

Network Security: A Practical Approach

Jan L. Harrington



AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Morgan Kaufmann is an imprint of Elsevier

MK
MORGAN KAUFMANN PUBLISHERS

Contents

Preface xi

Chapter 1: In the Beginning ... 1

- 1.0 Introduction 2
- 1.1 Defining Security 2
- 1.2 The Two Views of Network Security 3
 - 1.2.1 Sources of External Threats 3
 - 1.2.2 Sources of Internal Threats 7
- 1.3 The Organizational Security Process 10
 - 1.3.1 Top Management Support 10
 - 1.3.2 How Secure Can You Be? 12
 - 1.3.3 The Importance of a Security Policy 12
 - 1.3.4 Legal Issues 14
 - 1.3.5 Security Personnel 18
 - 1.3.6 Outsourcing Security 24
- 1.4 Preparing a Security Policy 25
- 1.5 Security Audits 31
- 1.6 Summary 33

Chapter 2: Basic Security Architecture 35

- 2.0 Introduction 36
- 2.1 Secure Network Layouts 36
- 2.2 Firewalls 39
 - 2.2.1 Packet Filtering Firewalls 41

- 2.2.2 Stateful Firewalls 42
- 2.2.3 Application Proxy Firewalls 43
- 2.2.4 Comparing Types of Firewalls 43
- 2.3 Hands On: Setting File and Directory Permissions 45
 - 2.3.1 Windows 46
 - 2.3.2 UNIX 47
 - 2.3.3 Mac OS X 51
- 2.4 Summary 51

Chapter 3: Physical Security 55

- 3.0 Introduction 56
- 3.1 Dealing with Theft and Vandalism 56
- 3.2 Protecting the System Console 59
- 3.3 Managing System Failure 60
 - 3.3.1 Backup Solutions 60
 - 3.3.2 Power Protection 69
- 3.4 Hands On: Providing Physical Security 72
 - 3.4.1 Physical Solutions 73
 - 3.4.2 Disaster Recovery Drills 76
- 3.5 Summary 78

Chapter 4: Information Gathering 79

- 4.0 Introduction 80
- 4.1 Social Engineering 80
 - 4.1.1 Electronic Social Engineering: Phishing 82
- 4.2 Using Published Information 84
- 4.3 Port Scanning 91
- 4.4 Network Mapping 94
- 4.5 Hands On 97
 - 4.5.1 Limiting Published Information 98
 - 4.5.2 Disabling Unnecessary Services and Closing Ports 98
 - 4.5.3 Opening Ports on the Perimeter and Proxy Serving 103
- 4.6 Summary 106

Chapter 5: Gaining and Keeping Root Access 109

- 5.0 Introduction 110
- 5.1 Root Kits 110
 - 5.1.1 Root Kit Threat Level 111
 - 5.1.2 How Root Kits Work 113
- 5.2 Brute Force Entry Attacks and Intrusion Detection 114
 - 5.2.1 Examining System Logs 115

- 5.2.2 Intrusion Detection Software 120
- 5.2.3 Intrusion Prevention Software 122
- 5.2.4 Honeypots 123
- 5.3 Buffer Overflow Attacks 123
- 5.4 Hands On 125
 - 5.4.1 Viewing and Configuring Windows Event Logs 126
 - 5.4.2 Patches and Patch Management 127
- 5.5 Summary 130

Chapter 6: Spoofing 133

- 6.0 Introduction 134
- 6.1 TCP Spoofing 134
- 6.2 DNS Spoofing 138
- 6.3 IP (and E-Mail) Spoofing 142
- 6.4 Web Spoofing 145
- 6.5 Hands On 148
 - 6.5.1 Detecting Spoofed E-mail 149
 - 6.5.2 Detecting Spoofed Web Sites 153
- 6.6 Summary 156

Chapter 7: Denial of Service Attacks 161

- 7.0 Introduction 162
- 7.1 Single Source DoS Attacks 162
 - 7.1.1 SYN Flood Attacks 162
 - 7.1.2 Ping of Death 164
 - 7.1.3 Smurf 164
 - 7.1.4 UDP Flood Attacks 165
- 7.2 Distributed DoS Attacks 165
 - 7.2.1 Tribe Flood Network 166
 - 7.2.2 Trinoo 166
 - 7.2.3 Stacheldraht 168
- 7.3 Hands On 168
 - 7.3.1 Using an IDS to Detect a DoS Attack 169
 - 7.3.2 Using System Logs to Detect a DoS Attack 170
 - 7.3.3 Handling a DoS Attack in Progress 171
 - 7.3.4 DoS Defense Strategies 176
 - 7.3.5 Finding Files 177
- 7.4 Summary 178

Chapter 8: Malware 181

- 8.0 Introduction 182

- 8.1 A Bit of Malware History 183
- 8.2 Types of Malware Based on Propagation Methods 183
- 8.3 Hands On 192
 - 8.3.1 “Virus” Scanners 192
 - 8.3.2 Dealing with Removable Media 199
 - 8.3.3 Lockdown Schemes 201
- 8.4 Summary 202

Chapter 9: User and Password Security 205

- 9.0 Introduction 206
- 9.1 Password Policy 206
- 9.2 Strong Passwords 207
- 9.3 Password File Security 209
 - 9.3.1 Windows 210
 - 9.3.2 UNIX 213
- 9.4 Password Audits 214
 - 9.4.1 UNIX: John the Ripper 214
 - 9.4.2 Windows: L0phtCrack 215
- 9.5 Enhancing Password Security with Tokens 217
- 9.6 Hands On: Password Management Software 218
 - 9.6.1 Centralized Password Management 218
 - 9.6.2 Individual Password Management 219
- 9.7 Summary 223

Chapter 10: Remote Access 225

- 10.0 Introduction 226
- 10.1 Remote Access Vulnerabilities 226
 - 10.1.1 Dial-In Access 226
 - 10.1.2 Remote Control Software 228
 - 10.1.3 Remote Access Commands 230
- 10.2 VPNs 234
- 10.3 Remote User Authentication 240
 - 10.3.1 RADIUS 240
 - 10.3.2 Kerberos 241
 - 10.3.3 CHAP and MS-CHAP 242
- 10.4 Hands On: OS VPN Support 243
 - 10.4.1 Windows VPN Support 243
 - 10.4.2 Macintosh OS X VPN Support 252
- 10.5 Summary 258

Chapter 11: Wireless Security 259

- 11.0 Introduction 260
- 11.1 Wireless Standards 261
 - 11.1.1 802.11 Wireless Standards 261
 - 11.1.2 Bluetooth 263
 - 11.1.3 The Forthcoming 802.16 264
- 11.2 Wireless Network Vulnerabilities 265
 - 11.2.1 Signal Bleed and Insertion Attacks 265
 - 11.2.2 Signal Bleed and Interception Attacks 266
 - 11.2.3 SSID Vulnerabilities 266
 - 11.2.4 Denial of Service Attacks 267
 - 11.2.5 Battery Exhaustion Attacks 267
- 11.3 Wireless Security Provisions 268
 - 11.3.1 802.11x Security 268
 - 11.3.2 Bluetooth Security 272
- 11.4 Hands On: Securing Your 802.11x Wireless Network 273
- 11.5 Summary 275

Chapter 12: Encryption 279

- 12.0 Introduction 280
- 12.1 To Encrypt or Not to Encrypt 280
- 12.2 Single Key Encryption Schemes 281
 - 12.2.1 Substitution Cyphers 281
 - 12.2.2 Single-Key Encryption Algorithms 284
 - 12.2.3 Key Management Problems 288
- 12.3 Two-Key Encryption Schemes 288
 - 12.3.1 The Mathematics of Public Key Encryption 289
- 12.4 Combining Single- and Two-Key Encryption 292
- 12.5 Ensuring Message Integrity 292
 - 12.5.1 Message Digest Algorithms 294
 - 12.5.2 Checksums 294
- 12.6 Message Authentication and Digital Certificates 297
 - 12.6.1 Authenticating with PKE Alone 297
 - 12.6.2 Authenticating with Digital Certificates 297
- 12.7 Composition and Purpose of PKI 299
- 12.8 Hands On 300
 - 12.8.1 Third-Party Certificate Authorities 300
 - 12.8.2 Encryption Software 301
- 12.9 Summary 316

Appendix A: The TCP/IP Protocol Stack 319

- A.0 Introduction 320
- A.1 The Operation of a Protocol Stack 320
- A.2 The Application Layer 322
- A.3 The Transport Layer 323
 - A.3.1 TCP 324
 - A.3.2 UDP 326
- A.4 The Internet Layer 327
- A.5 The Logical Link Control Layer 330
- A.6 The MAC Layer 330
- A.7 The Physical Layer 332

Appendix B: TCP and UDP Ports 335

- B.0 Well-Known Ports 336
- B.1 Registered Ports 340
- B.2 Port List References 341

Appendix C: Security Update Sites 343

- C.0 Professional Security Update Sites 344
- C.1 Other Sites of Interest 344

Glossary 347

Index 359

Photo Credits 366