CEH – Ethical Hacking and Countermeasures Pro v12

EC-Council

Com certificação

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

Sobre o curso

Certified Ethical Hacker (CEH) é a certificação de ethical hacking mais prestigiada e recomendada pelos empregadores a nível mundial. É a mais desejada certificação em ciber segurança e representa uma das credenciais valorizadas e também exigidas para profissionais que administrem infraestruturas críticas.

Desde o lançamento do CEH em 2003, esta certificação é reconhecida como um padrão dentro da comunidade de segurança da informação. A mais recente versão do CEH v12 continua a apresentar as técnicas de hacking mais recentes e as ferramentas e *exploits* mais avançadas utilizadas por hackers e profissionais de segurança da informação atualmente. As cinco fases de ethical hacking e a missão central original do CEH permanece válida e relevante hoje: ***"To beat a hacker, you need to think like a hacker"***

O CEH v12 cobre mais de 500 novas ameaças e cenários de vulnerabilidade. Inlcuindo APT, Fileless Malware, Web API Threats, Webhooks, Web Shell, OT Attacks, Cloud Attacks, AI, ML, e muito mais. Os conteúdos estão apenas focados em tecnologias recentes, mas também em tecnologias emergentes, como OT Technology e Container Technology.

Atualizações mais recentes do C|EH® v12:

- New Learning Methodology: Learn – Certify – Engage – Compete
- Compete: new challenges every month to test your job-ready skills!
- 100% Compliance to NICE 2.0 Framework
- Based on a comprehensive industry-wide job-task analysis
- Hands-on learning labs
- Practice Range
- Global C|EH community competitions
- Cheat Sheet

- Coverage of the latest malware
- Lab-intensive program (Every learning objective is demonstrated using labs)
- Hands-on program (More than 50% of training time is dedicated to labs)
- Lab environment simulates a real-time environment(Lab setup simulates real-life networks and platforms)
- Covers the latest hacking tools (Based on Windows, macOS, and Linux)
- Latest OS covered and a patched testing environment
- All the tool screenshots are replaced with the latest version
- All the tool listing slides are updated with the latest tools
- All the countermeasure slides are updated

Consulte a brochura oficial do curso

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

Construa sua carreira com a certificação de segurança informática mais requisitada do mundo!

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 Pro?

- eCourseware
- Voucher de Exame
- Acesso à próxima versão do eCourseware
- 6 Meses de acesso aos laboratórios oficiais
- Acesso ao C|EH Engage
- Acesso a 5 Ethical Hacking Video Library
- 3 Tentativas de Exame. Este benefício fornece aos candidatos o respectivo voucher de exame no portal ECC EXAM, mas exclui as taxas administrativas que serão aplicadas a cada tentativa de 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* v12 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.

Programa

- Introduction to Ethical Hacking
- Foot Printing 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 Hacking
- Cloud Computing
- Cryptography

Introduction to Ethical Hacking
Cover 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 foot printing 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, such as 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.

System Hacking
Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover
system and network vulnerabilities.

Malware Threats
Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.

Sniffing
Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as 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.

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
Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi sedcurity tools, and countermeasures.

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 IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

Cloud Computing
Learn different cloud computing concepts, such as container technologies and server less computing, various cloud computing threats, attacks, hacking methodology, 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.