Linux Essentials for Cybersecurity Lab Manual

Instructor's Answer Key

William "Bo" Rothwell

PEARSON IT CERTIFICATION

Linux Essentials for Cybersecurity Lab Manual

Instructor's Answer Key

ISBN-13: 978-0-7897-6055-5
ISBN-10: 0-7897-6055-X

Instructor's Answer Key

ISBN-13: 978-0-13-530516-4
ISBN-10: 0-13-530516-0

Library of Congress Control Number: 2018949197

01 18

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Acquisitions Editor
Mary Beth Ray

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Proofreader
Debbie Williams

Technical Editor
Denise Kinsey

Publishing Coordinator
Vanessa Evans

Designer
Chuti Prasertsith

Compositor
Bronkella Publishing

Contents at a Glance

Table of Contents

About the Author

At the impressionable age of 14, **William "Bo" Rothwell** crossed paths with a TRS-80 Micro Computer System (affectionately known as a "Trash 80"). Soon after the adults responsible for Bo made the mistake of leaving him alone with the TRS-80, he immediately dismantled it and held his first computer class, showing his friends what made this "computer thing" work.

Since that experience, Bo's passion for understanding how computers work and sharing this knowledge with others has resulted in a rewarding career in IT training. His experience includes Linux, Unix, and programming languages such as Perl, Python, Tcl, and BASH. He is the founder and president of One Course Source, an IT training organization.

Dedication

For the last three books, I have thanked my wife and daughter for their patience and my parents for all that they have done throughout my life. My gratitude continues, as always.
—William "Bo" Rothwell
May 2018

Acknowledgments

Thanks to everyone who has put in a direct effort toward making this book a success: You have my thanks, as always.

—William "Bo" Rothwell

May 2018

About the Technical Reviewer

Denise Kinsey, Ph.D., CISSP, CISCO, served as a Unix administrator (HP-UX) in the late 1990s and realized the power and flexibility of the operating system. This appreciation led to her home installation of different flavors of Linux and creation of several academic courses in Linux. With a strong background in cybersecurity, she works to share and implement best practices with her customers and students. Dr. Kinsey is an assistant professor at the University of Houston.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Reader Services

Register your copy of *Linux Essentials for Cybersecurity Lab Manual* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789760555 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Figure Credits

Figure 1-1 Courtesy of CentOS Corporation

Figure 9-1 Courtesy of CentOS Corporation

Figure 10-1 Courtesy of CentOS Corporation

Figure 10-2 Courtesy of CentOS Corporation

Figure 11-1 Courtesy of CentOS Corporation

Figure 11-2 Courtesy of CentOS Corporation

Introduction

While developing *Linux Essentials for Cybersecurity*, it became clear that having hands-on experience would be very useful. Reading new content gets you only so far. To really become a Linux cybersecurity expert, you need practice. From that idea, this lab guide was born.

You will note that there are three different types of labs in this book:

- Labs in which you are presented with a short problem that requires only a single operation to complete.
- Labs that are more complex but in which we provide you with a guide to perform each step, one at a time.
- Scenario labs in which you are asked to solve a problem entirely on your own. These labs are designed to pose a greater challenge.

No matter the type, these labs are designed to be performed on live systems. While you could just write down the answers in some cases, I highly encourage you to work on Linux systems to complete all the labs. Not only will you get a sense of accomplishment, but the concepts and practices that are explored in *Linux Essentials for Cybersecurity* are more likely to find a permanent home in your brain.

Enjoy the journey and remember to always stand on the light side of the cybersecurity force.

Who Should Read This Book?

It might be easier to answer the question "Who shouldn't read this book?" Linux distributions are used by a large variety of individuals, including the following:

- Software developers
- Database administrators
- Website administrators
- Security administrators
- System administrators
- System recovery experts
- Big data engineers
- Hackers
- Government organizations
- Mobile users and developers (Android is a Linux distribution.)
- Chip vendors (Embedded Linux is found on many chip devices.)
- Digital forensic experts
- Educators

This isn't even a complete list! Linux is literally everywhere. It is the operating system used on Android phones. A large number of web and email servers run on Linux. Many network devices, such as routers and firewalls, have a version of embedded Linux installed on them.

This book is for people who want to better use Linux systems and ensure that the Linux systems they work on are as secure as possible.

How This Book Is Organized

Chapter 1, "Distributions and Key Components," includes labs in which you will install the Linux distributions that you will use throughout the rest of this book.

Chapter 2, "Working on the Command Line," covers labs related to the essential commands needed to work in the Linux environment.

Chapter 3, "Getting Help," provides you with hands-on experience to get additional information on Linux topics.

Chapter 4, "Editing Files," incorporates labs in which you practice using the **vim** editor.

Chapter 5, "When Things Go Wrong," provides you with experience in how to handle problems that may arise in Linux.

Chapter 6, "Managing Group Accounts," contains labs that focus on group accounts, including how to add, modify, and delete groups.

Chapter 7, "Managing User Accounts," contains labs that focus on user accounts, including how to add, modify, and delete users. This chapter also has a lab for securing user accounts as well as a lab for configuring **sudo**.

Chapter 8, "Develop an Account Security Policy," provides you with practice creating a user security policy and how to test the security of accounts.

Chapter 9, "File Permissions," focuses on securing files using Linux permissions. These labs also dive into more advanced topics, such as special permissions, **umask**, access control lists (ACLs), SELinux, and file attributes.

Chapter 10, "Manage Local Storage: Essentials," includes labs that are related to the concepts involved with local storage devices, such as how to create partitions and filesystems and some additional essential filesystem features.

Chapter 11, "Manage Local Storage: Advanced Features," provides hands-on activities related to advanced features of local storage devices, including how to create encrypted filesystems. You will get practice creating and managing logical volumes.

Chapter 12, "Manage Network Storage," provides exercises that are focused on making storage devices available across the network. Filesystem sharing techniques such as Network File System, Samba, and iSCSI are included.

Chapter 13, "Develop a Storage Security Policy," provides you with the experience of creating a security policy using the knowledge you acquired in Chapters 9–12. There is also a very important lab that covers performing filesystem backups.

Chapter 14, "Crontab and At," includes labs for managing the **crontab** and **at** systems.

Chapter 15, "Scripting," provides you with experience in shell scripting by having you create two shell scripts.

Chapter 16, "Common Automation Tasks," includes labs on creating shell scripts that are commonly used to automate tasks on Linux systems.

Chapter 17, "Develop an Automation Security Policy," provides you with the experience to create a security policy using the knowledge you acquired in Chapters 14–16. This chapter also includes a hands-on lab on securing the **crontab** and **at** systems.

Chapter 18, "Networking Basics," provides labs that help you explore network components on Linux.

Chapter 19, "Network Configuration," covers the process of configuring your system to connect to a network, both on Ubuntu and CentOS.

Chapter 20, "Network Service Configuration: Essential Services," includes labs for configuring several network-based tools, including DNS and email servers.

Chapter 21, "Network Service Configuration: Web Services," provides the experience of configuring several network-based tools, including the Apache web server and Squid.

Chapter 22, "Connecting to Remote Systems," includes labs on configuring LDAP, FTP, and SSH servers.

Chapter 23, "Develop a Network Security Policy," provides you with the experience to create a security policy using the knowledge you acquired in Chapters 18–22.

Chapter 24, "Process Control," includes labs on starting, viewing, and controlling processes (programs).

Chapter 25, "System Logging," gives you hands-on experience with viewing system logs as well as how to configure a system to create custom log entries.

Chapter 26, "Red Hat–Based Software Management," includes labs on administering software on Red Hat–based systems such as Fedora and CentOS.

Chapter 27, "Debian–Based Software Management," includes labs on administering software on Debian–based systems, such as Ubuntu.

Chapter 28, "System Booting," gives you practice configuring GRUB and managing the boot process.

Chapter 29, "Develop a Software Management Security Policy," provides you with the experience to create a security policy using the knowledge you acquired in Chapters 26–28. In addition, you will explore CVE reports.

Chapter 30, "Footprinting," includes labs that cover the techniques that hackers use to discover information about systems.

Chapter 31, "Firewalls," explores labs focused on configuring software that protects your systems from network-based attacks.

Chapter 32, "Intrusion Detection," provides you with experience using tools and techniques that help you determine if someone has successfully compromised the security of your systems.

Chapter 33, "Additional Security Tasks," includes labs that cover a variety of additional Linux security features, including the fail2ban service, VPNs, and file encryption.

Chapter 1

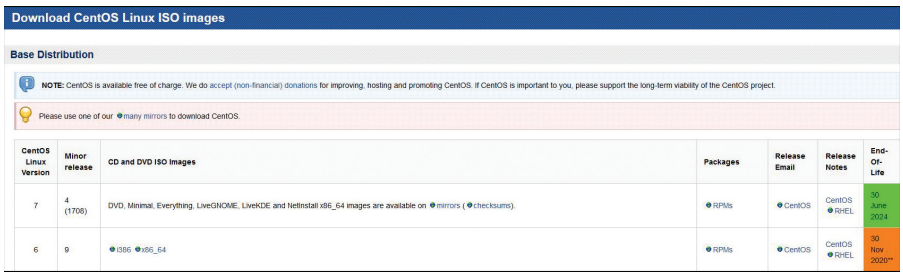
Distributions and Key Components

The goal of this lab is to help you install the three operating systems that you will use during the remainder of the labs. Oracle Virtual Box should be installed on your system before you proceed. You will also need at least 8GB of RAM (4GB for your host operating system and 4GB for the virtual machine). Note that while you will be installing three Linux distributions, only one will be "active" (booted up) at any given point during these labs.

You will also need 36GB total hard drive space for the three distributions (two distributions will use 10GB of space each, and the other will use 16GB of space).

Lab 1.1 Installing CentOS

STEP 1. Go to **https://wiki.centos.org/Download** and click the mirrors link for the ISO images:



STEP 2. Click on a mirror site of your choosing and then click on the **CentOS-7-x86_64-Everything-1708.iso** link to download the file. It takes some time for the file to download.

STEP 3. Start Oracle VirtualBox and then click the **New** button.

STEP 4. Enter **CENTOS 7 - for class** in the Name box.

STEP 5. Change the memory size to **4196 MB** and click the **Create** button.

STEP 6. Change the file size to **10.00 GB**.

STEP 7. Change the storage on physical hard disk to **Fixed Size** and click the **Create** button.

STEP 8. When you are returned to the main Oracle VirtualBox screen, click on the **Start** button.

STEP 9. Click on the small folder icon next to the drop-down list and navigate to the location where you downloaded the CentOS ISO file. Select that file and then click the **Open** button.

STEP 10. Click the **Start** button.

STEP 11. Click in the installation window and then at the CentOS 7 screen, either press the **Enter** key to start the installation or wait for the timer to run down and the installation to begin automatically.

> **NOTE** You can press the **Esc** key to avoid the lengthy media check. In addition, to "get out of" the virtual machine, press your right **Ctrl** key (the Ctrl key on the right side of your keyboard).

STEP 12. At the Welcome to CENTOS 7 screen, click the **Continue** button to accept the default installation language, English.

STEP 13. Click the **Installation Destination** button.

STEP 14. Under Local Standard Disks, click on the icon of the **10 GiB** disk multiple times until it is marked as selected. It is marked as selected when a checkmark appears next to the disk icon.

STEP 15. Click the **Done** button in the upper-left area of the window.

STEP 16. Click the **Network & Host Name** button.

STEP 17. Click the icon next to **Ethernet (enp0s3)** to change the value from **OFF** to **ON**.

STEP 18. Click the **Done** button to return to the INSTALLATION SUMMARY screen.

STEP 19. Click the **SOFTWARE SELECTION** button.

STEP 20. Click **GNOME Desktop** and then click the **Done** button.

STEP 21. Click the **Begin Installation** button.

STEP 22. While the installation is running, click on the **ROOT PASSWORD** button and set a password for the root account that is easy for you to remember. You may need to click the **Done** button twice if your password isn't very strong.

STEP 23. While the installation is running, click on the **USER CREATION** button.

STEP 24. For both full name and user name, enter **student**. Enter a password of your choosing and then click the **Done** button. You may need to click the **Done** button twice if your password isn't very strong. Do not make this account an administrator.

STEP 25. When the installation is complete, click the **Reboot** button.

STEP 26. After the system boots, when the INITIAL SETUP screen appears, click the **LICENSE INFORMATION** button.

STEP 27. Click the box next to **I accept the license agreement** and then click the **Done** button in the upper-left corner of the screen.

STEP 28. Click the **FINISH CONFIGURATION** button.

STEP 29. At the login screen, log in as the student user.

STEP 30. After logging in, click the **Next** button at the Welcome screen.

STEP 31. Click the **Next** button at the Typing screen.

STEP 32. Turn off **Location Services** and then click the **Next** button.

STEP 33. Click the **Skip** button at the Online Accounts screen.

STEP 34. Click the **Start using CentOS Linux** button.

STEP 35. If you are interested, you can view the help videos for using GNOME on the Getting Started screen. Close this window when finished.

STEP 36. For the next lab, you need to suspend the CentOS operating system. By suspending, you can start again quickly from the Oracle VirtualBox manager. To suspend, click the close box (the **X**) in the upper-right corner. Make sure **Save the machine state** is selected and then click the **OK** button. When you want to use CentOS again, just double-click the **CENTOS 7 - for class (Saved)** icon in the Oracle VM VirtualBox Manager window.

Lab 1.2 Installing Ubuntu

STEP 1. Go to **https://www.ubuntu.com/download/desktop** and click on the **Download** button.

STEP 2. Click the **Not now, take me to the download** link to download the file. It takes some time to download the file.

STEP 3. Start Oracle VirtualBox and click the **New** button.