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

Table of Contents

List of Tables

Chapter 6

List of Illustrations

Chapter 1

Chapter 2

Chapter 3

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.)

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 Author

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.

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

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+