uCertify

Course Outline

Certified Ethical Hacker Version 9

18 Apr 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: Introduction

   Chapter 2: An Introduction to Ethical Hacking

   Chapter 3: The Technical Foundations of Hacking

   Chapter 4: Footprinting and Scanning

   Chapter 5: Enumeration and System Hacking

   Chapter 6: Malware Threats

   Chapter 7: Sniffers, Session Hijacking, and Denial of Service

   Chapter 8: Web Server Hacking, Web Applications, and Database Attacks

   Chapter 9: Wireless Technologies, Mobile Security, and Attacks

   Chapter 10: IDS, Firewalls, and Honeypots

   Chapter 11: Physical Security and Social Engineering

   Chapter 12: Cryptographic Attacks and Defenses

   Chapter 13: Cloud Computing and Botnets

   Chapter 14: Final Preparation

   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

Prepare for the EC-Council CEH 312-50 exam with the Certified Ethical Hacker Version 9 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 course and lab cover CEH 312-50 exam objectives and include topics such as ethical hacking, technical foundations of hacking, footprinting, and scanning; and more. The labs also provide you with the tools and techniques used by hackers to break into an organization.

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. 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.

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: Introduction

- How to Use This Book
- Goals and Methods
- Who Should Read This Book?

- Strategies for Exam Preparation
- How This Book Is Organized

Chapter 2: An Introduction to Ethical Hacking

- Security Fundamentals
- Security Testing
- Hacker and Cracker Descriptions
- Ethical Hackers
- Test Plans—Keeping It Legal
- Ethics and Legality
- Summary
- Review All Key Topics
- Hands-On Labs
- Suggested Reading and Resources

Chapter 3: The Technical Foundations of Hacking

- The Attacker's Process
- The Ethical Hacker's Process

- Security and the Stack
- Summary
- Review All Key Topics
- Exercises
- Suggested Reading and Resources

Chapter 4: Footprinting and Scanning

- Overview of the Seven-Step Information-Gathering Process
- Information Gathering
- Determining the Network Range
- Identifying Active Machines
- Finding Open Ports and Access Points
- OS Fingerprinting
- Fingerprinting Services
- Mapping the Network Attack Surface
- Summary
- Review All Key Topics
- Exercises

- Suggested Reading and Resources

Chapter 5: Enumeration and System Hacking

- Enumeration
- System Hacking
- Summary
- Review All Key Topics
- Exercise
- Suggested Reading and Resources

Chapter 6: Malware Threats

- Viruses and Worms
- Trojans
- Covert Communication
- Keystroke Logging and Spyware
- Malware Countermeasures
- Summary
- Review All Key Topics
- Exercises

- Suggested Reading and Resources

Chapter 7: Sniffers, Session Hijacking, and Denial of Service

- Sniffers
- Session Hijacking
- Denial of Service and Distributed Denial of Service
- Summary
- Review All Key Topics
- Exercises
- Suggested Reading and Resources

Chapter 8: Web Server Hacking, Web Applications, and Database Attacks

- Web Server Hacking
- Web Application Hacking
- Database Hacking
- Summary
- Review All Key Topics
- Exercise

- Suggested Reading and Resources

Chapter 9: Wireless Technologies, Mobile Security, and Attacks

- Wireless Technologies
- Mobile Device Operation and Security
- Wireless LANs
- Summary
- Review All Key Topics
- Suggested Reading and Resources

Chapter 10: IDS, Firewalls, and Honeypots

- Intrusion Detection Systems
- Firewalls
- Honeypots
- Summary
- Review All Key Topics
- Suggested Reading and Resources

Chapter 11: Physical Security and Social Engineering

- Physical Security
- Social Engineering
- Summary
- Review All Key Topics
- Exercise
- Suggested Reading and Resources

Chapter 12: Cryptographic Attacks and Defenses

- Functions of Cryptography
- History of Cryptography
- Algorithms
- Public Key Infrastructure
- Protocols, Applications, and Attacks
- Summary
- Review All Key Topics
- Exercises
- Suggested Reading and Resources

Chapter 13: Cloud Computing and Botnets

- Cloud Computing
- Botnets
- Summary
- Review All Key Topics
- Exercise
- Suggested Reading and Resources

Chapter 14: Final Preparation

- Hands-on Activities
- Suggested Plan for Final Review and Study
- Summary

Videos and How To

uCertify course includes videos to help understand concepts. It also includes How Tos that help learners in accomplishing certain tasks.

188	12:03
VIDEOS	HOURS

12. Practice Test

Here's what you get

120	2	119
PRE-ASSESSMENTS QUESTIONS	FULL LENGTH TESTS	POST-ASSESSMENTS QUESTIONS

Features

uCertify provides video training courses that contain videos and test set questions based on the exam. These courses are interactive and engaging and the learners can view the content at their own pace, in their own time, and on any device. Learners can easily track the engagement levels so they immediately know which course components are easy to understand and which are more difficult. Test set in the courses closely follow the exam objectives and are designed to simulate real exam conditions.

Each pre and post assessment comes with interactive questions which help users in better understanding of the subject matter.

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

An Introduction to Ethical Hacking

- Examining Security Policies

The Technical Foundations of Hacking

- Checking IP/Subnet mask
- Checking Internet Access Availability
- Checking System Reference for Common Port/Name Assignments
- Checking DNS IP Address

Footprinting and Scanning

- Searching people using AnyWho
- Searching with Google Advance Search Operators
- Using Google Hacking Database (GHDB) to Search
- Mirroring the Entire Website
- Viewing A Records
- Viewing Mail Servers
- Viewing Full Zone Transfer

- Retrieving Whois Record of a website
- Searching People using Spokeo and Zabasearch
- Using LinkedIn to Find Details of an Employee
- Performing active reconnaissance
- Using Whois
- Performing Information Gathering
- Using arin.net to Find IP Ranges Assigned to Amazon
- Performing a Ping Sweep with nmap
- Scanning Network using nbtscan
- Scanning Target Hosts for their Open Ports Using nmap
- Viewing Which Ports are Up and Responding on the Local Host
- Performing OS Detection of the Localhost
- Performing OS Fingerprinting
- Determining Webserver Version
- Performing nmap Traceroute
- Performing ARP Spoofing

Enumeration and System Hacking

- Enumerating Data Using enum4linux
- Observing State of NTP on the Localhost
- Hiding Text File in Image by Steganography
- Clear Event Logs Using Meterpreter
- Detecting Rootkits
- Capturing Screenshot Using Metasploit

Malware Threats

- Disassembling: Convert Hexpair to Opcodes
- Using NetCat to Access a Shell Over the Network
- Using System Monitor
- Observing the Current Running Processes
- Observing the Listening Services
- Finding Active Network Connection

Sniffers, Session Hijacking, and Denial of Service

- Analyzing Protocols with Wireshark
- Analyzing Captured Packets using Sniffer
- Performing Passive OS Fingerprinting
- Using tcpdump to View Network Traffic
- Using tcpdump to View Data in tcp Traffic
- Using Wireshark to Sniff the Network
- Changing mac Address with macchanger
- Simulating a DoS Attack

Web Server Hacking, Web Applications, and Database Attacks

- Adding Netcraft Extension
- Launching OpenVas and Running a Scan
- Using Netcraft to Determine Server Version of fork.com
- Reviewing CVEs and Buffer Overflows
- Viewing Web Server Enumeration
- Cracking Password using Hydra
- Performing Banner Grabbing
- Exploiting SQL Injection
- Detecting Web Application Firewall using WAF00F

Wireless Technologies, Mobile Security, and Attacks

- Fragmenting Large Ping Packets

Physical Security and Social Engineering

- Browsing SSL Certificates
- Managing Disk Partitions
- Scanning a Network using nmap
- Using Social Engineering Techniques to Plan an Attack
- Hacking Web Browsers using BeEF

Cryptographic Attacks and Defenses

- Examining an SSL Certificate
- Observing MD5 Hash
- Using Openssl to Create a Public/Private Keypair
- Encrypting and Decrypting a Message
- Using PGP

Here's what you get

68

LIVE LABS

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