

Lab - Installing the Virtual Machines

Objectives

Part 1: Prepare a Personal 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 operate inside one 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

- Host computer with a minimum of 8 GB of RAM and 40GB of free disk space
- High speed internet access to download Oracle VirtualBox and the virtual machine image files

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 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.

- Navigate to <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>.
- Choose and download the appropriate installation file for your operating system.
- 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 of 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.

- Download the **cyberops_workstation.ova** and **security_onion.ova** image files from course resources and note the location of the downloaded VM.

Part 2: Import the Virtual Machine into the VirtualBox Inventory

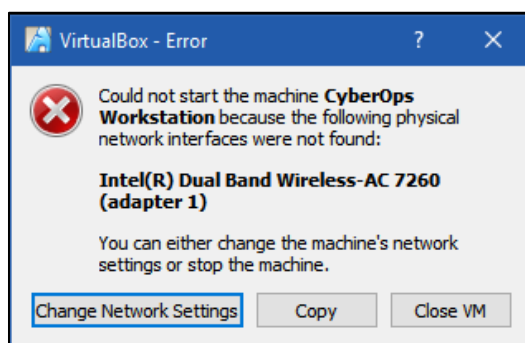
In Part 2, you will import the virtual machine image into VirtualBox and start the virtual machine.

Step 1: Import the virtual machine file into VirtualBox.

- Open **VirtualBox**. Click **File > Import Appliance...** to import the virtual machine image.
- In the Appliance to import window, specify the location of the .OVA file and click **Next**.
- The Appliance window presents the settings suggested in the OVA archive. Review the default settings and change as necessary. Click **Import** to continue.
- 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 virtual machine and log in.

- Select and start a newly-imported virtual machines. The CyberOps Workstation VM is used as an example in this lab.
- Click the green arrow **Start** button at the top portion of the VirtualBox application window. If you get the following dialog box, click **Change Network Settings** and set your Bridged Adapter. Click the dropdown list next the Name and choose your network adapter (will vary for each computer).



Note: If your network is not configured with DHCP services, click **Change Network Settings** and select **NAT** in the Attached to dropdown box. The network settings can also be access via **Settings** in the Oracle VirtualBox Manager or in the virtual machine menu, select **Devices > Network > Network Settings**. You may need to disable and enable the network adaptor for the change to take effect.

- Click **OK**. A new window will appear, and the virtual machine boot process will start.
- When the boot process is complete, the virtual machine will ask for a username and password. Use the following credentials to log into the virtual machine:

Username: **analyst**

Password: **cyberops**

You will be presented with a desktop environment: there is a launcher bar at the bottom, icons on the desktop, and an application menu at the top.

Note: 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 the Virtual Machine.

The virtual machine you just installed can be used to complete many of the labs in this course. Familiarize yourself with the icons in the list below:

The launcher bar icons are (from left to right):

- Show the desktop
- Terminal application
- File manager application
- Web browser application (Firefox)
- File search tool
- Current user's home directory

All course related applications are located under **Applications Menu > CyberOPs**.

- List the applications in the CyberOps menu.
- Open the **Terminal Emulator** application. Type **ip address** at the prompt to determine the IP address of your virtual machine.

What are the IP addresses assigned to your virtual machine?

- Locate and launch the web browser application.

Can you navigate to your favorite search engine?

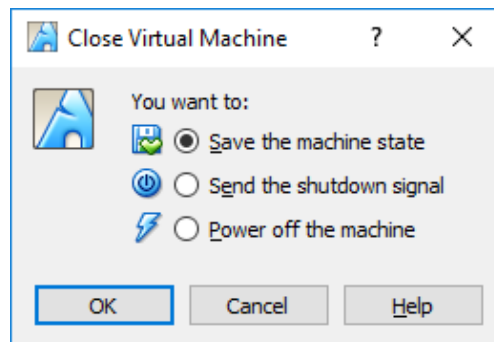
Step 4: Shut down the VMs.

When you are done with the VM, you can save the state of VM for future use or shut down the VM.

Closing the VM using GUI:

From the VirtualBox **File** menu, choose **Close...**

Click the **Save the machine state** radio button and 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.



The other two options are:

Send the shutdown signal: simulates pressing the power button on a physical computer

Power off the machine: simulates pulling the plug on a physical computer

Closing the VM using CLI:

To shut down the VM using the command line, you can use the menu options inside the VM or enter **sudo shutdown -h now** command in a terminal window and provide the password **cyberops** when prompted.

Rebooting the VM:

If you want to reboot the VM, you can use the menu options inside the VM or enter **sudo reboot** command in a terminal and provide the password **cyberops** when prompted.

Note: You can use the web browser in this virtual machine to research security issues. By using the virtual machine, you may prevent malware from being installed on your computer.

Reflection

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