INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES
ISSA
Security Strategies in Linux Platforms and Applications
THIRD EDITION
Ric Messier | Michael Jang
ACCESS CODE INSIDE
NAVIGATE eBOOK

TRANSITION GUIDE TO

Security Strategies in Linux Platforms and Applications

THIRD EDITION

Ric Messier and Michael Jang

Paperback with Navigate eBook Access
ISBN: 978-1-284-25585-0 | 500 pages | © 2023

Navigate eBook Access Only
ISBN: 978-1-284-25574-4 | © 2023

This transition guide serves to outline the updates and new content found in ***Security Strategies in Linux Platforms and Applications, Third Edition*** by Ric Messier and Michael Jang.

SUMMARY

The third edition of ***Security Strategies in Linux Platforms and Applications*** covers every major aspect of security on a Linux system. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk readers through the fundamentals of security strategies related to the Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion of the risks, threats, and vulnerabilities associated with Linux as an operating system using current examples and cases. 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 book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments.

FEATURES AND BENEFITS

- Mapped to Linux+ that spans Linux Essentials and Linux Security
- Accounts for the latest Linux distributions and kernels, including end of life for CentOS
- Covers new Linux-based technologies and security strategies
- Discusses the Microsoft acquisition of Red Hat and rise of commercialized Open Source
- Coverage of virtualization, including coverage of Docker and other sandboxing technologies like Firejai

APPLICABLE COURSES

- Linux Operating Systems
- Introduction to UNIX/ Linux
- Linux Operating System Security
- Linux Administration
- Securing Linux Systems
- Linux Networking and Security

INSTRUCTOR RESOURCES

- Instructor's Guide
- Syllabus
- PowerPoints
- Handouts
- Course Project
- Test Bank
- Mapping Guides

Continues on next page.

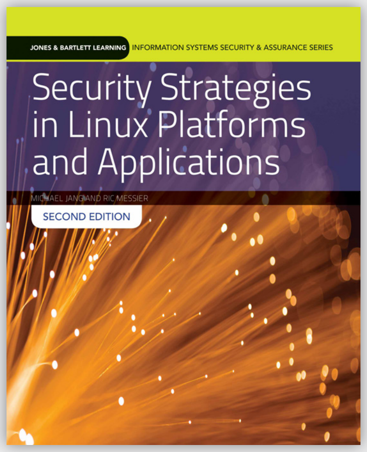
TRANSITION GUIDE TO

Security Strategies in Linux Platforms and Applications

THIRD EDITION

CHAPTER OUTLINE

This chapter outline has been created to help you easily transition to the third edition.


JONES & BARTLETT LEARNING
INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES
Security Strategies in Linux Platforms and Applications
MICHAEL JANG AND RIC MESSIER
SECOND EDITION

SECOND EDITION

CHAPTER 1 Security Threats to Linux

CHAPTER 2 Basic Components of Linux Security

CHAPTER 3 Basic Security: Facilities Through the Boot Process

CHAPTER 4 User Privileges and Permissions

CHAPTER 5 Filesystems, Volumes, and Encryption

CHAPTER 6 Every Service Is a Potential Risk

CHAPTER 7 Networks, Firewalls, and More

CHAPTER 8 Networked Filesystems and Remote Access

CHAPTER 9 Networked Application Security

CHAPTER 10 Kernel Security Risk Mitigation

CHAPTER 11 Managing Security Alerts and Updates

CHAPTER 12 Building and Maintaining a Security Baseline

CHAPTER 13 Testing and Reporting

CHAPTER 14 Detecting and Responding to Security Breaches

CHAPTER 15 Best Practices and Emerging Technologies

ISSA
INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES
Security Strategies in Linux Platforms and Applications
THIRD EDITION
Ric Messier | Michael Jang
ACCESS CODE INSIDE
NAVIGATE eBOOK

THIRD EDITION

CHAPTER 1 Security Threats to Linux

CHAPTER 2 Basic Components of Linux Security

CHAPTER 3 Starting Off: Getting Up and Running

CHAPTER 4 User Privileges and Permissions

CHAPTER 5 Filesystems, Volumes, and Encryption

CHAPTER 6 Securing Services

CHAPTER 7 Networks, Firewalls, and More

CHAPTER 8 Networked Filesystems and Remote Access

CHAPTER 9 Networked Application Security

CHAPTER 10 Kernel Security Risk Mitigation

CHAPTER 11 Building a Layered Linux Security Strategy

CHAPTER 12 Building and Maintaining a Security Baseline

CHAPTER 13 Testing and Reporting

CHAPTER 14 Detecting and Responding to Security Breaches

CHAPTER 15 Best Practices and Emerging Technologies

Continues on next page.

Jones & Bartlett Learning | 25 Mall Road | Burlington, MA | 01803
www.jblearning.com | phone: 1-800-832-0034 | fax: 978-443-8000

Source Code: Messier3eTG

TRANSITION GUIDE TO

Security Strategies in Linux Platforms and Applications

THIRD EDITION

KEY CHAPTER-BY-CHAPTER UPDATES

The following is a summary of key updates to the third edition, by chapter.

Across the board, all references to the versions of both distributions and kernels were updated. Previous versions included a suggestion that a root shell was used have been removed. It was in place before to indicate where root privileges were needed. As it's never a good practice to have a root shell, all command line examples that require root permissions now are shown with a regular user shell prompt and the use of sudo. The change in the purpose of CentOS and the emergence of Rocky Linux as a CentOS replacement is reflected where it is relevant. There are details about new security-oriented distributions.

This highlights significant changes on a chapter by chapter basis, since the changes may not be as noticeable in the table of contents

CHAPTER 1 Security Threats to Linux

- Updated statistics related to Linux usage
- Updated information related to Linux distributions
- Added information about Rocky Linux distribution
- **NEW** information about using Linux as a Security Information and Event Management system

CHAPTER 2 Basic Components of Linux Security

- Updated to reflect changes in the kernel development process
- Includes changes up to the 5.x series of the Linux kernel
- Updated secure boot instructions
- Updated Linux security options in the kernel

CHAPTER 3 Starting Off: Getting Up and Running

- Updated information about Linux distributions and changes to package management
- Updated discussion about Linux for virtualization
- Added information about using Linux in the cloud
- Updated details about the use of GRUB2 as a boot loader
- Removed most references to LILO, since it is no longer supported on modern systems

CHAPTER 4 User Privileges and Permissions

- Updated discussion around password hashing based on changes to the way Linux handles passwords since the last edition
- Updated to reflect changes in security directives in login.defs
- **NEW** details around the use of private groups
- Updated Pluggable Authentication Modules (PAM) configuration settings
- Updated polkit information due to changes in how it is used
- New details about how to create self-signed certificates

CHAPTER 5 Filesystems, Volumes, and Encryption

- Added new directories for the Filesystem Hierarchy Standard (FHS)
- Enhanced discussion about the /proc filesystem
- Updated all instructions related to encrypting files and filesystems
- Updated home directory encryption details

CHAPTER 6 Securing Services

- Updated details around multitasking
- Changed all details related to how package management works and the tools used
- Added instructions for the use of dnf, which has been added to Red Hat Linux-based distributions
- Updated service management instructions
- Updated instructions on the use of SELinux
- Updated AppArmor details
- Updated discussion on the use of development tools like Python

CHAPTER 7 Networks, Firewalls, and More

- Extensively revised discussion of the use of obscurity to reflect more modern approaches
- Updated details about the use of service banners
- Updated information related to the use of firewalls in different Linux distributions
- Added details about the use of IPv6 with firewalls
- Updated details about ufw and firewalld

Continues on next page.

TRANSITION GUIDE TO

Security Strategies in Linux Platforms and Applications

THIRD EDITION

CHAPTER 8 Networked Filesystems and Remote Access

- Updated details about NTP servers
- Updated details about Samba servers
- Updated details for SSH servers
- Removed old IPSec details because of a non-existent package
- Added new details about implementing IPSec with Linux

CHAPTER 9 Networked Application Security

- Updated details related to Apache server and the use of Nginx as an alternative web server
- Changed references about MySQL to include MariaDB
- Added the use of Apache as a Reverse Proxy to the Apache Web server section
- Changed the details about NTP servers to include updated packages in use with different distributions

CHAPTER 10 Kernel Security Risk Mitigation

- Extensively updated kernel options as a result of significant changes to kernel configuration settings
- Updated kernel package names based on changes to distributions
- Updated all usage to new kernel versions
- Updated instructions related to Red Hat kernel source downloads

CHAPTER 11 Building a Layered Linux Security Strategy

- Updated to reflect significant changes in the purpose of the CentOS Linux distribution
- Added information about Rocky Linux
- Updated details about the long-term stability options for distributions
- Updated details about the GNOME Desktop Environment
- Added a section on the use of Endpoint Detection and Response (EDR) for Linux systems
- Updated information related to filing bug reports with different projects
- Updated references to package management utilities

CHAPTER 12 Building and Maintaining a Security Baseline

- Updated directions on interrupting the Linux boot process
- Updated installation of Linux distributions to reflect changes to the distributions

CHAPTER 13 Testing and Reporting

- Added discussion about the NIST CSF related to developing a good defensive strategy
- Updated all utility instructions to reflect any changes in names or syntax
- Added more details about validating configurations for services
- Updated information about nmap scripting and the number of scripts currently available
- Updated guidance related to passwords
- Updated information about the use of virtual machines
- Updated details about different vulnerability scanners available for Linux

CHAPTER 14 Detecting and Responding to Security Breaches

- Added more details to guidance related to incident response
- Updated details where relevant

CHAPTER 15 Best Practices and Emerging Technologies

- Updated guidance related to what is necessary for using kvm as a virtualization host
- Updated support details for Canonical

JONES & BARTLETT LEARNING
www.jblearning.com

Jones & Bartlett Learning | 25 Mall Road | Burlington, MA | 01803
www.jblearning.com | phone: 1-800-832-0034 | fax: 978-443-8000

Source Code: Messier3eTG