CompTIA A+ Lab Series v2

Lab 5: Security

Document Version: 2015-04-21

Development was funded 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 an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction

This lab is part of a series of lab exercises designed to supplement coursework and provide students with a hands-on training experience based on real world applications. This series of lab exercises is intended to support courseware for CompTIA A+® certification.

Many users view security as an inconvenience. As a PC technician, you need to be mindful of the principle of least privilege: limiting access to resources at the minimum level needed to allow normal functionality in order to minimize the potential for security risk.

This lab includes the following tasks:

1. Managing User Accounts
2. Creating Local Group Policy
3. Sharing Folders and Permissions

Objective: Security Practices in Windows OS

Good security practices include creating standard user accounts for those who do not need administrator level access, educating users about good password practices and how to enforce them in group policies, and being careful about how and what resources are shared. This lab will look at ways to address these security practices.

Key terms for this lab:

Local Group Policy – A set of rules for what users and computers can and cannot do. Policies can be system wide or apply to a small group of users.

User Accounts – A user account identifies a person by username and password. Permissions are often tied to user accounts.

Standard Account – A basic user account with limited rights on a Windows operating system.

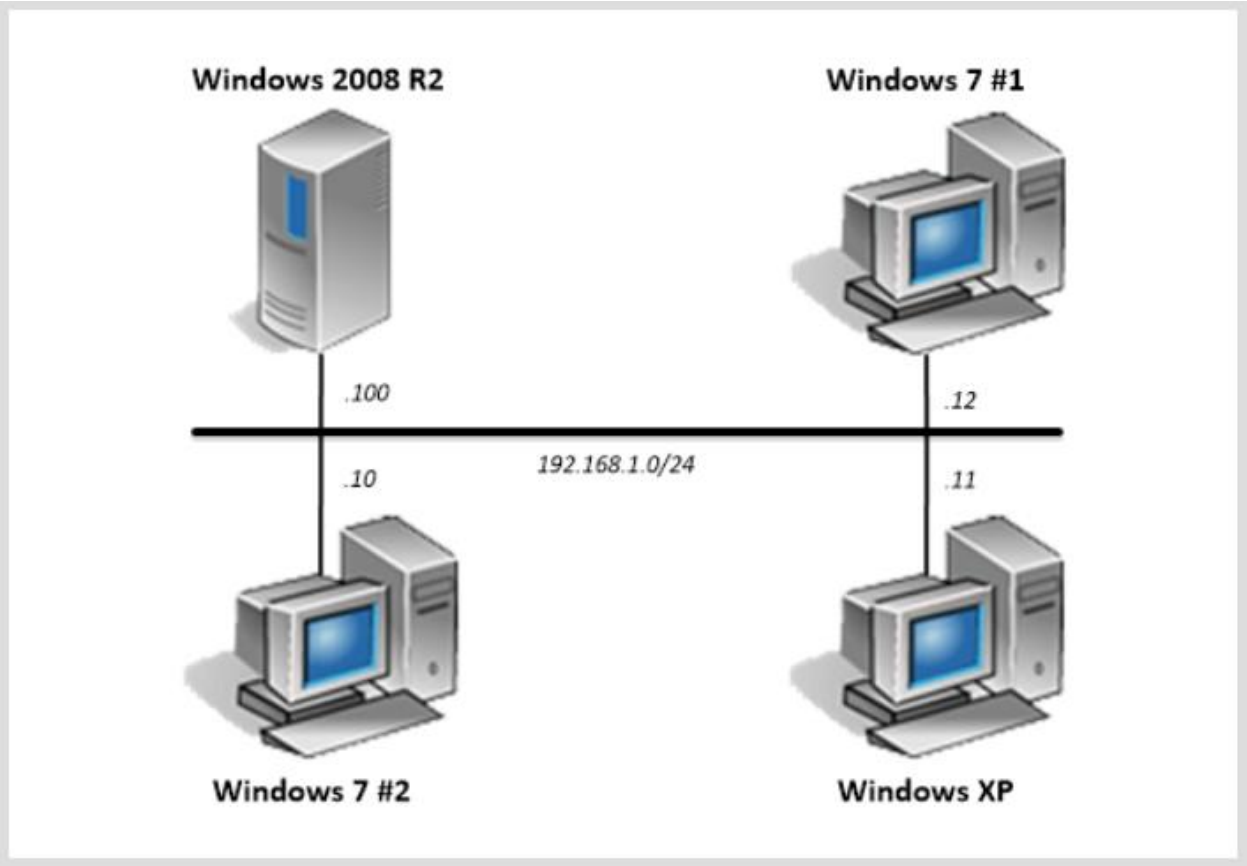
Administrator Account – Elevated user account with more rights than a standard account.

Permissions – Permissions dictate what a user can and cannot access.

Strong Password – A password containing 8 or more characters, numbers, both uppercase and lowercase letters, and symbols. Strong passwords are harder to guess or "crack".

Batch File – A set of commands for the computer to complete.

Lab Topology



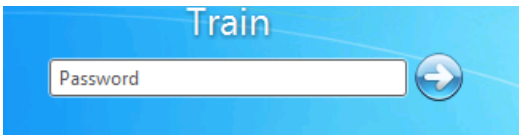
Lab Settings

The following table includes settings necessary to complete the lab. The Windows features referenced and used in this lab are consistent with those included with Windows 7 and Windows XP.

Log in to the following virtual machines before starting the tasks in this lab:

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Windows 7 #1	192.168.1.12/24	Train	Train1ng$
Windows 7 #2	192.168.1.10/24	Train	Train1ng$

1. Click on the icon on the topology that corresponds to the machine you wish to log into.
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. In the password text box, type **Train1ng$** and press **Enter** to log in.



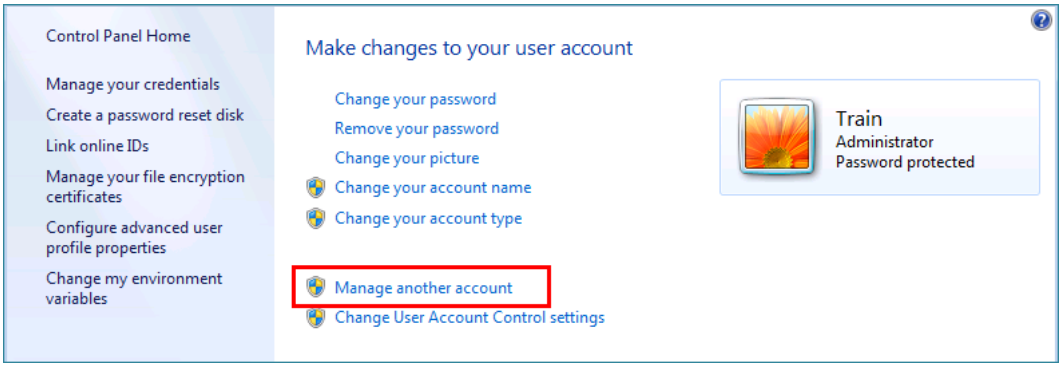
You are using the Train account, which has administrator privileges, to complete the tasks in this lab. You must be an administrator or have administrator privileges to complete some of the tasks in this lab.

1 Managing User Accounts in Windows 7

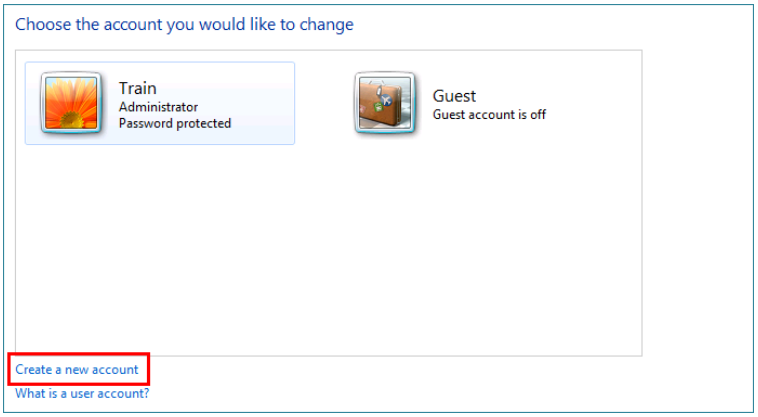
In this lab, you create user accounts and explore the differences between an administrator account and a standard user account.

1. Use the instructions provided in the **Lab Settings** section to log on to the Windows 7 #1 machine, if you are not logged in already.
2. Click **Start->Control Panel->User Accounts and Family Safety->User Accounts.**

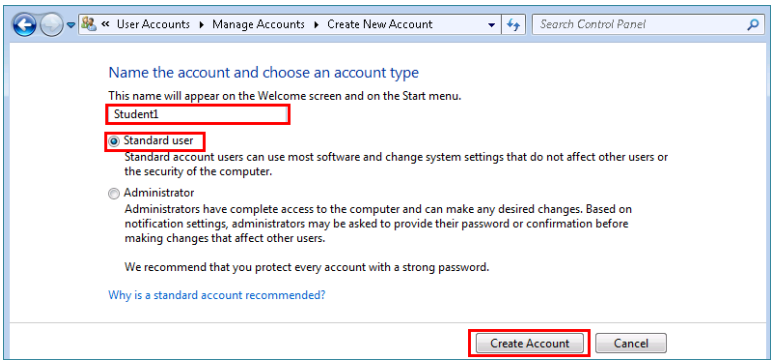
3. Click **Manage another account**.



4. Click **Create a new account**. The Create a new account window appears.

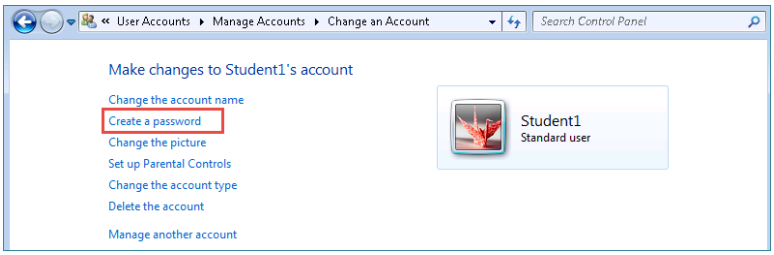


5. Type **Student1** for the account name.
6. Select the radio button next to **Standard** user.
7. Click **Create Account** and the Manage Account window opens.



8. Click on the user account you just made to open the **Change an Account** page.

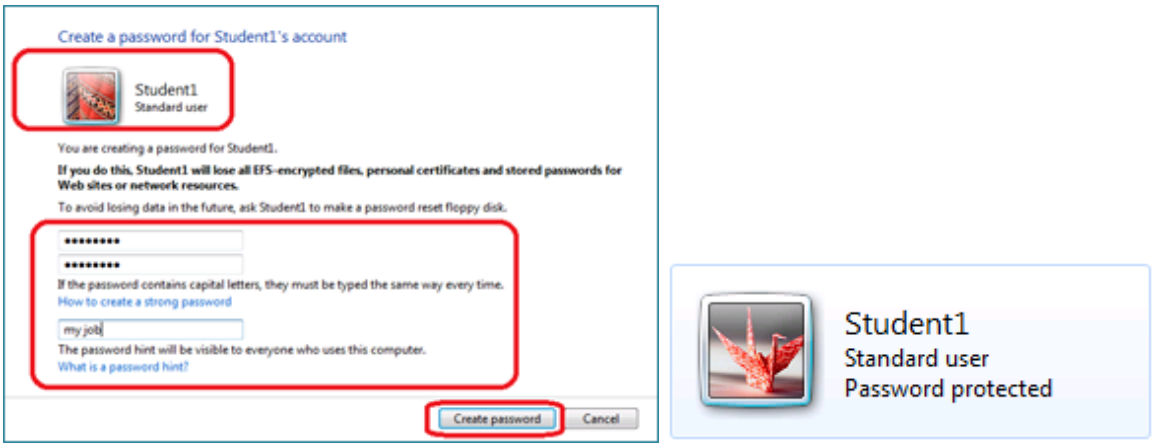
9. Click **Create a password.**



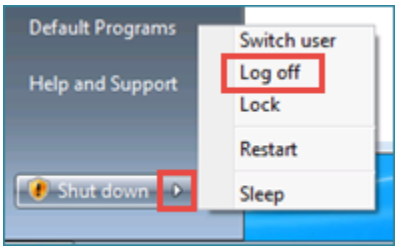
Passwords should be difficult to guess or "crack". Passwords keep unauthorized persons from accessing computers and resources they do not have permission to access. They keep accounts and the information they contain safe. Tips for account creation:

- Always use a password.
- Choose a password with a combination of upper and lower case letters, numbers, and keyboard symbols such as @ # $ % ^ & * ( ) _ +. (For example, T3cn1c1@n – a variation of Technician, with letters, numbers, upper and lowercase.)
- Choose a password containing at least eight characters. Longer, more complex passwords are harder for unauthorized persons to guess or "crack".

10. Type **T3cn1c1@n** as the password**.**
11. Type the hint, **my job**.
12. Click **Create password** and the account will now be indicated as Password protected.

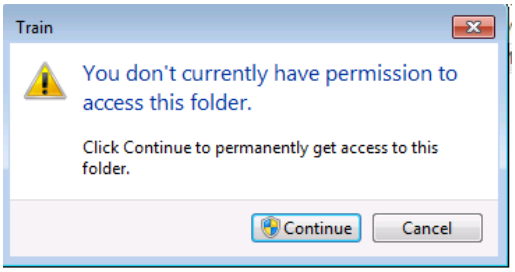


13. Click **Start**, click the triangle next to Shut down and click **Log Off**.

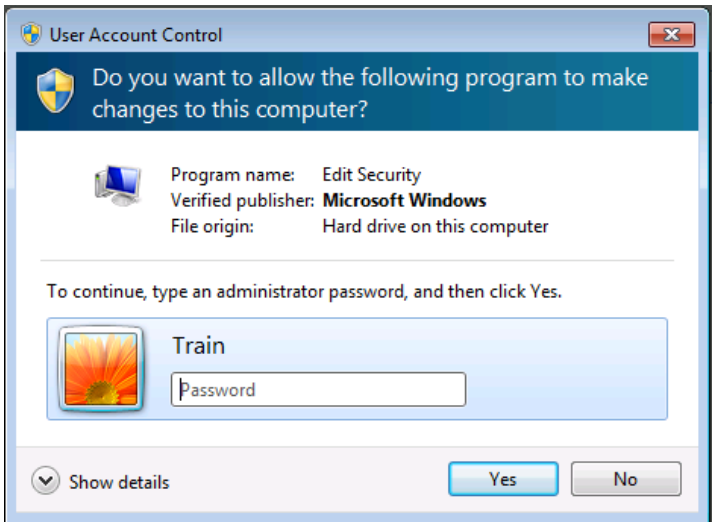


14. Log on as **Student1**.

15. Click **Start**->**Computer**-> **Local Disk (C:)**->**Users**->**Train**.



16. Click **Continue**.



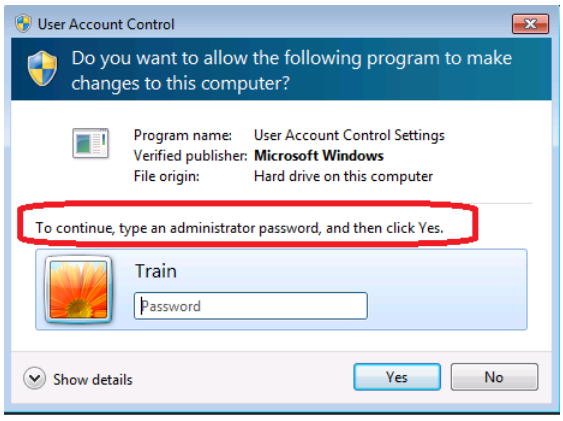
17. Click **No**.

You are locked out of the Train User folder because you are not authorized by your account credentials to access it.

18. Double-click **Student1**.

The **Student1** folder and its contents are available to you because you are authorized and have been authenticated by your account credentials.

19. Click **Start**->**Control Panel**->**User Accounts and Family Safety**->**User Accounts**
20. Click **Change User Account Control settings**.



The Account credentials for the **Train** user appear because the **Student1** account is a Standard User account with limited privileges and administrative privileges are need. **Train** is a user in the **Administrator Group**.

21. Log off and log back in as **Train**.

1.1 Conclusion

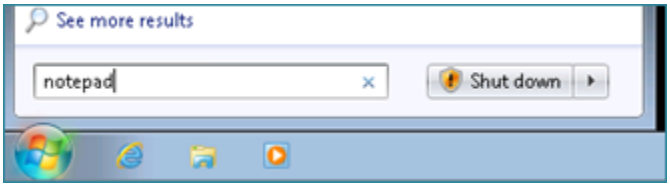
No matter how secure you make your computer, your computer is vulnerable if others have access to your password. Compromising a system by a user giving out a password to others or not using one that is strong is a major weakness in many businesses. In addition, there are many programs that attempt to determine passwords by guessing commonly used choices, by randomly generating possibilities and trying them all, or using a combination of both techniques.

The best defense is a "strong password" and user training on the importance of the password to security. A strong password is a combination of numbers, uppercase letters, lowercase letters, and, if possible, other characters. This makes the password less likely to guess. The longer and more complex the password, the harder it is to guess.

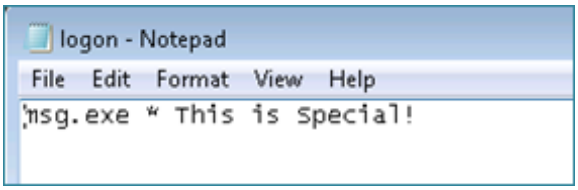
2 Creating Local Group Policy

In this lab, you configure and test local security policies.

1. Use the instructions provided in the Lab Settings section to log on to the Windows 7 #1 machine, if you are not logged in already.
2. Click **Start**, type **notepad** in the search box and press **Enter**.



3. In the document type **msg.exe * This is special!** in the text box and press **Enter** to move to the next line.

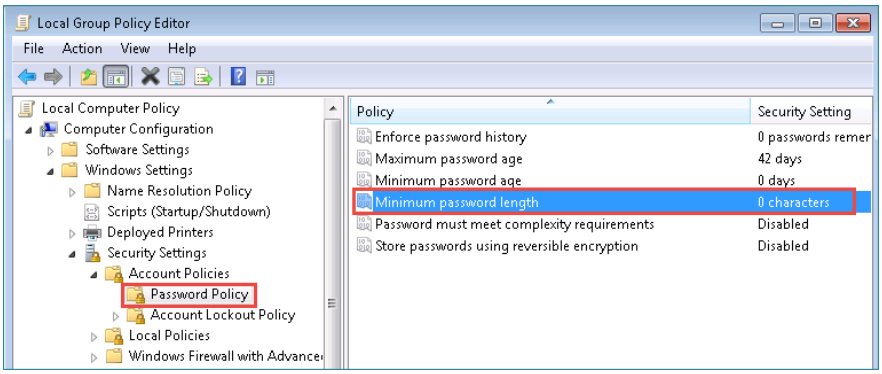


4. Click **File**->**Save As**.
5. Change the **Save as** type box to **All Files**.
6. Type **c:\users\train\logon.bat** in the File name box and click **Save**.

7. Click **Start**, type **gpedit.msc** in the search box. Press **Enter**.

8. In the left pane, click to the arrow next to **Computer Configuration** to expand, if it is not already expanded.
9. Click to the arrow next to **Windows Settings** to expand it
10. Click to the arrow next to **Security Settings** to expand it.
11. Click to the arrow next to **Account Policies** to expand it.
12. Click to select **Password Policy**.

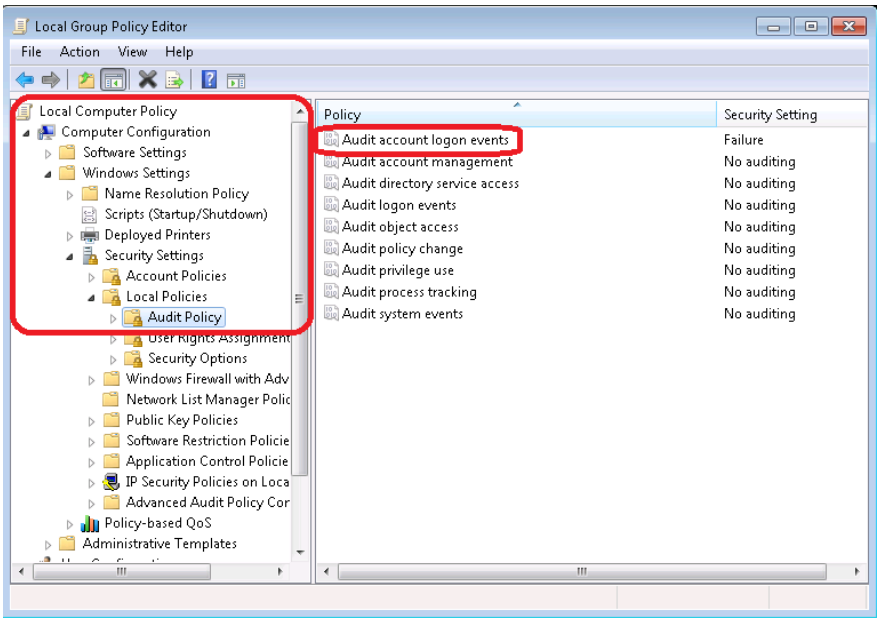
13. In the right pane under **Policy,** double-click **Minimum password length**.



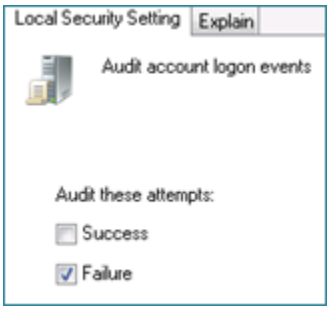
14. In the **Minimum password length** box, type **8** and click **OK**.

Now, all new passwords must have at least 8 characters.

15. In the left pane, click the arrow next to **Local Policies** to expand it.
16. Click to select **Audit Policy**.
17. In the right pane under **Policy,** double-click **Audit account logon events**.

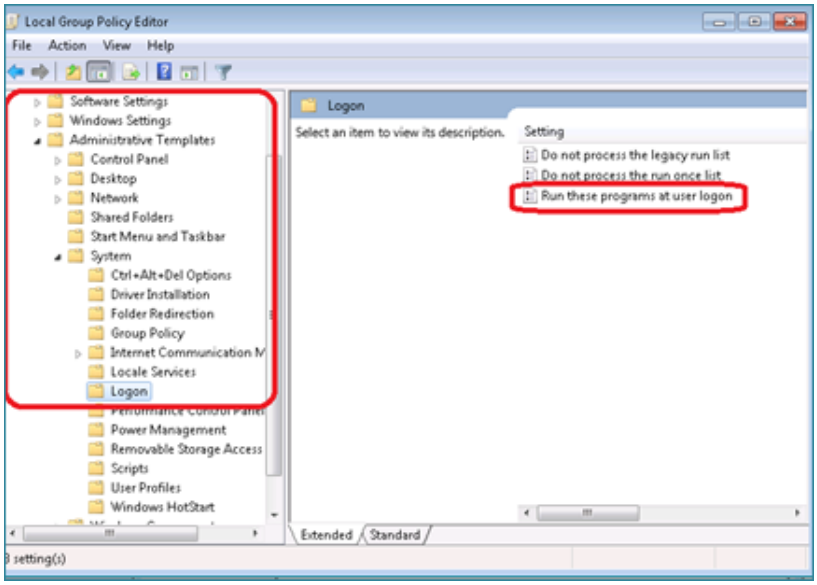


18. Click the **Failure** checkbox and click **OK**.

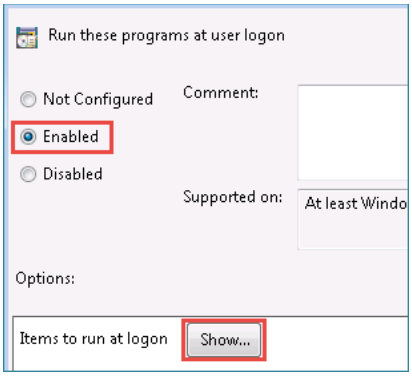


Now you will see any failed logon events in the **Event Viewer**.

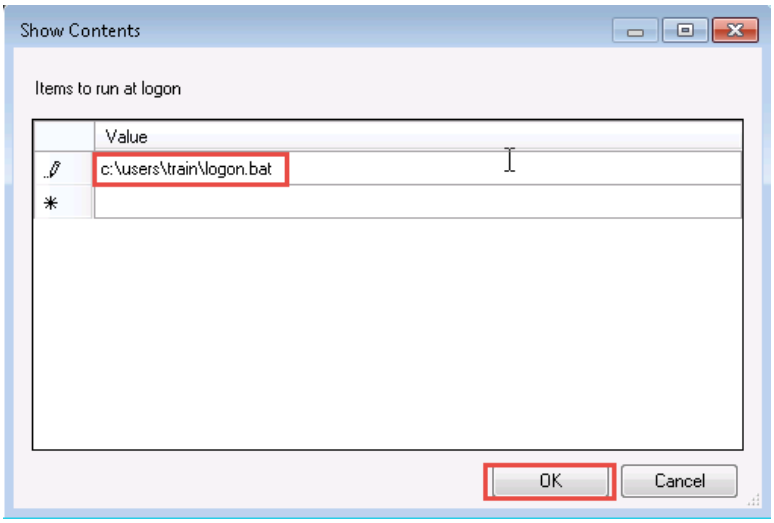
19. In the left pane, click the arrow next to **Computer Configuration** to compress it.
20. In the left pane, click the arrow next to **Administrative Templates** to expand it.
21. In the left pane, click the arrow next to **System** to expand it.
22. Click to select **Logon**.
23. In the right pane under **Logon,** double-click **Run these programs at user logon**.



24. Click the **Enabled** option and click the **Show…** button.

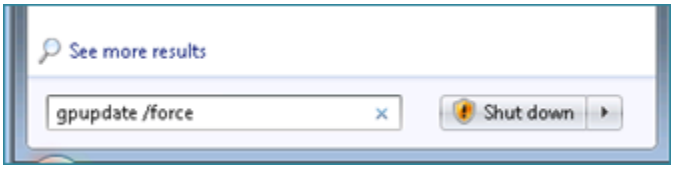


25. Type **c:\users\train\logon.bat** in the **Value** box. Press **Enter**.
26. Click **OK**.
27. Click **OK** to close the **Show Contents** window.

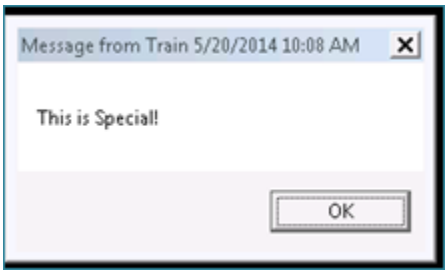


Now the logon.bat file that you created earlier in this task will be run at startup.

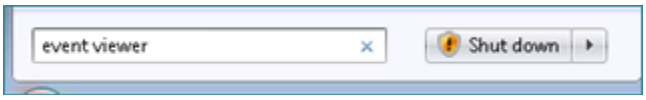
28. Close the **Local Group Policy Editor** window.
29. Close **notepad**.
30. Click **Start**, **type gpupdate /force** in the Start search box. Press **Enter**.



31. Click **Start**, click the **triangle** next to Shut Down, and click **Log Off**.
32. To create a logon failure event, Click **Train** type **1234** in the Password box and press **Enter**.
33. Click **OK**.
34. Log on as **Train** with a password of **Train1ng$**.
35. Click **OK** to close the message that the startup script opened.

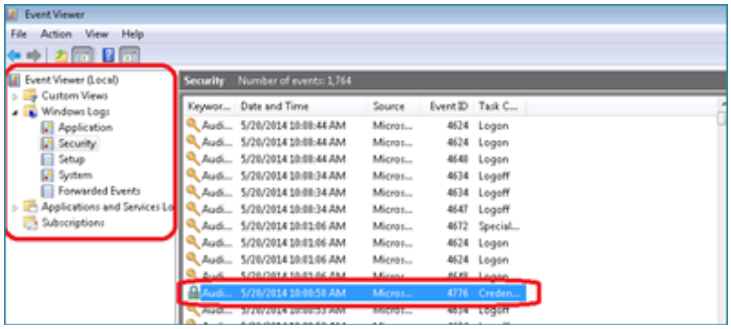


36. Click **Start**, type **event viewer** and press **Enter**.

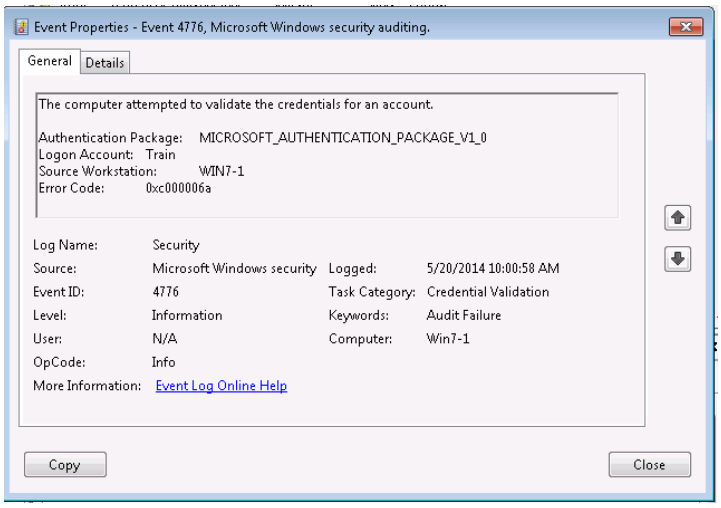


37. Click to expand **Windows Logs**.
38. Click to select **Security**.

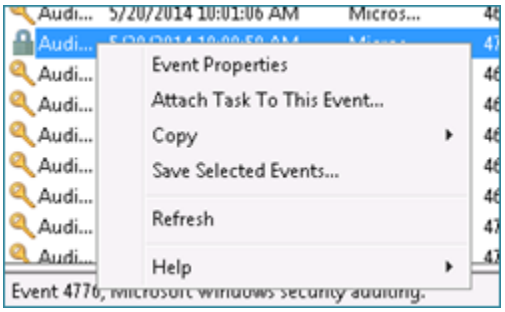
See if you can find the failed logon attempt that was audited. The Event ID should be **4776**.



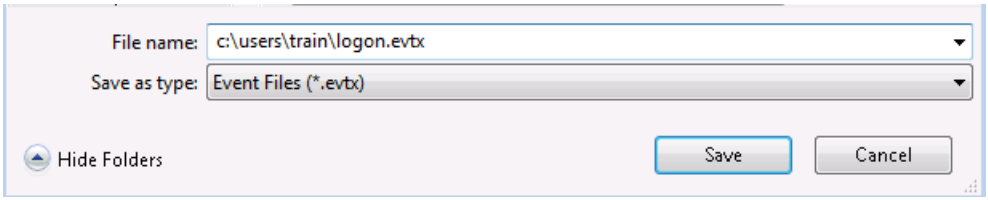
39. Double-click the event to read the properties.



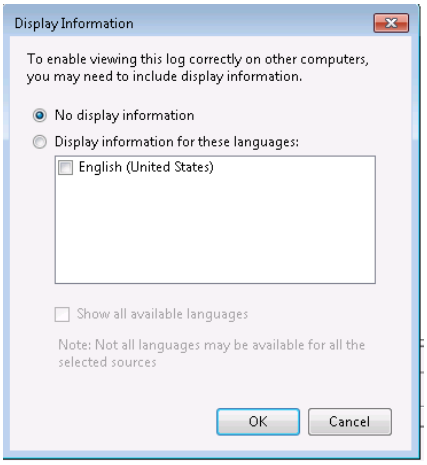
40. Click **Close**.
41. **Right-click** the event and click **Save Selected Events**.



42. Type **c:\users\train\logon.evtx** in the **File name** box and click **Save**.



43. Click **OK** to accept the default **No display information** when the Display Information dialog box appears.



44. Close the **Event Viewer**.

2.1 Conclusion

The Local Group Policy Editor provides an effective and centralized way for an administrator to edit local group settings such as: disable computer or user settings, use scripts for making announcements to users at log on, and ensuring that passwords are created with strong password requirements, even if users are unaware of how to do that.

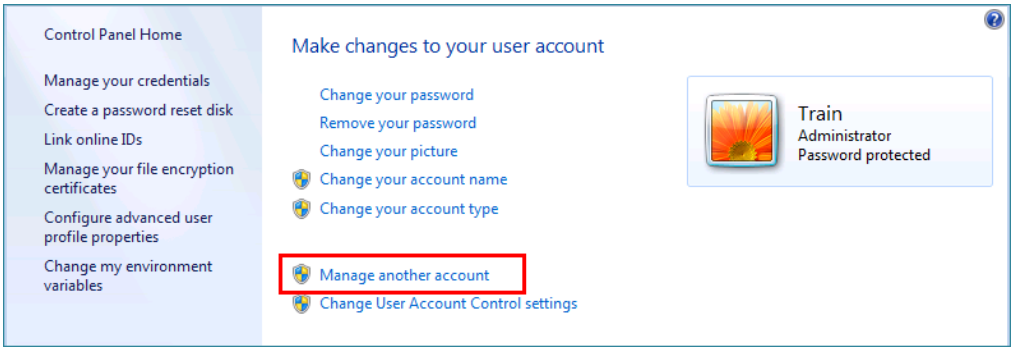
Technicians can use Event Viewer to view and manage event logs that contain information about hardware and software problems and about security events on your computer. Users can also use Event Viewer for troubleshooting most issues. The tool is purposeful, effective, and user-friendly. Administrative privileges are required to view some logs.

3 Sharing Folders and Permissions

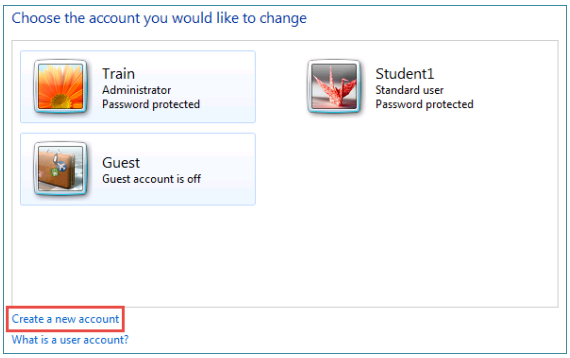
Files and folders created on local machine are by default not available to users other than the creator of them. Sharing folders can be useful for both personal and professional activities. In this task, you will be sharing and securing folders using Windows 7.

1. Use the instructions provided in the Lab Settings section to log on to the Windows 7 #1 machine, if you are not logged in already.
2. Click **Start** > **Control Panel**->**User Accounts and Family Safety**->**User Accounts.**

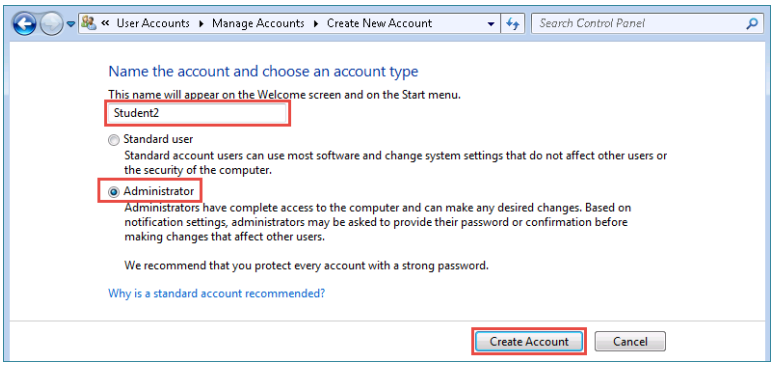
3. Click **Manage another account**.



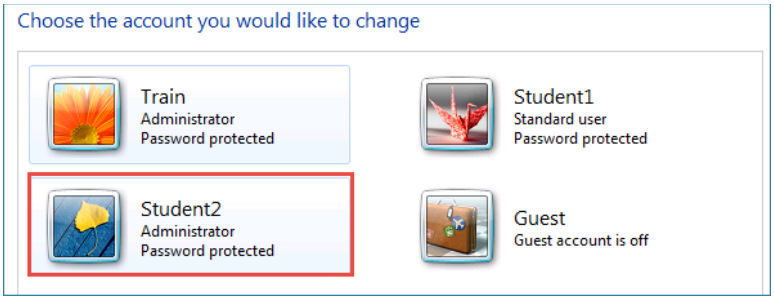
4. Click **Create a new account**. The Create a new account window appears.



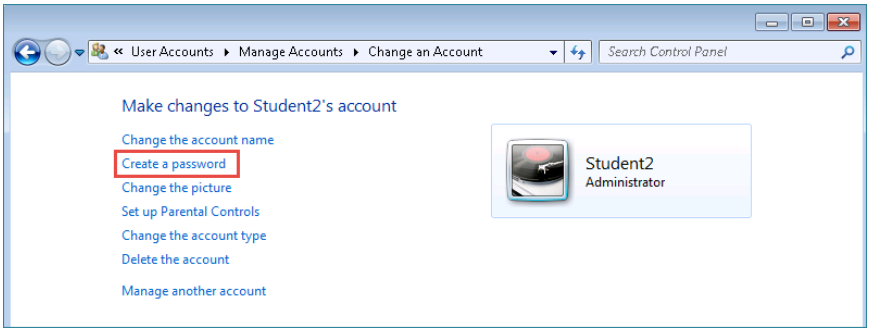
5. Type **Student2** for the account name.
6. Select the radio button next to **Administrator** user.
7. Click **Create Account** and the Manage Account window opens.



8. Click on the user account you just made to open the **Change an Account** page.

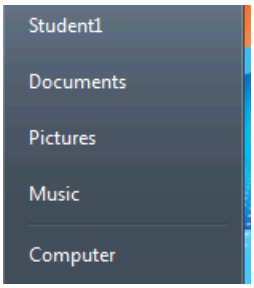


9. Click **Create a password**, or **Change the password** if the account already has one.



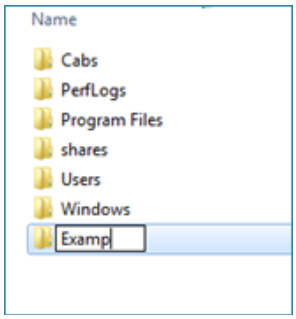
10. Type **T3cn1c1@n** as the password.
11. Type the hint, **my job**.
12. Click **Create the password** and the account is now indicated to be Password protected.
13. Click **Start**, click the triangle next to Shut down, and then click **Log Off**.
14. Log on as **Student1**.

15. Click **Start->Computer**.

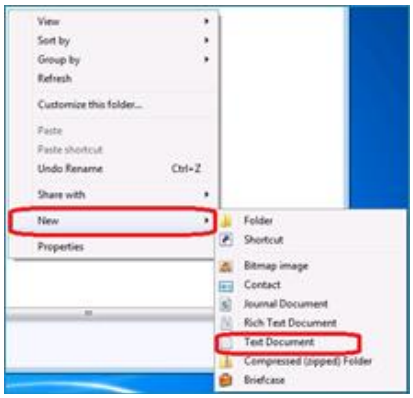


16. Double-click **Local Disk (C:)**.
17. Click the **New folder** button.

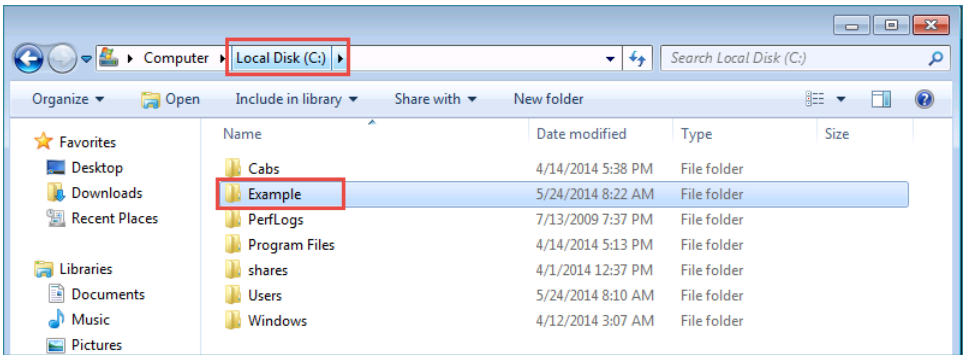
18. Type **Example** in the name box. Press **Enter**.



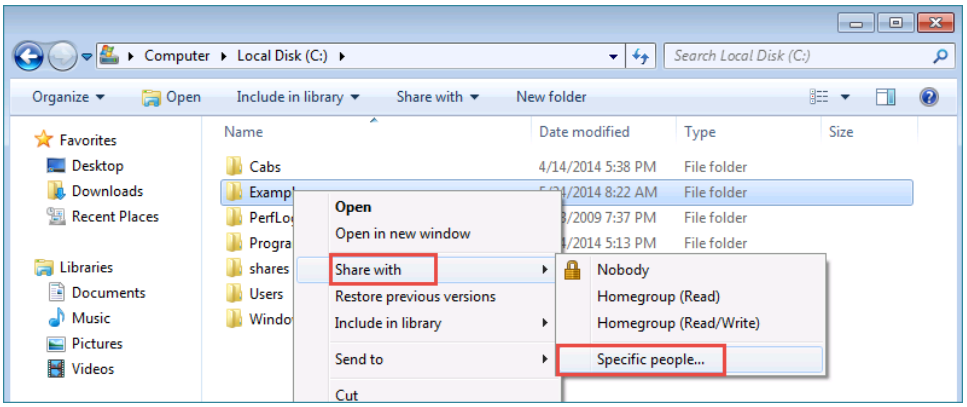
19. Double-click **Example** to open it.
20. Right-click an **empty space** in the **Example** folder, point to **New**, and click **Text Document**.



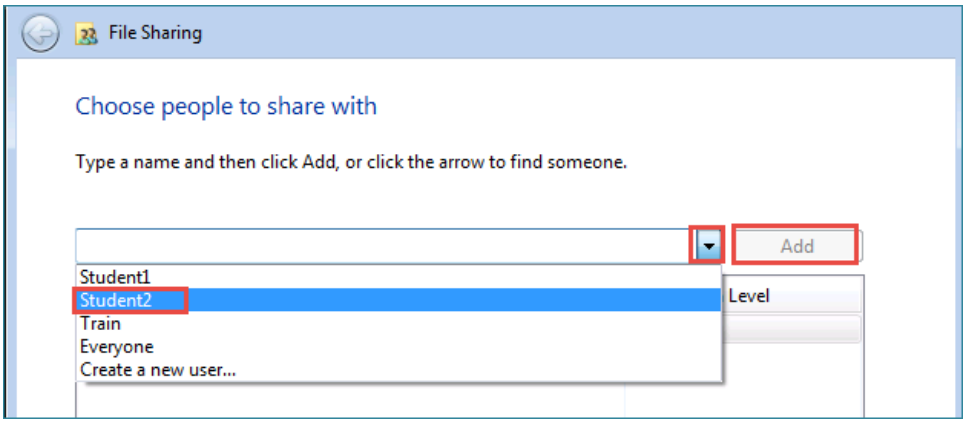
21. Type **ExampleNotes** in the name box. Press **Enter**.
22. Double-click **ExampleNotes** to open it.
23. Type **Hello** in the file. Click **File** and select **Save**.
24. Close **Notepad**.
25. Click **Local Disk (C:)** in the address bar.



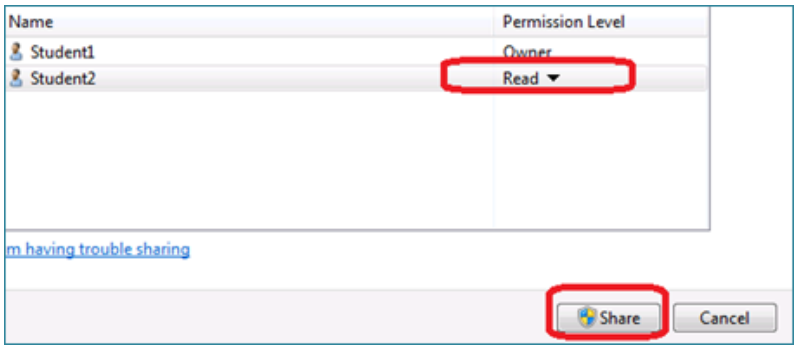
26. Right-click **Example**, select **Share with->Specific people**.



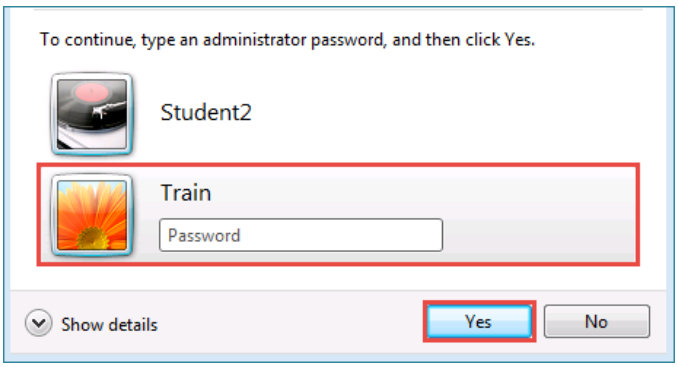
27. Select **Student2** from the drop-down list
28. Click **Add**.



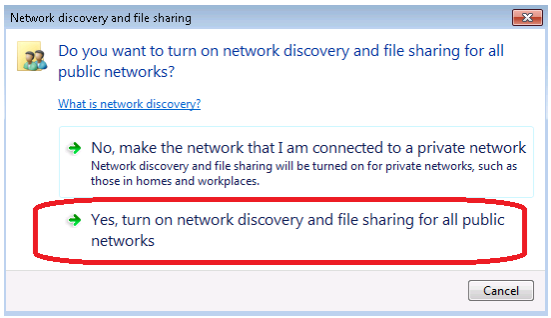
29. Ensure that Student2 only has Read permissions and click **Share**.



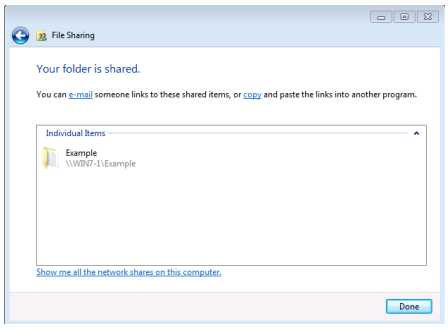
30. You are logged on as **Student1** and will need to provide administrator credentials to make changes. Click **Train** and type **Train1ng$** as the password. Click **Yes.**



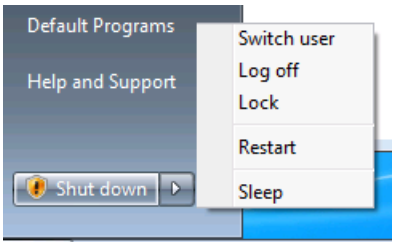
31. Click **Yes, Turn on network discovery …**



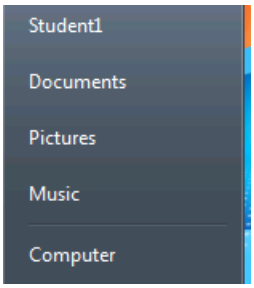
32. Click **Done**.



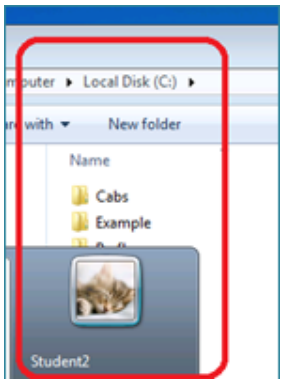
33. Click **Start**, click the **triangle** next to Shut down and click **Log Off**.



34. Log on as **Student2**.
35. Click **Start**->**Computer**.



36. Double-click **Local Disk (C:)** to access the shared folder **Example**.



37. Double-click on the shared folder **Example** ->double-click **ExamplesNotes**.
38. Close **ExampleNotes**.

3.1 Conclusion

Sharing folders can be useful for both personal and professional activities.

References

1. Computer Hope:
   http://www.computerhope.com/jargon.htm

2. Change password policy settings:
   http://windows.microsoft.com/en-us/windows-vista/change-password-policy-settings

3. Windows Group Policy Editor:
   http://www.techrepublic.com/blog/10-things/10-ways-to-tweak-windows-7-using-the-local-group-policy-editor/