

# Cyber Aces

## Module 1 – Operating Systems

### OS Background and CentOS Guest Installation

By Tom Hessman, Tim Medin, Mark Baggett, Doug Burks,  
Michael Coppola, Russell Eubanks, and Ed Skoudis

Presented by Tim Medin

v15Q1

This tutorial is licensed for personal use exclusively for students and teachers to prepare for the Cyber Aces competition. You may not use any part of it in any printed or electronic form for other purposes, nor are you allowed to redistribute it without prior written consent from the SANS Institute.

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

1

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.

# Overview of Operating Systems

- An operating system is software that manages and controls a computer's core functionality
  - Manages hardware and software resources
  - Provides an interface for other software to use for interaction with the user and the hardware
  - Implements security functions
- All computers, cell phones, printers, HDTV's, etc., have some form of an operating system

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

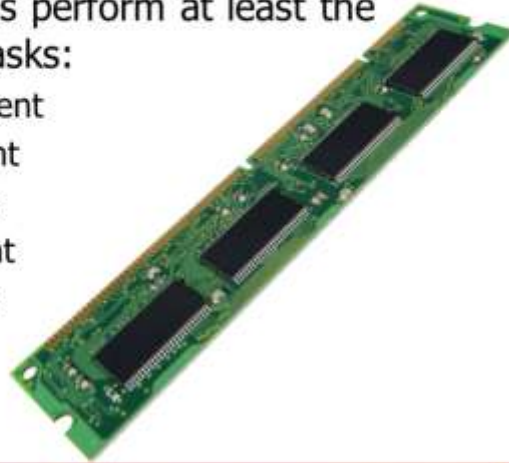
2

## Overview of Operating Systems

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.

# Core OS Tasks

- All operating systems perform at least the following six basic tasks:
  - Processor management
  - Memory management
  - Device management
  - Storage management
  - Application interface
  - User interface



Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

3

## Core OS Tasks

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".

**Application interface:** The OS provides an interface to the computer's functionality for programmers to use called an Application Programming Interface (API). This allows programs to be written to take advantage of the operating system's features and the computer's hardware using a standardized set of functions.

**User interface:** The OS provides an interface for the user to interact with the computer or device. The user interface could just be a shell with a command prompt, or it could be a graphical user interface such as the Windows desktop.

# User Mode vs. Kernel Mode

- Operating systems generally run applications in either Kernel Mode or User Mode
- Kernel Mode provides full, unrestricted access to the kernel and hardware resources
  - Runs in Ring 0 of the CPU
- User Mode imposes restrictions to protect the kernel
  - Runs in Ring 3 of the CPU
- A well designed OS limits all user interaction to User Mode, and only uses Kernel Mode when necessary
  - Attackers with full kernel access are only limited by their imagination and technical skill

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

4

## User Mode vs. Kernel Mode

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.

# Popular Operating Systems

- Microsoft Windows
  - Proprietary operating system created by Microsoft Corporation
  - Most popular desktop operating system
- Linux
  - Open source operating system built around the Linux kernel and GNU utilities (sometimes called GNU/Linux), inspired by Unix
    - The GNU project maintains a set of core OS utilities
  - Many companies and organizations release their own distributions of Linux, such as Red Hat, Fedora, and Ubuntu
  - Very popular on servers
- Mac OS X
  - Proprietary operating system created by Apple Inc.
  - Has a Unix backend with a very user friendly GUI
- This course will focus on Windows and Linux

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

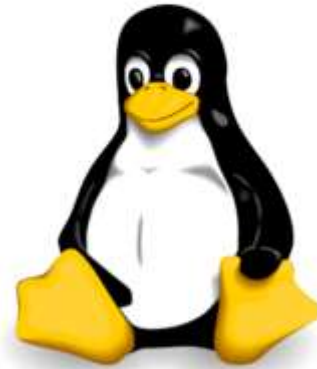
5

## Popular Operating Systems

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.

# Introduction to Linux

- Linux is an open source operating system kernel, based on Unix
- The kernel was originally developed by Linus Torvalds, who still leads the project
- Linux is not a complete operating system without user-space utilities, such as those from the GNU project
  - Some people refer to a complete system as GNU/Linux
- Linux is a very powerful and flexible framework that can be built upon



Tux

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

6

## Introduction to 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, who still leads the project. 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.



# Linux Distributions

- Several vendors distribute their own versions of Linux, which are called *distributions* (or *distro* for short)
- A distribution generally combines the Linux kernel with all necessary applications and utilities to form a complete operating system
- The most popular distributions are Red Hat/Fedora, CentOS, Ubuntu, and Suse
- There are TONS of distributions out there!



Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

7

## 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 <http://distrowatch.org>. To see a list of the major distributions click on the "Major Distributions" link at the top of the distrowatch.org website.

# CentOS

- CentOS is a free clone of Red Hat Enterprise Linux
  - RHEL is the most popular commercial distribution
- Like RHEL, CentOS has a long support cycle (10 years), whereas most popular distros drop support for old releases every 6-12 months
- We will use CentOS for our examples in this course, since it stays the same for much longer



Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

8


## CentOS

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):
  - [http://www.centos.org/docs/6/html/Installation\\_Guide-en-US/](http://www.centos.org/docs/6/html/Installation_Guide-en-US/)
  - [http://www.centos.org/docs/6/html/Deployment\\_Guide-en-US/](http://www.centos.org/docs/6/html/Deployment_Guide-en-US/)



# Linux Introductory Exercise

- For hands-on exercises, we will use CentOS running inside a VMware virtual machine
- To get started, download and install VMware Player or Fusion. See the earlier training on the installation of VMware Player and Fusion
- Then, download the CentOS 6.5 LiveCD from:
  - <http://mirror.symnds.com/distributions/CentOS-vault/6.5/isos/i386/CentOS-6.5-i386-LiveCD.iso>
  - <http://tinyurl.com/centos65livecd>  Shortened URL

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

9

## Linux Introductory Exercise

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. To get started, download and install VMware Player from this location: <http://www.vmware.com/go/downloadplayer/>

Then, download the CentOS 6.5 LiveCD from either of these locations (they both point to the same file, you only need one):

<http://mirror.symnds.com/distributions/CentOS-vault/6.5/isos/i386/CentOS-6.5-i386-LiveCD.iso>

<http://tinyurl.com/centos65livecd>

The .iso file here is a 32-bit LiveCD version of CentOS 6.5. The 32-bit version will run on both 64-bit and 32-bit hardware, but the reverse is not true. If you would like to use the 64-bit version, or download via torrent, you can find a full list of the CentOS LiveCD, LiveDVD, and other installs at this location:

<http://mirror.symnds.com/CentOS/>

## Creating the VM

- The setup instructions using VMware Player are much different than the instruction using VMware Fusion
- Mac OS X users using VMware Fusion should skip ahead to the page titled "Create the VM with Fusion"
- Windows and Linux users using VMware Player should continue to the next page

### Creating the VM

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.

# Creating the VM with Player (Windows and Linux Users)



- Start VMware Player and click "Create a New Virtual Machine"
- When prompted, select the CentOS ISO file you downloaded
- Click "Next" to continue



Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

11

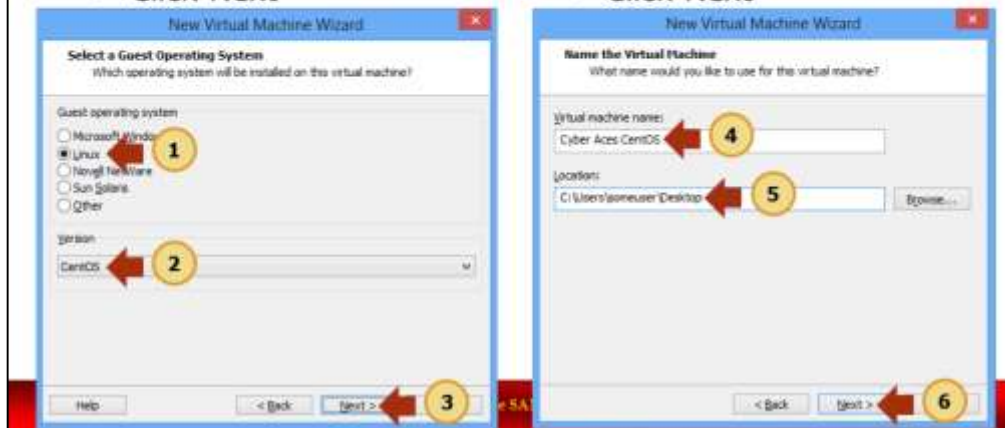
## Creating the VM with Player (Windows and Linux Users)

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.

## Creating the VM with Player (2)

- Select "Linux"
- Select "CentOS"
- Click Next
- Specify a Name
- Select a save location
- Click Next



### Creating the VM with Player (2)

On the next configuration screen, you will need to tell VMware what guest operating system will be used. You should select "Linux" as the Guest operating system and "CentOS" as the version. If you downloaded the 64-bit version of CentOS then select CentOS 64-bit. Click "Next" to continue to the next step.

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.

## Creating the VM with Player (3)

- On the "Specify Disk Capacity" screen, set the value as low as possible (0.001), as we will be running off the LiveCD ISO
- Click Next
- Click "Finish"



### Creating the VM with Player (3)

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 are using a LiveCD, so the hard drive will not be used. Select the smallest possible option of 0.001 GB. A LiveCD (or LiveDVD) runs the entire operating system in memory and does not use the hard drive. That means that any changes made in the VM will be lost as they are not saved to disk.

Click "Next", review the settings, and click "Finish" to finalize the creation of the VM.

## Creating the VM with Player (4)

- Click the green "Play virtual machine" button
- If prompted, skip the installation of VMware Tools by clicking "Remind Me Later"
  - Remember changes will be lost after reboot since this is a LiveCD so the install in the VM is not beneficial
- Congratulations, you have set up your Linux VM!
- **Note:** If the guest has control of your mouse and keyboard, press the Control and Alt Keys at the same time



Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

14

### Creating the VM with Player (4)

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.



# Creating the VM with Fusion



- Click the +
- Create a new VM
- Click "Install from disk or image"
- Click "Continue"
- Click "Use another disc or disc image"
- Select the ISO
- Click "Continue"



Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

15

## Creating the VM with Fusion

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".

## Creating the VM with Fusion (2)

- Select "Linux" and "CentOS", then click "Continue"
  - The LiveCD presented previously is 32-bit so don't select the 64-bit option on the screen shown on the top right
- Click "Customize Settings"
  - We will adjust the disk space shortly
  - Name the file
  - Save the File
- Click "Continue"



Cyber Aces Online Module 1 - ©2015 The SAN'S Institute. Redistribution Prohibited.

16

### Creating the VM with Fusion (2)

We need to tell Fusion what type of operating system we are installing. On the "Choose Operating System" screen, select "Linux" as your operating system and "CentOS" as the operating system version. The suggested .iso file is a 32-bit operating system and will work on both 32-bit and 64-bit hardware; as such you should NOT select "CentOS 64-bit", unless you specifically downloaded a 64-bit version of CentOS. After you have selected both of these options, click "Continue".

The creation is nearly complete, but before we finish we need to change a few settings. Do NOT click the "Finish" button, but click on "Customize Settings" instead. Before we can customize the VM we need to save it. Name the VM "Cyber Aces CentOS.vmwarevm" (or any name of your choosing) and click "Save".

## Creating the VM with Fusion (3)

- The .ISO is a LiveCD and doesn't need a hard disk
  - We can remove the hard disk to save space on your physical drive
- To remove the hard disk:
  - Click "Hard Disk"
  - Expand "Advanced Options"
  - Click "Remove Hard Disk"
  - Delete the disk by clicking "Move to Trash"
  - Close the window



### Creating the VM with Fusion (3)

The CentOS .ISO file we are using is a LiveCD. This means that the entire operating system will run in your computer's RAM, so the VM doesn't need a hard drive. We can then remove the hard drive from the VM to save space on your physical drive. Note, as this VM doesn't have a hard drive, all files and changes made in the VM will be lost upon reboot.

To remove the drive follow these steps. First, click on "Hard Disk" within the virtual machine's settings. A new window will open. Expand "Advanced Options" and click "Remove Hard Disk". When prompted, select "Move to Trash". You have removed the disk. You can close the window to confirm the changes.

## Creating the VM with Fusion (4)

- Click the "Start Up" button to start the VM
- Congratulations, you have set up your Linux VM! You have completed this exercise.
- Note: If the guest has control of your keyboard and mouse press Command and Ctrl keys to release control



### Creating the VM with Fusion (4)

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 its 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.

## Exercise Complete!

---

- Congratulations! You have set up your Linux VM