Course Ou

CompTIA CASP+ (C



20 Mar 2024

Contents

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: Cryptographic Tools and Techniques

   Chapter 3: Comprehensive Security Solutions

   Chapter 4: Securing Virtualized, Distributed, and Shared Computing

   Chapter 5: Host Security

   Chapter 6: Application Security and Penetration Testing

   Chapter 7: Risk Management

   Chapter 8: Policies, Procedures, and Incident Response

   Chapter 9: Security Research and Analysis

   Chapter 10: Enterprise Security Integration

   Chapter 11: Security Controls for Communication and Collaboration

   Chapter 12: Appendix: 3D Avatar-based Simulation

   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

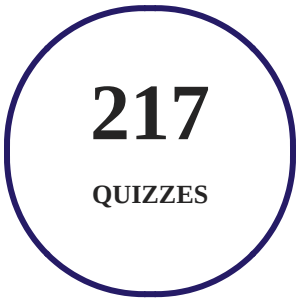
Kick start your prep for the CAS-003 exam with the CompTIA CASP CAS-003 Study Guide. The course has labs that provide a hands-on learning experience in a safe, online environment. The CASP training course provides complete coverage of the CAS-003 exam objectives and includes topics such as risk management, enterprise security architecture, enterprise security operations, technical integration of enterprise security, and research, development, and collaboration.

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

- Before You Begin the CompTIA CASP+ Certification Exam
- Who Should Read This Course
- What You Will Learn
- How This Course Is Organized
- How to Use This Course
- Tips for Taking the CASP+ Exam
- The CASP+ (2018 Edition) Exam Objective Map

Chapter 2: Cryptographic Tools and Techniques

- The History of Cryptography
- Cryptographic Services
- Symmetric Encryption
- Asymmetric Encryption
- Hybrid Encryption
- Hashing
- Digital Signatures
- Public Key Infrastructure
- Implementation of Cryptographic Solutions
- Cryptographic Attacks
- Exam Essentials
- Summary

Chapter 3: Comprehensive Security Solutions

- Advanced Network Design
- TCP/IP
- Secure Communication Solutions

- Secure Facility Solutions
- Secure Network Infrastructure Design
- Summary
- Exam Essentials

Chapter 4: Securing Virtualized, Distributed, and Shared Computing

- Enterprise Security
- Cloud Computing
- Virtualization
- Virtual LANs
- Virtual Networking and Security Components
- Enterprise Storage
- Summary
- Exam Essentials

Chapter 5: Host Security

- Firewalls and Network Access Control
- Host-Based Firewalls

- Persistent Agent
- Non-Persistent Agent
- Agent-Based Technology
- Agentless-Based Technology
- Trusted Operating Systems
- Endpoint Security Solutions
- Anti-Malware
- Host Hardening
- Asset Management
- Data Exfiltration
- Intrusion Detection and Prevention
- Network Management, Monitoring, and Security Tools
- Summary
- Exam Essentials

Chapter 6: Application Security and Penetration Testing

- Application Security Design Considerations
- Specific Application Issues

- Application Sandboxing
- Application Security Frameworks
- Software Assurance
- Development Approaches
- Secure Coding Standards
- Documentation
- Validation and Acceptance Testing
- Application Exploits
- Privilege Escalation
- Improper Storage of Sensitive Data
- Secure Cookie Storage and Transmission
- Context-Aware Management
- Malware Sandboxing
- Pivoting
- Open-Source Intelligence
- Memory Dumping
- Client-Side Processing vs. Server-Side Processing
- Security Assessments and Penetration Testing

- Red, Blue, and White Teaming
- Vulnerability Assessment Areas
- Security Assessment and Penetration Test Tools
- Summary
- Exam Essentials

Chapter 7: Risk Management

- Risk Terminology
- Identifying Vulnerabilities
- Operational Risks
- The Risk Assessment Process
- Best Practices for Risk Assessments
- Summary
- Exam Essentials
- Resources

Chapter 8: Policies, Procedures, and Incident Response

- A High-Level View of Documentation

- Business Documents Used to Support Security
- Documents and Controls Used for Sensitive Information
- Training and Awareness for Users
- Auditing Requirements and Frequency
- The Incident Response Framework
- Incident and Emergency Response
- Summary
- Exam Essentials

Chapter 9: Security Research and Analysis

- Applying Research Methods to Determine Industry Trends and Their Impact on the Enterprise
- Analyze Scenarios to Secure the Enterprise
- Summary
- Exam Essentials

Chapter 10: Enterprise Security Integration

- Integrate Enterprise Disciplines to Achieve Secure Solutions
- Integrate Hosts, Storage, Networks, and Applications into a Secure Enterprise Architecture
- Integrate Mobility Management

- Summary
- Exam Essentials

Chapter 11: Security Controls for Communication and Collaboration

- Selecting the Appropriate Control to Secure Communications and Collaboration Solutions
- Integrate Advanced Authentication and Authorization Technologies to Support Enterprise Objectives
- Implement Security Activities across the Technology Life Cycle
- Physical Security Tools for Security Assessment
- Summary
- Exam Essentials

Chapter 12: Appendix: 3D Avatar-based Simulation

11. Practice Test

Here's what you get

90	2	90
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.

12. 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

Cryptographic Tools and Techniques

- Using the MD Series Algorithm
- Using the SHA Series Algorithm
- Connecting to an SSH Server
- Using Steganography
- Installing Remote Access Server (RAS)
- Observe an SHA256-Generated Hash Value
- Spoofing MAC Address

Comprehensive Security Solutions

- Using Packet Filtering to Restrict Sites
- Capturing the ICMP Packets with Wireshark
- Attempting a Zone Transfer
- Installing and Configuring AD DS

Securing Virtualized, Distributed, and Shared Computing

- Creating a Virtual Switch
- Installing a Virtual Machine

Host Security

- Creating a Firewall Rule
- Configuring Iptables
- Testing an Antivirus Program
- Using PuTTY
- Running a Security Scanner to Identify Vulnerabilities
- Bypassing Command Shell Restrictions
- Using Netcat for Reverse Shell

Application Security and Penetration Testing

- Attacking a Website using XSS Injection
- Conducting Cross-site Request Forgery (CSRF or XSRF) Attacks
- Using Exiftool
- Using Burpsuite
- Exploiting a Website Using SQL Injection
- Performing ARP Poisoning
- Scanning TCP Ports
- Cracking a Linux Password using the John the Ripper Tool

Risk Management

- Tracking Vulnerabilities in Software
- Reviewing Security Policy

Policies, Procedures, and Incident Response

- Using Netstat
- Using TCPdump
- Cracking Windows Password using Ophcrack

Security Controls for Communication and Collaboration

- Using the NetBus Application
- Using Social Engineering Toolkit

Here's what you get

35	35	23
LIVE LABS	VIDEO TUTORIALS	MINUTES

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.

GET IN TOUCH:

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com