

## EC-Council CEHv9 Certification



### Course Outline

#### 1. Introduction to Ethical Hacking

- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts
- Hacking Phases
- Types of Attacks
- Information Security Controls

#### 2. Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting Threats
- Footprinting Methodology
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Penetration Testing

#### 3. Scanning Networks

- Overview of Network Scanning
- CEH Scanning Methodology

#### 4. Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- UNIX/Linux Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Enumeration Countermeasures
- SMB Enumeration Countermeasures
- Enumeration Pen Testing

#### 5. System Hacking

- Information at Hand Before System Hacking Stage
- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- CEH System Hacking Steps

#### 6. Trojans and Backdoors

- Trojan Concepts
- Trojan Infection
- Types of Trojans
- Trojan Detection
- Countermeasures
- Anti-Trojan Software
- Pen Testing for Trojans and Backdoors

#### 7. Viruses and Worms

- Virus and Worms Concepts
- Types of Viruses
- Computer Worms
- Malware Analysis
- Counter-measures
- Penetration Testing for Virus

#### 8. Sniffing

- Sniffing Concepts
- MAC Attacks
- DHCP Attacks
- ARP Poisoning
- Spoofing Attack
- DNS Poisoning
- Sniffing Tools

- Counter measures
- Sniffing Pen Testing

## 9. Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques
- Imperso-nation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures
- Social Engineering Pen Testing

## 10. Denial of Service

- DoS/DDoS Concepts
- DoS Attack Techniques
- Botnet
- DDoS Case Study
- DoS Attack Tools
- Counter-measures
- DoS/DDoS Protection Tools
- Denial-of-Service (DoS) Attack Penetration Testing

## 11. Session Hijacking

- Session Hijacking Concepts
- Network-level Session Hijacking
- Session Hijacking Tools
- Counter-measures
- Session Hijacking Pen Testing

## 12. Hacking Webservers

- Webserver Concepts
- Webserver Attacks
- Attack Methodology
- Webserver Attack Tools
- Counter-measures
- Patch Management
- Webserver Security Tools
- Webserver Pen Testing

## 13. Hacking Web Applications

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

## 14. SQL Injection

- SQL Injection Concepts

- Testing for SQL Injection
- Types of SQL Injection
- Blind SQL Injection
- SQL Injection Methodology
- Advanced SQL Injection
- Evasion Techniques
- Counter-measures

## 15. Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Counter-measures
- Wireless Security Tools
- Wi-Fi Pen Testing

## 16. Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Hacking Windows Phone OS
- Hacking BlackBerry
- Mobile Device Management (MDM)
- Mobile Security Guidelines and Tools
- Mobile Pen Testing

## 17. Evading IDS, Firewalls and Honeypots

- IDS, Firewall and Honeypot Concepts
- IDS, Firewall and Honeypot System
- Evading IDS
- Evading Firewalls
- Detecting Honeypots
- Firewall Evading Tools
- Countermeasures
- Penetration Testing

## 18. Buffer Overflows

- Buffer Overflow Concepts
- Buffer Overflow Methodology
- Buffer Overflow Examples
- Buffer Overflow Detection
- Buffer Overflow Counter-measures
- Buffer Overflow Security Tools
- Buffer Overflow Penetration Testing

## 19. Cryptography



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

## **20. Penetration Testing**

- Pen Testing Concepts
- Types of Pen Testing
- Pen Testing Techniques
- Pen Testing Phases
- Pen Testing Roadmap
- Outsourcing Pen Testing Services