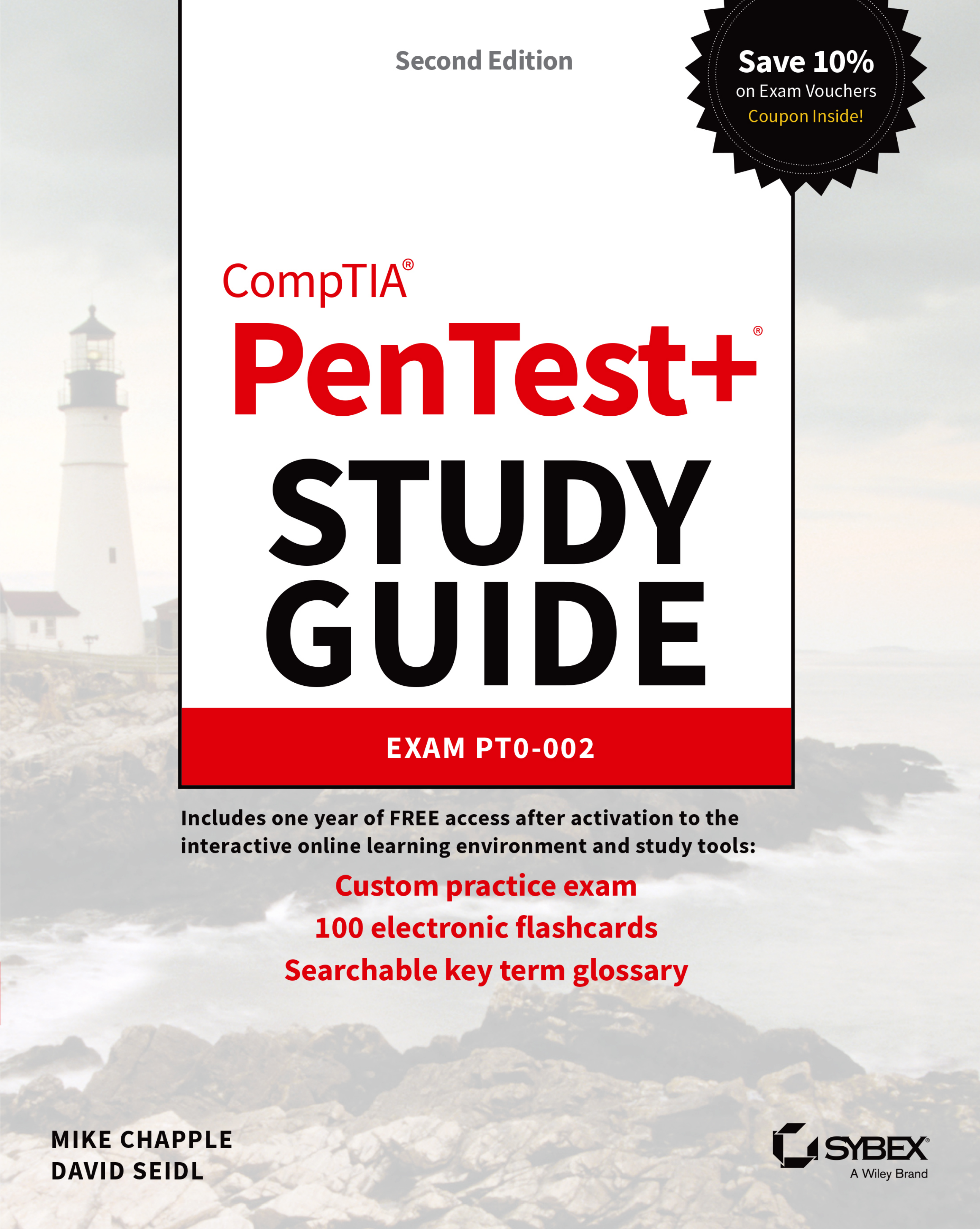


Second Edition

CompTIA® PenTest+® STUDY GUIDE

EXAM PT0-002

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

Custom practice exam
100 electronic flashcards
Searchable key term glossary

MIKE CHAPPLE
DAVID SEIDL

SYBEX®
A Wiley Brand

CompTIA®

PenTest+®

Study Guide

Exam PT0-002

Second Edition

Mike Chapple

David Seidl

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

978-1-119-82381-0
978-1-119-82383-4 (ebk.)
978-1-119-82382-7 (ebk.)

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware the Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at `www.wiley.com`.

Library of Congress Control Number: 2021944464

Cover image: © Getty Images Inc./Jeremy Woodhouse

Cover design: Wiley

This book is dedicated to Ron Kraemer—a mentor, friend, and wonderful boss.

Acknowledgments

Books like this involve work from many people, and as authors, we truly appreciate the hard work and dedication that the team at Wiley shows. We would especially like to thank Senior Acquisitions Editor Kenyon Brown. We have worked with Ken on multiple projects and consistently enjoy our work with him.

We also greatly appreciated the editing and production team for the book, including John Sleeva, our project editor, whose prompt and consistent oversight got this book out the door, and Barath Kumar Rajasekaran, our content refinement specialist, who guided us through layouts, formatting, and final cleanup to produce a great book. We'd also like to thank our technical editor, Nadean Tanner, who provided us with thought-provoking questions and technical insight throughout the process. We would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who make the book and companion materials into a finished product.

Our agent, Carole Jelen of Waterside Productions, continues to provide us with wonderful opportunities, advice, and assistance throughout our writing careers.

Finally, we would like to thank our families, friends, and significant others who support us through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

About the Authors

Mike Chapple, PhD, Security+, CISSP, CISA, PenTest+, CySA+, is a teaching professor of IT, analytics, and operations at the University of Notre Dame. He is also the academic director of the University's master's program in business analytics.

Mike is a cybersecurity professional with over 20 years of experience in the field. Prior to his current role, Mike served as senior director for IT service delivery at Notre Dame, where he oversaw the University's cybersecurity program, cloud computing efforts, and other areas. Mike also previously served as chief information officer of Brand Institute and an information security researcher with the National Security Agency and the U.S. Air Force.

Mike is a frequent contributor to several magazines and websites and is the author or coauthor of more than 25 books, including *CISSP Official (ISC)² Study Guide* (Wiley, 2021), *CISSP Official (ISC)² Practice Tests* (Wiley, 2021), *CompTIA Security+ Study Guide* (Wiley, 2020), *CompTIA CySA+ Study Guide* (Wiley, 2020), *CompTIA CySA+ Practice Tests* (Wiley, 2020), and *Cybersecurity: Information Operations in a Connected World* (Jones and Bartlett, 2021).

Mike offers free study groups for the PenTest+, CySA+, Security+, CISSP, and SSCP certifications at his website, `certmike.com`.

David Seidl, CISSP, PenTest+, is vice president for information technology and CIO at Miami University. During his IT career, he has served in a variety of technical and information security roles, including serving as the senior director for campus technology services at the University of Notre Dame, where he co-led Notre Dame's move to the cloud and oversaw cloud operations, ERP, databases, identity management, and a broad range of other technologies and service. He also served as Notre Dame's director of information security and led Notre Dame's information security program. He has taught information security and networking undergraduate courses as an instructor for Notre Dame's Mendoza College of Business, and he has written books on security certification and cyberwarfare, including co-authoring the previous editions of *CISSP (ISC)² Official Practice Tests* (Sybex, 2018) as well as *CISSP Official (ISC)² Practice Tests* (Wiley, 2021), *CompTIA Security+ Study Guide* (Wiley, 2020), *CompTIA Security+ Practice Tests* (Wiley, 2020), *CompTIA CySA+ Study Guide* (Wiley, 2020), *CompTIA CySA+ Practice Tests* (Wiley, 2020), and *Cybersecurity: Information Operations in a Connected World* (Jones and Bartlett, 2021), *and CompTIA Security+ Practice Tests: Exam SY0-601*, as well as other certification guides and books on information security.

David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University, as well as CISSP, CySA+, PenTest+, GPEN, and GCIH certifications.

About the Technical Editor

Nadean Hutto Tanner is the manager of Consulting-Education Services at FireEye/Mandiant, working most recently on building real-world cyber-range engagements to practice threat hunting and incident response. She has been in IT for more than 20 years and in cybersecurity specifically for over a decade. She holds over 30 industry certifications, including CompTIA CASP+ and ISC^2 CISSP.

Tanner has trained and consulted for Fortune 500 companies and the U.S. Department of Defense in cybersecurity, forensics, analysis, red/blue teaming, vulnerability management, and security awareness.

She is the author of the *Cybersecurity Blue Team Toolkit* (Wiley, 2019) and *CASP+ Practice Tests: Exam CAS-003* (Sybex, 2020). She also was the technical editor for the *CompTIA Security+ Study Guide: Exam SY0-601* (Sybex, 2021), written by Mike Chapple and David Seidl.

In her spare time, she enjoys speaking at technical conferences such as Black Hat, Wild West Hacking Fest, and OWASP events.

Contents at a Glance

Introduction *xxv*

Assessment Test *xxxix*

Chapter 1 Penetration Testing 1

Chapter 2 Planning and Scoping Penetration Tests 31

Chapter 3 Information Gathering 59

Chapter 4 Vulnerability Scanning 109

Chapter 5 Analyzing Vulnerability Scans 151

Chapter 6 Exploiting and Pivoting 195

Chapter 7 Exploiting Network Vulnerabilities 243

Chapter 8 Exploiting Physical and Social Vulnerabilities 287

Chapter 9 Exploiting Application Vulnerabilities 311

Chapter 10 Attacking Hosts, Cloud Technologies, and Specialized Systems 355

Chapter 11 Reporting and Communication 405

Chapter 12 Scripting for Penetration Testing 429

Appendix A Answers to Review Questions 485

Appendix B Solution to Lab Exercise 509

Index *511*

Contents

Introduction *xxv*

Assessment Test *xxxix*

Chapter 1 Penetration Testing 1

What Is Penetration Testing? 2
Cybersecurity Goals 2
Adopting the Hacker Mindset 4
Ethical Hacking 5
Reasons for Penetration Testing 5
Benefits of Penetration Testing 6
Regulatory Requirements for Penetration Testing 7
Who Performs Penetration Tests? 8
Internal Penetration Testing Teams 8
External Penetration Testing Teams 9
Selecting Penetration Testing Teams 10
The CompTIA Penetration Testing Process 10
Planning and Scoping 11
Information Gathering and Vulnerability Scanning 11
Attacks and Exploits 12
Reporting and Communication 13
Tools and Code Analysis 13
The Cyber Kill Chain 14
Reconnaissance 15
Weaponization 16
Delivery 16
Exploitation 16
Installation 16
Command and Control 16
Actions on Objectives 17
Tools of the Trade 17
Reconnaissance 20
Vulnerability Scanners 21
Social Engineering 21
Credential Testing Tools 22
Debuggers and Software Testing Tools 22
Network Testing 23
Remote Access 23
Exploitation 24
Steganography 24
Cloud Tools 25

Summary 25
Exam Essentials 25
Lab Exercises 26
Activity 1.1: Adopting the Hacker Mindset 26
Activity 1.2: Using the Cyber Kill Chain 26
Review Questions 27

Chapter 2 Planning and Scoping Penetration Tests 31

Scoping and Planning Engagements 34
Assessment Types 35
Known Environments and Unknown Environments 35
The Rules of Engagement 37
Scoping Considerations—A Deeper Dive 39
Support Resources for Penetration Tests 42
Penetration Testing Standards and Methodologies 44
Key Legal Concepts for Penetration Tests 46
Contracts 46
Data Ownership and Retention 47
Permission to Attack (Authorization) 47
Environmental Differences and Location Restrictions 48
Regulatory Compliance Considerations 49
Summary 51
Exam Essentials 52
Lab Exercises 53
Review Questions 54

Chapter 3 Information Gathering 59

Footprinting and Enumeration 63
OSINT 64
Location and Organizational Data 65
Infrastructure and Networks 68
Security Search Engines 74
Google Dorks and Search Engine Techniques 77
Password Dumps and Other Breach Data 77
Source Code Repositories 78
Passive Enumeration and Cloud Services 78
Active Reconnaissance and Enumeration 78
Hosts 79
Services 79
Networks, Topologies, and Network Traffic 85
Packet Crafting and Inspection 88
Enumeration 90
Information Gathering and Code 97
Avoiding Detection 99
Information Gathering and Defenses 99

Defenses Against Active Reconnaissance 100
Preventing Passive Information Gathering 100
Summary 100
Exam Essentials 101
Lab Exercises 102
Activity 3.1: Manual OSINT Gathering 102
Activity 3.2: Exploring Shodan 102
Activity 3.3: Running an Nmap Scan 103
Review Questions 104

Chapter 4 Vulnerability Scanning 109

Identifying Vulnerability Management Requirements 112
Regulatory Environment 112
Corporate Policy 116
Support for Penetration Testing 116
Identifying Scan Targets 117
Determining Scan Frequency 118
Active vs. Passive Scanning 120
Configuring and Executing Vulnerability Scans 121
Scoping Vulnerability Scans 121
Configuring Vulnerability Scans 122
Scanner Maintenance 129
Software Security Testing 131
Analyzing and Testing Code 131
Web Application Vulnerability Scanning 133
Developing a Remediation Workflow 138
Prioritizing Remediation 140
Testing and Implementing Fixes 141
Overcoming Barriers to Vulnerability Scanning 141
Summary 143
Exam Essentials 143
Lab Exercises 144
Activity 4.1: Installing a Vulnerability Scanner 144
Activity 4.2: Running a Vulnerability Scan 145
Activity 4.3: Developing a Penetration Test Vulnerability Scanning Plan 145
Review Questions 146

Chapter 5 Analyzing Vulnerability Scans 151

Reviewing and Interpreting Scan Reports 152
Understanding CVSS 156
Validating Scan Results 162
False Positives 162
Documented Exceptions 162
Understanding Informational Results 163

Reconciling Scan Results with Other Data Sources 164
Trend Analysis 164
Common Vulnerabilities 165
Server and Endpoint Vulnerabilities 166
Network Vulnerabilities 175
Virtualization Vulnerabilities 181
Internet of Things (IoT) 183
Web Application Vulnerabilities 184
Summary 186
Exam Essentials 187
Lab Exercises 188
Activity 5.1: Interpreting a Vulnerability Scan 188
Activity 5.2: Analyzing a CVSS Vector 188
Activity 5.3: Developing a Penetration Testing Plan 189
Review Questions 190

Chapter 6 Exploiting and Pivoting 195

Exploits and Attacks 198
Choosing Targets 198
Enumeration 199
Identifying the Right Exploit 201
Exploit Resources 204
Exploitation Toolkits 206
Metasploit 206
PowerSploit 212
BloodHound 213
Exploit Specifics 213
RPC/DCOM 213
PsExec 214
PS Remoting/WinRM 214
WMI 214
Fileless Malware and Living Off the Land 215
Scheduled Tasks and cron Jobs 216
SMB 217
DNS 219
RDP 220
Apple Remote Desktop 220
VNC 220
SSH 220
Network Segmentation Testing and Exploits 221
Leaked Keys 222
Leveraging Exploits 222
Common Post-Exploit Attacks 222
Cross Compiling 225
Privilege Escalation 226

Social Engineering 226
Escaping and Upgrading Limited Shells 227
Persistence and Evasion 228
Scheduled Jobs and Scheduled Tasks 228
Inetd Modification 228
Daemons and Services 229
Backdoors and Trojans 229
Data Exfiltration and Covert Channels 230
New Users 230
Pivoting 231
Covering Your Tracks 232
Summary 233
Exam Essentials 234
Lab Exercises 235
Activity 6.1: Exploit 235
Activity 6.2: Discovery 235
Activity 6.3: Pivot 236
Review Questions 237

Chapter 7 Exploiting Network Vulnerabilities 243

Identifying Exploits 247
Conducting Network Exploits 247
VLAN Hopping 247
DNS Cache Poisoning 249
On-Path Attacks 251
NAC Bypass 254
DoS Attacks and Stress Testing 255
Exploit Chaining 257
Exploiting Windows Services 257
NetBIOS Name Resolution Exploits 257
SMB Exploits 261
Identifying and Exploiting Common Services 261
Identifying and Attacking Service Targets 262
SNMP Exploits 263
SMTP Exploits 264
FTP Exploits 265
Kerberoasting 266
Samba Exploits 267
Password Attacks 268
Stress Testing for Availability 269
Wireless Exploits 269
Attack Methods 269
Finding Targets 270
Attacking Captive Portals 270
Eavesdropping, Evil Twins, and Wireless On-Path Attacks 271

Other Wireless Protocols and Systems 275
RFID Cloning 276
Jamming 277
Repeating 277
Summary 278
Exam Essentials 279
Lab Exercises 279
Activity 7.1: Capturing Hashes 279
Activity 7.2: Brute-Forcing Services 280
Activity 7.3: Wireless Testing 281
Review Questions 282

Chapter 8 Exploiting Physical and Social Vulnerabilities 287

Physical Facility Penetration Testing 290
Entering Facilities 290
Information Gathering 294
Social Engineering 294
In-Person Social Engineering 295
Phishing Attacks 297
Website-Based Attacks 298
Using Social Engineering Tools 298
Summary 302
Exam Essentials 303
Lab Exercises 303
Activity 8.1: Designing a Physical Penetration Test 303
Activity 8.2: Brute-Forcing Services 304
Activity 8.3: Using BeEF 305
Review Questions 306

Chapter 9 Exploiting Application Vulnerabilities 311

Exploiting Injection Vulnerabilities 314
Input Validation 314
Web Application Firewalls 315
SQL Injection Attacks 316
Code Injection Attacks 319
Command Injection Attacks 319
LDAP Injection Attacks 320
Exploiting Authentication Vulnerabilities 320
Password Authentication 321
Session Attacks 322
Kerberos Exploits 326
Exploiting Authorization Vulnerabilities 327
Insecure Direct Object References 327
Directory Traversal 328
File Inclusion 330
Privilege Escalation 331

Exploiting Web Application Vulnerabilities 331
Cross-Site Scripting (XSS) 331
Request Forgery 334
Clickjacking 335
Unsecure Coding Practices 335
Source Code Comments 335
Error Handling 336
Hard-Coded Credentials 336
Race Conditions 337
Unprotected APIs 337
Unsigned Code 338
Steganography 340
Application Testing Tools 341
Static Application Security Testing (SAST) 341
Dynamic Application Security Testing (DAST) 342
Mobile Tools 346
Summary 346
Exam Essentials 347
Lab Exercises 347
Activity 9.1: Application Security Testing Techniques 347
Activity 9.2: Using the ZAP Proxy 348
Activity 9.3: Creating a Cross-Site Scripting Vulnerability 348
Review Questions 349

Chapter 10 Attacking Hosts, Cloud Technologies, and Specialized Systems 355

Attacking Hosts 360
Linux 361
Windows 365
Cross-Platform Exploits 367
Credential Attacks and Testing Tools 368
Credential Acquisition 368
Offline Password Cracking 369
Credential Testing and Brute-Forcing Tools 371
Wordlists and Dictionaries 371
Remote Access 372
SSH 372
NETCAT and Ncat 373
Metasploit and Remote Access 373
Proxies and Proxychains 374
Attacking Virtual Machines and Containers 374
Virtual Machine Attacks 375
Containerization Attacks 377
Attacking Cloud Technologies 379
Attacking Cloud Accounts 379

Attacking and Using Misconfigured Cloud Assets 380
Other Cloud Attacks 382
Tools for Cloud Technology Attacks 383
Attacking Mobile Devices 384
Attacking IoT, ICS, Embedded Systems, and SCADA Devices 389
Attacking Data Storage 392
Summary 393
Exam Essentials 395
Lab Exercises 396
Activity 10.1: Dumping and Cracking the Windows SAM and Other Credentials 396
Activity 10.2: Cracking Passwords Using Hashcat 397
Activity 10.3: Setting Up a Reverse Shell and a Bind Shell 398
Review Questions 400

Chapter 11 Reporting and Communication 405

The Importance of Communication 409
Defining a Communication Path 409
Communication Triggers 410
Goal Reprioritization 410
Recommending Mitigation Strategies 411
Finding: Shared Local Administrator Credentials 412
Finding: Weak Password Complexity 413
Finding: Plaintext Passwords 414
Finding: No Multifactor Authentication 414
Finding: SQL Injection 416
Finding: Unnecessary Open Services 416
Writing a Penetration Testing Report 416
Structuring the Written Report 417
Secure Handling and Disposition of Reports 420
Wrapping Up the Engagement 421
Post-Engagement Cleanup 421
Client Acceptance 421
Lessons Learned 421
Follow-Up Actions/Retesting 422
Attestation of Findings 422
Retention and Destruction of Data 422
Summary 423
Exam Essentials 423
Lab Exercises 424
Activity 11.1: Remediation Strategies 424
Activity 11.2: Report Writing 424
Review Questions 425

Chapter 12 **Scripting for Penetration Testing** **429**

Scripting and Penetration Testing 431
Bash 432
PowerShell 433
Ruby 434
Python 435
Perl 435
JavaScript 436
Variables, Arrays, and Substitutions 438
Bash 439
PowerShell 440
Ruby 441
Python 441
Perl 442
JavaScript 442
Comparison Operations 444
String Operations 445
Bash 446
PowerShell 447
Ruby 448
Python 449
Perl 450
JavaScript 451
Flow Control 452
Conditional Execution 453
for Loops 458
while Loops 465
Input and Output (I/O) 471
Redirecting Standard Input and Output 471
Comma-Separated Values (CSV) 472
Error Handling 472
Bash 472
PowerShell 473
Ruby 473
Python 473
Advanced Data Structures 474
JavaScript Object Notation (JSON) 474
Trees 475
Reusing Code 475
The Role of Coding in Penetration Testing 476
Analyzing Exploit Code 476
Automating Penetration Tests 477
Summary 477
Exam Essentials 477

Lab Exercises 478
Activity 12.1: Reverse DNS Lookups 478
Activity 12.2: Nmap Scan 479
Review Questions 480

Appendix A Answers to Review Questions 485

Chapter 1: Penetration Testing 486
Chapter 2: Planning and Scoping Penetration Tests 487
Chapter 3: Information Gathering 489
Chapter 4: Vulnerability Scanning 491
Chapter 5: Analyzing Vulnerability Scans 493
Chapter 6: Exploiting and Pivoting 495
Chapter 7: Exploiting Network Vulnerabilities 497
Chapter 8: Exploiting Physical and Social Vulnerabilities 499
Chapter 9: Exploiting Application Vulnerabilities 501
Chapter 10: Attacking Hosts, Cloud Technologies, and Specialized Systems 503
Chapter 11: Reporting and Communication 505
Chapter 12: Scripting for Penetration Testing 506

Appendix B Solution to Lab Exercise 509

Solution to Activity 5.2: Analyzing a CVSS Vector 510

Index 511

Introduction

The *CompTIA® PenTest+® Study Guide: Exam PT0-002 Second Edition* provides accessible explanations and real-world knowledge about the exam objectives that make up the PenTest+ certification. This book will help you to assess your knowledge before taking the exam, as well as provide a stepping-stone to further learning in areas where you may want to expand your skill set or expertise.

Before you tackle the PenTest+ exam, you should already be a security practitioner. CompTIA suggests that test-takers should have intermediate-level skills based on their cybersecurity pathway. You should also be familiar with at least some of the tools and techniques described in this book. You don't need to know every tool, but understanding how to use existing experience to approach a new scenario, tool, or technology that you may not know is critical to passing the PenTest+ exam.

CompTIA

CompTIA is a nonprofit trade organization that offers certification in a variety of IT areas, ranging from the skills that a PC support technician needs, which are covered in the A+ exam, to advanced certifications like the CompTIA Advanced Security Practitioner, or CASP, certification. CompTIA divides its exams into three categories based on the skill level required for the exam and what topics it covers, as shown in the following table:

Beginner/Novice	**Intermediate**	**Advanced**
IT Fundamentals A+	Network+ Security+ CySA+ PenTest+	CASP

CompTIA recommends that practitioners follow a cybersecurity career path that begins with the IT fundamentals and A+ exam and proceeds to include the Network+ and Security+ credentials to complete the foundation. From there, cybersecurity professionals may choose the PenTest+ and/or Cybersecurity Analyst+ (CySA+) certifications before attempting the CompTIA Advanced Security Practitioner (CASP) certification as a capstone credential.

The CySA+ and PenTest+ exams are more advanced exams, intended for professionals with hands-on experience who also possess the knowledge covered by the prior exams.

CompTIA certifications are ISO and ANSI accredited, and they are used throughout multiple industries as a measure of technical skill and knowledge. In addition, CompTIA certifications, including the Security+ and the CASP, have been approved by the U.S. government as Information Assurance baseline certifications and are included in the State Department's Skills Incentive Program.

The PenTest+ Exam

The PenTest+ exam is designed to be a vendor-neutral certification for penetration testers. It is designed to assess current penetration testing, vulnerability assessment, and vulnerability management skills with a focus on network resiliency testing. Successful test-takers will prove their ability plan and scope assessments, handle legal and compliance requirements, and perform vulnerability scanning and penetration testing activities using a variety of tools and techniques, and then analyze the results of those activities.

It covers five major domains:

1. Planning and Scoping
2. Information Gathering and Vulnerability Scanning
3. Attacks and Exploits
4. Reporting and Communication
5. Tools and Code Analysis

These five areas include a range of subtopics, from scoping penetration tests to performing host enumeration and exploits, while focusing heavily on scenario-based learning.

The PenTest+ exam fits between the entry-level Security+ exam and the CompTIA Advanced Security Practitioner (CASP) certification, providing a mid-career certification for those who are seeking the next step in their certification and career path while specializing in penetration testing or vulnerability management.

The PenTest+ exam is conducted in a format that CompTIA calls "performance-based assessment." This means that the exam uses hands-on simulations using actual security tools and scenarios to perform tasks that match those found in the daily work of a security practitioner. There may be numerous types of exam questions, such as multiple-choice, fill-in-the-blank, multiple-response, drag-and-drop, and image-based problems.

CompTIA recommends that test-takers have three or four years of information security–related experience before taking this exam and that they have taken the Security+ exam or have equivalent experience, including technical, hands-on expertise. The exam costs $370 in the United States, with roughly equivalent prices in other locations around the globe. More details about the PenTest+ exam and how to take it can be found at:

`https://certification.comptia.org/certifications/pentest`

Study and Exam Preparation Tips

A test preparation book like this cannot teach you every possible security software package, scenario, and specific technology that may appear on the exam. Instead, you should focus on whether you are familiar with the type or category of technology, tool, process, or scenario presented as you read the book. If you identify a gap, you may want to find additional tools to help you learn more about those topics.

Additional resources for hands-on exercises include the following:

- `Exploit-Exercises.com` provides virtual machines, documentation, and challenges covering a wide range of security issues at `https://exploit-exercises.com`.
- Hacking-Lab provides capture-the-flag (CTF) exercises in a variety of fields at `https://www.hacking-lab.com/index.html`.
- The OWASP Hacking Lab provides excellent web application–focused exercises at `https://www.owasp.org/index.php/OWASP_Hacking_Lab`.
- PentesterLab provides a subscription-based access to penetration testing exercises at `https://www.pentesterlab.com/exercises`.

Since the exam uses scenario-based learning, expect the questions to involve analysis and thought rather than relying on simple memorization. As you might expect, it is impossible to replicate that experience in a book, so the questions here are intended to help you be confident that you know the topic well enough to think through hands-on exercises.

Taking the Exam

Once you are fully prepared to take the exam, you can visit the CompTIA website to purchase your exam voucher:

`https://store.comptia.org/Certification-Vouchers/c/11293`

CompTIA partners with Pearson VUE's testing centers, so your next step will be to locate a testing center near you. In the United States, you can do this based on your address or your zip code, while non-U.S. test-takers may find it easier to enter their city and country. You can search for a test center near you at:

`http://www.pearsonvue.com/comptia/locate`

Now that you know where you'd like to take the exam, simply set up a Pearson VUE testing account and schedule an exam:

`https://home.pearsonvue.com/comptia/onvue`

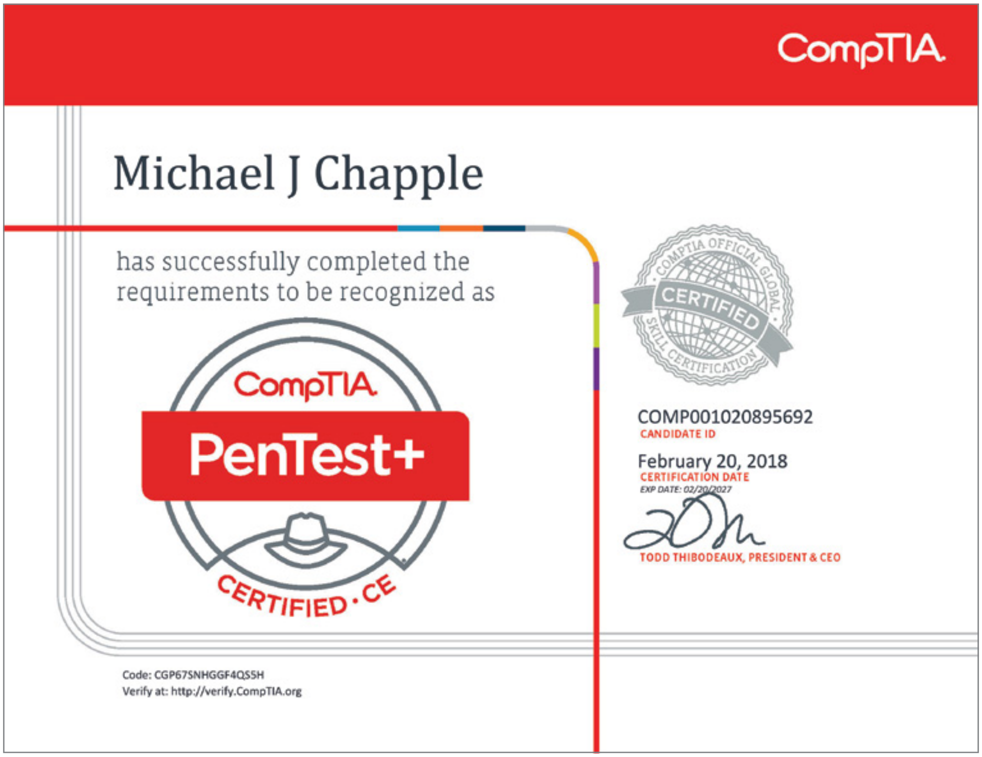
On the day of the test, take two forms of identification, and make sure to show up with plenty of time before the exam starts. Remember that you will not be able to take your notes, electronic devices (including smartphones and watches), or other materials in with you.

In some countries, including the United States, you may be eligible to take the test online from your home or office through the Pearson OnVUE program. For more information on this program and current availability, see:

`https://home.pearsonvue.com/Clients/CompTIA/OnVUE-online-proctored.aspx`

After the PenTest+ Exam

Once you have taken the exam, you will be notified of your score immediately, so you'll know if you passed the test right away. You should keep track of your score report with your exam registration records and the email address you used to register for the exam. If you've passed, you'll receive a handsome certificate, similar to the one shown here:



CompTIA

Michael J Chapple

has successfully completed the requirements to be recognized as

CompTIA PenTest+ CERTIFIED · CE

COMPTIA OFFICIAL GLOBAL SKILL CERTIFICATION CERTIFIED

COMP001020895692
CANDIDATE ID

February 20, 2018
CERTIFICATION DATE
EXP DATE: 02/20/2027

TODD THIBODEAUX, PRESIDENT & CEO

Code: CGP67SNHGGF4QS5H
Verify at: http://verify.CompTIA.org

Maintaining Your Certification

CompTIA certifications must be renewed on a periodic basis. To renew your certification, you can either pass the most current version of the exam, earn a qualifying higher-level CompTIA or industry certification, or complete sufficient continuing education activities to earn enough continuing education units (CEUs) to renew it.

CompTIA provides information on renewals via their website at:

```
https://certification.comptia.org/continuing-education/how-to-renew
```

When you sign up to renew your certification, you will be asked to agree to the CE program's Code of Ethics, to pay a renewal fee, and to submit the materials required for your chosen renewal method.