uCertify

Course Outline

Ethical Hacking Training: Beginner To Advanced Specialization

04 Aug 2025

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.

596

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.

312

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.

251

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.

251

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

- Goals and Methods
- Who Should Read This Course?
- Strategies for Exam Preparation
- How This Course Is Organized

Chapter 2: An Introduction to Ethical Hacking

- Security Fundamentals
- Security Testing

Chapter 3: The Technical Foundations of Hacking

- Exercises

Chapter 4: Footprinting, Reconnaissance, Scanning and Enumeration

- Footprinting
- Scanning
- Summary
- Review All Key Topics
- Exercises

Chapter 5: Enumeration and System Hacking and Attack Techniques

- Enumeration
- System Hacking Phases and Attack Techniques
- Establishing persistence
- Summary
- Review All Key Topics
- Exercise

Chapter 6: Social Engineering, Malware Threats, and Vulnerability Analysis

- Social Engineering

- Cloud Security
- IoT
- Botnets
- Summary
- Review All Key Topics

11. Practice Test

Here's what you get

125
PRE-ASSESSMENTS QUESTIONS

2
FULL LENGTH TESTS

125
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

An Introduction to Ethical Hacking

- Taking a Full Backup
- Taking an Incremental Backup
- Examining Security Policies
- Searching for Exposed Passwords

The Technical Foundations of Hacking

- Examining MITRE ATT&CK
- Analyzing Captured Packets Using a Sniffer
- Using the tracert Command

Footprinting, Reconnaissance, Scanning and Enumeration

- Performing Passive and Active Reconnaissance
- Using the whois Program
- Footprinting a Website
- Using the curl Command
- Performing Nmap Scanning

Enumeration and System Hacking and Attack Techniques

- Performing Enumeration Using enum4linux, nbtscan, and Nmap Scripts
- Converting an NTFS Partition to FAT32
- Managing NTFS Permissions
- Detecting Rootkits
- Viewing Syslog for Monitoring Logs
- Cracking a Linux Password Using John the Ripper
- Cracking Passwords Using Cain and Abel

Social Engineering, Malware Threats, and Vulnerability Analysis

- Performing a Phishing Attack
- Using Process Explorer
- Analyzing Malware Using MetaDefender
- Analyzing Malware Using VirusTotal
- Generating SHA
- Analyzing the WannaCry Ransomware Attack
- Creating RAT
- Understanding Keyloggers and Spyware
- Using the Windows Defender Antivirus
- Performing Vulnerability Scanning Using OpenVAS
- Conducting Vulnerability Scanning using Nessus

Sniffers, Session Hijacking, and Denial of Service

- Configuring DHCP Snooping

- Using TCPdump to Capture Packets
- Performing ARP Spoofing
- Spoofing a MAC Address
- Performing Session Hijacking Using Burp Suite
- Simulating a DDoS Attack

Web Server Hacking, Web Applications, and Database Attacks

- Exploring ExploitDB and GHDB
- Performing a Client-Side Attack Using BeEF
- Fuzzing Using OWASP ZAP
- Exploiting Windows 7 Using Metasploit
- Grabbing a Screenshot of a Target Machine Using Metasploit
- Defending Against a Buffer Overflow Attack
- Conducting a Cross-Site Request Forgery Attack
- Attacking a Website Using XSS Injection
- Performing SQL Injection in DVWA

Wireless Technologies, Mobile Security, and Attacks

- Setting a Secure Passcode on iPhone
- Setting a Data-Usage Limit
- Installing App and Configuring Permissions Settings
- Performing Factory Reset on a Android Phone
- Connecting a Printer to a Laptop via Bluetooth
- Connecting an iPhone to a Laptop via Bluetooth
- Connecting an iPhone to Wi-Fi
- Implementing MFA on Mobile Devices
- Updating iPhone iOS and Security Patches
- Creating a Home Wireless Network
- Securing a Wi-Fi Hotspot

Evading IDS, Firewalls, and Honeypots

- Implementing IDS and IPS
- Using the Hping Tool

- Configuring NAT
- Configuring a Network Firewall
- Setting Up a Honeypot

Cryptographic Attacks and Countermeasures

- Encrypting and Decrypting a File Using OpenSSL
- Performing Symmetric and Asymmetric Encryption
- Adding a Digital Certificate
- Examining PKI Certificates
- Implementing PGP for Secure Email and File Encryption
- Using a Digital Signature
- Hiding Text using Steganography
- Observing an MD5-Generated Hash Value
- Observing a SHA256-Generated Hash Value

Cloud Computing, IoT, and Botnets

- Creating a CI/CD Pipeline
- Creating an IoT Hub in Azure

Here's what you get

72

LIVE LABS

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.

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