

No. 151

CERTIFICATION GUIDE

CompTIA PenTest+ Study Guide

A plain-language guide to the PT0-003 exam

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 151

CompTIA PenTest+ Study Guide

A plain-language guide to the PT0-003 exam

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

CompTIA PenTest+ Study Guide
A plain-language guide to the PT0-003 exam

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. CompTIA and PenTest+ are trademarks of CompTIA, Inc. This guide is independent and is not affiliated with, sponsored by or endorsed by CompTIA. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this guide 1

PART I · THE CERTIFICATION

1 What PenTest+ is 4
2 Exam format 5
3 The domains 6
4 Law and ethics 7
5 Renewal 8
6 Building a lab 9
7 A study plan 10

PART II · ENGAGEMENT AND RECONNAISSANCE

8 Domain 1: the engagement 12
9 Pre-engagement documents 13
10 Scope and constraints 14
11 Frameworks 15
12 Communication 16
13 Domain 2: reconnaissance 17
14 Open-source intelligence 18
15 Enumeration concepts 19
16 Scripting 20
17 Domain 3: vulnerability discovery 21
18 Analysing results 22
19 Physical and social testing 23

PART III · ATTACKS AND POST-EXPLOITATION

20 Domain 4: attack concepts 25
21 Network attack concepts 26
22 Authentication attack concepts 27
23 Web and API attack concepts 28

FREE SAMPLE · ojayo.com

24 Cloud attack concepts 29
25 Wireless and mobile concepts 30
26 Testing AI systems 31
27 Domain 5: post-exploitation 32
28 Lateral movement concepts 33
29 Detection and evasion 34
30 Clean-up 35

PART IV · REPORTING AND EXAM SUCCESS

31 Reporting 36
32 Remediation recommendations 39
33 Practice questions 40
34 Answers 42
35 Performance-based questions 43
36 Exam day 44
37 Common mistakes 45
38 Careers 46
39 Next steps 47
Checklists 48
Glossary 49
Further reading 50

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this guide

What this guide covers, who it is for, and how to use it.

CompTIA PenTest+ is an intermediate certification for professionals who plan, perform and report authorized penetration tests. It covers the whole engagement, from scoping and rules of engagement to reporting and remediation advice.

This guide explains PenTest+ in plain language for the **PT0-003** exam, launched in December 2024. It covers the exam facts, each domain with diagrams, a study plan, original practice questions and exam-day advice. It explains attack techniques at the conceptual level needed for the exam and for defence; it does not provide step-by-step attack instructions.

What this guide is, and is not

- An independent study companion written in its own words.
- **Not** official CompTIA material; it does not reproduce exam questions or objectives.
- Use CompTIA's official exam objectives as your checklist, and practise only in legal labs.

Who this guide is for

- **Junior penetration testers** and vulnerability assessors.
- **Security analysts** wanting an offensive perspective.
- **Security+ holders** moving into testing.

FREE SAMPLE · ojayo.com

How the guide is organized

- **Part I — The certification** (Chapters 1–7): what PenTest+ is, format, domains, ethics and law, renewal, labs and a study plan.
- **Part II — Engagement and reconnaissance** (Chapters 8–19): Domains 1, 2 and 3.
- **Part III — Attacks and post-exploitation** (Chapters 20–30): Domains 4 and 5, at a conceptual level.
- **Part IV — Reporting and exam success** (Chapters 31–39): reporting, practice questions and next steps.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical study and exam advice.

IN PRACTICE
How a concept looks in a real engagement.

WATCH OUT
Common traps and legal risks.

KEY IDEA
The one thing to remember from a section.

A note on the law

Testing systems without written permission is illegal. Screens are **illustrations**, not real CompTIA exam screens.

FREE SAMPLE · ojayo.com

PART I

The certification

These chapters explain what PenTest+ is and how to prepare safely and legally.

FREE SAMPLE · ojayo.com

CHAPTER 1

What PenTest+ is

The penetration testing certification.

A definition

PenTest+ validates the skills to plan and scope an engagement, discover and analyse vulnerabilities, demonstrate exploitation safely, and report and communicate results.

Engagement focus

Unlike purely technical exams, PenTest+ gives real weight to scoping, legal issues, communication and reporting.

KEY IDEA

A penetration test is a professional service with clear permission, limits and a useful report.

FREE SAMPLE · ojayo.com

CHAPTER 2

Exam format

The exam.

- **Questions**: maximum of 90, multiple choice and performance-based.
- **Time**: 165 minutes.
- **Passing score**: 750 on a scale of 100 to 900.
- **Recommended experience**: three to four years in a penetration tester role, plus Network+ and Security+ level knowledge.

FREE SAMPLE · ojayo.com

CHAPTER 3

The domains

Five domains.

Domain	Weight
1 Engagement Management	13%
2 Reconnaissance and Enumeration	21%
3 Vulnerability Discovery and Analysis	17%
4 Attacks and Exploits	35%
5 Post-exploitation and Lateral Movement	14%

Figure 3.1 PenTest+ PT0-003 domains

What changed from PT0-002

PT0-003 reorganized the domains around the engagement lifecycle and added content on cloud, APIs, AI systems and modern attack paths.

FREE SAMPLE · ojayo.com

CHAPTER 4

Law and ethics

Law and ethics.

Always have written authorization from someone with authority, stay in scope, protect client data, report honestly and follow laws such as the US Computer Fraud and Abuse Act and the UK Computer Misuse Act. See **Ethical Hacking for Beginners**.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide (you are readin…
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

CompTIA PenTest+ Study Guide

Enjoyed it? The full book has 55 pages and 39 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.