uCertify

Course Outline

CompTIA PenTest+ (PT0-002)

17 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: Penetration Testing

   Chapter 3: Planning and Scoping Penetration Tests

   Chapter 4: Information Gathering

   Chapter 5: Vulnerability Scanning

   Chapter 6: Analyzing Vulnerability Scans

   Chapter 7: Exploiting and Pivoting

   Chapter 8: Exploiting Network Vulnerabilities

   Chapter 9: Exploiting Physical and Social Vulnerabilities

   Chapter 10: Exploiting Application Vulnerabilities

   Chapter 11: Attacking Hosts, Cloud Technologies, and Specialized Systems

   Chapter 12: Reporting and Communication

   Chapter 13: Scripting for Penetration Testing

   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

CompTIA PenTest+ (PT0-002) comes in handy as the PT0-002 study guide with well descriptive interactive lessons containing knowledge checks, quizzes, flashcards, and glossary terms to get a detailed understanding of the concepts, such as planning and scoping a penetration testing engagement, understanding legal and compliance requirements, performing vulnerability scanning and penetration testing using appropriate tools and techniques, and then analyzing the results, and so on. The live labs present in the course will give you a hands-on experience of penetration testing.

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. Quiz

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

- CompTIA
- The PenTest+ Exam
- What Does This Course Cover?

- CompTIA PenTest+ Certification Exam Objectives

Chapter 2: 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

Chapter 3: 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

Chapter 4: Information Gathering

- Footprinting and Enumeration
- Active Reconnaissance and Enumeration
- Information Gathering and Defenses
- Summary
- Exam Essentials
- Lab Exercises

Chapter 5: 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

Chapter 6: Analyzing Vulnerability Scans

- Reviewing and Interpreting Scan Reports
- Validating Scan Results
- Common Vulnerabilities
- Summary
- Exam Essentials
- Lab Exercises

Chapter 7: Exploiting and Pivoting

- Exploits and Attacks
- Exploitation Toolkits
- Exploit Specifics
- Leveraging Exploits
- Persistence and Evasion
- Pivoting

- Covering Your Tracks
- Summary
- Exam Essentials
- Lab Exercises

Chapter 8: Exploiting Network Vulnerabilities

- Identifying Exploits
- Conducting Network Exploits
- Exploiting Windows Services
- Identifying and Exploiting Common Services
- Wireless Exploits
- Summary
- Exam Essentials
- Lab Exercises

Chapter 9: Exploiting Physical and Social Vulnerabilities

- Physical Facility Penetration Testing
- Social Engineering
- Summary

- Exam Essentials
- Lab Exercises

Chapter 10: 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

Chapter 11: 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

Chapter 12: Reporting and Communication

- The Importance of Communication
- Recommending Mitigation Strategies
- Writing a Penetration Testing Report
- Wrapping Up the Engagement
- Summary
- Exam Essentials
- Lab Exercises

Chapter 13: 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

12. Practice Test

Here's what you get

80	2	80
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

- Using dig and nslookup Commands
- Performing Zone Transfer Using dig
- Using Maltego to Gather Information
- Using Recon-ng to Gather Information
- Using Nmap for Network Enumeration
- Performing Reconnaissance on a Network
- Performing an Intense Scan in Zenmap
- Using Nmap for User Enumeration
- Performing a UDP Scan Using Nmap
- Performing Nmap SYN Scan

Vulnerability Scanning

- Conducting Vulnerability Scanning Using Nessus

Analyzing Vulnerability Scans

- Understanding Local Privilege Escalation

Exploiting and Pivoting

- Performing Vulnerability Scanning Using OpenVAS
- Searching Exploits Using searchsploit
- Using Meterpreter to Display the System Information
- Using the Task Scheduler
- Understanding the Pass-the-hash Attack
- Using the Metasploit RDP Post-Exploitation Module

Exploiting Network Vulnerabilities

- Performing ARP Spoofing
- Conducting a Cross Site Scripting (XXS) attack
- Capturing Network Packets Using tcpdump
- Simulating the DDoS Attack
- Using the EternalBlue Exploit in Metasploit
- Exploiting SMB
- Exploiting SMTP
- Exploiting SNMP

Exploiting Physical and Social Vulnerabilities

- Using SET Tool to Plan an Attack
- Using BeEF

Exploiting Application Vulnerabilities

- Exploiting Command Injection Vulnerabilities
- Exploiting a Website Using SQL Injection
- Conducting a Cross-Site Request Forgery Attack
- Hiding Text Using Steganography
- Using OWASP ZAP
- Performing Session Hijacking Using Burp Suite

Attacking Hosts, Cloud Technologies, and Specialized Systems

- Cracking Passwords
- Cracking a Linux Password Using John the Ripper
- Creating Reverse and Bind Shells Using Netcat

Scripting for Penetration Testing

- Whitelisting an IP Address in the Windows Firewall
- Viewing Exploits Written in Perl
- Viewing the Effects of Hostile JavaScript in the Browser
- Finding Live Hosts by Using the Ping Sweep in Python
- Writing Bash Shell Script

Here's what you get

42	40	01:48
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