

Forum:[Hack Forums](#)

Thread: [\[TUT\] How to crack a Wi-Fi password \[TUT\]](#)

Keeper - March 18, 2012, 7:49 am

Hey guys. I now there are a lot of tutorials on wi-fi cracking and especially with Backtrack but one more won't do bad..?

In this tutorial I'll demonstrate how to crack a wireless password with WEP encoding.

Let's get started

For this purpose we are going to use the live cd distribution Backtrack 4 (could use version 5 as well) and some of the applications in it.

Note: You need to go in root first. For this purpose type "su -" and type your password.

Once we've got our Backtrack up and running it's time to open a terminal and pass over to mode monitoring using the following command:

```
# iwconfig wlan0 mode monitoring
```

Note: If some sort of error occurs type "# iwconfig" in a terminal to check for your wireless.

After that it's time to scan for a wireless network which we will compromise with educational purpose. This time we will use the command:

```
# airodump-ng wlan0
```

[img]http://store.picbg.net/pubpic/D5/68/be11f84f0e27d568.jpg[/img]

Once you've found one, abort the process with Ctrl+C. Now when we have got our target it's time to collect some information about the network. First of all copy the MAC Address of the access point which stands for BSSID (should look something like 00:15:EB:E7: ...). Another thing is that we need to know the channel it's currently working on (could see that under CH – e.g. 6). So let's gather our information with airodump-ng.

```
# airodump-ng -w wep -c 6 -bssid 00:15:EB:E7: ... wlan0
```

[img]http://store.picbg.net/pubpic/43/2C/8875fd4ff599432c.jpg[/img]

Now we need to open another terminal in which we will use ARP Reply attack to increase the amount of data packets and gather the initializing vectors or IV of the earlier chosen Access Point.

```
# aireplay-ng -3 -b 00:15:EB:E7: ... wlan0
```

[img]http://store.picbg.net/pubpic/E1/EE/b15c84ed10ebe1ee.jpg[/img]

Let's go to terminal 1 again and have a look at the data packets. We need to have collected over 20 000 packets. If so abort both airodump-ng and aireplay-ng.

Now we have everything required to decode the key of the wireless network. We do that with aircrack as shown below:

```
# aircrack-ng wep-03.cap
```

[img]http://store.picbg.net/pubpic/7C/01/537f3d09952d7c01.jpg[/img]

Then you should see that the key has been decrypted 100% successfully and the key itself.

GeeMann - March 18, 2012, 10:23 pm

Perhaps you should also mention that when attempting to access the network the "Key Found" should not contain any :

Bloodsports - March 21, 2012, 8:51 pm

Thanks alot.. This was use full....!!

ahmedtite1 - March 22, 2012, 5:18 am

Friend do i need a wireless card like alfa

Or can i use this tutrial on any laptop with wireless

I am waiting

Nuuskis - March 22, 2012, 5:36 am

I'm pretty sure that Google will tell you the answer. If you're too lazy to find out yourself, take a screencap from "lspci" command and post it here.

Keeper - March 22, 2012, 6:34 am

(Mar 22, 2012 05:18 AM)ahmedtite1 Wrote: [\[CITE\]](#) Friend do i need a wireless card like alfa
Or can i use this tutrial on any laptop with wireless

I am waiting

It's going to work just fine on a laptop with wireless.

ahmedtite1 - March 22, 2012, 7:11 am

Thank you very muck ...

And we are your wpa , wpa 2 hacking tutrial

Best wishes

Keeper - March 22, 2012, 7:15 am

(Mar 22, 2012 07:11 AM)ahmedtite1 Wrote: [\[CITE\]](#) Thank you very muck ...

And we are your wpa , wpa 2 hacking tutrial

Best wishes

There's a bit of difference with WPA/WPA2 encoding but I will make another tutorial for it soon.

Thanks for the comments!

xSpectrex - March 22, 2012, 1:03 pm

assuming your wireless card supports packet injection. a lot of them dont.

koylis94 - March 23, 2012, 5:23 am

when i get my wireless card i wanna try this!!

Walkers. - March 23, 2012, 4:13 pm

do you have to use a wordlist?

pretty sure that you do?

Keeper - March 24, 2012, 5:44 am

(Mar 23, 2012 04:13 PM)HackerAlert Wrote: [\[CITE\]](#) do you have to use a wordlist?

pretty sure that you do?

Actually, no. Bruteforce using wordlist is for WPA/WPA2 encoded networks.

Tw!st3d - March 24, 2012, 5:50 am

Thanks man, ill try it out as soon as i get home

/TeraByte/ - May 24, 2012, 4:28 pm

This guy is high quality. Don't judge him by his post count

ankr- - May 24, 2013, 4:55 pm

vouch, this method works, I used it to

Spoiler ([Click to View](#))

Hack a Wifi

