

CompTIA PenTest+ CertPrep (e-Learning)

CompTIA

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

Sobre o curso

Prepara-te para a certificação CompTIA PenTest+ e domina as principais fases de um teste de intrusão: planeamento, reconhecimento, análise de vulnerabilidades, exploração e report.

Neste curso, os formandos utilizam ferramentas e técnicas atuais de **Ethical Hacking** para compreender como ocorrem os ataques, identificar vulnerabilidades e aplicar medidas eficazes de mitigação.

A formação foi também desenvolvida para apoiar a preparação para o exame de certificação **CompTIA PenTest+**.

A certificação **CompTIA PenTest+** valida competências práticas para identificar, explorar, 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.

O exame de certificação CompTIA PenTest+ valida os conhecimentos e competências necessários para:

- Planear e definir o âmbito de uma atividade de teste de penetração;
- Compreender requisitos legais e de conformidade;
- Realizar análises de vulnerabilidades e testes de penetração com as ferramentas e técnicas adequadas;
- Analisar resultados e identificar medidas de correção;
- Produzir relatórios técnicos, comunicar resultados à equipa de gestão e apresentar recomendações práticas.

Este curso e-learning inclui:

- **Conteúdos formativos estruturados em e-learning:** Aprende e desenvolve competências de forma eficiente e autónoma, com conteúdos estruturados através de um modelo de progressão da aprendizagem. Este modelo ajuda-te a compreender conceitos e a desenvolver competências alinhadas com os objetivos do curso.
- **Vídeos e conteúdos interativos integrados:** Acede a explicações, demonstrações e exemplos no momento em que são mais relevantes para a tua aprendizagem.
- **Atividades em laboratório:** Realiza exercícios práticos em ambientes simulados e reais, com cenários próximos do contexto profissional e tarefas de nível básico e avançado.

- **Assessments e testes de preparação:** Valida os teus conhecimentos ao longo do curso através de avaliações e testes práticos.
 - **Voucher de exame e retake:** Inclui voucher de exame de certificação e a possibilidade de repetição em caso de reprovação.
-

Destinatários

- Profissionais TI que pretendem desenvolver competências práticas em ethical hacking e testes de penetração;
 - Técnicos e administradores de redes e sistemas que desejem reforçar os seus conhecimentos em avaliação e gestão de vulnerabilidades;
 - Especialistas e consultores de cibersegurança que procurem validar o seu conhecimento técnico através de uma certificação reconhecida internacionalmente;
 - Formandos que pretendam iniciar ou consolidar uma carreira na área de testes de intrusão e segurança ofensiva.
-

Objetivos

- Planear e executar testes de penetração
 - Explorar vulnerabilidades em redes, aplicações e sistemas
 - Elaborar relatórios técnicos e comunicar resultados
-

Condições

Notas

Após a formação, é possível adquirir, na Rumos, o exame de certificação do parceiro oficial com 10% de desconto.

Oferta válida até 6 meses após a conclusão do curso na modalidade live training ou presencial.

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; restante valor até 7 dias antes do início do curso.
- Possibilidade de pagamento faseado.
- 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 intermédios de conceitos de segurança da informação, tais como: gestão de identidades e acessos (IAM), conceitos e implementações de criptografia, conceitos e implementações de redes informáticas, e tecnologias de segurança comuns.
 - Experiência prática na proteção de ambientes informáticos.
-

Programa

- Introdução
- Testes de Penetração
- Planeamento e Definição do Âmbito de Testes de Penetração
- Recolha de Informação
- Scan de Vulnerabilidade
- Análise de Scans de Vulnerabilidade
- Exploit e Pivot
- Exploração de Vulnerabilidades de Rede
- Exploração de Vulnerabilidades Físicas e Sociais
- Exploração de Vulnerabilidades em Aplicações
- Exploração de Vulnerabilidades em Hosts
- Relatórios e Comunicação
- Scripting para Testes de Penetração

Introdução

- O Exame PenTest+
- O que Aborda Este Curso?
- Objetivos do Exame de Certificação CompTIA PenTest+

Testes de Penetração

- O que é o Teste de Penetração?
- Razões para Realizar Testes de Penetração
- Quem Realiza Testes de Penetração?
- O Processo de Penetration Testing da CompTIA
- A Cyber Kill Chain
- Ferramentas Utilizadas

Planeamento e Definição do Âmbito de Testes de Penetração

- Resumo das Atividades Preliminares
- Modelo de Responsabilidade Partilhada
- Conceitos Legais Fundamentais para Testes de Penetração
- Considerações de Conformidade Regulatória

- Normas e Metodologias de Penetration Testing
- Frameworks de Modelação de Ameaças

Recolha de Informação

- Reconhecimento e Enumeração
- Reconhecimento Ativo e Enumeração

Scan de Vulnerabilidade

- Identificação de Requisitos de Gestão de Vulnerabilidades
- Configuração e Execução de Scans de Vulnerabilidades
- Testes de Segurança de Software
- Desenvolvimento de um Workflow de Correção
- Superar Barreiras ao Vulnerability Scanning

Análise de Scans de Vulnerabilidade

- Revisão e Interpretação de Relatórios de Scan
- Validação de Resultados de Scan
- Vulnerabilidades Comuns

Exploit e Pivot

- Exploits e Ataques
- Pivoting e Movimentação Lateral
- Toolkits e Ferramentas de Exploração
- Detalhes Específicos de Exploits
- Utilização de Exploits
- Persistência e Evasão
- Ocultação de Rastos

Exploração de Vulnerabilidades de Rede

- Identificação de Exploits
- Execução de Exploits na Rede
- Exploração de Serviços Windows
- Exploração de Serviços Comuns
- Explorações Wireless

Exploração de Vulnerabilidades Físicas e Sociais

- Exploração de Vulnerabilidades Físicas
- Exploração de Vulnerabilidades Sociais

Exploração de Vulnerabilidades em Aplicações

- Exploração de Vulnerabilidades de Injeção
- Exploração de Vulnerabilidades de Autenticação

- Exploração de Vulnerabilidades de Autorização
- Exploração de Vulnerabilidades em Aplicações Web
- Práticas de Programação Insegura
- Ferramentas de Teste de Aplicações

Exploração de Vulnerabilidades em Hosts

- Ataques a Hosts
- Ataques a Credenciais e Ferramentas de Teste
- Acesso Remoto
- Ataques a Máquinas Virtuais e Contentores
- Ataques a Tecnologias Cloud
- Ataques a Dispositivos Móveis
- Ataques a Inteligência Artificial (IA)
- Ataques a IoT, ICS, Sistemas Embebidos e Dispositivos SCADA
- Ataques a Sistemas de Armazenamento

Relatórios e Comunicação

- A Importância da Colaboração e Comunicação
- Recomendar Estratégias de Mitigação
- Elaboração de um Relatório de Penetration Testing
- Encerramento da Atividade

Scripting para Testes de Penetração

- Scripting e Penetration Testing
- Variáveis, Arrays e Substituições
- Operações de Comparação
- Operações com Strings
- Controlo de Fluxo
- Input e Output (I/O)
- Gestão de Erros
- Reutilização de Código
- O Papel da Programação no Penetration Testing