# EC-Council Certified Ethical Hacker (C|EH) + Exam voucher

**Duration: 5 Days** **Course Code: CEH** **Version: 10**

## Overview:

A Certified Ethical Hacker (CEH) is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems. A Ethical Hacker 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.
This course will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. The security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment.
This ethical hacking course puts you in the driver's seat of a hands-on environment with a systematic process. Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be taught the five phases of ethical hacking and the ways to approach your target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.
The Certified Ethical Hacker course is regularly updated to ensure you are aware of the latest tools and techniques used by hackers and information security professionals. .
A Pearson Vue exam voucher is included, although you will need to schedule the exam at a Pearson Vue testing faclity. An additional 6 months access to the CEHv10 (iLabs) is provided once you have completed the course.

## Target Audience:

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

## Objectives:

- **During this course you should learn the:**
- Key issues plaguing the information security world, incident management process, and penetration testing.
- Various types of footprinting, footprinting tools, and countermeasures.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks.
- Different types of Trojans, Trojan analysis, and Trojan countermeasures.
- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.
- Packet sniffing techniques and how to defend against sniffing.
- Social Engineering techniques, identify theft, and social engineering countermeasures.
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures.
- Session hijacking techniques and countermeasures.
- Different types of webserver attacks, attack methodology, and countermeasures.
- Different types of web application attacks, web application hacking methodology, and countermeasures.
- SQL injection attacks and injection detection tools.
- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
- Mobile platform attack vector, android vulnerabilities, mobile security guidelines, and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.
- Various cloud computing concepts, threats, attacks, and security techniques and tools.
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.
- Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- Different threats to IoT platforms and learn how to defend IoT devices securely.

## Prerequisites:

**Attendees should meet the following prerequisites:**

- Have two years' IT work experience and a possess a basic familiarity of Linux and/or Unix.
- A strong working knowledge of:
- TCP/IP
- Windows Server

## Testing and Certification

**Recommended as prepartaion for the following exams:**

- **312-50** - Certified Ethical Hacker

The CEH exam can only be attempted if you meet the criteria specified by EC-Council

- Have attended the CEH Course with am Authorised EC-Council Provider (Exam Application process not required) **or**
- Have two years work experience in the Information Security domain and able to provide a proof of the same, this will need to be validated through the exam application process

## Follow-on-Courses:

**The following couses are recommended for further study:**

- Hone and validate your skills further by taking the new CEH (Practical) exam.
- **ECSA** - EC-Council Certified Security Analyst (ECSA): Penetration Testing

## Content:

### Introduction to Ethical Hacking

- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts
- Ethical Hacking Concepts
- Information Security Controls
- Penetration Testing Concepts
- Information Security Laws and Standards

### Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Countermeasures
- Footprinting Pen Testing

### Scanning Networks

- Network Scanning Concepts
- Scanning Tools
- Scanning Techniques
- Scanning Beyond IDS and Firewall
- Banner Grabbing
- Draw Network Diagrams
- Scanning Pen Testing

### Enumeration

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

### Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Assessment Solutions
- Vulnerability Scoring Systems
- Vulnerability Assessment Tools
- Vulnerability Assessment Reports

### System Hacking

- System Hacking Concepts
- Cracking Passwords
- Escalating Privileges

### 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
- Sniffing Pen Testing

### Social Engineering

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

### Denial-of-Service

- DoS/DDoS Concepts
- DoS/DDoS Attack Techniques
- Botnets
- DDoS Case Study
- DoS/DDoS Attack Tools
- Countermeasures
- DoS/DDoS Protection Tools
- DoS/DDoS Penetration Testing

### Session Hijacking

- Session Hijacking Concepts
- Application Level Session Hijacking
- Network Level Session Hijacking
- Session Hijacking Tools
- Countermeasures
- Penetration Testing

### Evading IDS, Firewalls, and Honeypots

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

### Hacking Web Servers

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

### SQL Injection

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

### Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Countermeasures
- Wireless Security Tools
- Wireless Pen Testing

### Hacking Mobile Platforms

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

### IoT Hacking

- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- IoT Hacking Tools
- Countermeasures
- IoT Pen Testing

### Cloud Computing

- Cloud Computing Concepts
- Cloud Computing Threats
- Cloud Computing Attacks
- Cloud Security
- Cloud Security Tools
- Cloud Penetration Testing

### Cryptography

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

- Executing Applications
- Hiding Files
- Covering Tracks
- Penetration Testing

Malware Threats

- Malware Concepts
- Trojan Concepts
- Virus and Worm Concepts
- Malware Analysis
- Countermeasures
- Anti-Malware Software
- Malware Penetration Testing

- Web Server Security Tools
- Web Server Pen Testing

Hacking Web Applications

- Web App Concepts
- Web App Threats
- Hacking Methodology
- Web App Hacking Tools
- Countermeasures
- Web App Security Testing Tools
- Web App Pen Testing

## Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278

training@globalknowledge.com.sa

www.globalknowledge.com/en-sa/

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Worood, Riyadh 3140, Saudi Arabia