uCertify

Course Outline

CEH v8 - Certified Ethical Hacker

25 May 2020

Lesson

Practice test

Contents

1. Course Objective

Gain hands-on expertise in EC-Council CEH 312-50 V8 exam with CEH V8 - Certified Ethical Hacker course. EC Council 312-50 V8 exam is designed to certify the competency of IT professionals to establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures; and reinforce ethical hacking. It also demonstrates competency in Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows, and Virus Creation. The CEH preparation course is intended for network administrators for building up the intensity to find vulnerable target systems and utilize white-hat hacking, with an honest intention to access the data resources. The CEH course presented by uCertify will change the upcoming hackers into capable certified security defenders. The preparation of CEH certification with the assistance of Test-Prep, Exercises, Quizzes, Lessons, and numerous different resources accessible with the course, will make aspirants well versed with all of the technologies required to protect and enhance organization's security system, making it hack-proof.

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 assignments. 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 5 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

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 to Ethical Hacking

- Gain knowledge on various hacking terminologies

- Understand the different types and implications of hacker attacks

Chapter 2: Footprinting and Reconnaissance

- Understand the term footprinting
- Understand how traceroute is used in footprinting
- Google hacking, Website mirroring, and email tracking

Chapter 3: Scanning Networks

- Understand the term port scanning, network scanning, and vulnerability scanning
- Understand ping sweeping, firewalk tool, and nmap command switches
- Understand scans
- Learn TCP communication flag types, and gain knowledge on War dialing techniques
- Understand banner grabbing using fingerprinting and other techniques and tools
- Learn vulnerability scanning using BidiBlah and other hacking tools
- Understand proxy servers, anonymizers, HTTP tunneling techniques, and IP spoofing techniques

Chapter 4: Enumeration

- Learn the system hacking cycle, and understand enumeration and its techniques

- Understand null sessions and their countermeasures
- Understand SNMP enumeration and its countermeasures

Chapter 5: System Hacking

- Understand the different types of passwords, password attacks, and password cracking techniques
- Authentication mechanism, password sniffing, various password cracking tools, and countermeasures
- Understand privilege escalation, key loggers, and other spyware technologies
- Identify different ways to hide files, understand rootkits, and understand alternate data streams
- Understand steganography technologies and tools used
- Understand covering tracks, tools used and erase evidences

Chapter 6: Trojans and Backdoors

- Define a Trojan
- Identify the ports used by a Trojan
- Identify listening ports using netstat
- Understand wrapping , reverse shell Trojan, and ICMP tunneling
- Understand Windows start up monitoring tools, and the Trojan horse constructing kit
- Learn Trojan detection and evading techniques

Chapter 7: Viruses and Worms

- Virus, characteristics of a virus, working of a virus, and virus hoaxes
- Understand the difference between a virus and a worm, and understand the life cycle of virus
- Virus writing technique and virus construction kits
- Understand antivirus evasion techniques, and understand virus detection methods and countermeasures
- Understand worm analysis

Chapter 8: Sniffers

- Sniffers, identify types of sniffing, and understand active and passive sniffing
- Understand Address Resolution Protocol (ARP), and the process of ARP spoofing
- Understand MAC duplicating
- Learn ethereal capture and display filters
- Understand MAC flooding, understand DNS spoofing techniques, and DNS spoofing countermeasures
- Know various sniffing tools, identify sniffing detection and defensive techniques

Chapter 9: Social Engineering

- Understand social engineering

- Identify the different types of social engineering
- Understand dumpster diving, human-based social engineering, and insider attack
- Understand phishing attacks, identify online scams, and understand URL obfuscation
- Identify social engineering countermeasures

Chapter 10: Denial of Service

- Understand a Denial of Service attack, and analyze symptoms of a DoS Attack
- Understand Internet Chat Query (ICQ), Internet Relay Chat (IRC), and botnets
- Assess DoS/DDoS attack tools
- Identify DoS/DDoS countermeasure, post-attack forensics, and Penetration Testing

Chapter 11: Session Hijacking

- Understand session hijacking and session hijacking techniques
- Understand session hijacking process and session hijacking in the OSI Model
- Understand the brute forcing attack, and HTTP referrer attack
- Understand application level session hijacking, and discuss session sniffing
- Describe man-in-the-middle, man-in-the-browser, Client-side, and cross-site script attacks
- Understand session fixation attack, and describe network level session hijacking

- Understand TCP/IP hijacking, session hijacking tools, and countermeasures of session hijacking

Chapter 12: Hacking Webservers

- Web server attacks
- Examine webserver misconfiguration, and understand directory traversal attacks
- Learn regarding HTTP response splitting attack, and understand Web cache poisoning attack
- Understand HTTP response hijacking, and discuss SSH bruteforce attack
- Examine man-in-the-middle attack, and learn webserver password cracking techniques
- Understand webserver attack methodology
- Identify webserver attack tools, and identify countermeasures against webserver attacks
- Understand patch management, assess webserver security tools

Chapter 13: Hacking Web applications

- Understand Web applications, Web application components, and working of Web applications
- Understand Web application architecture, parameter/form tampering, and injection flaws
- Discuss hidden field manipulation, cross-site scripting (XSS), and Web services attacks
- Identify Web application hacking and Web application security tools
- Understand Web application firewalls, and gain insights on Web application pen testing

Chapter 14: SQL Injection

- Understand SQL injection and SQL injection black box penetration testing
- Understand types of SQL injection and blind SQL injection
- Learn SQL injection methodology
- Examine advanced enumeration, describe password grabbing, and discuss grabbing SQL Server hashes
- SQL injection tools
- Understand defensive strategies against SQL injection attacks

Chapter 15: Hacking Wireless Networks

- Understand wireless networks, various types of wireless networks, and Wi-Fi authentication modes
- Identify types of wireless encryption, and understand WEP encryption and WPA/WPA2

- Understand wireless hacking methodology, and assess wireless hacking tools
- Understand Bluetooth hacking, and understand how to defend against Bluetooth hacking
- Understand how to defend against wireless attacks, and identify Wi-Fi security tools
- Examine Wireless Penetration Testing Framework

Chapter 16: Hacking Mobile Platform

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Hacking Windows Phone OS
- Hacking BlackBerry
- Mobile Device Management (MDM)
- Mobile Security Guidelines and Tools
- Mobile Pen Testing

Chapter 17: Evading IDS, Firewalls, and Honeypots

- Understand Intrusion Detection Systems (IDS)
- Understand what is a firewall, types of firewalls, and identify firewall identification techniques

- Understand honeypot
- Examine evading IDS, understand evading firewalls, and learn detecting honeypots
- Identify firewall evading tools

Chapter 18: Buffer Overflow

- Understand buffer overflows (BoF)
- Reasons for buffer overflow attacks, and skills required to program buffer overflow exploits
- Testing for heap overflow conditions: heap.exe, and understand OllyDbg debugger
- Understand buffer overflow countermeasures tools and buffer overflow pen testing

Chapter 19: Cryptography

- Understand cryptography, learn various types of cryptography, and understand ciphers
- Understand AES, RC4, RC5, RC6 algorithms, RSA, Message Digest Function: MD5, and SHA
- Identify cryptography tools, and understand Public Key Infrastructure (PKI), and digital signature
- Understand SSL, disk encryption, and cryptography attacks

Chapter 20: Penetration Testing

- Understand penetration testing (PT)

- Understand automated testing, manual testing, and penetration testing techniques
- Understand enumerating devices

Chapter 21: Video Tutorials

- Introduction
- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- System Hacking
- Trojans and Backdoors
- Viruses and Worms
- Denial of Service
- Social Engineering
- Sniffers
- Session Hijacking
- Hacking Web Servers
- Web Application Vulnerabilities

- SQL Injection
- Hacking Wireless Networks
- Evading IDS Firewalls and Honeypots
- Buffer Overflows
- Cryptography and Steganography
- Metasploit for Penetration Testing
- Business Process
- Lab Suggestions

Videos and How To

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

122	12:25
VIDEOS	**HOURS**

12. Practice Test

uCertify provides full length practice tests. These tests closely follow the exam objectives and are designed to simulate real exam conditions. Each course has a number of test sets consisting of hundreds of items to ensure that learners are prepared for the certification exam.

Here's what you get

15
PRE-ASSESSMENTS QUESTIONS

100
POST-ASSESSMENTS QUESTIONS

Features

Full Remediation

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.

Learn, Test and Review Mode

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. 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.

Have Any Query? We Are Happy To Help!

GET IN TOUCH:

Contact No

Email: sales@ucertify.com

www.uCertify.com