Lab 01 – Virtualizing Your Machine
That is, a Linux Virtual Machine

Introduction

Cybersecurity professionals practice and test defense and offense in protected environments. No matter what subfield you enter, installing and using a virtual machine is a useful tool for testing out new software and processes. In this lab, you will set up a virtual machine inside a virtual machine manager on your own computer.

Why might we want to use virtual machines? Here are a few reasons.

1) **Security:** What happens on the virtual machine stays on the virtual machine (usually). This protects your host machine and other VMs from any processes/tasks that may be harmful to your computer.
2) **Experimentation:** You can work with other operating systems and hardware simulations than the setup on your machine. Need we say more?!
3) **Flexibility:** You can freeze, suspend, pause, or reset a virtual machine. You can also take a snapshot of a given state and come back or restore to that state.
4) **Cloning:** You can create an operating system already bundled with the software packages you'd like to provide to others and create multiple instances of that version – we will use a Linux operating system bundled with a forensics toolkit.
5) **Efficiency:** The virtual machine manage can controls all access to system resources, including multiple, different OSes.

Terminology

- Your own computer is called the **host machine** or computer.
- The virtual machine you install is called the **guest machine** or computer.
- Virtual machines are housed in a **virtual machine manager** (**VMM**).
- An entire operating system (Windows, Macintosh, Linux) is a piece of software in and of itself. When treated as a file to be imported, exported, or investigated, we frequently refer to an operating system as an **image**.

The two major options for virtual machine managers are VirtualBox and VMWare.

- **VirtualBox** works with Windows and MacOS, and is open-source and free.
- **VMWare** has a free version for Windows (Player) only. However, the College of Business has a licensing arrangement for all cybersecurity to down VM Workstation (for Windows) or VM Fusion (for Macs). You can check your ASAP-preferred email for a recent subscription notice from "Kivuto".

For these lab instructions, we'll download VirtualBox … but you are free to use either manager.

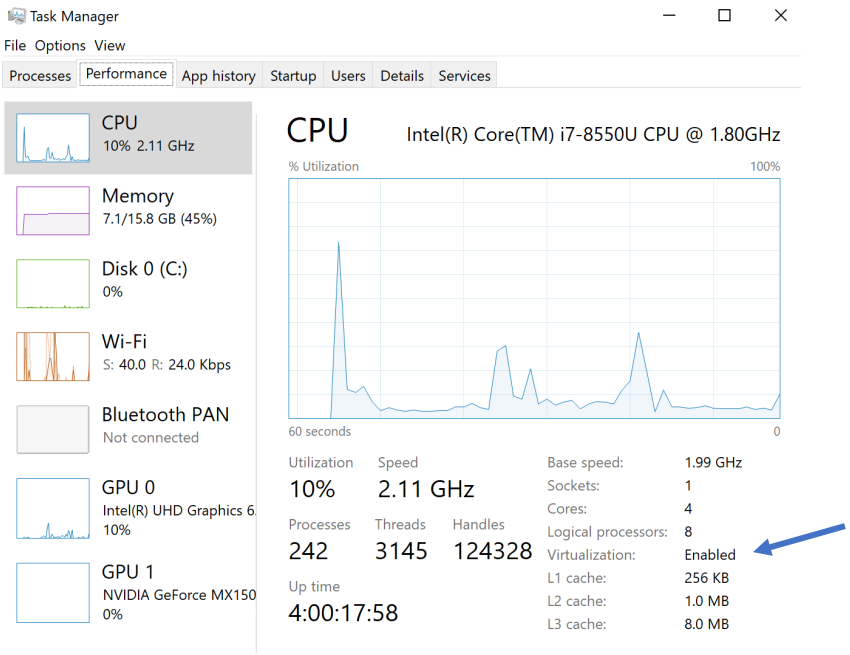
Okay, here we go! Please read Steps 0 through Steps 9 of these lab instructions thoroughly – and at least twice – before starting the lab. Take notes or highlight important points as you go along.

Step 0: Save, Secure, and Set Up!

- **Important Precaution #1**: Before you get started, ***please back up your files***! In case something goes wrong, make sure you have your files saved elsewhere…a flash drive, Google Drive, OneDrive, etc.
- **Important Precaution #2**: Set your computer to ***NEVER sleep or hibernate***. That way, you will not accidentally implement the issue under the next precaution.
- **Important Precaution #3**: Please ***do not click or double-click on the Linux operating system file*** (image) that you download. Repeat, ***please do not touch this image directly***. Rather, you will import it into your virtual machine manage through a file window.
- **Important Final Tip:** ***Set up your lab report before starting Step 1***. That way, you can take screenshots and insert as you go along, and revise or add your commentary later. To do this, open up the *lab report template* and save with the filenaming convention ***lastname_UTSAID*_1003_lab01.pdf**. You may want to write up the *Introduction* section as a draft and then return to it after you've completed the lab. The *Procedure* portion will consist of Step 3-6 below.

Step 1: Check Your BIOS Settings

Before you start installing your virtual machine, you may want to check your BIOS settings to make sure virtualization is *enabled*. On Windows, search for Task Manager in your search box, click on CPU, and look for the "virtualization" parameter. Here is one view – yours may look a little different.



(Macintosh systems should have this enabled by default. You may double-check using these steps: https://apple.stackexchange.com/questions/224870/how-to-check-vt-x-status-on-macbook-pro).

What if virtualization is not enabled?

These links may also be helpful for determining if virtualization is enabled on your system *and* then modifying that setting if virtualization is not enabled (in other words, you may actually need to access the BIOS settings).

- http://www.sysprobs.com/disable-enable-virtualization-technology-bios

- https://support.bluestacks.com/hc/en-us/articles/115003174386-How-can-I-enable-virtualization-VT-on-my-PC-

However, these links may not be relevant for your system. If they do not do the trick, perform a search in your favorite engine to find specific directions for your computer…for example, if you are working with a Windows 10 Dell machine, search with the string "enable virtualization in bios windows 10 Dell".

INCLUDE COMMENTARY AND SCREENSHOTS OF THIS STEP

Comment on how you found verified your BIOS settings and your results. If you run into trouble, post a comment on the **Lab 01 Slack channel** thread with a screenshot and description of your manufacturer, model, and issue. Someone else may have the same manufacturer and offer assistance. If you've figured out a solution, please post that as well to help your peers, and include it in this writeup.

Step 2: Do Some Reading and Watching

You can find many instructions on installing virtual machines on the Internet, both written and video. Search for a few to make sure you understand the process. You can include keywords such as "Install", Virtual Box", "Ubuntu 20.04" and "Windows 10". Try a few techniques. If you are too specific, you may not get the best hits, but you definitely want to narrow down your search to your virtual machine manager, your Linux operating system, and your own ("host") operating system.

I simply typed in "install ubuntu 20.0.4 virtualbox windows 10" and found these instructions, which I found helpful:
https://fossbytes.com/how-to-install-ubuntu-20-04-lts-virtualbox-windows-mac-linux/
You may find other links that you like better, however! Read the above and a few more until you feel comfortable moving forward.

Note of encouragement 😊: You may need to experiment a bit no matter which installation method you try, or start over from scratch to redo the settings. This is part of the process! One of the best things about virtual machines is that they can serve as temporary experiments and throwaways. You can delete them from your virtual machine manager at any time without deleting the actual image, and start over – or you can download the image again and start from scratch.

INCLUDE COMMENTARY OF THIS STEP

Save your links in the References section of your lab report.

Step 3: Download Your Virtual Machine Manager

Download the latest version of VirtualBox (at the time of this writing, 6.1.18, https://www.virtualbox.org/wiki/Downloads), making sure that you select the correct link for your operating system (Windows hosts or OS X Macintosh).

VirtualBox 6.1.18 platform packages

- Windows hosts
- OS X hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

After your download completes, you will see something like this file in your default Downloads folder – this file is for a Windows machine:

NO COMMENTARY OR SCREENSHOTS REQUIRED FOR THIS STEP

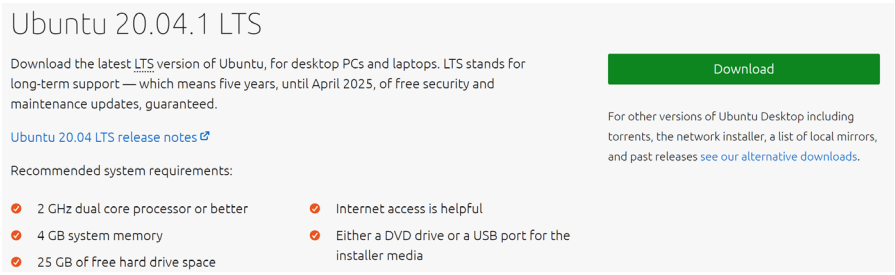
Step 4: Select and Download a Linux Distribution

Next, you will download your chosen operating system file (called an **ISO "image"**) – in Linux, these are called **distributions**, **distros**, or **flavors**, because so many variants exist.

(Are you already familiar with virtual machines and/or Ubuntu? You can check out some of the **alternatives** at the end of this document if you'd prefer to tackle something new.)

You can choose where you want to download your operating system file to—the default is often Downloads in Windows, but you can move this file to another location of your choosing. One good practice is to create a folder for your virtual machine images. The writer has about five operating system images on one computer under "Virtual Machine ISOs" right now, and a few more stored on Google Drive.

Many distributions (distros or flavors) of Linux exist. Most can be downloaded for free. For this lab, we will be setting up a user-friendly version, Ubuntu 20.04.1 LTS (https://ubuntu.com/download/desktop). (We are using this version because it has long-term support (LTS)). Make sure to read the recommended system requirements. Then click on the Download button.



You will see something like this file in your download folder.

Reminder of Precaution #3: ***Do not click on this file!!*** This might start an installation process that will write over your host computer's hard drive with the guest operating system!

INCLUDE COMMENTARY AND SCREENSHOTS OF THIS STEP

You should have completed #1 on the FossBytes site now. Please confirm by sharing a screenshot of your downloaded files, including their timestamps and a description of any issues you may have had, or a confirmation of no issues encountered.

Step 5: Install and Setup VirtualBox

Follow steps #2 and #3 in FossBytes to install VirtualBox. One edit you may want to make: Instead of 4 GB of virtual RAM for the recommended memory size, 2 GB (or 2048 MB) should be plenty.

INCLUDE COMMENTARY AND A SCREENSHOT OF THIS STEP

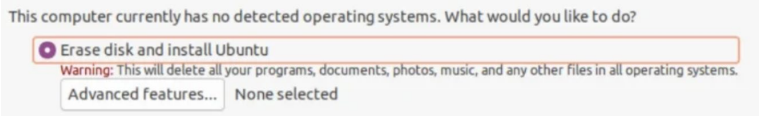
Take a screenshot of your VirtualBox interface and its settings. Include a brief commentary above your screenshot of any interesting challenges or insights you encountered during this process.

Step 6: Import Ubuntu Into VirtualBox

So why isn't VirtualBox "doing" anything? VirtualBox is a virtual machine **manager**. It's a house for your operating systems to live in. It does nothing on its own. So, you must, in addition to Virtual Box, have an **operating system** (or more than one!) to load into it.

Think of a manager of a company with no store, no products, no employees, and no vendors. There would be nothing for the manager to do. So now, you will import your Ubuntu operating system inside your virtual machine. Here's some important points regarding the FossBytes Steps #3-#6.

- When prompted at this screen, *do* choose the Erase disk option:



  This is not referring to your host operating system, but rather, the space reserved for your Ubuntu OS.
- Skip Step #5!
- In Step #6, pick a username that identifies you uniquely and includes at least your last name somewhere (for example, I often choose rita-mitra).
- Step #7 can be a little tricky, but it's worth it to have the full screen functionality. Post on Slack if you run into issues.

After you completed the setup, it's time to ***test*** it! Power down your Linux operating system and VirtualBox. Start your virtual machine back up, and power up your Linux operating system. Login. Is everything working? If not, it's time to troubleshoot. Search on the Internet, post on Slack, and/or contact your instructor.

Commentary and Screenshots of This Step:

This is the bulk of the lab. Describe your setup process and any challenges in detail. Include two screenshots to accompany the setup: 1) your VirtualBox interface and a display of the virtual machine properties/settings in the righthand pane and 2) your virtual machine desktop powered up and running. If you have any issues, post to the **Lab 01 Slack Channel**. Again, help your colleagues where you can.

Step 7: Explore Your New Operating System!

Click around the desktop and see what's there. What icons are on the desktop? What is the default browser? Comment on at least five features. One of these features should be the **terminal**, described next.

About the **terminal**: You are likely more comfortable using a graphical user interface of Windows or Mac. But cybersecurity folks need to also be familiar with the command-line interface (CLI), or terminal. GUIs are layered on top on the bare shell of an operating system to make them more user friendly, but we, as cybersecurity professionals, need to know how to use the terminal as well. See here for the differences: https://www.computerhope.com/issues/ch000619.htm.

You can open a terminal in Linux in a few ways, but one of the easiest is CTRL + ALT + T
See here for some other methods: https://www.lifewire.com/ways-to-open-a-terminal-console-window-using-ubuntu-4075024.

Commentary and Screenshots of This Step

Include the commentary of five features, as required above, along with any interesting screenshots. At a minimum, you should include a screenshot of your terminal with your username displaying.

Step 8: Write a Conclusion

Conclude your report with documentation of any issues still remaining. Your description of the current status of this lab is more important than successful completion of the installation.

In addition, share your experiences and thoughts on this lab – was it helpful? Not helpful? What would you like to explore further on this topic?

Step 9: Cites and Collaborations

List any references you used in this document and/or your searches on the Internet. Also, include a summary of how you utilizes Slack and/or online forums for this lab, whether you posted a problem, solution, or both. Your documentation and research will be essential in your future work in this field.

Step 10: The End

Turn in your lab report on Blackboard.

Alternatives to Lab 02

Some of you are taking this class after several others in the cybersecurity curriculum, and/or you've already familiar with virtual machines. If so, you are free to proceed with the above lab, and document in such a way that you can use the lab in your portfolio, and/or you may try out one of these alternatives.

1. Install Ubuntu Server instead: https://ubuntu.com/download/server. And then follow these instructions to set up SSH: https://hibbard.eu/install-ubuntu-virtual-box/ communication.
2. Do some research and install any security-related Linux operating system that you have not tried out yet: Kali, Parrot, QubesOS.

For either option, report on why you chose the operating system, any challenges you encountered, your solutions, and your opinion of the operating system. In addition, please complete Steps 6 and 7 above as part of your lab report.