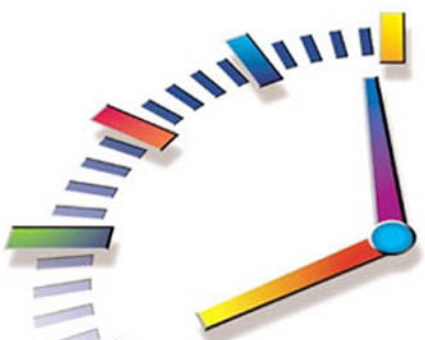
When you only have time for the answers™

24 proven one-hour lessons



SAMS Teach Yourself

Linux® Security Basics

in 24 Hours

Aron Hsiao

SAMS

Aron Hsiao

SAMS

Teach Yourself

Linux® Security Basics

in 24 Hours

SAMS

201 West 103rd St., Indianapolis, Indiana 46290 USA

Sams Teach Yourself Linux® Security Basics in 24 Hours

International Standard Book Number: 0-672-32091-6

Library of Congress Catalog Card Number: 00-111802

Printed in the United States of America

First Printing: April 2001

04 03 02 01 4 3 2 1

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Sams cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

The term Linux is a registered trademark of Linus Torvalds, the original author of the Linux kernel. Linux is freely distributed under the GNU General Public License (GPL).

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Associate Publisher
Jeff Koch

Acquisitions Editors
Maureen McDaniel
Katie Purdum

Development Editor
Mark Renfrow

Managing Editor
Matt Purcell

Project Editor
Natalie F. Harris

Copy Editors
Gene Redding
Mary Ellen Stephenson

Indexers
Sandra Henselmeier
Eric Schroeder

Proofreaders
Benjamin Berg
Matt Wynalda

Technical Editor
David Bandel

Team Coordinator
Vicki Harding

Interior Designer
Gary Adair

Cover Designer
Aren Howell

Page Layout
Darin Crone
Lizbeth Patterson
Gloria Schurick

Contents at a Glance

	Introduction	1
PART I	**Basic Security for All Roles**	**7**
Hour 1	Selecting and Installing a Linux Distribution	9
2	BIOS and Motherboards	31
3	Physical Security	45
4	The Boot Process	55
5	System and User Fundamentals	69
6	TCP/IP Network Security	83
7	File System Security	99
8	Extra File System Security Tools	121
9	Making the Most of Pluggable Authentication Modules (PAM)	135
PART II	**Network Security**	**147**
Hour 10	Using `ipchains` for Firewalling and Routing	149
11	Using `iptables` for Firewalling and Routing	163
12	Securing Apache, FTP, and SMTP Services	179
13	Network Security: DNS with BIND	199
14	Network Security: NFS and Samba	209
15	Securing X11R6 Access	223
PART III	**Data Encryption**	**235**
Hour 16	Encrypting Data Streams	237
17	Introduction to Kerberos	259
18	Encrypting Web Data	277
19	Encrypting File System Data	287
20	Encrypting E-Mail Data	299

PART IV Intrusion Detection, Auditing, and Recovery **311**

Hour 21 Auditing and Monitoring 313
22 Detecting Attacks in Progress 327
23 Preserving Data 337
24 Recovering from Attacks 351

PART V Appendixes **363**

Appendix A Configuration Files Important to Security 365
B System Account File Formats 369
C Security Web Sites of Note 371
D Quick Security Checklist 375
E Web Links to Documented Software 383
Index 385

Contents

Introduction 1

PART I Basic Security for All Roles 7

HOUR 1 Selecting and Installing a Linux Distribution 9

Establishing the Role of the Machine in Question 9
Choosing a Linux Distribution 11
The Features/Security Tradeoff 11
Choosing from the Major Linux Distributions 13
Security-Minded Linux Installation 17
Step 1: Get Linux Straight from the Source 18
Step 2: Define Multiple Partitions 19
Step 3: Install and Enable only the Essentials 20
Step 4: Finish Separating File Systems, Fix `/etc/fstab` 22
Step 5: Install All Current Updates 26
Summary 27
Q&A 28
New Terms 29

HOUR 2 BIOS and Motherboards 31

Linux Security Before Linux Is Loaded 32
The System BIOS 32
Entering Setup 33
Navigating Setup 33
BIOS Password Protection 34
Boot Password Protection 35
Boot Order Configuration 36
Secondary BIOSs 38
External/Attachable Devices 40
Controlling Flash BIOS Updates 41
Summary 41
Q&A 42
New Terms 43

HOUR 3 Physical Security 45

Why Is Physical Security Important? 45
Location, Location, Location! 46
Strategies for Difficult Locations 47
The Power Cycle 47
Boot Devices 49
Locking Down “the Box” 50

Access Auditing 51
Summary 52
Q&A 53
New Terms 54

HOUR 4 The Boot Process 55

The Linux Loader 55
The `/etc/lilo.conf` File 57
The `password` Keyword 58
The `restricted` Keyword 59
Putting `password` and `restricted` Together 60
The `prompt` and `timeout` Keywords 61
Saving Changes 62
Permissions for `/etc/lilo.conf` 63
The Init Program and the `/etc/inittab` File 63
Default Runlevel 63
The Three-Key Smash (Ctrl+Alt+Del) 65
Summary 65
Q&A 66
New Terms 66

HOUR 5 System and User Fundamentals 69

`/etc/securetty`, `/etc/shells`, and `.bash_logout` 70
The SysV-Style Init Process 71
Finding and Disabling Unnecessary Services 73
Reenabling Disabled Services 76
Creating User Accounts Securely 77
Shadow and MD5 77
Adding a User, Step 1: `/usr/sbin/groupadd` 78
Adding a User, Step 2: `/usr/sbin/useradd` 79
Adding a User, Step 3: `passwd` and `chage` 79
Summary 80
Q&A 81
New Terms 81
Exercises 82

HOUR 6 TCP/IP Network Security 83

Securing `inetd`, the Internet Daemon 84
Why `inetd` Is Risky 84
The `/etc/inetd.conf` File 84
The `/etc/services` File 87

Using TCP Wrappers Properly 89
TCP Wrappers Explained 90
Healthy Paranoia (The `/etc/hosts.deny` File) 90
Sparing Exceptions (The `/etc/hosts.allow` File) 91
More TCP Wrappers Tricks 93
Using `tcpdchk` and `tcpdmatch` 94
Logs, `syslogd`, and Security 95
Log Everything 95
Log Elsewhere 96
Summary 96
Q&A 96
New Terms 97
Exercises 98

HOUR 7 File System Security 99

Understanding Permissions 99
File Ownership 100
Access Rights 100
Permission Examples 104
Modifying Permissions 105
Using `chmod` in Symbolic Mode 105
Using `chmod` in Numeric Mode 106
Using `umask` to Set Default Permissions 107
Special Cases, Risks, and Solutions 109
Extra Directory Permissions 109
Device Nodes 109
SUID/SGID Executables 111
Setting SUID/SGID with `chmod` 112
Eliminating Unnecessary SUID/SGID Permissions 112
Checking for Anomalous SUID/SGID Instances 113
Keep SUID/SGID Binaries Current 113
Append-Only and Immutable Files 113
Read-Only `root` File System 114
Options for `mount` and `fstab` 116
Summary 117
Q&A 118
New Terms 119

HOUR 8 Extra File System Security Tools 121

POSIX Access Control Lists for Linux 122
A Sample Scenario Needing ACL Capability 122
POSIX ACLs for Linux 123
Syntax for the `setfacl` Command 126
Syntax for the `getfacl` Command 127

Default Permissions (`getfacl`, `setfacl`, and Directories) 128
ACL Mask Permissions 129
Copying ACLs Between Files 130
Caveats and Considerations 130
Secure File Deletion Tools 131
Summary 132
Q&A 132
New Terms 133

HOUR 9 Making the Most of Pluggable Authentication Modules (PAM) 135

How PAM Is Configured: The Basics 136
How PAM Works: The Basics 138
Putting PAM to Work: Expiring Passwords 140
Putting PAM to Work: Enforcing `wheel` 141
Putting PAM to Work: Other Authentication 143
Summary 144
Q&A 144
New Terms 144
Exercises 145

PART II Network Security 147

HOUR 10 Using `ipchains` for Firewalling and Routing 149

Network Security and the Kernel 150
Using `ipchains` 152
Understanding `ipchains` Rules 152
Calling Syntax for the `ipchains` Utility 153
A Simple Ruleset That Works 155
Masquerading 157
Port Forwarding 158
Putting It All Together 158
Summary 160
Q&A 161
New Terms 162
Exercises 162

HOUR 11 Using `iptables` for Firewalling and Routing 163

What Is `iptables`? What Happened to `ipchains`? 164
Network Security and the Kernel 164
Using `iptables` 166
Understanding `iptables` Rules 167
Calling Syntax for the `iptables` Utility 169
State-Based Matches 171

A Simple Ruleset That Works 172
Masquerading and NAT 173
Port Forwarding 174
Putting It All Together 174
Summary 176
Q&A 177
New Terms 177
Exercises 178

HOUR 12 Securing Apache, FTP, and SMTP Services 179

Security and the Apache HTTPD Server 180
Global Basic Security-Related Directives 180
Global Logging Directives 182
`Directory` and `DirectoryMatch` Scopes 184
Additional Scopes 186
Authentication 186
The `Options` and `AllowOverride` Directives 189
The Access File 190
Security and File Transfer Protocol 191
Anonymous Versus Private FTP 191
The `/etc/ftpaccess` File 192
The `/etc/ftpusers` File 193
Anonymous Upload Permissions 193
Security and `sendmail` 194
Securing Sendmail Through Packet Filtering 194
Securing Sendmail Using TCP Wrappers 195
`m4` and `sendmail.cf` Configuration Notes 196
Summary 196
Q&A 197
New Terms 198
Exercises 198

HOUR 13 Network Security: DNS with BIND 199

Pre-Chroot BIND Security 200
Packet Filtering for the Domain Port 200
Notes on `named.conf` 201
Running `named` in a Chroot Environment 203
Adding User and Group 203
Creating the Jail 204
Setting Up `syslogd` for Chroot `named` 205
Starting `named` in the Chroot Jail 206
Summary 206
Q&A 207
New Terms 207

HOUR 14 Network Security: NFS and Samba 209

Network File System (NFS) Security 210
Selecting an NFS Server 210
Including Kernel-Based NFS Support 210
Configuring the `/etc/exports` File 211
NFS Packet Filtering 214
Samba Security 215
Starting SWAT 216
Global Security Options in SWAT 217
Share Security Options in SWAT 218
Packet Filtering and Samba 220
Summary 221
Q&A 221
New Terms 222

HOUR 15 Securing X11R6 Access 223

Why Is X Security an Issue? 223
Host-Based Authentication 224
The `/etc/Xn.hosts` File 225
The `xhost` Command 225
Host-Based Authentication Problems 227
Token-Based Authentication 228
Using the `xauth` Command 228
Starting the X Server 229
Distributing the Cookie 229
Host-Based and Token-Based Authentication Interaction 230
The X Display Manager (XDM) 230
X and Packet Filtering 231
Summary 232
Q&A 233
New Terms 233

PART III Data Encryption 235

HOUR 16 Encrypting Data Streams 237

What Do SSH and OpenSSH Do? 237
Installing, Configuring, and Using SSH 238
Downloading and Installing SSH 238
Additional Configuration 241
Using SSH for Remote Logins 243
Host-Based Authentication 244
Public Key Authentication 245
Using SSH for FTP 246

Tunneling TCP Streams Through SSH 247
Improving X Security with SSH 248
Installing, Configuring, and Using OpenSSH 249
Downloading and Installing OpenSSL 249
Downloading and Installing OpenSSH 250
Additional Configuration 251
Using OpenSSH for Remote Logins 253
RhostsRSA Authentication 254
User-Based Public Key Authentication 255
Tunneling TCP Streams Through OpenSSH 255
Improving X Security with OpenSSH 256
Summary 256
Q&A 257
New Terms 258

HOUR 17 Introduction to Kerberos 259

What Is Kerberos? 259
Building a Key Distribution Center 260
Downloading and Installing Kerberos 5 261
Configuring Kerberos 5 262
Administrating Kerberos 5 266
Adding Administrator Principals 266
Adding and Configuring Host Principals 268
Adding User Principals 269
More on Kadmin 270
Using Kerberos 5 270
Getting a Ticket 271
Destroying a Ticket 272
Changing Your Password 273
Encrypting Data Streams 273
Summary 273
Q&A 273
New Terms 274

HOUR 18 Encrypting Web Data 277

Compiling and Installing `Apache+mod_ssl` 278
Downloading Apache, OpenSSL, and `mod_ssl` 278
Extracting and Compiling OpenSSL 279
Extracting, Configuring, and Compiling `mod_ssl` and Apache 279
Making a Self-Signed Certificate 280
Installing and Configuring the Apache Tree 282
Starting the SSL-Enabled Apache Server 283
Summary 284
Q&A 285
New Terms 286

HOUR 19 Encrypting File System Data 287

A Brief Overview of TCFS 288
Preparing to Install TCFS 288
An Empty EXT2 Partition 288
A Working NFS Installation 289
A Kernel 2.2.16– or 2.2.17–Ready System 289
Downloading and Installing TCFS 289
Extract Sources and Apply Patches 289
Compile and Install the TCFS Distribution 290
Compile the Patched Kernel 293
Building the Encryption Module and Enabling TCFS 293
Using TCFS 294
Enabling TCFS Access (Administrative Tasks) 294
Taking Advantage of Encryption (User Tasks) 295
Encrypting Files 295
Summary 296
Q&A 296
New Terms 297

HOUR 20 Encrypting E-Mail Data 299

A Quick PGP Overview 299
Getting and Installing GNU Privacy Guard (GPG) 300
Generating Your Keys 301
Working with Keys 303
Listing Keys 303
Importing and Exporting Keys 303
Signatures and Trust 304
Using GPG: Nuts and Bolts 306
Signatures for Data 306
Encrypting and Decrypting Data 307
Summary 309
Q&A 309
New Terms 310

PART IV Intrusion Detection, Auditing, and Recovery 311

HOUR 21 Auditing and Monitoring 313

Putting SAINT to Work 313
Downloading and Installing SAINT 314
Using SAINT 315

Staying Alert with SWATCH 320
Downloading and Installing SWATCH 320
Using SWATCH to Watch Logs 321
The Match File Format 321
Summary 324
Q&A 324
New Terms 325

HOUR 22 Detecting Attacks in Progress 327

What Is Snort? 327
Special Snort Requirements 328
Downloading and Installing Snort 328
Installing `libpcap` 329
Installing `libnet` 329
Installing Snort 330
Using Snort 331
Pretty Snort Reports 332
Practical SnortSnarf Use 333
Summary 333
Q&A 334
New Terms 334

HOUR 23 Preserving Data 337

Data Backups and Security 337
Preserving Your Valuable Data 338
Modified System Binaries 338
The Root Kit 338
Using `tar` and `afio` for Backups 339
Simple Backup and Restore with `tar` 339
Simple Backup and Restore with `afio` 341
Using `mt` to Operate Tape Devices 342
Using `mtx` to Operate Changer Devices 343
Scheduling, Rotating, and Preserving Backups 344
Scheduling Backups 344
Rotating Backups 345
Backups at Multiple Locations 346
Proprietary Backup Software 346
Backup and Restore Utility (BRU) 347
Arkeia 347
Summary 347
Q&A 348
New Terms 349

HOUR 24 Recovering from Attacks 351

The Telltale Signs 351
Worst-Case Scenario 352
Pull Offline Immediately 352
Stop Linux 353
Boot Cautiously 354
Archive What's Left 354
Understanding What Happened 355
Notify the Authorities 356
Getting Back Online 357
Reformat and Reinstall 357
Restore Important Data 357
Take Care of the Vulnerability 358
Pay Special Attention to Repeat Visitors 359
Go Back Online 359
Summary 359
Q&A 360
New Terms 361

PART V Appendixes 363

APPENDIX A Configuration Files Important to Security 365

APPENDIX B System Account File Formats 369

APPENDIX C Security Web Sites of Note 371

General Security 371
Computer Emergency Response Team—`http://www.cert.org` 371
Computer Incident Advisory Capability—`http://www.ciac.org` 372
The Cypherpunks Home Page—`ftp://ftp.csua.berkeley.edu/pub/cypherpunks/Home.html` 372
SecurityFocus.com—`http://www.securityfocus.com` 372
Linux-Specific Security 372
The Debian GNU/Linux Security Site—`http://security.debian.org` ..372
Red Hat Linux Errata Page—`http://www.redhat.com/support/errata/` 372
Caldera Systems—`http://www.calderasystems.com/support/security/` 372
Linux-Mandrake—`http://www.linux-mandrake.com/en/security/` 373
SuSE Linux—`http://www.suse.com/us/support/security/` 373
TurboLinux—`http://www.turbolinux.com/security/` 373
LinuxPPC—`http://linuxppc.org/security/advisories/` 373

APPENDIX D Quick Security Checklist 375

Hour 1: Selecting and Installing a Linux Distribution 375
Hour 2: BIOS and Motherboards 376
Hour 3: Physical Security 376
Hour 4: The Boot Process 376
Hour 5: System and User Fundamentals 376
Hour 6: TCP/IP Network Security 377
Hour 7: File System Security 377
Hour 8: Extra File System Security Tools 377
Hour 9: Making the Most of Pluggable Authentication Modules (PAM) 377
Hour 10: Using `ipchains` for Firewalling and Routing 378
Hour 11: Using `iptables` for Firewalling and Routing 378
Hour 12: Securing Apache, FTP, and SMTP Services 378
Hour 13: Network Security: DNS with BIND 379
Hour 14: Network Security: NFS and Samba 379
Hour 15: Securing X11R6 Access 379
Hour 16: Encrypting Data Streams 379
Hour 17: Introduction to Kerberos 380
Hour 18: Encrypting Web Data 380
Hour 19: Encrypting File System Data 380
Hour 20: Encrypting E-Mail Data 380
Hour 21: Auditing and Monitoring 380
Hour 22: Detecting Attacks in Progress 381
Hour 23: Preserving Data 381
Hour 24: Recovering from Attacks—A Mini-Checklist 381

APPENDIX E Web Links to Documented Software 383

Index 385

About the Author

ARON HSIAO is a computing entrepreneur and freelance consultant with a 15-year background in UNIX and UNIX-like operating systems. He has worked almost exclusively with Linux since 1994. As an independent contractor throughout the 1990s, Aron helped various dot-com firms with systems installation, network deployment, content production, and Internet marketing. He has also worked as a volunteer in a number of computing-related and educational capacities in his community. Aron has collaborated in the past with Sams Publishing and Que on Linux- and Unix-oriented texts as a technical editor and as an author. Aron served as the About.com guide to Linux from 1997 to 2000.

About the Technical Editor

DAVID BANDEL has over 10 years' worth of Unix system administration experience on a wide variety of systems, including DEC-5000 systems running Ultrix, SUN SparcStations running SunOS 4 and later Solaris 2.x, HP-9000's running HP-UX, RS-6000's running AIX, and Intel systems running SCO OpenServer and Linux. In February 1996, David retired after 20 years of active duty in the U.S. Army, where he was initially introduced to Unix System Administration. While still in the military, he became an avid fan of Linux, which provided the look, feel, and power of Unix on an Intel platform. Currently, David enjoys working as a Unix/Linux consultant, installing firewalls and providing network connectivity, and writing books and articles about Linux.

Dedication

To Ching-Chuan Hsiao, Chu-Ying Hsiao, Wilson Gutzman, and LaBerle Gutzman.

—Aron Hsiao

Acknowledgments

This project was undertaken during an interesting phase of my life, and I couldn't have finished it without the support of others. Thanks for this support go first and foremost to the members of my family, each of whom is always ready to listen and advise. (This includes you, Quincy and Baby—both of you have been very helpful in paradoxically keeping me calm and focused.)

Thanks also go to Carlos, Kelli, and Onyx, my second family, who have invested a great deal in me and my undertakings, especially when phone bills are considered. Finally, this book is quite simply the product of a great deal of patience and hard work on the part of everyone at Sams. Maureen, Kathryn, Natalie, Mark, and everyone else involved—my thanks go to the entire team for sticking with this project until it was done and done right.

Aron Hsaio

Tell Us What You Think!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As an Associate Publisher for Sams, I welcome your comments. You can fax, e-mail, or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books stronger.

Please note that I cannot help you with technical problems related to the topic of this book, and that due to the high volume of mail I receive, I might not be able to reply to every message.

When you write, please be sure to include this book's title and author as well as your name and phone or fax number. I will carefully review your comments and share them with the author and editors who worked on the book.

Fax: 317-581-4770

E-mail: `feedback@samspublishing.com`

Mail: Jeff Koch
Sams
201 West 103rd Street
Indianapolis, IN 46290 USA

Introduction

In the computing world, *security* is a strange topic. This is because the computing world as we know it has largely become a collection of technologies for the enabling of networks, and our conception of what a network should be is fundamentally opposed to our conception of what good security should be. A network is designed specifically to allow needed data to be retrieved and to allow connections to be made between otherwise unrelated computers and systems. The role of security, on the other hand, is largely to forbid data from being retrieved or to forbid one computer from making a connection with another. Clearly, then, the process of securing a system or a network is one in which context and balance are important. Security must function well enough within your own computing context to provide you and your users with an acceptable balance between allowing and forbidding.

Because of the context-specific nature of this opposition, which is inherent in phrases like *computer security* and *network security*, and because security is a nearly infinitely deep topic for those who care to study it in depth, no one book can ever be the final word on security—no one book can ever be used by every user or system administrator to secure every system.

But Why Is Security Important at All?

When it comes to large Internet servers full of users' credit card numbers or large government servers full of nuclear secrets, it is easy to see why information ought to be protected—why some system-to-system connections and some attempts at data retrieval ought to be forbidden. These types of risks, on the one hand financial and involving hundreds of thousands of individuals and on the other hand national or even global in scale, are easy to see. But what about the typical dial-up modem user, who connects to the Internet to browse the Web or to help the kids with their homework? And what about the small business user who runs a small Web site but hardly feels important or large enough to be a target for international terrorists or organized crime?

Unfortunately, the Internet, like the real world, is not always a friendly place. There are any number of small-time ne'er-do-wells who like to get their hands on just the 10 or 15 credit card numbers your server contains. Even more frighteningly, there are thousands of "script kiddies" roaming the Internet without any motive at all—they enjoy breaking into computer systems and erasing data simply for fun. Often, they're not even knowledgeable hackers, but instead download their exploits (tools used for breaking into other peoples' computers) from security-oriented Web sites.