

**CEH™**  
**Certified Ethical Hacker**  
**Study Guide**

Kimberly Graves



WILEY

Wiley Publishing, Inc.

# Acknowledgments

To my family and friends, who have been so supportive through countless hours spent writing and editing this book. All your comments and critiques were invaluable and I appreciate your efforts. Most importantly, I want to thank my husband Ed for his support in this endeavor. It has been no small task and I appreciate his understanding every step of the way.

I want to thank my technical editor, Keith Parsons, for his attention to detail and continual quest for excellence from himself and everyone he works with, this book being no exception. Thanks, Keith, I know it was a long road and you stuck with it until the very end.

Also thanks to the team at Sybex: Jeff Kellum, Pete Gaughan, and Angela Smith. Thank you for following through on this book and keeping me motivated.

# About the Author

Graduating in 1995 from American University, with a major in political science and a minor in computer information technology, Kimberly Graves quickly learned that the technical side of her degree was going to be a far more interesting and challenging career path than something that kept her “inside the Beltway.”

Starting with a technical instructor position at a computer training company in Arlington, Virginia, Kimberly used the experience and credentials gained from that position to begin the steady accumulation of the other certifications that she now uses in her day-to-day interactions with clients and students. Since gaining her Certified Novell Engineer Certification (CNE) in a matter of a few months at her first job, Kimberly’s expertise in networking and security has grown to encompass certifications by Microsoft, Intel, Aruba Networks, EC-Council, Cisco Systems, and CompTIA.

With over 15 cumulative years invested in the IT industry, Kimberly has amassed more than 25 instructor grade networking and security certifications. She has served various educational institutions in Washington, DC, as an adjunct professor while simultaneously serving as a subject matter expert for several security certification programs. Recently Kimberly has been utilizing her Security+, Certified Wireless Network Associate (CWNA), Certified Wireless Security Professional (CWSP), Certified Ethical Hacker (CEH), and Certified Information Systems Security Professional (CISSP) certificates to teach and develop course material for the Department of Veterans Affairs, U.S. Air Force, and the NSA. Kimberly currently works with leading wireless vendors across the country to train the next generation of wireless security professionals. In 2007, Kimberly founded Techsource Network Solutions to better serve the needs of her clients and offer additional network and security consulting services.

# Contents at a Glance

<i>Introduction</i>		<i>xxi</i>
<i>Assessment Test</i>		<i>xxx</i>
<b>Chapter 1</b>	Introduction to Ethical Hacking, Ethics, and Legality	1
<b>Chapter 2</b>	Gathering Target Information: Reconnaissance, Footprinting, and Social Engineering	31
<b>Chapter 3</b>	Gathering Network and Host Information: Scanning and Enumeration	63
<b>Chapter 4</b>	System Hacking: Password Cracking, Escalating Privileges, and Hiding Files	95
<b>Chapter 5</b>	Trojans, Backdoors, Viruses, and Worms	125
<b>Chapter 6</b>	Gathering Data from Networks: Sniffers	153
<b>Chapter 7</b>	Denial of Service and Session Hijacking	173
<b>Chapter 8</b>	Web Hacking: Google, Web Servers, Web Application Vulnerabilities, and Web-Based Password Cracking Techniques	195
<b>Chapter 9</b>	Attacking Applications: SQL Injection and Buffer Overflows	221
<b>Chapter 10</b>	Wireless Network Hacking	239
<b>Chapter 11</b>	Physical Site Security	261
<b>Chapter 12</b>	Hacking Linux Systems	281
<b>Chapter 13</b>	Bypassing Network Security: Evading IDSs, Honeypots, and Firewalls	301
<b>Chapter 14</b>	Cryptography	323
<b>Chapter 15</b>	Performing a Penetration Test	343
<b>Appendix</b>	About the Companion CD	359
<b>Glossary</b>		363
<i>Index</i>		<i>375</i>

# Contents

*Introduction* *xxi*

*Assessment Test* *xxx*

## **Chapter 1** **Introduction to Ethical Hacking, Ethics, and Legality** **1**

Defining Ethical Hacking	2
Understanding the Purpose of Ethical Hacking	3
An Ethical Hacker's Skill Set	6
Ethical Hacking Terminology	7
The Phases of Ethical Hacking	8
Identifying Types of Hacking Technologies	11
Identifying Types of Ethical Hacks	12
Understanding Testing Types	13
How to Be Ethical	16
Performing a Penetration Test	17
Keeping It Legal	18
Cyber Security Enhancement Act and SPY ACT	19
18 USC §1029 and 1030	20
U.S. State Laws	20
Federal Managers Financial Integrity Act	20
Freedom of Information Act (FOIA)	21
Federal Information Security Management Act (FISMA)	21
Privacy Act of 1974	22
USA PATRIOT Act	22
Government Paperwork Elimination Act (GPEA)	22
Cyber Laws in Other Countries	23
Summary	23
Exam Essentials	23
Review Questions	25
Answers to Review Questions	29

## **Chapter 2** **Gathering Target Information: Reconnaissance, Footprinting, and Social Engineering** **31**

Reconnaissance	33
Understanding Competitive Intelligence	34
Information-Gathering Methodology	37
Footprinting	38
Using Google to Gather Information	39
Understanding DNS Enumeration	40
Understanding Whois and ARIN Lookups	42
Identifying Types of DNS Records	46

	Using Traceroute in Footprinting	46
	Understanding Email Tracking	48
	Understanding Web Spiders	48
	Social Engineering	48
	The Art of Manipulation	50
	Types of Social Engineering-Attacks	50
	Social-Engineering Countermeasures	54
	Summary	54
	Exam Essentials	55
	Review Questions	56
	Answers to Review Questions	60
<b>Chapter 3</b>	<b>Gathering Network and Host Information: Scanning and Enumeration</b>	<b>63</b>
	Scanning	64
	The CEH Scanning Methodology	67
	Ping Sweep Techniques	68
	<i>nmap</i> Command Switches	70
	Scan Types	73
	TCP Communication Flag Types	73
	War-Dialing Techniques	76
	Banner Grabbing and OS Fingerprinting Techniques	77
	Scanning Anonymously	79
	Enumeration	81
	Null Sessions	82
	SNMP Enumeration	84
	Windows 2000 DNS Zone Transfer	85
	Summary	86
	Exam Essentials	87
	Review Questions	89
	Answers to Review Questions	93
<b>Chapter 4</b>	<b>System Hacking: Password Cracking, Escalating Privileges, and Hiding Files</b>	<b>95</b>
	The Simplest Way to Get a Password	96
	Types of Passwords	96
	Passive Online Attacks	97
	Active Online Attacks	98
	Offline Attacks	99
	Nonelectronic Attacks	101

Cracking a Password	102	
Understanding the LAN Manager Hash	103	
Cracking Windows 2000 Passwords	103	
Redirecting the SMB Logon to the Attacker	105	
SMB Relay MITM Attacks and Countermeasures	106	
NetBIOS DoS Attacks	107	
Password-Cracking Countermeasures	107	
Understanding Keyloggers and Other Spyware Technologies	109	
Escalating Privileges	110	
Executing Applications	111	
Buffer Overflows	111	
Understanding Rootkits	112	
Planting Rootkits on Windows 2000 and XP Machines	112	
Rootkit Embedded TCP/IP Stack	112	
Rootkit Countermeasures	113	
Hiding Files	113	
NTFS File Streaming	114	
NTFS Stream Countermeasures	114	
Understanding Steganography Technologies	115	
Covering Your Tracks and Erasing Evidence	116	
Summary	117	
Exam Essentials	118	
Review Questions	119	
Answers to Review Questions	123	
<b>Chapter 5</b>	<b>Trojans, Backdoors, Viruses, and Worms</b>	<b>125</b>
Trojans and Backdoors	126	
Overt and Covert Channels	128	
Types of Trojans	130	
How Reverse-Connecting Trojans Work	130	
How the Netcat Trojan Works	132	
Trojan Construction Kit and Trojan Makers	135	
Trojan Countermeasures	135	
Checking a System with System File Verification	138	
Viruses and Worms	141	
Types of Viruses	142	
Virus Detection Methods	145	
Summary	146	
Exam Essentials	146	
Review Questions	147	
Answers to Review Questions	151	

<b>Chapter 6</b>	<b>Gathering Data from Networks: Sniffers</b>	<b>153</b>
	Understanding Host-to-Host Communication	154
	How a Sniffer Works	158
	Sniffing Countermeasures	158
	Bypassing the Limitations of Switches	159
	How ARP Works	159
	ARP Spoofing and Poisoning Countermeasures	160
	Wireshark Filters	161
	Understanding MAC Flooding and DNS Spoofing	164
	Summary	166
	Exam Essentials	167
	Review Questions	168
	Answers to Review Questions	171
<b>Chapter 7</b>	<b>Denial of Service and Session Hijacking</b>	<b>173</b>
	Denial of Service	174
	How DDoS Attacks Work	177
	How BOTs/BOTNETs Work	179
	Smurf and SYN Flood Attacks	180
	DoS/DDoS Countermeasures	182
	Session Hijacking	183
	Sequence Prediction	184
	Dangers Posed by Session Hijacking	186
	Preventing Session Hijacking	186
	Summary	187
	Exam Essentials	188
	Review Questions	189
	Answers to Review Questions	193
<b>Chapter 8</b>	<b>Web Hacking: Google, Web Servers, Web Application Vulnerabilities, and Web-Based Password Cracking Techniques</b>	<b>195</b>
	How Web Servers Work	197
	Types of Web Server Vulnerabilities	198
	Attacking a Web Server	201
	Patch-Management Techniques	207
	Web Server Hardening Methods	208
	Web Application Vulnerabilities	209
	Web Application Threats and Countermeasures	210
	Google Hacking	211
	Web-Based Password-Cracking Techniques	212
	Authentication Types	212
	Password Attacks and Password Cracking	213



	Summary	215
	Exam Essentials	215
	Review Questions	216
	Answers to Review Questions	219
<b>Chapter 9</b>	<b>Attacking Applications: SQL Injection and Buffer Overflows</b>	<b>221</b>
	SQL Injection	222
	Finding a SQL Injection Vulnerability	224
	The Purpose of SQL Injection	225
	SQL Injection Using Dynamic Strings	226
	SQL Injection Countermeasures	228
	Buffer Overflows	229
	Types of Buffer Overflows and Methods of Detection	229
	Buffer Overflow Countermeasures	231
	Summary	232
	Exam Essentials	232
	Review Questions	233
	Answers to Review Questions	237
<b>Chapter 10</b>	<b>Wireless Network Hacking</b>	<b>239</b>
	Wi-Fi and Ethernet	240
	Authentication and Cracking Techniques	242
	Using Wireless Sniffers to Locate SSIDs	246
	MAC Filters and MAC Spoofing	248
	Rogue Access Points	250
	Evil Twin or AP Masquerading	250
	Wireless Hacking Techniques	251
	Securing Wireless Networks	251
	Summary	254
	Exam Essentials	254
	Review Questions	255
	Answers to Review Questions	259
<b>Chapter 11</b>	<b>Physical Site Security</b>	<b>261</b>
	Components of Physical Security	262
	Understanding Physical Security	264
	Physical Site Security Countermeasures	266
	What to Do After a Security Breach Occurs	274
	Summary	274
	Exam Essentials	274
	Review Questions	275
	Answers to Review Questions	279

<b>Chapter 12</b>	<b>Hacking Linux Systems</b>	<b>281</b>
	Linux Basics	282
	Compiling a Linux Kernel	285
	GCC Compilation Commands	288
	Installing Linux Kernel Modules	289
	Linux Hardening Methods	289
	Summary	293
	Exam Essentials	294
	Review Questions	295
	Answers to Review Questions	299
<b>Chapter 13</b>	<b>Bypassing Network Security: Evading IDSs, Honeypots, and Firewalls</b>	<b>301</b>
	Types of IDSs and Evasion Techniques	302
	Firewall Types and Honeypot Evasion Techniques	308
	Summary	316
	Exam Essentials	316
	Review Questions	317
	Answers to Review Questions	322
<b>Chapter 14</b>	<b>Cryptography</b>	<b>323</b>
	Cryptography and Encryption Techniques	324
	Types of Encryption	326
	Stream Ciphers vs. Block Ciphers	328
	Generating Public and Private Keys	329
	Other Uses for Encryption	333
	Cryptography Algorithms	335
	Cryptography Attacks	337
	Summary	337
	Exam Essentials	338
	Review Questions	339
	Answers to Review Questions	342
<b>Chapter 15</b>	<b>Performing a Penetration Test</b>	<b>343</b>
	Defining Security Assessments	344
	Penetration Testing	345
	Penetration Testing Steps	346
	The Pen Test Legal Framework	349
	Automated Penetration Testing Tools	349
	Pen Test Deliverables	350

	Summary	352
	Exam Essentials	352
	Review Questions	353
	Answers to Review Questions	357
<b>Appendix</b>	<b>About the Companion CD</b>	<b>359</b>
	What You'll Find on the CD	360
	Sybex Test Engine	360
	PDF of Glossary of Terms	360
	Adobe Reader	360
	Electronic Flashcards	360
	System Requirements	361
	Using the CD	361
	Troubleshooting	361
	Customer Care	362
<b>Glossary</b>		<b>363</b>
	<i>Index</i>	375