Certified Ethical Hacker (CEH) Course Outline

Duration: 40–50 Hours
Level: Intermediate to Advanced
Delivery Mode: Online / Offline
Target Audience: Cybersecurity professionals, IT professionals, Penetration testers, Network administrators
Prerequisites: Basic knowledge of networking, TCP/IP, and security concepts

---

Module 1: Introduction to Ethical Hacking

- What is Ethical Hacking?
- The Importance of Ethical Hacking in Cybersecurity
- Understanding the Legal and Ethical Implications of Hacking
- CEH Exam Overview and Structure
- Types of Hackers: White-hat, Black-hat, and Gray-hat
- Hacking Phases: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Clearing Tracks

---

Module 2: Footprinting and Reconnaissance

- Understanding Footprinting and its Importance
- Types of Footprinting: Active and Passive
- Tools for Reconnaissance: WHOIS, DNS Interrogation, Traceroute
- Using Google Dorks for Information Gathering
- Identifying Target Networks and Systems
- Data Mining and Extracting Information from Social Media

Module 3: Scanning Networks

- Introduction to Network Scanning
- Types of Scanning: Port Scanning, Network Scanning, Service Scanning
- Scanning Techniques: TCP, UDP, SYN, Ping Sweep
- Network Scanning Tools: Nmap, Netcat, and Hping
- Identifying Open Ports and Vulnerabilities in a Network
- Detecting Firewalls and IDS/IPS

Module 4: Enumeration

- What is Enumeration?
- Enumeration Techniques for Usernames, Shared Resources, and NetBIOS
- SNMP Enumeration for Network Devices
- DNS Enumeration for Domain and Host Information
- Active Directory Enumeration Techniques
- Using Tools like Netcat and SNMPwalk for Enumeration

Module 5: System Hacking

- Introduction to System Hacking Techniques
- Gaining Access: Password Cracking and Hashing Techniques
- Privilege Escalation: Exploiting Vulnerabilities to Gain Higher Access
- Maintaining Access: Rootkits, Trojans, and Backdoors
- Clearing Tracks: Logs and Audit Trails
- Post-Exploitation Techniques and Evidence Collection

Module 6: Malware Threats

- Overview of Malware: Types and Functions
- Viruses, Worms, Trojans, and Spyware
- How Malware is Delivered: Social Engineering, Email, Drive-By Downloads
- Analyzing Malware: Reverse Engineering and Static Analysis
- Keyloggers and Rootkits: Identification and Removal
- Prevention and Detection of Malware

Module 7: Sniffing and Evasion

- Introduction to Sniffing and its Role in Hacking
- Packet Sniffing Tools: Wireshark, tcpdump, and Ettercap
- How to Perform ARP Poisoning and DNS Spoofing
- Sniffing Unencrypted Network Traffic
- Session Hijacking and Mitigation Techniques
- Evasion Techniques to Bypass IDS/IPS

Module 8: Web Application Hacking

- Understanding Web Application Security
- SQL Injection: Techniques, Detection, and Prevention
- Cross-Site Scripting (XSS): Types and Countermeasures
- Cross-Site Request Forgery (CSRF) and Security Risks
- Directory Traversal and File Inclusion Vulnerabilities
- Web Application Scanning and Exploitation Tools: Burp Suite, OWASP ZAP
- Web Application Firewalls and How to Bypass Them

Module 9: Wireless Network Hacking

- Introduction to Wireless Networks and Protocols (WEP, WPA, WPA2)
- Cracking Wireless Networks: WPA/WPA2 Cracking using Aircrack-ng
- Wireless Sniffing and Eavesdropping Tools: Kismet, NetStumbler
- De-authentication and Denial of Service (DoS) Attacks
- Wi-Fi Hacking Prevention: Best Practices and Encryption Methods
- Wireless Network Configuration and Security

Module 10: Cloud Computing and Virtualization

- Introduction to Cloud Computing and Virtualization
- Types of Cloud Service Models: IaaS, PaaS, SaaS
- Cloud Hacking Techniques and Vulnerabilities
- Attacks on Virtualization Platforms (VMware, Hyper-V)
- Cloud Security Best Practices
- Penetration Testing in Cloud Environments

Module 11: Cryptography and Encryption

- Introduction to Cryptography and its Role in Security
- Symmetric and Asymmetric Encryption Algorithms
- Hashing Algorithms and Digital Signatures
- SSL/TLS and VPNs: Protecting Data in Transit
- Cryptographic Attacks: Man-in-the-Middle (MitM), Replay Attacks
- Using Tools for Cryptanalysis

Module 12: Penetration Testing Methodology

- Penetration Testing Lifecycle and Methodology
- Information Gathering and Scanning
- Vulnerability Analysis and Exploitation
- Reporting and Remediation of Findings
- Tools and Frameworks for Penetration Testing: Metasploit, Kali Linux, Nessus
- Creating and Delivering a Penetration Testing Report

Module 13: Cybersecurity Laws, Policies, and Ethics

- Overview of Cybersecurity Laws and Regulations
- Ethical Hacking Standards and Legal Constraints
- Confidentiality, Integrity, and Availability (CIA Triad)
- Privacy Laws: GDPR, HIPAA, and Other Compliance Regulations
- Best Practices for Legal and Ethical Hacking

Module 14: Final Project and Exam Preparation

- Hands-on Practical Penetration Testing Project
- Simulating Real-World Ethical Hacking Scenarios
- Preparing for the CEH Certification Exam: Tips and Strategies
- Practice Tests and Final Review