uCertify

Course Outline

Pearson CompTIA: Security SY0-401

20 May 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:

   Chapter 2: Introduction to Security

   Chapter 3: Computer Systems Security

   Chapter 4: OS Hardening and Virtualization

   Chapter 5: Application Security

   Chapter 6: Network Design Elements

   Chapter 7: Networking Protocols and Threats

   Chapter 8: Network Perimeter Security

   Chapter 9: Securing Network Media and Devices

   Chapter 10: Physical Security and Authentication Models

   Chapter 11: Access Control Methods and Models

   Chapter 12: Vulnerability and Risk Assessment

   Chapter 13: Monitoring and Auditing

   Chapter 14: Encryption and Hashing Concepts

   Chapter 15: PKI and Encryption Protocols

   Chapter 16: Redundancy and Disaster Recovery

   Chapter 17: Policies, Procedures, and People

   Chapter 18: Taking the Real Exam

1. Course Objective

Gain hands-on expertise in CompTIA Security+ certification exam by Pearson CompTIA: Security+ SY0-401 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. Pearson CompTIA: Security+ SY0-401 course and performance-based labs cover all the objectives of CompTIA Security+ SY0-401 exam which include the application of security controls to identify risk, participate in risk mitigation activities, provide infrastructure, information, operational, and application security.

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. 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:

Chapter 2: Introduction to Security

- Security 101
- Think Like a Hacker
- Chapter Review Activities

Chapter 3: Computer Systems Security

- Computer Systems Security Threats

- Implementing Security Applications
- Securing Computer Hardware, Peripherals, and Mobile Devices
- Chapter Review Activities
- Case Studies for Chapter 2

Chapter 4: OS Hardening and Virtualization

- Hardening Operating Systems
- Virtualization Technology
- Chapter Review Activities
- Case Studies for Chapter 3

Chapter 5: Application Security

- Securing the Browser
- Securing Other Applications
- Secure Programming
- Chapter Review Activities
- Case Studies for Chapter 4

Chapter 6: Network Design Elements

- Network Design
- Cloud Security and Server Defense
- Chapter Review Activities
- Case Studies for Chapter 5

Chapter 7: Networking Protocols and Threats

- Ports and Protocols
- Malicious Attacks
- Chapter Review Activities
- Case Studies for Chapter 6

Chapter 8: Network Perimeter Security

- Firewalls and Network Security
- NIDS Versus NIPS
- Chapter Review Activities
- Case Studies for Chapter 7

Chapter 9: Securing Network Media and Devices

- Securing Wired Networks and Devices

- Chapter Review Activities
- Case Studies for Chapter 8

Chapter 10: Physical Security and Authentication Models

- Physical Security
- Authentication Models and Components
- Chapter Review Activities
- Case Studies for Chapter 9

Chapter 11: Access Control Methods and Models

- Access Control Models Defined
- Rights, Permissions, and Policies
- Chapter Review Activities
- Case Studies for Chapter 10

Chapter 12: Vulnerability and Risk Assessment

- Conducting Risk Assessments
- Assessing Vulnerability with Security Tools
- Chapter Review Activities

- Case Studies for Chapter 11

Chapter 13: Monitoring and Auditing

- Monitoring Methodologies
- Using Tools to Monitor Systems and Networks
- Conducting Audits
- Chapter Review Activities
- Case Studies for Chapter 12

Chapter 14: Encryption and Hashing Concepts

- Cryptography Concepts
- Encryption Algorithms
- Hashing Basics
- Chapter Review Activities
- Case Studies for Chapter 13

Chapter 15: PKI and Encryption Protocols

- Public Key Infrastructure
- Web of Trust

- Security Protocols
- Chapter Review Activities
- Case Studies for Chapter 14

Chapter 16: Redundancy and Disaster Recovery

- Redundancy Planning
- Disaster Recovery Planning and Procedures
- Chapter Review Activities
- Case Study for Chapter 15

Chapter 17: Policies, Procedures, and People

- Environmental Controls
- Social Engineering
- Legislative and Organizational Policies
- Chapter Review Activities
- Case Studies for Chapter 16

Chapter 18: Taking the Real Exam

- Getting Ready and the Exam Preparation Checklist

- Tips for Taking the Real Exam
- Beyond the CompTIA Security+ Certification
- Case Study for Chapter 17

Chapter 19: Appendix A: Glossary

Chapter 20: Appendix B: Q&A Flash Cards

Chapter 21: Appendix C: Activities and Facts

Videos and How To

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

31	04:45
VIDEOS	HOURS

11. Practice Test

Here's what you get

105	2	100
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.  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

- Joining SpyNet community using Windows Defender
- Configuring Windows firewall settings
- Identifying types of viruses
- Identifying the filename extension
- Identifying types of malware
- Understanding classification of viruses
- Scanning the computer
- Protecting a computer by blocking communications
- Downloading and installing the Avast antivirus, and scanning the system
- Creating a new inbound rule
- Blocking a connection
- Identifying measures for spamming protection
- Identifying Intrusion detection key terms
- Understanding passive responses of intrusion
- Identifying sequence in which the IDS instructs the TCP to reset connections
- Identifying primary areas of security topologies
- Working with a host-based IDS
- Identifying causes of compromised security
- Viewing the Generate Random Password screenshot
- Enabling BitLocker
- Viewing the current version of BIOS
- Understanding security measures for mobile devices
- Identifying methods of updating an operating system
- Downloading the Windows 7 service pack
- Viewing the update history and details
- Understanding methods of OS hardening
- Sharing a folder with a different user on a single computer
- Understanding primary virtualization topics
- Editing a virtual hard disk file
- Configuring IE settings to avoid disruption in computer operations
- Configuring the settings in Content Advisor

- Customizing group and user access with MMC
- Deleting the web browsing history
- Understanding web-based applications
- Identifying ethical hacking approaches
- Understanding types of application attacks
- Understanding the network infrastructure devices
- Identifying device for network connectivity
- Identifying PBX system layers
- Understanding router protocols
- Understanding the network devices
- Identifying TCP/IP architecture layer protocols
- Understanding application layer protocols
- Understanding Internet layer protocols
- Spotting the intranet network
- Identifying technologies to create less vulnerable networks
- Identifying cloud computing service models
- Understanding cloud models
- Identifying service associated with cloud computing
- Installing the FTP server under the Web Server role
- Understanding email protocols
- Understanding TCP/IP protocols
- Identifying TCP ports
- Identifying ports and services
- Understanding protocols
- Viewing the ARP table
- Identifying types of system attack
- Identifying attacks
- Preventing IP address spoofing
- Identifying types of firewall
- Enabling LMHOSTS lookup
- Configuring wireless network settings
- Creating a network bridge
- Understanding WAP security levels
- Identifying physical security devices
- Configuring NPS Accounting

- Configuring NPS network policy
- Identifying the tunnel
- Identifying wireless protocols
- Understanding technologies used to communicate in the 802.11 standard
- Configuring NPS to provide RADIUS authentication
- Identifying authentication services
- Identifying types of authentication services
- Enabling the network policy server
- Identifying authentication protocols
- Identifying access control methods
- Turning off the guest account
- Configuring account time limits
- Identifying Information models
- Identifying risk actions
- Identifying security factors
- Understanding measures of risk calculation
- Identifying key aspects of standard documents
- Performing penetration testing
- Understanding quantitative risk assessment values
- Understanding code-breaking techniques
- Performing XArp software installation
- Identifying vulnerability scanning tasks
- Determining vulnerability of a network to attacks
- Understanding key areas of reporting
- Viewing disk configuration
- Viewing memory usage of programs
- Viewing the running processes of all the users
- Viewing details of an event in Windows Server
- Adding counters
- Understanding security posture methods
- Viewing different event details
- Checking the integrity of messages through MAC values
- Identifying approaches of non-mathematical cryptography
- Creating a virtual volume
- Mounting and dismounting an encrypted volume

- Understanding public cryptographic initiatives
- Identifying asymmetric algorithms
- Encrypting and decrypting a message
- Encrypting and decrypting a message using the RSA algorithm
- Encrypting a picture
- Understanding PKCS standards
- Identifying cryptographic attacks
- Identifying hashing algorithm
- Creating a hash rule in Windows Server 2012
- Identifying the authority process
- Examining certificate details
- Examining the Microsoft Root Authority certificate details
- Installing a subordinate Certification Authority
- Managing the certificate server using the mmc tool
- Adding the Active Directory Certificate Services role
- Creating and backing up an encryption certificate
- Backing up an encryption certificate and key
- Understanding trust models
- Understanding PKI trust models
- Identifying tunneling protocols
- Identifying protocols for secure connections
- Understanding models for improving system performance
- Identifying retardants of fire extinguishers
- Identifying social engineering attacks
- Identifying policies
- Understanding information categories
- Identifying areas to consider for the business policy

Here's what you get

128	51	25
PERFORMANCE BASED LAB	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