

Packet Sniffing

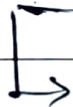
- We now need a program that can capture these packets for us.
- Use airodump-ng for this.
- enable monitor mode & then do:

```
# airodump-ng wlan0
```

(this is a dummy wireless adapter name)

→ ctrl + c to quit.

→ The output it shows is very useful.



- ① ESSID shows all wifi networks around.
- ② Other columns show more info about the network name we saw.
- ③ BSSID shows MAC Address of target.
- ④ PWR is power of network. (Higher the #, better the signal)
- ⑤ Beacons are frames sent by network to broadcast its existence.
- ⑥ #Data shows # of useful packets.
- ⑦ CH means channel.
- ⑧ ENC tells the encryption of the network.

⑨ Auth is the authentication used on that network.

★ WiFi Bands

- decides frequency range that can be used
- determines channels that can be used
- most common: 2.4ghz & 5ghz

★ → a: 5ghz only

→ airodump-ng only shows 2.4ghz networks.

→ use:

airodump-ng --band a wlan0

→ now it'll discover 5ghz networks if your wireless network adapter supports it.

→ abg: captures both 2.4 & 5ghz at same time.

★ Targeted Packet Sniffing

→ now we can target a particular network.

→ do:

airodump-ng --^(specific)bssid {bssid} --channel {ch} --write test wlan0

eg:

airodump-ng --bssid F8:23:B2:B9:50:A8 --channel 2 --write test wlan0

↓
writes all data to test file.

→ Once this is done, you'll see one more section that shows the clients connected to that network.

→ STATION column shows client's MAC address.

→ The data is captured & stored locally.

- test - 01. cap file stores everything saved.

★ Deauthentication Attack

↳ eg WEP, WPA & WPA2

↳ no need to know network key

↳ no need to connect to the network

★ This will disconnect target client from the given network.