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.

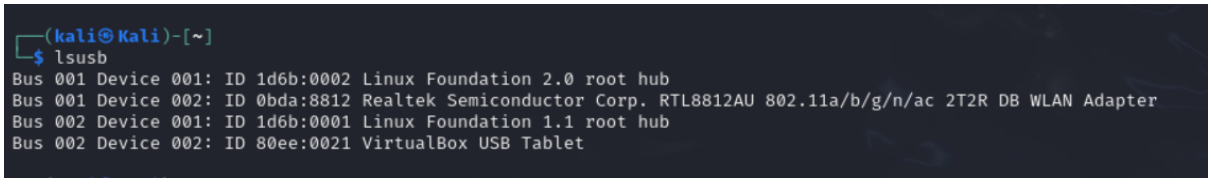
Or

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



Check device is being read in wireless interfaces : iwconfig

```
┌──(kali㉿Kali)-[~/rtl8812au]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

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

```
┌──(kali㉿Kali)-[~/rtl8812au]
└─$ sudo airmon-ng start wlan0

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    566 NetworkManager
    803 dhclient
  27951 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
                (monitor mode enabled)
```

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

```
┌──(kali㉿Kali)-[~/rtl8812au]
└─$ sudo airmon-ng check kill

Killing these processes:

    PID Name
    803 dhclient
  27951 wpa_supplicant
```

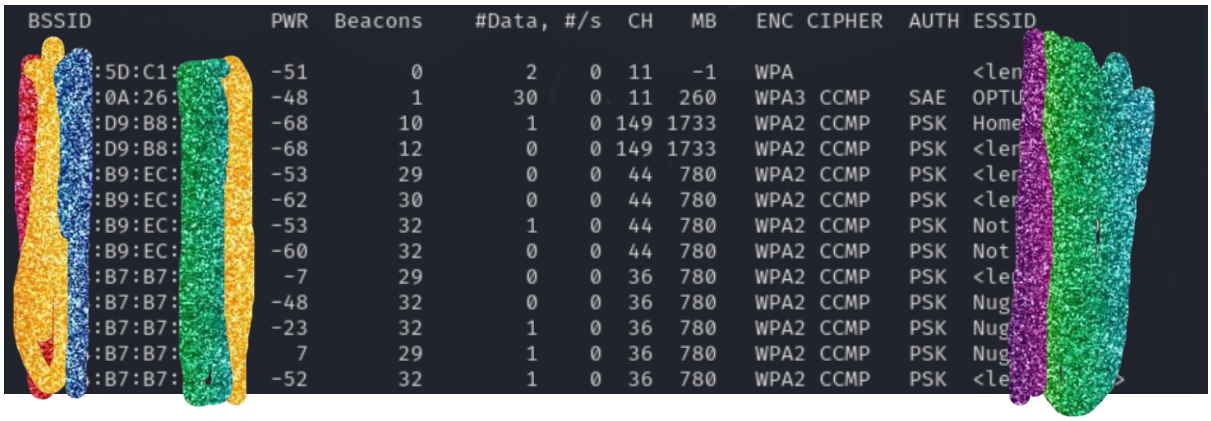
Now we must capture packets from the network of choice, these networks will belong to a frequency within the spectrum of the protocol band you are using.

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] The abbreviation F_0 designates each channel's fundamental frequency.

#	F_0 (MHz)	DSSS						OFDM												Most of world [3][4][5][6][7][8][9][10]	North America [3]	[hide] Japan [3]
		Frequency range (MHz)	Channel 22 MHz					Frequency range (MHz)	Channel 20 MHz					Center frequency index 40 MHz								
1	2412	2401–2423	1	2	3	—	—	2402–2422	1	2	3	—		3	—					Yes	Yes	Yes
2	2417	2406–2428				4		2407–2427				4				4	—					
3	2422	2411–2433					5	2412–2432	5	6	7				5		—					
4	2427	2416–2438	6	7	8			2417–2437				8				8		6	—			
5	2432	2421–2443				9		2422–2442						7			9					
6	2437	2426–2448					10	2427–2447	9	10	11	12			—	—		10				
7	2442	2431–2453				—		2432–2452						11			—					
8	2447	2436–2458						2437–2457														
9	2452	2441–2463	11	12	13			2442–2462														
10	2457	2446–2468						2447–2467														
11	2462	2451–2473						2452–2472														
12	2467	2456–2478						2457–2477													avoided[B]	
13	2472	2461–2483						2462–2482	13	—	—											
14	2484	2473–2495	14					—												No	No	11b only[C]

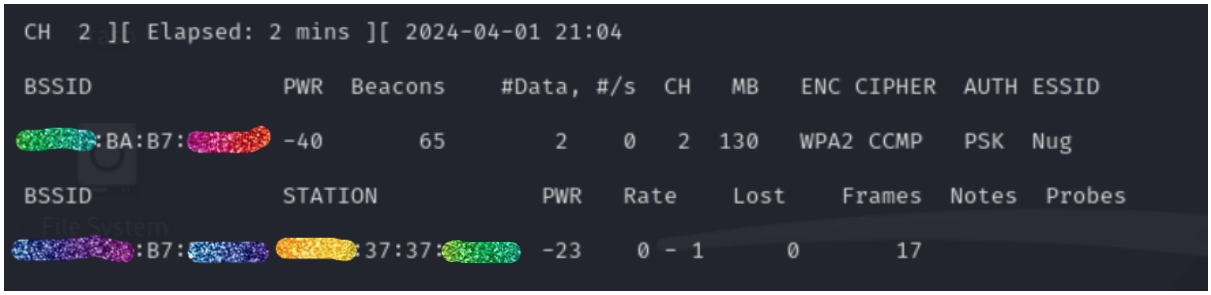
We can begin to investigate channels with the syntax: airodump-ng wlan0



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

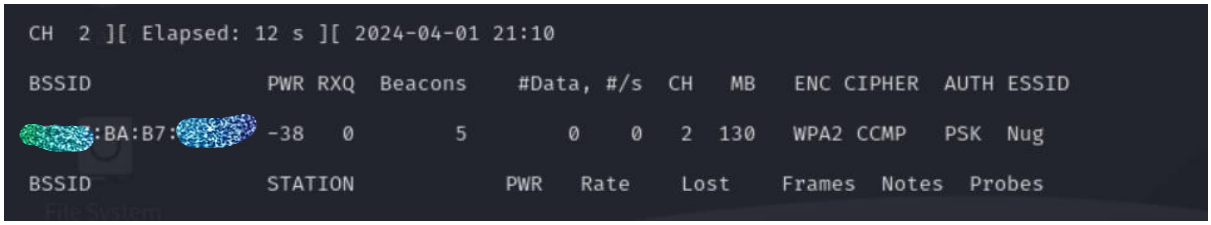
To filter only the network we want to see we can use:

sudo airodump-ng wlan0 -d <BSSID>

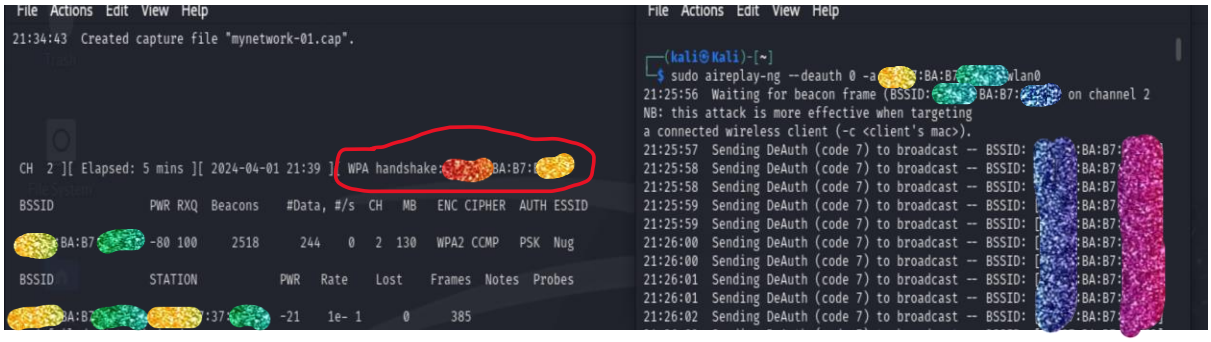


After narrowing down a network we can capture the data being sent over the network into a pcap file with the syntax:

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



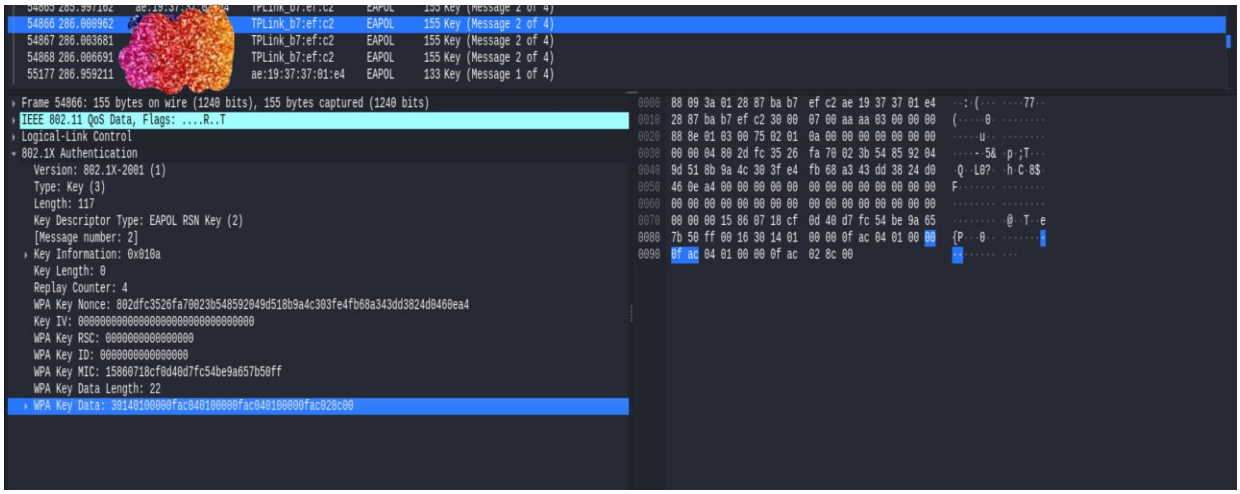
In a new terminal we can deauth users off the network in order to capture the Pre Shared Key(PSK) when they reconnect which contains the WPA2 key in hash form



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



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