GENERACIÓN DE UN PROCEDIMIENTO PARA REALIZAR PRUEBAS DE PENTEST EN REDES INALÁMBRICA UTILIZANDO DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID, MEDIANTE HERRAMIENTAS DE SOFTWARE LIBRE

NELSON FABIO PINZÓN BARRANTES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

GENERACIÓN DE UN PROCEDIMIENTO PARA REALIZAR PRUEBAS DE PENTEST EN REDES INALÁMBRICAS UTILIZANDO DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID, MEDIANTE HERRAMIENTAS DE SOFTWARE LIBRE

NELSON FABIO PINZÓN BARRANTES

Anteproyecto de la monografía para optar al título de
Especialista en Seguridad Informática

Director de Proyecto
Esp. Ing. JULIO ALBERTO VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

Nota de aceptación

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C, febrero de 2018

DEDICATORIA

A Dios

Por permitirme llegar a este momento de mi vida y tener la oportunidad de asumir este nuevo reto como es realizar este postgrado.

A mi Familia

Por todo el apoyo que recibo, por ser el soporte, el motor que cada día me impulsa para seguir creciendo y entregar lo mejor de mí.

A mis padres,

Por cada una de las cosas que me han enseñado y brindado, y por hacer la persona que soy y por todo el apoyo en las cosas que realizo.

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Ing. Julio Alberto Vargas, asesor del proyecto

A la Universidad Nacional abierta y a distancia –UNAD-

A todas aquellas personas que de una u otra forma han colaborado en la elaboración de este proyecto.

Tabla de contenido

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

pág.

GLOSARIO

ANDROID. Es un sistema operativo que se basa en Linux, diseñado para dispositivos móviles, como teléfonos, tabletas, computadoras entre otros, fue desarrollado inicialmente por Android Inc., una que firma que posteriormente fue adquirida por Google en 2005.[1]

DISPOSITIVO MÓVIL. Se considera un dispositivo móvil a un aparato con tamaño relativamente pequeño que cuenta con algunas características como: capacidad especial de procesamiento, conexión permanente o intermitente a una red, memoria limitada, diseñados para una función específica, pero con capacidad para realizar otras funciones adicionales, con operación y posesión individual. Una característica vital es el concepto de movilidad y su fácil uso durante su trasporte, así como la capacidad de conexión con redes inalámbricas y otros dispositivos.[2]

ETHICAL HACKING. Es una disciplina o rama que desprende de la seguridad informática, la cual se apoya en diferentes métodos, técnicas y herramientas con el fin de explorar y evidenciar vulnerabilidades conocidas y también desconocidas dentro de un sistema informático. Todo lo anterior para que el dueño del sistema pueda tomar las acciones preventivas para evitar ataques malintencionados.[3]

LINUX. Sistema operativo de software libre, no requiere licencia para instalarse en un equipo informático. Como es libre el código fuente está disponible para cualquier usuario tenga la posibilidad de analizarlo y modificarlo.[4]

PENTESTING. Se le llama pentesting o prueba de penetración a la práctica de atacar diferentes sistemas con el objetivo de hallar puntos vulnerables o fallas de seguridad, para poder prevenir que estas sean explotadas y así prevenir atacas externos e internos al sistema.[5]

RED INALÁMBRICA. Es una red compuesta por dos más dispositivos, que no necesita un medio físico para conectarse, las cuales se fundamentan en un enlace

---

[1]ESTHEFANY AND YERIKA. Definición Android. [En línea] mayo de 2012 [citado 15 de octubre de 2017] disponible en: http://tecnologiasandroid.blogspot.com.co/2012/05/definicion-android.html

[2]GUEVARA SORIANO,Anaid. Dispositivos móviles. [En línea] agosto de 2010 [citado 15 de octubre de 2017] disponible en:https://revista.seguridad.unam.mx/numero-07/dispositivos-moviles

[3]TECNOXXI, ¿Qué es ethical hacking? [En línea] noviembre de 2016 [citado 15 de octubre de 2017] disponible en:https://www.tecnoxxi.com/blog/seguridad-informatica/que-es-ethical-hacking/

[4]L TECNOLOGÍA, Definición de Linux [En línea]mayo de 2011 [citado 15 de octubre de 2017] disponible en: http://conceptodefinicion.de/linux/

[5]ESAÚ, A. ¿Qué es pentesting? [En línea]junio de 2012 [citado 15 de octubre de 2017] disponible en: https://openwebinars.net/blog/que-es-el-pentesting/

que usa ondas electromagnéticas, permitiendo a un usuario seguir conectado mientras realiza desplazamientos en un área geográfica determinada.[6]

SOFTWARE LIBRE. Un software o programa libre, es aquel que entrega la libertad al usuario de: ejecutar como quiera, copiar, distribuir, estudiar, modificar y mejorar el software, es de decir no está relacionado con que sea gratuito, sino que entrega libertad.[7]

VULNERABILIDAD. Se refiere a una debilidad presente en un sistema informático, con diferentes orígenes y que permite ejecutar un ataque a dicho sistema, que puede afectar la confidencialidad, integridad, disponibilidad o control de acceso del sistema.[8]

WPA/ WPA2. Por su sigla en inglés (Wifi Protected Acces), es un mecanismo de seguridad para redes inalámbricas, surgió como consecuencia de problemas de seguridad del mecanismo anterior de seguridad llamado WEP. Fue desarrollado por Wi-Fi Alliance, propietario de la marca Wi-FI.[9]

[6] ES.CCM.NET. Redes inalámbricas [En línea] julio de 2017 [citado 15 de octubre de 2017] disponible en: https://openwebinars.net/blog/que-es-el-pentesting/
[7] ARTEAGA MEJÍA, Luis Miguel. ¿Qué es software libre? [En línea] junio de 2011 [citado 15 de octubre de 2017] disponible en: https://www.gnu.org/philosophy/free-sw.es.html
[8] ALEGSA, Leandro. Definición de vulnerabilidad [En línea] diciembre de 2010 [citado 15 de octubre de 2017] disponible en: http://www.alegsa.com.ar/Dic/vulnerabilidad.php
[9] ALEGSA, Leandro. Definición de WPA [En línea] diciembre de 2010 [citado 15 de octubre de 2017] disponible en: http://www.alegsa.com.ar/Dic/wpa.php

INTRODUCCIÓN

La tecnología hace parte importante de las actividades que se desarrollan en los campos laborales y personales, y cada día esta cambia buscando la comodidad y facilidad para realizar acciones, un ejemplo de ello es la eliminación de cables en la conexión de dispositivos.

Es una realidad verídica el crecimiento del uso e implementación de toda clase de redes inalámbricas, en ámbitos corporativos, pequeñas empresas, y también en hogares, estas redes ofrecen una gran cantidad de ventajas en comparación a las tradicionales redes cableadas. Son fáciles de instalar, mayor cobertura, movilidad, facilidad para expandir, entre otras; debido a esto es que las redes inalámbricas han tomado un gran auge en la actualidad

No obstante, dichas ventajas presentan una contra que son los problemas de seguridad, aunque son conocidos, en ocasiones no se toman las precauciones necesarias por el personal que administra dichas redes. Está demostrado que las redes inalámbricas son inseguras de forma intrínseca y se requiere mayor atención para su aseguramiento[10]*.*

Todos estos descuidos o falencias hacen que las redes sean vulnerables y que estén expuestas a ataques de cualquier tipo, por lo anterior en este documento se plantea un procedimiento para poner en evidencia los posibles puntos vulnerables que existan en una red inalámbrica, y así permitir que los administradores de la misma adopten las medidas para optimizar la seguridad de dicha red. Es decir que se estaría minimizando los puntos vulnerables de las redes inalámbricas.

Por lo anterior en esta monografía se pretende generar un procedimiento para la elaboración de pentest en redes inalámbricas utilizando dispositivos móviles con sistema operativo Android y herramientas de software libre, lo que permitirá evidenciar las posibles vulnerabilidades que existan en este tipo de infraestructuras tecnológicas que hoy en día se ha masificado de manera exuberante.

Con este procedimiento es posible suministrar a los administradores de sistemas de las organizaciones, un paso a paso para ser aplicado dentro de sus empresas y de esta manera mitigar el riesgo a que está expuesta la red y así poder tener una infraestructura inalámbrica con alto grado de disponibilidad, haciendo así que la información que se trasporta a través de este tipo de canales sea confiable e integra.

[10] OPEN COURSE WARE. Teoría de la señal y comunicaciones móviles y digitales. [en línea]. Madrid (España): Universidad politécnica de Madrid, 2016 [en línea]. [citado mayo 5, 2017]. Disponible en internet: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

1. FORMULACIÓN DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

Debido a que el medio de propagación de una red inalámbrica se realiza por radiofrecuencia, la información esta sensible a ser vulnerada fácilmente a menos que se implementen sistemas de control para el acceso con los cuales se asegure la confidencialidad e integridad de la información.

El hecho de que no se requieran cables para conectar dispositivos, es la razón principal para la popularidad que tienen las redes inalámbricas, pero esta característica es a su vez también el mayor problema que presentan este tipo de redes si hablamos de seguridad. Cualquier dispositivo que este dentro de un rango de 100 metros de un punto de acceso, este podría conectarse a la red inalámbrica. Un ejemplo de ello se presenta cuando en un edificio hay varias redes inalámbricas de diferentes organizaciones, un determinado dispositivo tiene a su alcance o está en rango de cobertura de varias redes, este dispositivo podría llegar a conectarse a cualquiera de estas redes incluso estando fuera del edificio.
Aun un gran número de organizaciones y personas no conocen el impacto negativo que podría generar el hecho de tener puntos de acceso inalámbricos dentro de un sistema informático sin la seguridad adecuada. Es habitual encontrarse con redes que poseen puntos de acceso inalámbrico sin ningún tipo de seguridad y difundiendo fuera de las instalaciones físicas, por lo que cualquier dispositivo podría conectarse a la red desde el exterior, accediendo a la información del sistema, con posibilidad de tener utilizar internet sin costo, utilizando este red para realizar ataques a otras redes sin ser identificado después desconectarse, realizar hurto de información o aplicaciones, realizar ataques dentro de esta red, u otro tipo acciones negativas para la organización[11]

Actualmente el uso de dispositivos móviles es muy alto y cada vez son lanzados al mercado diferentes tipos de estos dispositivos con diferentes fines y usos, pero con algo en común, que todos permiten conectarse a las redes inalámbricas lo cual hace que se requiera mayor seguridad en las redes, por lo que se hace muy necesario que se detecten todos los puntos vulnerables de la red para así cerrarlos y minimizar los riesgos de este tipo de redes.

[11] ROJAS, Hernán y CAMPOS, Diego. Metodología para la implementación de seguridad en redes inalámbricas WLAN para sistemas de información [en línea]. Cali, Agosto (citado mayo 15, 2017). Disponible en internet: http://miseriwlan.blogspot.com.co/2006/08/metodologia-para-la-implementacion-de.html

Si bien los dispositivos móviles facilitan muchas de las actividades que realizamos a diario, también pueden convertirse en una probabilidad de riesgo constante, para la información sensible que cada persona o negocio manipula o guarda y que es de gran valor por diferentes motivos, por lo que se hace indispensable que se mitiguen estos riesgos.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo hacer un procedimiento que permita realizar pentesting en una red inalámbrica desde un dispositivo móvil con sistema operativo Android y apoyando en herramientas de seguridad basadas en software libre?

2. JUSTIFICACIÓN

Los dispositivos móviles tienen gran demanda por la facilidad que brindan a la hora de movilidad y comodidad, y en especial por la simplicidad de conexión a las redes e internet, pero debido a esta facilidad de conexión y teniendo en cuenta la cobertura de la señal emitida por la redes inalámbricas hacen que estas sean un blanco más fácil para los accesos no autorizados o intrusiones, lo que lleva desde una simple conexión para acceder de manera gratuita (robo) a internet, así como también delitos informáticos de consecuencias mayores.

Por lo anterior se debe asegurar las redes inalámbricas básicamente para realizar un adecuado control de acceso y garantizar que no se capture o alteren datos de los usuarios durante trasmisión de la información, es decir que no se va vulnerada en ninguno de los principios de seguridad de la información, los cuales son integridad, confidencialidad y disponibilidad.

Para lograr lo anterior se deben encontrar los riesgos o vulnerabilidades que están presentes en la red inalámbrica, una vez que sean identificados los riesgos es posible contar con un balance del nivel de seguridad de la red inalámbrica y posteriormente se puede proceder a tomar medidas necesarias para mitigarlos los riegos identificados, una de las maneras para hallar estos riesgos es ejecutando un pentest, el cual para este caso podrá ser realizado desde un dispositivo móvil con sistemas operativo Android, apoyado con el uso de herramientas gratuitas que permitan realizar estas actividades de escaneo de vulnerabilidades. El procedimiento entregado se podrá aplicar a cualquier red inalámbrica.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Generar un procedimiento que permita realizar pruebas de PENTEST en una red inalámbrica a través de dispositivos móviles con sistema operativo Android, utilizando herramientas de software libre.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar un compendio de las vulnerabilidades y amenazas más conocidas a las cuales están expuestas las redes inalámbricas.

- Caracterizar como mínimo cinco herramientas de software libre, que permitan realizar pentest a redes inalámbricas desde dispositivos con sistema operativo Android, y seleccionar la más adecuada.

- Identificar la metodología utilizada para la realización de PENTEST y aplicar cada una de sus fases utilizando la herramienta seleccionada.

- Diseñar un procedimiento para elaborar pentest a una red inalámbrica con las herramientas seleccionadas desde dispositivos con sistema operativo Android

4. MARCO DE REFERENCIA

4.1 MARCO TEÓRICO

4.1.1. Dispositivos móviles.

Los dispositivos móviles se definen como dispositivos de tamaño pequeño, tienen la capacidad de procesamiento básico, que permiten conexión ya sea constante u ocasional a una red, los cuales poseen una memoria con limitaciones, el cual se ha diseñado para una función específica, pero generalmente es capaz de desempeñas funcionales adicionales. Actualmente existen un sin número de dispositivos móviles, tan sencillos como reproductores de audio, hasta unos tan complejos y sofisticados como teléfonos celulares, GPS, entre muchos más.

Debido al creciente número de funcionalidades asociados con dispositivos móviles, en 2005 T38 y *Dupont Global Mobility Innovation Team* vieron la necesidad de clasificación de estos dispositivos y propusieron la siguiente estandarización para definir la clasificación, así:

Dispositivo Móvil de Datos Limitados (*Limited Data Mobile Device*). Corresponden a esta los teléfonos móviles clásicos, caracterizados por poseer pequeña pantalla de tipos texto, brindando servicios limitados a SMS y acceso WAP.

Dispositivo Móvil de Datos Básicos (*Basic Data Mobile Device*). Caracterizados por poseer una pantalla de tamaño mediano, dotados con menú que permiten navegación basada en iconos, ofreciendo la posibilidad de manejo de emails, lista de direcciones, SMS, y posibilidad de un navegador web básico, dentro de los que se encuentran los teléfonos inteligentes (“smartphones”).

Dispositivo Móvil de Datos Mejorados (*Enhanced Data Mobile Device*). Caracterizados porque poseen pantallas por arriba de los 240 x 120 pixels, navegación de tipo stylus, brindando además de las características de los grupos anteriores aplicaciones nativas como aplicaciones de Microsoft Office Mobile (Word, Excel, PowerPoint) y aplicaciones corporativas usuales, en versión móvil, como Sap, portales intranet, etc. Este tipo de dispositivos incluyen los S.O. como Windows Mobile.

Los dispositivos móviles cuentan con su propio sistema operativo, que según su definición es la capa que se encentra entre el hardware y el usuario, es la interfaz que permite que el usuario utilice de manera fácil las herramientas que posee el dispositivo para realizar las tareas programadas, sin entender los complejos

procesos que internamente lleva a cabo. Existen varios sistemas operativos algunos de ellos son, Symbian, blackberry, Windows Mobile, IOS, Andriod, entre otros. El uso de uno u otro determina las capacidades de los dispositivos, y la manera como interactúa con el usuario, y también se trata de competencia entre fabricantes y demás temas comerciales[12].

4.1.2. Sistema operativo Android.

Es un sistema basado en Linux con un núcleo de sistema operativo libre y multiplataforma, diseñado para dispositivos móviles, que permite programar aplicaciones en Dalvik, una variación de java. El sistema brinda interfaces para que las aplicaciones puedan tener acceso a las funciones del teléfono de manera sencilla en lenguaje de programación java.

Lo anterior permite que una cantidad de aplicaciones estén disponibles para los usuarios de este sistema, gracias a la existencia de herramientas de programación gratuitas, una de las características de este sistema es que es totalmente libre lo que lo hace muy atractivo para los fabricantes de dispositivos y para los desarrolladores. Todos pueden bajar el código fuente, inspeccionarlo, compilarlo e incluso cambiarlo.[13]

4.1.3 Ethical Hacking. En todo el mundo los computadores están expuestos a ser atados por crackers o hackers que pueden comprometer los sistemas informáticos y robar valiosa información o borrar parte de ella. Por lo anterior el objetivo principal de un ethical hacking es descubrir las vulnerabilidades presentes en los sistemas analizados. Mediante los test de intrusión, con los cuales se verifican y evalúan la seguridad física y lógica de los sistemas de información, redes, aplicaciones web, bases de datos, servidores, entre otros.

El servicio de ethical Hacking, crea un ambiente simulado de posibles escenarios donde se realizan ataques de manera controlada, igual que actividades que son propias de delincuentes cibernéticos, para hallar las vulnerabilidades del sistema de interés. Ethical Hacking es una disciplina de la seguridad informática que utiliza una variada de métodos para realizar pruebas, incluyendo ingeniería social,

---

[12] BAZ, Arturo; FERREIRA, Irene; ÁLVAREZ, María y GARCÍA, Rosana. Dispositivos móviles [en línea]. Universidad de Oviedo. Disponible en:http://isa.uniovi.es/docencia/SIGC/pdf/telefonia_movil.pdf. pág. 1

[13]GONZÁLEZ, Alejandro. Que es Android. [En línea]. Washington, febrero 2011 [Citado el 8 de mayo de 2016] disponible en: (http://www.xatakandroid.com/sistema-operativo/que-es-android)

herramientas de hacking, metasploits que explotan vulnerabilidades conocidas y muchas más que permiten penetrar las áreas críticas de las organizaciones.[14]

4.1.4 Metodologías de ethical hacking. A continuación, algunas de las metodologías y técnicas más utilizadas en el mundo de ethical hacking.

OSSTMM (*Open-Source Security Testing Methodology Manual*). Esta metodología propone un proceso de evaluación de una serie de áreas que permite ver de manera acertada los niveles de seguridad presentes en la infraestructura a auditar, estos niveles son conocidos como dimensiones de seguridad y su objetivo es analizar factores como:

- Visibilidad
- Acceso
- Confianza
- Autenticación
- Confidencialidad
- Privacidad
- Autorización
- Integridad
- Seguridad
- Alarma

Para realizar un trabajo secuencial esta metodología tiene 6 ítems que comprenden todo el sistema actual, estos son:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las tecnologías de Internet
- Seguridad en las comunicaciones
- Seguridad inalámbrica
- Seguridad Física[15]

ISSAF (*Information Systems Security Assessment Framework*). Marco metodológico desarrollado por OISSG que permite clasificar la información de la

[14]REYES, Alejandro. Ethical Hacking, [En línea] [Citado el 25 de mayo de 2016] disponible en:(http://www.seguridad.unam.mx/descarga.dsc?arch=2776)

[15] ISAZA, Miguel Arturo. Metodologías y Herramientas de Ethical Hacking, [En línea]. Mountain View Estados Unidos, febrero de 2013 [Citado el 19 de mayo de 2016] disponible en: http://seguridadinformaticahoy.blogspot.com.co/2013/02/metodologias-y-herramientas-de-ethical.html

evaluación de seguridad en diferentes dominios usando diversos criterios de prueba, algunas de sus elementos más destacados son:

- Brindar medidas que permiten ver el estado de escenarios reales para evaluaciones de seguridad
- Enfocada en cubrir procesos de seguridad y las evaluaciones de los mismos para obtener un panorama completo de las vulnerabilidades existentes.

- Permite el desarrollo de matriz de riesgo para comprobar la efectividad en la implementación de controles.[16]

OWASP (*Open Web Application Security Project*). Metodología enfocada en la seguridad de aplicaciones, así pueden relacionar los costes de un software inseguro al impacto que tiene en el negocio, y así gestionar decisiones de negocio apropiadas para la gestión del riesgo, las características más relevantes son:

- Pruebas de firma digital de aplicaciones Web.
- Comprobaciones del sistema de autenticación.
- Pruebas de *Cross Site Scripting.*
- Inyección XML
- Inyección SOAP
- HTTP Smuggling
- Sql Injection
- LDAP Injection
- Polución de Parámetros
- Cookie Hijacking
- *Cross SiteRequestForgery*
- CEH (*CertifiedEthical Hacker*)
- Metodología de pruebas desarrollada por International Council of Electronic Commerce Consultants, algunas de las fases de esta metodología son:
- Obtención de Información.
- Obtención de acceso.
- Enumeración.
- Escala de privilegios.
- Reporte[17]

OFFENSIVE SECURITY. Esta metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad, encierra principalmente métodos para el desarrollo de estudios de seguridad encaminados en seguridad ofensiva y teniendo como guía la posibilidad real de explotación

[16]Ibíd.
[17]Ibíd.

independientemente de los indicadores de riesgo y vulnerabilidades, algunas de las ventajas de esta metodología son:

- Enfoque sobre la explotación real de las plataformas.
- Enfoque altamente intrusivo.
- Enfoque orientado a resultados tangibles y no a estadísticas generadas por herramientas.[18]

4.1.5 Herramientas de *Ethical Hacking*. Existen muchas herramientas y para todo tipo pen test, por este motivo un consultor debe identificar qué tipos de test va a realizar y así poder seleccionar las mejores herramientas. Algunas de estas herramientas son gratuitas y de código abierto, otras de pago y propietarias.

4.1.5.1 Herramientas pentesting para Android. Según el sitio creadpag, Linux está considerado como el mejor sistema operativo para hacking ético y pentesting o pruebas de penetración, y como Android es un sistema basado en Linux, hay varias aplicaciones de hacking disponibles para este sistema, para encontrar vulnerabilidades y errores se necesitan herramientas solidas de hacking[19].

A continuación, se mencionan algunas de ellas, con las que puede convertir un dispositivo Android en una máquina de ethical hacking:

AndroRAT. Es una herramienta de administración remota para dispositivo Android, este es una aplicación cliente servidor, su objetivo es realizar administración remota para permitir el control del sistema Android de forma remota y recuperar información de ella[20].

Red Spoofer. Es una aplicación que permite cambiar la página web en el ordenador de otras personas desde un móvil Android, solo conectándose a la red wifi. Esta aplicación se considera como una herramienta de hacking malicioso por los administradores de red[21].

APK Inspector. Permite visualizar paquetes Android compilados y su correspondiente código de DEX inversa, esta aplicación ofrece dos funciones de

[18]Ibíd.
[19]CREADPAG. 10 aplicaciones de hacking para Android para pentesters, aficionados e investigaciones, [En línea]. California Estados Unidos, enero 2017. [Citado el 20 de mayo de 2016] disponible en: https://creadpag.com/10-aplicaciones-de-hacking-para-android-para-pentesters-aficionados-e-investigaciones/
[20]Ibídem.
[21]Ibídem.

análisis y las características gráficas para poder obtener conocimiento profundo de las aplicaciones maliciosas[22]

Dsploit. Es una suite de pruebas de penetración libre desarrollada para Android, puede ser usado para realizar una serie de tareas relacionadas con la red, también contiene funciones de gran alcance que permiten analizar, capturar y manipular las transacciones de red. Puede escanear las de redes de dispositivos conectados, identificar el sistema operativo, funcionando los servicios y puertos abiertos, así como revisarlas en busca de vulnerabilidades[23].

Wi-fi Killer. Esta aplicación permite realizar el bloqueo de un usuario para el uso de la red wifi, también puede desactivar la conexión a internet para cualquier dispositivo que esté presente en una red wifi[24].

Revenssis. Es una suite de herramientas usadas en computadora y seguridad de uso del web, las herramientas que se incluyen, son, exploradores de App del web, laboratorio de investigación de vulnerabilidad, ForensicsLab, plus themust-haveutilities (Shell, SSH, DNS/WHOIS Lookup, Traceroute, Port Scanner, Spam DB Lookup, Netstat.)[25]

4.1.5.2 Prueba de penetración (pent test). Las pruebas de penetración o pen test son una práctica para colocar a prueba un sistema informático, red o aplicación web para detectar vulnerabilidades que un atacante podría explotar. Las estrategias utilizadas para este tipo de pruebas son:

Pruebas orientadas a un objetivo. Estas pruebas selectivas son llevadas a cabo en conjunto por el equipo de TI de la organización y el equipo del pen test. En esta todos están viendo el examen que se realiza.

Comprobación externa. Es dirigida a los dispositivos de la organización como servidores que son visibles externamente, tales como controladores de dominio, servidores de correo electrónico, firewalls entre otros. El objetivo es comprobar si un ataque externo es posible y hasta donde puede tener acceso.

---

[22]Ibídem.
[23]Ibídem.
[24]Ibídem.
[25]ISAZA, Miguel Arturo. Metodologías y Herramientas de Ethical Hacking, [En línea]. Mountain View Estados Unidos, febrero de 2013[Citado el 19 de mayo de 2016] disponible en: (http://seguridadinformaticahoy.blogspot.com.co/2013/02/metodologias-y-herramientas-de-ethical.html)

Pruebas internas. Esta consiste en un ataque interno realizado por un usuario autorizado, con privilegios de acceso estándar, esta es prueba permite medir hasta donde puede tener acceso un empleado o acceso interno.

Pruebas a ciegas. Esta prueba simula las acciones y procedimientos real de un atacante, en este caso la información proporcionada al equipo de pen test es muy limitada, generalmente solo se entrega el nombre de la empresa. A este tipo de prueba se le debe dedicar mucho tiempo por lo que la hace costosa.

Prueba de doble ciego. Las pruebas como esta, toman pruebas a ciegas y la llevan a otro plano, en este tipo de prueba, solo una o dos personas de la organización conocen de la realización de esta prueba. Este tipo de prueba suelen ser útiles para medir el monitoreo de seguridad, identificación de incidentes y procedimientos de respuesta.[26]

4.2 ANTECEDENTES

TITULO DEL PROYECTO: "DETECCIÓN DE VULNERABILIDADES EN REDES INALÁMBRICAS 802.11i, MEDIANTE EL ANÁLISIS DE TRÁFICO DE LA CAPA DE ENLACE"

AUTORES:

ASTUDILLO CABRERA JAIME JAVIER
TROYA ESTRELLA ANDRÉS SEBASTIÁN

Objetivo

Determinar las vulnerabilidades de una red inalámbrica que utiliza el estándar 802.11i, mediante el análisis del tráfico en la capa de enlace, de los paquetes de Control, Administración y Datos.

Resumen

En los últimos años se ha evidenciado el aumento del uso de redes inalámbricas debido a las características y ventajas que ofrecen sobre las redes cableadas; entre ellas: la movilidad de los usuarios manteniendo conectividad constante a la red local, la facilidad de incrementar el tamaño de la red y la configuración de diferentes topologías entre ellas el estándar 802.11i. Mediante la implementación de un escenario de prueba, se estudia el estándar 802.11i por medio de la captura de las tramas de Administración y Control. Se utiliza un

[26] ROUSE, Margaret. Prueba de penetración (pen test). [En línea] marzo de 2014 [Citado 04 de abril de 2017] Disponible en: http://searchdatacenter.techtarget.com/es/definicion/Prueba-de-penetracion-pen-test

analizador de paquetes como *AirPcapNx o Kismet* para interceptar información de la red inalámbrica que pueda ser analizada en Wireshark. Una vez obtenida esta información, se realizan ataques éticos utilizando software especializado como BT5r3 (BackTrack) para simular problemas en la seguridad como denegación de servicio (DoS)[27].

TITULO DEL PROYECTO: "Análisis de Vulnerabilidades de una Red Corporativa mediante Herramientas de Descubrimiento Activas"

AUTOR:

JAIRO MANUEL PALACIOS DOMÍNGUEZ

Objetivo

El objetivo principal de este trabajo es el estudio y la implantación de un framework que contiene algunas de las distintas herramientas de pentesting utilizadas en una auditoría de seguridad, principalmente en la fase de descubrimiento de vulnerabilidades.

Resumen

Este proyecto se ha realizado con el objetivo de realizar un análisis de vulnerabilidades de una red corporativa, utilizando para ello herramientas de descubrimiento activas, tales como NMap, OpenVAS, vFeed y Xprobe2. Este análisis de vulnerabilidades se ha desarrollado de forma que sea escalable a otras redes, y transparente para el usuario, de manera que el usuario final de este trabajo solo se deba encargar de introducir el direccionamiento IP de las subredes y el tipo de análisis a realizar, y automáticamente, en segundo plano, se realizarán todo tipo de análisis a través de las herramientas antes citadas, para, posteriormente, poder visualizar el resultado de las mismas a través de un dashboard interactivo, implementado a través de la pila de herramientas Elasticsearch, Logstash y Kibana, en el que se podrán seleccionar los campos que se consideren relevantes del análisis, para finalmente, evaluar el análisis de riesgos en función de los resultados obtenidos. El objetivo final es facilitar al auditor de seguridad el estudio de losresultados de los análisis realizados de una forma gráfica y lo más intuitiva posible, para que después de evaluar los riesgos, se puedan tomar decisiones y mejorar la seguridad en la empresa auditada, bien recomendando cambios en configuraciones, permisos o servicios que se estén ejecutando, o bien intentando abrir un punto de partida de negocio, en el que pudiera recomendar equipamiento existente en el mercado que satisfaga esas necesidades descubiertas, o por otro lado,

[27] ASTUDILLO, Jaime y TROYA, Andres. Detección De Vulnerabilidades En Redes Inalámbricas 802.11i, Mediante El Análisis De Tráfico De La Capa De Enlace. Universidad de las Fuerzas Armadas ESPE. Julio 2014. [citado enero 15, 2017]Disponible en internet: http://repositorio.espe.edu.ec/handle/21000/8890

continuar con la auditoría completa si así se requiere, intentando explotar dichas vulnerabilidades y escalar privilegios dentro de la organización, para después generar un informe completo del estado de la seguridad en la empresa.[28]

TITULO DEL PROYECTO: "Riesgos con las redes Wi-Fi públicas del centro de Medellín, Colombia**"**

AUTOR:

ROBERTO CARLOS GUEVARA CALUME

Objetivo

Documentar a través de mapas de cobertura el uso de las redes WiFi en la banda de 2.4 GHz, de libre acceso en puntos críticos de la comuna 10, para proponer una metodología que permita trazar estos mapas; además de aumentar los niveles de seguridad capacitando a las empresas en principios básicos de seguridad que protegen la información y el acceso no autorizado a las redes Wi-Fi de empresas geográficamente cercanas.

Resumen

El acceso a internet a través de redes inalámbricas Wi-Fi es cada vez más cotidiano; su bajo costo, sumado a la ventaja de no requerir cables, le ha traído gran popularidad no obstante la vulnerabilidad inherente ante accesos no autorizados. En Medellín, principalmente en el centro de la ciudad, se encuentran muchos sitios que ofrecen internet a través de redes Wi-Fi; además, muchas pymes también las usan para la comunicación interna entre sus computadores. En este documento se muestran los resultados del análisis de solapamiento de canales y problemas de interferencia que afectan la velocidad de transferencia en los puntos de acceso libre a internet que emplean tecnología Wi-Fi, suministrados por entidades públicas y privadas en el área de estudio, a través de la georreferenciación de planos digitales. Por último, se realiza una encuesta para identificar el uso que se da a las redes Wi-Fi. Se analizarán y mostrarán los resultados sobre el grado de seguridad de la red en las empresas localizadas cerca de estos puntos de acceso libre a internet para alertar y mejorar la seguridad ante intrusos que intenten acceder sin ser autorizados.[29]

[28] Palacios, Jairo. Análisis de Vulnerabilidades de una Red Corporativa mediante Herramientas de Descubrimiento Activas. Universidad de Sevilla. Julio de 2015 [citado febrero 16, 2018] Disponible en internet:
http://bibing.us.es/proyectos/abreproy/90522/fichero/Memoria+del+Trabajo+Fin+de+Grado.pdf
[29] Guevara, Roberto. Riesgos con las redes Wi-Fi públicas del centro de Medellín, Colombia. Corporación Universitaria Remington. Febrero de 2017 [citado febrero 16, 2018] Disponible en internet: http://www.uniremington.edu.co/images/investigacion/libros-investigacion/Wi-Fi-Ok-2.pdf

4.3 MARCO LEGAL

Dentro de la normatividad que rige en Colombia, que hacen referencia a delitos informáticos, los cuales se deben tener en cuenta para este proyecto son:

LEY 1273 DE 2009(enero 05)

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[30].

> *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 1000 salarios mínimos legales mensuales vigentes.*[31]
>
> *Artículo 269D. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, 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.*[32]
>
> *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.*[33]

PROYECTO DE LEY 241 DE 2011 SENADO. Por la cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet.[34]

---

[30]COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273. Bogotá. (enero 5 de 2009). Diario Oficial 47.223 de enero de 2009. p. 1-4

[31] Ibíd. p. 1

[32] Ibídem

[33] Ibídem

[34] COLOMBIA, SENADO DE LA REPÚBLICA. Ley 241 de 2011, [En línea] marzo de 2014 [Citado 04 de abril de 2017] Disponible en: http://servoaspr.imprenta.gov.co/gacetap/gaceta. mostrar_ documento?p_tipo=05&p_numero=241&pconsec=28543

Ley 527 de 1999 - COMERCIO ELECTRÓNICO. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones[35]

Ley 599 DE 2000. Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.[36]

Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.[37]

4.4 MARCO CONCEPTUAL

4.4.1 Seguridad de la Información. Seguridad de la información está definida como el grupo de acciones técnicas, legales y organizativas que contribuyen para garantizar la confidencialidad, integridad, y disponibilidad de la información.

Antes del auge de los sistemas informáticos, la información sensible de las organizaciones era física y se almacenaba en archivadores en grandes cantidades, presentando posteriores dificultades como, almacenamiento, acceso, trasporte y procesamiento.

Con la llegada de los sistemas informáticos es posible la digitalización de este gran volumen de información brindando la posibilidad de un fácil procesamiento y análisis, mejor presentación de dicha información y se evitan problemas de espacio físico y transporte. Pero se presentan otros problemas atados a estas facilidades,

---

[35] COLOMBIA, Congreso de la República. Ley 527 de 1999. Bogotá. (agosto 21 de 1999). Diario Oficial 43.673 del 21 de agosto de 1999. p. 1

[36] COLOMBIA, Congreso de la República. Ley 599 de 2000. Bogotá. (julio 24 de 2000). Diario Oficial 44097 del 24 de julio de 2000. p. 1

[37] COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL República de Colombia Departamento Nacional de Planeación. Documento Conpes. Bogotá (julio 14 de 2011), pág. 10.

presentando mayor vulnerabilidad a ser accedida, modificada o perdida, entre otros riesgos.

Desde el inicio de los básicos sistemas informáticos hasta la actualidad, donde el trabajo en red es usual, los inconvenientes asociados con la seguridad de la información han evolucionado y siguen presentes, obligando así a las soluciones a adaptarse a nuevas necesidades técnicas. Creciendo la innovación en los ataques y por ende crece la complejidad de la solución, pero conservando la esencia.[38]

4.4.2 Bases de la Seguridad Informática. Seguridad informática es el conjunto de medidas que tiene como objetivo la protección o conservación de la información valiosa de una organización, en sus diferentes formatos ya sea física papel impreso, en medio magnéticos e incluso en la memoria de las personas. La seguridad de la información se basa en tres principios específicos confidencialidad, integridad y disponibilidad**.**

Confidencialidad. En seguridad de la información, confidencialidad hace referencia a la necesidad de conservar la información y/o recursos en reserva, o secreto.

La confidencialidad tiene como objetivo la impedir la difusión sin autorización de la información.

En general, cualquier organización tiene información que necesita se mantenga en reserva, por variados motivos, diseños propios, seguridad en caso de entidades militares, mantenerlos fuera del alcance de la competencia, entre otros muchos motivos.

Integridad. En seguridad de la información, integridad se refiere a la fidelidad de la información y está relacionada a prevención de cambios no autorizados.

Entonces el objetivo de la integridad es evitar que la información sea modificada sin autorización.

La integridad de la información es referente a dos aspectos, el primero de ellos la integridad de los datos y el segundo a la integridad del origen.

[38] MIFSUD. Elvira, Introducción a la seguridad informática - Seguridad de la información / Seguridad informática. [En línea]. Ministerio de educación, cultura y deporte de España, marzo de 2012 [citado mayo 15 de 2017] disponible en: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

La integridad de los datos es la integridad del volumen de información, mientras que la integridad del origen hace referencia a la fuente de la información, que está directamente vinculada a la credibilidad y confianza de la información.

Disponibilidad. En seguridad de la información, disponibilidad significa que la información este accesible en todo momento para los elementos que estén autorizados.

Siendo entonces el objetivo de la disponibilidad, evitar interrupciones sin autorización o planeada de los recursos informáticos. Un sistema está disponible, cuando su diseño permite poner indisponible el sistema a voluntad.

Con la descripción anterior de las bases de la seguridad informática, se puede resumir que la seguridad radica en conservar el equilibrio entre los factores en mención. No tiene razón conseguir uno de ellos sacrificando los otros, por ejemplo, no tiene sentido mantener la confidencialidad de un archivo, si los usuarios autorizados no pueden acceder a él. [39]

4.4.3 Ciclo PHVA. Es la norma publicada por la ISO, suministra una metodología para gestionar adecuadamente la seguridad de la información de una organización, se centra en la protección de la integridad, confidencialidad y disponibilidad de la información de la organización, para esto realiza una evaluación de los riesgos presentes y define los métodos para mitigar dichos riesgos, por lo general las normas de seguridad son procedimientos, políticas e implementaciones técnicas, esta norma aplica el modelo de procesos PHVA.

Planificar (P)- establece la política, objetivos, procesos y procedimientos de seguridad para mejorar la seguridad de la información y así contribuir con la consecución de los objetivos de la organización.

Hacer (H)- implementar y operar la política, controles, procesos y procedimientos del sistema de gestión de seguridad e la información.

Verificar (V)- Evalúa y mide el desarrollo de los procesos y objetivos de seguridad e informa los resultados para su revisión.

Actuar (A)- Realizar acciones preventivas y correctivas con base en los resultados de la evaluación o auditoria, con el fin de lograr la mejora continua. [40]

[39]Ibídem
[40]Ibid, pág. 2

4.4.4 Vulnerabilidades en redes inalámbricas. Todos los equipos que hacen parte de una red son vulnerables a sufrir diferentes ataques informáticos, estos ataques se pueden agrupar en dos tipos, el primero de ellos se conoce como ataques pasivos, en este tipo de ataque el objetivo es obtener información, solo espiar sin modificar información o sin afectar el sistema.

El segundo tipo se le llama ataques activos, en este tipo de ataque la información es modificada, borrar o causar daños en el sistema.[41]

4.4.4.1 Ataques pasivos. En este tipo de ataque sucede cuando un usuario accede a la red sin autorización para observar la información, ya sea con el fin de curiosear, planear un ataque posterior o entregarla a un tercero para obtener beneficios.

Este ataque es muy difícil de detectar ya que solo se aloja, pero no realizar ninguna acción que lo ponga en evidencia, la forma de realizar una detección de este tipo de amenazas es realizando análisis de red. Dentro de los ataques pasivos más comunes se tienen:

Warchalking / Wardriving. Consiste en visitar diferentes lugares con un dispositivo que permita conectarse redes inalámbricas, buscando puntos de acceso con seguridad frágil o inseguros, una vez ubicados estos puntos se dibuja una de los tres símbolos utilizados para identificarlas, así:

Dos semicírculos opuestos, que identifica una red abierta con acceso total

Un circulo, que identifica una red abierta, pero con nivel bajo de seguridad que no representa un mayor esfuerzo para su acceso.

Un circulo con una W dentro, que identifica que es una red segura y que para su acceso se debe ser un experto.

El wardriving básicamente es igual, con la diferencia que es realizado desde un automóvil involucrando un GPS para obtener coordenadas de ubicación del punto de acceso.

Para la práctica del warchalking y wardriving, existe un software libre que se conoce como netstumbler, cuya función es la búsqueda de datos de acceso en adaptadores

[41]VALLEJO DE LEÓN, Tatiana. Vulnerabilidades y niveles de seguridad de redes WI-FI. WPA [En línea] Universidad de San Carlos de Guatemala agosto de 2010 [citado 16 de octubre de 2017] disponible en: http://biblioteca.usac.edu.gt/tesis/08/08_0266_EO.pdf

de redes wifi que posean chipset Hermes para identificar puntos de acceso que se encuentren en su rango de operación.[42]

- **Sniffing o intercepción de datos.** Este tipo de ataque se basa en escuchar trasmisiones de usuarios de una red, solo se requiere de un software y hardware adecuado para poder escuchar las comunicaciones de la red.

Programas conocidos como sniffer se encargan de capturar, almacenar e interpretar paquetes de datos, buscando la obtención de password, direcciones de correo, usuarios de aplicaciones, información bancaria entre muchos otros datos sensibles, pero este tipo de programas también pueden ser utilizados para el monitoreo de redes, para detectar intrusiones, filtrar contenidos sospechosos, es decir asegurar la red.

Algunos de los programas sniffer más conocidos son el spynet el cual posee un analizador de tráfico y de datos, capaz de reproducir contraseñas de mail, también identifica las direcciones MAC de cada equipo, protocolos de trasmisión y programas utilizados. El winsniffer con el cual es posible descubrir usuarios y contraseñas utilizando la versión pagas, ya que posee una versión gratuita con la cual solo se muestran los usuarios. Otro sniffer es el Aircrack, esta captura paquetes para romper el cifrado WEP, permitiendo la inyección de tráfico en la red.[43]

4.4.4.2 Ataques activos. Se producen cuando se realiza un acceso no autorizado para modificar el contenido de la información o impide que la misma se acceda o se utilice, dentro de los ataques más comunes se encuentran:

- **Enmascaramiento o suplantación.** Se le conoce también con robo de identidad o falsificación, en donde el intruso se hace pasar como un usuario autorizado o toma el lugar de un usuario desconectado suplantándolo. En este tipo de ataque también se puede suplantar un punto de acceso, dentro de los ataques por suplantación más comunes están:

- **Secuestro de sesión.** En este tipo de ataque el intruso monitorea la red hasta obtener y elige un usuario al cual desconecta mediante ataques de denegación de servicios, para luego tomar su lugar en la red, normalmente esta desconexión no es prolongada, para no ser descubierto para ellos suplanta diferentes usuarios cada vez.

[42]Ibíd. p. 39
[43]Ibíd. p. 41

- **Suplantación de dirección MAC.** Este tipo de ataque se presenta normalmente en tipos de redes protegidas por filtrado de direcciones MAC, en este tipo de ataque el método es similar al descrito anteriormente solo que se suplante una dirección MAC en lugar de un usuario, para ellos el atacante identifica la MAC a suplantar y la simula en su equipo, esto se logra con software tales como ethereal, netstumbler, air Jack entre otros.

- **Denegación de servicios (DoS).** En este tipo de ataque el objetivo dejar inoperante la red para desconectar a los usuarios y así poder suplantarlos, es de difícil detectarlos debido a que solo es posible en tiempo real y dura poco tiempo, las maneras más comunes de denegación de servicio son:

- **Saturar el ambiente con ruido de RF.** La relación señal-ruido, debe ser igual o mayor al 30% en los puntos de una red inalámbrica, por debajo de este valor la seña será anulada por el ruido lo que hace inoperante a la red, entonces este tipo de ataque consiste en inyectar ruido RF en el medio.

- **Torrente de autenticaciones.** En este el atacante envía al servidor radius repetidas peticiones de autenticación falsas de manera simultánea y reiterativa, la idea es ocupar la red intentando autenticar estas peticiones, para que los usuarios autorizados no puedan autenticarse y por ende no tengan acceso a la red.

- **Modificación de paquetes WPA.** La verificación de integridad de paquetes del WPA, puede ser utilizada con un ataque de denegación de servicio sin estar concebido para ello, el atacante modifica un par de paquetes, entonces TKIP-WPA si detecta 2 o más paquetes modificados, asume que está siendo atacado y desconecta automáticamente a todos los usuarios conectados momentáneamente, al volver a realizar la conexión el atacante altera de nuevo paquetes y así logra otra desconexión. Para ello se usa software como el airjack.

- **Signaling DOS.** Este tipo de ataque finaliza las sesiones móviles, consiste en él envió de pequeños paquetes de datos con el fin de reiniciar sesión después que esta haya sido liberada, este ataque de bajo volumen es capaz d crear congestión en el controlador de radio de la red, esta sobrecarga del radio da como resultado una denegación de servicio para un usuario.

- **Drenado de batería.** Este tipo de ataque consiste en enviar paquetes a un cliente evitando que este quede en modo suspensión y así consuma recursos de red y agotar la batería del dispositivo.

4.4.4.3 Retransmisión. Este tipo de ataque también se le llama hombre en el medio, consiste en que el atacante se pone en medio del cliente y el punto de acceso, luego de haber adquirido información como el SSID, MAC, DHCP entre otras e información de cliente, para poder emular el punto de acceso para evitar que llegue la información entre los puntos o modificándola para engañar al destinatario.[44]

4.4.4.4 Vulnerabilidad WPA/WPA2. Aunque estos protocolos son fuertes en seguridad, presentan debilidades minúsculas que pueden ser explotadas teniendo conocimiento al respecto, una de las vulnerabilidades más destacadas es el ataque a la clave PSK, debido a que la información que circula por la red viaja en formato texto, y es trasmitido en el momento que un usuario realiza autenticación en el llamado 4-handsshake. La explotación de esta vulnerabilidad es realizada por fuerza bruta o con diccionarios, para lo cual es procedimiento es igual, consiste en comparar varias claves contra la suma de chequeo del handshake, hasta lograr la que coincidan, para tener el acceso de la red. Que el ataque logre su cometido dependerá de la complejidad de la contraseña y otras opciones de seguridad alternas como el filtrado de MAC para dar seguridad a la red. En definitiva, la fuerza bruta pierde funcionalidad al combinar números letras y caracteres en una contraseña, ya que aumenta la cantidad de combinaciones haciendo casi imposible ser descifrada.[45]

4.4.4.5 Vulnerabilidad de WPS. WPS o Wifi ProtectedSetup es un estándar adoptado por la Wi-fi Alliance, que facilita la creación de redes seguras Wlan, WPS no es un mecanismo de seguridad, sino que es un grupo de sistemas cuyo fin es hacer más fácil al configurar una red inalámbrica con seguridad WPA2 de entornos domésticos y empresas pequeñas, este implanta métodos que permite a diferentes dispositivos conseguir credenciales requeridas para hacer autenticación en la red.

La principal vulnerabilidad de WPS se presenta porque es un estándar establecido por Wi-fi Alliance, por esto para que posea la certificación Wi-fi debe tener esta funcionalidad activada por default, como consecuencias se encuentran más dispositivos en el mercado con esta vulnerabilidad, en 2011 fue descubierta una vulnerabilidad que afecta dispositivos WPS, la cual permite recuperar el pin WPS a un atacante y de esta manera acceder a la contraseña WPA o WPA2 en un par de

[44]Ibíd. p. 40

[45] RUZ, J. RIVEROS, B. VARAS, A. Redes WPA/WPA2. [En línea] universidad técnica Federico Santa María, agosto de 2013 [citado 17 de octubre de 2017] disponible en: http:// profesores. elo.utfsm.cl/~agv/elo322/1s12/project/reports/RuzRiverosVaras.pdf

horas, el acceso que brinda un pin WPS permite desde el acceso a la red, llegando al punto de permitir el cambio de la configuración.[46]

4.4.4.6. Deficiencias en el método Shared Key. Shared key o llave compartida tiene como debilidad que basta solo con hallar la primera palabra de 1 keystream, para conseguir los datos de la clave secreta que se comparte.

El proceso radica en conseguir IVs que produzcan la falta de información de la llave para el keystream. Este fenómeno recibió el nombre de condición resuelta por parte de sus autores. Cada paquete que es resuelto presenta la falta los datos de 1 byte de la llave, el cual debe ser previsto de manera correcta de manera que el paquete que continua pueda entregar información del próximo byte de la llave. Para hacer más rápido el ataque, se debe localizar los IVs frágiles que tengan esta particularidad.[47]

4.4.4.7. Debilidad ACL(Access Control List). Uno de los métodos más frecuentes que son utilizados para otorgar seguridad en redes inalámbricas es limitar los dispositivos que pueden conectarse al punto de acceso mediante el filtrado de direcciones MAC. Para ello se realiza una table en el punto de acceso, donde se listan las direcciones MAC de los dispositivos que cuentan con autorización para conectarse a la red. Esta medida puede ser vulnerada ya que es posible de manera sencilla cambiar la dirección MAC de un dispositivo y asignar una dirección MAC que tenga autorización de acceso al punto de acceso y por ende a la red.[48]

[46]Ibíd. p 7
[47]ZUCCARDI, Giovanni, GUTIERREZ, Juan. Vulnerabilidades en 802.11. [En línea]. Universidad Javeriana, octubre de 2016, [citado 16 de febrero de 2018]. Disponible en: http://pegasus.javeriana.edu.co/~edigital/Docs/802.11/Vulnerabilidades/Vulnerabilidades%20v0.5.doc
[48]Ibíd. p 4

4.4.4.8. FreeBSD - IEEE 802.11 Buffer Overflow. Este sistema aplica un protocolo de negociación para redes inalámbricas. La vulnerabilidad es causada por el desborde de un integer en el conductor de paquetes que están corruptos de tipo beacon o probe response en IEEE 802.11 al hacer un escaneo buscando redes termina en un paquete que causa el desbordamiento de buffer. Lo que concede a un intruso hacer un paquete o probe response a mano y que sea enviado a todos los dispositivos y permitir la ejecución de un código que resulte arbitrario con el contexto del FreeBSD kernel de un procedimiento de escaneo por redes inalámbricas.[49]

4.4.4.9. Denegación de servicio en IEEE 802.11. Esta vulnerabilidad está presente cuando se realizar la implementación del hardware del protocolo inalámbrico IEEE 802.11 que se presta para realizar un ataque que afecte la disponibilidad de los dispositivos presentes en una red inalámbrica.

Es posible realizar un ataque mediante el uso de un dispositivo con tarjeta de red inalámbrica, ocasionando la interrupción importante del tráfico de la red, y este como consecuencia haría difícil que fuera ubicado el atacando.

Dicha vulnerabilidad está ligada con la MAC del protocolo IEEE 802.11, dispositivos móviles que ejecutan CSMA/CA lo que resta la trasmisión de 2 dispositivos de forma simultánea. Mediante la utilización de clear channel assessment por parte de todo el hardware que se basa en el estándar y que se realiza por la capa física en direct sequence spread spectrum. En un ataque el dispositivo simula que el canal está ocupado evitando que sea trasmitido cualquier dato.

Anteriormente ataques de indisponibilidad necesitaban de hardware especializado y estaban condicionados de la capacidad de saturación de la frecuencia de la red. La presente vulnerabilidad posibilita que un ataque tenga éxito con bajos costos y se realiza son necesidad de poseer conocimientos avanzados.[50]

4.4.4.10. Debilidades EAP. El protocolo de autenticación IEEE 802.1X es un medio creado inicialmente para redes cableadas, y cuenta con sistemas de autenticación, autorización y distribución de contraseñas y también integra control de acceso para los usuarios que se pretenden unir a la red. El protocolo IEEE 802.11 se compone por 3 elementos prácticos:

- El cliente que solicita acceso a la red
- El autenticador que realiza el control de acceso

[49]Ibíd. p 5
[50]Ibíd. p 5

- El servidor de autenticación

Para el caso de la red inalámbrica, el punto de acceso hace las veces de autenticador, cada puerto está dividido en dos lógicos, de esta forma la PAE (Port Acces Entity), la PAE de autenticación permanece abierta, permitiendo pasar los procesos de autenticación, por otro lado, el PAE de servicio abre una vez la autenticación haya sido de manera satisfactoria.

- **Vulnerabilidad en Kerberos.** Kerberos IV y V presenta vulnerabilidad a ataques con diccionario, los cuales pueden llegar a convertirse en potenciales, si se realizan en lugares donde se presentan alto número de intercambios de autenticación los cuales pueden ser capturados en un tiempo corto. No se debe hacer uso de Kerberos V sin utilizar mecanismo de brinden protección con ataques de diccionario offline.

- **Vulnerabilidad en el LEAP de Cisco.** Este es un algoritmo de autenticación mutua capaz de soportar desviación cambiante de llaves de sesión. Esta autenticación mutua está condicionada de un secreto compartido, el password de un cliente conocido por este y la red, y que se usa comunicación entre el cliente y el Radius (Remote Authentication Dial-In User Service). Al igual que los demás algoritmos que se basan en contraseñas, LEAP es vulnerable a los ataques realizados por diccionario, durante este ataque, los cambios de contraseñas son utilizadas para comprometer las contraseñas de autenticación del cliente.
  Cisco creo EAP-FAST (EAP-Flexible Authentication via Secure Tunneling) para clientes interesados en implementar una 802.1x que no necesite certificados digitales y que no es vulnerable a los ataques de diccionario.[51]

4.4.4.11 Debilidades del estándar IEEE 802.1x. La IEEE propuso para solucionar todas las falencias de seguridad presentadas en 802.11, RSN (Robust Security Network), este sistema utiliza protocolo 802.1x en el cual se basa para realizar el control de acceso, autenticación y administrar las llaves. Sin embargo, este sistema posee dos falencias de seguridad, el secuestro de sesión y permite hacer man in the middle.

- **Ausencia de autenticación mutua**. En esta arquitectura una de las falencias de seguridad presentes es la ausencia de autenticación entre el punto de acceso y el dispositivo de manera mutua o bidireccional, esto debido a que la autenticación en solo sentido permite dejar expuesto al dispositivo a un ataque

[51]Ibíd. p 7

man in the middle, donde el atacante simula ser un punto de acceso hacia el dispositivo y un dispositivo hacia el punto de acceso.

- **Debilidad de EAP de mensaje satisfactorio**. Un mensaje aprobatorio se envía desde el autenticador hasta el dispositivo, lo que indica que el proceso de autenticación ha sido efectiva ante el servidor Radius. independiente del mecanismo de autenticación superior, el mensaje no posee datos que permitan asegurar la integridad. De la misma forma ocurre en el dispositivo, el cual posee la situación de cambiar al estado autenticado sin que interese su condición anterior. El mensaje positivo EAP cambia de valor del botón eapSuccess, el cual hace de forma inmediata al estado autenticado lo que produce conexión a la red. Por lo anterior, el envió forzado por parte de un atacante de un paquete suplantando al autenticador, es el inicio de un ataque man in the middle.

- **Secuestro de sesión.** Con IEEE 802.1x, el proceso de autenticación de las capas posteriores pasa posterior a la asociación o reasociacion del RSN, es decir que existen dos dispositivos de estados, RSN y 802.1x. Las tareas compuestas de estos dos dispositivos realizan el proceso de autenticación. Por falta de comunicación directa entre los dispositivos, se hace posible hacer secuestros de sesión, explotando la ausencia de acople.[52]

[52] Ibíd. p 9

5. DISEÑO METODOLÓGICO

5.1 UNIDAD DE ANÁLISIS

Este proyecto está orientado a verificar el nivel de seguridad en general de las redes inalámbricas, tomando como referencia las redes inalámbricas ubicadas en el entorno, como empresas, centros comerciales y hogares, en la ciudad de Bogotá.

5.2 POBLACIÓN Y MUESTRA

5.2.1 Población. Con la elaboración de esta monografía se pretende llegar a que se utilice para la evaluación de redes inalámbricas que se encuentren ubicadas en los sectores productivos de la ciudad de Bogotá, donde se aplique la guía producto de este proyecto y así determinar las vulnerabilidades de estas redes inalámbricas.

5.2.2 Muestra. A la muestra para el desarrollo del proyecto se aplica a redes inalámbricas y de hogar, así como también en ambientes simulado, realizando de esta manera el procedimiento para las pruebas de pentest desde dispositivos móviles con sistema operativo Android, utilizando herramientas gratuitas.

5.3 ESTUDIO METODOLÓGICO

Este proyecto se basa en investigación descriptiva, proyectiva e interactiva, mediante la cual tiene como objetivo generar un procedimiento para realizar pruebas de pentest en redes inalámbricas desde dispositivos con sistema operativo Android, para descubrir vulnerabilidades en dichas redes.

5.3.1 Investigación Descriptiva. La investigación descriptiva tiene como objetivo central lograr la descripción o caracterización del evento de estudio dentro de un contexto particular. Según Dankbe (1986, c.p. Hernández Sampieri y otros, 1991), los estudios descriptivos son aquellos que buscan especificar las propiedades importantes de personas, grupos, comunidades, objetos o cualquier otro evento sometido a investigación; en otras palabras, miden diversos aspectos o dimensiones del evento investigado[53].

[53] HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. Pág. 224.

5.3.2 Investigación Proyectiva. También conocido como “proyecto factible”, consiste en la elaboración de una propuesta o modelo para solucionar determinadas situaciones. Se ubican las investigaciones para el diseño de programas de intervención social, de maquinarias, de programas informáticos, de inventos. Este tipo de investigación se ocupa de cómo deberían se las cosas, para alcanzar unos fines y funcionar adecuadamente[54].

5.3.3 Investigación Interactiva. La investigación interactiva implica la realización de acciones por parte del investigador, ya sea solo o conjuntamente con algún grupo o comunidad, con el propósito de modificar situaciones concretas a través de la aplicación de proyectos previamente diseñados. Para ello es necesario partir de proceso de indagación y explicación, visualizar posibilidades futuras, planificar un conjunto de actividades o diseñar alguna propuesta, y posteriormente llevarlas a cabo. La investigación interactiva ejecuta acciones para modificar un evento, y recoge información durante el proceso con el fin de reorientar la actividad[55].

[54]Ibid, pág. 325.
[55]Ibid, pág. 351.

6. METODOLOGÍAS PARA REALIZACIÓN DE PENTEST

Para el desarrollo de procedimiento de pruebas de pentest, se la seleccionado la metodología Issaf, teniendo en cuenta sus fases y etapas que son adaptables a la guía producto del presente trabajo, en el análisis de las vulnerabilidades presentes en las redes inalámbricas, objeto del proyecto.

6.1. Metodología ISSAF.

ISSAF o *InformationSystems Security Assessment Framework* por sus siglas en inglés, es una metodología estructura de análisis de seguridad, esta metodología para pruebas de penetración está concebida para realizar evaluación de una red, y sistemas. Está enfocada en tres fases, y 8 pasos de evaluación.

Las tres fases incluidas son:

Planificación y preparación. En esta etapa se realiza el levantamiento de la información, igualmente se planea y prepara la prueba, donde se aclara los términos, temas legales, los privilegios con que se otorgara, fechas y tiempos en los que realizara la prueba, es importante que se dejen claras las condiciones por ambas partes antes de realizar la prueba y evitar futuros inconvenientes.

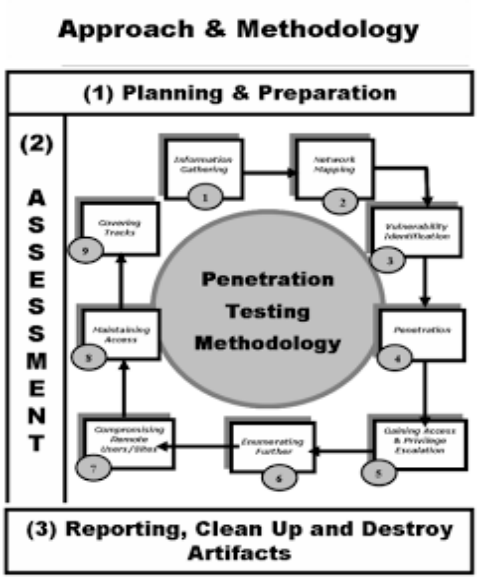
En esta etapa se identifican las siguientes fases:

- Identificación de contactos de ambas partes
- Definición de alcance, enfoque, método, privilegios entre otros

Evaluación. En esta etapa es en la cual se realizan las pruebas de penetración, para realizar esta evaluación es recomendable tener en cuenta estas los siguientes aspectos en y de acuerdo con el esquema de la figura:

- Recolección de Información
- Mapeo de la red de trabajo
- Identificación de vulnerabilidades
- Penetración
- Obtener Acceso y escalada de privilegios
- Enumeración
- Comprometer usuarios remotos y sitios
- Mantener Acceso

Figura 1. Diagrama de metodología ISSAF



Fuente: (INSECURE DATA, 2009)

Reportes, Limpieza y Destrucción de Objetos. Es en esta etapa donde se presentan los reportes de la evaluación, en caso de hallar una vulnerabilidad critica, esta debe ser informada de manera inmediata con el fin que la organización sea consciente de la situación, y que se busquen las medidas necesarias para contrarrestar los problemas críticos identificados.

Una vez concluidos todas las acciones definidas en las fases anteriores es decir terminada la prueba, se realiza un informe describiendo los resultados de las pruebas y las recomendaciones de mejora. Dicho informe contiene una estructura definida y documentación adecuada, dentro de los ítems que deben incluir se encuentran:

- Resumen de la Gestión realizada
- El alcance dado al proyecto
- Mencionar las herramientas utilizadas
- Las fechas y horas en las que se llevaron a cabo las pruebas.
- Los resultados de las pruebas realizadas (Los análisis de vulnerabilidad podrían adjuntarse como anexos).

Los documento o datos creados o almacenados dentro del sistema evaluado no pueden permanecer en el, si por algún motivo no fuese posible eliminar esta información por parte del evaluador, debe quedar consignado en el informe con las

rutas lógicas para que el personal con la competencia dentro del sistema se encargue de eliminarla.[56]

6.2 HERRAMIENTAS DE SOFTWARE LIBRE

Fueron seleccionadas cinco herramientas que cumplen con las características requeridas para cumplir con el objetivo del proyecto tal como se muestra a continuación con las características principales de cada una de ellas.

6.2.1 Routercheck: Es una sencilla herramienta para teléfonos inteligentes, diseñada para realizar un chequeo del estado de un router, pensada para realizar análisis a los router de hogar, es capaz de comunicarse con un servidor que permite verificar los últimos ataques lanzados para comprobar si el router es vulnerable a ellos, es muy fácil de usar, pero el análisis que realiza de manera automática es avanzado, verificando:

Configuración. Verificando que no haya configuraciones que representen peligros.

Contraseña. Verifica que se haya cambiado la contraseña por defecto del router o que no sea una de las comunes que se encuentran en los listados o diccionarios de los hackers.

Firmware. Verifica que el firmware sea el último actualizado por el fabricante.

Vulnerabilidades. Realizar un análisis de vulnerabilidades conocidas para el modelo y firmware del router.

Puertos abiertos. Verifica los puertos abiertos en internet.

DNS. Verifica si el DNS es confiable y seguro.

Resolución. Si halla algún inconveniente en el router de los analizados, muestra la guía para su solución.[57]

6.2.2 Dsploit. Es una aplicación para los dispositivos con sistema operativo Android desarrollada por Simone Margaritelli, está compuesta por varios paquetes que permiten realizar análisis de seguridad en redes inalámbricas, dentro de las funcionalidades se puedes destacar:

---

[56]ARAOZ, I. Metodología de test de intrusión ISSAF. [En línea] abril de 2009 [citado 19 de octubre de 2017] disponible en: http://insecuredata.blogspot.com.co/2009/04/metodologia-de-test-de-intrusion-issaf.html

[57] ROUTERCHECK. Routerchek [En línea] 2014 [Citado 20 de octubre de 2017] Disponible en: http://www.routercheck.com/

- Mapeo de puertos
- Búsqueda de vulnerabilidades
- Descifrado de contraseñas
- Ataques de hombre en el medio[58]

6.2.3 Wifinpect. Es una aplicación para sistema operático Android que permite que realice un monitoreo a redes inalámbricas, así como también verificar los dispositivos que se encuentran conectados a la red, en busca de vulnerabilidades así mismo análisis de tráfico que se genere. Dentro de sus funcionalidades destacadas están:

host information. Esta función permite detectar los equipos conectado en la red y conocer la información básica del host seleccionado.
portscan. Esta funcionalidad permite conocer los puertos abiertos en el equipo

Host VulnerabilityScan. Esta funcionalidad realiza un scan en busca de vulnerabilidades en el equipo host.

Access Point Scan. Realizar un análisis de la red en busca de los puntos de acceso, y devuelve la información sobre ellos.

Access Point Security Test. Esta función verifica la seguridad de la red inalámbrica, tal como es la clave de acceso.

Internal/External Network VulnerabilityScan. Esta funcionalidad busca vulnerabilidades internas o servidor externo y devuelve los datos.[59]

6.2.4 Fing – Network Tools. Es una aplicación para dispositivos con sistema operativo Android, que permite principalmente descubrir intrusos en la red inalámbrica, las funcionalidades que ofrece este aplicativo son:

- Asignar nombre al dispositivo
- Agregar notas
- Asignar iconos
- Descubrir los puertos abiertos
- Realizar ping

[58] FRANCESCO, Umberto. dSploit: Pentesting& Hacking WiFi desde Android. Mayo de 2014. [En línea] [Citado 25 de noviembre de 2016] disponible en: http://jadcode.blogspot.com.co/ 2014/05/ dsploit-pentesting-hacking-wifi-desde.html
[59]VELASCO, Rubén. Monitoriza la red con Wifinspect [En línea] 27 de mayo de 2013 [Citado 21 de octubre de 2017] Disponible en: https://www.redeszone.net/2013/05/27/monitoriza-la-red-con-wifinspect-ii/

- Realizar tracert
- Wake onlan

También permite guardar un registro de las redes que se han analizado.[60]

6.2.5 Intercepter-NG. Es una aplicación para dispositivos Android, que permite capturar el tráfico dentro de una red local, mediante atacas ARP, el uso más común que tiene esta herramienta es la auditoría de seguridad de caja negra evitando ser descubierto, permite descubrir los dispositivos conectados a la red inalámbrica, es posible realizar análisis profundos de los paquetes que transitan por la red, puesto que posee un snifer de tráfico general. Una de sus desventajas es que requiere ser root.[61]

6.2.6 Evaluación de herramientas. Para realizar la selección de la herramienta se han seleccionado las 5 descritas anteriormente, a las cuales se asigna un puntaje de entre 1 y 5, (donde 1 corresponde al puntaje más bajo y 5 el máximo puntaje a obtener), a cada una de las características que muestran en la siguiente tabla:

Tabla 1. Evaluación de herramientas

HERRAMIENTA / ASPECTOS A EVALUAR	Routercheck	Dsploit	Wifinspect	Fing-networktools	Intercepter-NG
Facilidad de manuales de uso	3	3	2	2	2
Complejidad de instalación	5	3	4	4	4
Optimización de recursos del sistema	5	1	3	2	4
Funcionalidades	5	5	5	5	5
Facilidad de uso	4	4	4	4	4
Informes de remediación	5	2	3	4	3
TOTAL PUNTOS	**27**	18	21	21	22

Fuente: autor

[60] MILLA ANCIN, David. Android: Cómo Administrar Nuestra Wifi con Fing. [En línea] 12 de diciembre de 2014 [Citado 25 de octubre de 2017]. Disponible en: http://curiotek. com/2014/12/12/android-como-administrar-nuestra-wifi-con-fing/

[61] SANCHO AZCOITIA, Sergio. Intercepter-NG: Auditar la red WiFi desde tu Android. [En línea] mayo 4 de 2016 [citado 25 de octubre de 2017]. Disponible en: http://www.elladodelmal. com/2016/05/intercepter-ng-auditar-la-red-wifi.html

Luego de analizar cada uno de los aspectos definidos a evaluar para cada una de las herramientas seleccionadas, y luego de asignar los puntos por cada uno ellos y como lo muestra la tabla, con los resultados, la herramienta que se ha seleccionado es routerchek.

A continuación, se encuentra en detalle el análisis de cada uno de los aspectos para cada una de las herramientas.

6.2.6.1 Facilidad de manuales de uso. Para evaluar este aspecto se considera la oportunidad en la consecución de manuales de uso, de cada una de las herramientas.

Routercheck. En el siguiente se encuentra una guía sobre los pasos para el uso del software.[62]

Dsploit. Para esta herramienta hay foros donde hay pequeñas instrucciones de uso, también se encuentran video tutoriales, como por ejemplo el siguiente[63]:

Wifinspector. Manual de uso para esta herramienta no se encuentran, solo hay foros donde se explica la aplicación de cada una de sus funcionalidades[64], como se muestra en el siguiente link: https://www.redeszone.net/2013/05/27/monitoriza-la-red-con-wifinspect-ii/

Fing-networktools. No se encontró manuales de uso de esta aplicación, se encentra información sobre características aplicaciones, y video tutoriales cortos como[65], por ejemplo: https://www.youtube.com/watch?v=k7A9rsvbBfE

Intercepter-NG. No se encontraron manuales de uso completos, solo foros donde muestran algunas pautas y descripción de funcionalidades[66], por ejemplo: http://www.elladodelmal.com/2016/05/intercepter-ng-auditar-la-red-wifi.html

---

[62] REDES ZONE. Comprueba la seguridad de tu router desde android. [En línea] mayo 4 de 2016 [citado 25 de octubre de 2017]. Disponible en: https://www. redeszone.net/2015/05/25/ routercheck-comprueba-la-seguridad-de-tu-router-desde-android/

[63] YOUTUBE. ¿Como hackear desde Android WiFi con dSploit? [En línea] mayo 4 de 2016 [citado 25 de octubre de 2017]. Disponible en: https://www.youtube.com/watch?v=c4fMQHoP7LA

[64] REDES ZONE. Monitoriza la red con Wifinspect. [En línea] mayo 4 de 2016 [citado 25 de octubre de 2017]. Disponible en: https://www.redeszone.net/2013/05/27/ monitoriza-la-red-con-wifinspect-ii/

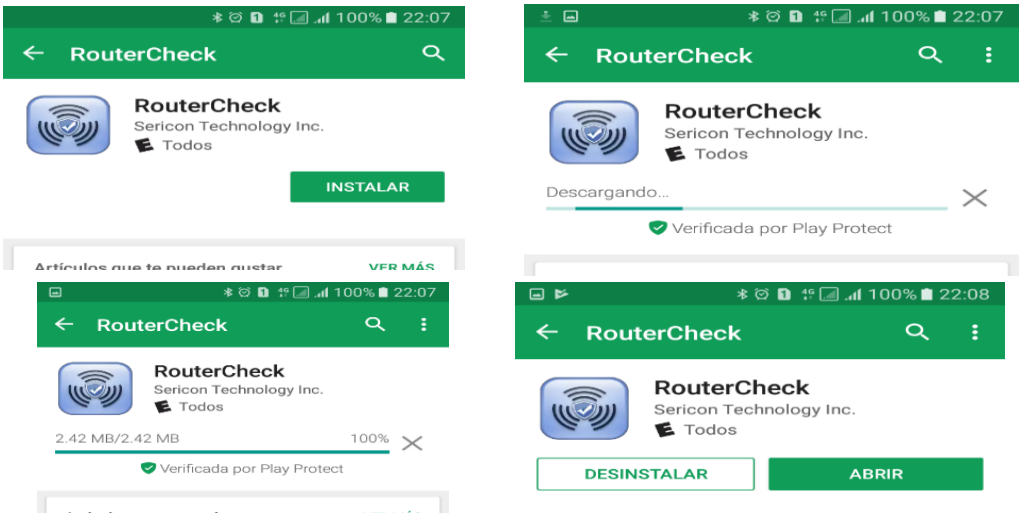
[65] YOUTUBE. Tutorial básico de la aplicación de móvil Fing. [En línea] mayo 4 de 2016 [citado 25 de octubre de 2017]. Disponible en: https://www.youtube.com/watch?v=k7A9rsvbBfE

[66] Ellado del mal. Un informático en el lado del mal: Intercepter-NG: Auditar la red WiFi. 2016. [En línea] mayo 4 de 2016 [citado 25 de octubre de 2017]. Disponible en: http://www.elladodelmal.com/ 2016/05/intercepter-ng-auditar-la-red-wifi.html

6.2.6.2 Complejidad de instalación. Para este aspecto se tiene en cuenta la facilidad en la instalación, consecución del instalador, si es necesario root del dispositivo y peso del archivo.

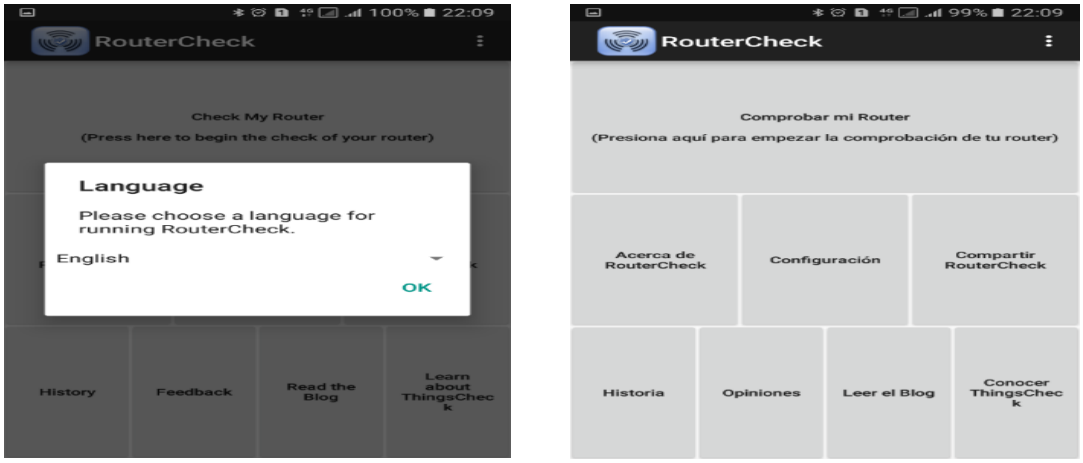
Routercheck. Esta aplicación no requiere root en el dispositivo, se encuentra en la playstore, es muy liviano (2,42MB) y su instalación es muy sencilla. Solo basta con dar clic en el botón instalar y él se ejecuta y se instala luego pide seleccionar el idioma y está listo para ser usado.

Figura 2. Instalacion routercheck



Fuente: autor

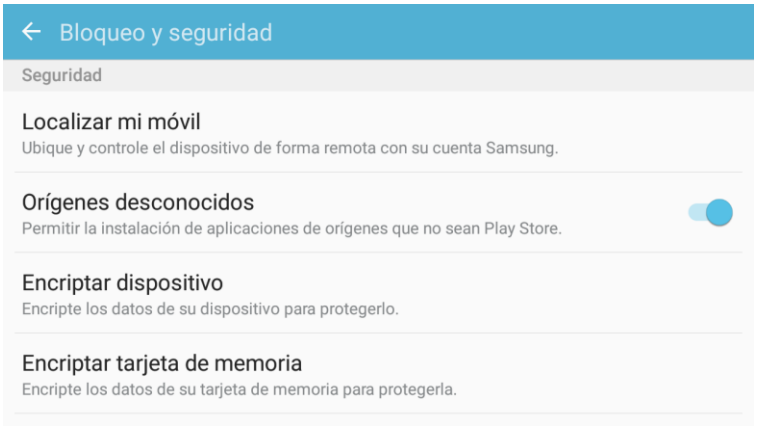
Figura 3. Configuracion de routercheck



Fuente: autor

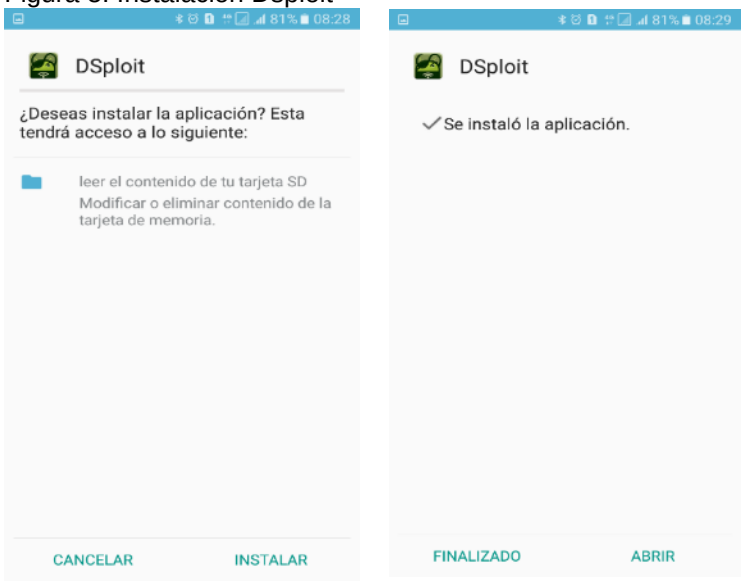
Dsploit. Esta herramienta no se encuentra en el playstore, se debe descargar el apk, desde la página https://dsploit.es.aptoide.com/, tiene un tamaño de 10MB, para realizar la instalación se debe habilitar la opción en el dispositivo orígenes desconocidos y posterior ejecutar el apk.

Figura 4. Configuración del dispositivo



Fuente: autor

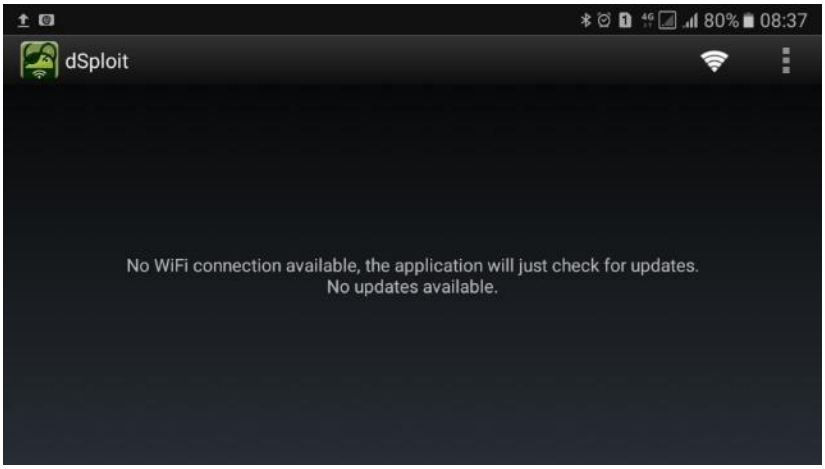
Figura 5. Instalación Dsploit



Fuente: autor

Posterior muestra que ya se instaló y está listo para ser usado

Figura 6. Dsploit instalado



Fuente: autor

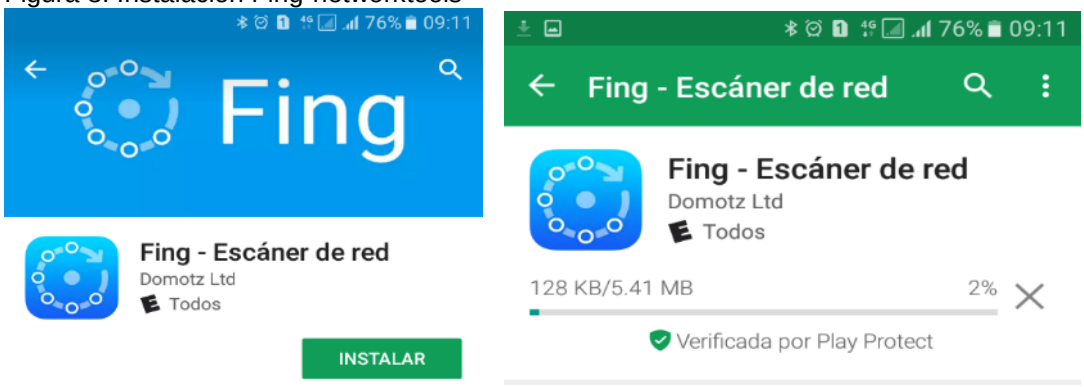
Wifinspector. Este aplicativo requiere root en el dispositivo, se encuentra en el playstore tiene un tamaño de 9,16MB y su instalación es sencilla solo basta con buscarlo y luego dar clic para iniciar la instalación, una vez ha terminado se abre, pide permisos de root y luego ya es posible iniciar con su uso.

Figura 7. Instalación Wifinspect

Fuente: autor

Fing-networktools. Esta aplicación se encuentra en la playstore, su tamaño es de 5,41MB no requiere de root en el dispositivo, es sencilla de instalar, solo basta con buscar en la playstore dar clic en el botón instalar y esperar unos cuantos segundos que termine a instalación y empezar a usar.

Figura 8. Instalación Fing-networktools



Fuente: autor

Figura 9. Fing-networktools

Fuente. autor

Intercepter-NG. sta aplicación no se encuentra en la playstore por lo que es necesario bajar el apk, el cual está disponible en su página oficial http://sniff.su/download.html su tamaño es de 5,2MB y requiere root en el

dispositivo, para su instalación solo basta con habilitar los orígenes desconocidos en el dispositivo y ejecutar el apk.

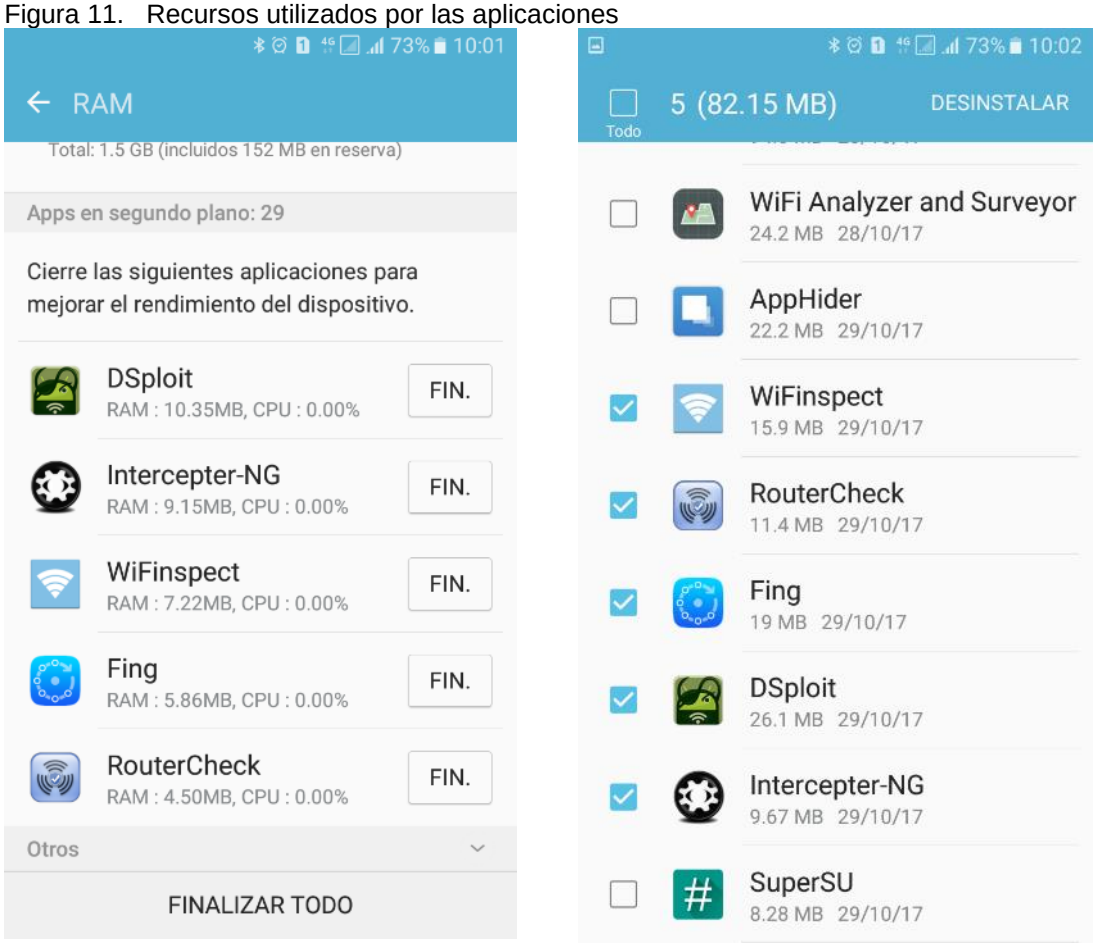
Figura 10. Instalación Interceptor-NG

Fuente: autor

6.2.6.3 Optimización de recursos del sistema

Routercheck. En este aspecto se mide los recursos del dispositivo que utiliza cada una de las aplicaciones caso de evaluación, para otorgar el mayor puntaje a la herramienta que menos recursos consume. En la siguiente figura se observa el consumo de memoria y espacio que utiliza cada una de las 5 aplicaciones instaladas en el dispositivo.

Figura 11. Recursos utilizados por las aplicaciones



Fuente: autor

6.2.6.4 Funcionalidades. Para evaluar este aspecto se verifica la funcionalidad que poseen las herramientas y si estas generan valor al proyecto, para ello se tienen en cuenta las principales funcionalidades de cada aplicativo.

Routercheck. Sus principales funcionalidades son:

- Verificación de configuración.
- Verifica que el router no tenga la contraseña por defecto
- Identifica que el router tenga el ultimo firmware
- Análisis de Vulnerabilidades.
- Puertos abiertos.
- Confiabilidad del DNS.
- Resolución de problemas

Dsploit. Las principales funcionalidades de dsploit son:

- Mapeo de puertos
- Búsqueda de vulnerabilidades
- Descifrado de contraseñas
- Ataques de hombre en el medio

Wifinspector. Las principales funcionalidades de wifinspector:

- Levantamiento de información de los hosts
- Escaneo de puertos
- Búsqueda de vulnerabilidad de los Host
- Búsqueda de puntos de acceso
- Test de seguridad de puntos de acceso.
- Escaneo de vulnerabilidad de red interna / externa

Fing-networktools. Las principales funcionalidades de fingnetworktools son:

- Asignar nombre al dispositivo
- Agregar notas
- Asignar iconos
- Descubrir los puertos abiertos
- Realizar ping
- Realizar tracert
- Wake onlan

Intercepter-NG. Las principales funcionalidades de Intercepter-NG son:

- Descubre lo dispositivos conectados en la red.
- Información sobre dispositivos
- Análisis de tráfico de red
- Análisis de exhaustivo de paquetes
- Recuperación de contraseñas
- Recuperación de archivos

6.2.6.5 Facilidad de uso. En este aspecto se evalúa la facilidad para utilizarlas y lograr los resultados esperados.

Las 5 herramientas seleccionadas son intuitivas y sencillas de usar, los menús son claros y de fácil entendimiento, por lo que se otorga a todas las herramientas el mismo puntaje en este aspecto.

6.2.6.6 Informes de remediación. En este aspecto se califica el detalle del informe de los análisis realizados, así como la soluciones que plantean o sugerencias de las mismas.

Routercheck. Routercheck entrega un informe detallado del problema encontrado, entregando también información de contextualización sobre los temas relacionados con la vulnerabilidad encontrada, posible solución y ofrece la posibilidad en algunos casos de solucionarla de manera automática. Lo que hace que la remediación de problemas sea muy completa y acertada.

Dsploit. Muestras las vulnerabilidades o fallas de seguridad encontrados en la red inalámbrica, pero no muestra informes detallados de los mismos, así como tampoco las posibles soluciones para corregirlos o solventarlos.

Wifinspect. No cuenta con sugerencias para remediación de los problemas encontrados, solo hace un informe con los fallos de seguridad detectados, lo que significa una debilidad ya que se debe conocer del tema para poder dar solución a los reportes que entrega la aplicación.

Fing-networktools. La herramienta fingnetworktools en el reporte que entrega al realizar el análisis de vulnerabilidad, muestra los detalles de los de los resultados de manera informativa, es decir, no presenta una guía de la manera como se puede brindar solución de las fallas detectadas.

Intercepter-NG. Esta aplicación entrega un informe detallado del tráfico que presenta la red, con lo que permite hacer análisis de los paquetes que se transfieren, pero no entrega una guía sobre la solución a las vulnerabilidades que presenta la red inalámbrica ni recomendación para tal fin.

7. DESARROLLO DE LA INVESTIGACIÓN

7.1 PROCEDIMIENTO PARA REALIZAR PRUEBAS DE PENTEST EN REDES INALÁMBRICAS UTILIZANDO DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID

A continuación, se presenta una guía paso a paso para realizar un análisis de falencias de seguridad en una red inalámbrica, desde un dispositivo móvil con sistema operativo Android, apoyado en una herramienta gratuita, que permite de manera sencilla y eficaz identificar aquellas vulnerabilidades presentes en la red inalámbrica que son un peligro latente de ser explotadas y recibir ataques, que exponen la información del sistema informático, ya sean bases de datos o datos personales almacenados en cualquiera de los dispositivos que se encuentre conectado a la red.

7.1.1 Alcance. Este procedimiento está diseñado para ser aplicado en las redes inalámbricas con topología estándar basadas en protocolo IEEE 802.11 b/g/n, con cifrado de seguridad WAP y WAP2. Para realizar el test se debe tener el aval pertinente ya que de lo contrario se podría incurrir en un delito, y así mismo tener el acceso a la red desde el dispositivo móvil.

7.1.2. Fallas de seguridad comunes. Aunque en la actualidad los sistemas de redes inalámbricas cuentan con los elementos necesarios para ser muy seguras, se encuentra redes que presentan grandes falencias de seguridad, y es que como es conocido no hay sistemas ciento por ciento seguros, debido a que las fallas humanas no se pueden erradicar de manera definitiva y esto sumado a la evolución en el desarrollo de las técnicas y sistemas de ataques, por lo anterior existen fallas de seguridad que es común que se encuentren en las redes inalámbricas en especial en redes de pequeñas empresas y hogares donde no da tanta relevancia al fortalecimiento en la seguridad de los sistemas informáticos en general, dentro de las fallas comunes se encuentran.

- **Fallas de configuración.** Una de las fallas más frecuentes en todos los sistemas y en las redes inalámbricas es la configuración de los dispositivos que conforman las redes. Esto debido a que no siempre se tienen los especialistas que están en capacidad de una óptima configuración por diversos motivos propios de cada organización, dentro de las falencias de configuración más comunes se encuentran.

a) **Contraseñas por defecto.** Una de las fallas de seguridad más frecuentes en las redes inalámbricas, es el hecho de mantener en los puntos de acceso los usuarios y contraseñas por defecto de los fabricantes. Debido a que estos usuarios cuentan con privilegios para administración de los dispositivos. La recomendación de seguridad en lo posible desactivar estos usuarios y crear usuarios diferentes, en caso contrario que se deba mantener estos usuarios cambiar la contraseñas, utilizando contraseñas fuertes que sean difíciles de adivinas o descifrar.

b) **Usuario de administración remota.** Otra de las fallas comunes es dejar activo los puertos de administración o gestión remota, esto ocasiona que el dispositivo sea visible y accesible desde internet, lo que puede posibilitar un ataque. La recomendación de seguridad es desactivar la administración remota o en su defecto cambiar los puertos y usuarios para tal fin.

c) **DMZ.** Los router cuentan con una zona desmilitarizada o DMZ, la cual permite direccionar servicios a una dirección IP dentro de la red LAN, permitiendo que se abran los puertos necesarios para publica los servicios requeridos. Esto a menudo se convierte en una falencia de seguridad puesto que se deja activa sin que sea utilizada, lo que hace que estén presentes huecos de seguridad o puertas traseras como se les conoce, la recordación es desactivar esta funcionalidad del dispositivo, a menos que se requiera en cuyo caso se debe configurar con todas las medidas de seguridad pertinentes.

d) **Wi-Fi Protected Setup** (**WPS).** Es un estándar que fue incluido como una funcionalidad que permite conectar de manera sencilla los dispositivos sin digitar la contraseña, el Router genera un código de 8 dígitos, el dispositivo debe introducir este código y así valida el acceso a la red. Pero esto se puede convertir en un foco inseguridad, a ataques de fuerza fruta para conseguir este código e ingresar son autorización a la red inalámbrica. Por ende, se recomienda como medida de seguridad prescindir de esa funcionalidad, desactivándolo en los dispositivos de la red.

e) **Administración.** Dentro de la administración de sistemas de redes inalámbricas una tarea relevante y necesaria es realizar un seguimiento continuo, que permita identificar los dispositivos que se conectan a la red, con el fin de detectar intrusos, realizar cambio de contraseñas periódicamente, y por su puesto realizar la verificación de la configuración para evitar las falencias expuestas en los puntos anteriores.

Las falencias de seguridad descritas anteriormente, sumados a las vulnerabilidades expuestas en el capítulo 4 de este documento, muestran que las redes inalámbricas están expuestas a constantes amenazas de sufrir ataques explotando todas las posibles falencias de seguridad. Pero para contrarrestar esta situación existen mecanismos para su detección, y así corregir o mitigar todas esas vulnerabilidades.

7.1.3. Herramientas para Ethical Hacking. Existen en el mercado una gran variedad de herramientas para realizar análisis de vulnerabilidades de las redes inalámbricas, hay comerciales, gratuitas, multiplataforma, para sistemas específicos, a continuación, se mencionan algunas de las más conocidas estas herramientas.

- **Nmap.** Esta es una herramienta de código abierto, es una de las herramientas más conocidas utilizada para el análisis de red, permite verificar la seguridad de un sistema informático, incluso de manera remota, entre sus principales funciones permite detección de puertos abiertos, puede medir el uso de los servicios de la red, permite verificar la configuración del equipo, las actividades de los equipos en la red, entre otras funciones.[67]

- **Metasploit.** Exploit se conoce a partes pequeñas de software creadas para detectar y explotar vulnerabildades presentes en aplicaciones o sistemas de software, esta herramienta es una de las suites más grandes, que posee una gran cantidad de exploits que permiten analizar la seguridad de un sistema, así como la fortaleza frente a estos tipos de ataques informáticos. Esta herramienta es de pago, y aunque tiene un alto costo es una de las utilizadas por especialistas de ethical hacking e investigadores de seguridad. Aunque también cuenta con una versión limitada y gratuita orientada para estudiantes y actividades básicas.[68]

- **Wireshark.** Es un sniffer que cuenta con características estándar de un analizador de protocolos, dispone de una interfaz gráfica sencilla y de fácil uso, permite ver todo el tráfico de la red, dentro de sus principales características se encuentran:

  - Disponible para Linux y Windows
  - Captura de paquetes en vivo desde una interfaz de red

[67] Velasco, Rubén. Las mejores 10 herramientas para hacking ético de este 2015. [En línea] 5 de diciembre de 2015 [Citado 16 de febrero de 2018]. Disponible en: https://www.redeszone.net/2015/12/05/las-mejores-10-herramientas-para-hacking-etico-de-este-2015/
[68] Ibid.

- Muestra los paquetes con información detallada de los mismos
- Abre y guarda paquetes capturados
- Importar y exportar paquetes en diferentes formatos
- Filtrado de información de paquetes
- Resaltado de paquetes dependiendo el filtro
- Crear estadísticas

Es una herramienta de código abierto, que resulta muy útil para realizar escaneos profundos a fin encontrar vulnerabilidades.[69]

- **Nessus.** Es analizador muy potente y sencillo de usar, cuenta con una gran base de datos de plugis que actualiza todos los días, actualmente es uno de los productos más utilizados e importantes de este tipo. Es un software multiplataforma, que consta de un daemon llamado nessusd el cual realiza escaneo en el sistema y un nessus el cliente que visualiza el avance e informa del estado mediante una consola gráfica.
  Las pruebas de vulnerabilidad, de las que dispone en una lista de plugins, son guardadas en NASL que es un lenguaje de ataque nessus. Tiene la opción de exportar los resultados del escaneo en varios formatos como, texto, XML, HTML y latex, los resultados también pueden ser incluidos en una base de conocimiento como referencia en posteriores escaneos de vulnerabilidades. Ciertas pruebas de vulnerabilidad de Nessus podrían ocasionar que los sistemas operativos y servicios se corrompan o se caigan, para prevenir que esto suceda se debe desactivar la opción unsafe test (pruebas no seguras) antes de iniciar el escaneo. Los análisis siguen ejecutándose en el servidor, pese a que se desconecte por cualquier motivo.[70]

- **Herramientas para Android.** Dentro de la gran cantidad de herramientas presentes, existen unas compatibles para sistema operativo Android, a continuación, se mencionan las herramientas que se seleccionaron para el presente proyecto, las cuales fueron las siguientes.

  a) **Routercheck:** Es una sencilla herramienta para teléfonos inteligentes, diseñada para realizar un chequeo del estado de un router, pensada para realizar análisis a los router de hogar, es capaz de comunicarse con un servidor que permite verificar los últimos ataques lanzados para comprobar

[69]Ibid.
[70]Dragonjar, Laboratorios: Hacking – Técnicas y contramedidas – Escaneo de vulnerabilidades III. [En linea]. Sin fecha. [citado 16 de febrero de 2018]. Disponible en: https://www.dragonjar.org/laboratorios-hacking-tecnicas-y-contramedidas-escaneo-de-vulnerabilidades-iii.xhtml

si el router es vulnerable a ellos, es muy fácil de usar, pero el análisis que realiza de manera automática es avanzado, verificando:

Configuración. Verificando que no haya configuraciones que representen peligros.

Contraseña. Verifica que se haya cambiado la contraseña por defecto del router o que no sea una de las comunes que se encuentran en los listados o diccionarios de los hackers.

Firmware. Verifica que el firmware sea el último actualizado por el fabricante.

Vulnerabilidades. Realizar un análisis de vulnerabilidades conocidas para el modelo y firmware del router.

Puertos abiertos. Verifica los puertos abiertos en internet.

DNS. Verifica si el DNS es confiable y seguro.

Resolución. Si halla algún inconveniente en el router de los analizados, muestra la guía para su solución.[71]

b) **Dsploit.** Es una aplicación para los dispositivos con sistema operativo Android desarrollada por Simone Margaritelli, está compuesta por varios paquetes que permiten realizar análisis de seguridad en redes inalámbricas, dentro de las funcionalidades se puedes destacar:

- Mapeo de puertos
- Búsqueda de vulnerabilidades
- Descifrado de contraseñas
- Ataques de hombre en el medio[72]

c) **Wifinpect.** Es una aplicación para sistema operático Android que permite que realice un monitoreo a redes inalámbricas, así como también verificar los dispositivos que se encuentran conectados a la red, en busca de

[71] ROUTERCHECK. Routerchek [En línea] 2014 [Citado 20 de octubre de 2017] Disponible en: http://www.routercheck.com/

[72] FRANCESCO, Umberto. dSploit: Pentesting& Hacking WiFi desde Android. Mayo de 2014. [En línea] [Citado 25 de noviembre de 2016] disponible en: http://jadcode.blogspot.com.co/ 2014/05/ dsploit-pentesting-hacking-wifi-desde.html

vulnerabilidades así mismo análisis de tráfico que se genere. Dentro de sus funcionalidades destacadas están:

host information. Esta función permite detectar los equipos conectado en la red y conocer la información básica del host seleccionado.
portscan. Esta funcionalidad permite conocer los puertos abiertos en el equipo
Host VulnerabilityScan. Esta funcionalidad realiza un scan en busca de vulnerabilidades en el equipo host.

Access Point Scan. Realizar un análisis de la red en busca de los puntos de acceso, y devuelve la información sobre ellos.

Access Point Security Test. Esta función verifica la seguridad de la red inalámbrica, tal como es la clave de acceso.

Internal/External Network VulnerabilityScan. Esta funcionalidad busca vulnerabilidades internas o servidor externo y devuelve los datos.[73]

d) **Fing – Network Tools.** Es una aplicación para dispositivos con sistema operativo Android, que permite principalmente descubrir intrusos en la red inalámbrica, las funcionalidades que ofrece este aplicativo son:

- Asignar nombre al dispositivo
- Agregar notas
- Asignar iconos
- Descubrir los puertos abiertos
- Realizar ping
- Realizar tracert
- Wake onlan

También permite guardar un registro de las redes que se han analizado.[74]

e) **Intercepter-NG.** Es una aplicación para dispositivos Android, que permite capturar el tráfico dentro de una red local, mediante atacas ARP, el uso más común que tiene esta herramienta es la auditoría de seguridad de caja negra evitando ser descubierto, permite descubrir los dispositivos conectados a la

[73]VELASCO, Rubén. Monitoriza la red con Wifinspect [En línea] 27 de mayo de 2013 [Citado 21 de octubre de 2017] Disponible en: https://www.redeszone.net/2013/05/27/monitoriza-la-red-con-wifinspect-ii/
[74] MILLA ANCIN, David. Android: Cómo Administrar Nuestra Wifi con Fing. [En línea] 12 de diciembre de 2014 [Citado 25 de octubre de 2017]. Disponible en: http://curiotek. com/2014/12/12/android-como-administrar-nuestra-wifi-con-fing/

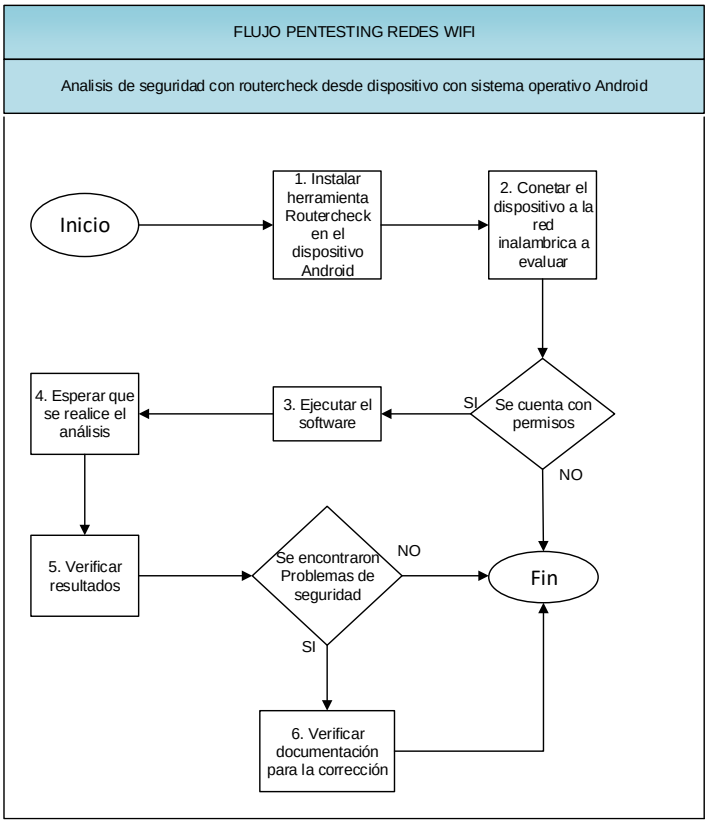
red inalámbrica, es posible realizar análisis profundos de los paquetes que transitan por la red, puesto que posee un snifer de tráfico general. Una de sus desventajas es que requiere ser root.[75]

7.1.4 Procedimientos paso a paso de pentesting. Para la realizar esta actividad de pentest se utiliza una aplicación gratuita llamada Routercheck, para realizar el procedimiento se requieren contar con los siguientes recursos:

- Dispositivo móvil con sistema operativo Android
- Conexión a internet
- El software super root (opcional)
- Acceso a la red inalámbrica a evaluar (permisos)
- Aplicación routercheck

[75] SANCHO AZCOITIA, Sergio. Intercepter-NG: Auditar la red WiFi desde tu Android. [En línea] mayo 4 de 2016 [citado 25 de octubre de 2017]. Disponible en: http://www.elladodelmal.com/2016/05/intercepter-ng-auditar-la-red-wifi.html

Figura 12. Icono de Root en Android



Fuente: autor

7.1.4.1 Rootear móvil con Android. Rootear un dispositivo con sistema operativo Android, consiste en asignar permisos elevado sobre el sistema operativo, más allá de las limitaciones que ha colocado el fabricante del software.

Advertencia. Un aspecto importante de este procedimiento es advertir que este procedimiento mal ejecutado puede causar daños sobre el dispositivo, y que para algunos proveedores de telefonía celular esta acción causa perdida de la garantía del dispositivo en caso de celulares y Tablet.

Este proceso se realiza, en unas acciones muy sencillas, los pasos para hacer la modificación de este sistema, este es específico para este modelo de teléfono.

Como paso número 1 se debe habilitar la opción de instalación desde fuentes desconocidos, para ello se sigue la cadena por los menús “Ajustes -> Pantalla bloqueo / Seguridad y se marca la check Fuentes desconocidas”

Posterior se descarga el archivo con extensión apk de super-root, requerido, la cual está disponible en: http://downloadsafe.org/file/0yF980

Con el archivo almacenado en el dispositivo móvil, se ejecuta de manera directa, al abrir se debe seleccionar installsuperSU en el primer menú.

Posterior se debe seleccionar la opción xploit y luego continuar con el proceso.

Este proceso demora unos minutos, una vez que termina la instalación la terminal se reiniciara automáticamente, cuando el sistema se inicia nuevamente el dispositivo debe estar rooteado, una manera de verificar es que aparece el icono de la aplicación **Supersu** dentro de las aplicaciones como se muestra en la figura 13.

Figura 13. Icono de Root en Android

Fuente: autor

7.1.4.2 Instalación de la herramienta routercheck. Es una sencilla herramienta para teléfonos inteligentes, diseñada para realizar un chequeo del estado de un router, pensada para realizar análisis a los router de una red, es capaz de comunicarse con un servidor que permite verificar los últimos ataques lanzados para comprobar si el router es vulnerable a ellos. Esta aplicación se encuentra dentro de las aplicaciones ofrecidas en la playstore lo que facilita de gran manera la instalación, para realizar la instalación basta con seguir estos sencillos pasos:

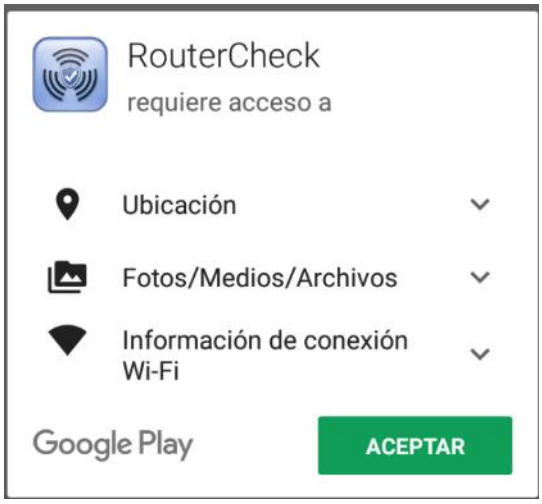
- Buscar en la playstore

Figura 14. Búsqueda de routercheck en la playstore

Fuente: autor

Luego se procede a dar clic sobre el botón instalar, posterior muestra la siguiente pantalla.

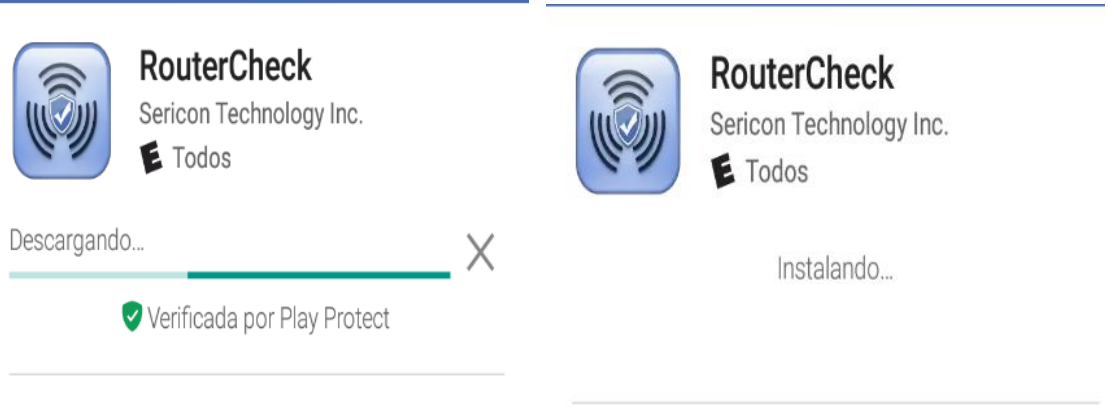
Figura 15.. Requisito de acceso de routercheck



Fuente: autor

Nuevamente se realiza clic sobre el botón aceptar, en pantalla se observa que se está realizando la descarga y posterior se muestra el progreso de instalación en el dispositivo.

Figura 16. Requisito de acceso de routercheck



Fuente: autor

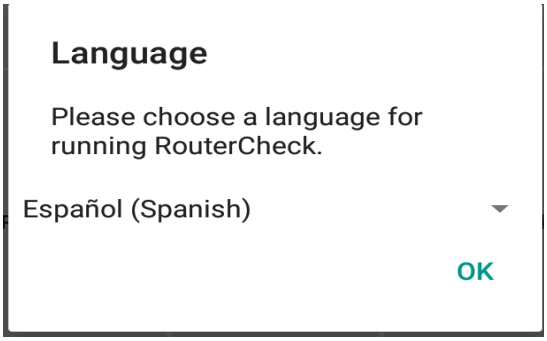
Luego de algunos segundos dependiendo de la velocidad de descarga del internet del dispositivo, indica que termino la instalación de la aplicación y se observa el icono dentro de las aplicaciones instaladas, también lo coloca por defecto en la pantalla de inicio del dispositivo si se tiene configurado el tema por defecto del Android.

Figura 17. Icono de Routercheck

Fuente: autor

Por último, se inicia la aplicación Routercheck para terminar la instalación configurando el idioma de preferencia, ya que la aplicación cuenta con varios idiomas y nos lo pregunta como requisito para terminar su instalación y poder utilizar la herramienta.

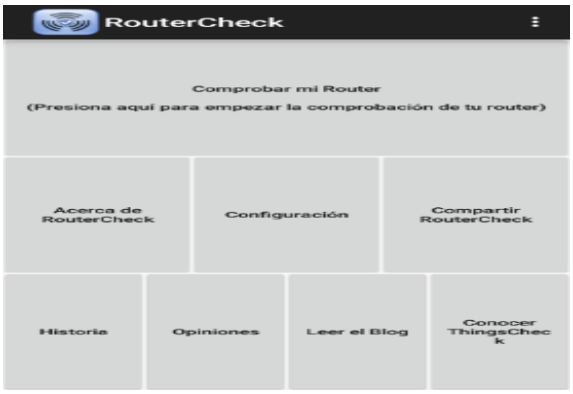
Figura 18. Configuración Routercheck



Fuente: autor

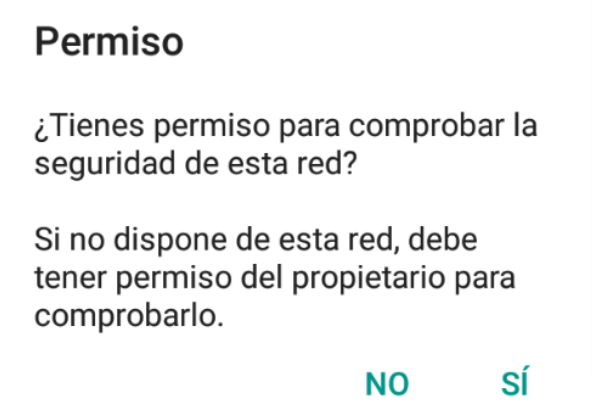
7.1.4.3 Prueba a la red inalámbrica con routercheck. Antes de ejecutar la aplicación se debe conectar el dispositivo a la red inalámbrica a evaluar, para ello se debe conocer la contraseña y disponer de los permisos para realizar el procedimiento, posterior se inicia la herramienta routercheck realizando clic sobre el icono, luego se hace clic sobre el icono comprobar mi router, donde se abre una ventana emergente con el título permiso, donde pregunta, si se tienen los permisos para comprobar la seguridad de la red, solo se hace clic en si y la aplicación inicia con la el evaluación.

Figura 19. Pantalla de inicio de Routercheck



Fuente: autor

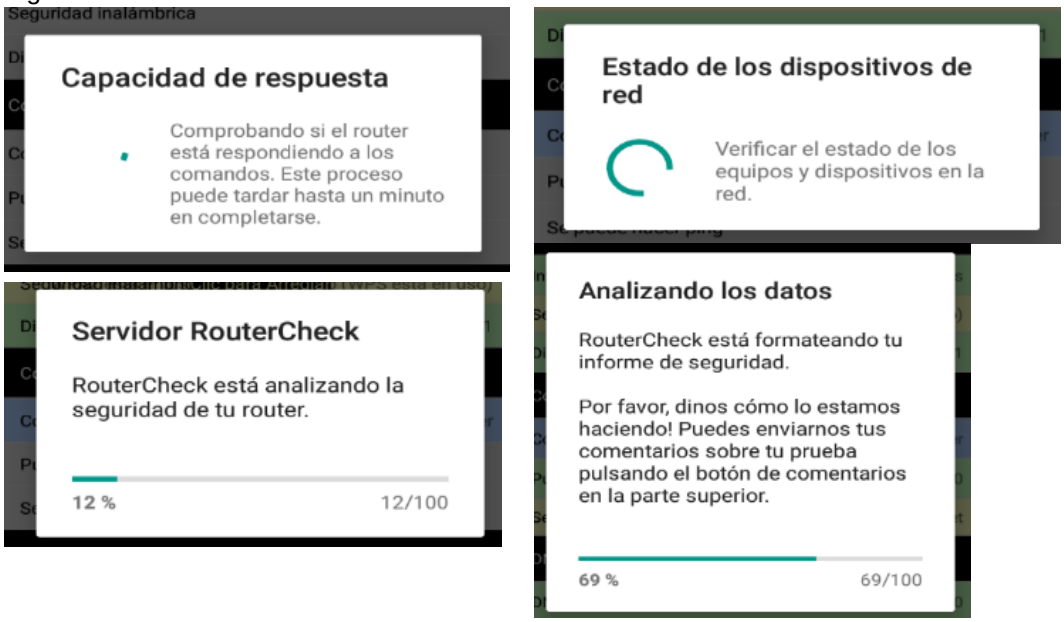
Figura 20. Pantalla permisos de Routercheck



Fuente: autor

A continuación, la herramienta inicia con el proceso de evaluación de la red, en este proceso muestra algunas pantallas de cada una de las etapas que lleva a cabo la aplicación durante el análisis, el tiempo que transcurre es relativamente corto, pero depende de algunas características propias de la red como la cantidad de dispositivos conectados, la complejidad de su topología y las vulnerabilidades presentes.

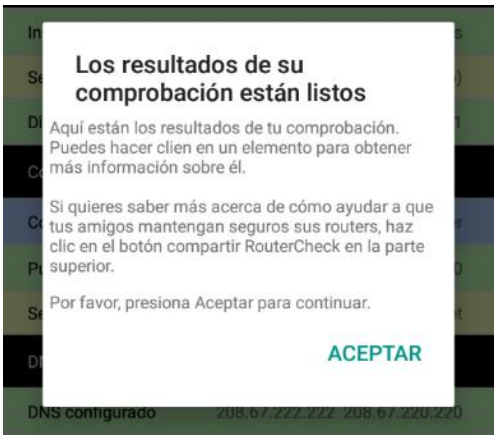
Figura 21. Routercheck durante la evaluación



Fuente: autor

7.1.4.4 Resultados del análisis de la red inalámbrica

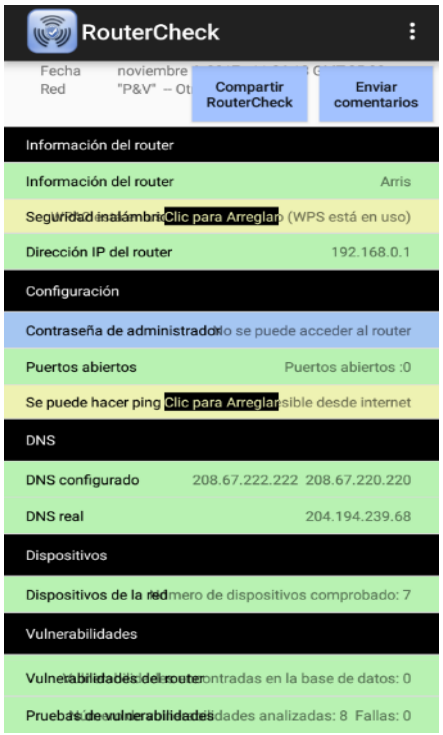
Figura 22. Routercheck resultados



Fuente: autor

Cuando la aplicación termina la muestra la ventana emergente donde indica que termino el procedimiento, como se observa en la figura 22, al dar clic en aceptar se accede al resultado de la evaluación.

Figura 23. Routercheck resumen de resultados



Fuente. Aplicación routercheck

En la figura 23 se muestra la pantalla de resultados que devuelve el aplicativo, en ella se muestran datos como:

- Nombre de red
- IP de router
- DNS configurado y real
- Numero de dispositivos de la red
- Las fallas detectadas

Al hacer clic sobre algunas de las líneas, muestra la información detallada sobre el ítem, y al hacer clic sobre la falla de seguridad detectada, entrega un informe detallado y una de las posibles maneras de solución, fuentes de información del tema, a continuación, se muestra el resultado de las unas fallas detectadas en el análisis de prueba realizado, donde se detalla cual es el problema, el riesgo que tiene con la falla, documentación del proveedor y la guía de solución. Para este caso la falla es que esta activo el WPS del router.

7.1.5. Resultado tomado de la aplicación routercheck. A continuación, se muestra los resultados con sugerencias realizadas por la aplicación para la solución de los problemas de vulnerabilidad encontrados.

“Arreglar el problema "WPS está activada" (Arris / UNKNOWN)

Nota: Si no puede solucionar el problema después de seguir estas instrucciones, tal vez podemos ayudar. Obtener

Aquí está tu problema

Estado	*WPA2 está en uso y es muy seguro (WPS está en uso)*

Comprender el problema «WPS está activada»

WPS (o configuración protegida Wi-Fi) es un sistema utilizado por muchos proveedores de router para hacer la tarea de configurar WiFi casa más fácil. Hay dos maneras que enrutadores habilitado WPS permiten conectar dispositivos: escribiendo en un perno (generalmente se encuentra en una pegatina en la parte inferior del router) o pulsando un botón en el router. Desafortunadamente, los hackers pueden entrar en enrutadores donde WPS está encendido, así que debe apagarse si es posible. Routers con WPS activado son presa fácil para los hackers, incluso si se utiliza WPA2.

Más información sobre este problema con el router de RouterCheck.

¿Cuál es el riesgo de no solucionar este problema?

La amenaza que para los problemas de seguridad WiFi es un poco diferente a las amenazas planteadas por otras vulnerabilidades. Un problema de seguridad WiFi es un problema muy localizado. Hackers a medio camino a través del mundo no pueden aprovecharse de la falta de seguridad WiFi y tratar de entrar en su red. La verdadera amenaza es con sus vecinos y personas en su vecindad inmediata de tratar de entrar en su red.

Gente local irrumpiendo en su red doméstica constituyen una amenaza muy diferente que hacer los piratas profesionales, y harán cosas muy diferentes. Considerando que los hackers organizados buscan para hacer dinero rápido encima por robar material sensible o volver a configurar la red para su beneficio, el aficionado local está buscando algo totalmente diferente.

En primer lugar, el aficionado puede simplemente estar buscando travesura. Se rompen en la red para la diversión - para ver si son capaces de hacerlo. Si lo hacen, entonces será mejor que eso es todo lo que hacen. Personas que entrar a las redes de otras personas a menudo siguen sus travesuras por borrar los archivos o causar otros problemas.

El otro tipo de persona que se rompe en la red de su vecino está en busca de algo diferente. Quieren utilizar la conexión a internet para hacer algo que no quieren trazables a sí mismos. Sea lo que sea que quieren hacer, ya sea peligroso, inmoral o acto ilegal, no quieren ser los que se remonta a. Si están en la red, no se remonta a ellos - se remonta a usted.

Documentación del proveedor

A menudo, es una buena idea mirar a través de la documentación del router para saber cómo solucionar los problemas. Ir a página de soporte del proveedor donde puede descargar documentación.

Cómo solucionar el problema "WPS está activada"

Step 1: Inicie sesión en su enrutador

Utilice un navegador web para interactuar con su router y solucionar sus problemas de configuración. Sin embargo, antes de que se puede interactuar con el navegador, debe iniciar sesión en él. RouterCheck

Step 2: Si entras en la página de tu router con éxito, se abre.

Step 3: Acceda a la página WPS (configuración protegida de Wifi).

¿Quieres encontrar una página que tiene configuración WPS (Nota: esto puede o no puede estar en la misma página que regulares de seguridad inalámbrica). El nombre de la página puede ser similar a:

Configuración WPS

Configuración inalámbrica

Seguridad inalámbrica

Seguridad de WiFi

Vaya a esta página haciendo clic en los botones y elementos de menú apropiado.

Step 4: Si se tiene éxito, WPS su enrutador (configuración protegida Wifi) página se abre.

Step 5: Desactivar WPS

Busque una casilla de verificación que le permite controlar si el WPS está activada o desactivada. Nota: Algunos routers no le permiten desactivar WPS.

Step 6: Vuelva a ejecutar RouterCheck.

Ahora que has arreglado tu problema, ejecute RouterCheck para verificar que realmente han solucionado el problema.

RouterCheckSupport | SericonTechnology Inc. © 2015-2017"

Fuente: ResultadosRouterchek.

8. RESULTADOS DE LA INVESTIGACIÓN

El problema más recurrente de seguridad en los sistemas informáticos en general es producido por el factor humano por varias causas como desconocimiento, engaños, descuidos, delitos, entre otros. Esta investigación no fue ajena a este fenómeno, puesto que una de las reacciones de los administradores o dueños de la red inalámbrica, es mostrarse reacio a permitir aplicar procedimientos como el de este proyecto a las redes inalámbricas, primero por la desconfianza que causa el hecho que se exponga la posibilidad de vulnerabilidad desde la red inalámbrica y pretenda ingresar a esta red a realizar pruebas de seguridad, por otro lado siempre se tiene la concepción que su red es segura y no será blanco de ataques. El desconocimiento es otro de las causas que hayan redes inalámbricas inseguras, aunque los fabricantes de equipos y software trabajan por mitigar las vulnerabilidades conocidas, otras por el contrario están presentes por falta de configuración adecuada de las redes en especial en sistemas pequeños, puesto que estos sistemas no cuentan con personal especializado, porque simplemente no se considera importante o porque no se cuenta con los recursos económicos para su adecuada implementación e infraestructura.

Superado lo anterior, se aplicó el procedimiento desarrollado en este proyecto, con tres redes inalámbricas de diferentes ámbitos como son, red inalámbrica de hogar, otra que es una red libre de acceso público y por último una red inalámbrica de una empresa, se verifico que cada uno de los pasos establecidos en la guía paso a paso permiten realizar el análisis de las redes inalámbricas con la herramienta seleccionada, en las tres inalámbricas en las que se utilizó, para comprobar la aplicabilidad del procedimiento desarrollado, la herramienta routercheck logro escanear la red y entregar los reportes.

Tanto en la red inalámbrica de hogar como en la red inalámbrica abierta de acceso libre, la herramienta de software libre encontró fisuras de seguridad, para caso de la red inalámbrica de hogar se encontró que está habilitado el uso de WPS y permite ping desde internet, el reporte de la herramienta indica que el uso WPS supone una falla de seguridad puesto un dispositivo dentro del área de cobertura podría acceder a la red descubriendo este código WPS de este, y el ping permite que el router sea visible como un objetivo activo. En caso de la red inalámbrica de acceso público encontró como falla de seguridad que están abiertos los puertos TCP http (80) y https (443), esto supone una falla de seguridad puesto que los hackers podrían ingresar a la administración del router. Aunque para los dos casos no son fallas de seguridad graves, si son puntos que pueden ser vulnerables y explotados por delincuentes informáticos, puesto que ellos poseen conocimientos necesarios para convertir estas pequeñas falencias en ataques incluso de grandes proporciones.

Figura 24. Comparativo de evaluación de redes inalámbricas

Fuente. Autor

En el caso de la red inalámbrica empresarial, al realizar la evaluación de seguridad con la herramienta Routerchek no se encontró ninguna falencia de seguridad, por el contrario la herramienta no pudo obtener a toda la información de la red por restricción del router, lo que indica que la red está asegurada y soporta ataques, esto obedece a que es una red inalámbrica robusta y cuenta adecuada configuración de seguridad, y administración por personal idóneo para realizar esta actividad, esto debería ser lo normal en grandes empresas, aunque se pueden encontrar casos donde no es así.

Como se observa el procedimiento que se generó en esta investigación es aplicable a las redes inalámbricas en general y entrega resultados satisfactorios, independiente de los diferentes ámbitos en los que se hallan las redes, este trabajo de investigación se convierte en una herramienta básica de seguridad para los administradores de redes inalámbricas que no cuenten con recursos necesarios para realizar análisis de seguridad en dichas redes, si se tiene en cuenta que el procedimiento está basado en una herramienta gratuita y utiliza elementos que están al alcance de cualquier persona que esté al frente al manejo o uso de una red inalámbrica.

Adicional es una guía muy fácil de seguir y fácil de ejecutar en su totalidad, hasta la interpretación de los resultados y en algunos casos es posible aplicar las soluciones sugeridas por la misma herramienta a las falencias de seguridad detectadas, lo anterior otorga una ventaja al procedimiento si se compara con muchos de los procedimientos que se encuentran disponibles en internet, en los cuales resulta difícil seguir porque se deben tener amplios conocimientos para desarrollar las actividades que en ellos se indican, y se termina con errores o procedimientos incompletos y sin lograr los resultados esperados.

El producto que se obtuvo en este proyecto de investigación es un procedimiento para realizar un pentest a una red inalámbrica con una única herramienta gratuita llamada Routercheck, desde un dispositivo móvil con sistema operativo Android, siguiendo una guía paso a paso fácil de desarrollar, que no requiere de conocimientos avanzados en sistemas ni en seguridad, lo requerido es tener acceso autorizado a la red inalámbrica en donde se realiza un análisis de seguridad sobre la red, en busca de las vulnerabilidades que puedan estar presentes en dicha red, para recibir un reporte de resultados con las falencias de seguridad encontradas, el riesgo al cual se está expuesto con estas falencias, una manera de solucionarlo e información del fabricante sobre tema y el sitio donde se puede ampliar dicha información.

9. DIVULGACIÓN

La divulgación de este documento que realiza por medio del entorno de evaluación y seguimiento de la plataforma dispuesta por la universidad abierta y a distancia UNAD, como requisito para la aprobación de la especialización de seguridad informática. Igualmente, para que haga parte del repositorio de la universidad para el uso de la comunidad de la UNAD.

Otro medio de divulgación será por correo electrónico al director del proyecto con el fin de comunicar los resultados de obtenidos, para las respectivas recomendaciones y correcciones.

10. CONCLUSIONES

- Se identificaron vulnerabilidades que pueden afectar las redes inalámbricas independiente del tamaño o del ámbito que esta se encuentre, y que, aunque son conocidas no siempre se toman las precauciones necesarias para corregirlas convirtiendo a las redes inalámbricas en blanco de los ataques que se han vuelto comunes con el desarrollo y la evolución de los sistemas informáticos y en especial con el aumento de uso de los dispositivos móviles y el aumento en la variedad, capacidad y funciones que estos permiten en el día a día de todas las personas.

- Las amenazas y vulnerabilidades de las redes inalámbricas son de diversos tipos, por lo que no es suficientes con la adecuada configuración de los sistemas, sino que se requiere de software especializado para evaluación de seguridad y de esta manera minimizar el riesgo de la existencia de puntos vulnerables en la red.

- Fueron preseleccionadas 5 herramientas (*routerchek, Dsploit, wifinpect, Fing-network y Intercepter-ng*) y luego de evaluar aspectos como facilidad de uso, funcionalidades e informes de remediación entre otros, fue seleccionada la herramienta routercheck, que mediante su sencilla interfaz y fácil uso realiza la prueba de seguridad de toda la red en corto tiempo, y finalmente entrega un informe detallado sobre los resultados, y brinda una guía sobre la manera como resolver las fallas detectadas, pero también entrega información sobre el tema relacionado, de manera que basta con tener conocimientos básico en sistemas para poder realizar todo el procedimiento.

- Se identifico la metodología de pentest ISSAF, esta se utilizó como marco de referencia para apoyar el procedimiento del presente proyecto, en la etapa de alistamiento o preparación del procedimiento, pasando a la prueba de seguridad sobre la red inalámbrica y finalizando con el reporte detallado sobre los resultados de la prueba realizada, tal como las fases de planeación, evaluación y reportes que instituye la metodología señalada.

- Se genero procedimiento con una guía paso a paso para realizar pentest a una red inalámbrica, utilizando una herramienta gratuita llamada routercheck desde un dispositivo móvil con sistema operativo Android, que permite realizar la evaluación en busca de vulnerabilidades de seguridad en la red, sin que sea necesario poseer conocimientos avanzados en sistemas informáticos.

- Se realizo un procedimiento que permite realizar una evaluación del estado de seguridad de una red inalámbrica, detectando los puntos vulnerables de la red,

siguiendo una guía sencilla de aplicar, a bajo costo y sin que se requiera la intervención de un especialista en seguridad informática.

BIBLIOGRAFÍA

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273. Bogotá. (enero 5 de 2009). Diario Oficial 47.223 de enero de 2009.

HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Referencias documentales para fuetes de información electrónicas NTC 4490. Bogotá D.C., Editado por ICONTEC, 1998

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Documentación; presentación; tesis; trabajos de investigación NTC 1486. Bogotá D.C., Editado por ICONTEC, 2008.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Referencias bibliográficas, contenido, forma y estructura NTC 5613. Bogotá D.C., Editado por ICONTEC, 2008

WEBGRAFÍA

ALEGSA, Leandro. Definición de vulnerabilidad [En línea] diciembre de 2010 [citado 15 de octubre de 2017] disponible en: http://www.alegsa.com.ar/ Dic/vulnerabilidad.php

ALEGSA, Leandro. Definición de Vulnerabilidad. [En línea]. Santa Fe Argentina, mayo 2010 [Citado 24 de octubre de 2016] disponible en: (http://www.alegsa.com.ar/Dic/vulnerabilidad.php)

ALEGSA, Leandro. Definición de WPA [En línea] diciembre de 2010 [citado 15 de octubre de 2017] disponible en: http://www.alegsa.com.ar/Dic/wpa.php

ARAOZ, I. Metodología de test de intrusión ISSAF. [En línea] abril de 2009 [citado 19 de octubre de 2017] disponible en:http://insecuredata.blogspot.com.co/2009/04/metodologia-de-test-de-intrusion-issaf.html

ARTEAGA MEJÍA, Luis Miguel. ¿Qué es software libre? [En línea] junio de 2011 [citado 15 de octubre de 2017] disponible en: https://www.gnu.org/philosophy/free-sw.es.html

BARRIOS, Joel. ¿Qué es WPA? ¿Por qué debería usarlo en lugar de WEP? [En línea]. Chiapas México, abril 2007. [Citado el 10 de septiembre de 2016] disponible en: (http://www.alcancelibre.org/article.php/20070404112747533)

BAZ, Arturo y Ferreira, Irene y Álvarez, María y García Rosana. Dispositivos móviles [en línea]. Universidad de Oviedo. Disponible en: http://isa.uniovi.es/docencia/SIGC/pdf/telefonia_movil.pdf

CREADPAG. 10 aplicaciones de hacking para Android para pentesters, aficionados e investigaciones, [En línea]. California Estados Unidos, enero 2017. [Citado el 20 de mayo de 2016] disponible en: https://creadpag.com/10-aplicaciones-de-hacking-para-android-para-pentesters-aficionados-e-investigaciones/

CREATIVE COMMONS. Los riesgos relacionados con las redes inalámbricas (802.11 o Wi. [En línea]. Paris Francia, octubre 2016. [Citado en 5 de octubre de 2016] disponible en: (http://es.ccm.net/contents/792-los-riesgos-relacionados-con-las-redes-inalambricas-802-11-o-wi**)**

DE LUZ, Sergio. WPSPIN v1.3 para Android ya disponible: Comprueba la seguridad Wi-Fi de tu router. [En línea]. New york Estados unidos ,julio 2015.[Citado 26 de Octubre de 2016] disponible en: (http://www.redeszone.net/2015/07/09/wpspin-v1-3-para-android-ya-disponible-comprueba-la-seguridad-wi-fi-de-tu-router/)

ECURED. Ataque informático [En Línea]. La habana Cuba, enero 2012. [Citado 24 de octubre de 2016] disponible en: (https://www.ecured.cu/Ataque_informático)

EFFECTHACKING. dSploit - Aplicación de Android para hackers. [En línea] 10 de abril 2015 [Citado 20 de octubre de 2017] Disponible en: http://www.effecthacking.com/2015/04/dsploit-android-app-for-hackers.html

ES.CCM.NET. Redes inalámbricas [En línea] julio de 2017 [citado 15 de octubre de 2017] disponible en: https://openwebinars.net/blog/que-es-el-pentesting/

ESAÚ, A. ¿Qué es pentesting? [En línea]junio de 2012 [citado 15 de octubre de 2017] disponible en: https://openwebinars.net/blog/que-es-el-pentesting/

ESTHEFANY AND YERIKA. Definición Android. [En línea] mayo de 2012 [citado 15 de octubre de 2017] disponible en: http://tecnologiasandroid.blogspot.com.co/2012/05/definicion-android.html
FANÁTICO, Andrés. Top10 Mejores Aplicaciones De Wifi Hacking Para Android 2016. [En línea]. Francia, mayo 2015. [Citado 26 de octubre de 2016] disponible en: (https://www.zonatopandroid.com/aplicaciones-para-hackear-wifi/) Francesco,

FRANCESCO, Umberto. dSploit: Pentesting& Hacking WiFidesde Android. Mayo de 2014. [En línea] [Citado 25 de noviembre de 2016] disponible en: http://jadcode.blogspot.com.co/2014/05/dsploit-pentesting-hacking-wifi-desde.html

GONZÁLEZ, Alejandro. Que es Android. [En línea]. Washington, febrero 2011 [Citado el 8 de mayo de 2016] disponible en: (http://www.xatakandroid.com/sistema-operativo/que-es-android)

GUEVARA SORIANO,Anaid. Dispositivos móviles. [En línea] agosto de 2010 [citado 15 de octubre de 2017] disponible en:https://revista.seguridad.unam.mx/numero-07/dispositivos-moviles

ISAZA, Miguel Arturo. Metodologías y Herramientas de Ethical Hacking, [En línea]. Mountain View Estados Unidos, febrero de 2013[Citado el 19 de mayo de 2016] disponible en: http://seguridadinformaticahoy.blogspot.com.co/2013/02/metodologias-y-herramientas-de-ethical.html

L TECNOLOGÍA, Definición de Linux [En línea]mayo de 2011 [citado 15 de octubre de 2017] disponible en: http://conceptodefinicion.de/linux/

MIFSUD. Elvira, Introducción a la seguridad informática - Seguridad de la información / Seguridad informática. [En línea]. Ministerio de educación, cultura y deporte de España, marzo de 2012 [citado mayo 15 de 2017] disponible en: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

MILLA ANCIN, David. Android: Cómo Administrar Nuestra Wifi con Fing. [En línea] 12 de diciembre de 2014 [Citado 25 de octubre de 2017]. Disponible en: http://curiotek.com/2014/12/12/android-como-administrar-nuestra-wifi-con-fing/

ORDENADORES Y PORTÁTILES. ¿Qué es y para qué sirve un punto de acceso? [En línea]. Scottsdale Estados unidos 2014 [Citado 24 de octubre de 2016] disponible en: (http://www.ordenadores-y-portatiles.com/punto-de-acceso.html)

PLANTILLA FANTÁSTICO, S.A. Seguridad de redes. [En línea] [Citado 24 de octubre de 2016] disponible en: (http://laseguridadenredes.blogspot.com.co/p/concepto-e-importancia.html)

PORTO, Julián y Merino, María. Red Inalámbrica. [En línea]. Florida Estados Unidos 2011. [citada, mayo 3 de 2016] disponible en: (http://definicion.de/red-inalambrica/)

REVENSSIS. Revenssis Penetration Testing Suite. [En línea]. California Estados unidos, diciembre de 2014. [Citado el 11 de mayo de 2016] disponible en: (https://sourceforge.net/projects/revenssis/)

REY, Carlos. Rootear Samsung Galaxy J5. 2015. [En línea] Octubre de 2015.[Citado 26 de noviembre de 2016] disponible en: http://androidphoria.com/tutoriales/tutorial-rootear-samsung-galaxy-j5-facil

REYES, Alejandro. Ethical Hacking, [En línea] [Citado el 25 de mayo de 2016] disponible en:(http://www.seguridad.unam.mx/descarga.dsc?arch=2776)

ROUSE, Margaret.Prueba de penetración (pen test). [En línea] marzo de 2014 [Citado 04 de abril de 2017] Disponible en: http://searchdatacenter.techtarget.com/es/definicion/Prueba-de-penetracion-pen-test

ROUTERCHECK. Routercheck. 2016. [En línea] [Citado 26 de noviembre de 2016] disponible en: http://www.routercheck.com/

RUZ, J. Riveros, B. Varas, A. Redes WPA/WPA2. [En línea] agosto de 2013 [citado 17 de octubre de 2017] disponible en:http://profesores.elo.utfsm.cl/~agv/elo322/1s12/project/reports/RuzRiverosVaras.pdf

TECNOXXI, ¿Qué es ethical hacking? [En línea] noviembre de 2016 [citado 15 de octubre de 2017] disponible en:https://www.tecnoxxi.com/blog/seguridad-informatica/que-es-ethical-hacking/

THOMAS, Gavin. Pentesting con Android usando dSploit. 2014. [En línea] [Citado 20 de noviembre de 2016] disponible en https://www.gadgetdaily.xyz/build-html5-charts-with-chart-js/

UNAM. Ataques a dispositivos móviles. [En Línea] mayo de 2014 [citado el 5 de octubre de 2016] disponible en: (http://redyseguridad.fi-p.unam.mx/proyectos/buenas-practicas/ataquesadispositivosmoviles.html)

UNT.BA. Sistema de seguridad de la información Norma - ISO 27000 [en línea]. Universidad Tecnológica Nacional. Buenos Aires Argentina. Disponible en: http://www.calidad.sceu.frba.utn.edu.ar/index.php/asesoramiento/152-%20%20sistema-de-seguridad-de-la-informacion-norma-iso-27000

VALLEJO DE LEÓN, T. Vulnerabilidades y niveles de seguridad de redes WI-FI. WPA [En línea] agosto de 2010 [citado 16 de octubre de 2017] disponible en: http://biblioteca.usac.edu.gt/tesis/08/08_0266_EO.pdf

VELASCO, Rubén. Monitoriza la red con Wifinspect [En línea] 27 de mayo de 2013 [Citado 21 de octubre de 2017] Disponible en: https://www.redeszone.net/2013/05/27/monitoriza-la-red-con-wifinspect-ii/

Guevara, Roberto. Riesgos con las redes Wi-Fi públicas del centro de Medellín, Colombia. [En línea] febrero de 2017 [citado febrero 16, 2018] Disponible en: http://www.uniremington.edu.co/images/investigacion/libros-investigacion/Wi-Fi-Ok-2.pdf

Palacios, Jairo. Análisis de Vulnerabilidades de una Red Corporativa mediante Herramientas de Descubrimiento Activas. Universidad de Sevilla. [En línea] julio de 2015 [citado febrero 16, 2018] Disponible en: http://bibing.us.es/proyectos/abreproy/90522/fichero/Memoria+del+Trabajo+Fin+de+Grado.pdf

ZUCCARDI, Giovanni, GUTIERREZ, Juan. Vulnerabilidades en 802.11. [En línea]. Universidad Javeriana, octubre de 2016, [citado 16 de febrero de 2018]. Disponible en: http://pegasus.javeriana.edu.co/~edigital/Docs/802.11/Vulnerabilidades/Vulnerabilidades%20v0.5.doc

Velasco, Rubén. Las mejores 10 herramientas para hacking ético de este 2015. [En línea]. Redes zona. 5 de diciembre de 2015 [Citado 16 de febrero de 2018].

Disponible en: https://www.redeszone.net/2015/12/05/las-mejores-10-herramientas-para-hacking-etico-de-este-2015/

ANEXOS

Anexo 1: RESUMEN PROYECTO - ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA UNAD

	FORMATO
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
Código:	**Versión: 01**
Fecha de Aprobación:	**Página** 83 **de** 3

1.Información General	
Tipo de documento	Trabajo de Grado
Acceso al documento	Universidad Nacional Abierta y a Distancia
Título del documento	Generación de un procedimiento para realizar pruebas de pentest en redes inalámbrica utilizando dispositivos móviles con sistema operativo android, mediante herramientas de software libre.
Autor(es)	PINZON BARRANTES, Nelson Fabio
Publicación	Bogotá. Universidad Nacional Abierta y a Distancia, 2017.
Palabras Claves	Seguridad, vulnerabilidad, Pentest, redes inalámbricas, procedimiento, metodología, guía, herramientas, software libre.
Descripción	En este proyecto se realizó un procedimiento que permite realizar pruebas de pentest a las redes inalámbricas, desde un dispositivo móvil con sistema operativo Android, usando una de herramienta de software libre que permita identificar las posibles vulnerabilidades que están presentes en dicha red inalámbrica.
Fuentes	Se utilizaron un total de 43 fuentes para esta monografía, dentro de las cuales se encuentran: COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273. Bogotá. (enero 5 de 2009). Diario Oficial 47.223 de enero de 2009.

	HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. ARAOZ, I. Metodología de test de intrusión ISSAF. [En línea] abril de 2009 [citado 19 de octubre de 2017] disponible en:http://insecuredata.blogspot.com.co/2009/04/metodologia-de-test-de-intrusion-issaf.html CREATIVE COMMONS. Los riesgos relacionados con las redes inalámbricas (802.11 o Wi. [En línea]. Paris Francia, octubre 2016. [Citado en 5 de octubre de 2016] disponible en: (http://es.ccm.net/contents/792-los-riesgos-relacionados-con-las-redes-inalambricas-802-11-o-wi**)** ES.CCM.NET. Redes inalámbricas [En línea] julio de 2017 [citado 15 de octubre de 2017] disponible en: https://openwebinars.net/blog/que-es-el-pentesting/
Contenido	Introducción Formulación del problema Justificación Objetivos Marco de referencia Diseño metodológico Desarrollo de la investigación Resultados de la investigación Divulgación Conclusiones Bibliografía Webgrafía
Metodología	Este proyecto se basa en investigación descriptiva, proyectiva e interactiva, mediante la cual tiene como objetivo generar un procedimiento para realizar pruebas de pentest en redes inalámbricas desde dispositivos con sistema operativo Android, para descubrir vulnerabilidades en dichas redes.
Conclusiones	Se genero procedimiento con una guía paso a paso para realizar pentest a una red inalámbrica, utilizando una herramienta gratuita llamada routercheck desde un

	dispositivo móvil con sistema operativo Android, que permite realizar la evaluación en busca de vulnerabilidades de seguridad en la red, sin que sea necesario poseer conocimientos avanzados en sistemas informáticos. Se realizo un procedimiento que permite realizar una evaluación del estado de seguridad de una red inalámbrica, detectando los puntos vulnerables de la red, siguiendo una guía sencilla de aplicar, a bajo costo y sin que se requiera la intervención de un especialista en seguridad informática