Ethical Hacking for Mobile

Tecnologias de Informação - Segurança

- **Nível:** Intermédio
- **Duração:** 14h

Sobre o curso

Este curso aborda as particularidades da segurança em plataformas móveis, com especial enfoque no sistema operativo Android.

Os formandos irão explorar vulnerabilidades comuns em aplicações móveis, aplicando técnicas de engenharia reversa, modificação de aplicações e análise estática e dinâmica.

Ao longo do curso serão preparados ambientes de teste com dispositivos físicos e virtuais, recorrendo a ferramentas como APKTool, MobSF e Burp Suite para identificar e explorar falhas de segurança. Este curso oferece uma abordagem prática, orientada para a realidade do ecossistema mobile atual.

Destinatários

Profissionais de cibersegurança, pentesters, especialistas em aplicações móveis, consultores de segurança, e outros técnicos que pretendam adquirir competências práticas na avaliação e exploração de vulnerabilidades em dispositivos e aplicações móveis.

Objetivos

- Compreender o funcionamento e a arquitetura do sistema operativo Android no contexto da segurança
- Utilizar ferramentas e técnicas de engenharia reversa e análise de aplicações móveis
- Realizar testes de segurança em ambientes simulados com dispositivos Android

---

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; 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 técnicos na área de sistemas operativos e redes
- Familiaridade com os conceitos básicos de cibersegurança e testes de penetração
- Conhecimentos prévios de Android são valorizados, mas não obrigatórios

---

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

- 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