



Certified Ethical Hacker (CEH v11)

Course Objective :

CEH is the world's most advanced ethical hacking course covering 20 of the most important security domains any individual will need when they are planning to beef-up the information security posture of their organization.

This course provides you with the tools and techniques used by hackers and information security professionals alike to break into any computer system. This course will immerse you into a "Hacker Mindset" in order to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver's seat with a hands-on training environment employing a systematic ethical hacking process.

You will learn how to scan, test, hack and secure target systems. The course covers the Five Phases of Ethical Hacking, diving into Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

Prerequisite:

Participants should be familiar with :

- Basic computer literacy & Basic PC operating system navigation skills
- Basic Internet usage skills & Basic IP address knowledge
- Understanding of network fundamentals

Training Methodology & Materials:

- Practical hands-on sessions, 70% lab-based and 30% theory-based.
- Additional and well-designed labs handouts are given to enhance further enhance the courseware given.

Certificate Of Attendance :

Certificate Of Attendance will be awarded to participants completing the course achieving minimum 75% attendance.

Training Duration:

Full-Time : 5 Weekdays or 5 Sats
Time : 9am - 6pm

Course Fee:

Normal Course Fee : S\$2500
Regn Fee : S\$50

Certified Ethical Hacker Certification Exam

This course will help the participants to prepare for the **CEH** Exam.
Exam Code : 312-50 (Pearson VUE).

* Course fee includes 1 CEH Exam voucher

All fees subject to prevailing GST.
Call us to check on latest promotion.

DETAILED COURSE OUTLINE

Module 01: Introduction to Ethical Hacking

- 1.1 Information Security Overview
- 1.2 Cyber Kill Chain Concepts
- 1.3 Hacking Concepts
- 1.4 Ethical Hacking Concepts
- 1.5 Information Security Controls
- 1.6 Information Security Laws and Standards

Module 02 : Footprinting and Reconnaissance

- 2.1 Footprinting Concepts
- 2.2 Footprinting through Search Engines
- 2.3 Footprinting through Web Services
- 2.4 Footprinting through Social Networking Sites
- 2.5 Website Footprinting
- 2.6 Email Footprinting
- 2.7 Whois Footprinting
- 2.8 DNS Footprinting
- 2.9 Network Footprinting
- 2.10 Footprinting through Social Engineering
- 2.11 Footprinting Tools
- 2.12 Footprinting Countermeasures

Module 03 : Scanning Networks

- 3.1 Network Scanning Concepts
- 3.2 Scanning Tools
- 3.3 Host Discovery
- 3.4 Port and Service Discovery

- 3.5 OS Discovery (Banner Grabbing/OS Fingerprinting)
- 3.6 Scanning Beyond IDS and Firewall
- 3.7 Draw Network Diagrams

Module 04: Enumeration

- 4.1 Enumeration Concepts
- 4.2 NetBIOS Enumeration
- 4.3 SNMP Enumeration
- 4.4 LDAP Enumeration
- 4.5 NTP and NFS Enumeration
- 4.6 SMTP and DNS Enumeration
- 4.7 Other Enumeration Techniques
- 4.8 Enumeration Countermeasures

Module 05: Vulnerability Analysis

- 5.1 Vulnerability Assessment Concepts
- 5.2 Vulnerability Classification and Assessment Types
- 5.3 Vulnerability Assessment Solutions and Tools
- 5.4 Vulnerability Assessment Reports

Module 06: System Hacking

- 6.1 System Hacking Concepts
- 6.2 Gaining Access
- 6.3 Escalating Privileges
- 6.4 Maintaining Access
- 6.5 Clearing Logs

Module 07: Malware Threats

- 7.1 Malware Concepts
- 7.2 ATP Concepts
- 7.3 Trojan Concepts
- 7.4 Virus and Worm Concepts
- 7.5 Fileless Malware Analysis
- 7.6 Malware Analysis
- 7.7 Countermeasures
- 7.8 Anti-Malware Software

Module 08: Sniffing

- 8.1 Sniffing Concepts
- 8.2 Sniffing Technique: MAC Attacks
- 8.3 Sniffing Technique: DHCP Attacks
- 8.4 Sniffing Technique: ARP Poisoning
- 8.5 Sniffing Technique: Spoofing Attacks
- 8.6 Sniffing Technique: DNS Poisoning
- 8.7 Sniffing Tools
- 8.8 Sniffing Detection Techniques

Module 09: Social Engineering

- 9.1 Social Engineering Concepts
- 9.2 Social Engineering Techniques
- 9.3 Insider Threats
- 9.4 Impersonation on Social Networking Sites
- 9.5 Identity Theft
- 9.6 Countermeasures

Module 10: Denial-of-Service

- 10.1 DoS/DDoS Concepts
- 10.2 DoS/DDoS Attack Techniques
- 10.3 Botnets
- 10.4 DDoS Case Study
- 10.5 DoS/DDoS Attack Tools
- 10.6 Countermeasures
- 10.7 DoS/DDoS Protection Tools

Module 11: Session Hijacking

- 11.1 Session Hijacking Concepts
- 11.2 Application Level Session Hijacking
- 11.3 Network Level Session Hijacking
- 11.4 Session Hijacking Tools
- 11.5 Countermeasures

Module 12: Evading IDS, Firewalls and Honeypots

- 12.1 IDS, IPS, Firewall and Honeypot Concepts
- 12.2 IDS, IPS, Firewall and Honeypot Solutions
- 12.3 Evading IDS
- 12.4 Evading Firewalls
- 12.5 IDS/Firewall Evading Tools
- 12.6 Detecting Honeypots
- 12.7 IDS/Firewall Evasion Countermeasures

Module 13: Hacking Web Servers

- 13.1 Web Server Concepts
- 13.2 Web Server Attacks
- 13.3 Web Server Attack Methodology
- 13.4 Web Server Attack Tools
- 13.5 Countermeasures
- 13.6 Patch Management
- 13.7 Web Server Security Tools

Module 14: Hacking Web Applications

- 14.1 Web Application Concepts
- 14.2 Web Application Threats
- 14.3 Web Application Hacking Methodology
- 14.4 Web API, Webhooks and Web Shell
- 14.5 Web Application Security

Module 15: SQL Injection

- 15.1 SQL Injection Concepts
- 15.2 Types of SQL Injection
- 15.3 SQL Injection Methodology
- 15.4 SQL Injection Tools
- 15.5 Evasion Techniques
- 15.6 Countermeasures

Module 16: Hacking Wireless Networks

- 16.1 Wireless Concepts
- 16.2 Wireless Encryption
- 16.3 Wireless Threats
- 16.4 Wireless Hacking Methodology
- 16.5 Wireless Hacking Tools
- 16.6 Bluetooth Hacking
- 16.7 Countermeasures
- 16.8 Wireless Security Tools

Module 17: Hacking Mobile Platforms

- 17.1 Mobile Platform Attack Vectors
- 17.2 Hacking Android OS
- 17.3 Hacking iOS
- 17.4 Mobile Device Management
- 17.5 Mobile Security Guidelines and Tools

Module 18: IoT and OT Hacking

- 18.1 IoT Hacking
- 18.2 IoT Concepts
- 18.3 IoT Attacks
- 18.4 IoT Hacking Methodology
- 18.5 IoT Hacking Tools
- 18.6 Countermeasures
- 18.7 OT Hacking
- 18.8 OT Concepts
- 18.9 OT Attacks
- 18.10 OT Hacking Methodology
- 18.11 OT Hacking Tools
- 18.12 Countermeasures

Module 19: Cloud Computing

- 19.1 Cloud Computing Concepts
- 19.2 Container Technology
- 19.3 Serverless Computing
- 19.4 Cloud Computing Treats
- 19.5 Cloud Hacking
- 19.6 Cloud Security

Module 20: Cryptography

- 20.1 Cryptography Concepts
- 20.2 Encryption Algorithms
- 20.3 Cryptography Tools
- 20.4 Public Key Infrastructure (PKI)
- 20.5 Email Encryption
- 20.6 Disk Encryption
- 20.7 Cryptanalysis
- 20.8 Countermeasures



Certified Ethical Hacker CEH v11



IT Enabler Consultancy Pte Ltd

(Co Reg No. 200211025Z)

35 Selegie Road #09-06 Parklane Shopping Mall Singapore 188307 | Tel: 6333 4843 | Fax: 6333 4883 | www.ienabler.com.sg