Certified Ethical Hacker (CEH v11)

Duration: 5 Days Course Code: CEH Version: 11

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.
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 that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help 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 everyethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure.
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.
Looking to obtain the CEH Master Accreditation, then why not purchase the CEH Pratical Exam aas well CEH Exam + CEH Practical Exam = CEH Master
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 CEHv11 (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:**
- Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.
- Perform footprinting and reconnaissance using the latest footprinting 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
- 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 techniques and tools.
- Penetration testing, security audit, vulnerability assessment, and

audit humanlevel vulnerabilities and suggest social engineering countermeasures.

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

penetration testing roadmap.

- Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
- Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools

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 preparation 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:

- Hone and validate your skills further by taking the new CEH (Practical) exam. **CEH EXAM + CEH Practical = CEH MASTER**

Content:

Introduction to Ethical Hacking

- Information Security Overview
- Cyber Kill Chain Concepts
- Hacking Concepts
- Ethical Hacking Concepts
- Information Security Controls
- 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
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures

Scanning Networks

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

Enumeration

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

Vulnerability Analysis

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

System Hacking

- System Hacking Concepts
- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

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

Social Engineering

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

Denial-of-Service

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

Session Hijacking

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

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

Hacking Web Servers

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

Hacking Web Applications

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

Hacking Mobile Platforms

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

IoT and OT Hacking

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

Cloud Computing

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

Cryptography

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

Malware Threats

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

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

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE