Course Outline for CEH v11

Module 01: Introduction to Ethical Hacking

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 02: Foot printing and Reconnaissance

Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Module 03: Scanning Networks

Learn different network scanning techniques and countermeasures.

Module 04: Enumeration

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and associated countermeasures.

Module 05: Vulnerability Analysis

Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems.

Module 06: System Hacking

Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

Module 07: Malware Threats

Get an introduction to the different types of malware, such as Trojans, viruses, and worms, as well as system auditing for malware attacks, malware analysis, and countermeasures.

Module 08: Sniffing

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Module 09: Social Engineering

Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Module 10: Denial-of-Service

Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Module 11: Session Hijacking

Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Module 12: Evading IDS, Firewalls, and Honeypots

Get introduced to firewall, intrusion detection system, and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Module 13: Hacking Web Servers

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Module 14: Hacking Web Applications

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

Module 15: SQL Injection

Learn about SQL injection attack techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts.

Module 16: Hacking Wireless Networks

Learn about wireless encryption, wireless hacking methodologies and tools, and Wi-Fi security tools.

Module 17: Hacking Mobile Platforms

Learn about mobile platform attack vectors, Android vulnerability exploits, and mobile security guidelines and tools.

Module 18: IoT Hacking

Learn how to secure and defend Internet of Things (IoT) and operational technology (OT) devices and possible threats to IoT and OT platforms.

Module 19: Cloud Computing

Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud-based threats and attacks, and cloud security techniques and tools.

Module 20: Cryptography

In the final module, learn about cryptography and ciphers, public-key infrastructure, cryptography attacks, and cryptanalysis tools.