UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES MEDIANTE INTERNET EN DISPOSITIVOS MÓVILES ANDROID, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN PREVIO AL DESARROLLO DE UNA APLICACIÓN MÓVIL QUE FACILITE LA PROTECCIÓN DE LOS DATOS SENSIBLES ALMACENADOS.

PROYECTO DE TITULACIÓN

Previa a la obtención del Título de:

INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

AUTORES:

PATRICIO RENÁN LANCHE LARA

FRANCISCO EMANUEL PAREDES SALINAS

TUTOR:

ING. ÁNGEL WILLIAM OCHOA FLORES, MSC.

GUAYAQUIL – ECUADOR

2018

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE GRADUACIÓN			
TÍTULO Y SUBTÍTULO:			
AUTOR(ES) (apellidos/nombres):	LANCHE LARA PATRICIO RENÁN PAREDES SALINAS FRANCISCO EMANUEL		
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	ING. CRESPO MENDOZA ROBERTO, MSIG. ING. OCHOA FLORES ÁNGEL WILLIAM, MSC.		
INSTITUCIÓN:	UNIVERSIDAD DE GUAYAQUIL		
UNIDAD/FACULTAD:	FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS		
MAESTRÍA/ESPECIALIDAD:			
GRADO OBTENIDO:	INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES		
FECHA DE PUBLICACIÓN:		No. DE PÁGINAS:	119
ÁREAS TEMÁTICAS:			
PALABRAS CLAVES /KEYWORDS:			
RESUMEN/ABSTRACT (150-250 palabras):			
ADJUNTO PDF:	[X] SI	[ ] NO	
CONTACTO CON AUTOR/ES:	Teléfono:	E-mail:	
CONTACTO CON LA INSTITUCIÓN:	Nombre:		
	Teléfono:		
	E-mail:		

CARTA DE APROBACION DEL TUTOR

En mi calidad de Tutor del trabajo de titulación, **"ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES MEDIANTE INTERNET EN DISPOSITIVOS MÓVILES ANDROID, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN PREVIO AL DESARROLLO DE UNA APLICACIÓN MÓVIL QUE FACILITE LA PROTECCIÓN DE LOS DATOS SENSIBLES ALMACENADOS."** elaborado por el Sr. PATRICIO RENÁN LANCHE LARA y el Sr. FRANCISCO EMANUEL PAREDES SALINAS **Alumnos no titulados** de la Carrera de Ingeniería en Networking y Telecomunicaciones de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Networking y Telecomunicaciones, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

Atentamente

ING. ÁNGEL WILLIAM OCHOA FLORES, MSC.

DEDICATORIA

Dedico el presente título a mi querida madre **PERFECTA LIBRADA LARA VALENCIA** que fue mi pilar y mi fuerza desde el primer momento que inicie esta carrera, hoy lamento mucho no tenerla físicamente en este acontecimiento tan importante, cuando también anhelabas esta crucial etapa y confieso que después de tu muerte repentina tuve el deseo fugaz de renunciar a seguir en este camino, pero como tu decías hay que estar de pie y seguir caminando hacia adelante que la vida continua que por muy duro que ella nos golpee siempre hay que sonreír, confieso que al escribir esta lirica profunda y dedicarte estas pocas palabras se me escapen algunas lágrimas al recordar todo lo bello que viví contigo y que me dejaste, ahora sé que desde el lugar que estés te sentirás orgullosa porque alcance el sueño de los dos, gracias madre por haberme labrado bien el camino y enseñarme a ser una persona de bien.

Gracias por todo y hasta siempre mamá, yo viviré eternamente agradecido.

PATRICIO RENÀN LANCHE LARA

DEDICATORIA

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor, ya que Él fue quien ilumino y guio siempre mi camino para llegar a cumplir una de mis metas es por eso q este sueño que ahora estoy cumpliendo se lo entrego a mi Dios de corazón gracias Padre Celestial por confiar siempre en mí.

A mi madre.

Por haberme ayudado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor y su dedicación conmigo, por su paciencia ya que ella no solo es mi madre si no también mi amiga ella estuvo siempre atenta en q no me falte nada y poder cumplir más que una meta, es mi sueño que en este momento lo estoy logrando gracias madre por el amor y dedicación que tiene conmigo, este logro es gracias a ti madre.

A mi padre.

Por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante, por su amor y dedicación conmigo por enseñarme que si uno tiene un sueño tiene q luchar para poder cumplirlo no importa que difícil sea, lo importante es cumplirlo siempre con amor, dedicación y perseverancia gracias padre por su esfuerzo y amor.

A mi esposa.

Por su aliento incondicional, por su perseverancia en nuestro hogar, por las ganas de luchar juntos en todo obstáculo que se nos atraviesa en esta vida y me motiva a luchar para formar una familia más unida gracias amor por tener siempre la confianza en mí y ayudarme en los momentos que para mí eran difíciles pero tu nuca dejaste de repetirme que con la bendición de Dios todo iba a salir bien gracias por regalarme tu amor.

A mis amigos.

Que nos apoyamos mutuamente en nuestra formación profesional y que hasta ahora, seguimos siendo amigos gracias por brindarme su amistas y les deseo éxitos y bendiciones en su futuro.

Finalmente, a los maestros, aquellos que marcaron cada etapa de nuestro camino universitario, y que me ayudaron en asesorías y dudas presentadas en la elaboración de la tesis quedo de corazón agradecido porque también gracias a ustedes llevo conmigo un buen aprendizaje, gracias por su tiempo y q Dios los bendiga siempre.

FRANCISCO EMANUEL PAREDES SALINAS

AGRADECIMIENTO

Agradezco en primer lugar a Dios, a mi familia, y a mi Tutor ING. ANGEL WILLIAM OCHOA FLORES, MSC., por ser mi guía en este proyecto de titulación, gracias por su valiosa ayuda y de saber que yo podía demostrar más, a su tenacidad y sapiencia de saberme encaminar en la senda del éxito y llegar a obtener el preciado y anhelado título de Ingeniería en Networking y Telecomunicaciones.

Patricio Renán Lanche Lara

AGRADECIMIENTO

Agradezco a Dios, por sus infinitas bendiciones en lo personal, y en lo laboral, por darme como premio el destino que me ha dado, por regalarme la maravillosa familia que tengo y todos mis seres queridos que son parte de este gran logro en mi vida.

A mis padres por brindarme todo su apoyo, por haberme inculcado los mejores valores que se puede tener en esta vida y de siempre ponerme las metas más altas, por sus sabios consejos en momentos difíciles, por todos sus sacrificios que han realizado por mí.

A mi esposa por su apoyo incondicional, luchando juntos en esta vida, brindándome su amor, su fe y las ganas de conseguir grandes metas juntos en esta vida.

A mi Tutor de Tesis, Ing. Ángel William Ochoa Flores, MSC., por su valiosa enseñanza, guía, paciencia y participación durante las clases y todo el proceso de desarrollo y revisión de tesis.

FRANCISCO EMANUEL PAREDES SALINAS

TRIBUNAL PROYECTO DE TITULACIÓN

Ing. Eduardo Santos Baquerizo, MSC.
DECANO DE LA FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

Ing. Harry Luna Aveiga, MGS.
DIRECTOR CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

Ing. Ángel Ochoa Flores, MSC.
PROFESOR DIRECTOR DEL PROYECTO DE TITULACIÓN

Ing. Roberto Crespo Mendoza, MSIG.
PROFESOR TUTOR REVISOR DEL PROYECTO DE TITULACIÓN

Ab. Juan Chávez Atocha, ESP.
SECRETARIO

DECLARACION EXPRESA

"La responsabilidad del contenido de este Proyecto de Titulación, me corresponden Exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL"

PATRICIO RENÁN LANCHE LARA

FRANCISCO EMANUEL PAREDES SALINAS

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES MEDIANTE INTERNET EN DISPOSITIVOS MÓVILES ANDROID, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN PREVIO AL DESARROLLO DE UNA APLICACIÓN MÓVIL QUE FACILITE LA PROTECCIÓN DE LOS DATOS SENSIBLES ALMACENADOS

Proyecto de Titulación que se presenta como requisito para optar por el título de
INGENIERO en NETWORKING Y TLECOMUNICACIONES

Autor: PATRICIO RENÁN LANCHE LARA
C.C.: 0918152935

FRANCISCO EMANUEL PAREDES SALINAS
C.C.: 0940289259

Tutor:
Ing. Ángel William Ochoa Flores, MSC.

Guayaquil, septiembre del 2018

CERTFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

CERTIFICO:

Que he analizado el Proyecto de Titulación presentado por los estudiantes PATRICIO RENÁN LANCHE LARA y FRANCISCO EMANUEL PAREDES SALINAS, como requisito previo para optar por el Título de Ingeniero en Networking y Telecomunicaciones cuyo tema es:

"ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES MEDIANTE INTERNET EN DISPOSITIVOS MÓVILES ANDROID, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN PREVIO AL DESARROLLO DE UNA APLICACIÓN MÓVIL QUE FACILITE LA PROTECCIÓN DE LOS DATOS SENSIBLES ALMACENADOS."

Considero aprobado el trabajo en su totalidad.

Presentado por:

Lanche Lara Patricio Renán C.C.: Nº 0918152935

Paredes Salinas Francisco Emanuel C.C.: Nº 0940289259

Tutor: Ing. Ángel William Ochoa Flores, MSC.

Guayaquil, septiembre del 2018

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

Autorización para Publicación de Proyecto de Titulación en Formato Digital

1. **Identificación del Proyecto de Titulación**

<table>
<tr><td colspan="2">Nombre del Alumno:
PATRICIO RENÁN LANCHE LARA;
FRANCISCO EMANUEL PAREDES SALINAS</td></tr>
<tr><td colspan="2">Dirección:
CDLA. LOS HELECHOS SECTOR 2 MZ. D3 SOLAR 3;
GUASMO SUR COOP. FLORIDA I MZ. 6 SOLAR 8.</td></tr>
<tr><td>Teléfono:
042815105 - 0995546238
042609903 - 0986332750</td><td>Email:
patricio.lanchel@ug.edu.ec
francisco.paredess@ug.edu.ec</td></tr>
<tr><td colspan="2">Facultad: CIENCIAS MATEMÁTICAS Y FÍSICAS</td></tr>
<tr><td colspan="2">Carrera: INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES</td></tr>
<tr><td colspan="2">Título al que opta: INGENIERO EN NETWORKING Y TELECOMUNICACIONES</td></tr>
<tr><td colspan="2">Profesor guía: ING. ÁNGEL WILLIAM OCHOA FLORES, MSC.</td></tr>
<tr><td colspan="2">Título del Proyecto de Titulación: “ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES MEDIANTE INTERNET EN DISPOSITIVOS MÓVILES ANDROID, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN PREVIO AL DESARROLLO DE UNA APLICACIÓN MÓVIL QUE FACILITE LA PROTECCIÓN DE LOS DATOS SENSIBLES ALMACENADOS.”</td></tr>
</table>

Tema del Proyecto de Titulación:

2. **Autorización de Publicación de Versión Electrónica del Proyecto de Titulación**

A través de este medio autorizo a la biblioteca de la Universidad de Guayaquil y a su Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de Titulación.

Publicación electrónica:

Inmediata		**Después de 1 año**	

Firma Alumno

3. **Forma de envío:**

El texto del Proyecto de Titulación debe ser enviado en formato Word, como archivo .Doc., O .RTF y. Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o TIFF.

DVDROM			CDROM	**X**		

INDICE GENERAL

Contenido

ABREVIATURAS

SO: Sistema Operativo.

TIC: Tecnologías de la Información y Comunicación

IOS: Sistema Operativo IPhone.

USB: Universal Serial Bus.

APP: Aplicación Móvil.

APK: Paquete de Aplicación de Android.

AHMYTH: Android RAT.

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

“ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES MEDIANTE INTERNET EN DISPOSITIVOS MÓVILES ANDROID, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN PREVIO AL DESARROLLO DE UNA APLICACIÓN MÓVIL QUE FACILITE LA PROTECCIÓN DE LOS DATOS SENSIBLES ALMACENADOS.”

Autores: Patricio Renán Lanche Lara - Francisco Emanuel Paredes Salinas
Tutor: Ing. Ángel William Ochoa Flores, MSC.

Resumen

En el presente proyecto de titulación se identificó que los dispositivos con sistema operativo Android no cuentan con una aplicación móvil que permita almacenar los archivos multimedia de forma segura, además presentan vulnerabilidades que permiten al atacante establecer una conexión remota en un Smartphone, en base a esto se define el marco teórico los conceptos relacionados con Android, aplicaciones móviles utilizadas por el usuario, vulnerabilidades en el Android, Malwares, herramientas de desarrollo y demás, explicando el funcionamiento de cada parte que se describe en dicho marco teórico. Se aplico como etapas de metodología del proyecto las fases de un Hackeo Ético, por medio de estas se realizó un ataque explotando los fallos de seguridad en un equipo Android a través de la red de internet. En los criterios de aceptación del producto se detallan el cumplimiento del proyecto y se culmina con las conclusiones y recomendaciones.

UNIVERSITY OF GUAYAQUIL
FACULTY OF MATHEMATICS AND PHYSICAL SCIENCES
CAREER OF ENGINEERING IN NETWORKING AND TELECOMMUNICATIONS

"ANALYSIS AND DETECTION OF INTERNET VULNERABILITIES IN ANDROID MOBILE DEVICES, USING INTRUSION TEST TOOLS PRIOR TO THE DEVELOPMENT OF A MOBILE APPLICATION THAT FACILITATES THE PROTECTION OF STORED SENSITIVE DATA."

Author: Patricio Renán Lanche Lara – Francisco Emanuel Paredes Salinas
Advisor: Ing. Ángel William Ochoa Flores, MSC.

Abstract

In the present project of qualifications there was identified that the devices with operating system Android do not rely on a mobile application that it should allow to store the files multimedia of sure form, in addition they present vulnerabilities that allow to the attacker to establish a remote connection in a Smartphone, on the basis of this the theoretical frame defines the concepts related to Android, mobile applications used by the user, vulnerabilities in the Android, Malwares, tools of development and others, explaining the functioning of every part that is described in the above mentioned theoretical frame. I apply to him as stages of methodology of the project the phases of an Ethical Hacker, by means of these an assault was realized exploiting the safety failures in an equipment Android across the Internet network.

INTRODUCCIÓN

Actualmente los dispositivos móviles con sistema operativo Android han evolucionado, logrando convertirse en una herramienta de trabajo de vital importancia para los usuarios que efectúan tareas empresariales. Además, estos teléfonos inteligentes poseen la capacidad de almacenar grandes cantidades de información como: Imágenes, Audios, Videos, documentos y demás. A través de un equipo Android los usuarios pueden enviar y recibir archivos por medio de aplicaciones móviles. Las compras en internet, las transacciones bancarias, los correos electrónicos y muchas otras funciones, se están realizando por estos medios. Es por esto que los piratas informáticos, han visto una oportunidad muy valiosa al tratar de vulnerar estos dispositivos.

La seguridad en Android estuvo comprometida en sus inicios y fue uno de los sistemas más vulnerados. Donde los atacantes podían acceder a la confidencialidad de la información de una forma fácil y sencilla. Sin embargo, Google con el transcurso del tiempo, ha ido generando versiones con el objetivo de fortalecer este sistema operativo, logrando convertir a Android en una de las plataformas móviles más seguras y utilizadas por los usuarios. Aún siguen existiendo vulnerabilidades que al ser explotadas por crackers puedan comprometer información crítica.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

UBICACIÓN DEL PROBLEMA EN UN CONTEXTO

Con la llegada de los dispositivos móviles con sistema operativo ANDROID los usuarios han logrado realizar tareas desde un teléfono inteligente con el objetivo de aumentar el rendimiento y disminuir tiempo y recursos. Además, los mismos poseen la capacidad de almacenar información tales como: imágenes, videos, audios, documentos y demás archivos. Los usuarios lo han adquirido por la cantidad de funciones que poseen estos equipos, pero estos han sido víctimas de ataques informáticos para el robo de información confidencial, por parte de personas maliciosas denominadas crackers que por medio de la sustracción de datos críticos han obtenido un beneficio económico.

Actualmente la tecnología ANDROID proporciona una mayor seguridad en los datos dependiendo de sus versiones pero no es suficiente para las personas que lo manejan por la cual estos equipos gestionan cualquier cantidad de funciones implementadas en ellos, donde los usuarios realizan transacciones en línea, mensajería instantánea, juegos en línea y contenido multimedia vía Streaming, además almacenan archivos como fotos y videos que al ser obtenidos por un pirata informático tiene la capacidad de comprometer la integridad del usuario.

La seguridad informática es aquella que consiste en garantizar que los datos sensibles almacenados en un dispositivo móvil Android estén protegido ante cualquier intrusión maliciosa con el objetivo de disminuir los riesgos de vulnerabilidades detectados por medio de herramientas de test de penetración y auditoria, una vez aplicados los métodos de protección adecuados se lograra

que los activos recopilados en los teléfonos móviles pueden ser únicamente accedidos por los propietarios de los mismos salvando la confidencialidad e integridad de los datos.

Por lo tanto, el presente proyecto se enfoca en analizar y detectar fallos o errores de seguridad que pueden presentarse en un dispositivo móvil con sistema operativo Android, con la finalidad de implementar los métodos de protección de datos en estos equipos salvaguardando así la confidencialidad de la información.

Con la herramienta APP-INVENTOR se desarrollará un módulo que se enfoca en la protección de los archivos como imágenes, videos y documentos que son enviados por medio de la aplicación de WhatsApp y que se almacenan en la galería de los dispositivos móviles.

SITUACIÓN CONFLICTO NUDOS CRÍTICOS

La problemática actual y presente en los dispositivos móviles surge por la falta de conocimiento de los usuarios al momento de almacenar información de carácter confidencial sin tener en consideración las posibles vulnerabilidades que pueden estar expuestas a piratas informáticos con el objetivo de explotarlas por medio de un ataque cibernético para el acceso no autorizado y la sustracción de los datos.

Además, la falta de implementación de aplicaciones que proporcionen seguridad en los dispositivos móviles ha producido un incremento de ataques a dichos equipos donde actualmente existen usuarios perjudicados por el robo de grandes cantidades de datos sensibles.

CAUSAS Y CONSECUENCIAS

A continuación, en la siguiente tabla se detalla las causas y consecuencias del problema.

Tabla No. 1 Causas y Consecuencias

Causas	Consecuencias
Falta de implementación de aplicaciones móviles seguras en los dispositivos Android.	Genera en un incremento excesivo de ataques a los dispositivos móviles Android.
Poco conocimiento de las posibles vulnerabilidades expuestas en el Android.	Produce que existan perdidas de grandes cantidades de datos sensibles afectando la integridad del usuario.
Falta de controles sobre el uso de los dispositivos móviles Android para obtener una mayor seguridad en los datos.	Uso indebido del Android para el almacenamiento de datos confidenciales.
Inversión en seguridad no considerable.	Información confidencial del usuario expuesta a piratas informáticos.

Fuente: Trabajo de Investigación
Autores: Renán Lanche-Francisco Paredes

DELIMITACIÓN DEL PROBLEMA

A través de la siguiente tabla se describe la delimitación del problema.

Tabla No. 2 Delimitación del problema

Campo	Seguridad en dispositivos móviles Android.
Área	Seguridades de redes informáticas
Aspecto	Dispositivos móviles Android.
Tema	Análisis y detección de vulnerabilidades mediante internet en dispositivos móviles Android, utilizando herramientas de test de intrusión previo al desarrollo de una aplicación móvil que facilite la protección de los datos sensibles almacenados.

Fuente: Trabajo de Investigación
Autores: Renán Lanche-Francisco Paredes

FORMULACIÓN DEL PROBLEMA

- A través de un análisis y detección de vulnerabilidades en los equipos Android los usuarios podrán tener conocimiento de los diferentes fallos de seguridad y además con el desarrollo de un prototipo de aplicación móvil segura se podrán disminuir las debilidades que presentan los dispositivos con sistemas operativos Android.

- El análisis de vulnerabilidades en los dispositivos Android es de vital importancia por lo cual los usuarios que almacenan su información en estos equipos podrán tener conocimiento de estos diferentes fallos de seguridad detectados y con el desarrollo de un prototipo de aplicación móvil Android se podrá conservar la confidencialidad, integridad y disponibilidad de los datos sensibles donde el usuario accederá a los archivos por medio de una cuenta.

EVALUACIÓN DEL PROBLEMA

Los aspectos por seleccionar dentro de la evaluación del problema son los siguientes:

- **Delimitado:** La manera de controlar los ataques informáticos realizados por un pirata informático a los dispositivos móviles con dispositivo Android no es la adecuada por la cual se presenta esta propuesta tecnológica donde por medio del desarrollo de una aplicación móvil se protegerá los datos sensibles almacenados en los teléfonos Android.

- **Claro:** Las herramientas de seguridad informática que se utilizarán en el desarrollo del proyecto definirán de forma clara los posibles fallos de seguridad presentes en los dispositivos móviles Android.

- **Evidente:** En este proyecto se logrará identificar el comportamiento del dispositivo móvil con sistema operativo Android cuando esté sometido a una intrusión maliciosa con el objetivo de aplicar medidas de seguridad para contrarrestar los ataques perpetuados en dichos dispositivos.

- **Relevante:** El proyecto de titulación a desarrollar se lo denomina relevante por el gran interés de los usuarios de conocer las posibles vulnerabilidades en sus dispositivos móviles Android y la forma de cómo evitar que estas sean explotadas por un ataque informático.

- **Factible:** Las distintas aplicaciones que se utilizaran para realizar las pruebas de Hackeo ético de dispositivos Android son de software libre,

en donde no se adquirirá licencias de programas de seguridad informática para efectuar los respectivos análisis y detección de vulnerabilidades.

- **Identifica los productos esperados:** El proyecto de titulación a desarrollar presenta una solución alternativa en base a las posibles vulnerabilidades que se analizaran y detectaran en el desarrollo de la propuesta tecnológica en la cual se implementara una aplicación móvil que proporcione seguridad en los dispositivos Android.

OBJETIVOS

OBJETIVO GENERAL

Realizar un análisis y detección de vulnerabilidades en los Smartphone con sistema operativo Android utilizando herramientas de Hackeo ético mediante la red de internet, para determinar los diferentes riesgos y amenazas, y a su vez plantear un prototipo de aplicación móvil que permita disminuir los fallos de seguridad que presenta los dispositivos Android.

OBJETIVOS ESPECÍFICOS

1. Identificar los diferentes archivos multimedia que se almacenan en los dispositivos móviles Android, para definir el tipo de vulnerabilidad expuesta.

2. Seleccionar las herramientas Open Source que se utilizaran en el ataque cibernético a los dispositivos móviles con Sistema Operativo Android para determinar el nivel de inseguridad.

3. Analizar las vulnerabilidades en los dispositivos móviles Android para establecer los parámetros requeridos de protección en el prototipo de aplicación móvil a desarrollar.

4. Determinar medidas de protección necesarias en los Smartphones para ser implementadas en un prototipo de aplicación móvil en desarrollo.

ALCANCES DEL PROBLEMA

El alcance del proyecto es la de reconocer los diferentes archivos multimedia almacenados en los dispositivos Android conectados a la red de internet y por medio de esto definir el tipo de vulnerabilidad expuesto, también se realizara una auditoría de seguridad informática para detectar y analizar las posibles debilidades donde se las presentara mediante un informe de auditoría las pruebas de Hackeo ético con sus respectivos parámetros de protección y por último se implementara un prototipo de aplicación móvil que proporcione seguridad en la información confidencial almacenada en los teléfonos Android. El prototipo que se desarrollará en la herramienta APP-INVENTOR cumplirá la función de traspaso de los datos almacenados en la Galería incluyendo memoria interna y externa en los dispositivos móviles y para acceder a la información el usuario ingresará una contraseña previamente solicitada por dicha aplicación.

JUSTIFICACIÓN E IMPORTANCIA

Con el análisis y detección de vulnerabilidades mediante la red de internet en dispositivos móviles Android se demostrará los tipos de fallos de seguridad en las aplicaciones en el propio sistema y las diferentes formas de explotación

con el objetivo de que los usuarios puedan conocer dichas vulnerabilidades para que puedan tomar las respectivas medidas de control que ayuden a mitigar estas falencias identificadas en el proceso de escaneo.

Además, con la implementación de una aplicación móvil se proporcionará protección en los datos sensibles almacenados en los teléfonos Android basado en los resultados de la auditoría de seguridad informática.

La investigación será de gran ayuda para plantear la solución a la problemática bosquejada sobre las posibles vulnerabilidades en los dispositivos Android, implementando medidas de seguridad que proporcionen un control de los fallos o errores del sistema Android.

Con la aplicación móvil a desarrollar proporcionará una medida de seguridad que solamente el usuario propietario del dispositivo móvil podrá tener acceso a la información almacenada en el mismo.

La aplicación móvil por desarrollar ayudará a que los archivos almacenados en la Galería incluyendo memoria interna, externa y WhatsApp de los dispositivos móviles estén protegidos conservando la confidencialidad, integridad y disponibilidad de la información.

Consiste en que los nuevos usuarios posean conocimiento de aplicaciones que protejan la información de carácter confidencial almacenada en el Android.

La utilidad de la aplicación móvil por desarrollar es la de prevenir ataques informáticos efectuados por personas inescrupulosas que poseen conocimientos de tecnología a los dispositivos Android con el objetivo de mantener protegida la información sensible.

METODOLOGÍA DEL PROYECTO

La metodología o ciclo de vida del proyecto a utilizar es cascada dado que el proyecto comprende de algunas fases relacionadas entre sí, para la realización de las pruebas de Hackeo ético en los dispositivos móviles Android.

- **Fase 1:** En esta fase se realizará un reconocimiento de los archivos multimedia almacenados en los dispositivos móviles Android.

- **Fase 2:** En esta fase se utiliza herramientas Open Source para realizar un ataque en los dispositivos móviles Android determinando el nivel de inseguridad.

- **Fase 3:** En esta fase se presentará los respectivos informes detallando las pruebas de Hackeo ético y los respectivos parámetros de protección.

- **Fase 4:** En esta última fase se implementará un prototipo de aplicación móvil que proporcione el traspaso de imágenes desde la memoria interna y externa del dispositivo móvil Android bloqueando los accesos no autorizados.

CAPÍTULO II

MARCO TEÓRICO

ANTECEDENTES DE ESTUDIO

Según José Dominicci estudiante de la Universidad Interamericana Recinto de Guayama detalla que la empresa McAfee reporto en el año 2011 un aumento de infección de malware o dispersión de código malicioso en los dispositivos móviles Android donde la cifra va en incremento del 37% respecto al año anterior.(Albarrán & Universidad, 2013)

Con un estudio realizado por la Ingeniera en Sistemas Computacionales Ruth Asqui en el año 2018 detalla que la utilización de dispositivos inteligentes con fines de negocio de forma acelerada día a día y los datos almacenados en los equipos Android surge la motivación de los piratas informáticos con el objetivo de realizar ataques cibernéticos finalmente obteniendo información sensible de los usuarios afectando la confidencialidad e integridad de los archivos produciendo grandes pérdidas de registros de manera exorbitante, además dicha autora indica que los sistemas operativos Android poseen mayor incidencia de intrusiones maliciosas referente a los sistemas IOS generando que la mayor parte de los datos estén expuestos a personas malintencionadas o ciberdelincuentes.(YÁNEZ, 2018)

Según estudios en el año 2014 mencionan que la mayoría de los malware o códigos maliciosos poseen como objetivo obtener la información de los usuarios tales como cuentas de redes sociales, archivos multimedia, documentos, cuentas bancarias e intercepción de llamadas, donde los piratas informáticos han sido causantes de comprometer la integridad de los propietarios de los dispositivos móviles Android accediendo a los datos de forma ilícita con el fin de beneficiarse económicamente.(Navarro, Londoño, Urcuqui López, & Gomez, 2014)

Mediante un estudio de seguridad informática en el año 2014 detallan que la plataforma Android, ha sido deliberadamente desarrollada con errores en la programación del mismo que desembocan a grandes vulnerabilidades que al ser explotadas por piratas informáticos se pueden producir riesgos de perdida de datos sensibles ocasionando daños a la integridad de los usuarios.(Milán, 2014)

A medida que los dispositivos móviles se abren paso en todos los aspectos de la vida cotidiana de cada usuario la necesidad de la seguridad y privacidad de la información se ha convertido en un elemento de vital importancia para los propietarios de los dispositivos Android con el transcurso del tiempo logrando evitar ataques cibernéticos a los equipos móviles. Según un estudio en e presente año mencionan que algunas de las características que se deben tomar en consideración para desarrollar una arquitectura móvil es la privacidad, confiabilidad, disponibilidad y poder de recuperación de datos.(Date & Type, 2018)

FUNDAMENTACIÓN TEÓRICA

Android

Es una plataforma de código abierto basada en el sistema operativo Linux diseñada para dispositivos móviles como se muestra en el gráfico No. 1, donde la empresa Google fue la creadora del Software que se utiliza actualmente en los teléfonos inteligentes. El objetivo de lanzar este sistema al mercado es para mejorar la innovación en tecnología móvil desarrollando una interfaz amigable para los usuarios en lo cual las personas que poseen un celular con sistema Android pueden gestionar servicios tales como: Transacciones en línea, Juegos en línea, Mensajería instantánea, Reproducción de contenido multimedia y demás lo que antes no se podía realizar con otros sistemas móviles.(YÁNEZ, 2018)

Android es un sistema operativo de código abierto basado en Linux para teléfonos inteligentes, además es una multiplataforma que puede ser utilizado por otras herramientas para la ejecución de aplicaciones como mensajería instantánea, multimedia, transacciones en línea y demás y por último es una combinación de Hardware y Software.(Bustos, 2015)

Características del Android

A continuación, se detallará las características más importantes del sistema operativo Android:

- El FRAMEWORK de las aplicaciones permite la reutilización de los componentes además se puede establecer reemplazo de algunos elementos del Android.
- Posee un almacenamiento estructurado que es integrado con las aplicaciones instaladas en el Android.
- Contiene un soporte de audios y videos con diferentes formatos.

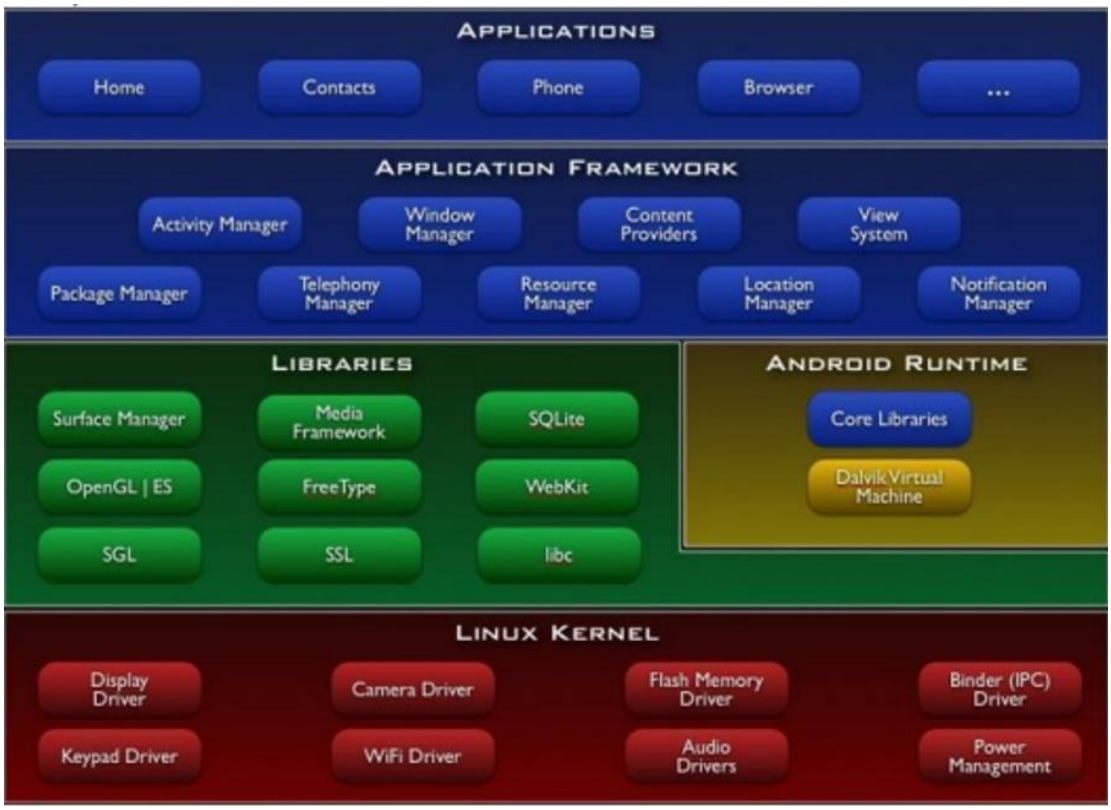
Gráfico No. 1 Android

Fuente: https://www.theinquirer.net/inquirer/news/3016494/google-is-already-working-on-android-p
Autor: Chris Merriman

Núcleo de Linux

Android es un sistema que tiene una relación de dependencia con el kernel de Linux como se aprecia en el gráfico No. 2 para los servicio base como la seguridad, gestión de memoria, gestión de proceso, pila de red y modelo de controladores, además el núcleo de Linux actúa como una capa de abstracción entre el hardware y el software.(YÁNEZ, 2018)

Gráfico No. 2 Núcleo de Android



Fuente:http://ingenieriacognitiva.com/developer/cursos/AndroidBasico/chapters/c2.php

Autor: Trabajo de Investigación

Servicios que se gestionan en el Android

Los dispositivos móviles con el transcurso del tiempo se han convertido en una mayor fuente de datos donde la conexión a la red de internet vía cable modem se ha visto de forma limitada produciendo que las personas que habitan en

zonas rurales no posean el acceso a la información de vital importancia, pero gracias a los Smartphone y la manera de que estos se pueden conectar a la red inalámbricamente los usuarios han podido realizar consultas en línea por medio de las aplicaciones instaladas en los teléfonos inteligentes, además poseen la capacidad de enviar grandes cantidades de datos utilizando la mensajería instantánea como fotos, videos, audios, animaciones, documentos y demás a grupos de usuarios logrando que el mensaje se propague por toda la red y llegue a su destinatario.(CANO, 2017)

A continuación, se detallarán los tipos de servicios en línea que se pueden gestionar en los dispositivos Android utilizando las redes inalámbricas fijas y móviles.

Transacciones en línea: Consiste en efectuar transferencias de dinero basado en compras de productos y pagos de servicios básicos utilizando las aplicaciones de entidades financieras y de empresas que venden mercadería por internet como se muestra en el gráfico No. 3, de forma directa optimizando tiempo y recursos computacionales.

Existen algunas aplicaciones móviles para realizar transacciones en línea que son las siguientes:

- Wish
- Amazon
- Banca móvil del Pacífico
- Banca móvil del Pichincha
- Alibaba
- EBay
- AliExpress

Gráfico No. 3 Aplicación móvil del banco del Pichincha

Fuente: http://sinmiedosec.com/aplicacion-banco-del-pichincha-para-dispositivos-moviles/
Autor: SINMIEDOSEC

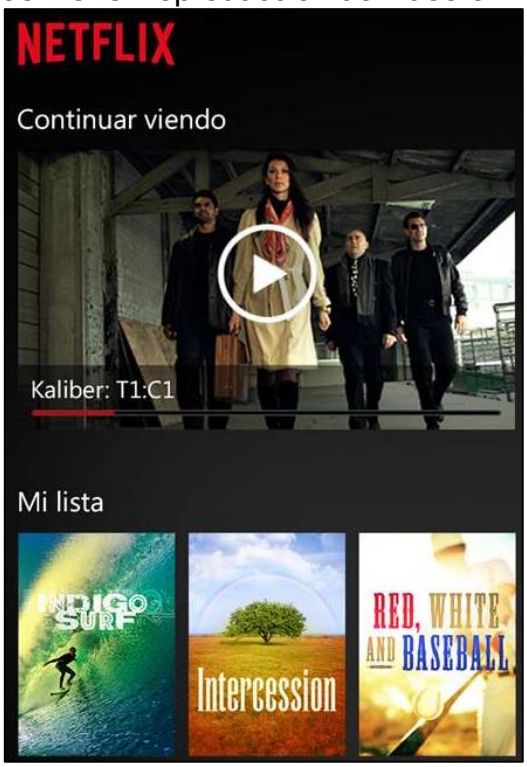
Mensajería instantánea: Consiste en enviar y recibir mensajes de texto y mensajes multimedia por medio de aplicaciones de chat tales como WhatsApp, Telegram, Line, Facebook Messenger y demás con el objetivo de aumentar la comunicación en línea entre dos o más usuarios. Antiguamente la información como imágenes, audio y video eran enviadas utilizando las redes bluetooth y aplicando el portal WAP donde él envió de mensajes multimedia los costos eran demasiado elevado. Verificar el gráfico No. 4 la evolución de la mensajería instantánea.

Gráfico No. 4 Evolución de la mensajería instantánea

Fuente: https://www.poblanerias.com/2014/02/como-evoluciono-la-mensajeria-instantanea/
Autor: Notimex

Reproducción multimedia: Antiguamente los usuarios transferían archivos multimedia utilizando la tecnología bluetooth e infrarrojo para reproducir archivos con formato MP3, MP4, 3GPP, AVI y demás. Con el transcurso del tiempo los avances tecnológicos han permitido que las personas ya no almacenan ficheros de audio y video en la memoria interna y externa de los dispositivos móviles debido a que las aplicaciones en línea como NETFLIX, YOUTUBE, IPTVPRO, ECUAPLAY, SPOTIFY, etc., reproducen contenido multimedia vía Streaming quedando la información acumulada en la red de internet como se muestra el gráfico No. 5.

Gráfico No. 5 Reproducción de video en Netflix



Fuente: https://www.microsoft.com/es-pe/store/p/netflix/9wzdncrfj3tj
Autor: Microsoft

Malware en los dispositivos móviles con sistema operativo Android

Actualmente los dispositivos móviles con sistema operativo Android son utilizados para ejecutar transferencias de datos entre dos o más usuarios debido a esto los piratas informáticos o cibercriminales realizan ataques para explotar vulnerabilidades expuestas en los Android pero antes de efectuar la intrusión maliciosa aplican un escaneo de fallos de seguridad para la detección de falencias en el sistema, logrando un beneficio económico produciendo daños de forma irreversible a la información.(CANO, 2017)

Hoy en día los códigos maliciosos ya no solamente se propagan en computadores de escritorios y laptops, si no en dispositivos móviles con sistema operativo Android donde los atacantes lo han visto como un blanco fácil para el acceso a la información confidencial con respecto a los IPHONES, los crackers han obtenido una mayor ventaja con el transcurso del tiempo debido a que los Android no analizan ni detectan virus cibernéticos integrados en las aplicaciones por lo cual los peligros referente a la perdida de datos afectando la integridad de los usuarios son eminentes. El objetivo de estos gusanos cibernéticos es infectar el hardware del dispositivo móvil para poder tener acceso a los datos de carácter privado.(Bustos, 2015)

A continuación, se detallará una lista de malwares para dispositivos móviles Android:

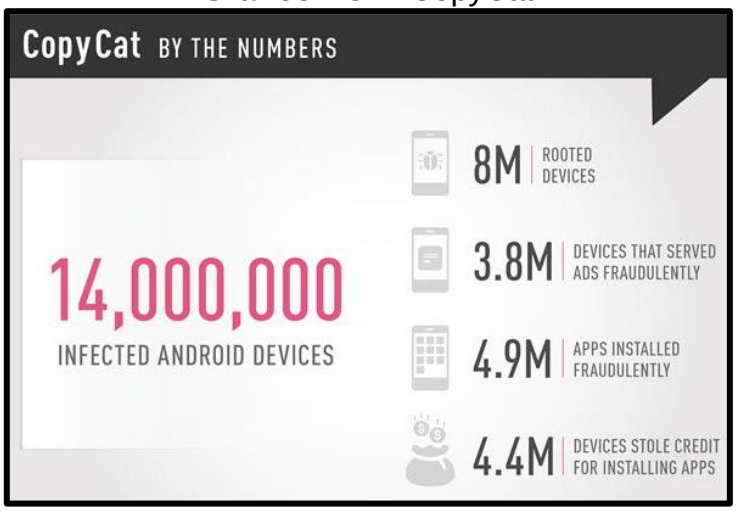
- **Cabir:** Es uno de los primeros códigos maliciosos que fue creado para dispositivos móviles, inicialmente este malware infectaba a los teléfonos inteligentes que funcionan con el sistema operativo Symbian como se muestra en el gráfico No. 6, pero con el transcurso del tiempo este virus informático fue migrando y encontrando la forma de afectar a los smartphones con S.O., Android. La manera de infectar un móvil es la de enviar el mensaje “Caribe”, donde se muestra en la pantalla del teléfono y aparece cada vez que éste es encendido, de este modo el gusano cibernético se propaga a otras terminales a través de señales inalámbricas tipo Bluetooth.(CANO, 2017)

Gráfico No. 6 Cabir

Fuente: http://www.eoi.es/blogs/ciberseguridad/2016/07/09/seguridad-en-dispositivos-moviles-malware-cabir/
Autor: E. García Cabañas

- **CopyCat:** Este código malicioso en el año 2017 infecto más de 14 millones de dispositivos móviles con sistema operativo Android como se muestra en el gráfico No. 7, donde este virus informático al ser propagado funciona como una falsa aplicación móvil la cual se descarga de una tienda externa a Google play, debido a esto se muestra como esta APP que simula ser inofensiva, al ser instalada en un equipo inteligente procede a recopilar datos sensibles en segundo plano, desencadenando exploits cuya operación es ejecutar la función de root o administrador en el dispositivo para el atacante que remotamente intenta obtener la información confidencial.(CANO, 2017)

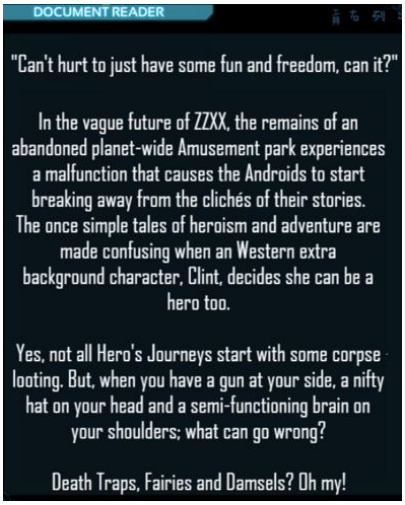
Gráfico No. 7 CopyCat



Fuente: https://www.tekcrispy.com/2017/07/08/copycat-malware-android/
Autor: Francisco Espinoza

- **Duts:** Este gusano cibernético infecta los archivos almacenados en los Android donde es el primer virus conocido por la plataforma Pocket PC como se muestra en el gráfico No. 8. El código malicioso infecta todos los archivos ejecutables (.exe) mayores a 4096 bytes en el directorio local.(CANO, 2017)

Gráfico No. 8 DUTS



Fuente: https://forums.spacebattles.com/threads/rust-to-dust-android-amusement-park-college-project-a-goofy-wander-through-cliches.636346/
Autor: Kanassa

- **Skulls:** Se enfoca en un fragmento de código troyano como se muestra en el gráfico No. 9. Una vez que la víctima descarga el virus cibernético, este reemplaza todos los iconos del escritorio del teléfono con imágenes de un cráneo. Además, deja inutilizable todas las aplicaciones instaladas en el dispositivo móvil, incluyendo la recepción y envió de mensajes de texto y multimedia.(CANO, 2017)

Gráfico No. 9 SKULLS

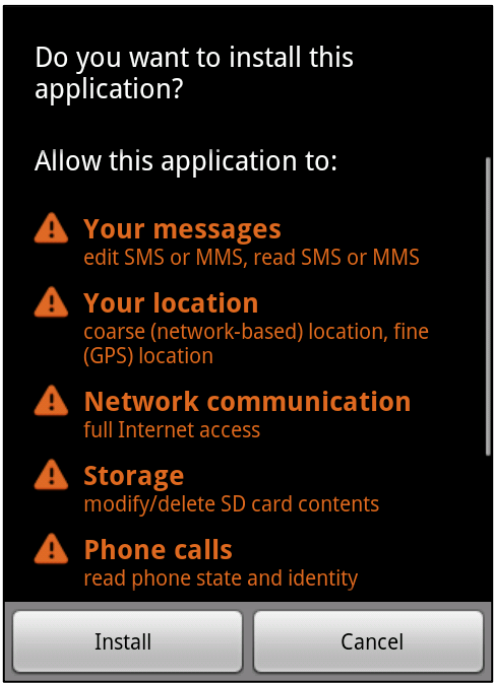
Fuente: https://apkpure.com/fake-virus-simulator/com.virus.maker.prank.simulator.remover.cleaner
Autor: APKPURE

- **Gingermaster:** Troyano desarrollado para la plataforma Android donde este se propaga por medio de la instalación de aplicaciones que incorporan de forma oculta el malware para su ejecución en segundo plano. El virus informático explota la vulnerabilidad de la versión Gingerbread del sistema operativo para utilizar los permisos de súper-usuario mediante una escalada de privilegios, luego crea un servicio

que sustrae la información del terminal infectado como: identificador del usuario, número SIM, número teléfono, IMEI, IMSI, resolución de pantalla y hora local, enviando los mismos a un servidor web remoto mediante peticiones HTTP.(CANO, 2017)

- **Droidkungfu:** Este troyano se oculta en las aplicaciones Android, que, al ser ejecutadas, obtiene los privilegios del super usuario e instala el archivo com.google.ssearch.apk, que contiene una puerta trasera que permite eliminar archivos de carácter confidencial, abrir páginas de inicio suministradas, cargar enlaces de direcciones web y descargar e instalar paquetes de aplicación como se muestra en el gráfico No. 10. Este gusano cibernético recolecta y envía a un servidor remoto todos los datos sensibles disponibles sobre el terminal.(CANO, 2017)

Gráfico No. 10 DROIDKUNGFU



Fuente: https://www.f-secure.com/v-descs/trojan_android_droidkungfu_c.shtml
Autor: F-Secure

- **Ikee:** Primer gusano creado para dispositivos móviles con sistema operativo iOS, donde solamente actúa en terminales que se les han realizado previamente un proceso de Jailbreak, y se propaga intentando acceder a otros equipos mediante el protocolo SSH (Security Shell), primero a través de una red inalámbrica que se encuentre conectado el teléfono inteligente. Luego, se repite el procedimiento generando un rango aleatorio y por último utiliza unos rangos preestablecidos que corresponden a direcciones IP de determinadas por compañías telefónicas. Una vez infectado el IPHONE, reemplaza el fondo de pantalla por una fotografía del cantante Rick Astley como se muestra en el gráfico No. 11.(CANO, 2017)

Gráfico No. 11 IKEE IOS

Fuente: https://www.applesfera.com/iphone/el-primer-gusano-que-ataca-a-los-iphone-jailbreakeados-y-como-evitarlo

Autor: APPLE-SFERA

Vulnerabilidades en los dispositivos Android

Vulnerabilidades

Las vulnerabilidades o debilidades son errores que aparecen en un sistema informático después de omitir actualizaciones en el servidor donde se ejecuta la aplicación, que al ser detectadas por cibercriminales estos poseen la capacidad de ejecutar ataques para que los sistemas operativos puedan realizar actividades no deseadas provocando el acceso al sistema de archivos de manera intencional, alterar el comportamiento normal del sistema y tomando el control total o parcial del dispositivo atacado remotamente. Verificar gráfico No. 12 los índices de vulnerabilidades en los sistemas operativos.(León, 2015)

En algunos de los casos las vulnerabilidades se manifiestan a causa de falta de soporte técnico y actualizaciones en los programas o plataformas diseñadas para determinados sistemas operativos. A veces los administradores de red con el transcurso del tiempo han omitido las medidas de protección, debido a esto existen una multitud de vulnerabilidades explotables a fallos de seguridad que no son estandarizados, pero que al ser descubiertas por piratas informáticos han representado un gran problema de seguridad en los sistemas de información, ya que en la mayoría de los argumentos, una simple falencia presente en un programa específico pone en riesgo todo el sistema afectando la productividad de la organización. Actualmente el sistema operativo Android cuenta con 523 vulnerabilidades desde el año 2016 respecto a los otros sistemas.(León, 2015)

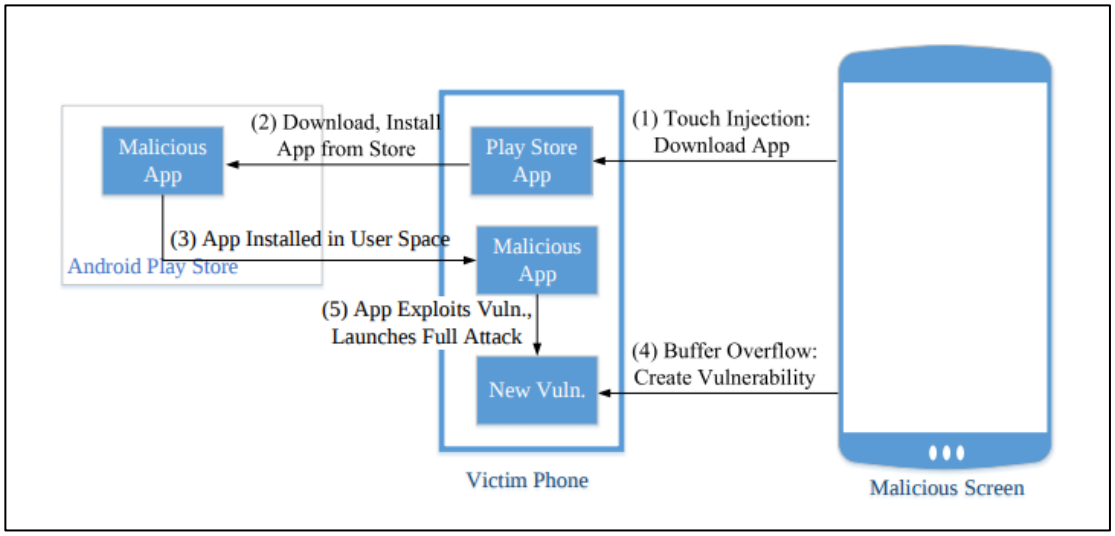
Gráfico No. 12 Vulnerabilidades de Android

Fuente: https://es.statista.com/grafico/7560/android-el-mas-expuesto-a-hackeos/
Autora: Guadalupe Moreno

Tipos de vulnerabilidades en los sistemas operativos Android

- **Desbordamiento de búfer:** Esta vulnerabilidad se presenta cuando un programa o sistema de información no toma en consideración el tamaño de los datos de entrada y al superar el tamaño en memoria reservado para ellos como se muestra en el gráfico No. 13, se sobre-escribe la dirección de memoria donde el procesador utilizado para ejecutar la próxima instrucción del programa, permite a un atacante malicioso tomar el control del flujo del mismo y ejecutar código arbitrario.(León, 2015)

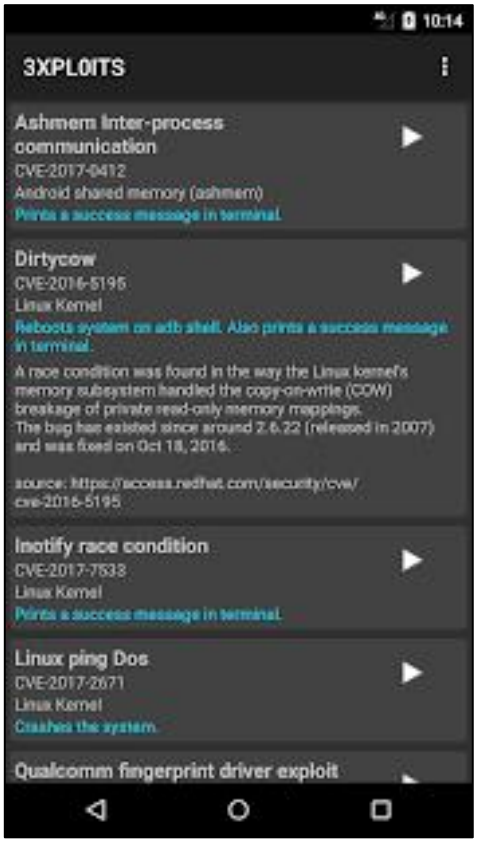
Gráfico No. 13 Desbordamiento de Búfer



Fuente: https://unaaldia.hispasec.com/2017/08/chip-in-middle-o-como-atacar-un.html
Autor: HISPASEC

- **Desbordamiento de entero:** En programación existen varios tipos de datos cuya función es representar valores numéricos enteros para después almacenarlos en memoria donde estos poseen un rango de valores limitados como se muestra en el gráfico No. 14. En algunos de los casos cuando se trata de almacenar un valor o efectuar una operación matemática que conlleva a exceder la capacidad de los tipos de datos, se produce un desbordamiento de entero, en lo cual no es considerado riesgoso, pero si el entero depende de una operación con memoria, existe la posibilidad de propiciar un desbordamiento de búfer.(León, 2015)

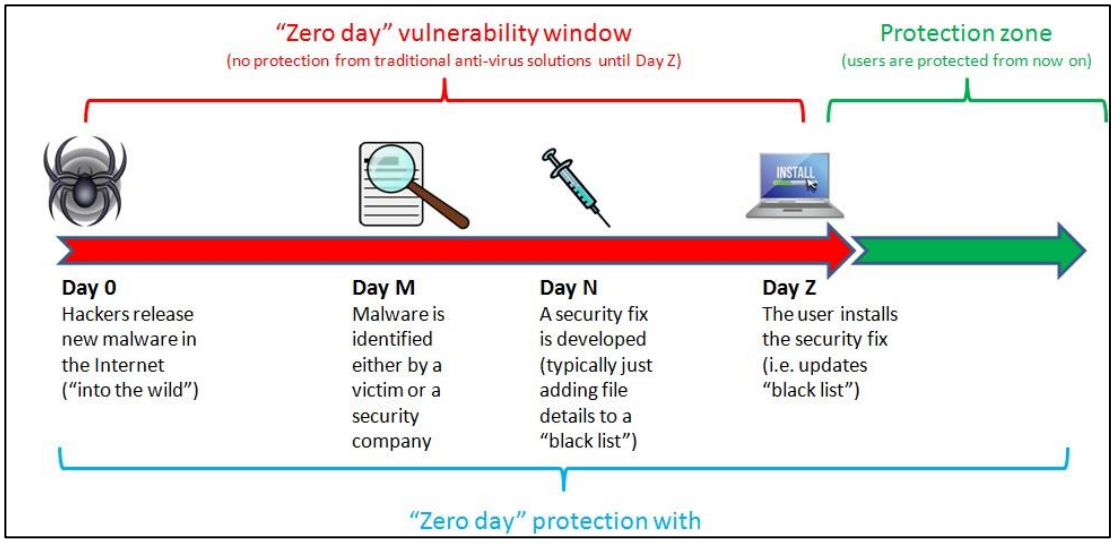
Gráfico No. 14 Desbordamiento entero



Fuente:https://play.google.com/store/apps/details?id=com.saroteck.exploittester&hl=es
Autor: PLAY STORE

- **Vulnerabilidades de día cero:** La vulnerabilidad día cero surge por la explotación de fallos de seguridad el mismo día en que son descubiertas por los ciberdelincuentes como se muestra en el gráfico No. 15, esta debilidad se extiende también a todas las vulnerabilidades que no han sido mitigadas en determinado periodo de tiempo. El peligro de esta vulnerabilidad reside por el surgimiento de los cibercriminales la detectan y la explotan antes de que el administrador de red la identifique.(León, 2015)

Gráfico No. 15 Vulnerabilidad día cero

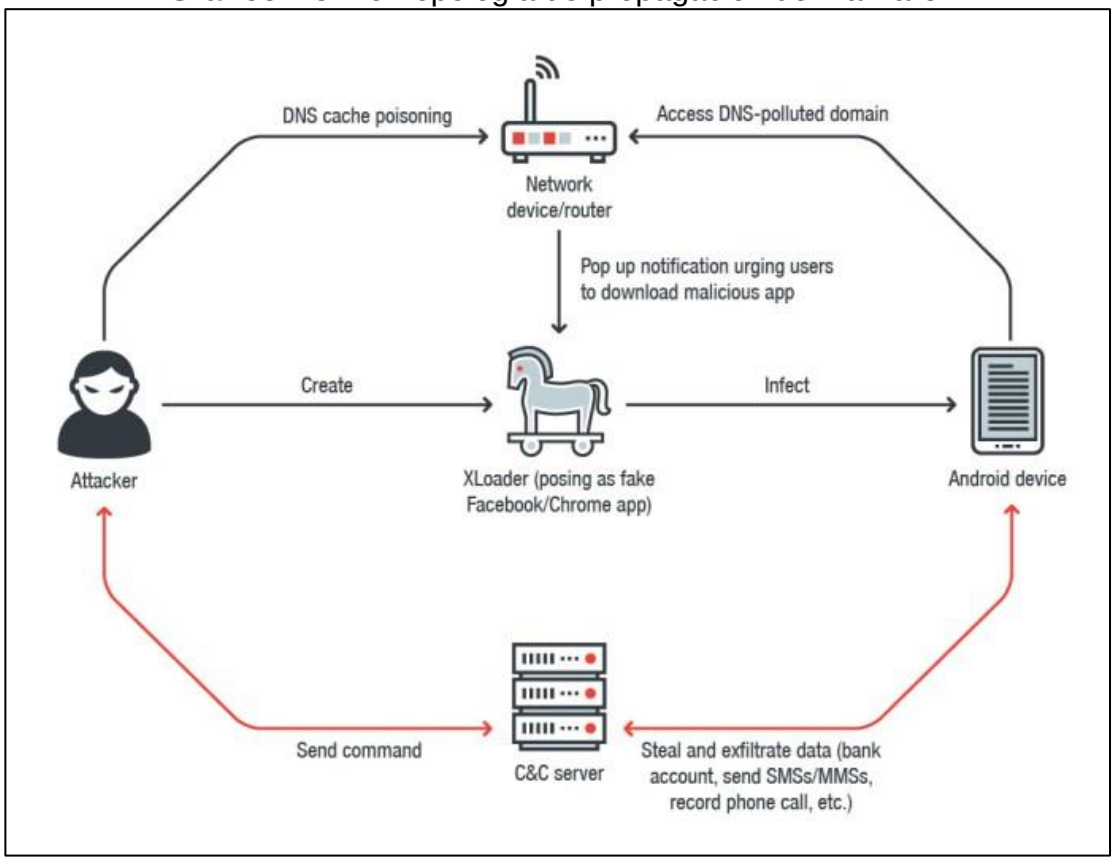


Fuente: https://finalavsecurity.com/site/key-advantages-1/
Autor: FINALVSECURITY

Herramienta utilizada para el hackeo de dispositivos móviles con sistema operativo Android.

Metasploit: El framework de Metasploit es una herramienta utilizada por atacantes maliciosos para ejecutar código abierto de explotación, explotando una vulnerabilidad detectada en un sistema operativo como: Android, Linux y Windows. Un exploit se lo denomina un código que es propagado por un pirata informático para la toma de control de un ordenador o dispositivo móvil como se muestra en el gráfico No. 16 con el objetivo de tener acceso a los archivos confidenciales almacenados en los equipos finales.(Gonsalves & Kulkarni, 2017)

Gráfico No. 16 Topología de propagación de malware

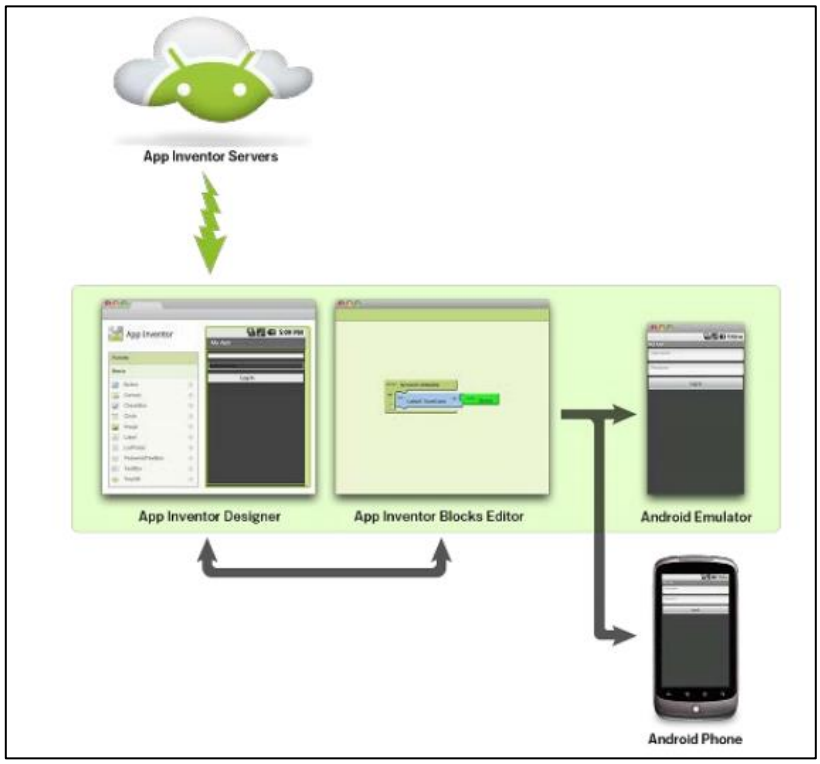


Fuente: https://www.seguridadyfirewall.cl/2018/04/malware-de-android-se-hace-pasar-por.html
Autor: Diego Cortes

APP INVENTOR

Es una aplicación que fue desarrollada por la empresa Google y proporcionando soporto por el Instituto Tecnológico de MASSACHUSETTS, esta herramienta permite a cualquier usuario no asociado con la programación desarrollar cualquier aplicación móvil para dispositivos Android, donde la interfaz gráfica muy similar al SCRATCH y el STARLOGO, en lo cual los desarrolladores de APPs Android pueden arrastrar y soltar objetos visuales para la creación de la aplicación, verificar gráfico No. 17.(Kryscia Ramírez Benavides, 2014)

Gráfico No. 17 APP INVENTOR



Fuente: (Kryscia Ramírez Benavides, 2014)
Autor: (Kryscia Ramírez Benavides, 2014)

Ventajas de APP INVENTOR

- No se requiere instalar un IDE.
- Los conocimientos de programación son mínimos para el desarrollo de aplicaciones móviles para dispositivos Android.
- Desarrollo de aplicaciones con bajos niveles de error y de forma inmediata.
- Almacenamiento en la nube.
- Soporte para todas las versiones de Android.

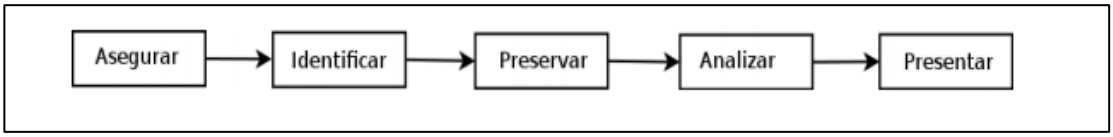
Desventajas de APP INVENTOR

- No cuenta con la capacidad de subir las aplicaciones al Android Market.
- No permite diferentes actividades en la aplicación.
- No permite aplicaciones complejas, aunque si completas.

Informática forense en dispositivos Android

La informática forense es una disciplina en la cual combina elementos de derecho y ciencias de la computación para la recopilación y análisis de información expuesta en sistemas informáticos, redes de comunicación y dispositivos de almacenamiento. Esta área aplica los métodos científicos, herramientas e infraestructura tecnológica para la investigación de sistemas digitales con la finalidad de: asegurar, identificar, preservar, analizar y presentar la evidencia de manera que sea admisible como prueba en un tribunal de justicia. Este proceso normalmente se ejecuta de forma secuencial.(Álvarez Murillo, 2016)

Gráfico No. 18 Fases de una informática forense



Fuente: (Alvarez Murillo, 2016)
Autor: Marco Álvarez

Evidencia digital

En ámbitos legales, la evidencia digital o electrónica es considerada como cualquier clase de información probatoria para la resolución de un caso judicial o extrajudicial, dicha información se puede encontrar almacenada en dispositivos móviles Android, IOS, Tablets, ordenadores y Laptops, además se transmite de manera digital con el objetivo de ser utilizada en una de las partes en un proceso judicial. El proceso para seguir se lo debe ejecutar con la suficiente atención en la recolección, procesamiento y almacenamiento de los objetos digitales o datos de carácter sensible. A menos que la evidencia no será utilizada en un procedimiento legal, procediendo a ejercer la debida precaución y protección de las pruebas. En algunos de los casos una investigación forense se inicia como una recopilación y análisis de los registros y archivos confidenciales convirtiéndola en un análisis criminal.(Álvarez Murillo, 2016)

Adquisición de la evidencia en los dispositivos móviles

Los dispositivos móviles con sistema operativo Android poseen una gran capacidad de almacenamiento de información en sus memorias internas y externas, en lo cual en su interior existe la posibilidad de obtener un material ilícito almacenado. Las evidencias digitales son aquellas que se pueden modificar o alterar e incluso son eliminadas por los cibercriminales para evitar ser descubiertos por entidades judiciales cibernéticas debido a esto se

requiere una valiosa protección que ayude a preservar la evidencia. Cuando un usuario decide borrar un archivo o fichero, el Sistema Operativo no lo elimina completamente, porque la mayoría de ellos cumplen la función de liberar los sectores que ocupa dicho archivo marcándolo como disponible, es decir si no se sobrescriben los sectores la información seguirá almacenada en la memoria del dispositivo Android. Por lo tanto, con la utilización de herramientas o aplicaciones de informática forense se puede recuperar los datos por completo, presentando una serie de pautas para la adquisición de evidencias, borrado seguro de datos y copia bit a bit.(Álvarez Murillo, 2016)

Modo de extracción de la evidencia digital en dispositivos móviles Android

- **Modo depuración USB:** El (USB Debugging) es aquel que permite abrir el acceso directo al sistema por medio del SDK de Android (Software Development Kit), donde es considerado indispensable para la conexión por cable USB entre los dispositivos móviles y el ordenador Una dificultad en el proceso de investigación forense es la habilitación del USB, si el sistema es Root, se encuentra habilitada la depuración USB, donde se procede a conectar el dispositivo móvil y el ordenador a través de la aplicación de consola ADB (Android Debug Bridge) para realiza la copia bit a bit.(Álvarez Murillo, 2016)

- **Habilitación del super usuario en Android o Jailbreak en iOS:** Actualmente la una mayor parte de los usuarios que utilizan dispositivos móviles inteligentes poseen la activación del Sistema Root en Android y Jailbreak en iOS, si es el caso, con la finalidad de poder establecer una conexión entre el ordenador y el dispositivo por medio de USB o por medio del servicio SSH, a partir de dicha conexión, se realiza la

adquisición física bit a bit del dispositivo. Si no es el caso, se procede a investigar aplicando otro método para poder detectar los bugs que permitan escalar privilegios en los Smartphones.(Álvarez Murillo, 2016)

- **Extracción Manual:** Este tipo de extracción se enfoca en la visualización y grabación de la información de la pantalla del dispositivo, con el objetivo de manipular los botones, teclado o pantalla táctil. Este método no permite acceder a los datos que se han eliminado normalmente. La información se recopila mediante fotografías de la pantalla LCD del móvil.(Álvarez Murillo, 2016)

- **Extracción lógica:** Esta extracción se la ejecuta por medio de la conexión del dispositivo Android (Cable USB, RSRs232, WIFI, IRDA Bluetooth.); con un ordenador. El analista forense toma en consideración los problemas asociados a este tipo de investigación, utilizando los protocolos y técnicas de conectividad para finalmente realizar modificaciones en los datos. La extracción se la realiza a través del uso de comandos, y la respuesta se envía a la estación de trabajo.(Álvarez Murillo, 2016)

- **Extracción física:** Esta extracción consiste en adquirir una imagen del material incautado para la ejecución del análisis forense, dicho método obtiene copias necesarias de la imagen original. Una vez que se realiza la copia, se lleva a cabo la investigación forense sin necesidad de utilizar el dispositivo físico, para este tipo de análisis es necesario realizar un backup de información con el objetivo de trabajar en una copia de seguridad conservando la evidencia original.(Álvarez Murillo, 2016)

FUNDAMENTACIÓN LEGAL

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

SECCIÓN VIII

CIENCIA, TECNOLOGÍA, INNOVACIÓN Y SABERES ANCESTRALES

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrán como finalidad:

Generar, adaptar y difundir conocimientos científicos y tecnológicos.

Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 386.- El sistema comprenderá programas, políticas, recursos, acciones, e incorporará a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y privados, empresas públicas y privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación.

CÓDIGO ORGÁNICO INTEGRAL PENAL

SECCIÓN TERCERA

Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Art. 178 Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona tiene una pena privativa de 1 a 3 años.

Artículo 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de

datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que: custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Artículo 233.- Delitos contra la información pública reservada legalmente. La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la cosa o servicio vendido, entregando fraudulentamente un distinto objeto o servicio ofertado en la publicidad, información o contrato o acerca de la naturaleza u origen de la cosa o servicio vendido, entregando una semejante en apariencia a la que se ha comprado o creído comprar, será sancionada con pena privativa de libertad de seis meses a un año.

Si se determina responsabilidad penal de una persona jurídica, será sancionada con multa de diez a quince salarios básicos unificados del trabajador en general.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

LEY DE COMERCIO ELECTRONICO

Art. 5.- Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Art. 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

HIPÓTESIS

1. **¿Existe la posibilidad de que con el desarrollo de una aplicación móvil para dispositivos Android los archivos almacenados en las memorias internas y externas puedan estar protegidos?**

2. **¿Considera usted que con el análisis de vulnerabilidades en los dispositivos móviles Android los usuarios podrán tener conocimiento de los fallos de seguridad detectados para poder aplicar medidas cautelares que ayuden a disminuir los riesgos?**

3. **¿Cree usted que los ataques que se han perpetuado a los Android han afectado la integridad de los usuarios?**

4. **¿Piensa usted que con el crecimiento de intrusiones maliciosas a los dispositivos Android los usuarios puedan emigrar a IPHONE para obtener mayor protección en los archivos?**

5. **¿Al realizar un ataque informático a los dispositivos Android cual sería el tipo de información que puedan comprometer la integridad de los usuarios?**

Variables de investigación

Tabla No. 3 Variables de Investigación

Variables	
Independiente	Análisis y detección de vulnerabilidades mediante internet en dispositivos móviles Android.
Dependiente	Herramientas de test de intrusión previo al desarrollo de una aplicación móvil que facilite la protección de los datos sensibles almacenados.

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

DEFINICIONES CONCEPTUALES

Sistema Operativo: Se lo denomina un software principal o un conjunto de aplicaciones que cumplen tareas específicas gestionando lo recursos de Hardware.

APP: Aplicación informática diseñada como herramienta para poder permitir a los usuarios que puedan realizar gestiones en línea de manera portable desde sus dispositivos móviles Android.

TIC: Tecnologías de la Información y Comunicación que son implementadas en organizaciones de carácter corporativo para ejecutar funciones asignadas por los altos mandos de está mejorando así los procesos de producción y rendimiento de las empresas.

Malware de Android: Es diseñado por los piratas informáticos para tomar el control total de un dispositivo Android conectado a una red de internet con el

objetivo de sustraer la información confidencial del mismo, estos virus son aplicaciones móviles con extensión APK.

Software: Un Software es denominado como un conjunto de repertorios de instrucciones y programas informáticos donde cumplen la función de permitir la ejecución de varias tareas a través de un dispositivo electrónico.

Aplicación: Una aplicación informática se la denomina un programa de software diseñado como un conjunto de herramientas, donde va a permitir realizar una diversidad de tareas que se encuentran disponibles para el usuario.

AHMYTH: Es una aplicación de puerta trasera para dispositivos móviles con sistema operativo Android, cumple las mismas funciones que el Metasploit Framework, pero esta emplea interfaz gráfica para la creación de los archivos virus con extensión APK.

NGROK: Es una herramienta que permite crear túneles de forma segura para establecer conexiones con el servidor de internet, generando un enlace WAN que permite el vínculo a múltiples redes.

APK: Un archivo con extensión .apk (Android Application Package), es un paquete para el sistema operativo Android donde es utilizado para distribuir e instalar componentes empaquetados en dispositivos Android sean: Smartphones, Tablets y demás.

CAPÍTULO III

PROPUESTA TECNOLÓGICA

ANÁLISIS DE FACTIBILIDAD

Según lo analizado en los capítulos uno y dos del proyecto de titulación, se detallaron que los dispositivos móviles con sistema operativo Android son vulnerables a cualquier tipo de virus informático o código malicioso donde los crackers pueden explotar las vulnerabilidades de estos teléfonos inteligentes con el objetivo de obtener el acceso a la información de carácter privado, para finalmente aplicar técnicas de chantaje en beneficio económico ocasionando daños a la integridad del usuario.

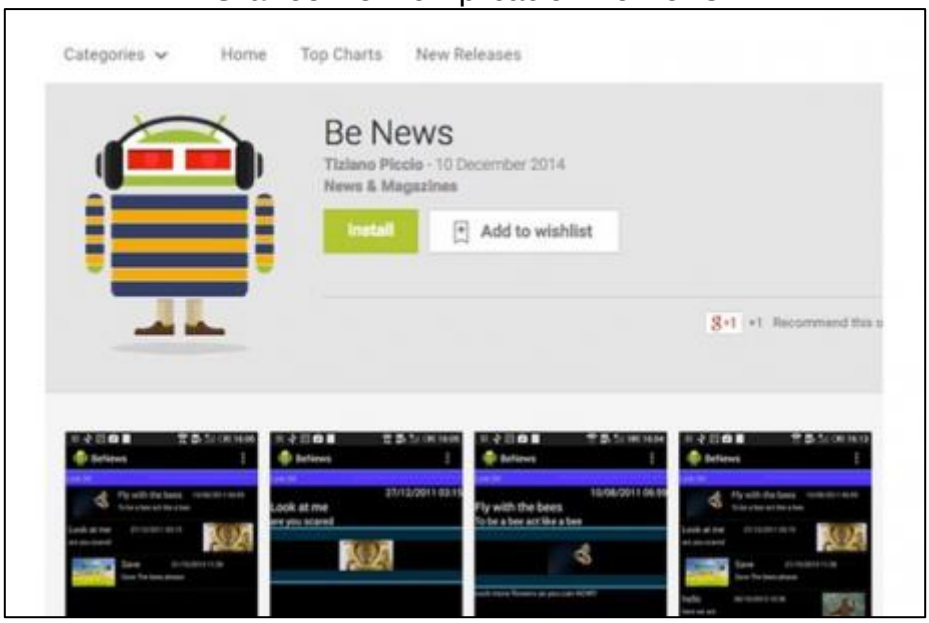
FACTIBILIDAD OPERACIONAL

Según la publicación realizada por Diario El Telégrafo del día 26 de marzo del año 2017, La compañía Operadora de Telefonía Celular (Otecel) que representa a la marca Movistar, revela que en el 2016 sus clientes reportaron como robados 70.462 equipos móviles dejando vulnerable los ficheros sensibles de los usuarios. A través de una encuesta que se realizó se determinó que existe un máximo apoyo por parte de los usuarios que utilizan los dispositivos móviles con sistema operativo Android ya que ellos manejan información multimedia de vital importancia, debido a esto ellos requieren que se desarrolle un prototipo de aplicación móvil Open Source que permita el traspaso de los archivos desde la galería de imágenes.

Según la noticia publicada por el Diario el Comercio en este presente año describe que Hacking Team un famoso pirata informático con ese acrónimo utilizaba una aplicación móvil de noticias falsa con el objetivo de obtener el acceso completo a los dispositivos Android de las víctimas que accedían a esta APP a través de Google Play. La aplicación tenía el nombre de Be News el mismo que poseía un portal web de noticias que existió entre el año 1998 y

2002, esta APP contenía una puerta trasera que permitía el acceso remoto desde internet a los equipos móviles Android una vez que el usuario la haya descargado, instalado y activado, el atacante después de haber tenido el control de un Smartphone este accedía a directorios donde se encontraba información confidencial almacenada, la intrusión de Backdoor explotaba la vulnerabilidad de escalamiento local de privilegios con código CVE-2014-3153 que estaba expuesta en dispositivos móviles Android con versiones 2.2 Froyo y 4.4.4 KitKat.

Gráfico No. 19 Aplicación Be News



Fuente: https://www.elcomercio.com/guaifai/hacking-team-utilizaba-app-falsa.html
Autor: Diario el Comercio

Tomando en consideración los riesgos presentes en los dispositivos Android sobre la perdida excesiva de datos sensibles, el proyecto de titulación faculta la ayuda necesaria a los usuarios con el fin de que ellos puedan tener conocimientos de las vulnerabilidades expuestas en los teléfonos inteligentes y las medidas de protección de información que ayude a reducir el índice de intrusiones maliciosas producidas por los crackers, además con esta

proporción de información referentes a los fallos de seguridad se puede generar un alto nivel de confiabilidad en los usuarios que utilizan estos equipos tecnológicos para gestionar sus actividades ejecutadas a diario.

FACTIBILIDAD TÉCNICA

Dentro de la factibilidad técnica se detallan los siguientes recursos informáticos que serán participes en el proyecto de titulación en desarrollo estos son los siguientes:

Elementos de Hardware

- Computadora Laptop Core i3 con Sistema Operativo Windows de 64 bits y memoria RAM de 4 Gigabytes.
- Tablet Samsung TAB-2
- Nokia 3 con Sistema operativo Android Nougat 7.0.
- Samsung Galaxy J2 PRIME.

Elementos de Software

- Sistema Operativo Kali Linux de 64 bits.
- AHMYTH y NGROK.
- App-Inventor para el desarrollo de aplicaciones Android.

FACTIBILIDAD ECONÓMICA

En esta etapa de la factibilidad económica se detallarán los gastos de los recursos informáticos generados en el proyecto que se muestran en la siguiente tabla, a excepción de los elementos de software por los que son Open Source.

Tabla No. 4 Costos del Proyecto

Descripción	Costo unitario
Samsung J2 PRIME	$ 200
NOKIA 3	$ 300
TABLET Samsung Tab 2	$ 280
Computadora Laptop Core I3	$ 700
Servicio de Internet	$ 20
Otros Gastos	$ 100
TOTAL	$ 1600

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

FACTIBILIDAD LEGAL

En el aspecto legal consiste que el presente proyecto se especifica todos los derechos de autor en cada uno de los expedientes y otros entregables que se desarrollaran en su momento, dichos expedientes se convierten en exclusiva para los usuarios involucrados, de manera radical quedando prohibida la distribución y utilización de este libro en cada una de sus etapas de desarrollo.

Dentro de la factibilidad legal del proyecto de titulación se indican que todas estas pruebas de hacking de dispositivos móviles con sistema operativo Android se las realiza con fines didácticos armando un escenario de prueba ya que con esto no se está vulnerando ni infringiendo las leyes vigentes de las

telecomunicaciones establecidas en la República del Ecuador ni el Código Orgánico Integral Penal.

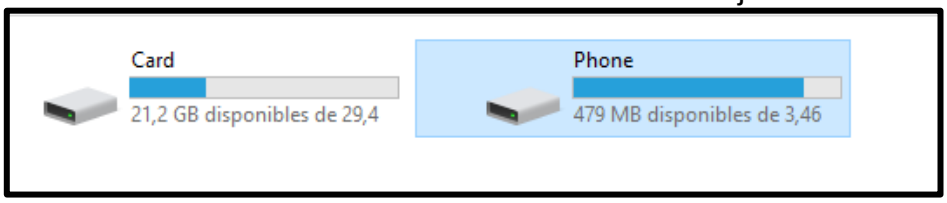
ETAPAS DE METODOLOGÍA DEL PROYECTO

En las etapas de metodología del proyecto se emplea la metodología de cascada donde se detallan las siguientes fases:

- **Fase 1:** En esta fase se realizará un reconocimiento de los archivos multimedia almacenados en los dispositivos móviles Android, una vez obtenido el acceso al Android mediante un ataque.

En la fase 1 se procede a reconocer las memorias integradas en el dispositivo Android como se muestra en el gráfico No. 49.

Gráfico No. 20 Reconocimiento de las tarjetas



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

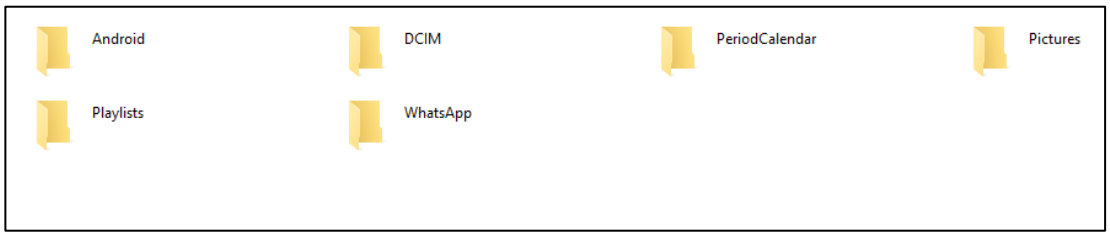
Una vez reconocida las memorias internas y externas se selecciona la primera para verificar los directorios almacenados como se muestra en el gráfico No. 20.

Gráfico No. 21 Reconocimiento de las carpetas almacenadas en la tarjeta de memoria

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

En este caso se procede a reconocer los directorios almacenados en la memoria externa como se muestra en el gráfico No. 21.

Gráfico No. 22 Reconocimiento de las carpetas almacenada en la tarjeta memoria

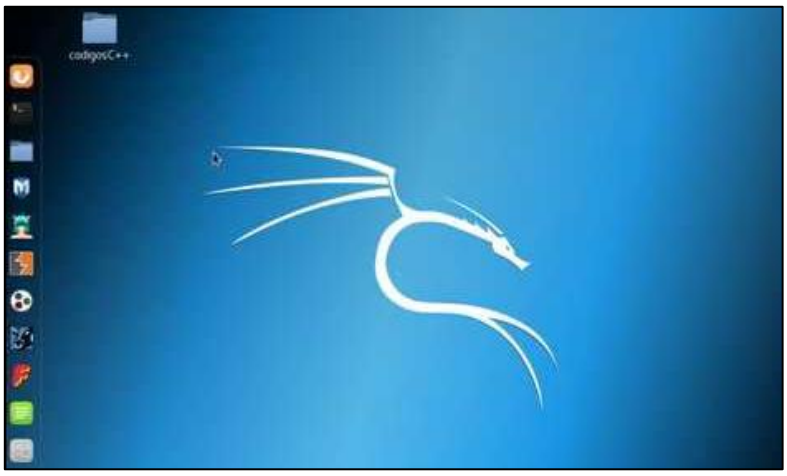


Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

- **Fase 2:** En esta fase se utiliza herramientas Open Source para realizar un ataque en los dispositivos móviles Android determinando el nivel de inseguridad.

Para el cumplimiento de la fase 2 se utilizará el Sistema Operativo Kali Linux para la realización del ataque a los dispositivos móviles Android.

Gráfico No. 23 Kali Linux



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

- **Fase 3:** En esta fase se presentará los respectivos informes detallando las pruebas de Hackeo ético y los respectivos parámetros de protección.

Para el cumplimiento de la fase se empleará un formato de auditoría como se muestra en el gráfico No. 23, para verificar el informe ver anexo III.

Gráfico No. 24 Informes de Auditoría Informática

INFORME DE AUDITORIA

OBJETIVO DE LA AUDITORIA: Verificar y Analizar las vulnerabilidades expuestas en un dispositivo móvil con sistema operativo Android.

ALCANCE DE LA AUDITORIA: Realizar pruebas de hackeo ético en un dispositivo Android determinando los riesgos que pueden ser provocados mediante un ataque informatico

CRITERIOS DE LA AUDITORIA:
Determinación de medidas de protección
Confidencialidad de la información recopilada
Pruebas de Hackeo Ético aplicando ambientes controlados
Definición de controles de seguridad

EQUIPO AUDITOR: Patricio Renan Lanche Lara; Francisco Emanuel Paredes Salinas

FECHA DE AUDITORIA: 25 de julio del 2018

RESULTADOS DE AUDITORIA Y RECOMENDACIONES:

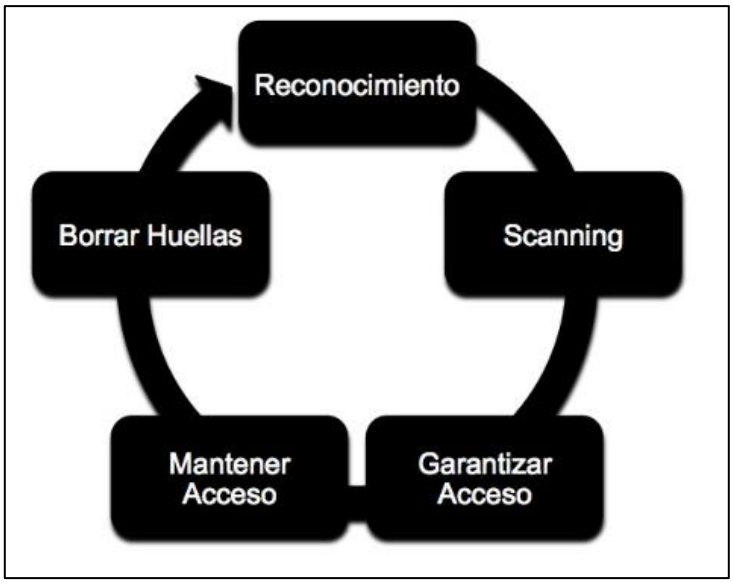
PROCESO	TIPO DE HALLAZGO	HALLAZGO
Explotación de Vulnerabilidades en el dispositivo Android.	Debilidad	Se evidencia el acceso al dispositivo móvil Android verificando la información confidencial multimedia y el nivel de criticidad alto de dicha información.
Análisis de los riesgos detectados.	Debilidad	Se verifica que los riesgos identificados mediante el proceso de test de intrusión en el dispositivo Android son de nivel alto ya que la información que se encuentra almacenada es sumamente sensible.
RECOMENDACIÓN	**TIPO DE RECOMENDACIÓN**	**METODO A EMPLEAR**
Disminuir los indices de ataques en los dispositivos Android.	Fortaleza	Instalar aplicaciones de Antivirus para evitar la propagación de malwares en los Android.
Mantener la información multimedia almacenada en un APP.	Fortaleza	Desarrollar aplicaciones móviles que permitan almacenar información y traspasar archivos desde la galería de imagenes.

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

- **Fase 4:** En esta última fase se implementará un prototipo de aplicación móvil que proporcione el traspaso de imágenes desde la memoria interna y externa del dispositivo móvil Android bloqueando los accesos no autorizados.

Dentro de las etapas de metodología del proyecto también se aplicarán las fases de un hackeo ético, para proceder con la implementación del mismo referente al análisis de vulnerabilidades en los dispositivos Android.

Gráfico No. 25 Fases de un hackeo ético



Fuente: https://www.mindmeister.com/fr/801184808/hacking-etico
Autor: MINDMEISTER

Reconocimiento: En esta fase de un hackeo ético se procederá a ejecutar un reconocimiento previo de los dispositivos móviles con sistema operativo Android aplicando las herramientas adecuadas que ayudarán a cumplir esta fase.

Escaneo: En esta fase de escaneo se procederá a escanear información sobre los dispositivos móviles Android como: direccionamiento IP, direcciones MAC, nombre del equipo móvil y demás datos que serán utilizados en el procese de ataque.

Obtención del acceso: Una vez ejecutado el proceso de escaneo de la información almacenada en los dispositivos móviles Android se utilizarán las

herramientas, para dar inicio con el ataque como: THEFATRAT, N-GROK y demás con el objetivo de determinar los riesgos presentes en las vulnerabilidades escaneadas.

Mantenimiento del acceso: En esta etapa se retendrá los privilegios de acceso a los dispositivos Android obtenidos en la fase anterior, con el objetivo de identificar que elementos pueden ser comprometidos en los Android.

Borrado de huellas: En esta última etapa se eliminará los rastros de acceso a los dispositivos móviles con sistema operativo Android aplicando las herramientas de ocultamiento de dirección IP y demás plataformas de seguridad informática.

Versiones de Android más utilizadas

Antes de proceder con las pruebas de hackeo ético en la siguiente tabla se demuestra las versiones de los sistemas operativos Android más utilizadas.

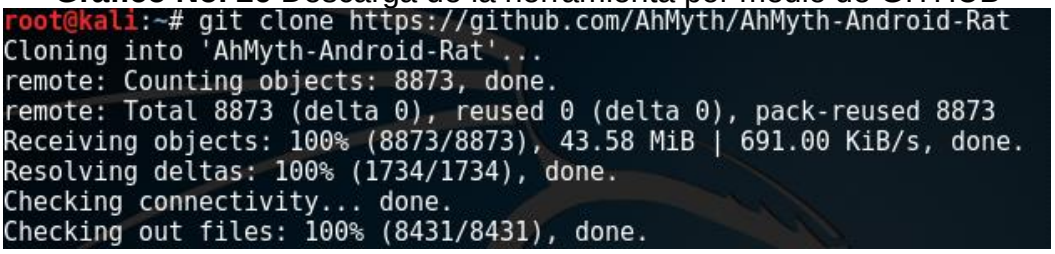
Tabla No. 5 Versiones de Android más utilizadas

Nombre del código	Número de la versión	Fecha de lanzamiento	Nivel del API
APPLE PIE	1.0	23 de septiembre del 2008	1
BANANA BREAD	1.1	9 de febrero del 2009	2
CUPCAKE	1.5	25 de abril del 2009	3
DONUT	1.6	15 de septiembre del 2009	4
ECLAIR	2.0-2.1	26 de octubre del 2009	5-7
FROYO	2.2-2.2.3	20 de mayo del 2010	8
GINGERBREAD	2.3-2.3.7	6 de diciembre del 2010	9-10
HONEYCOMB	3.0-3.2.6	22 de febrero del 2011	11-13
ICE CREAM SANDWICH	4.0-4.0.5	18 de octubre del 2011	14-15
JELLY BEAN	4.1-4.3.1	9 de julio del 2012	16-18
KIT KAT	4.4-4.4.4, 4.4W-4.4W.2	31 de octubre del 2013	19-20
LOLLIPOP	5.0-5.1.1	12 de noviembre del 2014	21-22
MARSHMALLOW	6.0-6.0.1	5 de octubre del 2015	23
NOGAUT	7.0-7.1-7.1.1-7.1.2	15 de junio del 2016	24-25
OREO	8.0-8.1	21 de agosto de 2017	26-27
P	9.0	Lanzamiento para agosto del 2018	28

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Para iniciar con la instalación de la herramienta AHMYTH-ANDROID se procede con la descarga de la aplicación desde la página de github.com

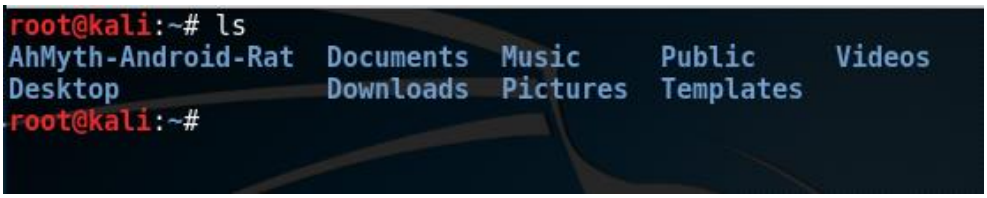
Gráfico No. 26 Descarga de la herramienta por medio de GITHUB



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

Después de haberse instalado el AHMYTH-ANDROID se accede al directorio raíz para la configuración de los archivos.

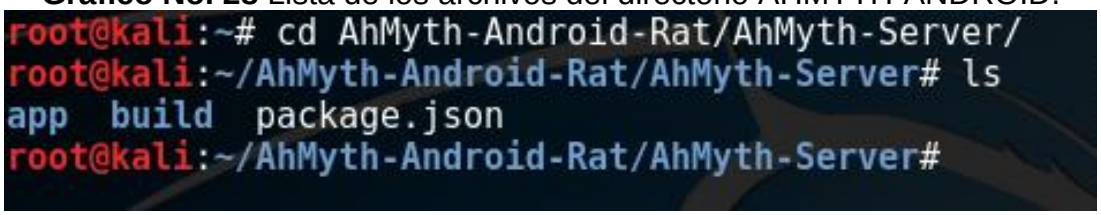
Gráfico No. 27 Acceso a la ruta de AHMYTH-ANDROID



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

En esta parte se lista los archivos que contiene el directorio AHMYTH-ANDROID.

Gráfico No. 28 Lista de los archivos del directorio AHMYTH-ANDROID.



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

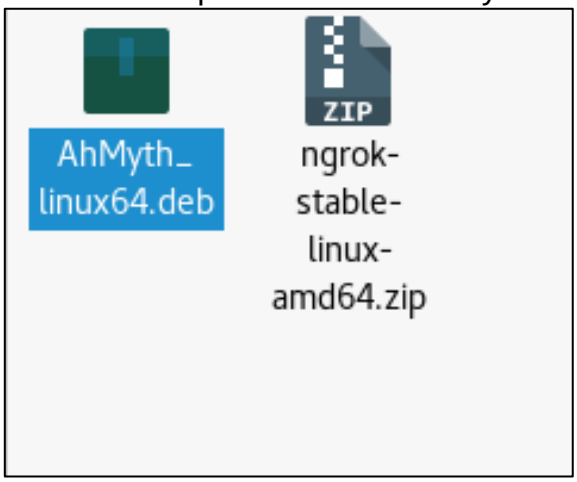
Una vez listado los archivos se dirige al navegador de Kali Linux y accedemos al enlace de github.com que es https://github.com/AhMyth/AhMyth-Android-RAT/releases/ y descargamos el siguiente archivo.

Gráfico No. 29 Descarga del archivo AhMyTH-Android

Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

Una vez descargado el archivo AhMyTH-Android se procede a copiarlo y pegarlo en el escritorio

Gráfico No. 30 Copia del Archivo AhMyth-Android



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

Después de haberse instalado AhMyth-Android se lo procede a buscar en el Kali Linux y se lo activa.

Gráfico No. 31 Instalación de AhMyth-Android

```
root@kali:~# dpkg -i AhMyth_linux64.deb
(Reading database ... 315632 files and directories currently installed.)
Preparing to unpack AhMyth_linux64.deb ...
Unpacking ahmyth (1.0.0) over (1.0.0) ...
dpkg: dependency problems prevent configuration of ahmyth:
 ahmyth depends on libappindicator1; however:
  Package libappindicator1 is not installed.

dpkg: error processing package ahmyth (--install):
 dependency problems - leaving unconfigured
Processing triggers for gnome-menus (3.13.3-8) ...
Processing triggers for desktop-file-utils (0.23-1) ...
Processing triggers for mime-support (3.60) ...
Processing triggers for hicolor-icon-theme (0.15-1) ...
Errors were encountered while processing:
 ahmyth
```

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 32 AhMyth-Android

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Listado de exploits para Android

Antes de proceder con el ataque cibernético a los dispositivos Android, se detallan los exploits que son utilizados para atacar a los dispositivos Android mediante la siguiente tabla.

Tabla No. 6 Listados exploits

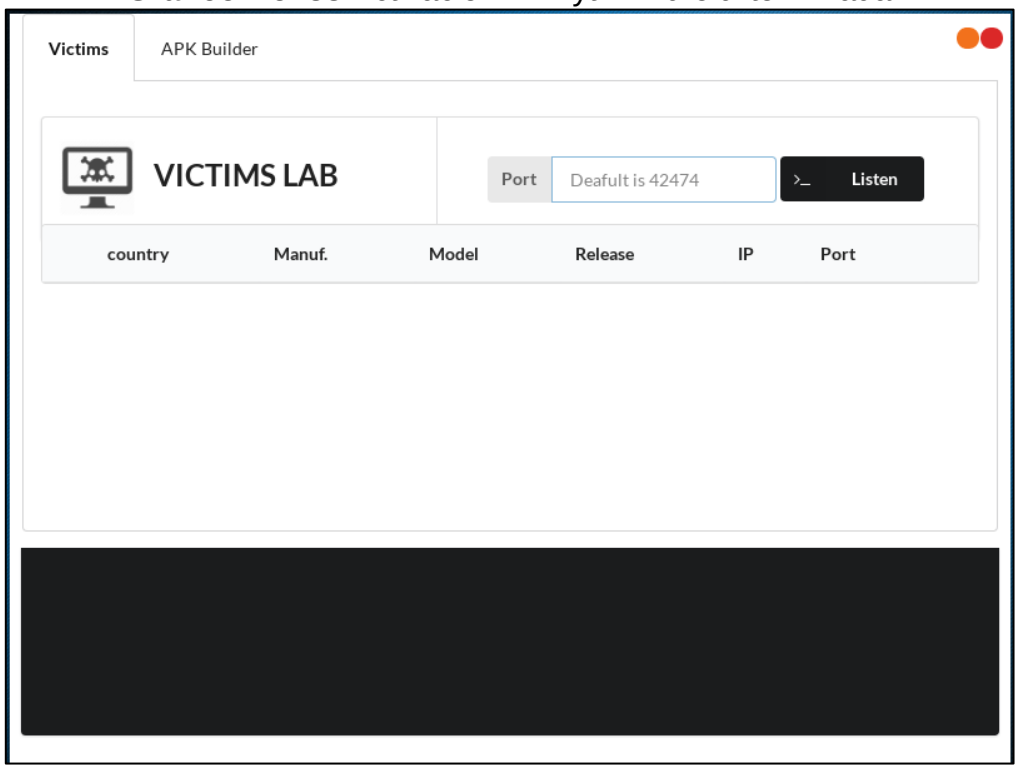
Nombre de los exploits	Dispositivos y servicios afectados
SWAMPMONKEY	Sin definir
BARONSAMEDI	Sin definir
CHRONOS	Ciertos dispositivos MSM con GPUs ADRENO
COLOBUS	Dispositivos equipados con GPUs ADRENO: ADRENO 225, ADRENO 320 y Nexus 7 OS 4.4.2
DUGTRIO	Android 4.0 - 4.1.2 Algunos dispositivos Samsung más recientes podrían tener la vulnerabilidad, pero no está garantizado
EERIEBATTER	Sin definir
EGGSMAYHEM	Navegador Google Chrome: versiones 32-39
FLAAFY	Sin definir
FREEDROID/EERIEINDIANA	Android 2.3.6 - 4.2 Poco fiable en Android 4.3 - 4.4
GALAGO	Galaxy Note 4
BONOBO	Sin definir
DRAGONFLY/BERACUDA	Sin definir
FLAMESKIMMER	Dispositivos con chip WIFI Broadcom 4.4.4 (actualizado julio 2015)
LEVITATOR	pre-2.3-2.3.5

TOTODILE	Dispositivos KitKat
LUGIA	Dispositivos Snapdragon hasta Android 4.4
NIGHTMONKEY	Sin definir
SALAMANDER	Versión Chrome 28.0.1500.94 Explorador Samsung
SALAZAR	Versión Chrome 35.0.1916.141, 37.0.2062.117 Versión Opera 21.0.1437.75710 Explorador Samsung
SIMIAN	Terminales con chip Snapdragon 800
SKOR	Android 2.2 - 2.36
SNUBBLE/SNUBULL	Samsung Galaxy S5 Samsung Galaxy Note 3 Samsung Galaxy S4
SPEARROW	Android 4.1.2
STARMIE	Android 4.0 -4.3 Samsung Galaxy TAB 2 de 10 pulgadas EPIC 4G TOUCH Samsung Galaxy Note
SULFUR	Samsung Galaxy Note 4 3G Samsung Galaxy Note 4
TOWELROOT, STEELIX	OS antes del 3 de junio de 2014

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Una vez activado el AhMyth como se muestra en el Gráfico No. 38 la ventana principal de la herramienta.

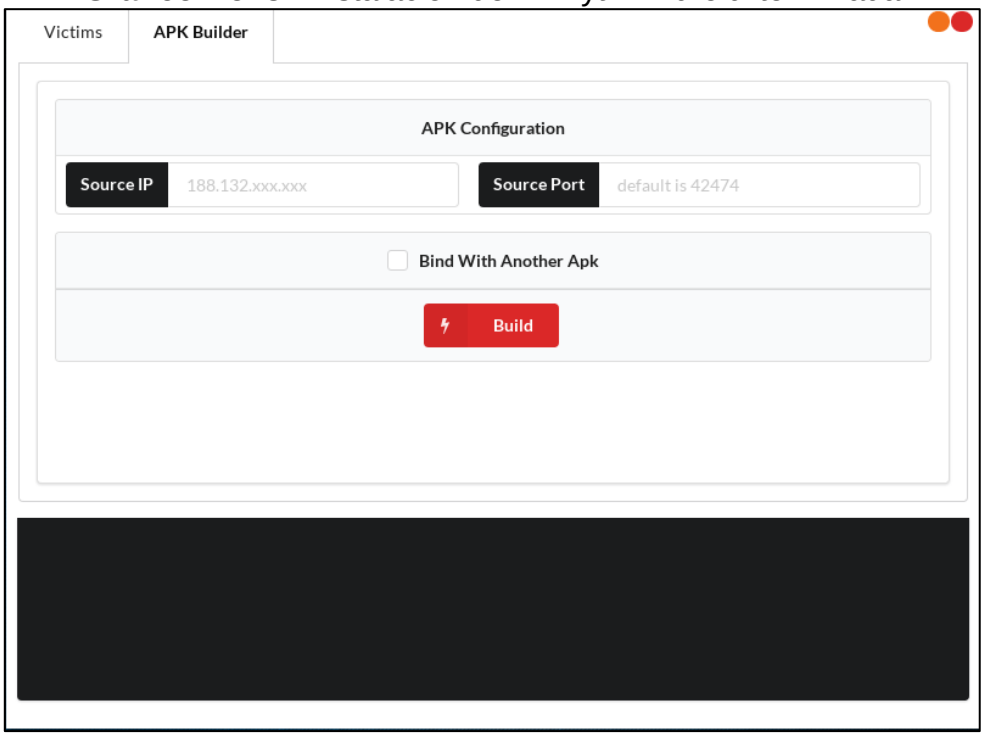
Gráfico No. 33 Activación AhMyth-Android terminada



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

En esta ventana se podrá verificar el dispositivo móvil infectado por un archivo APK.

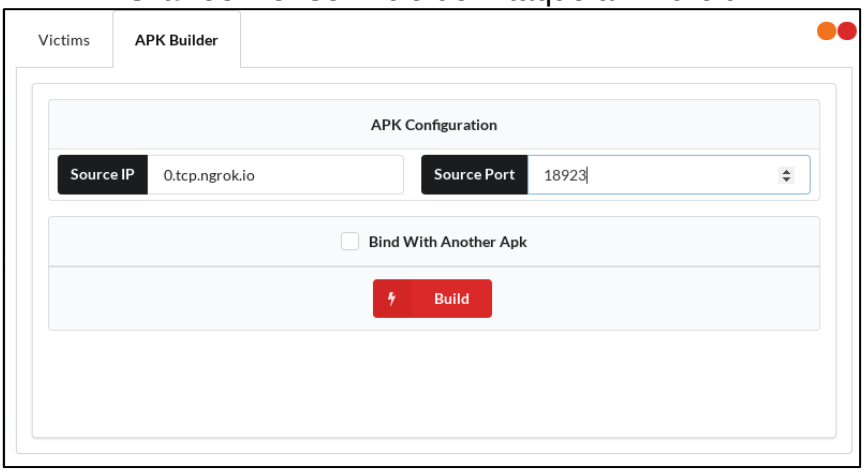
Gráfico No. 34 Instalación de AhMyth-Android terminada



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

En este caso se procede a ingresar el enlace generado por NGROK y el puerto y se le da clic en BUILD.

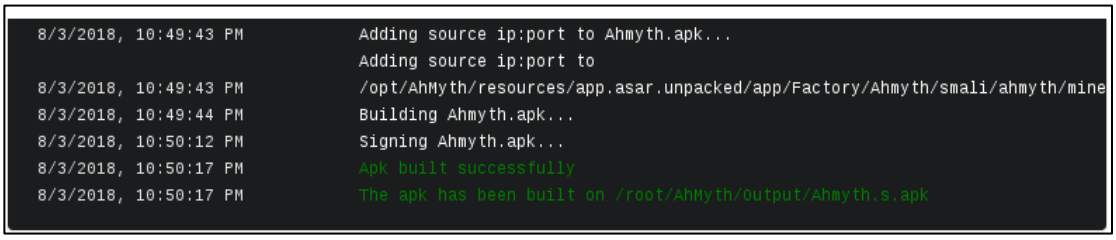
Gráfico No. 35 Inicio del Ataque al Android



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

En este caso se verifica la creación del archivo APK y se accede a la ruta donde se encuentra almacenada.

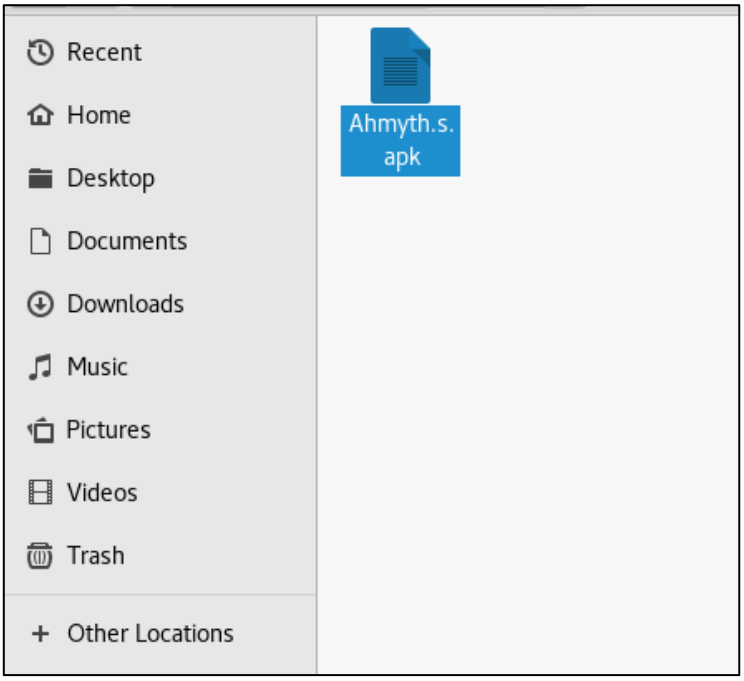
Gráfico No. 36 Creación del Archivo APK



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Una vez accedida a la ruta del archivo APK se procede a renombrarlo.

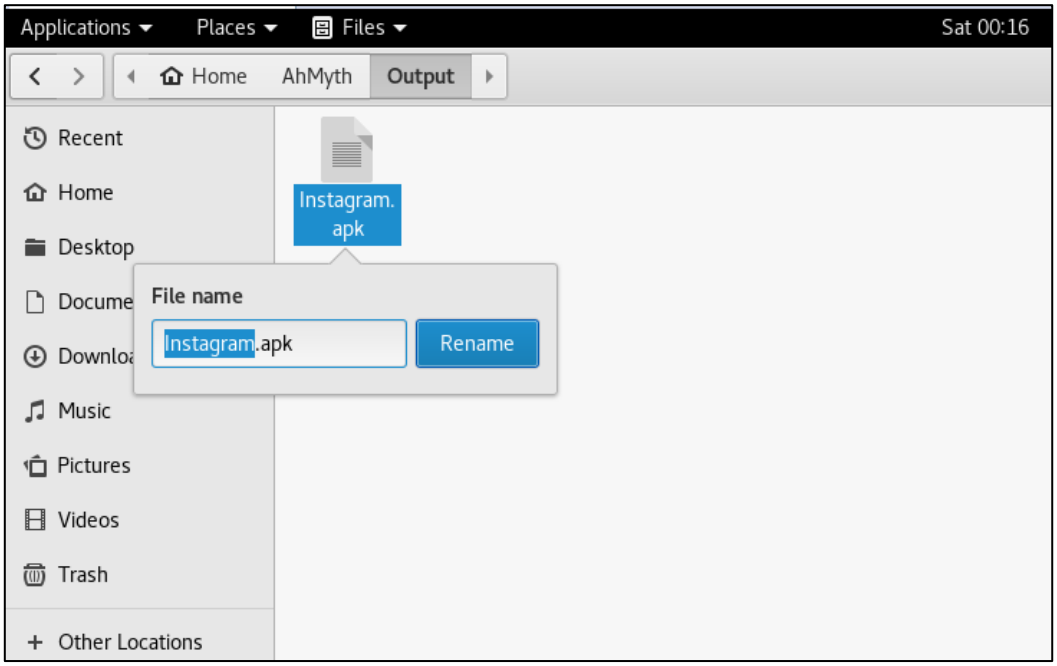
Gráfico No. 37 Acceso a la ruta del APK maliciosa



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

En este caso se verifica el cambio de nombre del archivo APK y se lo procede a copiar al dispositivo móvil víctima.

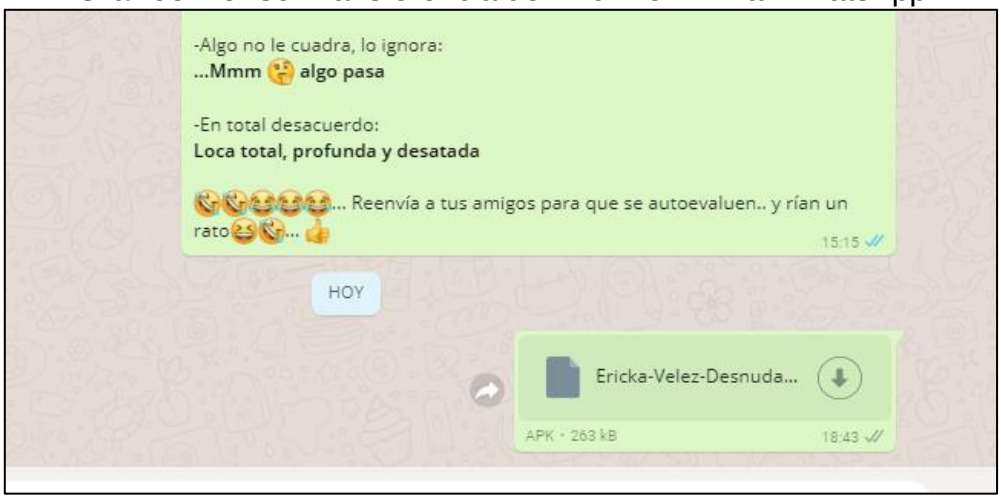
Gráfico No. 38 Cambio de nombre del Archivo



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

En este caso se utiliza WhatsApp como herramienta de transferencia de archivos APK.

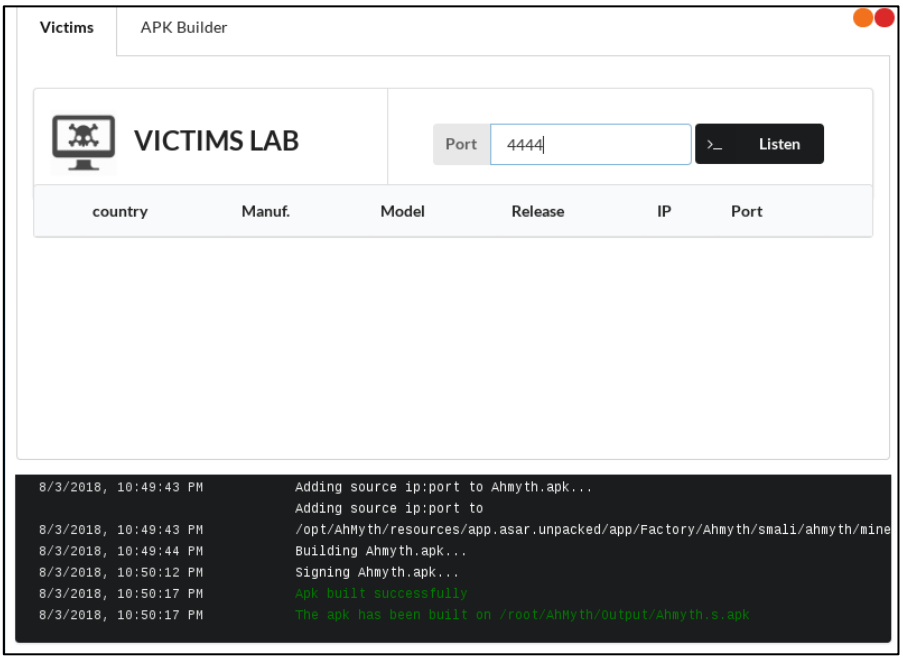
Gráfico No. 39 Transferencia del Archivo APK al WhatsApp



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

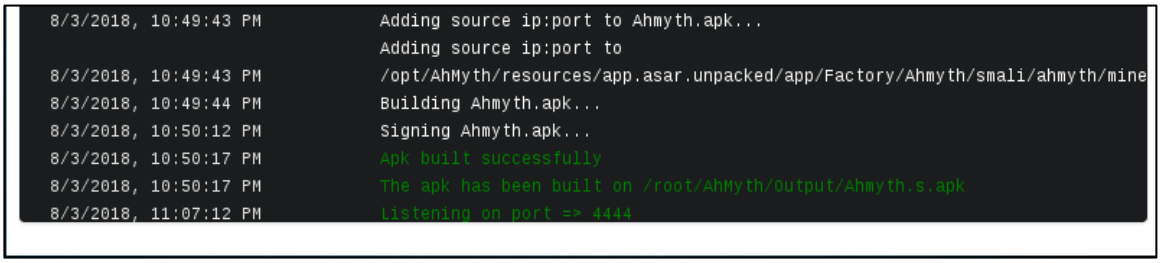
Después de establecer la copia del archivo por medio de WhatsApp se establece la escucha por medio del puerto 4444.

Gráfico No. 40 Puerto Escucha



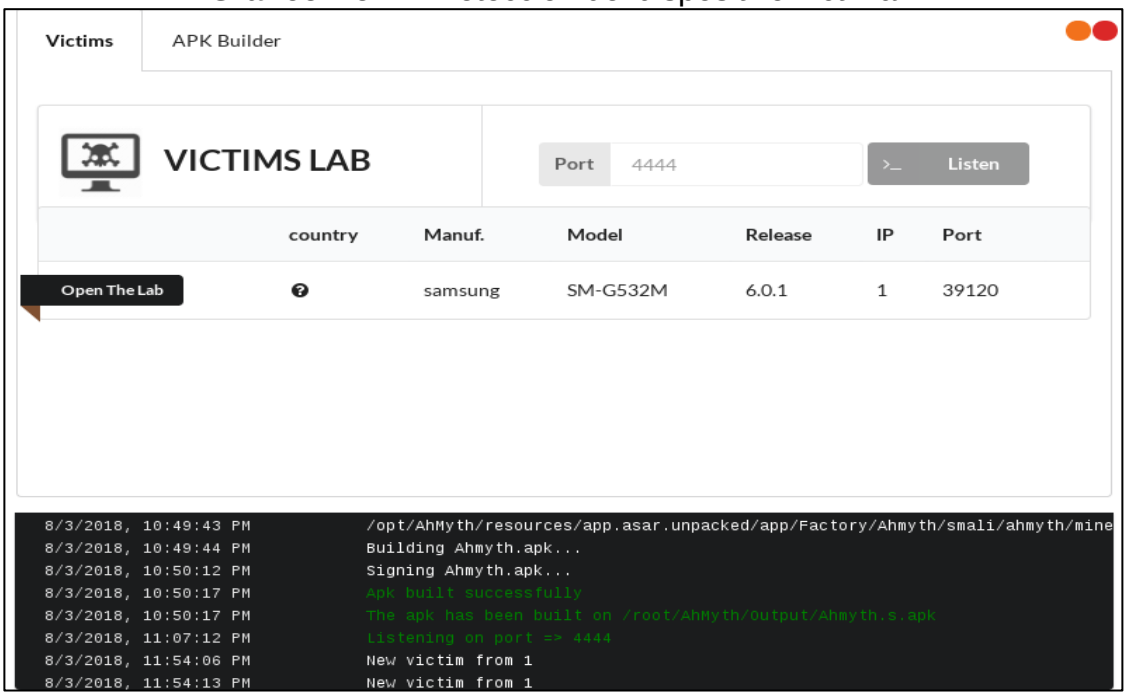
Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 41 Activación del Puerto 4444 en modo escucha



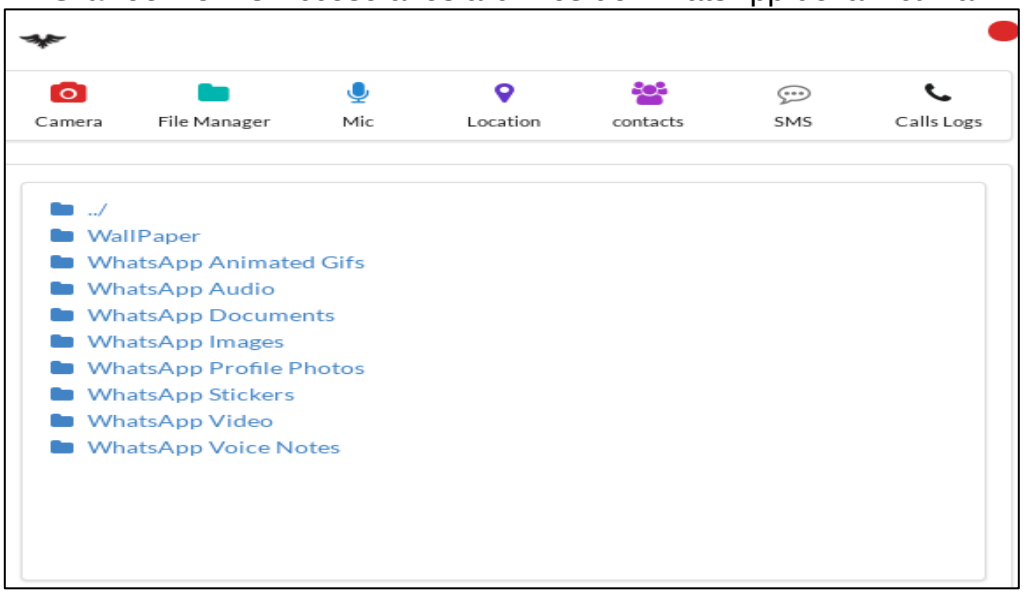
Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 42 Detección del dispositivo víctima



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 43 Acceso a los archivos de WhatsApp de la víctima



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

HACER ANALISIS Y EXPLICAR GRAFICOS

Aplicaciones que proporcionan seguridad informática en los dispositivos Android

En la siguiente tabla se detallan las aplicaciones de seguridad informática para dispositivos Android.

Tabla No. 7 Medios de protección del Android

Aplicación de seguridad informática Android	Descripción
SEEKDROID ANTITHEFT & SECURITY	Esta aplicación móvil cumple con la función de localizar el dispositivo Android en caso de que se genere una pérdida o robo
B-SECURE TRACKER	Esta APP Android proporciona un portal remoto donde por medio de Google Maps el usuario puede tomar fotos, grabar sonidos enviando estos archivos por medio de correo electrónico y localizar el dispositivo.
PERFECT APP PROTECTOR PRO	Esta aplicación de seguridad informática protege las diferentes aplicaciones de banca en línea, redes sociales y permite seleccionar que APP se debe de proteger, además proporciona seguridad en archivos multimedia y en componentes del dispositivo Android.
AIRCOVER SECURITY SUITE	Esta aplicación de seguridad informática proporciona algunos servicios como: protección de datos confidenciales, generación de alertas, protección del GPS, bloqueo remoto y copia de seguridad en la nube.
KASPERSKY INTERNET SECURITY FOR ANDROID	Esta aplicación mantiene los dispositivos móviles Android protegidos ante virus y amenazas presentes en la red de internet
KEEPSAFE	Oculta los archivos multimedia como imágenes y videos almacenados en la memoria interna y externa de los móviles, además esta APP permite que los usuarios ejecuten un traspaso de estos archivos desde las memorias del teléfono Android para almacenarlos en su aplicación eliminando así los ficheros de estos módulos de almacenamiento.

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

ENTREGABLES DEL PROYECTO

Los entregables del proyecto se los detallará a continuación:

- En el anexo I se demuestra el diseño del vector de ataque a los dispositivos Android detallando como se realizaría la intrusión mediante Kali Linux.

- Dentro del capítulo III se detallan las evidencias de los resultados referentes a las pruebas de hackeo ético en los dispositivos Android.

- En este capítulo III se detalla la instalación paso a paso de la herramienta APP Inventor.

- Por último, se detalla la programación de la aplicación móvil en APP Inventor.

INSTALACIÓN Y PROGRAMACIÓN DE LA APLICACIÓN DE GALERIA EN APP INVENTOR

Anexo antes de los entregables

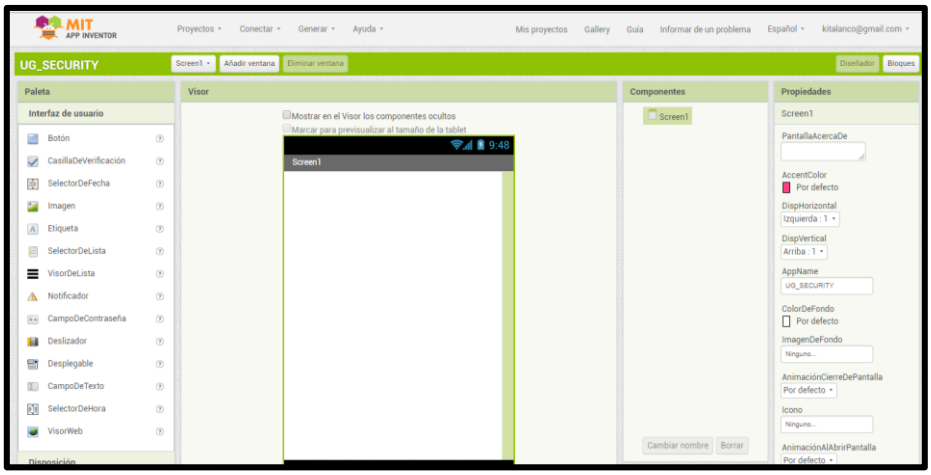
En esta parte se crea el nombre del proyecto UG_SECURITY.

Gráfico No. 44 Creación del proyecto en APP-INVENTOR

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Una vez creado el nombre del proyecto se visualiza la pantalla principal del APP-INVENTOR.

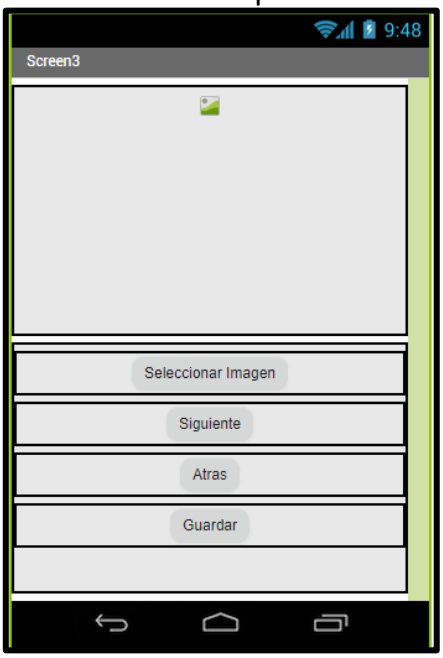
Gráfico No. 45 Inicio de APP-INVENTOR



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

En este caso se diseña la aplicación móvil en APP-INVENTOR.

Gráfico No. 46 Diseño de la Aplicación móvil de Galería



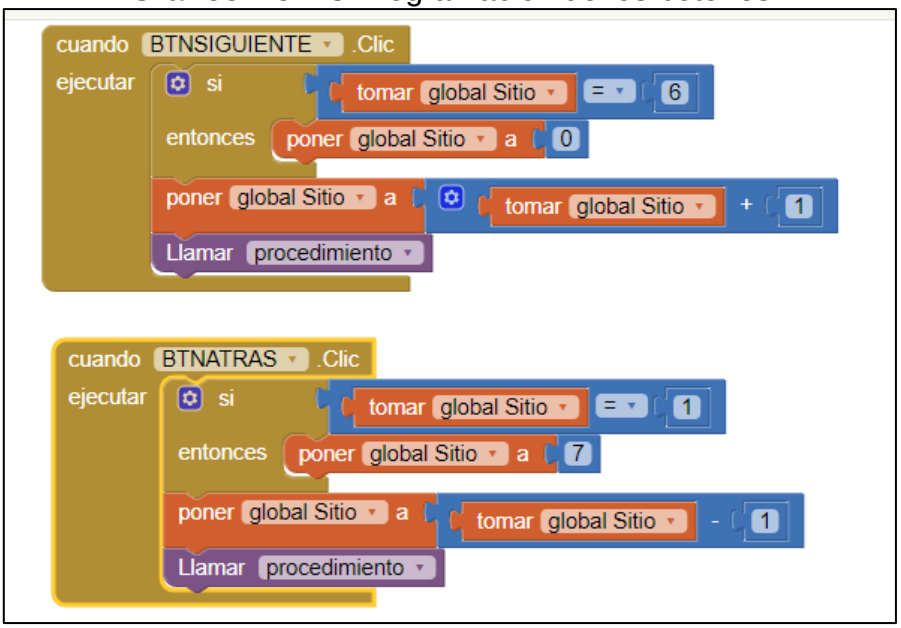
Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Una vez diseñada la pantalla de la aplicación móvil se codifica los botones siguientes y atrás y se invoca el respectivo procedimiento.

Gráfico No. 47 Creación de la variable y el procedimiento

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

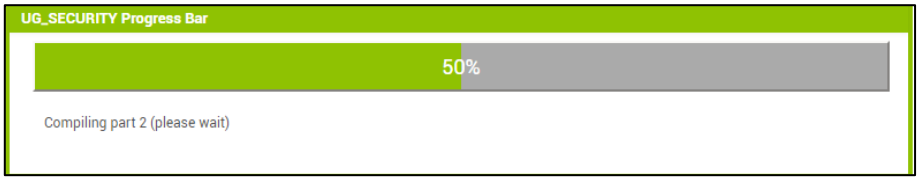
Gráfico No. 48 Programación de los botones



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Una vez codificado los botones Siguiente y Atrás se genera el archivo con extensión APK en el ordenador y se lo transfiere a un Smartphone para realizar las respectivas pruebas.

Gráfico No. 49 Generación del APK



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

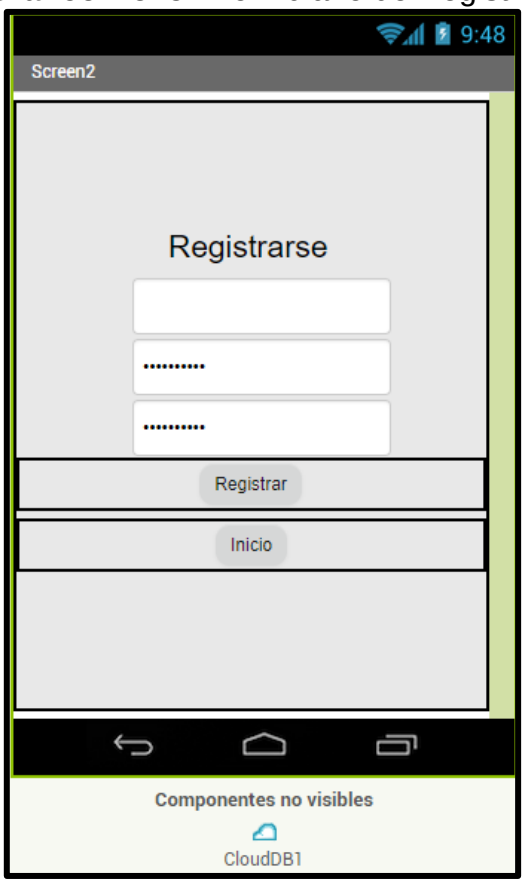
En este caso se crea la pantalla de logueo en APP-INVENTOR.

Gráfico No. 50 Inicio de sesión

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Después de crear la pantalla de logue se crea el formulario de registro en APP-IVENTOR.

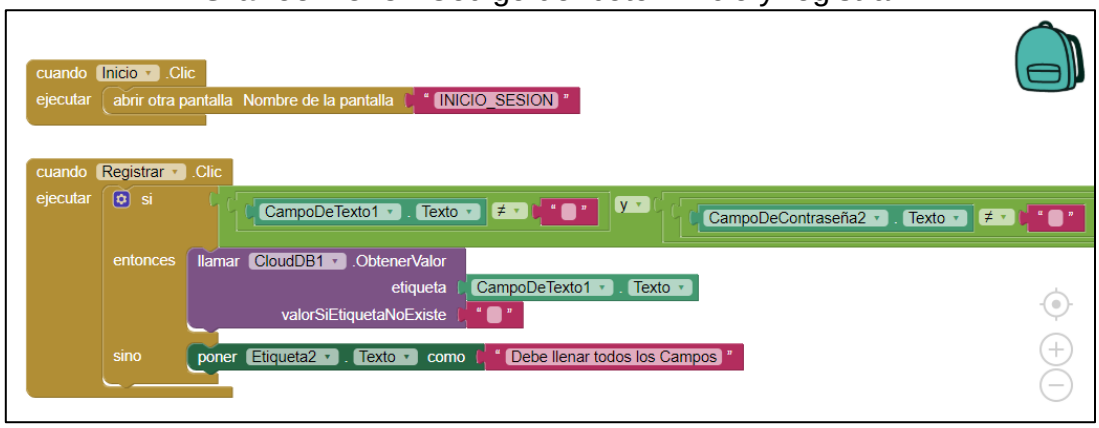
Gráfico No. 51 Formulario de Registro



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

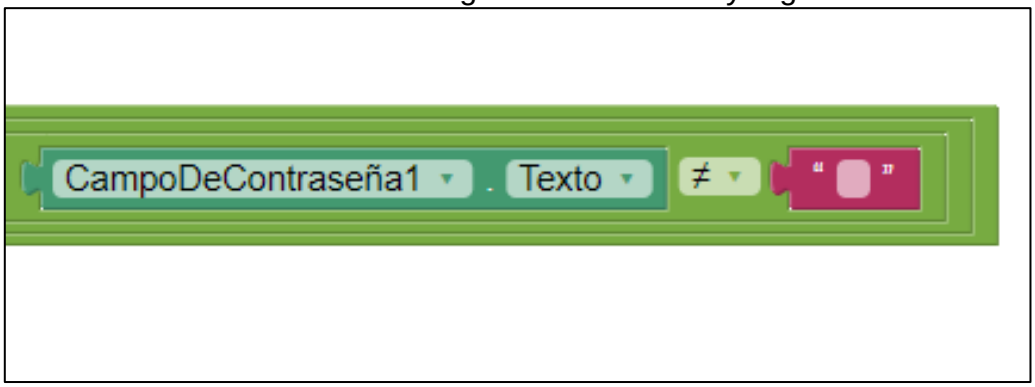
Una vez creada las dos pantallas se programa el botón de inicio y registrar.

Gráfico No. 52 Código del botón inicio y registrar



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 53 Código del botón inicio y registrar



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

En este caso se programa el botón inicio y registrar.

Gráfico No. 54 Código del botón inicio y registrar

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 55 Configuración del botón Ingresar y Registrarse

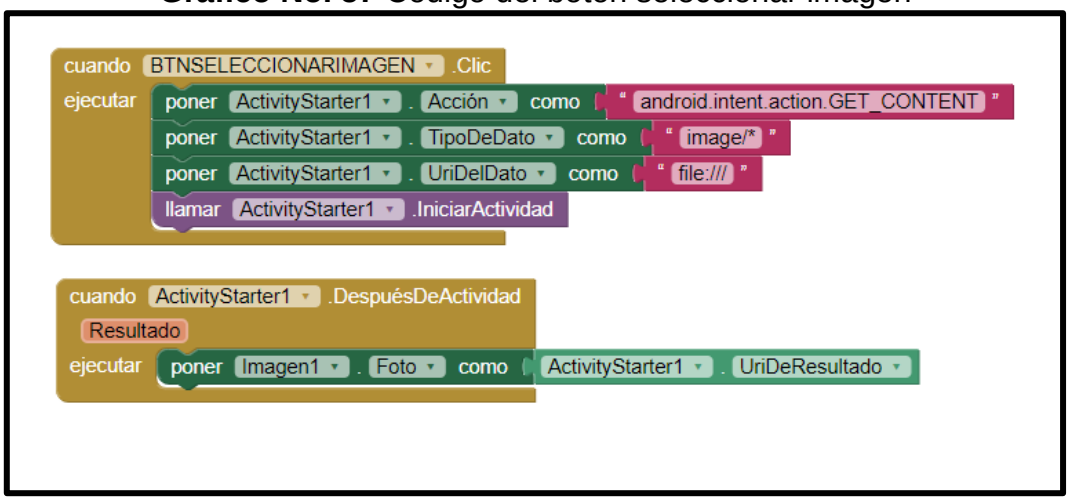
Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 56 Selección de Imagen

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

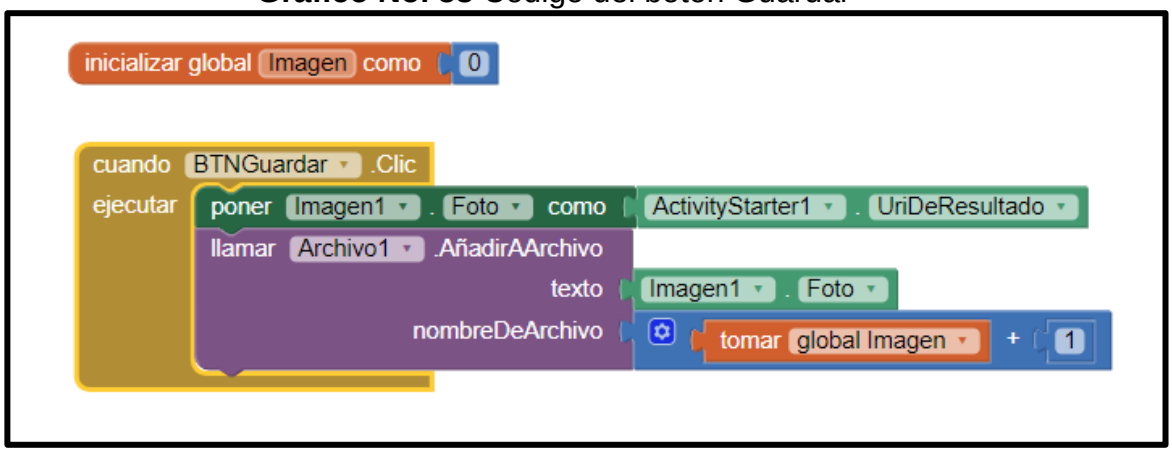
En este caso se programa el botón Seleccionar y Guardar.

Gráfico No. 57 Código del botón seleccionar imagen



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 58 Código del botón Guardar



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

CRITERIOS DE VALIDACIÓN DE LA PROPUESTA

En la siguiente tabla se detallarán los criterios de validación de la propuesta.

Tabla No. 8 Criterios de Validación de la Propuesta

Criterios	Cumple	No cumple	Observación
La propuesta tecnológica es una excelente alternativa para identificar las vulnerabilidades presentes en los dispositivos Android y obtener conocimientos de estas explotándolas a través de una intrusión.	X		
En esta propuesta existen un cumplimiento de los objetivos específicos planteados.	X		
La propuesta tecnológica es ajustable a las necesidades de los usuarios que poseen dispositivos Android.	X		

Los usuarios que posee equipos Android involucrados son los adecuados para la validación del proyecto	**X**		

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

PROCESAMIENTO Y ANÁLISIS

Para el procesamiento y análisis de las preguntas de encuestas se plantea lo siguiente:

- Planteamiento total de 6 preguntas con opciones de respuesta.
- Utilización de gráficos de pastel para la tabulación de los resultados.
- Utilización de la herramienta Google Form para aplicar la respectiva tabulación de los resultados a través de diagrama de pastel.
- Total, de encuestados 34 personas.

ANÁLISIS DE LAS ENCUESTAS

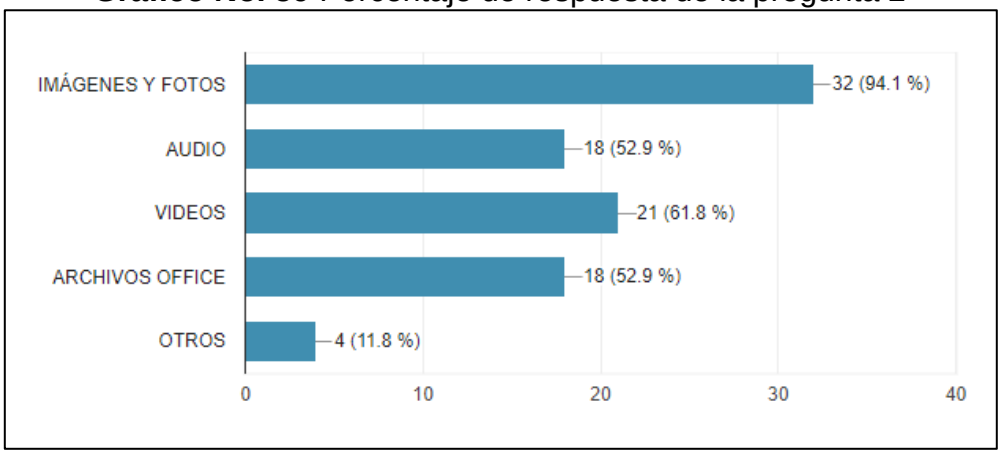
1. **¿Qué tipo de información almacena en su dispositivo móvil Android?**

Tabla No. 9 Pregunta 2

Opciones	Porcentaje
IMÁGENES Y FOTOS	94.10 %
AUDIO	52.90 %
VIDEO	61.80 %
ARCHIVOS OFFICE	52.90 %
OTROS	11.80 %

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 59 Porcentaje de respuesta de la pregunta 2



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Análisis: Durante la encuesta se verifico que la mayor parte de los usuarios almacenan en sus dispositivos móviles Android Imágenes, Fotos y Videos con el 94.10 % y 61.80 % respectivamente, en esta pregunta se aplicó opción múltiple.

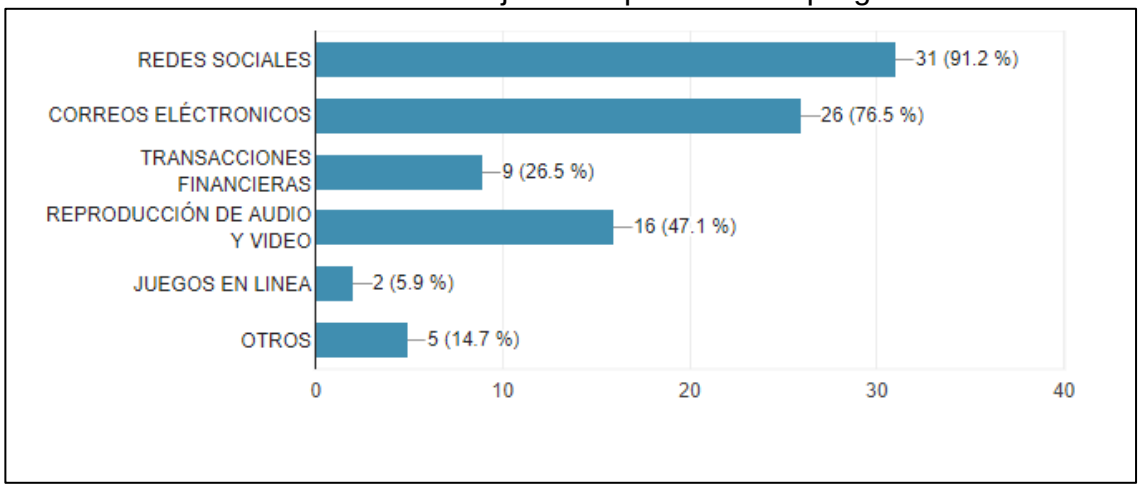
2. **¿Qué tipo de gestión en línea ejecuta en su dispositivo móvil Android?**

Tabla No. 10 Pregunta 3

Opciones	Porcentaje
REDES SOCIALES	92.10 %
CORREOS ELÉCTRONICOS	76.50 %
TRANSACCIONES FINANCIERAS	26.50 %
REPRODUCCIÓN DE AUDIO Y VIDEO	47.10 %
JUEGOS EN LÍNEA	5.90 %
OTROS	14.70 %

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 60 Porcentaje de respuesta de la pregunta 3



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Análisis: Durante la encuesta se verifico que la mayor parte de los usuarios ejecutan aplicaciones en línea en sus dispositivos móviles Android como Redes Sociales, Correos Electrónicos y Reproducción de Audio y Video con el 91.20 %, 76.50 % y 47.10 % respectivamente, en esta pregunta se aplicó opción múltiple.

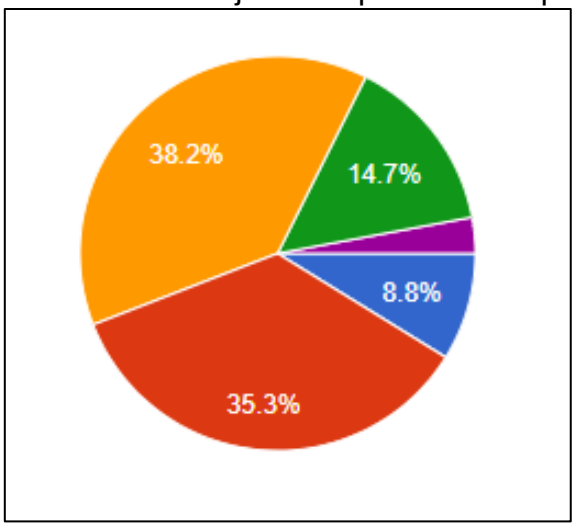
3. **¿De las diferentes aplicaciones que sirven para proteger los archivos que se almacenan en los dispositivos móviles Android existentes en Play Store cree usted que son 100% seguras?**

Tabla No. 11 Pregunta 4

Opciones	Cantidad	Porcentaje
TOTALMENTE DE ACUERDO	3	8.80 %
DE ACUERDO	12	35.30 %
NI DE ACUERDO, NI EN DESACUERDO	13	38.20 %
EN DESACUERDO	5	14.70 %
TOTALMENTE EN DESACUERDO	1	2.90 %
Total	34	100 %

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 61 Porcentaje de respuesta de la pregunta 4



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Análisis: Durante la encuesta se verifico que los usuarios no despiertan ningún interés en creer que las aplicaciones de la PLAY STORE son 100 % seguras

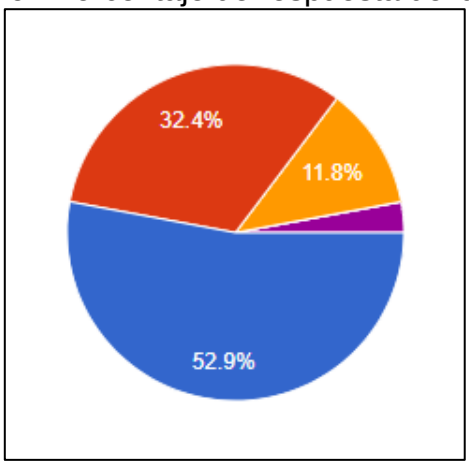
4. **¿Existen un sin número de aplicaciones que permiten interactuar al usuario con la web, usted tiene conocimiento de que al usarlas pueden estarle robando información importante sin que él se dé cuenta?**

Tabla No. 12 Pregunta 5

Opciones	Cantidad	Porcentaje
TOTALMENTE DE ACUERDO	18	52.90 %
DE ACUERDO	11	32.40 %
NI DE ACUERDO, NI EN DESACUERDO	4	11.80 %
EN DESACUERDO	0	0 %
TOTALMENTE EN DESACUERDO	1	2.90 %
Total	34	100 %

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 62 Porcentaje de respuesta de la pregunta 5



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Análisis: Durante la encuesta se verifico que los usuarios están totalmente de acuerdo que existen un sin número de aplicaciones que interactúan con los servicios WEB que al utilizarlas de mala manera los atacantes pueden sustraer información confidencial del usuario sin que él se dé cuenta de este proceso.

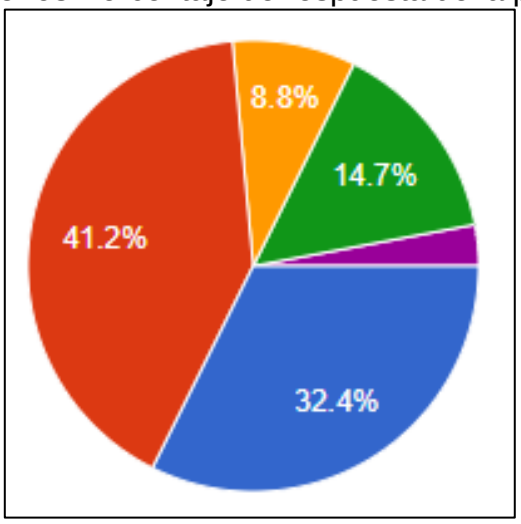
5. **Por cuestiones de licenciamiento en algunas aplicaciones que brindan seguridades, existen usuarios que no utilizan todos sus componentes y por este motivo se sienten limitados en la protección de su dispositivo móvil Android ¿Está usted de acuerdo que existan aplicaciones de software libre que tengan los mismos beneficios que las que son pagadas?**

Tabla No. 13 Pregunta 6

Opciones	Cantidad	Porcentaje
TOTALMENTE DE ACUERDO	11	32.40 %
DE ACUERDO	14	41.20 %
NI DE ACUERDO, NI EN DESACUERDO	3	8.80 %
EN DESACUERDO	5	14.70 %
TOTALMENTE EN DESACUERDO	1	2.90 %
Total	34	100 %

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 63 Porcentaje de respuesta de la pregunta 6



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Análisis: Durante la encuesta se verifico que los usuarios están de acuerdo que existan aplicaciones de software libre que tengan los mismos beneficios que las que son pagadas.

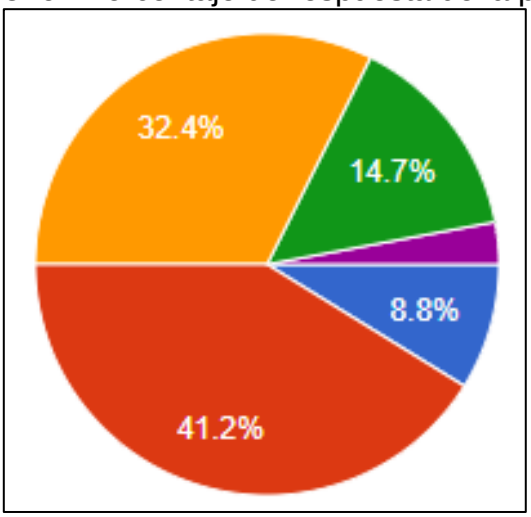
6. **De acuerdo con las aplicaciones que brindan seguridades a los archivos almacenados en los dispositivos móviles Android ¿Cree usted que se puede confiar en los resultados obtenidos?**

Tabla No. 14 Pregunta 7

Opciones	Cantidad	Porcentaje
TOTALMENTE DE ACUERDO	3	8.80 %
DE ACUERDO	14	41.20 %
NI DE ACUERDO, NI EN DESACUERDO	11	32.40 %
EN DESACUERDO	5	14.70 %
TOTALMENTE EN DESACUERDO	1	2.90 %
Total	34	100 %

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Gráfico No. 64 Porcentaje de respuesta de la pregunta 7



Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Análisis: Durante la encuesta se verifico que los usuarios están de acuerdo que las aplicaciones móviles Android creen que puedan presentar resultados obtenidos.

VALIDACIÓN DE LAS ENCUESTAS

Dentro de las personas encuestadas se verifico que la mayoría de ellos utilizan los Smartphones para realizar sus tareas a diario y los mismos están totalmente de acuerdo que se empleen medidas de seguridad en los dispositivos móviles y así evitar la sustracción de la información sensible que es causada por piratas informáticos de los cuales gran cantidad de usuarios están de acuerdo que existan aplicaciones Open Source para la protección de los archivos multimedia. También los usuarios utilizan los dispositivos Android para almacenar imágenes y fotos, navegar por redes sociales y demás.

CAPÍTULO IV

CRITERIOS DE ACEPTACIÓN DEL PRODUCTO O SERVICIO

Tabla No. 15 Criterios de Aceptación del Producto o Servicio

Requerimientos	Cumplimiento
Diseño del vector de ataque hacia los dispositivos móviles Android.	X
Ejecución del ataque aplicando las herramientas NGROK y AhMyth-Android.	X
Instalación de la aplicación APP INVENTOR.	X
Desarrollo de la aplicación móvil en APP INVENTOR.	X
Análisis de los resultados de las encuestas en Google FORM.	X
Adquisición del dispositivo móvil Android que participará en la prueba de ataque.	X
Aplicación de las fases de un hackeo ético para la ejecución del ataque.	X

Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

CONCLUSIONES

- Mediante la fase de reconocimiento que se realizó en el dispositivo móvil Android se detectó que estos manejan diferentes servicios por medio de sus aplicaciones donde las mismas se enlazan con servidor WEB para proporcionar los recursos a los usuarios.

- Por medio del análisis de vulnerabilidades en los dispositivos móviles con sistema operativo Android se identificó que estos poseen fallos de seguridad en su kernel, en lo cual a través de un archivo con extensión APK malicioso puede acceder a los ficheros almacenados en las memorias internas y externas y se detectó que la red móvil que los teléfonos emplean posee inseguridades ya que mediante la herramienta NGROK el ataque se lo puedo ejecutar desde la red de internet.

- Por medio de informes se pudo detallar los resultados obtenidos por medio del ataque hacia los dispositivos Android aplicando la herramienta NGROK y AHMYTH donde la primera permite establecer una conexión con el móvil desde el internet y la segunda crea el archivo APK malicioso.

- El desarrollo de aplicaciones móviles Android es de vital importancia ya que se puede elaborar una gran variedad de estas aplicando los diferentes entornos de trabajo y enfocándose en las necesidades del cliente, las aplicaciones Android es el medio más relevante ya que en su programación podemos implementar una función o método que permita proteger los archivos almacenados en los dispositivos Android ante ataques cibernéticos.

RECOMENDACIONES

- Implementar métodos de protección en cada aplicación a instalar en los dispositivos móviles Android validando los datos de los usuarios y empleando túneles de comunicación entre la aplicación Android y el usuario.

- Realizar auditorías de seguridad informática con el objetivo de seguir evaluando los dispositivos móviles y definir que nuevas técnicas de protección se pueden emplear en los dispositivos Android.

- Por medio de informes de auditoría de seguridad en dispositivos móviles dar a conocer y concientizar a los usuarios sobre el almacenamiento masivo de archivos confidenciales y los tipos de riesgos que se pueden acarrear al no llevar un control de toda la información grabada.

- Proponer el desarrollo de aplicaciones móviles para emplear medidas de protección en los dispositivos Android y evitar ataques cibernéticos que conlleven al robo de información confidencial que a su vez afecte la integridad del usuario.

BIBLIOGRAFÍA

Albarrán, J. A. D., & Universidad. (2013). MALWARE EN ANDROID.

Alvarez Murillo, M. A. (2016). Análisis forense en dispositivos móviles iOS y Android, 1–79. Retrieved from http://hdl.handle.net/10609/45641

Bustos, D. M. (2015). (ANDROID) Acceso a Internet, 1–12.

CANO, J. J. M. (2017). ESTUDIO MONOGRAFICO ACERCA DEL CIBERCRIMEN EN DISPOSITIVOS MÓVILES CON S.O. ANDROID.

Date, I., & Type, I. (2018). Hacking ético para dispositivos m ? viles inteligentes.

Gonsalves, A., & Kulkarni, C. (2017). A Tool for Preventing the Metasploit Attack on the Android OS, *5*(5), 325–328.

Kryscia Ramírez Benavides, R. (2014). App I nventor.

León, C. G. (2015).
Analisis_Y_Explotacion_De_Vulnerabilidades_En_Android.

Milán, M. (2014). Trabajo de fin de grado.

Navarro, A., Londoño, S., Urcuqui López, C. C., & Gomez, J. (2014). Análisis y caracterización de frameworks para detección de aplicaciones maliciosas en android. *Conference: XIV Jornada Internacional de Seguridad Informática ACIS 2014*, *14*, 1–12. Retrieved from

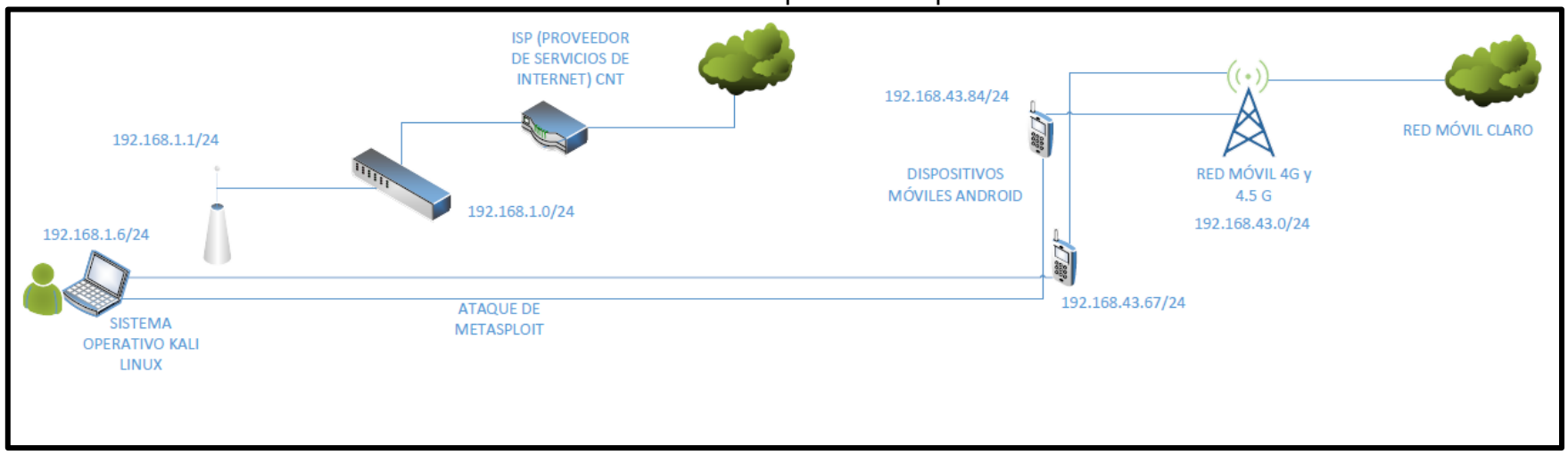
https://www.researchgate.net/publication/263236428_Analisis_y_caracterizacion_de_frameworks_para_deteccion_de_aplicaciones_maliciosas_en_android

YÁNEZ, R. A. A. (2018). ANÁLISIS COMPARATIVO EN TÉRMINOS DE SEGURIDAD DE LA INFORMACIÓN Y RENDIMIENTO ENTRE SISTEMAS OPERATIVOS ANDROID E IOS EN TELÉFONOS MÓVILES. PROYECTO, 1–36.

ANEXOS

Anexo I: Diseño del vector de ataque a los dispositivos Android

Gráfico No. 65 Diseño del vector de ataque a los dispositivos Android



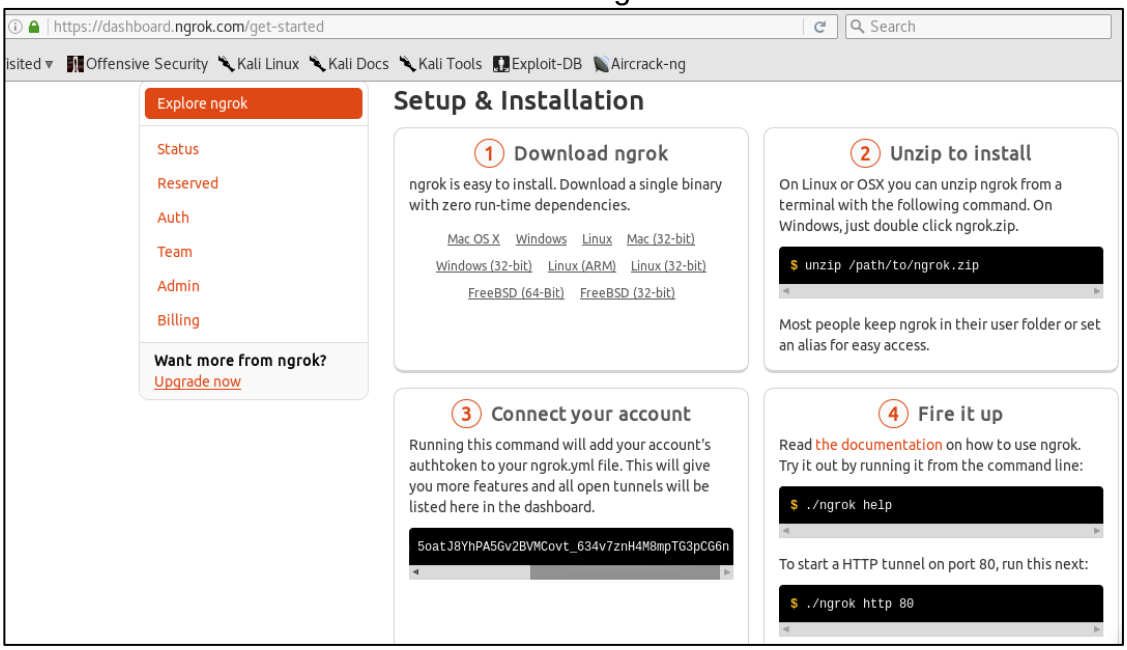
Fuente: Trabajo de Investigación
Autor: Renan Lanche-Francisco Paredes

Anexo II: Instalación de NGROK

Instalación de NGROK

Para iniciar con el ataque a un dispositivo Android se procede a instalar la herramienta NGROK que permitirá efectuar la intrusión desde el internet. En este caso se dirige a la siguiente URL https://dashboard.ngrok.com/get-started y con esto se ejecuta la descarga de NGROK.

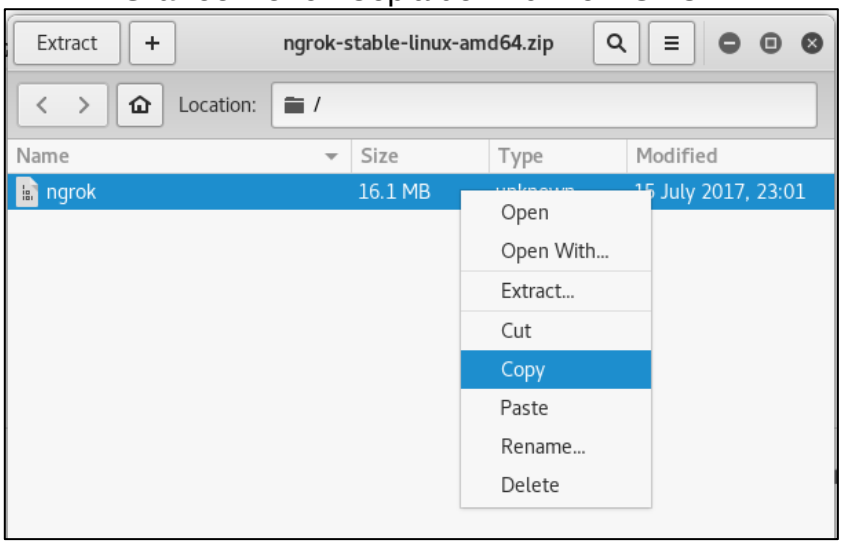
Gráfico No. 66 Descarga de NGROK



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

Después de haber descargado la herramienta NGROK se dirige a la ruta donde se almacena el archivo y se realiza una copia de este archivo al escritorio del sistema operativo Kali Linux.

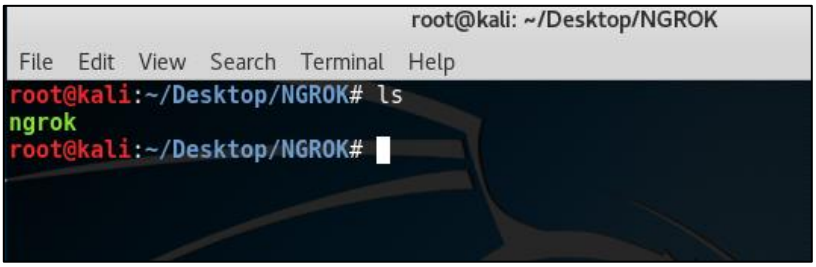
Gráfico No. 67 Copia del Archivo NGROK



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

Una vez establecida la copia del archivo a la nueva ruta se lista el directorio para verificar el archivo NGROK.

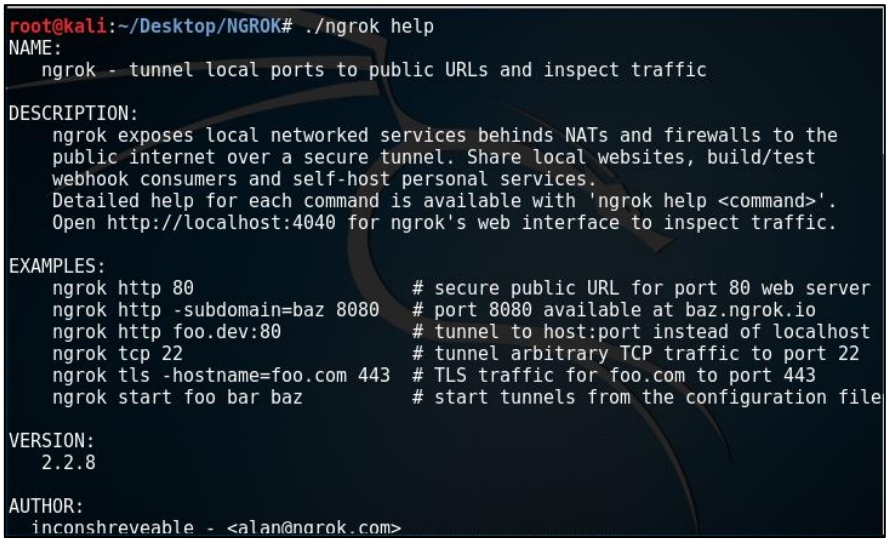
Gráfico No. 68 Acceso a la nueva ruta de NGROK



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

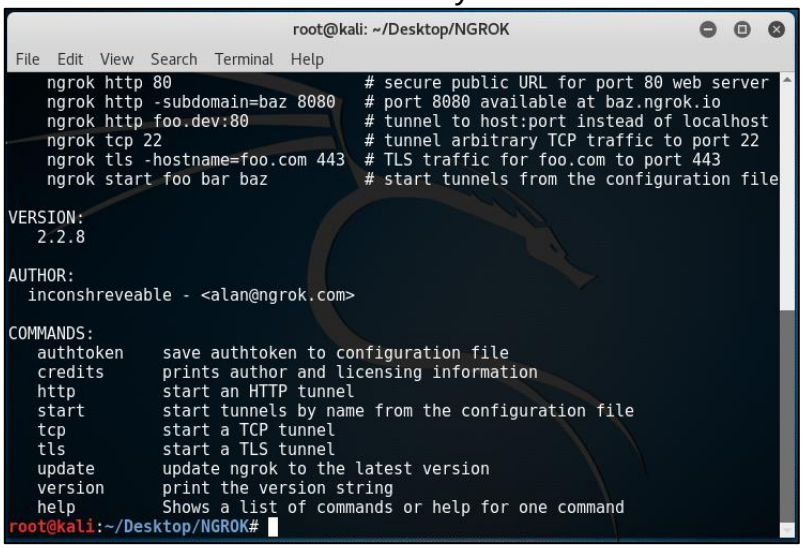
En esta ocasión se procede a verificar el modo ayudo que proporciona la herramienta NGROK.

Gráfico No. 69 Verificación del HELP del archivo NGROK



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

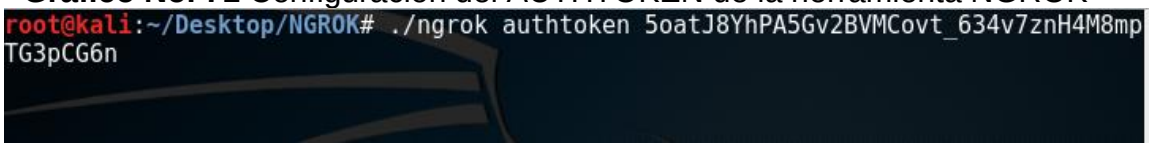
Gráfico No. 70 Verificación del modo ayuda de la herramienta NGROK



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

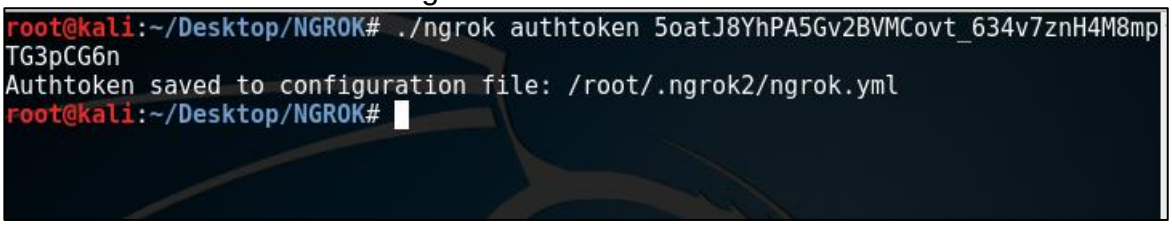
Antes de ejecutar la herramienta NGROK se procede con la configuración del AUTHTOKEN de la misma aplicación.

Gráfico No. 71 Configuración del AUTHTOKEN de la herramienta NGROK



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

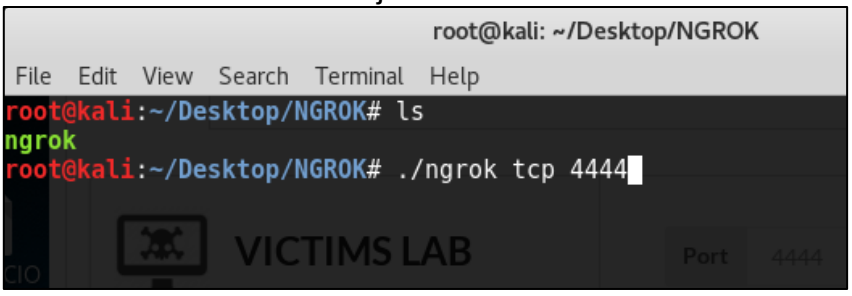
Gráfico No. 72 Configuración del AUTHTOKEN almacenada



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

Después de la configuración del AUTHTOKEN se procede con la ejecución de la herramienta NGROK.

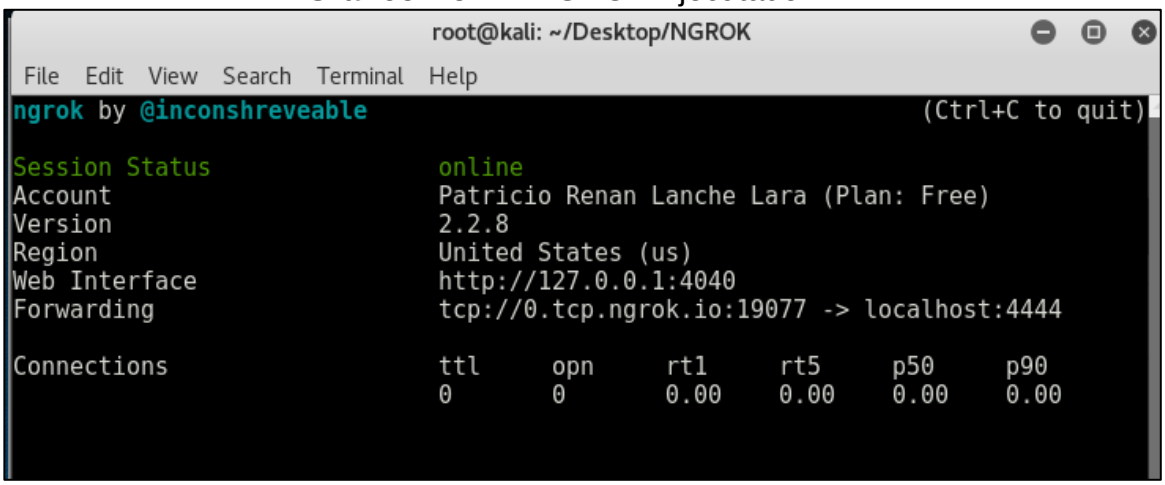
Gráfico No. 73 Inicio de la ejecución de la herramienta NGROK



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

Una vez ejecutada la herramienta NGROK se procede a verificar las características de esta aplicación para después dar inicio con el ataque a los dispositivos Android.

Gráfico No. 74 NGROK Ejecutado



Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

Anexo III: Informe de Auditoría

Gráfico No. 75 Informe de Auditoría

	INFORME DE AUDITORIA	

OBJETIVO DE LA AUDITORIA: Verificar y Analizar las vulnerabilidades expuestas en un dispositivo móvil con sistema operativo Android.		
ALCANCE DE LA AUDITORIA: Realizar pruebas de hackeo ético en un dispositivo Android determinando los riesgos que pueden ser provocados mediante un ataque informático		
CRITERIOS DE LA AUDITORIA: Determinación de medidas de protección Confidencialidad de la información recopilada Pruebas de Hackeo Ético aplicando ambientes controlados Definición de controles de seguridad		
EQUIPO AUDITOR: Patricio Renán Lanche Lara; Francisco Emanuel Paredes Salinas		
FECHA DE AUDITORIA: 25 de julio del 2018		
RESULTADOS DE AUDITORIA Y RECOMENDACIONES:		
PROCESO	**TIPO DE HALLAZGO**	**HALLAZGO**
Explotación de Vulnerabilidades en el dispositivo Android.	Debilidad	Se evidencia el acceso al dispositivo móvil Android verificando la información confidencial multimedia y el nivel de criticidad alto de dicha información.
Análisis de los riesgos detectados.	Debilidad	Se verifica que los riesgos identificados mediante el proceso de test de intrusión en el dispositivo Android son de nivel alto ya que la información que se encuentra almacenada es sumamente sensible.
RECOMENDACIÓN	**TIPO DE RECOMENDACIÓN**	**METODO A EMPLEAR**
Disminuir los índices de ataques en los dispositivos Android.	Fortaleza	Instalar aplicaciones de Antivirus para evitar la propagación de malwares en los Android.
Mantener la información multimedia almacenada en un APP.	Fortaleza	Desarrollar aplicaciones móviles que permitan almacenar información y traspasar archivos desde la galería de imágenes.

Fuente: Trabajo de Investigación
Autores: Renan Lanche-Francisco Paredes

Anexo IV: Carta de Juicio de Experto

CONSTANCIA DE JUICIO DE EXPERTO

Nombre del experto: Ing. Marlon Altamirano Di Luca M. Sia.

Por medio de la presente, hago constancia que se realizó la revisión de la ejecución del proyecto Análisis y Detección de Vulnerabilidades en los dispositivos móviles con Sistema Operativo Android, realizado por los estudiantes el Sr. Patricio Renán Lanche Lara y el Sr. Francisco Emanuel Paredes Salinas ambos estudiantes egresados de la carrera de Ingeniería en Networking Y telecomunicaciones de la Universidad de Guayaquil, quienes están realizando un trabajo para su titulación con el tema: **"ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES MEDIANTE INTERNET EN DISPOSITIVOS MÓVILES ANDROID, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN PREVIO AL DESARROLLO DE UNA APLICACIÓN MÓVIL QUE FACILITE LA PROTECCIÓN DE LOS DATOS SENSIBLES ALMACENADOS."**

Una vez indicadas las correcciones pertinentes del caso considero que dicho proyecto es válido para su aplicación.

Ing. Marlon Altamirano
Chief Executive Officer - CEO
NCSA
NET WORKING & CYBERSECURITY ACADEMY

ING. MARLON ALTAMIRANO DI LUCA M. SIA.

Anexo V: Carta de Aceptación del Producto

CONSTANCIA DE ACEPTACIÓN DEL PRODUCTO

Nombre del tutor del proyecto: Ing. Ángel William Ochoa Flores M. SC.

Por medio de la presente, hago constancia y acepto que se cumplieron los objetivos del proyecto de Análisis y Detección de Vulnerabilidades en los dispositivos móviles con Sistema Operativo Android, realizado por los estudiantes el Sr. Patricio Renán Lanche Lara y el Sr. Francisco Emanuel Paredes Salinas ambos egresados de la carrera de Ingeniería en Networking Y telecomunicaciones de la Universidad de Guayaquil, quienes están realizando un trabajo para su titulación con el tema: **"ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES MEDIANTE INTERNET EN DISPOSITIVOS MÓVILES ANDROID, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN PREVIO AL DESARROLLO DE UNA APLICACIÓN MÓVIL QUE FACILITE LA PROTECCIÓN DE LOS DATOS SENSIBLES ALMACENADOS."**

Una vez verificado el cumplimiento de los objetivos y alcances del proyecto dejo en constancia la aceptación de este.

ING. ÁNGEL WILLIAM OCHOA FLORES M. SC.