



LAB MANUAL



LINUX ESSENTIALS FOR CYBERSECURITY

WILLIAM "BO" ROTHWELL

Linux Essentials for Cybersecurity Lab Manual

William “Bo” Rothwell

PEARSON IT CERTIFICATION

Linux Essentials for Cybersecurity Lab Manual

Table of Contents

Cover

Title Page

Copyright Page

About the Author

Dedication

Acknowledgements

Table of Contents

Introduction

Part I: Introducing Linux

Chapter 1 Distributions and Key Components

Lab 1.1 Installing CentOS

Lab 1.2 Installing Ubuntu

Lab 1.3 Installing Kali

Chapter 2 Working on the Command Line

Lab 2.1 Manage Files

Lab 2.2 Using Shell Features

Lab 2.3 Compressing Files

Chapter 3 Getting Help

Lab 3.1 Getting Help with man

Lab 3.2 Getting Help with info

Chapter 4 Editing Files

Lab 4.1 Editing Files with the vim Editor

Chapter 5 When Things Go Wrong

Lab 5.1 Troubleshooting Linux Issues

Lab 5.2 Configuring User Notifications

Part II: User and Group Accounts



Table of Contents

Chapter 6 Managing Group Accounts

Lab 6.1 Managing Group Accounts

Lab 6.2 Managing Group Administrators

Chapter 7 Managing User Accounts

Lab 7.1 Managing User Accounts

Lab 7.2 Securing User Accounts

Lab 7.3 Configuring sudo

Chapter 8 Develop an Account Security Policy

Lab 8.1 Testing the Security of Accounts

Lab 8.2 Developing an Account Security Policy

Part III: File and Data Storage

Chapter 9 File Permissions

Lab 9.1 Managing File Permissions

Lab 9.2 Managing Special Permissions

Lab 9.3 Enabling Access Control Lists

Lab 9.4 Managing File Ownership and Attributes

Lab 9.5 Monitoring Security Issues with SELinux

Chapter 10 Manage Local Storage: Essentials

Lab 10.1 Creating Partitions and Filesystems

Lab 10.2 Mounting Filesystems at Boot

Lab 10.3 Managing Swap Devices

Chapter 11 Manage Local Storage: Advanced Features

Lab 11.1 Managing Encrypted Filesystems

Lab 11.2 Configuring Logical Volumes

Lab 11.3 Administering Disk Quotas

Lab 11.4 Managing Hard and Soft Links

Chapter 12 Manage Network Storage

Lab 12.1 Configuring Samba

Lab 12.2 Administering NFS

Lab 12.3 Managing iSCSI

Chapter 13 Develop a Storage Security Policy

Lab 13.1 Backing Up a Filesystem

Table of Contents

Lab 13.2 Developing a Backup Security Policy

Part IV: Automation

Chapter 14 Crontab and At

Lab 14.1 Managing crontab

Lab 14.2 Configuring at Commands

Chapter 15 Scripting

Lab 15.1 Script Project #1

Lab 15.2 Script Project #2

Chapter 16 Common Automation Tasks

Lab 16.1 Script Project #3

Lab 16.2 Script Project #4

Chapter 17 Develop an Automation Security Policy

Lab 17.1 Securing crontab and at

Lab 17.2 Creating an Automation Security Policy

Part V: Networking

Chapter 18 Networking Basics

Lab 18.1 Exploring Networking Components

Chapter 19 Network Configuration

Lab 19.1 Understanding Network Configuration on CentOS

Lab 19.2 Understanding Network Configuration on Ubuntu

Chapter 20 Network Service Configuration: Essential Services

Lab 20.1 Configuring a BIND Server

Lab 20.2 Configuring a Postfix Server

Chapter 21 Network Service Configuration: Web Services

Lab 21.1 Configuring and Administering an Apache Server

Lab 21.2 Configuring a Proxy Server

Chapter 22 Connecting to Remote Systems

Lab 22.1 Configuring an FTP Server

Lab 22.2 Administering an SSH Server

Chapter 23 Develop a Network Security Policy

Lab 23.1 Administering Kernel Security Parameters

Lab 23.2 Securing a System with TCP Wrappers

Table of Contents

Lab 23.3 Configuring Network Time Protocol

Lab 23.4 Creating a Networking Security Policy

Part VI: Process and Log Administration

Chapter 24 Process Control

Lab 24.1 Managing System Processes

Lab 24.2 Displaying System Information

Chapter 25 System Logging

Lab 25.1 Managing Log Files

Lab 25.2 Configuring Log Rotation

Part VII: Software Management

Chapter 26 Red Hat-Based Software Management

Lab 26.1 Managing Software Packages with rpm

Lab 26.2 Managing Software Packages with yum

Chapter 27 Debian-Based Software Management

Lab 27.1 Managing Software Packages with dpkg

Lab 27.2 Managing Software Packages with apt

Chapter 28 System Booting

Lab 28.1 Configuring GRUB Security

Lab 28.2 Managing the Startup Process

Chapter 29 Develop a Software Management Security Policy

Lab 29.1 Exploring Common Vulnerabilities and Exposure Reports

Lab 29.2 Managing and Securing Legacy Services

Part VIII: Security Tasks

Chapter 30 Footprinting

Lab 30.1 Using Probing Tools

Lab 30.2 Scanning the Network

Chapter 31 Firewalls

Lab 31.1 Creating a Firewall to Protect a System

Chapter 32 Intrusion Detection

Lab 32.1 Creating an Intrusion Detection Security Plan

Chapter 33 Additional Security Tasks

Table of Contents

Lab 33.1 Configuring fail2ban

Lab 33.2 Encrypting Files with gpg