Exploring the Lab Environment

Scenario

In this activity, you will familiarize yourself with the systems you will be using in the course activities.

Using the Lab Interface

To complete most of the labs in this course, you will use one or more Virtual Machines (VMs) hosted on a cloud platform. Each VM works very much like a physical computer, but you access them via your browser. The main thing to remember is that your **WINDOWS**/**START** key will work *on your own computer* not the VM. Take a few moments to familiarize yourself with some other features of the lab browser controls.

□ 1. In this pane, select the **Resources** tab heading. When you have reviewed the Resources tab contents, select the **Instructions** tab to follow these steps again.

The Resources area is used to show the VMs you have available to you plus any downloadable files that may be useful during a lab. You can choose a different ISO disc to load in each VM's DVD drive and also change the virtual network that the VM is connected to. You can also open each VM in a new window if you find it easier to switch between them that way.

□ 2. Looking at the **Instructions** tab again, notice that each of these tasks has a check box for you to use to record your progress. As you complete each step, select the box to mark it as complete.

□ 3. Select the **Help** tab. Select the **Instructions** tab to view these steps again afterwards.

You can use the Help page to get assistance with technical issues and view more advanced information about using the lab interface.

Also note that the Help tab features a zoom control to allow you to make these instructions appear in larger or smaller font. Finally, note the timer counting down below the lab title. You have the option of extending the lab when this reaches 10 minutes so do not worry too much about running out of time.

□ 4. Looking at the pane containing the VM, in the top-left corner, select the **Display** icon 🖥 and select **Full Screen**.

Working in full screen mode is usually best because it allows the maximum possible screen resolution for the VM you are operating. The other options in this menu allow you to fit the VM screen to the browser window or refresh the display, if it does not seem to be updating.

□ 5. If you are using a Windows computer to access these labs, press the **START** key on your keyboard. Notice that this activates the Taskbar on *your* PC. In some browsers, this might also cause the lab environment to exit full screen mode.

□ 6. If necessary, switch to Full Screen mode again then select the **Lightning** icon ⚡ to open the menu—do not select anything from the menu yet.

This menu allows you to send **START** key combinations and the **CTRL+ALT+DEL** key sequence *to the VM*.

There is also a virtual keyboard for use if you find you have trouble typing particular characters. The VMs use a US keyboard layout so if your own physical keyboard has a different layout you may find that some keys do not type the same symbols.

You can also use the **Power** menu to reset or turn off the VM. You should generally only do this if instructed.

□ 7. Select the following Ctrl+Alt+Delete button embedded in the instructions. This activates sign-in on the Windows VM.

□ 8. Now that you are familiar with the lab interface, let's look at the guest VMs you will be using. Select the **Next** button to continue.

Explore Windows VMs

The Windows network contains a domain controller and member server both running Windows Server 2016.

- 🖥 DC1 is configured as the network's domain controller (DC). Normally the DC role should not be combined with other roles, but to minimize the number of VMs you have to run, this machine is also configured as a DNS server and CA (certificate authority) server and will be used for a number of other services and configurations. This VM is configured with a static IP address (10.1.0.1).
- 🖥 MS1 is configured as a member server for running applications. It runs a DHCP service to perform auto addressing for clients connecting to the network. It has the web server IIS and the email server hMail installed. This VM is also configured with a static IP address (10.1.0.2).

You will usually use the username T 515support\Administrator to log on to the Windows PCs. Each user account uses the password T Pa$$w0rd (awful security practice, but it makes the activities simpler for you to complete).

□ 1. At each point in an activity, you should ensure that you are working within the correct virtual machine. The correct VM may usually be accessed by selecting a shortcut link in the instructions. For example, the MS1 VM is currently selected. To switch to the DC1 virtual machine, select 🖥 DC1

> 💡 Virtual machines may also be selected from a menu at the top of the lab user interface or from the **Resources** tab in this pane.

□ 2. With the 🖥 DC1 VM active, select Ctrl+Alt+Delete and then select the password box. Select the icon preceeding the following text to autotype it T Pa$$w0rd.

□ 3. Press **ENTER** or select the arrow button to submit the password and log on.

□ 4. Point to the network icon in the taskbar. The tooltip should read "corp.515support.com."

If a lab is not working as you expect, check that DC1 has identified the network link. If it is listed as "Unknown," disable and enable the adapter to reset it.

□ 5. Right-click the **Start** button and select **Network Connections**.

□ 6. In the *Network Connections* console, right-click the **Ethernet** adapter and select **Disable**.

□ 7. Right-click the **Ethernet** adapter and select **Enable**.

The connection should be identified as "corp.515support.com."

□ 8. Switch to the 🖥 MS1 VM and, if necessary, select the following link to submit Ctrl+Alt+Delete and dismiss the privacy screen. Enter the password T Pa$$w0rd.

□ 9. Point to the network icon in the taskbar. Again, the tooltip should read "corp.515support.com."

□ 10. In Server Manager, select **Tools > DHCP**. Expand the **ms1.corp.515support.com** server node.

The IPv4 node should show with a green tick. If the network on MS1 has been listed as "Unknown," you may also need to restart the DHCP server to activate the scope.

□ 11. Right-click the **ms1.corp.515support.com** server node, select **All Tasks**, and select **Restart**.

□ 12. Right-click the **ms1.corp.515support.com** server node and select **Refresh**.

□ 13. Select the **IPv4** node and confirm that it is shown with a green tick icon.

In some tasks, you will be asked to install software or other resources from a DVD. The lab user interface can load DVD ISO images for you.

□ 14. Select this link ODYSSEUS to load a DVD in MS1's optical drive.

□ 15. Open **File Explorer** from the taskbar and browse to the DVD drive. You should see the contents of the **Odysseus** DVD. Do not install any software at this time.

□ 16. Select **Start** and then right-click **Windows PowerShell** and select **Run as administrator** to open an elevated PowerShell prompt. Select **Yes** in the UAC prompt.

> In some exercises you will use the traditional Windows command prompt (cmd.exe) and in others you will use Windows PowerShell.

□ 17. The lab interface can automatically type commands for you when you are using Windows virtual machines. For example, select `hostname` and observe that the command is typed in the PowerShell console of the VM.

□ 18. Enter `Get-NetIPAddress` to display the IP address configuration for each interface.

□ 19. Enter `exit` to close PowerShell.

Explore PT1-Kali VM

The PT1-Kali VM is running the Kali pen testing/forensics Linux distribution, created and maintained by Offensive Security (kali.org). You will be using this VM for some security posture assessment and pen testing activities, as well as general Linux configuration management. Kali is based on the Debian Linux distribution with the GNOME desktop environment.

□ 1. Select the PT1-Kali VM. Note that this VM has not been started automatically. Select the **Start** button to boot it now.

> In some browsers, you may see the **Start** button superimposed on the previous VM desktop. This is a graphical bug, which should clear when you select the button.

□ 2. When the VM has started, log on with the username `root` and the password `Pa$$w0rd`.

> ⚠ In this virtualization environment, the Linux VMs can fail to register the first key press after you click into the screen. Also, you cannot use the automatic Type Text feature with the Linux virtual machines.

> Kali will screen lock if not used. To restore the screen, click-and-drag the privacy shader up, rather than just clicking it.

□ 3. Take a few moments to familiarize yourself with the desktop. Some key points to note are:

- The desktop contains shortcuts to some of the applications, notably Firefox (web browser), Thunderbird (email client), and Wireshark (packet capture and analysis).
- On the top menu panel, you can access shortcuts to all applications plus shortcuts for the file browser and terminal. When you open windows, you can use this panel to switch between them.
- The **Network** icon in the top menu panel allows you to change network settings using the Network Manager application.
- The **Power** icon allows you to reboot and shut down the VM.

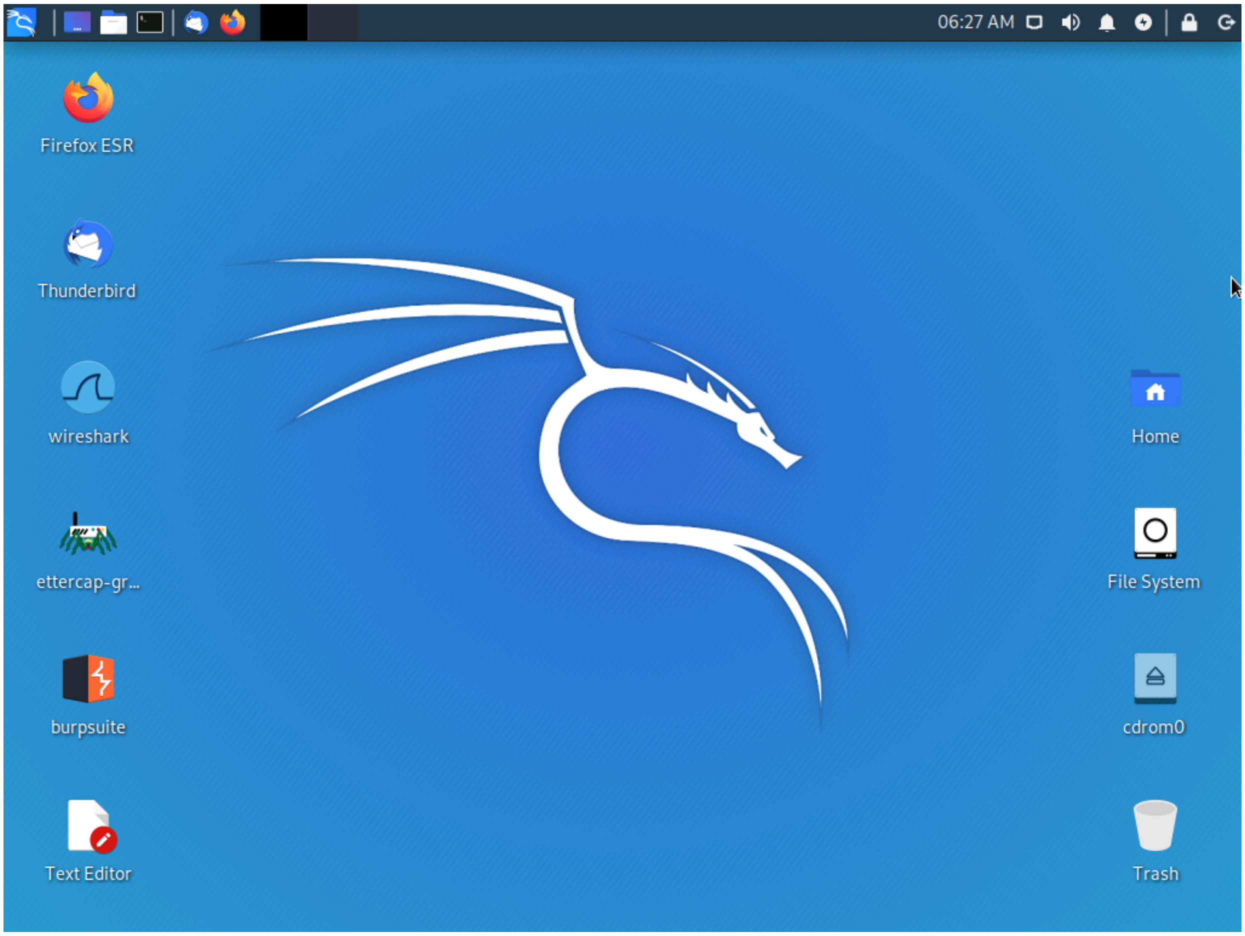

Figure: Gnome desktop in the KALI VM. Use the Dash to open applications and the menu bar to configure settings such as the network interface. (Screenshot used with permission from Offensive Security.)

□ 4. Right-click the desktop and select **Open Terminal Here**.

□ 5. Run `ip a` to check the network adapter configuration.

> Remember that the Linux command-line is case-sensitive. Also recall that Type Text is not available. You will have to manually enter commands when using the Linux virtual machines.

The main eth0 adapter is configured to use DHCP. The DHCP servers are configured to reserve an address where the last octet is .192 for the PT1-Kali VM.

□ 6. Run the following two commands to start the web server and open the local website in the browser:

```
systemctl start apache2
```

```
firefox http://localhost
```

Note the way that the commands are formatted within separate shaded boxes. When entering longer commands, ignore any line breaks *within* the shaded boxes.

Identify Appliance VMs

In the activities, you will use various security appliance VMs to implement network routing and security functions. These appliance VMs are as follows:

- RT1-LOCAL | RT2-ISP | RT3-INT VMs — these VMs are running the VyOS Linux distribution (vyos.io) and are used to route traffic between the different subnets configured on the various virtual switches. You will be discovering more about the network topology in later activities so we will not explain more here.

  > If you do want to investigate the VyOS configurations, the username is `vyos` and the password is `Pa$$w0rd`.

- UTM1 — this is a UTM security appliance created by Netgate (pfsense.org) from the OpenBSD version of UNIX. pfSense is operated using a web GUI (`http://10.1.0.254`). The username is `admin` and the password is `Pa$$w0rd`. This VM is not included in this orientation lab.

- SIEM1 — Security Onion (securityonion.net) is a network security monitoring (NSM) tool. It provides various GUI and web interfaces to its intrusion detection and incident monitoring tools. The username is `administrator` and the password is `Pa$$w0rd`. This VM is not included in this orientation lab.

Identify Linux Server VMs

There are also two Linux servers:

- LAMP is built on the Ubuntu Server distribution (ubuntu.com) and runs the familiar Linux, Apache, MySQL, and PHP functions of a web server. LAMP is also installed with email and DNS servers. As a server distribution, this VM has no GUI shell. The username is `lamp` and the password is `Pa$$w0rd`. This VM is not included in this orientation lab.
- LX1 is a CentOS Linux distribution (centos.org) that has been installed with intentionally vulnerable web services. This VM is usually positioned on the local network with the Windows VMs and has a DHCP reservation for the address `10.1.0.10`. The username is `centos` and the password is `Pa$$w0rd`

Assisted and Applied Lab Activities

To complete the labs in this series, you must submit a response to each scored task. This lab series comprises two different types of activity with different rules for scoring:

- Assisted labs confirm your knowledge and guide you through the steps to achieve a given configuration. In an assisted lab, if you get a scored question incorrect, you may repeat the question and achieve the correct answer. You do not need a correct answer to move forward through the lab.
- Applied labs challenge your ability to configure given settings and display knowledge of concepts, tools, and options without detailed step instructions. In an applied lab, if you get a scored question incorrect, you may not repeat the question or change your answer. You do not need a correct answer to move forward through the lab.

The type of activity—assisted or applied—is indicated in the lab title.

Many of the tasks are scored by a script that checks whether you have completed the required configuration or output. When completing a scripted task, you must use the same case-sensitive name, output folder, or other label as directed by the lab instructions or your response may be marked as incorrect. For example, if the task instructs you to create a user account named `user01`, then `user1` or `User01` would be marked as incorrect.

□ 1. On the MS1 VM, open PowerShell.

□ 2. Run the following command to output the IP configuration to a text file:

```
ipconfig /all >$env:USERPROFILE\Desktop\ipconfig.txt
```

Check

□ 3. What information is output by the ipconfig command?

○ Address information for local interfaces
○ Address information for remote interfaces
○ Port configuration for local services
○ Port configuration for remote services
○ All of the above

Check

Comprehensive questions

Each lab ends with a set of comprehensive questions. Answer these to ensure that you recognize the importance of the activity steps and the uses for the information you have learned.

□ 1. Which of the following domains should be identified by the network adapter configuration on the Windows VMs?

○ corp.515support.com
○ comptia.org
○ labs.comptia.org
○ Unknown network

Check

□ 2. In which type of lab can you change your response to a scored item?

○ Assisted lab
○ Applied lab

Check

Grade Lab

That concludes this lab. When you have finished a lab, please ensure you end it properly using the **Submit** button rather than just closing the browser window.

□ 1. Select **Submit** below to grade the lab. Once you select **Submit**, you will not be able to return to the lab environment.

> You can use the **Menu** button ☰ to save the lab state and return to it later. Note that you can only have a limited number of labs in a save state at any one time. You can also use the **Menu** to end (cancel) a lab. This means that no score will be recorded and that the next time you launch the lab it will be reset to its starting conditions.