uCertify

Course Outline

CompTIA Security+ Lab SY0-401

Lab

03 Jun 2017

Contents

1. Course Objective

Gain hands-on expertise in CompTIA Security+ certification exam by 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+ is an entry-level, international, vendor-neutral credential designed for IT security professionals to identify risk, participate in risk mitigation activities, provide infrastructure, information, operational, and application security. CompTIA Security+ SY0-401 exam covers the foundational principles for securing a network and managing risk, access control, identity management, and cryptography.

2. 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.

3. 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.

4. 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 assignments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

5. 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 3 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

6. 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

- Configuring NPS Accounting
- Identifying types of firewall
- Understanding the network infrastructure devices
- Identifying Intrusion detection key terms
- Understanding passive responses of intrusion
- Understanding web-based applications
- 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 email protocols
- Understanding the network devices
- Configuring IE settings to avoid disruption in computer operations
- Configuring the settings in Content Advisor
- Configuring Windows firewall settings
- Identifying primary areas of security topologies
- Viewing the ARP table
- Configuring NPS network policy
- Identifying cloud computing service models
- Understanding cloud models
- Enabling LMHOSTS lookup
- Identifying TCP/IP architecture layer protocols
- Understanding application layer protocols
- Understanding Internet layer protocols
- Identifying protocols for secure connections
- Understanding TCP/IP protocols
- Identifying TCP ports

- Identifying UDP port and services
- Understanding protocols
- Identifying the tunnel
- Spotting the intranet network
- Identifying wireless protocols
- Understanding technologies used to communicate in the 802.11 standard
- Understanding WAP security levels
- Configuring wireless network settings
- Understanding key areas of policy implementation
- Viewing the current version of BIOS
- Identifying risk actions
- Identifying service associated with cloud computing
- Identifying security factors
- Identifying policies
- Understanding measures of risk calculation
- Viewing disk configuration
- Identifying key aspects of standard documents
- Understanding information categories
- Identifying Information models
- Identifying physical security devices
- Identifying retardants of fire extinguishers
- Identifying areas to consider for the business policy
- Checking the integrity of messages through MAC values
- Creating and backing up an encryption certificate
- Identifying approaches of non-mathematical cryptography
- Creating a virtual volume
- Mounting and dismounting an encrypted volume
- Backing up an encryption certificate and key
- Identifying types of viruses
- Identifying the filename extension
- Identifying types of malware
- Understanding classification of viruses
- Understanding code-breaking techniques
- Performing XArp software installation

- Identifying types of system attack
- Understanding types of access attacks
- Identifying attacks
- Preventing IP address spoofing
- Identifying cryptographic attacks
- Identifying authentication protocols
- Identifying social engineering attacks
- Determining vulnerability of a network to attacks
- Viewing memory usage of programs
- Understanding security posture methods
- Understanding key areas of reporting
- Viewing different event details
- Viewing the running processes of all the users
- Viewing details of an event in Windows Server
- Working with a host-based IDS
- Identifying causes of compromised security
- Identifying technologies to create less vulnerable networks
- Joining SpyNet community using Windows Defender
- Identifying vulnerability scanning tasks
- 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
- Performing penetration testing
- Identifying measures for spamming protection
- Identifying ethical hacking approaches
- Understanding models for improving system performance
- Identifying methods of updating an operating system
- Downloading the Windows 7 service pack
- Viewing the update history and details
- Installing the FTP server under the Web Server role
- Creating DNS domains
- Understanding security measures for mobile devices

- Understanding acts to ensure privacy of information
- Understanding methods of OS hardening
- Understanding evaluation assurance levels
- Configuring pop-up blocker settings
- Editing a virtual hard disk file
- Understanding primary virtualization topics
- Sharing a folder with a different user on a single computer
- Configuring NPS to provide RADIUS authentication
- Understanding LDAP names
- Identifying authentication services
- Identifying types of authentication services
- Enabling the network policy server
- Creating a network bridge
- Creating a hash rule in Windows Server 2012
- Identifying tunneling protocols
- Viewing the Generate Random Password screenshot
- Identifying access control methods
- Customizing group and user access with MMC
- Turning off the guest account
- Configuring account time limits
- Deleting the web browsing history
- Identifying asymmetric algorithms
- Encrypting and decrypting a message
- Enabling BitLocker
- Adding counters
- Encrypting and decrypting a message using the RSA algorithm
- Encrypting a picture
- Identifying hashing algorithm
- Understanding public cryptographic initiatives
- Understanding PKCS standards
- Installing the Web Server IIS server role
- Managing the certificate server using the mmc tool
- 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

Here's what you get

55	01:04
VIDEO TUTORIALS	HOURS

Have Any Query? We Are Happy To Help!

GET IN TOUCH:

Call: +1-415-763-6300 Email: sales@ucertify.com www.ucertify.com