Ethical Hacking Lab Series

Lab 3: Using the SYSTEM Account

Certified Ethical Hacking Domain:
System Hacking

Document Version: 2013-07-18 (Beta)

Organization: Moraine Valley Community College
Author: Jesse Varsalone

.

The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

Contents

Introduction

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

This lab includes the following tasks:

- 1 - Introduction to Windows Accounts
- 2 - Using the SYSTEM Account on a Local Machine
- 3 - Using the SYSTEM Account on a Remote Machine

Domain: System Hacking

Hackers often utilize machine accounts not designed for users when they exploit systems. Under normal circumstances, the SYSTEM account would not be used by users. The SYSTEM account within Windows is actually a "reserved" machine account. There are certain folders within Windows, such as the System Volume Information folder, where the permissions are set so only the SYSTEM account can have access.

Here are some methods by which a hacker could utilize the SYSTEM account:

- Scheduling a Job
- Using PsExec
- Exploitation of a Service Running as SYSTEM

During this lab, students will utilize the SYSTEM account on a local and a remote machine. For this lab on using the SYSTEM account, the following five terms will be of use:

Local Users and Groups Management Console – There is a Local Users and Groups Management Console on computers running Windows 2000, XP, Server 2003, Vista, Windows 7, Server 2008, Windows 8, and Server 2012. However, the command to open the Local Users and Groups Management Console will not work on Windows 2000, 2003, 2008, or 2012 Servers that are Domain Controllers. The command will also not work on Home versions of the Microsoft client operating system. Any Microsoft Windows operating system that has Home, Home Basic, or Home Premium in its name will not have a local user manager.

net user – The net user command is built into all Windows NT based operating systems and can be used to add a user from the command line. The net user command allows the administrator to the give a new user a password or change the password of an existing user. You can also disable and enable accounts using the net user command. Some features of the net user command can be utilized even by non-administrative accounts, such as displaying user accounts or finding out information about a user.

PsExec – The PsExec command is not included with Windows. It is part of the PsTools suite from Sysinternals and can be downloaded from the following link: http://download.sysinternals.com/files/PSTools.zip. The PsExec tool has many useful functions for administrators, including allowing them to utilize the SYSTEM account.

at command – The at command is built into all Windows NT based operating systems and can be used to schedule a task in the future from the command line.

Windows Tasks – Tasks that are scheduled are listed in the Windows Task Scheduler.

Pod Topology

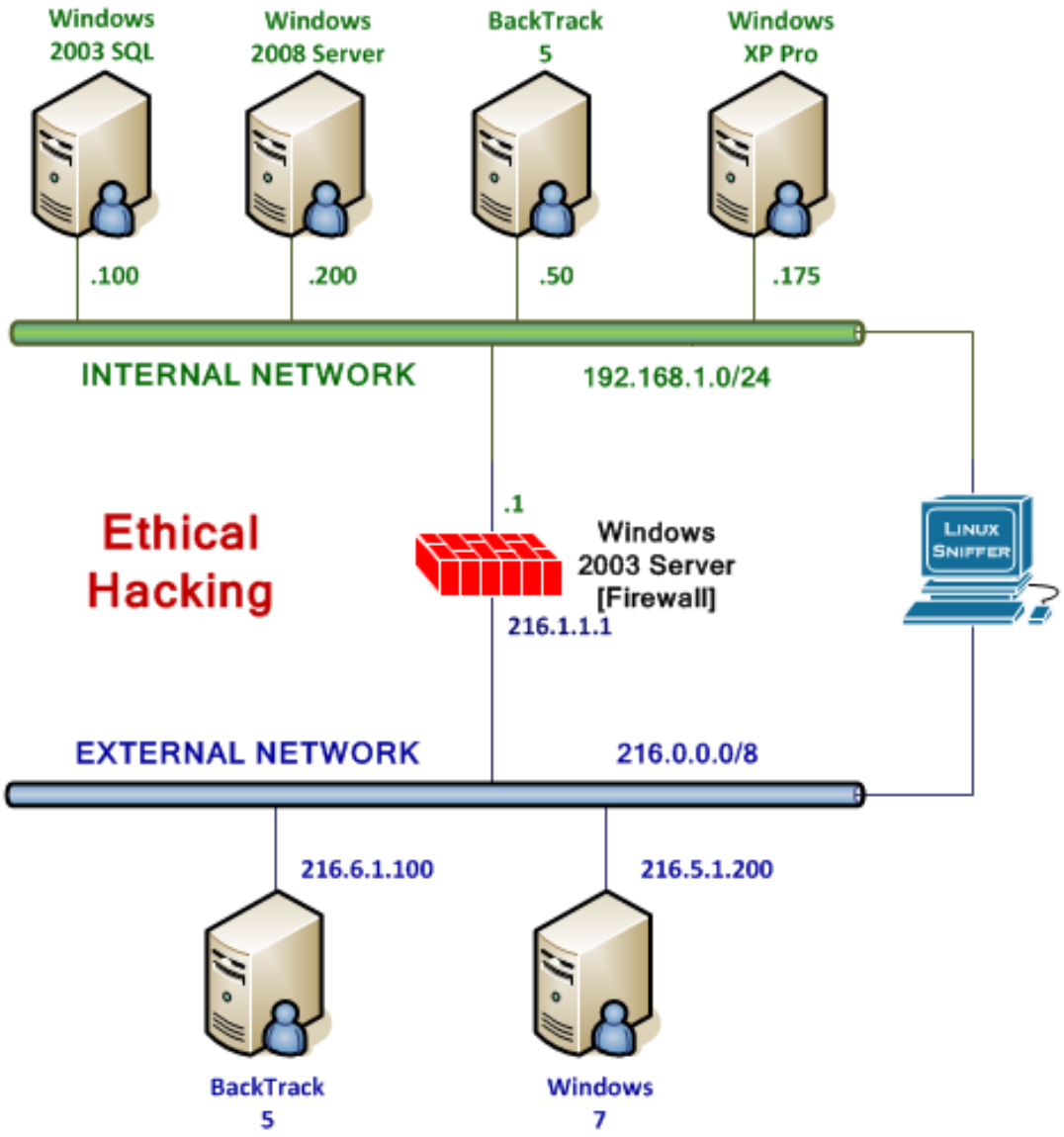

Figure 1: Lab Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

This lab requires the use of the internal machine running BackTrack 5 R3 and the Windows Internal Victim Machines running Windows XP, Windows 2003, Windows 7, and Microsoft Windows Server 2008.

Windows XP Pro	192.168.1.175
Windows XP **hacker** password	toor
BackTrack 5 Internal Machine	192.168.1.50
BackTrack 5 **root** password	toor
Windows 2008 Server - Victim Machine	192.168.1.200
Windows 2008 Server **admin** password	none

1 Introduction to Windows Accounts

On Microsoft Windows systems running Windows 2000, XP, Server 2003, Vista, Windows 7, Server 2008, Windows 8, and Server 2012, there are two useable accounts:

- Guest
- Administrator

On all versions of Windows, the Guest Account is disabled by default. On Client operating systems starting with Windows Vista, the administrator account is also disabled by default. The first user created on the system has administrative rights. There are also other special accounts that are utilized by the operating system including:

- SYSTEM
- Network Service
- Local Service

Although these accounts are not designed to be utilized by end users, some methods can be utilized to use these accounts. This lab will examine the use of the reserved SYSTEM account on Windows XP, Windows 2003, Windows 7, and Server 2008.

1.1 Examining Users on a Windows System

1. Log on as Administrator to the Windows XP Pro machine with the password of Ethicalhackin&.

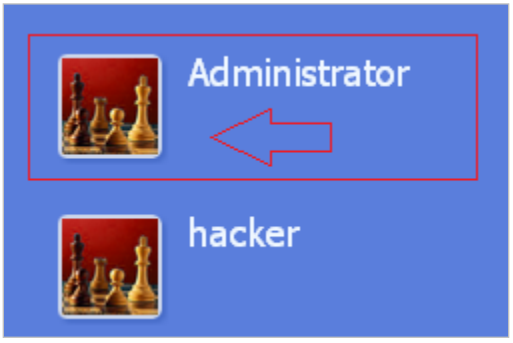

Figure 2: Logging in as Administrator

Next, we will open the Local Users and Groups Management Console by typing lusrmgr.msc; this command works on computers running Windows 2000, XP, Server 2003, Vista, Windows 7, Server 2008, Windows 8, and Server 2012. However, the command will not work on Windows 2000, 2003, 2008, or 2012 Servers that are Domain Controllers. The command will also not work on Home versions of the Microsoft client operating system. Any Microsoft Windows client operating system that has Home, Home Basic, or Home Premium in its name will not have a local user manager so the command lusrmgr.msc will not function.

Open the Local User Manager

2. On the XP system, click on Start, go up to the run box, and type the following: **Lusrmgr.msc**

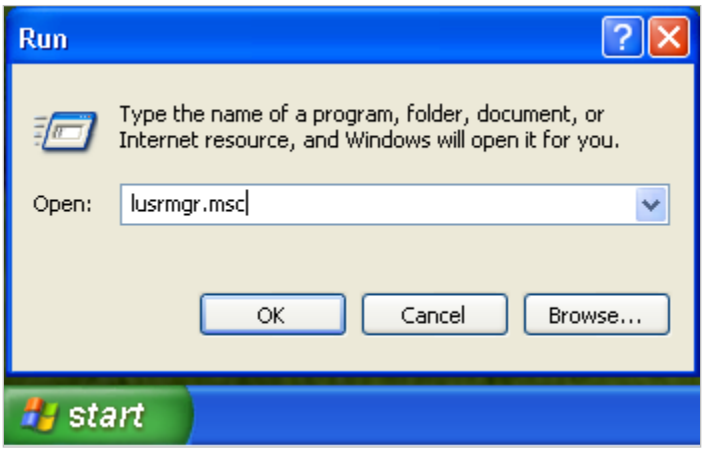

Figure 3: The lusrmgr.msc command

3. After you type lusrmgr.msc, the Local Users and Groups Management Console will appear. Double-click on the **Users** folder to view the system's user accounts.

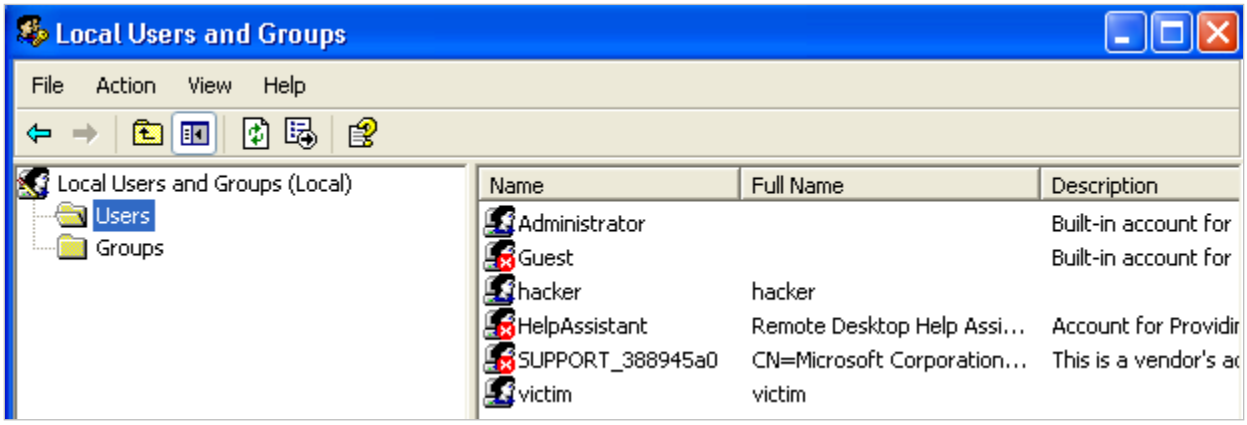

Figure 4: The Local Users and Groups Management Console

It is common to see the administrator and guest account as well as other accounts created by the administrator. On XP, you will also often see a Support and HelpAssistant account. If Internet Information Services (IIS) is installed, you will also see other accounts. Note that the SYSTEM account, network service, and local service accounts are not listed.

The SYSTEM account, network service, and local service accounts are not visible from the local user manager. We will attempt to locate the accounts by utilizing the net user command.

4. Open the **Command Prompt** on the Windows XP by clicking the desktop shortcut.

Figure 5: A Shortcut to the Command Prompt

5. To view accounts on the Windows XP system, type the following command:
C:\>**net user**

```
C:\>net user

User accounts for \\WINXP

-------------------------------------------------------------------------------
Administrator            Guest                    hacker
HelpAssistant            jesse                    SUPPORT_388945a0
victim
The command completed successfully.
```

Figure 6: The User Accounts are Listed

Once again, system, network service, and local service accounts are not visible. However, the accounts do exist on the system.

6. When attempting to add an account with the name SYSTEM and the password of password, you receive an error message stating that the account already exists.
C:\>**net user SYSTEM password /add**

```
C:\>net user SYSTEM password /add
The account already exists.

More help is available by typing NET HELPMSG 2224.
```

Figure 7: The SYSTEM account cannot be added

7. On the Windows XP system, type the following command to view hidden files:
   C:\>**dir /ah**

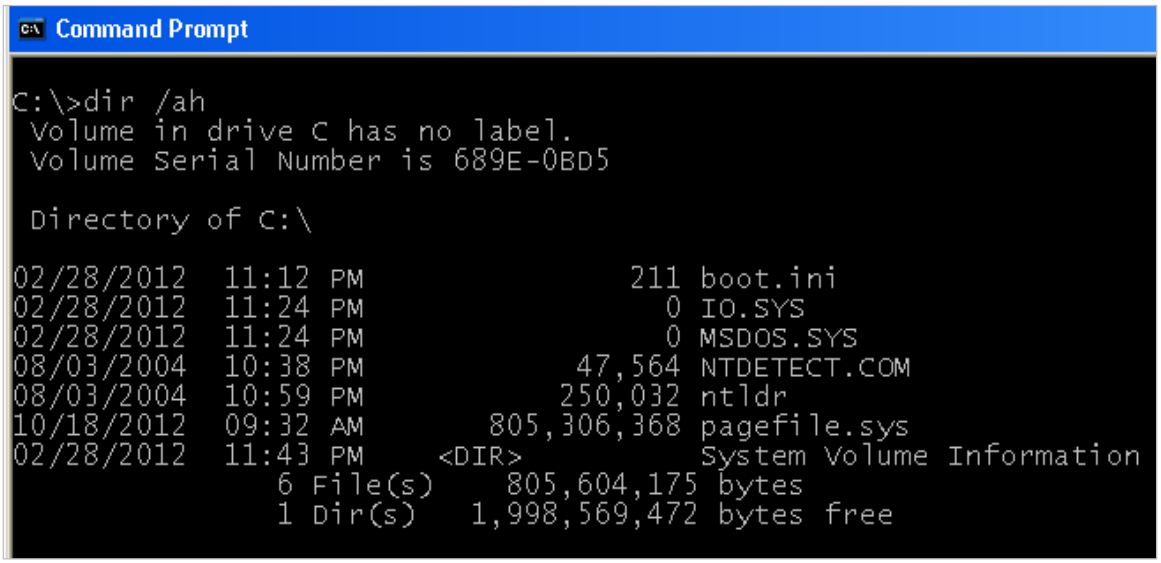

Figure 8: Listing Files with Hidden Attributes on the Root of C

8. Attempt to enter the system volume information folder by typing:
   C:\> **cd "System Volume Information"**

Figure 9: Access is denied

Even though we are utilizing the Administrator account, we cannot enter the System Volume Information folder because the only account that has access to that folder is the SYSTEM account, the SYSTEM account is reserved for the Windows operating system. Some of the items that exist in this folder include files needed for a System Restore.

Even the Administrator account cannot access the System Volume Information folder. For this reason, this folder can be a good place for hackers to store their malware. The System Volume Information folder can be a 'safe place' for malware because the administrator account cannot easily enter the folder to remove malware and some versions of anti-virus will not scan this folder. When attackers exploit systems, they often gain access to the SYSTEM account, which will allow them to enter this folder.

Viewing the NTFS Permissions

9. To view the NTFS permissions on the System Volume Information folder:
    a. Click on the Start button and go up to My Computer.
    b. Double-click on the C: Drive.
    c. Right-click on the System Volume Information folder and select properties.
    d. Click on the Security Tab to view the folder's NTFS permissions.

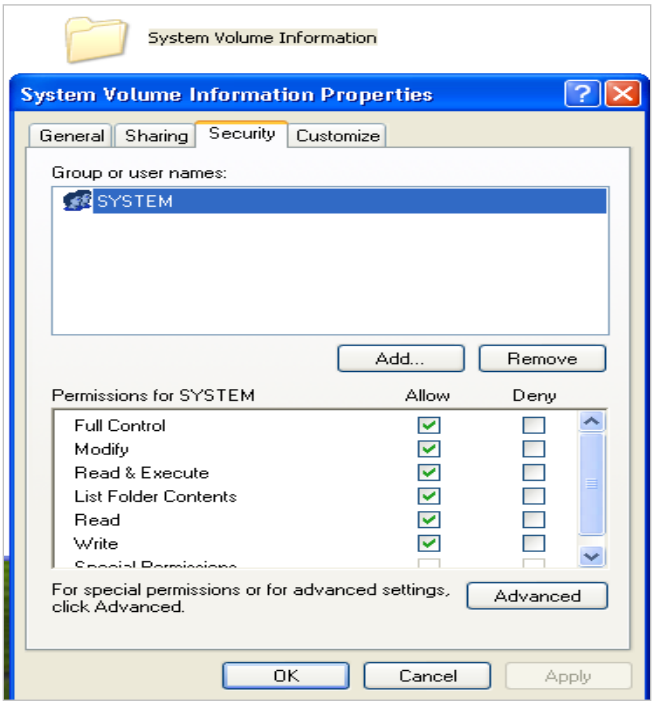

Figure 10: NTFS Permissions of the System Volume Information folder

1.2 Conclusion

The SYSTEM account is a special account that is normally not used for users. The SYSTEM account is reserved for the operating system, and has unique access to the drive. By default, the System Volume Information folder on the root of the C drive can only be accessed by the SYSTEM account. Even the Administrator account cannot access the folder. Hackers who get access to this account can store malware in this location.

1.3 Discussion Questions

1. Can you log into a Windows machine as the SYSTEM account?
2. Which folder within Windows can only the SYSTEM account access?
3. What happens if someone attempts to add a user called SYSTEM?
4. Is the SYSTEM account displayed within the Local Users and Groups Management Console?

2 Using the SYSTEM Account on a Local Machine

There are certain conditions when the SYSTEM account can be used by a user on a local system. This is not something that is normally done by an end user, but there are some workarounds that will allow the administrator to escalate their privileges to SYSTEM. One way this can be done on Windows XP or Server 2003 is by scheduling an interactive command prompt. On Vista and higher, this can be done by using the PsExec command.

2.1 Using the SYSTEM Account - Windows XP

1. Log on as Administrator to Windows XP with the password of Ethicalhackin&. and open the **Command Prompt** by clicking the shortcut on the desktop.

Figure 11: A Shortcut to the Command Prompt

2. To view the current time on your system, type the following command:
C:\>**time /t**

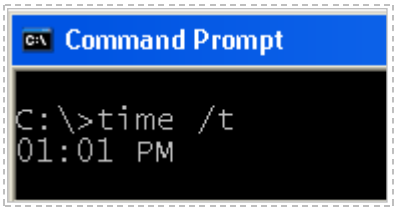

Figure 12: The Time is Displayed in Windows

3. To schedule the command prompt to run interactively, type the following:
C:\>**at XX:XX /interactive cmd**

Replace XX:XX with 4 minutes from current time, using military time.

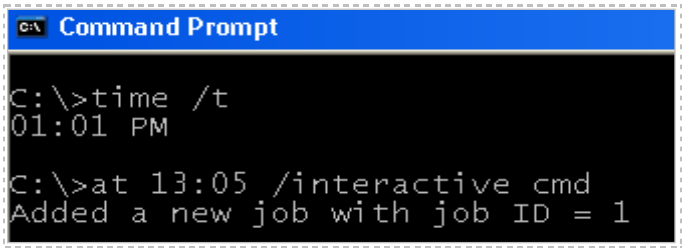

Figure 13: The Time is displayed in Windows

In 4 minutes, a new command prompt window should appear on the screen. You should notice in the title that the command prompt is displayed as:

C:\Windows\system32\svchost.exe.

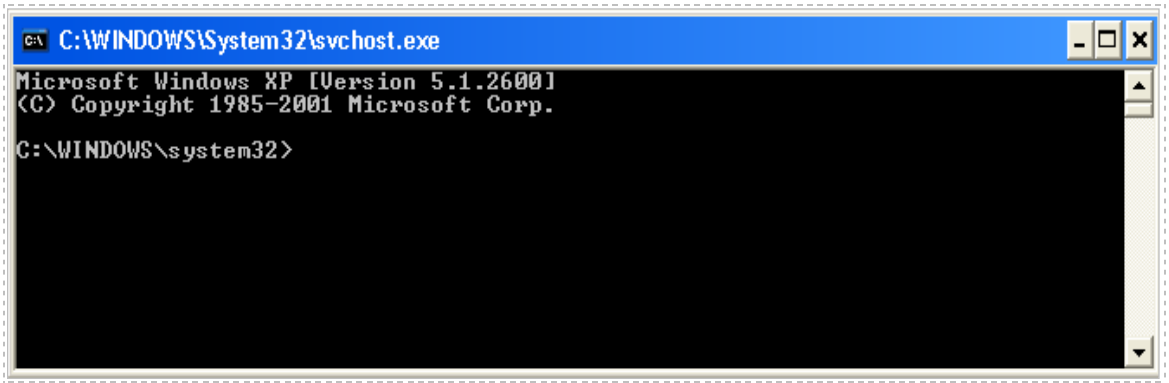

Figure 14: A command prompt titled "C:\Windows\system32\svchost.exe" appears

4. In the new command prompt window, go to the root of the C Drive by typing the following command:
   C:\>**cd **

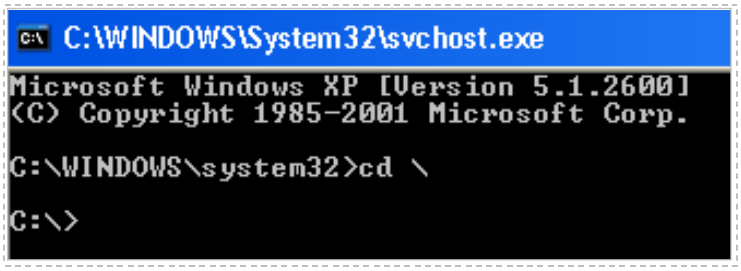

Figure 15: Navigating to the root of the C drive

5. Type the following command to enter the System Volume Information folder.
   C:\> **cd "System Volume Information"**

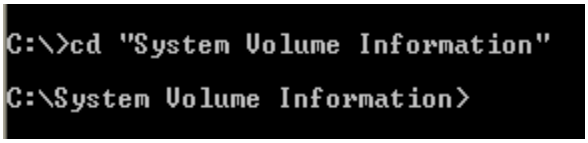

Figure 16: Entering the System Volume Information Folder

Previously, when we were logged in as Administrator, we were unable to enter the System Volume Information folder. Now that our privileges have been escalated to the SYSTEM account, we can enter the System Volume Information folder with ease.
Just to be sure that we are in fact running as the SYSTEM account, we will download a file called whoami.exe, (which is available as part of the Microsoft support tools) at the following link: http://www.microsoft.com/en-us/download/details.aspx?id=18546

Since the lab machines have no Internet access, we have made the whoami.exe file available on the BackTrack 5 machine on the internal network. In the following steps, we will use FTP to download the whoami.exe file to our Windows XP Pro machine:

6. Log on to the BackTrack machine on the internal network with the username of root and the password of toor (root spelled backwards) and type **startx** to bring up the GUI.
7. Open a terminal on the Internal BackTrack Linux system by clicking on the picture to the right of the word **System** in the taskbar at the top of the screen.

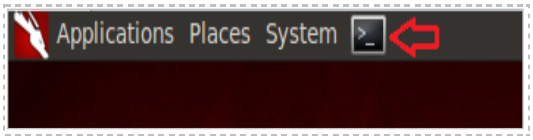

Figure 17: The Terminal Shortcut within BackTrack

After you click on the shortcut to the terminal, the terminal window will appear below.

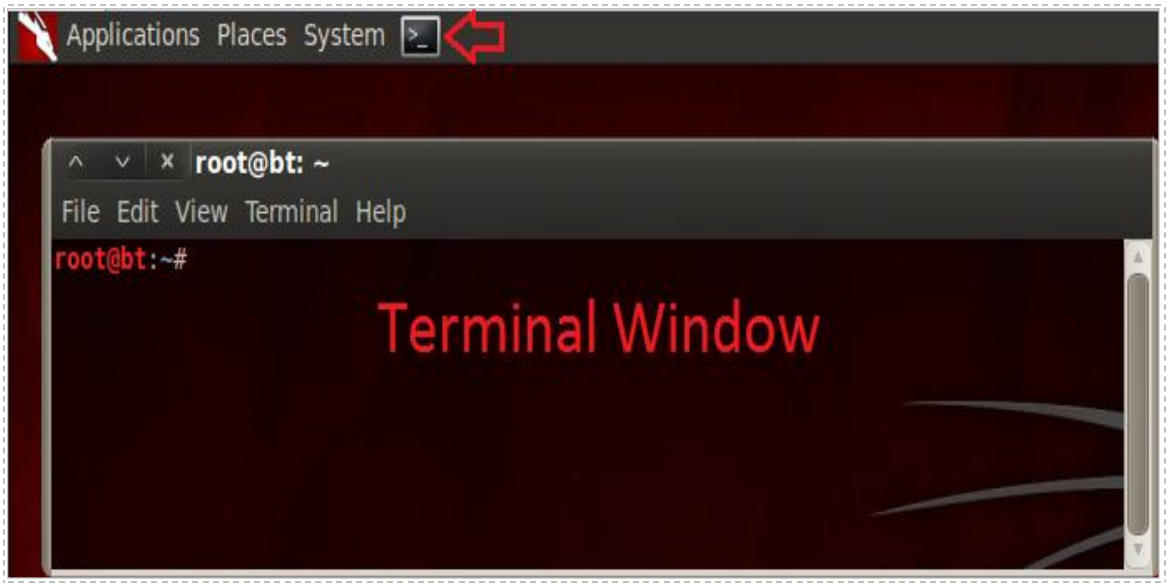

Figure 18: The BackTrack Terminal will appear

8. Type the following command to copy whoami.exe to the FTP directory for the user hax0r:
   root@bt:~# **cp /pentest/windows-binaries/tools/whoami.exe /home/hax0r**

Figure 19: Copying whomai.exe

9. To list the contents of the folder and verify that the file has been copied to /home/hax0r, type:
   root@bt:~# **ls /home/hax0r**

```
root@bt:~# ls /home/hax0r/
by.txt  hi.txt  wget.exe  whoami.exe
```

Figure 20: Viewing whoami.exe

10. Type the following command to determine the status of the vsftpd service:
    root@bt:~# **vsftpd status**

```
root@bt:~# service vsftpd status
vsftpd start/running, process 1553
```

Figure 21: VSFTPD is running

11. To verify the port on which VSFTPD is running, type:
    root@bt:~# **netstat -tanp | grep 21**

```
root@bt:~# netstat -tanp | grep 21
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
1553/vsftpd
```

Figure 22: Viewing the Running FTP Server

You will likely have a different Process ID (PID), than 1553 on your system.

As SYSTEM, we will utilize the FTP protocol to download whoami.exe, which is a command line tool that that will allow you to determine your level of access.

12. On the Windows XP Pro machine type the following to start the ftp connection:
    C:\System Volume Information>**ftp 192.168.1.50**

```
C:\System Volume Information>ftp 192.168.1.50
Connected to 192.168.1.50.
220 (vsFTPd 2.2.2)
```

Figure 23: FTP to the BackTrack Linux machine

13. You should see an ftp prompt asking for a username. Type the following:
    User (192.168.1.50:(none)): **hax0r**

```
User (192.168.1.50:(none)): hax0r
```

Figure 24: Specify the User Name

14. You should see an ftp prompt asking for a password. Type the following:
    Password: **hacker**

Figure 25: Specify the Password

You should receive a message, *230 Login successful*.

15. To switch to binary mode during the FTP session, type the following:
    ftp> bin

Figure 26: Switching to Binary Mode

You should receive a message, *200 Switching to Binary mode*.

Binary mode in FTP is used to transfer files other than ASCII files. Binary mode transmits all 8 bits of each byte, leaving less room for transmission errors. ASCII mode transmits 7 bits per byte.

16. To download the whomai.exe file from the FTP server, type the following:
    ftp> get whoami.exe

Figure 27: Transfer of the whoami.exe file is complete

You should receive the message, *226 Transfer Complete*.

17. To leave the FTP session with the remote server, type the following:
    ftp> bye

Figure 28: Exiting the FTP Session

You should receive the message, *221 Goodbye*.

18. To view the downloaded whoami.exe file on your local system, type the following:
    C:\System Volume Information>**dir**

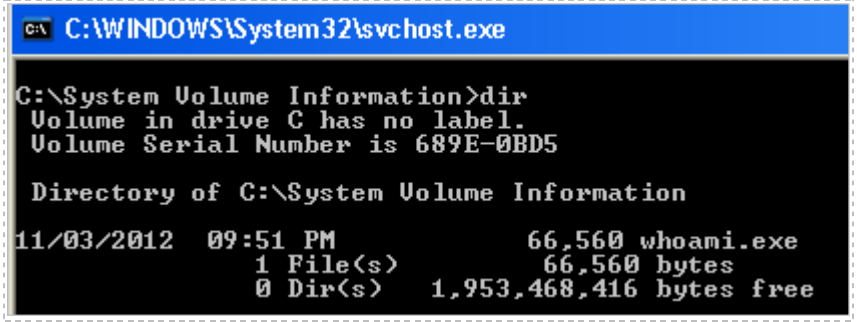

Figure 29: Viewing the Downloaded File

19. Type the following command to view your level of privilege:
    C:\System Volume Information>**whoami**

Figure 30: SYSTEM Level Access

While XP and 2003 allow users to run an interactive command prompt, that option is not present in Windows Vista, 7, 8, Server 2008, or Server 2012. However, the PsExec command can be utilized to gain SYSTEM level access on those operating systems.

20. On the internal BackTrack 5 machine, type the following command to copy psexec.exe to the FTP directory:
    root@bt:~# **cp /pentest/windows-binaries/sysinternals/psexec.exe /home/hax0r/**

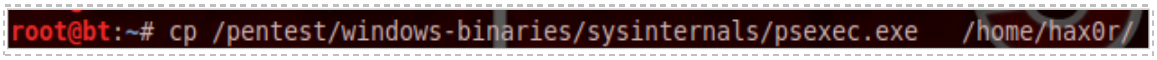

Figure 31: Copying psexec.exe

21. To list folder contents and verify that the file has been copied to the /home/hax0r folder, type:
    root@bt:~# **ls /home/hax0r**

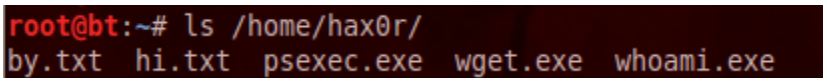

Figure 32: Viewing psexec.exe

22. On the **Windows 2008 Server** machine, right-click the shortcut to the Command Prompt on the desktop and select **Run as administrator**.

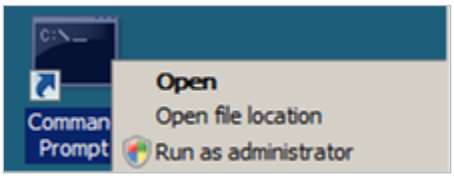

Figure 33: Opening the Command Prompt as Administrator

23. Click **Continue** when the User Account Control dialog box appears.

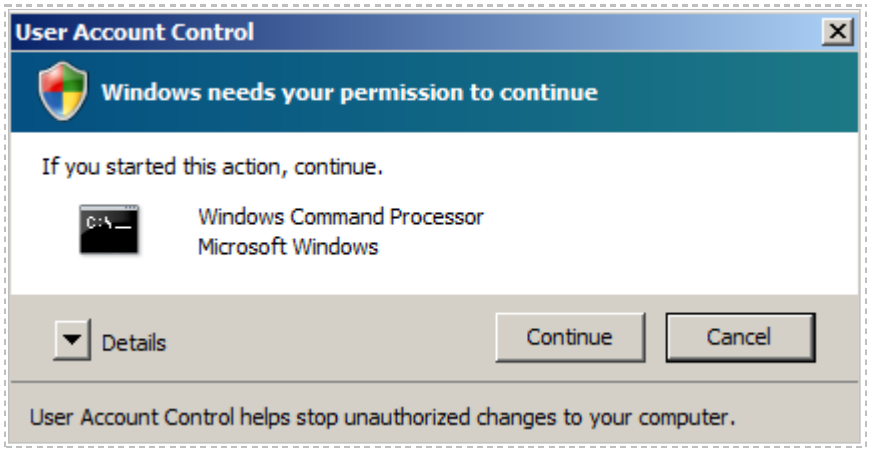

Figure 34: User Account Control

24. Type the following command to determine your level of access:
C:\Windows\system32>**whoami**

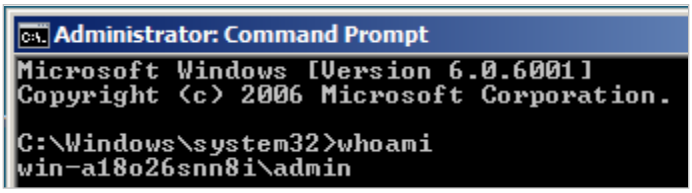

Figure 35: Viewing the Level of Privilege

25. On the Windows machine type the following to start the ftp connection:
C:\Windows\system32>>**ftp 192.168.1.50**

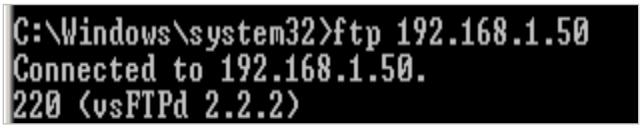

Figure 36: FTP to the BackTrack Linux machine

26. You should see an ftp prompt asking for a username. Type the following:
User (192.168.1.50:(none)): **hax0r**

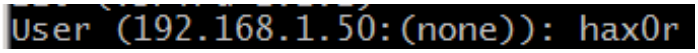

Figure 37: Specify the User Name

27. You should see an ftp prompt asking for a password. Type the following:
Password: **hacker**

Figure 38: Specify the Password

You should receive a message, *230 Login successful*.

28. To switch to binary mode during the FTP session, type the following:
ftp> bin

Figure 39: Switching to Binary Mode

You should receive a message, *200 Switching to Binary mode*.

29. To download the psexec.exe file from the FTP server, type the following:
ftp> get psexec.exe

Figure 40: Transfer of the psexec.exe file is complete

You should receive a message, *226 Transfer Complete*.

30. To leave the FTP session with the remote server, type the following:
ftp> bye

Figure 41: Exiting the FTP Session

You should receive the message, *221 Goodbye*.

31. To escalate your privileges to SYSTEM, type the following command:
C:\Windows\system32>**psexec -s cmd.exe**

```
C:\Windows\system32>psexec -s cmd.exe
```

Figure 42: Using the PsExec command

32. Click the **Agree** button to agree to the PsExec License Agreement.

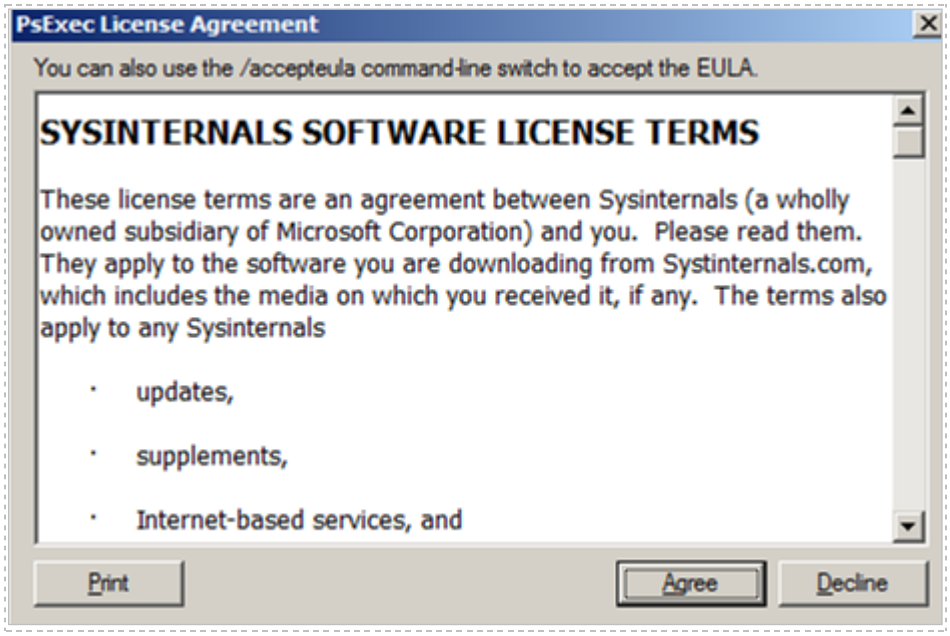

Figure 43: PsExec License Agreement

33. Type the following command to view your level of privilege:
C:\System Volume Information>**whoami**

```
C:\Windows\system32>whoami
nt authority\system
```

Figure 44: SYSTEM Level Access

Note that you now have SYSTEM level access.

2.2 Conclusion

The SYSTEM account is not intended to be utilized by users on Windows operating systems. There are, however, methods by which to gain control of this account. When the SYSTEM account is used, there are areas of the operating system, such as the System Volume Information folder, that can be accessed when running as the SYSTEM account. Hackers may use these methods to gain access to the System Volume Information folder. Since other users, including the Administrator account do not have access to this folder, hackers may use it to hide their malware.

2.3 Discussion Questions

1. How can SYSTEM level access be achieved locally on Server 2008?
2. How can SYSTEM level access be achieved locally on Windows XP?
3. What is the command to determine your level of access within Windows?
4. What account needs to be used to enter “SYSTEM VOLUME INFORMATION”?

3 Using the SYSTEM Account on a Remote Machine

In this section, you will be introduced to Armitage, a Graphical User Interface(GUI) front end for Metasploit. Armitage provides the user with a visual interface that will help them understand what is happening in the background of Metasploit.
When remote systems are exploited, SYSTEM level access is sometimes achieved.

3.1 Using the Armitage GUI

1. Open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the taskbar in the top of the screen in BackTrack version 5 R3.

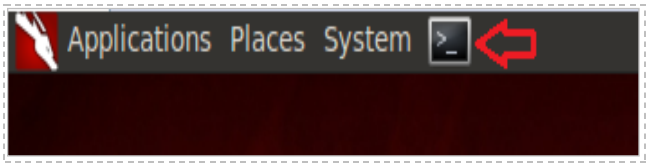

Figure 45: The Terminal Shortcut within BackTrack

2. Type **armitage** in the terminal to launch the Armitage program:
root@bt:~#**armitage**

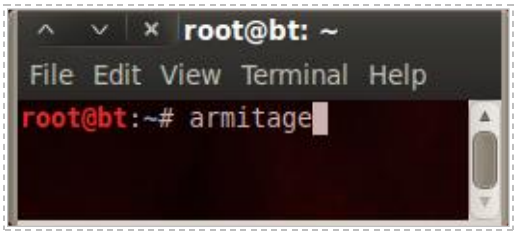

Figure 46: Launching Armitage

3. A Connect box will appear on your Screen. Click the **Connect** radio button.

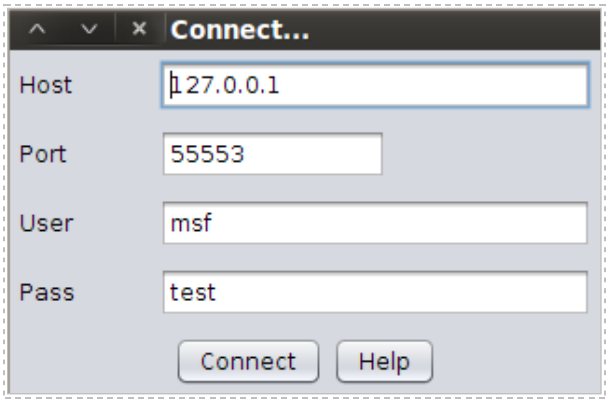

Figure 47: Click the Connect button to Launch Armitage

4. Click the **Yes** radio button when asked if you want to Start Metasploit. Ignore the connection warning error as it will disappear after a few minutes.

Figure 48: Click Yes

5. If you receive an Input box asking for an attack IP address, then type: **192.168.1.50**

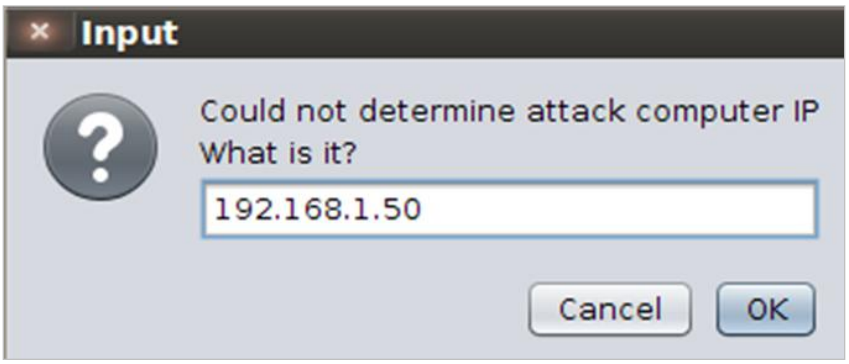

Figure 49: Adding a Host to Armitage

6. From the Armitage menu, click Hosts, and select **Add Hosts**.

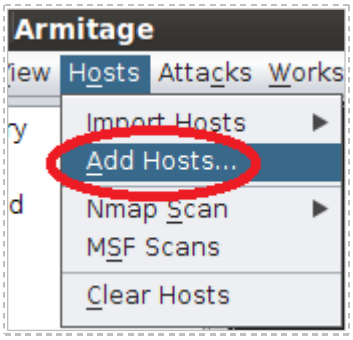

Figure 50: Adding a Host to Armitage

7. Type **192.168.1.200**, the IP address of the victim machine, and click Add.
8. You should receive a message that states, *Added 1 Host*. Click OK.

9. From the Armitage menu, choose Set Exploit Rank, and select **Poor**. This tells Armitage what rank exploit to scan for. Poor exploits may be old exploits that are widely patched; while excellent exploits have a greater chance of being successful.

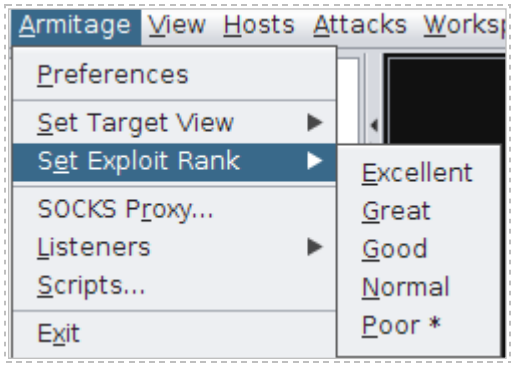

Figure 51: Adjusting the Auto-Layout Settings

10. Click **OK** to the message that states, *Updated minimum exploit rank*.

Figure 52: Minimum Exploit Rank Updated

11. Right-click on the host in the Armitage pane and select **Scan**. The scanning process may take up to 30 seconds.

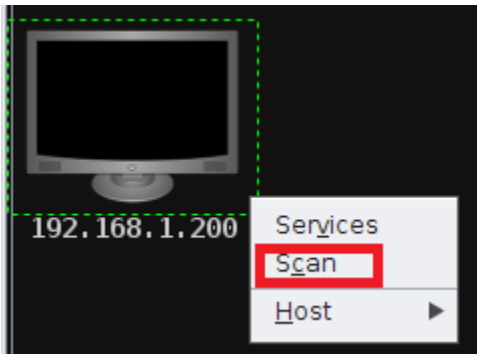

Figure 53: Scanning the Victim Machine

12. Once the scan is complete, your target will now be identified. If you hover over the icon, the remote machine will be identified as **Windows Server 2008 Standard without Hyper-V SP1**.

Figure 54: The Victim Machine Operating System is identified

13. From the Attacks menu in Armitage, select Attacks and then Find Attacks. Wait until you receive the message from Armitage that states, *Happy Hunting*.

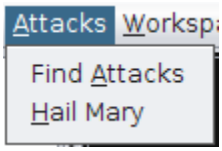

Figure 55: Finding Attacks

14. Right-click on the icon representing the victim in the Armitage pane and select **Attack >smb>ms09_050_smb2_negotiate_func_index**.

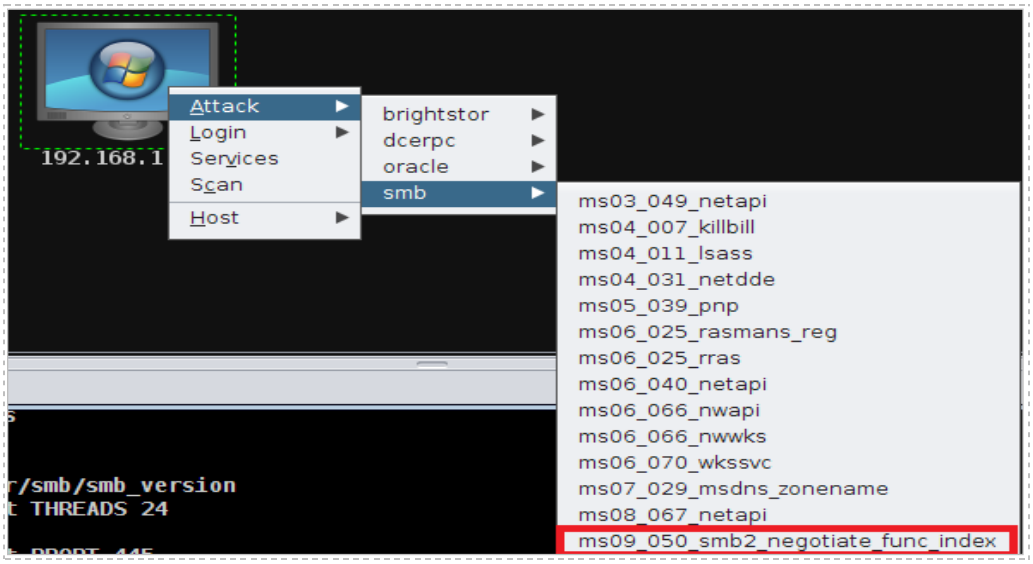

Figure 56: ms09_050_smb2_negotiate_func_index Attack

15. In the Launch Window, the title should be **Attack 192.168.1.200**. Notice that a description of the exploit is provided. Also, notice that the remote port of 445 is listed as the value of RPORT. Check the box that says Use a Reverse Connection and then click the **Launch Button** to attack the remote machine.

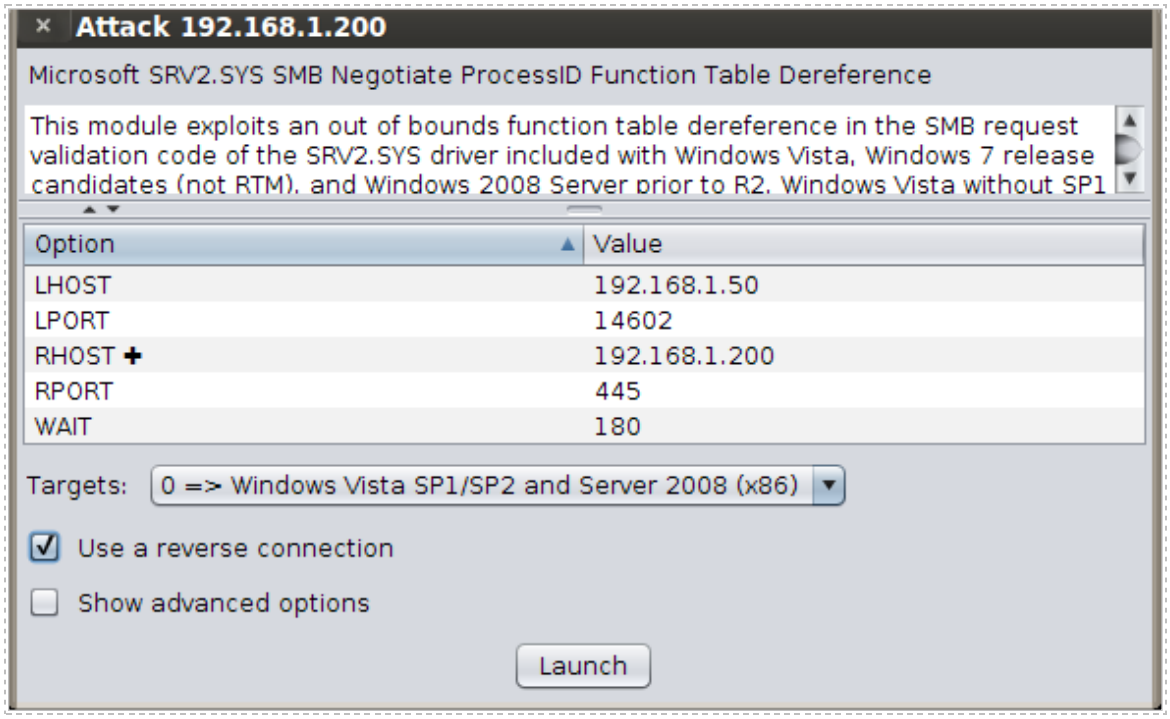

Figure 57: Launching the Attack against the Victim Machine

If the attack is successful, the victim machine icon will be displayed with a red border. If the attack does not work, you may need to attempt to launch the attack again. If all else fails, reboot the Windows 2008 Server machine at 192.168.1.200. Once the attack is successful, the victim is considered to be in a compromised state.

Figure 58: The Attacker is connected to the Victim Machine as SYSTEM

If the attack does not initially work, reboot the Windows 2008 Server machine. Perform steps 6-15 again and the exploit should work successfully. Notice that the level of access of **NT AUTHORITY\SYSTEM** is displayed by Armitage.

16. Right-click on the host, select **Meterpreter 1 > Interact > Meterpreter Shell**.

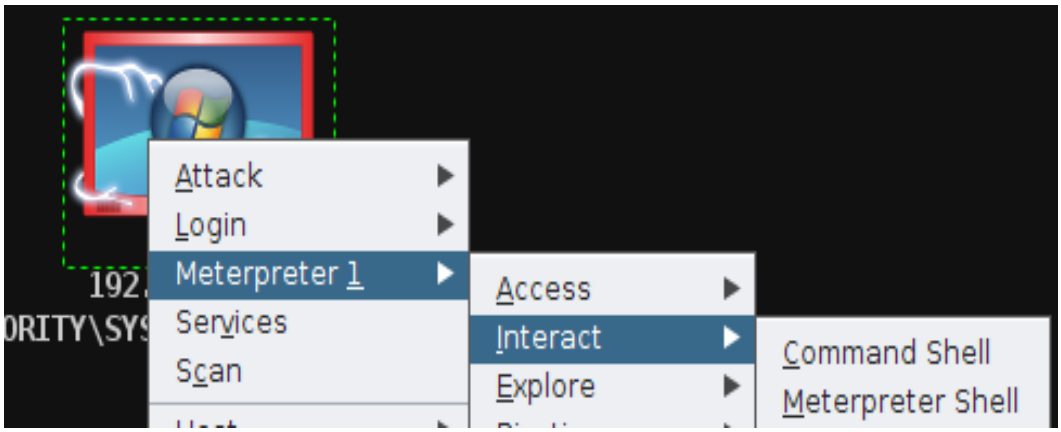

Figure 59: The Attacker is connected to the Victim Machine as SYSTEM

17. In the bottom Meterpreter 1 pane, type the following to determine access level:
meterpreter > **getuid**

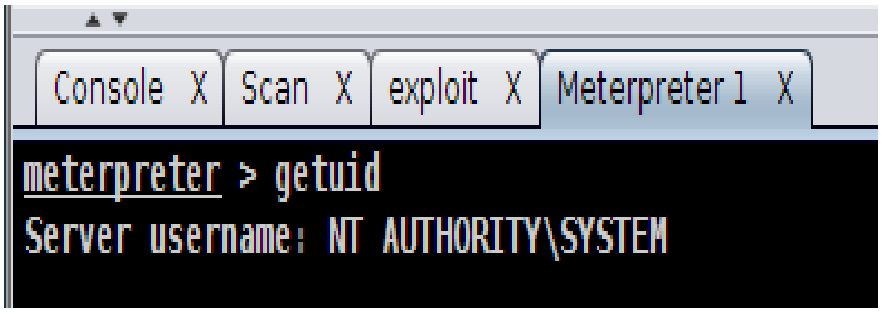

Figure 60: The getuid command indicates the Attacker is SYSTEM

18. In the bottom Meterpreter 1 pane, type the following to determine the process ID (PID):
meterpreter > **getpid**

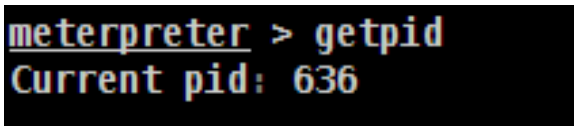

Figure 61: The getpid command indicates the PID the attacker is Using

Your PID will likely be different than 636.

.

19. In the bottom Meterpreter 1 pane, determine the owner of the PID by typing: meterpreter > **ps**

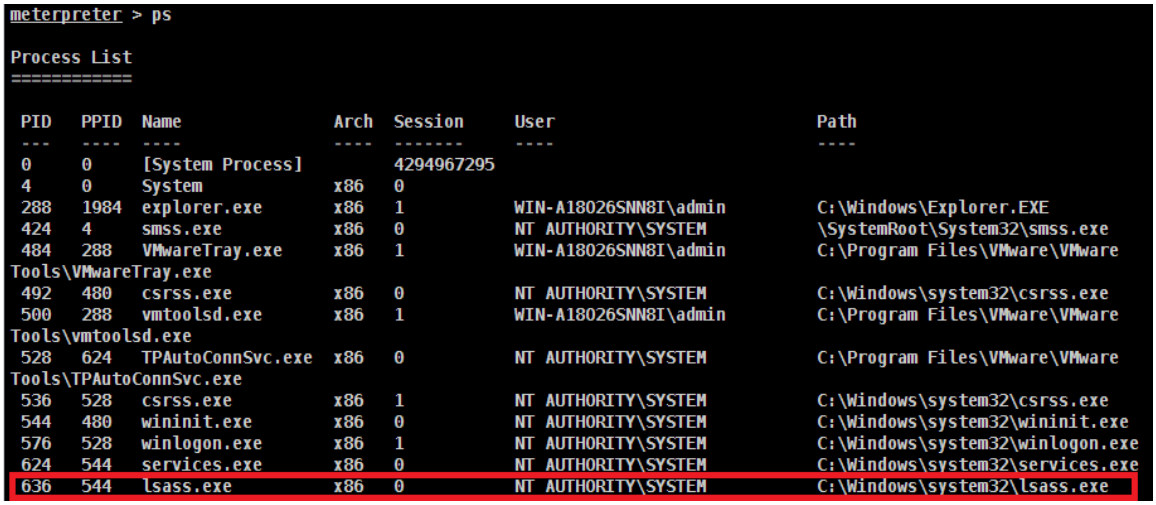

Figure 62: The Attack was against the lsass.exe service, which was running as the SYSTEM Account

3.2 Conclusion

Armitage is a GUI frontend for Metasploit that allows attackers to scan, identify, and exploit remote operating systems. After scanning a machine, Armitage will report what operating system and service pack level the target machine is using. The Armitage tool then allows the attacker to find attacks by open ports. If the attacker is able to successfully connect to a victim machine, the victim will be displayed with a red border. The attacker can determine their level of privilege by typing getuid command. The attacker can type the getpid command to determine the process ID (PID) they are using and ps to determine the process name.

3.3 Discussion Questions

1. What is the name the exploitation tool for which Armitage is a GUI front end?
2. What message does Armitage display after you try to find attacks?
3. What is the command to determine the level of access on the remote victim?
4. What is the command to determine the PID the attacker is utilizing?
5. After the PID is discovered, what command can be used to find the name of the process?

References

1. Windows Local User Manager:
   http://www.sevenforums.com/tutorials/7539-local-users-groups-manager-open.html

2. Net User Command:
   http://support.microsoft.com/kb/251394

3. PsExec:
   http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

4. AT Command:
   http://support.microsoft.com/kb/313565

5. Windows Local SYSTEM account:
   http://msdn.microsoft.com/en-us/library/windows/desktop/ms684190(v=vs.85).aspx

