Tel. +39 02 365738
info@overneteducation.it
www.overneteducation.it

EC001-V

EC-Council Certified Ethical Hacker (CEHv11) - VIRTUAL

Durata: 32 Ore

Descrizione

Nell'iscrizione a calendario è incluso il Kit CEHv11 che comprende:

- •2 student digital books
- •1 lab manual
- •Accesso della durata di 1 anno alla piattaforma ASPEN per usare gli strumenti online di supporto alla formazione
- •1 voucher per il relativo esame di certificazione con validità 1 anno

Il corso Certified Ethical Hacker (C|EH v11) è un corso riconosciuto a livello internazionale. Dalla sua creazione nel 2003, il corso Certified Ethical Hacker si è ampiamente diffuso nel mondo, si tratta di una certificazione riconosciuta e accreditata in conformità ANSI 17024, che dà credibilità e valore aggiunto ai membri certificati. È ora disponibile in versione 11. Il corso è stato aggiornato per fornire agli studenti gli strumenti e le tecniche utilizzate da hackers e professionisti della sicurezza, allo scopo di poter entrare in qualsiasi sistema informativo. Il programma farà immedesimare i partecipanti “nella mentalità dell’Hacker”, cioè insegnerà a pensare come un Hacker e difendersi meglio.
Gli studenti comprenderanno come scansionare, testare e proteggere un sistema. Il corso copre le 5 fasi dell’Ethical Hacking: “Reconnaissance, Gaining Access, Enumeration, Maintaining Access and Covering your tracks”.
Il corso è organizzato in una parte di aula con il docente e una parte in autoapprendimento. Il docente, all’inizio del corso, fornirà i dettagli delle parti da studiare in autoapprendimento.

A chi è rivolto?

- •Information Security Analyst / Administrator
- •Information Assurance (IA) Security Officer
- •Information Security Manager / Specialist
- •Information Systems Security Engineer / Manager
- •Information Security Professionals / Officers
- •Information Security / IT Auditors
- •Risk / Threat / Vulnerability Analyst
- •System Administrators
- •Network Administrators and Engineers

Prerequisiti

Consigliati:

- •conoscenza del protocollo TCP / IP
- •conoscenza base del sistema operativo Windows
- •conoscenza base del sistema operativo LINUX

Contenuti

Module 01: Introduction to Ethical Hacking

- •Information Security Overview
- •Cyber Kill Chain Concepts
- •Hacking Concepts
- •Ethical Hacking Concepts
- •Information Security Controls
- •Information Security Laws and Standards

Module 02: Footprinting and Reconnaissance

- •Footprinting Concepts
- •Footprinting through Search Engines
- •Footprinting through Web Services
- •Footprinting through Social Networking Sites
- •Website Footprinting
- •Email Footprinting
- •Whois Footprinting
- •DNS Footprinting
- •Network Footprinting
- •Footprinting through Social Engineering
- •Footprinting Tools
- •Footprinting Countermeasures

Module 03: Scanning Networks

- •Network Scanning Concepts
- •Scanning Tools
- •Host Discovery
- •Port and Service Discovery
- •OS Discovery (Banner Grabbing/OS Fingerprinting)
- •Scanning Beyond IDS and Firewall
- •Draw Network Diagrams

Module 04: Enumeration

- •Enumeration Concepts
- •NetBIOS Enumeration
- •SNMP Enumeration
- •LDAP Enumeration
- •NTP and NFS Enumeration
- •SMTP and DNS Enumeration
- •Other Enumeration Techniques
- •Enumeration Countermeasures

Module 05: Vulnerability Analysis

- •Vulnerability Assessment Concepts
- •Vulnerability Classification and Assessment Types
- •Vulnerability Assessment Solutions and Tools

- •Vulnerability Assessment Reports

Module 06: System Hacking

- •System Hacking Concepts
- •Gaining Access
- •Escalating Privileges
- •Maintaining Access
- •Clearing Logs

Module 07: Malware Threats

- •Malware Concepts
- •APT Concepts
- •Trojan Concepts
- •Virus and Worm Concepts
- •Fileless Malware Concepts
- •Malware Analysis
- •Countermeasures
- •Anti-Malware Software

Module 08: Sniffing

- •Sniffing Concepts
- •Sniffing Technique: MAC Attacks

- •Sniffing Technique: DHCP Attacks
- •Sniffing Technique: ARP Poisoning
- •Sniffing Technique: Spoofing Attacks
- •Sniffing Technique: DNS Poisoning
- •Sniffing Tools Countermeasures
- •Sniffing Detection Techniques

Module 09: Social Engineering

- •Social Engineering Concepts
- •Social Engineering Techniques
- •Insider Threats
- •Impersonation on Social Networking Sites
- •Identity Theft
- •Countermeasures

Module 10: Denial-of-Service

- •DoS/DDoS Concepts
- •DoS/DDoS Attack Techniques
- •Botnets
- •DDoS Case Study
- •DoS/DDoS Attack Tools
- •Countermeasures
- •DoS/DDoS Protection Tools

Module 11: Session Hijacking

- •Session Hijacking Concepts Application Level Session Hijacking
- •Network Level Session Hijacking
- •Session Hijacking Tools
- •Countermeasures

Module 12: Evading IDS, Firewalls, and Honeypots

- •IDS, IPS, Firewall, and Honeypot Concepts
- •IDS, IPS, Firewall, and Honeypot Solutions
- •Evading IDS
- •Evading Firewalls
- •IDS/Firewall Evading Tools
- •Detecting Honeypots
- •IDS/Firewall Evasion Countermeasures

Module 13: Hacking Web Servers

- •Web Server Concepts
- •Web Server Attacks
- •Web Server Attack Methodology
- •Web Server Attack Tools
- •Countermeasures

- Patch Management
- Web Server Security Tools

Module 14: Hacking Web Applications

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web API, Webhooks, and Web Shell
- Web Application Security

Module 15: SQL Injection

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Evasion Techniques
- Countermeasures

Module 16: Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology

- •Wireless Hacking Tools
- •Bluetooth Hacking
- •Countermeasures
- •Wireless Security Tools

Module 17: Hacking Mobile Platforms

- •Mobile Platform Attack Vectors
- •Hacking Android OS
- •Hacking iOS
- •Mobile Device Management
- •Mobile Security Guidelines and Tools

Module 18: IoT and OT Hacking

- •IoT Hacking
- •IoT Concepts
- •IoT Attacks
- •IoT Hacking Methodology
- •IoT Hacking Tools
- •Countermeasures
- •OT Hacking
- •OT Concepts
- •OT Attacks

- •OT Hacking Methodology
- •OT Hacking Tools
- •Countermeasures

Module 19: Cloud Computing

- •Cloud Computing Concepts
- •Container Technology
- •Serverless Computing
- •Cloud Computing Threats
- •Cloud Hacking
- •Cloud Security

Module 20: Cryptography

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

Appendix A: Ethical Hacking Essential Concepts - I

- •Operating System Concepts
- •File Systems
- •Computer Network Fundamentals
- •Basic Network Troubleshooting
- •Virtualization
- •Network File System (NFS)
- •Web Markup and Programming Languages
- •Application Development Frameworks and Their Vulnerabilities
- •Web Subcomponents
- •Database Connectivity

Appendix B: Ethical Hacking Essential Concepts - II

- •Information Security Controls
- •Network Segmentation
- •Network Security Solutions
- •Data Leakage
- •Data Backup
- •Risk Management Concepts
- •Business Continuity and Disaster Recovery
- •Cyber Threat Intelligence
- •Threat Modeling
- •Penetration Testing Concepts

- Security Operations
- Forensic Investigation
- Software Development Security
- Security Governance Principles
- Asset Management and Security

Certificazioni

Il corso è propedeutico per i seguenti esami:

- 312-50 - Certified Ethical Hacker