UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO VALLE DE CHALCO

SOFTWARE DE SEGURIDAD EN REDES WIFI

ENSAYO

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A

EDGAR HUERTA HERNÁNDEZ

ASESOR:

DR. EN C. MANUEL ÁVILA AOKI

VALLE DE CHALCO SOLIDARIDAD, MÉXICO JUNIO 2017.

OFICIO: **FT5**
Valle de Chalco, Méx. Lunes, 26 de junio de 2017

M. EN P. J. JUAN CARLOS HERNÁNDEZ HERNÁNDEZ
SUBDIRECTOR ACADÉMICO
DEL CENTRO UNIVERSITARIO *UAEM* VALLE DE CHALCO

PRESENTE.

Por este conducto, comunico a usted que el trabajo de Ensayo con el título:

"SOFTWARE DE SEGURIDAD EN REDES WIFI"

Llevado a cabo por C. EDGAR HUERTA HERNÁNDEZ con número de cuenta 1128987 de la licenciatura en INGENIERÍA EN COMPUTACIÓN registrado el día 17 del mes de FEBRERO de 2016 con Número de Registro ICO/08.03.16/418 ha concluido, y estamos de acuerdo para la impresión definitiva de Ensayo

	Nombre	**Firma**
Asesor	DR. MANUEL ÁVILA AOKI	
Revisor	DR. WILLIAM DE LA CRUZ DE LOS SANTOS	
Revisor	ING. FRANCISCO ARAGÓN CANSECO	

Sin más por el momento quedo de usted.

ATENTAMENTE

C. EDGAR HUERTA HERNÁNDEZ

CARTA DE CESIÓN DE DERECHOS DE AUTOR

El que suscribe Edgar Huerta Hernández Autor(es) del trabajo escrito de evaluación profesional en la opción de Ensayo con el título Software de seguridad en redes wifi, por medio de la presente con fundamento en lo dispuesto en los artículos 5, 18, 24, 25, 27, 30, 32 y 148 de la Ley Federal de Derechos de Autor, así como los artículos 35 y 36 fracción II de la Ley de la Universidad Autónoma del Estado de México; manifiesto mi autoría y originalidad de la obra mencionada que se presentó en Centro Universitario UAEM Valle de Chalco para ser evaluada con el fin de obtener el Título Profesional de Ingeniero En Computación.

Así mismo expreso mi conformidad de ceder los derechos de reproducción, difusión y circulación de esta obra, en forma NO EXCLUSIVA, a la Universidad Autónoma del Estado de México; se podrá realizar a nivel nacional e internacional, de manera parcial o total a través de cualquier medio de información que sea susceptible para ello, en una o varias ocasiones, así como en cualquier soporte documental, todo ello siempre y cuando sus fines sean académicos, humanísticos, tecnológicos, históricos, artísticos, sociales, científicos u otra manifestación de la cultura.

Entendiendo que dicha cesión no genera obligación alguna para la Universidad Autónoma del Estado de México y que podrá o no ejercer los derechos cedidos.

Por lo que el autor da su consentimiento para la publicación de su trabajo escrito de evaluación profesional.

Se firma la presente en la ciudad de Méx. Valle de Chalco, a los 26 días del mes de junio del 2017.

_____

Edgar Huerta Hernández

AGRADECIMIENTOS

A mis padres

Doy gracias por cada una de las palabras de ánimo durante las etapas de mi vida académica, base fundamental de motivación a diario. De igual forma darme claves esenciales para crecer como persona tales como respeto, humildad y responsabilidad.

Amigos

Que de manera directa o indirecta me brindaron ánimo y compartieron experiencias, conocimientos y lo más importante tiempo.

A mis hermanos

Por brindar opiniones y palabras de ánimo durante la licenciatura.

A mi asesor Dr. Manuel Ávila Aoki

Por brindarme enseñanzas, consejos, paciencia y compromiso, base fundamental para la dirección de este trabajo.

A mis revisores

Por brindar tiempo, para expresar opiniones y consejos para la mejora de la elaboración de este ensayo.

DEDICATORIA

A mi familia

Gracias a consejos y enseñanzas. Fue suficiente para tener un motivo para seguir adelante, superando obstáculos y manteniendo la unión familiar.

Cada recuerdo será base fundamental para crecer como persona y en aspectos profesionales.

SOFTWARE DE SEGURIDAD EN REDES WIFI

ÍNDICE

INTRODUCCIÓN

La seguridad actualmente se puede describir como un acto de protección y uso de medidas preventivas, aplicadas a medios de comunicación en este caso en particular a las redes wifi, considerando el enfoque de la seguridad informática la cual se define como.

Disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. (Aguilera, 2011).

Con ello conservar los objetivos de las comunicaciones.

Surge el requisito de atender dicha necesidad en la vida de las personas ya sea en aspectos laborales, académicos y domésticos, enfrentando las situaciones que se presenten diariamente.

En el contexto que se maneja la palabra seguridad, será en aspectos, del cuidado de la información, la cual estará relacionada en redes inalámbricas donde el medio de transmisión de la información se da por medio del aire y ondas.

Diariamente las redes particulares pueden estar expuestas a interrupciones en diferentes ámbitos, desde domésticos hasta corporativos todo esto debido a la gran creciente demanda de internet y el acelerado cambio de la tecnología. Donde uno o más dispositivos como teléfonos inteligentes, tablets, laptops, consolas de videojuegos, etc. Pueden conectarse utilizando la tecnología inalámbrica o wireless, sin el uso de cables este funcionamiento se da por medio del envío y recepción de ondas de radio, respetando un espectro electromagnético con similitud a la telefonía móvil.

Uno de los sucesos importantes a través de la historia es cuando por primera vez se logra realizar una comunicación de sonido, utilizando un canal

como medio de luz esto en los años 1880, posteriores trabajos con la utilización de ondas de radio, Rudolf Hertz logra la primera comunicación inalámbrica esto en el año 1888, con estas bases se requería un estándar el cual implementara normatividades en proceso de comunicación, donde influían aspectos como velocidad de transmisión donde inicialmente fueron de 5Mb/s, por parte del instituto de ingenieros eléctricos y electrónicos nueve años más tarde se define el estándar 802.11 y empresas como Nokia dan paso a fomentar el desarrollo de dispositivos electrónicos, teniendo en consideración la compatibilidad del estándar IEEE 802.11

La importancia de este ensayo, recae en la preponderancia que existe en conocer como la seguridad influye en redes inalámbricas, de igual manera sus alcances y cómo ha evolucionado diariamente, resaltando dicha relación entre seguridad y redes inalámbricas.

A principio se presentan temas actuales y su evolución con el paso de los años, en algunos temas se hace énfasis en el sistema operativo Windows haciendo uso de software y herramientas contenidas, en la parte final se puede apreciar mayor contenido donde se menciona una distribución del sistema operativo Linux, llamado Kali Linux. Caracterizando una propuesta de software, dando a conocer medidas de prevención por medio de este.

II. SOFTWARE DE SEGURIDAD EN REDES WIFI

2.1 Comunicación inalámbrica

Este tipo de comunicación está basada en el nulo uso de cables, a través de “ondas electromagnéticas, de radio, microondas o infrarrojo”, para el envío y recepción de señales a través de largas distancias.

Dicha conexión no es diferente de otros modos de conexiones en red. (Carballeiro, pág.148, 2014).

- Ondas electromagnéticas: propagación de un movimiento ondulatorio por medio del aire a causa de perturbaciones físicas o a través de un medio.

En este caso la propagación de dichas ondas es por medio de antenas wifi, modem, repetidores, etc. Cuyo principal objetivo es compartir recursos e información entre todos los elementos que conforman dicha comunicación, y de alguna manera obtener flexibilidad para optimizar tareas o procesos que realizan los usuarios.

2.1.1 Comunicación inalámbrica en la actualidad

Actualmente la adquisición de comunicación inalámbrica va en constante crecimiento donde se comienzan a utilizar dichas conexiones para procesos laborales tales como el comercio, salud, política, etc. Ya sea tanto para los empleados de un centro comercial o alguna persona en un sitio público.

Entre algunos datos importantes están el reporte de la OCDE, Organización para la Cooperación y el Desarrollo Económico, donde muestra que los dispositivos inalámbricos tienen una creciente demanda en la utilización de la comunicación inalámbrica para tareas de gran importancia.

Entre los países que integran la OCDE, se encuentra México que durante el periodo 2012 y 2013 la utilización de teléfonos inteligentes se tuvo un aumento del 30% y con ello crecieron las tareas a realizarse por medio de estos, como la navegación por internet, envío de correos electrónicos, usos de sitios de compras online, banca en línea, búsqueda de establecimientos, movilidad, etc. Con todas las herramientas que actualmente podemos encontrar en los dispositivos inteligentes.

Por otra parte, la consultora Gartner(2017) destaca que para 2020, existirán más de 30 mil millones de dispositivos y objetos cotidianos como aires acondicionados, refrigeradores, televisiones, entre otros, conectados con Internet escenario que impulsará la automatización de en edificios, hogares y oficinas.

Dicha tecnología inalámbrica, está ganando nuevas formas de implementación donde se ahorra tiempo y trabajo en la realización de tareas, un ejemplo claro es la reproducción de contenido en pantallas Smart TV´s, cámaras, cerraduras etc. Se le conoce como internet de las cosas, que surge gracias a la atención de las personas por tener conectados inalámbricamente y en red con un entorno de direcciones IP, aparatos de la vida cotidiana haciendo referencia a objetos inteligentes,

El internet de las cosas en relación con la tecnología inalámbrica de igual forma repercute en las personas, donde proyectos a mediano plazo plantean que las personas formen parte de esta comunicación con aplicaciones, esto dado por medio de la implantación micro chips con información personal historiales médicos, académicos, laborales donde de igual forma se retomaran retos de seguridad y alcances.

A diario nos podemos dar cuenta que la tecnología inalámbrica tiene un papel muy importante en aspectos de seguridad, para generar confianza en los

usuarios y así crear interés en nuevas tecnologías y planteara nuevos requisitos diseñados para los usuarios, tales que deben ser mucho más informados sobre características y funciones, que en ocasiones no se tiene conocimiento de algunos términos relacionados.

2.1.2 Medios de transmisión de redes inalámbricas

La propagación de la información tales como datos, voz, video, imágenes, etc. Está dada a consideración a rangos de frecuencias esto tendrá como resultado características propias de cada medio. Entre algunos medios se pueden describir:

- Ondas de radio: Utilización de ondas electromagnéticas, donde existe una propagación a través del espacio transportando diferentes campos electromagnéticos, regularmente la frecuencia va desde 300 a 3000 Hz.
- Microondas terrestres: Comunicación precisa punto a punto, haciendo uso de antenas procurando la evasión barreras físicas, ya que es necesario la alineación de emisor y receptor, donde se alcanzan frecuencias de 1 a 300 GHz y cubren coberturas de kilómetros.
- Microondas por satélite: Basado en la retrasmisión de información por medio de enlaces, donde la señal de las bases de la tierra son amplificadas con ayuda de un satélite cuya función primordial es realizar el reflejo de la señal a uno o varios puntos.
- Enlace dado por emisores y receptores donde la propagación de información es por medio de luz la cual no puede traspasar obstáculos, se enfoca en entornos interiores de salas trabajo temporal, sin interferencias de ruido y superar los 300 Ghz.

2.2 WIFI

2.2.1 Introducción al Wifi

El uso del mecanismo de conexión por parte de la variedad de dispositivos inalámbricos, están regidos por especificaciones que a lo largo de los años han cambiado, ya sea por nuevos requerimientos tanto de los dispositivos modernos como de los equipos usados para la comunicación, como dato histórico en el año 1997 se realizó una estandarización de red inalámbrica de área local WLAN con especificaciones 802.11, dichas abarcaba aspectos de la capa física y conexión de datos del modelo OSI.

Se mantuvo constantemente el promover dicho estándar y lograron, la certificación de dispositivos que garantizaban su buen funcionamiento. A partir de ese momento comenzó la validez de la certificación, Wireless Fidelity (Wi-Fi).

Como fueron avanzando los logros obtenidos, una variedad de fabricantes toman interés y posteriormente nace la asociación *Wireless Ethernet Compatibility Alliance* (WECA). Y finalmente se obtiene un organismo que se mantiene con el nombre de Wi-fi Alliance.

2.2.2 Clasificación de las redes Wifi

Este trabajo está enfocado principalmente a las redes inalámbricas de tipo local WLAN debido a su creciente expansión, que hace unos años no se tenía en mente el gran crecimiento de estas, sin embargo es importante mencionar, algunos alcances de las redes, ya que las computadoras pueden ser conectadas desde distintos lugares del mundo, simplemente con acceso a internet.

Esta clasificación de dichas redes se puede retomar considerando la misma manera en que se hace con las redes cableadas, considerando el alcance de las mismas como se muestra en la figura 1.

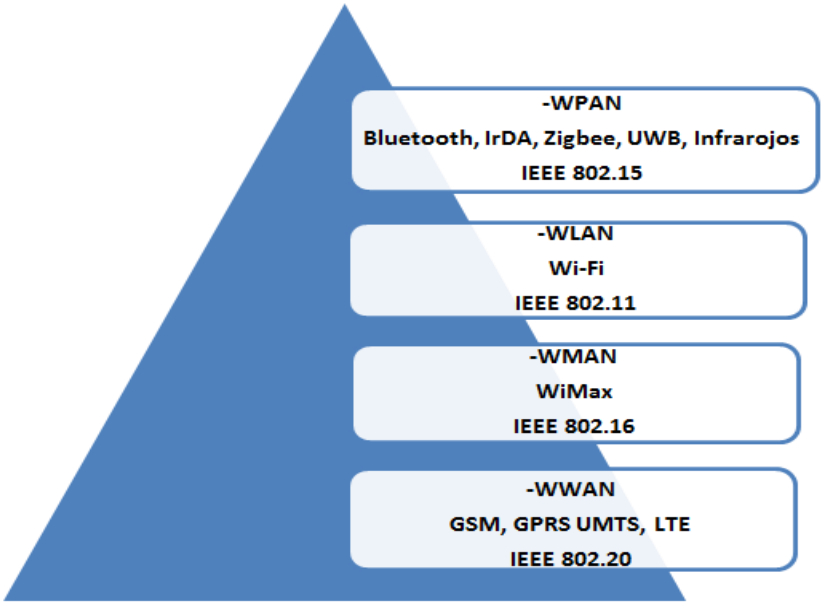


Figura 1. Diferentes tecnologías inalámbricas junto con sus estándares. Para WLAN, se tiene IEEE 802.11-Wifi. (http://secarcam.webcindario.com/?p=707&lang=es)

En las redes de la WLAN, como una red de área local inalámbrica opera a una banda de 2.4 GHz, se mantiene entre el rango de las bandas de frecuencia como se puede mostrar en la figura 2.

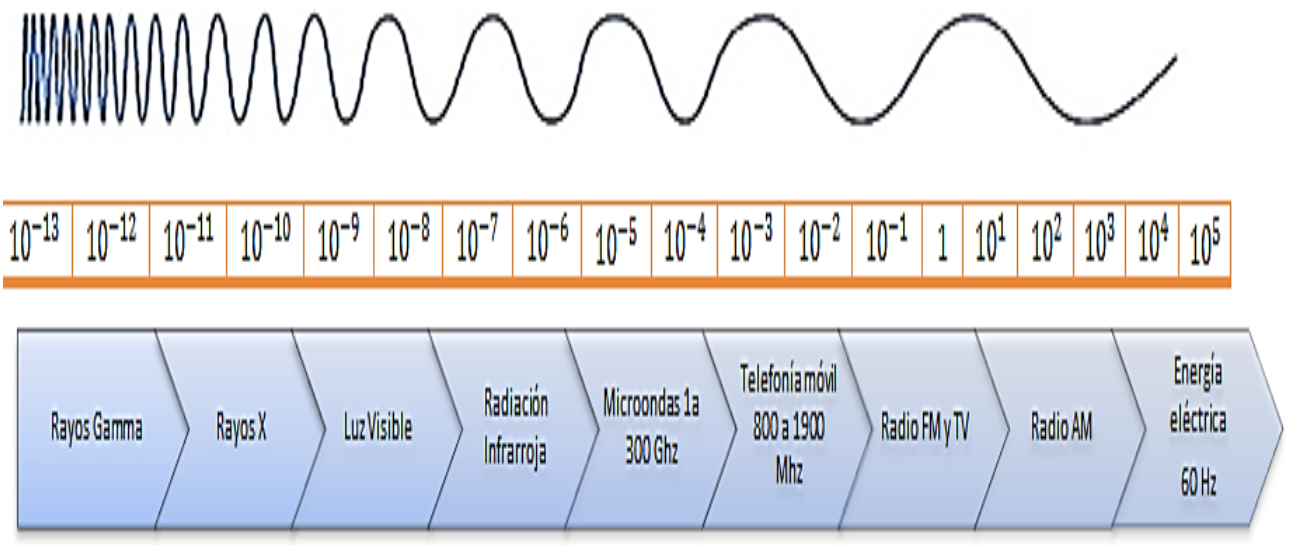


Figura 2. Espectro electromagnético de las bandas de frecuencia.
(http://docplayer.es/8195793-Radiacion-electromagnetica-de-telefonia-movil.html)

2.2.3 Estándares del Wifi

Las diferentes especificaciones son basadas principalmente en 802.11 originalmente, las cuales hacen uso de la capa física.

- IEEE 802.11b

Es dada a conocer en 1999 y su velocidad máxima de 11 Mbps y con una frecuencia de 2.4 GHz. (Dordoigne, pág. 288, 2013).

- IEEE 802.11a

Igualmente publicada en 1999 pero a diferencia que su capa física puede trabajar a 5 GHz. Y como transmisión máxima tiene 54 Mbps. mantienen una incompatibilidad con las antenas 802.11b. (Dordoigne, pág. 289, 2013).

- IEEE 802.11g

Utiliza la banda de los 2,4 GHz y permite velocidades de 54 Mbps. (Dordoigne, pág. 289, 2013).

- IEEE 802.11n

Tras la finalización de estándares 802.11 en 2009 tras versiones 1.0 y 1.1 se da a conocer la versión 2.0 que incluye servicios Wi-Fi multimedia para aplicaciones de VoIP Y streaming, trabajando a 2.4 GHz, 5 GHz y de velocidad 600 Mb/s. (Dordoigne, pág. 289, 2013).

- IEEE 802.11i

Este estándar fue creado con la finalidad brindar seguridad a principio la autenticación WEP, teniendo un subconjunto de este estándar WPA y finalizado en WPA2.

Con respecto a dispositivos wifi hoy en día, se basan principalmente en el estándar 802.11n que busca primordialmente el rendimiento y tiempos de espera reducidos en comunicación de las entidades vinculadas, una estación con un punto de acceso.

2.2.4 Ventajas

I. Flexibilidad de conexión, al poder estar en constante movimiento sin tener un espacio dedicado de conexión, teniendo solo como consideración el área disponible de red.

II. Poca planificación: No se debe pensar en la planificación de la distribución cableada de las maquinas, simplemente el cuidado que los aparatos conectados estén en la cobertura de dicha red o repetidores de señal.

III. Diseño: Variedad de dispositivos inalámbricos

IV. Robustez: Accidentes en cableado a causa de componentes físicos.

V. Portabilidad: Permite a los usuarios moverse junto con los dispositivos conectados a la red inalámbrica, tales como notebooks, o similares sin perder el acceso a la red.

2.2.5 Desventajas

I. Menor velocidad: Las redes cableadas trabajan con velocidades de 100 Mbps a 10000 Mbps, que se reduce en redes sin cables además se tienen puntos de nula conexión debido a barreras físicas.

II. Mayor inversión: En comparación con redes cableadas es mayor los costos de implantación.

III. Seguridad: Debido a la transmisión de señal por aire alguna persona no autorizada y con conocimientos sobre redes con algún equipo con un notebook, teléfono u otro dispositivo puede acceder a dicha red solo con estar en un área de cobertura.

2.3 SEGURIDAD EN REDES WIFI

El desarrollo acelerado de las computadoras y la necesidad de dicha herramienta como auxiliar en las actividades humanas, además presentes en todos los campos de la vida moderna se rige ante estos procesos tecnológicos que cada día se maneja un número creciente de información de toda naturaleza ya sea en lo técnico, profesional, científico, personal, etc.

Con todo esto se generan y se mejoran las formas al realizar delincuencia ya existente, donde la mayoría de estos actos ilícitos no se llegan a descubrir, esto hace tan necesario tener en mente la importancia de conocer el funcionamiento y seguridad de la transmisión de datos por medio de redes inalámbricas.

2.3.1 Delito informático

Es considerado por expertos y por organizaciones como “cualquier comportamiento antijurídico no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisión de datos” (OECD, 2017).

Esto de forma general se relaciona con el uso de PC´s o dispositivos que en vinculación con técnicas y procedimientos, se logran acciones informáticas de carácter ilegal, tales perjuicios pueden ser fraudes, robos, falsificación, estafas, sabotajes entre otros.

2.3.2 Como proteger nuestra red wifi

Algunas de las medidas de seguridad que nosotros mismos podemos tomar en cuenta a la hora de la configuración de nuestras redes están.

-Eliminación valores predeterminados de la red: evitar utilizar valores predeterminados por el router inalámbrico.

-Cifrado de datos con un protocolo seguro.

-Cerrar la red a dispositivos ajenos.

-Cifrado de la información y archivos

-Utilización del sistema de cifrado WPA2 que está enfocado en la mejora de seguridad de su predecesor WPA, se trata de la opción más segura soportada además de tener como característica el cifrado se implementa a través del protocolo AES.

-Limitar la ejecución incontrolada de software en el equipo.

-Proteger la privacidad del equipo por medio de la aceptación de permisos.

-Limitar el radio de propagación de la red inalámbrica.

-Instalación de certificados actualizados.

-Utilización de servidores propios hace referencia páginas más seguras

2.3.3 Riesgos de las redes wifi

Perdida de confidencialidad: Espionaje del tráfico que circula en la red, obteniendo sitios visitados, intercambio de información que no viaje de manera cifrada podría ser observada, con el uso de antenas dentro del rango de alcance.

Fraudes: Ciberdelincuentes podrían estar haciendo uso de nuestra red desprotegida para perpetrar desde ella acciones delictivas con fines económicos, y en caso de alguna investigación policial los conduciría hacia nosotros.

Judiciales: Se ofrecería la conexión a internet de manera sencilla, tomando este como medio para la realización de delitos, entre algunos están piratería, pornografía y pedofilia.

Mantener el acceso a la red: La persona no autorizada tendría el acceso a conexión en cualquier momento que lo desee, podría hacer uso de programas o aplicaciones que consumen demasiado ancho de banda, pondría en riesgo nuestra conexión.

2.4 Amenazas de las redes Wifi

En el momento que nuestros equipos se encuentran conectados a internet, por medio de nuestra propia red, existe la posibilidad de presentarse practicas no autorizadas ya sea la utilización de herramientas que existen para varios entornos de sistemas operativos, que causen daño a nuestros ordenadores los cuales directamente afectarían a nuestra información, sino se aplican algunas medidas de seguridad. Es importante conocer algunos elementos que se involucran directamente con estas amenazas tales como la intrusión, papeles que realizan los intrusos en nuestra red.

2.4.1 Intrusión: Acción de permitir el acceso no autorizado o aumentar los privilegios otorgados a un sistema.

2.4.2 Intrusos: Persona que en base a pruebas y procedimientos propios que comprende, consigue el acceso a datos o programas a los cuales no esta autorizado

Tipos de Intrusos.

- Usuarios suplantadores (externo): Penetración no autorizada a un sistema, para la obtención de privilegios del usuario legítimo.

- Usuario malicioso (interno): Se tiene el derecho a acceso a ciertos recursos, pero de alguna manera se acceden a datos, programas, contenido donde no se es autorizado.

- Usuario clandestino (ambos): Se logra tener el control en los accesos del sistema, además de la supervisión de este, el cual puede ser accedido en cualquier momento.

2.4.3 Sabotaje informático

Se trata del conjunto de intencionados actos sin autorización de carácter malicioso que detienen el funcionamiento normal de computadoras que comparten una red de comunicación, tales actos pueden ser borrar, modificar funciones así como configuración o información contenida, esto por medio de archivos ejecutables, o reproducción de programas informáticos de protección legal.

2.4.4 Escaneo a redes inalámbricas

Como paso inicial para la búsqueda de conexión a una red inalámbrica es necesario, detectar las que se encuentran disponibles cercanas y recolectar información sobre su configuración. En ocasiones es utilizada la herramienta incorporada en el sistema operativo en uso, para visualizar detalles como nombre de red, intensidad, tipo de radio y seguridad que se mantiene configurada.

Para lograr la conexión en redes donde no es autorizado el acceso, se requiere basarse en un método para la recopilación e interpretación de datos, las herramientas actuales se basan principalmente en:

Pasivo: Su limitación está en escuchar e interpretar la información que se recibe en algunos casos su identificador SSID.

Activo: No existe limitación al escuchar, su característica está en interactuar con la con la red logrando modificar, eliminar, o inyectando tráfico en la red,

ya sea con el punto de acceso, o los equipos de usuarios conectados a dicho punto de acceso.

2.4.5 Uso de algunas herramientas para el escaneo de redes

Para la realización de estas tareas se pueden hallar una gran cantidad de software, para el escaneo de redes cercanas y así poder recolectar la información ya mencionada, entre algunos los que más resaltan en la web pueden mencionarse.

CommView

Analizador de paquetes de conexiones inalámbricas para la monitorización de red 802.11 a/b/g/n. Como se muestra en la figura 3. Se está utilizando para la obtención detallada de redes cercanas y algunas de sus configuraciones.

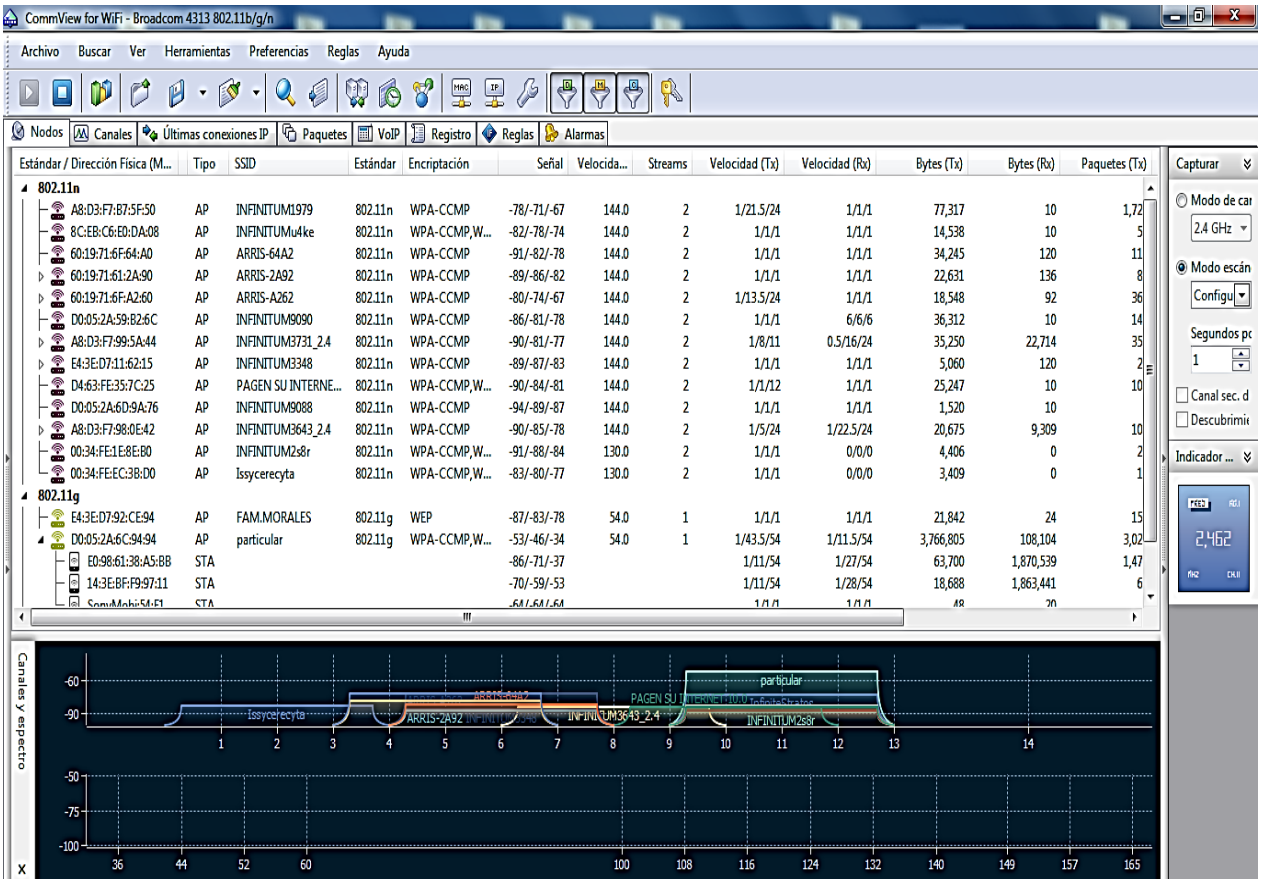


Figura 3. Señales Wifi detectadas por commView (Propio, 2017)

2.5 Vulnerabilidades en puntos de acceso de wifi

2.5.1 Utilización sistema WPS

Estándar para la configuración de redes Wlan que permite la conexión en algunos router de forma inalámbrica pulsando un botón, sin la necesidad de usar contraseña wifi, para identificar esta función se puede ver actualmente en routers Wifi integran la característica del sistema WPS (Wireless Protocol secure) que está configurado basándose a dos métodos de conexión.

- Configuración pulsando botón, tanto de nuestro dispositivo como de nuestro router wifi.
- PIN: conexión por medio de una cadena de caracteres dado por el router.

Entre las características de estas dos opciones están la rapidez y lo sencillo que es la conexión y como desventaja tenemos que con ayuda de software se puede tener la contraseña de acceso a la red.

Como ejemplo en la figura 4 y 5, se muestra la configuración de la tecnología WPS en un dispositivo móvil, además actualmente esta configuración está presente de igual forma en impresoras o adaptadores que integran funciones con su propio botón WPS para conexiones más sencillas.

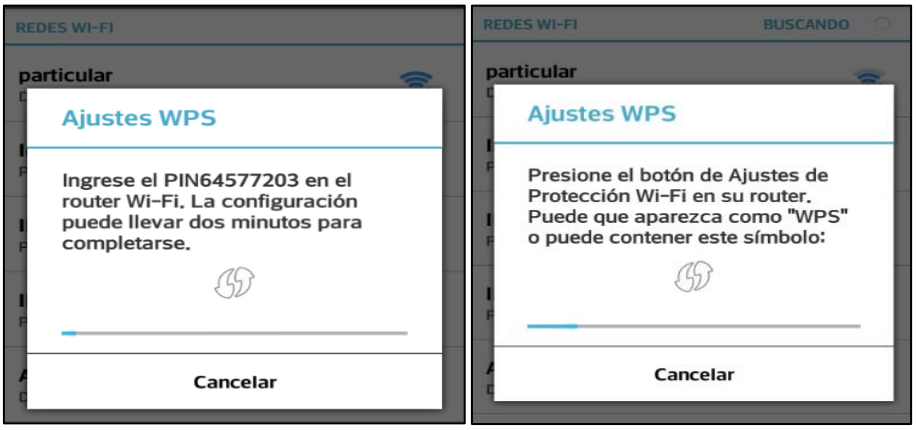


Figura 4 y 5. Conexión WPS por medio de celular (Propio, 2017)

Como desventaja está en la revelación de contraseñas de tipo WPA/WPA2 por medio de la función “reaver” que ayuda aun testeo de red que se mantiene activada por medio de la utilización de la función WPS.

Para dichas tarea hoy en día está en funcionamiento aplicaciones basadas en Windows, una de estas es *WPSCrackGUI*.

2.5.2 SSID

Para la identificación de nuestra red en conexiones inalámbricas por lo general en la configuración, del router se muestra el nombre de identificador de conjunto de servicios, el cual hace referencia a un valor alfanumérico que se puede extender hasta 32 caracteres, el cual su función es diferenciar el tráfico de los usuarios, al hacer uso del identificador de la red facilita la obtención de datos relevantes a la hora de la búsqueda de redes ocultas por medio de software tal como puede ser CommView.

2.5.3 Filtrado de direcciones Mac

El uso de las direcciones físicas de una interfaz de red (MAC) logra ser un punto importante para aumentar la seguridad en los accesos a una red de forma inalámbrica, esto puede ser por medio de la activación de un cortafuegos del mismo router que se está utilizando como punto de acceso, con la función de la denegación o aceptación de direcciones físicas, teniendo como base que no puede existir dos tarjetas con la misma MAC física.

Para este proceso existen dos tipos de listas que se las cuales son.

- Listas de denegación: se hace la comparación de las MAC entrantes y si coinciden con las no autorizadas se les niega la conexión.
- Listas de aceptación: Se realiza los pasos contrarios a las listas de denegación.

Sin embargo no se debe tener una totalidad de confianza en que nos garantiza evadirse de técnicas dirigidas a direcciones físicas.

En la figura 6 muestra la dirección física (MAC) de un ordenador, por medio del intérprete de comandos de Windows, para configuraciones futuras.

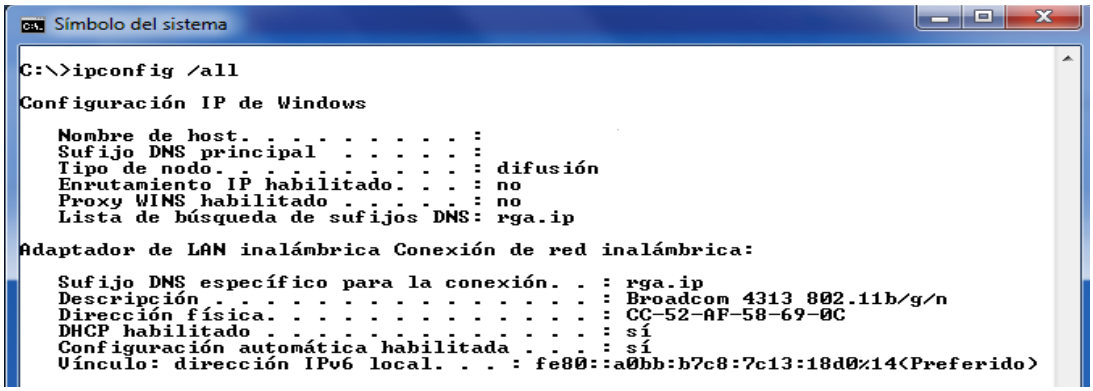


Figura 6. Dirección MAC (Propio, 2017)

Dicha dirección utilizarla en la configuración de cortafuegos de nuestro punto de acceso, para ser permitidas o denegadas. Como se ve en la figura 7, donde permite la captura de 32 direcciones.

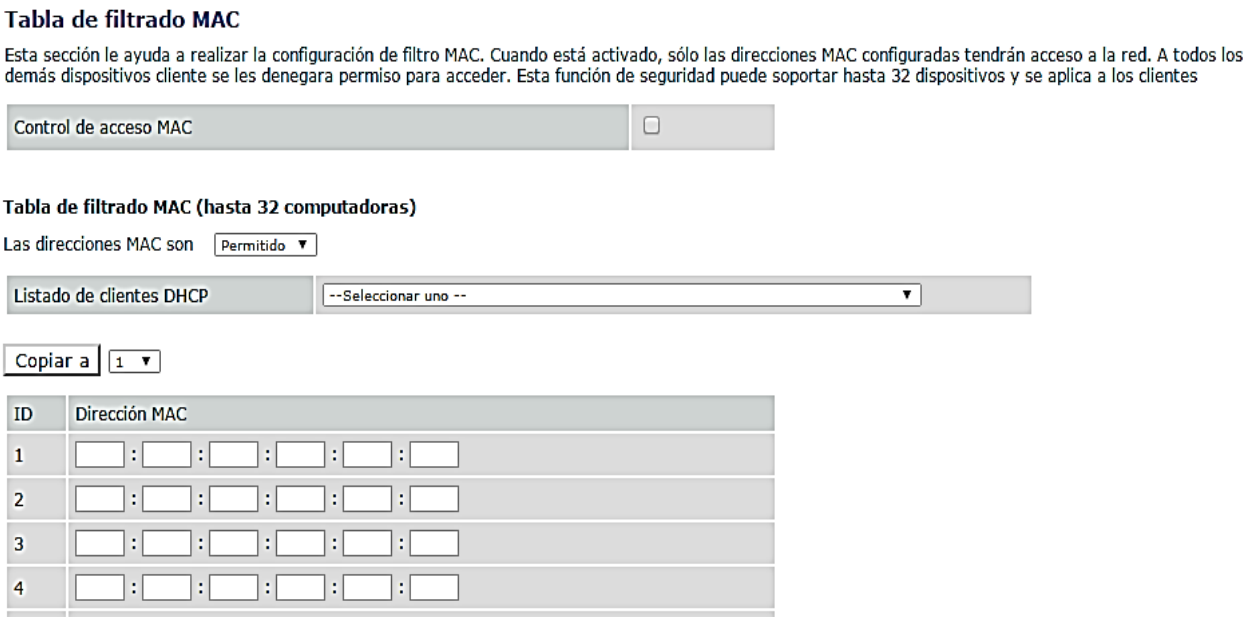


Figura 7. Filtrado mac en punto de acceso (Propio, 2017)

2.5.4 Packet Sniffing

Es importante tener en cuenta, el gran valor que se le agrega a la información por medio de las conexiones wifi en cada rol que se use, a causa de la posibilidad de ser esta monitoreada por la intercepción del tráfico (sin modificación) con la ayuda de husmeadores.

2.5.5 Spoofing

Conocido de manera común como engaño, es aplicado cuando se tienen vulnerabilidades en nuestras redes, donde se busca la suplantación de identidad, por medio de la comunicación falseada, con el propósito de la modificación de rutas de red para uso mal intencionado, además en los derivados del spoofing existe acciones tales como filtrado, sustitución, envió y recepción de datos, etc.

2.5.6 MAC Spoofing

Teniendo dos ideas en mente el spoofing y el proceso de comunicación entre las dos entidades, el punto de acceso y el cliente que llevan a cabo el intercambio de paquetes los cuales se dirigen a una dirección IP la cual debe estar asociada a un identificador único en este caso la dirección MAC. Puede ocurrir esta técnica que busca la simulación de un cliente legítimo, por medio de su dirección MAC.

El atacante puede hacer uso de escaneo de puertos y direcciones MAC validas conectadas, Por medio de Airodump-ng contenida en kali Linux podrá realizar la evasión de filtros MAC, manteniendo del anonimato.

Como una medida preventiva se debe tener en cuenta la utilización de un nivel de encriptación WPA-WPA2 y uso de certificados digitales.

2.6 Consecuencias de las conexiones no seguras

Cuando se toca este tema nos surge la necesidad de respondernos preguntas como ¿Qué tarea se está realizando para nuestra ciberseguridad?

Es importante identificar todo tipo de cambios y comportamientos extraños en nuestros dispositivos, con el paso del tiempo se siguen presentando amenazas básicas de seguridad algunas de estas por la falta de interés para reaccionar ante estas amenazas. A continuación se dan a conocer importantes riesgos que nos enfrentamos día a día.

2.6.1 Filtrado de paquetes Wireshark

Analizador de paquetes de red, es útil en la captura de información que pasa por medio de una conexión, puede ser útil para la localización de redes y el direccionamiento IP. En la figura 8 se puede apreciar el uso del software que al iniciarlo nos da información de la conexión establecida.

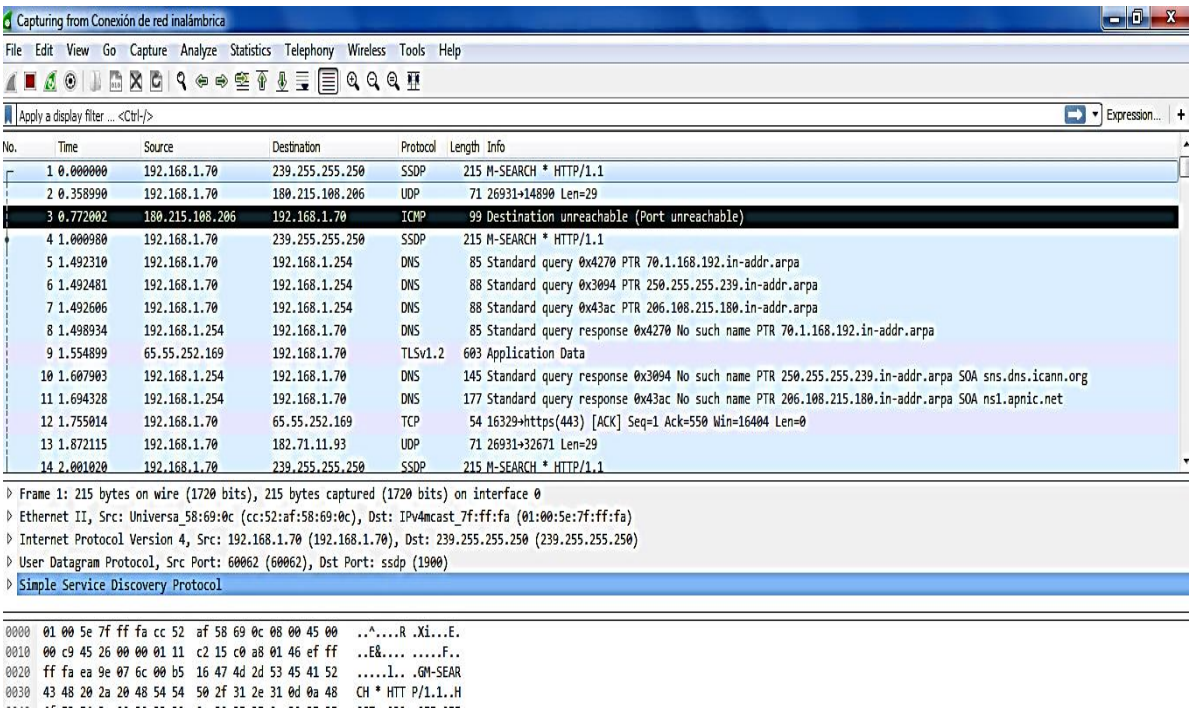


Figura 8. Software Wireshark (Propio, 2017)

Por medio de este se puede realizar filtros para determinados paquetes y al no verificar las páginas visitadas se puede obtener información con respecto a dicha conexión TCP como se muestra en la imagen 9, 10.

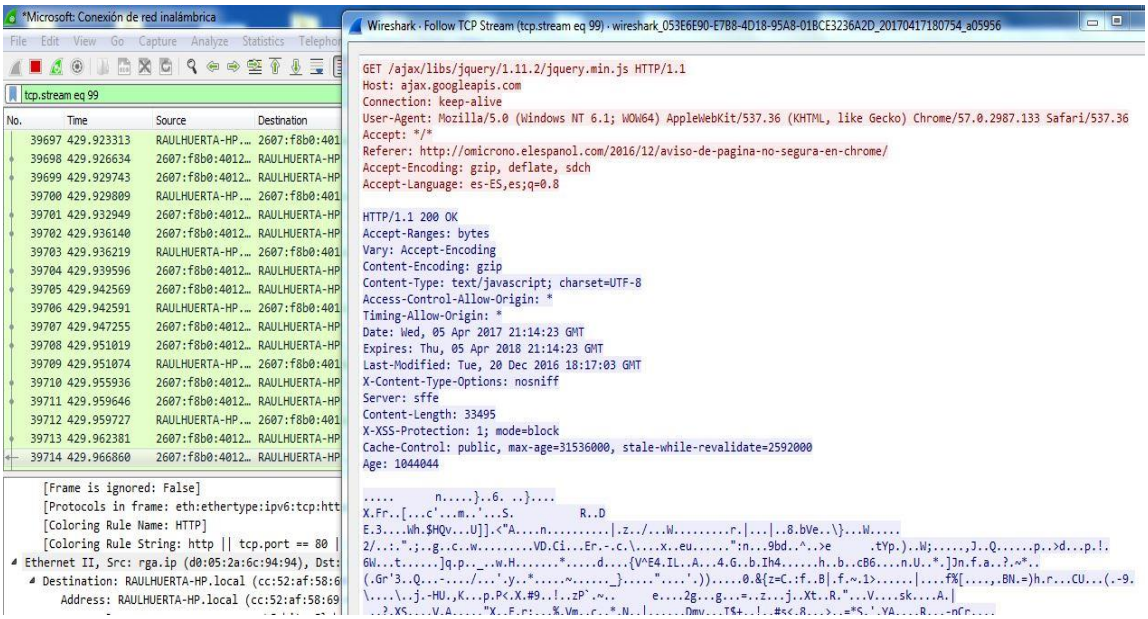


Figura 9. Filtrado de paquetes TCP (Propio, 2017)

Figura 10. Descripción de paquete TCP conexión no segura http (Propio, 2017)

2.6.2 Email Spofing

A la hora de tener conexión gratis en un sitio público, se pueden presentar personas que buscan información de usuarios que comparten la misma red, en específico se busca la captura de alguna dirección de correo electrónico. Con lo cual se hace uso de esta técnica, que consiste en enviar un correo electrónico o varios, haciendo uso de un nombre ficticio, haciéndose pasar por otra entidad.

Para que la víctima al checar este correo siga enlaces donde el atacante, tiene un dominio que actualmente en internet existen en gran cantidad, sin costo ofreciendo servicio de alojamiento de contenido de pequeño tamaño tal como 000webhost, donde se pueden crear portales ficticios engañosos, que almacenan contraseñas o acceso a algún servicio del cliente.

Es de gran importancia valorar el tiempo de conexión en sitios públicos donde la sensación de confianza es muy poca.

2.6.3 Spoofing DNS

Esta técnica de re direccionar a los usuarios de un sitio web a otro diferente con el nombre de dominio diferente al nombre de dominio registrado o se desea tener acceso García (2014).

Esto se logra por medio de la modificación de la información contenida en algún servidor de nombres de domino, realizando configuraciones de clonación de direcciones url y teniendo referencia de la dirección IP del equipo víctima, para que las peticiones a sitios pasen primeramente por la máquina del atacante y así obtener la captura de credenciales de inicio de sesiones. Ya que algunos servidores no cuentan con seguridad contra este tipo de ataques.

Como medida de prevención se debe ser muy observador al entrar a sitios visitados, desde mirar las fuentes y ver su comportamiento.

2.6.4 Pishing

Moderna forma de fraude en que le que se intenta robar la identidad de un usuario. Por medio de correos electrónicos u otro canal, se incita a visitar una página web donde se le solicitan sus credenciales de acceso a algún servicio, financiero, personal, laboral. Posteriormente, el pisher accederá a dicho servicio suplantando al usuario, obteniendo beneficios u algún fin (Álvarez Marañón, pág.11, 2009).

En los últimos años el porcentaje de ataques de pishing ha aumentado considerablemente, con gran énfasis en empresas con un número de empleados menor a 250, a causa de esto se generan campañas de información para empleados y público en general de igual manera en gran proporción. Dichos porcentajes que muestra *Symantec (2015)* arrojan un cremento del 9% en pequeñas empresas con respecto al año 2014-2015 como se muestra en la siguiente Tabla 1.

Tamaño de las empresas	2011	2012	2013	2014	2015
Grande empresa	50%	50%	39%	41%	35%
Mediana Empresa	32%	19%	31%	25%	22%
Pequeña Empresa	18%	31%	30%	34%	43%

Tabla 1.Porcentaje de crecimiento de pishing en pequeñas empresas (Symantec, 2015).

Entre puntos importantes para la identificación y evasión de Pishing esta:

-Solicitud de información sensible, sin ser solicitada.

-Acceso ha contenido por medio de suscripción a sitios desconocidos.

-Identificación de correos electrónicos sospechosos de ser pishiing.

-Evitar a sitios donde se ingrese información delicada por medio de links.

-Añadir medidas de seguridad en el ordenador.

-Verificar candado de seguridad de certificado digital.

-El Pishing cambia constantemente y en la actualidad abarcan la mayoría de idiomas.

-En el uso de correo para la obtención de información, los correos con pishing no muestran remitente.

Entre otros medios por los cuales obtener información de la víctima están:

-Robo de teléfonos celulares, para esto se debe realizar reporte de robo

-Robo de correspondencia

-Robo de carteras, con tarjetas de crédito e identificaciones

-Por medio de la obtención de la credencial de elector al entrar a un edificio y esta sea dejada como identificación.

-Evitar proporcionar gran cantidad de información por medio de redes sociales.

-Verificación de las fuentes de información de correos entrantes.

2.6.5 Spyware

En la utilización de redes públicas se puede incitar a la instalación de software que recopila información de dicho ordenador, para ser después transmitido a un entidad externa, sin aviso previo este término hace referencia a productos que se instalan inconscientemente como barras de acceso rápido, mostrar anuncios no permitidos, o cambiar la configuración del explorador, o él envió de información guardada en marcadores de nuestro buscador.

Este afecta a al ordenador tanto en rendimiento por la utilización de memoria RAM y el funcionamiento continuo hasta su eliminación (Álvarez Marañón, pág.12, 2009).

2.6.6 Recolección de información por medio del protocolo SNMP

El protocolo SNMP, Simple Network Management es de ayuda para recabar información sobre dispositivos con direccionamiento IP, que están conectados en una red, ya que se basa en la comunicación en la capa de aplicación en las redes por medio de petición-respuesta y como principal objetivo se tiene el control de dichos dispositivos, de los cuales como respuesta a estas peticiones se obtiene detalles de condiciones de conectividad, información de puertos, configuración de certificados, software y hardware en algunos casos la comunicación directa que en este caso particular será la red wifi publica.

En la siguiente imagen 11,12 se puede apreciar el uso de la aplicación gratuita *eznetscan* la cual hace uso de este protocolo, y podemos ver que solo con estar conectados a un punto de acceso, se puede obtener la información ya mencionada anteriormente de los dispositivos de la red wifi.

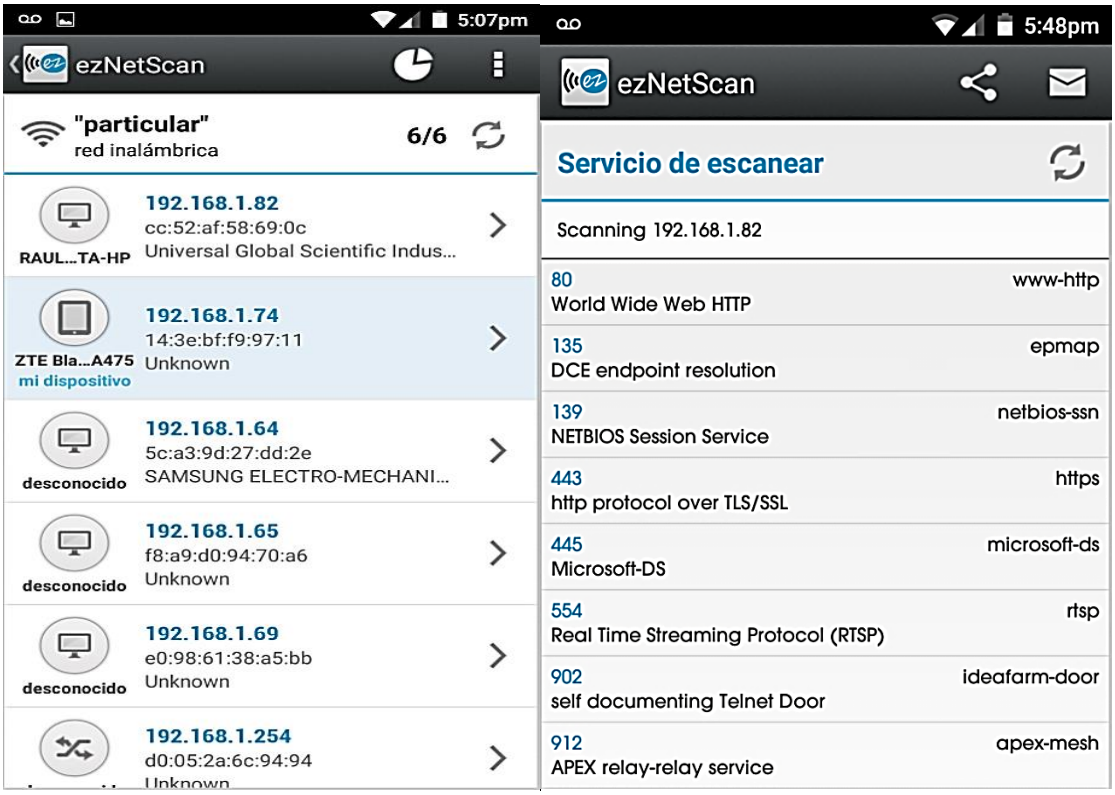


Figura 11.Información de dispositivo desde eznetscan (Propio, 2017)

Figura 12. Acciones a realizar con eznetscan (Propio, 2017)

2.7 Conexiones seguras

2.7.1 Uso de certificados digitales

La importancia de los certificados digitales radica en la verificación de las páginas web que visitamos, ofreciéndonos privacidad ante la posibilidad de copias muy precisas. Llevando a cabo una confirmación que dicho sitio web pertenece a quien dice ser, esto dado por compañías intermediarias que su función es ser autoridades de certificación, confirmando la autenticidad de dichas páginas web, dichos certificados son dados tras la veracidad de identidad y legitimidad.

Por otra parte nuestro navegador reconoce dicha autenticidad de manera automática y se podrá acceder a la página web que se desea visitar, sino es así nos ofrecerá como opción acceder a la página web con el certificado no reconocido, lo cual propone un riesgo ante nuestra seguridad.

En la figura 13. En la configuración avanzada de nuestro buscador, nos muestra nuestro certificado digital e información general con respecto a este como fecha de emisión y vencimiento, emisor, algoritmo de firma, etc.

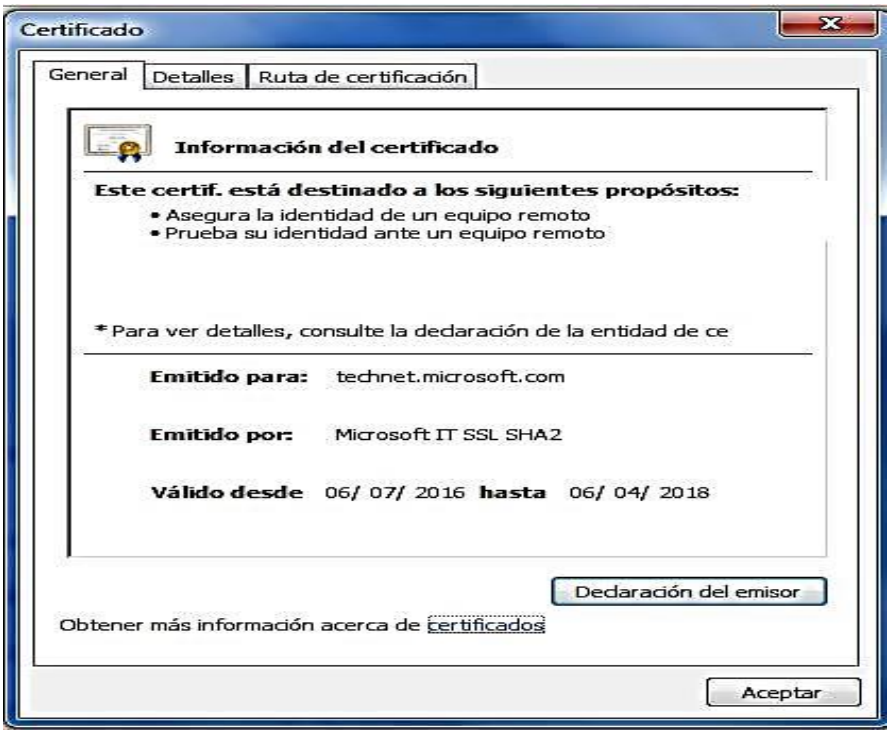


Figura 13. Uso de certificado en internet (Propio, 2017)

2.7.2 Uso de conexiones TLS

Las conexiones TLS nos proporcionan autenticación y cifrado para comunicaciones seguras en una red pública, tales como la revisión de correo electrónico, etc.

Ofrecen seguridad ante intercepciones y alteraciones en el envío y recepción de datos, es importante mantener estas normas actualizadas ya que con esta el cliente comprueba el servidor antes de establecer una conexión. En la figura 14 se logra ver la seguridad de la conexión que mantienen las comunicaciones cifradas.

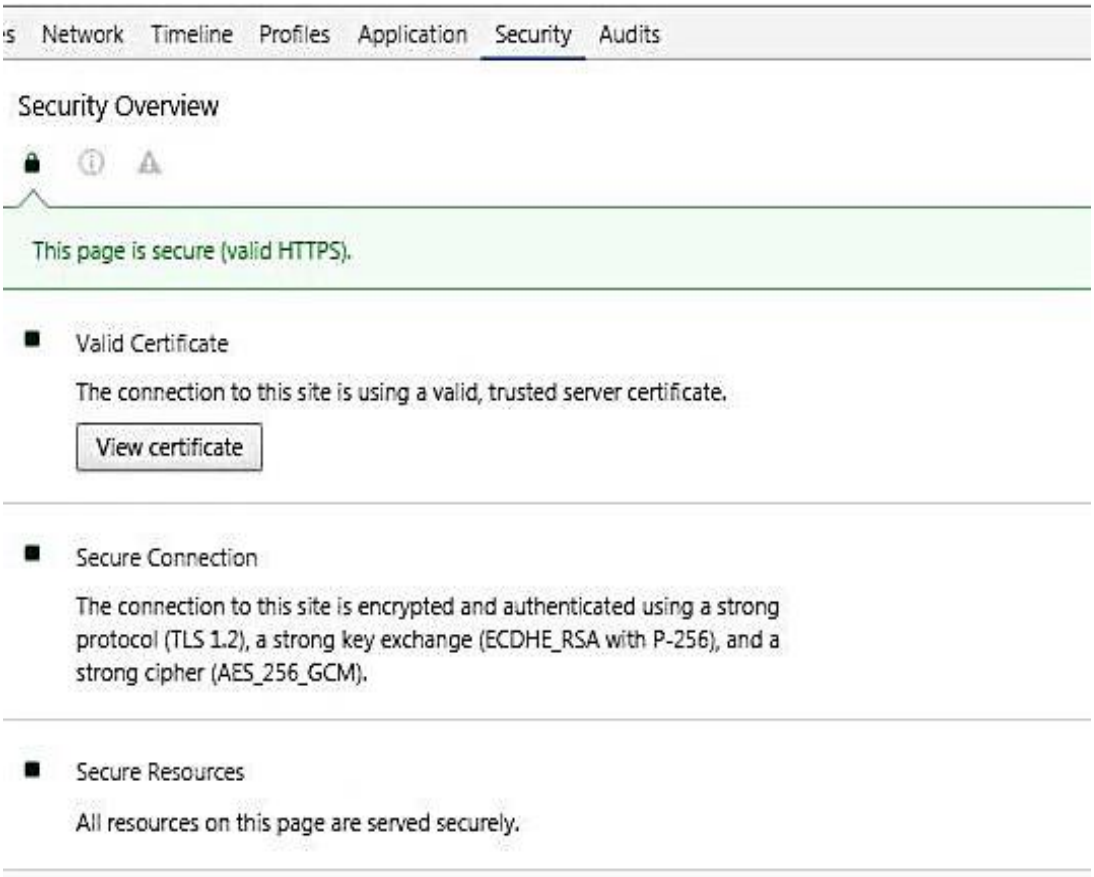


Figura 14. Uso de certificados TLS (Propio, 2017)

La manera de mantener las conexiones actualizadas en nuestro navegador es permitiéndoselo por medio de las configuración que añade, como se puede ver en la figura 15. Se coloca en la barra de direcciones *chrome://flags* en la parte de versión máxima de TLS permitiendo la versión más actualizada.

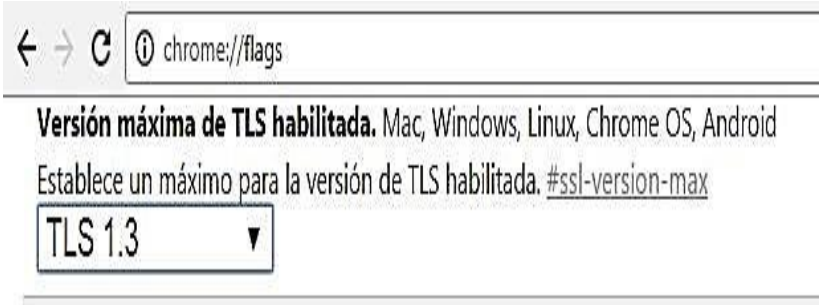


Figura 15. Configuración adicional en conexiones (Propio, 2017)

2.7.3 Peticiones a sitios seguros

Para la navegación segura es conveniente usar un protocolo seguro de transferencia de hipertexto *HTTPS*, lo cual es una versión segura de HTTP, los cambios radican en que el protocolo http usa el puerto 80 y https usa el 443 además de trabajar en una subcapa más baja de aplicación, además de añadir más seguridad para no permitir la captura de los datos sensibles.

Es muy importante utilizar conexiones seguras, y con más cuidado cuando se hacen uso de redes inalámbricas públicas, ya que en ocasiones paginas cifradas puedan contener enlaces que se remontan a sitios sin cifrar.

Una medida de seguridad a la hora de acceder a sitios es tener una extensión para el navegador web, que solicite la versión segura de un sitio a visitar un ejemplo de estas herramientas disponibles es HTTPS Everywhere que mejora la protección de sesiones web como se muestra en la Figura 16 y 17.

Figura 16. Petición a sitios seguros Everywhere. (https://www.eff.org/https-everywhere)

Figura 17. Uso de conexión segura (Propio, 2017)

Como medida complementaria en las propiedades de nuestro buscador en la Figura 18. Se muestra que se activa el marcar las conexiones HTTP como inseguras, esto nos permitirá redirigirnos nuevamente a un sitio seguro tal y como lo manejan los buscadores actualizados.

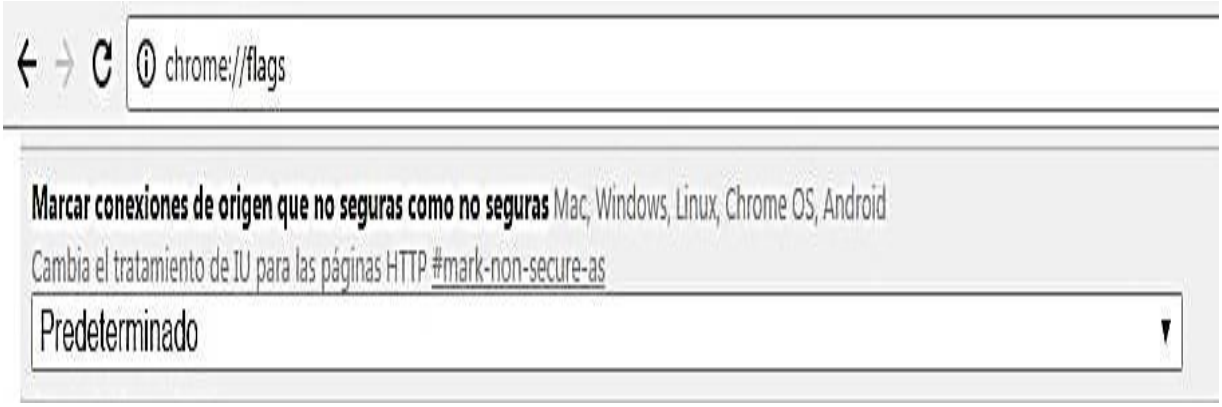


Figura 18. Modificación de los valores en buscador Chrome (Propio, 2017)

2.7.4 Análisis de URL sospechosas

Como medida adicional en los accesos a páginas web, que se miren sospechosas, y que se declinen en el robo de credenciales de sitios tales como Gmail, se pude recurrir a servicios online, para verificar si se tratan de una URL maliciosa o no, antes de realizar actividades en dicho sitio, uno de estos servicios es virus total.

Como se muestra en la figura 19, que pide al usuario introducir una URL y este servicio nos arroja un informe detallado de dicha URL con el cual obtenemos un resultado de un análisis, con la finalidad de identificar virus, gusanos, troyanos y contenido malicioso.

El propósito que se tienen estos servicios online es mejorar la seguridad personal por medio de la creación de herramientas y servicios gratuitos. Los cuales se llevan por lo general 30 segundos el análisis completo que a su vez

colaboran a la actualización de estas bases de datos, para su mejora y mantener a los usuarios alerta.

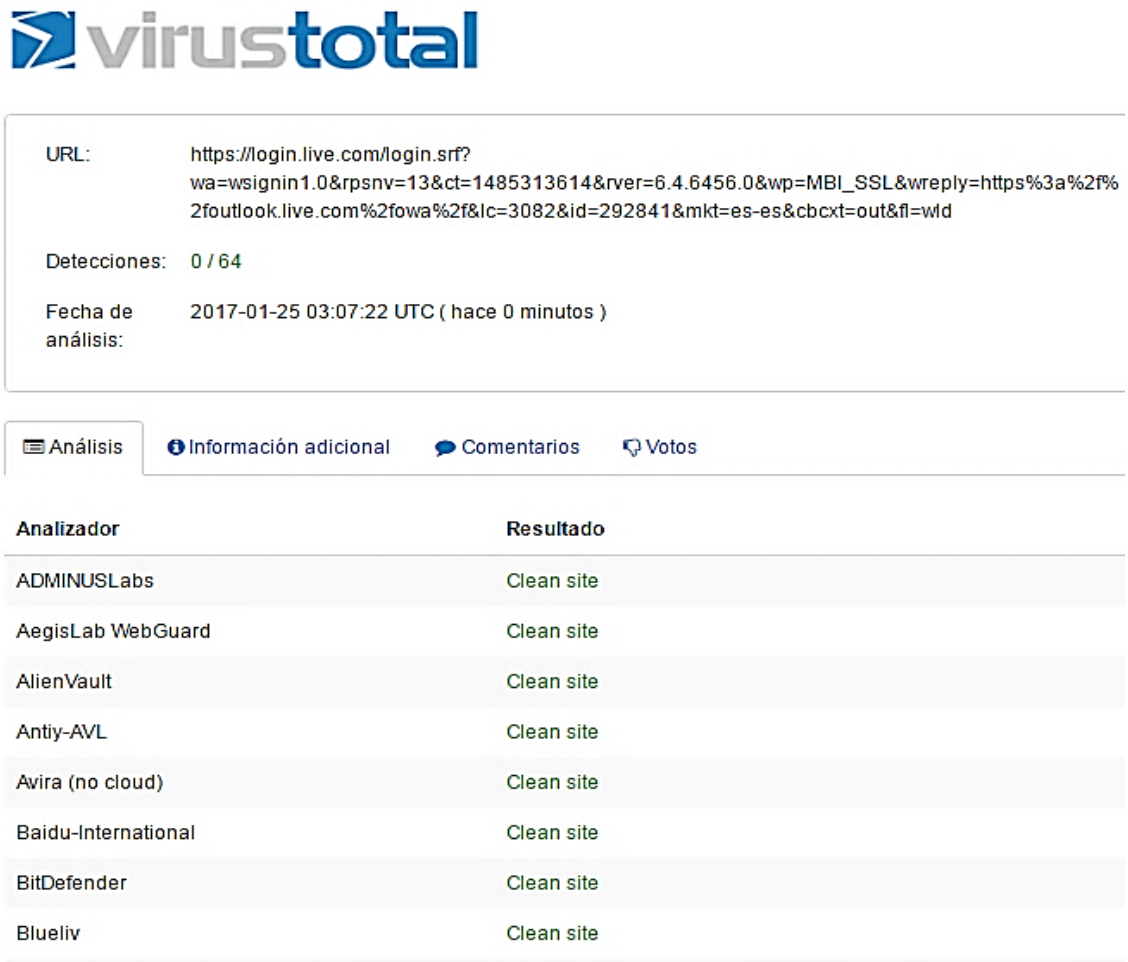


Figura 19. Análisis de URL con virus total (Propio, 2017)

Entre otros servicios online para el análisis de URL sospechosas, se encuentra URLVoid que funciona a base de reportes de listas negras y de reputación, realizados hacia paginas sospechosas o fraudulentas conforme la seguridad.

Dado en casos de descargas de contenido de gran demanda y su libre propagación por medio de enlaces fraudulentos, donde el principal objetivo es la no correspondencia de las necesidades del usuario, al hacer uso de estos servicios se estará más confiado en que la descarga es proveniente de un sitio libre de malware.

Como se ve en la figura 20 a principio arroja su primer resultado sobre amenazas activas, en el caso de la imagen no se encontraron amenazas o hubo reporte.

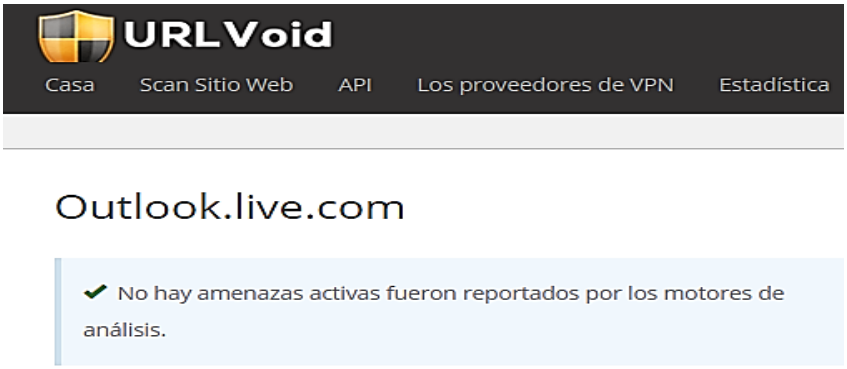


Figura 20. Análisis de URL con URL Void (Propio, 2017)

Figura 21, reporte detallado e información relevante a considerar, tal como dirección IP, propietario, región, etc.

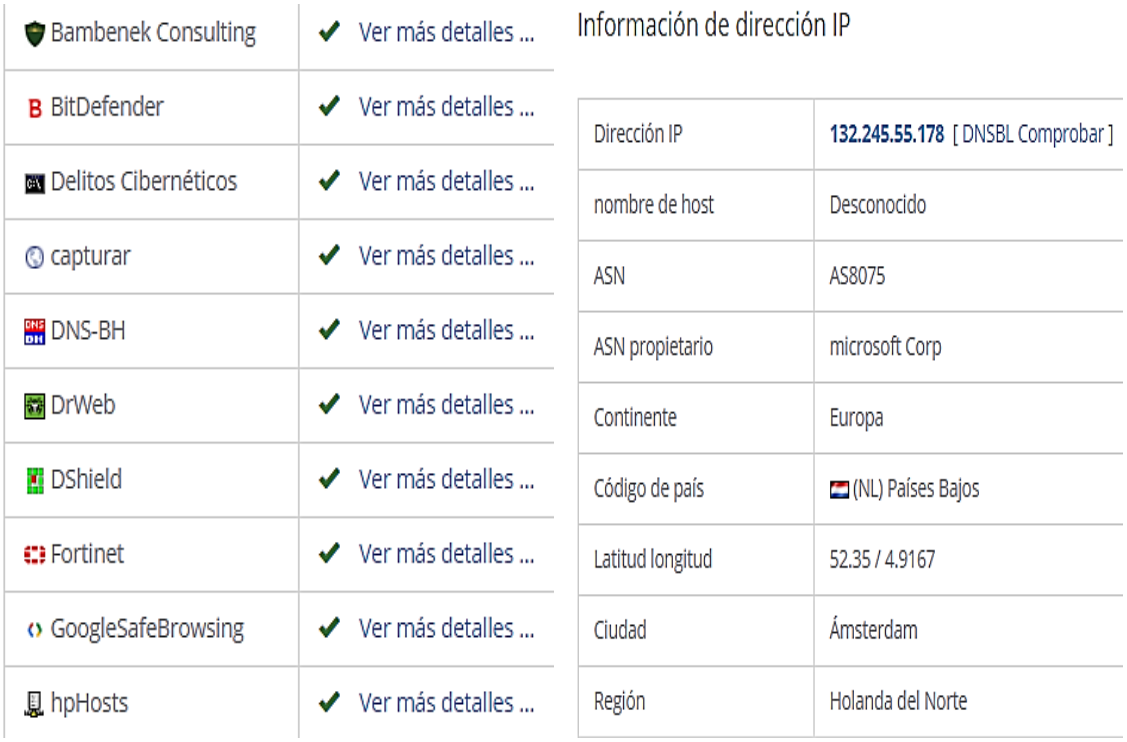


Figura 21. Reporte de URL con URL Void (Propio, 2017)

2.8 SOFTWARE PREVENTIVO

Al hacer uso de herramientas basadas en software, las cuales pueden ser comerciales o de código abierto, permitirán conocer el comportamiento de la red y obtenido estos resultados realizar cambios o cuestionar si el uso es adecuado de dicha red.

Existe un gran número de herramientas que son útiles para estas tareas por lo cual se menciona una distribución de Linux enfocada en la auditoria de seguridad, se retoma en base a que es gratis, mantiene una gran cantidad de documentación referente a cada herramienta que se puede adquirir, así como su compatibilidad y soporte a una gran variedad de dispositivos inalámbricos permitiendo la variedad de hardware.

2.8.1 Kali LINUX

Distribución GNU/Linux reorganizada para el análisis de seguridad, en uso profesional, con la cual se pueden tener un conjunto de herramientas dedicadas y orientadas a diferentes tareas en el ámbito de la seguridad informática, es útil para analizar las debilidades de seguridad en las redes, para así mantener nuestros sistemas seguros.

Entre las razones que se propone es por su usabilidad y rendimiento, además de ser de ámbito profesional, desarrollados solo para fines de los cuales está desarrollado.

"En la parte técnica su entorno se muestra liviano, abasteciendo de necesidades donde el tiempo de tener la herramienta funcionando es corto utilizando la virtualización del sistema". Documentación kali (2017).

Se puede mencionar aspectos en que destaca:

- Personalizable por los gustos de cada usuario.

- Posible utilización sin necesidad de modificación del equipo de cómputo ya que puede ser iniciado desde un LiveCD o LiveUSB.
- Entornos de desarrollo seguro, en el manejo de repositorios y manejo de protocolos seguros.
- Variedad de entornos gráficos (KDE, GNOME, XFCE).
- Multi-lenguaje manejo de soporte multilingüe para su manipulación.
- Utilización para proyectos domésticos o personales.
- Arquitectura de 32 y 64 bits.

Entre otros aspectos están los requerimientos ya definidos.

- Un mínimo de 8 GB de espacio en disco para la instalación de Kali Linux.
- Para las arquitecturas i386 y amd64, un mínimo de 512 MB de RAM.
- Lectora de CD/DVD / Soporte para iniciar desde una memoria USB

Hoy en día en internet hay un sin fin de software, dedicado tanto para la obtención de contraseñas para el acceso no permitido a redes wifi, así como para mantener las redes seguras. Pero dicho software se mantiene ejecutándose en segundo plano consumiendo espacio en disco duro varios de los servicios que contiene.

Además de no buscar escalabilidad, soporte, organización clara y precisa de cómo se manejan las tecnologías contenidas en estos. Al contar con estas carencias al ser descargados de sitios no seguros se pone en riesgos los equipos de cómputo. Un ejemplo de este software se puede nombrar:

Wifislax: Que aun que es parte de una distribución GNU/Linux en formato *.iso, y tiene la finalidad de la auditoria de seguridad. Es conocido por tener un concepto distinto a kali Linux, con el enfoque de uso no permitido de redes

inalámbricas, seguido de tener una gran cantidad de versiones disponibles y el manejo de este material en sitios inseguros poniendo en riego nuestros ordenadores.

Retomando acerca del software propuesto se puede decir que con la gran variedad de herramientas, que se proporcionan se pretende detectar vulnerabilidades, malas configuraciones, wireless no seguras que puedan provocar el robo de información sensible. Las herramientas más utilizadas serán descritas para conocer su funcionamiento y aplicarlas a necesidades que se tienen.

Como primer acercamiento a en la figura 22, entre el menú se puede ver la herramienta nmap la cual se explica a continuación.

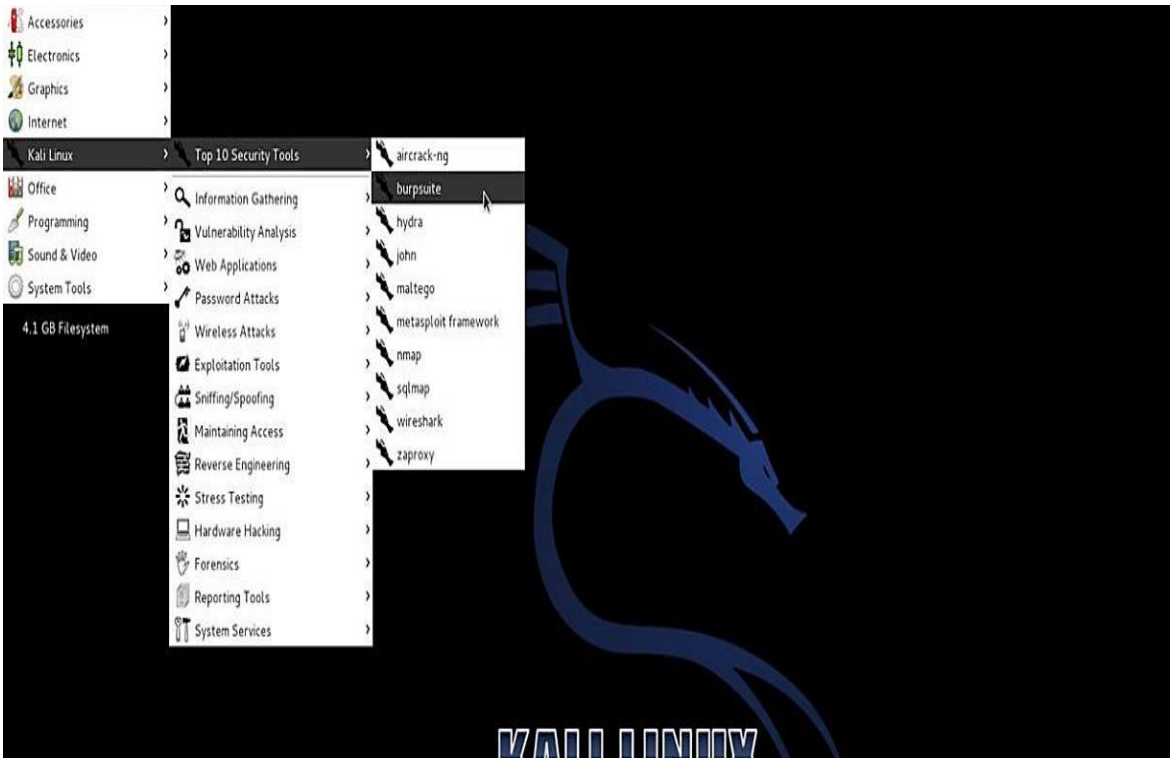


Figura 22. Entorno Kali Linux (Propio, 2017)

Dichas redes wireless generan gran atención, por la demanda de conexiones a internet, y es ahí donde inician las principales preguntas de su funcionamiento para los accesos a internet.

Para el funcionamiento correcto de la distribución expuesta y algunos de los pasos que se exponen, es importante mencionar el uso de un adaptador wifi USB, el cual trabaja bajo los estándares IEEE 802.11, que tienen la capacidad de ser configurado en modo monitor para la recepción de paquetes provenientes de las zonas wifi.

Dicho adaptador para su arranque solo necesita la instalación de un controlador localizándolo con el número de serie y arquitectura de nuestro ordenador, el cual para cada modelo hay un archivo.tar en la página oficial de *www.alfa.com*

Mediante kali se puede realizar primeramente una evaluación de la información que se tiene sobre la red en específico, de la cual se tiene la autorización de acceso para la realización de diferentes tareas que se menciona a continuación y para ello se describe de manera breve la herramienta:

Nmap: Esta función se ejecuta por medio de consola de comandos para el rastreo de puertos y se usa para evaluar la seguridad de sistemas informáticos, así como descubrir servicios o servidores en una red informática entre algunos de los usos que se le dan están.

-Identificación de los equipos de una red.

-Identificación de puertos abiertos de una computadora objeto.

-Determina que servicios se están ejecutando en la misma.

-Obtención de características del hardware de la red de la maquina testeada.

-Reconocimiento del sistema operativo

-Filtros en uso y cortafuegos

Dichas funciones aplican él envió de paquetes para la realización de análisis y como finalidad arrojar un resultado a base de reportes.

En la figura 23 se hace la petición de host y rutas por medio del comando: *nmap --iflist*

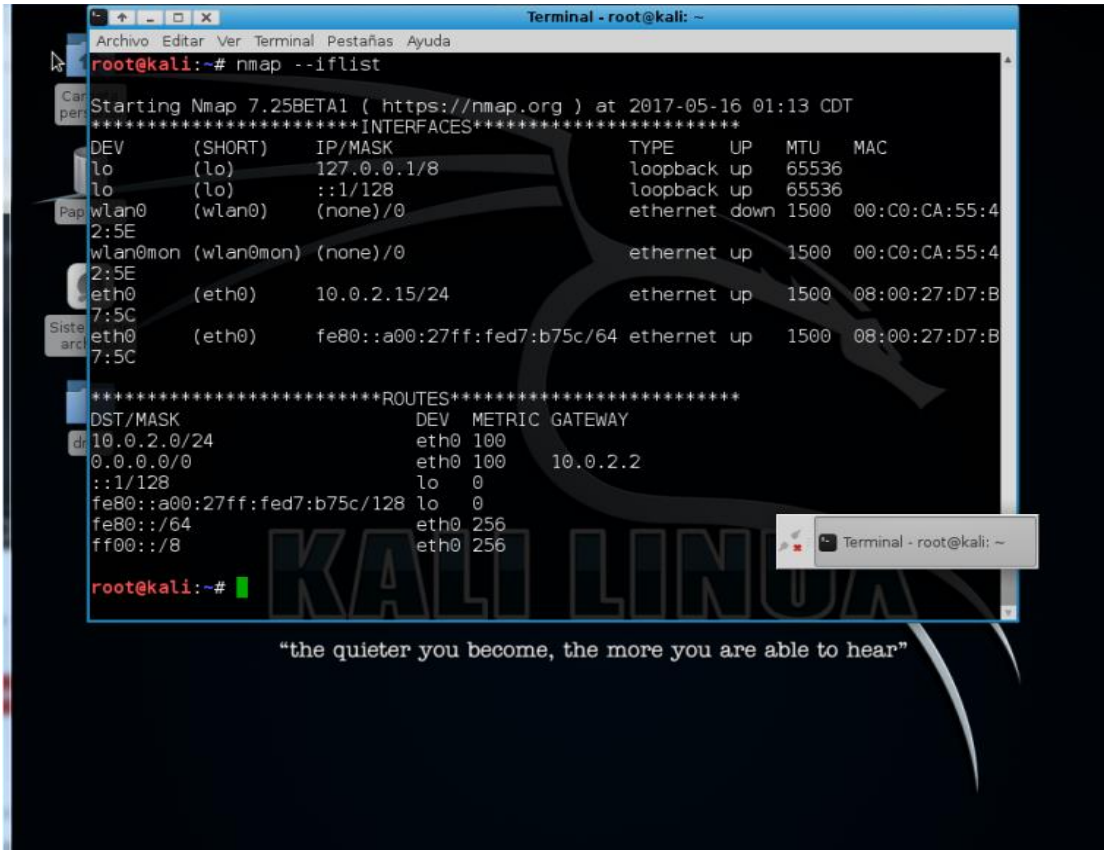


Figura 23. Recepción de interfaces y rutas por medio del comando nmap (Propio, 2017)

En la figura 24, se puede ver las demás herramientas wireless que se destacan.

Figura 24. Herramientas wireless kali Linux (Propio, 2017)

La variedad de herramientas Suite air: Como puede ser aircrack-ng, airmon-ng, airodump-ng, airbase-ng, etc. Con estas se logra hacer una búsqueda de vulnerabilidades en nuestras redes inalámbricas.

Cada una de estas se ejecutan por medio de comandos de consola, al iniciar una terminal solo con tener datos de la red tales como nombre de la red, canal de frecuencia, dirección Ip, etc.

Airmon-ng: Se modifica el modo en que trabaja la tarjeta inalámbrica a modo monitor, si la tarjeta dispone con esta característica.

En la imagen 25 se introduce el comando “airmon-ng” para el reconocimiento de nuestra tarjeta inalámbrica.

Figura 25. Reconocimiento de la tarjeta de red (Propio, 2017)

Y como se logra ver en la figura 26, se inicializa con el comando “airmon-ng start wlan0mon”

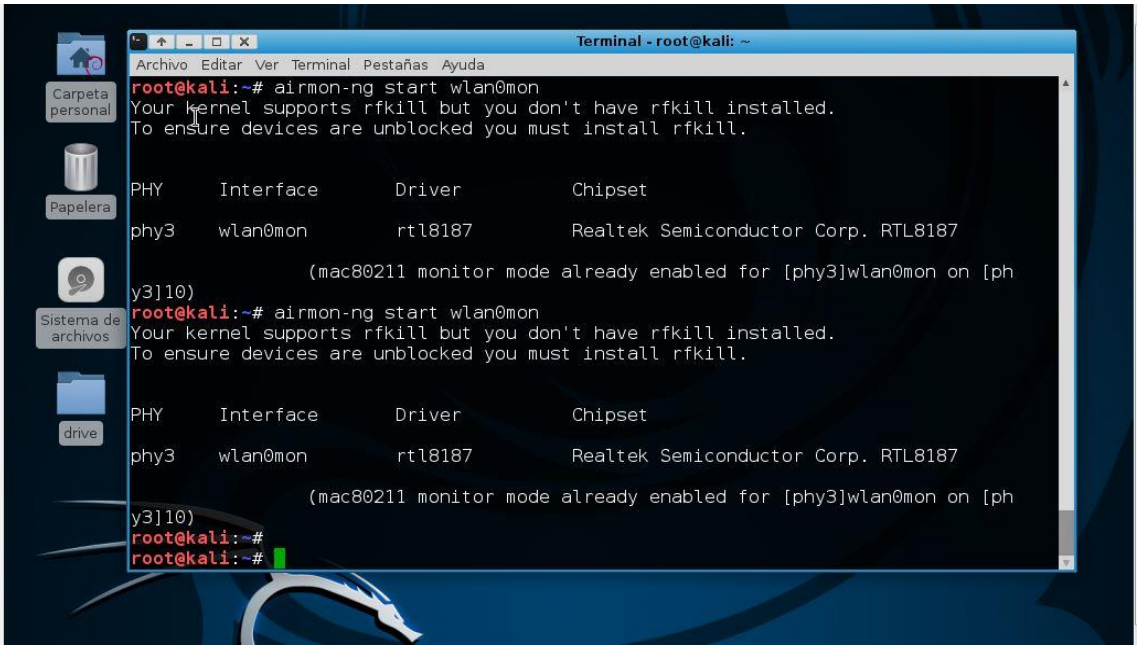


Figura 26. Tarjeta de red en modo monitor (Propio, 2017)

***Airodump-ng*:** Con esta herramienta se logra escuchar el tráfico que circula por el aire, con ayuda de la interfaz en modo monitor. Con este proceso se logran obtener identificación de la dirección MAC, intensidad de la señal, dirección Mac de un cliente asociado, tipo de cifrado de datos, método de autenticación, nombre de la red, etc.

Y con la utilización de airodump-ng y el nombre de la interfaz para recopilar información en este caso “airodump-ng wlan0mon” como se ve en la figura 27.

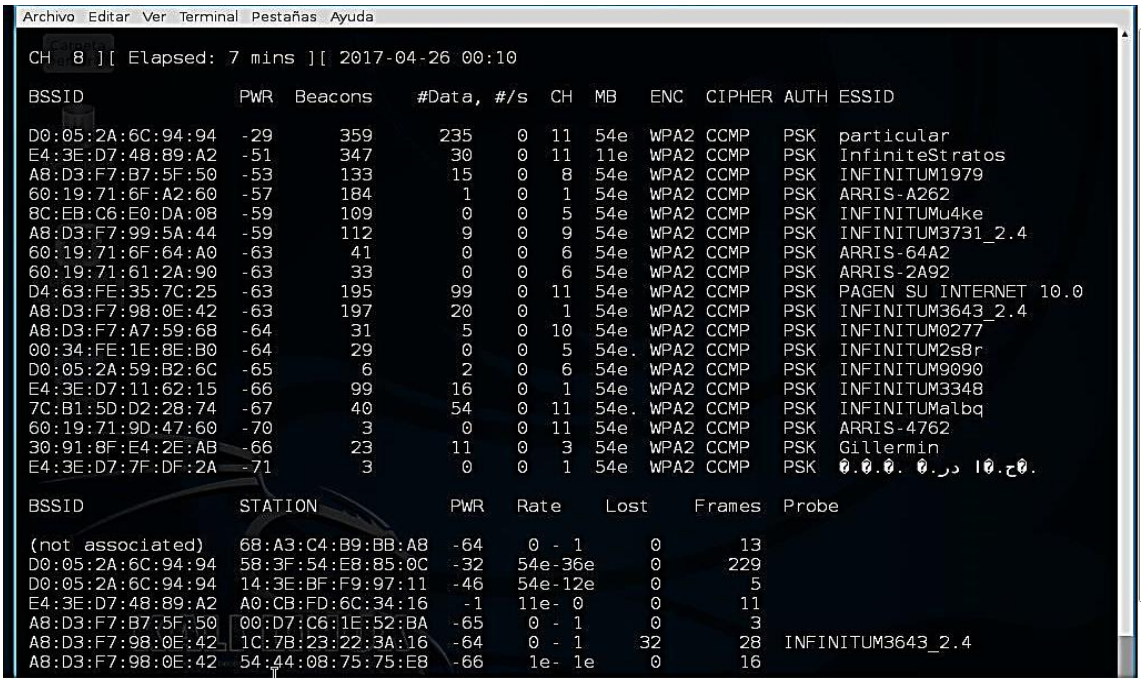


Figura 27. Escucha de tráfico con airodump-ng (Propio, 2017)

Este procedimiento presentado de igual forma se utilizara en demás casos más adelante. Entre las demás herramientas que se destacan y están integradas se menciona.

***Airolib-ng*:** Permite almacenar y manejar listas de ESSID y contraseñas, calcula las PMKs, Pairwise Master Keys y usarlas para el crackeo WPA/WPA2.

Aircrack-ng: Herramienta para ataques de fuerza bruta, diccionarios, estadísticos a capturas de tráfico a consideración del cifrado de la red y método que se quiera utilizar.

Para la búsqueda de claves por medio de fuerza bruta, está lográndola con una gran cantidad de combinaciones posibles y una cantidad de horas para el chequeo de cada una de estas contenidas en diccionarios se utilizan las herramientas que se describen a continuación.

Entre las demás herramientas importantes están:

Cowpatty: permite el realizar fuerza bruta por medio de diccionarios sobre el protocolo WPA y WPA2.

Kismet: Sniffer para localización de redes wifi, se basa en el protocolo 802.11, soporta cualquier tarjeta que soporte modo monitor y que pueda escuchar tráfico de redes 802.11b, 802.11a, 802.11g, 802.11n.

***Wifite*:** herramienta dedicada en la auditoria de redes basado en la configuración de WPS en redes con utilización de cifrado WEP/WPA, en su menú se muestran las acciones que se pueden realizar y no es enredoso su uso.

Reaver: Su función es realizar fuerza bruta contra el pin de WPS, consiguiendo la recuperación de los dígitos que conforman la contraseña. En la mayoría de routers modernos está incluida esta función WPS y en al tener valores por defecto pueda encontrarse activo.

2.8.2 Ataque Reaver

Al descuidar la configuración del punto de acceso con respecto a esta función que se encuentre habilitada, surge la posibilidad de uso de esta técnica mediante envió de cadenas de caracteres con el propósito de una coincidencia, a continuación se demuestra de manera breve.

En la figura 28 y 29, se realiza el reconocimiento de adaptador inalámbrico.

Figura 28.Comando necesario (Propio, 2017)

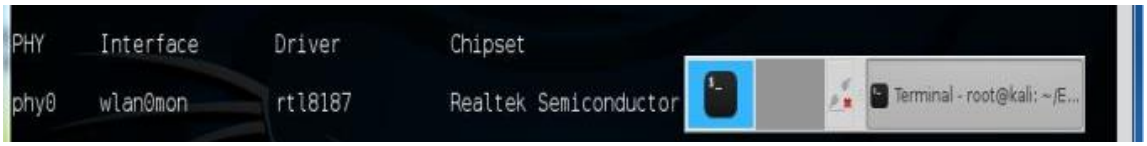


Figura 29. Reconocimiento del adaptador (Propio, 2017)

En la figura 30, se puede ver la inicialización de la interfaz en modo monitor

Figura 30. Inicialización del adaptador para captura (Propio, 2017)

En la figura 31, se realiza el análisis de router para verificar si se tiene activada la función de WPS por medio del comando “wash”.

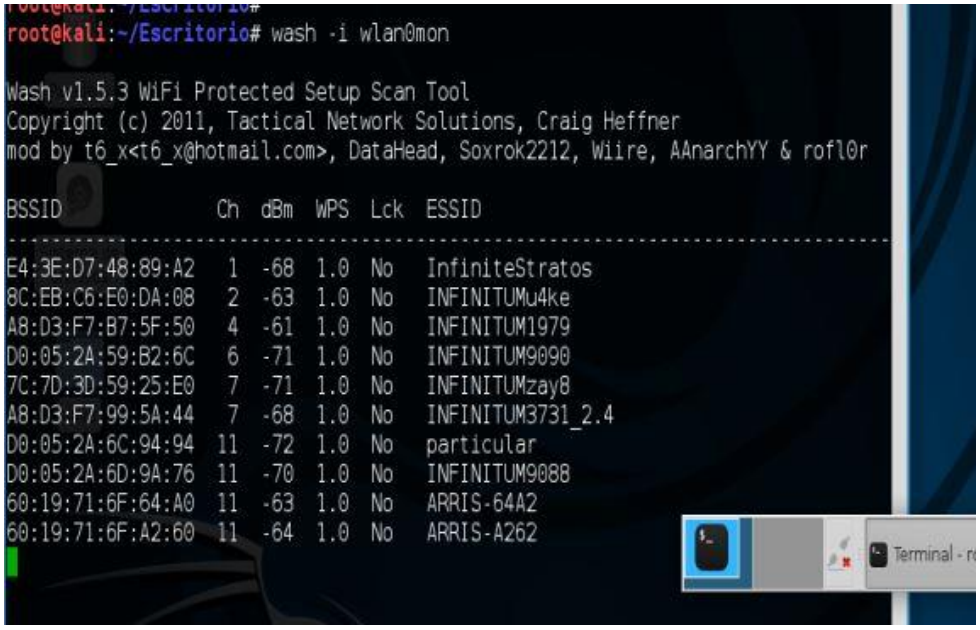


Figura 31. Utilización del comando wash (Propio, 2017)

Se puede observar si dicha red cuenta con la función reaver bloqueada, al tener un *no* como resultado se puede utilizar el siguiente comando.

En la figura 32, se ve la utilización del comando “reaver”, añadiendo los argumentos requeridos, y se pueden ver los opcionales para dicha acción.

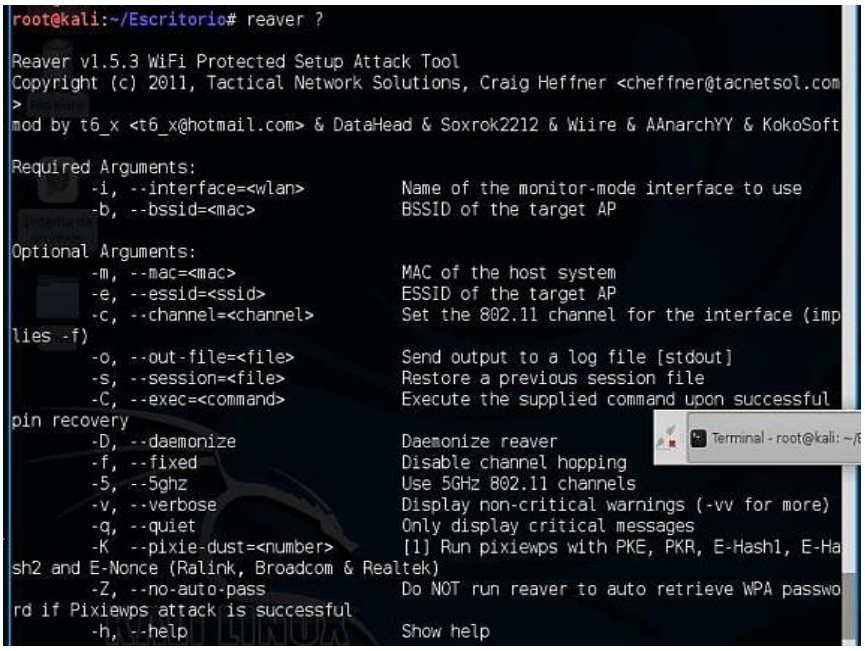


Figura 32. Argumentos y opciones del comando “reaver” (Propio, 2017)

En la figura 33 se hace uso de los argumentos necesarios en el comando y se ejecuta.

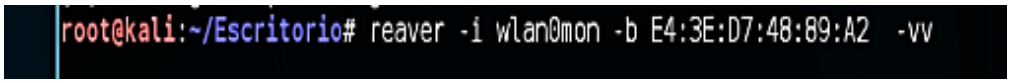


Figura 33.Utilización del comando “reaver” (Propio, 2017)

En la Figura 34, podemos darnos cuenta que comienza el envío de mensajes que llevan a cabo el proceso de fuerza bruta para la obtención de pin WPS.

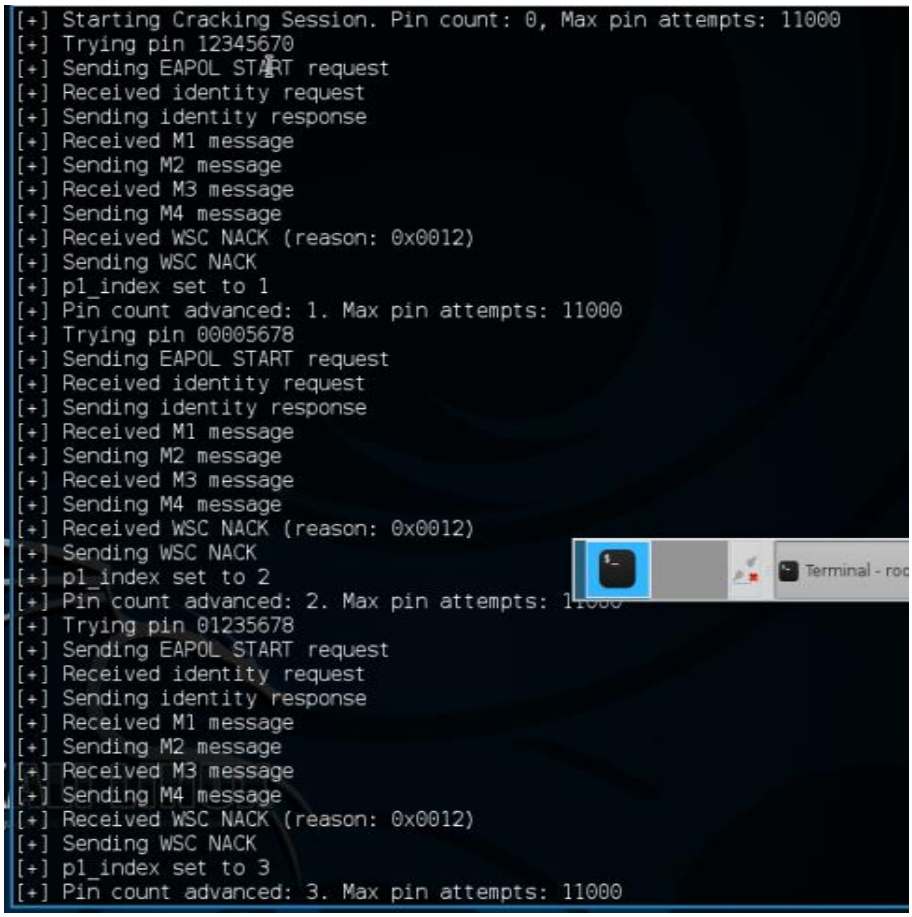


Figura 34. Envió de mensajes (Propio, 2017)

Dicho proceso puede ser muy tardado, pero se puede conseguir dicha conexión.

Como punto final se logra la obtención del pin WPS para conexiones por medio de esta función, como se puede ver en la imagen 35.

Figura 35. Obtención de PIN por medio de comando “reaver” (Propio, 2017)

2.8.3 Ataques WPA/PSK

A la hora de la autenticación de usuarios para la disposición de los recursos de la red en un hogar o pequeña empresa, esta puede ser de la forma WPA-PSK donde las conexiones se dan por medio de una clave manualmente generada conocida por los usuarios, la cual en conjunto con procesos entre algunos están, métodos temporales, aplicación de robustez en inicialización de 48 bits, secuenciación, intercambio de variables aleatorias, etc. En el caso de conexiones robustas hay necesidades especiales para proveer servicios con la característica de almacenar cada usuario con un nombre y una contraseña, como es el caso del servidor radius.

En la búsqueda para establecer comunicación con una red cercana que tienen implementada la autenticación WPA/PSK se debe tener noción de algunos conceptos siguientes.

- ESSID: Extended Service Set ID nombre para la identificación de la red.
- SSID (Service Set Identifier): dirección MAC del punto de acceso a conectarse.
- Supplicant: Conocido como el cliente.
- Authenticator: Punto de acceso.
- MIC: Código de integridad de mensaje, con este se hace la comprobación de que la información no ha sido alterada durante él envió.
- *Handshake:* Su nombre hace referencia a un apretón de manos, trasladado hacia las redes es un saludo entre el router wifi a un equipo que solicita la conexión, pasando información para su futura conexión de esta manera los ataques van enfocados hacia ese handshake, la

característica de esta recolección de información es que es mucha y es cifrada.

Por lo que es necesario pasarle esa información a un diccionario para que se realice la comparación de palabras, hasta que se logre la coincidencia de estas.

- WPA: Se maneja el cifrado RC4 y utiliza un mecanismo de generación de clave dinámica aleatorio entre el punto de acceso con el cliente, para cada sesión se utiliza un par de claves distinto a los demás clientes conectados, normalmente es usada la función PBKDF2.
- WPA2: mecanismo de cifrado por medio del algoritmo AES de gran complejidad, comparte la misma característica del manejo de 128-156 bits y se manejan tramas convertidas por operaciones matriciales.
- PBKDF2: Con este algoritmo se genera la llave psk (pre-shared key) que se caracteriza por la creación de una clave de 8 y 63 caracteres, lo que se ve al tener seguridad WPA considerando:

  a) Clave del access point

  b) SSID

  c) Longitud de SSID

  d) Número de codificación de passphrase(Contraseña)

  e) Longitud de clave psk

- PMK: Pairwise Master Key, combinación de caracteres para el establecimiento de conexión, la cual es guardada por el usuario o dispositivo conectado posteriormente de la conexión satisfactoria, ya que solo se usa una vez en la identificación y establecimiento de conexión.

- PSK: Cadena de 256 bits o de manera alternativa una frase de 8 a 63 caracteres utilizada de manera secreta y vulnerable en redes no robustas, proveniente del punto de acceso utilizado la comunicación WPA, esta no es utilizada directamente como autenticación de un cliente en el punto de acceso.

  La cual es compartida por usuarios y punto de acceso. “Donde el cliente acepta la cadena, es encriptada o codificada y si dicha clave recibida por el cliente coincide con la cadena original enviada al cliente se realiza la conexión” (CCNA, pág.102, 2011).

- PTK: Claves generadas por cada paquete que se intercambia entre los suplicant (clientes) y Authenticator (punto de acceso) utilizando las PSK generadas por cada una de las dos entidades retomando datos tales como Mac de punto del acceso, MAC cliente, dos valores creados aleatoriamente Anonce y Snonce .

- Rainbow tables: Tablas de búsqueda para la realización de ataques de fuerza bruta por medio cientos de SSID computados por medio de diccionarios.

- Fichero .Cap: Archivo generado tras la ejecución de un sniffer.

Estos conceptos van relacionados en el proceso que se lleva para la conexión entre un punto de acceso y un cliente en conexión por medio de la configuración WPA-PSK, lo cual se puede ir desglosando con los siguientes puntos.

Para su mayor comprensión, se manejaran por medio de puntos. Y en algunos de los casos se describen con imágenes de cómo se miran algunos de estos datos con la utilización del software Wireshark.

La comunicación de las dos entidades se inicia con él envió de un paquete “eapol start” del cliente hacia el punto de acceso.

1) El punto de acceso envía un mensaje al punto de acceso, con una cadena de valores aleatorio (ANonce), esto se puede ver en la figura 36.

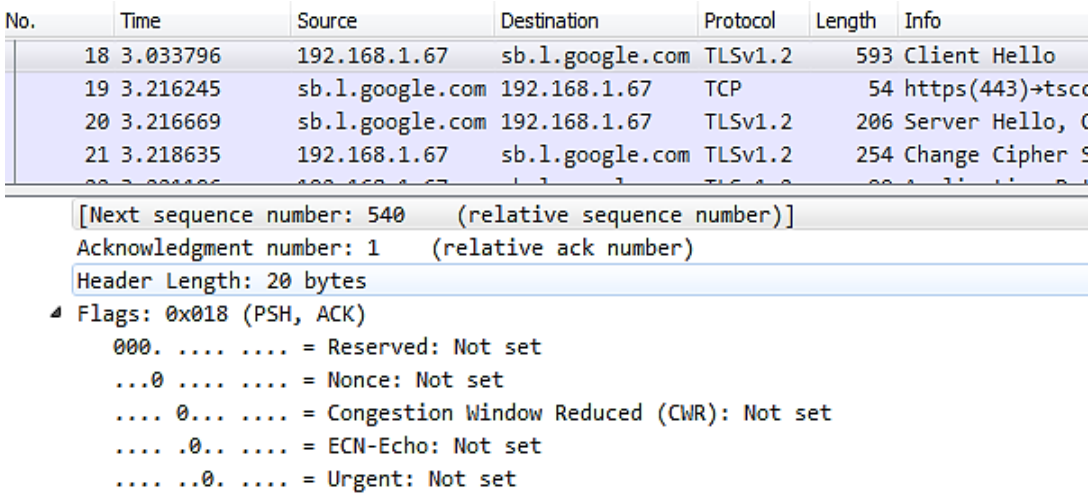


Figura 36. Cadena Nonce (Propio, 2017)

2) El cliente recibe esta cadena y es generada otra cadena aleatoria con el nombre de Snonce con las mismas características del punto 1, solo que este de parte del cliente.

Lo siguiente es generar una clave PMK la cual en pasos posteriores, es retomada en procedimiento de autenticación en donde se involucra información propia de cada entidad.

3) En este paso se hace uso del algoritmo PBKDF2 que tiene como finalidad una clave de 256 bits. Donde se consideran los siguientes parámetros.

   PMK= PBKDF2 (Frase secreta, ESSID, longitud (ESSID), 4096, 256)

4) El cliente realiza el PTK (claves temporales) para cada cadena intercambiada, aplicando una función aleatoria PRF-X. Donde se involucran los datos de:

   -PMK: llave creada a partir de la psk y en base a proceso de modificaciones donde se involucran

   -SNonce

   -ANonce

   -Direccion MAC punto de acceso

   -Direccion MAC Cliente

   Como valor final se obtendrá un valor MIC que este fue realizado por las operaciones de integridad mediante algoritmo Michael, direcciones MAC de las dos entidades quien envía y recibe y una parte de PTK. Todo esto alterado mediante una función hash HMAC_MD5.

5) Posteriormente forzosamente los MIC de las dos instancias deben coincidir y se establece el valor de 1, como se ve en la figura 37.

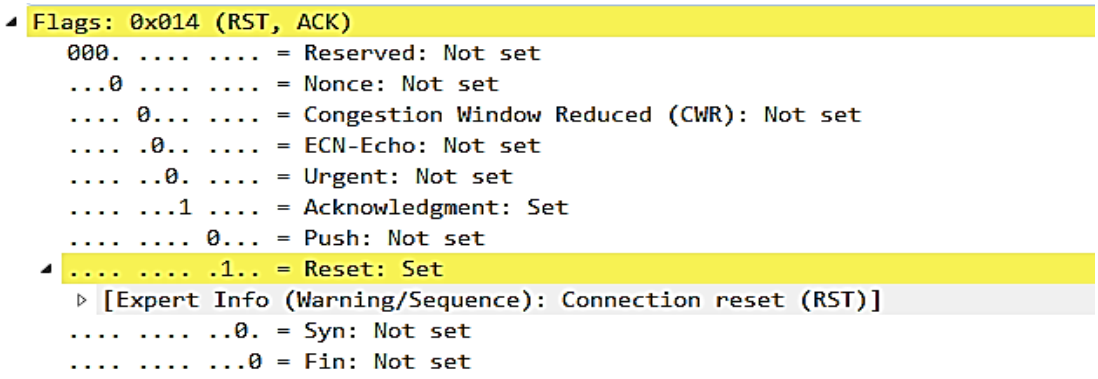


Figura 37. Reconocimiento de las MIC y se establece un 1 en Acknowledgment (Propio, 2017)

6) El punto de acceso manda un mensaje de instalación de la llave y finaliza el proceso.

7) Si la coincidencia de MIC, falla se manda mensaje de desautenticación.

En breve se pueden resumir dichos pasos en la siguiente figura 38. Donde se hace uso de un diagrama para su mayor comprensión.

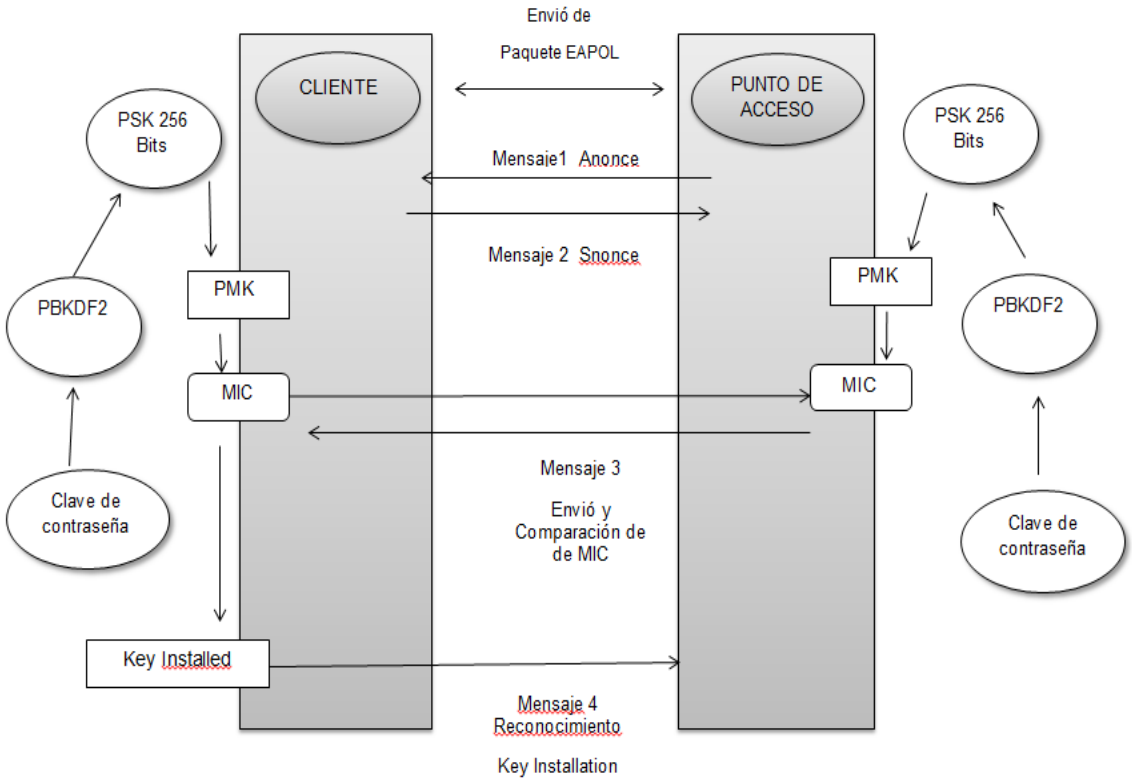


Figura 38. Diagrama de proceso de reconocimiento de cliente (Propio, 2017)

2.8.4 Estimación de WPA-PSK

En el caso de la búsqueda de contraseñas enfocadas a WPA-PSK se basan a la estimación, retomando la etapa de autenticación (handshake), para ello se pueden analizar el siguiente ejemplo con similitudes en algunos puntos de los anteriores. Y teniendo 4 pasos principales.

a) Captura de paquetes donde se pueda obtener SNonce

b) Captura de direcciones MAC del punto de acceso

c) Buscar la captura de MIC proveniente del punto de acceso.

d) Con los datos recabados realizar una previa clave MIC de igual forma con la función HASH SHA1

e) Realización de una comprobación de MIC creado con el del punto de acceso para verificar que se obtuvo la psk.

En el siguiente caso se iniciara la interfaz airmon-ng, e iniciando en modo monitor tal y como se muestra en la figura 39.

Figura 39.Inicializacion de herramienta airmon-ng (Propio, 2017)

Posteriormente se necesita por medio de airodump, ver el tráfico inalámbrico que nos rodea cerca de nuestro portátil, como se puede apreciar en la figura 40.

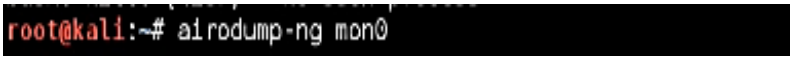
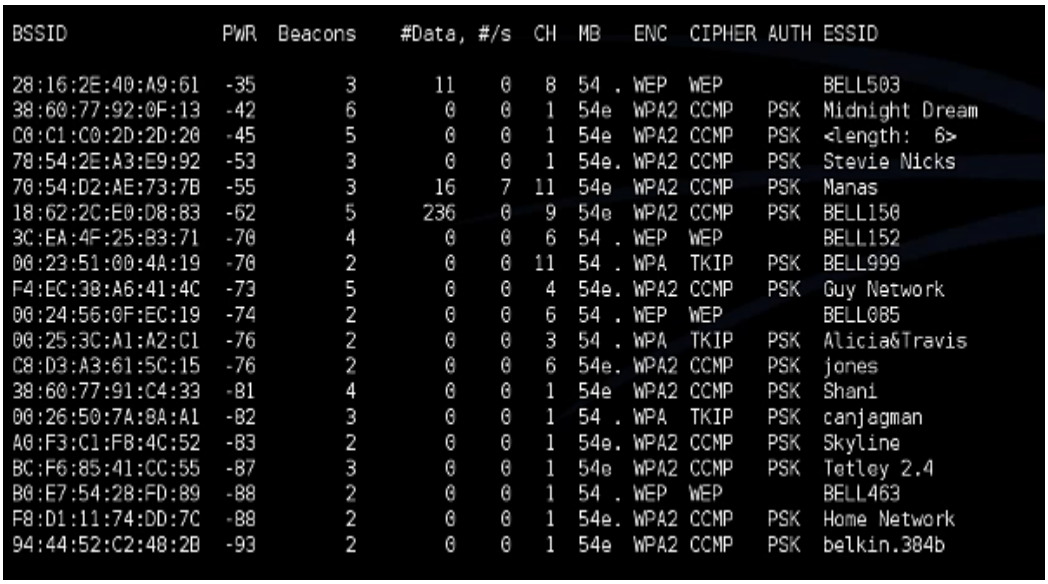


Figura 40.Ver tráfico por medio de airodump (Propio, 2017)

En la figura 41, se muestran las redes disponibles y un poco de información sobre estas.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
28:16:2E:40:A9:61	-35	3	11	0	8	54 .	WEP	WEP		BELL503
38:60:77:92:0F:13	-42	6	0	0	1	54e	WPA2	CCMP	PSK	Midnight Dream
C0:C1:C0:2D:2D:20	-45	5	0	0	1	54e	WPA2	CCMP	PSK	<length: 6>
78:54:2E:A3:E9:92	-53	3	0	0	1	54e.	WPA2	CCMP	PSK	Stevie Nicks
70:54:D2:AE:73:7B	-55	3	16	7	11	54e	WPA2	CCMP	PSK	Manas
18:62:2C:E0:D8:83	-62	5	236	0	9	54e	WPA2	CCMP	PSK	BELL150
3C:EA:4F:25:83:71	-70	4	0	0	6	54 .	WEP	WEP		BELL152
00:23:51:00:4A:19	-70	2	0	0	11	54 .	WPA	TKIP	PSK	BELL999
F4:EC:38:A6:41:4C	-73	5	0	0	4	54e.	WPA2	CCMP	PSK	Guy Network
00:24:56:0F:EC:19	-74	2	0	0	6	54 .	WEP	WEP		BELL085
00:25:3C:A1:A2:C1	-76	2	0	0	3	54 .	WPA	TKIP	PSK	Alicia&Travis
C8:D3:A3:61:5C:15	-76	2	0	0	6	54e.	WPA2	CCMP	PSK	jones
38:60:77:91:C4:33	-81	4	0	0	1	54e	WPA2	CCMP	PSK	Shani
00:26:50:7A:8A:A1	-82	3	0	0	1	54 .	WPA	TKIP	PSK	canjagman
A0:F3:C1:F8:4C:52	-83	2	0	0	1	54e.	WPA2	CCMP	PSK	Skyline
BC:F6:85:41:CC:55	-87	3	0	0	1	54e	WPA2	CCMP	PSK	Tetley 2.4
B0:E7:54:28:FD:89	-88	2	0	0	1	54 .	WEP	WEP		BELL463
F8:D1:11:74:DD:7C	-88	2	0	0	1	54e.	WPA2	CCMP	PSK	Home Network
94:44:52:C2:48:2B	-93	2	0	0	1	54e	WPA2	CCMP	PSK	belkin.384b

Figura 41.Resultados de redes disponibles (Propio, 2017)

Para analizar el canal de una red, se requiere la creación de un archivo, en la figura 42 se ve la instrucción donde se especifica dicha red por medio de su BSSID o dirección MAC, además de canal y nombre del archivo.

Figura 42. Análisis de canal (Propio, 2017)

Automáticamente se empezara a realizar la consulta de dicha red en específico y se muestran los datos principales de esta red, obteniendo la recepción de paquetes en el archivo con el nombre defcon, este procedimiento se dejara funcionando para el trabajo en conjunto con demás pasos más delante.

En la imagen 43 se muestran algunas de las iteraciones de dichos paquetes.

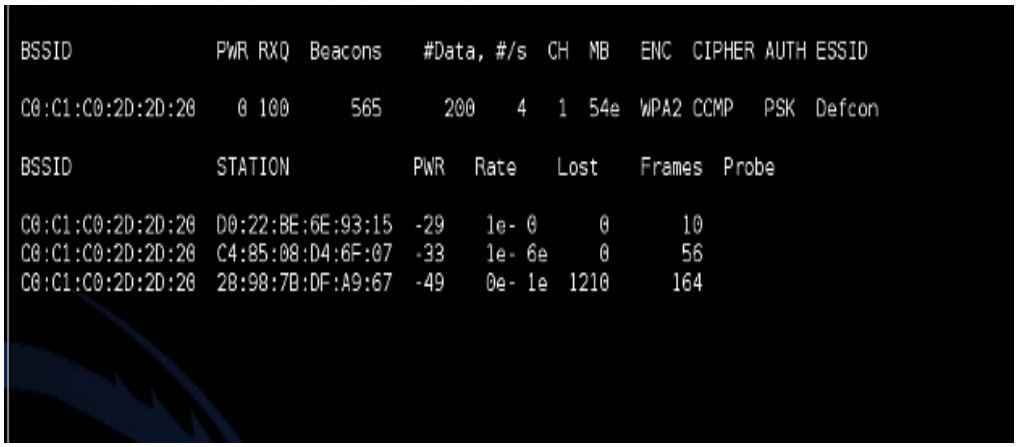


Figura 43. Búsqueda de un apretón de manos (Propio, 2017)

En la figura 44. Se invoca aireplay-ng para un envío de paquetes de desautenticación y se logra ver dicho envió.

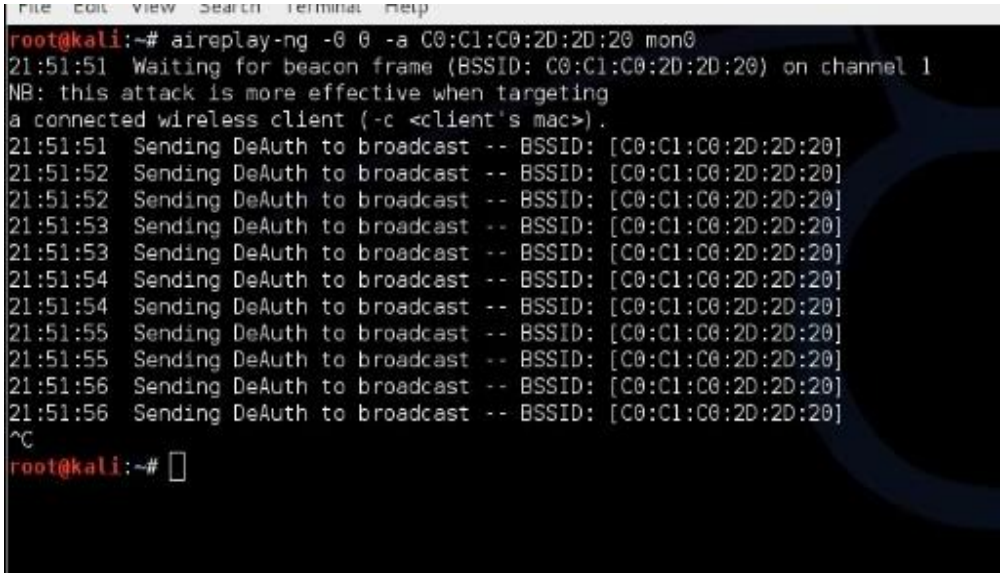


Figura 44.Envio de paquetes de autenticación (Propio, 2017)

Por otro lado se debe esperar que se logre un handshake con éxito, se muestra en la figura 45.

Figura 45. Apretón de manos con éxito (Propio, 2017)

En la figura 46 se muestra el archivo creado y muestra el apretón de manos.

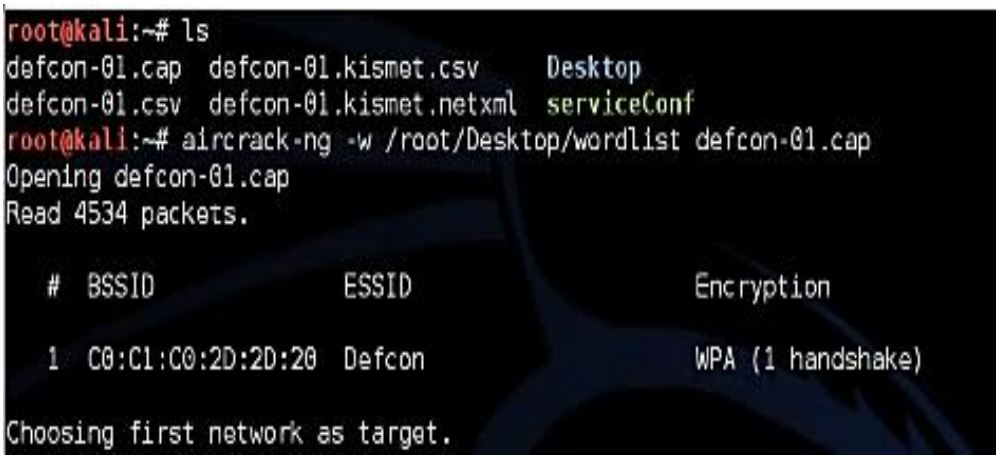


Figura 46. Apretón de manos con éxito (Propio, 2017)

Posteriormente se requerirá una lista de palabras figura 47, para hacer uso de la fuerza bruta.

Figura 47. Lista de palabras (Propio, 2017)

Y Se deben de retomar parámetros que se marcan, figura 48.

Figura 48.parametros a retomar (Propio, 2017)

En la figura 49, en conjunto con aircrack-ng se aplica la instrucción: *aircrack-ng –w wordList defcon-01.cap*

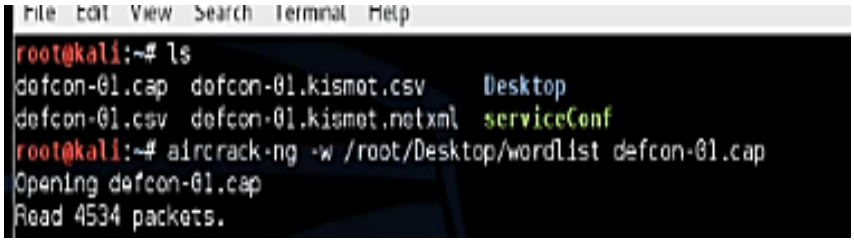


Figura 49. Uso de la lista de palabras (Propio, 2017)

Con uso de los recursos de la computadora se empezaran a analizar, todas las palabras posibles y su concurrencia, en la búsqueda puede ser similar a la figura 50.

Esto puede generar bastantes horas para poder lograr la coincidencia de la contraseña en algunas ocasiones no se logra dar con esta, a causa de características que posee.

Figura 50. Búsqueda de coincidencia de clave (Propio, 2017)

Después de un largo tiempo de espera y si la contraseña fue fijada de manera no cuidadosa, se puede lograr obtenerla, y se obtendrá algo similar a como se muestra en la figura 51.

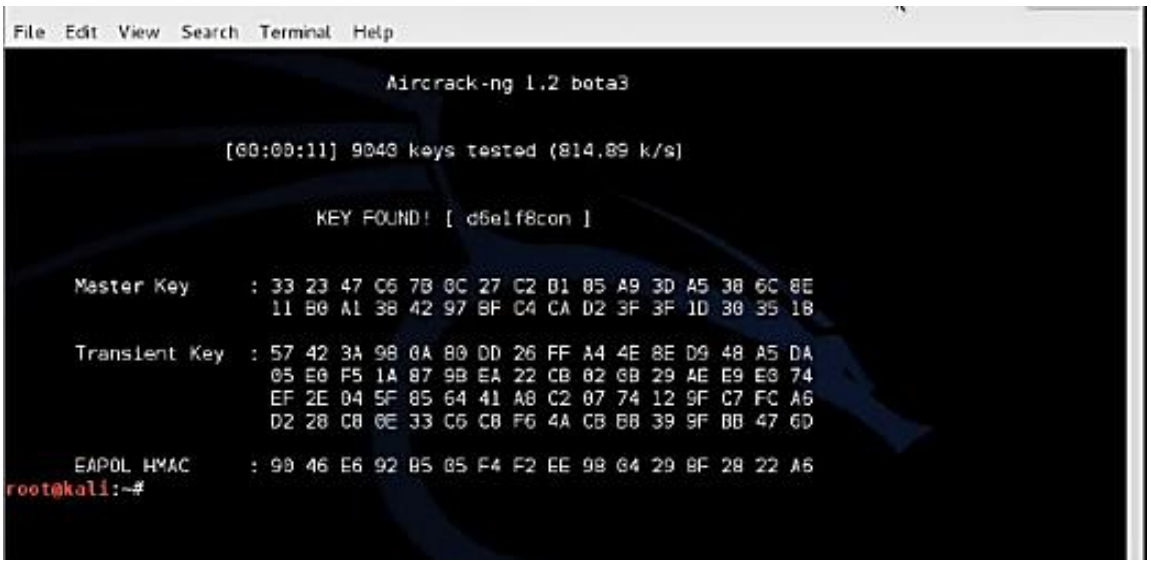


Figura 51. Final de análisis, coincidencia encontrada (Propio, 2017)

En las redes con cifrado WPA2 del estándar 802.11i, al manejar el algoritmo AES, se vuelve más complejo por la característica de su mecanismo de cifrado más robusto, siendo así la mejor opción en elección de protocolo de seguridad ya que maneja poca información en la transmisión de datos para que la confidencialidad e integridad sea mayor, aun teniendo como vulnerabilidad el uso de la fuerza bruta, este proceso se vuelve muy lento y se requiere de hardware con mayores recursos, obteniendo en la mayoría de los casos muy poco éxito.

CONCLUSIONES

La manipulación de los ordenadores y la gran gama de dispositivos móviles, hace retomar nuevos retos para el desarrollo, en aspectos tecnológicos, así mismo influyendo en las actividades tanto del hogar, transporte, trabajo y académicas fomentando la gran necesidad de las conexiones a internet. Con lo anterior se puede concluir que la seguridad wifi es altamente sensible al software protector.

El software protector dependerá del sistema operativo que emplee el usuario.

Las distribuciones Kali de Linux son las especializadas en el manejo de seguridad y sus ventajas entre otras son las siguientes.

1) Es adaptable a necesidades del usuario y además hay mucha documentación y herramientas, para fortalecer la seguridad con dicha distribución.
2) Para equipos MAC, la seguridad se puede optimizar por medio de máquinas virtuales, y desde ahí se puede regular la seguridad de dicho equipo.

Con ello surge la complejidad de los sistemas de seguridad, el usuario tiene un papel importante en el cuidado de su información y en el cuidado de los sitios que vista al navegar por internet, con el uso algunas configuraciones como pueden ser cortafuegos, actualizaciones, monitoreo, navegación segura, etc.

Con esto se puede mantener aspectos de privacidad y disponibilidad segura de nuestras redes inalámbricas, hasta cierto punto a causa del gran número de amenazas en seguridad de la información, que hace necesario tener nociones de las nuevas estrategias de uso de la información para usos ilícitos y soluciones con respecto a necesidades propias de seguridad.

REFERENCIAS DE CONSULTA

Álvarez Marañón, G. (2009). *Cómo protegernos de los peligros de internet*. 1ra ed. Madrid: Consejo Superior de Investigaciones Científicas, p.11.

Aguilera, P. (2010). *Seguridad Informática*. 1st ed. Editex, p.4.

Carballar, A. (2013). *Instalación, seguridad y aplicaciones*. España: Ra-Ma.

Carballeiro, G. (2014). *Redes: Dispositivos e instalación*. 1st ed. Buenos Aires: Valentin Almiron, p.148.

CCNA Networking para el hogar y pequeñas empresas. (2011). 4th ed. Naucalpan de Juárez, Edo. de México: Cisco, p.102.

Conducef. (2017). *Robo de Identidad*. [online] Disponible en: http://inicio.ifai.org.mx/nuevo/Guia%20Robo%20Identidad.pdf [Acceso 2 Feb. 2017].

Documentación Kali Linux. (2017). [online] Disponible en: http://docs.kali.org/installation/kali-linux-hard-disk-install [acceso 5 Mar. 2017].

Dordoigne, J. (2013). *Redes informáticas*. 5th ed. Barcelona: Eni.

Engst, A. (2011). *Introducción a las redes inalámbricas.* España: Anaya.

Evans, D. (2011). *Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo*. 1st ed. [ebook] Cisco Internet Business Solutions Group,

pp.9-10. Disponible en: http://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf [Accessed 25 Dec. 2016].

García, C. (2014). Hablemos de Spoofing. [Blog] *Cloud Security Service.* Disponible en: https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

Gartner (2017). *Technology Research* | *Gartner Inc.* [Online] Disponible en: http://www.gartner.com/technology/research/

GIGA (2015).*Tecnología inalámbrica* [Online] Disponible en:

González Pérez, P., Sánchez Garcés, G. and Soriano de la Cámara, J. (2013). *Pentesting con Kali*. 1st ed. Móstoles, Madrid: 0xWord.

https://www.ecured.cu/Revista_GIGA.

Oecd.org. (2017). *OECD.org - OECD*. [Online] Disponible en: https://www.oecd.org/

Roa Buendía, J. (2013). *Seguridad Informática.* 1st ed. España: McGraw-Hill, p.154.

Symantec. (2015). Objetivo de los atacantes, tanto grandes como pequeñas empresas. [Online] Disponible en:

https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf [Acceso 1 Mar. 2017].