PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Networks and Cybersecurity Essentials (ACCA4024)

Lab 5: Set up Virtual Lab

Cisco | Networking Academy®
Mind Wide Open™

paloalto NETWORKS
Cybersecurity Academy

n.kaliyamurthy@uwtsd.ac.uk | m.murira@uwtsd.ac.uk

Task

- **Set up a Lab Environment**
- **Use SBA Packet Tracer and complete the basic network configurations. (Self-marking Packet Tracer (.pka) file is available in Moodle)**
- **Decrypt SSH Traffic**
- **Back up Firewall Logs**

Description [1]

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.

What you need?

Computer with a minimum of 2 GB of RAM and 8 GB of free disk space
High speed Internet access to download Oracle VirtualBox and the virtual machine image file. While you can delete the image file after the virtual machine is imported, the 8 GB free disk space requirement is for users who decide to keep the image file.

Note: The image file is about 2.5 GB, and can grow up to 5 GB after the virtual machine is in operation.

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.

SET UP A LAB ENVIRONMENT

How to do?

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.

VMware Player and Oracle VirtualBox are two virtualization programs that you can download and install to support the image file.

[1] Cybersecurity Essentials – Cisco Networking academy

In this lab, you will use VirtualBox.

1) Navigate to https://www.virtualbox.org/
2) Choose and download the appropriate installation file for your operating system. (Download the latest version available along with extension pack)
3) When you have downloaded the VirtualBox installation file, run the installer and accept the default installation settings.
4) 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.
5) Navigate to the Cybersecurity Essentials Virtual Machines (VMs) page on netacad.com. Alternatively, download from this Link
6) Download the **Ubuntu_CyberEss.ova** image files and note the location of the downloaded VM.
7) Open **VirtualBox**. Click **File > Import Appliance...** to import the virtual machine image.
8) In the Appliance to import window, specify the location of the .OVA file and click **Next**.
9) The appliance settings appear. Check the Reinitialize the MAC address of all network cards box at bottom of the window. Leave all other settings as default. Click Import.
10) 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.
11) Select and start a newly-imported virtual machines.
12) In the inventory shown on the left, select the virtual machine you wish to use.
13) Click the Start button. It is the green arrow located at the top portion of the VirtualBox application window.
14) A new window will appear, and the virtual machine boot process will start.
15) When the boot process is complete, the virtual machine will ask for a username and password.
16) Use the following credentials to log into the virtual machine:

    Username: cisco

    Password: password
17) 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.
18) Use the Ubuntu_CyberEss virtual machine you just installed to complete the labs that require Ubuntu in this course. Familiarize yourself with the icons in the list below:

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

(i) Search Tool

(ii) File manager application

(iii) Firefox Web Browser

(iv) Ubuntu Software Center

(v) Amazon

(vi) System Settings

(vii) Terminal

(viii) Trash

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.

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 special software tools installed. 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.

Task 2: Use SBA Packet Tracer and complete the basic network configurations. (Refer to Lab 5.1 SBA Final in in Moodle. Download the file, Open with Packet Tracer, Complete the Work and Submit in Moodle)

Task 3: Decrypt SSH Traffic (Refer to Lab 6 from Palo Alto Network Security Fundamentals Course. Complete the activity using NDG Platform)

Task 4: Back up Firewall Logs (Refer to Lab 8 from Palo Alto Network Security Fundamentals Course. Complete the activity using NDG Platform)

Record your reflection
1. List out the options which are available in your virtual machine menu. 2. Find out the IP address of your virtual machine. 3. Could you browse through the Internet? 4. On your own words, share your experience on setting up the virtual machine. 5. What do you think as the pros and cons of using virtual machines?

Learnings from lab:

Part 1

- ✓ ***Build a Simple Network***
- ✓ ***Understand and configure IP Address***
- ✓ ***Use Ping/ Trace route Utility to check the connection status***
- ✓ ***Use ipconfig /all command to determine the MAC address of a Windows computer on an Ethernet network.***
- ✓ ***Analyze a MAC address to determine the manufacturer.***
- ✓ ***Analyze the Wired and Wireless Network connection.***
- ✓ ***Analyze Address Resolution Protocol (ARP).***
- ✓ ***Connect to a Wireless Router and configure the basic settings in a wireless router***
- ✓ ***Use nslookup command to understand the url to ip conversion***
- ✓ ***Build a Small Network, do basic configurations and establish a successful network connectivity.***
- ✓ ***Use simulated/real time environment in packet tracer.***
- ✓ ***Configure DHCP and Firewall***
- ✓ ***Create and Analyse Packet Captures***
- ✓ ***Work with Self Marking Packet Tracer Files***
- ✓ ***Decrypt SSH Traffic***
- ✓ ***Backup Firewall Log Files***

Part 2

- ✓ ***Set up a virtual lab environment***
- ✓ ***Troubleshoot (if required) the installation process of the virtual machine***
- ✓ ***Work with virtual machines***