Penetration Tester

Infrastructure - Cibersegurança

Live Training (também disponível em presencial)

Com certificação

- **Localidade:**
- **Data:** 23 Jan 2025
- **Preço:** 2585 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Pós-laboral e Sábados das 3ª e 5ª feiras 18h45 às 22h15 e sábados das 9h30 às 13h00
- **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 CompTIA PenTest+, 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 mercado de trabalho ao desenvolver competências práticas em testes de penetração, avaliação e gestão de vulnerabilidades.

Ao atingir estes objetivos, os formandos estarão aptos a enfrentar desafios reais e determinar a resistência a ataques, contribuindo para um ambiente digital mais seguro na sociedade.

Razões para frequentar esta Academia?

- 1 Certificação reconhecida Internacionalmente.
- Os melhores profissionais certificados do mercado como formadores.
- Formação qualificada, através da Rumos, uma das empresas líderes na área da formação e distinguida “Marca n.º 1 na Escolha dos Profissionais” pela ConsumerChoice.
- Acesso ao Employability Hub, um serviço dedicado a apoiar a integração e a progressão de carreira dos formandos das Academias da Rumos. Oferecemos um acompanhamento personalizado, focado na maximização do teu posicionamento no mercado de trabalho.

Inclui a Certificação:

- **CompTIA PenTest+**
  Esta certificação reconhece profissionais de cibersegurança com competências práticas para identificar, mitigar e reportar vulnerabilidades em sistemas. Abrange todas as fases dos testes de penetração em diferentes superfícies de ataque, incluindo cloud, aplicações web, APIs e dispositivos IoT.

Saídas Profissionais:

- Penetration & Vulnerability Tester
- Pentester
- Especialista de Cibersegurança

Diagnóstico de Conhecimento:

- Faça a nossa avaliação gratuita para verificar se detém os conhecimentos base para garantir uma boa aprendizagem neste curso.

Destinatários

- Destina-se a todos os interessados em aprofundar os seus conhecimentos de redes e sistemas com especialização em cibersegurança.
- Profissionais TI que pretendem desenvolver competências de PenTesting e gestão de vulnerabilidades em redes
- Profissionais se cibersegurança que pretendam obter a certificação CompTIA PenTest+.

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 testes de penetração e gestão de vulnerabilidade em redes:** 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 CompTIA PenTest+:** Proporcionar uma preparação abrangente e eficaz para o exame de certificação mundialmente reconhecido e valorizado pelas organizações.
- **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 ou no Starting Point de Cibersegurança;
- 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 Hands-on Lab
- 1 Ação de Preparação para Exame
- 1 Exame de Certificação
- Momentos de auto-estudo

Exame de Certificação

O exame de certificação CompTIA PenTest+ deverá preferencialmente ser realizado no final do respetivo módulo de formação;
A data é sugerida pela Rumos, 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;
O exame tem de ser realizado até 6 meses após a data de fim da formação.

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
- CompTIA PenTest+ CertPrep
- Ethical Hacking for Mobile
- Try to Hack Me - Penetration Tester (Hands-on Lab)
- Ação de Preparação para Exame PenTest+

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 estabelece os alicerces para a compreensão estruturada da cibersegurança, através do estudo do NIST Cybersecurity Framework. Desenvolvido pelo National Institute of Standards and Technology (NIST), este referencial tem como objetivo auxiliar organizações a identificar, proteger, detetar, responder e recuperar de incidentes de segurança. Os formandos irão explorar os cinco pilares do framework e a sua aplicabilidade prática, bem como outros referenciais relevantes.

Competências desenvolvidas:

- Compreensão dos componentes e objetivos do NIST Framework
- Capacidade de aplicar o modelo às operações de segurança de uma organização
- Conhecimento das interligações entre o NIST e outras normas e frameworks

Programa:

- 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 Five Functions of the Framwork
    - Identify
    - Protect
    - Detect
    - Respond
    - Recover
    - Other related frameworks and standards

Autoestudo dedicado a Fundamentos de PowerShell e Scripting

Neste momento de autoestudo, os formandos serão introduzidos ao ambiente PowerShell, explorando os conceitos básicos de scripting e a execução de tarefas automatizadas. Este conhecimento é particularmente útil para administradores de sistemas e profissionais de segurança que operam em ambientes Microsoft, nomeadamente em contextos de análise, auditoria e exploração de sistemas.

Competências desenvolvidas:

- Execução de comandos em PowerShell
- Criação e execução de scripts simples
- Aplicação prática em tarefas de administração e segurança

Programa:

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

Systems Hardening (28h)

Neste módulo serão abordadas práticas e ferramentas destinadas à proteção proativa de sistemas, com foco na eliminação de vulnerabilidades e na aplicação de políticas de segurança robustas. Serão exploradas estratégias de hardening aplicadas a vários níveis — desde aplicações e sistemas operativos, até bases de dados, redes e endpoints. O módulo inclui ainda a utilização de ferramentas para avaliação e medição da conformidade com baselines de segurança.

Competências desenvolvidas:

- Compreensão dos conceitos e objetivos do hardening

- Aplicação de medidas práticas de endurecimento de sistemas
- Utilização de ferramentas de avaliação de segurança e benchmarks

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)

Este módulo tem como finalidade sensibilizar os formandos para o enquadramento legal da cibersegurança, nomeadamente através da introdução a conceitos básicos de direito e ao estudo da Lei do Cibercrime. Serão analisados os principais tipos legais, responsabilidades individuais e institucionais, bem como as implicações do incumprimento legal.

Competências desenvolvidas:

- Conhecimento do enquadramento jurídico da cibersegurança
- Compreensão da Lei do Cibercrime e das suas aplicações
- Consciência das responsabilidades legais na área da segurança da informação

Programa:

- Noções básicas de direito
- Lei do Cibercrime

Autoestudo dedicado a Linux for Ethical Hackers

Neste momento de autoestudo, os formandos serão introduzidos à utilização do Kali Linux, uma distribuição amplamente utilizada em testes de intrusão. O conteúdo inclui instalação, navegação no sistema de ficheiros, gestão de utilizadores e serviços, comandos de rede e introdução ao scripting em Bash.

Competências desenvolvidas:

- Familiarização com o ambiente Kali Linux
- Execução de comandos básicos de administração e redes
- Introdução ao desenvolvimento de scripts em Bash

Programa:

- Installing VMWare/Kali Linux
- Kali Linux Overview
- Navigating the File Systen
- Users and Privileges
- Common Network Commands
- Viewing, Creating, and Editing Files
- Sarting and Stopping Services
- Installing and Updating Tools
- AdvaScripting with Bash

CompTIA PenTest+ CertPrep (35h)

Neste módulo são abordadas as principais fases de um teste de intrusão: planeamento, reconhecimento, análise de vulnerabilidades, exploração e report. Os formandos vão utilizar ferramentas e técnicas modernas de Ethical Hacking, com o objetivo de compreender como os ataques ocorrem e como mitigá-los. É também dado ênfase à preparação para o exame CompTIA PenTest+ (PT0-003).

Competências desenvolvidas:

- Planeamento e execução de testes de penetração
- Exploração de vulnerabilidades em redes, aplicações e sistemas
- Elaboração de relatórios técnicos e comunicação de resultados

Programa:

- Introduction
- Penetration Testing
- Planning and Scoping Penetration Tests
- Information Gathering
- Vulnerability Scanning
- Analyzing Vulnerability Scans
- Exploit and Pivot
- Exploiting Network Vulnerabilities
- Exploiting Physical and Social Vulnerabilities
- Exploiting Application Vulnerabilities
- Exploiting Host Vulnerabilities
- Reporting and Communication
- Scripting for Penetration Testing

Ethical Hacking for Mobile (14h)

Este módulo aborda as particularidades da segurança em plataformas móveis, com especial enfoque no sistema operativo Android. Serão exploradas vulnerabilidades comuns em aplicações móveis, bem como técnicas de engenharia reversa, modificação de aplicações e análise estática e dinâmica. Os formandos irão preparar ambientes de teste realistas, utilizando dispositivos físicos e virtuais, e aplicar ferramentas como APKTool, MobSF e Burp Suite para identificar e explorar falhas de segurança.

Competências desenvolvidas:

- Identificação de vulnerabilidades e falhas de segurança em aplicações móveis
- Aplicação de técnicas de engenharia reversa e modificação de aplicações Android
- Utilização de ferramentas de análise estática e dinâmica em ambiente controlado

Programa:

- Preparação do ambiente para testes de aplicações móveis
- Utilização de dispositivos Android físicos e virtuais (AVDs)
- Arquitetura e componentes do sistema Android (Dalvik, ART, JNI)
- Modelo de permissões e segurança do Android
- Utilização da linha de comandos (CLI) para interação com o sistema
- Anatomia e estrutura de um pacote APK
- Engenharia reversa de aplicações Android
- Modificação, recompilação e assinatura de aplicações
- Ferramentas de engenharia reversa: APKTool, SMALI, Dex2jar, JD-GUI, apksigner
- Técnicas de bypass de controlos de segurança
- Análise automatizada com QARK e MobSF
- Instalação e configuração do Android Studio e Android Virtual Devices
- Integração do Burp Suite para análise dinâmica de tráfego
- Estudo de caso prático: identificação e exploração de vulnerabilidades em app simulada

Try to Hack Me – Penetration Tester (Hand-on Lab) (14h)

Este laboratório prático permite aos formandos aplicar técnicas e ferramentas utilizadas por equipas Red Team, através de desafios reais na plataforma “Try to Hack Me”. O foco está na exploração de vulnerabilidades, escalada de privilégios e reporte de falhas de segurança.

Competências desenvolvidas:

- Aplicação de técnicas de Ethical Hacking em ambiente simulado mas próximos dos reais
- Utilização prática de ferramentas de ataque
- Capacidade de análise e exploração de vulnerabilidades

Ação de Preparação para Exame CompTIA PenTest+ (7h)

Durante esta ação, serão revistos os conteúdos principais do exame, esclarecidas dúvidas e abordadas boas práticas para a realização da prova. Serão ainda partilhadas estratégias de gestão de tempo e de abordagem a questões típicas.

Competências desenvolvidas:

- Consolidação dos conhecimentos essenciais para o exame
- Identificação de áreas críticas a reforçar
- Preparação estratégica para certificação CompTIA PenTest+