ETHICAL HACKING IOS MOBILE APPLICATION PENTESTING – (EHIOS)

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 40 hrs

O curso Ethical Hacking iOS Mobile Application Pentesting (EHIOS) apresenta os conceitos, técnicas e procedimentos necessários para realizar análise de vulnerabilidades e testes de invasão (Pentesting) em aplicativos móveis para iOS, utilizando práticas de engenharia reversa, análise estática, análise dinâmica e instrumentação em tempo real.

O aluno aprenderá sobre a superfície de ataque de aplicativos iOS, passando, inicialmente, e pelos fundamentos do Sistema Operacional iOS, arquitetura do sistema, mecanismos de segurança (como sandboxing, App Transport Security, Keychain, etc.), estrutura de pacotes ".ipa", além de configurar seu próprio ambiente de testes utilizando dispositivos com *jailbreak*, simuladores e ferramentas como Frida, Objection, Hopper, Radare2 e Cycript.

O treinamento é 100% prático (***hands-on***), baseado na experiência de pentesters em ambientes reais e estruturado com base nos padrões e metodologias do OWASP Mobile Top 10, focando nas principais falhas que afetam aplicativos iOS modernos.

Durante o curso, o aluno executará:

- Engenharia reversa de aplicativos iOS (.ipa)
- *Bypass* de *jailbreak* detection e SSL *pinning*
- Análise de tráfego de rede e interceptação
- Manipulação de dados armazenados localmente (NSUserDefaults, Keychain, etc.)
- Exploração de *deeplinks* e WebViews vulneráveis
- Instrumentação com Frida/Objection para *hook* de métodos e coleta de dados sensíveis
- *Patching* e reempacotamento de apps iOS
- Ataques contra autenticação, criptografia e comunicação

Ao final do curso, o aluno estará apto a identificar, explorar e relatar vulnerabilidades em aplicativos iOS, com responsabilidade e embasamento técnico, utilizando uma abordagem ética e metodológica.

MÓDULO 1 – Ambiente e Fundamentos (4h)

1. Configuração do ambiente de testes iOS
2. Preparação de ambiente com macOS, Xcode e simuladores
3. Uso de dispositivos reais e *jailbreak*
4. Instalação de ferramentas de análise
5. Introdução a aplicativos iOS
    - Estrutura de pacotes ".ipa"
    - Ciclo de vida das aplicações
    - Arquitetura e linguagens (Objective-C e Swift)

MÓDULO 2 – Debugging e Engenharia Reversa (6h)

1. Técnicas de *debugging* em iOS
    - LLDB
    - Debuggers, logs e crash reports
2. Engenharia reversa em apps iOS
    - Class-dump, Ghidra, Hopper, Radare2
    - Análise de binários e métodos

MÓDULO 3 – Containers, Sideloading e Frida (6h)

1. Containers e armazenamento de dados
    - Sandboxing e estrutura de diretórios
2. Técnicas de *sideloading*
    - Instalação de apps fora da App Store
3. Introdução ao Frida
    - Conceitos de instrumentação dinâmica
    - Primeiros scripts e *hooks* simples

MÓDULO 4 – Frida Avançado e Tracing (4h)

1. Instrumentação com Frida – prática aplicada
    - Modificação de comportamento de apps em tempo real
2. Frida avançado em aplicativos de mensageria
    - Técnicas de *tracing* em métodos sensíveis

MÓDULO 5 – Vetores de Ataque em iOS (8h)

1. Ataques por canais auxiliares (Side Channel Attacks)
    - Análise de tempo, consumo e comportamento
2. Análise e interceptação de tráfego de rede
    - mitmproxy, Charles Proxy, SSL *Pinning bypass*
3. Detecção e *bypass* de *jailbreak*
    - Técnicas de evasão e contramedidas

MÓDULO 6 – Vulnerabilidades e Exploração (8h)

1. Criptografia quebrada em iOS
    - Falhas comuns em implementações
2. Exploração de *deeplinks* e *WebViews*
    - Ataques via URL *handlers* inseguros
    - *WebView injection*
3. *Patching* e exploração de apps
    - Reempacotamento, alterações binárias, *payloads*

MÓDULO 7 – Automação e Evasão (4h)

1. Automação no Pentest iOS
    - Scripts e pipelines com Frida, Objection e afins
2. Técnicas anti-reversing e antifraude
    - Proteções modernas e estratégias de *bypass*

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
- Conhecimentos básicos de programação/lógica de programação
- Conhecimentos básicos 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) e o Ethical Hacking Mobile Application Pentesting (EHMOB)

PÚBLICO-ALVO

- Especialistas em Segurança da Informação
- Analistas de Segurança da Informação
- Pentesters
- Membros de Red Team e de Blue 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.
- **!IMPORTANTE! Dispositivo iOS compatível com Jailbreak e/ou conta na Corellium.**

MATERIAL RECEBIDO

- 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.

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Entender os fundamentos do Sistemas Operacional iOS
- Compreender a arquitetura dos sistemas e aplicações mobile para iOS
- Realizar análise dinâmica e estática de uma aplicação para iOS
- Dominar técnicas de engenharia reversa e análise de código de uma aplicação iOS
- Analisar tráfego e chamadas de uma aplicação cliente-servidor
- Manipular estrutura de uma aplicação a fim de identificar falhas de segurança
- Entender e realizar *bypass* em controles de segurança para apps iOS
- Compreender e utilizar a metodologia OWASP Top 10 – Mobile
- Analisar e identificar pontos de entrada vulneráveis em aplicativos iOS
- Realizar testes de invasão em aplicações para iOS
- Explorar falhas em API mobile iOS

ORYON FARIAS