

# Contents

<i>Introduction</i>		<i>xv</i>
<b>Chapter 1</b>	<b>Introduction to Ethical Hacking, Ethics, and Legality</b>	<b>1</b>
	Understanding Ethical Hacking Terminology	2
	Identifying Different Types of Hacking Technologies	3
	Understanding the Different Phases Involved in Ethical Hacking and Listing the Five Stages of Ethical Hacking	4
	Phase 1: Passive and Active Reconnaissance	5
	Phase 2: Scanning	5
	Phase 3: Gaining Access	5
	Phase 4: Maintaining Access	6
	Phase 5: Covering Tracks	6
	What Is Hacktivism?	6
	Listing Different Types of Hacker Classes	6
	Ethical Hackers and Crackers—Who Are They?	7
	What Do Ethical Hackers Do?	8
	Goals Attackers Try to Achieve	8
	Security, Functionality, and Ease of Use Triangle	9
	Defining the Skills Required to Become an Ethical Hacker	10
	What Is Vulnerability Research?	10
	Describing the Ways to Conduct Ethical Hacking	11
	Creating a Security Evaluation Plan	11
	Types of Ethical Hacks	12
	Testing Types	12
	Ethical Hacking Report	13
	Understanding the Legal Implications of Hacking	13
	Understanding 18 U.S.C. § 1029 and 1030 U.S. Federal Law	14
	Exam Essentials	14
	Review Questions	16
	Answers to Review Questions	18
<b>Chapter 2</b>	<b>Footprinting and Social Engineering</b>	<b>19</b>
	Footprinting	20
	Define the Term Footprinting	20
	Describe the Information Gathering Methodology	21
	Describe Competitive Intelligence	22
	Understand DNS Enumeration	23
	Understand Whois and ARIN Lookups	24
	Identify Different Types of DNS Records	27
	Understand How Traceroute Is Used in Footprinting	28

	Understand How E-Mail Tracking Works	29
	Understand How Web Spiders Work	29
	Exam Essentials	29
	Social Engineering	30
	What Is Social Engineering?	30
	What Are the Common Types Of Attacks?	32
	Understand Insider Attacks	33
	Understand Identity Theft	33
	Describe Phishing Attacks	34
	Understand Online Scams	34
	Understand URL Obfuscation	35
	Social-Engineering Countermeasures	35
	Exam Essentials	36
	Review Questions	37
	Answers to Review Questions	40
<b>Chapter 3</b>	<b>Scanning and Enumeration</b>	<b>41</b>
	Scanning	42
	Define the Terms Port Scanning, Network Scanning, and Vulnerability Scanning	42
	Understand the CEH Scanning Methodology	43
	Understand Ping Sweep Techniques	44
	Understand Nmap Command Switches	46
	Understand SYN, Stealth, XMAS, NULL, IDLE, and FIN Scans	48
	List TCP Communication Flag Types	49
	Understand War-Dialing Techniques	51
	Understand Banner Grabbing and OS Fingerprinting Techniques	52
	Understand How Proxy Servers Are Used in Launching an Attack	53
	How Do Anonymizers Work?	53
	Understand HTTP Tunneling Techniques	54
	Understand IP Spoofing Techniques	54
	Exam Essentials	55
	Enumeration	55
	What Is Enumeration?	56
	What Is Meant by Null Sessions?	56
	What Is SNMP Enumeration?	58
	Windows 2000 DNS Zone Transfer	59
	What Are the Steps Involved in Performing Enumeration?	60
	Exam Essentials	60
	Review Questions	62
	Answers to Review Questions	66

<b>Chapter 4</b>	<b>System Hacking</b>	<b>67</b>
	Understanding Password-Cracking Techniques	68
	Understanding the LanManager Hash	69
	Cracking Windows 2000 Passwords	70
	Redirecting the SMB Logon to the Attacker	70
	SMB Redirection	71
	SMB Relay MITM Attacks and Countermeasures	71
	NetBIOS DoS Attacks	72
	Password-Cracking Countermeasures	72
	Understanding Different Types of Passwords	74
	Passive Online Attacks	74
	Active Online Attacks	75
	Offline Attacks	77
	Nonelectronic Attacks	78
	Understanding Keyloggers and Other Spyware Technologies	78
	Understanding Escalating Privileges	79
	Executing Applications	80
	Buffer Overflows	80
	Understanding Rootkits	81
	Planting Rootkits on Windows 2000 and XP Machines	81
	Rootkit Embedded TCP/IP Stack	82
	Rootkit Countermeasures	82
	Understanding How to Hide Files	83
	NTFS File Streaming	83
	NTFS Stream Countermeasures	83
	Understanding Steganography Technologies	84
	Understanding How to Cover Your Tracks and Erase Evidence	85
	Disabling Auditing	85
	Clearing the Event Log	86
	Exam Essentials	86
	Review Questions	87
	Answers to Review Questions	89
<b>Chapter 5</b>	<b>Trojans, Backdoors, Viruses, and Worms</b>	<b>91</b>
	Trojans and Backdoors	92
	What Is a Trojan?	93
	What Is Meant by Overt and Covert Channels?	94
	List the Different Types of Trojans	94
	How Do Reverse-Connecting Trojans Work?	94
	Understand How the Netcat Trojan Works	96
	What Are the Indications of a Trojan Attack?	97
	What Is Meant by “Wrapping”?	97
	Trojan Construction Kit and Trojan Makers	97

x Contents

	What Are the Countermeasure Techniques in Preventing Trojans?	98
	Understand Trojan-Evading Techniques	98
	System File Verification Subobjective to Trojan Countermeasures	99
	Viruses and Worms	99
	Understand the Difference between a Virus and a Worm	99
	Understand the Types of Viruses	100
	Understand Antivirus Evasion Techniques	101
	Understand Virus Detection Methods	101
	Exam Essentials	101
	Review Questions	103
	Answers to Review Questions	106
<b>Chapter 6</b>	<b>Sniffers</b>	<b>107</b>
	Understand the Protocols Susceptible to Sniffing	108
	Understand Active and Passive Sniffing	109
	Understand ARP Poisoning	110
	Understand Ethereal Capture and Display Filters	110
	Understand MAC Flooding	111
	Understand DNS Spoofing Techniques	111
	Describe Sniffing Countermeasures	113
	Exam Essentials	114
	Review Questions	115
	Answers to Review Questions	117
<b>Chapter 7</b>	<b>Denial of Service and Session Hijacking</b>	<b>119</b>
	Denial of Service	120
	Understand the Types of DoS Attacks	120
	Understand How DDoS Attacks Work	122
	Understand How BOTs/BOTNETs Work	123
	What Is a “Smurf” Attack?	124
	What Is “SYN” Flooding?	124
	Describe the DoS/DDoS Countermeasures	124
	Session Hijacking	125
	Understand Spoofing vs. Hijacking	125
	List the Types of Session Hijacking	126
	Understand Sequence Prediction	126
	What Are the Steps in Performing Session Hijacking?	128
	Describe How You Would Prevent Session Hijacking	129
	Exam Essentials	130
	Review Questions	131
	Answers to Review Questions	135

<b>Chapter 8</b>	<b>Hacking Web Servers, Web Application Vulnerabilities, and Web-Based Password Cracking Techniques</b>	<b>137</b>
	Hacking Web Servers	138
	List the Types of Web Server Vulnerabilities	138
	Understand the Attacks against Web Servers	139
	Understand IIS Unicode Exploits	139
	Understand Patch Management Techniques	140
	Describe Web Server Hardening Methods	140
	Web Application Vulnerabilities	141
	Understanding How Web Applications Work	141
	Objectives of Web Application Hacking	142
	Anatomy of an Attack	142
	Web Application Threats	142
	Understand Google Hacking	143
	Understand Web Application Countermeasures	143
	Web-Based Password Cracking Techniques	144
	List the Authentication Types	144
	What Is a Password Cracker?	144
	How Does a Password Cracker Work?	144
	Understand Password Attacks: Classification	145
	Understand Password-Cracking Countermeasures	145
	Exam Essentials	145
	Review Questions	147
	Answers to Review Questions	149
<b>Chapter 9</b>	<b>SQL Injection and Buffer Overflows</b>	<b>151</b>
	SQL Injection	152
	What Is SQL Injection?	152
	Understand the Steps to Conduct SQL Injection	152
	Understand SQL Server Vulnerabilities	153
	Describe SQL Injection Countermeasures	153
	Buffer Overflows	154
	Identify the Different Types of Buffer Overflows and Methods of Detection	154
	Overview of Stack-Based Buffer Overflows	154
	Overview of Buffer Overflow Mutation Techniques	155
	Exam Essentials	155
	Review Questions	156
	Answers to Review Questions	158

<b>Chapter 10</b>	<b>Wireless Hacking</b>	<b>159</b>
	Overview of WEP, WPA Authentication Mechanisms, and Cracking Techniques	160
	Overview of Wireless Sniffers and Locating SSIDs, MAC Spoofing	162
	Understand Rogue Access Points	163
	Understand Wireless Hacking Techniques	163
	Describe the Methods Used to Secure Wireless Networks	164
	Exam Essentials	164
	Review Questions	165
	Answers to Review Questions	167
<b>Chapter 11</b>	<b>Physical Security</b>	<b>169</b>
	Physical Security Breach Incidents	170
	Understanding Physical Security	171
	What Is the Need for Physical Security?	171
	Who Is Accountable for Physical Security?	172
	Factors Affecting Physical Security	172
	Exam Essentials	172
	Review Questions	174
	Answers to Review Questions	176
<b>Chapter 12</b>	<b>Linux Hacking</b>	<b>177</b>
	Linux Basics	178
	Understand How to Compile a Linux Kernel	179
	Understand GCC Compilation Commands	180
	Understand How to Install Linux Kernel Modules	180
	Understand Linux Hardening Methods	181
	Exam Essentials	182
	Review Questions	183
	Answers to Review Questions	185
<b>Chapter 13</b>	<b>Evasion IDSs, Honeypots, and Firewalls</b>	<b>187</b>
	List the Types of Intrusion Detection Systems and Evasion Techniques	188
	List the Firewall Types and Honeypot Evasion Techniques	189
	Exam Essentials	191
	Review Questions	192
	Answers to Review Questions	194
<b>Chapter 14</b>	<b>Cryptography</b>	<b>195</b>
	Overview of Cryptography and Encryption Techniques	196
	Describe How Public and Private Keys Are Generated	197

	Overview of the MD5, SHA, RC4, RC5, and Blowfish Algorithms	197
	Exam Essentials	198
	Review Questions	199
	Answers to Review Questions	201
<b>Chapter 15</b>	<b>Penetration Testing Methodologies</b>	<b>203</b>
	Defining Security Assessments	204
	Overview of Penetration Testing Methodologies	204
	List the Penetration Testing Steps	205
	Overview of the Pen-Test Legal Framework	206
	List the Automated Penetration Testing Tools	207
	Overview of the Pen-Test Deliverables	208
	Exam Essentials	208
	Review Questions	209
	Answers to Review Questions	211
	<b>Glossary</b>	<b>213</b>
	<i>Index</i>	225

