Pre Connection Attacks

1. Packet Sniffing:

To capture the packets directed to the target network we use Airodump-NG while being in monitor mode.

- It is a part of the Aircrack-NG suit
- It is a packet sniffer
- used to capture all packets within the range
- displays detailed information such as MAC address, the channel encryption used, clients connected to the network of the networks around us.

1. Enable monitor mode
2. Run airodump-NG (2.4GHz networks)

airodump-ng mon0 (Quit this process using Ctrl+C)

This command results in the following values:

ESSID - name of wireless networks around us
BSSID - MAC address of the networks
PWR - signal strength/ power of the network (more value, more strength)
beacons - frames sent by the network in order to broadcast its existence. (even if it is set hidden)
#Data - no. of data packets
#/s - no. of data packets we collected in last 10s
CH - Channel is where networks work on
MB - maximum speed supported by network
ENC - encryption used by the network (WPA, WEP, WPA2)
* open networks does not use encryption i.e; no password.
AUTH - authentication used in the network (PSK - Pre-shared Key, MGT)

2. WiFi Bands

The band of a network means the frequency the clients or other computers need to support & use to connect to this network. The two main frequencies used are 2.4 GHz & 5GHz.

The frequency of networks sniffed on airodump-ng is 2.4 GHz. But if you see the list of networks of your host system wifi, it contains both 2.4GHz & 5GHz networks.

This is because the airodump-NG is only sniffing on 2.4GHz.

Most of the network adapters can see & communicate with 5GHz networks but don't support monitor mode & packet injection.

Recommended : network adapter Alpha AWUS036ACH to see 2.4GHz & 5GHz networks

To pick up 5GHz networks by wireless adapter, we use (if supported)
airodump-ng :

```
airodump-ng --band a mon0
```

a → band name
mon0 → network interface.

Specifying multiple bands (2.4GHz & 5GHz)

```
airodump-ng --band abg mon0
```

Problem with this is
- need a power adaptor to sniff on two bands with lot of channels
- airodump-ng has to hop on all of them & discover clients & networks broadcasting on all channels.

3. Targeted Packet Sniffing.

Considering a target network from list of network, now to sniff on target network

```
> airodump-ng --bssid F8:23:B2:B9:50:A8
  --channel 2 --write test mon0
```

- channel → channel on which target n/w broadcast
- test → data captured on network
- mon0 → n/w interface.
- F8:23:B2:B9:50:A8 → MAC address of target n/w

This command returns list of devices connected to the target network.

- BSSID - target network MAC address
- Station - clients / devices MAC address
- PWR - power or signal strength of each devices
- Rate - speed
- Lost - amount of data lost
- Packets - no. of frames/ packets captured
- Probe - list of devices still trying/probing for networks

Press ctrl+c to quit this process, now we can few files created in current directory

test-01.cap ★ test-01.csv (01 appended by airodump-ng) test-01.kismet.netxml test-01.kismet.csv

This cap file contains the data that we captured during the period that airodump-ng was working. This file contains everything that was sent to and from my target network like URLs, chats messages, username, passwords, everything devices did on internet as they are sent from & to router But these data is encrypted (WPA 2)

Open cap file using Wireshark.

To open Wireshark, use command.

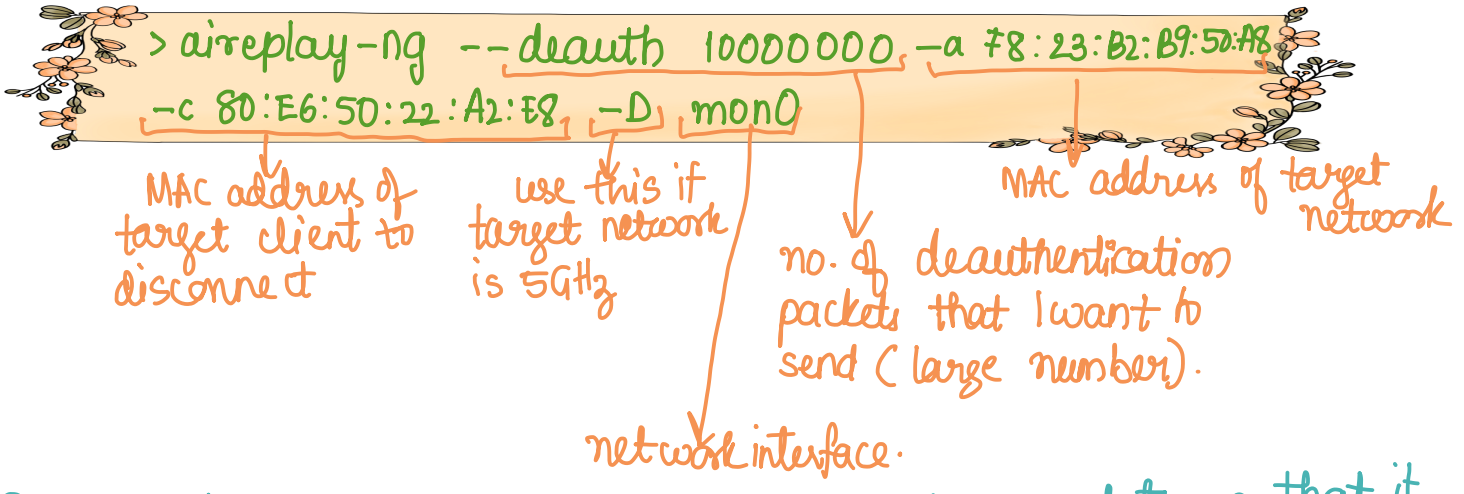
> wireshark

4. Deauthentication attack- pre-connection attack.

This attack allows us to disconnect any device from any network before connecting to any of these networks or without need to know the password for the network.

Strategy: We are going to pretend to the client that we want to disconnect from you. Then we are going to pretend to be router again, by changing our MAC address to router's MAC address and tell the client that you requested to be disconnected so I am going to disconnect you. This successfully disconnects or deauthenticates client from any network.

Now this is done using tool called aireplay-ng



* Give a large number of deauthentication packets so that it keeps sending these packets to both the router & target device for a very long period of time. To get router & client connected, quit aireplay-ng by pressing ctrl+C

* This command will only disconnect the target client from specified network. So if there are other network that target clients can connect to, it will automatically connect to them.

So in many cases it might connect to 5GHz

version of the network or it might connect to completely different network that it already knows the password to. If it is a mobile device, it may use data plan for internet

To avoid this, open a new terminal & run exact command same client & new target network

To perform deauthentication attack successfully,

In a terminal window run airodump-ng against target network

```
airodump-ng --bssid F8:23:B2:B9:50:A8
--channel 2 mon0
```

In another terminal run aireplay-ng

```
aireplay-ng --deauth 1000000 -a F8:23:B2:
B9:50:A8 -c 40:98:AD:98:51:70 mon0
```

Now the client cannot access any network
To connect back quit aireplay-ng, airodump-ng.

Attacks possible using Deauthentication Attack:

- Used in social engineering attack
- Used in creating fake access point & attack
- used to capture handshake to perform WPA Cracking