uCertify

Course Outline

CompTIA PenTest+ (PT0-001)

Lesson Practice test Lab Live-Lab

04 Sep 2021

Contents

Videos and How To

9. Practice Test

   Here's what you get

   Features

10. Performance Based Labs

    Lab Tasks

    Here's what you get

11. Post-Assessment

1. Course Objective

Gain hands-on experience to pass the PT0-001 exam with the CompTIA PenTest+ PT0-001 course and lab. The lab is a simulator that provides a virtual environment for users to explore and learn. The CompTIA PenTest+ study guide covers the PT0-001 exam objectives and knowledge to exploit network, wireless, application, and RF-based vulnerabilities; summarize physical security attacks and perform post-exploitation techniques, and many more.

2. Pre-Assessment

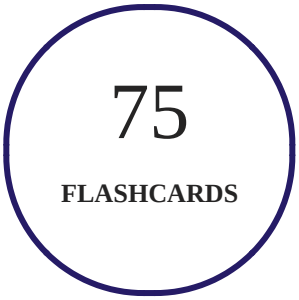
Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

3. 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.

4. 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.



5. 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.

6. 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.

7. 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.

8. 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.

9. 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

10. 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
- Key Legal Concepts for Penetration Tests
- Understanding Compliance-Based Assessments
- 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: Exploit and Pivot

- 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

- Conducting Network Exploits
- Exploiting Windows Services
- 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
- Application Testing Tools
- Summary
- Exam Essentials
- Lab Exercises

Chapter 11: Exploiting Host Vulnerabilities

- Attacking Hosts
- Remote Access
- Attacking Virtual Machines and Containers

- Physical Device Security
- Attacking Mobile Devices
- Credential Attacks
- Summary
- Exam Essentials
- Lab Exercises

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
- Summary
- Exam Essentials

- Lab Exercises

Chapter 13: 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 14: Appendix: Video Tutorials

Videos and How To

uCertify course includes videos to help understand concepts. It also includes How Tos that help learners in accomplishing certain tasks.

192	07:26
VIDEOS	**HOURS**

11. Practice Test

Here's what you get

80
PRE-ASSESSMENTS QUESTIONS

2
FULL LENGTH TESTS

80
POST-ASSESSMENTS QUESTIONS

Features

Full Remediation

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.

Learn, Test and Review Mode

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.

12. Performance Based Labs

uCertify's performance-based labs are Live Labs. Learn the real world skills using Live Labs. uCertify Labs are cloud-based, device-enabled and can be easily integrated with an LMS. Features of uCertify labs:

- Provide hands-on experience in a safe, online environment
- Labs simulate real world, hardware, software & CLI environment
- Flexible and inexpensive alternative to physical Labs
- Comes with well-organized component library for every task
- Highly interactive - learn by doing
- Explanations and remediation available
- Videos on how to perform

Lab Tasks

- Studying SOW, MSA, and NDA
- Examining Penetration Testing Execution Standard (PTES)
- Examining Open Source Security Testing Methodology Manual
- Examining NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
- Performing Domain Enumeration
- Performing Zone Transfer Using dig
- Using ExifTool
- Using the theHarvester Tool to Gather Information about a Victim
- Using Maltego
- Studying the Communication Plan and the Main Elements of a Pen Test Report
- Performing Nmap SYN Scan
- Performing Nmap UDP Scan

- Using Nmap for Host Enumeration
- Using Nmap for User Enumeration
- Using Nmap for Network Share Enumeration
- Using Nmap for Web Application Enumeration
- Using Nmap for Network Enumeration
- Using Zenmap
- Using Nslookup for Passive Reconnaissance
- Examining the OWASP Web Testing Methodologies and Testing Guide
- Using Nikto
- Studying CVSS Exercises with the CVSS Calculator
- Using Searchsploit
- Using OpenVAS
- Using meterpreter
- Exploiting SMB
- Using the Metasploit RDP Post-Exploitation Module
- Using the SET Tool
- Performing ARP Spoofing
- Performing the Man-in-the-Middle Attack
- Using the EternalBlue Exploit in Metasploit
- Exploiting SNMP
- Exploiting SMTP
- Exploiting SQL Injection Vulnerabilities
- Exploiting Blind SQL Injection Vulnerabilities
- Exploiting Command Injection Vulnerabilities
- Understanding Credential based Brute-force Attack
- Performing Session Hijacking
- Exploiting Local File Inclusion Vulnerabilities
- Exploiting Remote File Inclusion Vulnerabilities
- Exploiting the Stored (Persistent) XSS Attack
- Exploiting the DOM-Based XSS Attack
- Exploiting the Reflected XSS Attack
- Exploiting the Cross-site Request Forgery (CSRF or XSRF) Attacks
- Using Burp and the OWASP ZAP Attack Proxy

- Understanding the Pass-the-hash Attack
- Understanding SUID or SGID and Unix Program
- Understanding Local Privilege Escalation
- Exploiting SAM Database
- Creating Reverse and Bind Shells using Netcat
- Using Apktool to Decode and Analyze apk File
- Using Bash for Penetration Testing
- Using Python for Penetration Testing
- Using PowerShell for Penetration Testing

Here's what you get

54	55
PERFORMANCE BASED LAB	**VIDEO TUTORIALS**

13. Live Labs

Live-Lab is a real computer equipment, networked together and conveniently accessible over the internet using virtualization. A live-lab has equipments such as a computer, server, switch or router in it that a user is free to configure.

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

Planning and Scoping Penetration Tests

- Studying SOW, MSA, and NDA

Information Gathering

- Examining Penetration Testing Execution Standard (PTES)
- Examining Open Source Security Testing Methodology Manual
- Examining NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
- Performing Domain Enumeration
- Performing Zone Transfer Using dig
- Using ExifTool
- Using the theHarvester Tool to Gather Information about a Victim
- Using Maltego
- Studying the Communication Plan and the Main Elements of a Pen Test Report
- Performing Nmap SYN Scan
- Performing Nmap UDP Scan
- Using Nmap for Host Enumeration
- Using Nmap for User Enumeration

- Using Nmap for Network Share Enumeration
- Using Nmap for Web Application Enumeration
- Using Nmap for Network Enumeration
- Using Zenmap
- Using Nslookup for Passive Reconnaissance

Vulnerability Scanning

- Examining the OWASP Web Testing Methodologies and Testing Guide
- Using Nikto

Analyzing Vulnerability Scans

- Studying CVSS Exercises with the CVSS Calculator

Exploit and Pivot

- Using Searchsploit
- Using OpenVAS
- Using meterpreter
- Exploiting SMB
- Using the Metasploit RDP Post-Exploitation Module
- Using the SET Tool

Exploiting Network Vulnerabilities

- Performing ARP Spoofing
- Performing the Man-in-the-Middle Attack
- Using the EternalBlue Exploit in Metasploit
- Exploiting SNMP
- Exploiting SMTP

Exploiting Application Vulnerabilities

- Exploiting SQL Injection Vulnerabilities

- Exploiting Blind SQL Injection Vulnerabilities
- Exploiting Command Injection Vulnerabilities
- Understanding Credential based Brute-force Attack
- Performing Session Hijacking
- Exploiting Local File Inclusion Vulnerabilities
- Exploiting Remote File Inclusion Vulnerabilities
- Exploiting the Stored (Persistent) XSS Attack
- Exploiting the DOM-Based XSS Attack
- Exploiting the Reflected XSS Attack
- Exploiting the Cross-site Request Forgery (CSRF or XSRF) Attacks
- Using Burp and the OWASP ZAP Attack Proxy

Exploiting Host Vulnerabilities

- Understanding the Pass-the-hash Attack
- Understanding SUID or SGID and Unix Program
- Understanding Local Privilege Escalation
- Exploiting SAM Database
- Creating Reverse and Bind Shells using Netcat
- Using Apktool to Decode and Analyze apk File

Scripting for Penetration Testing

- Using Bash for Penetration Testing
- Using Python for Penetration Testing
- Using PowerShell for Penetration Testing

Here's what you get

54
LIVE LABS

55
VIDEO TUTORIALS

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.

CONNECT WITH US

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com