

Network Intrusion Detection

Third Edition

Stephen Northcutt
Judy Novak

**New
Riders**

www.newriders.com

201 West 103rd Street, Indianapolis, Indiana 46290

An Imprint of Pearson Education

Boston • Indianapolis • London • Munich • New York • San Francisco



TABLE OF CONTENTS

TCP/IP

- 1 **IP Concepts** 3
 - The TCP/IP Internet Model 4
 - Packaging (Beyond Paper or Plastic) 7
 - Addresses 11
 - Service Ports 15
 - IP Protocols 16
 - Domain Name System 18
 - Routing: How You Get There from Here 19
 - Summary 20

- 2 **Introduction to TCPdump and TCP** 23
 - TCPdump 24
 - Introduction to TCP 31
 - TCP Gone Awry 38
 - Summary 42

- 3 **Fragmentation** 43
 - Theory of Fragmentation 44
 - Malicious Fragmentation 53
 - Summary 56

- 4 **ICMP** 57
 - ICMP Theory 58
 - Mapping Techniques 61
 - Normal ICMP Activity 65
 - Malicious ICMP Activity 69
 - To Block or Not to Block 76
 - Summary 78

5 Stimulus and Response 79

- The Expected 81
- Protocol Benders 88
- Abnormal Stimuli 92
- Summary 10

6 DNS 103

- Back to Basics: DNS Theory 104
- Using DNS for Reconnaissance 115
- Tainting DNS Responses 119
- Summary 122

II Traffic Analysis**7 Packet Dissection Using
TCPdump 125**

- Why Learn to Do Packet Dissection? 127
- Sidestep DNS Queries 129
- Introduction to Packet Dissection Using
TCPdump 131
- Where Does the IP Stop and the Embedded
Protocol Begin? 133
- Other Length Fields 133
- Increasing the Snaplen 135
- Dissecting the Whole Packet 137
- Freeware Tools for Packet Dissection 139
- Summary 142

8 Examining IP Header Fields 143

- Insertion and Evasion Attacks 143
- IP Header Fields 147
- The More Fragments (MF) Flag 151
- Summary 159

**9 Examining Embedded
Protocol Header Fields 161**

- TCP 161
- UDP 178
- ICMP 181
- Summary 183

10 Real-World Analysis 185

- You've Been Hacked! 186
- Netbus Scan 189
- How Slow Can you Go? 194
- RingZero Worm 197
- Sunnary 200

11 Mystery Traffic 203

- The Event in a Nutshell 204
- The Traffic 204
- DDoS or Scan 205
- Fingerprinting Participant Hosts 210
- Summary 218

III Filters/Rules for Network Monitoring

12 Writing TCPdump Filters 221

- The Mechanics of Writing TCPdump Filters 222
- Bit Masking 224
- TCPdump IP Filters 227
- TCPdump UDP Filters 229
- TCPdump TCP Filters 231
- Summary 236

13 Introduction to Snort and Snort Rules 237

- An Overview of Running Snort 238
- Snort Rules 240
- Summary 248

14 Snort Rules—Part II 249

- Format of Snort Options 250
- Rule Options 250
- Putting It All Together 266
- Summary 269

IV Intrusion Infrastructure

- 15 **Mitnick Attack** 273
 - Exploiting TCP 274
 - Detecting the Mitnick Attack 285
 - Network-Based Intrusion-Detection Systems 286
 - Host-Based Intrusion-Detection Systems 288
 - Preventing the Mitnick Attack 289
 - Summary 290

- 16 **Architectural Issues** 291
 - Events of Interest 292
 - Limits to Observation 294
 - Low-Hanging Fruit Paradigm 296
 - Human Factors Limit Detects 298
 - Severity 300
 - Countermeasures 303
 - Calculating Severity 304
 - Sensor Placement 307
 - Outside Firewall 308
 - Push/Pull 311
 - Analyst Console 312
 - Host- or Network-Based Intrusion Detection 316
 - Summary 318

- 17 **Organizational Issues** 319
 - Organizational Security Model 320
 - Defining Risk 324
 - Risk 326
 - Defining the Threat 332
 - Risk Management Is Dollar Driven 336
 - How Risky Is a Risk? 336
 - Summary 338

18 Automated and Manual Response 339

- Automated Response 341
- Honeypot 347
- Manual Response 349
- Summary 358

**19 Business Case for
Intrusion Detection 359**

- Part One: Management issues 361
- Part Two: Threats and Vulnerabilities 367
- Part Three: Tradeoffs and Recommended
Solution 372
- Repeat the Executive Summary 377
- Summary 378

20 Future Directions 379

- Increasing Threat 379
- Defending Against the Threat 383
- Defense in Depth 388
- Emerging Techniques 392
- Summary 396

V Appendixes

**A Exploits and Scans
to Apply Exploits 401**

- False Positives 401
- IMAP Exploits 409
- Scans to Apply Exploits 413
- Single Exploit, Portmap 417
- Summary 423

B Denial of Service 425

- Brute-Force Denial-of-Service Traces 426
- Elegant Kills 430
- nmap 433
- Distributed Denial-of-Service Attacks 435
- Summary 438

Detection of Intelligence**Gathering 439**

Network and Host Mapping 440

NetBIOS-Specific Traces 450

Stealth Attacks 452

Measuring Response Time 457

Worms as Information Gatherers 460

Summary 464

Index 465