



CompTIA Security+® Lab Series

Lab 3: Protocols and Default Network Ports - Transferring Data Using TCP/IP

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 Using Hyper Text Transfer Protocol (HTTP) to Transfer Files	8
1.1 Transferring Files with HTTP	8
1.2 Conclusion	15
1.3 Discussion Questions.....	15
2 Using File Transfer Protocol (FTP) to Transfer Files	16
2.1 Using FTP	16
2.2 Conclusion	23
2.3 Discussion Questions.....	23
3 Transferring Files Securely Using SCP	24
3.1 Using SCP	24
3.2 Conclusion	26
3.3 Discussion Questions.....	26
References	27

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 transfer files using the FTP, HTTP, and SCP protocols. Protocols like HTTP, FTP, and SCP can be used to transfer files from one computer to another. File transfers are unencrypted by default when the FTP or HTTP protocols are used. File transfers will be encrypted if SCP is used. In this lab, the student will have the opportunity to configure servers and utilize file transfer client utilities.

This lab includes the following tasks:

- 1 - Using Hyper Text Transfer Protocol (HTTP) to transfer files
- 2 - Using File Transfer Protocol (FTP) to transfer files
- 3 - Transferring Files Securely Using SCP

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

It is important to know how files can be uploaded, downloaded, and securely transferred using protocols within the TCP/IP suite. Windows, Linux, UNIX, and the Mac OS X operating systems can be used as HTTP, FTP, and SSH servers. Some of the operating systems have the ability to run these servers without needing any third party applications. Windows comes with FTP and HTTP clients, while Linux, UNIX, and Mac OS come with clients for HTTP, FTP, and SCP. The third party application **pscp.exe** can be used on the Windows operating systems to perform secure file copies.

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

FTP – File Transfer Protocol, or FTP, can be used to transfer files from one computer to another. The FTP protocol uses the Transmission Control Protocol (TCP) and two ports, 20 and 21. Port 21 is used for the commands and port 20 is used for the data transfer. Credential and files that are transferred using FTP are sent in clear text.

HTTP – Hyper Text Transfer Protocol, or HTTP, can be used to download files. The HTTP protocol uses the Transmission Control Protocol (TCP) and port 80. HTTP clients include browsers and wget.exe. Web Server software includes Microsoft's Internet Information Services (IIS) and Apache.

SCP – The Secure Copy Protocol, or SCP, can be used encrypt file transmissions. In order to use the SCP protocol the destination server must be running the SSH protocol. The SSH protocol uses the Transmission Control Protocol (TCP) and port 22. Credential and files that are transferred using SCP are encrypted.

IIS – Microsoft's Internet Information Services, or IIS, is available on their server and some of their professional client operating systems. The administrator can configure various servers within IIS, such as FTP and HTTP servers. When IIS was first introduced, there were many vulnerabilities. However, Microsoft has improved the security of IIS over the years.

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

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

Wget - A program that provides non-interactive download of files from the Web. Wget supports HTTP, HTTPS, and FTP protocols. Wget can work in the background, while the user is not logged on.

Pod Topology

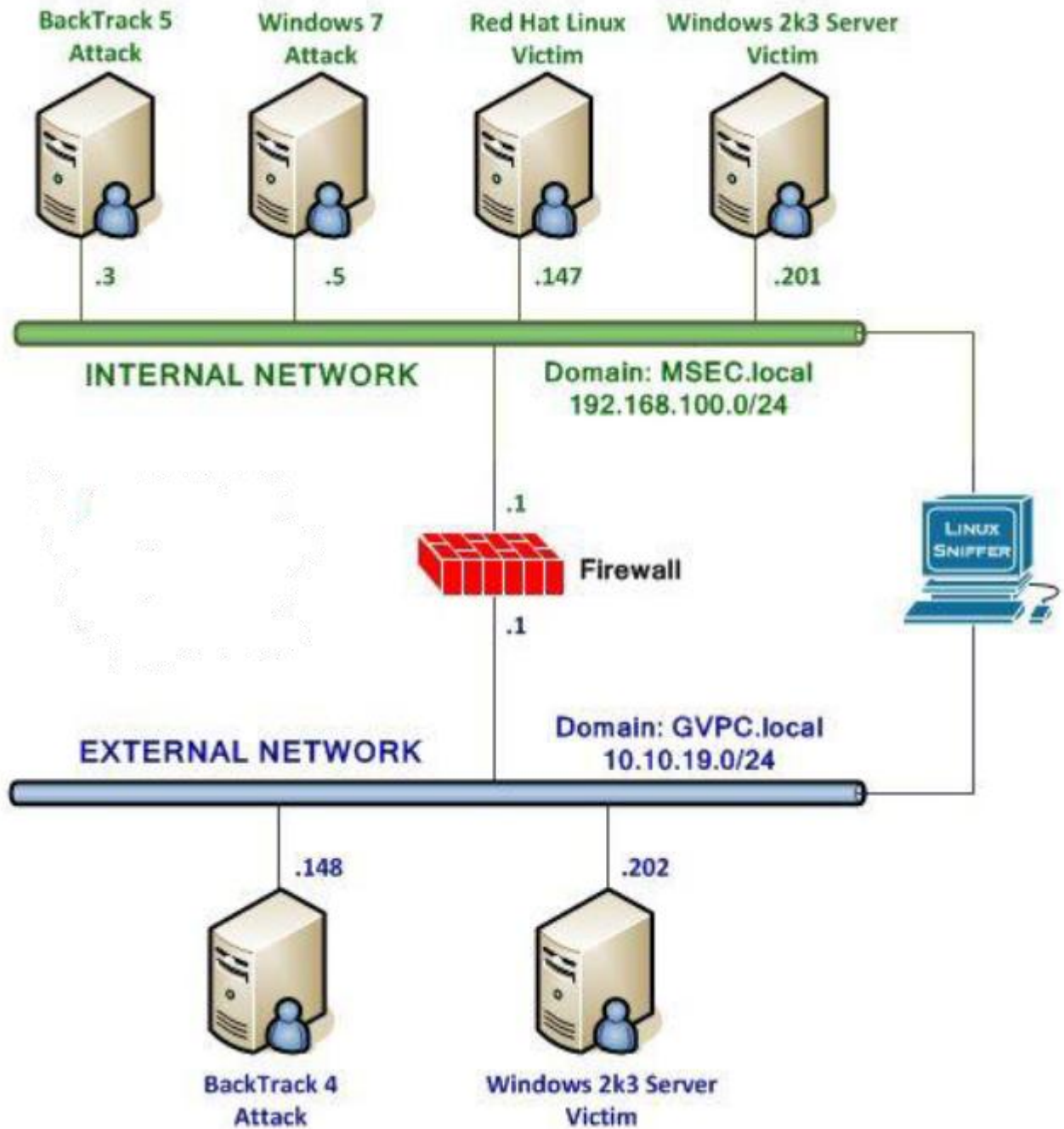


Figure 1: Topology

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
Red Hat Linux Enterprise Internal Victim Machine	192.168.100.147
Red Hat Linux Enterprise root password	password
Windows 2k3 Server Internal Victim Machine	192.168.100.201
Windows 2k3 Server administrator 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 and press **Enter**.
3. Type **password** at the Password: prompt and press **Enter**.

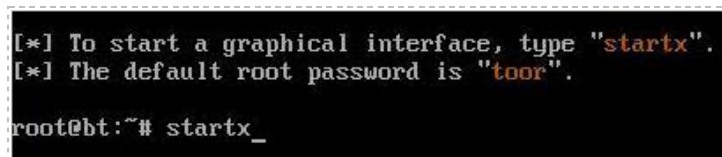
For security purposes, the password will not be displayed.



```
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 and press **Enter**.



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

Figure 3: BackTrack 5 GUI start up

Red Hat Linux Enterprise Internal Victim Login:

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

For security purposes, the password will not be displayed.

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

```
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 4: RHEL login

Windows 2k3 Server Internal Victim Server 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 5: Windows 2k3 login

1 Using Hyper Text Transfer Protocol (HTTP) to Transfer Files

Most people are familiar with the process of how to download a file from a web server. However, people who don't do network administration might not know how to configure a HTTP server. In this exercise, you will configure an Apache server on a Linux machine so that a client can download files to their machine. 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.

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

1.1 Transferring Files with HTTP

Start the Apache Server on the Attack Machine

1. Open a terminal on the in BackTrack 5 Internal Attack system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen. Start the Apache server by typing the following command at the terminal:
`root@bt:~#apache2ctl start`

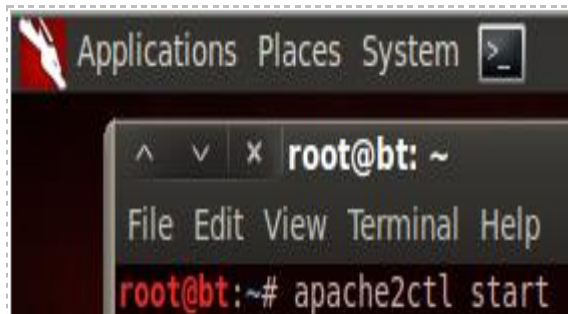


Figure 6: Starting Apache

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

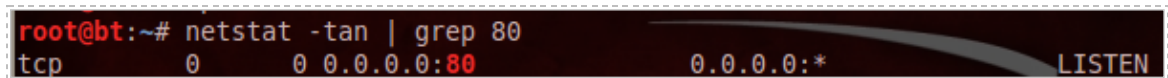


Figure 7: Verifying that the Apache Web Server is Running

To test that the web server is functioning with a valid home page, you can attempt to connect to it from the Windows 2k3 Server Machine by connecting to it from your browser.

3. Log on to the **Windows 2k3 Server Internal Victim Machine**. 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). Log on with the username of **Administrator** and the password of **password**.

If you are already logged into the machine, you may skip this step.



Figure 8: Logging on to Windows 2k3

2. On the Windows 2k3 Internal Victim Machine, open Internet Explorer , by clicking on the shortcut to Internet Explorer in the Quick Launch toolbar, and type the following URL: <http://192.168.100.3> - You should see the message, *It works!*, on the webpage.

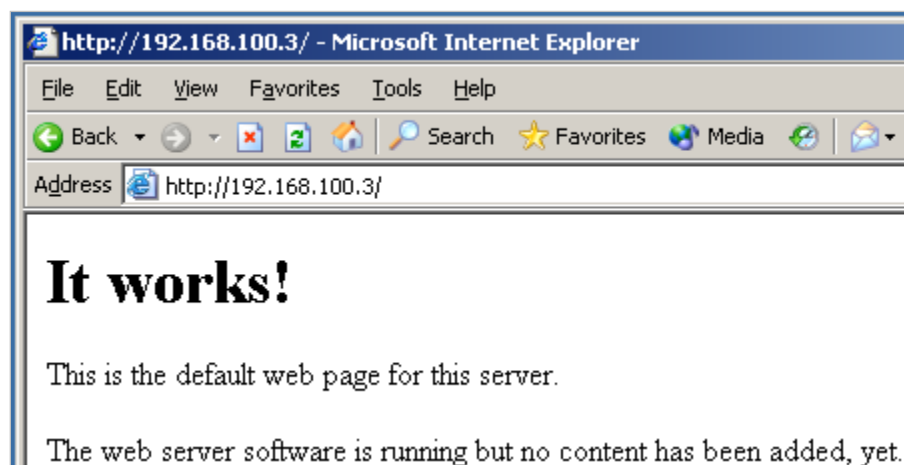


Figure 9: Viewing the Default Web Page

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

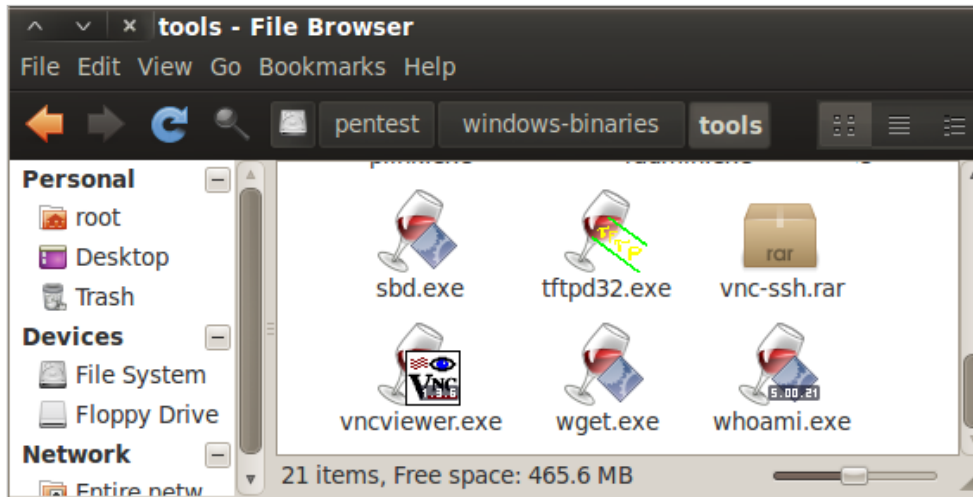


Figure 10: Windows Binaries on the BackTrack Distribution

3. To copy **wget.exe** to the Apache directory, type the following at the terminal of the BackTrack 5 Internal Attack Machine:

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

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

Figure 11: Copying wget.exe to the WWW Directory

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

4. 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 wget.exe wstool
```

Figure 12: Contents of the WWW Directory

5. Download the wget file from the BackTrack Linux Machine running Apache by typing the following URL in your browser of the Windows 2k3 Internal Victim Machine: <http://192.168.100.3/wget.exe>

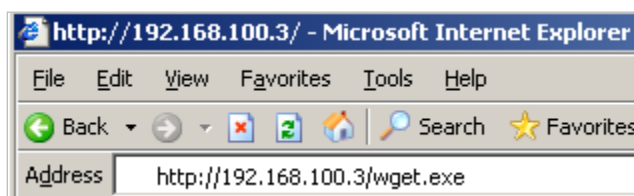


Figure 13: The URL in the Browser

- Click the **Save** button at the **File Download** Screen.

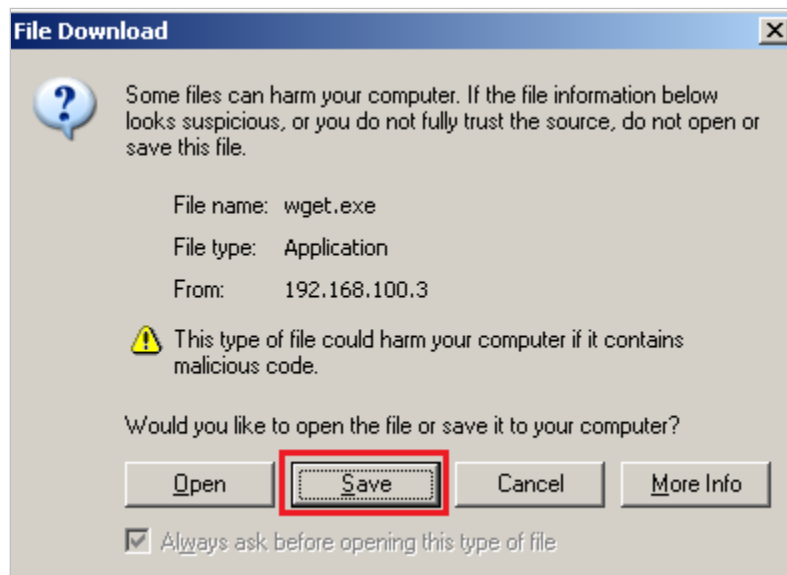


Figure 14: File Download Security Box

- Click on **My Computer**, then double-click **Local Disk (C:)** and **Windows**. Click **Save**.

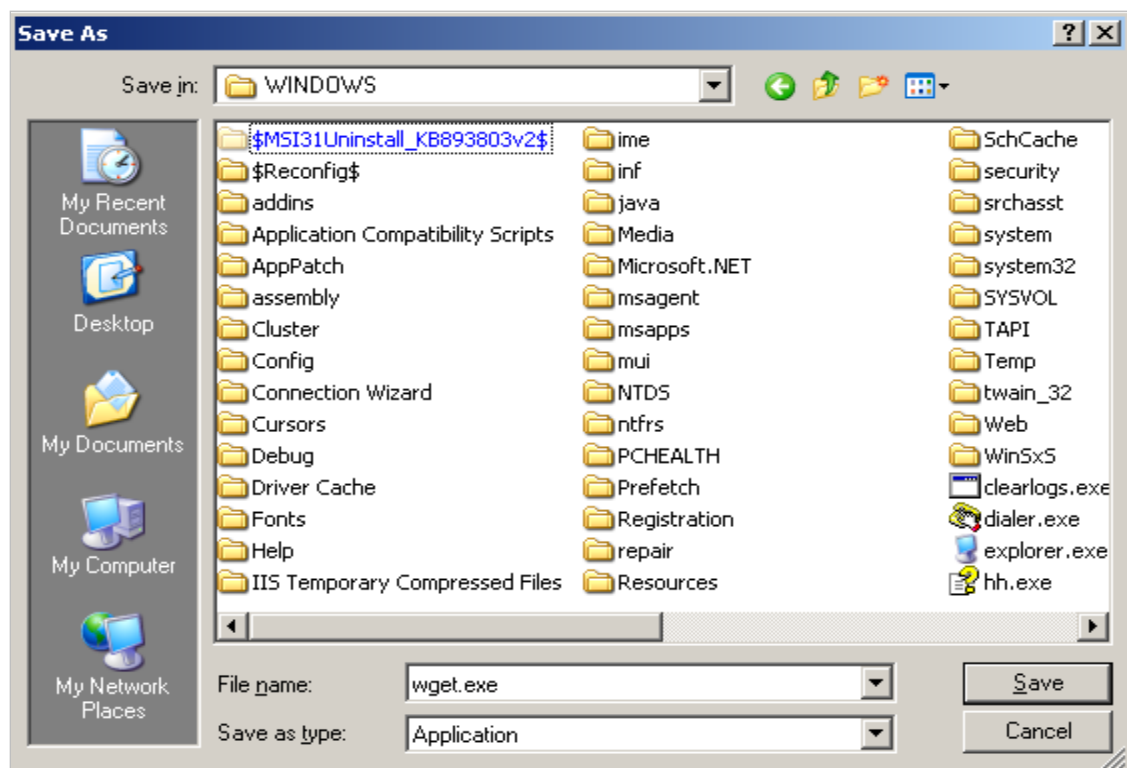


Figure 15: Downloading the Executable to the Windows Directory

Click **Close** to close the download complete dialog box. 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.

8. Open a command prompt on the Windows 2k3 Internal Victim Machine by double-clicking on the **Command Prompt** shortcut on the desktop.

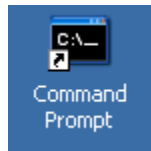


Figure 16: Opening a Command Prompt on Windows 2k3

9. Type the following command to verify that the wget file transferred correctly:
C:\wget --help

```

C:\>wget --help
GNU Wget 1.9.1, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
-V, --version          display the version of Wget and exit.
  
```

Figure 17: Displaying the options for the wget command

Wget is a command line utility that allows you to download web pages and files.

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

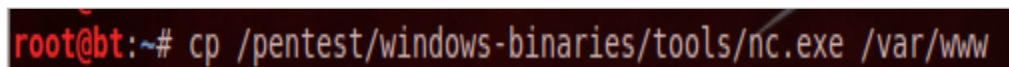
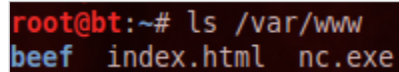


Figure 18: Copying Netcat to the WWW Directory

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

11. To verify that the file is present in the destination directory, type the following:

```
root@bt:~#ls /var/www
```

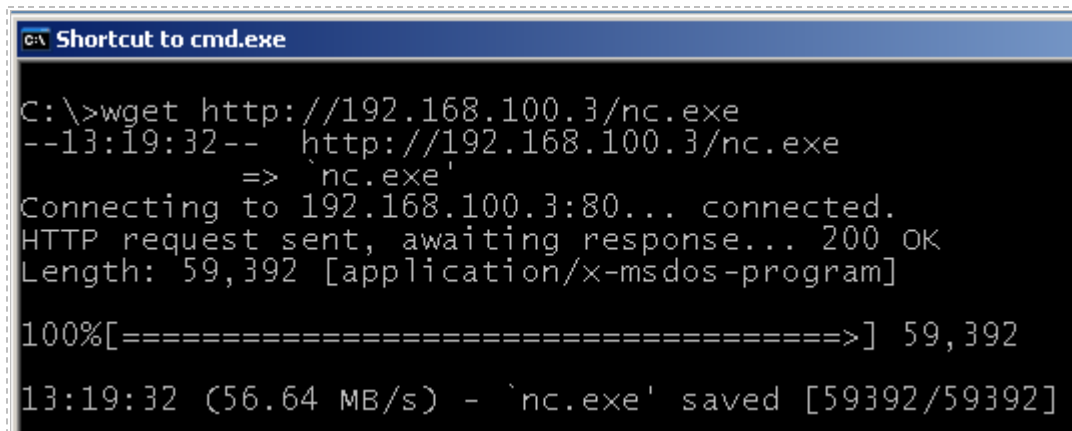


```
root@bt:~# ls /var/www
beef  index.html  nc.exe
```

Figure 19: Verifying that Netcat is in the WWW Directory

12. On the Windows 2k3 Internal Victim Machine, use wget.exe from the command line to download nc.exe

```
C:\>wget http://192.168.100.3/nc.exe
```



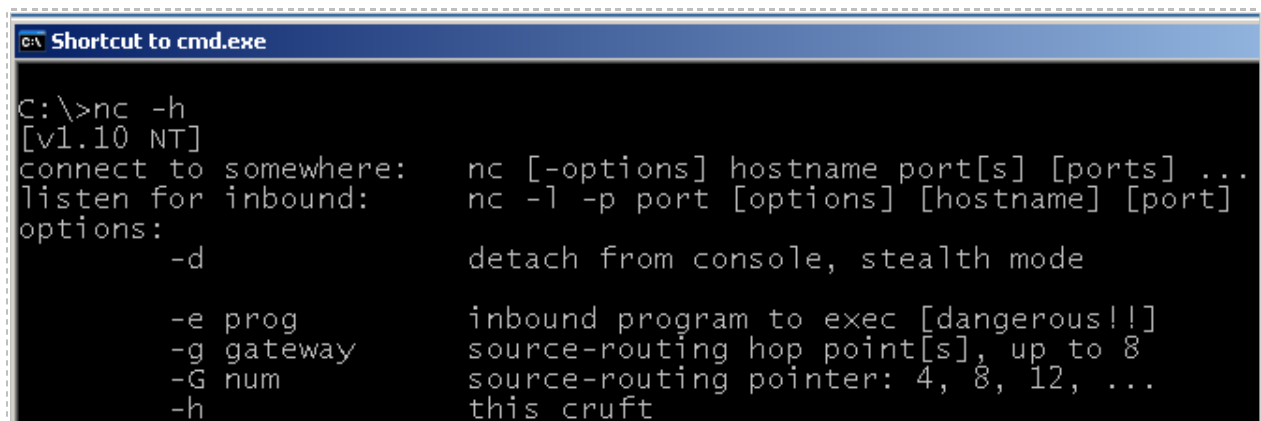
```
C:\>wget http://192.168.100.3/nc.exe
--13:19:32-- http://192.168.100.3/nc.exe
=> `nc.exe'
Connecting to 192.168.100.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 59,392 [application/x-msdos-program]

100%[=====>] 59,392
13:19:32 (56.64 MB/s) - `nc.exe' saved [59392/59392]
```

Figure 20: Starting a Netcat Listener on Port 443

13. Type the following command to verify that the netcat file transferred correctly:

```
C:\>nc -h
```



```
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 craft
```

Figure 21: Displaying the Options for the Netcat Command

14. In the BackTrack 5 Internal Attack Machine terminal, type **wireshark** (all lowercase) to bring up the wireshark program.

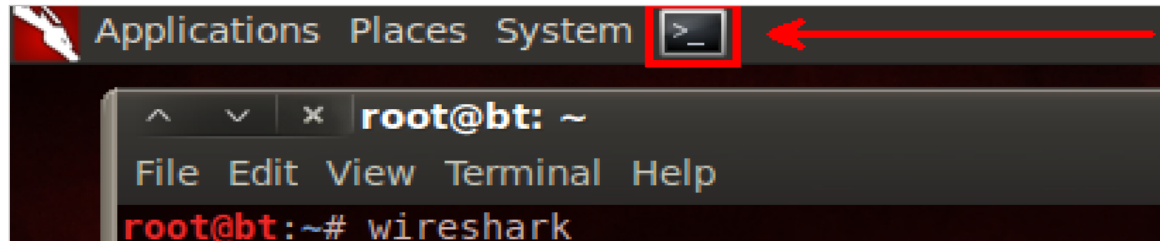


Figure 22: The Terminal Windows within BackTrack

15. Click the button that says **Don't show this message again**, and click **OK**.

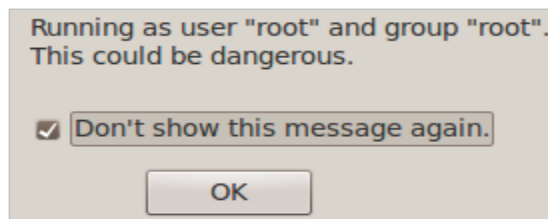


Figure 23: Allow Wireshark to run as root

Wireshark is a protocol analyzer that allows you to capture network traffic in real time. You can also use it to analyze network traffic that you have captured previously. We will examine a file containing previously captured data in the steps below.

16. Select **file** from the Wireshark menu and select **open**.
Double-click on the **root** folder, and then double-click on the **lab3** folder.
Double-click on the file **lab3.pcap**

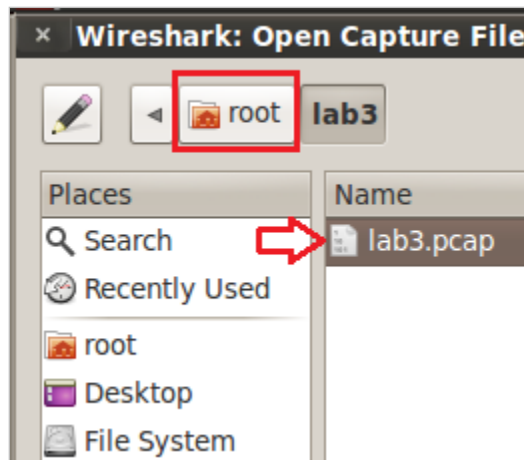


Figure 24: Selecting the lab3.pcapfile

17. From the Wireshark menu, select **File > Export > Objects > HTTP**.

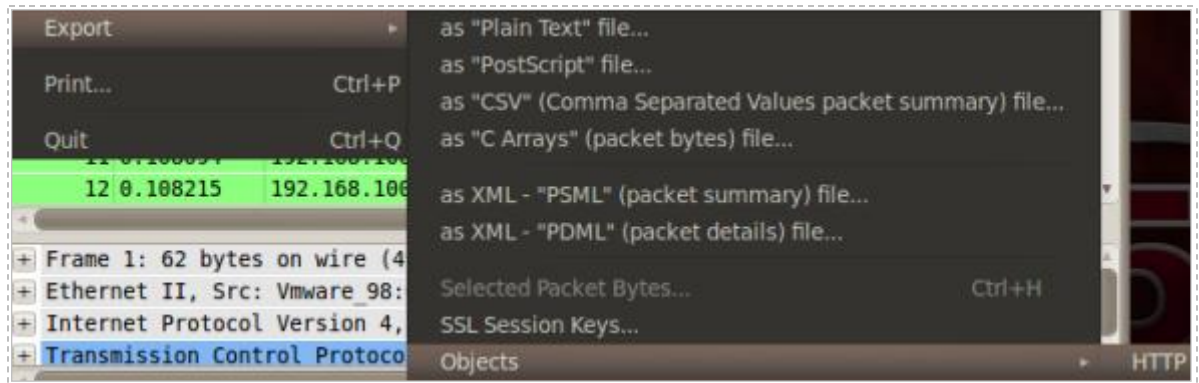


Figure 25: Parsing HTTP Objects

18. A new window will open with hostnames and filenames. You can see the names of the two files that were downloaded, wget.exe and nc.exe. When finished, click Cancel and exit Wireshark.

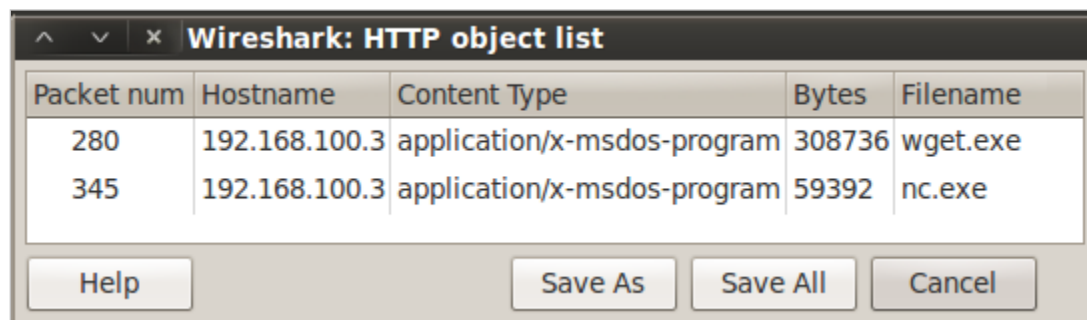


Figure 26: The HTTP Object List

1.2 Conclusion

Apache is web server software that is included with the BackTrack Linux distribution. The HTTP protocol uses port 80, and files can be downloaded from an HTTP server with a browser, such as Internet Explorer, or a command line utility like wget. You can parse out objects that were transferred via the HTTP protocol over port 80 within Wireshark.

1.3 Discussion Questions

1. What is the command to check to see if the web server is running on Linux?
2. How do you parse HTTP objects out of Wireshark?
3. How can you display all of the options for the wget command?
4. What does HTTP stand for and what port does it use?

2 Using File Transfer Protocol (FTP) to Transfer Files

File Transfer Protocol, or FTP, uses Transmission Control Protocol and ports 20 and 21. FTP can be used to upload or download files. FTP sends everything across the wire in clear text by default, so its use should be avoided in favor of SCP if at all possible.

2.1 Using FTP

You can use FTP from a browser or from the command line. FTP is more powerful from the command line and offers many more options. You can use FTP to upload or download files as long as the account you are using has permission. Some FTP sites allow anonymous access while others require a username and password. By default, all transmissions using the FTP protocol are sent over the wire in clear text.

1. Open a command prompt on the Windows 2k3 Internal Victim Machine by double-clicking on the **Command Prompt** shortcut on the Desktop.

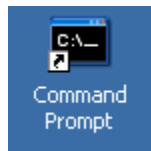


Figure 27: Opening a Command Prompt on Windows 2k3

By default, users who connect to the FTP server on this Windows 2k3 system will see the files and folders located within the **C:\Inetpub\ftproot** directory.

2. To view which files users will see when they connect to your FTP server, type **C:\>dir C:\Inetpub\ftproot**

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

Directory of C:\Inetpub\ftproot

01/18/2010  10:19 AM    <DIR>          .
01/18/2010  10:19 AM    <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s)  1,349,976,064 bytes free
```

Figure 28: Viewing the ftproot directory

- Copy the **Bliss** file to the **C:\Inetpub\ftproot** directory by typing the following:
C:\> copy c:\WINDOWS\web\Wallpaper\Bliss.jpg c:\Inetpub\ftproot

```
C:\>copy c:\WINDOWS\web\Wallpaper\Bliss.jpg c:\Inetpub\ftproot
1 file(s) copied.
```

Figure 29: Copying a JPG file to the C:\Inetpub\ftproot directory

You should receive the message, *1 file(s) copied*, if your file is copied successfully.

Now, we will transfer the file from the Windows 2k3 Internal Victim Machine to the BackTrack 5 Internal Attack Machine.

- 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. Connect to the FTP server by typing the following command:
root@bt:~#ftp 192.168.100.201

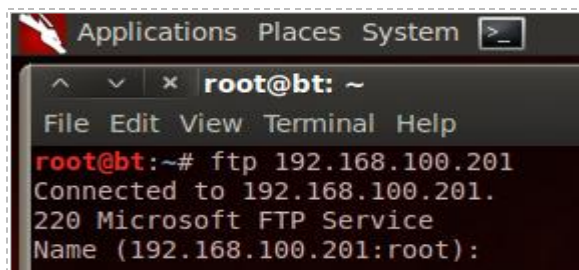


Figure 30: FTP to a Remote Machine

- For the username, type **ftp**. For the password, type **securityplus**.

For security reasons, the password will not be displayed when you type it.

```
Name (192.168.100.201:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-Welcome to the ptest.org FTP site.
230 Anonymous user logged in.
Remote system type is Windows_NT.
ftp>
```

Figure 31: Logging in as FTP

FTP sites allowing anonymous connections will allow you to login as **ftp** or **anonymous**.
 Note: you should receive the message *Anonymous user logged in*.

6. Type the following command to view the files on the remote Windows system:
ftp>ls

```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
03-25-03 07:00AM 51127 Bliss.jpg
226 Transfer complete.
ftp>
```

Figure 32: Viewing the files on the Remote FTP Site

Before the file can be transferred, you need to switch to binary mode if you are downloading or uploading anything that is not a text file, like a picture or an executable.

7. Type the following command to switch to binary mode:
ftp>bin

```
ftp> bin
200 Type set to I.
ftp>
```

Figure 33: Switching to Binary Mode

8. To download the file, type the following command (case sensitive):
ftp>get Bliss.jpg

```
ftp> get Bliss.jpg
local: Bliss.jpg remote: Bliss.jpg
200 PORT command successful.
150 Opening BINARY mode data connection for Bliss.jpg(51127 bytes)
226 Transfer complete.
51127 bytes received in 0.04 secs (1223.6 kB/s)
ftp>
```

Figure 34: Downloading the File

9. Close the ftp session by typing the following command at the ftp prompt:
ftp>bye

```
ftp> bye
221 Thanks for visiting.
root@bt:~#
```

Figure 35: Leaving the FTP Site

View the file by looking within root's home folder.

10. Click on **Places** from the menu bar and select **Home Folder**, view **Bliss.jpg**. Close the Home Folder when you are finished.

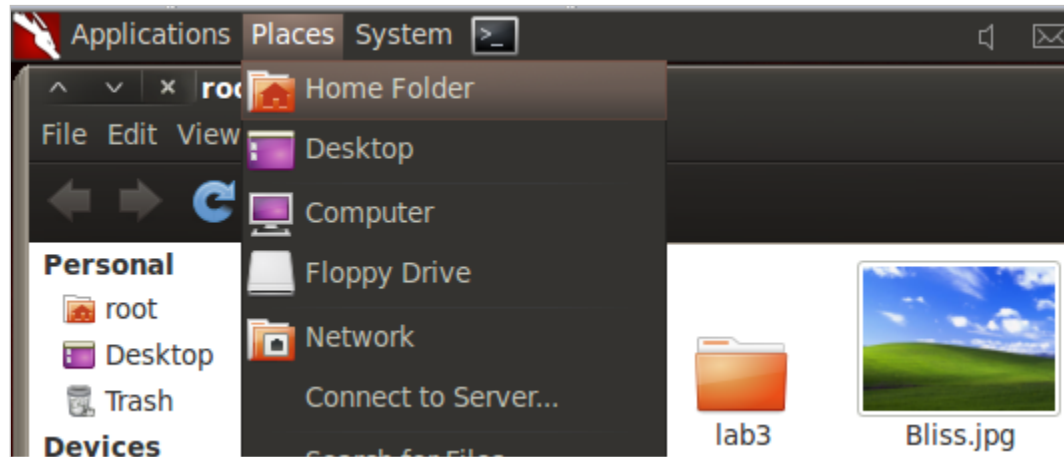


Figure 36: Viewing the Uploaded File

This Windows 2003 FTP Server allows users to download, but not upload files. In order to allow users to upload files, we must enable write permissions on the FTP server.

11. On the Windows 2k3 Internal Victim Machine, click on the **Start** button, select **Administrative Tools**, and open **Internet Information Services (IIS) Manager**.

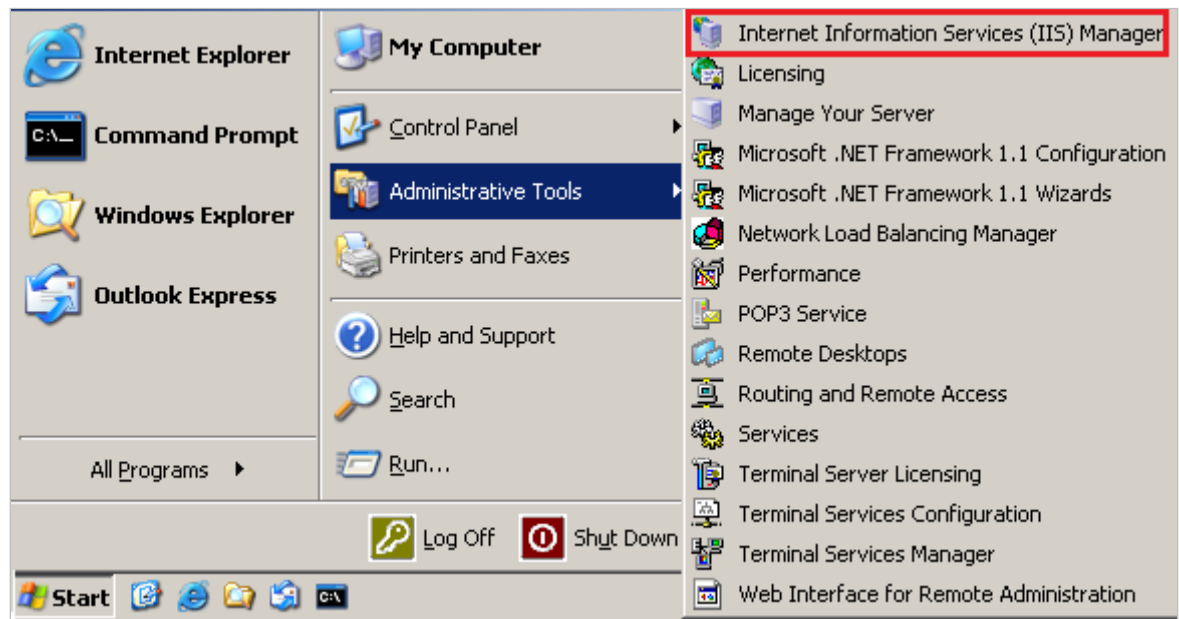


Figure 37: Opening Internet Information Services (IIS) Manager

12. Click the plus (+) sign next to the server name to view all available sites. Expand FTP Sites by clicking the plus (+) sign next to it. Right-click on **Default FTP Site** and go to **Properties**. Click on the **Home Directory** tab. Check the **Write** box and click **OK** to close the **Default FTP Site Properties** window. Close the Internet Information Services (IIS) Manager.

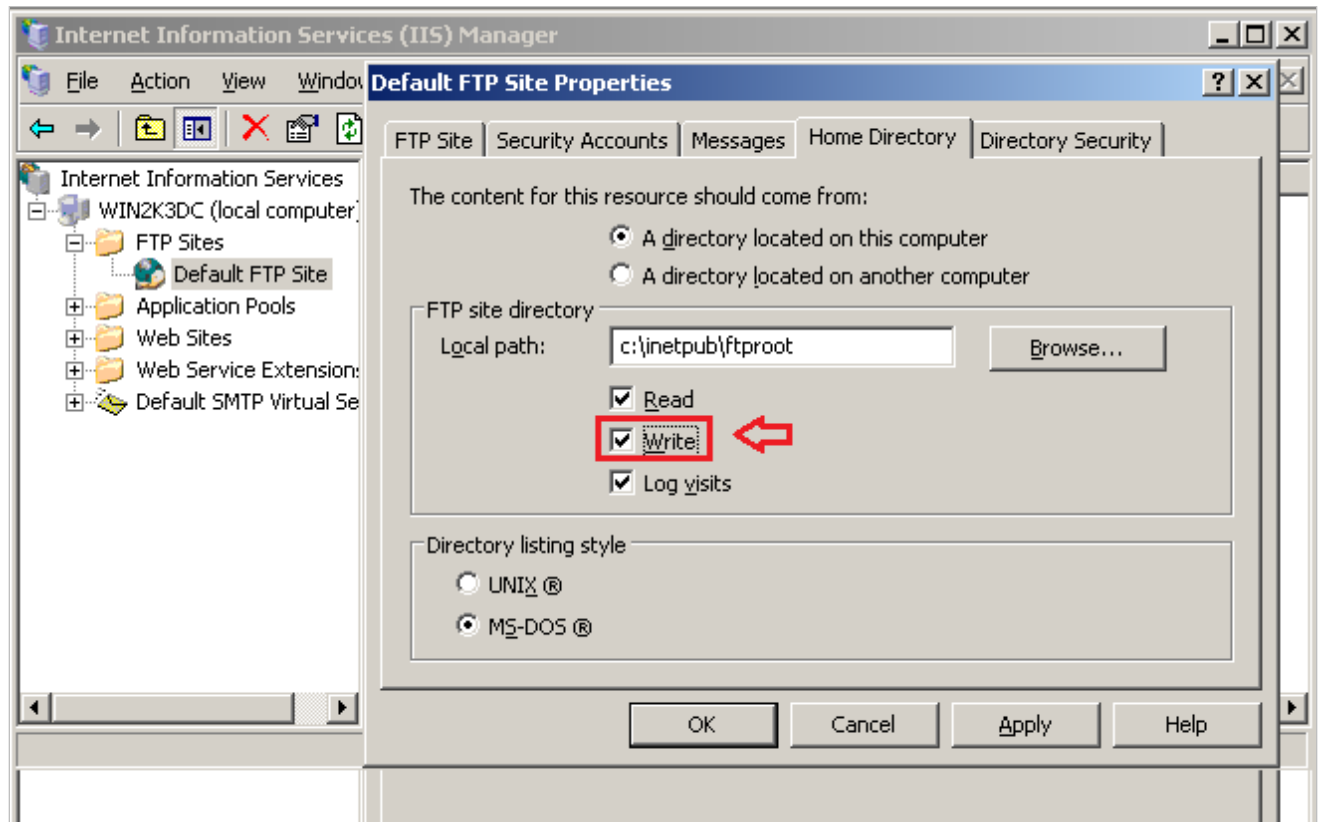


Figure 38: Allowing Write Access for the FTP Site

13. On the BackTrack 5 Internal Attack Machine, copy the BackTrack wallpaper to the root directory by typing the following:
`root@bt:~#cp /usr/share/wallpapers/backtrack/Backtrack_5_blue.jpg /root`

```
root@bt:~# cp /usr/share/wallpapers/backtrack/Backtrack_5_blue.jpg /root
```

Figure 39: Copying the Wallpaper file

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

14. Type the following command to view the file in the root directory:
`root@bt:~#ls`

```
root@bt:~# ls
Backtrack_5_blue.jpg
```

Figure 40: Listing the File with the ls command

15. Connect to the FTP server by typing the following command:

```
root@bt:~#ftp 192.168.100.201
```

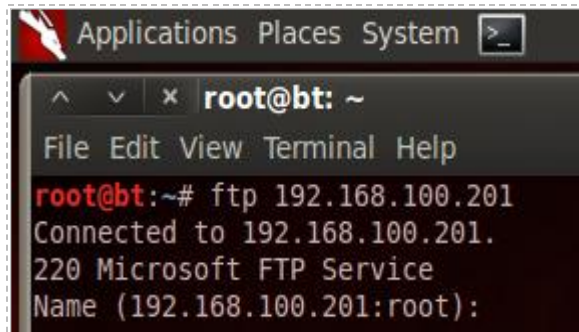


Figure 41: Copying a JPG file to the C:\Inetpub\ftproot directory

16. For the username, type **ftp**. For the password, type **securityplus**.

For security reasons, the password will not be displayed when you type it.

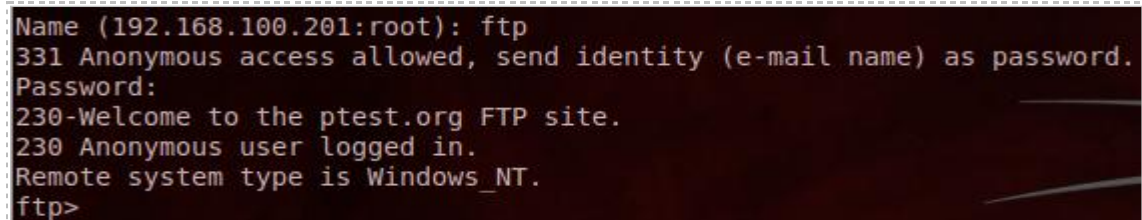


Figure 42: Logging in as FTP

FTP Sites allowing anonymous connections will allow you to login as **ftp** or **anonymous**.

Note: you should receive the message, *Anonymous user logged in*.

17. Type the following command to view the files on the remote Windows system:

```
ftp>ls
```

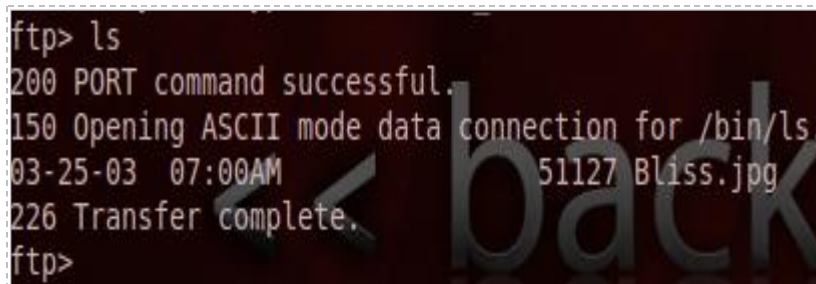
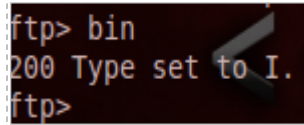


Figure 43: Viewing the files on the Remote FTP Site

Before the file can be transferred, you need to switch to binary mode if you are downloading or uploading anything that is not a text file, like a picture or an executable.

18. Type the following command to switch to binary mode:

ftp>**bin**

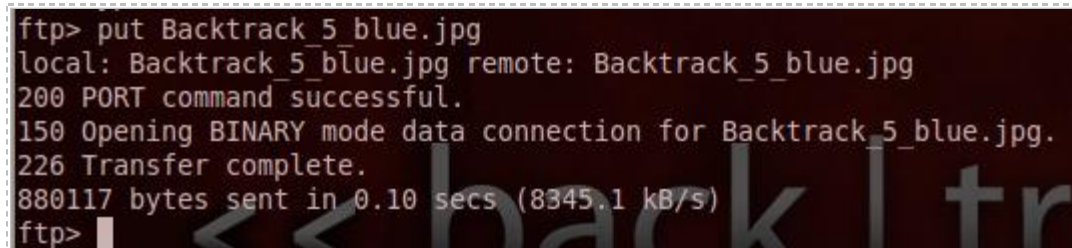


```
ftp> bin
200 Type set to I.
ftp>
```

Figure 44: Switching to Binary Mode

19. To upload the file, type the following command (case sensitive):

ftp>**put Backtrack_5_blue.jpg**

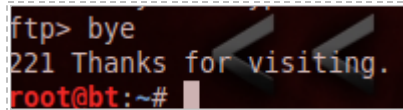


```
ftp> put Backtrack_5_blue.jpg
local: Backtrack_5_blue.jpg remote: Backtrack_5_blue.jpg
200 PORT command successful.
150 Opening BINARY mode data connection for Backtrack_5_blue.jpg.
226 Transfer complete.
880117 bytes sent in 0.10 secs (8345.1 kB/s)
ftp>
```

Figure 45: Uploading the File

20. Close the ftp session by typing the following command at the ftp prompt:

ftp>**bye**



```
ftp> bye
221 Thanks for visiting.
root@bt:~#
```

Figure 46: Leaving the FTP Site

21. On the Windows 2k3 Internal Victim Machine, double-click on **My Computer** and double-click on **Local Disk (C:)**. Double-click on the **Inetpub** directory, then double-click on **ftproot**. Double-click on the **Backtrack_5_blue.jpg** file to open it.

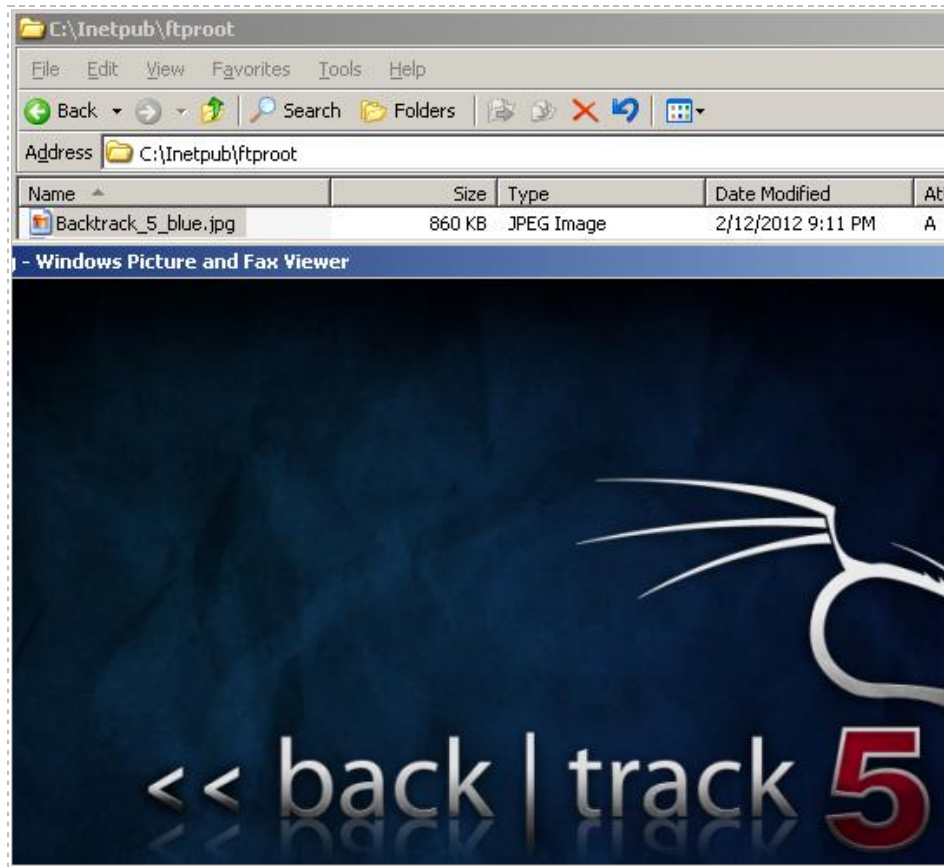


Figure 47: The Uploaded FTP File

22. Close all open windows.

2.2 Conclusion

Like HTTP, the FTP protocol can be used to download files. FTP also can be used to upload files if the user has permission to do so. Many FTP sites allow users to login anonymously. FTP uses Ports 20 and 21 and transmits data in clear text by default.

2.3 Discussion Questions

1. What are the two ports that FTP uses?
2. What is the command to upload a file to an FTP server?
3. Which ftp command should be used before uploading a picture file?
4. What is the default directory where Windows FTP files are stored?

3 Transferring Files Securely Using SCP

In this section, you will securely copy a file from the BackTrack 5 Internal Attack Machine to the Red Hat Enterprise Linux (RHEL) Internal Victim Machine using SCP. Unlike FTP transmissions, SCP transmissions are encrypted. Port 22, Secure Shell, is used for SCP.

3.1 Using SCP

SCP can be used to securely send a file to a remote system.

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. Copy the BackTrack wallpaper to the root user's directory by typing the following:

```
root@bt:~#cp /usr/share/wallpapers/backtrack/Backtrack_5_camo.jpg /root
```

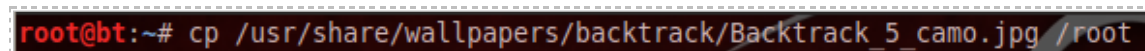
A terminal window with a dark background. The prompt is 'root@bt:~#'. The command entered is 'cp /usr/share/wallpapers/backtrack/Backtrack_5_camo.jpg /root'. The command is highlighted in red.

Figure 48: Copying the BackTrack Wallpaper

2. Type the following command to view the file in the root directory:

```
root@bt:~#ls Backtrack_5_camo.jpg
```

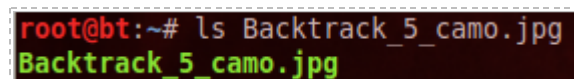
A terminal window with a dark background. The prompt is 'root@bt:~#'. The command entered is 'ls Backtrack_5_camo.jpg'. The output 'Backtrack_5_camo.jpg' is shown in green.

Figure 49: The Wallpaper File in root's Home Directory

3. Copy the file to the root directory of the RHEL Machine by typing the following:
root@bt:~#scp Backtrack_5_camo.jpg root@192.168.100.147:/root/Backtrack_5_camo.jpg

SCP command syntax: **scp** *[filename to copy]* *[username]@[machine name or IP address of machine]:[path to copy file to]*

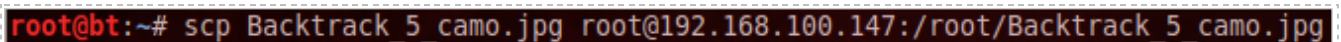
A terminal window with a dark background. The prompt is 'root@bt:~#'. The command entered is 'scp Backtrack_5_camo.jpg root@192.168.100.147:/root/Backtrack_5_camo.jpg'. The command is highlighted in red.

Figure 50: Using the scp command

Hit the Enter key after you type the **scp** command on your BackTrack Linux Machine.

4. If prompted, type **yes** when you are asked if you are sure you want to continue connecting. If you do not receive the prompts (as seen below), continue to #5.

```
root@bt:~# scp Backtrack_5_camo.jpg root@192.168.100.147:/root/Backtrack_5_camo.jpg
The authenticity of host '192.168.100.147 (192.168.100.147)' can't be established.
RSA key fingerprint is c8:79:74:50:d9:78:c1:83:9c:e4:a1:53:4c:7d:15:3a.
Are you sure you want to continue connecting (yes/no)? yes
```

Figure 51: Connection Warning

5. Type the password of **password**. The file transfer status should go to 100%.

```
root@192.168.100.147's password:
Backtrack_5_camo.jpg 100% 1019KB 1.0MB/s 00:01
```

Figure 52: Transferred File Status

6. On the Red Hat Internal Victim Machine, click on **Places** and select **Home Folder** to view the copied file. Close the window when you are finished.

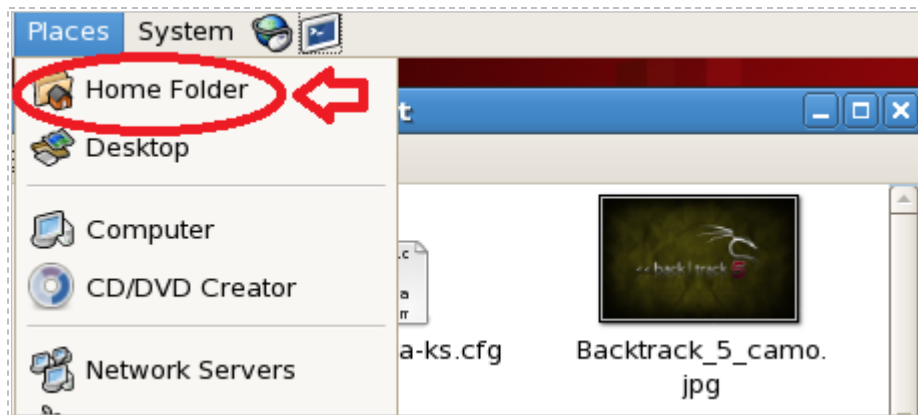


Figure 53: Transferred File

3.2 Conclusion

The Secure Copy Protocol is a way to securely transfer files from one system to another. Unlike FTP, SCP encrypts the transmission so usernames and passwords will not be seen going across the wire like they can be with FTP. Use SCP rather than FTP whenever possible.

3.3 Discussion Questions

1. What port does SSH and SCP use by default?
2. What does SCP stand for?
3. How is SCP different from the FTP protocol?
4. What benefits does using SCP provide over other protocols?

References

1. FTP Commands:
<http://unixhelp.ed.ac.uk/CGI/man-cgi?ftp>
2. SCP:
<http://kb.iu.edu/data/agye.html>
3. Internet Information Services:
<http://www.iis.net/>
4. Apache:
<http://www.apache.org/>
5. BackTrack Linux:
<http://www.backtrack-linux.org/>
6. Netcat:
<http://netcat.sourceforge.net/>