Penetration Tester

Infrastructure - Cibersegurança

Live Training (também disponível em presencial)

Com certificação

- **Localidade:**
- **Data:** 25 Sep 2024
- **Preço:** 2585 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Pós-Laboral das 2ª, 4ª e 6ª feiras das 18h45 às 22h15
- **Nível:** Intermédio
- **Duração:** 126h

Sobre o curso

Esta Academia combina o conhecimento teórico com aplicação prática, capacitando os formandos a enfrentarem desafios reais em cibersegurança e prepararem-se para a certificação internacional CEH Practical, como reconhecimento internacional das competências.

Com um programa abrangente, os formandos vão abordar técnicas essenciais e críticas para se tornarem especialistas em teste de penetração. Esta academia está direcionada para quem procura destacar-se no universo da cibersegurança e entrar na mente de um *hacker*, através do domínio de técnicas avançadas em *ethical hacking* e testes de intrusão em redes e sistemas. Ao atingir estes objetivos, os formandos estarão aptos a enfrentar desafios reais, contribuindo para um ambiente digital mais seguro na sociedade.

Razões para frequentar esta Academia?

- Formação imersiva e com forte componente prática nos principais domínios de ataque e defesa em cibersegurança
- 3 Certificações reconhecidas internacionalmente
- Os melhores profissionais certificados do mercado como formadores
- Possibilidade de estágio no final da formação
- Formação qualificada

Inclui a Certificação:

- CEH: Certified Ethical Hacking – Practical

Saídas Profissionais:

- Penetration & Vulnerability Tester
- Pentester
- Especialista de Cibersegurança

Destinatários

- Destina-se a todos os interessados em aprofundar os seus conhecimentos de redes e sistemas com especialização em cibersegurança.
- Profissionais se cibersegurança que pretendam obter a certificação CEH: Certified Ethical Hacker – Practical

---

Objetivos

- **Dominar conceitos e framework de cibersegurança:** Compreender os princípios fundamentais de segurança cibernética e aplicar um framework robusto para avaliação e mitigação de riscos.
- **Desenvolver competências práticas em Ethical Hacking e Penetration Testing:** Adquirir conhecimentos teóricos e práticos em técnicas avançadas de Ethical Hacking para identificar e corrigir vulnerabilidades e realizar testes de penetração intrusivos.
- **Preparação para Certificação CEH (Practical):** Proporcionar uma preparação abrangente e eficaz para o exame de certificação CEH (Practical)
- **Aplicar conhecimentos alinhados com as necessidades das organizações:** Capacitar os participantes a aplicar os conhecimentos adquiridos na implementação de estratégias de defesa cibernética eficazes em ambientes reais.

Condições

- Taxa de inscrição: 290€, dedutível no valor total do curso.
- Formandos não residentes no território nacional, terão de efetuar um pagamento de 50% do valor total da propina no momento da inscrição.
- Inscrições a título particular de pessoas que se encontrem em situação de desemprego, beneficiam de um desconto de 10%, mediante apresentação de comprovativo da situação atual (não acumulável com outras campanhas em vigor).
- Condições especiais para Alumni de Academias ou Pós-graduações GALILEU.
- Os valores apresentados não incluem IVA. Isenção do valor do IVA a particulares.

Modalidades de Pagamento

- Pronto pagamento: Liquide o valor total do curso no momento da inscrição e beneficie de um desconto adicional de 5%.
- Cofidis Pay: Financie o seu curso em até 12 prestações mensais sem juros, com um valor máximo de 2.500€. (Sujeito a aprovação, consulte as condições com a GALILEU.)

Desconto – Profissionais em situação de desemprego

- **10% de desconto** válido **para inscrições a título particular de pessoas que se encontrem em situação de desemprego**, para o efeito, será solicitado **documento comprovativo da situação atual –** Não acumulável com outras campanhas em vigor.

Pré-requisitos

- Conhecimentos de Inglês técnico: é aconselhável que o formando seja capaz de compreender manuais técnicos na língua inglesa;
- Conhecimentos técnicos em redes e sistemas ao nível dos conhecimentos que se adquirem na Academia Técnico de Informática;
- O percurso não apresenta quaisquer pré-requisitos a nível de habilitações académicas ou experiência profissional.

Metodologia

- Constituído por módulos de formação, integrados numa ótica de sessões mistas de teoria e prática.
- Serão elaborados exercícios e simulações de situações práticas garantindo uma aprendizagem mais eficaz.
- Os conteúdos ministrados durante o percurso foram desenvolvidos pela Rumos, em consulta a organizações parceiras, e são devidamente acompanhados por material didáctico, distribuídos aos participantes.
- Existem ainda, ao longo da Academia, momentos de autoestudo onde serão facultados guiões, ou materiais, que servirão como um roteiro valioso durante a jornada individual de aprendizagem do formando.

Composição:

- 126 Horas de Formação
- 5 Ações de Formação TI
- 1 Ação de Preparação para Exame
- 1 Exame de Certificação
- Momentos de auto-estudo

Exame de Certificação

Este rigoroso exame prático, pretende validar a aplicação dos conhecimentos de técnicas em ethical hacking.

Através de cenários reais simulados, o candidato terá acesso a uma rede corporativa através de máquinas virtuais, redes e aplicações em tempo real, projetado para testar as competências e demonstrar a aplicação dos seus conhecimentos e encontrar soluções em desafios reais.

- 1 exame de certificação: CEH (Pratical) – Realização apenas disponível em formato remoto;
- O voucher do exame CEH Practical deverá ser resgatado pelo formando durante a realização da frequência do respetivo módulo CEH e após o resgate o formando tem 1 ano para realizar o exame;
- As datas são sugeridas pela GALILEU, no entanto, a marcação é feita pelo formando no momento em que se sentir preparado para tal;
- A marcação deve ser efetuada com 10 dias úteis de antecedência à data pretendida.

Programa

- NIST Cybersecurity Framework
- Autoestudo dedicado a Fundamentos de PowerShell e Scripting
- Systems Hardening
- Noções básicas de direito + Lei do Cibercrime
- Autoestudo dedicado a Linux for Ethical Hackers
- Ethical Hacking and Penetration Testing
- Practical Ethical Hacking - CEH
- APE: Ação de Preparação para Exame CEH (Practical)

Apresentação

Sessão de boas-vindas para esclarecimento de todos os processos e procedimentos existentes.

NIST Cybersecurity Framework (21h)

A primeira etapa para quem está a iniciar-se ou a especializar-se em cibersegurança, é conhecer as boas práticas reconhecidamente eficazes pelos profissionais.

Este módulo foca-se no “NIST Cybersecurity Framework”, uma abordagem estruturada desenvolvida pelo National Institute of Standards and Technology (NIST) dos Estados Unidos da América, destinada a auxiliar organizações na melhoria da sua postura de cibersegurança. O NIST é uma agência governamental encarregada de promover e desenvolver padrões em várias áreas, incluindo a cibersegurança. O “NIST Cybersecurity Framework” foi concebido em resposta às ameaças digitais crescentes, visando fortalecer a resiliência de organizações públicas e privadas contra ciberataques. Este framework consiste em diretrizes, padrões e melhores práticas que orientam as organizações no planeamento, implementação, monitorização e aperfeiçoamento das suas medidas de cibersegurança.

Programa:

- Introduction to Cybersecurity
- What is the NIST Cybersecurity Framework, and how can it be used by an organization
- History and Creation of the Framework
- Uses and Benefits of the Framework

- Cybersecurity Framework Components
- The Six Functions of the Framework
    - Govern
    - Identify
    - Protect
    - Detect
    - Respond
    - Recover
- Other related frameworks and standards

Autoestudo dedicado a Fundamentos de PowerShell e Scripting

Neste momento de autoestudo, pretende-se que os formandos possam adquirir os conceitos fundamentais de PowerShell que atualmente são utilizados em ferramentas de exploração de sistemas Windows, bem como uma primeira abordagem ao desenvolvimento de scripts.

Programa:

- Introduction to PowerShell
- Introduction to scripting in PowerShell
- Create and run scripts by using Windows PowerShell

Systems Hardening (28h)

O Systems Hardening consiste na utilização de ferramentas, técnicas e boas práticas para proteger sistemas informáticos contra ciberataques. Neste módulo vamos aprender a mitigar os riscos, eliminando potenciais vetores de ataque e minimizando a superfície de ataque à segurança dos sistemas.

Programa:

- Introduction to Systems Hardening
- Security Baselines
- Security Protocols and Specifications
- Vulnerability Assessment Tools
- Tools for assessment, measurement, and enforcement of security baselines
- Systems Hardening
- Application hardening
- Operating system hardening
- Endpoint hardening
- Server hardening
- Database hardening
- Network hardening

Noções básicas de direito + Lei do Cibercrime (7h)

Neste módulo iremos dar a conhecer os pontos chave da legislação em vigor relacionados com a cibersegurança e quais as consequências do seu não cumprimento.

Programa:

- Noções básicas de direito
- Lei do Cibercrime

Autoestudo dedicado a Linux for Ethical Hackers

Neste momento de autoestudo, serão facultados conteúdos de aproximadamente duas horas em formato de vídeo, que servirão como um guia individual de aprendizagem aos sistemas Linux através da distribuição Kali Linux.

Programa:

- Installing VMWare/Kali Linux
- Kali Linux Overview
- Navigating the File System
- Users and Privilegies
- Common Network Commands
- Viewing, Creating, and Editing Files
- Starting and Stopping Services
- Installing and Updating Tools
- Advanced Bash-Scripting

Ethical Hacking and Penetration Testing (31,5h)

Contrariamente aos hackers maliciosos, os ethical hackers atuam com a devida autorização dos proprietários do sistema, tomando todas as precauções necessárias para assegurar a confidencialidade dos resultados.

Este módulo pretende dotar os formandos com as técnicas de hacking mais recentes e as técnicas de pentest mais avançadas utilizadas pelos hackers e profissionais de segurança informática, para que possam conhecer as ameaças e os cenários de vulnerabilidade que são originados pelos vários tipos de ataques, podendo assim criar estratégias de defesa e mitigar futuros ataques.

Programa:

- Introdução ao Hacking Ético
- Reconhecimento, Scanning e Enumeração
- System Hacking: Análise de Vulnerabilidades; Password Cracking; Acesso aos Sistemas e Esconder o Rasto
- Sniffing
- Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS)
- Ameaças com Malware
- Engenharia Social
- Ténicas de evasão aos sistemas de Segurança
- Ataques a Web Servers e Web Applications (inclui Session Hijacking)
- SQL Injection
- Ataques a redes Wireless
- Ataques a Dispositivos Móveis
- Ataques a Cloud Computing

- Ataques a dispositivos IoT
- Ataques a plataformas OT
- Criptografia – algoritmos e ferramentas

Practical Ethical Hacking (35h)

Neste curso inteiramente prático, os formandos vão aplicar várias técnicas e também preparar-se para o exame prático de CEH da EC-Council. Este curso oferece uma experiência prática em técnicas avançadas de hacking ético, capacitando profissionais para identificar, avaliar e fortalecer sistemas contra ameaças.

Programa:

- Attack vectors
- Perform network scanning
- Identify live and vulnerable machines in a network
- OS banner grabbing
- Service
- User emulation
- System hacking
- Steganography
- Steganalysis attacks
- Cover attacks
- Identify and use viruses
- Computer worms
- Malware to exploit systems
- Packet sniffing
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Cryptography attacks
- Security loopholes
- Communication infrastructure
- End systems

Ação de Preparação para Exame Pratical CEH (3,5h)

Tem como objetivo preparar os formandos o exame prático de CEH da EC-Council, esclarecendo dúvidas/questões bem como alertar para cuidados a que devem ser levados em conta, na altura em que se está envolvido no processo de exame.