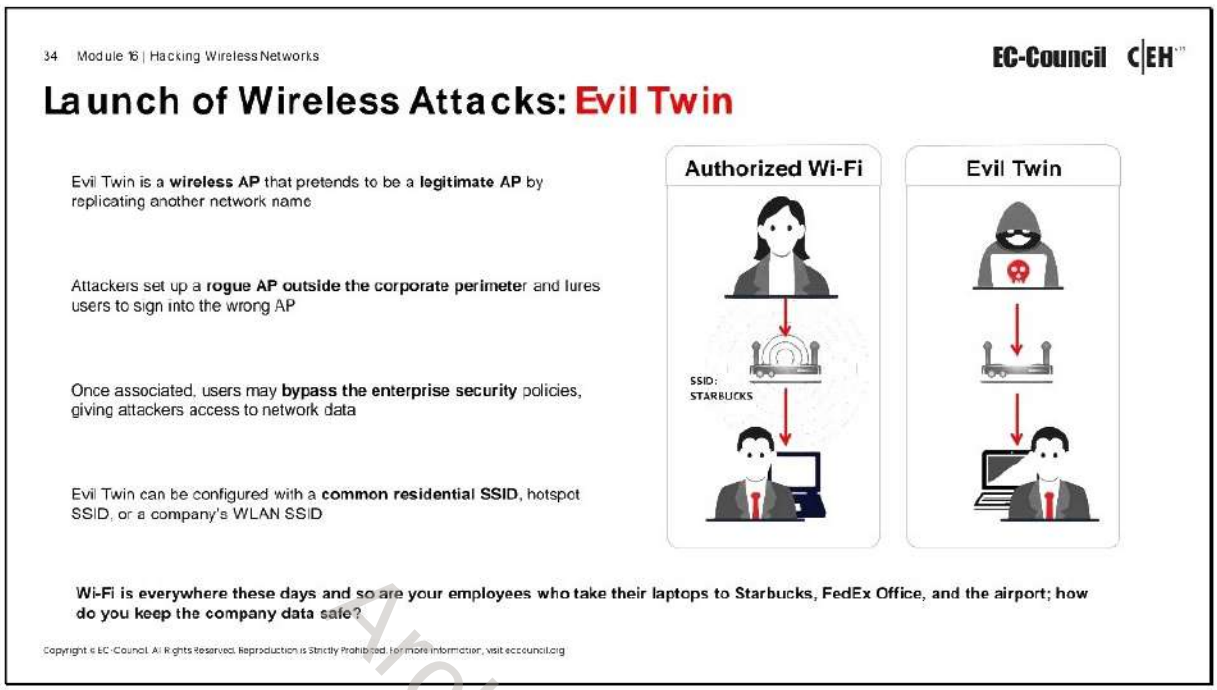


Figure 16.61: Screenshot displaying the output of start-nat-simple.sh

- Once the rogue AP is operational, use a Windows machine or mobile device having a different wireless card to connect to the rogue AP.
- In the Wi-Fi-enabled device, search for the Internet connection that is not password protected (**Free Internet** is used here) and connect to it.

Figure 16.62: Screenshot displaying available networks in the mobile device

- Once connected to the Internet through the rogue AP, all the data packets from the device flows through the rogue AP. Now, tools such as tcpdump and Wireshark can be used to capture and analyze the packets.



Evil Twin

An evil twin is a wireless AP that pretends to be a legitimate AP by imitating its SSID. It poses a clear and present danger to wireless users on private and public WLANs. An attacker sets up a rogue AP outside the network perimeter and lures users to sign in to this AP. The attacker uses tools such as KARMA, which monitors station probes to create an evil twin. The KARMA tool passively listens to wireless probe request frames and can adopt any commonly used SSID as its own SSID to lure users. The attacker can configure an evil twin with a common residential SSID, hotspot SSID, or the SSID of an organization's WLAN. An attacker who can monitor legitimate users can target APs that do not send SSIDs in probe requests.

WLAN stations usually connect to specific APs based on their SSIDs and signal strength, and the stations automatically reconnect to any SSID used in the past. These issues allow attackers to trick legitimate users by placing an evil twin near the target network. Once associated, the attacker may bypass enterprise security policies and gain access to network data.

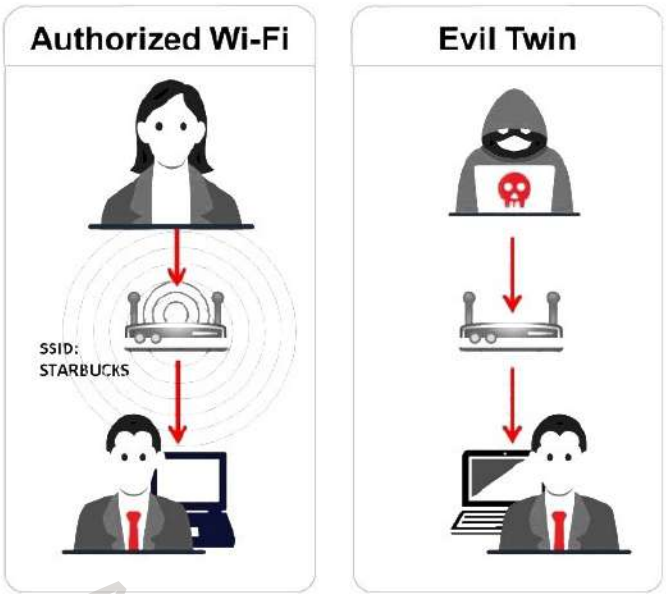


Figure 16.63: Evil twin

Because the employees of a company may take their corporate laptops to establishments with public Wi-Fi networks, it is challenging to keep company data safe.

Set Up of a Fake Hotspot (Evil Twin)

Hotspots in an area may not always be legitimate because an evil twin mounted by an attacker may pretend to be a legitimate hotspot. It is difficult to differentiate between a legitimate hotspot and an evil twin. For example, a user who attempts to log in may find two APs, one of which is legitimate. If the user connects to the network through the evil twin, the attacker may obtain login information and access to the victim's computer. Any login attempt of the user would fail, and they are likely to assume that the attempt randomly failed. A fake hotspot can be set up using a laptop with Internet connectivity (3G or a wired connection) and a mini AP through the following steps.

1. Enable **Internet Connection Sharing** in Windows or **Internet Sharing** in macOS.

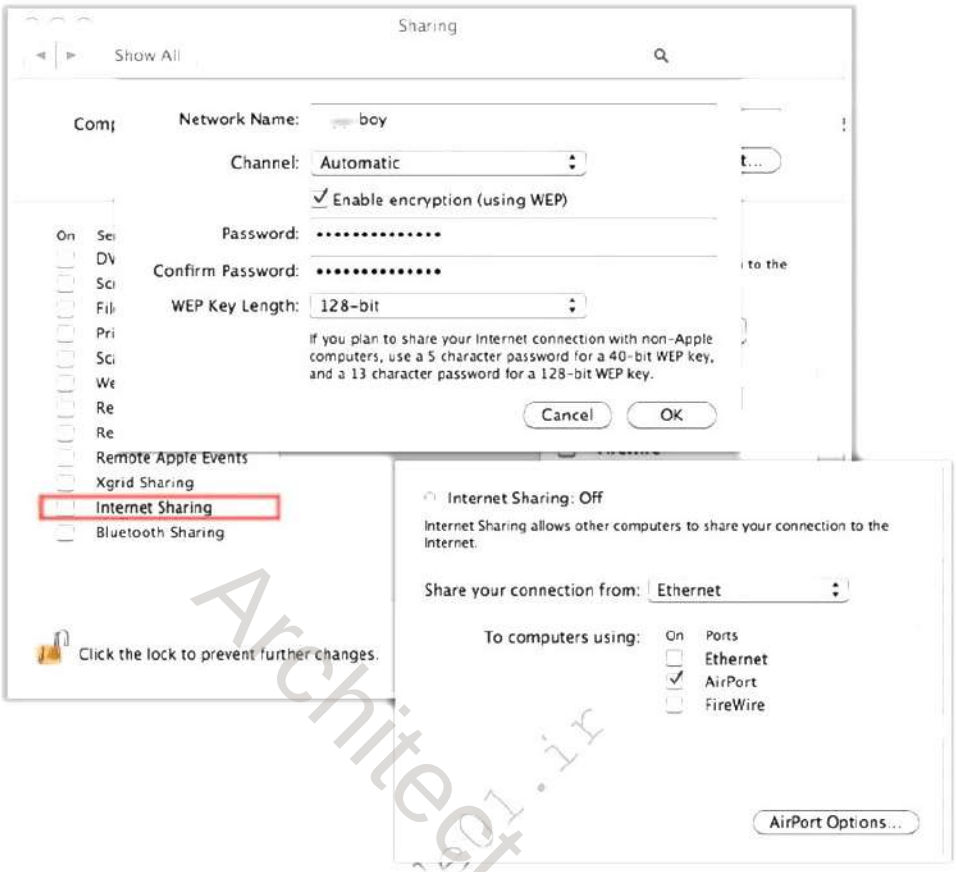
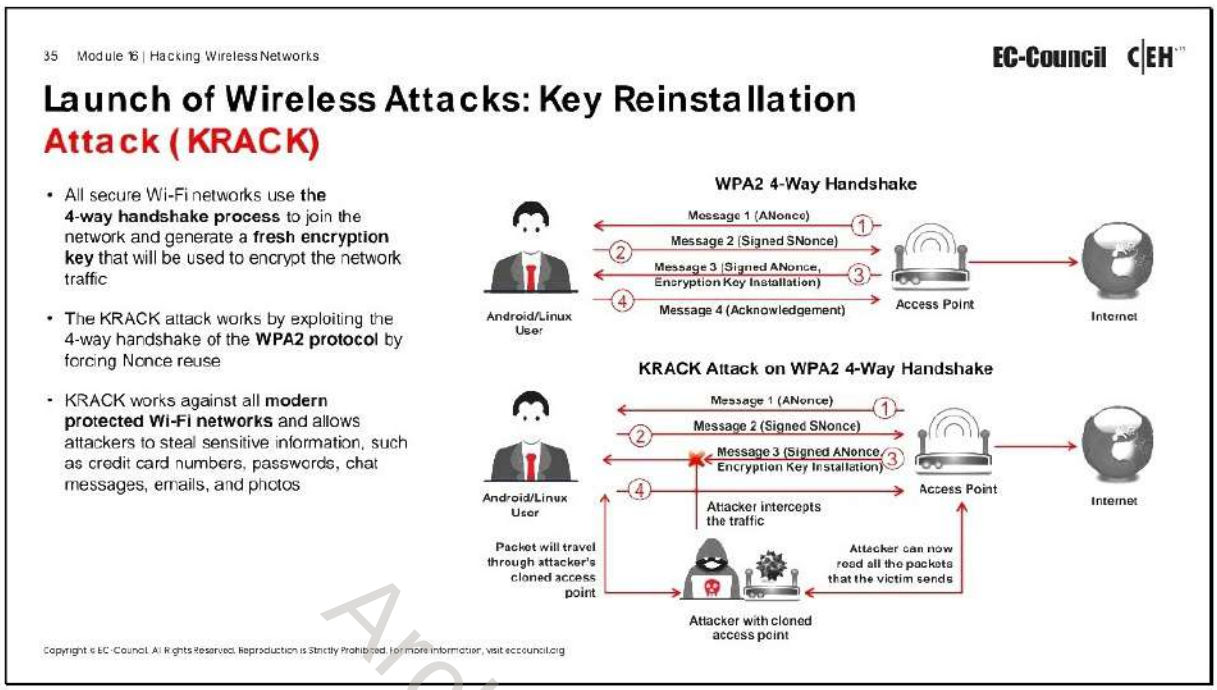


Figure 16.64: Screenshot of the Internet Sharing window in macOS

2. Broadcast the Wi-Fi connection and run a sniffer program to capture passwords.

Figure 16.65: Set up of a fake hotspot



Key Reinstallation Attack (KRACK)

The key reinstallation attack (KRACK) exploits the flaws in the implementation of the four-way handshake process in the WPA2 authentication protocol, which is used to establish a connection between a device and an AP. All secure Wi-Fi networks use the four-way handshake process to establish connections and to generate a fresh encryption key that will be used to encrypt the network traffic.

Figure 16.66: Four-way handshake process in WPA2

The attacker exploits the four-way handshake of the WPA2 protocol by forcing Nonce reuse. In this attack, the attacker captures the victim's ANonce key that is already in use to manipulate and replay cryptographic handshake messages. This attack works against all modern protected Wi-Fi networks (both WPA and WPA2); personal and enterprise networks; and the ciphers WPA-TKIP, AES-CCMP, and GCMP. It allows the attacker to steal sensitive information such as credit-card numbers, passwords, chat messages, emails, and photos. Any device that runs Android, Linux, Windows, Apple, OpenBSD, or MediaTek are vulnerable to some variant of the KRACK attack.

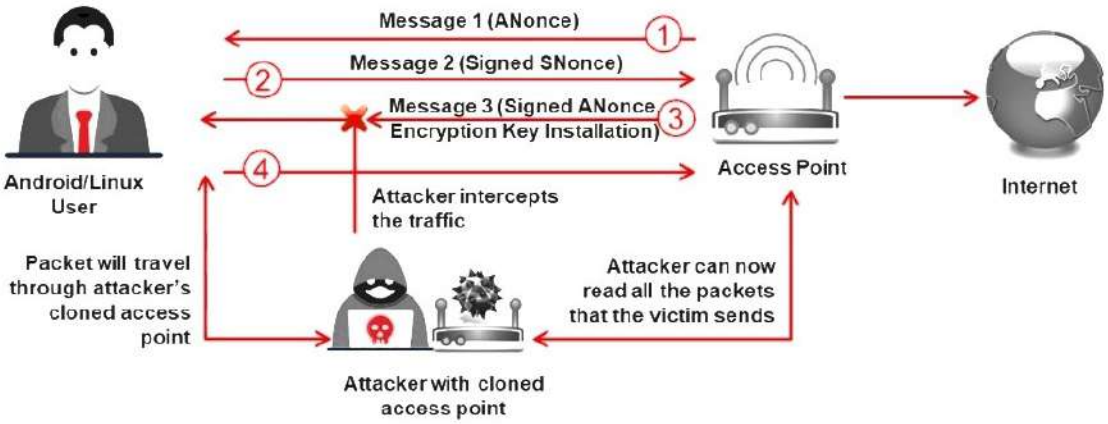
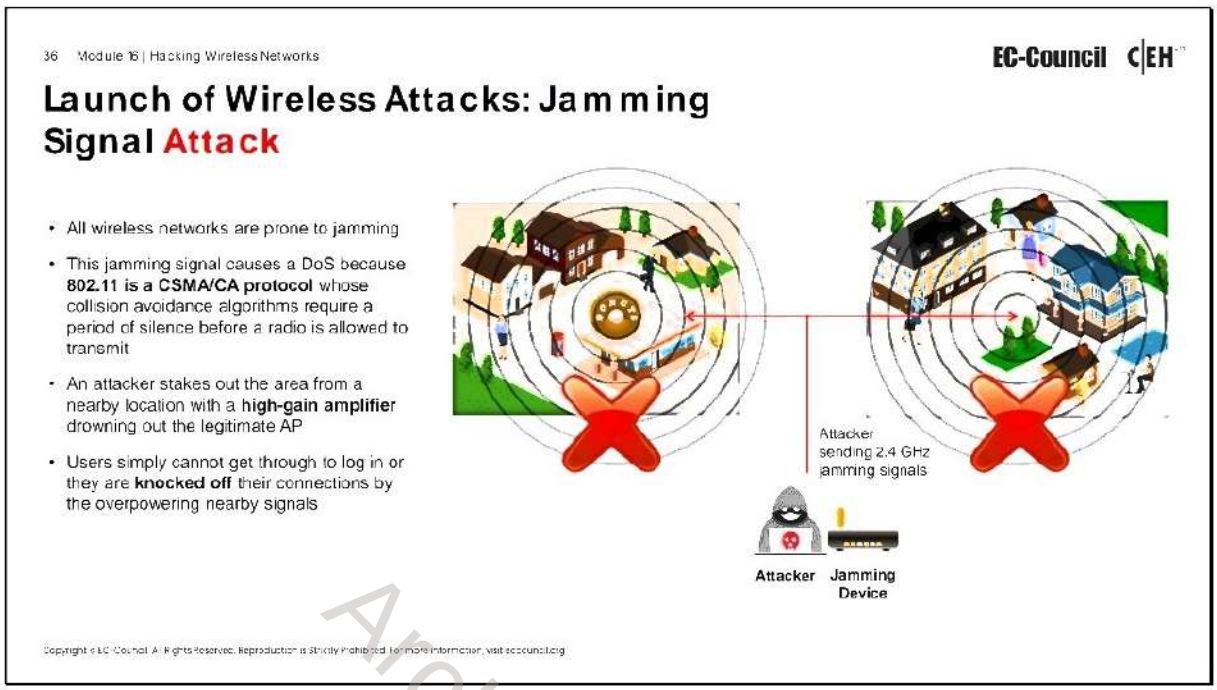


Figure 16.67: KRACK attack exploiting the four-way handshake process in WPA2



Jamming Signal Attack

Jamming is an attack performed on a wireless network to compromise it. In this type of exploitation, overwhelming volumes of malicious traffic result in a DoS to authorized users, obstructing legitimate traffic. All wireless networks are prone to jamming, and spectrum jamming attacks usually block all communications completely.

An attacker uses specialized hardware to perform this kind of attack. The signals generated by jamming devices appear to be noise to the devices on the wireless network, which causes them to hold their transmissions until the signal has subsided, resulting in a DoS. Furthermore, jamming signal attacks are not easily noticeable. The procedure of a jamming signal attack is summarized as follows.

- An attacker stakes out the target area from a nearby location with a high-gain amplifier that drowns out a legitimate AP.
- Users are unable get through to log in or are disconnected by the overpowering nearby signal.
- The jamming signal causes a DoS because 802.11 is a CSMA/CA protocol, the collision-avoidance algorithms of which require a period of silence before a radio is allowed to transmit.

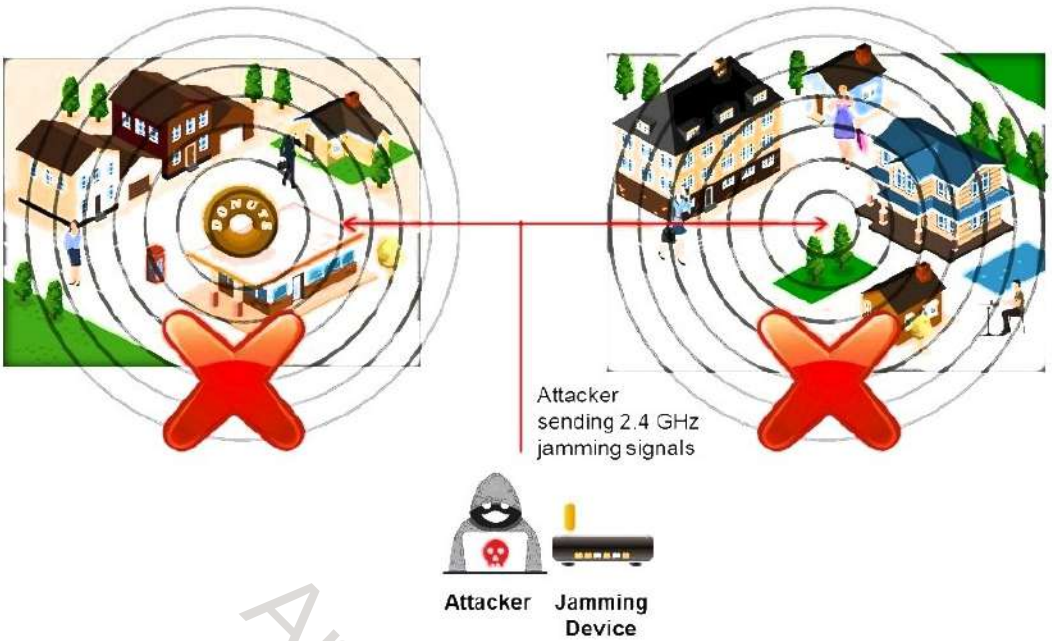
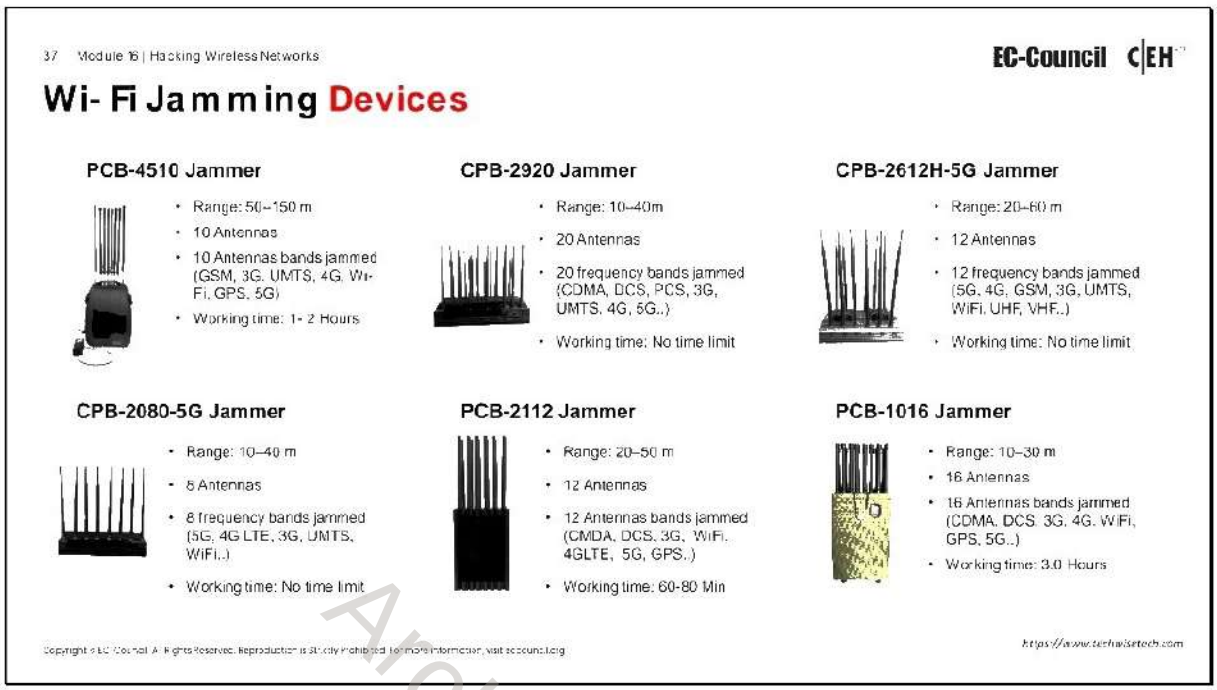


Figure 16.68: Jamming signal attack



Wi-Fi Jamming Devices

An attacker can jam a wireless network by using a Wi-Fi jammer. This device uses the same frequency band as the trusted network. This causes interference with legitimate signals and temporarily disrupts network services.

The following are examples of Wi-Fi jamming devices:

Source: *https://www.techwisetech.com*

- **PCB-4510 Jammer**
  - Range: 50–150 m
  - 10 antennas
  - 10 frequency bands jammed (GSM, 3G, UMTS, 4G LTE, Wi-Fi 11.b&g, GPS, 5G, Wi-Fi 11.a)
  - Working time: 1-2 hours

Figure 16.69: PCB-4510 jammer

- **CPB-2920 Jammer**
  - Range: 10–40m
  - 20 antennas
  - 20 frequency bands jammed (CDMA, DCS, PCS, 3G, UMTS, 4G, WiFi 11.b & g, 4G WiMAX Sprint, 5G, GPS, Lojack, VHF, Car Remote, UHF)
  - Working time: No time limit

Figure 16.70: CPB-2920 jammer

- **CPB-2612H-5G Jammer**
  - Range: 20–60 m
  - 12 antennas
  - 12 frequency bands jammed (5G, 4G, GSM, DCS, 3G, UMTS, WiFi 11.b & g, Lojack Car Tracking, UHF, VHF)
  - Working time: No time limit

Figure 16.71: CPB-2612H-5G jammer

- **CPB-2080-5G Jammer**
  - Range: 10–40 m
  - 8 antennas
  - 8 frequency bands jammed (5G, 4G, GSM900, DCS, 3G, UMTS, WiFi 11.b & g)
  - Working time: No time limit

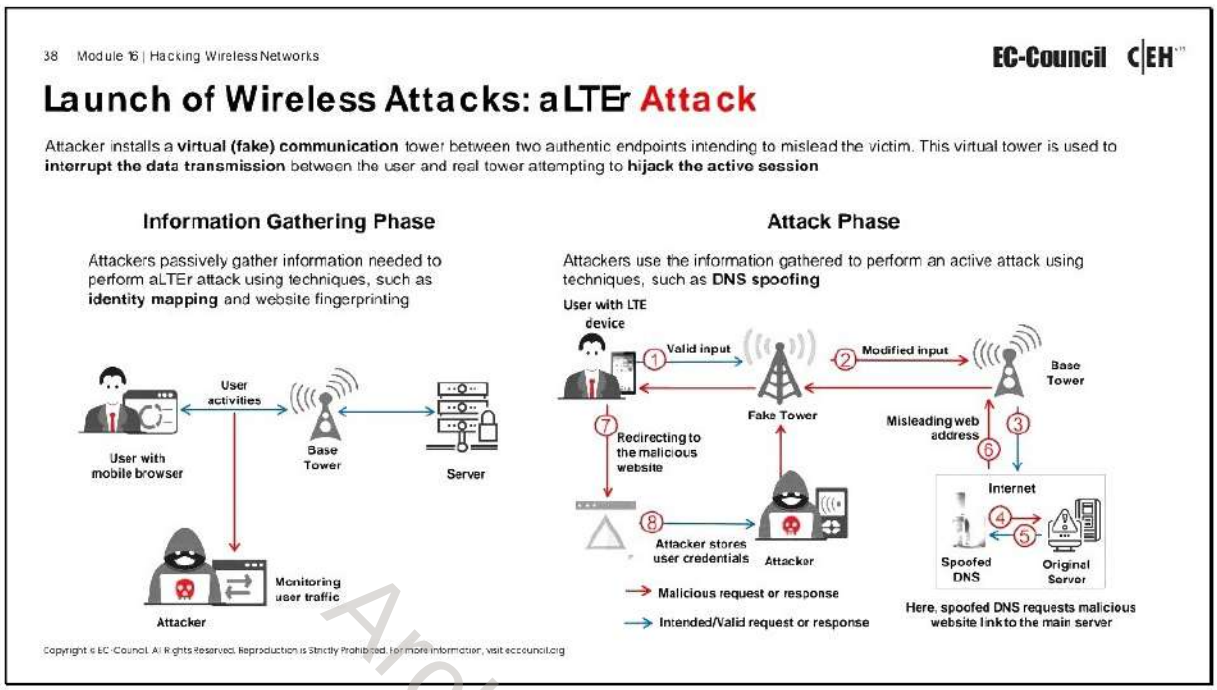
Figure 16.72: CPB-2080-5G jammer

- **PCB-2112 Jammer**
  - Range: 20–50 m
  - 12 antennas
  - 12 frequency bands jammed (CMDA, DCS, 3G, WiFi 11a, 4G, 5G, GPS VHF, UHF)
  - Working time: 60-80 minutes

Figure 16.73: PCB-2112 jammer

- **PCB-1016 Jammer**
  - Range: 10–30 m
  - 16 antennas
  - 16 frequency bands jammed (CDMA, DCS, PCS, 3G, UMTS, 4G, 5G, WiFi, 11.b & g, 4G WiMAX Sprint, GPS, UHF Remote Control, 5G LTE)
  - Working time: 3.0 hours

Figure 16.74: PCB-1016 jammer



aLTEr Attack

Long-Term Evolution (LTE), or 4G, is wireless broadband communication standard developed as a successor to 3G to improve the speed and security of wireless mobile networks. It features bandwidth scalability and supports preceding technologies, such as the Global System for Mobile Communications (GSM; 2G) and Universal Mobile Telecommunications System (UMTS; 3G). Although the technology is designed to overcome all the shortcomings of wireless networks, it is susceptible to data hijacking attacks.

The aLTEr attack is usually performed on LTE devices that encrypt user data in the AES counter (AES-CTR) mode, which provides no integrity protection. To perform this attack, the attacker installs a virtual (fake) communication tower between two authentic endpoints to mislead the victim. The attacker uses this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, the attacker manipulates the traffic with the virtual tower and redirects the victim to malicious websites.

This attack is carried out on "Layer 2," known as the datalink layer, which is responsible for sharing information through wireless networks with standard data encryption technologies. It also enables multiple users to access the network resources and defines how to transfer data between two nodes without any obstacles. By leveraging vulnerabilities or design flaws within this layer, the attacker attempts to take control over browsing data and modifies user inputs with a spoofed DNS server, redirecting the user to unintended or harmful websites. The steps involved in an aLTEr attack are summarized as follows.

- The attacker installs a malicious tower masquerading as a real tower.

- The attacker determines the user's position and sends a packet that appears as a valid request to the real tower.
- The real tower responds with the requested web link.
- The attacker connects the user to unwanted or harmful websites.

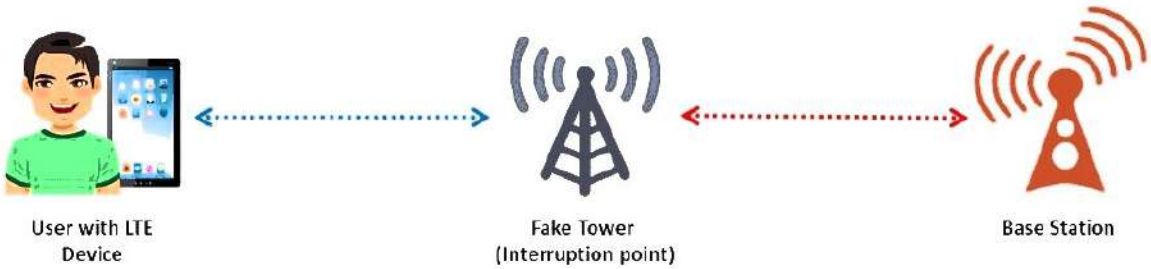


Figure 16.75: aLTEr attack

An aLTEr attack has the following two phases.

- **Information gathering phase**: Attackers passively gather information needed to perform an aLTEr attack using techniques such as identity mapping and website fingerprinting.
- **Attack phase**: Attackers use the information gathered to perform an active attack using techniques such as DNS spoofing.

Information Gathering Phase

Attackers snoop on the websites that users attempt to access and record how often they visit those websites. Attackers only spy or monitor the transmission between the base station and the end user, and they do not modify any credentials or information in this attack.

Attackers use the following techniques to gather information passively.

- **Identity mapping**: The attacker initially maps the identity to locate the target device. Once the target is determined, the attacker devises a strategy to implement the next two attacks.
- **Website fingerprinting**: The attacker records the amount of traffic the client is accessing and keeps track of the user's online activities and other meta information.

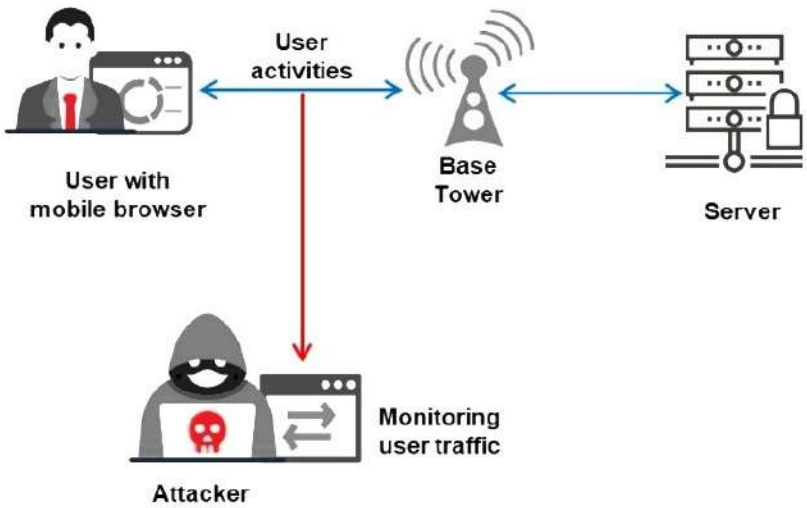


Figure 16.76: Information-gathering phase of an aLTEr attack

Attack Phase

After snooping on or gathering information about the target users, the attacker launches an MITM attack using a fake tower impeding and manipulating the user data, which are intended to be shared with the real tower. The attacker uses DNS spoofing to redirect the victim to a malicious website or a website of their choice, where the attacker records all the sensitive information entered by the victim such as usernames and passwords.

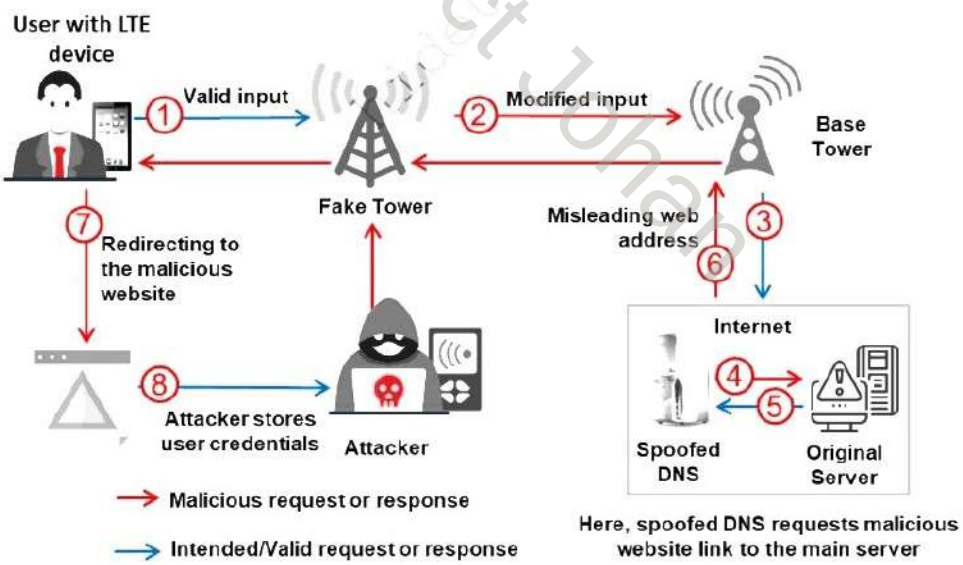


Figure 16.77: Attack phase of an aLTEr attack

39 Module 16 | Hacking Wireless Networks

EC-Council CEH

Launch of Wireless Attacks: Wi- Jacking Attack

Step 1 Send **deauth requests** to the victim's device using aireplay-ng to disconnect the victim from his/her legitimate Wi-Fi network

Step 2 Now, perform Karma attack using **hostapd-wpe**, thus luring the victim to connect to the malicious Wi-Fi network

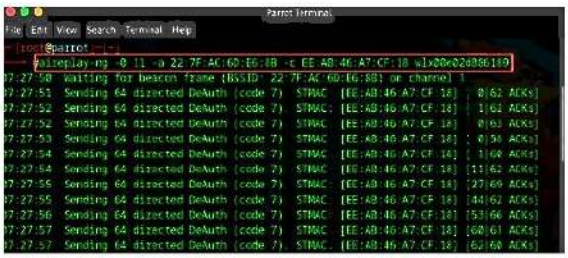
Step 3 Use tools, such as **dnsmasq** and python scripts, to inject malicious URL and lure the victim's browser to load the malicious URL

Step 4 Now, **wait for the victim to access the HTTP page**, and at this moment, the victim's router is updated and restarts automatically

Step 5 Once the victim opens the malicious page, the **browser will automatically load the page**, which has stored credentials

Step 6 Now, stop the Karma attack, and **allow the victim to connect back to his/her legitimate network**; the malicious page remains in the router's admin interface origin along with admin credentials loaded into the JavaScript

Step 7 Use **XMLHttpRequest** to login to the router to extract the victim's WPA2 PSK and further perform any other required malicious changes



Wi-Jacking Attack

Attackers use a Wi-Jacking attack for gaining access to an enormous number of wireless networks. In this attack, the Wi-Fi information of the nearest victims can be retrieved without using any cracking mechanisms. This attack can be used when credentials are saved in the victim's browser, when the victim accesses the same website multiple times, and when the router uses an unencrypted HTTP connection to access the router configuration interface in the browser. Attackers can take advantage of these vulnerabilities to crack WPA/WPA2 networks without going through a single handshake process. The following conditions must be met to perform a Wi-Jacking attack.

- At least one active client device must be connected to the target network.
- The client device must have already connected to any open network and allow automatic reconnection to that network.
- The client device must use a chromium-based web browser.
- The client device's browser must store the admin interface credentials of the router.
- The target network's router must use an unencrypted HTTP connection for the router configuration interface.

Attackers launch a Wi-Jacking attack through the following steps.

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

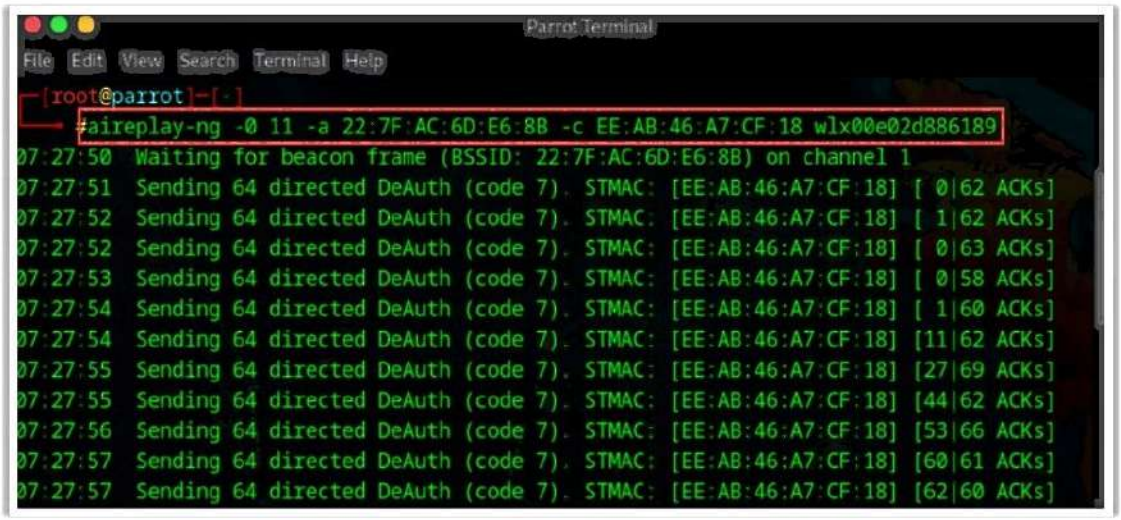


Figure 16.78: Screenshot displaying de-authentication requests sent via aireplay-ng

- Perform a KARMA attack using "hostapd-wpe," luring the victim to connect to the malicious Wi-Fi network.
- After successful de-authentication, use tools such as "**dnsmasq**" and Python scripts to inject a malicious URL and force the victim's browser to load that malicious URL. Based on the BSSID and ESSID, the URL/page pair to be sent can be detected.
- Wait for the victim to access the HTTP page. At this moment, the victim's router is updated and automatically restarted.

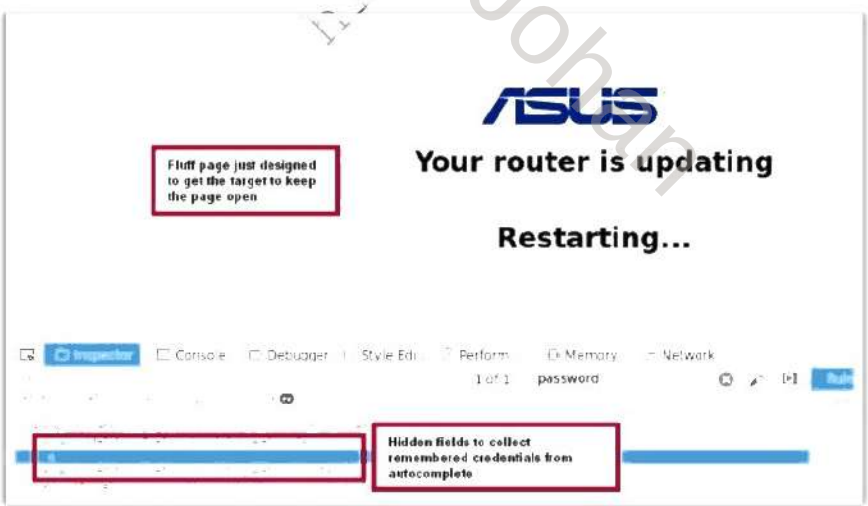


Figure 16.79: Screenshot showing the update and restarting of the router

- Once the victim opens the malicious page, the browser will check the following two conditions to automatically load the page having stored credentials:
  - Do the malicious URL and the router's admin interface have the same origin?
  - Do the input fields of the page and the router's admin interface match?
- After receiving the credentials, the victim is made to access the page for some more time. Subsequently, stop the KARMA attack and allow the victim to connect back to their legitimate network. Once the victim's device is connected to the legitimate network, the malicious page remains in the router's admin interface, along with admin credentials loaded into the JavaScript.
- Use XMLHttpRequest to login to the router to extract the victim's WPA2 PSK and further perform any other malicious changes as necessary. Using this PSK and other credentials, the victims' private network can be hacked, and critical data can be accessed and tampered using the Wi-Jacking technique.

RFID Cloning Attack

RFID cloning involves capturing the data from a legitimate RFID tag and then creating its clone using a new chip. In other words, data from one RFID tag are copied into another tag by changing the tag ID (TID), but the form factor and data may remain the same. The cloned copy is different from the original RFID tag and may be easily detected. Attackers use iCopy-X, RFIDler, Flipper Zero etc. to clone RFID tags.

- **iCopy-X**

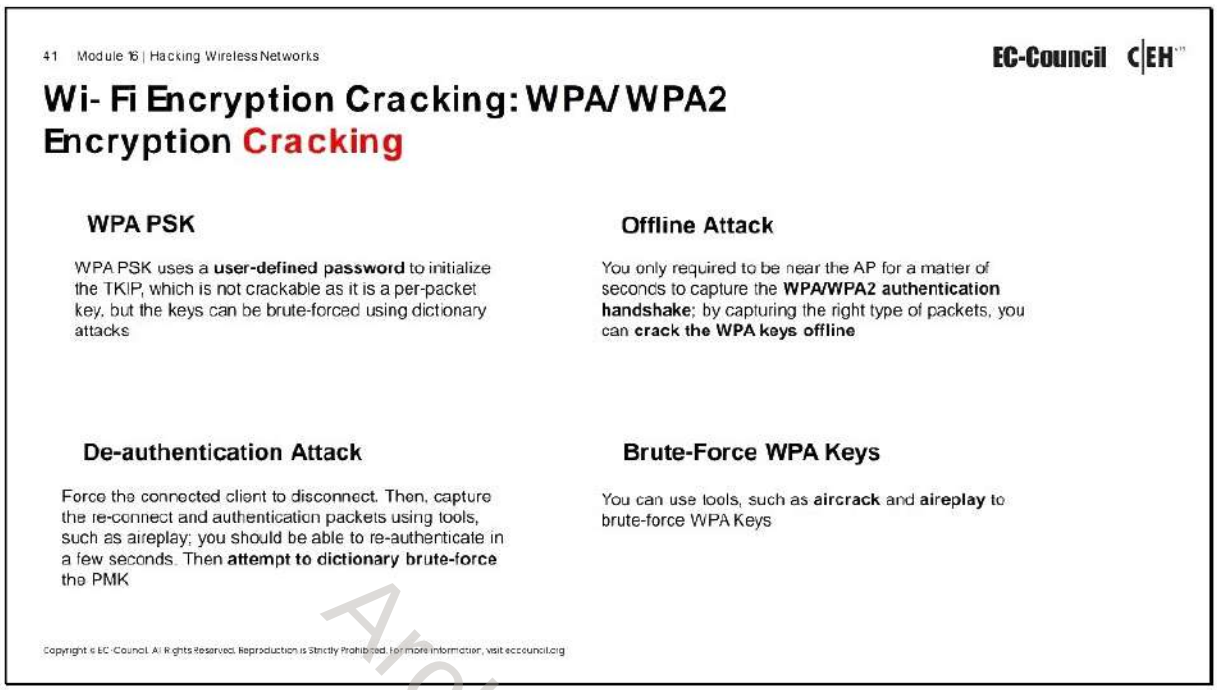
  Source: *https://icopyx.com*

  iCopy-X is a portable RFID cloning device that can be used by attackers to clone RFID tags. It is an entirely stand-alone device with an integrated screen and buttons, providing the functionality of a Proxmark but without the need for 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

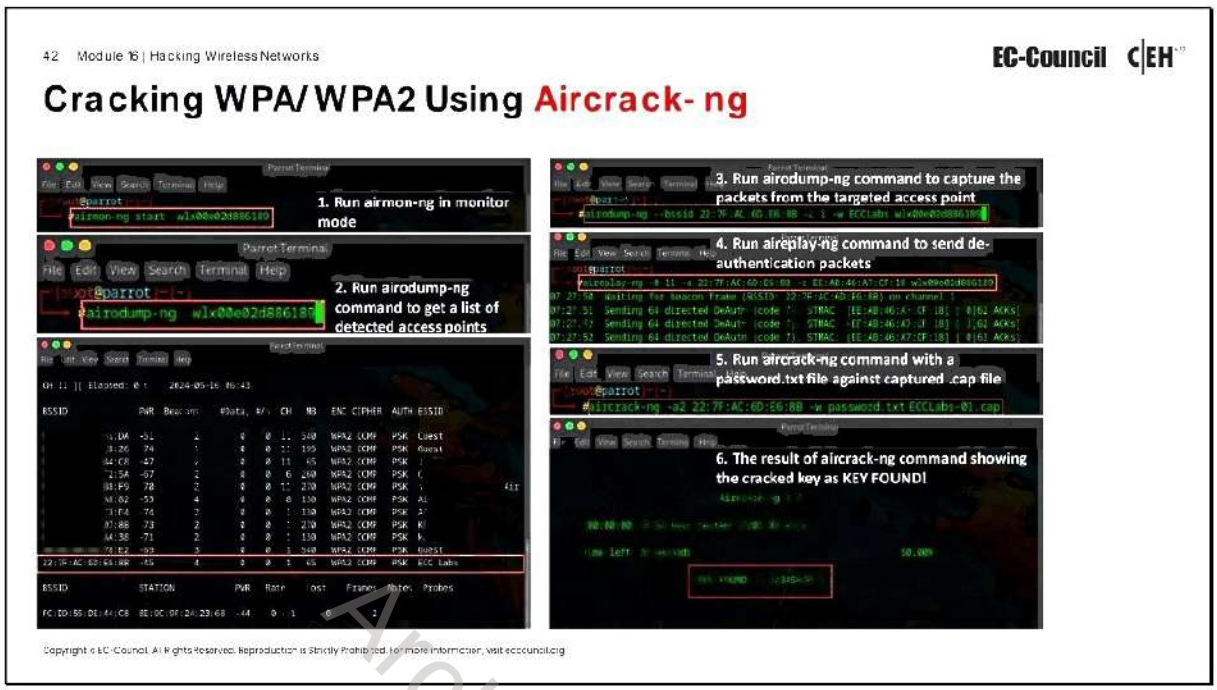
After an attacker succeeds in obtaining unauthorized access to a target network through methods such as wireless attacks, rogue APs, and evil twins, the attacker must crack the security imposed by the target wireless network. Generally, for securing wireless communication, Wi-Fi networks use WPA/WPA2/WPA3 encryption, which the attacker must crack. In this section, we examine how an attacker can crack these encryption systems to breach the wireless network security.

WPA/WPA2 Encryption Cracking

WPA encryption is less exploitable than WEP encryption. However, an attacker can still crack WPA/WPA2 encryption by capturing the necessary type of packets. The attacker can perform this offline but needs to be near the AP for a few moments. The following are some types of techniques used to crack WPA encryption.

- **WPA PSK**: WPA PSK uses a user-defined password to initialize the four-way handshake. An attacker cannot crack this password, because it is a per-packet key, but the keys can be brute-forced using dictionary attacks. A dictionary attack can compromise most consumer passwords.
- **Offline attack**: To perform an offline attack, an attacker needs to be near the AP for a few seconds to capture the WPA/WPA2 authentication handshake. By capturing the necessary type of packets, WPA encryption keys can be cracked offline. In WPA handshakes, the protocol does not send the password across the network, because the WPA handshake typically occurs over insecure channels and in plaintext. Capturing a full authentication handshake from a client and the AP helps in breaking the WPA/WPA2 encryption without any packet injection.

- **De-authentication attack**: To perform a de-authentication attack to crack the WPA encryption, an attacker needs to find an actively connected client. The attacker forces the client to disconnect from the AP, following which they use tools such as aireplay to capture the authentication packet when the client attempts to reconnect. The client should be able to re-authenticate itself with the AP in a few seconds. The authentication packet includes the pairwise master key (PMK), which the attacker can crack by dictionary or brute-force attacks to recover the WPA key.
- **Brute forcing of WPA keys**: Brute-force techniques are useful in breaking WPA/WPA2 encryption keys. An attacker can perform a brute-force attack on WPA encryption keys using a dictionary or using tools such as aircrack and aireplay. The brute-force technique has a substantial impact on WPA encryption because of its compute-intensive nature. Breaking WPA keys through a brute-force technique may take hours, days, or even weeks.



Cracking WPA/WPA2 Using Aircrack-ng

Cracking WPA/WPA2 using aircrack-ng involves a series of steps to ensure the security of Wi-Fi networks. The process begins by enabling monitor mode on a compatible Wi-Fi adapter to capture traffic. Airodump-ng is then used to capture a WPA/WPA2 handshake, which is often facilitated by sending deauthentication packets to force client reconnection. Once a handshake is captured, aircrack-ng attempts to crack the password by comparing it with a wordlist of potential passwords.

The following are the steps to crack WPA-PSK:

- Monitor wireless traffic with airmon-ng using the following command:

  airmon-ng start <wireless interface>

  Note: Run the command airmon-ng check kill if an error saying finds two processes that could cause trouble

Figure 16.81: Screenshot displaying the execution of airmon-ng

- Run airodump-ng command to get a list of detected access points and connected clients.

  airodump-ng <Wireless Interface>

Figure 16.82: Screenshot displaying the execution of airodump-ng

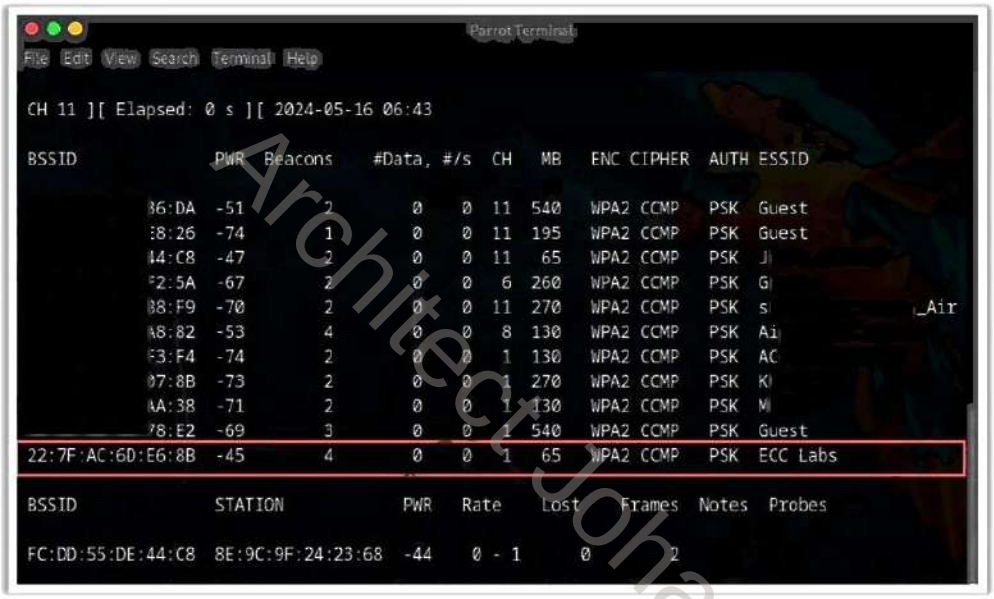


Figure 16.83: Screenshot showing list of detected access points

- From the above screenshot, select the target wireless access point
- Open a new terminal and run the following airodump-ng command to capture packets from the targeted access point as the root user and leave the terminal.

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

Figure 16.84: Screenshot displaying the execution of airodump-ng

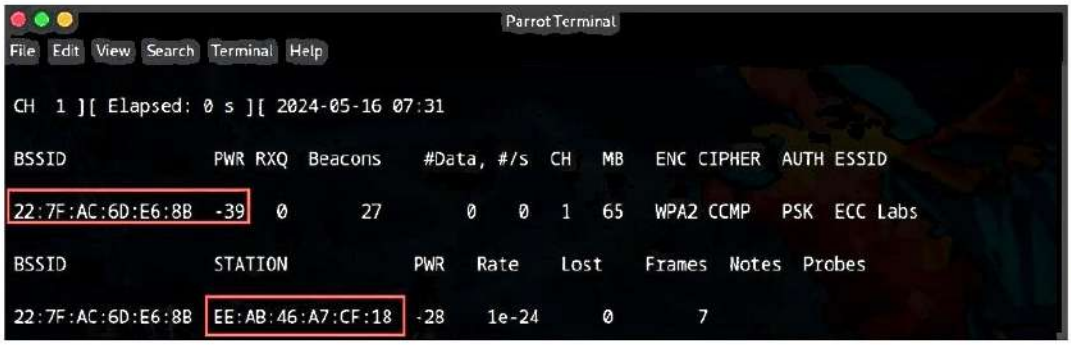


Figure 16.85: Screenshot displaying the result of airodump-ng

- Open a new terminal and run the following aireplay-ng command multiple times to send a large number of deauthentication packets to the connected device.

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

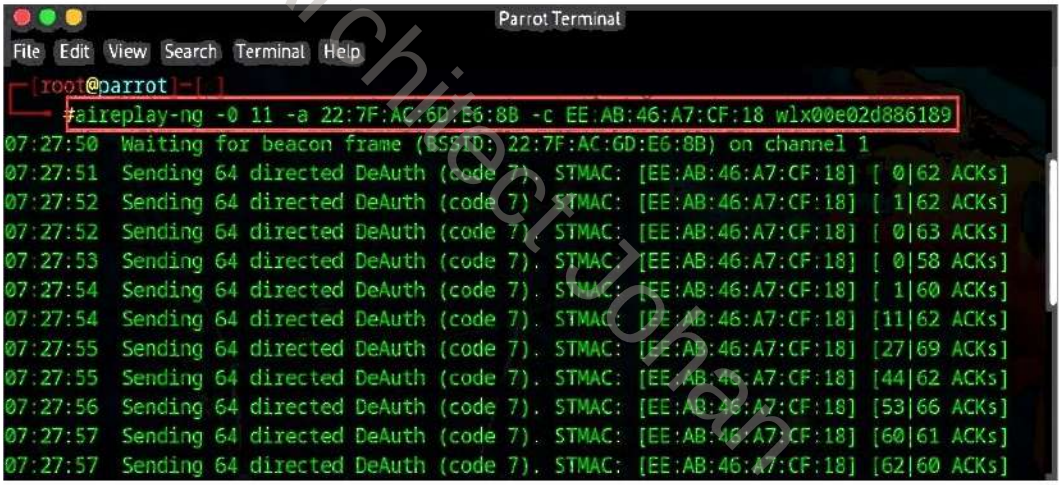


Figure 16.86: Screenshot displaying the execution of aireplay-ng

- Switch to the airodump-ng terminal that is left running and keep capturing packets until the WPA handshake: 22:7 F: AC: 6D: E6:8 B packet is received. The captured packets were saved in a .cap file.
- In another net terminal, run the following aircrack-ng command as root user with a password.txt file against the captured .cap file.

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

Figure 16.87: Screenshot displaying the execution of aircrack-ng

- The result of the aircrack-ng command is as follows: show the cracked key as KEY FOUND!. If the password is complex, it takes longer to crack.

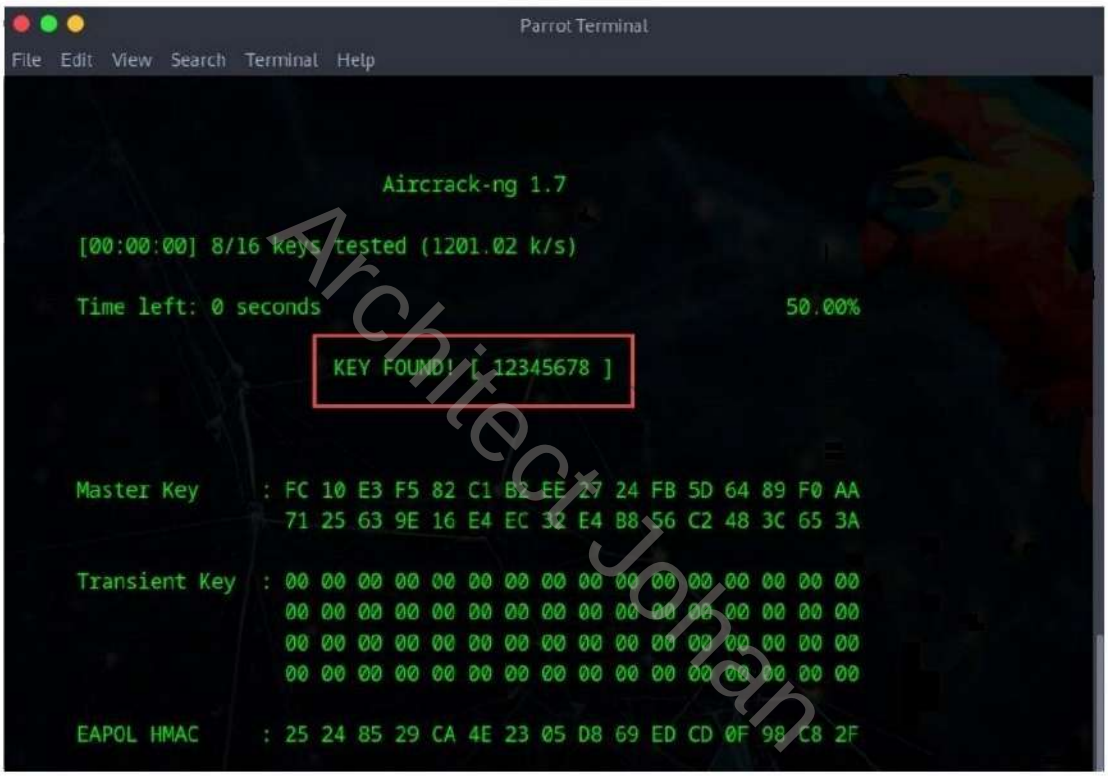
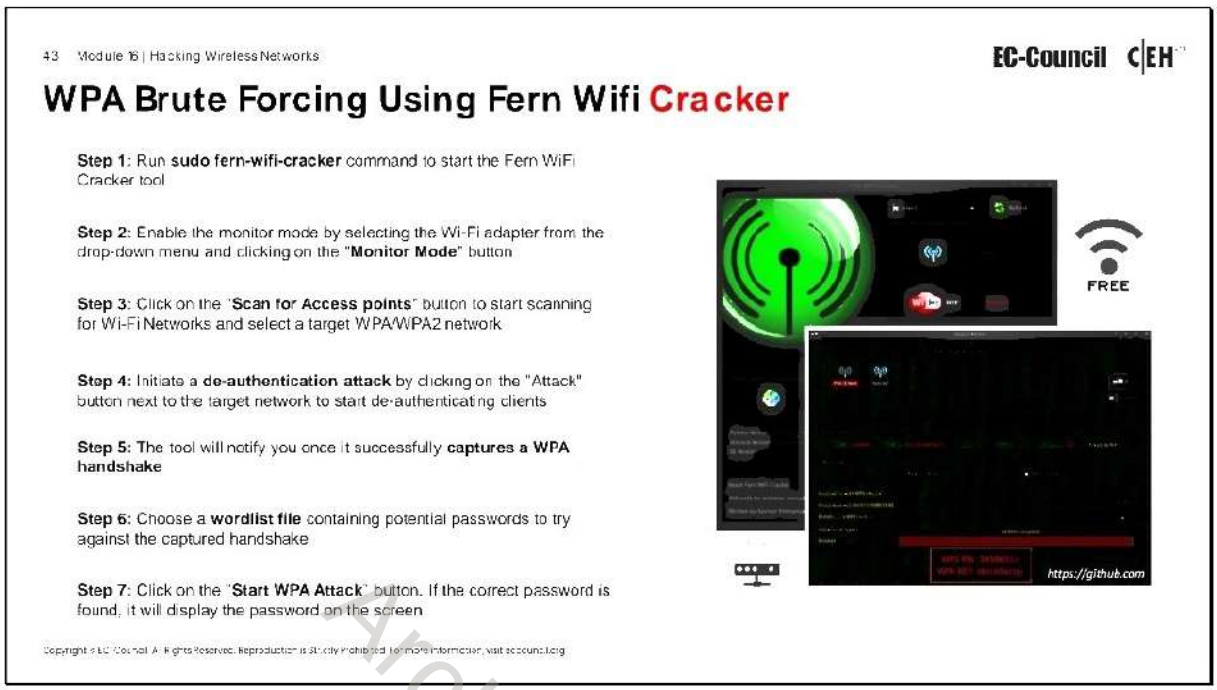


Figure 16.88: Screenshot displaying the result of aircrack-ng cracking the WPA/WPA2 password

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

Source: *https://github.com*

Fern Wi-Fi Cracker is a wireless security auditing and attack software written using the Python programming language and the Python Qt graphical user interface (GUI) library. The program can crack and recover WPA/WPS keys and execute other network-based attacks on wireless or Ethernet-based networks.

Steps to perform WPA brute forcing:

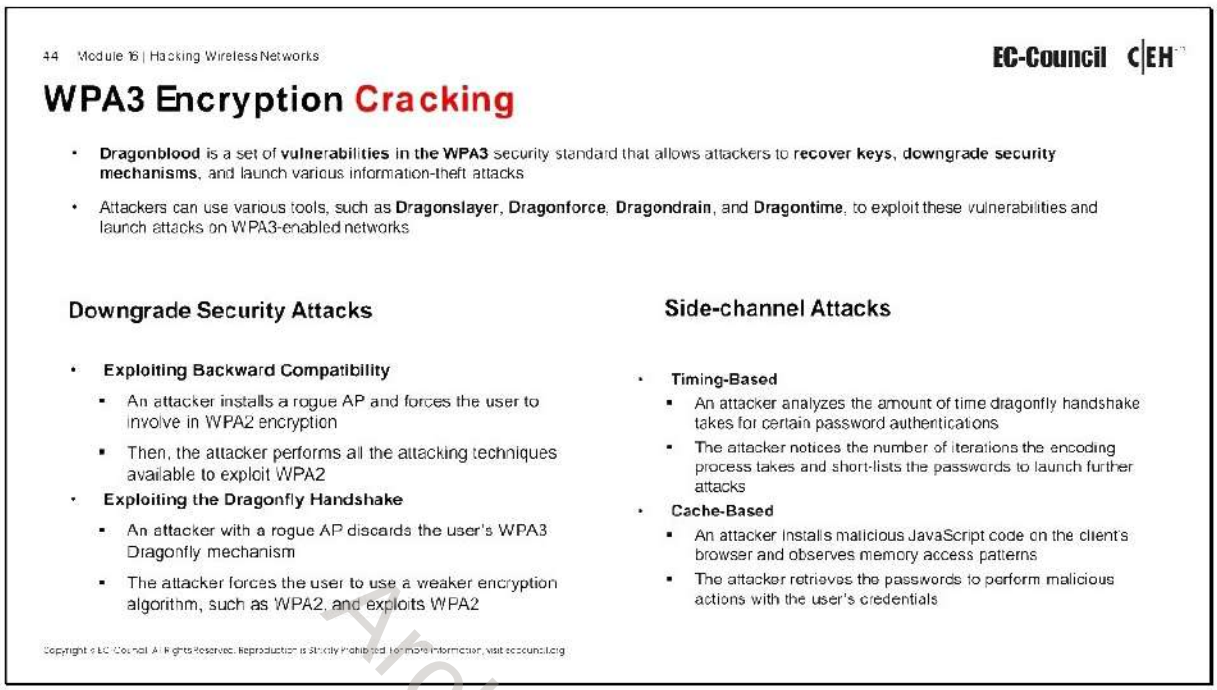
- **Step 1:** Run the following command to start the Fern WiFi Cracker tool:

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

- **Step 2:** Enable Monitor Mode by selecting the Wi-Fi adapter from the drop-down menu and clicking on the "**Monitor Mode**" button.
- **Step 3:** Click on the "**Scan for Access points**" button to start scanning for Wi-Fi Networks and select a target **WPA/WPA2** network from the list of discovered networks.
- **Step 4:** Now, initiate a de-authentication attack by clicking on the "**Attack**" button next to the target network to start de-authenticating clients. This forces a connected client to re-authenticate and capture the WPA handshake during the process.
- **Step 5:** The tool notifies the user once it successfully captures a WPA handshake.
- **Step 6:** Choose a wordlist file containing potential passwords to try against the captured handshake (e.g., rockyou.txt, located in /usr/share/wordlists/).

- **Step 7:** Click the "**Start WPA Attack**" button. It begins by testing each password in the wordlist against a captured handshake. If the correct password is found, it is displayed on the screen, as shown in the screenshot.

Figure 16.89: Screenshot displaying 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 (also known as SAE) handshake function to supply the strongest password-based authentication to date. However, it is still vulnerable to password-cracking attacks. Dragonblood is a set of vulnerabilities in the WPA3 security standard that allows attackers to recover keys, downgrade security mechanisms, and launch various information-theft attacks. Attackers can use various tools such as Dragonslayer, Dragonforce, Dragondrain, and Dragontime to exploit these vulnerabilities and launch attacks on WPA3-enabled networks. The following are some of the techniques used to crack WPA3 encryption.

- **Downgrade Security Attacks**

  To launch this attack, the client and AP should support both WPA3 and WPA2 encryption mechanisms. Here, the attacker forces the user to follow the older encryption method, WPA2, to connect to the network.

  A downgrade security attack can be implemented in the following two ways.

  - **Exploiting backward compatibility:** If a user and AP are compatible with both WPA2 and WPA3 encryption mechanisms, then the attacker installs a rogue AP with only WPA2 compatibility in the vicinity and forces the client to go through the four-way handshake (WPA2) to get connected. Once the connection is established, the attacker uses all the attack tools available to exploit or crack the WPA2 encryption.
  - **Exploiting the Dragonfly handshake:** In this method, the attacker masquerades as an authentic AP. When a user attempts to exchange keys to access the Internet using the WPA3 authentication mechanism, the attacker informs the user that it does not support the WPA3 method. Then, the attacker suggests the use of a

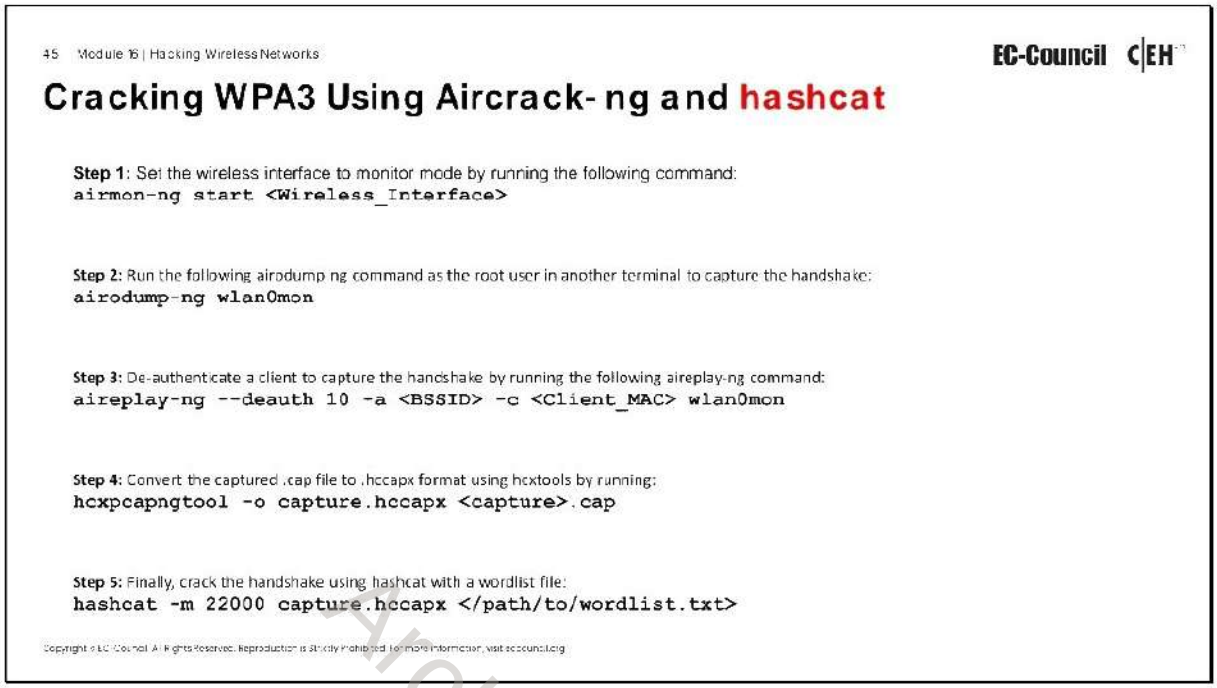
weaker encryption mechanism such as WPA2 for accessing the Internet. Subsequently, the attacker can use various techniques to exploit or crack the WPA2 encryption.

- **Side-Channel Attacks (Information-Leaking Attack)**

  Attackers target protocols or encryption mechanisms used by devices that attempt to connect to a network. During the key-exchange process, the attacker launches this attack to capture leaked information. This information is further used by the attacker to launch brute-force or dictionary attacks to obtain all the data of the target user.

  A side-channel attack can be implemented in the following two ways.

  - **Timing-based attack:** In this attack, the attacker analyzes the time taken by the Dragonfly handshake to encode a certain password authentication process. In the analysis, the attacker observes the iterations of encoding process and short-lists possible passwords. After obtaining a list of passwords, the attacker attempts to gain access to the target user's device using various techniques.
  - **Cache-based attack:** In this attack, the attacker injects a malicious JavaScript or web application in the target user's web browser. This allows the attacker to take control of the user's web browser and further observe memory access patterns to retrieve password information.



Cracking WPA3 Using Aircrack-ng and hashcat

Source: *https://github.com, https://hashcat.net*

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

- **Step1:** Set the wireless interface to monitor mode by running the following command:

  airmon-ng start <Wireless_Interface>

- **Step 2:** Run the following airodump-ng command as the root user on another terminal to capture the handshake:

  airodump-ng wlan0mon

  Alternatively, focus on a target network with the command:

  airodump-ng --bssid <BSSID> --channel <CH> --write capture wlan0mon

- **Step 3:** De-authenticate the client to capture the handshake by running the following aireplay-ng command:

  aireplay-ng --deauth 10 -a <BSSID> -c <Client_MAC> wlan0mon

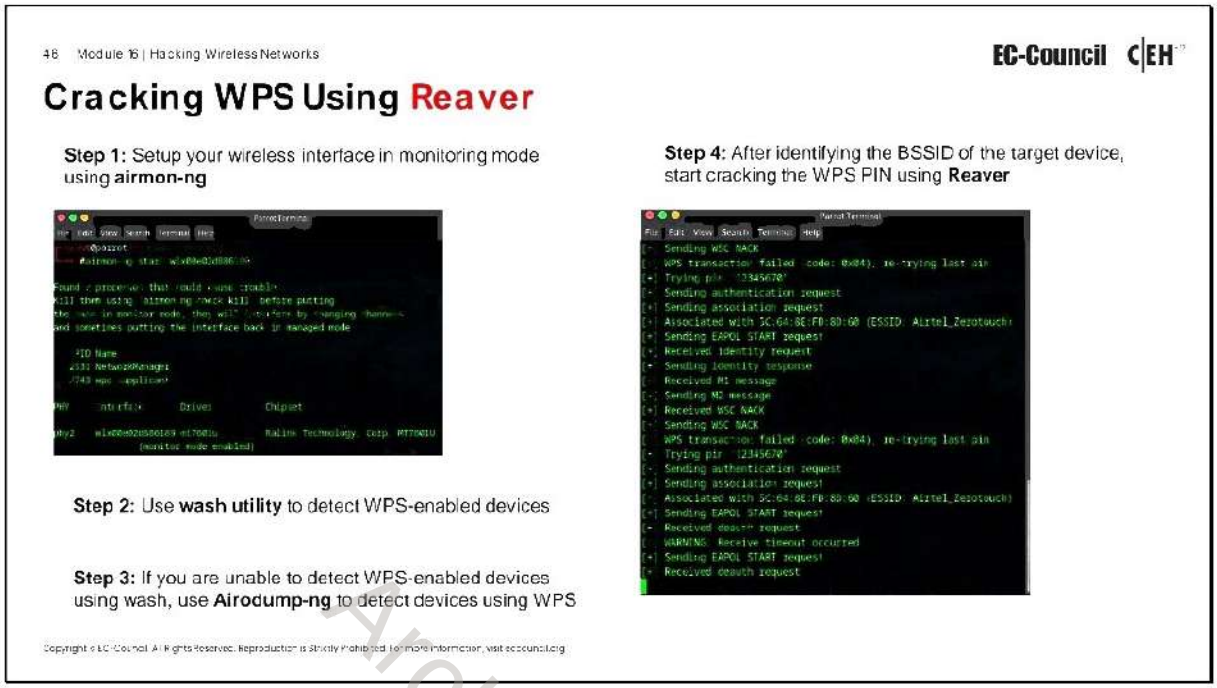
  This command forces a client to reconnect, capturing the handshake in the process.

- **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:

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



Cracking WPS Using Reaver

Source: *https://github.com*

Reaver is designed to be a robust and practical attack tool against Wi-Fi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases, and it has been tested against a wide variety of APs and WPS implementations. WPS PIN can be cracked using Reaver through the following steps.

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

  airmon-ng <start|stop> <interface>

  For example,

  airmon-ng start wlan0

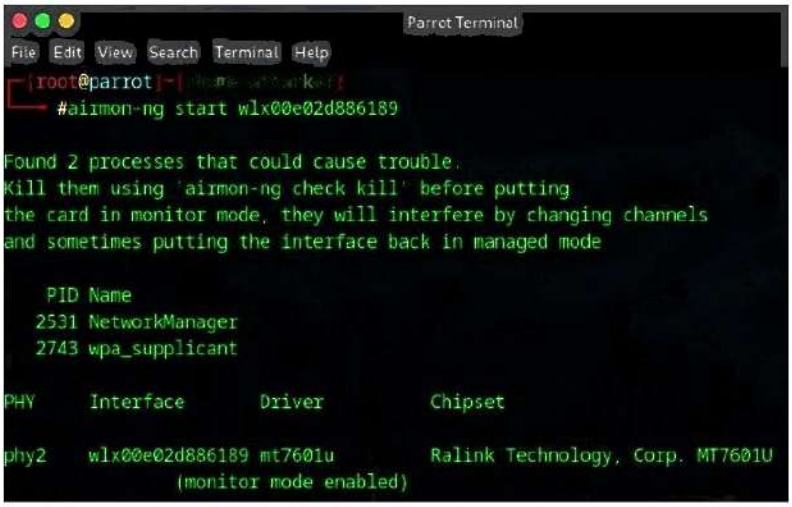


Figure 16.90: Screenshot of airmon-ng

- Use the Wash utility to detect WPS-enabled devices using the following command:

  wash -i <interface>

  For example,

  wash -i mon0

- If WPS-enabled devices could not be detected using the Wash utility, use Airodump-ng to detect devices using WPS through the following command:

  airodump-ng <interface>

  For example, if the device configuration in the monitor mode was observed as **wlan0mon** in the previous step, the command should be

  airodump-ng wlan0mon

  This command displays all the available BSSIDs (MAC addresses of APs).

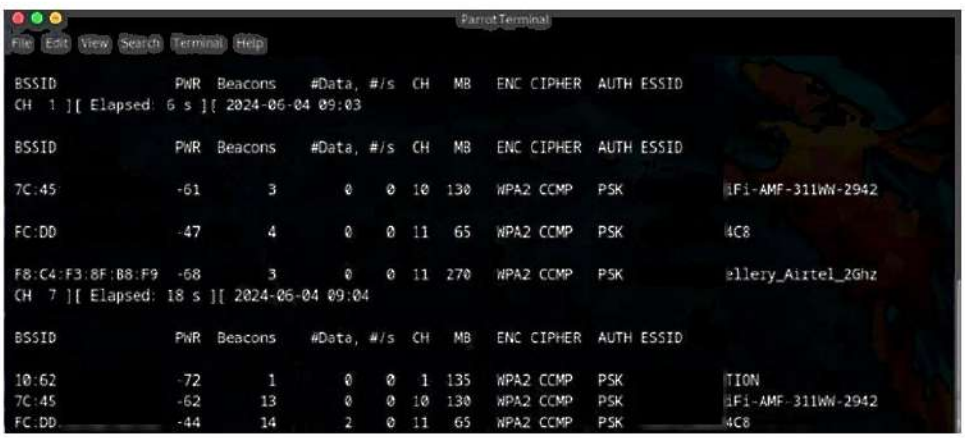


Figure 16.91: Screenshot of airodump-ng

- After identifying the BSSID of the target device, start cracking the WPS PIN using Reaver through the following command:

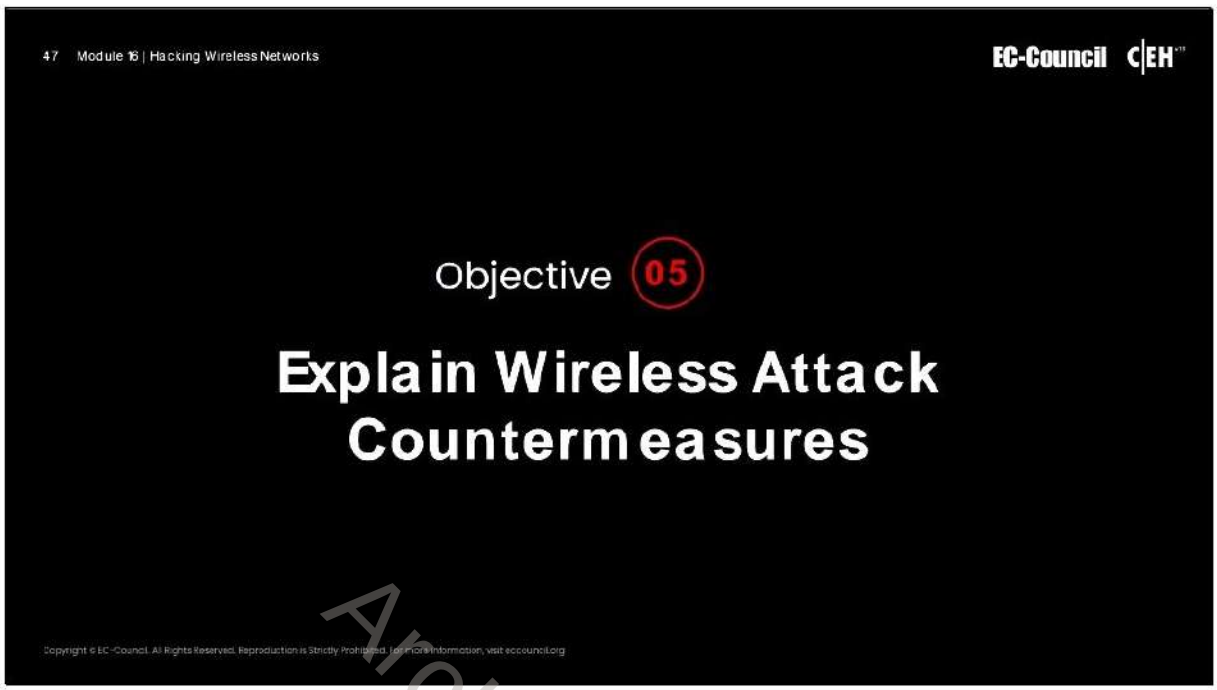
  reaver -i <Name of the monitor-mode interface to use> -b < BSSID of the target AP> -vv <Display non-critical warnings>

  For example,

  reaver -i wlan0mon -b B4:75:0E:89:00:60 -vv

  The above command scans all the WPS PINs available until it finds a matching PIN. After detecting the WPS PIN, it starts exploitation.

Figure 16.92: Screenshot of Reaver displaying the output



Wireless Attack Countermeasures

The previous sections explained how attackers hack wireless networks to obtain sensitive data. An ethical hacker works on increasing the security of a wireless network. To secure a wireless network, it is important to implement and adopt appropriate countermeasures. This section lists the countermeasures and best practices for wireless network security.

Wireless Security Layers

A wireless security mechanism has six layers. This layered approach increases the scope of preventing an attacker from compromising a network and increases the possibility of catching the attacker. The below figure shows the structure of wireless security layers.

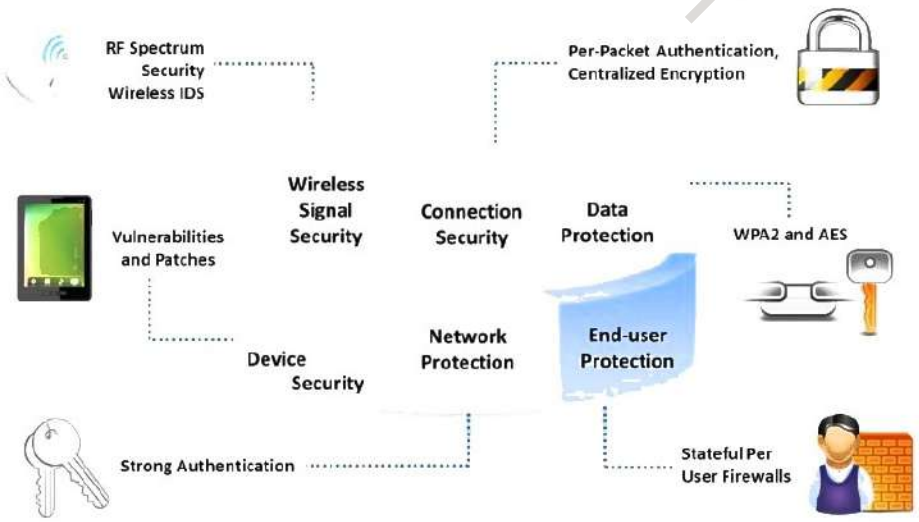
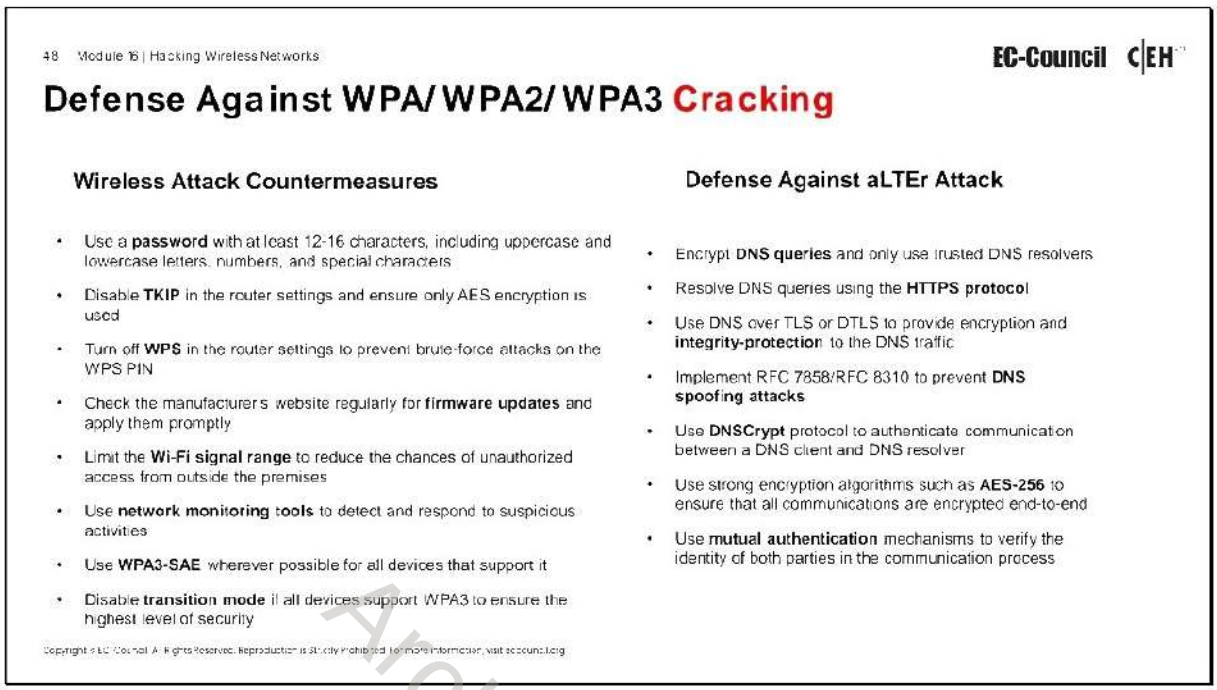


Figure 16.93: Structure of wireless security layers

- **Wireless signal security**: In wireless networks, the network and RF spectrum within the environment should be continuously monitored and managed to identify the threats and awareness capability. A wireless intrusion detection system (WIDS) analyzes and monitors the RF spectrum. Alarm generation helps detect unauthorized wireless devices that violate the security policies of the network. Activities such as increased bandwidth usage, RF interferences, and unknown rogue wireless APs might indicate a malicious intruder on the network. Continuous monitoring of the network is the only measure that can prevent such attacks and secure the network.
- **Connection security**: Per frame/packet authentication provides protection against MITM attacks. It prevents an attacker from sniffing data when two genuine users communicate with each other, thereby securing the connection.
- **Device security**: Both vulnerability and patch management are important components of the security infrastructure.
- **Data protection**: Encryption algorithms such as WPA3, WPA2, and AES can protect data.
- **Network protection**: Strong authentication ensures that only authorized users gain access to a network.
- **End-user protection**: Even if the attacker has associated with APs, personal firewalls installed on the end user systems on the WLAN prevents the attacker from accessing files.



Defense Against WPA/WPA2/WPA3 Cracking

- **Use Strong Passwords**
  - Ensure that the WiFi password (pre-shared key) is strong, complex, and difficult to guess.
  - Use a password that is at least 12-16 characters long, including uppercase and lowercase letters, numbers, and special characters.
- **Client Settings**
  - Use WPA2 with AES/CCMP encryption only.
  - Set proper client settings (e.g., validate the server, specify server address, and do not prompt for new servers).
  - Regenerate keys for every new connection.
- **Additional Controls**
  - Use virtual-private-network (VPN) technologies such as remote access VPN, extranet VPN, and intranet VPN.
  - Implement protocols such as IPsec and SSL/TLS for secure communication.
  - Implement a network access control (NAC) or network access protection (NAP) solution for additional control over end-user connectivity.
- **Disable TKIP**
  - Disable TKIP in the router settings and ensure only AES encryption is used.

- **MAC Address Filtering**
  - Allow only devices with specific MAC addresses to connect the network.
- **Upgrade to WPA3**
  - WPA3 can prevent exploitation of connected devices and offers better protection against brute-force attacks.
- **Disable Remote Management**
  - Turn off remote management features on routers to prevent external attacks.
- **Disable WPS**
  - WPS has known vulnerabilities that can be exploited to gain access to the network. Turn off WPS in the router settings to prevent brute-force attacks on the WPS PIN.
- **Regularly Update Router Firmware**
  - Keep the router's firmware up to date with patch known vulnerabilities. Check the manufacturer's website regularly for firmware updates and promptly apply them.
- **Reduce Signal Range**
  - Limit the Wi-Fi signal range to reduce the chances of unauthorized access from outside the premises. Adjust the router's transmission power and place it centrally within the desired location.
- **Monitor Network Activity**
  - Regularly monitor the network for any unusual activity or unauthorized devices. Use network monitoring tools to detect and respond to suspicious activities.
- **Enable WPA3-SAE**
  - WPA3-SAE provides stronger security by protecting against offline dictionary attacks and offering forward secrecy. Use WPA3-SAE whenever possible for all devices that support it.
- **Disable Transition Mode**
  - WPA3 allows for WPA2/WPA3 mixed mode, which can pose a potential security risk. Disable the transition mode if all devices support WPA3 to ensure the highest level of security.

Defense Against KRACK Attacks

The following are some countermeasures to prevent KRACK attacks.

- Update all the routers and Wi-Fi devices with the latest security patches.
- Turn on auto updates for all the wireless devices and patch the device firmware.
- Avoid using public Wi-Fi networks.
- Browse only secured websites and do not access sensitive resources when the device is connected to an unprotected network.

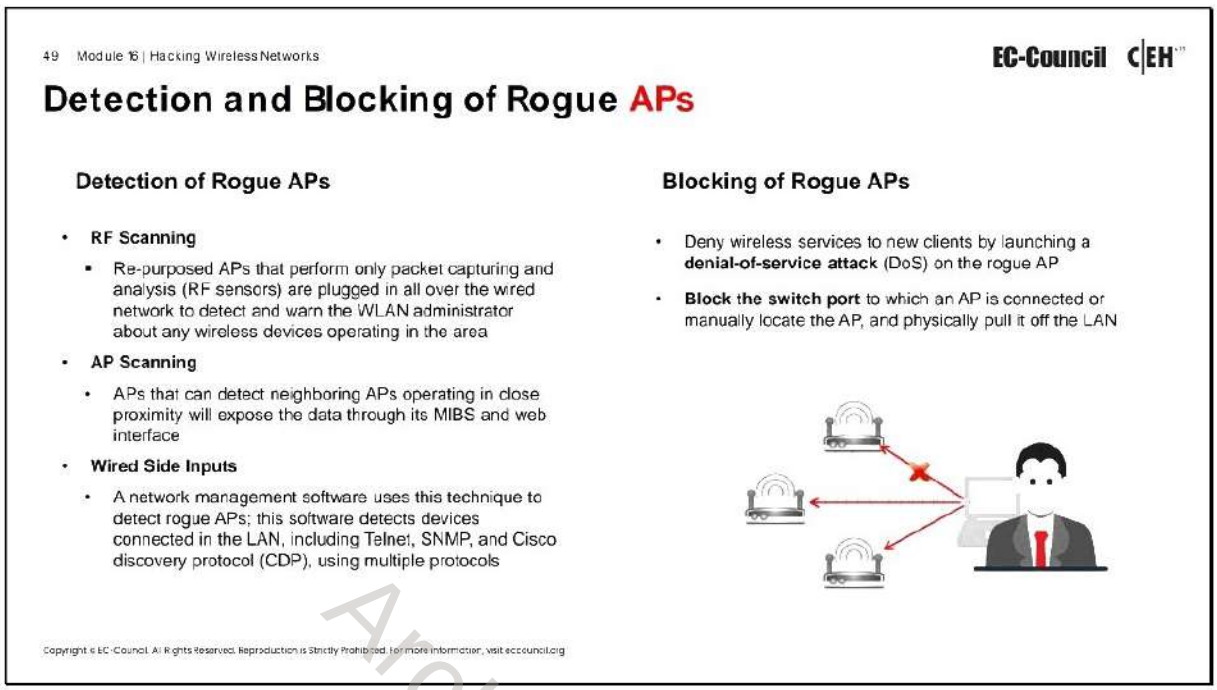
- If there are IoT devices, audit the devices and do not connect to insecure Wi-Fi routers.
- Always enable the HTTPS Everywhere extension.
- Enable two-factor authentication.
- Use a VPN to secure information in transit.
- Always use the Wi-Fi Protected Access 3 (WPA3) security protocol for wireless networks.
- Disable fast roaming and the repeater mode in wireless devices to improve the mitigation of KRACK attacks.
- Employ the EAPOL-key replay counter to ensure that the AP recognizes only the latest counter value.
- Use a backup wired connection (Ethernet) or mobile data immediately when a vulnerability to KRACK attacks is detected.
- Employ alternative third-party routers instead of ISP-provided routers if they do not provide sufficient security patches.
- Use network segmentation to separate critical parts of a network from general user access to limit the potential impact of a KRACK attack.
- Temporarily disable the 802.11r protocol, which is susceptible to KRACK attacks. Turn off 802.11r in the wireless network settings if not needed for seamless roaming.
- Use 802.1X authentication for an added layer of security. Implement 802.1X with RADIUS server authentication for enterprise networks.

Defense Against aLTEr Attacks

The foremost recommended method to defend a network from aLTEr attacks is to encrypt DNS queries with proper security standards. To implement this measure, Cisco, in collaboration with Apple, developed an app named "Cisco Security Connectors" that prevents clients from entering unintended websites. This app encrypts DNS queries and loads them into the Cisco Umbrella (intelligence block) for further validation. It protects the network from hijacking at the IP level as well as the DNS level. The following countermeasures can be adopted to defend against aLTEr attacks.

- Encrypt DNS queries and use only trusted DNS resolvers.
- Resolve DNS queries using the HTTPS protocol.
- Access only websites having HTTPS connections.
- Use DNS over the Transport Layer Security (TLS) or DNS over datagram TLS (DTLS) to encrypt the DNS traffic and for integrity protection.
- Implement RFC 7858/RFC 8310 to prevent DNS spoofing attacks. It can also increase the encryption and intelligent policies for name resolution.
- Add a message authentication code (MAC) to user plane packets.
- Use the DNSCrypt protocol to authenticate communication between a DNS client and a DNS resolver.

- Use mobile device tools such as Zimperium to detect phishing and other attacks from malicious sites.
- Use correct HTTPS parameters, such as HSTS, to avoid being redirected to a malicious website.
- Use a virtual network tunnel with integrity protection and endpoint authentication.
- Upgrade to 5G network connection.
- Implement eSIM technology for improved authentication and encryption.
- Implement DNSSEC to secure DNS lookup processes, which ensures authenticity of response data.
- Ensure that all LTE network infrastructure components such as base stations and core network equipment have the latest firmware and software updates.
- Regularly apply patches from network equipment vendors to fix known vulnerabilities.
- Employ robust encryption methods to protect data transmitted over LTE networks. Use strong encryption algorithms such as AES-256 and ensure that all communications are encrypted end-to-end.
- Ensure that both the user equipment (UE) and network authenticate each other to prevent unauthorized access. Use mutual authentication mechanisms to verify the identity of both parties in the communication process.
- Deploy secure SIM cards with enhanced security features to protect against cloning and unauthorized access. Use SIM cards that support advanced security features such as over-the-air (OTA) updates and secure storage.
- Restrict access to network services based on the geographical location of the user equipment. se location-based access controls to limit access to sensitive network services from unauthorized locations.
- Ensure that physical network infrastructure is secure and protected from tampering. Use physical security measures such as surveillance, access controls, and tamper-evident seals to protect network equipment.



Detection and Blocking of Rogue APs

- **Detection of Rogue APs**
  - **RF scanning**: Re-purposed APs that perform only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the WLAN administrator about any wireless devices operating in the area.
  - **AP scanning**: APs that have the functionality of detecting neighboring APs will expose the data through its MIBS and web interface.
  - **Wired side inputs**: Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, and Cisco Discovery Protocol (CDP), using multiple protocols.
  - **Comparison with authorized AP list**: Maintain a list of authorized APs and compare them with the detected APs to identify unauthorized devices. Use tools such as the AirMagnet WiFi Analyzer to compare the detected APs with a predefined list of authorized APs.
  - **Signal strength analysis:** Analyze the signal strength of detected APs to identify those that may be physically close but not authorized. Tools such as the Ekahau Survey for Wi-Fi Planning and Analysis can help identify unexpected APs based on the signal strength.
  - **MAC address filtering:** Monitor the network for MAC addresses of known authorized APs and flag any unknown MAC addresses. Use Cisco Wireless LAN Controllers that provide built-in rogue AP detection and MAC address-filtering features.

- **Blocking of Rogue APs**
  - Deny wireless service to new clients by launching a denial-of-service (DoS) attack on the rogue AP.
  - Block the switch port to which the AP is connected or manually locate the AP and physically remove it from the LAN.
  - Use Wireless intrusion prevention systems (WIPS) to continuously monitor the wireless spectrum for unauthorized devices and perform automated actions to block rogue APs.
  - Use access control lists (ACLs) to restrict network access to known, authorized MAC addresses.
  - Implement 802.1X authentication to control access to the network and ensure that only authenticated users and devices are connected.
  - Segment the network to isolate critical resources from general wireless access.
  - Disable broadcasting of open SSIDs to reduce the risk of unauthorized connections.
  - Maintain a whitelist of authorized MAC addresses and configure the wireless controller to block all others.

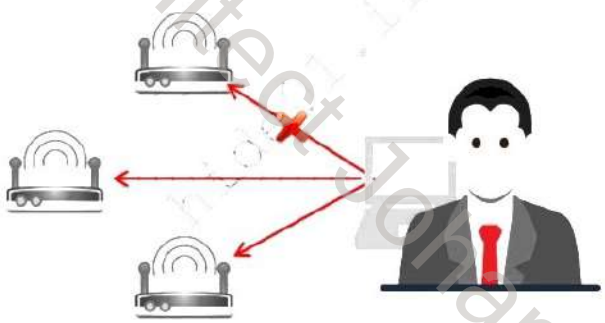
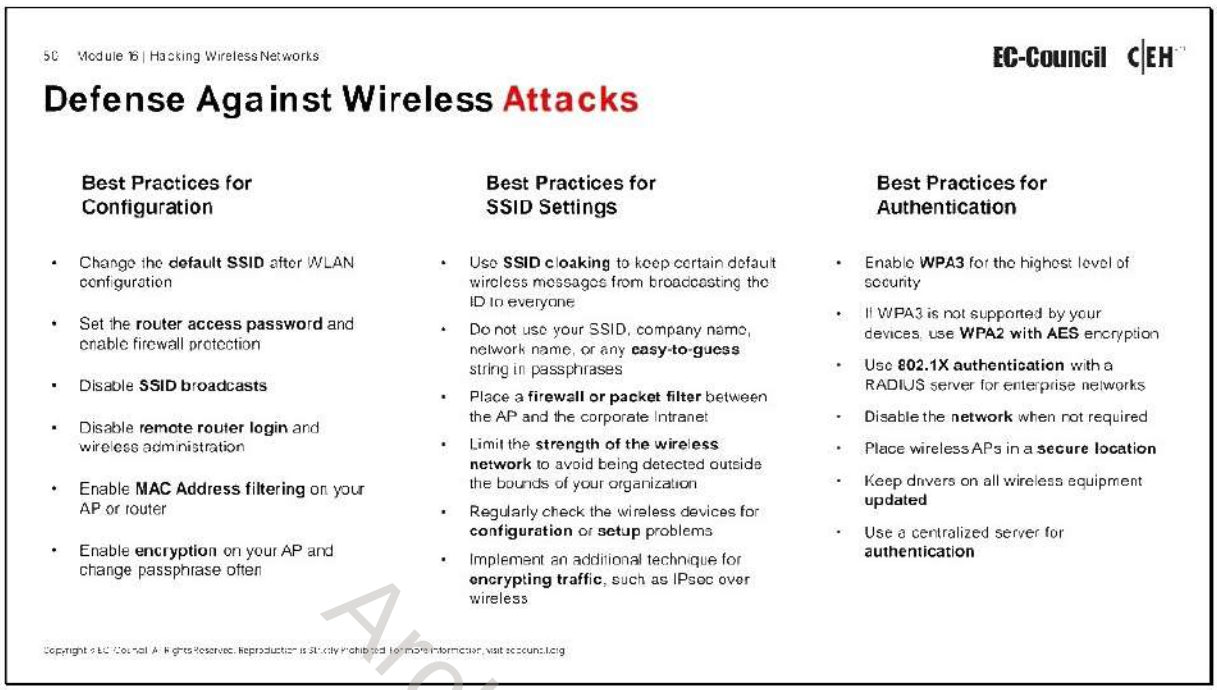


Figure 16.94: Blocking of rogue APs



Defense Against Wireless Attacks

- **Best Practices for Configuration**
  - Change the default SSID after WLAN configuration.
  - Set the router access password and enable firewall protection.
  - Disable SSID broadcasts.
  - Disable remote router login and wireless administration.
  - Enable MAC address filtering on APs or routers.
  - Enable encryption on APs and change passphrases often.
  - Close all unused ports to prevent attacks on APs.
  - Segregate the network to ensure that guests are not given access to the private network.
  - Employ closed networks and provide the SSID to the employees, instead of allowing them to select it from a broadcast list.
  - Disable the Dynamic Host Configuration Protocol (DHCP) and rely on static IP addresses.
  - Disable the Simple Network Management Protocol (SNMP). If it is required, configure the settings to the least privileges.
  - Change the default IP address of the router console.
  - Always use WPA3 encryption if supported. If WPA3 is not available, use WPA2 with AES encryption.

- Turn off WPS on the router.
- Use VLANs or separate SSIDs to segment different types of traffic.
- Adjust the transmission power of the router to limit the Wi-Fi signal range to the required premises.
- Turn off services and close ports that are not needed for the network operations.
- Use the built-in firewall on the router to filter incoming and outgoing traffic.
- Set up a separate guest network for visitors with restricted access to the main network resources.

- **Best Practices for SSID Settings**
  - Use SSID cloaking to keep certain default wireless messages from broadcasting the SSID to everyone.
  - Do not use the SSID, company name, network name, or any easy-to-guess string in passphrases.
  - Place a firewall or packet filter between an AP and the corporate Intranet.
  - Limit the strength of the wireless network so that it cannot be detected outside the bounds of the organization.
  - Check the wireless devices for configuration or setup problems regularly.
  - Implement an additional technique for encrypting traffic, such as IPsec over wireless.
  - Modify the SSID with some unique characters and strings, instead of using the manufacturer's default SSID.
  - Use a separate SSID for guest users to isolate them from the organizational network.
  - Separate the organizational network into multiple zones with their own SSIDs to reduce the level of exploitation during attacks.
  - Always keep the SSID broadcast of the organization's wireless devices in the hidden mode.
  - Ensure that each SSID is protected with WPA3 encryption if supported or WPA2 with AES encryption as the minimum.
  - Periodically change SSIDs and associated passwords.
- **Best Practices for Authentication**
  - Enable WPA3 for the highest level of security, as it provides enhanced encryption and protection against attacks.
  - If WPA3 is not supported by the device, use WPA2 with AES encryption (avoid using WPA or TKIP).

- Use 802.1X authentication with a RADIUS server for enterprise networks to provide individual credentials for each user.
- Where possible, implement multifactor authentication to add an extra layer of security.
- For 802.1X deployments, ensure proper management of digital certificates, including using strong encryption and regularly updating certificates.
- Disable the network when not required.
- Place wireless APs in a secured location.
- Keep drivers on all wireless equipment updated.
- Use a centralized server for authentication.
- Enable server verification on the client side using 802.1X authentication to prevent MITM attacks.
- Enable two-factor authentication as an added line of defense.
- Deploy rogue-AP detection or wireless intrusion prevention/detection systems to prevent wireless attacks.

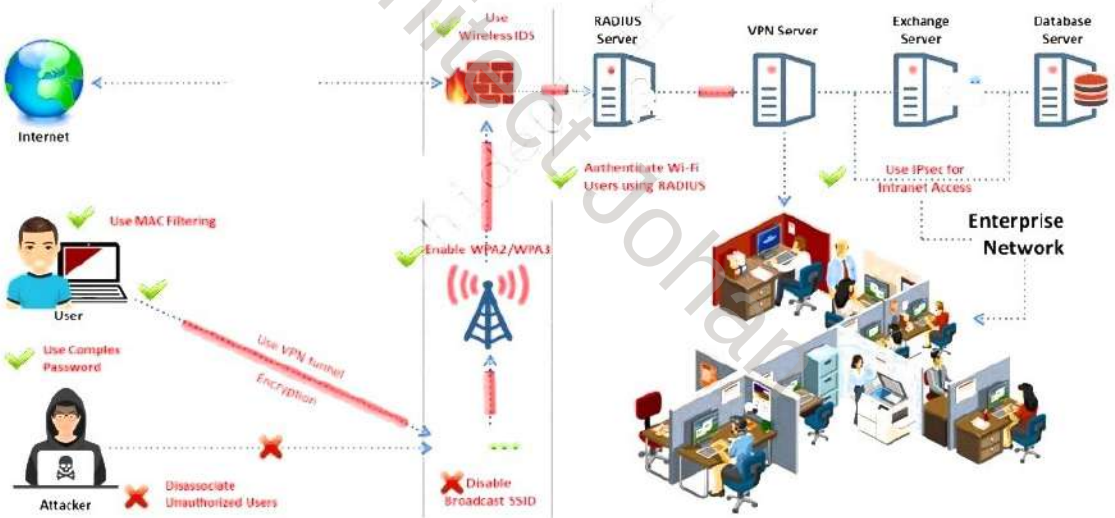


Figure 16.95: Defense against wireless attacks

Wireless Intrusion Prevention Systems

A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum to detect APs (intrusion detection) without the host's permission in nearby locations. It can also implement countermeasures automatically. WIPSs protect networks against wireless threats and provide administrators the ability to detect and prevent various network attacks.

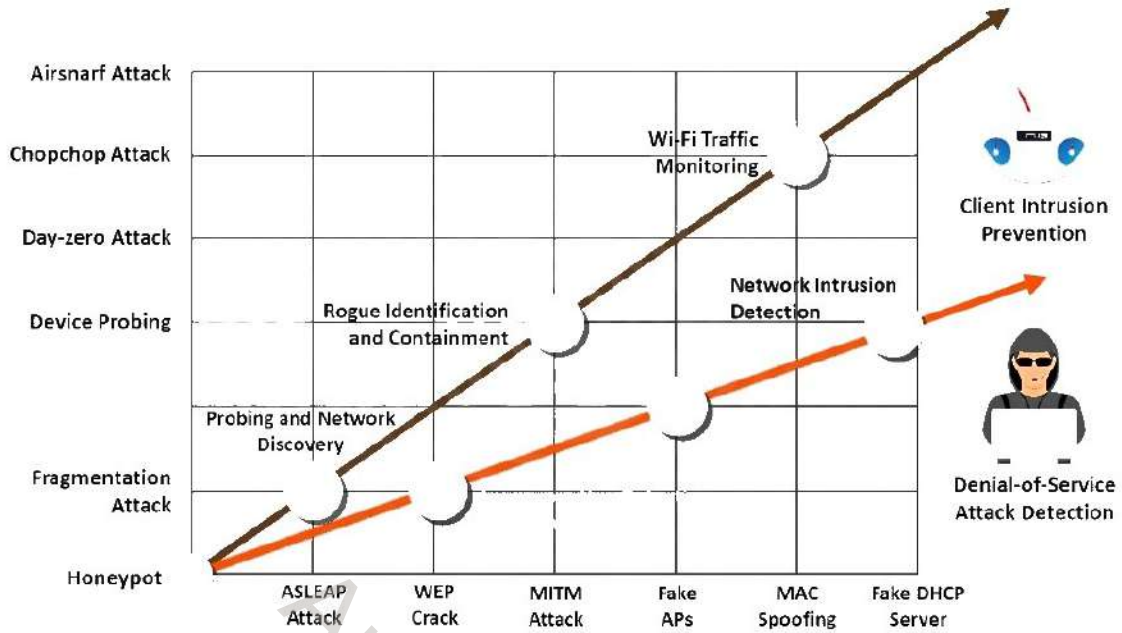


Figure 16.96: Wireless attacks and their prevention methods

WIPS Deployment

A WIPS consists of several components that work together to provide a unified security monitoring solution. Cisco's WIPS deployment includes the following component functions:

- **APs in monitor mode**: This mode provides constant channel scanning with attack detection and packet capture capabilities.
- **Mobility services engine (running a wireless IPS service)**: It is the central point of alarm aggregation from all controllers and their respective wireless IPS monitor-mode APs. Alarm information and forensic files are stored on the system for archival.
- **Local mode AP(s)**: This mode provides wireless service to clients in addition to time-sliced rogue and location scanning.
- **Wireless LAN controller(s)**: These controllers forward attack information from wireless IPS monitor-mode APs to the MSE and distributes configuration parameters to APs.
- **Wireless control system**: Provides the means to configure the wireless IPS service on the MSE, push wireless IPS configurations to the controller, and set APs in the wireless IPS monitor mode. It is also used for viewing wireless IPS alarms, forensics, reporting, and accessing the threat encyclopedia.

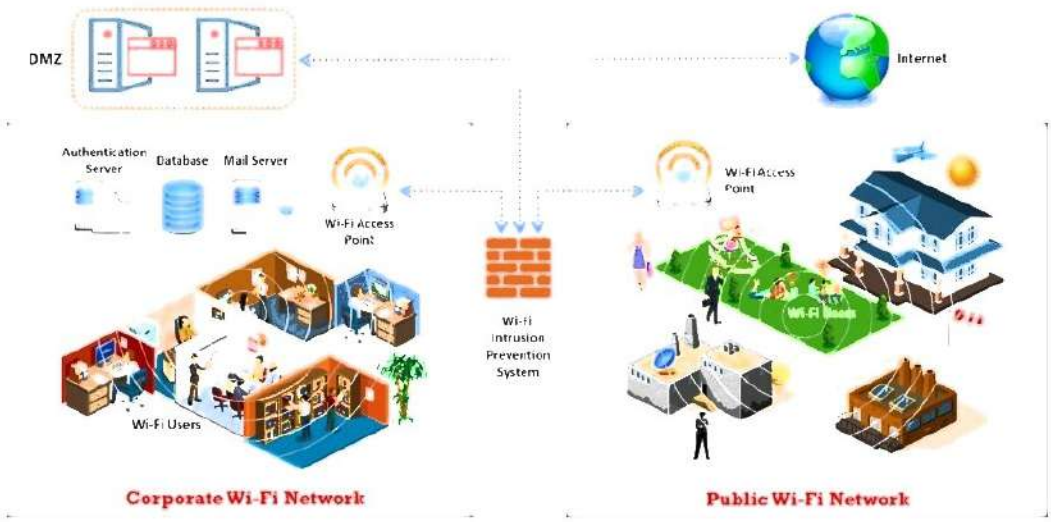
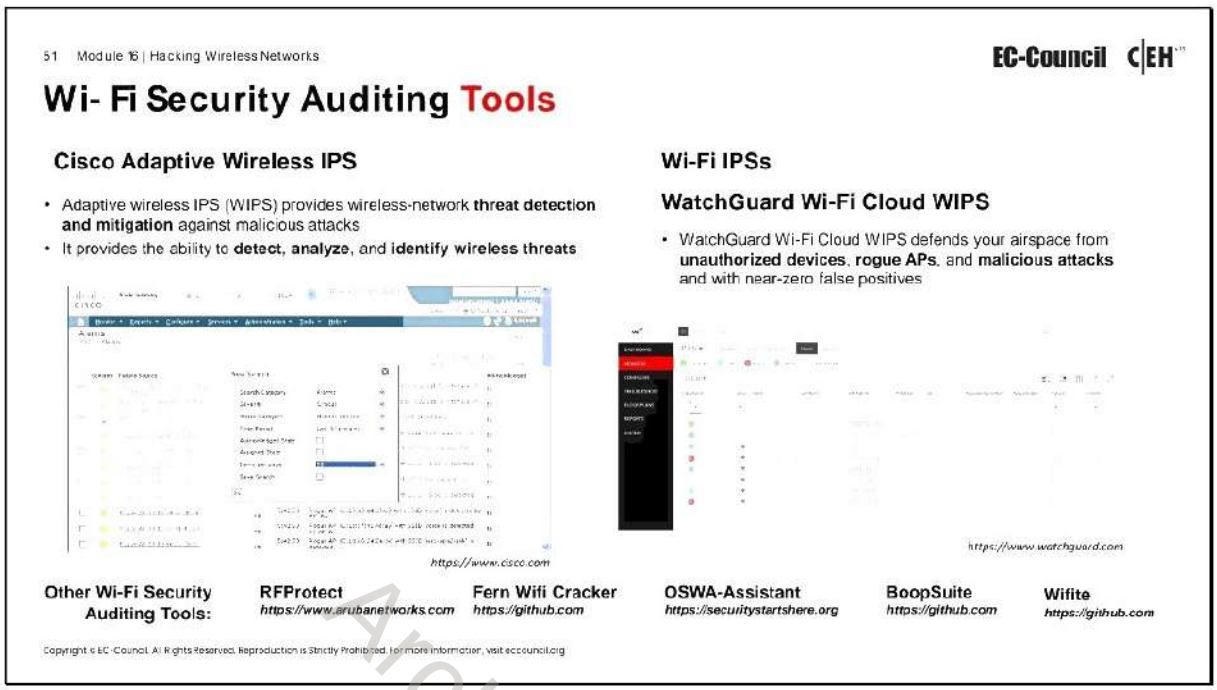


Figure 16.97: WIPS deployment



Wi-Fi Security Auditing Tools

- **Cisco Adaptive Wireless IPS**

  Source: *https://www.cisco.com*

  Cisco Adaptive Wireless Intrusion Prevention System (IPS) offers advanced network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. Fully integrated with the Cisco Unified Wireless Network, this solution delivers integrated visibility and control across the network, without the need for an overlay solution. Adaptive WIPS provides wireless-network threat detection and mitigation against malicious attacks and security vulnerabilities. It also provides security professionals with the ability to detect, analyze, and identify wireless threats.

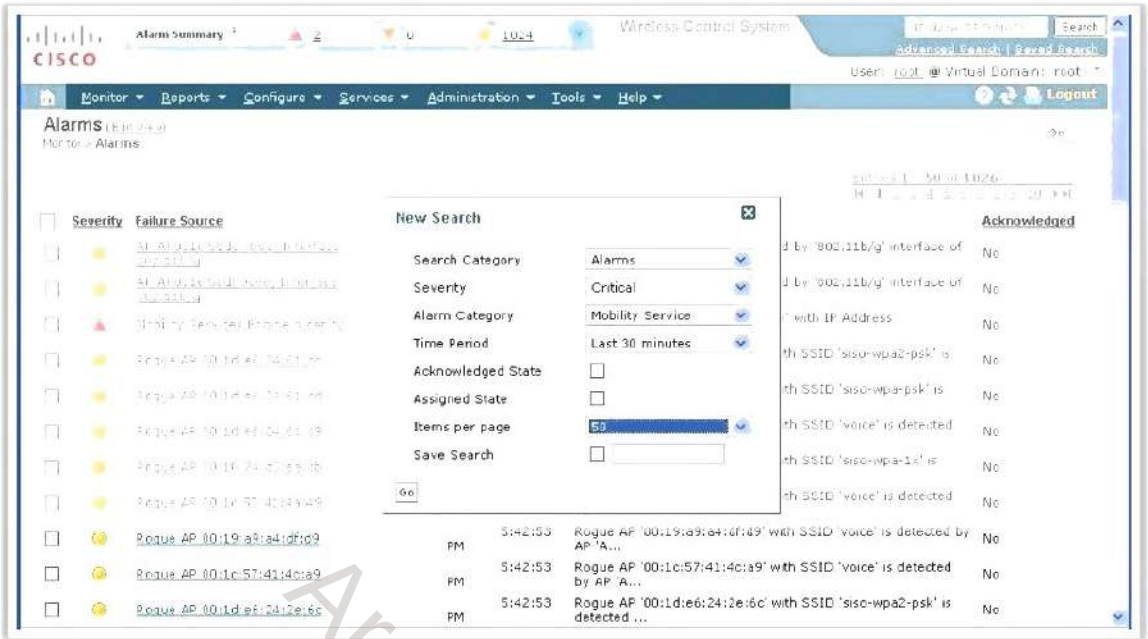


Figure 16.98: Screenshot of Cisco Adaptive Wireless IPS

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 IPSs block wireless threats by automatically scanning, detecting, and classifying unauthorized wireless access and rogue traffic to the network, thereby preventing neighboring users or skilled hackers from gaining unauthorized access to the Wi-Fi networking resources.

- **WatchGuard Wi-Fi Cloud WIPS**

  Source: *https://www.watchguard.com*

  WatchGuard Wi-Fi Cloud WIPS defends against unauthorized devices and rogue Aps, prevents evil twins, and shuts down malicious attacks such as DoS attacks with close to zero false positives while ensuring high-performance wireless connectivity.

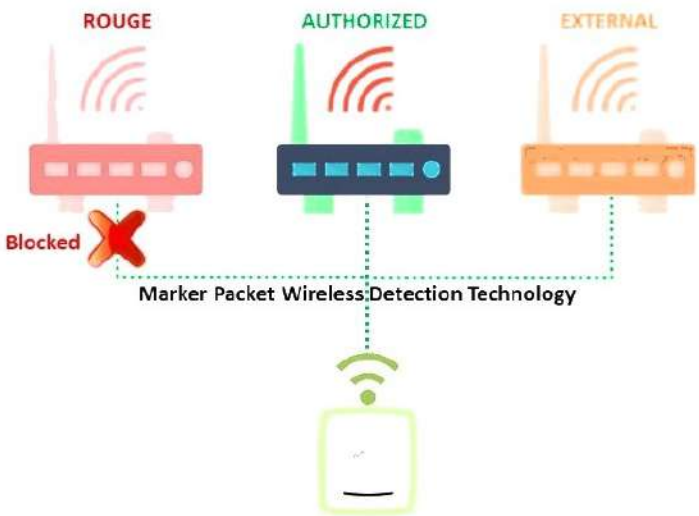


Figure 16.99: Conceptual diagram of WatchGuard WIPS

Figure 16.100: Screenshot of 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*)

Module Summary

In this module, we discussed wireless network concepts, along with different types of wireless encryption technologies. We also discussed in detail various wireless threats and the wireless hacking methodology comprising Wi-Fi discovery, wireless traffic analysis, the launch of wireless attacks, and Wi-Fi encryption cracking. This module also illustrated various wireless hacking tools. Additionally, we discussed various countermeasures to prevent wireless network hacking attempts by threat actors. Finally, this module presented a detailed discussion on how to secure wireless networks using wireless security tools.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform mobile hacking to compromise mobile devices.