VKonSec
We Konnect & Secure

[Certified Ethical Hacker]AI
Get the AI Edge with the new CEH v13 and boost your career

Benefits of Doing a CEH (Certified Ethical Hacker) Course

1. **Comprehensive Understanding of Cybersecurity:**
   a. The CEH course covers various hacking tools, techniques, and methodologies used by both ethical hackers and cybercriminals. It provides in-depth knowledge on how to identify and fix vulnerabilities in an organization's network.
2. **Global Recognition:**
   a. CEH is one of the most widely recognized certifications in the cybersecurity field. It is recognized by top companies worldwide and is a strong addition to your resume when pursuing jobs in information security.
3. **Hands-On Practice:**
   a. The course emphasizes practical experience by simulating real-world cyberattacks in controlled lab environments. This prepares candidates to face actual cybersecurity threats and vulnerabilities.
4. **Opens Up Various Career Paths:**
   a. CEH certification can lead to positions such as Ethical Hacker, Penetration Tester, Security Analyst, and IT Auditor, among others.
5. **Increased Salary Potential:**
   a. Ethical hackers are in demand, and certified professionals are often offered higher salaries due to their specialized skills. The certification can help boost salary expectations in the cybersecurity field.
6. **Stay Updated with the Latest Threats:**
   a. The CEH curriculum is regularly updated to ensure that certified professionals are aware of the latest cyber threats and the latest penetration testing techniques.
7. **Fulfills Job Role Requirements:**

a. Many government and private sector jobs, especially in the IT security domain, require a CEH certification as part of their job requirements.

8. **Strengthens Knowledge of Attack Vectors:**
   a. CEH equips you with knowledge about various attack vectors, such as social engineering, malware, viruses, DDoS attacks, SQL injection, and more, allowing you to defend against them effectively.

Prerequisites for CEH Course

1. **Basic Knowledge of Networking:**
   a. Understanding fundamental concepts such as IP addressing, subnetting, OSI Model, and basic networking protocols is crucial before pursuing CEH.
2. **Understanding of Operating Systems:**
   a. Familiarity with Windows and Linux environments is essential, as most ethical hacking practices are executed in these systems.
3. **Experience in IT:**
   a. While it is not mandatory, having at least 2 years of work experience in the information security domain is recommended. It can help you grasp the CEH material more easily.
4. **Knowledge of Security Concepts:**
   a. Basic knowledge of security concepts such as firewalls, IDS/IPS, encryption, and authentication mechanisms can be beneficial.
5. **Desire to Understand Hacking Techniques:**
   a. A strong interest in learning about how cyberattacks are carried out and mitigated is necessary to succeed in CEH.
6. **Completion of EC-Council's CEH Training Program (Optional):**
   a. If you don't have the required work experience, you can attend an official CEH training program provided by EC-Council, which qualifies you to sit for the CEH exam.
7. **No Mandatory Prerequisite (Self-Study):**

a. For individuals opting for self-study, there are no strict prerequisites. However, familiarity with networking and security basics is highly recommended to understand the course content.

CEH certification is a vital step toward building a career in cybersecurity, providing both theoretical knowledge and hands-on skills to combat evolving cyber threats.

Certified Ethical Hacker (CEH) course could be structured, outlining day-to-day content with suggested time allocations for each topic. The course typically lasts about 5 days, depending on the delivery pace and depth of each topic.

Day 1: Introduction to Ethical Hacking

- **Overview of Ethical Hacking and Cybersecurity (1 hour)**
  - Definition of Ethical Hacking
  - Overview of Cybersecurity and Threat Landscape
  - Role of Ethical Hackers and Legal Implications
  - Types of Hackers (Black Hat, White Hat, Gray Hat)
- **Footprinting and Reconnaissance (3 hours)**
  - Information Gathering Techniques (active & passive)
  - Footprinting through Social Engineering
  - Tools: Maltego, Shodan, Google Dorking
  - Lab: Practicing Footprinting
- **Scanning Networks (3 hours)**
  - Overview of Network Scanning Techniques
  - Identifying Live Hosts and Open Ports (Nmap, Netcat)
  - Understanding the Scanning Process (SYN, TCP, UDP Scans)
  - Lab: Conducting Scans on a Virtual Network

Day 2: System and Network Vulnerabilities

- **Enumeration (2 hours)**

  - Understanding Enumeration Techniques
  - Extracting Usernames, Groups, Network Shares
  - Enumeration Tools: NetBIOS, NBTScan, SNMP
- **System Hacking (5 hours)**
  - Password Cracking Techniques (Brute Force, Dictionary)
  - Exploiting Vulnerabilities in OS and Software
  - Privilege Escalation Techniques
  - Maintaining Access: Rootkits, Backdoors, Trojans
  - Lab: Hands-on with Password Cracking Tools (John the Ripper, Hashcat)

Day 3: Network Security and Exploitation

- **Malware Threats (3 hours)**
  - Understanding Malware Types (Viruses, Worms, Ransomware)
  - How Malware is Delivered (Phishing, Drive-by Downloads)
  - Techniques for Defending Against Malware
  - Lab: Working with Antivirus Bypass Techniques
- **Sniffing (3 hours)**
  - Packet Sniffing Techniques (Wireshark, TCPdump)
  - Spoofing (ARP Poisoning, MAC Spoofing)
  - MITM Attacks (Man-in-the-Middle)
  - Lab: Capturing Traffic and Analyzing Network Packets
- **Social Engineering (2 hours)**
  - Types of Social Engineering Attacks
  - Phishing, Pretexting, Baiting, Quid Pro Quo
  - Real-World Examples of Social Engineering
  - Lab: Simulating Social Engineering Attacks

Day 4: Advanced Hacking Techniques

- **Denial of Service (2 hours)**
  - Understanding DoS and DDoS Attacks
  - Tools for DoS (LOIC, HOIC)

  - Lab: Simulating Denial of Service Attacks in a Controlled Environment
- **Session Hijacking (2 hours)**
  - Techniques for Session Hijacking
  - Exploiting Weaknesses in Session Management
  - Lab: Simulating a Session Hijacking Attack
- **Hacking Web Servers and Web Applications (4 hours)**
  - Web Server Attacks: Directory Traversal, Misconfigurations
  - Web Application Attacks: SQL Injection, XSS (Cross-Site Scripting)
  - OWASP Top 10 Vulnerabilities
  - Lab: Identifying and Exploiting Web Application Vulnerabilities

Day 5: Advanced Tools and Countermeasures

- **Evading IDS, Firewalls, and Honeypots (3 hours)**
  - Methods for Bypassing Intrusion Detection Systems (IDS)
  - Techniques to Evade Firewalls
  - Deploying Honeypots to Capture Malicious Traffic
  - Lab: Evading Firewalls and IDS
- **Cryptography (2 hours)**
  - Basic Concepts of Cryptography (Symmetric & Asymmetric)
  - Hashing Techniques and Digital Signatures
  - Tools for Cryptography (OpenSSL)
  - Lab: Encrypting and Decrypting Data
- **Cloud and Mobile Hacking (2 hours)**
  - Overview of Cloud Security Issues
  - Mobile Hacking Techniques (Android, iOS Vulnerabilities)
  - Lab: Simulating Attacks on Mobile Devices
- **Penetration Testing Framework (1 hour)**
  - Overview of the Penetration Testing Process
  - Tools for Pen Testing (Metasploit)
  - Creating and Delivering a Penetration Testing Report

Time Allocation Summary

- **Day 1:** 7 hours
- **Day 2:** 7 hours
- **Day 3:** 8 hours
- **Day 4:** 8 hours
- **Day 5:** 8 hours

This daily breakdown helps in structuring the CEH training course while ensuring there is enough time allocated for theory, practical labs, and hands-on exercises.