



BULLETPROOF

Education Services

EC-Council Certified Ethical Hacker (CEH) v9.0

In 18 comprehensive modules, the course covers 270 attack technologies, commonly used by hackers. Throughout the CEH course, you will be immersed in a hacker's mindset, evaluating not just logical, but physical security.

Length Days: 5 | **Length Hours: 40**

TARGET AUDIENCE

The Certified Ethical Hacking v9.0 course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

COURSE OUTLINE

1 - INTRODUCTION TO ETHICAL HACKING

- Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds
- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts, Types, and Phases
- Ethical Hacking Concepts and Scope
- Information Security Controls
- Information Security Laws and Standards

2 - FOOTPRINTING AND RECONNAISSANCE

- Footprinting Concepts
- 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
- LDAP Enumeration
- NTP Enumeration
- SMTP 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
- Hiding Files
- Covering Tracks
- Penetration Testing

6 - MALWARE THREATS

- Introduction to Malware
- Trojan Concepts
- Types of Trojans
- Virus and Worms Concepts
- Malware Reverse Engineering
- Malware Detection
- Countermeasures
- Anti-Malware Software
- Penetration Testing

7 - SNIFFING

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

- Follow TCP Stream in Wireshark
- Display Filters in Wireshark
- Additional Wireshark Filters
- Sniffing Tool
- Packet Sniffing Tool: Capsa Network Analyzer
- Network Packet Analyzer
- Counter measures
- Sniffing Detection Techniques
- Sniffing Pen Testing

8 - SOCIAL ENGINEERING

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures
- Penetration Testing

9 - DENIAL-OF-SERVICE

- DoS/DDoS Concepts
- DoS/DDoS Attack Techniques
- Botnets
- DDoS Case Study
- DoS/DDoS Attack Tools
- Counter-measures
- DoS/DDoS Protection Tools
- DoS/DDoS Attack Penetration Testing

10 - SESSION HIJACKING

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

11 - HACKING WEBSERVERS

- Webserver Concepts
- Webserver Attacks
- Attack Methodology
- Webserver Attack Tools

- Counter-measures
- Patch Management
- Webserver Security Tools
- Webserver Pen Testing

12 - HACKING WEB APPLICATIONS

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

13 - SQL INJECTION

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Evasion Techniques
- Counter-measures

14 - 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

15 - 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

16 - EVADING IDS, FIREWALLS, AND HONEYPOTS

- IDS, Firewall and Honeypot Concepts
- IDS, Firewall and Honeypot System
- Evading IDS
- Evading Firewalls
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Counter-measures
- Penetration Testing

17 - CLOUD COMPUTING

- Introduction to Cloud Computing
- Cloud Computing Threats
- Cloud Computing Attacks
- Cloud Security
- Cloud Security Tools
- Cloud Penetration Testing

18 - CRYPTOGRAPHY

- Market Survey 2014: The Year of Encryption
- Case Study: Heartbleed
- Case Study: Poodlebleed
- Cryptography Concepts
- Encryption Algorithms
- Cryptography Tools
- Public Key Infrastructure(PKI)
- Email Encryption
- Disk Encryption
- Cryptography Attacks
- Cryptanalysis Tools