

Ethical Hacking and Countermeasures v11 (CEH)

- **Formato do curso:** Presencial e Live Training
- **Localidade:** Live Training
- **Com certificação:** EC-Council Certified Ethical Hacking (CEH)
- **Data:** 04 Jul. 2022 a 08 Jul. 2022
- **Preço:** 1900€
- **Horário:** Laboral - das 9h00 às 18h00
- **Nível:** Intermédio
- **Duração:** 40 horas

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 v11 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 v11 cobre mais de 500 novas ameaças e cenários de vulnerabilidade. Incluindo 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.

Esta nova versão inclui as mais recentes táticas de análise de malware para ransomware, malware bancário e financeiro, botnets IoT, análise de malware OT, malware Android entre outras tais como:

- Incorporating Parrot Security OS
- Re-Mapped to NIST/NICE Framework
- Enhanced Cloud Security, IoT, and OT Modules
 - Cloud-Based Threats
 - IoT Threats
 - Operational Technology (OT) Attacks
- Modern Malware Analysis
- Covering the Latest Threats - Fileless Malware
- New Lab Designs and Operating Systems

- Increased Lab Time and Hands-on Focus
- Industry's Most Comprehensive Tools Library

O curso inclui o respetivo exame de certificação, a ser obrigatoriamente realizado presencialmente, num dos centros de Exames Rumos ou Galileu. Caso opte pela modalidade remota terá de suportar um custo adicional de 75€ + IVA (Isenção do valor do IVA a particulares) .

Este curso também está disponível no formato E-Learning. Para mais informações aceda ao link: [Ethical Hacking and Countermeasures v11 \(CEH\)](#)

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

Pré-requisitos

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

Metodologia

A **formação presencial / 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 / live training
- Mais de 140 laboratórios digitais que simulam cenários reais
- Mais de 2200 ferramentas utilizadas habitualmente por *hackers*
- Mais de 1685 slides, ricos em gráficos e informação, e especialmente desenhados para apreender aprofundadamente conceitos de segurança informática.

Certificação

O exame C|EH pode ser realizado após a conclusão do curso completo e oficial C|EH. Os candidatos que passem no exame receberão o seu certificado C|EH e privilégios associados.

Este curso inclui um voucher para o exame CEH – *Certified Ethical Hacker v11* 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 curso inclui o respetivo exame de certificação, a ser obrigatoriamente realizado presencialmente, num dos centros de Exames Rumos ou Galileu. Caso opte pela modalidade remota terá de suportar um custo adicional de 75€ + IVA (Isenção do valor do IVA a particulares) .

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 Hacking
- Cloud Computing
- Cryptography