M-CIB-04

Metodología General de Pruebas de Intrusión a Aplicaciones Móviles Android e iOS

Responsables

Elaboró:	Especialista Ciberinteligencia
Revisó:	Control de Documentos
Aprobó:	Dirección General

Control de versiones

Versión	Fecha	Descripción del cambio
1	29/09/2022	Emisión Inicial

Clave del formato de manual: F-SGI-004 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Introducción 3
2. Alcance 3
3. Definiciones 3
4. Descripción del manual 4
A. Técnicas de ataque por fase de la metodología 5
1. Data Storage 5
2. Cryptographic APIs 5
3. Local Authentication 5
4. Network APIs 5
5. Platform APIs 6
6. Code Quality and Build Settings 6
7. Tampering and Reverse Engineering 6
8. Anti-Reversing Defenses 6
B. Herramientas por fases de la metodología 7
5. Anexos 10

1. Introducción

Silent4Business ha alineado las pruebas técnicas a metodologías mundialmente reconocidas como SEC575del SANS Institute, OWASP MSTG, OSSTMM e ISSAF PTF. El equipo de Silent4Business utiliza las metodologías mencionadas para realizar las pruebas de penetración a aplicativos móviles Android e iOS.

A continuación, se muestra la metodología empleada para la realización de las pruebas de penetración a aplicativos móviles Android e iOS en la modalidad de caja negra, que contempla la ejecución de técnicas manuales, técnicas automatizadas y actividades de verificación que nos permiten descubrir riegos antes de que se materialicen.

2. Alcance

Este proceso es de uso del área de ciberinteligencia, es aplicable para servicios ejecutados a clientes externos y/o para Silent4Business.

3. Definiciones

Activo

Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza

Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque

Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Comprometer

Evasión de controles de seguridad causando posible de pérdida o daño en un activo de cómputo.

Exploit

Código o técnica que es usada por una amenaza para tomar ventaja de una vulnerabilidad.

Impacto

Medición de la consecuencia al materializarse una amenaza.

Mitigación

Acciones para remediar vulnerabilidades identificadas en los activos.

Probabilidad

Es la posibilidad que existe entre una amenaza y las variables de entorno para que una vulnerabilidad sea aprovechada.

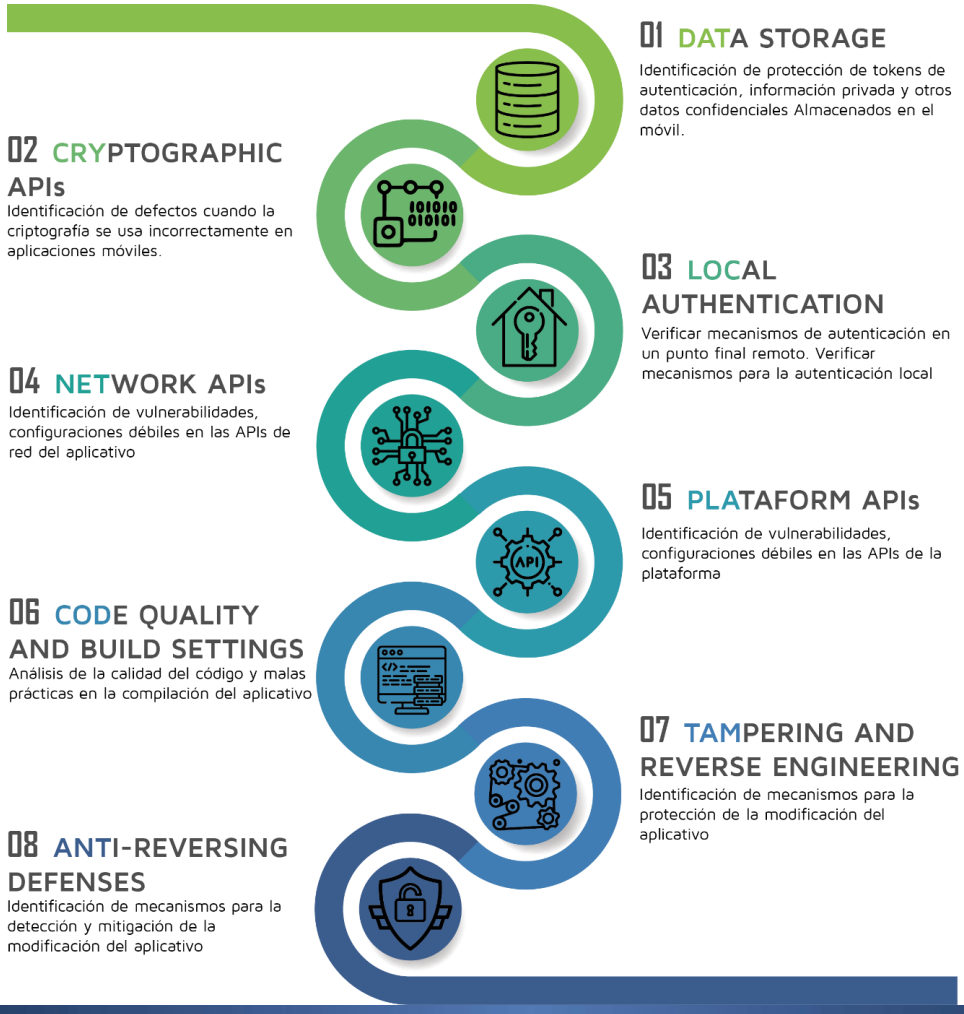
Riesgo

Es la probabilidad de que una amenaza explote una vulnerabilidad con su correspondiente impacto al negocio.

Vulnerabilidad

Son debilidades que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

4. Descripción del manual



A. Técnicas de ataque por fase de la metodología

Por cada fase de la metodología, el equipo de SILENT4BUSINESS está capacitado para realizar técnicas de ataques específicos a aplicaciones móviles Android o iOS. A continuación, se detallan algunas técnicas de ataque:

1. Data Storage

- Análisis del almacenamiento local en búsqueda de información sensible.
- Análisis de almacenamiento local para la validación de entrada de datos.
- Análisis de los logs en búsqueda de información sensible.
- Análisis para la identificación de si datos sensibles son enviados a terceros.
- Análisis de la memoria caché del teclado para identificar datos sensibles ingresados a la aplicación.
- Análisis para identificar que la aplicación elimine los datos confidenciales de manera correcta.
- Análisis para determinar si los datos almacenados confidenciales se han expuesto a través de mecanismos de IPC.
- Identificación de divulgación de datos confidenciales a través de la interfaz de usuario.
- Análisis de Backups para identificar datos confidenciales.
- Identificación de información confidencial en capturas de pantalla autogeneradas.
- Comprobación de la memoria para la identificación de datos confidenciales expuestos.
- Análisis de Device-Access-Security Policy.

2. Cryptographic APIs

- Análisis de la configuración de algoritmos estándar criptográficos.
- Análisis de Random Number Generation.
- Análisis de Key Management (Keystore, KeyChain).
- Identificación de implementaciones criptográficas débiles.
- Análisis de la reutilización de claves criptográficas.

3. Local Authentication

- Análisis al mecanismo implementado para la confirmación de credenciales local.
- Análisis al mecanismo implementado para la confirmación de credenciales biométricas.
- Análisis a la política mínima de seguridad de acceso al aplicativo.
- Análisis de los métodos de autenticación utilizados por el aplicativo móvil.

4. Network APIs

- Análisis a APS (App Transport Securit).
- Análisis a de los mecanismos para la identificación de identidad de Endpoint (Certificados).
- Análisis de Security Provider (CA).
- Análisis de los canales de comunicación implementados en la aplicación.
- Identificación de los protocolos de cifrado utilizados.
- Análisis de las suites de cifrado implementadas.
- Análisis de los certificados y SSL Pinning.
- Análisis del Almacenamiento de los certificados y SSL Pinning.

- Análisis de la configuración de seguridad de la red.

5. Platform APIs

- Análisis de los permisos de la aplicación.
- Análisis en lo parámetros de entrada del aplicativo para la identificación de ataques de tipo inyección.
- Identificación de vulnerabilidades del tipo Fragment.
- Análisis de esquema de URL personalizadas.
- Análisis de las configuraciones de las Instant Apps.
- Identificación funcionalidades sensibles expuestas a través de IPC.
- Análisis de ejecuciones de JavaScript en WebViews.
- Análisis de los Handlers de WebViews.
- Identificación de objetos de Java expuestos a través de WebViews.
- Identificación de objetos persistentes.
- Identificación de actualización forzada.

6. Code Quality and Build Settings

- Análisis para identificar si la aplicación cuenta con una firma digital apropiada.
- Análisis para identificar si la aplicación es “debuggable”.
- Análisis de los símbolos de debugging.
- Análisis de los códigos de depuración y los registros de los errores.
- Análisis de las librerías de terceros para la identificación de vulnerabilidades.
- Análisis del manejo de excepciones.
- Análisis de lo errores de corrupción de memoria.
- Análisis de las características de seguridad.

7. Tampering and Reverse Engineering

- Pruebas de ingeniería inversa.
- Pruebas de Disassembling and Decompiling.
- Análisis estático del aplicativo.
- Modificación del binario.
- Re empaquetar aplicación.

8. Anti-Reversing Defenses

- Análisis de detección de Root/JailBreak
- Identificación de mecanismos de detección de Anti-Debugging
- Análisis de comprobación de integridad de los archivos
- Detección de herramientas de ingeniería inversa
- Análisis a los mecanismos de detección de emulador
- Análisis de las comprobaciones de integridad en tiempo de ejecución
- Pruebas de ofuscación
- Pruebas para la identificación de ataques de “Device Binding”

B. Herramientas por fases de la metodología

A continuación, se listan las herramientas que usa el equipo de SILENT4BUSINESS durante las diferentes fases de la metodología.

Fase de la Metodología	Herramienta	Descripción
Data Storage	**Android Backup Extractor**	Utilidad para extraer y re empaquetar copias de seguridad de Android creadas con adb backup(ICS +).
	Logcat	Es una herramienta de línea de comandos que vuelca un registro de mensajes del sistema, incluidos los seguimientos de pila, los casos de error del sistema y los mensajes que escribas desde la app con la clase Log.
	Memory Monitor	Memory Profiler es un componente de Android Profiler que te ayuda a identificar fugas y pérdidas de memoria que puedan generar inestabilidades, fallas e incluso bloqueos de apps.
	Burp Suite Professional	Burp Suite es un conjunto de herramientas basada en java que permite comprobar la seguridad de aplicaciones web
	Drozer	Proporciona herramientas para ayudar a usar y compartir exploits públicos para Android.
	Fridump	Fridump es una herramienta de descarga de memoria de código abierto. Fridump está utilizando el Framework Frida para volcar direcciones de memoria accesibles desde cualquier plataforma compatible.
	LiME	LiME es un módulo de núcleo cargable (LKM), que permite la adquisición de memoria volátil de dispositivos basados en Linux y Linux, como los que funcionan con Android. La herramienta admite la adquisición de memoria en el sistema de archivos del dispositivo o en la red.
	Objetion	Es un kit de herramientas de exploración móvil en tiempo de ejecución, desarrollado por Frida , creado para ayudar a evaluar la postura de seguridad de las aplicaciones móviles
Cryptographic APIs	**MobSF**	Mobile Security Framework (MobSF) es una aplicación móvil todo en uno automatizada (Android / iOS / Windows), análisis de malware y evaluación de seguridad, capaz de realizar análisis estáticos y dinámicos.

Fase de la Metodología	Herramienta	Descripción
	Burp Suite Professional	Burp Suite es un conjunto de herramientas basada en java que nos permite comprobar la seguridad de aplicaciones web
Local Authentication	**Swizzler 2**	Es una herramienta para analizar aplicaciones MDM / EMS iOS.
	Frida	Es un kit de herramientas de instrumentación de código dinámico. Le permite inyectar fragmentos de JavaScript o su propia biblioteca en aplicaciones nativas en Windows, macOS, GNU / Linux, iOS, Android y QNX.
	Needle	Es un marco Framework de código abierto que tiene como objetivo agilizar todo el proceso de realización de evaluaciones de seguridad de aplicaciones iOS.
Network APIs	**Burp Suite Professional**	Burp Suite es un conjunto de herramientas basada en java que nos permite comprobar la seguridad de aplicaciones web
	Nmap	Es un programa de código abierto que sirve para efectuar rastreo de puertos y servicios
	Frida	Es un kit de herramientas de instrumentación de código dinámico. Le permite inyectar fragmentos de JavaScript o su propia biblioteca en aplicaciones nativas en Windows, macOS, GNU / Linux, iOS, Android y QNX.
	Nessus Professional	Nessus le permite escanear redes en búsqueda de servicios vulnerables a fallos de seguridad conocidos
	Android-SSL-TrustKiller	Herramienta para evitar la fijación de certificados SSL para la mayoría de las aplicaciones que se ejecutan en un dispositivo
	SSLUnpinning	Módulo Android Xposed para evitar la validación del certificado SSL (fijación de certificados).
	TrustKit	Fácil validación y creación de informes SSL para iOS, macOS, tvOS y watchOS.
	SSL Kill Switch 2	Herramienta para deshabilitar la validación de certificados SSL, incluida la fijación de certificados, en aplicaciones iOS y OS X.
Platform APIs	**Burp Suite Professional**	Burp Suite es un conjunto de herramientas basada en java que nos permite comprobar la seguridad de aplicaciones web

Fase de la Metodología	Herramienta	Descripción
	Drozer	Proporciona herramientas para ayudar a usar y compartir exploits públicos para Android.
	Frida	kit de herramientas de instrumentación de código dinámico. Le permite inyectar fragmentos de JavaScript o su propia biblioteca en aplicaciones nativas en Windows, macOS, GNU / Linux, iOS, Android y QNX.
	Idb	idb es una herramienta para simplificar algunas tareas comunes para la investigación y pentesting de iOS.
Code Quality and Build Settings	**SonarQube**	SonarQube permite a todos los desarrolladores escribir código más limpio y seguro.
	Class-dump	Es una utilidad de línea de comandos para examinar el segmento Objective-C de los archivos Mach-O. Genera declaraciones para las clases, categorías y protocolos.
	RetireJS	El objetivo de Retire.js es detectar el uso de librerías JavaScript con vulnerabilidades conocidas.
	Idb	Es una herramienta para simplificar algunas tareas comunes para la investigación y pentesting de iOS.
Tampering and Reverse Engineering	**Angr**	Es un Framework de Python para analizar binarios. Combina análisis simbólico estático y dinámico, haciéndolo aplicable a una variedad de tareas.
	apktool	Es una herramienta para la ingeniería inversa de aplicaciones de Android binarias cerradas de terceros. Puede decodificar recursos a su forma casi original y reconstruirlos después de hacer algunas modificaciones.
	IDA	IDA Pro es un desensamblador y depurador multiplataforma, multiprocesador
	JAD Decompiler	Jad (Java Decompiler) es un descompilador sin para el lenguaje de programación Java, proporciona una interfaz de usuario de línea de comandos para extraer el código fuente de los archivos de clase .
	Radare2	Framework de ingeniería inversa libre y portable
	Class-dump-dyld	Esta herramienta permite inyectar y volcar aplicaciones.
	Cycript	Cycript permite explorar y modificar aplicaciones en ejecución en iOS o Mac OS X utilizando un híbrido de sintaxis Objective-C ++ y JavaScript a través de una consola interactiva
	Optool	Es una herramienta que interactúa con los binarios de

Fase de la Metodología	Herramienta	Descripción
		MachO para insertar / eliminar comandos de carga, eliminar firmas de código, renunciar y eliminar aslr.
Anti-Reversing Defenses	**Appsync Unified**	AppSync Unified perminte instalar parches para permitir la instalación de paquetes IPA firmados, sin firma, falsificados o ad-hoc en un dispositivo iOS.
	Frida	Es un kit de herramientas de instrumentación de código dinámico. Le permite inyectar fragmentos de JavaScript o su propia biblioteca en aplicaciones nativas en Windows, macOS, GNU / Linux, iOS, Android y QNX.
	Keychain Dumper	Una herramienta para verificar qué elementos del Keychain están disponibles para un atacante una vez que un dispositivo iOS ha sido liberado
	adb	Android Debug Bridge (ADB) es una herramienta de línea de comandos versátil que permite instalar y depurar apps, y proporciona acceso a un shell de Unix que permite ejecutar distintos comandos en un dispositivo.

5. Anexos

NA