<CHN>CHAPTER TWELVE

<CHT>ACCESS MANAGEMENT

<COOT>Labs included in this chapter

* <COOH1>Lab 12.1 Setting NTFS Permissions
* Lab 12.2 Using NTFS Permissions
* Lab 12.3 Setting and Testing Share Permissions
* Lab 12.4 Auditing Permissions

<COOBT>CompTIA Security+ Exam Objectives

<COOBL>Domain Lab

<COOB>Technologies and Tools 12.1, 12.2, 12.3, 12.4

Identity and Access Management 12.1, 12.2, 12.3, 12.4

# <H1>Lab 12.1 Setting NTFS Permissions

<H2>Objectives

<TX1>An access control list (ACL) is the foundation of access control. It is associated with Windows files, folders, drives, printers, and so on. The ACL is actually an attribute of the object, such as a file or folder. It contains access control entries that specify the security principals (user accounts, group accounts, computer accounts) with access to the object and what that level of access is (permissions). For example, the modify permission allows a user to change or delete a file, whereas the read permission allows reading the file but prohibits changing or deleting it.

<TX2>Windows uses two types of permissions: Share and NTFS (New Technology File System). You will work with Share permissions later in this chapter. In this lab, you work with NTFS permissions. Note that NTFS permissions can only be applied to objects on partitions that are formatted in NTFS. NTFS permissions apply to folders and files and are in effect whether the user accesses the resource locally (logs on to the computer that hosts the resource) or remotely (accesses the resource over the network from a different computer).

<TX2>After completing this lab, you will be able to:

* <BL>Determine NTFS permissions of security principals
* Set NTFS permissions
* Create, implement, and test group policy objects

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016

**<H2>Activity**

<FE1TX1>Estimated completion time: **15–20 minutes**

<TX1>In this activity, you create a folder, examine the NTFS permissions that apply to the folder, and then modify NTFS permissions for a security group.

1. <NL\_FIRST>Log on to Windows Server as Administrator.
2. <NL\_MID>Click the Folder Icon on the task bar, click **This PC**, then double-click Local Disk (C:).
3. To create a Sales folder on the C drive, do the following: in the root of C:, right-click the white space in the right pane; click New; and then click Folder. In the highlighted file name box, type Sales and press Enter.
4. Double-click the Sales directory to open it. Right-click the white space in the right pane, click New, and click Text Document. Name the document January.
5. Return to the root of C:. Right-click the Sales folder, click Properties, and click the Security tab. Your results should be similar to what is shown in Figure 12-1. In the Group or user names box, only security groups are listed. (The icon to the left of the group names shows two people, which indicates that the item is a group. If it were a user account, there would only be one person in the icon.)

[Insert Figure 12-1 Here]

1. There are four security groups listed as having NTFS permissions to the Sales directory: SYSTEM, Administrators, Users, and if you completed previous labs then Sales Manager and Sales Associates groups will also appear. It seems clear that the Administrators and Users groups are security entities that are stored in the local computer’s security accounts management database because the parenthetical additions list the hostname of the computer. The SYSTEM account is to give operating system processes access to the folder. But what about Authenticated Users? How are they different from Users? If Authenticated Users does not appear in the window, click Edit, then click Add. In the “Enter the object name to select” box, type Authenticated and then click Check Names. Click OK twice. Leave the Sales Properties window open. Open the Administrative tools window.
2. In Server Manager, click Tools, Active Directory Users and Computers, then right-click the Users folder (see Figure 12-2). Click New, then click User.

[Insert Figure 12-2 Here]

1. Click the Users group in the left pane, and then create a non-administrative user named Nicole Diver with the username ndiver and the password Pa$$word. Close the Active Directory Users and Computers window.
2. Close the Sales Properties window. Open C:\Sales, right-click January, and then click Properties. Click the Security tab. Click each of the security groups one at a time and watch the permissions change in the Permissions window. Notice that the Authenticated Users group has more permissions than the Users group. Examine the permissions shown from Full control through Special permissions at the bottom. Notice that the check marks in the Allow column are a faded gray. This indicates that the permissions are inherited from the container in which the January file was placed—that is, C:\Sales. In the January Properties window, click Edit.
3. By experimentation, you can determine that you can add permissions but you can’t change any permissions that are already set. Do not add any permissions. Click Users (Windows Server\Users) and click Remove. The resulting error message discusses the need to block inheritance of permissions before such an action can be taken. Click OK and click Cancel in the Permissions for January window.
4. In the January Properties window, click Advanced. This window shows more details about the permissions set, but you can’t change permissions on this window. Double-click Authenticated Users in the Permission entries box. Here, you see the detailed NTFS permissions that are combined to create the standard NTFS permissions you saw in Step 5 and in Figure 12-1. You may have to click the Show advanced permissions link to see all permissions. Scroll through these permissions. Note that when an entry has more than one permission separated by a backslash, the permission on the left would be in force if the object were a directory; however, if the object were a file, as is the case here, the permission on the right of the backslash applies. By clicking around this window, you’ll discover that you cannot change permissions. Click Close on the Permission Entry for January window. Navigate to the C:\Sales\January.txt document, right-click it, and click Properties. Click the Security tab.
5. Click Users (WINDOWS SERVER\Users). Notice that the permissions are still dimmed. Click Cancel in the January Properties window. Click Advanced, then click Disable inheritance and click Convert inherited permissions into explicit permissions on this object. You are now blocking inheritance of permissions from the root of C:. Select Users and click Edit, then click Select a principal. In the “Enter the object name to select” box, type Administrators and click Check Names, then click OK. Select the administrators for Windows Server, then click OK. In the Permission Entry for January window, click the check box in the Full control row. If necessary, select Allow from the Type drop-down, as shown in Figure 12-3. Click OK three times.
6. You may want to keep the system running while you answer the Review Questions.

[Insert Figure 12-3 Here]

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.

**<H2>Review Questions**

1. <FIB>In this lab, you discovered that there were different default permissions assigned to the Authenticated Users security group and the Users security group. An example of a user who would be able to gain authorized access to a resource on the Windows 10 system but who would not have been authenticated would be one in the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ group.
2. <FIBA>Power Users
3. **IIS\_IUSRS**
4. Replicator
5. Distributed COM Users
6. <TF>Changes to a user’s group membership are not effective until the next time the user logs on. **True** or False?
7. <FIB>You are logged on to a Windows 10 computer that is a member of a domain. You are logged on with the credentials of the domain administrator. You are trying to change the NTFS permissions on a file. You notice that, when you click a check box that already has a check mark in it, you are unable to remove the check mark. The most likely reason is that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
8. <FIBA>the file does not belong to you
9. **the file is inheriting permissions from its parent container**
10. you don’t have permission to modify the file
11. the file is locked
12. <MULT>Which of the following is an example of an NTFS permission? (Choose all that apply.)
13. **<MULTA>Read attributes**
14. **Read permissions**
15. Read only
16. **Take ownership**
17. <MULT>Which of the following statements is true?
18. <MULTA>Access control lists contain the names and passwords of the users to which they provide permissions.
19. By default, non-administrative users cannot change permissions on the files they create.
20. **By default, changing permissions on a folder will result in similar changes of permissions on a file inside that folder.**
21. When a file is deleted and then restored from the Recycle Bin, the file permissions revert to the default permissions for the location to which it was restored.

# <H1>Lab 12.2 Using NTFS Permissions

**<H2>Objectives**

<TX1>In a domain environment, it is important to make distinctions between local accounts and domain accounts. Except for domain controllers, every domain computer holds its own database of local user and groups accounts. Normally, users log on using their domain accounts. This provides them all the benefits and restrictions that have been configured by the domain administrator. Usually, local accounts are used only by junior administrators who are not members of the Domain Admins group. With a local user administrative account, they can perform tasks such as loading drivers and correcting networking configurations.

<TX2>As the Domain Admins group is made a member of the local Administrators group, domain administrators have full access to and control of computers in the domain. That doesn’t mean that network administrators are entitled to access every file and folder. After all, they aren’t administrators of the company, just of the network.

<TX2>In this lab, you learn more about NTFS permissions and how an administrator can recover files for which he has no permissions.

<TX2>After completing this lab, you will be able to:

* <BL>Explain the functional difference between local and domain accounts
* Configure and test NTFS permissions
* Take ownership of files and folders

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016
* Windows 10 VM
* Completion of Lab 12-1

**<H2>Activity**

<FE1TX1>Estimated completion time: **10–15 minutes**

<TX1>In this lab, you configure and test NTFS permissions and take ownership of a file.

1. <NL\_FIRST>Create a user account on the Windows Server for Nicole Diver. Username ndiver, password Pa$$word. Make sure that Nicole Diver’s account is local to Windows Server; and not a domain account. Log onto the server with this account.
2. <NL\_MID>Navigate to C:\Sales. Open January, type I can change this file, and save the file. Try to create a new text file in C:\Sales called February. Delete January. If necessary, click Continue in the File Access Denied box. A User Account Control box appears. Nicole Diver does not have permission to delete the file and, unless she knows an administrative account in the domain, she won’t be able to delete the file even though she has permission to read and modify it. Click No.
3. Navigate to C: and create a directory named Nicole. In C:\Nicole, create a text file called Diver. In the file, type This is Nicole’s file. Save and close the file. Use what you have learned in Lab 12.1 to remove Authenticated Users, Administrators, and Users from the NTFS permissions for C:\Nicole\Diver.txt. However, leave the SYSTEM account. If necessary, add Nicole Diver and assign her full control to the file C:\Nicole\Diver.txt. Your results should look like what is shown in Figure 12-4. Click OK. Log off.

[Insert Figure 12-4 Here]

1. Log on to Windows Server as the domain administrator and navigate to C:\Nicole. Open Diver.txt. Does it seem odd that the administrator of the domain can’t access this file? What if this file contained crucial company information that was needed immediately and Nicole was unreachable? Click OK in the Notepad window and close Notepad.
2. Right-click Diver, click Properties, and click the Security tab. The system reminds you that, because you do not even have permission to view the properties of the object, you need to take ownership of the file. Click the Advanced button, then click Continue. Follow the directions on the dialog and click Change. In the “Enter the object name to select” box, type Administrators, then click Check Names. Click OK, then click Apply. Read the Windows Security window, and click OK. Close the windows until you get to C:\Nicole, right-click Diver, and select Properties. Click the Security tab.
3. Click Edit, click Add, type Domain Admins in the Enter the object name to select box, and click OK. In the Diver Properties window, click Advanced, then select Domain Admins and click Edit. Click Show advanced permissions. If necessary, click to select the boxes for the following items:

<UL>Traverse folder/execute file

List folder/read data

Read attributes

Read extended attributes

Read permissions</UL>

Your results should be similar to what is shown in Figure 12-5.

[Insert Figure 12-5 Here]

1. Click OK three times.
2. Open Diver.
3. You may want to leave the systems running while you answer the Review Questions.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices

**<H2>Review Questions**

1. <FIB>In this lab, an administrator took ownership of a user’s file. If the administrator wanted to hide the fact that she had done so, she could \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
2. <FIBA>use a third-party tool to modify the file’s Date modified attribute
3. **assign ownership of the file back to the original owner**
4. place object access auditing on the file before taking ownership
5. reset the original owner’s password
6. <TF>After Step 5 of the lab, the Windows Server 2016 administrator would have been able to open Diver.txt. True or **False**?
7. <MULT>Which of the following statements regarding the lab is true?
8. **<MULTA>The only domain workstation Nicole Diver can log on to is Windows 10 VM.**
9. Any local user on Windows 10 VM would be able to log on to any workstation in the domain.
10. The Windows 10 VM administrator would be able to log on to any workstation in the domain.
11. Nicole Diver’s account can be changed to a domain account by logging in as Windows Server\ndiver.
12. <MULT>Which of the following statements regarding the lab is true?
13. <MULTA>After Step 5 in this lab, Nicole Diver could log in and take ownership of Diver.txt.
14. At the start of this lab, Authenticated Users and Users (Windows 10 VM\Users) would not be able to open the Nicole directory.
15. At the end of this lab, Authenticated Users and Users (Windows 10 VM\Users) would be able to open the Nicole directory but would not see that the Diver.txt file was inside the directory.
16. **At the end of this lab, Nicole is still able to change permissions on Diver.**
17. <TF>At the end of this lab, the administrative user you created when you installed Windows 10 VM would not be able to open Diver.txt. **True** or False?

# <H1>Lab 12.3 Setting and Testing Share Permissions

**<H2>Objectives**

<TX1>While NTFS permissions apply whether access is local or remote, Share permissions apply only when network protocols are used to access the folder. Share permissions can only be set on folders, drives, and printers; they cannot be set on files. Share permissions don’t require that the partition be formatted in NTFS; FAT partitions also support Share permissions. And whereas NTFS permissions are granular, Share permissions are simple: allow or deny full access, change, or read.

<TX2>An important consideration is the effect of combined permissions. For example, suppose a user is a member of a group that has been assigned full control Share permission to a folder but is also a member of a group that has been assigned read Share permission to the same folder. What is the effective Share permission?

<TX2>After completing this lab, you will be able to:

* <BL>Set Share permissions on folders
* Test Share permissions
* Troubleshoot Share permissions

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016
* Windows 10 VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **30 minutes**

<TX1>In this lab, you configure and troubleshoot Share permissions.

1. <NL\_FIRST>Log on to Windows Server as administrator. In Server Manager, click Tools, then click Active Directory Users and Computers. If necessary, expand the domain, right-click the Users container, click New, and click Group. Create a group named Research. Verify that the group is configured to be a global security group. Repeat this process to create two more groups named Quality and Audit.
2. <NL\_MID>Right-click the Users container, click New, and click User. Create the user accounts listed in Table 12-1. Uncheck the box to the left of User must change password at next logon, and then check the box to the left of Password never expires. Double-click each user, click the Member Of tab, click Add, type the name of the appropriate group in the Enter the object names to select box, click OK, and then click OK again.

**[Insert Table 12-1 Here]**

1. Click File Explorer on the task bar, and navigate to the root of C:. Create the folders listed in Table 12-2. In each folder, create the listed new text document. To set Share permissions on each folder, right-click the folder, click Properties, click the Sharing tab, click Advanced Sharing, click the box to the left of Share this folder, click Permissions, verify that the Everyone group is selected, click Remove, click Add, type the name of the appropriate security group(s) in the Enter the object names to select box, and click OK. In the Group or user names box, click the appropriate group. In the Permissions box, click the appropriate Allow/Deny boxes, and click OK. When you set Deny permissions, a Windows Security window appears. Read this warning, click Yes, click OK, and click Close. Figure 12-6 shows how the Manuscripts folder’s permissions should be configured.

**[Insert Table 12-2 Here]**

[Insert Figure 12-6 Here]

1. Log out of Windows Server and then log in as Patty Mallow. Click the File Explorer icon on the task bar and open Local Disk (C:). Open each of the three new folders—Manuscripts, Glossaries, and Contracts—and attempt each of the following:
2. <LL>Open the file in the folder.
3. Type UserirstName wrote this, where UserirstName is the first name of the user that has logged on, and then save the file.
4. Add a new file to the folder using the first name of the logged-in user as the filename.</LL>
5. Log in as the other two users you created in this lab and repeat the procedures in Step 4. Make notes of your results. Were these results consistent with the Share permissions you set on the folders?
6. Log on to Windows 10 VM as Patty Mallow. Open the Control Panel, click Network and Internet, and in the Network and Sharing Center section, click View network computers and devices. If an information bar appears about Network discovery, click it, and then click Turn on network discovery and file sharing. Enter the administrator credentials, and click Yes. Double-click Windows Server. Here, you should see the three folders you shared. Complete the tests you performed in Step 4 (add a “2” to the end of the filename when you create a new file in each directory), then log in to the other two users created in this lab and repeat the Step 4 tasks. Make notes of the results.
7. You may want to leave your systems running while you answer the Review Questions.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.

**<H2>Review Questions**

1. <TF>NTFS permissions take precedence over Share permissions. True or **False**?
2. <FIB>In Step 6 of this lab, Tanzy Williams could not modify the Taliesin file because \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
3. <FIBA>she is a member of the Quality group
4. she is a member of the Research group
5. **the file has restrictive permissions**
6. the Quality group does not have change permissions on the Manuscripts folder
7. <FIB>In Step 6 of this lab, William Strunk could not modify the GNU file because \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
8. <FIBA>he is a member of the Audit group
9. he is a member of the Quality group
10. **the file has restrictive permissions**
11. the Audit group does not have change permissions on the Contracts folder
12. <FIB>In Step 6 of this lab, Patty Mallow could not create a new file in the Manuscripts folder because \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
13. **<FIBA>she is a member of the Research group**
14. she is a member of the Quality group
15. the file has restrictive permissions
16. the Quality group does not have change permissions on the Manuscripts folder
17. <FIB>In Steps 4 and 5 of this lab, the Share permissions did not provide access control because \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
18. **<FIBA>the resources were accessed locally**
19. the users had not logged out and then logged back in
20. Active Directory authentication is only enforced for remote access
21. the permissions on the objects were not configured locally

# <H1>Lab 12.4 Auditing Permissions

**<H2>Objectives**

<TX1>In the IT world, rights and permissions are dangerous things, even more dangerous than user accounts. A user account that has no rights or permissions, when in the wrong hands, cannot do your network much harm. However, a user account that has rights and permissions, when in the wrong hands, can be used to cause serious damage.

<TX2>To perform their business tasks, most users need rights and permissions. Permissions determine the level of access to a resource that a user has (for example, read, modify, full control). Rights enable a user to perform system tasks (for example, shut down the system or change the system clock).

<TX2>In a Windows Server 2016 environment, Share permissions and NTFS permissions allow users to access network resources. Share permissions have one purpose: to control the use of resources accessed over the network. If the resource is not shared, it will not be “seen” on the network. NTFS permissions have more varied capabilities. They apply to resource access both over the network and interactively—that is, while a user is logged on to the system itself and accessing the resource directly through the local hard drive. NTFS permissions are also more granular than Share permissions so that they give system administrators a much more detailed level of control over the resource.

<TX2>Configuring, monitoring, and troubleshooting permissions can get complicated. Inheritance of permissions from parent objects, the combining of permissions, careless planning, and careless administration can make managing permissions confusing. Windows Server 2016 has some command-line utilities to track permissions, but these are cumbersome and are better used for scripting than for auditing. In this lab, you use a third-party utility designed to audit permissions.

<TX2>After completing this lab, you will be able to:

* <BL>Configure Share and NTFS permissions
* Analyze combined Share and NTFS permissions
* Install and configure a permissions auditing utility

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016
* Windows 10 VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **40–50 minutes**

<TX1>In this lab, you configure Share and NTFS permissions and use EMCO Permissions Audit Professional to audit permissions.

1. <NL\_FIRST>Log on to Windows 10 VM with an administrative account. Turn Windows Firewall off.
2. <NL\_MID>Log on to Windows Server as the domain administrator. Turn Windows Firewall off.
3. Open a web browser, navigate to <URL>http://emcosoftware.com/permissions-audit/download</URL>, click Download, and save the PermissionsAuditSetup.exe to your desktop.

**[Insert Icon Here]**

It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “EMCO Permissions Audit.”

1. Double-click the downloaded file to install EMCO Permissions Audit 2. Select all the defaults during the installation. Uncheck the box to the left of Launch EMCO Permissions Audit XML Professional and click Finish.
2. In Server Manager, click Tools, then double-click Active Directory Users and Computers. Expand your domain. Right-click your domain, click New, create one OU called Research and another OU called Marketing.
3. Right-click the Research OU, click New, and then click User. Use the information in Table 12-3 to create the users in the Research OU.

**[Insert Table 12-3 Here]**

1. Use the information in Table 12-4 to create the users in the Marketing OU.

**[Insert Table 12-4 Here]**

1. Right-click the Users folder, click New, and then click Group. Create a global security group named SF-Marketing and a global security group named SF-Research. Right-click the SF-Marketing group, click Properties, click the Members tab, and add the users who are in the Marketing OU to the SF-Marketing group using the Add button. Add the users in the Research OU to the SF-Research group.
2. On Windows 10 VM, create a folder as follows: click Start, click File Explorer, and double-click Local Disk (C:**)**. Right-click a blank space, click New, click Folder, and name the folder Performance Evaluations.
3. Set Share permissions on the folder as follows: right-click Performance Evaluations, click Properties, and click the Sharing tab. Click the Advanced Sharing button, place a check mark in the box to the left of Share this folder, and click the Permissions button. Select the Everyone group and click the Remove button. Click the Add button and, because you are going to assign Share permissions to domain accounts, not local computer accounts, make sure the name of your domain appears in the From this location box. In the Enter the object names to select box, type Administrator; SF-Research; tandrews and click the Check Names button. Although you did not type the complete names of the security principals, your entries were not ambiguous and the correct accounts were located. Your results should look like what is shown in Figure 12-7.

[Insert Figure 12-7 Here]

**[Insert Icon Here]**

Depending on how your virtual machine or network is configured, the server name/location may differ from what is shown in the figure.

Click OK. On the Permissions for Performance Evaluations window, select Administrator and then place a check mark in the Full Control box under the Allow column. Select the SF-Research group and verify that they have the default permission of Read. Select Tony Andrews and then place a check mark in the Change box under the Allow column. Click OK in the Permissions for Performance Evaluations window, and then click OK in the Advanced Sharing window.

1. Set NTFS permissions on the folder as follows: click the Security tab, click the Edit button, select Authenticated Users, and click Remove. Read the Windows Security message and click OK. To block inheritance of permissions from the parent container, click Cancel in the Permissions for Performance Evaluations window, click Advanced in the Performance Evaluations Properties window, click the Change Permissions button, then remove the check mark from “Include inheritable permissions from this object’s parent.” When given the option to Add, Remove, or Cancel, click Add, click OK in the Advanced Security Settings for Performance Evaluations window, and click OK again. In the Performance Evaluations Properties window, click Edit, select Authenticated Users, and click Remove. Also remove the Users group, but do not modify the SYSTEM or Administrators settings. Click Add. In the Enter the object names to select box, type SF-Research; tandrews, and click the Check Names button. Click OK. Select SF-Research and verify that they have the standard Read permissions: Read & execute, List folder contents, and Read. Select Tony Andrews, click Full control in the Allow column, and click OK. Click Close in the Performance Evaluations Properties window.
2. Using the techniques demonstrated in Steps 10 and 11, create the folder and permissions structure shown in Table 12-5. Be sure to remove any default permissions for regular user accounts (for example, the Everyone, Authenticated Users, Users groups), but leave any administrative or system accounts untouched. Also note that “Read” in the NTFS Permissions column of Table 12-5 references the default Read permissions, which are Read & execute, List folder contents, and Read.

**[Insert Table 12-5 Here]**

1. Open the EMCO Permissions Audit Professional application. Because this is a demonstration version, you may run it only 30 times. Click Evaluate. If necessary, if the Permission Audit 2 dialog opens select Remember my choice and click **Increase Priority**.
2. Press Ctrl-A. In the Domain dropdown select your Domain Controller. Click the **Test Credentials** button. Click **OK**. Your result should be similar to what is shown in Figure 12-8, although you may see domains other than just your own.

[Insert Figure 12-8 Here]

1. Press **Ctrl-F**. This will fetch all the shared drives on the network.
2. Notice that in the right pane, the fetch identifies the shares that exist on the network. Click on any Performance Evaluation folder, notice who the folder is shared with.
3. Close all windows and log off both systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.

**<H2>Review Questions**

1. <MULT>In this lab, permissions were configured for the folder Performance Evaluations. When accessing the Performance Evaluations shared folder over the network, what are Tony Andrews’s effective permissions?
2. <MULTA>Full Control
3. **Change**
4. Read
5. No Access
6. <MULT>Sebastian Knight is a developer responsible for creating interface standards between drivers and programs for a video game company. He is a member of the Developers group, and he is also a member of the Hardware Systems group. He needs to work on a project that requires that he be given the right to log on locally to a game server so he can test drivers. The folder he needs to access on the server is C:\WingsOfFlight\Programs. You set the following permissions on the Programs folder:

<UL>Share Permissions: Developers—Read, Hardware Systems—Read, Sebastian Knight—Change

NTFS Permissions: Developers—Read, Hardware Systems—Change, Sebastian Knight—Full Control</UL>

What are Sebastian’s effective permissions when he accesses the C:\WingsOfFlight\Programs folder?

1. **<MULTA>Full Control**
2. Change
3. Read
4. No Access
5. <TF>The SYSVOL share on Windows Server is used by network management programs to track disk space usage on a domain controller. True or **False**?
6. <MULT>In this lab, what are ebarnes’s effective permissions to the folder Staff within the Performance Evaluations folder when accessed over the network?
7. <MULTA>Full Control
8. Change
9. Read
10. **No Access**
11. <MULT>In this lab, what are the SF-Research group’s effective permissions to the folder Staff within the Performance Evaluations folder when accessed over the network?
12. <MULTA>Full Control
13. Change
14. **Read**
15. No Access

**[Start Table 12-1 Here]**

|  |  |  |  |
| --- | --- | --- | --- |
| <TBCH>Name | User Name | Password | Group Membership</TBCH> |
| <TBTX1>Patty Mallow | pmallow | Pa$$word | Research, Quality |
| Tanzy Williams | twilliams | Pa$$word | Quality |
| William Strunk | wstrunk | Pa$$word | Audit</TBTX1> |

<TBN>Table 12-1 User accounts

<TBFGS>Cengage Learning

**[End Table 12-1 Here]**

**[Start Table 12-2 Here]**

|  |  |  |
| --- | --- | --- |
| <TBCH>Folder Name | Contents (file) | Share Permissions</TBCH> |
| <TBTX1>Manuscripts | Taliesin | Quality: Allow Change, Read  Research: Deny Full Control, Change, Read |
| Glossaries | Merck | Research: Read |
| Contracts | GNU | Audit: Change, Read</TBTX1> |

<TBN>Table 12-2 Shared folders

<TBFGS>Cengage Learning

**[End Table 12-2 Here]**

**[Start Table 12-3 Here]**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| <TBCH>First Name | Last Name | User Logon Name | Password | User Must Change Password | Password Never Expires | Account is Disabled</TBCH> |
| <TBTX1>Tony | Andrews | tandrews | Pa$$word | unchecked | checked | unchecked |
| Jennett | Marsh | jmarsh | Pa$$word | unchecked | checked | unchecked |
| Angus | Hudson | ahudson | Pa$$word | unchecked | checked | Checked</TBTX1> |

<TBN>Table 12-3 Research OU users

<TBFGS>Cengage Learning

**[End Table 12-3 Here]**

**[Start Table 12-4 Here]**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| <TBCH>First Name | Last Name | User Logon Name | Password | User Must Change Password | Password Never Expires | Account is Disabled</TBCH> |
| <TBTX1>Eddie | Barnes | ebarnes | Pa$$word | unchecked | checked | checked |
| Catherine | Bridges | cbridges | Pa$$word | unchecked | checked | unchecked |
| Jim | Bellamy | jbellamy | Pa$$word | unchecked | checked | Checked</TBTX1> |

<TBN>Table 12-4 Marketing OU users

<TBFGS>Cengage Learning

**[End Table 12-4 Here]**

**[Start Table 12-5 Here]**

|  |  |  |
| --- | --- | --- |
| <TBCH>C:\Performance Evaluations\Staff</TBCH> | | |
| *<TBTX1>Security Principles* | *Share permissions* | *NTFS Permissions* |
| Tandrews | folder not shared | Full Control |
| ebarnes (disabled) | folder not shared | Deny Full Control |
| SF-Research | folder not shared | Read |
| Administrator | folder not shared | Full Control</TBTX1> |
| <TBCH>C:\References</TBCH> | | |
| <TBTX1>Cbridges | Read Full | Control |
| SF-Research | Full Control | Read |
| SF-Marketing | Full Control | Modify |
| Administrator | Full Control | Full Control</TBTX1> |

<TBN>Table 12-5 Folder and permission structure

<TBFGS>Cengage Learning

**[End Table 12-5 Here]**