uCertify

Course Outline

CompTIA Security (Course & Lab)



29 Mar 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: Measuring and Weighing Risk

   Chapter 2: Monitoring and Diagnosing Networks

   Chapter 3: Understanding Devices and Infrastructure

   Chapter 4: Access Control, Authentication, and Authorization

   Chapter 5: Protecting Wireless Networks

   Chapter 6: Securing the Cloud

   Chapter 7: Host, Data, and Application Security

   Chapter 8: Cryptography

   Chapter 9: Malware, Vulnerabilities, and Threats

   Chapter 10: Social Engineering and Other Foes

   Chapter 11: Security Administration

   Chapter 12: Disaster Recovery and Incident Response

   Chapter 13: Video Tutorials

   Chapter 14: Mapping Videos to CompTIA® Security+® Exam SY0-401

   Videos and How To
9. Practice Test

   Here's what you get

   Features

10. Performance Based labs
    - Lab Tasks
    - Here's what you get
11. Post-Assessment

1. Course Objective

Start preparing for CompTIA Security+ certification exam with CompTIA Security+ course and performance-based labs. Performance-based labs simulate real-world, hardware, software & command line interface environments and can be mapped to any text-book, course & training. CompTIA Security course and performance-based labs cover all the objectives of CompTIA Security+ SY0-401 exam which include the application of security controls to maintain confidentiality, integrity, and availability; identification of appropriate technologies and products; troubleshooting security events and incidents, and much more.

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.

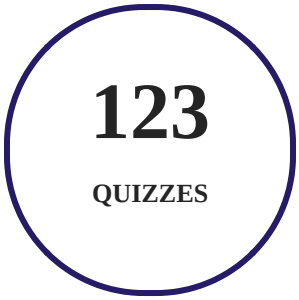
3. Exercises

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.



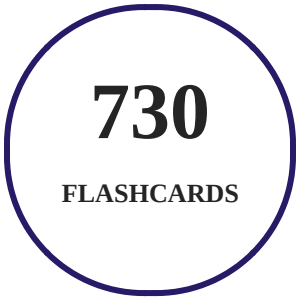
4. Quizzes

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: Measuring and Weighing Risk

- Risk Assessment
- Developing Policies, Standards, and Guidelines
- Summary

- Exam Essentials

Chapter 2: Monitoring and Diagnosing Networks

- Monitoring Networks
- Understanding Hardening
- Securing the Network
- Security Posture
- Reporting Security Issues
- Differentiating between Detection Controls and Prevention Controls
- Summary
- Exam Essentials

Chapter 3: Understanding Devices and Infrastructure

- Mastering TCP/IP
- Designing a Secure Network
- Understanding the Various Network Infrastructure Devices
- Summary
- Exam Essentials

Chapter 4: Access Control, Authentication, and Authorization

- Understanding Access Control Basics
- Understanding Remote Access Connectivity
- Understanding Authentication Services
- Understanding Access Control
- Implementing Access Controlling Best Practices
- Summary
- Exam Essentials

Chapter 5: Protecting Wireless Networks

- Working with Wireless Systems
- Understanding Wireless Devices
- Wireless Vulnerabilities to Know
- Summary
- Exam Essentials

Chapter 6: Securing the Cloud

- Working with Cloud Computing

- Working with Virtualization
- Security and the Cloud
- Summary
- Exam Essentials

Chapter 7: Host, Data, and Application Security

- Application Hardening
- Host Security
- Protecting Data Through Fault Tolerance
- Application Security
- Best Practices for Security
- Summary
- Exam Essentials

Chapter 8: Cryptography

- An Overview of Cryptography
- Modern Cryptography
- Using Cryptographic Systems
- Understanding Cryptography Standards and Protocols

- Using Public Key Infrastructure
- Summary
- Exam Essentials

Chapter 9: Malware, Vulnerabilities, and Threats

- Understanding Malware
- Surviving Viruses
- Understanding Various Types of Attacks
- Identifying Types of Application Attacks
- Tools for Finding Threats
- Summary
- Exam Essentials

Chapter 10: Social Engineering and Other Foes

- Understanding Social Engineering
- Understanding Physical Security
- Environmental Controls
- Control Types

- Data Policies
- Summary
- Exam Essentials

Chapter 11: Security Administration

- Third-Party Integration
- Understanding Security Awareness and Training
- Classifying Information
- Information Access Controls
- Complying with Privacy and Security Regulations
- Mobile Devices
- Alternative Methods to Mitigate Security Risks
- Summary
- Exam Essentials

Chapter 12: Disaster Recovery and Incident Response

- Issues Associated with Business Continuity
- Reinforcing Vendor Support
- Penetration Testing

- Summary
- Exam Essentials

Chapter 13: Video Tutorials

- Introduction
- Security Fundamentals and Controls
- Security and Risk
- Business Continuity and Load Balancing
- Threats, Vulnerabilities, and Assessment Tools
- Application, Data, and Host Security
- Access Control and Identity Management
- Security Controls and Cryptography
- Virtual Private Networks
- Conclusion

Chapter 14: Mapping Videos to CompTIA® Security+® Exam SY0-401

Videos and How To

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

48	05:47
VIDEOS	HOURS

12. Practice Test

Here's what you get

94	5	108
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. Performance Based Labs

uCertify's performance-based labs are simulators that provides virtual environment. Labs deliver hands on experience with minimal risk and thus replace expensive physical 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

- Identifying risk actions
- Identifying service associated with cloud computing
- Understanding measures of risk calculation
- Understanding key areas of policy implementation
- Identifying areas to consider for the business policy
- Downloading the Windows 7 service pack
- Identifying key aspects of standard documents
- Identifying policies
- Viewing different event details
- Viewing details of an event in Windows Server
- Viewing the current version of BIOS
- Understanding methods of OS hardening
- Installing the Web Server IIS server role
- Sharing a folder with a different user on a single computer
- Configuring NPS Accounting
- Creating a network bridge

- Deleting the web browsing history
- Understanding security posture methods
- Understanding key areas of reporting
- Understanding email protocols
- Viewing the ARP table
- Identifying TCP/IP architecture layer protocols
- Understanding application layer protocols
- Understanding Internet layer protocols
- Understanding TCP/IP protocols
- Identifying TCP ports
- Identifying ports and services
- Identifying primary areas of security topologies
- Understanding protocols
- Identifying the tunnel
- Identifying technologies to create less vulnerable networks
- Understanding the network infrastructure devices
- Spotting the intranet network
- Identifying Intrusion detection key terms
- Understanding passive responses of intrusion
- Identifying device for network connectivity
- Identifying PBX system layers
- Understanding router protocols
- Identifying sequence in which the IDS instructs the TCP to reset connections
- Understanding the network devices
- Configuring the settings in Content Advisor
- Working with a host-based IDS
- Joining SpyNet community using Windows Defender
- Scanning the computer
- Viewing the update history and details
- Identifying types of firewall
- Viewing disk configuration
- Identifying authentication protocols
- Creating a hash rule in Windows Server 2012
- Customizing group and user access with MMC
- Turning off the guest account

- Viewing the Generate Random Password screenshot
- Configuring NPS to provide RADIUS authentication
- Identifying tunneling protocols
- Configuring NPS network policy
- Understanding LDAP names
- Identifying authentication services
- Enabling the network policy server
- Identifying types of authentication services
- Identifying access control methods
- Performing XArp software installation
- Protecting a computer by blocking communications
- Blocking a connection
- Understanding evaluation assurance levels
- Configuring account time limits
- Identifying wireless protocols
- Understanding technologies used to communicate in the 802.11 standard
- Enabling LMHOSTS lookup
- Understanding WAP security levels
- Configuring wireless network settings
- Identifying cloud computing service models
- Understanding primary virtualization topics
- Editing a virtual hard disk file
- Understanding cloud models
- Identifying methods of updating an operating system
- Understanding models for improving system performance
- Configuring IE settings to avoid disruption in computer operations
- Configuring Windows firewall settings
- Downloading and installing the Avast antivirus, and scanning the system
- Installing the FTP server under the Web Server role
- Creating DNS domains
- Configuring pop-up blocker settings
- Creating a new inbound rule
- Mounting and dismounting an encrypted volume
- Identifying approaches of non-mathematical cryptography
- Identifying asymmetric algorithms

- Identifying hashing algorithm
- Understanding code-breaking techniques
- Creating a virtual volume
- Encrypting and decrypting a message
- Encrypting and decrypting a message using the RSA algorithm
- Checking the integrity of messages through MAC values
- Identifying protocols for secure connections
- Creating and backing up an encryption certificate
- Backing up an encryption certificate and key
- Viewing memory usage of programs
- Adding counters
- Encrypting a picture
- Understanding public cryptographic initiatives
- Understanding PKCS standards
- Adding the Active Directory Certificate Services role
- Understanding trust models
- Identifying the authority process
- Examining certificate details
- Examining the Microsoft Root Authority certificate details
- Understanding PKI trust models
- Installing a subordinate Certification Authority
- Enabling BitLocker
- Managing the certificate server using the mmc tool
- Identifying the filename extension
- Identifying types of malware
- Viewing the running processes of all the users
- Identifying types of viruses
- Understanding classification of viruses
- Identifying attacks
- Determining vulnerability of a network to attacks
- Identifying types of system attack
- Preventing IP address spoofing
- Understanding web-based applications
- Understanding types of application attacks
- Identifying security factors

- Identifying vulnerability scanning tasks
- Identifying social engineering attacks
- Identifying measures for spamming protection
- Identifying physical security devices
- Identifying retardants of fire extinguishers
- Identifying causes of compromised security
- Understanding information categories
- Identifying Information models
- Understanding acts to ensure privacy of information
- Understanding security measures for mobile devices
- Identifying storage mechanism
- Identifying auditing processes
- Identifying backup types
- Understanding backup plans
- Identifying various alternate site
- Identifying steps to be followed on occurrence of an incident
- Identifying SLAs measures
- Identifying ethical hacking approaches
- Performing penetration testing
- Identifying testing types

Here's what you get

141	55	44
PERFORMANCE BASED LAB	VIDEO TUTORIALS	MINUTES

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