

# CONTENTS

Foreward . . . . .	xvii
Introduction . . . . .	ixx
<b>Part I</b> Introduction to Ethical Disclosure . . . . .	<b>I</b>
<b>Chapter 1</b> Ethics of Ethical Hacking . . . . .	<b>3</b>
References . . . . .	8
How Does This Stuff Relate to an Ethical Hacking Book? . . . . .	8
Vulnerability Assessment . . . . .	9
Penetration Testing . . . . .	10
References . . . . .	11
The Controversy of Hacking Books and Classes . . . . .	11
The Dual Nature of Tools . . . . .	12
References . . . . .	14
Recognizing Trouble When It Happens . . . . .	14
Emulating the Attack . . . . .	15
Where Do Attackers Have Most of Their Fun? . . . . .	16
Security Does Not Like Complexity . . . . .	16
References . . . . .	17
Summary . . . . .	18
Questions . . . . .	18
Answers . . . . .	20
<b>Chapter 2</b> Ethical Hacking and the Legal System . . . . .	<b>23</b>
References . . . . .	24
Addressing Individual Laws . . . . .	24
18 USC Section 1029 . . . . .	24
References . . . . .	27
18 USC Section 1030 . . . . .	27
References . . . . .	32
A State Law Alternative . . . . .	32
References . . . . .	34
18 USC Sections 2510 and 2701 . . . . .	34
References . . . . .	36
Digital Millennium Copyright Act . . . . .	37
References . . . . .	38
Cyber Security Enhancement Act of 2002 . . . . .	38

**Gray Hat Hacking: The Ethical Hacker's Handbook**

X

Summary	39
Questions	40
Answers	42
<b>Chapter 3 Proper and Ethical Disclosure</b>	<b>45</b>
Different Teams and Points of View	46
How Did We Get Here?	47
CERT's Current Process	48
Full Disclosure Policy (RainForest Puppy Policy)	50
Organization for Internet Safety (OIS)	51
Discovery	52
Notification	53
Validation	55
Resolution	58
Release	59
Conflicts Will Still Exist	59
Case Studies	60
Pros and Cons of Proper Disclosure Processes	60
Vendors Paying More Attention	64
So What Should We Do from Here on Out?	65
iDefense	66
References	66
Summary	67
Questions	67
Answers	69
<b>Part II Penetration Testing and Tools</b>	<b>71</b>
<b>Chapter 4 Pen-Testing Process</b>	<b>73</b>
Types of Tests	73
References	75
Ramping Up	75
Building a Team	75
Building a Lab	76
Contracts, Safety, and Staying Out of Jail	77
Assessment Process	78
Assessment Planning	78
On-Site Meeting with the Customer to Kick Off Assessment	79
Penetration Test Process	79
References	81
Red Teaming Process	81
System Test Process	84
Footprinting with lsof	86
References	89
Reporting Out	89

Summary	90
Questions	91
Answers	92
<b>Chapter 5 Beyond Hacking Exposed: Advanced Tools for Today's Hacker</b>	<b>95</b>
Scanning in the "Good Old Days"	96
Paketto Keiretsu (scanrand, paratrace)	96
References	107
Past and Present Forms of Fingerprinting	108
xprobe2	109
References	114
p0f	114
References	118
amap	118
References	122
Winfingerprint	122
Sniffing Tools	125
libpcap and WinPcap	126
References	127
Passive Sniffing vs. Active Sniffing	127
References	134
References	137
Defenses Against Active Sniffing	137
Sniffing for Usernames and Passwords	138
References	139
Sniffing and Hacking LAN Manager Logon Credentials	140
Using the Challenge and Hashes (the Hard Way)	143
Using ettercap (the Easy Way)	144
References	146
Sniffing and Cracking Kerberos	146
Summary	148
Questions	150
Answers	151
<b>Chapter 6 Automated Penetration Testing</b>	<b>153</b>
Python Survival Skills	154
Getting Python	154
Hello, World	154
Python Objects	155
References	160
Automated Penetration Testing Tools	161
Core IMPACT	161
References	164
Immunity CANVAS	165
References	169

**Gray Hat Hacking: The Ethical Hacker's Handbook**

..  
Xii

Metasploit .....	169
References .....	177
Summary .....	177
Questions .....	177
Answers .....	179
<b>Part III</b> Exploits 101 .....	<b>181</b>
<b>Chapter 7</b> Programming Survival Skills .....	<b>183</b>
Programming .....	184
The Problem-Solving Process .....	184
Pseudo-code .....	185
Programmers vs. Hackers .....	187
References .....	188
C Programming Language .....	188
Basic C Language Constructs .....	188
Sample Program .....	193
Compiling with gcc .....	193
References .....	194
Computer Memory .....	194
Random Access Memory (RAM) .....	195
Endian .....	195
Segmentation of Memory .....	195
Programs in Memory .....	196
Buffers .....	197
Strings in Memory .....	197
Pointers .....	197
Putting the Pieces of Memory Together .....	198
References .....	198
Intel Processors .....	199
Registers .....	199
Arithmetic Logic Unit (ALU) .....	199
Program Counter .....	200
Control Unit .....	200
Buses .....	200
References .....	202
Assembly Language Basics .....	202
Machine vs. Assembly vs. C .....	202
AT&T vs. NASM .....	202
Addressing Modes .....	204
Assembly File Structure .....	205
Assembling .....	206
References .....	206

Debugging with gdb	206
gdb Basics	206
Disassembly with gdb	208
References	209
Summary	209
Questions	210
Answers	212
<b>Chapter 8 Basic Linux Exploits</b>	<b>213</b>
Stack Operations	213
Stack Data Structure	214
Operational Implementation	214
Function Calling Procedure	214
References	215
Buffer Overflows	216
Example Buffer Overflow	216
Overflow of meet.c	217
Ramifications of Buffer Overflows	220
References	221
Local Buffer Overflow Exploits	221
Components of the Exploit	222
Exploiting Stack Overflows by Command Line	223
Exploiting Stack Overflows with Generic Exploit Code	225
Exploitation of meet.c	226
Exploiting Small Buffers	227
References	229
Remote Buffer Overflow Exploits	229
Client/Server Model	229
Determining the Remote esp Value	232
Manual Brute Force with Perl	232
References	234
Summary	234
Questions	235
Answers	237
<b>Chapter 9 Advance Linux Exploits</b>	<b>239</b>
Format String Exploits	239
The Problem	240
Reading from Arbitrary Memory	243
Writing to Arbitrary Memory	245
Taking .dtors to root	247
References	250
Heap Overflow Exploits	250
Heap Overflows	251
Memory Allocators (malloc)	252

**Gray Hat Hacking: The Ethical Hacker's Handbook**

**XIV**

dmalloc	253
Exploiting Heap Overflows	257
Alternative Exploits	261
References	261
Memory Protection Schemes	262
Libsafe	262
GRSecurity Kernel Patches and Scripts	262
Stackshield	263
Bottom Line	263
References	264
Summary	264
Questions	265
Answers	267
<b>Chapter 10 Writing Linux Shellcode</b>	<b>269</b>
Basic Linux Shellcode	269
System Calls	270
Exit System Call	272
setreuid System Call	274
Shell-Spawning Shellcode with execve	276
References	279
Port-Binding Shellcode	279
Linux Socket Programming	279
Assembly Program to Establish a Socket	282
Test the Shellcode	284
References	287
Reverse Connecting Shellcode	287
Reverse Connecting C Program	287
Reverse Connecting Assembly Program	288
References	290
Summary	290
Questions	292
Answers	294
<b>Chapter 11 Writing a Basic Windows Exploit</b>	<b>295</b>
Compiling and Debugging Windows Programs	295
Compiling on Windows	295
Debugging on Windows	297
Building a Basic Windows Exploit	306
Summary	313
Questions	314
Answers	315

<b>Part IV</b>	<b>Vulnerability Analysis</b>	<b>317</b>
<b>Chapter 12</b>	<b>Passive Analysis</b>	<b>319</b>
	Ethical Reverse Engineering	319
	References	320
	Why Reverse Engineering?	320
	Reverse Engineering Considerations	321
	Source Code Analysis	321
	Source Code Auditing Tools	322
	The Utility of Source Code Auditing Tools	323
	Manual Source Code Auditing	325
	References	329
	Binary Analysis	329
	Automated Binary Analysis Tools	329
	References	332
	Manual Auditing of Binary Code	332
	References	345
	Summary	345
	Questions	346
	Answers	347
<b>Chapter 13</b>	<b>Advanced Reverse Engineering</b>	<b>349</b>
	Why Try to Break Software?	350
	The Software Development Process	350
	Instrumentation Tools	351
	Debuggers	352
	Code Coverage Tools	354
	Profiling Tools	354
	Flow Analysis Tools	354
	Memory Monitoring Tools	356
	References	361
	Fuzzing	361
	Instrumented Fuzzing Tools and Techniques	362
	A Simple URL Fuzzer	362
	Fuzzing Unknown Protocols	365
	SPIKE	365
	SPIKE Proxy	369
	Sharefuzz	369
	References	370
	Summary	371
	Questions	371
	Answers	373

<b>Chapter 14</b>	<b>From Vulnerability to Exploit</b> .....	<b>375</b>
	Exploitability .....	376
	Debugging for Exploitation .....	376
	References .....	380
	Understanding the Problem .....	380
	Preconditions and Postconditions .....	380
	Repeatability .....	381
	References .....	390
	Documenting the Problem .....	390
	Background Information .....	390
	Circumstances .....	391
	Research Results .....	391
	Summary .....	391
	Questions .....	392
	Answers .....	394
<b>Chapter 15</b>	<b>Closing the Holes: Mitigation</b> .....	<b>397</b>
	Mitigation Alternatives .....	397
	Port Knocking .....	398
	References .....	398
	Migration .....	398
	References .....	399
	Patching .....	400
	Source Code Patching Considerations .....	400
	Binary Patching Considerations .....	402
	References .....	406
	Summary .....	406
	Questions .....	406
	Answers .....	408
	Index.....	411