DETERMINAR LOS PRINCIPALES ATAQUES A LOS QUE SE EXPONEN LOS USUARIOS QUE UTILIZAN LA RED WIFI “IDEA INTERNET EN EL PARQUE” DEL MUNICIPIO DE URRAO

GEOVANNY ALONSO RAMÍREZ HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLÍN
2017

DETERMINAR LOS PRINCIPALES ATAQUES A LOS QUE SE EXPONEN LOS USUARIOS QUE UTILIZAN LA RED WIFI “IDEA INTERNET EN EL PARQUE” DEL MUNICIPIO DE URRAO

GEOVANNY ALONSO RAMÍREZ HERRERA

TRABAJO DE GRADO

Asesor de proyecto

ERIKA LILIANA VILLAMIZAR TORRES
Ingeniera, Especialista y Master en seguridad informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLÍN
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Medellín, 25 de julio de 2017

DEDICATORIA:

Dedico este proyecto de grados a Dios Todopoderoso mi creador, mi fuerte pilar, mi fuente de inspiración, la sabiduría, el conocimiento y la comprensión. Ha sido la fuente de mi fuerza a través de este programa y en sus alas sólo me he proyectado. También dedico este trabajo a mi esposa Yurany Serna, de pie junto a mí durante toda mi carrera. Ella ha sido mi inspiración y motivación para continuar mejorando mis conocimientos en pro de esforzarme para seguir adelante. También agradezco a mi hijo maravilloso: Christopher Ramírez Serna, el cual siempre me hace sonreír y me impulsa a demostrarle que todos podemos ser seres maravillosos. Dios los bendiga.

AGRADECIMIENTOS

Mi más profundo agradecimiento a Dios que ha proporcionado todo lo que se necesitaba para completar este proyecto de grados y el programa para el que se llevó a cabo. Nunca hubo falta o necesidad de ningún elemento. A lo largo de todo este estudio, se ocupó de todo lo que me habría detenido en seco y me dio fuerzas, incluso a través de mis momentos más difíciles.

También quiero dedicarle este proyecto a mi padre Mario Ramírez Montoya, que me enseñó que el mejor tipo de conocimiento que tienen es el que se aprende por sí mismo. También está dedicado a mi madre Ruth Herrera Moreno, que me enseñó que incluso la tarea más grande se puede lograr si se hace un paso a la vez, se lograran excelentes resultados.

A la Ingeniera Lorena Suarez Sierra, la cual fue la primera persona en guiarme en los primeros pasos para dar inicio con este gran proyecto. También al Ingeniero Salomón González, el cual ha sido el director ideal para culminar este proyecto de grado. Sus sabios consejos, críticas interesantes y certeras, cuyo apoyo firme de este proyecto fueron muy necesarios y muy apreciados para mí. También al Ingeniero William Steven Tavera, el cual ha sido el asesor encargado de pulir y encaminar este proyecto de la mejor manera posible, hacia el logro de todos sus objetivos.

Por último, quisiera dar las gracias a los directores de cada curso, tutores, al Rector del CEAD Medellín, el Doctor Juan Bayona Ferreira, a la Ingeniera María Ángela Rodríguez Cubillos, así como a la Ingeniera Erika Liliana Villamizar Torres, la cual me ayudo de una manera excepcional, estando siempre atenta con el cumplimiento de los tiempos en cada una de las etapas finales de la construcción del proyecto, en la entrega final del mismo. También agradezco a los concejeros y administradores de las diferentes oficinas de la UNAD, que me ayudaron a escalar cada día más hacia la consecución de este proyecto, donde su entusiasmo y disposición para proporcionar información hicieron posible la conclusión de investigar hacia el logro de una experiencia agradable.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACCESS POINT: un dispositivo de red inalámbrico que recibe las señales y los retransmite, sin proporcionar acceso directo a la red cableada. Los repetidores se utilizan normalmente para aumentar el rango de redes inalámbricas pueden cubrir.

AMENAZA COMBINADA: una descripción general para los programas maliciosos que combinan elementos de múltiples tipos de *malware*, representados en virus, gusanos, troyanos, entre otros.

AMENAZA: cualquier circunstancia o evento con el potencial de afectar negativamente a las operaciones de la organización (incluyendo la misión, funciones, imagen o reputación), activos de la organización, los individuos, otras organizaciones, o de la Nación a través de un sistema de información a través de un acceso no autorizado, destrucción, divulgación, modificación de la información, y / o de denegación de servicio.

ANÁLISIS DE AMENAZAS: el examen de los orígenes de las amenazas contra las vulnerabilidades del sistema para determinar las amenazas para un sistema en particular en un entorno operativo en definido.

ANÁLISIS DE RIESGOS: el proceso de identificación de los riesgos para la seguridad del sistema y la determinación de la probabilidad de ocurrencia, el impacto resultante, y las medidas de seguridad adicionales que mitiguen este impacto. Parte de la gestión de riesgos y sinónimo de evaluación de riesgos.

ANÁLISIS DEL TRÁFICO: una forma de ataque pasivo en el que un intruso observa información sobre las llamadas (aunque no necesariamente el contenido de los mensajes) y hace inferencias, por ejemplo, de la fuente y el número de destino, o la frecuencia y la longitud de los mensajes.

ANTENA: un transductor que convierte especializada de radiofrecuencia (RF) Los campos en corriente alterna (AC) o viceversa. Hay dos tipos básicos: la antena de recepción, que intercepta energía RF y suministra CA a equipos electrónicos, y la antena de transmisión, que se alimenta con corriente alterna de los equipos electrónicos y genera un campo de RF.

ATAQUE DE DICCIONARIO: método utilizado para romper la contraseña de un usuario o dispositivo inalámbrico, donde el comando del ataque va pasando a través de todas las palabras en un diccionario de palabras relacionadas; cuya finalidad es analizar cada palabra, hasta que encuentra una contraseña que funciona.

AUTENTICACIÓN DE CLAVE COMPARTIDA: puede ser fácilmente explotado a través de un ataque pasivo por escuchas ilegales tanto en el desafío y la respuesta entre el punto de acceso y el cliente de autenticación. un ataque de este tipo es posible porque el atacante puede capturar tanto el texto en claro (el reto) y el texto cifrado (la respuesta).

AUTENTICACIÓN: un cliente puede ser requerido para autenticar a la red inalámbrica antes de que pueda pasar los datos entre sí y otros huéspedes. La autenticación puede ser abierta, pero también puede requerir un certificado, nombre de usuario / contraseña o clave pre-compartida.

AUTENTIFICACIÓN DE SISTEMA ABIERTO: La autenticación de sistema abierto es el protocolo de autenticación por defecto para el estándar 802.11. Se compone de una solicitud de autenticación simple que contiene el ID de estación y una respuesta de autenticación que contiene los datos de éxito o fracaso.

CIBERCRIMINALES: los cibercriminales son *hackers, crackers* y otros usuarios maliciosos que usan Internet para cometer crímenes como el robo de identidad, el secuestro de equipos, el *spam* ilegal, *Phishing, pharming* y otros tipos de fraude.

CANAL: un canal es la ruta de acceso a la red para transmisiones inalámbricas. Cada estándar WiFi tiene numerosos canales, cada uno de los cuales es una frecuencia central.

CIBEROCUPACIÓN: el registro, tráfico o uso de un nombre de dominio con intenciones maliciosas para aprovecharse de la buena fe o de una imagen de marca que pertenece a otro. El ciber ocupante suele ofrecer la venta del dominio a la persona o empresa a la que pertenece la marca contenida en el nombre, a precios muy elevados. Los ciber ocupantes también suelen registrar variaciones del nombre de marcas populares como manera de distribuir su *malware*.

CIFRADO: un método para ocultar la información de tal manera que sólo el remitente y el destinatario puedan leerlo.

CÓDIGO MALICIOSO: código diseñado para dañar un sistema y los datos que contiene, recopilar información delicada, obtener acceso no autorizado o evitar que el sistema se use de la manera habitual.

CÓDIGO MALICIOSO: software o *firmware* destinado a realizar un proceso no autorizado que tendrá un impacto adverso sobre la confidencialidad, integridad o disponibilidad de un sistema de información. Un virus, gusano, troyano, u otra entidad basada en el código que infecta a un huésped. El software espía y algunas formas de *adware* son también ejemplos de código malicioso.

CONFIDENCIALIDAD: la confidencialidad es un requisito cuyo propósito es mantener la información sensible se divulgue a receptores no autorizados.

CONTRASEÑA: es la combinación de palabras que se usan para proporcionar autenticación WEP de seguridad a una red inalámbrica, donde se puede utilizar entre 40 bits o 104 frases de paso fijo, mientras que WPA y WPA2 pueden usar frases de paso de longitud arbitraria.

CONTROLES DE SEGURIDAD: la gestión, operativos y controles técnicos (es decir, salvaguardas o contramedidas) recetados por un sistema de información para proteger la confidencialidad, integridad y disponibilidad de la instalación o de la información.

DIRECCIÓN MAC: un MAC (Medios de acceso de control) de direcciones es un identificador único, basado en hardware utilizado para diferenciar entre los usuarios conectados. Mientras que las direcciones MAC son inicialmente hardware basado, que también pueden modificarse. Esto se llama "*Spoofing*", y tiene varios usos en el mundo real, aunque la mayoría de la gente direcciones de suplantación de identidad asociado de ningún tipo con la piratería.

Disponibilidad: la disponibilidad es un requisito destinado a garantizar que los sistemas funcionan con prontitud y el servicio no se les niega a los usuarios autorizados.

DISTANCIA: trayecto entre un punto de acceso y un cliente (o entre dos puntos de acceso, ver el puente de grupo de trabajo) sobre las que las transmisiones de WiFi pueden tener éxito. Cuanto mayor es el rango, mayor será la atenuación de una señal y el más bajo es el rendimiento global será.

EL HOMBRE EN MEDIO DEL ATAQUE: un método utilizado para interceptar el tráfico entre el dispositivo de un usuario y el sistema de destino seleccionado.

EXPLOTACIONES DE LA RED: *exploits* que se aprovechan de los defectos del software en el sistema operativo móvil u otro software que funciona en redes locales (por ejemplo, Bluetooth, Wifi) o celulares. A menudo no requieren ninguna interacción del usuario, que los hace especialmente peligrosos si se utilizan para aprovechar la propagación de *malware*.

FILTRADO DE DIRECCIONES MAC: una aproximación a la restricción del acceso a una red inalámbrica por los clientes sólo permite la conexión si su dirección MAC está en una lista. Filtrado de direcciones MAC no es escalable, y puesto que la mayoría de tarjetas de red inalámbricas se pueden configurar para usar cualquier MAC.

FIREWALL: una puerta de enlace que limita el acceso entre redes, de conformidad con la política de seguridad local.

GEMELO MALVADO: un punto de acceso inalámbrico de fabricación casera que se presenta como una legítima para recopilar información personal o corporativa sin el conocimiento del usuario final. Es bastante fácil para un atacante crear un gemelo malvado por el simple uso de un ordenador portátil, una tarjeta inalámbrica y algún software fácilmente disponible.

HACKER: usuario no autorizado que intenta tener el acceso a un sistema de información ajeno u empresarial.

HACKERS HERRAMIENTAS Y MÉTODOS: el objetivo del hacker es romper las normas de seguridad a medida que se desarrollan, que a su vez mantiene los ocupados en desarrollo nuevos estándares IEEE. Varias herramientas de detección y romper el cifrado, así como el intercambio de "cómo" documentos / artículos se ponen a disposición en Internet de forma gratuita, añadiendo al

problema. Como resultado, incluso el usuario inalámbrico novato puede intentar algunas de las técnicas de piratería proporcionados en línea.

HOTSPOT: un punto de acceso configurado específicamente para proporcionar acceso a Internet a los usuarios. Los *Hotspot* son populares en las cafeterías, restaurantes y otros lugares accesibles al público, y por lo general no requieren ningún tipo de autenticación u ofrecer ningún tipo de cifrado.

INALÁMBRICO FIJO: los dispositivos inalámbricos o sistemas en ubicaciones fijas, tales como viviendas y oficinas. Dispositivos inalámbricos fijos por lo general derivan su energía eléctrica de la red de servicios públicos, a diferencia móvil inalámbrica móvil o portátil, que tienden a ser alimentado por batería. Aunque los sistemas móviles y portátiles se pueden utilizar en ubicaciones fijas, la eficiencia y el ancho de banda están en peligro en comparación con los sistemas fijos.

INTEGRIDAD: la integridad es un requisito objeto garantizar que la información y los programas sólo se cambian de una manera específica y autorizado.

INTEGRIDAD: protección contra la modificación o destrucción de información inadecuada, e incluye garantizar que la información no repudio y la autenticidad.

ITINERANCIA: en una red inalámbrica con múltiples puntos de acceso, un cliente que se mueve desde el área de cobertura proporcionada por un punto de acceso a la proporcionada por otro está en itinerancia. Se debe disociarse del primer AP antes de que pueda asociarse a la siguiente AP.

LOS PUNTOS DE ACCESO: según (Anónimo). [1]"Consiste en antenas y routers, son la principal fuente que transmitir y recibir ondas de radio. Antenas trabajar más fuerte y tienen una transmisión de radio más largo con un radio de 300-500 pies, que se utilizan en las zonas comunes, mientras que el router, pero eficaz más débil es más conveniente para los hogares con una transmisión de radio de 100-150 pies".

MALWARE MÓVIL: software con propósitos maliciosos que suele realizar acciones sin el conocimiento del usuario. Puede estar diseñado para dañar su teléfono, controlar remotamente su dispositivo, enviar mensajes no autorizados a

[1] Tomado de WI-FI conceptos a trabajar. Disponible en línea desde la URL: http://www.w3ii.com/es/wi-fi/wifi_working_concepts.html

la lista de contactos del usuario, realizar cargos a la factura telefónica o robar información valiosa. El malware móvil usa las mismas técnicas que el malware de PC para infectar los dispositivos móviles.

MALWARE: un programa que se inserta en un sistema, por lo general de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo de la víctima.

OLFATEANDO / ESPIONAJE: el método de escuchar pasivamente a los datos en la red sin el conocimiento del usuario engañando a la red en pasar todos los datos a través de la computadora del hacker primero.

PHISHING: engañar a las personas para que revelen información personal a través de medios basados en computadoras engañosas.

PROTOCOLO WEP: es una característica de seguridad básica en el estándar IEEE 802.11, destinado a proporcionar confidencialidad sobre una red inalámbrica mediante el cifrado de la información enviada a través de la red. Una falla clave-programación se ha descubierto en WEP, por lo que ahora se considera como no garantizados debido a una clave WEP puede ser violada en pocos minutos con la ayuda de herramientas automatizadas. Por lo tanto, WEP no debe utilizarse a menos que un método más seguro no está disponible.

PUENTE: un dispositivo de red que interconecta dos tipos de redes diferentes. Un punto de acceso puede actuar como un puente entre las redes cableadas e inalámbricas, pero también puede servir como una conexión inalámbrica entre dos segmentos de cable.

PUERTO: una entrada física o punto de salida de un módulo criptográfico que proporciona acceso al módulo de señales físicas, representada por los flujos de información lógica (puertos separados físicamente no comparten el mismo pasador física o alambre).

PUNTO CALIENTE: nodo inalámbrico que proporciona conexión a Internet y acceso de red privada virtual (VPN) desde un lugar determinado. Un viajero de negocios, por ejemplo, con un ordenador portátil equipado para Wifi se puede buscar un lugar caliente local, póngase en contacto con él, y conectarse a través de su red para llegar a la Internet y su propia empresa de forma remota con una

conexión segura. Cada vez más, los lugares públicos, como aeropuertos, hoteles y cafeterías están proporcionando acceso inalámbrico gratuito para los clientes.

RED ABIERTA: una red inalámbrica abierta permite la asociación y la autenticación sin requerir una frase de contraseña, certificado o credenciales. Las redes abiertas son a menudo llamados puntos calientes y proporcionan acceso a Internet gratis a cualquier persona dentro del alcance. Muchas cafeterías y restaurantes se desplegarán estos para atraer a los clientes. Todavía pueden incorporar un portal cautivo.

RED DE ÁREA LOCAL INALÁMBRICA (WLAN): una red de área local (LAN) que los usuarios acceden a través de una conexión inalámbrica. 802.11 normas especifican las tecnologías WLAN. WLAN son con frecuencia una parte de una LAN cableada.

RED WIFI NO SEGURA: una red wifi no segura es una red inalámbrica que no solicita al usuario la autentificación para acceder a él a través de la utilización de un nombre de usuario y contraseña. Estos por lo general se muestran como las redes abiertas.

RIESGO: el nivel de impacto en las operaciones de la organización (incluyendo la misión, funciones, imagen o reputación), activos de la organización o individuos que resultan de la operación de un sistema de información dado el impacto potencial de una amenaza y la probabilidad de que se produzca una amenaza.

RIESGOS DE SEGURIDAD: las operaciones de la organización (incluyendo la misión, funciones, imagen, reputación), activos de la organización, los individuos, otras organizaciones, y la Nación debido a la posibilidad de acceso no autorizado, uso, divulgación, alteración, modificación o destrucción de la información y / o sistemas de información.

ROGUÉ PUNTOS DE ACCESO / ROGUÉ AP: puntos de acceso inalámbricos instalados en la red de una empresa sin el conocimiento de la empresa. Estos puntos de acceso tienen prioridad sobre el que verdaderamente es el legítimo de la red organización, de tal modo que permite al pirata informático, la oportunidad de manipular los datos de ataque e interceptar las medias de seguridad.

SEGURIDAD WIRELESS TRANSPORT LAYER (WTLS): el nivel de seguridad para las aplicaciones de Protocolo de Aplicaciones Inalámbricas (WAP), desarrollado para abordar las cuestiones problemáticas que rodean los dispositivos de red móviles - como un poder limitado de procesamiento y capacidad de memoria y ancho de banda bajo - y para proporcionar autenticación adecuada, integridad de los datos, y los mecanismos de protección de la privacidad.

SEÑALES DE RADIO: las señales de radio son las claves, que hacen posible la creación de redes Wifi. Estas señales de radio transmitidas desde antenas Wifi son recogidos por receptores Wifi, tales como computadoras y teléfonos celulares que están equipadas con tarjetas Wifi. Cada vez, un ordenador recibe cualquiera de las señales dentro del alcance de una red Wifi, que normalmente es 300 - 500 pies de altura para antenas de este tipo, donde la tarjeta Wifi lee las señales y por lo tanto crea una conexión a Internet entre el usuario y la red sin el uso de un cable.

SPYWARE: software que se produce o subrepticiamente instalado en un sistema de información para reunir información sobre personas u organizaciones sin su conocimiento; un tipo de código malicioso.

VULNERABILIDAD DE PROTOCOLO: los datos que pasan a través de una LAN inalámbrica con WEP desactivado (que es la configuración por defecto para la mayoría de los productos) es susceptible a ataques de escucha y de modificación de datos. Sin embargo, incluso cuando está activado WEP, la confidencialidad y la integridad de tráfico inalámbrico se encuentra todavía en riesgo debido a una serie de defectos en WEP han sido revelados, los cuales perjudican gravemente sus pretensiones a la seguridad.

VULNERABILIDAD: la debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos, o la aplicación que podría ser aprovechada o desencadenada por una fuente de amenaza.

WAP: hace referencia al Protocolo de Aplicaciones Inalámbricas, de comunicación que son utilizados para estandarizar la forma en que los dispositivos inalámbricos, puedan ser manipulados para el acceso a Internet.

WAP: protocolo de aplicaciones inalámbricas. Un servicio para dispositivos móviles con acceso a Internet. Los dispositivos móviles tienen pantallas más

pequeñas que lo que la mayoría de los sitios web fueron diseñados. La mayoría de los WAP se utilizan para agregar capacidad wifi a una red cableada ya establecida.

WEP: (*wired equivalent Privacy)* es el esquema de cifrado original, implementado en las redes inalámbricas. El uso de RC4 de 40 bits, ó bien sea una tecla de 104 bits pre-compartida, WEP proporciona aproximadamente el mismo nivel de privacidad, ya que hace uso de un concentrador en una red cableada. Se rompen fácilmente, WEP está normalmente sólo desplegado en redes domésticas.

WIFI HOTSPOT: un punto de acceso wifi se crea mediante la instalación de un punto de acceso a una conexión a Internet. El punto de acceso transmite una señal inalámbrica a una distancia corta.

WIFI NO SEGURA: la conectividad inalámbrica que no utiliza ningún tipo de encriptación (WEP / WPA) para proteger los datos a medida que viaja a través del aire entre un dispositivo y el punto de acceso inalámbrico. Los datos transmitidos a través de una red WiFi no segura pueden ser interceptadas o vistos por usuarios no autorizados.

WIFI PROTECTED ACCESS (WPA): es un protocolo de seguridad inalámbrico diseñado para abordar y solucionar los problemas de seguridad conocidos en WEP. WPA proporciona a los usuarios un mayor nivel de seguridad de que sus datos estarán protegidos mediante el uso de *Temporal Key Integrity Protocol* (TKIP) para el cifrado de datos. la autenticación 802.1x se ha introducido en este protocolo para mejorar la autenticación del usuario.

WIFI PROTECTED ACCESS 2 (WPA2): basado en IEEE 802.11i, es un nuevo protocolo de seguridad inalámbrica en el que sólo los usuarios autorizados puedan acceder a un dispositivo inalámbrico, con las características que apoyan la criptografía fuerte (por ejemplo, Norma de codificación avanzada o AES), Control de autenticación fuerte.

WiFi: se define como una especificación para un conjunto de protocolos de comunicación para estandarizar la forma en que los dispositivos inalámbricos, puedan ser utilizados para acceso a Internet.

WIRELESS LOCAL ÁREA NETWORK: una red de área local inalámbrica (WLAN) es un tipo de red de área local que utiliza ondas de radio de alta frecuencia en lugar de cables para la comunicación entre dispositivos habilitados para red.

WPA: el acceso WiFi Protected es un protocolo de seguridad para redes inalámbricas que fue diseñado para reemplazar WEP. Utiliza TKIP para cifrar los datos y es mucho más resistente a los ataques que WEP, pero todavía tiene vulnerabilidades criptográficas que hacen que sea indeseable para el uso. WPA fue un proyecto IEEE 802.11i.

WPA: WPA o *Wifi Protected Access*, es una forma muy mejorada de cifrado de datos inalámbricos. Carece de las vulnerabilidades de WEP que tenía, mientras que al mismo tiempo facilita la instalación y el uso de las redes WiFi.

WPA2: *wifi Protected Access v2* es actualmente el protocolo de cifrado más potente disponible para redes inalámbricas, y es el estándar 802.11i actual. Se utiliza el cifrado AES de datos y es considerado criptográficamente fuerte. WPA2 Personal utiliza una PSK para establecer la autenticación inicial, pero WPA2 Enterprise puede utilizar varios métodos de EAP para garantizar una autenticación fuerte sin la necesidad de un PSK.

WPS: *wiFi Protected Setup* hace que sea más fácil para los usuarios añadir clientes WiFi para redes inalámbricas WPA y WPA2 protegida. Fue pensado para ayudar a los usuarios domésticos no técnicos implementar la seguridad WPA, pero es vulnerable a un ataque de fuerza bruta y no debe ser utilizado. WPS puede utilizar una PSK, la configuración de cifrado transferidos mediante una memoria USB, un PIN, NFC, o con un enfoque simple pulsador.

RESUMEN

El siguiente trabajo se orienta a determinar los principales ataques a los que se exponen los usuarios que utilizan la red Wifi "**IDEA internet en el parque**", la cual hace parte de la estrategia del Instituto para el Desarrollo de Antioquia - IDEA, el cual ofrece internet libre en el parque Rafael Uribe Uribe del Municipio de Urrao. Además de ello, se busca identificar los principales ataques que se pueden presentar dentro de la radiofrecuencia, que brinda la señal a los habitantes, transeúntes, turistas, entre otros más; del parque en cuestión. Por consiguiente, se han planteado varios objetivos, para identificar y medir la seguridad que la red wifi brinda a los usuarios. Al desarrollar el objetivo general y los objetivos específicos, se ha edificado con varias pruebas técnicas; que la red wifi en cuestión, ostenta brechas de seguridad para los datos sensibles de los usuarios. También recomienda varias técnicas que los usuarios pueden implementar a la hora de conectarse y disfrutar los beneficios de tener una zona Wifi gratuita y pública son específicos a al modo de operar, lo que significa que hay un lugar más donde pueda conectarse a un mundo en el que se sienta cómodo, donde pueda investigar, este puede ser el parque más cercano, la cafetería de un amigo, entre otros, para ver fotos de aventuras de los amigos, y averiguar los datos de que quiera consultar, sin gastar el plan de datos. Pero aparte de lo que permite a los usuarios, hay muchos otros beneficios de tener una zona pública de conexión Wifi; pero, ante todo, implica que el usuario este expuesto a amenazas y vulnerabilidades.

El estado de la seguridad Wifi ha mejorado significativamente en los últimos años, pero la mayoría de los usuarios no conocen la seguridad que este tema requiere en la actualidad, donde es necesario identificar y aplicar, las recomendaciones de los expertos, sobre la seguridad que se debe tener presente en las redes Wifi gratis, ya que la confidencialidad, la integridad y la disponibilidad de los datos está en riesgo y los administradores de la seguridad de la información, todavía tienen que mantenerse al tanto de las nuevas amenazas, evaluar su riesgo, y tomar las medidas apropiadas.

Palabras clave: Seguridad Wifi, redes inalámbricas, riesgos, expertos, amenazas, ataques, vulnerabilidades.

INTRODUCCIÓN

El Instituto para el Desarrollo de Antioquia – IDEA, ha logrado una sinergia con el gobierno local, la academia, la industria y los ciudadanos para crear un entorno propicio para la ciencia, la innovación y el uso de las tecnologías de la información y las comunicaciones (TIC), son ingredientes claves para el desarrollo de la sociedad; dentro de los parques principales de los 115 municipios antioqueños ubicados por fuera de la subregión del Área Metropolitana; donde los dirigentes creen que las TIC proporcionarán las herramientas para el empoderamiento ciudadano, la equidad y el acceso a los servicios proporcionados por el gobierno local a través la implementación de la estrategia Internet libre en el parque del Municipio de Urrao, el cual es denominado "**IDEA internet en el parque**", programa ha sido pionero en el uso de las tecnologías digitales desde junio del 2011 y faculta a la participación del público mediante la creación de reuniones físicas y virtuales donde los ciudadanos pueden dar su opinión sobre el desarrollo de políticas públicas y fomentar la creación de proyectos que pueden mejorar la calidad de vida de la 44.648 habitantes del Municipio.

En términos de aprovechamiento de las TIC, la Gobernación de Antioquia, ha establecido objetivos que deben cumplirse para apoyar la estrategia "**Internet en el parque**", incluyendo una conexión Wifi abierta con un perímetro de 115 municipios Antioqueños, donde los parques públicos serán dotados de internet wifi gratuito; los cuales son destinados para uso de los residentes, comerciantes, incluyendo todo lo relacionado con la internet, desde las tareas de investigación, la interacción social, entre otros aspectos más. También cuentan con la implementación de formación relacionada con cursos dictados por el SENA, los cuales son centrados en el uso de la Internet de una manera segura y protegida, así como el uso de dispositivos móviles y servicios en línea.

Esta innovación ha hecho que los usuarios que poseen dispositivos móviles, quieran aprovechar esta ventaja que le ofrece la estrategia "**Internet al parque**", donde la tecnología Wifi ha cambiado significativamente la forma en que se realizan las consultas en la red; además de permitir interactuar con el mundo digital desde cualquier lugar del mundo físico. Por otra parte, las personas que viven, trabajan o se desplazan por el parque Rafael Uribe Uribe, del municipio de Urrao; usen sus dispositivos electrónicos tales como los ordenadores portátiles o los teléfonos inteligentes para conectarse a la red "**IDEA internet en el parque**", ya que esta se transporta a través de las ondas de radio que se desplazan por las tiendas, los cafés, locales comerciales, las cadenas de restaurantes, entre otros. Esta libertad tiene un precio muy alto, sin embargo, pocos entienden

realmente los riesgos asociados con las redes Wifi públicas y las conexiones que se crean con estas redes de datos. Aprender a proteger los datos personales, asegurarán la integridad de los datos sensibles que reposan en cada dispositivo que se conecta a la red Wifi.

1. DEFINICIÓN DEL PROBLEMA

El instituto de desarrollo de Antioquia – IDEA, ofrece el servicio de "**Internet al parque**", cuya finalidad o estrategia, es brindar una conexión a internet en los principales parques de 115 municipios antioqueños ubicados por fuera de la subregión del Área Metropolitana. Entre los municipios beneficiados por el proyecto, se encuentra el municipio de Urrao, el cual ostenta el parque Rafael Uribe Uribe, donde también es conocido como la "**Plaza Rafael Uribe**", el cual es muy visitado, por transeúntes y turistas que lo visitan a diario, por su gran estructura y más que todo por la belleza que este ostenta, pues posee varias estructuras diseñadas por Maestro internacional Humberto Elías Vélez Escobar, y es apetecido para descansar, relajarse y tomarse fotos; además de brindar acceso a la red Wifi "**IDEA internet en el parque**". Pero la mayoría de las personas solo piensan en la opción de poder conectarse a acceder a las redes Wifi de internet libre en los parques, además de ser un servicio totalmente gratis; pero estos usuarios no saben a ciencia cierta, sobre los problemas de seguridad asociados con ataques informáticos a los que exponen sus datos e integridad personal, además de las vulnerabilidades de seguridad que hacen parte de la utilización de las tecnologías inalámbricas; donde los puntos de acceso Wifi gratuitos son deseables para los consumidores, por ende se hacen deseables para los hackers; al saber que no requiere autenticación para establecer una conexión de red. Esto crea una oportunidad increíble para el hacker para obtener un acceso sin restricciones a los dispositivos sin garantía en la misma red.

Donde según (SCHLESINGER, 2016), la empresa de Ciberseguridad *Symantec*, ha realizado un estudio sobre la manera de cómo la mayoría de las personas desconocen los riesgos de usar Wi-Fi pública de los consumidores estadunidenses. Las actividades comunes en Wi-Fi público incluyen el acceso a las cuentas de correo electrónico personal (58%), acceso a medios sociales (56%) y acceso a información bancaria o financiera (22%). Otro 13 por ciento ha ingresado información de identificación personal. Toda esta información podría ser robada si la conexión Wi-Fi no es segura.

1.1 FORMULACIÓN DEL PROBLEMA

¿A que ataques informáticos están expuestos los usuarios que se conectan a la red wifi “**¿IDEA internet en el parque”, del municipio de Urrao?**

1.2 OBJETIVOS

1.2.1 Objetivo General

I. Determinar los principales ataques y las vulnerabilidades informáticas que intervienen, en la red WIFI "**IDEA internet en el parque**", de la plaza Rafael Uribe Uribe, del municipio de Urrao.

1.2.2 Objetivos específicos

I. Investigar tres tipos de ataques a los que están expuestas las redes WIFI.

II. Realizar tres tipos de ataques controlados a la red WIFI "**IDEA internet en el parque**" para determinar si esta posee vulnerabilidades que afectan a la red y a sus usuarios.

III. Analizar y recomendar buenas prácticas de seguridad para que sean tenidas en cuenta por los usuarios de la red WIFI "IDEA internet en el parque", de la Plaza Rafael Uribe Uribe del municipio de Urrao antes de conectarse a la red.

IV. Recomendar mejoras de seguridad de la información en la configuración de la red "**IDEA internet en el parque**", de la Plaza Rafael Uribe Uribe para prevenir ataques que puedan afectar a la red y a sus usuarios.

1.2 JUSTIFICACIÓN

Este proyecto pretende ilustrar diversos que ponen a prueba la seguridad de datos a través de redes inalámbricas y la seguridad global de las redes. Determinar los ataques a los que se exponen los usuarios que utilizan la red Wifi "**IDEA internet en el parque**", de la plaza Rafael Uribe Uribe, del municipio de Urrao. De tal modo que se procederá a identificar las falencias de seguridad que la red ostenta, al ser de puntos de acceso Wifi gratuitos deseables para los consumidores hacen deseables para los hackers; a saber, que no requieren autenticación para establecer una conexión de red. Esto crea una oportunidad increíble para los hackers logren el acceso sin restricciones a los dispositivos sin garantía en la misma red. La mayor amenaza para la seguridad Wifi gratis, es la oportunidad para que los hackers se posicionen entre los usuarios y el punto de conexión, proporcionando una abertura para todo tipo de robo de datos, en particular las contraseñas e información privada.

Las contribuciones que hace este proyecto con la solución del problema que se presenta en la red wifi, resalta en la manera de como los usuarios tienen la oportunidad de proteger los datos sensibles de los ataques informáticos, por medio de la implementación de varias técnicas defensivas y recomendaciones de seguridad, además de gozar del beneficio del acceso a las redes Wifi de internet en el parque, con la confianza de ingresar al mundo de la tecnología inalámbrica, proporcionándoles numerosos beneficios, y aumentando la confianza en los puntos de acceso públicos, por medio del despliegue de este tipo de redes, los cuales se encuentran localizados en 115 municipios que ofrecen acceso a zonas Wifi, sin costo en los principales municipios del departamento de Antioquia; por lo tanto, los usuarios, disfrutaran de espacios aptos para la generación de oportunidades, a través del acceso a recursos técnicos y tecnológicos que promuevan el desarrollo social, el cual traerá un enorme beneficio para los ciudadanos y a la vez, les permitirá el ingreso hacia el uso de las tecnologías de la información y la comunicación, por ende les mejorara su calidad de vida.

2. MARCO REFERENCIAL

Es importante conocer el surgimiento de la historia de la tecnología, para comprender mejor la situación a la que hay que enfrentarse en la actualidad, por lo tanto resulta muy atractivo conocer cuántos sucesos tuvieron que ocurrir para llegar a la conclusión o el análisis de la seguridad que se aplica a los datos de los usuarios, además de conocer quiénes fueron las personas que pensaron e imaginaron los diferentes desarrollos tecnológicos e incluso establecer hacia dónde se dirige la tecnología y de la misma manera saber hacia dónde apunta el desarrollo de las grandes ciudades, con el apoyo de las tecnologías de la comunicación, representado en las redes inalámbricas Wifi, las cuales requieren de un conocimiento básico sobre la seguridad informática.

En el pasado se han llevado a cabo diversas propuestas, análisis, estudios, formatos de evaluación, manuales de evaluación y apartados técnicos sobre la investigación y determinación de las situaciones de seguridad informática que generaron gran brecha de seguridad de la información en las redes Wifi públicas, las cuales se han presentado problemas relacionados con los ataques informáticos y vulnerabilidades, que han sido aprovechadas por los hackers. Por ello, se requiere la adopción de una serie de estrategias e implementación técnicas de defensa y recomendaciones a seguir, las cuales deben ser apoyadas por personal cualificado, sobre la seguridad informática que se debe tener, antes de conectarse a redes Wifi gratis.

2.1 ANTECEDENTES

Si bien es cierto que existen en el momento varias propuestas, estrategias, manuales, modelos y los respectivos formatos de evaluación de seguridad de la información en redes Wifi, no todos estos contienen toda la información suficiente; siendo la totalidad de ellas demasiado breves, o contienen poca información sobre los procesos que se llevan a cabo, o por el contrario son muy pocos los casos, en que resultan muy extensas y de difícil uso en contextos de incidencia, aunque no con todos los datos que se requieren únicamente para evaluar las condiciones de seguridad ante posibles vulnerabilidades, las cuales son ataques, ya que a veces incluyen información legal, financiera, daños detallados de los datos y partes físicas de los equipos. Por lo tanto, en ciudades o en entidades del país se han venido preparando planes, estrategias, procedimientos y mejoramiento de

gobierno TI en las Instituciones Educativas que permitan reaccionar oportunamente ante algún imprevisto ocurrido o por ocurrir que afecta los datos y la información.

Comenta (Herranz, 2016) “cuando llegamos a fin de mes pelados con los megas, o vemos que no vamos a llegar estamos buscando estas zonas, y es que el WiFi quien tienta. Para empezar, no utilizar los datos y no gastar, nos tira lo que es gratis”.

Las redes wifi publicas contiene demasiados agujeros de seguridad, donde según (Monica, 2016), en su informe sobre *wifi Risk Report 2016*, en el que se ha encuestado a más de 9.000 personas en nueve países, la confusión sobre la seguridad de las redes wifi públicas puede hacer que los usuarios se conviertan en objetivos fáciles para los hackers.

Según (Marina, 2014), el equipo de Avast ha realizado un experimento de hacking a nivel global, donde los expertos de seguridad de Avast han viajado a ciudades de Estados Unidos, Europa y Asia para observar la actividad WIFI en nueve áreas metropolitanas, cuyo experimento ha revelado que la mayoría de los usuarios de dispositivos móviles no toman las medidas necesarias para proteger sus datos y su privacidad de los cibercriminales. En Estados Unidos, los expertos de Avast visitaron Chicago, Nueva York Y San Francisco; en Europa visitaron Barcelona, Berlín y Londres; en Asia visitaron Hong Kong, Seúl y Taipéi.

El estudio reveló que los usuarios en Asia son más propensos a los ataques. Los usuarios en San Francisco y en Barcelona suelen tomar más medidas para proteger la navegación web; en Europa son más conscientes de los riesgos de utilizar redes inseguras. Los usuarios en Asia se conectan a redes abiertas con más frecuencia, mientras que los europeos y los americanos lo hacen con menos frecuencia. En Seúl, 99 de cada 100 usuarios se conectan a redes inseguras, mientras que en Barcelona y San Francisco lo hacen 80 de cada 100. Gracias al experimento, se pudo descubrir que una significante proporción de usuarios de dispositivos móviles navegan, principalmente, en sitios HTTP inseguros. El 97% de los usuarios en Asia se conectan a redes WiFi abiertas e inseguras. Siete de cada diez Reuters protegidos con contraseña utilizan métodos de cifrado débiles y sencillos de hackear. Cerca de la mitad del tráfico Web en Asia se realiza en sitios HTTP desprotegidos, mientras que en Estados Unidos es una tercera parte y en Europa una cuarta parte del tráfico Web. Esto se puede atribuir al hecho de que en Europa y Estados Unidos hay más páginas web que utilizan el protocolo HTTPS que en Asia.

Conectarse a una red WIFI pública tiene sus riesgos. (Ashton, 2015), especialista en seguridad informática de la consultora Druidics, explica cuáles son y brinda recomendaciones para que los usuarios eviten pérdida de plata y dolores de cabeza, aconseja no abrir páginas o sitios sensibles que requieren claves y contraseñas en conexiones públicas, también recuerda que en la barra de direcciones de los sitios sensibles que se utilizan debe aparecer la imagen de candadito de seguridad. Si no aparece, está roto o aparece una pantalla que dice que hay un error en el certificado de seguridad, es conveniente no seguir adelante y desconectarse.

Aclaran (Keita Sory Fanta, 211), sobre las vulnerabilidades existentes en los protocolos implementados para la seguridad en redes WIFI, tales como las de los protocolos WEP, existen vulnerabilidades inherentes al formato y uso de las tramas MAC dependiendo del tipo de trama que se está analizando. Estas vulnerabilidades constituyen unas de las bases de las amenazas a las cuales están sometidas las *WLANs*; donde además de ello las tramas de administración en el estándar 802.11 no tienen protección criptográfica implementada. Los paquetes de manejo de la comunicación viajan en texto claro, posibilitando la obtención de la dirección MAC del AP o del nodo cliente por simple análisis del tráfico capturado por parte del atacante.

Según (Anónimo, 2014), una red de hackers, empleo durante al menos cuatro años la red WiFi de hoteles de lujo en varios países para hacerse con información sensible de ejecutivos y analistas del sector privado de empresas estadunidenses y asiáticas, como parte de una campaña de robo de datos; según informe de la empresa de seguridad informática *Kaspersky Labs*, descubrió que los denominados ataques "*DarkHotel*", se llevaron a cabo durante al menos cuatro años. Los hackers aprovechan las vulnerabilidades que las redes WIFI, ostentan, lo cual es ocasionado por malas configuraciones, por lo tanto, seleccionan su objetivo, luego realizan la fase de reconocimiento y luego realizan la explotación de la información, por medio de los ataques cibernéticos.

Un estudio realizado por Avast en Brasil, ha demostrado que cuatro de cada cinco hogares conectados a Internet están en riesgo de ataques a través de sus routers inalámbricos, los cuales se pueden representar en un 81% de las redes WIFI; según un estudio reciente realizado por Avast Software. Si un router no es adecuadamente seguro, los ciberdelincuentes pueden acceder fácilmente a la información personal de un individuo, incluyendo información financiera, contraseñas, fotos y el historial del navegador Internet, según estudio publicado por (Marina, 2014).

Las consecuencias de conectarse a redes WIFI gratis en entornos públicos, sin tener en cuenta las consecuencias que esto puede acarrear; las cuales se pueden manifestar con la medida de dejarle la puerta abierta a todos los hackers que deseen esculcar en nuestros archivos, para luego hacerse pasar por los usuarios en redes sociales e, incluso, infectar con un virus los dispositivos que se han conectado, según (Lab, 2016).

Según (Segurity, 2015), las personas no piensan cuánto cuesta el valor del robo de tus datos personales en una red WIFI pública, las cuales están disponibles en hoteles, restaurantes, bibliotecas, aeropuertos, parques y estaciones de tren. Donde lo que necesita un atacante, son tan solo 70 euros, un coeficiente intelectual medio y un poco de paciencia, defiende el hacker (*Wouter Slotboom*). Este experto en seguridad ha demostrado cómo, en tan solo 20 minutos, es capaz de conseguir los datos personales de casi todos los usuarios de una cafetería de Ámsterdam e incluso un historial de sus últimas búsquedas en Google.

Según (María, 2014), tener acceso a Internet a través de una Wifi pública es una alternativa válida y útil para estar siempre conectados, dentro y fuera de casa y con cualquier dispositivo, además de permitirnos ahorrar en nuestra tarifa de datos. Pero este tipo de conexiones entrañan una serie de riesgos a tener en cuenta antes de dar al botón de “conectar”.

Según (Antonio, 2014), el uso de puntos de acceso Wifi públicos puede ser muy atractivo con la llegada del verano y los viajes, pero los usuarios deben conocer los riesgos que ello implica y tomar precauciones para mejorar su seguridad. Algunos consejos pueden prevenir problemas y aumentar la protección de los usuarios y sus datos al usar ese tipo de redes de conexión.

Comenta (Zordan, 2015). “Conectarse a una red Wifi desconocida es muy arriesgado, ya que todos los datos que se envían o reciben pueden ser interceptados fácilmente. Los usuarios ponen en riesgo la seguridad de su información personal, su identidad digital y su dinero”, advierte Dmitry Bestuzhev, director del Equipo de Investigación y Análisis de *Kaspersky Lab*.

Según (Ruben, 2012). ESET Latinoamérica acaba de publicar los resultados de una encuesta efectuada en Latinoamérica en el que recoge un grupo de elementos importantes en relación a este tipo de conexiones, en el mencionado estudio el 36.5% de los usuarios afirmó conectarse a cualquier red inalámbrica sin evaluar siquiera si esta es de confianza o cumple con las condiciones mínimas de seguridad establecida.

El mayor peligro con acceso Wifi es el hecho de que toda la información que está transfiriendo entre el ordenador y el equipo que se está teniendo acceso está disponible para todo el mundo en la red. Tal como se ha visto, según (Eduardo, 2016), el Wifi público, que permite conectarse a internet de manera gratuita, puede convertirse en un arma de doble filo. Según expertos en el tema, este tipo de redes son una puerta abierta para los cibercriminales. El afán de estar en sintonía con el mundo virtual genera, en ocasiones, que los usuarios pasen por alto las reglas básicas de seguridad informática.

Se observa claramente que según (Samuel, 2014), en muchas en ocasiones no tenemos la posibilidad de contar con datos móviles que nos faciliten adelantar algún trabajo, buscar información, alguna dirección o enviar fotos, videos, mensajes, archivos, etc. Y al encontrarnos con algún punto donde se encuentre una red gratuita al momento queramos tomar mano de ella. Sin dudas a todos nos ha pasado, más si se presenta alguna emergencia o el tiempo de llegada a casa u oficina no será de manera inmediata. Por ello las redes WiFi públicas están en todas partes. Todos lo usamos, pero la mayoría de nosotros no somos conscientes de los riesgos y no se toman las precauciones necesarias para proteger a nosotros mismos.

Una de las mayores preocupaciones de los usuarios inalámbricos es asegurarse de que su router y la red inalámbrica son seguros. Según (Nora, 2015), desafortunadamente, muchas redes Wifi están configuradas para capturar comunicaciones seguras y esperar que los usuarios acepten el certificado de servidor. Una vez aceptado, puede ser reutilizado más adelante sin que el usuario se dé cuenta. Por lo tanto, la configuración de una Wifi pública es insegura por naturaleza.

La conectividad inalámbrica es tan omnipresente que difícilmente se puede imaginar la vida sin ella. Casi todas las empresas y los usuarios tienen al menos un punto de acceso o enrutador desplegado en las instalaciones. La tecnología Wifi le ayuda a moverse más rápido y fácil conexión a la web, sin necesidad de cables, cables de red u otros medios físicos. La parte negativa es que puede permitir a los hackers aprovechen las vulnerabilidades. Por las consideraciones anteriores, se añade que según (Sergio, 2015), se ha descubierto una nueva vulnerabilidad en las redes inalámbricas Wifi 802.11n que no tienen habilitado cifrado WPA o WPA2, es decir, todas aquellas redes Wifi que utilicen el estándar 802.11n y estén abiertas, podrían estar afectadas. Este fallo tiene consecuencias graves como por ejemplo la desautenticación de clientes, ARP Spoofing o saltarse las reglas de un firewall; este se conoce como *Injection Attacks on 802.11n MAC Frame Aggregationes*.

Según las conexiones Wifi representan un eslabón importante en la tecnología; sin embargo, hay ciertas recomendaciones que debemos recordar sobre la implementación de las redes Wifi públicas plantean muchos riesgos de seguridad para los usuarios, pero afortunadamente hay muchos consejos a emplear para mantenerse a salvo y seguro en línea

Los profesionales de seguridad tienen que asegurarse de que los usuarios finales a comprender las implicaciones y riesgos involucrados en el envío de un correo electrónico del trabajo a través de una red pública, por lo que no hay que subestimar el poder de la educación continua a todos los empleados de gente de nivel inicial hasta el final hasta a los ejecutivos, los cuales requieren acatar los concejos de expertos sobre el buen uso y la forma segura de conectarse a redes Wifi de forma segura. Comenta (Antonio, 2014). El uso de puntos de acceso Wifi públicos puede ser muy atractivo con la llegada del verano y los viajes, pero los usuarios deben conocer los riesgos que ello implica y tomar precauciones para mejorar su seguridad. Algunos consejos pueden prevenir problemas y aumentar la protección de los usuarios y sus datos al usar ese tipo de redes de conexión.

Hay algunos grandes problemas con el uso de una red Wifi públicas, donde la naturaleza de ser la red abierta, permite el espionaje; además de que la red podría estar llena de máquinas comprometidas, o lo más preocupante, la zona interactiva en sí podría ser maliciosa. Asegura (Agudo, 2015), “Wifi Gratis: Una amenaza para usuarios confiados, puede que más de uno hayamos usado alguna de estas redes alguna que otra vez pensando que teníamos un chollo en las manos. Si hay algo que podemos asegurar es que, si algo es demasiado bueno para ser cierto, entonces probablemente lo sea. Lo mejor para evitar problemas, como decimos siempre, es usar el sentido común como primera línea de defensa”.

Se ha vuelto mucho más común hoy en día para encontrar ciudades que ofrecen WiFi gratuito para sus habitantes, especialmente en las zonas de mayor confrontación y educación. Sin embargo, hay que analizar qué ventajas y desventajas se logran con esta estrategia. (Martínez, 2012). La integración de los dispositivos móviles, Internet y la conectividad inalámbrica ofrece una oportunidad extraordinaria para que las organizaciones puedan extender su información y servicios hasta los profesionales y clientes móviles.

2.2 MARCO TEÓRICO

La demanda de redes inalámbricas wifi, nos hacen vulnerables a las amenazas y más que todo cuando estas son de son de acceso público, debido a que permiten que cualquier persona en el rango de la zona activa, pueda utilizar el servicio, con buenas o malas intenciones. Aunque la mayoría de los usuarios creen que ingresan a la red de manera segura, pero no saben que los piratas informáticos se están volviendo más inteligentes y las redes públicas son los servidores ideales para comprometer los datos y cuentas sin que las víctimas se den cuenta. Como individuos podemos trabajar para protegernos en línea y los anfitriones de la red deben tener como prioridad principal, la seguridad de las conexiones del Internet, para que la navegación sea segura en las redes públicas. La comodidad que proporciona las redes WiFi es indispensable, pero sacrificar la seguridad de la conectividad tiene sus consecuencias. Las grandes redes públicas ostentan un alto grado de susceptibilidad con las actividades fraudulentas.

Comenta (Pacheco), es de oficial conocimiento que los puntos de acceso públicos de restaurantes, hoteles, aeropuertos, entre otros, son focos vulnerables a los ataques cibernéticos, porque normalmente, no suelen ser redes protegidas. De tal modo que la seguridad en la red WIFI "**IDEA internet en el parque**", de la Plaza Rafael Uribe Uribe del municipio de Urrao; es un factor importante a considerar; ya que enmarca un factor que puede ser utilizado por personas malintencionados, con la finalidad de acceder a los archivos privados e información sensible del usuario en cuestión.

Según (Rodríguez, 2015), comenta sobre los riesgos que las redes wifi publicas contemplan, donde el director técnico de *PandaLabs* en *Panda Security*, Luis Corrons advierte que, "si no sabemos de dónde procede ni quién maneja esta conexión, lo mejor es no probarla". Además de ello, explica Corrons, la manera de como "Sería muy fácil que intentase infectar tu dispositivo con *malware* o redirigiese tu tráfico a páginas fraudulentas para robar tus datos". Por desgracia, estos puntos de acceso abiertos pueden atraer a los usuarios maliciosos que buscan robar datos. Si está utilizando su equipo celular en una red sin cifrar, puede ser posible que un hacker para robar su ID de usuario, contraseñas e incluso números de tarjetas de crédito.

La seguridad de las redes inalámbricas Wifi, permanecerán siendo áreas de investigación interesantes, las cuales apoyan las tecnologías de todos los dispositivos que hay en el mercado actual; ya que estos permiten facilidad de uso y la flexibilidad de las comunicaciones en el mundo de la informática sin manipular el contenido existente. "Comenta (Anabalón P, 2005), es muy común encontrar

redes en las que el acceso a Internet se protege adecuadamente con un firewall bien configurado, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior del edificio. Cualquier persona que desde el exterior capte la señal del punto de acceso, tendrá acceso a la red de la compañía, con la posibilidad de navegar gratis en la Internet, emplear la red de la compañía como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, entre muchas otras cosas; además de convertirse en una puerta trasera que vulnera por completo la seguridad informática"

Los detalles de por qué una conexión no segura puede ser un problema es más oscuro, sin embargo, los métodos que se pueden utilizar para reforzar su seguridad, incluso cuando se utiliza un punto de acceso público sin garantía, se debe conocer los riesgos exactos de seguridad Wifi en redes públicas, y las soluciones que hay disponibles, hacen frente a esos riesgos, pero en la actualidad los ciberdelincuentes han desarrollado técnicas que sobrepasan los niveles que están preestablecidos en estudios recientes. En verdad, la obtención de datos, incluso a través de una red Wifi pública requiere un cierto nivel de conocimiento acerca de software, tales como: *Kali Linux*, escáneres Wifi, entre otros más; además de que la persona promedio simplemente no posee las habilidades necesarias. Sí, hay herramientas como la extensión *Firesheep* para *Firefox* que puede secuestrar sesiones fácilmente en teoría, pero en la práctica algunos conocimientos técnicos se requieren generalmente para hacer algo verdaderamente malicioso.

Es importante poner de relieve las principales especificaciones de las normas comunes de seguridad en las redes wifi, tales como WEP, WPA y WPA2. En la misma luz, el estudio explora el concepto de red inalámbrica de acceso metropolitano y sus especificaciones de seguridad, además de la vulnerabilidad a la violación de la seguridad. Por último, el estudio resume con varias técnicas de defensa, recomendaciones acerca de la seguridad de la red inalámbrica, junto con amplias propuestas para mejorar la seguridad inalámbrica, especialmente en un entorno público; además de un informe detallado sobre sobre la regulación y los niveles trabajan en el ámbito de la seguridad de la red, sobre todo en la red inalámbrica, además de verificar el cumplimiento bajo los estándares de la ley.

Del mismo modo, el estudio examinó los trabajos realizados por otros investigadores en materia de seguridad en una red inalámbrica, y las medidas de protección inalámbricas actuales. Se estableció que las medidas indicadas por estos investigadores fueron en gran medida insatisfactorias, debido a los avances en la tecnología que sirven para poner en peligro las medidas empleadas. El investigador analizó diferentes herramientas que utilizan, para atacar a una red

inalámbrica y con éxito se identificaron varios tipos de ataques, poniendo en evidencia algunas lagunas en la red Wifi analizada. El estudio concluyó que las redes inalámbricas no pueden hacerse completamente segura, y sólo deben utilizarse para atender las necesidades de las organizaciones, en lugar de uno de conveniencia. De acuerdo con estos hallazgos y conclusiones, el estudio recomienda la adopción de medidas sirven para mejorar la seguridad en un lugar de despliegue inalámbrico.

2.3 MARCO LEGAL

Ley 1273 de 2009, “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

Ley 1341 de 2009, según (Alcaldía de Bogotá, 2009), contempla de los siguientes artículos:

Artículo 1°. Objeto. La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

Artículo 2°. Principios orientadores. La investigación, el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones son una política de Estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los Derechos Humanos inherentes y la inclusión social.

Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

Son principios orientadores de la presente ley:

I. Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones. El Estado y en general todos los agentes del sector de las Tecnologías de la Información y las Comunicaciones deberán colaborar, dentro del marco de sus obligaciones, para priorizar el acceso y uso a las Tecnologías de la Información y las Comunicaciones en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación, los contenidos y la competitividad.

Artículo 3°. Sociedad de la información y del conocimiento. El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

Artículo 4°. Intervención del Estado en el sector de las Tecnologías de la Información y las Comunicaciones. En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:

a) Proteger los derechos de los usuarios, velando por la calidad, eficiencia y adecuada provisión de los servicios.
b) Promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal.
c) Promover el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen Tecnologías de la Información y las Comunicaciones y la masificación del Gobierno en Línea.
d) Promover la oferta de mayores capacidades en la conexión, transporte y condiciones de seguridad del servicio al usuario final, incentivando acciones de prevención de fraudes en la red.
e) Promover y garantizar la libre y leal competencia y evitar el abuso de la posición dominante y las prácticas restrictivas de la competencia.
f) Garantizar el despliegue y el uso eficiente de la infraestructura y la igualdad de oportunidades en el acceso a los recursos escasos, se buscará la expansión, y cobertura para zonas de difícil acceso, en especial beneficiando a poblaciones vulnerables.

g) Garantizar el uso adecuado del espectro radioeléctrico, así como la reorganización del mismo, respetando el principio de protección a la inversión, asociada al uso del espectro. Los proveedores de redes y servicios de telecomunicaciones responderán jurídica y económicamente por los daños causados a las infraestructuras.

h) Promover la ampliación de la cobertura del servicio.

i) Garantizar la interconexión y la interoperabilidad de las redes de telecomunicaciones, así como el acceso a los elementos de las redes e instalaciones esenciales de telecomunicaciones necesarios para promover la provisión y comercialización de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones.

j) Imponer a los proveedores de redes y servicios de telecomunicaciones obligaciones de provisión de los servicios y uso de su infraestructura, por razones de defensa nacional, atención y prevención de situaciones de emergencia y seguridad pública.

k) Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones.

l) Incentivar y promover el desarrollo de la industria de tecnologías de la información y las comunicaciones para contribuir al crecimiento económico, la competitividad, la generación de empleo y las exportaciones.

m) Propender por la construcción, operación y mantenimiento de infraestructuras de las tecnologías de la información y las comunicaciones por la protección del medio ambiente y la salud pública

2.4 MARCO CONTEXTUAL

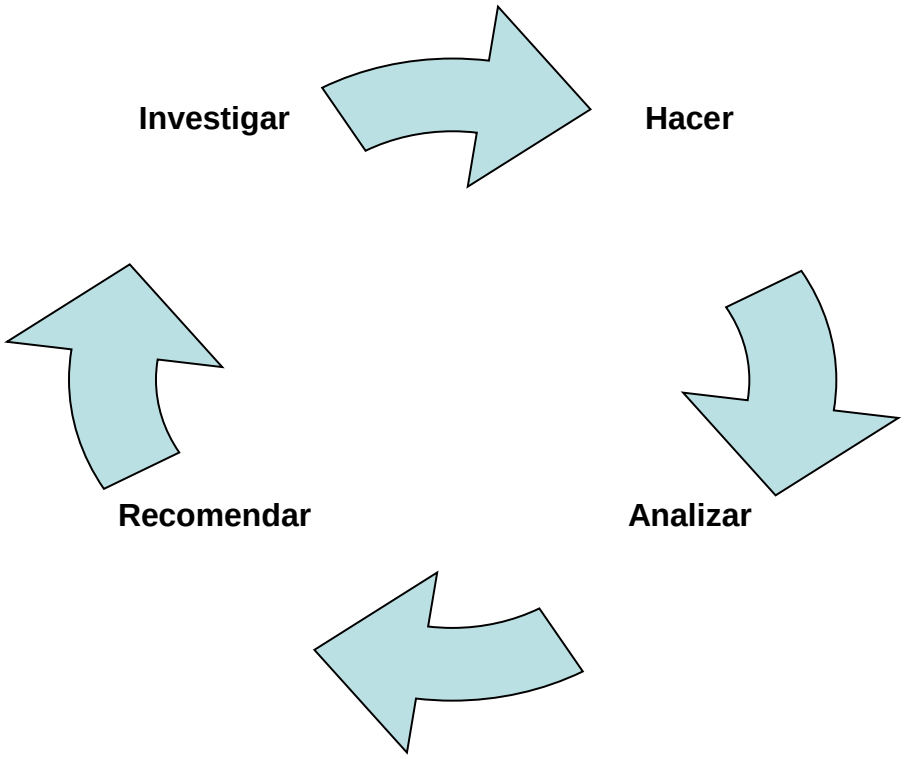
El presente proyecto se desarrolló en el Municipio de Urrao, más precisamente en el parque Rafael Uribe Uribe, cuya localización se aprecia al final del documento, en los anexos del proyecto. En dicho parque se realizó varias pruebas técnicas sobre los ataques más comunes que se presentan frecuentemente en las redes wifi públicas, tales como lo son los ataques de Spoofing o suplantación de DNS, ataque de denegación de servicio o *DoS*, ataques de *Phishing*, *Man in the middle y ARP Spoofing*; siendo estas algunas de las formas más comunes de que la privacidad se puede romper durante el uso de acceso a cualquier red wifi, donde el parque Rafael Uribe Uribe, del municipio de Urrao, le brinda a la comunidad más cercana, el beneficio de acceder a la red wifi "**Idea internet en el parque**" donde además se realizó el análisis de cada una de las pruebas obtenidas. Por desgracia, los puntos de acceso a redes wifi públicos, también permiten a

cualquier persona dentro de la zona; leer potencialmente datos que no se dirigen a ellos, convirtiéndose en un problema de seguridad, debido a que la red wifi, cuenta con poca protección de datos, de tal modo que es muy importante la realización del proyecto, en pro de alertar a los usuarios sobre los riesgos a los que exponen la seguridad de la información y la integridad de los usuarios.

3. METODOLOGÍA DE DESARROLLO

El presente proyecto, se desarrolló teniendo en cuenta las siguientes etapas:

Figura 1. Etapas del proyecto



Fuente: El autor

3.1 Investigar

Se realizo la investigación referente a los tipos de ataques que pueden afectar a la red wifi ““**IDEA internet en el parque**”, de la Plaza Rafael Uribe Uribe del municipio de Urrao”, y se describe en el proyecto los ataques más comunes, teniendo en cuenta su funcionamiento e impacto con respecto a los efectos que puede causar a la seguridad de la información.

3.2 Hacer

Por medio de pruebas de *pentesting* y análisis de vulnerabilidades, las cuales fueron ejecutadas a través de un computador portátil, el cual fue programado con el sistema operativo *Kali Linux* o del sistema *Parrot Security OS*, los cuales están dotados del repertorio de herramientas para pruebas de penetración y escaneo de vulnerabilidades en todo tipo de redes. También se debe mencionar, que las pruebas se desarrollaron cada tres días de la semana durante un mes, para poder analizar el tráfico de la red, con la finalidad de identificar tendencias entre días y semanas. Seguidamente se ha requerido de 65 días, para tabular la información y analizar e interpretar los hallazgos; además de realizar el informe final. Para ello, se debe seguir los procedimientos del *Hacking* Ético, y la delimitación del acceso no autorizado de la información confidencial de los usuarios; los cuales son apoyados por el decreto 1273 de 2009, sobre los delitos informáticos.

3.3 Analizar

Se analizaron los resultados de las pruebas ejecutadas en los diferentes ataques, para realizar las recomendaciones de mejora enfocada a la seguridad de la información.

3.4 Recomendar

Los hallazgos de los informes generados, fueron sometidos a un análisis detallado, para descubrir los niveles de seguridad que esta red ofrece y a la vez se puede determinar el porcentaje y tipo de ataques, que se pueden presentar, durante el desarrollo de las respectivas pruebas, los cuales permitirán la aplicación de varias técnicas de defensa en este tipo de red, según sea el tipo de ataques

que se presenten; además del diseño de varias recomendaciones, alusivas para los usuarios de la red WIFI "**IDEA internet en el parque**", de la Plaza Rafael Uribe Uribe del municipio de Urrao; las cuales deben ser tenidas en cuenta, antes de acceder a esta red.

Se debe tener en cuenta, que las redes inalámbricas presentan muchas ventajas para la productividad y la accesibilidad a los recursos de la información y las comunicaciones; pero la tecnología inalámbrica también crea nuevas amenazas y altera el perfil de riesgo seguridad de la información existente; donde los objetivos generales de seguridad de la información, deben preservar la confidencialidad, asegurando la integridad y el mantenimiento la disponibilidad de los sistemas de información y de la comunicación, además de ofrecerle una ayuda para los administradores de la red, en la toma de decisiones, proporcionándoles una comprensión básica de la naturaleza de las diversas amenazas asociadas con las redes inalámbricas y los controles de defensa que se deben implementar.

3.5 Área de conocimiento General y Específica

- **Área del Conocimiento:** Seguridad en Redes
- **Área Específica***:* Pentesting en redes LAN y WLAN

3.6 Investigadores y/o colaboradores

GEOVANNY ALONSO RAMÍREZ HERRERA

3.7 Productos a entregar

El proyecto de grados denominado: "**DETERMINAR LOS PRINCIPALES ATAQUES A LOS QUE SE EXPONEN LOS USUARIOS QUE UTILIZAN LA RED WIFI "IDEA INTERNET EN EL PARQUE" DEL MUNICIPIO DE URRAO**"

4. RESULTADOS

4.1 ATAQUES A LOS QUE ESTÁN EXPUESTAS LAS REDES WIFI.

Se realizó la investigación, consultando diferentes fuentes bibliográficas, en la cual se concluye que los ataques más comunes en las redes wifi son los siguientes:

4.1.1 Ataques pasivos

Estos ataques no son perjudiciales para las redes que se llevan a cabo para la recopilación de información. Un usuario malintencionado sólo escucha el tráfico entrante y saliente de una red inalámbrica. El tráfico contiene los paquetes y cada paquete contiene información jugosa como números de paquetes de secuencias, dirección MAC, y mucho más. La naturaleza de estos ataques es silenciosa, es por eso que son difíciles de detectar. Un atacante malicioso puede realizar un ataque activo a la red inalámbrica, cuyo propósito es únicamente para obtener información sobre el objetivo y no hay datos se cambia en el objetivo. Los ataques pasivos incluyen: El reconocimiento activo y reconocimiento pasivo.

Fases de los ataques pasivos

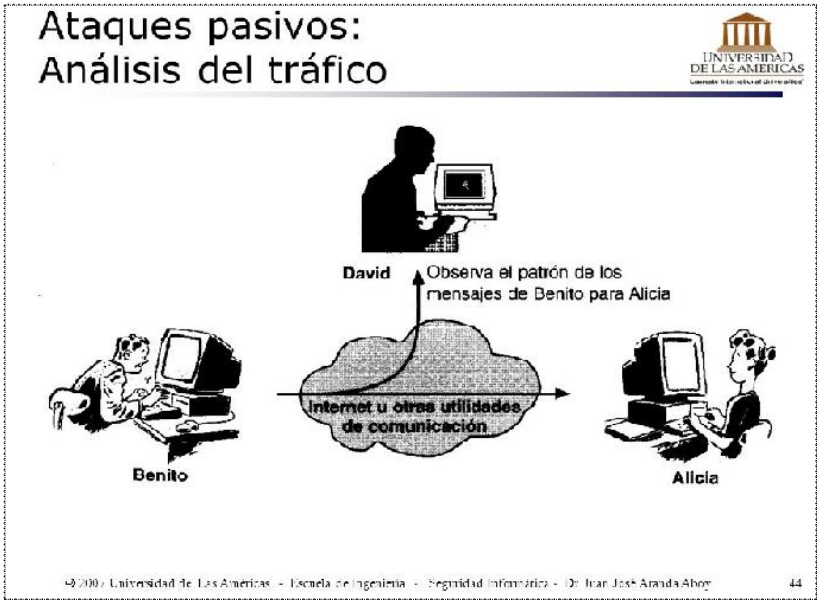
a) **Fase de reconocimiento**

Durante la fase de reconocimiento, el objetivo de un atacante, es descubrir una red de destino, y luego reunir información acerca de la red; donde el atacante realiza el reconocimiento de una manera que es imperceptible, sin embargo, algunos de los medios de reconocimiento pueden ser detectados por un sistema de detección de intrusos. Hay dos métodos utilizados en la ejecución de los ataques pasivos indetectable: espionaje, y análisis de tráfico.

- ✓ **Espionaje**: Es la capacidad de supervisar las transmisiones de contenido del mensaje, donde el atacante intercepta y escucha las señales inalámbricas entre el punto de acceso inalámbrico y cliente.

- ✓ **Análisis de tráfico**: Es la capacidad de obtener inteligencia mediante el control de la transmisión de los patrones de comunicación, o llevar a cabo el análisis de paquetes. Esto se puede llevar incluso cuando los mensajes se cifran y no se puede descifrar.

Figura 2. Ataques pasivos

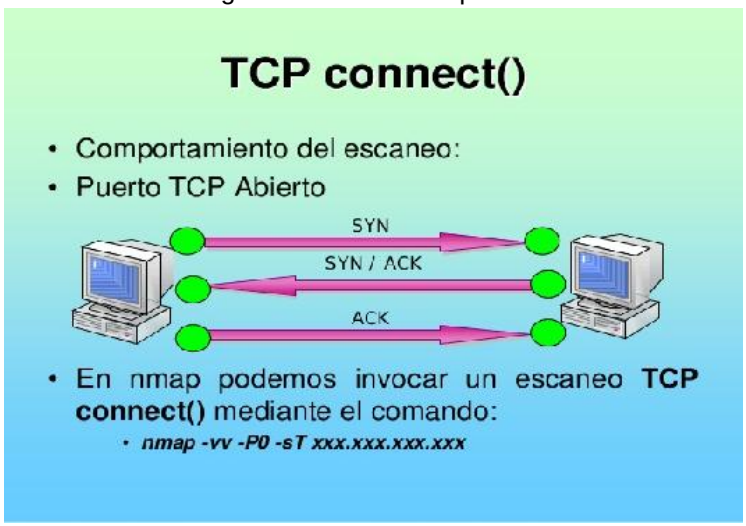


Fuente (Aranda, Dr.Juan José, 2007)

b) Fase de escaneo de puertos

Escanear puertos en las redes de datos, se implementa para identificar qué puertos TCP y UDP están abiertos y escuchar, lo que indica todos los servicios que este sistema está compartiendo con otros hosts TCP / IP. Esto es a menudo utilizado por los administradores para comprobar la seguridad de las redes y para identificar los servicios que se ejecutan en un host y explotar vulnerabilidades. Un escaneo de puertos o escaneo, es un proceso que envía las solicitudes de cliente a un rango de direcciones de puerto del servidor en un host, con el objetivo de encontrar un puerto activo; esto no es un proceso nefasto en sí mismo. La mayoría de los usos de un escaneo de puertos no son ataques, pero en ocasiones se emplean sondas simples para determinar los servicios disponibles en una máquina remota.

Figura 3. Escaneo de puertos



Fuente (Gutierrez, Robert Puican, 2013)

La fase de escaneo de puertos se realizará con la herramienta *Nmap*, la cual permite descubrir qué puertos TCP abiertos en su host de destino. Los puertos de red son los puntos de entrada a una máquina que está conectado a Internet. Un servicio que escucha en un puerto es capaz de recibir datos desde una aplicación cliente, procesarlo y enviar una respuesta de vuelta. Clientes malintencionados pueden explotar varias vulnerabilidades en el código del servidor para que tengan acceso a datos sensibles o ejecutar código malicioso en la máquina remota. Es por ello que es necesario someter a prueba todos los puertos con el fin de lograr una verificación de seguridad a fondo. La exploración de puertos se hace generalmente en la fase inicial de una prueba de penetración con el fin de descubrir todos los puntos de entrada de red en el sistema de destino. La exploración de puertos se realiza de forma diferente para los puertos TCP y UDP, por ello, se dispone de diferentes herramientas.

Parámetros

- ✓ **Objetivo:** Este es el nombre de host de la dirección IP (es) para escanear
- ✓ **Puertos para escanear - Comunes**: Esta opción le indica a Nmap para analizar sólo los mejores puertos TCP 100 más comunes (Nmap -F).
- ✓ **Puertos para escanear - Rango**: Se puede especificar un rango de puertos que deben analizarse. Los puertos válidos están entre 1 y 65535.

- ✓ **Puertos para escanear - Lista**: Puede especificar una lista separada por comas de los puertos que va a escanear.
- ✓ **Detectar versión de servicio**: En este caso Nmap intentará detectar la versión del servicio que se ejecuta en cada puerto abierto. Esto se realiza utilizando múltiples técnicas como agarrar la bandera, la lectura de las cabeceras del servidor y el envío de solicitudes específicas.
- ✓ **Detectar sistema operativo**: Si está habilitada, Nmap tratará de determinar el tipo y la versión del sistema operativo que se ejecuta en el host de destino. El resultado no es siempre 100% exacto, dependiendo de la forma en que el objetivo responde a peticiones de sondeo.
- ✓ **Hacer traceroute**: Si está habilitada, Nmap también hará un traceroute para determinar los paquetes que llevan una ruta, desde un servidor de origen y para un servidor de destino, incluyendo las direcciones IP de todos los nodos de la red (routers).
- ✓ **No anfitrión de ping**: Si está habilitada, Nmap no va a tratar de ver si el anfitrión es antes de escanearlo (que es el comportamiento por defecto). Esta opción es útil cuando el host de destino no responder a las peticiones ICMP, pero es realmente para arriba y tiene puertos abiertos.

Funcionamiento

La herramienta Nmap, se ejecuta con los parámetros adecuados a fin de proporcionar la velocidad y precisión. La exploración se realiza mediante el envío de paquetes a cada puerto y la escucha para las respuestas. La técnica de exploración se llama 'SYN', que envía paquetes TCP SYN a cada puerto. Si un puerto responde con SYN-ACK, que se encuentra en posición abierta y un RST es enviado de vuelta por nuestra herramienta. De esta manera no hay una conexión TCP completa establecida con el host de destino.

Efectos de los ataques pasivos

La finalidad de los ataques pasivos, se caracteriza por el análisis y la búsqueda de vulnerabilidades para abrir puertos o aprovechar los que estén abiertos, cuyo propósito es únicamente para obtener información sobre el objetivo y no hay datos que se cambien en el momento. Por lo tanto, la red Wifi "**IDEA internet en el parque**", está expuesta a los ataques pasivos, debido a que, por lo general, en

casi todos los tipos de ataques cibernéticos, se emplea la búsqueda de vulnerabilidades exponenciales.

4.1.2 Ataques activos

Un ataque activo es aquel mediante el cual se intenta realizar un cambio no autorizado del sistema, lo que podría incluir la modificación de los datos transmitidos o almacenados, la creación de nuevos flujos de datos o limitar la disponibilidad de la red Wifi. Los ataques activos pueden adoptar la forma de uno de los cuatro tipos o combinaciones:

Efectos de los ataques activos

La finalidad de los ataques activos y de reconocimiento, están predestinados para determinar las vulnerabilidades del sistema y la recolección de información en lugar de explotar activamente los dispositivos que sean vulnerables dentro del radio de la red, para después proceder con ataques más contundentes; por lo tanto, la red Wifi "**IDEA internet en el parque**", de la plaza Rafael Uribe Uribe, es vulnerable a estos tipos de ataques.

4.1.3 Ataque de enmascaramiento

Es un ataque activo en el que el atacante se hace pasar por un usuario autorizado y por lo tanto obtiene ciertos privilegios no autorizados. Podría intentarse a través del uso de las identificaciones y contraseñas de inicio de sesión robada, a través de la búsqueda de agujeros de seguridad en los programas, para pasar el mecanismo de autenticación del usuario. Una vez que la entrada se hace y el derecho de acceso a los datos críticos de la organización es permitido, el atacante puede ser capaz de modificar y eliminar software y datos, y hacer cambios en la configuración de la red y la información de enrutamiento.

Efectos de los ataques de enmascaramiento

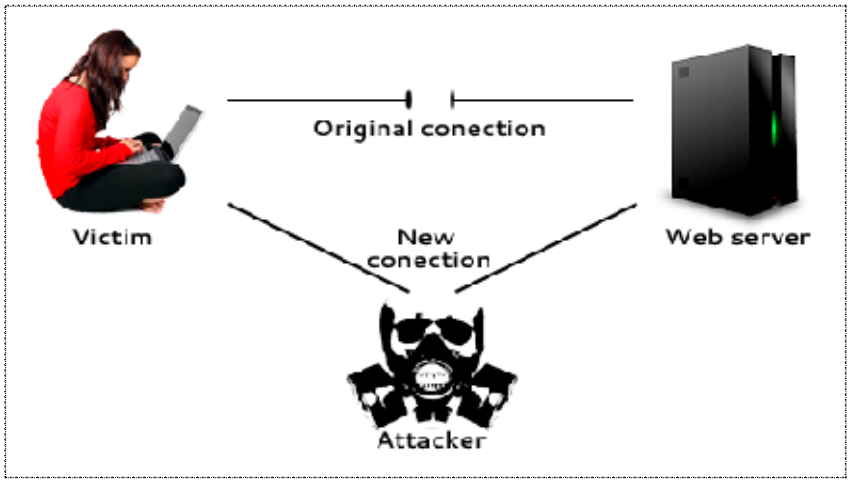
Los usuarios de la red Wifi "IDEA internet en el parque", de la plaza Rafael Uribe Uribe, se verían afectados por este tipo de ataque, debido a que, en la mayoría de los ataques, los Hackers buscan la manera de escalar privilegios, además de robar contraseñas de usuarios para hacerse pasar por un usuario legitimo a la

hora de realizar un inicio de sesión robada, por lo tanto, pueden ingresar y realizar actividades fraudulentas.

4.1.4 Ataque de reproducción

También conocido como "***Man-in-the-middle***" es un ataque de repetición, donde el hacker supervisa las transmisiones de la red objetivo y para luego ser retransmitidas de una manera fraudulenta, para engañar al usuario en operaciones no autorizadas tales como la falsificación de identificación o autenticación o una transacción duplicada. Supongamos que un cliente tiene una conexión TCP con cualquier servidor, entonces el delincuente será el hombre en el medio, el cual divide la conexión TCP en dos conexiones separadas. Así que la primera conexión es de cliente a un atacante, y la segunda conexión será desde el suplantador al servidor. Así que cada uno y cada petición y la respuesta se llevarán a cabo entre el cliente y el servidor a través de un atacante. Por lo que un atacante puede robar la información que pasa en el aire entre ellos.

Figura 4. Ataque Man-in-the-middle



Fuente (Bitendian, 2016)

Efectos del ataque de reproducción

En el momento que el atacante, escucha las transmisiones e intercepción de los datos, este procede con la captura de los datos, donde a veces, estos datos pueden ser modificados en el proceso de transmisión para tratar de engañar al usuario final para divulgar información sensible, tales como registro de credenciales o datos vitales, por lo tanto, la información que sea capturada dentro

del radio de la red WiFi, pondrá en riesgo la información de los usuarios implicados.

Funcionamiento

El hombre en medio del ataque intercepta una comunicación entre dos sistemas. Por ejemplo, en una transacción http el objetivo es la conexión TCP entre el cliente y el servidor. El uso de diferentes técnicas, el atacante divide la conexión TCP original en dos nuevas conexiones, una entre el cliente y el atacante y el otro entre el atacante y el servidor, como se muestra en la figura cinco.

Una vez que se intercepta la conexión TCP, el atacante actúa como un proxy, la capacidad de leer, insertar y modificar los datos en la comunicación interceptada.

El ataque "***Man-in-the-middle***", es muy eficaz debido a la naturaleza del protocolo http y transferencia de datos que están todos en base ASCII. De esta manera, es posible ver dentro del protocolo http y también en los datos transferidos. Así, por ejemplo, es posible capturar una cookie de inicio de sesión al leer la cabecera HTTP, pero también es posible cambiar una cantidad de transacción de dinero dentro del contexto de aplicación.

El ataque "***Man-in-the-middle***", también podría hacerse a través de una conexión HTTPS mediante el uso de la misma técnica; la única diferencia consiste en el establecimiento de dos sesiones SSL independientes, uno sobre cada conexión TCP, donde el navegador instaura una conexión SSL con el atacante, y el atacante establece otra conexión SSL con el servidor web. En general, el navegador avisa al usuario de que el certificado digital que se utiliza no es válido, pero el usuario puede ignorar la advertencia, ya que no entiende la amenaza. En algunos contextos específicos es posible que la advertencia no aparezca.

El ataque "***Man-in-the-middle***", no es sólo una técnica de ataque, sino que también se utiliza generalmente durante la etapa de desarrollo de una aplicación web o todavía se utiliza para estudios de vulnerabilidad Web.

Herramientas de ataque MITM

Las herramientas que hay disponibles para realizar un ataque "***Man-in-the-middle***", son particularmente eficientes en entornos de red LAN, porque implementan funcionalidades adicionales, como la capacidad de ARP falsos que

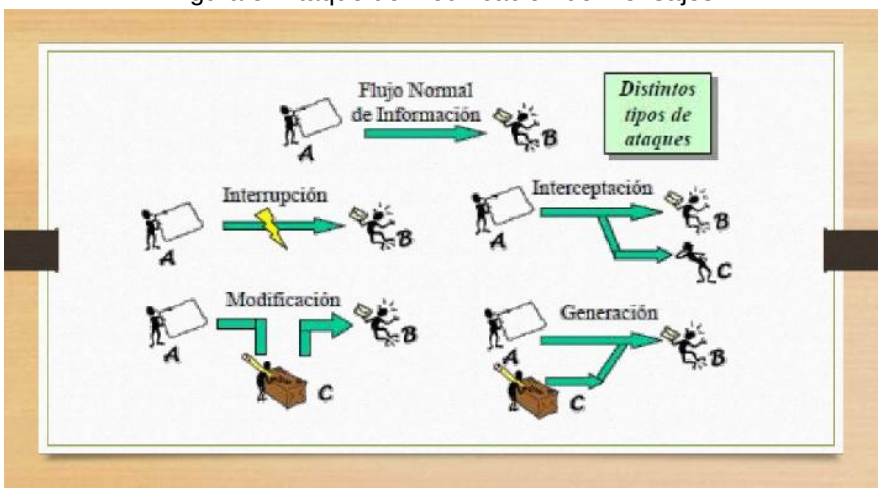
permiten la interceptación de la comunicación entre los hosts, se puede encontrar en la actualidad los siguientes:

- ✓ *PacketCreator*
- ✓ *Ettercap*
- ✓ *Dsniff*
- ✓ *Caín Abel*

4.1.5 Ataque de modificación de mensajes

El atacante altera un mensaje legítimo mediante la supresión, lo que implica la eliminación, inserción o alteración de la información de forma no autorizada que está destinado a aparecer genuina para el usuario. Estos ataques pueden ser muy difíciles de detectar. La motivación de este tipo de ataque puede ser plantar información, cambiar los grados en una clase, alterar los registros de tarjetas de crédito, o algo similar; además de modificaciones de sitios web.

Figura 5. Ataque de modificación de mensajes



Fuente (Moran, Ana Karen Cordova, 2013)

Funcionamiento

El atacante corta una o más secciones de texto cifrado y vuelve a ensamblar estas secciones de manera que los datos descifrados se traducirán en información coherente pero no válido. La modificación de mensajes, es un tipo de misión de modificación de ataque; donde el atacante elimina un mensaje del tráfico de la red, la altera, y vuelve a insertar. Esto se conoce como un ataque activo, porque se trata de un intento de cambiar la información; En comparación, un ataque pasivo, tales como la inhalación de contraseña, busca la información, pero no en sí modificar la información válida, aunque puede ser usado en conjunción con una forma activa de ataque para diversos fines.

Cuando el dato modificado en el ataque implica empresa crítica o información personal, el ataque de cortar y pegar puede suponer una grave amenaza para la seguridad. Un uso típico de un ataque de cortar y pegar es la modificación de la información en un formulario de pedido del cliente para la compra de bienes o servicios a través de Internet.

Efectos de los ataques de modificación de mensajes

En muchas ocasiones, los usuarios envían datos importantes por medio de las redes Wifi públicas, sin saber que en ese instante se está realizando un ataque de modificación de mensajes y su paquete cae dentro de los capturados, cuando este llega al destinatario final, la información contenida ya no es la misma, de tal modo que dependiendo la importancia de los datos enviados, el usuario pone en riesgo su integridad ante la entidad receptora y más que todo cuando se trata de datos financieros o empresariales.

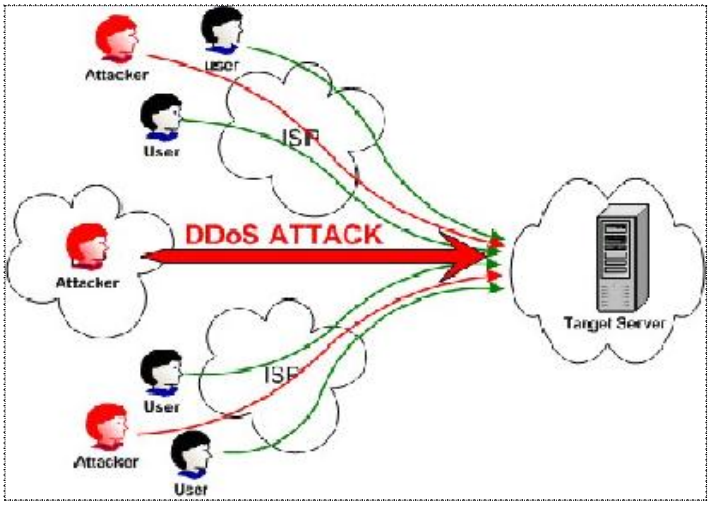
4.1.6 Ataque de denegación de servicio (*DoS*)

El atacante impide o prohíbe el uso normal o la gestión de instalaciones de comunicaciones, las cuales pueden variar desde la destrucción física de los equipos, la interrupción de ciertos servicios de red a una persona o sistema específico, la prevención de un individuo en particular el acceso a un servicio a la inundación de una red, evitando de este modo el tráfico de red legítimo. A veces las redes inalámbricas no utilizan la transmisión de radio.

Con el fin de reducir el consumo, que requiere la comunicación de ese nodo en particular, un usuario malintencionado puede tomar ventaja de este mecanismo,

agotando la fuente de alimentación del dispositivo, con el fin de hacer que la vida del nodo sea más corta, o atacar a la capa MAC para reducir el período de funcionamiento. Si un número de nodos drenados pasa a alta, toda la red puede ser interrumpida. Sólo el protocolo MAC tiene una capacidad de crear una duración del funcionamiento más largo. Sin eso, no se puede extender la vida útil de la red inalámbrica.

Figura 6. Ataque DDoS



Fuente (Zerial, 2009)

Funcionamiento

El tipo más común de ataque DoS es simplemente enviar más tráfico a una dirección de red que los programadores que planearon sus datos de búfer anticipadamente. El hacker puede ser consciente de que el sistema de destino tiene una debilidad que puede ser explotado o simplemente se puede generar un ataque en caso de que podría funcionar. El atacante construye una red de sistemas infectados, inmediatamente comienza con la difusión de correos electrónicos maliciosos y software. Después de ser infectado, estos sistemas pueden ser controlados de forma remota y por lo tanto utilizan para desplegar un ataque DDoS.

Cuando se inicia una sesión entre el programa de control de transporte y el servidor en una red, un espacio muy pequeño tampón existe para manejar el intercambio rápido de datos o mensajes que por lo general establece o se requieren en los inicios de sesión. El de establecimiento de sesiones de paquetes, incluyen campos que identifica la secuencia en el intercambio de mensajes. Un atacante puede enviar un número de peticiones de conexión muy rápidamente y

luego dejar de responder a la respuesta. Por consecuencia, el aumento inesperado de tráfico puede hacer que el sitio cargue muy lentamente a los usuarios legítimos. A veces, el tráfico es suficiente para cerrar el sitio por completo.

Este tipo de ataque de denegación de servicio explota la forma en que el Protocolo de Internet (IP) requiere un paquete que es demasiado grande para el siguiente enrutador, lo que requiere que este se divida en fragmentos. El paquete fragmento identifica un desplazamiento al comienzo de la primera carga de paquetes, para ser vuelto a montar por el sistema de recepción. En el ataque de partícula, IP del atacante pone un valor de desplazamiento confuso en el segundo o posterior fragmento. Si el sistema operativo de recepción no tiene un plan para esta situación, puede provocar que el sistema se bloquee.

Efectos del ataque de denegación del servicio DoS

Los ataques de denegación de servicio, se realizan con una variedad de razones, y se dirigen a una amplia gama de recursos importantes, de los bancos o entidades que manejan grandes cantidades dinero, por lo que los usuarios que realicen consultas o transferencias, pueden poner en riesgo su cuenta, debido a que algunos hackers lo hacen simplemente por el derecho a presumir, mientras que los delincuentes cibernéticos a menudo lo hacen adquirir dinero.

4.1.7 Ataque de interferencia de radio

En este escenario de ataque, se utilizan señales de radio inalámbricas. Un atacante puede tener una antena más fuerte para un generador de señales. En primer lugar, el atacante identifica los patrones de señales a su alrededor o el punto de acceso de destino. A continuación, él o ella crean las mismas señales de radio del patrón de frecuencia y comienza a transmitir en el aire con el fin de crear un tornado de señal de una red inalámbrica. Además de lo anterior, el nodo de usuario legítimo también se atasca por las señales que se están produciendo; por consiguientes la conexión AP se desactiva entre un usuario legítimo de la red inalámbrica, la cual es la red legitima. Existen principalmente tres razones para la interferencia de radio en la red inalámbrica:

- ✓ **Diversión**: Evita que el usuario legítimo deje de recibir cualquier tipo de datos de Internet.

- ✓ ***Spy***: El retraso en el despliegue de paquetes para el usuario legítimo puede dar más tiempo a un atacante para descifrar el paquete con el fin de robar la información.
- ✓ **Ataque**: El atacante puede inundar de paquetes y enviarlo a la víctima con el fin de tomar el control de la máquina del usuario o de la red.

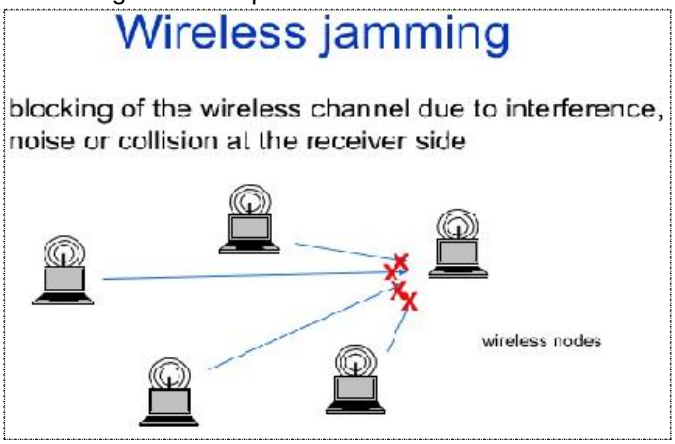
Funcionamiento

Este es un tipo de ataque DOS en las redes inalámbricas. Este ataque tiene lugar cuando las frecuencias de RF falsos o muy gruesos están haciendo problemas con el funcionamiento de la red inalámbrica legítima. En algunos casos, son falsos positivos, tales como un teléfono inalámbrico que utiliza la frecuencia idéntica a la red inalámbrica. Así que, en ese caso, es posible ver algunos resultados en el software de monitorización inalámbrica o mecanismo, pero en realidad no es una interferencia de la señal. No es un ataque muy común, ya que requiere una gran cantidad de hardware para poder realizarlo.

Por lo tanto, ataques de denegación de servicio en la capa física podría ser involuntaria, como la interferencia de otras señales dentro del rango de espectro o interferencia intencional como interferencia por los nodos maliciosos. La interferencia es una de las principales razones para la lentitud y la inestabilidad en las redes de datos inalámbricas. Dado que la transmisión de radio para comunicaciones de datos en redes inalámbricas se transmiten tipo, cualquier receptor dentro del alcance de un transmisor puede escuchar las transmisiones. También operan varios puntos de acceso (AP) estrechamente dentro de una sola Wifi da lugar a la interferencia debida a la colisión de señales. Del mismo modo, cuando varios de los clientes conectados a un solo AP están en estrecha proximidad, la interferencia se produce, cuando la señal surge de las Wifi vecinas.

Hay algunos otros ataques también que son posibles amenazas a las redes inalámbricas. Esos ataques se mencionan y describen a continuación. Antes de entender los diferentes ataques de red inalámbrica, lo que necesitamos saber dónde un ataque inalámbrico puede ser realizado por un atacante.

Figura 7. Ataque de interferencia de señal



Fuente (J., 2012)

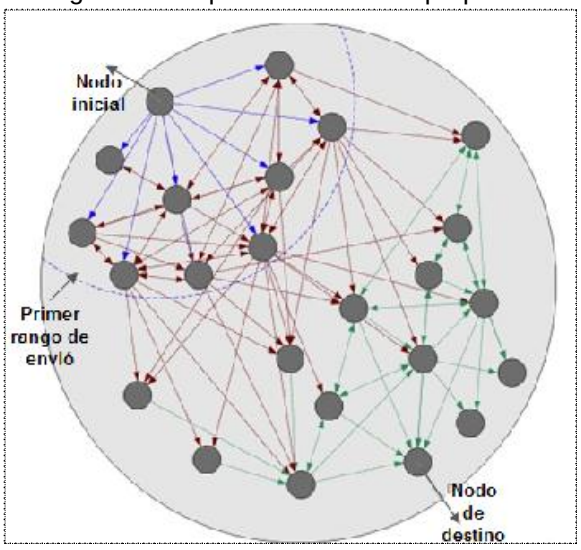
Efectos del ataque de interferencia de radio

Los usuarios de la red Wifi “IDEA internet en el parque”, estarían afectados por este tipo de ataque, debido a que la señal de radio de la antena se muestra y cuando se conectan al servicio resultan conectados a la señal del atacante; además de lo anterior si el atacante no cumple su objetivo en primera instancia, el servicio Wifi se atasca, evitando la conexión hacia la internet y si este es requerido con urgencia, por los usuarios, estarían sin opción de acceder a la red.

4.1.8 Ataque inundaciones de paquetes

Hay un montón de ataques de denegación de servicio que reducen la vida de la red de diferentes maneras. Uno de los métodos más comunes es ataque de denegación de servicio. Un atacante envía una gran cantidad de paquetes a fin de detener la red de comunicación con diferentes nodos. El objetivo principal de este ataque es de agotamiento de los recursos en la máquina de la víctima.

Figura 8. Ataque inundación de paquetes



Fuente: El autor

Funcionamiento

Este tipo de ataque puede forzar un equipo de diferentes maneras. Una de ellas, es causar un DoS mediante la búsqueda y explotación de un servicio que se ejecuta en un host remoto. Se puede hacer que el programa de bucle o

haga reaccionar de una manera que no se pretende, haciendo que el host remoto utilice todos sus recursos, poniéndolo efectivamente fuera de línea. También podríamos desencadenar lo que se llama una inundación UDP.

Un ataque de inundación UDP puede iniciarse mediante el envío de un gran número de paquetes UDP al azar. Como resultado, el anfitrión distante hará lo siguiente:

- ✓ Compruebe si la aplicación está escuchando en ese puerto.
- ✓ Ver que ninguna aplicación escucha en ese puerto.
- ✓ Responder con un ICMP de destino de paquete inaccesible.

Por lo tanto, para un gran número de paquetes UDP, el sistema víctima se vio obligado a enviar muchos paquetes ICMP, causando que sean eventualmente inalcanzables por otros clientes. El atacante también puede suplantar la dirección IP de los paquetes UDP, lo que garantiza que los paquetes ICMP sean excesivos

en su retorno, disociando de manera efectiva la ubicación del atacante en la red, de tal modo que la red Wifi, quedara bloqueada.

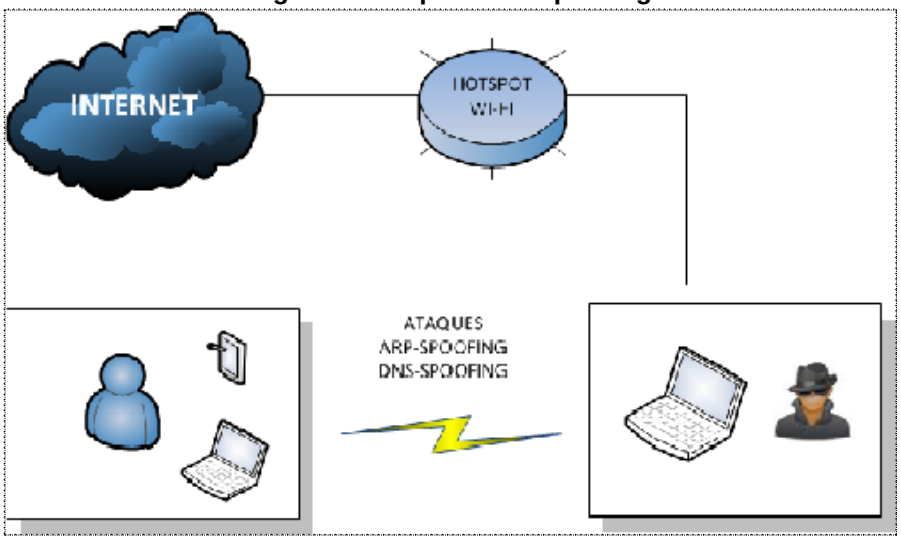
Efectos del ataque de inundación de paquetes

Las consecuencias que generaría este tipo de ataque en la red Wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, evitaría que los usuarios se conecten a la red, debido a que, por medio de la inundación de paquetes, los atacantes pueden bloquear los equipos que brindan la señal de la antena, por consiguiente, los usuarios quedarían sin el servicio de internet libre en parque, hasta que se termine el ataque o los administradores lo mitiguen.

4.1.9 Ataque de IP Spoofing

Suplantación en DNS, donde también es conocido como el envenenamiento de caché DNS. Es un ataque por el que un host con ninguna autoridad es la dirección de un servidor de nombres de dominio (DNS) y todas sus peticiones. Esto significa básicamente que un atacante podría redirigir todas las peticiones DNS, y por lo tanto todo el tráfico, a su máquina, la manipulación de un modo malicioso y posiblemente robar datos que pasan a través. Este es uno de los ataques más peligrosos ya que es muy difícil de detectar.

Figura 9. Ataque de IP Spoofing



Fuente (Ariza, Diego, 2012)

Si un usuario interactúa con el contenido dinámico en una página falsificada, el secuestrador puede tener acceso a información sensible o equipos o recursos de red; de tal modo que podía robar o alterar datos sensibles, tales como un número de tarjeta de crédito o contraseña, o instalar software malicioso. El secuestrador también sería capaz de tomar el control de un equipo comprometido para utilizarlo como parte de un ejército de *zombis* con el fin de enviar *spam*.

Funcionamiento

Los ataques de suplantación de IP, tiene su funcionamiento cuando hay una sobrecarga de los objetivos con el tráfico, lo que consiste en simplemente inundar un destino seleccionado con los paquetes de múltiples direcciones. Este método funciona enviando directamente una víctima más datos de los que puede manejar.

Otro método consiste en que simule la dirección IP del destino y enviar paquetes desde esa dirección a varios destinatarios de la red, de tal modo que la otra máquina recibe un paquete, se transmitirá automáticamente un paquete al remitente en respuesta. Puesto que los paquetes falsificados parecen ser enviado desde la dirección IP del destino, todas las respuestas a los paquetes falsificados serán enviadas a (e inundaciones) la dirección IP del destino.

Estas dos formas de funcionamiento de los ataques de *IP Spoofing* permite que las partes maliciosas, generen la suplantación de identidad para hacerse pasar por máquinas con permisos de acceso a la red y medidas de seguridad basadas en la confianza de derivación e inmediatamente pueden lograr sus objetivos de robo de información sensible.

Efectos del ataque IP Spoofing

Los usuarios de la red Wifi "**IDEA internet en el parque"** de la plaza Rafael Uribe Uribe, estarían afectados por este tipo de ataque, donde la simulación de direcciones IP, generara una sobrecarga entre la red, los dispositivos y los paquetes que parecen provenir de direcciones IP de origen legítimo, pero estos, tendrían su origen de una dirección de origen falsa, con el fin de disfrazarse y obtener información de sus víctimas, de tal modo que los atacantes pueden obtener las credenciales de los usuarios fácilmente.

4.1.10 Ataque de sincronización

En este ataque, el atacante intenta modificar los indicadores de control y, a veces los números de secuencia con el fin de forjar los paquetes o mensajes. Como resultado, el atacante limita el usuario legítimo de intercambio de los mensajes entre el servidor y el cliente. Se solicitará de forma continua la retransmisión de los mensajes. Este ataque provoca un ciclo infinito de retransmisión. Adquiere una gran cantidad de energía. También podemos decir que el atacante perturba la conexión que se establece entre dos puntos finales. Los ataques de sincronización se presentan bajo tres protocolos:

Protocolos RBS, TPSN y FTSP

Para RBS, un ataque a la sincronización que puede ejecutarse fácilmente. RBS funciona de receptor a receptor de sincronización en el que ambos nodos reciben la baliza de referencia y luego calcular su desplazamiento uno con el otro. Un ataque sería tan simple como poner en peligro uno de los nodos con una hora incorrecta. El nodo no comprometido calculará entonces un desplazamiento incorrecto durante el período de intercambio.

a) Protocolo TPSN

PSN es un emisor al receptor de protocolo, basado en árbol con dos fases, la fase de descubrimiento de nivel y la fase de sincronización. Las fases son iniciadas por el nodo raíz. En la fase de sincronización, el número de nivel y el tiempo son enviados tanto a través del árbol. Un ataque sería simplemente para comprometer un nodo no root con el tiempo incorrecto. Esto se propagará a través del árbol, comprometiendo el nodo raíz, ocasionando una sincronización incorrecta.

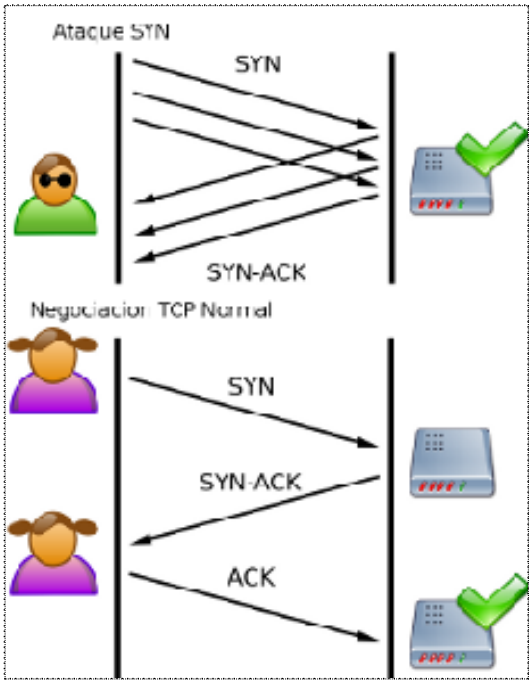
También un nodo podría mentir acerca de su nivel. Eso provocaría otros nodos para solicitar información de sincronización en las que podría dar información inexacta. Ese nodo también podría negarse a participar en la fase de descubrimiento de nivel, lo que podría eliminar a sus hijos desde la red.

b) Protocolo FTSP

El problema fundamental en FTSP, radica en que este permite que el usuario pueda elegir cualquier nodo, a sí mismo la raíz de un período de tiempo. Un nodo corrupto podría reclamar cualquier nodo como la raíz y ahora los otros nodos responderán a su información de temporización en vez de la información correcta desde el nodo raíz real. La voluntad, por supuesto, se propaga a través de la red hasta que todos los nodos han calculado incorrectamente su posición oblicua.

Dado que ninguno de los protocolos fue diseñado pensando en la seguridad. Los ataques a la sincronización se ejecutan fácilmente siguiendo las reglas del protocolo. Un ataque instituirá más daño debido a que se propagará a través de la red.

Figura 10. Ataque de sincronización



Fuente (Dany Martinez, 2010)

Protocolos de sincronización

Hay un problema común entre los tres protocolos presentados. Todos ellos fueron desarrollados para ser eficiente, precisa energía, robusta, y así sucesivamente, pero ninguno de ellos se ha desarrollado pensando en la seguridad. Al igual que

en todos los protocolos de seguridad informática es siempre un problema y los ataques a los protocolos es inevitable.

Efectos causados por los ataques de sincronización

Este tipo de ataque, afectaría a los usuarios de la red Wifi, cuyo el objetivo es convencer de alguna manera a los nodos vecinos que están trabajando en la respectiva capa, pero estos están en un momento diferente a lo que realmente son. Desde el momento que sucede la sincronización global entre los dispositivos y la conexión hacia la red, los protocolos que se basan en los nodos vecinos pasan la información de sincronización, comprometiendo que un nodo pueda interrumpir la sincronización global y por ende la sincronización sería incorrecta y se solicitarían más datos para restablecer la conexión, estas solicitudes se pueden repetir infinitamente, con la finalidad de obtener la mayor cantidad de información de la víctima.

4.1.11 Ataque *Forwarding* o reenvió selectivo

También se puede referir como " **ataque agujero gris'**. En esta forma de ataque, el atacante puede detener el nodo de pasar a través de paquetes mediante el envío o dejar caer esos mensajes. En una forma de ataque de reenvío selectivo, un nodo rechaza selectivamente los paquetes, dejando caer los que entren en esa red de un nodo individual o un grupo de nodos individuales.

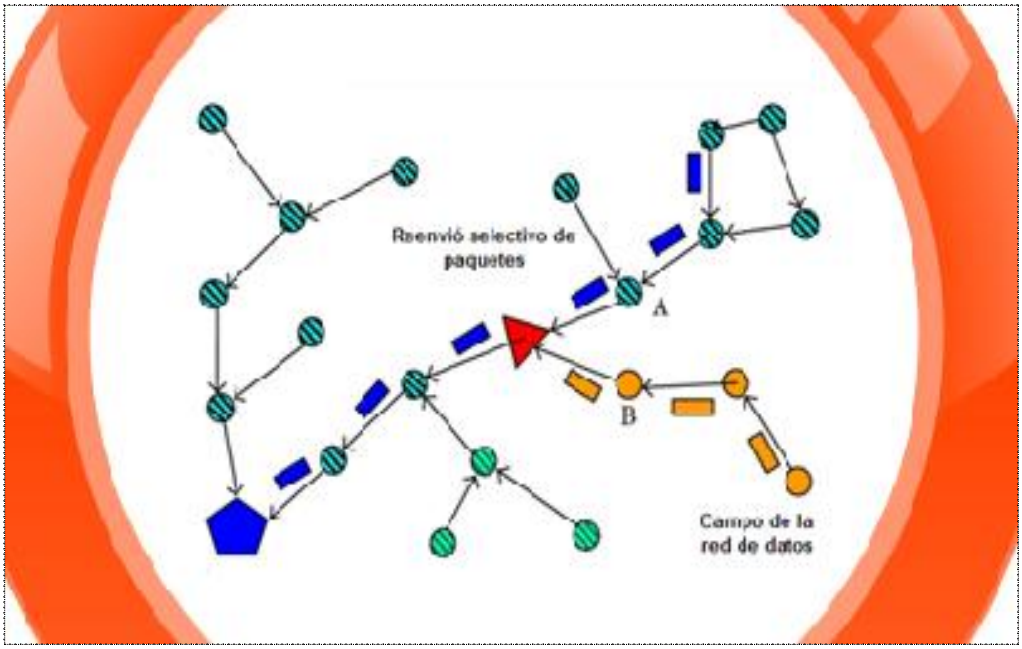
Funcionamiento

Cuando un nodo de punto de control recibe un paquete de evento, se genera un paquete A para el evento de paquetes y luego entregado a los nodos anteriores. El camino seguido por el paquete A, permanece igual al que ha sido enviado con anterioridad. Los paquetes de alerta, se generan en los nodos intermedios cuando los nodos son detectados como sospechosos. Una vez generados, los paquetes de alerta se enviarán al nodo de origen o de la estación base a través de múltiples saltos. La idea básica de este esquema es el siguiente. Los nodos intermedios, que vienen en la ruta de transmisión se seleccionan como punto de control nodo. El camino a continuación, se divide en varios segmentos por estos los nodos de control. Cada vez que un evento especial es detectado por nodo de origen, se genera un paquete de evento.

Efectos causados por el ataque de Forwarding o reenvió selectivo

La red Wifi "**IDEA internet en el parque**", se vería afectada por este tipo de ataque, debido a que, por medio del reenvío selectivo de paquetes, los nodos maliciosos tratan de detener los paquetes que circulan en red, además de negarse a transmitirlos o dejar caer los mensajes que pasan a través de ellos. El nodo malicioso puede reenviar los mensajes al camino equivocado, creando información de enrutamiento infiel en la red. De lo contrario, el nodo implicado puede reenviar el paquete a un nodo malicioso desconocido a través de una ruta de alta calidad para espionaje, por lo que los usuarios serían seriamente afectados.

Figura 11. Ataque de reenvió selectivo de paquetes



Fuente: El autor

4.1.12 Ataque de enrutamiento no autorizado

En el proceso de enrutamiento, muchos componentes están implicados, destacando los anfitriones de la estación base, los puntos de acceso, los nodos, los protocolos de enrutamiento, entre otros. Un usuario malintencionado puede tratar de actualizar toda esta información con el fin de actualizar la tabla de enrutamiento. Puede ser posible que, debido a este ataque, consiga que algunos de los nodos queden aislados de la estación de base. Además, una partición de

red puede ocurrir debido a este ataque. Los paquetes pueden ser retirados después de la TTL expira. Además de lo anterior, estos pueden ser enviados a cualquier usuario no autorizado. Todos estos incidentes son el impacto de este ataque.

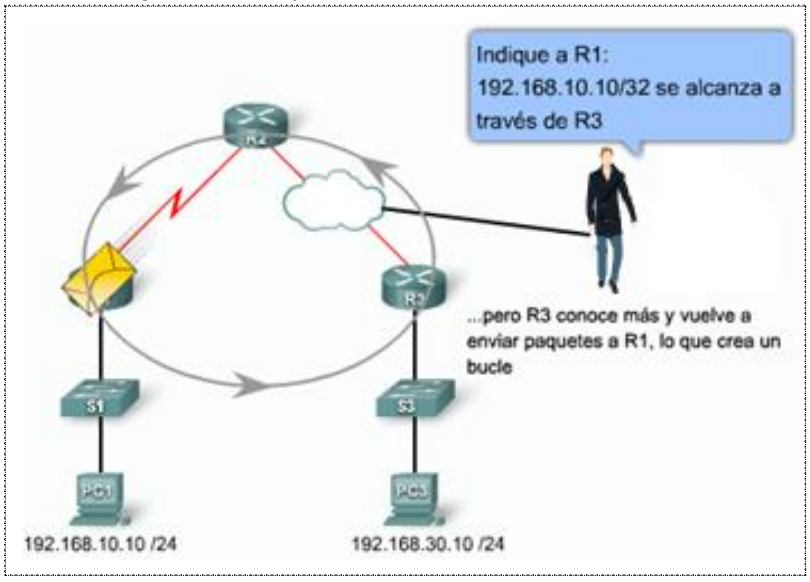
Funcionamiento

El usuario es el suplicante que solicita la autentificación de un servidor de autenticación dentro del radio de la señal Wifi o, en algunos casos, el nodo de acceso en sí, donde el autenticado, normalmente las puertas de acceso AP verifican la información de solicitud del usuario, hasta que se haya autenticado el usuario. La autenticación el intercambio se produce entre el cliente y el servidor de autenticación que utiliza el protocolo EAP, que encapsula el tipo específico de autenticación.

Efectos causados por el ataque de enrutamiento no autorizado

La red Wifi “IDEA internet en el parque”, sería afectada por este tipo de ataque, debido a que la información contenida en cada uno de los paquetes enviados por los usuarios, pueden estar comprometidos con un enrutamiento no autorizado, los cuales pueden ser programados por los atacantes y a la vez puede ocasionar otros tipos de ataques.

Figura 12. Ataque de enrutamiento no autorizado

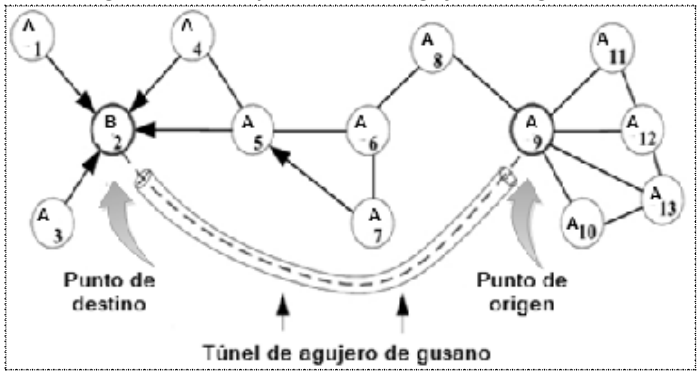


Fuente (Cisco Networking Academy, 2015)

4.1.13 Ataque agujero negro o de gusano

En este tipo de ataque, un atacante copias del conjunto de paquetes o el mensaje por un túnel a otra red del originador. A continuación, el atacante los transmite al nodo de destino. Cuando el atacante transmite los mensajes o paquetes copiados en el nodo de destino, los transmite rápidamente, de tal manera que copian los paquetes que llegan al nodo de destino antes de que los paquetes originales, lleguen a su destinatario. Para hacer eso, el atacante utiliza un túnel de agujero de gusano.

Figura 13. Ataque túnel de agujero de gusano



Fuente: El autor

Funcionamiento

Consiste en registrar el tráfico de una región de la red y reproducirla en una zona diferente. Se lleva a cabo por un nodo intruso X ubicados dentro del alcance de transmisión de los nodos legítimos A y B, donde A y B no están dentro del alcance de transmisión del Intruso “nodo X”. Los túneles de tráfico de control entre A y B (y viceversa), sin la modificación presunta por el protocolo de enrutamiento.

Efectos causados por el ataque agujero negro o de gusano

Los usuarios de la red Wifi “**IDEA internet en el parque**” de la plaza Rafael Uribe Uribe, son perjudicados por este ataque, debido a que los atacantes, lanzarían ataques pasivos para identificar el perfil de la víctima potencial, la recopilación de información sobre los hábitos de Internet, el historial de sitios web visitados, entre otros más. Luego el atacante utiliza ese conocimiento para inspeccionar los sitios web públicos legítimos específicos para localizar las vulnerabilidades. Si alguna de

estas vulnerabilidades las encuentra el atacante, este compromete el sitio web con su propio código malicioso.

4.1.14 Ataque Sybil

Este ataque es muy común y conocido, donde el atacante puede obtener la dirección IP de la persona legítima o la dirección MAC con el fin de robar su identidad, luego el atacante puede atacar a otra víctima y puede hacer un montón de cosas con esa nueva identidad robada del usuario legítimo. Un ataque *Sybil* es una versión avanzada de un ataque de suplantación en el que un usuario malintencionado (atacante) puede robar identidades múltiples. En términos técnicos, un nodo malicioso representa a sí mismo a los demás compañeros de nodos mediante la adquisición de múltiples identidades dentro de sí mismo. Los efectos serán los mismos que en un ataque de suplantación.

Funcionamiento

El atacante genera sus identidades *Sybil,* donde todos los usuarios que participan en la red Wifi a la vez, mientras que una entidad de hardware en particular sólo puede actuar como una sola identidad a la vez, puede desplazarse a través de estas identidades para que parezca que todos están presentes al mismo tiempo; además de ello, alternativamente, el atacante podría presentar un gran número de identidades en un período de tiempo, mientras que sólo en calidad de un menor número de identidades en cualquier momento dado. El atacante puede hacer esto por tener una identidad, salen de la red, y tienen otra identidad para unirse nuevamente como un usuario legítimo.

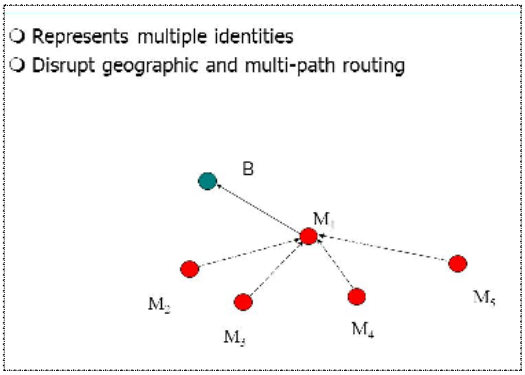
Una identidad que es robada, en particular podría salir y unirse a múltiples veces, o el atacante sólo podría utilizar una vez cada identidad. Otra posibilidad es que el atacante podría tener varios dispositivos físicos en la red, y podría tener estos dispositivos de intercambio identidades. Aunque el número de identidades utiliza el atacante es igual al número de dispositivos físicos, cada dispositivo presenta diferentes identidades en diferentes momentos.

Efectos causados por el ataque *Sybil*

La red Wifi “**IDEA internet en el parque**” de la plaza Rafael Uribe Uribe, está expuesta al ataque Sybil, debido a que un atacante con muchas identidades

puede utilizarlos para actuar maliciosamente, ya sea por el robo de información de comunicación o con la interrupción del servicio.

Figura 14. Ataque Sybil



Fuente (Olea, Izabelle, 2015)

4.1.15 Ataque de Phishing o suplantación de identidad

Un atacante establece un punto de acceso inalámbrico que se hace pasar como una legítima AP (mismo SSID corporativo, tal vez incluso el mismo BSSID). Si el cliente no utiliza la autenticación mutua, es posible que el atacante para atraer a la incauta legítima los usuarios conectarse a su AP. El atacante puede utilizar una variedad de técnicas para extraer información privada (por ejemplo, para olfatear contraseñas). El sistema *DAIR* puede detectar ataques de *Phishing*. Sin embargo, no describimos soluciones a los ataques de *Phishing* en este documento.

Funcionamiento

El ataque *Phishing*, es una estafa que involucra a los ladrones de identidad, cuya función radica en hacerse pasar como una legítima, con la finalidad de pescar información personal y financiera de los usuarios en cuestión. Así es como funciona:

- ✓ Un consumidor recibe un correo electrónico que parece provenir de una institución financiera, agencia gubernamental u otra entidad conocida y de buena procedencia.
- ✓ El mensaje describe una razón urgente debe verificar o volver a presentar, casi diario se relaciona con información personal o confidencial haciendo clic en un enlace incluido en el mensaje.

- ✓ El enlace proporcionado parece ser el sitio web de la institución financiera, agencia gubernamental u otra entidad conocida de buena reputación, pero en las estafas, el sitio web pertenece a los autores del fraude, en otras palabras, al atacante.
- ✓ Una vez dentro del sitio web fraudulento, el consumidor puede pedir que proporcione números de seguridad social, números de cuenta, contraseñas u otra información que se utilizan para identificar el consumidor, tales como el nombre de soltera de la madre del consumidor o lugar de nacimiento del consumidor.
- ✓ Otras estafas de *Phishing* incluyen mensajes de texto llamadas telefónicas o mensajes grabados que solicitan la verificación de su tarjeta de crédito o cuenta bancaria y los correos electrónicos que se encuentran ofertas de trabajo, encuestas, premios y premios, certificados de regalo, patrocinadores u organizaciones benéficas o esquemas de lavado de dinero.

Efectos causados por el ataque de Phishing o suplantación de identidad

La red Wifi, puede ser implicada por un Hacker para obtener información confidencial y conseguir acceso a los archivos personales de los usuarios, donde pueden utilizar diferentes ataques a la vez, para convencer a la víctima, para que lean los enlaces o mensajes publicados en los sitios de redes sociales que atraen al usuario con su contenido y convencerlo de que haga clic en ellos, al instante la información del usuario implicado, caería en manos de un atacante y la integridad de la víctima será afectada.

Figura 15. Ataque de Phishing

Fuente (Diario Libre, 2014)

4.1.16 Ataques de diccionario

Se realizan generalmente por los hackers que ya tienen conocimiento sobre el tráfico en la red Wifi del lugar seleccionado, con el fin de acceder a los dispositivos particulares conectados a la red atacada, el atacante pasa a través de una lista de contraseñas, del modo que puede seleccionar sus candidatos.

Funcionamiento

El objetivo del ataque es recuperar la contraseña, sin la necesidad de capturar las cuatro vías, que requieren el apretón de manos entre un cliente inalámbrico y el punto de acceso legítimo. Nuestro software de forma automática trata de adivinar la contraseña larga mediante la selección de una determinada frase de paso de una lista de palabras del diccionario y la creación de mensajes dos del protocolo de enlace de cuatro vías. Entonces, el programa envía el mensaje dos con la AP y espera una respuesta. Si el punto de acceso responde con el mensaje tres a continuación, se ha adivinado que la frase correcta.

Efectos causados por los ataques de diccionario

Los usuarios de la red Wifi “IDEA internet en el parque” de la plaza Rafael Uribe Uribe, están expuestos, debido a que los *Hackers* por medio de este tipo de ataque, extrae contraseñas, para recopilar información sensible de sus víctimas, para luego ser analizada y utilizada para suplantación de identidad.

Figura 16. Ataque de diccionario

Fuente (Mara, 2013)

4.1.17 Ataque gemelo malvado

El ataque consiste en la creación de un punto de acceso dudoso de Wifi, que parece ser un legítimo dentro del radio que proporciona la antena en su señal Wifi, pero en realidad ha sido creado para espiar las comunicaciones inalámbricas. Un gemelo malvado es la versión inalámbrica de la estafa de *Phishing*. Un atacante engaña a los usuarios inalámbricos en la conexión de un ordenador portátil o teléfono móvil a un punto de acceso contaminada haciéndose pasar por un proveedor legítimo.

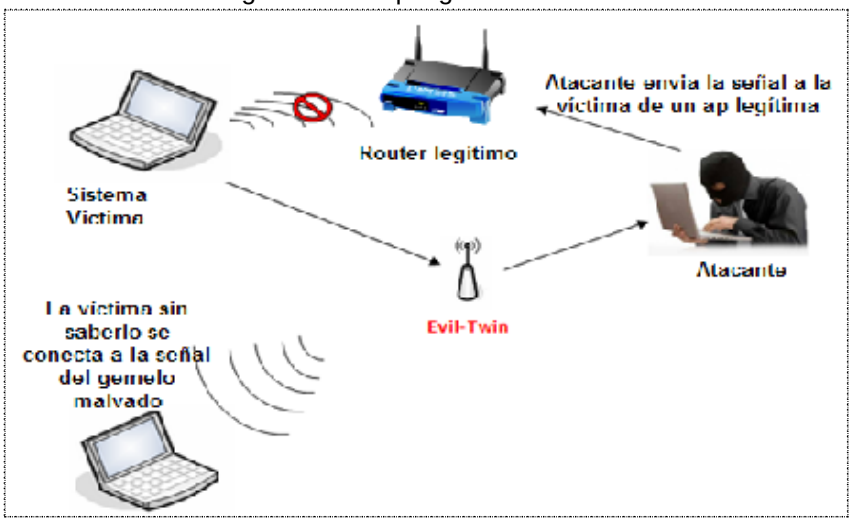
Funcionamiento

El atacante instauró un punto de acceso Wifi falsa, que tienen por objeto proporcionar servicios de Internet inalámbricos y de la escucha el tráfico del usuario, el atacante puede saber todo lo que su está haciendo cada web abierta y acceso por medio de contraseñas que se escriben; si el atacante solo quiero saber las credenciales Wifi, le brindará a sus víctimas una página de acceso falsa pidiendo que el usuario se conecte y se autentifique, además de ello, los datos sensibles estarán disponibles para las manos del atacante, una vez que se conecte a una Wifi falso, el escenario de ataque podrían ser explotados para ejecutar *Man-in-the-middle* o para servir de software malicioso para los equipos de la red de destino.

Efectos causados por el ataque gemelo malvado

La red Wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, pone en riesgo la seguridad de los datos de los usuarios, debido a que este tipo de ataque, representa un peligro claro y presente para los usuarios inalámbricos de redes públicas, donde con sólo colocar un gemelo malvado cerca de los usuarios del radio de la señal de la antena, puede ser suficiente para engañar todos los dispositivos inalámbricos en la relación con un AP falso. Un atacante que se impacienta esperando a los usuarios moverse hacia la señal de un gemelo malvado, puede utilizar una herramienta como Aireplay para anular la que todos están utilizando, obligándolos a realizar una reasociación inmediata, por ende, caerán en sus manos y usar su posición ventajosa para poner en marcha muchos otros ataques.

Figura 17. Ataque gemelo malvado



Fuente: El autor

4.1.18 Ataque de envenenamiento de DNS

La caché DNS puede llegar a ser envenenado si contiene una entrada incorrecta, de tal modo que el atacante obtiene el control de un servidor DNS y cambia algo de la información en él; por ejemplo, no podrían decir que *www.google.com* realidad apunta a una dirección IP que el atacante posee, debido a que ese servidor DNS diría a los usuarios que hacen la petición de buscar para *www.google.com* en la dirección equivocada. La dirección del atacante podría contener algún tipo de sitio web de suplantación de identidad maliciosa. A continuación, se extiende al router de la red Wifi y las memorias caché de DNS en los dispositivos portátiles hasta la entrada DNS, recibiendo así la respuesta incorrecta, donde a la vez lo almacena.

Funcionamiento

El atacante puede encontrar una manera de hacer el informe de resolución de vuelta la dirección IP incorrecta, entonces cualquiera que trate de llegar a una dirección web será enviada a una falsa, sin ninguna forma obvia para que el usuario detecte que algo está mal. Del mismo modo, el correo electrónico podría ser entregado a un destino equivocado, y así sucesivamente. El problema de fondo es uno de configuración del servidor DNS los cuales tienden a ser olvidados, y su configuración por defecto no es necesariamente segura. Posteriormente, el atacante aprovecha esta vulnerabilidad, donde el usuario debe hacer uso del proceso de ingreso de la URL en una dirección IP específica se lleva a cabo por una pequeña colección de sistema de nombres de dominio (DNS). El problema es

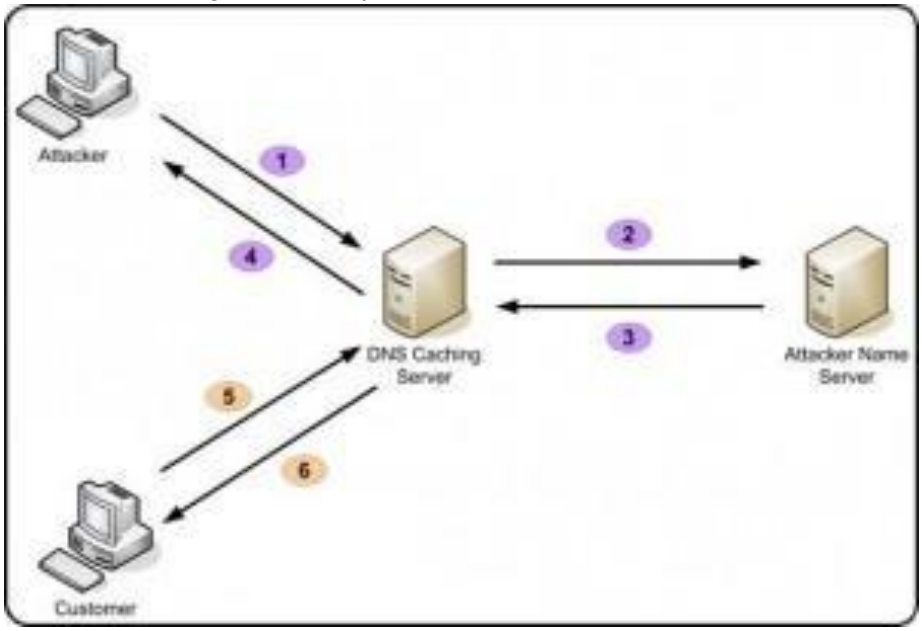
que, si alguien logró alterar el servidor DNS, a continuación, los usuarios podrían no estar seguros de que estaban siendo dirigidos al sitio adecuado.

Efectos causados por el ataque de envenenamiento de DNS

La red Wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, puede verse comprometida con este tipo de ataque, debido a un Hacker puede crear varios problemas. En primer lugar, los usuarios piensan que están en un sitio seguro, pero no lo es así. A diferencia de un ataque de Phishing, donde un usuario de alerta puede detectar una URL sospechosa, en este caso, la URL es genuina; por lo que no hay intervención de ningún tipo por parte de los usuarios y, puesto que nada inusual ha sucedido, no tienen ninguna razón para sospechar.

Otro problema es que cientos o incluso miles de usuarios pueden ser redirigidos si un atacante inserta correctamente una sola entrada falsa en un servidor de almacenamiento en caché. La magnitud del problema se amplifica por el que se solicita la popularidad del dominio. Bajo estas circunstancias, incluso un hacker experimentado moderadamente puede causar un montón de problemas, obtención de contraseñas y otra información valiosa o sensible.

Figura 18. Ataque de envenenamiento de DNS



Fuente (Rodriguez, Juan, 2010)

4.2 REALIZACIÓN DE TRES TIPOS DE ATAQUES CONTROLADOS A LA RED WIFI "IDEA INTERNET EN EL PARQUE" PARA DETERMINAR SI ESTA POSEE VULNERABILIDADES QUE AFECTAN A LA RED Y A SUS USUARIOS.

De acuerdo a la investigación realizada, se concluye que existen tres ataques principales, los cuales en su orden de ejecución son el ataque Spoofing o suplantación de DNS; el cual se caracteriza por la imitación de un usuario, dispositivo o cliente en Internet. A menudo se utiliza durante un ataque cibernético para disfrazar el origen del tráfico de ataque.

Posteriormente, se ejecuta el ataque de denegación de servicio o *DoS*; cuyas características principales son destinadas para atacar múltiples sistemas de la red wifi u ordenadores comprometidos, causando una denegación de servicio a los usuarios del recurso objetivo.

Luego se ejecuta los ataques de *Phishing, Man in the middle y ARP Spoofing*, en un solo ataque. El ataque de *Phishing* se emplea para la creación de una réplica de una página web existente para engañar al usuario a la hora de ingresar datos de carácter personal, luego se procede con el ataque de *Man in the middle* para interceptar o alterar las comunicaciones entre dos partes que normalmente no son conscientes de que el atacante está presente en sus comunicaciones o transacciones. La tarea del ataque de *ARP Spoofing* se utiliza para enviar mensajes falsificados ARP, a través de la red wifi, con la finalidad de lograr una vinculación de la dirección MAC de un atacante con la dirección IP de un equipo legítimo o servidor en la red, la cual será suplantada a la hora de capturar contraseñas de los usuarios que ingresen a *Hotmail*

Estos ataques se caracterizan por vulnerar las redes wifi que están expuestas; además de ser unas pruebas de *hacking* ético controladas, las cuales se han desarrollado, con herramientas que se pueden utilizar para hackear éticamente los sistemas de almacenamiento y descubrir las vulnerabilidades que podrían exponer la red y la información sensible de los usuarios de las localidades que son objetivos atractivos para los atacantes, debido a que no cuentan con las medidas de seguridad necesarias para garantizar que los datos de los usuarios que se conectan diariamente, no están expuestos. En las redes wifi publicas abiertas, se puede demostrar por medio de pruebas técnicas y análisis, que estos ataques son los que se ejecutan con mayor frecuencia en este tipo de redes, los cuales podrían dirigirse a los usuarios que utilizan la conexión Wifi "**IDEA internet en el parque**", de la plaza Rafael Uribe Uribe del municipio de Urrao.

Los tipos de ataques más comunes en redes wifi públicas son:

4.2.1 Ataque Spoofing o suplantación de DNS:

Para proceder a realizar el ataque "***Spoofing* o suplantación de identidad**", se procede con establecer conexión con la red "**IDEA internet en el parque**", tanto en la máquina del atacante "***Kali Linux***" y la máquina victima "***Windows 7***".

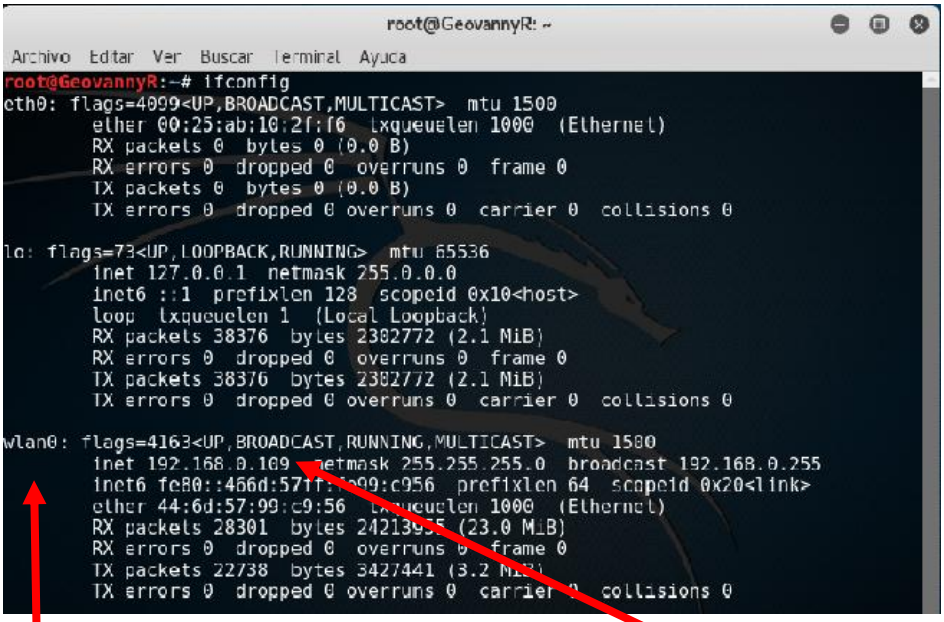
Para la ejecución de este tipo de ataque "***Spoofing* o suplantación de identidad**", se requiere la intervención de tres máquinas:

- ✓ La primera hace referencia a la persona que va a realizar el ataque, la cual está dotada del sistema operativo *Kali Linux 2.0* en una máquina física.
- ✓ La segunda máquina está representada por el usuario que va a solicitar el servicio a "x" página, la cual está dotada del sistema operativo *Windows 7* 64 bits, instalado en una máquina física.
- ✓ La tercera máquina, está representada por el sistema que es suplantado por el atacante.

Para comenzar, se debe ingresar a la terminal de *Kali Linux* en modo súper usuario o root, para proceder con la configuración de la tarjeta de red que se va a utilizar, o verificar si este cumple con los parámetros necesarios para realizar este tipo de ataque.

Se debe ingresar el comando (ifconfig)

Figura 19. Ejecución comando ifconfig



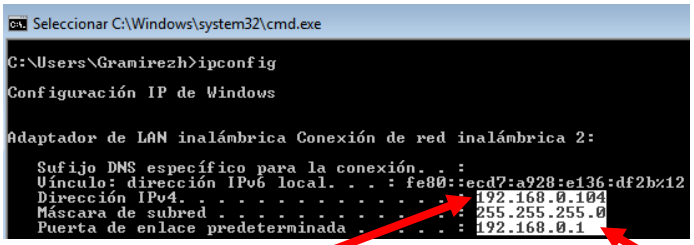
Fuente el autor

Se puede observar que el equipo está conectado a la red IDEA internet en el parque por medio de la wlan0

La dirección IP de la máquina atacante, es la **192.168.0.109**

También procederé a verificar la dirección IP de la segunda máquina, la cual tiene instalado *Windows 7* 64 bits. Para ello, hay que dirigirse a inicio e invocar el "**CMD**", para luego introducir en la consola de CMD el comando "**ipconfig**".

Figura 20. Ejecución consola CMD



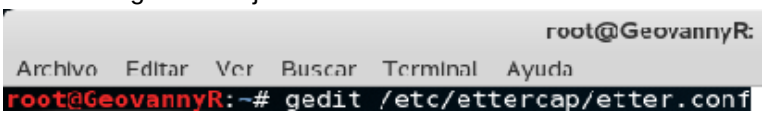
Fuente el autor

Dirección IP: **192-.168.0.104**

Puerta de enlace: **192.168.0.1**

Con estos datos, hay que dirigirse a configurar el "***Ettercap***", ya que es la aplicación de elección para el desarrollo de este trabajo. Se debe ejecutar el comando **gedit /etc/ettercap/etter.conf** y abrir el archivo para editar el archivo.

Figura 21. Ejecución terminal de Kali Linux 2.0



Fuente el autor

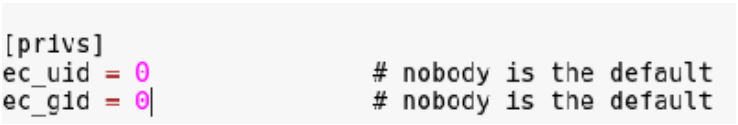
Así que ahora queremos editar los ec_uid y ec_gid valores en la parte superior para hacer que den como resultado "0"

Figura 22. Configuración archivo etter. conf

Fuente el autor

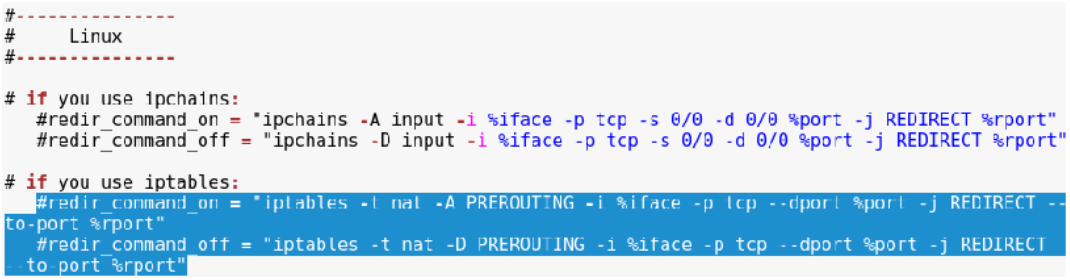
Ahora hay que desplazarse hacia abajo hasta encontrar el encabezado que dice ***Linux***, para eliminar los signos # debajo de donde dice "si se utiliza ***iptables***".

Figura 23. Configuración archivo etter.conf



Fuente el autor

Figura 24. Selección de campos para cambiar en archivo etter.conf



Fuente el autor

Figura 25. Cambios en archivo etter.conf

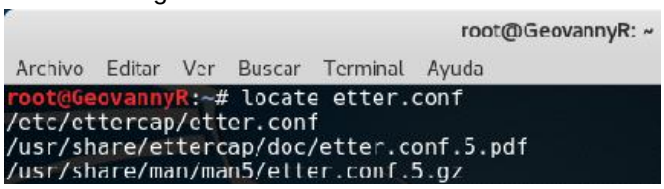
```
#-------------
#     Linux
#-------------

# if you use ipchains:
   #redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
   #redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"

# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --
to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --
to-port %rport"
```

Fuente el autor

Proceder a guardar para continuar.

Seguidamente se debe proceder a verificar la localización de la aplicación "***Ettercap***", ejecutando el comando (**locate etter.conf**).

Figura 26. Ruta archivo etter. conf

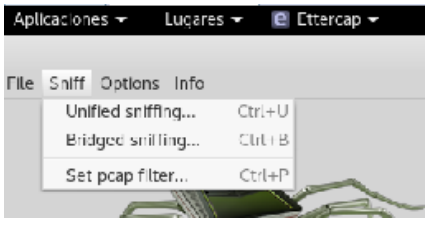


Fuente el autor

Ejecución de Ettercap

Ahora se debe proceder a ejecutar la aplicación "***Ettercap* en modo grafico**". Para ello, hay que dirigirse a (Aplicaciones > Husmeando/Envenenamiento > ettercap). Ya estando con la aplicación en ejecución, hay que dirigirse a *Sniff* y luego seleccionar la opción *Uniffied sniffing*.

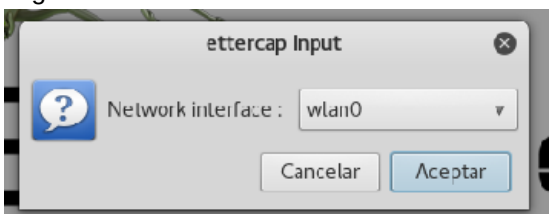
Figura 27. Ejecución herramienta ettercap



Fuente el autor

Seguidamente, hay que seleccionar la Interfax de la tarjeta de red en cuestión, la cual fue consultada con anterioridad "**wlan0"**, presionar aceptar para continuar.

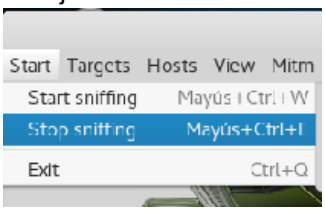
Figura 28. Selección de interfaz de red wlan0



Fuente el autor

Ahora se debe detener la ejecución de la herramienta ettercap, debido a que al seleccionar la interfaz de la tarjeta de red, esta se ejecuta. Para detenerla hay que ingresar a *Start > Stop sniffing*.

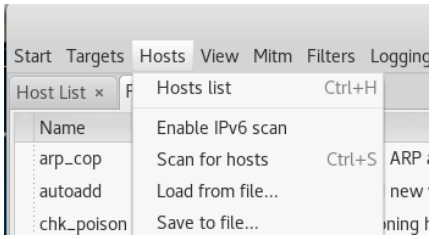
Figura 29. Ejecución herramienta ettercap



Fuente el autor

En este apartado, hay que dirigirse a la pestaña *Hosts > Scan for hosts*.

Figura 30. Escaneando los hosts disponibles

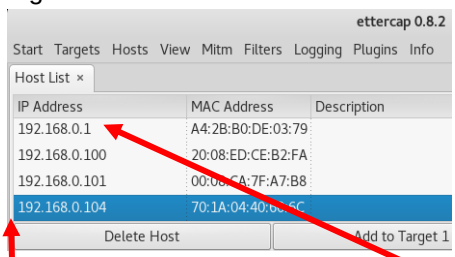


Fuente el autor

Al seleccionar la opción "***Scan for hosts***", se puede ver una barra de progreso que indica la búsqueda de *hosts* disponibles dentro de la red.

Podemos observar en la opción "***Hosts list***" las direcciones que la herramienta ettercap a capturado por medio del escaneo que se ha realizado.

Figura 31. Lista de hosts encontrados



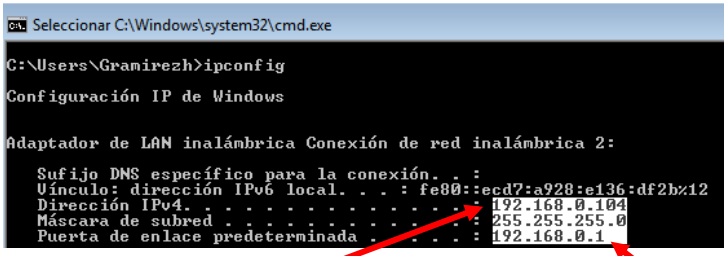
Fuente el autor

Podemos observar que la dirección IP de la víctima aparece en la lista de los hosts encontrados.

Podemos observar que la dirección de la puerta de enlace víctima aparece en la lista de los hosts encontrados.

Seguidamente, hay que dirigirse a la segunda máquina, la cual es la de la víctima, para verificar si la dirección IP y la puerta de enlace, aparecen dentro de las direcciones que ettercap ha capturado, por medio del escaneo. En pasos anteriores se había consultado, pero se puede consultar nuevamente. Para ello, hay que dirigirse a inicio e invocar el "**CMD**", para luego introducir en l consola de CMD el comando "***ipconfig***".

Figura 32. Ejecución consola CMD consultas máquina víctima



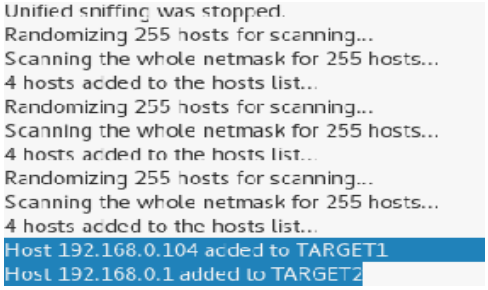
Fuente el autor

Dirección IP: **192-.168.0.104** de la máquina víctima

Puerta de enlace: **192.168.0.1** de la máquina víctima.

Ahora, se procede a agregar la dirección IP de la víctima al "**add to Target 1**", la cual en este caso es "**192.168.0.104**" y la puerta de enlace al "**Add to Target 2**", la cual en este caso es "**192.168.0.1**"

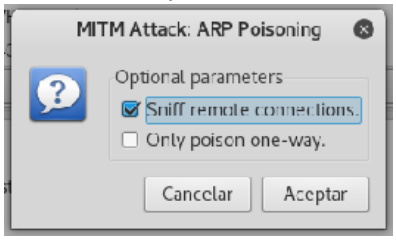
Figura 33. Agregando direcciones a target 1 y target 2



Fuente el autor

Seguidamente hay que dirigirse a la opción "***Mitm***", luego a la opción "***ARP poisining***", Al seleccionar las opciones anteriores, se abre una ventana, en la cual debemos seleccionar la opción "***Sniff remote connections***", la cual nos permita husmear conexiones remotas o cercanas a la red.

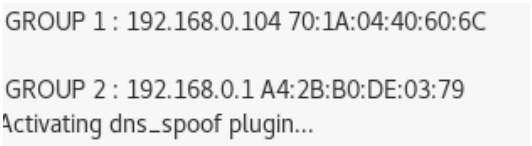
Figura 34. Selección de opción Sniff remote connections



Fuente el autor

En este apartado, hay que seleccionar los plugins que se va a implementar en el ataque. Para ello, hay que dirigirse a la opción "***Plugins***" y luego a la opción "***Manage the plugins***". Se debe seleccionar "***dns_spoof***", lo que indica que el sistema atacante, empezará a enviar respuestas dns falsificadas a la máquina víctima.

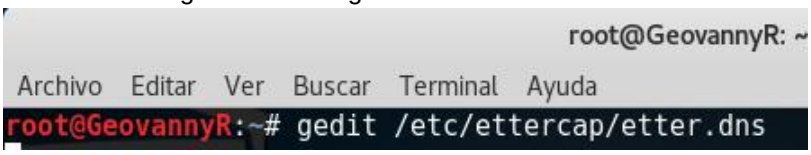
Figura 35. Selección de plugins dns_spoof



Fuente el autor

Seguidamente, hay que ejecutar el comando **gedit /etc/ettercap/etter.dns** y abrir el archivo con un editor de texto como "***gedit o nano***" y editar el archivo, donde se hace referencia al DNS. Es necesario utilizar terminal para este paso.

Figura 36. Configuración archivo etter.dns



Fuente el autor

El archivo **etter.dns**, es el archivo del host y es responsable de desvío de las peticiones DNS específicas que se están realizando. Fundamentalmente, si el objetivo entra en *facebook.com* que va a ser redirigido a la página web de Facebook, pero este archivo puede cambiar todo eso. Aquí es donde sucede el ataque, así que es necesario editarlo de la siguiente manera:

a. En primer lugar, hay que redirigir el tráfico de cualquier sitio web hacia la máquina de *Kali Linux*. Para ello, hay que desplazarse hacia abajo, hasta donde termina los comentarios del archivo, los cuales son el texto encerrado dentro de signos de numeración; y procedemos a agregar en la primera línea la dirección del sitio web que se va a suplantar, en este caso es *Facebook.com*. Además de cambiar la dirección IP de la máquina de *Kali Linux*, la cual en la consulta anterior es **192.168.0.109.**

También se procederá a cambiar la siguiente línea, la cual es un subdominio del dominio, en cual se agregan los mismos datos del paso anterior.

En la tercera línea que aparece, también se procede a agregar los mismos datos del primer punto, cuya finalidad es hacer el retorno del nombre *www.facebook.com*, donde traduce de nombre a dirección web, pero esta línea, si se desea se puede eliminar.

Teniendo este archivo configurado, se debe guardar.

Figura 37. Archivo etter.dns sin cambios

```
################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A   107.170.40.56
*.microsoft.com    A   107.170.40.56
www.microsoft.com  PTR 107.170.40.56
```

Fuente el autor

Figura 38. Archivo etter.dns con los cambios realizados.

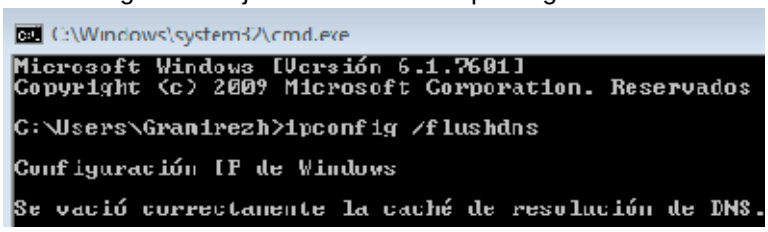
```
################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

facebook.com      A   192.168.0.109
*.facebook.com    A   192.168.0.109
www.facebook.com  PTR 192.168.0.109
```

Fuente el autor

Se procede a guardar para conservar los cambios realizados.

Es necesario reiniciar los "*Flusfdns*", en la maquina víctima, con la finalidad de evitar errores en la ejecución del ataque de *spoofing*. Para ello es necesario ingresar a la consola "CMD" y ejecutar el comando (**ipconfig /flushdns**)

Figura 39. Ejecución comando ipconfig /flushdns



Fuente el autor

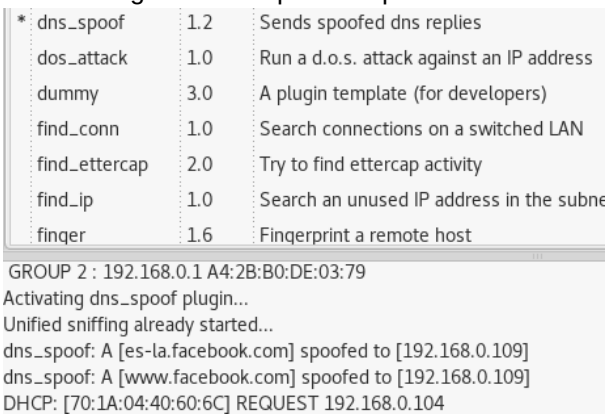
Seguidamente se debe ejecutar la opción "***Start***" de la herramienta ***ettercap*** y luego se procede a abrir Internet Explorer, para volver a ingresar la URL "*facebook.com*" y se puede observar que ahora si tenemos acceso a la página web *Facebook*.

Figura 40. Acceso a la página web facebook.com

Fuente el autor

Inmediatamente, se puede evidenciar que la máquina del atacante ha comenzado a realizar el ataque de *Spoofing* y a capturar la información sobre el DNS del sitio web que se está suplantando, en este caso "*facebook.com*"

Figura 41. Captura de peticiones



Fuente el auto

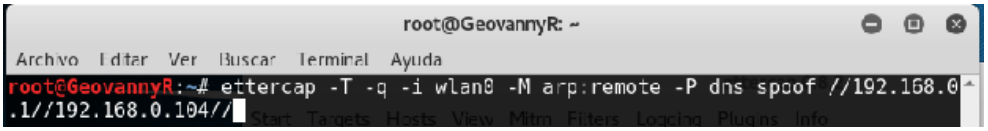
Se puede observar en la figura 39, que se han hecho varias peticiones de acceso a la URL de facebook.com, las cuales son dirigidas a la IP de la máquina del atacante "**192.168.0.109**"

Teniendo configurado y en ejecución el plugins de *ettercap*, se debe proceder a introducir el comando (**ettercap –T –q –i eth0 –M arp:remote -P dns_spoof //192.168.0.1//192.168.0.104//**), donde:

- ✓ –T Es un parámetro que solo permite ver texto como única Interfax.
- ✓ –q Actúa en modo silencioso, e indica que no puede mostrar el contenido del paquete

- ✓ -i Indica por cual Interfaz se quiere realizar la captura del tráfico.
- ✓ eth0: Representa la Interfaz de la tarjeta de red.
- ✓ M Lugar donde se almacena el archivo.
- ✓ *Arp_spoof*: Representa el tipo de ataque o envenenamiento
- ✓ -P Por lo general, ettercap pondrá la interfaz en modo promiscua para oler todo el tráfico.
- ✓ dns_spoof: Es el *plugins* que se va a implementar.

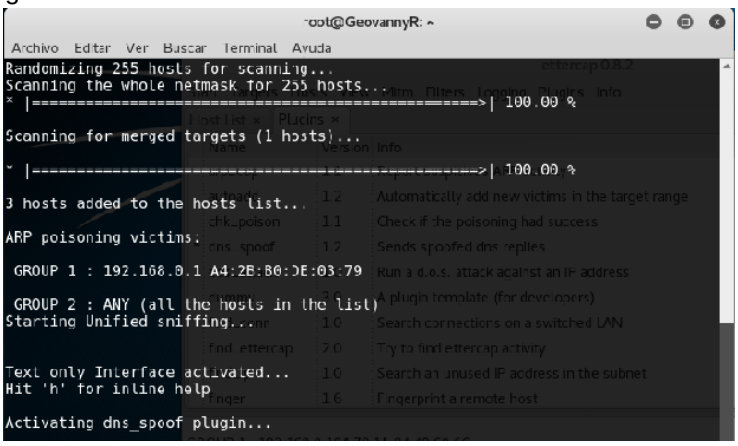
Figura 42. Ejecución de comando en Kali Linux



Fuente el autor

Una vez determinados los parámetros, se presiona enter para iniciar el servicio de ***Ettercap***

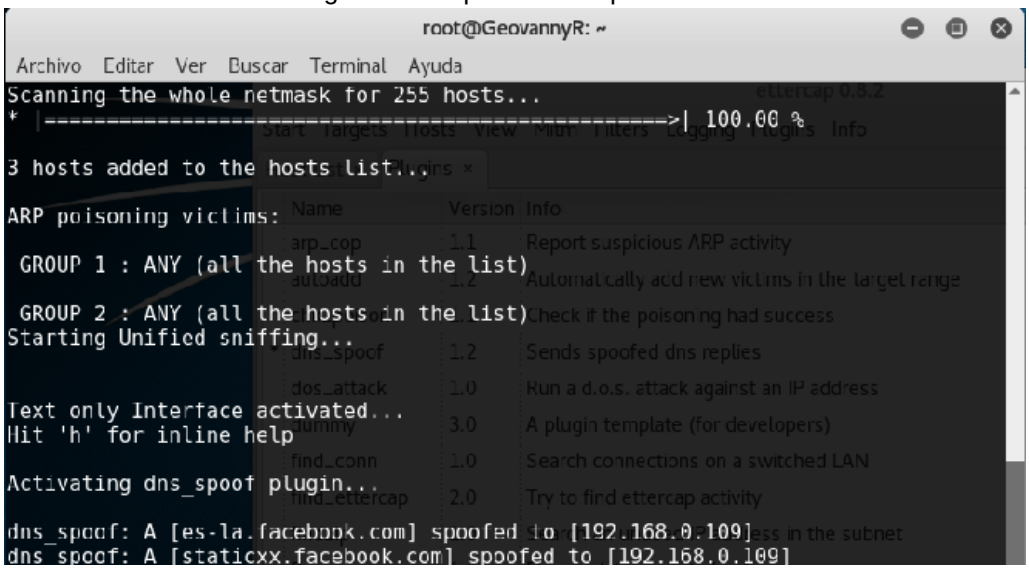
Figura 43. Lanzamiento de escaneo en el host víctima o marcado



Fuente el autor

Se puede observar que el **plugins** ha sido activado, además de establecer conexión con la interfaz de la máquina víctima.

Figura 44. Captura de las peticiones



Fuente el autor

Se puede observar al final de la figura 42, como el ataque ha comenzado a capturar las peticiones realizadas por la máquina víctima y estas son enviadas por medio del plugins "***dns_spoof***", por medio de las solicitudes dns falsificadas, destinadas hacia la máquina víctima.

Impactos generados por los ataques de Spoofing o suplantación de identidad

Como resultado de los ataques de *Spoofing*, tiene su mayor impacto en la falsificación de las credenciales de la víctima, donde el receptor no tiene manera de determinar su veracidad antes de responder. El DNS también es capaz de generar una respuesta mucho más grande que consulta, ante los ataques de suplantación de IP, donde estos también pueden ser utilizados para eludir la autenticación basada en direcciones IP. Este proceso puede ser muy difícil, y se utiliza sobre todo cuando las relaciones de confianza están en su lugar entre máquinas en una red y sistemas internos. Las relaciones de confianza utilizan direcciones IP, más que todo en los inicios de sesión de usuario, para verificar las identidades de las máquinas. Esto permite a las partes maliciosas para usar los ataques de suplantación de hacerse pasar por máquinas con permisos de acceso a la red y medidas de seguridad basadas en la confianza de derivación.

Además de lo anterior, los dispositivos que se conectan a Internet u otras redes privadas se basan en el DNS para resolver las direcciones URL, direcciones de

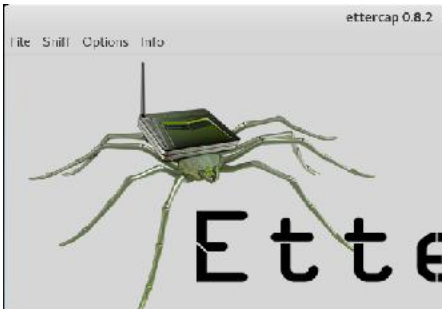
correo electrónico y otros nombres de dominio legibles en sus correspondientes direcciones IP. En un ataque de suplantación de servidor DNS, un usuario malintencionado modifica el servidor DNS con el fin de redirigir un nombre de dominio específico a una dirección IP diferente. En muchos casos, la nueva dirección IP será para un servidor que está efectivamente controlada por el atacante, el cual puede proceder a infectar los archivos con malware o virus e incluso a robarlos.

Otros impactos que no se pueden dejar de comentar, es que los ataques de Spoofing, suelen ser utilizados para facilitar otros tipos de ataques, incluyendo ataques de denegación de servicio, el secuestro de sesión y man-in-the-middle ataques, los cuales pueden ocasionar mayores daños a la información de los usuarios e incluso a la integridad de la persona

4.2.2 Ataque de denegación de servicio o *DoS*.

Para comenzar con el ataque de denegación de servicio en la red wifi "**IDEA internet en el parque**", de la plaza Rafael Uribe Uribe, del municipio de Urrao, hay que ejecutar la herramienta "***ettercap***", la cual nos permite realizar el ataque con unos simples pasos, pero con muy buena efectividad.

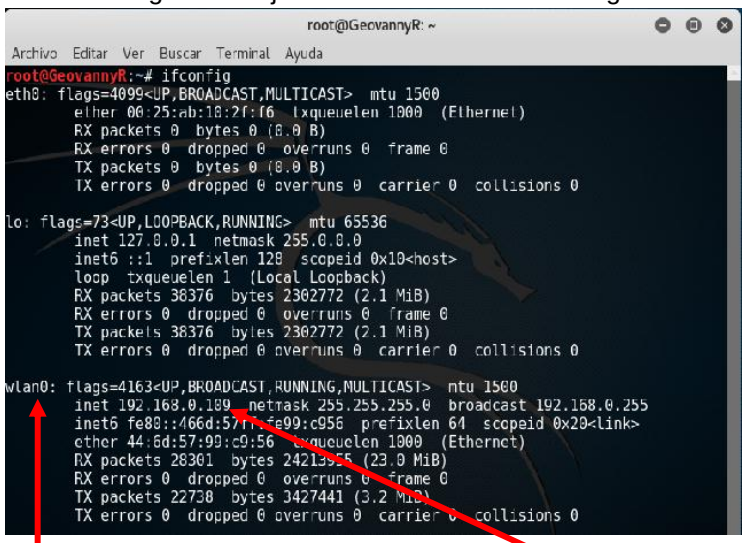
Figura 45. Ejecución de ettercap



Fuente el autor

Seguidamente hay que dirigirse a seleccionar el tipo de red la cual la verificaremos por medio de la terminal de *Kali Linux*, ejecutando el comando (**ifconfig**), para identificar el tipo de red y la dirección IP de la máquina atacante.

Figura 46. Ejecución del comando ifconfig



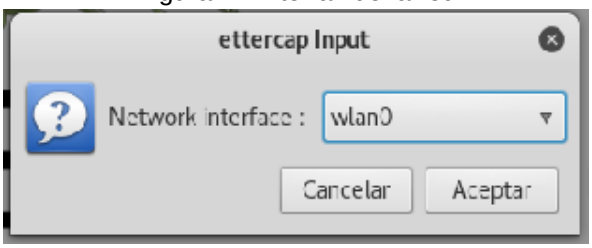
Fuente el autor

Se puede observar que el equipo está conectado a la red IDEA internet en el parque por medio de la wlan0

La dirección IP de la máquina atacante, es la **192.168.0.109**

Ahora se procede a seleccionar el tipo de la red, la cual se puede observar en la figura 45, que nos muestra que es la “wlan0”, además de verificar la respectiva IP “**192.168.0.109**”

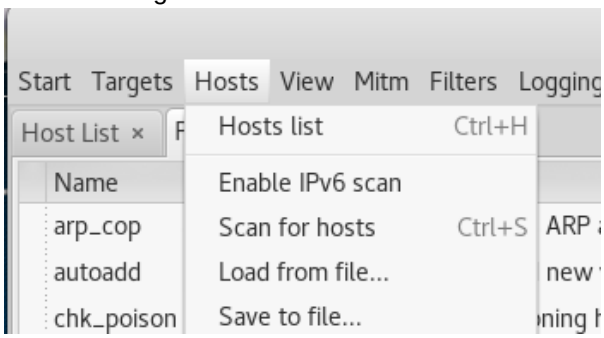
Figura 47.Interfaz de la red



Fuente el autor

En este apartado, hay que dirigirse a la pestaña *Hosts* > *Scan for hosts*.

Figura 48. Escaneo de Hosts

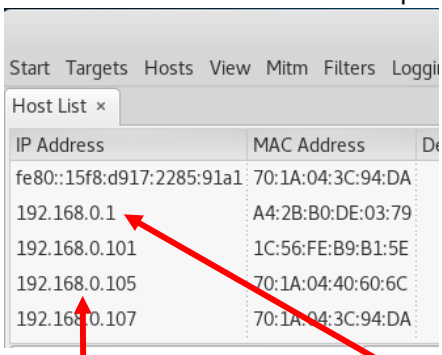


Fuente el autor

Al seleccionar la opción "***Scan for hosts***", se puede ver una barra de progreso que indica la búsqueda de hosts disponibles dentro de la red.

Podemos observar en la opción "***Hosts list***" las direcciones que la herramienta ettercap ha capturado por medio del escaneo que se ha realizado.

Figura 49. Verificación de los hosts disponibles



Fuente el autor

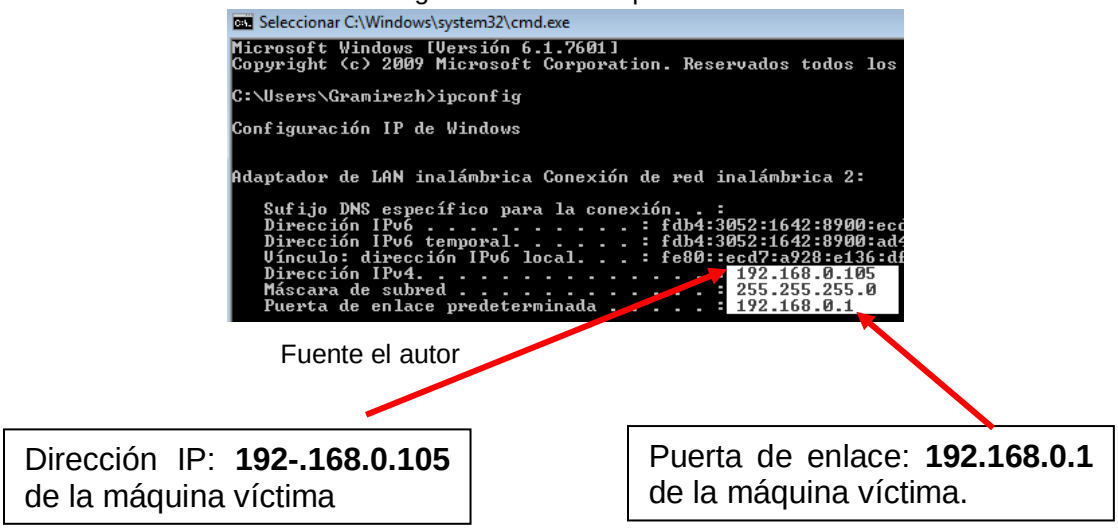
Podemos observar que la dirección IP de la víctima aparece en la lista de los hosts encontrados.

Podemos observar que la dirección de la puerta de enlace víctima aparece en la lista de los hosts encontrados.

Seguidamente, hay que dirigirse a la segunda máquina, la cual es la de la víctima, para verificar si la dirección IP y la puerta de enlace, aparecen dentro de las direcciones que ettercap ha capturado, por medio del escaneo. En pasos anteriores se había consultado, pero se puede consultar nuevamente. Para ello,

hay que dirigirse a inicio e invocar el "**CMD**", para luego introducir en l consola de CMD el comando "**ipconfig**".

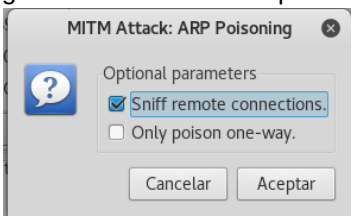
Figura 50. Consulta por CMD



Fuente el autor

Seguidamente hay que dirigirse a la opción "***Mitm***", luego a la opción "***ARP poisining***", Al seleccionar las opciones anteriores, se abre una ventana, en la cual debemos seleccionar la opción "***Sniff remote connections***", la cual nos permita husmear conexiones remotas o cercanas a la red.

Figura 51. Activando ataque ARP



Fuente el autor

En este apartado, hay que seleccionar los plugins que se va a implementar en el ataque. Para ello, hay que dirigirse a la opción "***Plugins***" y luego a la opción "***Manage the plugins***". Se debe seleccionar "***dos_attack***", lo que significa que se va a ejecutar un ataque dos contra la dirección IP de la máquina víctima.

Figura 52. Activación plugins dos_attack

```
Activating dos_attack plugin...
dos_attack: Invalid IP address.
Activating dos_attack plugin...
dos_attack: Starting scan against 192.168.0.105 [Fake Host: 192.168.0.109]
dos_attack: Port 80 added
dos_attack: Port 443 added
dos_attack: Starting attack...
Unified sniffing already started...
Unified sniffing was stopped.
```

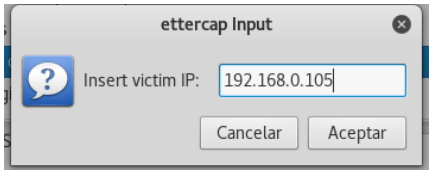
Fuente el autor

Al seleccionar el plugins “**dos_attack**”, se procede a ingresar la dirección IP de la máquina víctima, la cual es “**192.168.0.105**”.

Figura 53. Selección del plugins dos_attack

Fuente el autor

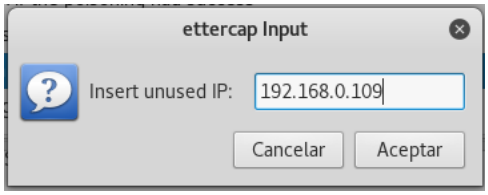
Figura 54. Ingreso de la dirección IP de la víctima



Fuente el autor

Seguidamente, se procede a ingresar la dirección IP de la máquina del atacante, la cual es “**192.168.0.109**”.

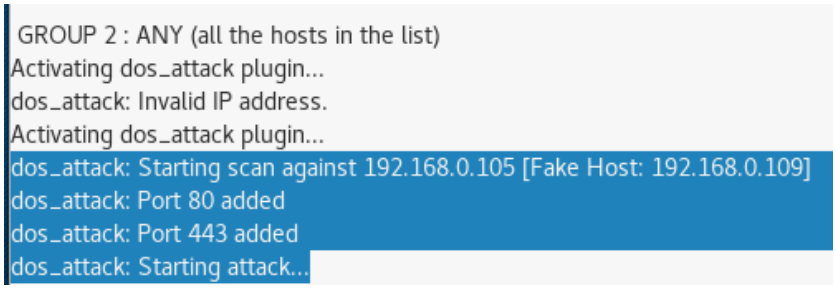
Figura 55. Ingreso de la dirección IP del atacante.



Fuente el autor

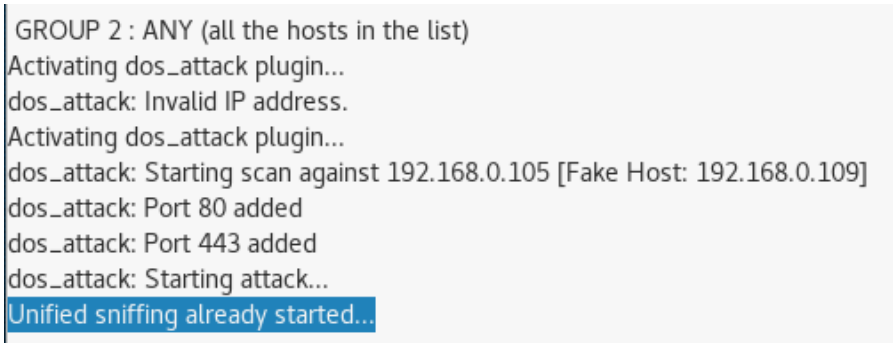
Ahora, se debe proceder con la activación del ataque ejecutando la opción "***Start***" de la herramienta ***ettercap*.**

Figura 56. Ejecución del ataque dos_attack



Fuente el autor

Figura 57. Inicio del sniffing unificado

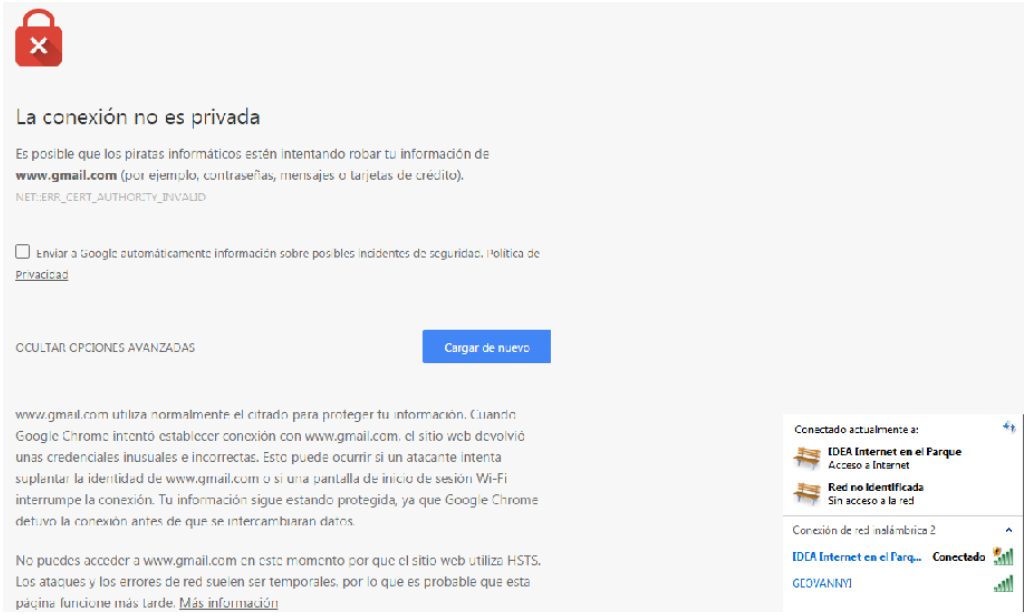


Fuente el autor

Se puede observar en la figura cincuenta y tres, como el ataque comienza su ejecución, mostrando que la máquina del atacante comienza a explorar contra la dirección IP **192.168.0.105**, anfitrión falso **192.168.0.109**, empieza a enviar una gran cantidad de paquetes, hasta hacer que la maquina víctima no tenga acceso a la internet, por medio de la red wifi "**IDEA internet en el parque**".

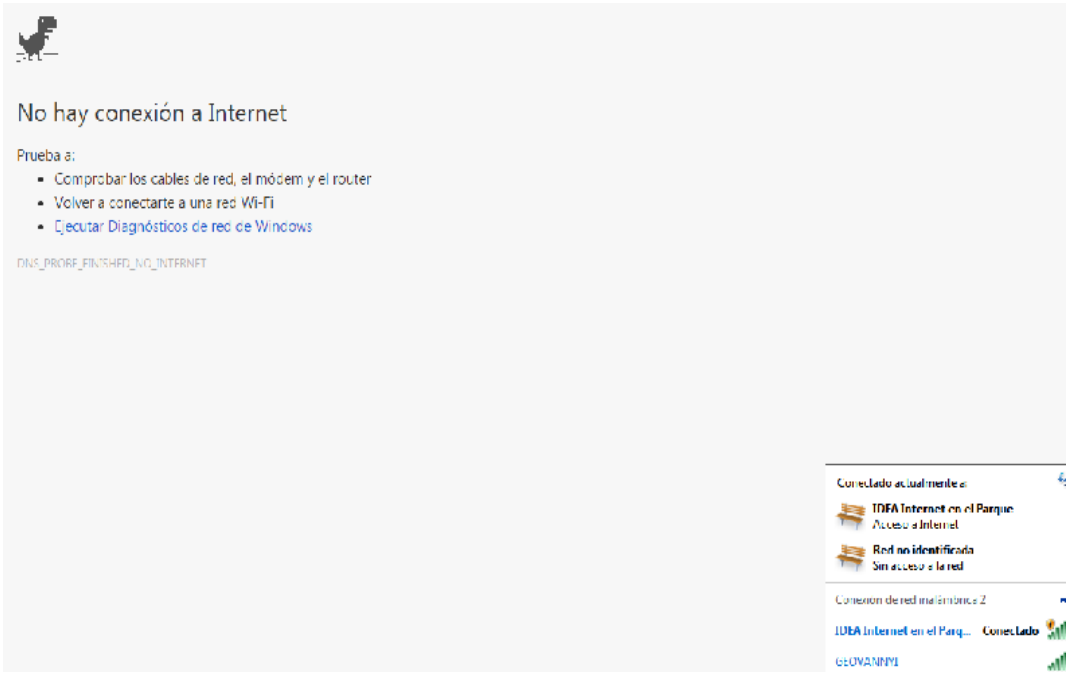
Para verificar, que máquina víctima no tiene conexión se probara el acceso a varios sitios web (*www.gemail.com, Facebook.com, www.hotmail.com*), los cuales se pueden verificar en las figuras 53, 57 y 58.

Figura 58. Acceso a la página web www.gmail.com



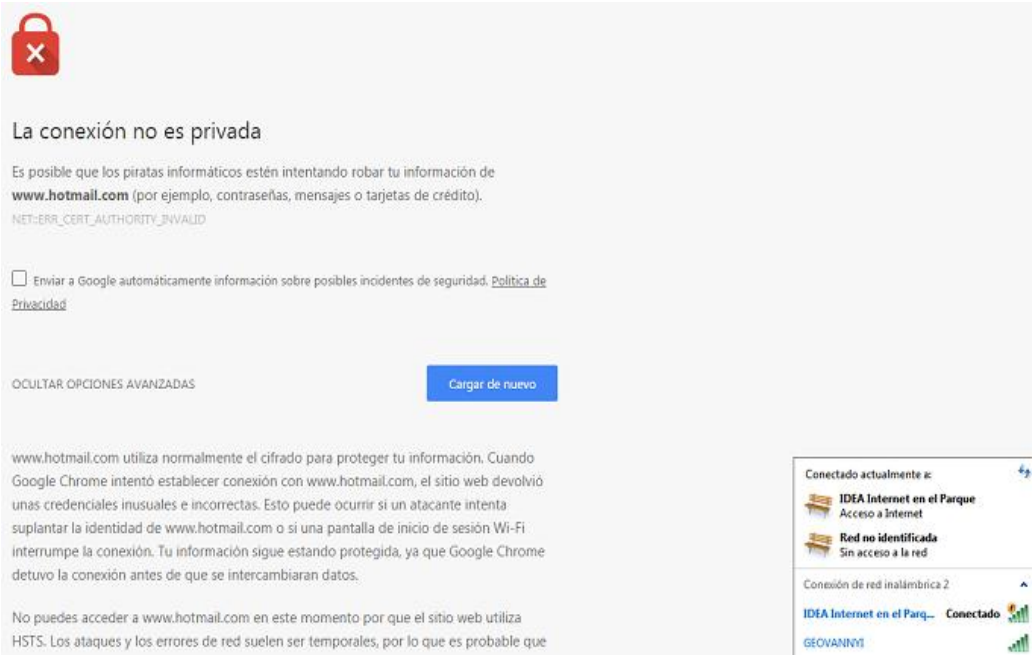
Fuente el autor

Figura 59. Acceso a la página web facebook.com



Fuente el autor

Figura 60. Acceso a la página web www.hotmail.com



Fuente el autor

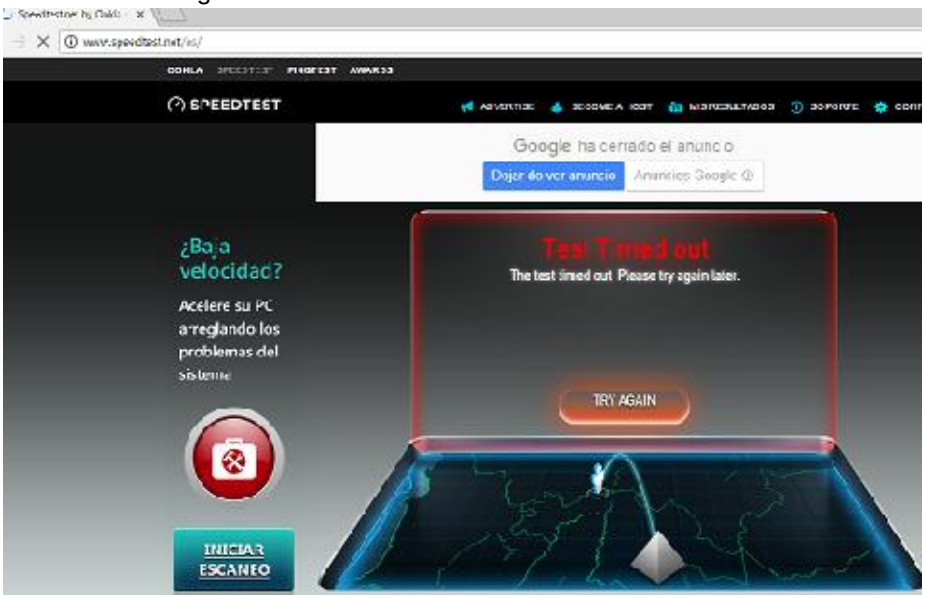
Se puede observar que, en cada una de las páginas web, no hay acceso al servicio de internet, por medio de la red wifi "**IDEA internet en el parque**", donde dos de los sitios web, advierten sobre posibles ataques o errores.

Impactos generados por los ataques de denegación de servicio DoS.

Con las evidencias adquiridas durante el desarrollo del ataque de denegación de servicio *DoS*, el cual se ha desarrollado utilizando la conexión de la red wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, del municipio de Urrao. Significa que el ataque *DoS* causa un impacto efectivo para interrumpir los servicios de Internet de toda la red; donde el ataque se centra en los servidores web reales, cortafuegos y equilibradores de carga para interrumpir las conexiones, lo que resulta en agotar su número finito de conexiones simultáneas que el dispositivo puede soportar.

Verificando la velocidad de la red wifi "**IDEA internet en el parque**", con la herramienta "*ESPEEDTEST*", se puede observar en la figura 59, que ni siquiera la herramienta de medición, es capaz de medir el ancho de banda, durante las etapas del ataque *DoS*.

Figura 61. Medición de la velocidad de la red wifi



Fuente el autor

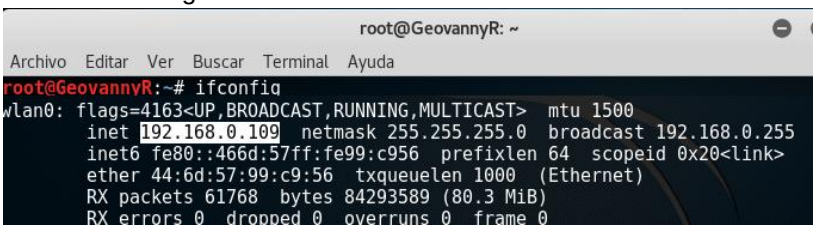
En pocas palabras, los ataques DoS paralizan las operaciones relacionadas con el servicio de internet wifi "**IDEA internet en el parque**"; por ello, la administración debe tener en cuenta que el potencial de daño es alto, el cual puede ser aprovechado por delincuentes, los cuales pueden servirse de la distracción causada para agarrar y clonar los datos privados de aprovechar los fondos, propiedad intelectual y más.

4.2.3 Ataques de Phishing, Man in the middle y ARP Spoofing

El siguiente ataque de Phishing se ha realizado a Hotmail, con la finalidad de capturar las contraseñas de los usuarios, usando iptables; además de ello se empleará el ataque del "***Man-in-the-middle***", por medio del sistema operativo *Kali Linux 2.0*, además de usar *iptables*. Este ataque se redirigirá todo el tráfico que pasa por el puerto 80 a un sitio de *Phishing* en la red de wifi, usando Iptables y Arpspoof. Este ataque se puede hacer en cualquier sistema *Linux* y en cualquier sistema operativo de destino.

Para comenzar, se procede identificando la dirección IP de la tarjeta de red que el equipo posee. Para ello, se procede abriendo l terminal de *Kali Linux* e introduciendo el comando ifconfig, donde se puede evidenciar que la IP de la máquina es "**192.168.0.109**".

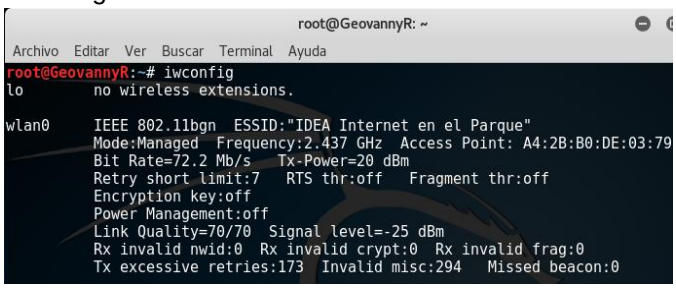
Figura 62. Identificación de interfaz de red



Fuente el autor

Seguidamente se procede identificando la red inalámbrica sobre la que se conectará la maquina atacante, para realizar el respectivo ataque. Para ello, se ingresa en la terminal de *Kali Linux*, el comando (iwconfig). Donde se apreciar que la red se llama "**IDEA internet en el parque**".

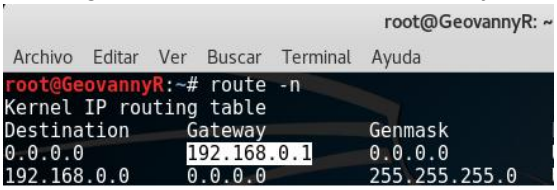
Figura 63. Identificación nombre de la red wifi



Fuente el autor

Ahora se procede a identificar el "*Gateway*" de la máquina atacante. Se debe ingresar a la terminal de *Kali Linux*, el comando (route -n), donde se aprecia en la figura 62 que la dirección es "**192.168.0.1**"

Figura 64. Identificación de Gateway

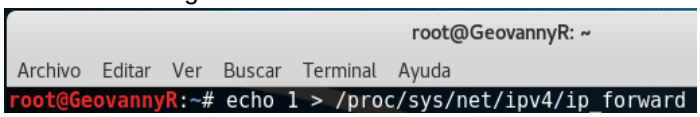


Fuente el autor

Seguidamente se procede a descargar el archivo de Repositorio para el Marco *Pentest Smartphone* (**SPF-master**) del sitio oficial "git clone https://github.com/georgiaw/Smartphone-Pentest-Framework.git", y se descomprime en el escritorio.

Ahora se debe activar el "***IP forwarding***" en el computador atacante, debido a que este actuará como ruteador, ingresando en la terminal de *Kali Linux*, el comando (**echo > 1 /proc/sys/net/ipv4/ip_forward**).

Figura 65. Activación IP forward



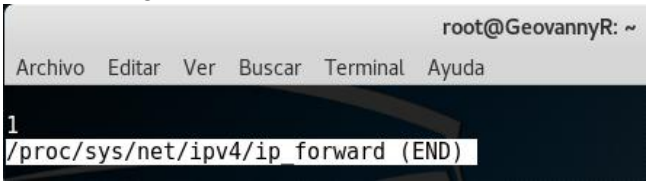
Fuente el autor

Seguidamente se procede a verificar si el archivo que ha sido creado en el paso anterior, se ha guardado correctamente. Se debe ingresar a la terminal de *Kali Linux* e ingresar el comando **(less /proc/sys/net/ipv4/ip_forward**), el cual nos servirá para visualizar archivos de texto almacenados en disco.

Figura 66. Comando less

Fuente el autor

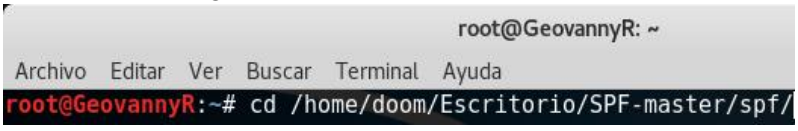
Figura 67. Visualización de archivo



Fuente el autor

En este apartado hay que ubicarnos en el lugar donde está guardado el archivo de Repositorio para el Marco *Pentest Smartphone* (**SPF-master**). Para ello, se debe ingresar en la terminal de *Kali Linux* el comando (**cd /home/doom/Escritorio/SPF-master/spf**)

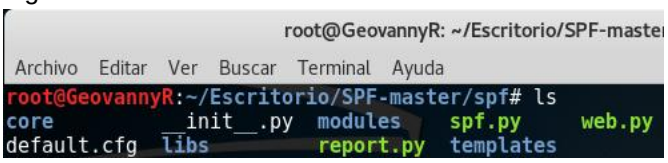
Figura 68. Localización archivo SPF



Fuente el autor

Ahora se debe ingresar en la terminal de *Kali Linux* el comando (ls), para ver contenido de los archivos que están actualmente en la ruta solicitada por el usuario.

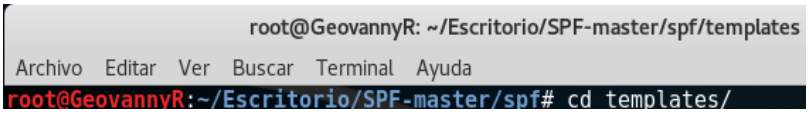
Figura 69. Verificación de contenido de la ruta solicitada



Fuente el autor

Continuando, se debe ingresar en la terminal de *Kali Linux* el comando (**cd templates/**), para abrir dicho archivo y ver los ficheros.

Figura 70. Apertura de archivo



Fuente el autor

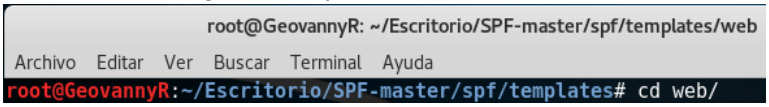
Ahora se debe ingresar en la terminal de *Kali Linux* el comando (ls), para ver contenido de los ficheros que están actualmente en la ruta requerida por el usuario.

Figura 71. Verificación de contenido de la ruta solicitada

Fuente el autor

Seguidamente, se procede ingresando en la terminal de *Kali Linux*, el comando (**cd web/)**, para entrar al directorio fichero solicitado por el usuario.

Figura 72. Apertura de fichero web



Fuente el autor

Ahora se debe ingresar en la terminal de *Kali Linux* el comando (ls), para ver contenido de los ficheros que están actualmente en la ruta requerida por el usuario.

Figura 73. Verificación de los ficheros

Fuente el autor

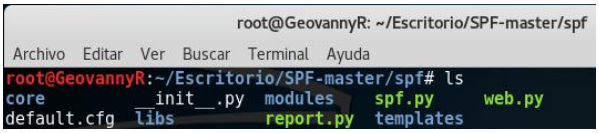
En este apartado, hay que devolverse dos veces, para localizar el directorio "***templates***", ingresando en la terminal de *Kali Linux* el comando cd. En dos ocasiones.

Figura 74. Retroceso de ficheros

Fuente el autor

Una vez instalado en el directorio requerido, se debe ingresar en la terminal de *Kali Linux* el comando (ls), para ver contenido de los ficheros que están actualmente en la ruta requerida por el usuario.

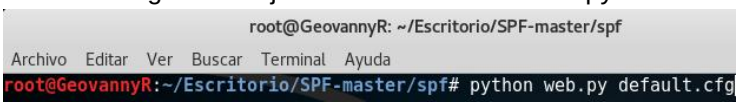
Figura 75. Verificación de ficheros



Fuente el autor

Ahora se procede a ejecutar en la terminal de *Kali Linux*, el comando (**Python web.py default.cfg**), para que el Repositorio para el *Marco Pentest Smartphone* (**SPF-master**), se ejecute en la máquina.

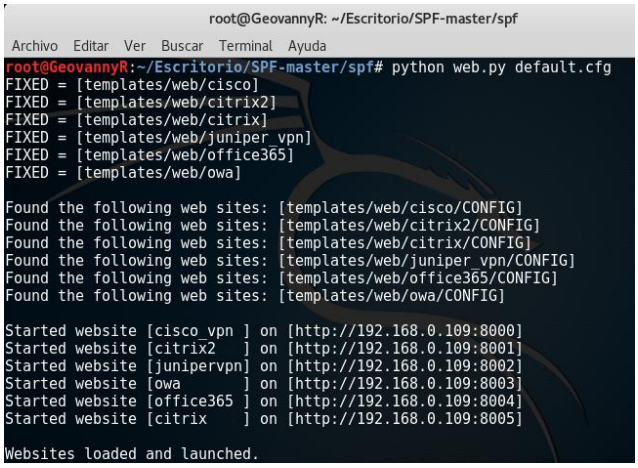
Figura 76. Ejecución de comando web.py



Fuente el autor

Se puede observar en la figura 75, la ejecución correcta del Repositorio para el *Marco Pentest Smartphone* (**SPF-master**), el cual se ejecuta correctamente.

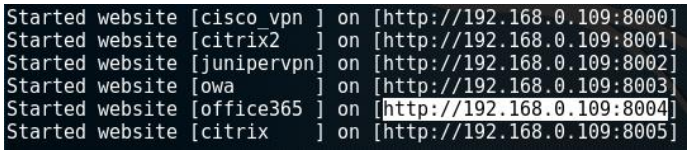
Figura 77. Lanzamiento de aplicación web.py



Fuente el autor

Seguidamente, se debe seleccionar la dirección IP del sitio web "*office365*", la cual se puede observar en la figura 76. Cabe recordar que el ataque se basa, en la realización de *Phishing a Hotmail*, donde copiaremos la dirección IP para proceder con el siguiente paso.

Figura 78. Selección de IP de office365

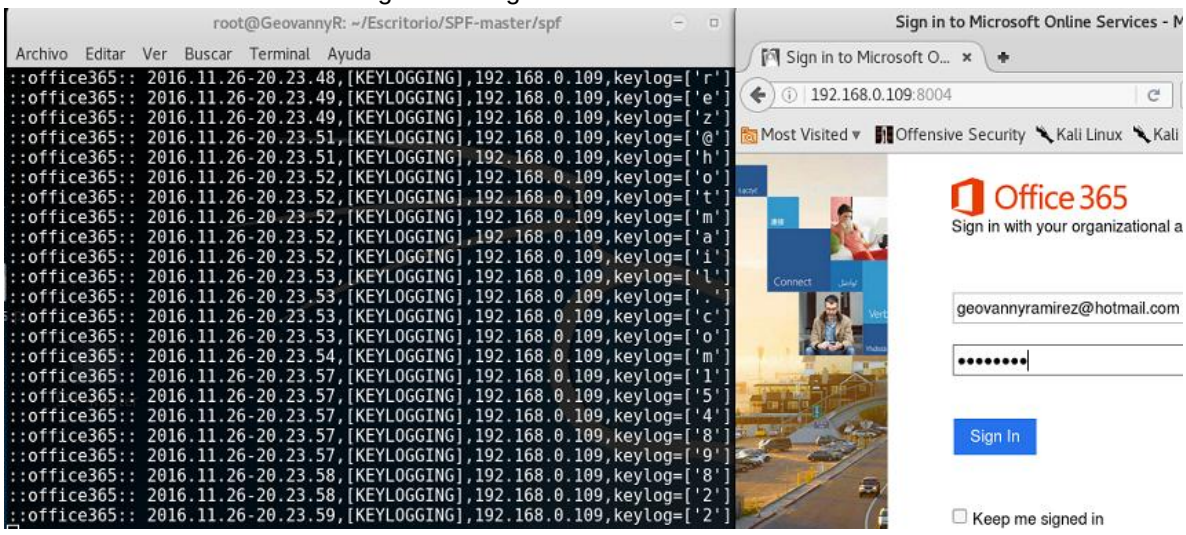


Fuente el autor

Inmediatamente, se procede a ingresar la dirección IP en la URL del navegador, donde se debe Introducir una cuenta de *Hotmail* y una contraseña, para ver si la máquina atacante, está capturando el tráfico.

En la figura 77, se evidencia el ingreso de correcto de una cuenta de *Hotmail*, así como su respectiva clave

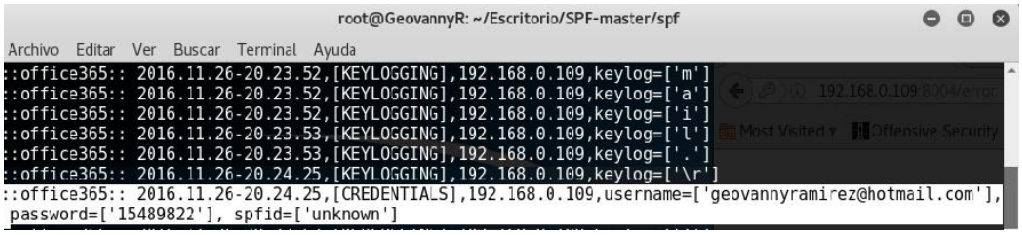
Figura 79. Ingreso de cuenta de Hotmail



Fuente el autor

En la figura 78, se evidencia que al final de la misma, la maquina atacante captura correctamente el tráfico de la red, así como los datos que se han introducido para dicha prueba.

Figura 80. Captura del tráfico de la red



Fuente el autor

Para los siguientes pasos se debe verificar el puerto que está manejando "*office365*". Para ello se verifica en la figura 76, donde se identifica el puerto Nº 8004.

Ahora se procede a ingresar en la terminal de *Kali Linux* el comando (**iptables -t nat -A PREROUTING -p tcp - -dport 80 -j REDIRECT - -to- port 8004**). Lo que se busca es redireccionar el tráfico que pase por el puerto 80 y capturar las credenciales que los usuarios ingresen a *Hotmail,* mientras están conectados a la red wifi.

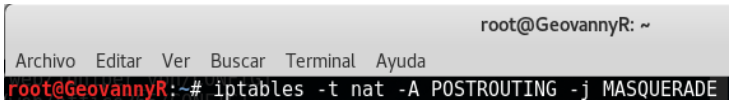
Figura 81. Comando Iptables Nat

Fuente el autor

Con el comando que se ha ejecutado en la figura 79, las solicitudes que vengan del puerto 80 serán redirigidas con la regla de *Nat iptables*, hacia la máquina atacante.

Ahora se procede a ingresar en la terminal de *Kali Linux* el comando (**iptables -t nat -A POSROUTING -j MASQUERADE**), donde, Aunque nat se hace pasar por la función fundamental de la dirección real a otra, los detalles difieren ligeramente. Más notablemente, haciéndose pasar elige la dirección IP de origen para el paquete de salida de la IP asociada a la interfaz a través del cual saldrá del paquete, hacia la máquina del atacante.

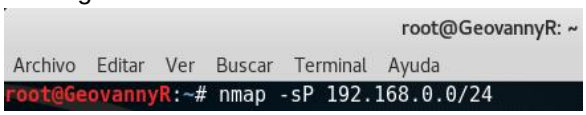
Figura 82. Cambio de rutas de los paquetes



Fuente el autor

Seguidamente, se procede a ingresar en la terminal de *Kali Linux*, el comando (**nmap -sP 192.168.0.1/24**), donde la dirección IP que se ha introducido en el comando, es la de la máquina atacante, destinada para identificar las direcciones de los equipos que están conectados a la red wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe.

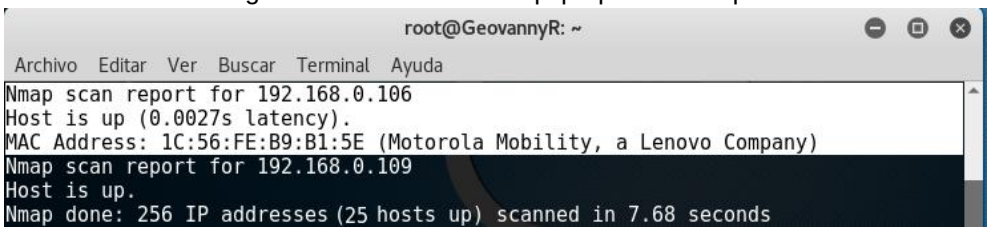
Figura 83. Verificación de direcciones IP



Fuente el autor

Al realizar el escaneo con la herramienta nmap, se procede a seleccionar la dirección IP "**192.168.0.106**", la cual es la dirección de mi teléfono celular.

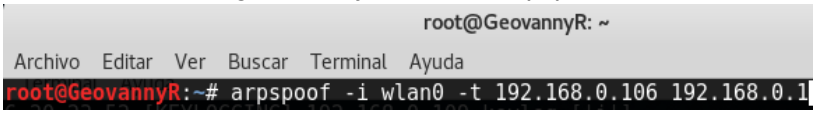
Figura 84. Selección de equipo para el ataque



Fuente el autor

Ahora se comience con la realización del ataque simulado ARP en la víctima, donde se ha seleccionado la dirección IP "**192.168.0.106"** y el *Gateway*, el cual se ha consultado en la figura 62 "**192.168.0.1**".

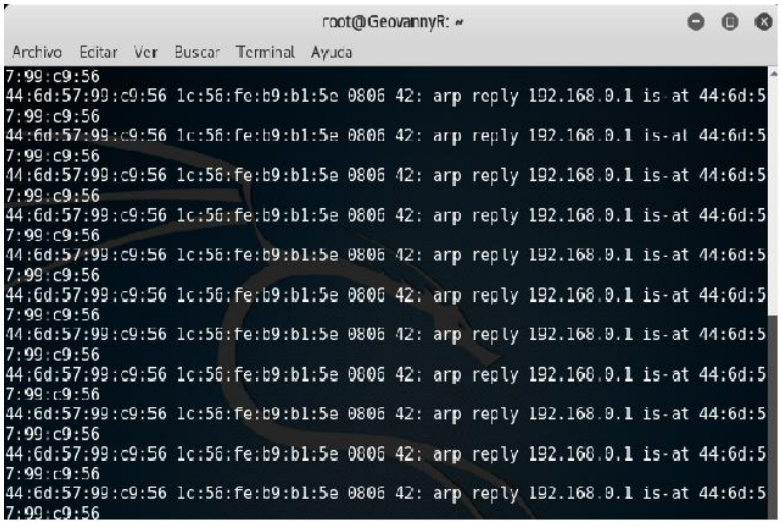
Figura 85. Ejecución de Arpspoof



Fuente el autor

Cuando se ejecuta el ataque de *Arpspoof*, la máquina atacante comienza a realizar el ataque simulado con él envió de réplicas, lo cual se puede apreciar en la figura 84.

Figura 86. Replicas hacia la máquina víctima

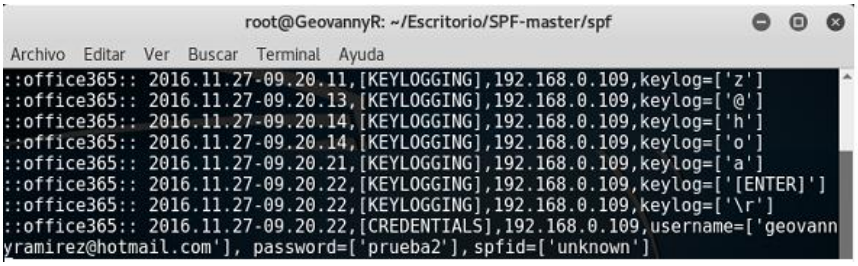


Fuente el autor

Para demostrar que el equipo celular es de propiedad del autor, en los anexos se adjunta imagen que muestra la respectiva dirección IP y la dirección MAC.

Al final se procede a ingresar a "***office365***" por medio del equipo celular, donde se procede ingresando una cuenta de Hotmail y su respectivo *password*. Se puede evidenciar en la figura 85, como la maquina víctima ha capturado el tráfico de la red, representado en credenciales de acceso, y al final de la misma figura, se observa los resultados obtenidos durante el desarrollo de los respectivos ataques.

Figura 87. Captura de credenciales prueba2



Fuente el autor

Nota: Este ataque se puede hacer contra cualquier dispositivo incluyendo *Android, iPhone, Windows, Linux y Mac*.

Impactos generados por los Ataques de Phishing, Man in the middle y ARP Spoofing

a) Impactos generados por el ataque de Phishing

El Phishing es un tema importante, ya que ya no es algo que sólo puede ser realizado por los piratas informáticos, sino por cualquier persona con acceso a Internet. Un ataque de *Phishing* exitoso puede tener consecuencias desastrosas para las víctimas que conducen a pérdidas financieras y el robo de identidad. En este proyecto, se evidencia la facilidad para realizar este tipo de ataques y las consecuencias que pueden conllevar en un futuro; donde el ordenador de la víctima, se convierte en un objetivo y el atacante procede a utilizar varios programas y técnicas para espiar las comunicaciones con los sitios web y recoger información sensible de los usuarios que utilicen la red wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe del municipio de Urrao.

Los ataques de Phishing representan un aspecto de las amenazas de seguridad cada vez más complejas y convergentes que enfrentan los usuarios y las empresas hoy en día. Los métodos utilizados por los *spammers* se han vuelto más sofisticados, y el correo basura ahora se combina cada vez más con el malware y se utiliza como una herramienta para el fraude en línea o robo.

El daño causado por el Phishing no sólo se aplica a la propiedad monetaria por sí sola. Los frágiles lazos de confianza que las organizaciones establecen con sus constituyentes se hacen añicos en el proceso. Referente a la individualización de las personas, conlleva a la pérdida de fe en la fiabilidad de los métodos de comunicación electrónica, en las compañías causan la pérdida de la base de datos de los clientes. En los casos de desastres, la gente puede gastar miles de millones en preparación, para analizar las debilidades y mejorar el tiempo de recuperación, donde todos estos casos, surgen de los ataques de *Phishing*. Esto a su vez provoca una pérdida significativa de dinero, recursos y tiempo.

b) Impactos generados por el ataque *Man in the middle*.

Los ataques de ***Man in the middle*,** el caso de las redes inalámbricas wifis públicas, son un buen punto para que los atacantes realicen actividades ilegales, tales como el robo de datos, el cual puede ser en realidad un poco más fácil; donde los atacantes, explotan las vulnerabilidades de diseño en redes Wifi, por lo que un punto de acceso ficticio se configura en la red, con la misma firma SSID, y una señal más fuerte. El siguiente paso consiste en interrumpir el tráfico del cliente al router inalámbrico legítimo de bienes, ya sea mediante la suplantación de identidad o sometiendo el router a un ataque de denegación de servicio mediante una tormenta de paquetes. Una vez que el router se da por vencido, una conexión Wifi es establecida por el router ficticia, que inicia el rastreo de paquetes y el robo de datos. Hay algunas otras ideas, tales como la tala en el router real utilizando un método de fuerza bruta, y la creación de un enlace inalámbrico con el router ficticio, o falsificar la dirección MAC del router real para engañar y atraer a los clientes Wifi al router simulado, entre otras características más.

Debido a la utilización de señales inalámbricas, desafortunadamente es posible que el atacante pueda robar datos sin ser detectados, casi siempre. Debido a la falta de conocimiento, es muy común tener routers inalámbricos en el hogar o en el trabajo, que no están configurados correctamente, o no garantizados utilizar claves o contraseñas adecuadas. Es importante tener en cuenta que los ataques MITM son posibles en los componentes de red críticos, así como con nuevas tecnologías. *Routers y Switches* administrados pueden ser falseadas que resulta en un mayor impacto en la seguridad de los usuarios de la red wifi "**IDEA internet**

en el *Man in the middle* parque", de la plaza Rafael Uribe Uribe, donde los usuarios también pueden ser engañados para entregar el tráfico legítimo a una máquina sin escrúpulos.

Como resultado final, un ataque, es realmente difícil de abordar, y por lo tanto debe ser tomado en serio por el equipo de gestión de tecnologías de la información. Puede resultar en el robo de datos, mala imagen de la reputación y pérdidas económicas, tanto a los usuarios y a las empresas.

c) Impactos generados por el ataque *ARP Spoofing*.

Los ataques de suplantación *ARP Spoofing*, pueden tener efectos graves para los usuarios de la red wifi "**IDEA internet en el parque**", de la plaza Rafael Uribe Uribe del municipio de Urrao. En su nivel más básico, los ataques de suplantación ARP se utilizan para robar información sensible de los usuarios, para ser utilizada en la suplantación de identidad, por medio del robo de credenciales de acceso. Además de lo anterior, los ataques de *ARP Spoofing*, se utilizan a menudo para facilitar otros ataques, tales como:

a) Ataques de denegación de servicio: Se utilizan *ARP Spoofing* para enlazar varias direcciones IP en una red, además de capturar la dirección MAC en un solo objetivo. Debido a esto, el tráfico que está destinada a diferentes direcciones IP será redirigido a la dirección MAC del destino, sobrecargando así el objetivo con el tráfico.
b) Secuestro de sesiones: Los ataques de secuestro de sesión pueden hacer uso de *ARP Spoofing* para robar los identificadores de sesión, garantizando así el acceso a los atacantes y los sistemas privados de datos.
c) *Man-in-the-middle* ataques: Se pueden utilizar *ARP Spoofing* para interceptar y o modificar el tráfico entre dos víctimas.

Análisis de las pruebas técnicas realizadas

Se ha podido evidenciar que en la red Wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, del municipio de Urrao, es una red de conexión a internet publica, en la cual, las personas inescrupulosas, pueden realizar fácilmente ataques cibernéticos, poniendo en riesgo la integridad de los datos de los usuarios, así como la integridad y la moral de los mismos.

En la práctica realizada de varios ataques cibernéticos, los cuales son los que más se presentan en las redes wifi públicas, se ha comprobado que a pesar de que, al usuario, solo se le permite una conexión de tan solo 90 minutos y luego de una desconexión de 30 minutos, se puede volver a reconectar, es un tiempo más que suficiente para que un atacante, realice gran variedad de ataques cibernéticos, con la finalidad de sustraer información de las víctimas. Entre los ataques realizados, están:

Práctica del ataque *Spoofing* o suplantación de DNS

Los atacantes cibernéticos, suelen abusar maliciosamente de los defectos de ejecución del DNS, donde las fallas en la implementación del protocolo DNS permiten que sea explotado y utilizado para actividades maliciosas. Debido a que DNS es un protocolo tan crítico para las operaciones de Internet, un sinnúmero de sistemas operativos y aplicaciones, operadores y administradores deben endurecer la seguridad de los servidores DNS para evitar que sean utilizados maliciosamente. Algunos de estos defectos se presentan en este documento para informar a los operadores cómo pueden ser utilizados maliciosamente.

Los DNS abiertos *Resolvers*, en un servidor DNS que permite a los clientes DNS que no son parte de su dominio administrativo de usar ese servidor para llevar a cabo la resolución de nombres recursivo. En esencia, un dispositivo de resolución DNS proporciona respuestas abiertas a las preguntas de cualquier persona que hace una pregunta. Y el DNS resolutor este abierto, es vulnerable a múltiples actividades maliciosas. Estos ataques son posibles porque el dispositivo de resolución abierta responderá a las preguntas de cualquier persona que hace una pregunta. Los atacantes utilizan estos DNS resolución de puertas abiertas para actividades maliciosas mediante el envío de mensajes de DNS para los resolutores abiertas usando una dirección IP de origen forjado que es el objetivo del ataque. Cuando los resolutores abiertos reciben los mensajes de consulta DNS imitan, responden mediante el envío de mensajes de respuesta DNS a la dirección de destino. Los ataques de este tipo utilizan varias resoluciones de DNS abiertos así se magnifican los efectos sobre los dispositivos de destino. Entre los ataques que genera el Spoofing DNS están:

a) DNS ataques de envenenamiento de caché
b) DNS ataques de envenenamiento de caché
c) ataques de utilización de recursos
d) Denegación de servicio (DoS) o distribuidos de denegación de servicio (DDoS)

La implementación de esta variedad de ataques, requieren la utilización de recursos en la resolución de DNS abiertos consumen recursos en el dispositivo. Ejemplos de tales recursos incluyen CPU, la memoria y buffers de los conectores. Este tipo de ataques tratan de consumir todos los recursos disponibles para impactar negativamente en las operaciones de la resolución abierta. El impacto de estos ataques puede requerir que el dispositivo sea reiniciado o un servicio para detener y reiniciar.

Recomendaciones ante el ataque Spoofing o suplantación de DNS

La solución de todo el sistema estándar para las vulnerabilidades DNS es DNSSEC. Sin embargo, hasta que se aplique universalmente, resolución de DNS abiertos deben tomar de forma independiente algunas medidas para mitigar las amenazas conocidas. Se han propuesto muchas técnicas las cuales se han implementado para hacer el DNS más resistente contra respuestas forjadas para una visión general de la mayoría de ellos. Se recomienda, los siguientes enfoques:

I. Asegurar su código contra desbordamientos de *buffer*, en particular el código responsable de analizar y serializar mensajes DNS.

II. Recursos de la máquina de exceso de aprovisionamiento para proteger contra ataques DoS directas en los mismos resolutores. Dado que las direcciones IP son triviales para los atacantes para forjar, es imposible bloquear las consultas basadas en la dirección IP o subred; la única manera efectiva de manejar este tipo de ataques es simplemente para absorber la carga.

III. La implementación básica de la validez de comprobación de los paquetes de respuesta del servidor y de la credibilidad del nombre, son necesarios para proteger contra el envenenamiento de caché sencilla. Estos son mecanismos estándar y la cordura comprueba que cualquier resolución de caché compatible con los estándares se debe realizar.

IV. Adición de entropía de los mensajes de petición, para reducir la probabilidad de más sofisticados ataques de envenenamiento de suplantación de cache. Hay muchas técnicas recomendadas para la adición de la entropía, incluyendo la aleatorización de puertos de origen; aleatorios en la elección de los servidores de nombres (direcciones IP de destino); randomizing caso de las solicitudes de nombres; y añadiendo prefijos nonce para nombrar peticiones. A continuación, damos una visión general de los beneficios, limitaciones y desafíos de cada una de estas técnicas, las cuales pueden ser implementadas:

a) Extracción de consultas duplicadas, para combatir la probabilidad de ataques cibernéticos, como puede ser el *Spoofing DNS*.
b) Limitante de la velocidad de solicitudes, para prevenir ataques DoS y amplificación.
c) Monitorear el servicio para las direcciones IP de los clientes que utilizan el más ancho de banda y que experimentan la proporción de tamaño más alto de respuesta a la solicitud.

Practica del ataque de denegación de servicio o DoS

Además de la IP y filtrado de direcciones hacia las peticiones del DNS, los ataques de Denegación de Servicio se han convertido en una herramienta importante en la denegación de los servicios de red para los usuarios legítimos. Si el atacante utiliza múltiples nodos para realizar un ataque de denegación de servicio, estos ataques se pueden realizar mediante la alteración de los archivos de configuración, componentes de red físicamente dañinos o el consumo de recursos de la red wifi.

El ataque se llevó a cabo de una manera controlada, implementando la conexión de la red Wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, del municipio de Urrao, se ha comprobado que los ataques de Denegación de servicio, requieren enfoques de detección de tráfico de fondo, donde los resultados muestran que los enfoques de detección necesitan ser optimizados para red operativa, teniendo en cuenta los requisitos de utilización de la red y de retardo de detección.

Además de lo anterior, con el ataque de Denegación de servicio, se ha demostrado dos puntos débiles principales. En primer lugar, las direcciones del remitente del paquete de datos (Atacar) han sido falsificadas (*IP Spoofing*), y, en segundo lugar, se han instalado programas no autorizados, los cuales se han ejecutado antes del envió de los ataques hacia los equipos seleccionados, los cuales demostraron que no están protegidos adecuadamente. La característica particular de los ataques *DDoS* es que son capaces de afectar a los que de otra manera se han protegido de forma óptima contra los intrusos de Internet. Esto significa que los equipos en los que no se han aplicado incluso las medidas adecuadas de protección básicas, no sólo son un peligro para la red en cuestión, sino también para los demás dispositivos que están conectados a la red wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, creando varios "agujeros" de seguridad para los usuarios que a diario se conectan de esta red.

Recomendaciones ante el ataque de denegación de servicio o DoS

El medio más exitoso de combatir los ataques de DoS incluiría la aplicación de una serie de técnicas de prevención. Estas prácticas incluyen, pero no se limitan al filtrado estricto de paquetes, la inhabilitación de servicios de red no utilizados, el cambio de dirección IP y la actualización periódica de software en servidores. El cambio de dirección IP hace que el atacante exitoso tenga que modificar su ataque siempre que el destinatario cambie su dirección. La actualización regular del software eliminará muchos de los bugs que los atacantes pueden explotar al montar un ataque. Estas dos prácticas no solo, harán un cambio significativo en la amenaza de un ataque. Los atacantes pueden automatizar la actualización de los nodos participantes una vez que se publica la nueva dirección IP, y el nuevo software estará siempre en la versión con nuevos errores para explotar.

La implementación de estas prácticas es significativamente menos efectiva si los demás usuarios de la red wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, no lo hacen.

Recomendaciones ante ataques de *Phishing, Man in the middle y ARP Spoofing* (En un solo ejercicio)

Al realizar el ataque de *Phishing*, el cual requiere de la mezcla de los ataques *"Man in the Middle*" y "*ARP Spoofing*", además de la implementación de dispositivos de propiedad del autor, se ha conseguido demostrar que capturar las credenciales de inicio de sesión de los usuarios, que inician sesión en "*Hotmail*", donde las credenciales comprometidas permiten al atacante obtener acceso fraudulento a su cuenta de correo electrónico y a los recursos, que dependen de la información que esté contenida allí, además de ser muy probable que las mismas credenciales se pueden utilizar para iniciar la sesión en otros sistemas a nombre del usuario implicado. Esto puede resultar en una violación de datos que tiene un impacto significativo en la red wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, del municipio de Urrao.

Cabe recordar que los ataques de robo de credenciales tienden a pasar por alto el software tradicional de seguridad de las tecnologías de la información y las comunicaciones. Pero los ataques son complejos y conllevan múltiples pasos. Por lo tanto, los administradores del servicio de internet gratis en el parque, deben contratar personal especializado que sea capaz de detectarlos en sus procesos, y responder con rapidez y eficacia suficiente para detener los atacantes y

restablecer la seguridad, es esencial para la seguridad de red wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe.

Recomendaciones ante los ataques de *Phishing, Man in the middle y ARP Spoofing*

Hay varias cosas que se pueden hacer para reducir el riesgo de robo de credenciales dentro de la utilización de los recursos de internet en la red wifi. En primer lugar, no se debe iniciar sesión en aplicaciones sensibles de los dispositivos que no estén protegidos; además de asegurarse de que el antivirus está actualizado y, si es posible, utilizar soluciones de seguridad especiales diseñados para bloquear el *malware* que roba información para proteger su equipo.

Se recomienda cambiar las contraseñas a menudo, donde es necesario utilizar contraseñas complejas y no utilice las mismas credenciales a través de múltiples sistemas. Para los sistemas que son especialmente críticos para el usuario, considere el uso de la autenticación de dos factores. Esto añade requisitos adicionales de información de usuario al iniciar la sesión y por lo tanto es más difícil de poner en peligro.

Nota: Estos Ataques se han realizado de una manera controlada, sobre equipos de propiedad del autor, los cuales se han utilizado para medir la seguridad de la red wifi "**IDEA internet en el parque**" de la plaza Rafael Uribe Uribe, del municipio de Urrao; además de garantizar que no se ha incumplido con las leyes que protegen la seguridad de las tecnologías de la información y las comunicaciones, donde su finalidad primordial es netamente educativo.

4.3 RECOMENDACIONES GENERALES PARA LOS USUARIOS QUE SE CONECTAN A LA RED WIFI "IDEA INTERNET EN EL PARQUE", DE LA PLAZA RAFAEL URIBE URIBE DEL MUNICIPIO DE URRAO"

Según el análisis de los diferentes ataques, las recomendaciones y consejos útiles, los cuales pueden servir, para que los usuarios de la red wifi "**IDEA internet en el parque**", de la plaza Rafael Uribe Uribe, del municipio de Urrao, para que puedan disfrutar del servicio, por medio de una conexión segura, son las siguientes:

4.3.1 La configuración

En primer lugar, se debe iniciar por realizarle los ajustes del sistema y de las aplicaciones, para mantenerlas a salvo; además de asegurarse de que éstos estén activados en cualquier momento y más que todo cuando estás conectado en una red wifi pública, así sea protegida o no con contraseña; además de si hay conectadas en la misma red, otras personas que no conoces.

4.3.2 Desactivar el uso compartido

Cuando estén en el hogar, es posible compartir archivos, impresoras, o incluso permitir el acceso remoto de otros dispositivos hacia la red. Es diferente cuando hay conexión hacia una red pública, donde es necesario excluirlas, debido a que cualesquiera, puede acceder a ellos, ni siquiera tienen que ser un hacker, y dependiendo de su configuración, probablemente resulten generando vulnerabilidades, debido a que no es protegido por contraseña. Para desactivar el uso compartido, se procede de la siguiente manera:

- ✓ **Windows 7**: Abra el Panel de control, a continuación, vaya a Redes e Internet> Centro de redes y recursos compartidos, haga clic en Elegir Cambiar configuración de uso compartido avanzado. Una vez aquí, debería desactivar compartir archivos e impresoras, y usted también puede desactivar la detección de redes y el uso compartido de carpetas públicas. Algo de esto se realiza automáticamente por Windows si se especifica la red como pública.
- ✓ **Windows 8**: Ir a Panel de control> Redes e Internet> Ver estado de la red y las tareas> Cambiar la configuración de uso compartido avanzado>

Desactivar compartir archivos e impresoras y detección de redes> Guardar cambios.

- ✓ **Windows 10**: Haga clic en el icono de Windows> Configuración> Redes e Internet> Wifi> Desplácese hasta avanzada compartir ajustes Desconectar compartir archivos e impresoras y detección de redes> Guardar cambios.
- ✓ **Sistemas operativos OS X**: Ir a Preferencias del Sistema> Compartir y asegúrese de que todas las casillas estén marcadas. También se recomienda desactivar la detección de redes, que se encuentran en el mismo lugar. Esto evitará que otros ni siquiera ver a su equipo en la red, lo que significa que es menos probable de ser blanco de un ataque, debido a que permanece en modo oculto y estar bajo la configuración avanzada del servidor de seguridad.

4.3.3 Habilitar el servidor de seguridad

La mayoría de los sistemas operativos vienen con al menos un firewall básico hoy en día, y es un paso sencillo para mantener a los usuarios locales no deseados de esculcar en su ordenador. Es posible que ya esté utilizando un servidor de seguridad, pero por si acaso, entrar en la configuración de seguridad.

En Windows en el Panel de *control> Sistema y seguridad> Firewall de Windows*, y en un Mac bajo Preferencias del sistema> Seguridad y Privacidad> Firewall. Hay que asegurarse de que su firewall está activado; donde también se puede editar las aplicaciones que tienen permiso para acceder haciendo clic en (**Permitir que un programa o característica**) de Windows y (**Avanzado**) en OS X. El servidor de seguridad no les pondrá fin a todos los problemas de seguridad, pero siempre es una buena idea asegúrese de que esté habilitado el servidor de seguridad del sistema.

4.3.4 Desactivar Wifi cuando no lo esté utilizando

Para garantizar la seguridad de su información, se recomienda apagar su red Wifi. Esto es muy fácil, tanto en *Windows y OS* X u otros sistemas operativos. En Windows, puede simplemente con hacer clic en el icono de red inalámbrica en la barra de tareas para apagarlo. En un Mac, basta con hacer clic en el icono Wifi en la barra de menú y seleccione la opción a su vez fuera del aeropuerto. Una vez más, esto no es del todo útil si necesitas internet, pero cuando no se está utilizando activamente, no es una mala idea simplemente apagarla por el

momento. Cuanto más tiempo permanezca conectado, le brindas la posibilidad a un atacante para empezar a husmear.

4.3.5 Automatizar la configuración de la seguridad Wifi Pública

Se recomienda ajustar manualmente todos estos ajustes cada vez que vaya de ida y vuelta hacia la plaza Rafael Uribe Uribe y la red doméstica segura. Afortunadamente, hay algunas maneras de automatizar el proceso para que pueda obtener de forma automática una protección adicional cuando se conecta a una red Wifi pública.

4.3.6 Sistemas Windows

Al conectarse por primera vez a cualquier red en Windows, el sistema le preguntará si se va a conectar a una red en su hogar, de trabajo o si es público, donde cada una de estas opciones va a ejecutar el cambio de una lista preestablecida de configuraciones que el usuario ostente. El lugar público, como es natural, le dará la mayoría de la seguridad; además de que puede personalizar los pre ajustes, lo que implica la apertura de su panel de control y navegación, que lo dirige hacia el centro de redes y recursos compartidos> Configuración de uso compartido avanzado. A partir de ahí, puede activar la detección de redes, el intercambio de archivos, uso compartido de carpetas públicas, medios de transmisión, y otras opciones dentro o fuera de los diferentes perfiles.

4.3.7 En sistemas OS X

En los sistemas operativos OS X no tiene estas opciones integradas como Windows, pero una aplicación como ControlPlane puede hacer una buena cantidad de personalización. Con él, usted puede encender el servidor de seguridad, desactivar el uso compartido, conectarse a una VPN, y mucho más, todo en función de la red a la que ha hecho la conexión.

4.3.8 En el navegador

HTTPS Everywhere extensión para Firefox elige automáticamente la opción segura HTTPS para un montón de sitios web más populares, incluyendo *Twitter, Facebook, Google*, entre otros más, asegurando conexiones HTTPS seguras a cualquier sitio web compatible, cada vez que sea visitado por el usuario. El usuario

puede incluso añadir su propia para su archivo de configuración XML. Se debe tener en cuenta que, como una extensión de *Firefox*, esto funciona en *Windows*, *Mac y Linux*; permitiendo una mayor seguridad mientras se visitan ciertos sitios web.

4.3.9 Olvidar la configuración de conexión de red

Una vez que el usuario termine la navegación por la web, hay que asegurarse de cerrar la sesión en los servicios que se firmaron. A continuación, informe a su dispositivo para que se olvide de la configuración de la red wifi. Esto significa que el teléfono, el computador o el dispositivo, no se conecte automáticamente de nuevo a la red si usted está en el rango de la señal, sin que el usuario se dé cuenta.

En Windows, puede desmarcar la opción "Conectar automáticamente" casilla de verificación al lado del nombre de la red antes de conectar, o dirigirse al Panel de control> Centro de redes y recursos compartidos y haga clic en el nombre de la red. Haga clic en "Propiedades inalámbricas" y luego desactive la casilla "Conectar automáticamente si esta red está en rango."

4.3.10 En sistemas OS X

Para olvidar la conexión automática de una red Wifi, evitando que el Mac se una automáticamente de nuevo cuando el usuario este dentro del rango de la señal, se debe proceder con los siguientes pasos:

a. Despliegue el icono del menú Wifi y elegir la opción "Abrir preferencias de red", o ir al panel de preferencias "red" de menú *Apple* y Preferencias del Sistema
b. Seleccione "Wifi" de la barra lateral del panel de red, a continuación, haga clic en el botón "Opciones avanzadas" en la esquina
c. Ir a la pestaña "Wifi" y encontrar el enrutador / red de olvidar en la lista de "proveedores preferidos"
d. Seleccione la red y luego elegir el botón negativo para eliminar (no recuerdo) de la red inalámbrica
e. Confirmar olvidar la red wifi seleccionando "Eliminar"
f. Repita según sea necesario para otras redes wifi para olvidar

g. Haga clic en "Aceptar", a continuación, salir de Preferencias del sistema, seleccione "Aplicar" si se le pide.

Una vez que una red inalámbrica se ha olvidado, OS X ya no conecte automáticamente, incluso si es la única red wifi que hay disponible.

4.3.11 En sistemas Android

Para eliminar una red Wifi guardada desde su teléfono o *Tablet,* todo lo que tiene que hacer es ir a la sección de conexiones inalámbricas y redes, se ingresa a la sesión wifi y selecciona y luego se da olvidar. En algunos dispositivos Android, también hay una opción de modificar, que en su mayoría es una buena manera de cambiar la contraseña Wifi guardado en el dispositivo, este aspecto se relaciona según sea la versión que este instalada.

4.3.12 Confirmar el nombre de la red

En ocasiones, los hackers crean y configuran una red Wifi falsa para atraer a los usuarios involuntarios en las redes wifi públicas. La conexión a una red falsa podría poner el dispositivo en las manos de un atacante y poner en riesgo la seguridad de los datos en cuestión. Si no está seguro de si se está conectando a la red legitima del lugar, pregunte a las autoridades que están ubicadas en los “CAI” de la Policía del lugar.

4.3.13 Proteja sus contraseñas

Uso de contraseñas únicas para diferentes cuentas pueden ayudar si uno de sus cuentas está comprometido. Hacer un seguimiento de múltiples contraseñas seguras puede ser complicado, así que usar un gestor de contraseñas como los son:

- ✓ *KeePassX* | *Linux, OS X, Windows*
- ✓ *LastPass* | *Linux, OS X, Windows, iOS, Android*
- ✓ *KeePassX* | *Linux, OS X, Windows*
- ✓ *DashLane* | *OS X, Windows, iOS, Android*

Estos gestores de contraseñas, pueden ayudar a mantener a salvo y seguro loas datos de los usuarios.

4.3.14 No realizar consultas en banca en línea y otras transacciones.

La banca en línea viene con su propio conjunto de riesgos, pero esos riesgos a menudo tienen menos que ver con la tecnología que con los usuarios utilizan. Por ello no es recomendable que realice consultas en línea y más que todo si está conectado a una red wifi pública. Tomar medidas para proteger sus cuentas mientras se asegura de que su banco utiliza la tecnología de seguridad estándar de la industria.

4.3.15 Utilice una cuenta de invitado al conectarse a redes públicas

Si utiliza *Windows 10* o cualesquiera otras versiones anteriores de *Windows*, que posiblemente puede utilizar una cuenta de invitado en la conexión a Wifi pública para una mejor protección de línea.

4.3.16 Lea los términos y condiciones cuidadosamente

Cuando se conecte a una red de Internet gratis, evite hacer clic a través de cualquier link o propaganda publicitaria que lo saque o desvié de la web que está visitando, lo que implica tener mucho cuidado a la hora de comprobar lo que está aceptando o firmando. Una gran parte de las redes Wifi son instaladas en lugares públicos por parte de los proveedores de comercialización que están dispuestos a darle un poco de ancho de banda a cambio de un número de dirección de correo electrónico, datos personales, entre otros más.

4.3.17 Evitar el acceso a la información sensible

Por lo general, las redes Wifi públicas no deben ser utilizados para acceder al correo electrónico, cuentas bancarias y tarjetas de crédito en línea, o cualquier otra información confidencial de la materia. Se recomienda esperar que llegue a su hogar u oficina, donde dispone de internet ofrecido por un proveedor de este tipo de redes, entregado con un router, el cual viene configurado con contraseña y protegida por un cortafuego, de este modo puede tener una mejor seguridad.

4.4 RECOMENDACIONES TÉCNICAS DE CONFIGURACIÓN DE UNA RED WIFI PARA UNA MAYOR SEGURIDAD

Al realizar los tres ataques cibernéticos controlados y verificando su respectivo análisis, se ha concluido que a pesar de que los dispositivos inalámbricos vienen con una configuración de seguridad determinada de fábrica, esta no es lo suficientemente fuerte, debido a que los atacantes ya conocen las vulnerabilidades que han sido explotadas en dichos equipos, bien sea por parte del software, mala configuración, instalación de software infectado ó código malicioso.

A pesar de los riesgos, las opciones de defensa existentes son eficaces en la mitigación de amenazas por parte de la mayoría de las fuentes que brindan el servicio y los usuarios que se conectan a las redes wifi públicas. Sin embargo, los usuarios de una red wifi publica, debe decidir si el costo de la defensa es más que el costo esperado debido a la pérdida que le puede ocasionar el no saber qué seguridad brinda la red inalámbrica.

4.4.1 Proteger el punto de acceso

La mayoría de los puntos de acceso se configuran con la seguridad desactivada, una contraseña de administrador por defecto y un ID de conjunto de servicios (SSID) predeterminado para la red Wifi, donde los usuarios normalmente no cambian estos valores predeterminados. Esta combinación permite que los hackers secuestren fácilmente la red inalámbrica y, posiblemente, a tener acceso a la administración del punto de acceso también. Con el fin de proteger el punto de acceso, las siguientes acciones deben ser tenidas en cuenta por los administradores del punto de acceso Wifi "**IDEA internet en el parque**", del municipio de Urrao:

a) Requerir una contraseña de administrador para gestionar el acceso al punto de cobertura de la señal.
b) Cambiar la contraseña de administrador de forma regular.
c) Cambiar el SSID por defecto a algo inocuo (Es decir, algo que no identifica a la marca y modelo del punto de acceso o el nombre de la red Wifi).
d) Si es posible, configurar el punto de acceso para que no difunda su SSID.
e) Cambie las claves de cifrado sobre una base mensual o anual y elegir una clave más larga.

4.4.2 Habilitar la autenticación y el cifrado a través del canal inalámbrico

A menos que los protocolos de autenticación y cifrado que se utilizan en la red Wifi "**IDEA internet en el parque**", del municipio de Urrao, sean verificados en cuanto al grado de protección que le brindan al usuario, para proteger la integridad de todos los datos transmitidos por la red inalámbrica, donde estos pueden ser monitorizados de forma pasiva. Los protocolos deben ser escogidos con cuidado, ya que no todos los protocolos de autenticación y cifrado son seguros.

4.4.3 Implementación de seguridad con WPA 2

Aunque WPA proporciona una seguridad suficiente para la mayoría de los usuarios, WPA2 es el protocolo oficial de seguridad que implementa el estándar de seguridad 802.11i completa; proporciona una seguridad de nivel empresarial mediante el uso de *Advanced Encryption Standard (AES)* y no es susceptible a un ataque de falsificación de paquetes como sucede con el protocolo WPA.

4.4.4 Utilizar el estándar 802.11i

Los administradores de la red Wifi "**IDEA internet en el parque**", del municipio de Urrao, deben considerar la implementación de soluciones completas tales como el estándar 802.11i con el fin de proteger los datos de los usuarios. 802.11i admite la autenticación mutua, además de proporcionar una mejor encriptación para redes que utilizan el popular 802.11a, 802.11b (Que incluye Wifi) y 802.11g estándares. El estándar 802.11i implementa un nuevo cifrado de claves, conocido como Protocolo de integridad de clave temporal *(TKIP) y Advanced Encryption Standard (AES).*

4.4.5 Autenticación adicional con el cifrado de extremo a extremo

La encriptación y autenticación de protocolos tales como WPA2 y 802.11x, requieren la implementación de las tecnologías asociadas con cifrar y autenticar los datos que viajan a través de la red Wifi "**IDEA internet en el parque**". Sin embargo, si un atacante accede a la red inalámbrica sin autorización y la red inalámbrica se conecta un usuario, los datos confidenciales en la red podrían estar expuestos. Para mitigar esta amenaza, es necesario implementar la autenticación adicional y el cifrado como la proporcionada red privada virtual (de VPN), la cual permite cifrar los datos de extremo a extremo.

4.4.6 Definir y aplicar políticas de seguridad para la red Wifi

Políticas bien definidas pueden restringir o permitir el acceso inalámbrico, se pueden utilizar para reducir la probabilidad de ataques a los datos que viajan a través de la red Wifi "**IDEA internet en el parque**", los usuarios deben tener en cuenta las políticas de seguridad, destinadas para proteger los recursos de las personas no autorizadas. Algunas políticas posibles:

a) **Activar 802.11i cifrado para que los datos sean incoherentes para los usuarios no autorizados**: A diferencia de 802.11a, b y g especificaciones, todas las cuales definen las cuestiones de la capa física, 802.11i define un mecanismo de seguridad que opera entre la subcapa de control de acceso al medio (MAC) y la capa de red. Otro elemento de la 802.11i es robusta seguridad de la red (RSN), que negocia dinámicamente los algoritmos de autenticación y cifrado que se utilizarán para las comunicaciones entre los WAP y los clientes inalámbricos. Esto significa que a medida que las nuevas amenazas que se descubren y se mitigan, se pueden añadir nuevos algoritmos de seguridad.

b) **Utilizar la tecnología virtual basada en *IPsec Private Network (VPN)* para la seguridad de extremo a extremo**: Si los usuarios necesitan acceder a aplicaciones sensibles de los puntos de acceso Wifi, sin duda utilizar un sistema VPN para proporcionar suficiente cifrado y control de acceso de extremo a extremo. Una solución VPN, ofrece una buena seguridad, pero llega a ser costoso y difícil de manejar cuando hay cientos de usuarios conectados a la red (debido principalmente a la necesidad de servidores VPN).

c) **Establecer una red inalámbrica Wifi con servidores por separado**: Un servidor de seguridad, puede ayudar a mantener a los piratas informáticos alejados de la red Wifi, lo que evitara que estos tengan un fácil acceso a los servidores corporativos ubicados en los diferentes sitios de acceso, es decir, que no son accesibles desde la red inalámbrica. De esta manera, la red inalámbrica aplicará mecanismos de cifrado y autenticación para el acceso a la red Wifi "**IDEA internet en el parque**".

d) **Garantizar que el firmware está al día en las tarjetas de cliente y puntos de acceso**: Los vendedores suelen implementar modificaciones del firmware que fijan los problemas de seguridad. De manera continua, lo convierten en un hábito para comprobar que todos los dispositivos inalámbricos tienen las más recientes versiones de firmware, de tal modo que la seguridad se puede certificar.

e) **Garantizar que sólo las personas autorizadas puedan restablecer los puntos de acceso**: Algunos puntos de acceso volverán a los ajustes

predeterminados de fábrica (es decir, no hay seguridad en absoluto) cuando alguien empuja el botón de reinicio en el punto de acceso, de tal modo que los administradores de la red Wifi "**IDEA internet en el parque**", deben proporcionar seguridad física adecuada para el hardware de punto de acceso.

f) **Desactivar los puntos de acceso durante periodos breves**: Si es posible, se deben apagar los puntos de acceso, en periodos breves. Esto limita la ventana de oportunidad para que un atacante pueda aprovechar un punto de acceso a una interfaz débil para ingresar al resto de la red.

g) **Poner en práctica los cortafuegos personales:** Si un atacante es capaz de asociarse con un punto de acceso, que es extremadamente probable si no hay cifrado o autenticación configurado, el atacante puede acceder fácilmente a los archivos guardados en los dispositivos de otros usuarios que están asociados con un punto de acceso en la misma red Wifi. Como resultado de ello, es crucial que todos los usuarios deshabilitar el uso compartido de archivos para todas las carpetas y utilizan los cortafuegos personales.

4.4.7 Utilizar dispositivos que sean fáciles de configurar

Muchos ataques cibernéticos son causados por malas configuraciones. Este es un resultado directo de la dificultad para el usuario medio para configurar sus sistemas correctamente.

4.4.8 Utilizar soluciones de detección de intrusos

Con el fin de detectar la actividad inadecuada o anómala en la red Wifi "**IDEA internet en el parque**", las soluciones de detección de intrusos, se pueden emplear. Hoy en día existen productos de fácil manejo, donde en muchas ocasiones, se puede optar por software libre, el cual cuenta con la mejor herramienta de Pentesting de la actualidad "*Kali Linux*", con muchas herramientas dedicadas a la seguridad y explotación de las redes Wifi.

4.4.9 Educar a los usuarios finales permanentemente

Toda la tecnología disponible es inútil a menos que las empresas que distribuyen los sistemas y sus periféricos comprendan los fundamentos de las medidas de defensa. Además, la educación sobre los procedimientos adecuados para la divulgación y protección de la información sensible, esto hará menos susceptibles

a los ataques a los que se exponen los usuarios de la red Wifi "**IDEA internet en el parque**".

En realidad, la forma en que se puede ayudar a los usuarios, para proteger los datos, es a través de una mejor formación y educación. Los artículos de entrenamiento y recordatorios constantes promoverán los conocimientos de que la Wifi público baje los niveles de riesgos que representa para los usuarios normales. La clave aquí está mostrando a los usuarios de que un poco de molestias a través de capas de SSL o VPN, o esperando para consultar el correo electrónico en una red segura, es la mejor forma de protección de datos. A pesar de que es más de una molestia, evitando estos puntos Wifi públicos, de este modo protegerán mejor su integridad.

4.4.12 Carnadas para confundir a los atacantes

Ciertas opciones de defensa implican carnadas para tentar a los atacantes, para atacar un blanco fácil. De acuerdo con el principio contrario, si dos redes inalámbricas están disponibles y uno parece mucho más fácil de cortar que el otro, es probable que la red inalámbrica sea más segura.

4.4.13 Utilizar honeypot Wifi

Para detectar los posibles atacantes, así como para obtener una visión sobre los nuevos métodos de ataque, los *honeypot* Wifi se pueden emplear. Un honeypot es un sistema informático de señuelo para atrapar a los piratas informáticos o el seguimiento de métodos de piratería no convencionales o nuevas. Honeypot están diseñadas para involucrar a propósito y engañar a los piratas informáticos e identificar actividades maliciosas realizadas a través de Internet.

4.4.14 Utilizar la seguridad HTTPS

Los intentos de leer los datos, a veces pueden ser frustrados por la primera línea de defensa en una red Wifi pública, donde el cifrado del sitio web o del servicio necesitan respaldar los datos de los usuarios. Por ejemplo, cuando se escribe y envía su contraseña a través de una red, no tiene por qué ser, e idealmente no

debe ser, enviado como "Texto sin formato". En su lugar, debe ser encriptado a través de HTTPS o SSL. Lo mismo ocurre con toda la información potencialmente sensible.

Muchos sitios cambiarán automáticamente a HTTPS cuando se visita una página que requiere el intercambio de información potencialmente sensible. Algunos sitios, como Google, Facebook, entre otros, le dan la opción de permanecer en HTTPS en todo momento. Se puede disminuir el riesgo al usar cualquier red pública, asegurándose de que cualquier sitio en el que está introduciendo potencialmente información sensible está asegurado. Por lo general, esto es tan simple como ver el prefijo "https" en la dirección URL. Si estás en una red pública, y el sitio no está asegurado, a continuación, sólo tiene que esperar hasta que esté en casa antes de entrar en cualquier información importante. Aunque HTTPS pueden ser grandes, no depende de la implementación del sitio web, que es algo que no tiene control sobre la seguridad que debe brindarle a los usuarios. Un sitio HTTPS mal diseñada podría tener enormes agujeros de seguridad y nunca es prudente asumir que un sitio tiene una gran seguridad sólo porque es de un nivel público y además de ser gratis.

4.4.14 Usar una VPN

Los administradores de la red Wifi "**IDEA internet en el parque**", puede optar por implementar una red virtual (VPN), brindándoles a los usuarios finales una, conexión segura y cifrada. La seguridad SSL es en realidad un tipo de VPN; sin embargo, se puede optar por establecer una red VPN IPsec, la cual es una aplicación con un nivel de seguridad que es capaz de cifrar el flujo de datos. Además, esta capa de seguridad puede cumplir otras reglas y políticas, la protección de datos adicionales de los usuarios que se conectan a la red Wifi. VPN IPsec puede limitar la división de túnel, asegurar que los programas de seguridad se actualicen, permanezcan encendidos, y activar otros controles de protección de punto final como lo son los cortafuegos.

Una VPN es una gran manera de hacer pública Wifi segura para su uso 100% de las veces. VPN es sinónimo de red privada virtual, y es un método para crear una conexión segura incluso en una red que es público y no garantizado para los usuarios que conocen del tema. En lugar de conectar directamente a Internet, se conecta a un servidor específico, que es a su vez está conectado a Internet. La conexión entre el dispositivo y el servidor está cifrada, por lo que la información que se envíe se encuentre protegida, incluso en redes Wifi no segura.

4.4.15 Mantener el software al día

La seguridad de datos es una carrera de armamentos, y para mantener las defensas, es crucial y vital, la ejecución de las últimas actualizaciones de los sistemas operativos y los navegadores. No existe una fórmula mágica para la seguridad de los datos. Mientras que los propietarios de sitios y los minoristas deben dar un paso claramente su juego en la protección de nuestra privacidad, también tenemos que hacer nuestra parte en la eliminación de al menos de uno de los puntos débiles para los hackers. Afortunadamente, con un poco de conciencia, y estos sencillos pasos, se proteger sus datos y aun así disfrutar de la comodidad del Wifi público.

4.4.16 Sistema de prevención de intrusiones inalámbricas (WIPS)

Tener una capa de seguridad complementaria en forma de un WIPS para obtener esta visibilidad puede ser muy útil dentro de la red Wifi "**IDEA internet en el parque**", además de sus capacidades, un WIPS puede utilizarse para bloquear las amenazas relacionadas con el cliente Wifi y prohibir el uso de determinados tipos de dispositivos Wifi (*WiFi pineapple*). El WIPS actúa como una capa complementaria, siempre y cuando un cliente Wifi dentro de la cobertura de la red pública o la distancia de acceso Wifi, tiene que depender de agentes de punto final.

4.4.17 Habilitar el aislamiento del cliente SSID pública

Esta suele ser una casilla de verificación, ya sea "Aislamiento del cliente" o "Aislamiento de la estación" que, cuando está activado, evita que los clientes en el mismo AP de intercomunicación. Algunos puntos de acceso también tienen una función de "Aislamiento", que evita que los clientes que están ubicados en diferentes puntos de acceso (pero con el mismo SSID) de intercomunicación, no pueden interceptar los datos de los demás usuarios. Si el punto de acceso de la red Wifi tiene esa característica, lo utilizan. Si no es así, no hay que preocuparse, porque este nivel de protección también se puede implementar en los puntos de acceso de la red Wifi "**IDEA internet en el parque**".

4.4.18 Instalar y utilizar software antivirus y antispyware

La instalación de un programa antivirus y antispyware software y mantenerla al día es un paso crítico en la protección de su dispositivo. Existen muchos tipos de software antivirus y antispyware pueden detectar la posible presencia de malware mediante la búsqueda de patrones en los archivos o la memoria de sus

dispositivos. Este software utiliza las firmas de virus proporcionados por proveedores de software en busca de *malware*. Fabricantes de antivirus con frecuencia crean nuevas firmas para mantener su software eficaz contra el malware recién descubierto. Muchos programas antivirus y antispyware ofrecen actualizaciones automáticas. Habilitar esta característica para que su software siempre tenga las firmas más actuales. Si las actualizaciones automáticas no se ofrecen, asegúrese de instalar el software de una fuente confiable, como el sitio web oficial del proveedor.

Aunque el software anti virus es mucho mejor para detectar el software espía que por desgracia no detecta todos los programas espía, debido a que los hackers cada día se actualizan y emplean ataques más sofisticados. Por esta razón, es crucial para ayudar a asegurar su red Wifi para tener un software anti-spyware instalado en su ordenador. Es bueno saber que no es 100% segura y de buena reputación libre de software anti-spyware disponible para su descarga en línea.

4.4.19 Activar y configurar un servidor de seguridad

El firewall es un dispositivo que controla el flujo de información entre el ordenador e Internet, similar a un router. La mayoría de los sistemas operativos modernos incluyen un firewall de software. Además de servidor de seguridad del sistema operativo.

4.4.20 Modificar las características predeterminadas innecesarias

La eliminación de software innecesario y deshabilitar los servicios no esenciales, donde la modificación de las características predeterminadas innecesarios elimina oportunidades para los atacantes. Revisar las características que venía habilitadas de forma predeterminada en el equipo y desactivar o personalizar los que no es necesario o planea usar. Al igual que con los servicios no esenciales, asegúrese de investigar estas características antes de inhabilitar o modificarlas.

4.4.21 Eliminar software innecesario

Los atacantes pueden arremeter su dispositivo mediante la explotación de vulnerabilidades de software, es decir, defectos o debilidades, que se encuentran en las aplicaciones, configuraciones, parches de seguridad, entre otros; por lo menos el software que se ha desinstalado, crea menos vías para un posible

ataque potencial. Compruebe el software instalado en el equipo, donde si usted no sabe lo que hace un programa de software y no lo usa, debe acudir a la investigación o a la opinión de personal especializado con el tema, para determinar si es necesario.

4.4.23 Obtener una herramienta de análisis y configurarla correctamente

Con el fin de combatir las redes WLAN sin escrúpulos, se recomienda utilizar un escáner inalámbrico o sistema de detección y prevención de intrusiones inalámbricas (IDS / IPS). Donde los administradores de la red Wifi deben asegurarse de que las herramientas de exploración son utilizadas por muchas organizaciones para brindar mayor seguridad a sus usuarios. Se Recomienda tecnologías de análisis e IDS inalámbricos como de *Fluke Networks AirMagnet, Short*, entre otras.

Una vez que se ha seleccionado una herramienta de análisis, es el momento para la aplicar la configuración del dispositivo de lectura inalámbrico, los cuales no son excesivamente complejos, pero es importante tener en cuenta la gestión de registro de la herramienta y funciones de alerta. Debe habilitar las alertas automáticas y un mecanismo de contención para eliminar los puntos inalámbricos sin escrúpulos.

4.4.24 Decidir dónde escanear

Puesto que un dispositivo no autorizado puede mostrar potencialmente en cualquier parte de la señal de la red Wifi, es importante que se preste atención a dónde va a escanear. De acuerdo con la norma PCI DSS, los lugares que almacenan, procesan o transmiten datos de titulares de tarjetas de bancos, son escaneados con regularidad, por ello, los IDS / IPS inalámbrico deben ser empleados en esos lugares. Se le mostrará cómo los datos de la tarjeta se mueven dentro de su entorno y ayudarle a analizar exactamente qué partes debe escanear con base en los lugares que almacenan, procesan o transmiten datos de titulares de tarjetas.

4.4.25 Verificar el estado del dispositivo antes de acceder a la red

Los dispositivos utilizados para acceder a otras redes inalámbricas tienen el potencial de haber estado expuesto a virus, malware o cualquier otro código malicioso. Esto presenta un riesgo de seguridad ya que estos dispositivos sin

darse cuenta podrían estar infectando a otros dispositivos en redes inalámbricas, aprovechando el acceso legítimo de un usuario para robar información confidencial o afectar la disponibilidad de la red Wifi. Entre las principales medidas que se pueden utilizar para ayudar en los dispositivos que se conectan a redes WiFi, incluyen:

- ✓ Utilizar la última versión del sistema operativo y de las aplicaciones
- ✓ Aplicar los últimos parches de seguridad para el sistema operativo y las aplicaciones
- ✓ El uso de un producto de seguridad anti virus o de Internet con archivos de base de firmas, hasta la fecha actual.
- ✓ Usar cortafuegos personales que proporciona tanto el filtrado del tráfico entrante y saliente de la eliminación de todas las aplicaciones no autorizadas
- ✓ Tener listas blancas de aplicaciones para asegurar que sólo se ejecutan las que han sido aprobadas por el usuario, donde por lo general se utilizan en lugar de las cuentas de administrador
- ✓ Usar contraseñas seguras para las cuentas de usuario que se cambian de forma regular
- ✓ Desactivar las funciones de intercambio de archivos.
- ✓ Los dispositivos deben ser validados como seguro a través del uso de control de acceso a la red antes de conceder el acceso a las redes inalámbricas.
- ✓ Con el control de acceso a la red Wifi, los administradores de sistemas pueden establecer políticas para las necesidades de mantenimiento del sistema. Esto puede incluir una comprobación de que todos los parches del sistema operativo están al día, un programa antivirus está instalado y todas las firmas están al día, y que un firewall de software está instalado y se está utilizando. Los dispositivos que cumplen con todos los requisitos de la salud pueden tener acceso a las redes inalámbricas mientras que los dispositivos que no son saludables pueden ser puestos en cuarentena o permitirse el acceso limitado.
- ✓ Credenciales almacenadas en los dispositivos que acceden a redes inalámbricas deben ser protegidos mediante la aplicación de cifrado de disco completo. Esto también protege la información que un usuario puede haber descargado a su dispositivo cuando se accede a la red Wifi “**IDEA internet en el parque**”, y cualquier otra red inalámbrica o fija que se conecten.

4.4.26 Uso de un cortafuegos o Firewall

Utilizar un cortafuego que permita controlar el tráfico que pasa a través de sus puertos de red, si se trata de entrar en o salir. El software actúa como un guardián y le permite decidir qué programas llegar a enviar y recibir información. Un firewall bloquea el acceso no autorizado a su equipo al tiempo que permite el acceso a Internet. Windows viene con un *firewall* incorporado, el cual está activado en *Windows* 7, por defecto.

4.4.27 Uso Anti-Malware

Posiblemente la forma más fácil para que un *Hacker* pueda colarse en su sistema, es mediante el uso de las instalaciones de software maliciosos autorizadas o no autorizadas por el usuario ingenuo. En algunos casos, el usuario no necesita ni siquiera para autorizar nada, ya que los programas espías, se instalan automáticamente y tan pronto como el usuario abre un archivo o una secuencia de comandos permite ejecutar de un sitio web que no está solicitando. El software *anti-malware* puede proteger sus datos mediante la detección de la actividad maliciosa en su equipo y la prevención de una infección.

4.4.28 Cifrar los datos confidenciales

Al almacenar datos sensibles en su disco duro o en un dispositivo de almacenamiento externo cifrarlo. De esta manera es de difícil acceso, incluso si un hacker logra acceder a la computadora y se las arregla para copiar los datos, estos pueden estar a salvo por medio del cifrado. Se puede optar por software de pago o de software libre.

4.4.29 Software de bloqueo de software espía

El *spyware* es un programa que recopila en secreto la información sobre los usuarios. En general, el software espía no es peligroso, aunque algunos programas espía contiene virus y otros programas maliciosos. Los antivirus identifican el software espía que está en la computadora, este indica el nivel de amenaza que plantea el software espía, y le da la oportunidad de eliminar el software espía.

5. CONCLUSIONES

a. Se concluyó con el desarrollo del proyecto, que los usuarios de la red wifi "**IDEA internet en el parque**" del municipio de urrao, están expuestos a ataques de *Spoofing* o suplantación de DNS, ataque de denegación de servicio o *DoS*, ataques de *Phishing, Man in the middle y ARP Spoofing*; poniendo en riesgo los datos, la información sensible y la privacidad de los usuarios.

b. Es necesario que los usuarios de las redes wifi públicas, sean educados en la configuración correcta de los dispositivos y la aceptación de las recomendaciones de seguridad, a la hora de conectarse a redes públicas; para entender la importancia de la ciberseguridad; lo que requiere la implementación de las recomendaciones simples, que se discute en este documento, las cuales pueden ayudad a mitigar amenazas tales como los ataques de *Spoofing o suplantación de DNS*, ataque de denegación de servicio o *DoS*, *ataques de Phishing, Man in the middle y ARP Spoofing*, cuya finalidad, es la construcción de una caja fuerte y resistente ante dichos ataques.

c. Se ha demostrado con el desarrollo del proyecto, que, debido al deseo de una continua conectividad a Internet, los usuarios a menudo descuidan la seguridad a favor de una conexión wifi gratuita. Esto a menudo significa conectarse a redes inalámbricas no seguras y no confiables. Aún peor, una vez conectados a estas redes no seguras, los usuarios a menudo no toman medidas para protegerse. En el proyecto, se demostró con varias pruebas técnicas, cuya finalidad, expuso que los ataques de Spoofing o suplantación de DNS, ataque de denegación de servicio o *DoS*, ataques de *Phishing, Man in the middle y ARP Spoofing*; se ejecutan fácilmente, contra el usuario común que se conecta a redes inalámbricas no seguras y no confiables.

6. BIBLIOGRAFÍA

AGUDO, Sergio. 2015. 7 peligros por los que evitar redes Wifi gratis. [En línea] 10 de 11 de 2015. http://www.malavida.com/es/listas/7-peligros-por-los-que-evitar-redes-wifi-gratis-005734.

ALCALDÍA DE BOGOTÁ. 2009. LEY 1341 DE 2009. [En línea] 30 de 7 de 2009. [Citado el: 20 de 9 de 2016.] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913.

ANABALÓN P, CANALES J, CASTRO C. 2005. Trabajo de Investigación "Redes Inalámbricas". [En línea] 6 de 6 de 2005. [Citado el: 22 de 9 de 2016.] http://docplayer.es/6315343-Trabajo-de-investigacion-redes-inalambricas.html.

ANÓNIMO. 2014. Hackers usaron por años Wifi de hoteles para atacar a huéspedes. [En línea] 13 de 11 de 2014. [Citado el: 25 de 9 de 2016.] http://elcomercio.pe/tecnologia/actualidad/hackers-usaron-anos-wifi-hoteles-atacar-huespedes-noticia-1771074.

ARANDA, Dr.Juan José. 2007. Seguridad Informática Unidad 1 - Principios de la seguridad Informática. [En línea] 2007. [Citado el: 28 de 9 de 2016.] http://slideplayer.es/slide/2261933/.

ARIZA, Diego. 2012. Cuidado con la seguridad de las redes WIFi en los hoteles. [En línea] 12 de 8 de 2012. [Citado el: 28 de 9 de 2016.] http://diegoariza.com/cuidado-con-la-seguridad-de-las-redes-wifi-en-los-hoteles.

ASHTON, Leslie. 2015. Advierten sobre los riesgos de conectarse a una red Wi-Fi pública. [En línea] 04 de 02 de 2015. http://www.clarin.com/sociedad/advierten-riesgos-conectarse-red-Wi-Fi-publica_0_1297670496.html.

BANQUELLS PÉREZ, Nora. 2015. Cómo navegar de forma segura en redes Wi-Fi públicas. [En línea] 31 de 8 de 2015. http://www.opera.com/blogs/la-spain/2015/08/como-navegar-de-forma-segura-en-redes-wi-fi-publicas/.

BITENDIAN. 2016. ¿Qué es el man-in-the-middle? [En línea] 16 de 3 de 2016. [Citado el: 28 de 9 de 2016.] http://www.bitendian.com/es/que-es-el-man-in-the-middle/.

CARDENAL, Juan Pablo. 2013. Ciber espionaje, piratas y mafias en la Red. [En línea] 19 de 2 de 2013. [Citado el: 25 de 9 de 2016.] http://elpais.com/elpais/2013/02/19/eps/1361281322_025092.html.

CISCO NETWORKING ACADEMY. 2015. Seguridad de la red. [En línea] 2015. [Citado el: 28 de 9 de 2016.] http://docplayer.es/505250-Seguridad-de-la-red-redes-de-area-ampliada-wan-capitulo-4-ite-pc-v4-0-chapter-1-2007-cisco-systems-inc-all-rights-reserved.html.

CÓRDOBA MORÁN, Ana Karen. 2013. Seguridad en la red. [En línea] 31 de 5 de 2013. [Citado el: 28 de 9 de 2016.] http://es.slideshare.net/AnaKarenCordovaMoran/seguridad-en-la-red-22235372.

DE LUZ, Sergio. 2015. Conoce la última vulnerabilidad en redes Wi-Fi 802.11n sin contraseña (abiertas). [En línea] 5 de 7 de 2015. http://www.redeszone.net/2015/07/05/conoce-la-ultima-vulnerabilidad-en-redes-wi-fi-802-11n-sin-contrasena-abiertas/.

DIARIO LIBRE. 2014. Ataques "phishing" desviaron más de RD$120 millones de bancos. [En línea] 12 de 2 de 2014. [Citado el: 28 de 9 de 2016.] http://www.diariolibre.com/noticias/ataques-phishing-desviaron-ms-de-rd120-millones-de-bancos-GLdl478961.

GANDINI, Isabella. ISAZA, Andrés y DELGADO Alejandro. 2009. [En línea] 2009. [Citado el: 20 de 9 de 2016.] http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia.

GARCÍA FRÍAS, Antonio. 2014. CONÉCTATE DE FORMA SEGURA A REDES WIFI PÚBLICAS CON ESTOS CONSEJOS. [En línea] 22 de 7 de 2014. [Citado el: 28 de 9 de 2016.] http://cincodias.com/cincodias/2014/07/21/lifestyle/1405950095_577871.html.

GUTIERREZ, Robert Puican. 2013. Clase práctica seguridad escaneo con nmap pdf. [En línea] 1 de 7 de 2013. [Citado el: 28 de 9 de 2016.] http://es.slideshare.net/RobertPuicanGutierrez/clase-practica-seguridad-escaneo-con-nma-pf-23733850.

HERRANZ, Gorka. 2016. El riesgo de los puntos públicos. [En línea] 18 de 5 de 2016. [Citado el: 28 de 9 de 2016.] https://neupic.com/articles/redes-wi-fi.

J., AJALA. 2012. Amenazas en la comunicación inalámbrica. [En línea] 6 de 3 de 2012. [Citado el: 28 de 9 de 2016.] http://www.slideshare.net/ajal4u/ajal-jamming.

JH, NET-SECURITY. 2015. Experimento global expone peligros en uso de puntos de acceso Wi-Fi. [En línea] 4 de 3 de 2015. [Citado el: 2016 de 9 de 25.] http://www.seguridad.unam.mx/noticia/?noti=2155.

LAB, KASPERKY. 2016. Riesgos de las redes WiFi públicas y por qué no debes temerlas. [En línea] 2016. [Citado el: 25 de 9 de 2016.] http://www.kaspersky.es/internet-security-center/internet-safety/public-wifi-risks.

MARA. 2013. Ataques por fuerza bruta. [En línea] 1 de 1 de 2013. [Citado el: 28 de 9 de 2016.] http://ensaladadebits.blogspot.com.co/2013/01/4-ataques-por-fuerza-bruta.html.

MARTÍNEZ RAMÍREZ, Jesús y DÍAZ, José Vicente. 2012. Las redes inalámbricas, más ventajas que desventajas. [En línea] 12 de 2012. [Citado el: 25 de 9 de 2016.]

MARTÍNEZ, Dany. 2010. Tipos de ataques Denial-of-Service. [En línea] 15 de 9 de 2010. [Citado el: 28 de 9 de 2016.] https://dan1t0.wordpress.com/2010/09/15/tipos-de-ataques-denial-of-service/.

NORIEGA, Samuel. 2014. Riesgos al Utilizar Redes WI-FI Gratuitas. [En línea] 2014. https://www.certstopshop.com/blog/riesgos-al-utilizar-redes-wi-fi-gratuitas.

OLEA, Izabelle. 2015. REDES INALÁMBRICAS Máster de Ingeniería de Computadores-DISCA Redes Inalámbricas – Tema 7. Seguridad. [En línea] 2015. [Citado el: 28 de 9 de 2016.] http://slideplayer.es/slide/4134240/.

PÉREZ VALENZUELA, Oscar Eduardo. 2016. Formas seguras de usar una red wi-fi pública. [En línea] 27 de 7 de 2016. [Citado el: 24 de 9 de 2016.] http://www.arcsoftware.com.co/index.php/actualidad-tecnologica/109-seguridad-red-wifi-publica.

PORTELLES, Rubén. 2012. ESET publica su Guía de Seguridad para Redes Inalámbricas. [En línea] 20 de 8 de 2012. [Citado el: 28 de 9 de 2016.] http://www.tecnovirus.com/blog/eset-publica-su-guia-de-seguridad-para-redes-inalambricas/.

RODRÍGUEZ MOSQUERA, Eva. 2015. Los peligros de las redes Wifi públicas. [En línea] 20 de 10 de 2015. http://www.elmundo.es/tecnologia/2015/10/20/56265c73268e3ec1428b45dd.html.

RODRÍGUEZ, Juan. 2010. ¿Que es un ataque DNS Poisoning Attack? (envenenamiento de DNS). [En línea] 3 de 11 de 2010. [Citado el: 28 de 9 de 2016.] http://es.paperblog.com/que-es-un-ataque-dns-poisoning-attack-envenenamiento-de-dns-325753/.

ROJAS, Zordan. 2015. Conectarse a una red wifi pública esconde grandes riesgos. [En línea] 2 de 1 de 2015. [Citado el: 28 de 9 de 2016.] http://diario.elmercurio.com/detalle/index.asp?id={6c20f8db-6417-490a-b39c-830e29ad714e}.

SEGURITY, PANDA. 2015. ¿Cuánto cuesta robar tus datos en una wifi pública? 70€. [En línea] 9 de 4 de 2015. [Citado el: 28 de 9 de 2016.] http://www.pandasecurity.com/spain/mediacenter/seguridad/cuanto-cuesta-robar-tus-datos-en-una-wifi-publica-70e/.

SORY FANTA, Keita y BALUJA GARCÍA, Walter. 2011. Vulnerabilidades en el formato y uso de la trama 802.11. [En línea] 9 de 2011. http://revistatelematica.cujae.edu.cu/index.php/tele/article/download/29/27.. 1729-3804.

VALERO, María. 2014. Usar redes wi-fi públicas con seguridad. [En línea] 23 de 10 de 2014. [Citado el: 28 de 9 de 2016.] http://economia.elpais.com/economia/2014/10/23/actualidad/1414073128_799835.html.

VALLE, Mónica. 2016. La mayoría de los usuarios creen que sus datos están seguros en las redes Wi-Fi públicas. [En línea] 28 de 6 de 2016. [Citado el: 19 de 9 de 2016.] http://globbsecurity.com/inseguridad-redes-wifi-publicas-38910/.

VALLEJO, Germán. 2016. Top 5 'Otros' mejores pueblos de Antioquia (Antioquia). [En línea] 24 de 3 de 2016. [Citado el: 27 de 11 de 2016.] http://www.viajarenverano.com/top-5-otros-mejores-pueblos-de-antioquia-antioquia/.

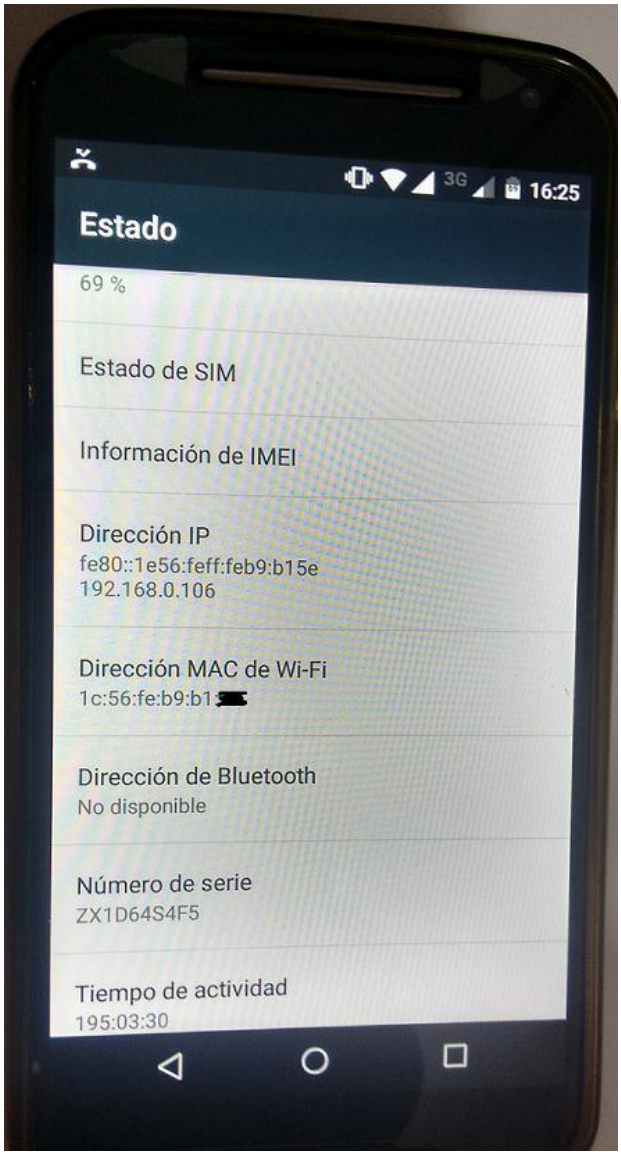
Wi-Fi - Conceptos Trabajar. [En línea] [Citado el: 10 de 23 de 2016.] http://es.w3eacademy.com/wi-fi/wifi_working_concepts.htm.

ZERIAL. 2009. Cómo Provocar Un Ataque DDoS Mediante SQL Injection. [En línea] 20 de 7 de 2009. [Citado el: 28 de 9 de 2016.] https://blog.zerial.org/seguridad/como-provocar-un-ataque-ddos-mediante-sql-injection/.

ZIEGLER, Marina. 2014. Avast expone el gran riesgo de seguridad de las redes Wi-Fi abiertas. [En línea] 13 de 11 de 2014. [Citado el: 28 de 9 de 2016.] https://press.avast.com/es-ar/un-studio-de-avast-revela-que-el-78-de-las-redes-domesticas-argentinas-se-encuentran-vulnerable-frente-ataques-ciberseguridad.

ANEXOS

Anexos 1.Dirección IP y MAC trabajadas en el tercer ataque



Fuente el autor

Dirección IP y MAC del equipo celular, trabajado en los Ataques de Phishing, Man in the middle y ARP Spoofing

Anexos 2. Fotografía del Parque Rafael Uribe Uribe

Fuente: (Vallejo, 2016)

Anexos 3. Imagen satelital del parque del parque Rafael Uribe Uribe

Fuente: (maps)