uCertify

Course Outline

CompTIA Security+ (SY0-601)

26 Apr 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: Comparing and Contrasting Different Types of Social Engineering Techniques

   Chapter 3: Analyzing Potential Indicators to Determine the Type of Attack

   Chapter 4: Analyzing Potential Indicators Associated with Application Attacks

   Chapter 5: Analyzing Potential Indicators Associated with Network Attacks

   Chapter 6: Understanding Different Threat Actors, Vectors, and Intelligence Sources

   Chapter 7: Understanding the Security Concerns Associated with Various Types of Vulnerabilities

   Chapter 8: Summarizing the Techniques Used in Security Assessments

   Chapter 9: Understanding the Techniques Used in Penetration Testing

   Chapter 10: Understanding the Importance of Security Concepts in an Enterprise Environment

   Chapter 11: Summarizing Virtualization and Cloud Computing Concepts

   Chapter 12: Summarizing Secure Application Development, Deployment, and Automation Concepts

   Chapter 13: Summarizing Authentication and Authorization Design Concepts

   Chapter 14: Implementing Cybersecurity Resilience

   Chapter 15: Understanding the Security Implications of Embedded and Specialized Systems

   Chapter 16: Understanding the Importance of Physical Security Controls

Here's what you get

11. Post-Assessment

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

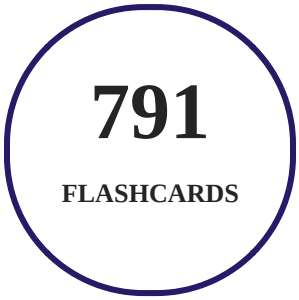
There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

4. 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.

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

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

Chapter 2: Comparing and Contrasting Different Types of Social Engineering Techniques

- Social Engineering Fundamentals
- User Security Awareness Education
- Review Key Topics

Chapter 3: Analyzing Potential Indicators to Determine the Type of Attack

- Malicious Software (Malware)
- Password Attacks
- Physical Attacks
- Adversarial Artificial Intelligence
- Supply-Chain Attacks
- Cloud-based vs. On-premises Attacks
- Cryptographic Attacks
- Review Key Topics

Chapter 4: Analyzing Potential Indicators Associated with Application Attacks

- Privilege Escalation

- Cross-Site Scripting (XSS) Attacks
- Injection Attacks
- Pointer/Object Dereference
- Directory Traversal
- Buffer Overflows
- Race Conditions
- Error Handling
- Improper Input Handling
- Replay Attacks
- Request Forgeries
- Application Programming Interface (API) Attacks
- Resource Exhaustion
- Memory Leaks
- Secure Socket Layer (SSL) Stripping
- Driver Manipulation
- Pass the Hash
- Review Key Topics

Chapter 5: Analyzing Potential Indicators Associated with Network Attacks

- Wireless Attacks
- On-Path Attacks
- Layer 2 Attacks
- Domain Name System (DNS) Attacks
- Distributed Denial-of-Service (DDoS) Attacks
- Malicious Code or Script Execution Attacks
- Review Key Topics

Chapter 6: Understanding Different Threat Actors, Vectors, and Intelligence Sources

- Actors and Threats
- Attributes of Threat Actors
- Attack Vectors
- Threat Intelligence and Threat Intelligence Sources
- Research Sources
- Review Key Topics

Chapter 7: Understanding the Security Concerns Associated with Various Types of Vulnerabilities

- Cloud-based vs. On-premises Vulnerabilities

- Zero-day Vulnerabilities
- Weak Configurations
- Third-party Risks
- Improper or Weak Patch Management
- Legacy Platforms
- The Impact of Cybersecurity Attacks and Breaches
- Review Key Topics

Chapter 8: Summarizing the Techniques Used in Security Assessments

- Threat Hunting
- Vulnerability Scans
- Logs and Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)
- Review Key Topics

Chapter 9: Understanding the Techniques Used in Penetration Testing

- Penetration Testing
- Passive and Active Reconnaissance

- Exercise Types
- Review Key Topics

Chapter 10: Understanding the Importance of Security Concepts in an Enterprise Environment

- Configuration Management
- Data Sovereignty and Data Protection
- Site Resiliency
- Deception and Disruption
- Review Key Topics

Chapter 11: Summarizing Virtualization and Cloud Computing Concepts

- Cloud Models
- Cloud Service Providers
- Cloud Architecture Components
- Virtual Machine (VM) Sprawl Avoidance and VM Escape Protection
- Review Key Topics

Chapter 12: Summarizing Secure Application Development, Deployment, and Automation Concepts

- Software Development Environments and Methodologies
- Application Provisioning and Deprovisioning
- Software Integrity Measurement
- Secure Coding Techniques
- Open Web Application Security Project (OWASP)
- Software Diversity
- Automation/Scripting
- Elasticity and Scalability
- Review Key Topics

Chapter 13: Summarizing Authentication and Authorization Design Concepts

- Authentication Methods
- Biometrics
- Multifactor Authentication (MFA) Factors and Attributes
- Authentication, Authorization, and Accounting (AAA)
- Cloud vs. On-premises Requirements
- Review Key Topics

Chapter 14: Implementing Cybersecurity Resilience

- Redundancy
- Replication
- On-premises vs. Cloud
- Backup Types
- Non-persistence
- High Availability
- Restoration Order
- Diversity
- Review Key Topics

Chapter 15: Understanding the Security Implications of Embedded and Specialized Systems

- Embedded Systems
- Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS)
- Internet of Things (IoT)
- Specialized Systems
- Voice over IP (VoIP)
- Heating, Ventilation, and Air Conditioning (HVAC)

- Drones
- Multifunction Printers (MFP)
- Real-Time Operating Systems (RTOS)
- Surveillance Systems
- System on a Chip (SoC)
- Communication Considerations
- Embedded System Constraints
- Review Key Topics

Chapter 16: Understanding the Importance of Physical Security Controls

- Bollards/Barricades
- Access Control Vestibules
- Badges
- Alarms
- Signage
- Cameras
- Closed-Circuit Television (CCTV)
- Industrial Camouflage

- Personnel
- Locks
- USB Data Blockers
- Lighting
- Fencing
- Fire Suppression
- Sensors
- Drones
- Visitor Logs
- Faraday Cages
- Air Gap
- Screened Subnet (Previously Known as Demilitarized Zone [DMZ])
- Protected Cable Distribution
- Secure Areas
- Secure Data Destruction
- Review Key Topics

Chapter 17: Summarizing the Basics of Cryptographic Concepts

- Digital Signatures
- Key Length
- Key Stretching
- Salting
- Hashing
- Key Exchange
- Elliptic-Curve Cryptography
- Perfect Forward Secrecy
- Quantum
- Post-Quantum
- Ephemeral
- Modes of Operation
- Blockchain
- Cipher Suites
- Symmetric vs. Asymmetric Encryption
- Lightweight Cryptography
- Steganography
- Homomorphic Encryption

- Common Use Cases
- Limitations
- Review Key Topics

Chapter 18: Implementing Secure Protocols

- Protocols
- Use Cases
- Review Key Topics

Chapter 19: Implementing Host or Application Security Solutions

- Endpoint Protection
- Antimalware
- Next-Generation Firewall
- Host-based Intrusion Prevention System
- Host-based Intrusion Detection System
- Host-based Firewall
- Boot Integrity
- Database

- Application Security
- Hardening
- Self-Encrypting Drive/Full-Disk Encryption
- Hardware Root of Trust
- Trusted Platform Module
- Sandboxing
- Review Key Topics

Chapter 20: Implementing Secure Network Designs

- Load Balancing
- Network Segmentation
- Virtual Private Network
- DNS
- Network Access Control
- Out-of-Band Management
- Port Security
- Network Appliances
- Access Control List

- Route Security
- Quality of Service
- Implications of IPv6
- Port Spanning/Port Mirroring
- Monitoring Services
- File Integrity Monitors
- Review Key Topics

Chapter 21: Installing and Configuring Wireless Security Settings

- Cryptographic Protocols
- Authentication Protocols
- Methods
- Installation Considerations
- Review Key Topics

Chapter 22: Implementing Secure Mobile Solutions

- Connection Methods and Receivers
- Mobile Device Management
- Mobile Device Management Enforcement and Monitoring

- Mobile Devices
- Deployment Models
- Review Key Topics

Chapter 23: Applying Cybersecurity Solutions to the Cloud

- Cloud Security Controls
- Solutions
- Cloud Native Controls vs. Third-Party Solutions
- Review Key Topics

Chapter 24: Implementing Identity and Account Management Controls

- Identity
- Account Types
- Account Policies
- Review Key Topics

Chapter 25: Implementing Authentication and Authorization Solutions

- Authentication Management
- Authentication/Authorization

- Access Control Schemes
- Review Key Topics

Chapter 26: Implementing Public Key Infrastructure

- Public Key Infrastructure
- Types of Certificates
- Certificate Formats
- PKI Concepts
- Review Key Topics

Chapter 27: Using the Appropriate Tool to Assess Organizational Security

- Network Reconnaissance and Discovery
- File Manipulation
- Shell and Script Environments
- Packet Capture and Replay
- Forensics
- Exploitation Frameworks
- Password Crackers

- Data Sanitization
- Review Key Topics

Chapter 28: Summarizing the Importance of Policies, Processes, and Procedures for Incident Response

- Incident Response Plans
- Incident Response Process
- Exercises
- Attack Frameworks
- Stakeholder Management
- Communication Plan
- Disaster Recovery Plan
- Business Continuity Plan
- Continuity of Operations Planning (COOP)
- Incident Response Team
- Retention Policies
- Review Key Topics

Chapter 29: Using Appropriate Data Sources to Support an Investigation

- Vulnerability Scan Output
- SIEM Dashboards
- Log Files
- syslog/rsyslog/syslog-ng
- journalctl
- NXLog
- Bandwidth Monitors
- Metadata
- NetFlow/sFlow
- Protocol Analyzer Output
- Review Key Topics

Chapter 30: Applying Mitigation Techniques or Controls to Secure an Environment

- Reconfigure Endpoint Security Solutions
- Configuration Changes
- Isolation
- Containment
- Segmentation

- SOAR
- Review Key Topics

Chapter 31: Understanding the Key Aspects of Digital Forensics

- Documentation/Evidence
- Acquisition
- On-premises vs. Cloud
- Integrity
- Preservation
- E-discovery
- Data Recovery
- Nonrepudiation
- Strategic Intelligence/Counterintelligence
- Review Key Topics

Chapter 32: Comparing and contrasting the Various Types of Controls

- Control Category
- Control Types
- Review Key Topics

Chapter 33: Understanding the Importance of Applicable Regul...orks That Impact Organizational Security Posture

- Regulations, Standards, and Legislation
- Key Frameworks
- Benchmarks and Secure Configuration Guides
- Review Key Topics

Chapter 34: Understanding the Importance of Policies to Organizational Security

- Personnel Policies
- Diversity of Training Techniques
- Third-Party Risk Management
- Data Concepts
- Credential Policies
- Organizational Policies
- Review Key Topics

Chapter 35: Summarizing Risk Management Processes and Concepts

- Risk Types

- Risk Management Strategies
- Risk Analysis
- Disaster Analysis
- Business Impact Analysis
- Review Key Topics

Chapter 36: Understanding Privacy and Sensitive Data Concepts in Relation to Security

- Organizational Consequences of Privacy and Data Breaches
- Notifications of Breaches
- Data Types and Asset Classification
- PII
- PHI
- Privacy Enhancing Technologies
- Roles and Responsibilities
- Information Lifecycle
- Impact Assessment
- Terms of Agreement
- Privacy Notice

- Review Key Topics

Chapter 37: Final Preparation

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

12. Practice Test

Here's what you get

104	2	104
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

Comparing and Contrasting Different Types of Social Engineering Techniques

- Using SET
- Performing Website Reconnaissance

Analyzing Potential Indicators to Determine the Type of Attack

- Cracking a Password Using the John the Ripper Tool
- Simulating a DoS Attack
- Using Rainbow Tables
- Detecting Rootkits
- Creating a Remote Access Trojan (RAT)
- Using NetBus in Windows 10

Analyzing Potential Indicators Associated with Application Attacks

- Defending Against a Buffer Overflow Attack
- Performing Session Hijacking Using Burp Suite
- Exploiting a Website Using SQL Injection

Analyzing Potential Indicators Associated with Network Attacks

- Performing ARP Spoofing

Understanding the Techniques Used in Penetration Testing

- Identifying Search Options in Metasploit
- Using OWASP ZAP

Understanding the Importance of Security Concepts in an Enterprise Environment

- Setting Up a Honeypot

Implementing Cybersecurity Resilience

- Configuring RAID 5
- Taking an Incremental Backup
- Taking a Full Backup

Summarizing the Basics of Cryptographic Concepts

- Observing an MD5-Generated Hash Value
- Performing Symmetric Encryption
- Examining Asymmetric Encryption
- Hiding Text Using Steganography

Implementing Secure Protocols

- Configuring an SSH Server
- Configuring DNSSEC on an Active Directory Integrated Zone

- Configuring IPSec

Implementing Host or Application Security Solutions

- Configuring Inbound Rules for a Firewall
- Using Windows Firewall

Implementing Secure Network Designs

- Configuring a Tunnel Group for Clientless SSL VPN
- Configuring Clientless SSL VPNs on ASA
- Configuring Site-to-Site IPsec VPN Topology
- Performing IDS Configuration with Snort
- Using Performance Monitor
- Creating a VLAN and Viewing its Assignment to Port Mapping
- Creating a DMZ Zone
- Setting Up a VPN Server with Windows Server 2016
- Implementing Port Security
- Configuring a BPDU Guard on a Switch Port
- Configuring NetFlow and NetFlow Data Export

Implementing Secure Mobile Solutions

- Turning on Airplane Mode of an iPhone
- Setting Up a VPN in Android

Applying Cybersecurity Solutions to the Cloud

- Performing a MITM Attack

Implementing Identity and Account Management Controls

- Stopping Permissions Inheritance
- Managing NTFS Permissions
- Creating a User Account in the Active Directory

Implementing Authentication and Authorization Solutions

- Creating a Network Policy for 802.1X

Implementing Public Key Infrastructure

- Revoking and Exporting a Certificate
- Examining PKI Certificates

Using the Appropriate Tool to Assess Organizational Security

- Performing Memory Analysis with Volatility
- Using Wireshark
- Manipulating a File in Linux
- Conducting Vulnerability Scanning Using Nessus
- Using the theHarvester Tool
- Creating Reverse and Bind Shells Using Netcat
- Using the netstat Command
- Using the hping Program
- Using pathping and ping Commands
- Scanning Live Systems Using Nmap
- Using dig and nslookup Commands
- Tracing a Route Using Tracert
- Using the ifconfig Command

Using Appropriate Data Sources to Support an Investigation

- Viewing the System Logs
- Using Windows Event Viewer

Understanding the Key Aspects of Digital Forensics

- Completing the Chain of Custody
- Analyzing Forensics with Autopsy

Here's what you get

64	65	02:30
LIVE LABS	VIDEO TUTORIALS	HOURS

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