Gathering Information

- In section 1 we saw how we can user airodump-ng to discover all the AP's around us and the clients associated with them.
- Now that we are connected to a specific AP, we can gather more detailed info about the clients connected to this AP.
- There is a number of programs that can be used to do this, we shall talk about 3 programs starting with the simplest and quickest one.

Netdiscover

Netdiscover is a program that can be used to discover the connected clients to our current network, its very quick but it does not show detailed information about the clients: IP , MAC address and some times the hardware manufacturer for the client's wireless card.

Usage:

```
netdiscover -i [INTERFACE] -r [RANGE]
ex: netdiscover -i wlan0 -r 192.168.1.1/24
```

Autoscan

Autoscan is another program that can be used to discover the connected clients to our current network, its not as quick as net discover, but it shows more detailed information about the connected devices and it has a graphical user interface.

You can download Autoscan from:

```
http://autoscan-network.com/download/
```

Then open the directory where you extracted it and run

```
./AutoScan*.sh
```

Nmap

- Namp is a network discovery tool that can be used to gather detailed information about any client or network.
- We shall have a look on some of its uses to discover connected clients and gather information about them.
- We are going to use Zenmap – the GUI for Nmap.

1. Ping scan: Very quick – only shows connected clients.

2.Quick scan plus: Quick – shows MAC and open ports.

3.Quick scan plus: Slower then the 2 above, more detailed info.

These are just sample scans, you can experiment with the scan options and see the difference between them.