
CONTENTS AT A GLANCE

Chapter 1	Ethical Hacking Basics	1
Chapter 2	Cryptography 101	27
Chapter 3	Reconnaissance: Information Gathering for the Ethical Hacker ...	53
Chapter 4	Scanning and Enumeration	85
Chapter 5	Hacking Through the Network: Sniffers and Evasion	121
Chapter 6	Attacking a System	155
Chapter 7	Low Tech: Social Engineering and Physical Security	193
Chapter 8	Web-Based Hacking: Servers and Applications	219
Chapter 9	Wireless Network Hacking	251
Chapter 10	Trojans and Other Attacks	283
Chapter 11	The Pen Test: Putting It All Together	311
Appendix A	Tool, Sites, and References	325
Appendix B	About the CD	337
Glossary	339
Index	373

CONTENTS

	Acknowledgments	xvii
	Introduction	xix
Chapter 1	Ethical Hacking Basics	1
	Introduction to Ethical Hacking	2
	Security Basics: CIA	2
	Defining the Ethical Hacker	5
	Hacking Terminology and Attacks	11
	Legal Hacking: Laws and Guidelines You Need to Know	14
	U.S. Cyber Crime Laws	15
	International Cyber Crime Laws	18
	Chapter Review	20
	Questions	22
	Answers	24
Chapter 2	Cryptography 101	27
	Cryptography and Encryption Overview	28
	Encryption Algorithms and Techniques	28
	PKI, the Digital Certificate, and Digital Signatures	38
	The PKI System	39
	Digital Certificates	40
	Digital Signatures	43
	Encrypted Communication and Cryptography Attacks	44
	Data Encryption: At Rest and While Communicating	44
	Cryptography Attacks	46
	Chapter Review	47
	Questions	49
	Answers	51
Chapter 3	Reconnaissance: Information Gathering for the Ethical Hacker ...	53
	Vulnerability Research	54
	Footprinting	58
	Footprinting with DNS	62
	Determining Network Range	71
	Google Hacking	74
	Other Tips and Tools	77
	Chapter Review	78
	Questions	81
	Answers	83

Chapter 4	Scanning and Enumeration	85
	Scanning for Targets	86
	Identifying Active Machines	87
	Port Scanning	91
	Other Scanning Tips and Tools	105
	Enumeration	107
	Windows Security Basics	108
	Enumeration Techniques	110
	Chapter Review	113
	Questions	117
	Answers	119
Chapter 5	Hacking Through the Network: Sniffers and Evasion	121
	Sniffing	122
	Communications Basics	122
	Sniffing Techniques and Tools	127
	Network Roadblocks	136
	Intrusion Detection	136
	Firewalls and Honeypots	144
	Chapter Review	149
	Questions	151
	Answers	153
Chapter 6	Attacking a System	155
	Windows System Hacking	156
	Password Cracking	156
	Escalating Privileges and Maintaining Stealth	168
	Linux Hacking	177
	Linux Essentials	177
	Hardening a Linux Machine	184
	Chapter Review	187
	Questions	189
	Answers	192
Chapter 7	Low Tech: Social Engineering and Physical Security	193
	Social Engineering	194
	Human-Based Attacks	195
	Computer-Based Attacks	197
	Physical Security	202
	Physical Security 101	202
	Chapter Review	213
	Questions	214
	Answers	217

Chapter 8	Web-Based Hacking: Servers and Applications	219
	Attacking Web Servers	220
	Web Services Architecture	220
	Web Attacks	225
	Web Applications	230
	Application Attacks	230
	Protecting Your Web Resources	240
	Chapter Review	244
	Questions	246
	Answers	249
Chapter 9	Wireless Network Hacking	251
	Wireless 101	252
	Network Architecture and Standards	252
	Finding and Identifying Wireless Networks	259
	Wireless Hacking	265
	Wireless Attacks	265
	Bluetooth Attacks	273
	Chapter Review	274
	Questions	279
	Answers	282
Chapter 10	Trojans and Other Attacks	283
	The “Malware” Attacks	284
	Trojans, Backdoors, Viruses, and Worms	284
	Remaining Attacks	295
	Denial of Service	295
	Session Hijacking	298
	Chapter Review	301
	Questions	306
	Answers	308
Chapter 11	The Pen Test: Putting It All Together	311
	Methodology and Steps	312
	The Security Assessments	312
	Security Assessment Deliverables	318
	Chapter Review	319
	Questions	321
	Answers	323
Appendix A	Tool, Sites, and References	325
	Vulnerability Research Sites	325
	Footprinting Tools	326
	Website Research Tools	326

DNS and WHOIS Tools	326
Traceroute Tools and Links	326
Website Mirroring Tools and Sites	327
E-mail Tracking	327
Google Hacking	327
Scanning and Enumeration Tools	327
Ping Sweep	327
Scanning Tools	328
War Dialing	328
Banner Grabbing	328
Vulnerability Scanning	328
Proxy, Anonymizer, and Tunneling	329
Enumeration	329
System Hacking Tools	330
Password Hacking Tools	330
Sniffing	330
Keyloggers and Screen Capture	330
Covering Tracks	331
Packet Crafting/Spoofing	331
Session Hijacking	331
Cryptography and Encryption	331
Encryption Tools	331
Hash Tools	332
Steganography	332
Cryptanalysis	332
Sniffing	332
Packet Capture	332
Wireless	333
MAC Flooding/Spoofing	333
ARP Poisoning	333
Trojans and Malware	333
Wrappers	333
Monitoring Tools	333
Attack Tools	334
IDS	334
Evasion Tools	334
Wireless	334
Web Attacks	335
SQL Injection	335
Miscellaneous	336
Pen Test Suites	336
Extras	336
Linux Distributions	336
Tools, Sites, and References Disclaimer	336

Appendix B	About the CD	337
	System Requirements	337
	Installing and Running MasterExam	337
	MasterExam	337
	Electronic Book	338
	Help	338
	Removing Installation(s)	338
	Technical Support	338
	LearnKey Technical Support	338
Glossary	339
Index	373