uCertify

Course Outline

Cybersecurity Essentials



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: Introduction

   Chapter 2: Infrastructure Security in the Real World

   Chapter 3: Understanding Access-Control and Monitoring Systems

   Chapter 4: Understanding Video Surveillance Systems

   Chapter 5: Understanding Intrusion-Detection and Reporting Systems

   Chapter 6: Infrastructure Security: Review Questions and Hands-On Exercises

   Chapter 7: Local Host Security in the Real World

   Chapter 8: Securing Devices

   Chapter 9: Protecting the Inner Perimeter

   Chapter 10: Protecting Remote Access

   Chapter 11: Local Host Security: Review Questions and Hands-On Exercises

   Chapter 12: Local Network Security in the Real World

   Chapter 13: Networking Basics

   Chapter 14: Understanding Networking Protocols

   Chapter 15: Understanding Network Servers

   Chapter 16: Understanding Network Connectivity Devices

   Chapter 17: Understanding Network Transmission Media Security

   Chapter 18: Local Network Security: Review Questions

Chapter 19: Perimeter Security in the Real World
Chapter 20: Understanding the Environment
Chapter 21: Hiding the Private Network
Chapter 22: Protecting the Perimeter
Chapter 23: Protecting Data Moving Through the Internet
Chapter 24: Tools and Utilities
Chapter 25: Identifying and Defending Against Vulnerabilities
Chapter 26: Perimeter Security: Review Questions and Hands-On Exercises
Chapter 27: Appendix A: NIST Preliminary Cybersecurity Framework
Videos and How To
9. Practice Test
Here's what you get
Features
10. Live labs
Lab Tasks
Here's what you get
11. Post-Assessment

1. Course Objective

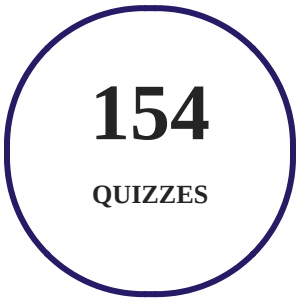
Enroll yourself in the Cybersecurity Essentials course and lab to master the concepts and methodologies being used in the field of cybersecurity. The lab provides a hands-on learning experience in a safe and online environment. The cybersecurity course and lab will help you learn the cybersecurity basics and teach you how to work with infrastructure security, network security, security devices, local network security, and access control monitoring systems.

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. 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.



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: Introduction

- Security Challenges
- Who Should Read This Course
- What Is Covered in This Course

Chapter 2: Infrastructure Security in the Real World

- Security Challenges
- Summary

Chapter 3: Understanding Access-Control and Monitoring Systems

- A Quick Primer on Infrastructure Security
- Access Control
- Security Policies
- Physical Security Controls
- Access-Control Gates
- Authentication Systems
- Remote-Access Monitoring
- Hands-On Exercises

Chapter 4: Understanding Video Surveillance Systems

- Video Surveillance Systems
- Hands-On Exercises

Chapter 5: Understanding Intrusion-Detection and Reporting Systems

- Intrusion-Detection and Reporting Systems
- Hands-On Exercises

Chapter 6: Infrastructure Security: Review Questions and Hands-On Exercises

- Summary Points
- Security Challenge Scenarios
- Review Questions

Chapter 7: Local Host Security in the Real World

- Security Challenges
- Summary

Chapter 8: Securing Devices

- The Three Layers of Security
- Securing Host Devices
- Hands-On Exercises

Chapter 9: Protecting the Inner Perimeter

- The Inner Perimeter
- Hands-On Exercises

Chapter 10: Protecting Remote Access

- Protecting Local Computing Devices

- Implementing Local Protection Tools
- Using Local Intrusion-Detection Tools
- Configuring Browser Security Options
- Defending Against Malicious Software
- Hardening Operating Systems
- Overseeing Application Software Security
- Applying Software Updates and Patches
- Hands-On Exercises

Chapter 11: Local Host Security: Review Questions and Hands-On Exercises

- Summary Points
- Security Challenge Scenarios
- Review Questions

Chapter 12: Local Network Security in the Real World

- Security Challenges
- Summary

Chapter 13: Networking Basics

- Understanding the Basics of Networking
- The OSI Networking Model
- Data Transmission Packets
- OSI Layer Security
- Network Topologies
- Logical Topologies
- Hands-On Exercises

Chapter 14: Understanding Networking Protocols

- The Basics of Networking Protocols
- Network Control Strategies
- Hands-On Exercises

Chapter 15: Understanding Network Servers

- The Basics of Network Servers
- Hands-On Exercises

Chapter 16: Understanding Network Connectivity Devices

- Network Switches

- Routers
- Gateways
- Network Bridges
- Wireless Network Connectivity
- Hands-On Exercises

Chapter 17: Understanding Network Transmission Media Security

- The Basics of Network Transmission MEDIA
- Transmission Media Vulnerabilities
- Hands-On Exercises

Chapter 18: Local Network Security: Review Questions

- Summary Points
- Security Challenge Scenarios

Chapter 19: Perimeter Security in the Real World

- Security Challenges
- Summary

Chapter 20: Understanding the Environment

- The Basics of Internet Security
- Understanding the Environment
- Hands-On Exercises

Chapter 21: Hiding the Private Network

- Understanding Private Networks
- Hands-On Exercises

Chapter 22: Protecting the Perimeter

- Understanding the Perimeter
- Firewalls
- Network Appliances
- Proxy Servers
- Demilitarized Zones (DMZs)
- Honeypots
- Extranets
- Hands-On Exercises

Chapter 23: Protecting Data Moving Through the Internet

- Securing Data in Motion
- Cryptography
- Hands-On Exercises

Chapter 24: Tools and Utilities

- Using Basic Tools
- Monitoring Tools and Software
- Hands-On Exercises

Chapter 25: Identifying and Defending Against Vulnerabilities

- Zero Day Vulnerabilities
- Software Exploits
- Social Engineering Exploits
- Network Threats and Attacks
- Dictionary Attacks
- Denial of Service (DoS) Attacks
- Spam
- Other Exploits

- Hands-On Exercises

Chapter 26: Perimeter Security: Review Questions and Hands-On Exercises

- Summary Points
- Security Scenario Review
- Review Questions

Chapter 27: Appendix A: NIST Preliminary Cybersecurity Framework

- Identify
- Protect
- Detect
- Respond
- Recover

11.  Practice Test

Here's what you get

79	83
PRE-ASSESSMENTS QUESTIONS	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.  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

Protecting the Inner Perimeter

- Converting a FAT32 Partition to NTFS Using Disk Management
- Converting a FAT32 Partition to NTFS Using PowerShell
- Converting a FAT32 Partition to FAT Using Disk Management
- Establishing a VPN Connection
- Configuring Inbound Rules for Firewall
- Establishing Lockout Policies
- Configuring Auditing in Windows
- Using BitLocker Data Encryption Tools
- Configuring Firewall Settings
- Encrypting and Decrypting a File Using AES Crypt
- Creating Folder Permissions
- Using Microsoft File Encryption Tools
- Configuring Application Control Policy
- Establishing User and Group Account
- Enabling Event Logging
- Knowing Filesystem in Linux
- Configuring Share Permissions
- Adding a Printer
- Observing the Impact of Moving an Encrypted File

Protecting Remote Access

- Setting Password Policies
- Capturing the Network Traffic Using Wireshark
- Creating a TCP Outbound Rule
- Creating an ICMP Outbound Rule

Networking Basics

- Configuring File and Share Permissions

Understanding Networking Protocols

- Assigning File or Folder Permissions
- Using the PING Command
- Configuring Advanced Permissions
- Using the nbtstat and tracert Utilities
- Using the arp and netstat Utilities
- Modifying the Command Prompt Window
- Knowing MAC, IPv4, and IPv6 addresses
- Adding a Loopback Adapter and Class A/B/C IPv4 Addresses

Understanding Network Servers

- Monitoring the Denial of Service (DoS) Attack
- Viewing the Application, Security, and System Logs
- Scanning Vulnerabilities Using Microsoft Baseline Security Analyzer
- Adding Users or Groups in a Linux Distribution

Understanding the Environment

- Examining Browsing History Options
- Configuring Pop-up Blocker Settings
- Accessing the Security Settings in Internet Explorer
- Adding a Site to a Security Zone

Hiding the Private Network

- Creating a Virtual Switch
- Checking Hyper-V Compatibility
- Enabling Hyper-V in Windows
- Pinning Hyper-V Manager to the Taskbar
- Installing a Linux Distribution in Hyper-V

Protecting Data Moving Through the Internet

- Using MD5 Hash Algorithms

Tools and Utilities

- Using the nslookup and tracert Utilities
- Capturing Packet Using Wireshark
- Scanning Network Using Nmap
- Using the ipconfig and ping Commands

Identifying and Defending Against Vulnerabilities

- Creating a New Software Restriction Policy

Here's what you get

51	51	59
LIVE LABS	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