Certified Ethical Hacker

Duration: 5 Days **Course Code: CEH** **Version: 12**

Overview:

The Certified Ethical Hacker has been battle-hardened over the last 20 years, creating hundreds of thousands of Certified Ethical Hackers employed by top companies, militaries, and governments worldwide.

In its 12th version, the Certified Ethical Hacker provides comprehensive training, hands-on learning labs, practice cyber ranges for engagement, certification assessments, cyber competitions, and opportunities for continuous learning into one comprehensive program curated through our new learning framework: 1. Learn 2. Certify 3. Engage 4. Compete.

The C|EH v12 also equips aspiring cybersecurity professionals with the tactics, techniques, and procedures (TTPs) to build ethical hackers who can uncover weaknesses in nearly any type of target system before cybercriminals do.

Target Audience:

The Certified Ethical Hacking training course will significantly benefit security officers, Cybersecurity auditors, security professionals, Site administrators, Security Analyst 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 including Footprinting thru Web Services & Social Networking Sites 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 threats (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.
- Firewall, IDS , IPS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for 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.
- Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
- Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
- Cryptography ciphers, Public Key Infrastructure (PKI), Email encryption, cryptography attacks, and Cryptography Attack Countermeasures.

Prerequisites:

- Have two years 'IT Security experience and a possess a basic familiarity of Linux and/or Unix.
- Familiarity with cybersecurity Concepts
- 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 an Authorized 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:

- Validate your skills further by taking the CEH (Practical) exam. CEH EXAM + CEH Practical = CEH MASTER

Content:

This Course Includes 20 Modules That Help You Master the Foundations of Ethical Hacking and Prepare to Take the C|EH Certification Exam

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. Different types of vulnerability assessment and vulnerability assessment tools.

Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware 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 discovernetwork-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Module 12

Evading IDS, Firewalls, and Honeypots

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 attacks, evasion techniques, and SQL injection Countermeasures.

Module 16

Hacking Wireless Networks

Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi security tools, and countermeasures.

Module 17

Hacking Mobile Platforms

Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

Module 18

IoT Hacking

Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

Module 19

Cloud Computing

Learn different cloud computing concepts, such as container technologies and server less computing, various cloud computing threats, attacks, hacking methodology, and cloud security techniques and tools.

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 introduced to firewall, intrusion detection system (IDS), 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

Module 20

Cryptography

Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

HANDS-ON LEARNING LABS

With over 220 hands-on labs conducted in our cyber range environment, you will have the opportunity to practice every learning objective on live machines and vulnerable targets in the course. Pre-loaded with over 3,500 hacking tools and various operating systems, you will gain unprecedented exposure and hands-on experience with the most common security tools, latest vulnerabilities, and widely used operating systems in the industry. Our range is web accessible, making it easier for you to learn and practice from anywhere.

Additional Information:

WHAT'S NEW IN THE C|EH® V12
LEARN | CERTIFY | ENGAGE | COMPETE
The C|EH® v12 is a specialized and one-of-a-kind training program to teach you everything you need to know about ethical hacking with hands-on training, labs, assessment, a mock engagement (practice), and global hacking competition. Stay on top of the game with the most in-demand skills required to succeed in the field of cybersecurity.

Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

info@globalknowledge.ie

www.globalknowledge.com/en-ie/

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1