ETHICAL HACKING MOBILE APPLICATION PENTESTING – EHMOB

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 40 hrs

O curso Ethical Hacking Mobile Application Pentesting (EHMOB) apresenta conceitos, técnicas e procedimentos para realizar análise de vulnerabilidades e teste de invasão (*pentesting*) em aplicativos móveis, com foco na plataforma Android, por meio de engenharia reversa, análise estática e análise dinâmica.

O aluno aprenderá sobre a superfície de ataque dos aplicativos Android passando, inicialmente, pelos fundamentos do sistema operacional Android, aspectos de segurança, processo de construção de aplicações, estrutura do *Android Application Pack* (APK), compilar/assinar aplicativos e como configurar seu próprio ambiente de teste.

O treinamento é 100% prático (*hands-on*), baseado na experiência em Pentests de dispositivos móveis e estruturado segundo os padrões e metodologia do OWASP Mobile Top 10, onde serão exploradas aplicações Android por meio de uma bateria de exercícios e laboratórios.

Neste curso, serão trabalhadas técnicas de engenharia reversa em APK, detecção de root de dispositivos, análise de tráfego de aplicativos móveis (*certificate pinning bypass*), além da análise estática, onde serão exploradas falhas como SQL injection, path transversal, activities vulneráveis, receivers vulneráveis, preferências compartilhadas inseguras, logs inseguros, ofuscação de código, bypass de proteção de screenshot entre outros.

MÓDULO 0

1. Configuração e Preparação do Ambiente
   - Instalação do Android Studio
   - Configurando o Android Studio no Windows
   - Configurando o Android Studio no Linux
   - Configurando o Android Studio no MacOS
   - Configurando um Android Virtual Device (AVD)
   - Conectando dispositivos (físicos e virtuais)
   - Ativando o modo desenvolvedor no dispositivo

MÓDULO 1

1. Arquitetura Android
   - Estrutura do sistema Android
   - Bibliotecas e componentes
   - Detalhes da aplicação
   - Activities
   - Services
   - Broadcast Receivers
   - Content Providers
   - Conhecendo e entendendo o arquivo androidmanifest.xml
   - Android Debug Bridge (ADB)
2. Maquina Virtual Android (AVM)
   - Estrutura do modelo Dalvik
   - Estrutura do modelo ART
   - Estrutura do modelo JNI
3. Modelo de segurança – Android
   - UID (Permissões do usuario)
   - Sandbox
4. **Laboratório**

MÓDULO 2

1. Engenharia reversa de APK
   - APKTool
   - SMALI/BAKSMALI
   - Dex2jar / Enjarify
   - JD-GUI
   - apksigner
   - Estrutura de um APK
   - Modificando e recompilando uma App
   - Assinando um aplicativo com certificado auto-assinado
   - Bypass de controles de segurança
   - QARK
   - MobSF
2. **Laboratório**

MÓDULO 3

1. Hooking
   - Enumerando classes
   - Hooking de classes e métodos
   - Modificando variáveis
   - Modificando dados em variáveis privadas

MÓDULO 4

1. Detectando proteções em aplicativos
   - Detecção de emulador
   - Detecção de Frida
   - Captura de tela (*screenshot*)
   - Detecção de root

2. Bypass em proteções
   - Antiemulation
   - Antifrida
   - Screenshot
   - Antiroot
   - Código ofuscado

3. **Laboratório**

MÓDULO 5

1. Interceptação do tráfego de rede
   - Instalação de certificado digital CA do Burp
   - Configuração de proxy no AVD
   - Configuração de proxy em dispositivos físicos
   - Interceptando comunicações
   - Interceptando tráfego SSL/TLS
   - Estrutura da cadeia de certificação
   - Pinagem de certificado (*Certificate/SSL Pinning*)
   - Redirecionamento de portas internas – ADB/IPtables
   - Bypass de múltiplas proteções de *Certificate/SSL Pinning*
   - *Manipulando código ofuscado*

2. **Laboratório**

MÓDULO 6

1. Vulnerabilidades em aplicações Android
   - Visão geral do OWASP Mobile Top 10
   - Log inseguro
   - Armazenamento inseguro de dados
   - SQL Injection
   - Exploração de Content Providers
   - Abuso de bibliotecas Nativas da aplicação
   - Abuso e exploração de dados via Screenshot
   - Abuso de falhas no controle de acesso
   - Vazamento de informações via *screenshot* (captura de tela)
2. **Laboratório**

MÓDULO 7

1. Plugins do Burp
   - Estrutura de plugins
   - Criando plugin para o burp
   - Adulterando tráfego utilizando plugin
2. **Laboratório**

MÓDULO 8

1. Criptografia, Token e senhas
   - Reconhecendo métodos de autenticação e criptografia em app
   - Sequestro de chaves criptográficas
   - Quebra de comunicação criptográfica com plugin personalizado (burp)
   - Man-in-The-Middle (interceptando e alterando dados: Android-BackEnd)
   - Time-Bases One-Time Password (TOTP)
   - Obtendo a Secret Key do TOTP
   - Gerando requisições com o TOTP
2. **Laboratório**

MÓDULO 9

1. Desafios (CTF)
2. Laboratórios Extras

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows (linha de comando)
- Conhecimentos básicos em Sistema Operacional Linux (linha de comando)
- Conhecimentos básicos de Rede de Computadores, Serviços e Protocolos de Rede
- Conhecimento básico de programação/lógica de programação
- Conhecimento básico de linguagens de programação
- Familiaridade com a distribuição Kali Linux
- Familiaridade com a ferramenta Metasploit
- Familiaridade com ferramentas de Virtualização – VMWare e VirtualBox
- Recomendável ter realizado o curso Ethical Hacking Penetration Testing (**EHPT**)

PÚBLICO ALVO

- Especialistas em Segurança da Informação
- Analista de Segurança da Informação
- Pentesters
- Membros de Red Team
- DevSecOps
- Desenvolvedores de *softwares*
- Membros de CSIRT
- Pesquisadores da área de Segurança da Informação
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação
- Entusiastas de Segurança da Informação

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho (Windows, Linux ou Mac OS), com a capacidade de executar até 02 (duas) Máquinas Virtuais (VM) simultaneamente
- Configuração mínima de 8GB de RAM, 40 GB de espaço livre em disco, porta USB e placa de rede (RJ45 ou *wireless*) para acesso à Internet
- Desejável 02 (dois) monitores para incremento na produtividade
- Software de Virtualização: VMWare ou VirtualBox, preferencialmente, a versão mais atualizada

MATERIAL RECEBIDO

- As Máquinas Virtuais com as aplicações utilizadas nos exercícios
- Slides do Curso no formato PDF
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)
- Acesso ao Portal do Aluno, o GoHacking Academy
- Acesso às gravações das sessões do curso (*)

(*) Caso o aluno tenha adquirido com curso com as gravações no momento da inscrição

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Realizar análise dinâmica e estática de uma aplicação para Android
- Dominar técnica de engenharia reversa e analise de código de uma aplicação
- Analisar tráfego e chamadas (activities) de uma aplicação cliente-servidor
- Manipular estrutura de uma aplicação afim de identificar falhas de segurança
- Entender e realizar bypass em controles de segurança
- Compreender e utilizar a metodologia OWASP Top 10 – Mobile
- Analisar e identificar pontos de entrada vulneráveis em aplicativos android
- Realizar testes de invasão em aplicações para Android
- Explorar falhas em API mobile Android

ORYON FARIAS