Using RAID, SAN, or Storage Appliances 66
Using Linux Software RAID 66
Using Hardware RAID 67
Using Storage-Area Networks (SANs) 67
Using Storage Appliances 67
Using a RAM-Based Filesystem 68

Part II Network and Service Performance

Chapter 4 Network Performance 75
Tuning an Ethernet LAN or WAN 75
Using network segmentation technique for performance 77
Using switches in place of hubs 80
Using fast Ethernet 81
Using a network backbone 82
Understanding and controlling network traffic flow 83
Balancing the traffic load using the DNS server 85
IP Accounting 85
IP accounting on a Linux network gateway 86
Chapter 5 Web Server Performance 89
Compiling a Lean and Mean Apache 89
Tuning Apache Configuration 95
Controlling Apache processes 96
Controlling system resources 100
Using dynamic modules 103
Speeding Up Static Web Pages 103
Reducing disk I/O for faster static page delivery 104
Using Kernel HTTP daemon 105
Speeding Up Web Applications 105
Using mod_perl 106
Using FastCGI 114
Installing and configuring FastCGI module for Apache 115
Using Java servlets 117
Using Squid proxy-caching server 118
Chapter 6 E-Mail Server Performance 125
Choosing Your MTA 125
Tuning Sendmail 126
Controlling the maximum size of messages 127
Caching Connections 127
Controlling simultaneous connections 130
Limiting the load placed by Sendmail 131

Saving memory when processing the mail queue 131
Controlling number of messages in a queue run 132
Handling the full queue situation 132
Tuning Postfix 133
Installing Postfix 133
Limiting number of processes used 134
Limiting maximum message size 135
Limiting number of messages in queue 135
Limiting number of simultaneous delivery to a single site 135
Controlling queue full situation 135
Controlling the length a message stays in the queue 136
Controlling the frequency of the queue 136
Using PowerMTA for High-Volume Outbound Mail 136
Using multiple spool directories for speed 137
Setting the maximum number of file descriptors 137
Setting a maximum number of user processes 138
Setting maximum concurrent SMTP connections 138
Monitoring performance 139

Chapter 7 NFS and Samba Server Performance 141
Tuning Samba Server 142
Controlling TCP socket options 142
Tuning Samba Client 145
Tuning NFS Server 145
Optimizing read/write block size 146
Setting the appropriate Maximum Transmission Unit 149
Running optimal number of NFS daemons 149
Monitoring packet fragments 150

Part III System Security

Chapter 8 Kernel Security 155
Using Linux Intrusion Detection System (LIDS) 155
Building a LIDS-based Linux system 156
Administering LIDS 163
Using libsafe to Protect Program Stacks 173
Compiling and installing libsafe 175
libsafe in action 178

Chapter 9 Securing Files and Filesystems 179
Managing Files, Directories, and User Group Permissions 179
Understanding file ownership & permissions 180
Changing ownership of files and directories using chown 181

Changing group ownership of files and directories with chgrp 182
Using octal numbers to set file and directory permissions 182
Using permission strings to set access permissions 185
Changing access privileges of files and directories using chmod 185
Managing symbolic links 186
Managing user group permission 188
Checking Consistency of Users and Groups 190
Securing Files and Directories 198
Understanding filesystem hierarchy structure 198
Setting system-wide default permission model using umask 201
Dealing with world-accessible files 203
Dealing with set-UID and set-GID programs 204
Using ext2 Filesystem Security Features 208
Using chattr 209
Using lsattr 210
Using a File Integrity Checker 210
Using a home-grown file integrity checker 210
Using Tripwire Open Source, Linux Edition 215
Setting up Integrity-Checkers 230
Setting up AIDE 230
Setting up ICU 231
Creating a Permission Policy 239
Setting configuration file permissions for users 239
Setting default file permissions for users 240
Setting executable file permissions 240

Chapter 10 PAM 241

What is PAM? 241
Working with a PAM configuration file 243
Establishing a PAM-aware Application 245
Using Various PAM Modules to Enhance Security 248
Controlling access by time 255
Restricting access to everyone but root 257
Managing system resources among users 258
Securing console access using mod_console 260

Chapter 11 OpenSSL 263

Understanding How SSL Works 263
Symmetric encryption 264
Asymmetric encryption 264
SSL as a protocol for data encryption 264
Understanding OpenSSL 266
Uses of OpenSSL 266
Getting OpenSSL 267

Installing and Configuring OpenSSL 267
OpenSSL prerequisites 267
Compiling and installing OpenSSL 268
Understanding Server Certificates 270
What is a certificate? 270
What is a Certificate Authority (CA)? 271
Commercial CA 272
Self-certified, private CA 272
Getting a Server Certificate from a Commercial CA 273
Creating a Private Certificate Authority 275
Chapter 12 Shadow Passwords and OpenSSH 277
Understanding User Account Risks 278
Securing User Accounts 279
Using shadow passwords and groups 280
Checking password consistency 282
Eliminating risky shell services 283
Using OpenSSH for Secured Remote Access 285
Getting and installing OpenSSH 285
Configuring OpenSSH service 286
Connecting to an OpenSSH server 293
Managing the root Account 298
Limiting root access 299
Using su to become root or another user 300
Using sudo to delegate root access 302
Monitoring Users 307
Finding who is on the system 308
Finding who was on the system 309
Creating a User-Access Security Policy 309
Creating a User-Termination Security Policy 310
Chapter 13 Secure Remote Passwords 313
Setting Up Secure Remote Password Support 313
Establishing Exponential Password System (EPS) 314
Using the EPS PAM module for password authentication 315
Converting standard passwords to EPS format 316
Using SRP-Enabled Telnet Service 317
Using SRP-enabled Telnet clients
from non-Linux platforms 319
Using SRP-Enabled FTP Service 319
Using SRP-enabled FTP clients
from non-Linux platforms 322

Chapter 14 xinetd 323
What Is xinetd? 323
Setting Up xinetd 325
Getting xinetd 325
Compiling and installing xinetd 325
Configuring xinetd for services 329
Starting, Reloading, and Stopping xinetd 333
Strengthening the Defaults in /etc/xinetd.conf 334
Running an Internet Daemon Using xinetd 335
Controlling Access by Name or IP Address 337
Controlling Access by Time of Day 338
Reducing Risks of Denial-of-Service Attacks 338
Limiting the number of servers 338
Limiting log file size 339
Limiting load 339
Limiting the rate of connections 340
Creating an Access-Discriminative Service 341
Redirecting and Forwarding Clients 342
Using TCP Wrapper with xinetd 345
Running sshd as xinetd 345
Using xadmin 346

Part IV Network Service Security

Chapter 15 Web Server Security 351
Understanding Web Risks 351
Configuring Sensible Security for Apache 352
Using a dedicated user and group for Apache 352
Using a safe directory structure 352
Using appropriate file and directory permissions 354
Using directory index file 356
Disabling default access 358
Disabling user overrides 358
Using Paranoid Configuration 359
Reducing CGI Risks 360
Information leaks 360
Consumption of system resources 360
Spoofing of system commands via CGI scripts 361
Keeping user input from making system calls unsafe 361
User modification of hidden data in HTML pages 366
Wrapping CGI Scripts 372
suEXEC 372
CGIWrap 375
Hide clues about your CGI scripts 377

Reducing SSI Risks 378
Logging Everything 379
Restricting Access to Sensitive Contents 382
Using IP or hostname 382
Using an HTTP authentication scheme 385
Controlling Web Robots 390
Content Publishing Guidelines 392
Using Apache-SSL 394
Compiling and installing Apache-SSL patches 394
Creating a certificate for your Apache-SSL server 395
Configuring Apache for SSL 396
Testing the SSL connection 398
Chapter 16 DNS Server Security 399
Understanding DNS Spoofing 399
Checking DNS Configuring Using Dlint 400
Getting Dlint 401
Installing Dlint 401
Running Dlint 402
Securing BIND 405
Using Transaction Signatures (TSIG) for zone transfers 405
Running BIND as a non-root user 409
Hiding the BIND version number 409
Limiting Queries 410
Turning off glue fetching 411
chrooting the DNS server 412
Using DNSSEC (signed zones) 412
Chapter 17 E-Mail Server Security 415
What Is Open Mail Relay? 415
Is My Mail Server Vulnerable? 417
Securing Sendmail 419
Controlling mail relay 422
Enabling MAPS Realtime Blackhole List (RBL) support 425
Sanitizing incoming e-mail using procmail 429
Outbound-only Sendmail 437
Running Sendmail without root privileges 438
Securing Postfix 440
Keeping out spam 440
Hiding internal e-mail addresses by masquerading 442
Chapter 18 FTP Server Security 443
Securing WU-FTPD 443
Restricting FTP access by username 445
Setting default file permissions for FTP 447

Using a chroot jail for FTP sessions 448
Securing WU-FTPD using options in /etc/ftpaccess 452
Using ProFTPD 455
Downloading, compiling, and installing ProFTPD 456
Configuring ProFTPD 456
Monitoring ProFTPD 462
Securing ProFTPD 462
Chapter 19 Samba and NFS Server Security 473
Securing Samba Server 473
Choosing an appropriate security level 473
Avoiding plain-text passwords 476
Allowing access to users from trusted domains 477
Controlling Samba access by network interface 477
Controlling Samba access by hostname or IP addresses 478
Using pam_smb to authenticate all users via a Windows NT server 479
Using OpenSSL with Samba 481
Securing NFS Server 483
Using Cryptographic Filesystems 487

Part V Firewalls

Chapter 20 Firewalls, VPNs, and SSL Tunnels 491
Packet-Filtering Firewalls 491
Enabling netfilter in the kernel 496
Creating Packet-Filtering Rules with iptables 498
Creating a default policy 498
Appending a rule 498
Listing the rules 499
Deleting a rule 500
Inserting a new rule within a chain 500
Replacing a rule within a chain 500
Creating SOHO Packet-Filtering Firewalls 501
Allowing users at private network access to external Web servers 504
Allowing external Web browsers access to a Web server on your firewall 505
DNS client and cache-only services 506
SMTP client service 508
POP3 client service 508
Passive-mode FTP client service 509
SSH client service 510
Other new client service 510

Creating a Simple Firewall 511
Creating Transparent, proxy-arp Firewalls 512
Creating Corporate Firewalls 514
Purpose of the internal firewall 515
Purpose of the primary firewall 515
Setting up the internal firewall 516
Setting up the primary firewall 518
Secure Virtual Private Network 528
Compiling and installing FreeS/WAN 529
Creating a VPN 530
Stunnel: A Universal SSL Wrapper 536
Compiling and installing Stunnel 536
Securing IMAP 536
Securing POP3 538
Securing SMTP for special scenarios 539
Chapter 21 Firewall Security Tools 541
Using Security Assessment (Audit) Tools 541
Using SAINT to Perform a Security Audit 541
SARA 549
VetesCan 550
Using Port Scanners 550
Performing Footprint Analysis Using nmap 550
Using PortSentry to Monitor Connections 552
Using Nessus Security Scanner 558
Using Strobe 561
Using Log Monitoring and Analysis Tools 562
Using logcheck for detecting unusual log entries 562
Swatch 565
IPTraf 565
Using CGI Scanners 566
Using cgichk.pl 566
Using Whisker 568
Using Malice 569
Using Password Crackers 569
John The Ripper 570
Crack 571
Using Intrusion Detection Tools 571
Tripwire 571
LIDS 571
Using Packet Filters and Sniffers 572
Snort 572
GShield 575

Useful Utilities for Security Administrators 575
Using Netcat 575
Tcpdump 580
LSOF 581
Ngrep 586

Appendix A IP Network Address Classification 589
Appendix B Common Linux Commands 593
Appendix C Internet Resources 655
Appendix D Dealing with Compromised Systems 661
Appendix E What's On the CD-ROM? 665

Index 669

End-User License Agreement 691