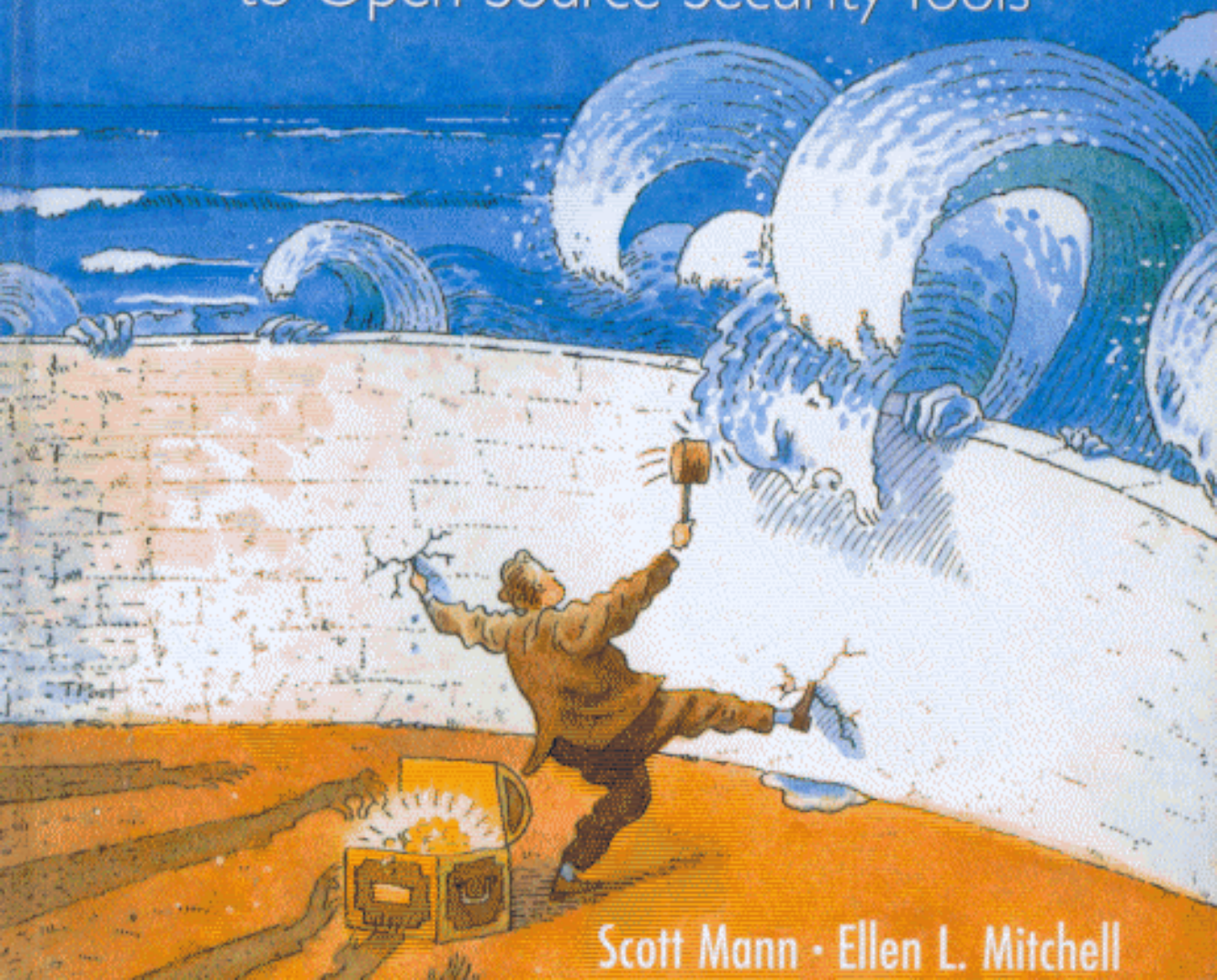
PRENTICE HALL SERIES IN COMPUTER NETWORKING AND DISTRIBUTED SYSTEMS

LINUX SYSTEM SECURITY

The Administrator's Guide to Open Source Security Tools



Scott Mann · Ellen L. Mitchell

Contents

Figures xix
Examples xxi
Tables xxix
Preface xxxiii

Chapter 1 **Vulnerability Survey** 1

How Did That Happen?

What Happened? 2
Other Cracker Activities 3
So, Are You Going to Show Us How to Break into Systems? 3
A Survey of Vulnerabilities and Attacks 4
Technical 4
Social 6
Physical 6
Summary 7
For Further Reading 7
Books 7
Interesting Cracker Tales 8
Web Sites 8
Full-Disclosure Resources 9

Chapter 2 **Security Policies** 11

Imagine That! You're Big Brother!

What Is Computer and Network Security? 13
Elements of a Computing Environment 13
Risk Analysis 14
The Security Policy 14
Securing Computers and Networks 15
User Privacy and Administrator Ethics 18
Summary 18
For Further Reading 18
Books 18
Web Resources 19
Other Resources 19

Chapter 3 **Background Information** 21
This 'n That
BIOS Passwords 22
Linux Installation and LILO 22
A Note about LILO 22
Recovering a Corrupt System 24
Installation and LILO Resources 24
Start-Up Scripts 24
Red Hat Package Manager 26
Verifying Packages with RPM 26
Checking PGP Signatures with RPM 27
RPM Resources 28
RPM Mailing List 28
TCP/IP Networking Overview 28
The TCP/IP Model Layers 30
Remote Procedure Call Applications 36
Trusted Host Files and Related Commands 36
Some Major Applications 37
Network Monitoring 38
General TCP/IP Networking Resources 39
NFS, Samba, NIS, and DNS Resources 40
Request for Comment 40
Cryptography 41
The Purpose of Cryptography 41
Algorithm Types 42
Hash Functions and Digital Signatures 44
Passwords Aren't Encrypted, They're Hashed! 45
An Overview of PGP 45
Cryptography References 47
Testing and Production Environments 47
Security Archives 47
Software Testing 48
Source Code Auditing 48
Pristine Backups 49
Security Resources 49
Licenses 50

Chapter 4 **Users, Permissions, and Filesystems** 57
Of Course, I Trust My Users!
User Account Management 57
Good Passwords 58
All Accounts Must Have Passwords! Or Be Locked! 59
Password Aging and the Shadow File 61
Restricted Accounts 64
Shell History 66

The Root Account 66
Using the Root Account 66
Multiple root Users 67
Minimizing the Impact of root Compromise 68
Configuring /etc/securetty 68
Group Account Management 69
File and Directory Permissions 70
User File and Directory Permissions 71
System File and Directory Permissions 73
SUID and SGID 74
File Attributes 75
Using xlock and xscreensaver 77
Filesystem Restrictions 78
Summary 79
For Further Reading 80
System Administration 80
System Security 80

Chapter 5 **Pluggable Authentication Modules 81**

Been Cracked? Just Put PAM On It!

PAM Overview 82
PAM Configuration 83
PAM Administration 86
PAM and Passwords 86
PAM and Passwords Summary 92
PAM and login 93
Time and Resource Limits 95
Access Control with pam_listfile 100
PAM and su 103
Using pam_access 104
Using pam_lastlog 105
Using pam_rhosts_auth 106
One-Time Password Support 108
PAM and the other Configuration File 108
Additional PAM Options 109
PAM Logs 109
Available PAM Modules 109
PAM-Aware Applications 112
Important Notes about Configuring PAM 112
The Future of PAM 114
Summary 114
For Further Reading 114
On-Line Documentation 115

Chapter 6 *Just Once, Only Once!*

One-Time Passwords **117**
The Purpose of One-Time Passwords 118
S/Key 118
S/Key OTP Overview 119
S/Key Version 1.1b 121
S/Key Version 2.2 132
OPIE 132
Obtaining and Installing OPIE 133
Implementing and Using OPIE 139
OPIE and PAM 143
Obtaining and Installing `pam_opie` 143
Obtaining and Installing `pam_if` 144
Implementing `pam_opie` and `pam_if` 144
Which OTP System Should I Use? 147
Advantages and Disadvantages of S/Key 147
Advantages and Disadvantages of OPIE 147
S/Key and OPIE Vulnerabilities 147
Summary 148
For Further Reading 148
Programming 148
E-Mail Lists 148

Chapter 7 *Bean Counting*

System Accounting **149**
General System Accounting 149
Connection Accounting 150
The `last` Command 151
The `who` Command 152
One Other Command 153
Process Accounting 153
The `sa` Command 154
The `lastcomm` Command 155
Accounting Files 156
Summary 157
For Further Reading 157
Books 157
On-Line Documentation 157

Chapter 8 *And You Thought Wiretapping Was for the Feds!*

System Logging **159**
The `syslog` System Logging Utility 159
Overview 160
The `/etc/syslog.conf` File 160
Invoking the `syslogd` Daemon 164
Configuring `/etc/syslog.conf` 164
The `klogd` Daemon 170

Other Logs 170
Alternatives to syslog 171
The auditd Utility 171
Summary 171
For Further Reading 172
General System Logging 172
Intrusion Detection 172

Chapter 9 **Superuser Do (sudo) 173**

Want to Be root?

What Is sudo? 173
Obtaining and Implementing sudo 174
Features of Version 1.5.9p4 174
Implementing Version 1.5.9p4 175
Using sudo 178
The Functionality of sudo 178
The /etc/sudoers File 178
General Syntax of /etc/sudoers 181
The visudo Command 184
Options to the sudo Command 184
A More Sophisticated Example 185
Setting Up sudo Logging 188
Reading sudo Logs 188
PAM and sudo 189
Disabling root Access 190
Vulnerabilities of sudo 191
Summary 191
For Further Reading 191
Reference Books 191
E-Mail Lists 192
Web Sites 192
On-Line Documentation 192
Kerberos Resources 192
FWTK Resources 192

Chapter 10 **Securing Network Services: TCP_wrappers, portmap, and xinetd 193**

Which Doors Are Open?

TCP_Wrappers 194
Building TCP_Wrappers 196
Access Control with TCP_Wrappers 202
TCP_Wrappers Utility Programs 216
TCP_Wrappers Vulnerabilities 218
The Portmapper 218
Building the Portmapper 219
Implementing Portmapper Access Control 223

The portmap Log Entries 224
Gracefully Terminating and Recovering the Portmapper 224
Portmapper Vulnerabilities 226
Unwrapped Services 226
Replacing inetd with xinetd 226
Advantages of xinetd 227
Disadvantages of xinetd 228
Obtaining xinetd 228
Building xinetd 229
The xinetd Configuration File 232
The xinetd Daemon 250
Which One Should I Use? 252
Summary 253
For Further Reading 253
Resources for TCP_Wrappers 253
Resources for the Portmapper 254
Resources for xinetd 254
Internet Services Resources 255

Chapter 11 The Secure Shell 257

Let 'Em Sniff the Net!

Overview of SSH 257
Host-Based Authentication Using RSA 257
Authenticating the User 259
Available Versions of SSH 263
Obtaining and Installing SSH 264
Compiling SSH 265
Configuring the Secure Shell 267
Configuring the Server Side 269
Configuring the Client Side 275
Using SSH 282
Configuring SSH Authentication Behavior 282
sshd Missing in Action 282
Authentication Flow of Events 283
Nonpassword Authentication 289
Password-Based Authentication 304
Exploring ssh Functionality 304
ssh Examples 304
scp Examples 306
Port Forwarding and Application Proxying 307
Secure Shell Alternatives 310
Summary 312
For Further Reading 312

Chapter 12 **Crack** **313**

So You Think You've Got a Good Password!

Obtaining Crack 314
Major Components of Crack 314
Crack Overview 315
Building Crack 318
Modifying Crack for Linux 318
Modifying Crack for MD5 319
Modifying Crack for Bigcrypt 319
Preparing Crack for `crypt(3)` 320
Compiling and Linking Crack 320
Compiling Crack Itself 320
Crack Dictionaries 321
Obtaining Other Crack Dictionaries 323
Using Crack 323
Running Crack 323
Running Crack over the Network 328
`Crack7` 330
Crack Rules 330
What Do We Do about Cracked Passwords? 336
The White Hat Use of Crack 337
Effectively Using Crack 338
Summary 339
For Further Reading 339

Chapter 13 **Auditing Your System with `tiger`** **341**

What's Been Happening?

Overview of `tiger` 341
Obtaining `tiger` 342
Major Components of `tiger` 342
Overview of `tiger` Configuration 347
Overview of Run-Time Operation 360
`tiger` Scripts 361
Installing `tiger` to Run through `cron` 368
Which Scripts Should I Run? 370
`cronrc` for a Development Machine 372
Running Crack from `tiger` 373
Deciphering `tiger` Output 373
Troubleshooting `tiger` 375
Modifying `tiger` 375
Modifying Scripts 376
Adding New Checks 376
Signatures 377
Recommendations 379
Summary 379

For Further Reading 379
Mailing List for `tiger` 379
`sendmail` Resources 379

Chapter 14 Tripwire 381

Setting the Trap

Tripwire Overview 382
Obtaining and Installing Tripwire 383
Tripwire Version 1.2 383
The Tripwire Configuration File 386
Extending the Configuration File 389
Effectively Building the Tripwire Configuration File 391
Example Configuration File for Red Hat Linux 393
The `tripwire` Command 395
Tripwire Initialize Mode 396
Effective Tripwire Initialization 397
Storing the Database 398
Routine Tripwire Runs—Compare Mode 399
A Note on Performance 402
Tripwire Update Mode 402
Summary 403
For Further Reading 404
On-Line Documentation 404
Web Site 404

Chapter 15 The Cryptographic and Transparent Cryptographic Filesystems 405

Space, the Cracker Frontier

Overview of the Cryptographic File System 405
CFS Flow of Events 406
Obtaining and Installing CFS 406
CFS Administrative Tasks 408
Using CFS 410
Creating and Attaching CFS Directories 410
The CFS Commands and Daemon Detailed 414
Using CFS over NFS 416
Vulnerabilities of CFS 416
Overview of TCFS 416
Obtaining and Installing TCFS 417
The TCFS Client Side 417
The TCFS Server Side 424
Using TCFS 425
Configuring TCFS for Use with PAM 425
TCFS Administrative Tasks 426
Extended Attributes for TCFS 427
Setting up the Encrypted Directory 428
TCFS Groups 429
TCFS Key Management 429

Vulnerabilities of TCFS 430
CFS and TCFS Comparison 431
Securely Deleting Files 431
Alternatives to CFS and TCFS 432
Summary 432
For Further Reading 433
Papers 433
E-Mail Lists 433

Chapter 16 Packet Filtering with `ipchains` 435

We Must Censor!

Packet Filtering 436
Configuring the Kernel for `ipchains` 437
`ipchains` Overview 437
Behavior of a Chain 438
Malformed Packets 438
Analysis of an Inbound Packet 438
Analysis of an Outbound Packet 440
The Loopback Interface 440
Custom Chains 440
Introduction to Using `ipchains` 440
The `ipchains` Command 441
Some Simple Examples 446
Packet Fragments 457
IP Masquerading 458
Adding Custom Chains 461
ICMP Rules in a Custom Chain 461
Antispoofing Rules 463
Rule Ordering Is Important! 464
Saving and Restoring Rules 465
Rule Writing and Logging Tips 466
Changing Rules 467
`ipchains` Start-up Scripts 467
Building Your Firewall 469
Simple Internal Network 469
Simple Internal Network Using DHCP 481
`ipchains` Isn't Just for Firewalls! 484
One More Thing 484
Supplementary Utilities 484
Other Examples 484
Port Forwarding 485
The `fwconfig` GUI 485
Mason 485
The Network Mapper (`nmap`) 486
Additional Firewall Software 486
Virtual Private Networks and Encrypted Tunnels 486

The Next Generation... 486
Summary 487
For Further Reading 487
ipchains Documentation 487
Masquerading Documentation 487
ISP Connectivity-Related Resources 487
General Firewall References 488
DMZ Resources 488
ICMP-Related References 488
A Special Acknowledgment 489

Chapter 17 Log File Management 491

Wiretapping Is Not So Much Fun, After All!

General Log File Management 491
logrotate 492
Obtaining and Installing logrotate 492
Configuring logrotate 492
Pulling It All Together 498
swatch 498
Obtaining swatch 499
Installing swatch 500
Configuring and Running swatch 503
logcheck 507
Obtaining logcheck 507
Major Components of logcheck 508
Configuring and Installing logcheck 508
logcheck Output 513
Troubleshooting logcheck 514
Summary 514

Chapter 18 Implementing and Managing Security 515

This Is an Awful Lot of Work!

So, Where Do I Start? 516
Hardening Linux 516
Selecting the Right Tools 523
Reducing the Workload 523
What if My Systems Are Already in the Production Environment? 524
The Internal Network 524
Critical Internal Servers 524
Internal Maintenance 525
Firewalls and the DMZ 525
External Maintenance 526
Break-in Recovery 526
Adding New Software 526
Only through Knowledge... 527

Appendix A Keeping Up to Date 529

Appendix B Tools Not Covered 543

Glossary 547

Index 555