CEH – Certified Ethical Hacker v13

EC-Council

Com certificação

- **Nível:** Intermédio
- **Duração:** 40h

Sobre o curso

Progride na carreira com o Certified Ethical Hacker (CEH), agora com novas capacidades de IA (Inteligência Artificial).

O **Certified Ethical Hacker (CEH)** oferece uma compreensão aprofundada das fases de hacking ético, vários vetores de ataque e medidas preventivas. O CEH v13, agora potenciado com capacidades de IA, vai ensinar como os hackers pensam e agem, para que cada profissional esteja melhor preparado para configurar a sua infraestrutura de segurança e defender-se de contra ataques. Ao fornecer uma compreensão das fraquezas e vulnerabilidades dos sistemas, o curso de CEH ajuda os formandos a aprenderem a proteger as suas organizações e a fortalecer os seus controlos de segurança, de forma a minimizar o risco de um ataque malicioso.

O CEH v13, potenciado com capacidades de IA, foi desenvolvido para incorporar um ambiente prático e um processo sistemático em cada domínio e metodologia de hacking ético, oferecendo-te a oportunidade de demonstrar os conhecimentos e competências necessários para obter a credencial CEH e desempenhar a função de hacker ético

Na sua 13.ª versão, o CEH continua a evoluir com os mais recentes sistemas operativos, ferramentas, táticas, exploits e tecnologias. O CEH v13 traz o poder da IA:

- Competências de Cibersegurança Impulsionadas por IA
- Aprende várias ferramentas de IA e GPT
- Aprendizagem Adaptativa
- Domina utilização de competências de IA.
- Automatização de tarefas repetitivas
- Relatórios Aprimorados
- Aprende a hackear sistemas de IA.

O que traz de novo a V13?

A mais recente versão adiciona as capacidades de IA. Estruturado em 20 módulos de aprendizagem que abrangem mais de 550 técnicas de ataque, o CEH fornece-te o conhecimento fundamental necessário para ter sucesso como profissional de Segurança Informática.

Sabia que:

- 92% dos empregadores preferem profissionais formados no curso CEH para empregos de hacking ético.
- Os módulos estão mapeados para mais de 45 funções na área da Segurança Informática.
- 4 em 5 empresas afirmam que a IA é uma prioridade estratégica.
- 1 em cada 2 profissionais recebeu promoções após o CEH.

Relatório Dados CEH 2023

Destinatários

Um Certified Ethical Hacker é um especialista que normalmente trabalha num ambiente *red-team*, que está focado em atacar sistemas e obter acesso a redes, aplicações, bases de dados e outros dados críticos em sistemas protegidos. Um CEH compreende as estratégias de ataque, diferentes ângulos de ataque e imita as estratégias de ataque de hackers mal-intencionados. Ao contrário de hackers maliciosos, os Ethical Hackers certificados operam com permissão dos proprietários do sistema e todas as precauções para garantir que os resultados permaneçam confidenciais. *Bug bounty researchers* são especialistas que usam suas competências de ataque para descobrir vulnerabilidades nos sistemas.

Destinatários:

- 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

Objetivos

Formandos participantes no curso de CEH vão aprender:

- Questões-chave que afetam o mundo da segurança da informação, metodologias e estruturas de hacking, controlos de segurança da informação, e leis e normas de segurança da informação.
- Diferentes tipos de footprinting, ferramentas de footprinting e medidas de contra-ataque.
- Técnicas de análise de redes e medidas de contra-ataque para análise.
- Técnicas de enumeração e medidas de contra-ataque à enumeração.
- Diferentes tipos de avaliação de vulnerabilidades e ferramentas para avaliação de vulnerabilidades.
- Metodologia de hacking de sistemas

- Diferentes tipos de malware (Trojan, vírus, worms, etc.), APT (Ameaças Persistentes Avançadas) e malware sem ficheiros, procedimentos de análise de malware e medidas de contra-ataque ao malware.
- Várias técnicas de captura de pacotes e medidas de contra-ataque à captura.
- Técnicas de engenharia social, roubo de identidade e medidas de contra-ataque.
- Técnicas de ataque DoS/DDoS, botnets, ferramentas de ataque DDoS e medidas de contra-ataque a DoS/DDoS.
- Técnicas de sequestro de sessão e medidas de contra-ataque.
- Firewall, IDS (Sistema de Detecção de Intrusões), IPS (Sistema de Prevenção de Intrusões), honeypot, NAC (Controlo de Acesso à Rede) e técnicas de evasão de endpoint, ferramentas de evasão e medidas de contra-ataque.
- Diferentes tipos de ataques a servidores web, aplicações web e APIs web, metodologia de hacking, ferramentas de hacking e medidas de contra-ataque.
- Ataques de injeção SQL, metodologia de injeção, técnicas de evasão e medidas de contra-ataque à injeção SQL.
- Diferentes tipos de encriptação sem fios, ameaças sem fios, metodologia de hacking sem fios, ferramentas de hacking sem fios, ferramentas de segurança Wi-Fi e medidas de contra-ataque.
- Vetores de ataque em plataformas móveis, hacking em Android e iOS, gestão de dispositivos móveis, diretrizes de segurança móvel e ferramentas de segurança.
- Diferentes tipos de ataques a IoT e OT, metodologia de hacking, ferramentas de hacking e medidas de contra-ataque.
- Várias tecnologias de computação em cloud, ameaças à computação em cloud, ataques, metodologia de hacking (AWS, Microsoft Azure, Google Cloud e hacking de contêineres), e técnicas e ferramentas de segurança.
- Diferentes tipos de algoritmos de encriptação, ferramentas de criptografia, aplicações da criptografia, ataques à criptografia e ferramentas de criptoanálise
- Hacking ético impulsionado através de IA.

Condições

Mensalidades (apenas para particulares): Taxa de inscrição de 10% + pagamento do valor restante em prestações flexíveis, sem juros, à escolha do cliente, através do parceiro Cofidis Pay. (Sujeito a aprovação, consulta-nos para mais informações).

Pré-requisitos

- Experiência em segurança informática
- Fortes conhecimentos práticos de TCP/IP

Metodologia

A **formação presencial ou live training** permite juntar o apoio do formador ao benefício de colaborar com os

restantes formandos, seus pares na segurança informática, desenvolvendo competências aplicáveis no mundo real.

- 40 horas de formação presencial ou live training 100% online sincrona
- 20 módulos de formação que vão ajudar a dominar os fundamentos de Ethical Hacking e preparar para o exame de certificação
- Mais de 220 laboratórios renovados que simulam cenários reais
- Mais de 3500 ferramentas utilizadas habitualmente por *hackers* para poder praticar as mais recentes vulnerabilidade
- Manual digital com mais de 3000 páginas especialmente desenhados para apreender aprofundadamente conceitos de segurança informática.

O que está incluído na versão CEH Elite?

- eCourseware
- Knowledge Exame
- Exame Prático
- 6 Meses de acesso aos laboratórios oficiais
- Acesso ao CEH Engage
- Acesso ao CEH Compete
- Acesso a 10 Ethical Hacking Video Library
- 1 Retake incluído de Knowledge Exame

CERTIFICAÇÃO O exame C|EH pode ser realizado após a conclusão do curso completo e oficial C|EH. Os candidatos quem passem no exame receberão o seu certificado C|EH e privilégios associados. Este curso inclui o voucher para o exame CEH – *Certified Ethical Hacker* v13 exam (312-50). Os objetivos da certificação CEH são:

- Definir e gerir os padrões mínimos para a certificação de profissionais especialistas em Segurança Informática, em *ethical hacking*.
- Informar o público da existência de profissionais certificados, que cumprem ou excedem os padrões mínimos.
- Reforçar o *Ethical Hacking* como uma profissão única e autoreguladora.

Exame:

- Certified Ethical Hacker (ANSI)
- Número de perguntas: 125
- Duração: 4 horas
- Formato de teste: Escolha múltipla
- Prefixo do exame: 312-50

O exame EC-Council incluido no valor do curso deve ser obrigatoriamente realizado presencialmente, num dos centros de Exames GALILEU/Rumos. Caso não tenha disponibilidade ou não pretenda realizar o exame de forma presencial e prefira uma solução remota acresce uma taxa de 89€ ao valor do curso. **Contacte-nos,** caso tenha alguma dúvida específica sobre os exames. **Consultar Informação acerca dos Exames**

Programa

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

Introduction to Ethical Hacking

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

Foot Printing and Reconnaissance

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

Scanning Networks

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

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 included as well.

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.

Malware Threats

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

Sniffing

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

Social Engineering

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

Denial-of-Service

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

Session Hijacking

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

Evading IDS, Firewalls, and Honeypots

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

Hacking Web Servers

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

Hacking Web Applications

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

SQL Injection

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

Hacking Wireless Networks

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

Hacking Mobile Platforms

Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

IoT and OT Hacking

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

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.

Cryptography

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