EC-Council Certified Ethical Hacker (CEH) v12

Duration	Delivery Methods
5 Days	VILT, Private Group

CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so you will be better positioned to setup your security infrastructure and defend against future attacks. An understanding of system weaknesses and vulnerabilities helps organizations strengthen their system security controls to minimize the risk of an incident. CEH was built to incorporate a hands-on environment and systematic process across each ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to achieve the CEH credential. You will be exposed to an entirely different posture toward the responsibilities and measures required to be secure. Now in its 12th version, CEH continues to evolve with the latest operating systems, tools, tactics, exploits, and technologies.

This course includes an exam voucher.

Who Should Attend

The Certified Ethical Hacking v12 course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Course Objectives

- Information security controls, laws, and standards.
- Various types of footprinting, footprinting tools, and countermeasures.
- 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 against sniffing.
- Social engineering techniques and how to identify theft attacks to audit human-level vulnerabilities and 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, and cryptographic weaknesses and countermeasures.
- Webserver attacks and a comprehensive attack methodology to audit vulnerabilities in webserver infrastructure, and countermeasures.
- Web application attacks, 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), the working of various threats and attacks, and security techniques and tools.
- Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Threats to IoT and OT platforms and defending IoT and OT devices.
- Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

Agenda

1 - INTRODUCTION TO ETHICAL HACKING

- Information Security Overview
- Cyber Kill Chain Concepts
- Hacking Concepts
- Ethical Hacking Concepts
- Information Security Controls
- Information Security Laws and Standards

EDUCATE 360
877.243.6690
info@educate360.com

2 - 2 - FOOT-PRINTING AND RECONNAISSANCE

- Footprinting Concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Who is Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures

3 - SCANNING NETWORKS

- Network Scanning Concepts
- Scanning Tools
- Host Discovery
- Port and Service Discovery
- OS Discovery (Banner Grabbing/OS Fingerprinting)
- Scanning Beyond IDS and Firewall
- Draw Network Diagrams

4 - ENUMERATION

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP and NFS Enumeration
- SMTP and DNS Enumeration
- Other Enumeration Techniques
- Enumeration Countermeasures

5 - VULNERABILITY ANALYSIS

- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment Types
- Vulnerability Assessment Solutions and Tools
- Vulnerability Assessment Reports

6 - SYSTEM HACKING

- System Hacking Concepts
- Gaining Access

EDUCATE 360
877.243.6690
info@educate360.com

- Escalating Privileges
- Maintaining Access
- Clearing Logs

7 - MALWARE THREATS

- Malware Concepts
- APT Concepts
- Trojan Concepts
- Virus and Worm Concepts
- Fileless Malware Concepts
- Malware Analysis
- Countermeasures
- Anti-Malware Software

8 - SNIFFING

- Sniffing Concepts
- Sniffing Technique: MAC Attacks
- Sniffing Technique: DHCP Attacks
- Sniffing Technique: ARP Poisoning
- Sniffing Technique: Spoofing Attacks
- Sniffing Technique: DNS Poisoning
- Sniffing Tools
- Countermeasures
- Sniffing Detection Techniques

9 - SOCIAL ENGINEERING

- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Countermeasures

10 - DENIAL-OF-SERVICE

- DoS/DDoS Concepts
- DoS/DDoS Attack Techniques
- BotnetsDDoS Case Study
- DoS/DDoS Attack Tools
- Countermeasures
- DoS/DDoS Protection Tools

11 - SESSION HIJACKING

- Session Hijacking Concepts

EDUCATE 360
877.243.6690
info@educate360.com

- Application Level Session Hijacking
- Network Level Session Hijacking
- Session Hijacking Tools
- Countermeasures

12 - EVADING IDS, FIREWALLS, AND HONEYPOTS

- IDS, IPS, Firewall, and Honeypot Concepts
- IDS, IPS, Firewall, and Honeypot Solutions
- Evading IDS
- Evading Firewalls
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures

13 - HACKING WEB SERVERS

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Tools
- Countermeasures
- Patch Management
- Web Server Security Tools

14 - HACKING WEB APPLICATIONS

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web API, Webhooks, and Web Shell
- Web Application Security

15 - SQL INJECTION

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Evasion Techniques
- Countermeasures

16 - HACKING WIRELESS NETWORKS

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology

EDUCATE 360
877.243.6690
info@educate360.com

- Wireless Hacking Tools
- Bluetooth Hacking
- Countermeasures
- Wireless Security Tools

17 - HACKING MOBILE PLATFORMS

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Device Management
- Mobile Security Guidelines and Tools

18 - IOT AND OT HACKING

- IoT Hacking
- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- IoT Hacking Tools
- Countermeasures
- OT Hacking
- OT Concepts
- OT Attacks
- OT Hacking Methodology
- OT Hacking Tools
- Countermeasures

19 - CLOUD COMPUTING

- Cloud Computing Concepts
- Container Technology
- Serverless Computing
- Cloud Computing Threats
- Cloud Hacking
- Cloud Security

20 - CRYPTOGRAPHY

- Cryptography Concepts
- Encryption Algorithms
- Cryptography Tools
- Public Key Infrastructure (PKI)
- Email Encryption
- Disk Encryption
- Cryptanalysis
- Countermeasures

EDUCATE 360
877.243.6690
info@educate360.com

Prerequisite Courses Recommended

- CompTIA Linux+
- CompTIA Security+

EDUCATE 360
877.243.6690
info@educate360.com