ISSA

INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

Ethical Hacking: Techniques, Tools, and Countermeasures

FOURTH EDITION

Michael G. Solomon | Sean-Philip Oriyano

JONES & BARTLETT
LEARNING

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

World Headquarters
Jones & Bartlett Learning
25 Mall Road
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

The content, statements, views, and opinions herein are the sole expression of the respective authors and not that of Jones & Bartlett Learning, LLC. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement or recommendation by Jones & Bartlett Learning, LLC and such reference shall not be used for advertising or product endorsement purposes. All trademarks displayed are the trademarks of the parties noted herein. *Ethical Hacking: Techniques, Tools, and Countermeasures, Fourth Edition* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product.

There may be images in this book that feature models; these models do not necessarily endorse, represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious but are used for instructional purposes only.

24911-8

Production Credits
Vice President, Product Management: Marisa R. Urbano
Vice President, Content Strategy and Implementation: Christine Emerton
Director, Product Management: Ray Chew
Product Owner, Labs: Garret Donaldson
Director, Content Management: Donna Gridley
Manager, Content Strategy: Carolyn Pershouse
Content Strategist: Melissa Duffy
Content Coordinator: Mark Restuccia
Director, Project Management and Content Services: Karen Scott
Manager, Program Management: Kristen Rogers
Program Manager: Kathryn Leeber
Senior Digital Project Specialist: Angela Dooley
Director, Marketing: Andrea DeFronzo
Marketing Manager: Mark Adamiak
Content Services Manager: Colleen Lamy
Vice President, Manufacturing and Inventory Control: Therese Connell
Product Fulfillment Manager: Wendy Kilborn
Composition: Straive
Cover Design: Briana Yates
Media Development Editor: Faith Brosnan
Rights & Permissions Manager: John Rusk
Rights Specialist: James Fortney
Cover Image (Title Page, Part Opener, Chapter Opener): © Bocos Benedict/Shutterstock
Printing and Binding: McNaughton & Gunn

Library of Congress Cataloging-in-Publication Data
Names: Solomon, Michael (Michael G.), 1963– author.
Title: Ethical hacking : techniques, tools, and countermeasures / Michael G. Solomon, PhD, CISSP, PMP, CISM, PenTest+, CySA+.
Other titles: Hacker techniques, tools, and incident handling
Description: Fourth edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2024] | Previous edition: Hacker techniques, tools, and incident handling. Third edition. Burlington, MA : Jones & Bartlett Learning, 2020. | Includes bibliographical references and index.
Identifiers: LCCN 2022026903 | ISBN 9781284248999 (paperback)
Classification: LCC TK5105.59 .O786 2024 | DDC 005.8–dc23/eng/20220826
LC record available at https://lccn.loc.gov/2022026903

6048

Printed in the United States of America
26 25 24 23 22 10 9 8 7 6 5 4 3 2 1

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

This text is dedicated to our readers and students and the IT professionals who are pursuing careers in information systems security. May you find learning about hacking for ethical purposes to be a rewarding endeavor, and have a lot of fun in the process.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Contents

© Bocos Benedict/Shutterstock.

Preface xvii

Acknowledgments xix

About the Authors xxi

PART I **Hacker Techniques and Tools** 1

CHAPTER 1 **Hacking: The Next Generation** 3

Profiles and Motives of Different Types of Hackers 4

Controls 6
The Hacker Mindset 6
Motivations of Hackers 7

A Look at the History of Computer Hacking 9

Ethical Hacking and Penetration Testing 10

The Role of Ethical Hacking 11
Ethical Hackers and the C-I-A Triad 13

Common Hacking Methodologies 14

Performing a Penetration Test 15

The Role of the Law and Ethical Standards 18

CHAPTER SUMMARY 20
KEY CONCEPTS AND TERMS 20
CHAPTER 1 ASSESSMENT 20

CHAPTER 2 **Linux and Penetration Testing** 23

Linux 24

Introducing Kali Linux 26

Working with Linux: The Basics 27

A Look at the Interface 27
Basic Linux Navigation 28
Important Linux Directories 28
Commonly Used Commands 28
The Basic Command Structure of Linux 30
Wildcard Characters in Linux 32

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Live CDs/DVDs 32

Special-Purpose Live CDs/DVDs 34
Virtual Machines 34

CHAPTER SUMMARY 35

KEY CONCEPTS AND TERMS 35

CHAPTER 2 ASSESSMENT 36

CHAPTER 3 TCP/IP Review 37

Exploring the OSI Reference Model 38

The Role of Protocols 39
Layer 1: Physical Layer 40
Layer 2: Data Link Layer 41
Layer 3: Network Layer 42
Layer 4: Transport Layer 42
Layer 5: Session Layer 43
Layer 6: Presentation Layer 43
Layer 7: Application Layer 44
The Role of Encapsulation 44
Mapping the OSI Model to Functions and Protocols 44
OSI Model Layers and Services 45

TCP/IP: A Layer-by-Layer Review 46

Physical or Network Access Layer 47
Network or Internet Layer 51
Host-to-Host Layer 58
Application Layer 60

CHAPTER SUMMARY 64

KEY CONCEPTS AND TERMS 64

CHAPTER 3 ASSESSMENT 64

CHAPTER 4 Cryptographic Concepts 67

Cryptographic Basics 69

Authentication 70
Integrity 70
Nonrepudiation 71

Symmetric and Asymmetric Cryptography 71

Cryptographic History 72

What Is an Algorithm or Cipher? 75

Symmetric Encryption 77

Asymmetric Encryption 80

Hashing 83

Birthday Attacks 85

Digital Signatures 85

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Public Key Infrastructure 86

The Role of Certificate Authorities 89
Registration Authority 89
Certificate Revocation List 89
Digital Certificates 90
PKI Attacks 91

Common Cryptographic Systems 92

Cryptanalysis 93

Future Forms of Cryptography 96

CHAPTER SUMMARY 97
KEY CONCEPTS AND TERMS 97
CHAPTER 4 ASSESSMENT 98

PART II A Technical and Social Overview of Hacking 99

CHAPTER 5 Passive Reconnaissance 101

The Information-Gathering Process 102

Information on a Company Website and Available Through Social Media 103

Discovering Financial Information 106

Google Hacking 108

Exploring Domain Information Leakage 111

Manual Registrar Query 112
Nslookup 113
Automatic Registrar Query 116
Whois 116
Internet Assigned Numbers Authority 118
Determining a Network Range 120
Traceroute 121

Tracking an Organization's Employees 122

Using Social Networks 124

Using Basic Countermeasures 125

CHAPTER SUMMARY 126
KEY CONCEPTS AND TERMS 127
CHAPTER 5 ASSESSMENT 127

CHAPTER 6 Active Reconnaissance 129

Determining Address Ranges of Networks 130

Identifying Active Machines 131

Wardialing 131

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Wardriving and Related Activities 131
Pinging 133
Port Scanning 134

Active Reconnaissance Countermeasures 137

Mapping Open Ports 138

Nmap 138
Free IP Scanner 140
Angry IP Scanner 141
Advanced IP Scanner 141

Operating System Fingerprinting 143

Active OS Fingerprinting 144
Passive OS Fingerprinting 145

Mapping the Network 147

Analyzing the Results 148

CHAPTER SUMMARY 149

KEY CONCEPTS AND TERMS 149

CHAPTER 6 ASSESSMENT 150

CHAPTER 7 **Enumeration and Exploitation 151**

Windows Basics 152

Controlling Access 153
Users 153
Groups 155
Security Identifiers 156
Commonly Attacked and Exploited Services 156

Enumeration 157

Performing Enumeration Tasks 158

NULL Session 158
Working with nbtstat 160
SuperScan 161
SNScan 162

Reporting 162

Exploitation 163

Password Cracking 164

Passive Online Attacks 165
Active Online Attacks 165
Offline Attacks 166
Nontechnical Attacks 169
Using Password Cracking 170

Privilege Escalation 170

Active@ Password Changer 171

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Reset Windows Password 171
Stopping Privilege Escalation 174

Planting Backdoors 174

Using PsTools 175
Rootkits 175

Covering Tracks 177

Disabling Auditing 177
Data Hiding 178

CHAPTER SUMMARY 179

KEY CONCEPTS AND TERMS 180

CHAPTER 7 ASSESSMENT 180

CHAPTER 8 Malware 183

Malware 184

Malware's Legality 186
Types of Malware 187
Malware's Targets 187

Viruses 188

The History of Viruses 188
Types of Viruses 189
Prevention Techniques 192

Worms 193

How Worms Work 194
Stopping Worms 195

Trojans 196

Use of Trojans 197
Targets of Trojans 198
Known Symptoms of an Infection 198
Detection of Trojans 199
Distribution Methods 202

Backdoors 203

Covert Communication 204

Keystroke Loggers 205

Software 205
Hardware 206

Port Redirection 206

Spyware 208

Methods of Infection 208
Bundling with Software 209

Adware 210

Scareware 210

Ransomware 211

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

CHAPTER SUMMARY 212
KEY CONCEPTS AND TERMS 212
CHAPTER 8 ASSESSMENT 213

CHAPTER 9 Web and Database Attacks 215

Attacking Web Servers 216

Categories of Risk 217

Vulnerabilities of Web Servers 218

Improper or Poor Web Design 218
Buffer Overflow 219
Denial of Service Attack 219
Distributed Denial of Service Attack 219
Banner Information 220
Permissions 221
Error Messages 221
Unnecessary Features 222
User Accounts 223

Structured Query Language (SQL) Injection 223

Examining a SQL Injection Attack 223

Vandalizing Web Servers 225

Input Validation 225
Cross-Site Scripting Attack 226

Anatomy of Web Applications 227

Insecure Logon Systems 227
Scripting Errors 228
Session Management Issues 229
Encryption Weaknesses 230

Database Vulnerabilities 230

Types of Databases 231
Vulnerabilities 232
Locating Databases on the Network 232
Database Server Password Cracking 233
Locating Vulnerabilities in Databases 234

Cloud Computing 235

CHAPTER SUMMARY 236
KEY CONCEPTS AND TERMS 237
CHAPTER 9 ASSESSMENT 237

CHAPTER 10 Sniffers, Session Hijacking, and Denial of Service Attacks 239

Sniffers 240

Passive Sniffing 241
Active Sniffing 242
Sniffing Tools 246

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

What Can Be Sniffed? 247

Session Hijacking 247

Identifying an Active Session 248
Seizing Control of a Session 250
Session Hijacking Tools 250
Thwarting Session Hijacking Attacks 251

Denial of Service Attacks 251

Types of DoS Attacks 252
Tools for DoS Attacks 254

Distributed Denial of Service Attacks 254

Characteristics of DDoS Attacks 255
Tools for DDoS Attacks 256

Botnets and the Internet of Things 257

CHAPTER SUMMARY 258

KEY CONCEPTS AND TERMS 259

CHAPTER 10 ASSESSMENT 259

CHAPTER 11 **Wireless Vulnerabilities 261**

The Importance of Wireless Security 262

Emanations 262
Common Support and Availability 263

A Brief History of Wireless Technologies 264

802.11 264
802.11b 265
802.11a 265
802.11g 266
802.11n 266
802.11ac 266
802.11ax 267
Other 802.11 Variants 267
Other Wireless Technologies 267

Working with and Securing Bluetooth 268

Bluetooth Security 269
Securing Bluetooth 272

Working with Wireless LANs 272

CSMA/CD Versus CSMA/CA 272
Role of Access Points 273
Service Set Identifier 273
Association with an AP 274
The Importance of Authentication 274
Working with RADIUS 274
Network Setup Options 274
Threats to Wireless LANs 275
Countermeasures to Wireless LAN Threats 278

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

The Internet of Things 279

Wireless Hacking Tools 280

Homedale 280
The inSSIDer Program 281
Protecting Wireless Networks 282
Default AP Security 282
Placement 282
Dealing with Emanations 282
Dealing with Rogue APs 282
Use Protection for Transmitted Data 283
MAC Filtering 283

CHAPTER SUMMARY 284

KEY CONCEPTS AND TERMS 284

CHAPTER 11 ASSESSMENT 284

CHAPTER 12 **Social Engineering 287**

What Is Social Engineering? 288

Types of Social Engineering Attacks 289

Phone-Based Attacks 289
Dumpster Diving 289
Shoulder Surfing 290
Attacks Through Social Media 290
Persuasion/Coercion 290
Reverse Social Engineering 290

Technology and Social Engineering 291

The Browser as a Defense Against Social Engineering 291
Other Good Practices for Safe Computing 292

Best Practices for Passwords 294

Know What the Web Knows About You 294
Creating and Managing Your Passwords 294
Invest in a Password Manager 295

Social Engineering and Social Networking 295

Think Before You Post 296
Risks Associated with Social Networking 296

Social Networking in a Corporate Setting 299

Particular Concerns in a Corporate Setting 300
Mixing the Personal with the Professional 300

Facebook Security 302

CHAPTER SUMMARY 303

KEY CONCEPTS AND TERMS 304

CHAPTER 12 ASSESSMENT 304

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

PART III Defensive Techniques and Tools 307

CHAPTER 13 Defensive Techniques 309

What Is a Security Incident? 310

The Incident Response Process 311

Incident Response Policies, Procedures, and Guidelines 312
Phases of an Incident and Response 313
Incident Response Team 314
Incident Response Plans 315
Business Continuity Plans 315

Recovering Systems 318

Recovering from a Security Incident 318
Loss Control and Damage Assessment 319
Business Impact Analysis 319

Planning for Disaster and Recovery 320

Testing and Evaluation 321

Preparation and Staging of Testing Procedures 322
Frequency of Tests 323
Analysis of Test Results 323

Evidence Handling and Administration 323

Evidence Collection Techniques 323
Types of Evidence 324
Chain of Custody 325
Computer or Device Removal 325
Rules of Evidence 325

Security Reporting Options and Guidelines 326

Requirements of Regulated Industries 327

CHAPTER SUMMARY 328
KEY CONCEPTS AND TERMS 329
CHAPTER 13 ASSESSMENT 329

CHAPTER 14 Defensive Tools 331

Defense in Depth 332

Intrusion Detection Systems 332

IDS Components 336
Setting Goals for an IDS 339
Accountability 340
Limitations of an IDS 340

Intrusion Prevention Systems 341

Firewalls 342

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

How Firewalls Work 342
Firewall Methodologies 343
Limitations of a Firewall 344
Implementing a Firewall 345
Authoring a Firewall Policy 346

Honeypots and Honeynets 348

Goals of Honeypots 348
Legal Issues 349

The Role of Controls 349

Administrative Controls 350
Technical Controls 350
Physical Controls 352

Security Best Practices 353

Security Information and Event Management 353
Sources for Guidance 354

CHAPTER SUMMARY 354

KEY CONCEPTS AND TERMS 355

CHAPTER 14 ASSESSMENT 355

CHAPTER 15 **Physical Security 357**

Basic Equipment Controls 358

Hard Drive and Mobile Device Encryption 358
Fax Machines and Printers 361
Voice over Internet Protocol 362

Physical Area Controls 362

Fences 363
Perimeter Intrusion Detection and Assessment Systems 364
Gates 364
Bollards 365

Facility Controls 366

Doors, Mantraps, and Turnstiles 366
Walls, Ceilings, and Floors 367
Windows 368
Guards and Dogs 368
Construction 369

Personal Safety Controls 369

Lighting 370
Alarms and Intrusion Detection 370
Closed-Circuit TV and Remote Monitoring 371

Physical Access Controls 372

Locks 372
Tokens and Biometrics 373

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Avoiding Common Threats to Physical Security 374

Natural, Human, and Technical Threats 374
Physical Keystroke Loggers and Sniffers 375
Wireless Interception and Rogue Access Points 376

Defense in Depth 377

CHAPTER SUMMARY 378
KEY CONCEPTS AND TERMS 378
CHAPTER 15 ASSESSMENT 378

APPENDIX A Answer Key 381

APPENDIX B Standard Acronyms 383

Glossary of Key Terms 385

References 393

Index 397

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Preface

© Bocos Benedict/Shutterstock.

Purpose of This Text

This text is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (www.jblearning.com). Designed for courses and curricula in IT security, cybersecurity, information assurance, and information systems security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), the text delivers comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these texts are not just current but also forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow as well.

The first part of this text on information security examines the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It covers the history of hacking and the standards of ethical hacking. The second part provides a technical overview of hacking: how attackers target networks and the methodology they follow. It reviews the various techniques attackers apply, including passive and active reconnaissance, port scanning, enumeration, malware, sniffers, denial of service, and social engineering. The third part of the text reviews incident response and defensive technologies, including how to respond to hacking attacks and how to fend them off, especially in an age of increased reliance on cloud environments and distributed applications.

Learning Features

The writing style of this text is practical and conversational. Each chapter begins with a statement of learning objectives. Step-by-step examples of information security concepts and procedures are presented throughout the text. Illustrations are used to both clarify the material and vary the presentation. Sprinkled throughout are a wealth of Notes, Tips, FYIs, Warnings, and sidebars to alert the reader to additional helpful information related to the subject under discussion. Chapter Assessments appear at the end of each chapter, with solutions provided in the back of the text.

Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

New to This Edition

This new edition has been updated to better reflect the infrastructures and security threats readers are most likely to encounter in today's organizations. The content has been slightly reorganized, extended, and refreshed to ensure that it covers the latest cybersecurity attack trends, tools and techniques, and industry best practices.

Part I, Foundations of Hacking, covers many of the threats that today's distributed IT environments face, along with some skills and basic knowledge that ethical hackers need to be successful. The chapter that covers Linux and penetration testing was moved into this part so that readers would be introduced to ethical hacking activities earlier in the text.

Part II, Hacker Techniques and Tools, continues the discussion from Part I to form the core technical material of the text. In Part II, we dig into the various aspects of carrying out ethical hacking activities, including reconnaissance, enumeration exploitation, and attacks on web, database, wireless, and mobile environments. This edition retains the technical information from previous editions but updates the tools and techniques to reflect the latest state of the art. Additional emphasis is placed on planning, scoping, and carrying a penetration testing plan.

Finally, Part III, Defensive Tools and Techniques, extends the content from previous editions to go beyond incident response and cover key defensive techniques and best practices. This latest edition provides the most comprehensive coverage to date of how to implement an ethical hacking initiative as a strategic organizational objective.

Audience

This material is suitable for undergraduate or graduate computer science majors or information science majors, students at a two-year technical college or community college who have a basic technical background, and readers who have a basic understanding of IT security and want to expand their knowledge.

Cloud Labs

This text is accompanied by Cloud Labs. These hands-on virtual labs provide immersive mock IT infrastructures where students can learn and practice foundational cybersecurity skills as an extension of the lessons in this text. For more information or to purchase the labs, visit http://go.jblearning.com/ethicalhacking4e.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Acknowledgments

© Bocos Benedict/Shutterstock.

I want to thank God for blessing me so richly with such a wonderful family and with their support throughout the years. My best friend and wife of more than three decades, Stacey, is my biggest cheerleader and supporter through many professional and academic projects. I would not be who I am without her.

Both our sons have always been sources of support and inspiration as well. I thank Noah, who still challenges me, keeps me sharp, and tries to keep me relevant, and Isaac, who left us far too early. We miss you.

Michael G. Solomon

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

About the Authors

© Bocos Benedict/Shutterstock.

Michael G. Solomon, PhD, is an educator; a full-time security, privacy, compliance, and blockchain consultant; a speaker; and an author who specializes in leading teams in achieving and maintaining secure and effective IT environments. Michael is a professor of Information Systems Security and Information Technology at the University of the Cumberlands. As an industry consultant since 1987, he has led project teams for many *Fortune 500* companies and has authored and contributed to more than 30 books and numerous training courses. Michael holds the CISSP, PMP, PenTest+, CySA+, and CISM certifications, and has a PhD in Computer Science and Informatics from Emory University.

Sean-Philip Oriyano has been actively working in the IT field since 1990. Throughout his career, he has held positions such as support specialist to consultants and senior instructor. Currently he is an IT instructor who specializes in infrastructure and security topics for various public and private entities. Sean has instructed for the US Air Force, Navy, and Army at locations both in North America and internationally. Sean is certified as a CISSP, CHFI, CEH, CEI, CNDA, SCNP, SCPI, MCT, MCSE, and MCITP, and he is a member of EC-Council, ISSA, Elearning Guild, and Infragard.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.