uCertify

Course Outline

Mastering Network Forensics

04 Aug 2025

9. Live labs

    Lab Tasks

    Here's what you get

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. 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.

40

EXERCISES

3. 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.

100

QUIZ

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.

50

FLASHCARDS

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.

50

GLOSSARY OF 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

Chapter 2: Foundations of Network Forensics

- Introduction
- Types of network forensics
- Setting up the environment for analysis
- Case study: Suspicious Web Server
- Conclusion
- Long questions

Chapter 3: Protocols and Deep Packet Analysis

- Introduction
- The OSI model
- The TCP/IP model
- The Packet structure
- Case study: Curious case of protocol misuse
- Deep Packet Inspection
- Case study: Investigating Distributed Denial of service attacks
- Conclusion
- Long questions

Chapter 4: Flow Analysis versus Packet Analysis

- Introduction
- Statistical Flow analysis
- Flow Record and FRP Systems
- Uniflow and BitFlow
- Types of Sensor deployment

- Flow analysis
- Conclusion
- Long questions

Chapter 5: Conducting Log Analysis

- Introduction
- Investigating Remote Login attempts on SSH
- Investigating Web Server Attacks with Splunk
- Investigating Proxy Logs
- Conclusion
- Long questions

Chapter 6: Wireless Forensics

- Introduction
- Basics of Radio Frequency Monitoring
- The 802.11 standard
- Evidence types in wireless local area networking
- Other wireless attacks and their analysis
- Conclusion

- Long questions

Chapter 7: TLS Decryption and Visibility

- Introduction
- Techniques to decrypt SSL/TLS communication
- Examining SSL/TLS traffic using proxy
- Conclusion
- Long questions

Chapter 8: Demystifying Covert Channels

- Introduction
- Identifying covert communication using proxies
- Using MitmProxy to decrypt Dropbox traffic
- Using Dropbox API to gather attack details
- Uncovering the attack pattern
- Uncovering DNS misuse
- Conclusion
- Long questions

- Investigating Meterpreter Reverse Shell
- Investigating Meterpreter Stageless Reverse Shell
- Conclusion
- Long questions

Chapter 14: Investigating Attacks on Email Servers

- Introduction
- Analysis of ProxyLogon attack
- Investigating Email authentication logs
- Conclusion
- Long questions

Chapter 15: Investigating Web Server Attacks

- Introduction
- Web Server attack analysis
- Conclusion
- Long questions

11. 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.

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

Foundations of Network Forensics

- Capturing Network Packets Using TCPDump
- Performing Network Analysis Using Wireshark

Protocols and Deep Packet Analysis

- Using tshark to Filter Data from a PCAP File

Flow Analysis versus Packet Analysis

- Generating IPFIX from PCAP
- Analyzing SiLK Flow Records

Conducting Log Analysis

- Investigating SSH Logs

TLS Decryption and Visibility

- Capturing Browser Requests Using mitmproxy

Demystifying Covert Channels

- Resolving IP Addresses for Network Analysis
- Investigating DNS Misuse

Automating Network Forensics

- Performing IP Reputation Analysis

Backtracking Malware

- Monitoring a TeamViewer Session
- Investigating AnyDesk Sessions

Investigating Ransomware Attacks

- Analyzing the WannaCry Ransomware Attack

Investigating Command and Control Systems

- Investigating the Metasploit Reverse Shell

Investigating Attacks on Email Servers

- Investigating the ProxyLogon Attack

Here's what you get

15

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