INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Security Strategies in Linux Platforms and Applications

THIRD EDITION

Ric Messier | Michael Jang

JONES & BARTLETT
LEARNING

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

World Headquarters Jones & Bartlett Learning
25 Mall Road
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

The content, statements, views, and opinions herein are the sole expression of the respective authors and not that of Jones & Bartlett Learning, LLC. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement or recommendation by Jones & Bartlett Learning, LLC and such reference shall not be used for advertising or product endorsement purposes. All trademarks displayed are the trademarks of the parties noted herein. *Security Strategies in Linux Platforms and Applications, Third Edition* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product.

There may be images in this book that feature models; these models do not necessarily endorse, represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious but are used for instructional purposes only.

25593-5

Production Credits
Vice President, Product Management: Marisa R. Urbano
Vice President, Content Strategy and Implementation: Christine Emerton
Director, Content Management: Donna Gridley
Manager, Content Strategy: Carolyn Pershouse
Product Director: Ray Chew
Technical Editor: Richard Blum
Content Strategist: Melissa Duffy
Content Coordinator: Mark Restuccia
Director, Project Management and Content Services: Karen Scott
Manager, Project Management: Jackie Reynen
Project Manager: Erin Bosco
Senior Digital Project Specialist: Angela Dooley
Director, Marketing: Andrea DeFronzo
Marketing Manager: Mark Adamiak
Content Services Manager: Colleen Lamy
VP, Manufacturing and Inventory Control: Therese Connell
Product Fulfillment Manager: Wendy Kilborn
Composition: Straive
Project Management: Straive
Cover Design: Briana Yates
Media Development Editor: Faith Brosnan
Rights & Permissions Manager: John Rusk
Rights Specialist: James Fortney
Cover Image (Title Page, Part Opener, Chapter Opener):
© John_Dakapu/Shutterstock
Printing and Binding: Gasch Printing

Library of Congress Cataloging-in-Publication Data

Names: Messier, Ric, author.
Title: Security strategies in Linux platforms and applications / Ric Messier.
Description: Third edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2024] | Includes bibliographical references and index. | Summary: "Incorporating real-world examples and exercises throughout, Security Strategies in Linux Platforms and Applications discusses every major aspect of security on a Linux system, including coverage of the latest Linux distributions and kernels. Written by industry experts, the text opens with a review of the risks, threats, and vulnerabilities associated with Linux as an operating system. Part 2 discusses how to take advantage of the layers of security available to Linux - user and group options, filesystems, and security options for important services. The text concludes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments"— Provided by publisher.
Identifiers: LCCN 2022019834 | ISBN 9781284255850 (paperback)
Subjects: LCSH: Linux. | Operating systems (Computers) | Computer security.
Classification: LCC QA76.76.O63 J385 2024 | DDC 005.8—dc23/eng/20220527
LC record available at https://lccn.loc.gov/2022019834

Library of Congress Cataloging-in-Publication Data

Library of Congress Cataloging-in-Publication Data unavailable at time of printing.

LCCN: 2019947448

6048

Printed in the United States of America
26 25 24 23 22 10 9 8 7 6 5 4 3 2 1

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© John_Dakapu/Shutterstock

Contents

Purpose of This Book xix

Acknowledgments xxiii

About the Authors xxv

PART ONE Is Linux Really Secure? 1

CHAPTER 1 **Security Threats to Linux 3**

The Origins of Linux 5

Security in an Open-Source World 7

Linux Distributions 9

The C-I-A Triad 10

Linux as a Security Device 12

Linux in the Enterprise 14

Recent Security Issues 16

CHAPTER SUMMARY 18

KEY CONCEPTS AND TERMS 18

CHAPTER 1 ASSESSMENT 19

CHAPTER 2 **Basic Components of Linux Security 21**

Linux Security Relates to the Kernel 22

- The Basic Linux Kernel Philosophy 23
- Basic Linux Kernels 23
- Distribution-Specific Linux Kernels 24
- Custom Linux Kernels 24
- Linux Kernel Security Options 27

Securing a System During the Boot Process 28

- Unified Extensible Firmware Interface (UEFI) 28
- Physical Security 29
- The Threat of the Live CD 29
- Boot Process Security 29
- More Boot Process Issues 30
- Virtual Physical Security 30

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Linux Security Issues Beyond the Basic Operating System 30

Service Process Security 31
Security Issues with the GUI 32

Linux User Authentication Databases 32

Protecting Files with Ownership, Permissions, and Access Controls 34

Firewalls and Mandatory Access Controls in a Layered Defense 35

Firewall Support Options 35
Mandatory Access Control Support 37

Protecting Networks Using Encrypted Communication 38

Tracking the Latest Linux Security Updates 39

Linux Security Updates for Regular Users 39
Linux Security Updates for Home Hobbyists 39
Linux Security Updates for Power Users 40
Security Updates for Linux Administrators 40
Linux Security Update Administration 41

The Effect of Virtualization on Security 41

Variations Between Distributions 42

A Basic Comparison: Red Hat and Ubuntu 43
More Diversity in Services 44

CHAPTER SUMMARY 46

KEY CONCEPTS AND TERMS 47

CHAPTER 2 ASSESSMENT 47

PART TWO Layered Security and Linux 49

CHAPTER 3 **Starting Off: Getting Up and Running 51**

Picking a Distribution 52

Picking a Delivery Platform 56

Physical System 57
Virtual Machines 58
Cloud Services 61
Infrastructure as a Service 61
Platform as a Service 63

Choosing a Boot Loader 63

Linux Loader 63
Grand Unified Boot Loader 64

Services 66

Runlevels 71
Wrappers 73

inetd and xinetd 74

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

CHAPTER SUMMARY 76
KEY CONCEPTS AND TERMS 77
CHAPTER 3 ASSESSMENT 77

CHAPTER 4 User Privileges and Permissions 79

The Shadow Password Suite 80
/etc/passwd 81
/etc/group 81
/etc/shadow 82
/etc/gshadow 83
Defaults for the Shadow Password Suite 84
Shadow Password Suite Commands 86
Available User Privileges 87
Securing Groups of Users 89
User Private Group Scheme 89
Create a Special Group 90
Configuring the Hierarchy of Administrative Privileges 91
Administrative Privileges in Services 92
The su and sg Commands 92
Options with sudo and /etc/sudoers 93
Basic Options in /etc/sudoers 93
More Detailed Options with /etc/sudoers 94
Use the sudo Command 95
Regular and Special Permissions 96
The Set User ID Bit 96
The Set Group ID Bit 97
The Sticky Bit 97
Tracking Access Through Logs 98
Authorization Log Options 99
Authorization Log Files 99
Pluggable Authentication Modules 99
The Structure of a PAM Configuration File 100
PAM Configuration for Users 102
Authorizing Access with the Polkit 102
How the Polkit Works 102
Polkit Concepts 103
Network User Verification Tools 103
NIS If You Must 104
LDAP Shares Authentication 105
Best Practices: User Privileges and Permissions 107

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

CHAPTER SUMMARY **108**
KEY CONCEPTS AND TERMS **109**
CHAPTER 4 ASSESSMENT **109**

CHAPTER 5 **Filesystems, Volumes, and Encryption** **111**

Filesystem Organization 112
- Filesystem Basics 112
- The Filesystem Hierarchy Standard 113
- Good Volume Organization Can Help Protect a System 116
- Read-Only Mount Points 119

How Options for Journals, Formats, and File Sizes Affect Security 120
- Partition Types 121
- The Right Format Choice 122
- Available Format Tools 123

Using Encryption 123
- Encryption Tools 123
- Encrypted Files 124
- Encrypted Partitions and Volumes 129

Local File and Folder Permissions 131
- Basic File Ownership Concepts 132
- Basic File-Permission Concepts 132
- Changing File Permissions 133

Networked File and Folder Permissions 135
- NFS Issues 135
- Samba/CIFS Network Permissions 136
- Network Permissions for the vsftp Daemon 137

Configuring and Implementing Quotas on a Filesystem 138
- The Quota Configuration Process 139
- Quota Management 140
- Quota Reports 141

How to Configure and Implement Access Control Lists on a Filesystem 142
- Configure a Filesystem for ACLs 142
- ACL Commands 143
- Configure Files and Directories with ACLs 143

Best Practices: Filesystems, Volumes, and Encryption 144

CHAPTER SUMMARY **145**
KEY CONCEPTS AND TERMS **146**
CHAPTER 5 ASSESSMENT **146**

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

CHAPTER 6 **Securing Services 149**

Starting a Hardened System 151

Service Management 157

- SysV Init 157
- Upstart 162
- Systemd 164

Hardening Services 165

Using Mandatory Access Controls 168

- Security Enhanced Linux 169
- AppArmor 170

Servers Versus Desktops 172

Protecting Against Development Tools 173

CHAPTER SUMMARY 175

KEY CONCEPTS AND TERMS 176

CHAPTER 6 ASSESSMENT 176

CHAPTER 7 **Networks, Firewalls, and More 179**

Services on Every TCP/IP Port 180

- Protocols and Numbers in /etc/services 181
- Protection by the Protocol and Number 182

Obscurity and the Open Port Problem 182

- Obscure Ports 183
- Opening Obscure Open Ports 183
- Obscurity by Other Means 183

Protect with TCP Wrapper 185

- What Services Are TCP Wrapped? 185
- Configure TCP Wrapper Protection 186

Packet-Filtering Firewalls 187

- Basic Firewall Commands 188
- Firewalld 199
- A Firewall for the DMZ 202
- A Firewall for the Internal Network 203

Alternate Attack Vectors 204

- Attacks Through Nonstandard Connections 204
- Attacks on Scheduling Services 206

Wireless-Network Issues 208

- Linux and Wireless Hardware 208

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Encrypting Wireless Networks 208
Bluetooth Connections 209

Security Enhanced Linux 209

The Power of SELinux 210
Basic SELinux Configuration 211
Configuration from the Command Line 211
The SELinux Administration Tool 213
The SELinux Troubleshooter 213
SELinux Boolean Settings 214

Setting Up AppArmor Profiles 217

Basic AppArmor Configuration 218
AppArmor Configuration Files 218
AppArmor Profiles 219
AppArmor Access Modes 220
Sample AppArmor Profiles 220
AppArmor Configuration and Management Commands 221

Best Practices: Networks, Firewalls, and TCP/IP Communications 221

CHAPTER SUMMARY 222

KEY CONCEPTS AND TERMS 223

CHAPTER 7 ASSESSMENT 223

CHAPTER 8 Networked Filesystems and Remote Access 225

Basic Principles for Systems with Shared Networking Services 226

Configure an NTP Server 227
Install and Configure a Kerberos Server 227
Basic Kerberos Configuration 228
Additional Kerberos Configuration Options 230

Hardening NFS as If It Were Local 231

Configure NFS Kerberos Tickets 231
Configure NFS Shares for Kerberos 232

Keeping vsftp Very Secure 232

Configuration Options for vsftp 232
Additional vsftp Configuration Files 234

Linux as an Alternative Windows Server 234

Samba Global Options 235
Samba as a Primary Domain Controller 240

Making Sure SSH Services Remain Protected 241

The SSH Server 241
The SSH Client 244
Create a Secure Shell Passphrase 244

Basic Principles of Encryption on Networks 246

Host-to-Host IPSec 247
Network-to-Network IPSec 249

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Helping Users Who Must Use Telnet 250
Securing Modem Connections 250
The Basics of RADIUS 251
RADIUS Configuration Files 251
Moving Away from Cleartext Access 251
The Simple rsync Solution 251
Email Clients 253
Best Practices: Networked Filesystems and Remote Access 254
CHAPTER SUMMARY 256
KEY CONCEPTS AND TERMS 256
CHAPTER 8 ASSESSMENT 257

CHAPTER 9 Networked Application Security 259
Options for Secure Websites with Apache 260
The LAMP Stack 261
Apache Modules 263
Security-Related Apache Directives 265
Configure Protection on a Website 269
Adding Encryption to Your Website 269
Configure a Certificate Authority 269
mod_security 271
Apache as a Reverse Proxy 273
Working with Squid 274
Basic Squid Configuration 274
Security-Related Squid Directives 276
Limit Remote Access with Squid 276
Protecting DNS Services with BIND 277
The Basics of DNS on the Internet 277
DNS Network Configuration 277
Secure BIND Configuration 278
A BIND Database 279
DNS Targets to Protect 279
Domain Name System Security Extensions 280
Mail Transfer Agents 281
Open Source sendmail 282
The Postfix Alternative 284
Dovecot for POP and IMAP 286
More Email Services 286
Using Asterisk 286
Basic Asterisk Configuration 287
Security Considerations with Asterisk 288
Limiting Printers 289
Printer Administrators 289

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Shared Printers 289
Remote Administration 290
The CUPS Administrative Tool 290
Protecting Time Services 291
Best Practices: Networked Application Security 292
CHAPTER SUMMARY 293
KEY CONCEPTS AND TERMS 293
CHAPTER 9 ASSESSMENT 294

CHAPTER 10 Kernel Security Risk Mitigation 297
Distribution-Specific Functional Kernels 298
Kernels by Architecture 298
Kernels for Different Functions 299
The Stock Kernel 301
Kernel Numbering Systems 301
Production Releases and More 302
Download the Stock Kernel 302
Stock Kernel Patches and Upgrades 303
Managing Security and Kernel Updates 304
Stock Kernel Security Issues 304
Distribution-Specific Kernel Security Issues 305
Installing an Updated Kernel 305
Development Software for Custom Kernels 306
Red Hat Kernel Development Software 307
Ubuntu Kernel Development Software 307
Kernel-Development Tools 308
Before Customizing a Kernel 308
Start the Kernel Customization Process 308
Kernel-Configuration Options 310
Building Your Own Hardened Kernel 316
Download Kernel Source Code 317
Download Ubuntu Kernel Source Code 317
Download Red Hat Kernel Source Code 317
Install Required Development Tools 317
Navigate to the Directory with the Source Code 318
Compile a Kernel on Ubuntu Systems 319
Compile a Kernel on Red Hat Systems 319
Compile a Stock Kernel 319
Install the New Kernel and More 319
Check the Boot Loader 320
Test the Result 320
Increasing Security Using Kernels and the /proc/ Filesystem 320
Don’t Reply to Broadcasts 321
Protect from Bad ICMP Messages 321

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Protect from SYN Floods 321
Activate Reverse Path Filtering 322
Close Access to Routing Tables 322
Avoid Source Routing 322
Don’t Pass Traffic Between Networks 323
Log Spoofed, Source-Routed, and Redirected Packets 323
Best Practices: Kernel Hardening 324
CHAPTER SUMMARY 325
KEY CONCEPTS AND TERMS 325
CHAPTER 10 ASSESSMENT 326

PART THREE Building a Layered Linux Security Strategy 327

CHAPTER 11 **Managing Security Alerts and Updates 329**
Keeping Up with Distribution Security 330
Red Hat Alerts 331
Red Hat Enterprise Linux 331
Rocky Linux 331
Fedora Core Linux 332
Ubuntu Alerts 332
Keeping Up with Application Security 333
GNOME Desktop Environment 334
Web Browsers 334
Adobe Applications 335
Service Applications 335
Antivirus Options for Linux Systems 337
The Clam AntiVirus System 338
SpamAssassin 339
Detecting Other Malware 339
Endpoint Security for Linux Systems 340
Using Bug Reports 340
Ubuntu’s Launchpad 340
Red Hat’s Bugzilla 341
Application-Specific Bug Reports 342
Security in an Open-Source World 344
The Institute for Security and Open Methodologies 344
The National Security Agency 345
The Free Software Foundation 345
User Procedures 345
Deciding Between Automated Updates or Analyzed Alerts 346
Do You Trust Your Distribution? 346
Do You Trust Application Developers? 347

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Do You Trust Service Developers? 347

Linux Patch Management 348

Standard dnf Updates 348
Updates on Fedora 349
Updates on Red Hat Enterprise Linux 350
Standard apt-* Updates 350

Options for Update Managers 352

Configuring Automated Updates 352
Automatic Red Hat Updates 353
Pushing or Pulling Updates 354
Local or Remote Repositories 354
Configuring a Local Repository 355

Commercial Update Managers 356

The Red Hat Network 356
Canonical Landscape 357
Micro Focus' ZENworks 358

Open-Source Update Managers 358

Various apt-* Commands 358
Various dnf commands 359
Red Hat Spacewalk 361

Best Practices: Security Operations Management 361

CHAPTER SUMMARY 362

KEY CONCEPTS AND TERMS 362

CHAPTER 11 ASSESSMENT 363

CHAPTER 12 Building and Maintaining a Security Baseline 365

Configuring a Simple Baseline 366

A Minimal Red Hat Baseline 367
A Minimal Ubuntu Baseline 369

Read-Only or Live Bootable Operating Systems 369

Appropriate Read-Only Filesystems 370
Live CDs and DVDs 371

Keeping the Baseline Up to Date 371

A Gold Baseline 371
Baseline Backups 374

Monitoring Local Logs 374

The System and Kernel Log Services 374
Logging with journald 377
Logs from Individual Services 377

Consolidating and Securing Remote Logs 379

Default rsyslog Configuration 379
The Standard rsyslog Configuration File 380

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Identifying a Baseline System State 382

Collect a List of Packages 383
Compare Files, Permissions, and Ownership 383
Define the Baseline Network Configuration 383
Collect Runtime Information 385

Checking for Changes with Integrity Scanners 385

Tripwire 386
Advanced Intrusion Detection Environment 387

Best Practices: Building and Maintaining a Secure Baseline 388

CHAPTER SUMMARY 389

KEY CONCEPTS AND TERMS 389

CHAPTER 12 ASSESSMENT 389

CHAPTER 13 Testing and Reporting 391

Testing Every Component of a Layered Defense 392

Testing a Firewall 393
Testing Various Services 393
Testing Passwords 397
Testing Mandatory Access Control Systems 397

Checking for Open Network Ports 397

The `telnet` Command 398
The `netstat` Command 398
The `lsof` Command 402
The `nmap` Command 402

Running Integrity Checks of Installed Files and Executables 408

Verifying a Package 409
Performing a Tripwire Check 410
Testing with the Advanced Intrusion Detection Environment 411

Ensuring That Security Does Not Prevent Legitimate Access 414

Reasonable Password Policies 414
Allowing Access from Legitimate Systems 416

Monitoring Virtualized Hardware 417

Virtual Machine Hardware 417
Virtual Machine Options 417
Using Virtual Machines on Linux 418

Standard Open-Source Security-Testing Tools 419

Snort 420
Netcat and the nc Command 422

Vulnerability Scanners for Linux 423

Nessus 423
OpenVAS 425
Nexpose 425

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Where to Install Security-Testing Tools 427
Hint: Not Where Attackers Can Use Them Against You 427
Some Tools Are Already Available on Live CDs 428
Other Distributions 429
Best Practices: Testing and Reporting 431
CHAPTER SUMMARY 432
KEY CONCEPTS AND TERMS 432
CHAPTER 13 ASSESSMENT 432

CHAPTER 14 Detecting and Responding to Security Breaches 435
Performing Regular Performance Audits 436
The Basic Tools: ps and top 437
The System Status Package 438
For Additional Analysis 438
Making Sure Users Stay Within Secure Limits 439
Appropriate Policies 440
Education 441
User Installation of Problematic Services 441
Logging Access into the Network 442
Identifying Users Who Have Logged In 442
System Authentication Logs 443
Monitoring Account Behavior for Security Issues 443
Downloaded Packages and Source Code 443
Executable Files 444
Creating an Incident Response Plan 444
Increased Vigilance 445
Should You Leave the System On? 446
Acquiring the Memory Contents 447
Having Live Linux CDs Ready for Forensics Purposes 450
Helix Live Response 450
SANS Investigative Forensics Toolkit 452
Digital Evidence and Forensics Toolkit 452
Build Your Own Media 452
Forensic Live Media 452
When You Put Your Plan into Action 453
Confirming the Breach 454
Identifying Compromised Systems 454
Having Replacement Systems in Place 455
Secure Backup and Recovery Tools 455
Disk Images for Later Investigation 455
The `rsync` Command 456
Mount Encrypted Filesystems 457

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

The Right Way to Save Compromised Data as Evidence 458

Basic Principles for Evidence 458
Remembering the Volatile Data 458
Preserving the Hard Disks 458

Disaster Recovery from a Security Breach 459

Determining What Happened 459
Prevention 460
Replacement 460

How and When to Share with the Open-Source Community 460

If the Security Issue Is Known… 460
If the Security Issue Has Not Been Reported… 461

Best Practices: Security Breach Detection and Response 461

CHAPTER SUMMARY 462

KEY CONCEPTS AND TERMS 463

CHAPTER 14 ASSESSMENT 463

CHAPTER 15 Best Practices and Emerging Technologies 465

Maintaining a Gold Baseline 466

Monitoring Security Reports 467
Working Through Updates 467
Recalibrating System Integrity 467

Ensuring Availability with Redundancy 468

A Gold Physical Baseline 468
A Gold Virtual Baseline Host 468

Identifying Your Support Options 470

Red Hat Support Options 471
Canonical Support Options 471
Open-Source Community Support 472

Checking Compliance with Security Policies 472

User Security 472
Administrator Security 473

Keeping the Linux Operating System Up to Date 473

Baseline Updates 474
Functional Bugs 474
New Releases 474

Keeping Distribution-Related Applications Up to Date 475

Server Applications 476
Desktop Applications 477

Managing Third-Party Applications 477

Licensing Issues 477
Support Issues 478

Sharing Problems and Solutions with the Community 479

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Which Community? 480
Sharing with Developers 480
Sharing on Mailing Lists 481
Testing New Components Before Putting Them into Production 481
Testing Updates 482
Documenting Results 482
Beta Testing 483
Keeping Up with Security on Your Systems 483
A New Firewall Command 483
More Mandatory Access Controls 483
Penetration-Testing Tools 484
Single Sign-On 485
Incident Response 485
CHAPTER SUMMARY 486
KEY CONCEPTS AND TERMS 487
CHAPTER 15 ASSESSMENT 487
APPENDIX A Answer Key 489
APPENDIX B Standard Acronyms 491
Glossary of Key Terms 495
References 509
Index 515

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

To my beautiful wife, Donna,
who has made life worth living again
—Michael Jang

To my wife, partner, and friend, Robin,
who opened my world
—Ric Messier

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© John_Dakapu/Shutterstock

Purpose of This Book

This book is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (*www.jblearning.com*). Designed for courses and curriculums in IT security, cybersecurity, information assurance, and information systems security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information-security principles packed with real-world applications and examples. Authored by professionals experienced in information systems security, they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow as well.

Security Strategies in Linux Platforms and Applications, Third Edition covers major aspects of security on a Linux system. The first part of this book describes the risks, threats, and vulnerabilities associated with Linux as an operating system. Linux is a common operating system used for Internet infrastructure. As a result, a big focus for this book is on implementing strategies that you can use to protect your system implementations, even in cases where they are public facing. To that end, this book uses examples from two of the major distributions built for the server: Red Hat Enterprise Linux and Ubuntu (Server Edition).

With Linux, security is much more than just firewalls and permissions. Part Two of the book shows you how to take advantage of the layers of security available to Linux—user and group options, filesystems, and security options for important services, as well as the security modules associated with Application Armor (AppArmor) and Security Enhanced Linux (SELinux). It also covers encryption options where available.

The final part of this book explores the use of both open source and proprietary tools when building a layered security strategy for your Linux operating system environments. With these tools, you can define a system baseline, audit the system state, monitor system performance, test network vulnerabilities, detect security breaches, and more. You will also learn basic practices associated with security alerts and updates, which are just as important.

As with any operating system, a Linux implementation requires strategies to harden it against attack. Linux is based on another operating system with a very long history, and it inherits the lessons learned over that history as well as some of the challenges. With Linux, you get a lot of eyes looking at the programs, which many consider to be a benefit of using open source programs and operating systems. While there are advantages, however, there are risks associated as well. Fortunately, a large community is built around improving Linux and the various software packages that go into it. This includes the National Security Agency, which initially developed a set of security extensions that has since been implemented into the Linux kernel itself.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

When you are finished with this book, you will understand the importance of custom firewalls, restrictions on key services, golden baseline systems, and custom local repositories. You will even understand how to customize and recompile the Linux kernel. You will be able to use open source and commercial tools to test the integrity of various systems on the network. The data you get from such tools will identify weaknesses and help you create more secure systems.

Learning Features

The writing style of this book is practical and conversational. Each chapter begins with a statement of learning objectives. Step-by-step examples of information security concepts and procedures are presented throughout the text. Illustrations are used both to clarify the material and to vary the presentation. The text is sprinkled with notes, tips, FYIs, warnings, and sidebars to alert the reader to additional helpful information related to the subject under discussion. Chapter assessments appear at the end of each chapter, with solutions provided in the back of the book.

Throughout this book are references to commands and directives. They may be included in the body of a paragraph in a monospaced font, like this: `apt-get update`. Other commands or directives may be indented between paragraphs, like the directive shown here:

```
deb http://us.archive.ubuntu.com/ubuntu/ lucid main restricted
```

When a command is indented between paragraphs, it's meant to include a Linux command line prompt. You will note two different prompts in the book. The first prompt is represented with a `$`. As shown here, it represents the command-line prompt from a regular user account:

```
$ ls -ltr > list_of_files
```

The second prompt is represented by a `#`. As shown here, it represents the command-line prompt from a root administrative account:

```
# /usr/sbin/apachectl restart
```

Sometimes, the command or directive is so long, it has to be broken into multiple lines due to the formatting requirements of this book. Line wraps are indicated by a curved arrow, as is shown at the start of what looks like the second line of the `iptables` command. It is just a continuation arrow, which would be typed as a continuous command on the command line or an appropriate configuration file.

```
iptables -A RH-Firewall-1-INPUT -i eth0 -s 10.0.0.0/8→
➥-j LOG --log-prefix “Dropped private class A addresses”.
```

Chapter summaries are included in the text to provide a rapid review of the material and to help students understand the relative importance of the concepts presented.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Audience

The material is suitable for undergraduate or graduate computer science majors or information science majors, students at a two-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge. It assumes basic knowledge of Linux administration at the command-line interface.

New to This Edition

While much of Linux remains the same, because it's based on Unix, which has worked much the same for decades, there have been changes in distributions and certainly current versions of common applications have changed. This edition covers any necessary updates to common applications used in Linux.

Most importantly, there have been shake-ups in the space of Linux distributions. For years now, and in the past two editions of this book, CentOS has been the free, binary-identical version of Red Hat Enterprise Linux. This has made CentOS a downstream implementation of Red Hat Enterprise Linux. This has changed in the last year, however. CentOS is now an upstream distribution of Red Hat Enterprise Linux. CentOS Stream is still a Linux distribution, but you won't find the same features or reliability as you would with Red Hat Enterprise Linux since Stream is more of a testing distribution to validate changes. Instead, Rocky Linux is available as a binary-identical implementation of Red Hat Enterprise Linux. This is not widely recognized as yet, though, so there are still some challenges to using Rocky Linux.

Finally, there are some changes to how to implement virtual private networks (VPNs) with Linux since the package described in previous editions of this book, Racoon, is no longer supported. This is a problem with open-source software packages. Sometimes the development team doesn't have enough support, they can't keep up with changes, or they lose interest. This can end up making a piece of software defunct or unsupported. Given the needed integration with the kernel for something like a VPN, application development has to keep up with kernel development. In this edition, the package covered is LibreSwan rather than Racoon.

We also cover some additional security-oriented Linux distributions like Parrot OS. This is a general purpose Linux distribution that focuses on including a large number of software packages that would be used by a security professional, particularly someone who was doing security testing.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© John_Dakapu/Shutterstock

Acknowledgments

Writing any book is a process. Revising an existing book for a second edition is also a process. It takes a team of people to get from conception to completion. Thanks to Melissa for helping me get this to the goal line, Robin for supporting me, and, as always, my agent Carole for all she has done for me.

Mostly, I'd like to acknowledge all those people who jump into things without any idea what they are getting themselves into. This fearlessness is the best way to jump into something new and guarantee that you are going to learn a lot. Try it sometime if you haven't already.

Ric Messier

I would like to thank Jones & Bartlett Learning and David Kim of Security Evolutions for the opportunity to write this book and be a part of the Information Systems Security & Assurance Series project. This book required a more substantial team effort than ordinary book projects.

In addition, I acknowledge the gracious help of Billy Austin of the SAINT corporation, along with Mike Johnson of AccessData with respect to their products. The author also acknowledges the fortitude of Linux security professionals everywhere, white-hat hackers at heart who have to deal with cultural biases from the mainstream security community along with the legitimate fears of the open-source community.

Most importantly, I could not do what I do without the help and support of my wife, Donna. She makes everything possible for me.

Michael Jang

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© John_Dakapu/Shutterstock

About the Authors

RIC MESSIER has been working with Unix and Unix-like operating systems since the mid-1980s. In the intervening decades, he has done system administration, network engineering, penetration testing, and programming; developed managed security services; and worked in operations security and a number of other jobs in between.

Ric is a security professional who has worked with a number of companies from large Internet service providers to small software companies. He has run a small networking and security consulting practice for the last several years. Additionally, he has taught courses at both the graduate and undergraduate level. Currently, in addition to writing books and recording training videos, he is a Principal Consultant with Mandiant.

MICHAEL JANG is a full-time writer, specializing in Linux and related certifications. His experience with computers dates back to the days of badly shuffled punch cards. He has written books such as *RHCE Red Hat Certified Engineer Study Guide*, *LPIC-1 In Depth*, *Ubuntu Server Administration*, and *Linux Annoyances for Geeks*. He is also the author of numerous video courses and teaches preparation courses on Red Hat certification.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.