Hacking WEP wifi passwords

Today there are a lot of available WiFi networks and this tutorial will show you how to crack them!

BEFORE CONTINUING READ OUR DISCALIMER.

Tools Needed.
The ultimate pen testing or hacking OS, BackTrack will suffice, if you are a windows user, it is a lot more complicated, I will post a tutorial when I find out how!

BackTrack 3 or 4.
Download it from http://remote-exploit.org

Selecting your wireless card and setting up.
Open up Konsole in BackTrack(remember this is linux, everything is typed).
Type:
airmon-ng
You will see the name of your wireless card. (mine is named "ath0") From here on out, replace "ath0" with the name of your card.

Now type:
airmon-ng stop ath0
then type:
ifconfig wifi0 down
then:
macchanger --mac 00:11:22:33:44:55 wifi0
then: airmon-ng start wifi0
What these steps do is spoof your mac id so that even if you cannot be traced in case you are caught!

Now it's time to discover some networks to break into
Type: airodump-ng at
Now you will see a list of wireless networks start to populate. Some will have a better signal than others and it is a good idea to pick one that has a decent signal otherwise it will take forever to crack or you may not be able to crack it at all.

Once you see the network that you want to crack, do this: hold down ctrl and tap c
This will stop the display

http://www.hacktohell.org/2011/04/hacking-wep-wifi-passwords.html#_Toc68xQNNs
**Now from here on out, when I tell you to type a command, you need to replace whatever is in parenthesis with what I tell you to from your screen.**

For example: if I say to type: `-c (channel)` then don't actually type in `-c (channel)` Instead, replace that with whatever the channel number is...so, for example you would type: `-c 6` Can't be much clearer than that...lets continue... Now find the network that you want to crack and MAKE SURE that it says the encryption for that network is WEP. If it says WPA or any variation of WPA then move on...you can still crack WPA with backtrack and some other tools but it is a whole other ball game and you need to master WEP first.

Once you've decided on a network, take note of its channel number and bssid. The bssid will look something like this --> 05:59:30:56:92:2n The Channel number will be under a heading that says "CH". Now, in the same Konsole window,

type: `airodump-ng -c (channel) -w (file name) --bssid (bssid) ath0`

the FILE NAME can be whatever you want. This is simply the place that airodump is going to store the packets of info that you receive to later crack. You don't even put in an extension...just pick a random word that you will remember. I usually make mine "wepkey" because I can always remember it.

**Side Note: if you crack more than one network in the same session, you must have different file names for each one or it won't work. I usually just name them wepkey1, wepkey2, etc.**

Once you typed in that last command, the screen of airodump will change and start to show your computer gathering packets. You will also see a heading marked "IV" with a number underneath it. This stands for "Initialization Vector" but in beginner terms all this means is "packets of info that contain clues to the password." Once you gain a minimum of 5,000 of these IVs, you can try to crack the password. I've cracked some right at 5,000 and others have taken over 60,000. It just depends on how long and difficult they made the password.

Now if you are thinking, "I'm screwed because my IV's are going up really slowly." Well, don't worry, now we are going to trick the router into giving us HUNDREDS of IV's per second.

Actually cracking the WEP password

Now leave this Konsole window up and running and open up a 2nd Konsole window. In this one

type: `aireplay-ng -1 0 -a (bssid) -h 00:11:22:33:44:55 ath0`
This will send some commands to the router that basically cause it to associate with your computer even though you are not officially connected with the password. If this command is successful, you should see about 4 lines of text print out with the last one saying something similar to "Association Successful :-)") If this happens, then good! You are almost there. Now type:

```
 aireplay-ng -3 -b (bssid) -h 00:11:22:33:44:55 ath0
```

This will generate a bunch of text and then you will see a line where your computer is gathering a bunch of packets and waiting on ARP and ACK. Don't worry about what these mean...just know that these are your meal tickets. Now you just sit and wait. Once your computer finally gathers an ARP request, it will send it back to the router and begin to generate hundreds of ARP and ACK per second. Sometimes this starts to happen within seconds...sometimes you have to wait up to a few minutes. Just be patient. When it finally does happen, switch back to your first Konsole window and you should see the number underneath the IV starting to rise rapidly. This is great! It means you are almost finished! When this number reaches AT LEAST 5,000 then you can start your password crack. It will probably take more than this but I always start my password cracking at 5,000 just in case they have a really weak password.

Now you need to open up a 3rd and final Konsole window. This will be where we actually crack the password. Type:

```
 aircrack-ng -b (bssid) (filename)-01.cap
```

Remember the filename you made up earlier? Mine was "wepkey". Don’t put a space in between it and -01.cap here. Type it as you see it. So for me, I would type wepkey-01.cap

Once you have done this you will see aircrack fire up and begin to crack the password. Typically you have to wait for more like 10,000 to 20,000 IV's before it will crack. If this is the case, aircrack will test what you've got so far and then it will say something like "not enough IV's. Retry at 10,000." DON'T DO ANYTHING! It will stay running...it is just letting you know that it is on pause until more IV's are gathered. Once you pass the 10,000 mark it will automatically fire up again and try to crack it. If this fails it will say "not enough IV's. Retry at 15,000." and so on until it finally gets it.

If you do everything correctly up to this point, before too long you will have the password! now if the password looks goofy, dont worry, it will still work. some
passwords are saved in ASCII format, in which case, aircrack will show you exactly what characters they typed in for their password. Sometimes, though, the password is saved in HEX format in which case the computer will show you the HEX encryption of the password. It doesn't matter either way, because you can type in either one and it will connect you to the network.

Take note, though, that the password will always be displayed in aircrack with a colon after every 2 characters. So for instance if the password was "hacktohell", it would be displayed as:

```
ha:ck:to:he:ll
```

This would obviously be the ASCII format. If it was a HEX encrypted password that was something like "0FKW9427VF" then it would still display as:

```
0F:KW:94:27:VF
```

Just omit the colons from the password, boot back into whatever operating system you use, try to connect to the network and type in the password without the colons and you are in

This may seem a bit complicated if you are doing this for the first time, you will get used to it
You might like:

- Hack your friend by using BackTrack 5 | Backtrack 5 tutorial
- Hack A computer over LAN via ARP poisoning using BackTrack | Back Track 5 Tutorial
- How to run Back Track 5 in Windows Virtual PC in Windows 7 | Back Track 5 Tutorial - HackToHell
- Remove the facebook Right Sidebar or News Bar ticker

Posted by hackr at 2:17 PM 2 Comments and 0 Reactions

Tag Cloud

- What is java update
- Replacement Window
- Security System
- Learn Java
- 0 apr discover
- What is java

Add New Comment

Optional: Login below.

Showing 2 comments

Sort by Popular now

gowtham ★ 2 months ago

http://www.linuxquestions.org/... this thread , http://www.garage4hackers.com/... this must help you configure it :)

http://www.hacktohell.org/2011/04/hacking-wep-wifi-passwords.html#.To_h6BxQNNs
Xeragon_samuja  2 months ago

i use backtrack5 i type airmon-ng nothing below the interface chipset driver..how? i using laptop

Like  Reply