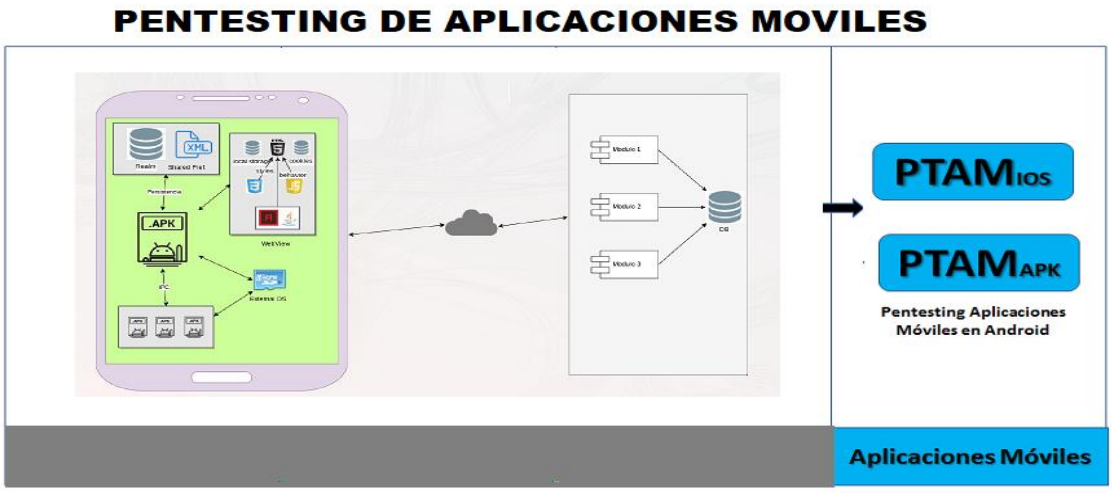
Pentesting de Aplicaciones Móviles

Programa : Pentesting de Aplicaciones Moviles

Duración : 48 Horas



El Programa de Pentesting de Aplicaciones Moviles ha sido desarrollado con el objetivo de entregar a los participantes el conocimiento de técnicas y metodología para el Análisis de Aplicaciones Moviles desarrollado en APK con en IPA.

Esta dirigido a profesionales de TI que quieran adquirir los conocimientos para poder realizar el Análisis de Aplicaciones Moviles, Análisis estático de Aplicaciones (APK/IPA) , Análisis dinámico , captura de tráfico seguro, reversing de código fuente

Durante el curso los participantes trabajaran con Aplicaciones Moviles reales

Detalle del Programa :

- Modulo 1 : Pentesting de Aplicaciones Moviles en Android (24 Hrs)

- Modulo 2 : Pentesting de Aplicaciones Moviles en IOS (24 Hrs)

Mod 1: Pentesting de Aplicaciones Moviles en Android (24 Hrs)

- En este curso se le mostrará cómo realizar actividades profesionales de pruebas de penetración contra aplicaciones móviles Android, mediante ingeniería inversa, análisis estático y análisis dinámico.
- Primero, aprenderá todo sobre la superficie de ataque de las aplicaciones de Android y las técnicas para explotar cada vulnerabilidad cubierta (incluida la ingeniería inversa).
- Se presentan primero los fundamentos del sistema operativo Android (VM de Android, modelo de seguridad de Android, etc.), el proceso de compilación (estructura de APK, aplicaciones de compilación / firma, etc.) y cómo configurar su propio entorno de prueba.
- Como atacar las aplicaciones de Android. Los APK de ingeniería inversa para la recopilación de información, el enraizamiento de dispositivos y toda la superficie de ataque de las aplicaciones de Android se tratan en detalle para que estén al tanto de lo que explota cada ataque.
- Análisis de tráfico de aplicaciones móviles (incluidas Bypass Certified Pinning).
- Durante el módulo de análisis estático, explotará la inyección de SQL y las vulnerabilidades de Path Traversal, así como las actividades vulnerables, los receptores vulnerables, los servicios vulnerables y las preferencias compartidas inseguras, entre otros.
- Análisis dinámico, aprovechará ADB para lograr la depuración en vivo y la interacción de la base de datos con fines de explotación.

CONTENIDO DEL CURSO

- Arquitectura Android
- Android Security Module
- Configuración de Ambientes de Testing
- Android Studio
- Proceso de Construcción Android
- Reversing de Aplicaciones APK
- Rooting de dispositivos android
- Fundamentos de Aplicaciones Android
- Técnicas de Inspección
- Inspección de Trafico de Red
- TapJacking
- Análisis de código Estático
- Análisis de Código Dinámico

Duración: 24 horas.

Mod 2 Pentesting de Aplicaciones Moviles en IOS (24 Hrs)

- En este curso, aprenderá todo sobre la superficie de ataque de las aplicaciones iOS y las técnicas para explotar cada vulnerabilidad (incluida la ingeniería inversa).
- Los fundamentos de iOS (arquitectura de seguridad, enclave seguro, touchID, firma de código), proceso de construcción (identidad de aprovisionamiento, programa de desarrollador de Apple, ofuscación, etc.) y cómo configurar su propio entorno de prueba.
- Se tratara en detalle ingeniería inversa para las aplicaciones de iOS, para la recopilación de información, el jailbreak de dispositivos y toda la superficie de ataque de las aplicaciones de iOS.
- Se cubrira el análisis de tráfico de aplicaciones móviles (incluidas Certificate pinning bypasses).
- Durante el módulo de análisis estático, aprenderá todo sobre el keychain, plist, controladores de URI personalizados y SDK de terceros.
- Durante el módulo de análisis dinámico, aprenderá a analizar en tiempo de ejecución de Objective-C, Cycript, atacar aplicaciones personalizadas y eludir la autenticación de una aplicación a través de runtime instrumentation, entre otros.

CONTENIDO DEL CURSO

- Arquitectura iOS
- Jailbreaking de Dispositivos iOS
- Configuracion de Ambientes de Testing
- Instalacion de Herramientas y Uso Basico
- Proceso de Contruccion iOS
- Reversing de Aplicaciones iOS
- Fundamentos de Aplicaciones iOS
- Fundamentos de Pruebas de iOS
- Tecnicas de Inspeccion
- Inspeccion de Trafico de Red
- Administracion de Dispositivos
- Analisis Dinamico

Duración: 24 horas.