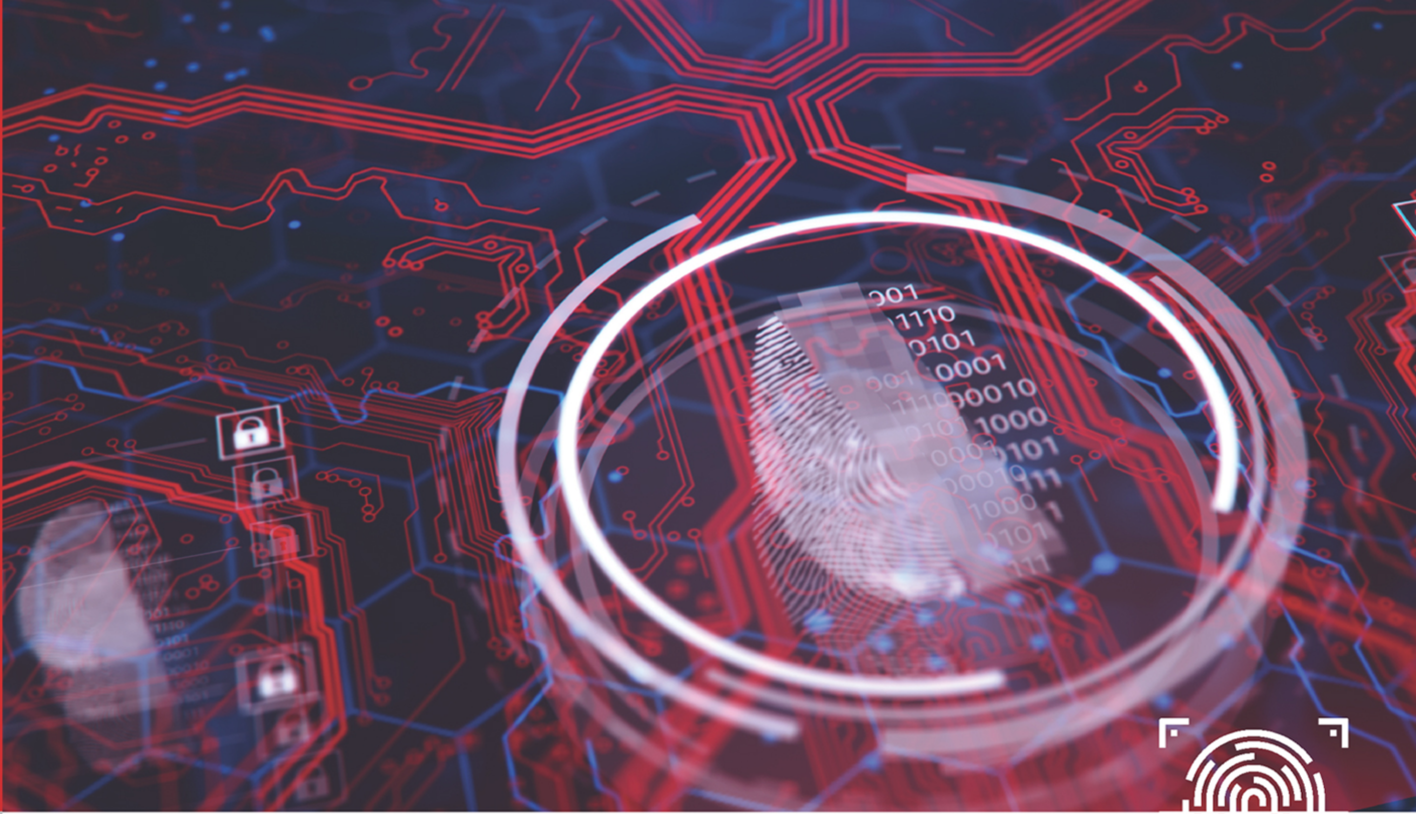
PEARSON IT CYBERSECURITY CURRICULUM



LINUX ESSENTIALS FOR CYBERSECURITY

WILLIAM "BO" ROTHWELL
DENISE KINSEY, PhD

Linux Essentials for Cybersecurity

William "Bo" Rothwell

Denise Kinsey

Pearson

Linux Essentials for Cybersecurity

Table of Contents

Cover

Title Page

Copyright Page

Table of Contents

Introduction

Part I: Introducing Linux

Chapter 1 Distributions and Key Components

Introducing Linux

Linux Distributions

Shells

GUI Software

Installing Linux

Which Distro?

Native or Virtual Machine?

Installing a Distro

Summary

Key Terms

Review Questions

Chapter 2 Working on the Command Line

File Management

The Linux Filesystem

Command Execution

The pwd Command

The cd Command

The ls Command

File Globbing

The file Command

The less Command

The head Command

Table of Contents

- The tail Command
- The mdkir Command
- The cp Command
- The mv Command
- The rm Command
- The rmdir Command
- The touch Command

Shell Features

- Shell Variables
- echo
- set
- unset
- The PS1 Variable
- The PATH Variable
- Environment Variables
- env
- Initialization Files
- Alias
- Command History
- History Variables
- The .bash_history File
- Redirecting Input and Output
- Piping
- Subcommands

Advanced Commands

- The find Command
- Regular Expressions
- The grep Command
- The sed Command
- Compression Commands
- The tar Command
- The gzip Command
- The gunzip Command
- The bzip2 Command
- The xz Command

Summary

- Key Terms

Table of Contents

Review Questions

Chapter 3 Getting Help

Man Pages

Man Page Components

Man Page Sections

Man Page Locations

Command Help Options

The help Command

The info Command

The /usr/share/doc Directory

Internet Resources

Summary

Key terms

Review Questions

Chapter 4 Editing Files

The vi Editor

What Is vim?

Essential vi Commands

Use Basic vi Modes

Entering the Insert Mode

Movement Commands

Repeater Modifiers

Undoing

Copying, Deleting, and Pasting

Finding Text

Find and Replace

Saving and Quitting

Expand Your vi Knowledge

Additional Editors

Emacs

gedit and kwrite

nano and joe

lime and bluefish

Summary

Key Terms

Review Questions

Table of Contents

Chapter 5 When Things Go Wrong

The Science of Troubleshooting

Step 1: Gathering Information

Step 2: Determine the Likely Cause

Step 3: Document Your Plan of Attack (POA)

Step 4: Perform the Actions

Steps 5 and 6: Is the Problem Solved?

Step 7: Are There Other Problems?

Step 8: Store the Documentation

Step 9: Prevent Future Problems

Notifying Users

Pre- and Post-login Messages

The /etc/issue File

The /etc/issue.net File

Additional Pre-login Messages

The /etc/motd File

Broadcasting Messages

The wall Command

The shutdown Command

Summary

Review Questions

Part II: User and Group Accounts

Chapter 6 Managing Group Accounts

What Are Groups Used For?

Primary versus Secondary Groups

The /etc/group File

Special Groups

User Private Groups

The /etc/gshadow File

Managing Groups

Creating Groups

Modifying Groups

Deleting Groups

Adding Users to Groups

Group Administrators

Summary

Table of Contents

Key Terms

Review Questions

Chapter 7 Managing User Accounts

The Importance of User Accounts

User Account Information

The /etc/passwd File

Special Users

The /etc/shadow File

Managing Users

Creating Users

Setting the Account Password

Using Defaults

Using Skel Directories

Modifying Users

Managing GECOS

Deleting Users

Restricted Shell Accounts

Network-Based User Accounts

Using su and sudo

Restricting User Accounts

PAM Categories

PAM Control Values

PAM Modules

Using PAM to Alter the Password Policy

Summary

Key Terms

Review Questions

Chapter 8 Develop an Account Security Policy

Introducing Kali Linux

Security Principles

Creating a Security Policy

Securing Accounts

Physical Security

Educating Users

Account Security

User Account Names

Table of Contents

Users with No Password

Preventing a User from Changing a Password

Application Accounts

Enabling Process Accounting

Avoiding Commands Being Run as the Superuser

Security Tools

The john and Johnny Tools

The hydra tool

Summary

Review Questions

Part III: File and Data Storage

Chapter 9 File Permissions

Standard Permissions

Viewing Permissions

Files Versus Directories

Changing Permissions

Default Permissions

Special Permissions

SUID

SGID

Sticky Bit

Access Control Lists (ACLs)

The mask Value

Default ACLs

Changing Ownership

chown

chgrp

File Attributes

Introduction to SELinux

Users Create Security Holes

Daemon Processes Create Security Holes

SELinux Essentials

Security Context

SELinux Conclusion

Summary

Key Terms

Table of Contents

Review Questions

Chapter 10 Manage Local Storage: Essentials

Filesystem Essentials

Partitions

Filesystems

Why So Many Partitions/Filesystems?

Which Partitions/Filesystems Should Be Created?

Filesystem Types

Managing Partitions

MBR

GPT

Creating MBR Partitions

Creating MBR Partitions

Creating Filesystems

Ext-Based Filesystem Tools

fsck.*

dumpe2fs

tune2fs

debugfs

Xfs-Based Filesystem Tools

xfsdump and xfsrestore

xfs_info

xfs_check and xfs_repair

Additional Filesystem Tools

du

df

Mounting Filesystems

The umount Command

The mount Command

Mounting Filesystems Manually

Problems Unmounting Filesystems

Mounting Filesystems Automatically

Device Descriptors

Mount Options

Mounting Removable Media

Swap Space

Creating Swap Devices

Table of Contents

Summary

Key Terms

Review Questions

Chapter 11 Manage Local Storage: Advanced Features

Encrypted Filesystems

Managing autofs

Logical Volume Manager

Logical Volume Manager Concepts

Advantages of LVM on a System with a Single Drive

LVM Essentials

Extents

Logical Volumes

Device Naming

Using Logical Volumes and Additional LVM Commands

Displaying LVM Information

Additional LVM Commands

Resizing Logical Volumes

LVM Snapshots

Disk Quotas

Setting Up a Disk Quota for a Filesystem

Editing, Checking, and Generating User Quota Reports

quotaon

edquota

quota

repquota

Hard and Soft Links

Why Use Links?

Creating Links

Displaying Linked Files

Summary

Key Terms

Review Questions

Chapter 12 Manage Network Storage

Samba

SAMBA Configuration

The [global] Section

Table of Contents

    - The [homes] Section
    - The [printers] Section
    - Custom Shares
    - SAMBA Server
    - SAMBA Accounts
    - Mapping Local Accounts
    - Accessing SAMBA Servers
    - Mounting SAMBA Shares
  - Network File System
    - Configuring an NFS Server
    - The /etc/exports File
    - User ID Mapping
    - NFS Server Processes
    - Understanding portmap
    - NFS Server Commands
    - Configuring an NFS Client
    - iSCSI
    - Target Configuration
    - Initiator Configuration
  - Summary
    - Key Terms
    - Review Questions
- Chapter 13 Develop a Storage Security Policy
  - Developing the Plan
  - Backing Up Data
    - Creating a Backup Strategy
    - What Needs to Be Backed Up?
    - How Often?
    - Full or Incremental?
    - Where Will the Backup Be Stored?
    - What Backup Tool Will Be Used?
    - Standard Backup Utilities
    - The dd Command
    - The tar Command
    - The rsync Command
    - Third-party Backup Utilities
    - Amanda

Table of Contents

Bacula

Summary

Key Terms

Review Questions

Part IV: Automation

Chapter 14 crontab and at

Using crontab

Configure User Access to the cron Service

/etc/crontab

/etc/anacrontab

Using at

atq

atrm

Configure User Access to at Services

Summary

Key Terms

Review Questions

Chapter 15 Scripting

Linux Programming

BASH Shell Scripting

Perl Scripting

Python Scripting

Basics of BASH Scripting

Conditional Expressions

Integer Comparisons

File Test Comparisons

Flow Control Statements

The while Loop

The for Loop

Loop Control

The case Statement

User Interaction

Using Command Substitution

Additional Information

Summary

Table of Contents

- Key Terms
- Review Questions

Chapter 16 Common Automation Tasks
- Exploring Scripts that Already Exist on Your System
  - The /etc/cron.* Directories
  - logrotate
  - man-db.cron
  - mlocate
  - Repositories
- Creating Your Own Automation Scripts
- Summary
  - Key Terms
  - Review Questions

Chapter 17 Develop an Automation Security Policy
- Securing crontab and at
- Securing BASH Scripts
  - Access to Scripts
  - Script Contents
  - Dealing with Data
  - Shell Settings
  - Shell Style
- Summary
  - Review Questions

Part V: Networking

Chapter 18 Networking Basics
- Network Terminology
- IPv4 Versus IPv6
- IPv4 Addresses
  - Determining a Network Address from an IP Address and Subnet
  - Private IP Addresses
- Common Protocol Suites
- Network Ports
- Summary
  - Key Terms
  - Review Questions

Table of Contents

Chapter 19 Network Configuration

Ethernet Network Interfaces

Displaying Ethernet Port Configurations

Changing Ethernet Port Settings

Network Configuration Tools

The arp Command

The route Command

The ip Command

The hostname Command

The host Command

The dig Command

The netstat Command

Persistent Network Configurations

The /etc/hostname File (Universal)

The /etc/hosts File (Universal)

The /etc/resolv.conf File (Universal)

The /etc/nsswitch.conf File (Universal)

The /etc/sysctl.conf File (Universal)

The /etc/sysconfig/network File (Red Hat)

The /etc/sysconfig/network-scripts/ifcfg-interface-name Files (Red Hat)

The /etc/network/interfaces File (Debian)

Network Troubleshooting Commands

The ping Command

The traceroute Command

The netcat Command

Access to Wireless Networks

The iwconfig Command

The iwlist Command

Summary

Key Terms

Review Questions

Chapter 20 Network Service Configuration: Essential Services

DNS Servers

Essential Terms

How Name Resolution Works

Basic BIND Configuration

Table of Contents

- The /etc/named.conf File
- The allow-query Setting
- Additional /etc/named.conf Settings

Zone Files

- Zone File Basics
- Zone File Entries in the /etc/named.conf File
- Zone File Syntax
- Zone Record Types
- The SOA Record Type
- The Address Record Type
- The Canonical Name Type
- The Name Server Record Type
- The Mail eXchange Record Type
- The Pointer Record Type
- Putting It All Together
- Slave BIND Servers
- Testing the DNS Server
- The dig Command

Securing BIND

- Sending BIND to Jail
- Creating the chroot Directory and Files
- Configuring named to Start in the Jail
- Split BIND Configuration
- Transaction Signatures
- The dnssec-keygen Command
- The dnssec-signzone Command

DHCP Server

- DHCP Configuration Basics
- The ddns-update-style and ignore client-updates Directives
- The subnet Directive
- Configuring Static Hosts
- DHCP Log Files

Email Servers

- SMTP Basics
- Configuring Postfix
- Postfix Configuration File
- Important Postfix Settings

Table of Contents

- Aliases
- Postfix Virtual Domains

Managing Local Email Delivery

- procmail Basics
- procmail Rules
- procmail Examples
- mbox and Maildir Formats

Remote Email Delivery

- IMAP and POP Essentials
- The Dovecot Server

Summary

- Key Terms
- Review Questions

Chapter 21 Network Service Configuration: Web Services

Apache Web Server

Basic Apache Web Server Configuration

- Starting the Apache Web Server
- Apache Web Server Log Files
- Enable Scripting

Apache Web Server Security

- Essential Settings
- User Authentication

Virtual Hosts

- Configuring IP-Based Virtual Hosts
- Configuring Name-Based Virtual Hosts

HTTPS

- SSL Essentials
- SSL Issues
- Self-Signing

SSL and Apache

- SSL Server Certificate
- Apache SSL Directives

Proxy Servers

- Tunneling Proxy
- Forward Proxy
- Reverse Proxy

Table of Contents

Squid Basics

Squid Access Rules

Built-In ACLs

Understanding the Squid Rules

Nginx Configuration

Client Configuration

Summary

Key Terms

Review Questions

Chapter 22 Connecting to Remote Systems

LDAP

Key LDAP Terms

The slapd.conf File

Customizing Your LDAP Domain

Configuring Logging

Configuring the Database Directory

Starting the LDAP Server

OpenLDAP Objects

OpenLDAP Schemas

OpenLDAP Database Changes

Using the ldapdelete Command

Using the ldapsearch Command

Using the ldappasswd Command

Connecting to an LDAP Server

FTP Servers

Configuring vsftpd

Anonymous FTP

Limiting User Accounts

Additional Settings

Connecting to an FTP server

Active versus Passive Mode

Secure Shell

Configuring the Secure Shell Server

Basic Configuration Settings

Settings That Affect User Access

Secure Shell Client Commands

The ssh_config File

Table of Contents

The ssh Command

The scp and sftp Commands

Advanced SSH Features

Summary

Key Terms

Review Questions

Chapter 23 Develop a Network Security Policy

Kernel Parameters

The /etc/sysctl.conf File

Ignoring ping Requests

Ignoring Broadcast Requests

Enabling TCP SYN Protection

Disabling IP Source Routing

TCP Wrappers

Network Time Protocol

Setting the System Clock Manually

Setting the System Time Zone Manually

Setting the System Date Using NTP

Summary

Key Terms

Review Questions

Part VI: Process and Log Administration

Chapter 24 Process Control

Viewing Processes

The ps Command

The pgrep Command

The top Command

The uptime Command

The free Command

Running Processes

Pausing and Restarting Processes

Killing Processes

The kill Command

The pkill Command

The killall Command

The xkill Command

Table of Contents

The nohup Command

Process Priority

The nice Command

The renice Command

Summary

Key Terms

Review Questions

Chapter 25 System Logging

Syslog

The syslogd Daemon

The /var/log Directory

The /etc/syslog.conf File

The /etc/rsyslog.conf File

Creating Your Own /etc/syslog.conf Entry

Adding an Entry

Using the logger Command

The logrotate Command

The /etc/logrotate.conf File

The journalctl Command

The /etc/systemd/journald.conf file

Summary

Key Terms

Review Questions

Part VII: Software Management

Chapter 26 Red HatBased Software Management

Red Hat Packages

How to Obtain Packages

The /var/lib/rpm Directory

Using the rpm Command

Listing rpm Information

Viewing Package Dependencies

Package Listing Tricks

Installing Packages with rpm

Before You Install That Package

Removing Packages with rpm

rpm2cpio

Table of Contents

- The yum Command
  - Repositories
  - Accessing a Repo
  - Creating a Repo
  - Using the yum Command
  - Displaying Package Information with yum
  - Software Groups
  - Installing Software with yum
  - Removing Software with yum
  - Using yum Plug-Ins
- Additional Tools
- Summary
  - Key Terms
  - Review Questions

Chapter 27 Debian-Based Software Management

- Managing Packages with dpkg
  - Listing Package Information with dpkg
  - Installing Software with dpkg
  - Reconfiguring Software with dpkg
  - Extracting Files from a Debian Package
  - Removing Packages with the dpkg Command
- Managing Packages with APT
  - APT Repositories
  - Creating a Source Repository
- Listing Package Information with APT Commands
  - Installing Packages with APT Commands
  - Removing Packages with APT Commands
  - Additional APT Features
- Summary
  - Key Terms
  - Review Questions

Chapter 28 System Booting

- Phases of the Boot Process
  - The BIOS/UEFI Phase
  - The Bootloader Phase
  - The Kernel Phase

Table of Contents

The Post-Kernel Phase

GRUB

Legacy GRUB Configuration

Changing Legacy GRUB During Boot

Booting to Single-User Mode in Legacy GRUB

Securing Legacy GRUB

GRUB 2 Configuration

Saving GRUB 2 Changes

GRUB 2 Titles

Booting to Single-User Mode in GRUB 2

Securing GRUB 2

Kernel Components

Kernel Documentation

Tweaking the Kernel

Kernel Images

Kernel Modules

Module Files

Listing Modules That Are Loaded

Loading Modules into Memory

Unloading Modules from Memory

Listing Module Information

The /proc/sys Filesystem

The init Phase

Configuring Systemd

Using Service Units

Using Target Units

Summary

Key Terms

Review Questions

Chapter 29 Develop a Software Management Security Policy

Ensuring Software Security

Keep Packages Up to Date

Consider Removing Unnecessary Packages

Ensure You Install from Trusted Sources

CVE

Distribution-Specific Security Alerts

xinetd

Table of Contents

Summary

Key Terms

Review Questions

Part VIII: Security Tasks

Chapter 30 Footprinting

Understanding Footprinting

Common Footprinting Tools

The nmap Command

The netstat Command

The lsof Command

The nc Command

The tcpdump Command

Additional Utilities

Kali Linux Utilities

Essential Information Gathering

DNS Analysis Tools

Host Identification Tools

OSINT Tools

Route Analysis Tools

Summary

Key Terms

Review Questions

Chapter 31 Firewalls

Introduction to Firewalls

Essentials of the iptables Command

Overview of Filtering Packets

Important Terms

Using iptables to Filter Incoming Packets

Filtering by Protocol

Multiple Criteria

Filtering Based on Destination

Changing the Default Policy

Revisiting the Original Rules

Saving the Rules

Using iptables to Filter Outgoing Packets

Table of Contents

Implementing NAT

Summary

Key Terms

Review Questions

Chapter 32 Intrusion Detection

Introduction to Intrusion Detection Tools

Determining If a Security Breach Has Occurred

Taking Action

Intrusion Detection Network Tools

The netstat Command

The nmap Command

The tcpdump Command

Intrusion Detection File Tools

Modifying the /etc/passwd and /etc/shadow Files to Create a Backdoor

Creating an SUID Program to Create a Backdoor

Incorporating File-Change Tools in the Intrusion Detection Plan

Additional Intrusion Detection Tools

Summary

Key Terms

Review Questions

Chapter 33 Additional Security Tasks

The fail2ban Service

OpenVPN

Configuring the Certificate Authority

Generating the VPN Server Certificate

Generating the VPN Client Certificate

Setting Up the Basic Server

Setting Up the Basic Client

gpg

Security Alert Services

Summary

Key Terms

Review Questions

Appendix A: Answers to Review Questions

Appendix B: Resource Guide

Table of Contents

Glossary

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

Index

Pearson