# Apply Local Security Policies

Time required: 30 minutes

**How to Create Screenshots:** Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

## Lab Description

Follow these steps to set a few important security policies on the local computer.

**NOTE:** Do this lab on your Windows virtual machine.

# Create a Snapshot

A Snapshot allows us to go back to a previous version of our VM.

Before starting your Windows VM 🡪 Go to the Snapshot menu -> Take 🡪 Click OK.

# Apply Local Security Policies

1. Sign into Windows using an administrator account on a virtual machine using Windows.
2. To start Group Policy. Click Start 🡪 Start typing gpedit.msc 🡪 Click Local Group Policy Editor.

**Change default user names**. A hacker is less likely to hack into the built-in Administrator account or Guest account if you change the names of these default accounts.

1. To change the name of the Administrator account, drill down in the Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options group. In the right pane, double-click Accounts: Rename administrator account. In the Properties box for this policy, change the name and click OK. To change the name of the Guest account, use the policy Accounts: Rename guest account.
2. The Properties box for many policies offers the Explain tab. Use this tab to read more about a policy and how it works.
3. **Require user passwords**. To require that all user accounts have passwords, drill down to the Computer Configuration, Windows Settings, Security Settings, Account Policies, Password Policy group. Use the Minimum password length policy and set the minimum length to eight characters. Additionally, reduce the password expiration time frame so users must create new passwords frequently. Use the Maximum password age policy to require users to reset their password every 60 days. (Best practice is to set the Maximum password age in the range of 30 to 90 days.)
4. **Insert a screenshot:**

Click or tap here to enter text.

1. **Set failed logon restrictions**. Windows can be configured to lock a user account if too many incorrect logons are attempted. Drill down to the Computer Configuration, Windows Settings, Security Settings, Account Policies, Account Lockout Policy group. Use the Account lockout threshold to set the number of invalid logon attempts. When the number is exceeded, the account will be locked.
2. **Insert a screenshot:**

Click or tap here to enter text.

1. **Restrict logon hours.** In many cases, users should only be allowed access to a workstation during specific hours, such as during office hours. Preventing access at other times of the day and throughout the weekend can increase a workstation’s security. The schedule for a user’s or group’s logon hours is set through Active Directory, but individual workstations can be configured to respond differently once a user’s logon hours have expired. To configure a workstation’s response to the expiration of a user’s logon hours, drill down to the User Configuration, Administrative Templates, Windows Components, Windows Logon Options group. Use the Set action to take when logon hours expire policy to choose Lock, Disconnect, or Logoff. If this policy is not enabled, the user’s session will continue, but the user will not be able to log on outside of the assigned logon hours once the current session has been terminated.
2. **Insert a screenshot:**

Click or tap here to enter text.

1. **Audit logon failures**. Group Policy offers several auditing policies that monitor and log security events. These Security logs can then be viewed using Event Viewer. For example, to set an audit policy to monitor a failed logon event, drill down to the Computer Configuration, Windows Settings, Security Settings, Local Policies, Audit Policy group. Use the Audit logon events policy. You can audit logon successes and failures. To keep the log from getting too big, you can select Failure to only log these events.
2. **Disable AutoRun and AutoPlay.** When attaching a USB flash drive or external hard drive, or inserting a disc in the optical drive, Windows automatically accesses the storage media and then requests instructions on what to do next. Media files can be played automatically, which is called AutoPlay. Executable files can be run automatically, which is called AutoRun. You can disable both of these features to add yet another layer of security protection. To disable AutoPlay, drill down to Computer Configuration, Administrative Templates, Windows Components, AutoPlay Policies group. Enable the Turn off Autoplay policy. To disable AutoRun, enable the Set the default behavior for AutoRun and use the Disabled option.
3. **Insert a screenshot:**

Click or tap here to enter text.

1. When you finish setting your local security policies, close the Local Group Policy Editor console. To put into effect the changes you have made, reboot the system or enter the command gpupdate.exe in a command prompt window. The gpupdate command refreshes local group policies as well as group policies set in Active Directory on a Windows domain.
2. Change your local policy settings to the default settings. You can also apply a checkpoint you created earlier.

Attach this completed document to the assignment in BlackBoard.