Third Edition

CompTIA® PenTest+® STUDY GUIDE

EXAM PT0-003

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
ROBERT SHIMONSKI
DAVID SEIDL

SYBEX®
A Wiley Brand

CompTIA®

PenTest+®

Study Guide

Third Edition

CompTIA®

PenTest+®

Study Guide

Exam PT0-003

Third Edition

Mike Chapple

Robert Shimonski

David Seidl

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394285006 (paperback), 9781394285020 (ePDF), 9781394285013 (ePub)

Library of Congress Control Number: 2025930423

Cover image: © Jeremy Woodhouse/Getty Images

Cover design: Wiley

This book is dedicated to Shahla Pirnia, in deepest gratitude for your unwavering dedication and meticulous care, which have shaped so many of my works. Your attention to detail and passion for excellence will always inspire me. May your legacy live on in every word we've crafted together.
— Mike

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 Pete Gaughan, managing editor, who made sure everything worked smoothly; Christine O'Connor, our project manager, whose prompt and consistent oversight got this book out the door; and Saravanan Dakshinamurthy, 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, Rishalin Pillay, 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 25 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 as 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 50 books, including *CISSP Official ISC2 Study Guide* (Wiley, 2024), *CISSP Official ISC2 Practice Tests* (Wiley, 2024), *CompTIA Security+ Study Guide* (Wiley, 2023), *CompTIA CySA+ Study Guide* (Wiley, 2023), *CompTIA CySA+ Practice Tests* (Wiley, 2023), and *Cybersecurity: Information Operations in a Connected World* (Jones and Bartlett, 2021).

Mike offers free study groups for the PenTest+, CySA+, Security+, CISSP, and other major certifications at his website, `http://certmike.com`.

Robert Shimonski, CASP+, CySA+, PenTest+, Security+, is a technology executive specializing in health care IT for one of the largest health systems in America. In his current role, Rob is responsible for bringing operational support and incident response into the future with the help of new technologies such as cloud and artificial intelligence. His current focus is on deploying securely to Cloud (Azure, AWS, and Google), DevOps, DevSecOps and AIOps. Rob has spent over 25 years in the technology "trenches" handling networking and security architecture, design, engineering, testing, and development efforts for global projects. A go-to person for all things security-related, Rob has been a major force in deploying security-related systems for many years. Rob also worked for various companies reviewing and developing curriculum as well as other security-related books, technical articles, and publications based on technology deployment, testing, hacking, pen testing, and many other aspects of security. Rob holds dozens of technology certifications to include 20+ CompTIA certifications, `SANS.org` GIAC, GSEC, and GCIH as well as many vendor-based cloud specialized certifications from Google, Microsoft Azure, and Amazon Web Services. Rob is considered a leading expert in prepping others to achieve certification success.

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 services. 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* (Sybex, 2021), 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

Rishalin Pillay is a seasoned cybersecurity expert with extensive experience in offensive security, cloud security, threat, and incident response, and is recognized as a trusted authority in the field. As an accomplished Pluralsight author, he has created in-depth courses like Red Team Tools and Threat Protection, and has authored or coauthored influential books such as *Learn Penetration Testing* (Packt Publishing, 2019), *Ethical Hacking Workshop* (Packt Publishing, 2023), and *Offensive Shellcode from Scratch* (Packt Publishing, 2022). Additionally, Rishalin has contributed to numerous publications on topics including dark web analysis, Kali Linux, security operations, and essential study guides for networking and Microsoft technologies. His dedication to advancing the field has earned him prestigious accolades, including the Microsoft Content Publisher Gold and Platinum awards and the Event Speaker Gold award, reflecting his impactful presence as a writer, educator, and Tier-1 business event speaker. Whether through writing, teaching, or presenting, Rishalin continues to make a lasting impact on the cybersecurity industry.

Contents at a Glance

Introduction		*xxix*
Assessment Test		*xl*
Chapter 1	Penetration Testing	1
Chapter 2	Planning and Scoping Penetration Tests	21
Chapter 3	Information Gathering	57
Chapter 4	Vulnerability Scanning	113
Chapter 5	Analyzing Vulnerability Scans	151
Chapter 6	Exploit and Pivot	193
Chapter 7	Exploiting Network Vulnerabilities	253
Chapter 8	Exploiting Physical and Social Vulnerabilities	299
Chapter 9	Exploiting Application Vulnerabilities	329
Chapter 10	Exploiting Host Vulnerabilities	379
Chapter 11	Reporting and Communication	443
Chapter 12	Scripting for Penetration Testing	471
Appendix A	Answers to Review Questions	515
Appendix B	Solution to Lab Exercise	539
Index		*541*

Contents

Introduction *xxix*

Assessment Test *xl*

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? 9
Internal Penetration Testing Teams 9
External Penetration Testing Teams 10
Selecting Penetration Testing Teams 10
The CompTIA Penetration Testing Process 11
Engagement Management 12
Reconnaissance and Enumeration 12
Vulnerability Discovery and Analysis 13
Attacks and Exploits 13
Post-exploitation and Lateral Movement 14
The Cyber Kill Chain 14
Reconnaissance 15
Weaponization 16
Delivery 16
Exploitation 16
Installation 16
Command and Control 17
Actions on Objectives 17
Tools of the Trade 17
Summary 18
Exam Essentials 18
Lab Exercises 19
Activity 1.1: Adopting the Hacker Mindset 19
Activity 1.2: Using the Cyber Kill Chain 19

Chapter 2 Planning and Scoping Penetration Tests 21

Summarizing Pre-engagement Activities 25
Scope Definition 26
Scoping Considerations—A Deeper Dive 27

Support Resources for Penetration Tests 29
Defining Assessment Types 32
Known Environments and Unknown Environments 33
The Rules of Engagement 34
Rules of Engagement Considerations 36
Basic Considerations 36
Agreement Types 37
Target Selection 37
Assessment Types 38
Shared Responsibility Model 39
Hosting Provider Responsibilities 39
Customer Responsibilities 40
Penetration Tester Responsibilities 41
Third-Party Responsibilities 41
Key Legal Concepts for Penetration Tests 41
Authorization Letters 42
Mandatory Reporting Requirements 42
Risk to the Penetration Tester 42
Contracts 43
Data Ownership and Retention 44
Environmental Differences and Location Restrictions 44
Regulatory Compliance Considerations 45
Penetration Testing Standards and Methodologies 47
Testing Standards 47
Threat Modeling Frameworks 49
Summary 50
Exam Essentials 50
Lab Exercises 52
Review Questions 53

Chapter 3 Information Gathering 57

Reconnaissance and Enumeration 60
Active and Passive Reconnaissance 61
Active Reconnaissance and Enumeration 80
CVE and CWE 80
What Is Enumeration? 81
Operating System (OS) Fingerprinting 81
Perform Vulnerability Scanning 95
Summary 105
Exam Essentials 106
Lab Exercises 107
Activity 3.1: Gathering OSINT Manually 107
Activity 3.2: Exploring Shodan 107
Activity 3.3: Running an Nmap Scan 107
Review Questions 109

Chapter 4 Vulnerability Scanning 113

Identifying Vulnerability Management Requirements 115
Regulatory Environment 115
Corporate Policy 119
Support for Penetration Testing 119
Identifying Scan Targets 119
Determining Scan Frequency 121
Active vs. Passive Scanning 123
Configuring and Executing Vulnerability Scans 123
Scoping Vulnerability Scans 124
Configuring Vulnerability Scans 125
Scanner Maintenance 132
Software Security Testing 134
Analyzing and Testing Code 135
Web Application Vulnerability Scanning 136
Developing a Remediation Workflow 138
Prioritizing Remediation 140
Testing and Implementing Fixes 141
Overcoming Barriers to Vulnerability Scanning 141
Summary 142
Exam Essentials 143
Lab Exercises 144
Activity 4.1: Installing a Vulnerability Scanner 144
Activity 4.2: Running a Vulnerability Scan 144
Activity 4.3: Developing a Penetration Test Vulnerability Scanning Plan 144
Review Questions 146

Chapter 5 Analyzing Vulnerability Scans 151

Reviewing and Interpreting Scan Reports 152
Understanding CVSS 156
Validating Scan Results 162
Vulnerability Scanning Errors 162
Scan Completeness 163
Troubleshooting Scan Configurations 163
Documented Exceptions 164
Understanding Informational Results 164
Reconciling Scan Results with Other Data Sources 165
Public Exploit Selection 166
Trend Analysis 166
Common Vulnerabilities 167
Server and Endpoint Vulnerabilities 168

Network Vulnerabilities 174
Virtualization Vulnerabilities 180
Internet of Things (IoT) 182
Web Application Vulnerabilities 183
Summary 185
Exam Essentials 186
Lab Exercises 187
Activity 5.1: Interpreting a Vulnerability Scan 187
Activity 5.2: Analyzing a CVSS Vector 187
Activity 5.3: Developing a Penetration Testing Plan 187
Review Questions 188

Chapter 6 Exploit and Pivot 193

Exploits and Attacks 198
Choosing Targets 198
Pivoting and Lateral Movement 199
Lateral Movement 199
Pivoting 199
Relay Creation 201
Enumeration 202
Identifying the Right Exploit 205
Exploit Resources 207
Exploitation Toolkits and Tools 209
Metasploit 209
PowerSploit 216
BloodHound 217
Other Methods of Access 217
Daemons and Services 217
Command and Control (C2) Frameworks 218
Rootkit 218
LOLBins 218
Command-Line Tools 218
Exploit Specifics 223
RPC/DCOM 223
PsExec 223
PS Remoting/WinRM 223
WMI 224
Fileless Malware and Living Off the Land 224
Scheduled Tasks and cron Jobs 225
SMB 226
DNS 229
LDAP 229
File Transfer Protocol (FTP) 229
Telnet 229

HTTP/HTTPS 230
Line Printer Daemon (LPD) 230
JetDirect 230
RDP 230
Apple Remote Desktop 231
VNC 231
SSH 231
Network Segmentation Testing and Exploits 232
Leaked Keys 232
Leveraging Exploits 233
Common Post-Exploit Attacks 233
Cross-Compiling 236
Privilege Escalation 236
Social Engineering 237
Escaping and Upgrading Limited Shells 238
Persistence and Evasion 239
Scheduled Jobs and Scheduled Tasks 239
Inetd Modification 239
Daemons and Services 239
Backdoors and Trojans 240
Data Exfiltration and Covert Channels 240
New Users 241
Covering Your Tracks 242
Summary 243
Exam Essentials 244
Lab Exercises 245
Activity 6.1: Exploit 245
Activity 6.2: Discovery 246
Activity 6.3: Pivot 246
Review Questions 248

Chapter 7 Exploiting Network Vulnerabilities 253

Identifying Exploits 256
Conducting Network Exploits 256
Default Credentials 256
Certificate Services 257
VLAN Hopping 257
DNS Cache Poisoning 259
On-Path Attacks 260
NAC Bypass 264
Segmentation Bypass 265
DoS Attacks and Stress Testing 266
Misconfigured Services 267
Share Enumeration 268

Exploit Chaining 268
Exploiting Windows Services 269
NetBIOS Name Resolution Exploits 269
SMB Exploits 273
Identifying and Exploiting Common Services 273
Identifying and Attacking Service Targets 274
SNMP Exploits 274
SMTP Exploits 276
FTP Exploits 276
Kerberoasting 277
Samba Exploits 279
Password Attacks 280
Stress Testing for Availability 280
Wireless Exploits 281
Attack Methods 281
Finding Targets 282
Attacking Captive Portals 284
Eavesdropping, Evil Twins, and Wireless On-Path Attacks 284
Other Wireless Protocols and Systems 288
RFID Cloning 289
Signal Jamming 290
Repeating 291
Summary 291
Exam Essentials 292
Lab Exercises 292
Activity 7.1: Capturing Hashes 292
Activity 7.2: Brute-Forcing Services 293
Activity 7.3: Wireless Testing 294
Review Questions 295

Chapter 8 Exploiting Physical and Social Vulnerabilities 299

Exploiting Physical Vulnerabilities 302
Physical Facility Penetration Testing 302
Site Surveys 303
Entering Facilities 303
Information Gathering 307
Exploiting Social Vulnerabilities 308
Social Engineering 308
In-Person Social Engineering 309
Phishing Attacks 312
Website-Based Attacks 312
Using Social Engineering Tools 314
Summary 319

Exam Essentials 320
Lab Exercises 321
Activity 8.1: Designing a Physical Penetration Test 321
Activity 8.2: Brute-Forcing Services 322
Activity 8.3: Using BeEF 322
Review Questions 324

Chapter 9 Exploiting Application Vulnerabilities 329

Exploiting Injection Vulnerabilities 332
Input Validation 332
Web Application Firewalls 333
SQL Injection Attacks 334
Code Injection Attacks 337
Command Injection Attacks 337
LDAP Injection Attacks 338
Server-Side Template Injection 339
Deserialization Attacks 339
Exploiting Authentication Vulnerabilities 339
Password Authentication 340
Session Hijacking Attacks 341
JWT Manipulation 346
Kerberos Exploits 346
Exploiting Authorization Vulnerabilities 347
Insecure Direct Object References 347
Directory Traversal 348
File Inclusion 350
Privilege Escalation 352
Exploiting Web Application Vulnerabilities 352
Cross-Site Scripting (XSS) 352
Request Forgery 355
Clickjacking 356
Unsecure Coding Practices 356
Source Code Comments 356
Error Handling 357
Hard-Coded Credentials 357
Race Conditions 358
API Abuse 358
Unsigned Code 359
Application Testing Tools 361
Static Application Security Testing (SAST) 361
Software Composition Analysis 362
Dynamic Application Security Testing (DAST) 362
Interactive Application Security Testing (IAST) 367

Database Scanning 368
Secrets Scanning 369
Summary 369
Exam Essentials 369
Lab Exercises 371
Activity 9.1: Application Security Testing Techniques 371
Activity 9.2: Using the ZAP Proxy 371
Activity 9.3: Creating a Cross-Site Scripting Vulnerability 371
Review Questions 373

Chapter 10 Exploiting Host Vulnerabilities 379

Attacking Hosts 385
Linux 386
Windows 391
Cross-Platform Exploits 393
Credential Attacks and Testing Tools 397
Authentication Attacks 397
Credential Acquisition 400
Offline Password Cracking 401
Credential Testing and Brute-Forcing Tools 403
Wordlists and Dictionaries 404
Remote Access 404
SSH 404
Netcat and Ncat 405
Metasploit and Remote Access 405
PowerShell and WinRM 406
Proxies and Proxychains 407
Attacking Virtual Machines and Containers 407
Container Scans 408
Virtual Machine Attacks 409
Containerization Attacks 411
Attacking Cloud Technologies 412
Attacking Cloud Accounts 414
Attacking and Using Misconfigured Cloud Assets 415
Other Cloud Attacks 416
Tools for Cloud Technology Attacks 417
Attacking Mobile Devices 419
Attacking Artificial Intelligence (AI) 424
Prompt Injection 425
Model Manipulation 425
Attacking IoT, ICS, Embedded Systems, and SCADA Devices 426
CAN Bus Attack 427
OT, Embedded, and IoT Systems 427
Attacking Data Storage 430

Summary 431
Exam Essentials 433
Lab Exercises 434
Activity 10.1: Dumping and Cracking the Windows SAM and Other Credentials 434
Activity 10.2: Cracking Passwords Using Hashcat 435
Activity 10.3: Setting Up a Reverse Shell and a Bind Shell 436
Review Questions 438

Chapter 11 Reporting and Communication 443

The Importance of Collaboration and Communication 447
Defining an Escalation Path 447
Communication Triggers 448
Goal Reprioritization 449
Recommending Mitigation Strategies 449
Finding: Shared Local Administrator Credentials 450
Finding: Weak Password Complexity 451
Finding: Plain-Text Passwords 452
Finding: No Multifactor Authentication 452
Finding: SQL Injection 454
Finding: Unnecessary Open Services 454
Writing a Penetration Testing Report 454
Structuring the Written Report 455
Reporting Considerations 460
Secure Handling and Distribution of Reports 462
Wrapping Up the Engagement 462
Post-Engagement Cleanup 462
Client Acceptance 463
Lessons Learned 463
Follow-Up Actions/Retesting 464
Attestation of Findings 464
Retention and Destruction of Data 464
Summary 464
Exam Essentials 465
Lab Exercises 466
Activity 11.1: Remediation Strategies 466
Activity 11.2: Report Writing 466
Review Questions 467

Chapter 12 Scripting for Penetration Testing 471

Scripting and Penetration Testing 473
Bash 474
PowerShell 475
Python 476

Variables, Arrays, and Substitutions 477
Bash 478
PowerShell 479
Python 479
Comparison Operations 480
String Operations 480
Bash 482
PowerShell 483
Ruby 484
Python 485
Flow Control 486
Conditional Execution 487
for Loops 490
while Loops 494
Input and Output (I/O) 499
Redirecting Standard Input and Output 500
Comma-Separated Values (CSV) 500
Error Handling 501
Bash 501
PowerShell 501
Python 502
Reusing Code 502
The Role of Coding in Penetration Testing 503
Information Gathering 503
Data Manipulation 503
Analyzing Exploit Code 504
Automating Penetration Tests 504
Summary 506
Exam Essentials 507
Lab Exercises 508
Activity 12.1: Reverse DNS Lookups 508
Activity 12.2: Nmap Scan 508
Review Questions 509

Appendix A Answers to Review Questions 515

Chapter 2: Planning and Scoping Penetration Tests 516
Chapter 3: Information Gathering 518
Chapter 4: Vulnerability Scanning 520
Chapter 5: Analyzing Vulnerability Scans 522
Chapter 6: Exploit and Pivot 524
Chapter 7: Exploiting Network Vulnerabilities 526
Chapter 8: Exploiting Physical and Social Vulnerabilities 528

Chapter 9: Exploiting Application Vulnerabilities 530
Chapter 10: Exploiting Host Vulnerabilities 532
Chapter 11: Reporting and Communication 535
Chapter 12: Scripting for Penetration Testing 536

Appendix B Solution to Lab Exercise 539

Index *541*