

Forum:[Hack Forums](#)

Thread: [Wireless - A comprehensive guide about wi-fi hacking/recovering](#)

Magnus - June 23, 2011, 6:58 pm

Hello and welcome to my tutorial about wireless networking. Today I'll be teaching you how easy it is to obtain access to a wireless protected network. There are lots of questions coming from the beginners on how to crack WEP/WPA/WPA2 keys and accessing their neighbor's connection. The purpose of this tutorial is to answer them. Judging from the "tutorials" on youtube which are either obsolete, or simply misguiding the listeners, this tutorial will be different. I will be covering all of the aspects and ways of hacking a network and gaining access to the router. This tutorial will be divided in 2 parts, such as WEP and WPA/WPA2 hacking. Please read below on what you need to succeed.

[Backtrack 5](#) - I would suggest GNOME, 32Bit, ISO & Direct

Compatible Wireless Card

WPA Word List - Search via torrents to find one

Making a bootable USB

WEP encrypted networks

WPA/WPA2 encrypted networks

Commands Used

This is the most vital step that you need to succeed in before learning how to use backtrack and actually hack WEP/WPA networks. Please follow the easy steps below:

Download & Run [UNetbootin](#)

Tick Diskimage instead of Distribution

Select USB Drive as the type, and select your USB drive name - Example: F:\

Click OK and wait a couple of minutes - Note: It may freeze at some point, don't worry about that

What you need for this crack are a few simple things, a copy of backtrack 5 booting off a DVD or a flash drive and a compatible wireless card that supports packet injection. Now if you can't get to this screen, and you are stuck at the terminal you get when booting into backtrack, you need to type startx and wait a couple of minutes for the desktop to show. Okay so let's begin, so first we need to open a terminal. To do that, just click the little icon that's on the right side from System. Please see the image below:

Now type airmon-ng and that command displays our interfaces. In my case I have wlan0, and now we are going to put it into monitor mode. To do that, type airmon-ng start wlan0. As you can see on the picture below it says (monitor mode enabled on mon0), and we are going to be using mon0 instead of wlan0 as our interface.

Type airodump-ng mon0 and that will start scanning for wi-fi networks. As you can see, there is a network called SKIDHACKER. Take a note of the BSSID the DATA, the CHANNEL and the type of ENCRYPTION. Please refer to the image below, if you have any trouble getting to that point.

Now we are going to set it to lock on a specific network named SKIDHACKER. To do that, type airodump-ng -c (channel) -w WEPcrack --bssid (bssid of the network) mon0. Replace (channel) with the channel of the network you are trying to crack, and replace (bssid of the network) with the bssid of the network you want to crack.

Okay so as you can probably see the data is going really slow, and we need to boost that up. We are going to need a lot more data, so let's preform one of the aireplay commands that will boost that data. Firstly, open up a new terminal and type aireplay-ng -1 0 -a (bssid) mon0 where (bssid) is the bssid of the network. Now if your wi-fi card is supported, you should see Association successful :-), if you don't see that then your card is not supported.

Now we are going to type in aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0. And now when the question Use this packet ? pops up, just push the letter y. And now as you can see in the image below, the data went high drastically.

Okay so now lets open a new terminal and we are going to attempt to crack it with the amount of data we have. I recommend getting over 20000 data before trying to crack it. So let's type

aircrack-ng WEPcrack*.cap. Replace WEPcrack with the filename you chose before when capturing the data, and don't forget to add that asterisk after the file and the extension which is .cap.

And now it will attempt to crack the password. Just wait a couple of minutes for it to complete, and once it did it will say KEY FOUND! [XX:XX:XX:XX:XX] where the X's will be random numbers and/or letters. That's not it, now to connect you will need to remove the semicolumns. For an example, if we were to have 12:34:52:66:59, the password would be 1232526659. Just log in to your Windows OS, and connect using that password.

So lets begin. What you will need for this crack is a dictionary file that we are going to use to crack the WPA/WPA2 password. Remember, the bigger the dictionary file is the greater the chance you have in cracking the password. So now you are probably wondering, where do I get a dictionary file? Well, I don't know if this is allowed or not but I recently downloaded a 1.9GB dictionary file.

To get the file please PM me, I can't risk getting this tutorial taken down. Okay, so firstly open up a terminal and once we have the terminal open we are going to type in airmon-ng which will display our wireless interfaces. In my case I have wlan0, and now we are going to put it into monitor mode. To do that, type airmon-ng start wlan0. As you can see on the picture below it says (monitor mode enabled on mon0), and we are going to be using mon0 instead of wlan0 as our interface.

Lets type in airodump-ng mon0 and this command is going to initiate the scanning process for Wi-Fi networks. As you can see in the picture below, a few WPA encrypted networks should pop up. I'm going to attempt to crack the network under the essid SKIDH?CKER. Take a note of the channel, and you want to copy the BSSID for later use.

Now we are going to type in airodump-ng -c (channel) -w (filename) --bssid (bssid) mon0, and replace the values to fit what you got from the last step. Don't forget to remember what filename you chose, because we are going to need that at the end.

What is needed to crack a WPA or WPA2 key is something called a WPA Handshake. You can obtain a handshake by kicking someone off the network, and those computers will automatically reconnect which will give you the handshake. This means, if there is no one on the network, you can't get a handshake, and you can't crack the WPA network. So how do we know if someone is connected? Well look at the lower part of the airodump command, and you will notice something as STATION, and underneath that if someone is connected it wil show you their mac address.

Once you get a handshake, airodump will alert you in the top screen, and the handshake will be

located right from the time stamp. Okay, so lets open up a new terminal and we are going to kick off the computers connected. Lets type in `aireplay-ng -1 0 -a (bssid) mon0`. replace bssid with the network you are trying to crack and hit enter. It is going to attempt to kick off a client, and if it succeeds you will see the wpa handshake at the top right corner, if you don't run the aireplay command a couple of times.

So now that we have a wpa handshake file, we are going to attempt to crack it. Lets stop the scan by pressing `CONTROL + C` on the terminal where airodump is running. Now in order to find the handshake file, you need to go in the top menu and chose Places > Home Folder. Okay, so lets open up a terminal and we are going to type in `aircrack-ng -w (dictionary) /root/(filename)`. Where filename is the filename you specified when capturing the wpa handshake and the dictionary is the path of the wordlist you downloaded. This can be done by dragging in the handshake file into the terminal after the `aircrack-ng -w (dictionary)` command and it will parse in it's directory. All you need to do is hit enter. The password needs to be in the dictionary file, so the bigger the wordlist is the bigger are the chances of you getting the password.

If the password is in the wordlist, it will give you a success message and the key in brackets. Happy hacking, hackers!

`airmon-ng`This command displays the wireless interfaces.

`airmon-ng start wlan0`This command starts monitoring mode on a wi-fi device.

`airodump-ng mon0`This command shows all of the wi-fi networks online.

`airodump-ng -c (channel) -w (filename) --bssid (bssid) mon0`This command specifies the wi-fi device to concentrate to one network.

`aireplay-ng -1 0 -a (bssid) mon0`This command kicks off clients that are connected, and gets the handshake.

`aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0`This command boosts the data, when cracking WEP.

`aircrack-ng -w (dictionary) (wpa handshake)`This command is used when cracking WPA or WPA2 networks.

aircrack-ng (filename)*.cap This command is used when cracking WEP networks.

These were the commands I used in the whole guide.

Author's Comment: Thank you for reading my tutorial on how to crack WPA/WPA2/WEP encrypted networks. I have spent quite a lot of time on this tutorial, and I appreciate if you at least say thanks. You know how hard it is to do a couple of restarts only to get screenshots. If you have any questions regarding any part of the tutorial, please PM me them and I will be glad to answer. As for the WPA wordlist, you need to PM me to get it. I won't risk getting my tutorial deleted because I put up a torrent link. Again, thanks for reading.

~ Magnus

merforga - June 23, 2011, 7:43 pm

Awesome tutorial. I love the layout and clear pictures and instructions. Keep up the good work!

icnhzabot - June 23, 2011, 8:03 pm

Awesome work-- thanks for all the information. It's very easy to understand.

Magnus - June 23, 2011, 8:11 pm

No problem guys, glad you liked it in the first place. I managed to take the pictures and put a little shadow so it looks more appealing. :)

icnhzabot - June 23, 2011, 8:15 pm

Could you please PM me that wordlist you talked about? 1.9 gb seems massive :O

Magnus - June 23, 2011, 8:17 pm

Yeah, hold on a second icnhzabot. Let me fetch the torrent link. You'll receive the wordlist in a few seconds.

PorkHunt - June 23, 2011, 8:18 pm

Great tutorial. Easy on the eyes, and full of easy to understand info.

icnhzabot - June 23, 2011, 8:26 pm

Thanks again Magnus.

Better go get a better flash drive now; the only functional one I have is full of junk XD

Magnus - June 23, 2011, 8:28 pm

Haha, icnhzabot. Get a portable HDD and fill it in with lots of wordlists and when u want to crack a WPA just plug it in and enjoy. :)

icnhzabot - June 23, 2011, 8:38 pm

hm good idea, I might do that.

just wondering, do we need to create a bootable USB for Backtrack or could we just download

[aircrack?](#)

LinusT - June 23, 2011, 8:42 pm

I already know all of this, but great tut for anyone new. you seem HQ, +rep man.

id just recommend expanding it and showing jacktheripper and cowpatty.

Magnus - June 23, 2011, 8:52 pm

(Jun 23, 2011 08:38 PM)icnhzabot Wrote: [\[CITE\]](#) hm good idea, I might do that.

just wondering, do we need to create a bootable USB for Backtrack or could we just download [aircrack](#)? You need to have the full Backtrack 5 in order to do this. I suggest making a bootable USB, yes.

Glassy - June 23, 2011, 9:00 pm

This is a wonderful guide you have created. Good job.

HackRain - June 23, 2011, 9:51 pm

Code aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0
what type of attack is this called?

can anyone say stickie?

dallascoury - June 24, 2011, 1:40 am

Thank you so much for this post, Very helpful and clear.

Dallas C.

BlueBit - June 24, 2011, 4:08 am

This is probably one of the largest tutorials on the internet, thanks for posting man!

John 15:13 - June 24, 2011, 4:30 am

PMed you right now for the wordlist.

maximusnl - June 24, 2011, 8:00 am

Great tutorial. Thank you!

Valour - June 24, 2011, 8:29 am

Awesome tutorial and very interesting to be read.. Also a very nice setup of points, images, stylish text, and awesome use of colors which made it very attractive too :) .. Thanks a lot for putting up so many efforts :)

Magnus - June 24, 2011, 5:43 pm

Thanks for the wonderful comments, guys. I think that this tutorial will solve all of the questions asked around about cracking WEP/WPA.

Acolyte - June 26, 2011, 2:22 am

A very appealing tutorial, Magnus. Going to bookmark it for future use. Thanks!

Magnus - June 26, 2011, 7:40 am

Yeah, Acolyte. I was doing the graphics first, then writing the thread. I always liked the fact that my work always looks good.

Wellbloud - June 26, 2011, 11:44 am

Thank you very much for this tutorial, but i stucked at the aireplay-ng -2 -p 0841 -c FF:FF:FF... etc. command, with running line Read (number) packets ... and it already run like 10 minutes and nothing happen (im on number 7500) :D

//10 000 packets... was on 50 000 still nothing.. also, i would like to ask for the Wordlist .)

Magnus - June 26, 2011, 1:22 pm

It really depends. You don't need data when you are cracking WPA/WPA2 encrypted networks.

Wellbloud - June 26, 2011, 1:26 pm

(Jun 26, 2011 01:22 PM)Magnus Wrote: [CITE](#) It really depends. You don't need data when you are cracking WPA/WPA2 encrypted networks.

Im cracking WEP ...

??
??
??

Middle - June 26, 2011, 1:28 pm

Bet OP feels like a massive cock for the spelling mistake in the title of such a well thought out thread

Magnus - June 26, 2011, 1:44 pm

Oh, crap. I must have somehow missed the letter 'O'. I can't edit it anymore :(

Minea Korosu - June 27, 2011, 1:39 am

I'll rep you again when I get ub3r. :)

Vouch for this guy! Even gave me the torrent for the world list. I'll get hold of my HDD. :)

Nice bro!

Magnus - June 27, 2011, 6:09 am

Thanks, Furie. Yep, the wordlist is actually 13GB and not 1.9GB as I said. Another 11GB wouldn't hurt anyone, now would they?

Mr Kewl - June 27, 2011, 6:47 am

I am glad we have members like you,
Make HF proud me son. Great Tutorial.

xWiFi - June 27, 2011, 8:54 am

Great Tutorial man, really impressive

PATEL - June 27, 2011, 8:57 am

good workig man great job..

sstef - June 27, 2011, 12:39 pm

Thank you very much for this tutorial!

Regicide - June 27, 2011, 1:43 pm

Wow, this guide is so helpful. Thanks so much!!

Epiczz - June 27, 2011, 7:57 pm

awesome tut man great job

polyester120667 - June 29, 2011, 2:36 am

hey huys sorry about this but i have a question :

which is better for hacking windows or linux?and if its linux wich distribution is the best?

thank u i appreciate your help :)

Magnus - June 29, 2011, 3:13 am

Linux is best for hacking, and I would prefer Backtrack.

John* - June 29, 2011, 9:42 am

Very great tutorial written by you my dear friend. This should get sticky! ;)

ignite2030 - June 29, 2011, 10:04 am

thanks, great tutorial! good job.

rayray420x - June 29, 2011, 3:39 pm

hey can i get the dictionary file

LiamLC - June 29, 2011, 5:35 pm

So when I try to type in airmon-ng all it says is interface chipset and driver and no other info to go along with it. I have BT5 in VMware.

Please help

polyester120667 - June 30, 2011, 1:08 am

thank u magnus ? i will use ubuntu is it ok?

polyester120667 - June 30, 2011, 1:08 am

thank u magnus ? i will use ubuntu is it ok?

firzen515 - June 30, 2011, 1:11 am

Do you need to start wicd or has that been replaced by airmon-ng?

Stenography - June 30, 2011, 6:39 am

I'm going to try it right now !

I'm on a park right now, hacked a unportected WIFI router,

and hacked one of the conected computers and finaly, changed the name of the WIFI to :

H4ck3d by PolarX

and changed the pass and fucked up the router that the only thing you can do is just to find it on the network.

Most of WIFI networks in my range are protected by password so i can't wait to try it out !

EDIT:

PM'ed you :)

Magnus - June 30, 2011, 7:53 am

(Jun 29, 2011 05:35 PM)LiamLC Wrote: [\[CITE\]](#) So when I try to type in airmon-ng all it says is interface chipset and driver and no other info to go along with it. I have BT5 in VMware.

Please helpYou must have an USB wireless adapter if u wish to run it with VMWare. You can try and boot from an USB and check if by typing airmon-ng if your devices are shown. If not, it means that your wi-fi adapter is not compatible.

G-Star Raw - June 30, 2011, 8:04 am

Thanks for this tut mate very helpful!

AcroneSF - July 1, 2011, 6:07 am

Excellent tutorial mate!

I have a question though. When I type 'airodump-ng -c (channel) -w WEPcrack --bssid (bssid of the network) mon0' the scanned networks pop up but it appears to continue to scan? if you get what I mean. In your screenshot it took 4 seconds. When I try it I just continues to scan and doesnt bring up the 'root@root:~#' where you type the next command.

Forgive my lack of the right terminology, I cant think straight at the moment.

Any help would be greatly appreciated.

AcroneSF

Middle - July 1, 2011, 6:57 am

(Jul 1, 2011 06:07 AM)AcroneSF Wrote: [\[CITE\]](#) Excellent tutorial mate!

I have a question though. When I type 'airodump-ng -c (channel) -w WEPcrack --bssid (bssid of the network) mon0' the scanned networks pop up but it appears to continue to scan? if you get what I mean. In your screenshot it took 4 seconds. When I try it I just continues to scan and doesnt bring up the 'root@root:~#' where you type the next command.

Forgive my lack of the right terminology, I cant think straight at the moment.

Any help would be greatly appreciated.

AcroneSF

It will keep going till it is stopped by you, to do that press CTL+C to kill the command

Magnus - July 1, 2011, 12:30 pm

Yep. The CTRL+C is the basic command to stop a process in Linux.

Mullet Mcnasty - July 1, 2011, 5:08 pm

Exellent tutorial. Well presented and easy to follow.

Magnus - July 2, 2011, 3:53 am

Thanks for the nice words, Mullet Mcnasty. Graphics are a good part of the tutorial.

editorstefan - July 2, 2011, 4:23 am

I dont need a Compatible Wireless Card if i have a laptop?

I only need something that are able to connect WiFi ?

Or do i need a Compatible Wireless Card ?

thanks

No??????? - July 2, 2011, 7:48 am

That looks like a really nice tutorial, keep up the good work mate. :)

Magnus - July 2, 2011, 8:25 am

You need a compatible wireless card to inject. It doesn't matter if it's a laptop or not.

Frida - July 2, 2011, 9:32 am

Holy shit, amazing tutorial, deserves 5 stars and a sticky.

Magnus - July 2, 2011, 10:21 am

Thanks for your opinion, Disciple. It's really appreciated!

Dr. A. NonyMouse - July 2, 2011, 3:20 pm

Wow... All of this time spent on this thread and you misspell the title.

Great thread though. I downloaded this page.

Magnus - July 3, 2011, 2:39 am

The sad thing is, I didn't misspell the thread, my 'u' letter was probably broken at that time. My keyboard tends to write 2x letters, and sometimes it eats them.

scientific10 - July 3, 2011, 8:30 am

Can i crack wep 128 bit with this? password lenght is 26 symbols.

goddard007 - July 3, 2011, 10:51 am

hi i need help on hacking my wirless box for learning perpases please could some one point me to the right direction its a talktalk wirless roughter plus im on windows 7 if they is anything out there compatible with it thanks if you could help me and if you no how to could you email me on adam.goddard123@yahoo.com thanks

Darco969 - July 3, 2011, 9:52 pm

Awesome tut. I like the layout and ting.

bobjoemike - July 4, 2011, 12:01 am

How do u know if ur Wireless Card is compatible? does most laptop come with them? if not where can i get them?

AcroneSF - July 4, 2011, 2:17 am

(Jul 4, 2011 12:01 AM)bobjoemike Wrote: [\[CITE\]](#) How do u know if ur Wireless Card is compatible? does most laptop come with them? if not where can i get them? You can type 'airmon-ng' into the console. If no devices show up your Wireless Card is not compatible.

Magnus - July 4, 2011, 4:42 am

(Jul 4, 2011 02:17 AM)AcroneSF Wrote: [\[CITE\]](#) You can type 'airmon-ng' into the console. If no devices show up your Wireless Card is not compatible. Sorry, I couldn't answer on time but that's the correct answer. Thanks AcroneSF.

-Collman - July 4, 2011, 6:23 am

Extremely amazing tutorial. Clear, neat and well presented. Can't ask for anything else.

Thanks =)

Delmont - July 4, 2011, 7:25 am

This is an amazingly clear and straight-forward tutorial. I've been watching several vids, and none of them are as clear as this. Thanks so much for putting this up, it's immensely helpful to people such as myself. :)

slone417 - July 4, 2011, 7:33 am

awesome tut bro. Is there any alternative for dictionary attack? My neighbor's WPA passcode is very strong. lol. used 1.6Gb wordlist. its not workin. any recommended alternatives for WPA cracking? Thank in advance. and keep up the good work! :)

Magnus - July 4, 2011, 7:38 am

Well, you could always go and visit his house, ask him if you could use the internet and infect him with a RAT. After that, google for any tutorials on how to change a WPA encryption into a WEP one and you're done.

rand0 - July 4, 2011, 8:22 am

So I've seen a few questions go insufficiently answered. So here goes:

@PandaMonix: This is the interactive frame selection option in aireplay-ng. I'm not exactly positive, but it looks like you're allowed to pick which packet you use to replay to the router. This is generally an arp packet, or a modified Grat ARP or something. The point is to replay a legitimate packet so that the router puts out even more packets. I just use the -3 option, and the attack generally goes fine for me. I'm going to make a more detailed and less script kiddie-ish TuT on cracking WEP keys, so keep an eye out if you are really interested in understanding hacking WEP on a deeper level.

@LiamLC: To me it just seems like you have incorrectly or incompletely set up BackTrack in VM. I don't think it's that you necessarily have incompatible hardware. Like OP said, you can try booting from a usb and typing `Code iwconfig` If your interfaces show up then chances are you're supported. If you don't have a free usb to use, you can try googling to see if your stuff is compatible in BackTrack. Now, I generally use virtualBox, but I can try to help you if you're still lost. Just post a new topic so you don't spam up the thread for this TuT. :)

@Scientific10: Totes! It may take a bit longer for aircrack, and/or you may have to get more weak IVs, but yes. All WEP can be easily cracked :)

Magnus - July 4, 2011, 8:31 am

Thanks for helping me, 3k1yp2. I tried to answer them as professional as I could.

rand0 - July 4, 2011, 8:31 am

(Jul 4, 2011 08:31 AM)Magnus Wrote: [\[CITE\]](#) Thanks for helping me, 3k1yp2. I tried to answer them as professional as I could.

Hey. No problem, man. I love to help any way I can! And it's a very nice TuT, by the way. I totally appreciate the work you put into this. Very HQ. I haven't yet seen a Tut on wireless key cracking using BT5, so great work!

Can you tell me a bit more about your interactive frame selection attack? I've never used it, although I've used aircrack suite fairly extensively. I'm focusing on Wifi related hacking at the moment, so I'd love to learn something new.

Magnus - July 5, 2011, 3:36 am

If anyone else is having problems, don't hesitate to post or PM me. I'll be glad to help you!

JackChitt - July 5, 2011, 4:38 am

Nice, REAL Nice!! Oh, Middle looks like you got sum competition brother :)

Magnus - July 5, 2011, 4:58 am

Hehe, Middle understands stuff better then me. :)

Vipe® - July 5, 2011, 4:38 pm

Great job, that's just awesome!

Magnus - July 5, 2011, 6:58 pm

Thanks for the nice and cool comment, Viper. It's appreciated!

Vipe® - July 5, 2011, 7:28 pm

No problem, I'm sure you took alot of time to do that. :)

Magnus - July 5, 2011, 7:43 pm

Yep, took me something from 2 to 6 hours. I'm not sure, it might be 4-5 :)

Sh3llc0d3 - July 6, 2011, 2:31 am

Nice tutorial, to really make it comprehensive you could have included other attacks - chop chop etc :)

(Jun 23, 2011 08:15 PM)icnhzabot Wrote: [\[CITE\]](#) Could you please PM me that wordlist you talked about? 1.9 gb seems massive :O
1.9gb for a wordlist isn't very big.

Derkek - July 6, 2011, 4:29 am

Nice work. I did this in Ubuntu and got the key, now I tried connecting to the network and was prompted to enter a Network Security Key.

I was able to connect just fine under Ubuntu and browsed the web a bit before reboot into windows. Any suggestions?

Edit: Didn't expect the image to be shown here, just a link xD

Magnus - July 6, 2011, 4:40 am

(Jul 6, 2011 04:29 AM)Derkek Wrote: [\[CITE\]](#) Nice work. I did this in Ubuntu and got the key, now I tried connecting to the network and was prompted to enter a Network Security Key.

I was able to connect just fine under Ubuntu and browsed the web a bit before reboot into windows. Any suggestions?

Edit: Didn't expect the image to be shown here, just a link xDWhat kind of encryption were you able to crack? WPA, WPA2 or WEP?

Derkek - July 6, 2011, 5:05 am

(Jul 6, 2011 04:40 AM)Magnus Wrote: [\[CITE\]](#) What kind of encryption were you able to crack? WPA, WPA2 or WEP?
WEP

Spoiler ([Click to View](#))Hurr durr reply . the message must be longer than 25 characters.

Magnus - July 6, 2011, 5:25 am

(Jul 6, 2011 05:05 AM)Derkek Wrote: [\[CITE\]](#) WEP

Spoiler ([Click to View](#))Hurr durr reply . the message must be longer than 25 characters.If it was WEP, you need to take the semi-columns out and you will get a number/letters combination. Enter that when it asks for a pass phrase.

Derkek - July 6, 2011, 5:59 am

(Jul 6, 2011 05:25 AM)Magnus Wrote: [\[CITE\]](#) If it was WEP, you need to take the semi-columns out and you will get a number/letters combination. Enter that when it asks for a pass phrase.

Well, that was derpy. I was did that the first time.

after entering the key, another window came up (the one in the screen cap) and now I typed it again and it worked.

It requested I enter the key twice apparently.

Magnus - July 6, 2011, 6:08 am

Well sometimes Windows does shit like that. :) I'm glad you have free internet now!

PCWorldAnn - July 6, 2011, 6:24 am

Awsome thankyou :) is there any way that you could put a PDF version of this up ?

Magnus - July 6, 2011, 2:12 pm

I will try to convert it into a PDF version, PCWorldAnn just for you. Keep checking every now and then and I'll upload the PDF version.

rebeln_n - July 6, 2011, 2:24 pm

Cheers mate, the best tutorial that I have seen so far! ++

Magnus - July 6, 2011, 2:52 pm

Thanks for the comment, Akiii. It's maybe your first best tutorial because you only have 1 posts :)

Middle - July 6, 2011, 3:48 pm

Here is a PDF i made :)

<http://www.filedropper.com/ahmfvkc>

Enjoy it!

jackrobert420 - July 6, 2011, 3:49 pm

Hi mate. Really nice tutorial. Nice and easy to follow and understand. Could you please PM me the wordlist if you could.

Thanks

Magnus - July 6, 2011, 8:22 pm

Yeah, sure thing jackrobert420. I'll PM it right now!

jackrobert420 - July 7, 2011, 3:11 am

Waiting for it. thanks alot.

Magnus - July 7, 2011, 5:58 am

Alright. Sorry for waiting, because I fell a sleep yesterday.

jackrobert420 - July 7, 2011, 8:47 am

(Jul 7, 2011 05:58 AM)Magnus Wrote: [\[CITE\]](#) Alright. Sorry for waiting, because I fell a sleep yesterday.

No problem. thanks for the list.

Magnus - July 7, 2011, 8:49 am

Glad I could help you, jackrobert420. If anyone needs any help just shoot me a PM, or post here!

Y2KTHUG - July 7, 2011, 9:13 am

Hey bro', I just PM'd you. Can't Wait for that Dictionary file?
Magnus, Does this work well with windows7?

GeneralStarshade - July 7, 2011, 9:20 am

Thanks for the word list magnus! You're the best.

Magnus - July 7, 2011, 9:46 am

(Jul 7, 2011 09:13 AM)Y2KTHUG Wrote: [\[CITE\]](#) Hey bro', I just PM'd you. Can't Wait for that Dictionary file?

Magnus, Does this work well with windows7? I don't quite understand, because this is all done in backtrack.

clarkent - July 7, 2011, 7:02 pm

can you please send me a list also. Thank you for the great tut

Magnus - July 7, 2011, 7:06 pm

I'm going to send you the list right now clarkent. Thanks for posting, you made the 100th post!

clarkent - July 7, 2011, 7:09 pm

and also can i get the directory file? great work

Dude seriously this is so thorough, what do you think about the alfa antenna

Magnus - July 7, 2011, 8:28 pm

Finally, PMed you clarkent. HF was crashing every time I wanted to PM a member.

clarkent - July 7, 2011, 8:40 pm

Thank you for the list, I have one other question. I can not run back track 5. I used UNetbootin Just like you said but after i reboot all i get is a list of files i cannot actually run backtrack 5? I formatted my disk drive to FAT32 but i am on a 64 bit system do you think this is why? I could not format it to EXFAT64. thanks

swordfish2270 - July 7, 2011, 9:47 pm

"

aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b 00:1A:92:EA:2B:E9 mon0No source MAC (-h) specified. Using the device MAC (00:23:4D:9D:26:1A)
^Cad 182757 packets...

"

getting stuck here and it never asks me if i want to use these packets. any ideas?

Freight - July 8, 2011, 2:57 am

Amazing guide, thanks for the info!

Icsea - July 8, 2011, 3:06 am

do the standard wireless cards work with packet injection, or would i have to buy 1? on my device manager it just says 802.11g/b mini wireless card adapter and its a laptop also

Magnus - July 8, 2011, 6:12 am

@swordfish: You need to wait for it to say that.

@lcsea: When you type airmon-ng, if it doesn't show any device then you need to buy one.

swordfish2270 - July 8, 2011, 6:43 am

ok so after it collected a little over a million packets it worked ;)

awesome got all the way to the end and "Failed. Next try with 5000 IVs" I take it i just wait for it to collect 5000 ivs?

btw great guide

awesome got it past that part. now getting stuck at

"

[00:01:04] Tested 148177 keys (got 115 IVs)

KB	depth	byte(vote)
0	15/ 16	F9(512) 04(256) 08(256) 09(256) 0E(256)
1	20/ 21	02(512) 01(256) 0B(256) 0C(256) 0F(256)
2	2/ 5	F8(768) 00(512) 08(512) 16(512) 1C(512)
3	2/ 3	AF(768) 1C(512) 41(512) 5F(512) 6C(512)
4	3/ 4	FD(768) 1C(512) 21(512) 26(512) 38(512)

Failed. Next try with 5000 IVs.

"

I take it i just wait for it to collect 5000 ivs?

kk waited like you said and it finally gave in to me. but now it seems to do stopping again.

"

[00:01:09] Tested 148177 keys (got 115 IVs)

KB	depth	byte(vote)
0	15/ 16	F9(512) 04(256) 08(256) 09(256) 0E(256)
1	20/ 21	02(512) 01(256) 0B(256) 0C(256) 0F(256)
2	2/ 5	F8(768) 00(512) 08(512) 16(512) 1C(512)
3	2/ 3	AF(768) 1C(512) 41(512) 5F(512) 6C(512)
4	3/ 4	FD(768) 1C(512) 21(512) 26(512) 38(512)

Failed. Next try with 5000 IVs.

"

any ideas on that?

22saad22 - July 8, 2011, 8:33 am

thx man for the tutorial it's very nice and thx for the link.

Y2KTHUG - July 8, 2011, 8:40 am

Hey Magnus, I meant to say that can I do all the above in window7 or must I have Linux first?

Thanks

Hey Magnus, I meant to say that can I do all the above in window7 or must I have Linux first?

Thanks

Magnus - July 8, 2011, 8:52 am

@swordfish: You need to collect at least 5000 data packets.

@Y2KTHUG: You are booting in backtrack, so yes.

boobootm - July 8, 2011, 11:45 am

thanks for the nice tutorial, do you think you can message me the word list? Thanks again!

king_hendra - July 8, 2011, 9:24 pm

i hope my laptop can detect wifi signal in my home...

code11a - July 9, 2011, 2:09 am

Excellent clear tutorial. All I need know is a 1.9GB wpa/wpa2 dictionary file.

iVision - July 9, 2011, 6:15 am

Nice tutorial

Hope it works downloading Backtrack..

But can I see before I've done everything if my card is compatible for boosting?

And can you pm me the wordlist?

Magnus - July 9, 2011, 7:37 am

I don't think that's possible, iVision. You check if your card is compatible by using the airmon-ng command.

swordfish2270 - July 9, 2011, 9:53 am

im still not having any luck. I let it run all night and still only have 115 data packets. any ideas boss man?

Magnus - July 9, 2011, 10:11 am

@swordfish: You are far away from the router. That's the only explanation!

Evil. - July 9, 2011, 12:28 pm

Just letting you know you spelt " About " wrong on the title.

Magnus - July 9, 2011, 1:19 pm

Yep. I know there is no way I could edit that out because I'm not upgraded. :(

code11a - July 10, 2011, 12:58 am

Thanks for the link. Top man.

Xemphis - July 10, 2011, 12:22 pm

Great written tutorial, it's easy to follow and read.

SeedyAre - July 11, 2011, 3:27 pm

I have an error when trying to crack WPA

Quote: aireplay-ng -1 0 -a <bssid> mon0

gives me the following:

Quote: No source MAC (-h) specified. Using the device mac (M:A:C:H:E:R:E)

Waiting for beacon frame (BSSID: <BSSID-MAC>)

No Such BSSID available

Please specify an ESSID (-e)

Any help?

Edit:

Also;

Your command Quote:aireplay-ng -1 0 -a <MAC> mon0

gives me:

Quote:Sending Authentication Request (Open System) [ACK]

Authentication Successful

Sending Authentication Request [ACK]

Denied (Code 12), wrong ESSID or WPA ?

VanillaFace - July 11, 2011, 5:01 pm

Great tut. Gonna give it a shot :)

Magnus - July 11, 2011, 5:37 pm

@SeedyAre: you need to replace the MAC with the MAC you got from the airodump, and the bssid of the network!

Killer1478 - July 11, 2011, 6:25 pm

I failed with 66 thousand, is this normal? Should i try 200K next time?

hondamars - July 11, 2011, 6:49 pm

Should I need to format my OS and install this one? Sorry for this question..

Killer1478 - July 11, 2011, 6:50 pm

(Jul 11, 2011 06:49 PM)hondamars Wrote: [\[CITE\]](#) Should I need to format my OS and install this one? Sorry for this question..but no it is not required for this

Holy crap the forum is slow to post stuff

SeedyAre - July 12, 2011, 2:02 am

(Jul 11, 2011 05:37 PM)Magnus Wrote: [\[CITE\]](#) @SeedyAre: you need to replace the MAC with the MAC you got from the airodump, and the bssid of the network!

Thats what I was doing! I just edited it out here so it wasn't on show!

Magnus - July 12, 2011, 5:46 am

@SeedyAre: Are you writing the bssid in between < and > ?

sam-the-man - July 12, 2011, 7:35 am

I read thru this but wish it was in a video format as I would probably understand it better n quicker 2

zarnilwin - July 12, 2011, 8:28 am

Cool That's what I am looking for. Clear image . Thanks

Xaverage - July 12, 2011, 9:23 am

Awesome tutorial!!! Thanks for all of the info man!

Magnus - July 12, 2011, 12:16 pm

No problem guys. If you had any issues, just PM me. I'm soon going to get a router myself, and I'll make a video tutorial so you don't have to worry about that one.

hondamars - July 12, 2011, 6:24 pm

It is possible to crack the password even the router have a mac filter security?

Magnus - July 12, 2011, 6:38 pm

I'm not entirely sure, hondamars. I guess try to bypass the filtering somehow.

Anonymous1200 - July 12, 2011, 7:21 pm

Ty for the tutorial.

Vouch

hondamars - July 12, 2011, 10:44 pm

Hello, I encounter that my neighbors wi-fi is encryp with OPN. Do you have any solution with this dude?

Hello, I encounter that my neighbors wi-fi is encryp with OPN. Do you have any solution with this dude?

Magnus - July 13, 2011, 2:39 am

Thanks for the comment, Anonymous1200.

Edit: If it's OPN, then it doesn't have any encryption on it.

Xaverage - July 13, 2011, 1:32 pm

I find the most useful information on this forum, but some posts just make me want to facepalm. I feel like there should be a minimum amount of knowledge required before becoming aware of this forum's existence.

Magnus - July 13, 2011, 2:52 pm

Like something to prove that you are human, and not an alien.

Unknow16 - July 13, 2011, 3:07 pm

wow, very elaborated post.

Thanks

Dan08 - July 14, 2011, 2:10 am

i seriously love this tutorial!! i love the images and very organised ;) and 2 in 1 (wep - wpa/wpa2)

Dan08 xx

Magnus - July 14, 2011, 5:01 am

No problem, Dan08. You forgot the 3 in 1 (wep - wpa/wpa2 - bootable usb).

zerocool - July 14, 2011, 6:00 am

Awesome tutorial , the best i have seen in a long time ... great job

Anonymous1200 - July 14, 2011, 6:21 am

I need help again..When i type "airodump mon0" i get some error about something not being installed/found or something...

E?!M - July 14, 2011, 8:08 am

great tut thanks for posting!!

Dan08 - July 14, 2011, 8:29 am

(Jul 14, 2011 06:21 AM)Anonymous1200 Wrote: [\[CITE\]](#) I need help again..When i type "airodump mon0" i get some error about something not being installed/found or something...
if u cant tutorials, just go have a nap mate :p

dan08 xx

Magnus - July 14, 2011, 12:05 pm

(Jul 14, 2011 06:21 AM)Anonymous1200 Wrote: [\[CITE\]](#) I need help again..When i type "airodump mon0" i get some error about something not being installed/found or something...Correct is: airodump-ng mon0. Notice the -ng after airodump?

SidiOu5 - July 14, 2011, 12:10 pm

Brilliant tutorial dude! Thanks!

SeedyAre - July 14, 2011, 1:02 pm

(Jul 12, 2011 05:46 AM)Magnus Wrote: [\[CITE\]](#) @SeedyAre: Are you writing the bssid in between < and > ?
Of course lol,

Take this for example;

```
aireplay-ng -1 0 -a XX:XX:XX:XX:XX:XX mon1
```

XX:XX:XX:XX:XX:XX is of course the bssid that has someone connected to it via WPA2, I didn't actually use XX:XX.. as the BSSID, its the MAC address that I wont post here.

When I do the above aireplay-ng command I get this:

```
Sending Authentication Request (Open System) [ACK]
Authentication Successful
Sending Association Request [ACK]
Denied (Code 12) Wrong ESSID or WPA ?
```

Magnus - July 14, 2011, 1:18 pm

I seriously don't know what's wrong, SeedyAre. Try re-booting in the backtrack and use mon0.

SeedyAre - July 14, 2011, 1:25 pm

I think it could be because the AP has MAC filtering, according to:

<http://forum.aircrack-ng.org/index.php?PHPSESSID=811fe996a3274a095973ad0fa652e8ab&topic=1236.0>

I'll continue working on it - Thanks for your help though.

Edit: One youtube video has this:

```
aireplay-ng -0 0 -a <bssid> -c <station-mac-address-here> wlan0
```

that got it sending DeAuth's, but so far I still haven't got a handshake in airodump which was/has/is running in a different shell

Anonymous1200 - July 14, 2011, 1:55 pm

(Jul 14, 2011 12:05 PM)Magnus Wrote: [\[CITE\]](#) Correct is: airodump-ng mon0. Notice the -ng after

airodump?

Thats what i typed. It said something wasnt found,Or somethin like that

SeedyAre - July 14, 2011, 2:06 pm

Final update:

I got a WPA handshake!

Thank you

Magnus - July 14, 2011, 2:45 pm

@Anonymous: You didn't start wlan0 or whatever is your device.

@SeedyAre: That's great mate. :) Good luck cracking it!

bobbyprince89 - July 14, 2011, 4:03 pm

Awesome toot. I want this as a PDF! Any chance...?? ;)

Magnus - July 14, 2011, 5:53 pm

Yep. It was posted as a PDF bobbyprince89. Just look back a few pages, a member under the name ~Middle posted it..

zyd - July 14, 2011, 10:05 pm

Hello,awesome tutorial,i have one problem when i write airodump-ng mon0 and start searching, the BAT (i think is time left) is 1 hour, is normally? (i have around 30-35 wifi around me)

bobbyprince89 - July 15, 2011, 3:29 am

(Jul 14, 2011 05:53 PM)Magnus Wrote: [\[CITE\]](#) Yep. It was posted as a PDF bobbyprince89. Just look back a few pages, a member under the name ~Middle posted it..

Unfortunately it looks like the link he posted:

<http://www.filedropper.com/ahmfnnvk>

is dead...

Hey Middle, any chance of a re-up? :)

Magnus - July 15, 2011, 9:52 am

I will ask him to re-upload the PDF file, bobbyprince89. Hold on.

@zyd: Once you get the wi-fi u want to crack, u don't need to wait the time remaining, just press CTRL+C.

zyd - July 15, 2011, 10:24 am

(Jul 15, 2011 09:52 AM)Magnus Wrote: [\[CITE\]](#) I will ask him to re-upload the PDF file, bobbyprince89. Hold on.

@zyd: Once you get the wi-fi u want to crack, u don't need to wait the time remaining, just press CTRL+C.

Perfect,it's traceable the cracking? or only when you connect? if you change mac you are untraceable? or need some more.. thanks again!

Magnus - July 15, 2011, 10:50 am

Yeah, it depends. If u are WPA2/WPA cracking, it's better to change the MAC.

zyd - July 15, 2011, 11:28 am

(Jul 15, 2011 10:50 AM)Magnus Wrote: [\[CITE\]](#) Yeah, it depends. If u are WPA2/WPA cracking, it's better to change the MAC.

but i mean,if i crack wpa/wpa2 or wep,with the mac changed im untraceable,right? but still could be sniffed? how can i solve that?

P.d:and how i change the ip in backtack? Macchanger --mac?

Thanks.

SeedyAre - July 15, 2011, 12:31 pm

(Jul 15, 2011 11:28 AM)zyd Wrote: [\[CITE\]](#) P.d:and how i change the ip in backtack? Macchanger --mac?

Try:

```
ifconfig wlan0 down
macchanger -r wlan0
ifconfig wlan0 up
```

do that before you begin the tutorial with:
airmon-ng start wlan0

*Of course, thats if your wifi device is wlan0, do a "airmon-ng" command first to find out. (My laptop has inbuilt wifi that takes wlan0 so I use wlan1 for my Alfa)

zyd - July 15, 2011, 1:33 pm

(Jul 15, 2011 12:31 PM)SeedyAre Wrote: [\[CITE\]](#) Try:

```
ifconfig wlan0 down
macchanger -r wlan0
ifconfig wlan0 up
```

do that before you begin the tutorial with:
airmon-ng start wlan0

*Of course, thats if your wifi device is wlan0, do a "airmon-ng" command first to find out. (My laptop has inbuilt wifi that takes wlan0 so I use wlan1 for my Alfa)Great i tried it and work,when i got the key, i should log with a vpn right?

Magnus - July 15, 2011, 2:52 pm

No, why vpn? Log in through the connection manager from backtrack, or in windows.

zyd - July 15, 2011, 3:22 pm

(Jul 15, 2011 02:52 PM)Magnus Wrote: [\[CITE\]](#) No, why vpn? Log in through the connection manager from backtrack, or in windows.

and i can't be sniffed?

Btw,when i start sending packets with airodump,it says:attack failed,but i readed that my netcard is compatible: Atheros AR2985

Magnus - July 15, 2011, 3:43 pm

Maybe you are writing the aerodump command wrong? What do you care if your neighbor finds out

that you are using his internet? It's not his fault he left it unsecured!

erblanko - July 15, 2011, 4:22 pm

Thanks for this wonderful tutorial! It is really well made and easy to follow. Compliments!

zyd - July 15, 2011, 4:44 pm

(Jul 15, 2011 03:43 PM)Magnus Wrote: [\[CITE\]](#) Maybe you are writing the airodump command wrong? What do you care if your neighbor finds out that you are using his internet? It's not his fault he left it unsecured!

he could(sniff me and steal my accounts) or call police,or im wrong?

P.d:now sayed connect succesful but when i use: aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0. it scanned about 70.000+ and doesn't pop up nothing

Magnus - July 15, 2011, 5:16 pm

You need to press CTRL+C on the aireplay-ng command. Btw, neighbors are always stupid.

bejiita - July 15, 2011, 5:25 pm

can i have the dictionary?

Magnus - July 15, 2011, 5:31 pm

You would have to PM me for the dictionary, bejiita.

zyd - July 15, 2011, 6:19 pm

Oh lol,when i write airodump-ng mon0 it show me it WEP but when i do the airodump for that router,it appear like WPA/WPA2,it happened me in 5 tries of diferent routers.

Magnus - July 15, 2011, 7:23 pm

Did you put the right channel, zyd? Also verify the BSSID and ESSID.

zyd - July 15, 2011, 7:58 pm

okay now i tried with a WEP and still reading packets but nothing pop ups.. if i make a vid you could check it?

P.D:it appeared as WEP but after packet 70,000+- it changed to wpa2

Magnus - July 15, 2011, 8:35 pm

Yep, make a video I might be able to help you.

Cozmikk - July 15, 2011, 11:03 pm

Best thread ever. I wish I could rep.

delanoman - July 16, 2011, 10:36 am

Nice tutorial 5 stars ?

Magnus - July 16, 2011, 10:48 am

You gonna get upgraded sooner or later, Cozmikk. Anyways, if anyone of u needs any help just write.

zakabet170 - July 16, 2011, 10:58 am

Great tutorial. Thanks :)

Magnus - July 16, 2011, 11:07 am

No problem, zakabet170. I wish you get some free internet!

theblackplauge - July 16, 2011, 11:13 am

awesome tut this is exactly wat i was looking for

SuburbanInsanity - July 16, 2011, 1:01 pm

Fuck off, my backtrack 5 is KDE, 64 bit, VMware even if I don't have it and torrent :(

Magnus - July 16, 2011, 1:07 pm

What was your point, demoniax?

delanoman - July 16, 2011, 5:15 pm

When I type airodump-ng mon0 star to scan but I been waiting 45 min and don't stop

How I can stop the scan

Thanks

Magnus - July 16, 2011, 5:24 pm

Stop the scan with CTRL+C.

7u7u7 - July 16, 2011, 6:03 pm

thank you but for the usb boot do i just download the backtrack and put it on my usb drive or do i need to download a linux distro aswell

Magnus - July 16, 2011, 6:12 pm

Nope. You just follow the bootable usb tutorial, don't do anything else.

insert_username - July 17, 2011, 10:23 am

thank you very much for this guide, very detailed :)

hello all, does anyone have any suggestions for a word list until Magnus is online - i dont mind how big the file is, thanks - sorry for bad english - im very computer illiterate and know more about virus's and normal RAT hacking than you care to imagine, if you attempt to hack or infect me - you will regret it.

thanks anyone who can help me :) <3

Magnus - July 17, 2011, 12:39 pm

There, the thread has been updated to fix the spelling error. I'm going to PM you the list right now, insert_username!

insert_username - July 17, 2011, 12:54 pm

(Jul 17, 2011 12:39 PM)Magnus Wrote: [\[CITE\]](#) There, the thread has been updated to fix the spelling error. I'm going to PM you the list right now, insert_username!

thankyou very much for the list - downloading now :) your a legend

Magnus - July 17, 2011, 1:57 pm

No problem, insert_username. Hope you use it wisely, lol. :D

shahqais - July 17, 2011, 2:25 pm

awesome tutorial can you please forward me the torrent link of words-list. thank you in advance and keep up the good work.

insert_username - July 17, 2011, 2:37 pm

shahqais, i have forwarded the link to you via pm, :) enjoy :P

Magnus - July 17, 2011, 2:39 pm

Wow, thanks for doing that insert_username. You saved me a few clicks :D

shahqais - July 17, 2011, 7:40 pm

(Jul 17, 2011 02:37 PM)insert_username Wrote: [\[CITE\]](#) shahqais, i have forwarded the link to you via pm, :) enjoy :P

thank you very much. I am going to download the file and then try both. I have many networks around. both WPA and WEP.

Magnus - July 17, 2011, 7:42 pm

Wow, this thread has reached 200 replies. I never knew it would get that far!

SeedyAre - July 18, 2011, 12:16 am

Can I get a link to the wordlist? I have 2 lists atm, one 700mb that seems useless, and one that when unpacked will be 13gb.

Whats yours? I'm just looking for a "common" password type list if its possible. Not a huge one (Running it on a netbook so about 200 keys p/s).

archies4000 - July 18, 2011, 12:37 am

none of the images are loading...please see...really want to learn this...

sandy038 - July 18, 2011, 1:31 am

Great Tutorial.Please PM the Torrent link for the word list.

SeedyAre - July 18, 2011, 1:45 am

(Jul 18, 2011 12:37 AM)archies4000 Wrote: [\[CITE\]](#) none of the images are loading...please see...really want to learn this...

They work here, try holding down SHIFT on the keyboard and then pressing the "Refresh" or "reload" button on your browser as seen below.

[img]<http://goodstuff568.files.wordpress.com/2007/12/internet-explorer-6.jpg>[/img]

insert_username - July 18, 2011, 8:45 am

SeedyAre, sandy038 - I have Pm'ed you the torrent list :) enjoy

Artursiidla - July 18, 2011, 9:13 am

I type in startx and then it starts loading backtrack , once it loaded it rapidly jumps to terminal again , help ?

insert_username - July 18, 2011, 9:33 am

sorry for dumb question, but what program shall i use to extract the word list in BackTrack? do i need to download WinRar for linux and extract it that way?

SeedyAre - July 18, 2011, 9:38 am

pff, i've been seeding that wordlist already, why's it a secret?

I've already upped 80gigs of it. Someone on an iMac in the UK was getting 1.5mb/s from me on it a few hours ago!

insert_username - try <http://opencheese.com/2009/05/08/ubuntu-how-to-unrar-rar-files-with-ubuntu/>

Hopefully it will help.

Magnus - July 18, 2011, 9:49 am

(Jul 18, 2011 09:13 AM)Artursiidla Wrote: [\[CITE\]](#) I type in startx and then it starts loading backtrack , once it loaded it rapidly jumps to terminal again , help ?I don't know, I've never had this problem :(((

insert_username - July 18, 2011, 9:56 am

(Jul 18, 2011 09:38 AM)SeedyAre Wrote: [\[CITE\]](#) pff, i've been seeding that wordlist already, why's it a secret?

I've already upped 80gigs of it. Someone on an iMac in the UK was getting 1.5mb/s from me on it a few hours ago!

insert_username - try <http://opencheese.com/2009/05/08/ubuntu-how-to-unrar-rar-files-with-ubuntu/>

Hopefully it will help.

thanks - and wasn't me :) but i am in the UK ;P)

Hello all, i thought this was the best place to post, as most here are using BackTrack or know how to use it and can help me :)

I have a 4.9GB word list which needs extracting, i have tried using terminal but it doesn't seem to be able to find the file which is placed on a partion of an external hard drive of mine. So here i am wishing your help - I've gotten up to here, i have tried all of these terminal commands....

```
unrar e wordlist.rar
```

```
unrar wordlist.rar
```

```
unrar e wordlist.rar /media/James! < what my partion is called, they all come up with this response....
```

```
root@root:~# unrar e wordlist.rar /media/James!
```

```
UNRAR 3.90 beta 2 freeware Copyright © 1993-2009 Alexander Roshal
```

```
Cannot open wordlist.rar  
No such file or directory  
No files to extract
```

Any help at all would be very much appreciated - thanks guys :)

Frankerton - July 18, 2011, 11:22 am

Thanks for the tut/guide. this will help

Magnus - July 19, 2011, 10:21 am

No problem AEsir.

@ insert_username, just copy them to the /root/ dir.

Dax - July 19, 2011, 10:36 am

Great Tutorial, helped me a lot

insert_username - July 19, 2011, 10:45 am

(Jul 19, 2011 10:21 AM)Magnus Wrote: [\[CITE\]](#) @ insert_username, just copy them to the /root/ dir. thank you very much sir :) its unzipping now :)
thank you mate :) extracted my rar now :)

johngilbert_31 - July 20, 2011, 12:09 am

Where can I get the Backtrack 5? Sorry. I really don't know anything bout hacking. Hope you could help me

SeedyAre - July 20, 2011, 1:10 am

(Jul 20, 2011 12:09 AM)johngilbert_31 Wrote: [\[CITE\]](#) Where can I get the Backtrack 5? Sorry. I really don't know anything bout hacking. Hope you could help me

Don't worry that you don't know anything about hacking, but i'm sure you've heard of this fantastic new service called Google? Would have saved yourself some time and you would have had it downloaded by now if you googled rather than waited for me to point you there instead (I googled it anyway).. <http://goo.gl/DaCSo>

Magnus - July 20, 2011, 6:14 am

(Jul 20, 2011 12:09 AM)johngilbert_31 Wrote: [\[CITE\]](#) Where can I get the Backtrack 5? Sorry. I really don't know anything bout hacking. Hope you could help melt is linked on the word "Backtrack" on the very 1st page.

NYHCxPurity - July 20, 2011, 8:29 am

Type airodump-ng mon0 and that will start scanning for wi-fi networks. As you can see, there is a network called SKIDHACKER. Take a note of the BSSID the DATA, the CHANNEL and the type of ENCRYPTION. Please refer to the image below, if you have any trouble getting to that point.

Now we are going to set it to lock on a specific network named SKIDHACKER. To do that, type airodump-ng -c (channel) -w WEPcrack --bssid (bssid of the network) mon0. Replace (channel) with the channel of the network you are trying to crack, and replace (bssid of the network) with the bssid of the network you want to crack.

ok, So after I Scan for networks, "Root@root:~#" does not pop up again. So what do i do to Lock on?... Start a new terminal. Or control C to stop it then continue. Very Noob question but i wanna make sure.

Magnus - July 20, 2011, 8:48 am

Control + C to stop it, and then lock it on.

Mario1 - July 20, 2011, 11:40 am

You are such a fucking boss.

Cyanide666 - July 20, 2011, 12:20 pm

(Jul 20, 2011 11:40 AM)Mario1 Wrote: [\[CITE\]](#) You are such a fucking boss.What he said.

But due to problems with ATI Switchable Graphics, it will take me some time to try out your method

(I used to use a different injection method on my old laptop).?

Michelangelo - July 20, 2011, 2:55 pm

Thank you for a great Guide! ?

NYHCxPurity - July 20, 2011, 3:35 pm

Two things for you Magnus.

The first time i tried to inject packets it worked. Now it doesnt.

Second, I cant pm you because i do not have 5 posts and im not going to Go around posting shit on things i have no clue about or not interested in. So do you mind mind sending me the WPA list you have?

Lets make this 3 things.

WPA seems quicker/Easier then trying to crack WEP. True?

Magnus - July 20, 2011, 4:55 pm

I have sent you the WPA wordlist, NYHCxPurity. Enjoy!

Riku9182 - July 20, 2011, 7:48 pm

I liek the guide thanks alot :0

LostSoul - July 20, 2011, 9:21 pm

This is a great guide Magnus, it's really easy to understand. Good job!

Can you pm me that WPA wordlist?

erk2525 - July 20, 2011, 9:25 pm

What's my problem if my packets keep counting up to like 21k and I never get asked do you want to send packets? Y or n? Thanks for the help in advance!

nike1123 - July 21, 2011, 12:09 pm

Which disk image file do I load on the usb using UNetbootin?

Magnus - July 21, 2011, 1:21 pm

You need to load the GNOME 32 bit version you downloaded.

nike1123 - July 21, 2011, 1:21 pm

How do u get back out of monitor mode once you have the key cracked??

thanks Magnus for the last answer

I found that "airmon-ng stop [wireless interface]" puts it back into managed mode

Magnus - July 21, 2011, 1:36 pm

Yep, nike1123. That's the right command.

nike1123 - July 21, 2011, 2:06 pm

Magnus, please PM me the dictionary file...thanks

regarding "Replace WEPcrack with the filename you chose before when capturing the data"

I don't see the step where you chose a filename?

EnUfor - July 21, 2011, 7:13 pm

Overall wonderful job on the tutorial including pictures and a well written out description of both parts

and incorporating a good layout. I'm going to PM you about the wordlist because I have not really had success with the ones I have used so far.

wanttoben01 - July 22, 2011, 8:02 am

nice work dude thank u very much

Magnus - July 22, 2011, 8:07 am

No problem, wanttoben01. I just try to help members as much as I can!

w1ns0ck - July 22, 2011, 8:20 am

Hey great tut dude , ive been trying to use this on my own router to get it to work but it seems I'm getting a ton of "Lost" and even if I get up 500k Data it still won't crack the WEP key. Anything I should do? I followed the tut word for word and its not getting me anywhere.

Magnus - July 22, 2011, 8:28 am

Maybe you are making a mistake somewhere, w1ns0ck?

w1ns0ck - July 22, 2011, 8:55 am

I just rebooted my laptop and ran it again the "lost" went down big time just waiting on enough data to see if it actually works.

NYHCxPurity - July 22, 2011, 3:05 pm

Magnus

Concerning the Dictionary, that you so Graciously gave me, Im using Frostwire to download it. Simply because its what i have. How and where would i put it on my USB drive after i have finished downloading it onto Frostwire/PC.

So i just refreshed a bunch of times, Not seeing my last post go up. So here we go again.

Concerning the Dictionary file you So eloquently provided me with. Using frostwire to DL it. After its Downloaded. will it be unzipped? as in will it be a 13gb file for me to put it on my USB. or will it be the size of what i downloaded it as. which is 4900mb. Due to the fact is all i have is a 8Gb USB im using. If its bigger than that is there a way to shrink it possibly with it still having a chance. to crack WPA.

Magnus,

Do i have to decompress the Zipped Dictionary file? or can i put it on my USB like it is?

kevinrestiaens - July 23, 2011, 5:36 am

Daamn ;o you make your tut's like a pro ;o

Don't stop making great tutorials!!

This is the best tut I ever saw!!

big_bird - July 23, 2011, 5:51 am

damn do you really need all 13gb?? I don't have the money to buy a HDD :(I guess I can't do this tutorial

alexander_ru - July 23, 2011, 7:00 am

Very good job. Thanks for this incredible tut. Keep it up !

Magnus - July 23, 2011, 7:34 am

No, you don't need the 13GB wordlist. You can use any other ones.

NYHCxPurity - July 23, 2011, 1:56 pm

Magnus,

Do i have to decompress the zip file of the WPA wordlists or can i put it on my usb as is?

stevedabomb - July 23, 2011, 6:11 pm

could you pm me the link for the word list cheers

Magnus - July 23, 2011, 6:21 pm

(Jul 23, 2011 01:56 PM)NYHCxPurity Wrote: [\[CITE\]](#) Magnus,

Do i have to decompress the zip file of the WPA wordlists or can i put it on my usb as is?Yes you do. Because if you don't via Windows, it's harder via Linux.

H1ppy - July 24, 2011, 12:55 pm

One of the best Wifi Hacking TuT's i have seen in a while job well done mate!

Spoonergod - July 24, 2011, 2:05 pm

Thank you this was really helpful ?

joshuano - July 24, 2011, 2:18 pm

Very detailed guide thanks

Magnus - July 24, 2011, 2:25 pm

No problem guys. Just helping out. And it seems like 80% of the people that posted are newbie posters with only 10 or less posts. :)))

Rogue.Asasino - July 24, 2011, 9:39 pm

Very good guide. I will try this when i get back home :D

Magnus - July 24, 2011, 9:54 pm

Alright. You should do that, Rogue.Asasino.

insert_username - July 25, 2011, 5:25 am

im no newbie ;P well i was :P

Jummez - July 25, 2011, 11:14 am

Thanks awesome guide helped me alot

babana - July 25, 2011, 1:52 pm

Great tutorial. Easy on the eyes, and full of easy to understand info.

Spark! - July 25, 2011, 4:46 pm

Can you send me the torrent for the wordlist?

snipper man11 - July 26, 2011, 5:39 pm

Hey, noob question here. But why would I need a wireless card if one is already built into my laptop?

tuzzinflubs - July 27, 2011, 1:11 am

thank for the tut very informative

aDeal - July 27, 2011, 9:18 pm

wonderful ..really nice work man

Could you please PM me that wordlist, pls

thx ^^

epiphanyro - July 27, 2011, 10:42 pm

Thanks for the guide, it was very easy to follow.

nike1123 - July 27, 2011, 10:56 pm

Magnus,

could really use that dictionary u were offering... ur pm quota is full...thx

Mr.Oug - July 28, 2011, 1:37 am

How to save the data wep*cap i cant follow that step

hey magnus please explain the place where you save the cap file thanks. :)

Stewie™ - July 28, 2011, 2:11 am

Good, In depth Tutorial.

I suggest anyone who wants to "Test" the Security of Wireless Networks actually goes and educates themselves about how WEP/WPA encryption works. Otherwise you'll just be inputting commands into the Aircrack suite without really understanding what you are doing. The Aircrack Team have plenty of documentation on this; <http://www.aircrack-ng.org/>

For anyone looking to Crack WPA, there's a 36GB wordlist sitting around on these forums; Just search for it. It's a 700MB .zip file so it won't take long to download (everyone seems to think it's an actual uploaded 36GB text file without the compression). Save it to a suitable storage device and start the dictionary attacks through whichever WPA cracker you choose on Backtrack (Aircrack, CowPatty, Pyrit etc.).

nike1123 - July 28, 2011, 5:39 am

ANYONE got that wordlist that they can PM me?...thx

MikeTheNumbers - July 28, 2011, 6:06 am

Nice job :D

Really helped me out

xxbadzvincexx - July 28, 2011, 11:42 pm

thanks for this sir magnuz ?

Asid Burn - July 29, 2011, 6:43 am

thanks for sharing

can i have the word list torrent

nike1123 - July 29, 2011, 5:15 pm

anyone have a WORDLIST that is not corrupted? the 30GB+ one I got from the megavideo was corrupted

jpsanjuan - July 29, 2011, 7:11 pm

What do I do if the terminal can't be open?

It keeps on saying that it has an error...

seawolve1 - July 30, 2011, 11:58 am

WOW.... Great information... Thanks for putting it together and sharing with us!

drnick2 - July 30, 2011, 3:02 pm

Wow a tutorial for everybody to understand, great job and layout. I would love the link to download the wordlist you mentioned, can you PM me with that.

Momo - July 30, 2011, 3:24 pm

Thanks for this tutorial!

iTzAs1anAiD4n - July 30, 2011, 6:56 pm

Can i have the WPA Word List? BTW Awesome Tutorial! I have Been Looking For A While :) And i have a question, Your using a WLAN but how do i know what I use?

Wheelz - July 31, 2011, 3:48 am

This is an awesome tutorial, thanks so much for it : D

Efz - July 31, 2011, 10:55 am

Perfect job! More tutorials like this ! :) keep going!

mkarmi - July 31, 2011, 12:39 pm

Great tutorial ,easy to understand Thnx :)

AlexT - July 31, 2011, 4:26 pm

That must be the best TUT i have seen on here, well done poster.

kinoman5 - August 2, 2011, 12:19 am

Great tutorial!

I have a question. The WPA lists I obtained are in text format and there are quite a lot of them. For the last step when you have to input the list, do I have to merge them into one file or put them into a folder?

Thank you!

Shudsy - August 2, 2011, 12:25 am

Excellent guide, very easy to follow. Thanks.

Duncskunk - August 2, 2011, 2:52 am

Awesome tut, easy to understand thanks ;)

jinzo12 - August 2, 2011, 9:08 pm

This is a GREAT tutorial, Thanks so much.

Demonic Wraith - August 3, 2011, 5:47 am

thanks for this very informative - yeah if anyone has a word can they either post in here or pm search doesnt have many word lists on here either

Dayates78 - August 3, 2011, 2:35 pm

Why Cant This Be Simple, I mean dont get me wrong its fun and challenging but sometimes people just dont have the time to do it the long way

The3CrYs1s - August 3, 2011, 3:21 pm

GOOD JOB MAN!!! this is really good, keep it up
AND THANK YOU SO MUCH BY THE WAY

pelly120 - August 3, 2011, 6:08 pm

Thank you so much for posting, Magnus. It really helps

kenny457802550 - August 4, 2011, 2:43 am

thanks man. u really helped me out here :D

SoMuchMudkip - August 4, 2011, 4:40 am

Does anyone have this wordlist? The OP has been away for several weeks.

Nosspeedca - August 4, 2011, 11:46 am

awesome so helpfull!

Any links for a good word list?

ikid - August 4, 2011, 2:40 pm

Awesome!

Thanks a lot!

I'm new here but already in love:D

elemein - August 4, 2011, 2:44 pm

(Aug 3, 2011 02:35 PM)Dayates78 Wrote: [\[CITE\]](#) Why Cant This Be Simple, I mean dont get me wrong its fun and challenging but sometimes people just dont have the time to do it the long way
You could do it without a wordlist or the backtrack distro and just use aircrack on its own. No pyrit or coWPATTY.

This is simple kid. Dont like it? Too bad.

Flowz - August 4, 2011, 3:10 pm

Thanks :) I knew how this worked a year ago and I needed someone to fresh it up for me :D

jamezon3_18 - August 4, 2011, 5:27 pm

Thank for this man! I'll going to try this if I have vacant time.

Anyway! How can I get Wordlist?

Does Backtrack 5 functional to Windows Vista sir?

Can You PM me the link for Wordlist please?

ntarun009 - August 5, 2011, 8:01 am

how will we open the pendrive as the booting program????

jamezon3_18 - August 5, 2011, 8:14 am

(Aug 4, 2011 03:10 PM)Flowz Wrote: [\[CITE\]](#) Thanks :) I knew how this worked a year ago and I needed someone to fresh it up for me :D

Sir Flowz, Can I ask a copy of your Word List please?

Flegy - August 5, 2011, 9:39 am

hey can you tell me what wireles card is the best use for crash wifi, my isnt compatible.thanks

D3r0gat0ry - August 5, 2011, 12:37 pm

I already have BT5 on a thumbdrive; is it possible to unzip the wordlist in windows onto my hard drive, and then access it from BT?

I have done this before when everything is on one drive, but never for two separate drives.

Jamann - August 5, 2011, 1:56 pm

Hey could I have a link to the torrent for the wordlist?

S?arlet - August 6, 2011, 12:46 pm

beautiful tutorial! thanks for posting this

gun404 - August 6, 2011, 1:57 pm

hey, can you share the wordlist with me too via PM?

also you might wanna add that you cant simply kick people from their wifi connection like that. it works on some routers, but not all.

Flegy - August 8, 2011, 2:55 am

(Aug 5, 2011 09:39 AM)Flegy Wrote: [\[CITE\]](#) hey can you tell me what wireles card is the best use for crack wifi, my isnt compatible.thanks
every answer is welcome?

zz again is

dvan - August 8, 2011, 6:16 pm

thank you. i read that you spent al lot of time makeing this and you right you deserve a thks. it helped me a lot appreciated i t

LePrestige - August 9, 2011, 9:38 am

Hello!

I've selected Disk-image in Unetbooting. However, can find the driver name.

When I try to click OK, it said, I need to reformat my USB driver to FAT32.

I use portable hard driver 500GB.

Can someone help me.

Thanks.

Maker909 - August 9, 2011, 6:16 pm

just wondering do i need to go out and buy a Compatible Wireless Card even though i have a laptop with Wi-Fi and all ?

also if i do can u send me a link to a good one ? :D

Flegy - August 11, 2011, 12:37 pm

(Aug 9, 2011 06:16 PM)Maker909 Wrote: [\[CITE\]](#) just wondering do i need to go out and buy a Compatible Wireless Card even though i have a laptop with Wi-Fi and all ?

also if i do can u send me a link to a good one ? :D

yes you need buy compatible wireless some laptops dont have it,first check did is compatible,I also looking for one compatible

TheNullz - August 11, 2011, 3:15 pm

Can you please PM me the dictionary file? Thanks in advance because I am unable to send to a private message \:

wanako1 - August 11, 2011, 11:17 pm

Thanks Man...
Nice Tutorial
I will Try it as Soon as Possible

Rafe_D - August 11, 2011, 11:23 pm

Awesome tutorial mate. Thanx. Could you PM a link to the dictionary please. I haven't posted enough to P.M. yet.

brandonnye - August 11, 2011, 11:30 pm

confusing but I'm going to watch it 50 times over until I understand it lol

MikeTheNumbers - August 12, 2011, 1:16 pm

Your pm inbox is full.. Could you pm me the link or something like that :D

Bamarah - August 13, 2011, 3:50 am

Definitely 1 of the best tutorials I have read. Great job! Keep up the good work!

rikkyyy - August 13, 2011, 12:25 pm

Very nice Tutorial, I'll use it if i got a "Compatible Wireless Card"
Thanks alot

falcon22 - August 13, 2011, 2:48 pm

Im trying to make the bootable usb but get a "you must select a disk image to use" message when pressing ok. the tut doesn't say anything about selecting a disk image to use after ticking the box that says "diskimage" instead of "distribution". do in need to have all the backtrack files on the usb beforehand and choose one of those as the diskimage. if so, which one? (im doing this in windows, to then be used in ubuntu, by the way, cos ubuntu is an absolute nightmare to do anything with! also, whats actually wrong with just selecting Backtrack in the distribution options? could i not just do that?

AnAngryBlackMan - August 13, 2011, 3:13 pm

Love your guide :) Easy to understand and follow, but can you PM me the wordlist plz?

Thanks in advance ;)

falcon22 - August 13, 2011, 3:22 pm

hey, AnAngryBlackMan, dont suppose you could tell me what Im supposed to do at the point where i should choose a disk image file to open, whilst making the bootable usb? idk what image it means? Nice name by the way.
nevermind, i followed the guide from the backtrack site, turns out i had the wrong backtrack on my usb! jesus iv been such a spaz today.

nike1123 - August 17, 2011, 5:35 pm

Getting the handshake...no problem. Getting the authentication and association...no problem. Being able to run aircrack-ng on a file larger than 1.5 gigs....BIG PROBLEM. Any ideas....anyone?!! Feel free to pm me

Bonsai99 - August 17, 2011, 6:04 pm

(Aug 17, 2011 05:35 PM)nike1123 Wrote: [\[CITE\]](#) Getting the handshake...no problem. Getting the authentication and association...no problem. Being able to run aircrack-ng on a file larger than 1.5 gigs....BIG PROBLEM. Any ideas....anyone?!! Feel free to pm me
I don't see why you would ever have a capture file that large, I think you are doing it wrong.

4nt190v - August 17, 2011, 8:48 pm

this is the best tutorial i ever watched..keep it up

10halec - August 17, 2011, 10:53 pm

Thank you for the post, very informative!!

Ryan` - August 18, 2011, 9:57 am

very nice guide.. goodjob, and thanks for the post

uphero - August 19, 2011, 10:08 am

very very nice i like this tut its very usefull i hack one pass wi-fi now

sadia06 - August 19, 2011, 1:03 pm

hye..im new here...is it can be done if im using ubuntu as my platform ? already got 2os inside my laptop..so kind of waste to install backtrack some more..) thx in advance

JackChitt - August 19, 2011, 4:05 pm

(Aug 19, 2011 01:03 PM)sadia06 Wrote: [\[CITE\]](#) hye..im new here...is it can be done if im using ubuntu as my platform ? already got 2os inside my laptop..so kind of waste to install backtrack some more..) thx in advance

boot from flash drive or live disk.. :) (message but got to the point)

nike1123 - August 19, 2011, 6:14 pm

(Aug 17, 2011 06:04 PM)Bonsai99 Wrote: [\[CITE\]](#) I don't see why you would ever have a capture file that large, I think you are doing it wrong.

Not the capture file...the dictionary. I've run aircrack-ng without errors with smaller dictionaries but the password was not found. When i try to use larger dictionaries i get "can not open" errors. I think i saw someone say aircrack has a 2 gig limit and you have to split up larger files but I don't remember where that thread was to get to syntax

Terrified - August 19, 2011, 11:16 pm

So during the attack i did, my Live USB ran out of disk space while trying to reach 10k IV's. Is there a way to get more space or change the home directory for it? I just realized it gives itself it's own set amount of disk space, and the Wep*.cap, ended up filling that up before it had enough time to finish. So therefore, leaving me without a paddle.

Well I got it to save the data to my HDD and somehow it saving the IV's are now like 30x faster than before when it was saving to itself. I assume that's normal. Too bad I have to remount my HDD everytime I load my Live USB though.

timmy2000 - August 20, 2011, 2:28 pm

Could someone please PM me the torrent link to the dictionary file. I'm not quite at the point where I need it yet (having issues with handshaking) but hopefully it won't be long.

Flegy - August 20, 2011, 2:42 pm

anyone know wich one is compatible need buy one...

goku944 - August 20, 2011, 5:33 pm

thanks its wonderful and easy..could you please pm me wpa wordlist..

necdet_87 - August 20, 2011, 5:58 pm

thank you very much for your help.. I tried this on my netbook, it didn't work. I will try this on my friend's notebook.. I hope it will work..

I need word list, can anyone send its link to me? Because I can't send any pm to Magnus.. =(

rl1dragon - August 20, 2011, 7:01 pm

(Aug 13, 2011 12:25 PM)rikkyyy Wrote: [\[CITE\]](#) Very nice Tutorial, I'll use it if i got a "Compatible Wireless Card"

Thanks alot

If you dont have a "Compatible Wireless Card", i would suggest you get the Alfa AWUS036H USB adaptor, since it is fairly cheap, Ebay ~ \$2X. It is also packet inject compatable.

I always had this one question also. Once you are able to get access to the router from this method, is there a way to use the router to get access to the computers connected to the router?

Maker909 - August 21, 2011, 12:56 am

is this adapter a good choice ?

<http://www.amazon.com/USB-N13-Wireless-N-Adapter-802-11b-Wireless/dp/B002UVNW5W>

still dont really know.. do i need a usb adapter no matter what laptop i have or do some come with a adapter inside ? and if so then how do i check it ?

thx alot for help :D

sadia06 - August 21, 2011, 1:21 am

(Aug 19, 2011 04:05 PM)JackChitt Wrote: [\[CITE\]](#) boot from flash drive or live disk.. :) (message but got to the point)hye jack..so its mean I really need to use ONLY backtrack to done this ?

No way for me to use ubuntu ? can I know the reason ?

I know how to liveboot from flash drive or else..just want to know the reason..thx in advance..:)

papungskie - August 21, 2011, 4:07 am

awsome tutorial man...thanks for this...

pugothefake - August 21, 2011, 5:43 am

Hey i need to know something.

I got a BT5 KDE and have installed it in the VM VirtualBox 4.1.0

Now when i am using airmon-ng i am not able to see any Interface.

This is what i see...

```
root@bt:~# airmon-ng
```

```
Interface Chipset Driver
```

```
root@bt:~# _
```

```
..
```

is there some problem in my network settings?? or is there something else.?

also when i type ifconfig .. i only get these options with their details..

eth1 (and its details)

lo (and its details)

but no wlan0 anywhere...!

do let me know man....

thanks....

Terrified - August 22, 2011, 2:36 am

(Aug 21, 2011 05:43 AM)pugothefake Wrote: [\[CITE\]](#) Hey i need to know something.
I got a BT5 KDE and have installed it in the VM VirtualBox 4.1.0
Now when i am using airmon-ng i am not able to see any Interface.

This is what i see...

```
root@bt:~# airmon-ng
```

```
Interface Chipset Driver
```

```
root@bt:~# _
```

```
..
```

is there some problem in my network settings?? or is there something else.?

also when i type ifconfig .. i only get these options with their details..

eth1 (and its details)

lo (and its details)

but no wlan0 anywhere...!

do let me know man....

thanks....

I think that's because when you use VMWare, it normally bridges the connection and uses your Windows MAC and Windows IP, as well as your Windows Network Adapter. When it does this, Backtrack sees your connection as a Wired connection and not wireless. Now I THINK you can change this by when you start up your VMWare for Backtrack, you'll see a list of icons at the bottom right. Should be one for your CD drive, HDD, Sound, and Internet connectivity. As well as the Wireless Network USB, if you're using a USB network adapter that is. If it is a USB, right click, and choose (Connect, Disconnect from Host) and see if it can find your wireless now. If not, try to reboot the VMWare and try again. If it's built in, I won't be quite sure. If it is, maybe you can make a Live USB and go from there.

lil Bullseye - August 22, 2011, 7:49 am

great tutorial but this is so goddamn frustrating DX I've tried to install BackTrack 3 times, then I finally get it and it turns out that it's the wrong bit(virtual pc is only 32 bit D:) and it took me 2 MORE downloads because my computer kept losing the source if I let the computer hibernate(2 hour

download) then I finally get the right version and NetBootin keeps being weird until I realize (obviously) I need to use a USB drive, but the only drive I could find was only 2GB (way too small) and the only other drive I had was an external hard drive holding my complete old computer. I deleted some stuff from it, and tried to use it but it was not found because it wasn't FAT32 so I spend 4 hours trying to format the stupid thing only to have my computer freeze and crash at over half way. Then I looked for a program to do it for me and find one that will format to FAT32 on windows 7, go through a couple programs, and get one that I THOUGHT would work but after formatting it still didn't show up, so I'm back now to trying to format it using DOS and I'm praying it will actually work this time(because this is the second time the first time after the software my computer restarted for updates while I was asleep) I HOPE THIS FUCKING WORKS. But yeah great tutorial ^.^

Terrified - August 22, 2011, 8:41 am

(Aug 22, 2011 07:49 AM)lil Bullseye Wrote: [\[CITE\]](#) great tutorial but this is so goddamn frustrating DX I've tried to install BackTrack 3 times, then I finally get it and it turns out that it's the wrong bit(virtual pc is only 32 bit D:) and it took me 2 MORE downloads because my computer kept losing the source if I let the computer hibernate(2 hour download) then I finally get the right version and NetBootin keeps being weird until I realize (obviously) I need to use a USB drive, but the only drive I could find was only 2GB (way too small) and the only other drive I had was an external hard drive holding my complete old computer. I deleted some stuff from it, and tried to use it but it was not found because it wasn't FAT32 so I spend 4 hours trying to format the stupid thing only to have my computer freeze and crash at over half way. Then I looked for a program to do it for me and find one that will format to FAT32 on windows 7, go through a couple programs, and get one that I THOUGHT would work but after formatting it still didn't show up, so I'm back now to trying to format it using DOS and I'm praying it will actually work this time(because this is the second time the first time after the software my computer restarted for updates while I was asleep) I HOPE THIS FUCKING WORKS. But yeah great tutorial ^.^

Dude just make a free partition with that drive, boot Backtrack with a Live CD, and then install Backtrack onto that drive as a Dual Boot OS with the install option once you load Backtrack. It would be 100x simpler if you did so.... You could even do 64 bit if your computer is 64 bit

The_Varuker - August 22, 2011, 7:36 pm

finally got it working... Didnt use BT tho, just ubuntu and aircrack-ng. Worked like a charm after the 20th time....

Maker909 - August 22, 2011, 9:03 pm

can some1 please send me the file :D

Stage0 - August 22, 2011, 10:25 pm

why am i stuck at 39% =(! its been 2min!!

rikkyyy - August 24, 2011, 10:58 am

im getting this is that meaning my Card isnt Comaptible or something?

[IMG][http://i56.\[censored\].com/10orars.png](http://i56.[censored].com/10orars.png)[IMG]

Sorry for being noob(:

Regards

Rikkyyy

Btw i have a Atheros AR9285 802.11b/g/n WiFi Adapter

any help please?:(

nike1123 - August 24, 2011, 3:02 pm

WORDLIST ISSUE: when i used one wordlist it showed that it was going through the different psd's. when using another one that i had to split up cause it was too big it doesn't do that....just says "password not in dictionary". Is that an error, should i see it parsing through the dictionary?

Oechikr - August 25, 2011, 1:54 am

Thanks for this tutorial, it helped me crack my first network. It took 400,000 packets and 23,621 IV's to crack it.

Aaron565 - August 27, 2011, 2:33 pm

Im on windows....:(can someone tell me a way to hack into a network on Windows 7? Or at least tell me how to get linux

Jummez - August 27, 2011, 5:14 pm

Thanks for the Tut it was awesome and helped alot

Frag - August 27, 2011, 8:02 pm

This tutorial is fuckin beautiful.

+rep for your awesome contribution to HF :)

arbarwings - August 28, 2011, 12:27 am

Any 1 have a ubuntu download lin for my ?

BigBud - August 28, 2011, 5:22 am

Programme a télécharger : <https://#.com/files/725129736/MKS-Hack.rar> ,
<http://www.#/?d=K0YGABH1> Bon Hack a tous ;)

Bendfella - August 28, 2011, 9:54 am

this is the best clear wep tutorial on the whole internet. i never liked changing the mac address at all. takes unnessecary time

Kisna - August 30, 2011, 7:56 am

Thanks a ton man. Worked like a charm for me.

pugothefake - August 30, 2011, 9:06 am

(Aug 22, 2011 02:36 AM)Terrified Wrote: [\[CITE\]](#) I think that's because when you use VMWare, it normally bridges the connection and uses your Windows MAC and Windows IP, as well as your Windows Network Adapter. When it does this, Backtrack sees your connection as a Wired connection and not wireless. Now I THINK you can change this by when you start up your VMWare for Backtrack, you'll see a list of icons at the bottom right. Should be one for your CD drive, HDD, Sound, and Internet connectivity. As well as the Wireless Network USB, if you're using a USB network adapter that is. If it is a USB, right click, and choose (Connect, Disconnect from Host) and see if it can find your wireless now. If not, try to reboot the VMWare and try again. If it's built in, I won't be quite sure. If it is, maybe you can make a Live USB and go from there.

Yeup... i'll have to use the Live Boot option from the HDD and do it...

thanks... :)

pOgon - September 4, 2011, 6:46 am

Amazing tutorial, yes. I will defenetly use it! (I just noticed it though)

pr0xibus - September 4, 2011, 11:52 am

One of the many tutorials about, but i like that you used "aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0". Not alot of people use this one. good tut one of the better ones.

cthulhu57 - September 5, 2011, 3:53 am

Awesome tutorial, worked great for me! Thank you very much!

Arkash - September 5, 2011, 5:35 am

Well done guide and very understandable.

Magnus - September 8, 2011, 4:19 am

Wow, for the time being I was trying to gain access to my account this thread went up to 355+ replies.

m7_jalal - September 8, 2011, 3:17 pm

thank a lot that's I want .. that's I'm looking for)

P47R!K - September 9, 2011, 4:51 pm

Best best, in real sence of the word! I only can tell awesome 5/5 and a big TANKS for such a structured art. Hats down?

baquajean - September 9, 2011, 7:43 pm

Hey Magnus!

Great JOB! any tip about the dictionary?Im downloading one rar that has 1.35, but yours is bigger. Any links?

Thanks in advance

B.

Click Me - September 10, 2011, 12:18 pm

Great tut, thanks very much :D

Tooshortforme

jules_erich - September 12, 2011, 5:37 am

thank you very much!

very informative...

Middle - September 12, 2011, 1:12 pm

Howry shiiiite we got a mother fucking sticky!!

Woop Woop! Dats da sound of da modz! Woop Woop!

Dear Magnus, mind if i write a FAQ to go at the top of your thread? And then you could include links to all the other good tutorials and stuff?

Cheers :D

Jacksonova - September 12, 2011, 6:23 pm

Hey can i get that 13GB wordlist please

Thanks in advance

beastmode16 - September 12, 2011, 9:45 pm

very nice job man... great share.. Thanks for it! They're very valuable..

khm2008 - September 13, 2011, 7:25 am

Tanxs been messing with back track never got it to do anything il try this way tanxs again for the time to write/post up

sBep - September 13, 2011, 9:41 am

Finally a sticky here ?

Hopefully now there won't be so much n00bish repetitive threads.

beanheadkid - September 14, 2011, 9:13 am

good detailed guide! thanks alot :D

Magnus - September 14, 2011, 2:13 pm

(Sep 12, 2011 01:12 PM)Middle Wrote: [\[CITE\]](#) Howry shiiiite we got a mother fucking sticky!!

Woop Woop! Dats da sound of da modz! Woop Woop!

Dear Magnus, mind if i write a FAQ to go at the top of your thread? And then you could include links to all the other good tutorials and stuff?

Cheers :DYeah, answered to your PM. Write up to 10 questions and answers and I'll put it up there.

acidburn123 - September 14, 2011, 11:59 pm

where i can find ..Places > Home Folder?

Sno - September 15, 2011, 3:18 pm

Thanks man, im going to try this tonight..?

thanks man, going to try this tonight

Magnus - September 15, 2011, 3:35 pm

Places > Home Folder is on the menu you see on the very top.

raax42 - September 16, 2011, 5:04 am

Can you tell me what to do if passphrase is not in Dictionary.

Thanks

samhussain - September 17, 2011, 7:56 am

awesome tutorial brother, i really like it, can you please how to download this software? please... pm meee pleaseee

twitchydude117 - September 17, 2011, 4:02 pm

thanks for the great tutorial it really helped

slzy405 - September 18, 2011, 5:32 pm

great post. easy to follow. thanx a million. keep up the good work

siefer69baby - September 20, 2011, 12:48 pm

thanks a lot. very detailed. i will try these out

neophreaky - September 22, 2011, 10:49 am

I love this post. It is very helpful. Thank you.

magnu3 - September 22, 2011, 12:34 pm

looks great, Ive been looking for something like this thanks

N3vvl3_H4C3R-77 - September 22, 2011, 5:55 pm

hello, im a new hacker as my name implies, but i have a couple of questions and ive done some extensive research in the field of WEP and WPA hacking and id appreciate it if you would answer some of those questions. (im too lazy to post 10 times otherwise i would've pm'ed you... lol)

Vmk2 - September 22, 2011, 6:31 pm

Fantastic guide. thank you. once i get a flash drive i'll give it a go.

Magnus - September 22, 2011, 9:46 pm

Post the questions away, Newbie hacker.

Capps - September 22, 2011, 9:54 pm

M49nU2 12 4 n008. 1m 53r10U2 h3 12. Only N07 r34lLY, H3 12 7h3 8357 N3w813 h4x0R3R w17 u83R 5k1LL2. 1 w4N7 70 H4X0r L1K3 h3 D032.

Magnus - September 23, 2011, 4:04 am

Everyone wants to hax0r like me, Bentley. ?

CannyH - September 23, 2011, 10:56 am

Very nice Tutorial Magnus.

I want the dictionary file but I can't PM you because I have under 10 posts.. can you send me the file?

??????M1kep?????? - September 24, 2011, 9:27 am

Amazing tutorial i did this with no experience at all in any linux related operating system thx!!!

dexpaulw - September 24, 2011, 10:14 am

Great Work. My internet speed is rather slow. Still downloading and at 45%. Thanks

Spike.Bosen - September 25, 2011, 7:01 pm

Great tutorial! Could I get a copy of your dictionary file. I would pm you but I have too few posts.

ManUnited - September 26, 2011, 5:37 am

Damn that is one awesome TUT right there. Congratulations on the Sticky it's well deserved.

Invulnerability - September 26, 2011, 10:27 am

Great tutorial...I understand all info that u give

Thanks magnus

thedamu5150 - September 26, 2011, 10:48 am

magnus great tutorial i have 2 questions can you send me the torrent link for the word list and when reading you said to use a usb or dvd could you explain to me how to get it bootable on a dvd thanks

Okay so now lets open a new terminal and we are going to attempt to crack it with the amount of data we have. I recommend getting over 20000 data before trying to crack it. So let's type aircrack-ng WEPcrack*.cap. Replace WEPcrack with the filename you chose before when capturing the data, and don't forget to add that asterisk after the file and the extension which is .cap.

i dont get the part replace wep crack with file name what is the file name

Noxar - September 27, 2011, 12:02 am

Awesome work! Easy to understand and the pictures are nice and avery good explaining text! :D (Y)

MarkW7 - September 27, 2011, 7:28 am

Nice layout. Congratulations on the sticky, it might finally stop people posting threads about the same thing.

COR7AKE - September 28, 2011, 9:04 pm

Hi nice tutorial I love it it was really useful for me but can I know why you recommend Gnome ? I always used KDE

DFTCHE - September 28, 2011, 9:50 pm

How do we know if we have a compatible wireless card?
Great tut.

jclark123 - September 30, 2011, 9:01 am

Excellent work, very detailed. I would also be interested in the dictionary word file, can you provide a link?

Many Many Thanks,
JC

BTW, the PCMCIA card I'm using is a D-Link AirPlus G, model DWL-G630, seems to work fine.

JC

SIM-747925 - September 30, 2011, 12:38 pm

thanks a lot really helped me out :)

Amorous - September 30, 2011, 2:04 pm

Can you send me the words list torrent please.

Regards,

Amorous

AcidSuit - September 30, 2011, 4:06 pm

wow gret tutorial cant wait to use it hehehe

baquajean - October 1, 2011, 2:35 pm

Hey ! Really good tutorial

I cant PM, hope you dont mind I am asking about 1.9 GB file...

Thanks in advance

B.

ximar - October 2, 2011, 11:04 am

thanks for sharing.very interesting , tut is AMAZING

thanks for sharing.very interesting , amazing TuT

DBoome - October 2, 2011, 6:51 pm

Wow great tut man, thx, its people like you that keep forums like these alive and open to new (and

yes, sometimes a little slow) users.

This guide worked almost perfectly (besides a few problems I rectified along the way) right up until the last step in WEP cracking. It seems that no matter how many data packets (i only tried after 20,000 collected) i collect my IVs remain at a constant 17190, no matter how far I am to the access point or router. I've googled my ass off and i've peaked around the aircrack forums too but I can't seem to understand this, anyone else have this problem or any ideas?

Any help or even a point in the right direction would be greatly appreciated, I'll keep screwing with it in the mean time.

Also, how do you specify a channel with the `aireplay-ng -1 0 -a (bssid) mon0` command? My computer almost seems to be picking a random channel to search for the BSSID, and its kind of a crap shoot whether or not I get the right channel.

jtchow - October 3, 2011, 8:58 pm

awesome tut man my friend challenged me to hack his wifi and this was perfect. you got me 20 bucks :D

Lunahack25 - October 5, 2011, 1:29 am

Thanks for a great tutorial, and my 1st post, I've come a long way this week, from not knowing squat about linux/backtrack, to getting to grips with the basics or cracking.

This pictorial has helped loads. Respect m8!

usman2k_us - October 5, 2011, 3:15 am

well its good but its very lengthy to understand please explain in a very simple step by step

jtjoe33 - October 5, 2011, 3:29 pm

AMAZING You helped me so much I cant even tell you!

Accidental Suicide † - October 5, 2011, 8:39 pm

?

Awesome tut!! Thanks! Works great!

omigaaad - October 7, 2011, 7:24 am

Awesome!! Nice and detailed :D going to try on my own Wi-fi :)

AdverseYaw - October 7, 2011, 5:28 pm

Thanks for the tut! Very well put together. Magnus if you still read this thread I would love a PM with the link to the dictionary file. Thanks!

boyg3nius - October 7, 2011, 7:13 pm

Awesome! I'm DL'ing BackTrack now and will be looking to get a word list soon... I'm PM you but I still have to make like 9 more posts ?

N3vvl3_H4C3R-77 - October 7, 2011, 10:53 pm

i like the tutorial so far, im currently trying to download the backtrack 5 but for some reason its taking forever... :/ anyways this tutorial deffinitely explains how to crack WEP keys better than any other tutorial ive ever seen>>> and trust me thats a lot good work :)

xraye - October 8, 2011, 9:02 pm

Wow this is a great tutorial. I've been trying to understand this for awhile but haven't been able to. But something like this that explains the basics is great and lead to me understanding the detailed tutorials on their site.

Bernd_Klaus - October 10, 2011, 4:05 am

Nice work!

Awesome tut dude!

Can you please PM me because of the wordlist, 'cause i need 10 posts :/

Xhizor14 - October 11, 2011, 6:11 am

Thanks for spending your time on creating such a detailed guide.

Edit: Also like Bernd_Klaus ^ said. Could you please PM me the torrent link to the dictionary file, I would very much appreciate it.

Thanks once again. :)

Ditolak - October 11, 2011, 9:02 am

Wow, great stuff here. Going to do this later.

scrivana88 - October 12, 2011, 9:19 am

Nice Post! Perfect for beginners. I think people should understand networking before they get into cracking. Understanding terms is key

Strategist - October 12, 2011, 2:17 pm

Thank you for the great tutorial dude! Appreciate the hard work you put into it!

Luke- - October 16, 2011, 3:01 am

Good work!

A clear and concise tutorial.

Well done[/u]

loldongs - October 16, 2011, 6:20 pm

Can I get the wordlist Since I cant pm yet. Thanks I would really appreciate it.

usman2k_us - October 16, 2011, 6:41 pm

well everything is completed. so there i can't search the other users passwords,how can i watch?

iRead - October 16, 2011, 11:36 pm

Hello and welcome to my tutorial about wireless networking. Today I'll be teaching you how easy it is to obtain access to a wireless protected network. There are lots of questions coming from the beginners on how to crack WEP/WPA/WPA2 keys and accessing their neighbor's connection. The purpose of this tutorial is to answer them. Judging from the "tutorials" on youtube which are either obsolete, or simply misguiding the listeners, this tutorial will be different. I will be covering all of the aspects and ways of hacking a network and gaining access to the router. This tutorial will be divided in 2 parts, such as WEP and WPA/WPA2 hacking. Please read below on what you need to succeed.

Backtrack 5 - I would suggest GNOME, 32Bit, ISO & Direct

Compatible Wireless Card
WPA Word List - Search via torrents to find one

Making a bootable USB
WEP encrypted networks
WPA/WPA2 encrypted networks
Commands Used

This is the most vital step that you need to succeed in before learning how to use backtrack and actually hack WEP/WPA networks. Please follow the easy steps below:

Download & Run UNetbootin
Tick Diskimage instead of Distribution
Select USB Drive as the type, and select your USB drive name - Example: F:\
Click OK and wait a couple of minutes - Note: It may freeze at some point, don't worry about that

What you need for this crack are a few simple things, a copy of backtrack 5 booting off a DVD or a flash drive and a compatible wireless card that supports packet injection. Now if you can't get to this screen, and you are stuck at the terminal you get when booting into backtrack, you need to type startx and wait a couple of minutes for the desktop to show. Okay so let's begin, so first we need to open a terminal. To do that, just click the little icon that's on the right side from System. Please see the image below:

Now type airmon-ng and that command displays our interfaces. In my case I have wlan0, and now we are going to put it into monitor mode. To do that, type airmon-ng start wlan0. As you can see on the picture below it says (monitor mode enabled on mon0), and we are going to be using mon0 instead of wlan0 as our interface.

Type airodump-ng mon0 and that will start scanning for wi-fi networks. As you can see, there is a network called SKIDHACKER. Take a note of the BSSID the DATA, the CHANNEL and the type of ENCRYPTION. Please refer to the image below, if you have any trouble getting to that point.

Now we are going to set it to lock on a specific network named SKIDHACKER. To do that, type airodump-ng -c (channel) -w WEPcrack --bssid (bssid of the network) mon0. Replace (channel) with the channel of the network you are trying to crack, and replace (bssid of the network) with the bssid of the network you want to crack.

Okay so as you can probably see the data is going really slow, and we need to boost that up. We are going to need a lot more data, so let's preform one of the aireplay commands that will boost that data. Firstly, open up a new terminal and type aireplay-ng -1 0 -a (bssid) mon0 where (bssid) is the bssid of the network. Now if your wi-fi card is supported, you should see Association successful :-), if you don't see that then your card is not supported.

Now we are going to type in aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0. And now when the question Use this packet ? pops up, just push the letter y. And now as you can see in the image below, the data went high drastically.

Okay so now lets open a new terminal and we are going to attempt to crack it with the amount of data we have. I recommend getting over 20000 data before trying to crack it. So let's type aircrack-ng WEPcrack*.cap. Replace WEPcrack with the filename you chose before when capturing the data, and don't forget to add that asterisk after the file and the extension which is .cap.

And now it will attempt to crack the password. Just wait a couple of minutes for it to complete, and

once it did it will say KEY FOUND! [XX:XX:XX:XX:XX] where the X's will be random numbers and/or letters. That's not it, now to connect you will need to remove the semicolumns. For an example, if we were to have 12:34:52:66:59, the password would be 1232526659. Just log in to your Windows OS, and connect using that password.

So lets begin. What you will need for this crack is a dictionary file that we are going to use to crack the WPA/WPA2 password. Remember, the bigger the dictionary file is the greater the chance you have in cracking the password. So now you are probably wondering, where do I get a dictionary file? Well, I don't know if this is allowed or not but I recently downloaded a 1.9GB dictionary file.

To get the file please PM me, I can't risk getting this tutorial taken down. Okay, so firstly open up a terminal and once we have the terminal open we are going to type in airmon-ng which will display our wireless interfaces. In my case I have wlan0, and now we are going to put it into monitor mode. To do that, type airmon-ng start wlan0. As you can see on the picture below it says (monitor mode enabled on mon0), and we are going to be using mon0 instead of wlan0 as our interface.

Lets type in airodump-ng mon0 and this command is going to initiate the scanning process for Wi-Fi networks. As you can see in the picture below, a few WPA encrypted networks should pop up. I'm going to attempt to crack the network under the essid SKIDH?CKER. Take a note of the channel, and you want to copy the BSSID for later use.

Now we are going to type in airodump-ng -c (channel) -w (filename) --bssid (bssid) mon0, and replace the values to fit what you got from the last step. Don't forget to remember what filename you chose, because we are going to need that at the end.

What is needed to crack a WPA or WPA2 key is something called a WPA Handshake. You can obtain a handshake by kicking someone off the network, and those computers will automatically reconnect which will give you the handshake. This means, if there is no one on the network, you can't get a handshake, and you can't crack the WPA network. So how do we know if someone is connected? Well look at the lower part of the airodump command, and you will notice something as STATION, and underneath that if someone is connected it wil show you their mac address.

Once you get a handshake, airodump will alert you in the top screen, and the handshake will be located right from the time stamp. Okay, so lets open up a new terminal and we are going to kick off the computers connected. Lets type in aireplay-ng -1 0 -a (bssid) mon0. replace bssid with the network you are trying to crack and hit enter. It is going to attempt to kick off a client, and if it succeeds you will see the wpa handshake at the top right corner, if you don't run the aireplay command a couple of times.

So now that we have a wpa handshake file, we are going to attempt to crack it. Lets stop the scan by pressing CONTROL + C on the terminal where airodump is running. Now in order to find the handshake file, you need to go in the top menu and chose Places > Home Folder. Okay, so lets open up a terminal and we are going to type in aircrack-ng -w (dictionary) /root/(filename). Where filename is the filename you specified when capturing the wpa handshake and the dictionary is the path of the wordlist you downloaded. This can be done by dragging in the handshake file into the terminal after the aircrack-ng -w (dictionary) command and it will parse in it's directory. All you need to do is hit enter. The password needs to be in the dictionary file, so the bigger the wordlist is the bigger are the chances of you getting the password.

If the password is in the wordlist, it will give you a success message and the key in brackets. Happy hacking, hackers!

airmon-ng

This command displays the wireless interfaces.

`airmon-ng start wlan0`

This command starts monitoring mode on a wi-fi device.

`airodump-ng mon0`

This command shows all of the wi-fi networks online.

`airodump-ng -c (channel) -w (filename) --bssid (bssid) mon0`

This command specifies the wi-fi device to concentrate to one network.

`aireplay-ng -1 0 -a (bssid) mon0`

This command kicks off clients that are connected, and gets the handshake.

`aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0`

This command boosts the data, when cracking WEP.

`aircrack-ng -w (dictionary) (wpa handshake)`

This command is used when cracking WPA or WPA2 networks.

`aircrack-ng (filename)*.cap`

This command is used when cracking WEP networks.

These were the commands I used in the whole guide.

Nice

Hello and welcome to my tutorial about wireless networking. Today I'll be teaching you how easy it is to obtain access to a wireless protected network. There are lots of questions coming from the beginners on how to crack WEP/WPA/WPA2 keys and accessing their neighbor's connection. The purpose of this tutorial is to answer them. Judging from the "tutorials" on youtube which are either obsolete, or simply misguiding the listeners, this tutorial will be different. I will be covering all of the aspects and ways of hacking a network and gaining access to the router. This tutorial will be divided in 2 parts, such as WEP and WPA/WPA2 hacking. Please read below on what you need to succeed.

Backtrack 5 - I would suggest GNOME, 32Bit, ISO & Direct
Compatible Wireless Card
WPA Word List - Search via torrents to find one

Making a bootable USB
WEP encrypted networks
WPA/WPA2 encrypted networks
Commands Used

This is the most vital step that you need to succeed in before learning how to use backtrack and actually hack WEP/WPA networks. Please follow the easy steps below:

Download & Run UNetbootin
Tick Diskimage instead of Distribution
Select USB Drive as the type, and select your USB drive name - Example: F:\
Click OK and wait a couple of minutes - Note: It may freeze at some point, don't worry about that

What you need for this crack are a few simple things, a copy of backtrack 5 booting off a DVD or a flash drive and a compatible wireless card that supports packet injection. Now if you can't get to this screen, and you are stuck at the terminal you get when booting into backtrack, you need to type `startx` and wait a couple of minutes for the desktop to show. Okay so let's begin, so first we need to open a terminal. To do that, just click the little icon that's on the right side from System. Please see the image below:

Now type `airmon-ng` and that command displays our interfaces. In my case I have `wlan0`, and now

we are going to put it into monitor mode. To do that, type `airmon-ng start wlan0`. As you can see on the picture below it says (monitor mode enabled on mon0), and we are going to be using mon0 instead of wlan0 as our interface.

Type `airodump-ng mon0` and that will start scanning for wi-fi networks. As you can see, there is a network called SKIDHACKER. Take a note of the BSSID the DATA, the CHANNEL and the type of ENCRYPTION. Please refer to the image below, if you have any trouble getting to that point.

Now we are going to set it to lock on a specific network named SKIDHACKER. To do that, type `airodump-ng -c (channel) -w WEPcrack --bssid (bssid of the network) mon0`. Replace (channel) with the channel of the network you are trying to crack, and replace (bssid of the network) with the bssid of the network you want to crack.

Okay so as you can probably see the data is going really slow, and we need to boost that up. We are going to need a lot more data, so let's perform one of the aireplay commands that will boost that data. Firstly, open up a new terminal and type `aireplay-ng -1 0 -a (bssid) mon0` where (bssid) is the bssid of the network. Now if your wi-fi card is supported, you should see Association successful :-), if you don't see that then your card is not supported.

Now we are going to type in `aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0`. And now when the question Use this packet ? pops up, just push the letter y. And now as you can see in the image below, the data went high drastically.

Okay so now let's open a new terminal and we are going to attempt to crack it with the amount of data we have. I recommend getting over 20000 data before trying to crack it. So let's type `aircrack-ng WEPcrack*.cap`. Replace WEPcrack with the filename you chose before when capturing the data, and don't forget to add that asterisk after the file and the extension which is .cap.

And now it will attempt to crack the password. Just wait a couple of minutes for it to complete, and once it did it will say KEY FOUND! [XX:XX:XX:XX:XX] where the X's will be random numbers and/or letters. That's not it, now to connect you will need to remove the semicolons. For an example, if we were to have 12:34:52:66:59, the password would be 1232526659. Just log in to your Windows OS, and connect using that password.

So let's begin. What you will need for this crack is a dictionary file that we are going to use to crack the WPA/WPA2 password. Remember, the bigger the dictionary file is the greater the chance you have in cracking the password. So now you are probably wondering, where do I get a dictionary file? Well, I don't know if this is allowed or not but I recently downloaded a 1.9GB dictionary file.

To get the file please PM me, I can't risk getting this tutorial taken down. Okay, so firstly open up a terminal and once we have the terminal open we are going to type in `airmon-ng` which will display our wireless interfaces. In my case I have wlan0, and now we are going to put it into monitor mode. To do that, type `airmon-ng start wlan0`. As you can see on the picture below it says (monitor mode enabled on mon0), and we are going to be using mon0 instead of wlan0 as our interface.

Let's type in `airodump-ng mon0` and this command is going to initiate the scanning process for Wi-Fi networks. As you can see in the picture below, a few WPA encrypted networks should pop up. I'm going to attempt to crack the network under the essid SKIDH?CKER. Take a note of the channel, and you want to copy the BSSID for later use.

Now we are going to type in `airodump-ng -c (channel) -w (filename) --bssid (bssid) mon0`, and replace the values to fit what you got from the last step. Don't forget to remember what filename you chose, because we are going to need that at the end.

What is needed to crack a WPA or WPA2 key is something called a WPA Handshake. You can obtain a handshake by kicking someone off the network, and those computers will automatically reconnect which will give you the handshake. This means, if there is no one on the network, you can't get a handshake, and you can't crack the WPA network. So how do we know if someone is connected? Well look at the lower part of the airodump command, and you will notice something as STATION, and underneath that if someone is connected it will show you their mac address.

Once you get a handshake, airodump will alert you in the top screen, and the handshake will be located right from the time stamp. Okay, so let's open up a new terminal and we are going to kick off the computers connected. Let's type in `aireplay-ng -1 0 -a (bssid) mon0`. replace bssid with the network you are trying to crack and hit enter. It is going to attempt to kick off a client, and if it succeeds you will see the wpa handshake at the top right corner, if you don't run the aireplay command a couple of times.

So now that we have a wpa handshake file, we are going to attempt to crack it. Let's stop the scan by pressing `CONTROL + C` on the terminal where airodump is running. Now in order to find the handshake file, you need to go in the top menu and choose Places > Home Folder. Okay, so let's open up a terminal and we are going to type in `aircrack-ng -w (dictionary) /root/(filename)`. Where filename is the filename you specified when capturing the wpa handshake and the dictionary is the path of the wordlist you downloaded. This can be done by dragging in the handshake file into the terminal after the `aircrack-ng -w (dictionary)` command and it will parse in its directory. All you need to do is hit enter. The password needs to be in the dictionary file, so the bigger the wordlist is the bigger are the chances of you getting the password.

If the password is in the wordlist, it will give you a success message and the key in brackets. Happy hacking, hackers!

`airmon-ng`

This command displays the wireless interfaces.

`airmon-ng start wlan0`

This command starts monitoring mode on a wi-fi device.

`airodump-ng mon0`

This command shows all of the wi-fi networks online.

`airodump-ng -c (channel) -w (filename) --bssid (bssid) mon0`

This command specifies the wi-fi device to concentrate to one network.

`aireplay-ng -1 0 -a (bssid) mon0`

This command kicks off clients that are connected, and gets the handshake.

`aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0`

This command boosts the data, when cracking WEP.

`aircrack-ng -w (dictionary) (wpa handshake)`

This command is used when cracking WPA or WPA2 networks.

`aircrack-ng (filename)*.cap`

This command is used when cracking WEP networks.

These were the commands I used in the whole guide.

Nice

codebytes4u - October 17, 2011, 2:08 am

can someone would help a noob like me? :-)) where can i download the said wordlist?

boyg3nius - October 17, 2011, 4:16 pm

(Sep 26, 2011 10:48 AM)thedamu5150 Wrote: [\[CITE\]](#) Replace WEPcrack with the filename you chose before when capturing the data, and don't forget to add that asterisk after the file and the extension which is .cap.

i dont get the part replace wep crack with file name what is the file name
I'm way new to this so I'm guessing here, but I'm pretty sure it's a partial file name - the beginning of it - from the command:
airodump-ng -c (channel) -w (filename) --bssid (bssid) mon0

In the tutorial, Magnus uses this command in the 4th paragraph/section:
"airodump-ng -c (channel) -w WEPcrack --bssid (bssid of the network) mon0" where WEPcrack is the filename

In the screenshots, Magnus actually uses "wep" instead of "WEPcrack" - so if you're following the screenshots... he uses "wep" - if you follow the text, he's using WEPcrack and you really don't have to replace anything if you're following his commands verbatim... does that make sense?

I apologize if this has already been covered, but I've found that the last two WEP's that I've cracked I needed way more than 20,000 Data - I'm wondering if Magnus missed a zero... 20,000 didn't seem to be doing the trick, so I let it run up to 500,000+ and it popped out a KEY FOUND! in less than a minute... is anyone else finding this to be true for cracking WEP encryption or is it just me?

I also noticed that the Data column showed 0 when I first ran the airodump-ng command and didn't start escalating until I initiated the aireplay-ng commands - would this have something to do with it? Does that mean it's a dormant network and you need more collected data? (I know, I'm being kind of lazy... and this goes for you other lazy asses out there...) I could read up on the aircrack-ng.org site... but I'm hoping someone who knows will impart a little bit of wisdom for us noobs.

(Sep 28, 2011 09:50 PM)Cherub Wrote: [\[CITE\]](#) How do we know if we have a compatible wireless card?

Great tut.

when you first run the command airmon-ng, you will only see:
Interface [tab] Chipset [tab] Driver
[empty space]

[command prompt]

If you have a compatible wifi card, it will list it and it's properties in those columns.

I poked around on the www.aircrack-ng.org site for compatible wifi adapters and then found the Alfa AWUS036H on Amazon for only \$32 - it got great reviews and one of them said it works great with Backtrack 5 - it arrives in a couple of days so I'm really looking forward to reaching out to more networks in my apartment complex... see who's got the best (and least used) network to pull from...
... and while I'm at it... i find that it's BS that my successive posts are only being counted as ONE post... especially being they are relative and (hopefully) helpful. Can a moderator give me a little extra credit here?

nemonarendra - October 17, 2011, 11:56 pm

please bro pm me the dictionary file link

bvj94 - October 18, 2011, 7:42 am

nice work.. this is very usefull :)

ih5416 - October 18, 2011, 11:21 pm

Thanks! I'm pretty new to this but this tutorial was really helpful and informative.

BI4ckh4t - October 20, 2011, 4:09 pm

Does this only work for linux? If so what are good alternatives for windows?

usman2k_us - October 20, 2011, 10:51 pm

i have installed backtrack 64 bit but the setup is not working

Salox - October 22, 2011, 4:34 am

Vey nice post! Is it possible to get the link for the word list?

Cowhead2000 - October 23, 2011, 2:57 am

very nice tutorial, its the best out here :D

Papopirata - October 23, 2011, 10:48 pm

please I need the dictionaries

thanks in advance

Han. - October 25, 2011, 7:35 am

The tutorial helped out a lot man thanks :D

Capps - October 25, 2011, 7:01 pm

Wow magnus, why did you get banned? I was the one that upgraded you, and your repfucked? Explain?

BI4ckh4t - October 30, 2011, 7:42 am

What's the difference between the 32 and 64bit version. I have a 64bit PC.

Matatan - October 30, 2011, 2:23 pm

Fffuu!!!!I hope to steal the pass to the neighbor who has screwed me several times

Razer Ramon - October 31, 2011, 3:32 pm

All works well cracked a few WEP's a lil easier than the WPA, also once you get the hang of the program backtracker has an auto feature to make it that much more simple for you. Great post/tutorial.

coolguy742 - October 31, 2011, 3:52 pm

This is extremely useful, I've had BT5 for a while I've just never figured out the features lol

kinoman5 - November 1, 2011, 9:38 pm

Can someone please link a good wordlist?? For WPA

chegevara - November 3, 2011, 2:54 am

thanks very much bro so this very helpfull tutorial... i was hack all wlan in my town xD xD (Tbilisi).
work 100%..

MirrorDude - November 3, 2011, 9:20 pm

i used this tut to hack my neighbors network...glad to see its a sticky!!!

y Magnus banned?

anwarhashmi564 - November 4, 2011, 2:08 am

can u tell me compatible adapter for packet injection available in india..with cheap price..

A++++ - November 4, 2011, 1:59 pm

Great tutorial about wirelesses. Thanks for sharing!

FZ4NZ - November 4, 2011, 9:39 pm

Nice tutorial, maybe one of these days I'll make a tutorial on how to crack clientless wep and wep-psk (not open auth)

XD or better yet, attacking a client instead of the router, comes in handy

Krox - November 5, 2011, 4:06 pm

very nice tutorial! :) thank you ! :)

Onodera Kosaki - November 5, 2011, 4:28 pm

Hello, very nice guide you have here. :) It's my first post here on hackforum.

I got 2 questions.

1. Can you PM Me the link please?

2. Are there only english words in the dictionary, or are there other languages like norwegian in it?

-Oaheie

Demon_Jester - November 5, 2011, 11:18 pm

I would love to use BT5 in few months (once I get familiar with kubuntu and be more familiar with python) but I feel like its cheap to use a program for hacking. Then again IDK, Is BT5 frowned upon from the higher up, more experienced hackers?

Genius™ - November 6, 2011, 1:49 am

I wish i could give you 100+ reps , but your a/c is closed ,, you helped me lot man , Great Tut !!

anongroup - November 6, 2011, 6:04 am

when i click on ok after i click on diskimage and set everything up an error comes up saying 'you must create a disk image file to load' so what am i supposed to click on, what disk image?

Proximity16 - November 6, 2011, 2:23 pm

yo this is awesome please pm me the file or email it to me at chollet.dominick@yahoo.com and does it have to be an exact word in the dictionary or does mix words and letters?

Dread Pirate Roberts - November 6, 2011, 3:38 pm

Nice guide, very informative. Will definitely bookmark and come back later.

pyromonkee - November 6, 2011, 8:38 pm

thanks for the info :D looks legit :P

EXPENDABLE! - November 7, 2011, 6:39 am

I very much appreciate how well you did on this tutorial. This is exactly what I have been looking for!

JustJohn - November 7, 2011, 3:17 pm

This was a pain in the balls to figure out how to set it up with vmware. But I do have it working. Your accounts closed so I guess you can't be reached for that dictionary file : /

SIM-1029192 - November 7, 2011, 11:42 pm

This is amazing and thank you :) but the main problem that i am having right now is getting that dictionary file because the internet connection is very slow here in my place. Lets hope for the best :) Thank you :)

fodasse - November 9, 2011, 3:28 pm

MY REALTEK SEEEMS TO DOESNT WORK; OOO SHIT! I USE RTL8191SE

Ohh, the tut is very good, 5 stars explanation

Synster - November 9, 2011, 3:47 pm

good layout. more tutorials should be written like this

Infinity. - November 10, 2011, 1:01 am

This is awesome mate..luckily my isp provides me wifi connections wanna try for him..:)

hasib360 - November 10, 2011, 9:31 am

Thanks for the TUT.Going to try this.Regards.

p.jignesh23 - November 10, 2011, 9:52 am

how can we do this in windows 7??
can u plz help us.. :(

Cloud102 - November 11, 2011, 12:08 am

Props for the great and easy to follow TUT. MUCH appreciated. I can't PM you though. If possible please PM with the Word List. :D

tikinisky - November 12, 2011, 3:36 pm

Thanks for the TUT! looks amazing and organized. thanks again mate! [:

always2u - November 13, 2011, 1:04 pm

good tut bro... 100% complete... great work... thanks for the tutorial :D

willezzz - November 15, 2011, 9:16 am

Really easy to understand. Good tutorial :D

Adderall XR - November 15, 2011, 1:29 pm

Thanks so much for the guide and the time you took writing it! cheers :]

?AY?ØY - November 16, 2011, 6:33 am

Thanks man easy explained!

Like it!

TheNeutron - November 17, 2011, 4:37 am

Wow! awesome. Just bought a Router and was looking for something like this. Thanks for this.

Reflexo - November 18, 2011, 4:29 pm

Awesome guide, thank you so much for sharing it.

yacked2 - November 19, 2011, 7:12 am

Please send me your wordlist, thanks

PeskyPete - November 24, 2011, 10:00 am

Hey when I scan for networks it never seems to stop it just keeps scanning and scanning...

I tried just leavinh it, writing down the details and doing the rest of the guide but it doesn't seem to work.

Is there a way to manually stop the scan?

1mmaculate - November 25, 2011, 7:01 am

Pesky, just press CTRL+C?

Thanks for the great guide, none of the others I found from google worked completely. One question though, if anyone still even watches this thread, how long is the actual cracking supposed to take? I'm testing this on my own wifi, and the password is like 20 characters of letters and numbers. I scanned for about 7 hours yesterday but it was still failing to get the password..."Failed. Next try with 820000 IVs."

What am I doing wrong? Does it just take a long time because of how big my password is?

zeus88 - November 25, 2011, 7:37 am

After a long search finally the right found and also understood thank you. It could me one please PM. due to the word list send thank you

para02 - November 26, 2011, 11:35 am

Hi, can someone help me with a link to a dictionary please?

kisskiss - November 28, 2011, 10:48 am

hi thanks for this tuto

i ve a problem airmon-ng do not displays my interface

how can i resolve this?

nb: i ve Intel Wifi Link 5100 AGN

please Help me

Appliance Warehouse - November 29, 2011, 9:28 pm

Is there a place where I can see if I have a compatable wireless card?

I don't want to go through the trouble if I don't have a good card?

:T

Benny3101 - November 30, 2011, 3:07 am

Thanks ... it's a great and easy understandable tutorial

Can anybody send me the wordlist or the link to it please!?

iqbalsmart - December 1, 2011, 8:53 am

Could you please PM me that wordlist you talked about? 1.9 gb seems massive

george_torn - December 2, 2011, 3:49 pm

well done mate.. !!

This was very helpful !

chacha13 - December 3, 2011, 7:22 am

This tutorial is Awesome.

Thank you Magnus

muhammadnauman67 - December 5, 2011, 12:43 am

really very very comprehensive this tutorial is.. so great dude :-)
will you pls send me the link of that dictionary file?? wordlist
muhammadnauman67@yahoo.com

acidburn123 - December 5, 2011, 2:31 am

hello mate.. i need the world list or the dictionary file can u send it to me.

iliasdahacker - December 5, 2011, 7:44 am

it seems pro man good job man keep it up <3
it seems pro man good job man keep it up <3

Liamwitdre - December 6, 2011, 4:48 am

Sorry i'm a noob to all this and was wondering what is the point in making a bootable usb for this?
Personally im looking to hack WPA whether or not that has any significance?

Mustachio - December 11, 2011, 10:40 am

(Dec 6, 2011 05:48 AM)Liamwitdre Wrote: [\[CITE\]](#) Sorry i'm a noob to all this and was wondering what is the point in making a bootable usb for this? Personally im looking to hack WPA whether or not that has any significance?

Liam the purpose of making a bootable usb is so that it can be more portable and more convenient. This will allow you to be able go to any computer you want and boot up BackTrack5 as long as the USB ports haven't been disabled.

I hope this answered your question.

Apenknul - December 12, 2011, 10:04 am

Great tutorial, I'm trying it right now. Well explained and nice screenshots. Thanks a bunch

Nokeer - December 14, 2011, 4:03 am

Could you please PM me that wordlist you talked about? as I'm new here I couldn't PM you.

respect

warisbad - December 14, 2011, 8:30 am

solid info on here,a great tutorial 2 thumbs up

iridehonda - December 16, 2011, 2:37 pm

Very nice guide. Thanks for sharing.

faree_2029 - December 17, 2011, 4:59 am

I installed backtrack 5RI on my usb. when i boot with the USB , everything works fine but i can't open new terminal. There is no menu bar and there are no windows either. Its just one black screen like DOS. How can i open a new terminal.

NSPlayer - December 17, 2011, 5:49 am

Would someone be so kind as to PM me the wordlist if they have it? this would really help me out tonnes with those pesky WPA-PSK connections.

Cheers.

Also, a very thorough, well thought out and well laid out guide. I have bookmarked this and will pass on the information to others.

D3m3r - December 18, 2011, 1:25 am

Great tutorial. Easy on the eyes, and full of easy to understand info.

A++++ - December 18, 2011, 3:15 am

Thanks for sharing, but I have a problem: it captures data and does not ask the "Use this packet?" thing. And how can I save the captured data? It's not totally clean for me.

sayoNara10 - December 18, 2011, 4:26 am

Can I install backtrack5 in my external hard drive?

BaMBuS - December 18, 2011, 6:17 am

One of the best tutorials i've ever seen! Awesome!

wordalive - December 21, 2011, 12:02 am

Awesome Tut's :D great job man :P you are amazing

EpsilonBeta21 - December 21, 2011, 7:01 pm

Thanks. I'm am going to try this tomorrow

OpticVox - December 23, 2011, 11:41 am

how do i know if the wireless card is compatible before i buy it? other than that i love this guide!! it needs to be more detailed on what to do and what to get!!! only in the beginning tho!

DillchipHacker - December 24, 2011, 9:46 am

Looks nice. I will try this soon. mohahahahahahaha!

greenmandin - December 25, 2011, 12:19 pm

When I try to type commands into the terminal, I'm told they are invalid. It's driving me mad, can somebody tell me what on earth I'm doing wrong?

John2k15 - December 26, 2011, 10:51 am

i am gonna start this now and edit this when i do it with my results (if it works)

i have found a few grammar and typing errors regarding, but im sure others would of posted them ^

HeyGuise - December 26, 2011, 10:00 pm

Is BackTrack itself a viable OS for things other than aircrack/aerodump?

grapeFRUIT - December 27, 2011, 3:28 am

Yeah it is, HeyGuise. It's a Linux-based 'OS', let's call it that.

Advanced - December 27, 2011, 7:45 pm

I have a intel pro wireless 3945abg adapter, and it can't inject packets. How can I make it inject packets?

Danial1369 - December 28, 2011, 1:25 pm

if you can hack wpa without dic then you are pro.

Advanced - December 28, 2011, 2:55 pm

It says FAILED, next try within 5000 IVs after I try to crack it..

Zain - December 28, 2011, 6:45 pm

Is it possible to have an app on a mobile device that would allow you to crack a WEP code? Given the password must be pretty basic, it would be extremely useful to people who are often on the go, such as myself. My iPod Touch is probably too weak for the job but has anyone heard of an app on Cydia that could accomplish this task?

Advanced - December 28, 2011, 7:05 pm

There is, but its only brute forcing. Considering that a mobile's device does not exceed 1GHZ, it would take days to crack a SIMPLE WEP key.

piffkush - December 28, 2011, 10:12 pm

why do we need to PM the OP about the word list?

Whats the big deal about posting words? Its not like these words are copy written...

I see the OP account says closed, can someone kindly direct me where to get this word list?

I am very mad, I pay \$650 a month for a tiny room, and the savage landland changed the password on me because she says I was downloading music and she got a letter from the ISP or something, and I was NOT downloading music.

Im tethered on my android leeching off an obscure wifi signal that is free, but for some reason only my phone can pick it up

panfilo - December 29, 2011, 1:32 pm

Just helped some bitches hack their neighbors wi-fi :P Thanks (:

Flipster - December 31, 2011, 4:18 pm

I clicked okay and i needed to select a disc image to load... Help!?

joshernater9 - January 1, 2012, 1:45 pm

Hey, I have a Centrino advanced-n 6200 wireless card, And when I do the airmon-ng start wlan0 command, it says the normal info, but when it says the interfaces and all that, it doesnt show any, and it doesnt say that its entered monitor mode..It also doesnt show anything when i put airmon-ng, it just says the Interfaces, Drivers, Etc. But no cards under the sections. It does work when i do ifconfig though..Any help?

JarkTheShark17 - January 2, 2012, 8:23 am

Very good tutorial, thanks bro. It helped a lot.

zorro007 - January 3, 2012, 1:40 pm

Just send me wpa password list . it would b pleasure to have :)

torn - January 5, 2012, 9:03 pm

ould i please have the wpa password list mate thanks alot

themido - January 6, 2012, 5:30 pm

Absolute great tutorial. I was amazed by the good structure and layout.
Even for me as a n00b it was easy to understand!

lp640 - January 6, 2012, 6:18 pm

Just a suggestion: a WPS cracking tutorial could be made and added, as a follow-up after the WPA/WPA2 section in this thread.

Hoiboi - January 8, 2012, 1:50 pm

My computer wont bootup backtrack. need help please

dr.hadrn - January 8, 2012, 1:50 pm

amazing thread ,very simplified ,than you very much ,ive been waiting for such tutorial for awhile .

FabioTMW - January 8, 2012, 5:28 pm

Great tutorial, will try it as soon as i can.

jollyrogers - January 9, 2012, 8:16 am

can i have copy of dictionary list please

temoc - January 10, 2012, 7:14 pm

Yay it worked! thanks a lot and great tut. Nice pics.

RadioactiveRetard - January 13, 2012, 3:23 pm

HELP! when i write airmon-ng this is all i get
Interface Chipset Driver

and it doesnt say what i have

S U I C I D E - January 15, 2012, 5:41 pm

Hello Neighbors connection lolz thanks for the tut man works like a charm :D

Hacker_vb - January 15, 2012, 7:49 pm

Its Really good.. But is it work on window 7 ?....

piffkush - January 18, 2012, 3:10 pm

with the dictionary files, can you place all the text files in one folder and then when needed to crack a handshake just put the directory of the folder or does it have to be one text file at a time?

SoftwareeModding - January 18, 2012, 6:57 pm

will this work the wireless card i already have built into my laptop?

gdor80 - January 21, 2012, 5:55 am

Nice guide! I'll try it if I will ever actually install any kind of linux on my PC...

barto90 - January 21, 2012, 7:15 am

Hi

After I got the handshake, I get the following error message, when I use the aireplay command:

```
Sending Authentication Request
Authentication successful
Sending Association Request
Association successful
Denied (Code 1) is WPA in use?
```

I have followed the tutorial, so why is it saying that?

I've read that it's because I can't use fake authentication, but I don't think I have used that.

leswatts - January 22, 2012, 7:52 am

Fantastic work very comprehensive cheers

AXXO™ - January 23, 2012, 12:32 am

fucking awesome i loved it.best tuts so far!

dansklancapu - January 23, 2012, 7:22 am

Keep the nice work on,

Congrats.

nickmilan - January 23, 2012, 11:57 am

hi i would like to have the WPA wordlist..please PM me.i have already hacked some networks with WEP key and i look forward to hacking some WPA.thanks in advance

malabar123 - January 24, 2012, 5:18 am

Hello i am trying to crack my own wifi that is WPA2.

my result after using command "aireplay-ng -1 0 -a (bsid) mon0"

08:13:09 Sending Authentication Request (Open System) [ACK]

08:13:09 Authentication successful

08:13:09 Sending Association Request [ACK]

08:13:09 Denied (code 1), is WPA in use ?

So I assumes that my card is not supported. am i right?

Also tell me some card models from Lightwave and Alpha Branding that could support this. and one more this plz pm me the wordlists.

Zikk - January 24, 2012, 7:28 am

thanks a lot ! Awesome tutorial bro !

thealgorithm - January 25, 2012, 4:29 am

I don't have the option to write commands after I type airodump-ng mon0

sffe - January 25, 2012, 5:36 am

very good tutorial m8 thnx for posting!!

thealgorithm - January 25, 2012, 1:30 pm

great tutorials, but im having trouble getting a handshake

Edgar090 - January 25, 2012, 8:34 pm

dam do you need linux for this wifi hack? i really wanted to do the wifi hack

barto90 - January 26, 2012, 6:13 am

(Jan 24, 2012 06:18 AM)malabar123 Wrote: [\[CITE\]](#) Hello i am trying to crack my own wifi that is WPA2.

my result after using command "aireplay-ng -1 0 -a (bsid) mon0"

08:13:09 Sending Authentication Request (Open System) [ACK]

08:13:09 Authentication successful

08:13:09 Sending Association Request [ACK]
08:13:09 Denied (code 1), is WPA in use ?

So I assumes that my card is not supported. am i right?

Also tell me some card models from Lightwave and Alpha Branding that could support this. and one more this plz pm me the wordlists.

I get the same error message as you, but I have bought the Alfa AWUS036H card which i was told should work.

Does anyone know how to solve this problem?

iRawrZero - January 26, 2012, 6:23 am

wifi, hi-five, hackig, smacking, rambling, spam :/

tigerz09 - January 28, 2012, 6:08 am

Hey, may someone please pm me the Wordlist, I really need it please.

-I will not have internet for 7 Days(From 31/1/12 midnight till 7/2/12) because of Virgin Media are closing down due to upgrade their Internet Connection. And I have switch to sky but as you they take ages to do it ?.

I'll really appreciate it if someone gives me a worldlist I'll give +rep ?.
Thanks in Advance! ?

~Tiger~

nos_ - January 28, 2012, 9:15 pm

Extremely helpful; thank you very much!

paddy-p - January 29, 2012, 12:48 am

awsome but couldn't they backtrack me ?

tigerz09 - January 29, 2012, 3:25 am

i find problem with showing the place of the wordlist in Terminal

any advice pls?

~Tiger~

reggae fever - January 29, 2012, 9:26 pm

super nice and easy to understand thank.

oprez - January 30, 2012, 2:15 am

very very nic tut; thank you very much!

FuhrerWulf - January 30, 2012, 7:47 am

Very nice tutorial you made man. Going to try and see if my shit is compatible for doing this. Nice job! ?

Vircolac - January 30, 2012, 7:55 pm

MAY i have the wordlist used please :D IT WOULD REALLY HELP ALOT :D THANKS IN ADVANCE

bolthacker - January 30, 2012, 11:25 pm

Nice TUT

thanks for sharing :)

--bolty--

Senor_Reed - January 31, 2012, 1:47 pm

Great tutorial! I'm going to try this out for myself

ISO - January 31, 2012, 1:50 pm

Very nice guide !

Sad to see the OP is gone.

seadfinder - February 1, 2012, 8:46 am

cool het werkt dank je heb alles gedownload en nu zit ik via draad loos

ramtastic05 - February 1, 2012, 11:32 am

Great tutorial, very nice. I thought it was a much harder process, but I guess not.

Can I please get the word list or the link to it?

Thanks if advance.

chethuspeu - February 2, 2012, 1:19 am

Great Tutorial! Very easy to understand! Good job! :)

nour123 - February 2, 2012, 10:16 am

hi,i have a very big problem.when getting packets in order to crack WEP password,it reaches about 400,000 Data and then stops and says not enough disk space available.why does that happen??i tried it on my 4gb USB and on my c: hard drive using UNetBootin but still does the same.plz help

johnkaslik - February 5, 2012, 2:02 am

Hi

I read your tutorial on WEP and WPA hacking

It is a good easy comprehensive explanation Congrats

My question is that I find WEP relatively easy but struggle with wpa mainly because my dictionary file is not good. You mention you have a comprehensive 1.9 Gb one Could you guide me in the direction to download same

Thanks for your help

John

Swuzne - February 5, 2012, 5:13 am

Awesome guide.. helped alot thanks man

M4dMax - February 5, 2012, 9:24 am

so nice ! thanks for this topic ! i try it now

klauskitkonorit - February 6, 2012, 9:54 am

Guys, what could be the problem if I can see WEP networks when I'm in Windows mode scanning for wifi networks but when I go through backtrack the WEP networks are not shown. I have to mention also that in windows mode the signal of them is only fair. But WPA networks with fair signal appears on my backtrack straight away. Thanks for help

mr. smith - February 6, 2012, 12:54 pm

awesome guide man!!!

thnx a lot!!! :)

Dik_In_D_Ai - February 6, 2012, 8:15 pm

Nice Tut really like it thanks so much

Dik_In_D_Ai

nour123 - February 11, 2012, 6:17 pm

thankss so much for the tutorial :)

snider.wes - February 12, 2012, 10:55 am

Very nice guide, RIP OP.

Spoiler ([Click to View](#))msg35char

boobi3 - February 12, 2012, 2:42 pm

could someone fwd me the worldlist. Thank you.

asdfghjkl - February 12, 2012, 4:18 pm

AMAZING TUT MAN!!! Walked me through each step perfectly!!

gruffy - February 13, 2012, 6:45 pm

you're the freaking best man. i am definitely using this to get some free wifi

Oynatan - February 14, 2012, 1:59 am

it's a really good tutorial:) thanks man

mausie94 - February 14, 2012, 2:27 am

thanks a lot this was really help full

jayfiraweaver - February 15, 2012, 3:05 pm

wow this tutorial is amazing i love it ty for all the info u have posted :D

gmine44 - February 15, 2012, 4:47 pm

i have been hacking wep for 2 years, but here in UK, the wep are getting fewer and fewer...i'm wondering if any of you have the dictionary for sky passwords ...or for bt ,talktalk..as all come with standard generated passwords...(sky with 8 letter AKSJHJDH) and the other have number....but the sky are always capital letters...

jdub666 - February 15, 2012, 8:01 pm

very good tut. nice job keep it up!

?Eatos - February 16, 2012, 1:10 am

Does it mean that this doesn't work on my computer if it shows no interfaces?

rikagorii - February 16, 2012, 5:26 am

Friend,

where can i download backtrack5 .

Thanks in advance

Prologue - February 16, 2012, 10:29 pm

what if i have a built in wifi adapter,may i still be able to do this correct and if not,is there another way to do so?

Please help

rikagorii - February 17, 2012, 8:53 am

Thanks Buddy..Awesome tutorial. layouts & pictures are clear and instructions fantastic.

Thanks Again :)

Aweson - February 19, 2012, 12:44 am

i tried BT4 and it worked me for WEP ..

but sometimes it get stuck on Channel difference.. is That one same in BT5 or fixed..

could any one PM me wordlist link..

Pisnge1120 - February 19, 2012, 8:44 pm

can i use backtrack 5 R1? plsss reply

Archansor - February 20, 2012, 10:36 am

amazing how so much time and effort went into this thread, and the account is now closed =(

alicjk - February 20, 2012, 3:07 pm

Great Tutorial..very clear and easy to understand ...thanks mate

Cr.s - February 20, 2012, 11:18 pm

thANK You for this step by step guide there shouldn't be any more post about I need help... smh

sidestrafe - February 21, 2012, 10:10 am

well thank you for the clarity of the tutorial. definitely better to just read this rather than buy a book on how lawlercoaster. you saved the rest of us lots of teh cashmoneyz

darksrc - February 21, 2012, 8:34 pm

Awesome, detailed tutorial. Thanks op, even though you can't read this

~Ultim8um ?

Capps - February 21, 2012, 9:57 pm

(Feb 20, 2012 11:36 AM)Archansor Wrote: [CITE](#) amazing how so much time and effort went into this thread, and the account is now closed =(

Funny thing is, I upgraded him to ub3r before he was repfucked+banned/closed.
He lied, the whole time, 3 days, he lied.
Thats why I will not upgrade anyone else on hf.

hmmmpf - February 23, 2012, 5:07 am

can you send me the WPA word list from 1.9 gb ? tnx!

hack_knightzz - February 23, 2012, 10:46 am

hello great tutorial but can you give me the download link of that word list please

sml555 - February 24, 2012, 7:27 am

this is really good
i read the book
hacking for dummies and this is better :)
this is really good
i read the book
hacking for dummies and this is better :)

Bago47 - February 25, 2012, 9:27 am

What to do now: I downloaded that .iso file with backtrack 5 and burnt it to a DVD, but when I put DVD back in comp it doesn't work? I don't even know how to open that backtrack 5 program. Pls help

deebee1 - February 27, 2012, 2:34 am

how do i get it to be bootable on usb. iv read the tut but just cant seem to get my head round it....

Critical_Hax - February 27, 2012, 4:04 am

on the first step when I need to type in: airmon-ng it doesn't even shows me my driver-chipset-interface it's blank under it
WPA WORD LIST http://#.se/torrent/5977355/WPA_word_list

deebee1 - February 27, 2012, 4:24 am

can someone pm me a wordlist please.

thank you
once i send packets to get the data above 20000 what do i do, the packets are being sent but i am not sure what file it is saved as?
please help

Coecane - February 28, 2012, 8:01 pm

when i type airmong -ng i dont get anything under it.. but i have a wifi card... why is that? please PM me

Predator_Crack - February 29, 2012, 5:00 am

(Feb 28, 2012 09:01 PM)Coecane Wrote: [\[CITE\]](#) when i type airmong -ng i dont get anything under it.. but i have a wifi card... why is that? please PM me

Do you refer to backtrack or any other linux disto that you are trying to use with? If yes please mention the version of that. (5 r1 for example)

What is your wireless lan adapter ? (model)

L33tPerson11 - February 29, 2012, 10:28 am

Awesome work. thanks for all the information.

yehia1919 - March 1, 2012, 12:12 pm

Really excellent tutorial you have there mate.

opejporjdweqpkq3je - March 1, 2012, 12:46 pm

I use a virtual machine for run backtrack in windows but , aircrack don't function...

sorry for my bad english

Predator_Crack - March 2, 2012, 5:23 am

(Mar 1, 2012 01:46 PM)opejporjdweqpkq3je Wrote: [\[CITE\]](#) I use a virtual machine for run backtrack in windows but , aircrack don't function...

sorry for my bad english

Do the rest tools work for you ? I refer for example to airodump-ng and anything else and of course for the actual functionality of your current wireless lan card.

Han. - March 3, 2012, 1:55 pm

Very nice tutorial man, this may come in useful if my neighbours start getting annoying ?

hotmagnet - March 6, 2012, 8:25 am

red ur tutorial today, yeah i know kinda late but i just couldn't stop myself from appreciating ur work, awesome tut. beautiful layout, easy expalnation via pictures, well it was a complete mind-blowing job, HATS OFF ..

:-) also i was wondering if i could get that file, plz... thanks

aframestor - March 7, 2012, 1:22 am

what if you have the password and you are connected, but the person on the other end blocked you out. Is there a way to connect then?

afiq10 - March 7, 2012, 6:23 am

Nice Information Ya Sharing... Thanks .. Now I Can Slow Down My Neighbour's Internet :P.. lol

deviantthread - March 7, 2012, 2:48 pm

Hey can anybody send me the wordlist torrent link? I don't have the 10 posts to PM anyone yet.

thanks much

Flepz - March 9, 2012, 8:01 am

Awesome post.thanks for all the information. It's very easy to understand.

caca22 - March 10, 2012, 10:44 am

What can I do if my card isn't supported?

hotmagnet - March 10, 2012, 11:00 am

in that case bro u got to buy a new one simple..

IAmAustralian - March 13, 2012, 6:24 pm

Nice work bro. Keep up the good work. Great Tut. :)

xXCobraReaperXx - March 18, 2012, 1:20 pm

Awesome. Good and clear for dummies like me.

De1337ath - March 20, 2012, 10:08 pm

Im a bit sketchy on the fact that he has a closed account and -9 rep...
Mhmm , not sure... should i download that backtrack 5?

zvezdakiki - March 21, 2012, 9:09 am

bratle dava nqkakva greshka na men nese polu4ava :((

Ronnie Coleman - March 24, 2012, 9:36 am

Great Tutorial. I'd like to have the dictionary file via PM. Thanks!

xFinally - March 24, 2012, 2:27 pm

hey :) ima noob here and i have 1 question.. but 1st:

AWESOME TUTORIAL dude :) helped me very much...

now: id did everything like u did at the end.. when i write "aircrack-ng ..." and it tries to crack the code, it says that it failed... but ih had more than 200.000 data..

why? :(thanks for help

?Ñâzg?l - March 25, 2012, 3:49 pm

(Mar 20, 2012 10:08 PM)De1337ath Wrote: [\[CITE\]](#) Im a bit sketchy on the fact that he has a closed account and -9 rep...

Mhmm , not sure... should i download that backtrack 5?

HAHAHAHA

Its Safe Because you are downloading it from The official Site.

I Dont know how he got that Reputation Before it was positive.

iZerovirus - March 25, 2012, 7:58 pm

Thank you for the tutorial, ive found myself using tutorials, as more of an open-book test, this actually gives me the knowledge i want to understand... the definition of the commands, id also like a pm to that torrent link, im gonna go searching for it now. And to the directory its concerning, does it change ever depending on the hardware/software?

zaven - March 26, 2012, 1:47 am

Great Tutorial, easy to follow. Thanks for this

10er512 - March 27, 2012, 2:15 am

once inside,how do you access the files of other users connected to the network?

xxchisxx - March 28, 2012, 12:02 pm

This is very well done, thank you very much for the tut!

Zihv - April 1, 2012, 7:25 pm

I would say thank you, but his account was closed. What a shame...

Objection - April 2, 2012, 3:41 pm

Does anyone know where to get the stuff needed

Backtrack 5 - I would suggest GNOME, 32Bit, ISO & Direct

Compatible Wireless Card

WPA Word List - Search via torrents to find one

Jooping - April 2, 2012, 5:51 pm

good contribution, no one to thank.

razen7 - April 3, 2012, 3:33 am

UNetbootin is not compatable with 64bit win 7...i m using...can u suggest me something please

Hm.. - April 4, 2012, 12:25 am

Great tutorial, thank you, uh? "closed". Layout was quite excellent I must say.

rocky45 - April 4, 2012, 10:32 am

Hi.My card doesn't support packet injections. Is there any other method to hack WEP/WPA/WP2 AP's?

hackerman235 - April 4, 2012, 1:15 pm

i just downloaded it from here <http://www.backtrack-linux.org/downloads/>

SP!D3R - April 4, 2012, 6:59 pm

Thanks Really Useful :) downloaded backtrack 5 R2 and gona try it
SPIDER

alex1993 - April 7, 2012, 4:58 pm

Awesome work-- thanks for all the information. It's very easy to understand.

gigearo - April 7, 2012, 11:06 pm

I am trying wep encryption and when i am on the part where i need type airodump-ng mon0 it just keeps searching and refreshing. it have searched now like 8 hours and still not stopped. There is like 10 wlans nearby me.

king9901 - April 9, 2012, 2:09 am

cool back track.. but im not good with back track
can you make one but in windows os?

JOW - April 9, 2012, 10:30 am

Good tutorial I will try this later on this week I'll post some feedback :D

Pygowsky - April 9, 2012, 9:03 pm

I would definitely like to try the WPA/WPA2 but does anyone have a copy of the 13 GB file to use since the OP isn't around anymore?

HarmfulMushroom - April 13, 2012, 1:11 pm

Very helpful, used this tutorial to get into my neighbors internet. Thanks!

GrantIsHot - April 13, 2012, 4:02 pm

(Apr 7, 2012 11:06 PM)gigearo Wrote: [\[CITE\]](#) I am trying wep encryption and when i am on the part where i need type airodump-ng mon0 it just keeps searching and refreshing. it have searched now like 8 hours and still not stopped. There is like 10 wlans nearby me.

They're probably all WPA or WPA2 then.

LJayden - April 14, 2012, 10:30 am

Awzome work Dude! Realy good guide!

gommee - April 16, 2012, 10:13 pm

(Apr 9, 2012 09:03 PM)Pygowsky Wrote: [\[CITE\]](#) I would definitely like to try the WPA/WPA2 but does anyone have a copy of the 13 GB file to use since the OP isn't around anymore?

I too would be interested in acquiring the 13 GB Word file. Please PM me.

Thank you

Gommee

jdsilly - April 18, 2012, 5:37 pm

is there any way of infiltrating systems with just the hands and a computer

ALF1930 - April 19, 2012, 3:18 am

He uses the wrong command in wpa2 cracking. aireplay-ng -1 0 -a (bssid) mon0 is the command to fake auth and connect to the acces point. In the screenshot is the correct command. Aireplay-ng 0 5 -a (bssid) -h (fake mac) interface. This is the command to kick another user of the network. Time to edit the thread PPL!

Tony_dude - April 20, 2012, 6:45 am

thanx so much works :D ty :D:D:D:D:D

NewbieBOT - April 21, 2012, 11:38 am

USEFULL! Thank you very much I will do my way and start hack some networks thank you again!

Se7ensins1234 - April 22, 2012, 1:55 pm

Great tutorial. Easy on the eyes, and full of easy to understand info.

goldman - April 24, 2012, 12:03 pm

Thanks Magnus ,

Great tutorial ;)

ophelielareine - April 24, 2012, 1:36 pm

Thanks you for this tutorial. Good job :D

whitepanda - April 25, 2012, 4:08 am

amazing tutorial :P

very easy to understand

CodeLoad - April 25, 2012, 1:43 pm

Can backtrack hack school networks?

world limit:..

.X0911. - April 25, 2012, 3:58 pm

Everything works perfectly.

I seem to have only 1 problem:

Sometimes, while it's capturing IVs, it stops. Continues capturing packets & such but stops capturing IVs.

What can I do to it up again? (Continue capturing IVs)

UnknownPerson2012 - April 26, 2012, 5:13 am

im stuck anyone help me plz in at the setting of the diskimage help me plz

Drugo - April 26, 2012, 5:39 am

Bellissima guida molto chiare e esplicita!

.X0911. - April 26, 2012, 3:35 pm

(Apr 26, 2012 05:13 AM)UnknownPerson2012 Wrote: [\[CITE\]](#) im stuck anyone help me plz in at the setting of the diskimage help me plz

You could always burn Backtrack to a DVD-R using just ImgBurn and the .iso & it works fine.

breadloavez - May 2, 2012, 1:02 am

this is sick! You did a good job presenting this, wanna try it :P

Laraangelg - May 2, 2012, 2:36 pm

Great tutorial!! Keep up the good work!! :)

Ramkiller1 - May 2, 2012, 7:08 pm

back track is the best, Really it is!

joey_777 - May 5, 2012, 1:00 am

great tutorial ? visit this for a 4 gb wordlist

http://#.org/torrent/5945498/WPA-PSK_WORDLIST_3_Final_%2813_GB%29.rar ?

Yousef04 - May 6, 2012, 10:57 pm

Where can i download the program pls ?

E_-mC cUb3D - May 10, 2012, 2:39 pm

Why was the OP's account closed? O.o

indigoxe - May 11, 2012, 2:12 pm

Thank you so much for this tut!!!! Great and super helpful! I messed around with 4 but never had a good tut as this, and better yet 5 haha. I was also wondering if you still have the link to the wordlist? If so, could you PM that to me? If not that's cool, still awesome.

Thanks again,
SysteEm

Crystal Clear - May 16, 2012, 6:56 am

Nice tutorial. A bit quirky in some places. An effective learning tool for beginners. Where's Magnus? Why banned? Thanks anyway.

sQQI - May 16, 2012, 12:17 pm

Having problem finding interface via terminal airmon-ng command.

I'm connected to internet, but after trying all guides I'm still unsucsessfull finding the ech0.

Using Backtracker 5 64BIT vmware version.

Wireless USB connection with a old Dlink DWA-142 software.

Wireshark can't find the ech0 either.

infamousdice - May 16, 2012, 7:48 pm

Awesome tutorial. I love the layout and clear pictures and instructions. Keep up the good work!

el_furiano34 - May 17, 2012, 5:20 am

thanks for all the information. It's very easy to understand.

darkknightofdevil - May 18, 2012, 1:42 am

tutorial very good but not much concept explaining....is this possible on windows too???

RandomHoax - May 18, 2012, 4:06 am

good tut dude i will see how it will help me

JudithMartin - May 18, 2012, 2:26 pm

I'm trying the WEP crack on my test system and everything look OK, correct BSSID and aireplay shows over 148,000 packets sent- but airodump doesn't show any increase in the data #... and it seems to show lost packets. The beacon # is going way up- but little movement on the data #.

update: Over 2 million packets sent, 2 hours and 27 minutes in- and I have 16,334 beacons / 85 data.

I have more data from the open AP down the street. (19,000 / 2300)

What am I doing wrong?

Intelligence - May 18, 2012, 3:44 pm

Thank you very much for the tutorial, it helped a lot.

Innenstadt - May 18, 2012, 4:27 pm

Thank your men very nice! u helped me :)

JudithMartin - May 18, 2012, 4:31 pm

Fantastic tutorial.

That being said- after wading through 600+ posts- I want to kick some of you mouthbreathers in the nuts.

I would humbly suggest that a mod clean up this thread and delete :

posts from idiots that ask if this works in Windows.

posts from neckbeards asking for a word list from someone with a closed account

posts from windowlickers that can't figure out where to find a freakin' wordlist torrent file

posts from morans that didn't read 3 lines of text and are asking how to see if their card is compatable.

Thank you for your attention to this matter.

Sundistasya - May 23, 2012, 1:33 am

after startx my screen becomes black and never shows desktop.
can anyone have faced same problem?

blackwidow - May 23, 2012, 8:01 am

nice tutorial i will got into it when i have the BT5 installed

retestreak - May 23, 2012, 9:16 am

(Jun 23, 2011 09:51 PM)PandaSec Wrote: [CITE](#) Code aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b (bssid) mon0

what type of attack is this called?

can anyone say stickie?

U should try the command : aireplay-ng --help

Zombiefreak83 - May 24, 2012, 2:13 am

Great help, now my roommate will never lock me out again :D

roflniggs - May 24, 2012, 3:58 am

how do you know which wifi card is comatible or not? is there a list?

A White Hat - May 24, 2012, 4:09 am

This tutorial is older than my grandmother and should be redid with today's method

The Butcher - May 25, 2012, 3:20 pm

Great thread, much thanks given.

~Butcher

120ck0 - May 25, 2012, 9:07 pm

I just posted this to change the number of replies ;D

LurkingGrue - May 29, 2012, 11:02 am

Nice tutorial, it works awesome on my desktop. The only problem occurs when I try and use this on my laptop. When I enter the command "airodump-ng mon0" I'm presented with "Interface mon0: ioctl(SIOCGIFINDEX) failed: No such device". When I enter "airodump-ng wlan", I'm prompted with "ioctl(SIOCSIFFLAGS) failed: Unknown error 132". Can anyone lend a hand?

P.S: For reference I'm using BT5R2, not sure if anyone else is using it here, as this tutorial is a bit dated.

0x45 - June 1, 2012, 9:23 pm

For those who couldnt get handshake(Well i couldnt)

I used

airplay-ng -0 5 -a (bssid) mon0

Xin R

jackmos - June 2, 2012, 10:36 am

Cn somebody tell me how can i locate my dictionary file that is on D:/ drive of my computer?

Autolite - June 3, 2012, 6:40 pm

Thanks for this. I'm going to try this out!

Yourgod912144 - June 4, 2012, 3:39 am

Wow very good and well explained thred!

hack-pour-hack - June 4, 2012, 11:42 pm

can i have the dictionary please?? ^^

cncc - June 8, 2012, 3:08 pm

is it easy and how long it takes to know the pass??

crashfire - June 9, 2012, 6:45 pm

Thanks for this guide, but a video will be nice :)

Dynasty@HF - June 10, 2012, 7:16 am

one of the best tuts on this site. everytime i read this it gives me more ideas.

Lil Gh0sT - June 13, 2012, 9:46 pm

nice post i say ? i used backtrack but now every one is using wapa2

hfiowhqioprh - June 14, 2012, 1:35 pm

dont make me eat a burrito on my white shirt

lilnigathatcould - June 15, 2012, 12:47 am

hey thanks for the info im about to go try it out

sayoNara10 - June 15, 2012, 7:01 am

can i have the dictionary please?? ^^

RoldaX - June 15, 2012, 7:50 am

Great tutorial. Easy on the eyes, and full of easy to understand info.

cokolol - June 15, 2012, 2:44 pm

Two hundred million dictionary words can be downloaded via [How to hack wifi](#)

347eat - June 16, 2012, 7:41 am

Will this work in wifi in the Philippines?

angelfiredustice - June 19, 2012, 10:15 am

wifi in the philippines is miserable.

Original poster has account closed??, yes it will work in the philippines.

SiPleX™ - June 22, 2012, 9:03 am

Would this still work is Backtrack was on a VM?

hariibo123 - June 22, 2012, 5:24 pm

nice tutorial ill be sure to try it out sometime

Prominent - June 23, 2012, 4:05 pm

Thats a great tutorial and explains a lot of the process. Sad to see the user banned.

bx bugs - June 24, 2012, 3:34 pm

I did everything right, & I get over 100k packets but when I go to crack the WEP, it won't crack it. It says "Failed. Try again with 5000 IV." What am I doing wrong? Do I need more packets?

Flaffy - June 28, 2012, 10:33 am

Please hack this IP, 68.146.18.12, ruin this guy's day. If you can hack his MC account his name is coolspenc, hack his computer too. Douches like him don't deserve to live. ?

Matrix Hacker 51 - June 28, 2012, 10:25 pm

thanks for the help ur help will be my tutor for the future

thanks..i...hope you will bring this type of help in the tomorrow days also.

new to this - June 29, 2012, 12:12 am

great job i will try this soon thanks alot

Pianist - June 30, 2012, 5:07 pm

Very helpful, thanks. Although it took me a while to figure out, it's very helpful

Aeronx - July 1, 2012, 4:20 pm

Thank you very much!

P.s. why was his account closed

ZeferiniX - July 1, 2012, 10:11 pm

I'll try this once I get BackTrack 5 >:D

abuzai - July 2, 2012, 11:52 am

Thank you very much thanks to this I was able to connect to my neighbor.

Actionplayer - July 5, 2012, 10:36 am

This is indeed very interesting!
very very interesting XD

DevilMacabre - July 9, 2012, 7:21 am

thank you for the tutorial.. it really helped a lot :D

chesis - July 9, 2012, 3:46 pm

HQ Tutorial !!

Thank you very much , work great

Iced. - July 10, 2012, 6:14 pm

nice format.. ill give it a try..vewfdwdaqw

sseksp - July 11, 2012, 6:53 am

Admirable invention heroe ts so smart of u 2 come up with such a marvelous output

SickeM - July 12, 2012, 2:20 am

This is a very HQ Thread. Nice & Clean, Thanks for the help!

LucidZephyr - July 12, 2012, 5:48 pm

Thank you so much! I could never get back track to work until now

abuzai28 - July 13, 2012, 8:01 am

nice tutorial i will got into it when i have the BT5 installed

SIM-99212 - July 13, 2012, 12:38 pm

I keep getting an error:

```
Code root@bt:~# airmon-ng start eth1
```

Found 3 processes that could cause trouble.

If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID Name

19576 wpa_suplicant

19582 dhclient
19600 dhclient
Process with PID 19576 (wpa_supplicant) is running on interface eth1
Process with PID 19600 (dhclient) is running on interface eth1

Interface Chipset Driver

eth1 Intel 2200BG/2915ABG ipw2200 - [phy0]mon0: ERROR while getting interface flags: No such device

(monitor mode enabled on mon0)

root@bt:~# airodump-ng mon0
Interface mon0:
ioctl(SIOCGIFINDEX) failed: No such device
when I run it on a Thinkpad T43 that has an Intel 2915 ABG wireless card.

Is there an way I can fix this?

MasterCoder - July 13, 2012, 9:12 pm
Anyone have that 1.9GB Dictionary file?

Mikeops - July 14, 2012, 5:56 pm
Great job!

Could you please send me the link to the 1.9 gb word list you discussed in the tutorial. If you found something better, please advise. Thank you in advance.

xanthar - July 15, 2012, 9:19 am
Hi super tutorial 10 out of 10.

Just a note.

For beginners, try Google wifite
Its a script for Backtrack it just automate The aircrack but its a Nice handy helper for quick access and cracking. Includes a 100.000 words wordlist (checked local neighbourhood, 2 went under The included wordlist LOL)

Xanthar

KHRYS TAL - July 15, 2012, 9:26 am
nice tutorial i will got into it when

MasterCoder - July 15, 2012, 7:00 pm
Can someone find a good place to find a dictionary file, or just a good dictionary file? Sort of like Magnus used, the 1.9Gb one? Thanks!

guillhouf - July 15, 2012, 10:59 pm
is it possible to get caught?? just saying im new to hack forums.

23732 - July 16, 2012, 5:08 am
(Jul 15, 2012 07:00 PM)MasterCoder Wrote: [\[CITE\]](#) Can someone find a good place to find a dictionary file, or just a good dictionary file? Sort of like Magnus used, the 1.9Gb one? Thanks!

Check out my signature, I have some ;-)

xiigruntiix - July 16, 2012, 2:43 pm

thanks nice tutorial by the way and it really helped me when i had some trouble doing and really easy to follow thanks

Objection - July 17, 2012, 12:35 pm

(Jul 16, 2012 05:08 AM)23732 Wrote: [\[CITE\]](#) Check out my signature, I have some ;-)
which ones are they? I am new to this :p

Damon Salvator - July 17, 2012, 1:19 pm

thanks for the share mate...it is really helpful...

demig0d - July 17, 2012, 7:05 pm

Thanks so much! awesome tut. I'll try it right away!

Oscar36 - July 19, 2012, 11:24 pm

Awesome work. I think it will be easy to do now. thanks!

23732 - July 21, 2012, 11:22 am

(Jul 17, 2012 12:35 PM)Objection Wrote: [\[CITE\]](#) which ones are they? I am new to this :p
All of them are wordlists, except the one named "27 rainbow tables" ;-)

Objection - July 21, 2012, 5:16 pm

(Jul 21, 2012 11:22 AM)23732 Wrote: [\[CITE\]](#) All of them are wordlists, except the one named "27 rainbow tables" ;-)
Thanks a lot man, which one would you recommend I use?

Devious Hacker - July 22, 2012, 1:35 am

This is some good meterial, I going to have fun reading it, since I just skimmed it.

23732 - July 22, 2012, 8:17 am

Take all of them ;-)

Spoiler ([Click to View](#))Stupid35characterlimitshit

DesuDesuDesuDesu - July 22, 2012, 1:54 pm

Thanks for the great tutorial, could you give me that dictionary file or not?

Thanks in advance. :D

Objection - July 22, 2012, 4:18 pm

(Jul 22, 2012 08:17 AM)23732 Wrote: [\[CITE\]](#) Take all of them ;-)

Spoiler ([Click to View](#))Stupid35characterlimitshit

alrighty then, and when I download backtrack5.1 it shows up as I have to copy it to a disk, is that normal?

Monchie - July 23, 2012, 12:19 pm

thanks for the tutorial, gonna try to hack my brother's hacked wi-fi

Zylihard - July 24, 2012, 7:11 pm

Thanks for the interesting tutorial Nice. :)

Strahotni - July 25, 2012, 9:50 pm

Hi guys...i tested this by my fried and it works.then i testet it at home and found key but it doesnt work.limited acces no network connection...any help??

boss211 - July 26, 2012, 1:35 am

Awesome Tutorial Buddy !!! Very Informative :) :) :)

Objection - July 26, 2012, 9:33 pm

For some reason I cant download the programs, anyone else having this problem?

NetFree - July 27, 2012, 8:33 am

Great tutorial. Easy on the eyes, and full of easy to understand info.

roux115551 - July 28, 2012, 5:06 am

Good idea, This is great + Nice writing titles :O

SuperDean - July 28, 2012, 3:41 pm

Awesome tutorial. I love the layout and clear pictures and instructions. Keep up the good work!

AnonymousG1 - July 29, 2012, 8:02 pm

Can you please pm the list :) ty

And great tutorial !!!!

xswitch - July 31, 2012, 4:20 am

Great Tutorial . The picture really helped aswell

Can you please PM the wordlist

rs329 - July 31, 2012, 4:38 am

great tutotirla,this picture helped me as well!

great tutotirla,this picture helped me as well!

KiPE - August 1, 2012, 10:37 pm

Very thanks

I love this "tutorial" ^^

xploiter1 - August 2, 2012, 9:17 am

this is a nice guide ... i have been looking for somthing related to backtrack

?Nano_Curie? - August 4, 2012, 11:07 am

I'm using backtrack 5 inside of a oracle box VM and

When i open the terminal and type airmon-ng it has

No interfaces chipsets or drivers , if there any way to

Fix this please? , thankyou for any responses.

rizan - August 5, 2012, 4:30 am

just wondering, do we need to create a bootable USB for Backtrack

Nonfatkibbles - August 6, 2012, 12:38 am

Worked perfectly! Easy to follow and well put together thanks man

DevilMacabre - August 6, 2012, 8:49 pm

Nice tutorial, I've been trying some other WEP cracking but sometimes it doesn't work. I don't know if they are blocking me or something. Could I get the wordlist for the WPA cracking? really appreciate it :D

kazkal - August 7, 2012, 3:51 pm

Really liked this TuT. 100% thumbs up!

xploiter1 - August 9, 2012, 4:22 am

seems to be a better tut. I have tried others but they didn't work .. account closed .. anyone with word list ?

chaosdarky - August 11, 2012, 9:31 pm

I found this word list site on the net but it's kinda big. It is a 39.1G Wordlist but compressed into 4.8G 7zip file. [Click Here](#)

The bigger the better :D

ateun - August 12, 2012, 7:44 pm

I read through the whole guide, but I am still not sure where that bootable usb drive comes into play here...someone explain please? Or pm, thanks.

after airodump-ng mon0, how do I keep typing? it just keeps going on and on forever

wonderbread24 - August 13, 2012, 10:08 pm

Unless you have Backtrack installed on your machine or you don't have another machine to install a dedicated Linux OS too, the bootable USB drive comes into play. You can install Backtrack to a USB drive and boot to that drive. Now you have Backtrack up and running on almost any computer that can boot from USB without losing the OS currently on that machine.

Press Ctrl + C to stop airodump

Elderum - August 15, 2012, 6:38 am

Can someone tell me if this guide is legit? Still stickied yet his acc is closed :\$

__init__ - August 16, 2012, 6:40 am

Awesome tutorial! Wonder why this guy got banned :/

23732 - August 17, 2012, 5:06 pm

On the WPA part, in order to deauthenticate a client, use -0 instead of -1.

IneedtoHACK - August 17, 2012, 8:20 pm

best tutorial I've seen for this so far good job and all this does work so anybody who doesn't think it's worth it just do it (nike symbol here)

element25 - August 18, 2012, 9:05 pm

Could I download UNetbootin and then mount it using DaemonTools, or would that not work?..

JpmD - August 18, 2012, 10:59 pm

I followed this tutorial to the dot. But my data collection for the WEP is way too slow. Only 2 data in 8 min. Can someone help me please. Wireless card is tl-wn821n

hackerdentist - August 19, 2012, 1:05 am

well can i use vmware workstation ?

dreamr4c3r - August 20, 2012, 11:16 am

This thread is the BEST thread I've found on this forum so far. :)

Thank you SO much, I literally memorized all the commands necessary...

With your help, I cracked my neighbor's stupid wifi "FBI SURVEILLANCE VAN #4" and changed it to "FBI FRAUD REPORTED" hahaha x'D

Well, thanks a load buddy, let me know if there's anything I can help you with!

Solo04 - August 20, 2012, 11:18 am

i never get hand-chake, i have tried litterly 100+ times,
different configs.

but i have Beacons 114 Data 6 after 25 mins of one try.

i just see the list pick one and then in the next screen i got only one row of info nothing devlops.i
really wants to learn this,
i feel kinda stupid =D

ekkamina420 - August 20, 2012, 8:48 pm

I HOPE YOUR GUIDE WILL TURN OUT USEFUL FOR ME SOON :) thanks anyway

pleasure - August 21, 2012, 7:45 pm

Can i have the dictionary please . thank you

Woof - August 22, 2012, 7:18 pm

nice post i really got to try this one day :)

Ove?lo?d - August 24, 2012, 6:42 pm

This is a great TuT bro! Thanks so much!

pleasure - August 24, 2012, 8:28 pm

can i have the dictionary please thank you

triger1031 - August 26, 2012, 10:23 pm

Can you please send pm to me for a link for the dictionary file? Thank you

GreyPhantom - August 27, 2012, 3:58 am

Is it possible for LinkSys WiFi , my WiFi have password too which I don't know what.

BelmontKS - August 28, 2012, 6:21 pm

Very confusing, but it's very detailed good post!

thankyoufreaksvids - August 28, 2012, 8:46 pm

Thank you very much1!!! much needed!!!

jennliml - August 29, 2012, 4:38 pm

Thank you for this great tutorial..

pleasure - September 16, 2012, 12:02 pm

Does anyone else has wpa wordlist dictionary? thank you

Autolite - October 12, 2012, 5:21 pm

Thanks alot for this.

I'm gonna be using it for sure!

Mr.Oug - October 19, 2012, 10:40 pm

I am bringing this up this is an awesome tutorial...!!!

marlopez - December 19, 2012, 2:01 am

Awesome tutorial!!!

Got handshake here!

i already try rockyou and darcode list

But it says password is not in dictionary

could you help me crack this one..

Here's the handshake:

<http://depositfiles.com/files/ckaf4fpx8>

FreizJah - January 26, 2013, 1:57 pm

Nice Tutorial ?

Pictures helped me too!

ngangsiaa - February 4, 2013, 10:07 am

this tutorial is more than an engineering egree in mit, lol

you are goo man this is really cool

SIM-5027354 - June 2, 2021, 12:34 pm

this is a good guide.. thanks friend.

John.xx - June 11, 2021, 11:12 pm

Thank

For the share man it helped

2xTheTap115 - June 23, 2021, 10:02 am

Great instruction, it's just a pity that the OP didn't set up an account on the forum.

You can see immediately that it would be HQ :)

48392jdd2 - June 24, 2021, 8:01 am

This is great, but I can't reach out for the word list.... Could someone PM it please?