ESTUDIO MONOGRAFICO ACERCA DEL CIBERCRIMEN EN DISPOSITIVOS MÓVILES CON S.O. ANDROID

JOSE JAIR MACIAS CANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DICIEMBRE DE 2017

ESTUDIO MONOGRAFICO ACERCA DEL CIBERCRIMEN EN DISPOSITIVOS MÓVILES CON S.O. ANDROID

JOSE JAIR MACIAS CANO

PROYECTO DE SEGURIDAD INFORMÁTICA II
Monografía para optar por el título de Especialista en Seguridad Informática

ING. SALOMON GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DICIEMBRE DE 2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D.C. Diciembre 12 de 2017

DEDICATORIA

Dedico este desarrollo intelectual plasmado en este proyecto de grado a todos aquellos estudiantes y personas interesadas en el estudio de la criminalidad basada en las redes informáticas y a todos aquellos que se apasionen por el estudio forense.

AGRADECIMIENTOS

Aunque estamos en una etapa preliminar desde ya agradezco a Dios primeramente y a mi familia quienes han hecho posible que el alcance de mis logros y metas de hayan dado y se continúen desarrollando, agradezco a los tutores quienes serán mis guías y directores de encausamiento académico para lograr este objetivo de desarrollar una gran propuesta respecto del análisis del Cibercrimen en Colombia.

CONTENIDO

Pág.

LISTA DE ANEXOS

Pág.

LISTA DE IMÁGENES

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCION

El mundo es muy cambiante y dinámico las tecnologías de la información y las comunicaciones juegan un papel muy importante en la vida de todas las personas, desafortunadamente así como va en auge el crecimiento tecnológico y la ciencia, paralelamente va en auge la maldad en el ser humano, que en una sinergia con los avances descubre la manera de dañar estropear y ultrajar lo que le pertenece a los ciudadanos de bien; y es dentro del concepto de la privacidad, que la mayoría de delincuentes encuentran su éxito, al tratar de acceder a lugares no permitidos.

Mediante el desarrollo del presente estudio monográfico se pretende evidenciar el alcance que tienen a nivel tecnológico los diferentes actores del mundo criminal para realizar diversos ataques a la población colombiana, población que sin darse cuenta es ultrajada y sus datos confidenciales entre otra información personal es puesta a disposición de personas indeseables, al punto de acceder a claves de correos electrónicos cuentas bancarias y datos íntimos.

1. DEFINICION DEL PROBLEMA

1.1 DESCRIPCION

Uno de los antecedentes que dan valor al estudio del cibercrimen en dispositivos móviles, se evidencia en el hecho que la mayoría de usuarios de estos dispositivos, ya sean tabletas, Smartphones, o computadores portátiles, no muestran interés por la protección de los datos que manipulan en mencionados aparatos, del mismo modo al ser éstos el producto de mayor consumo en Colombia la cifra de personas vulnerables a un ataque aumentará considerablemente teniendo en cuenta que en pocos años existirá más dispositivos móviles conectados a internet que personas habitando este planeta, lo cual genera una gran preocupación hablando en términos de la protección de la información que será compartida en estos dispositivos.

Ahora bien analizando las causas del porque la ciudadanía no se preocupa por la protección de sus datos, se ha encontrado que todo radica en la falta de educación, ya que a la población colombiana no se le enseña otra cosa diferente a cuales son las formas más prácticas y rápidas para guardar, publicar y compartir toda su información, ya sea bancaria, personal, laboral y familiar a un dispositivo móvil, enseñanza que ha sido promovida los mismos fabricantes y que se ha convertido en una necesidad descontrolada. Derivado de lo anterior hay que mencionar que los nuevos lanzamientos de Smartphones son otra de las causas que han hecho que la ciudadanía no piense en seguridad, mucho se ha hablado de fallos de seguridad que se presentan cuando se lanza un nuevo Smartphone sin importar el fabricante, pero con tal de tener el ultimo celular las personas son capaces de arriesgar su propia intimidad.

Hacer un estudio acerca del cibercrimen en dispositivos móviles permite generar normas y estándares para una sociedad que carece de cibercultura ya que en la actualidad no hay disciplina ni tampoco hay educación para la seguridad y defensa para los datos digitales que tiene una persona en su dispositivo. No se trata de ir en contra de la tecnología, tampoco de no almacenar todo tipo de datos en un dispositivo Android, que es el sistema operativo objeto de este estudio, o de no poder acceder al último dispositivo móvil que haya salido al mercado; se trata de ir en contra de no asegurar o prevenir aquellas situaciones que pueden poner en riesgo los datos de cualquier persona que en ultimas es su activo más valioso.

1.1 FORMULACION DEL PROBLEMA

¿Ahora bien cuál es la importancia de crear una cultura de protección de los datos que son manipulados en un dispositivo móvil?

2. JUSTIFICACION

Actualmente en Colombia el auge de la cibercriminalidad está en aumento, situación que pone en riesgo a la gran mayoría de la población incluyendo a las corporaciones, pero sobre todo a la población colombiana de a pie, que es a quien va dirigido el presente estudio. Este riesgo va en aumento gracias a la falta de una política de protección de la información de parte de, los proveedores de servicios de internet, los fabricantes de tecnologías móviles y las entidades del estado que propenden por la seguridad de todos los colombianos; protección que va más allá de proporcionar un servicio de antivirus, ya que lo que se debe crear por pare de estos actores es crear una cultura de protección de la información, para la prevención del cibercrimen.

Es importante indicar que existen recomendaciones elaboradas por algunos expertos en Colombia, así como por agentes de seguridad del estado especializados en torno a la protección de la información en dispositivos móviles, recomendaciones que pueden encontrarse, por ejemplo, en la web, pero que si se analizan de manera profunda no cuentan con el análisis y desarrollo con el que cuenta este documento. De hecho, si se consulta con los responsables de las áreas de Informática Forense de las entidades del estado, cual es el porcentaje de casos de cibercrimen a dispositivos móviles, sin especificar el tipo de sistema operativo, la respuesta va ser si no nula, que menos del 10%.

Pero, ¿porque resulta importante hacer un estudio acerca del cibercrimen en dispositivos móviles y sobre todo que tengan sistema operativo Android?, por dos razones, inicialmente porque en aras de delimitar este estudio se escogió Android por ser el sistema operativo móvil más utilizado en el mundo además en Colombia esta estadística va en aumento y de otra parte porque en Colombia no hay cultura de protección de la información en dispositivos móviles. Esto último justificado en el hecho que son muchos los casos de personas que han sido víctimas de cibercrimen en sus dispositivos móviles.

De aquí la necesidad de establecer un modelo de protección que se convierta en una cultura que avance a la par con la tecnología para que se convierta en la costumbre de todos los colombianos y de las autoridades que están dentro de esta sociedad tecnológica, para que el colombiano común y corriente, aquel que aunque conozca de la necesidad de protegerse, no lo hace o no esté totalmente familiarizado con este concepto conozca la importancia de protegerse.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Realizar un estudio monográfico acerca del cibercrimen en dispositivos móviles con sistema operativo Android que permita conocer y describir algunas técnicas y métodos utilizados por Ciberdelincuentes para infiltrarse en este tipo de dispositivos con el propósito de generar conciencia y prevención respecto de los ataques más frecuentes a estos aparatos.

3.2. OBJETIVOS ESPECÍFICOS

- Realizar el estado del arte sobre las metodologías y técnicas utilizadas en ataques a dispositivos móviles.
- Describir mediante informática forense algunos ataques realizados a dispositivos Android.
- Desarrollar una guía con las principales técnicas recomendadas por expertos para evitar ser víctimas de ataques en dispositivos Android.

4. ALCANCE Y DELIMITACION DEL PROYECTO

Partiendo de la información que se obtiene de diversas fuentes abiertas, así como académicas, delimitará cuales son los patrones de referencia más comunes de casos y tipos de ataques que se hayan presentado a dispositivos móviles con sistema operativo Android, lo anterior teniendo en cuenta que el porcentaje de casos no denunciados bajo estos ataques, es bastante alto y esto gracias a la falta de educación en la materia. Como es conocido se han presentado a nivel nacional infiltraciones por parte de Ciberdelincuentes en zonas WiFi, por lo general gratuitas, razones por la cual se pretende concientizar en este estudio que éstas son las zonas de mayor riesgo de ataque.

Al conocer algunos tipos de ataque informático a dispositivos Android, se logrará determinar cuál es el modus operandi de un Ciberdelincuente, para así simular un ataque que permita explicar los pasos que un criminal realiza al momento de ejecutar un malware y que consecuencias acarrea consigo esto, es decir conocer el tipo de afectación que ocasiona, para que quede plasmada en el presente estudio monográfico.

Como la finalidad del actual documento es enseñar la importancia de la protección de la información de los datos que se almacenan en un dispositivo Android, se propenderá por definir algunas normas y recomendaciones que permitan servir de parámetro o marco de referencia no solo al estudio para abordaje de casos de cibercrimen si no como documento se enseñanza para la protección de datos de cualquier ciudadano que aunque no cuente con un dispositivo Android entienda lo importante de proteger sus datos de un ataque informático móvil.

Finalmente es importante aclarar que áreas de estudio que aborda esta monografía se enfocan a las zonas de acceso a internet WiFi libre, que se ubican en aeropuertos, centros comerciales, pero también a zonas de WiFi de hogares ya que estas son blanco fácil al no contar con normas de protección o claves seguras.

5. MARCO REFERENCIAL

5.1. MARCO TEORICO

Los dispositivos móviles son la mayor fuente de información y de traspaso de datos entre personas, razón por la cual la mayoría de Ciberdelincuentes aprovechan esta situación para buscar vulnerabilidades y acceder a esta información para lograr un beneficio personal, causando un daño a veces irreversible e irreparable. De hecho, son muchas las herramientas de las que se valen estas personas malintencionadas, para realizar estos ataques, es por ello que revierte importancia conocer algunas de ellas como las que se indican a continuación:

- Cabir: Por ser uno de los primeros malware que existió para móviles, se hace imperioso hablar de él; inicialmente este malware infectaba a teléfonos móviles que funcionan con el sistema operativo Symbian, pero a medida que pasó el tiempo fue migrando y encontrando la posibilidad de afectar smartphones con S.O., Android. La manera en que opera es, cuando un teléfono está infectado, el mensaje “Caribe” se muestra en la pantalla del teléfono y aparece cada vez que éste se enciende de esta manera el gusano intenta propagarse a otras terminales a través de señales inalámbricas tipo Bluetooth[1].
- CopyCat: Este malware logró infectar en 2017 más de 14 millones de dispositivos con S.O. Android, y es que este virus al funcionar como una falsa app la cual se descarga de una tienda externa a google play, razón por la cual se muestra como una aplicación inofensiva pero que después de ser instalada en el equipo empieza a recoger datos en segundo plano del mismo y desatando exploits que hacen que el dispositivo se ponga en modo root o administrador para la persona que remotamente intenta obtener estos datos.[2].
- Duts: Este virus parasitario infecta archivos y es el primer virus conocido para la plataforma Pocket PC. Intenta infectar todos los archivos ejecutables (.exe) mayores a 4096 bytes en el directorio local[3].
- Skulls: Se trata de un fragmento de código troyano. Una vez descargado, el virus reemplaza todos los iconos del escritorio del teléfono con imágenes de un cráneo. También inutiliza todas las aplicaciones del teléfono, incluyendo la recepción y envió de SMS y MMS[3].

[1] Tomado de: https://latam.kaspersky.com/blog/10-curiosidades-sobre-cabir-el-virus-de-smartphones-que-cumplio-10-anos/3300/

[2] Tomado de: http://reunir.unir.net/bitstream/handle/123456789/3622/VILLANOVA%20PASCUAL%2c%20OSCAR.pdf?sequence=1&isAllowed=y

- Gingermaster: Troyano desarrollado para plataforma Android que se propaga mediante la instalación de aplicaciones que incorporan de forma oculta el malware para su instalación en segundo plano. Aprovecha la vulnerabilidad de la versión Gingerbread (2.3) del sistema operativo para utilizar los permisos de súper-usuario mediante una escalada de privilegios. Luego crea un servicio que roba información del terminal infectado (identificador del usuario, número SIM, número teléfono, IMEI, IMSI, resolución de pantalla y hora local) enviando los mismos a un servidor remoto mediante peticiones HTTP[3].
- DroidKungFu: troyano contenido en aplicaciones de Android, que al ser ejecutadas, obtiene privilegios de root e instala el archivo com.google.ssearch.apk, que contiene una puerta trasera que permite eliminar ficheros, abrir páginas de inicio suministradas, abrir direcciones web y descargar e instalar paquetes de aplicación. Éste virus recopila y envía a un servidor remoto todos los datos disponibles sobre el terminal[3].
- Ikee: primer gusano conocido para plataformas iOS. Solo actúa en terminales que se les han hecho previamente un proceso de jailbreak, y se propaga intentando acceder a otros dispositivos mediante protocolo SSH, primero a través de la subred en que esté conectado el dispositivo. Luego, repite el proceso generando un rango aleatorio y por último utiliza unos rangos preestablecidos que corresponden a direcciones IP de determinadas compañías telefónicas. Una vez infectado el equipo, substituye el fondo de pantalla por una fotografía del cantante Rick Astley[3].

Afortunadamente son muchas las fuentes de información en donde se detallan algunos casos de cibercriminalidad que ocurren en Colombia y otras partes del mundo, razón por la cual es importante documentarse para así tener marcos de referencia que permitan prevenir y contrarrestar estas herramientas maliciosas; dentro de estas fuentes es posible tener a las entidades del gobierno encargadas de la administración de justicia como la Fiscalía y sus entes investigativos así como a la Policía Nacional, que con sus diferentes grupos forenses pueden aportar información del cómo han operado históricamente en los últimos años casos donde se han visto vulnerados colombianos del común.

No se pueden dejar de lado los institutos forenses independientes quienes también aportan gran información arrojada de su experiencia para el análisis de casos y técnicas usadas al respecto y también es importante tener presente las fuentes abiertas de información como periódicos entre otros.

Ahora bien, una vez definidas algunas herramientas maliciosas de ataque a dispositivos móviles, es necesario continuar con definir algunos conceptos importantes dentro del presente estudio monográfico ya que se habla y se hablará muy a menudo en este documento sobre el término Forense. La informática forense es un área relativamente nueva, es una rama de la ciencia forense que nace de la necesidad de encontrar una nueva fuente de evidencia; los investigadores forenses encontraron que los dispositivos electrónicos podían brindar ese tipo de evidencia.

Cano (2006) interpreta la informática forense de dos maneras: 1. *"Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura describir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso"*, también, 2. "*Como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación forense ofrece un análisis de la información residente en dichos equipos"*.[3]

El proceso forense busca recolectar, analizar, verificar y validar todo tipo de información existente o información que se considera como borrada usando un conjunto de herramientas y técnicas.

Es por ello que a nivel de modelos forenses podemos hablar que desde sus inicios se han desarrollado algunos modelos forenses para ayudar a desarrollar de mejor forma el proceso por el cual pasa la información desde la extracción hasta la etapa final de la entrega del informe pericial. Algunos de los modelos que han surgido a través de los años son: Casey en el año 2000, el modelo publicado por el Departamento de Justicia de los Estados Unidos en el año 2001, el modelo Lee en el año 2001, el modelo Reith, Carr y Gunsch en el años 2002, el modelo integrado de Brian Carrier en el año 2002 el de Eugene Spafford en el año 2003 respectivamente, el modelo mejorado propuesto por Venansius Baryamureeba y Flerence Tuchable en el años 2004 y el modelo extendido de SéamusÓCiardhuáin en el año 2004.

El modelo de Casey ha evolucionado desde su primera aparición en el año 2000 pero para hablar de él es importante hablar de las fases que lo componen las cuales son:

- Autorización y preparación

[3] Tomado de, http://revistas.ufpso.edu.co/index.php/rsemilleros/article/download/114/76

- Identificación
- Documentación
- Adquisición y Conservación
- Extracción de información y análisis
- Reconstrucción
- Publicación de conclusiones

Teniendo como fundamento las técnicas y proceso forenses avalados hasta el momento y conociéndolos de una forma sustancial, por lo menos en el campo de aplicación, es posible aprender a desarrollar técnicas que permitirán el abordaje desarrollar mejor la presente monografía.

Resulta interesante que en el campo de aplicación forense para dispositivos móviles es muy poco el avance que se ha dado en materia de prevención a ataques móviles, algunos avances se han dado teniendo en cuenta las características propias de dichas terminales, como su fabricante, tecnología software etc.; es por esto que al consultar los procedimientos forenses para dispositivos móviles, éstos son los mismos que se aplican a los equipos y componentes de escritorio obviamente porque la mayoría de dispositivos móviles son catalogados como computadores portátiles que varían de tamaño y funcionalidad.

Ahora resulta importante describir técnicamente un Smartphone, por ejemplo, hay que decir que todos los Smartphones tienen un procesador, una memoria RAM, un dispositivo de almacenamiento, un sistema operativo, una tarjeta madre y unos accesorios entre otro componentes reducidos en un aparato que no sobrepasa las dimensiones necesarias para ser transportado en un bolsillo de la camisa o del pantalón, situación que lo hace muy versátil, dado que adicionalmente cuenta con una antena inalámbrica que le permite conectarse a internet sin necesidad de usar cables, claro está que los Desktops de hoy día también vienen con tarjeta inalámbrica para conectarse a redes WiFi por lo general en el hogar y también vienen con otras características que los asemejan a los Smartphones actuales, obviamente la diferencia entre los Desktops y Laptops con los Smartphones y tabletas radican en el tamaño, peso y robustez de componentes lo que hace que el consumidor opte por comprar un dispositivo móvil ya sea Smartphone o Tableta a un equipo Desktop o Laptop haciendo que la relación de compra sea de 10 a 1, es decir por cada 10 compradores solo hay 1 que compra un computador de escritorio o un portátil y 9 que prefieren comprar un Smartphone o una tableta.

Razón por la cual el internet de las cosas advierte que en el mundo se está dando que ya hay más dispositivos móviles que personas, es por ello que en el foro ESET sobre tendencias en seguridad informática se indicó que *"continuaremos viendo ataques de empresas y organizaciones en busca de su información, así como ataques y mayor regionalización del malware. Aumenta la preocupación de los usuarios por su información y quién accede a ella. Por demás, el crecimiento del Internet de las Cosas (IoT, por sus siglas en inglés) pondrá a prueba sus defensas contra las vulnerabilidades, mientras se desarrollarán nuevas amenazas para dispositivos móviles, haciendo destacado el rol de los investigadores de seguridad".*[4]

El Informe de ESET, "Tendencias 2016: (In) security everywhere. La interconexión de las cosas", revela que todos los dispositivos actuales son vulnerables. Y esto adquiere un mayor significado si tenemos en cuenta que 4,900 millones de dispositivos estarán conectados en 2015, y 25,000 millones lo estarán para 2020, según Gartner, explicó Pablo Ramos, Head of LATAM Research Lab de ESET, quien presentó el estudio. Entre los problemas que enfrenta, por ejemplo, la tendencia del Internet de las cosas, se encuentran la privacidad, el login de los dispositivos, el cifrado, la interfaz web y el software en sí. El IoT sin duda será un reto para los niveles de seguridad de los dispositivos el año que está por venir. [4]

Otro tema relevante es el secuestro en la era digital, que deja al usuario indefenso, y le permite al atacante intimidarlo. Para 2016 aumentarán los secuestros de información con el crecimiento el cibercrimen, por la rentabilidad de los ataques, la vulnerabilidad de los usuarios y el que cada vez hay más dispositivos a atacar. Según ESET, en los últimos 15 meses las víctimas de Ransomware perdieron $15.000.000 de dólares. A esto se adiciona que la generación del malware se ha industrializado. Estudios recientes indican que más de 1,900 ataques generaron en promedio $7.7 millones de dólares de perdida. Las cifras son alarmantes. [4] *más atrás*

En 2015, explica Ramos, se detectaron más de 2,000 familias de malware para Android y 30 para IOS. Hoy es una tendencia en aumento. "Nosotros como empresa de seguridad no tenemos que fallar nunca, pero por otro lado el atacante solo necesita ser exitoso una vez para poder entrar a la información de las empresas. Puede hacerlo engañando al usuario, infectando un sistema, obteniendo una credencial de acceso, esperando…, el cibercriminal tiene todo el tiempo del mundo para acceder a las credenciales que necesita para su ataque, persistiendo hasta obtener lo que realmente fue a buscar", expresó el orador. [4] *más atrás*

[4] Tomado de http://www.eset-la.com/pdf/business-v6/ESET-Business-Solutions.pdf

Y es que la mayoría de congresos como los que produce ESET así como otros congresos auspiciados por otras corporaciones, son una fuente bibliográfica de conocimiento que advierte acerca de las tendencias en ataques cibernéticos actuales del mismo modo que provee un escenario de conocimiento que ilustra que las técnicas y normas que se están usando en el mundo para el fortalecimiento de la defensa; por ejemplo ESET en temas de seguridad para dispositivos móviles provee un abanico de servicios denominados ESET ENDPOINT SECURITY.

Allí se propende por la administración remota de dispositivos móviles para poder bloquear, desbloquear y generar un borrado seguro de los datos incluidos en el dispositivo; también se predica acerca de la seguridad para dispositivos que genera advertencias acerca de si el aparato cumple o no con los estándares de protección; de otra parte también genera un control de aplicaciones para monitorear las mismas con el fin de evitar aplicaciones fraudulentas y finalmente la protección de datos almacenados también conocida como Anti-Theft que funciona como un token que remotamente administra para protección el acceso al dispositivo.

Lo anterior es un servicio de tipo preventivo y correctivo para dispositivos móviles que aportan conocimiento y soporte en las acciones que podrían estandarizar un nivel de seguridad para dispositivos móviles en redes WiFi.

Es importante entender las tendencias en Ciberseguridad ya que el mercado global de la Ciberseguridad está en continuo crecimiento y se estima que alcance los 170 mil millones de dólares para el año 2025, a una tasa de crecimiento compuesta anual del 9,8% según las cifras de los expertos; dentro de todo esto nace un concepto denominado BYOD o bring your own device dentro del marco de la seguridad gestionada, los servicios basados en la nube, la protección de datos en movilidad, las amenazas persistentes avanzadas (APT), el Internet de las cosas y la seguridad en Smart Grid que son algunos de los segmentos que experimentarán más crecimiento según lo indican los expertos.

Es por ello que se hace imperioso clasificar estos conceptos en:

- Seguridad en dispositivos móviles, BYOD: El uso de dispositivos móviles para acceder a los datos corporativos es una tendencia creciente entre los empleados, tanto si se trata de dispositivos de propiedad de las mismas empresas, como de sus empleados, fenómeno este último conocido como

BYOD como ya se mencionó antes razón que los hace objetivo de los cibercriminales.[5]

- Seguridad de las infraestructuras críticas: centrales y redes de energía, transportes, sistema financiero, etc. son recursos fundamentales que, en el caso de sufrir un ataque, causarían gran impacto en la seguridad de un Gobierno o Nación lo cual aunque no se enmarca en la presente monografía, es importante mencionarlo y tenerlo en cuenta puesto que la normatividad tiene influencia en la terminología objeto de estudio.[5]
- Seguridad en Smart Grid: se incluye dentro del concepto de infraestructura crítica porque las Smart Grid son las redes eléctricas inteligentes y su protección de los ciberataques es clave. Los hackers, por ejemplo, pueden tomar el control de aplicaciones y servidores y acceder a información confidencial.[5] más atrás
- Seguridad en el internet de las cosas: Algunas organizaciones dedicadas al estudio de prevención y proyección de riesgos indican que para 2020 existirán 30 mil millones de dispositivos conectados en la red, por tanto, son objetivo de los actuales y potenciales ciberdelincuentes.[5] más atrás
- Vulnerabilidades técnicas: permiten a los atacantes ejecutar un código dañino en el sistema. La mayoría de estas vulnerabilidades están relacionadas con una mala configuración del servidor.[5] más atrás

Es por eso que hay que entender que la Ciberseguridad estudiada en dispositivos móviles no es un problema exclusivamente tecnológico en la mayoría de los ataques de mayor envergadura, la tecnología representa únicamente una herramienta y las motivaciones son más bien económicas o por razones de política, la guerra, el activismo y el espionaje lo que hace suponer que se trata de un fuerte negocio en el cual los Ciberdelincuentes, comercian los datos robados y obtenidos por medio de, en nuestro caso de estudio, las redes WiFi generando software de tipo malware. Esto a pesar que existen las mejoras en seguridad móvil, y que empresas con servicios avanzados, generan una gestión segura de grandes bases de datos con los llamados White Hat Hackers que son desarrolladores que ayudan en la lucha contra los delitos y fomentan el conocimiento de los problemas de seguridad.

[5] Fuente: http://searchdatacenter.techtarget.com/es/consejo/BYOD-Como-evaluar-los-nuevos-dispositivos-y-sus-riesgos-de-seguridad

5.1.1. QUE ES EL CIBERCRIMEN

Mucho se habla acerca de Hackers y los ataques que presuntamente son perpetrados por estos mal llamados Ciberdelincuentes; es muy común escuchar hoy día cosas cómo, *"me hackearon la cuenta de correo"*, *"me hackearon el Facebook"*, *"me hackearon el computador"*, entre otros comentarios, utilizando siempre el término hacker. Pero antes de seguir es importante mencionar que en varias fuentes abiertas y académicas como por ejemplo la manera en que se aborda el término en el libro ***"EL CIBERCRIMEN Fenomenología y criminología de la delincuencia en el ciberespacio"*** escrito por Fernando Miró Llinares, define a Hacker como un individuo con capacidades de lograr superarse o superar algo que informáticamente se cree invulnerable, a pesar que se ha socializado que un hacker es un Ciberdelincuente y también se han realizado correcciones al respecto para tratar de hacer la diferencia y enmendar un error gramatical que se ha extendido a lo largo de un buen tiempo, pero que gracias al avance de la tecnología se han dado cuenta que, es gracias a los Hackers, que el mundo tiene una red social como Facebook, tiene un celular como un Iphone, tiene y programas de entretenimiento a la medida como Netflix, servicios de transporte como Uber y demás que les han facilitado la vida, y todo esto ha sido por Hackers[6].

Entonces de acuerdo a lo anterior y a las fuentes de estudio históricas de la informática, un hacker es una persona con grandes habilidades que explota su conocimiento en favor del bien; por lo tanto clasificar a un hacker como un Ciberdelincuente es algo que no encaja; por lo cual un Ciberdelincuente es toda persona que con ciertas habilidades de programación pero motivado por el daño que pueda causar y del cual pueda obtener algún tipo de beneficio ya sea económico, político o religioso entre otras motivaciones logra generar un daño en determinada persona por medio del uso de medios de comunicación o utilizando algún tipo de software con código malicioso para acceder a una información en especial.

Por lo tanto, lo que hace un Ciberdelincuente se le conoce como cibercrimen, ya que, al traspasar las barreras de la intimidad, la privacidad y la confidencialidad de las personas o corporaciones con fines de destrucción y de lucro económico particular, se presume que está cometiendo un delito; esto ocurre porque por lo general lo que hace un cibercriminal es secuestrar información con la cual logra un beneficio y esto es penalizado por las autoridades. Razón que concluye que la persona que dice que le *"Hackearon"* su cuenta de Facebook o de correo

[6] Ver más en la compilación de estos 5 documentales realizados por Discovery Channel en la URL, https://www.youtube.com/watch?v=Xe7YWI0RI-M&feature=youtu.be

electrónico, realmente lograron obtener el acceso a ella de manera ilegal, fraudulenta y enviando un código malicioso a la víctima que parece confiable y se convierte en algo criminal porque el Ciberdelincuente está ejerciendo un daño a la víctima ejecutando acciones que no son propias de la víctima.

5.1.2. TIPOS DE DISPOSITIVOS MÓVILES

Uno de los mercados más emergentes y por lo tanto más exitosos en el mundo es el de los dispositivos móviles; la tecnología móvil se ha vuelto un viral en expansión exponencial que hasta la fecha no tiene límites, el consumidor cada vez quiere más y mejores dispositivos.

Entonces para poder describir los diversos tipos de dispositivos móviles hay que comenzar por definir que un dispositivo móvil es un aparato tecnológico con un conjunto de técnicas de avanzada que lo hace casi inteligente, casi porque aún depende del usuario para poder funcionar, pero que con sus características internas y su software se pueden hacer labores, básicas como comunicarse de manera bidireccional vía telefónica con otro dispositivo, avanzadas como poder consultar correo electrónicos, redes sociales, escuchar música, ver videos y dependiendo el tipo de dispositivo un sinnúmero de tareas digitales que cada vez se vuelven incontables e interesantes para cualquier persona.

Es por ello que el mercado está saturado de un sinnúmero de dispositivos móviles por lo cual hablar de todos sería algo un poco engorroso; es importante definir que para el presente estudio monográfico se entenderá como dispositivo móvil a aquellos celulares y tabletas que utilicen un sistema operativo Android, claro está que para efectos de explicar los tipos de dispositivos móviles es importante mencionar que aparte del S.O., Android, existen otros S.O., tales como IOS de Apple y Windows Phone de Microsoft. Entonces para efectos prácticos en este documento se tomará como referencia las 3 marcas de empresas que producen estos tres tipos de sistemas operativos para dispositivos móviles (Android, IOS y WinPhone) para describir sus terminales móviles más emblemáticas y conocer así un poco acerca de ellas.

A continuación, se hace un listado de las empresas con mayor número de ventas y más conocidas en el mercado occidental por la fabricación de dispositivos móviles:

- Samsung (Dispositivos con S.O. Android)

- Apple (Dispositivos con S.O. IOS)
- Huawei (Dispositivos con S.O. Android)
- Microsoft (Dispositivos con S.O. Windows Phone)
- Motorola (Dispositivos con S.O. Android)
- Sony (Dispositivos con S.O. Android)

Obviamente existen otras más y en el mercado Europeo y Asiático el listado cambia un poco. Ahora bien, dado que en el mercado mundial Samsung es la empresa con mayor número de ventas de dispositivos Android, se toma como referencia para hablar acerca de sus dispositivos de manera general.

- Samsung: Es una empresa surcoreana que en su línea de venta de dispositivos móviles con S.O. Android ha logrado mucho éxito sus dispositivos más relevantes son:

  Celulares gama alta, Samsung Galaxy S6, S7, Note 4, Note 5, S8 y Note 7 (éstos dos últimos próximos a salir al mercado): Estos terminales al igual que sus predecesores son los dispositivos que año a año han sido los más emblemáticos de esta corporación por contar con todas las características de tecnología de punta y mejor desempeño respecto de las demás referencias o gamas de esta marca. Esta empresa ha desarrollado otras líneas de gama media conocidas como Samsung Galaxy J y Galaxy Alpha que cuentan con unas especificaciones un poco menor pero con una calidad que en ventas arrasa en el mercado[7].

  En tabletas Samsung ha diseñado cuatro líneas de tabletas: Las Galaxy Tab A, S y E que al igual que los celulares de gama alta cuentan con especificaciones un poco similares a diferencia que sus pantallas son más grandes para un uso más ofimático[8].

- Apple: Es una empresa Estadounidense que se especifica en el desarrollo de dispositivos y software para computadores y dispositivos móviles con un diseño propio; sus líneas de ventas en estos dispositivos cuentan con un sistema operativo denominado IOS el cual ya va en su versión 10.2.1 son:

[7] Fuente http://www.samsung.com/co/smartphones/
[8] Fuente http://www.samsung.com/co/tablets/

Celulares Iphone 5, 5S, 6, 6S y el recién lanzado Iphone 7: Son los dispositivos celulares más emblemáticos de esta compañía, éstos contienen unas especificaciones que año a año van aumentando con los avances que el mercado va demandando, esta compañía también ha desarrollado unos dispositivos de gama baja denominados Iphone línea C que cuentan con el mismo software pero con especificaciones de hardware más bajas[9].

Tabletas Ipad Pro, Air 2, Mini 4 y mini 2: Al igual que los Iphone poseen el mismo software solo que con pantallas y resoluciones más altas por la dimensión de las mismas[10].

- Microsoft: Es una empresa Estadounidense que se especializa en el desarrollo de software para computadores desde hace más de 40 años cuyo fundador es el varias veces primer hombre más rico del mundo, Bill Gates y cuyo software para computadoras es el más conocido y comercializado por todo el mundo, Windows. Microsoft desde hace aproximadamente 10 años ha estado incursionando en el mercado de los dispositivos móviles.

  Con los celulares, Microsoft realizó en 2010 aproximadamente una alianza con Nokia, lo cual le dio la puerta de entrada para posteriormente entrar de lleno en este mercado y poder construir sus propios terminales a pesar que en la actualidad este mercado no ha logrado ser tan fuerte como lo proyectaba. De todas maneras, algunas otras marcas como HP entre otras han adoptado el S.O., WinPhone como una alternativa para sus dispositivos móviles celulares.

  Los celulares más emblemáticos de Microsoft, son los Lumia 650, 950 y 950XL, los cuales cuentan con la última versión del S.O., Windows 10 adaptado para celulares y que cuentan con unas especificaciones que los sitúan a la altura de toros terminales móviles del mercado; lo interesante de estos dispositivos es la total compatibilidad que hay entre estos aparatos y una máquina de escritorio con sistema Windows[11].

  En tabletas, Microsoft no ha innovado mucho, Microsoft ha lanzado al mercado una tableta llamada Surface, que funciona como un portátil con S.O.

[9] Fuente http://www.apple.com/co/iphone/
[10] Fuente http://www.apple.com/co/ipad/
[11] Fuente https://www.microsoft.com/es-mx/movil/

Windows 10 para escritorio pero con las funcionalidades de una terminal móvil[12].

5.1.3. EL SISTEMA OPERATIVO ANDROID Y SUS VERSIONES

Uno de los sistemas operativos móviles más importantes que han surgido en la historia y el más utilizado en el mundo es el sistema operativo Android, fue desarrollado por la empresa de tecnología Google en el año 2005 y al igual que Windows ha tenido un auge vertiginoso por su bajo coste y gran variedad de dispositivos que lo implementan y es que según las estadísticas, los dispositivos Android se venden más que los sistemas operativos Windows Phone e IOS juntos[13].

Android fue creado en conjunto con la Open Hand Set Alliance (OHA), que es un compendio de 84 compañías dedicadas al desarrollo de software libre para dispositivos móviles, quienes a su vez también lanzaron desde esa época y hasta la actualidad una SDK con el propósito que se le pudieran incluir mejoras al S.O., por parte de programadores o desarrolladores que observaran vulnerabilidades al sistema; es decir el ser abierto es un mensaje para que sea mejorado. Un hecho curioso y que quizá muchos desconozcan es que cada versión de Android es nombrada en el sentido del orden del abecedario, es un hecho obvio pero que tal vez algunos usuarios no han analizado, pero que básicamente se debe a un propósito de tipo criptográfico, es decir mantener una secuencia dentro del desarrollo y seguridad del software; otro dato curioso es el nombre que cada versión tiene el cual está relacionado con nombres de postres, ideado inicialmente por el líder de ese proyecto Ryan Gibson[14]. Actualmente Android está en su versión 7 denominada Nougat o Turrón en español, pero en su trasegar de existencia han existido las siguientes versiones:

Tabla 1 Versiones del Sistema operativo Android.

NOMBRE	VERSIÓN
Apple Pie	1.0
Banana Bread	1.1
Cupcake	1.5

[12] Fuente https://www.microsoft.com/es-es/surface
[13] Fuente http://www.ibtimes.com/android-vs-ios-whats-most-popular-mobile-operating-system-your-country-1464892
[14] Ver más en https://books.google.es/books?hl=es&lr=&id=TOP-BiaYYiQC&oi=fnd&pg=PT246&dq=versiones+de+android&ots=mKne5xnwr6&sig=K_-lSVY1OBp14BANd1LnLJ8AzpM#v=onepage&q=versiones%20de%20android&f=false

Donut	1.6
Éclair	2.0 - 2.1
Froyo	2.2
Gingerbread	2.3
Honeycomb	3.0 - 3.1 - 3.2
Ice Cream Sandwich	4.0
Jelly Bean	4.1 - 4.2 - 4.3
KitKat	4.4
Lollipop	5.0/5.1
Marshmallow	6.0
Nougat	7.0 - 7.1

Fuente: https://books.google.es/books?hl=es&lr=&id=TOP-BiaYYiQC&oi=fnd&pg=PT246&dq=versiones+de+android&ots=mKne5xnwr6&sig=K_-lSVY1OBp14BANd1LnLJ8AzpM#v=onepage&q=versiones%20de%20android&f=false

Podría decirse que el S.O., Android ha tenido un comportamiento comercial para los usuarios de terminales móviles muy similar al del S.O., Windows en computadoras y portátiles.

5.2. ANTECEDENTES

Dentro del marco de antecedentes es indispensable definir algunos proyectos, propuestas e invenciones que se han desarrollado en el mercado mundial y que son muy similares y coadyuvan con el presente estudio acerca del cibercrimen en dispositivos móviles con S.O. Android, que como sustento han originado un interés en la elaboración e investigación para desarrollar la presente monografía.

5.2.1. LATCH

Uno de estos proyectos de Ciberseguridad móvil es, Latch[15], es el que más se resalta dentro del presente estudio monográfico, aunque no es exclusivo del S.O., Android puesto que también está disponible para plataformas IOS y Windows Phone, inicialmente las pruebas y diseño de Latch se realizaron con este S.O. Latch es la nueva invención del grupo empresarial Telefónica de España, por medio de su unidad de Ciberseguridad llamada Eleven Paths la cual es dirigida por el reconocido

[15] Página oficial de Latch https://latch.elevenpaths.com/www/index.html

Hacker, Chema Alonso y que tiene entre otros objetivos, proporcionar una verdadera protección a cualquier terminal móvil sin importar la plataforma.

Primero que todo, es importante mencionar que Latch es un proyecto global que está diseñado para proporcionar protección a diferentes plataformas y servicios digitales tanto para equipos de escritorio, servidores en diferentes plataformas o sistemas operativos, así como para dispositivos móviles; estos servicios de seguridad pueden ser aplicados tanto para empresas como para usuarios independientes. Latch funciona de manera similar para cualquier servicio, es decir su operación consiste, a groso modo en, generar un cerrojo digital para cualquier servicio que requiera de usuario y contraseña con el fin de impedir que un tercero que no sea el usuario original del servicio descrito, pueda ingresar de manera fraudulenta a la aplicación y aparte informarle al usuario que alguien está tratando de ingresar a su aplicación.

Ahora, Latch para dispositivos móviles, es una aplicación totalmente gratuita que protege las cuentas y servicios que están conectados a internet, entre otros datos de un terminal móvil cuando no se estén utilizando; para utilizar Latch es muy sencillo[16], el primer paso es registrarse con una cuenta de correo electrónico cualquiera, directamente en la página oficial de Latch esto con el propósito de poder ingresar a la aplicación con una cuenta de correo reconocida y verificada por Latch.

El segundo paso es descargar la aplicación Latch, como el presente documento está orientado a terminales con S.O. Android, se debe descargar directamente del Play Store, verificando que sea una aplicación distribuida directamente por Telefónica Digital, una vez descargada la aplicación en el Smartphone, se abre, se ingresan los datos referente a la cuenta de correo registrada en la página de Latch, y se empareja la terminal móvil con Latch; este proceso es recomendable hacerlo con una Laptop o un Desktop y el dispositivo móvil para ingresar el código que genera la aplicación para cada servicio que se desea Latchear, Facebook, Twitter, YouTube, etc.

Por último y una vez emparejado Latch con los servicios a proteger, se configura desde la aplicación, el tipo de protección que se desea aplicar en el terminal móvil,

[16] Cómo utilizar Latch https://latch.elevenpaths.com/www/how.html

es decir, si se desea un bloqueo permanente o por horarios, esto se hace dentro de la aplicación.

5.2.2. APLICACIÓN TRUECALLER

No solo la seguridad debe pensarse hacia el uso de datos móviles, es decir cuando se unas un Smartphone como terminal de trabajo, también es importante pensar en la seguridad de la comunicación en sí; como es sabido un Smartphone es un dispositivo que permite la comunicación entre dos o más individuos, de hecho es un teléfono; pues precisamente una de las aplicaciones que desde hace tiempo motivo la creación de este estudio investigativo fue el proyecto o aplicación TrueCaller que da protección y seguridad a las comunicaciones telefónicas de un Smartphone.

TrueCaller es una aplicación que utiliza un dialer que integra servicios de identificación de llamadas, TrueCaller hace referencia a la herramienta que posibilita, por ejemplo, realizar y recibir llamadas a través del teléfono celular y que integra, además, la funcionalidad de bloqueo para aquellas que no son deseadas por el usuario.

Las ventajas de TrueCaller son:

- TrueCaller incorpora en su servicio el bloqueo de llamadas no deseadas.
- TrueCaller cuenta con una herramienta de identificación de números desconocidos, bien sea en la bandeja de entrada de mensajes de texto o en el historial de llamadas.
- TrueCaller integra los medios sociales para conservar la agenda del usuario actualizada con datos de interés como el cumpleaños o fotografía.
- TrueCaller está disponible en las tiendas que vienen con los dispositivos de acuerdo al sistema operativo. Es decir, es compatible con dispositivos Android, iOS, Tizen, BlackBerry 10, Firefox OS, Windows Phone y muchos más.
- Con TrueCaller también es posible bloquear mensajes de textos, permitiendo que el usuario sólo conecte con aquellas personas que de verdad le importan.
- TrueCaller posee un tema minimalista.
- Al igual que otros servicios, también incluye la opción para compartir la ubicación de la persona con amigos, familiares y conocidos.
- TrueCaller cuenta con los populares Emojis.

- TrueCaller bloquea también contenido considerado como spam o telemarketing, haciendo que el proceso de comunicación sea eficiente y seguro.

Con este concepto ahora tenemos una mayor visión de las tendencias del Marketing Digital y de las nuevas tecnologías actuales.

5.3. MARCO LEGAL

Hablar del marco legal para delitos informáticos dentro de la temática del presente proyecto es hablar de la normatividad legal y penal en materia informática que hay en Colombia, es decir la ley 1273 la cual parte del hecho que esta ley protege el bien jurídico tutelado de la información y el dato posicionando al país en el contexto jurídico internacional toda vez que se encontraba en mora por hacerlo; es por ello que surge paralelamente al desarrollo tecnológico informático y al continuo auge de las innovadoras tendencias delictivas de elaboración de fraudes y otros delitos que con frecuencia van más rápido que los códigos penales. De una u otra forma la comisión de un delito informático afecta a un mayor número de ciudadanos frente a un fenómeno que va en alza por lo cual se impone la necesidad de prevención y protección que son deber de todos los participantes en esta problemática es decir el Estado, los entes de control, Las empresas y la ciudadanía en general.

Es importante indicar que con la entrada en vigencia de la ley 1273 de 2009 y siguiendo los propósitos de ICITAP (Internacional Criminal Investigative Assitance Program) el país entra a los más altos estándares para contrarrestar el delito informático; esto conlleva a evitar tipificaciones erradas como se hacía antiguamente con la publicación indebida e ilegal de datos personales en redes sociales, conexión o acceso a redes sin autorización, uso de software malicioso etc. Todo lo anterior para decir que con esta ley se preservan integralmente los sistemas que utilicen las tecnologías de la información y las telecomunicaciones.

Se podrá clasificar como delitos informáticos más comunes en Colombia los siguientes:

- Art. 269 A. Acceso abusivo a un sistema informático
- Art. 269 B. Obstaculización ilegitima de sistema informático o red de telecomunicaciones
- Art. 269 C. Interceptación de datos informáticos
- Art. 269 D. Daño informático
- Art. 269 E. Uso de Software Malicioso

- Art. 269 F. Violación de datos personales
- Art. 269 G. Suplantación de sitios web para capturar datos personales
- Art. 269 I. Hurtos por medios informáticos y semejantes
- Art. 269 J. Transferencia no consentida de activos

Esta ley permite proteger y blindar de manera tecnológica a las corporaciones y empresas que manejan información importante de cualquier tipo, obviamente que dentro del flujo de la información y activos se manifiesta de manera magnética; es por ello que se establecieron los tipos penales para atacar estas conductas de tipo cibercriminal.

5.4. MARCO CONCEPTUAL

A continuación, se define el marco conceptual:

- Sistema Operativo: Es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes (aunque puede que parte de él se ejecute en espacio de usuario).[17]
- Android: Android es un sistema operativo inicialmente pensado para teléfonos móviles, al igual que iOS, Symbian y Blackberry OS. Lo que lo hace diferente es que está basado en Linux, un núcleo de sistema operativo libre, gratuito y multiplataforma. El sistema permite programar aplicaciones en una variación de Java llamada Dalvik. El sistema operativo proporciona todas las interfaces necesarias para desarrollar aplicaciones que accedan a las funciones del teléfono (como el GPS, las llamadas, la agenda, etc.) de una forma muy sencilla en un lenguaje de programación muy conocido como es Java.[18]
- Cibercrimen: Cibercrimen lo podríamos dividir en dos palabras, Ciber y Crimen, según el diccionario de la Real Academia Española de la lengua, ciber se define como: “cibernético, ciberespacio, cibernauta.”; según el sitio definiciones.org, ciber se define como: “Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.). Su origen es la palabra griega kibernao, que significa pilotar una nave.” Ahora según el diccionario de la

[17] Tomado de http://elvex.ugr.es/decsai/JAVA/pdf/1A-intro.pdf
[18] Tomado de https://www.xatakandroid.com/sistema-operativo/que-es-android

Real Academia Española de la lengua, crimen se define como: “Delito grave”, también Acción indebida o reprensible.[19]

- Forense: La palabra forense dispone de un uso muy recurrente en el ámbito del derecho dado que de ese modo se denomina al profesional médico que se encuentra trabajando dentro de un juzgado de instrucción y que entonces dentro de él se ocupa especialmente de intervenir en los casos y situaciones que ese juzgado investiga y que requieren por su naturaleza de la certificación oficial de un médico. Por ejemplo, el médico forense es el profesional que por excelencia determinará las causas y el horario de muerte de un individuo. Gracias a su formación profesional podrá identificar en la víctima determinadas características que lo harán dilucidar esos datos.[20]

[19] Tomado de http://www.marcialpons.es/static/pdf/9788415664185.pdf
[20] Tomado de http://www.urru.org/papers/Rrfraude/InformaticaForense_OL_HA_RL.pdf

6. DISEÑO METODOLOGICO

El presente estudio monográfico pretende demostrar y evidenciar cuales fueron los factores han contribuido al auge de la cibercriminalidad en el país, y más específicamente en el sector de la tecnología móvil de Smartphones con sistema operativo Android; para poder desarrollar el presente estudio e investigación se consultaron diversas fuentes académicas, también fuentes abiertas y se consultó con funcionarios judiciales que trabajan en el área forense de algunas entidades estatales quienes aportan información de la realidad que es ampliamente conocida en el país a cual es una falta de cultura hacia el cuidado de la información digital.

Para ello se realizó un estudio básico con algunas pruebas de tipo técnico en ambientes virtuales y simulados que permiten enfocar la presente investigación monográfica hacia la publicación de un nuevo conocimiento basado en la prevención, así como ampliar aquellos criterios preconcebidos que hay en la sociedad acerca del manejo y seguridad de la información que se almacena en un Smartphone con sistema operativo Android.

En cuanto al tipo de estudio, este tuvo como criterio o fundamente el bibliográfico, ya que estuvo orientado hacia la búsqueda, organización y análisis crítico de literatura científica en el campo de la Ciberseguridad; del mismo modo se realizó un estudio de tipo experimental al poder descubrir y plasmar aquellos factores que son evidentes en el fenómeno del aumento de la cibercriminalidad que cada vez aumenta en Colombia.

En cuento a la población muestra objeto del presente estudio, al ser un estudio monográfico donde se hace una simulación, no existe como tal, ya que la población estudio es cualquier persona que utilice un Smartphone con sistema operativo Android y así explicar lo que podría ocurrirle si no toma las recomendaciones o precauciones respecto de aquellas situaciones que podrían poner en riesgo la seguridad de la información que viaja o se almacena en su terminal móvil.

7. RESULTADOS Y DISCUSIÓN

7.1. METODOLOGÍAS Y TÉCNICAS UTILIZADAS EN ATAQUES A DISPOSITIVOS MÓVILES ANDROID

El auge de la tecnología ha hecho que la inseguridad llegue hasta los linderos de los mismos avances tecnológicos en dispositivos móviles, razón por la cual se hace imperioso inicialmente conocer cuáles son las técnicas y metodologías utilizadas por parte de los cibercriminales para generar aplicaciones maliciosas que se aprovechan de la inseguridad que la gran mayoría de dispositivos móviles Android presentan y así lograr éxito en su intención de causar un daño a las usuarios para poder lucrarse del mismo, que es lo que los caracteriza.

Pero de qué manera estos Ciberdelincuentes realizan estos ataques a los sistemas operativos Android; algunos de los virus o software malicioso que envían estos Ciberdelincuentes, una vez se depositan en la carpeta raíz del Smartphone, comienzan a adueñarse del dispositivo y a desatar publicidad con anuncios no deseados por parte del usuario, mientras, van absorbiendo información confidencial y/o privada del usuario, como fotos, videos, documentos cuentas de correo y demás información que un usuario tenga dentro del dispositivo al punto que el Ciberdelincuente obtiene un gran volumen de información la cual por lo general es vendida a terceros con fines delincuenciales pero el aparato por la operación tan fuerte del virus y la cantidad excesiva de publicidad por lo general queda inservible o para ser reparado[21].

En este orden de ideas a continuación se describen las metodologías más comunes que son utilizadas para realizar ataques con software malicioso a dispositivos móviles Android:

- Ataques por medio de caballos troyanos: Este ataque muy común se apoya por medio de las herramientas de explotación Metasploit que con comandos como Meterpreter que es un conjunto de herramientas per se, con la cual se logra hacer una penetración digital con un código a modo de backdoor o en español de puerta trasera, es decir que sin que el usuario del dispositivo se dé cuenta se le ha hecho una inserción de código malicioso el cual trabaja en segundo plano accediendo a toda la información.

[21] Artículo de referencia de http://www.eltiempo.com/archivo/documento/CMS-16425666

Ahora este procedimiento descrito anteriormente se logra mediante la creación de un archivo de tipo APK por lo general mediante la ejecución de una línea de código como, por ejemplo:

#sudo msfpayload android/meterpreter/reverse_tcp LHOST=192.168.x.x LPORT=4444 R > /root/Desktop/juegos.apk

Con la cual se crea un archivo malicioso denominado *juegos.apk* que será el archivo infectado que se enviará posteriormente a un dispositivo Android; este tipo de ataque se verá simulado y explicado con mayor profundad en el ítem 8 del presente documento, por lo pronto se verán las generalidades y métodos que pueden ser usados con ésta categoría de infección.

Entonces este tipo de infección puede provocarse por medio de dos vías, la primera de ellas es generando un código de tipo QR, utilizados para redireccionar y acceder de manera rápida a una página web de un fabricante o acceder a la instalación de una aplicación.

Imagen No. 1. Apariencia gráfica de un código de tipo QR.

Fuente: http://masquevinilo.com/vinilos-decorativos/208-vinilo-decorativo-codigo-bidi-qr.html

La segunda vía para trasmitir un troyano infeccioso para dispositivos móviles Android de tipo APK, es creando una página web falsa de tipo Phishing o de suplantación de identidad.

Para el caso de la generación de un código QR, los Ciberdelincuentes suben el archivo de tipo APK a un servidor cualquiera para que desde allí se pueda generar la aplicación y para la segunda vía es crear una página falsa, como se muestra a continuación.

- Ataques por medio de Spoofing: El presente es un método muy común utilizado para desarrollar ataques a dispositivos móviles y busca mediante la utilización de ataque de ingeniería social conocer los datos de usuario y contraseña de una red social como Facebook, por medio de su aplicación.

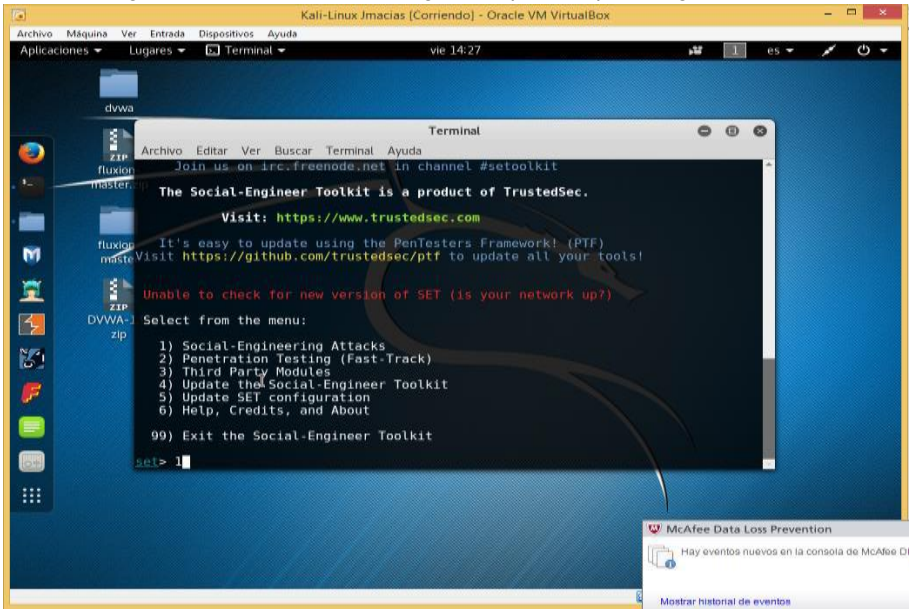
Con la herramienta de Kali Linux social *engineering setoolkit* la cual se ubica en la ruta que muestra la figura siguiente se observa el desarrollo de cómo se realiza este ataque:

Imagen No. 2. Aplicación de la herramienta Social Engineering de Kali Linux para la configuración de la prueba spoofing.

Fuente: El autor.

Una vez abierta la aplicación se configuran los parámetros necesarios para realizar el ataque, para ello se selecciona la opción 1 que determina que es un ataque de ingeniería social, como se muestra en la siguiente imagen:

Imagen No. 3. Parámetros de configuración para ataque de ingeniería social.



Fuente: El autor.

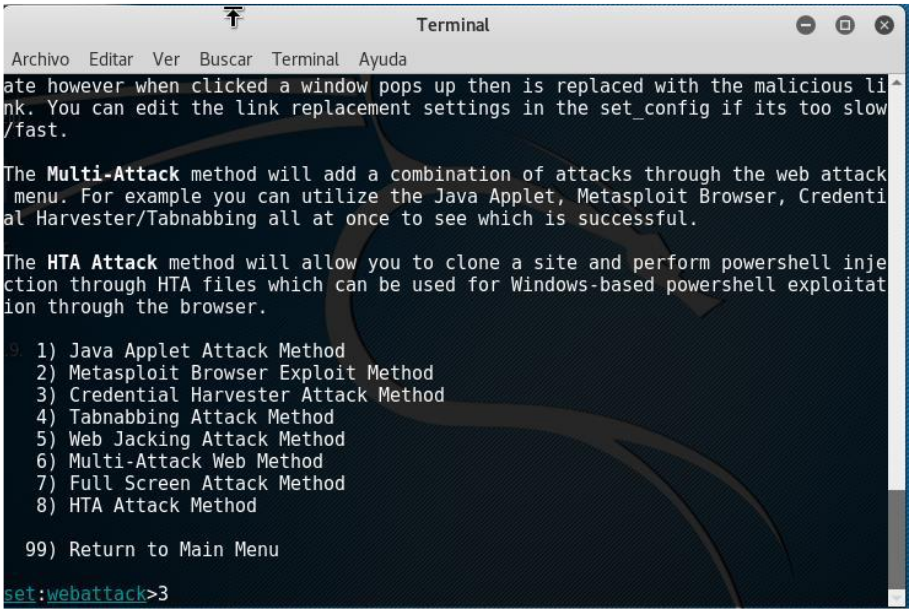
Posteriormente se selecciona la opción 2 de ataque a un sitio web como se muestra en la figura:

Imagen No. 4. Parámetros de configuración para ataque de ingeniería social

Fuente: El autor.

Luego la opción de método de ataque que para este caso es un método de obtención de credenciales, opción 3, como se muestra en la figura:

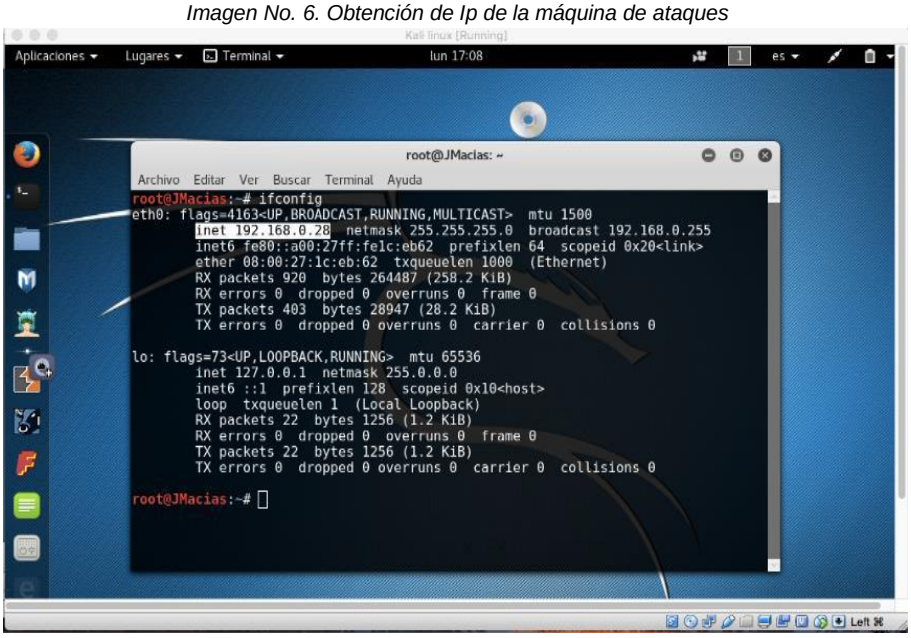
Imagen No. 5. Parámetros de configuración para ataque de ingeniería social



Fuente: El autor.

Es necesario conocer la ip de la máquina que hace los ataques, en este caso la Ip de Kali Linux para establecerla en los parámetros de la aplicación Social Engineering de Kali Linux, dentro de la opción Site Cloner que se mostrará más adelante, entonces para ello dentro de Kali Linux se abre una terminal y se ejecuta el comando *ifconfig* como se muestra en la figura:

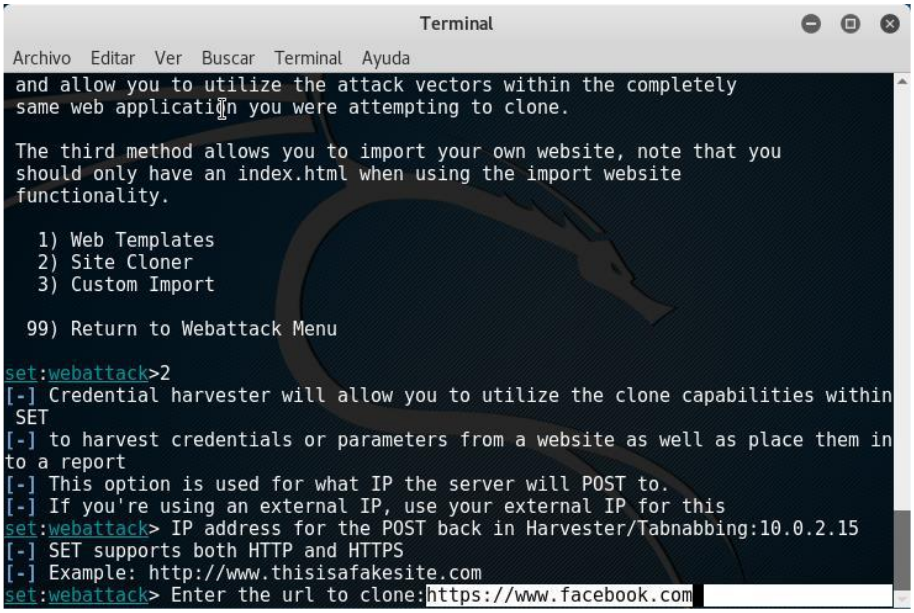
Imagen No. 6. Obtención de Ip de la máquina de ataques



Fuente: El autor.

Seguidamente se selecciona el parámetro de clonación de un sitio web, opción 2, como se muestra en la siguiente figura y se establece la Ip de Kali Linux (se aclara que la Ip que se colocó es la correspondiente a la 192.168.0.28 y no la Ip 10.0.2.15) para que la máquina atacada sea re direccionada a la máquina de ataques por medio de la URL que se quiere clonar, que para este caso es Facebook:

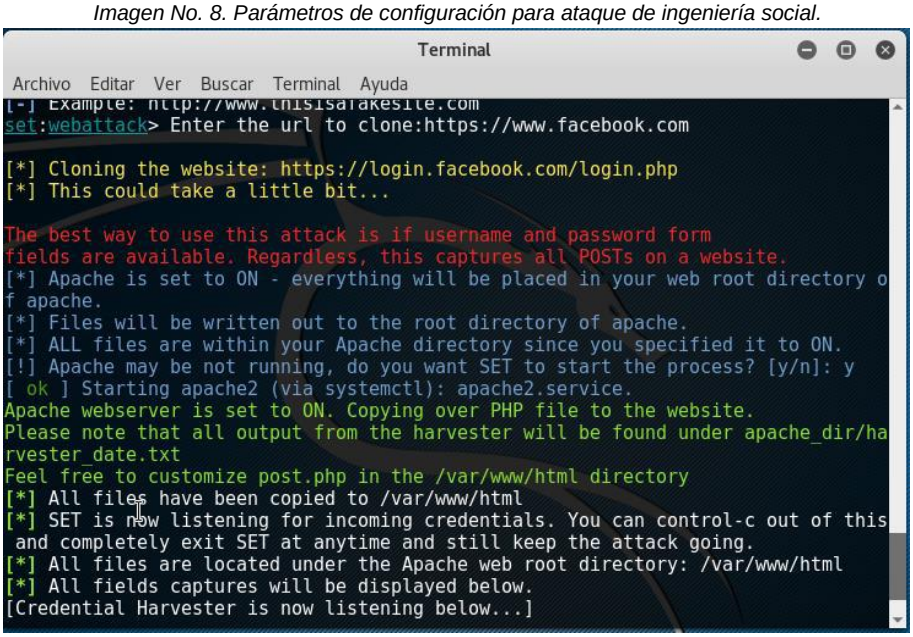
Imagen No. 7. Parámetros de configuración para ataque de ingeniería social.



Fuente: El autor.

Con los parámetros anteriormente indicados el sitio web queda clonado y la aplicación Social Engineering, arroja el mensaje de clonación exitosa como se muestra en la figura:

Imagen No. 8. Parámetros de configuración para ataque de ingeniería social.

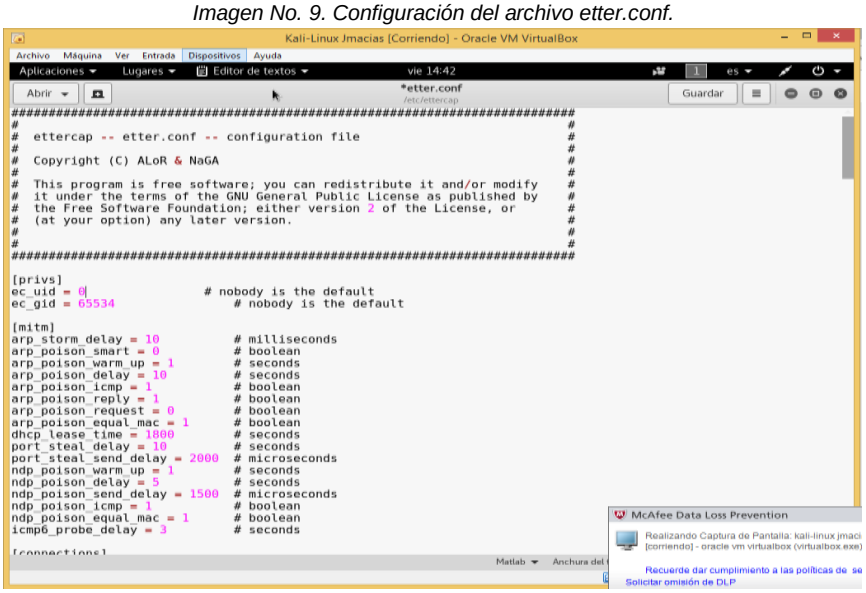


Fuente: El autor.

Ahora se procede a hacer uso de la aplicación o herramienta ETTERCAP de Kali Linux para la ejecución del ataque, para ello se procede a configurar el archivo

etter.conf cambiando los valores 65534 que aparecen en este archivo a cero (0) guardando estos cambios tal y como se muestra en la figura siguiente. La ubicación de este archivo se encuentra dentro de la ruta Equipo/ettercap/ettercap.conf:

Imagen No. 9. Configuración del archivo etter.conf.



Fuente: El autor.

Posteriormente se procede a configurar el archivo etter.dns que se encuentra en la misma ruta indicada anteriormente cambiando las URL de Microsoft que están por defecto en este archivo por las URL de Facebook y la Ip que aparecer por defecto también se cambia por la Ip de la máquina Kali Linux es decir la Ip 10.0.2.15 y se guarda, tal y como se muestra en la figura.

Imagen No. 10. Configuración del archivo etter.dns.

Fuente: El autor.

Se abre la aplicación Ettercap la cual se localiza tal y como se muestra en la figura siguiente y se despliega la opción unified sniffing del menú sniff para iniciar pruebas de Sniff en la máquina Kali, esto se muestra:

Imagen No. 11.Ruta para la ejecución de la aplicación Ettercap.

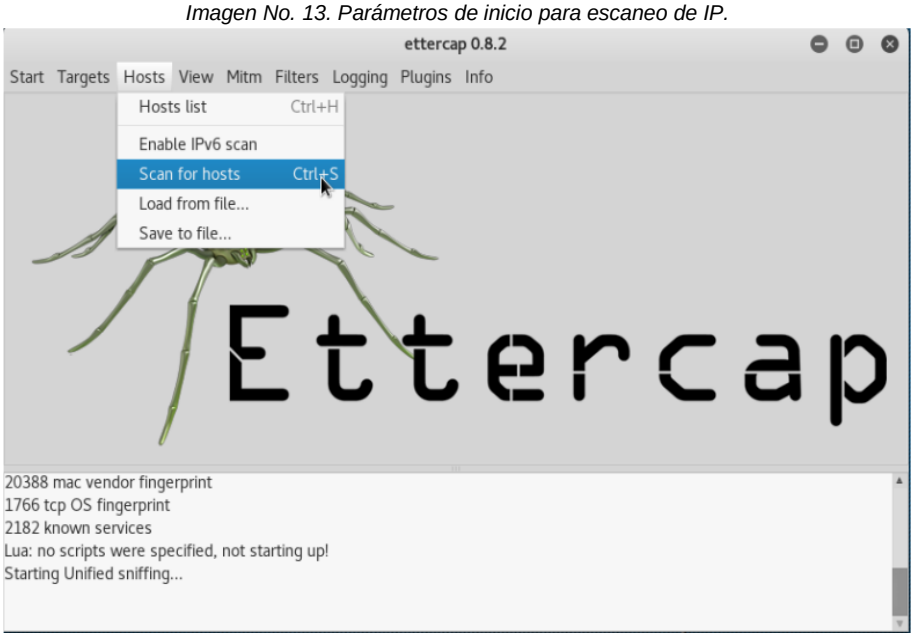
Fuente: El autor.

Imagen No. 12. Parámetros de inicio para escaneo de IP.

Fuente: El autor.

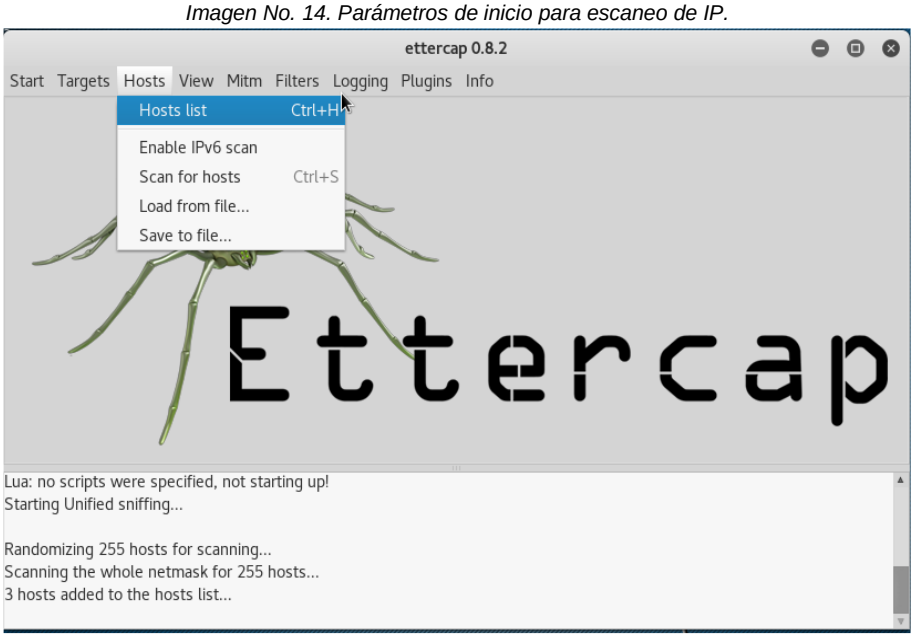
Se selecciona la opción scan for host del menú host para escaneo de Ip´s, tal y como se muestra en la figura siguiente y se enlistan mediante la opción que se muestra en la figura 14:

Imagen No. 13. Parámetros de inicio para escaneo de IP.



Fuente: El autor.

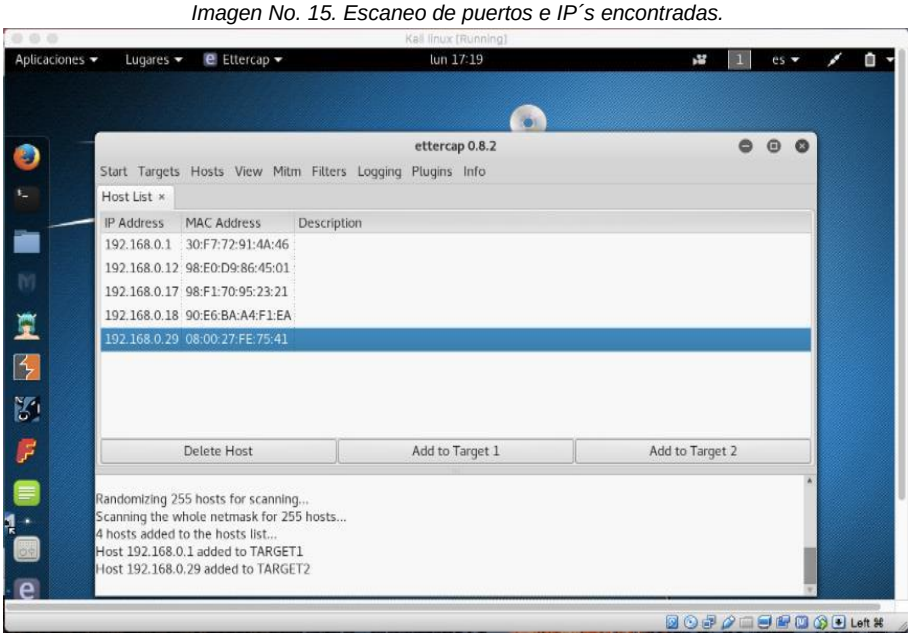
Imagen No. 14. Parámetros de inicio para escaneo de IP.



Fuente: El autor.

Como se observa en la siguiente figura fueron localizadas 5 direcciones Ip las cuales corresponden entre otras, a la máquina de ataques, a la máquina víctima y a la máquina física donde se está trabajando.

Imagen No. 15. Escaneo de puertos e IP´s encontradas.

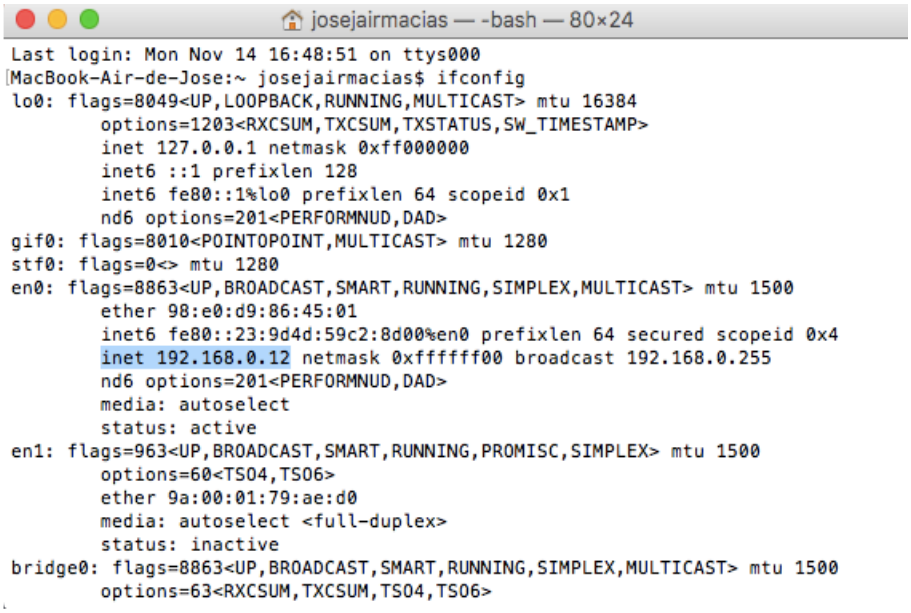


Fuente: El autor.

A continuación, y siguiendo los mismos pasos anteriormente enunciados se procede a realizar la práctica en otra máquina física con otras IP diferentes, lo anterior dado que para efectos prácticos de la presente actividad no fue posible continuar la práctica en el PC con las IP anteriormente mostradas en las gráficas, pero se obvian los pasos anteriores toda vez que son los mismos y solo cambian las IP.

Entonces en este sentido primero se procede a conocer la IP atacante que es la IP de la máquina virtual con Kali Linux y posteriormente la IP de la máquina física que para este caso es la IP de un portátil Mac, es decir para corroborar que las IP que se escanearon con Ettercap son correctas se muestran las figuras que siguen las cuales corresponden a las IP que muestra el escaneo de ettercap:

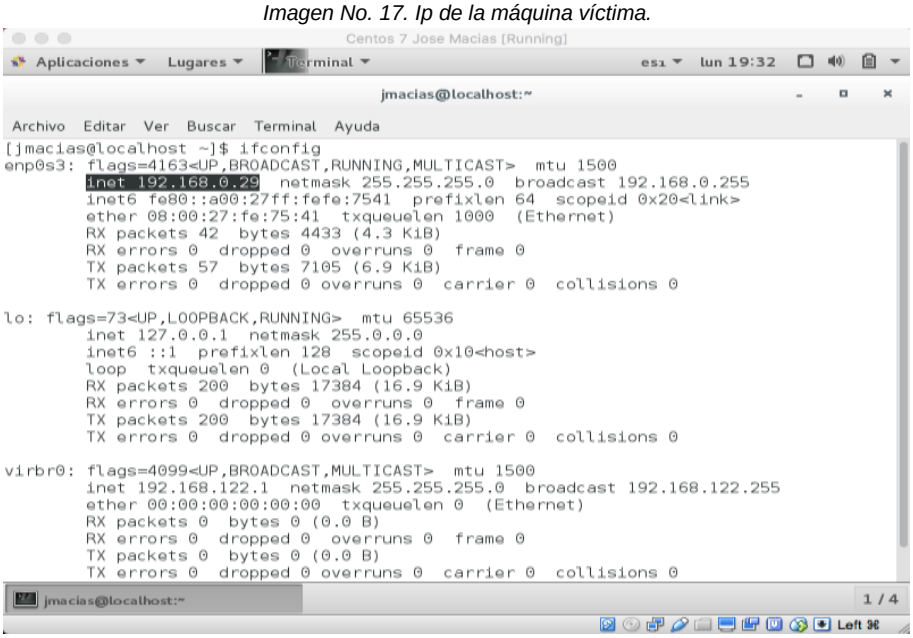
Imagen No. 16. Ip de la máquina física.



Fuente: El autor.

Seguidamente la IP de la máquina virtual que va hacer las veces de víctima, para este caso se trabajó con una máquina virtual con SO Centos 7 ambiente gráfico:

Imagen No. 17. Ip de la máquina víctima.

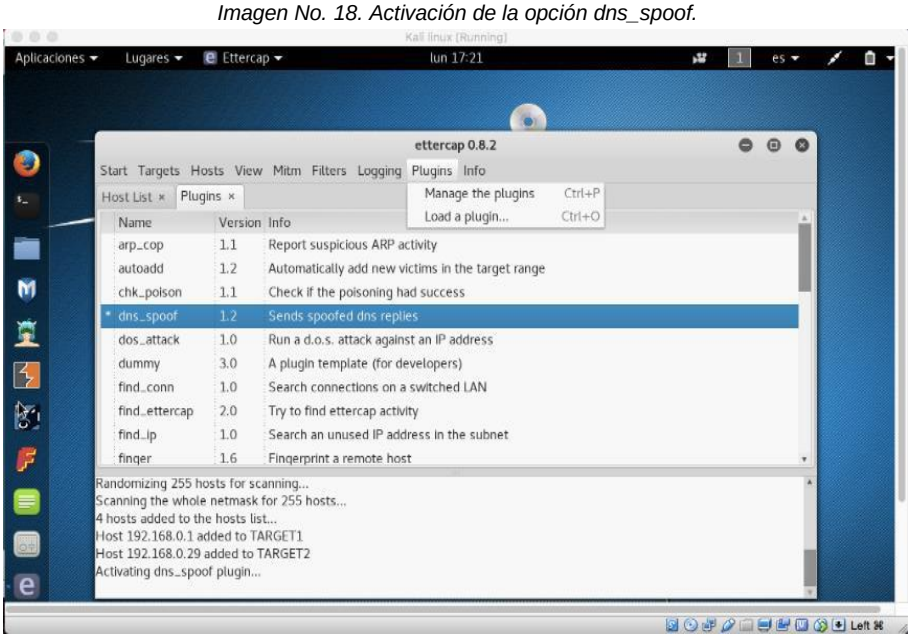


Fuente: El autor.

Se vuelve a abrir la herramienta Ettercap de Kali Linux para escanear y enlistar los puertos que se van a atacar, se observa que se detectaron la IP víctima, la IP de la

máquina física pero la primera IP es la del router de la red interna que permite la conexión y salida a internet, por lo tanto se agregan como objetivo 1 o Target 1 el router que da la salida a internet y el target 2, la víctima para prueba de spoofing cómo se observa y se activa la opción dns_spoof para que se ejecute solamente este tipo de ataque en la víctima:

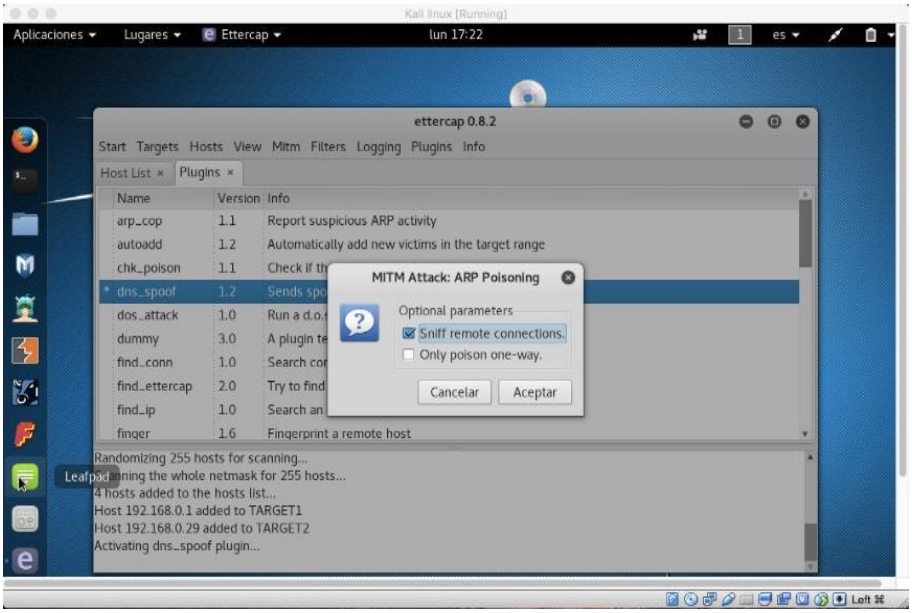
Imagen No. 18. Activación de la opción dns_spoof.



Fuente: El autor.

Se le da el parámetro para que realice un sniff a la máquina víctima como se observa en la figura:

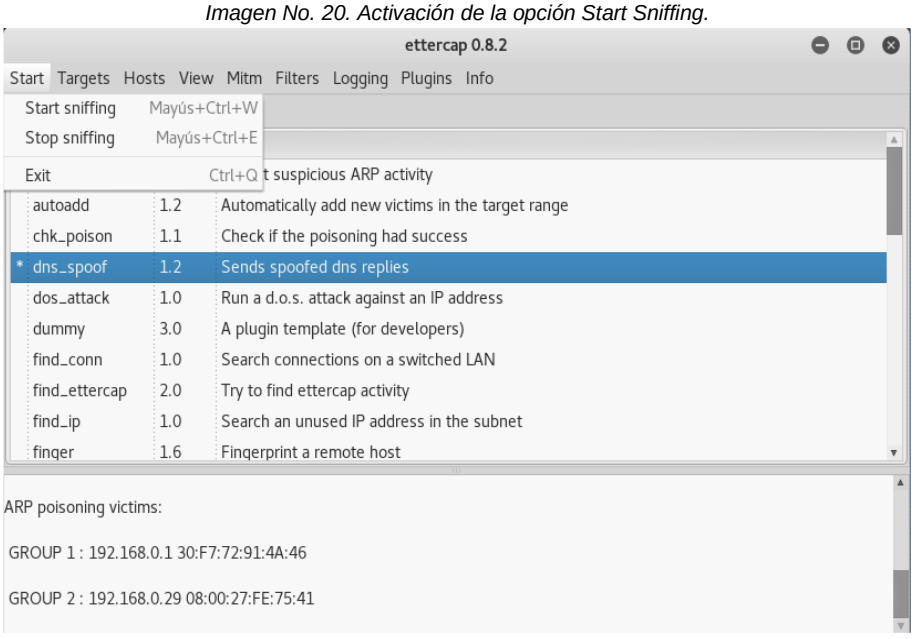
Imagen No. 19. Activación de la opción Sniff remote connections



Fuente: El autor.

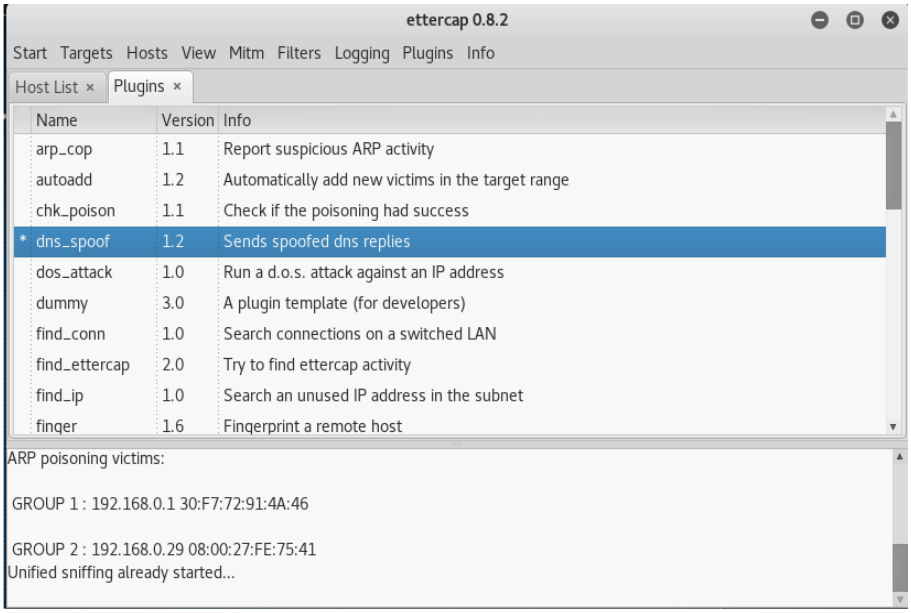
Y por último se activa el ataque por la opción start sniffing como se observa en las figuras:

Imagen No. 20. Activación de la opción Start Sniffing.



Fuente: El autor.

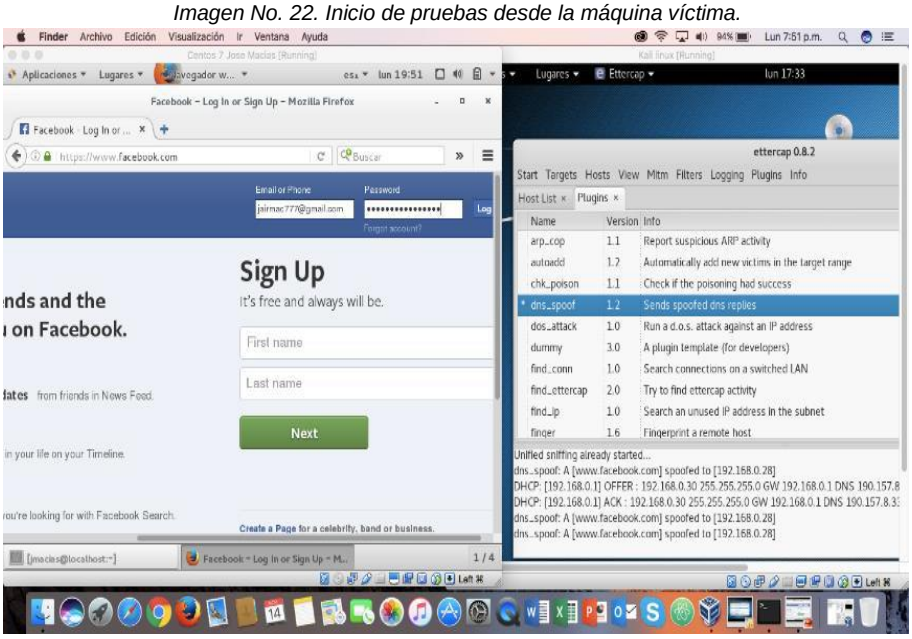
Imagen No. 21. Activación de la opción Start Sniffing.



Fuente: El autor.

Se abre la página www.facebook.com en la máquina Centos, que fue la página a clonar observando que automáticamente es detectada por la herramienta Ettercap tal y como se observa a la derecha de la siguiente figura:

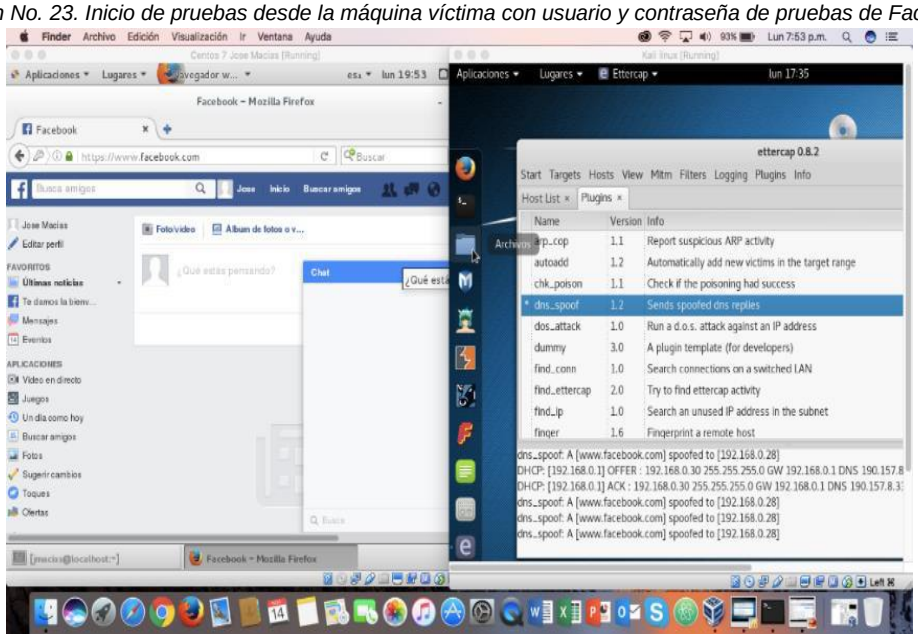
Imagen No. 22. Inicio de pruebas desde la máquina víctima.



Fuente: El autor.

Se ingresa con un usuario y contraseña de pruebas lo cual también es detectado en la herramienta Ettercap tal y como se muestra en la figura:

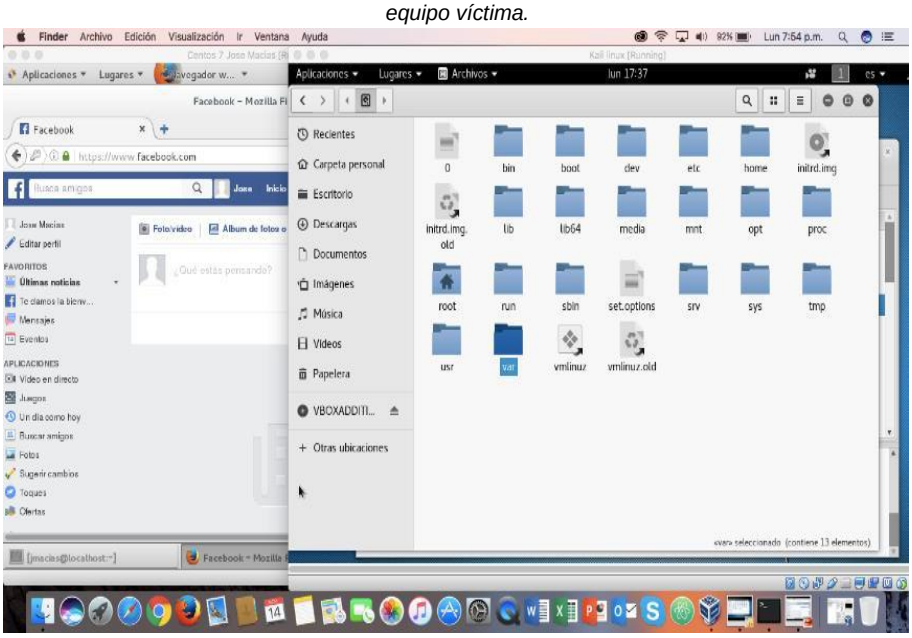
Imagen No. 23. Inicio de pruebas desde la máquina víctima con usuario y contraseña de pruebas de Facebook.



Fuente: El autor.

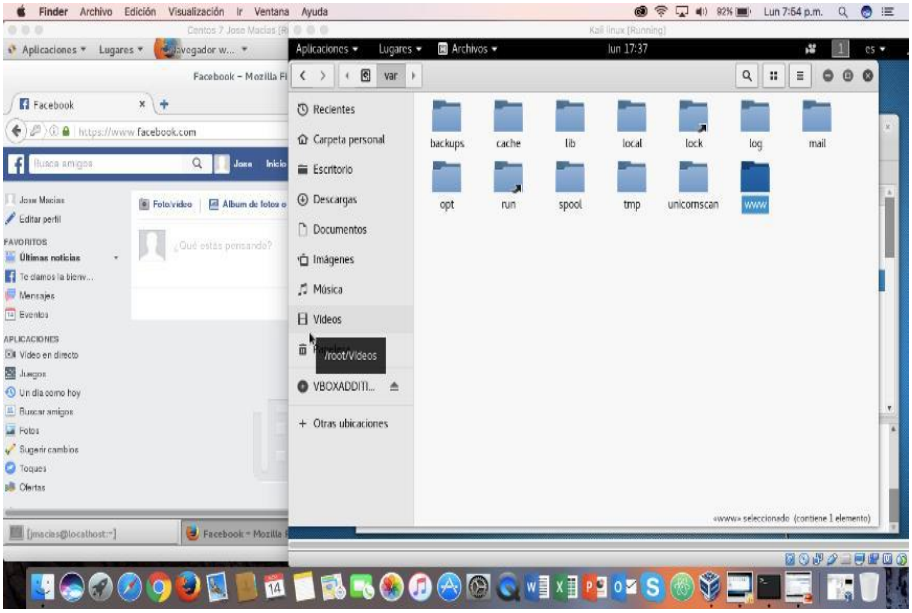
Y en este momento ya son captados por la herramienta Ettercap los datos de usuario y contraseña los cuales se ubican en la ruta de Kali Linux, *Equipo/var/www/html/harvester.txt*, este último archivo puede cambiar de nombre dependiendo el equipo pero siempre será esta la ubicación; la anterior ruta se muestra en las siguientes tres figuras:

Imagen No. 24. Ruta de acceso al archivo creado por Ettercap de captura de datos de usuario y contraseña de Facebook en equipo víctima.



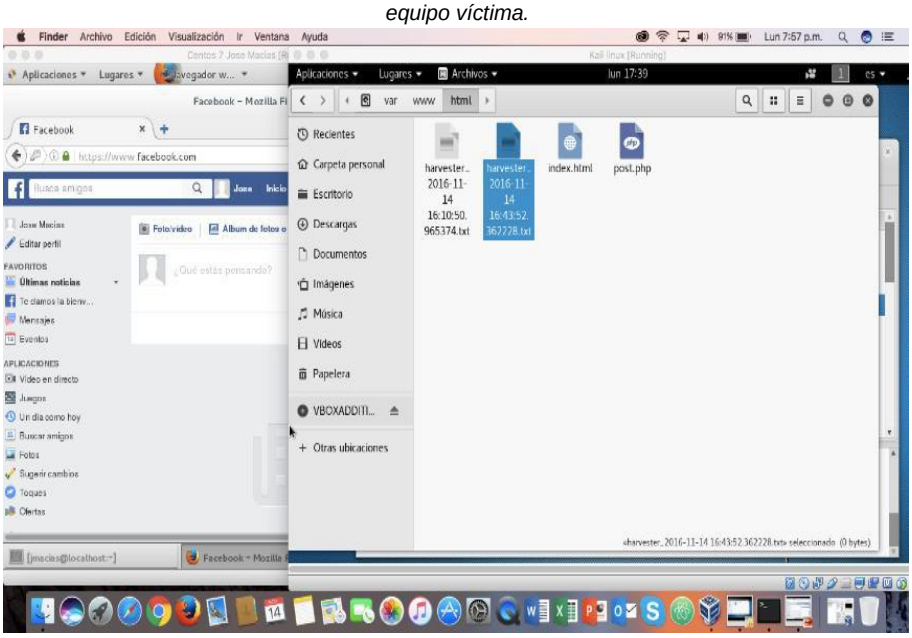
Fuente: El autor.

Imagen No. 25. Ruta de acceso al archivo creado por Ettercap de captura de datos de usuario y contraseña de Facebook en equipo víctima.



Fuente: El autor.

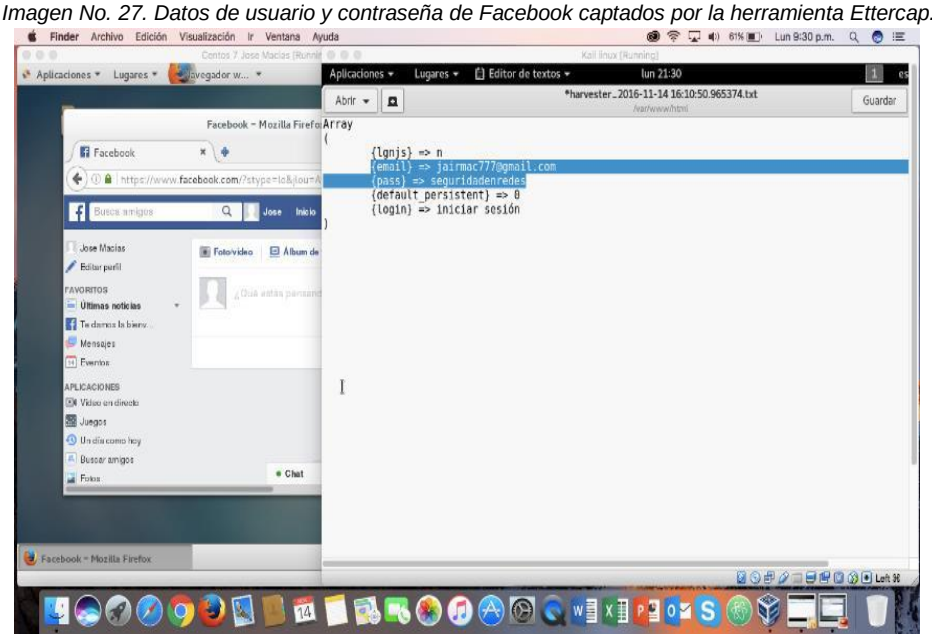
Imagen No. 26. Ruta de acceso al archivo creado por Ettercap de captura de datos de usuario y contraseña de Facebook en equipo víctima.



Fuente: El autor.

Por último, se obtienen los datos de usuario y contraseña de pruebas extraídos del equipo que puede ser cualquier terminal móvil tal y como se observa en la siguiente figura:

Imagen No. 27. Datos de usuario y contraseña de Facebook captados por la herramienta Ettercap.

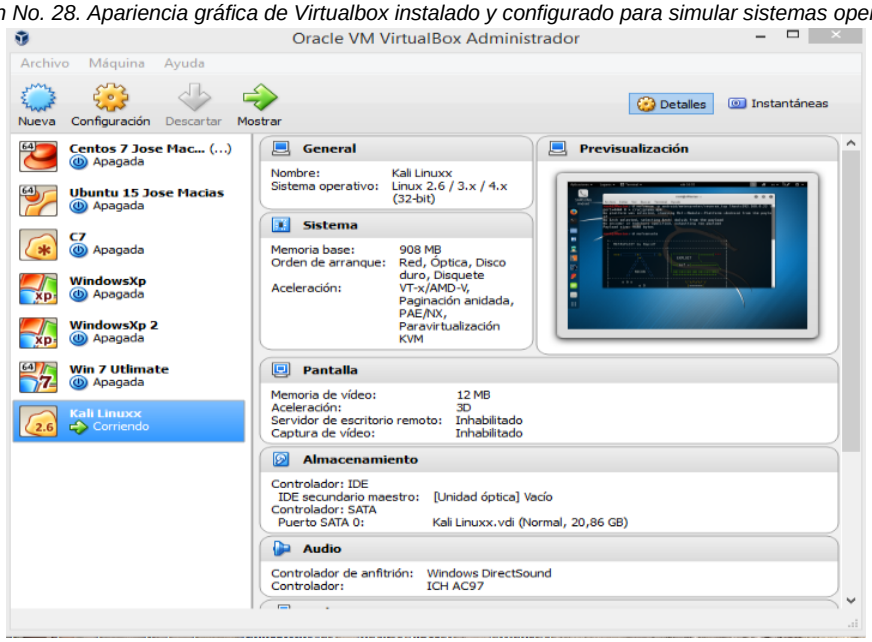


Fuente: El autor.

7.2. DESCRIPCIÓN DE ATAQUES DENTRO DE RED LAN A DISPOSITIVO ANDROID MEDIANTE INFORMATICA FORENSE

Dentro del presente estudio monográfico se hace necesario realizar la simulación de un ataque a un dispositivo móvil con S.O., Android; para ello se trabajará con herramientas de virtualización que permitan demostrar sin inconvenientes reales, de qué manera se realiza y se presenta un ataque a una terminal con ese S.O. Primero se trabajará con un software de virtualización llamado Virtualbox, el cual se descarga de su página oficial[22].

Imagen No. 28. Apariencia gráfica de Virtualbox instalado y configurado para simular sistemas operativos.



Fuente: El autor.

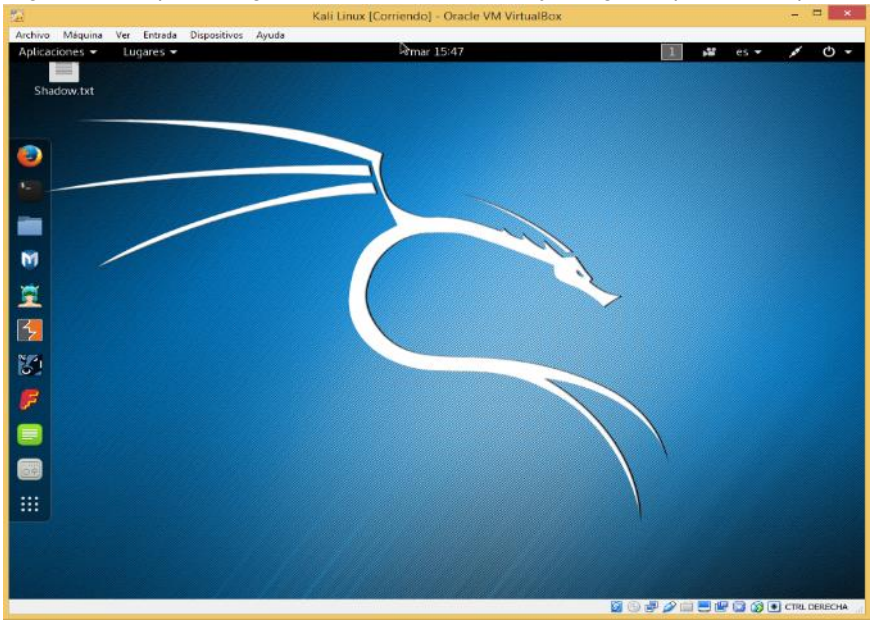
Virtualbox permite simular un sistema operativo S.O., de cualquier fabricante y de cualquier tecnología, ya sea Linux, Unix o Windows con el fin de hacer pruebas de comportamiento o para poder optimizar los recursos de este S.O., sin que la máquina física se vea afectada, salvo que los recursos de la máquina física cómo la memoria RAM o el disco duro se disminuyen mientras se ejecuta una virtualización ya que es otro proceso ejecutado[23]. Una de las grandes ventajas de Virtualbox es que es un software de acceso libre es decir no hay que pagar por su utilización y en cualquier momento que se realice un proceso de virtualización el usuario que instale un S.O., puede eliminarlo o desinstalarlo sin tener que hacer otra tarea más que un clic para desinstalar.

[22] Descarga de Virtualbox, página oficial https://www.virtualbox.org/
[23] Cómo instalar y utilizar Virtualbox https://www.youtube.com/watch?v=nQiR5_iGVJI

Para realizar las pruebas de simulación, se utilizará el S.O. Kali Linux[24], un sistema operativo muy completo y dedicado específicamente para realizar Pentest o Hacking Ético, esto por medio de herramientas y técnicas que también utilizan los cibercriminales pero para poder, analizar, aprender y deducir como contrarrestar cualquier ataque malicioso que un Ciberdelincuente realice. Kali Linux está basado en tecnología Linux-Debian y tiene más de 300 herramientas de simulación de ataques reales, razón por la cual es importante manejar este sistema operativo con mucho cuidado.

Kali Linux es un S.O., gratuito y su descarga puede realizarse mediante imagen ISO para Virtualizar o por medio de una USB para hacer particionado en una máquina física[25].

Imagen No. 29. Apariencia gráfica de Kali Linux instalado y configurado para simular pruebas.



Fuente: El autor.

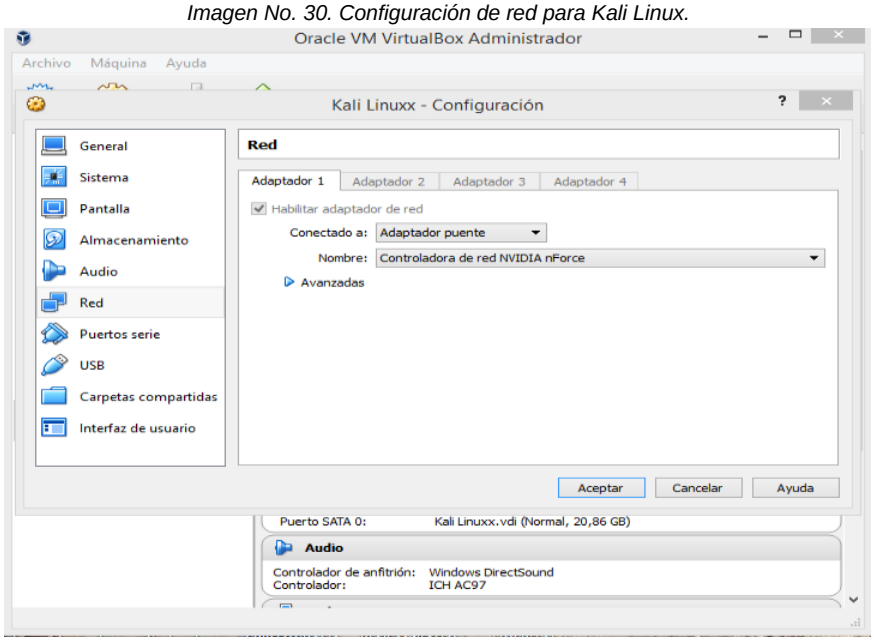
Como ya se mencionó, Kali Linux tiene más de 300 herramientas para hacer pruebas de Penetración, con las cuales desarrollar simulaciones exitosas de ataques en diferentes aspectos, de red, WiFi, a dispositivos móviles entre muchos otros más. Como el objeto del presente estudio es hacer una simulación de un ataque a un dispositivo móvil Android, se ha escogido una herramienta denominada Metasploit con la cual se desarrollará un ataque de ingeniería inversa dentro de una red LAN a un celular Samsung Galaxy S4. Metasploit permite lanzar con una de sus herramientas un ataque a cualquier dispositivo de forma inofensiva e invisible, por

[24] Página oficial para descarga de Kali Linux https://www.kali.org/
[25] Cómo instalar Kali Linux en Virtualbox https://www.youtube.com/watch?v=voYhIW0eHqc

medio de un archivo infectado que al ser recibido por una víctima la herramienta hace explotar el archivo con código malicioso y remotamente se logra tener un acceso de manera casi total del dispositivo infectado, esto se muestra a continuación.

Para poder simular un ataque a dispositivo Android, es importante primero que todo configurar el tipo de red que va a utilizar Kali Linux ya que este ataque se hace dentro de una misma red LAN, por lo tanto la Ip que va a utilizar Kali debe estar dentro del rango de la máquina física donde está virtualizado, entonces se conecta en Adaptador Puente tal y como se muestra en la siguiente imagen:

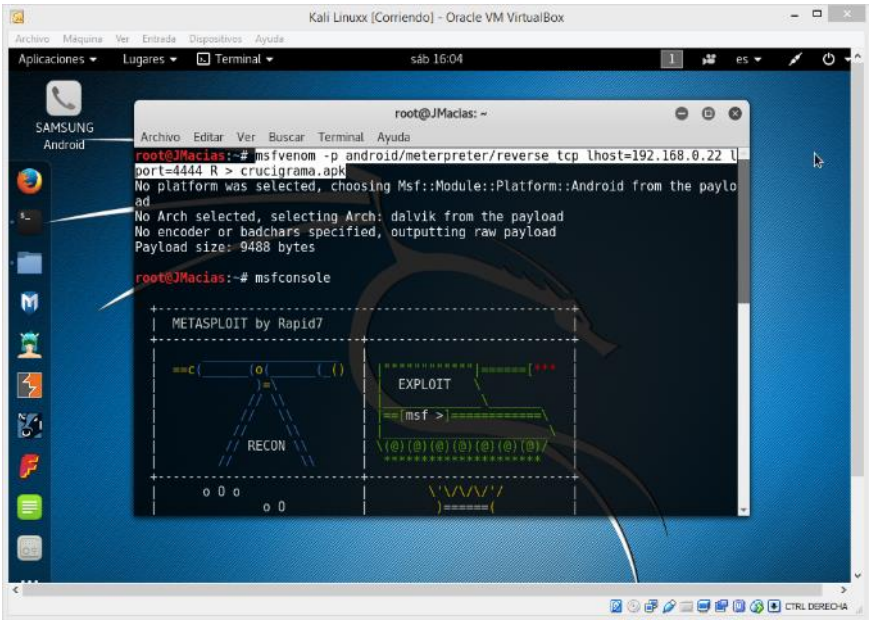
Imagen No. 30. Configuración de red para Kali Linux.



Fuente: El autor.

A continuación, se procede con la ejecución de la línea de comando mostrada en la imagen No. 4, con la función Meterpreter, para un ataque de ingeniería inversa que permite crear un archivo infectado de tipo APK, lo anterior desde la IP 192.168.0.22 que corresponde a la máquina Kali Linux:

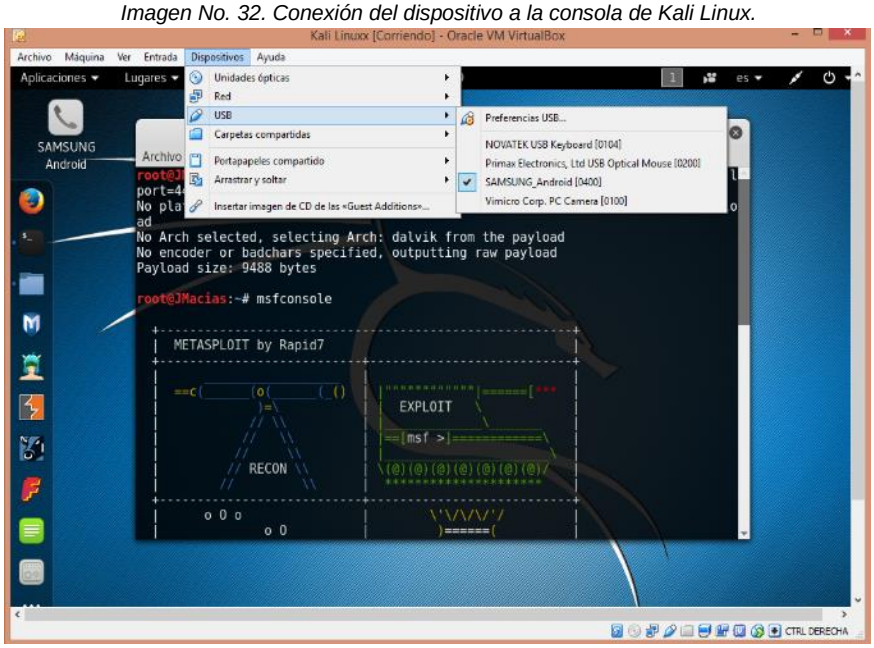
Imagen No. 31. Ip de la máquina atacante.



Fuente: El autor.

La ejecución del comando anterior crea un archivo malicioso, el cual se nombró crucigrama.apk para que sea llamativo e inofensivo para cualquier usuario que lo intente instalar, con un tamaño de 9,4 KB. Lo siguiente es conectar el dispositivo móvil a la consola de Kali Linux para colocar este archivo en la memoria interna del dispositivo Android de pruebas:

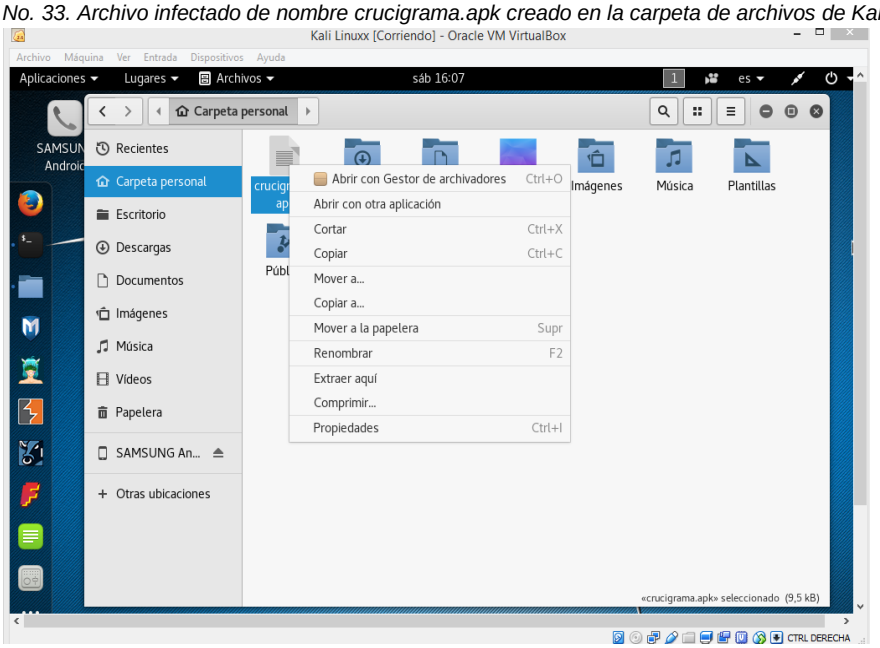
Imagen No. 32. Conexión del dispositivo a la consola de Kali Linux.



Fuente: El autor.

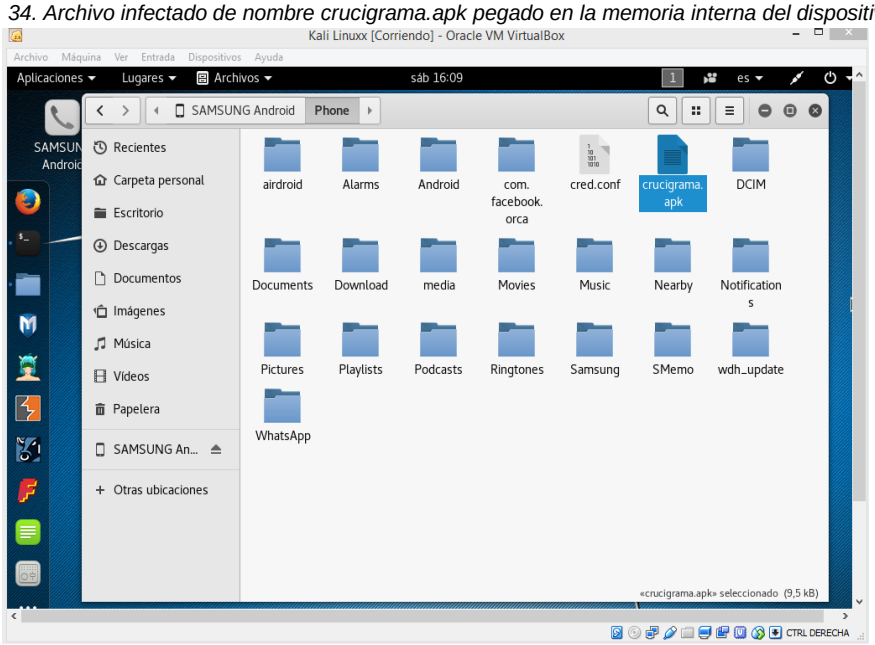
A continuación, se localiza el archivo crucigrama.apk, en la carpeta de documentos de Kali Linux donde quedó guardado una vez se crea, se copia y se pega en la memoria interna del dispositivo Android que para este caso es un celular Samsung Galaxy S4, tal y como se observa en las siguientes dos imágenes:

Imagen No. 33. Archivo infectado de nombre crucigrama.apk creado en la carpeta de archivos de Kali Linux.



Fuente: El autor.

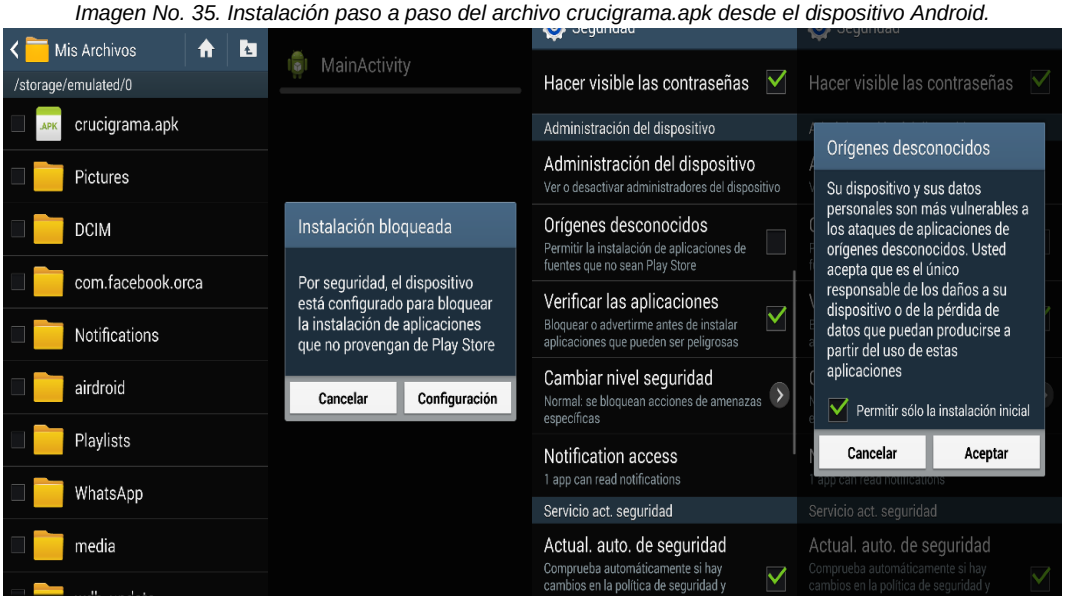
Imagen No. 34. Archivo infectado de nombre crucigrama.apk pegado en la memoria interna del dispositivo Android.



Fuente: El autor.

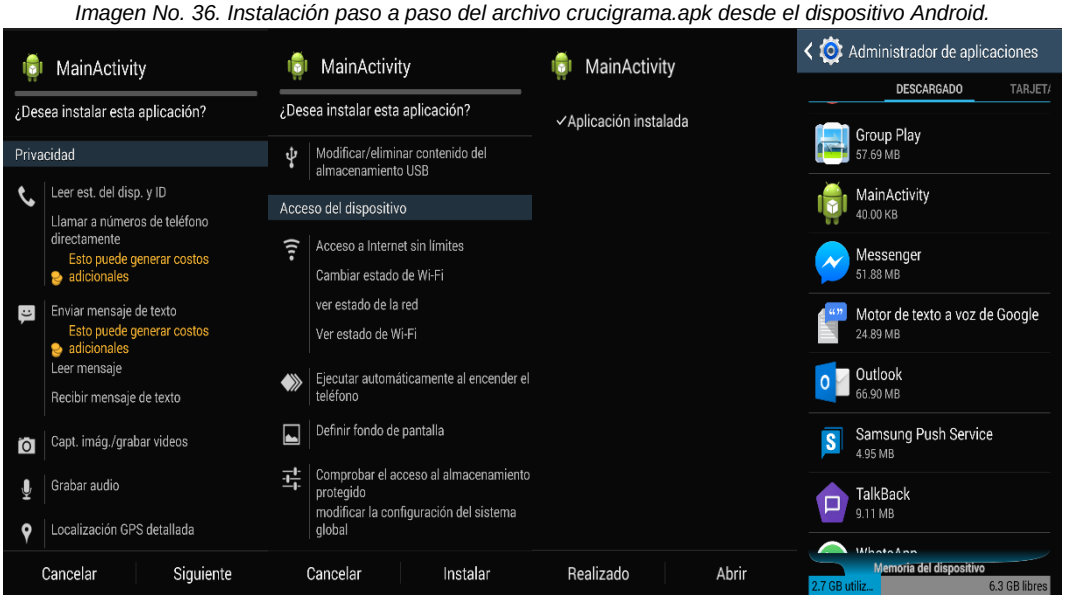
Una vez el archivo de nombre crucigrama.apk está en la memoria interna del dispositivo Android, se procede a instalarlo y ejecutarlo dentro del dispositivo tal y como se observa en las siguientes dos imágenes:

Imagen No. 35. Instalación paso a paso del archivo crucigrama.apk desde el dispositivo Android.



Fuente: El autor.

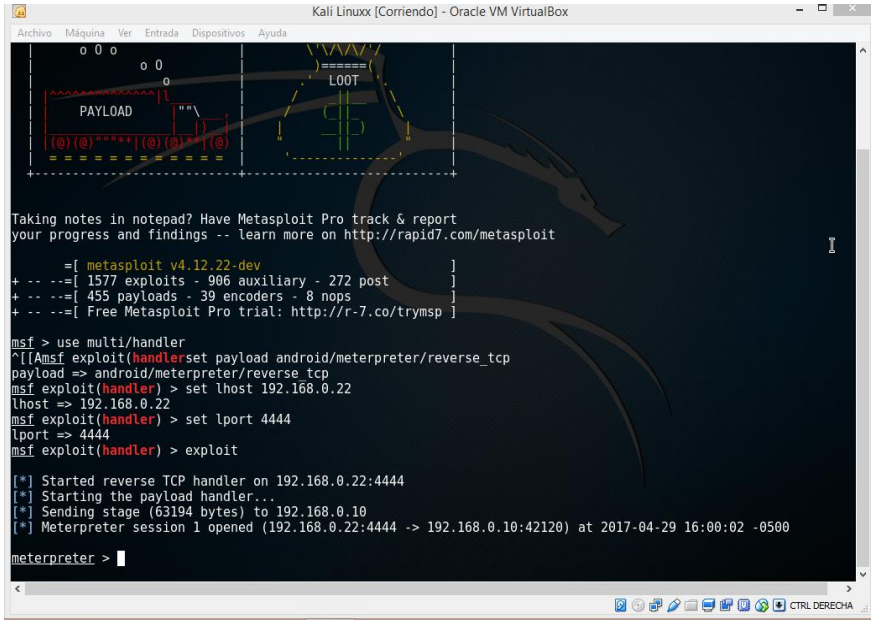
Imagen No. 36. Instalación paso a paso del archivo crucigrama.apk desde el dispositivo Android.



Fuente: El autor.

Posterior a lo anterior y teniendo en cuenta que ya se había iniciado una sesión de consola de Metasploit previamente configurada para dejarla en modo de escucha para que una vez se abra la aplicación en el dispositivo se inicie el control remoto al mismo así:

Imagen No. 37. Control del dispositivo Android desde la consola de Metaspolit.



Fuente: El autor.

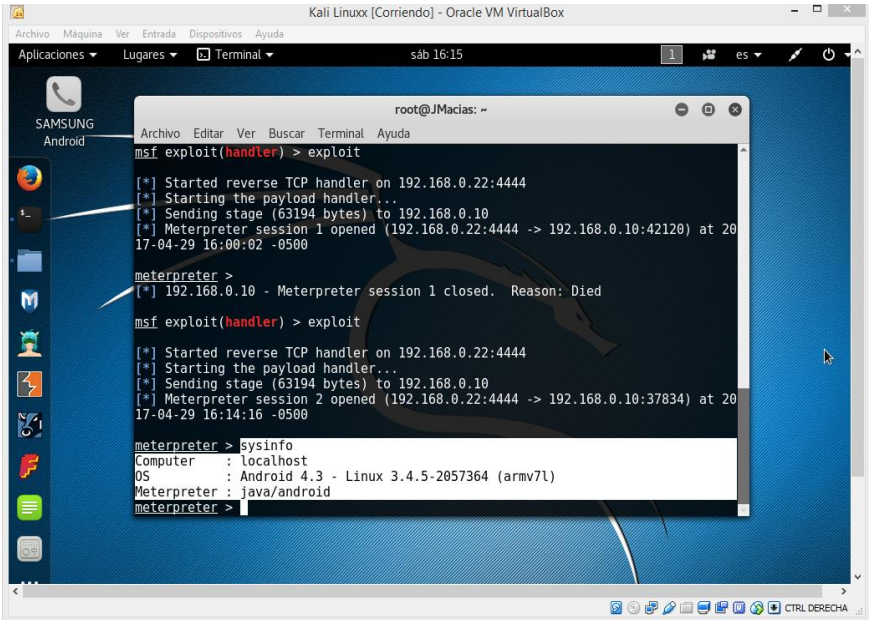
Es importante mencionar que, para que el ataque pueda tener resultado primero se debe abrir una consola de Metasploit con el comando msfconsole, configurar el tipo de ataque, la dirección Ip, el puerto por donde saldrá y ejecutar el exploit que equivale a dejar en modo de escucha la herramienta; luego, desde el dispositivo se debe instalar la aplicación y ejecutarla.

Una vez se inicia la comunicación entre la consola y el dispositivo se procede a hacer uso de las herramientas de Metasploit, para poderlo controlar; para ello se ejecutan una serie de comandos y se despliega el menú de opciones que permitirán entre otras cosas, poder acceder a las cámaras del dispositivo en tiempo real, conocer los mensajes de texto que le han llegado al usuario del móvil, realizar capturas de pantalla en tiempo real y guardar toda esta información en la carpeta de documentos de Kali Linux. Lo interesante de todo esto es que el usuario no se da por enterado que esta información se le está sustrayendo de manera ilegal desde su dispositivo ya que son acciones que ocurren en segundo plano.

Se hace la aclaración que las pruebas realizadas se utilizó un celular de pruebas de propiedad de quien suscribe el presente documento.

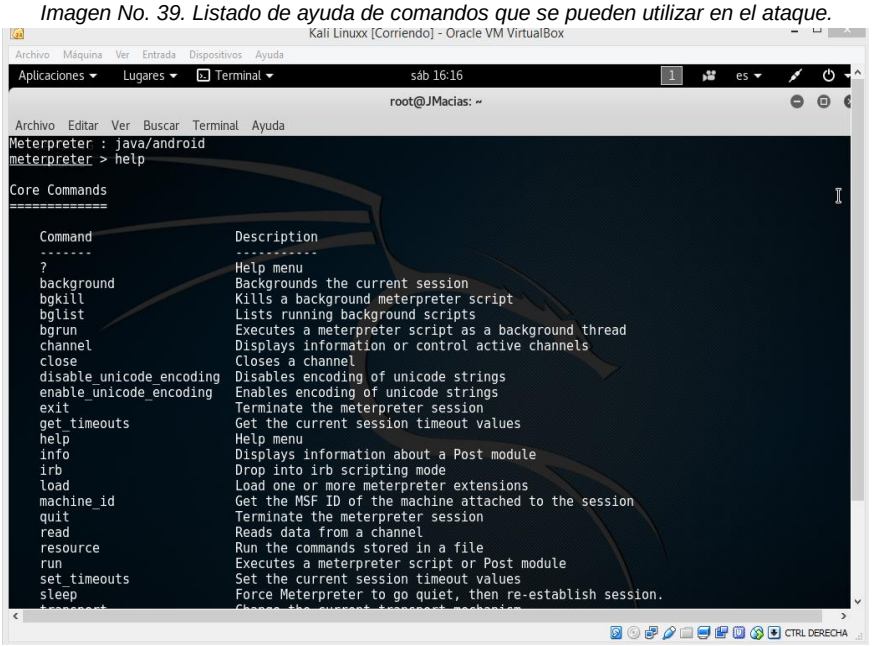
El resultado de la explotación exitosa del archivo crucigrama.apk en el móvil, que permitieron el control remoto en segundo plano del mismo, se muestran en las siguientes imágenes:

Imagen No. 38. Obtención de información de fábrica del dispositivo Android con el comando sysinfo.



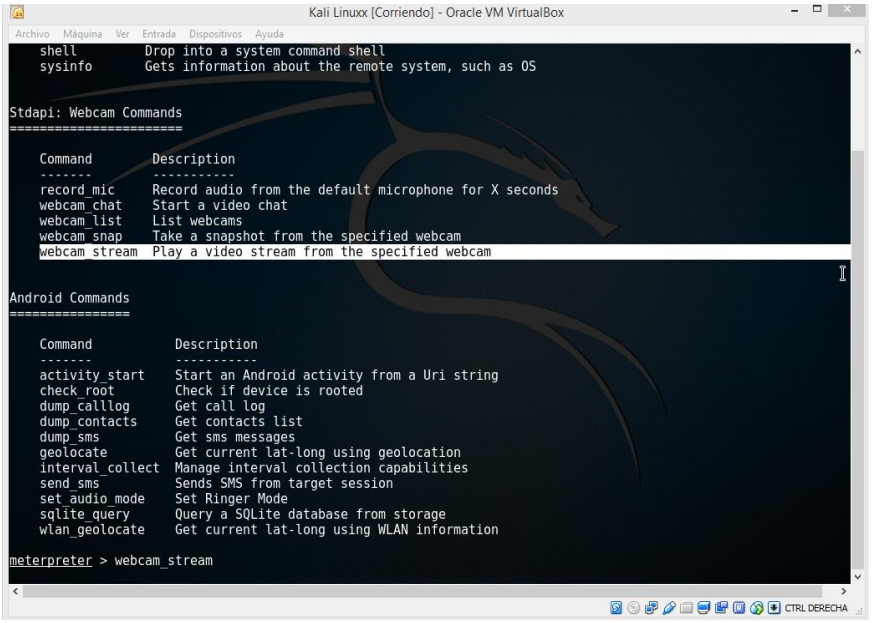
Fuente: El autor.

Imagen No. 39. Listado de ayuda de comandos que se pueden utilizar en el ataque.



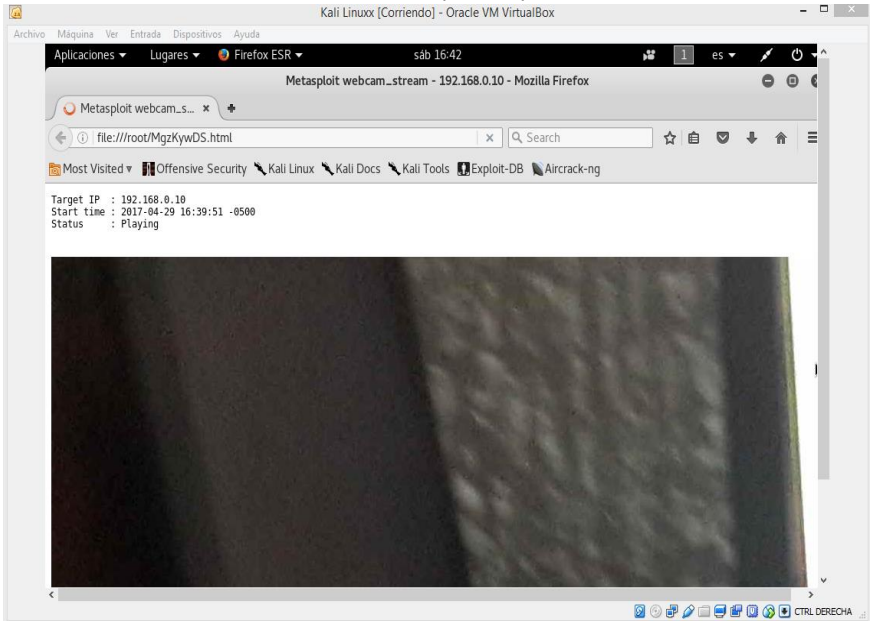
Fuente: El autor.

Imagen No. 40. Control de la cámara trasera del dispositivo por medio del comando webcam_stream.



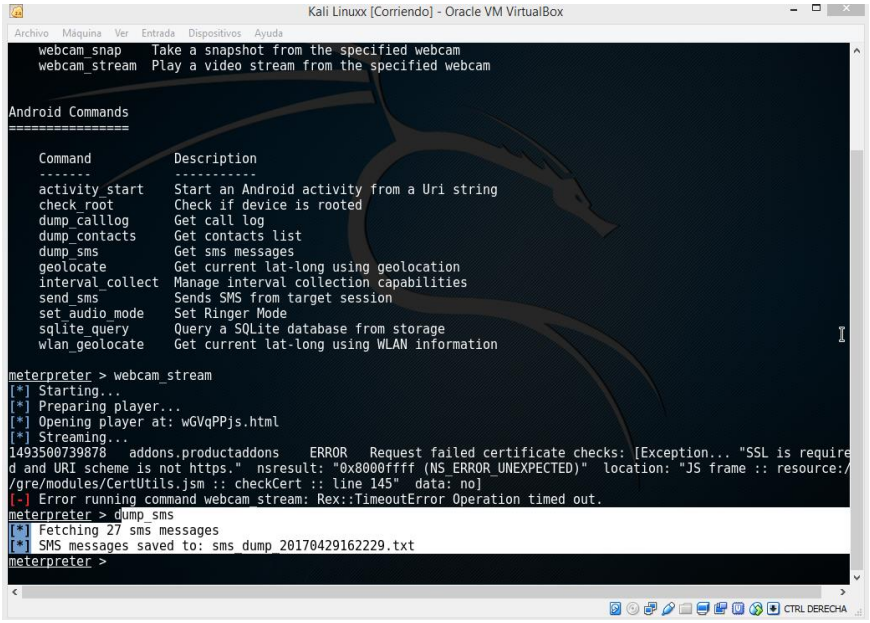
Fuente: El autor.

Imagen No. 41. Control de la cámara trasera del dispositivo por medio del comando webcam_stream.



Fuente: El autor.

Imagen No. 42. Obtención de los mensajes de texto por medio de la ejecución del comando dump_sms.



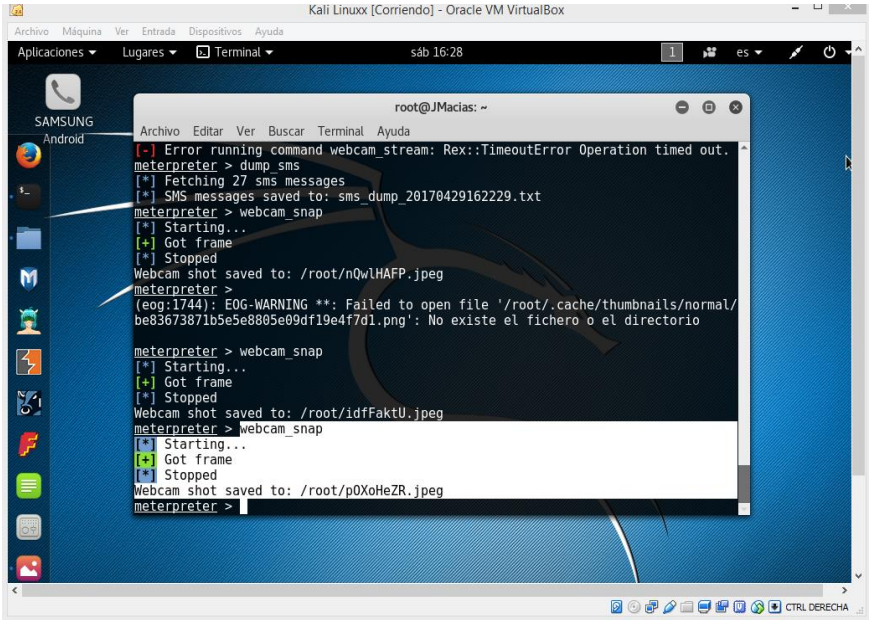
Fuente: El autor.

Imagen No. 43. Obtención de los mensajes de texto por medio de la ejecución del comando dump_sms.

Fuente: El autor.

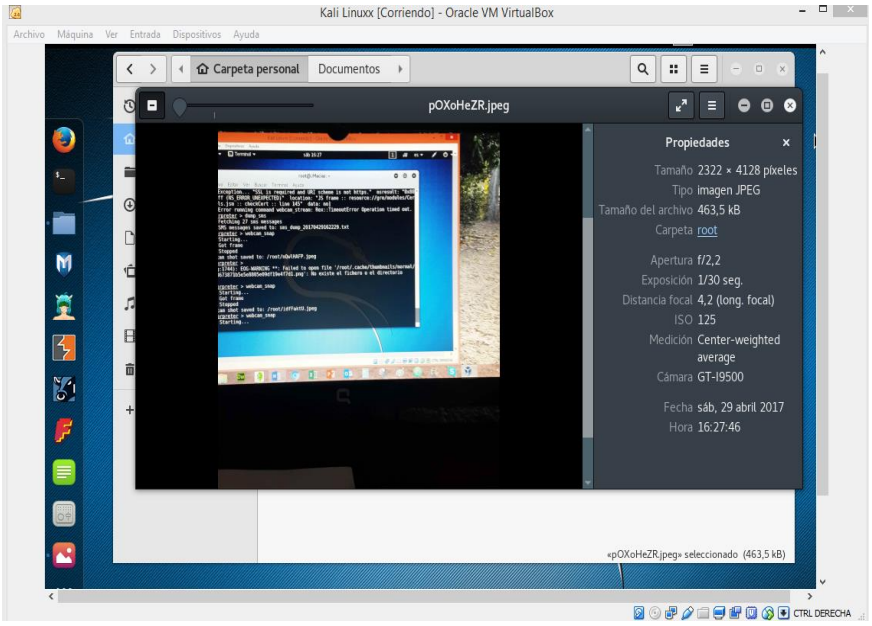
La última prueba realizada fue una captura de pantalla instantánea con la cámara trasera del dispositivo con el comando webcam_snap, esto se evidencia en las siguientes dos imágenes:

Imagen No. 44. Captura instantánea con la cámara trasera del dispositivo con el comando webcam_snap.



Fuente: El autor.

Imagen No. 45. Captura instantánea con la cámara trasera del dispositivo con el comando webcam_snap.



Fuente: El autor.

Por medio de Metasploit se pueden realizar más tipos de ataques a dispositivos móviles, del mismo modo con la herramienta Meterpreter de Metasploit es posible ejecutar más tipos de control remoto a dispositivos que han sido infectados con archivos de tipo APK, tales como control del audio, grabaciones, llamadas entre

otras y esto gracias a que los archivos APK (Android Application Package)[26] que son archivos que contienen información empaquetada para dispositivos Android, una vez son explotados ejecutan una codificación que permite realizar controles internos dentro de la configuración de un dispositivo y enviar información remota.

Con este archivo APK se logró desasegurar el dispositivo de pruebas y se le crearon una serie de reglas internas al mismo que le otorgaron permisos de control total al atacante para que pudiera acceder al móvil por medio de funciones ejecutadas en segundo plano, es decir sin que la víctima se diera cuenta que alguien estaba usando su teléfono, ya que esto no es visible para el usuario del móvil.

El objetivo de esta simulación fue lograr conocer de qué manera y con qué propósito los Ciberdelincuentes intentan obtener de manera ilegal y abusiva información de tipo privada y confidencial de un usuario cualquiera para poder en algunos casos extorsionar a cambio de dinero, a sus víctimas para no publicar en sus mismas redes sociales, fotos intimas, información comprometedora o en otros casos robar claves bancarias y extraer dinero. Ahora, es claro que la instalación de un archivo malicioso de estas características no es una labor que se logre de manera abrupta o con fuerza bruta (aunque hay técnicas que si lo logran), por lo general y como se observó estos ataques se dieron gracias a que un usuario recibió un archivo en su celular y decidió por su propia cuenta instalarlo.

Para el presente caso el archivo fue pegado directamente desde la consola de Kali Linux en la memoria interna del dispositivo para efectos demostrativos, pero en la realidad, este archivo también puede ser enviado vía correo electrónico desde una dirección falsa de un amigo, por WhatsApp por un contacto falso, por Facebook o por cualquier otra red social, con un nombre llamativo, una publicidad atractiva o una página falsa; cualquiera puede caer en el engaño de aceptar el APK y ejecutarlo, y esto puede ocurrir en una zona WiFi, de un aeropuerto, de un Café o en la misma casa.

Entonces como se pudo observar el archivo de nombre crucigrama.apk que posterior a su instalación y ejecución se convierte en una aplicación denominada Main Activity, puede ser desinstalado y eliminado del dispositivo si se cuenta con los conocimientos previos, y la disciplina necesaria para proteger un móvil; es claro que la seguridad es fácilmente vulnerable pero también hay maneras de complicarle el acceso a los Ciberdelincuentes y así como se instala un archivo malicioso así

[26] Véase también http://www.androidpit.es/android-para-principiantes-apk

mismo puede ser eliminado; para el presente caso la manera de eliminar y evitar este ataque es desinstalar la aplicación directamente desde el menú de configuración del equipo y del mismo modo eliminar el archivo de instalación denominado crucigrama.apk, de la siguiente manera:

Imagen No. 46. Desinstalación de la aplicación Main Activity.

Fuente: El autor.

Imagen No. 47. Eliminación del archivo de instalación malicioso.

Fuente: El autor.

Si se mantiene la costumbre de no aceptar cualquier aplicación desconocida por medio de archivos de dudosa reputación se previene un ataque por parte de un Ciberdelincuente.

7.3. PRINCIPALES TÉCNICAS RECOMENDADAS POR EXPERTOS PARA EVITAR SER VÍCTIMAS DE ATAQUES EN DISPOSITIVOS ANDROID

Son muchas las recomendaciones y técnicas que expertos en Ciberseguridad, empresas fabricantes de, celulares y de sistemas operativos, entre otras han aportado a la sociedad para generar prevención y evitar que sean víctimas de cibercriminales que se apoderen de sus datos personales y/o les afecten en su diario vivir; claramente en la presente monografía se ha evidenciado que el porcentaje de vulnerabilidad que presenta una persona que utiliza un dispositivo con S.O. Android es bastante alto.

Es por ello que a continuación se plasman de manera puntual algunas recomendaciones que expertos en Ciberseguridad han realizado con base en su experiencia y conocimiento y que son de gran utilidad y aplicabilidad en un mundo en el cual no se acostumbra a tener una cultura de la protección de los datos. Del mismo modo se plantea el uso de algunas aplicaciones muy útiles

7.3.1. PRIMERA RECOMENDACIÓN TÉCNICA: CÓMO PROTEGER UN MÓVIL ANDROID DEL ATAQUE DE UN VIRUS

Es muy importante conocer el ámbito en el cual se mueven los cibercriminales, la experta en temas de seguridad informática del banco BBVA Ana Gómez Blanco quien trabaja como Global Cybersecurity Awareness en esa entidad, hace frecuentemente recomendaciones al respecto y en algunos de sus blogs aporta sugerencias para seguridad en Android.

Los malware y virus informáticos móviles son cada vez más frecuentes y nuevos en su forma de ser combatidos y éstos pueden ser adquiridos ya sea en la descarga de alguna aplicación o a través de algún mensaje circulando por cualquiera de las redes que se tienen instaladas en el dispositivo. En este sentido la forma de propagación provoca que los virus viajen de móvil a móvil de forma rápida lo que hace necesario el no confiar en cualquier enlace, foto, o documento sospechoso que llegue por estos medios.

Una de las estafas y ataques más conocidos es el ‘phishing’, la estrategia como ya es conocida, consiste en suplantar la identidad de webs oficiales en los que el gancho suele ser súper descuentos o suscripciones gratuitas a Netflix, entre otras pero que en realidad se trata de estafas virales cuya finalidad es generar suscripciones de pago a servicios PREMIUM de forma fraudulenta. Además, este

tipo de fraude está diseñado para que el usuario infectado comparta, sin querer, a todos sus contactos la URL que contiene el virus. Algo involuntario que no evita que toda su agenda reciba dicha comunicación maliciosa.

Esto es muy común, pero para evitar y frenar estas suscripciones involuntarias es importante tener máxima precaución ante este tipo de propuestas tentadoras, por lo cual, y para mayor seguridad indica la experta, es importante también contactar con la compañía telefónica donde se tiene el plan y cancelar los servicios de tarificación adicional que no se han adquirido. Otra situación de malware en Android es que las aplicaciones pueden introducir virus en los dispositivos ocasionando inconvenientes a sus propietarios, como el robo de información o contaminación de anuncios que invaden el terminal y a veces dejan inservible el dispositivo.

Indica la experta lo que ya es conocido por mucho, lo cual es para tener en cuenta y es que, una de las características de Android es que es posible descargar e instalar aplicaciones desde fuera de los canales oficiales, como Google Play, lo que supone un riesgo adicional para el dispositivo y por esta razón, es importante prestar atención a cada aplicación, y descargar aplicaciones solo de canales oficiales, como Play Store, fuentes y desarrolladores de confianza, para el caso bancario usar aplicaciones de la fuente oficial como la app de BBVA y revisar los comentarios de los que ya la han usado y descargado estas aplicaciones.

Aunado a lo anterior es importante revisar los permisos que requiere una aplicación; es necesario comprobar si son importantes para su funcionalidad, si resultan excesivos se debería evitar instalarla, seguro que hay otra alternativa que requiera solo los permisos necesarios, sobre todo en aquellas aplicaciones que no lo requieren, pero aun así lo solicitan.

Indica la experta la importancia de utilizar una ‘herramienta lupa’ para revisar las aplicaciones que se tienen en el dispositivo Android como por ejemplo CONAN, desarrollada por la empresa INCIBE que permite identificar las aplicaciones potencialmente peligrosas, conocer el grado de actualización y revisar los permisos otorgados en las mismas; coadyuvando con esto no se debe dejar de lado instalar un antivirus en el terminal, ya sea gratuito o de pago. En la página oficial de la OSI (Oficina de Seguridad del Internauta) existen diferentes opciones de antivirus validados por este organismo.

Como se puede observar es muy importante como recomendación utilizar aplicaciones seguras y de fabricantes conocidos, es muy común y sobre todo en las

aplicaciones bancarias que exista la suplantación de identidad, porque el activo por el cual los cibercriminales van, primordialmente es el dinero y al igual que en la vida 'offline', el sentido común y la desconfianza ante lo desconocido, extraño o demasiado bueno para ser real es necesario y no está demás.[27]

7.3.2. SEGUNDA RECOMENDACIÓN TÉCNICA: CONSEJOS PARA MEJORAR LA SEGURIDAD DE ANDROID

Enrique Pérez es un editor del portal web de España denominado el Androide Libre, es un experto y apasionado entre otros temas por todo lo concerniente a protección de información para dispositivos Android; a continuación, se plasman algunas recomendaciones que hace en materia de protección informática con estos dispositivos.

Y es que el uso de Smartphones es cada vez más frecuente y con el paso del tiempo se guarda mucha información sensible e importante en ellos, razón por la cual menciona el experto es muy importante proteger la seguridad de los Android.

- Como primera medida se debe descargar Apps solo de Google Play: Son muchas las formas que hay para acceder a la privacidad de un dispositivo móvil, a pesar que Google trabaja para que Android sea un sistema seguro, la verdad es que muchas situaciones quedan fuera de su responsabilidad, en ese entendido una gran cantidad de malware viene de orígenes desconocidos sin contar que en Android se tiene acceso a modo root y muchas maneras de instalar APKs.

  En este sentido indica el experto es importante conocer que para instalar aplicaciones seguras la ruta en el dispositivo Android es, ajustes, seguridad, desactivar la casilla de 'fuentes desconocidas' y marca también la casilla de 'Verificar aplicaciones'.

- Crear y utilizar contraseñas seguras: Los datos para crear contraseñas deben evitar datos como '12345', el nombre, la fecha de nacimiento o utilizar cualquier contraseña que se pueda adivinar fácilmente, por ello es recomendable las combinaciones de letras mayúsculas, números y símbolos; del mismo modo, es recomendable cambiar con frecuencia el patrón de desbloqueo del teléfono. La ruta para lo anterior es, ajustes, seguridad,

[27] Tomado de la URL https://www.bbva.com/es/proteger-movil-android-ataque-virus-2/

seleccionar Bloqueo de pantalla y allí elegir la contraseña, luego ir a ajustes, seguridad y desactivar también la casilla de contraseñas visibles.

- Encriptar los datos: El S.O. Android 5.0 Lollipop viene cifrado de fábrica específicamente para los dispositivos como el Nexus 6 o Nexus 9, pero los Android de versiones 4.4 KitKat o anteriores también pueden activar el cifrado, para ello se debe ir a ajustes, seguridad, cifrado y elegir 'Cifrar dispositivo' y 'cifrar tarjeta SD externa', esto tiene un problema, y es que reduce la velocidad de lectura pero por otro lado nadie podrá acceder al contenido en caso que se roben el móvil o que se pierda.

- Permisos de las aplicaciones: Es importante verificar al momento de descargar una aplicación los permisos para que esta pueda solicitar para acceder a muchos componentes del teléfono, ya sea el WiFi, las llamadas, los contactos, entre otros ya que esto es algo delicado, por ello es importante vigilar cuáles pide cada aplicación. Para el caso de un juego, si este llega a pedir acceso a los contactos puede ser normal porque querrá saber qué amigos juegan, pero si una app de linterna los pide es algo bastante sospechoso. Es importarte controlar y averiguar para qué se utilizan, precisamente por eso en Google Play se tiene la opción de 'Ver Permisos', para ello se debe ir a Ajustes de Google, aplicaciones activadas y allí seleccionar esta opción.

- Conexiones WiFi: Las conexiones WiFi son un canal muy común utilizado por los ciberdelincuentes para robar la información, sobre todo cuando se tratan de redes públicas (aeropuertos, centros comerciales etc.) desactivar la conexión automática es una buena medida para empezar. ¿Cómo se hace? Fácil. Se debe ir a Ajustes, conexiones inalámbricas, redes, ajustes avanzados y desactivar la casilla de 'buscar redes siempre', es algo sencillo[28].

Como puede denotarse la coincidencia de recomendación de un par de expertos recae en el uso de aplicaciones seguras, a decir verdad, la puerta de entrada de un Ciberdelincuente se hace por medio de una aplicación sospechosa, que traducida en lo que ya se ha hablado en este documento no es más que un malware que se apodera silenciosamente del dispositivo y en un segundo plano extrae todo lo que se le permita extraer o que no haya sido asegurado que por lo general es todo.

[28] Tomado de la URL, https://elandroidelibre.elespanol.com/2014/12/10-sencillos-consejos-para-mejorar-la-seguridad-de-tu-android.html

7.3.3. APLICACIONES ELABORADAS POR EXPERTOS PARA PREVENCIÓN DE ATAQUES A DISPOSITIVOS ANDROID

Son varias las herramientas y aplicaciones utilizadas en seguridad informática móvil, algunas de ellas tienen gran utilidad a nivel corporativo, pero la verdad es que sea para una organización o para un usuario final, la seguridad de un dispositivo móvil siempre será una responsabilidad individual.

Es poco lo que se conoce en materia de recursos en seguridad de las comunicaciones empresariales en el territorio nacional, en esta materia, a veces por el desconocimiento o por el poco interés al respecto ya que la mayor inversión, se realiza a la planta tecnológica computacional como ya se mencionó y esto es común en las empresas y en las personas. Para el presente caso se toma como herramienta de interés la encriptación de comunicaciones móviles tipo PKI que se sugiere serán de interés y gran importancia dentro de una compañía o para cualquier usuario final.

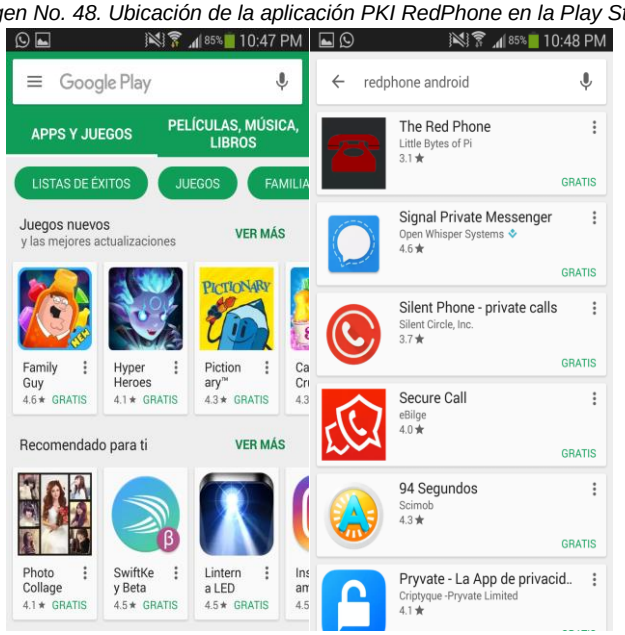
Una aplicación que usa herramientas de encriptación es una aplicación móvil denominada RedPhone; esta es una aplicación gratuita disponible para dispositivos con sistema operativo Android que funciona como cualquier otra aplicación, pero en la cual se demanda que tanto el emisor como el receptor para poder realizar una llamada telefónica, deben ambos tener la aplicación instalada y configurada en sus terminales móviles, esto implica que para el caso de una compañía se propende que en la adquisición de sus teléfonos móviles corporativos se realice la instalación de esta aplicación y sea de estricto y obligatorio uso para todos los funcionarios de la compañía, o se sugiere que para un usuario final no corporativo piense en la importancia de instalar esta aplicación para blindar sus llamadas telefónicas.

RedPhone funciona encriptando las comunicaciones entre los terminales, es decir una llamada telefónica es convertida en un texto cifrado el cual se transporta como un dato por medio de la red celular y llega a la otra terminal y la aplicación del destinatario se encarga de des encriptarla para conocer el mensaje enviado; esto ocurre de manera transparente para los usuarios de la aplicación quienes realizan la llamada de manera normal solo que utilizando una aplicación diferente a la del teléfono. Esta aplicación ofrece una protección o blindaje para todas las comunicaciones inalámbricas corporativas ya que no solamente protege las conversaciones que se realizan por la aplicación si no que impide que cualquier tipo de intrusión pueda afectar la red corporativa; es bien sabido que por medio de BTS falsas es posible interceptar las comunicaciones de un dispositivo móvil y lograr tener acceso no solo a la información de fábrica del aparato sino también a toda la

información que tenga almacenada en sus memorias.

Ahora, a continuación, se muestra de manera gráfica el paso a paso para mostrar la manera en que se debe instalar y configurar la aplicación; inicialmente se debe ir a la Play Store y buscarla por el nombre y luego continuar los pasos descritos en las imágenes 48 a 54.

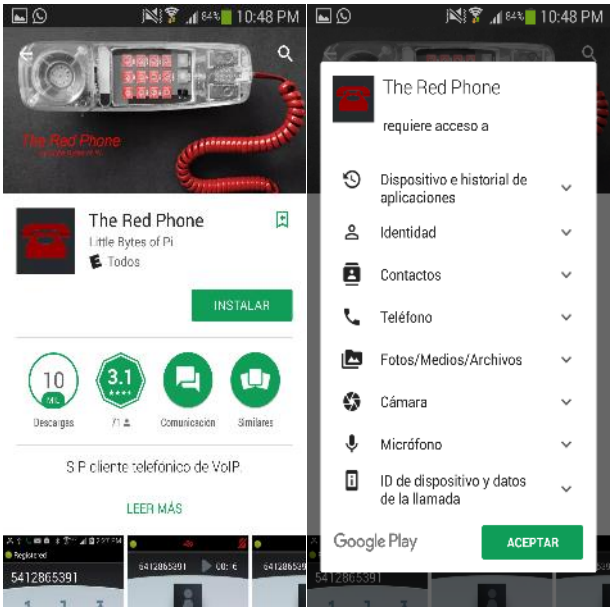
Imagen No. 48. Ubicación de la aplicación PKI RedPhone en la Play Store.



Fuente: Celular del autor

Como se muestra en la figura 48, inicialmente se hace la ubicación de la aplicación en la tienda de Google o Play Store, para identificar que corresponda a la aplicación que aquí se sugiere es decir The Red Phone.

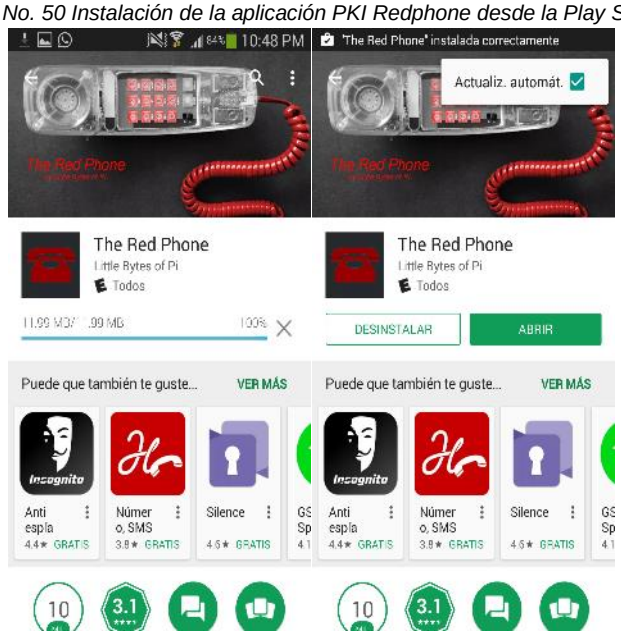
Imagen No. 49 Instalación de la aplicación PKI Redphone desde la Play Store.



Fuente: Celular del autor

Al dar click en la aplicación se despliega el acceso a los cuales podrá tener la aplicación en el dispositivo, a los cuales se les dará la aceptación ya que la misma trabajará en segundo plano a efectos de brindar una protección en la utilidad que dispone, tal y como se muestra en la imagen 49.

Imagen No. 50 Instalación de la aplicación PKI Redphone desde la Play Store.



Fuente: Celular del autor

Cómo se observa en la anterior imagen el tamaño de la aplicación instalada en el

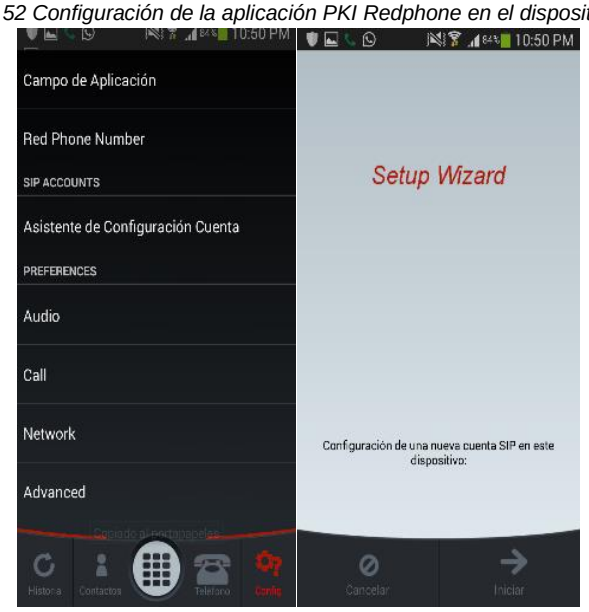
dispositivo es de 11.29 MB y una vez instalada se ubica en el sistema de aplicaciones del S.O., Android.

Imagen No. 51 Aplicación PKI Redphone correctamente instalada en el dispositivo móvil.

Fuente: Celular del autor

Cuando la aplicación queda finalmente instalada se crea un acceso directo o ícono en el escritorio del dispositivo móvil cómo se observa en la figura 51, y al dar click se abre la aplicación mostrando la apariencia de un teclado telefónico.

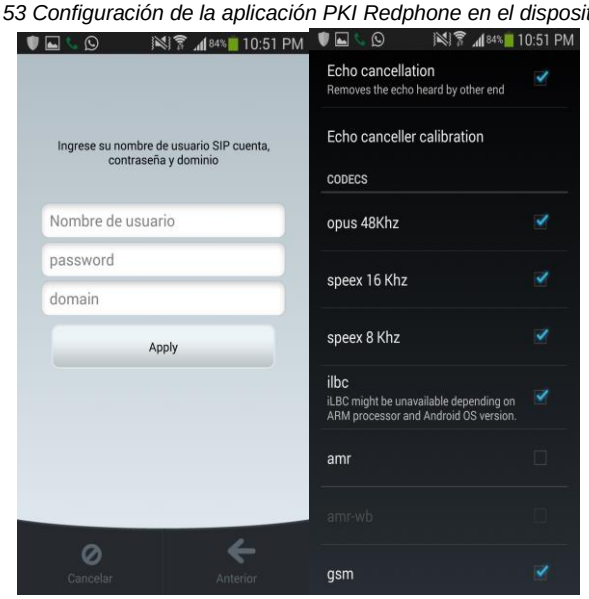
Imagen No. 52 Configuración de la aplicación PKI Redphone en el dispositivo móvil.



Fuente: Celular del autor

Posteriormente se hace la configuración directamente desde el menú de configuración como se observa en la imagen 24 desde donde se le dan los parámetros de uso y si se desea se le ingresan los datos para activación de cuenta tipo SIP como se observa en la imagen 53.

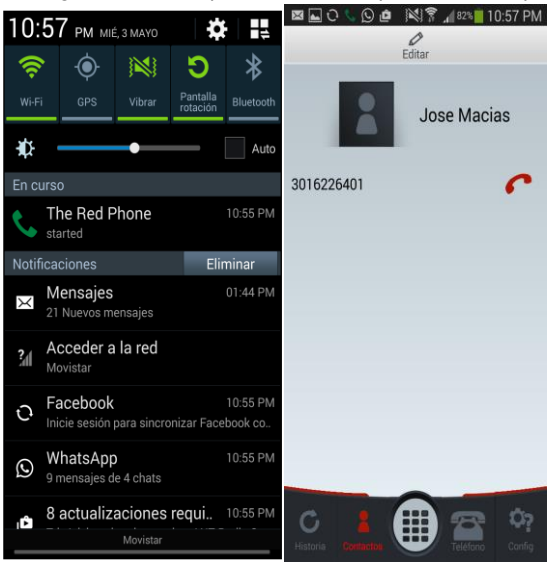
Imagen No. 53 Configuración de la aplicación PKI Redphone en el dispositivo móvil.



Fuente: Celular del autor

Desde el menú de configuración se observa el tipo de llamada, la velocidad y otros parámetros técnicos que tiene para establecer comunicación.

Imagen No. 54 Configuración de la aplicación PKI Redphone en el dispositivo móvil



Fuente: Celular del autor

Finalmente, cuando la aplicación queda correctamente instalada se observa en el menú de notificaciones del Smartphone, que la aplicación está en modo Started es decir activa; esto se puede observar en la imagen 54. De otra parte, esta aplicación permite agregar contactos para ser guardados en el celular entre otras funciones de tipo telefónico que son para comunicación.

Como ya se mencionó una de las grandes ventajas de esta aplicación es que mantiene el nivel de encriptación de las comunicaciones durante la transmisión brindando un gran nivel de seguridad de extremo a extremo.

8. CONCLUSIONES

Con el desarrollo del presente estudio monográfico se ha podido dar un acercamiento de manera implícita a la definición o concepto de lo que significa la seguridad informática móvil, orientada a aquellos dispositivos con sistema operativo Android obviamente, y esta definición se logra gracias a la necesidad de involucrar a estos terminales dentro de todo el campo de la Ciberseguridad, no por parte de los expertos solamente ya que ciertamente desde hace mucho tiempo se ha trabajado en pro de la protección informática móvil por parte de los expertos, si no también y sobre todo por parte de los usuarios finales que en últimas son las víctimas o beneficiarios dentro del mundo digital a quienes se les comparte la importancia de crear una cultura de protección de los datos para todos sus dispositivos móviles que utilicen un sistema operativo Android.

Al desarrollar el presente estudio monográfico se ha podido encontrar que las técnicas y metodologías de protección de los datos presentes en dispositivos móviles, cuando son aplicadas de manera correcta y sobre todo oportuna, proporcionan un verdadero nivel de seguridad que si bien no es garantía permanente de inmunidad ante cualquier ataque malicioso, por lo menos cierra el espectro y aumenta el porcentaje de probabilidad que una amenaza cualquiera fracase en un dispositivo con S.O. Android; razón por la cual es necesario conocer las técnicas y metodologías de protección y hacerlas públicas a un gran número de usuarios del sistema operativo Android, en primer lugar porque ésta es la plataforma tecnológica más utilizada en terminales móviles en el mundo y en segundo lugar porque de esta manera se extiende la cultura de la seguridad informática móvil.

Se ha podido corroborar que la mayoría de las personas y usuarios de dispositivos con S.O. Android e incluso de cualquier otro tipo de sistema operativo móvil, son susceptibles de ser engañados por medio de publicidad engañosa, páginas falsas, aplicaciones de origen desconocido y enlaces de dudosa reputación y esto sucede gracias a una característica humana denominada, la curiosidad, la cual conduce a las personas a querer saber que hay detrás de una publicidad que por lo general contiene la palabra gratis. Esta característica humana es un punto a favor que los Ciberdelincuentes han aprovechado muy bien desde hace mucho tiempo logrando casi inhibir el raciocinio de casi cualquier usuario que por lo general pudiera ser un comprador con tendencia compulsiva pero que efectivamente no ha adoptado una cultura de seguridad informática móvil.

Las herramientas de seguridad móvil como las aplicaciones que se instalan para asegurar la información revierten mucha importancia para la protección de la información en dispositivos con S.O. Android, por lo cual el desconocer la funcionalidad y aplicabilidad de éstas es un riesgo que a futuro se puede convertir en un fallo de seguridad. Aplicaciones como Latch o Red Phone ya mencionadas en el presente documento u otras como CONAN, son apps que le imprimen si ningún desgaste, gran protección a todos los datos que viajan o se guardan en el dispositivo.

Por mencionar alguna situación, cuando un criminal tiene oportunidad de hurtarse un aparato que por descuido está desbloqueado, para un usuario que ha instalado Latch muy probablemente no le surgirá más preocupación que el costo del mismo ya que aunque el dispositivo se encuentra sin patrón de seguridad, Latch hace que para ingresar a cualquier aplicación o a todos los íconos del dispositivo si así se desea, primero se deba autenticar con doble código en algunos casos para acceder a la App, algo que es muy útil para aquellos que acostumbran a realizar transacciones monetarias con aplicaciones móviles.

9. DIVULGACIÓN

El desarrollo del presente proyecto está estipulado para que sea publicado por parte de la universidad en el repositorio institucional para su consulta por parte de la comunidad académica, tanto de la UNAD como de aquellas personas y entidades que por medio de este convenio tengan acceso a esta información académica.

BIBLIOGRAFÍA

INFOLAFT, Anticorrupción, Fraude y LA/FT. Lo que se debe saber sobre el cibercrimen en Colombia [En línea], Publicado el 10 de Noviembre de 2014 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: http://www.infolaft.com/es/art%C3%ADculo/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia.

EL TIEMPO, Economía y Negocios. Ciberdelitos valen $917 mil millones, según estudio [En línea], Publicado el 19 de Septiembre de 2014 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: http://www.eltiempo.com/economia/indicadores/ciberdelitos-en-colombia-4-de-cada-10-usuarios-de-internet-son-victimas/14561876.

CONDE, German. Cómo descifrar claves WiFi Fácilmente [En línea], Publicado el 10 de Octubre de 2014 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: https://www.youtube.com/watch?v=dLyLgEpXmZI.

UDEAM REDALYC.ORG, Red de Revistas Científicas de América Latina y el Caribe España y Portugal. Virus Telefónicos [En línea], Publicado en Julio de 2006 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: http://www.redalyc.org/pdf/944/94403214.pdf.

RUEDA, Johan. Análisis Forense Digital en Dispositivos Móviles [En línea], Publicado el 28 de Agosto de 2014 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: http://revistas.ufpso.edu.co/index.php/rsemilleros/article/download/114/76.

JOHNSON, Kevin. BYOD: Cómo evaluar los nuevos dispositivos y sus riesgos de seguridad [En línea], Publicado el 28 de Febrero de 2014 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: http://searchdatacenter.techtarget.com/es/consejo/BYOD-Como-evaluar-los-nuevos-dispositivos-y-sus-riesgos-de-seguridad.

SCAMBRAY, Joel, Editorial McGraw-Hill. HACKERS 2 Secretos y soluciones para seguridad de redes [En línea], Publicado en Noviembre de 2001 [Revisado el 22 de Octubre de 2017]. Disponible en Internet: http://www.revistasic.com/revista47/pdf_47/SIC_47_bibliografia.PDF.

RENDON, Arturo. Documental Hackers [En línea], Publicado el 24 de Junio de 2008 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: https://www.youtube.com/watch?v=Xe7YWI0RI-M&feature=youtu.be.

MAHAPATRA, Lisa. Android Vs. iOS: What's The Most Popular Mobile Operating System In Your Country? [En línea], Publicado el 11 de Noviembre de 2013 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: http://www.ibtimes.com/android-vs-ios-whats-most-popular-mobile-operating-system-your-country-1464892.

GIRONES, Jesús Tomás. Editorial Marcombo ediciones técnicas. El gran libro de Android [En línea], Publicado en el año 2012 [Revisado el 22 de Octubre de 2017]. Disponible en Internet: https://books.google.es/books?id=TOP-BiaYYiQC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

TELEFONICA DIGITAL ESPAÑA, Latch. Página oficial de la aplicación [En línea], Publicada el 01 de Enero de 2017 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: https://latch.elevenpaths.com/www/index.html.

TANENBAUM, Andrew S. Editorial Pearson Educación. Sistemas operativos modernos [En línea], Publicado en el año 2003 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: https://books.google.es/books?hl=es&lr=&id=g88A4rxPH3wC&oi=fnd&pg=PR22&dq=sistemas+operativos&ots=yuTAOCkO1P&sig=MS7-__PFKwIgOYLzItqAddWDWNg#v=onepage&q=sistemas%20operativos&f=false.

NIETO GONZALEZ, Alejandro. ¿Qué es Android? [En línea], Publicado el 8 de Febrero de 2011 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: https://www.xatakandroid.com/sistema-operativo/que-es-android.

AGUILAR, Rusia. Cibercrimen [En línea], Publicado el 28 de Diciembre de 2011 [Revisado el 31 de Mayo de 2017]. Disponible en Internet: http://rusia-aguilar.blogspot.com.co/2011/12/cibercrimen.html.

ANEXOS

ANEXO A: RESUMEN ANALÍTICO RAE

TITULO	RESUMEN ANALITICO RAE ESTUDIO MONOGRAFICO ACERCA DEL CIBERCRIMEN EN DISPOSITIVOS MÓVILES CON S.O. ANDROID
AUTOR	JOSE JAIR MACIAS CANO
PALABRAS CLAVES	Cibercrimen, Sistema Operativo, Malware, Metasploit, Hacker, Informática Forense, Android, Linux, Kali Linux, Código Malicioso, Red LAN, Dispositivo Móvil y Exploit.
DESCRIPCIÓN	El presente trabajo es un estudio de tipo monográfico en el cual se presenta de manera detallada un estudio práctico sobre los ataques que se pueden presentar a un dispositivo Android y de qué manera se puede evitar. Este estudio monográfico se realiza como opción de grado y así obtener el título de especialista en seguridad informática en la Universidad Nacional Abierta y a Distancia UNAD.
FUENTES BIBLIOGRÁFICAS	Enck, W., Octeau, D., McDaniel, P., y Chaudhuri, S. (2011, agosto). Un estudio de la seguridad de las aplicaciones de Android. En simposio seguridad USENIX (Vol. 2, p. 2). Archidona, M. I. (2010). Seguridad WIFI. Agresiones posibles (Doctoral dissertation). Guevara, R., & Flórez, G. (2015). Concentration of WiFi networks in central places–Study case in the center of Medellin city, Colombia Concentración de redes Wifi en sitios céntricos-Caso de estudio Centro de la ciudad de Medellín Colombia. Actas de Ingeniería, 1, 196-200. Rueda, J. S. R., & Bautista, D. R. (2014). ANÁLISIS FORENSE DIGITAL EN DISPOSITIVOS MÓVILES. Revista de Semilleros de Investigación, 1(1). Luna, J. S., & Martín, J. F. (2013). La gestión segura de la información en movilidad ante el fenómeno BYOD:¿ Bring Your Own Device= Bring Your Own Disaster. Revista SIC: Ciberseguridad, seguridad de la información y privacidad, 104, 65-73.

	Camero Martín, J. (2017). Integrando Latch y OpenWRT para el control de acceso. O'Gorman, J., Kearns, D., y Aharoni, M. (2011). Metasploit: guía del probador de penetración. Sin Almidón Press.
CONTENIDO	Se realizó un estudio monográfico acerca del cibercrimen en dispositivos móviles con sistema operativo Android esto permitió conocer y describir algunas técnicas y métodos utilizados por Ciberdelincuentes para infiltrarse en este tipo de dispositivos con lo cual se propende generar conciencia y prevención respecto de los ataques más frecuentes a estos aparatos. De qué manera; al identificar las metodologías y técnicas utilizadas en ataques a dispositivos móviles, se logra describir mediante informática forense algunos ataques realizados a dispositivos Android, y con una guía de técnicas recomendadas por expertos para evitar ser víctimas de ataques en dispositivos Android se socializa a la comunidad en general.
METODOLOGIA	El presente estudio monográfico fue realizado mediante una investigación de tipo científica en la cual se utilizaron algunos conceptos y herramientas de informática forense dentro de un contexto de seguridad informática móvil, para desarrollar de manera práctica las metodologías que llevaron a la elaboración de los resultados materializados en recomendaciones que pueden evitar a una persona ser víctima de un ciberataque a su dispositivo Android.
CONCLUSIONES	Con el desarrollo del presente estudio monográfico se ha podido dar un acercamiento de manera implícita a la definición o concepto de lo que significa la seguridad informática móvil, orientada a aquellos dispositivos con sistema operativo Android obviamente, y esta definición se logra gracias a la necesidad de involucrar a estos terminales dentro de todo el campo de la Ciberseguridad, no por parte de los expertos solamente ya que ciertamente desde hace mucho tiempo se ha trabajado en pro de la protección informática móvil por parte de los expertos, si no también y sobre todo por parte de los

	usuarios finales que en últimas son las víctimas o beneficiarios dentro del mundo digital a quienes se les comparte la importancia de crear una cultura de protección de los datos para todos sus dispositivos móviles que utilicen un sistema operativo Android. Al desarrollar el presente estudio monográfico se ha podido encontrar que las técnicas y metodologías de protección de los datos presentes en dispositivos móviles, cuando son aplicadas de manera correcta y sobre todo oportuna, proporcionan un verdadero nivel de seguridad que si bien no es garantía permanente de inmunidad ante cualquier ataque malicioso, por lo menos cierra el espectro y aumenta el porcentaje de probabilidad que una amenaza cualquiera fracase en un dispositivo con S.O. Android; razón por la cual es necesario conocer las técnicas y metodologías de protección y hacerlas públicas a un gran número de usuarios del sistema operativo Android, en primer lugar porque ésta es la plataforma tecnológica más utilizada en terminales móviles en el mundo y en segundo lugar porque de esta manera se extiende la cultura de la seguridad informática móvil.
RECOMENDACIONES	El desarrollo del presente proyecto está estipulado para que sea publicado por parte de la universidad en el repositorio institucional para su consulta por parte de la comunidad académica, tanto de la UNAD como de aquellas personas y entidades que por medio de este convenio tengan acceso a esta información académica.
FECHA DE REALIZACION	28 DE MAYO DE 2017