uCertify

Course Outline

CompTIA Security+ (SY0-701)

05 Jul 2024

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

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

   Syllabus

   Chapter 1: Introduction

   Chapter 2: Comparing and Contrasting the Various Types of Controls

   Chapter 3: Summarizing Fundamental Security Concepts

   Chapter 4: Understanding Change Management's Security Impact

   Chapter 5: Understanding the Importance of Using Appropriate Cryptographic Solutions

   Chapter 6: Comparing and Contrasting Common Threat Actors and Motivations

   Chapter 7: Understanding Common Threat Vectors and Attack Surfaces

   Chapter 8: Understanding Various Types of Vulnerabilities

   Chapter 9: Understanding Indicators of Malicious Activity

   Chapter 10: Understanding the Purpose of Mitigation Techniques Used to Secure the Enterprise

   Chapter 11: Comparing and Contrasting Security Implications of Different Architecture Models

   Chapter 12: Applying Security Principles to Secure Enterprise Infrastructure

   Chapter 13: Comparing and Contrasting Concepts and Strategies to Protect Data

   Chapter 14: Understanding the Importance of Resilience and Recovery in Security Architecture

   Chapter 15: Applying Common Security Techniques to Computing Resources

   Chapter 16: Understanding the Security Implications of Hardware, Software, and Data Asset Management

   Chapter 17: Understanding Various Activities Associated with Vulnerability Management

   Chapter 18: Understanding Security Alerting and Monitoring Concepts and Tools

1. 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.

2. 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.

3. 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.

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

- Goals and Methods
- Who Should Read This Course?
- CompTIA Security+ Exam Topics

Chapter 2: Comparing and Contrasting the Various Types of Controls

- Control Categories
- Control Types
- Review Key Topics
- Review Questions

Chapter 3: Summarizing Fundamental Security Concepts

- Confidentiality, Integrity, and Availability (CIA)
- Non-repudiation
- Authentication, Authorization, and Accounting (AAA)
- Gap Analysis
- Zero Trust

- Physical Security
- Deception and Disruption Technology
- Review Key Topics
- Review Questions

Chapter 4: Understanding Change Management’s Security Impact

- Business Processes Impacting Security Operations
- Technical Implications
- Documentation
- Version Control
- Review Key Topics
- Review Questions

Chapter 5: Understanding the Importance of Using Appropriate Cryptographic Solutions

- Public Key Infrastructure (PKI)
- Encryption
- Transport/Communication
- Symmetric Versus Asymmetric Encryption

- Key Exchange
- Algorithms
- Key Length
- Tools
- Trusted Platform Module
- Hardware Security Module
- Key Management System
- Secure Enclave
- Obfuscation
- Steganography
- Hashing
- Salting
- Digital Signatures
- Key Stretching
- Blockchain
- Open Public Ledger
- Certificates
- Review Key Topics

- Review Questions

Chapter 6: Comparing and Contrasting Common Threat Actors and Motivations

- Threat Actors
- Attributes of Actors
- Motivations
- War
- Review Key Topics
- Review Questions

Chapter 7: Understanding Common Threat Vectors and Attack Surfaces

- Message-Based
- Image-Based
- File-Based
- Voice Call
- Removable Device
- Vulnerable Software
- Unsupported Systems and Applications

- Unsecure Networks
- Open Service Ports
- Default Credentials
- Supply Chain
- Human Vectors/Social Engineering
- Review Key Topics
- Review Questions

Chapter 8: Understanding Various Types of Vulnerabilities

- Application
- Operating System (OS)–Based
- Web-Based
- Hardware
- Virtualization
- Cloud Specific
- Supply Chain
- Cryptographic
- Misconfiguration

- Mobile Device
- Zero-Day Vulnerabilities
- Review Key Topics
- Review Questions

Chapter 9: Understanding Indicators of Malicious Activity

- Malware Attacks
- Physical Attacks
- Network Attacks
- Application Attacks
- Cryptographic Attacks
- Password Attacks
- Indicators
- Review Key Topics
- Review Questions

Chapter 10: Understanding the Purpose of Mitigation Techniques Used to Secure the Enterprise

- Segmentation

- Access Control
- Isolation
- Patching
- Encryption
- Monitoring
- Least Privilege
- Configuration Enforcement
- Decommissioning
- Hardening Techniques
- Review Key Topics
- Review Questions

Chapter 11: Comparing and Contrasting Security Implications of Different Architecture Models

- Architecture and Infrastructure Concepts
- Considerations
- Review Key Topics
- Review Questions

Chapter 12: Applying Security Principles to Secure Enterprise Infrastructure

- Infrastructure Considerations
- Secure Communication/Access
- Selection of Effective Controls
- Review Key Topics
- Review Questions

Chapter 13: Comparing and Contrasting Concepts and Strategies to Protect Data

- Data Types
- Data Classifications
- General Data Considerations
- Methods to Secure Data
- Review Key Topics
- Review Questions

Chapter 14: Understanding the Importance of Resilience and Recovery in Security Architecture

- High Availability
- Site Considerations
- Platform Diversity

- Multi-Cloud System
- Continuity of Operations
- Capacity Planning
- Testing
- Backups
- Power
- Review Key Topics
- Review Questions

Chapter 15: Applying Common Security Techniques to Computing Resources

- Secure Baselines
- Hardening Targets
- Wireless Devices
- Mobile Solutions
- Connection Methods
- Wireless Security Settings
- Application Security
- Sandboxing

- Monitoring
- Review Key Topics
- Review Questions

Chapter 16: Understanding the Security Implications of Hardware, Software, and Data Asset Management

- Acquisition/Procurement Process
- Assignment/Accounting
- Monitoring/Asset Tracking
- Disposal/Decommissioning
- Review Key Topics
- Review Questions

Chapter 17: Understanding Various Activities Associated with Vulnerability Management

- Identification Methods
- Analysis
- Vulnerability Response and Remediation
- Validation of Remediation

- Reporting
- Review Key Topics
- Review Questions

Chapter 18: Understanding Security Alerting and Monitoring Concepts and Tools

- Monitoring and Computing Resources
- Activities
- Tools
- Review Key Topics
- Review Questions

Chapter 19: Modifying Enterprise Capabilities to Enhance Security

- Firewall
- IDS/IPS
- Web Filter
- Operating System Security
- Implementation of Secure Protocols
- DNS Filtering
- Email Security

- File Integrity Monitoring
- DLP
- Network Access Control (NAC)
- Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR)
- User Behavior Analytics
- Review Key Topics
- Review Questions

Chapter 20: Implementing and Maintaining Identity and Access Management

- Provisioning/De-provisioning User Accounts
- Permission Assignments and Implications
- Identity Proofing
- Federation
- Single Sign-On (SSO)
- Interoperability
- Attestation
- Access Controls
- Multifactor Authentication (MFA)

- Password Concepts
- Privileged Access Management Tools
- Review Key Topics
- Review Questions

Chapter 21: Understanding the Importance of Automation and Orchestration Related to Secure Operations

- Use Cases of Automation and Scripting
- Benefits
- Other Considerations
- Review Key Topics
- Review Questions

Chapter 22: Understanding Appropriate Incident Response Activities

- Process
- Training
- Testing
- Root Cause Analysis
- Threat Hunting

- Digital Forensics
- Review Key Topics
- Review Questions

Chapter 23: Using Data Sources to Support an Investigation

- Log Data
- Data Sources
- Review Key Topics
- Review Questions

Chapter 24: Summarizing Elements of Effective Security Governance

- Guidelines
- Policies
- Standards
- Procedures
- External Considerations
- Monitoring and Revision
- Types of Governance Structures

- Roles and Responsibilities for Systems and Data
- Review Key Topics
- Review Questions

Chapter 25: Understanding Elements of the Risk Management Process

- Risk Identification
- Risk Assessment
- Risk Analysis
- Risk Register
- Risk Tolerance
- Risk Appetite
- Risk Management Strategies
- Risk Reporting
- Business Impact Analysis
- Review Key Topics
- Review Questions

Chapter 26: Understanding the Processes Associated with Third-Party Risk Assessment and Management

- Vendor Assessment
- Vendor Selection
- Agreement Types
- Vendor Monitoring
- Questionnaires
- Rules of Engagement
- Review Key Topics
- Review Questions

Chapter 27: Summarizing Elements of Effective Security Compliance

- Compliance Reporting
- Consequences of Non-compliance
- Compliance Monitoring
- Attestation and Acknowledgment
- Privacy
- Review Key Topics
- Review Questions

Chapter 28: Understanding Types and Purposes of Audits and Assessments

- Attestation
- Internal
- External
- Penetration Testing
- Review Key Topics
- Review Questions

Chapter 29: Implementing Security Awareness Practices

- Phishing
- Anomalous Behavior Recognition
- User Guidance and Training
- Reporting and Monitoring
- Development
- Execution
- Review Key Topics
- Review Questions

Chapter 30: Final Preparation

- Hands-on Activities
- Suggested Plan for Final Review and Study
- Summary

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

Summarizing Fundamental Security Concepts

- Identifying Access Badge Areas
- Implementing Physical Security

Understanding the Importance of Using Appropriate Cryptographic Solutions

- Examining PKI Certificates
- Creating Asymmetric Key Pairs
- Using Symmetric Encryption
- Using BitLocker in Windows 10
- Performing Steganography Using OpenStego
- Encrypting Files with EFS
- Creating Certificates with OpenSSL

Understanding Common Threat Vectors and Attack Surfaces

- Scanning the Network

- Using Social Engineering Techniques to Plan an Attack

Understanding Various Types of Vulnerabilities

- Exploiting a TOCTOU Vulnerability
- Exploiting an Overflow Vulnerability
- Examining Application Vulnerabilities
- Performing SQL Injection in DVWA
- Performing an XSS Attack in DVWA
- Detecting Virtualization

Understanding Indicators of Malicious Activity

- Opening OWASP ZAP and Starting Brute Force Attack
- Examining Spyware
- Spoofing a MAC Address with SMAC
- Launching a DoS Attack
- Observing an MD5-Generated Hash Value
- Conducting a Cross-Site Request Forgery Attack
- Cracking Passwords
- Cracking a Linux Password Using John the Ripper

Understanding the Purpose of Mitigation Techniques Used to Secure the Enterprise

- Using the chmod Command

Applying Security Principles to Secure Enterprise Infrastructure

- Implementing a Proxy Server
- Binding a Site Using IIS
- Configuring a VPN
- Examining Kerberos Settings

Comparing and Contrasting Concepts and Strategies to Protect Data

- Creating File Hashes

Understanding the Importance of Resilience and Recovery in Security Architecture

- Gathering Site Information
- Scheduling a Server Backup

Applying Common Security Techniques to Computing Resources

- Enforcing a Security Template
- Enforcing Password Policies
- Installing a RADIUS Server

Understanding Security Alerting and Monitoring Concepts and Tools

- Conducting Vulnerability Scanning Using Nessus
- Consulting a Vulnerability Database

Modifying Enterprise Capabilities to Enhance Security

- Configuring a Network Firewall

Implementing and Maintaining Identity and Access Management

- Examining Active Directory Objects

Understanding Appropriate Incident Response Activities

- Examining MITRE ATT&CK
- Completing the Chain of Custody

Using Data Sources to Support an Investigation

- Viewing Linux Event Logs
- Viewing Windows Event Logs
- Capturing Credentials On-Path

Summarizing Elements of Effective Security Governance

- Cracking Passwords Using Rainbow Tables

Understanding Types and Purposes of Audits and Assessments

- Using the theHarvester Tool

Implementing Security Awareness Practices

- Using Anti-Phishing Tools

Here's what you get

48	48	01:48
LIVE LABS	VIDEO TUTORIALS	HOURS

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