UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2022 – MAYO 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE LAS VULNERABILIDADES DE LA INFRAESTRUCTURA WIRELESS DEL GAD PARROQUIAL DE ANTONIO SOTOMAYOR

ESTUDIANTE:

WENDDY EVELIN BASURTO LÓPEZ

TUTOR:

ING. JOSÉ DANILO VILLARES PAZMIÑO, MG.

AÑO 2023

CONTENIDO

RESUMEN

Las redes inalámbricas hoy en día son muy utilizadas para establecer una conexión, pero también suele tener una desventaja ya que cualquier individuo teniendo conocimiento de cómo vulnerar la red podrá hacerlo con tal de estar dentro de la cobertura puede descomponer la seguridad de la red por eso suele ser un medio de comunicación inseguro que tiene precauciones.

El problema del GAD Parroquial de Antonio Sotomayor radica en que no tiene determinadas las vulnerabilidades a las que está expuesta la institución, y no cuenta con personal especializado en lo que es el sistema del software, para efectuar los mantenimientos.

La presente investigación busco determinar las vulnerabilidades a la red informática mediante la herramienta Nessus, con la cual se realizó un escaneo de red a la institución.

El tipo de metodología con el cual se realizó la investigación fue de tipo aplicada en conjunto con la metodología OMMTSS donde se utilizó la herramienta Nessus para realizar el escaneo de red.

Como resultados se determinaron las vulnerabilidades y amenazas a la que está expuesta la red y cuál era el nivel de impacto que tendría, se llegó a la conclusión que en la red informática del GAD Parroquial de Antonio Sotomayor existen varias vulnerabilidades ; por ende el sistema no está totalmente seguro, se recomendó implementar metodologías de hacking éticos, realizar capacitaciones al personal para que tengas más conocimientos sobre la importancia de recursos informáticos que tiene el GAD.

Palabras claves: vulnerabilidades, amenazas, red informática, seguridad.

PLANTEAMIENTO DEL PROBLEMA

Las redes inalámbricas son las más utilizadas en la actualidad , pero a veces tiene sus desventaja ya que cualquier usuario teniendo conocimiento de cómo entrar a la red podrá hacerlo con tal de estar dentro de la cobertura puede descomponer la seguridad de la red por eso suele ser un medio de comunicación inseguro que tiene precauciones. Los ataques a las redes informáticas de instituciones publica se dan por diferentes causas puede ser por extorciones de información, lo cual la institución sea afectada.

En el Ecuador existen varias instituciones públicas que no hacen uso de sistema de seguridad para asegurar sus bases de datos de cualquier tipo de amenaza informática, ya sea por el alto costo de la implementación de estos sistemas o no le dan importancia a dicha información. En otros casos existen instituciones que utilizan software gratuito, lo cual no son confiable a la integridad de la información.

El Gobierno Autónomo Descentralizado Parroquial Antonio Sotomayor está ubicado en la avenida 13 de enero y calle San Genaro, es una institución pública de autonomía política, administrativa y financiera y estará integrado por las siguientes funciones: Participación Ciudadana, Legislación y Fiscalización y Ejecutiva. Tiene como finalidad beneficiar a los a habitantes de la parroquia.

En este presente caso de estudio se plantea realizar un análisis a la red para poder detectar las vulnerabilidades que existen en el GAD, con el objetivo de perfeccionar los servicios y tener una red más segura y tenga menos propensa a ataques.

En lo mencionado anteriormente nos lleva a plantearnos la siguiente interrogante ¿Cómo el análisis de las vulnerabilidades de la infraestructura Wireless, ayudara en la seguridad de la información del GAD Parroquial de Antonio Sotomayor?

El problema del GAD Parroquial de Antonio Sotomayor es que no tienen determinadas las vulnerabilidades a las que se encuentras expuestas diariamente. En la actualizada el software no cuentan con un administrador de software, que realice los mantenimientos del mismo, ocasionando retrasos en los procesos administrativos del GAD.

La información guarda corre el riesgo de no ser confidencial. Debido a que la persona encargada no es parte del GAD y este proceso lo realiza eventual. Así se ven afectados por el riesgo de robo, acceso a la información o corrupción de datos personales, entre otros.

JUSTIFICACIÓN

Hoy en día la tecnología inalámbrica ha convertido en un componente crítico, la información sobre vulnerabilidades se va liberando día a día, esto es un riesgo si bien es cierto esto no puede ser eliminado en totalidad, pero si se lo puede disminuir. Por eso es necesario aplicar métodos de seguridad a las redes inalámbricas para evitar ciertas falencias.

Es importante destacar los beneficios que tendrá tanto para la institución como para las personas de la parroquia porque ayuda a identificar las vulnerabilidades, se podrá tomar medidas de seguridad para prevenir posibles ataques informáticos, lo que garantiza la seguridad de la información y las protecciones de los datos personales de los usuarios. Además, también permitirá mejorar la eficiencia de la red inalámbrica y optimizará su rendimiento lo que mejorará la calidad de servicio para los usuarios.

El presente análisis tiene relevancia ya que se trata de una institución pública que maneja información sensible y confidencial. Por lo cual, la protección de la información es de suma importancia para determinar la privacidad de los usuarios y prevenir posibles ataques informáticos. En la actualidad muchas de las actividades de la institución dependen del correcto funcionamiento de la infraestructura wireless, por lo que su vulnerabilidad puede tener consecuencias para el normal desarrollo de sus actividades.

En el presente caso de estudio, se caracteriza por ser factible en los términos metodológicos y técnicos. Existen diversas herramientas que permiten llevar un análisis de vulnerabilidades de manera efectiva y eficiente. Por lo que se realizó un escaneo de vulnerabilidades a la red mediante una herramienta open sourse, para determinar las vulnerabilidades de la red y realizar las observaciones en cuanto al resultado del análisis.

OBJETIVOS

Objetivo general:

Analizar las vulnerabilidades de la infraestructura Wireless del GAD Parroquial de Antonio Sotomayor.

Objetivos específicos:

- Determinar los referentes teóricos sobre la seguridad en infraestructura Wireless del GAD Parroquial de Antonio Sotomayor.
- Buscar, analizar e interpretar la información de campo relacionada con la seguridad de la infraestructura Wireless del GAD parroquial.
- Formular una propuesta de solución a las debilidades encontradas en la infraestructura Wireless de del GAD parroquial de Antonio Sotomayor.

LÍNEAS DE INVESTIGACIÒN

El presente caso de estudio está enfocado en la línea de investigación sistema de información y comunicación, emprendimiento e innovación, sujeta por la sublínea de investigación de redes y tecnologías inteligentes de software y hardware. Comprendiendo así, el proceso de recolección y gestión de información con la finalidad que la investigación efectué la política de supervisión de la institución.

Esta investigación se relaciona con la línea de investigación ya que trata sobre sistemas de información se refiere a la manipulación o administración de información mediante dispositivos computacionales. También a estos sistemas se los suele considerar seguros siempre y cuando mantenga la disponibilidad e integridad de la información.

En cuanto a la sublínea de investigación el cual rige el caso de estudio, en relación con las redes informáticas podemos recalcar que estas estructuras tienen como objetivo transportar datos, compartir recursos e información y ofrecer un servicio. Esto procesos son posible gracias a los equipos que se encuentra conectados. Es necesario que la información que se transporta por medio de la red sea siempre respaldada ya que es posible que la red sea vulnerable en ciertas áreas.

MARCO CONCEPTUAL

El Gobierno Autónomo Descentralizado Parroquial correspondiente a la Parroquia Antonio Sotomayor del Cantón Vinces Provincia de Los Ríos. Se encuentra ubicada en la avenida 13 de enero y calle San Genaro, La red que se encuentra en el GAD es una red LAN, en el cual se guarda toda la información.

Existen varias partes que se pueden ver afectada la integridad y disponibilidad de los datos y por esto se considera importante aplicar los protocolos de seguridad por motivo que cada vez aumentan los ataques de red.

Sistema de información

Un sistema de información (SI) es un conjunto de herramientas que tienen como objetivo la gestión eficiente de datos e información para su fácil acceso y procesamiento. Un SI está conformado por diversos recursos interrelacionados que se organizan de manera apropiada en función de la finalidad del sistema, que puede ser desde la recolección de información personal hasta el procesamiento de estadísticas o la gestión de archivos (editorial, 2021).

Los sistemas de información son un conjunto organizado de software, hardware, datos, procesos y personas que utilizan para recopilar, procesar, almacenar y distribuir la información. Son importante en organizaciones porque son los que ayudan a reducir los procesos, mejora la eficiencia y la calidad de servicio y mejora la colaboración de los miembros de la organización.

Red inalámbrica

Una red inalámbrica es un tipo de red de computadoras que utiliza tecnología inalámbrica, como Wi-Fi, para conectar dispositivos a la red sin la necesidad de cables físicos. En una red inalámbrica, los dispositivos se conectan mediante señales de radiofrecuencia que permiten la transmisión de datos y la comunicación entre ellos. Las redes inalámbricas son comunes en hogares, empresas, y lugares públicos como cafeterías, aeropuertos y hoteles, entre otros. Las redes inalámbricas ofrecen una mayor movilidad y flexibilidad, ya que los dispositivos pueden conectarse a la red desde cualquier lugar dentro del alcance de la señal inalámbrica.

Tipos de redes informáticas

Los tipos de redes informáticas menciona el autor (Implika, 2021)que se clasifican en:

Red de área personal (PAN): Se refiere a una red que se compone de dispositivos de una sola persona y permite la trasferencia de datos de manera rápida y fácil entre ellos sin la necesidad de cables o conexiones físicas.

Red inalámbrica de área personal (WPAN): es una red de corto alcance que permite la conexión y la transferencia de datos entre dispositivos electrónicos en una zona cercana a una persona.

Red de área local (LAN): Esta red es utilizada para conectar dispositivos dentro del área geográfica limitada, como un edificio u oficina, con el objetivo de compartir recursos y datos entre ellos.

Red de área local inalámbrica (WLAN): Es una red de área local que utiliza tecnología inalámbrica para conectar dispositivos electrónicos en el área geográfica limitada, permitiendo a

los usuarios accedan a recursos compartidos de manera inalámbrica desde cualquier lugar dentro de la misma red.

Red de área de campus (CAN): Es una red de comunicación de datos de alta velocidad utilizada en la industria automotriz, sistemas de control industrial y aplicaciones de automatización, caracterizada por su alta velocidad, capacidad de transmisión de datos en tiempo real, y su robustez para trabajar en ambientes ruidosos y hostiles.

Red de área metropolitana (MAN): Es una red de comunicaciones de datos que abarca una extensión geográfica mayor que la LAN y menor que la WAN, con una velocidad de transmisión de datos más alta que la WAN y menor que la LAN. Es adecuada para conectar redes LAN de diferentes edificios o proporcionar conectividad de alta velocidad a través de una región geográfica determinada.

Red de área amplia (WAN): Es una red de comunicación de datos que cubre una amplia área geográfica y conecta diferentes redes LAN o MAN a través de tecnologías de transmisión de datos como líneas telefónicas, fibra óptica y satélites. Se utiliza para proporcionar servicios de comunicación a larga distancia y para conectar diferentes oficinas y sucursales en diferentes ubicaciones geográficas.

Red LAN lógica (VLAN): Es una red de área local que permite a los administradores de red crear redes lógicas separadas dentro de una red física. Los dispositivos se agrupan en función de su ubicación lógica y no física, lo que permite un mayor control del tráfico de la red y una mejora en la seguridad. La implementación se realiza mediante el uso de switches de red que permiten la configuración de puertos y VLANs.

Infraestructura de red

La infraestructura de red hace referencia a todos los recursos que forman parte de una red y que permiten su conectividad, gestión, operaciones y comunicación, ya sea internamente o en Internet. Se compone de una combinación de hardware y software, dispositivos y sistemas, que posibilitan la comunicación y la informática entre usuarios, servicios, aplicaciones y procesos. Todo lo que integra la red, desde los servidores hasta los routers inalámbricos, se unen para conformar la infraestructura de red de un sistema. Gracias a ella, se puede lograr una comunicación y un servicio eficiente entre los distintos elementos que integran la red, como los usuarios, dispositivos, aplicaciones y servicios, entre otros (TecnologiaMix, 2021).

La infraestructura de red es fundamental en el correcto funcionamiento de la red informática. Es importante que la infraestructura sea confiable, segura y escalable para satisfacer las necesidades de los usuarios y las organizaciones que la utilizan. La implementación apropiada de la infraestructura de red puede mejorar su eficiencia y productividad de la organización, así como la calidad y velocidad de la comunicación y la transferencia de información.

Router

Un router es un componente de hardware que posibilita la interconexión de computadoras en una red. Este dispositivo opera en la capa 3 del modelo de referencia OSI, lo que le permite la interconexión y el intercambio de datos entre varias redes o computadoras que compartan la misma conexión a Internet. Los routers emplean un protocolo de enrutamiento que les permite comunicarse con otros dispositivos similares y compartir información para determinar la ruta más eficiente y apropiada para enviar los datos a su destino. Un enrutador típico opera en el plano de control (en el que el dispositivo recibe información sobre la salida más eficiente para un paquete

especifico de datos) y en el plano directo (en este plano, el dispositivo es responsable de enviar el paquete de datos recibido a otra interfaz) (Bembibre, 2023).

Switch

Un switch es un dispositivo que se utiliza para conectar varios elementos en una red. En un hogar, puede usarse para conectar una impresora, una computadora, una consola de videojuegos o un televisor. En una oficina, un switch puede servir como un puente para conectar cientos de equipos de escritorio. Hay switches básicos que tienen cuatro puertos Ethernet, pero también hay switches más avanzados que tienen cientos de puertos y funciones de gestión de red avanzadas. El objetivo principal del switch es permitir que cada dispositivo conectado en la red envíe mensajes o archivos a un dispositivo específico. Para lograr esto, el switch utiliza la dirección MAC de la tarjeta de red del dispositivo, que es como una matrícula única que identifica cada dispositivo en la red. La dirección MAC es una cadena alfanumérica que tiene un formato específico, como por ejemplo "00:1e:c2:9e:28:6b". Además, la información que se transmite a través del switch se envía en un formato conocido como "frame" (CABRERA, 2019).

Tipología de red

La topología de red se refiere al diseño físico o lógico de una red que permite el intercambio de datos. Se trata de la forma en que se han conectado las diferentes partes de una red. Es importante tener en cuenta que una red se define como un conjunto de nodos interconectados, donde cada nodo es un punto en el que una curva se cruza consigo misma. El tipo de nodo en particular dependerá del tipo de red que se esté utilizando. (Luis, 2019).

Tipos de topología de red

Los tipos de topología según el autor (Luis, 2019) menciona que los tipos de topología de red hacen alusión a la topología lógica mediante la cual se presentan las interconexiones entre los nodos de la red. Es una referencia a una forma geométrica o una forma lógica en la que se distribuyen las estaciones de trabajo y cada uno de los medios que las conectan.

- Topología en anillo
- Topología de anillo doble
- Topología de árbol
- Topología de bus
- Topología de estrella
- Topología de malla
- Topología híbrida

Topología en anillo

Es un tipo de estructura de red donde cada equipo estará conectado a otros dos, y así van formando un anillo cerrado o un círculo. Los datos se transmiten en una sola dirección a través del anillo, cada dispositivo en el anillo recibe los datos y los retransmite al siguiente dispositivo hasta que llegan al último. Esta arquitectura de red es muy confiable ya que si un dispositivo falla, los demás dispositivos pueden continuar funcionando sucesivamente.

Topología de anillo doble

También llamada anillo dual, es una topología en donde se utilizan dos anillos conectados por dispositivos, lo que proporciona una ruta de comunicación redundante en caso de que falla en uno de los anillos. Una ventaja de a topología de anillo doble es su alta confiabilidad y tolerancias a fallas, ya que, si un anillo se rompe, los paquetes pueden ser enviados a través de otro anillo sin la interrupción en la comunicación. Esta topología puede ser más compleja y costosa de implementar que otras topologías de red.

Topología de árbol

Esta topología de red se basa en una estructura jerárquica, en los nodos de red están organizados en una estructura de árbol. En esta topología los nodos se conectan en una estructura ramificada en la que cada nodo puede tener varios nodos hijos, y a su vez cada uno de estos nodos hijos pueden tener sus propios nodos hijos y así sucesivamente formando una estructura jerárquica. Los nodos se conectan a través de un enlace de punto a punto, lo que significa que cada nodo está conectado directamente a un nodo padre y a varios nodos hijos. Esta estructura jerárquica permite la administración y gestión más sencillas de la red ya que se puede controlar y configurar de manera más eficiente. Una desventaja de esta topología es que en caso de falla de un nodo central o de la línea principal, toda la red puede verse afectada.

Topología de bus

Esta topología de red es la que los nodos de la red se conectan a través de un único cable central llamado “bus” o “trunk”. En esta topología cada nodo está conectado al bus mediante un conector o una interfaz y comparten la misma línea de comunicación para enviar y recibir datos. La comunicación se realiza mediante un sistema de transmisión unidireccional lo que significa que solo un nodo se puede transmitir datos a la vez, mientas que los otros nodos escuchan la señal en

espera del turno. Si dos nodos intentan transmitir al mismo tiempo se reduce la colisión de datos. Lo que provoca la pérdida de información y la necesidad de retransmitir los datos.

Topología de estrella

En esta topología los dispositivos se conectan directamente al nodo central formando una estructura de forma de estrella. Si un dispositivo desea comunicarse con otros dispositivos, la información primero se envía al nodo central y luego se transmite al dispositivo de destino. La topología de red tiene muchas ventajas, pero también tiene muchas desventajas, si el nodo central falla, toda la red debe de verse afectada. Esta topología requiere más cables y conexiones que otras configuraciones de red, lo que puede ser más costoso y más fácil de implementar.

Topología de malla

Es un tipo de tipología de red en la que cada dispositivo de red está conectado directamente a todos los demás dispositivos. En esta red de malla, cada dispositivo actúa como punto de enrutamiento para el tráfico de datos lo que significa que los datos pueden llegar al final de varias formas diferentes. Esta topología es escalable y tolerantes a fallos. Si uno de los dispositivos falla, los datos todavía pueden encontrar una ruta alternativa para llegar al final. La topología de malla es muy resistente a interrupciones ya que la eliminación de un nodo no afecta al resto de red.

Topología hibrida

Es una combinación de dos o más tipos de topología de red, se utilizan varios tipos de topología para conectar diferentes segmentos de la red, lo que permite aprovechar las ventajas y disminuir las desventajas. Se puede utilizar la topología de árbol para conectar diferente subred puede estar configurada con la topología de estrella o de bus. La topología hibrida proporciona una

mayor flexibilidad y escalabilidad con comparación con una sola topología de red. También suele ser más resistente a los fallos, ya que si una falla en el segmento de la red no afectara a toda la red. Sin embargo, la topología hibrida puede ser más compleja de configurar y mantener una topología única.

Vulnerabilidades informáticas

Una vulnerabilidad de computadora se refiere a cualquier tipo de defecto o equivocación encontrada en el software o hardware que permite a un atacante o hacker dañar la integridad y confidencialidad de los datos que se manejan en un sistema. Estos errores pueden ser el resultado de un diseño inadecuado, una mala configuración o prácticas incorrectas en el proceso. La existencia de vulnerabilidades es una de las principales causas de posibles ataques informáticos en una empresa, lo que enfatiza la importancia de la ciberseguridad. (Chavez, 2023).

Según lo antes mencionado sobre vulnerabilidades informáticas (Castillo, 2020) dice que Una vulnerabilidad se define como una falla o debilidad existente en un sistema operativo, software o sistema que posibilita a un atacante el acceso no autorizado o manipulación de los datos y aplicaciones, violando así la privacidad, integridad, disponibilidad, control de acceso y coherencia del sistema. Estas debilidades se originan por errores en el diseño del software, aunque también pueden ser producto de las limitaciones inherentes a la tecnología para la cual fue creado.

Amenazas

Según (Quiroa, 2020) “Se considera una amenaza empresarial a cualquier factor proveniente del entorno externo de una empresa que pueda tener un efecto negativo en su progreso y expansión, llegando incluso a poner en peligro su permanencia en el mercado”.

Amenazas se refieren a cualquier evento o acción malintencionada que pueda comprometer la seguridad de los sistemas, redes, datos y dispositivos informáticos. Estas amenazas pueden ser llevadas a cabo por personas malintencionadas, como hacker, crackers o ciberdelincuentes o pueden ser causadas por errores humanos o por fallos del software o hardware. Algunos ejemplos de amenazas comunes como: virus informáticos, malware, spyware, phishing, ataque de denegación de servicio (DDoS), ransomware, ataques de ingeniería social, robo de identidad, etc.

Seguridad informática

La seguridad informática también llamada ciberseguridad se refiere a la protección de la información es un conjunto de medidas que se enfocan en resguardar la integridad de los datos y su procesamiento, evitando que sean manipulados o accedidos por personas no autorizadas. Su objetivo principal es asegurar la protección tanto de los equipos tecnológicos como de los datos, para prevenir cualquier tipo de daño o amenaza originada por terceros. (UNIR, 2021).

La seguridad informática se refiere a las prácticas y medidas para proteger los sistemas, redes, datos de una organización contra amenazas de seguridad como el acceso no autorizado, la divulgación de información, robo de datos.

Las áreas que componen la seguridad son las siguientes:

Confidencialidad: Es aquella que solo los usuarios que tienen autorización pueden acceder a los recurso, datos o información.

Integridad: Es aquella que solo los usuarios autorizados pueden modificar los datos cuando sean necesario.

Disponibilidad: Es la que los datos deben de estar disponible para cuando los usuarios necesiten de ellos.

Autenticación: Es la que los datos comuniquen lo que el usuario quiera que comuniquen y que sean auténticos.

Open Source

Según (Fuente, 2021) dice que open source o también denominado código abierto es un modelo de software que se basa en la colaboración abierta. Un programa que puede resultar muy favorable como lo son los diferentes tipos de erp para las empresas, siempre y cuando tengamos claras las diferencias entre crm y erp.

Se refiere a un código de programación diseñado con el propósito de ser accesible al público, permitiéndoles ver, modificar y distribuir dicho código de la manera que más les convenga. Este tipo de software ofrece una serie de características y beneficios únicos, ya que los desarrolladores pueden acceder al código fuente de una aplicación específica, leerlo y modificarlo para mejorarlo, añadir nuevas funcionalidades y solucionar cualquier problema que se encuentre. Como resultado, el programa compilado final estará mejor diseñado que la versión original creada por el programador.

Análisis de vulnerabilidades

Las herramientas de gestión y análisis de vulnerabilidades pretenden obtener una visión de todas las partes del sistema que pueden estar afectadas por una o varias vulnerabilidades, cuyo proceso consiste en identificarlas, evaluar su impacto y corregirlas. Existen multitud de herramientas, como pueden ser Nmap, Nessus o Qualys (POSTIGO PALACIOS, 2020).

El análisis de vulnerabilidades es el proceso de identificación y evaluación de las debilidades o vulnerabilidades en los sistemas, aplicaciones, redes o infraestructura de una organización que podría ser explotado por un atacante para comprender la seguridad informática. Puede ser llevado a cabo mediante pruebas manuales o automatizadas, con el objetivo de identificar las debilidades en la seguridad del sistema, en este proceso incluye el escaneo de red, la evaluación de las configuraciones de seguridad, el análisis del código fuente entre otros. Este análisis es una parte importante de la gestión de la seguridad ya que ayuda a las organizaciones a identificar y reducir los riesgos de seguridad y mantener la confidencialidad, integridad y disponibilidad de la información.

Escáner de vulnerabilidades

Según menciona el autor (Mercado, 2023) Los escáneres de vulnerabilidades son herramientas que pueden automatizar la auditoría de seguridad y desempeñar un papel importante en la protección de su sistema de tecnología de la información. Estas herramientas pueden analizar su red y sitios web en busca de miles de posibles riesgos de seguridad y generar una lista de prioridades de aquellos que deben ser corregidos. Además, los escáneres describen las vulnerabilidades encontradas y brindan pasos sobre cómo remediarlas.

El escáner de vulnerabilidades es una herramienta de seguridad informática que se utiliza para identificar debilidades o vulnerabilidades en sistemas de redes y otros componentes de tecnología de la información. Funciona mediante un sin número de pruebas automatizada en los sistemas, en busca de vulnerabilidades conocidas o debilidades que pueden ser explotadas por atacantes. Los resultados de estas pruebas se presentan en informes que detallan las debilidades encontradas y las medidas recomendadas para solucionarlas. Los escáneres de vulnerabilidades

pueden ser utilizados para la automatizar la detección de vulnerabilidades y reducir el tiempo y el costo asociados a la evaluación de la seguridad informática.

Escáner de vulnerabilidades Nessus

Nessus es un programa que escanea vulnerabilidades para todos los sistemas operativos. Consiste en un demonio Nessus que realiza el escaneo del sistema operativo objetivo, y Nessus el cliente que muestra el progreso e informa de todo lo que va encontrando en los diferentes escaneos. Nessus puede ser ejecutado tanto a través de comandos de consola como mediante una interfaz gráfica de usuario. El escaneo de puertos es lo primero que se suele hacer en un pentesting, por lo que Nessus comienza por realizar un escaneo de puertos utilizando la potencia de Nmap para ello, aunque también cuenta con su propio escáner de puertos abiertos. Además, esta herramienta permite exportar los resultados del escaneo en diferentes formatos, como texto plano, XML, HTML y LaTeX, y toda la información se almacena en una base de datos de "conocimiento" para futuras revisiones. Actualmente, Nessus tiene una versión gratuita con limitaciones y una versión de pago mucho más completa con soporte de la empresa que lo respalda. (Luz, 2022).

El programa Nessus Essentials puede ser instalado en diferentes sistemas operativos como Windows, macOS y varias distribuciones de Linux/Unix. Tiene una interfaz gráfica de usuario web, donde se pueden visualizar fácilmente los tipos de análisis incluidos, tales como el descubrimiento de hosts y el análisis de vulnerabilidades. Aunque algunos tipos de escaneo están restringidos por la licencia, se pueden ver los que están disponibles en la edición profesional, como el escaneo de vulnerabilidades para dispositivos móviles y el escaneo de cumplimiento. (Mercado, 2023).

Nmap

Nmap es una herramienta de escaneo de redes que se utiliza para descubrir hosts y servicios en una red, así como para identificar puertos abiertos y servicios que se ejecutan en esos puertos. Nmap es una herramienta muy poderosa que puede ayudar a los administradores de red y a los expertos en seguridad a identificar vulnerabilidades en una red y a protegerla contra posibles ataques.

Descubrir hosts activos en una red: Nmap puede identificar los dispositivos activos en una red, lo que puede ser útil para los administradores de red para asegurarse de que no haya dispositivos no autorizados o inactivos que estén consumiendo recursos de la red.

Identificar puertos abiertos: Nmap puede descubrir puertos abiertos en un dispositivo, lo que puede ayudar a los administradores de red a identificar qué servicios están en ejecución y a asegurarse de que solo se ejecuten los servicios necesarios.

Identificar el sistema operativo: Nmap puede determinar el sistema operativo que se ejecuta en un dispositivo, lo que puede ser útil para identificar posibles vulnerabilidades específicas del sistema operativo.

Analizar la seguridad de la red: Nmap puede utilizarse para evaluar la seguridad de una red, identificando posibles puntos débiles y vulnerabilidades que podrían ser explotadas por un atacante.

Kali Linux

Kali Linux se utiliza comúnmente en entornos de pruebas de seguridad y en el ámbito académico para enseñar sobre seguridad informática. También se utiliza por profesionales de la

seguridad informática y hackers éticos para realizar pruebas de penetración en sistemas y redes de seguridad, con el objetivo de identificar y corregir vulnerabilidades antes de que sean explotadas por atacantes malintencionados.

Metodología OSSTMM

La OSSTMM es una norma profesional para realizar pruebas de seguridad en cualquier entorno, ya sea desde fuera o dentro de la organización. Esta norma incluye pautas de acción, ética profesional, legislación sobre pruebas de seguridad y un conjunto completo de pruebas. El enfoque principal de esta metodología es evaluar y ejecutar las pruebas aplicables hasta obtener los resultados deseados dentro de un plazo determinado. Solo de esta manera, el tester habrá cumplido con el modelo OSSTMM y su informe será considerado lo suficientemente exhaustivo. Esta metodología propone varios tipos de análisis de seguridad, y para fines del proyecto, se asemeja a un análisis de vulnerabilidades. (Ovallos-Ovallos & Rico-Bautista, 2020)

MARCO METODOLÓGICO

El tipo de investigación que se aplicó en el presente caso de estudio es la investigación aplicada, ya que está orientada a resolver problemas concretos y prácticos de la sociedad o de la institución. La investigación aplicada permite solucionar problemas reales no ficticios.

En la investigación se empleó la metodología OSSTMM, que es una guía utilizada para pruebas de seguridad y es mantenida por el instituto de Seguridad y Metodologías Abiertas (ISECOM). Para llevar a cabo esta metodología se utilizó la herramienta de escaneo de vulnerabilidades de código abierto Nessus y Nmap, con el objetivo de identificar las vulnerabilidades, ver los puertos que están abiertos y los dispositivos que se encuentran conectados en la red.

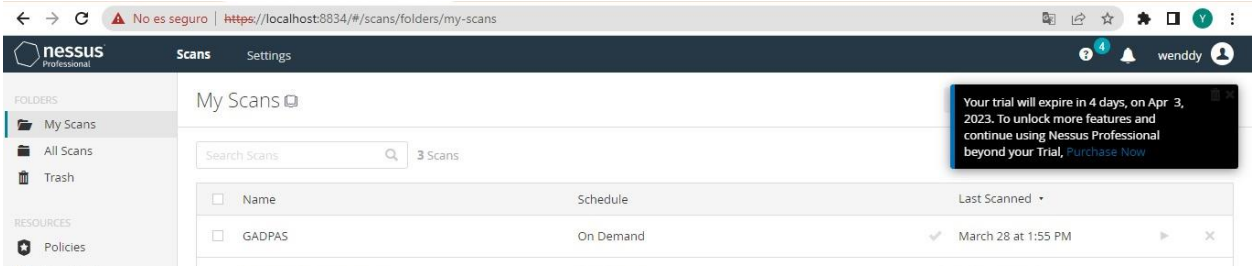
Técnicas e instrumentos que se utilizó en el presente caso de estudio, para llevar a cabo esta investigación fue la revisión documental de la información proporciona en los sitios web, libros para la recopilación de información y también se realizó una entrevista al secretario que utiliza la red dentro del GAD para indagar sobre los fallos que existen en la red.

RESULTADOS

Para establecer los resultados del estudio de caso se realiza el proceso de escaneo de red informática para determinar las vulnerabilidades con la herramienta Nessus, la cual nos permite realizar un escaneo de toda la red mostrándonos las vulnerabilidades para prevenir posibles ataques informáticos.

Una vez realizada la configuración correspondiente continuamos con el siguiente paso ejecutar el escaneo de la red como se muestra en la Figura 1. El escaneo de vulnerabilidades en la red informática del GAD Parroquial de Antonio Sotomayor, fue realizado el día 28 de Marzo a las 13:55 pm y tuvo una duración de 8 minutos.

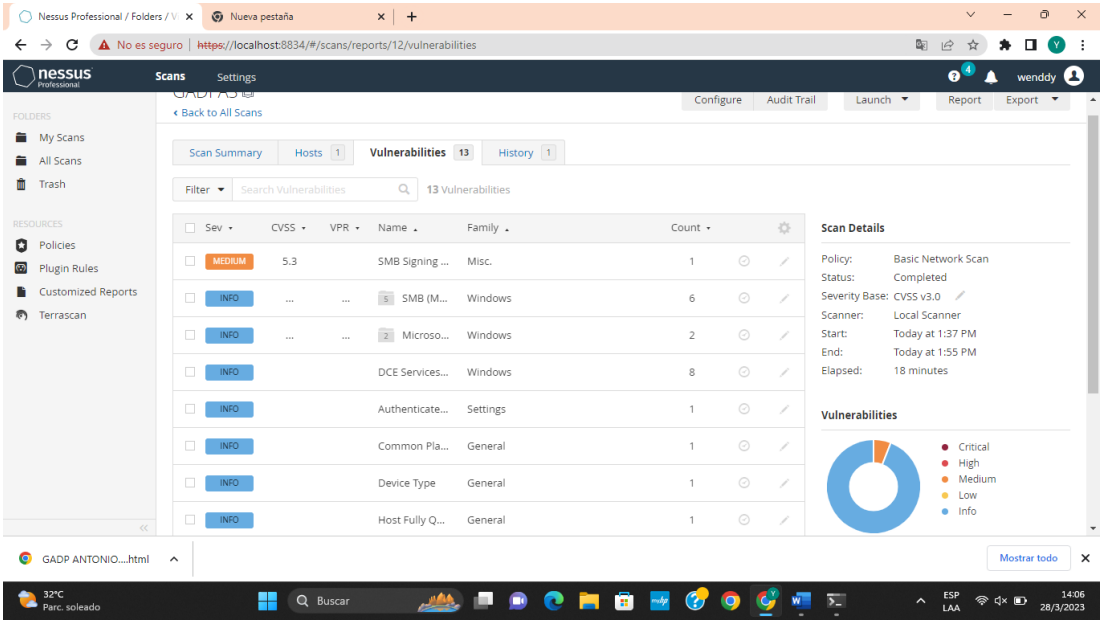
Figura 1 Inicio del Escaneó en Nessus



Fuente: (Wenddy Evelin Basurto López, 2023)

Terminado el escaneo de red fue posible observar y evidenciar las vulnerabilidades y amenazas. Nessus nos muestra en la figura 2 de manera general.

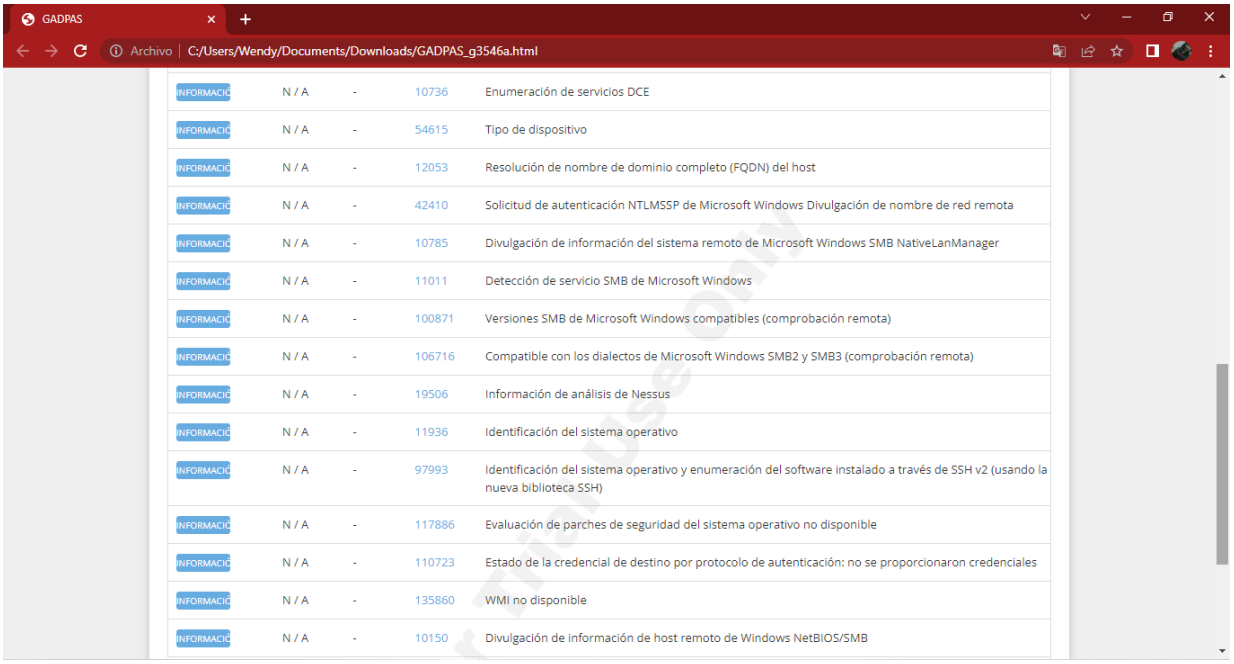
Figura 2 Resultados del escaneo



Fuente: (Wenddy Evelin Basurto López, 2023)

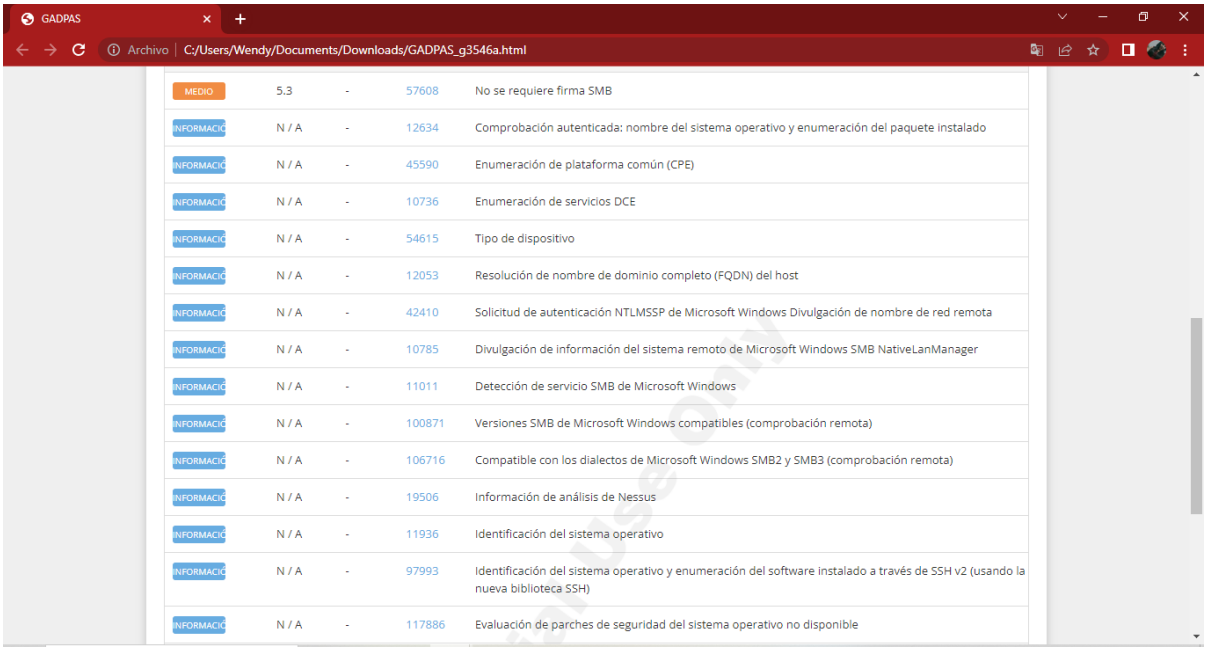
La herramienta Nessus también nos muestra un listado de las debilidades encontradas a través del análisis como lo muestra en la figura 3 y 4.

Figura 3 Lista de vulnerabilidades



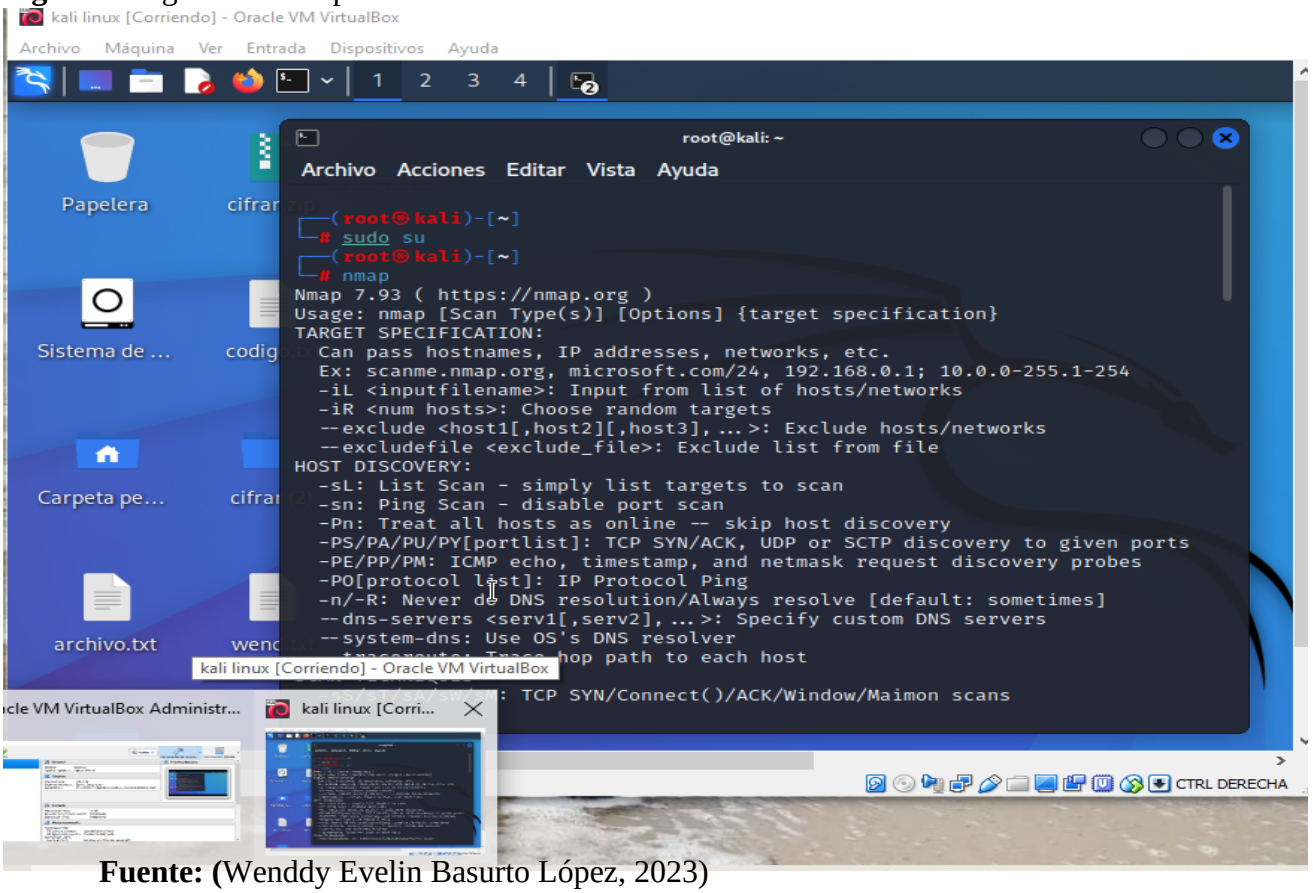
Fuente: (Wenddy Evelin Basurto López, 2023)

Figura 4 Lista de vulnerabilidades



Fuente: (Wenddy Evelin Basurto López, 2023)

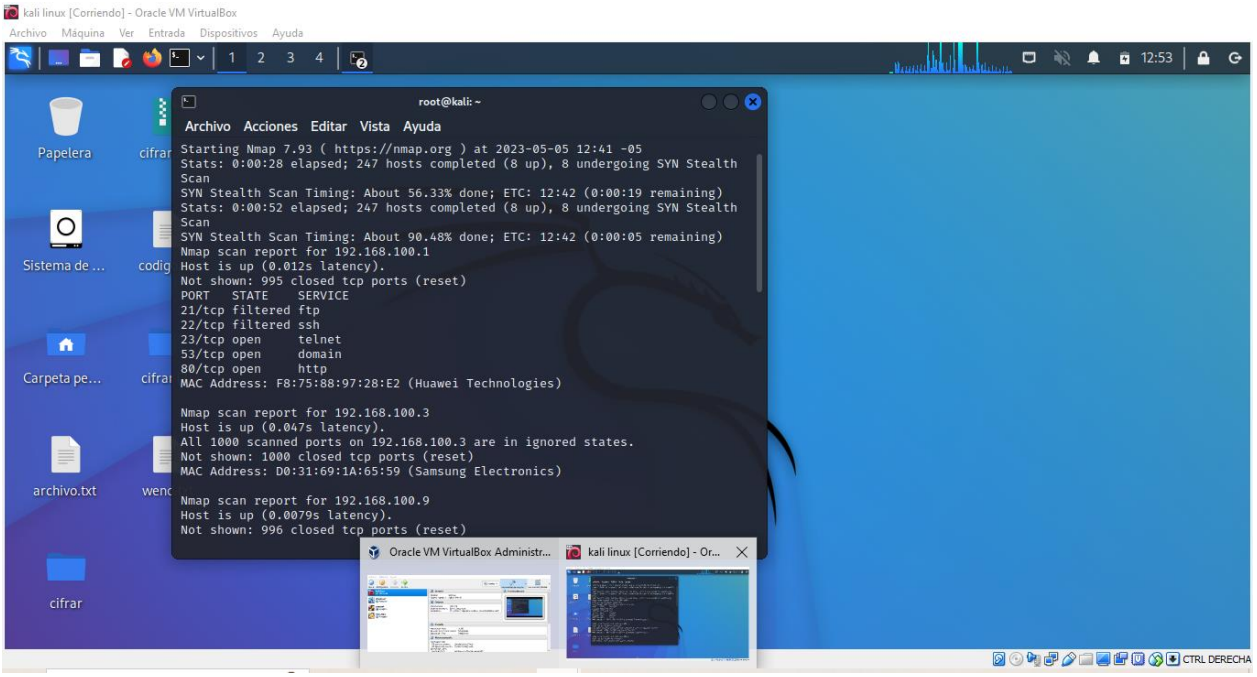
Figura 5 Ingresar a Nmap



Fuente: (Wenddy Evelin Basurto López, 2023)

También se realizó la herramienta Nmap para realizar un escaneo a los puertos de la red inalámbrica como vemos en la figura 6.

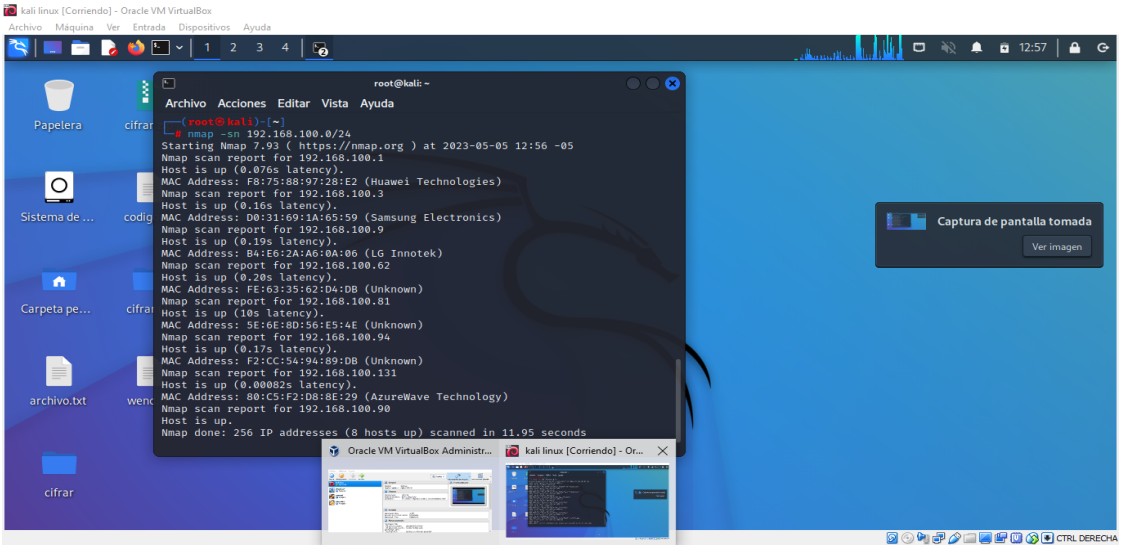
Figura 6 Puertos abiertos en la red inalambrica



Fuente: (Wenddy Evelin Basurto López, 2023)

En Nmap podemos ver los dispositivos que están conectados en la red inalámbrica como vemos en la figura 7.

Figura 7 Dispositivos conectados



Fuente: (Wenddy Evelin Basurto López, 2023)

DISCUSIÓN DE RESULTADOS

Como se pudo observar en las ilustraciones referentes a los resultados, la herramienta Nessus a través del proceso de escaneo nos mostró vulnerabilidades de impacto, medio. Se identificó un total de 13 vulnerabilidades que se dividen en 1 medio y 13 de información mediante las cuales se puedo determinar que los sistemas informáticos que utiliza actualmente el GAD de Antonio Sotomayor tienen pocas falencias lo cual reduce los niveles de seguridad.

La debilidad encontrada de medio es que no se requiere firma SMB quiere decir que no es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de intermedio contra el servidor SMB.

Encontramos una vulnerabilidad de información de detección de servicio de Microsoft Windows es el servicio remoto comprende el protocolo CIFS (Common Internet File System) o Server Message Block (SMB), que se utiliza para proporcionar acceso compartido a archivos, impresoras, etc. entre nodos de una red.

Otra vulnerabilidad es Enumeración de servicios DCE, al enviar una solicitud de búsqueda al mapeador de puertos (TCP 135 o EPmapper PIPE), fue posible enumerar los servicios del entorno de computación distribuida (DCE) que se ejecutan en el puerto remoto. Usando esta información, es posible conectarse y vincularse a cada servicio enviando una solicitud RPC al puerto/tubería remoto.

CONCLUSIONES

Determinar los referentes teóricos para la seguridad de la infraestructura Wireless es un paso importante para analizar las vulnerabilidades de la infraestructura Wireless y finalmente implementar medidas eficientes para garantizar la seguridad de la red.

La información de campo recopilada también ayuda a evaluar las políticas y procedimientos de seguridad existentes, identificar áreas de mejora y sugerir soluciones para mejorar la seguridad. Al analizar y evaluar la información se puede identificar posibles vulnerabilidades y brechas de seguridad en la infraestructura Wireless del GAD Parroquial Antonio Sotomayor.

Una vez que se identifican las vulnerabilidades potenciales en una red inalámbrica, se debe desarrollar una solución que incluya medidas específicas para mitigar los riesgos de seguridad y garantizar la integridad y confidencialidad de la información transmitida a través dela red inalámbrica.

RECOMENDACIONES

Se recomienda realizar una revisión exhaustiva de las referencias teóricas identificadas para garantizar que se cubran todos los aspectos necesarios para el análisis de vulnerabilidad de lainfraestructura Wireless.

Se deben realizar inspecciones y evaluaciones en el sitio para recopilar información relevante y analizarla para identificar posibles vulnerabilidades y brechas de seguridad en la infraestructura Wireless GAD de la parroquia. En base a la información obtenida, se puede ofrecersoluciones para mejorar la seguridad.

El punto central estará en el desarrollo de soluciones específicas para mitigar los riesgos de seguridad en la infraestructura inalámbrica del GAD Parroquial Antonio Sotomayor. Además, se deben identificar las posibles vulnerabilidades de la red Wireless y se debe desarrollar un plan de acción que incluya pasos específicos para abordar cada vulnerabilidad. Es importante considerarsoluciones de implementación y viables, teniendo en cuenta los recursos disponibles y laslimitaciones técnicas.

REFERENCIAS

Bembibre, V. (Febrero de 2023). Obtenido de https://www.definicionabc.com/tecnologia/router.php#cerrar

CABRERA, J. (27 de Diciembre de 2019). Obtenido de https://www.nobbot.com/que-es-un-switch-y-como-funciona/

Castillo, R. (02 de Diciembre de 2020). Obtenido de https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

Chavez, J. J. (2023). Obtenido de https://www.deltaprotect.com/blog/vulnerabilidad-informatica

editorial, E. (5 de Agosto de 2021). Obtenido de https://concepto.de/sistema-de-informacion/

Fuente, J. d. (6 de Junio de 2021). Obtenido de https://www.incentro.com/es-ES/blog/que-es-open-source-codigo-abierto

Implika. (14 de Abril de 2021). Obtenido de https://www.implika.es/blog/que-son-redes-informaticas

Luis, J. (27 de Octubre de 2019). Obtenido de https://247tecno.com/topologia-de-red-tipos-caracteristicas/

Luis, J. (27 de Octubre de 2019). Obtenido de https://247tecno.com/topologia-de-red-tipos-caracteristicas/

Luz, S. D. (22 de Noviembre de 2022). Obtenido de https://www.redeszone.net/tutoriales/seguridad/mejores-escaner-vulnerabilidades-gratis-hacker/

Mercado, R. B. (06 de Enero de 2023). Obtenido de https://www.rberny.com/2023/01/06/escaneres-de-vulnerabilidad-de-red-gratuitos/

Ovallos-Ovallos, J. A., & Rico-Bautista, D. (2020). Guía práctica para el análisis de vulnerabilidades de un entorno cliente-servidor GNU/Linux mediante una metodología de pentesting. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 339-343. Obtenido de https://www.proquest.com/openview/a2803956d6c8a33bcf45b8c267f13344/1?pq-origsite=gscholar&cbl=1006393

POSTIGO PALACIOS, A. (19 de Mayo de 2020). Seguridad informática. En A. POSTIGO PALACIOS, *Seguridad informática.* Obtenido de https://books.google.es/books?id=UCjnDwAAQBAJ&dq=seguridad+inform%C3%A1tica&lr=&hl=es&source=gbs_navlinks_s

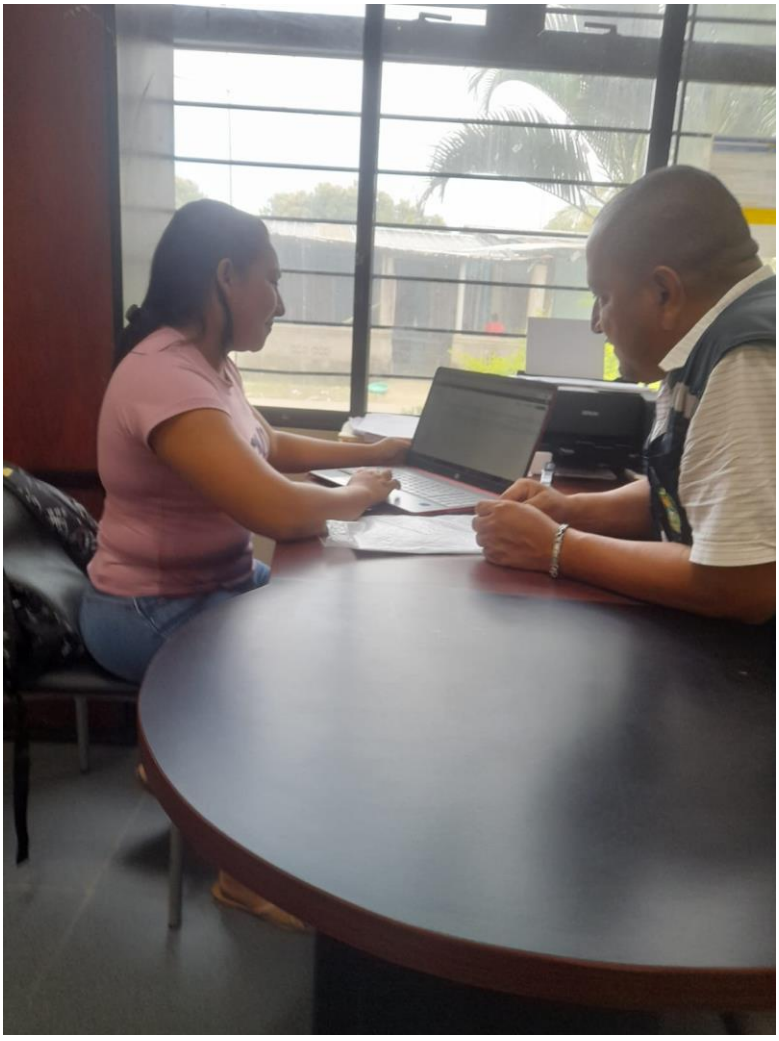
Quiroa, M. (1 de Marzo de 2020). Obtenido de https://economipedia.com/definiciones/amenazas-de-una-empresa.html

TecnologiaMix. (13 de Marzo de 2021). Obtenido de https://www.tecnologiamix.com/que-es-una-infraestructura-de-red/

UNIR. (15 de Junio de 2021). Obtenido de https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

ANEXOS

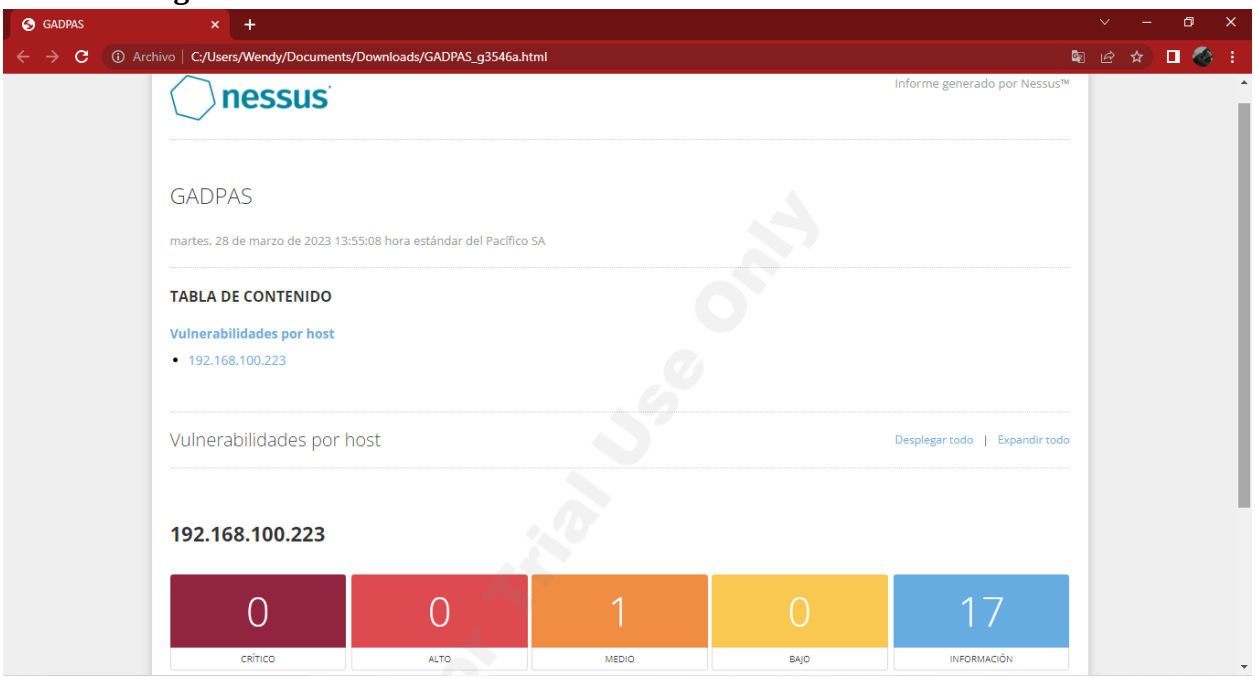
Figura 8 Proceso de escaneo de red



Fuente: (Wenddy Evelin Basurto López, 2023)

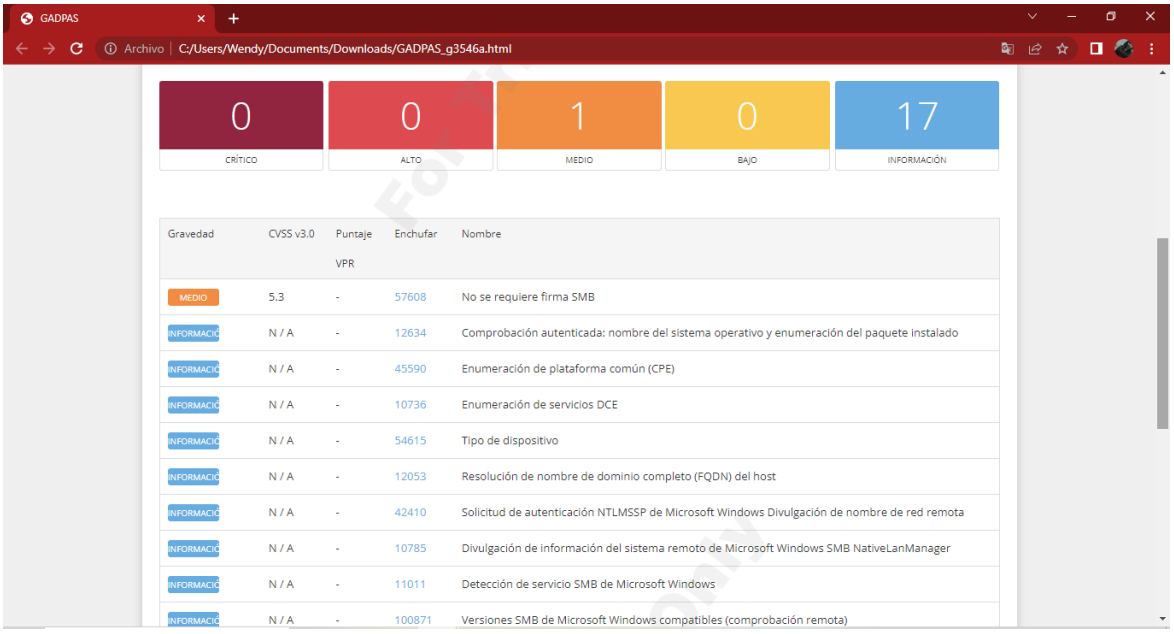
Análisis de vulnerabilidades de red informática mediante la herramienta Nessus de GAD Parroquial de Antonio Sotomayor

Figura 9 Vulnerabilidades



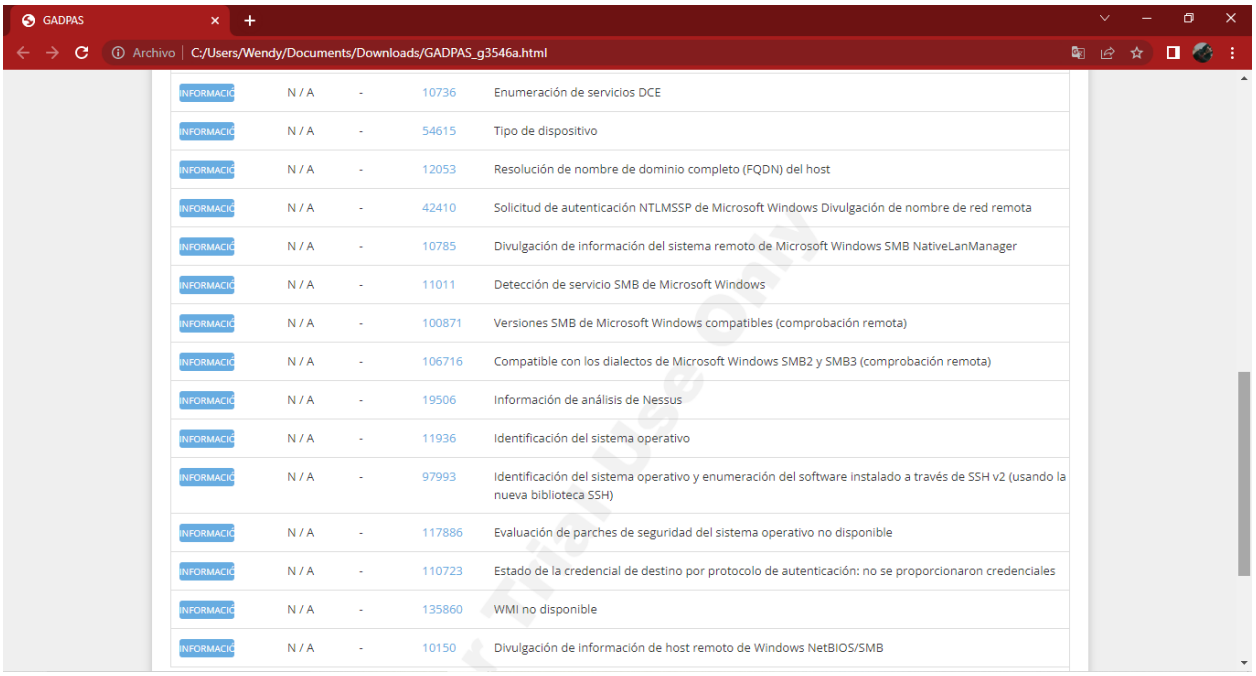
Fuente: (Wenddy Evelin Basurto López, 2023)

Figura 10 Lista de vulnerabilidades



Fuente: (Wenddy Evelin Basurto López, 2023)

Figura 11 Lista de vulnerabilidades



INFORMACIÓ	N / A	-	10736	Enumeración de servicios DCE
INFORMACIÓ	N / A	-	54615	Tipo de dispositivo
INFORMACIÓ	N / A	-	12053	Resolución de nombre de dominio completo (FQDN) del host
INFORMACIÓ	N / A	-	42410	Solicitud de autenticación NTLMSSP de Microsoft Windows Divulgación de nombre de red remota
INFORMACIÓ	N / A	-	10785	Divulgación de información del sistema remoto de Microsoft Windows SMB NativeLanManager
INFORMACIÓ	N / A	-	11011	Detección de servicio SMB de Microsoft Windows
INFORMACIÓ	N / A	-	100871	Versiones SMB de Microsoft Windows compatibles (comprobación remota)
INFORMACIÓ	N / A	-	106716	Compatible con los dialectos de Microsoft Windows SMB2 y SMB3 (comprobación remota)
INFORMACIÓ	N / A	-	19506	Información de análisis de Nessus
INFORMACIÓ	N / A	-	11936	Identificación del sistema operativo
INFORMACIÓ	N / A	-	97993	Identificación del sistema operativo y enumeración del software instalado a través de SSH v2 (usando la nueva biblioteca SSH)
INFORMACIÓ	N / A	-	117886	Evaluación de parches de seguridad del sistema operativo no disponible
INFORMACIÓ	N / A	-	110723	Estado de la credencial de destino por protocolo de autenticación: no se proporcionaron credenciales
INFORMACIÓ	N / A	-	135860	WMI no disponible
INFORMACIÓ	N / A	-	10150	Divulgación de información de host remoto de Windows NetBIOS/SMB

Fuente: (Wenddy Evelin Basurto López, 2023)

Preguntas de entrevistas

1. **¿Qué tipo de red utilizan?**

   Red LAN

2. **¿Realizan proceso de respaldo de la información?**

   Si

3. **¿Cada que tiempo realizan mantenimiento a la red?**

   Solo cuando falla la red

4. **¿Qué acciones toman al momento de presentar fallos en la red?**

   Llamar al proveedor del internet

5. **¿Qué sistema operativo utilizan en la actualidad?**

   Windows 10

6. **¿En el GAD cuenta con Internet estable y rápido?**

   A veces si

7. **¿Cuál es el proveedor del servicio se internet?**

   Teccial

8. **¿Si existen fallas en la red cual es el tiempo que se tardan en detectar el problema?**

   Depende el fallo a veces en 3 hora detectan el daño

9. **¿Cuántas veces en el año cambian la contraseña de Internet?**

   2 veces

10. **¿Cómo considera usted la calidad de la red inalámbrica?**

    Calidad media

CERTIFICADO DE ANÁLISIS
magister

Wenddy Basurto Trabajo final

5% Similitudes

< 1% Texto entre comillas
0% similitudes entre comillas

2% Idioma no reconocido

Nombre del documento: Wenddy Basurto Trabajo final.docx
ID del documento: 9a2ffb40de43c8927b209773a4b358e2e9f68720
Tamaño del documento original: 567,26 ko

Depositante: VILLARES PAZMIÑO JOSE DANILO
Fecha de depósito: 3/4/2023
Tipo de carga: interface
fecha de fin de análisis: 3/4/2023

Número de palabras: 5306
Número de caracteres: 34.128

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.redeszone.net | Mejores escáner de vulnerabilidades gratis para hacker ético https://www.redeszone.net/tutoriales/seguridad/mejores-escaner-vulnerabilidades-gratis-hacker/	2%		Palabras idénticas : 2% (97 palabras)
2	247tecno.com | TOPOLOGIA DE RED - QUE ES, TIPOS Y CARACTERISTICAS https://247tecno.com/topologia-de-red-tipos-caracteristicas/	1%		Palabras idénticas : 1% (66 palabras)
3	TRABAJO FINAL.docx | Trabajo final #f8c5c3 El documento proviene de mi grupo 1 fuente similar	< 1%		Palabras idénticas : < 1% (29 palabras)
4	www.tecnologiamix.com | ¿Qué es una infraestructura de red? | Tecnología Mix https://www.tecnologiamix.com/que-es-una-infraestructura-de-red/ 2 fuentes similares	< 1%		Palabras idénticas : < 1% (30 palabras)
5	dspace.utb.edu.ec | Análisis de amenazas y vulnerabilidades de la gestión de proce... http://dspace.utb.edu.ec/bitstream/49000/11816/3/E-UTB-FAFI-SIST.INF-000012.pdf.txt 1 fuente similar	< 1%		Palabras idénticas : < 1% (22 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.linkedin.com | Escáner de vulnerabilidades de Red Gratuitos https://www.linkedin.com/pulse/escáner-de-vulnerabilidades-red-gratuitos-guzmán-mercado#:~:text=...	< 1%		Palabras idénticas : < 1% (26 palabras)
2	ciberseguridad.com | ¿Qué es OSSTMM? Definición, historia y características https://ciberseguridad.com/guias/desarrollo-seguro/osstmm/	< 1%		Palabras idénticas : < 1% (10 palabras)
3	techinfo.wiki | Topología de la red – Techinfo https://techinfo.wiki/topologia-de-la-red/	< 1%		Palabras idénticas : < 1% (14 palabras)
4	dspace.utb.edu.ec | Análisis de la Infraestructura de Red de la Junta Parroquial de l... http://dspace.utb.edu.ec/bitstream/49000/7691/3/RONQUILLO CARRASCO.pdf.txt	< 1%		Palabras idénticas : < 1% (13 palabras)
5	dspace.utb.edu.ec | Cultura Organizacional del Gobierno Autónomo Descentralizado... http://dspace.utb.edu.ec/bitstream/49000/7561/3/LOPEZ MONTOYA.pdf.txt	< 1%		Palabras idénticas : < 1% (11 palabras)