

# Forum:[Hack Forums](#)

Thread: [A simple guide on how to hack your neighbour wifi](#)

dolentanon - October 14, 2023, 3:15 pm

What you need:

A computer with linux, a password word list like rockyou.txt (very easy to find, but I suggest you look for better ones) , and a tool called aircrack-ng.

What to do:

First of all you don't already have aircrack you might wanna install it, to do so type the command:  
`sudo apt install aircrack-ng`

Now you need to find out the name of your wireless interface, to do so type the command `ip a`. The name of your wireless interface

will usually start with a w, for example: wlan1, wlp2s0. IMPORTANT in all this guide I will use wlp2ex0 as a name holder, you will need to replace it with your own wireless interface name.

Once you have the name of your wireless interface we wanna put it in monitor mode. Note that doing so will kill your internet on your pc (don't worry a simple restart will fix it). To put your interface in monitor mode use the command: `airmon-ng start wlp2ex0`.

Once you have done that you might wanna use the command `airmon-ng check kill` this will kill the processes that are preventing your wireless interface to enter or to stay in monitor mode. If you are not sure if you were successful or not you can use the command `iwconfig` by looking for the name of your interface on the output of the command you will see in which mode your interface is. If it is not in monitor mode (usually managed mode) just repeat the process.

Now that our interface is in monitor mode we basically wanna start listening to the networks around us. To do so use the command `airodump-ng wlp2ex0`. Note that in some cases your wireless interface may have changed name in "name+mon", in the command put the current name.

Basically a list of networks will appear on your terminal, now you just have to choose which one you wanna get into. What you wanna save of the network you wanna get into is the BSSID (for example A6:92:B4:C2:B8:09) and the channel (1,2,3,4...).

Press `ctrl c` in order to stop listening to networks. Now use the command `airodump-ng -d A6:92:B4:C2:B8:09 -w file_name -c 1 wlp2ex0` (where A6:92:B4:C2:B8:09 is the BSSID and 1 the channel, and filename is a name you can chose for a file that will contain the handshake that we will capture).

With this command we can now see all the devices that are connected to a specific network, what we basically wanna do is capture a handshake from a device that connects to the network. In order to do so we will force a disconnect from one of the current connected devices, with a deauthentication attack. Open a second terminal and type `aireplay-ng -0 10 -a BSSID -c station wlp2ex0` (where -0 is for deauthentication, 10 is the number of packets we will send).

Now we are sending a deauthentication attack. If you are able to capture the handshake it will appear on the top left of the screen near the date and time. This might not be successful the first time and you might have to repeat this a few times, if it does not work on one device try on another.

Once we have captured the handshake, we can exit with `ctrl c`, and if we type the command `ls` we will see that in our current directory there are some new files. Now we wanna basically compare 1 on 1 all the passwords on the wordlist with the handshake we captured to do so use the command: `aircrack-ng -w directory_of_your_text_file` (for example `/usr/share/wordlists/rockyou.txt`) `file_name.cap`. Now let it run until you find the password or your wordlists ends. Note that your success rate is directly proportional to the quality of your wordlist. You can create a custom wordlist

if you know your target well.

This ends this guide, sorry if the formatting quality is low it is my first thread. If there are mistakes they will be fixed. Byte donations (if they exist) are very welcome as I would love to obtain some stuff here on the forum.

**Enrique78600725** - *October 15, 2023, 10:55 am*

Thanks for the method. i was really looking for it hope it works

**dolentanon** - *October 15, 2023, 10:40 pm*

(Oct 15, 2023 10:55 AM)Enrique78600725 Wrote: [\[CITE\]](#) Thanks for the method. i was really looking for it hope it works

It works, its works. If you have any problem feel free to quote me ore pm me.

**Pirate101** - *October 22, 2023, 11:36 am*

im a bit of a noob with all of this. but can this be done when running linux via a VM

**British Guy 23959** - *October 22, 2023, 3:42 pm*

hobos are gonna love this one

**arav** - *October 24, 2023, 12:21 pm*

if my pc doesn't support the monitor mode ?

**ipppp** - *October 25, 2023, 11:24 pm*

great job my bro keep going

**B3A** - *October 26, 2023, 12:16 am*

Seems like a clean written tutorial