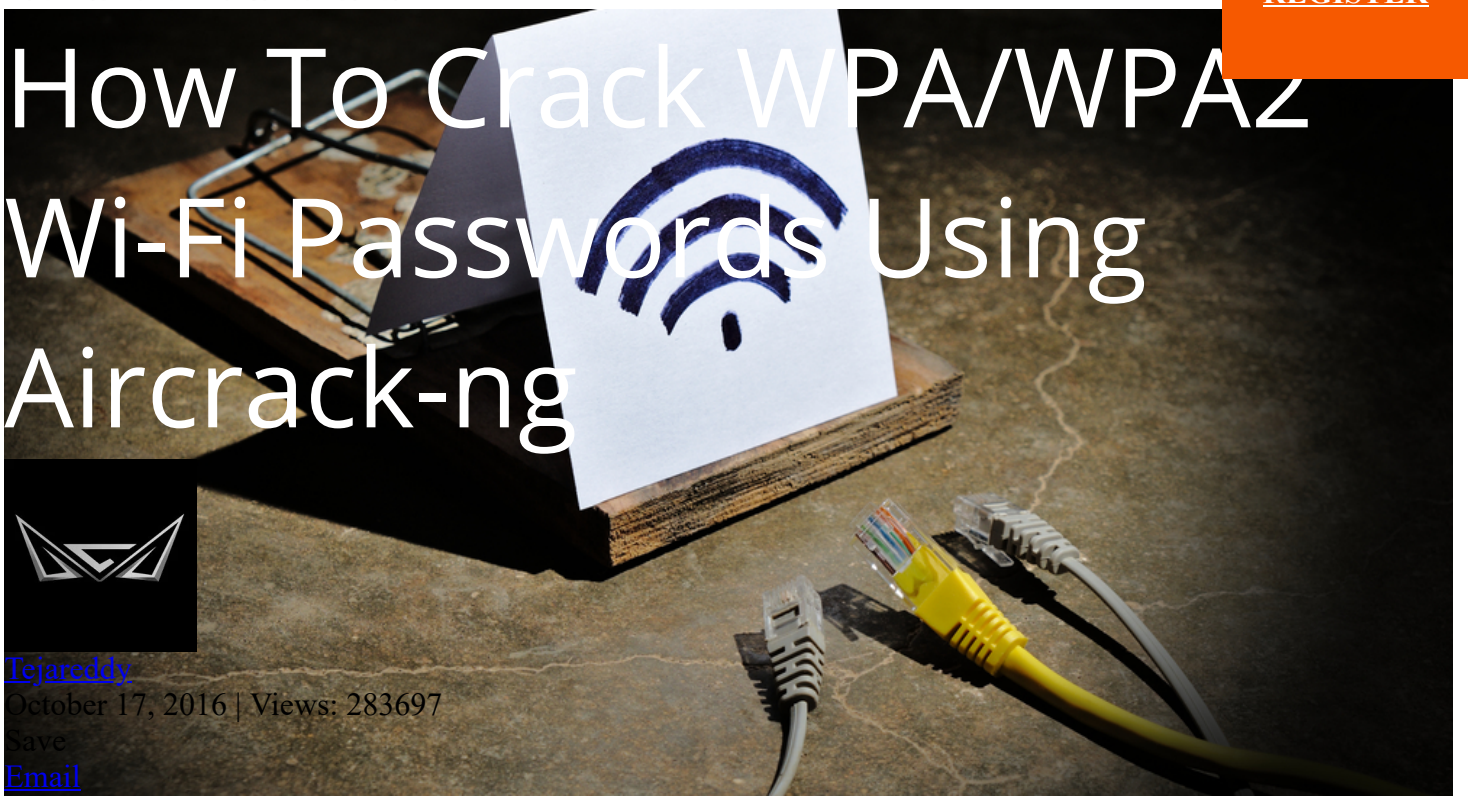
How To Crack WPA/WPA2 Wi-Fi Passwords Using Aircrack-ng



Tejareddy
October 17, 2016 | Views: 283697

Begin Learning Cyber Security for FREE Now!

In this post I will tell you how to crack wpa/wpa2 wi-fi in kali linux using aircrack-ng. To do this, first you should install kalinux or you can use live kali linux.
To make a kali-linux bootable **click here.**
To crack Wi-Fi, first, you need a computer with kali linux and a wireless card which supports monitor/injection mode. If your wireless card is not able to do this, you need to get an external wireless card which is capable of monitor/injection mode.

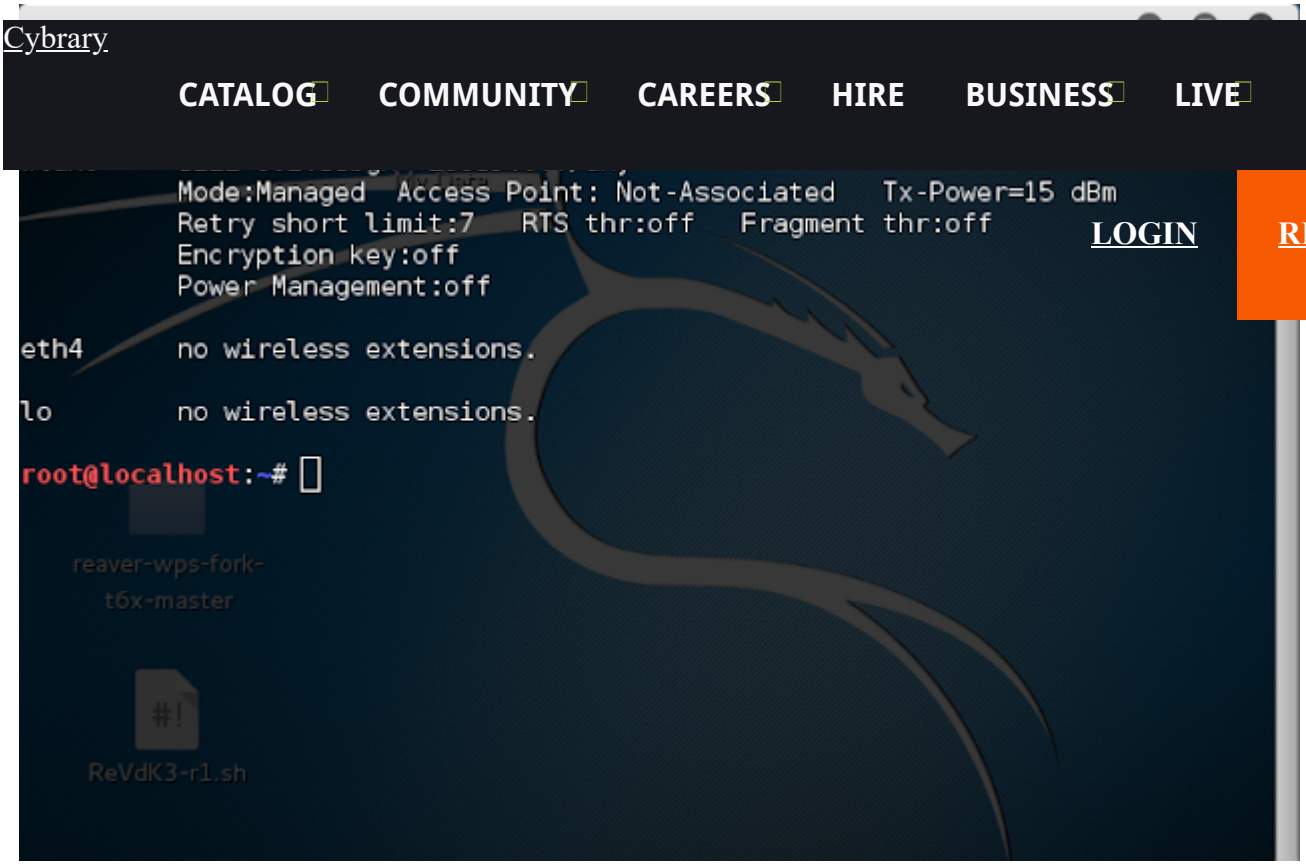
Apart from these tools, you need to have a word-list to crack the password from the captured packets.

First you need to understand how Wi-Fi works. Wi-Fi transmits signal in the form of packets in air so we need to capture all the packets in air so we use airodump to dump all the packets in air .After that we should see that if any one is connected to the victim Wi-Fi. If anyone is not connected the Wi-Fi, cracking is not possible as we need a wpa handshake. We can capture handshake by sending deauthentication packets to client connected to Wi-Fi. Aircrack cracks the password.

Step-1:-

First open terminal. We need to know the name of the wireless adapter connected to the computer because computer has many adapters connected.

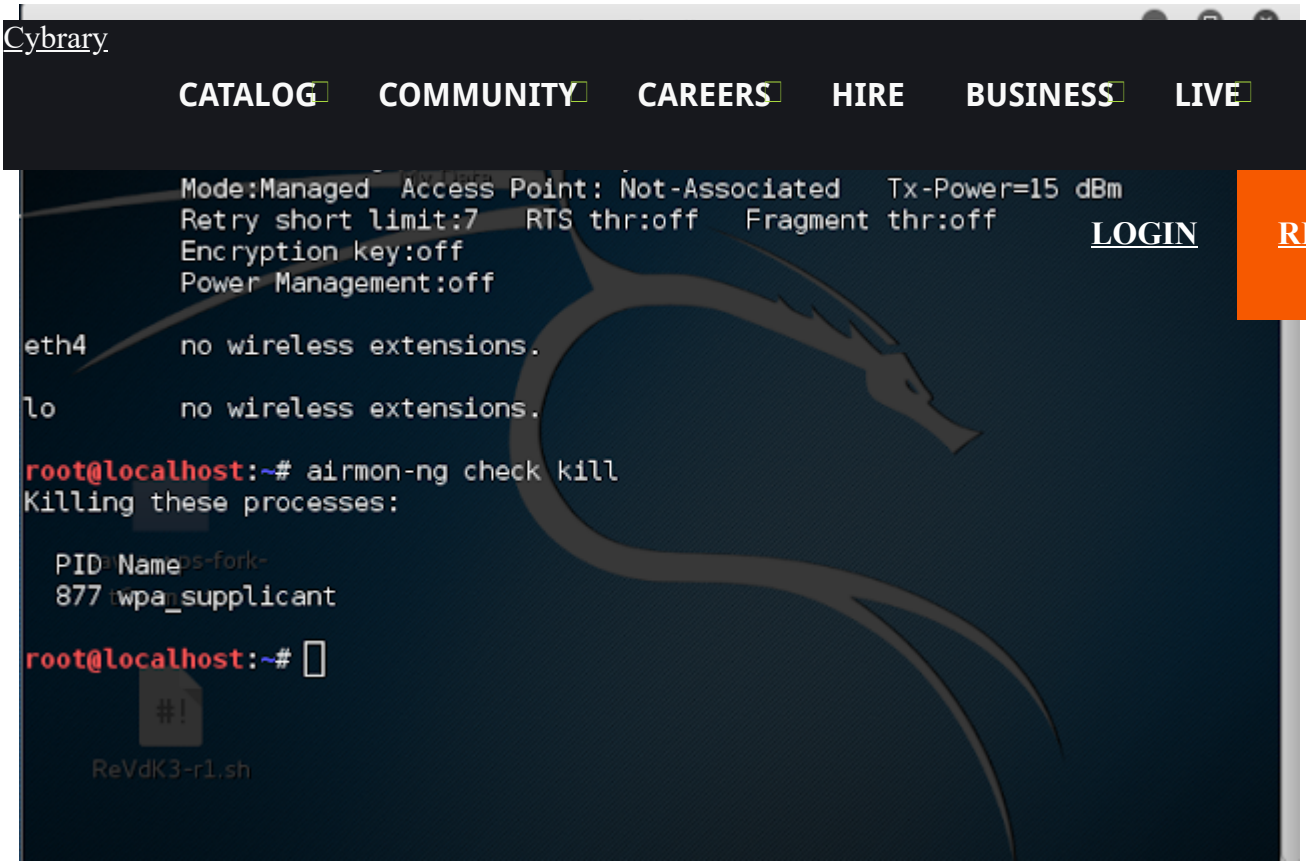
command for this is **iwconfig.**



In my case, my wireless adapter is with the name wlan0. In your case, it may be different. If connected to an external wireless card, it may be wlan1or2.

Step-2:-

For some wireless cards, it gives error messages to enable monitor mode on wireless cards. For that, you should use **airmon-ng check kill.**

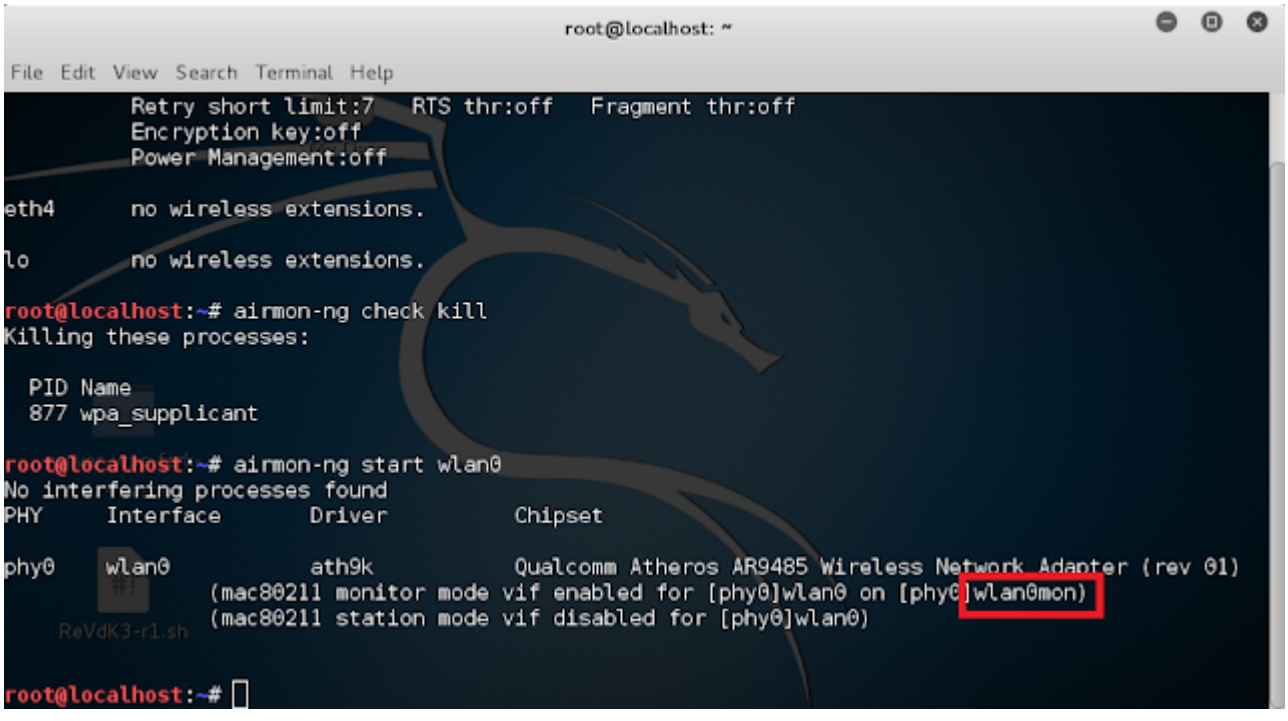


step-3:-

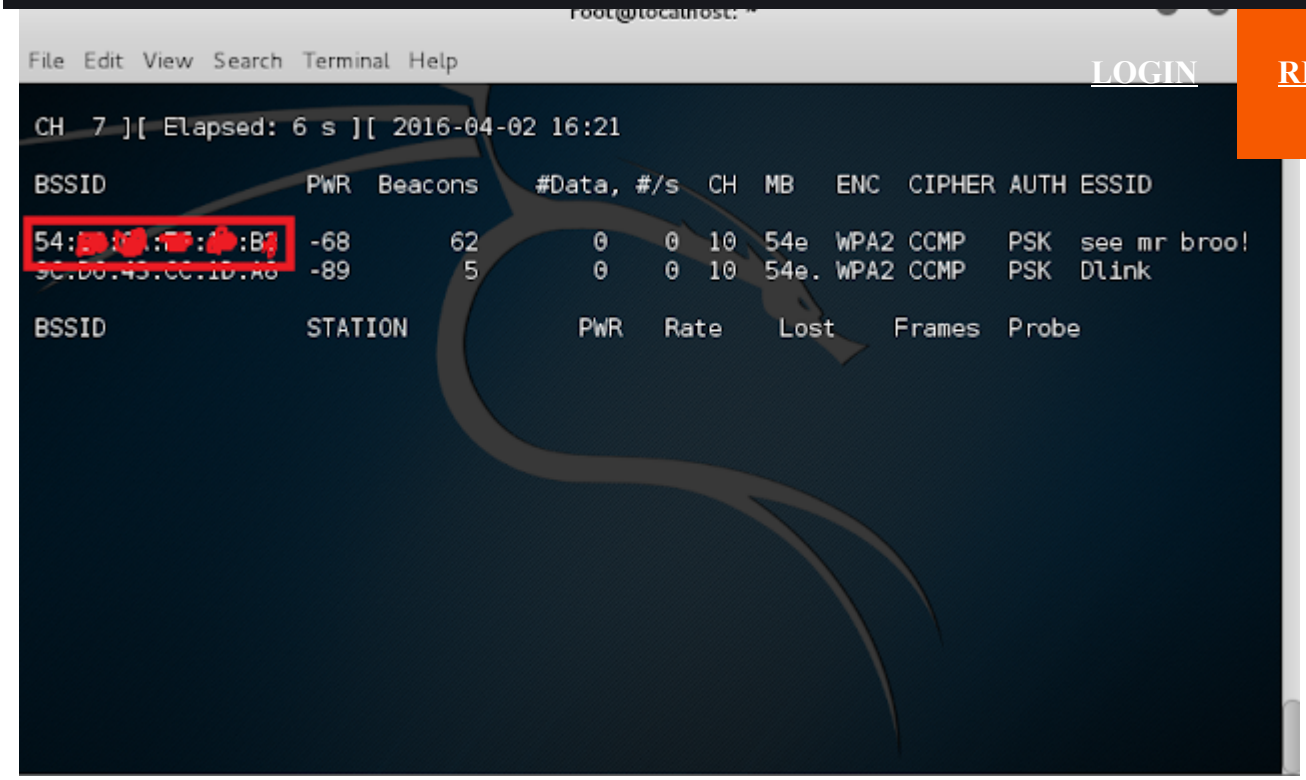
In this step, you need to enable the monitor mode on the wireless card. The command is as follows:

airmon-ng start wlan0(interface of wireless card).

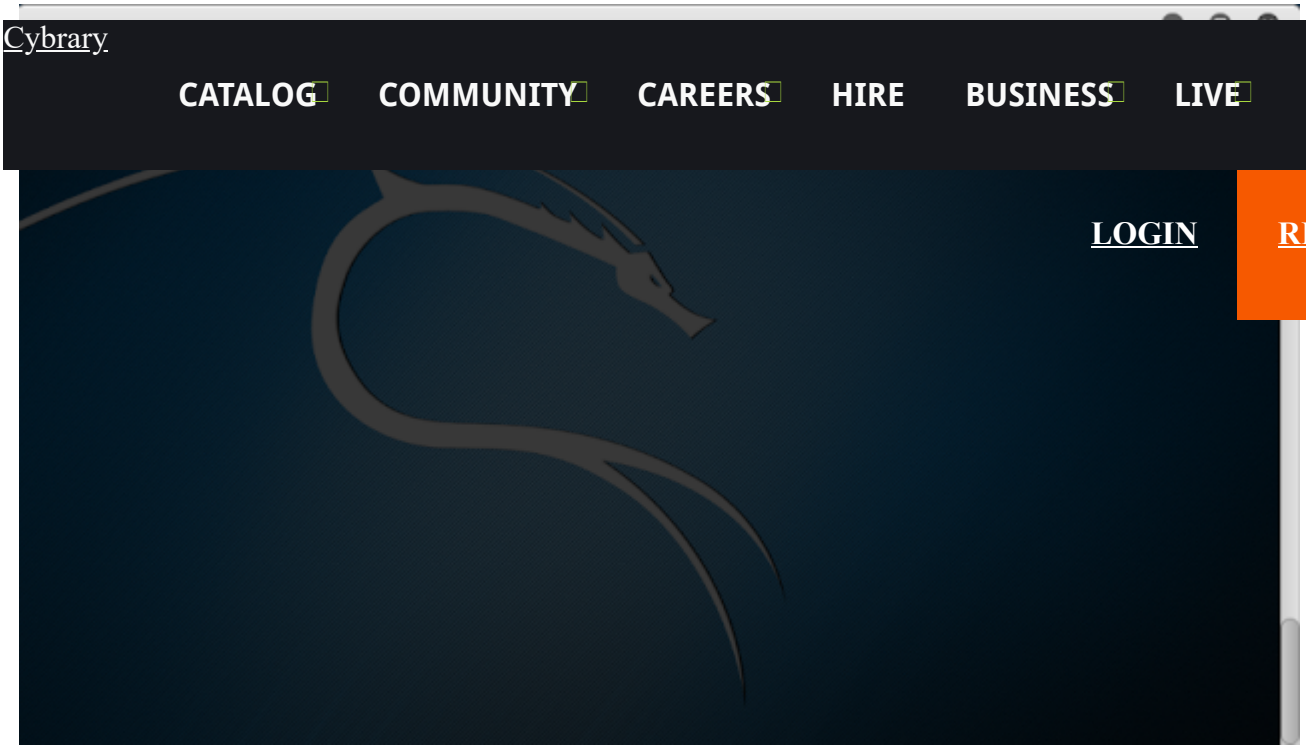
Now this command will enable the monitor mode on the wifi card. So while using interface in any terminal or command line use wlan0mon.



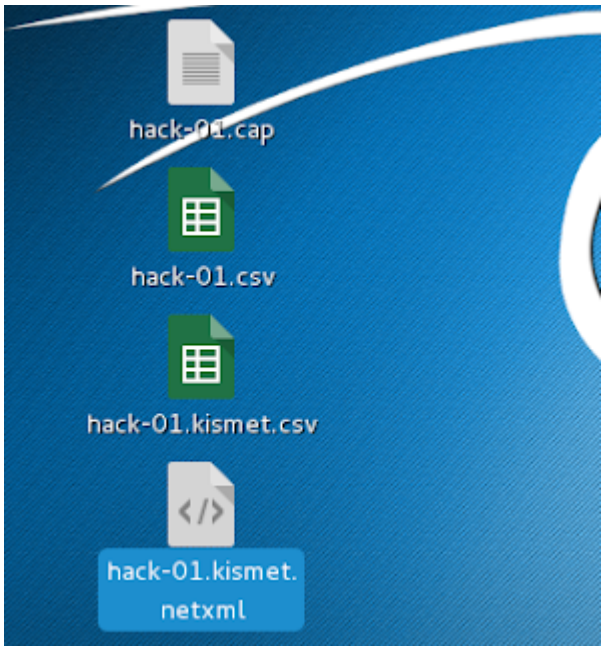
Note:You should use the interface which is indicated with red mark.



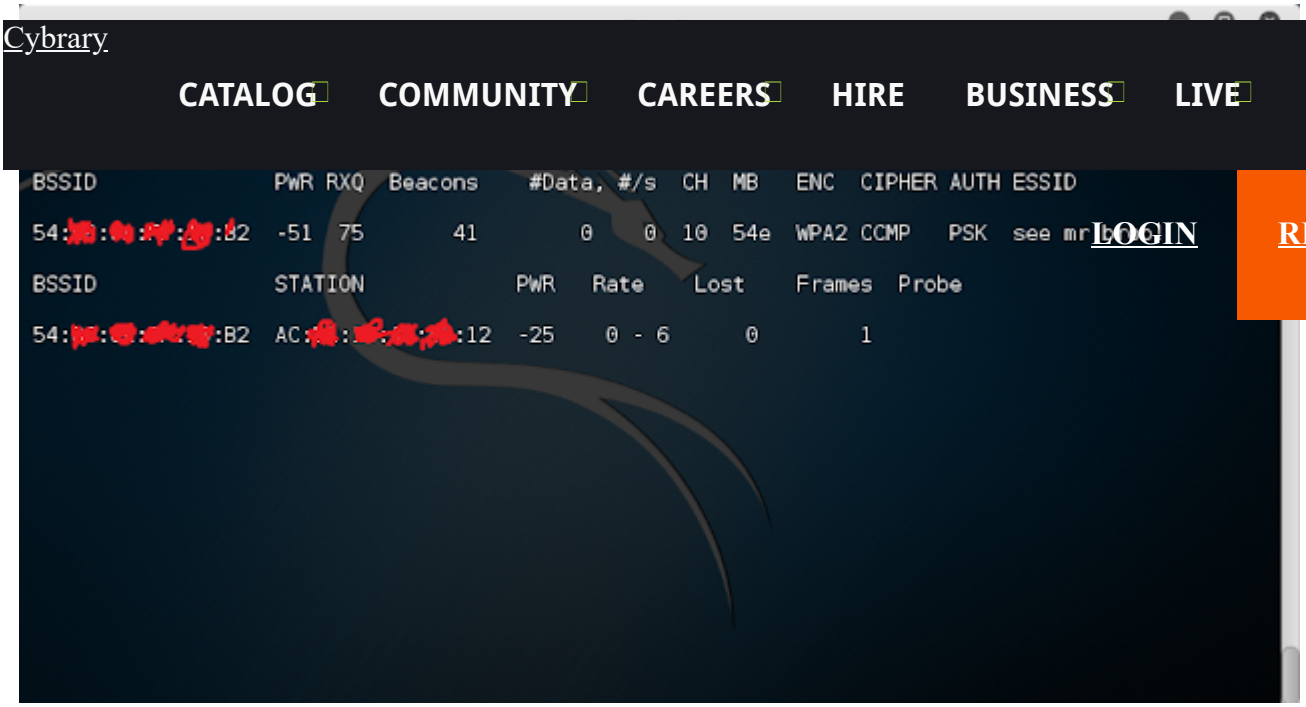
Now this command captures the packets in the air. This will gather data from the wireless packets in the air.
Note:Do not close this terminal. This will be used to know wpa has been captured or not.
step-5:-
In this step we will add some parameters to airodump-ng.
command is **airodump-ng -c channel –bssid [bssid of wifi] -w [path to write the data of packets] wlan0mon[interface].**
-bssid in my case bssid is indicated with red mark.
-c channel is the channel of victim wifi in my case it is 10(see in previous screenshot for channel number)
-w It is used to write the captured data to a specified path in my case it is '**/root/Desktop/hack'.**
Interface in my case is wlan0mon.



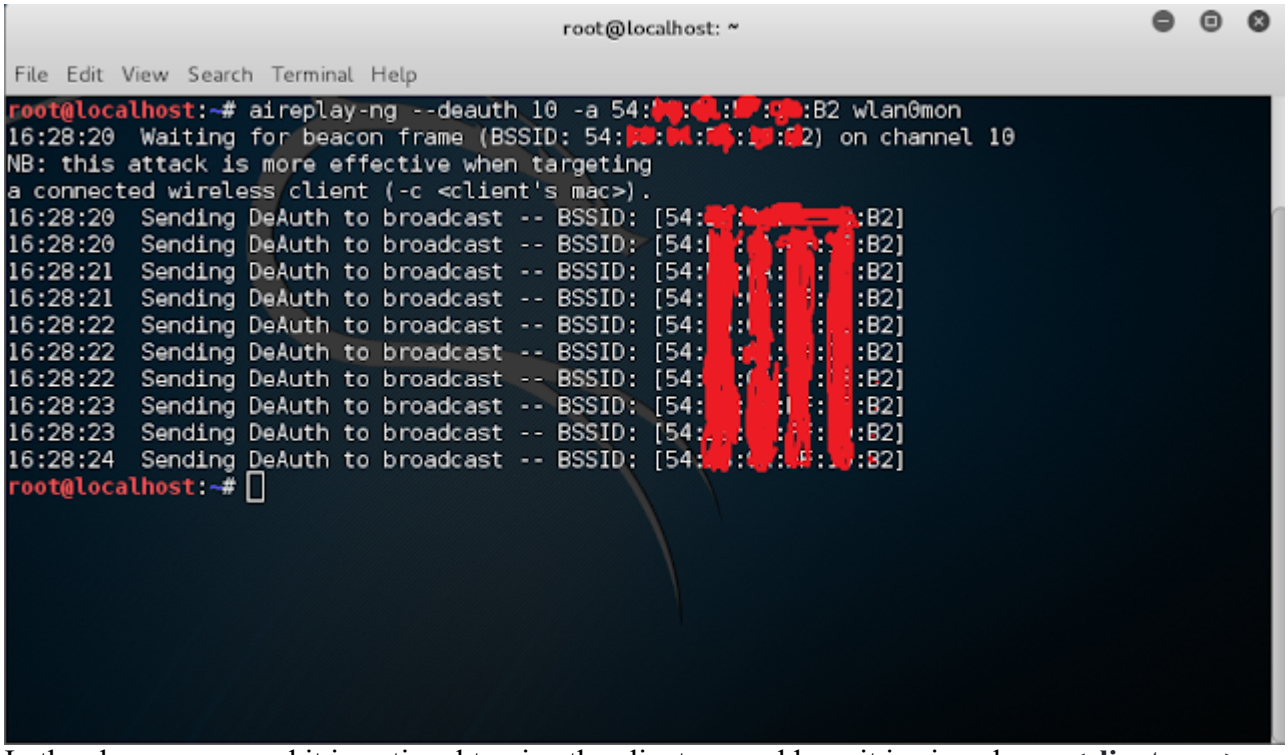
In the above command the path /root/Desktop/hack hack is the name of the file to be saved.



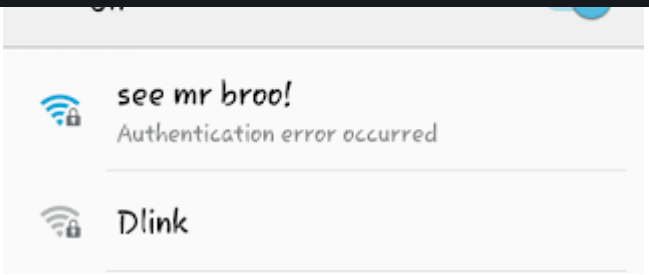
Above command displays this terminal.



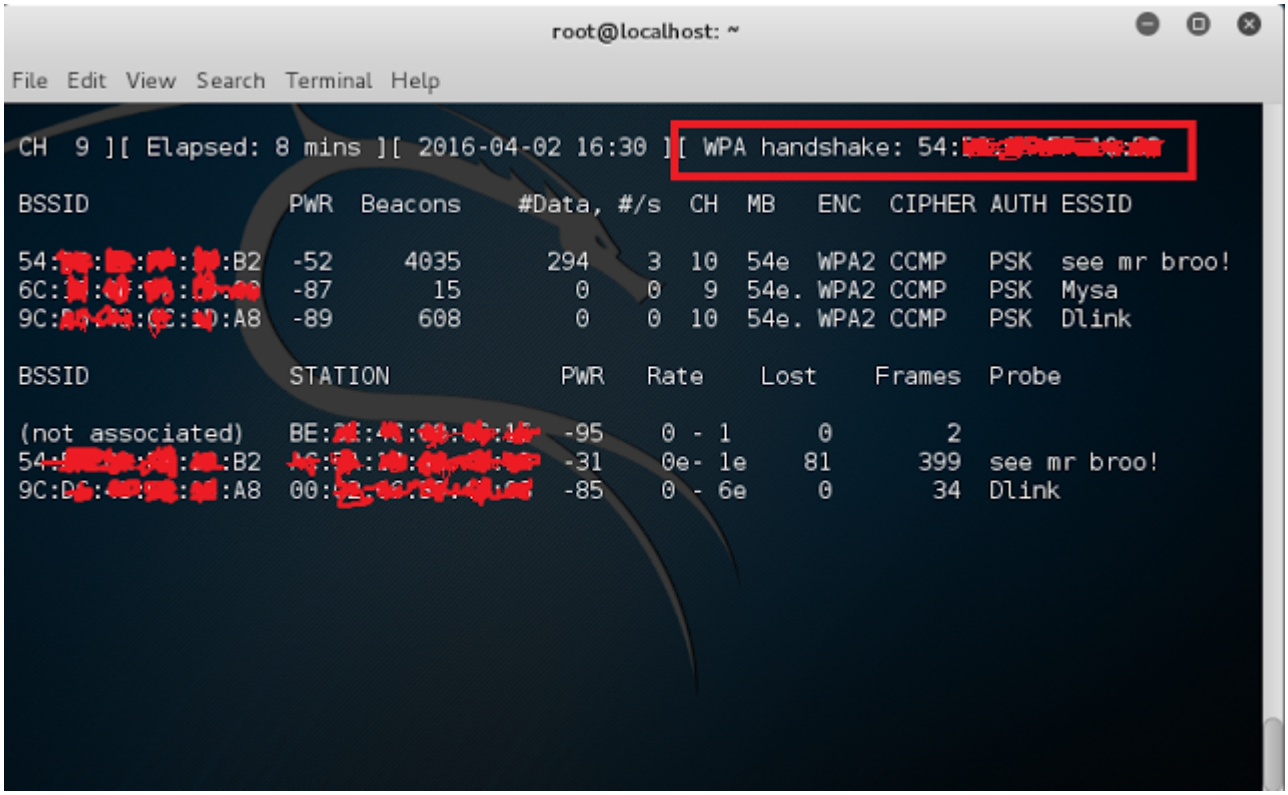
step-6
In this step we deauthenticate the connected clients to the Wi-Fi.
The command is **aireplay-ng –deauth 10 -a [router bssid] interface**



In the above command it is optional to give the client mac address it is given by **-c <client mac>**
This will disconnects the client from access point.
Screen shot of a client connected to access point.



After this the client tries to connect to the Wi-Fi again. At that time, we will capture the packets which sends from client. From this result, we will get wpa handshake.



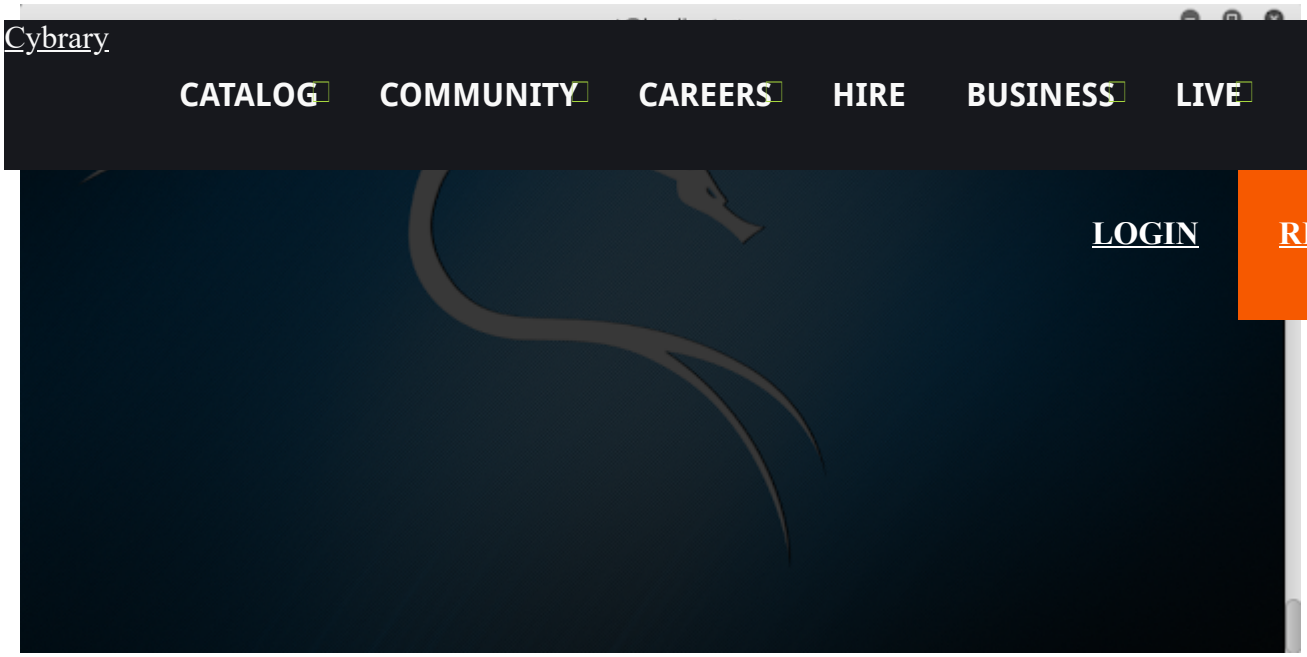
step-7:-

Now we should start cracking the Wi-Fi with captured packets command for this is

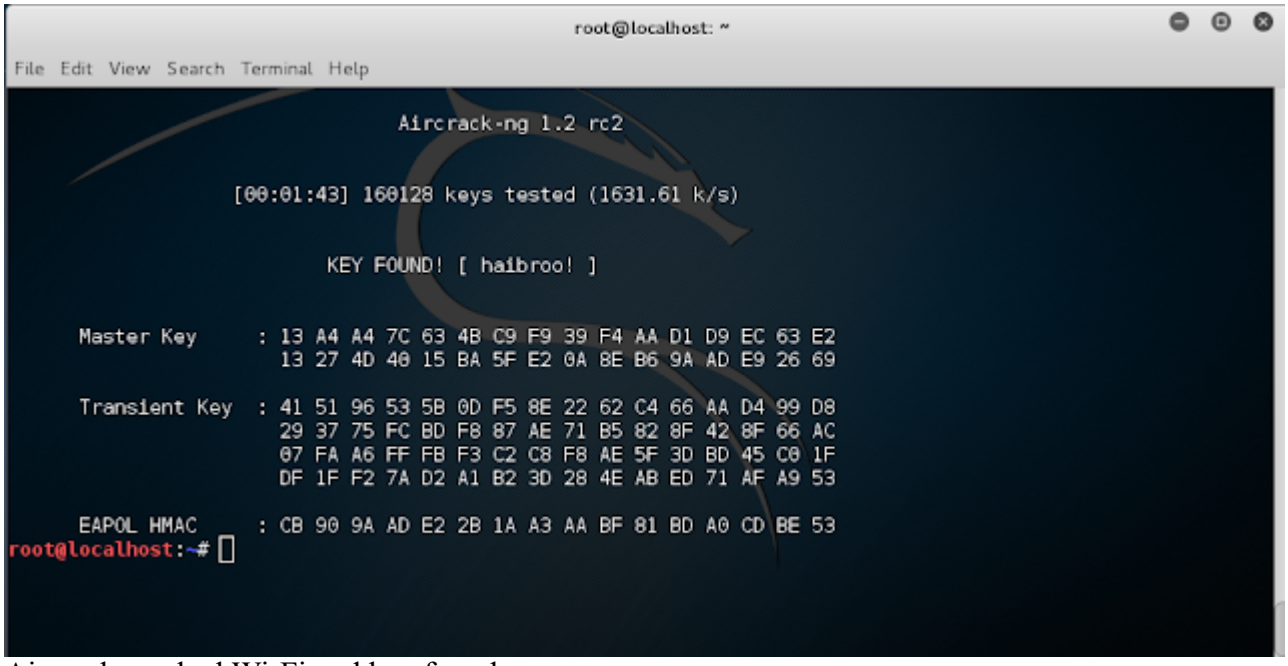
aircrack-ng -b [bssid of router] -w [path to word list] [path to capture packets]

-w path to word list in my case it is '**/root/Desktop/wordlist.txt**'

If you did not have word list, get one. If you want to generate your custom wordlist, you can visit our other post: How generate word list using crunch.



Now press enter aircrack will start cracking the Wi-Fi.



Aircrack cracked Wi-Fi and key found.

Note:To use this method you need to have wordlist compulsory there are many wordlists available in internet you can download them.

This is my previous post on How To Create the Word list Click Here

Leave a comment below in comment section if you have any related queries.

Share with Friends

Use Cybytes and
Tip the Author!
Join
Share with Friends

20 Comments

1. 

   nishanth97
   6:06 am on January 30, 2018

   How to create and download world list?

   Log in to Reply

   - 

     nerkxei
     1:47 am on March 9, 2018

     Hey, Use CUPP. It can generate a wordlist based of your target, for example i went to the swimming pool yesterday, and in the lobby i made a wordlist using cupp. The password was in the list (Uszoda2009) Uszoda means swimming pool in my laungage btw. Cupp is powerful!

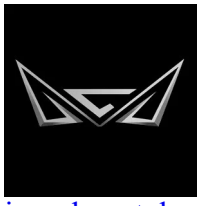
     Log in to Reply

2. 

   santymaan
   1:30 am on July 16, 2017

   Great post here is another post about WPA wifi hacking

   Log in to Reply

3. 

   joseph metobo
   4:21 am on February 26, 2017

Does this only work with mac laptops?

Mantis
11:09 pm on December 24, 2016

Can this be done on the 5ghz band?

Log in to Reply

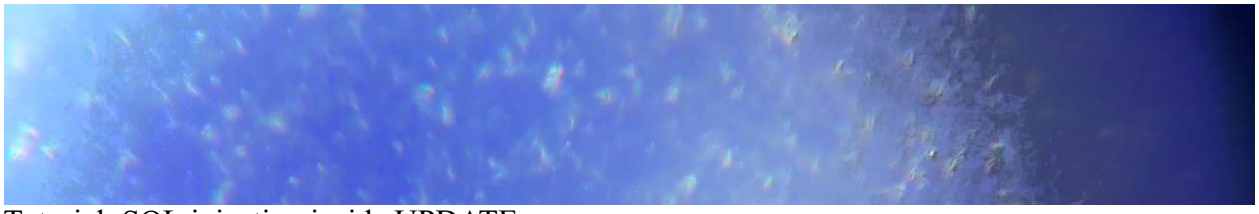
Page 2 of 2 « 1 2

Comment on This

You must be logged in to post a comment.

Related Reads
Hacking WPS via Pixie Dust Attack

April 22, 2016
By: Joshua H.
61878



Tutorial: SQL injection inside UPDATE query

September 15, 2016
By: danielkhaoticen
8824

Blender Case Study: FinTech Drops The Box

February 9, 2017
By: Cato Networks
625

Binge Read Our Pen Testing Active Directory Series

February 8, 2017
By: Varonis
420