Certified Ethical Hacker v10 (Bundle)

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Day**

Overview

A Certified Ethical Hacker (CEH) is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

The Purpose of the CEH credential is to:

- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.
- Inform the public that credentialed individuals meet or exceed the minimum standards.
- Reinforce ethical hacking as a unique and self-regulating profession.

The CEHv10 course is now accredited under the GCHQ Certified Training (GCT) Scheme.

What's Included?

Included in our CEHv10 {*training}:

- CEHv10 (ANSI) & CEHv10 (ANSI) Exam Voucher
- CEHv10 iLabs (Post Course CEHv10 Lab Access - 6 months)

'I had an exceptional learning experience with Certified Ethical Hacker (C|EH)! Every bit of the program was filled with a lot of information. It gave me full-fledged exposure to various pen testing techniques and helped me build the skills required for an amazing InfoSec career. I absolutely loved the high-quality content of the program and the virtual labs included in it. For me, the theory and practical sessions of the program supported each other brilliantly.'

Jeffery Osuya, Network Security Analyst at NHS

Prerequisites

Before attending this accelerated ethical hacking {*training}, you should hold two years' IT work experience and possess a basic familiarity of Linux and/or Unix. We also recommend you possess a strong working knowledge of:

- TCP/IP
- Windows Server

Delegates will not be able to access the EC Council CEHv10 course material until they receive their login details, which they are given on the first day of the course.

What You Will Learn

CEHv10 (ANSI) What will you learn?

1. Key issues plaguing the information security world, incident management process, and penetration testing.

2. Various types of foot printing, foot printing tools, and countermeasures.

3. Network scanning techniques and scanning countermeasures.

4. Enumeration techniques and enumeration countermeasures.

5. System hacking methodology, steganography, steganalysis attacks, and covering tracks.

6. Different types of Trojans, Trojan analysis, and Trojan countermeasures.

7. Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.

8. Packet sniffing techniques and how to defend against sniffing.

9. Social Engineering techniques, identify theft, and social engineering countermeasures.

10. DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures.

11. Session hijacking techniques and countermeasures.

12. Different types of webserver attacks, attack methodology, and countermeasures.

13. Different types of web application attacks, web application hacking methodology, and countermeasures.

14. SQL injection attacks and injection detection tools.

15. Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.

16. Mobile platform attack vector, android vulnerabilities, mobile security guidelines, and tools.

17. Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.

18. Various cloud computing concepts, threats, attacks, and security techniques and tools.

19. Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

20. Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.

21. Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.

22. Different threats to IoT platforms and learn how to defend IoT devices securely.

CEHv10 (iLabs) - 6 months post course access

Delegates will dynamically access a host of Virtual Machines preconfigured with vulnerabilities, exploits, tools, and scripts from anywhere with an internet connection. This is a cloud based subscription service from EC-Council designed to deliver serious hands on practice for the information security professional.

The cloud portal enables a course participant to launch an entire range of target machines and access them remotely with just a few clicks. It is the most cost effective, easy to use, live range lab solution available globally today. This product consists of 6 months access to EC-Council virtual lab environment for CEHv10.

EXAM

Exam Title: CEHv10 (ANSI) Exam:

Number of Questions: 125

Passing Score: 70%

Test Duration: 4 hours

Test Format: Multiple Choice

Outline

Module 01: Introduction to Ethical Hacking

Module 02: Footprinting and Reconnaissance

Module 03: Scanning Networks

Module 04: Enumeration

Module 05: Vulnerability Analysis

Module 06: System Hacking

Module 07: Malware Threats

Module 08: Sniffing

Module 09: Social Engineering

Module 10: Denial-of-Service

Module 11: Session Hijacking

Module 12: Evading IDS, Firewalls, and Honeypots

Module 13: Hacking Web Servers

Module 14: Hacking Web Applications

Module 15: SQL Injection

Module 16: Hacking Wireless Networks

Module 17: Hacking Mobile Platforms

Module 18: IoT Hacking

Module 19: Cloud Computing

Module 20: Cryptography

Plus;

Post course access to EC Council CEH (iLabs) to prepare you for the CEHv10 (ANSI) exam

Exam vouchers for CEHv10 (ANSI) exam