



CompTIA Security+® Lab Series

Lab 8: Configuring Backups

CompTIA Security+® Domain 2 - Compliance and Operational Security

Objective 2.7: Execute disaster recovery plans and procedures

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 |
| Objectives: Execute disaster recovery plans and procedures | 3 |
| Pod Topology | 4 |
| Lab Settings | 5 |
| 1 Backing Up Files to a Network Drive | 8 |
| 1.1 Mapping a Network Drive | 8 |
| 1.2 Conclusion | 23 |
| 1.3 Discussion Questions..... | 23 |
| 2 Backing Up Files to an FTP Server..... | 24 |
| 2.1 Backing up Files to an FTP Server..... | 24 |
| 2.2 Conclusion | 28 |
| 2.3 Discussion Questions..... | 28 |
| 3 Backing up Files using SCP | 29 |
| 3.1 Using SCP | 29 |
| 3.2 Conclusion | 32 |
| 3.3 Discussion Questions..... | 32 |
| References | 33 |

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 configure backups.

This lab includes the following tasks:

- 1 – Backing Up Files to a Network Drive
- 2 – Backing Up Files to an FTP Server
- 3 – Backing Up Files using SCP

Objectives: Execute disaster recovery plans and procedures

Companies need to protect their data by backing it up. A successful disaster recovery plan includes backup procedures that will allow a company to return to operational status quickly. Different methods can be utilized to backup critical files and data.

SCP – Secure copy (SCP) is a means of securely transferring files between a local host and a remote host or between two remote hosts, based on Secure Shell (SSH) protocol. Files can be uploaded using the SSH protocol with SCP. The files will be encrypted when sent over the network.

FTP – File Transfer Protocol, or FTP allows for users to transfer files from one machine to another remotely. The drawback to using FTP is data is sent in clear text.

Network Drive – A Network Drive is storage on another computer that is assigned a drive letter. In some cases, a user will only have read access to the network drive, so they will not be able to store any files. If write permissions exist, the user can store files.

Net use – The net use command can be used to map a remote system's drives.

Net view – The net view command will display a list of the system's network shares.

Pod Topology

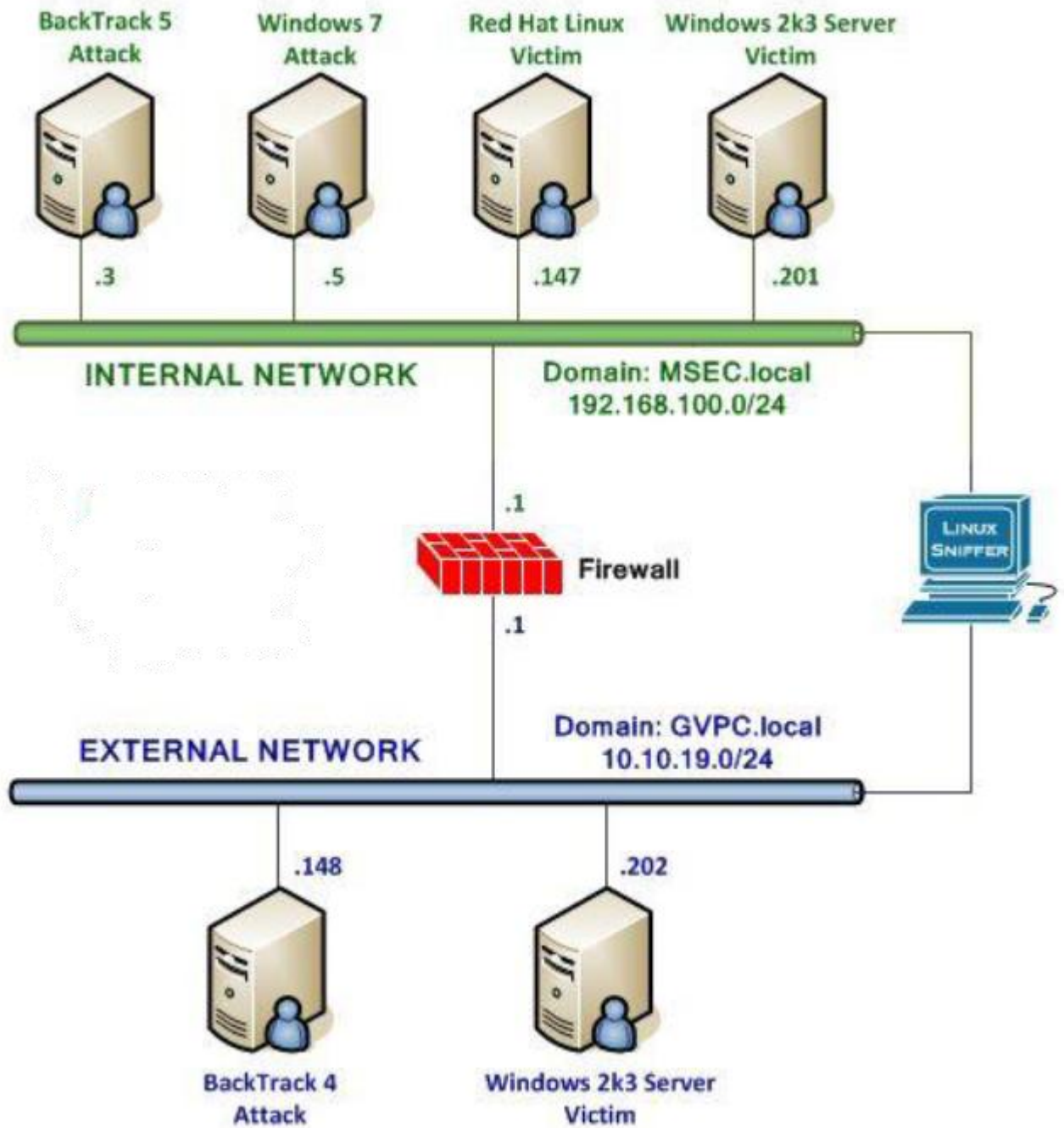


Figure 1: Topology

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 | 192.168.100.147 |
| Red Hat Enterprise Linux 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 and press enter.
3. At the password prompt, type **password** and press **enter**.

A screenshot of a terminal window showing the BackTrack 5 login process. The text displayed is: "BackTrack 5 R1 - Code Name", "bt login: root", and "Password:". The cursor is positioned at the end of the password prompt.

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

Figure 2: BackTrack 5 login

For security purposes, the password will not be displayed.

Windows 2003 Server Login:

1. Click on the **Windows2k3 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 3: Windows 2k3 login

Red Hat Enterprise Linux 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**.

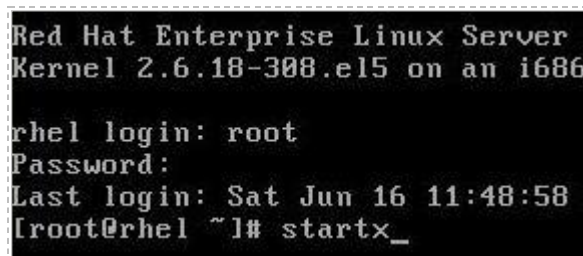


Figure 4: RHEL login

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 5: Windows 7 login

1 Backing Up Files to a Network Drive

A network drive allows users to use storage on a remote machine. In many cases, end users are using a server that has a large storage capacity and better hardware resources than their workstation. Microsoft server operating systems, like Server 2003, 2008, and 2012, also can allow a large number of connections, depending on their licensing model. Client operating systems, like XP and Windows 8 allow a limited number of connections.

1.1 Mapping a Network Drive

1. On the **Windows 7 Internal Attack Machine**, open a command prompt by clicking on the shortcut on the desktop.

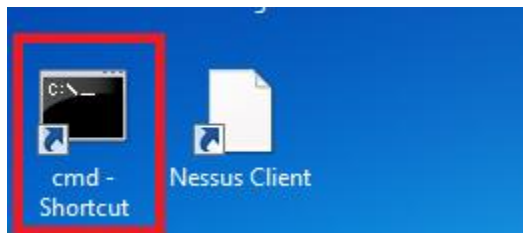


Figure 6: Opening the Command Prompt

2. Type the following command to make a directory called **share** on the root of C:
C:\mkdir share



Figure 7: Making a Directory

3. Type the following command to list all files and folder on the root of C:
C:\dir

```
C:\>dir
Volume in drive C has no label.
Volume Serial Number is E8D7-61E9

Directory of C:\

07/03/2013  11:03 AM                1,024 .rnd
06/10/2009  05:42 PM                 24 autoexec.bat
11/29/2011  08:49 PM             <DIR>      class_tools
06/10/2009  05:42 PM                 10 config.sys
03/15/2012  11:27 PM             <DIR>      mame
07/13/2009  10:37 PM             <DIR>      PerfLogs
05/31/2012  01:23 AM             <DIR>      Program Files
07/03/2013  10:31 PM             <DIR>      share
10/17/2011  06:33 PM             <DIR>      Users
05/31/2012  01:50 AM             <DIR>      Windows
               3 File(s)                1,058 bytes
               7 Dir(s)          1,076,322,304 bytes free
```

Figure 8: Directory Listing

4. Type the following command to share the **share** directory on the root of C:
C:\net share share=c:\share

```
C:\>net share share=c:\share
share was shared successfully.
```

Figure 9: Sharing share

5. Type the following command to view all shares on the system:
C:\net share

```
C:\>net share

Share name      Resource          Remark
-----
C$              C:\              Default share
IPC$            C:\              Remote IPC
ADMIN$          C:\windows       Remote Admin
share           c:\share
The command completed successfully.
```

Figure 10: Listed Shares

6. **On the Windows2k3 Server Internal Victim Machine**, open a command prompt by clicking on the shortcut on the desktop.

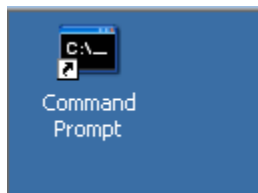


Figure 11: Open the command prompt

7. Type the following command to map a drive to the Windows 7 share (for the username, type **student** and for the password type **password**):

C:\net use x: [\\192.168.100.5\share](#)

```
C:\>net use x: \\192.168.100.5\share
The password or user name is invalid for \\192.168.100.5\share.

Enter the user name for '192.168.100.5': student
Enter the password for 192.168.100.5:
The command completed successfully.
```

Figure 12: Mapping a Drive

8. Type the following command to view your mapped network drives:

C:\net use

```
C:\>net use
New connections will be remembered.

Status          Local        Remote              Network
-----
Disconnected X:  \\192.168.100.5\share  Microsoft Windows Network
The command completed successfully.
```

Figure 13: Viewing Mapped Drives

- Click on the **Start** Button and select **My Computer** from the Start Menu.



Figure 14: Start Menu

- Click **View** from the My Computer Menu Bar and select **Tiles**.

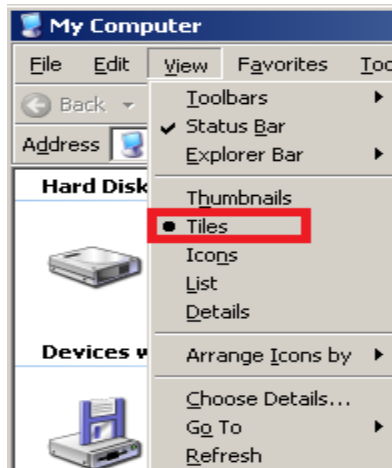


Figure 15: My Computer Menu Bar

11. Double-click on the **X:** Drive under **Network Drives**.

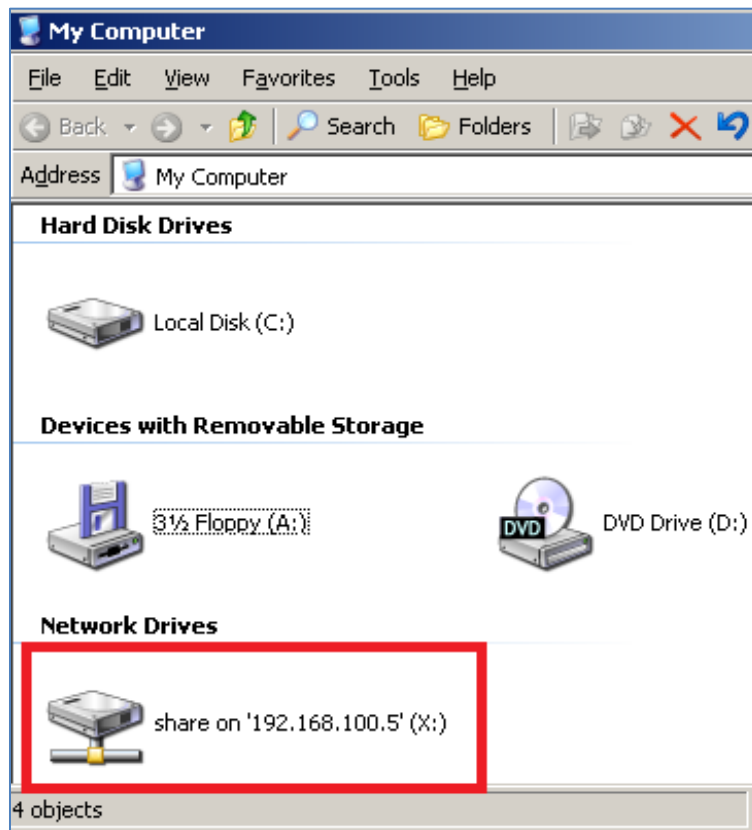


Figure 16: Network Drive in My Computer

12. Click **File** and select **New**, and then select **Folder**.

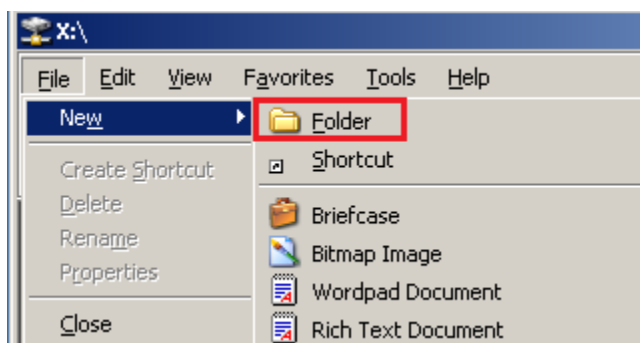


Figure 17: Attempt to Write to the Drive

13. You will receive a message stating, *Unable to create the folder... Access is denied.*

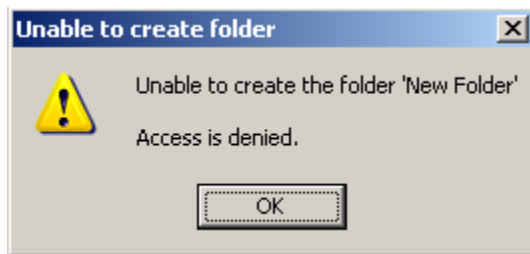


Figure 18: Applying Changes to the Folder

14. On the **Windows 7 Internal Attack Machine**, click on the **start** button and click **Computer**.

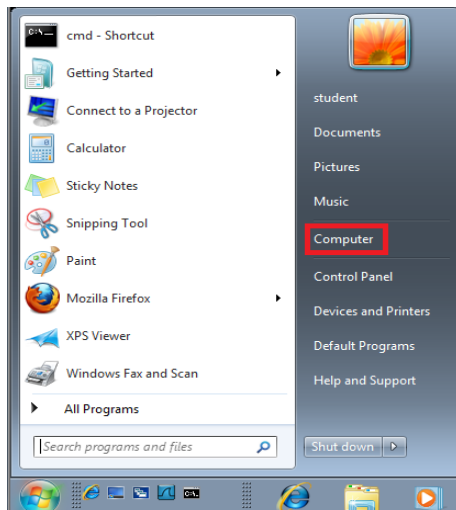


Figure 19: Start Menu Computer Link

15. Under Hard Disk Drives (1), Double click on **Local Disk (C:)**

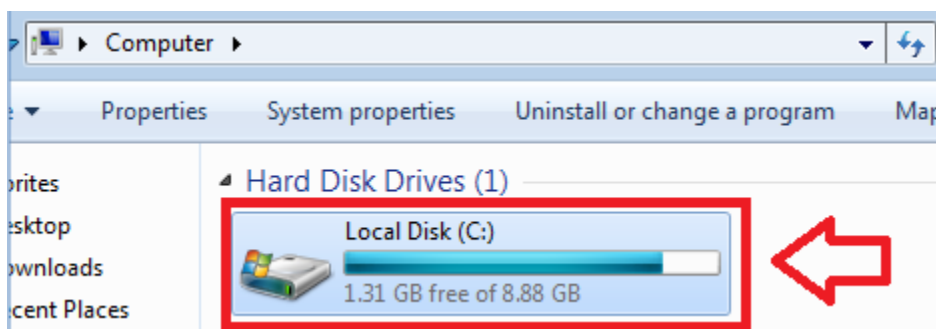


Figure 20: The C: Drive

We will need to assign write permissions to the share folder on the Windows 7 system.

16. Right-click on the **share** folder and go to **properties**.

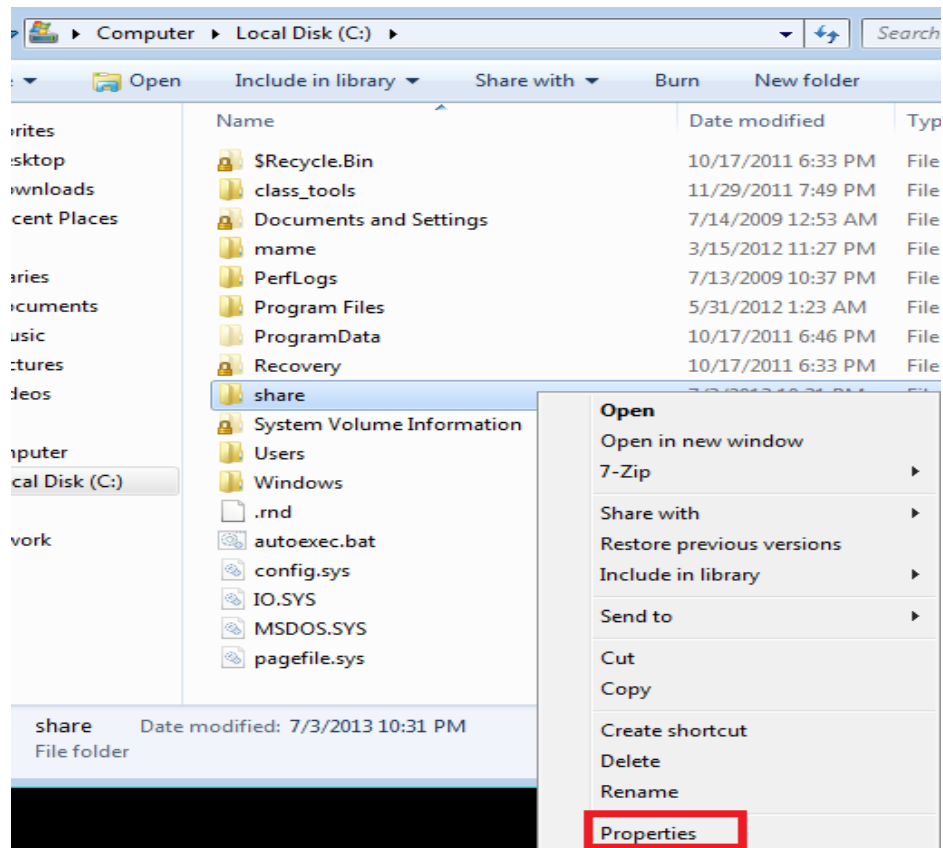


Figure 21: The Share Folder

17. Click the **Sharing** tab, then click the **Advanced Sharing** button.

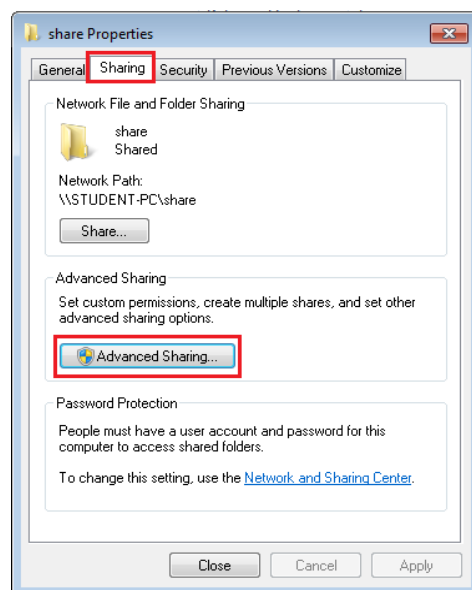


Figure 22: Sharing Tab

18. In the **Advanced Sharing** Window, click the **Permissions** tab.

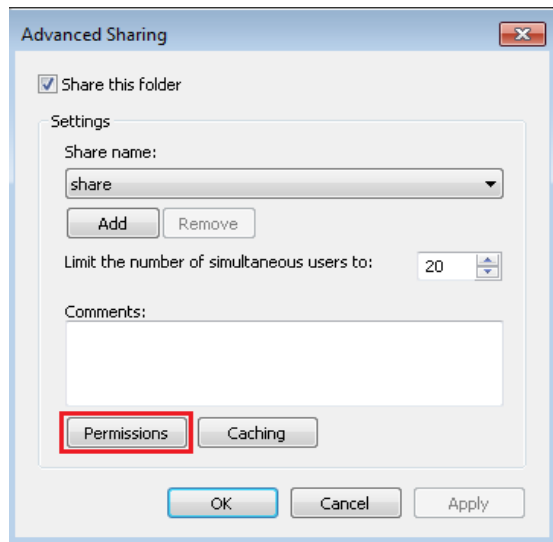


Figure 23: Creating a User

19. Check **Allow** next to **Full Control** under **Permissions for Everyone**. Click **OK**, then close.

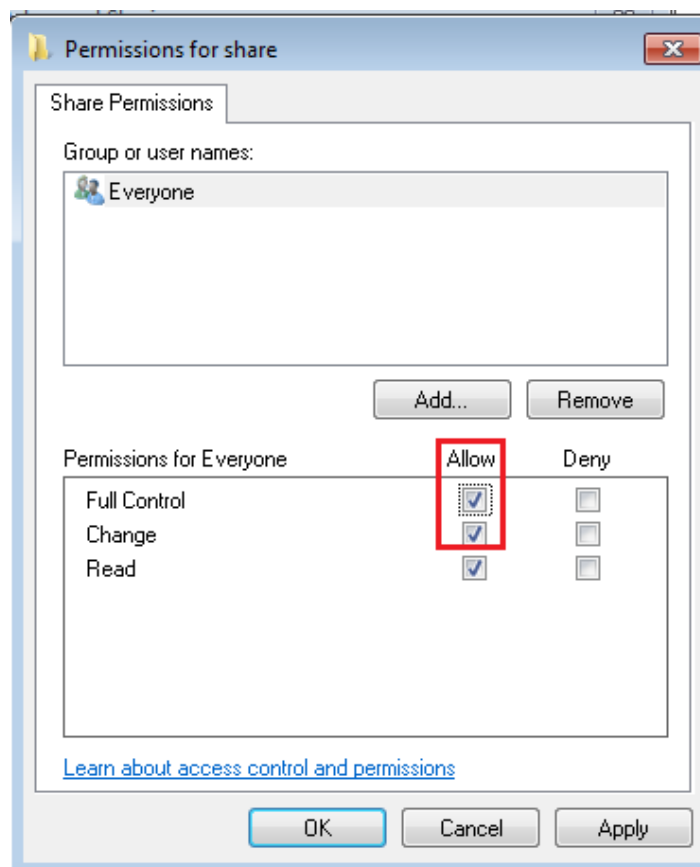


Figure 24: Allow Full Control

20. Return to the **Windows 2k3 Server Internal Victim Machine**. Click **File** and select **New**, and then select **Folder**.

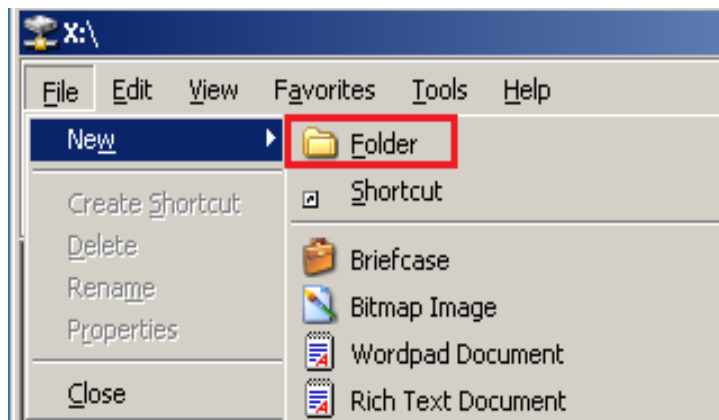


Figure 25: Attempt to Write to the Drive

21. You will see the "New Folder" folder. You can now write to the Network Drive.

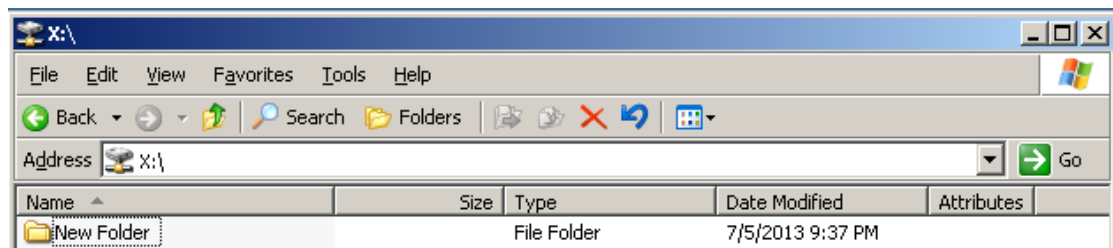


Figure 26: The Folder is Created

22. Right-click **New Folder** and select **Rename**. Type **backup** for the new folder name.

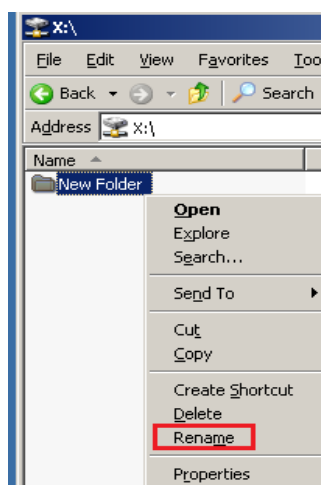


Figure 27: Renaming the folder

23. The folder named **backup** should now appear on the network drive.

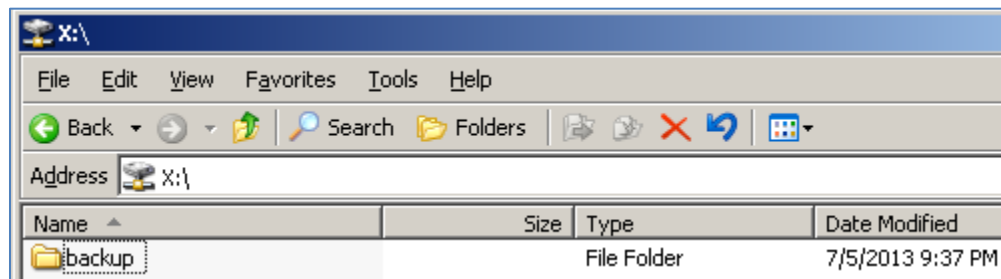


Figure 28: Folder is now called backup

24. Click on the **Start** Button, then **run** and type **ntbackup** and click **OK**.

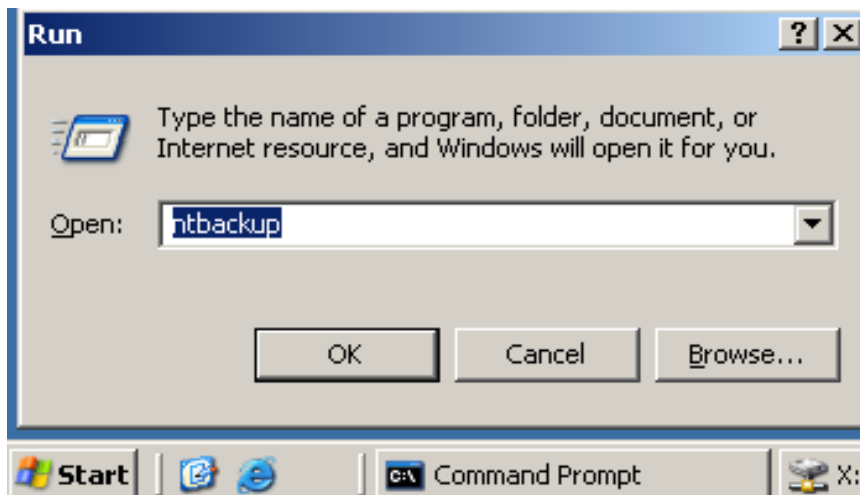


Figure 29: The ntbackup command

25. Click **Next** at the **Welcome to the Backup or Restore Wizard**.

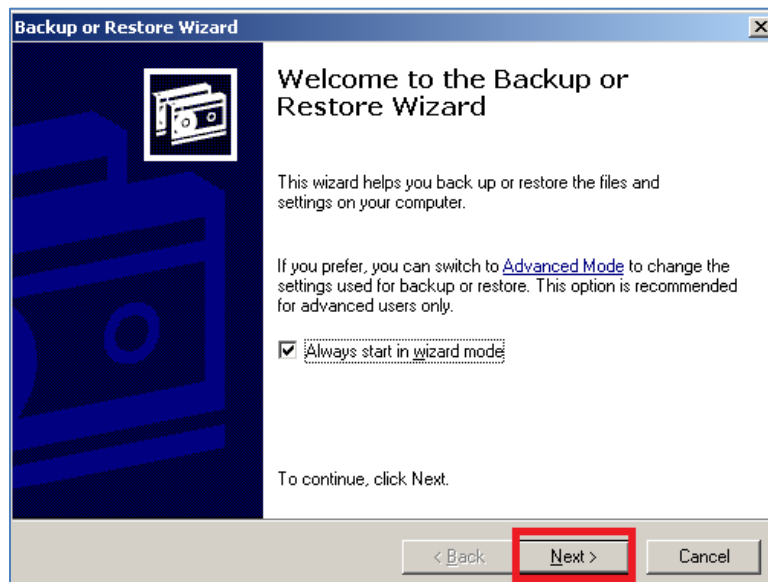


Figure 30: Backup Wizard

26. Select **Back up files and settings** and click **next**.

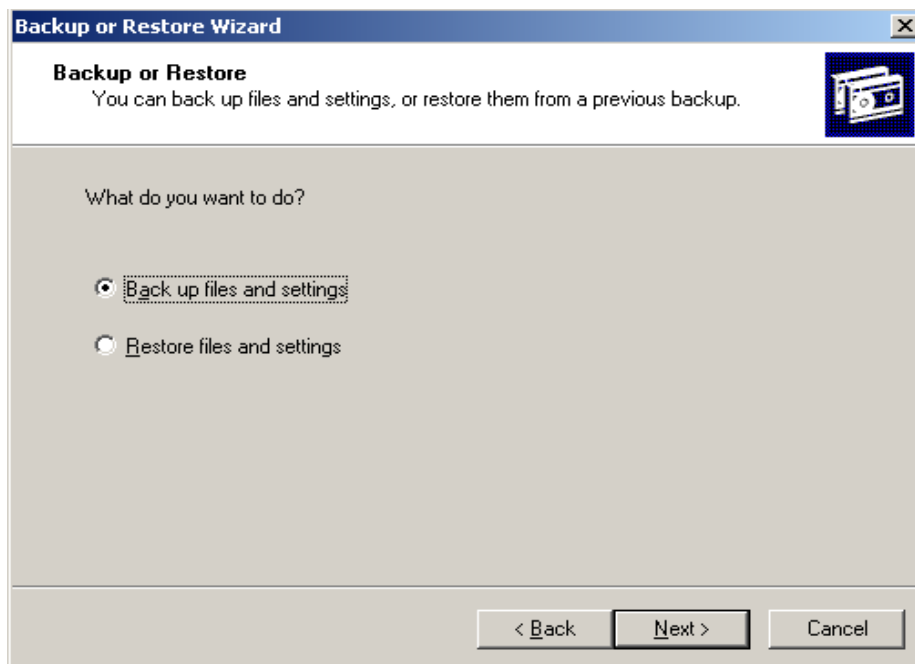


Figure 31: Back up files and settings

27. Select **Let me choose what to back up** and click **next**

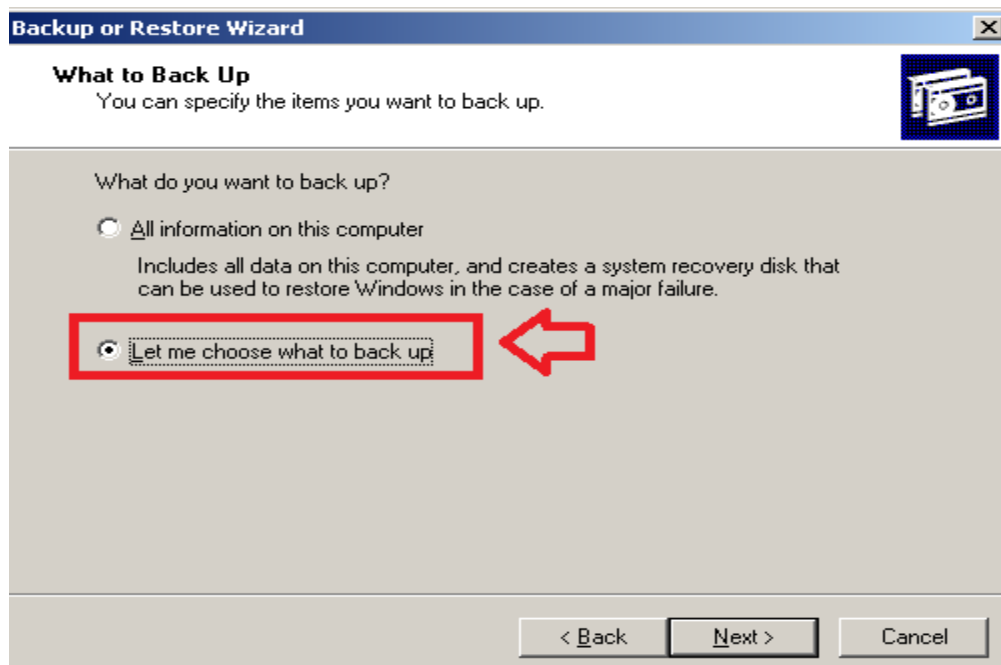


Figure 32: Let me Choose what to back up

We will backup the Active Directory Database. Active Directory is Microsoft's Directory Service. In order to backup Active Directory, we need to backup the System State.

28. Expand **Computer** and Select **System State** and then click **next**,

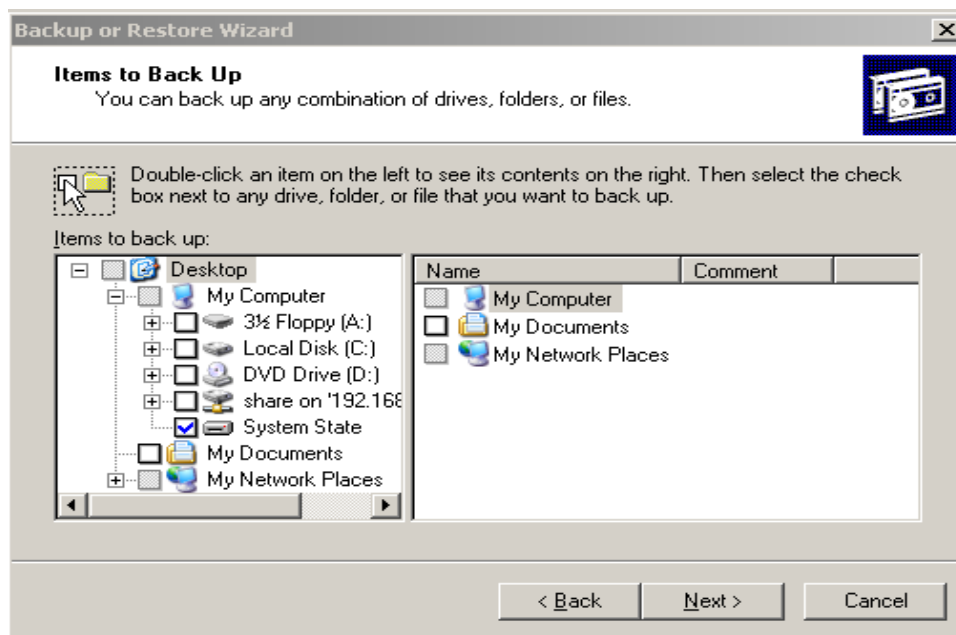


Figure 33: Items to Backup Screen

29. At the Backup Type, Destination and Name Screen, click the **Browse** Button.

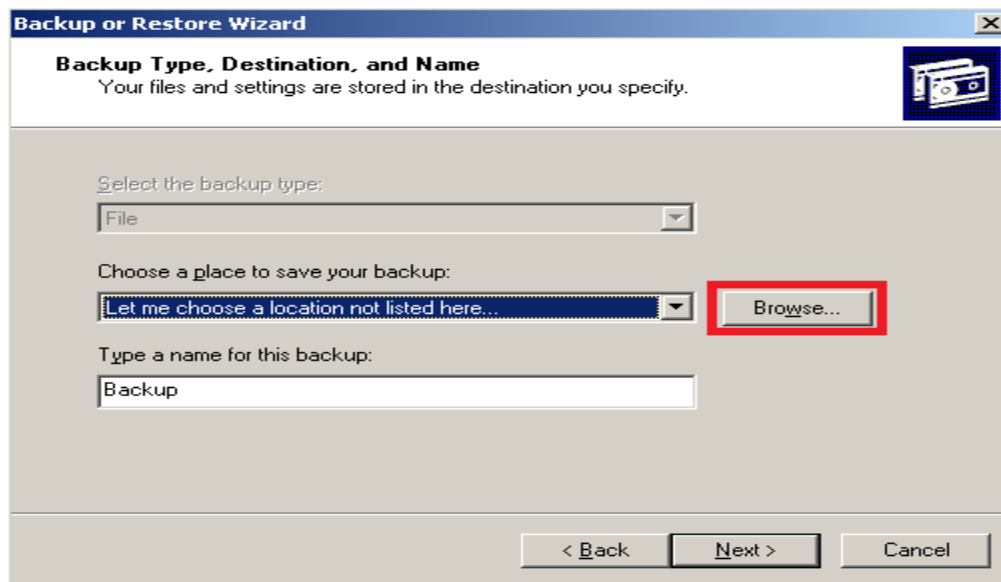


Figure 34: Browse to Location

30. In the **Save as** box, click **My Computer** on the left. Double-click **X:**, then click **backup**. Click **Save**.

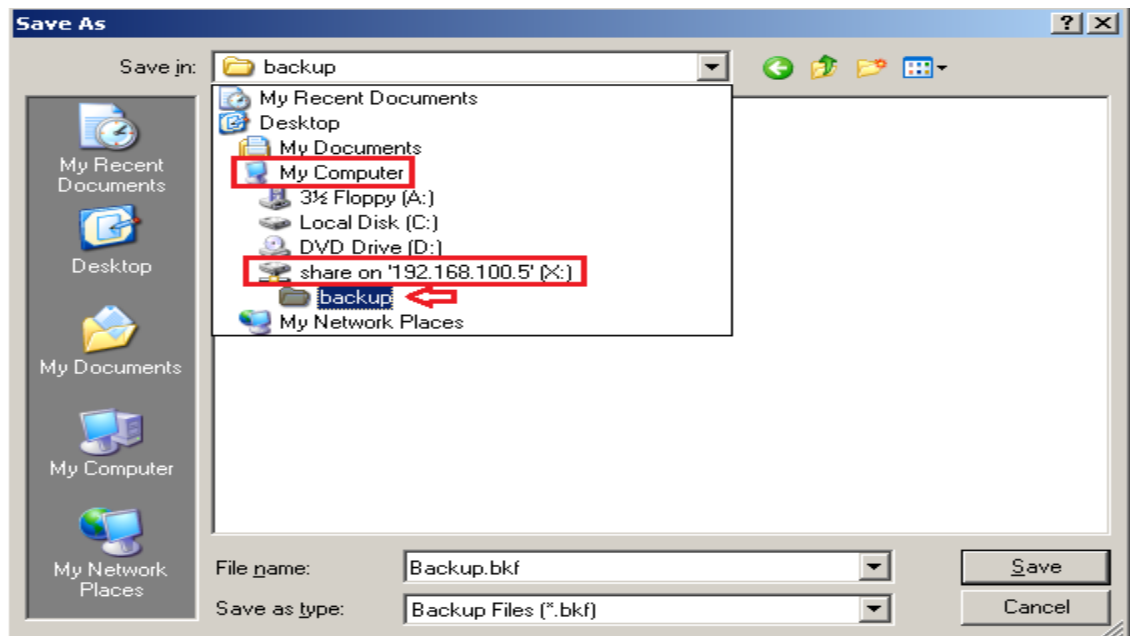


Figure 35: Browse to Location

31. Verify that the place to save the backup is **X:\backup**. Click **Next**.

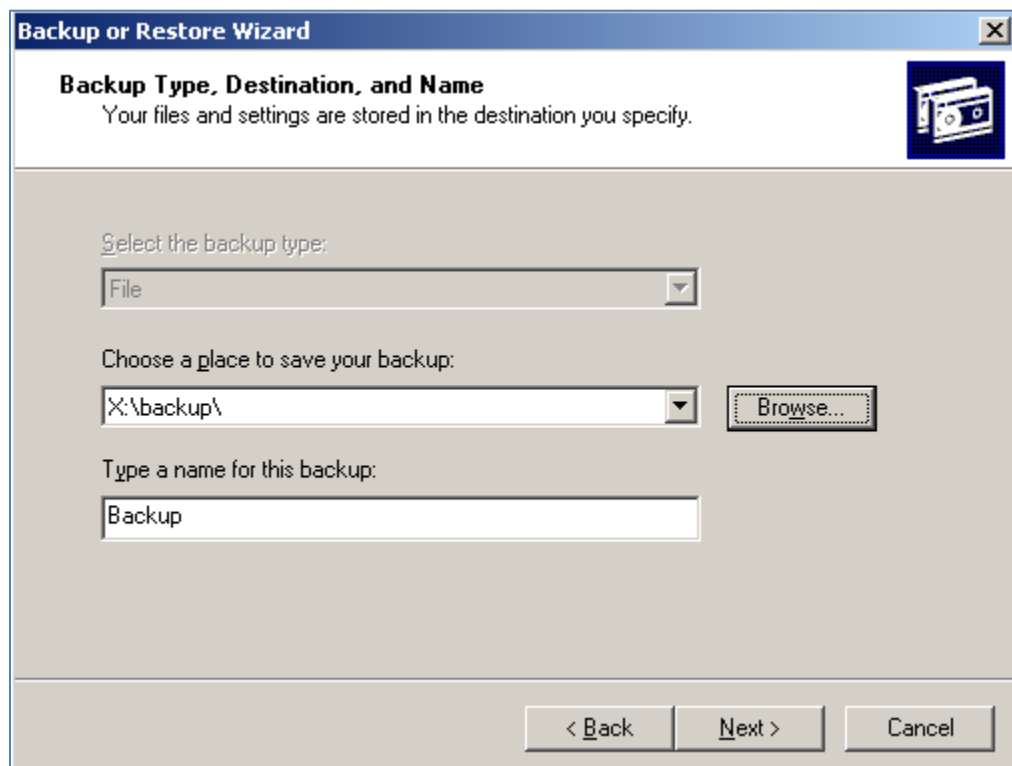


Figure 36: Backup Path

32. Click **Finish** at the Completing the Backup or Restore Wizard.

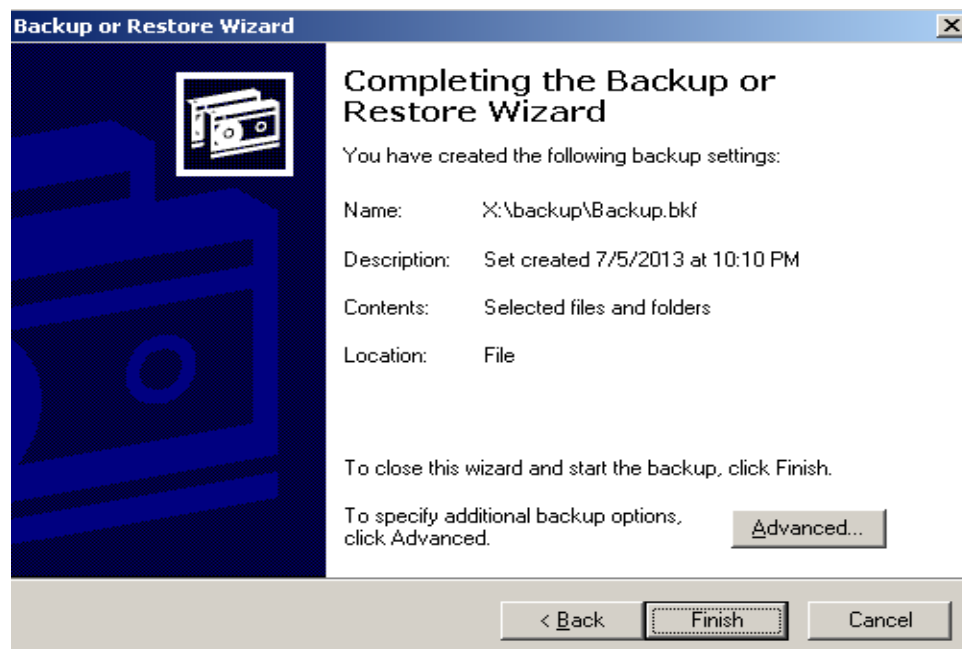


Figure 37: Completing the Backup

33. Monitor the Backup Progress and wait until it reaches 100 percent.

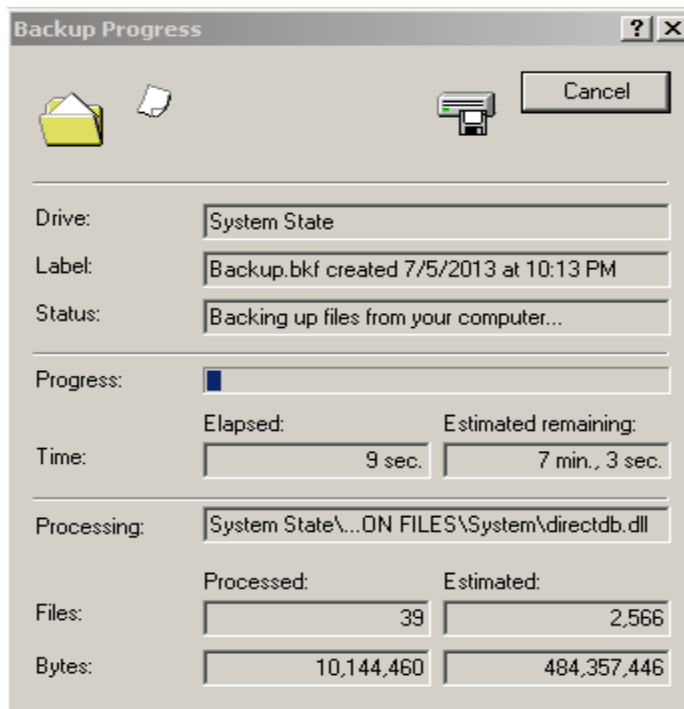


Figure 38: Backup in Progress

34. When the backup is complete, click **close**.

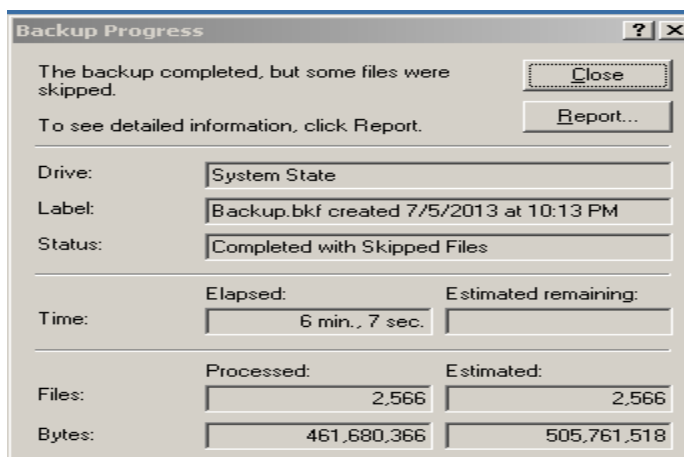


Figure 39: Backup is Complete

35. Go back to the Windows 7 Attack machine, go to the **shares** directory on the root of C: and then open the **backup** folder. Next, right click on **Backup.bkf**. In the submenu, hover over **7-Zip** and select **Add to "backup.7z"**

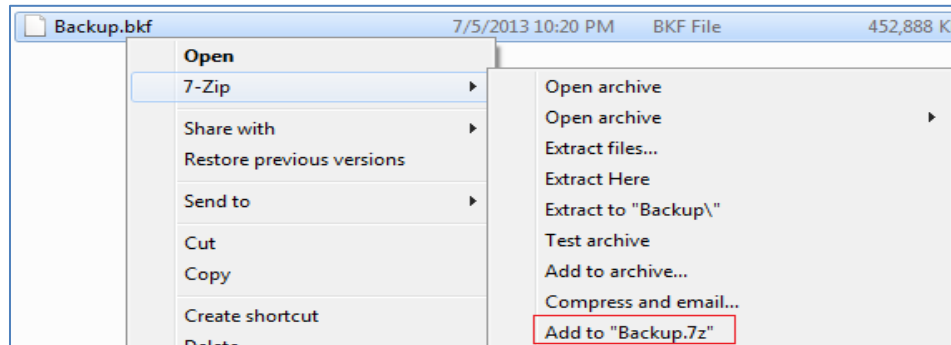


Figure 40: 7-zip the File

1.2 Conclusion

The net use command can be used to map a drive on a remote system, and can also be utilized to display all mapped drives. A network drive can be used to retrieve or store files. In order to store data to a network drive, write permissions are required.

1.3 Discussion Questions

1. What command allow you to start a backup on Windows 2003 server?
2. What command allows you to map a drive from the command line?
3. What command allows you to view all of your network shares
4. What is the System State?

2 Backing Up Files to an FTP Server

File Transfer Protocol (FTP) can be used to transfer files from one system to another. The disadvantage of using FTP is that it sends the user name, password, and data, over the wire in clear text. If security is paramount, use secure copy (SCP).

2.1 Backing up Files to an FTP Server

In this exercise, we will backup files to the Red Hat Enterprise Linux Internal Victim Machine.

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

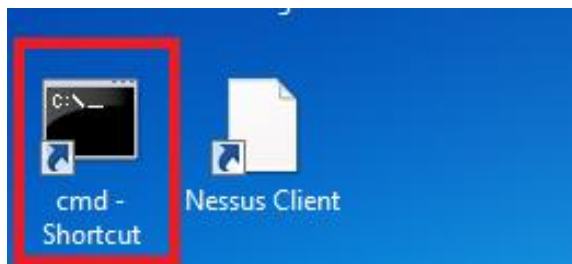


Figure 41: Opening the Command Prompt

2. Type the following command to ftp to the Red Hat Enterprise Linux Internal Victim Machine;
C:\ftp 192.168.100.147

```
C:\>ftp 192.168.100.147
Connected to 192.168.100.147.
220 (vsFTPd 2.0.5)
User (192.168.100.147:(none)):
```

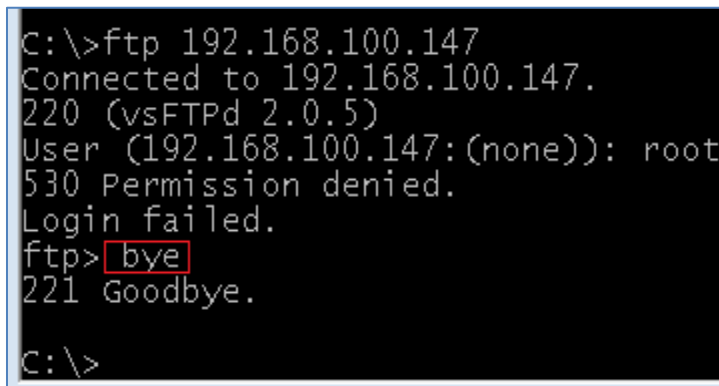
Figure 42: FTP to the Remote Site

3. Type **root** for the username. You will receive a **Permission denied** message.

```
C:\>ftp 192.168.100.147
Connected to 192.168.100.147.
220 (vsFTPd 2.0.5)
User (192.168.100.147:(none)): root
530 Permission denied.
Login failed.
ftp>
```

Figure 43: Login Failed

4. Type the following command to leave the ftp sub-prompt on Windows:
ftp> **bye**

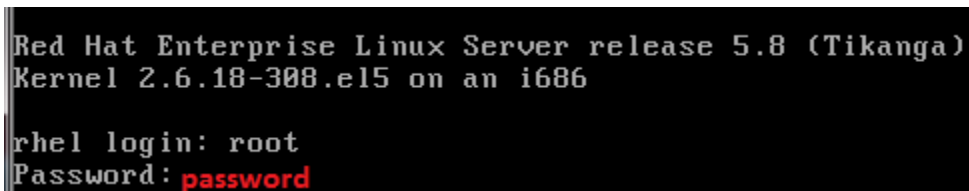


```
C:\>ftp 192.168.100.147
Connected to 192.168.100.147.
220 (vsFTPd 2.0.5)
User (192.168.100.147:(none)): root
530 Permission denied.
Login failed.
ftp> bye
221 Goodbye.
C:\>
```

Figure 44: Leaving the FTP Session

The FTP protocol sends the user name and password in clear text. For that reason, the server is not configured to allow root to use ftp. We will create a different account.

5. Log on to the Red Hat Enterprise Linux Internal Victim Machine, with the username of **root** and password of **password**.



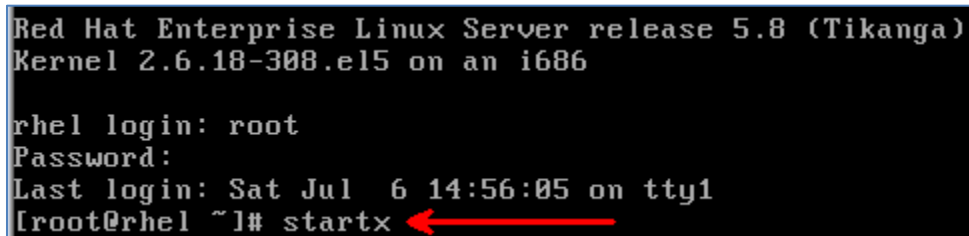
```
Red Hat Enterprise Linux Server release 5.8 (Tikanga)
Kernel 2.6.18-308.el5 on an i686

rhel login: root
Password: password
```

Figure 45: Logging In

The password will not be displayed for security purposes.

6. Type the following command to launch the Graphical User Interface
[root@rhel ~]# **startx**



```
Red Hat Enterprise Linux Server release 5.8 (Tikanga)
Kernel 2.6.18-308.el5 on an i686

rhel login: root
Password:
Last login: Sat Jul  6 14:56:05 on tty1
[root@rhel ~]# startx
```

Figure 43: Starting the X Server

7. Right-click on the desktop and select **Open Terminal** to open a terminal

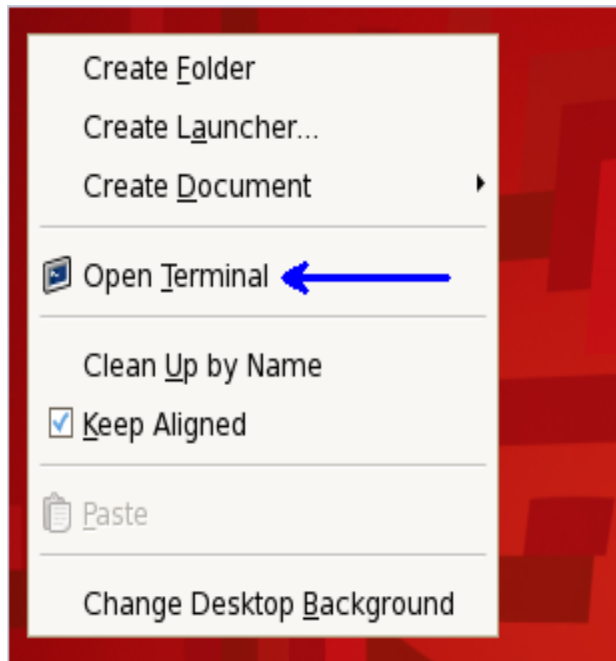


Figure 46: Opening a Terminal on Linux

8. Type the following command to add a user to the system named jesse:
`[root@rhel ~]# useradd jesse`

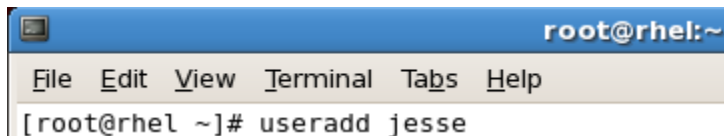


Figure 47: Adding a User

9. Type the following command to set the password for the user jesse:
`[root@rhel ~]# passwd jesse`

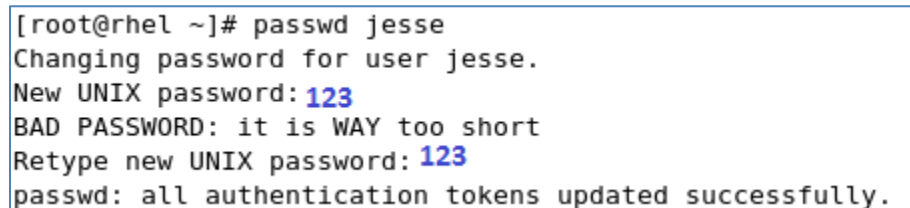


Figure 48: Changing the Password

10. To view the home folder created for **jesse**, type the following command:

```
[root@rhel ~]# ls /home  
jesse student
```

Figure 49: The Home Folder

11. On the **Windows 7 Internal Attack Machine**, type the following command to move the backup.7z to the root directory:

```
c:\>move c:\share\backup\Backup.7z c:\
```

```
c:\>move c:\share\backup\Backup.7z c:\  
1 file(s) moved.
```

Figure 50: Moving the Backup.7z file

12. Type the following to ftp to the Red Hat Enterprise Linux Internal Victim Machine:

```
C:\ftp 192.168.100.147
```

```
C:\>ftp 192.168.100.147  
Connected to 192.168.100.147.  
220 (vsFTPd 2.0.5)  
User (192.168.100.147:(none)):
```

Figure 51: FTP to the Remote Site

13. For the ftp user name, type **jesse**. For the password, type **123**.

```
User (192.168.100.147:(none)): jesse  
331 Please specify the password.  
Password: 123  
230 Login successful.
```

Figure 52: Username and Password

14. During the FTP Session, type the following command to switch to binary mode:
ftp> bin

```
ftp> bin  
200 Switching to Binary mode.
```

Figure 53: Switch to Binary Mode

15. Type the following to upload the compressed backup file to the FTP Server.

ftp> **put Backup.7z**

```
ftp> put Backup.7z
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 File receive OK.
ftp: 137159834 bytes sent in 4.48Seconds 30588.72Kbytes/sec.
ftp>
```

Figure 54: Uploading Backup.7z

16. Type the following command to leave the ftp sub-prompt on Windows:

ftp> **bye**

```
226 File receive OK.
ftp: 137159834 bytes sent in 4.48Seconds 30588.72Kbytes/sec.
ftp> bye
221 Goodbye.

c:\>
```

Figure 55: Leaving FTP

17. On the Red Hat Enterprise Linux Internal Victim Machine , type the following to view the uploaded file:

[root@rhel ~]# **ls /home/jesse/**

```
[root@rhel ~]# ls /home/jesse/
Backup.7z
```

Figure 56 Viewing the Uploaded File

2.2 Conclusion

FTP is a great way to move files from one system to another. The disadvantage to using FTP is that the user name and password are sent over the network in plain text.

2.3 Discussion Questions

1. What is the command to add a user from the command line in Linux?
2. What is the command to change a user's password in Linux?
3. When a user is added to a Linux system, where is there home folder located?
4. What is the disadvantage of using the FTP protocol to transfer files?

3 Backing up Files using SCP

Secure copy (SCP) is a means of securely transferring files between a local host and a remote host or between two remote hosts, based on Secure Shell (SSH) protocol. Files can be uploaded using the SSH protocol with SCP. The files will be encrypted when sent over the network.

3.1 Using SCP

In this exercise, we will backup files using SCP to the BackTrack Internal Linux Server.

1. On the **BackTrack 5 Internal Attack Machine**, open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen in BackTrack version 5 R1.

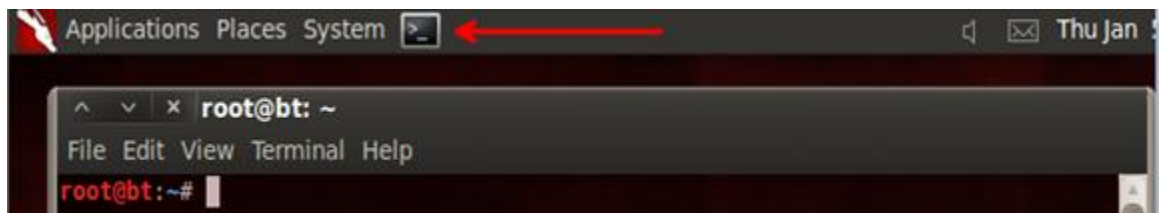


Figure 57: The Terminal Windows within BackTrack

2. Type the following to determine if an SSH server is running.
root@bt:~#netstat -tan



Figure 58: The netstat Command

3. To generate the Secure Shell Keys, type the following command:
root@bt:~#ssh-keygen

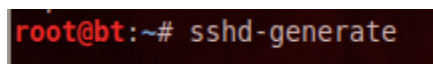


Figure 59: ssh-keygen

- You will see a message that says the Public and Private Key are generated.

```
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
81:5c:4e:10:65:c8:24:31:36:e7:ad:d7:a6:92:98:61 root@bt
The key's randomart image is:
+--[ DSA 1024]-----+
  *+==
  . BoB
    + +
    . o
  E . S o
    + o o
    o o .
  .
+-----+
backtrack
```

Figure 60: Key Generation

- From the **Applications** menu, select **BackTrack, Services, SSHD, sshd start**

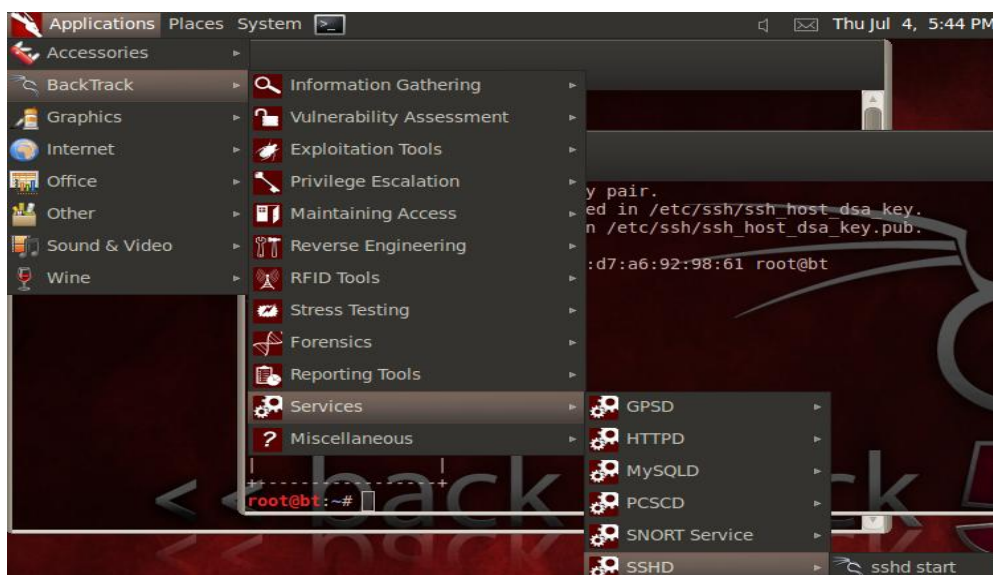


Figure 61: Starting SSHD

- On BackTrack, Type the following to determine if an SSH server is running.
root@bt:~#netstat -tan

```
root@bt:~# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:7175          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::1:7175                :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

Figure 62: The netstat command

7. On the **Red Hat Enterprise Linux Internal Victim Machine**, Right Click on the desktop and select **Open Terminal**.

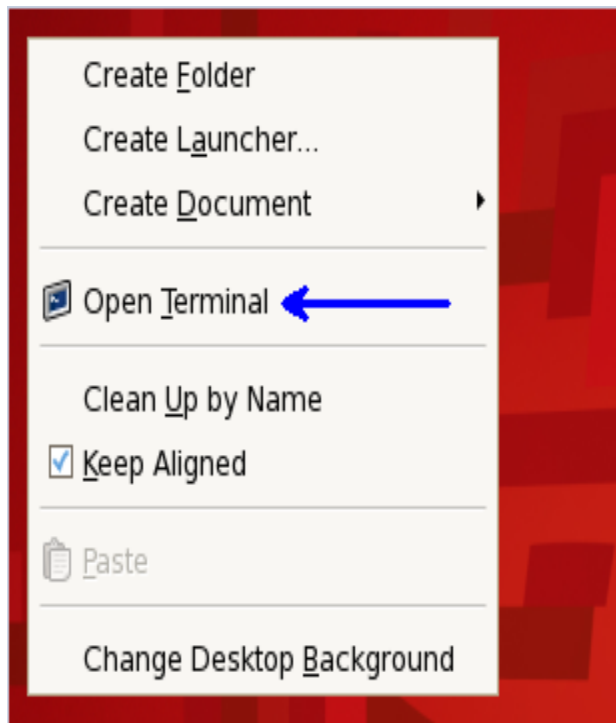


Figure 63: Opening a Terminal on Linux

8. Type the following command to enter the user's home directory:

```
[root@rhel ~]# cd /home/jesse/
```

Figure 64: Changing Directories

9. Type the following command to backup the file using SCP to the remote Linux system:

```
[root@rhel jesse]# scp Backup.7z root@192.168.100.3:/root
```

- When you are asked if you are sure you want to continue connecting, type **yes**.
- When you are asked for root@192.168.100.3's password, type **password**.

```
[root@rhel jesse]# scp Backup.7z root@192.168.100.3:/root
The authenticity of host '192.168.100.3 (192.168.100.3)' can't be established.
RSA key fingerprint is 0e:f5:39:c3:c4:cf:51:16:f7:b5:ec:60:cc:9c:26:76.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.100.3' (RSA) to the list of known hosts.
root@192.168.100.3's password: password
Backup.7z                                     100% 131MB 26.2MB/s 00:05
```

Figure 65: Start Menu

3.2 Conclusion

Secure Copy (SCP), can be used to copy files securely from one system to another. In order to use SCP, an SSH server must be running on the destination machine. Most versions of Linux and Unix support SSH natively. When you copy a file to a remote Linux system, you need to specify the user name, IP address, and destination location.

3.3 Discussion Questions

1. What command can be used to determine if an ssh server is running?
2. What needs to be done before starting the SSH Service?
3. How is sshd started from the BackTrack menu?
4. What needs to be specified when you copy a file using Secure copy (SCP)?

References

1. The useradd Command:
<http://www.computerhope.com/unix/useradd.htm>
2. The passwd command:
<http://www.computerhope.com/unix/upasswor.htm>
3. Net use command:
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/net_use.mspx?mfr=true
4. SCP:
<http://linux.die.net/man/1/scp>
5. ntbackup:
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ntbackup_command.mspx?mfr=true