

Forum:[Hack Forums](#)

Thread: [GAIN REMOTE ACCESS ON REMOTE COMPUTERS!!!! LINK](#)

tumaeka123 - May 2, 2012, 11:26 pm

im forced to ask this on HF coz whenever i search about this they use it backtrack which is impossible for me to download and would take many motnhs to complete.

my connection is only a dsl - 512 kbps

so my question would be.

can i gain remote access using metasploit on my windows 7 starter laptop?

if not then can i just mini linux out there?? not ubuntu but more smaller that can be installed on a 1gb usb.

matt_ - May 2, 2012, 11:35 pm

Download crunchbang and build your own backtrack. Create a persistent file system on your thumb drive, install all the tools you'll need and your good to go.

You dont want to use Metasploit on windows 7, its a pain in the ass to get running properly.

tumaeka123 - May 2, 2012, 11:44 pm

but is it really possible even if it's a pain in the ass?

im gonna tryt that both. try onwinods 7 first coz this is what i have only..

and can you help me or make tut about your saying? im a 101% noob.

so what tools im gonna need to make backtrack?

p.s do you mean to run metasploit on backtrack i will make?

pls help me..

but is it really possible to use metasploit on windows 7 even if it is a pain in the ass?

could make a tut or pm or post here how to make my own backtrack?
will i download large file? 500mb is large for me.

sorry double posts.. i thought i failed to reply.

Vvrouter - May 3, 2012, 12:22 am

(May 2, 2012 11:35 PM)matt_ Wrote: [\[CITE\]](#) Download crunchbang and build your own backtrack. Create a persistent file system on your thumb drive, install all the tools you'll need and your good to go.

You dont want to use Metasploit on windows 7, its a pain in the ass to get running properly.

I disagree. I installed metasploit succesfully on a windows 7 32bit system. Worked like a charm. Can prove with 3 meterpreter sessions.

My tut for installing metasploit on windows.
Go to google.
Typ metasploit.
Go to the first link (rapid7)
Download metasploit (which can take a while if u have 512kb/s)
Install metasploit by pressing next a couple of times
Done

What most people don't get (apparently) is that backtrack is just ubuntu with a whole lot of pentest/vuln scan/SET tools on it. Ur asking what tools u need to make a similar backtrack distro? Well what are you gonna use it for? Don't install stuff you don't need or never gonna use, thats a waste of disk space or in your case a waste of bandwidth.

tumaeka123 - May 3, 2012, 1:34 am

PLEASE HELP ME!!! I BEG YOU ALL PENTESTERS OUT THERE

i saw a tut but it is only for backtrack.. how sad. but it is stated in there that i could do it on windows.

but when i saw the first command the author typed in i think it wouldn't work on me.

it is written on that thread to run the terminal/shell which i know is same to cmd but a windows version only and type in msfpayload.. i already anticipated that it would only command not found on cmd.

source: <https://hackforums.net/showthread.php?tid=1183602>

ok thanks sir.. i thought i could only hack if im on linux. you restore my hope again..

another question.. if i access them tru metasploit can i run their cmd tru my local pc?

HEY I JUST FOUND A TUTORIAL ACCESS SOMEONE'S SYSTEM REMOTELY..

link:
<http://null-byte.wonderhowto.com/blog/hack-like-pro-exploit-and-gain-remote-access-pcs-running-windows-xp-0134709/>

hahahha. i whis this would work on me too.

Vvrouter - May 3, 2012, 3:16 am

(May 3, 2012 01:34 AM)tumaeka123 Wrote: [\[CITE\]](#) 1.

i saw a tut but it is only for backtrack.. how sad. but it is stated in there that i could do it on windows.

but when i saw the first command the author typed in i think it wouldn't work on me.

it is written on that thread to run the terminal/shell which i know is same to cmd but a windows version only and type in msfpayload.. i already anticipated that it would only command not found on cmd.

2.
ok thanks sir.. i thought i could only hack if im on linux. you restore my hope again..

another question.. if i access them tru metasploit can i run their cmd tru my local pc?

3.

hahahha. i whis this would work on me too.

1. The first command is indeed in a linux shell. But basicly what he does is creating a backdoor.exe in 1 command. I don't know if this feature is available in windows (try google), but there are many other ways to gain acces to a remote system if you only have windows. When you do try the shells-command in cmd.exe, go to your metasploit folder first. The reason cmd says he doesn't find the command is because msfpayload isn't located in the system32 folder. Just browse to the folder (in cmd.exe) containing msfpayload and try again.

2. Yes you can.

3. And if you scan your target correctly, it CAN be that easy. I'm not saying it will tho..

trololo - May 3, 2012, 6:27 am

yes you can, portforward ur machine and use the correct exploit and set LHOST as your external IP
forward the ports u use 2 your local IP
voila?? :D

happyhaxor - May 7, 2012, 12:07 pm

@trololo : I have heard that we need to rwaek the exploit code as well..have you done that ?? and did you exploit a remote server ?? Please reply honestly coz if you havent then ill reserch on it :)

trololo - May 9, 2012, 10:52 am

i can hack on wan, but i didnt binded the server, but i got access on the wan
if u wanna know this