Lab - Deploy a Pre-Built Kali Linux Virtual Machine (VM)

# Objectives

In this lab, you will complete the following objectives:

Part 1: Deploying a Customized Kali Linux VM on AMD or Intel Chip-based Computer

Part 2: Deploying a Customized Kali Linux VM on ARM M1/M2 based MacOS Computer

Part 3: Exploring Linux

# Background / Scenario

Computing power and resources have increased tremendously in a short period of time. A benefit of multi-core processors and large amounts of RAM is the ability to run multiple operating systems on a computer using virtualization.

With virtualization, one or more virtual computers can operate on a single physical computer. Virtual computers that run on physical computers are called virtual machines (VMs). 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.

In this lab, you will first install a desktop virtualization application, such as Oracle VirtualBox, and deploy a virtual machine running a Kali Linux OS.

# Required Resources

* Computer with a minimum of 4 GB of RAM and 50 GB of free disk space
* Internet access to download virtualization software, Oracle Virtualbox or UTM, and VM image

# Instructions

Even though most modern computers can support virtualization, if you are not sure, perform an internet search to determine the capability of virtualization on your PC and enable virtualization as necessary.

Depending on the architecture of your PC, you will either use Oracle VirtualBox or UTM for your virtualization software.

## Deploying a Pre-Built Customized Kali VM on AMD or Intel Chip-based Computer

**Note**: Go to the next part if you have M1/M2 MacOS or other ARM-based devices that can support UTM.

### Download and install VirtualBox.

VMware Workstation Player and VirtualBox are two virtualization programs that you can download and install to run the Kali VM file. In this lab, you will use the VirtualBox application.

* + - 1. Navigate to <https://www.virtualbox.org/>. Click the download link on this page.
			2. Choose and download the appropriate installation file based on your operating system.
			3. After the VirtualBox installation file is downloaded, run the installer and accept the default installation settings.

### Download the pre-built customized Kali.

* + - 1. Navigate to the [Resource Hub](https://skillsforall.com/resources/lab-downloads?courseLang=en-US) from skillsforall.com.
			2. Download the OVA file for this course. Note the location of the downloaded OVA file on your computer.

### Deploy the VM in VirtualBox.

* + - 1. Open **VirtualBox**.
			2. Click **File** > **Import Appliance** to import the downloaded OVA file, **Kali.ova**. Click **Next** to continue.
			3. Review the appliance settings. Increase the amount of RAM if desired. Click **Finish** to continue.
			4. Click **Start** to power up the newly created VM after the appliance has been imported.

## Deploying a Pre-Built Customized Kali VM on ARM M1/M2 Chip-based Computer

**Note**: Do the previous part if you have an AMD or Intel Chip-based Computer.

### Download and install UTM.

In this lab, you will use the free version of the UTM app.

* + - 1. Navigate to <https://mac.getutm.app/>. Click **Download** to download the free version.
			2. After the file is downloaded, install UTM.

### Download and load the pre-built customized Kali.

* + - 1. Navigate to the [Resource Hub](https://skillsforall.com/resources/lab-downloads?courseLang=en-US) from skillsforall.com.
			2. Download the Kali.utm.zip file. Note the location of the downloaded Kali.utm.zip file.
			3. Unzip the zip archive.
			4. Double-click the unzipped file to open the VM in UTM.

## Exploring Linux

### Root Privileges

The root user in Linux is equivalent to the administrator user on windows. The commands **su** and **sudo** allow you to gain root permissions.

The **su** command allows you to become the root user after providing the root password. When you are done with running commands, you will need to type the **exit** command to leave the root shell and back to your own account.

With the **sudo** command, only a single command is run with root privileges using the current user’s password by default.

For the pre-built customized Kali for this course, the user **kali** is configured to use the **sudo** command to access root privileges.

**Note**: These commands are for demonstration only. You will be more familiar with these commands as you become more fluent with Linux.

* + - 1. Root privilege is required to view and edit the file /etc/sudoers. To illustrate the use of root privileges, enter the command **visudo** at the command prompt.

┌──(kali㉿Kali)-[~]

└─$ **visudo**

visudo: /etc/sudoers: Permission denied

Note that you do not have permission to view and edit the file.

* + - 1. To temporarily elevate your permission for root access, enter **sudo visudo** at the prompt. Provide the password **kali** when prompted.

┌──(kali㉿Kali)-[~]

└─$ **sudo visudo**

* + - 1. Scroll toward the end of the file. The highlighted configurations allow any users in the sudo group to execute any commands. Press Ctrl +x to exit the file and do not save any changes.

# Allow members of group sudo to execute any command

%sudo ALL=(ALL:ALL) ALL

* + - 1. Verify that the user kali is part of the sudo group. The **grep** command only prints out the lines that match the given pattern. In this example, the command searches for the word sudo in the file /etc/group and prints out that line. The result confirms that the user kali is in the group sudo.

┌──(kali㉿Kali)-[~]

└─$ **grep sudo /etc/group**

**sudo**:x:27:kali

### Keyboard shortcuts

As you work in the terminal, you may find yourself retyping some commands or trying to remember a command, filename, or folder name. A few keyboard shortcuts can help you become more efficient at the terminal.

* + - 1. You can use the up or down arrow keys to locate and execute the previously entered command. In the terminal, press the up arrow until you find the visudo command.

#### Questions:

*How many times did you need to press up arrow?* **Do not press enter unless you want to run the command again.**

Type your answers here.

*If you wanted to locate the command sudo visudo, how many times would you need to press the down arrow to find it?* **Do not press enter unless you want to run the command again.**

Type your answers here.

* + - 1. What if you were looking for a command that you used a while ago? The command **history** allows you to view all the commands that you have used recently in the same terminal. At the prompt, delete the displayed command if necessary. Enter the **history** command to see a list of recently used commands.

┌──(kali㉿Kali)-[~]

└─$ **history**

 1 visudo

 2 sudo visudo

 3 grep sudo /etc/group

 4 history

The output displays the list of commands with a number beside each command that you just used in the previous step.

* + - 1. You can use a combination of the exclamation point (!) and history number or command string to repeat previously used commands.

#### Questions:

*At the prompt, enter* ***!3****. What command is displayed?*

Type your answers here.

*At the prompt, enter* ***!his****. What command is displayed?*

Type your answers here.

* + - 1. The tab key can help you complete a partial command or file or folder name.

#### Question:

*At the prompt, enter* ***hi*** *and press the tab key. What is the output?*

Type your answers here.

* + - 1. You can continue to add more letters to the command until histo is displayed. Now when you press tab, the command is completed because it is unique to the system.
			2. Tab completion can also be used on files and folders. Enter ls /me and press the tab key. Because the string me is unique in the listing of file and folder names in the root directory, you should see the command completed as ls /media. Press Enter to view the contents of the /media folder.

# Reflection Question

What are the benefits of using either the installer image or the pre-built image to create the Kali VM?

Type your answers here.

end of document