Contents

Preface *xiii*

Acknowledgments *xxi*

About the Authors *xxiii*

1 Honeypot and Networking Background 1

1.1 Brief TCP/IP Introduction 1

1.2 Honeypot Background 7

1.2.1 High-Interaction Honeypots 9

1.2.2 Low-Interaction Honeypots 10

1.2.3 Physical Honeypots 11

1.2.4 Virtual Honeypots 11

1.2.5 Legal Aspects 12

1.3 Tools of the Trade 13

1.3.1 Tcpdump 13

1.3.2 Wireshark 15

1.3.3 Nmap 16

2 High-Interaction Honeypots 19

2.1 Advantages and Disadvantages 20

2.2 VMware 22

2.2.1 Different VMware Versions 25

2.2.2 Virtual Network with VMware 26

2.2.3 Setting Up a Virtual High-Interaction Honeypot 29

2.2.4 Creating a Virtual Honeypot 33

2.2.5 Adding Additional Monitoring Software 37

2.2.6 Connecting the Virtual Honeypot to the Internet 39

2.2.7 Building a Virtual High-Interaction Honeynet 40

2.3 User-Mode Linux 41

2.3.1 Overview 41

2.3.2 Installation and Setup 42

2.3.3 Runtime Flags and Configuration 46
2.3.4 Monitoring UML-Based Honeypots 50
2.3.5 Connecting the Virtual Honeypot to the Internet 51
2.3.6 Building a Virtual High-Interaction Honeynet 52
2.4 Argos 52
2.4.1 Overview 53
2.4.2 Installation and Setup for Argos Honeypots 54
2.5 Safeguarding Your Honeypots 62
2.5.1 Honeywall 63
2.6 Summary 69

3 Low-Interaction Honeypots 71
3.1 Advantages and Disadvantages 72
3.2 Deception Toolkit 73
3.3 LaBrea 74
3.3.1 Installation and Setup 75
3.3.2 Observations 81
3.4 Tiny Honeypot 81
3.4.1 Installation 82
3.4.2 Capture Logs 83
3.4.3 Session Logs 85
3.4.4 Netfilter Logs 85
3.4.5 Observations 86
3.5 GHH — Google Hack Honeypot 87
3.5.1 General Installation 87
3.5.2 Installing the Transparent Link 91
3.5.3 Access Logging 92
3.6 PHP.HoP — A Web-Based Deception Framework 94
3.6.1 Installation 95
3.6.2 HipHop 96
3.6.3 PhpMyAdmin 97
3.7 Securing Your Low-Interaction Honeypots 98
3.7.1 Chroot Jail 98
3.7.2 Systrace 101
3.8 Summary 103

4 Honeyd — The Basics 105
4.1 Overview 106
4.1.1 Features 107
4.1.2 Installation and Setup 108

4.2 Design Overview 109
4.2.1 Interaction Only via the Network 111
4.2.2 Multiple IP Addresses 111
4.2.3 Deceiving Fingerprinting Tools 111
4.3 Receiving Network Data 112
4.4 Runtime Flags 114
4.5 Configuration 115
4.5.1 create 117
4.5.2 set 117
4.5.3 add 121
4.5.4 bind 123
4.5.5 delete 124
4.5.6 include 125
4.6 Experiments with Honeyd 125
4.6.1 Experimenting with Honeyd Locally 125
4.6.2 Integrating Virtual Honeypots into Production Networks 128
4.7 Services 129
4.8 Logging 131
4.8.1 Packet-Level Logging 131
4.8.2 Service-Level Logging 133
4.9 Summary 134

5 Honeyd — Advanced Topics 135
5.1 Advanced Configuration 136
5.1.1 set 136
5.1.2 tarpit 137
5.1.3 annotate 138
5.2 Emulating Services 139
5.2.1 Scripting Languages 139
5.2.2 SMTP 139
5.3 Subsystems 142
5.3.1 Optimizing Subsystems 145
5.4 Internal Python Services 146
5.5 Dynamic Templates 148
5.6 Routing Topology 150
5.7 Honeydstats 154
5.8 Honeydctl 156
5.9 Honeycomb 158
5.10 Performance 160
5.11 Summary 161

6 Collecting Malware with Honeypots 163

6.1 A Primer on Malicious Software 164

6.2 Nepenthes — A Honeypot Solution to Collect Malware 165

6.2.1 Architecture of Nepenthes 167

6.2.2 Limitations 176

6.2.3 Installation and Setup 177

6.2.4 Configuration 179

6.2.5 Command Line Flags 181

6.2.6 Assigning Multiple IP Addresses 183

6.2.7 Flexible Deployment 185

6.2.8 Capturing New Exploits 186

6.2.9 Implementing Vulnerability Modules 187

6.2.10 Results 188

6.2.11 Lessons Learned 196

6.3 Honeytrap 197

6.3.1 Overview 197

6.3.2 Installation and Configuration 200

6.3.3 Running Honeytrap 203

6.4 Other Honeypot Solutions for Learning About Malware 204

6.4.1 Multipot 204

6.4.2 HoneyBOT 205

6.4.3 Billy Goat 205

6.4.4 Learning About Malicious Network Traffic 206

6.5 Summary 207

7 Hybrid Systems 209

7.1 Collapsar 211

7.2 Potemkin 214

7.3 RolePlayer 220

7.4 Research Summary 224

7.5 Building Your Own Hybrid Honeypot System 224

7.5.1 NAT and High-Interaction Honeypots 224

7.5.2 Honeyd and High-Interaction Honeypot 228

7.6 Summary 230

8 Client Honeypots 231

8.1 Learning More About Client-Side Threats 232

8.1.1 A Closer Look at MS04-040 233

8.1.2 Other Types of Client-Side Attacks 236

8.1.3 Toward Client Honeypots 238

8.2 Low-Interaction Client Honeypots 241

8.2.1 Learning About Malicious Websites 241
8.2.2 HoneyC 246
8.3 High-Interaction Client Honeypots 253
8.3.1 Design of High-Interaction Client Honeypots 254
8.3.2 HoneyClient 258
8.3.3 Capture-HPC 260
8.3.4 HoneyMonkey 262
8.4 Other Approaches 263
8.4.1 Studying Spyware on the Internet 264
8.4.2 SpyBye 267
8.4.3 SiteAdvisor 270
8.4.4 Further Research 271
8.5 Summary 272

9 Detecting Honeypots 273
9.1 Detecting Low-Interaction Honeypots 274
9.2 Detecting High-Interaction Honeypots 280
9.2.1 Detecting and Disabling Sebek 281
9.2.2 Detecting the Honeywall 285
9.2.3 Circumventing Honeynet Logging 286
9.2.4 VMware and Other Virtual Machines 289
9.2.5 QEMU 297
9.2.6 User-Mode Linux 298
9.3 Detecting Rootkits 302
9.4 Summary 305

10 Case Studies 307
10.1 Blast-o-Mat: Using Nepenthes to Detect Infected Clients 308
10.1.1 Motivation 309
10.1.2 Nepenthes as Part of an Intrusion Detection System 311
10.1.3 Mitigation of Infected Systems 312
10.1.4 A Modern Trojan: Haxdoor 316
10.1.5 Lessons Learned with Blast-o-Mat 320
10.1.6 Lightweight IDS Based on Nepenthes 321
10.1.7 SURFnet IDS 325
10.2 Search Worms 327
10.3 Red Hat 8.0 Compromise 332
10.3.1 Attack Summary 334
10.3.2 Attack Timeline 335
10.3.3 Tools Involved 338
10.3.4 Attack Evaluation 343

10.4 Windows 2000 Compromise 343
10.4.1 Attack Summary 344
10.4.2 Attack Timeline 345
10.4.3 Tools Involved 347
10.4.4 Attack Evaluation 350
10.5 SUSE 9.1 Compromise 351
10.5.1 Attack Summary 351
10.5.2 Attack Timeline 352
10.5.3 Tools Involved 354
10.5.4 Attack Evaluation 356
10.6 Summary 357

11 Tracking Botnets 359
11.1 Bot and Botnet 101 360
11.1.1 Examples of Bots 362
11.1.2 Spyware in the Form of Bots 366
11.1.3 Botnet Control Structure 369
11.1.4 DDoS Attacks Caused by Botnets 372
11.2 Tracking Botnets 373
11.2.1 Observing Botnets 375
11.3 Case Studies 376
11.3.1 Mocbot and MS06-040 381
11.3.2 Other Observations 384
11.4 Defending Against Bots 387
11.5 Summary 390

12 Analyzing Malware with CWSandbox 391
12.1 CWSandbox Overview 392
12.2 Behavior-Based Malware Analysis 394
12.2.1 Code Analysis 394
12.2.2 Behavior Analysis 395
12.2.3 API Hooking 396
12.2.4 Code Injection 400
12.3 CWSandbox — System Description 401
12.3.1 Architecture 402
12.4 Results 405
12.4.1 Example Analysis Report 406
12.4.2 Large-Scale Analysis 411
12.5 Summary 413

Bibliography 415

Index 423