Certified Ethical Hacker (CEH) v13

CODICE	**DT0100**
DURATA	**5 gg**
PREZZO	**3.390,00 €**
EXAM	

DESCRIZIONE

Il primo programma di cybersecurity sul mercato a integrare l'IA!

Il programma Certified Ethical Hacker (CEH) v13 si distingue per l'integrazione completa dell'IA in tutte le fasi dell'ethical hacking, offrendo ai partecipanti un aumento del 40% dell'efficienza e una produttività raddoppiata.

A differenza del CEHv12, il CEHv13 include strumenti e tecniche di IA per automatizzare il rilevamento delle minacce, prevedere le violazioni della sicurezza e rispondere rapidamente agli incidenti, oltre a offrire competenze per proteggere le tecnologie basate sull'IA.

Il programma comprende 221 laboratori pratici, oltre 550 tecniche di attacco e l'utilizzo di più di 4.000 strumenti di hacking. Riconosciuta a livello globale e accreditata da organizzazioni come il DoD statunitense e l'ANAB, la CEH è la certificazione leader a livello mondiale nel campo dell'ethical hacking da oltre 20 anni!

Cosa ti offre il corso C|EH

CEH Methodology

La formazione CEHv13 offre un programma completo di cybersecurity. Questa certificazione di hacking etico si basa su quattro punti fondamentali: Imparare, Certificare, Impegnarsi e Sfidare - (Learn, Certify, Engage and Compete). Questa metodologia in 4 fasi vi fornirà una grande quantità di risorse di apprendimento, laboratori, tecnologie e tecniche attuali, simulazioni il più possibile accurate e sfide mensili per farvi confrontare con la realtà del settore.

Quali sono le novità del CEHv13?

1. Integrazione dell'intelligenza artificiale
2. Efficienza e produttività
3. Hacking dei sistemi di intelligenza artificiale

4. Nuovi strumenti di IA
5. Nuovi laboratori pratici
6. Ambiente di cyber range basato su cloud
7. Competizioni CTF globali

Queste nuove caratteristiche rendono il CEHv13 un programma di formazione avanzato e completo, adatto alle sfide odierne della cybersecurity.

TARGET

Questa formazione si rivolge ai responsabili sicurezza, agli auditor, ai professionisti della sicurezza, agli amministratori di siti ma anche a tutte le persone coinvolte nelle problematiche di stabilità dei sistemi informativi.

PREREQUISTI

Conoscenza di base del protocollo TCP/IP.

- Conoscenza di base dei sistemi operativi Windows.
- Conoscenza di base dei sistemi operativi Linux.

CONTENUTI

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