
EC-Council
C|EH
Module 16
Hacking Wireless Networks

Learning Objectives

01 Summarize Wireless Concepts

02 Explain Different Wireless Encryption Algorithms

03 Explain Different Wireless Threats

04 Demonstrate Wireless Hacking Methodology

05 Explain Wireless Attack Countermeasures

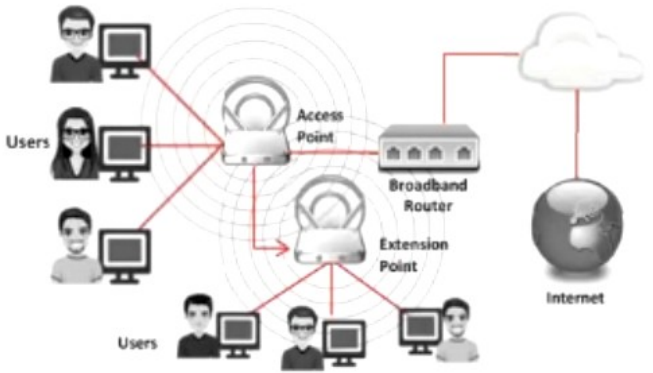
Objective 01

Summarize Wireless Concepts

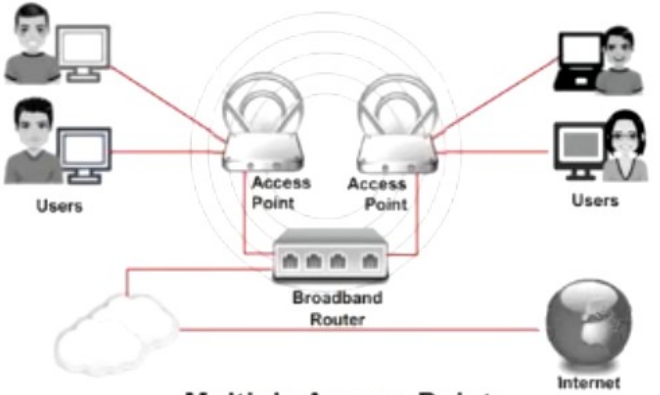
Wireless Networks

- Wireless network (Wi-Fi) refers to WLANs based on **IEEE 802.11standard**, which allows a device to access the network from anywhere within an **AP range**
- Devices, such as a personal computer, video-game console, and smartphone, use Wi-Fi to connect to a **network resource**, such as the Internet, via a **wireless network AP**

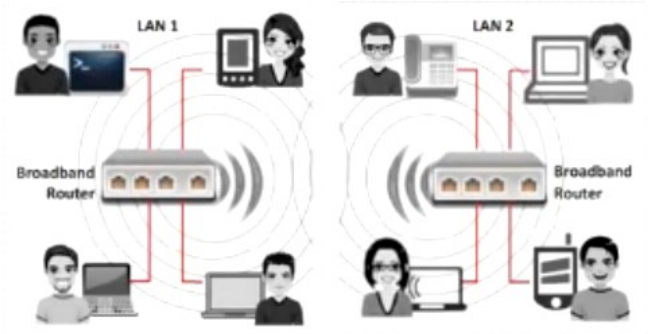
Types of Wireless Networks



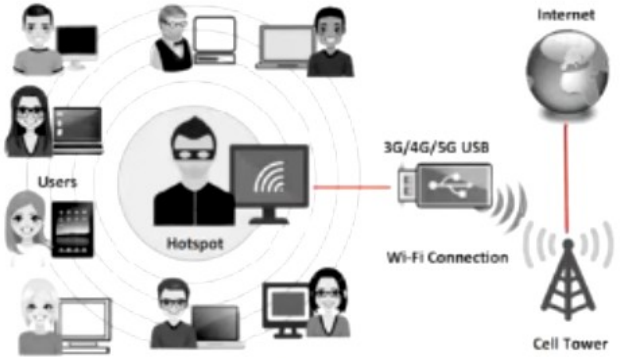
Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network



3G/4G/5G Hotspot

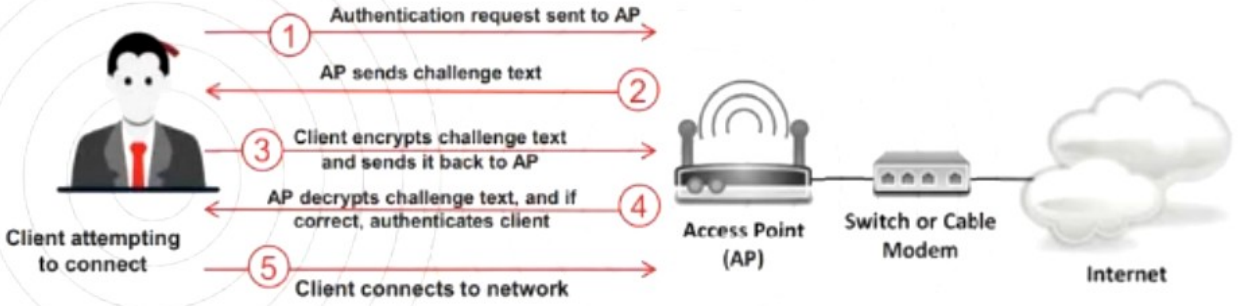
Wireless Standards

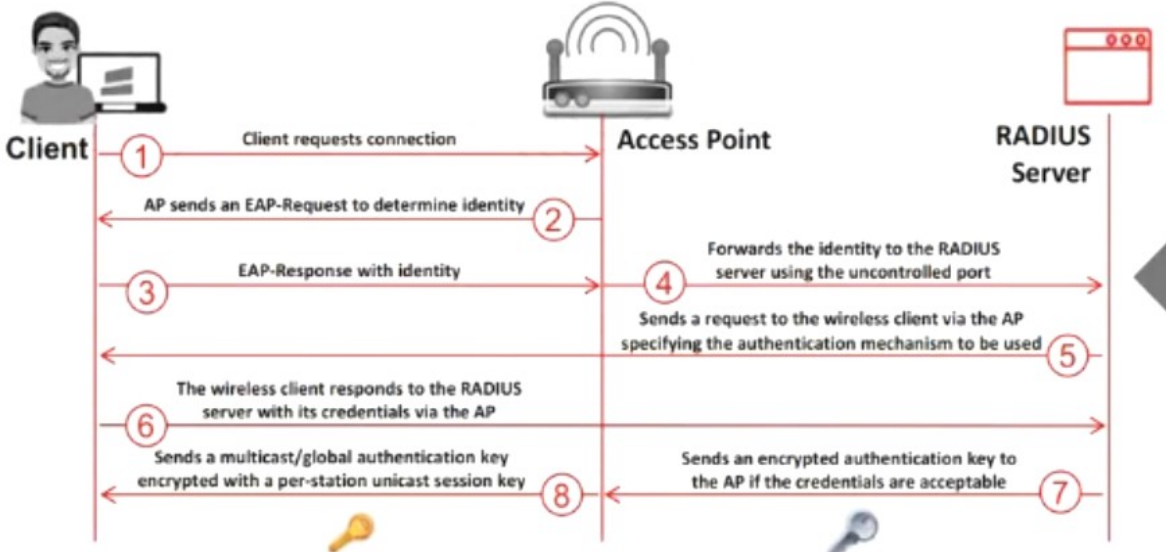
Amendments	Frequency (GHz)	Modulation	Speed (Mbps)	Range (Meters)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20 – 100
802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35 – 100
	3.7			5000
802.11ax	2.4 to 5	1024-QAM	2400	240
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140
802.11be	2.4, 5, 6	QAM	3000	120
802.11d	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			
802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
802.11i	A standard for wireless local area networks (WLANs) that provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	MIMO-OFDM	54 – 600	70 – 250
802.15.1 (Bluetooth)	2.4	GFSK, π/4-DPSK, 8DPSK	25 – 50	10 – 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1 – 100
802.16 (WiMAX)	2 – 11	SOFDMA	34 – 1000	1609.34 - 9656.06 (1-6 miles)

Wi-Fi Authentication Process

Pre-Shared Key (PSK) Mode

- Pre-Shared Key (PSK) Wi-Fi authentication mode, also known as WPA-PSK or WPA2-PSK, is a method used to secure wireless networks where a **single, shared password is used for authentication**





Centralized Authentication Mode

- A centralized authentication server known as the remote authentication dial-in user service (**RADIUS**) sends authentication keys to both the AP and client that require authentication with the AP
- Each user is assigned **unique credentials**, providing enhanced security by **independently verifying** each user's access

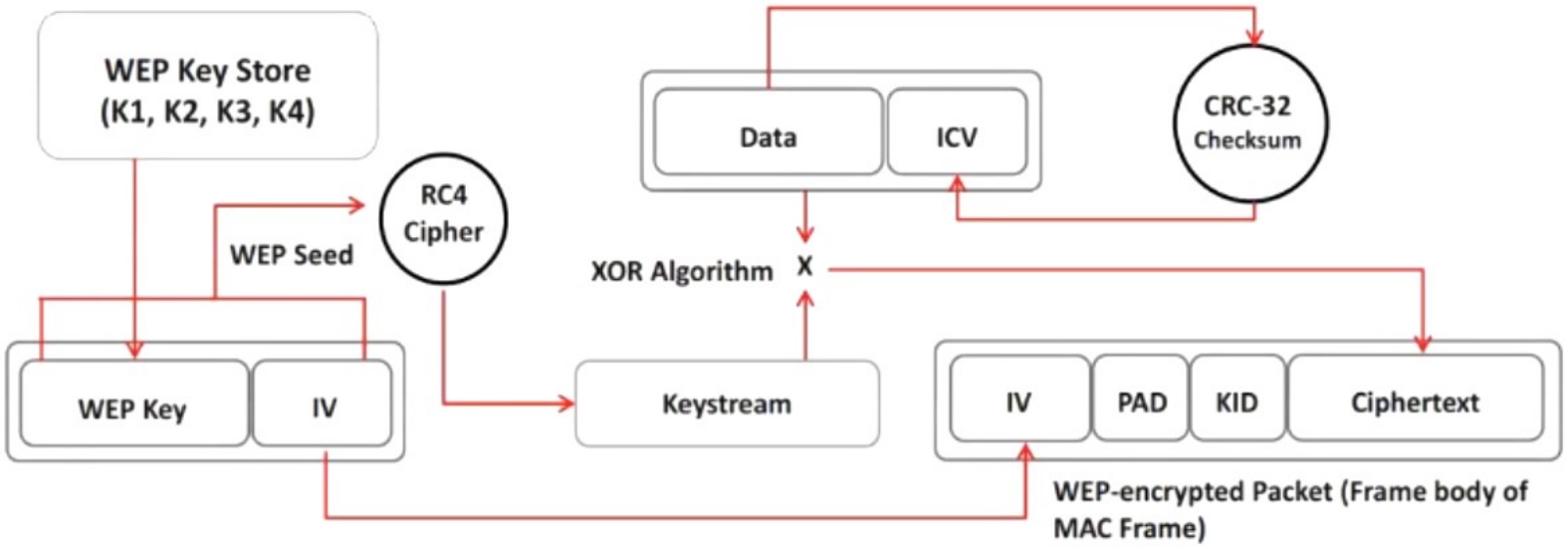
Objective 02

Explain Different Wireless Encryption Algorithms

Wireless Encryption: Wired Equivalent Privacy (WEP)

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

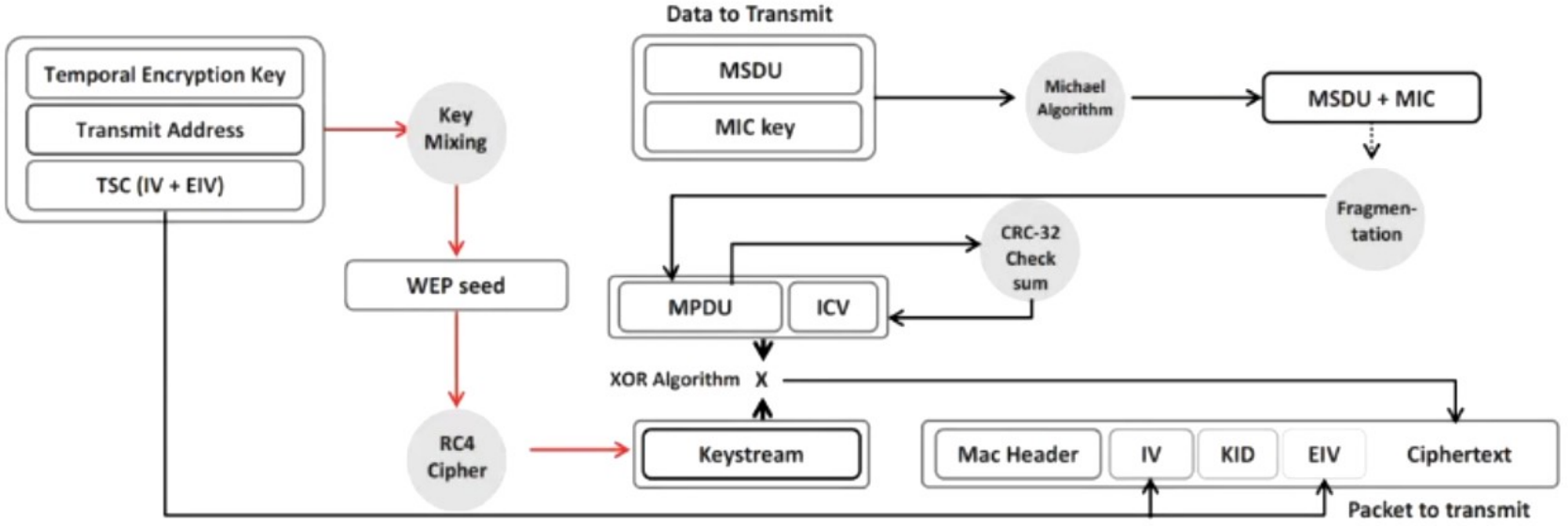
How WEP Works



Wireless Encryption: Wi-Fi Protected Access (WPA)

- WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes **the RC4 stream cipher encryption** with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication
- WPA uses TKIP to eliminate the weaknesses of WEP by including **per-packet mixing functions**, **message integrity checks**, **extended initialization vectors**, and **re-keying mechanisms**

How WPA Works



Wireless Encryption: WPA2

- WPA2 is an **upgrade to WPA**, and it includes mandatory support for counter mode with cipher block chaining message authentication code protocol (**CCMP**), **an AES-based encryption mode** with strong security

Modes of Operation

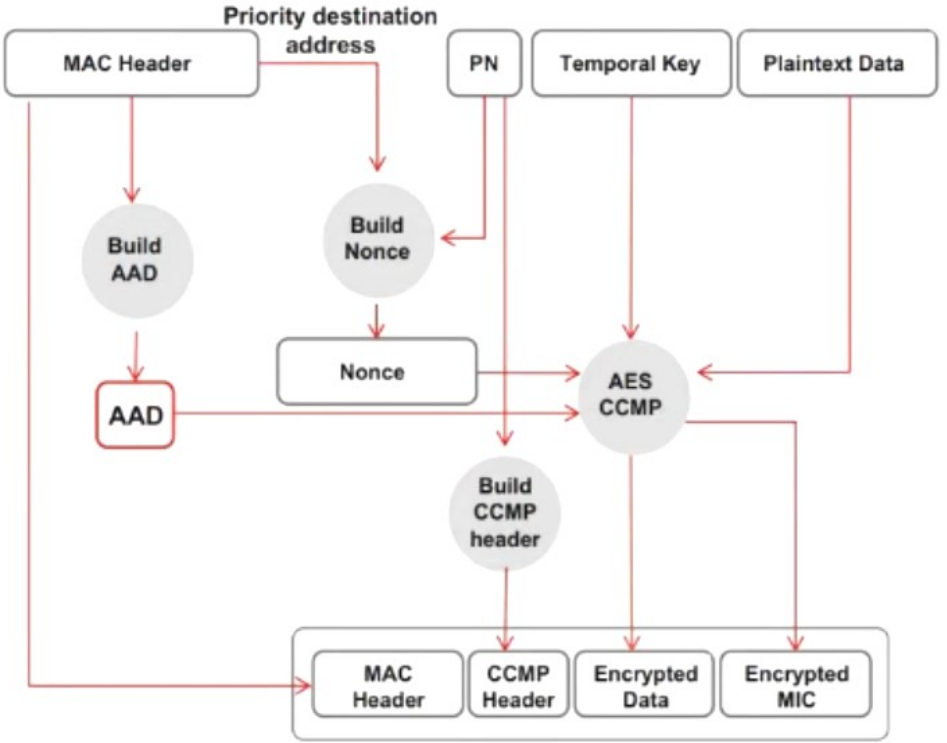
WPA2-Personal

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

WPA2-Enterprise

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

How WPA2 Works



WPA2 MAC Frame

Wireless Encryption: WPA3

- WPA3 is an advanced implementation of WPA2 providing trailblazing protocols and uses the **AES-GCMP 256** encryption algorithm

Modes of Operation

WPA3 - Personal

- It is mainly used to deliver **password-based authentication** using the SAE protocol, also known as Dragonfly Key Exchange
- It is resistant to offline dictionary attacks and key recovery attacks

WPA3 - Enterprise

- It **protects sensitive data** using many cryptographic algorithms
- It provides authenticated encryption using GCMP-256
- It uses HMAC-SHA-384 to generate cryptographic keys
- It uses ECDSA-384 for exchanging keys

Comparison of WEP, WPA, WPA2, and WPA3

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

WEP, WPA	X	Should be replaced with more secure WPA2 and WPA3
WPA2	✓	Incorporates protection against forgery and replay attacks
WPA3	✓	Provides enhanced password protection and secured IoT connections; encompasses stronger encryption techniques

Issues with WEP, WPA, WPA2, and WPA3

Issues with WEP

- CRC-32 does not ensure complete cryptographic integrity
- IVs are 24 bits and sent in cleartext
- Vulnerable to **known plaintext attacks**
- Prone to **password cracking attacks**
- Associate/disassociate messages are not authenticated
- One can easily construct a decryption table of reconstructed key streams
- Lack of centralized key management
- IV is a part of the RC4 encryption key, which leads to an **analytical attack**

Issues with WPA

- Pre-shared key is vulnerable to **eavesdropping** and dictionary attacks
- Lack of forward secrecy
- WPA-TKIP is vulnerable to **packet spoofing** and decryption attacks
- Insecure random number generator (RNG) in WPA allows the **discover of GTK** generated by AP
- Vulnerabilities in TKIP allow attackers to guess the IP address of the subnet

Issues with WPA2

- Pre-shared key is vulnerable to eavesdropping and **dictionary attacks**
- Lack of forward secrecy
- Hole96 vulnerability makes WPA2 vulnerable to **MITM and DoS attacks**
- Insecure random number generator (RNG) in WPA2 allow attackers to **discover GTK** generated by AP
- **KRACK vulnerabilities** make WPA2 vulnerable to packet sniffing, connection hijacking, malware injection, and decryption attacks

Issues with WPA3

- WPA3 uses more complex **encryption algorithms**, which can demand more **processing power** from devices
- Simultaneous **Authentication of Equals (SAE)** vulnerable to **timing attacks**
- Vulnerable to **cache-based side-channel** attacks, exposing sensitive information from **cache access patterns**
- Errors in configuration such as **weak passwords** and **poor network setup**, can leave networks vulnerable to intrusion, despite the advanced protections offered by **WPA3**

Objective 03

Explain Different Wireless Threats

Wireless Threats

Access Control Attacks

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

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

Integrity Attacks

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

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

Confidentiality Attacks

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

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

Wireless Threats (Cont'd)

Availability Attacks

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

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

Authentication Attacks

- The objective of authentication attacks is to **steal the identity of Wi-Fi clients**, their personal information, login credentials, etc. to gain unauthorized access to network resources

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

Objective 04

Demonstrate Wireless Hacking Methodology

Wireless Hacking Methodology

- The objective of the wireless hacking methodology is to **compromise a Wi-Fi network** to gain unauthorized access to network resources

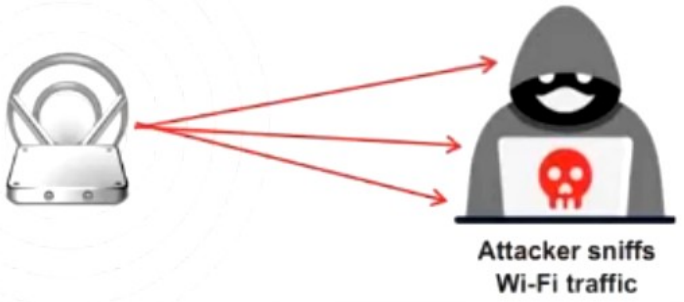
1. **Wi-Fi Discovery**
2. **Wireless Traffic Analysis**
3. **Launch of Wireless Attacks**
4. **Wi-Fi Encryption Cracking**
5. **Compromise the Wi-Fi Network**

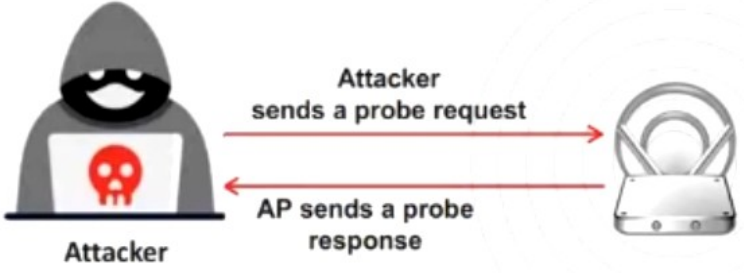
Wi-Fi Discovery: Wireless Network Footprinting

- Attacking a wireless network begins with **discovering** and **footprinting** the wireless network actively or passively

Passive Footprinting Method

An attacker can passively **detect the existence of an AP** by sniffing the packets from the airwaves, which will reveal the AP, SSID, and attacker's wireless devices that are live



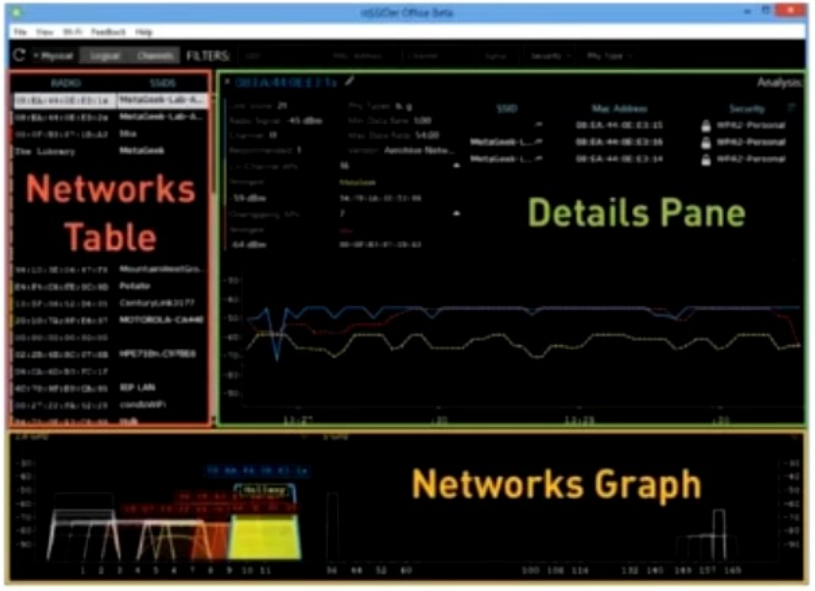


Active Footprinting Method

In this method, an attacker's wireless device **sends out a probe request with the SSID** to see if an AP responds; if the wireless device does not have the SSID at the beginning, it will send the probe request with an empty SSID

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

- The first task an attacker will go through when searching for Wi-Fi targets is **checking the potential networks** that are in range to find the best one to attack
- Drive around with Wi-Fi enabled laptop installed with a wireless discovery tool such as **inSSIDer** and map out active wireless networks



https://www.metageek.com

https://nutsaboutnets.com

Other Wi-Fi Discovery Tools:

Wi-Fi Scanner	Acrylic WiFi Heatmaps	WirelessMon	Ekahau Wi-Fi Heatmaps
https://lizardsystems.com	*https://www.acrylicwifi.com*	*https://www.passmark.com*	*https://www.ekahau.com*

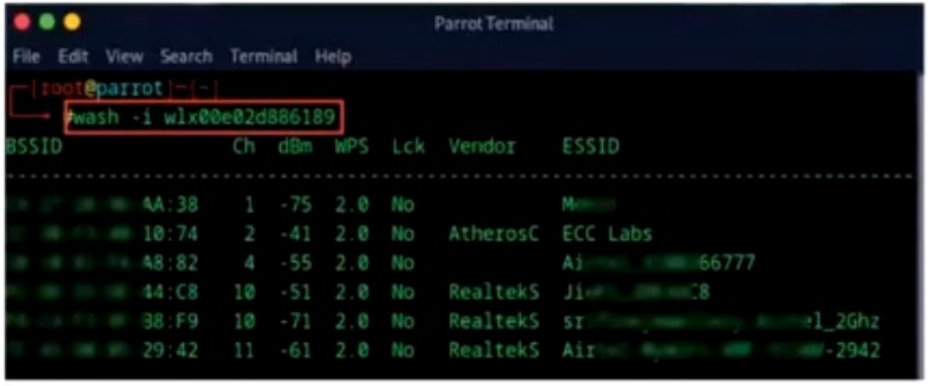
Wi-Fi Discovery: Finding WPS-Enabled APs

- Attackers use **Wash utility** to identify the WPS-enabled APs and detect if the AP is in locked or unlocked state

- Most of the WPSs in the routers usually lock when brute-forced for more than five times and can be unlocked only in the administrator interface of the router manually

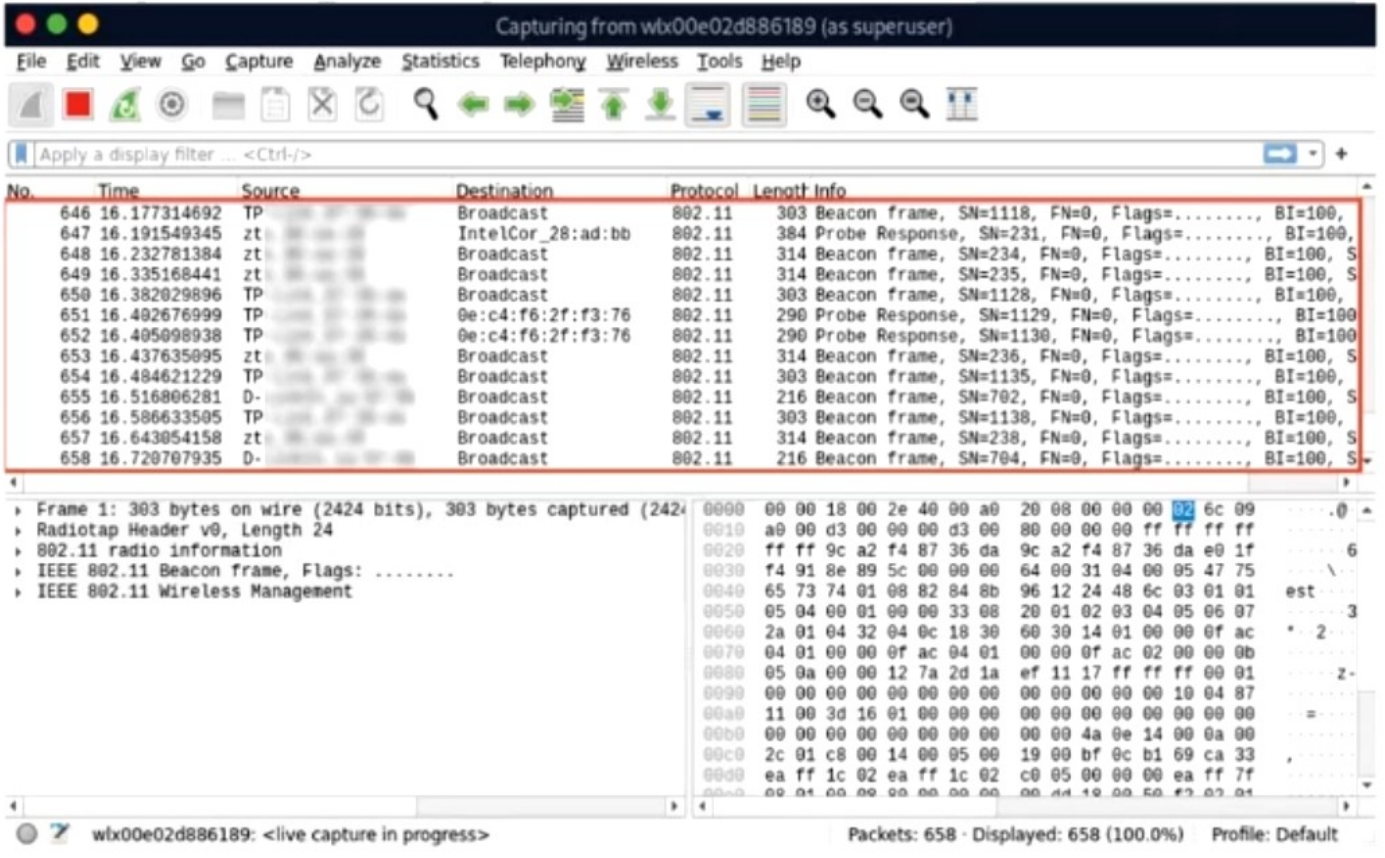
- The Wash command can support the 5 GHz channel

- The attacker **discovers the AP**, **ESSID**, and **BSSID of a device or router** using the following wash command
  - **# sudo wash -i wlan0**



Wireless Traffic Analysis

- Wireless traffic analysis enables attackers to **identify vulnerabilities** and susceptible victims in a target wireless network
- Attackers analyze a wireless network to **determine the broadcast SSID**, presence of multiple access points, possibility of recovering SSIDs, authentication method used, WLAN encryption algorithms, etc.
- Attackers use **Wi-Fi packet analyzer tools**, such as AirMagnet™ G3 Pro, Wireshark, OmniPeek, and CommView for Wi-Fi, to capture and analyze the traffic of a target wireless network



https://www.wireshark.org

Choosing the Optimal Wi-Fi Card

- Selecting the ideal Wi-Fi card for Wi-Fi hacking requires **choosing hardware that supports essential features** for Wi-Fi hacking
- **Choosing the optimal Wi-Fi card** is very important for an attacker as certain tools, such as Aircrack-ng and KisMAC, only work with selected wireless chipsets

Factors to consider when choosing the optimal Wi-Fi card:

1. **Determine the Wi-Fi requirements**
2. **Learn the capabilities of a wireless card**
3. **Determine the chipset of the Wi-Fi card**
4. **Verify the chipset capabilities**
5. **Determine the drivers and patches required**

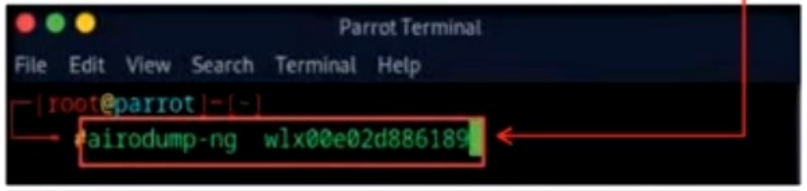
Launch of Wireless Attacks: Aircrack-ng Suite

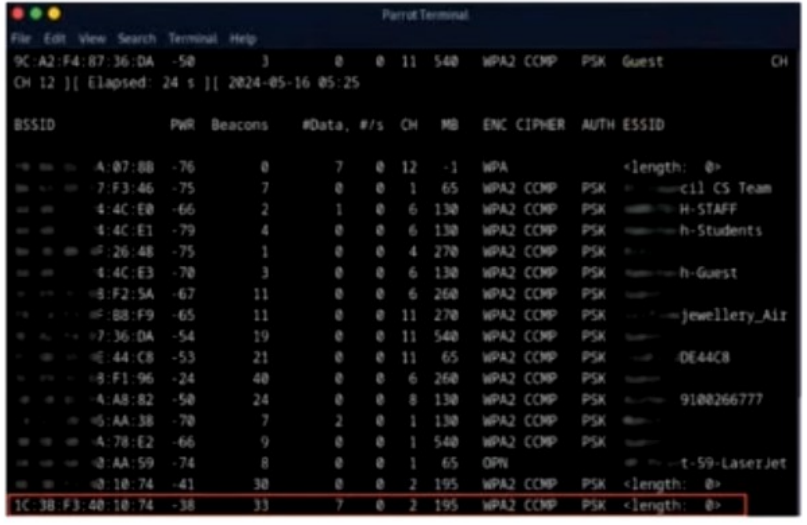
- Aircrack-ng is a **network software suite** consisting of a detector, packet sniffer, WPA PSK (WPA 1 and 2) cracker, and an analysis tool for 802.11 wireless networks; the program runs in Linux and Windows

Airbase-ng	Captures WPA/WPA2 handshake and can act as an ad-hoc AP	**Aireplay-ng**	Effective for gathering WEP IVs and WPA handshakes
Aircrack-ng	De facto WEP and WPA/WPA2-PSK cracking tool	**Airmon-ng**	Used to enable monitor mode on wireless interfaces from managed mode and vice versa
Airdecap-ng	Decrypts WEP/WPA/WPA2 and can be used to strip the wireless headers from Wi-Fi packets	**Airodump-ng**	Used to capture packets of raw 802.11 frames and collect WEP IVs
Airdrop-ng	Used for targeted, rule-based de-authentication of users	**Airolib-ng**	Stores and manages ESSID and password lists used in WPA/WPA2 cracking

https://www.aircrack-ng.org

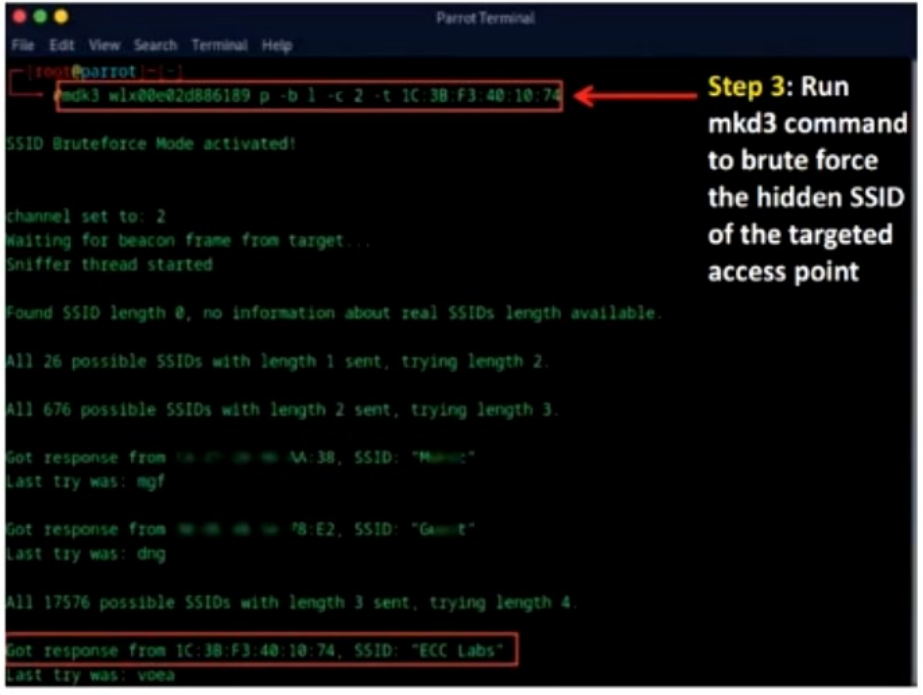
Launch of Wireless Attacks: Detection of Hidden SSIDs





Step 1: Run airmon-ng in monitor mode

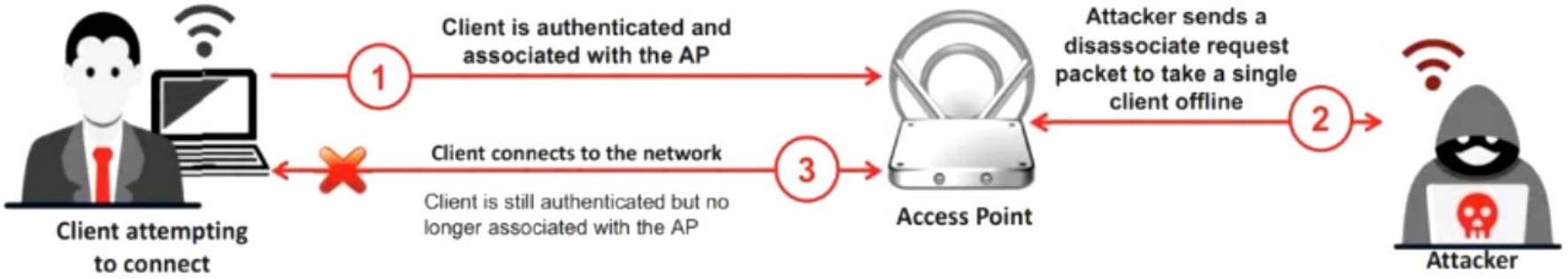
Step 2: Start airodump-ng to discover SSIDs on interface



Step 3: Run mkd3 command to brute force the hidden SSID of the targeted access point

Launch of Wireless Attacks: Denial-of-Service

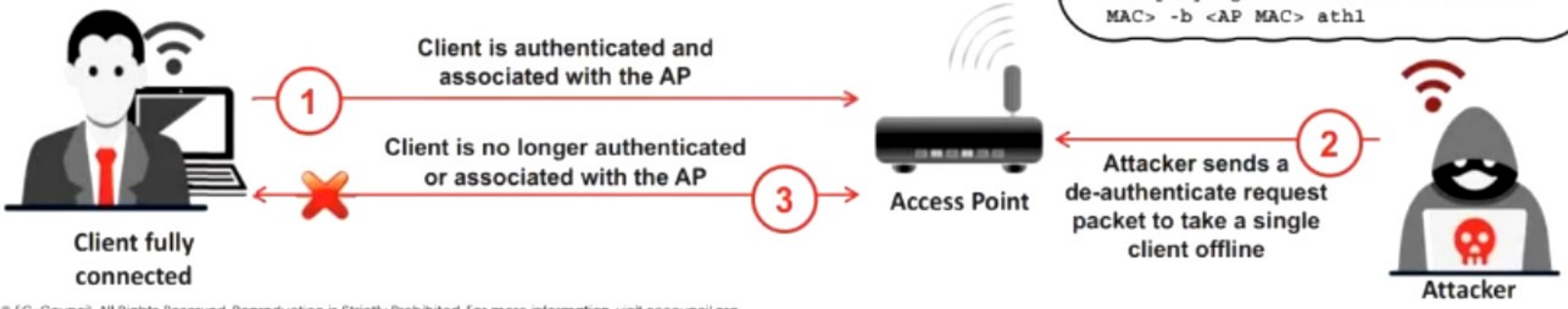
Disassociation Attack



De-authentication Attack

Deauth command:

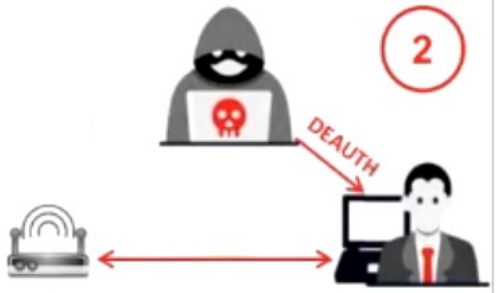
```
aireplay-ng --deauth 25 -h <TARGET MAC> -b <AP MAC> ath1
```



Launch of Wireless Attacks: Man-in-the-Middle Attack

Attacker sniffs the victim's **wireless parameters** (the MAC address, ESSID/BSSID, number of channels)

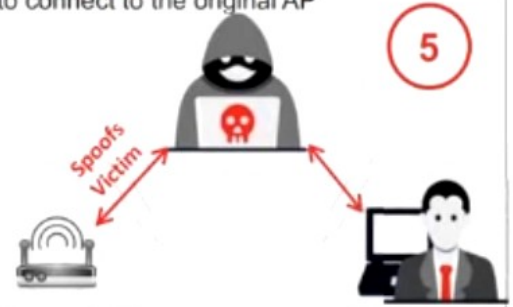
Sends a **deauthentication (deauth) request** to the victim with the spoofed source address of the victim's AP



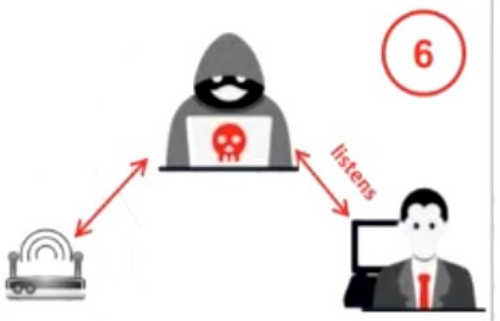
Victim is deauthenticated and starts to search all channels for a new valid AP

Attacker sets a **forged AP** on a new channel with the **original MAC address** (BSSID) and ESSID of the victim's AP

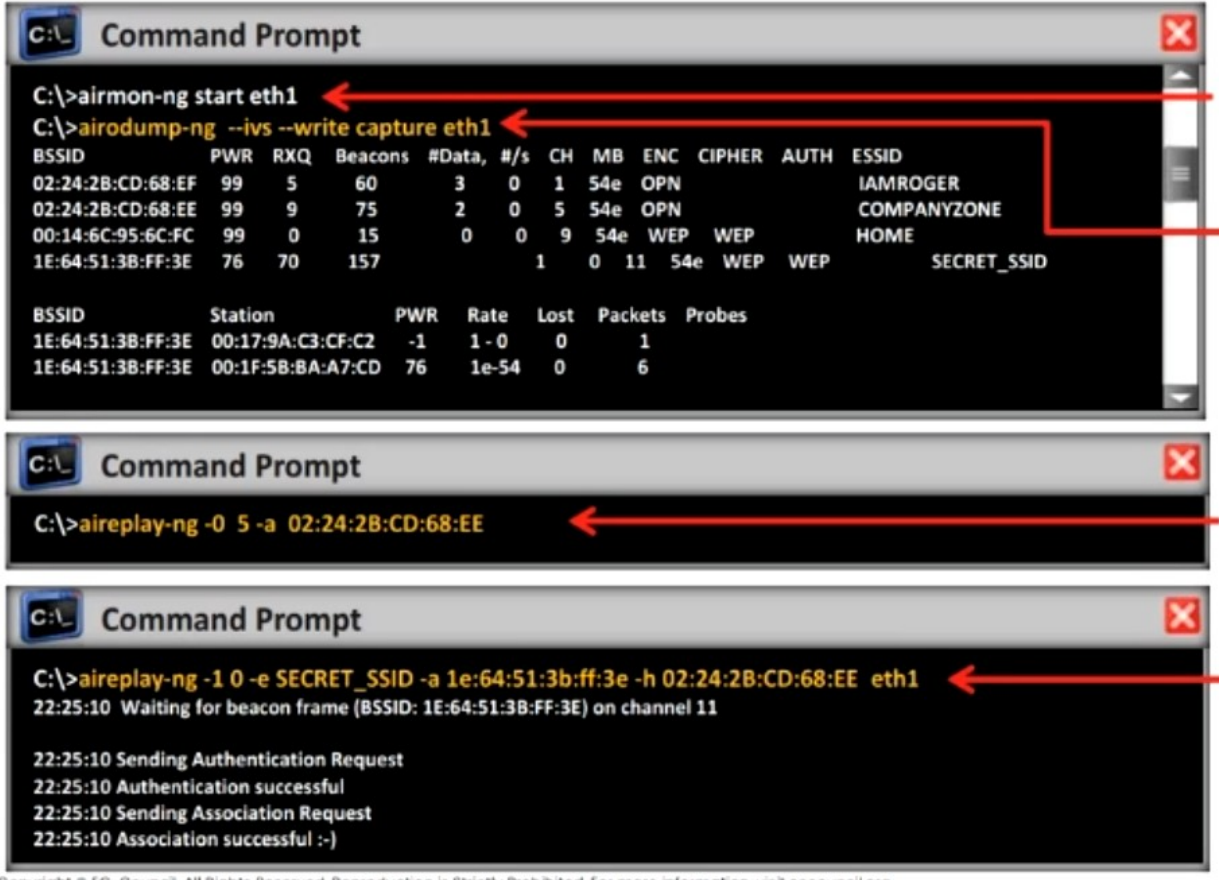
After the victim's successful association to the forged AP, the attacker **spoofs victim** to connect to the original AP



Attacker sits in between the AP and the victim and **listens** to all the traffic



Launch of Wireless Attacks: MITM Attack Using Aircrack-ng



Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on interface

Step 3: De-authenticate the client using Aireplay-ng

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

Launch of Wireless Attacks: MAC Spoofing Attack

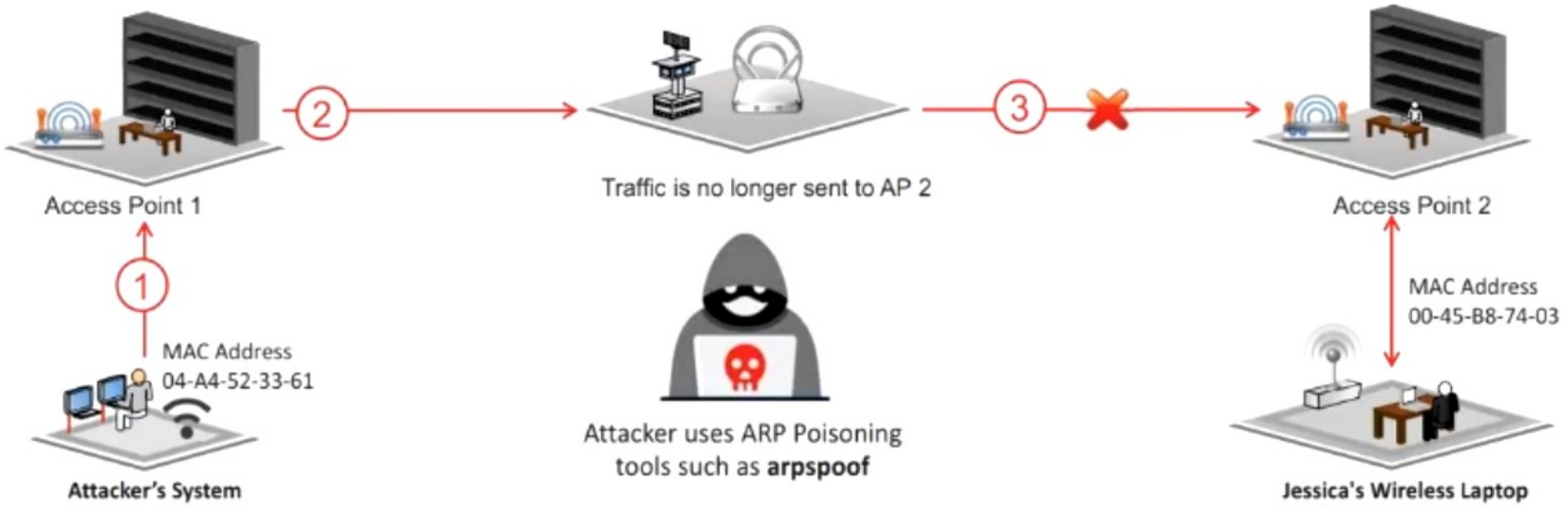
- In Media Access Control (MAC) spoofing, attackers **change the MAC address** to that of an authenticated user to bypass the MAC filtering configured in an AP
- To spoof a MAC address, the attacker needs to set the value returned from ifconfig to **another hex value** in the format of aa:bb:cc:dd:ee:ff
- Attackers use MAC spoofing tools, such as **Technitium MAC Address Changer** and LizardSystems Change MAC Address tool, to change the MAC address

Technitium MAC Address Changer

Technitium MAC Address Changer allows you to change (spoof) the **MAC Address** of your **Network Interface Card** (NIC) instantly

https://technitium.com

Launch of Wireless Attacks: Wireless ARP Poisoning Attack



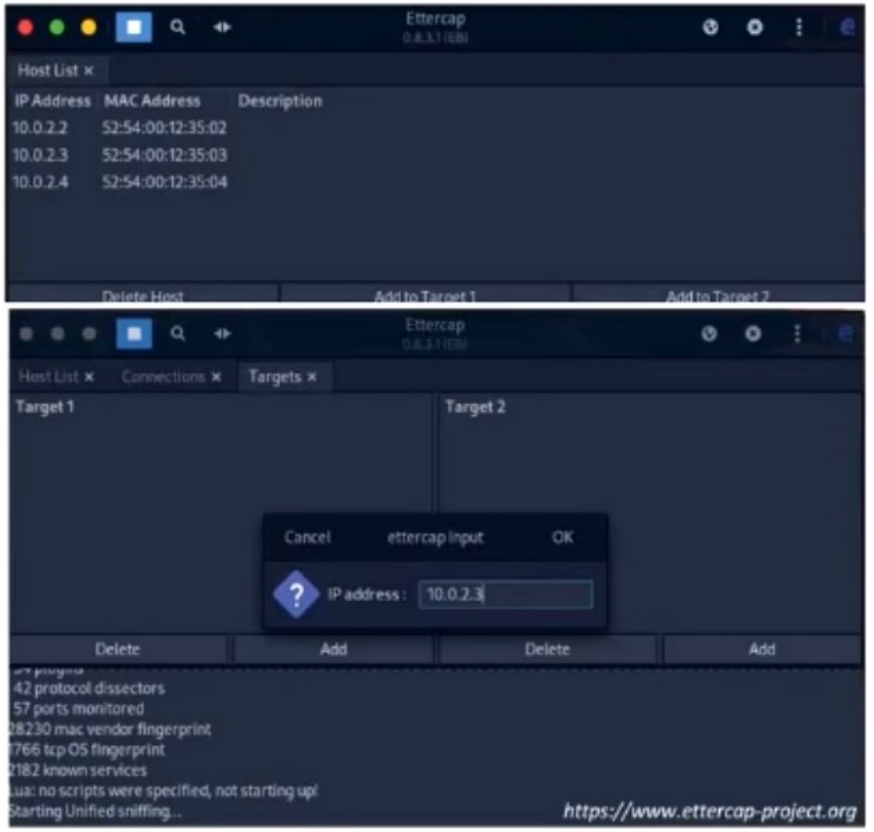
1. Attacker **spoofs the MAC** address of Jessica's wireless laptop and attempts to authenticate to AP1

2. AP1 sends **updated MAC address** info to the network routers and switches, which in turn **update** their routing and switching tables

3. Traffic now **destined** from the network backbone to Jessica's system is no longer sent to AP2

ARP Poisoning Attack Using Ettercap

- Launch Ettercap and enable the unified sniffing option by selecting **Sniff → Unified Sniffing** from the menu bar
- In the Ettercap **Setup** pop-up window, set the **Primary interface** to sniff and then click **OK**
- Select **Hosts → Scan for Hosts**. Ettercap performs a scan of all the live hosts in the network and displays the host list
- Select **Hosts → Hosts List** to view all the hosts discovered on the local network
- Select **View → Connections** to start snooping on the identified connections
- Go to the **Hosts** window and select the target IP address. Then, select **Targets → Current targets** to add a list of target hosts
- Navigate to the **MITM** menu and select **MITM → ARP poisoning**. A pop-up window appears. Select the **Sniff remote connections** option and click **OK** to launch an ARP poisoning attack



Launch of Wireless Attacks: Rogue APs

A rogue AP **provides backdoor access** to the target wireless network

Scenarios for Rogue AP Installation and Setup

- A **compact**, **pocket-sized rogue AP** device plugged into an Ethernet port of a corporate network
- A **rogue AP device** connected to corporate networks over a Wi-Fi link
- A **USB-based rogue AP** device plugged into a corporate machine
- A **software-based rogue AP** running on a corporate Windows machine

Steps to Deploy a Rogue AP

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

Creation of a Rogue AP Using MANA Toolkit

Step 1 Modify the **hostapd-mana.conf** MANA's configuration file using any text editor to setup a fake AP

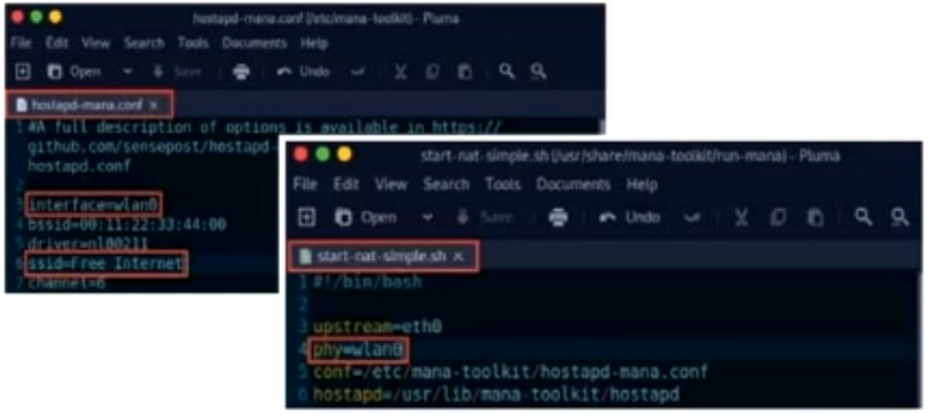
Step 2 Modify the **start-nat-simple.sh** script used to launch the rogue AP

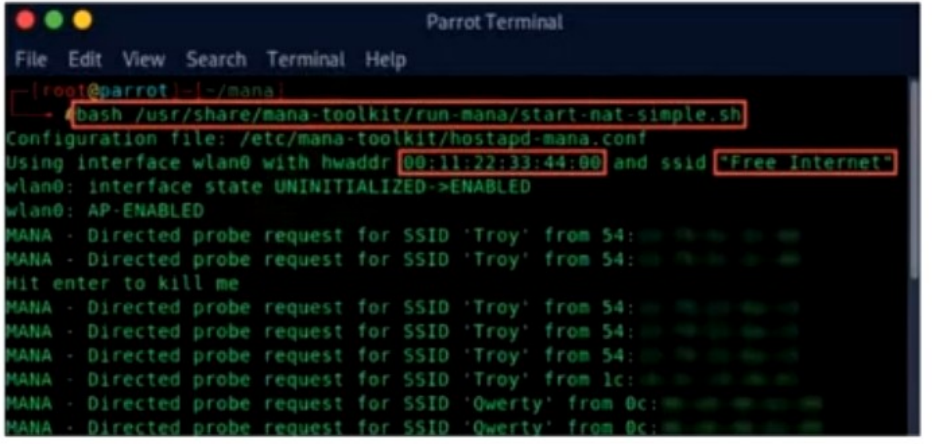
Step 3 Execute the script file **start-nat-simple.sh** using the bash command

Step 4 After the rogue AP is up, use a Windows machine or mobile device (having a different wireless card) to connect to the rogue AP

Step 5 In the Wi-Fi enabled device, search for the Internet connection that is not password-protected and connect to it

Step 6 All the data packets from your machine flow through the rogue AP; now, you can use tools, such as **tcpdump** and Wireshark, to capture and analyze the packets





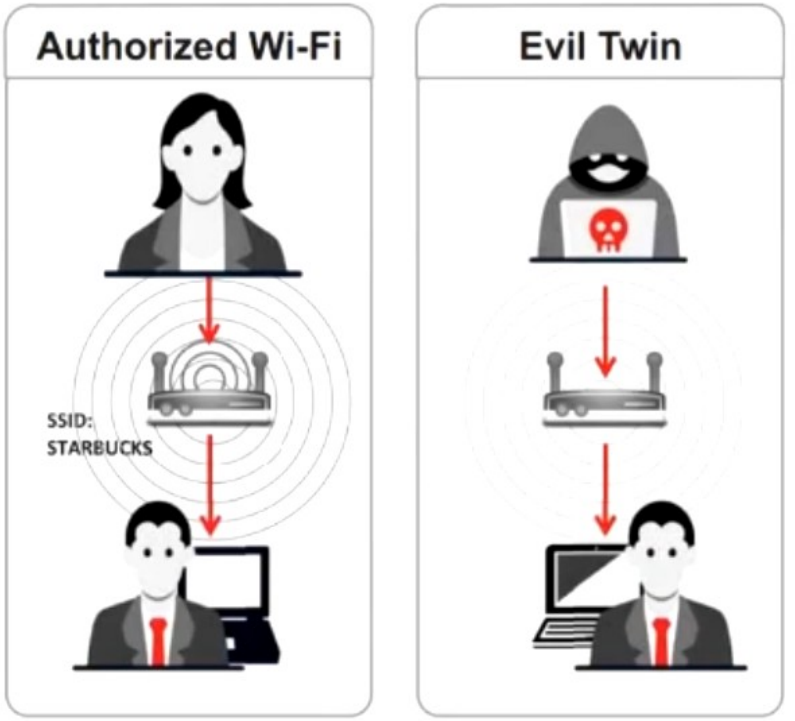
Launch of Wireless Attacks: Evil Twin

Evil Twin is a **wireless AP** that pretends to be a **legitimate AP** by replicating another network name

Attackers set up a **rogue AP outside the corporate perimeter** and lures users to sign into the wrong AP

Once associated, users may **bypass the enterprise security** policies, giving attackers access to network data

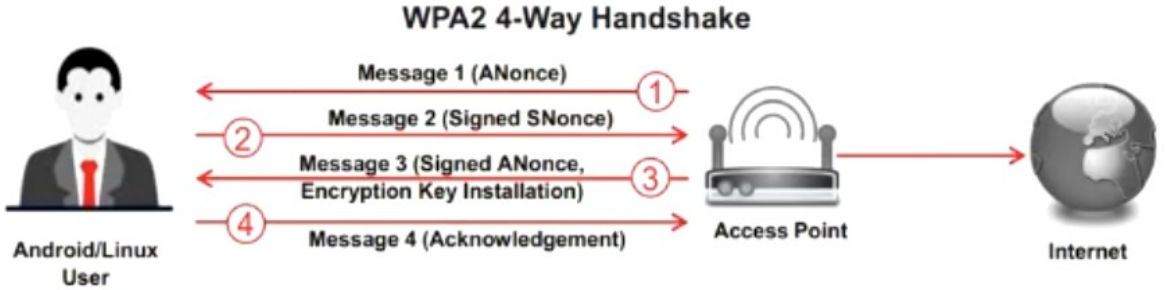
Evil Twin can be configured with a **common residential SSID**, hotspot SSID, or a company's WLAN SSID

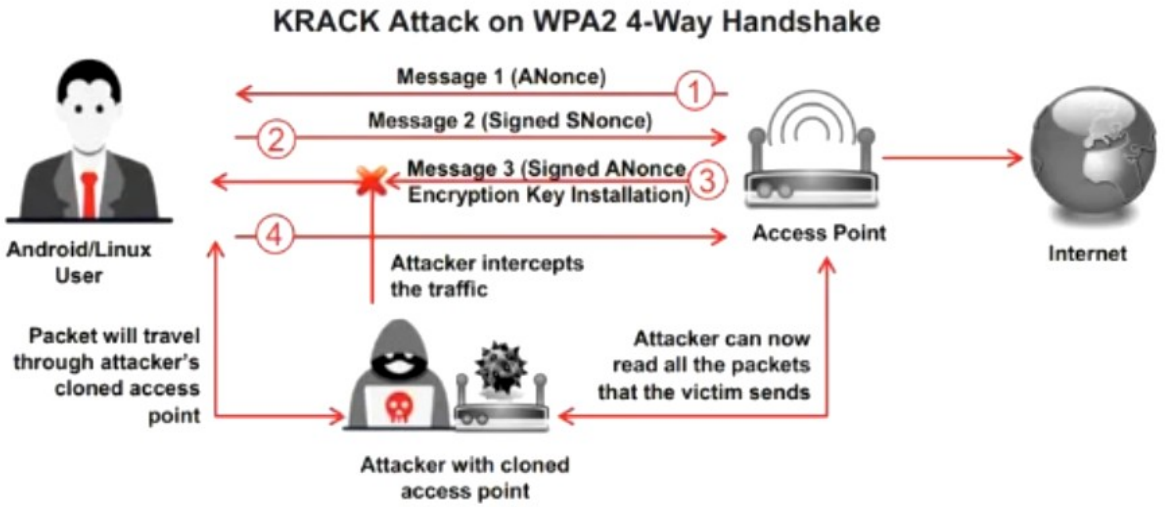


Wi-Fi is everywhere these days and so are your employees who take their laptops to Starbucks, FedEx Office, and the airport; how do you keep the company data safe?

Launch of Wireless Attacks: Key Reinstallation Attack (KRACK)

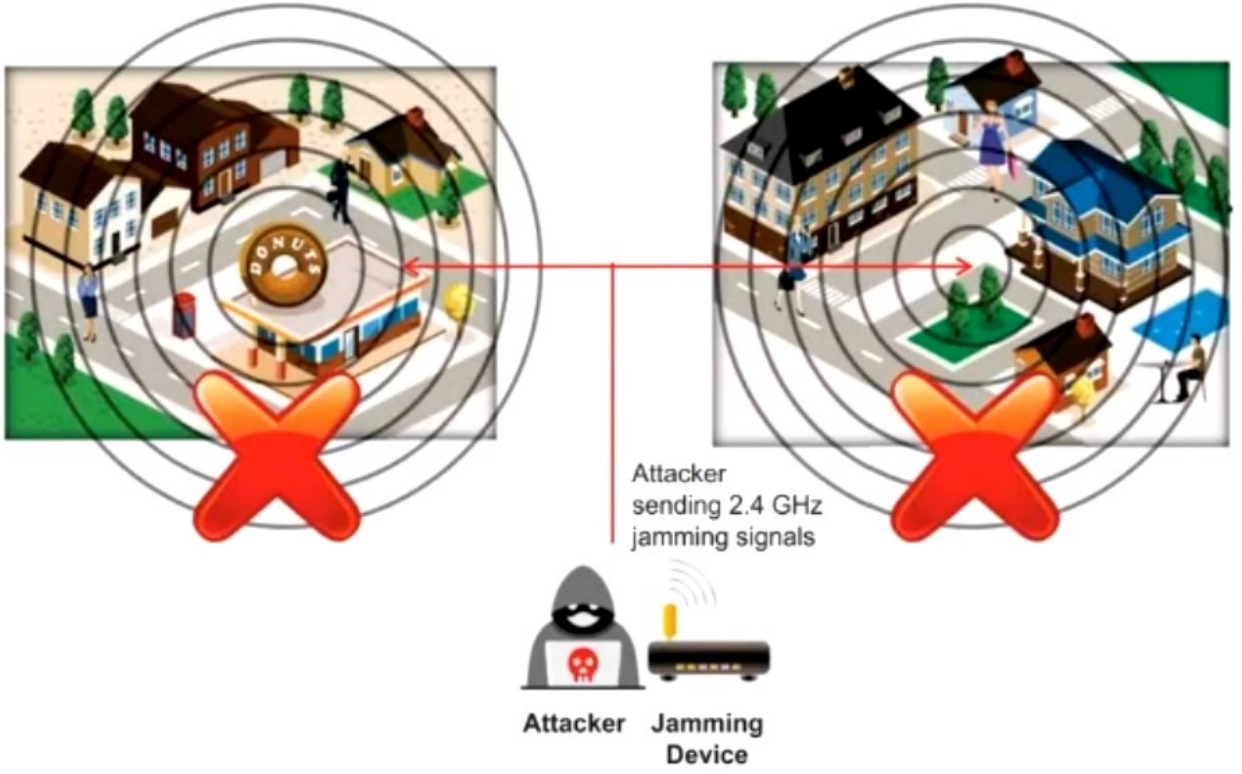
- All secure Wi-Fi networks use **the 4-way handshake process** to join the network and generate a **fresh encryption key** that will be used to encrypt the network traffic
- The KRACK attack works by exploiting the 4-way handshake of the **WPA2 protocol** by forcing Nonce reuse
- KRACK works against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





Launch of Wireless Attacks: Jamming Signal Attack

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



Wi-Fi Jamming Devices

PCB-4510 Jammer

- Range: 50–150 m
- 10 Antennas
- 10 Antennas bands jammed (GSM, 3G, UMTS, 4G, Wi-Fi, GPS, 5G)
- Working time: 1- 2 Hours

CPB-2920 Jammer

- Range: 10–40m
- 20 Antennas
- 20 frequency bands jammed (CDMA, DCS, PCS, 3G, UMTS, 4G, 5G..)
- Working time: No time limit

CPB-2612H-5G Jammer

- Range: 20–60 m
- 12 Antennas
- 12 frequency bands jammed (5G, 4G, GSM, 3G, UMTS, WiFi, UHF, VHF..)
- Working time: No time limit

CPB-2080-5G Jammer

- Range: 10–40 m
- 8 Antennas
- 8 frequency bands jammed (5G, 4G LTE, 3G, UMTS, WiFi..)
- Working time: No time limit

PCB-2112 Jammer

- Range: 20–50 m
- 12 Antennas
- 12 Antennas bands jammed (CMDA, DCS, 3G, WiFi, 4GLTE, 5G, GPS..)
- Working time: 60-80 Min

PCB-1016 Jammer

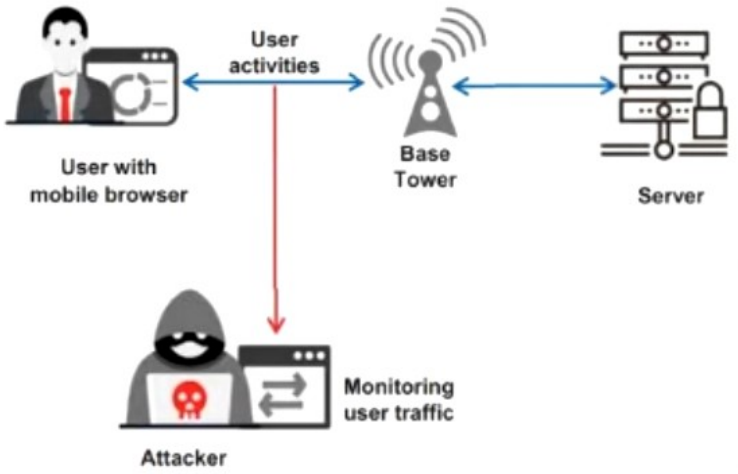
- Range: 10–30 m
- 16 Antennas
- 16 Antennas bands jammed (CDMA, DCS, 3G, 4G, WiFi, GPS, 5G..)
- Working time: 3.0 Hours

Launch of Wireless Attacks: aLTEr Attack

Attacker installs a **virtual (fake) communication** tower between two authentic endpoints intending to mislead the victim. This virtual tower is used to **interrupt the data transmission** between the user and real tower attempting to **hijack the active session**

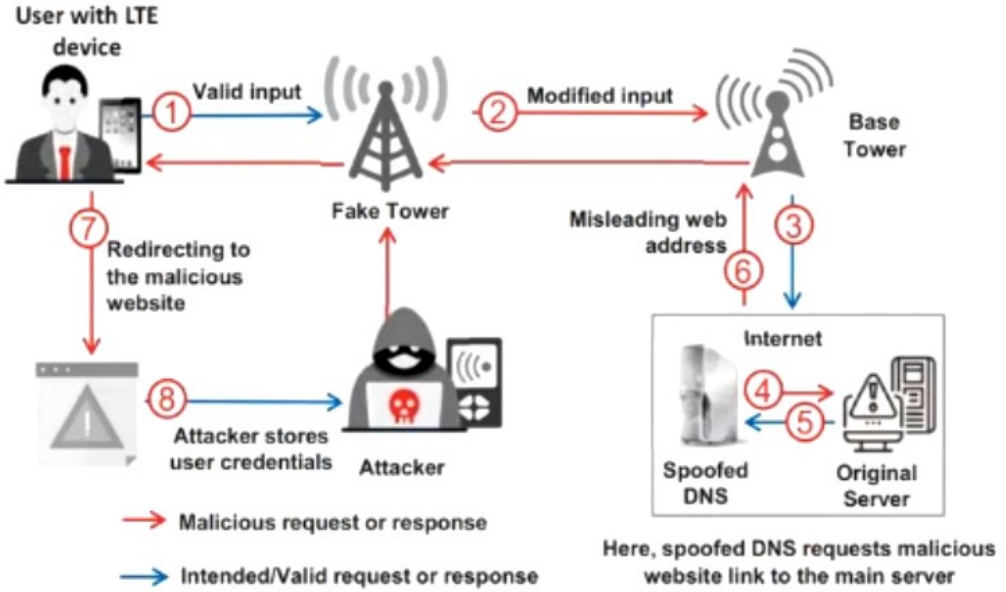
Information Gathering Phase

Attackers passively gather information needed to perform aLTEr attack using techniques, such as **identity mapping** and website fingerprinting



Attack Phase

Attackers use the information gathered to perform an active attack using techniques, such as **DNS spoofing**



Launch of Wireless Attacks: Wi-Jacking Attack

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

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

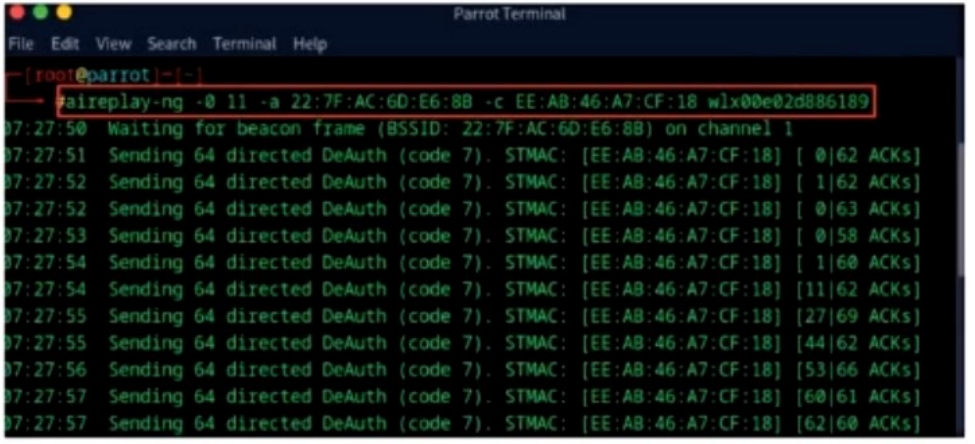
Step 3 Use tools, such as **dnsmasq** and python scripts, to inject malicious URL and lure the victim's browser to load the malicious URL

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

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

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

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



Launch of Wireless Attacks: RFID Cloning Attack

- RFID cloning involves **capturing the data** from a legitimate RFID tag and then **creating its clone** using a new chip
- Attackers use tools such as **iCopy-X** and **RFIDIerto** to clone RFID tags

iCopy-X | iCopy-X is an entirely stand-alone and portable RFID cloning device that can used by attackers to **clone RFID tags**

https://icopyx.com

Additional RFID Cloning Tools

RFIDler
https://www.github.com

RFID Mifare Cloner
https://github.com

Flipper Zero
https://flipperzero.one

Boscloner Pro
https://www.boscloner.com

Wi-Fi Encryption Cracking: WPA/WPA2 Encryption Cracking

WPA PSK

WPA PSK uses a **user-defined password** to initialize the TKIP, which is not crackable as it is a per-packet key, but the keys can be brute-forced using dictionary attacks

Offline Attack

You only required to be near the AP for a matter of seconds to capture the **WPA/WPA2 authentication handshake**; by capturing the right type of packets, you can **crack the WPA keys offline**

De-authentication Attack

Force the connected client to disconnect. Then, capture the re-connect and authentication packets using tools, such as aireplay; you should be able to re-authenticate in a few seconds. Then **attempt to dictionary brute-force** the PMK

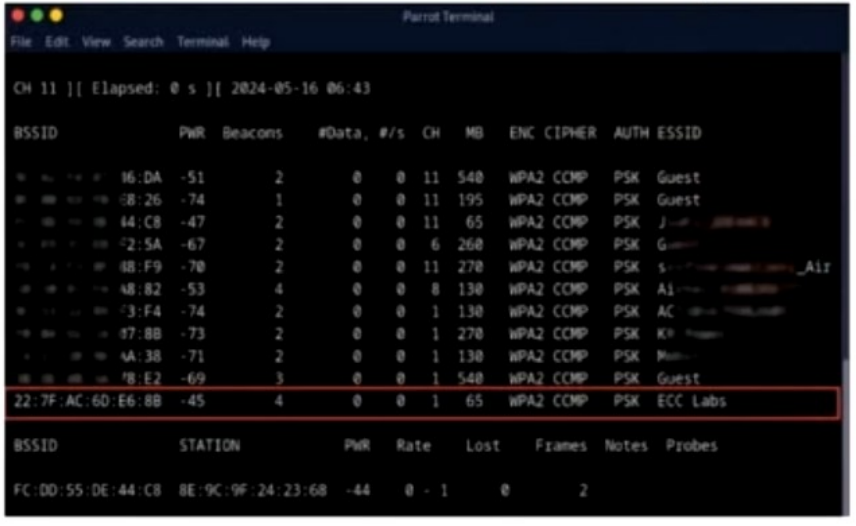
Brute-Force WPA Keys

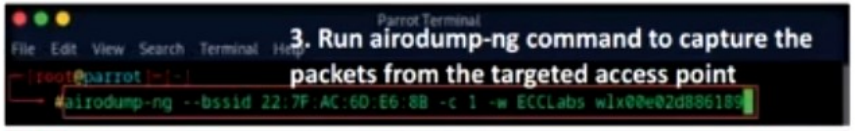
You can use tools, such as **aircrack** and **aireplay** to brute-force WPA Keys

Cracking WPA/WPA2 Using Aircrack-ng

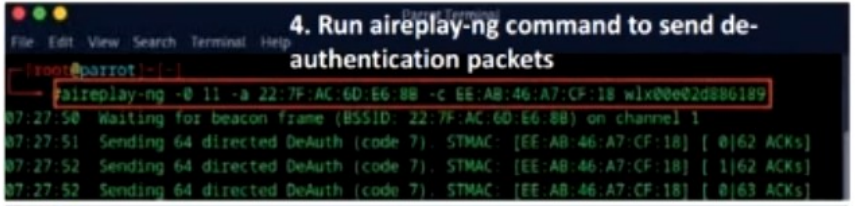
1. Run airmon-ng in monitor mode

2. Run airodump-ng command to get a list of detected access points

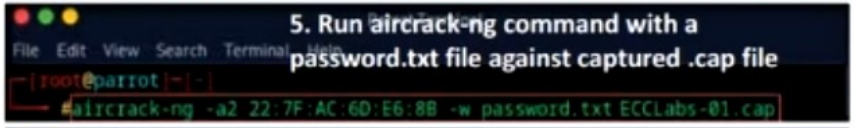




3. Run airodump-ng command to capture the packets from the targeted access point



4. Run aireplay-ng command to send de-authentication packets



5. Run aircrack-ng command with a password.txt file against captured .cap file

6. The result of aircrack-ng command showing the cracked key as KEY FOUND!

WPA Brute Forcing Using Fern Wifi Cracker

Step 1: Run **sudo fern-wifi-cracker** command to start the Fern WiFi Cracker tool

Step 2: Enable the monitor mode by selecting the Wi-Fi adapter from the drop-down menu and clicking on the "**Monitor Mode**" button

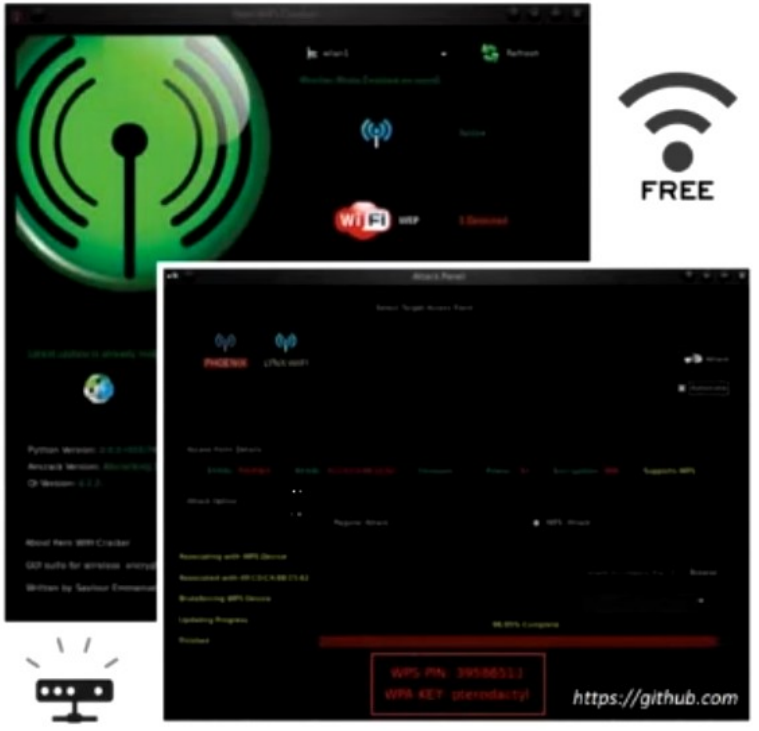
Step 3: Click on the "**Scan for Access points**" button to start scanning for Wi-Fi Networks and select a target WPA/WPA2 network

Step 4: Initiate a **de-authentication attack** by clicking on the "Attack" button next to the target network to start de-authenticating clients

Step 5: The tool will notify you once it successfully **captures a WPA handshake**

Step 6: Choose a **wordlist file** containing potential passwords to try against the captured handshake

Step 7: Click on the "**Start WPA Attack**" button. If the correct password is found, it will display the password on the screen



WPA3 Encryption Cracking

- **Dragonblood** is a set of **vulnerabilities in the WPA3** security standard that allows attackers to **recover keys**, **downgrade security mechanisms**, and launch various information-theft attacks
- Attackers can use various tools, such as **Dragonslayer**, **Dragonforce**, **Dragondrain**, and **Dragontime**, to exploit these vulnerabilities and launch attacks on WPA3-enabled networks

Downgrade Security Attacks

- **Exploiting Backward Compatibility**
  - An attacker installs a rogue AP and forces the user to involve in WPA2 encryption
  - Then, the attacker performs all the attacking techniques available to exploit WPA2
- **Exploiting the Dragonfly Handshake**
  - An attacker with a rogue AP discards the user's WPA3 Dragonfly mechanism
  - The attacker forces the user to use a weaker encryption algorithm, such as WPA2, and exploits WPA2

Side-channel Attacks

- **Timing-Based**
  - An attacker analyzes the amount of time dragonfly handshake takes for certain password authentications
  - The attacker notices the number of iterations the encoding process takes and short-lists the passwords to launch further attacks
- **Cache-Based**
  - An attacker installs malicious JavaScript code on the client's browser and observes memory access patterns
  - The attacker retrieves the passwords to perform malicious actions with the user's credentials

Cracking WPA3 Using Aircrack-ng and hashcat

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

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

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

```
airodump-ng wlan0mon
```

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

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

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

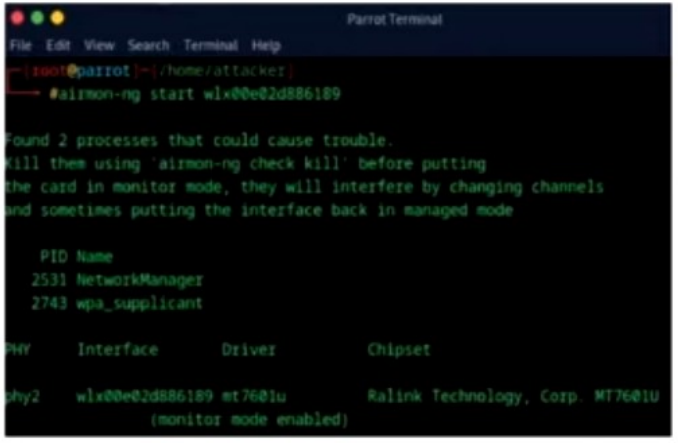
```
hcxpcapngtool -o capture.hccapx <capture>.cap
```

Step 5: Finally, crack the handshake using hashcat with a wordlist file:

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

Cracking WPS Using Reaver

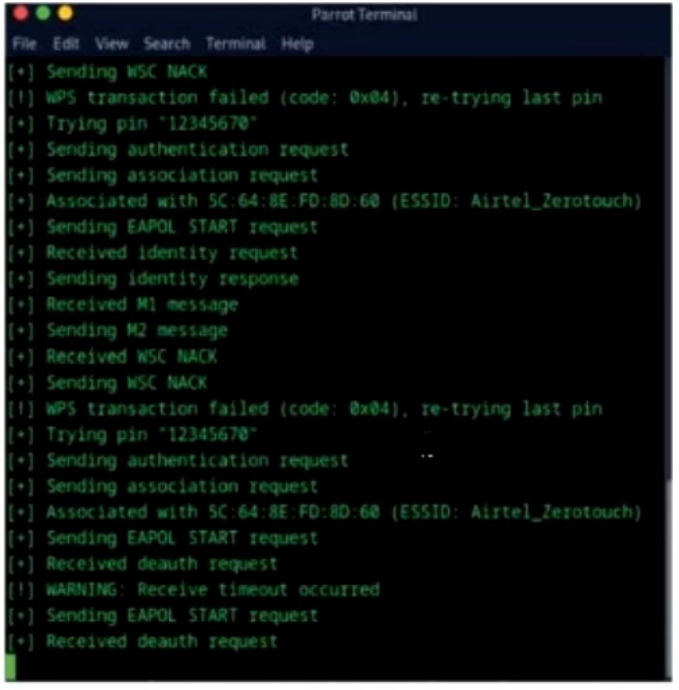
Step 1: Setup your wireless interface in monitoring mode using **airmon-ng**



Step 2: Use **wash utility** to detect WPS-enabled devices

Step 3: If you are unable to detect WPS-enabled devices using wash, use **Airodump-ng** to detect devices using WPS

Step 4: After identifying the BSSID of the target device, start cracking the WPS PIN using **Reaver**



Objective 05

Explain Wireless Attack Countermeasures

Defense Against WPA/WPA2/WPA3 Cracking

Wireless Attack Countermeasures

- Use a **password** with at least 12-16 characters, including uppercase and lowercase letters, numbers, and special characters
- Disable **TKIP** in the router settings and ensure only AES encryption is used
- Turn off **WPS** in the router settings to prevent brute-force attacks on the WPS PIN
- Check the manufacturer's website regularly for **firmware updates** and apply them promptly
- Limit the **Wi-Fi signal range** to reduce the chances of unauthorized access from outside the premises
- Use **network monitoring tools** to detect and respond to suspicious activities
- Use **WPA3-SAE** wherever possible for all devices that support it
- Disable **transition mode** if all devices support WPA3 to ensure the highest level of security

Defense Against aLTEr Attack

- Encrypt **DNS queries** and only use trusted DNS resolvers
- Resolve DNS queries using the **HTTPS protocol**
- Use DNS over TLS or DTLS to provide encryption and **integrity-protection** to the DNS traffic
- Implement RFC 7858/RFC 8310 to prevent **DNS spoofing attacks**
- Use **DNSCrypt** protocol to authenticate communication between a DNS client and DNS resolver
- Use strong encryption algorithms such as **AES-256** to ensure that all communications are encrypted end-to-end
- Use **mutual authentication** mechanisms to verify the identity of both parties in the communication process

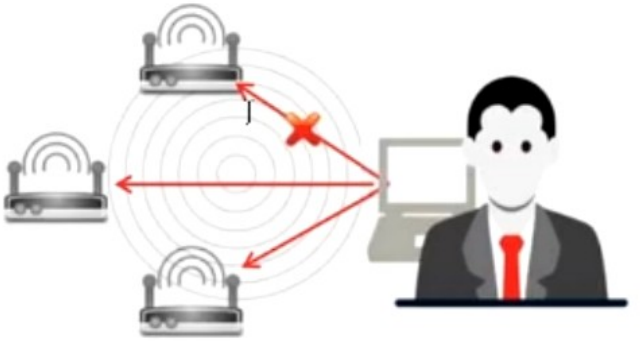
Detection and Blocking of Rogue APs

Detection of Rogue APs

- **RF Scanning**
  - Re-purposed APs that perform only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the WLAN administrator about any wireless devices operating in the area
- **AP Scanning**
  - APs that can detect neighboring APs operating in close proximity will expose the data through its MIBS and web interface
- **Wired Side Inputs**
  - A network management software uses this technique to detect rogue APs; this software detects devices connected in the LAN, including Telnet, SNMP, and Cisco discovery protocol (CDP), using multiple protocols

Blocking of Rogue APs

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



Defense Against Wireless Attacks

Best Practices for Configuration

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

Best Practices for SSID Settings

- 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** between the AP and the corporate Intranet
- Limit the **strength of the wireless network** to avoid being detected outside the bounds of your organization
- Regularly check the wireless devices for **configuration** or **setup** problems
- Implement an additional technique for **encrypting traffic**, such as IPsec over wireless

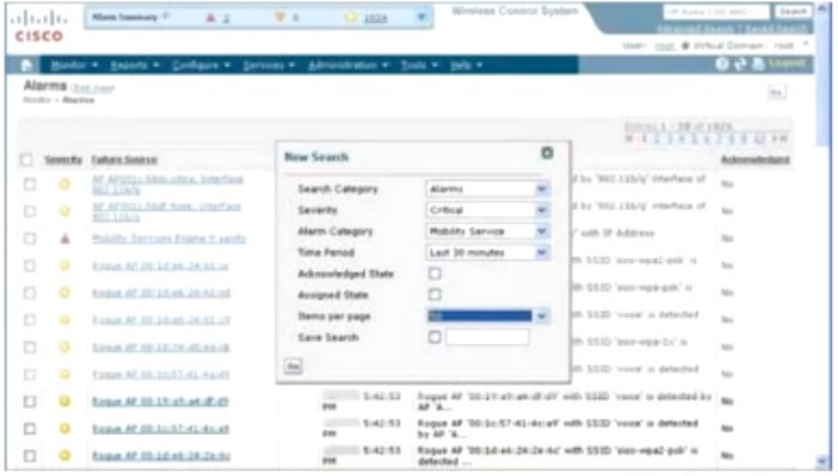
Best Practices for Authentication

- Enable **WPA3** for the highest level of security
- If WPA3 is not supported by your devices, use **WPA2 with AES** encryption
- Use **802.1X authentication** with a RADIUS server for enterprise networks
- Disable the **network** when not required
- Place wireless APs in a **secure location**
- Keep drivers on all wireless equipment **updated**
- Use a centralized server for **authentication**

Wi-Fi Security Auditing Tools

Cisco Adaptive Wireless IPS

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

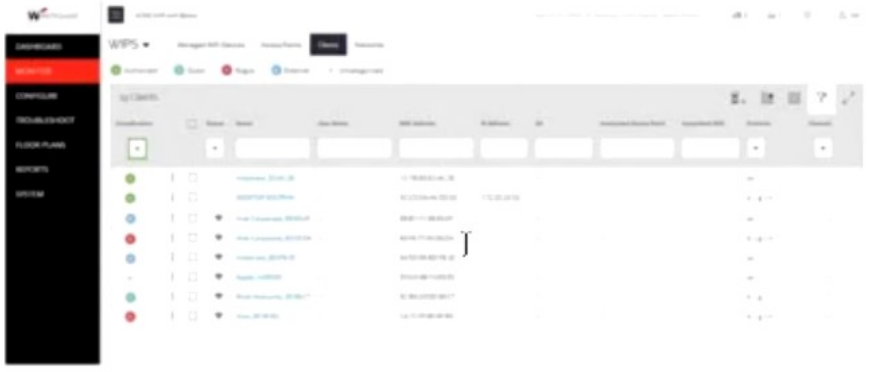


https://www.cisco.com

Wi-Fi IPSs

WatchGuard Wi-Fi Cloud WIPS

- WatchGuard Wi-Fi Cloud WIPS defends your airspace from **unauthorized devices**, **rogue APs**, and **malicious attacks** and with near-zero false positives



https://www.watchguard.com

Other Wi-Fi Security Auditing Tools:

RFProtect
https://www.arubanetworks.com

Fern Wifi Cracker
https://github.com

OSWA-Assistant
https://securitystartshere.org

BoopSuite
https://github.com

Wifite
https://github.com

Module Summary

- In this module, we have discussed the following:
  - Wireless network concepts and different types of wireless encryption technologies
  - Various wireless threats
  - Wireless hacking methodology, which includes Wi-Fi discovery, wireless traffic analysis, launching wireless attacks, and cracking Wi-Fi encryption
  - Various wireless hacking tools
  - Various countermeasures to prevent wireless network hacking attempts by threat actors
  - How to secure wireless networks using wireless security tools
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform mobile hacking to compromise mobile devices