**WIFI HACKING**

# TOOLS REQUIRED:

Network adapter

Kali Linux machine

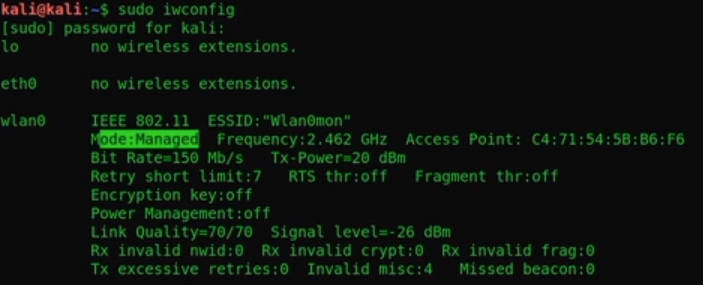
To hack or to know a wifi password ensure that you have network adapter. A network adapter is a piece of hardware that acts as an interface for a computer to a network. An external adapter has two modes. Firstly the manage mode which allows you to manage only one connection. Secondly the monitor mode by which we can monitor the surroundings and hackers have multiple routers as option.

To hack a wifi password the following steps are to be followed.

* Using monitor mode setup a target router
* Know how many connections are available in his target router
* Wait for a device to connect
* When the device is connecting, a session key will be created, note the session key
* Create a dictionary password list
* Compare the session key with dictionary password list
* Get the password!!!

# STEP 1:

Open kali Linux and use “iwconfig” command in terminal. You will see that it is in the manage mode.



Convert it to monitor mode using the command



Recheck if the mode has been converted. Then use the below code to monitor the signals around you



Then decide on which wifi to hack.

# STEP 2:

Discover the devices connected your target. Capture the packages or the data that are given to the devices and store it use the below code. This will let you know the devices connected



Target BSS ID

# STEP 3:

Wait for a device to get connected. You can also disconnect a device and wait for the device to reconnect. While reconnecting that is after typing the password, authentication starts during which a session key is created.

To send a de-authentication packages to the connected devices use the code



This disconnects the router and the device and the device has to reconnect again

# STEP 4:

When the device reconnects you will be able to capture the session key. Multiple session keys can be recorded if multiple devices are disconnected. To ensure that the session keys are really captured use the below line for assurance.



File name

This will show many packages. But to view only authentication packages you can use the command “eapol”. This will show you the authentication packages

# STEP 5:

Once authentication packages are recorded, you should create a dictionary password list with which you will be able to compare and get the password. To create this you can use crunch. Crunch displays various combinations of numerical, alphabets and symbols. A wifi password has an upper and lower limit has 8 and setting the password length as 8 you will be able to see various password combinations. Store in a file.



Use –O test.txt to save it in a file

# STEP 6:

Compare your session key file with your dictionary password list file using the below line



Session key file password list file path

# STEP 7:

VOILA!!! You got your password….