
CONTENTS

	Foreword: Giving the Hackers a Kick Where It Hurts	xv
	Preface	xix
Chapter 1	The Sting: My Fascination with Honeypots	I
	The Lure of Honeypots	3
	How I Got Started with Honeypots	5
	Perceptions and Misconceptions of Honeypots	9
	Summary	9
	References	10
Chapter 2	The Threat: Tools, Tactics, and Motives of Attackers	II
	Script Kiddies and Advanced Blackhats	11
	Everyone Is a Target	12
	Methods of Attackers	13
	Targets of Opportunity	14
	Targets of Choice	25
	Motives of Attackers	27
	Adapting and Changing Threats	29
	Summary	30
	References	31

Chapter 3	History and Definition of Honeypots	33
	The History of Honeypots	33
	Early Publications	34
	Early Products	36
	Recent History: Honeypots in Action	38
	Definitions of Honeypots	40
	How Honeypots Work	41
	Two Examples of Honeypots	42
	Types of Honeypots	44
	Summmary	46
	References	46
Chapter 4	The Value of Honeypots	49
	Advantages of Honeypots	49
	Data Value	49
	Resources	51
	Simplicity	52
	Return on Investment	52
	Disadvantages of Honeypots	53
	Narrow Field of View	53
	Fingerprinting	54
	Risk	55
	The Role of Honeypots in Overall Security	55
	Production Honeypots	55
	Research Honeypots	68
	Honeypot Policies	70
	Summary	70
	References	71
Chapter 5	Classifying Honeypots by Level of Interaction	73
	Tradeoffs Between Levels of Interaction	74
	Low Interaction Honeypots	78
	Medium-Interaction Honeypots	80
	High-Interaction Honeypots	81
	An Overview of Six Honeypots	83
	BackOfficer Friendly	83
	Specter	84
	Honeyd	84

	Homemade	84
	ManTrap	85
	Honeynets	85
	Summary	86
	Reference	86
Chapter 6	BackOfficer Friendly	87
	Overview of BOF	87
	The Value of BOF	91
	How BOF Works	93
	Installing, Configuring, and Deploying BOF	95
	Information Gathering and Alerting Capabilities	100
	Risk Associated with BOF	102
	Summary	103
	Tutorial	103
	Step 1—Installation	104
	Step 2—Configure	104
	Step 3—Netstat	105
	Step 4—Attack System	105
	Step 5—Review Alerts	107
	Step 6—Save Alerts	107
	References	108
Chapter 7	Specter	109
	Overview of Specter	109
	The Value of Specter	112
	How Specter Works	115
	Installing and Configuring Specter	119
	Operating System	120
	Character	121
	Services	123
	Intelligence, Traps, Password Types, and Notification	124
	Additional Options	126
	Starting the Honeypot	127
	Deploying and Maintaining Specter	127
	Information-Gathering and Alerting Capabilities	129
	Short Mail	129
	Alert Mail	130

	Log Analyzer	132
	Event Log	133
	Syslog	134
	Intelligence Gathering	135
	Risk Associated with Specter	137
	Summary	138
	References	139
Chapter 8	Honeyd	141
	Overview of Honeyd	142
	Value of Honeyd	143
	How Honeyd Works	145
	Blackholing	146
	ARP Spoofing	147
	ARP Proxy	153
	Responding to Attacks	154
	Installing and Configuring Honeyd	157
	Deploying and Maintaining Honeyd	162
	Information Gathering	163
	Risk Associated with Honeyd	165
	Summary	165
	Resources	166
Chapter 9	Homemade Honeyd	167
	An Overview of Homemade Honeyd	168
	Port Monitoring Honeyd	169
	The Value of Port Monitoring	170
	How Homemade Port Monitors Work	173
	Risk Associated with Homemade Port Monitors	181
	Jailed Environments	182
	The Value of Jails	184
	How Jails Work	186
	Installing and Configuring Jails	187
	Deploying and Maintaining Jails	188
	Information Gathering with Jails	189
	Risk Associated with Jails	190
	Summary	191
	References	192

Chapter 10	ManTrap	193
	Overview of ManTrap	193
	The Value of ManTrap	195
	Prevention	195
	Detection	196
	Response	198
	Research	198
	Nontraditional Applications	199
	Limitations	199
	How ManTrap Works	200
	Adjustments to the Kernel	201
	How ManTrap Handles the File System	202
	The Resulting Cages and Their Limitations	204
	Installing and Configuring ManTrap	205
	Building the Host System	206
	iButton and Configuration Options	207
	Client Administration	209
	Customizing the Cages	210
	Deploying and Maintaining ManTrap	211
	Information Gathering	214
	Data Capture in Practice: An Example Attack	215
	Viewing Captured Data	218
	Data Capture at the Application Level	220
	File Recovery	221
	Using a Sniffer with ManTrap	222
	Using iButton for Data Integrity	223
	Risk Associated with ManTrap	225
	Summary	227
	References	227
Chapter 11	Honeynets	229
	Overview of Honeynets	229
	The Value of Honeynets	231
	Methods, Motives, and Evolving Tools	232
	Trend Analysis	235
	Incident Response	236
	Test Beds	238
	How Honeynets Work	238
	Controlling Data	239

Capturing Data	240	
Collecting Data	241	
Honeynet Architectures	242	
GenI	242	
GenII	256	
Virtual Honeynets	261	
Sweetening the Honeynet	262	
Deploying and Maintaining Honeynets	263	
Information Gathering: An Example Attack	265	
Risk Associated with Honeynets	274	
Summary	275	
References	276	
Chapter 12	Implementing Your Honeypot	277
Specifying Honeypot Goals	277	
Selecting a Honeypot	280	
Interaction Level	281	
Commercial Versus Homemade Solutions	282	
Platform	283	
Determining the Number of Honeypots	285	
Selecting Locations for Deployment	286	
Placement for Prevention	287	
Placement for Detection	288	
Placement for Response	289	
Placement for Research	290	
Implementing Data Capture	291	
Maximizing the Amount of Data	291	
Adding Redundancy to Data Capture	293	
IP Addresses Versus Resolved Names	295	
Logging and Managing Data	295	
Using NAT	298	
NAT and Private Addressing	298	
The Role of NAT with Honeypots	301	
Mitigating Risk	302	
Mitigating Fingerprinting	305	
Summary	307	
References	308	

Chapter 13	Maintaining Your Honeybot	309
	Alert Detection	310
	Reliability of Alerts	310
	Critical Content	311
	Prioritizing Alerts	312
	Archiving	314
	Response	315
	Determining Reaction Practices and Roles	316
	Documenting Reaction Practices	318
	Remote Access and Data Control	319
	Data Analysis	320
	A Simple Scenario: Low-Interaction Honeybots	320
	A Complex Scenario: High-Interaction Honeybots	325
	Updates	338
	Summary	339
	Resources	339
Chapter 14	Putting It All Together	341
	Honeyp.com	341
	Matching Goals to Honeybot Solutions	343
	Deploying the Honeybots	346
	Maintaining the Honeybots	352
	Surviving and Responding to an Attack	356
	Honeyp.edu	360
	Matching Goals to Honeybot Solutions	361
	Deploying the Honeybot	362
	Maintaining the Honeybot	364
	Analyzing Attacks	365
	Summary	366
	References	366
Chapter 15	Legal Issues	367
	Are Honeybots Illegal?	367
	Precedents	369
	Privacy	371
	The Fourth Amendment	372
	Stored Information: The Electronic Communications Privacy Act	374

Real-Time Interception of Information: The Wiretap Act and the Pen/Trap Statute	374
Entrapment	380
Liability	381
Summary	383
References	383
Resources	384
Chapter 16 Future of Honeypots	387
From Misunderstanding to Acceptance	387
Improving Ease of Use	388
Easier Administration	389
Prepackaged Solutions	390
Closer Integration with Technologies	391
Targeting Honeypots for Specific Purposes	392
Expanding Research Applications	393
Early Warning and Prediction	395
Studying Advanced Attackers	395
Identifying New Threats	396
Deploying in Distributed Environments	396
A Final Caveat	397
Summary	397
References	398
Appendix A BackOfficer Friendly ASCII File of Scans	399
Appendix B Snort Configuration File	407
Appendix C IP Protocols	411
Appendix D Definitions, Requirements, and Standards Document	415
Appendix E Honeynet Logs	423
Index	429