Master Interuniversitario en Seguridad de las TIC

ANÁLISIS DE RIESGOS DE VULNERABILIDADES Y AUDITORÍAS

SEGURIDAD EN SMARTPHONES

Título: Trabajo Final de Master, Master Interuniversitario en Seguridad de las TIC

Autor: Carlos García Altarejos, carlosg.altarejos@gmail.com, charly84@uoc.edu

Tutor: Marco Antonio Lozano Merino, mlozanome@uoc.edu

Fecha: 12 de Enero de 2017

"EXISTEN DOS TIPOS DE EMPRESAS: LAS QUE HAN SIDO HACKEADAS Y LAS QUE AÚN NO SABEN QUE FUERON HACKEADAS"

John Chambers, Ex CEO de CISCO

RESUMEN

- Desarrollar una metodología para realizar un análisis de riesgos de vulnerabilidades y auditorias de dispositivos.
- Estudio de las herramientas y técnicas para detectar las amenazas y las vulnerabilidades.
- Los sistemas operativos móviles que se estudiarán son Android(Google) e IOS(Apple).

OBJETIVOS

- Análisis de riesgos.
- Auditoría de dispositivos.
- Identificar amenazas.
- Detección de vulnerabilidades.
- Prevención de ataques.
- Análisis de datos.

FASES DE LA METODOLOGÍA

- 1. Identificación
- 2. Análisis
- 3. Acceso
- 4. Resultados
- 5. Informes

CLASIFICACIÓN DE LAS AMENAZAS

- **CRIMINALES**: causadas por la intervención humana con intencionalidad delictiva, como robo, fraude, espionaje, malware, etc.
- **FÍSICAS:** acciones directas sobre los dispositivos , como podría ser un accidente físico, inundación, sobrecarga, etc.
- **NEGLIGENTES**: acciones, decisiones u omisiones por parte de los usuarios del dispositivo. Por ejemplo la pérdida de información debido a un mal uso por falta de capacitación o mal manejo del dispositivo.

TIPOS DE AMENAZAS

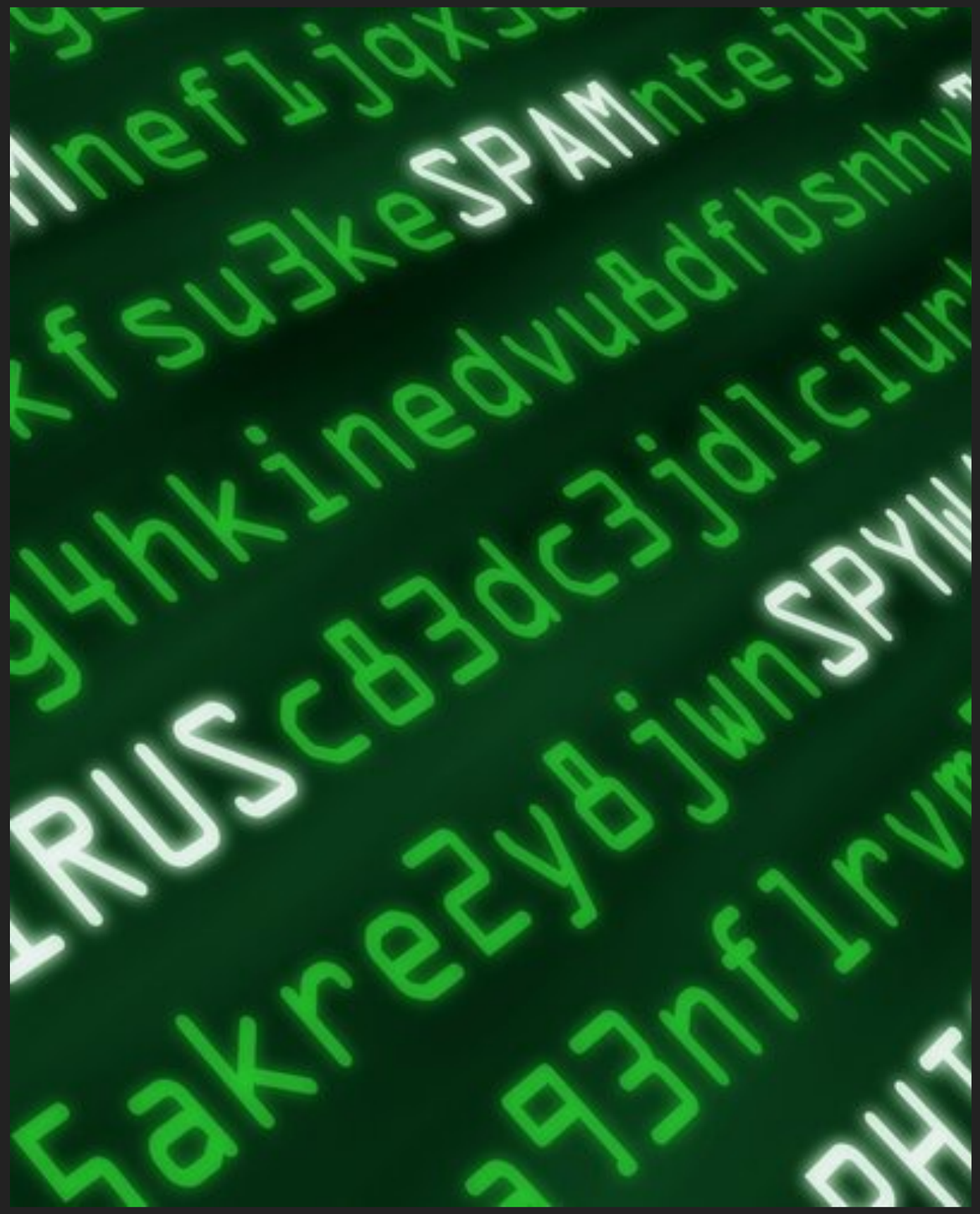
- Pérdida de información.
- Robo del dispositivo.
- Rotura del dispositivo.
- Robo de credenciales.
- Suplantación de identidad.
- Acceso a datos confidenciales.
- Robo de información.
- Fragmentación.
- Control remoto del dispositivo.
- Deterioro del terminal.
- Descarga de aplicaciones no deseadas.
- Infección por malware.
- Ataques de phising.
- Sideloading.
- Perfiles iOS maliciosos.
- Uso de sistemas no seguros.

¿QUÉ ES EL MALWARE?

El malware, también llamado badware, código maligno, software malicioso,software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

TIPOS DE MALWARE

- Virus
- Ransomware
- Gusano
- Troyano
- Spyware
- Adware
- Riskware
- Rootkit



VÍAS DE ACCESO

- Vulnerabilidades
- Ficheros
- Navegación web
- Redes Wi-fi
- Apps fraudulentas
- Configuraciones erróneas
- Jailbreak y Rooteo
- Contraseñas débiles
- Ataques de red

SISTEMAS OPERATIVOS MÓVILES

- Windows Phone
- Blackberry
- Symbian OS
- Firefox OS
- Ubuntu Touch
- Android
- iOS

SISTEMA OPERATIVO IOS

- Desarrollado por Apple Inc.
- Sistema Operativo basado en UNIX.
- Arquitectura por capas.
- Datos encriptados.
- Control de acceso mediante huella o pin.
- Apps firmadas.
- Comprobación del firmware en el arranque.

SISTEMA OPERATIVO ANDROID

- Desarrollado por Android Inc. propiedad de Google.
- Sistema Operativo Open Source basado en Linux.
- Arquitectura por capas.
- Cifrado de datos y apps firmadas.
- Control de acceso mediante huella, frase, patrón o pin.
- Multimarca.

VULNERABILIDADES

"LAS VULNERABILIDADES SON PUNTOS DÉBILES DEL SOFTWARE QUE PERMITEN QUE UN ATACANTE COMPROMETA LA INTEGRIDAD, DISPONIBILIDAD O CONFIDENCIALIDAD DEL MISMO. ALGUNAS DE LAS VULNERABILIDADES MÁS SEVERAS PERMITEN QUE LOS ATACANTES EJECUTEN CÓDIGO ARBITRARIO, DENOMINADAS VULNERABILIDADES DE SEGURIDAD, EN UN SISTEMA COMPROMETIDO."

Wikipedia.org

VULNERABILIDADES EN IOS

- Página oficial de Apple donde poder consultarlas:

  https://support.apple.com/es-es/HT201222

- Página de CVE Details donde aparecen todas las que han sido reportadas desde la primera versión:

  https://www.cvedetails.com

  984 Vulnerabilidades reportadas.

VULNERABILIDADES EN ANDROID

- Página oficial de Google donde poder consultarlas:

  https://source.android.com/security/bulletin/

- Página de CVE Details donde aparecen todas las que han sido reportadas desde la primera versión:

  https://www.cvedetails.com

  690 Vulnerabilidades reportadas.

JAILBREAK EN IOS

- Se lleva a cabo explotando vulnerabilidades.
- Proceso de liberación de las restricciones.
- Control total sobre el dispositivo.
- Eliminación de controles y limitaciones.
- Permite instalar apps no firmadas.

HERRAMIENTAS DE JAILBREAK

- Las herramientas a utilizar dependen de la versión de iOS.
- Asistente para consultar las aplicaciones a utilizar para nuestra versión de iOS. http://es.jailbreakwizard.info
- No requieren conocimientos técnicos avanzados para su uso.
- Herramientas más conocidas:
  - TaiG Jailbreak
  - Pangu
  - PP

ROOT EN ANDROID

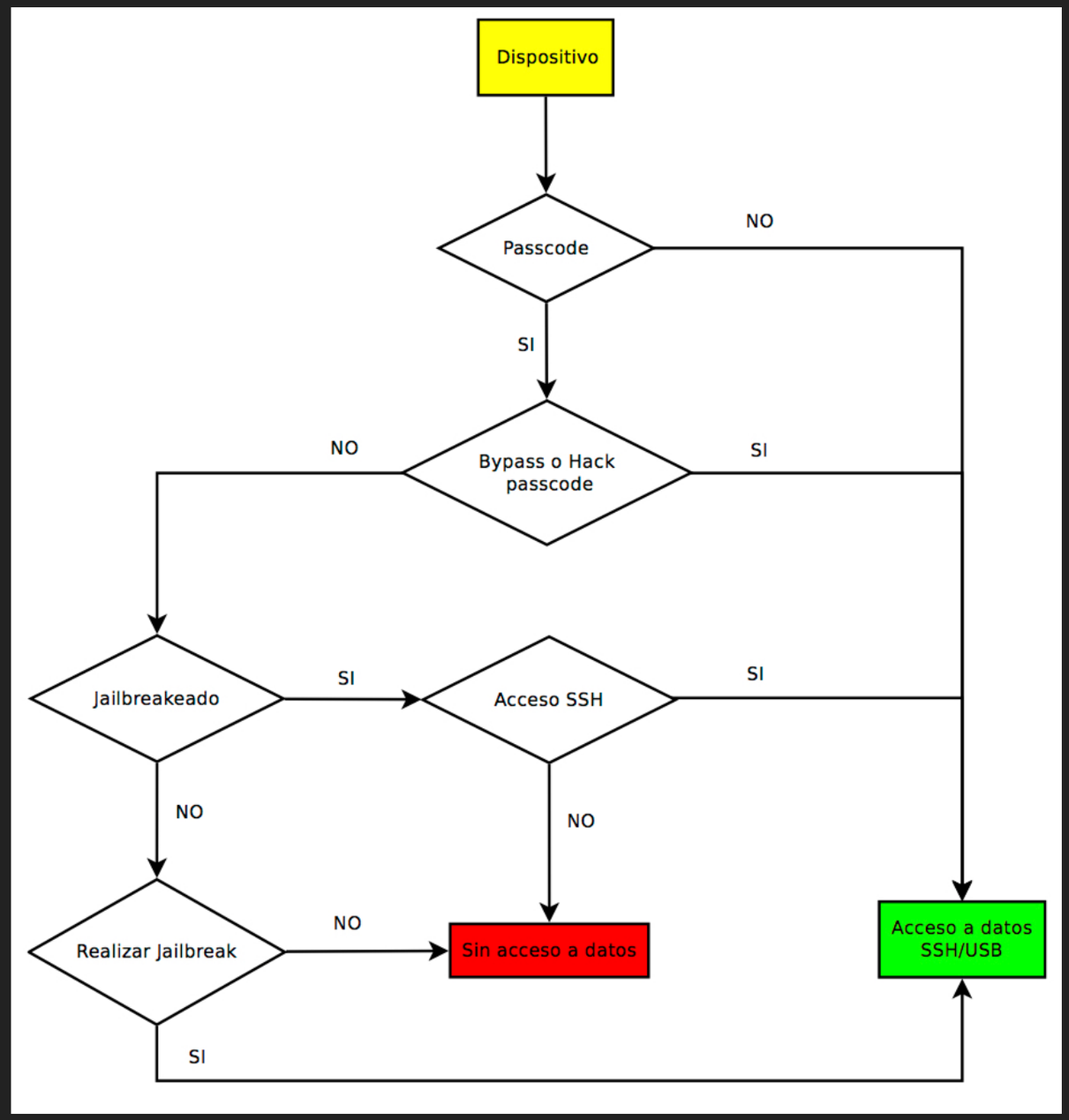
- Es equivalente al Jailbreak en iOS.
- Obtención de permisos de superusuario.
- Control total sobre el dispositivo.
- Acceso a funciones avanzadas.
- Pérdida de garantía y actualizaciones en línea.

HERRAMIENTAS DE ROOTEO

- Existen más de 24.000 modelos diferentes de dispositivos.
- Existe un gran número de herramientas diferentes.
- No requieren conocimientos técnicos avanzados para su uso.
- Herramientas más conocidas:
  - Root Genius
  - Frama Root
  - Kingo Root

ACCESO A DISPOSITIVOS CON IOS

1. Identificar modelo
2. Verificar passcode
3. Comprobar Jailbreak
4. Acceder al dispositivo.



ACCESO A DISPOSITIVOS CON ANDROID

1. Identificar el dispositivo
2. Comprobar activación de "Depuración USB"
3. Verificar el sistema de desbloqueo
4. Analizar servicios de red en escucha
5. Conectar al PC y actualizar
6. Verificar Root y/o Rootear

ANÁLISIS CON OXYGEN FORENSICS SUITE

- Herramienta comercial para el análisis forense de dispositivos móviles.
- Compatible con la mayoría de los teléfonos del mercado, y especializada en la extracción y análisis en smartphones.
- Es necesario conectar los dispositivos por USB al PC.
- Extracción de datos y análisis de ficheros de texto, BBDD, multimedia, registros, mapas, etc.
- Sistema de detección de apps fraudulentas.

ANÁLISIS CON OXYGEN FORENSICS SUITE

- Herramienta comercial para el análisis forense de dispositivos móviles.
- Compatible con la mayoría de los teléfonos del mercado, y especializada en la extracción y análisis en smartphones.
- Es necesario conectar los dispositivos por USB al PC.
- Extracción de datos y análisis de ficheros de texto, BBDD, multimedia, registros, mapas, etc.
- Sistema de detección de apps fraudulentas.

RECOMENDACIONES

- Mantener el sistema operativo y las aplicaciones actualizadas.
- Utilizar sistemas de seguridad para desbloquear.
- No conectarse a redes desconocidas.
- Instalar aplicaciones solo de sitios oficiales.
- No realizar Jailbreak o Root.
- Ser precavidos al navegar y descargar archivos.
- Instalar un software de antivirus y/o antimalware.
- Cumplir la política de seguridad respecto a contraseñas.

CONCLUSIONES

- Es complejo definir una metodología única.
- Las principales amenazas son de tipo criminal, y el malware es una de las más comunes.
- Para agilizar y mejorar los resultados del análisis es necesario apoyarse en herramientas especializadas.
- Debemos estar al día en materia de seguridad informática, para conocer las novedades respecto a técnicas, descubrimientos y actualizaciones.

Universitat Oberta de Catalunya

www.uoc.edu

Master Interuniversitario en Seguridad de las TIC

SEGURIDAD EN SMARTPHONES

GRACIAS POR SU ATENCIÓN

CARLOS GARCÍA ALTAREJOS