**Lab 1.1 Encrypting a File and Folder**

*Objective*: To provide security for a particular file and folder, enable encryption using Windows 7

*Parts*: A computer with Windows 7 loaded with at least one NTFS partition

1. Open *Windows Explorer*. Create a text file called *Security Test.txt* and save in the *Documents* folder.
2. Right-click the *Security text.txt* file and select *Properties*. From the *General* tab, select the *Advanced* button.
3. Enable the *Encrypt contents to secure data* and click *OK*. Click the *Apply* button and review the warning message.



1. The default would be to encrypt the Security text.txt file and to encrypt the *Documents* folder. This may not be what you want to do. Select the *Encrypt the file only* radio button and the *OK* button on the screen and the one that follows.
2. In Windows Explorer, click on an empty spot in the right pane.

Is there any indication the file is encrypted? If so, what is it?

**9.** In Windows Explorer, access the *Properties* window of the *Security text.txt* file again and select the *Advanced* button. From the *Advanced Attributes* window, select the *Details* button. If this is not available, ensure you are on a file (and not a folder).

What user(s) can access the encrypted file?

**10.** Notice the certificate thumbprint number to the right of the user. EFS can request a digital certificate from a CA (certificate authority) such as a server or if one is not available, EFS can use a self-signed certificate.

What are the first 16 hexadecimal digits used for the digital certificate?

Compare these digits with a fellow classmate. Are the digital certificates the same?

If so, why do you think they are the same?

If they are different, why do you think they are different?

**11.** Notice the data recovery agent section at the bottom of the window. One or more users (such as the administrator) can be designated as a data recovery agent. A data recovery agent is issued a recovery certificate used for EFS data recovery on encrypted files. Click *Cancel* on three different windows to exit the *Properties* window.

**12.** From Windows Explorer, open the *Security Test.txt* file, modify it, and save it.

From Windows Explorer, does the file appear to still be encrypted?

**13.** Log off the computer and log back on as a different user. If a different user does not exist, create one by using the *User Accounts* Control Panel if possible.

**14.** Use Windows Explorer, to locate and open the *Security Test.txt* file located under the other username. Modify the file and save it, if possible.

Were there any problems opening, modifying, or saving the file?

In one or more complete sentences, explain what happened and why you think it occurred this way.

**15.** Log off the computer and log back on as the original user.

**16.** Access the *My Documents/Documents* folder and create a new folder called *Test*. Copy the *Security Test.txt* file into the new *Test* folder.

Is the copied file encrypted in the *Test* folder?

**17.** Within the *Test* folder, create a new text file called *Security Test2.txt*.

Is the newly created file encrypted?

**18.** Encrypt the *Test* folder using the default encryption setting.

Does it change anything within the folder? If so, what does it change?

**19.** Within the *Test* folder, create and save a new file called *Security Test3.txt*.

Is the newly created file encrypted?

**20.** Delete the *Security Test.txt*, *Security Test2.txt*, and *Security Test3.txt* files.

Was there any indication that the files were encrypted when they were deleted?

**21.** Permanently delete the *Test* folder and any files created in the *My Documents/Documents* folder.

**Lab 15.2 Using Windows 7 System Protection**

*Objective*:   To manually control the settings involved with system restore points using System Protection

*Parts*:          A computer with Windows Vista/7 loaded with at least one NTFS partition

*Note*:          This lab requires local administrator rights.

*Procedure*:  Complete the following procedure and answer the accompanying questions.

**1.** Power on the computer and log on using the user ID and password provided by the instructor or lab assistant.

**2.** Access Windows Explorer and right-click *Computer* > *Properties* > *System Protection* tab.

In the *Protection Settings* section, document the available drives.

Document whether protection is currently on or off for each of the available drives.

**3.** Click *Configure*.

What three options are available for *Restore Settings*?

Microsoft says, “System Protection can keep copies of system settings and previous versions of files.” Do you think that this means system files, user data files, or both? Explain your reasoning.

Thinking as a technician, which setting is optimum for most users?

Give one situation where you think that a technician would select the *Only restore previous versions of files* option.

Give one situation where a technician would recommend the *Turn off system protection* option.

**4.** Ensure that the *Restore system settings and previous versions of files* radio button is enabled. By default, Windows uses a maximum of 10 percent of the hard drive for System Protection. However, the system allows you to adjust this amount in the Disk Space Usage section. Note that if you turn off system protection, you cannot use System Restore.

What is the current *Max Usage*?

Describe a situation where a technician would want to configure the machine for more than 10 percent of the hard disk space reserved for system protection.

**5.** Click *Cancel*.

Can a restore point be manually created from the System Properties window? [ Yes | No ]

**6.** Click *Cancel*.

***Instructor initials:*** \_\_\_\_\_\_\_\_\_\_\_\_\_

**Lab 15.5 Sharing a Folder in Windows 7**

*Objective*:   To be able to share a folder and understand the permissions associated with a network share

*Parts*:          Access to two Windows 7 computers with a user ID that has administrator rights

*Procedure*:  Complete the following procedure and answer the accompanying questions.

**1.** Turn on both computers and verify that the operating system loads. Log in to Windows 7 using the user ID and password that has full administrator rights and that is provided by your instructor or lab assistant.

**2.** On the first computer, use Windows Explorer to created two folders under *Documents*. Name the folders *READ* and *WRITE*.

**3.** Within the *READ* folder, create a text document called *readme.txt*. Within the *WRITE* folder, create a text file called *changeme.txt*.

**4.** On both computers, determine the computer name by accessing the *System* Control Panel link. Determine the IP addresses of both computers using the ipconfig command.

Document your findings.

**5.** On both computers, access the *Network and Sharing Center* Control Panel link to document the current *Advanced Sharing Settings*.

**6.** On both computers, enable the following settings.

• File and Printer Sharing

• Public folder sharing

• Network discovery

**7.** On both computers, ensure that the Windows 7 *Use Sharing Wizard* is enabled by typing folder options in the *Search programs and files* Start button option. Select the *Folder Options* item from the resulting list > *View* tab > locate the *Advanced Settings* section > locate the *Use Sharing Wizard (Recommended)* option and ensure it is enabled. Apply changes as necessary.

What is the current setting for the *Use Sharing Wizard* option? [Enabled | Disabled]

**8.** In Windows Explorer on the first computer, right-click the *READ* folder > *Properties* > *Sharing* tab.

Document the share network path that appears in the window.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**9.** Select the *Advanced sharing* button > enable the *Share this folder* checkbox > select the *Caching* button.

**10.** Select the *Configure Offline Availability for a Shared Folder help* link.

What is the purpose of caching?

[Y | N] Is offline availability enabled by default for a shared folder?

What command can be used from a command prompt to configure caching options for a shared folder?

**11.** Close the help window.

**12.** In the Offline Settings window, leave the option to the default.

What is the default setting for offline access?

**13.** Click *OK*. In the Advanced Sharing window, select the *Permissions* button. Notice how the Everyone group is listed by default.

*Notes*: If you want to share with someone who is not listed, use the *User Accounts* Control Panel to create the account, then select that account name in the Permissions window.

If the local or domain policy requires a password, one should be put on the user account. Best practice is to require passwords on all user accounts.

If the Everyone user account is selected and password protection is being used, a user account is still needed to gain access.

What permissions are enabled by default for the Everyone group? [Full control | Change | Read]

**14.** Click *OK* on the two windows and then click the *Close* button.

**15.** Open the *Computer Management* console. Expand *System Tools* and *Shared Folders*. Click *Shares* in the left pane. The READ share lists in the right pane. If the share is missing, redo this lab from the beginning. Close the *Computer Management* window.

**16.** On the second computer, log on as the user given access in Step 13 or use the user ID and password provided by the instructor or lab assistant.

**17.** On the second computer, open *Windows Explorer*. Select *Network* in the left pane. In the right pane, locate and double-click the name of the first computer.

*Notes*: If the computer does not list, click the *Start* button and in the *Search programs and files* textbox, type \\computer\_name (where computer\_name is the name of the first computer). Press .

**18.** On the second computer, locate the *READ* share and the *readme.txt* document. Double-click the *readme.txt* file.

[ Y | N ] Did the file open?

**19.** Add a few words to the file. Click the *File* > *Save* menu option. Leave the filename the same and click the *Save* button. When asked if you want to replace the file, click *Yes*.

[ Y | N ] Did the file save?

**20.** Close the file and close the window that contains the file.

**21.** On the second computer inside the *Search programs and files* Start button option, type the share path documented in Step 8 and press . If an error occurs, check your typing or redo the steps to get a correct share path documents in Step 8.

What happened?

**22.** Close the window. On the second computer, open *Windows Explorer*. Right-click *Computer* in the left pane and select *Map Network Drive*. Use the *Drive* drop-down menu to select a drive letter. In the *Folder* textbox, type the share path for the READ share documented in Step 8. Click *Finish*. The share opens with the drive letter documented in the path at the top of the window. Note that you may have to expand the left pane to see the drive letter.

***Instructor initials:*** \_\_\_\_\_\_\_\_\_\_\_\_\_

**23.** On the second computer, again access *Windows Explorer* and locate the drive letter that was just mapped to a network drive. Because Windows share paths can be lengthy, a common practice is to use a mapped network drive for the share.

How can you easily identify mapped drive letters in Windows Explorer (besides a quite high drive letter in some cases)?

**24.** Close all windows on the second computer.

**25.** In Windows Explorer on the first computer, right-click the *WRITE* folder > *Properties* > *Sharing* tab.

Document the share network path that appears in the window.

**26.** Select the *Advanced Sharing* button > enable the *Share this folder* checkbox.

**27.** Select the *Permissions* button.

**28.** Select the correct username or group and enable the *Change Allow* checkbox. Click *OK* on two windows and then click the *Close* button.

**29.** On the second computer, locate the *changeme.txt* document.

**30.** Modify and save the *changeme.txt* file.

**31.** On the first computer, open the *changeme.txt* file.

[Y | N] Was the file changed?

***Instructor initials:*** \_\_\_\_\_\_\_\_\_\_\_\_\_

**32.** On the second computer, try changing the name of the *changeme.txt* file.

[Y | N] Could you change the name of the *changeme.txt* file?

**33.** Verify whether the filename changed on the first computer.

[Y | N] Did the filename change on the first computer? If so, what is the new name?

**34.** On the second computer, right-click the *WRITE* folder and select *Always available offline*.

What indication is given that a folder is available offline?

[Y | N] Can a particular file be given this same attribute?

**35.** Disconnect the second computer from the network by removing the network cable from the network adapter.

**36.** From a command prompt on the second computer, ping the first computer using the IP address documented in Step 4.

[Y | N] Did the ping succeed?

**37.** So with no network access, open the *WRITE* folder and access the *changeme.txt* file. Modify the file and save it.

**38.** Reconnect the second computer to the network.

**39.** From the first computer, access the *WRITE* folder.

[Y | N] Were the document changes made when computer two was disconnected from the network saved on the first computer?

**40.** On the second computer, again access the *changeme.txt* file and try to permanently delete the file.

[Y | N] Could you permanently delete the *changeme.txt* file?

**41.** On the first computer, create a subfolder under the *READ* folder. Name the folder *SUB\_READ*. Create a text file in the *SUB\_READ* folder called *sub\_file.txt*.

**42.** On the second computer, locate and right-click the *SUB\_READ* shared folder. Select *Properties*.

What attributes does this folder have? [Read-only | Hidden | None]

**43.** On the second computer in *Windows Explorer*, locate the *sub\_file.txt* file. Select *Properties*.

What attributes, if any, are shown as enabled by default? [Read-only | Hidden | None]

**44.** Click *Cancel*. Try to modify the *sub\_file.txt* file.

[Y | N] Could you change the *sub\_file.txt* file?

***Instructor initials:*** \_\_\_\_\_\_\_\_\_\_\_\_\_

**45.** On the second computer, remove the mapped drive (and any drive that you created on your own) by using *Windows Explorer* to locate the mapped drive letter under *Computer* in the left pane. Right-click the mapped drive and select *Disconnect*.

**46.** On the first computer, permanently delete the *READ* and *WRITE* folders and all files and subfolders contained within them.

**47.** On the first computer, put the *Advanced sharing settings* options back to the original configuration. Refer to the documentation in Step 5. Put the *Use Sharing Wizard* back to the original setting as documented in Step 7. Show your lab partner the documented settings and the current configuration. Have your lab partner use the table that follows to document that the computer has been put back to the original configuration.

**48.** On the second computer, put the *Advanced sharing settings* options back to the original configuration. Refer to the documentation in Step 5. Put the *Use Sharing Wizard* back to the original setting as documented in Step 7. Show your lab partner the documented settings and the current configuration. Have your lab partner use the table that follows to document that the computer has been put back to the original configuration.

**49.** On both computers, delete any user accounts that have been created. Note that you must be logged in as an administrator in order to delete user accounts.

**Lab 15.7 Windows Defender in Windows 7**

*Objective*:   To be able to use System Configuration and Windows Defender to troubleshoot boot and spyware problems

*Parts*:          Computer with Windows 7 installed

User logon that has administrator rights

*Note*:          In this lab, you will explore various options that can be used within the System Configuration and Windows Defender windows.

If the computer has a third-party security suite such as Norton or McAfee that has antispyware or antimalware, the Windows Defender application may not be enabled.

*Procedure*:  Complete the following procedure and answer the accompanying questions.

**1.** Turn on the computer and verify that the operating system loads. Log in to Windows 7 using the user ID and password provided by your instructor or lab assistant.

**2.** Open *Windows Explorer*. From the *Organize* menu option > *Folder and Search Options* > *View* tab.

What is the current setting for the Hidden files and folders section? [Do not show hidden files and folders enabled | Show hidden files and folders enabled]

What is the current setting for the *Hide extensions for known file types* option? [Enabled | Disabled]

What is the current setting for the *Hide protected operating system files (Recommended)* option? [Enabled | Disabled]

**3.** Configure the following Windows Explorer settings:

• *Show hidden files, folders, and drives radio button*—enabled (checked)

• *Hide extensions for known file types*—disabled (unchecked)

• *Hide protected operating system files (Recommended)*—disabled (unchecked)

Click *Yes* (if prompted) > *Apply* > *OK*. Close *Windows Explorer*.

**4.** Open the *Start* menu and in the *Search Programs and Files* textbox, type defender > click *Windows Defender*. Note that if a note appears that Windows Defender is turned off, select the *click here to turn it on* option. You might have to obtain updates before continuing.

Was Windows Defender disabled? [ yes | no ]

**5.** Select the *Tools* menu option > *Options*.

What actions are defined from this window?

**6.** Select the *Tools* menu option > *Quarantined items*.

List any software that Windows Defender has prevented from executing.

**7.** Select the *Tools* menu option > *Allowed items*.

List any software that is not be monitored by Windows Defender.

What happens if an item is removed from the list and how did you find this information?

**8.** Select the *Tools* menu option > *Options* > *Real-time protection* from the left pane.

Is real-time protection enabled? [ yes | no ]

What options are available besides enabling real-time protection?

**9.** Select *Excluded file types* from the left pane.

What file extension is given as an example of a file type to exclude?

**10.** Select the *Advanced* option from the left pane.

What type of scanning is enabled? [ scan archive files | scan email | scan removable drives | use heuristics | create restore point ]

What will a machine do if it uses heuristics?

**11.** Select *Advanced* from the left pane.

What two options are configured from here?

**12.** If Windows Defender was disabled when you started this lab. See the answers found in Steps 6 and 8. Deselect the *Use this program* checkbox. If Windows Defender was disabled when you started this lab, click *Automatic scanning* from the left pane. Ensure the *Automatically scan my computer (recommended)* option is disabled (unchecked). Click *Save*. You receive a message that Windows Defender is turned off.

**13.** Return Windows Explorer to the original settings. See the settings as the answers found in Step 2.

**14.** Show the instructor that the settings are re-configured to the original settings.

***Instructor initials:*** \_\_\_\_\_\_\_\_\_\_\_\_\_

**16.** Close the *Windows Defender* window.

**Lab 15.8 Configuring a Secure Wireless Network**

*Objective*:   To be able to configure a secure wireless AP (access point) or router and attach a wireless client

*Parts*:          One wireless access point or router

A computer with an integrated wireless NIC or a wireless NIC installed as well as an Ethernet NIC

One straight-through cable

*Procedure*:  Complete the following procedure and answer the accompanying questions.

**1.** Obtain the documentation for the wireless AP or router from the instructor or Internet.

**2.** Reset the wireless AP or router as directed by the wireless device manufacturer.

Document the current Ethernet NIC IPv4 settings. [ DHCP | static IP address ]

If a static IP address is assigned, document the IP address, subnet mask, default gateway, and DNS configuration settings.

**3.** Attach a straight-through cable from the computer’s Ethernet NIC to the wireless AP or router.

**4.** Power on the computer and log on, if necessary.

**5.** Configure the computer with a static IP address or DHCP, as directed by the wireless device manufacturer.

**6.** Open a web browser and configure the wireless AP or router with the following parameters:

• Change the default SSID

• Disable SSID broadcasting enabled for this lab

• Configure the most secure encryption and authentication supported by both the wireless NIC client and the wireless AP or router

• Change the default password used to access the wireless AP or router

Document the settings after you have configured them:

SSID:

SSID broadcasting disabled? [ yes | no ]

Password for wireless device access:

Type of security used:

**7.** Save the wireless AP or router configuration.

**8.** Disconnect the Ethernet cable.

**9.** Enable the wireless NIC and configure it for the appropriate SSID.

**10.** Configure the wireless NIC for a static IP address or DHCP, as directed by the wireless AP/router manufacturer.

**11.** Open a web browser and access the wireless AP or router. If access cannot be obtained, troubleshoot as necessary or reset the wireless AP or router to default configurations and restart the lab.

What frequency (channel) is being used by the wireless AP or router and the wireless NIC for connectivity?

**12.** Show the instructor the connectivity.

***Instructor initials:*** \_\_\_\_\_\_\_\_\_\_\_\_\_

**13.** Open a command prompt and type netsh wlan show settings to see the wireless network settings.

**14.** If Windows XP is being used, use the sc query w2csvc command. (Vista/7 do not have the Wireless Zero Control service.)

**15.** Reset the wireless AP or router to the default configuration settings.

**16.** Reset the computer(s) to the original configuration settings.

***Instructor initials:*** \_\_\_\_\_\_\_\_\_\_\_\_\_