How to Hack Wi-Fi Getting Started with the Aircrack-Ng Suite of Wi-Fi Hacking Tools

null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893

occupytheweb

Welcome back, my fledgling hackers!

In the first part of my series on Wi-Fi hacking, we discussed the basic terms and technologies associated with Wi-Fi. Now that you have a firm grip on what Wi-Fi is exactly and how it works, we can start diving into more advance topics on how to hack Wi-Fi.

In this article, we'll take a look at the world's best Wi-Fi hacking software, **aircrack-ng**, which we previously used to bump your annoying neighbor off their own Wi-Fi network. We'll be using aircrack-ng in nearly all of the subsequent hacks, so I think it's wise to start with some basics on what is included and how to use everything.

For this to work, we'll need to use a compatible wireless network adapter. Check out our 2017 list of Kali Linux and Backtrack compatible wireless network adapters in the link above, or you can grab our most popular adapter for beginners here.

Check out our post on picking the best adapter for Wi-Fi hacking! *Image by SADMIN/Null Byte*

First of all, aircrack-ng is not a single tool, but rather a suite of tools for manipulating and cracking Wi-Fi networks. Within this suite, there is a tool called **aircrack** for cracking passwords, but to get to the cracking we need to do several steps using other tools. In addition, aircrack-ng is capable of doing DOS attacks as well rogue access points, caffe latte, evil twin, and many others.

So, let's get started with the aircrack-ng suite!

Quick Note

The **ng** stands for **new generation**, as aircrack-ng replaces an older suite called **aircrack** that is no longer supported.

Step 1Iwconfig

Before we get started with aircrcak-ng, we need to make certain that BackTrack recognizes your wireless adapter. We can do this within any Linux system by typing:

bt > iwconfig

We can see here that BackTrack recognizes my USB wireless card, and it tells me that it's capable of 802.11bgn, that the ESSID is off, that the mode is managed, etc.

Okay, now we're ready to start using aircrack-ng.

Step 2Airmon-Ng

The first tool we will look at and need in nearly ever WiFi hack is **airmon-ng**, which converts our wireless card into a promiscuous mode wireless card. Yes, that means that our wireless card will hookup with anyone!

Well, that's almost correct. When our network card is in promiscuous mode, it means that it can see and receive all network traffic. Generally, network cards will only receive packets intended for them (as determined by the MAC address of the NIC), but with airmon-ng, it will receive all wireless traffic intended for us or not.

We can start this tool by typing **airmon-ng**, the **action** (start/stop), and then the **interface** (mon0):

bt > airmon-ng start wlan1

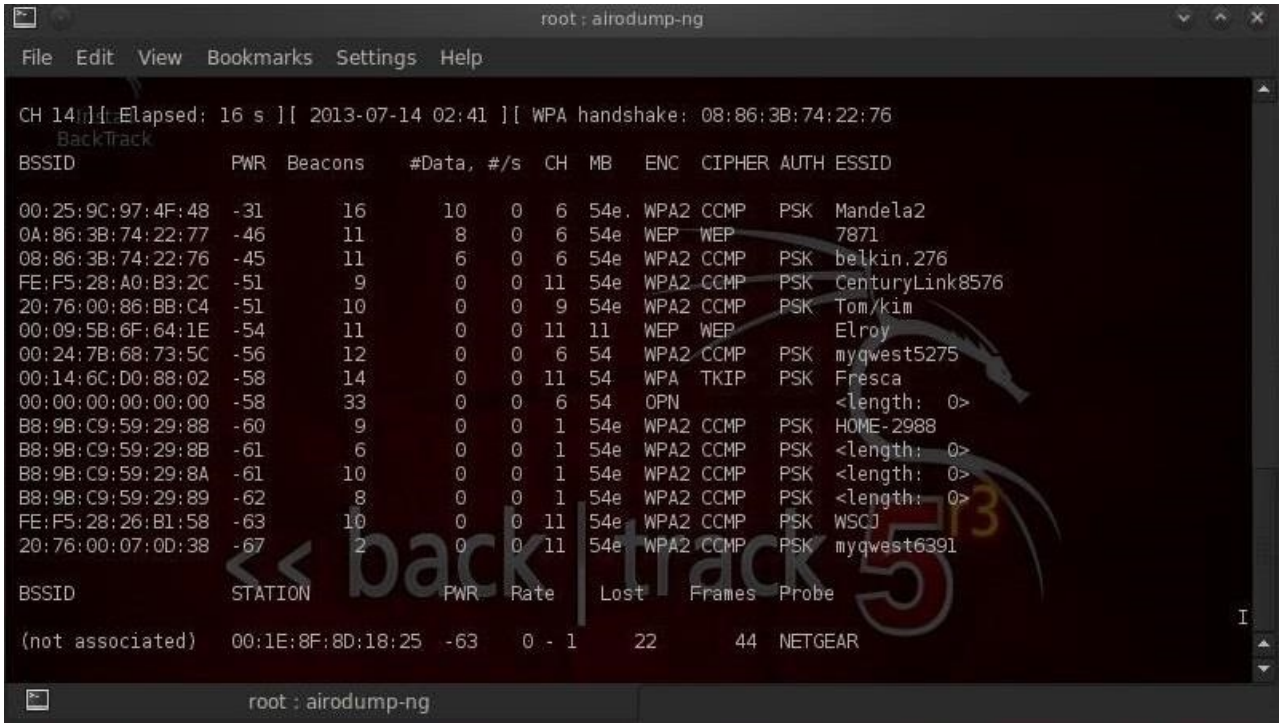
Airmon-ng responds with some key information on our wireless adapter including the chipset and driver. Most importantly, note that it has changed the designation for our wireless adapter from wlan1 to mon0.

Step 3Airodump-Ng

The next tool in the aircrack-ng suite that we will need is **airodump-ng**, which enables us to capture packets of our specification. It's particularly useful in password cracking.

We activate this tool by typing the **airodump-ng** command and the **renamed monitor interface** (mon0):

bt >airodump-ng mon0



As we can see in the screenshot above, airodump-ng displays all of the APs (access points) within range with their BSSID (MAC address), their power, the number of beacon frames, the number of data packets, the channel, the speed, the encryption method, the type of cipher used, the authentication method used, and finally, the ESSID.

For our purposes of hacking WiFi, the most important fields will be the BSSID and the channel.

Step 4Aircrack-Ng

Aircrack-ng is the primary application with the aircrack-ng suite, which is used for password cracking. It's capable of using statistical techniques to crack WEP and dictionary cracks for WPA and WPA2 after capturing the WPA handshake.

Step 5Aireplay-Ng

Aireplay-ng is another powerful tool in our aircrack-ng arsenal, and it can be used to generate or accelerate traffic on the AP. This can be especially useful in attacks like a deauth attack that bumps everyone off the access point, WEP and WPA2 password attacks, as well as ARP injection and replay attacks.

Aireplay-ng can obtain packets from two sources:

1. A live stream of packets, or
2. A pre-captured pcap file

The pcap file is the standard file type associated with packet capture tools like libpcap and winpcap. If you've ever used Wireshark, you've most likely worked with pcap files.

We can see in the screenshot above of the first half of the aireplay-ng help screen, that aireplay can filter by the BSSID of the access point, the MAC address of either source or destination, the minimum and maximum packet length, etc. If we scroll down the help screen, we can see some of the attack options using aireplay-ng:

These include deauth, fake deauth, interactive, arpreplay (necessary for fast WEP cracking), chopchop (a form of statistical technique for WEP packet decrypting without cracking the password), fragment, caffe latte (attacking the client side), and others.

These four tools in the aircrack-ng suite are our Wi-Fi hacking work horses. We'll use each of these in nearly every Wi-Fi hack. Some of our more hack-specific tools include airdecap-ng, airtun-ng, airolib-ng and airbase-ng. Let's take a brief look at each of

these.

Step 6Airdecap-Ng

Airdecap-ng enables us to decrypt wireless traffic once we have cracked the key. In other words, once we have the key on the wireless access point, not only can we use the bandwidth on the access point, but with airdecap-ng we can decrypt everyone's traffic on the AP and watch everything they're doing (the key is used for both access and for encryption).

Step 7Airtun-Ng

Airtun-ng is a virtual tunnel interface creator. We can use airtun-ng to set up an IDS on the wireless traffic to detect malicious or other traffic on the wireless access point. So, if we're looking to get an alert of a particular type of traffic (see my tutorial on creating a PRISM-like spy tool), we can use airtun-ng to set up a virtual tunnel that connects to an IDS like Snort to send us alerts.

Step 8Airolib-Ng

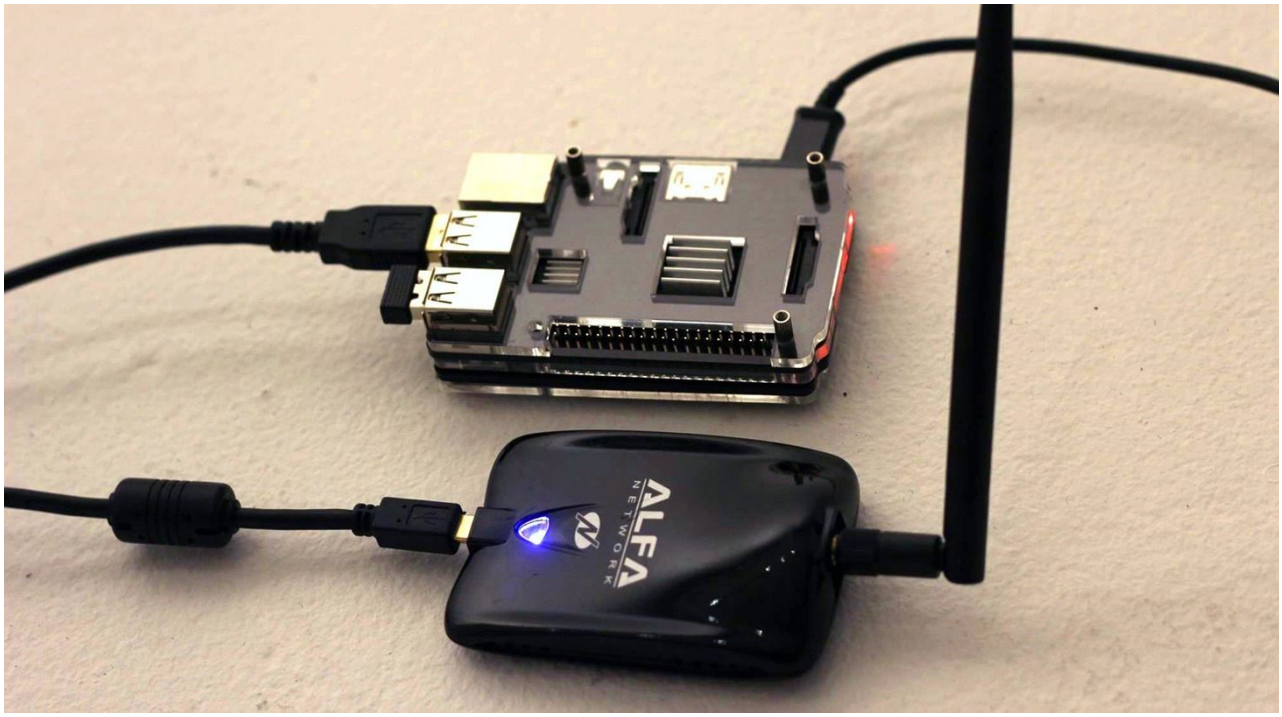
Airolib-ng stores or manages ESSID's (the name of the access point) and password lists that will help speed up WPA/WPA2 password cracking.

Step 9Airbase-Ng

Airbase-ng enables us to turn our laptop and wireless card into an AP. This can be especially useful when doing a rogue access point or evil twin attacks. Basically, airbase-ng allows us to attack the clients, rather than the AP, and encourages the clients to associate with us rather than the real AP.

That's It for Now

These are the primary tools in the aircrack-ng suite that we'll be using as we explore Wi-F hacking. There are other tools, but these are the ones we'll be focusing on. If you're looking for a cheap, handy platform to get started working with aircrack, check out our Kali Linux Raspberry Pi build using the $35 Raspberry Pi.



Aircrack-ng works great on the Kali Linux Raspberry Pi.*Image by SADMIN/Null Byte*

Aerial symbol and Wireless router photos via Shutterstock