uCertify

Course Outline

CompTIA Security (SY0-601)

13 Jul 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: Today's Security Professional

   Chapter 3: Cybersecurity Threat Landscape

   Chapter 4: Malicious Code

   Chapter 5: Social Engineering, Physical, and Password Attacks

   Chapter 6: Security Assessment and Testing

   Chapter 7: Secure Coding

   Chapter 8: Cryptography and the Public Key Infrastructure

   Chapter 9: Identity and Access Management

   Chapter 10: Resilience and Physical Security

   Chapter 11: Cloud and Virtualization Security

   Chapter 12: Endpoint Security

   Chapter 13: Network Security

   Chapter 14: Wireless and Mobile Security

   Chapter 15: Incident Response

   Chapter 16: Digital Forensics

   Chapter 17: Security Policies, Standards, and Compliance

   Chapter 18: Risk Management and Privacy

1. Course Objective

Gain hands-on experience to pass the CompTIA Security+ certification exam with the CompTIA Security+ (SY0-601) course and lab. Interactive chapters and hands-on labs comprehensively cover the SY0-601 exam objectives and provide knowledge in areas such as security concepts, operating systems, application systems, and many more. The CompTIA Security+ study guide will help you get a full understanding of the challenges you'll face as a security professional.

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

- The Security+ Exam
- What Does This Course Cover?
- Exam SY0-601 Exam Objectives

- SY0-601 Certification Exam Objective Map

Chapter 2: Today's Security Professional

- Cybersecurity Objectives
- Data Breach Risks
- Implementing Security Controls
- Data Protection
- Summary
- Exam Essentials

Chapter 3: Cybersecurity Threat Landscape

- Exploring Cybersecurity Threats
- Threat Data and Intelligence
- Summary
- Exam Essentials

Chapter 4: Malicious Code

- Malware
- Malicious Code

- Adversarial Artificial Intelligence
- Summary
- Exam Essentials

Chapter 5: Social Engineering, Physical, and Password Attacks

- Social Engineering
- Password Attacks
- Physical Attacks
- Summary
- Exam Essentials

Chapter 6: Security Assessment and Testing

- Vulnerability Management
- Security Vulnerabilities
- Penetration Testing
- Training and Exercises
- Summary
- Exam Essentials

Chapter 7: Secure Coding

- Software Assurance Best Practices
- Designing and Coding for Security
- Software Security Testing
- Injection Vulnerabilities
- Exploiting Authentication Vulnerabilities
- Exploiting Authorization Vulnerabilities
- Exploiting Web Application Vulnerabilities
- Application Security Controls
- Secure Coding Practices
- Summary
- Exam Essentials

Chapter 8: Cryptography and the Public Key Infrastructure

- An Overview of Cryptography
- Goals of Cryptography
- Cryptographic Concepts
- Modern Cryptography

- Symmetric Cryptography
- Asymmetric Cryptography
- Hash Functions
- Digital Signatures
- Public Key Infrastructure
- Asymmetric Key Management
- Cryptographic Attacks
- Emerging Issues in Cryptography
- Summary
- Exam Essentials

Chapter 9: Identity and Access Management

- Identity
- Authentication and Authorization
- Authentication Methods
- Accounts
- Access Control Schemes
- Summary

- Exam Essentials

Chapter 10: Resilience and Physical Security

- Building Cybersecurity Resilience
- Response and Recovery Controls
- Physical Security Controls
- Summary
- Exam Essentials

Chapter 11: Cloud and Virtualization Security

- Exploring the Cloud
- Virtualization
- Cloud Infrastructure Components
- Cloud Security Issues
- Cloud Security Controls
- Summary
- Exam Essentials

Chapter 12: Endpoint Security

- Protecting Endpoints
- Service Hardening
- Operating System Hardening
- Securing Embedded and Specialized Systems
- Summary
- Exam Essentials

Chapter 13: Network Security

- Designing Secure Networks
- Secure Protocols
- Attacking and Assessing Networks
- Network Reconnaissance and Discovery Tools and Techniques
- Summary
- Exam Essentials

Chapter 14: Wireless and Mobile Security

- Building Secure Wireless Networks
- Managing Secure Mobile Devices

- Understanding Policy Documents
- Personnel Management
- Third-Party Risk Management
- Complying with Laws and Regulations
- Adopting Standard Frameworks
- Security Control Verification and Quality Control
- Summary
- Exam Essentials

Chapter 18: Risk Management and Privacy

- Analyzing Risk
- Managing Risk
- Risk Analysis
- Disaster Recovery Planning
- Privacy
- Summary
- Exam Essentials

12. 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.

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

Malicious Code

- Identifying Virus Threats
- Detecting Rootkits

Social Engineering, Physical, and Password Attacks

- Using Social Engineering Techniques to Plan an Attack
- Cracking a Linux Password Using John the Ripper

Security Assessment and Testing

- Conducting Vulnerability Scanning Using Nessus

Secure Coding

- Exploiting a Website Using SQL Injection
- Conducting a Cross-Site Request Forgery Attack
- Attacking a Website Using XSS Injection
- Defending Against a Buffer Overflow Attack

Cryptography and the Public Key Infrastructure

- Performing Symmetric Encryption
- Examining Asymmetric Encryption
- Observing an SHA-Generated Hash Value

- Observing an MD5-Generated Hash Value
- Examining PKI Certificates
- Using Rainbow Tables to Crack Passwords

Identity and Access Management

- Examining Kerberos Settings
- Installing a RADIUS Server

Resilience and Physical Security

- Configuring RAID 5

Endpoint Security

- Using the chmod Command
- Examining File Manipulation Commands

Network Security

- Configuring a Standard ACL
- Implementing Port Security
- Configuring a BPDU Guard on a Switch Port
- Configuring VLANs
- Using Windows Firewall
- Performing ARP Poisoning
- Using the ifconfig Command
- Using the traceroute Command
- Capturing Packets Using Wireshark
- Performing Reconnaissance on a Network
- Using the theHarvester Tool to Gather Information about a Victim
- Using the hping Program
- Using Reconnaissance Tools

Incident Response

- Viewing Linux event logs

- Using Event Viewer
- Making Syslog Entries Readable

Digital Forensics

- Using FTK Imager

Security Policies, Standards, and Compliance

- Configuring a Password Policy

Here's what you get

38

LIVE LABS

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