UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA.

F.A.F.I

PROCESO DE TITULACION

JUNIO – NOVIEMBRE 2021

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

INGENIERIA EN SISTEMAS

PREVIO A LA OBTENCION DEL TITULO DE INGENIERIA EN SISTEMAS

TEMA:

ANÁLISIS DE LAS VULNERABILIDADES DE LAS REDES INALÁMBRICAS DEL GAD MUNICIPAL DEL CANTÓN VINCES

AUTOR:

JACINTO JOHAN FELIX FAJARDO

TUTOR:

ING. ENRRIQUE DELGADO

BABAHOYO – LOS RIOS – ECUADOR

2021

RESUMEN

En la actualidad las redes Inalámbricas son unos de los medios de conexión más usados para acceder a internet y tener una buena comunicación con otros dispositivos. Por este motivo las personas buscan incorporar equipos informáticos en su ámbito laboral como los routers, los cuales permiten mantener una comunicación en su mayor parte estable por medio de las señales de wifi, esto permite a los usuarios estar conectados entre sí por medio de una red con acceso a internet. Esto genera que las personas quieran acceder a dichas redes de forma indebida, ver la información que las personas naturales o trabajadores brindan al acceder en páginas web que solicitan esta información. El desarrollo de este proyecto tendrá una línea de investigación cualitativa y una investigación de campo que usará la entrevista como técnica o instrumento de investigación, con la finalidad de tener conocimiento sobre la situación actual de las redes inalámbricas y a su vez identificar las amenazas y vulnerabilidades que afecten en la red. El objetivo de la investigación es realizar un análisis de las vulnerabilidades existentes en las diferentes redes inalámbricas, con el fin de ayudar y proporcionar información o Recursos a los profesionales de tecnologías de información para mejorar la seguridad en las redes inalámbricas con las que cuenta el GAD Municipal.

Palabras Claves: Redes Inalámbricas, Vulnerabilidad, GAD Municipal

ABSTRACT

At present, Wireless networks are one of the most used means of connection to access the Internet and have good communication with other devices. For this reason, people seek to incorporate computer equipment in their work environment such as routers, which allow to maintain communication for the most part stable through Wi-Fi signals, this allows users to be connected to each other through a network with internet access. This causes people to want to access said networks improperly, to see the information that natural persons or workers provide when accessing web pages that request this information. The development of this project will have a qualitative research line and field research that will use the interview as a technique or research instrument, in order to gain knowledge about the current situation of wireless networks and in turn identify the threats and vulnerabilities that affect the network. The objective of the research is to carry out an analysis of the existing vulnerabilities in the different wireless networks, in order to help and provide information or Resources to information technology professionals to improve security in the wireless networks that the GAD has. Municipal.

Keywords: Wireless Networks, Vulnerability, Municipal GAD

INTRODUCCIÓN

El presente proyecto trata sobre el análisis de las vulnerabilidades que presenta la red inalámbrica del GAD municipal del cantón Vinces perteneciente a la provincia de los Ríos.

"Las redes inalámbricas han provocado un gran impacto en todos los ámbitos sociales y económicos. Tanto la comunicación por voz como la transferencia de datos, han pasado de ser herramientas ancladas a un lugar y conectadas con cables a elementos que pueden ser transportados y utilizados mientras nos movemos, en cualquier momento y en cualquier lugar. Por tanto, se han convertido en dispositivos con tecnologías que permiten realizar actividades que antes sólo podíamos desarrollar sentados en la oficina de una empresa, en el hogar o en un centro de investigación." **(Francisco Jose - Luis Cabezas, 2016).**

Con el pasar del tiempo se ha podido evidenciar que el uso de las redes inalámbricas nos brinda una mejor experiencia de conectividad inalámbrica y así poder realizar un mejor uso a los dispositivos que usan este tipo de conexión en la actualidad. Los dispositivos que comúnmente utilizan las redes inalámbricas incluyen ordenadores portátiles, ordenadores de escritorio, netbooks, asistentes digitales personales, teléfonos móviles, tablets y dispositivos localizadores. Las redes inalámbricas funcionan de manera similar a las redes cableadas, sin embargo, las redes inalámbricas deben convertir las señales de información en una forma adecuada para la transmisión a través del medio de aire. Las redes inalámbricas sirven a muchos propósitos.

En algunos casos se utilizan en sustitución a las redes cableadas, mientras que en otros casos se utilizan para proporcionar acceso a datos corporativos desde ubicaciones remotas. Las redes inalámbricas permiten a los dispositivos remotos que se conecten sin

dificultad, independientemente que estos dispositivos estén a unos metros o a varios kilómetros de distancia. Todo ello sin necesidad de romper paredes para pasar cables o instalar conectores esto ha hecho que el uso de esta tecnología sea muy popular, extendiéndose muy rápidamente.

Este análisis se basara en el uso de la metodología de investigación cualitativa usando el método inductivo que ayudaran a la resolución del mismo donde se utilizara las técnicas de la Entrevista y la Observación con el objetivo de tener el conocimiento sobre la situación actual de las redes inalámbricas del GAD Municipal y a su vez identificar las amenazas y vulnerabilidades que afectan a la red, además se utilizara la herramienta NESSUS para determinar las vulnerabilidades de la Red, y la herramienta web Speed test para medir la velocidad de la red.

Este trabajo estará incluido bajo las líneas de investigación de la Universidad Técnica de Babahoyo, en especial bajo la línea de Sistemas de Información y Comunicación Emprendimiento e Innovación y la sub línea de redes y tecnologías inteligentes de software y Hardware.

DESARROLLO

La seguridad en internet son todas aquellas precauciones que se toman para proteger todos los elementos que hacen parte de la red, como infraestructura e información, que suele ser la más afectada por delincuentes cibernéticos. La seguridad informática se encarga de crear métodos, procedimientos y normas que logren identificar y eliminar vulnerabilidades en la información y equipos físicos, como los computadores. Este tipo de seguridad cuenta con bases de datos, archivos y equipos que hacen que la información importante no caiga en manos de personas equivocadas Los delincuentes cibernéticos usan varios modos para atacar a una víctima en la red como los virus con los que logran

vulnerar sistemas y alterar el funcionamiento de los dispositivo electrónicos, o el phishing, que consiste en que un cibercriminal se hace pasar por una persona diferente por medio de correos electrónicos, mensajería instantánea o redes sociales para adquirir información confidencial como contraseñas, tarjetas de crédito, entre otros.

La seguridad se viene ejecutando y poniendo en práctica desde varios años atrás en diferentes campos. En la actualidad contamos con la tecnología de las redes inalámbricas y se debe de establecer una seguridad muy prolongada e infalible, ya que contamos con diversa información muy valiosa para así no ser propenso a ningún tipo de vulnerabilidades, mucho menos ser objeto de intrusos y no permitir el ingreso de forastero con el propósito de hurto y arrebato de dicha información.

El GAD Municipal del cantón Vinces perteneciente a la provincia de los Ríos cuya dirección es administrada por el Sr alcalde. Alfonzo Montalván Cerezo desde el pasado 9 de junio del 2019, cuenta con varias falencias administrativas de la pasada administración en los diferentes departamentos que con los que cuenta la Municipalidad del Cantón, el cableado se encuentra en deterioro, Cuentan con un cableado de categoría 5E, las redes no se encuentran segmentadas, no cuentan con suficientes puntos de accesos para los ordenadores, la intensidad de las redes Wifi es débil, la red no cuentan con la seguridad informática adecuada tomando en cuenta la información que se maneja en esta administración.

El municipio cuenta con 13 Departamentos con 6 Routers de la Marca (TP-link-WR841N –300Mbps –2 antenas) y 12 Switch Repetidor de la marca TP-Link los cuales hacen uso las personas que laboran en la institución al conectarse a las redes inalámbricas.

Un análisis de vulnerabilidades es un proceso mediante el cual una organización define e identifica, las debilidades y el nivel de exposición de las aplicaciones ante una o muchas

amenazas en específico. En nivel de exposición se debe tener en cuenta los aplicativos más críticos para la organización, esto quiere decir, los aplicativos que manejen más información sensible de la organización o los que interactúen con un usuario y solicite información personal sensible. En temas de aplicaciones se le puede realizar una prueba de análisis de vulnerabilidades a una página web, aplicativo móvil (sistema operativo Android – IOS), switch, router, servidores en la nube o físico (Público o privado).

"La seguridad de red combina varias capas de defensa en el perímetro y la red. Cada capa de seguridad de red implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad. Las redes inalámbricas no son tan seguras como las redes cableadas. Sin medidas de seguridad estrictas, instalar una LAN inalámbrica es como poner puertos Ethernet por doquier, incluso en el estacionamiento. Para evitar un ataque, necesita productos específicamente diseñados para proteger la red inalámbrica" **(cisco, 2018)**

"La matriz de análisis dafo o foda, es una conocida herramienta estratégica de análisis de la situación de la empresa. El principal objetivo de aplicar la matriz dafo en una organización, es ofrecer un claro diagnóstico para poder tomar las decisiones estratégicas oportunas y mejorar en el futuro. Su nombre deriva del acrónimo formado por las iniciales de los términos: debilidades, amenazas, fortalezas y oportunidades. La matriz de análisis dafo permite identificar tanto las oportunidades como las amenazas que presentan nuestro mercado, y las fortalezas y debilidades que muestra nuestra empresa."

A continuación, se adjunta una matriz de Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas).

FORTALEZAS	OPORTUNIDADES
• Cuentan con internet estable de 40 Mbps 33Mbps para Descarga y 35 Mbps para Carga	• Realizar una nueva estructuración del cableado • Realizar una segmentación de la Red • Incrementar en Ancho de Banda • Renovación de equipos
DEBILIDADES	**AMENAZAS**
• El Cableado se encuentra deteriorado • Los Routers y Switch no se encuentran en lugares estratégicos	• Falta de Seguridad

Ilustración 1 por Johan Felix Fajardo

La metodología de Investigación que se empleó en este Caso de estudio es la metodología cualitativa haciendo uso de del método inductivo, el cual permitió realizar un Análisis de las vulnerabilidades de las redes Inalámbricas con las que cuenta el municipio, para así poder llegar a una conclusión en específico también se usó la técnica de la observación y entrevista para la recopilación de información el uso de estas técnicas nos permitió conocer a detalle las debilidades con las que cuenta el municipio en el ámbito de redes inalámbricas y cableado, la entrevista se realizó en el departamento de sistemas la cual permitió recopilar información para el desarrollo del caso de estudio, los instrumentos utilizados para la implementación de la metodología fueron la entrevista y la observación, Las cuales se realizaron de Manera formal al Analista. Jacinto López Segura, jefe del departamento de sistemas el cual de la manera más amable accedió a brindar la información correspondiente y necesaria para el desarrollo del caso de estudio, así como

también compartió el acceso a ciertos equipos para realizar los análisis respectivos y detectar los errores y vulnerabilidades de la Red Inalámbrica.

La municipalidad del Cantón Vinces cuenta con varios equipos los cuales emiten señal de acceso inalámbrica como es el caso de:

Equipos de Red

Equipo	**Cantidad**	**Características**
Router Tp-Link	6	TL-WR841HP 300Mbps – 2 Antena
Switch Principal	1	TL-SL3452 Switch gestionado L2 Lite con 48 puertos 10/100 Mbps + 4 puertos Gigabit
Switch	12	TL-SF1008D Switch de sobremesa con 8 puertos a 10/100 Mbps

Ilustración 2 Elaborado por: Johan Felix Fajardo

"Una red inalámbrica permite que los dispositivos permanezcan conectados a la red, pero sin usar cables. Los puntos de acceso amplifican las señales de Wi-Fi, de manera que un dispositivo puede estar lejos de un router, pero permanecer conectado a la red. Cuando se conecta a una zona Wi-Fi en un café, un hotel, una sala de estar de aeropuerto u otro lugar público, se conecta a la red inalámbrica de dicha empresa." **(cisco, 2020)**

Algunos de los Beneficios que nos brinda usar una red inalámbrica son los siguientes:

Comodidad: acceda a los recursos de red desde cualquier ubicación del área de cobertura de la red inalámbrica o desde cualquier zona Wi-Fi.

Movilidad: no está atado al escritorio, como sí sucede con una conexión cableada. Usted y sus empleados pueden conectarse en las reuniones de sala de conferencias, por ejemplo.

Productividad: el acceso inalámbrico a Internet y a las aplicaciones y los recursos esenciales de la empresa ayuda al personal a cumplir su trabajo y fomenta la colaboración.

Fácil configuración: no hace falta pasar cables, por lo que la instalación puede ser rápida y rentable.

Capacidad de expansión: puede ampliar fácilmente las redes inalámbricas con los equipos existentes, mientras que una red cableada puede requerir cableado adicional.

Seguridad: los avances en redes inalámbricas proporcionan sólidas protecciones de seguridad.

Costo reducido: como las redes inalámbricas eliminan o reducen los gastos de cableado, pueden costar menos que las redes cableadas para su operación.

"Según **(Salazar, 2017)** Las redes inalámbricas se pueden clasificar en cuatro grupos específicos según el área de aplicación y el alcance de la señal

- Redes inalámbricas de área personal (Wireless Personal-Area Networks - WPAN)
- Redes inalámbricas de área local (Wireless Local-Area Networks - WLAN)
- Redes inalámbricas de área metropolitana (Wireless Metropolitan-Area Networks - WMAN)

- Redes inalámbricas de área amplia (Wireless Wide-Area Networks - WWAN)”

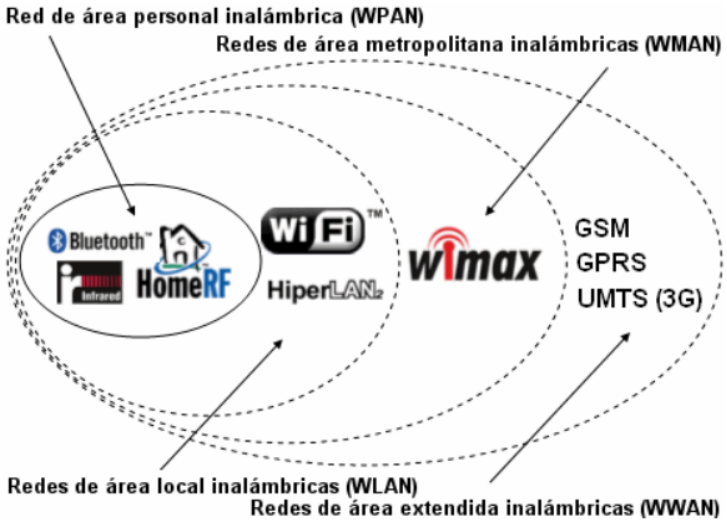

Ilustración 3 Imagen tomada de Google Sities

Las redes inalámbricas pueden dividirse también en dos grandes segmentos: de corto y de largo alcance. Inalámbrica de corto alcance se refiere a las redes confinadas en un área limitada. Esto se aplica a las redes de área local (LAN), como edificios corporativos, los campus escolares y universitarios, fábricas o casas, así como a las redes de área personal (PAN) donde los ordenadores portátiles necesitan estar muy cerca entre sí para comunicarse.

Además, pueden dividirse en 4 grupos de redes importantes y dependiendo al tipo de conexión a internet que desee se escogerá el tipo de Red.

Redes inalámbricas de área local estas redes permiten a los usuarios establecer conexiones inalámbricas dentro del área de cobertura. Es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros, podría cubrir, por ejemplo, un edificio corporativo, un campus empresarial, o en un espacio público como un aeropuerto.

Redes inalámbricas de área metropolitana estas redes permiten a los usuarios establecer conexiones inalámbricas entre varias ubicaciones dentro de un área metropolitana, por

ejemplo, entre varios edificios de oficinas de una ciudad o en un campus universitario, sin el alto coste que supone la instalación de cables de fibra o cobre y el alquiler de las líneas.

"Redes de área personal inalámbricas estas redes permiten establecer comunicaciones inalámbricas para dispositivos como teléfonos celulares y equipos portátiles que se utilizan dentro de un espacio operativo personal (POS). Un POS es el espacio que rodea a una persona, hasta una distancia de 10 metros aproximadamente. Red inalámbrica de área amplia la cual nos permite conectarnos o incorporarnos a internet desde cualquier zona o espacio físico que contenga señal de internet o cobertura de datos móviles." **(Yan Cerro, 2015).**

"Una red inalámbrica conecta los equipos sin utilizar cables de red. Las computadoras utilizan comunicaciones de radio para enviar datos entre sí. Puede comunicarse directamente con otras computadoras inalámbricas, o conectarse a una red existente a través de un AP inalámbrico." **(Intel, 2021)**

En la actualidad las redes inalámbricas nos brindan una mejora estética en una infraestructura, ya que estas redes no hacen uso de cables ni conectores ya que emplean una conexión de ondas electromagnéticas y Antenas.

Una vulnerabilidad de red en seguridad informática es la debilidad o fallos en cuanto a la protección que se puede tener en un sistema Estas vulnerabilidades pueden permitir que una red o un sistema de información sean vulnerados en caso de que ocurra un ataque informático dentro del área informática hay que tener en consideración tener una buena seguridad para no ser víctimas ataques y evitar el robo de información y su mala manipulación.

El diagnostico de las vulnerabilidades exige la identificación anticipada de riesgos para tomar acciones preventivas y con responsabilidad en las redes inalámbricas que fueron creadas por la necesidad de brindar acceso a red a dispositivos portátiles como es el caso de Tablet, Celulares, Laptops, la creación de estas redes atrajo problemas hacia el medio de transmisión, por cuanto los intrusos pueden acceder a la red libremente dando una posibilidad virtual de no ser detectados. Diagnóstico de vulnerabilidad es infalible y ofrecen una alerta de un atentado en proceso, para poder estar pendiente de cualquier tipo de ataque.

"Según **(VERA NAVARRETE, 2018)** "La seguridad informática se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático."

Normas de red inalámbrica

"Existen tres tipos de redes inalámbricas básicas (En realidad más, pero nos enfocaremos en estás tres). Estos tipos de redes inalámbricas son las siguientes: redes personales en la que encontramos infrarrojo, bluetooth y Zigbee, también las redes locales encontramos el popular wifi y finalmente una red más grande que es de área metropolitana, en la que se encuentra WiMax. Las diferentes redes poseen un tipo de norma basada en el estándar IEEE, se hablará de manera concreta y simple de las variantes más relevantes dentro de estas normas. La utilización de las normas es a nivel mundial, significa que en cada lugar donde vayamos podremos conectarnos de la misma forma o similar. Las empresas se

adaptan a estas normas, lo que significa que no importa la marca o tipo de producto, mientras este normalizado para la tarea que va a realizar, podremos utilizarla sin ningún tipo de problema.” **(Google, s.f.)**

NORMA 802.11: Esta es la norma que regula todo lo que se trata de redes inalámbricas locales (WLAN), esta norma regula en general tres aspectos importantes, la frecuencia, velocidad y alcance que tiene la red inalámbrica local.

Estándares Wireless 802.11

Estándar WLAN	802.11b	802.11a	802.11g	802.11h	HiperLAN2	Bluetooth
Organismo	IEEE(USA)	IEEE	IEEE	IEEE	ETSI(euro)	Bluetooth SIG
Finalización	1999	2002	Jun,2003	2003	2003	2002
Denominación	Wi-Fi	Wi-Fi5				
Banda frecuencias	2.4GHz (ISM)	5 GHz	2.4GHz (ISM)	5 GHz	5 GHz	2.4 GHz
Velocidad máx.	11 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	0.721Mbit/s
Throughput medio	5,5 Mbps	36 Mbps			45 Mbps	
Interfaz aire	SSDS/FH	OFDM	OFDM	OFDM	OFDM	DSSS/FHSS
Disponibilidad	>1000	algunos	algunos	algunos	(2004)	Muchos
Otros aspectos				TPC, DFA		
Nº de canales	3c no solapados	12 no solapados	3 no solapados	19 no solapados		

Ilustración 4 Imagen tomada de http://bibing.us.es/

NORMA 802.15: Fue diseñada con el fin de lograr una transferencia eficiente y rápida de datos en WPAN's (Wireless Personal Área Network o redes inalámbricas de área personal). Existen diferentes tipos de esta red en la que están incluidas Bluetooth y Zigbee. Pero nos enforcaremos en la primera por ser la más utilizada en la actualidad.

NORMA 802.16: (Redes inalámbricas de área metropolitana), con el nombre de WiMAX, permite accesos de unos 50 a 80 kilómetros y velocidades que pueden llegar a 1Gbps, funcionan en las frecuencias de 2 hasta 11 Ghz y 11 a 66 Ghz. Se puede dar a entender WiMAX con una gran red inalámbrica constituida de pequeñas WLAN.

Red

Una red es un sistema que nos permite la comunicación entre varios dispositivos independientes. Una red es un alcance que nos permite tener una conectividad con múltiples dispositivos pudiendo abarcar una inmensa área de comunicación.

Ilustración 5 Imagen Tomada de Sities Google

Seguridad de la red

"La seguridad de red combina varias capas de defensa en el perímetro y la red. Cada capa de seguridad de red implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos." **(Cisco, s.f.)**

Métodos de Seguridad de Red.

Existen varias técnicas de seguridad de res para implementar un tipo de defensa en profundidad:

Firewalls: Los firewalls ponen una barrera entre sus redes internas de confianza y las redes externas que no son de confianza, como Internet. Usan un conjunto de reglas definidas para permitir o bloquear el tráfico.

Segmentación de la red: La segmentación definida por software clasifica el tráfico de red en distintas categorías y facilita la aplicación de políticas de seguridad.

Control de acceso: No todos los usuarios deben tener acceso a la red. Para evitar posibles ataques, debe reconocer a todos los usuarios y dispositivos.

Seguridad de las aplicaciones: Cualquier software que utilice para operar su negocio debe estar protegido, ya sea que su personal de TI lo construya o lo compre.

Prevención de pérdida de datos: Las organizaciones deben asegurarse de que el personal no envíe información confidencial fuera de la red

Seguridad de dispositivos móviles: Los ciberdelincuentes cada vez se centran más en los dispositivos y las aplicaciones móviles.

Administración de eventos e información de seguridad: Los productos SIEM reúnen la información que el personal de seguridad necesita para identificar y responder a las amenazas.

VPN: Una red privada virtual cifra la conexión desde un terminal a la red, generalmente por Internet.

Seguridad web: Una solución de seguridad web es controlar el uso de la web por parte del personal, bloquea las amenazas web y bloquea el acceso a sitios web maliciosos.

Seguridad inalámbrica: Las redes inalámbricas no son tan seguras como las redes cableadas. Sin medidas de seguridad estrictas, instalar una LAN inalámbrica es como poner puertos Ethernet por doquier, incluso en el estacionamiento.

Técnicas y Herramientas Utilizadas.

Se realizo la entrevista al jefe del departamento de sistemas el cual nos brindó la información necesaria, en el anterior mandato no se realizaron las debidas adecuaciones en los sistemas y en el cableado la red no se encuentra segmentado y no se encuentra estructurado además nunca se ha realizado un análisis de vulnerabilidad a la red y desconocen si la red es vulnerable y accesible para cualquier ataque, los routers no se encuentran bien ubicados y están colgando al aire libre, también nos comunicó que el internet es proveído por una empresa privada y no del estado.

Para llevar a cabo el análisis en la red de la municipalidad se utilizaron las herramientas, Inssider, SpeedTest, Nessus

Inssider: "Es un programa gratuito para analizar el espectro de redes inalámbricas e identificar visualmente el canal menos saturado para optimizar la calidad de tu conexión Wifi con el router. Es recomendable sobre todo en bloques de pisos donde existen multitudes de redes inalámbricas diferentes." **(Guerra, 2018)**

Nessus: "Es el escáner de vulnerabilidades más utilizado en el mundo. Esta herramienta de alto nivel detecta amenazas en tiempo real y gracias a su precisión evita la ocurrencia de falsos positivos. Nessus previene de manera eficiente los ataques a la red al identificar debilidades y errores de configuración que pueden usarse para permitir que las amenazas ingresen al sistema." **(advisors, 2018)**

Speedtest: "Mide la velocidad entre tu dispositivo y un servidor de prueba, utilizando la conexión a internet de tu dispositivo. Algunos factores involucrados en la prueba pueden generar como resultado velocidades imprevistas." **(speedtest.net, s.f.)**

"Las empresas constantemente están amenazadas con sufrir daños en sus sistemas informáticos, estos daños pueden incitar perdidas de muchos tipos. Las amenazas son

mayores cuando en un sistema existen ciertas brechas de seguridad llamadas vulnerabilidades que pueden perjudicar de gran manera a las organizaciones.” **(Baca, 2016).**

La mayor parte de las empresas son objeto de cualquier tipo de intimidación para provocar perjuicios en diferentes áreas, y muchas cuando el sistema presenta irregularidades.

- Se realizo el análisis de velocidad de la Red del GAD Municipal con la herramienta SpeedTest la cual mostro como resultado una velocidad de descarga de 33,97 Mbps y una velocidad de carga de 35.21 Mbps

Ilustración 6 Elaborado por Johan Felix Fajardo

- Se realizo una analisis con la herramienta Inssider la cual nos muestra el nivel potencia de señal de la red del GAD Municipal la cual tiene -77 dBm a -83 dBm siento una señal inestable para abarcar a toda la municipalidad la potencia debe abarcar una rango de -50dBm a -60dBm.

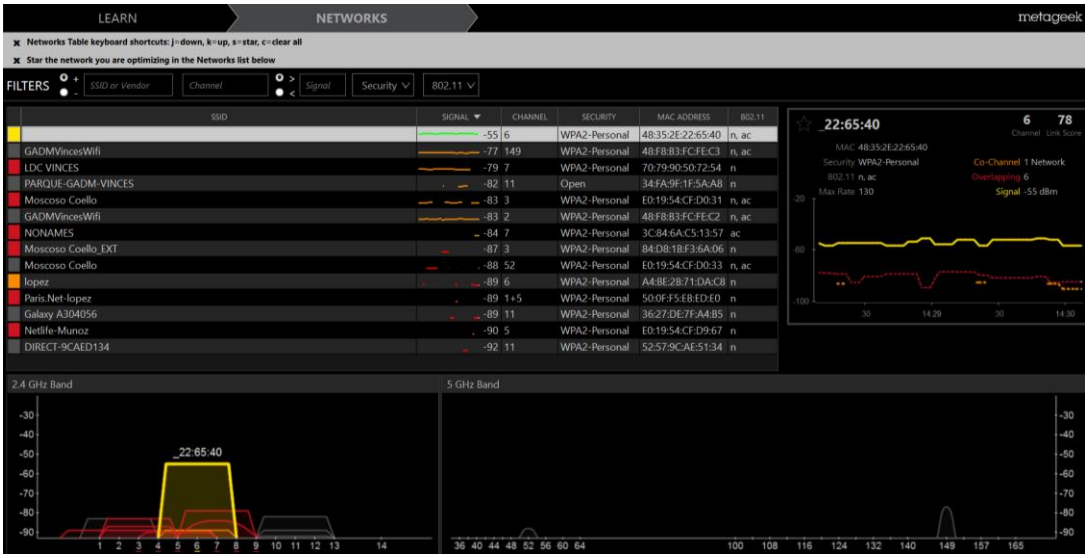

Ilustración 7 Elaborado por Johan Felix Fajardo

- Procedimos a acceder en la plataforma Nessus con nuestro usuario y contraseña creados previamente

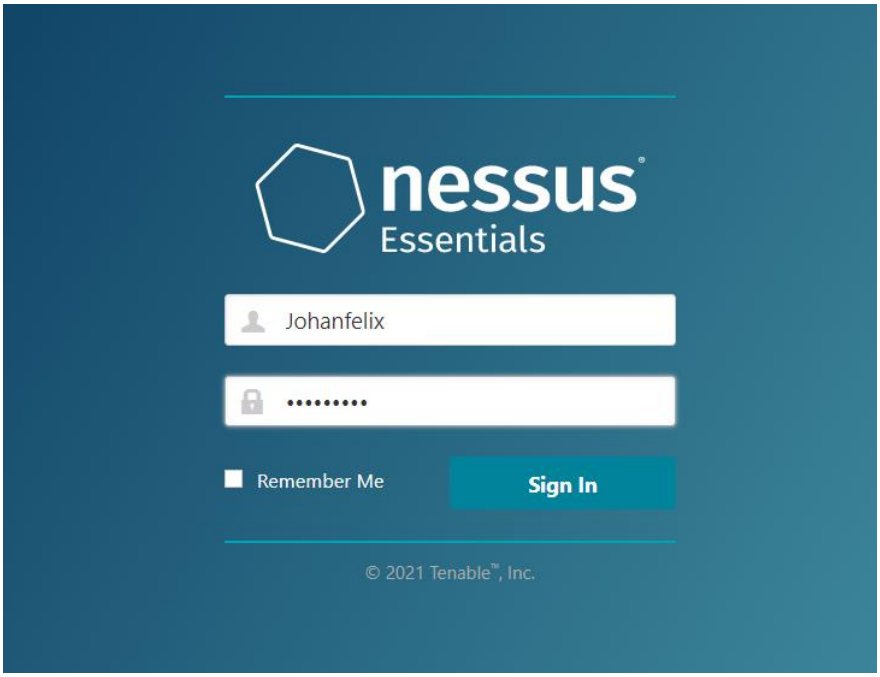

Ilustración 8 Elaborado por Johan Felix Fajardo

- Se procedió a agregar la dirección IP del dispositivo (Router) al cual se le realizara el escaneo

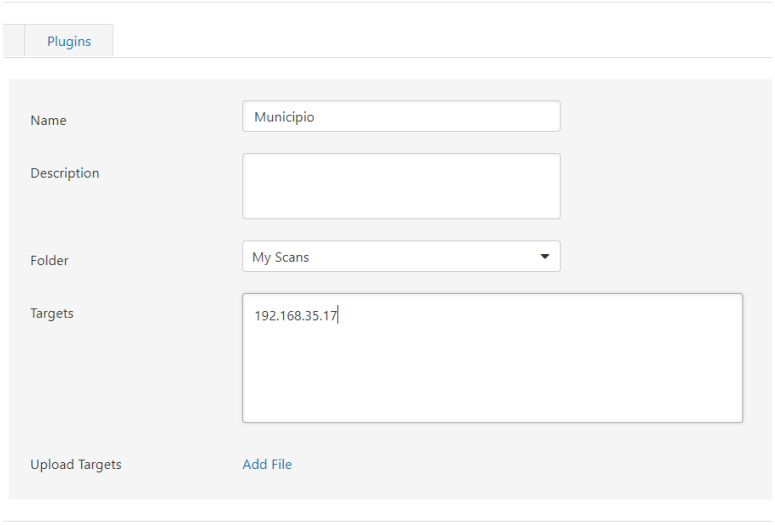

Ilustración 9 Elaborado por Johan Felix Fajardo

- Se realizo el análisis de las vulnerabilidades con la herramienta Nessus El análisis dio como resultado la muestra de 27 falencias que se encuentran en la red y su nivel de gravedad se encuentra especificado en el grafico por colores

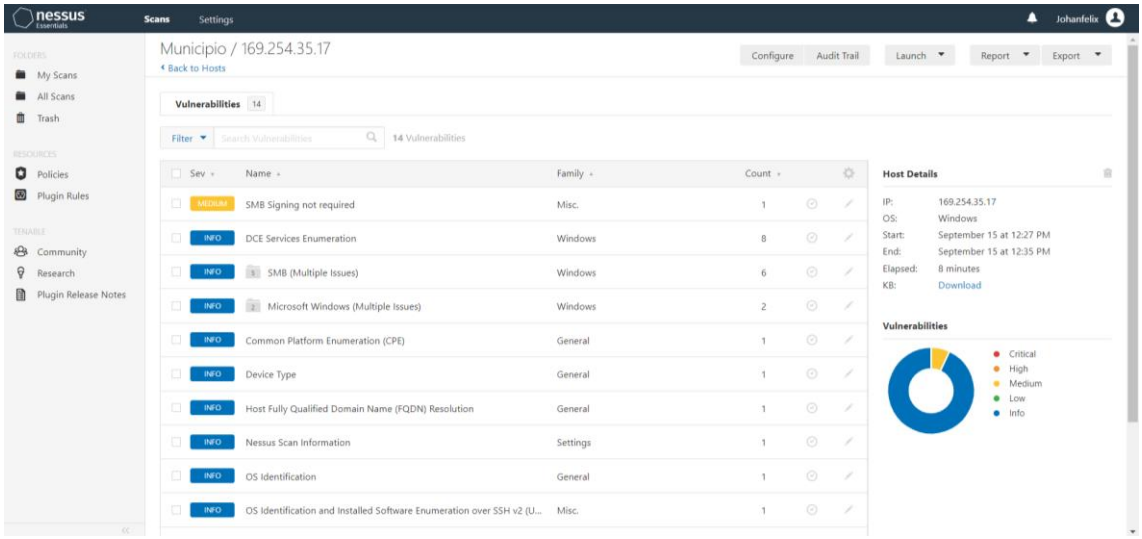

Ilustración 10 Elaborado por Johan Felix Fajardo

- El resultado del analisis muestra una vulnerabilidad de nivel medio en el servidor SMB especificando la falencia y mostrandonos el numero de puerto en el que se encuentra

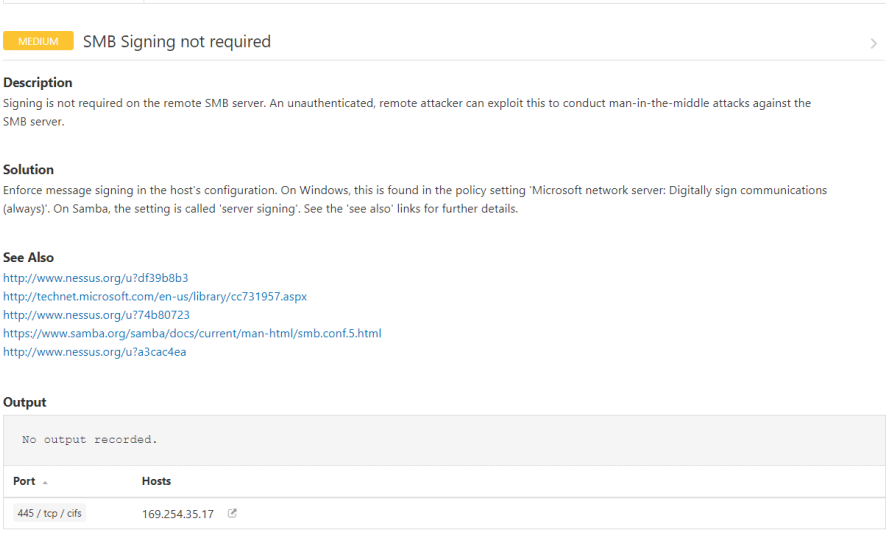

Ilustración 11 por Johan Felix Fajardo

- Otro resultado que nos muestra el analisis es que usando combinaciones de sondas remotas (TCP/IP) se puede adivinar el nombre del sistema operativo en uso

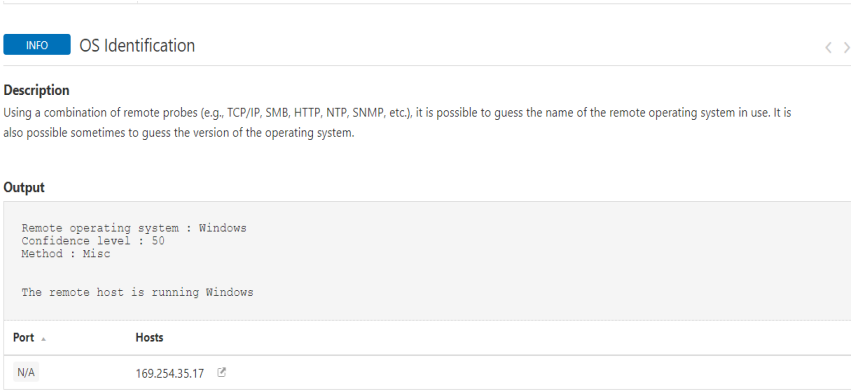

Ilustración 12 Elaborado por Johan Felix Fajardo

- Según el sistema operativo remoto, es posible determinar cuál es el tipo de sistema remoto, por ejemplo: una impresora, enrutador, computadora de uso general

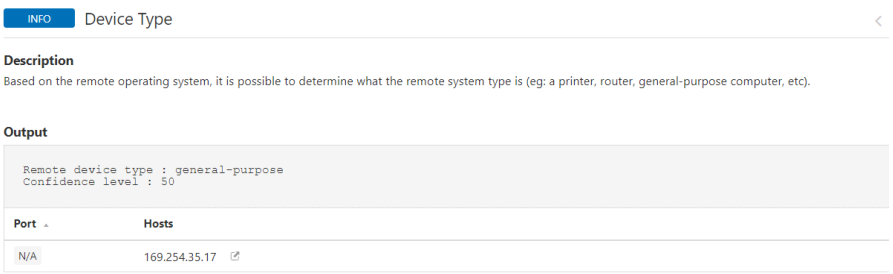

Ilustración 13 Elaborado por Johan Felix Fajardo

- **Lista de Algunas Vulnerabilidades**

Vulnerabilidad	Nivel	Puerto - IP
No se requiere firma SMB	Medio	445 / tcp / cifs
Enumeración de servicios DCE	Medio	135 / tcp / epmap
Resolución de nombre de dominio más completo (FQDN)	Información	N/A
Detección de servicio SMB de Microsoft Windows	Información	139 / tcp / smb 445 / tcp / cifs
Enumeración de plataforma común (CPE)	Información	N/A

CONCLUSIONES

El desarrollo de este caso de estudio sobre el análisis de las vulnerabilidades de las redes inalámbricas del Gad municipal Vinces nos mostró como resultado que las redes actualmente cuentan con varias falencias las cuales pueden ser descubiertas fácilmente exponiendo la información con la que cuenta el municipio y podrían ser utilizadas por personas ajenas a esta institución con fines de lucro o malas intenciones.

- La municipalidad no cuenta con un cableado estructurado ni con una segmentación por áreas para cada uno de los departamentos los cuales son 13 en total
- El cableado con el que cuenta a municipalidad es un Cableado de categoría 5E
- El uso de la Herramienta Nessus nos dio como resultado 27 vulnerabilidades en la red
- No cuentan con normativas de seguridad informática
- Los certificados SSL de la municipalidad no son confiables
- A los dispositivos inalámbricos (Routers) no se les cambia la contraseña

RECOMENDACIONES

Luego de concluir con el estudio realizado, se evidencio que la red si tiene vulnerabilidades, las cuales podrían ser utilizados por terceras personas con el objetivo de acceder a la red poniendo en riesgo la seguridad de la información, por lo cual se recomienda lo siguiente.

- Realizar un nuevo cableado y que este sea estructurado
- Segmentar la red por Áreas o departamentos de trabajos
- Realizar el cambio de claves de acceso a los routers trimestral mente
- Aplicar normativas de seguridad informática

Bibliografía

advisors. (2018). *advisors*. Obtenido de advisors: https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/

Baca, G. (2016). *Introducción a la seguridad informática.* Mexico: Grupo Editorial Patria.

cisco. (2018). Obtenido de cisco: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

cisco. (2020). *cisco*. Obtenido de cisco.com: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/wireless-network.html

Cisco. (s.f.). *www.cisco.com*. Obtenido de www.cisco.com: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

Francisco Jose - Luis Cabezas. (2016). *Redes inalámbricas.* Anaya Multimedia.

Google, S. (s.f.). *Google Sites*. Obtenido de Google Sites: https://sites.google.com/site/wredwiki/normas/normas-de-redes-inalambricas

Guerra, J. R. (13 de Julio de 2018). *computerhoy*. Obtenido de computerhoy: https://computerhoy.com/paso-a-paso/software/optimiza-mejora-tu-conexion-inalambrica-inssider-4711

Intel. (15 de Junio de 2021). *www.intel.la*. Obtenido de www.intel.la: https://www.intel.la/content/www/xl/es/support/articles/000006856/wireless/legacy-intel-wireless-products.html

Salazar, J. (2017). *Redes Inalámbricas.* TechPedia.

speedtest.net. (s.f.). Obtenido de speedtest.net: https://www.speedtest.net/es/mobile/android/help#:~:text=Speedtest%20mide%20la%20velocidad%20entre,generar%20como%20resultado%20velocidades%20imprevistas.&text=Algunos%20servidores%20de%20Speedtest%20pueden%20tener%20mejor%20desempe%C3%B1o%20que%20otros.

VERA NAVARRETE, R. C. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMATICA Y EL ANALISIS DE VULNERABILIDADES .* Editorial Área de Innovación y Desarrollo,S.L.

Yan Cerro, S. C. (30 de Marzo de 2015). *sites.google.com*. Obtenido de sites.google.com: https://sites.google.com/site/redesinalambricas3/tipos-de-redes-inalambricas

ANEXOS

Entrevista al jefe del departamento de sistemas Sr. Jacinto López Segura

1. **¿Poseen con normativas de seguridad informática?**

   No

2. **¿Cuántos Routers disponen en el municipio?**

   6 Routers

3. **¿Con cuántos switch disponen en el municipio?**

   11 Swicth más 1 Principal

4. **¿Cuántas veces por año cambian claves en los dispositivos?**

   Nunca se Cambia

5. **¿Qué sistema operativo usan en el municipio?**

   Windows 10

6. **¿Qué topología de red implementan en el municipio?**

   Cableado simple

7. **¿Qué tipo de antivirus utilizan en los dispositivos?**

   Windows defender, es el que viene por defecto en el sistema

8. **¿El internet con el que trabaja el municipio es del estado o empresa privada?**

   Privada

ALCALDÍA VINCES 2019 - 2023

Oficio Nº 530-A-OF-GADMVINCES-JAMC-2021
Vinces, 20 de septiembre de 2021

Asunto: Aceptación de caso de estudio

Ingeniera
Gina Carrasco Echeverría
DECANA DE LA FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
UNIVERSIDAD TECNICA DE BABAHOYO
Presente.-

De mis consideraciones:

Reciba mi cordial saludo, en atención a su Oficio D-FAFI-UTB-071-UT-2021, de fecha 27 de agosto de 2021, mediante el cual solicita el permiso respectivo para el señor **FELIX FAJARDO JACINTO JOHAN** con C. I. # 1207380807, estudiante de la Carrera de Ingeniería en Sistemas, realice el caso de estudio titulado: Análisis de las vulnerabilidades de las redes inalámbricas del GAD Municipal del cantón Vinces.

Por lo expuesto, me permito darle a conocer que ha sido aceptada la petición formulada por usted, y se le ha permitido al estudiante antes mencionado el desarrollo del caso de estudio, bajo la supervisión del Lcdo. Jacinto López Segura Analista del Departamento de Sistemas del GAD Municipal de este Cantón.

Particular que comunico a usted para los fines pertinentes.

Atentamente,

Firmado electrónicamente por:
JUAN ALFONSO MONTALVAN CEREZO

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE VINCES
ALCALDIA VINCES ALCALDIA

Sr. Alfonso Montalván Cerezo
ALCALDE DEL CANTÓN VINCES
C.c. Archivo
JAMC/jggf

Anexos

Ilustración 14 Entrevista al jefe del Dpto. de sistemas

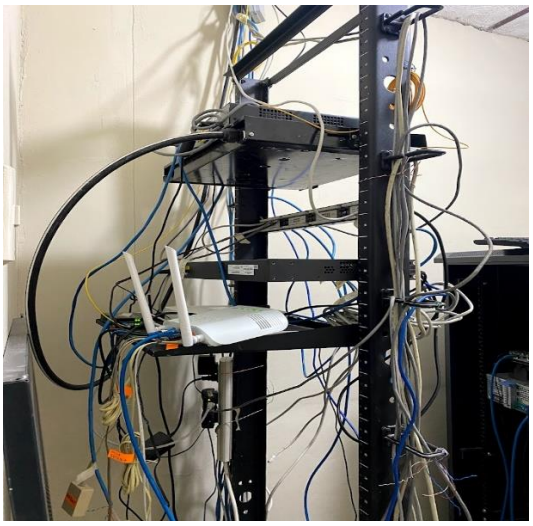

Ilustración 15 Cableado en el Swicth Principal

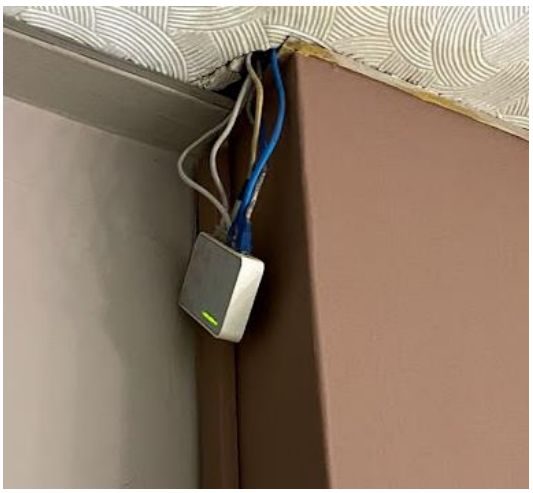

Ilustración 16 Ubicación de los repetidores

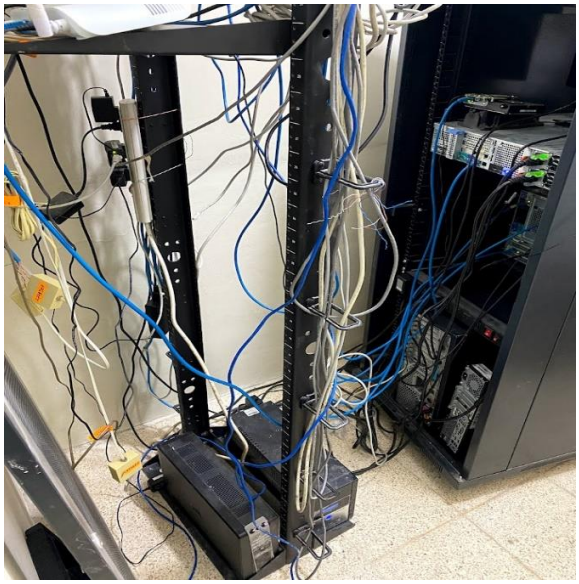

Ilustración 17 Muestra del cableado hacia el Servidor Principal

Ilustración 18 Ubicación de los Routers

Ilustración 19 Análisis de La Red

Resultado del escaneo a la Red

Sev	Name	Family	Count
MEDIUM	SMB Signing not required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	SMB (Multiple Issues)	Windows	6
INFO	Microsoft Windows (Multiple Issues)	Windows	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	Nessus Scan Information	Settings	1
INFO	OS Identification	General	1
INFO	OS Identification and Installed Software Enumeration over SSH v2 (U...	Misc.	1
INFO	OS Security Patch Assessment Available	Settings	1
INFO	Target Credential Issues by Authentication Protocol - No Issues Found	Settings	1
INFO	Target Credential Status by Authentication Protocol - Valid Credenti...	Settings	1
INFO	VMware ESX/GSX Server detection	Service detection	1

Plugin ID: 11936

Ilustración 20