

Forum:[Hack Forums](#)

Thread: [\[TUT\] Wi-Fi Hacking WPA-WPA2 Networks \[TUT\]](#)

Zee - February 20, 2020, 1:48 am

In this tutorial I will teach you how to hack nearby WPA & WPA2 WiFi Networks with Kali Linux. This is a simple but useful tutorial that will give you an introduction to hacking WiFi networks. I advice you to only try this on your own network, or a network you have been given permission to attack. Anyways, let's get started.

Step 1) First of all we have to determine the name/number of our WiFi card. Start by typing this command within a terminal:

Code `ifconfig`

If you scroll down, you should now see your identified WiFi card. Usually it will say wlan0, wlan1, or wlan2. Depending on the WiFi card you are using for this.

Step 2)

Now we have to put our WiFi adapter into monitor mode. To do this, we will be using this command:

Code `airmon-ng start wlan0`

And now we have got monitormode on wlan0.

Step 3)

This means we can now use the airodump tool to see all available networks within the range of the WiFi adapter. To see this, you will have to enter the following command within the terminal:

Code `airodump-ng mon0`

Airodump will now start scanning for all nearby networks. Press CTRL + C to stop scanning once it have found a few networks. Identify the ESSID (The name) of the network you want to attack, and copy the whole line into a notepad. This will make it easier when launching commands.

Step 4)

We now have to capture a 4-way handshake. WPA/WPA2 uses a 4-way handshake to authenticate devices to the network. These handshakes occur whenever a device connects to the network. We can capture this handshake by using airmon-ng to monitor traffic on the network using the channel and bssid values discovered from the previous command. To monitor the traffic on the network, we have to use this command:

Code `airodump-ng -c ENTERCHANNEL— bssid ENTERBSSID -w . mon0`

Replace ENTERCHANNEL with the channel number, and replace ENTERBSSID with the BSSID of the network you want to attack. The channel and BSSID should be found within the Notepad file we created earlier, or within the Airodump terminal if you still have it open.

Now we have to wait for a device to connect to the network. If you are feeling impatient, you can send deauthentication packets to force a device to reconnect. When you have captured a handshake, you should see something similar to this:

Code WPA handshake: bc:d6:c3:ef:d4:39

Step 5) Once the handshake is captured, you should press CTRL + C to quit airodump-ng. Now there should be a .cap file in your Desktop. It will most likely be called -01.cap. We will use this file to crack the password of the network. Rename the .cap file to whatever you'd like for making it easier to find it.

Now the only thing there is left to do is the actual cracking of the password. We will be using Aircrack for this tutorial, but using Hashcat is also another great alternative. In this tutorial we will be running a dictionary attack on the WiFi network. This means that the attack will try a bunch of passwords that we have stored within a Wordlist file. I recommend you to download the Rockyou.txt wordlist for this attack, but you can create your own Wordlist as well by following my tutorial on HackForums: <https://hackforums.net/showthread.php?tid=6051126>

Step 6) Anyways, the Rockyou.txt wordlist should be available within Kali linux in this directory "/usr/share/wordlists/". If it is not there already, you can download it by running this command with a new terminal:

Code `curl -L -o rockyou.txt`

<https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>

Once you have downloaded the wordlist, all there is left to do is run the attack. To start the bruteforcing, type the following command:

Code `aircrack-ng -a2 -b ENTERBSSID -w rockyou.txt FILENAME.cap`

Code a2 = specifies we are running WPA2

b = is the BSSID

w = is the wordlist

Replace ENTERBSSID and FILENAME, and the command is ready to go. Aircrack will now start bruteforce attacking the WiFi searching for a password. If the password is cracked you will see a KEY FOUND! message in the terminal followed by the plain text version of the network password.

Voilà! you have now learned how to attack a WiFi network, if you have any questions, feel free to post them within the thread or send me a private message.

Dotexe - February 20, 2020, 2:04 am

At least give the credits and appreciate the author, I've seen this shit million of times

Zee - February 20, 2020, 2:08 am

(Feb 20, 2020 03:04 AM)Dotexe Wrote: [\[CITE\]](#) At least give the credits and appreciate the author, I've seen this Clay Davis million of times

I wrote this thread myself, the method isn't new, but it should still give a basic introduction to beginners.

Zee - February 20, 2020, 2:10 am

(Feb 20, 2020 03:09 AM)Lowkey Wrote: [\[CITE\]](#) Pictures would definitely help but this is a simple and straightforward explanation overall! Thank you for sharing

You are right, I should have included some pictures. I will update the thread with some pictures as well later today.

R321 - February 20, 2020, 3:28 am

i just hope there would be some pictures in this tutorial
but it was cool

Zee - February 20, 2020, 3:31 am

(Feb 20, 2020 04:28 AM)R321 Wrote: [\[CITE\]](#) i just hope there would be some pictures in this tutorial
but it was cool

I will try to add pictures to the tutorial later today. However, it should be very straight forward, all of it is within the terminal.

R321 - February 20, 2020, 3:36 am

(Feb 20, 2020 04:31 AM)Zepro Wrote: [\[CITE\]](#) I will try to add pictures to the tutorial later today.

However, it should be very straight forward, all of it is within the terminal.
that's ok to me
thx u for your answer