



Certified Ethical Hacker v9

Course Outline



Program Overview

CEH v9 is a comprehensive ethical hacking and information systems security auditing program that focuses on latest security threats. It consists of practical real-time demonstration of latest hacking techniques, methodologies, tricks, and security measures. The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Students need to pass the online exam to receive CEH certification.

Duration

5 - Day Program

Learning Objectives

At the end of this training, participants will be able to:

- Key issues plaguing the information security world, incident management process, and penetration testing
- Various types of footprinting, footprinting tools, and countermeasures
- Network scanning techniques and scanning countermeasures
- Enumeration techniques and enumeration countermeasures
- System hacking methodology, steganography, steganalysis attacks, and covering tracks
- Different types of Trojans, Trojan analysis, and Trojan countermeasures
- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures
- Packet sniffing techniques and how to defend against sniffing
- Social Engineering techniques, identify theft, and social engineering countermeasures
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
- Session hijacking techniques and countermeasures
- Different types of webserver attacks, attack methodology, and countermeasures
- Different types of web application attacks, web application hacking methodology, and countermeasures
- SQL injection attacks and injection detection tools
- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi-fi security tools
- Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools
- Packet sniffing techniques and how to defend against sniffing
- Social Engineering techniques, identify theft, and social engineering countermeasures
- Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures
- Various cloud computing concepts, threats, attacks, and security techniques and tools
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools
- Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap



What You Get:

- CEH v9 Certification exam voucher
- 5 days of high quality classroom training
- 18 comprehensive modules
- 40% of class hours dedicated to labs
- 270 attack techniques
- 1685 slides
- More than 2,200 tools
- Certified EC-Council Instructor
- Course Completion Certificate
- Lunch, morning and afternoon refreshments
- Access to EC-Council Student Portal

About the Exam

- 125 questions
- 4 hours
- Multiple choice
- 70% passing score

Target Audience

- security officers / auditors
- security professionals
- site administrators
- anyone who is concerned about the integrity of their network infrastructure

Prerequisites:

- Basic networking knowledge
- MCSE or CCNA certification beneficial, but not required



Program Structure and Outline

Introduction to Ethical Hacking

- 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

Footprinting and Reconnaissance

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

Scanning Networks

- Overview of Network Scanning
- CEH Scanning Methodology

Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- Enumeration Countermeasures
- SMB Enumeration Countermeasures
- Enumeration Pen Testing

System Hacking

- Information at Hand Before System Hacking Stage
- System Hacking: Goals
- CEH System Hacking Steps



- Hiding Files
- Covering Tracks
- Penetration Testing

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

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
- Packet Sniffing Tool: Capsa Network Analyzer
- Network Packet Analyzer
- Counter measures
- Sniffing Detection Techniques
- Display Filters in Wireshark

Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites



SPARTAN

Allied Services

Deliver Results - Create Value

- Identity Theft
- Social Engineering Countermeasures
- Penetration Testing

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

Session Hijacking

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

Hacking Webservers

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

Hacking Web Applications

- Web App Concepts
- Web App Threats
- Web App Hacking Methodology



SPARTAN

Allied Services

Deliver Results - Create Value

- Web Application Hacking Tools
- Countermeasures
- Security Tools
- Web App Pen Testing

SQL Injection

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

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

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



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

Cloud Computing

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

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



Why Choose SAS Management Inc.

We Deliver Results

SAS Management Inc. has consistently proven its capability to deliver and exceed our clients' expectations. We are the only PEOPLECERT® Accredited Training Organization (ATO) in the Philippines. Our pool of consultants and trainers are seasoned industry veterans who have above average qualifications and certifications such as Business Management, Process Improvement, and Organizational Development Programs.

We Create Value

SAS Management Inc. believes in ensuring that our services meet the intended needs of our clients. To us, it is more than just providing training and consulting but rather ensuring that these are the things that our clients really need. This is why SAS Management Inc. is probably the only training provider that does a thorough needs assessment prior to providing a proposal. Our goal for every proposal is to CREATE VALUE for your organization.

SAS Management, Inc. is affiliated and endorsed by the following organizations:

