**Aircrack-NG/Airodump-NG/Airmon-NG Tutorial**

Aircrack-NG is a suite of tools used for penetration testing WiFi networks. It can be used in conjunction with Wireshark to analyse pcap files generated by packet captures. Useful network information can be observed along with the WPA-2 hash which can be cracked with dictionary lists and rainbow tables.

Ensure you have the correct drivers installed for your NIC adapter, Follow my driver installation tutorial on github for the AWUS036ACH

## Starting/getting kali to read your NIC Troubleshooting

Note: Connecting a USB Nic and having Kali register it can be temperamental, 2 tactics that I have used are:

Open kali, let it load, link usb via virtualbox settings, UNPLUG AND PLUG IN, link again, iwconfig, airmon-ng start wlan0, sudo wifite.

Or

Open kali, let it load, connect usb nic device via virtualbox, run sudo airmon-ng start wlan0, run sudo airmon-ng check kill. Disconnect usb, reconnect, run sudo airmon-ng start wlan0, run sudo wifite to check

• First of all, you need configure the Oracle VM: File – Preferences – Proxy – select Direct Connection to Internet

• Then you configure your Kali Linux VM: plug your network adapter in USB – go to Settings – in Net select Bridge mode – in USB you must add your network adapter – then edit the filter, Remote must be No

• Then, VERY IMPORTANT, UNPLUG YOUR NETWORK ADAPTER FROM USB

• After that start your Kali Linux VM

• After the Kali Linux being ready, then, just then, PLUG YOUR NETWORK ADAPTER IN USB

• In this point you are going to listen 2 noises, one for the connection in the host other for the connection in VM

• You can check the status in Devices – USB, you must see your network adapter already selected

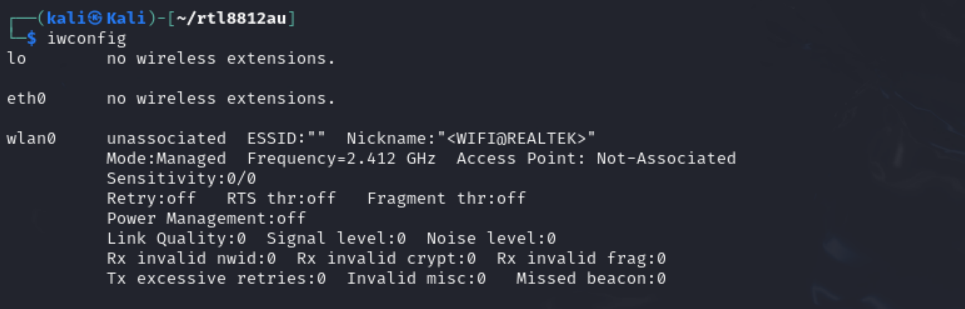
## Regular Procedure once kali reading your NIC Adapter

Check device is reading with: lsusb

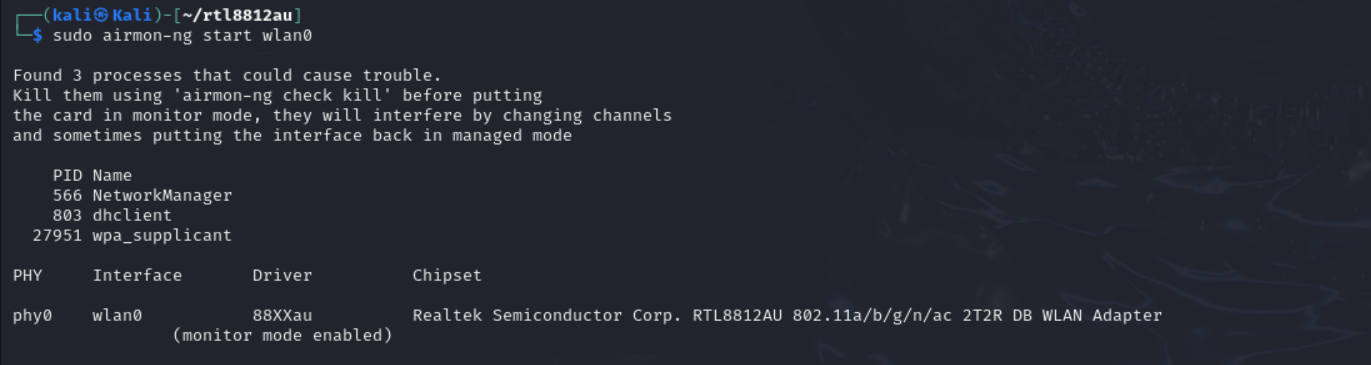
A computer screen with white text

Description automatically generated

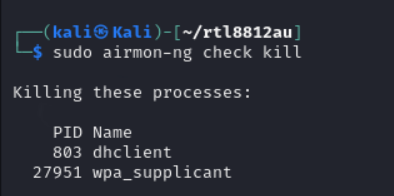
Check device is being read in wireless interfaces : iwconfig



Use airmon-ng to enable the wireless adapter to promiscuous mode



Conflicting processes can cause issue so terminate them with: airmon-ng check kill



Now we must capture packets from the network of choice, these networks will belong to a frequency within the spectrum of the protocol band you are using.

**2.4 GHz (802.11b/g/n/ax)**

14 channels are designated in the 2.4 GHz range, spaced 5 MHz apart from each other except for a 12 MHz space before channel 14.[[2]](https://en.wikipedia.org/wiki/List_of_WLAN_channels#cite_note-3) The abbreviation F0 designates each channel's fundamental frequency.

A white rectangular object with black text

Description automatically generated with medium confidence

We can begin to investigate channels with the syntax: airodump-ng wlan0

A screen shot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

I have hidden details due to ethical reasons and will only select my home network. Ensure to follow local laws of your jurisdiction.

To filter only the network we want to see we can use:

sudo airodump-ng wlan0 -d <BSSID>

A screenshot of a computer

Description automatically generated

After narrowing down a network we can capture the data being sent over the network into a pcap file with the syntax:

sudo airodump-ng -w <filename> -c <channel#> --bssid <MAC Address> wlan0

A screen shot of a computer

Description automatically generated

In a new terminal we can deauth users off the network in order to capture the Pre Shared Key(PSK) when they reconnect which contains the WPA2 key in hash form

A screenshot of a computer

Description automatically generated



Once the deauth is successfully completed and captured the WPA2 key we will receive the message circled in red

From here we can access the pcap file in wireshark



We can see the WPA Key Data in the second handshake

A computer screen with blue and white text

Description automatically generated

Now we have the key we can run offline dictionary attacks against the key until we find a match for the hash

