ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ANALISIS DE VULNERABILIDADES EN REDES WIFI AD-HOC MEDIANTE SOFTWARE LIBRE PARA MEJORAR LA SEGURIDAD EN AMBIENTES OUTDOOR

MARÍA ALEXANDRA PILCO LLUMITAXI

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA-ECUADOR

NOVIEMBRE 2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE INVESTIGACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado **ANALISIS DE VULNERABILIDADES EN REDES WIFI AD-HOC MEDIANTE SOFTWARE LIBRE PARA MEJORAR LA SEGURIDAD EN AMBIENTES OUTDOOR**, de responsabilidad de la señorita María Alexandra Pilco Llumitaxi, ha sido minuciosamente revisado y se autoriza su presentación.

LUIS EDUARDO HIDALGO ALMEIDA

Firmado digitalmente por LUIS EDUARDO HIDALGO ALMEIDA
Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000445780, cn=LUIS EDUARDO HIDALGO ALMEIDA
Fecha: 2021.11.29 11:53:52 -05'00'

Ing. Luis Eduardo Hidalgo Almeida; Ph.D.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
WILIAN XAVIER SANCHEZ LABRE

Ing. Wilian Xavier Sanchez Labré; Mag.
DIRECTOR

Firmado electrónicamente por:
DARWIN PAUL CARRION BUENANO

Ing. Darwin Paul Carrión Buenaño; Mag.
MIEMBRO DEL TRIBUNAL

Ing. Danilo Geovanny Barreno Naranjo; Mag.
MIEMBRO DEL TRIBUNAL

Riobamba, noviembre 2021

DERECHOS INTELECTUALES

Yo, María Alexandra Pilco Llumitaxi, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo** y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

María Alexandra Pilco Llumitaxi

No. Cédula: 0201977501

DECLARACIÓN DE AUTENTICIDAD

Yo, María Alexandra Pilco Llumitaxi, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autora, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

_____

María Alexandra Pilco Llumitaxi

No. Cédula: 0201977501

DEDICATORIA

Dedico este peldaño más de mi vida profesional en primer lugar a Dios y la Virgen por ser quienes son los autores de mis días.

A mi padre por su apoyo y comprensión, a mi madre quien con su infinito amor ha estado siempre a mi lado brindándome sus palabras de aliento para continuar en alcanzar mis objetivos, por ser ejemplo de constancia, perseverancia y apoyo incondicional; siendo ella mi inspiración y mi guía para culminar este peldaño.

A mis hermanos David y Anthony que con sus palabras de aliento y ayuda han sabido motivarme a seguir mis objetivos y han sido mi apoyo para levantarme y continuar en la lucha, gracias por siempre confiar en mí y apoyarme en todo momento.

A mi compañero de vida Roque, por estar pendiente de mí y motivarme a plasmar siempre lo mejor que hay en mí y alcanzar mis metas.

A todos mis familiares y amigos que han estado brindándome sus palabras de aliento para no desmayar y lograr cumplir mis sueños.

Este logro es ¡para ustedes!

Alexita

AGRADECIMIENTO

A Dios por seguirme dando la salud y la vida para continuar en este largo trajinar.

A la noble institución que me dio la oportunidad de seguirme preparando y a los docentes por compartir sus conocimientos y ayudarme a conseguir este peldaño más en mi vida profesional.

Al Ing. Wilian Sánchez, Tutor de esta investigación y a los ingenieros Darwin Carrión y Danilo Barreno por su colaboración en el desarrollo.

A todas las personas quienes con su apoyo, amistad y cariño han sido parte de la realización de esta investigación.

Alexita

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

El presente proyecto de investigación tuvo como objetivo analizar las vulnerabilidades existentes en las redes WiFi Ad-Hoc mediante el empleo de software libre como es Kali-Linux que proporciona herramientas de hacking, para mejorar la seguridad en este tipo de redes, mediante la implementación de una Guía de mejores prácticas de seguridad. Mediante el análisis de vulnerabilidades a través de un determinado servicio y en caso de existir que acciones serian recomendadas para mitigar este riesgo de seguridad en la red. La metodología empleada para realizar la investigación fue recolección de información mediante las pruebas realizadas, análisis de las vulnerabilidades y explotación de las vulnerabilidades para saber si son consideradas un riesgo para la seguridad de la información. Para recolectar la información se realizó ataques de fuerza bruta con la herramienta Aircrack y escaneo de puertos con la herramienta nmap, para luego proceder a explotar cada uno de los puertos mediante el empleo de Metasploit Framework. Una vez realizadas todas las pruebas y mediante el empleo de estadística referencial a través de la aplicación de la prueba Chi-Cuadrado (X2) los resultados apoyan a la hipótesis planteada; al aplicar el análisis de vulnerabilidades en redes WiFi Ad-Hoc en ambientes outdoor utilizando software libre se permitió mejorar la seguridad. Dentro de los resultados obtenidos se logró mejorar la seguridad en estas redes WiFi Ad-Hoc en un 98% en la mitigación de los riesgos existentes en el escenario 2, permitiendo así evitar ataques de fuerza bruta, ataques de man in the middle, y garantizar la confidencialidad, integridad y disponibilidad de la información.

Palabras claves: <VULNERABILIDADES>, <ATAQUES DE FUERZA BRUTA>, <MAPEO DE PUERTOS>, <INTEGRIDAD>, <CONFIDENCIALIDAD>, <DISPONIBILIDAD>, <SEGURIDAD DE LA INFORMACIÓN>, <MEJORES PRÁCTICAS>, <PROTOCOLOS>.

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602766974, cn=LUIS ALBERTO CAMINOS VARGAS
Fecha: 2021.11.09 11:53:46 -05'00'

UNIDAD DE PROCESOS TÉCNICOS DBRA DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE ESPOCH

SUMMARY

The current research project analyzed the existing vulnerabilities in Ad-Hoc WiFi networks through the use of free software such as Kali-Linux that provides hacking tools to improve security in this type of networks through the implementation of a Security Best Practices Guide. By analyzing vulnerabilities through a specific service and, if any, what actions would be recommended to mitigate this security risk on the network. The methodology used to carry out the investigation was the collection of information through the tests carried, an analysis of the vulnerabilities and by exploitation of the vulnerabilities to find out if they are considered a risk for the security of the information. To collect the information brute force attacks were carried out with the Aircrack tool and port scanning with the nmap tool and then proceeded to exploit each of the ports using the Metasploit Framework. Once all the tests were carried out and through the use of referential statistics through the application of the Chi-Square test (X2), the results support the hypothesis by applying the vulnerability analysis in Ad-Hoc WiFi networks in outdoor environments using free software. It was possible to improve security. Among the results got, it was possible to improve security in these Ad-Hoc WiFi networks by 98% in mitigating the existing risks in scenario 2. It allowed to avoid brute force attacks, man-in-the-middle attacks, and to insure the confidentiality, integrity and availability of the information.

Keywords: <VULNERABILITIES>, < BRUTE FORCE ATTACKS>, <PORT MAPPING>, <INTEGRITY>, <CONFIDENTIALITY>, <AVAILABILITY>, <INFORMATION SECURITY>, <BEST PRACTICES>, <PROTOCOLS>, <MAN IN THE MIDDLE>.

CAPÍTULO I

1. INTRODUCCIÓN

En la actualidad la información es considerada el activo más importante dentro de las empresas, por consiguiente, se debe buscar tener mayor seguridad dentro de los sistemas para con ello evitar pérdidas económicas y emitir una buena imagen en tanto a la confidencialidad, disponibilidad e integridad de la empresa o institución.

Gracias a la evolución de la tecnología en el área inalámbrica, estas permiten cada vez la transmisión de mayor cantidad de información, logrando de están manera agilizar los procesos y minimizar el tiempo de respuesta, pero como todo progreso tecnológico tiene su desventaja, surge con esto las amenazas y vulnerabilidades a las redes MANETs.

Hoy en día la creciente popularidad de las redes móviles ad-hoc (MANETS) se están convirtiendo en el auge tecnológico debido a su bajo costo de implementación, utilización de poco espacio para su funcionamiento, facilidad de comunicación entre los diferentes tipos de dispositivos inalámbricos (sensores inalámbricos, tablets, laptos, access point, etc) y a su vez estas características han permitido el desarrollo de sistemas basados en esta tecnología para su uso cotidiano.

El auge de esta tecnología provoca que haya ataques maliciosos a estas redes, utilizando distintos tipos de software para poder sustraer, remplazar o filtrar la información procedente de las redes MANETs. Con el objetivo de causar malestar y perdidas económicas en las empresas.

Al hablar de avance tecnológico esto hace referencia a que se debe poner mayor énfasis en la seguridad con la finalidad de brindar a las empresas integridad, disponibilidad y confidencialidad en los activos.

1.1. Planteamiento del problema

1.1.1. Situación Problemática

En vista de que la seguridad es un proceso de continua evolución y por ende todo sistema que transmita información requiere un elevado nivel de atención con el fin de tener una comunicación integra, confidencial y que se encuentre disponible cuando se requiera de ella.

En la actualidad todavía se requiere de mucho esfuerzo sobre la seguridad en redes MANETs. Debido a este problema la seguridad en las redes MANETs se ha convertido en un pilar fundamental dentro de los entornos de trabajo, debido a que la información es el activo más importante de las empresas y por ende es lo que más se debe precautelar.

Las redes MANETs son, quizás, las más extendidas y desarrolladas en la actualidad, debido a su facilidad de implementación y su escalabilidad, permitiendo satisfacer las necesidades del mundo actual, como es la movilidad, la flexibilidad y la capacidad de auto configurarse. Han sido clasificadas como poseedoras de una capacidad de cómputo media-alta y una movilidad media-baja.

El presente proyecto está enfocado en realizar un análisis de la red inalámbrica Ad-Hoc en ambientes outdoor para detectar vulnerabilidades, utilizando herramientas que permitan observar el nivel de seguridad, efectuando ataques y de esta manera plantear recomendaciones para mejorar la seguridad de las redes Ad-hoc en ambientes outdoor.

El proyecto de investigación propuesto busca y tiene la finalidad de contribuir al fortalecimiento de la seguridad de las redes wifi ad-hoc, mediante la utilización de software libre, para determinar qué tan vulnerables se encuentran las redes wifi ad-hoc a los diferentes ataques existentes, así como también permitirá ver el grado de incidencias de seguridad que se tiene.

1.2. Formulación del Problema

¿Cómo analizar las vulnerabilidades de seguridad en redes wifi ad-hoc mediante software libre para la detección de intrusos en ambientes outdoor?

1.3. Preguntas Directrices o Específicas de la Investigación

¿Cómo se puede determinar el grado de vulnerabilidad de seguridad en redes wifi ad-hoc en ambientes outdoor?

¿Qué herramientas de software libre se utilizará para determinar las vulnerabilidades?

¿Cómo afecta los incidentes de seguridad a las redes wifi ad-hoc?

¿Determinar cuáles son los problemas a los que están expuestas las redes wifi ad-hoc en ambientes outdoor?

¿Qué resultados se obtiene al realizar el análisis de vulnerabilidades?

1.4. Justificación de la Investigación

Debido a la evolución tecnológica de las redes en la actualidad, permitiendo así la transmisión de mayor cantidad de información, logrando de esta manera agilizar los procesos y minimizar el tiempo de respuesta, pero como todo avance tecnológico tiene su desventaja, surge con esto las amenazas y vulnerabilidades a las redes.

El presente proyecto de investigación propuesto busca y tiene la finalidad de contribuir al fortalecimiento de la seguridad de las redes wifi ad-hoc, mediante la utilización de software libre, para determinar qué tan vulnerables se encuentran las redes wifi ad-hoc a los diferentes ataques existentes, así como también permitirá ver el grado de incidencias de seguridad que se tiene.

En vista de que la seguridad es un proceso de continua evolución y por ende todo sistema que transmita información requiere un elevado nivel de atención con el fin de tener una comunicación integra, confidencial y que se encuentre disponible cuando se requiera de ella.

El presente proyecto está enfocado en realizar un análisis de la red inalámbrica ad-hoc para detectar vulnerabilidades, utilizando herramientas que permitan observar el nivel de seguridad efectuando ataques y plantear recomendaciones para mejorar la seguridad de las redes Ad-hoc.

Luego de implementar el escenario para la aplicación de las herramientas para la detección de intrusos, la implementación se realizará en ambientes Outdoor, para determinar los incidentes de seguridad mediante la herramienta de software libre empleada para la realización del proyecto de investigación.

1.5. Objetivos de la Investigación

1.5.1. Objetivo General

Analizar y evaluar las vulnerabilidades en redes WiFi ad-hoc en ambientes outdoor mediante software libre para mejorar la seguridad.

1.5.2. Objetivos Específicos

- Analizar las vulnerabilidades asociadas a las redes WiFi ad-hoc en ambientes outdoor.
- Realizar ataques a la red wifi ad-hoc con la herramienta seleccionada para determinar los tipos de vulnerabilidades existentes en la red wifi ad-hoc en ambientes outdoor.
- Evaluar y establecer recomendaciones que ayuden a solucionar los problemas de seguridad en la red wifi ad-hoc en ambientes outdoor.

1.6. Hipótesis

Al aplicar el análisis de vulnerabilidades en redes wifi ad-hoc en ambientes outdoor utilizando software libre permitió mejorar la seguridad.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Estado del Arte

Para el desarrollo del proyecto de investigación se recurre a las investigaciones realizadas anteriormente sobre temas afines o acordes al tema a tratar con la finalidad de que respalden la investigación.

Las redes ad hoc son un nuevo paradigma de redes inalámbricas para hosts móviles, estas redes inalámbricas móviles que forman una red temporal sin ayuda de ninguna infraestructura establecida o centralizada, permitiendo que se comuniquen de una manera auto-organizada.

La seguridad en redes MANET es un componente esencial para las funciones básicas de la red, como el reenvío de paquetes y el enrutamiento: el funcionamiento de la red se puede poner en peligro fácilmente si las contramedidas no están integradas en las funciones básicas de la red en las primeras etapas de su diseño. A diferencia de las redes que usan nodos dedicados para admitir funciones básicas como el reenvío de paquetes, el enrutamiento y la administración de la red, en las redes ad hoc esas funciones las realizan todos los nodos disponibles. Esta misma diferencia está en el núcleo de los problemas de seguridad que son específicos de las redes ad hoc. A contraste de los nodos dedicados de una red clásica, no se puede confiar en los nodos de una red ad hoc para la ejecución correcta de las funciones críticas de la red. (Molva, 2015)

El funcionamiento correcto de la red requiere no solo la ejecución correcta de las funciones críticas de la red por parte de cada nodo participante, sino que también requiere que cada nodo realice una parte justa de la función, para no poner en peligro la confiabilidad de las funciones básicas de la red como lo es el enrutamiento de paquetes.

En la tesis de "HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A." desarrollada por (Buenaño Rojas, ä8) nos aporta con las siguientes líneas de investigación:

- El nivel de infraestructura tecnológica es un factor decisivo a la hora de sufrir un ataque informático ya que implica una adecuada gestión de configuración en los servicios implementados y una correcta administración y despliegue de actualizaciones en sistemas operativos y aplicaciones.

La investigación científica realizada por (Yan, 2014) hace referencia a que se requieren medidas de prevención de intrusiones, como el cifrado y la autenticación, para proteger el funcionamiento de la red. Pero estas medidas no pueden defender los nodos comprometidos, que llevan sus claves privadas. Las redes ad hoc tienen vulnerabilidades inherentes que no se pueden prevenir fácilmente. La detección de intrusos presenta un segundo muro de defensa y es una necesidad en cualquier red de alta disponibilidad.

Las conclusiones que aporto esta investigación son:

- La detección de intrusos se puede usar como la segunda línea de protección para capturar datos de auditoría y extraer evidencia en los datos para determinar si el sistema está bajo ataque.
- En las redes ad hoc, los datos de auditoría útiles en el nodo incluyen las actividades del sistema y del usuario dentro del nodo móvil, las actividades de comunicación de este nodo, así como las actividades de comunicación dentro del rango de radio y la observación del nodo.

2.2. Bases Teóricas

2.2.1. Tecnologías Inalámbricas

Las redes inalámbricas en el trascurso del tiempo han ido evolucionando debido a que se han convertido en el auge tecnológico de este siglo, esto es debido a que en la actualidad existen dispositivos que utilizan las redes inalámbricas para comunicarse. El auge de las tecnologías inalámbricas surge gracias a que permiten flexibilidad, propagación de la red, menor costo de implementación, escalabilidad, entre otras características. El objetivo de las tecnologías inalámbricas es mantener conectados a todos los dispositivos que no pueden conectarse a medios guiados, facilitando de esta manera la comunicación entre ellos.

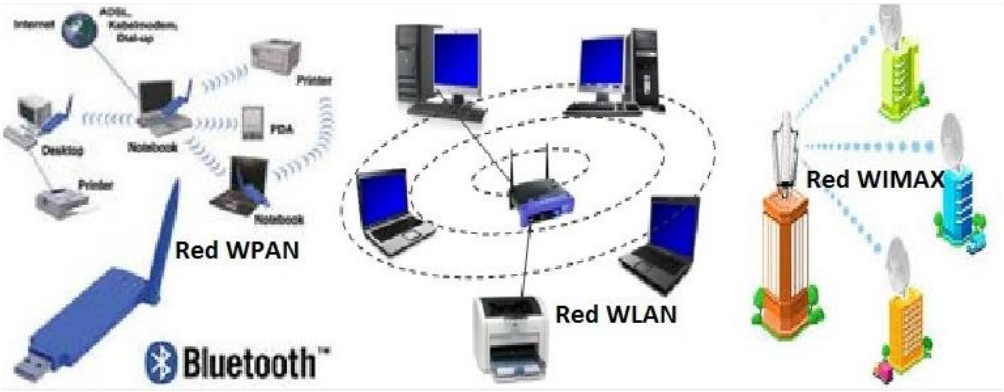

Figura 1-2. Redes Inalámbricas

Fuente: (Fabio Asecio, 2013)

2.2.2. Clasificación de las Redes Inalámbricas

Debido a la proliferación de la tecnología han surgido los distintos tipos de tecnologías inalámbricas como se las puede clasificar dependiendo al alcance de la señal y el área de aplicación en la figura 2-1, se observa las cuatro categorías en las que se clasifican las redes inalámbricas:

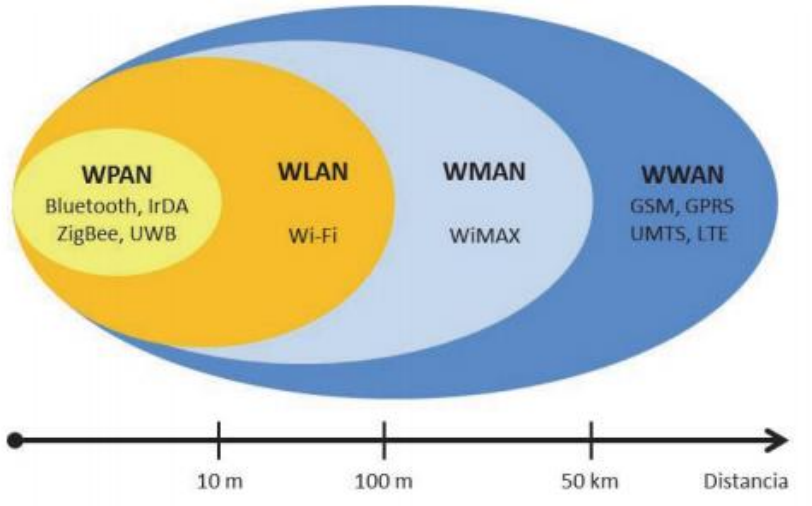

Figura 2-2. Clasificación de las redes inalámbricas

Fuente: (SALAZAR, 2016)

Dentro de la clasificación de las redes inalámbricas por su área de aplicación se tiene:

- **Wireless Personal Area Network (WPAN)**

  Las redes WPAN son consideradas de área personal y se basan en el estándar 802.15, permiten la conexión de equipos sin cable como es celulares, cámaras, PDAs, dentro de esta clasificación se encuentran las tecnologías: Bluetooth, HomeRF e Infrarrojos IRDA. Uno de los inconvenientes principales es su corto alcance debido a que tiene una cobertura de un par de metros y su baja velocidad de transmisión. Estas redes se caracterizan por su bajo consumo de energía permitiendo de esta manera ahorrar energía en el caso de los sensores utilizados en aplicaciones de campo, etc.

  Las redes inalámbricas consideradas dentro de la clasificación por su alcance son:

- **Wireless Local Area Network (WLAN)**

  Son redes inalámbricas de área local están diseñadas para un rango de cobertura típica de 100 metros. Proporciona a los usuarios la capacidad de moverse dentro del área de cobertura y mantenerse conectados a la red. Son utilizadas en el hogar, escuelas, universidades, instituciones, etc.

Estas redes se basan en el estándar 802.11 y comercializadas con el nombre de WI-FI. En la actualidad es el estándar más utilizado en el área comercial que se emplea para la interconexión de redes. El estándar IEEE 802.11 tiene unas variantes que son: 802.11b, 802.11g, 802.11a, 802.11e, 802.11h, etc.

- **Wireless Metropolitan Area Nerwork (WMAN)**

Son redes inalámbricas metropolitanas se basan en el estándar IEEE 802.16, están diseñadas para la conexión de enlaces a grandes distancias y a una alta velocidad de transmisión de datos. La arquitectura usada en estas redes es punto multipunto, permitiendo una cobertura de hasta 50 km. Estas redes son utilizadas como redes backup dentro de las grandes industrias debido a su alta velocidad de transmisión, permitiendo transmitir la información en caso de pérdida del enlace cableado.

- **Wireless Wide Area Network (WWAN)**

Son redes inalámbricas de área extendida estas redes están diseñadas para cubrir grandes áreas como por ejemplo ciudades o países mediante la instalación de antenas que dividen el área en celdas o satélites. Dentro de estas redes se encuentran las tecnologías móviles (GSM, GPRS, UMTS) y satélites. Estas redes inalámbricas son conocidas como sistemas de segunda generación debido a que permite el acceso a internet desde áreas exteriores. (Kanika Sharma, 2014)

2.2.3. Ventajas y desventajas de las Redes Inalámbricas

Dentro del siguiente cuadro comparativo podemos observar las ventajas y desventaja de las redes inalámbricas:

Ventajas

- Movilidad: admite la transmisión de información desde cualquier lugar en tiempo real, permitiendo con esto mejorar la productividad de la empresa.
- Escalabilidad: permite ir agregando dispositivos de acuerdo a la demanda de los usuarios dentro de la red.

- Flexibilidad: permite llegar con la cobertura donde no se puede llegar con la red cableada esto puede ser en interiores o exteriores de un lugar u oficina.
- Facilidad de instalación: permite reducir el uso de cables de esta manera se mejora la estética de los lugares, reduciendo así el tiempo de instalación.
- Bajo costo de instalación: permite generar un ahorro en el momento de la instalación de la red.
- Facilidad de uso: Permite la conexión automática de usuarios sin la necesidad de usar cables.

Desventajas

- Seguridad: Debido a que la información es transmitida por el aire esta puede ser interceptada con mayor facilidad, es por ello que surgen los distintos tipos de ataques para interceptar los datos transmitidos por este medio.
- Interferencias: Esto es debido a la distancia de transmisión de cada tecnología inalámbrica y a los obstáculos que se presenten.
- Capacidad de Rendimiento se ve afectada cuando hay más de una conexión.

2.2.4. Tipos de Redes Inalámbricas

Las redes inalámbricas AD HOC tienen dos tipos de topología que son: de modo infraestructura y de modo ad-hoc.

2.2.4.1. Modo de Infraestructura.

Son redes inalámbricas que usan una infraestructura de red previamente instalada para su funcionamiento, dentro de este tipo de redes se tiene los sistemas satelitales, Wireless LAN, entre otras. En este tipo de infraestructura los puntos de acceso inalámbricos son routers o switches que transmiten la información de la red inalámbrica a la red Ethernet interactuando entre sí como un puente. Al área de cobertura de un punto de acceso se le conoce con el nombre de Basic Service Set (BSS) y se le denomina con el nombre de red denominado Service Set Identifier (SSID). Para el funcionamiento de este tipo de redes se necesita de (González, 2014):

- Punto de Acceso (AP) es el dispositivo o nodo central que permite la conexión con los demás dispositivos que requieren conectarse a la red. Los AP pueden ser routers, swicthes, etc. Esta topología permite mayor seguridad, escalabilidad, estabilidad y facilidad de gestión dentro de la red inalámbrica, con un inconveniente de que tiene un mayor costo de implementación debido al uso de puntos de acceso (Flores, 2015).

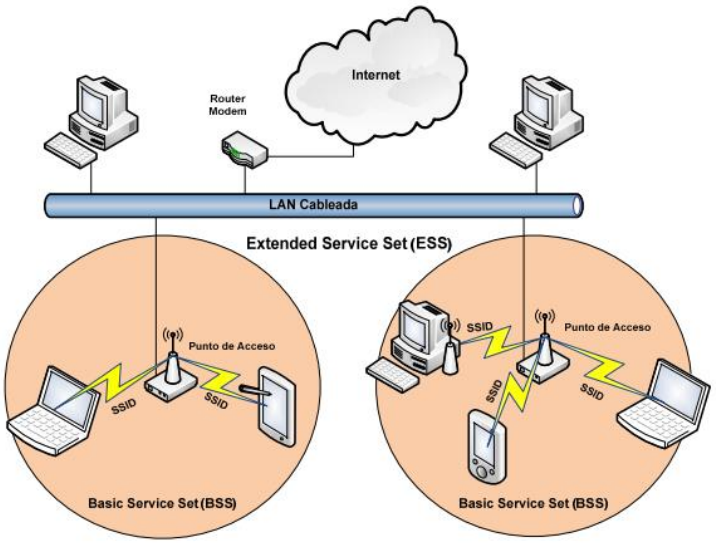

Figura 2-2. Esquema de red en modo infraestructura.

Fuente: (Lorenzana, 2015)

Los clientes de estas redes tienen libertad de movimiento dentro del rango de cobertura o de un punto de acceso a otro y seguir manteniendo la conexión de red sin perder la transmisión, debido a que se conectan automáticamente a otro punto de acceso que se encuentre dentro de otro rango de cobertura.

El modo de infraestructura ofrece mejor seguridad, facilidad de gestión (SALAZAR, 2016) a los clientes, y permite tener escalabilidad y estabilidad dentro de las áreas de cobertura. Con una desventaja debido a que tiene un costo adicional, causando un elevado gasto debido al despliegue de puntos de acceso en la red.

2.2.4.2. Redes Ad Hoc

Las redes ad hoc son redes inalámbricas dispersadas que no dependen de una infraestructura previa para su funcionamiento, permitiendo establecer una comunicación punto a punto con los nodos que conforman la red, la comunicación es tratada de manera

dinámica, proporcionando flexibilidad y autonomía, debido a que todos los nodos tienen la misma capacidad de transmisión (Flores, 2015).

Estas redes punto a punto se denominan Independent Basic Service Set (IBSS) y a las conexiones se les da un identificador de nombre Independent Basic Service Set Identifier (IBSSID).

En el modo Ad-Hoc el rendimiento de la red se ve afectada si se incrementan dispositivos, al igual que los dispositivos pueden fácilmente desconectarse de la red al azar lo que provoca que la gestión de la red sea complicada también tiene otra desventaja y es sin la instalación de pasarelas especiales, las redes en modo ad hoc no pueden conectarse con una red de área local cableada lo que provoca que no puede acceder a Internet.

Una ventaja del modo ad hoc es que funciona bien en un entorno pequeño siendo la forma más fácil y menos costosa de configurar una red inalámbrica.

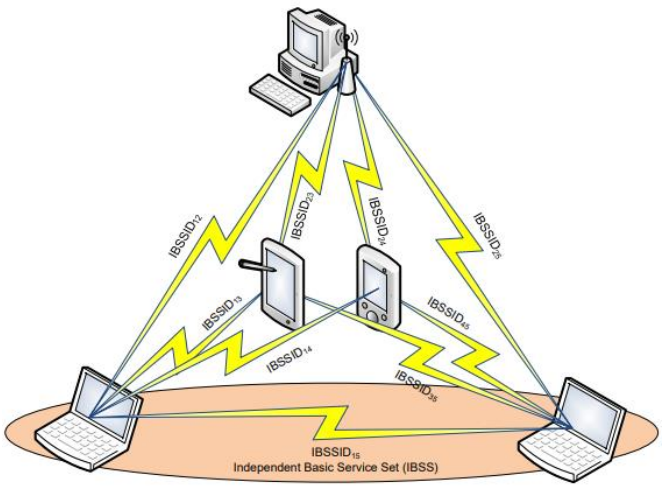

Figura 3-2. Esquema de red en modo Ad-Hoc.

Fuente: (Lorenzana, 2015)

2.2.4.2.1. Características de las Redes AD-HOC

Dentro de las características más relevantes de estas redes se tiene:

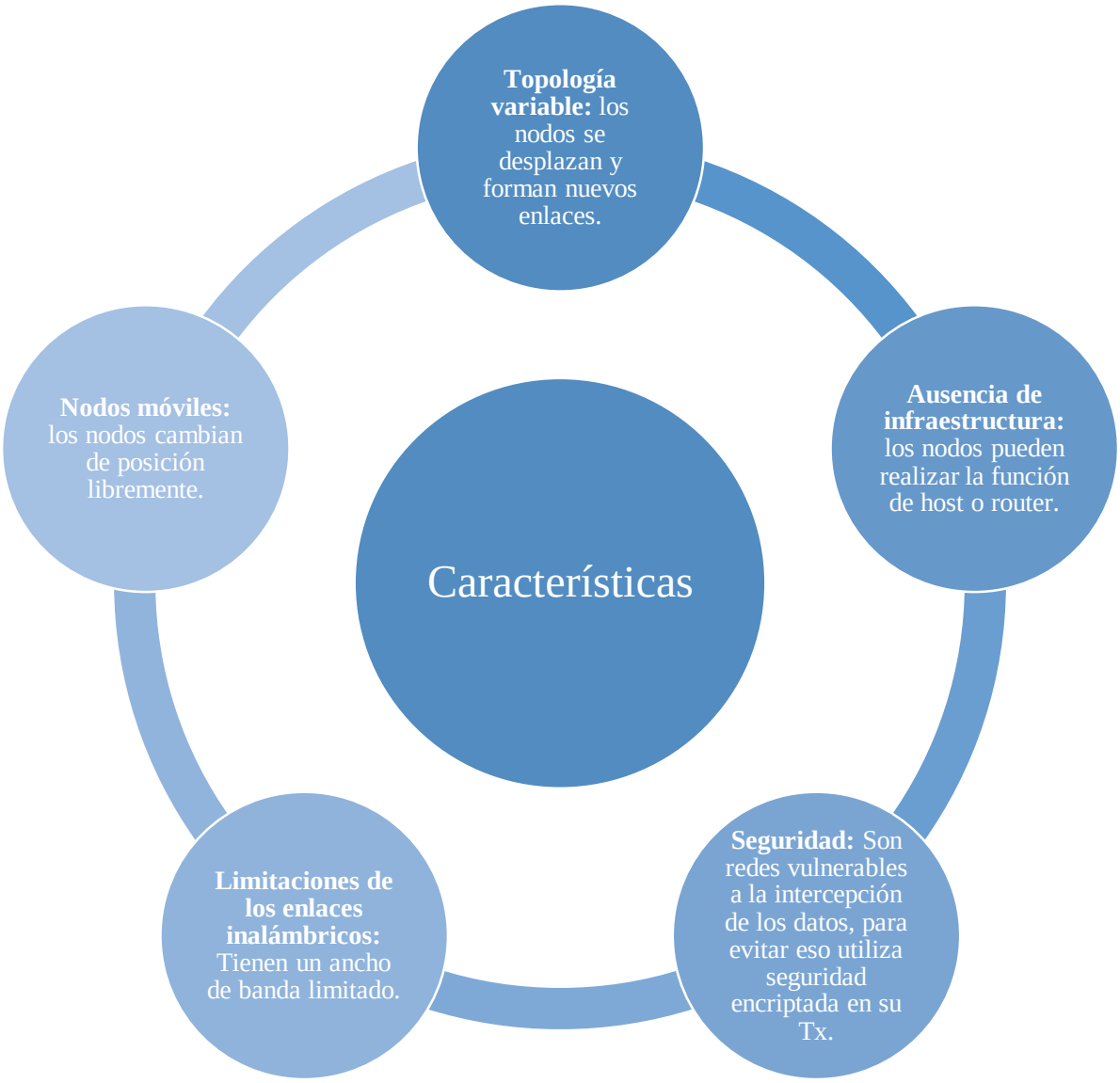

Figura 4-2. Características de las redes Ad-Hoc.

Fuente: (González, 2014)

2.2.4.2.2. Tipos de redes AD HOC

Las redes AD HOC se las puede clasificar dependiendo de su tipo de aplicación como es:

- **Mobile Ad Hoc Networks (MANETS)**

Son redes inalámbricas formadas por un conjunto de estaciones móviles, los cuales son auto configurables, tienen una topología eficiente, las rutas entre los nodos de la red contienen variados saltos y no requieren de una infraestructura existente, dentro de los inconvenientes que presentan estas redes es el área de cobertura limitada (Universidad, 2014).

Las redes MANETs pueden trabajar de manera separada o pueden también conectarse a otros puntos de red, con el inconveniente de que la calidad de la transmisión de datos puede variar dependiendo del: área de cobertura, localización de los nodos y las interferencias en el momento de la transmisión, con esta característica se logra una conectividad multi-salto dentro de los nodos a pesar de que los nodos no se encuentren dentro de la misma área de cobertura.

Dentro de las características más relevantes se tiene que: permite flexibilidad dentro de la red, fácil implementación y son usadas en situaciones de emergencia.

- **Redes Inalámbricas Mesh**

Son redes tipo malla están compuestas por redes ad hoc y redes de infraestructura, con la ventaja de que son redes más robustas y pueden cambiar la ruta para la transmisión de los datos en el caso de surgir inconvenientes.

- **Redes de Sensores**

Son redes inalámbricas que están conformadas por dispositivos autónomos y necesitan de sensores para poder monitorear condiciones ambientes físicas.

2.2.4.2.3. Desventajas de las redes MANETs

- Problemas de inestabilidad del enlace y por ende poca eficiencia dentro de la red.
- La batería tiene un tiempo limitado de funcionamiento.
- No solo el enrutamiento sino también el estado y la asignación de la densidad de los nodos influyen en gran medida en el rendimiento de la red.
- El alcance de cobertura de la red es limitado lo que produce que los nodos se desconecten de la red. (Shohei Sato & Barolli, 2011)

2.2.4.2.4. Usos de las redes MANETs

Las principales aplicaciones que se le dan a estas redes son:

- Entornos civiles
- Entornos militares
- Desastres naturales
- Redes de área personal (PAN's)

Son usadas para recopilar información y compartirla entre los usuarios que se encuentran conectados a la red, en entornos universitarios y campus son usadas para clases virtuales y conferencias.

2.2.5. Estándar IEEE 802.11

El estándar IEEE 802.11 es sencillo y permite mayor escalabilidad, fue desarrollado en 1997 por la asociación técnico-profesional ANSI/IEEE (Instituto Nacional Estadounidense de Estándares/Institute of Electrical and Electronics Engineers), con la finalidad de brindar a los dispositivos, estaciones de trabajo libre movimiento sin perder la conexión entre los dispositivos.

IEEE 802.11 es un conjunto de estándares de comunicaciones que fue desarrollado en el año de 1997 por la asociación técnico-profesional ANSI/IEEE (Institute of Electrical and Electronics Engineers), este estándar se encuentra en continua evolución permitiendo velocidades de conexión más avanzadas a las versiones anteriores. El estándar 802.11 define la modalidad de interconexión entre estaciones en áreas limitadas utilizando el aire como medio de transmisión; constituye uno de los estándares de mayor interés para la evolución de las tecnologías de interconexión, permitiendo la conexión de los nodos sin pérdida o interferencia en la comunicación.

Este estándar es usado para implementar redes inalámbricas de área local en las bandas de frecuencias 2,4 GHz, 5 GHz, y 60 GHz

IEEE 802.11 define como usar los protocolos en los niveles bajos del modelo OSI, que son la capa física y la capa de enlace de datos, permitiendo crear una red de área local inalámbrica. Estas dos capas permiten hacer una separación funcional del estándar y lo más importante, que permite que un único protocolo de datos pueda usarse con varios métodos de transmisión.

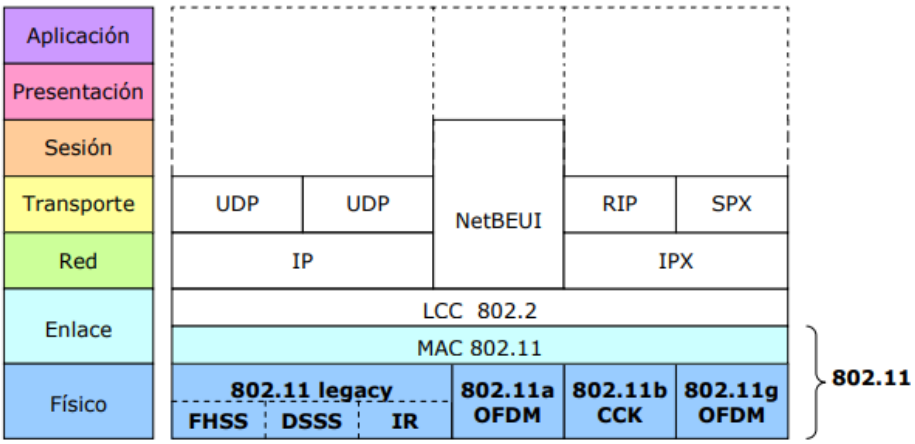

Figura 5-2. Modelo OSI y familia de protocolos 802.11.

Fuente: (Lorenzana, 2015)

2.2.6. Protocolos de Seguridad Inalámbrica

El rápido crecimiento de las redes inalámbricas ha convertido la seguridad de los datos en un tema esencial en la actualidad. En donde los protocolos de seguridad inalámbrica no sólo evitan que las partes no deseadas se conecten a su red inalámbrica, sino que también encriptan sus datos privados enviados a través de las ondas de radio.

Se averigua el funcionamiento de las redes inalámbricas, específicamente como está resguardada la información de quienes están conectados a la red. En las redes Wi-fi la información se encuentra en un estado de encriptación de sus datos. Con el objetivo de impedir que personas no deseadas obtengan acceso a la información, existen diferentes sistemas de seguridad, como es WEP, WPA, WPA2 entre otros y estos protocolos se rigen bajo las normas del IEEE que es la encargada de estandarizar estos protocolos de seguridad. En la actualidad no hay sistema que sea cien por ciento seguro, debido a que siempre habrá personas con la mala intención de causar daño.

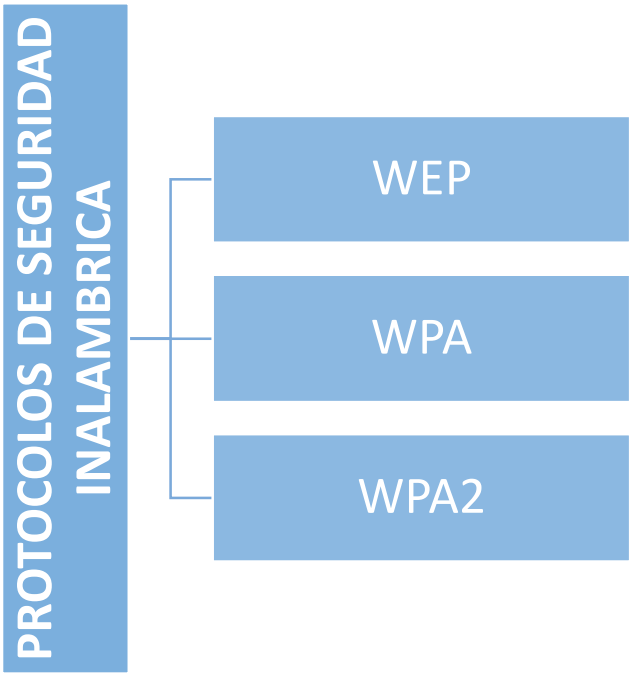

Figura 6-2. Tipos de protocolos de **seguridad.**

Fuente: (Pilco, 2021)

Los mecanismos de cifrado que se basan en una estructura de clave estática, como WEP (802.11) y TKIP (802.1x), son vulnerables al descifrado de claves mediante la captura de paquetes inalámbricos (Debao Xiao, 2006).

2.2.7. Seguridad a Nivel de Protocolo

La seguridad a nivel de protocolo se encarga de que los datos transmitidos por una WLAN no puedan ser interceptados por una persona no autorizada a la red. Por consiguiente, la red debe de tener un algoritmo de codificación y gestión de claves (Manuel Ramírez, 2015).

Uno de los inconvenientes más relevantes a los que se enfrenta WiFi es la seguridad, debido a que la información es transmitida por un medio de propagación de libre acceso, y por ende una red inalámbrica puede verse obstaculizada a nivel de acceso no autorizado, usurpación, suplantación de identidad, interferencias aleatorias, denegación de servicio, etc. (College, 2010). Para precautelar la información es necesario otorgar a las redes inalámbricas de mecanismos que garanticen la seguridad de la comunicación.

En la figura 8-1, se observa los principales niveles en los que se debe aplicar la seguridad en una red WLAN.

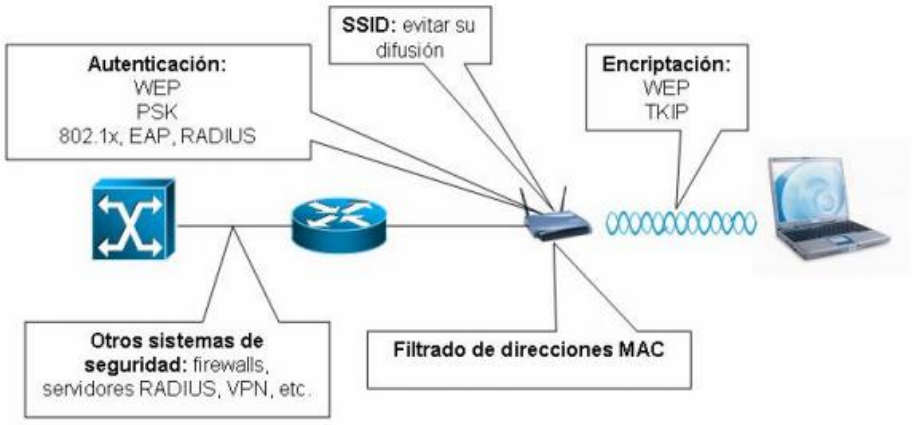

Figura 7-2. Niveles de seguridad en una WLAN.

Fuente: (College, 2010)

2.2.8. Niveles de seguridad WLAN

Dentro de los principales elementos que se debe considerar para brindar seguridad se tiene:

- **SSID (Service Set ID)**

Es el identificador de la WLAN

2.2.8.1 WEP (Wired Equivalent Privacy)

El protocolo WEP fue desarrollado y aprobado como estándar de seguridad wifi en septiembre de 1999, es el mecanismo de cifrado básico opcional definido en el estándar IEEE 802.11. Utiliza el algoritmo de cifrado RC4 (Rivest Cipher 4), para cifrar todos los datos que se intercambian entre los clientes y el punto de acceso. WEP tenía muchos defectos como era la reutilización del vector de inicialización, del cual se derivan ataques estadísticos que permiten recuperar la clave WEP. Consiguiente a este la IEEE publico el estándar WPA.

2.2.8.2 WPA (Wifi Protect Access)

WPA es el protocolo de seguridad que lanzó la Alianza Wi-Fi para dar solución a los problemas de seguridad evidenciados del protocolo WEP.

Este protocolo implementa las siguientes mejoras:

- Autenticación del usuario mediante el IEEE 802.1x (control de acceso a red basada en puertos).
- Soluciona la debilidad del vector inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits).
- Utiliza el intercambio dinámico de claves mediante el protocolo TKIP (Temporal Key Integrity Protocol).
- El algoritmo de cifrado utilizado por WPA sigue siendo RC4 como en WEP, pero para comprobar la integridad de los mensajes, se cambió el código de detección de errores CRC-32 por uno nuevo llamado MIC (Message Integrity Code).

Continuamente el IEEE publicó el estándar 802.11i, también conocido como WPA2.

2.2.8.3 WPA2

Este protocolo está basado en el estándar de seguridad inalámbrica 802.11i, que se introdujo en 2004. Aunque tiene el inconveniente de no ser compatible con el hardware anterior, tiene la ventaja de ser mucho más seguro. Incluye el intercambio dinámico de la clave, un cifrado mucho más fuerte, y la autenticación de usuario, pero añade las mejoras siguientes:

- Nuevo algoritmo de cifrado AES (Advanced Encryption Standard). Se trata de un algoritmo de cifrado de bloque simétrico. Utiliza el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) para asegurar la integridad y la autenticidad de los mensajes transmitidos por la red.

2.2.9. Seguridad en redes 802.11

Las redes inalámbricas no son tan seguras como las redes cableadas debido a que utilizan el aire como medio de transmisión, lo que puede ocasionar que alguna persona intercepte

el mensaje, es por ello que las redes inalámbricas requieren de un mayor esfuerzo para mantener la seguridad.

Dentro de las comunicaciones es indispensable que la información transmitida llegue a su destinatario de forma íntegra tal cual fue enviado para poder cumplir con las tres columnas fundamentales que son, confidencialidad, integridad y disponibilidad.

- Confidencialidad es la capacidad de garantizar que la información que es transmitida por la red va a estar disponible únicamente para aquellos usuarios autorizados.
- Integridad es la capacidad de garantizar que los datos transmitidos no han sido modificados en ninguna instancia de su transmisión, permitiendo así que la información sea válida y consistente.
- Disponibilidad es la capacidad de garantizar que la información siempre va a estar disponible para los usuarios autorizados que requieran de ella.

2.2.10. Evaluación de la seguridad de la información

Existen 4 categorías que se deben analizar para realizar la evaluación de la seguridad dentro de una organización las cuales son según (Petar Čisar, 2018):

- **Evaluación de vulnerabilidades**

  Una evaluación de vulnerabilidad (escaneo) es una evaluación técnica diseñada para generar la mayor cantidad de vulnerabilidades posible en un entorno, junto con información de prioridad de corrección y gravedad.

- **Test de penetración interna/externa.**

  Es un ataque a un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar con la intención de encontrar debilidades de seguridad, así obtener acceso a él, su funcionalidad y datos confidenciales de la organización.

- **Evaluación de la aplicación**

  Se utiliza una evaluación de la aplicación (generalmente pruebas de recuadro blanco o negro) para evaluar la funcionalidad y la resistencia de una aplicación o de la red para determinar amenazas de seguridad que incluyen ataques a los programas, archivos, contraseñas entre otros. En esta fase se evalúa todos los componentes de una infraestructura de aplicaciones o de la red, incluida la forma de implementación de cada componente y la manera de comunicación con los entornos de cliente y servidor.

  Los expertos en seguridad de la información emplean un conjunto de herramientas de código abierto y en algunos de los casos de software licenciado para ejecutar las pruebas en la red.

- **Pruebas de cumplimiento o auditoria**

  Su rol principal es determinar cómo una organización determinada se hace frente a un estándar particular. Como regla general, las auditorías no prueban la seguridad directamente, sino que prueban el cumplimiento de un estándar. Las fallas de seguridad que existen en el sistema están identificadas por las evaluaciones de vulnerabilidad sin medir su impacto con el objetivo de que estas pruebas explotan las vulnerabilidades existentes y así evaluar las consecuencias dentro de la organización (Castro, y otros, 2018).

2.2.11. Tipos de ataques o vulnerabilidades

Entre las clases de vulnerabilidad (ataques) más extendidas se pueden enumerar las siguientes:

- Denegación de servicio (DoS); este ataque consiste en romper el comportamiento de una aplicación, con el objetivo de que sea inaccesible, corrupción de memoria (por ejemplo, desbordamiento de búfer, manipulación de la memoria de proceso, permitiendo con frecuencia la ejecución de un código malicioso del atacante), estos ataques son contra la capa física/enlace de datos, este tipo de ataques son los más temidos debido a que el atacante puede dañar servicios, sistemas o dañar las redes.
- Vulnerabilidades web: estas atacan a los servicios web utilizando técnicas como inyección SQL y XSS.
- Ataques de contraseña esta vulnerabilidad ataca contra el sistema de autenticación; a menudo aprovechan las listas de contraseñas para atacar las credenciales de servicio y del cliente -ataques laterales.

2.2.12. Kali Linux

Kali Linux es una nueva distribución de código abierto que facilita las pruebas de penetración. Destinado a pruebas de penetración avanzadas y auditorías de seguridad.

Este sistema operativo también ha mejorado los repositorios de software que están sincronizados con los repositorios de Debian para que sea más fácil mantenerlo actualizado, aplicar parches y agregar nuevas herramientas (Abdulrahman, 2016).

Kali trae por defecto cientos de herramientas diseñadas para realizar un sin número de actividades de seguridad de la información, incluidas pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa. Las herramientas de las cuales dispone Kali entre las principales son:

- **Escáner de red:**

Los escáneres de red se puede usar para descubrir hosts en la red, averiguar qué puertos y servicios podrían estar abiertos en un host, sistemas operativos de huellas digitales e identificar versiones de servicios que ejecutan Nmap o zenmap

- **Escáneres de vulnerabilidad web**

Los escáneres de aplicaciones web analizan las aplicaciones en sí, a veces se centran en tipos particulares de vulnerabilidades, como las vulnerabilidades de scripting entre sitios (XSS) o de inyección SQL (SQLi).

- **Proxies interceptores:**

Los proxies interceptores actúan como un "hombre en el medio" que inspecciona las solicitudes y respuestas mientras viajan de aquí para allá, lo que les permite ser analizadas o incluso modificadas en vuelo.

- **Herramientas de Explotación:**

  Las herramientas de explotación no se usan para encontrar vulnerabilidades, sino para explotarlas claramente, podrían usarse como verdaderas herramientas de piratas informáticos, pero también pueden usarse para demostrar que las vulnerabilidades particulares son reales y explotables.

- **Gestión de vulnerabilidades**

  Los sistemas de gestión de vulnerabilidades se utilizan para auditar sistemas, rastrear vulnerabilidades y diferenciar nuevos hallazgos y falsos positivos.

2.2.13. Pruebas de penetración

Las pruebas de penetración son un ejercicio legítimo de explotar un sistema con un escenario de atacante de la vida real, incluido el acceso ilegal y la práctica de actividades maliciosas. El proceso de pruebas de penetración comienza desde identificar las vulnerabilidades del sistema, realizar una explotación, descubrir e informar vulnerabilidades y disolver las vulnerabilidades que pueden causar daños al sistema (Teddy Surya Gunawan, 2018).

Las pruebas de Penetration testing son de vital importancia, debido a que permite ver el nivel de gravedad que tiene la red dentro de la organización y de esta manera poder prevenir ataques en la organización y evitar perdida de la información y poder lograr tener disponibilidad, integridad y confidencialidad en los activos de la empresa.

El proceso de prueba de penetración implica lo siguiente:

- Planificación y preparación
- Recopilar información sobre el objetivo antes de la prueba (reconocimiento)
- Detección de vulnerabilidad: posibles puntos de entrada identificación (escaneo de puertos)
- Intento de penetración: intentar un robo (virtual o real)
- Análisis e informes

2.2.13.1. Inyecciones SQL (SQLi)

La inyección SQL se produce cuando un atacante inyecta las consultas SQL con nuevos parámetros en los valores de entrada para ingresar y obtener acceso a la base de datos sin autorización. El ataque ocurre cuando las palabras clave u operadores obtienen del usuario el servidor de aplicaciones ejecutado en la consulta SQL actualizada comprometida.

2.2.13.2. Cross Site Scripting (XSS)

XSS es una técnica en la que se planta JavaScript, VBScript, ActiveX, Flash o HTML junto con el enlace malicioso XSS. Cuando el enlace infectado se ejecuta o se carga, el atacante obtendrá el privilegio de root y todos los datos e información confidenciales quedarán expuestos al atacante.

2.2.13.3. Inclusión de archivos locales (LFI) e inclusión de archivos remotos (RFI)

La inclusión local de archivos (LFI) es un ataque en el que el atacante ejecuta comandos en algunos archivos ubicados en el servidor web después de explotar las aplicaciones web.

La inclusión remota de archivos (RFI) se produce cuando cualquier tipo de entrada del usuario se acepta de forma remota sin pasar por una validación y desinfección adecuada por parte del servidor. Este ataque RFI es muy peligroso ya que los datos personales y confidenciales podrían ser robados y manipulados y podrían paralizar el funcionamiento del servidor web.

2.2.13.4. Denegación de servicio distribuida (DDoS)

Los ataques de (DDoS) son fatales. En este tipo de ataque, los usuarios legítimos no tendrían acceso a un recurso de red específico porque la red y los servicios se han inundado con una solicitud de servicio falsa.

2.2.13.5. Hombre en el medio (MITM)

El ataque MITM es un tipo de ataque donde viola dos de los objetivos de seguridad discutidos anteriormente; confidencialidad e integridad. En este ataque, el atacante escucha a escondidas los flujos de datos en el enlace de comunicación entre los puntos finales.

2.2.13.6. Vulnerabilidades de día cero

Las vulnerabilidades de día cero se refieren al riesgo de seguridad que podría ser explotado por un pirata informático pero que el proveedor de software aún conoce.

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipo y Diseño de la Investigación

El diseño de la investigación es del tipo Descriptiva-aplicada, debido a que se analizan los diferentes tipos de vulnerabilidades que se pueden encontrar en las redes WIFI AD-HOC en ambientes outdoor y que podrían ser utilizados por los atacantes. Consiguientemente, se plantearían algunas recomendaciones para mitigar los riesgos presentes en este tipo de redes y así permitir mejorar la seguridad en las redes wifi ad-hoc.

3.1.1. Métodos de Investigación

Para la realización del trabajo de investigación se utilizó los siguientes métodos:

Método Documental: este método fue utilizado para la recopilación de la información de las redes wifi ad-hoc de fuentes documentales, permitiendo descubrir, analizar y sugerir recomendaciones a los problemas encontrados, para poder llevar a cabo este proceso se empleó revistas científicas, libros y tesis los cuales son mencionados en la bibliografía del proyecto de investigación.

Método Científico: este método permitió formular el problema de la investigación, mediante la observación logrando definir y delimitar el tema a estudiar para de esta manera plantear las recomendaciones una vez analizadas las vulnerabilidades existentes en las redes wifi ad-hoc. Este método consta de las siguientes etapas:

- Planteamiento del problema
- Formulación de la hipótesis
- Levantamiento de la información
- Análisis e interpretación de resultados
- Comprobación de la hipótesis
- Difusión de resultados

Método Inductivo: Este método se planteó en la etapa de observación para la formulación de la hipótesis con el objetivo de que brinde una solución al problema planteado.

Método Analítico: Con este método de investigación se pudo revisar y analizar separadamente los elementos que forman parte del proyecto de investigación, permitiendo una comparación entre las variables específicas.

Método Deductivo: Permite analizar las vulnerabilidades existentes y los problemas que pueden ocasionar en el caso de suceder, con los activos de la información; mediante este método se lograra dar las recomendaciones necesarias para mejorar la integridad, disponibilidad y confidencialidad de la información.

Método Experimental: Este método permite integrar nuevos conocimientos adquiridos mediante las pruebas realizadas y los ataques ejecutados a la red, de esta manera examinar las vulnerabilidades encontradas en la red.

3.1.2. Enfoque de la Investigación

El enfoque que se da a la presente investigación es el: Enfoque cuantitativo, debido a que se encargara de recopilar un determinado número de vulnerabilidades para analizar.

3.1.3. Alcance de la Investigación

El alcance que se da a la investigación es de tipo Descriptivo, ya que se va a detallar las fases en las que se realizó los ataques a la red para de esta manera brindar las recomendaciones para mejorar la seguridad.

3.1.4. Técnicas

Las técnicas que van hacer empleadas son las brindadas por la investigación científica siendo:

Revisión Documental: fue empleada para la obtención de archivos de datos, con la finalidad de recoger información relacionada a la investigación planteada.

Preguntas Socráticas: esta técnica permitió plantearse preguntas interrogantes claves de una forma fundamentada y lógica con el propósito de hallar respuestas a estas preguntas planteadas con relación a la investigación.

Observación: es utilizada para verificar las vulnerabilidades existentes en la red y brindar recomendaciones.

3.2. Instrumentos

Los instrumentos utilizados para realizar la investigación y permitir la recopilación de los datos son los siguientes:

Kali Linux: es la distribución especializada en auditoría y seguridad informática. Kali tiene un sinnúmero de herramientas disponibles y orientadas a la seguridad informática y al hacking ético como es: pruebas de penetración, informática forense, ingeniería inversa, etc. (KALI, 2021)

VirtualRouter Plus: es un programa que permite convertir un ordenador en un router y compartir de manera inalámbrica cualquier conexión de internet esta puede ser: WiFi, LAN, módem de acceso telefónico, red móvil, etc. con cualquier otro equipo. Para poder realizar este trabajo de investigación se optó por convertirlo en un router AD-HOC.

3.3. Proceso para el desarrollo de las mejores prácticas de seguridad.

El análisis a realizar mediante un test de penetración que se realiza en este proyecto de investigación, es un proceso específico para encontrar vulnerabilidades existentes en la red y que permita establecer un conjunto de recomendaciones para mejorar la seguridad en este tipo de redes.

Para la realización de esta investigación se tiene 3 fases que permitirán desarrollar el proyecto de manera secuencial, una vez realizado estas fases se procederá a dar un reporte de las vulnerabilidades existentes en la red y así proceder a desarrollar las mejores prácticas para mejorar la seguridad en las redes wifi Ad-Hoc.

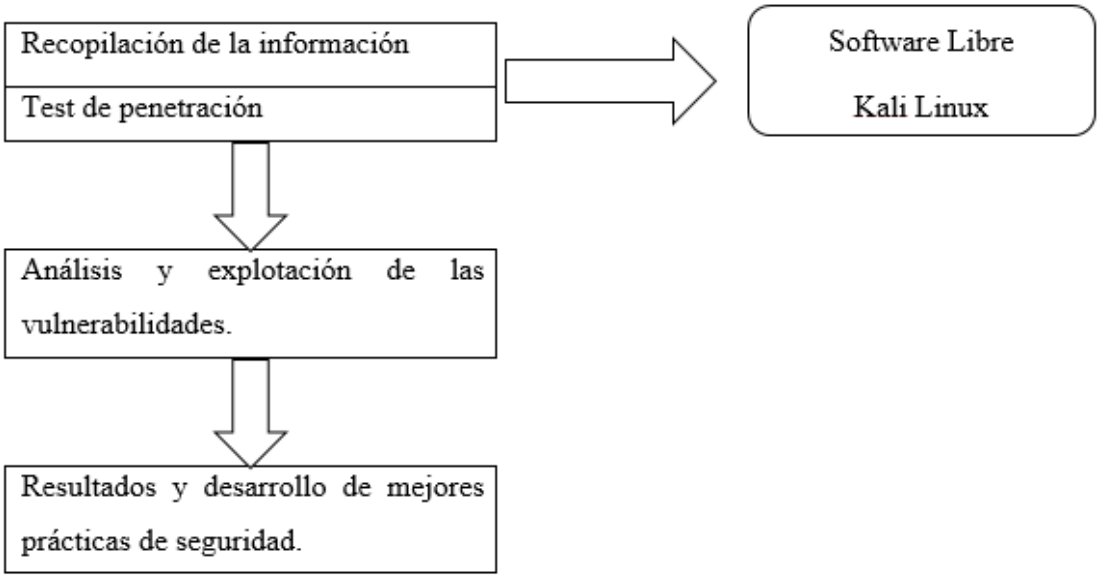

Figura 1 - 3. Diagrama de bloques de la investigación.

Realizado por: (Pilco, 2021)

3.4. Planteamiento de la hipótesis.

Al aplicar el análisis de vulnerabilidades en redes wifi ad-hoc en ambientes outdoor utilizando software libre se permitirá mejorar la seguridad.

3.4.1. Determinación de variables

De acuerdo a la hipótesis planteada se han determinado las siguientes variables:

- ✓ Variable independiente.
  La variable independiente está definida por: Análisis de vulnerabilidades en redes wifi Ad-Hoc mediante software libre en ambientes outdoor.
- ✓ Variable dependiente está definida por: Seguridad de la Información.

3.4.2. Operacionalización Conceptual de Variables

La tabla 1-3, muestra la operacionalización conceptual de las variables determinadas.

Tabla 1 -3. Operacionalización conceptual de las variables determinadas.

VARIABLES	TIPO	DEFINICIÓN
Análisis de vulnerabilidades en las redes wifi AD-HOC mediante software libre en ambientes outdoor.	Independiente.	Estudio de análisis de vulnerabilidades en las redes wifi Ad-Hoc realizados a través de software libre en ambientes outdoor.
Seguridad de la información.	Dependiente.	La seguridad de la información se basa en la confidencialidad, integridad y la disponibilidad de la información dentro de la empresa.

Realizado por: (Pilco, 2021)

3.4.3. Operacionalización Metodológica de Variables.

Tabla 2 - 3. Operacionalización metodológica de las variables determinadas.

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO/FUENTE
Análisis de vulnerabilidades en las redes wifi AD-HOC mediante software libre en ambientes outdoor.	• Número de ataques • Número de puertos abiertos	Búsqueda de información Pruebas Observación	Kali Linux Análisis Estadística.
Seguridad de la información	• N° de puertos explotados. • Facilidad de intrusión	Pruebas Observación Análisis	Kali Linux Observación Implementación

Realizado por: (Pilco, 2021)

3.5. Población y muestra de estudio

3.5.1. Población

La población de la investigación son las pruebas de vulnerabilidad que se realizan en las redes wifi Ad-hoc.

3.5.2. Muestra

El tamaño de la muestra es los ataques que se realiza a la red wifi Ad-Hoc.

3.5.2.1. Herramienta de recolección de datos.

Para la recolección de datos tanto primarios como secundarios se utilizan las herramientas que se tiene en Kali Linux tanto antes de la mitigación como después de la mitigación, para posteriormente realizar un análisis estadístico inferencial.

Tabla 3 - 1. Herramientas de recolección de datos.

HERRAMIENTA	**TIPO DE USO**
Aircrack	Recolección de información primaria de la red.
Zenmap	Escaneo y rastreo de puertos.
Ettercap (Man in the middle)	Permite interceptar conexiones en tiempo real tanto de la red como de un host.
Nessus	Análisis de vulnerabilidades dentro de la red.

Realizado por: (Pilco, 2021)

Las herramientas anteriormente mencionadas, en la actualidad son muy conocidas, de software libre y altamente empleadas para la obtención de información y de esta manera obtener las vulnerabilidades existentes en las redes wifi Ad-Hoc.

3.6. Escenario de pruebas

El escenario de pruebas es en el servidor wifi Ad-Hoc en donde se va a realizar todas las pruebas para determinar las vulnerabilidades existentes en este tipo de redes.

Para continuar con el proceso de la investigación, se ha proseguido con la selección del escenario en donde se va a efectuar el ataque a la red, mediante las herramientas que contiene el sistema operativo empleado para auditoria de redes inalámbricas con el objetivo de escanear y encontrar las vulnerabilidades que presentan estas redes inalámbricas ad-hoc.

3.6.1. Diseño de la red

Para el diseño de la red se tomó en cuenta N usuarios que se van a conectar a la red, con la única limitante del ancho de banda debido a que mientras más usuarios se conecten a la red disminuirá el ancho de banda.

La idea principal es tener una red en la cual se encuentren conectados dispositivos inalámbricos como es: celulares, tablets, laptops entre otros equipos y que puedan hacer uso de internet, mediante el cual se encuentres compartiendo información, realizando video llamadas, envió de documentos, navegar en internet, uso de las redes sociales, entre otras aplicaciones. Ya una vez armada la red se procederá a ejecutar el análisis de vulnerabilidades con Kali Linux que es la herramienta que se emplea para el análisis, como se muestra en la figura 3-2.

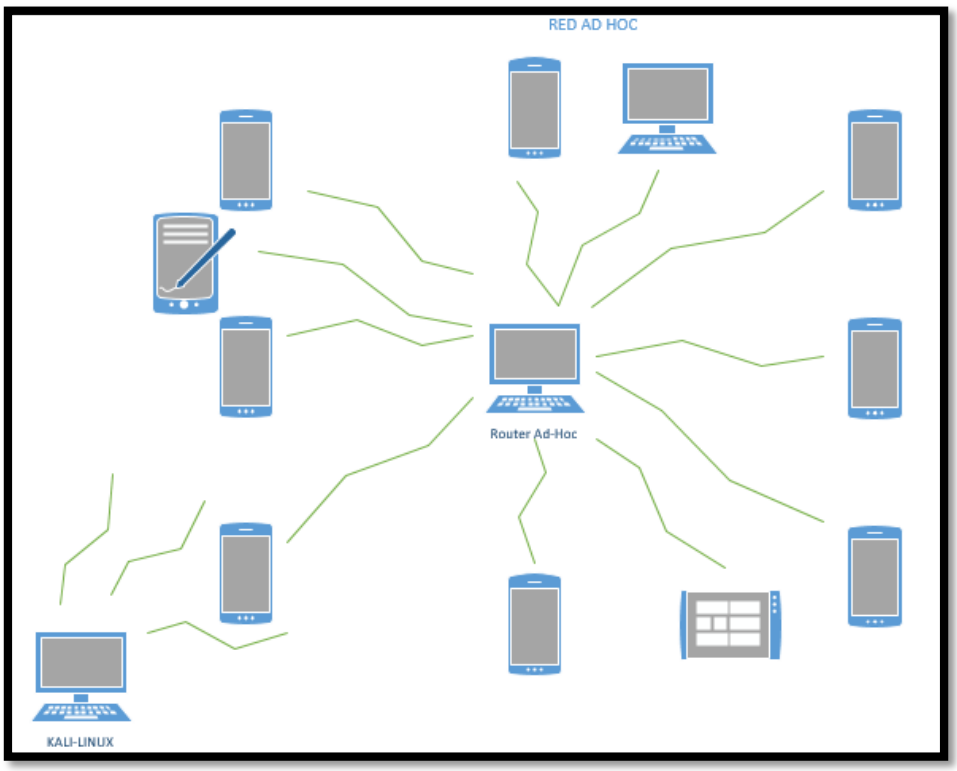

Figura 2 - 3. Diagrama de la red Ad-Hoc.

Realizado por: (Pilco, 2021)

La red está formada por varios dispositivos inalámbricos en donde como router Ad Hoc se encuentra una laptop con conexión Ethernet a internet, en este pc se encuentra instalado el programa Connectify Hotspot, este programa permite convertir al pc en un punto de acceso mediante el cual se va a encargar de repartir internet a los dispositivos que se encuentren al alcance de la red.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

Es este capítulo se realizan las pruebas en el escenario planteado en donde se van analizar y comparar los resultados obtenidos en el análisis a la red, y de esta manera demostrar la hipótesis planteada.

En la siguiente sección se presenta el análisis de los resultados obtenidos en la investigación aplicando los métodos y técnicas definidos, así como su relación con los objetivos y la hipótesis plateada.

4.1. Desarrollo de pruebas

Para el desarrollo de las pruebas se utilizó Kali Linux que contiene herramientas para realizar auditoria en las empresas y seguridad informática. Está basada en Debian/GNU Linux.

4.1.1. Explotación de vulnerabilidades a nivel de red

Para realizar la explotación de vulnerabilidades existentes en las redes wifi Ad-Hoc se realizó varios ataques entre los cuales se tiene:

4.1.1.1. Ataques de fuerza bruta escenario 1.

Se realizó ataques de fuerza bruta a la red wifi Ad-Hoc en el escenario 1 para, analizar qué nivel de seguridad tiene implementado en sus contraseñas. Para de esta manera implementar la guía con las mejores prácticas de seguridad.

Para la ejecución de los ataques de fuerza bruta se procedió a utilizar la herramienta Aircrack de Kali Linux como se muestra en la Figura 1-4.

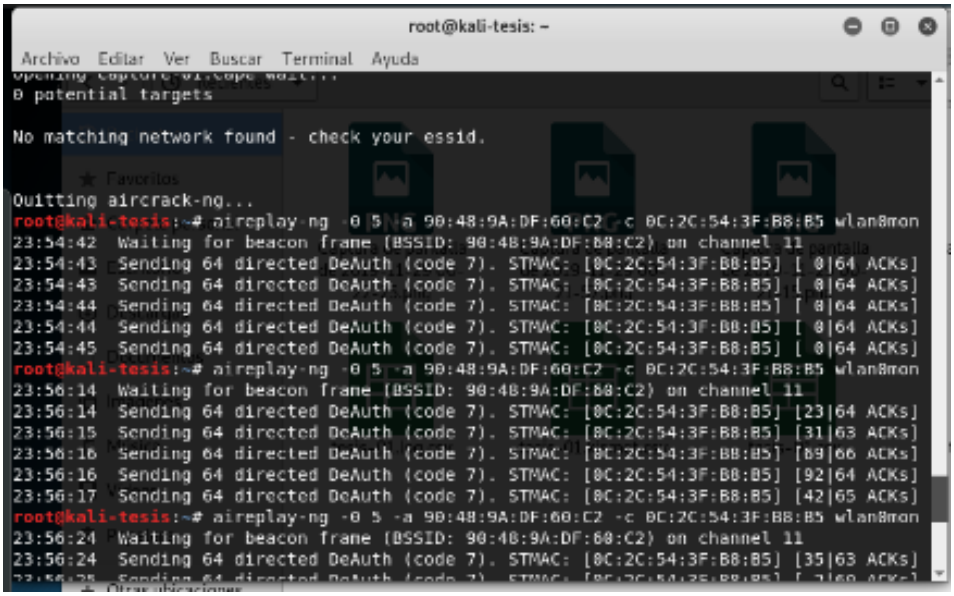

Figura 1 - 4. Escaneo de redes.

Realizado por: (Pilco, 2021)

En la Figura 2-4 al ejecutar el comando aireplay –ng comienza a escanear las redes que se encuentran al alcance y una vez identificada la red que se va atacar se procede a capturar el BSSID de la red Ad Hoc y se comienza a hacer el ataque.

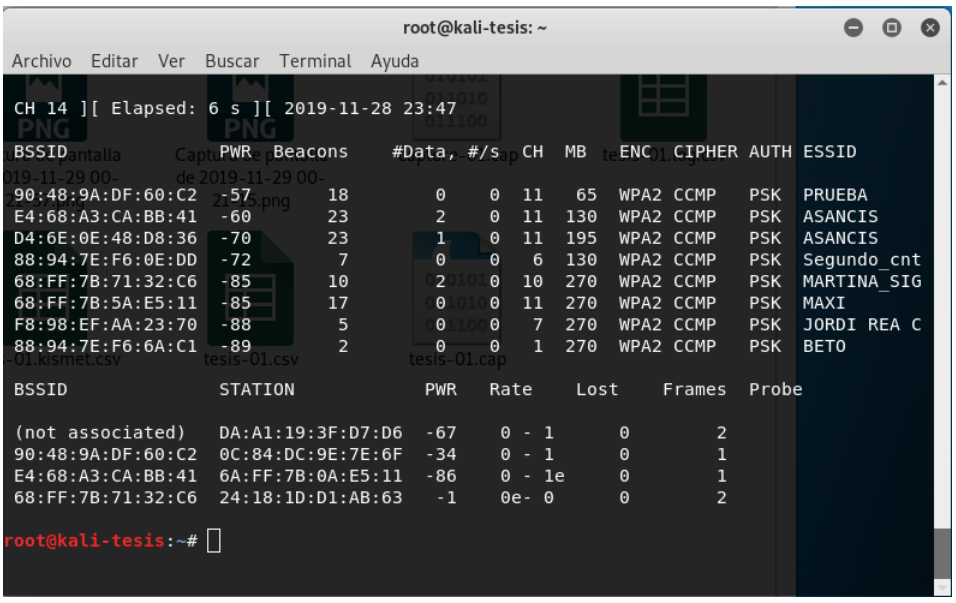

Figura 2 - 4. Identificación de redes WiFi Ad-Hoc.

Realizado por: (Pilco, 2021)

Una vez identificado el BSSID de la red se prosigue a realizar el ataque en donde se selecciona la mac del dispositivo a desconectar para que el equipo que realiza el ataque capture la contraseña, después de unos minutos de realizar el ataque se verificara que se visualiza la palabra handshake, como se puede observar en la figura 3-4, que indica que ya se tiene capturada la contraseña de la red.

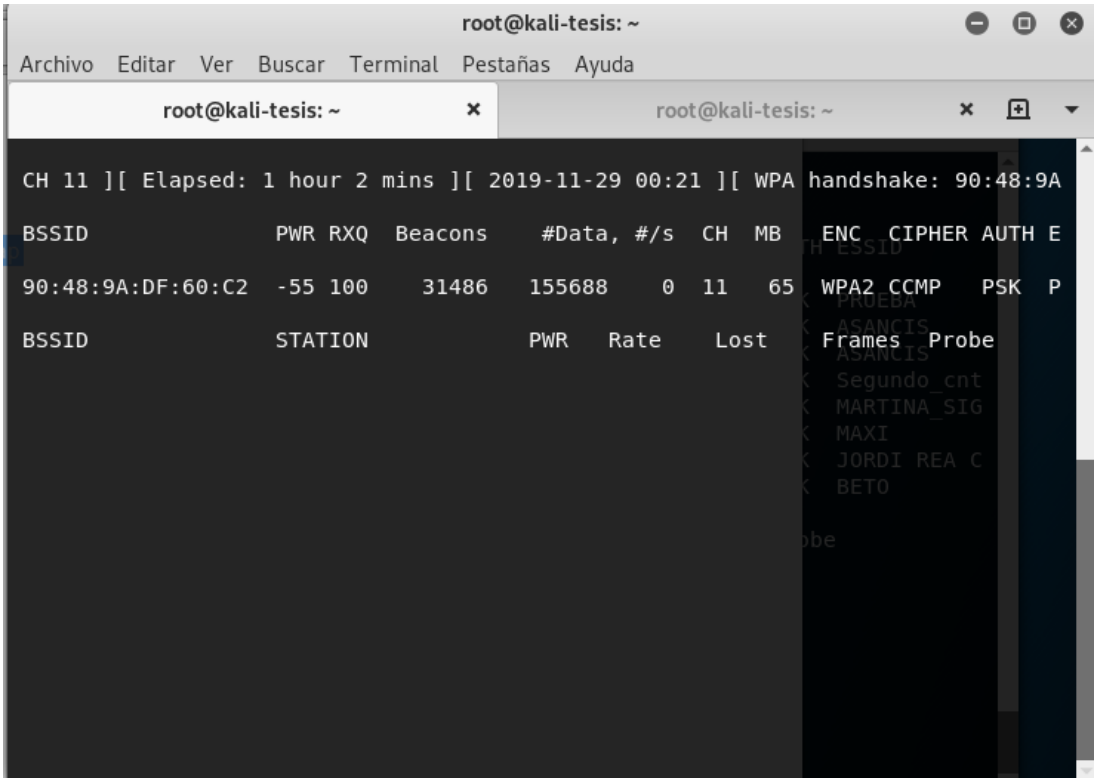

Figura 3 - 4. Generación de handshake.

Realizado por: (Pilco, 2021)

Al generarse el handshake de la red ad hoc se puede verificar que existe la vulnerabilidad de acceso a la red esto debido a que el dispositivo que realiza la función de punto de acceso solo permite la configuración de la seguridad de conexión a la red de tipo WPA, este programa no permite configurar la seguridad WIFI AES que en la actualidad es más robusta debido a que contiene un cifrado de 128 bits.

La generación del handshake es guardado en un documento .cap con el nombre de capture-01.cap como se muestra en la Figura 4-4.

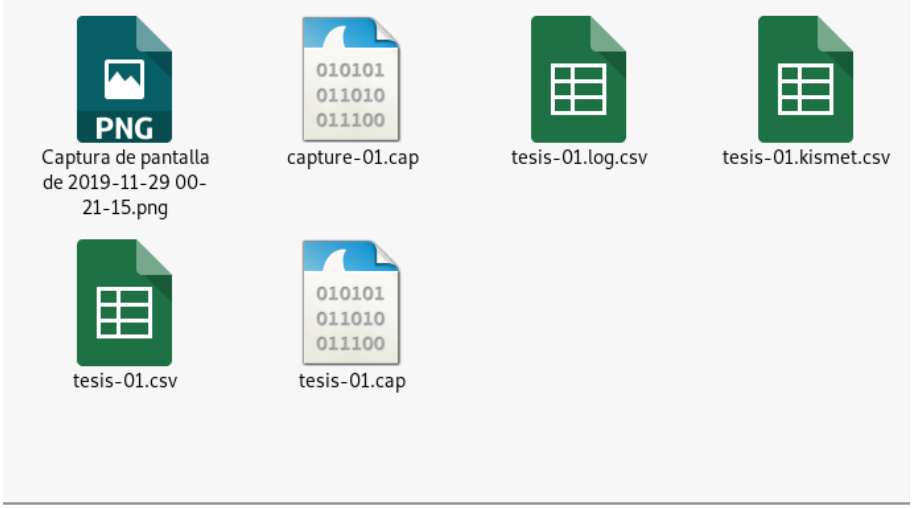

Figura 4 - 4. Archivo generado handshake.

Realizado por: (Pilco, 2021)

En este archivo se encuentra la contraseña de la red, para poder desencriptar se procede a ejecutar la siguiente línea de comando que se visualiza en la figura 5-4.

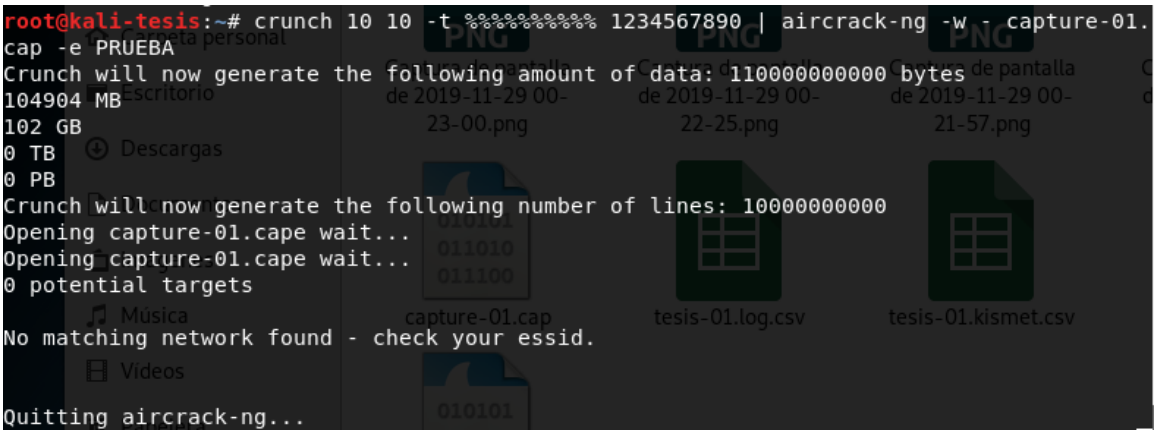

Figura 5 - 4. Des-encriptación handshake.

Realizado por: (Pilco, 2021)

Este proceso tarda unos minutos en des encriptar el hadshake, luego de esto aparece en el editor la palabra KEY FOUND con la contraseña como se muestra en la Figura 6-4.

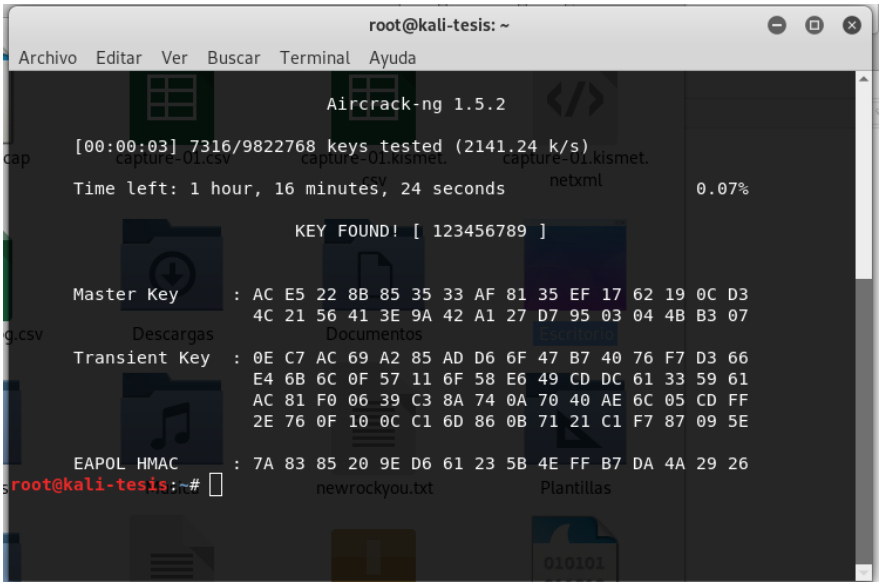

Figura 6 - 4. Handshake des-encriptado.

Realizado por: (Pilco, 2021)

Para analizar qué tan susceptible a este tipo de ataques se realizó también pruebas con la herramienta John de Ripper en donde también se logró descifrar la contraseña de la red y acceder a ella.

Figura 7 - 4. Ataque de fuerza bruta John the Ripper.

Realizado por: (Pilco, 2021)

4.1.1.2. Ataques de fuerza bruta escenario 2.

Para realizar los ataques de fuerza bruta en el escenario 2 se procede a realizar el mismo procedimiento que se realizó en el escenario 1.

Figura 8 - 4. Ataque de fuerza bruta con aircrack fallido.

Realizado por: (Pilco, 2021)

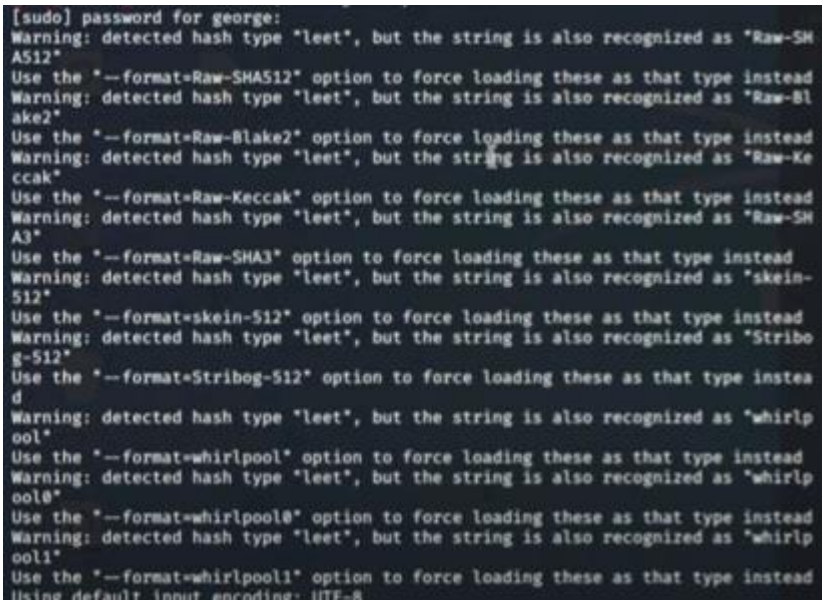

Figura 9 - 4. Ataque de fuerza bruta John the Ripper no exitoso.

Realizado por: (Pilco, 2021)

Tabla 1 - 4. Tabla de resultados de ataques de fuerza bruta efectivos.

Ataques	Escenario 1	Escenario 2	Porcentaje de reducción
Aircrack	5	0	100%
John the Ripper	5	0	100%
Total	10	0	100%

Realizado por: (Pilco, 2021)

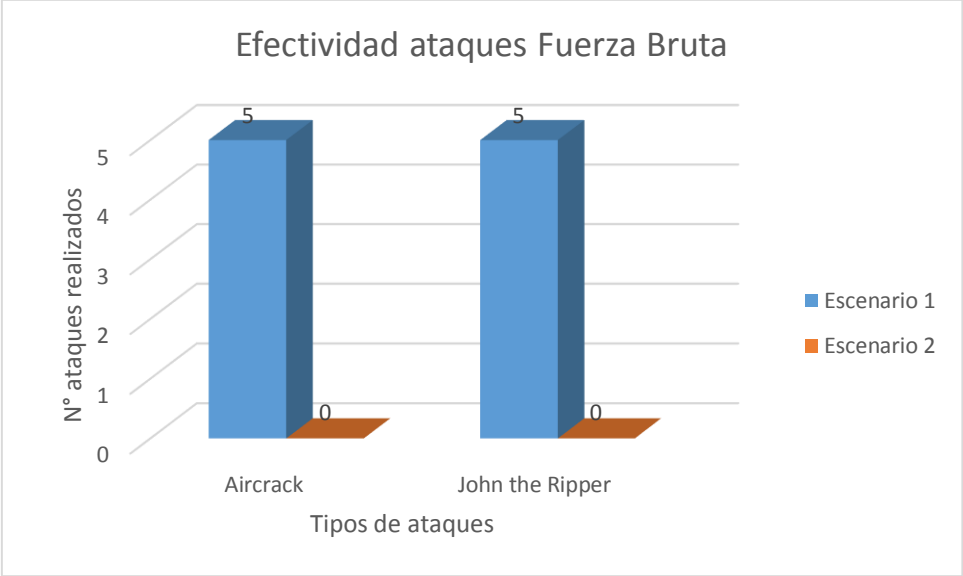

Gráfico 1 - 4. Comparativo efectividad ataques de fuerza bruta.

Realizado por: (Pilco, 2021)

4.2. Escaneo de puertos con Zenmap

Una vez ingresado a la red se procede a escanear los puertos existentes en el servidor wifi mediante la herramienta Zenmap en donde se encuentra la siguiente información como se observa en la Figura 10-4.

El servidor wifi se encuentra con la dirección ip: 192.168.x.x. en donde se puede visualizar los puertos que se encuentran abiertos en el servidor y por donde puede ocurrir algún incidente de seguridad.

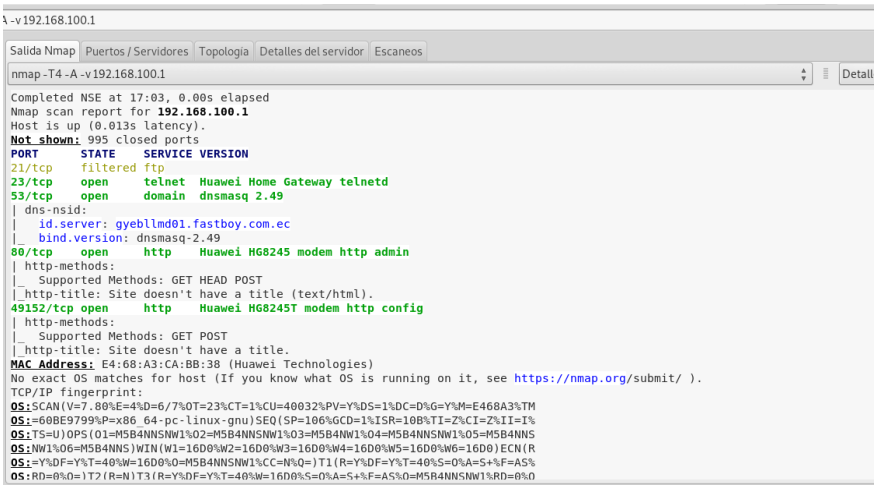

Figura 10 - 4. Escaneo de puertos de la IP 192.168.X.X

Realizado por: (Pilco, 2021)

Una vez realizado el escaneo de puertos existentes en la red se puede observar que se encuentra abierto el puerto 23 de TCP que da al servicio de Telnet, también se encuentra abierto el puerto 53 que es el servicio de DNS, al igual que el puerto 80 de TCP por el cual corre el servicio de HTTP, entre otros puertos más.

Tabla 2 - 4. Puertos que se encuentran abiertos en el servidor WiFi Ad-Hoc escenario 1.

N° Puerto	Protocolo	Servicio	Función
23	Tcp	TELNET	Establecer conexión remota con otros equipos.
53	TCP	DNS	Resolución del nombre de dominio.
80	TCP	HTTP	El servidor HTTP escucha la petición hecha por un cliente.

Realizado por: (Pilco, 2021)

El mismo procedimiento se realiza para escanear los puertos en el escenario 2 en donde solamente se encontró un puerto abierto.

Tabla 3 - 4. Puertos que se encuentran abiertos en el servidor WiFi Ad-Hoc escenario 2.

N° Puerto	Protocolo	Servicio	Función
3389	Tcp	RDP	Establecer conexión remota con otros equipos.

Realizado por: (Pilco, 2021)

4.2.1. Explotación de vulnerabilidades en el servidor wifi Ad-Hoc.

Para la realización de la explotación de la vulnerabilidad encontrada en el escaneo de puertos en el servidor wifi, se utiliza la herramienta de Metasploit de Kali Linux, la cual permitirá ver si esta vulnerabilidad representa un riesgo para la red.

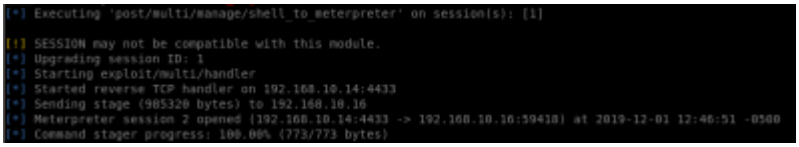

Figura 11 - 4. Ejecución ataque telnet.

Realizado por: (Pilco, 2021)

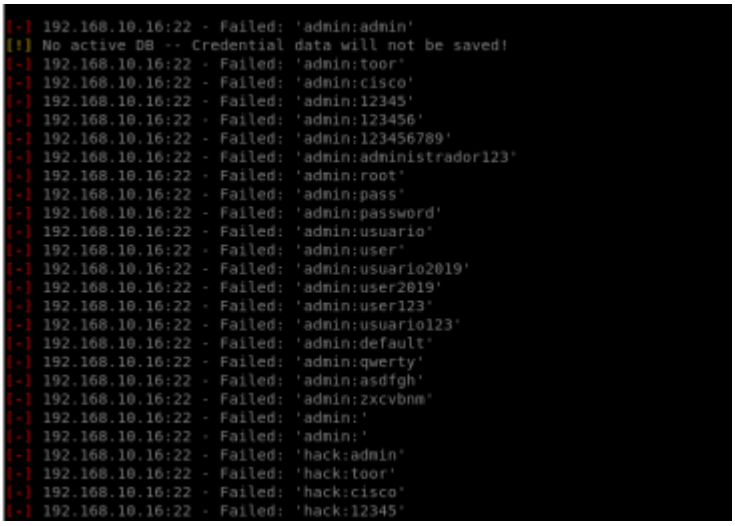

Figura 12 - 4. Ataque telnet exitoso en el server WiFi Ad-Hoc.

Realizado por: (Pilco, 2021)

Inicio del ataque al puerto 53 DNS del servidor WiFi Ad-Hoc.

Figura 13 - 4. Metasploit al puerto 53 DNS server WiFi Ad-Hoc.

Realizado por: (Pilco, 2021)

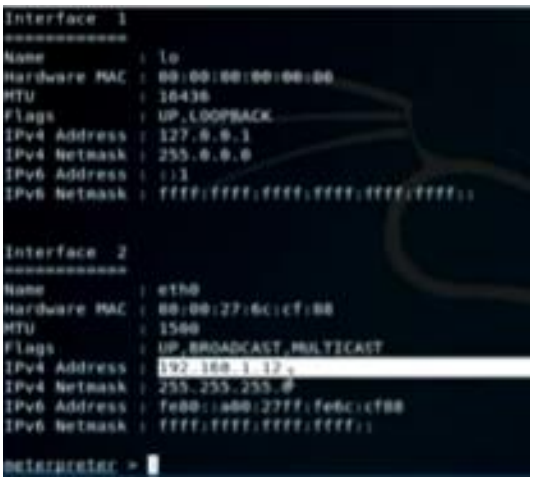

Figura 14 - 1. Ataque exitoso al puerto 53 DNS del server WiFi Ad-Hoc.

Realizado por: (Pilco, 2021)

Ejecución de ataque al puerto 80 escenario 1.

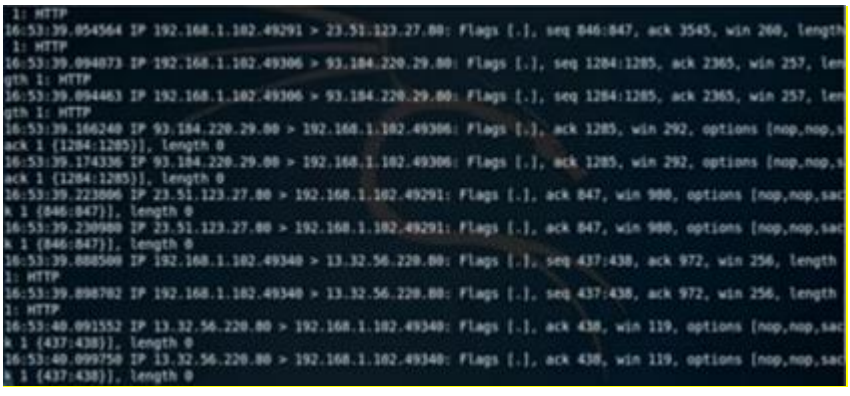

Figura 15 - 4. Ataque puerto 80.

Realizado por: (Pilco, 2021)

Como se puede observar en la figura 4-16 cuando comienza a realizar el ataque al puerto 80.

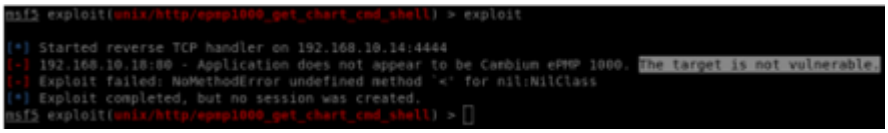

Figura 16 - 4. Puerto 80 no es vulnerable.

Realizado por: (Pilco, 2021)

En esta figura 16-4 se puede observar que el puerto 80 no es vulnerable a este tipo de ataque.

4.3. Ataque Man in the Middle (MITM)

Este ataque se procedió a realizar a la ip del servidor wifi, se realizó un ARP Poisoning a la red para poder capturar el tráfico que se encontraba en la red.

Para realizar este ataque se utilizó la herramienta de Ettercap de Kali Linux.

Figura 17 - 4. Ataque Main in the Middle.

Realizado por: (Pilco, 2021)

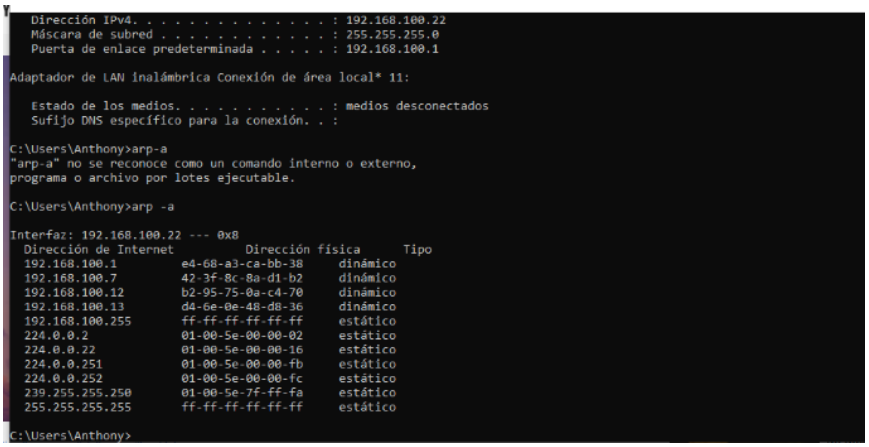

Figura 18 - 4. Ataque efectivo.

Realizado por: (Pilco, 2021)

En la figura 18-4 se puede observar en la máquina a la cual se estaba dirigiendo el ataque, como la maquina con Kali Linux empieza a buscar que el caché de la máquina atacada empiece a registrar y tenga como dirección MAC la del atacante y de esta manera mantenga la dirección IP real de una de las máquinas de la red. Con el objetivo de que todo el tráfico que circule por esa red en dirección a la IP atacada, primeramente, pasará por el terminal atacante, y de esta manera poder el mensaje ser leído, modificado o borrado.

4.4. Análisis de vulnerabilidades con Nessus

Esta herramienta permite escanear las vulnerabilidades existentes en tiempo real en la red, identificando las debilidades existentes en la red y de esta manera evitar el ingreso no autorizado al sistema.

Tabla 4 - 1. Vulnerabilidades en el server WiFi Ad-Hoc escenario 2.

Servidor WIFI Ad-Hoc Huawei HG8245		
	Escala	Tipo de ataque
Vulnerabilidades informáticas	0	
Vulnerabilidades Bajas	0	
Vulnerabilidades Medias	1	CVE -2020-1181 - RDP/DoS
Vulnerabilidades Altas	0	
Vulnerabilidades Criticas	0	

Realizado por: (Pilco, 2021)

De los datos obtenidos en el análisis con la herramienta Nessus al servidor WiFi, se pudo observar el siguiente gráfico.

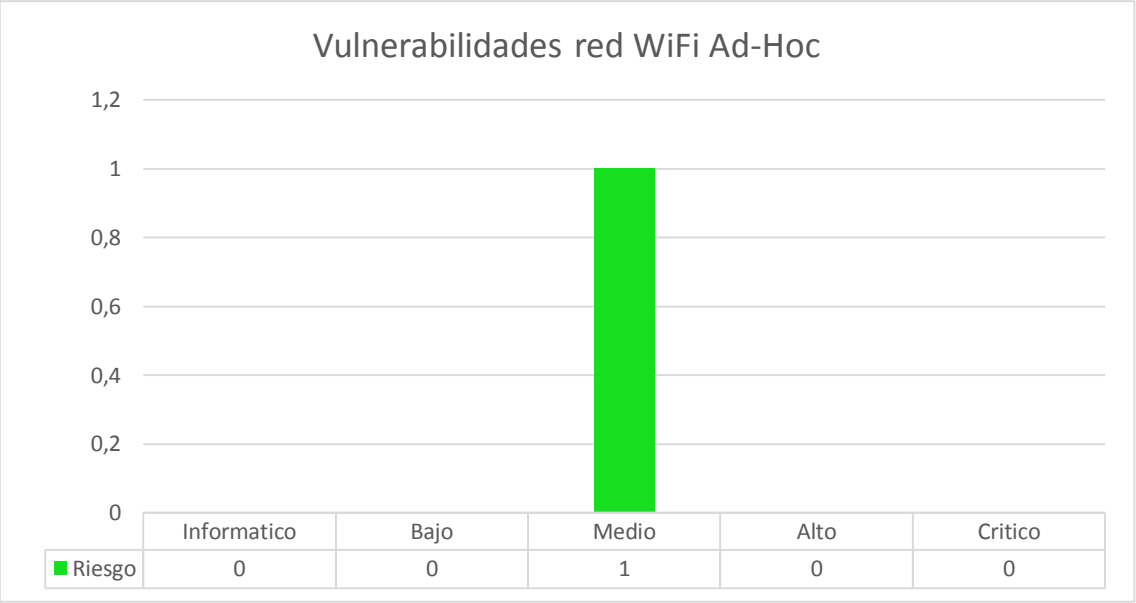

Gráfico 2 - 4. Vulnerabilidades server WiFi Ad-Hoc.

Realizado por: (Pilco, 2021)

4.5. Mitigación de riesgos existentes en el servidor WiFi Ad-Hoc.

CVE -2020-1181 - RDP/DoS

Factor de riesgo: Medio

Sinopsis: Denegación de Servicios (DoS).

Descripción: El servidor WiFi Ad-Hoc tiene habilitado la opción de acceso remoto, lo que es considerado como una vulnerabilidad ya que el atacante puede acceder por este medio al servidor.

Para mitigar los ataques de intrusión a la vulnerabilidad encontrada mediante la herramienta Nessus en el servidor wifi se tiene la siguiente solución:

Solución: Deshabilitar la opción de acceso remoto en el server WiFi Ad-Hoc.

Análisis de vulnerabilidades después de aplicar la mitigación del riesgo.

Tabla 5 - 4. Vulnerabilidades en el server WiFi Ad-Hoc.

Servidor WIFI Ad-Hoc Huawei HG8245		
	Impacto	Tipo de ataque
Vulnerabilidades informáticas	0	
Vulnerabilidades Bajas	0	

Vulnerabilidades Medias	0	
Vulnerabilidades Altas	0	
Vulnerabilidades Criticas	0	

Realizado por: (Pilco, 2021)

En la siguiente tabla se muestra los valores de las vulnerabilidades posteriores a la mitigación.

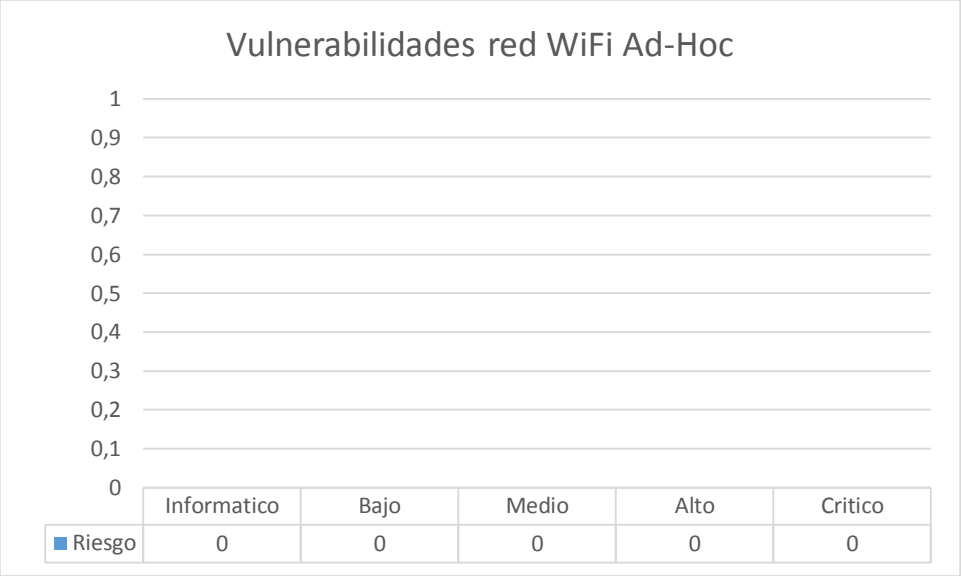

Gráfico 3 - 4. Vulnerabilidades mitigadas.

Realizado por: (Pilco, 2021)

Para poder mitigar el problema de los puertos abiertos sería una solución de cerrar todos los puertos, pero no es una opción recomendable.

Figura 19 - 4. Escaneo de puertos al server WiFi Ad-Hoc después de la mitigación.

Realizado por: (Pilco, 2021)

De acuerdo al código encontrado para explotación de los puertos en estudio, se tiene la siguiente tabla:

Tabla 6 - 4. Amenazas encontradas por servicio.

No.	Servicio	Protocolo	Cantidad de amenazas	Amenazas por s.o.	% de amenazas
1	TELNET	TCP	56	22	39.29
2	DNS	TCP	2434	55	2.26
3	HTTP	TCP	1084	15	1.38
4	RDP	TCP	97	17	17.53

Realizado por: (Pilco, 2021)

- **Porcentaje de riesgo**

Para encontrar este valor se utiliza la ecuación del riesgo, en referencia al análisis obtenido con la herramienta NESSUS.

Tabla 7 - 4. Numero de vulnerabilidades encontradas con NESSUS.

Puerto	Vulnerabilidad	Nivel Impacto	WiFi Ad-Hoc
telnet	crítica	4	0
alta	Alta	3	0
media	Media	2	1
baja	Baja	1	2
dns	crítica	4	0
alta	Alta	3	0
media	Media	2	1
baja	Baja	2	0
http	crítica	4	0
alta	Alta	3	0
media	Media	2	1
baja	Baja	1	1
rdp	crítica	4	0
alta	Alta	3	0
media	Media	2	0
baja	Baja	1	0

Realizado por: (Pilco, 2021)

Para la obtención del valor del impacto de la vulnerabilidad, se multiplica los valores de las vulnerabilidades encontradas por el nivel de impacto mostrado en la herramienta Nessus.

Tabla 8 - 4. Impacto de vulnerabilidad.

Puerto	WiFi Ad-Hoc
telnet	0
	0
	2
	2
Dns	0

	0
	2
	0
http	0
	0
	2
	1
Rdp	0
	0
	2
	0

Realizad por: (Pilco, 2021)

Para establecer un valor de vulnerabilidad por puerto en el servidor, se suman los valores de la tabla anterior.

Tabla 9 - 4. Vulnerabilidades por puerto.

Puerto	**WiFi Ad-Hoc**
telnet	4
dns	2
http	3
rdp	2

Realizado por: (Pilco, 2021)

Para el cálculo del Riesgo se considera la siguiente ecuación (CIIFEN, 2017).

Riesgo = **Vulnerabilidad** x **Amenaza**

Tabla 10 - 4. Calculo del riesgo (Tabla 6-4 X Tabla 9-4)

Puerto	**WiFi Ad-Hoc**
telnet	88
dns	110
http	45
rdp	34
Total	277

Realizado por: (Pilco, 2021)

4.6. Valoración de las variables independientes

Con base al indicador de la variable independiente se ha planteado la siguiente tabla de valores con:

- **Ataques realizados**

Se procede a realizar un análisis y calificación de los dos escenarios planteados.

Tabla 11 - 4. Ataques realizados a la red WiFi Ad-Hoc escenario 1.

Tipo de ataque	Números de ataques
Fuerza Bruta	5
Escaneo de Puertos	1

Realizado por: (Pilco, 2021)

Tabla 12 - 4. Ataques realizados a la red WiFi Ad-Hoc escenario 2.

Tipo de ataque	Números de ataques
Fuerza Bruta	0
Escaneo de Puertos	1

Realizado por: (Pilco, 2021)

- **Números de puertos abiertos.**

En la siguiente tabla se muestra los números de puertos abiertos que se encontraron en el servidor WiFi Ad-Hoc antes y después de la mitigación.

Se considera que todo puerto abierto dentro de una red puede ser explotado.

Tabla 13 - 4. Puertos abiertos encontrados en el escenario 1.

N°	Servicio	Puerto
1	Telnet	23
2	DNS	53
3	HTTP	80

Realizado por: (Pilco, 2021)

Tabla 14 - 4. Puertos abiertos encontrados en el escenario 2.

N°	Servicio	Puerto
1	RDP	3389

Realizado por: (Pilco, 2021)

4.7. Valoración de la variable dependiente

Variable Dependiente: Seguridad de la información

Para valorar esta variable se realiza una observación de la validación respecto del cumplimiento de los indicadores planteados antes y después de la aplicación de los mecanismos de mitigación.

- **Número de puertos explotados**

  Para realizar la valoración de la variable dependiente se tomó en cuenta los tres puertos que fueron explotados.

Tabla 15 - 4. Puertos explotados.

N°	SERVICIO	PROTOCOLO	PUERTO
1	telnet	TCP	23
2	DNS	TCP	53
3	HTTP	TCP	80

Realizado por: (Pilco, 2021)

- **Facilidad de intrusión**

Para la valoración de este factor se tomó en cuenta la escala de Likert (Matas, 2018), permitiendo obtener una valoración con respecto a la facilidad de intrusión a una red WiFi Ad-Hoc se observa el resultado respecto a este indicador.

Tabla 16 - 4. Escala Likert.

Escala	Valoración
No es posible	1
Poco Fácil	2
Moderado	3
Fácil	4
Muy fácil	5

Realizado por: (Pilco, 2021)

Tabla 17 - 42. Facilidad de intrusión en función de los ataques realizados escenario 1.

Ataques	Servidor WiFi Ad-Hoc
Fuerza Bruta	25
Puertos Explotados	15
TOTAL	**40**

Realizado por: (Pilco, 2021)

Facilidad de intrusión: 40 (correspondiente al 100%), debido a que todos los ataques realizados tuvieron una valoración de 5 (muy fácil para intrusión).

- **Porcentaje de mitigación**

Esta valoración se mide en relación al porcentaje de riesgo de Seguridad existente en el escenario 1, para ello se considera que inicialmente no se han establecido mecanismos de mitigación.

Tabla 18 - 4. Porcentaje de mitigación del riesgo.

	WiFi Ad-Hoc
Total	0

Realizado por: (Pilco, 2021)

El porcentaje de mitigación es 0, debido a que en el escenario 1 no se realizó ninguna medida de mitigación.

Tabla 19 - 4. Facilidad de intrusión en función de los ataques realizados escenario 2.

Ataques	**Servidor WiFi Ad-Hoc**
Fuerza Bruta	0
Puertos explotados	1
TOTAL	**1**

Realizado por: (Pilco, 2021)

Facilidad de intrusión: 1 (correspondiente al 20%), ya que si el puerto abierto tuviera una valoración de 5 (muy fácil para intrusión) se tendría un total de 5 (que equivale al 100%).

- **Porcentaje de mitigación**

El porcentaje de mitigación del riesgo después de aplicar la mitigación a los problemas encontrados es los siguientes:

Tabla 20 - 4. Porcentaje de mitigación después de la mitigación.

	WiFi Ad-Hoc
Total	80

Realizado por: (Pilco, 2021)

Esta valoración se mide en relación a la facilidad de intrusión antes y después de aplicar las mitigaciones.

- **Porcentaje de mitigación en los dos escenarios.**

Tabla 21 - 4. Porcentaje de mitigación del riesgo.

	Servidor WiFi Ad-Hoc
Facilidad antes	40
Facilidad después	1
Porcentaje de facilidad	2,5%
Porcentaje de mitigación después	97,5%

Realizado por: (Pilco, 2021)

Tomando en cuenta que el valor de la facilidad antes de la mitigación sería el 100%, se calcula con una regla de tres la obtención del Porcentaje de Facilidad posterior a la mitigación.
El porcentaje de Mitigación correspondería al complemento al 100% del porcentaje de Facilidad obtenido. Por lo que, en promedio, el Porcentaje de Mitigación es del 98%.

4.8. Comprobación de Hipótesis.

Para la comprobación de la hipótesis general "Al aplicar el análisis de vulnerabilidades en redes WiFi Ad-Hoc en ambientes outdoor utilizando software libre se permite mejorar la seguridad", se utilizó estadística inferencial a través de la aplicación de la prueba Chi-Cuadrado (X^2).

Luego de realizar los respectivos análisis y, luego de la obtención de los datos se define la Hipótesis de investigación Hi y la Hipótesis nula Ho:

Hipótesis de investigación Hi: "Al aplicar el análisis de vulnerabilidades en redes WiFi Ad-Hoc en ambientes outdoor utilizando software libre **si** permitirá mejorar la seguridad". **Hipótesis de Nula H_0:** "Al aplicar el análisis de vulnerabilidades en redes WiFi Ad-Hoc en ambientes outdoor utilizando software libre **no** permitirá mejorar la seguridad".

La tabla siguiente muestra la frecuencia de los valores encontrados en las pruebas realizadas, estos valores son empleados en el cálculo de la prueba.

Tabla 22 - 4. Frecuencia de valores encontrados.

	Escenario 1	**Escenario 2**	**Total**
Vulnerabilidades Encontradas	15	1	16
Vulnerabilidades Solventadas	0	1	1
Total	15	2	17

Realizado por: (Pilco, 2021)

Para la obtención de la tabla de frecuencias esperadas se aplica la siguiente fórmula en cada valor de la tabla.

$$\text{Fe} = \frac{Total\ columna * Total\ fila}{Suma\ total}$$

Después de la aplicación de la formula en cada valor de la tabla 4-15, se obtuvo los siguientes valores de frecuencias esperadas.

Tabla 23 - 4. Frecuencias esperadas.

	Escenario 1	**Escenario 2**	**Total**
Vulnerabilidades Encontradas	14,1176471	1,88235294	16
Vulnerabilidades Solventadas	0,88235294	0,11764706	1
Total	15	2	17

Realizado por: (Pilco, 2021)

Seguidamente, se calcula el valor de X^2eempleando la siguiente formula:

$$X^2 = \sum \frac{(FO-FE)^2}{FE}$$

Dónde:

FO: Frecuencia observada por celda.

FE: Frecuencia esperada por celda.

$$X^2 = \frac{(15-14.1176)^2}{14.1176} + \frac{(1-1.8823)^2}{1.8823} + \frac{(0-0.8823)^2}{0.8823} + \frac{(1-0.1176)^2}{0.1176}$$

$$X^2 = 0.05515 + 0.41.36 + 0.8823 + 6.6176$$

$$X^2 = 7.968$$

A continuación, se procede a calcular los grados de libertad:

$$v = (r-1)\ x\ (k-1)$$

Dónde:

r: Número de filas

k: Número de columnas

$$v = (2 - 1)\ x\ (2 - 1)$$

$$v = 1$$

En referencia a la tabla de la distribución de Chi-Cuadrado (Figura xx), y determinando el valor de significancia de 0.05% obtenemos el punto crítico con 1 como valor de grados de libertad.

Tabla 24 - 4. Distribución Chi Cuadrado

TABLA 3-Distribución Chi Cuadrado χ^2

P = Probabilidad de encontrar un valor mayor o igual que el chi cuadrado tabulado, ν = Grados de Libertad

ν/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

Fuente: (Universidad Rey Juan, 2020)

$$X^2 crítico = 3{,}8415$$

Dado los datos anteriores Ho debe ser aceptada si sucede el siguiente condicionante:

$$X^2 calculado \leq X^2 crítico$$

Caso contrario se rechaza Ho y se Acepta Hi.

Con los datos obtenidos anteriormente donde $X^2 = 7.968$ y $X^2 crítico = 3{,}8415$ se puede aplicar el criterio de decisión, obteniendo que:

$$X^2 calculado\ 7.968 > X^2 crítico\ 3{,}8415$$

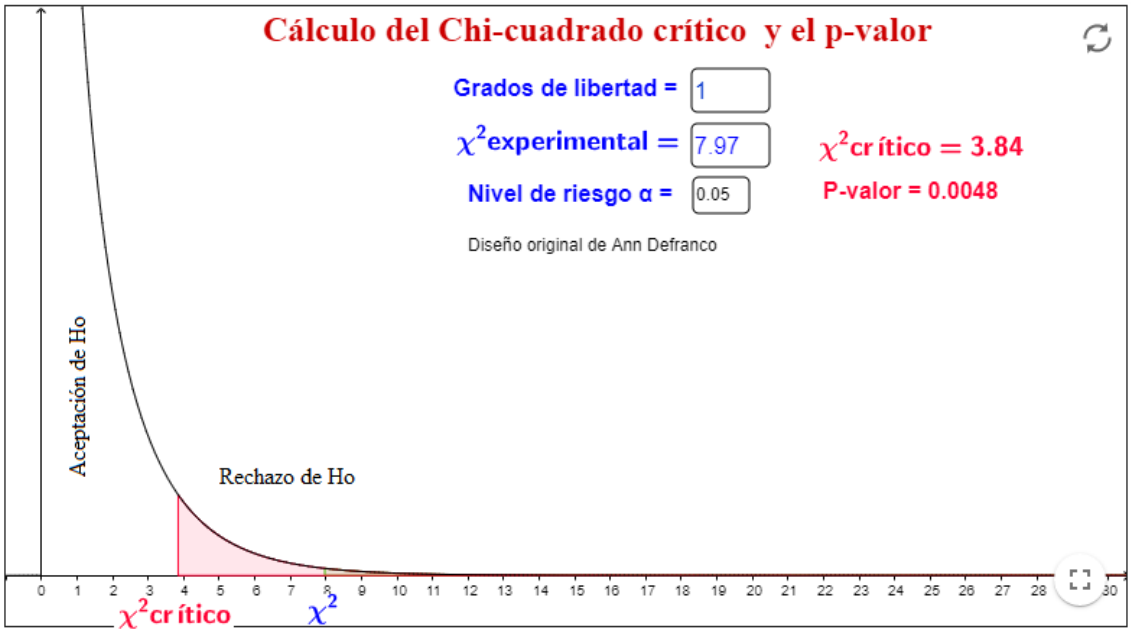

Gráfico 4 - 1. Chi Cuadrado y criterios de aceptación de Hi.

Fuente: (Geogebra, 2019)

Realizado por: (Pilco, 2021)

4.9. Interpretación y análisis

Consecuentemente con los datos obtenidos y de acuerdo a la gráfica se concluye que:

Se rechaza la Hipótesis nula Ho y se acepta la Hipótesis alternativa Hi, con un nivel de confianza de 95% y un nivel de significancia de 5%.

CAPÍTULO V

5. PROPUESTAS DE UNA GUÍA DE BUENAS PRACTICAS PARA MEJORAR LA SEGURIDAD EN LAS REDES WIFI AD-HOC.

Las buenas prácticas en el uso de las redes WiFi Ad-Hoc permite crear un entorno seguro y confiable, en la actualidad en todo entorno en el que se convive se tiene que hacer uso de las redes WiFi debido a que las labores cotidianas están inmersas en el uso del internet, es por ello que surge esta guía para permitir mejorar la seguridad en este tipo de redes y minimizar lo más que se pueda las vulnerabilidades.

Se da en aclaratoria que algunos de los casos expuestos no tienen una solución definitiva, debido a que según va avanzando la tecnología siguen surgiendo nuevas técnicas de atacar.

Uno de los objetivos principales de esta guía es asegurar las redes WIFI Ad-Hoc ante vulnerabilidades existentes:

5.1. Descripción de ataques y técnicas de mitigación.

Dentro de los ataques realizados a la red AD-HOC y por ende a los protocolos TCP/IP se tiene:

5.1.1. Ataques por fuerza bruta.

Esta técnica de fuerza bruta es una modalidad de ataque mediante la cual se intenta obtener acceso no autorizado realizando intentos reiterados y sistemáticos de login sobre un servicio de red, a través de la utilización de credenciales potencialmente válidas. (Traberg, 2015)

Este tipo de ataques puede darse de diferentes maneras como es:

- ✓ Estándar: Consiste en repetir a través de todas las contraseñas posibles, almacenadas dentro del dispositivo atacante, una a la vez. Es usado comúnmente en archivos locales, donde no hay límites para la cantidad de intentos que se realiza.
- ✓ Diccionario: este ataque consiste en usar una lista de palabras y contraseñas comunes que se tiene almacenado y de esta manera atacar de una mejor manera a la red y ahorrar tiempo en la ejecución del ataque.
- ✓ De arco iris: Este tipo de ataque parten de valor hash para reproducir los pasos de la cadena hasta obtener la contraseña. Muchas veces el valor no se encuentra en la tabla; por lo que se recrea al reducir el valor con la misma función con la cual se creó la cadena. (Traberg, 2015)

5.1.1.1. Medidas de mitigación del ataque de Fuerza bruta.

- ✓ Contraseñas: dentro de la configuración del equipo se debe de utilizar el tipo de encriptación AES, que es la más segura y se encuentra actualizada, aunque ya existen ataques para este tipo de encriptación. Para tener un servidor seguro se debe investigar el tipo de encriptación que se puede configurar.
- ✓ Utilizar contraseñas robustas, es decir que contengan tanto caracteres alfanuméricos, numéricos y caracteres especiales y que no haya repetición de letras.

5.2. Ataques de escaneo de puertos

Este ataque permite analizar de manera automática todos los puertos abiertos de un equipo y a su vez permiten analizar cuáles de los puertos tienen protocolos de seguridad pocos seguros.
Estas falencias en seguridad son conocidas como agujeros de seguridad y es por donde los atacantes pueden ingresar y cometer los atracos que deseen realizar como es robar la información personal de la empresa, capturar contraseñas, etc.
Se debe tener en cuenta que existen 65.535 puertos y cada uno de ellos cumple una función específica, hay q tener en cuenta que muchos de los puertos pueden estar abiertos y es criterio del personal de seguridad si cierra o no estos puertos.
Para conocer si un puerto está abierto o no este responderá con un ACK y enviará alguna información y en el caso de que el puerto se encuentre cerrado este responderá con un RESET (RST).
Este tipo de ataque son uno de los primeros que los hackers realizan con la finalidad de tener conocimiento de que puertos están abiertos y así de esta manera planificar mejor los ataques a los servicios que están ejecutándose en esa IP escaneada.
Para realizar este tipo de ataque existen varias herramientas para ejecutar, pero en este caso se usó NMAP.
NMAP: es una herramienta que permite monitorear la red en busca de puertos abiertos para de esta manera poder realizar otro ataque a los servicios que se están ejecutando.
Escaneo del puerto 53/TCP del servidor WiFi Ad-Hoc.

Figura 1 - 5. Explotación de vulnerabilidades del puerto 53.

Realizado por: (Pilco, 2021)

5.2.1.1. 4. Medidas de mitigación del ataque Escaneo de puertos

- ✓ Para evitar este tipo de ataque lo más recomendado es no abrir todos los puertos y al abrir los puertos se debe realizar solo los puertos necesarios.
- ✓ Utilizar un firewall para evitar el ingreso de intrusos en la red, también es una buena práctica tener actualizados los servicios de los puertos que se encuentran abiertos.
- ✓ Implementar SNORT dentro del servidor WiFi Ad-Hoc, ya que este permite la prevención y detección de intrusos dentro de la red, proporcionando la información en el caso de que estén escaneando los puertos del servidor.

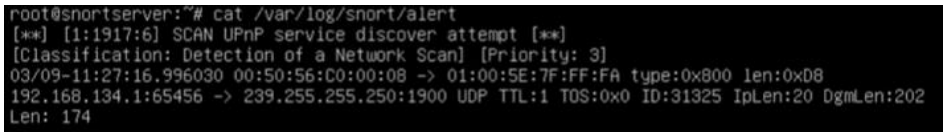

Figura 2 - 5. Logs recibidos de la regla de SNORT configurado ante escaneo de puertos.

Realizado por: (Pilco, 2021)

5.2.2. Ataques de Denegación de Servicio (DoS)

Un ataque de denegación de servicio, tiene como objeto inhabilitar el uso de un sistema, una aplicación o una máquina, con la finalidad de bloquear el servicio que presta dentro de la red. Este tipo de ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática (Internauta, 2018).

5.2.2.1. Medidas de Mitigación de los ataques de Denegación de Servicio (DoS)

Para poder mitigar estos ataques se debe realizar las siguientes recomendaciones:

- Todos los servicios, aplicaciones y sistemas operativos mantenerlos siempre actualizados, para evitar que se encuentren fallas que van surgiendo con el desarrollo de la tecnología.
- Implementar tiempos mínimos de conexión, debido a que algunos servidores vienen configurados con un tiempo de conexión de 3000 segundos, lo que se considera demasiado tiempo ya que en este tiempo se puede aprovechar para abrir conexiones.
- Implementar un IDS que permita monitorear las conexiones realizadas y emita alertas en el caso de accesos no autorizados.

5.3. Ataques de Man in the Middle

Este ataque consiste en interceptar la información entre dos partes y a su vez puede simplemente escuchar o a su vez puede copiar, modificar o eliminar la información.
Existen diferentes tipos de ataques Man in the Middle como son:

- Simulación de un punto de acceso inalámbrico: Consiste en configurar conexiones WiFi con nombres que parecen genuinos con el objetivo de monitorear la actividad del usuario conectado a esta red y de esta manera capturar la información que circula por esta red.
- Ataques basados en servidores DNS: consiste en crear un servidor DNS falso conocido con el nombre de "spoofing" para ello el DNS falso enruta el nombre de un sitio web real a una dirección IP diferente, para cuando la víctima visite el sitio web falso el atacante pueda capturar la información confidencial de la víctima.
- ARP cache poisoning: consiste en que un usuario envía una solicitud ARP y un pirata informático envía una respuesta falsa.

5.3.1. *Medidas de Mitigación a Ataques Man in the Middle.*

- Mantener actualizado el software y el firmware mediante políticas que permitan actualizar el sistema y de esta manera evitar este tipo de ataques.
- Educar y concientizar a las personas que deben estar pendientes de ingresar a enlaces incorrectos y siempre que estén pendientes de cuando navegan en internet se encuentren en páginas que contengan certificados SSL.

- Cifrado y VPN: usar siempre cifrado en todos los dispositivos que contienen información sumamente importante y si fuera el caso usan VPN para crear un canal de comunicación seguro y encriptado.

CONCLUSIONES

- Al analizar las redes WiFi Ad-Hoc en ambientes outdoor se logró encontrar vulnerabilidades asociadas a este tipo de redes, las cuales se pudo explotarlas para verificar que tan vulnerable se encuentran las redes a los tipos de ataques que se ejecutó como fue los ataques de fuerza bruta y escaneo de puertos.

- Para realizar los ataques a la red WiFi Ad-Hoc se lo hizo mediante el uso de herramientas de hacking del sistema Kali-Linux como es Aircrack, Nmap, John the Ripper, con las cuales se pudo determinar las vulnerabilidades existentes en las redes WiFi Ad-Hoc en ambientes outdoor, que fueron susceptibles a ataques de fuerza bruta y también permitió realizar escaneo de puertos en donde se pudo observar que existían puertos abiertos de protocolo TCP.

- Luego de haber analizado las vulnerabilidades encontradas en estas redes, se planteó el escenario con sistemas virtualizados para poder realizar la explotación de las vulnerabilidades existentes y acceder a la información que se encontraba en la red, las vulnerabilidades fueron solventadas siempre que se realice un escaneo a la red con el objetivo de precautelar la información y solucionar los huecos de seguridad que se presenten, mediante la aplicación de una guía de mejores prácticas.

- Mediante los valores obtenidos en la estadística referencial se obtuvo chi-cuadrado con un nivel de significancia de 0.05 y con base en la tabla de distribución son: tabla de $X^2 = 3.84$, mientras que el valor X^2 calculado en la investigación es de 7.968, siendo este último mayor a X^2 de la tabla de distribución, y a la vez que se encuentra en el sector de NO aceptación de la Hipótesis Ho con un resultado estadístico significativo, por lo que se acepta la Hipótesis investigativa Hi.

- El estudio de investigación ha permitido ver de una manera práctica los riesgos de seguridad que tienen estas redes, permitiendo de esta manera desarrollar una guía de mejores prácticas para mitigar los riesgos existentes.

RECOMENDACIONES

- Se recomienda que siempre en todas las redes que se tengan se realice un análisis de vulnerabilidades una vez cada seis meses para de esta manera evitar cualquier incidente de seguridad que pueda ir surgiendo y evitar que se puedan explotar las vulnerabilidades encontradas en las redes WiFi Ad-Hoc en ambientes outdoor.

- Como se conoce que los ataques de intrusión pueden realizarse tanto interna como externamente se recomienda tener una red informática bien robusta tanto a nivel de hardware como de software al igual que mantener actualizados los firewalls de los equipos y si es el caso de las maquinas o servidores Linux implementar IDS para mejorar la seguridad de la misma y realizar ataques de manera preventiva a la red para ver qué tan robusta se encuentra la red WiFi Ad-Hoc.

- Siempre en toda empresa u organización que se tenga una red WiFi Ad-Hoc se debe tener una guía de mejores prácticas para irlas empleando de manera continua para así mejorar la seguridad en este tipo de redes.

- Se recomienda mantener los sistemas actualizados de toda la red y solo mantener los puertos abiertos en el caso que sea necesario para de esta manera evitar ataques por este medio.

- Para brindar mayor seguridad hay que tener configurado el tipo de encriptación más actual como es el caso de la encriptación tipo AES.

BIBLIOGRAFÍA

Abdulrahman, A. A. (2016). MULTI-LEVEL WINDOWS EXPLOITATION USING LINUX OPERATING SYSTEM. *Asian Journal of Natural & Applied Sciences* , 2-8.

Buenaño Rojas, A. I. (2018). *HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD.* Ambato: UTA.

Castro, M. I., Moràn, G. L., Navarrete, D. S., Cruzatty, J. E., Anzúles, G. R., Mero, C. J., . . . Merino, M. A. (17 de Octubre de 2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES* . Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

College, W. L. (2010). *Familia IEEE 802.11*. Obtenido de Diseño de la WLAN de Wheelers Lane Technology College: http://bibing.us.es/proyectos/abreproy/11579/fichero/f.+Cap%C3%ADtulo+2+-+Familia+IEEE+802.11.pdf+

Debao Xiao, M. W. (2006). Secure-SPIN: Secure Sensor Protocol for Information via Negotiation for Wireless Sensor Networks. *School of Information Engineering, WuHan University of Technology Wuhan, Hubei Province, China, 430070* , 1-5.

Fabio Asecio, P. C. (2013).

Flores, R. (2015). Redes Inalámbricas. *Colegio Nacional de Educación Profesional Técnica*, 1-15.

Geogebra. (2019).

González, A. (2014). REDES AD HOC . *Departamento de Electrónica Universidad Técnica Federico Santa María*, 1-7.

Internauta, O. d. (21 de Agosto de 2018). *Ataques DoS* . Obtenido de https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

KALI. (22 de Abril de 2021). *Kali Linux.* Obtenido de https://www.kali.org/docs/introduction/what-is-kali-linux/

Kanika Sharma, N. D. (2014). A Study of Wireless Networks: WLANs, WPANs, WMANs, and WWANs with Comparison. *International Journal of Computer Science and Information Technologies*, 7810-7813.

Lorenzana, V. R. (2015). *Redes Inalambricas.* Obtenido de Redes Inalambricas : http://bibing.us.es/proyectos/abreproy/11460/fichero/Memoria%252F3.-+Redes+Inal%C3%A1mbricas.pdf+

Manuel Ramírez, C. P. (Mayo de 2015). *Seguridad Inalambrica.* Obtenido de http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf

Matas, A. (2018). Diseño del formato de escalas tipo Likert: un estado de la cuestión. *Revista electrónica de investigación educativa*.

Molva, P. M. (2015). Ad hoc networks security. *citeseerx*, 1-28.

Petar Čisar, S. M. (2018). Security Assessment with Kali Linux. *BÁNKI KÖZLEMÉNYEK 1. ÉVFOLYAM 1. SZÁM*, 49-52.

Pilco, A. (2021). Tesis. Ecuador.

SALAZAR, J. (2016). *Redes Inalambricas* . Obtenido de Redes Inalambricas : https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

Shohei Sato, A. K., & Barolli, L. (2011). MANET-Viewer II: A Visualization System for Visualizing Packet Flow in Mobile Ad-hoc Networks . *Workshops of International Conference on Advanced Information Networking and Applications*, 549.

Teddy Surya Gunawan, M. K. (2018). On the Review and Setup of Security Audit Using Kali Linux. *Indonesian Journal of Electrical Engineering and Computer Science*, 51-59.

Traberg, G. (Mayo de 2015). *Swarming - Implementación para la ejecución inteligente de ataques de fuerza bruta.* Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/48092/Documento_completo__.pdf?sequence=1&isAllowed=y

Universidad Rey Juan, C. (2020). *Tabla de la distribución chi-cuadrado.*

Universidad, M. (15 de Abril de 2014). *INTRODUCCIÓN A LAS REDES MANETS.* Obtenido de SIMULACIÓN DE PROTOCOLOS DE ENRUTAMIENTO PARA MANET CON NS3: http://repositorio.cedia.org.ec/bitstream/123456789/960/1/T1_Introduction_MANET_vf.pdf

Yan, Z. (2014). Security in Ad Hoc Networks. *Helsinki University of Technology*.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: *29 / 11 / 2021*

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: *María Alexandra Pilco Llumitaxi*
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: *Magíster en Seguridad Telemática*
f. Analista de Biblioteca responsable*:* *Lic. Luis Caminos Vargas Mgs.*

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602766974, cn=LUIS ALBERTO CAMINOS VARGAS
Fecha: 2021.11.29 13:02:28 -05'00'

0109-DBRAI-UPT-IPEC-2021