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.

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

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

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

Now, let’s see the original backdoor inside the folder. Here you can see the metsrv.dll and exe files.
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
```
Now, we need to check all fields by giving the “show options” command.

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

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.
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. 😊