How to Hack WiFi Password ?

First of all you need to scan for available wireless networks.
you can use"NetStumbler" or "Kismet" for Windows and Linux and
KisMac for Mac. It'll also show how the Wi-fi network is encrypted. The two most common encryption techniques are:
1) WEP (Wire Equivalent Privacy)
2) WAP(Wireless Application Protocol)

WEP allows a hacker to crack a WEP key easily whereas WAP is currently
the most secure and best option to secure a wi-fi network It can't be easily cracked as WEP
because the only way to retreive a WAP key is to use a brute-force attack or dictionary atack.
How to Crack WEP To crack WEP we will be using Live Linux distribution called BackTrack
to crack WEP....Posted by #anoop

BackTrack have lots of preinstalled softwares but for this time
The tools we will be using on Backtrack are:

a)Kismet – a wireless network detector
b)airodump – captures packets from a wireless router
c)aireplay – forges ARP requests
d)aircrack – decrypts the WEP keys

Follow the steps One by One
1) First of all we have to find a wireless access point along with its
bssid, essid and channel number. To do this we will run kismet by
opening up the terminal and typing in kismet. It may ask you for the
appropriate adapter which in my case is ath0. You can see your
device's name by typing in the command iwconfig.

2) To be able to do some of the later things, your wireless adapter
must be put into monitor mode. Kismet automatically does this and
as long as you keep it open, your wireless adapter will stay in monitor
mode.

3) In kismet you will see the flags Y/ N/0. Each one stands for a different
type of encryption. In our case we will be looking for access points
with the WEP encryption. Y=WEP N=OPEN 0=OTHER(usually WAP).

4) Once you find an access point, open a text document and paste in
the networks broadcast name (essid) , its mac address (bssid) and its
channel number. To get the above information, use the arrow keys to
select an access point and hit to get more information about it.

5) The next step is to start collecting data from the access

point with airodump. Open up a new terminal and start airodump by typing in the command:

airodump-ng -c [channel#] -w [filename] –bssid [bssid] [device]

In the above command airodump-ng starts the program, the channel of your access point goes after -c , the file you wish to output the data goes after -w , and the MAC address of the access point goes after –bssid. The command ends with the device name. Make sure to leave out the brackets.

6) Leave the above running and open another terminal. Next we will generate some fake packets to the target access point so that the speed of the data output will increase. Put in the following command:

aireplay-ng -1 0 -a [bssid] -h 00:11:22:33:44:55:66 -e [essid][device]

In the above command we are using the airplay-ng program. The -1 tells the program the specific attack we wish to use which in this case is fake authentication with the access point. The 0 cites the delay between attacks, -a is the MAC address of the target access point, -h is your wireless adapters MAC address, -e is the name (essid) of the target access point, and the command ends with the your wireless adapters device name.

7) Now, we will force the target access point to send out a huge amount of packets that we will be able to take advantage of by using them to attempt to crack the WEP key. Once the following command is executed, check your airodump-ng terminal and you should see the ARP packet count to start to increase. The command is:

aireplay-ng -3 -b [bssid] -h 00:11:22:33:44:5:66 [device]

In this command, the -3 tells the program the specific type of attack which in this case is packet injection, -b is the MAC address of the target access point, -h is your wireless adapters MAC address, and the wireless adapter device name goes at the end.

Once you have collected around 50k-500k packets, you may begin the attempt to break the WEP key. The command to begin the cracking process is:

aircrack-ng -a 1 -b [bssid] -n 128 [filename].ivs

In this command the -a 1 forces the program into the WEP attack mode, the -b is the targets MAC address,and the -n 128 tells the program the WEP key length. If you don't know the -n , then leave it out. This should crack the WEP key within seconds. The more packets you capture, the bigger chance you have of cracking the WEP key.

Download backtrack iso file and make bootable usb and you can plug and play backtrack easily Hit maximum likes n share in this post so I think that u need more...via Technology era

DOWNLOAD BACKTRACK FROM>>>http://www.backtrack-linux.org/downloads/