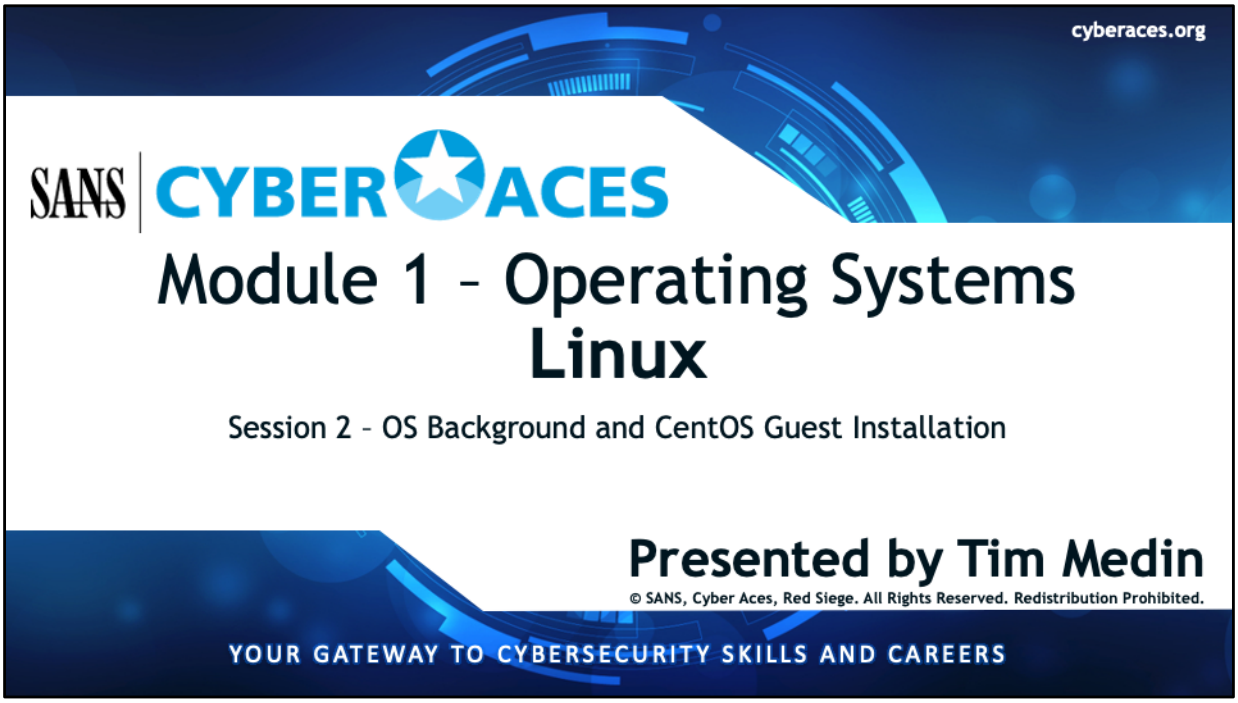
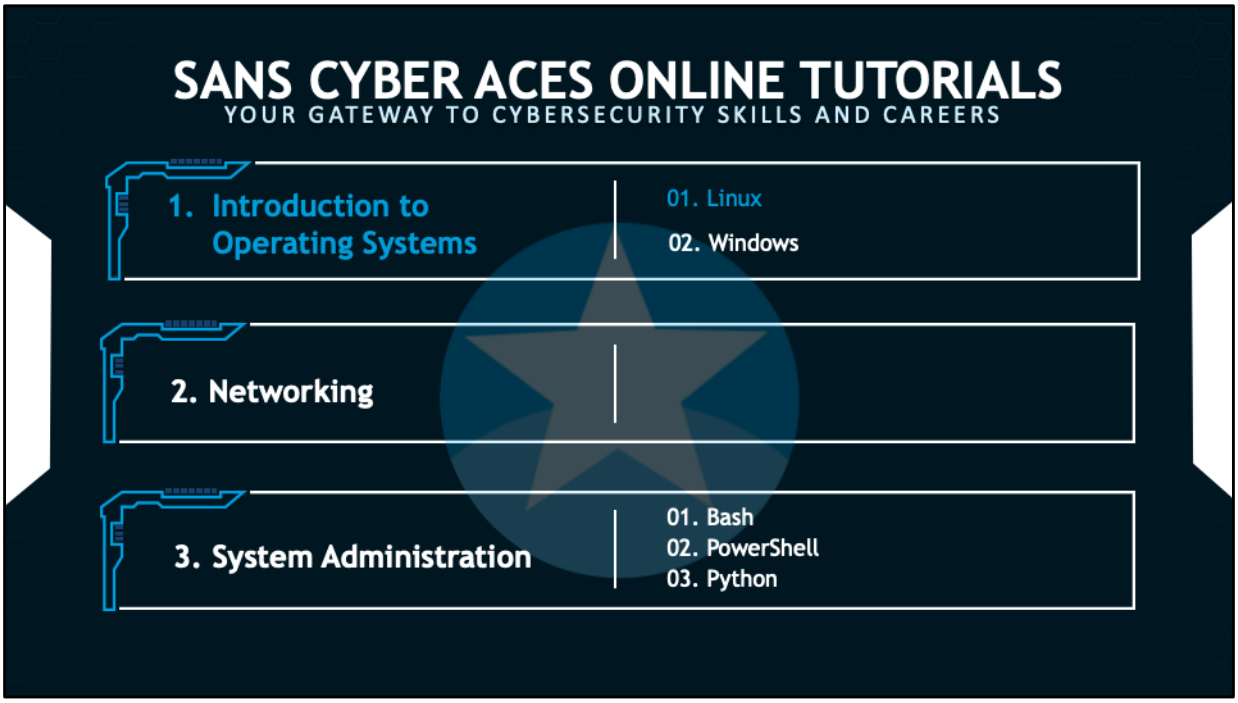


Welcome to Cyber Aces, Module 1! A firm understanding of operating systems is essential to being able to secure or attack one. This module provides a brief introduction to operating systems in general, and then we dive into installing a Linux VM.

In this session, we'll start off by covering the basics of what constitutes an operating system. Then, we'll walk through the installation of a CentOS (Linux) virtual machine in preparation for our future hands-on labs.

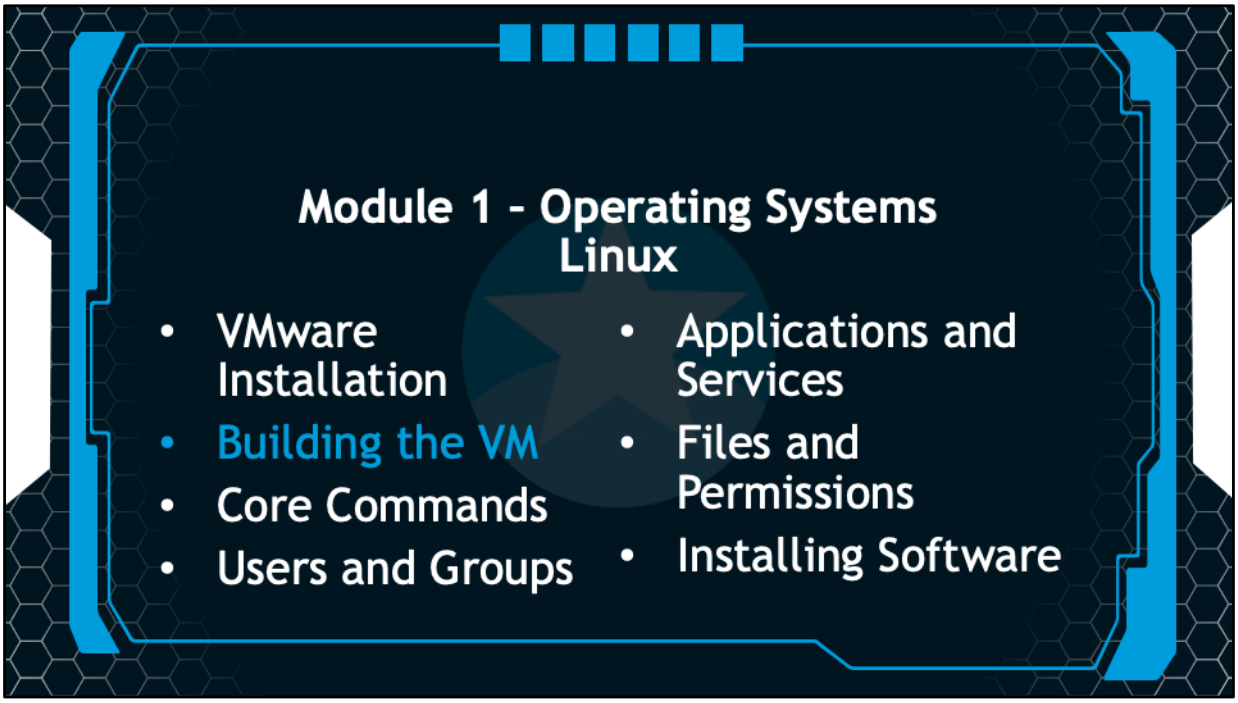
Content in this session has been developed by Tom Hessman, Tim Medin, Mark Baggett, Doug Burks, Michael Coppola, Russell Eubanks, Ed Skoudis, and Red Siege.



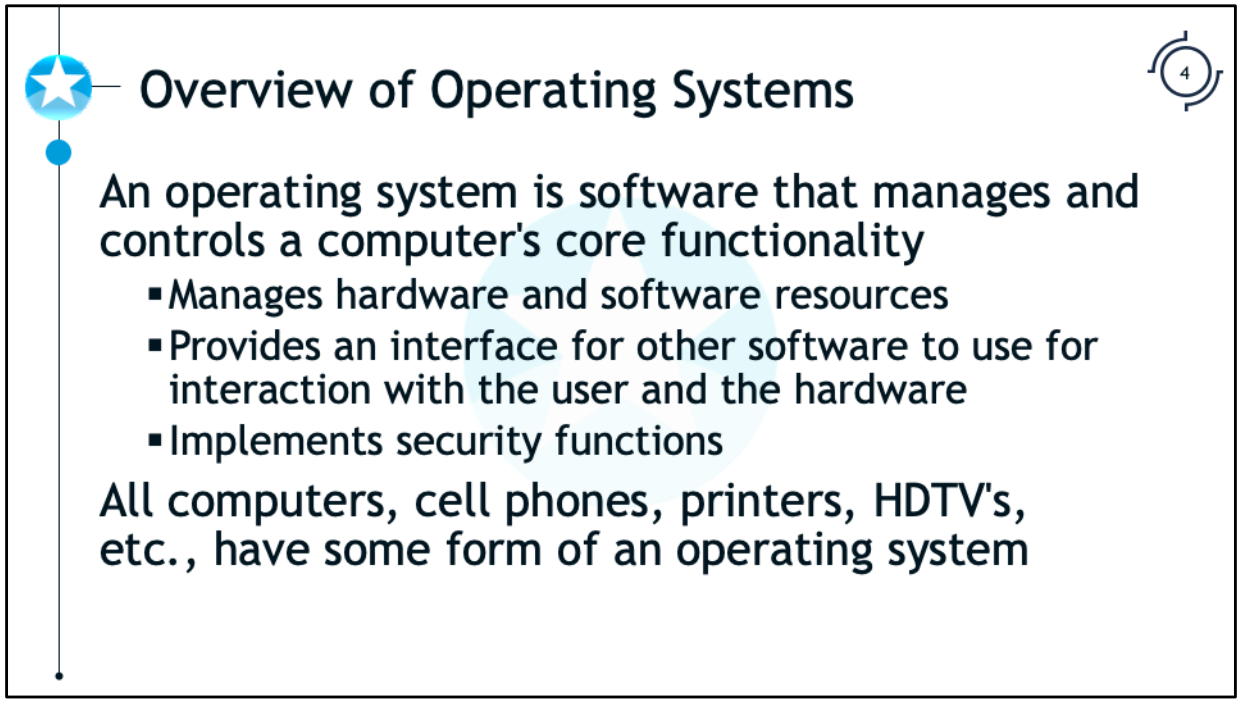
This training material was originally developed to help students, teachers, and mentors prepare for the Cyber Aces Online Competition. This module focuses on the basics of what an operating systems is as well as the two predominant OS's, Windows and Linux. This session is part of Module 1, Introduction to Operating Systems. This module is split into two sections, Linux and Windows. In this session, we will continue our examination of Linux.

The three modules of Cyber Aces Online are Operating Systems, Networking, and System Administration.

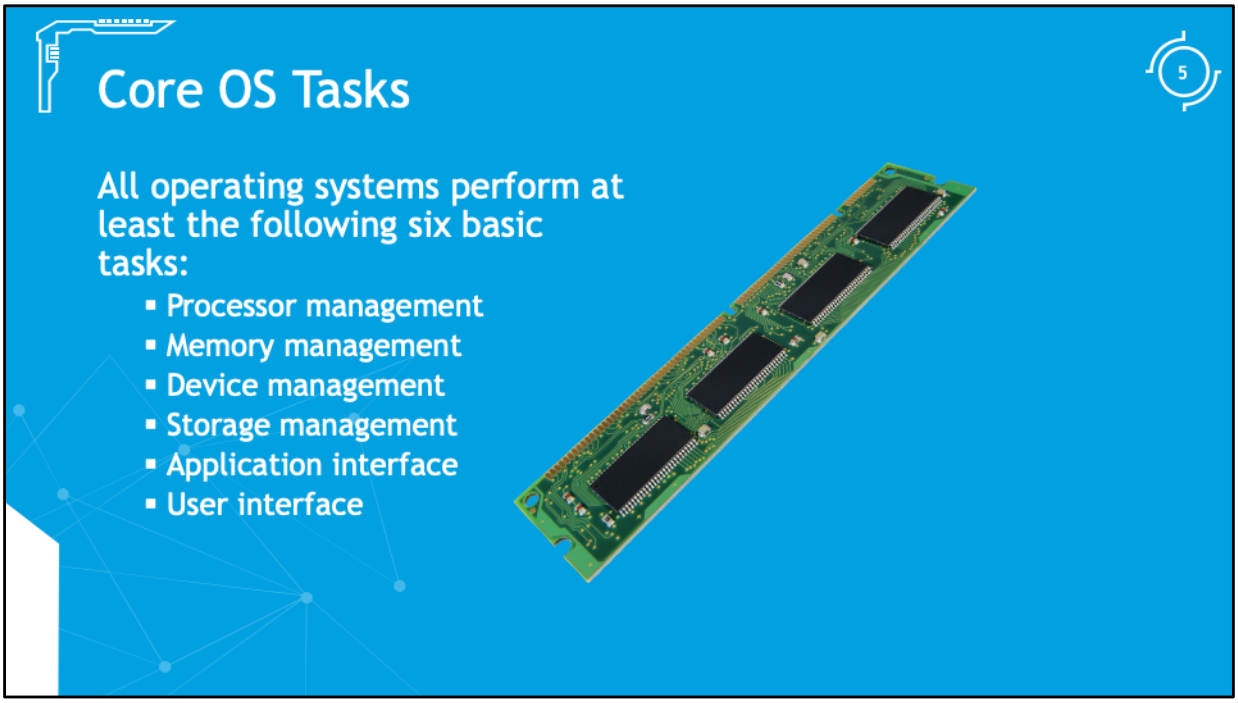
For more information about the Cyber Aces program, please visit the Cyber Aces website at https://CyberAces.org/.



In this session we are going to build a CentOS (Linux) virtual machine.



An operating system (or "OS") is a foundational piece of software that provides an interface to the hardware of a computer or device. Programs are written by application developers to utilize this interface, which are in turn utilized by human users and other programs to perform tasks and effectively manage the resources of the computer. Operating systems typically manage the interaction of the user and other software applications with the computer's hardware, provide the ability to load and execute other programs, and implement important security functions. All computers, cell phones, printers, cable modems, HDTV's, and your laptop PC have some form of an operating system.



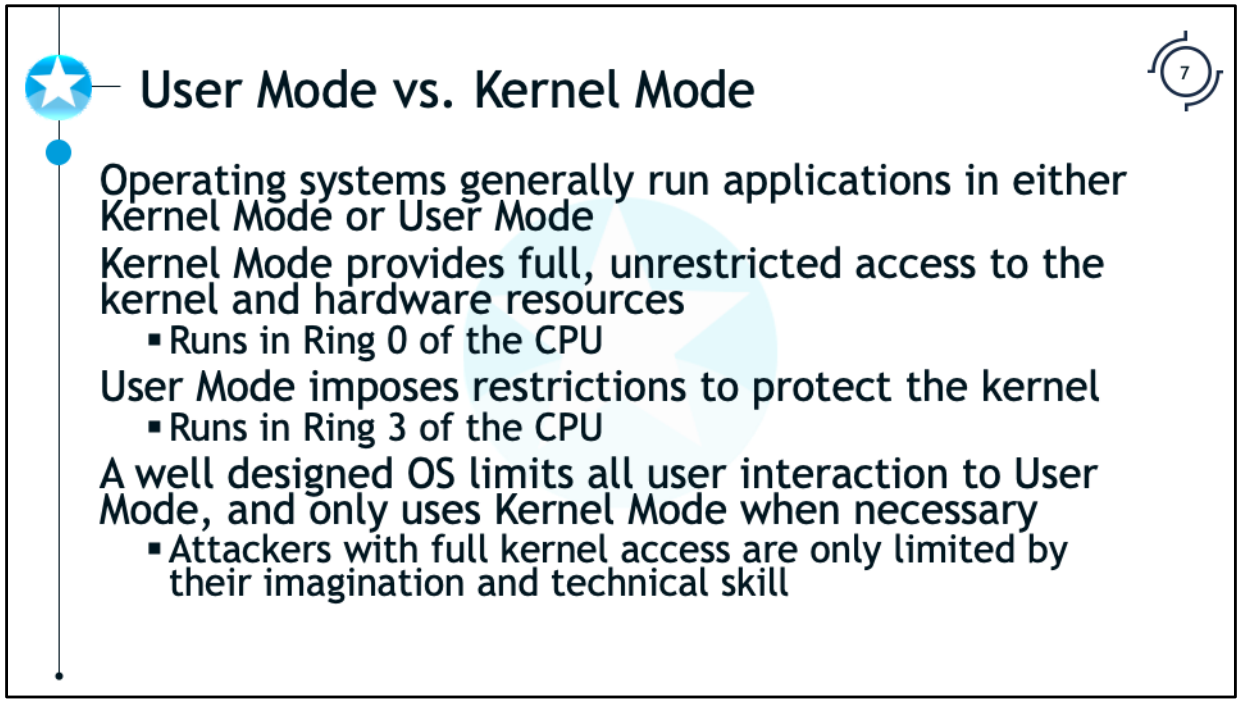
While modern operating systems have many different functions, all operating systems, no matter the device, perform at least the following six basic tasks:

Processor management: A single core CPU can only run one process at a time (adding more cores or CPU's allows for true multitasking). The operating system manages CPU scheduling so that each process (of the same priority) gets equal CPU time, switching between them so rapidly that it gives the appearance of multiple tasks running simultaneously. The OS also watches for Interrupts, which tell the CPU/OS that something else needs attention.

Memory management: Computers store programs and data that is actively being used in physical RAM (Random Access Memory). The OS manages the physical RAM, structuring it to control how much each process gets, and ensuring that they don't overlap or otherwise conflict with one another. The OS also controls swapping inactive data out of physical RAM into virtual memory, which temporarily stores the contents of inactive RAM on the hard disk to make room for other data.

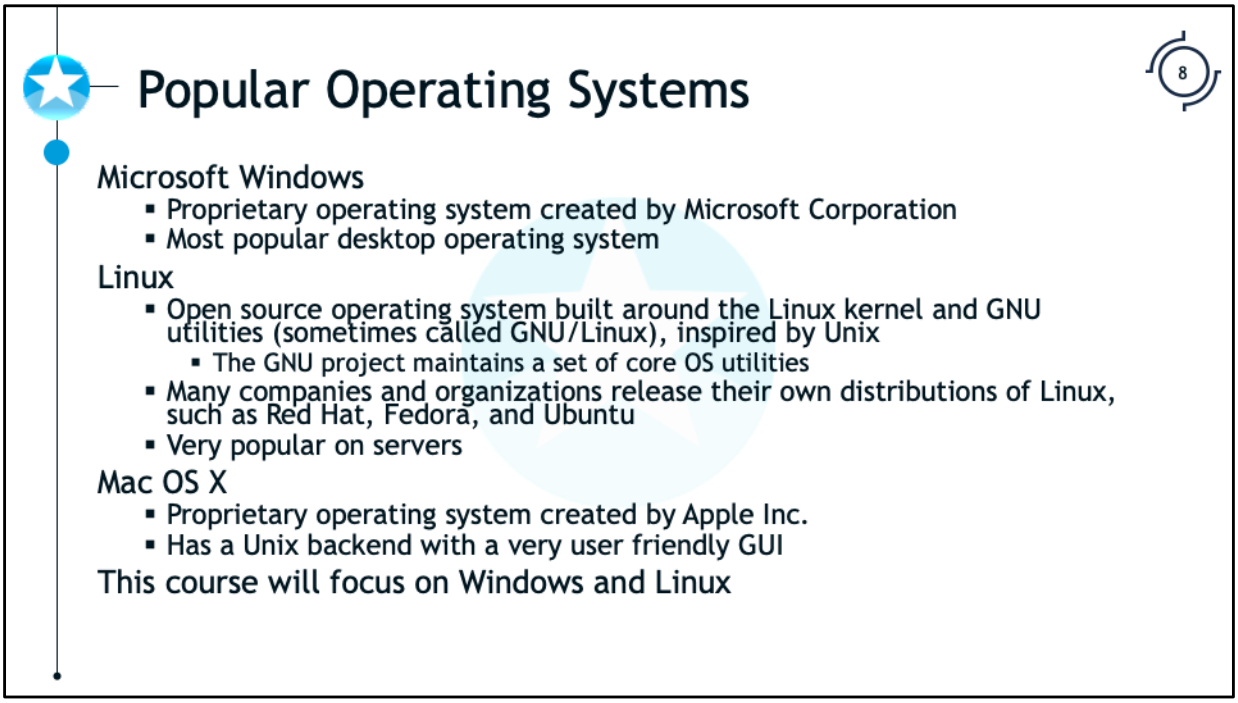
Device management: The OS manages all interaction with hardware devices, both those inside the computer and external devices connected through means such as USB.

Storage management: The OS uses a filesystem to structure files on the computer's permanent storage device, such as a hard disk drive. The filesystem is responsible for keeping track of the physical representation of files on the disk, and can also apply access control. Modern versions of Windows use NTFS as their primary filesystem, while older versions of Windows and most portable storage devices use FAT (File Allocation Table). Linux supports many filesystems, but typically uses EXT2, EXT3, or EXT4. Mac OS X typically uses HFS+, also called "Mac OS Extended".

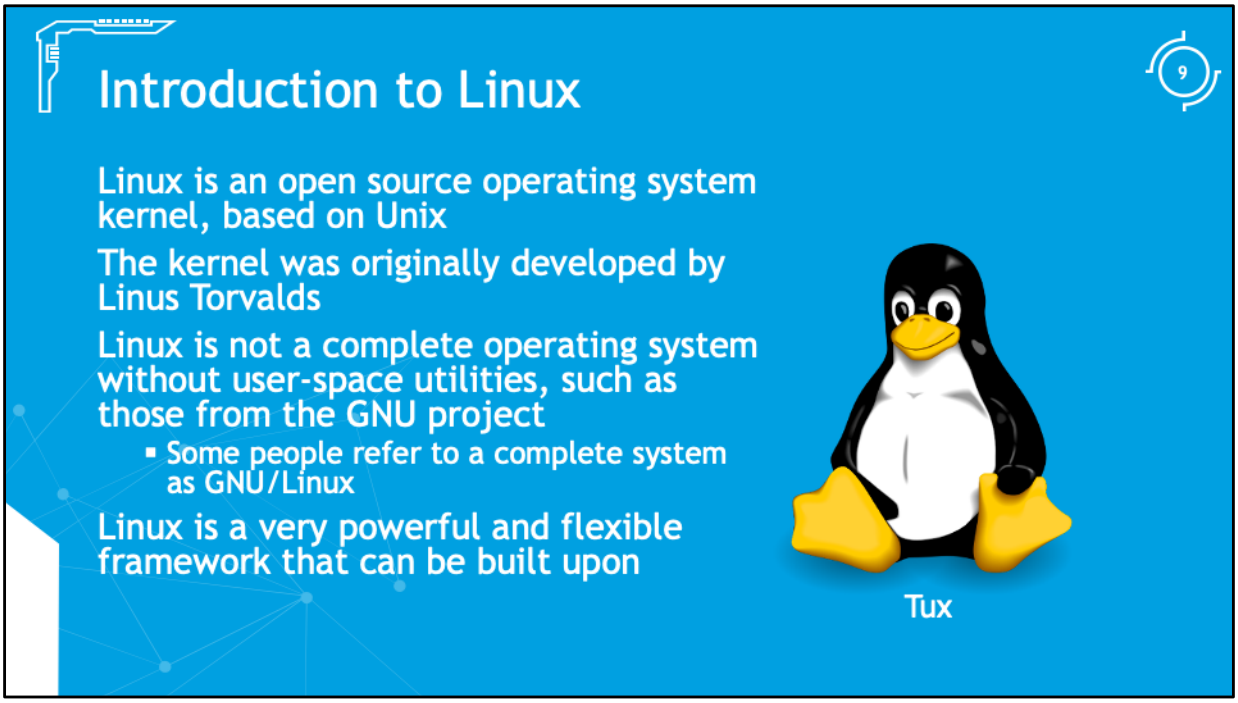


When security is taken into consideration during the Operating Systems design, operating systems typically have applications that run in one of two modes: Kernel Mode or User Mode. In Kernel Mode, applications have full unrestricted access to all computing resources. In User Mode, applications are limited by CPU enforced restrictions. The typical operating system will limit all user interaction to User Mode and will only use Kernel Mode functionality for interacting with hardware and managing other processes.

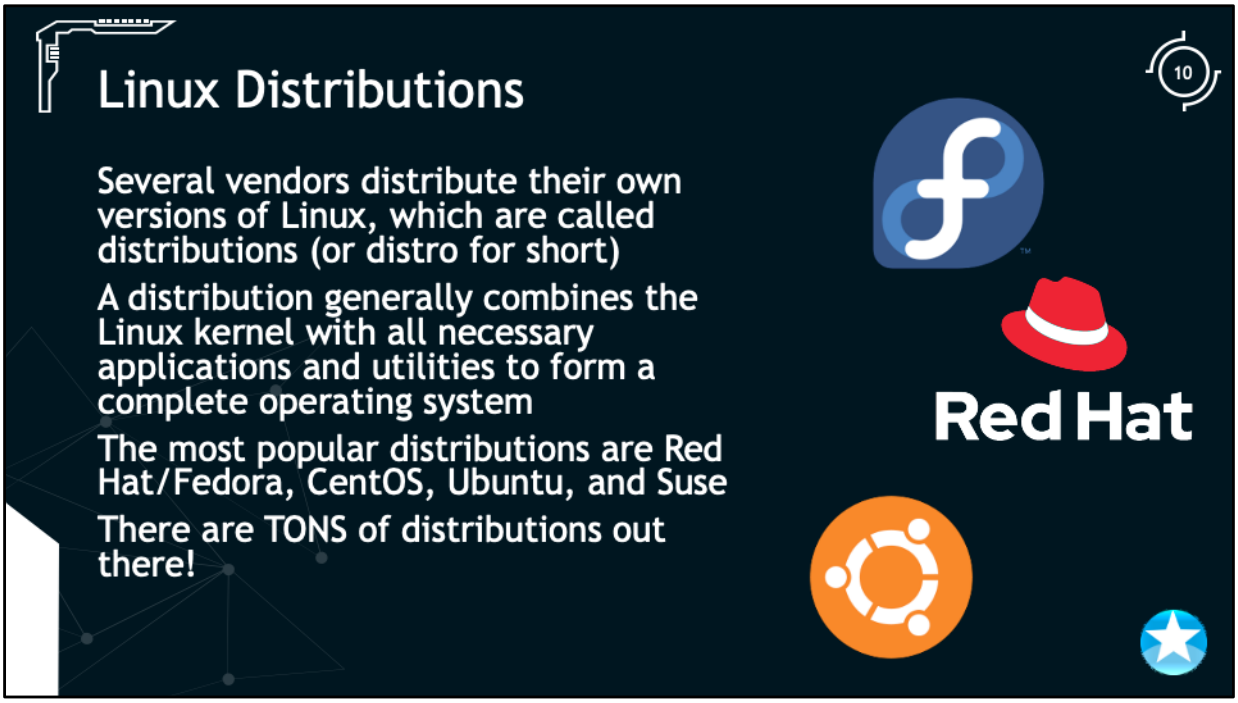
An attacker who has gained access to an operating system's kernel is only limited by his imagination and technical skill. Good security professionals know that you protect the kernel or the game is over. Many operating systems will have different types of user accounts: "administrative users" and "limited users". Administrators have the ability to modify the kernel, and limited users typically do not.



In the personal computing world, three main families of operating systems dominate the market. They are Microsoft Windows, Apple Mac OS X, and GNU/Linux. Both Mac OS X and GNU/Linux, along with many other variants, were inspired by an operating system known as UNIX. In this training we will work with Linux and the Windows Operating Systems. First, let's look at Linux.

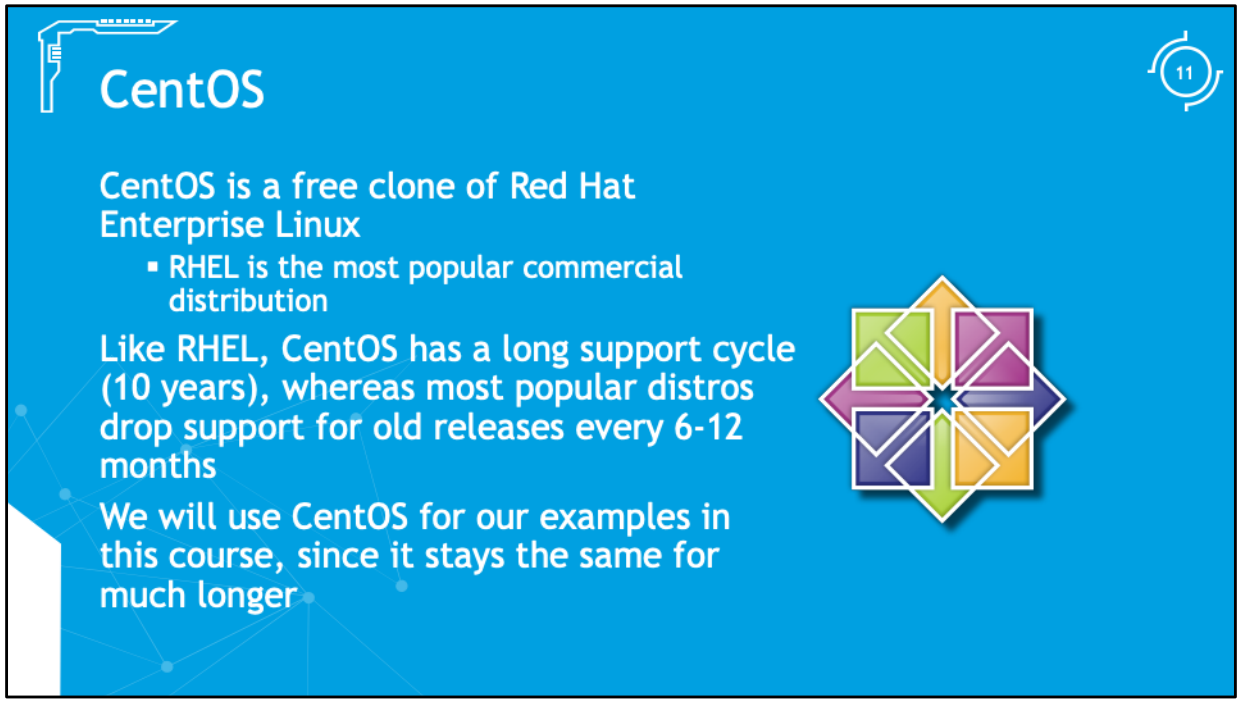


Linux is an open-source operating system kernel based on UNIX (it is a clone that adheres to the Unix specifications, but does not use any original Unix code). It was originally developed by Linus Torvalds. Linux itself is just a kernel, and is not a complete operating system without user-space utilities, such as those from the GNU project. For this reason, some people refer to a complete Linux system as GNU/Linux. However, Linux can also be used with other user-space utilities, such as BusyBox. Linux is a very powerful and flexible framework on which you can build many different operating systems. Many of the web pages and databases you communicate with every day on the Internet are running one of these Linux distributions.



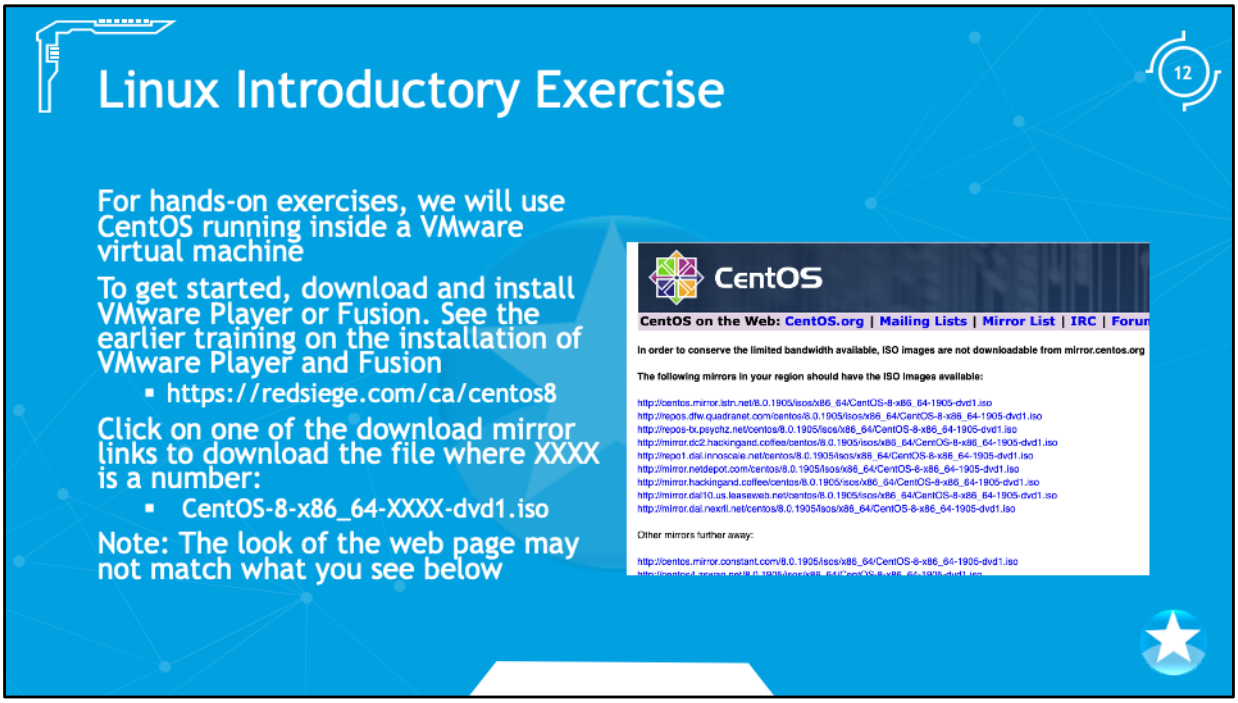
Several vendors distribute the Linux kernel along with all of the necessary applications and services to form a complete operating system. The most popular distributions of Linux are Red Hat/Fedora, CentOS (based on Red Hat), Ubuntu, and Suse. There are TONS of distributions, both commercially supported and community driven.

A list of many of the distributions (distro for short) available is available at distrowatch.org. To see a list of the major distributions click on the "Major Distributions" link at the top of the distrowatch.org website.



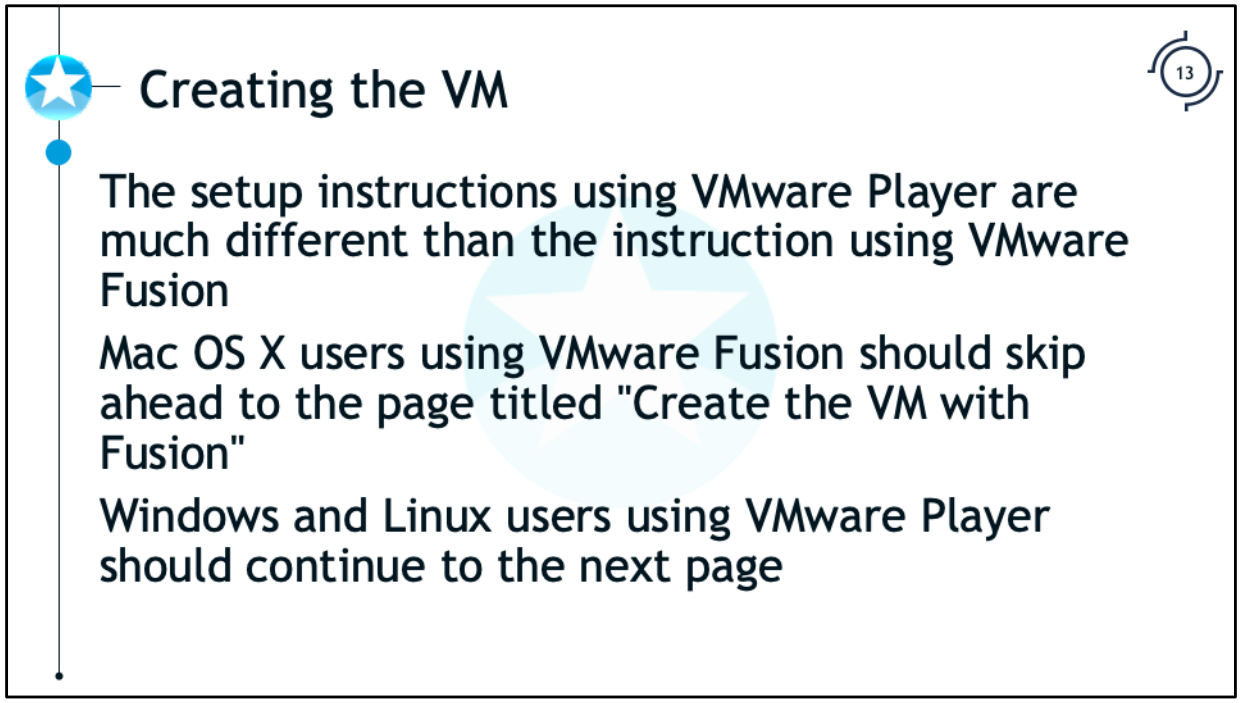
In this course, we are focusing on CentOS Linux. There are several reasons we chose to use CentOS for these demonstrations. Among those reasons are:

- Most organizations in the United States that are running Linux are running Red Hat Enterprise Linux (RHEL), but it is a commercial product. CentOS is a free clone of RHEL. Familiarizing yourself with CentOS is an inexpensive way to build a valuable skill set you can use in the commercial work space.
- CentOS, being based on RHEL, has a long support cycle so the tools and commands don't change as often as they do in community Linux distributions (such as Fedora and Ubuntu) that have brand new releases every 6-12 months (and that subsequently drop support for older releases every 6-12 months). So this courseware and the skills you learn here will have a longer lifespan.
- CentOS supplies extensive documentation (based on the original RHEL documentation): https://docs.centos.org/en-US/centos/install-guide/



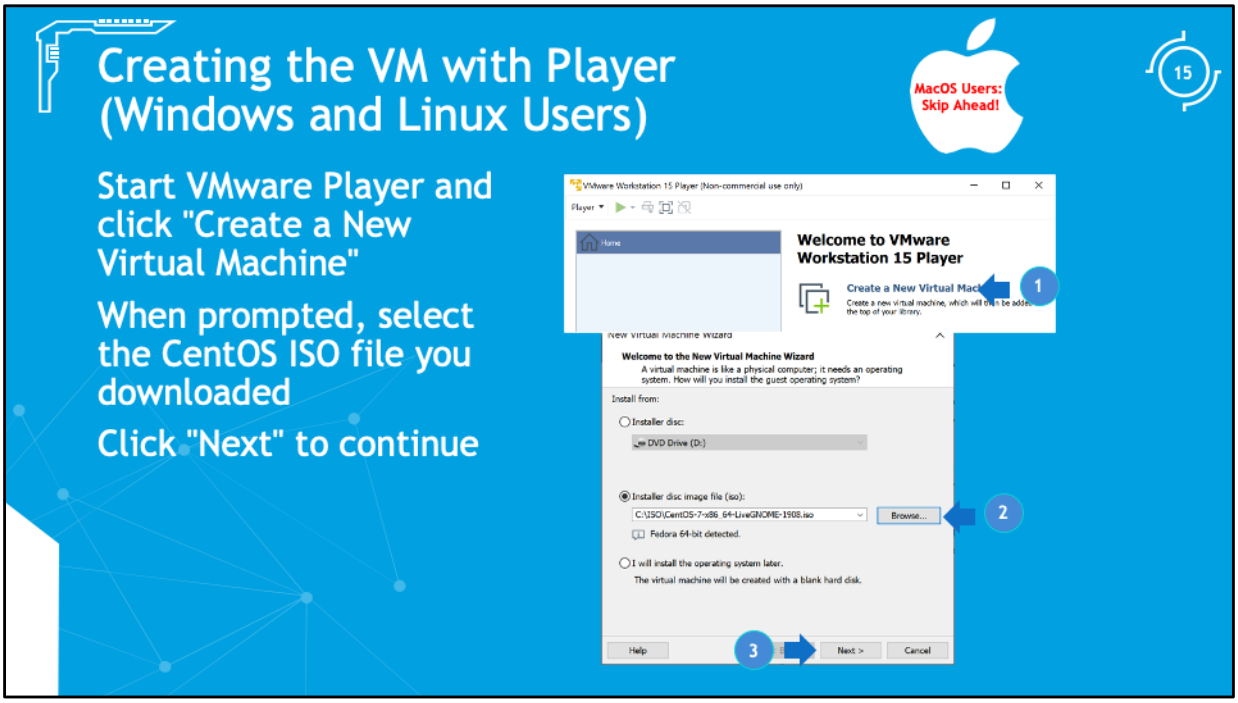
For hands-on Linux exercises, we will use CentOS running inside a VMware virtual machine. This allows for easy experimentation without modifying your host system.

Dowlnoad the CentOS 8 Live DVD using one of the download mirrors listed here: https://redsiege.com/ca/centos8.



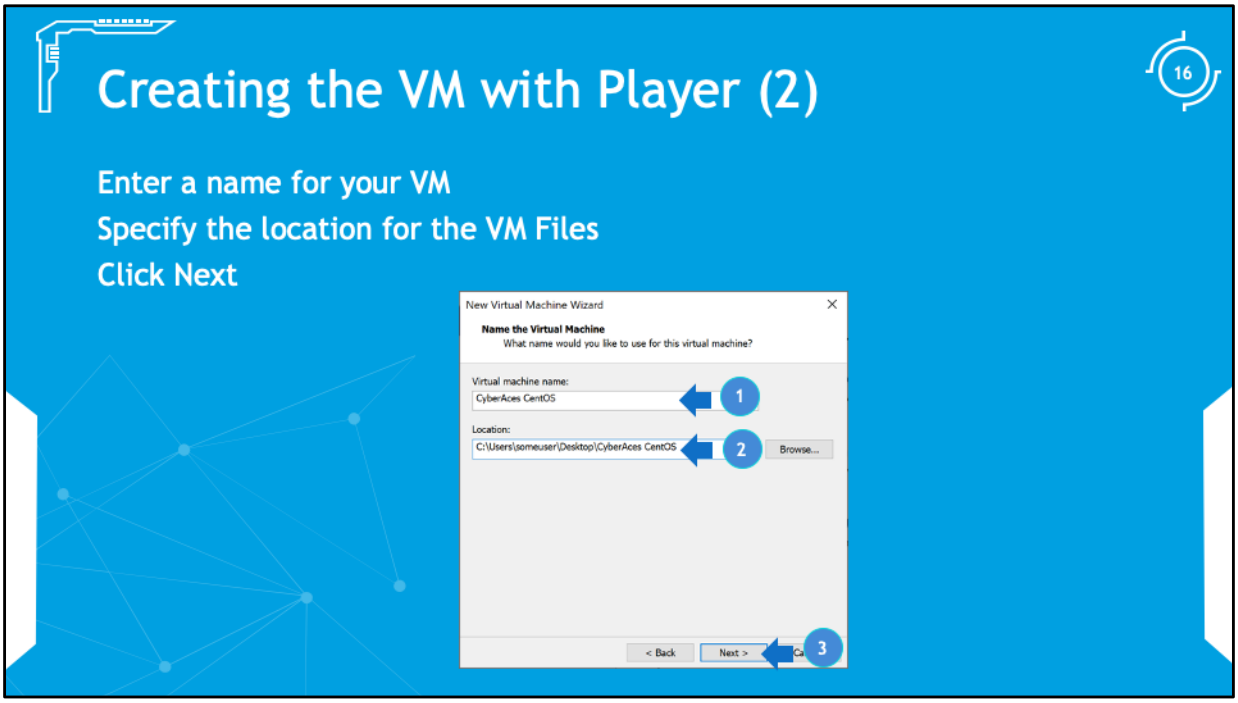
The instructions for creating a VM in VMware Player are significantly different from the instructions for creating a VM in VMware Fusion. If you are using VMware Fusion (all Apple/Mac users) then you should skip ahead to the page titled "Create the VM with Fusion". If you are using VMware Player in Windows or Linux, continue to the next page.

The following steps are for installation on Windows. MacOS users, please skip ahead to the MacOS installation instructions.

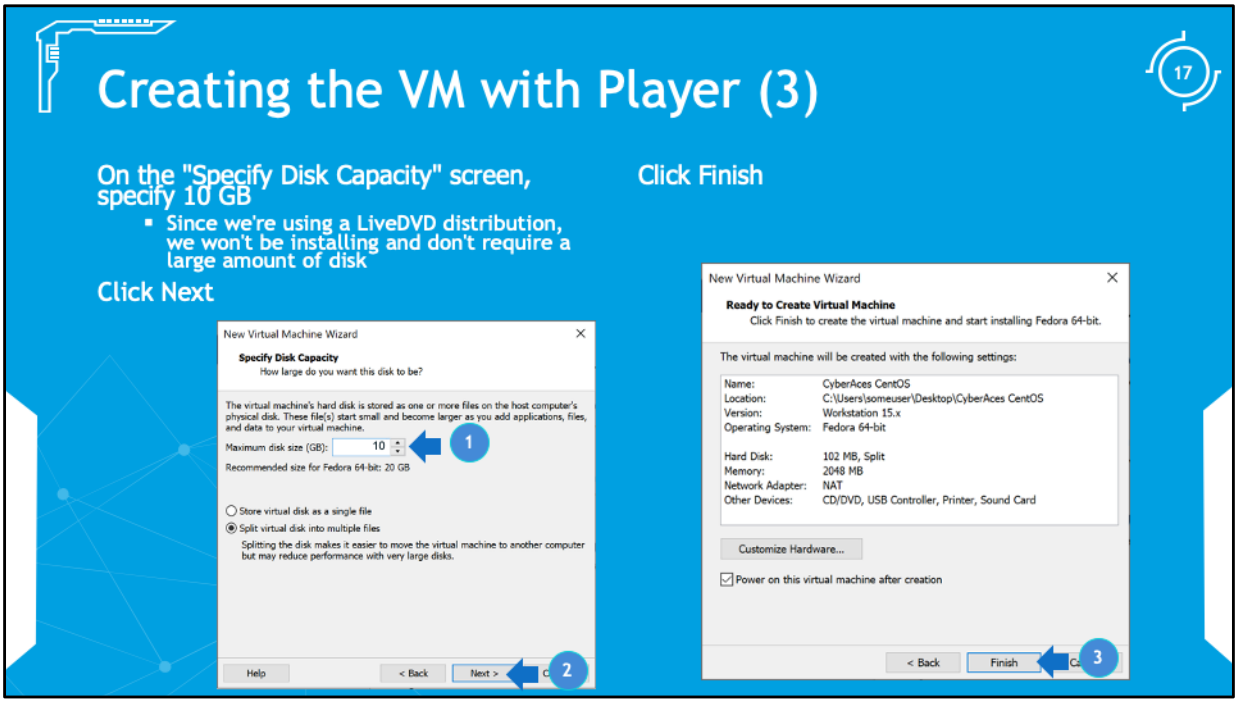


To begin the creation of our VM you will first need to start VMware Player. After the application is started, click on the "Create a New Virtual Machine" icon or text on the right. This will allow us to configure the options for our new CentOS VM.

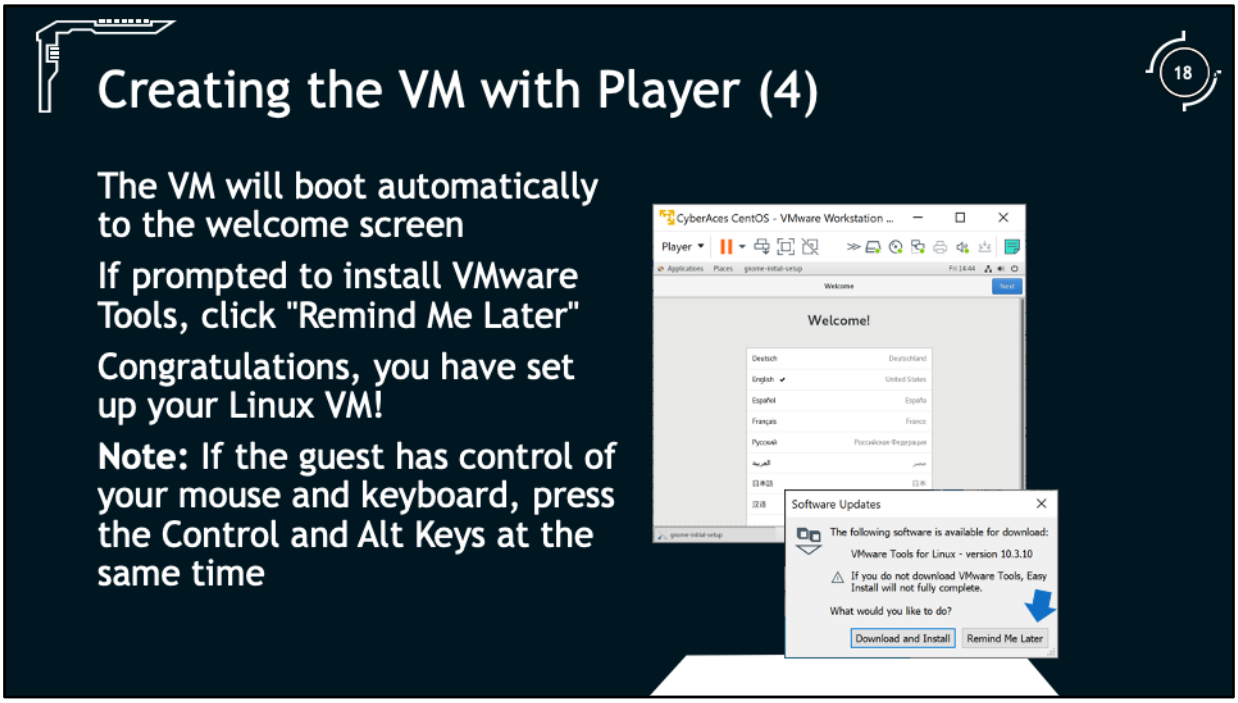
Click the "Browse" button and select the CentOS ISO file that you just downloaded. Then, click "Next" to continue.



You are now prompted to name the VM and specify a location where the VM will be saved. Name the Virtual Machine "Cyber Aces CentOS" and choose a location that you will remember and can easily access. Click "Next" to continue to the next step.



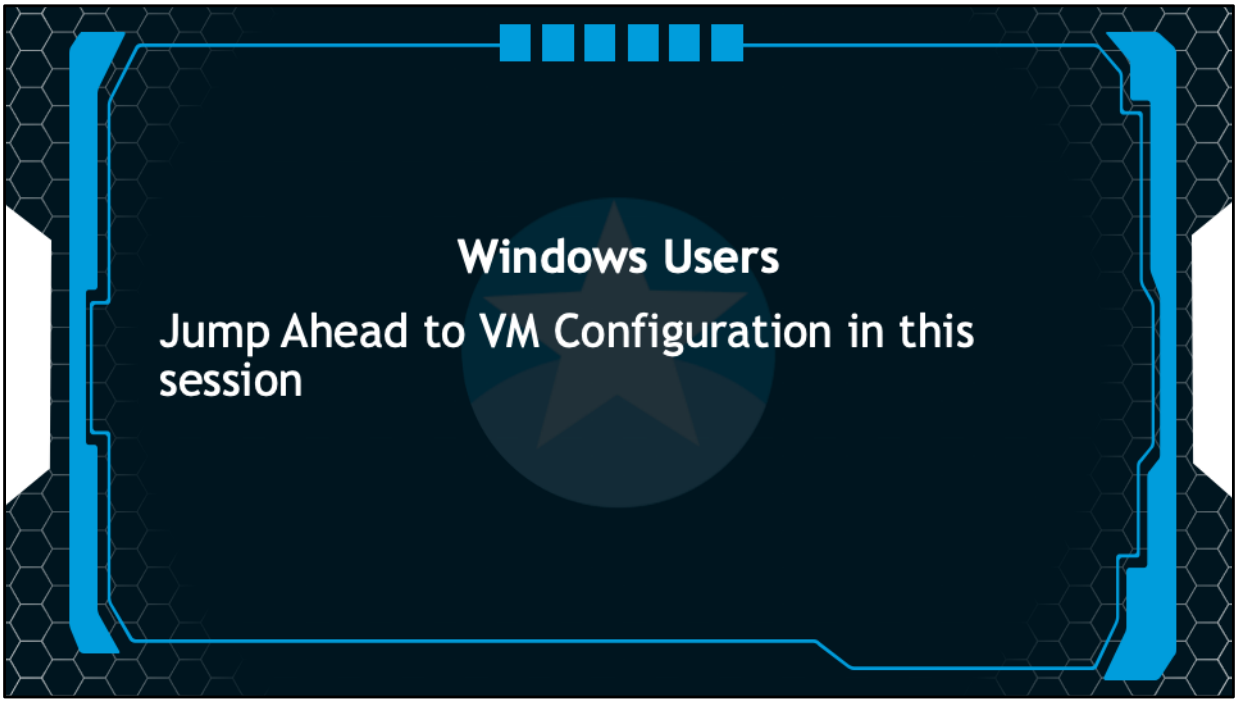
The Specify Disk Capacity screen allows us to configure the size and storage options for the virtual hard drive on which our newly installed operating system will reside. We will be installing the CentOS in Virtual Machine. We need at least 10GB of hard drive space to complete the install. Enter 10GB and select "Next" to continue to the next screen. Click "Next", review the settings, and click "Finish" to finalize the creation of the VM.



Click the green "Play virtual machine" button to boot the VM. You should then see the Linux system begin its boot process. If you are prompted to install VMware Tools, you can skip the installation by selecting "Remind Me Later". The VMware Tools offer better performance of the VM as well as additional features such as drag and drop between the host and guest. However, as this is a LiveCD, the changes in the operating system will be lost after reboot so there is no benefit to installing the tools.

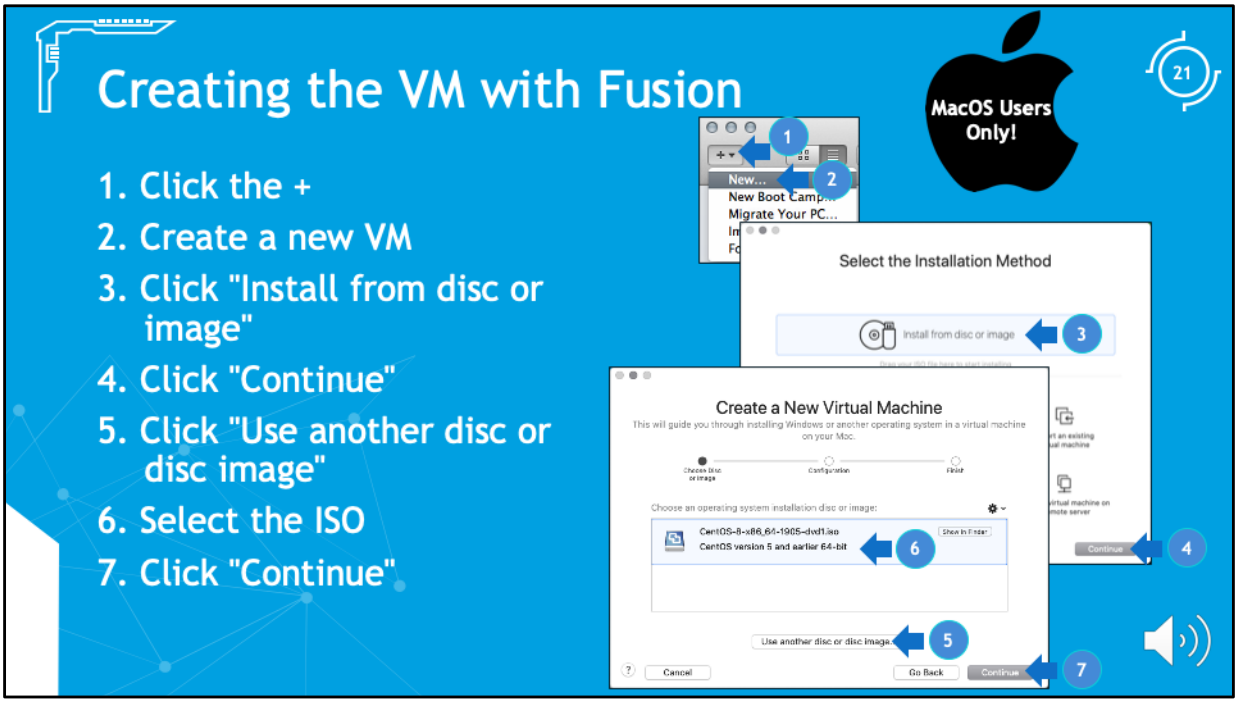
Note: when typing or using your mouse in your VM, your keyboard and mouse might get stuck in the VM. To release control of the keyboard and mouse to your host, press the Control and Alt keys at the same time.

At this point you have completed the exercise and you should have a working Linux VM! The remainder of this session includes instruction on creating the Linux VM within VMware Fusion. Unless you are using a Mac, you can skip the remainder of this session.



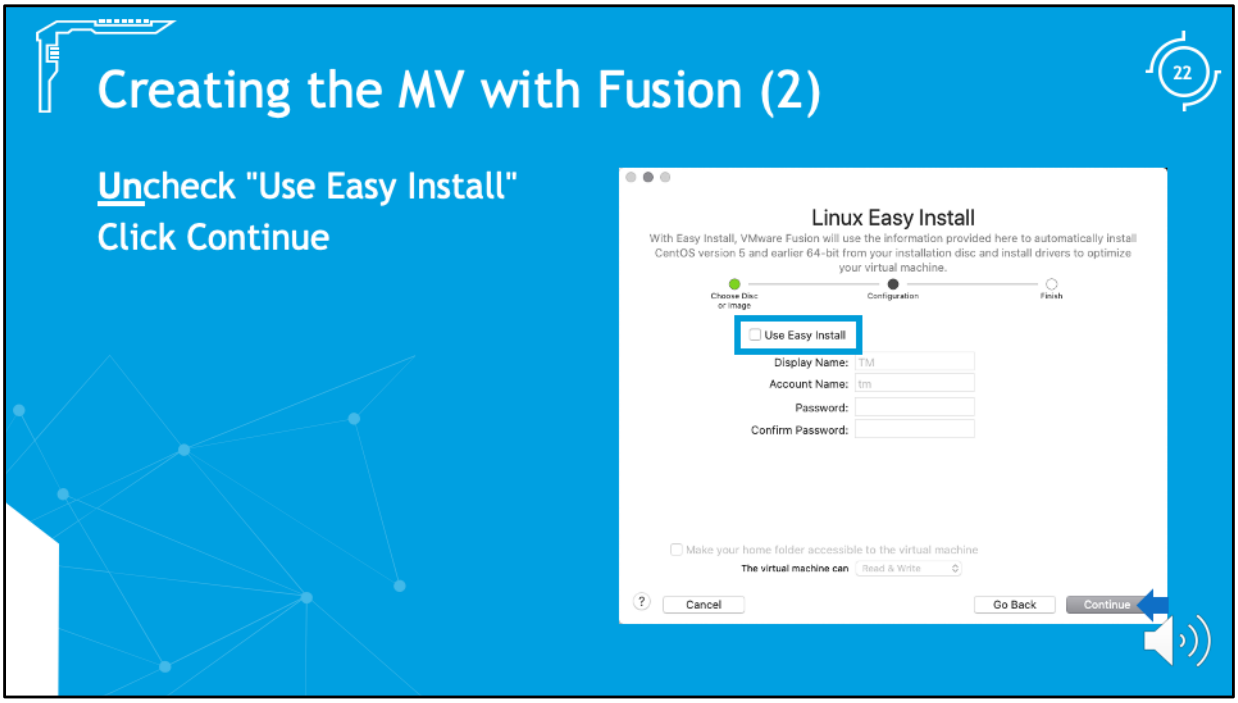
Jump ahead to the "VM Configuration" section in this session.

The following steps are for installation on MacOS.

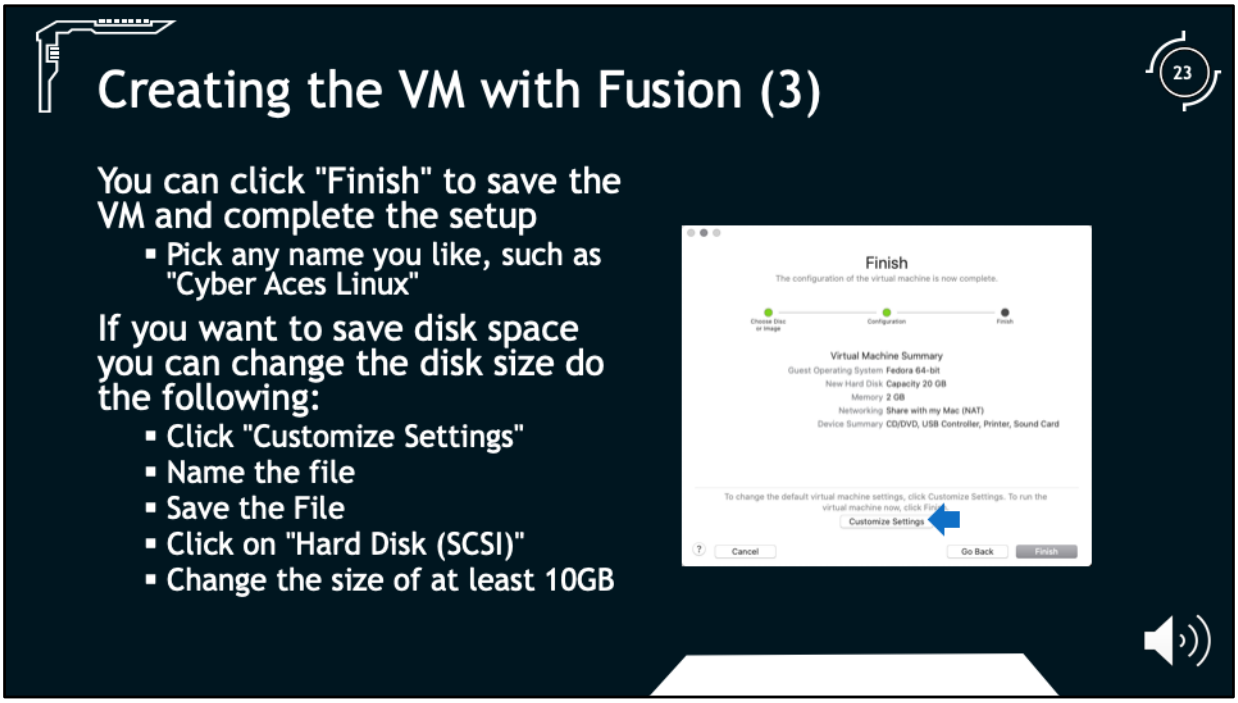


If you are using VMware Fusion on OS X, you should now have Fusion installed and opened. To create a new virtual machine, click on the plus (+) in the top left corner of the window and select "New…".

Next, click on the picture of a DVD and then click "Continue". On the next screen, click on "Use another disc or disc image.." and then find the .iso file you downloaded earlier, select it, and click "Open". You should see the .iso file in the center of the window. Click "Continue".

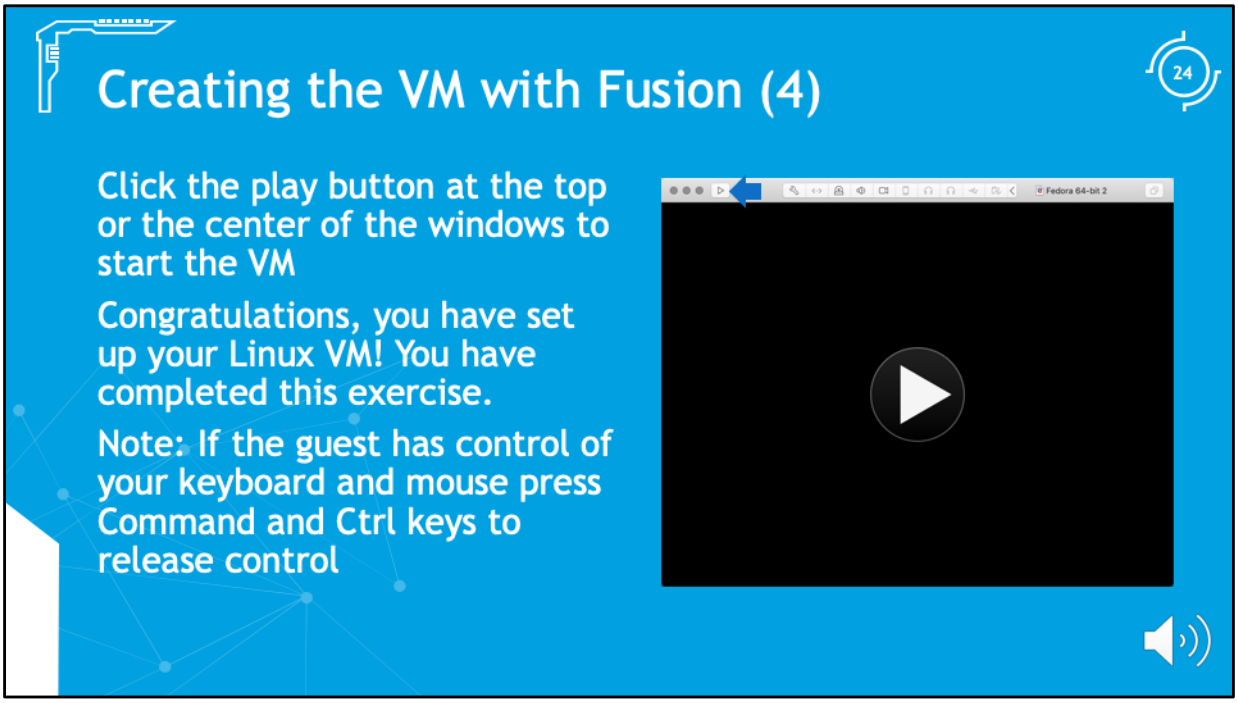


We will manually install the operating system, so uncheck "Use Easy Install" then click "Continue".



At this point the setup is essentially complete. If you have plenty of drive space, then click "Finish" and turn the the next page. If you want to reduce the disk size then follow the directions below.

To make the VM disk smaller, click on "Customize Settings". You will be prompted to name the file. Click on "Hard Disk (SCSI)" then change the size to a size no smaller than 10GB. Close the window.

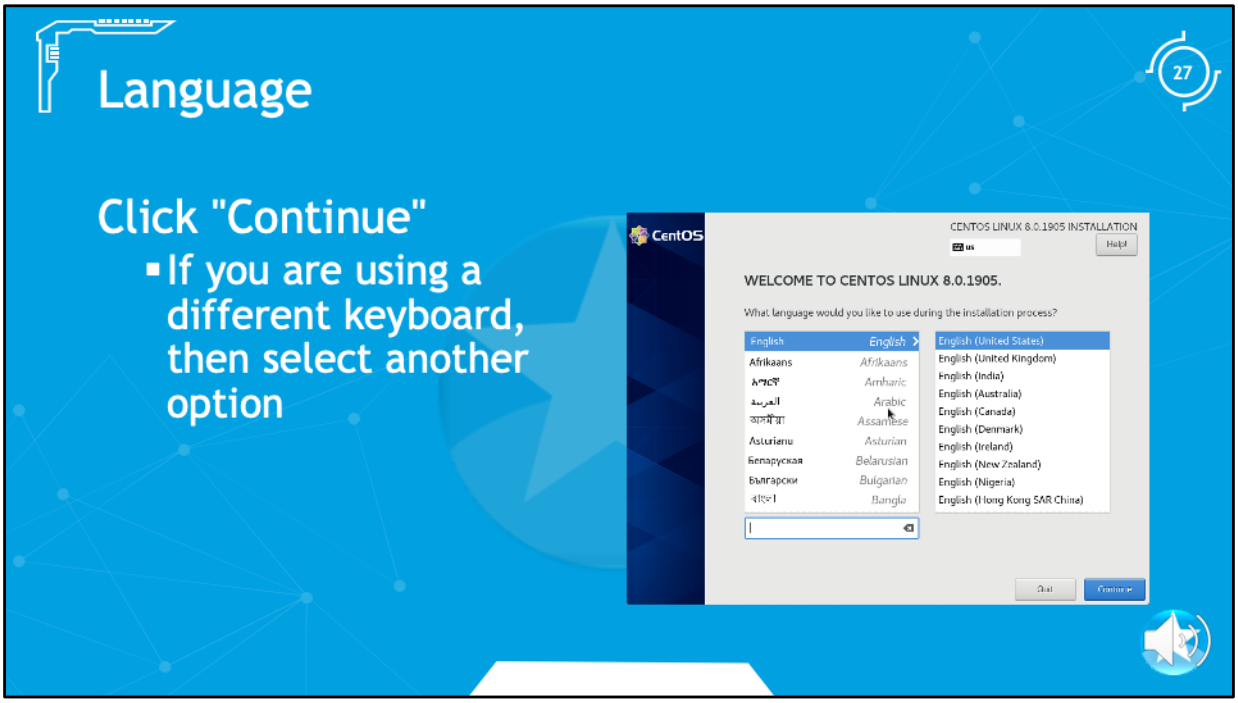


Your virtual machine is now configured with the expected operating system and virtual hardware and is ready to use. To start the VM click on the play button labeled "Start Up". You should see the VM begin it's boot process. You have completed the creation of the VM. Congratulations, you have completed the exercise!

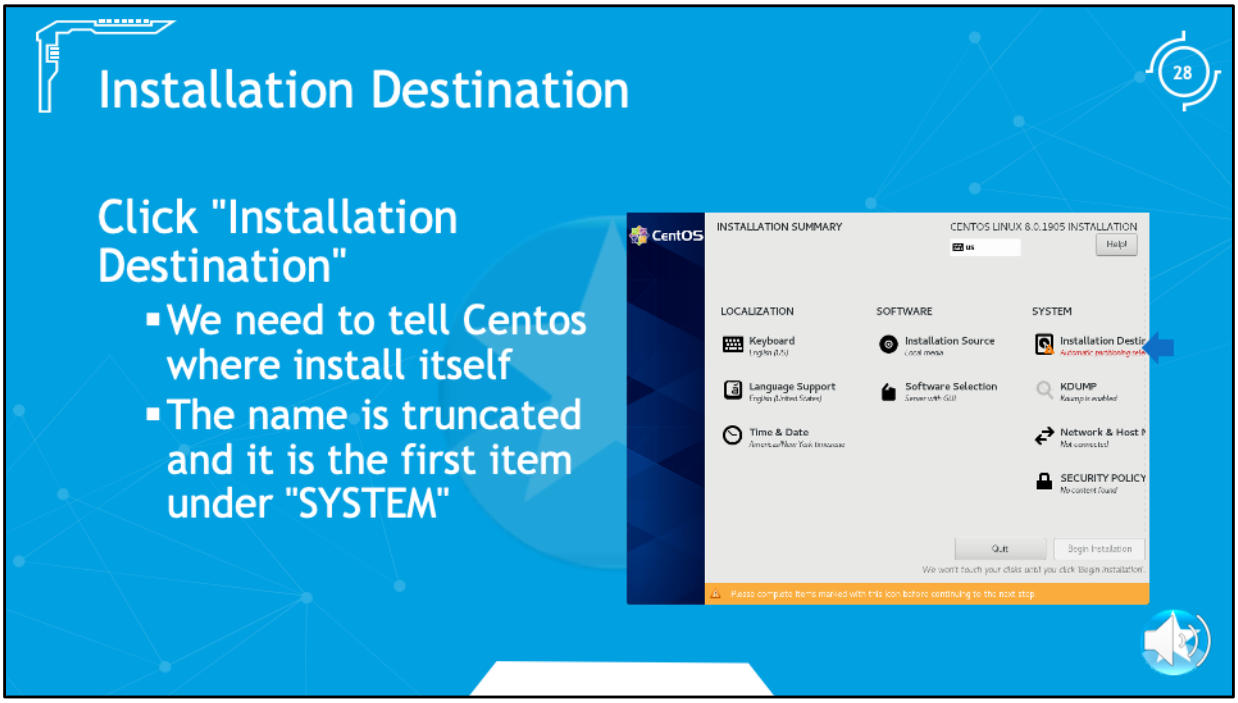
Note: If your guest has control of your keyboard and mouse press Command and Ctrl to release control.

The following portion of this presentation should be completed by both Windows and MacOS users.

Use your arrow keys to select the first option, then press Enter to begin installation. It will then take a few moments for the VM to boot to the installation screen.



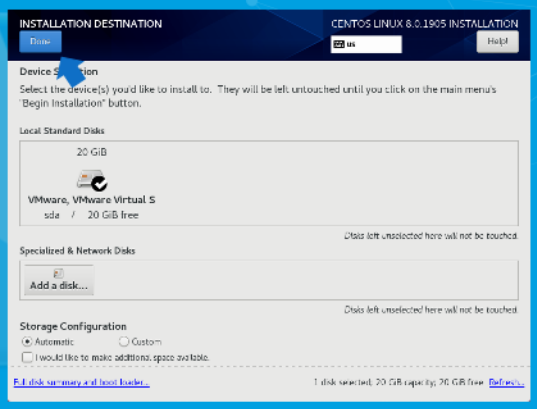
Select your language and then press "Continue". If you are in the US then you can simply click Continue. If you are are using a non-American keyboard then select the appropriate keyboard. If you select another language other than English, be aware that your screen will look different that what you will see in these tutorials.



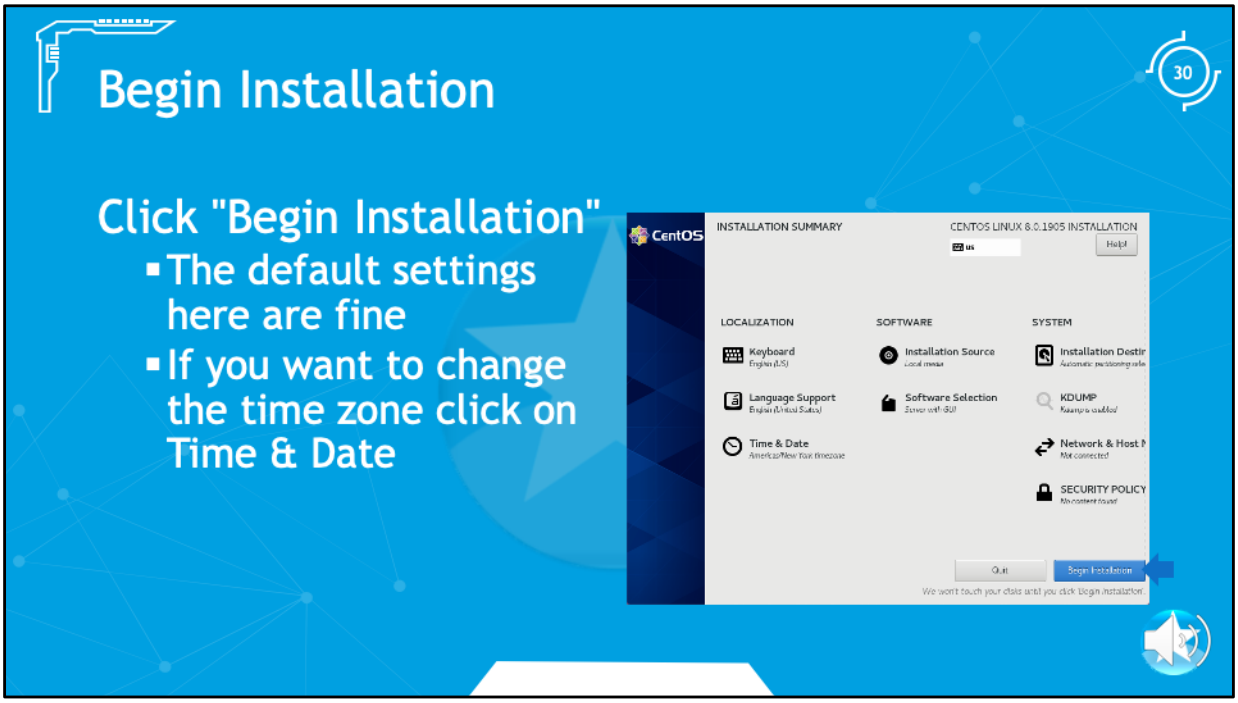
We need to select the install location for our VM. Click the first item under "SYSTEM". The words "Installation Destination" is likely truncated like it is in our screenshot.

Installation Destination

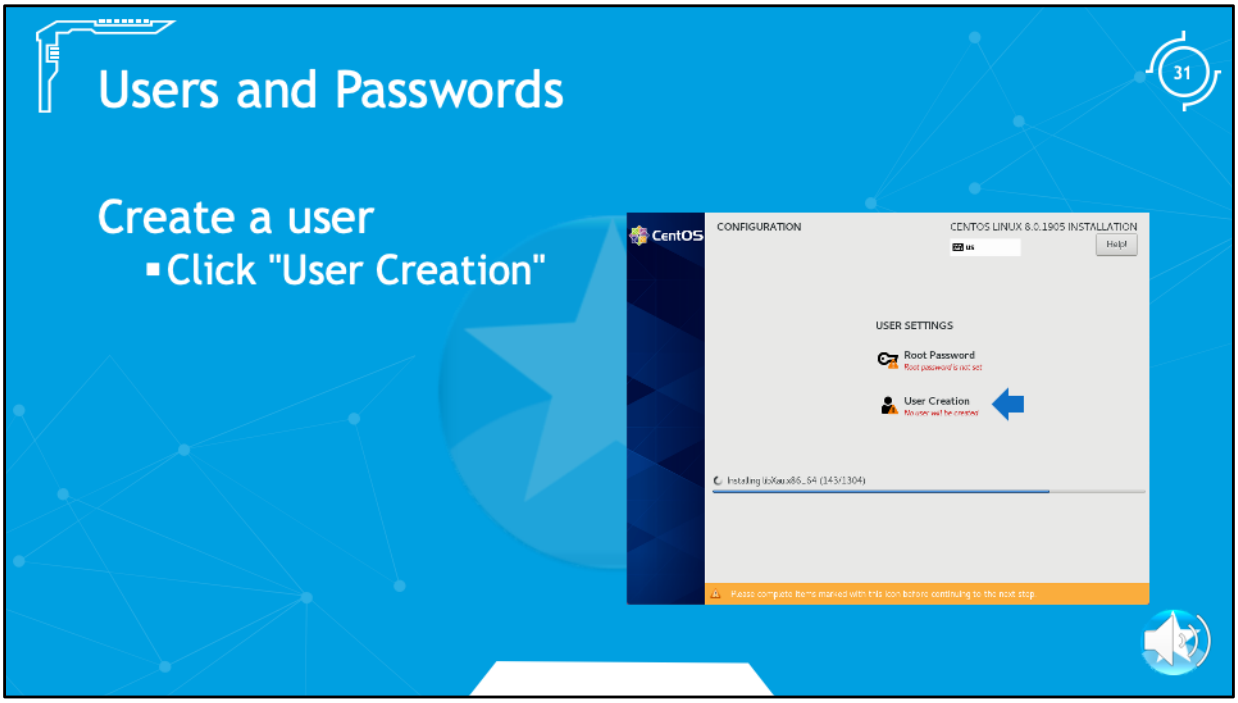
You can use the defaults by simply clicking "Done" in the top left



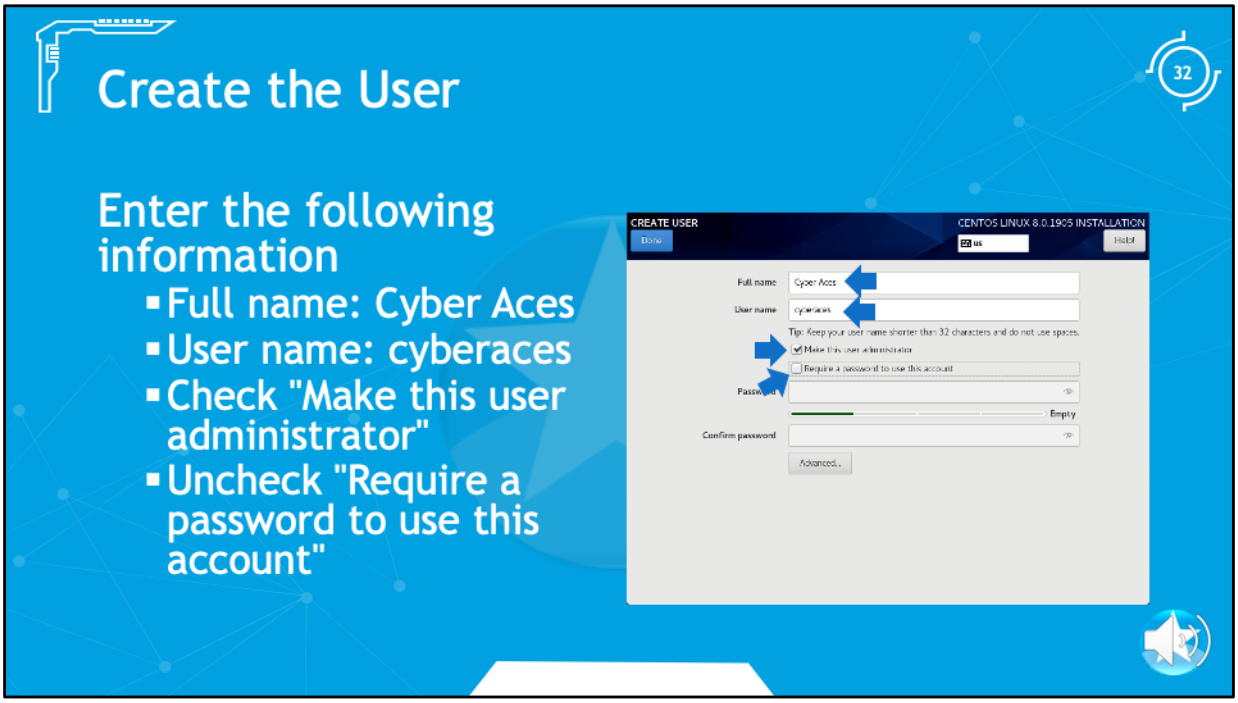
We can use the defaults here to use the entirety of our VMs hard disk.



The default values here are fine. However, if you want to change any of the settings, such as time zone, then feel free to do so. Once you are ready, click "Begin Installation".



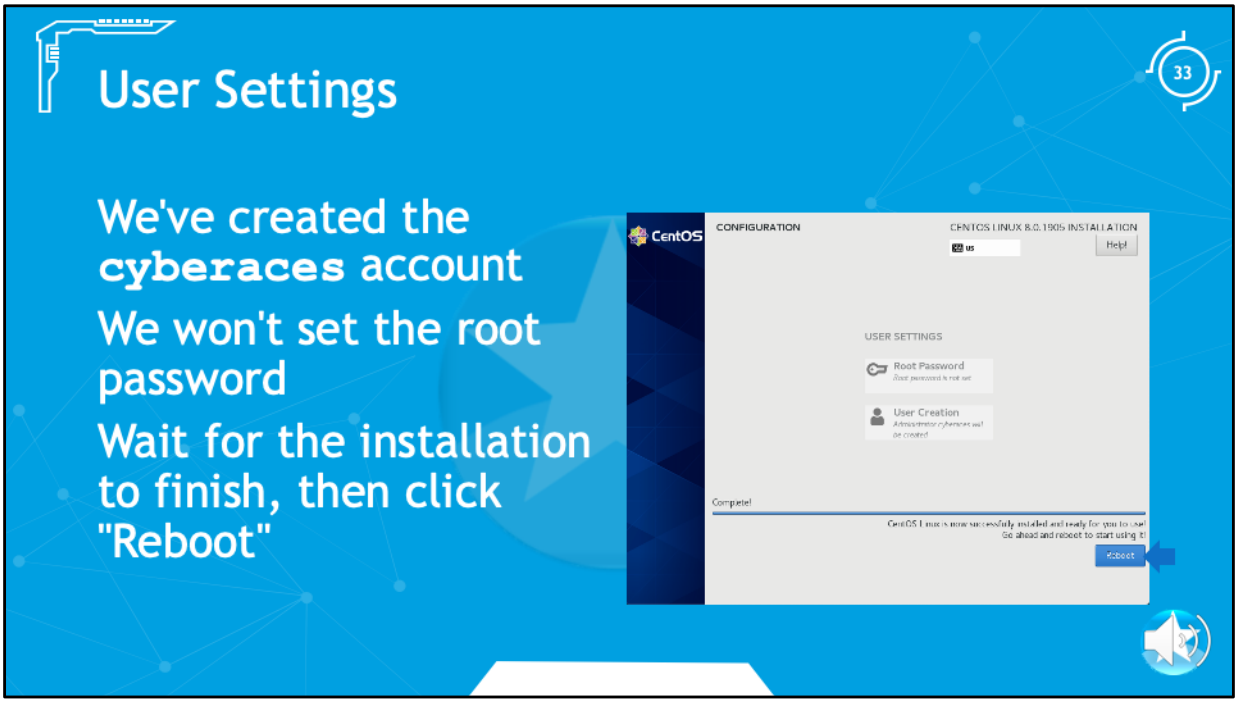
We now need to create a user. Click "User Creation" then go to the next page.



You need to provide details for a new user. Use the following information:

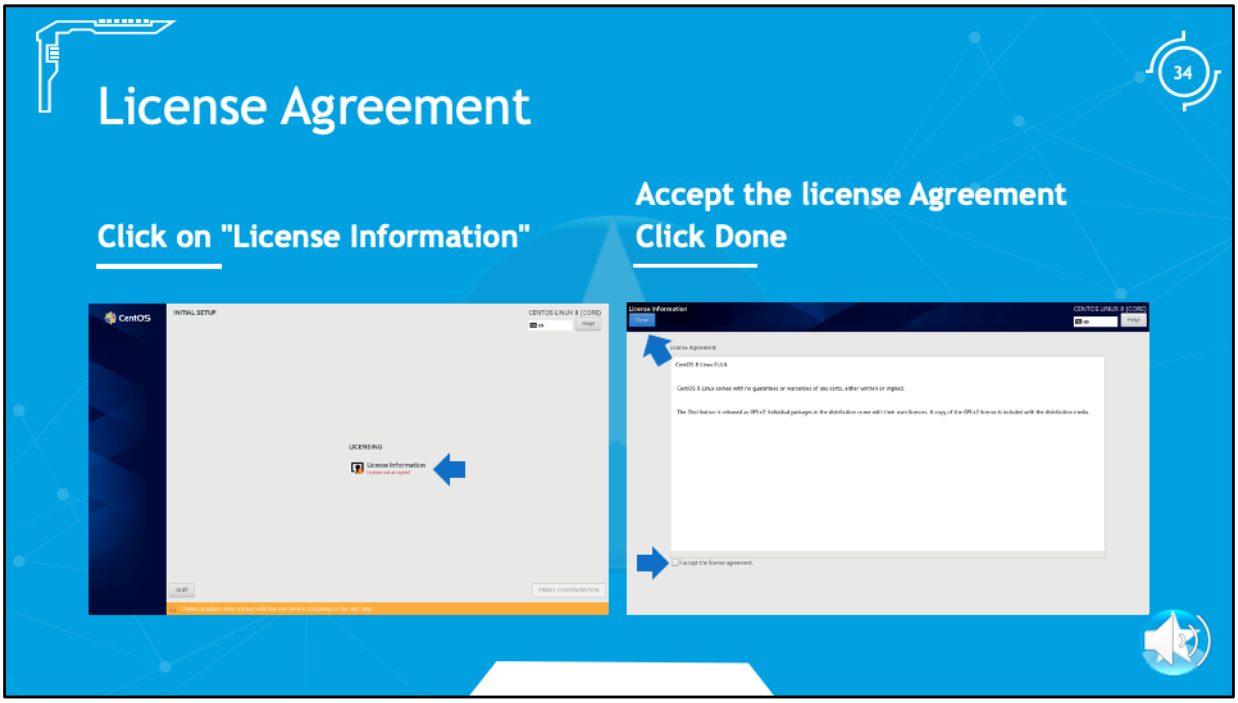
- Full name: Cyber Aces
- User name: cyberaces
- Make this user administrator: Checked
- Require a password to use this account: Unchecked

Normally we'd select a password for this user for better security. Since this is just a training VM we can use the less secure option.



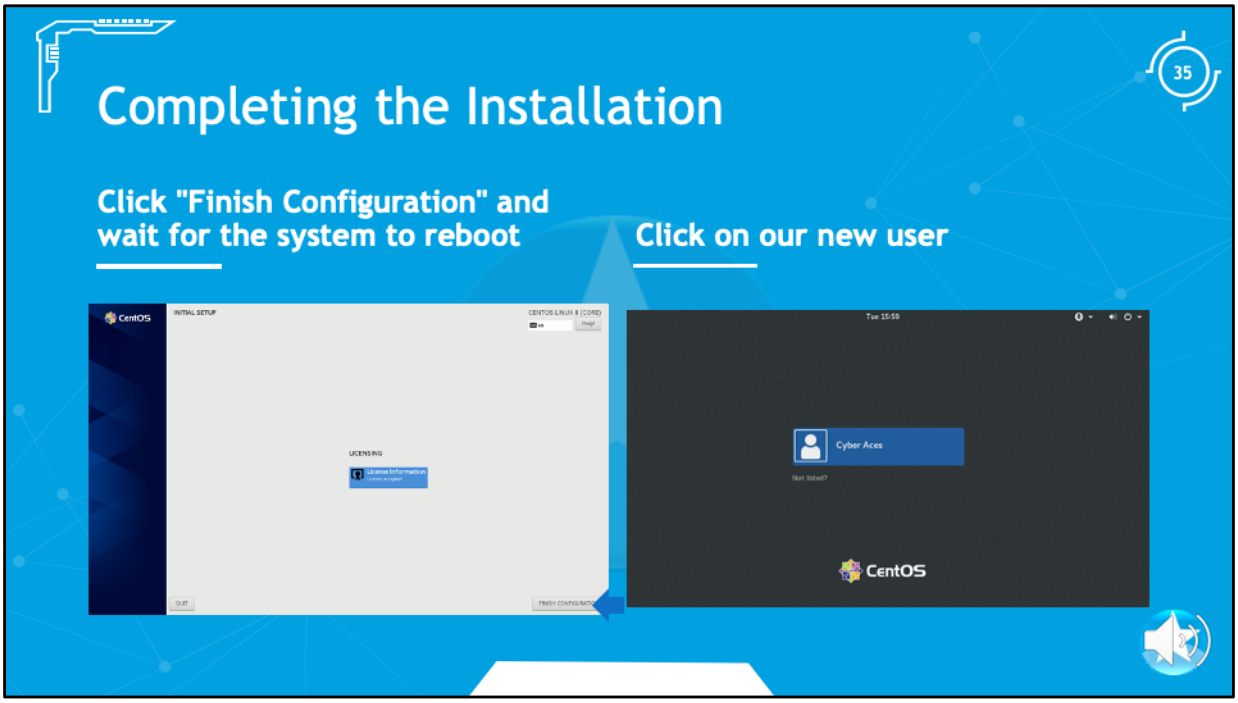
We have now created the **`cyberaces`** account. We won't set the **`root`** password at this time and we'll use our administrator account to administer the system.

The installation can take a while. Once the installation is complete, click the "Reboot" button.

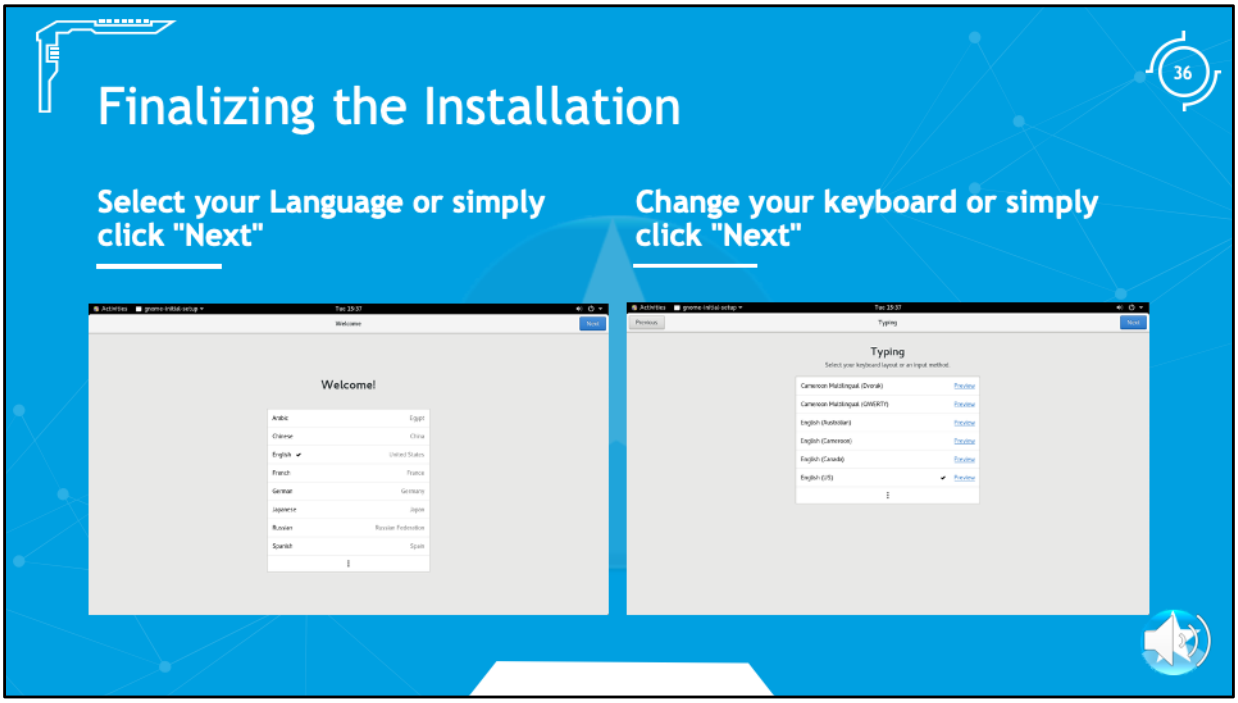


We need to agree to the license before we can finalize the setup. Click the "License Information" button in the middle of the screen.

On the next screen, click "I accept the license agreement", then click "Done"



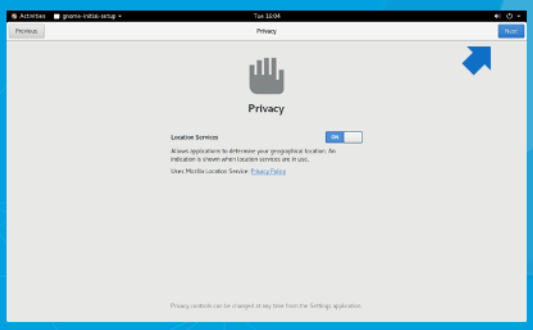
After agreeing to the licensing terms, click "Finish Configuration" and then wait for the system to reboot. After the system as rebooted, click on the newly created "Cyber Aces" user.



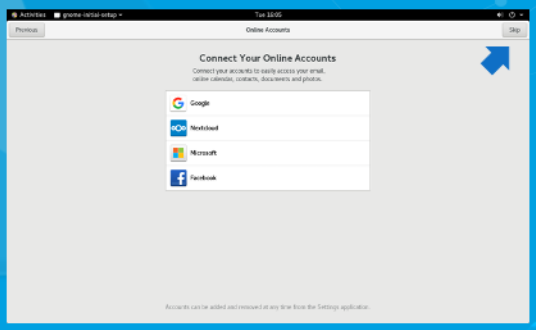
First, select your language. We highly recommend using the defaults here and simply click "Next" on both of these screens. Note: If you select a language other than English your user interface will likely look different than the tutorials.

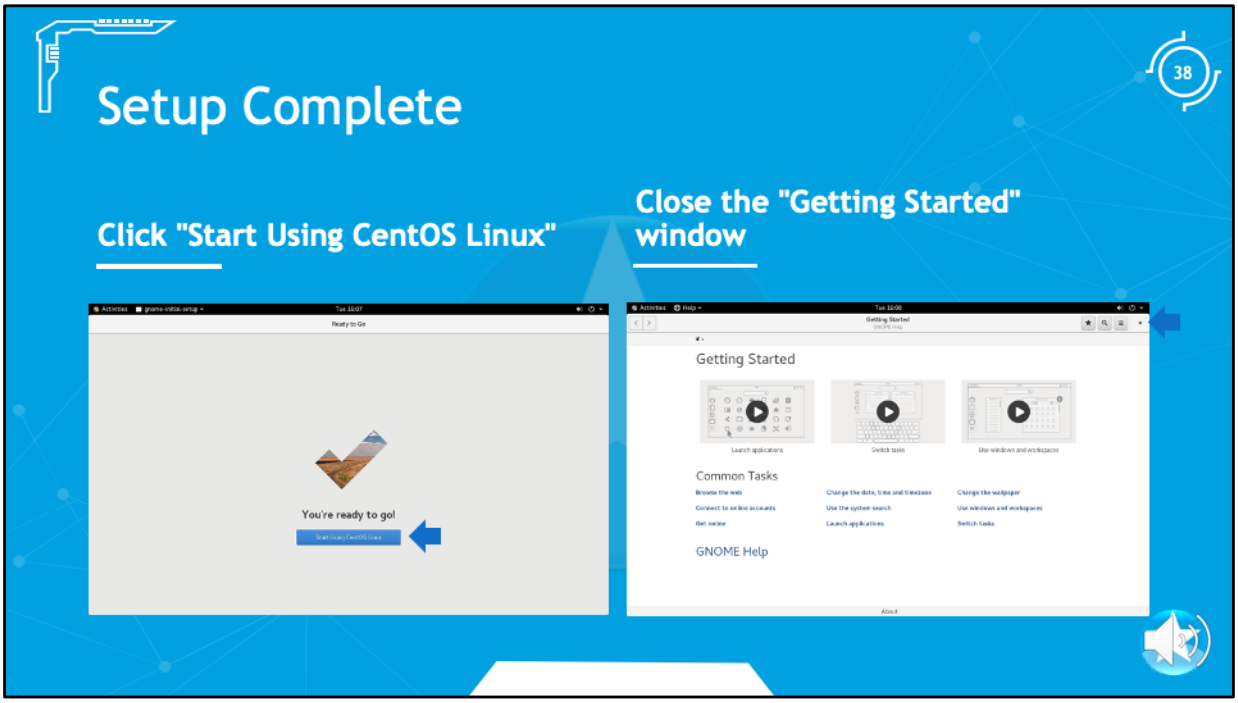
Wrapping up the Installation

Toggle Location Services or simply click "Next"

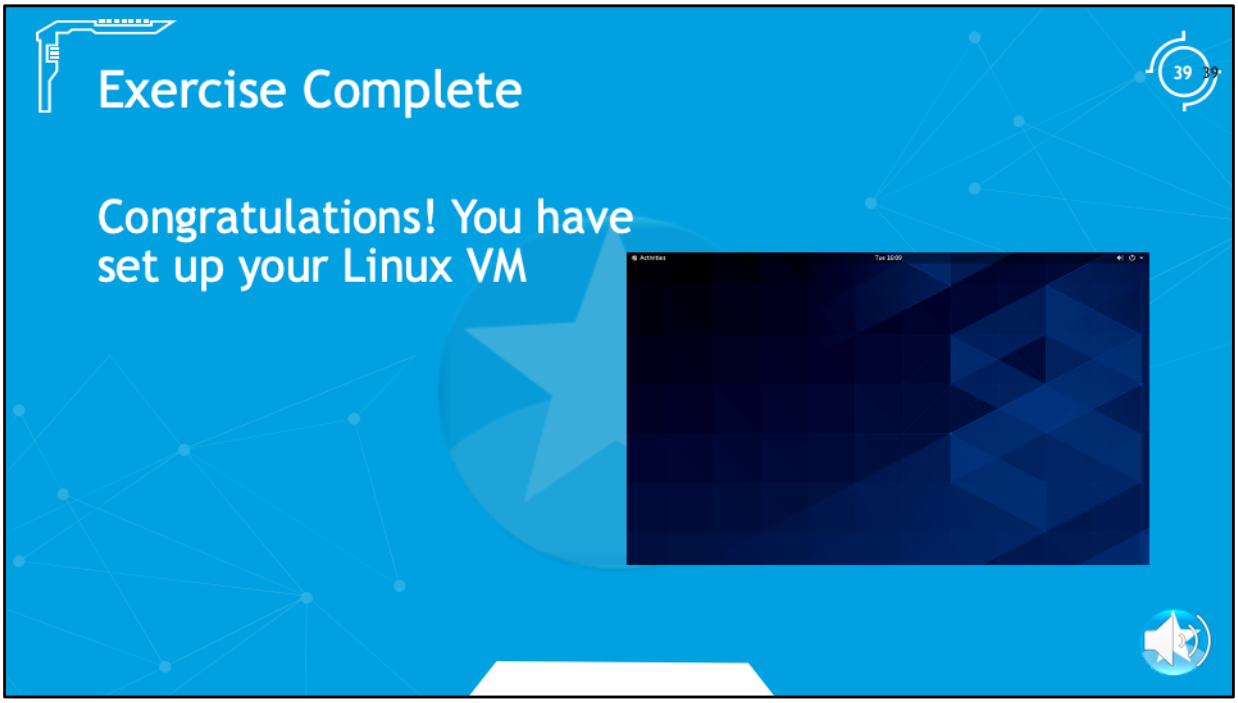


"Skip" connecting online accounts

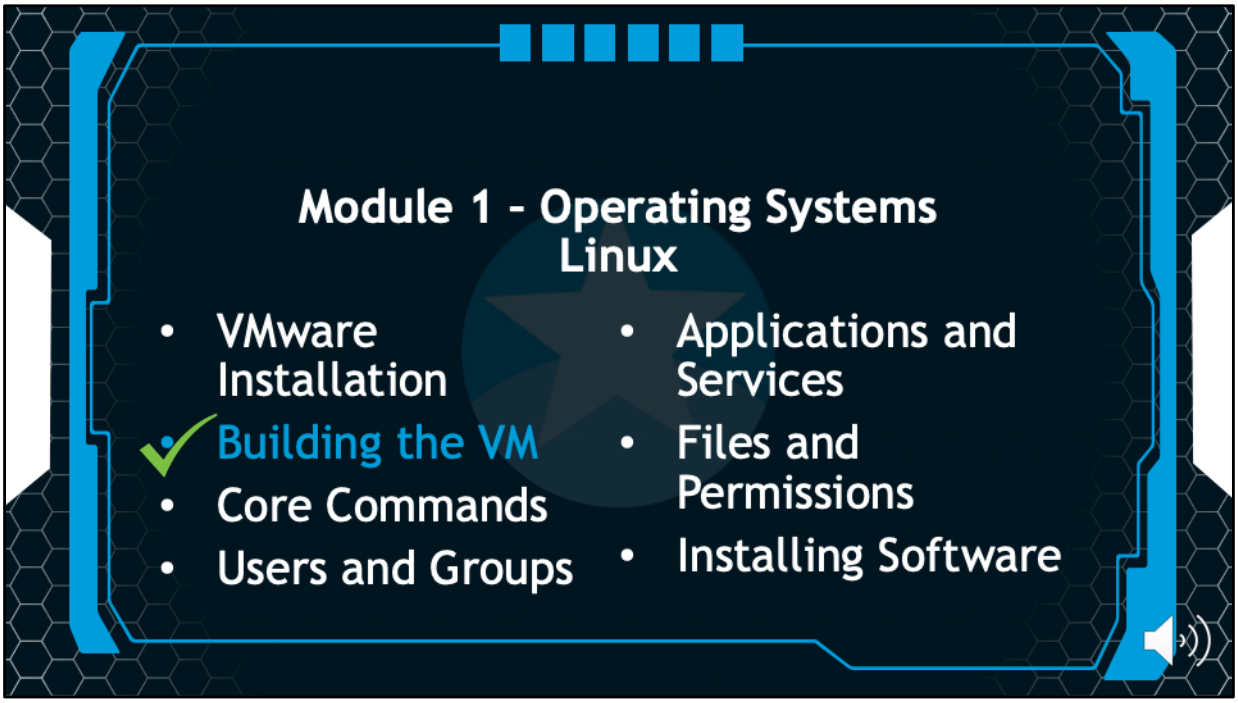




The setup is nearly complete. Click the "Start Using CentOS Linux" button. You will then be shown a "Getting Started" window. You can simply close this window.



Congratulations! You have set up your Linux VM.



We have just completed building the CentOS virtual machine. In the next session, we'll discuss core commands that all Linux users need to know.