**Practice 2**

**2.1 Install a Virtual Machine on a Personal Computer**

**Objectives**

**Part 1: Prepare a Computer for Virtualization**

**Part 2: Import a Virtual Machine into VirtualBox Inventory**

**Background / Scenario**

Computing power and resources have increased tremendously over the last 10 years. A benefit of having multicore processors and large amounts of RAM is the ability to use virtualization. With virtualization, one or more virtual computers can operate inside a single physical computer. Virtual computers that run within physical computers are called virtual machines. Virtual machines are often called guests, and physical computers are often called hosts. Anyone with a modern computer and operating system can run virtual machines.

A virtual machine image file has been created for you to install on your computer. In this lab, you will download and import this image file using a desktop virtualization application, such as VirtualBox.

**Required Resources**

* Computer with a minimum of extra 4 GB of RAM and 50 GB of free disk space allocated to run virtual machines
* High speed internet access to download Oracle VirtualBox and the virtual machine image file

**Note**: The image file is about 4 GB, and can grow up to 50 GB after the virtual machines are in operation. While you can delete the image file after the virtual machine is imported, the 50 GB free disk space requirement is for users who decide to keep the image file.

**Note**: To install and run 64bit virtual machines on a host physical computer, the computer needs to be a 64bit system and have hardware virtualization technology enabled in BIOS. If you are unable to install the virtual machine image you may need to reboot your computer and enter setup mode in BIOS to enable hardware virtualization technology under advanced system settings.

**Instructions**

**Part 1: Prepare a Host Computer for Virtualization**

In Part 1, you will download and install desktop virtualization software, and also download an image file that can be used to complete labs throughout the course. For this lab, the virtual machine is running Linux.

**Step 1: Download and install VirtualBox.**

VMware Workstation Player and Oracle VirtualBox are two virtualization programs that you can download and install to support the image file. In this lab, you will use VirtualBox.

1. Navigate to [**https://www.virtualbox.org**](https://www.virtualbox.org).
2. Choose and download the appropriate installation file based on your operating system.
3. When you have downloaded the VirtualBox installation file, run the installer and accept the default installation settings.

**Step 2: Download the Virtual Machine image file.**

The image file was created in accordance with the Open Virtualization Format (OVF). OVF is an open standard for packaging and distributing virtual appliances. An OVF package has several files placed into one directory. This directory is then distributed as an OVA package. This package contains all the OVF files necessary for the deployment of the virtual machine. The virtual machine used in this lab was exported in accordance with the OVF standard.

Click [**here**](https://www.netacad.com/resources/lab-downloads) to download the **CSE-LABVM** and the **Security Workstation** OVA files.

**Note:** The files are about 5 GB in total, and it may take over an hour to download, depending on the speed of your internet connection.

**Part 2: Import the Virtual Machine into the VirtualBox Inventory**

In Part 2, you will import the virtual machine images into VirtualBox and start the virtual machines.

**Step 1: Import the virtual machine files into VirtualBox.**

1. Open **VirtualBox**. Click **File** > **Import Appliance...** to import the virtual machine image.
2. In the Appliance to import window, specify the location of the .OVA file. Click **Next** to continue.
3. The appliance settings window appears. In the Machine Base Folder field, you may need to click the dropdown arrow and change the destination by selecting Other and browsing to a folder (you can use your user’s Documents folder). Set the MAC Address Policy to **Generate new MAC addresses for all network adapters**. Leave all other settings as default. Click Import.
4. When the import process is complete, you will see the new Virtual Machine added to the VirtualBox inventory in the left panel. The virtual machine is now ready to use.

**Step 2: Start the CSE-LABVM virtual machine and log in.**

1. In the inventory shown on the left, select the virtual machine you wish to use. In this example, you will select the virtual machine **CSE-LABVM**.
2. Click the **Start** button. It is the green arrow located at the top portion of the VirtualBox application window. A new window will appear, and the virtual machine boot process will start.

**Note**: If the virtual machine fails to start, either disable the USB Controller by going into the virtual machine’s settings and unchecking the USB controller setting under USB, or go to the VirtualBox download webpage and download and install the Oracle VM VirtualBox Extension Pack.

1. When the boot process is complete, the virtual machine will automatically login and load the desktop. If you need superuser access at anytime, use the following credentials for the virtual machine **CSE-LABVM**:

Username: **cisco**

Password: **password**

**Note**: The window running the virtual machine is a completely different computer than your host. Functions such as copy and paste will not work between the two without changing the default settings in VirtualBox. Notice the keyboard and mouse focus. When you click inside the virtual machine window, your mouse and keyboard will operate the guest operating system. Your host operating system will no longer detect keystrokes or mouse movements. Press the right **CTRL** key to return keyboard and mouse focus to the host operating system.

**Step 3: Familiarize yourself with CSE-LABVM.**

The **CSE-LABVM** virtual machine you just installed is one of the VMs that you will be using in the course. Familiarize yourself with the icons in the list below:

The launcher icons are on the left (from top to bottom):

* **cisco's Home** - home directory for the user, **cisco**
* **DPI Scanling** - shortcut command for increasing the resolution
* **Firefox Web Browser** - internet browser
* **jcryptool** - cryptography and cryptanalysis tool
* **Keyboard** - quick access to change your keyboard layout
* **Terminal** - command line access
* **Wireshark** - packet sniffer and network protocol analyzer

1. Open the terminal application. Type the **ip address** command at the prompt to determine the IP address of your virtual machine.

What are the IP addresses assigned to your virtual machine?

Your answer:

1. Locate and launch the web browser application.

Can you navigate to your favorite search engine?

Your answer:

**Step 4: Shutdown the CSE-LABVM.**

1. Press the right ctrl key to release the cursor from the virtual machine. Now go to the menu at the top of the virtual machine window and choose **File** > **Close** to close the virtual machine.

What options are available?

Your answer:

1. Click the Save the machine state radio button and then click OK. The next time you start the virtual machine, you will be able to resume working in the operating system in its current state.

**Step 5: Import and Start the Security Workstation virtual machine and log in.**

1. To import the **Security Workstation**, follow the same procedures you used to import the **CSE-LABVM**.
2. In the inventory shown on the left, select the **Security Workstation**.
3. Click the **Start** button and the virtual machine boot process will start.
4. If you get an error about your Ethernet adapter, click **Change Network Settings**. From the **Name** dropdown list, choose the network adapter your computer is using to connect to the internet, and then click **OK**.
5. When prompted, change the user to **analyst**, enter **cyberops** as the password, and then click **Log in**.

**Step 6: Familiarize yourself with Security Workstation.**

The **Security Workstation** virtual machine is based on the Arch Linux distribution so that you can run a variety of services with minimal impact to your host machine's resources. Feel free to explore the VM as much as you like. However, this VM will be explored in more detail in later labs.

**Step 7: Shutdown the Security Workstation.**

In the VirtualBox menu, choose File > Close, choose Save the machine state, and then click OK.

**Reflection**

What are the advantages and disadvantages of using a virtual machine?

Your answer:

**2.2 Getting Familiar with the Linux Shell**

### Introduction

In this lab, you will use the Linux command line to manage files and folders, and perform some basic administrative tasks.

**Part 1: Shell Basics**

**Part 2: Copying, Deleting, and Moving Files**

### Recommended Equipment

* Security Workstation virtual machine

### Instructions

### Part 1: Shell Basics

The shell is the term used to refer to the command interpreter in Linux. Also known as Terminal, Command Line and Command Prompt, the shell is very powerful way to interact with a Linux computer.

### Step 1: Access the Command Line

1. Log on to the CyberOps Workstation VM as the analyst using the password **cyberops**. The account analyst is used as the example user account throughout this lab.
2. To access the command line, click the terminal icon located in the Dock, at the bottom of VM screen. The terminal emulator opens.

### Step 2: Display Manual Pages from the command line.

You can display command line help using the **man** command. A man page, short for manual page, is a built-in documentation of the Linux commands. A man page provides detailed information about a given command and all its available options.

1. To learn more about the man page, type:

[analyst@secOps ~]$ **man man**

Name a few sections that are included in a man page.

Your answer:

1. Type **q** to exit the man page.
2. Use the **man** command to learn more about the **cp** command:

[analyst@secOps ~]$ **man cp**

What is the function of the **cp** command?

Your answer:

What command would you use to find out more information about the **pwd** command? What is the function of the **pwd** command?

Your answer:

### Step 3: Create and change directories.

In this step, you will use the change directory (cd), make directory (mkdir), and list directory (ls) commands.  
**Note**: A directory is another word for folder. The terms directory and folder are used interchangeably throughout this lab.

1. Type **pwd** at the prompt.

[analyst@secOps ~]$ **pwd**  
/home/analyst

What is the current directory?

Your answer:

1. Navigate to the **/home/analyst** directory if it is not your current directory. Type **cd /home/analyst**

[analyst@secOps ~]$ **cd /home/analyst**

1. Type **ls -l** at the command prompt to list the files and folders that are in the current folder. Standing for list, the **-l** option displays file size, permissions, ownership, date of creation and more.

[analyst@secOps ~]$ **ls -l**

|  |
| --- |
| total 20 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Mar | 22 | 2018 | Desktop |
| drwxr-xr-x | 3 | analyst | analyst | 4096 | Apr | 2 | 14:44 | Downloads |
| drwxr-xr-x | 9 | analyst | analyst | 4096 | Jul | 19 | 2018 | lab.support.files |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Mar | 21 | 2018 | second\_drive |
| -rw-r--r-- | 1 | analyst | analyst | 255 | Apr | 17 | 16:42 | space.txt |

1. In the current directory, use the **mkdir** command to create three new folders: **cyops\_folder1**, **cyops\_folder2**, and **cyops\_folder3**. Type **mkdir cyops\_folder1** and press **Enter**. Repeat these steps to create **cyops\_folder2** and **cyops\_folder3**.

[analyst@secOps ~]$ **mkdir cyops\_folder1**

[analyst@secOps ~]$ **mkdir cyops\_folder2**

[analyst@secOps ~]$ **mkdir cyops\_folder3**

[analyst@secOps ~]$

1. Type **ls -l** to verify that the folders have been created:

[analyst@secOps ~]$ **ls -l**

|  |
| --- |
| total 32 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Aug | 16 | 15:01 | cyops\_folder1 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Aug | 16 | 15:02 | cyops\_folder2 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Aug | 16 | 15:02 | cyops\_folder3 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Sep | 26 | 2014 | Desktop |
| drwx------ | 3 | analyst | analyst | 4096 | Jul | 14 | 11:28 | Downloads |
| drwxr-xr-x | 8 | analyst | analyst | 4096 | Jul | 25 | 16:27 | lab.support.files |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Mar | 3 | 15:56 | second\_drive |
| -rw-r--r-- 1 | 1 | analyst | analyst | 254 | Aug | 16 | 13:38 | space.txt |

1. Type **cd /home/analyst/cyops\_folder3** at the command prompt and press **Enter**.

[analyst@secOps ~]$ **cd /home/analyst/cyops\_folder3**

[analyst@secOps cyops\_folder3]$

Which folder are you in now?

Your answer:

**Note**:In the **[analyst@secOps ~]$** prompt above: The tilde symbol ~ represents the current user’s home directory. In this example, the current user’s home directory is **/home/analyst**. After the **cd /home/analyst/cyops\_folder3** command, the current user’s home directory is now **/home/analyst/cyops\_folder3**.

**Note**:**$** (dollar sign) indicates regular user privilege. If a **‘#’** (hashtag or pound sign) is displayed at the prompt, it indicates elevated privilege **(root user)**.

**Note**: While these symbols, conventions and main concepts remain the same, the prompt of a terminal window is highly customizable in Linux. Therefore, the prompt structure seen in the CyberOps Workstation VM will likely differ from the prompt in other Linux installations..

**Challenge**: Type the command **cd ~** and describe what happens.

Why did this happen?

Your answer:

1. Use the **mkdir** command to create a new folder named **cyops\_folder4** inside the **cyops\_folder3** folder:

[analyst@secOps ~]$ **mkdir /home/analyst/cyops\_folder3/cyops\_folder4**

[analyst@secOps ~]$

1. Use the **ls -l** command to verify the folder creation.

[analyst@secOps ~]$ **ls –l /home/analyst/cyops\_folder3**

total 4

drwxr-xr-x 2 analyst analyst 4096 Aug 16 15:04 cyops\_folder4

1. Up to this point, we have been using full or absolute paths. Absolute path is the term used when referring to paths that always start at the root (/) directory. It is also possible to work with relative paths. Relative paths reduce the amount of text to be typed. To understand relative paths, we must understand the . and .. (dot and double dot) directories. From the **cyops\_folder3** directory, issue a **ls –la**:

[analyst@secOps ~]$ **ls –la /home/analyst/cyops\_folder3**

total 12

drwxr-xr-x 3 analyst analyst 4096 Aug 16 15:04 .

drwxr-xr-x 20 analyst analyst 4096 Aug 16 15:02 ..

drwxr-xr-x 2 analyst analyst 4096 Aug 16 15:04 cyops\_folder4

The **-a** option tells **ls** to show all files. Notice the . and .. listings shown by **ls**. These listings are used by the operating system to track the current directory (.) and the parent directory (..) You can see the use of the . and .. when using the **cd** command to change directories. Using the **cd** command to change the directory to the . directory incurs no visible directory change as the . points to the current directory itself.

1. Change the current directory to /home/analyst/cyops\_folder3:

[analyst@secOps ~]$ **cd /home/analyst/cyops\_folder3**

[analyst@secOps cyops\_folder3]$

1. Type **cd** .

[analyst@secOps cyops\_folder3]$ **cd** .

[analyst@secOps cyops\_folder3]$

What happens?

Your answer:

1. Changing the directory to the .. directory, will change to the directory that is one level up. This directory is also known as parent directory. Type cd ..

[analyst@secOps cyops\_folder3]$ **cd ..**

[analyst@secOps ~]$

What happens?

Your answer:

What would be the current directory if you issued the **cd ..** command at [analyst@secOps ~]$?

Your answer:

What would be the current directory if you issued the **cd** .. command at [analyst@secOps home]$?

Your answer:

What would be the current directory if you issued the **cd ..** command at [analyst@secOps /]$?

Your answer:

### Step 4: Redirect Outputs.

Another powerful command line operator in Linux is known as redirect. Represented by the > symbol, this operator allows the output of a command to be redirected to some location other the current terminal window (the default).

1. Use the **cd** command to change to the **/home/analyst/ (~)** directory:

[analyst@secOps /]$ **cd /home/analyst/**

[analyst@secOps ~]$

1. Use the echo command to echo a message. Because no output was defined, echo will output to the current terminal window:

analyst@secOps ~]$ **echo This is a message echoed to**

**the terminal by echo.**

This is a message echoed to the terminal by echo.

1. Use the > operator to redirect the output of echo to a text file instead of to the screen:

analyst@secOps ~]$ **echo This is a message echoed to the terminal by echo. > some\_text\_file.txt**

No output was shown.

Is that expected? Explain.

Your answer:

1. Notice, that even though the **some\_text\_file.txt** file did not exist, prior to the echo command, it was automatically created to receive the output generated by echo. Use the **ls -l** command to verify if the file was really created:

[analyst@secOps /]$ **ls –l some\_text\_file.txt**

-rw-r--r-- 1 analyst analyst 50 Feb 24 16:11 some\_text\_file.txt

1. Use the cat command to display the contents of the **some\_text\_file.txt** text file:

[analyst@secOps ~]$ **cat some\_text\_file.txt**

This is a message echoed to the terminal by echo.

1. Use the > operator again to redirect a different echo output of echo to the **some\_text\_file.txt** text file:

[analyst@secOps ~]$ **echo This is a DIFFERENT message, once again echoed to the terminal by echo. > some\_text\_file.txt**

1. Once again, use the **cat** command to display the contents of the **some\_text\_file.txt** text file:

[analyst@secOps ~]$ **cat some\_text\_file.txt**

This is a DIFFERENT message, once again echoed to the terminal by echo.

What happened to the text file? Explain.

Your answer:

### Step 5: Redirect and Append to a Text File.

1. Similar to the > operator, the >> operator also allows for redirecting data to files. The difference is that >> appends data to the end of the referred file, keeping the current contents intact. To append a message to the some\_text\_file.txt, issue the command below:

[analyst@secOps /]$ **echo This is another line of text. It will be APPENDED to the output file. >> some\_text\_file.txt**

1. Use the **cat** command to display the contents of the **some\_text\_file.txt** text file yet again:

analyst@secOps ~]$ **cat some\_text\_file.txt**

This is a DIFFERENT message, once again echoed to the terminal by echo.

This is another line of text. It will be APPENDED to the output file.

What happened to the text file? Explain.

Your answer:

### Step 6: Work with hidden files in Linux.

1. In Linux, files with names that begin with a ‘.’ (single dot) are not shown by default. While dot-files have nothing else special about them, they are called hidden files because of this feature. Examples of hidden files are **.file5, .file6, .file7**.
2. **Note**: Do not confuse dot-files with the current directory indicator “.” symbol. Hidden file names begin with a dot (period), followed by more characters while the dot directory is a hidden directory comprised of only a single dot.
3. Use **ls -l** to display the files stored in the analyst home directory.

[analyst@secOps ~]$ **ls –l**

How many files are displayed?

Your answer:

1. Use the **ls -la** command to display all files in the home directory of analyst, including the hidden files.

[analyst@secOps ~]$ **ls –la**

How many more files are displayed than before? Explain.

Your answer:

Is it possible to hide entire directories by adding a dot before its name as well? Are there any directories in the output of ls -la above?

Your answer:

Give three examples of hidden files shown in the output of **ls -la** above.

Your answer:

1. Type the **man ls** command at the prompt to learn more about the **ls** command.

[analyst@secOps /]$ **man ls**

1. Use the down arrow key (one line at a time) or the space bar (one page at a time) to scroll down the page and locate the -a option used above and read its description to familiarize yourself with the **ls -a** command.

### Part 2: Copying, Deleting, and Moving Files

**Step 1: Copying Files**

1. The **cp** command is used to copy files around the local file system. When using cp, a new copy of the file is created and placed in the specified location, leaving the original file intact. The first parameter is the source file and the second is the destination. Issue the command below to copy **some\_text\_file.txt** from the home directory to the **cyops\_folder2** folder:

[analyst@secOps ~]$ **cp some\_text\_file.txt cyops\_folder2/**

Identify the parameters in the cp command above.

What are the source and destination files? (use full paths to represent the parameters)

Your answer:

1. Use the **ls** command to verify that **some\_text\_file.txt** is now in **cyops\_folder2:**

[analyst@secOps ~]$ **ls cyops\_folder2/**

some\_text\_file.txt

1. Use the **ls** command to verify that **some\_text\_file.txt** is also in the home directory:

[analyst@secOps ~]$ ls -l

|  |
| --- |
| total 36 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Aug | 16 | 15:01 | cyops\_folder1 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Aug | 16 | 15:11 | cyops\_folder2 |
| drwxr-xr-x | 3 | analyst | analyst | 4096 | Aug | 16 | 15:04 | cyops\_folder3 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Sep | 26 | 2014 | Desktop |
| drwx------ | 3 | analyst | analyst | 4096 | Jul | 14 | 11:28 | Downloads |
| drwxr-xr-x | 8 | analyst | analyst | 4096 | Jul | 25 | 16:27 | lab.support.files |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Mar | 3 | 15:56 | second\_drive |
| -rw-r--r-- 1 | 1 | analyst | analyst | 142 | Aug | 16 | 15:09 | some\_text\_file.txt |
| -rw-r--r-- 1 | 1 | analyst | analyst | 254 | Aug | 16 | 13:38 | space.txt |

### Step 2: Deleting Files and Directories

1. Use the **rm** command to remove files. Issue the command below to remove the file **some\_text\_file.txt** from the home directory. The ls command is then used to show that the file **some\_text\_file.txt** has been removed from the home directory:

[analyst@secOps ~]$ **rm some\_text\_file.txt**

[analyst@secOps ~]$**ls -l**

|  |
| --- |
| total 32 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Aug | 16 | 15:01 | cyops\_folder1 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Aug | 16 | 15:11 | cyops\_folder2 |
| drwxr-xr-x | 3 | analyst | analyst | 4096 | Aug | 16 | 15:04 | cyops\_folder3 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Sep | 26 | 2014 | Desktop |
| drwx------ | 3 | analyst | analyst | 4096 | Jul | 14 | 11:28 | Downloads |
| drwxr-xr-x | 8 | analyst | analyst | 4096 | Jul | 25 | 16:27 | lab.support.files |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Mar | 3 | 15:56 | second\_drive |
| -rw-r--r-- 1 | 1 | analyst | analyst | 254 | Aug | 16 | 13:38 | space.txt |

1. In Linux, directories are seen as a type of file. As such, the **rm** command is also used to delete directories but the **-r** (recursive) option must be used. Notice that all files and other directories inside a given directory are also deleted when deleting a parent directory with the -r option. Issue the command below to delete the **cyops\_folder1** folder and its contents:

[analyst@secOps ~]$ **rm –r cyops\_folder1**

[analyst@secOps ~]$**ls -l**

|  |
| --- |
| total 28 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Aug | 16 | 15:11 | cyops\_folder2 |
| drwxr-xr-x | 3 | analyst | analyst | 4096 | Aug | 16 | 15:04 | cyops\_folder3 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Sep | 26 | 2014 | Desktop |
| drwx------ | 3 | analyst | analyst | 4096 | Jul | 14 | 11:28 | Downloads |
| drwxr-xr-x | 8 | analyst | analyst | 4096 | Jul | 25 | 16:27 | lab.support.files |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Mar | 3 | 15:56 | second\_drive |
| -rw-r--r-- 1 | 1 | analyst | analyst | 254 | Aug | 16 | 13:38 | space.txt |

### Step 3: Moving Files and Directories

1. Moving files works similarly to copying files. The difference is that moving a file removes it from its original location. Use the mv commands to move files around the local filesystem. Like the cp commands, the mv command also requires source and destination parameters. Issue the command below to move the **some\_text\_file.txt** from **/home/analyst/cyops\_folder2** back to the home directory:

[analyst@secOps ~]$ **mv cyops\_folder2/some\_text\_file.txt .**

[analyst@secOps ~]$**ls –l cyops\_folder2/**

total 0

[analyst@secOps ~]$**ls –l /home/analyst/**

|  |
| --- |
| total 32 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Aug | 16 | 15:11 | cyops\_folder2 |
| drwxr-xr-x | 3 | analyst | analyst | 4096 | Aug | 16 | 15:04 | cyops\_folder3 |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Sep | 26 | 2014 | Desktop |
| drwx------ | 3 | analyst | analyst | 4096 | Jul | 14 | 11:28 | Downloads |
| drwxr-xr-x | 8 | analyst | analyst | 4096 | Jul | 25 | 16:27 | lab.support.files |
| drwxr-xr-x | 2 | analyst | analyst | 4096 | Mar | 3 | 15:56 | second\_drive |
| -rw-r--r-- 1 | 1 | analyst | analyst | 142 | Aug | 16 | 15:11 | some\_text\_file.txt |
| -rw-r--r-- 1 | 1 | analyst | analyst | 254 | Aug | 16 | 13:38 | space.txt |

What command did you use to accomplish the task?

Your answer:

### Reflection

What are the advantages of using the Linux command line?

Your answer: