uCertify

Course Outline

Network Security Essentials

17 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

   Chapter 3: Symmetric Encryption and Message Confidentiality

   Chapter 4: Public-Key Cryptography and Message Authentication

   Chapter 5: Key Distribution and User Authentication

   Chapter 6: Network Access Control and Cloud Security

   Chapter 7: Transport-Level Security

   Chapter 8: Wireless Network Security

   Chapter 9: Electronic Mail Security

   Chapter 10: IP Security

   Chapter 11: Malicious Software

   Chapter 12: Intruders

   Chapter 13: Firewalls

   Chapter 14: Network Management Security

   Chapter 15: Legal and Ethical Aspects

   Chapter 16: SHA-3

   Chapter 17: Appendix A: Some Aspects of Number Theory

   Chapter 18: Appendix B: Projects for Teaching Network Security

Chapter 19: Appendix C: Standards and Standard-Setting Organizations
Chapter 20: Appendix D: TCP/IP and OSI
Chapter 21: Appendix E: Pseudorandom Number Generation
Chapter 22: Appendix F: Kerberos Encryption Techniques
Chapter 23: Appendix G: Data Compression Using ZIP
Chapter 24: Appendix H: PGP
Chapter 25: Appendix I: The International Reference Alphabet
Chapter 26: Appendix J: The Base Rate Fallacy
Chapter 27: Appendix K: Radix-64 Conversion
Chapter 28: References
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

Network Security Essentials is your key to mastering the art of securing networks and data. Whether you're a student or a professional, this course covers everything you need to know about network security. From fundamental concepts to advanced topics, you'll learn how to protect sensitive information and defend against cyber threats. With interactive lessons and hands-on labs, you'll gain practical experience that will set you on the path to becoming a network security pro. Don't just learn about network security—practice it and excel in this critical field.

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. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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

11. 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: Preface

- What’s New in the Sixth Edition
- Objectives
- Support of ACM/IEEE Computer Science Curricula 2013

- Plan of the Text
- Projects and other Student Exercises
- Relationship to Cryptography and Network Security
- Acknowledgments

Chapter 2: Introduction

- Computer Security Concepts
- The OSI Security Architecture
- Security Attacks
- Security Services
- Security Mechanisms
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- A Model for Network Security
- Standards
- Review Questions, and Problems

Chapter 3: Symmetric Encryption and Message Confidentiality

- Symmetric Encryption Principles
- Symmetric Block Encryption Algorithms
- Random and Pseudorandom Numbers
- Stream Ciphers and RC4
- Cipher Block Modes of Operation
- Review Questions, and Problems

Chapter 4: Public-Key Cryptography and Message Authentication

- Approaches to Message Authentication
- Secure Hash Functions
- Message Authentication Codes
- Public-Key Cryptography Principles
- Public-Key Cryptography Algorithms
- Digital Signatures
- Review Questions, and Problems

Chapter 5: Key Distribution and User Authentication

- Remote User Authentication Principles
- Symmetric Key Distribution Using Symmetric Encryption

- Kerberos
- Key Distribution Using Asymmetric Encryption
- X.509 Certificates
- Public-Key Infrastructure
- Federated Identity Management
- Review Questions, and Problems

Chapter 6: Network Access Control and Cloud Security

- Network Access Control
- Extensible Authentication Protocol
- IEEE 802.1X Port-Based Network Access Control
- Cloud Computing
- Cloud Security Risks and Countermeasures
- Data Protection in the Cloud
- Cloud Security as a Service
- Addressing Cloud Computing Security Concerns
- Review Questions, and Problems

Chapter 7: Transport-Level Security

- Web Security Considerations
- Transport Layer Security
- HTTPS
- Secure Shell (SSH)
- Review Questions, and Problems

Chapter 8: Wireless Network Security

- Wireless Security
- Mobile Device Security
- IEEE 802.11 Wireless LAN Overview
- IEEE 802.11i Wireless LAN Security
- Review Questions, and Problems

Chapter 9: Electronic Mail Security

- Internet Mail Architecture
- E-mail Formats
- E-mail Threats and Comprehensive E-mail Security
- S/MIME

- Pretty Good Privacy
- DNSSEC
- DNS-Based Authentication of Named Entities
- Sender Policy Framework
- Domainkeys Identified Mail
- Domain-Based Message Authentication, Reporting, and Conformance
- Review Questions, and Problems

Chapter 10: IP Security

- Ip Security Overview
- Ip Security Policy
- Encapsulating Security Payload
- Combining Security Associations
- Internet Key Exchange
- Cryptographic Suites
- Review Questions, And Problems

Chapter 11: Malicious Software

- Types of Malicious Software (Malware)

- Advanced Persistent Threat
- Propagation—Infected Content—Viruses
- Propagation—Vulnerability Exploit—Worms
- Propagation—Social Engineering—Spam e-mail, Trojans
- Payload—System Corruption
- Payload—Attack Agent—Zombie, Bots
- Payload—Information Theft—Keyloggers, Phishing, Spyware
- Payload—Stealthing—Backdoors, Rootkits
- Countermeasures
- Distributed Denial of Service Attacks
- Review Questions, and Problems

Chapter 12: Intruders

- Intruders
- Intrusion Detection
- Password Management
- Review Questions, and Problems

Chapter 13: Firewalls

- The Need for Firewalls
- Firewall Characteristics and Access Policy
- Types of Firewalls
- Firewall Basing
- Firewall Location and Configurations
- Review Questions, and Problems

Chapter 14: Network Management Security

- Basic Concepts of SNMP
- SNMPv1 Community Facility
- SNMPv3
- Recommended Reading
- References
- Review Questions, and Problems

Chapter 15: Legal and Ethical Aspects

- Cybercrime and Computer Crime
- Intellectual Property

- Privacy
- Ethical Issues
- Recommended Reading
- References
- Review Questions, and Problems

Chapter 16: SHA-3

- The Origins of SHA-3
- Evaluation Criteria for SHA-3
- The Sponge Construction
- The SHA-3 Iteration Function f
- Recommended Reading and Referencess
- Review Questions, and Problems

Chapter 17: Appendix A: Some Aspects of Number Theory

- Prime and Relatively Prime Numbers
- Modular Arithmetic

Chapter 18: Appendix B: Projects for Teaching Network Security

- Research Projects
- Hacking Project
- Programming Projects
- Laboratory Exercises
- Practical Security Assessments
- Firewall Projects
- Case Studies
- Writing Assignments
- Reading/Report Assignments

Chapter 19: Appendix C: Standards and Standard-Setting Organizations

- The Importance of Standards
- Internet Standards and the Internet Society
- The National Institute of Standards and Technology
- The International Telecommunication Union
- The International Organization for Standardization
- Significant Security Standards and Documents

Chapter 20: Appendix D: TCP/IP and OSI

- Protocols And Protocol Architectures
- The TCP/IP Protocol Architecture
- The Role Of An Internet Protocol
- IPV4
- IPV6
- The OSI Protocol Architecture

Chapter 21: Appendix E: Pseudorandom Number Generation

- Prng Requirements
- Pseudorandom Number Generation Using a Block Cipher
- Pseudorandom Number Generation Using Hash Functions and MACs

Chapter 22: Appendix F: Kerberos Encryption Techniques

- Password-To-Key Transformation
- Propagating Cipher Block Chaining Mode

Chapter 23: Appendix G: Data Compression Using ZIP

- Compression Algorithm
- Decompression Algorithm

Chapter 24: Appendix H: PGP

- Notation
- Operational Description
- Cryptographic Keys And Key Rings
- Public-Key Management
- Pgp Random Number Generation

Chapter 25: Appendix I: The International Reference Alphabet

Chapter 26: Appendix J: The Base Rate Fallacy

- Conditional Probability and Independence
- Bayes' Theorem
- The Base-Rate Fallacy Demonstrated
- References

Chapter 27: Appendix K: Radix-64 Conversion

Chapter 28: References

12. Practice Test

Here's what you get

3	5
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.

13. 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

Symmetric Encryption and Message Confidentiality

- Configuring a Wireless AP
- Establishing a SSH Connection
- Observing a SHA256-Generated Hash Value
- Examining Asymmetric Encryption
- Observing an MD5-Generated Hash Value
- Generating a Symmetric Key
- Performing Symmetric Encryption

Key Distribution and User Authentication

- Examining Kerberos Settings
- Examining PKI Certificates

Wireless Network Security

- Exploiting SNMP
- Securing a Wi-Fi Hotspot
- Creating a Network Policy for 802.1X
- Using a Wireless AP for MAC Address Filtering

Electronic Mail Security

- Configuring DNS Information

IP Security

- Configuring an IPsec Policy

Malicious Software

- Creating a Remote Access Trojan (RAT)
- Installing Antivirus Software
- Configuring IPSec
- Testing an Antivirus Program
- Simulating a DoS Attack
- Simulating a DDoS Attack

Intruders

- Understanding Local Privilege Escalation
- Setting Up a Honeypot

Firewalls

- Using Windows Firewall
- Whitelisting an IP Address in the Windows Firewall
- Creating Outbound and Inbound Rules for a Firewall

Network Management Security

- Configuring SNMPv2c
- Configuring SNMPv3

Here's what you get

28	28	01:07
LIVE LABS	VIDEO TUTORIALS	HOURS

14. 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