Pontificia Universidad Católica del Ecuador

Facultad De Ingeniería

Escuela de Sistemas

TEMA:

ANALISIS DEL ESTADO DE RED EMPRESARIAL A TRAVÉS DE HERRAMIENTAS OPEN SOCURCE. CASO DE ESTUDIO: ASISTECOOPER S.A

AUTOR:

MATEO RAUL SANDOVAL IBADANGO

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE INFORMACIÓN

QUITO, 2023 – 2024

DEDICATORIA

A mi madre

Quien siempre me ha brindado un apoyo incondicional, motivándome y guiándome por el camino correcto. A lo largo de mi vida académica, siempre ha estado a mi lado, dispuesta a ayudarme en todo momento y buscando soluciones a cualquier obstáculo. Me ha enseñado que no importa cuántas veces falle o cometa errores, ella siempre estará presente para mí, ella es mi todo en este mundo.

A mis hermanas.

Nicol y Carolina son mi gran motivación en la vida. A lo largo de su propia travesía, han demostrado una admirable fuerza y perseverancia frente a las adversidades. Han sido quienes me han cuidado, apoyado y enseñado a lo largo de mi camino. Gracias a su ejemplo, cada vez que estoy a punto de rendirme, encuentro fuerzas renovadas para seguir adelante, las quiero hermanas.

A mis abuelos.

Me inculcaron el valor del esfuerzo y me enseñaron qué hacer para alcanzar el éxito. Siempre me recordaron que las cosas no son fáciles y sus sabios consejos han sido de gran ayuda en mi vida y mis estudios. Les agradezco de corazón por su constante apoyo. Los quiero mucho.

AGRADECIMIENTO

Quiero agradecer a Daniela Morejón quien ha sido un pilar fundamental en toda mi vida y siempre me ha apoyado en los buenos y malos momentos, dándome fuerza he inspiración nunca olvidare el día que te conocí y agradezco a dios por a verte puesto en mi vida.

A mi mejor amigo y hermano Carlos Oscullo quien siempre estuvo presente en los peores momentos de mi vida y supo cómo hacerme reír y aconsejarme. Agradecer también a Mario, Josué y Zabdiel quienes me ayudaron con sus conocimientos y tuvieron la paciencia para enseñarme, a Ronald y Jorge. que hicieron de la universidad un lugar agradable y divertido en los tiempos libres, a Viviana, Majo, Milena, Vale, Pame, Luciana, Katherine, Lu, Karo, Gabriela, Dayanna y Yvonne que siempre haya una forma de alegrarme el día.

RESUMEN

Este proyecto presenta un análisis profundo del estado actual de la red de internet de AsisteCooper. Se llevará a cabo un análisis exhaustivo utilizando herramientas de código abierto para evaluar el rendimiento de los puntos de acceso e identificar posibles problemas de conectividad o interferencias que puedan estar afectando negativamente la red. Además, se utiliza una herramienta de análisis de vulnerabilidades.

Es esencial que las empresas realicen análisis periódicos de su red para evitar fallos de conexión y proteger la información confidencial. Mediante un análisis detallado del estado de la red, es posible identificar puntos débiles y áreas que requieren mejoras, lo que permite tomar medidas preventivas y correctivas para garantizar un rendimiento óptimo y una seguridad sólida.

INDICE

INDICE DE GRAFICOS Y FIGURAS

Capítulo I: Introducción

6.1. Marco Referencial

6.1.1. Justificación

El avance de las redes inalámbricas va progresando cada año, logrando mejorar diferentes aspectos con el pasar del tiempo, como la velocidad del ancho de banda, los canales de frecuencia y su seguridad, sin embargo, al mismo tiempo se va desarrollando tecnología que tiene como finalidad penetrar la red de internet o los equipos para realizar robo de información o perjudicar el Hardware de la empresa a su vez la configuración e instalación de los equipos está hecha por personas lo cual presenta el factor o "error" humano con respecto a la eficiencia de la red.

La mayoría de las empresas privadas del mercado manejan herramientas de pago, que les ayudan hacer un análisis de la red, las aplicaciones de pago no siempre son las mejores, debido a que algunas solo funcionan con determinados equipos sin opción a escalabilidad y casi siempre tienen las mismas funciones que una herramienta open source, la mayoría de las empresas las usan debido a que el estatus de la marca garantiza seguridad.

El análisis de la red tiene como objetivo recolectar datos sobre el estado de la WLAN de internet de la empresa AsisteCooper haciendo diferentes pruebas en la seguridad, equipos y eficiencia de la misma red de internet. Esto permitirá encontrar fallos en la red, detectar los diferentes problemas y vulnerabilidades de los equipos y determinar si la red está funcionando con eficiencia.

6.1.2. Planteamiento del Problema

Realizar un análisis de la Red es una práctica fundamental que todas la empresas públicas o privadas deben realizar con la finalidad de mitigar fallos también en el caso de que se presente uno poder resolverlo de manera inmediata garantizando así la eficiencia y estabilidad de la red, la mayoría de las empresas invierte grandes cantidades de dinero para mantener una red libre de cualquier evento de fallo.

Analizar el estado de la red de internet es un proceso el cual tiene que ser realizado por personal especializado y con las herramientas indicadas que ayuden al especialista encontrado fallos, en el proceso de análisis, se debe presentar un informe el cual detalle las vulnerabilidades y en el caso de ser encontradas que se podría llegar a corregir, para que le empresa mejore su servicio de red.

El análisis del estado de red se realiza con diferentes tipos de herramientas, para el escaneo se ha considerado usar Vistumbler es una herramienta gratuitita que permite ver información detalladas de la red y los equipos mientras que para el proceso de análisis de vulnerabilidades se ha considerado tomar el sistema Operativo Kali Linux-Greenbone debido a que es una herramienta gratuita que permite el análisis de vulnerabilidades y presenta las posibles soluciones para las mismas vulnerabilidades.

6.1.3. Objetivo General

Analizar el estado de la red empresarial utilizando herramientas Open Source

6.1.4. Objetivos Específicos

1. Analizar si existen fallos de la señal inalámbrica dentro de la red LAN de la empresa Asitecooper
2. Realizar un análisis de la infraestructura de los Wireless access points utilizando la herramienta Vistumbler
3. Realizar análisis de vulnerabilidades a la red utilizando el software Kali Linux y Greenbone

6.1.5. Antecedentes

Desde que la tecnología inalámbrica fue creada, esta se ha usado de una manera correcta por todo el mundo la mayoría de las veces brindando diferentes ventajas a las personas y ayudando a conectar lugares en los cuales una red por cable no podue llegar, el acceso a la información ahora está a la disponibilidad de todas las personas y solo se necesitan dos cosas un dispositivo inteligente y conexión a internet. Pero en los pocos casos, en los cuales no se ha usado de manera correcta, las personas buscan debilidades o vulnerabilidades las cuales quieren o buscan para usarlas a su favor.

La mayoría de las empresas en la actualidad utiliza diferentes herramientas para garantizar su seguridad y proteger sus datos esto también tiene más beneficios, en consecuencia, de mejorar la seguridad, también se logra mejorar la eficiencia de la red.

El trabajo de (MM Espinoza Alarcón, MI Tejena Vergara, 2019) presenta claramente, acerca de la importancia que tiene el realizar un análisis de red exhaustivo con el fin de encontrar diferentes fallas en la red y como consecuencia presenta un plan de mejora para la eficiencia de la red como el uso de VLAN, limitación del ancho de banda y filtrado de contenido web.

En el caso de seguridad uno de los más comunes es el escaneo de puertos en los equipos de hardware que estén conectados a la red, de acuerdo con el proyecto presentado por (LJ Rios Aliaga,2021) dice que el escaneo de puertos es una de las técnicas más usadas para encontrar vulnerabilidades, desarrollando así un sistema el cual evita estos escaneos al tener algoritmos que encuentran comportamientos anormales en la red agregando también teoría de lo peligroso que puede llegar a ser para una empresa no tener la seguridad adecuada en sus puertos.

6.1.6. Alcance

Este trabajo tiene como alcance, la entrega de un documento donde se presentan los datos recolectados del análisis de una red WLAN para la empresa AsisteCooper, este análisis de red se llevará a cabo en las instalaciones de la empresa durante un periodo de tiempo de un mes.

Como resultado las herramientas que se utilizan presentarán las falencias que existen dentro de la red de internet y puntos de acceso de la empresa, en el caso de haberlas, todo este proceso se realizara para poder tener una mejor visión acerca de la red de internet y estado.

Este análisis se lleva a cabo debido a que la empresa de desarrollo necesita eficiencia en su ancho de banda ya que es su principal herramienta, con base en el análisis, dependiendo del error que la herramienta entregue, se proporcionará una recomendación para corregir dicha falencia con respecto al ancho de banda. Garantizar la seguridad de su red detentando errores que serán presentados en el trabajo de titulación para que la empresa pueda tomar las medidas correspondientes debido a que manejan información de otras instituciones por lo cual se debe realizar análisis de vulnerabilidades además de un análisis de eficiencia.

Capítulo II: Fundamentación Teórica

7.1. Marco Teórico

7.1.1. Redes Inalámbricas

"Las redes inalámbricas son redes que utilizan ondas de radio para conectar los dispositivos, sin la necesidad de utilizar cables de ningún tipo" (Salzar, 2017, pág. 6). Al ser ondas de radio, poseen diferentes tipos de frecuencia, distinto rango de cobertura y diferentes tipos de velocidades, en la actualidad casi todos los dispositivos usan redes inalámbricas. la infraestructura WLAN es la más usada para la mayoría de las casas y empresas PYMES. Para realizar la conexión se necesita cierta parte de infraestructura física la cual llegara por medio de cable a un Access Point que brinda señal inalámbrica al resto de ubicaciones. Existen diferentes componentes de Hardware que puede ayudar a mejorar la señal como los repetidores o swichts.

La mayoría de las empresas opta por las redes inalámbricas debido a que su coste de instalación es menor en comparación de las redes tradicionales, a la flexibilidad que da a los trabajadores pudiendo realizar sus labores desde cualquier parte dentro del área, dado el caso de que la expansión a futuro este presente hacer crecer una red WLAN no es complicado y actualmente las redes inalámbricas se acercan mucho en cuanto ancho de banda y velocidad que ofrece una red de cableado (Salzar, 2017).

Aunque las redes inalámbricas ofrecen varios beneficios, también tienen algunos problemas los cuales radican en que utilizan ondas de radio, por esto mismo se presenta regulaciones legales en las ondas de radio o en el espectro electromagnético, para evitar problemas de interferencia “Todos los países necesitan regulaciones que definan los rangos de

frecuencia y potencia de transmisión permitidos para cada tecnología" (Salzar, 2017, pág. 6). Otro problema que presentan las redes inalámbricas es que sus ondas no se pueden delimitar, por lo tanto, siempre están propensas a ser atacadas y los ataques pueden llevarse sin problemas si los paquetes de datos no están codificados por lo cual se debe tomar medidas para evitar estos problemas como la codificación o utilización de Firewalls.

7.1.2. Tipos de redes Inalámbricas

Las redes inalámbricas tienen cuatro clasificaciones, para ser clasificadas se toma en cuenta dos cosas el área de la aplicación y el alcance que posee.

WPAN (Wireless Personal-Area Networks) permite comunicación de corto alance con una distancia aproximada de 10 metros. Implica casi nula infraestructura, es siempre implementada en pequeños dispositivos, para la compartición de pequeñas cantidades de datos un ejemplo es Bluetoo.

WLAN (Wireless Local-Area Networks) la comunicación de estas redes aumenta hasta una distancia aproximada de 100 metros casi siempre son usadas para empresas, escuelas o hogares, la WLAN se basa en el estándar 802.11 de la IEEE y su nombre comercial es WIFI.

WMAN (Wireless Metropolitan-Area Networks) son parecidas a las WLAN con la diferencia que su rango de distancia es equiparable al tamaño de una ciudad, se basan en el estándar IEEE 802.16 su comunicación es de punto o multipunto esto permite que las redes WLAN se conecten a WIMAX (Worldwide Interoperability for Microwave Access) que es la tecnología que permite la comunicación punto o multipunto.

WWAN (Wireless Wide-Area Networks) tienen un rango mayor a 50 kilómetros, utilizan frecuencias con licencia estas mantienen conexión para ciudades o países, debido a que se

utilizan sistemas satelitales o antenas, existen solo dos tecnologías disponibles red de telefonía móvil y los satélites. (Salzar, 2017).

7.1.3. Problemas en las Redes Inalámbricas

Las redes inalámbricas ofrecen grandes beneficios sin embargo estas también presentan problemas o inconvenientes. El más claro e importante viene a ser que no se puede limitar con exactitud el área de cobertura debido a esto siempre será un blanco de ataques por eso existe un mayor riesgo de que los datos sean robados si no se usa algún tipo de cifrado.

La señal inalámbrica puede encontrar obstáculos físicos, como paredes u objetos metálicos, lo que provoca interferencias en la señal y reduce la calidad y velocidad de la conexión inalámbrica. La señal puede ser reflejada, dispersada o absorbida al encontrarse con estos obstáculos. Otro factor que puede causar interferencias es la operación de múltiples redes inalámbricas en la misma área con frecuencias similares. Esto también puede provocar interferencias en la señal y disminuir la calidad de la conexión inalámbrica (Salzar, 2017)

La velocidad aun que hoy es equiparable a la de una red con cableado, la transmisión de datos siempre va a ser mejor con cable si la red inalámbrica no posee estándares o protocolos que ayuden en la optimización del funcionamiento como lo son una buena selección del ancho de banda, buena ubicación y posición del enrutador, actualización del firmware, por esto es recomendable hacer análisis de su estado por la pérdida de ancho de banda que puede llegar a ocurrir por una mala configuración

El costo en cuanto a implementación de una red inalámbrica grande como lo son WMAN Y WWAN puede ser más costoso que una red cableada esto debido a la infraestructura necesaria

para cubrirá grandes áreas ya que se requiere múltiples antenas y satélites, lo que aumenta el coste del hardware. Además, la seguridad de las redes inalámbricas debe ser tomada en cuenta en la implementación de redes a gran escala. La seguridad en redes inalámbricas es especialmente crítica debido a la facilidad con la que los intrusos pueden acceder a ellas desde el área de cobertura. (Sanchez, 2012).

7.1.4. Seguridad de WLAN

La evolución de los protocolos de seguridad ha ido aumentando la seguridad en las redes WLAN. Sin embargo, todos los protocolos de seguridad se basan en tres principios conocidos como la triada CIA, que incluyen la integridad, la confidencialidad y la disponibilidad. Los protocolos de seguridad son implementados de manera obligatoria en todas las redes, sin embargo, la seguridad inalámbrica es más difícil de implementar. El estándar IEEE 802.11 definió dos mecanismos se seguridad los cuales son identificación y encriptación. (García A. , 2018)

Con estos mecanismos nacieron los protocolos de seguridad los cuales ayuda a que hackers intente romper la confidencialidad el cual es el punto más débil de las redes inalámbricas si uno de los tres principios de la triada CIA es corrompido se considera ataque de vulnerabilidad. Una vulnerabilidad se refiere a una debilidad fallo en un sistema, aplicación, infraestructura o cualquier otro componente que pueda ser explotado por un atacante para comprometer la seguridad y permitir acciones no autorizadas. Las vulnerabilidades pueden existir debido a errores de programación, configuraciones incorrectas, deficiencias en el diseño o incluso debido a factores externos.

Protocolo WEB se aprobó en 1999 y fue el primer protocolo de seguridad implementado por la IEEE 802.11 es un protocolo de encriptación y se creó con el fin de tener control sobre el acceso, privacidad, autentificación e integridad. Utilizaba una clave secreta de 40 a 104 bits

Protocolo WPA/WPA2, WPA dio solución a todos los problemas de vulnerabilidades del protocolo WEB, es muy seguro debido a su principal característica que es la distribución dinámica de claves, esta fue diseñada como un remplazo temporal de WEB mientras se terminaba el desarrollo del estándar 802.11i (WP2), el cual aumenta las métricas de seguridad su principal diferencia aumenta las claves de cifrado aún más que su antecesor WPA, utilizando el algoritmo MIC. (Andreu, Pellejero, & Lesta, 2006).

7.1.5. Ancho de Banda

En la investigación de (González & Zebadúa, 2011) se realizó un análisis de tráfico de red y control de ancho de banda de la UPCH. Según los autores, el ancho de banda se refiere a la cantidad de información que se envía a través de una conexión de red y se mide en bits por segundo (bps), kilobits por segundo (Kbps) o megabits por segundo (Mbps).

En términos generales, el ancho de banda en una conexión de red inalámbrica es una medida de la cantidad de datos que pueden ser transmitidos y recibidos en un período de tiempo determinado. Cuanto mayor sea el ancho de banda, mayor será la cantidad de datos que se pueden enviar y recibir, lo que se traduce en una conexión de red más rápida y eficiente. Sin embargo, las redes inalámbricas pueden experimentar una serie de problemas relacionados con el ancho de banda, como:

Interferencia de señal: esto puede ocurrir cuando hay múltiples redes inalámbricas en la misma área o cuando dispositivos electrónicos cercanos emiten señales de radio que pueden interferir con la señal de la red inalámbrica.

Distancia: la distancia entre un dispositivo y un punto de acceso inalámbrico puede afectar la velocidad de la conexión, ya que la señal se debilita a medida que se aleja del punto de acceso.

Sobrecarga de dispositivos: cuando hay muchos dispositivos conectados a la misma red inalámbrica, puede haber una sobrecarga en el ancho de banda, lo que puede ralentizar la velocidad de la conexión.

En cuanto a las frecuencias que normalmente se utilizan en las redes inalámbricas, las dos frecuencias principales son 2.4 GHz y 5 GHz. La frecuencia de 2.4 GHz se utiliza comúnmente debido a su capacidad para proporcionar una cobertura más amplia, pero también es más susceptible a la interferencia. La frecuencia de 5 GHz es menos propensa a la interferencia, pero su cobertura es más limitada (Salzar, 2017).

7.1.6. Sistema Operativo

El sistema operativo es considerado el programa principal que administra de manera eficiente los recursos de una computadora o dispositivo móvil, permitiendo que el usuario final haga uso adecuado de los mismos. El sistema operativo actúa como intermediario entre el

hardware y los programas o aplicaciones que se ejecutan en el equipo, garantizando el uso eficiente de los recursos disponibles. (García, Medina, & Muñoz, 2022).

El sistema operativo es el software básico que se instala en una computadora al momento de su fabricación o adquisición, y es esencial para que los programas y aplicaciones puedan funcionar correctamente en el equipo. Además de controlar los recursos del hardware, el sistema operativo también proporciona una interfaz gráfica de usuario (GUI) que permite a los usuarios interactuar con la computadora a través de ventanas, iconos y menús.

Existen varios tipos de sistemas operativos, incluyendo los sistemas operativos de escritorio, como Windows, macOS y Linux, y los sistemas operativos móviles, como Android e iOS. También hay sistemas operativos de servidor, que se utilizan para administrar y controlar servidores de redes y sistemas empresariales. El sistema operativo es fundamental para el funcionamiento de cualquier dispositivo informático, desde computadoras de escritorio hasta smartphones y servidores empresariales.

7.1.7. Open Source

Open source se refiere a software cuyo código fuente es de acceso público y está disponible para su uso, modificación y distribución por cualquier persona. El término "open source" significa que el código fuente de un programa es de libre acceso y puede ser modificado y mejorado por cualquier persona o comunidad de desarrolladores, de forma colaborativa y sin restricciones (Páez, 2019)

El software open source suele estar protegido por licencias que permiten su uso y distribución, a menudo sin coste alguno. Estas licencias también permiten la creación y distribución de versiones derivadas del software original, siempre y cuando se mantengan las mismas condiciones de la licencia.

El movimiento open source se originó en el ámbito del software libre, con el objetivo de fomentar el intercambio y la colaboración entre desarrolladores, así como de promover la innovación y el desarrollo de software de alta calidad a través de la colaboración abierta y transparente. El uso de software open source ha aumentado en popularidad en los últimos años debido a su capacidad para permitir que los desarrolladores construyan aplicaciones más rápidamente, reduzcan los costos y mejoren la calidad del software a través de la colaboración y la retroalimentación de la comunidad de desarrolladores. Algunos ejemplos de software open source populares incluyen el sistema operativo Linux, el gestor de contenidos WordPress, el navegador web Firefox, el paquete de ofimática OpenOffice y el servidor web Apache.

7.1.8. Vistumbler

Vistumbler es una herramienta de software que se utiliza para escanear y visualizar redes inalámbricas. Proporciona información detallada sobre las redes Wi-Fi disponibles en el área, como su nombre (SSID), intensidad de la señal (RSSI), canal, seguridad y otras características.

Al ejecutar Vistumbler en un dispositivo con capacidad de Wi-Fi, como una computadora portátil, permite detectar y mapear las redes inalámbricas cercanas. La información recopilada se muestra en una interfaz gráfica fácil de entender, lo que permite a los usuarios identificar y analizar redes inalámbricas cercanas, así como realizar un seguimiento de su intensidad de señal en diferentes ubicaciones.

7.1.9. Greenbone

Greenbone es una suite de software de seguridad y análisis de vulnerabilidades. Se basa en la plataforma OpenVAS (Open Vulnerability Assessment System) y es utilizado para realizar escaneos de seguridad y evaluaciones de vulnerabilidades en redes y sistemas.

Greenbone Security Assistant (GSA) es la interfaz web proporcionada por Greenbone para administrar y configurar escaneos de vulnerabilidades. Permite configurar objetivos de escaneo, programar escaneos automáticos, analizar resultados de escaneos y generar informes detallados sobre las vulnerabilidades encontradas.

Al utilizar Greenbone en Kali Linux, los profesionales de seguridad y los especialistas en pruebas de penetración pueden aprovechar las capacidades de escaneo y análisis de vulnerabilidades de Greenbone para identificar y solucionar posibles problemas de seguridad en redes y sistemas

7.1.10. Estándar IEEE 802.11

El estándar IEEE 802.11, también conocido como Wi-Fi, es un conjunto de estándares desarrollados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para redes de área local inalámbricas WLAN. El estándar IEEE 802.11 establece las especificaciones para la comunicación inalámbrica entre dispositivos, permitiendo la conexión y transmisión de datos a través de ondas de radio.

El estándar IEEE 802.11 define varios aspectos de las redes inalámbricas, como la frecuencia de operación, los métodos de acceso al medio, la seguridad y el rendimiento. Algunas de las versiones más comunes del estándar IEEE 802.11 incluyen:

- IEEE 802.11b: Introducido en 1999, opera en la banda de frecuencia de 2.4 GHz y proporciona velocidades de hasta 11 Mbps.
- IEEE 802.11a: Introducido también en 1999, opera en la banda de frecuencia de 5 GHz y proporciona velocidades de hasta 54 Mbps.
- IEEE 802.11g: Introducido en 2003, opera en la banda de frecuencia de 2.4 GHz y proporciona velocidades de hasta 54 Mbps.
- IEEE 802.11n: Introducido en 2009, opera tanto en la banda de frecuencia de 2.4 GHz como en la de 5 GHz, y proporciona velocidades de hasta varios cientos de Mbps.
- IEEE 802.11ac: Introducido en 2013, opera en la banda de frecuencia de 5 GHz y proporciona velocidades de varios cientos de Mbps a varios gigabits por segundo.

- IEEE 802.11ax (también conocido como Wi-Fi 6): Introducido en 2019, opera en ambas bandas de frecuencia y ofrece mejoras en la eficiencia y el rendimiento en comparación con las versiones anteriores. (IEEE, 2016)

A continuación, se muestran el estándar comun de señal Wi-Fi y sus rangos correspondientes en dBm:

- Excelente señal: -30 dBm a -50 dBm. Esta es la mejor señal posible, con una excelente calidad de conexión y rendimiento.
- Buena señal: -51 dBm a -67 dBm. Aunque no es tan fuerte como una señal excelente, sigue siendo una señal fuerte y proporciona una buena calidad de conexión y rendimiento.
- Señal aceptable: -68 dBm a -70 dBm. La señal se considera aceptable y es suficiente para una conexión estable, pero puede experimentar algunas fluctuaciones o pérdidas ocasionales.
- Señal débil: -71 dBm a -85 dBm. La señal es débil y puede haber una degradación significativa en el rendimiento y la calidad de la conexión. Es posible que se experimenten desconexiones intermitentes o una velocidad reducida.
- Señal muy débil: -86 dBm y más bajo. La señal es muy débil y es probable que la conexión sea inestable o inutilizable en este nivel. (IEEE, 2016).

Capítulo III: Metodología

8.1. Metodología de Desarrollo

La metodología para aplicar en el proyecto de trabajo de titulación estará enfocada en el análisis de los 4 access points que la empresa posee dentro de sus instalaciones. Los cuatro access points constituyen toda la red de la empresa, no hay más equipos. No se maneja una red de datos cableada. Para ello, se utilizarán dos herramientas de código abierto: Vistumbler y Greenbonne-Kali Linux.

Vistumbler es una herramienta de análisis de red que proporciona información relevante sobre los access points, tales como dirección MAC, frecuencia y canal de comunicación utilizado. Esta herramienta permitirá obtener información detallada sobre cada access point y conocer su estado actual.

Por otro lado, Greenbonne-Kali Linux es una herramienta de análisis de vulnerabilidades que se puede emplear en access points, servidores y computadoras. Esta herramienta, solo necesita la dirección IP para llevar a cabo un análisis de las vulnerabilidades presentes en el access point. Además, proporciona comentarios sobre las medidas necesarias para eliminar las vulnerabilidades. No se usa el método de análisis de riesgos, la herramienta Greenbone ya entrega un análisis. El análisis de vulnerabilidades realizado por Greenbone implica la búsqueda y evaluación de posibles debilidades en la seguridad de una infraestructura de TI. Esto incluye la identificación de vulnerabilidades conocidas, como brechas de seguridad en sistemas operativos, aplicaciones y servicios, así como la detección de configuraciones inseguras.

La metodología se basará en la utilización de Vistumbler y Greenbonne-Kali Linux para analizar cuatro access points de la empresa con estas herramientas, se podrá obtener información detallada sobre cada access point y conocer su estado actual, así como identificar las

vulnerabilidades presentes y tomar las medidas necesarias para eliminarlas. La metodología permitirá mejorar la seguridad de los access points y, por ende, de toda la red de la empresa.

8.1.1. Investigación Cualitativa

Para llevar a cabo una investigación cualitativa, es necesario seleccionar un problema de investigación, identificar la muestra, el tipo de información a levantar y el método de análisis de los datos con los que se pretende trabajar. (Conejero, 2020)

El tipo de investigación a realizar se clasifica como analítico cualitativo, con el propósito de obtener una comprensión profunda de los puntos de acceso y su seguridad mediante la búsqueda de patrones en la información proporcionada por las herramientas. Para ello, se llevará a cabo un análisis, de los datos recopilados con el fin de establecer medidas de seguridad para mejorar la red inalámbrica de internet.

8.1.2. Investigación Aplicativa

La investigación aplicada busca obtener nuevos conocimientos que permitan la solución de problemas prácticos en diferentes ámbitos, como la industria, la medicina, la tecnología, la educación, entre otros. (Álvarez, 2020)

El estado de la red inalámbrica de internet será determinado por los datos recolectados durante el análisis realizado con la herramienta Vistumbler. Para llevar a cabo el análisis de los acces points, se llevará a cabo un monitoreo diario durante un periodo de 2 horas, con un intervalo horario específico de 1:00 PM hasta 3:00 PM. El horario de análisis corresponde a un intervalo de trabajo típico para los empleados, lo que permitirá analizar el impacto de las operaciones normales en la red. La empresa cuenta con un número bajo de trabajadores, lo cual

evita que la red alcance niveles de alto tráfico. Además, el análisis de seguridad se realizará a cada uno de los acces points al final del análisis de red, con el objetivo de identificar todas las vulnerabilidades presentes en la red.

Se debe destacar que la herramienta solo necesita ser ejecutada una vez y que el tiempo estimado para analizar cada punto de acceso es de alrededor de una hora. Todo el proceso se llevará a cabo de forma sistemática.

Capitulo IV: Desarrollo de la Investigación

9.1. Estado actual de la empresa AsisteCooper

La empresa AsisterCooper se encuentra ubicada en el segundo piso de un edificio, donde alquila sus oficinas. En cuanto al estado actual de la red de internet que maneja, cuenta con un plan de internet de 300mb/s , una infraestructura que consta de 4 puntos de acceso, uno para cada área de la empresa, y utiliza una topología de red en forma de estrella. La configuración e instalación de la red fueron realizadas por el equipo de informática. En cuanto a la seguridad y las políticas de acceso, todo se encuentra en estado automático.

9.2. Instalación de la Herramienta Vistumbler

Para iniciar el proceso de análisis de la red de internet, es necesario instalar la herramienta Vistumbler, puesto que esta sirve para el monitoreo de red. Vistumbler es una herramienta que brinda funciones que ayudan en el análisis de redes inalámbricas. Sus apartados muestran información detallada de las redes Wi-Fi.

Para la instalación de la herramienta Vistumbler se necesita ir a su página oficial donde se puede descargar.:

- Vistumbler:https://www.acrylicwifi.com/wifi-analyzer/

Se procede a descargar dando clic en EXE installer.

Figura 1

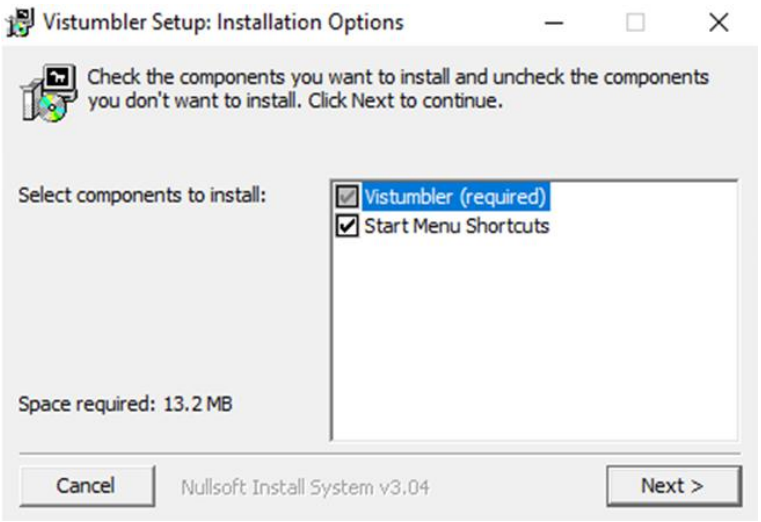
Página web de la herramienta Vistumbler.

Nota: Para que pueda acceder a la página oficial, debe desactivar el antivirus, ya que este detecta que la página es una amenaza. Extraído de página oficial de Vistumbler. Elaborado por: Sandoval, M. (2023).

Al terminar la descarga se debe abrir el archivo EXE, desplegando una pantalla para seleccionar los componentes a instalar.

Figura 2

Ventana de selección de componentes.

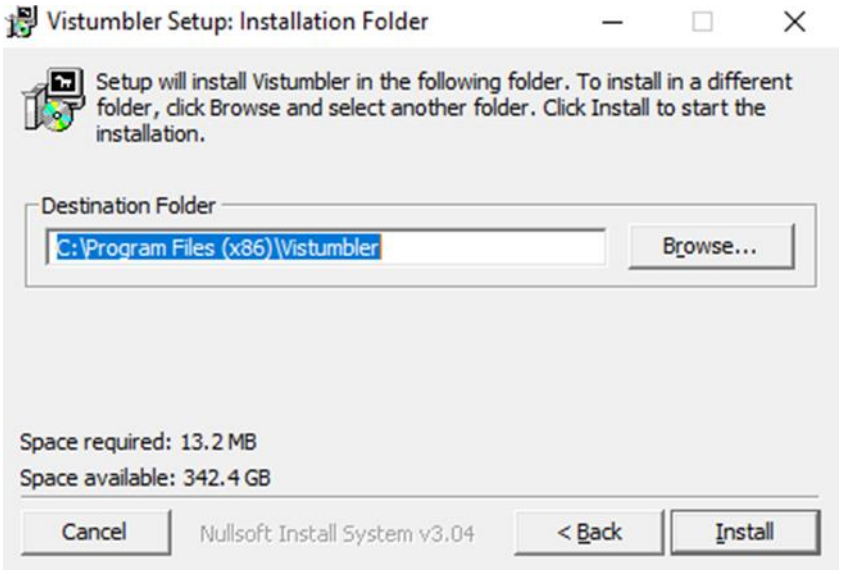


Nota: Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023)

Seleccionar la carpeta de destino, dentro del equipo, se visualiza el tamaño de descarga.

Figura 3

Ventana de selección de destino.

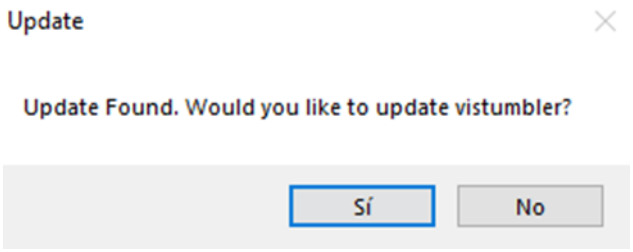


NOTA: Es recomendable escoger la ubicación predeterminada. Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

Se acepta que la descarga se realice y también se acepta que la aplicación inicie al finalizar la descarga.

Figura 4

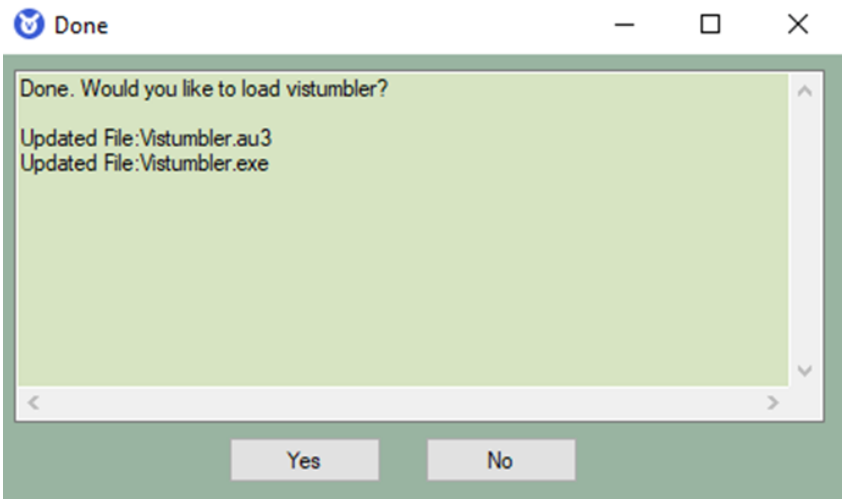
Confirmación de descarga.



Nota: Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

Figura 5

Confirmación de inicio de la herramienta.

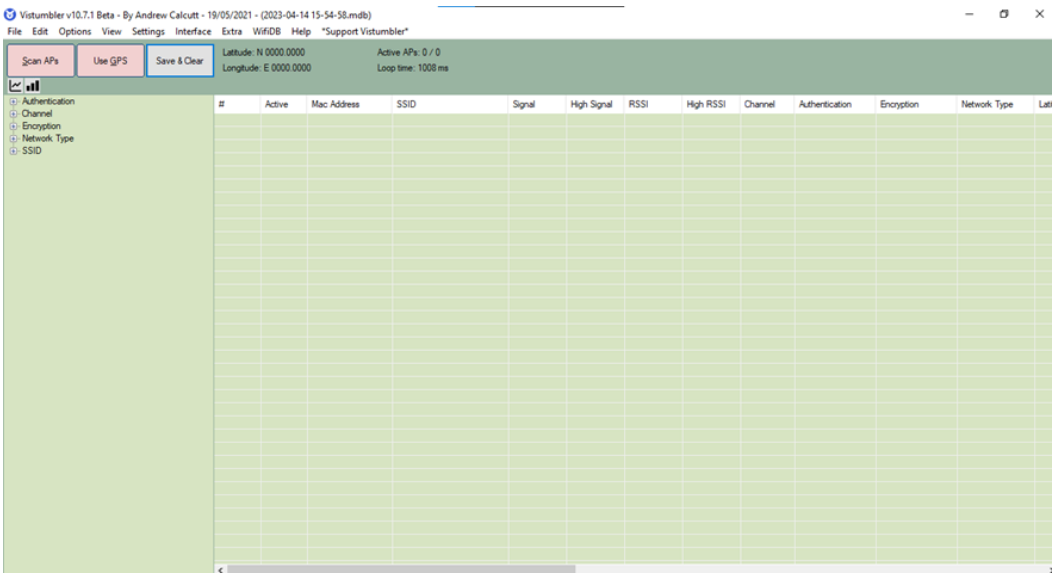


Nota: Se recomienda aceptar el inicio o carga rápida para que se compruebe que la aplicación no tiene errores. Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

La aplicación esta lista, para realizar un análisis.

Figura 6

Interfaz-Vistumbler para Análisis de Red



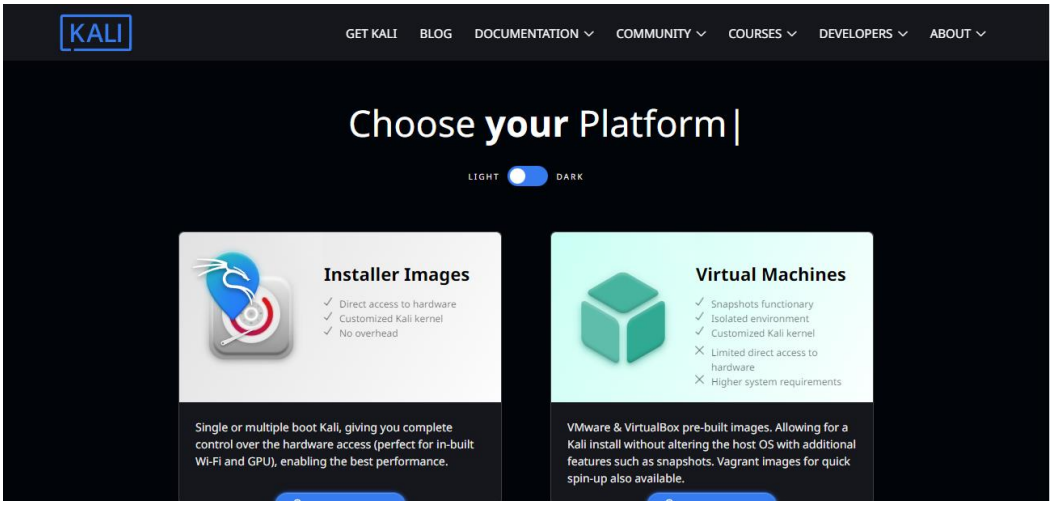
Nota: El panel principal de escaneo proporciona información crucial para el análisis. Extraído de la herramienta Vistumnler Elaborado por: Sandoval, M. (2023).

9.3. Creación de la máquina virtual Kali e Instalación de Greenbone

Para instalar Greenbone, es necesario crear una máquina virtual utilizando el sistema operativo Kali. Antes de proceder con la instalación y uso de Kali Linux, es importante descargarlo. Puedes obtener Kali Linux desde el sitio web oficial de Kali Linux en http://www.kali.org/downloads/. En la página de descarga, se puede elegir la imagen oficial de Kali Linux basada en diferentes criterios, como la arquitectura de la máquina y el tipo de imagen, permitiendo seleccionar la configuración adecuada para tus necesidades.

Figura 7

Página web de Kali

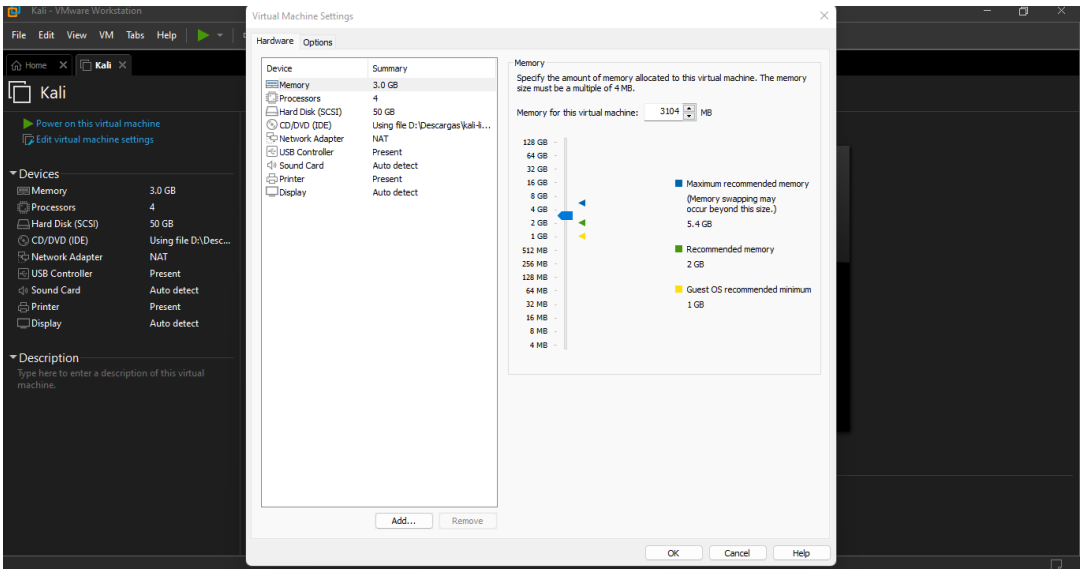


Nota: Se puede descargar la imagen y configurarla o descargar una imagen preconstruida con el sistema ya configurado. Extraído de la página web de Kali. Elaborado por: Sandoval, M. (2023).

Al terminar la descarga de la imagen o la imagen preconstruida, se configura el entorno en donde se instala el sistema Kali utilizando un hipervisor, el hipervisor es un software que se encarga de gestionar, supervisar la virtualización de recursos en un entorno de computación., también conocido como VMM (Virtual Machine Monitor) permitiendo el funcionamiento de múltiples sistemas operativos de forma aislada en un mismo servidor físico, como lo pueden ser VirtualBox o VMware.

Figura 8

Creación de Máquina virtual con sistema operativo Kali Linux



Nota: El panel de configuración de recursos para la máquina virtual permite al usuario ajustar y asignar de manera precisa los recursos necesarios, como la memoria, el almacenamiento y la capacidad de procesamiento, para garantizar un rendimiento óptimo del entorno virtualizado. Extraído de la herramienta VMware WorkStation. Elaborado por: Sandoval, M. (2023).

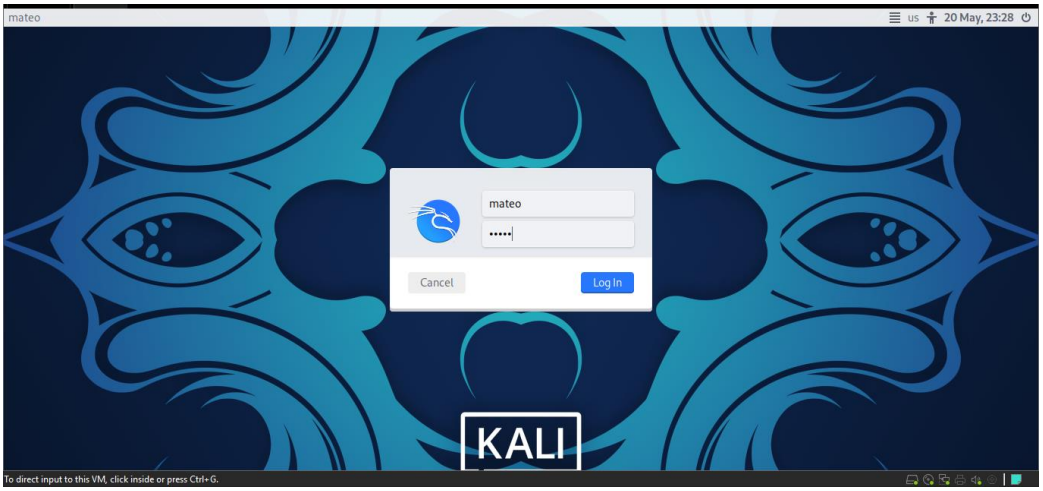
Se inicia la máquina virtual y se procede a configurar el sistema Kali como usuarios, teclado, leguaje, fecha y hora, una vez finalizada la configuración del sistema se inicia con el usuario y contraseña previamente configurado.

Usuario: Mateo

Contraseña: Mateo

Figura 9

Pantalla de inicio Máquina Virtual.



Elaborado por: Sandoval, M. (2023)

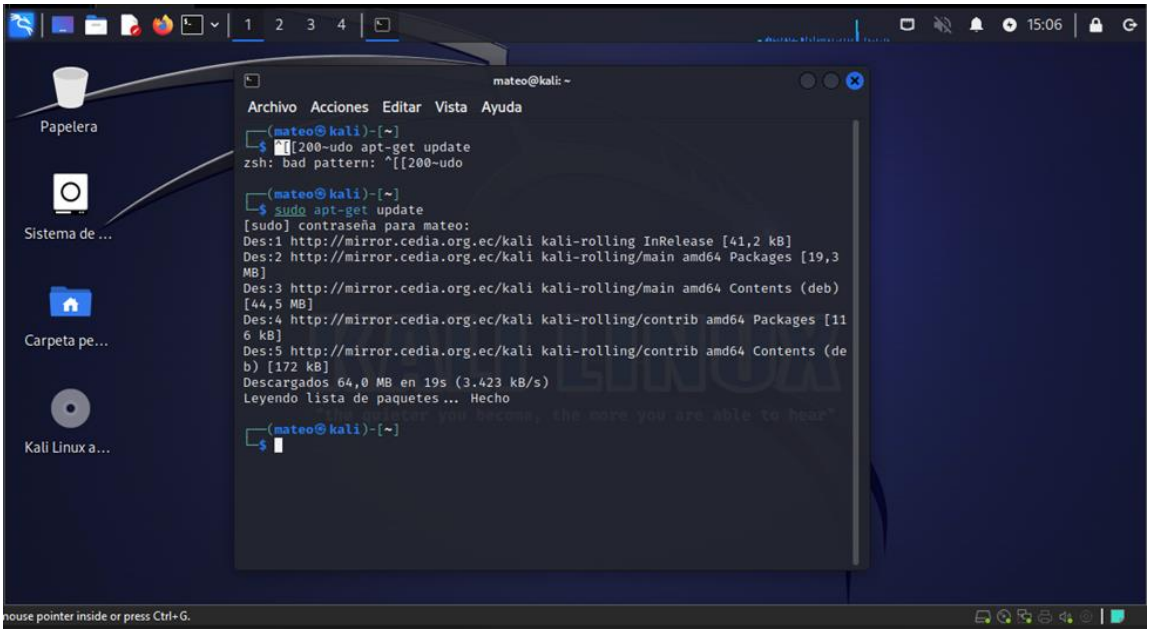
Con la máquina lista se procederá a instalar la herramienta Greenbone. Se debe abrir el panel de comandos de Kali Linux, se puede hacer la instalación con el Usuario Normal: Mateo o con el Super Usuario: Root.

Se debe asegurar que el sistema operativo Kali se encuentra actualizado, se abre la terminal y se ejecuta lo siguiente:

sudo apt-get update

Figura 10

Actualización del sistema operativo Kali.



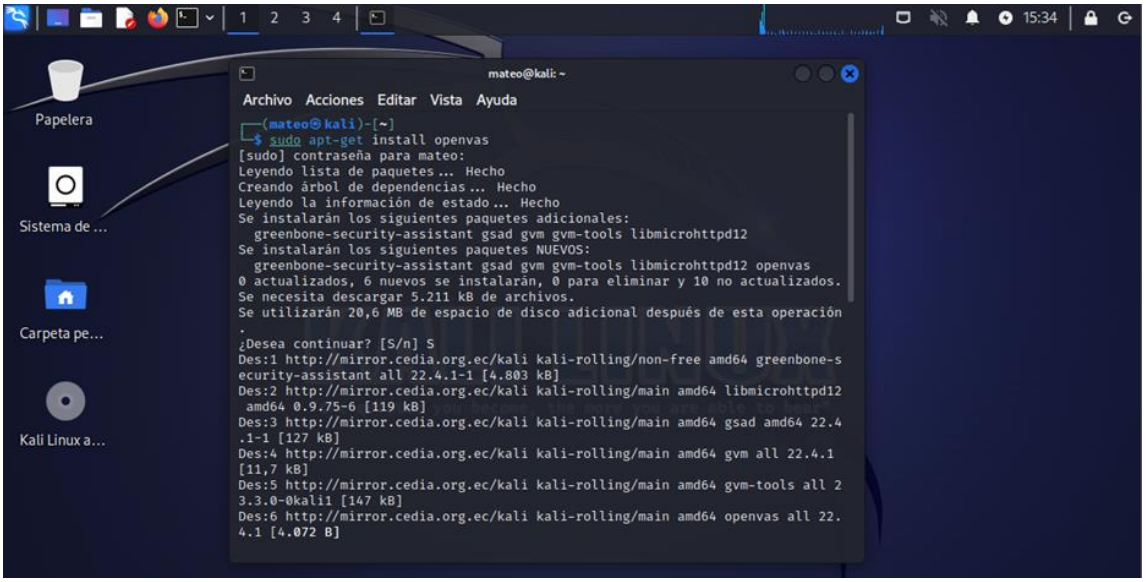
Nota: El comando update actualiza el sistema operativo. Elaborado por: Sandoval, M. (2023)

Una vez finalizada la actualización del dispositivo, se procede a la instalación de OpenVas, el cual es requerido para el funcionamiento de Greenbone, ya que forma parte del paquete de la misma herramienta, OpenVas es un escaner de vulnerabilidades se encarga de identificar posibles vulnerabilidades y brechas de seguridad en los sistemas. Para la instalación se ejecuta el siguiente comando:

Sudo apt-get install openvas

Figura 11

Instalación de complemento – Escáner OpenVas



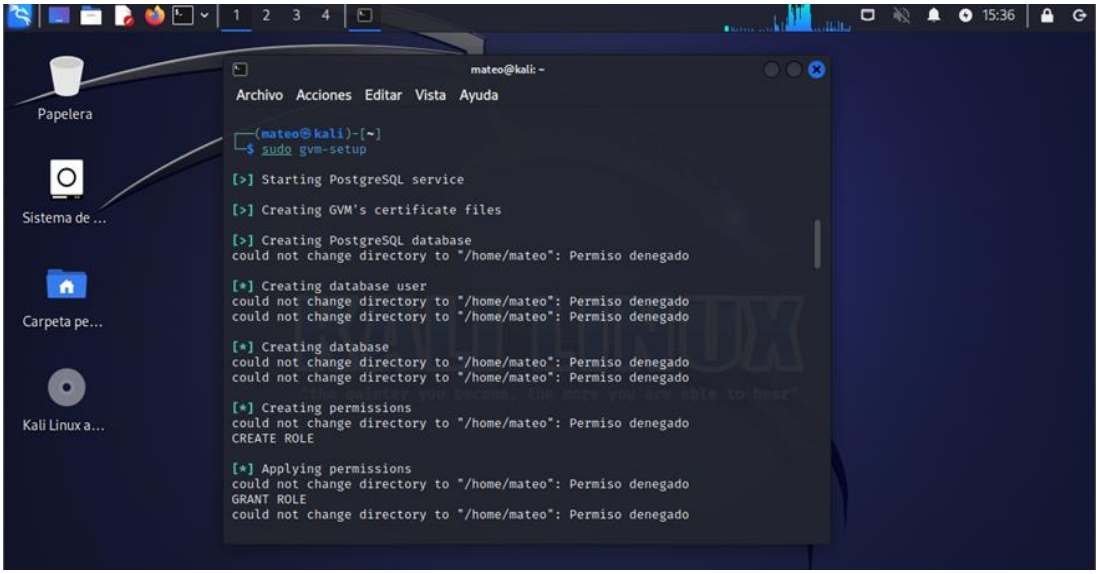
Nota: Esta instalación dura 20 minutos aproximadamente, si su instalación sobrepasa ese tiempo se recomienda cancelar la instalación e intentar de nuevo. Elaborado por: Sandoval, M. (2023)

Una vez finalizada la instalación de OpenVAS, se procede a instalar la otra parte necesaria para completar el paquete, que es GVM (Greenbone Vulnerability Manager). Greenbone es la unión de OpenVAS y GVM. GVM se instala utilizando el siguiente comando:

Sudo gvm-setup

Figura 12

Instalación de herramienta Greenbone

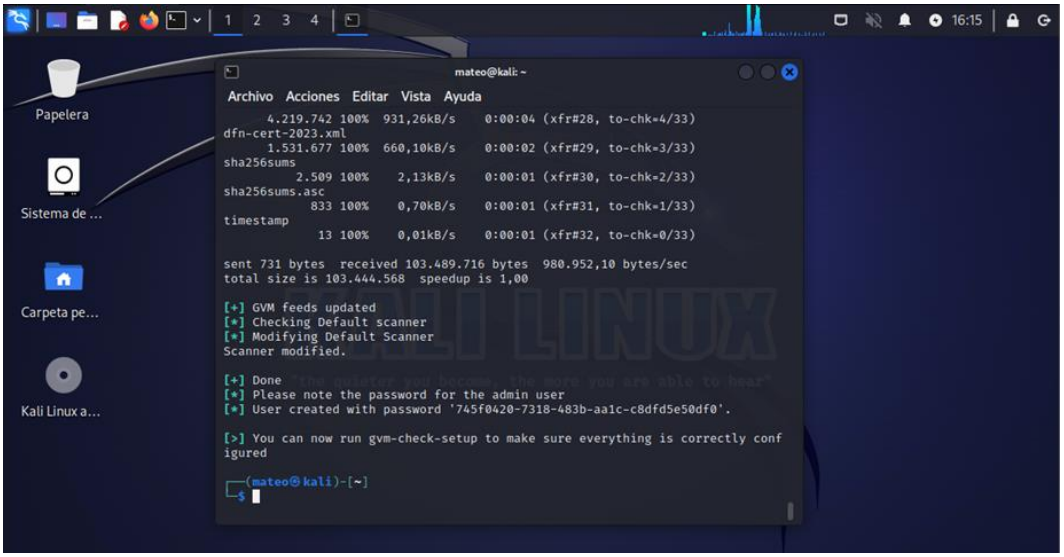


Nota: Esta instalación puede llegar a durar más de 2 horas. Elaborado por: Sandoval, M. (2023).

Una vez que se complete la instalación, se proporcionará al usuario un nombre de usuario y contraseña, los cuales serán utilizados para acceder a la herramienta mediante la interfaz web

Figura 13

Usuario y contraseña de Greenbone



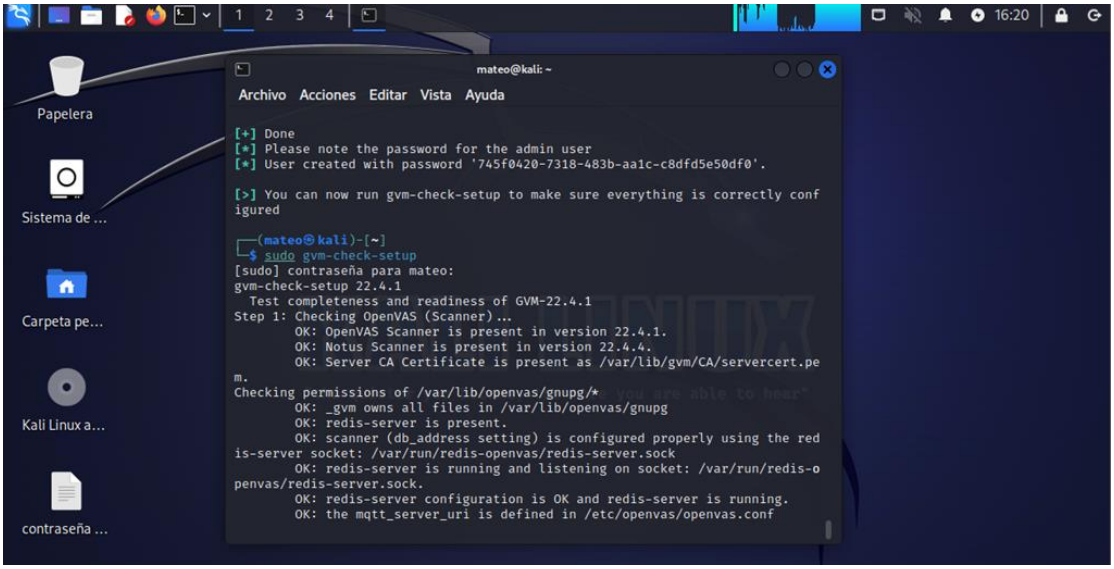
Nota: Se recomienda guardar la contraseña en un bloc de notas. Elaborado por: Sandoval, M. (2023).

Se verifica si la instalación fue exitosa con si siguiente comando:

Sudo gvm-check-setup

Figura 14

Chequeo de componentes para el funcionamiento de Greenbone.



Nota: Se recomienda realizar la instalación desde cero si algún componente falta. Elaborado por: Sandoval, M. (2023).

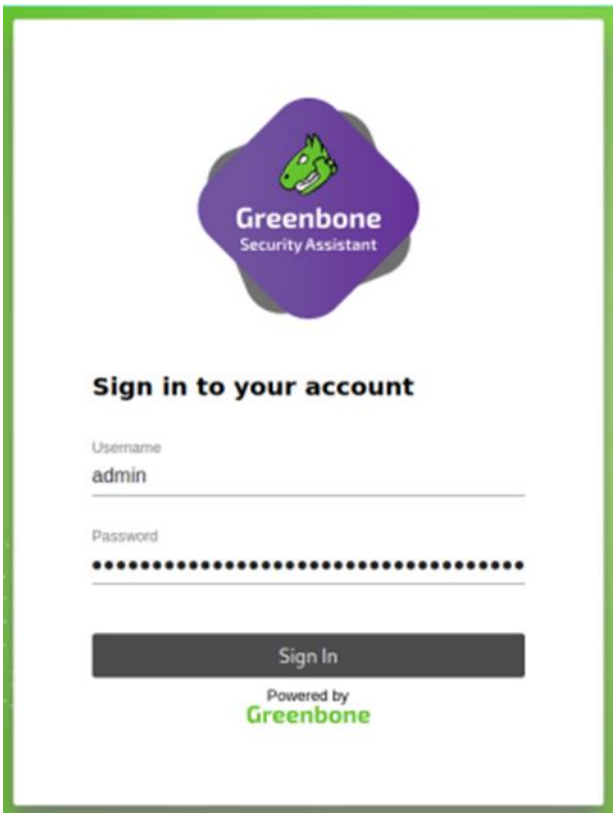
La aplicación inicia automáticamente, para acceder a la interfaz se debe escribir lo siguiente en el navegador:

https://127.0.0.1;9392

Se solicita el usuario y contraseña obtenidos durante la instalación para iniciar sesión

Figura 15

Ventana de inicio de sesión para Greenbone.

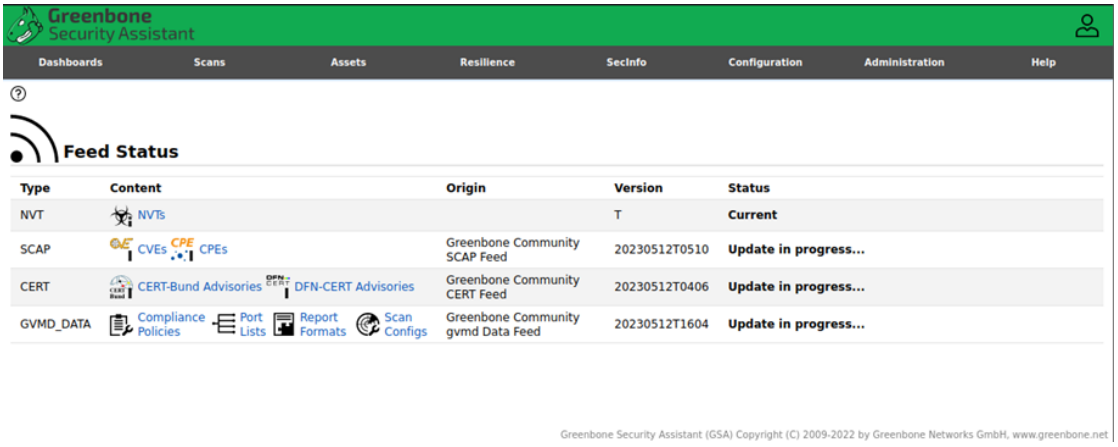


Nota: el usuario siempre es admin, esto se debe a que la herramienta carga una configuración predeterminada, se puede cambiar el usuario dentro de la herramienta. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Al iniciar la aplicación, todavía no se podrá realizar análisis debido a que deben actualizarse los feeds los cuales son bases de datos que tienen toda la información sobre las vulnerabilidades y que la herramienta utiliza para los análisis, esta descarga de feeds es automática.

Figura 16

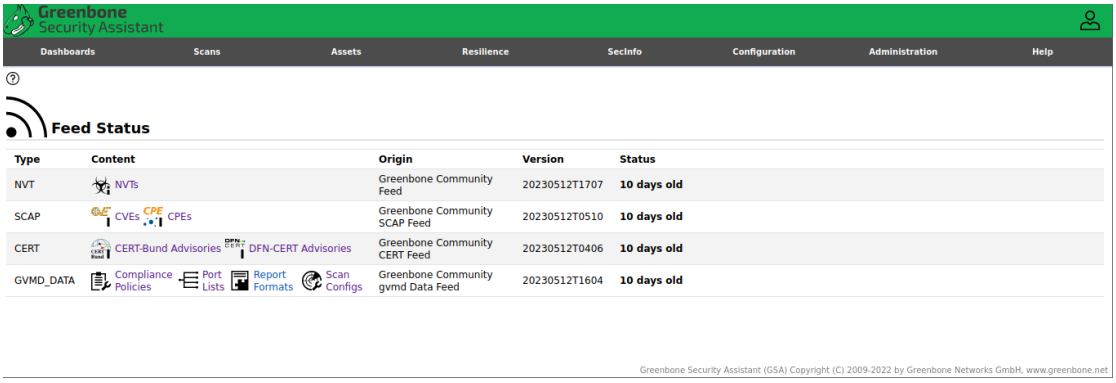
Feed Status – inicio de la descarga automática de los Feeds.



Nota: los Feed Status se encuentran en el apartado Administration. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 17

Feed Status – fin de la descarga.



Nota: Se recomienda revisar frecuentemente los feeds en busca de posibles actualizaciones. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Al finalizar la descarga ya se podrá realizar análisis.

9.4. Análisis de los Access Points con la Herramienta Vistumbler.

Para poder hacer un análisis de los AccessPoints se usará la herramienta Vistumbler la cual capturará los AccesPoints y muestra información relevante sobre los AccesPoints. Vistumbler captura los AccesPoints sin un orden en específico. La captura de los puntos de acceso se llevó a cabo en una ubicación central dentro de las oficinas.

Figura 18

Puntos de Acceso de la empresa AsisteCooper

#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption
1	Active	84:D3:43:9B:72:EC	AsisteCooper1	100%	100%	-47 dBm	-24 dBm	1	WPA2-Personal	CCMP
2	Active	B2:13:15:05:79:9A	AsisteCooper4	55%	55%	-70 dBm	-68 dBm	6	WPA2-Personal	CCMP
3	Active	2A:F5:A2:B7:6C:B9		15%	15%	-82 dBm	-82 dBm	6	WPA2-Personal	CCMP
4	Active	AC:84:C6:19:54:ED	PARRA CNT_EXT	15%	15%	-86 dBm	-86 dBm	1	WPA2-Personal	CCMP
5	Active	32:07:4D:47:E3:DF	AsisteCooper3	45%	45%	-78 dBm	-78 dBm	10	WPA2-Personal	CCMP
6	Active	04:8D:38:1B:29:4E	AsisteCooper2	100%	100%	-16 dBm	-16 dBm	10	WPA2-Personal	CCMP
7	Active	F8:AF:DB:FB:3D:9F	APUNTE_CNT	75%	85%	-76 dBm	-71 dBm	9	WPA2-Personal	CCMP
8	Active	AE:25:A2:67:E2:FA	DANIEL74	100%	100%	-60 dBm	-60 dBm	8	WPA2-Personal	CCMP
9	Active	AE:25:A2:67:E2:F6	DANIEL74	25%	25%	-79 dBm	-79 dBm	8	WPA2-Personal	CCMP
10	Active	AE:25:A2:67:F7:EE	DANIEL74	75%	75%	-70 dBm	-70 dBm	8	WPA2-Personal	CCMP
11	Active	AC:15:A2:67:F7:EE		65%	65%	-72 dBm	-72 dBm	8	WPA2-Personal	CCMP
12	Active	AC:15:A2:67:E2:FA		100%	100%	-59 dBm	-59 dBm	8	WPA2-Personal	CCMP
13	Active	AC:15:A2:67:E2:F6		25%	25%	-79 dBm	-79 dBm	8	WPA2-Personal	CCMP

Nota: Visumbler captura todos los AccessPoints posibles. Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

En el edificio donde se encuentran las oficinas de AsisteCooper, se han detectado 13 puntos de acceso (AccesPoints), sin hacer distinción entre las frecuencias de 2.4GHz y 5GHz. Sin embargo, utilizando el canal, es posible identificar la frecuencia utilizada por cada punto de acceso. Con esta herramienta, se pueden visualizar diferentes elementos, entre los cuales se destaca la dirección MAC del punto de acceso, el SSID. En este caso, los puntos de acceso

mantienen el mismo nombre para todos, pero se diferencian numéricamente del uno al cuatro para que los trabajadores puedan identificar el punto de acceso correspondiente a cada área. Además, se muestra el porcentaje de intensidad de la señal transmitida por cada punto de acceso. Por último, cabe destacar el apartado de "Manufacturer", el cual en algunos casos indica el fabricante del equipo.

Los puntos de acceso que se analizan a continuación son cuatro los cuales pertenecen cada uno a un área en particular, el AccePoint AsisteCooper1 pertenece al área de desarrollo, el AccesPoint AsisteCooper2 pertenece al área de desarrollo móvil, el AccesPoint AsisteCooper3 pertenece al área de Soporte y el AccesPoint AsisteCooper4 pertenece al área de Contabilidad.

Figura 19

Punto de Acceso AsisteCooper-Desarrollo

#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption
1	Active	84:D3:43:9B:72:EC	AsisteCooper1	100%	100%	-38 dBm	-23 dBm	1	WPA2-Personal	CCMP

Nota: El fabricante de este punto de acceso que, brinda la herramienta es Calix. Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

En ese punto de acceso, se puede observar que la señal alcanza el 100%, al igual que su nivel máximo. Esta situación puede interpretarse como una excelente señal para los dispositivos cercanos. Es importante tener en cuenta que la intensidad de la señal no se mantiene siempre al 100%, ya que esto depende de la distancia respecto al punto de acceso. Sin embargo, en general, se puede afirmar que el punto de acceso está funcionando adecuadamente y no se detectan problemas en el equipo.

Al analizar el RSSI, se observa que el punto de acceso presenta un valor de -38 dBm, con un máximo de -23 dBm. Esta situación indica una intensidad de excelente señal, según la IEEE, lo que se traduce en una buena velocidad de transferencia de datos y la ausencia de interrupciones o pérdidas de conexión en este punto de acceso.

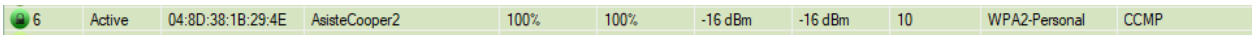
El punto de acceso opera en el canal uno, lo que indica que hay una señal eficiente de intensidad y poca interferencia en ese canal. La selección del canal de los puntos de acceso está configurada en automático, lo que permite adaptarse y elegir el canal óptimo según las condiciones del entorno. A través del número de canal, se puede confirmar que el punto de acceso trabaja en la frecuencia de 2.4GHz.

En cuanto a la autenticación, se utiliza el tipo WPA2-Personal, que se considera una de las formas más seguras de autenticación hasta la fecha de redacción de este documento. Además, se implementa la encriptación CCMP, la cual es un estándar reconocido y se encuentra entre las opciones de encriptación más seguras disponibles. Esta configuración garantiza un alto nivel de seguridad en este punto de acceso.

Un aspecto importante proporcionado por la herramienta es el estándar 802.11 que utiliza el punto de acceso. En el caso de este punto de acceso, se utiliza el estándar 802.11n, el cual pertenece a la cuarta generación. Aunque este estándar se considera común y aceptable, a pesar de ser antiguo, es ideal utilizar el estándar más actualizado, el 802.11ax. Este estándar cuenta con varias mejoras y ofrece un rendimiento mejorado en comparación con sus predecesores.

Figura 20

Punto de Acceso AsisteCooper-Desarrollo Movil



Nota: El fabricante de este punto de acceso que, nos da la herramienta es Netcore Technology. Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

En este punto de acceso, se puede observar que la intensidad de la señal alcanza el 100%, mostrando su nivel máximo. Esta situación se interpreta como una señal eficiente para los dispositivos cercanos. Sin embargo, es importante tener en cuenta que la intensidad de la señal puede variar dependiendo de la distancia al punto de acceso, por lo que no siempre se mantendrá en 100%. A pesar de esto, se puede afirmar que el punto de acceso está funcionando correctamente y no se han detectado problemas en el equipo.

Al analizar el RSSI, se observa que el punto de acceso mantiene un valor de -16 dBm. Este valor indica que la intensidad de la señal no solamente es buena, sino excelente. Es importante destacar que a partir de los -20 dBm, se experimenta una pérdida significativa en la intensidad de la señal. Por lo tanto, se puede afirmar que el punto de acceso demuestra un nivel de señal excepcional, según la IEEE, proporcionando una conexión robusta y confiable para los dispositivos conectados.

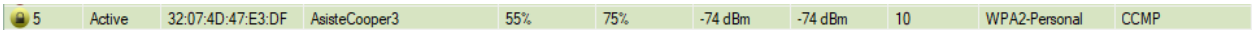
El punto de acceso opera en el canal 10, lo cual indica una señal eficiente de intensidad y una baja interferencia, similar al punto de acceso mostrado en la figura 18. La selección del canal de acceso está configurada en automático, lo que le permite adaptarse y elegir el canal óptimo según las condiciones del entorno. A través del número de canal, se confirma que el punto de acceso trabaja en la frecuencia de 2.4GHz.

En cuanto a la autenticación, se utiliza el tipo WPA2-Personal, al igual que el punto de acceso de la figura 18, lo cual se considera una de las formas más seguras de autenticación. Además, se emplea la misma encriptación CCMP, lo que asegura un alto nivel de seguridad en este punto de acceso.

El estándar 802.11 que utiliza este punto de acceso es el 802.11n el cual es aceptable, pero al igual que el punto de acceso de la figura 18 es ideal utilizar el estándar 802.11ax.

Figura 21

Punto de Acceso AsisteCooper-Soporte



Nota: El fabricante de este punto de acceso, que brinda la herramienta es Desconocido. Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

En este punto de acceso, se puede observar que la señal alcanza un nivel del 55%, con una señal máxima de 75%. Esta situación puede interpretarse como una señal poco eficiente. Es importante destacar que cuando la señal alcanza el 75%, se consideraría una señal eficiente, aunque esta condición solo se mantiene durante períodos cortos de tiempo. Se puede afirmar que el punto de acceso está funcionando adecuadamente y no se detecta problemas en el equipo.

Al analizar el RSSI, se observa que el punto de acceso presenta un valor de -74 dBm, con un máximo de -74 dBm. Esta situación indica una intensidad de señal débil , según la IEEE, lo

que se traduce como una señal que es lo suficientemente fuerte para mantener una conexión estable, pero puede haber una degradación significativa en el rendimiento.

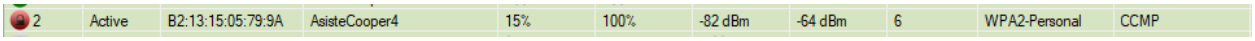
El punto de acceso opera en el canal 10, lo que indica que hay una buena eficiente de intensidad y baja interferencia en ese canal, al igual que los puntos de acceso de las figuras 19 y 18. La selección del canal es automática, lo que permite que el punto de acceso se adapte y elija el canal óptimo según el entorno. A través del número de canal, se confirma que el punto de acceso trabaja en la frecuencia de 2.4GHz.

La autenticación, utiliza WPA2-Personal con encriptación CCMP, lo que garantiza un alto nivel de seguridad en este punto de acceso.

En cuanto al estándar 802.11 que utiliza es el 802.11n, pero es ideal utilizar el estándar más actual 802.11ax.

Figura 22

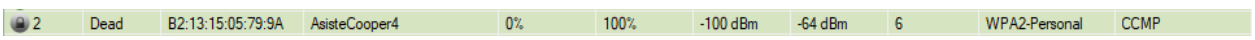
Punto de Acceso AsisteCooper-Contabilidad



Nota: El fabricante de este punto de acceso, que brinda da la herramienta es Desconocido. Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

Figura 23

Punto de Acceso AsisteCooper-Contabilidad



Nota: el punto de acceso se encuentra inactivo. Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

En este punto de acceso se puede observar que la señal alcanza un 15% con un nivel máximo de 100%, lo que se traduce como una señal poco eficiente y en el caso de que llegue a 100% la señal sería considerada eficiente, pero esto solo pasa durante periodos cortos de tiempo.

En la figura 22 se muestra el punto de acceso inactivo debido a un apagado repentino. Esto indica un mal funcionamiento del punto de acceso, posiblemente debido a daños en su entrada de corriente causados por una caída, golpe al equipo. Como resultado, el punto de acceso se apaga con movimientos bruscos. Se puede afirmar que es un punto de acceso defectuoso y que posee un problema de hardware.

Al analizar el RSSI, se observa que el punto de acceso presenta un valor -82 dBm, con un máximo de -64 dBm, Esta situación indica una intensidad de señal aceptable, según la IEEE, lo que se traduce en una señal que no alcanza niveles óptimos, pero se encuentra dentro de los rangos aceptables para un rendimiento adecuado.

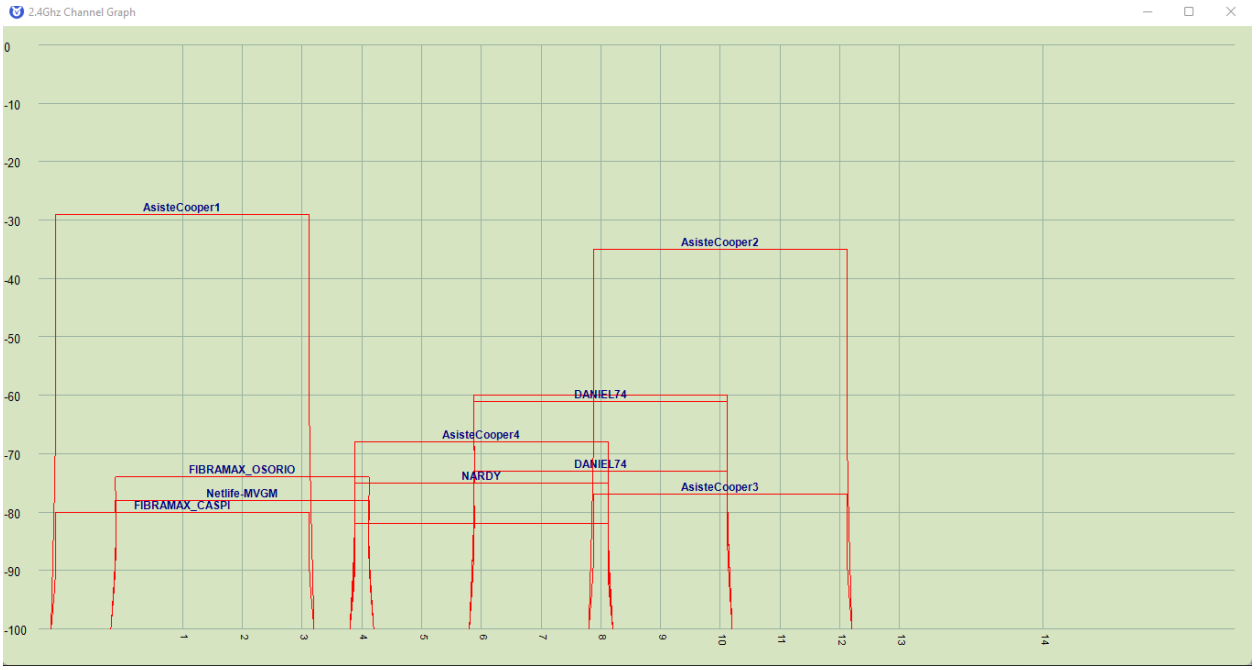
El punto de acceso opera en el canal seis, lo que indica que es el mejor canal en términos de intensidad de señal para este punto de acceso. La selección del canal para el punto de acceso es automática, y se ha determinado que el canal seis presenta una intensidad de señal especialmente baja en comparación de los otros canales, lo cual es favorable para el rendimiento y la calidad de la conexión. A través del número de canal, se confirma que el punto de acceso trabaja en la frecuencia de 2.4 GHz.

En este punto de acceso, se emplea la autenticación mediante WPA2-Personal y se utiliza la encriptación CCMP, lo cual proporciona un nivel de seguridad alto.

El estándar utilizado por este punto de acceso es el 802.11n, sin embargo, se recomienda migrar al estándar más reciente, el 802.11ax

Figura 24

Gráfico AccesPoint - Edificio - Oficinas AsisteCooper 2.4GHz



Nota: Vistumbler muestra una gráfica de todos los AccesPoints encontrados. Extraído de la herramienta Vistumbler. Elaborado por: Sandoval, M. (2023).

Se muestra un gráfico general de los puntos de acceso de la empresa AsisteCooper en funcionamiento, en la frecuencia de 2.4GHz, donde la mayoría de ellos se ubican en un rango promedio de intensidad de señal que va desde -29 dBm hasta -76 dBm.

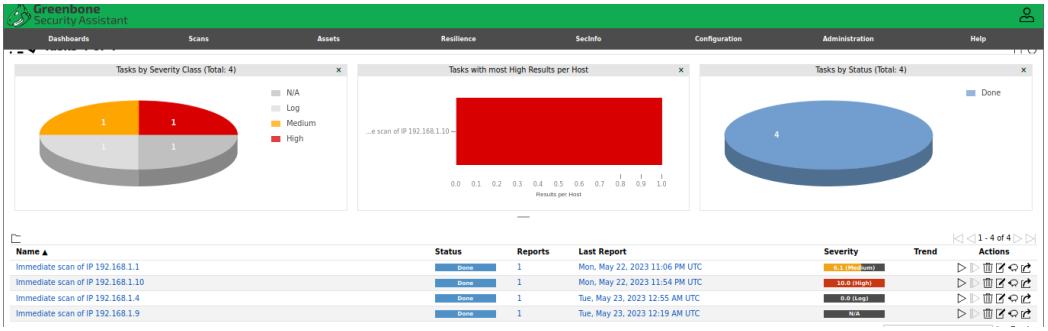
9.5. Análisis de vulnerabilidades de los Acces Points con la herramienta Greenbone

Con la herramienta Greebone, se realiza un análisis de las vulnerabilidades presentes en los puntos de acceso. Esta herramienta se emplea como una herramienta de escaneo de seguridad que permite identificar posibles debilidades y vulnerabilidades en los puntos de acceso de la red para la empresa AsisteCooper. Luego se hará un análisis a cada punto de acceso.

Para utilizar la herramienta Greenbone y analizar las vulnerabilidades de los puntos de acceso, es necesario contar con las direcciones IP de cada uno de ellos. Es importante destacar que las direcciones IP de los puntos de acceso no son estáticas, sino que son asignadas a través del protocolo DHCP (Dynamic Host Configuration Protocol). Esto significa que las direcciones IP de los puntos de acceso pueden cambiar dinámicamente en función de la configuración de la red.

Figura 25

Panel de control - Apartado Task.



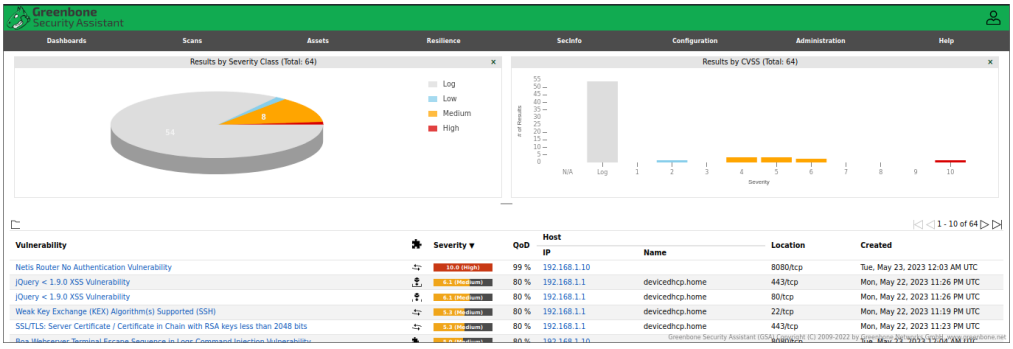
Nota: Se puede utilizar la información de este apartado para el análisis, sin embargo, existen secciones más adecuadas con información más precisa y mejor organizada. Extraído de la herramienta Greenbone.

Elaborado por: Sandoval, M. (2023).

En la herramienta Greenbone, se realizaron cuatro escaneos correspondientes a los cuatro puntos de acceso de la empresa. Esta información se encuentra en la sección de "Scans" dentro del apartado de "Task". La herramienta proporciona detalles sobre la severidad de cada escaneo, identificando el escaneo con el mayor número de vulnerabilidades y mostrando el estado del escaneo, el cual en este caso está completado y se muestra como "Done". Este apartado tiene como objetivo principal brindar un control visual del estado del escaneo, más que mostrar el resultado final del mismo. Su propósito es permitir la visualización y seguimiento del progreso del escaneo en tiempo real.

Figura 26

Panel de control - Apartado Result

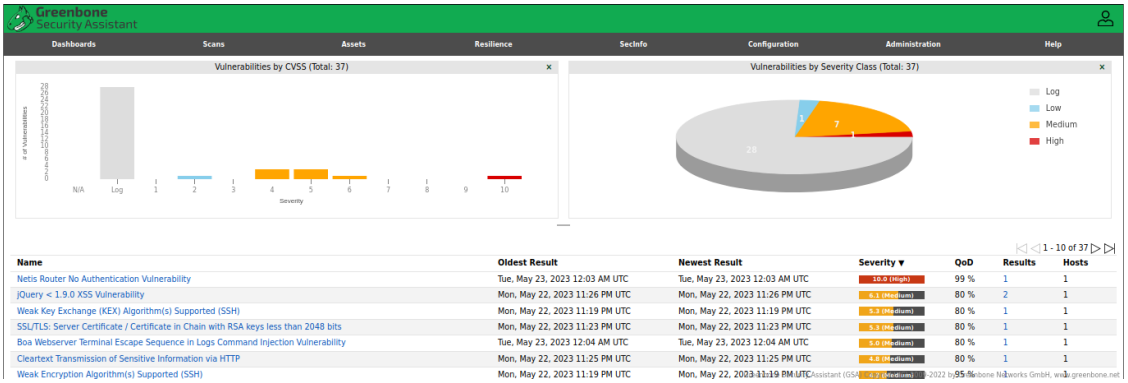


Nota: El apartado puede llegar a estar saturado de log´s, debido a que su función principal es mostrar todo lo que se encuentra en el escaneo, esta sección presenta información relevante y también información de menor importancia, los log´s son información que se clasifican como menor importancia o importancia media. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La herramienta Greenbone ofrece el apartado "Result" en la sección "Scan", donde se puede visualizar los resultados de los escaneos y las vulnerabilidades encontradas. Además, es importante destacar que este apartado también muestra los logs, que son registros detallados de las actividades y eventos relacionados con los escaneos y la seguridad. Los logs proporcionan información adicional sobre las acciones realizadas, las configuraciones aplicadas y otros eventos relevantes o con ninguna relevancia. Sin embargo, es importante tener en cuenta que los logs en sí no representan vulnerabilidades, sino que sirven como un registro de seguimiento para comprender mejor el estado y las acciones realizadas en el sistema. Los logs desempeñan un papel crucial en la auditoría, el análisis forense y la detección de posibles incidentes de seguridad.

Figura 27

Panel de Control - Apartado vulnerabilities



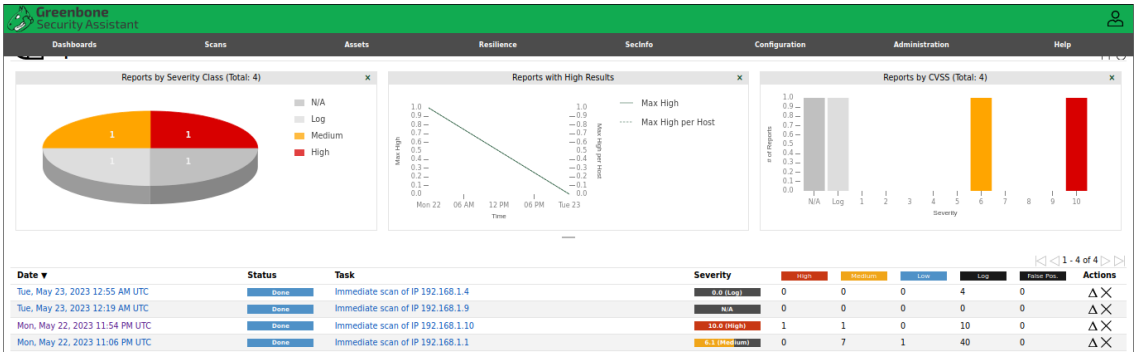
Nota: Este apartado muestra todas las vulnerabilidades sin clasificación por escaneo. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

En el apartado "Vulnerabilities", se presentan todas las vulnerabilidades detectadas en los escaneos realizados. Aquí se muestra información detallada sobre cada vulnerabilidad, como su nombre, descripción, nivel de severidad y posibles soluciones. Además, en este apartado también

se incluyen los logs relacionados, que proporcionan registros de eventos y actividades relevantes. Sin embargo, a diferencia del apartado "Result", en el apartado "Vulnerabilities" se muestran únicamente los logs con un mayor grado de importancia, aquellos que están relacionados directamente con las vulnerabilidades detectadas. Esto permite a los usuarios enfocarse en los eventos más críticos y tomar medidas adecuadas para abordar las vulnerabilidades identificadas en el sistema.

Figura 28

Panel de control - Apartado Reports



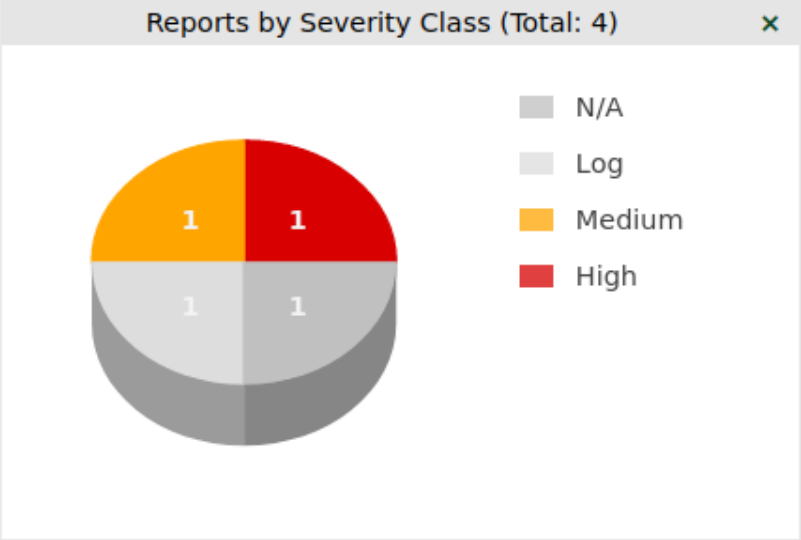
Nota: muestra la información de los tres apartados anteriores, Vulnerabilities, Task, Result. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La herramienta Greenbone ofrece el apartado "Reports", el cual se destaca por ser completo y altamente organizado. En este apartado, se presentan datos resumidos de manera eficiente. Cada escaneo cuenta con un sub-apartado ubicado en la columna "Date". Al presionar en la fecha de un escaneo específico, se accede a un subapartado que proporciona información detallada sobre dicho escaneo. A la derecha, se muestran el número de vulnerabilidades encontradas y la clasificación por niveles, junto con el número de logs importantes encontrados

durante cada escaneo. Este apartado es fundamental para llevar a cabo el análisis de vulnerabilidades en la red.

Figura 29

Clasificación de severidad de los Puntos de Acceso.

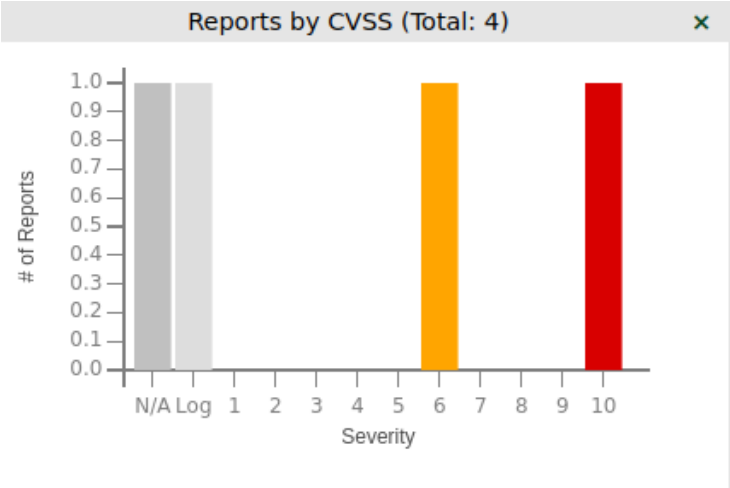


Nota: muestra la severidad promedio de cada escaneo. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Durante el escaneo de vulnerabilidades, se detectó que dos de los cuatro puntos de acceso presentaban vulnerabilidades. En uno de los puntos de acceso, se encontraron únicamente logs, los cuales no se consideran vulnerabilidades, mientras que en el otro punto de acceso no se detectó ningún problema. Con base en estos resultados, se puede interpretar que hay dos puntos de acceso que requieren atención y acciones para abordar las vulnerabilidades identificadas.

Figura 30

Clasificación de Severidad por CVSS



Nota: Se recomienda utilizar la clasificación CVSS para el análisis, ya que es más específica en cuanto al nivel de amenaza que presenta. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La herramienta Greenbone proporciona la clasificación CVSS para obtener una mejor comprensión del nivel de gravedad de cada escaneo. Durante el proceso de escaneo, se detectó un punto de acceso con una severidad de nivel seis, lo cual se cataloga como una severidad de grado medio según los estándares establecidos. Las vulnerabilidades de este nivel tienen un impacto significativo, pero su explotación puede ser difícil y requerir condiciones específicas. Además, se identificó un punto de acceso con una severidad de nivel 10, que se clasifica como una severidad de grado crítico. Estas vulnerabilidades representan un riesgo extremadamente alto y son altamente explotables según los estándares establecidos. Basándonos en estos resultados se puede interpretar que es necesario tomar medidas urgentes para abordar las vulnerabilidades encontradas en el punto de acceso con severidad de nivel 10 y que se debe tomar acciones para mitigar las vulnerabilidades de nivel seis.

Figura 31

Punto de Acceso AsisteCooper-Desarrollo

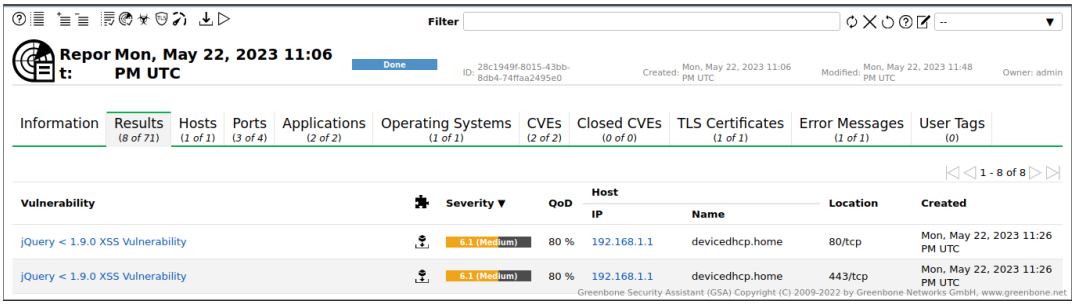
Date ▲	Status	Task	Severity	High	Medium	Low	Log	False Pos.
Mon, May 22, 2023 11:06 PM UTC	Done	Immediate scan of IP 192.168.1.1	6.1 (Medium)	0	7	1	40	0

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

En el punto de acceso con la dirección IP 192.168.1.1, se ha identificado una severidad promedio de nivel medio, con una puntuación de severidad CVSS de 6.1. Se han detectado siete vulnerabilidades de nivel medio y una vulnerabilidad de nivel bajo. Además, se registraron 40 logs durante el escaneo, sin encontrar ningún falso positivo. Estos resultados indican la presencia de ciertas vulnerabilidades que requieren atención y acciones adecuadas para fortalecer la seguridad en el punto de acceso.

Figura 32

Sub-apartado Reports - Desarrollo



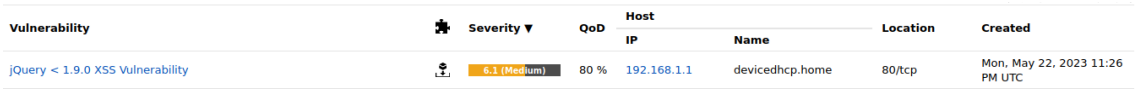
Nota: la sección Results tiene la mayor cantidad de información resumida. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

En el sub-apartado de Reports, se puede encontrar información similar a la del apartado Result. Sin embargo, la diferencia radica en que aquí solo se muestran las vulnerabilidades específicas encontradas en el escaneo de un punto de acceso en particular. Además, es importante mencionar que, aunque en la parte superior del apartado se muestra "8 of 71", esto se refiere a la cantidad total de log´s registrados más las vulnerabilidades, los cuales no se visualizan ya que no son considerados como vulnerabilidades, en este punto de acceso se detectaron 63 log´s y 8 vulnerabilidades dando un total de 71.

Dentro de este subapartado, se encuentran varias secciones que brindan información más detallada y específica. Estos apartados, como "Hosts", "Ports", "Applications", "Operating Systems", "Closed CVEs" y "User Tags", presentan datos que pueden considerarse redundantes o de menor prioridad para el trabajo en cuestión. Sin embargo, el apartado más relevante y sin redundancia es el de "CVEs", el cual representa un identificador asignado a las vulnerabilidades detectadas. Este identificador facilita el seguimiento de las vulnerabilidades, ya que se utiliza un registro centralizado de CVEs para mantener un control y una referencia unificada de las mismas.

Figura 33

Punto de Acceso - Desarrollo - Vulnerabilidad 1.



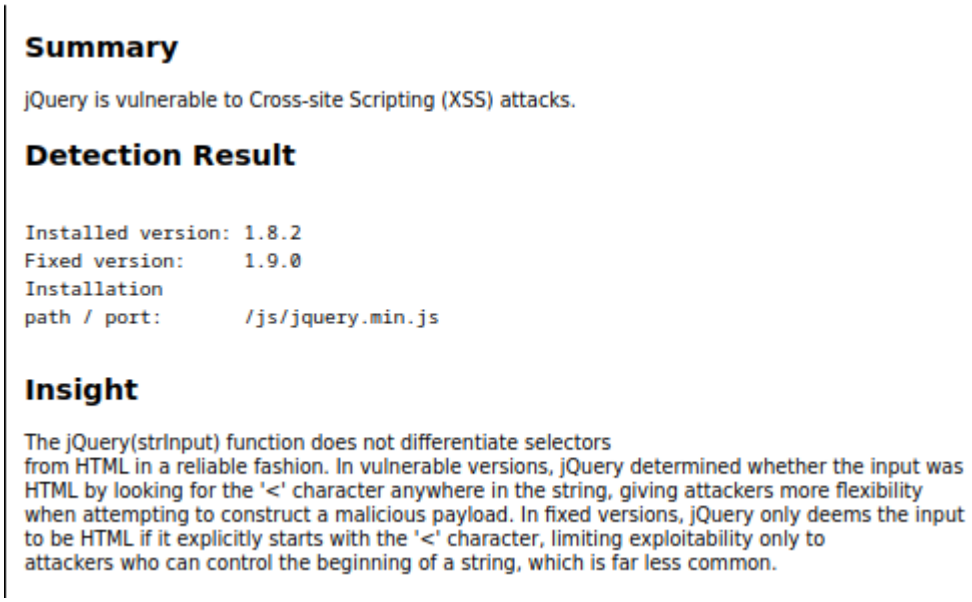
Vulnerability	Severity ▼	QoD	Host		Location	Created
			IP	Name		
jQuery < 1.9.0 XSS Vulnerability	6.1 (Medium)	80 %	192.168.1.1	devicedhcp.home	80/tcp	Mon, May 22, 2023 11:26 PM UTC

Nota: Locación puerto 80/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Al hacer clic sobre una vulnerabilidad en Greenbone, se despliega información detallada sobre la misma en el apartado correspondiente. Esta información incluye un resumen de la vulnerabilidad, la descripción de su funcionamiento, el método de detección utilizado, el impacto que puede tener y las posibles soluciones para mitigarla.

Figura 34

Punto de Acceso - Desarrollo - Vulnerabilidad 1- Ficha de vulnerabilidad



Summary

jQuery is vulnerable to Cross-site Scripting (XSS) attacks.

Detection Result

```
Installed version: 1.8.2
Fixed version:     1.9.0
Installation
path / port:       /js/jquery.min.js
```

Insight

The jQuery(strInput) function does not differentiate selectors
from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 35

Punto de Acceso - Desarrollo - Vulnerabilidad 1- Solución de Vulnerabilidad

Detection Method

Checks if a vulnerable version is present on the target host.

Details: jQuery < 1.9.0 XSS Vulnerability OID: 1.3.6.1.4.1.25623.1.0.141636

Version used: 2021-06-11T08:43:18Z

Affected Software/OS

jQuery prior to version 1.9.0.

Solution

Solution Type: Vendorfix
Update to version 1.9.0 or later.

References

CVE CVE-2012-6708

CERT DFN-CERT-2020-0590
WID-SEC-2022-0673
CB-K22/0045
CB-K18/1131

Other https://bugs.jquery.com/ticket/11290

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La vulnerabilidad detectada en jQuery es conocida como Cross-site Scripting (XSS). Esta vulnerabilidad permite a un atacante insertar código malicioso en una página web que utiliza la biblioteca jQuery. Cuando un usuario accede a esa página comprometida, el código malicioso se ejecuta en su navegador, lo que puede resultar en diversas consecuencias negativas.

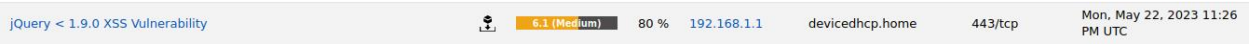
La solución para abordar la vulnerabilidad de Cross-site Scripting (XSS) en jQuery es actualizar a la versión 1.9.0 o posterior. Esta actualización proporciona una solución proporcionada por el proveedor (Vendorfix) que aborda la vulnerabilidad y se aplican

actualizaciones de software a las posibles brechas de seguridad asociadas con esta versión específica de jQuery.

Con toda esta información se puede interpretar que la vulnerabilidad de Cross-site Scripting (XSS) en jQuery es de nivel 6.1 CVSS y representa un riesgo significativo para la seguridad de las aplicaciones web que utilizan esta biblioteca.

Figura 36

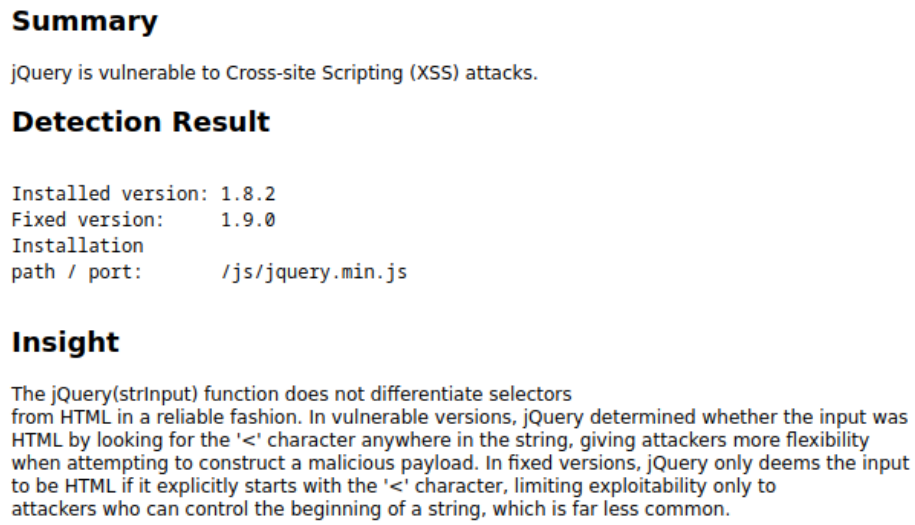
Punto de Acceso - Desarrollo - Vulnerabilidad 2



Nota: Locación puerto 443/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 37

Punto de Acceso - Desarrollo - Vulnerabilidad 2- Ficha de vulnerabilidad



Summary

jQuery is vulnerable to Cross-site Scripting (XSS) attacks.

Detection Result

```
Installed version: 1.8.2
Fixed version:     1.9.0
Installation
path / port:       /js/jquery.min.js
```

Insight

The jQuery(strInput) function does not differentiate selectors
from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was
HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility
when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input
to be HTML if it explicitly starts with the '<' character, limiting exploitability only to
attackers who can control the beginning of a string, which is far less common.

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 38

Punto de Acceso - Desarrollo - Vulnerabilidad 2- Solución de Vulnerabilidad

Detection Method

Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.9.0 XSS Vulnerability OID: 1.3.6.1.4.1.25623.1.0.141636
Version used: 2021-06-11T08:43:18Z

Affected Software/OS

jQuery prior to version 1.9.0.

Solution

Solution Type: Vendorfix
Update to version 1.9.0 or later.

References

CVE CVE-2012-6708
CERT DFN-CERT-2020-0590
WID-SEC-2022-0673
CB-K22/0045
CB-K18/1131
Other https://bugs.jquery.com/ticket/11290

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La vulnerabilidad de Cross-site Scripting (XSS) en jQuery permite a los atacantes insertar código malicioso en páginas web que utilizan esta biblioteca. Para solucionar esta vulnerabilidad, se recomienda actualizar a la versión 1.9.0 o posterior, que incluye una solución proporcionada por el proveedor (Vendorfix). Con esta información se interpreta que la vulnerabilidad es de nivel 6.1 CVSS y representa un riesgo significativo para la seguridad de las aplicaciones web que utilizan jQuery.

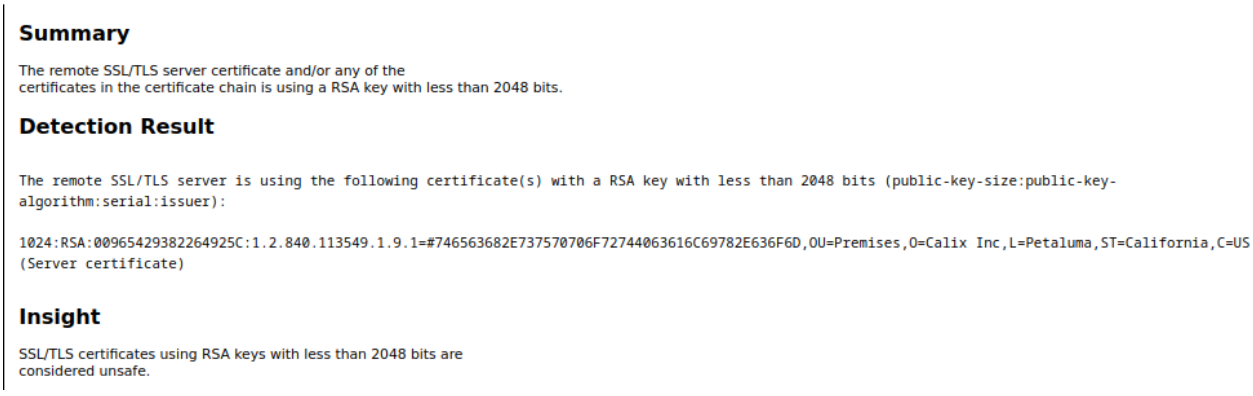
Figura 39

Punto de Acceso - Desarrollo - Vulnerabilidad 3

Nota: localización puerto 443/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 40

Punto de Acceso - Desarrollo - Vulnerabilidad 3- Ficha de Vulnerabilidad



Summary

The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

Detection Result

The remote SSL/TLS server is using the following certificate(s) with a RSA key with less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):

1024:RSA:00965429382264925C:1.2.840.113549.1.9.1=#746563682E737570706F72744063616C69782E636F6D,OU=Premises,O=Calix Inc,L=Petaluma,ST=California,C=US (Server certificate)

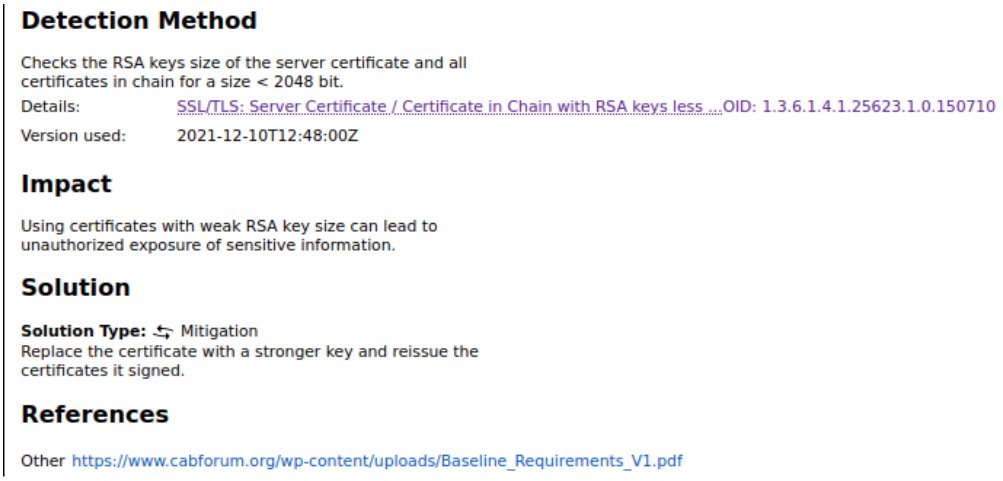
Insight

SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 41

Punto de Acceso - Desarrollo - Vulnerabilidad 3 - Solución de Vulnerabilidad



Nota: Extraído de la herramienta Greenbone.Elaborado por: Sandoval, M. (2023).

La vulnerabilidad identificada en el certificado del servidor remoto SSL/TLS y/o en alguno de los certificados de la cadena indica que se está utilizando una clave RSA con una longitud inferior a 2048 bits. Esto representa un problema, ya que la fortaleza criptográfica se encuentra por debajo de los estándares recomendados, lo que podría exponer el sistema a ataques de fuerza bruta y comprometer la seguridad de la comunicación.

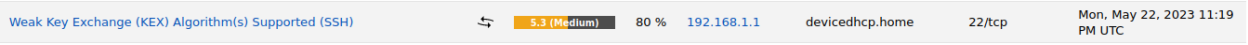
La solución propuesta para abordar esta vulnerabilidad consiste en mitigar el problema mediante la sustitución del certificado actual por uno que utilice una clave más fuerte, con una longitud igual o superior a 2048 bits. Además, es necesario reemitir los certificados que hayan sido firmados por el certificado afectado.

Es importante destacar que esta solución se considera una medida de mitigación, debido a que, si bien reduce el riesgo asociado a la vulnerabilidad, no representa una solución definitiva. Sin embargo, al implementar esta medida, se mejora la seguridad del sistema y se reduce la probabilidad de explotación de la debilidad en la clave RSA.

Con esta información se puede afirmar que la vulnerabilidad tiene un nivel de 5.3 CVSS y está relacionada con el uso de una clave RSA inferior a 2048 bits en el certificado SSL/TLS requiere la adopción de acciones de mitigación, como la actualización del certificado y la emisión de nuevos certificados firmados. Estas medidas contribuyen a fortalecer la seguridad de la comunicación y proteger los sistemas involucrados.

Figura 42

Punto de Acceso - Desarrollo - Vulnerabilidad 4



Nota: Localización en el puerto 22/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 43

Punto de Acceso - Desarrollo - Vulnerabilidad 4- Ficha de Vulnerabilidad

Summary

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Detection Result

The remote SSH server supports the following weak KEX algorithm(s):

KEX algorithm	Reason
diffie-hellman-group1-sha1	Using Oakley Group 2 (a 1024-bit MODP group) and SHA-1

Insight

- 1024-bit MODP group / prime KEX algorithms:

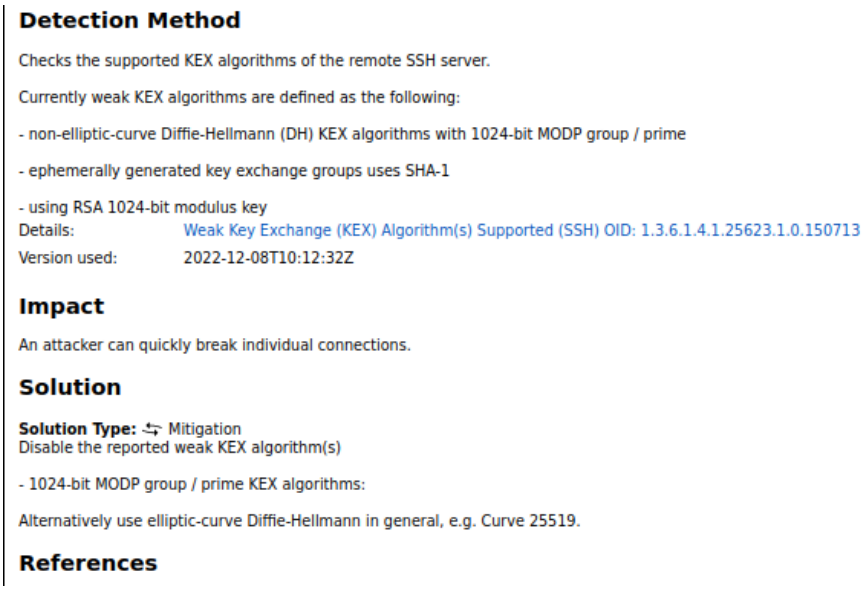
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.

A nation-state can break a 1024-bit prime.

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 44

Punto de Acceso - Desarrollo - Vulnerabilidad 4 – Solución de Vulnerabilidad



Detection Method

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime

- ephemerally generated key exchange groups uses SHA-1

- using RSA 1024-bit modulus key

Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) OID: 1.3.6.1.4.1.25623.1.0.150713

Version used: 2022-12-08T10:12:32Z

Impact

An attacker can quickly break individual connections.

Solution

Solution Type: Mitigation
Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

References

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La vulnerabilidad detectada indica que el servidor SSH remoto está configurado para permitir o admitir algoritmos de intercambio de claves (KEX) débiles. Los algoritmos de intercambio de claves débiles son aquellos que no ofrecen una suficiente seguridad criptográfica y pueden ser más susceptibles a ataques de fuerza bruta o criptoanálisis.

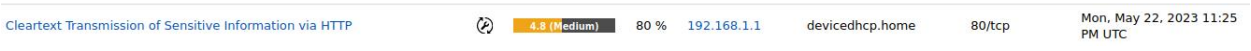
La presencia de algoritmos de intercambio de claves débiles en la configuración del servidor SSH puede comprometer la seguridad de las comunicaciones. Un atacante podría aprovechar estas debilidades para interceptar o modificar la información transmitida, comprometiendo así la confidencialidad y la integridad de los datos.

La solución propuesta para abordar la vulnerabilidad de permitir algoritmos de intercambio de claves débiles en el servidor SSH es mitigar el problema mediante la desactivación de los algoritmos de KEX débiles reportados.

La solución se clasifica como mitigación, ya que implica tomar medidas para reducir el riesgo asociado a la vulnerabilidad, aunque no la elimina por completo. Con toda esta información se puede afirmar que la vulnerabilidad es de nivel 5.3 CVSS y esta no puede ser eliminada del punto de acceso, solo mitigada.

Figura 45

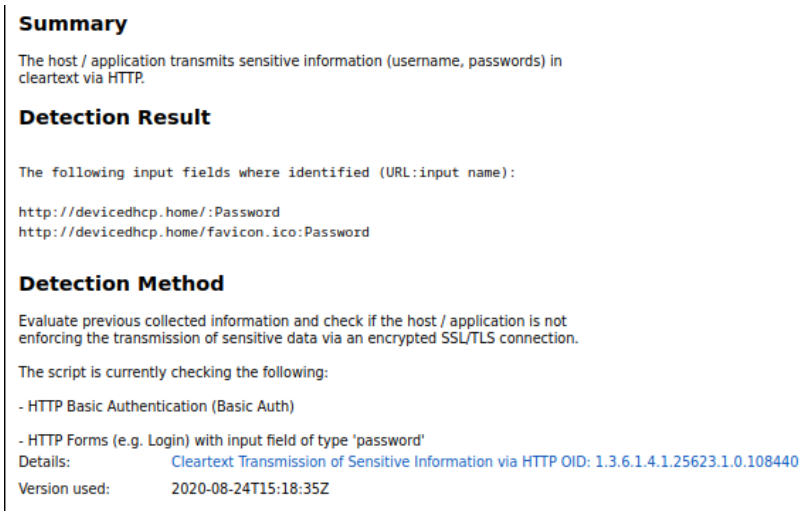
Punto de Acceso - Desarrollo - Vulnerabilidad 5



Nota localización en el puerto 80/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 46

Punto de Acceso - Desarrollo - Vulnerabilidad 5 – Ficha de Vulnerabilidad.



Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Detection Result

The following input fields where identified (URL:input name):

http://devicedhcp.home/:Password
http://devicedhcp.home/favicon.ico:Password

Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)

- HTTP Forms (e.g. Login) with input field of type 'password'

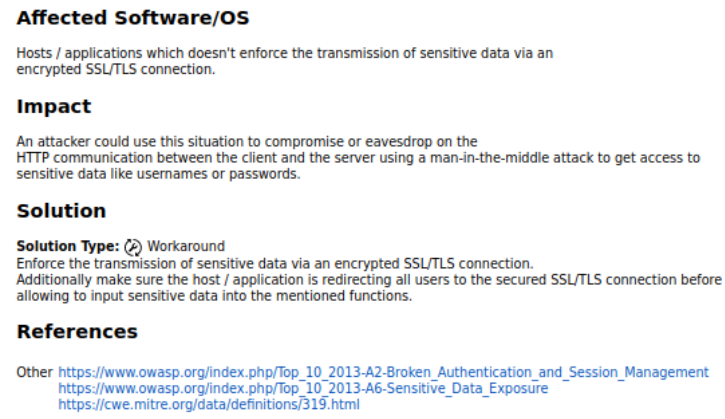
Details: Cleartext Transmission of Sensitive Information via HTTP OID: 1.3.6.1.4.1.25623.1.0.108440

Version used: 2020-08-24T15:18:35Z

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 47

Punto de Acceso - Desarrollo - Vulnerabilidad 5 - Solución de Vulnerabilidad.



Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution

Solution Type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

References

Other https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management
https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
https://cwe.mitre.org/data/definitions/319.html

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La vulnerabilidad detectada indica que el host o la aplicación transmite información sensible, como nombres de usuario y contraseñas, en texto plano a través del protocolo HTTP.

Esto significa que la información confidencial se envía sin cifrar, lo que puede permitir que un atacante intercepte y acceda fácilmente a estos datos.

La solución propuesta para abordar la vulnerabilidad de transmitir información sensible en texto plano a través de HTTP es aplicar un enfoque temporal conocido como "workaround". Este enfoque implica implementar medidas para garantizar la transmisión de datos sensibles a través de una conexión SSL/TLS cifrada.

Con esta información se interpreta que la vulnerabilidad de transmitir información sensible en texto plano a través de HTTP puede ser mitigada aplicando un enfoque temporal conocido como "workaround" que garantiza la transmisión de datos sensibles a través de una conexión SSL/TLS cifrada y que esta tiene un nivel 4.8 en CVSS.

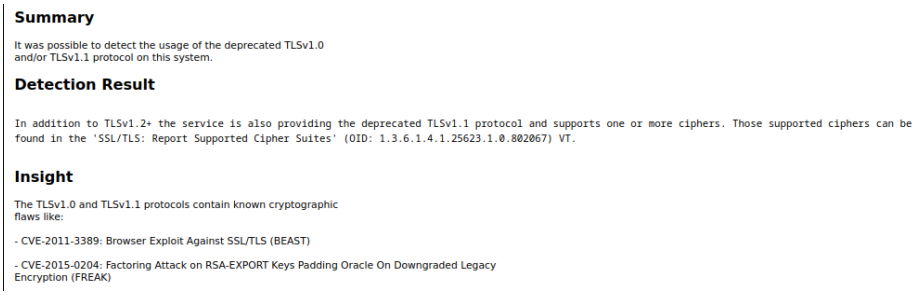
Figura 48

Punto de Acceso - Desarrollo - Vulnerabilidad 6

Nota: Localización en el puerto 443/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 49

Punto de Acceso - Desarrollo - Vulnerabilidad 6 - Ficha de Vulnerabilidades



Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Detection Result

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.1 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

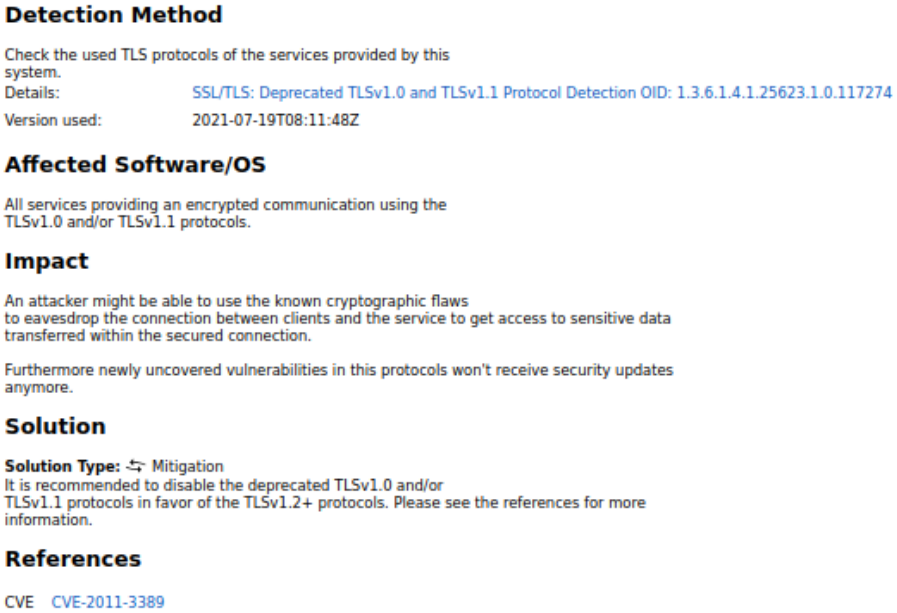
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 50

Punto de Acceso - Desarrollo - Vulnerabilidad 6 – Solución de Vulnerabilidades



Detection Method

Check the used TLS protocols of the services provided by this system.

Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID: 1.3.6.1.4.1.25623.1.0.117274

Version used: 2021-07-19T08:11:48Z

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution

Solution Type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

References

CVE CVE-2011-3389

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La vulnerabilidad detectada indica que en este sistema usa del protocolo TLSv1.0 y/o TLSv1.1, los cuales están obsoletos y no ofrecen un nivel adecuado de seguridad. Estos

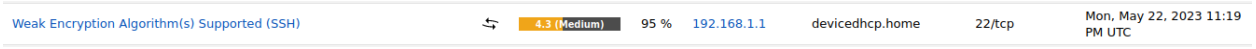
protocolos presentan vulnerabilidades conocidas que pueden ser explotadas por atacantes para comprometer la confidencialidad e integridad de las comunicaciones.

La solución propuesta, clasificada como mitigación, consiste en deshabilitar los protocolos TLSv1.0 y/o TLSv1.1 obsoletos en favor de los protocolos TLSv1.2 o superiores. Esto se recomienda para abordar la vulnerabilidad detectada y mejorar la seguridad de las comunicaciones.

Con esta información se interpreta que la vulnerabilidad detectada es, protocolos obsoletos que tiene que ser actualizados para mitigar los riesgos y que el nivel de la vulnerabilidad es de 4.3 CVSS.

Figura 51

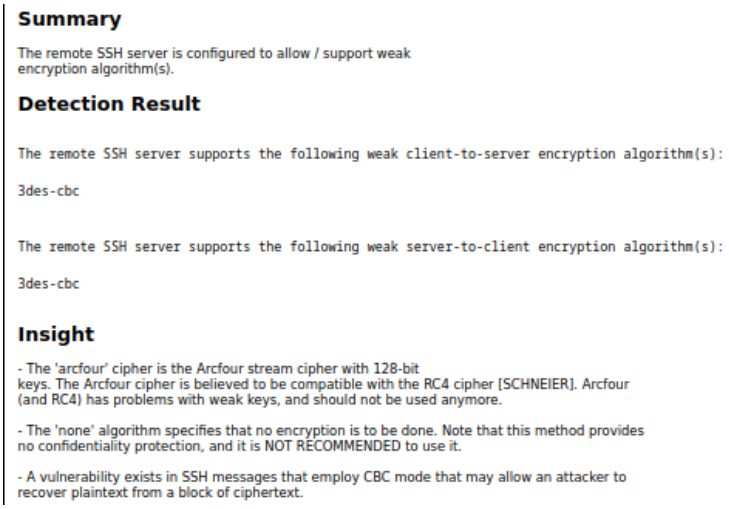
Punto de Acceso - Desarrollo - Vulnerabilidad 7



Nota: Localización en el puerto 22/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 52

Punto de Acceso - Desarrollo - Vulnerabilidad 7- Ficha de Vulnerabilidad



Summary

The remote SSH server is configured to allow / support weak encryption algorithm(s).

Detection Result

The remote SSH server supports the following weak client-to-server encryption algorithm(s):

3des-cbc

The remote SSH server supports the following weak server-to-client encryption algorithm(s):

3des-cbc

Insight

- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 53

Punto de Acceso - Desarrollo - Vulnerabilidad 7- Solución de Vulnerabilidad.

Detection Method

Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak encryption algorithms are defined as the following:

- Arcfour (RC4) cipher based algorithms

- none algorithm

- CBC mode cipher based algorithms

Details: Weak Encryption Algorithm(s) Supported (SSH) OID: 1.3.6.1.4.1.25623.1.0.105611

Version used: 2022-12-09T10:11:04Z

Solution

Solution Type: Mitigation
Disable the reported weak encryption algorithm(s).

References

Other https://www.rfc-editor.org/rfc/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

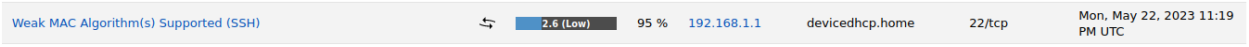
La vulnerabilidad detectada indica que el servidor SSH remoto está configurado para permitir o admitir algoritmos de cifrados débiles. Los algoritmos de cifrados débiles son aquellos que no proporcionan un nivel adecuado de seguridad criptográfica y pueden ser más susceptibles a ataques de fuerza bruta o criptoanálisis.

La solución propuesta para abordar esta vulnerabilidad es deshabilitar los algoritmos de cifrados débiles reportados. Esto implica configurar el servidor SSH para permitir solo algoritmos de cifrados fuertes y seguros, que brinden un nivel adecuado de protección para las comunicaciones.

Con esta información se puede afirmar que el nivel CVSS de esta vulnerabilidad es de 4.3 y que la presencia de algoritmos de cifrados débiles en el servidor SSH representa un riesgo significativo para la seguridad de las comunicaciones. Es recomendable tomar medidas para deshabilitar estos algoritmos y garantizar el uso exclusivo de algoritmos de cifrados fuertes y seguros.

Figura 54

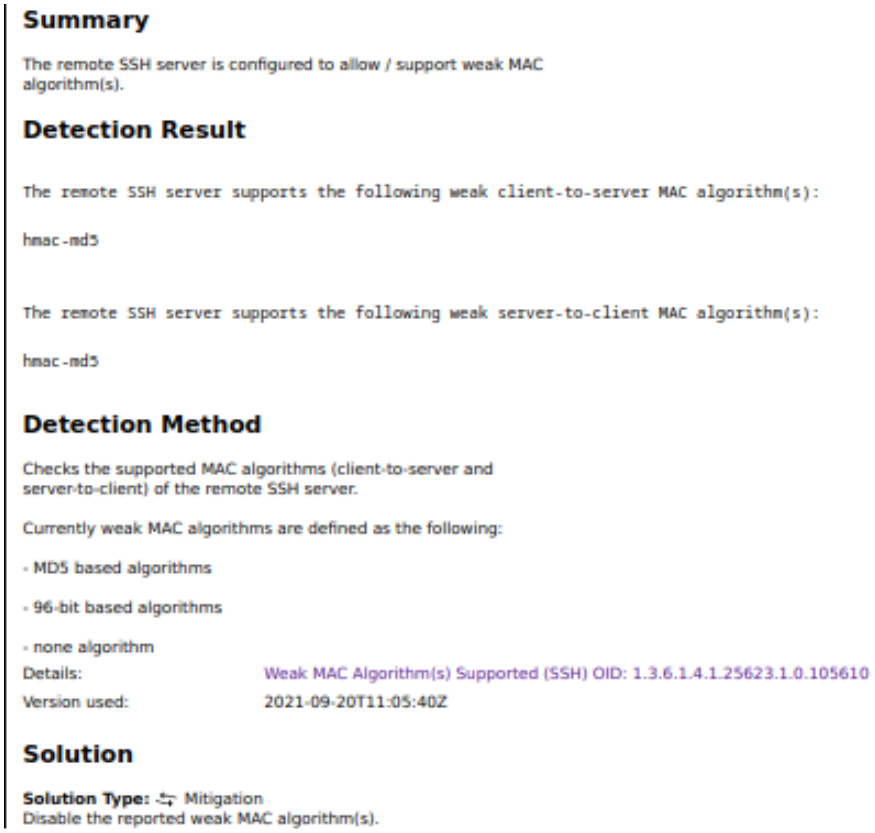
Punto de Acceso - Desarrollo - Vulnerabilidad 8



Nota: Localización en el puerto 22/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 55

Punto de Acceso - Desarrollo - Vulnerabilidad 8 – Ficha y Solución de Vulnerabilidad



Summary

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Detection Result

The remote SSH server supports the following weak client-to-server MAC algorithm(s):

hmac-md5

The remote SSH server supports the following weak server-to-client MAC algorithm(s):

hmac-md5

Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms
- 96-bit based algorithms
- none algorithm

Details: Weak MAC Algorithm(s) Supported (SSH) OID: 1.3.6.1.4.1.25623.1.0.105610

Version used: 2021-09-20T11:05:40Z

Solution

Solution Type: Mitigation

Disable the reported weak MAC algorithm(s).

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La vulnerabilidad detectada indica que el servidor SSH remoto está configurado para permitir o admitir algoritmos de autenticación de mensajes (MAC) débiles. Los algoritmos de MAC débiles son aquellos que ofrecen una menor seguridad y pueden ser más susceptibles a ataques de falsificación o manipulación de mensajes.

La solución propuesta para abordar la vulnerabilidad de permitir algoritmos de autenticación de mensajes (MAC) débiles en el servidor SSH es desactivar los algoritmos débiles

reportados. Esta solución se clasifica como mitigación, ya que implica tomar medidas para reducir el riesgo asociado a la vulnerabilidad, aunque no la elimina por completo.

Con esta información, se puede afirmar que la presencia de algoritmos de MAC débiles en el servidor SSH representa un riesgo significativo para la integridad de las comunicaciones y es necesario tomar medidas para mitigar esta vulnerabilidad desactivando los algoritmos débiles y utilizando opciones más seguras.

Figura 56

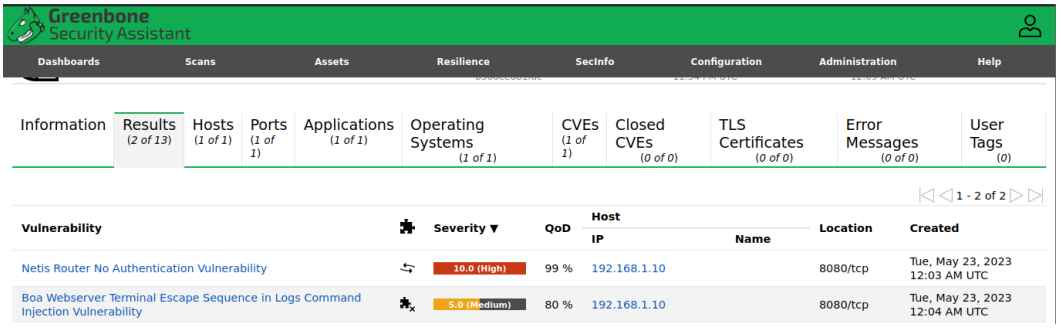
Punto de Acceso AsisteCooper-Desarrollo Móvil

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

En el punto de acceso con la dirección IP 192.168.1.10, se ha identificado una severidad promedio de nivel alto, con una puntuación de severidad CVSS de 10.0. Se han detectado una vulnerabilidad de nivel alto y una vulnerabilidad de nivel medio. Además, se registraron 10 log´s durante el escaneo, sin encontrar ningún falso positivo. Estos resultados indican la presencia de dos vulnerabilidades que requieren atención urgente y acciones inmediatas ya que representan un gran peligro para la red.

Figura 57

Sub-apartado Reports - Desarrollo Móvil

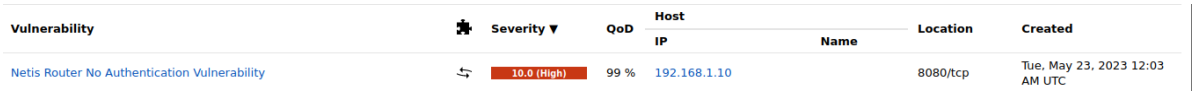


Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

En el apartado Reports se puede observar dos vulnerabilidades de nivel alto y que la vulnerabilidad de nivel CVSS 10.0 tiene un QoD de 99% lo que indica que el escaneo no sufrió ninguna interrupción al momento de encontrar la vulnerabilidad.

Figura 58

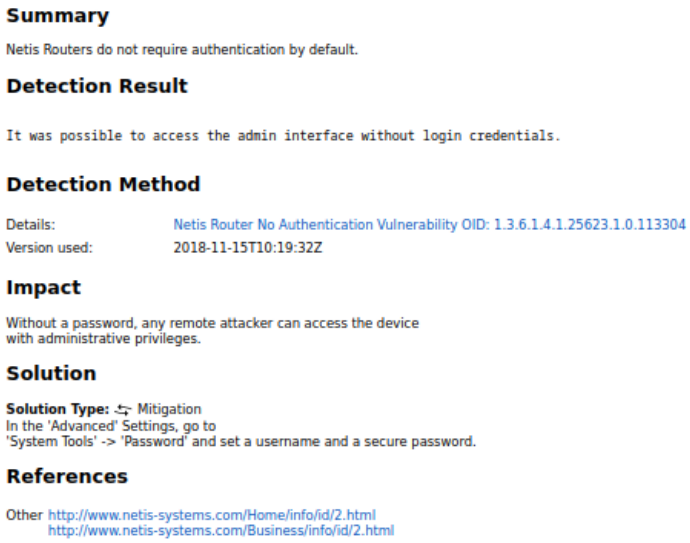
Punto de Acceso - Desarrollo Móvil - Vulnerabilidad 1



Nota: Localización en el puerto 8080/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 59

Punto de Acceso - Desarrollo Móvil - Vulnerabilidad 1- Ficha y Solución de Vulnerabilidad.



Summary

Netis Routers do not require authentication by default.

Detection Result

It was possible to access the admin interface without login credentials.

Detection Method

Details: Netis Router No Authentication Vulnerability OID: 1.3.6.1.4.1.25623.1.0.113304
Version used: 2018-11-15T10:19:32Z

Impact

Without a password, any remote attacker can access the device with administrative privileges.

Solution

Solution Type: Mitigation
In the 'Advanced' Settings, go to 'System Tools' -> 'Password' and set a username and a secure password.

References

Other http://www.netis-systems.com/Home/info/id/2.html
http://www.netis-systems.com/Business/info/id/2.html

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

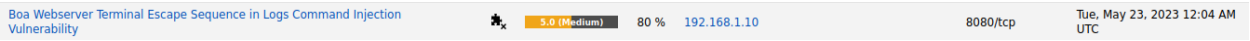
La vulnerabilidad detectada indica que los enrutadores Netis no requieren autenticación de forma predeterminada. Esto significa que, al configurar un enrutador Netis, no se solicita al usuario que establezca credenciales de inicio de sesión, como un nombre de usuario y una contraseña. Esta falta de autenticación representa un riesgo significativo para la seguridad de la red, ya que cualquier persona que tenga acceso físico o remoto al enrutador puede acceder a su interfaz de administración sin ninguna barrera de protección.

La solución recomendada para abordar esta vulnerabilidad es configurar de forma adecuada la autenticación en los enrutadores Netis. Esto implica establecer credenciales de inicio de sesión seguras y personalizadas, como un nombre de usuario y una contraseña fuertes.

Con esta información se interpreta que la falta de autenticación por defecto en los enrutadores Netis representa un riesgo significativo para la seguridad de la red y eso es lo que le da el nivel 10.0 en CVSS.

Figura 60

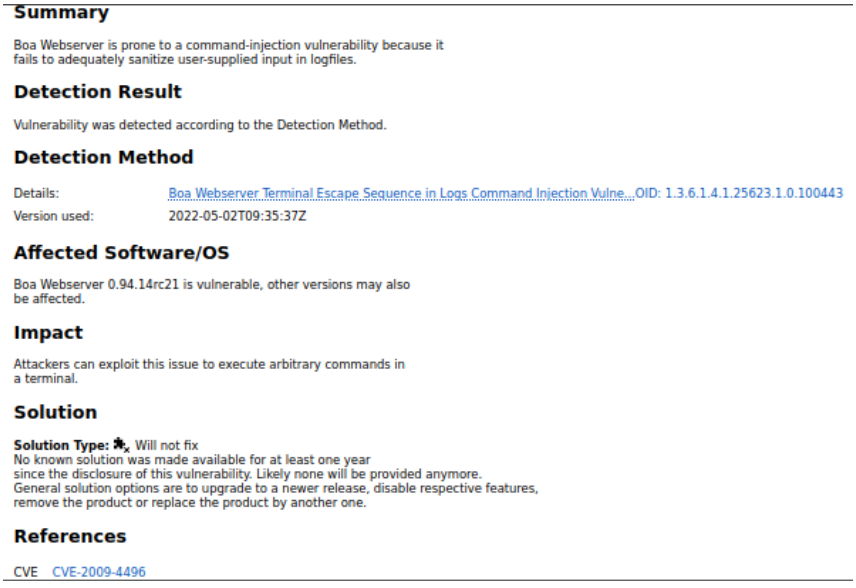
Punto de Acceso - Desarrollo Móvil - Vulnerabilidad 2



Nota: Localización en el puerto 8080/tcp. Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

Figura 61

Punto de Acceso - Desarrollo Móvil - Vulnerabilidad 2 - Ficha y Solución de Vulnerabilidad.



Nota: Extraído de la herramienta Greenbone.Elaborado por: Sandoval, M. (2023).

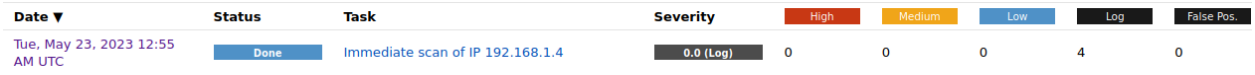
La vulnerabilidad detectada en el servidor web Boa se refiere a una vulnerabilidad de inyección de comandos. Esta vulnerabilidad ocurre debido a la falta de sanitización adecuada de la entrada proporcionada por el usuario en los archivos de registro. Al no realizar una validación y filtrado adecuados de los datos ingresados por el usuario, un atacante malintencionado puede aprovechar esta vulnerabilidad para ejecutar comandos arbitrarios en el sistema afectado.

Greenbone no ha proporcionado soluciones conocidas durante al menos un año desde la divulgación de esta vulnerabilidad. Es probable que ya no estén disponibles opciones de solución. Las posibles acciones para abordar esta vulnerabilidad incluyen la actualización a una versión más reciente del software, la desactivación de las funciones relevantes, la retirada del producto o su sustitución por otro.

Con esta información se interpreta que la vulnerabilidad en cuestión no ha sido corregida durante un período de al menos un año desde su descubrimiento. Es posible que no exista una solución disponible o que el proveedor del software no haya proporcionado una y es por esta razón que tiene un nivel de 5.0 en CVSS.

Figura 62

Punto de Acceso AsisteCooper-Soporte



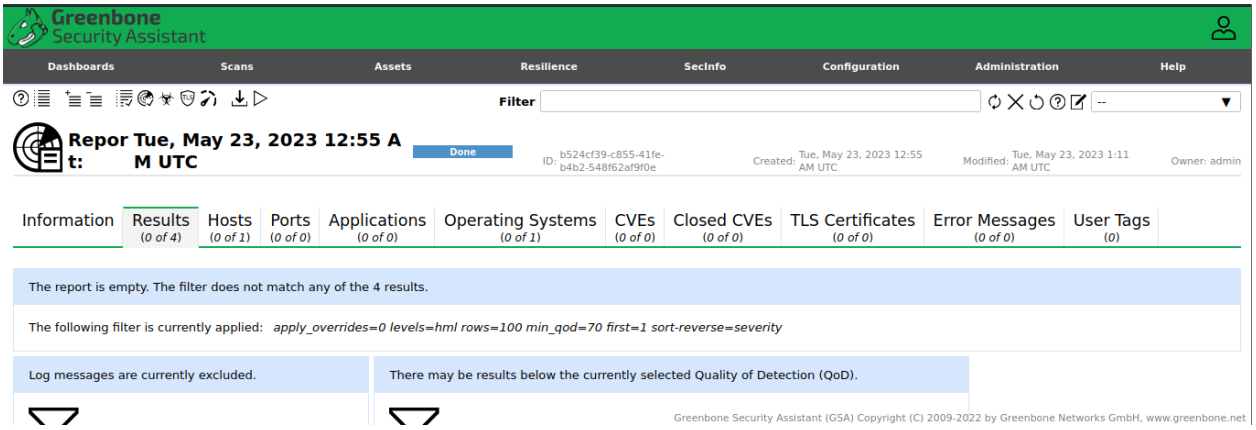
Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.
Tue, May 23, 2023 12:55 AM UTC	Done	Immediate scan of IP 192.168.1.4	0.0 (Log)	0	0	0	4	0

Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

En el punto de acceso con la dirección IP 192.168.1.4, no se ha identificado una severidad solo se han registrado cuatro logs´s durante el escaneo, sin encontrar ningún falso positivo. Estos resultados indican que no existe ninguna presencia de vulnerabilidades en el punto de acceso.

Figura 63

Sub-apartado Reports - Soporte

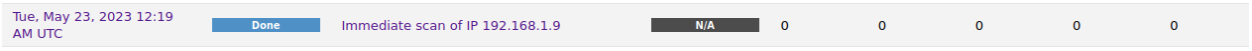


Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La herramienta no muestra ninguna vulnerabilidad debido a la ausencia de estas. Sin embargo, registra los logs importantes como se puede observar en el apartado "result" donde se indica que no se encontraron vulnerabilidades "0 of 4". Es importante destacar que los log´s mencionados no deben considerarse como vulnerabilidades. Con esto se puede afirmar que el punto de acceso tiene una seguridad buena.

Figura 64

Punto de Acceso AsisteCooper-Contabilidad

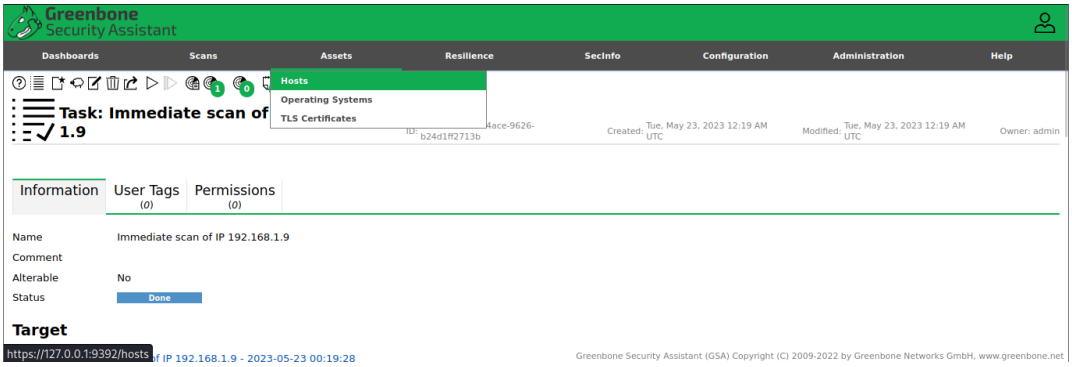


Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

En el punto de acceso con la dirección IP 192.168.1.9, no se ha identificado ninguna severidad ni se han registrado logs durante el escaneo realizado. Estos resultados indican que no existe presencia de vulnerabilidades en el punto de acceso y no se han registrado eventos relevantes durante el proceso de escaneo.

Figura 65

Sub-apartado Reports - Contabilidad



Nota: Extraído de la herramienta Greenbone. Elaborado por: Sandoval, M. (2023).

La herramienta no muestra ninguna vulnerabilidad debido a la ausencia de estas. Debido a que no se ha encontrado ni log´s ni vulnerabilidades la herramienta Greebone no despliega la interfaz con todos sus apartados. Con esta información se puede afirmar que el punto de acceso tiene una seguridad buena.

Conclusiones y Recomendaciones

10.1. Conclusiones

- Según el análisis realizado mediante la herramienta Vistumbler y el estándar de la IEEE para señal dbm, el rendimiento de señal de los cuatro puntos de acceso de la red de AsisteCooper es aceptable en general, el maximo dbm que se obtuvo en cada punto de acceso fue: AP Desarrollo -23dbm, AP D-Movil -16dbm, AP Soporte -74dbm y AP Contabilidad -64dbm. Esto indica que la infraestructura de red está proporcionando una cobertura adecuada y estable en las áreas cubiertas por estos puntos de acceso.
- A través del análisis realizado con Vistumbler, se ha identificado que el punto de acceso de contabilidad presenta fallas de hardware, lo que está afectando negativamente la potencia del equipo en esa ubicación específica. Esta situación indica una debilidad en la infraestructura de red en relación con ese punto en particular.
- Mediante el uso de la herramienta Greenbone se ha determinado la presencia de vulnerabilidades en dos de los cuatro puntos de acceso de la red de AsisteCooper, presentan un nivel de severidad medio. Si bien esto indica que la red presenta problemas de seguridad, es alentador destacar que la mayoría de las vulnerabilidades identificadas pueden ser mitigadas mediante las soluciones proporcionadas por la herramienta. Estas vulnerabilidades incluyen desactualización de algunos servicios y protocolos, así como malas configuraciones de los Puntos de Acceso. Lo cual podría ser peligroso

considerando que la empresa maneja información confidencial de clientes bancarios.

10.2. Recomendaciones

- Se recomienda que la empresa AsisteCooper tome acciones inmediatas para abordar las fallas de hardware identificadas en el punto de acceso de contabilidad, llevando una revisión del equipo y, de ser necesario, su remplazo.
- Se recomienda tomar acciones inmediatas para abordar las vulnerabilidades identificadas como la implementación de las soluciones propuestas por la herramienta Greenbone.
- Se recomienda que la empresa AsisteCooper realice análisis de estado de red con más frecuencia para garantizar un monitoreo continuo y una detección temprana de posibles fallas o vulnerabilidades.
- En trabajos futuros realizar pruebas de ping para comprobar la latencia de transmisión pudiendo identificar los problemas de rendimiento y encontrar los cuellos de botella mejorando asi el análisis de la red de internet a una empresa.

Bibliografía

Álvarez, A. (2020). *repositorio.ulima.* Obtenido de https://repositorio.ulima.edu.pe/handle/20.500.12724/10818

Andreu, F., Pellejero, I., & Lesta, A. (2006). *books.google.* Obtenido de https://books.google.cl/books?hl=es&lr=&id=k3JuVG2D9lMC&oi=fnd&pg=PA1&dq=Fundamentos+y+Aplicaciones+de+Seguridad+en+Redes+WLAN:+Fundamentos+y+Aplicaciones+de+Seguridad&ots=8Gub4sdXaN&sig=Jzzr58XLLCnTrLq-TLsMkx12Fww#v=onepage&q&f=false

Conejero, J. (2020). *Sociedad Chilena de Neumología* . Obtenido de https://www.neumologia-pediatrica.cl/index.php/NP/article/view/57

García, A. (2018). *repositorioinstitucionaluacm.* Obtenido de https://repositorioinstitucionaluacm.mx/jspui/bitstream/123456789/1117/3/Alcal%C3%A1%20Garc%C3%ADa%2C%20Magnolia_Mitigaci%C3%B3n%20de%20vulnerabilidades%20en%20una%20WLAN%20con%20la%20implementaci%C3%B3n%20de%20hardening_unlocked.pdf

García, J., Medina, C., & Muñoz, D. (2022). *riul.unanleon.* Obtenido de http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/9373/1/249736.pdf

González, A., & Zebadúa, A. d. (2011). *repositoriodigital.tuxtla.* Obtenido de http://repositoriodigital.tuxtla.tecnm.mx/xmlui/bitstream/handle/123456789/88/48241.pdf?sequence=1&isAllowed=y

IEEE. (2016). *IEEE S.A*. Obtenido de https://standards.ieee.org/ieee/802.11/7028/

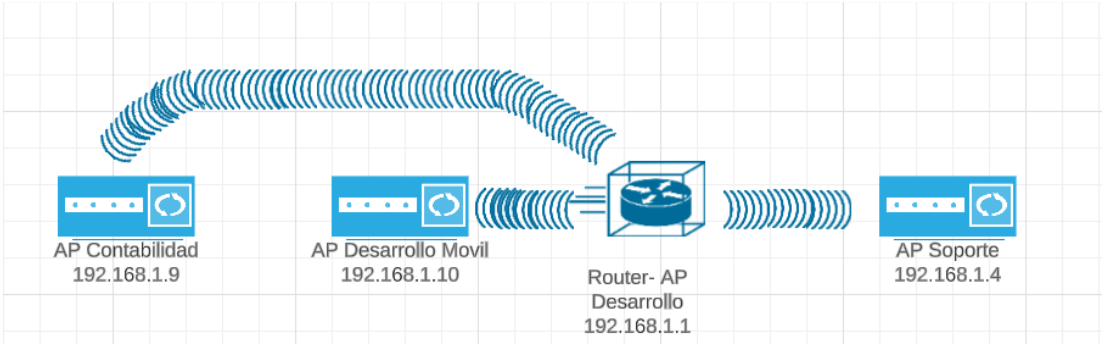
Páez, S. (2019). *repositorio.puce.* Obtenido de http://repositorio.puce.edu.ec/handle/22000/17060

Salzar, J. (2017). *Redes Inalambricas.* Obtenido de TechPedia: https://www.psm.fei.stuba.sk/pages/9/LM01_F_ES.pdf

Sanchez, J. (2012). *UV.MX.* Obtenido de https://www.uv.mx/iiesca/files/2012/12/redes2008-2.pdf

Anexos

Anexo A: Topología de la Red de Internet.



Anexo B: AP Calix 813G-2 Router

Anexo C: AP Netis WF 2411

Anexo D: AP TP-LINK AC1200


1200Mbps
2.4G 5.0G
tp-link