



## CEH - CERTIFIED ETHICAL HACKER WITH AI - EC-Council

EC-Council - Offensive Cybersecurity - Cyber Security

Durata:

**5 Giorni**

Lingue:

**Italiano**

Certificazione:

**CEH v13 AI**

### ITCore Group

Via Balestra, 12  
6900 Lugano (CH)  
+41.091.9760019  
[www.itcoregroup.com](http://www.itcoregroup.com)

Via Lanino, 36  
21047 Saronno (VA)  
+39.02.84108669  
[www.itcoregroup.com](http://www.itcoregroup.com)

## Descrizione del corso

Il corso CEH v13 è basato sull'intelligenza artificiale, è ed la prima certificazione di hacking etico al mondo che sfrutta la potenza dell'intelligenza artificiale.

Permette di conoscere le tecniche basate sull'intelligenza artificiale per aumentare l'efficienza della difesa informatica del 40%, semplificando al contempo il proprio flusso di lavoro.

Il nuovo programma di studi è stato aggiornato e arricchito di contenuti per poter meglio padroneggiare le più recenti tecniche di attacco ed imparare le ultime tendenze nelle contromisure.

### Obiettivi del corso:

Il corso prevede un iter formativo fortemente interattivo nel quale verrà mostrato come effettuare scanning, testing e hacking dei propri sistemi al fine di renderli più sicuri. L'impiego di laboratori ed esercitazioni pratiche è mirato a dare una conoscenza approfondita unita all'esperienza concreta sui fondamentali sistemi di sicurezza.

Il corso entra nel futuro della sicurezza informatica con una formazione che integra l'intelligenza artificiale in tutte le fasi dell'hacking etico.

Una prima fase importante è dedicata a comprendere il funzionamento delle difese perimetrichi e verranno mostrati e condotti degli scanning e attacchi alle proprie reti.

Una seconda fase è dedicata ad apprendere le tecniche impiegate dagli intrusi per l'escalation dei privilegi e quali passi possono essere attuati per mettere in sicurezza un sistema.

Approfondimenti specifici sono dedicati all'intrusion detection, alla policy creation, al social engineering, agli attacchi DDoS, ai buffer overflow e alla creazione di virus.

### Destinatari:

Professionisti, che già lavorano come sistemisti o programmati, che aspirano a diventare ethical hacker come arricchimento del proprio bagaglio di competenze e per cogliere le opportunità del mercato del lavoro che sempre più richiede questa figura.

### Prerequisiti:

- Conoscenza del protocollo TCP/IP
- Conoscenza di base dei sistemi operativi Windows
- Conoscenza di base dei sistemi operativi Linux

### ITCore Group

Via Balestra, 12  
6900 Lugano (CH)  
+41.091.9760019  
[www.itcoregroup.com](http://www.itcoregroup.com)

Via Lanino, 36  
21047 Saronno (VA)  
+39.02.84108669  
[www.itcoregroup.com](http://www.itcoregroup.com)

## Programma

- **Module 01: Introduction to Ethical Hacking**

Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

- **Module 02: Footprinting and Reconnaissance**

Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking

- **Module 03: Scanning Networks**

Learn different network scanning techniques and countermeasures.

- **Module 04: Enumeration**

Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.

- **Module 05: Vulnerability Analysis**

Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included.

- **Module 06: System Hacking**

Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.

- **Module 07: Malware Threats**

Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.

- **Module 08: Sniffing**

Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.

- **Module 09: Social Engineering**

Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

- **Module 10: Denial-of-Service**

### ITCore Group

Via Balestra, 12  
6900 Lugano (CH)  
+41.091.9760019  
[www.itcoregroup.com](http://www.itcoregroup.com)

Via Lanino, 36  
21047 Saronno (VA)  
+39.02.84108669  
[www.itcoregroup.com](http://www.itcoregroup.com)

Learn about different Denial of Service (DoS) and Distributed DoS(DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

- **Module 11: Session Hijacking**

Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

- **Module 12: Evading IDS, Firewalls, and Honeypots**

Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

- **Module 13: Hacking Web Servers**

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

- **Module 14: Hacking Web Applications**

Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures.

- **Module 15: SQL Injection**

Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.

- **Module 16: Hacking Wireless Networks**

Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.

- **Module 17: Hacking Mobile Platforms**

Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

- **Module 18: IoT Hacking**

Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.

- **Module 19: Cloud Computing**

Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security

**ITCore Group**

Via Balestra, 12  
6900 Lugano (CH)  
+41.091.9760019  
[www.itcoregroup.com](http://www.itcoregroup.com)

Via Lanino, 36  
21047 Saronno (VA)  
+39.02.84108669  
[www.itcoregroup.com](http://www.itcoregroup.com)

techniques and tools.

- **Module 20: Cryptography**

Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

**ITCore Group**

Via Balestra, 12  
6900 Lugano (CH)  
+41.091.9760019  
[www.itcoregroup.com](http://www.itcoregroup.com)

Via Lanino, 36  
21047 Saronno (VA)  
+39.02.84108669  
[www.itcoregroup.com](http://www.itcoregroup.com)