- Acknowledgments p. xi
- Introduction p. xv
- Part 1 Building a Multisystem Tiger Box p. 1
- Chapter 1 Basic Windows 2000/Windows 2000 Server Installation and Configuration p. 11
- Launching Windows 2000 Server p. 11
- Basic Windows 2000/Windows 2000 Server Configuration p. 15
- Active Directory p. 16
- TCP/IP Customization p. 40
- Domain Name Service p. 46
- Chapter 2 Basic Linux and Solaris Installations and Configurations p. 53
- NIX Minimum System Requirements (Intel-Based) p. 53
- Installing and Configuring Red Hat Linux p. 54
- Installing and Configuring Solaris 8 p. 64
- Installation Completion p. 69
- Chapter 3 Mac OS X Tiger Box Solutions p. 71
- Minimum System Requirements: Step 1 p. 71
- Installing Mac OS X: Step 2 p. 72
- Installing OS X p. 72
- Upgrading to OS X p. 73
- Installing Developer Tools: Step 3 p. 73
- Downloading the Software p. 73
- Installing and Configuring a Port Scanner Infrastructure: Step 4 p. 76
- Installing Netscape p. 81
- Enabling the Root Account p. 81
- Modifying the PATH p. 82
- Nessus Security Scanner Example Configuration p. 83
- Logging In with the Client p. 91
- Conclusion p. 92
- Chapter 4 Installing and Configuring a Testing Target p. 93
- Minimum Hardware Requirements p. 93
- Installation Methods p. 94
- Server Licensing p. 95
- Server Types p. 96
- Step-by-Step Installation p. 97
- Logging In p. 99
- Optional Services for Your Testing Target p. 100
- Installing WINS p. 100
- Setting Preferences for WINS Manager p. 102
- Configuring a WINS Server p. 103
- WINS Static Mappings p. 104
- WINS Database p. 106
- Installing DNS p. 106
- DNS Zones, Hosts, and Records p. 108
- Internet Information Server Step by Step p. 110

- IIS Installation and Configuration p. 110
- IIS Administration Utility p. 111
- Conclusion p. 120
- Part 2 Using Security Analysis Tools for Your Windows-Based Tiger Box Operating System p. 121
- Chapter 5 Cerberus Internet Scanner p. 135
- System Requirements p. 136
- Installation p. 136
- Target Configuration p. 137
- Vulnerability Scanning p. 146
- Reporting p. 147
- Chapter 6 CyberCop Scanner p. 157
- System Requirements p. 158
- Installation p. 158
- Initial Configuration and Product Update p. 159
- Welcome to Update p. 163
- Setup Configuration Options p. 164
- Target Configuration p. 170
- Selecting Modules for a Scan p. 170
- Vulnerability Scanning p. 175
- Performing Intrusion Detection System Software Tests p. 176
- Advanced Software Utilities p. 179
- CASL p. 180
- Creating and Sending an Example Packet p. 182
- Crack p. 184
- SMB Grind p. 186
- Reporting p. 188
- Network Map p. 190
- Output File p. 191
- Example Report p. 192
- Chapter 7 Internet Scanner p. 199
- System Requirements p. 199
- Installation p. 200
- Starting Internet Scanner for the First Time p. 200
- Command-Line Option p. 201
- Target Configuration p. 202
- Vulnerability Scanning p. 209
- Scanning from the GUI Mode p. 209
- Scanning from the Console Mode p. 210
- Scanning from the Command-Line Mode p. 211
- Reporting p. 212
- Sample Report p. 214
- Chapter 8 Security Threat Avoidance Technology Scanner p. 231
- System Requirements p. 233

- Installation p. 233
- Starting STAT Scanner for the First Time p. 234
- Target Configuration p. 236
- Target Selection p. 237
- Vulnerability Selection p. 238
- Vulnerability Scanning p. 239
- Command-Line Usage p. 242
- Vulnerability Display p. 243
- Reporting p. 245
- Sample Report p. 246
- Chapter 9 TigerSuite 4.0 p. 257
- Installation p. 257
- Local Installation Method p. 258
- Mobile Installation Method p. 261
- Program Modules p. 261
- System Status Modules p. 262
- Hardware Modules p. 262
- System Status Internetworking Modules p. 265
- TigerBox Toolkit p. 269
- TigerBox Tools p. 269
- TigerBox Scanners p. 275
- TigerBox Penetrators p. 277
- TigerBox Simulators p. 281
- Using the Session Sniffers p. 283
- PortSpy Communication Sniffer p. 283
- TigerWipe Active Processes p. 285
- Practical Application p. 286
- Tracing Back with TigerSuite p. 286
- Part 3 Using Security Analysis Tools for NIX and Mac OS X p. 291
- Chapter 10 hping/2 p. 315
- Idle Host Scanning and IP Spoofing p. 316
- System Requirements p. 325
- Linux Installation and Configuration p. 326
- Other Installations p. 329
- Using hping/2 p. 329
- Chapter 11 Nessus Security Scanner p. 339
- System Requirements p. 340
- Installation and Configuration p. 341
- Automatic Installation p. 346
- Configuring Nessus Security Scanner p. 347
- Starting the Server Daemon p. 350
- Additional Notes for Linux and Solaris Users p. 354
- For Mac OS X Users p. 355
- Vulnerability Scanning p. 356

- Plugins p. 358
- Scan Options p. 359
- Target Configuration p. 360
- Reporting p. 362
- Chapter 12 Nmap p. 371
- System Requirements p. 373
- Installation and Configuration p. 373
- Other Installations p. 380
- For Mac OS X Users p. 380
- Using Nmap p. 382
- TCP Scanning p. 383
- UDP Scanning p. 384
- Half-Open (Stealth) Scanning p. 384
- Operating System Fingerprinting p. 385
- Mixing It Up p. 391
- Chapter 13 SAINT p. 393
- System Requirements p. 393
- Installation and Configuration p. 394
- Vulnerability Scanning with SAINT p. 398
- SAINT Home p. 403
- Data Management p. 403
- Configuration Management p. 404
- Target Selection p. 404
- Reporting p. 407
- Vulnerabilities p. 408
- Host Information p. 409
- Severity Levels p. 410
- Using SAINT Remotely p. 411
- The config/passwd File p. 412
- The Command-Line Interface p. 413
- Scheduling Scans Using cron p. 414
- Summing Up p. 415
- Chapter 14 SARA p. 417
- System Requirements p. 418
- Installation and Configuration p. 418
- Advanced Configurations p. 423
- SARA Database Format p. 424
- Vulnerability Scanning p. 426
- Target Configuration and Starting a Scan p. 429
- From the Command Line p. 431
- Reporting p. 432
- Part 4 Vulnerability Assessment p. 439
- Chapter 15 Comparative Analysis p. 441
- Target Network Specifications p. 441

- Windows NT Server 4.0 p. 442
- Red Hat Linux 7.3 Professional p. 444
- Sun Solaris 8 SPARC p. 445
- NT and NIX Auditing Checklists p. 446
- Windows NT System Security Checklist p. 446
- Vulnerability Scanner Results and Comparison p. 469
- What's Next p. 477
- Firewalls and Intrusion Detection System Software p. 477
- Network Monitors p. 477
- Appendix A Linux/Unix Shortcuts and Commands p. 479
- Linux Essential Keyboard Shortcuts and Sanity Commands p. 479
- Additional KDE Keyboard Shortcuts p. 483
- System Info p. 485
- File Management p. 491
- Process Control p. 493
- Administration Commands p. 495
- Hard Drive/Floppy Disk Utilities p. 502
- Management of User Accounts and File Permissions p. 505
- Accessing Drives/Partitions p. 508
- Network Administration Tools p. 509
- Appendix B What's on the CD-ROM p. 513
- Index p. 523