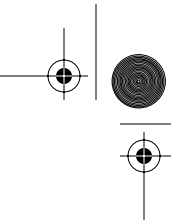


# Contents

Preface		xi
Foreword		xv
Chapter 1	The Battleground	1
<b>PART I</b>	<b>THE HONEYNET</b>	7
Chapter 2	What a Honeynet Is	9
	Honeypots	9
	Honeynets	12
	Value of a Honeynet	13
	The Honeypots in the Honeynet	15
	Summary	17
Chapter 3	How a Honeynet Works	19
	Data Control	20
	Data Capture	30
	Access Control Layer	31
	Network Layer	35
	System Layer	38
	Off-Line Layer	40
	Social Engineering	41
	Risk	42
	Summary	43



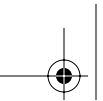


## CONTENTS

---

<b>Chapter 4</b>	<b>Building a Honeynet</b>	<b>45</b>
	Overall Architecture	45
	Data Control	47
	Data Capture	51
	Maintaining a Honeynet and Reacting to Attacks	53
	Summary	54
<b>PART II</b>	<b>THE ANALYSIS</b>	<b>55</b>
<b>Chapter 5</b>	<b>Data Analysis</b>	<b>57</b>
	Firewall Logs	57
	IDS Analysis	60
	System Logs	70
	Summary	73
<b>Chapter 6</b>	<b>Analyzing a Compromised System</b>	<b>75</b>
	The Attack	75
	The Probe	77
	The Exploit	78
	Gaining Access	83
	The Return	88
	Analysis Review	92
	Summary	93
<b>Chapter 7</b>	<b>Advanced Data Analysis</b>	<b>95</b>
	Passive Fingerprinting	95
	The Signatures	97
	The ICMP Example	100
	Forensics	103
	Summary	109
<b>Chapter 8</b>	<b>Forensic Challenge</b>	<b>111</b>
	Images	111
	The Coroner's Toolkit	112
	MAC Times	114
	Deleted Inodes	117
	Data Recovery	119
	Summary	122



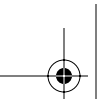


CONTENTS

---

<b>PART III</b>	<b>THE ENEMY</b>	<b>123</b>
<b>Chapter 9</b>	<b>The Enemy</b>	<b>125</b>
	The Threat	125
	The Tactics	126
	The Tools	130
	The Motives	132
	Changing Trends	134
	Summary	137
<b>Chapter 10</b>	<b>Worms at War</b>	<b>139</b>
	The Setup	140
	The First Worm	141
	The Second Worm	144
	The Day After	146
	Summary	149
<b>Chapter 11</b>	<b>In Their Own Words</b>	<b>151</b>
	The Compromise	152
	Reading the IRC Chat Sessions	163
	Day 1, June 4	164
	Day 2, June 5	171
	Day 3, June 6	185
	Day 4, June 7	202
	Day 5, June 8	226
	Day 6, June 9	244
	Day 7, June 10	257
	Analyzing the IRC Chat Sessions	260
	Profiling Review	260
	Psychological Review	262
	Summary	264
<b>Chapter 12</b>	<b>The Future of the Honeynet</b>	<b>267</b>
	Future Developments	267
	Conclusion	270
<b>Appendix A</b>	<b>Snort Configuration</b>	<b>271</b>
	Snort Start-Up Script	271
	Snort Configuration File, snort.conf.	272





## CONTENTS

---

Appendix B	Swatch Configuration File	275
Appendix C	Named NXT HOWTO	277
Appendix D	NetBIOS Scans	285
Appendix E	Source Code for bj.c	297
Appendix F	TCP Passive Fingerprint Database	299
Appendix G	ICMP Passive Fingerprint Database	301
Appendix H	Honeynet Project Members	303
Index		315

