uCertify

# Course Outline

## Practical Network Security

04 Aug 2025

www.uCertify.com

## 1. 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.

## 2. 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.

**200**

**QUIZ**

## 3. 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.

## 4. 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.

## 5. 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.

## 6. 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

## 7. 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

### Chapter 2: Basics of Information Security

- Why Information Security
- What is Information Security
- Goals
- Methods
- Tools
- Beyond Confidentiality Integrity Availability (CIA)

- Responsibility of Information Security
- Perspective of Information Security

## Chapter 3: Threat Paradigm

- Threats Paradigm
- Attackers or Threat agents
- Threat Motivation
- Threat Impact
- Types of Attacks

## Chapter 4: Information Security Controls

- Information Security Controls
- Examples of Information Security Controls

## Chapter 5: Decoding Policies Standards Procedures & Guidelines

- Documents Hierarchy
- Policy
- Standards
- Procedures and Guidelines

- Document Format
- Decoding Policies and Standards

## Chapter 6: Network Security Design

- Network Security Design Principles
- Defense in Depth
- Security Zones And Network Segmentation
- Secure Remote Access
- Secure Third Party Access
- Least Privilege
- Segregation Of Duties
- Encryption
- High Availability
- Network Access Control (NAC)
- Security Of Test Environment

## Chapter 7: Know Your Assets

- Identifying Assets

- Different Types of Assets
- Asset Responsibility
- Asset Valuation
- Asset Classification/Rating Review
- Audit Requirement

## Chapter 8: Implementing Network Security

- Introducing Assets to Production Environment
- Pre-Production Check List
- Best Practices for Network Design
- Best Practices for Firewall
- Best Practices For Router And Switches
- Best Practices for VPN
- Best Practices For Wireless Network

## Chapter 9: Secure Change Management

- Change Management
- Secure Change Management Process
- Audit Requirements

## Chapter 10: Vulnerability and Risk Management

- Vulnerability and Risk Management
- Common Vulnerabilities Found in Network Environment
- Vulnerability and Risk Management Process
- Handling Zero Day
- Audit Requirements

## Chapter 11: Access Control

- Introduction
- Identification
- Authentication
- Authorization
- Accounting
- Access Control Policies And Procedures
- Access Control Implementation
- User Registration And De-Registration
- Password Management

- Asset Classification
- Access Provisioning
- Network Admission Control (NAC)
- Privilege User Access Management
- Remote Access Management
- Third Party Access Management
- User Access Review
- Audit Requirements

## Chapter 12: Capacity Management

- Capacity Management
- Documented Policies and Procedures
- Capacity Management Process
- Audit Requirements

## Chapter 13: Log Management

- Logging
- Log Management Process and Documentation
- Log Generation

- Log Transmission
- Log Storage
- Log Analysis
- Log Disposal
- Audit Requirements

## Chapter 14: Network Monitoring

- Monitoring
- Physical, Environmental And Content Monitoring
- System Monitoring Standards and Procedures
- Traffic Monitoring
- Device Monitoring
- Log Monitoring - Security Information and Event Management
- Audit Requirements

## Chapter 15: Information Security Audit

- Information Security Audit
- Audit Management From Auditor’s Side

- Audit Management From Auditee's Side

## Chapter 16: Technical Compliance Audit

- Technical Compliance Audit
- Technical Compliance Audit from Auditor's Point of view
- Technical Compliance Audit from Auditee's Point of View
- Good Practices To Avoid Compliance Findings

## Chapter 17: Penetration Testing

- Penetration Testing (Pen Test)
- Stages of Penetration testing
- Pen-Testing vs. Vulnerability Assessment
- Pen Testing from Auditee's Point
- Good Practices to Avoid Vulnerabilities

## Chapter 18: Appendix

- Appendix 1: Vulnerability Management Sheet
- Appendix 2: Risk Management Sheet
- Appendix 3: Sample Compliance Task List

- Appendix 4: Risk Acceptance Form

# 8. Practice Test

## Here's what you get

## 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.

# 9. Performance Based Labs

uCertify's performance-based labs are Live Labs. Learn the real world skills using Live 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

- Creating a RAT
- Analyzing the WannaCry Ransomware Attack
- Examining Spyware
- Conducting Vulnerability Scanning Using Nessus
- Capturing Packets Using Wireshark
- Cracking Passwords Using Cain and Abel
- Using Rainbow Tables for Cracking Passwords
- Configuring WPA/WPA2/WPA3 for Personal and Enterprise Use
- Performing ARP Spoofing
- Configuring a Wireless AP
- Analyzing Malware Using VirusTotal
- Performing a Phishing Attack Using a SET
- Detecting Rootkits
- Simulating a DDoS Attack
- Configuring IPSec
- Configuring a Windows Firewall
- Implementing Physical Security
- Performing Symmetric and Asymmetric Encryption
- Observing an SHA-256 Generated Hash Value
- Observing an MD5-Generated Hash Value
- Examining PKI Certificates
- Using a Digital Signature
- Configuring a VPN
- Configuring Security Zones
- Implementing Least Privileged Access

- Enabling an ACL
- Assigning Different Classes of IP Addresses
- Configuring NAT
- Managing Windows Firewall Using the Control Panel
- Creating a DMZ
- Configuring a Router
- Configuring AAA for Device Access Control
- Implementing MFA on Mobile Devices
- Enforcing a Password Policy
- Disabling User Accounts
- Managing User Accounts
- Viewing and Exporting Event Logs
- Configuring Syslog and Observing the Log Settings
- Analyzing Linux Logs for Security Intelligence
- Configuring Firewall Rules and Monitoring Network Logs Using pfsense
- Monitoring the Network
- Exploiting SNMP
- Performing Reconnaissance on a Network
- Using Nmap for Network and User Enumeration
- Performing Vulnerability Scanning Using OpenVAS

## Here's what you get

**45**

**PERFORMANCE BASED LAB**

## 10. 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

**Threat Paradigm**

- Creating a RAT
- Analyzing the WannaCry Ransomware Attack
- Examining Spyware
- Conducting Vulnerability Scanning Using Nessus
- Capturing Packets Using Wireshark
- Cracking Passwords Using Cain and Abel
- Using Rainbow Tables for Cracking Passwords
- Configuring WPA/WPA2/WPA3 for Personal and Enterprise Use
- Performing ARP Spoofing
- Configuring a Wireless AP
- Analyzing Malware Using VirusTotal
- Performing a Phishing Attack Using a SET
- Detecting Rootkits
- Simulating a DDoS Attack

**Information Security Controls**

- Configuring IPSec
- Configuring a Windows Firewall
- Implementing Physical Security

- Performing Symmetric and Asymmetric Encryption
- Observing an SHA-256 Generated Hash Value
- Observing an MD5-Generated Hash Value
- Examining PKI Certificates
- Using a Digital Signature
- Configuring a VPN

**Network Security Design**

- Configuring Security Zones
- Implementing Least Privileged Access
- Enabling an ACL

**Implementing Network Security**

- Assigning Different Classes of IP Addresses
- Configuring NAT
- Managing Windows Firewall Using the Control Panel
- Creating a DMZ
- Configuring a Router
- Configuring AAA for Device Access Control

**Access Control**

- Implementing MFA on Mobile Devices
- Enforcing a Password Policy
- Disabling User Accounts
- Managing User Accounts

**Log Management**

- Viewing and Exporting Event Logs
- Configuring Syslog and Observing the Log Settings
- Analyzing Linux Logs for Security Intelligence

**Network Monitoring**

- Configuring Firewall Rules and Monitoring Network Logs Using pfsense

- Monitoring the Network
- Exploiting SNMP

**Penetration Testing**

- Performing Reconnaissance on a Network
- Using Nmap for Network and User Enumeration
- Performing Vulnerability Scanning Using OpenVAS

## Here's what you get

**45**

**LIVE LABS**

You can’t stay away! Get
in touch with our team to

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com