

CEH Syllabus

Module 01 - Introduction to Ethical Hacking

- 01 - Information Security Overview
- 02 - Information Security Threats and Attack Vectors
- 06 - Penetration Testing Concepts
- 03 - Hacking Concepts
- 04 - Ethical Hacking Concepts
- 05 - Information Security Controls
- 07 - Information Security Laws and Standards

Module 02 - Footprinting and Reconnaissance

- 01 - Footprinting Concepts
- 02 - Footprinting through Search Engines
- 03 - Footprinting through Web Services
- 04 - Footprinting through Social Networking Sites
- 05 - Website Footprinting
- 06 - Email Footprinting
- 07 - Competitive Intelligence
- 08 - Whois Footprinting
- 09 - DNS Footprinting
- 10- Network Footprinting
- 11- Footprinting through Social Engineering
- 12 - Footprinting Tools
- 13 - Countermeasures
- 14 - Footprinting Pen Testing



Module 03 - Scanning Networks

- 01 - Network Scanning Concepts
- 02 - Scanning Tools
- 03 - Scanning Techniques
- 04 - Scanning Beyond IDS and Firewall
- 05 - Banner Grabbing
- 06 - Draw Network Diagrams
- 07 - Scanning Pen Testing

Module 04 - Enumeration

- 01 - Enumeration Concepts
- 02 - NetBIOS Enumeration
- 03 - SNMP Enumeration
- 04 - LDAP Enumeration
- 05 - NTP Enumeration
- 06 - SMTP Enumeration and DNS Enumeration
- 07 - Enumeration Countermeasures
- 08 - Other Enumeration Techniques
- 09 - Enumeration Pen Testing

Module 05 - Vulnerability Analysis

- 01 - Vulnerability Assessment Concepts
- 02 - Vulnerability Assessment Solutions
- 03 - Vulnerability Scoring Systems
- 04 - Vulnerability Assessment Tools
- 05 - Vulnerability Assessment Reports



Module 06 - System Hacking

- 01 - System Hacking Concepts
- 02 - Cracking Passwords
- 03 - Escalating Privileges
- 04 - Executing Applications
- 05 - Hiding Files
- 06 - Covering Tracks
- 07 - Penetration Testing

Module 07 - Malware Threats

- 01 - Malware Concepts
- 02 - Trojan Concepts
- 03 - Virus and Worm Concepts
- 04 - Malware Analysis
- 05- Countermeasures
- 06- Anti-Malware Software
- 07- Malware Penetration Testing

Module 08 - Sniffing

- 01- Sniffing Concepts
- 02- Sniffing Technique: MAC Attacks
- 03- Sniffing Technique: DHCP Attacks
- 04- Sniffing Technique: ARP Poisoning
- 05- Sniffing Technique: Spoofing Attacks
- 06- Sniffing Technique: DNS Poisoning
- 07- Sniffing Tools
- 08- Countermeasures
- 09- Sniffing Detection Techniques
- 10- Sniffing Pen Testing



Module 09- Social Engineering

- 01 - Social Engineering Concepts
- 02 - Social Engineering Techniques
- 03- Insider Threats
- 04 - Impersonation on Social Networking Sites
- 05 - Identity Theft
- 06 - Countermeasures
- 07 - Social Engineering Penetration Testing

Module 10- Denial-of-Service

- 01 - DoS/DDoS Concepts
- 02 - DoS/DDoS Attack Techniques
- 03 - Botnets
- 04 - DDoS Case Study
- 05 - DoS/DDoS Attack Tools
- 06 - Countermeasures
- 07 - DoS/DDoS Protection Tools
- 08 - DoS/DDoS Attack Penetration Testing

Module 11- Session Hijacking

- 01- Session Hijacking Concepts
- 02- Application Level Session Hijacking
- 03- Network Level Session Hijacking
- 04- Session Hijacking Tools
- 05- Countermeasures
- 06- Penetration Testing



Module 12 - Evading IDS, Firewalls, and Honeypots

01- IDS, Firewall, and Honeypot Concepts

02- IDS, Firewall, and Honeypot Solutions

03- Evading IDS

04- Evading Firewalls

05- IDS/Firewall Evading Tools

06- Detecting Honeypots

07- IDS/Firewall Evasion Countermeasures

08- Penetration Testing

Module 13- Hacking Web Servers

01- Web Server Concepts

02- Web Server Attacks

03- Web Server Attack Methodology

04- Web Server Attack Tools

05- Countermeasures

06- Patch Management

07- Web Server Security Tools

08- Web Server Pen Testing

Module 14- Hacking Web Applications

01 - Web App Concepts

02 - Web App Threats

03 - Hacking Methodology

04 - Web Application Hacking Tools

05 - Countermeasures

06 - Web App Security Testing Tools

07 - Web App Pen Testing



Module 15- SQL Injection

- 01 - SQL Injection Concepts
- 02 - Types of SQL Injection
- 03 - SQL Injection Methodology
- 04 - SQL Injection Tools
- 05 - Evasion Techniques
- 06 - Countermeasures

Module 16- Hacking Wireless Networks

- 01 - Wireless Concepts
- 02 - Wireless Encryption
- 03 - Wireless Threats
- 04 - Wireless Hacking Methodology
- 05 - Wireless Hacking Tools
- 06 - Bluetooth Hacking
- 07 - Countermeasures
- 08 - Wireless Security Tools
- 09 - Wi-Fi Pen Testing

Module 17- Hacking Mobile Platforms

- 01- Mobile Platform Attack Vectors
- 02- Hacking Android OS
- 03- Hacking iOS
- 04- Mobile Spyware
- 05- Mobile Device Management
- 06- Mobile Security Guidelines and Tools
- 07- Mobile Pen Testing



Module 18- IoT Hacking

- 01- IoT Concepts
- 02- IoT Attacks
- 03- IoT Hacking Methodology
- 04- IoT Hacking Tools
- 05- Countermeasures
- 06- IoT Pen Testing

Module 19- Cloud Computing

- 01 - Cloud Computing Concepts
- 02 - Cloud Computing Threats
- 03 - Cloud Computing Attacks
- 04 - Cloud Security
- 05 - Cloud Security Tools
- 06 - Cloud Penetration Testing

Module 20- Cryptography

- 01- Cryptography Concepts
- 02- Encryption Algorithms
- 03- Cryptography Tools
- 04- Public Key Infrastructure (PKI)
- 05- Email Encryption
- 06- Disk Encryption
- 07- Cryptanalysis
- 08- Countermeasures

