COURSE OUTLINE

Course Code: EC-CEH

Course Name: EHC: EC-Council Ethical Hacking and Countermeasures v11

DURATION	SKILL LEVEL	DELIVERY METHOD	TRAINING CREDITS	TECHNOLOGY
5 day (s)	Advanced	In Class	N/A	Ethical Hacking

Course Overview

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH v11 continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: “To beat a hacker, you need to think like a hacker.

Prerequisites

There are no Prerequisites for this course.

Target Audience

- Information Security Analyst /
- Administrator
- Information Assurance (IA) Security
- Officer
- Information Security Manager /
- Specialist
- Information Systems Security Engineer /
- Manager
- Information Security Professionals /
- Officers
- Information Security / IT Auditors
- Risk / Threat/Vulnerability Analyst
- System Administrators
- Network Administrators and Engineers

Topics

Module 1: Introduction to Ethical Hacking

Module 2: Foot printing and Reconnaissance

Module 3: Scanning Networks

Module 4: Enumeration

Module 5: Vulnerability Analysis

Module 6: System Hacking

Module 7: Malware Threats

Module 8: Sniffing

Module 9: 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 and OT Hacking

Module 19: Cloud Computing

Module 20: Cryptography

Exams and Certifications

At course completion

• Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.

• Perform foot printing and reconnaissance using the latest foot printing techniques and tools as a critical pre-attack phase required in ethical hacking.

Network scanning techniques and scanning countermeasures.

• Enumeration techniques and enumeration countermeasures.

• Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.

• System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.

• Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.

• Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.

• Social engineering techniques and how to identify theft attacks to audit human level vulnerabilities and suggest social engineering countermeasures.

• DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.

• Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.

Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server

infrastructure, and countermeasures.

• Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.

• SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.

• Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.

• Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.

• Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.

• Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security.