uCertify

Course Outline

Network Defense and Countermeasures

01 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: Preface

   Chapter 2: Introduction to Network Security

   Chapter 3: Types of Attacks

   Chapter 4: Fundamentals of Firewalls

   Chapter 5: Firewall Practical Applications

   Chapter 6: Intrusion-Detection Systems

   Chapter 7: Encryption Fundamentals

   Chapter 8: Virtual Private Networks

   Chapter 9: Operating System Hardening

   Chapter 10: Defending Against Virus Attacks

   Chapter 11: Defending against Trojan Horses, Spyware, and Adware

   Chapter 12: Security Policies

   Chapter 13: Assessing System Security

   Chapter 14: Security Standards

   Chapter 15: Physical Security and Disaster Recovery

   Chapter 16: Techniques Used by Attackers

   Chapter 17: Introduction to Forensics

   Chapter 18: Cyber Terrorism

1. Course Objective

Learn about the concepts of computer network defense with the Network Defense and Countermeasures, 3e course and lab. The lab simulates real-world, hardware, software, and command-line interface environments and can be mapped to any text-book, course, or training. The Network security course completely covers the techniques and methodologies related to network defense and gives you the knowledge and practical applications of firewalls; intrusion detection systems, and 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. 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

- Classifications of Threats
- Likely Attacks
- Threat Assessment
- Understanding Security Terminology
- Choosing a Network Security Approach
- Network Security and the Law
- Using Security Resources
- Summary
- Test Your Skills

Chapter 3: Types of Attacks

- Introduction
- Understanding Denial of Service Attacks
- Defending Against Buffer Overflow Attacks
- Defending Against IP Spoofing
- Defending Against Session Hijacking
- Blocking Virus and Trojan Horse Attacks
- Summary

- Test Your Skills

Chapter 4: Fundamentals of Firewalls

- Introduction
- What Is a Firewall?
- Implementing Firewalls
- Selecting and Using a Firewall
- Using Proxy Servers
- Summary
- Test Your Skills

Chapter 5: Firewall Practical Applications

- Introduction
- Using Single Machine Firewalls
- Windows 10 Firewall
- User Account Control
- Linux Firewalls
- Using Small Office/Home Office Firewalls
- Using Medium-Sized Network Firewalls

- Using Enterprise Firewalls
- Summary
- Test Your Skills

Chapter 6: Intrusion-Detection Systems

- Introduction
- Understanding IDS Concepts
- IDS Components and Processes
- Understanding and Implementing IDSs
- Understanding and Implementing Honeypots
- Summary
- Test Your Skills

Chapter 7: Encryption Fundamentals

- Introduction
- The History of Encryption
- Learning About Modern Encryption Methods
- Identifying Good Encryption

- Understanding Digital Signatures and Certificates
- Understanding and Using Decryption
- Cracking Passwords
- Steganography
- Steganalysis
- Quantum Computing and Quantum Cryptography
- Summary
- Test Your Skills

Chapter 8: Virtual Private Networks

- Introduction
- Basic VPN Technology
- Using VPN Protocols for VPN Encryption
- IPSec
- SSL/TLS
- Implementing VPN Solutions
- Summary
- Test Your Skills

Chapter 9: Operating System Hardening

- Introduction
- Configuring Windows Properly
- Configuring Linux Properly
- Patching the Operating System
- Configuring Browsers
- Summary
- Test Your Skills

Chapter 10: Defending Against Virus Attacks

- Introduction
- Understanding Virus Attacks
- Virus Scanners
- Antivirus Policies and Procedures
- Additional Methods for Defending Your System
- What to Do If Your System Is Infected by a Virus
- Summary
- Test Your Skills

Chapter 11: Defending against Trojan Horses, Spyware, and Adware

- Introduction
- Trojan Horses
- Spyware and Adware
- Summary
- Test Your Skills

Chapter 12: Security Policies

- Introduction
- Defining User Policies
- Defining System Administration Policies
- Defining Access Control
- Defining Developmental Policies
- Summary
- Test Your Skills
- Projects

Chapter 13: Assessing System Security

- Introduction
- Risk Assessment Concepts
- Evaluating the Security Risk
- Conducting the Initial Assessment
- Probing the Network
- Vulnerabilities
- McCumber Cube
- Security Documentation
- Summary
- Test Your Skills

Chapter 14: Security Standards

- Introduction
- COBIT
- ISO Standards
- NIST Standards
- U.S. DoD Standards
- Using the Orange Book

- Using the Rainbow Series
- Using the Common Criteria
- Using Security Models
- U.S. Federal Regulations, Guidelines, and Standards
- Summary
- Test Your Skills

Chapter 15: Physical Security and Disaster Recovery

- Introduction
- Physical Security
- Disaster Recovery
- Ensuring Fault Tolerance
- Summary
- Test Your Skills

Chapter 16: Techniques Used by Attackers

- Introduction
- Preparing to Hack

- The Attack Phase
- Wi-Fi Hacking
- Summary
- Test Your Skills

Chapter 17: Introduction to Forensics

- Introduction
- General Forensics Guidelines
- FBI Forensics Guidelines
- Finding Evidence on the PC
- Gathering Evidence from a Cell Phone
- Forensic Tools to Use
- Forensic Science
- To Certify or Not to Certify?
- Summary
- Test Your Skills

Chapter 18: Cyber Terrorism

- Introduction

- Defending Against Computer-Based Espionage
- Defending Against Computer-Based Terrorism
- Choosing Defense Strategies
- Summary
- Test Your Skills

11. Practice Test

uCertify provides full length practice tests. These tests closely follow the exam objectives and are designed to simulate real exam conditions. Each course has a number of test sets consisting of hundreds of items to ensure that learners are prepared for the certification exam.

Here's what you get

100	100
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

Introduction to Network Security

- Assigning Different Classes of IP Addresses
- Viewing the MAC Address on Different Interfaces
- Understanding Protocols
- Tracing Route Using tracert
- Using the netstat Command

Types of Attacks

- Conducting a DoS Attack Using a SYN Flood
- Conducting a DoS Attack Using the Smurf Attack
- Defending Against a Buffer Overflow Attack
- Defending against IP Spoofing
- Performing Session Hijacking Using Burp Suite
- Installing Antivirus Software
- Scanning and Classifying Different Types of Viruses

Fundamentals of Firewalls

- Creating ACL in the Router
- Using Windows Firewall
- Creating a DMZ Zone

Firewall Practical Applications

- Configuring User Access Control Settings
- Configuring a Linux Firewall Using the Iptable
- Using the Cisco ASA Firewall

Intrusion-Detection Systems

- Intercepting Packets
- Configuring Snort
- Setting Up a Honeypot

Encryption Fundamentals

- Using a Symmetric Algorithm
- Using an Asymmetric Algorithm
- Observing a Digital Certificate
- Creating a PGP Certification
- Using the John the Ripper Tool
- Using Rainbow Tables

- Hiding Text Using Steganography

Virtual Private Networks

- Setting Up a VPN Server with Windows Server 2016
- Creating an L2TP VPN Using Openswan
- Configuring IPSec

Operating System Hardening

- Configuring a User Account
- Setting Security Policies
- Using Registry Editor
- Configuring the Security Setting in a Popular Browser
- Using Encryption File System
- Restricting the Null Session
- Shutting Down a Service in Windows

Defending Against Virus Attacks

- Creating a Remote Access Trojan (RAT)
- Performing Malware Scanning

Defending against Trojan Horses, Spyware, and Adware

- Using the NetBus Application
- Using eLiTeWrap
- Using an Anti-Spyware Tool

Security Policies

- Defining User Access Control
- Managing a User Using an Existing Security Policy
- Examining Security Policy
- Creating a Security Policy

Assessing System Security

- Filtering Ports Using Windows Firewall
- Using the Advanced IP Scanner
- Conducting Vulnerability Scanning Using Nessus
- Using MBSA
- Configuring Windows Update

Security Standards

- Observing the Security Event Log

Techniques Used by Attackers

- Conducting Passive Scanning Using Netcraft
- Conducting Active Scanning Using Nsauditor
- Using ShareEnum
- Performing Active Scanning Using Nmap
- Cracking Windows Password Using Ophcrack
- Performing the SQL Injection

Introduction to Forensics

- Observing the Windows Log
- Retrieving Deleted Files Using Disk Digger
- Performing Logical Imaging Using AccessData FTK Imager

Cyber Terrorism

- Using BitLocker in Windows 10
- Using EtherDetect

Here's what you get

64	64	02:17
LIVE LABS	VIDEO TUTORIALS	HOURS

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