

Official Certified Ethical Hacker Review Guide

Steven DeFino

Intense School, Senior Security Instructor and Consultant

Contributing Authors

Barry Kaufman, Director of Intense School

Nick Valenteen, Intense School, Senior Security Instructor

Larry Greenblatt, Intense School, Senior Security Instructor



COURSE TECHNOLOGY
CENGAGE Learning™

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

Contents

INTRODUCTION	vii
CHAPTER ONE Ethical Hacking	1
Know the Definition of Ethical Hacking	2
Know the Concepts of Threat Modeling	3
Know the Five Phases of an Attack	5
Know the Concepts of Vulnerability Research and Testing	7
CHAPTER TWO Hacking Laws	11
Know the Legal Issues of Ethical Hacking	12
Know the Challenges of Legal Enforcement	12
Know the Ins and Outs of Protecting Intellectual Property	13
Know the Important Legal Statutes	16
CHAPTER THREE Footprinting	21
Know the Information Gathering Methodology	22
Know Several Different Passive Information Gathering Techniques	25
Know How to Use DNS and the Regional Internet Registrars	27
CHAPTER FOUR Google Hacking	33
Know What the Google Toolset Offers	34
Know What You Are Looking for	38
Know About Some of the Other Google Tools	40
CHAPTER FIVE Scanning	45
Know the Scanning Methodology	46
Know How ICMP Works	52
Know the TCP Handshake	52
Know the Types of Scans	54
Know about Scanning Tools	57
CHAPTER SIX Enumeration	61
Know the Value of the Enumeration Step	62
Know How to Create a NULL Session	62
Know the File Sharing Ports	63
Know What the “RestrictAnonymous” Key Is	65
Know How to Recognize Windows SIDs	66
Know How to Use the Netstat and NBTstat Tools	66
Know How to Enumerate a Linux Host	67
Know How to Use SNMP for Enumeration	70
Know How to Use LDAP for Enumeration	71
CHAPTER SEVEN System Hacking	73
Know Password Cracking Techniques	74
Know Eavesdropping and Privilege Escalation	81
Know the Techniques of Steganography	85
CHAPTER EIGHT Trojans and Backdoors	91
Know What Trojan Applications Can Do	92
Know the Infection Vectors	94
Know How to Build a Server	100
Know How to Detect an Infection	103

CHAPTER NINE	Viruses and Worms	107
	Know the History and Evolution of Viruses and Worms	108
	Know the Types of Viruses and Worms	114
	Know About Virus Detection and Removal	118
CHAPTER TEN	Sniffers, Spoofing, and Session Hijacking	123
	Know How Sniffing Works	124
	Know How to Use Packet Capture Tools	127
	Know How to Exploit Vulnerable Protocols	131
	Know How Session Hijacking Works	132
CHAPTER ELEVEN	Social Engineering	137
	Know About Social Engineering	138
	Know About Phishing Scams	142
	Know About Hacking E-mail Accounts	144
	Know About Social Networks	146
CHAPTER TWELVE	Denial of Service	149
	Know the Types of DoS Attacks	150
	Know How DDoS Attacks Work	153
	Know How Botnets Work	156
CHAPTER THIRTEEN	Buffer Overflows	161
	Know the Theory Behind Buffer Overflows	162
	Know How to Work with Overflow Exploits	167
	Know the Tools for Performing Exploits	170
CHAPTER FOURTEEN	Hacking Web Servers and Web Applications	173
	Know How Web Servers Work	174
	Know How Web Applications Work	179
	Know the Attacks and Risks of Web Applications	183
CHAPTER FIFTEEN	Wireless Networks	191
	Know the Basics of Designing a Wireless Network	192
	Know How WEP and WPA Work	196
	Know the Important Security Risks of WiFi Networks	199
	Know the Basics of Bluetooth	202
CHAPTER SIXTEEN	Cryptography	205
	Know the Basic Concepts of Cryptography	206
	Know How Symmetric Encryption Works	210
	Know How Asymmetric Encryption Works	214
	Know How Hashing Algorithms Work	217
	Know About Cryptosystems and Key Management	221
	Know Advanced Attacks Against Cryptography	223
CHAPTER SEVENTEEN	Hacking with Linux	227
	Know the Origins and Story of GNU/Linux	228
	Know Some Important Features of Linux	232
	Know About Important Linux Security Features	238
CHAPTER EIGHTEEN	IDS, Firewalls, and Honey pots	243
	Know the Classes of Firewalls	244

Know the Classes of Intrusion Detection Systems	248
Know How to Deploy Honey Pots	254
Know the Testing and Evasion Techniques	256
CHAPTER NINETEEN Summary of Optional Modules	261
Approaching the Weird Questions	262
Know the Basics Behind the Topics in the Optional Materials	263
CHAPTER TWENTY Penetration Testing	277
Know General Penetration Testing Methodologies	278
Know the Basic Requirements of an Engagement	281
Know How to Write an Effective Report	285
Style and Tone	285
Elements to Include in the Report	286
Know How to Stay Current with Information	289
PRACTICE EXAMS QUESTIONS	293
PRACTICE EXAMS ANSWERS	336
INDEX	353

List of Try It Out Exercises

The “Try it out” exercises in this book represent exercises that are designed to help the student become comfortable with a few important elements before attending the intense lab environment of the official training experience.

For quick reference, the following is a list of the exercises. You might want to use this as a checklist and make sure to try each one before your training date. Some of these exercises will be expanded on, and the student should be prepared with questions as a result of trying them.

Chapter One: Ethical Hacking

1. Research hacker culture
2. Research the vulnerability databases

Chapter Two: Hacking Laws

3. Research intellectual property law

Chapter Three: Footprinting

4. Utilize the RFCs to understand network ranges
5. Banner grabbing
6. Collecting data
7. Competitive intelligence gathering
8. Watch “Privacy is dead, get over it”
9. Obtain a Who is record
10. Attempt a zone transfer

Chapter Four: Google Hacking

11. Visit Google Labs
12. Setup Google reader
13. Google search examples

Chapter Five: Scanning

14. Read RFC 826
15. Scanning a local segment
16. Angry IP
17. Read RFC 1574
18. Read RFC 793
19. Read RFC 791
20. Demo Core Impact
21. Read RFC 792
22. Read RFC 768
23. Using Netcat as a scanner
24. Using HPing as a scanner
25. Using Nmap as a scanner
26. Download and try graphical scanners

Chapter Six: Enumeration

27. Creating a NULL session
28. Changing the Restrict Anonymous key setting
29. Using the Netstat and NBTStat tools
30. Run the SMB Client command
31. Finger a user
32. Finding the SUID bit

Chapter Seven: System Hacking

33. Calculating password combinations
34. Read RFC 1510
35. Create a user from the windows command line
36. Alternate data streams

Chapter Eight: Trojans and Backdoors

37. Configure a USB “autostart” script
38. Research the two letter TLDs
39. Using the \$PTAH variable in Linux
40. Using the \$PATH variable in Windows

Chapter Ten: Sniffers, Spoofing, and Session Hijacking

41. Research advance ARP procedures
42. Using TCP Dump
43. Research advanced Wireshark capture filters
44. Experiment with the GUI based packet analyzers
45. Research advanced Wireshark display filters

Chapter Eleven: Social Engineering

46. Using a disposable email address
47. Sending a spoofed email

Chapter Twelve: Denial of Service

48. Read about the GRC denial of service attack
49. Visit the CATCH team and regional CERT websites
50. Connect to IRC

Chapter Thirteen: Buffer Overflows

51. Read the original “Smashing the stack” article
52. Create a simple buffer overflow script
53. Disassemble the buffer overflow exploit example
54. Use the Metasploit framework tool

Chapter Fourteen: Hacking Web Servers and Web Applications

55. Learn more about building web pages
56. Use the Lynx browser
57. Banner grabbing
58. Explore URL encoding and obfuscation

Chapter Fifteen: Wireless Networks

59. Generate a strong WPA2 PSK
60. Research cracking WPA/WPA2
61. View a map of discovered WiFi networks
62. Learn the warchalking symbols

Chapter Sixteen: Cryptography

63. Meet Alice and Bob
64. Research symmetric encryption vocabulary terms
65. Research asymmetric encryption vocabulary terms
66. Experiment with hashes
67. Use PGP to encrypt Email

Chapter Seventeen: Hacking with Linux

- 68. Investigate Linux distribution choices
- 69. Downloading a Linux VM appliance
- 70. Installing an application in Linux
- 71. Using man pages
- 72. Using basic Linux commands
- 73. Tools for hacking with Linux

Chapter Eighteen: IDS, Firewalls, and Honeypots

- 74. Learn more about IP Tables
- 75. Learn more about snort
- 76. Learn more about honeypots
- 77. Explore the hping tool

Chapter Nineteen: Summary of Optional Modules

- 78. Investigate VoIP Hacking Tools

Chapter Twenty: Penetration Testing

- 79. Research some of the common vulnerability databases
- 80. Gather a few good resources