

Second Edition

**Save 10%**  
on Exam Vouchers  
Coupon Inside!

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

[Cover](#)

[Title Page](#)

[Copyright](#)

[Dedication](#)

[Acknowledgments](#)

[About the Author](#)

[About the Technical Editor](#)

[Introduction](#)

[CompTIA](#)

[The PenTest+ Exam](#)

[What Does This Book Cover?](#)

[CompTIA PenTest+ Certification Exam Objectives](#)

[Assessment Test](#)

[Answers to Assessment Test](#)

[Chapter 1: Penetration Testing](#)

[What Is Penetration Testing?](#)

[Reasons for Penetration Testing](#)

[Who Performs Penetration Tests?](#)

[The CompTIA Penetration Testing Process](#)

[The Cyber Kill Chain](#)

[Tools of the Trade](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 2: Planning and Scoping Penetration Tests](#)

[Scoping and Planning Engagements](#)

[Penetration Testing Standards and Methodologies](#)

[Key Legal Concepts for Penetration Tests](#)

[Regulatory Compliance Considerations](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 3: Information Gathering](#)

[Footprinting and Enumeration](#)

[Active Reconnaissance and Enumeration](#)

[Information Gathering and Defenses](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 4: Vulnerability Scanning](#)

[Identifying Vulnerability Management Requirements](#)

[Configuring and Executing Vulnerability Scans](#)

[Software Security Testing](#)

[Developing a Remediation Workflow](#)

[Overcoming Barriers to Vulnerability Scanning](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 5: Analyzing Vulnerability Scans](#)

[Reviewing and Interpreting Scan Reports](#)

[Validating Scan Results](#)

[Common Vulnerabilities](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 6: Exploiting and Pivoting](#)

[Exploits and Attacks](#)

[Exploitation Toolkits](#)

[Exploit Specifics](#)

[Leveraging Exploits](#)

[Persistence and Evasion](#)

[Pivoting](#)

[Covering Your Tracks](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 7: Exploiting Network Vulnerabilities](#)

[Identifying Exploits](#)

[Conducting Network Exploits](#)

[Exploiting Windows Services](#)

[Identifying and Exploiting Common Services](#)

[Wireless Exploits](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 8: Exploiting Physical and Social Vulnerabilities](#)

[Physical Facility Penetration Testing](#)

[Social Engineering](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 9: Exploiting Application Vulnerabilities](#)

[Exploiting Injection Vulnerabilities](#)

[Exploiting Authentication Vulnerabilities](#)

[Exploiting Authorization Vulnerabilities](#)

[Exploiting Web Application Vulnerabilities](#)

[Unsecure Coding Practices](#)

[Steganography](#)

[Application Testing Tools](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 10: Attacking Hosts, Cloud Technologies, and Specialized Systems](#)

[Attacking Hosts](#)

[Credential Attacks and Testing Tools](#)

[Remote Access](#)

[Attacking Virtual Machines and Containers](#)

[Attacking Cloud Technologies](#)

[Attacking Mobile Devices](#)

[Attacking IoT, ICS, Embedded Systems, and SCADA Devices](#)

[Attacking Data Storage](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 11: Reporting and Communication](#)

[The Importance of Communication](#)

[Recommending Mitigation Strategies](#)

[Writing a Penetration Testing Report](#)

[Wrapping Up the Engagement](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

## [Chapter 12: Scripting for Penetration Testing](#)

[Scripting and Penetration Testing](#)

[Variables, Arrays, and Substitutions](#)

[Comparison Operations](#)

[String Operations](#)

[Flow Control](#)

[Input and Output \(I/O\)](#)

[Error Handling](#)

[Advanced Data Structures](#)

[Reusing Code](#)

[The Role of Coding in Penetration Testing](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Appendix A: Answers to Review Questions](#)

[Appendix B: Solution to Lab Exercise](#)

[Solution to Activity 5.2: Analyzing a CVSS Vector](#)

[Index](#)

[End User License Agreement](#)

## List of Tables

### Chapter 1

[Table 1.1 Penetration testing tools covered by the PenTest+ exam](#)

### Chapter 3

[TABLE 3.1 Common ports and services](#)

### Chapter 5

[TABLE 5.1 CVSS attack vector metric](#)

[TABLE 5.2 CVSS attack complexity metric](#)

[TABLE 5.3 CVSS privileges required metric](#)

[TABLE 5.4 CVSS user interaction metric](#)

[TABLE 5.5 CVSS confidentiality metric](#)

[TABLE 5.6 CVSS integrity metric](#)

[TABLE 5.7 CVSS availability metric](#)

[TABLE 5.8 CVSS scope metric](#)

[TABLE 5.9 CVSS Qualitative Severity Rating Scale](#)

## Chapter 6

[TABLE 6.1 Metasploit exploit quality ratings](#)

[TABLE 6.2 Metasploit search terms](#)

# List of Illustrations

## Chapter 1

[FIGURE 1.1 The CIA triad](#)

[FIGURE 1.2 The DAD triad](#)

[FIGURE 1.3 CompTIA penetration testing stages](#)

[FIGURE 1.4 The Cyber Kill Chain model](#)

[FIGURE 1.5 Cyber Kill Chain in the context of the CompTIA model](#)

## Chapter 2

[FIGURE 2.1 A logical dataflow diagram](#)

## Chapter 3

[FIGURE 3.1 ExifTool metadata with location](#)

[FIGURE 3.2 FOCA metadata acquisition](#)

[FIGURE 3.3 WHOIS query data for google.com](#)

[FIGURE 3.4 Host command response for google.com](#)

[FIGURE 3.5 nslookup for netflix.com](#)

[FIGURE 3.6 WHOIS of 52.41.111.100](#)

[FIGURE 3.7 tracert of netflix.com](#)

[FIGURE 3.8 Shodan result from an exposed Cisco device](#)

[FIGURE 3.9 Censys IOS host view](#)



[FIGURE 3.10 A Google search for passwords.xls](#)  
[FIGURE 3.11 Nmap scan using OS identification](#)  
[FIGURE 3.12 Nmap output of a Windows 10 system](#)  
[FIGURE 3.13 Zenmap topology view](#)  
[FIGURE 3.14 Scapy packet crafting for a TCP ping](#)  
[FIGURE 3.15 ARP query and response](#)  
[FIGURE 3.16 Harvesting emails using Metasploit](#)  
[FIGURE 3.17 Netcat banner grabbing](#)  
[FIGURE 3.18 Excerpt of strings run on the Netcat binary](#)

## Chapter 4

[FIGURE 4.1 FIPS 199 Standards](#)  
[FIGURE 4.2 Qualys asset map](#)  
[FIGURE 4.3 Configuring a Nessus scan](#)  
[FIGURE 4.4 Sample Nessus scan report](#)  
[FIGURE 4.5 Nessus scan templates](#)  
[FIGURE 4.6 Disabling unused plug-ins](#)  
[FIGURE 4.7 Configuring authenticated scanning](#)  
[FIGURE 4.8 Choosing a scan appliance](#)  
[FIGURE 4.9 National Cyber Awareness System Vulnerability Summary](#)  
[FIGURE 4.10 Setting automatic updates in Nessus](#)  
[FIGURE 4.11 Acunetix web application scan vulnerability report](#)  
[FIGURE 4.12 Nikto web application scan results](#)  
[FIGURE 4.13 Running a Wapiti scan](#)

[FIGURE 4.14 WPScan WordPress vulnerability scanner](#)

[FIGURE 4.15 Nessus web application scanner](#)

[FIGURE 4.16 Tamper Data session showing login data](#)

[FIGURE 4.17 Scanning a database-backed application with SQLmap](#)

[FIGURE 4.18 Vulnerability management life cycle](#)

[FIGURE 4.19 Qualys scan performance settings](#)

## Chapter 5

[FIGURE 5.1 Nessus vulnerability scan report](#)

[FIGURE 5.2 Qualys vulnerability scan report](#)

[FIGURE 5.3 OpenVAS vulnerability scan report](#)

[FIGURE 5.4 Scan report showing vulnerabilities and best practices](#)

[FIGURE 5.5 Vulnerability trend analysis](#)

[FIGURE 5.6 Vulnerabilities exploited in 2015 by year of initial discovery...](#)

[FIGURE 5.7 Missing patch vulnerability](#)

[FIGURE 5.8 Unsupported operating system vulnerability](#)

[FIGURE 5.9 Dirty COW website](#)

[FIGURE 5.10 Code execution vulnerability](#)

[FIGURE 5.11 Spectre and Meltdown dashboard from QualysGuard](#)

[FIGURE 5.12 FTP cleartext authentication vulnerability](#)

[FIGURE 5.13 Debug mode vulnerability](#)

[FIGURE 5.14 Outdated SSL version vulnerability](#)

[FIGURE 5.15 Insecure SSL cipher vulnerability](#)

[FIGURE 5.16 Invalid certificate warning](#)

[FIGURE 5.17 DNS amplification vulnerability](#)

[FIGURE 5.18 Internal IP disclosure vulnerability](#)

[FIGURE 5.19 Inside a virtual host](#)

[FIGURE 5.20 SQL injection vulnerability](#)

[FIGURE 5.21 Cross-site scripting vulnerability](#)

[FIGURE 5.22 First vulnerability report](#)

[FIGURE 5.23 Second vulnerability report](#)

## Chapter 6

[FIGURE 6.1 OpenVAS/Greenbone vulnerability report](#)

[FIGURE 6.2 Distributed Ruby vulnerability](#)

[FIGURE 6.3 phpinfo\(\) output accessible](#)

[FIGURE 6.4 phpinfo.php output](#)

[FIGURE 6.5 The Metasploit console](#)

[FIGURE 6.6 Running show exploits in Metasploit](#)

[FIGURE 6.7 Selecting an exploit](#)

[FIGURE 6.8 Setting module options](#)

[FIGURE 6.9 Successful exploit](#)

[FIGURE 6.10 WMIImplant WMI tools](#)

[FIGURE 6.11 CrackMapExec's main screen](#)

[FIGURE 6.12 Responder capture flow](#)

[FIGURE 6.13 Pass-the-hash flow](#)

[FIGURE 6.14 John the Ripper](#)

[FIGURE 6.15 Pivoting](#)

## Chapter 7

[FIGURE 7.1 Double-tagged Ethernet packet](#)

[FIGURE 7.2 Yersinia 802.1q attack selection](#)

[FIGURE 7.3 DNS cache poisoning attack](#)

[FIGURE 7.4 ARP spoofing](#)

[FIGURE 7.5 Manually configuring a MAC address in Windows 10](#)

[FIGURE 7.6 Metasploit SYN flood](#)

[FIGURE 7.7 NetBIOS name service attack](#)

[FIGURE 7.8 Responder sending poisoned answers](#)

[FIGURE 7.9 Responder capturing hashes](#)

[FIGURE 7.10 Output from snmpwalk](#)

[FIGURE 7.11 THC Hydra SSH brute-force attack](#)

[FIGURE 7.12 WiGLE map showing access point density in a metropolitan area](#)

[FIGURE 7.13 RFID cloner and tags](#)

## Chapter 8

[FIGURE 8.1 A typical security vestibule design](#)

[FIGURE 8.2 SET menu](#)

[FIGURE 8.3 SET loading the Metasploit reverse TCP handler](#)

[FIGURE 8.4 BeEF hooked browser detail](#)

[FIGURE 8.5 BeEF commands usable in a hooked browser](#)

## Chapter 9

[FIGURE 9.1 Web application firewall](#)

[FIGURE 9.2 Account number input page](#)

[FIGURE 9.3 Account information page](#)

[FIGURE 9.4 Account information pageafter blind SQL injection](#)

[FIGURE 9.5 Account creation page](#)

[FIGURE 9.6 Zyxel router default password](#)

[FIGURE 9.7 Session authentication with cookies](#)

[FIGURE 9.8 Session cookie from CNN.com](#)

[FIGURE 9.9 Session hijacking with cookies](#)

[FIGURE 9.10 Kerberos authentication process](#)

[FIGURE 9.11 Example web server directory structure](#)

[FIGURE 9.12 Directory scanning with DirBuster](#)

[FIGURE 9.13 Message board post rendered in a browser](#)

[FIGURE 9.14 XSS attack rendered in a browser](#)

[FIGURE 9.15 SQL error disclosure](#)

[FIGURE 9.16 \(a\) Unaltered photograph \(b\). Photograph with hidden message embe...](#)

[FIGURE 9.17 Zed Attack Proxy \(ZAP\).](#)

[FIGURE 9.18 Burp Proxy.](#)

[FIGURE 9.19 The american fuzzy lop performing fuzz testing](#)

[FIGURE 9.20 Gobuster DNS enumeration](#)

## Chapter 10

[FIGURE 10.1 SUID files in Kali](#)

[FIGURE 10.2 SUID files with details](#)

[FIGURE 10.3 Abusing\\_sudo\\_rights](#)

[FIGURE 10.4 Checking Linux kernel version information](#)

[FIGURE 10.5 Dumping the Windows SAM with Mimikatz](#)

[FIGURE 10.6 Hashcat cracking Linux passwords](#)

[FIGURE 10.7 Metasploit reverse TCP shell](#)

[FIGURE 10.8 Detecting virtualization on a Windows system](#)

[FIGURE 10.9 Detecting virtualization on Kali Linux](#)

[FIGURE 10.10 Side-channel attack against a virtual machine](#)

[FIGURE 10.11 A simple SCADA environment design example](#)

## Chapter 11

[FIGURE 11.1 Smartphone-based multifactor authentication](#)

## Chapter 12

[FIGURE 12.1 Executing Hello, World! using JavaScript in the Chrome browser](#)

[FIGURE 12.2 Executing the cupcake calculator using JavaScript in the Chrome ...](#)

[FIGURE 12.3 URL encoding using JavaScript in the Chrome browser](#)

[FIGURE 12.4 Identifying the language of a conditional execution statement](#)

[FIGURE 12.5 Identifying the language of a for loop](#)

[FIGURE 12.6 Identifying the language of a while loop](#)

[FIGURE 12.7 Storing DNS information in a tree data structure](#)

**Take the Next Step  
in Your IT Career**

**Save  
10%  
on Exam Vouchers\***

**(up to a \$35 value)**

\*Some restrictions apply. See web page for details.

**CompTIA®**

**Get details at  
[www.wiley.com/go/sybextestprep](http://www.wiley.com/go/sybextestprep)**

To get the discount code, you'll need to register and log on the test bank. Then go to Resources.







# **CompTIA® PenTest+® Study Guide**

**Exam PT0-002**

**Second Edition**



**Mike Chapple  
David Seidl**



Copyright © 2022 by John Wiley & Sons, Inc. All rights reserved.

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.)

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at [www.copyright.com](http://www.copyright.com). Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

**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](http://www.wiley.com).

**Library of Congress Control Number: 2021944464**

**Trademarks:** WILEY, the Wiley logo, Sybex, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. CompTIA and PenTest+ are trademarks or registered trademarks of The Computing Technology Industry Association, Inc. DBA CompTIA, Inc. All other trademarks are the property of their respective owners.

John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

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](http://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)<sup>2</sup> Official Practice Tests* (Sybex, 2018) as well as *CISSP Official (ISC)<sup>2</sup> 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<sup>2</sup> 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:

<b>Beginner/Novice</b>	<b>Intermediate</b>	<b>Advanced</b>
------------------------	---------------------	-----------------

<b>Beginner/Novice</b>	<b>Intermediate</b>	<b>Advanced</b>
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+