



CompTIA Security+® Lab Series

Lab 4: Protocols and Default Network Ports - Connecting to a Remote System

CompTIA Security+® Domain 1 - Network Security

Objective 1.4: Implement and use common protocols

Objective 1.5: Identify commonly used default network ports

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 (TAACCCT) 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
Objectives: Implement and Use Common Protocols	3
Identify Commonly Used Default Network Ports	3
Pod Topology	5
Lab Settings	6
1 Connecting to a Windows System through the Command Line	9
1.1 Using TELNET to Perform Remote Administration	9
1.2 Conclusion	16
1.3 Discussion Questions.....	16
2 Connecting to a Linux System through the Command Line	17
2.1 Using SSH to Connect to a Remote Linux System	17
2.2 Conclusion	24
2.3 Discussion Questions.....	24
3 Analyzing Remote Connections in Network Traffic.....	25
3.1 Using Wireshark to Analyze Connections to a Remote Linux System	25
3.2 Conclusion	30
3.3 Discussion Questions.....	30
References	31

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 connect to remote systems running Windows and Linux and run commands to perform administrative tasks. Students will use the TELNET protocol to connect to remote Windows system and the SSH protocol to connect to a system running Linux. Students will then analyze both protocols within network traffic to determine whether the protocol uses encryption or clear text.

This lab includes the following tasks:

- 1 - Connecting to a Windows System through the Command Line
- 2 - Connecting to a Linux System through the Command Line
- 3 - Analyzing Remote Connections in Network Traffic

Objectives: Implement and Use Common Protocols Identify Commonly Used Default Network Ports

Network Administrators often have to perform maintenance on servers from remote locations. The server could be on a system within the same building or across the globe. Network administration can be done remotely through a GUI-based program like Microsoft Terminal Services or Virtual Network Connector (VNC), but the use of command line tools like TELNET and SSH is extremely common. It is very common to have a Linux system running without a GUI, and there are even some distributions of Windows, like Server Core, that have no GUI interface. It is critically important for network administrators to understand command line utilities in order to have a good grasp of computer security concepts.

TELNET – The TELNET protocol, which uses port 23, allows someone to remotely administrator a computer, router, and switch. All traffic sent using the TELNET protocol is sent in clear text, which means usernames and passwords will be visible to anyone examining the traffic. For security reasons, the use of TELNET should be avoided.

SSH – Secure Shell, which uses port 22, allows a user to securely connect to a remote device. Unlike TELNET connections that are in clear text, SSH connections are encrypted. While Linux and Mac have support for SSH natively, Windows does not.

Windows 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.

Linux Bash Shell – The Linux Bourne Again Shell, or Bash, is one of many shells that are available in a Linux environment. Linux servers are often managed from the command line; therefore, network administrators need to be comfortable with bash.

Wireshark – Wireshark is a protocol analyzer that will allow you to capture and analyze network traffic. Wireshark can be used to inspect traffic and examine the clear text communication of TELNET and encrypted communication of SSH.

Pod Topology

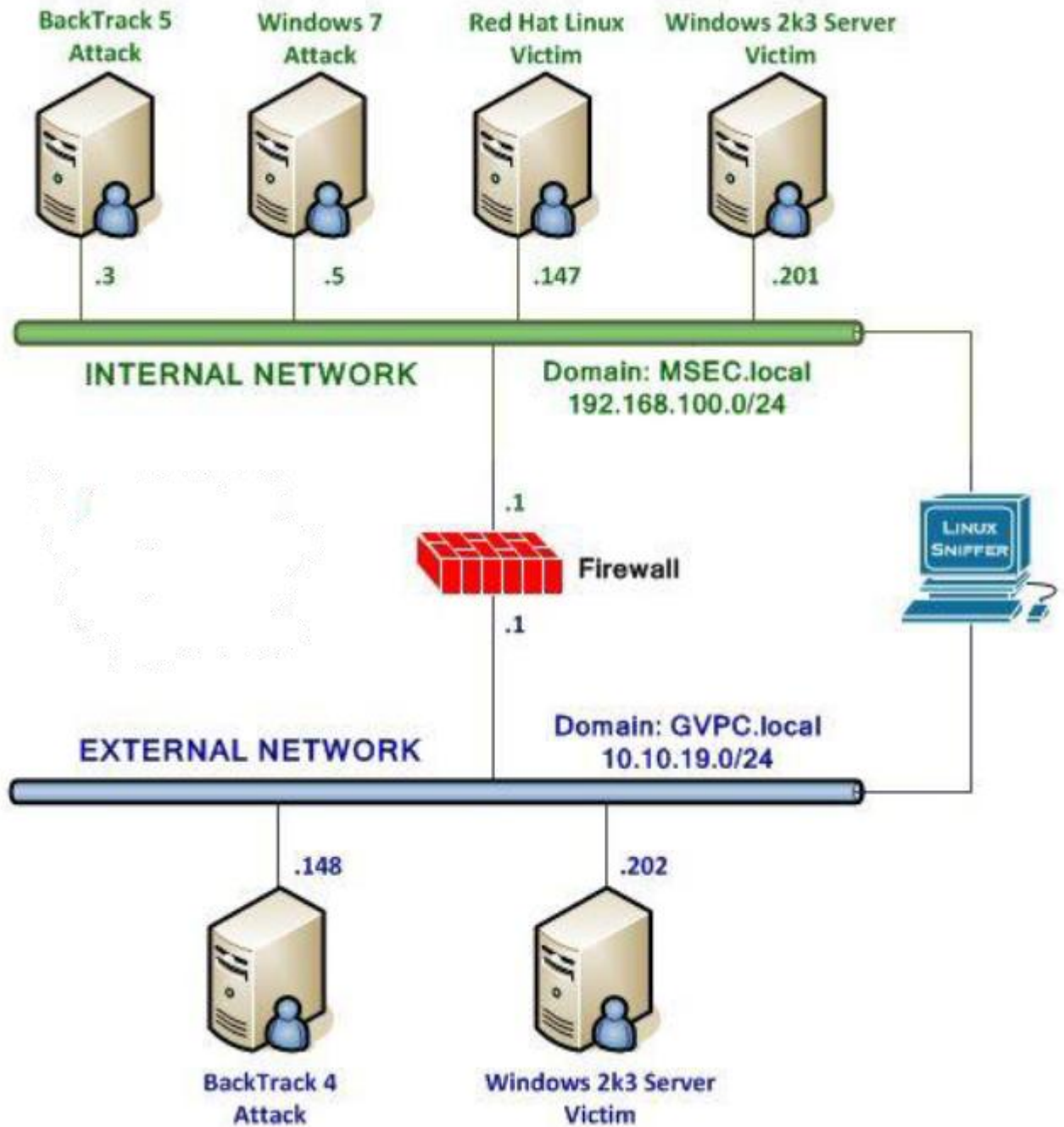


Figure 1: Topology

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 2k3 Server Internal Victim Machine	192.168.100.201
Windows 2k3 Server administrator password	password
Red Hat Enterprise Linux Internal Victim Machine	192.168.100.3
Red Hat Enterprise Linux root password	password
Windows 7 Internal Attack Machine	192.168.100.201
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 screenshot of a terminal window titled "BackTrack 5 R1 - Code Name". The prompt "bt login: root" is displayed, followed by "Password:" and a cursor. The terminal background is black with white text.

```
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.

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

Figure 3: BackTrack 5 GUI start up

Windows 2k3 Server Internal Victim Login:

1. Click on the **Windows 2k3 Server Internal Victim** icon on the topology
2. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer).
3. Enter the User name, **Administrator** (verify the username with your instructor).
4. Type in the password, **password**, and click the **OK** button (verify the password with your instructor).



Figure 4: Windows 2k3 login

Red Hat Enterprise Linux Internal Victim Login:

1. Click on the **Red Hat Linux Internal Victim** icon on the topology.
2. Type **root** at the **rhel login:** prompt.
3. Type **password** at the **Password:** prompt.

For security purposes, the password will not be displayed.

4. To start the GUI, type **startx** at the **[root@rhe ~]#** prompt.

```
Red Hat Enterprise Linux Server
Kernel 2.6.18-308.el5 on an i686

rhel login: root
Password:
Last login: Sat Jun 16 11:48:58
[root@rhel ~]# startx_
```

Figure 5: RHEL login

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).

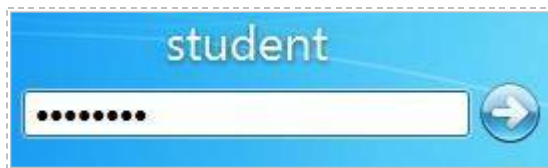


Figure 6: Windows 7 login

1 Connecting to a Windows System through the Command Line

For a variety of reasons, network administrators may need to perform tasks on a remote system. TELNET can be used to perform remote administration on computers, routers, switches, and other devices. The disadvantage of using TELNET is that it sends everything across the wire in clear text including usernames, passwords, and commands. For this reason, the use of TELNET should be avoided if possible.

First, we will scan the victim machine to determine if the TELNET port is open. We will specify the default TELNET port of 23 when conducting the Nmap scan.

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

1.1 Using TELNET to Perform Remote Administration

Open a Command Prompt to Get Started

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

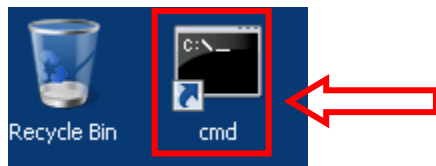


Figure 7: Opening a Command Prompt on Windows 7

2. Before you start, determine the IP address of the Windows 7 Internal Attack Machine by typing:
C:\ipconfig

```
C:\>ipconfig

Windows IP Configuration

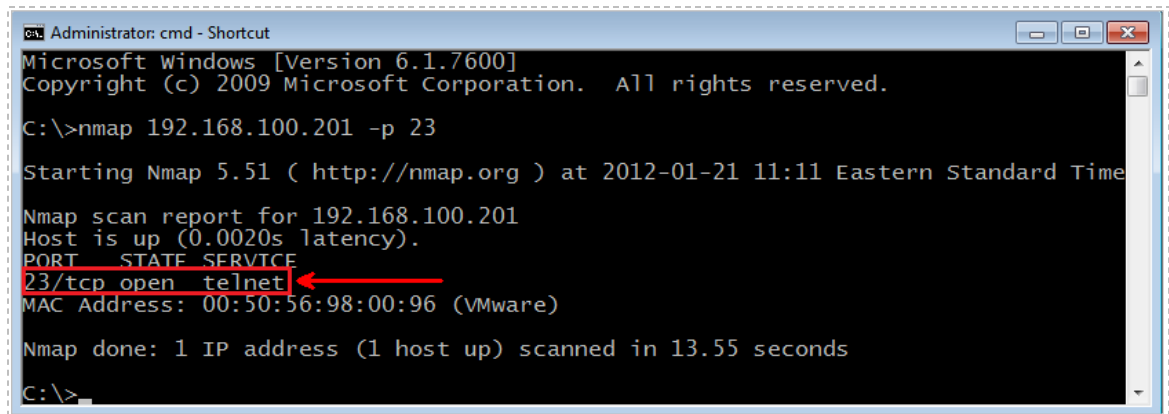
Ethernet adapter Local Area Connection:

    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 8: The IP address Information of the Windows 7 Machine

3. Type the following to determine if port 23 is open on the remote system.

C:\nmap 192.168.100.201 -p 23



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

C:\>nmap 192.168.100.201 -p 23

Starting Nmap 5.51 ( http://nmap.org ) at 2012-01-21 11:11 Eastern Standard Time

Nmap scan report for 192.168.100.201
Host is up (0.0020s latency).
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 00:50:56:98:00:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds
C:\>
```

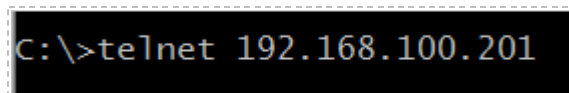
Figure 9: The Results of an Nmap Scan

The results of the Nmap scan indicate that the TELNET port is open on the remote system. In order to connect via TELNET, you need to have a user account and the password for the remote system. This information is sent over the network in clear text.

The TELNET client is not installed by default on Windows Vista or Windows 7. It must be added through the Add Programs and Features applet in the Control Panel. We have already added the TELNET client feature on the Windows 7 Internal Attack Virtual Machine.

4. From the command prompt, type the following command

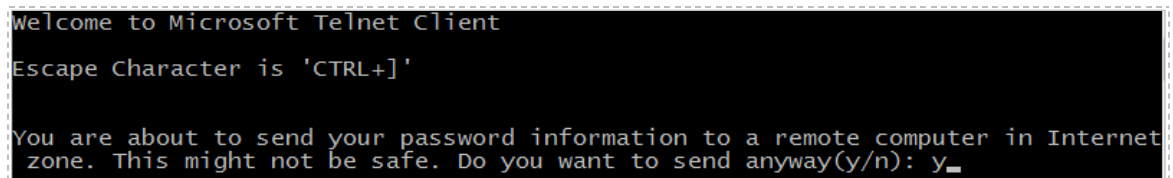
C:\telnet 192.168.100.201



```
C:\>telnet 192.168.100.201
```

Figure 10: Using the TELNET command in Windows

5. You will be warned that it might not be safe to send your password. Type **y** and press **Enter** to send it anyway.



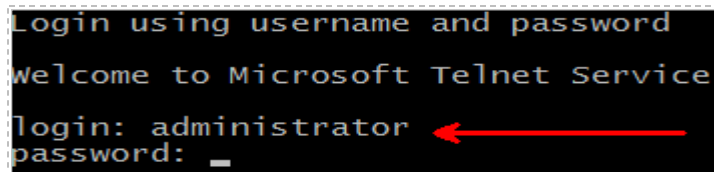
```
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+]'

You are about to send your password information to a remote computer in Internet
zone. This might not be safe. Do you want to send anyway(y/n): y_
```

Figure 11: Warnings about the Danger of Using Telnet

You will be prompted for the username and password. The username will be displayed as you type it, but the password is not displayed for security reasons.

6. For the username, type **administrator** and for the password type **password**.

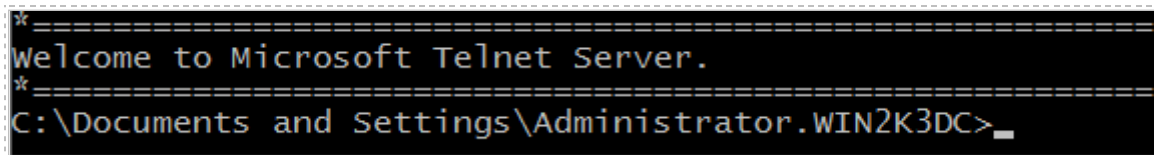


```

Login using username and password
Welcome to Microsoft Telnet Service
login: administrator
password: _
    
```

Figure 12: Inputting the Username and Password of the Remote System

After a successful login, you will receive the message *Welcome to Microsoft Telnet Server*. You will start in the **Documents and Settings Folder** of the user's account.

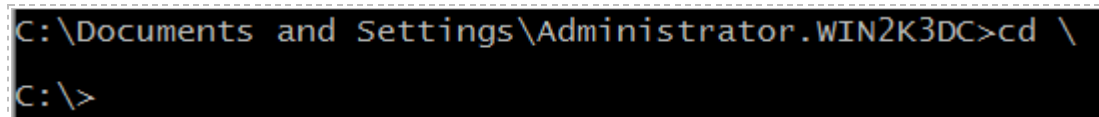


```

Welcome to Microsoft Telnet Server.
C:\Documents and Settings\Administrator.WIN2K3DC>_
    
```

Figure 13: A Successful TELNET connection was made

7. Type the following command to change directories to the root of the C drive:
C:\Documents and Settings\Administrator.WIN2K3DC>cd \

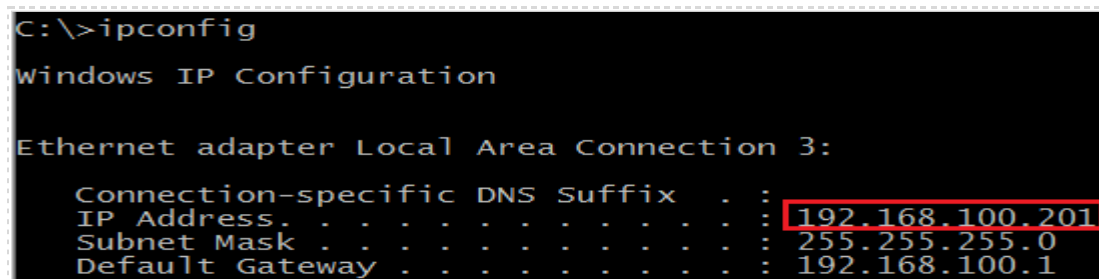


```

C:\Documents and Settings\Administrator.WIN2K3DC>cd \
C:\>
    
```

Figure 14 Changing Directories to the Root of C:

8. Type the following command to view the IP address information of the remote system running Windows Server 2003 you are connected to through TELNET.
C:\>ipconfig



```

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.100.201
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1
    
```

Figure 15: Displaying the IP address of the Remote machine

9. To view the active telnet connection from the Windows 7 Internal Attack Machine to the Windows Server 2k3 Internal Victim Machine in the network connections, type the following:
C:\netstat -an | findstr 23

```
C:\>netstat -an | findstr 23
TCP    0.0.0.0:23          0.0.0.0:0          LISTENING
TCP    192.168.100.201:23  192.168.100.5:1052 ESTABLISHED
UDP    127.0.0.1:123      *: *
UDP    192.168.100.201:123 *: *
```

Figure 16: Viewing the TELNET Network Connection from Windows 7 to Server 2003

The **netstat** data first indicates that the Windows Server 2003 is listening on port 23:

```
TCP 0.0.0.0:23      0.0.0.0:0      LISTENING
```

The second connection indicates a TELNET connection from the Windows 7 Internal Attack Machine with the IP address of 192.168.100.5 to Windows Server 2k3 Internal Victim Machine with IP address 192.168.100.201.

The other two connections displayed are dealing with Network Time Protocol, which uses UDP and port 123. TELNET, on the other hand, uses TCP and port 23.

10. Type the following command to view the files on the root of the C drive. of the remote Windows 2003 Server Internal Victim Machine .

C:\dir

```
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 7834-3125

Directory of C:\

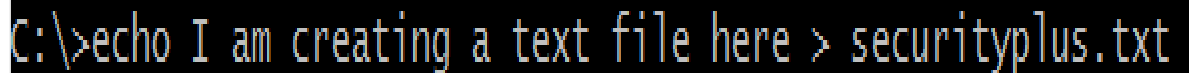
07/03/2008  04:50 PM                0 AUTOEXEC.BAT
07/03/2008  04:50 PM                0 CONFIG.SYS
10/24/2011  01:11 PM             734 DcList.xml
10/24/2011  01:10 PM             702 DNSRecords.txt
11/11/2010  08:21 PM          <DIR> Documents and Settings
03/25/2003  07:00 AM        28,160 DOMAIN-RENAME-README.DOC
10/24/2011  01:10 PM        1,320 Domainlist.xml
03/25/2003  07:00 AM       41,984 GPFIXUP.EXE
07/03/2008  05:06 PM          <DIR> I386
01/18/2010  10:19 AM          <DIR> Inetpub
12/02/2009  01:30 PM          <DIR> Program Files
03/25/2003  07:00 AM       120,320 REMDOM.EXE
07/21/2008  07:55 PM          <DIR> Temp
10/25/2011  11:28 AM          <DIR> WINDOWS
07/03/2008  04:50 PM          <DIR> wmpub
                        8 File(s)      193,220 bytes
                        7 Dir(s)    1,357,406,208 bytes free
```

Figure 17: Displaying the Files on the Remote System

In the next step, we will make a text file on a remote system through the command line. Notepad and WordPad are GUI applications and cannot be utilized in a TELNET session. Using the **edit** command is not a good idea either because there is a good likelihood you will get stuck in the editor. In order to create a text file, we will use the **echo** command along with a redirect (>). This technique can be used in Windows or Linux.

11. Type the following command to create a text file through the command line:

C:\>echo I am creating a text file here > securityplus.txt

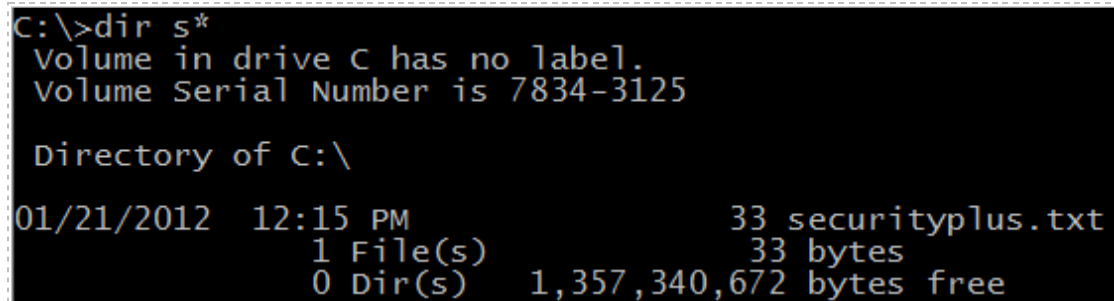


```
C:\>echo I am creating a text file here > securityplus.txt
```

Figure 18: Creating a Text File Using Echo

12. Type the following command to view the newly created file.

C:\>dir s*



```
C:\>dir s*
Volume in drive C has no label.
Volume Serial Number is 7834-3125

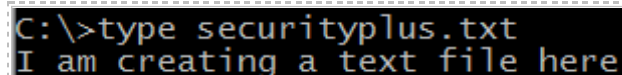
Directory of C:\

01/21/2012  12:15 PM                33 securityplus.txt
               1 File(s)                33 bytes
               0 Dir(s)  1,357,340,672 bytes free
```

Figure 19: Listing the File Created on the Remote System

13. To view what is written inside the file, type the following command:

C:\>type securityplus.txt



```
C:\>type securityplus.txt
I am creating a text file here
```


Figure 20: Displaying the Contents of the Text File on the Remote System

There are attributes you can add to a file from the command line, including:

- Hidden – File is not displayed in a directory listing.
- Read Only – File is readable, but cannot be changed or deleted.
- System – File is used by the operating system.
- Archive –Used for backup purposes.

Attributes can be applied to files by using the **attrib** command. The **attrib** command followed by a plus (+) and the name of the file will add the attribute to the file. The **attrib** command followed by a minus sign (-) and the name of the file will remove the attribute from the file. A directory (**dir**) command along with a forward slash and the symbol representing the attribute will display the files with those attributes.

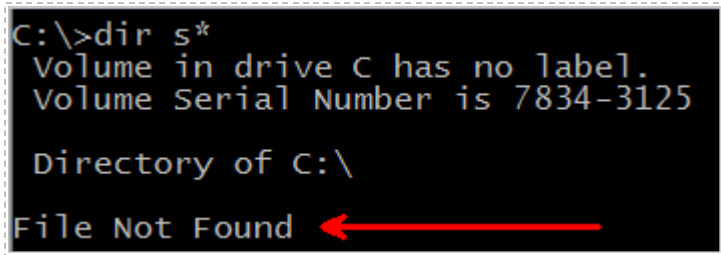
14. To hide the text file, type the following command
C:\attrib +H securityplus.txt



```
C:\>attrib +H securityplus.txt
```

Figure 21: Hiding a File on the Remote System using the attrib Command

15. After applying the attribute, try to view the hidden securityplus.txt file
C:\dir s*



```
C:\>dir s*
Volume in drive C has no label.
Volume Serial Number is 7834-3125

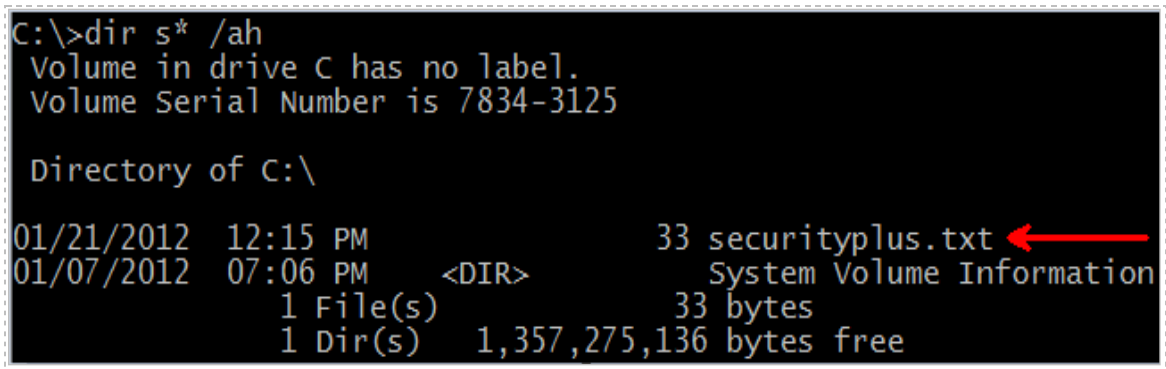
Directory of C:\

File Not Found
```

Figure 22: The Hidden File is not displayed on the Remote System

16. To display the hidden securityplus.txt file, type the following command:
C:\dir s* /ah

Notice the switch used with the dir command. The “/a” switch means look for files with a specific attribute; the “h” specifies the hidden attribute.



```
C:\>dir s* /ah
Volume in drive C has no label.
Volume Serial Number is 7834-3125

Directory of C:\

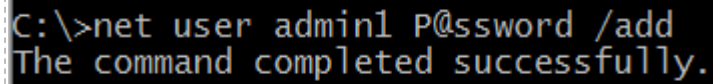
01/21/2012  12:15 PM                33 securityplus.txt
01/07/2012  07:06 PM          <DIR>          System Volume Information
               1 File(s)                33 bytes
               1 Dir(s)  1,357,275,136 bytes free
```

Figure 23: Displaying the Hidden File on the Remote System

Displaying, creating, and hiding files can be done on a remote system using TELNET. An Administrator can also perform other tasks, such as account and service maintenance

17. To create a user on the remote system type the following command:

C:\>net user admin1 P@ssword /add



```
C:\>net user admin1 P@ssword /add
The command completed successfully.
```

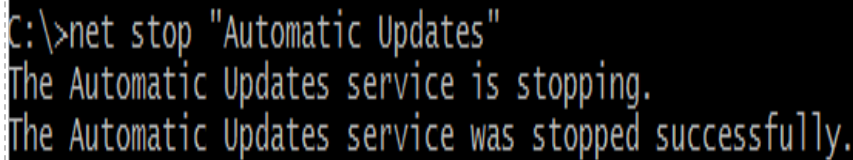
Figure 24: Adding a User through the Command Line

Be aware that only administrative accounts have the capability to add users.

You should receive the message that *the command completed successfully*. The user created will have an account named **admin1** and a password of **P@ssw0rd**. The administrator logged into the system remotely through the command line can also view, stop, and start services by using the **net start** and **net stop** commands. One service that should not be stopped is the TELNET service or the connection will die.

18. To stop the **Automatic Updates** service on the remote machine, type:

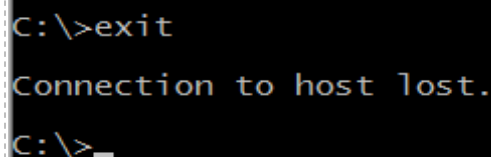
C:\>net stop "Automatic Updates"



```
C:\>net stop "Automatic Updates"
The Automatic Updates service is stopping.
The Automatic Updates service was stopped successfully.
```

Figure 25: Stopping the Automatic Updates Service

19. Type **exit** to leave the command prompt session on the remote machine.



```
C:\>exit
Connection to host lost.
C:\>
```

Figure 26: Leaving the TELNET session

20. To be sure that your TELNET session to the Windows Server is disconnected, type **ipconfig** and the IP address of the Windows 7 Internal Attack Machine should be displayed again.

C:\ipconfig

```
C:\>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 27: The IP address Information of the Windows 7 Machine

1.2 Conclusion

A network administrator can use TELNET to remotely connect to a computer to run commands. A TELNET connection can be used to display and create files on the remote system, as well as perform other administrative tasks, like maintenance of accounts and services. TELNET uses TCP port 23 and sends information over the network in clear text.

1.3 Discussion Questions

1. What command can be used to show an active TELNET connection?
2. What is the command that can be used to display files on a remote system when an administrator is connected via a TELNET session?
3. How can you create a file on a remote system during a TELNET session?
4. What command can be used to determine if a remote system is running TELNET?

2 Connecting to a Linux System through the Command Line

Most people would agree with the fact that since its inception, Linux has always been an operating system that took security seriously. Most distributions of Linux come with a built in SSH server as well as an SSH client that will allow you to connect to servers running SSH. The SSH, or secure shell, protocol, use Transmission Control Protocol port 22. Unlike TELNET, everything sent over the wire using SSH is encrypted.

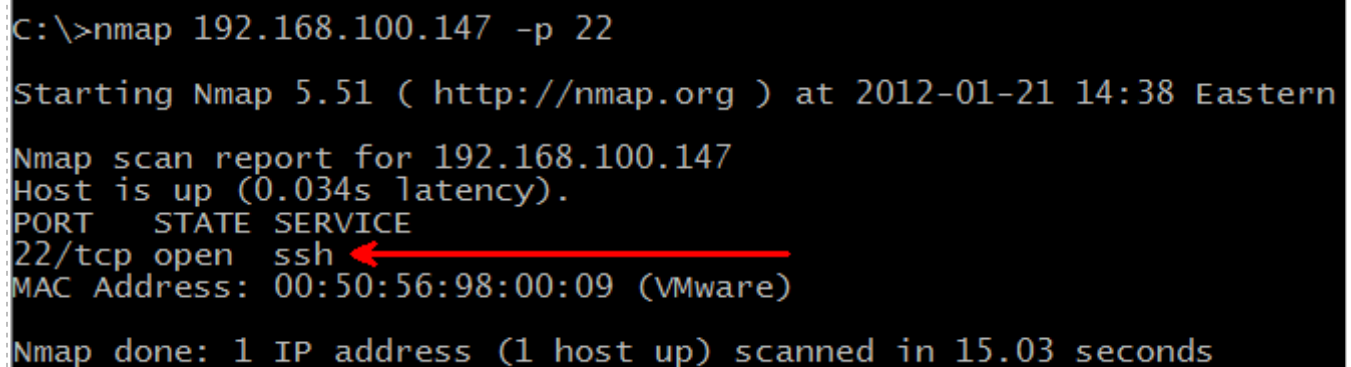
2.1 Using SSH to Connect to a Remote Linux System

Warning - This must be done before starting Task 2:

The Red Hat Linux Internal Victim Machine needs to be logged into using the **root** username with the password: **password** (the password will not be displayed for security reasons). Once you have logged in, issue the command **startx** to start the GUI (Graphical User Interface). See Lab Settings, section 0 for details. **Until this procedure has been performed, Task 2 cannot be started.**

1. From a command prompt on the Windows 7 Internal Attack Machine, type the following to determine if port 22 is open on the remote Linux system:

C:\>nmap 192.168.100.147 -p 22



```
C:\>nmap 192.168.100.147 -p 22
Starting Nmap 5.51 ( http://nmap.org ) at 2012-01-21 14:38 Eastern
Nmap scan report for 192.168.100.147
Host is up (0.034s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:50:56:98:00:09 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 15.03 seconds
```

Figure 28: Determining if SSH Port 22 is Open on the Remote Machine

Microsoft Windows does not have a Secure Shell (SSH) client built into the operating system. However, third-party SSH client and server applications can be used to make SSH connections to other systems or to allow incoming SSH connections. PuTTY is a third-party application that will allow you to connect to a remote system running SSH.

2. Double-click on putty.exe to launch the third-party SSH client application.

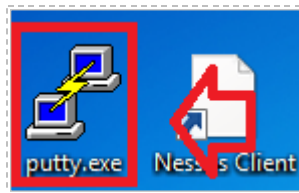


Figure 29: Launching putty.exe on the Windows 7 Machine

The PuTTY Configuration will open. Users can choose the following connection types:

- Raw
- Telnet
- Rlogin
- SSH (the default)
- Serial

PuTTY makes a great choice for Windows Vista and Windows 7 users who need to connect to remote devices because Windows no longer comes with HyperTerminal.

3. In the Host Name (or IP address) box, type IP **192.168.100.147** and click **Open**.

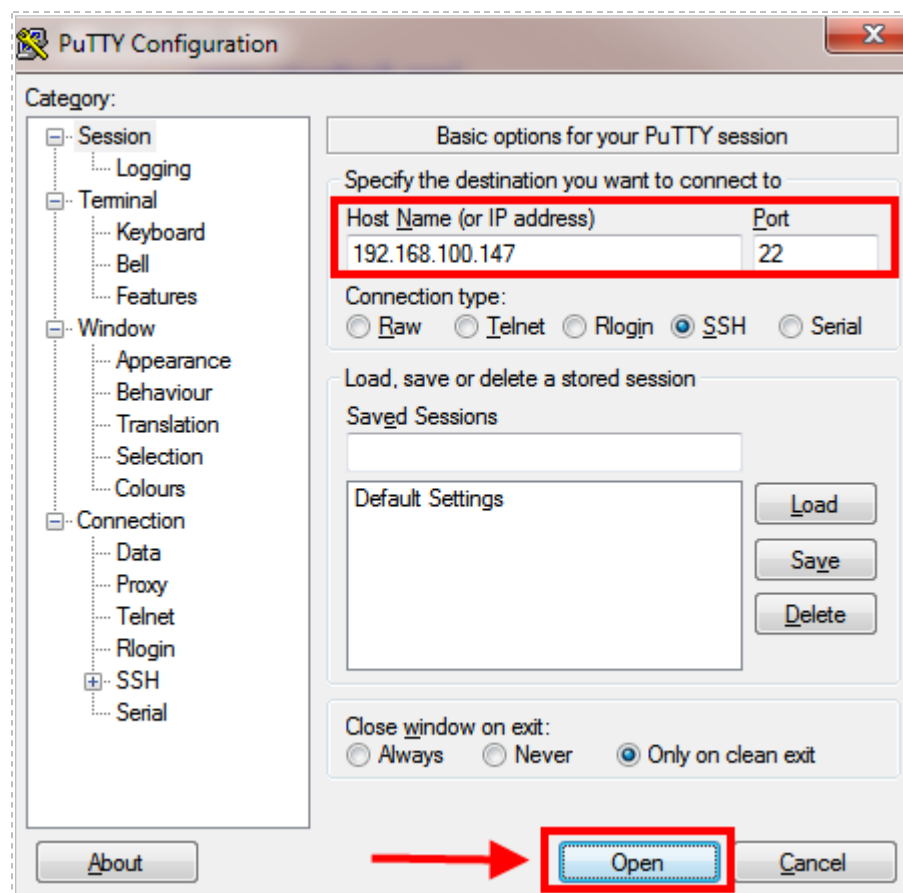


Figure 30: PuTTY Configuration Dialog Box

4. A PuTTY Security Alert Dialog will pop up. Click **Yes** to the Warning.

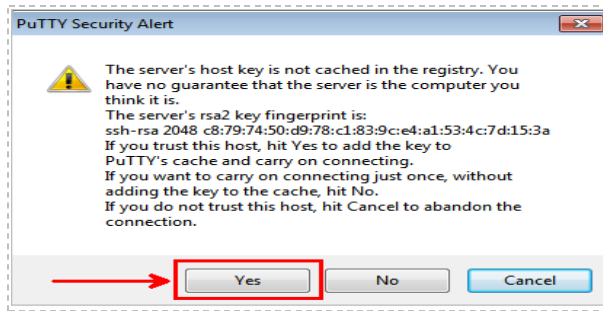


Figure 31: Security Alert Dialog

5. When you receive the login prompt, type **root**. The password is **password**. Note: the password will not appear when you type it for security reasons.

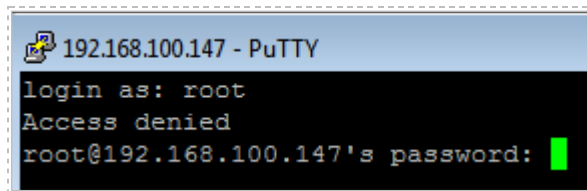


Figure 32: Logging in to the Remote Machine via SSH

After a successful login, you will receive a *Last Login* message and a prompt.

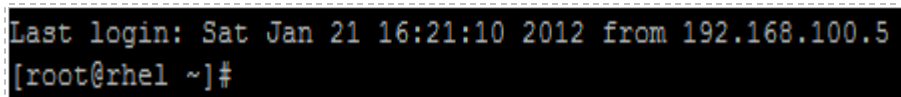


Figure 33: A Successful Login to the SSH Server Displays the Last Login Time

6. Checking the IP address of the machine you are connecting to remotely is never a bad idea. To display IP address information in Linux, type the following:
[root@rhel ~]#**ifconfig**

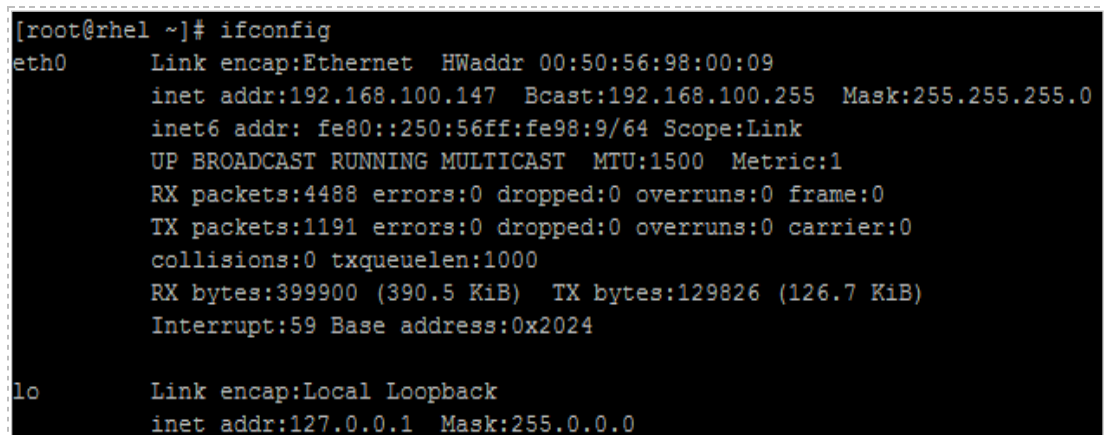
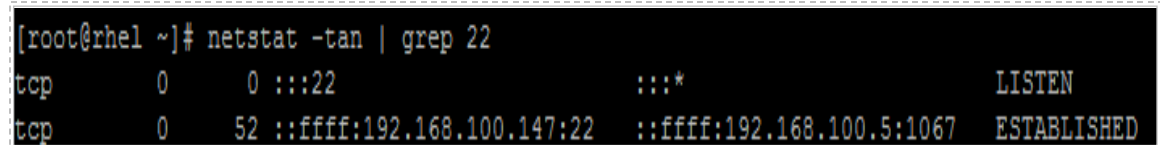


Figure 34: Displaying the IP address of the Remote Linux Machine

The first IP address shown is for the first NIC in the system. The second is the loopback address.

7. To view the TCP secure shell (SSH) connection between the Windows 7 Internal Attack Machine and the Red Hat Linux Internal Victim Machine, type the following command:

```
[root@rhel ~]# netstat -tan | grep 22
```



```
[root@rhel ~]# netstat -tan | grep 22
tcp        0      0 :::22                :::*                  LISTEN
tcp        0  52 :::ffff:192.168.100.147:22 :::ffff:192.168.100.5:1067 ESTABLISHED
```

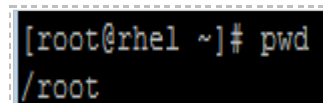
Figure 35: Viewing the Established SSH connection

The **netstat** command, which works in Windows and Linux, displays active network connections. By using the **-tan** switch, you will only display TCP connections. You can narrow down the output by piping (|) the command into **grep**, Global Regular Expressions Print, and using port 22. The first line of the **netstat** output tells you that the Linux Machine is listening on port 22. The second line of the **netstat** output shows the established connection between the Windows 7 Internal Attack Machine with the IP address of 192.168.100.5 and the Red Hat Linux Internal Victim Machine with the IP address of 192.168.100.147.

To find out what directory you reside in on the Linux file system, type **pwd**. The command **pwd** is short for both *print working directory* and *present working directory*. The tilde (~) symbol tells you the current user is in their home directory.

8. To view your current location on the file system in Linux, type:

```
[root@rhel ~]# pwd
```

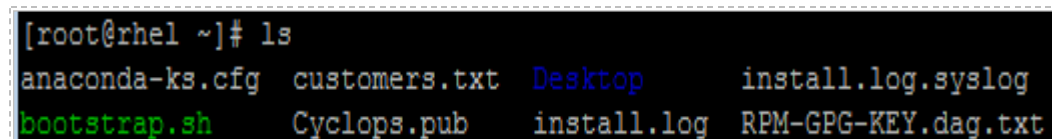


```
[root@rhel ~]# pwd
/root
```

Figure 36: Printing the Present Working Directory

9. List files in the root's home directory by typing the following:

```
[root@rhel ~]# ls
```

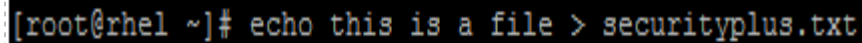


```
[root@rhel ~]# ls
anaconda-ks.cfg  customers.txt  Desktop      install.log.syslog
bootstrap.sh     Cyclops.pub   install.log  RPM-GPG-KEY.dag.txt
```

Figure 37: Using the ls command in Linux to View Files and Folders

The **ls** command usually display files as different colors than folders. Also, files with executable permissions are typically displayed using a green font color. Another common practice is to have folders start with a capital letter, although this is not a requirement.

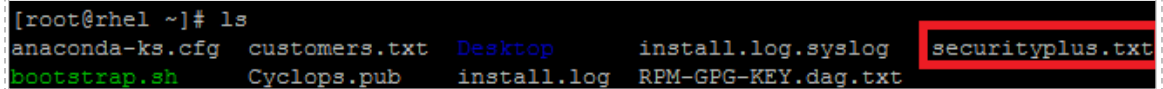
10. Creating a file in Linux can be done by using the **VI Editor** or by using the **echo** command and a redirect symbol (>), like in Microsoft Windows. To make a file called **securityplus.txt** with the phrase *"this is a file"* in it, type the following:
[root@rhel ~]# **echo this is a file > securityplus.txt**



```
[root@rhel ~]# echo this is a file > securityplus.txt
```

Figure 38: Creating a File in Linux

11. Type **ls** to view the created securityplus.txt file within root's home directory.
[root@rhel ~]# **ls**

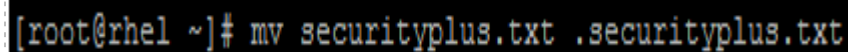


```
[root@rhel ~]# ls
anaconda-ks.cfg  customers.txt  Desktop      install.log.syslog  securityplus.txt
bootstrap.sh     Cyclops.pub   install.log  RPM-GPG-KEY.dag.txt
```

Figure 39: Displaying Files with the ls Command

In Linux, the **mv** (move) command is used to rename a file. By placing a period (.) at the beginning of a file name, that file will be hidden. This is the equivalent to using the **attrib** command to add the hidden attribute to a file in Windows.

12. To hide the file, rename it using the **mv** command and put a period in the front.
[root@rhel ~]# **mv securityplus.txt .securityplus.txt**

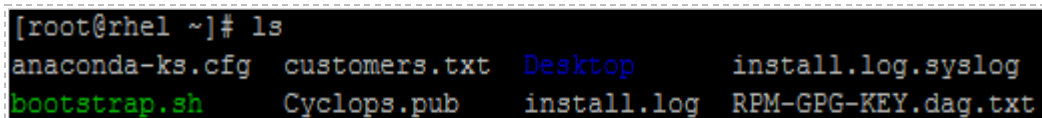


```
[root@rhel ~]# mv securityplus.txt .securityplus.txt
```

Figure 40: Renaming and Hiding a File

The file is now hidden and will not be displayed when **ls** is used without any switches.

13. Type **ls** to see that the securityplus.txt file is no longer displayed.
[root@rhel ~]# **ls**



```
[root@rhel ~]# ls
anaconda-ks.cfg  customers.txt  Desktop      install.log.syslog
bootstrap.sh     Cyclops.pub   install.log  RPM-GPG-KEY.dag.txt
```

Figure 41: The Hidden File is not Displayed with ls

14. To view hidden files within the root's home directory, type the following:

```
[root@rhel ~]#ls -a
```



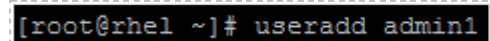
```
[root@rhel ~]# ls -a
.                  .config           .gnome2           .nautilus         .serverauth.3738
..                .cshrc            .gnome2_private   .recently-used.xbel .serverauth.6047
anaconda-ks.cfg   customers.txt      .gstreamer-0.10   .redhat           .serverauth.6774
.bash_history     Cyclops.pub       .gtkrc-1.2-gnome2 RPM-GPG-KEY.dag.txt .ssh
.bash_logout      Desktop           .ICEauthority     .securityplus.txt  .tcshrc
.bash_profile     .dmrc             install.log        .serverauth.2934   .thumbnails
.bash_profile~    .eggcup           install.log.syslog .serverauth.3147   .Trash
.bash_profile.old .esd_auth         .lessht           .serverauth.3607   .Xauthority
.bash_profile.old~.gconf            .metacity         .serverauth.3639
.bashrc           .gconfd          .mozilla          .serverauth.3697
bootstrap.sh      .gnome            .mysql_history    .serverauth.3712
```

Figure 42: Displaying Hidden Files in Linux

Displaying, creating, and hiding files can be done on a remote system using SSH. The root account can also perform other tasks, such as account and service maintenance

15. To add a user to the Red Hat Linux Internal Victim Machine, type the following:

```
[root@rhel ~]#useradd admin1
```



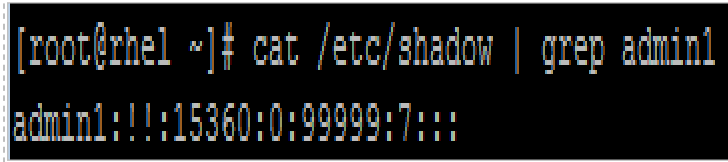
```
[root@rhel ~]# useradd admin1
```

Figure 43: Adding a User to the Remote Linux System

The **passwd** and **shadow** files in the **/etc** directory store the names of the users. The **shadow** file also stores the user's password hash. Linux users can use the **cat** command, which stands for concatenate, to display the contents of a file like the shadow file.

Some files can contain pages of information. To narrow the display results, the **grep** command can be used. GREP, which stands for Global Regular Expressions Print, can be used to search for a character or a string of characters within a given output set.

16. To view the admin1 user created within the shadow file, type the following:
[root@rhel ~]#cat /etc/shadow | grep admin1

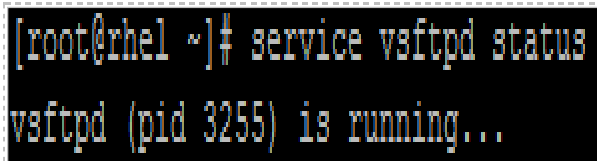


```
[root@rhel ~]# cat /etc/shadow | grep admin1
admin1:!!:15360:0:99999:7:::
```

Figure 44: Using GREP to Filter Search Results

The service command can be used to stop, start, and view server status.

17. To view the status of the **Very Secure FTP Daemon9** (vsftpd), type the following:
[root@rhel ~]#service vsftpd status



```
[root@rhel ~]# service vsftpd status
vsftpd (pid 3255) is running...
```

Figure 45: Viewing the Status of the vsftpd Service

18. To stop the **vsftpd** service on the remote Linux system, type the following:
[root@rhel ~]#service vsftpd stop



```
[root@rhel ~]# service vsftpd stop
Shutting down vsftpd: [ OK ]
```

Figure 46: Shutting Down the vsftpd service

19. To end the SSH session on the remote Linux system, type the following:
[root@rhel ~]#exit



```
[root@rhel ~]# exit
```

Figure 47: Typing Exit to Leave the SSH Session

The PuTTY Window will close and the SSH session will be terminated.

2.2 Conclusion

Secure Shell, or SSH, allows users to remotely connect and administer computers running the Linux, Unix, and Mac operating systems as well other network devices such as routers and switches. Secure Shell encrypts the traffic, unlike TELNET, so the usernames, passwords, and commands will not be visible to anyone inspecting network traffic. It is strongly recommended that SSH be used instead of TELNET when possible.

2.3 Discussion Questions

1. What port does Secure Shell use?
2. Is there a native SSH client or server on Microsoft Windows system?
3. What is the file in Linux that contains the password hash?
4. What are two methods that can be used for creating a file during a remote secure shell (SSH) connection within Linux?

3 Analyzing Remote Connections in Network Traffic

In this section, you will analyze a preexisting network capture file with TELNET and SSH traffic. You will be able to view the clear text communication during the TELNET session, but you will be unable to view the encrypted communication of the SSH connection.

3.1 Using Wireshark to Analyze Connections to a Remote Linux System

Wireshark is a protocol analyzer, which will allow you to inspect and capture network traffic. The 32-bit and 64-bit versions can be downloaded from www.wireshark.org.

Open a Terminal to Get Started

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. Type **wireshark** (all lowercase) to bring up the Wireshark program.

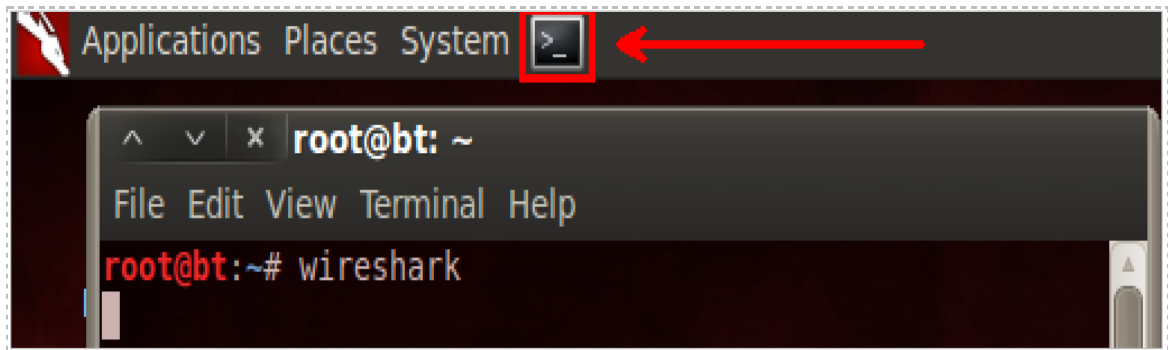


Figure 48: The Terminal Windows within BackTrack

2. If you receive a message about running Wireshark as root can be dangerous, click the button that says **Don't show this message again**, and click **OK**.

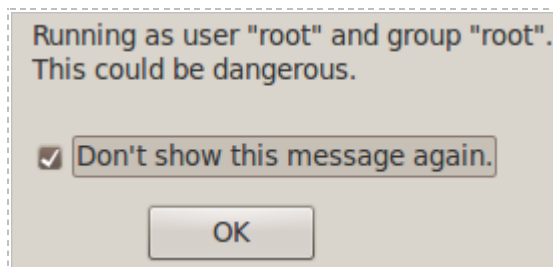


Figure 49: Allow Wireshark to run as root

3. Select **file** from the Wireshark menu and select **open**. Double click on the **root** folder then double click on the **lab4** folder. Double click on the file **telnetssh.pcap**

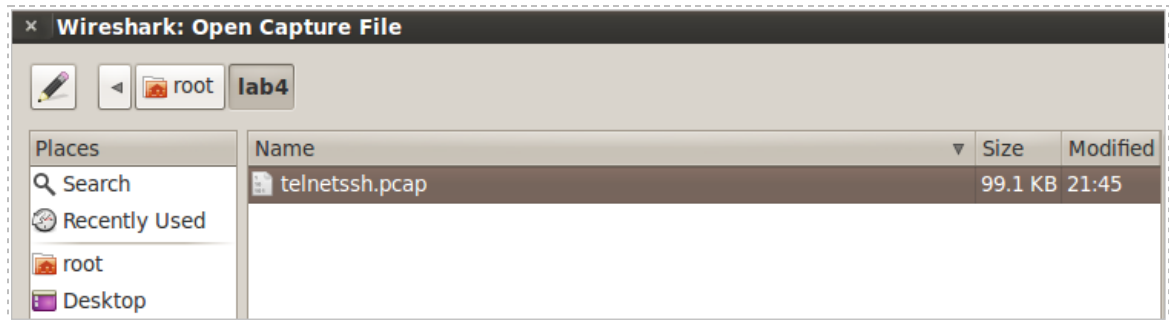


Figure 50: Opening the Wireshark file

Examining TELNET traffic can be done by using either of the two filters within Wireshark:

- telnet
- tcp.port == 23

If TELNET is used on a Windows system, the following filter can be used (case sensitive):

- frame contains Microsoft Windows

Examining SSH traffic can be done by using either of the two filters within Wireshark:

- ssh
- tcp.port == 22

4. To examine the TELNET traffic, type **telnet** in the filter pane and click **Apply**.

 The image shows the Wireshark packet list pane with the filter 'telnet' applied. The table displays four packets, all of which are TELNET. The 'Protocol' column for each packet is highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length	Info
21	15.360096	192.168.100.201	192.168.100.5	TELNET	75	Telnet Data
22	15.360905	192.168.100.5	192.168.100.201	TELNET	57	Telnet Data
23	15.361917	192.168.100.201	192.168.100.5	TELNET	62	Telnet Data
24	15.362220	192.168.100.5	192.168.100.201	TELNET	81	Telnet Data

Figure 51: The telnet Filter in the Wireshark Pane

5. Right click on the first frame in the list and select **Follow TCP Stream**.

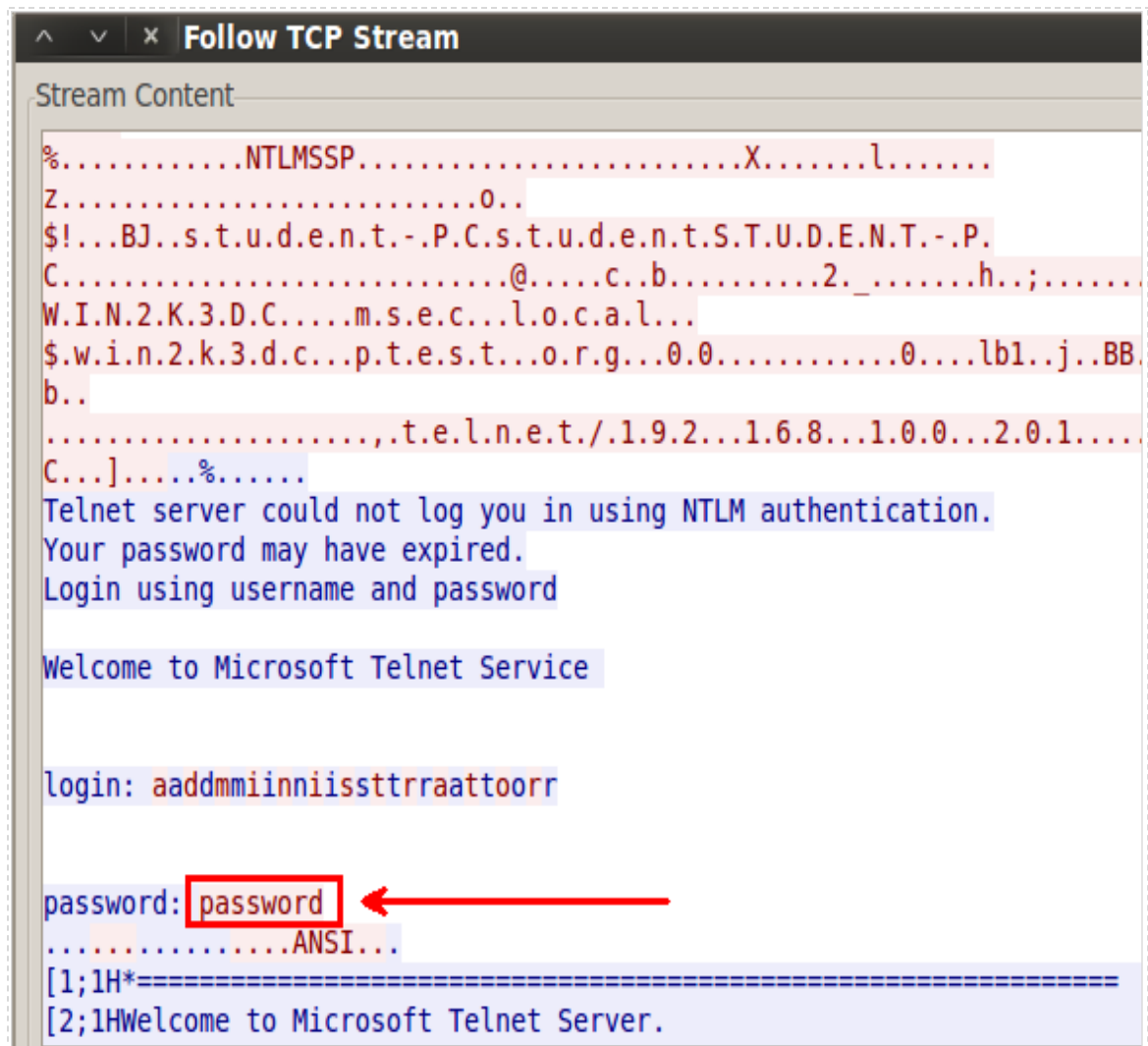


Figure 52: Following a TCP Stream

You can scroll down through the conversation to try to interpret what was happening. Notice how you can view the traffic because TELNET transmits in clear text. Both sides of the conversation between the TELNET server and client are displayed. To see a specific side of the conversation, click the arrow to the right of Entire conversation.

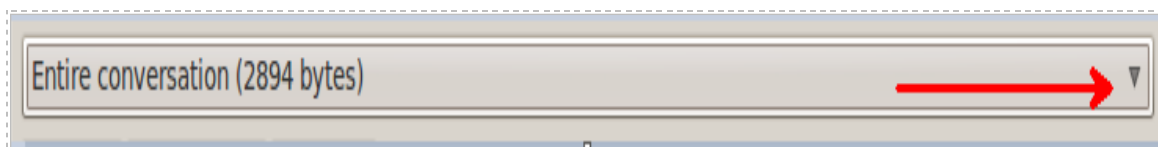


Figure 53: The telnet Filter in the Wireshark Pane

6. Select the conversation from the client with the IP address of 192.168.100.5 to the telnet server with the IP address of 192.168.100.201 by clicking the arrow to the right of **Entire conversation**, and selecting the first conversation in the drop box.

In the figure below, you may notice the dots (.) included in the net user and net stop commands. This occurs if the user entered a command incorrectly and pressed the backspace key to correct their mistake.

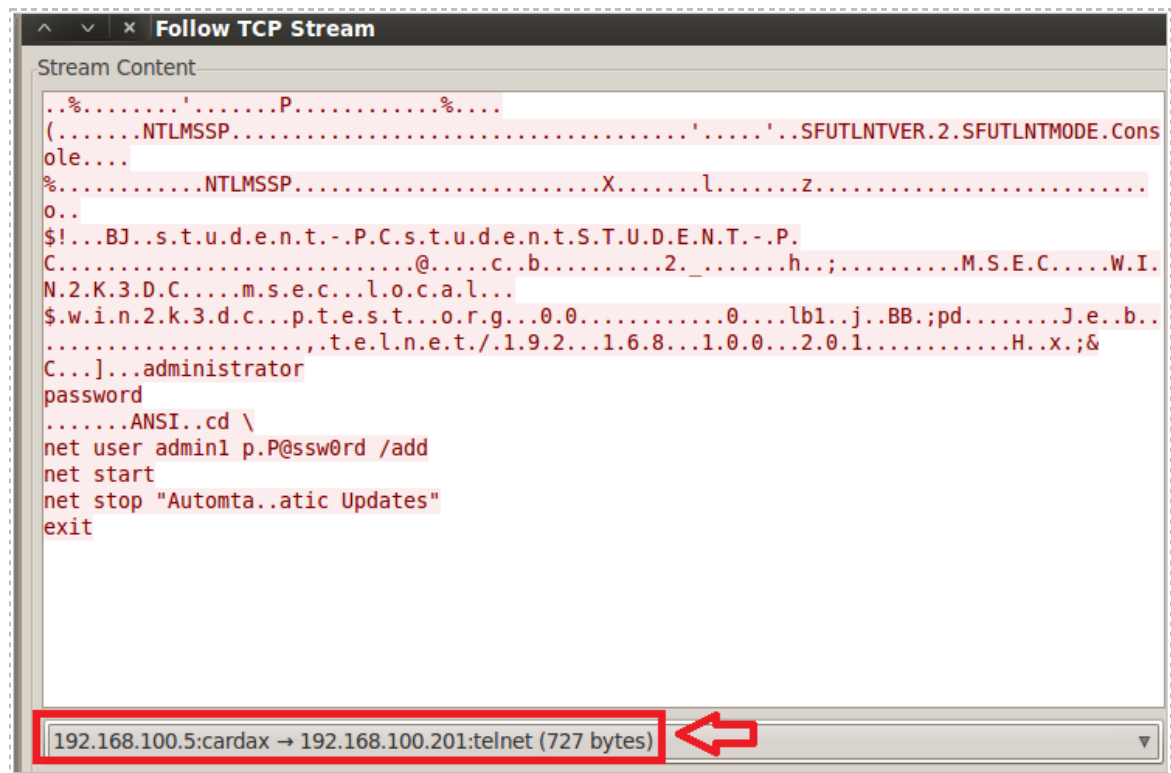


Figure 54: The Commands Sent to the TELNET Server

The client sent the username of *administrator* and password of *password* to the TELNET server. The client sent the command to add a user called *admin1* with the password of *P@ssw0rd*. The client also sent a net start command to the server to list the services, and then stopped the Automatic Updates service. The session terminated with the command exit. Viewing the details of this conversation illustrates why the use of TELNET should not be avoided. When SSH traffic is examined, it will be unreadable.

7. Click the **Close** button in the bottom right of Wireshark to close the TCP stream.

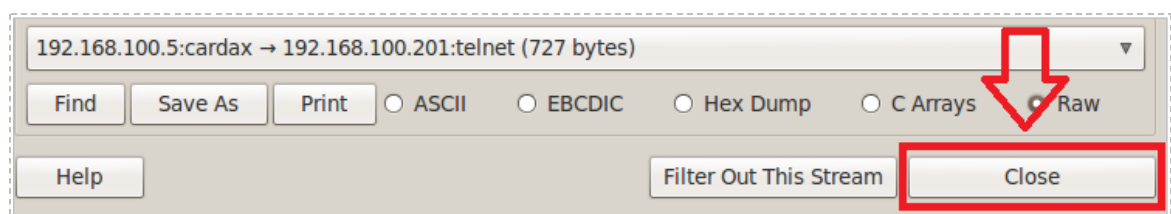


Figure 55: Closing the TCP Stream

- In the Wireshark filter Pane, clear the previous entry then type **ssh** and click the **Apply** button.

No.	Time	Source	Destination	Protocol	Length	Info
33	16.088370	192.168.100.147	192.168.100.5	SSHv2	74	Server Protocol: SSH-2.0-OpenSSH_4.3
34	16.253878	192.168.100.5	192.168.100.147	SSHv2	82	Client Protocol: SSH-2.0-PuTTY_Release_0.61
36	16.256152	192.168.100.147	192.168.100.5	SSHv2	758	Server: Key Exchange Init
38	16.261416	192.168.100.5	192.168.100.147	SSHv2	182	Client: Key Exchange Init
40	16.264334	192.168.100.5	192.168.100.147	SSHv2	70	Client: Diffie-Hellman Key Exchange Init
41	16.267060	192.168.100.147	192.168.100.5	SSHv2	334	Server: Diffie-Hellman Key Exchange Reply

Figure 56: Viewing SSH Traffic

- Right click on the first frame in the list and select *Follow TCP Stream*.

Stream Content

```
SSH-2.0-OpenSSH_4.3
SSH-2.0-PuTTY_Release_0.61
.....l.....jM.=....Ydiffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-
sha1...ssh-rsa,ssh-dss...aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-
cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr...aes128-cbc,3des-cbc,blowfish-
cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-
ctr,aes256-ctr...Uhmact5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96...Uhmact5,
hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-
md5-96...none,zlib@openssh.com...none,zlib@openssh.com.....|....l5$3<....0.....diffie-
hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-
sha1,rsa2048-sha256,rsa1024-sha1...ssh-rsa,ssh-dss...aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-
ctr,aes192-cbc,aes128-ctr,aes128-cbc,blowfish-ctr,blowfish-cbc,3des-ctr,3des-cbc,arcfour256,arcfour128...aes256-
ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,blowfish-ctr,blowfish-
cbc,3des-ctr,3des-cbc,arcfour256,arcfour128...hmac-sha1,hmac-sha1-96,hmac-md5...hmac-sha1,hmac-sha1-96,hmac-
md5...none,zlib...none,zlib.....-..U.....X.....M...2..Q.....S.....C...Tao.S
h...X.....1@
A>..[...HIs.SH5.....D(Zg
..>.[^..0; .....lH.V.....<..l...X.....jB.....t?MN(..ie%.N....7..ij,...T...t...../.G..".'.G.+T~.t.+I4.Fq
+..~..,Z!
[:.....q..w..G.<.....~sR....6.k.-})...^F )...k.....i.....d..S....8..C.xVF...o{
.....!.....%:.I..|.0.4a.w2xd.=..#.M..3.pk.....a...B..la>k.....3IY..Y..r.....^a.....0.)}{..F.D...9.
[=5@.#.c.^..j...s.....8..;i@p.+.]...g.h9..m..8.M.=.5....\{mk.....}j.....am+!.|.....|..XS9T.v?.G..H.Y
{.7.H..3..&...<.!.....ssh-rsa...#.....+.....nX.....Q\...4XIsn.pl..#
].YWKY0.0..).a.9.R..h..l...0.....q.Cs..B.S...rY.h..Lb.....S.....k...:M.TY...>.#.2-...
[.I.kS.;...%R...}.l.0...>.0>.A.Qh...L.....e.[0..^..6M.a..61!g..F..L..l..(3.....[G..s...ZPV<
.t.....R.(...I.....^1.: "0=.....H.j...J....4...(.
.$Q.G7V.x0.A...Dt'.....-..CZ.....U.V./tr .#.z.#G.u,..g.e|.....P.*9..)/..U5b=:.....]...X
```

Figure 57: Viewing the Encrypted SSH Communication

Although you are able to see the names of ciphers used for encrypting the SSH session, you will not be able to see any of the communication between the client and server. Click the **Close** Button in the bottom right of Wireshark to close the TCP stream.

- Close all open windows and terminals.

3.2 Conclusion

TELNET uses TCP port 23 and sends everything over the network in clear text. When examining TELNET traffic, you are able to see usernames, passwords, and commands. Secure Shell (SSH) uses TCP port 22 and provides a secure channel for remote administration tasks. Examining SSH traffic provides you with no details of what occurred during the session between the SSH client and the SSH server.

3.3 Discussion Questions

1. Type **frame contains PuTTY** in the Wireshark filter pane and click Apply. Determine which version of PuTTY is in use.
2. If you type **frame contains shadow** in the Wireshark filter pane, why are there no results that show the root account viewed the shadow file remotely?

Type **frame contains "Microsoft"** in the Wireshark filter pane and click Apply. Right click on the first frame and select *Follow TCP Stream* to answer Questions 3 and 4.

3. Name a user account that was displayed in the clear text traffic.
4. Name the file that was created, and then hidden.

References

1. SSH MAN Page:
<http://linux.die.net/man/1/ssh>
2. Wireshark:
www.wireshark.org/
3. PuTTY home Page:
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
4. BackTrack Linux:
<http://www.backtrack-linux.org/>
5. Telnet Commands for Windows:
<http://technet.microsoft.com/en-us/library/c.aspx>