

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 1lwconfig

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

bt > iwconfig



```
root: bash
File Edit View Bookmarks Settings Help
root@bt:~# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

root@bt:~# iwconfig
lo          no wireless extensions.

wlan1       IEEE 802.11bgn  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated  Tx-Power=0 dBm
            Retry  long limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:on
eth0        no wireless extensions.

root@bt:~#
```

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 every 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** (mono):

bt > airmon-ng start wlan1



```
root@bt:~# airmon-ng start wlan1
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
root@bt:~# airmon-ng start wlan1
Found 1 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
1650     dhclient3

Interface      Chipset      Driver
wlan1          Ralink RT2870/3070  rt2800usb - [phy0]
               (monitor mode enabled on mon0)
root@bt:~#
```

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 mono.

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** (mono):

bt > airodump-ng mono

```

root : airodump-ng
File Edit View Bookmarks Settings Help
CH 14 Elapsed: 16 s | 2013-07-14 02:41 | WPA handshake: 08:86:3B:74:22:76
BackTrack
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:25:9C:97:4F:48 -31 16 10 0 6 54e WPA2 CCMP PSK Mandela2
0A:86:3B:74:22:77 -46 11 8 0 6 54e WEP WEP 7871
08:86:3B:74:22:76 -45 11 6 0 6 54e WPA2 CCMP PSK belkin.276
FE:F5:28:A0:B3:2C -51 9 0 0 11 54e WPA2 CCMP PSK CenturyLink8576
20:76:00:86:BB:C4 -51 10 0 0 9 54e WPA2 CCMP PSK Tom/kim
00:09:5B:6F:64:1E -54 11 0 0 11 11 WEP WEP Elroy
00:24:7B:68:73:5C -56 12 0 0 6 54 WPA2 CCMP PSK myqwest5275
00:14:6C:D0:88:02 -58 14 0 0 11 54 WPA TKIP PSK Fresca
00:00:00:00:00:00 -58 33 0 0 6 54 OPN <length: 0>
B8:9B:C9:59:29:88 -60 9 0 0 1 54e WPA2 CCMP PSK HOME-2988
B8:9B:C9:59:29:8B -61 6 0 0 1 54e WPA2 CCMP PSK <length: 0>
B8:9B:C9:59:29:8A -61 10 0 0 1 54e WPA2 CCMP PSK <length: 0>
B8:9B:C9:59:29:89 -62 8 0 0 1 54e WPA2 CCMP PSK <length: 0>
FE:F5:28:26:B1:58 -63 10 0 0 11 54e WPA2 CCMP PSK WSCJ
20:76:00:07:0D:38 -67 2 0 0 11 54e WPA2 CCMP PSK myqwest6391
BSSID STATION PWR Rate Lost Frames Probe
(not associated) 00:1E:8F:8D:18:25 -63 0 - 1 22 44 NETGEAR
root : airodump-ng

```

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.


```
root@bt:~# aireplay-ng --help
Install
Aireplay-ng 1.1 r2178 - (C) 2006-2010 Thomas d'Otreppe
Original work: Christophe Devine
http://www.aircrack-ng.org

usage: aireplay-ng <options> <replay interface>

Filter options:

-b bssid : MAC address, Access Point
-d dmac  : MAC address, Destination
-s smac  : MAC address, Source
-m len  : minimum packet length
-n len  : maximum packet length
-u type  : frame control, type field
-v subt  : frame control, subtype field
-t tods  : frame control, To DS bit
-f fromds : frame control, From DS bit
-w iswep : frame control, WEP bit
-D       : disable AP detection

Replay options:

-x nbpps : number of packets per second
```

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:

```
Source options:
Install
-b interface : capture packets from this interface
-r file      : extract packets from this pcap file

Miscellaneous options:

-R           : disable /dev/rtc usage
--ignore-negative-one : if the interface's channel can't be determined,
                        ignore the mismatch, needed for unpatched cfg80211

Attack modes (numbers can still be used):

--deauth      count : deauthenticate 1 or all stations (-0)
--fakeauth    delay : fake authentication with AP (-1)
--interactive  : interactive frame selection (-2)
--arpreply    : standard ARP-request replay (-3)
--chopchop    : decrypt/chopchop WEP packet (-4)
--fragment    : generates valid keystream (-5)
--caffe-latte  : query a client for new IVs (-6)
--cfrag       : fragments against a client (-7)
--migmode     : attacks WPA migration mode (-8)
--test        : tests injection and quality (-9)

--help        : Displays this usage screen
```

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 6 Airdecap-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 7 Airtun-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 8 Airolib-Ng

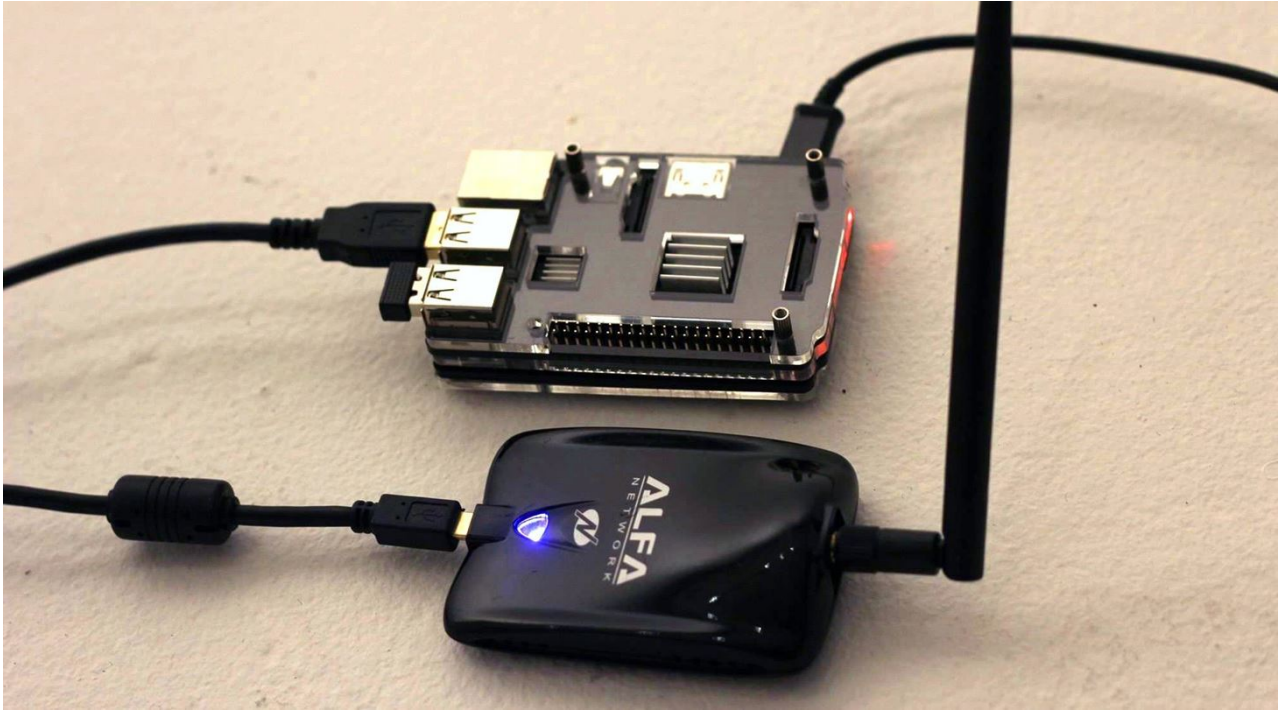
Airolib-ng stores or manages ESSID's (the name of the access point) and password lists that will help speed up WPA/WPA2 password cracking.

Step 9 Airbase-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-Fi 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