uCertify

Course Outline

Pearson CompTIA Cybersecurity Analyst (CySA+)

09 Nov 2019

Lesson Practice test Lab

Contents

1. Course Objective

Gain hands-on experience to pass the CompTIA CySA+ CS0-001 certification exam with the CompTIA Cybersecurity Analyst (CySA+) course and lab. The lab is cloud-based, device-enabled, and can be easily integrated with an LMS. Interactive chapters comprehensively cover CompTIA CySA+ CS0-001 certification exam objectives and teach you how to configure and use threat detection tools; perform data analysis, and interpret the interpret the reports to protect an organization by identifying vulnerabilities, threats, and risks.

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 assignments. 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 5 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

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

- Goals and Methods
- Who Should Read This Book?
- Strategies for Exam Preparation

Chapter 2: Applying Environmental Reconnaissance Techniques

- Procedures/Common Tasks
- Variables
- Tools
- Review All Key Topics

Chapter 3: Analyzing the Results of Network Reconnaissance

- Point-in-Time Data Analysis
- Data Correlation and Analytics
- Data Output
- Tools
- Review All Key Topics

Chapter 4: Recommending and Implementing the Appropriate Response and Countermeasure

- Network Segmentation
- Honeypot
- Endpoint Security
- Group Policies
- ACLs
- Hardening
- Network Access Control
- Review All Key Topics

Chapter 5: Practices Used to Secure a Corporate Environment

- Penetration Testing
- Reverse Engineering
- Training and Exercises
- Risk Evaluation
- Review All Key Topics

Chapter 6: Implementing an Information Security Vulnerability Management Process

- Identification of Requirements
- Establish Scanning Frequency
- Configure Tools to Perform Scans According to Specification
- Execute Scanning
- Generate Reports
- Remediation
- Ongoing Scanning and Continuous Monitoring
- Review All Key Topics

Chapter 7: Analyzing Scan Output and Identifying Common Vulnerabilities

- Analyzing Output Resulting from a Vulnerability Scan
- Common Vulnerabilities Found in Targets Within an Organization
- Review All Key Topics

Chapter 8: Identifying Incident Impact and Assembling a Forensic Toolkit

- Threat Classification
- Factors Contributing to Incident Severity and Prioritization
- Forensics Kit

- Forensic Investigation Suite
- Review All Key Topics

Chapter 9: The Incident Response Process

- Stakeholders
- Purpose of Communication Processes
- Role-Based Responsibilities
- Using Common Symptoms to Select the Best Course of Action to Support Incident Response
- Review All Key Topics

Chapter 10: Incident Recovery and Post-Incident Response

- Containment Techniques
- Eradication Techniques
- Validation
- Corrective Actions
- Incident Summary Report
- Review All Key Topics

Chapter 11: Frameworks, Policies, Controls, and Procedures

- Regulatory Compliance
- Frameworks
- Policies
- Controls
- Procedures
- Verifications and Quality Control
- Review All Key Topics

Chapter 12: Remediating Security Issues Related to Identity and Access Management

- Security Issues Associated with Context-Based Authentication
- Security Issues Associated with Identities
- Security Issues Associated with Identity Repositories
- Security Issues Associated with Federation and Single Sign-on
- Exploits
- Review All Key Topics

Chapter 13: Security Architecture and Implementing Compensating Controls

- Security Data Analytics
- Manual Review
- Defense in Depth
- Review All Key Topics

Chapter 14: Application Security Best Practices

- Best Practices During Software Development
- Secure Coding Best Practices
- Review All Key Topics

Chapter 15: Using Cybersecurity Tools and Technologies

- Preventative Tools
- Collective Tools
- Analytical Tools
- Exploit Tools
- Forensics Tools
- Review All Key Topics

Chapter 16: Module 1: Threat Management

- Lesson 1: Reconnaissance Techniques
- Lesson 2: Network Reconnaissance
- Lesson 3: Response and Counter Measures
- Lesson 4: Securing Corporate Environments

Chapter 17: Module 2: Vulnerability Management

- Lesson 5: Implementing the Information Security Vulnerability Management Process
- Lesson 6: Analyze Output of Vulnerability Scan
- Lesson 7: Compare and Contrast Common Vulnerabilities

Chapter 18: Module 3: Cyber Incident Response

- Lesson 8: Determine Impact of an Incident
- Lesson 9: Forensics Tools and Investigation
- Lesson 10: Incident Reporting and Communications
- Lesson 11: Analyzing Incident Response Symptoms and Recovery Techniques
- Lesson 12: Post-Incident Response Process

Chapter 19: Module 4: Security Architectures and Tool Sets

- Lesson 13: Frameworks, Common Policies, Controls, and Procedures
- Lesson 14: Access Control and Access Management Remediation
- Lesson 15: Reviewing Security Architectures
- Lesson 16: Software Development Lifecycle (SDLC) Best Practices
- Lesson 17: Cybersecurity Tools and Technologies

Videos and How To

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

175	21:35
VIDEOS	HOURS

11. Practice Test

uCertify provides full length practice tests. These tests closely follow the exam objectives and are designed to simulate real exam conditions. Each course has a number of test sets consisting of hundreds of items to ensure that learners are prepared for the certification exam.

Here's what you get

85	2	87
PRE-ASSESSMENTS QUESTIONS	FULL LENGTH TESTS	POST-ASSESSMENTS QUESTIONS

Features

Video Lessons

uCertify provides video training courses that contain videos and test set questions based on the exam. These courses are interactive and engaging and the learners can view the content at their own pace, in their own time, and on any device. Learners can easily track the engagement levels so they immediately know which course components are easy to understand and which are more difficult. Test set in the courses closely follow the exam objectives and are designed to simulate real exam conditions.

Interactive Questions

Each pre and post assessment comes with interactive questions which help users in better understanding of the subject matter.

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

- Performing reconnaissance on a network
- Downloading and running scanning tools
- Assessing the impact of malware
- Consulting a vulnerability database
- Initiating an SSH session from your Windows 10 client to your Windows Server
- Opening the policy template and setting the company name
- Reviewing and modifying the policy items
- Adding revision to the revision history
- Identifying security apps available for Android

- Accessing remotely the DT_Watch folder to generate audit logs
- Acquiring the Trojan horse simulator
- Uploading the Trojan horse simulator to VirusTotal
- Uploading the Trojan horse simulator to Malwr
- Identifying a suspicious account on the System User Groups
- Enabling auditing of the DT_Watch folder
- Enabling logging for audited objects
- Examining the audited events
- Making syslog entries readable
- Implementing security during the SDLC
- Collecting network-based security intelligence
- Installing Wireshark and WinPcap
- Acquainting yourself with Wireshark's interface
- Analyzing the capture file to find the attack(s)
- Generating network traffic and using filter
- Examining the traffic between client and server
- Confirming the spoofing attack in Wireshark
- Conducting vulnerability scans
- Installing Splunk on the server
- Manipulating Kali Linux VM's network interfaces
- Starting a live packet capture
- Using Process Explorer to view specific details about running processes on the system
- Examining the ipconfig options and creating the activity log
- Identifying search options in Metasploit
- Performing initial scan

Here's what you get

34

PERFORMANCE BASED LAB

13. 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.