Hands-on Keyboard: Cyber Experiments for Strategists and Policy Makers

VirtualBox and Ubuntu

1. Introduction

Linux is a (mostly) free and (mostly) open-source alternative to the Windows and Macintosh operating systems (OS). There are many different distributions of Linux, including Ubuntu, Red Hat, Fedora, Mandriva, and Slackware. See the website distrowatch.com for additional distributions. Ubuntu is very popular because it is easy to use and works "out of the box" with most hardware.

VirtualBox is a free program used to create virtual machines. For example, VirtualBox enables users to run a Linux virtual environment on a Windows host, a Windows virtual environment on a Linux host, a Windows 7 virtual environment on Windows 7 host, etc. This brief activity introduces you to VirtualBox and the Ubuntu OS. The goal of this exercise is to create a virtual Ubuntu machine and execute a few Linux commands.

1.1. Objectives

- Create a virtual machine with VirtualBox
- Install the Ubuntu Linux OS in the virtual machine
- Execute basic Linux commands on the virtual machine

The Air Force Cyber College thanks the Advanced Cyber Engineering program at the Air Force Research Laboratory in Rome, NY, for providing the information to assist in educating the general Air Force on the technical aspects of cyberspace.

1.2. Materials

- Computer with access to an account with administrative rights
- VirtualBox
- Ubuntu OS iso file

1.3. Assumptions

- The instructions provided for this activity were tested using a Windows 8 physical machine and an Ubuntu 15.10 image. Instructions may vary for other OS.
- The student has administrative access to their system and possesses the right to install programs.
- The student's computer has Internet access.

1.4. Hash Functions

A hash function takes a variable-length data set and returns a value of a fixed length. Cryptographic hash functions allow easy verification that an input maps to a given hash value but makes it difficult (computationally expensive) to reconstruct the original input given a hashed value. Any change to a given file results in an entirely different hash value. A hash value is used to determine whether any changes have occurred to a file. For example, the hash value is calculated before the file is transferred and again once the file is received. If the hash values are the same, then the file was likely not compromised.

Two common hash functions are Message Digest 5 (MD5) and Secure Hash Algorithm (SHA). MD5 returns a 128-bit hash. In 1996, the first flaw with MD5 was found. In the years that followed, more serious flaws were discovered. MD5 is not collision resistant. It is possible to produce two different files with the same MD5 sum. There are four different SHA algorithms named SHA-0, SHA-1, SHA-2, SHA-3. SHA-1 corrects the error found in SHA-0. Security flaws were found in SHA-1 in 2005. There have been no successful attacks on SHA-2 to date. However, SHA-2 can be broken with a brute force attack. The newest hash standard, SHA-3, was announced in October 2012 and released in August 2015.

For further information on MD5 and SHA see:
https://help.ubuntu.com/community/HowToMD5SUM
https://help.ubuntu.com/community/HowToSHA256SUM

1.5. Hypervisors

A "hypervisor" (also known as a virtual machine monitor [VMM]) is a software or hardware device that abstracts away the details of hardware so that another "virtual machine" can run on top of the virtual "hardware." In this sense, a hypervisor provides a software version of what the OS above it believes is hardware. A software layer directly above the basic input/output system (BIOS) and other firmware is typically necessary to provide this "virtualized hardware." The hypervisor acts as a mediator between the OS layer and the underlying hardware. This allows

multiple virtual machines (VM) to share a hardware pool or platform. Virtualization provides numerous benefits ranging from logical segregation of systems to transparent geographic separation.

As shown in figure 1, hypervisors are generally categorized as either Type-1 (native) or Type-2 (hosted). Type-1 hypervisors run "on bare metal"—in other words, these hypervisors are not run on top of an OS. Type-2 hypervisors run on top of another OS.

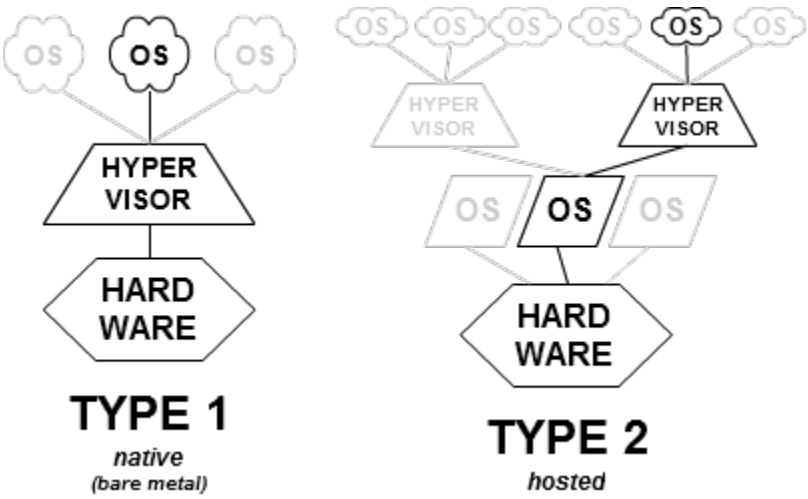


Figure 1. Hypervisor types (Reprinted from https://en.wikipedia.org/wiki/hypervisor#/media/file:hyperviseur.png)

Hypervisors such as Oracle VirtualBox and Client Hyper-V enable personal computers to host several logically segregated virtual machines on the same "host" machine. This lab will use VirtualBox.

2. Download and Install VirtualBox

2.1. Download

- Navigate to https://www.virtualbox.org/wiki/Downloads.
- Download the latest VirtualBox binary for your OS.

2.2. Install

- Start the installation by double-clicking the downloaded file and clicking run.
- Follow the on-screen prompts to complete the installation of VirtualBox.

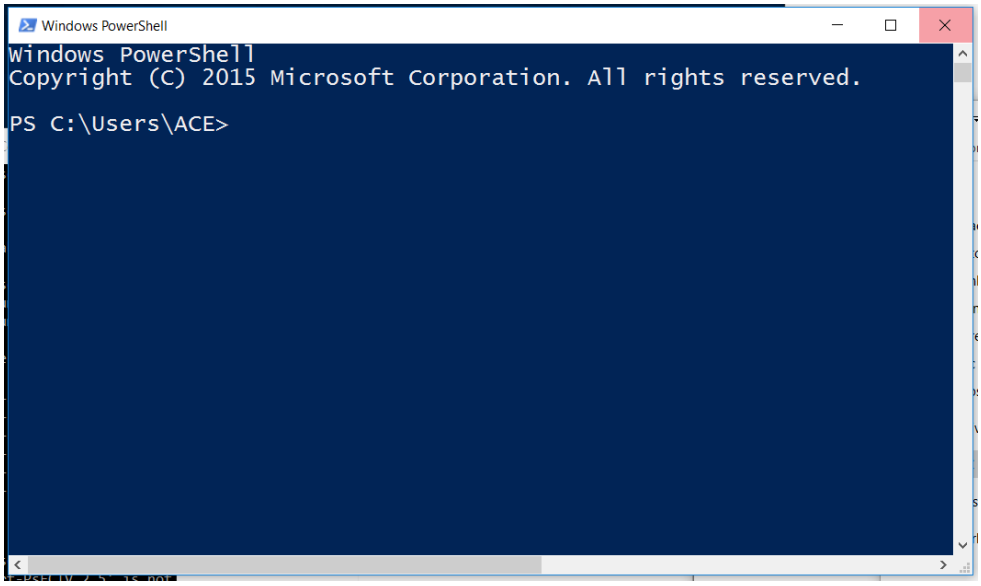
3. Download Ubuntu OS .iso File

- Download the latest Ubuntu .iso file from http://www.ubuntu.com/download/desktop.

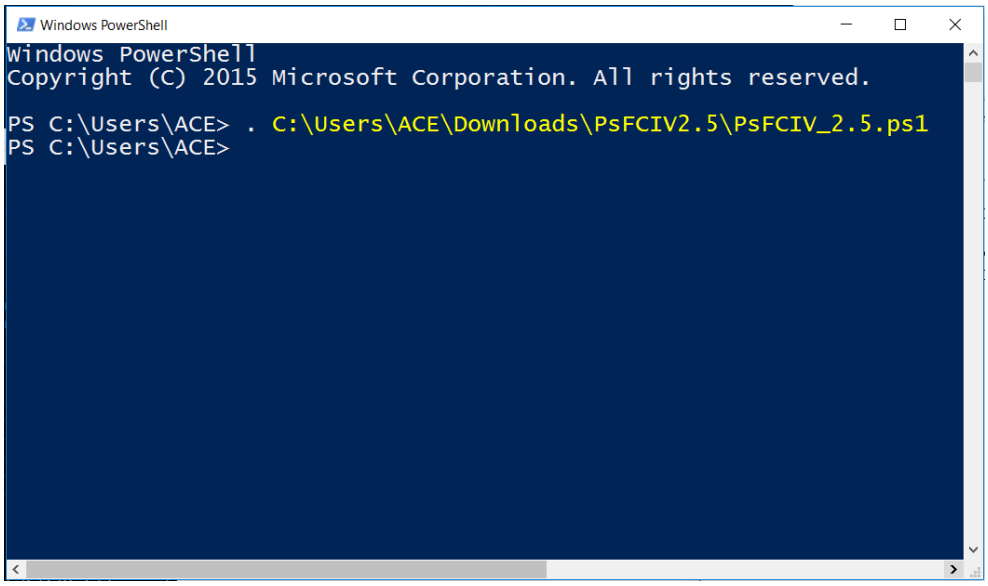
- Use the drop-down menu to choose 32 bit or 64 bit, depending on your processor (when in doubt, choose 32 bit).
- Click "Get Ubuntu."
- Scroll down on the following page and select "Not now, take me to the download" in the bottom left corner. This will begin download of the Ubuntu .iso file.
- Find a list of Ubuntu MD5sums to verify the file downloaded correctly at https://help.ubuntu.com/community/UbuntuHashes.

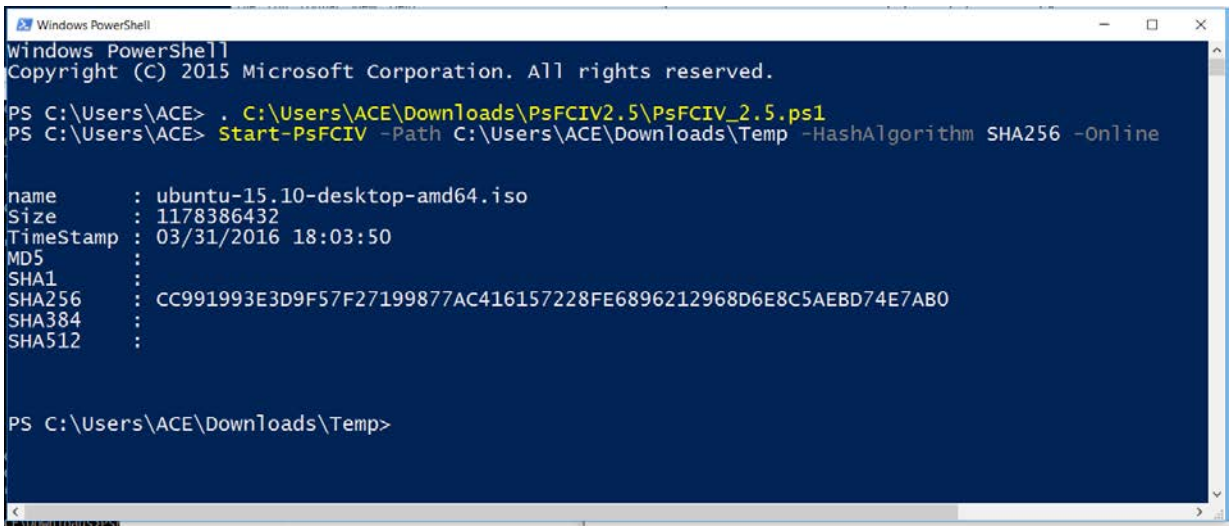
4. Download PowerShell File Checksum Integrity Verifier (PsFCIV)

- Go to https://gallery.technet.microsoft.com/PowerShell-File-Checksum-e57dcd67 and download and unzip PsFCIV.
- As its name states, PsFCIV runs in Windows PowerShell. Open PowerShell on your machine. It will look like the screenshot below:

1. 

- The PowerShell script must be dot-sourced. To do this, type "***.filepath_to_PsFCIV_2.5.ps1***" as shown below:

2. 

- PsFCIV works by calculating the hash of all items within a given folder. To limit the number of unnecessary calculations, navigate back to File Explorer and create a Temp directory with only the Ubuntu iso.
- The format for calculating the SHA-256 hash of a set of files in a directory is "**Start-PsFCIV –Path *filepath_to_your_iso* –HashAglorithm SHA256 –Online**." This will produce the following output:
- 3. 

- Compare the SHA 256 hash calculated using PsFCIV and the SHA 256 hash listed on the Ubuntu website. They should be the same.

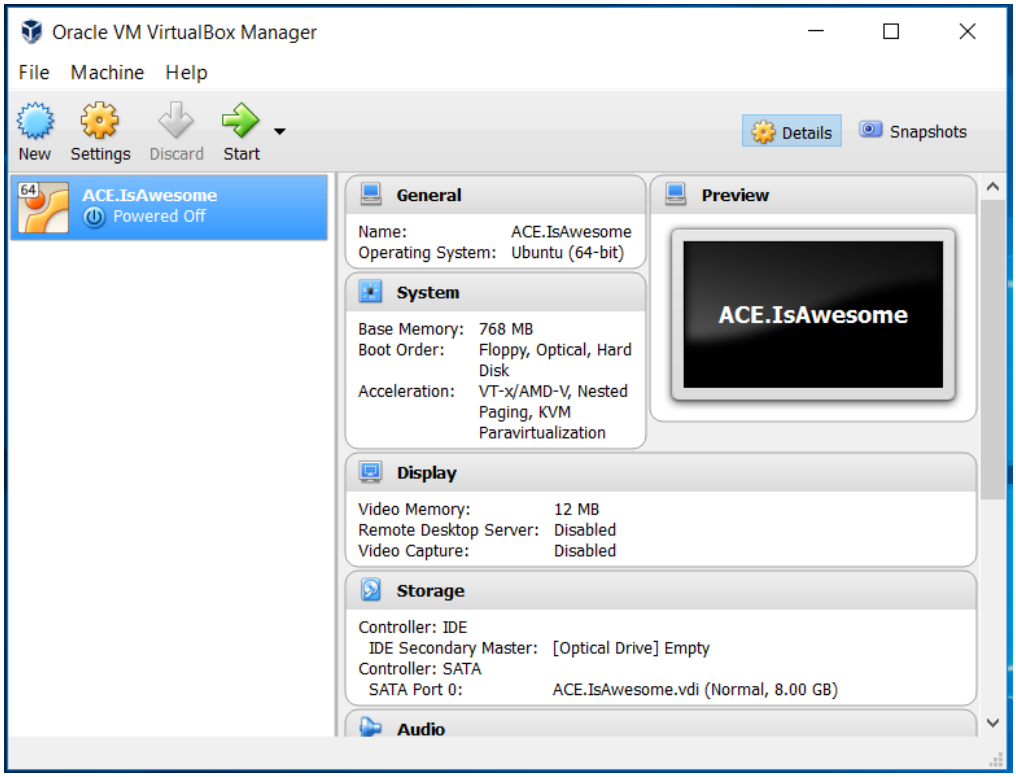
5. Run VirtualBox

5.1. Start VirtualBox

- Click on Desktop icon OR go to Start→All Programs→Oracle VM VirtualBox→Oracle VM VirtualBox.

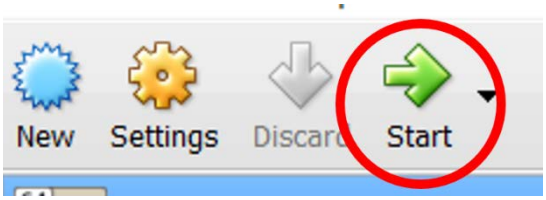
5.2. Create a Virtual Machine

- Select "New" on the welcome screen for VirtualBox.
- Name your VM <your_first_name>.<your_last_name>.
- Select "Linux" as the type and "Ubuntu" or "Ubuntu (64 bit)" as the version, depending on your device. Then click ***Next***.
- Select the recommended memory size for your VM. Then click ***Next***.
- Select "Create a virtual hard drive now," then click ***Create***.
- Select "VDI (VirtualBox Disk Image)" then click ***Next***.
- Select "Dynamically Allocated" then click ***Next***.
- Select 8.00 GB for the file size then click ***Create***. Your newly created VM should look like the screenshot below.

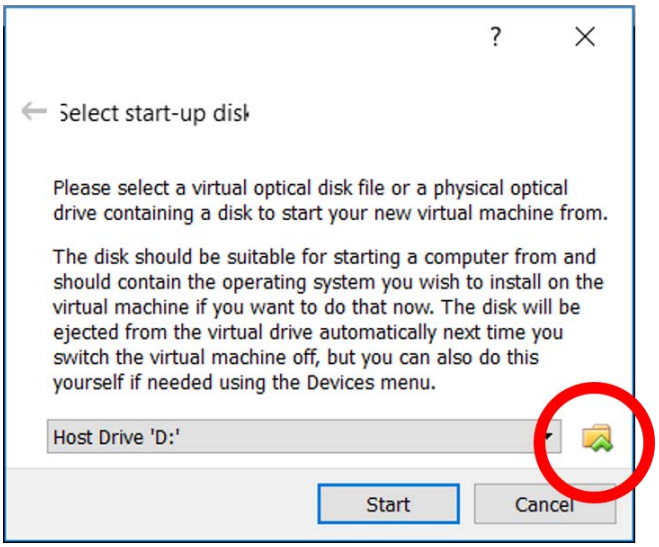


4.
5.
6.

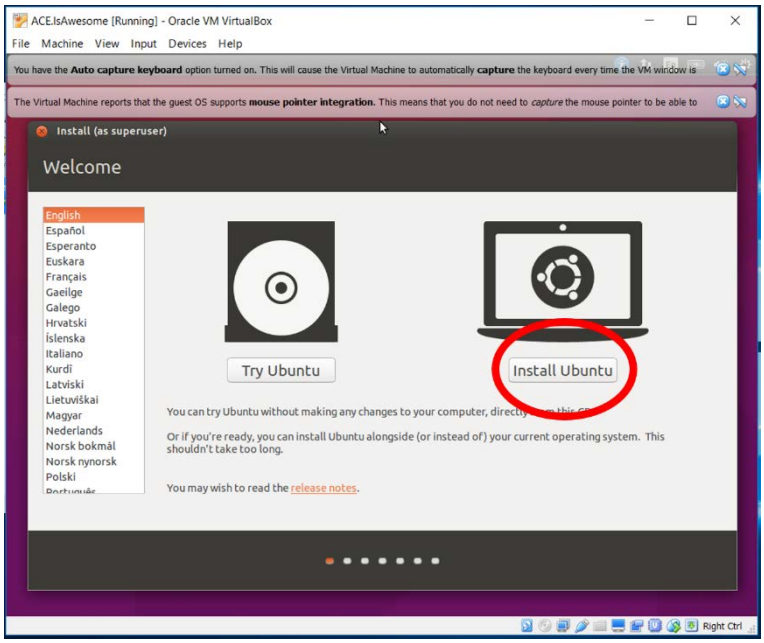
- To power on your VM, click the green start arrow in the upper left hand corner of VirtualBox window.

7. 

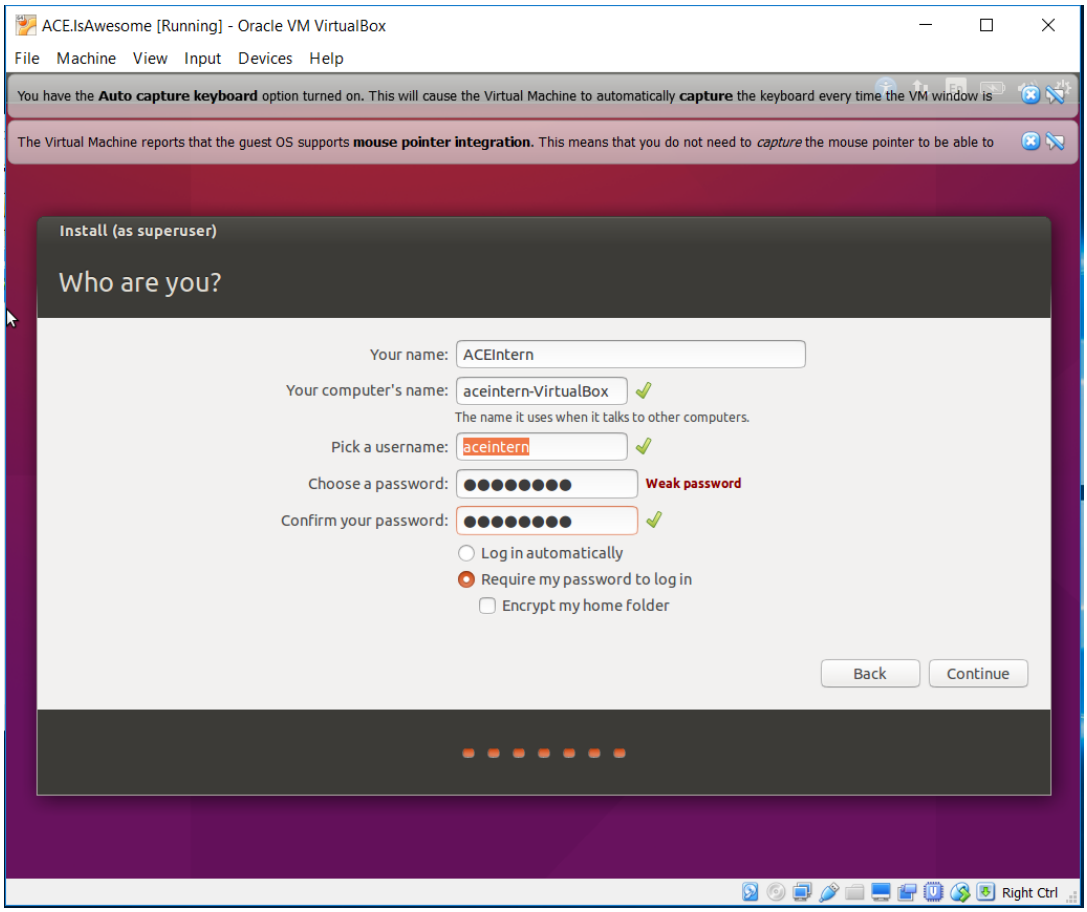
- A window titled "Select start-up disk" will appear. Click the folder to the right of the drop-down menu and browse to the Ubuntu .iso folder you downloaded earlier.

8. 

- Click ***Start***.
- Click ***Ok*** for any information boxes.
- When your VM has loaded, click ***Install Ubuntu***.

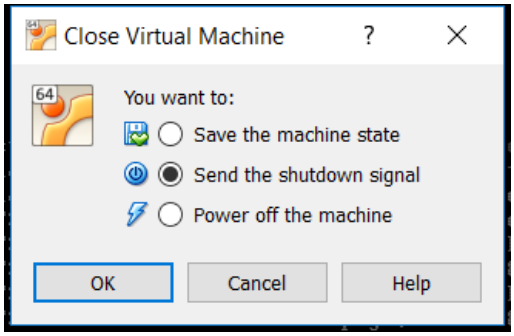
9. 

- Ensure that your computer has the necessary requirements, then click ***Continue***.
- Select "Erase disk and install Ubuntu" then click ***Continue***. This will begin the installation process.
- While Ubuntu is installing, select your location and keyboard layout.
- On the "Who are you?" window, specify your name as ACEIntern and your password as password. (Note: we recommended you change the password to something more secure if you decide to use your image for anything important or beyond the IA exercises.)

10. 

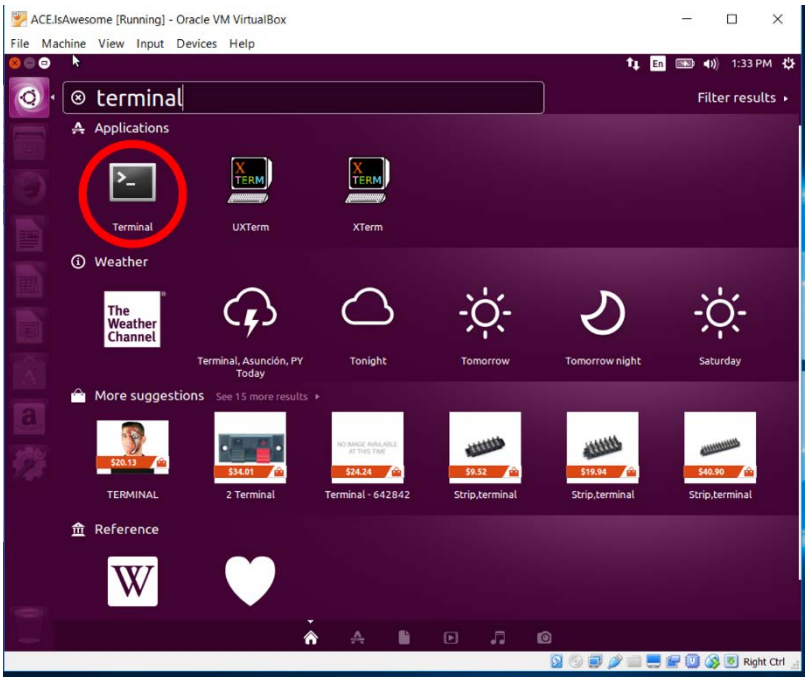
11.

- When the installation completes, click ***Restart Now***. After clicking ***Restart Now***, on the toolbar, select ***Machine***. On the drop down menu, select ***Close***. On the Close Virtual Machine window, select "Send the shutdown signal" and click ***OK***.

12. 

6. Execute a Linux Command

- Log into your newly created VM.
- Open a terminal by selecting ***Dash Home*** type ***Terminal*** in the search bar and select the terminal application.



- Type the following commands into the command prompt:
  - ***whoami***: list the user name you are currently using.
  - ***man whoami***: the man or "manual" command gives you information about topics, commands, etc.
  - ***whoami --help***: adding "- - help" is another way to get information about topics commands, etc.
  - ***apropos whoami***: apropos is yet another way to get help
  - ***perl -h***: adding a single dash followed by h is another way to get help, but it does not work with whoami.
  - ***ls***: list files in a directory.
  - ***pwd***: list the present working directory.
  - ***sudo -s***: enter your password when prompted. This gives you administrative or root access. It is required for shutting down the system.
  - ***shutdown -h now***: power off the system.
  - For more information on commands, visit https://help.ubuntu.com/community/UsingTheTerminal.