uCertify

Course Outline

CompTIA PenTest+ Cert Guide (PT0-002)

12 May 2024

1. Course Objective
2. Pre-Assessment
3. Exercises, Quizzes, Flashcards & Glossary

   Number of Questions
4. Expert Instructor-Led Training
5. ADA Compliant & JAWS Compatible Platform
6. State of the Art Educator Tools
7. Award Winning Learning Platform (LMS)
8. Chapter & Lessons

   Syllabus

   Chapter 1: Introduction

   Chapter 2: Introduction to Ethical Hacking and Penetration Testing

   Chapter 3: Planning and Scoping a Penetration Testing Assessment

   Chapter 4: Information Gathering and Vulnerability Scanning

   Chapter 5: Social Engineering Attacks

   Chapter 6: Exploiting Wired and Wireless Networks

   Chapter 7: Exploiting Application-Based Vulnerabilities

   Chapter 8: Cloud, Mobile, and IoT Security

   Chapter 9: Performing Post-Exploitation Techniques

   Chapter 10: Reporting and Communication

   Chapter 11: Tools and Code Analysis

   Videos and How To
9. Practice Test

   Here's what you get

   Features
10. Live labs

    Lab Tasks

    Here's what you get
11. Post-Assessment

1. Course Objective

Gain hands-on experience to pass the CompTIA Pentest+ certification exam with the CompTIA Pentest+ Cert Guide course and lab. Interactive chapters and hands-on labs comprehensively cover the (PT0-002) exam objectives and provide knowledge in areas such as penetration testing engagement including vulnerability scanning, understanding legal and compliance requirements, analyzing results, and producing a written report with remediation techniques and many more.

2. Pre-Assessment

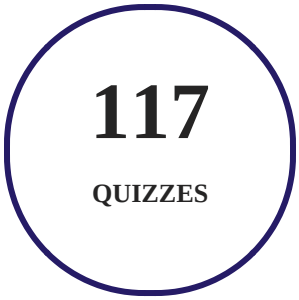
Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

3. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

4. Quizzes

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.



5. flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.

6. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.

7. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

8. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

9. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

10. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been

recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
    1. Best Postsecondary Learning Solution

- **2015**
    1. Best Education Solution
    2. Best Virtual Learning Solution
    3. Best Student Assessment Solution
    4. Best Postsecondary Learning Solution
    5. Best Career and Workforce Readiness Solution
    6. Best Instructional Solution in Other Curriculum Areas
    7. Best Corporate Learning/Workforce Development Solution

- **2016**
    1. Best Virtual Learning Solution
    2. Best Education Cloud-based Solution
    3. Best College and Career Readiness Solution
    4. Best Corporate / Workforce Learning Solution
    5. Best Postsecondary Learning Content Solution
    6. Best Postsecondary LMS or Learning Platform
    7. Best Learning Relationship Management Solution

- **2017**
    1. Best Overall Education Solution
    2. Best Student Assessment Solution
    3. Best Corporate/Workforce Learning Solution
    4. Best Higher Education LMS or Learning Platform

- **2018**
    1. Best Higher Education LMS or Learning Platform

2. Best Instructional Solution in Other Curriculum Areas
3. Best Learning Relationship Management Solution

- **2019**
  1. Best Virtual Learning Solution
  2. Best Content Authoring Development or Curation Solution
  3. Best Higher Education Learning Management Solution (LMS)

- **2020**
  1. Best College and Career Readiness Solution
  2. Best Cross-Curricular Solution
  3. Best Virtual Learning Solution

11.  Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: Introduction

- The Goals of the CompTIA PenTest+ Certification
- The Exam Objectives (Domains)
- Steps to Earning the PenTest+ Certification

- Facts About the PenTest+ Exam
- About the CompTIA PenTest+ PT0-002 Cert Guide

Chapter 2: Introduction to Ethical Hacking and Penetration Testing

- Understanding Ethical Hacking and Penetration Testing
- Exploring Penetration Testing Methodologies
- Building Your Own Lab
- Review All Key Topics

Chapter 3: Planning and Scoping a Penetration Testing Assessment

- Comparing and Contrasting Governance, Risk, and Compliance Concepts
- Explaining the Importance of Scoping and Organizational or Customer Requirements
- Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and Integrity
- Review All Key Topics

Chapter 4: Information Gathering and Vulnerability Scanning

- Performing Passive Reconnaissance
- Performing Active Reconnaissance
- Understanding the Art of Performing Vulnerability Scans

- Understanding How to Analyze Vulnerability Scan Results
- Review All Key Topics

Chapter 5: Social Engineering Attacks

- Pretexting for an Approach and Impersonation
- Social Engineering Attacks
- Physical Attacks
- Social Engineering Tools
- Methods of Influence
- Review All Key Topics

Chapter 6: Exploiting Wired and Wireless Networks

- Exploiting Network-Based Vulnerabilities
- Exploiting Wireless Vulnerabilities
- Review All Key Topics

Chapter 7: Exploiting Application-Based Vulnerabilities

- Overview of Web Application-Based Attacks for Security Professionals and the OWASP Top 10

- How to Build Your Own Web Application Lab
- Understanding Business Logic Flaws
- Understanding Injection-Based Vulnerabilities
- Exploiting Authentication-Based Vulnerabilities
- Exploiting Authorization-Based Vulnerabilities
- Understanding Cross-Site Scripting (XSS) Vulnerabilities
- Understanding Cross-Site Request Forgery (CSRF/XSRF) and Server-Side Request Forgery Attacks
- Understanding Clickjacking
- Exploiting Security Misconfigurations
- Exploiting File Inclusion Vulnerabilities
- Exploiting Insecure Code Practices
- Review All Key Topics

Chapter 8: Cloud, Mobile, and IoT Security

- Researching Attack Vectors and Performing Attacks on Cloud Technologies
- Explaining Common Attacks and Vulnerabilities Against Specialized Systems
- Review All Key Topics

Chapter 9: Performing Post-Exploitation Techniques

- Creating a Foothold and Maintaining Persistence After Compromising a System
- Understanding How to Perform Lateral Movement, Detection Avoidance, and Enumeration
- Review All Key Topics

Chapter 10: Reporting and Communication

- Comparing and Contrasting Important Components of Written Reports
- Analyzing the Findings and Recommending the Appropriate Remediation Within a Report
- Explaining the Importance of Communication During the Penetration Testing Process
- Explaining Post-Report Delivery Activities
- Review All Key Topics

Chapter 11: Tools and Code Analysis

- Understanding the Basic Concepts of Scripting and Software Development
- Understanding the Different Use Cases of Penetration Testing Tools and Analyzing Exploit Code
- Review All Key Topics

12. Practice Test

Here's what you get

85	2	85
PRE-ASSESSMENTS QUESTIONS	FULL LENGTH TESTS	POST-ASSESSMENTS QUESTIONS

Features

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In test mode, learners can take a timed test simulating the actual exam conditions. In review mode, learners can read through one item at a time without attempting it.

13. Live Labs

The benefits of live-labs are:

- Exam based practical tasks
- Real equipment, absolutely no simulations
- Access to the latest industry technologies
- Available anytime, anywhere on any device
- Break and Reset functionality

- No hardware costs

Lab Tasks

Information Gathering and Vulnerability Scanning

- Performing Zone Transfer Using dig
- Using dnsrecon
- Using Recon-ng to Gather Information
- Performing Reconnaissance on a Network
- Performing a UDP Scan Using Nmap
- Using Nmap for User Enumeration
- Using Nmap for Network Enumeration
- Performing Nmap SYN Scan
- Conducting Vulnerability Scanning Using Nessus

Social Engineering Attacks

- Using BeEF
- Using SET Tool to Plan an Attack

Exploiting Wired and Wireless Networks

- Using the EternalBlue Exploit in Metasploit
- Simulating the DDoS Attack
- Performing a DHCP Starvation Attack
- Understanding the Pass-the-hash Attack
- Performing ARP Spoofing
- Exploiting SMTP
- Exploiting SNMP
- Searching Exploits Using searchsploit
- Exploiting SMB

Exploiting Application-Based Vulnerabilities

- Conducting a Cross Site Scripting (XXS) attack
- Using curl to Make the HTTP GET Request
- Capturing Network Packets Using tcpdump
- Exploiting Command Injection Vulnerabilities
- Exploiting a Website Using SQL Injection
- Performing Session Hijacking Using Burp Suite
- Cracking Passwords
- Conducting a Cross-Site Request Forgery Attack

Cloud, Mobile, and IoT Security

- Understanding Local Privilege Escalation

Performing Post-Exploitation Techniques

- Using OWASP ZAP
- Using the Task Scheduler
- Writing Bash Shell Script
- Performing an Intense Scan in Zenmap
- Using dig and nslookup Commands
- Creating Reverse and Bind Shells Using Netcat
- Hiding Text Using Steganography
- Using the Metasploit RDP Post-Exploitation Module

Tools and Code Analysis

- Finding Live Hosts by Using the Ping Sweep in Python
- Whitelisting an IP Address in the Windows Firewall
- Viewing Exploits Written in Perl
- Viewing the Effects of Hostile JavaScript in the Browser
- Using Meterpreter to Display the System Information
- Performing Vulnerability Scanning Using OpenVAS
- Enumerating Data Using enum4linux

- Using Maltego to Gather Information
- Cracking a Linux Password Using John the Ripper

Here's what you get

46	42	01:34
LIVE LABS	VIDEO TUTORIALS	HOURS

14. Post-Assessment

After completion of the uCertify course Post-Assessments are given to students and often used in conjunction with a Pre-Assessment to measure their achievement and the effectiveness of the exam.

GET IN TOUCH:

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com