CEH v12 Lesson 9 : Exploiting Wireless Vulnerabilities

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Wireless Concepts
- Exercise 2 — Wireless Prevention

After completing this module, you will have further knowledge of:

- Wireless Networks
- Wireless Standards
- Wireless Encryption
- Authentication Protocols
- Wireless Connecting Methods
- Wireless Threats
- Wireless Hacking Methodology and Tools
- Bluetooth Hacking
- Wireless Network Countermeasures
- Wireless Security Tools

Lab Duration

It will take approximately **30 minutes** to complete this lab.

Exercise 1 — Wireless Concepts

Wireless networks are everywhere now. The biggest advantage of a wireless network is that it allows user mobility. Unlike a wired network, where the user is restricted due to a cable being used, a wireless network allows the user to be mobile and connected within a certain range. For the user, it is easy to connect to the wireless network. However, many

considerations have to be thought over for an administrator while installing, managing and maintaining the wireless network.

In this exercise, you will learn various wireless networking concepts.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Wireless Networks
- Wireless Standards
- Wireless Encryption
- Authentication Protocols
- Wireless Connecting Methods
- Wireless Threats
- Wireless Hacking Methodology and Tools
- Bluetooth Hacking

Wireless Networks

Wired networks restrict the physical location of a computing device. A wireless network, on the other hand, provides the freedom to move around while still connected to a network. Most computing devices are equipped with a wireless network card proving connectivity to a wireless network.

Let's look at the advantages and disadvantages of wireless networks.

Advantages

The key advantages are:

- **Minimal wiring required**: The wireless portion of a wireless network itself does not need wiring. However, should connection to rest of the local area network or internet be required, the (WAP) wireless access point will need to be connected to those networks. That is generally accomplished using cables.

- **Mobility**: The limitations of a cable are not there anymore. A user can freely roam around and still be connected with wireless connectivity.
- **Extended connectivity**: A user can connect more devices with a wireless network. With wired networks, a user can connect one device per cable. However, with the wireless network, this limitation is removed.
- **Cost-effective**: The wireless network is cost-effective. Your investment in a cabled infrastructure is reduced.
- **Easy to Manage**: The wireless networks are easy to manage. In most cases, you set it up, and then there is nothing much to do except change the passwords periodically.

Disadvantages

The following are some of the key disadvantages:

- **Security**: In wireless networks, security can be a key concern. There can be serious security threats if it is set up with a weak encryption protocol.
- **Bandwidth:** With fewer devices, the wireless network bandwidth may suffice. However, as the number of devices increases, the bandwidth may suffer.
- **Upgrades:** The upgrades may require a change of wireless router and the network interface cards (NICs) in the devices.
- **Interference:** The wireless network can be prone to interference from other electrical appliances. If the wireless network is configured at 2.4 GHz frequency, you can expect interferences from appliances like microwaves and cordless telephones.

Wireless Standards

802.11a802.11a was the first amendment to the original 802.11 standard. It operated as the 5Ghz band with a speed at 54Mbps using Orthogonal Frequency Division Multiplexing (OFDM) modulation. It had a range of 35–120 meters. Users will only encounter this standard in an academic setting if at all.**802.11b**IEEE 802.11b provides data rates of up to 11 Mbps in the 2.4 GHz band. It utilizes the Direct Sequencing Spread Spectrum (DSSS) modulation scheme much like the original 802.11 standard. Range for this standard is 35–140 meters.**802.11g**IEEE 802.11g supports the 2.4 GHz band and provides data rates of up to 54 Mbps with a range of 170 feet. It uses OFDM modulation and is backwards compatible with the 802.11b standard.**802.11n**IEEE 802.11n supports

both the 2.4 and 5 GHZ bands. It uses multiple input/multiple output (MIMO) antennas with 40 MHz channels giving it a network speed of 600 Mbps and a maximum range of 230 feet. Much like 802.11g, this standard also uses the OFDM modulation scheme.**802.11ac**IEEE 802.11ac has wider channels (80 or 160 MHz compared to 40 MHz for 802.11n) in the 5 GHz band, more spatial streams (up to 8), and the addition of Multi-User MIMO (MU-MIMO) antennas utilizing OOFDM modulation. These upgrades allow the transmission of data up to 1.33 Gigabits at a range of 75 meters.**802.11ax**IEEE 802.11ax is the sixth generation of the Wi-Fi standard. It operates at the 2.4, 5, and 6 GHZ bands. Wi-Fi 6 technology is all about better and more efficient use of the existing radio frequency medium. It provides a more predictable performance for advanced applications such as 4K or 8K video, high-density high-definition collaboration apps, all-wireless offices, and the Internet of Things (IoT). Higher data rates and wider channels are not the goals of Wi-Fi 6.

Despite the speed and range of different wireless standards, they need to be used correctly. For example, if the wireless router or access points are not hardened, then no standard is safe for use.

Wireless Encryption

A wireless network can use different cryptographic protocols, which have evolved over the years. Even though, at one time, Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA) were popular protocols and were widely used, they are now deprecated and should not be used. WPA2 is the default cryptography protocol supported by all wireless access points. WPA3 will soon become the standard as it is resistant to all current attacks.

In this task, you will learn about the cryptographic protocols in a wireless network.

Wired Equivalency Protocol (WEP)

WEP is the original 802.11b security standard meant to provide Wireless LAN (WLAN) with security levels like that of a wired network. WEP uses a 24-bit initialization vector (IV) and 40, 104, or 232 bit keys creating 64, 127, and 256 bit WEP versions. Encryption is accomplished using RC4 with a 32-bit cyclical redundancy check (CRC-32) for integrity checking. the 24-bit IV and RC4 are very weak and therefore WEP has been deprecated and should no longer be used.

Wi-Fi Protected Access (WPA)

The IEEE 802.11i standard sought to improve the weaknesses in WEP. The draft standard first release still called for RC4 for encryption and added Temporal Key Integrity Protocol (TKIP) for added security. The CRC-32 integrity check was also upgraded with the Michael Algorithm creating the CRC-MIC check. Finally, WPA introduced IEEE 802.1X authentication with Pre-Shared Key (PSK) and enterprise operating modes.

Wi-Fi Protected Access 2 (WPA2)

The IEEE 802.11i final standard introduced WPA2 utilizing AES for encryption with Counter Cipher Block Chain Message Authentication Protocol (CCMP). CBC-MAC is the term used as the integrity check. WPA2 incorporates protection against forgery and replay attacks. While it was the default encryption for many years the Key Reinstallation Attack (KRACK) is an exploit for a significant vulnerability in WPA2 allowing attackers to decrypt transmissions. WPA2 can be implemented in two different operating modes:

- **Pre-shared key (WPA2-Personal**): A password is set in advance; therefore, it is called pre-shared mode. The wireless router generates the encryption key made of the password, SSID, and the TKIP protocol. Each encryption key generated is unique for each wireless client. As a new wireless client connects, a new key is generated. On every connection, a new unique encryption key is generated. The encryption is never static with any client.
- **Authentication server(WPA2-Enterprise**): An authentication server authenticates the client. A ciphered key is assigned to each device that needs to connect. The user cannot share the ciphered key with anyone.

Wi-Fi Protected Access III (WPA3)

WPA is the successor of WPA2. It adds several new capabilities that did not exist in WPA2. For example, it adds some of the key capabilities, such as:

- Protection from several attacks, such as de-authentication, handshake capture dictionary, PMKID Hash Dictionary, KRACK exploit, and handshake capture encrypts/decrypt.
- Uses WiFi Easy Connect instead of WiFi Protected Setup (WPS). WiFi Easy Connect uses Device Provisioning Protocol (DPP).
- Replaces Pre-Shared Key (PSK) with Simultaneous Authentication of Equals (SAE)

- Replaces AES-CCMP with AES-GCMP with the BIP-GMAC-256 integrity check.
- Blocks authentication after a certain number of failed attempts

WPA3 also uses the WPA2-Personal and WPA2-Enterprise mode.

Encryption AlgorithmAES-GCM & Elliptical Curve Cryptography of CNSA Suite B**Encryption Key**192-Bits for Enterprise, 128-bit for Personal**Integrity Check Method**Secure Hash Algorithm

Simultaneous Authentication of Equals (SAE)

If a typical wireless network does not have enterprise mode enabled, you need to provide a password to connect to it. Simultaneous Authentication of Equals or SAE adds another element to the authentication process. Along with the password, it also enforces the MAC address authentication.

At the base of it, SAE uses the Diffie-Hellman key exchange method. However, it adds an authentication requirement to authenticate the MAC address. The SAE process starts with the SAE exchange, after which the client and the wireless access point (WAP) create an encryption key that is further used to create a session key. After the session key is generated, the client can connect to the WAP.

The key advantage of SAE is that each time the session key is uniquely generated. If one key is compromised, the other sessions are not impacted.

Authentication Protocols

There are several different types of authentication protocols. However, only your requirement will help you decide which type of protocol to use. For example, you may want a certificate-based protocol to be used. If you do not have a certificate authority (CA), you can choose a protocol that does not require certificate-based authentication.

Let's look at some of the key authentication protocols.

IEEE 802.1X

IEEE 802.1X uses port-based network access control. When a device attempts to connect to the network, the protocol authenticates it and opens a virtual port on the wireless access point. However, if authentication fails, the device cannot access the network. Essentially, three components play a critical role:

- **Suppliant**: Is the device that wants to connect to the network.
- **Authenticator**: Is the wireless access point of a wireless network.
- **Authentication Server**: Is the authentication server that grants/denies access. Typically, this role is played by a RADIUS server.

When a suppliant attempts to connect to the network, the authenticator immediately sets the ports to which the suppliant is connected to the unauthenticated state. The authenticator sends a set of frames requesting authentication credentials. The suppliant provides the authentication credentials. After receiving the credentials, the authenticator sends the credentials to the authentication server, verifying the credentials and informing the authenticator. After receiving the response from the authentication server, if credentials are accepted, the authenticator sets the port status to authenticated. After the device disconnects from the network, the authenticator changes the port status to unauthenticated.

Extensible Authentication Protocol (EAP)

EAP is a framework for communicating the authentication protocol that can be used in IEEE 802.1x. Originally, EAP supported only PAP and CHAP. However, since both of these are unsecure protocols, additional protocols were added including EAP-TLS, EAP-TTLS, PEOP, LEAP and EAP-FAST. Each of these offer various levels of security with different methods to handle credentials.

Wireless Connecting Methods

A wireless network can be accessed in a variety of ways, with It being possible that a password is not required. However, a password is most likely required if the wireless network is configured correctly. In this task, you will learn about different accessing a wireless network.

Pre-shared key (PSK) vs. Enterprise vs. Open

A wireless network can be configured in different modes: PSK, enterprise, or open. When users attempt to connect to a wireless network, they are authenticated based on their user credentials. Encrypted session keys are sent from a RADIUS server to a client. To make the authentication more secure, certificates can be incorporated with a private/public key pair.

In pre-shared mode, a client and the wireless access point must exchange and negotiate a key before the communication can begin. It does not utilize a RADIUS server as communication takes place directly between the client and wireless access point. In open mode, there is no authentication, and it is unsecured. It is usually used in public wireless access points with no access to sensitive data.

Wireless Threats

The wireless networks are prone to various types of threats. Some of the common threats to a wireless network are:

- Rogue Access Points
- Ad-Hoc Networks
- Denial of Service (DoS)
- Configuration Issues
- Passive Capturing

In this task, you will learn about wireless network threats in detail.

Rogue Access Points

A Rogue Access Point is a WAP that an attacker has set up outside the corporate perimeter but with enough signal strength to be available to corporate wireless devices. The attacker sets up the SSID of the rogue access point to be the same or very similar to the SSID of the corporate network. The goal of the rogue access point is to lure unwary corporate wireless users to connect to it. The attacker can gather credentials by capturing all traffic sent through it. Sometimes, the term “Evil Twin” is associated with this type of rogue access point.

Denial of Service (DoS) Wireless access points (WAP) that provide connectivity to a wireless network can also be prone to DoS attacks. The sole purpose of the DoS attack is to bring down the WAP or any system and prevent it from serving legitimate users. In this attack, traffic is sent to the WAP in a large quantity, more than WAP can handle.**Configuration Problems**

When a wireless access point (WAP) is set up, its default configuration must be changed. However, in many cases, this does not happen. Users tend to keep the default

configuration, making the wireless network vulnerable to external attackers. For example, a user may leave the WAP with the default configuration, such as:

- Default admin password
- Default SSID
- Use of weak authentication protocol, such as WEP

Jammingn attacker uses a specialized tool with a high-gain amplifier that drowns out a legitimate WAP. This is a type of Denial of Service (DoS) attack.**MAC spoofing**An organization with a wireless network can choose to implement MAC filtering, which will allow the system to connect only if its MAC address is listed in the WAP configuration. However, an attacker can also break this security method by getting access to a safelisted MAC address and replacing it with the captured one. Now, an attacker's system has the captured MAC address. The wireless network will check for the MAC address, and since it is safelisted in its configuration, the attacker's system will connect to the wireless network.**Man-in-the-middle**A man-in-the-middle attacker allows users on the wireless network to connect to their WAP. Using another wireless connection on the same system, an attacker connects to the real WAP and allows the traffic to flow from his WAP to the real WAP, meanwhile intercepting the traffic.**De-authentication Attack**Using software like Air Jack, an attacker can force the users to disconnect from the real WAP and connect to their WAP. It is easy for an attacker to intercept the information from the connected systems.**KRACK Attack**KRACK, an attack discovered in 2016, is a replay attack that can be performed on WPA2 connections and was the reason that WPA3 was created.

Controller and Access Point Security

A WAP is the point to which the users connect. You would typically see one WAP that handles the wireless network traffic in a home or small office environment. However, in a large network, hundreds of WAPs may be installed. It is not administratively possible for these WAPs to be individually managed. Therefore, you use a wireless controller, which provides a centralized platform to manage all the available WAPs. You can monitor the WAPs in real-time.

It is critical to ensure security for WAP and the controller. Several steps must be performed to secure both the controller and the WAPs. Some of the key steps that you should perform are:

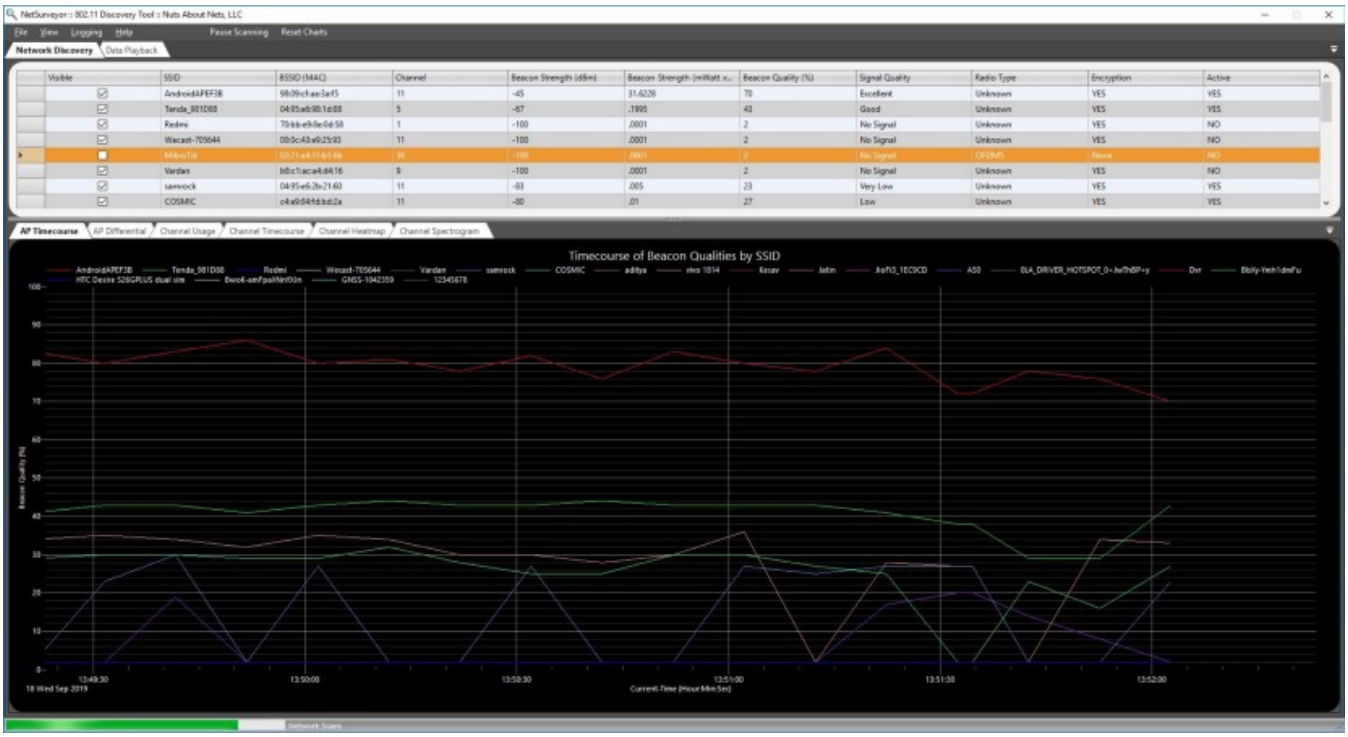
- Change the default admin passwords
- Restrict logical and physical access
- Enable encryption
- Hide the SSIDs
- Update the controller and WAPs with software patches
- Enable MAC filtering
- Enable authentication

Wireless Hacking Methodology and Tools

There are various methods that you can use to initiate wireless hacking. Some of the key ones are:

WiFi Discovery

Like a normal attack on a system or a network, the wireless network is also probed for more information using active or passive Footprinting. There are tools like NetSurveyor that can provide a lot of information about the nearby wireless network. Another tool that can be used is inSSIDer Plus.



GPS Mapping

You can use the GPS to create a list of the discovered wireless networks. This information can be shared between the hackers to explore further the opportunities to exploit them in their regions.

Some of the key tools that you can use are:

- WiGLE
- Maptitude Mapping Software
- Skyhook
- ExpertGPS
- GPS Visualizer
- Mapwel
- TrackMaster

Traffic Analysis

You can monitor and capture the wireless network traffic, which can help you with the following information:

- SSID of the wireless network
- Authentication method
- Encryption type

Such information can be crucial in planning an attack on the wireless network. Some of the important tools that can help in gathering information are:

- Wireshark
- Omnipeek Network Protocol Analyzer
- Commview for WiFi
- SteelCentral Packet Analyzer
- Kismet
- AirMagnet WiFi Analyzer PRO

- Capsa Portable Network Analyzer
- PRTG Network Monitor

Wireless Attacks

There are various types of attacks that can be conducted on a wireless network. There is no rule to use a single type of attack. The attack would depend on the information you have captured and finding a weakness or a loophole. For example, if the wireless network uses a specific WAP type, you can explore and find out if this WAP has a security vulnerability. If you are lucky, the WAP is not patched. You will have an easy time exploiting the vulnerability.

Some of the wireless attacks that you can conduct are:

- Man-in-the-Middle (MITM)
- ARP Poisoning
- MAC Spoofing
- De-authentication

Some of the key tools that you can use are:

- WPA/WPA2 Brute Forcing
- WEP Cracking
- Reaver
- Wifiphisher
- Aircrack-ng
- MANA Toolkit
- Ettercap

Bluetooth Hacking

Bluetooth comes as a handy technology for sharing data over a short-range between two mobile devices. When two mobile devices connect, it is known as pairing. However,

Bluetooth is known to be vulnerable to various types of attacks. Let's look at some of them.

- **Bluesmacking**: occurs by sending oversized ping packets to the target device, which cannot handle them, and a buffer overflow occurs.
- **Bluejacking**: is like spamming. It is about sending unwanted messages to the recipients.
- **Bluesnarfing**: is performed by exploiting Object Exchange (OBEX) to gain access to sensitive information.
- **Bluebugging**: is performed by remotely accessing a Bluetooth-enabled device.
- **BluePrinting**: is performed to collect information about the Bluetooth device, such as model and make.
- **Btlejacking**: is a Man-in-the-Middle (MITM) attack performed on Bluetooth Low Energy (BLE) devices.
- **Key Negotiation of Bluetooth (KNOB) attack**: is performed on the Bluetooth chip and exploits the weakness in the firmware, which allows the attacker to conduct a MITM attack.
- **MAC spoofing attack**: allows the attacker to spoof the MAC address of the receiver to receive the data.
- **MITM attack**: is about intercepting and manipulating the information between two Bluetooth devices.

Exercise 2 — Wireless Prevention

As you learned in the previous exercise, wireless networks are prone to different attacks. You need to use methods that can strengthen the wireless network's security. It is important to remember that no single method can prevent a wireless network. You must ensure the protection methods are customized to meet the wireless network's architecture requirements.

In this exercise, you will learn about some common methods to harden a wireless network.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Wireless Network Countermeasures
- Wireless Security Tools

Wireless Network Countermeasures

Wireless networks must be protected using various methods. It is always best to evaluate a method that meets your need and fits the wireless architecture. However, six different layers must be secured to break down the wireless security. These six layers are:

- Wireless signal
- Connection
- Device
- Data
- Network
- End-user

You need to ensure security at each level. Let's look at some of the methods for each layer.

- **Wireless Signal Security**: The wireless signals need to be continuously monitored. You can use Wireless Intrusion Detection System (WIDS) to monitor the signals continuously. With the help of WIDS, you can track issues like excessive bandwidth usage and interferences from electrical appliances or devices.
- **Connection Security**: You can use centralized encryption or per-packet authentication to prevent signal interception attacks like Man-in-the-Middle.
- **Device Security**: Each device connecting to the wireless network can have vulnerabilities. You need to scan each device for vulnerabilities and patch them. After the patches are applied, you should once again scan them for vulnerabilities
- **Data Security**: You need to use WPA2 or WPA3 to encrypt your data.
- **Network Security**: The wireless network should be configured with strong authentication. Rather than using a password, you can use certificates to

authenticate users.

- **End-user Security**: The end-user needs to protect themselves along with the data. Therefore, each device should have a firewall with appropriate rules to filter traffic.

Other than this, there are generic countermeasures that should be applied.

Encryption

The WAP will be receiving and transmitting the information to the clients. You need to ensure that the WAP, which you are using, can use encryption. If you use an outdated WAP, consider replacing it with a newer one to use encryption.

In some cases, the manufacturers do not enable the encryption and leave it to the user to configure it. In such cases, you must enable encryption to protect the information sent and received.

Security Protocol Remember to use a security protocol that can protect the wireless network. In an organization, it would be good to use WPA2 or WPA3-Enterprise.**Antivirus and Firewalls**Systems on the wireless network are no different from those on a wired network. The systems on the wireless network also need basic protection, such as an antivirus and a firewall. However, having an antivirus and a firewall does not protect the systems. You need to ensure that you regularly update the systems with the latest patches for antivirus, operating systems, and applications.**SSID Broadcasting**By default, most wireless networks are configured to broadcast their SSIDs. You should disable SSID broadcasting. This can prevent attacks, such as wardriving. Even though a hacker can still use a tool, such as NetSurveyor, to discover it, SSID will not be discovered by the systems without a tool.**Default Admin Password**

All WAPs have a default admin password used for initial login and configuration. However, you must change the default admin password and replace it with a complex password.

It is important to note that websites provide the default username and passwords for different WAP models. Anyone can go and find the username and password for a specific model.

Enable MAC Filtering Even though MAC filtering is not a complete solution to protect a wireless network from hackers, it still protects it from unwanted individuals connecting to it. With the whitelisting of MAC addresses, you can only allow specific

systems to connect to the wireless network.**Radio Transmission**You should lower the radio transmission to prevent the wireless network from being broadcasted to a large area. This can prevent attacks, such as wardriving.**Network Auditing**You must audit the wireless network regularly. In the audit, you can track rogue access points or unwanted individuals who have connected (when you don't have MAC filtering enabled).**Continuous Updates**The wireless network, devices, and endpoints should regularly be scanned for missing updates and vulnerabilities. They should be patched regularly.**Remote Login**It is always better to disable the remote login on the wireless router. In some cases, this may not be possible, but you should disable remote login if it is. You should rather use a physical Ethernet cable to connect to the wireless router for administration purposes.**Wireless Signals**You should limit the wireless signals to avoid wardriving attacks. The wireless signals should not reach outside the boundaries of your office.**Physical Security**You need to ensure that you physically secure the wireless router and access points. They should be placed securely.**Authentication**Wherever possible, you should use a centralized authentication mechanism, like RADIUS. It is always better to use two-factor authentication to secure user accounts.

Wireless Security Tools

Several tools can be used to secure a wireless network. These can be divided into several categories. Let's look at some of them.

Wireless Intrusion Prevention System (WIPS)

A WIPS monitors the wireless network traffic, and if a threat is detected, it can prevent it immediately. It usually has several capabilities like running the access points in monitor mode to detect any threats, a wireless control system to control the access points, and a mobility services engine that collects all alarms

Some key tools include:

- Cisco Adaptive Wireless IPS
- WatchGuard WIPS
- Extreme Defense
- SonicWall SonicPoint N2
- SonicPoint Wireless Security Access Point Series

- Network Box IDP

Wireless Network Security Auditing Tools

It is always better to audit the wireless network security regularly. Several tools can be used for this purpose.

Some key tools include:

- Cisco Adaptive Wireless IPS
- AirMagnet WiFi Analyzer PRO
- BoopSuite
- Fern WiFi Cracker
- RFProtect
- OSWA-Assistant

Wireless Predictive Planning Tools

Wireless Predictive Planning tools help you manage your wireless network right from planning, maintaining, and troubleshooting them.

Some key tools include:

- AirMagnet Planner
- Cisco Prime Infrastructure
- Ekahau Pro
- Tamo Graph
- NetSpot
- AirTight Planner

Wireless Vulnerability Scanning Tools

Wireless Vulnerability Scanning tools are used for locating vulnerabilities in a wireless network.

Some key tools include:

- Zenmap
- Network Security Toolkit
- Nessus Pro
- Nexpose
- Penetrator Vulnerability Scanner
- SILICA