

PEARSON IT  
CERTIFICATION

Save 10%  
on Exam  
Voucher

See Inside



Practice  
Tests



Flash  
Cards



Review  
Exercises



Study  
Planner

# Cert Guide

Advance your IT career with hands-on learning

## CompTIA® **PenTest+**

### PT0-002



OMAR SANTOS

# Special Offer

## **Save 80% on Premium Edition eBook and Practice Test**

The *CompTIA PenTest+ PT0-002 Cert Guide Premium Edition and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

**See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.**

# CompTIA PenTest+ PT0-002 Cert Guide

## Table of Contents

- Cover
- Title Page
- Copyright Page
- Contents at a Glance
- Contents
- About the Author
- Dedication
- Acknowledgments
- About the Technical Reviewer
- We Want to Hear from You
- Introduction
- Chapter 1 Introduction to Ethical Hacking and Penetration Testing
  - Do I Know This Already? Quiz
  - Foundation Topics
  - Understanding Ethical Hacking and Penetration Testing
    - Why Do We Need to Do Penetration Testing?
    - Threat Actors
  - Exploring Penetration Testing Methodologies
    - Why Do We Need to Follow a Methodology for Penetration Testing?
    - Environmental Considerations
    - Surveying Different Standards and Methodologies
  - Building Your Own Lab

# **Table of Contents**

Requirements and Guidelines for Penetration Testing Labs

What Tools Should You Use in Your Lab?

What if You Break Something?

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

## **Chapter 2 Planning and Scoping a Penetration Testing**

### **Assessment**

Do I Know This Already? Quiz

Foundation Topics

Comparing and Contrasting Governance, Risk, and Compliance Concepts

Regulatory Compliance Considerations

Regulations in the Financial Sector

Regulations in the Healthcare Sector

Payment Card Industry Data Security Standard (PCI DSS)

Key Technical Elements in Regulations You Should Consider

Local Restrictions

Legal Concepts

Contracts

Disclaimers

Explaining the Importance of Scoping and Organizational or Customer  
Requirements

Rules of Engagement

Target List and In-Scope Assets

Validating the Scope of Engagement

Strategy: Unknown vs. Known Environment Testing

Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and

# **Table of Contents**

Integrity

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

## **Chapter 3 Information Gathering and Vulnerability Scanning**

Do I Know This Already? Quiz

Foundation Topics

Performing Passive Reconnaissance

Active Reconnaissance vs. Passive Reconnaissance

DNS Lookups

Identification of Technical and Administrative Contacts

Cloud vs. Self-Hosted Applications and Related Subdomains

Social Media Scraping

Cryptographic Flaws

Company Reputation and Security Posture

Password Dumps

File Metadata

Strategic Search Engine Analysis/Enumeration

Website Archiving/Caching

Public Source Code Repositories

Open-Source Intelligence (OSINT) Gathering

Reconnaissance with Recon-ng

Shodan

Performing Active Reconnaissance

Nmap Scan Types

TCP Connect Scan (-sT)

UDP Scan (-sU)

TCP FIN Scan (-sF)

# **Table of Contents**

Host Discovery Scan (-sn)

Timing Options (-T 0-5)

Types of Enumeration

Host Enumeration

User Enumeration

Group Enumeration

Network Share Enumeration

Additional SMB Enumeration Examples

Web Page Enumeration/Web Application Enumeration

Service Enumeration

Exploring Enumeration via Packet Crafting

Packet Inspection and Eavesdropping

## **Understanding the Art of Performing Vulnerability Scans**

How a Typical Automated Vulnerability Scanner Works

Types of Vulnerability Scans

Unauthenticated Scans

Authenticated Scans

Discovery Scans

Full Scans

Stealth Scans

Compliance Scans

Challenges to Consider When Running a Vulnerability Scan

Considering the Best Time to Run a Scan

Determining What Protocols Are in Use

Network Topology

Bandwidth Limitations

Query Throttling

Fragile Systems/Nontraditional Assets

## **Understanding How to Analyze Vulnerability Scan Results**

# **Table of Contents**

Sources for Further Investigation of Vulnerabilities

US-CERT

The CERT Division of Carnegie Mellon University

NIST

JPCERT

CAPEC

CVE

CWE

The Common Vulnerability Scoring System (CVSS)

How to Deal with a Vulnerability

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

## **Chapter 4 Social Engineering Attacks**

Do I Know This Already? Quiz

Foundation Topics

Pretexting for an Approach and Impersonation

Social Engineering Attacks

Email Phishing

Spear Phishing

Whaling

Vishing

Short Message Service (SMS) Phishing

Universal Serial Bus (USB) Drop Key

Watering Hole Attacks

Physical Attacks

Tailgating

# Table of Contents

Dumpster Diving

Shoulder Surfing

Badge Cloning

## Social Engineering Tools

Social-Engineer Toolkit (SET)

Browser Exploitation Framework (BeEF)

Call Spoofing Tools

## Methods of Influence

## Exam Preparation Tasks

## Review All Key Topics

## Define Key Terms

## Q&A

## Chapter 5 Exploiting Wired and Wireless Networks

### Do I Know This Already? Quiz

### Foundation Topics

### Exploiting Network-Based Vulnerabilities

Windows Name Resolution and SMB Attacks

NetBIOS Name Service and LLMNR

SMB Exploits

DNS Cache Poisoning

SNMP Exploits

SMTP Exploits

SMTP Open Relays

Useful SMTP Commands

Known SMTP Server Exploits

FTP Exploits

Pass-the-Hash Attacks

Kerberos and LDAP-Based Attacks



# **Table of Contents**

Kerberoasting  
On-Path Attacks  
ARP Spoofing and ARP Cache Poisoning  
Downgrade Attacks  
Route Manipulation Attacks  
DoS and DDoS Attacks  
Direct DoS Attacks  
Reflected DoS and DDoS Attacks  
Amplification DDoS Attacks  
Network Access Control (NAC) Bypass  
VLAN Hopping  
DHCP Starvation Attacks and Rogue DHCP Servers

## **Exploiting Wireless Vulnerabilities**

Rogue Access Points  
Evil Twin Attacks  
Disassociation (or Deauthentication) Attacks  
Preferred Network List Attacks  
Wireless Signal Jamming and Interference  
War Driving  
Initialization Vector (IV) Attacks and Unsecured Wireless Protocols  
Attacks Against WEP  
Attacks Against WPA  
KRACK Attacks  
WPA3 Vulnerabilities  
Wi-Fi Protected Setup (WPS) PIN Attacks  
KARMA Attacks  
Fragmentation Attacks  
Credential Harvesting  
Bluejacking and Bluesnarfing  
Bluetooth Low Energy (BLE) Attacks

# **Table of Contents**

Radio-Frequency Identification (RFID) Attacks

Password Spraying

Exploit Chaining

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

## **Chapter 6 Exploiting Application-Based Vulnerabilities**

Do I Know This Already? Quiz

Foundation Topics

Overview of Web Application-Based Attacks for Security

Professionals and the OWASP Top 10

The HTTP Protocol

Web Sessions

OWASP Top 10

How to Build Your Own Web Application Lab

Understanding Business Logic Flaws

Understanding Injection-Based Vulnerabilities

SQL Injection Vulnerabilities

A Brief Introduction to SQL

SQL Injection Categories

Database Fingerprinting

The UNION Exploitation Technique

Booleans in SQL Injection Attacks

Out-of-Band Exploitation

Stacked Queries

The Time-Delay SQL Injection Technique

Surveying a Stored Procedure SQL Injection

# **Table of Contents**

SQL Injection Mitigations

Command Injection Vulnerabilities

Lightweight Directory Access Protocol (LDAP) Injection Vulnerabilities

## **Exploiting Authentication-Based Vulnerabilities**

Session Hijacking

Redirect Attacks

Default Credentials

Kerberos Vulnerabilities

## **Exploiting Authorization-Based Vulnerabilities**

Parameter Pollution

Insecure Direct Object Reference Vulnerabilities

## **Understanding Cross-Site Scripting (XSS) Vulnerabilities**

Reflected XSS Attacks

Stored XSS Attacks

XSS Evasion Techniques

XSS Mitigations

## **Understanding Cross-Site Request Forgery (CSRF/XSRF) and Server-Side Request Forgery Attacks**

## **Understanding Clickjacking**

## **Exploiting Security Misconfigurations**

Exploiting Directory Traversal Vulnerabilities

Cookie Manipulation Attacks

## **Exploiting File Inclusion Vulnerabilities**

Local File Inclusion Vulnerabilities

Remote File Inclusion Vulnerabilities

## **Exploiting Insecure Code Practices**

Comments in Source Code

Lack of Error Handling and Overly Verbose Error Handling

Hard-Coded Credentials

# **Table of Contents**

Race Conditions

Unprotected APIs

Hidden Elements

Lack of Code Signing

Additional Web Application Hacking Tools

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

## **Chapter 7 Cloud, Mobile, and IoT Security**

Do I Know This Already? Quiz

Foundation Topics

Researching Attack Vectors and Performing Attacks on Cloud

Technologies

Credential Harvesting

Privilege Escalation

Account Takeover

Metadata Service Attacks

Attacks Against Misconfigured Cloud Assets

Resource Exhaustion and DoS Attacks

Cloud Malware Injection Attacks

Side-Channel Attacks

Tools and Software Development Kits (SDKs)

Explaining Common Attacks and Vulnerabilities Against Specialized  
Systems

Attacking Mobile Devices

Attacking Internet of Things (IoT) Devices

Analyzing IoT Protocols

# **Table of Contents**

IoT Security Special Considerations

Common IoT Vulnerabilities

Data Storage System Vulnerabilities

Management Interface Vulnerabilities

Exploiting Virtual Machines

Vulnerabilities Related to Containerized Workloads

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

## **Chapter 8 Performing Post-Exploitation Techniques**

Do I Know This Already? Quiz

Foundation Topics

Creating a Foothold and Maintaining Persistence After Compromising  
a System

Reverse and Bind Shells

Command and Control (C2) Utilities

Scheduled Jobs and Tasks

Custom Daemons, Processes, and Additional Backdoors

New Users

Understanding How to Perform Lateral Movement, Detection Avoidance,  
and Enumeration

Post-Exploitation Scanning

Legitimate Utilities and Living Off the Land

PowerShell for Post-Exploitation Tasks

PowerSploit and Empire

BloodHound

Windows Management Instrumentation for Post-Exploitation Tasks

# **Table of Contents**

Sysinternals and PsExec

Windows Remote Management (WinRM) for Post-Exploitation Tasks

Post-Exploitation Privilege Escalation

How to Cover Your Tracks

Steganography

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

## **Chapter 9 Reporting and Communication**

Do I Know This Already? Quiz

Foundation Topics

Comparing and Contrasting Important Components of Written Reports

Report Contents

Storage Time for Report and Secure Distribution

Note Taking

Common Themes/Root Causes

Analyzing the Findings and Recommending the Appropriate Remediation  
Within a Report

Technical Controls

Administrative Controls

Operational Controls

Physical Controls

Explaining the Importance of Communication During the Penetration  
Testing Process

Communication Triggers

Reasons for Communication

Goal Reprioritization and Presentation of Findings

# **Table of Contents**

## Explaining Post-Report Delivery Activities

- Post-Engagement Cleanup

- Additional Post-Report Delivery Activities

## Exam Preparation Tasks

- Review All Key Topics

- Define Key Terms

- Q&A

## Chapter 10 Tools and Code Analysis

- Do I Know This Already? Quiz

- Foundation Topics

- Understanding the Basic Concepts of Scripting and Software Development

  - Logic Constructs

  - Data Structures

  - Libraries

  - Procedures

  - Functions

  - Classes

  - Analysis of Scripts and Code Samples for Use in Penetration Testing

  - The Bash Shell

  - Resources to Learn Python

  - Resources to Learn Ruby

  - Resources to Learn PowerShell

  - Resources to Learn Perl

  - Resources to Learn JavaScript

- Understanding the Different Use Cases of Penetration Testing Tools and Analyzing Exploit Code

  - Penetration Testing Focused Linux Distributions

# **Table of Contents**

Kali Linux

Parrot OS

BlackArch Linux

Common Tools for Reconnaissance and Enumeration

Tools for Passive Reconnaissance

Tools for Active Reconnaissance

Common Tools for Vulnerability Scanning

Common Tools for Credential Attacks

John the Ripper

Cain

Hashcat

Hydra

RainbowCrack

Medusa and Ncrack

CeWL

Mimikatz

Patator

Common Tools for Persistence

Common Tools for Evasion

Veil

Tor

Proxychains

Encryption

Encapsulation and Tunneling Using DNS and Protocols Such as NTP

Exploitation Frameworks

Metasploit

BeEF

Common Decompilation, Disassembly, and Debugging Tools

The GNU Project Debugger (GDB)

Windows Debugger



# Table of Contents

OllyDbg

edb Debugger

Immunity Debugger

IDA

Objdump

Common Tools for Forensics

Common Tools for Software Assurance

SpotBugs, Findseccbugs, and SonarQube

Fuzzers and Fuzz Testing

Peach

Mutiny Fuzzing Framework

American Fuzzy Lop

Wireless Tools

Steganography Tools

Cloud Tools

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Q&A

## Chapter 11 Final Preparation

Tools for Final Preparation

Pearson Test Prep Practice Test Engine

Accessing the Pearson Test Prep Software Online

Accessing the Pearson Test Prep Software Offline

Customizing Your Exams

Updating Your Exams

Premium Edition

Chapter-Ending Review Tools

Suggested Plan for Final Review/Study

# **Table of Contents**

Summary

Glossary of Key Terms

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Appendix A: Answers to the Do I Know This Already?  
Quizzes and Q&A Sections

# **Table of Contents**

Appendix B: CompTIA® PenTest+ PT0-002 Cert Guide Exam  
Updates

Index

Appendix C: Study Planner