OSCP Exam Preparation

Tecnologias de Informação - Segurança

- **Nível:** Intermédio
- **Duração:** 21h

Sobre o curso

A certificação OSCP (Offensive Security Certified Professional) é uma das mais prestigiadas e exigentes do mundo em cibersegurança ofensiva. Reconhecida globalmente, é altamente valorizada por equipas Red Team, consultoras de segurança, MSSPs e organizações que exigem profissionais capazes de executar testes de intrusão em cenários reais.

O curso **OSCP Exam Preparation** foi desenvolvido para apoiar profissionais com experiência prévia em ethical hacking a estruturarem o estudo, consolidarem competências práticas e treinarem em laboratórios semelhantes ao ambiente do exame.

Ao longo da formação, os formandos irão reforçar conhecimentos essenciais em enumeração, exploração, pós-exploração, escalada de privilégios, automação com scripts e buffer overflow, bem como praticar a elaboração de relatórios técnicos de acordo com o modelo exigido no exame.

Esta preparação prática e intensiva aumenta significativamente as probabilidades de sucesso, fornecendo um roteiro claro, exercícios orientados e simulações realistas.

O curso não inclui o voucher do exame OSCP. A inscrição e certificação devem ser feitas diretamente através da plataforma da Offensive Security.

Destinatários

- Profissionais certificados em CEH, CompTIA PenTest+ ou outras formações de ethical hacking que pretendam aprofundar competências práticas e obter uma certificação internacional de referência.
- Técnicos de segurança com experiência equivalente em redes, sistemas operativos e fundamentos de ethical hacking.
- Candidatos ao exame OSCP que necessitem de apoio estruturado para organização do estudo e treino em ambiente prático.

Objetivos

- Aplicar técnicas e metodologias de Penetration Testing com foco no exame OSCP.
- Reconhecer e explorar vulnerabilidades em sistemas Linux e Windows.
- Automatizar tarefas com Bash e Python.
- Executar elevação de privilégios manual e através de scripts de enumeração.
- Documentar e apresentar evidências técnicas em relatórios formais.
- Gerir tempo e estratégia de ataque segundo o modelo do exame.
- Praticar em laboratórios semelhantes ao ambiente real do OSCP.

Condições

Para particulares

• 10% do valor total pago no ato da inscrição; restante valor até 7 dias antes do início do curso.

• Formandos não residentes em Portugal: pagamento de 50% no ato da inscrição.

• Possibilidade de pagamento em até 12 prestações mensais sem juros via Cofidis Pay (até 2.500€, sujeito a aprovação).

• Possibilidade de beneficiar do Cheque Formação+Digital até 750€ (conforme elegibilidade).

• Isenção de IVA para particulares.

Para empresas

• Empresas nacionais: pagamento a 30 dias, contra fatura (acresce IVA à taxa legal em vigor).

• Empresas da UE e fora da UE: valores isentos de IVA e pagamento a pronto.

Pré-requisitos

- Conhecimentos sólidos de redes TCP/IP, Linux e Windows.
- Familiaridade com comandos CLI e ferramentas como Nmap, Netcat, Burp Suite.
- Experiência básica em scripting (Bash, Python).
- Recomenda-se vivência prévia com ambientes de laboratório como TryHackMe ou Hack The Box.

Programa

- Fundamentos Técnicos e Estratégia de Preparação
- Technical Lab: Essential Skills for OSCP
- Information Gathering e Scanning
- Technical Lab: Discovery & Enumeration
- Gaining Access
- Technical Lab: Initial Access Techniques
- Linux Privilege Escalation
- Technical Lab: Privilege Escalation - Linux
- Windows Privilege Escalation

- Technical Lab: Privilege Escalation - Windows
- Pós-exploração e Buffer Overflow (BOF) Básico
- Technical Lab: Buffer Overflow Essentials
- Estratégia de Exame e Escrita do Relatório Técnico
- Technical Lab: OSCP Reporting Simulation

Fundamentos Técnicos e Estratégia de Preparação

Neste módulo, os formandos vão rever os conhecimentos essenciais de redes, Linux, Windows e scripting, alinhar as expectativas e estabelecer um plano de estudo eficaz para a certificação OSCP.

- Estrutura e regras do exame OSCP
- Revisão técnica: Linux, redes, Windows, scripting
- Metodologia PTES e OSCP mindset
- Integração com TryHackMe e plano de estudo prático

Technical Lab: Essential Skills for OSCP

Neste laboratório, autónomo, serão reforçados os fundamentos técnicos e operacionais que serão exigidos em todas as fases do exame.

- Linux Fundamentals
- Network Services

Information Gathering e Scanning

Nesta sessão, os formandos vão dominar técnicas de reconhecimento e varrimento de redes/hosts como primeira fase do processo de pentesting.

- Reconhecimento passivo e ativo
- Nmap (scans, scripts, detecção de serviços)
- Gobuster, enumeração de diretórios, Nikto
- Enumeração de serviços típicos (FTP, SMB, DNS, etc.)

Technical Lab: Discovery & Enumeration

Neste laboratório, autónomo, será consolidado o processo de identificação e enumeração de alvos com ferramentas-chave para o exame.

- Nmap,
- Intro to Pentesting

Gaining Access

Os participantes vão aplicar técnicas manuais e automatizadas de exploração para obter acesso inicial a sistemas vulneráveis.

- Exploração com Metasploit
- Exploração manual de falhas comuns (RCE, LFI, uploads, brute force)

- Shells interativos, reverse shells

Technical Lab: Initial Access Techniques

Neste laboratório, autónomo, os participantes vão reforçar a abordagem manual e adaptativa à exploração, uma competência crítica no OSCP

- Vulnversity
- Simple CTF

Linux Privilege Escalation

Neste módulo, os participantes vão identificar e explorar caminhos de escalada de privilégios em sistemas Linux.

- LinPEAS e enumeração detalhada
- Técnicas de escalada: sudo, cron, SUID, PATH
- Enumeração manual e automação

Technical Lab: Privilege Escalation – Linux

Neste laboratório, autónomo, será treinada a capacidade de identificar vetores de escalada e interpretar resultados de scripts, essencial para obter os pontos extra no OSCP.

- Linux PrivEsc

Windows Privilege Escalation

Nesta sessão, os formandos vão aprender a aplicar técnicas de escalada de privilégios em sistemas Windows.

- WinPEAS e PowerUp
- Serviços vulneráveis, binários inseguros, tokens
- Password harvesting e abuso de permissões.

Technical Lab: Privilege Escalation – Windows

Este laboratório, autónomo, foca-se na análise pós-exploração e elevação de privilégios em ambientes Windows, que frequentemente surgem no exame.

- Windows PrivEsc Arena

Pós-exploração e Buffer Overflow (BOF) Básico

Esta sessão servirá para consolidar técnicas de pós-exploração e introduzir conceitos fundamentais de BOF.

- Recolha de credenciais
- Lateral movement básico
- Introdução ao buffer overflow: stack, EIP, padrões
- Ferramentas: Immunity Debugger, msf-pattern, mona.py.

Technical Lab: Buffer Overflow Essentials

Neste laboratório, autónomo, os formandos vão treinar a base mínima para resolver a máquina BOF exigida no OSCP, onde um exploit personalizado é necessário.

- Buffer Overflow Prep

Estratégia de Exame e Escrita do Relatório Técnico

Este módulo irá preparar os formandos para gerir o tempo e relatar de forma eficaz as explorações realizadas durante o exame.

- Plano de ataque para as 24h
- Estratégias de pontuação, gestão de stress
- Estrutura do relatório técnico: evidência, clareza, prova
- Ferramentas de documentação e templates.

Technical Lab: OSCP Reporting Simulation

Este laboratório, autónomo, irá simular o processo de documentação técnica conforme exigido no exame OSCP, com base numa exploração real feita no lab.

- Relatório sobre uma máquina