CEH - CERTIFIED ETHICAL HACKER WITH AI - EC-Council

EC-Council - Offensive Cybersecurity - Cyber Security

Durata:	Lingue:	Certificazione:
5 Giorni	**Italiano**	**CEH v13 AI**

Descrizione del corso

The CEH v13 course is based on artificial intelligence and is the world's first ethical hacking certification to harness the power of artificial intelligence. It teaches AI-based techniques to increase cyber defense efficiency by 40% while streamlining your workflow.
The new curriculum has been updated and enriched with content to better master the latest attack techniques and learn the latest trends in countermeasures.

Focus:
The course features a highly interactive training program that demonstrates how to scan, test, and hack systems to make them more secure. Labs and practical exercises are designed to provide in-depth knowledge combined with hands-on experience with fundamental security systems.
The course delves into the future of cybersecurity with training that integrates artificial intelligence into all phases of ethical hacking.
A first, important phase is dedicated to understanding how perimeter defenses work, and scanning and attacks on your networks will be demonstrated and conducted.
A second phase focuses on the techniques used by intruders to escalate privileges and the steps that can be taken to secure a system.
Specific in-depth studies are dedicated to intrusion detection, policy creation, social engineering, DDoS attacks, buffer overflows, and virus creation.
Prerequisites:

- Knowledge of TCP/IP
- Basic Knowledge of Windows operative system
- Basic Knowledge of Linux operative system

ITCore Group

Via Balestra, 12
6900 Lugano (CH)
+41.091.9760019
www.itcoregroup.com

Via Lanino, 36
21047 Saronno (VA)
+39.02.84108669
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**

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

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.