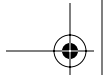


Contents

Preface		xix
Foreword		xxvii
PART I	THE HONEYNET	1
Chapter 1	The Beginning	3
	The HoneyNet Project	3
	The Information Security Environment Before HoneyNets	4
	A Changing Environment: Enter the HoneyPot	5
	A Growing Group: The HoneyNet Project and GenI HoneyNets	7
	HoneyNet Challenges	8
	GenII HoneyNets	10
	The HoneyNet Research Alliance	10
	Managing It All: Lessons We've Learned	12
	Keep It Small	12
	Make It Fun	13
	Have Multiple Activities Going on at All Times	13
	Communicate	14
	Summary	15
Chapter 2	HoneyPots	17
	Definition of HoneyPots	17
	HoneyPot Advantages and Disadvantages	19



CONTENTS

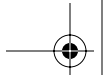
	Types of Honey pots	21
	Low-Interaction Honey pots	21
	Low-Interaction Honey pot Example: Honeyd	23
	High-Interaction Honey pots	25
	High-Interaction Honey pot Example: Symantec Decoy Server	26
	Low-Interaction Versus High-Interaction Honey pots	26
	Uses of Honey pots	27
	Preventing Attacks	28
	Detecting Attacks	29
	Responding to Attacks	29
	Using Honey pots for Research Purposes	30
	Summary	30
Chapter 3	Honey nets	33
	The Value of a Honey net	34
	The Honey net Architecture	35
	Data Control	37
	Data Capture	39
	Data Collection	40
	Risk	41
	Types of Honey nets	44
	Summary	45
Chapter 4	GenI Honey nets	47
	GenI Honey net Architecture	48
	GenI Options for Data Control	50
	GenI Data Control Categories	51
	Technology Choices for GenI Data Control	51
	GenI Technology in Action	52
	GenI Functionality for Data Capture	53
	GenI Data Capture Technology Categories	55
	Data Capture Technology Review	62
	Technology Choices for GenI Data Capture	63
	A Complete GenI Honey net Setup Example	73
	Step 1: Obtain and Prepare the Necessary Hardware and Software	76
	Step 2: Install and Configure the Firewall Machine to Handle Primary Data Control	79
	Step 3: Install and Configure the Firewall IDS Machine to Handle Primary Data Capture	83





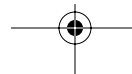
	Step 4: Install, Configure, and Prepare the Victim (Honeynet) Machine	85
	Step 5: Network the Machines Together and Test the Data Control and Data Capture Systems	88
	Step 6: Connect the Honeynet to the Internet	89
	How It All Works Together: Example Attack Capture	90
	Summary	93
Chapter 5	GenII Honeynets	95
	GenII Honeynet Improvements	95
	GenII Honeynet Architecture	96
	GenII Data Control Overview	97
	GenII Data Capture Overview	98
	GenII Data Control	99
	GenII Data Control Implementation: The Honeywall as a Bridging Gateway	99
	Honeywall Management	101
	IPTables	102
	Snort-Inline and IPTables	106
	The Honeywall Data Control Modes	109
	An Abstract Description of Data Control	118
	Data Capture	120
	Data Capture Layer 1: Firewall Logging	122
	Data Capture Layer 2: IDS	124
	Data Capture Layer 3: Honeybots	128
	GenII Honeynet Deployment	133
	The Topology of the ISLab Honeynet	133
	Honeynet Components	136
	Internet Connection	138
	Honeybots	138
	Remote Syslog Server Honeybot	146
	HNRouter	148
	The Honeywall (Honeynet Gateway)	148
	Summary of the Example ISLab Honeynet Deployment	180
	Summary	180
Chapter 6	Virtual Honeynets	183
	What Is a Virtual Honeynet?	183
	Self-Contained Virtual Honeynets	186
	Hybrid Virtual Honeynets	188





CONTENTS

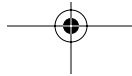
	Possible Implementation Solutions	189
	Option 1: VMware Workstation	190
	Option 2: VMware GSX Server	191
	Option 3: User-Mode Linux	198
	Summary	205
Chapter 7	Distributed Honeynets	207
	What Is a Distributed Honeynet?	208
	Physical Distribution	208
	Honeywall CD-ROM	210
	Deployment Options	211
	Honeypot Farms	212
	The Latency Problem	215
	Setting Up a Honeypot Farm	216
	Technology Review	216
	Honeypot Farm Example Using Linux	218
	Issues Common to All Distributed Honeynets	222
	Summary	223
Chapter 8	Legal Issues	225
	Monitoring Network Users	226
	U.S. Constitutional Provisions	226
	U.S. Statutes	227
	U.S. Contracts and Policies	238
	Laws Outside the U.S.	238
	Crime and the Honeynet	238
	Common Types of Criminal Activity	239
	Protocol for Dealing with Illegal Conduct and Contraband	246
	Entrapment	249
	Do No Harm: Liability to Others	250
	Summary	251
PART II	THE ANALYSIS	253
Chapter 9	The Digital Crime Scene	255
	The Purpose and Value of Data Analysis	255
	Capturing Different Types of Data Within the Honeynet	256
	Firewall Logs	257
	Network Binary Logs	259





CONTENTS

ASCII SESSION Logs	263
Snort Intrusion Detection Alerts	264
System Logs	268
Keystroke Logs	269
The Multiple Layers of Data Analysis and Their Value	272
Network Forensics	273
Computer Forensics	275
Reverse Engineering	276
Summary	279
Chapter 10 Network Forensics	281
Performing Network Forensics	282
Network Traffic 101	282
The IP Header Through the Analyst's Glasses	283
The TCP Header Through the Analyst's Glasses	285
Capturing and Analyzing Network Traffic	288
Snort Basics	289
A Case Study from the HoneyNet	295
Alerts, One April Morning ...	295
Reconstructing the Attack Session	298
Reconstructing the Rootkit	303
The Follow-Through of the Attack	304
Capturing the IRC Chat	305
Analyzing Nonstandard Protocols	307
Detecting Nonstandard Protocols	307
Common Traffic Patterns for Forensic Analysts	311
The Broadcast Pattern	312
The DNS Reverse Lookup Pattern	313
The Proxy Scanning Pattern	313
The 169.254.x.x Pattern	314
The Traceroute Pattern	314
Passive Fingerprinting	316
A TCP Example of Passive Fingerprinting	318
An ICMP Example of Passive Fingerprinting	320
p0f version 2	324
Summary	325





CONTENTS

Chapter 11	Computer Forensics Basics	327
	Overview	328
	Legal Considerations	329
	The Scientific Method	329
	Data Handling	331
	Key Concepts	332
	Analysis Environment	333
	Hardware Considerations	333
	Linux-Based Analysis System	334
	Linux-Based Analysis Tools	335
	Windows-Based Analysis System	340
	Windows-Based Analysis Tools	341
	Data Acquisition	341
	Concepts	342
	Basic Guidelines	342
	Types of Data	344
	Shutdown Considerations	344
	Acquisition Techniques	344
	Summary	346
Chapter 12	UNIX Computer Forensics	347
	Linux Background	348
	Start-Up	348
	Data Hiding	350
	File Systems	351
	Data Acquisition	357
	Volatile Data Acquisition	357
	Nonvolatile Data Acquisition	359
	Disks and Partitions	363
	The Analysis	366
	Setup	367
	Quick Hits	371
	Filling in the Holes	383
	Readiness Steps	403
	Summary	403
Chapter 13	Windows Computer Forensics	405
	Windows File Systems	406
	FAT Basics	406
	The NTFS File System	408

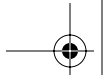




CONTENTS

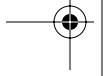
Data Acquisition	412
Volatile Data Acquisition	412
Nonvolatile Data Acquisition	415
Output Options	420
Analysis of the System	422
Establishing Your Setup	422
Viewing the File System Contents	423
Quick Hits	426
Filling in the Holes	430
Analysis with Autopsy and the Sleuth Kit	435
Browsing Files	436
Conducting Keyword Searches	437
File Categorizing	438
File Activity Timelines	439
Recovering Deleted Files	442
Summary	444
Chapter 14 Reverse Engineering	447
Introduction	447
Prerequisites	449
Methods of Analysis	450
Static Analysis	452
Information Gathering	452
Disassembly	456
Symbol Table Regeneration	458
Decompilation Techniques	459
Methodologies for Determining the Order of Decompiling Subroutines	463
Active Analysis	464
Sandboxing the Analysis Environment	464
Black Box Analysis	465
Tracing	466
Antidebugging Tricks	467
Debugging	468
A Walkthrough: The Honeynet Reverse Challenge	469
Information Gathering	470
Obtaining a Disassembly Listing	473
Decompilation/Analysis	474
Summary	482
Further Reading	483





CONTENTS

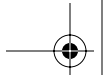
Chapter 15	Centralized Data Collection and Analysis	485
	Centralizing Data	486
	Firewall Logs	487
	IDS Logs	489
	tcpdump Logs	490
	System Logs	492
	Keystroke Logs	494
	Data Centralization Summary	496
	The HoneyNet Security Console	497
	Description	497
	Data Correlation Example	497
	Summary	500
PART III	THE ENEMY	503
Chapter 16	Profiling	505
	A Sociological Analysis of the Whitehat/Blackhat Community	506
	Hacker, Cracker, Blackhat, Whitehat: Identity Crisis and the Power of Labels	507
	Motives Within the Community: A Key to Understanding Individuals, Groups, and Their Actions	509
	Section Summary	519
	The Social Structure of the Whitehat/Blackhat Community	520
	Section Summary	530
	“A Bug’s Life”: The Birth, Life, and Death of an Exploit	531
	The Discovery Stage: Finding a Vulnerability	531
	Techniques in Finding Vulnerabilities	532
	The Process of Finding a Vulnerability	533
	The Birth of the Exploit	534
	The Initial Deployment of an Exploit	536
	Exploit Discovery	536
	Parameters that Contribute to Discovery	537
	Life Cycle of an Exploit	538
	A Dangerous Exchange	540
	The Death of an Exploit	541
	Measuring the Risks	541
	Intelligence-Based Information Security: Profiling and Much More	543
	Characteristics of the Event	544
	Consequences of the Event	545





CONTENTS

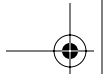
Characteristics of the Blackhat	545
Characteristics of the Target	547
Bringing It All Together	548
Acid Falz	548
IRC Profiling: Another View	551
Summary	556
Chapter 17 Attacks and Exploits: Lessons Learned	557
Overview	558
Types of Attacks	558
Active Attacks	560
Who Is Performing Attacks?	562
Common Steps to Exploiting a System	563
Step 1: Active Reconnaissance	563
Step 2: Exploiting the System	565
Step 3: Keeping Access: Backdoors and Trojans	571
Step 4: Covering One's Tracks	572
Summary	574
Chapter 18 Windows 2000 Compromise and Analysis	575
Honeypot Setup and Configuration	576
Honeynet Setup and Configuration	576
The Attack Log	578
Day 1: 1 March 2003	578
Day 2: 2 March 2003	581
Day 3: 3 March 2003	582
Day 4: 4 March 2003	584
Day 5: 5 March 2003	587
Attack Log Summary	589
Threat Analysis/Profile	591
Blackhats	591
Warez Traders	592
Carders	592
Spammers	592
Lessons Learned for Defense	593
Lessons Learned About Attackers	593
Summary	594



CONTENTS

Chapter 19	Linux Compromise	595
	HoneyNet Setup and Configuration	596
	Forensics Procedure	597
	Indication of Activity	597
	Evidence Collection	598
	Follow-Through of the Attack	607
	Identifying the Exploits	621
	Examining the Downloaded Packages	624
	The Days After	629
	Event Summary	633
	Summary	634
Chapter 20	Example of Solaris Compromise	635
	HoneyNet Setup and Configuration	636
	The Events for Day 1	637
	Detecting the Intrusion	637
	Investigating the Exploit	638
	Reconstructing the Events	644
	Recovering the Intruder's Tools (Day 1)	645
	Recovering the RootKit (Day 1)	646
	Eliminating Competition (Day 1)	650
	Examining IRC Traffic (Day 1)	652
	Locating the Intruder's Denial of Service (DoS) Tool (Day 1)	654
	Day 1 Summary of Events	658
	The Events for Day 3	659
	Examining the DoS Attack (Day 3)	659
	Examining More IRC Traffic (Day 3)	663
	Looking at the SSH Backdoor Access and IPv6 Traffic (Day 3)	666
	The Intruder Setting Up the IPv6 Tunnel (Day 3)	670
	Day 3 Summary of Events	674
	Profiling of the Intruder	674
	Summary	678
Chapter 21	The Future	679
	Distributed HoneyNets	680
	Advanced Threats	681
	Insider Threats	681
	Law Enforcement Applications	682





CONTENTS

Use and Acceptance	682
Blackhat Response	682
Summary	683
Appendix A IPTables Firewall Script	685
Appendix B Snort Configuration	703
Appendix C Swatch Configuration	705
Appendix D Network Configuration Summary	709
Appendix E Honeywall Kernel Configuration	713
Appendix F GenII rc.firewall Configuration	717
Resources and References	721
About the Authors	737
Index	743

