

Forum:[Hack Forums](#)

Thread: [Question about Pivoting](#)

Lian - November 15, 2012, 5:57 pm

Hello guys. How are you doing?

So here is the scenario:

Backtrack is connected to Windows 8

Windows 8 is connected to Linux Server

Backtrack cannot communicate with Linux Server because they are not in the same subnet.

Using the latest java exploit I can get System in the Windows 8 Machine.

Question: There are many ways how to do pivoting, metasploit, ssh, ncat, proxychain.

I have tried all these but I haven't been able to scan the Linux Machine. For some reasons metasploit scan comes out blank. Do you guys have any idea what to do in order to get direct access from my backtrack via windows to the linux server such that I can run commands on my Backtrack directly against Linux Server?

Vile Soul - November 15, 2012, 5:59 pm

theres your problem. you said windows 8

windows 8 =shit

Lian - November 15, 2012, 6:11 pm

(Nov 15, 2012 06:59 PM)ilikecake21 Wrote: [\[CITE\]](#) theres your problem. you said windows 8

windows 8 =shit

I agree with you, I really hate it. But this is not the answer I am looking for :)

unname2012 - November 15, 2012, 6:14 pm

(Nov 15, 2012 06:57 PM)Lian Wrote: [\[CITE\]](#) Hello guys. How are you doing?

So here is the scenario:

Backtrack is connected to Windows 8

Windows 8 is connected to Linux Server

Backtrack cannot communicate with Linux Server because they are not in the same subnet.

Using the latest java exploit I can get System in the Windows 8 Machine.

Question: There are many ways how to do pivoting, metasploit, ssh, ncat, proxychain.

I have tried all these but I haven't been able to scan the Linux Machine. For some reasons metasploit scan comes out blank. Do you guys have any idea what to do in order to get direct access from my backtrack via windows to the linux server such that I can run commands on my Backtrack directly against Linux Server?now,when backtrack connect to window 8 ,you should use feature route add in metasploit to add subnet,and then you can exploit linux server
syntax :

metepreter>run get_local_subnets (get subnet)

msf>route add [gateway] [netmask] [session id]

msf>route print (printing the result)

Regards

Lian - November 15, 2012, 6:26 pm

Yes as I already said above I am familiar with pivoting and I know how to use route command. Question is how to I run lets say a python script on my backtrack against let's say port 10.000 on Linux Server?

unname2012 - November 15, 2012, 6:34 pm

in this case,you should use payload sock4a

firstly ,setting SRVHOST is your IP,SRVPORT is your port

secondly you using route add feature

then,on backtrack,you using proxychain to load sock

ex : proxychain nmap -A -sS -sV -PN [IP server linux]