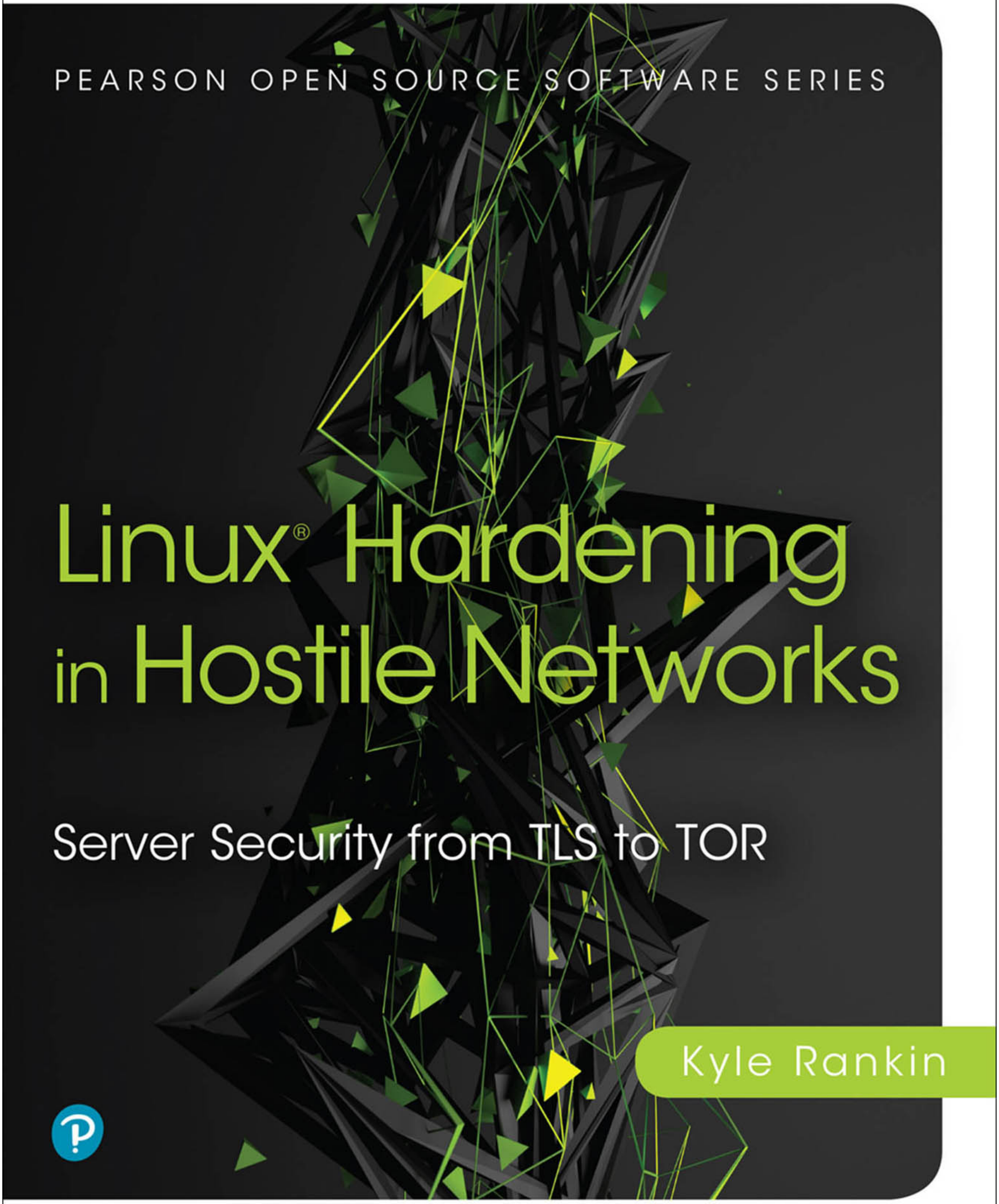

PEARSON OPEN SOURCE SOFTWARE SERIES

Linux® Hardening in Hostile Networks

Server Security from TLS to TOR

Kyle Rankin

Contents

Foreword **xiii**

Preface **xv**

Acknowledgments **xxiii**

About the Author **xxv**

1 Overall Security Concepts **1**

Section 1: Security Fundamentals **1**

- Essential Security Principles **2**
- Basic Password Security **4**

Section 2: Security Practices Against a Knowledgeable Attacker **10**

- Security Best Practices **10**
- Password-Cracking Techniques **13**
- Password-Cracking Countermeasures **16**

Section 3: Security Practices Against an Advanced Attacker **20**

- Advanced Password-Cracking Techniques **20**
- Advanced Password-Cracking Countermeasures **22**

Summary **24**

2 Workstation Security **25**

Section 1: Security Fundamentals **25**

- Workstation Security Fundamentals **25**
- Web Security Fundamentals **27**
- Introduction to Tails **29**
- Download, Validate, and Install Tails **29**
- Use Tails **30**

Section 2: Additional Workstation Hardening **33**

- Workstation Disk Encryption **33**
- BIOS Passwords **33**
- Tails Persistence and Encryption **34**

Section 3: Qubes **37**

- Introduction to Qubes **38**
- Qubes Download and Installation **41**
- The Qubes Desktop **43**
- An AppVM Compartmentalization Example **46**

Split GPG **49**

USB VM **50**

Summary **52**

3 Server Security 53

Section 1: Server Security Fundamentals **53**

Fundamental Server Security Practices **53**

SSH Configuration **54**

Sudo **55**

Section 2: Intermediate Server-Hardening Techniques **58**

SSH Key Authentication **58**

AppArmor **63**

Remote Logging **66**

Section 3: Advanced Server-Hardening Techniques **68**

Server Disk Encryption **68**

Secure NTP Alternatives **70**

Two-Factor Authentication with SSH **72**

Summary **74**

4 Network 75

Section 1: Essential Network Hardening **76**

Network Security Fundamentals **76**

Man-in-the-Middle Attacks **78**

Server Firewall Settings **79**

Section 2: Encrypted Networks **87**

OpenVPN Configuration **87**

SSH Tunnels **93**

SSL/TLS-Enabled Load Balancing **95**

Section 3: Anonymous Networks **100**

Tor Configuration **101**

Tor Hidden Services **106**

Summary **107**

5 Web Servers 109

Section 1: Web Server Security Fundamentals **109**

Permissions **109**

HTTP Basic Authentication **110**

Section 2: HTTPS **113**

Enable HTTPS **114**

Redirect HTTP to HTTPS **115**

HTTPS Reverse Proxy **116**

HTTPS Client Authentication **117**

Section 3: Advanced HTTPS Configuration **118**

HSTS **118**

HTTPS Forward Secrecy **119**

Web Application Firewalls **120**

Summary **131**

6 Email 133

Section 1: Essential Email Hardening **133**

Email Security Fundamentals **134**

Basic Email Hardening **135**

Section 2: Authentication and Encryption **137**

SMTP Authentication **138**

SMTPS **139**

Section 3: Advanced Hardening **141**

SPF **141**

DKIM **146**

DMARC **152**

Summary **156**

7 DNS 157

Section 1: DNS Security Fundamentals **158**

Authoritative DNS Server Hardening **159**

Recursive DNS Server Hardening **160**

Section 2: DNS Amplification Attacks and Rate Limiting **161**

DNS Query Logging **162**

Dynamic DNS Authentication **163**

Section 3: DNSSEC **166**

How DNS Works **166**

DNS Security Issues **168**

How DNSSEC Works **168**

DNSSEC Terminology **171**

Add DNSSEC to a Zone **172**

Summary **175**

8 **Database 177**

Section 1: Database Security Fundamentals **177**

Essential Database Security **177**

Local Database Administration **179**

Database User Permissions **182**

Section 2: Database Hardening **185**

Database Network Access Control **186**

Enable SSL/TLS **188**

Section 3: Database Encryption **191**

Full Disk Encryption **192**

Application-Side Encryption **192**

Client-Side Encryption **195**

Summary **195**

9 **Incident Response 197**

Section 1: Incident Response Fundamentals **197**

Who Performs Incident Response? **197**

Do You Prosecute? **197**

Pull the Plug **198**

Image the Server **199**

Server Redeployment **199**

Forensics **199**

Section 2: Secure Disk Imaging Techniques **200**

Choose the Imaging System **201**

Create the Image **201**

Introduction to Sleuth Kit and Autopsy **202**

Section 3: Walk Through a Sample Investigation **209**

Cloud Incident Response **213**

Summary **214**

A **Tor 215**

What Is Tor? **215**

Why Use Tor? **215**

How Tor Works **216**

Security Risks **219**

Outdated Tor Software **219**

Identity Leaks **219**

B SSL/TLS 221

What Is TLS? **221**

Why Use TLS? **221**

How TLS Works **222**

Deciphering Cipher Names **223**

TLS Troubleshooting Commands **224**

View the Contents of a Certificate **224**

View the Contents of a CSR **224**

Troubleshoot a Protocol over TLS **224**

Security Risks **224**

Man-in-the-Middle Attacks **225**

Downgrade Attacks **225**

Forward Secrecy **226**

Index 229