

ALL ■ IN ■ ONE

# Gray Hat Hacking

The Ethical Hacker's  
Handbook

---

## ABOUT THE AUTHORS

**Shon Harris**, MCSE, CISSP, is the president of Logical Security, an educator and security consultant. She is a former engineer of the U.S. Air Force Information Warfare unit and has published several books and articles on different disciplines within information security. Shon was also recognized as one of the top 25 women in information security by *Information Security Magazine*.

**Allen Harper**, CISSP, is the president and owner of n2netSecurity, Inc. in North Carolina. He retired from the Marine Corps after 20 years. Additionally, he has served as a security analyst for the U.S. Department of the Treasury, Internal Revenue Service, Computer Security Incident Response Center (IRS CSIRC). He speaks and teaches at conferences such as Black Hat.

**Chris Eagle** is the associate chairman of the Computer Science Department at the Naval Postgraduate School (NPS) in Monterey, California. A computer engineer/scientist for 22 years, his research interests include computer network attack and defense, computer forensics, and reverse/anti-reverse engineering. He can often be found teaching at Black Hat or playing capture the flag at Defcon.

**Jonathan Ness**, CHFI, is a lead software security engineer at Microsoft. He and his coworkers ensure that Microsoft's security updates comprehensively address reported vulnerabilities. He also leads the technical response of Microsoft's incident response process that is engaged to address publicly disclosed vulnerabilities and exploits targeting Microsoft software. He serves one weekend each month as a security engineer in a reserve military unit.

*Disclaimer: The views expressed in this book are those of the author and not of the U.S. government or the Microsoft Corporation.*

### About the Technical Editor

**Michael Baucom** is a software engineer working primarily in the embedded software area. The majority of the last ten years he has been writing system software and tools for networking equipment; however, his recent interests are with information security and more specifically securing software. He co-taught Exploiting 101 at Black Hat in 2006. For fun, he has enjoyed participating in capture the flag at Defcon for the last two years.

ALL ■ IN ■ ONE

# Gray Hat Hacking

The Ethical Hacker's  
Handbook  
Second Edition

Shon Harris, Allen Harper, Chris Eagle,  
and Jonathan Ness



New York • Chicago • San Francisco • Lisbon  
London • Madrid • Mexico City • Milan • New Delhi  
San Juan • Seoul • Singapore • Sydney • Toronto

The **McGraw-Hill** Companies

Cataloging-in-Publication Data is on file with the Library of Congress

McGraw-Hill books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. For more information, please write to the Director of Special Sales, Professional Publishing, McGraw-Hill, Two Penn Plaza, New York, NY 10121-2298. Or contact your local bookstore.

### Gray Hat Hacking: The Ethical Hacker's Handbook, Second Edition

Copyright © 2008 by The McGraw-Hill Companies. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

1 2 3 4 5 6 7 8 9 0 FGR FGR 0 1 9 8 7

ISBN 978-0-07-149568-4

MHID 0-07-149568-1

**Sponsoring Editor**

Jane Brownlow

**Editorial Supervisor**

Janet Walden

**Project Manager**

Madhu Bhardwaj,  
International Typesetting and Composition

**Acquisitions Coordinator**

Jennifer Housh

**Technical Editor**

Michael Baucom

**Copy Editor**

Jan Jue

**Proofreader**

Bev Weiler

**Indexer**

Claire Splan

**Production Supervisor**

George Anderson

**Composition**

International Typesetting and Composition

**Illustration**

International Typesetting and Composition

**Art Director, Cover**

Jeff Weeks

**Cover Designer**

Pattie Lee

Information has been obtained by McGraw-Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill, or others, McGraw-Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

To my loving and supporting husband, David Harris,  
who has continual patience with me as I take  
on all of these crazy projects! —*Shon Harris*

To the service members forward deployed around the world.  
Thank you for your sacrifice. —*Allen Harper*

To my wife, Kristen, for all of the support she has given me  
through this and my many other endeavors! —*Chris Eagle*

To Jessica, the most amazing and beautiful person  
I know. —*Jonathan Ness*



## CONTENTS AT A GLANCE

<b>Part I</b>	Introduction to Ethical Disclosure .....	1
<b>Chapter 1</b>	Ethics of Ethical Hacking .....	3
<b>Chapter 2</b>	Ethical Hacking and the Legal System .....	17
<b>Chapter 3</b>	Proper and Ethical Disclosure .....	41
<b>Part II</b>	Penetration Testing and Tools .....	73
<b>Chapter 4</b>	Using Metasploit .....	75
<b>Chapter 5</b>	Using the BackTrack LiveCD Linux Distribution .....	101
<b>Part III</b>	Exploits 101 .....	119
<b>Chapter 6</b>	Programming Survival Skills .....	121
<b>Chapter 7</b>	Basic Linux Exploits .....	147
<b>Chapter 8</b>	Advanced Linux Exploits .....	169
<b>Chapter 9</b>	Shellcode Strategies .....	195
<b>Chapter 10</b>	Writing Linux Shellcode .....	211
<b>Chapter 11</b>	Basic Windows Exploits .....	243
<b>Part IV</b>	Vulnerability Analysis .....	275
<b>Chapter 12</b>	Passive Analysis .....	277
<b>Chapter 13</b>	Advanced Static Analysis with IDA Pro .....	309
<b>Chapter 14</b>	Advanced Reverse Engineering .....	335
<b>Chapter 15</b>	Client-Side Browser Exploits .....	359
<b>Chapter 16</b>	Exploiting Windows Access Control Model for Local Elevation of Privilege .....	387
<b>Chapter 17</b>	Intelligent Fuzzing with Sulley .....	441
<b>Chapter 18</b>	From Vulnerability to Exploit .....	459
<b>Chapter 19</b>	Closing the Holes: Mitigation .....	481

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

---

⋮  
viii

<b>Part V</b>	Malware Analysis .....	497
<b>Chapter 20</b>	Collecting Malware and Initial Analysis .....	499
<b>Chapter 21</b>	Hacking Malware .....	521
	Index .....	537

# CONTENTS

Foreword	xix
Acknowledgments	xxi
<b>Part I</b> Introduction to Ethical Disclosure	<b>I</b>
<b>Chapter 1</b> Ethics of Ethical Hacking	<b>3</b>
How Does This Stuff Relate to an Ethical Hacking Book?	10
The Controversy of Hacking Books and Classes	11
The Dual Nature of Tools	12
Recognizing Trouble When It Happens	13
Emulating the Attack	14
Security Does Not Like Complexity	15
<b>Chapter 2</b> Ethical Hacking and the Legal System	<b>17</b>
Addressing Individual Laws	19
18 USC Section 1029: The Access Device Statute	19
18 USC Section 1030 of The Computer Fraud and Abuse Act	23
State Law Alternatives	30
18 USC Sections 2510, et. Seq. and 2701	32
Digital Millennium Copyright Act (DMCA)	36
Cyber Security Enhancement Act of 2002	39
<b>Chapter 3</b> Proper and Ethical Disclosure	<b>41</b>
You Were Vulnerable for How Long?	45
Different Teams and Points of View	47
How Did We Get Here?	49
CERT's Current Process	50
Full Disclosure Policy (RainForest Puppy Policy)	52
Organization for Internet Safety (OIS)	54
Discovery	55
Notification	55
Validation	57
Resolution	60
Release	62
Conflicts Will Still Exist	62

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

X

Case Studies	62
Pros and Cons of Proper Disclosure Processes	63
iDefense	67
Zero Day Initiative	68
Vendors Paying More Attention	69
So What Should We Do from Here on Out?	70
<b>Part II Penetration Testing and Tools</b>	<b>73</b>
<b>Chapter 4 Using Metasploit</b>	<b>75</b>
Metasploit: The Big Picture	75
Getting Metasploit	75
Using the Metasploit Console to Launch Exploits	76
Exploiting Client-Side Vulnerabilities with Metasploit	83
Using the Meterpreter	87
Using Metasploit as a Man-in-the-Middle Password Stealer	91
Weakness in the NTLM Protocol	92
Configuring Metasploit as a Malicious SMB Server	92
Brute-Force Password Retrieval with the LM Hashes + Challenge	94
Building Your Own Rainbow Tables	96
Downloading Rainbow Tables	97
Purchasing Rainbow Tables	97
Cracking Hashes with Rainbow Tables	97
Using Metasploit to Auto-Attack	98
Inside Metasploit Modules	98
<b>Chapter 5 Using the BackTrack LiveCD Linux Distribution</b>	<b>101</b>
BackTrack: The Big Picture	101
Creating the BackTrack CD	102
Booting BackTrack	103
Exploring the BackTrack X-Windows Environment	104
Writing BackTrack to Your USB Memory Stick	105
Saving Your BackTrack Configurations	105
Creating a Directory-Based or File-Based Module with dir2lzm	106
Creating a Module from a SLAX Prebuilt Module with mo2lzm	106
Creating a Module from an Entire Session of Changes Using dir2lzm	108
Automating the Change Preservation from One Session to the Next	109

Creating a New Base Module with	
All the Desired Directory Contents .....	110
Cheat Codes and Selectively Loading Modules .....	112
Metasploit db_autopwn .....	114
Tools .....	118
<b>Part III</b> Exploits 101 .....	<b>119</b>
<b>Chapter 6</b> Programming Survival Skills .....	<b>121</b>
C Programming Language .....	121
Basic C Language Constructs .....	122
Sample Program .....	126
Compiling with gcc .....	127
Computer Memory .....	128
Random Access Memory (RAM) .....	128
Endian .....	128
Segmentation of Memory .....	129
Programs in Memory .....	129
Buffers .....	130
Strings in Memory .....	130
Pointers .....	130
Putting the Pieces of Memory Together .....	131
Intel Processors .....	132
Registers .....	132
Assembly Language Basics .....	133
Machine vs. Assembly vs. C .....	133
AT&T vs. NASM .....	133
Addressing Modes .....	135
Assembly File Structure .....	136
Assembling .....	137
Debugging with gdb .....	137
gdb Basics .....	137
Disassembly with gdb .....	139
Python Survival Skills .....	139
Getting Python .....	140
Hello World in Python .....	140
Python Objects .....	140
Strings .....	141
Numbers .....	142
Lists .....	143
Dictionaries .....	144
Files with Python .....	144
Sockets with Python .....	146

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

---

..  
XII

<b>Chapter 7 Basic Linux Exploits</b> .....	<b>147</b>
Stack Operations .....	148
Function Calling Procedure .....	148
Buffer Overflows .....	149
Overflow of meet.c .....	150
Ramifications of Buffer Overflows .....	153
Local Buffer Overflow Exploits .....	154
Components of the Exploit .....	155
Exploiting Stack Overflows by Command Line .....	157
Exploiting Stack Overflows with Generic Exploit Code .....	158
Exploiting Small Buffers .....	160
Exploit Development Process .....	162
Real-World Example .....	163
Determine the Offset(s) .....	163
Determine the Attack Vector .....	166
Build the Exploit Sandwich .....	167
Test the Exploit .....	168
<b>Chapter 8 Advanced Linux Exploits</b> .....	<b>169</b>
Format String Exploits .....	169
The Problem .....	170
Reading from Arbitrary Memory .....	173
Writing to Arbitrary Memory .....	175
Taking .dtors to root .....	177
Heap Overflow Exploits .....	180
Example Heap Overflow .....	181
Implications .....	182
Memory Protection Schemes .....	182
Compiler Improvements .....	183
Kernel Patches and Scripts .....	183
Return to libc Exploits .....	185
Bottom Line .....	192
<b>Chapter 9 Shellcode Strategies</b> .....	<b>195</b>
User Space Shellcode .....	196
System Calls .....	196
Basic Shellcode .....	197
Port Binding Shellcode .....	197
Reverse Shellcode .....	199
Find Socket Shellcode .....	200
Command Execution Code .....	201
File Transfer Code .....	202
Multistage Shellcode .....	202
System Call Proxy Shellcode .....	202
Process Injection Shellcode .....	203

Other Shellcode Considerations	204
Shellcode Encoding	204
Self-Corrupting Shellcode	205
Disassembling Shellcode	206
Kernel Space Shellcode	208
Kernel Space Considerations	208
<b>Chapter 10 Writing Linux Shellcode</b>	<b>211</b>
Basic Linux Shellcode	211
System Calls	212
Exit System Call	214
setreuid System Call	216
Shell-Spawning Shellcode with execve	217
Implementing Port-Binding Shellcode	220
Linux Socket Programming	220
Assembly Program to Establish a Socket	223
Test the Shellcode	226
Implementing Reverse Connecting Shellcode	228
Reverse Connecting C Program	228
Reverse Connecting Assembly Program	230
Encoding Shellcode	232
Simple XOR Encoding	232
Structure of Encoded Shellcode	232
JMP/CALL XOR Decoder Example	233
FNSTENV XOR Example	234
Putting It All Together	236
Automating Shellcode Generation with Metasploit	238
Generating Shellcode with Metasploit	238
Encoding Shellcode with Metasploit	240
<b>Chapter 11 Basic Windows Exploits</b>	<b>243</b>
Compiling and Debugging Windows Programs	243
Compiling on Windows	243
Debugging on Windows with Windows Console Debuggers	245
Debugging on Windows with OllyDbg	254
Windows Exploits	258
Building a Basic Windows Exploit	258
Real-World Windows Exploit Example	266
<b>Part IV Vulnerability Analysis</b>	<b>275</b>
<b>Chapter 12 Passive Analysis</b>	<b>277</b>
Ethical Reverse Engineering	277
Why Reverse Engineering?	278
Reverse Engineering Considerations	279

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

**XIV**

Source Code Analysis	279
Source Code Auditing Tools	280
The Utility of Source Code Auditing Tools	282
Manual Source Code Auditing	283
Binary Analysis	289
Manual Auditing of Binary Code	289
Automated Binary Analysis Tools	304
<b>Chapter 13 Advanced Static Analysis with IDA Pro</b>	<b>309</b>
Static Analysis Challenges	309
Stripped Binaries	310
Statically Linked Programs and FLAIR	312
Data Structure Analysis	318
Quirks of Compiled C++ Code	323
Extending IDA	325
Scripting with IDC	326
IDA Pro Plug-In Modules and the IDA SDK	329
IDA Pro Loaders and Processor Modules	332
<b>Chapter 14 Advanced Reverse Engineering</b>	<b>335</b>
Why Try to Break Software?	336
The Software Development Process	336
Instrumentation Tools	337
Debuggers	338
Code Coverage Tools	340
Profiling Tools	341
Flow Analysis Tools	342
Memory Monitoring Tools	343
Fuzzing	348
Instrumented Fuzzing Tools and Techniques	349
A Simple URL Fuzzer	349
Fuzzing Unknown Protocols	352
SPIKE	353
SPIKE Proxy	357
Sharefuzz	357
<b>Chapter 15 Client-Side Browser Exploits</b>	<b>359</b>
Why Client-Side Vulnerabilities Are Interesting	359
Client-Side Vulnerabilities Bypass Firewall Protections	359
Client-Side Applications Are Often Running with Administrative Privileges	360
Client-Side Vulnerabilities Can Easily Target Specific People or Organizations	360

Internet Explorer Security Concepts	361
ActiveX Controls	361
Internet Explorer Security Zones	362
History of Client-Side Exploits and Latest Trends	363
Client-Side Vulnerabilities Rise to Prominence	363
Notable Vulnerabilities in the History of Client-Side Attacks	364
Finding New Browser-Based Vulnerabilities	369
MangleMe	370
AxEnum	372
AxFuzz	377
AxMan	378
Heap Spray to Exploit	383
InternetExploiter	384
Protecting Yourself from Client-Side Exploits	385
Keep Up-to-Date on Security Patches	385
Stay Informed	385
Run Internet-Facing Applications with Reduced Privileges	385
<b>Chapter 16 Exploiting Windows Access Control Model for</b>	
<b>Local Elevation of Privilege</b>	<b>387</b>
Why Access Control Is Interesting to a Hacker	387
Most People Don't Understand Access Control	387
Vulnerabilities You Find Are Easy to Exploit	388
You'll Find Tons of Security Vulnerabilities	388
How Windows Access Control Works	388
Security Identifier (SID)	389
Access Token	390
Security Descriptor (SD)	394
The Access Check	397
Tools for Analyzing Access Control Configurations	400
Dumping the Process Token	401
Dumping the Security Descriptor	403
Special SIDs, Special Access, and "Access Denied"	406
Special SIDs	406
Special Access	408
Investigating "Access Denied"	409
Analyzing Access Control for Elevation of Privilege	417
Attack Patterns for Each Interesting Object Type	418
Attacking Services	418
Attacking Weak DACLs in the Windows Registry	424
Attacking Weak Directory DACLs	428
Attacking Weak File DACLs	433

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

XVI

What Other Object Types Are out There? .....	437
Enumerating Shared Memory Sections .....	437
Enumerating Processes .....	439
Enumerating Other Named Kernel Objects (Semaphores, Mutexes, Events, Devices) .....	439
<b>Chapter 17 Intelligent Fuzzing with Sulley .....</b>	<b>441</b>
Protocol Analysis .....	441
Sulley Fuzzing Framework .....	443
Installing Sulley .....	443
Powerful Fuzzer .....	443
Blocks .....	446
Sessions .....	449
Monitoring the Process for Faults .....	450
Monitoring the Network Traffic .....	451
Controlling VMware .....	452
Putting It All Together .....	452
Postmortem Analysis of Crashes .....	454
Analysis of Network Traffic .....	456
Way Ahead .....	456
<b>Chapter 18 From Vulnerability to Exploit .....</b>	<b>459</b>
Exploitability .....	460
Debugging for Exploitation .....	460
Understanding the Problem .....	466
Preconditions and Postconditions .....	466
Repeatability .....	467
Payload Construction Considerations .....	475
Payload Protocol Elements .....	476
Buffer Orientation Problems .....	476
Self-Destructive Shellcode .....	477
Documenting the Problem .....	478
Background Information .....	478
Circumstances .....	478
Research Results .....	479
<b>Chapter 19 Closing the Holes: Mitigation .....</b>	<b>481</b>
Mitigation Alternatives .....	481
Port Knocking .....	482
Migration .....	482
Patching .....	484
Source Code Patching Considerations .....	484
Binary Patching Considerations .....	486
Binary Mutation .....	490
Third-Party Patching Initiatives .....	495

<b>Part V</b>	<b>Malware Analysis</b>	<b>497</b>
<b>Chapter 20</b>	<b>Collecting Malware and Initial Analysis</b>	<b>499</b>
	Malware	499
	Types of Malware	499
	Malware Defensive Techniques	500
	Latest Trends in Honeynet Technology	501
	Honeypots	501
	Honeynets	501
	Why Honeypots Are Used	502
	Limitations	502
	Low-Interaction Honeypots	503
	High-Interaction Honeypots	503
	Types of Honeynets	504
	Thwarting VMware Detection Technologies	506
	Catching Malware: Setting the Trap	508
	VMware Host Setup	508
	VMware Guest Setup	508
	Using Nepenthes to Catch a Fly	508
	Initial Analysis of Malware	510
	Static Analysis	510
	Live Analysis	512
	Norman Sandbox Technology	518
	What Have We Discovered?	520
<b>Chapter 21</b>	<b>Hacking Malware</b>	<b>521</b>
	Trends in Malware	521
	Embedded Components	522
	Use of Encryption	522
	User Space Hiding Techniques	522
	Use of Rootkit Technology	523
	Persistence Measures	523
	Peeling Back the Onion—De-obfuscation	524
	Packer Basics	524
	Unpacking Binaries	525
	Reverse Engineering Malware	533
	Malware Setup Phase	533
	Malware Operation Phase	534
	Automated Malware Analysis	535
	<b>Index</b>	<b>537</b>



---

## FOREWORD

This book has been developed by and for security professionals who are dedicated to working in an ethical and responsible manner to improve the overall security posture of individuals, corporations, and nations.



## ACKNOWLEDGMENTS

**Shon Harris** would like to thank the other authors and the team members for their continued dedication to this project and continual contributions to the industry as a whole. She would also like to thank Scott David, partner at K&L Gates LLP, for reviewing and contributing to the legal topics of this book.

**Allen Harper** would like to thank his wonderful wife, Corann, and daughters, Haley and Madison, for their support and understanding through this second edition. You gave me the strength and the ability to achieve my goals. I am proud of you and love you each dearly.

**Chris Eagle** would like to thank all of his students and fellow members of the Sk3wl of r00t. They keep him motivated, on his toes, and most of all make all of this fun!

**Jonathan Ness** would like to thank Jessica, his amazing wife, for tolerating the long hours required for him to write this book (and hold his job and his second job and third "job" and the dozens of side projects). He would also like to thank his family, mentors, teachers, coworkers, pastors, and friends who have guided him along his way, contributing more to his success than they'll ever know.

## Introduction

*There is nothing so likely to produce peace as to be well prepared to meet the enemy.*

—George Washington

*He who has a thousand friends has not a friend to spare, and he who has one enemy will meet him everywhere.*

—Ralph Waldo Emerson

*Know your enemy and know yourself and you can fight a hundred battles without disaster.*

—Sun Tzu

The goal of this book is to help produce more highly skilled security professionals who are dedicated to protecting against malicious hacking activity. It has been proven over and over again that it is important to understand one's enemies, including their tactics, skills, tools, and motivations. Corporations and nations have enemies that are very dedicated and talented. We must work together to understand the enemies' processes and procedures to ensure that we can properly thwart their destructive and malicious behavior.

The authors of this book want to provide the readers with something we believe the industry needs: a holistic review of ethical hacking that is responsible and truly ethical in its intentions and material. This is why we are starting this book with a clear definition of what ethical hacking is and is not—something society is very confused about.

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

---

### XXii

We have updated the material from the first edition and have attempted to deliver the most comprehensive and up-to-date assembly of techniques and procedures. Six new chapters are presented and the other chapters have been updated.

In Part I of this book we lay down the groundwork of the necessary ethics and expectations of a gray hat hacker. This section:

- Clears up the confusion about white, black, and gray hat definitions and characteristics
- Reviews the slippery ethical issues that should be understood before carrying out any type of ethical hacking activities
- Surveys legal issues surrounding hacking and many other types of malicious activities
- Walks through proper vulnerability discovery processes and current models that provide direction

In Part II we introduce more advanced penetration methods and tools that no other books cover today. Many existing books cover the same old tools and methods that have been rehashed numerous times, but we have chosen to go deeper into the advanced mechanisms that real gray hats use today. We discuss the following topics in this section:

- Automated penetration testing methods and advanced tools used to carry out these activities
- The latest tools used for penetration testing

In Part III we dive right into the underlying code and teach the reader how specific components of every operating system and application work, and how they can be exploited. We cover the following topics in this section:

- Program Coding 101 to introduce you to the concepts you will need to understand for the rest of the sections
- How to exploit stack operations and identify and write buffer overflows
- How to identify advanced Linux and Windows vulnerabilities and how they are exploited
- How to create different types of shellcode to develop your own proof-of-concept exploits and necessary software to test and identify vulnerabilities

In Part IV we go even deeper, by examining the most advanced topics in ethical hacking that many security professionals today do not understand. In this section we examine the following:

- Passive and active analysis tools and methods
- How to identify vulnerabilities in source code and binary files

- How to reverse-engineer software and disassemble the components
- Fuzzing and debugging techniques
- Mitigation steps of patching binary and source code

In Part V we added a new section on malware analysis. At some time or another, the ethical hacker will come across a piece of malware and may need to perform basic analysis. In this section, you will learn:

- Collection of your own malware specimen
- Analysis of malware to include a discussion of de-obfuscation techniques

If you are ready to take the next step to advance and deepen your understanding of ethical hacking, this is the book for you.

We're interested in your thoughts and comments. Please e-mail us at [book@grayhathackingbook.com](mailto:book@grayhathackingbook.com). Also, browse to [www.grayhathackingbook.com](http://www.grayhathackingbook.com) for additional technical information and resources related to this book and ethical hacking.

