VULNERABILIDADES MÁS IMPORTANTES EN PLATAFORMAS ANDROID

Leaño Ardila, Victor Hugo
Vl182a@yahoo.es
Universidad Piloto de Colombia

***Abstract*—Today technological advances have led us to seek mechanisms to access information quickly and timely for that reason so mobile devices have become the items most commonly used by people to consult email, shopping payments and other types of transactions. This so daily activity for users of the technology is exploited by ill-intentioned people who want to take advantage of the failures on used operating systems, this paper make an analysis of the most exploited vulnerabilities in the Android operating system one of the most used worldwide additional mind safety recommendations will be made to avoid becoming a victim of theft, modification or loss of data.**

***Keywords* — Android, vulnerability, security, mobile device.**

***Resumen*—En la actualidad los avances tecnológicos nos han llevado a buscar mecanismos de acceder a la información de manera rápida y oportuna por tal motivo los dispositivos móviles se han convertido en objetos más usados por las personas, para realizar consultas de correo electrónico, compras pagos y otros tipos de transacciones. Esta actividad tan cotidiana para los usuarios de la tecnología es aprovechada por personas mal intencionadas que quieren aprovecharse de las falencias en los sistemas operativos usados, este documento realizara un análisis de las vulnerabilidades más explotadas del sistema operativo Android uno de los más usados a nivel mundial además se realizaran recomendaciones de seguridad para evitar ser víctima de robo, modificación o perdida de información.**

***Palabras clave* --- Android, vulnerabilidad, seguridad, dispositivo móvil.**

I. INTRODUCCIÓN

Actualmente según cifras del Ministerio de tecnologías de la información y lascomunicaciones de Colombia (Mintic) en el segundo trimestre de 2016 se reporto un

total de 57.292.621 usuarios activos usando dispositivos móviles, en la figura [1] se observan la distribución usuarios de telefonía móvil según datos suministrados por los proveedores de redes lo cual indica que 8 de cada 10 personas tienen acceso a dispositivos móviles con conexión a internet.

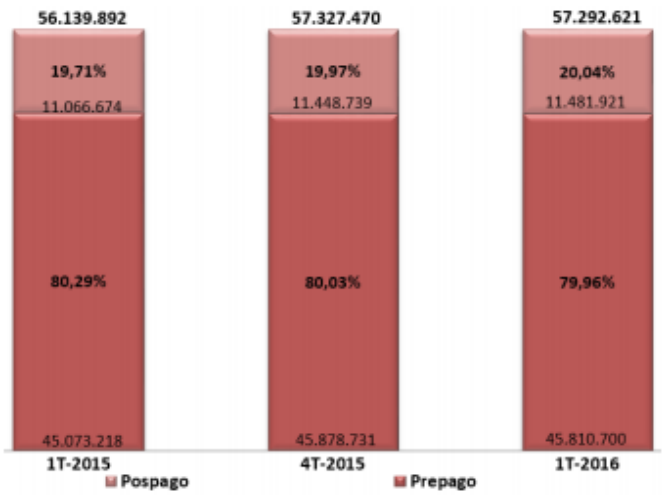


Figura 1.Abonados servicio telefonía móvil [1]

Según comscore en su reporte de Enero de 2016 los sistemas operativos más usados en dispositivos móviles a nivel mundial, Android tiene la participación más alta del mercado con 52.8% seguido por IOS con una participación del 43.2%.

Contextualizando el mercado de los dispositivos móviles, eneste documento se analizara el sistema operativo Android. Al ser una plataforma de código libre (Open-Source) permite la construcción de aplicaciones de forma muy sencilla y facilita el desarrollo de códigos

poco seguros o con fines maliciosos haciendo que los usuarios sean sensibles a que su información sea vulnerada. Existen muchas recomendaciones para disminuir las vulnerabilidades de seguridad presentes en Android, se realizara un análisis de las vulnerabilidades más explotadas, adicionalmente se darán recomendaciones que permitan mitigar los riesgos, abarcando desde la ingeniería social hasta aplicativos que permitan salvaguardar la información.

TABLA 1
Top 3 plataformas de dispositivos móviles con mayor participación en el mercado [9]

	Share (%) of Smartphone Subscribers		
	Oct-15	Jan-16	Point Change
Total Smartphone Subscribers	*100.0%*	*100.0%*	*N/A*
Android	52.9%	52.8%	-0.1
Apple	43.3%	43.6%	0.3
Microsoft	2.7%	2.7%	0.0

II. ESTRUCTURA ANDROID Y MODELO DE SEGURIDAD

El sistema operativo Android fue desarrollado sobre una modificación del kernel Linux, la estructura de este sistema operativo está conformada por 5 capas:

1. Capa de Aplicaciones: contiene aplicaciones por defecto y las descargas por el usuario.
2. Framework de Aplicaciones:contiene el conjunto de herramientas de para desarrollo de cualquier aplicación.
3. Librerías: librerías usadas por Android escritas en C++(Libc,Surface,Manager,OpenGLISISL,Medialibraries,FreeType).
4. Tiempo de Ejecución Android:esta al mismo nivel de las librerías pero en tiempo de ejecución, contiene clases java y la maquina visual Dalvik.
5. Kernel de Linux: es una capa de abstracción para el hardware disponible en los dispositivos móviles. Contiene los controladores necesarios para que cualquier componente de hardware pueda ser utilizado.

Esta arquitectura indica que las capas inferiores son más susceptibles a tener más vulnerabilidades y como su estructura es jerárquica los niveles superiores sustentan gran aparte de su seguridad en las capas inferiores.

Android en su arquitectura contempla un ciclo de desarrollo enfocado a fortalecer las debilidades en seguridad de los dispositivos móviles, este ciclo contempla las siguientes etapas:

1) Revisión del Diseño.
2) Pentest.
3) Revisión del código.
4) Respuesta a incidentes.

Adicionalmente se contemplan elementos de seguridad pre instalados en el sistema operativo en cada nivel de su estructura como:

- **APIs Protegidas:**se requiere de permisos especiales para acceder a información personal como micrófono, cámara, GPS, metadatos.
- **Administración Dispositivos:**administra el dispositivo haciendo uso de API permitiendo configurar borrados remotos y restauración de sistema.
- **Seguridad administración memoria:**administra de manera eficiente la memoria seleccionada de forma aleatoria sectores importantes prevenir desbordamiento de buffer y ejecución de código en Pila.
- **Permisos "Root**": algunas aplicaciones principales y el kernel se ejecutan con permisos root, este perfil puede modificar el sistema operativo y aplicaciones. Al momento de que el usuario otorga privilegios de root aumenta el riesgo de ejecución de códigos maliciosos.
- **SandBox:**cada aplicación instalada en el dispositivo debe pasar por un proceso de identificación ya que el sistema operativo posee políticas de acceso dependiendo del origen y funcionalidad de la aplicación, en estos casos el usuario tiene total responsabilidad de autorizar o no el acceso al sistema.
- **Modo Seguro:**permite al usuario usar las funciones del sistema operativo en una partición que contiene las aplicaciones básicas del sistema permitiendo el uso del dispositivo en un escenario protegido de aplicaciones no nativas.
- **Firma Aplicaciones:**permite identificar el autor del código en cada aplicación.
- **Kernel de Linux:**se basa en permisos y restricción de acceso aislando a procesos del sistema elimina partes innecesarias que representan riesgo para el sistema.
- **Permisos Sistema Archivo:**protege los archivos asegurando que usuarios no tengan ningún tipo de acceso ya sea de escritura o lectura de otro usuario ya

que las aplicaciones se ejecutan únicamente con el usuario local.

- **Cifrado:** Android proporciona cifrado completo de ficheros, las datos son cifrados en el kernel usando un contraseña derivada de la clave del usuario se combina con una sal y un hash al momento del cifrado así minimizar el éxito de un ataque de fuerza bruta con datos de diccionario. Adicionalmente cuenta con políticas de complejidad en contraseñas que son ejecutadas por el sistema operativo.
- **Contraseñas:**el usuario puede definir una contraseña antes de acceder al sistema operativo la cual está cifrada esto con el fin de evitar accesos no autorizados.

III. VULNERABILIDADES MÁS IMPORTANTES EN 2016 PARA PLATAFORMAS ANDROID.

Aunque Android y su equipo de diseño y desarrollo contemplan la seguridad y se han hecho avances en el mejoramiento de la protección de su sistema existen puntos débiles, estas vulnerabilidades se incrementan gradualmente según CVE Details Google Android que contiene información registrada sobre vulnerabilidades de seguridad se evidencia que al transcurrir de los años el número de vulnerabilidades va en aumento ya que en 2015 se registraron 131 y a lo corrido de 2016 van 257 esto representa un incremento del 49.9 % [2],la principal vulnerabilidad explotada hace referencia a escalar privilegios, seguido por denegación de servicio[3].

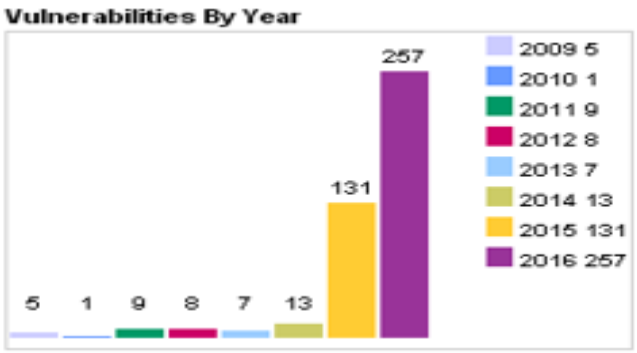


Figura 2. Vulnerabilidades documentadas para plataformas Android,cvedetails.[2]

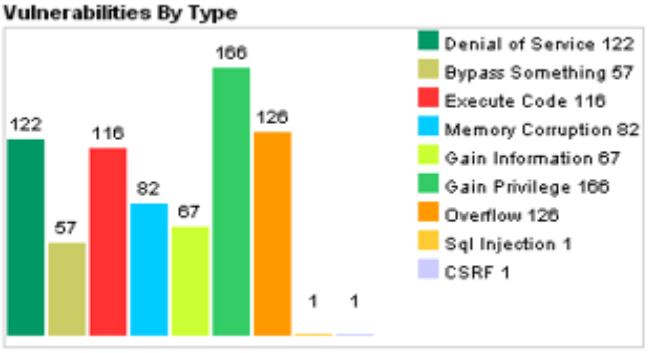


Figura3.Escala de vulnerabilidades más explotadas, cvedetails[2]

a.Vulnerabilidad Stagefridht-CVE-2015-29:vulnerabilidad fue reportada en 2015, los dispositivos Android contienen una carpeta "Stagefright" en la cual están alojados los archivos multimedia para su visualización y reproducción, el exploit inicia con él envió de un mensaje de texto alterado con código malicioso este malware se ejecuta en el sistema haciendo un llamado a la librería Stagefright tomando el control del dispositivo de manera remota accediendo a toda la información personal , todo esto sin intervención alguna de la víctima. Actualmente y a pesar de las últimas versiones de Android que contemplaron la mitigación de esta vulnerabilidad la empresa israelí Northbit creó un método de explotación denominado "Metaphor" que funciona en las versiones Android 2.2 a 5.1.

En la tabla [2] se realiza el análisis de la vulnerabilidadStagefrightCVE-2015-3829según CVE Details, en la cual se detalla cómo se identifica el nivel de criticidad en una escala de 1 a 10 donde 1 es un riesgo mínimo y 10 es un riesgo crítico.

TABLA 2

Vulnerabilidad Stagefright CVE-2015-3829. [2].

Impacto	Descripción
Confidencialidad	Completa-Divulga todos los archivos a los que tiene acceso.
Integridad	Completa-Perdida completa de la protección del sistema.
Disponibilidad	Completa-Desconexión total del recurso.
Complejidad de acceso	Baja- Se requiere muy poco conocimiento para explotar.
Autenticación	No requiere.

b.Vulnerabilidad CVE-2016-0728: vulnerabilidad fue reportada en 2016 haciendo uso de la función

join_session_keyring / llaves / process_keys.c permitiendo al usuario atacante tener privilegios de acceso root convirtiéndose en administrador, con lo cual puede sobrescribir códigos nativos de Android logrando acceder a claves de cifrado y datos sensibles también se puede causar una denegación de servicio así lograr indisponibilidad total del sistema operativo.En la tabla [3] se realiza el análisis de la vulnerabilidad StagefrightCVE-2016-0728según CVE Details.

TABLA 3
Vulnerabilidad CVE-2016-0728.[2].

Impacto	Descripción
Confidencialidad	Completa-Divulga todos los archivos a los que tiene acceso.
Integridad	Completa-Perdida completa de la protección del sistema.
Disponibilidad	Completa-El atacante puede hacer que el recurso totalmente disponible.
Complejidad de acceso	Baja- Se requiere muy poco conocimiento para explotar.
Autenticación	No requiere.

c.Vulnerabilidad CVE-2016-0822 Mediate:vulnerabilidad reportada en 2016 y consiste en una puerta trasera creada por los desarrolladores de los chips Mediatek la cual al ser explotada por los hackers permite un acceso total al software nativo del sistema operativo con lo cual se puede sobrescribir logrando acceder a claves de cifrado, datos sensibles y total control del dispositivo, esta falla para ser explotada requiere un alto conocimiento del código fuente por lo tanto es muy complejo de realizar.
En la tabla [4] se realiza el análisis de la vulnerabilidad StagefrightCVE-2016-0822 segúnCVE Details.

TABLA 4
VulnerabilidadCVE-2016-0822.[2].

Impacto	Descripción
Confidencialidad	Completa-Divulga todos los archivos a los que tiene acceso.
Integridad	Completa-Perdida completa de la protección del sistema.
Disponibilidad	Completa-El atacante puede hacer que el recurso totalmente disponible.
Complejidad de acceso	Alta- Se requiere una serie de condiciones especiales para explotar el recurso.
Autenticación	No requiere.

c.Vulnerabilidad CVE 2016-0801: vulnerabilidad reportada en 2016, es de las fallas más explotadas se basa en él envió de paquetes de control inalámbrico a través de redes wifi, estos paquetes son modificados para a corromper la memoria del kernel permitiendo la ejecución y sobrescribir código así el atacante tiene acceso a la información sensible del usuario víctima, el hacker solo puede ejecutar el ataque si la victima está conectada a la misma red.En la tabla [5] se realiza el análisis de la vulnerabilidad StagefrightCVE 2016-0801segúnCVE Details.

TABLA 5
VulnerabilidadCVE 2016-0801. [2].

Impacto	Descripción
Confidencialidad	Completa-Divulga todos los archivos a los que tiene acceso.
Integridad	Completa-Perdida completa de la protección del sistema.
Disponibilidad	Completa-El atacante puede hacer que el recurso totalmente disponible.
Complejidad de acceso	Baja- Se requiere muy poca habilidad para explotar el recurso.
Autenticación	No requiere.

IV. FALENCIAS DE SEGURIDAD ANDROID

Según el análisis realizado a las vulnerabilidades de Android se pueden identificar fallas en el diseño lógico del sistema entre las que podemos numerar las siguientes:

- Al ser una herramienta de código abierto permite la masificación de los usuarios lo cual hace que sea usado por más personas y el interés de los hackers aumente.
- Como las aplicaciones son instaladas con autorización del usuario es complejo identificar malware por lo general los ataques son identificados cuando ya han causado daño.
- Aunque Android tiene un mecanismo de seguridad sanbox que no contempla regular la comunicación entre aplicaciones por lo que apps con pocos privilegios pueden aprovechar a otras con mayores privilegios y materializar un ataque.
- Fragmentación como todos los dispositivos funcionan con versiones diferentes lo parches de seguridad no son lanzados por el fabricante puesto que se corre el riesgo de incompatibilidad y por ende interrumpir la disponibilidad del sistema operativo.

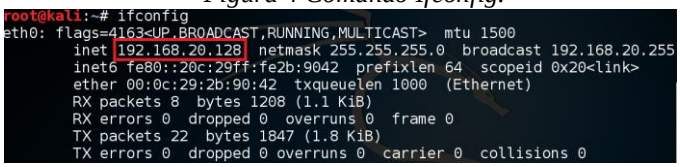
- Filtración de apps maliciosas en los repositorios de google, malware que es descargado de la apps store oficial.
- Baja restricción de privilegios para instalar aplicaciones, el usuario tiene total libertad de otorgar privilegios en las aplicaciones que desee utilizar lo cual se convierte en un potencial riesgo ya que sin saberlo pude estar instalando software malicioso.

V. EXPLOTACIÓN VULNERABILIDAD ANDROID

Para este caso práctico usaremos la herramienta metasploit la cual sirve para ejecutar pentesten equipos remotos, el ataque consistirá en tener acceso a un dispositivo móvil por medio de una app infectada que nos permita tener privilegios sobre la víctima y poner en riesgo la integridad, confidencialidad y disponibilidad de la información alojada en el dispositivo.

Para dar inicio la explotación usaremos la máquina virtual kali Linux. Identificamos por medio del comando ifconfig la dirección iplocal para este caso es la 192.168.20.128. [4].

Figura 4 Comando Ifconfig.



Fuente El Autor

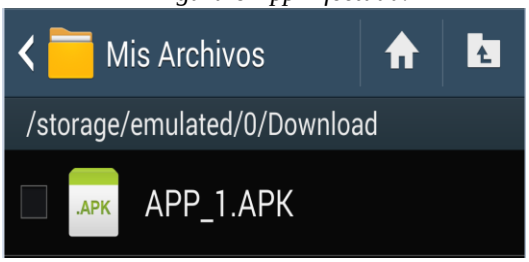
El siguiente paso es crear un .APK infectada la cual funcionara como un backdoor para Android, es decir una puerta trasera, esta app mapeara la dirección ip y el puerto de la maquina atacante a la cual se conectara la víctima, cuando se ejecute e instale la .APK así nos permitirá el total acceso al dispositivo, con el uso del comando msfvenom crearemos la aplicación infectada asignaremos la dirección ip local 192.168.20.128 y el puerto de escucha No 8888, nombraremos la .APK APP_1.APK [5].

Figura 5 comando msfvenom para crear nuestra .APK infectada.

Fuente El Autor

Procedemos a descargar e instalar aplicación creada anteriormente. [6]

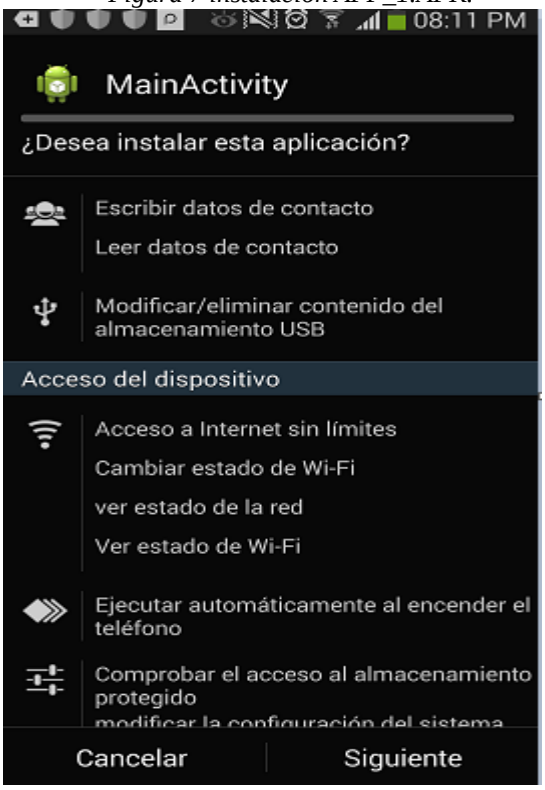
Figura 6 App infectada.



Fuente El Autor

Para este paso ejecutamos la app infectada y notamos que como usuarios tenemos total libertad de otorgar los privilegios que consideremos necesarios para que la aplicación se ejecute [7].

Figura 7 instalación APP_1.APK.



Fuente El Autor

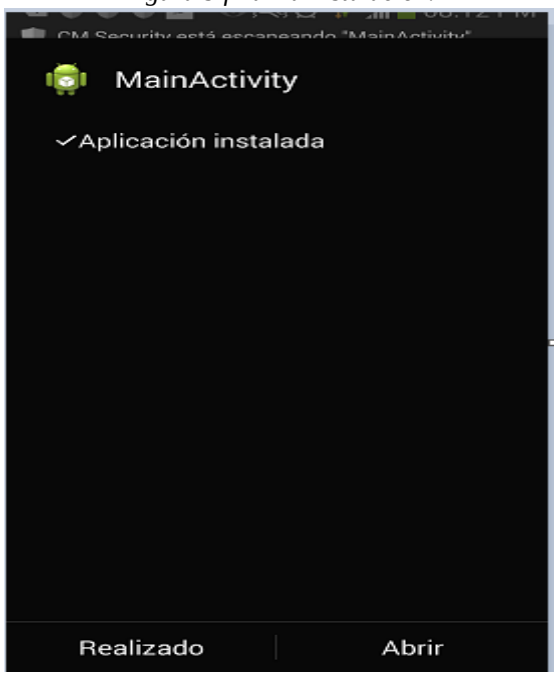
Otorgamos total acceso y privilegios a la aplicación instalada [8].

Figura 8 se le otorga todos privilegios a nuestra app.

Fuente El Autor

Finalizamos la instalación de nuestra aplicación [9].

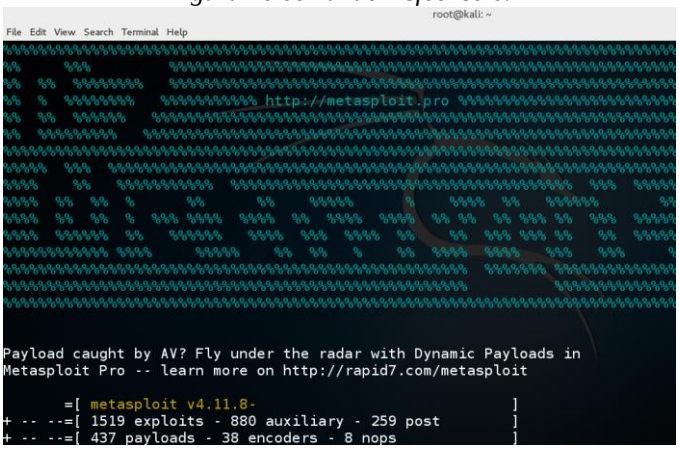
Figura 9 finaliza instalación.



Fuente El Autor.

Ahora que la víctima ya tiene la app modificada instalada es hora de hacer la explotación del backdoor, usamos la terminal de kali Linux y por medio del comando mfsconsole ejecutamos metasploit [10].

Figura 10 comando msfconsole.



Fuente El Autor

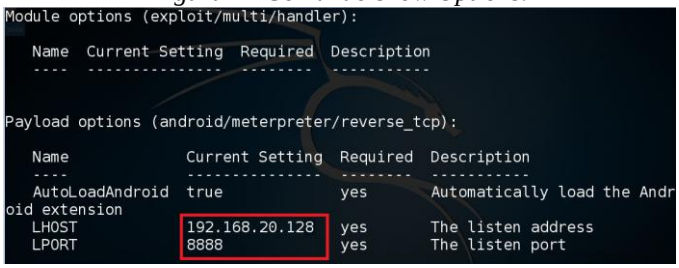
Una vez iniciadomsfconsole hacemos uso del comando multi/handler el cual cumple la función de conectar, dependiendo del reverse payload que quedara a la escucha para iniciar la conexión contra el host víctima, se determina la ip local 192.168.20.128y el puerto de escucha para este caso se seleccionó el puerto No 8888 [11].

Figura 11 comando multi/handler.

Fuente El Autor

Se verifica la configuración de la ip y el puerto de escucha para efectuar el ataque con el comando show options [12].

Figura 12 Comando show Options.



Fuente El Autor

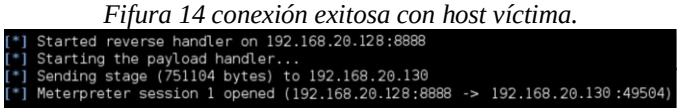
El siguiente paso es realizar la explotación por medio del comando exploit, ahora el handler quedara en espera de recibir la conexión.exitosa [13].

Figura 13 comando exploit.

Fuente El Autor

Como estamos a la espera de un reverse Shell, en el momento que se envié el payload hacia el host víctima, nuestro handler recibirá una conexión exitosa y lograremos un Shell de meterpreter [14].

Fifura 14 conexión exitosa con host víctima.



Fuente El Autor

Es este paso ya estamos conectados por medio de una sesión de meterpreter con la víctima y tenemos todo el acceso a la información que se desee acceder por ejemplo usando los comandos tendremos a la mano todo tipo de información confidencial de nuestra víctima como los siguientes:

- **record_mic:**por medio de este comando se enciende el micrófono del dispositivo móvil atacado y se iniciara una grabación de audio.
- **Webcam_snap:**este comando permite encender la cámara y tomar una foto instantánea.
- **Webcam_stream:**este comando permite encender la cámara de video y realizar una grabación en tiempo real.
- **dump_contacts:**este comando permite listar los contactos guardados en el dispositivo móvil.
- **dump_sms:**este comando permite listar y acceder a todos los mensajes de texto alojados en la memoria del dispositivo móvil.
- **geolocalizar:**este comando permite identificar con exactitud latitud y longitud geográfica de la ipatacada.

VI. RECOMENDACIONES DE SEGURIDAD PARA DISPOSITIVOS MÓVILES

Para evitar ser víctima de ataques que conlleven a la perdida sustancial o total de la información es importante que los usuarios tengan en cuenta las siguientes recomendaciones sobre el uso responsable de sus datos:

- Documentarse bien sobre los permisos necesarios que requieren las aplicaciones a ser instaladas.
- Instalar aplicaciones de las apps store oficiales para el caso de Android Google Play.
- Instalar parches de seguridad y actualizaciones lanzadas al mercado por el fabricante.
- Si se tienen dudas sobre la procedencia de una aplicación es recomendable no instalarla hasta documentarse adecuadamente.
- Instalar Anti Malware que proteja el dispositivo de virus existentes en la red, algunos recomendados son – Eset Mobile Securiyt – NQ Mobile Security – Norton Antivirus - .Karpersky.
- Para proteger el acceso crear un bloqueo de pantalla, si es posible complemente con una contraseñaalfanumérica que contenga caracteresespeciales con ello crear una autenticación de dos factores.
- Instalar aplicaciones que permitan restringir el acceso a las configuraciones del sistema adicionalmente a aplicaciones empresariales instaladas por defecto algunas aplicaciones pueden ser SecureAuth y PhoneFactor.
- Evite compartir la conexión a internet ya que esto es una puerta abierta para acceder a la información de su dispositivo.

VII. CONCLUSIONES

Según lo expuesto en este artículo se evidencio que el crecimiento de usuarios con dispositivos móviles está aumentando exponencialmente, además que la plataforma más asequible por ser de código abierto a nivel mundial es Android por ende se convierte en el blanco predilecto de los hackers que mejoran sus estrategias para robar información, como se demostró el aumento en vulnerabilidades explotadas y documentadas de 2015 a 2016 presento un incremento del 49.9% lo cual prende las alarmas de los fabricantes que se esfuerzan por mejorar su arquitectura de seguridad y brindarle a sus clientes un producto fiable.

Analizando el contexto de las vulnerabilidades más explotas a lo corrido de 2016 evidenciamos que el eslabón más débil de la cadena es el usuario, ya que la falta de conocimiento en temas de seguridad hace que conceda accesos no debidos a aplicaciones mal intencionadas, además de no tener precauciones con sus datos personales y restringir el uso a herramientas del sistema.

Como se demostró en la explotación de la vulnerabilidad hay numerosas herramientas que sirven para realizar ethical hacking que nos permitan obtener un panorama más amplio del nivel de seguridad que tiene los

dispositivos móviles, pero hay que resaltar que el mal uso de estos recursos como metasploit puede causar daños o perdida de información poniendo en riesgo los pilares de la seguridad informática como los son la integridad, confidencialidad y disponibilidad.

Podemos concluir que la evolución tecnológica hace que los fabricantes mejoren sus productos pero siempre existirán vulnerabilidades que pondrán en riesgo nuestra información por lo tanto los usuarios somos responsables de tomar las medidas necesarias para hacer uso seguro y responsable de los datos que almacenamos el los dispositivos móviles.

REFERENCIAS

[1] Oficina asesora de planeación y estudios sectoriales, "Informe trimestral telefonía móvil Ministerio deTecnologías de la Información y las Comunicaciones de Colombia", Julio de 2016. Tomado:http://colombiatic.mintic.gov.co/602/w3-propertyvalue-715.html

[2] NationalVulnerabilityDatabase, "El repositorio de los Estados Unidos de América de información sobre vulnerabilidades" Junio de 2016. Tomado:http://www.cvedetails.com/

[3] Androidinterfaces and architetecture,"Arquitectura de Android diseño plataforma", Mayo de 2016. Tomado: HTTPS://source.android.com/devices/

[4] Historia de Android, "Evolución sistema operativo Android", Mayo de 2016. Tomado:https://www.android.com/intl/es19_mx/history/

[5] Enrique MP, "Post sobre las vulnerabilidades más explotadas en 2016 para plataforma Android". Febrero de 2016. Tomado:http://tabletzona.es/2016/02/18/las-vulnerabilidades-de-android-mas-importantes-en-2016/

[6] Kali Linux oficial documentación, "Uso y configuración de metasploitkalilinux". Enero de 2016. Tomado:http://es.docs.kali.org/general-use-es/iniciando-el-metasploit-framework

[7] SebastianBortink, "Herramientas para realizar pruebas de penetración". Julio de 2013. Tomado:http://revista.seguridad.unam.mx/numero-18/pruebas-de-penetraci%C3%B3n-para-principiantes-5-herramientas-para-empezar

[8] Cyber Security information, "Portal con recomendaciones de seguridad para dispositivos móviles".Agosto de 2016. Tomado: http://www.cybersecurity.hk/en/safety-mobile-android.php

[9] The Global Mobile Report, "Reporte global de participación en el mercado de plataformas para dispositivos móviles", Enero de 2016. Tomado:http://www.comscore.com/Insights