UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

NOVIEMBRE 2020 – MAYO 2021

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

ANÁLISIS DE LAS VULNERABILIDADES DE LAS REDES INALÁMBRICAS DE RG INTELLIGENT DE LA PARROQUIA LA UNIÓN, PARA MEJORAR LA DISPONIBILIDAD DEL SERVICIO

EGRESADO:

JUAN CARLOS GAIBOR MANZO

TUTOR:

ING. HUGO GUERRERO TORRES

AÑO 2021

INTRODUCCIÓN

El presente caso de estudio trata sobre el análisis de las vulnerabilidades de la red inalámbrica de la empresa RG INTELLIGENT de la parroquia la Unión.

Las redes inalámbricas de área local (WLAN) tienen una labor cada vez más fundamental en las comunicaciones del mundo de hoy. Debido a su fácil instalación y conexión, se han transformado en una buena elección para ofrecer conectividad en sitios donde es difícil o imposible dar el servicio con una red cableada. La fama de estas redes ha aumentado tanto que los fabricantes de computadoras y tarjetas madre están incorporando dispositivos para acceso a WLAN en sus equipos; tal es el caso de Intel, que fabrica el chipset Centrino para computadoras portátiles.

La problemática más grande de este tipo de redes es en cuanto a la seguridad ya que cualquier persona con los conocimientos suficientes en hackeo de redes inalámbricas podría vulnerar la seguridad de la red, robaría información vital de la empresa y podría afectar la velocidad del internet.

Por este motivo el objetivo de este caso de estudio es proporcionar un análisis de las vulnerabilidades de la red inalámbricas de la empresa RG INTELLIGENT ubicada en la parroquia la Unión, para mejorar la disponibilidad del servicio, aplicando teorías, metodología, métodos e instrumentos de investigación.

Este análisis se lo realizo para comprobar si la entidad está expuesta, esta investigación está basado en la recopilación de información después de haber realizado un análisis exhaustivo a la red de la empresa RG INTELLIGENT, poder identificar sus vulnerabilidades.

Se escaneo la red utilizando la herramienta Nessus que busca vulnerabilidades en la red, este trabajo estará basado en toda la información que se haya recopilado, tabulado y compilado después de haberse realizado visitas técnicas, observación directa al entorno de la red de forma implícita con el fin de identificar sus fallas.

Después de haber realizado el respectivo análisis a la red se encontró una vulnerabilidad la cual es SMB Signing not required, para solucionar este inconveniente se debe aplicar la firma de mensajes en la configuración del host, ser observo la red de la empresa y se constató que el router y el switch estaban sobre una mesa al aire libre expuestos a la suciedad y a la manipulación de personas ajenas al negocio, los cables estaban

desordenados, los equipos no estaban conectados a un regulador de voltaje o sistema de respaldo de energía y además los equipos les hacía falta un mantenimiento ya que tenían polvo. Se recomienda al dueño del negocio que adquiera un rack, también se recomienda que adquiera un regulador de voltaje o un ups y cada cierto tiempo dar mantenimiento a sus equipos de red.

DESARROLLO

Las redes inalámbricas son utilizadas por las mayorías de las personas hoy en día debido a su sencilla manipulación y conectividad entre los diversos dispositivos. El aumento de las redes inalámbricas y la acogida de las conexiones Wifi; hacen más fácil la manera de detectar una red inalámbrica.

Estas redes se caracterizan debido a que no hacen uso de un cableado de forma estructurada estas se utilizan por medio de conexiones que son por medio de ondas electromagnéticas. La variedad de las comunicaciones inalámbricas radica en el desplazamiento en diversas áreas logrando por medio de esto sostener la conexión como si se hiciera de una forma cableada, dicha conexión deber están en el perímetro que contiene la cobertura de la red.

Las redes inalámbricas son vulnerables a ataques por ejemplo un usuario no autorizado podría entrar a la red sin autorización con el fin de espiar información y robar información valiosa de esa empresa, para ello debemos estar protegidos ante cualquier posible ataque.

El presente caso de estudio se lo realizo en la empresa RG INTELLIGENT ubicada en la Parroquia la Unión, la entidad se dedica a la reparación, mantenimiento de computadoras, ventas de computadoras, impresoras y demás componentes electrónicos.

Como objetivo general de este caso de estudio es proporcionar un análisis de las vulnerabilidades de la red inalámbricas de la empresa RG INTELLIGENT ubicada en la parroquia la Unión, para mejorar la disponibilidad del servicio.

Para lograr este objetivo se debe realizar un análisis de vulnerabilidad en la red inalámbrica de la entidad, hacer visitas técnicas para observar el entorno de la red.

Se desea conocer si en la red inalámbrica de la empresa RG INTELLIGENT los medios tecnológicos que utilizan para la conexión son seguros y cumplen a cabalidad sus funciones de forma adecuada, donde se quiere determinar si existen fallos de conectividad, conocer los procesos de transmisión de datos.

Las redes inalámbricas son aquellas redes conformadas por dispositivos electrónicos capaces de intercomunicarse entre sí o con otra red (como Internet), sin la necesidad de usar cables que las conecten. Existen muchos tipos de redes inalámbricas cuya diferencia radica en algunos aspectos como la arquitectura, tecnología o estándares de comunicación entre otros, como por ejemplo las redes de área local inalámbricas (WLAN) o redes wifi. (Incibe, 2019).

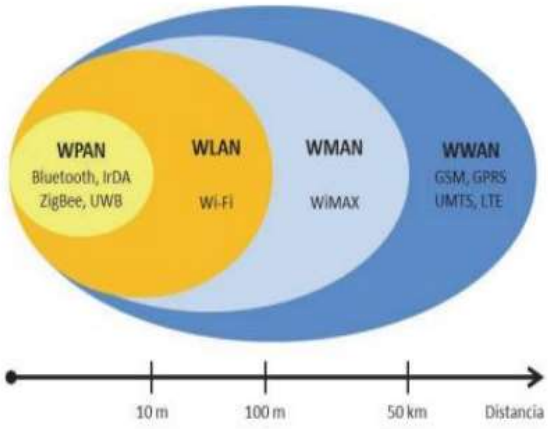
Las redes inalámbricas están compuestas por equipos de cómputo que están interconectados, por medio de ondas de radio o como también de infrarrojo. Estas redes inalámbricas son similares con las redes cableadas ya que tienen distintos rangos de cobertura entre los dos, la red inalámbrica contara con segmentos que poseerán esta característica, estas redes inalámbricas se da el caso de que en variado de los casos pueden tal vez estar conectada de esta red inalámbrica se descubra de que está conectada a otra por medio con la conexión de un cableado. Las redes inalámbricas pueden ser híbridas, dependiendo de si se estudia un segmento de red o la totalidad de la misma. (GUSTAVO, 2019).

Las redes inalámbricas son una tecnología que permite la conexión inalámbrica de dispositivos y equipos que se encuentran en una misma red. Los dispositivos habilitados con Wifi pueden conectarse entre ellos o tener acceso a internet pasando por un punto de acceso de red inalámbrica. (CISET, 2021).

Este tipo de redes permiten que los dispositivos que se encuentre dentro del perímetro que cubra el dispositivo acceder a la red, esto es lo que hace que estas tengan más acogidas todavía en el mercado. Las redes inalámbricas abarcan 4 grandes grupos que son:

- Redes inalámbricas de área personal (WPAN).
- Redes inalámbricas de área local (WLAN).
- Redes inalámbricas de áreas metropolitanas (WMAN).
- Redes inalámbricas de área amplia (WWAN).

Ilustración 1: Tipos de redes inalámbricas



Fuente: (CHULLI PAREDES JORGE VIDAL, 2019)

Las redes inalámbricas se clasifican en las siguientes subdivisiones:

Wireless PAN (Personal Area Network): Conecta dispositivos con una distancia considerada de metros, como es el caso del bluetooth, una de las tecnologías que más se utilizan hoy en día.

Es una red que integra todos los dispositivos en el entorno local y cercano al usuario, es decir que la componen de todos los aparatos que están cerca del mismo. Su característica principal de este tipo de red es que le permite al usuario establecer una comunicación con sus dispositivos de forma sencilla, práctica y veloz. (Marker, 2020).

Ilustración 2: Wireless PAN

Fuente: https://www.alegsa.com.ar/Dic/pan.php

Las Local Area Network (LAN): o Redes de Área Local en español, son el tipo de red más extendido, usándose primordialmente para el intercambio de datos y recursos entre las computadoras ubicadas en un espacio pequeño, como un edificio o grupo de ellos, como por ejemplo instituciones educativas o gubernamentales y hasta en nuestros propios hogares. (Marker, 2020).

Ilustración 3: Wireless LAN

Fuente: (CHULLI PAREDES JORGE VIDAL, 2019)

Wireless WMAN (Wireless Metropolitan Network): Las redes inalámbricas de área metropolitana (Wman) son un tipo de red inalámbrica que se instala dentro de una misma área metropolitana. Es decir, el objetivo es establecer distintas conexiones inalámbricas dentro de ese espacio. Esto quiere decir que van a tener un alance de varios kilómetros. Es, como mucho más compleja que una simple red wifi doméstica o en un centro comercial. (Jiménez, 2019).

Las redes inalámbricas de área metropolitana (WMAN) forman parte del tercer grupo de redes inalámbricas. Las WMAN se basan en el estándar IEEE 802.16, denominado WiMAX (Worldwide Interoperability for Microwave Access). WiMAX es una tecnología de comunicaciones con arquitectura punto a multipunto orientada a proporcionar una alta velocidad de transmisión de datos a través de redes inalámbricas de área metropolitana. Esto permite que las redes inalámbricas LAN más pequeñas puedan ser interconectadas por WiMAX creando una gran WMAN. Resulta que la creación de redes entre ciudades puede lograrse sin la necesidad de cableado costoso.

Ilustración 4: Wireless WMAN

Fuente: (CHULLI PAREDES JORGE VIDAL, 2019)

Wireless WAN (Wide Area Network): Es aquella red de equipos informáticos muy extensa, por ejemplo, las redes que existen en universidades, edificios, entre otros organismos tanto públicos como privados. Estas redes utilizan las redes tanto telefónicas o las conocidas líneas muertas.

El acrónimo WWAN hace referencia a grandes redes inalámbricas que les permiten a los dispositivos móviles conectarse a internet. Estas también comprenden las redes LTE. Las WWAN que están a cargo de operadores móviles que utilizan antenas móviles. (Ecom, 2019).

Ilustración 5: Wireless WAN

Fuente: (CHULLI PAREDES JORGE VIDAL, 2019)

Las redes Wifi poseen las siguientes ventajas:

- Las personas al usar una red WIFI se sienten muy cómodas porque pueden hacer uso de la misma, varios dispositivos dentro de una zona limitada, en comparación con una red LAN.
- Si comparamos un smartphone con una red WIFI, la red WIFI puede ser utilizada en cualquier país del mundo, mientras que el smartphone es restringido el uso en algunos países.
- En la infraestructura las redes WIFI no se gasta dinero mientras que en las redes LAN los gastos son muy elevados.
- Las redes WIFI usan la banda 2,4 GHz, es decir no necesita consentimientos de regulación.

Las desventajas de las redes WIFI son las siguientes:

- Problemas de redes colapsadas.
- En cuanto a su seguridad, son muy vulnerables, porque son las redes wifi las que son constantemente atacadas por los hackers.
- La intensidad de la red en ocasiones es mala porque son muchos dispositivos que se conectan a la red. (CHULLI PAREDES JORGE VIDAL, 2019).

Estándar IEEE 802.11: es un estándar para las redes inalámbricas definido por el Institute of Electrical and Electronics Engineers (IEEE). Se trata de un instituto de investigación y desarrollo sin fines de lucro, con un gran reconocimiento y prestigio,

cuyos miembros pertenecen a decenas de países entre profesores y profesionales de las nuevas tecnologías.

IEEE 802.11 es un estándar que continúa evolucionando, debido a que existen diversos grupos de investigación, trabajando en paralelo para mejorar el estándar, a partir de las especificaciones originales. (Torres, 2017)

Fue implementada en el año 1997, cabe mencionar que este estándar fue pionero en transferir información bajo velocidades entre 1 y 2 Mbit/s con una frecuencia de 2,4 GHz lo que limitaba ejecutar aplicaciones corporativas. (FLORES, 2019)

Básicamente, la atracción por estas redes inalámbricas ha posibilitado su rápida evolución y poner en el mercado tres estándares derivados del original. Los tres estándares derivados que existen en la actualidad en el mercado son:

IEEE 802.11g: trabaja en la banda de frecuencia de 2,4 GHz y proporciona velocidades de hasta 54 Mbps. Por lo tanto, los dispositivos que utilizan este estándar operan en la misma radiofrecuencia y tienen una magnitud de hasta 802.11b, pero con un ancho de banda de 802.11a. (Medios de red, 2019).

IEEE 802.11n: Este estándar comenzó a operar en 2008 aunque se definió en 2004. Su velocidad asciende a los 600 Mbps en conexiones como máximo de 3×3 (3 antenas). Utiliza de manera simultánea las bandas de 2,4 GHz y 5 GHz. Fue el primero en implementar la tecnología MIMO (Multiple Input – Multiple Output) que permite utilizar varios canales a la vez para el envío y recepción de datos con hasta 3 antenas.

Aún no se ha llegado a tasas de velocidad comparables a cableado LAN, pero el poder usar ambas frecuencias con un mismo punto inalámbrico toda a los dispositivos de gran cobertura. (Castillo, 2020).

Tabla 1: Estándares IEEE 802.11

Estándar	Tasa de transmisión (Mbps)	Tasa de recepción (Mbps)	Paquetes perdidos (%)	Paquetes transmitidos
802.11b	1.00	0.99	0	227
	2.00	1.99	0	453
	3.00	2.94	0.3	680
	4.00	3.89	8.4	906
	3.80	3.78	2.1	861
802.11g	1.00	0.99	0	227
	2.00	1.99	0	453
	4.00	3.99	0	906
	6.00	5.98	0.6	1359
	7.00	6.80	7.6	1586
	6.50	6.48	2.4	1472
802.11n	1.00	1.00	0	227
	3.00	2.99	0	680
	5.00	4.98	0	1133
	8.00	7.99	0	1812
	12.00	11.72	8.4	2718
	11.00	10.98	1.4	2491

Fuente: (Cristopher Stalin Caiza Páez, 2019)

La seguridad de las redes inalámbrica es un proceso de diseño, implementación y garantía de la seguridad en una red informática inalámbrica. Es un subconjunto de seguridad de red que añade protección para una red inalámbrica de computadoras. (DELGADO, 2019).

Las redes inalámbricas son amenazadas por los mismos riesgos que las redes cableadas agregando también riesgos específicos del ámbito inalámbrico. En la siguiente lista se incluyen algunos de los más comunes:

- Eavesdropping**.** Cuando alguien no autorizado utiliza alguna herramienta (generalmente antenas de gran alcance) para capturar de forma pasiva el tráfico inalámbrico. Este tráfico le sirve para poder espiar información (en caso de que no vaya cifrada) y para detectar patrones de comportamiento.
- Denegación del Servicio (Denial of Service). Cuando la red inalámbrica queda incapacitada para dar el servicio, por ejemplo, cuando una persona no autorizada

inyecta peticiones masivas de asociación a los AP dejándolos incapacitados para responder a las peticiones de los clientes legítimos.

- Man-in-the-middle. Cuando una persona no autorizada se coloca en medio de la comunicación inalámbrica entre emisor y receptor, suplantando a una de las partes y haciéndole creer a la otra que está hablando con el comunicante legítimo. Desde ese punto, se pueden ejecutar multitud de ataques posteriores (captura de credenciales, de tráfico, etc.).
- MAC Spoofing. Los AP pueden tener configurada una lista de direcciones MAC (Media Access Control) permitidas. A pesar de ello, alguien no autorizado puede suplantar una dirección MAC autorizada para lograr tener el acceso.
- Acceso de dispositivos no autorizados que están conectados al dispositivo cliente autorizado y que a través de él pueden lograr acceso a la red inalámbrica y por tanto a la red cableada de la entidad pudiendo introducir software dañino. (Castaño, 2018).

Seguridad física de una red: Otra vulnerabilidad a la que hay que prestarle atención es la seguridad física de los dispositivos. Si la red quedase expuesta a riesgos físicos, un atacante puede denegar el uso de dichos recursos.

Las amenazas físicas que existen son las siguientes:

- **Amenazas de hardware:** daños físicos a los equipos de la red como los routers, switches, servidores, cableado y estaciones de trabajo.
- **Amenazas ambientales:** temperatura o humedad.
- **Amenazas eléctricas:** picos de voltaje, suministro de voltaje insuficiente, omitir el uso de reguladores de voltaje y caída total de la alimentación.
- **Amenazas de mantenimiento:** manejo ineficaz de los componentes eléctricos clave (descarga electrostática), poca limpieza a los equipos, falta de repuestos críticos, cableado y etiquetado ineficientes. (Guillermo, 2020)

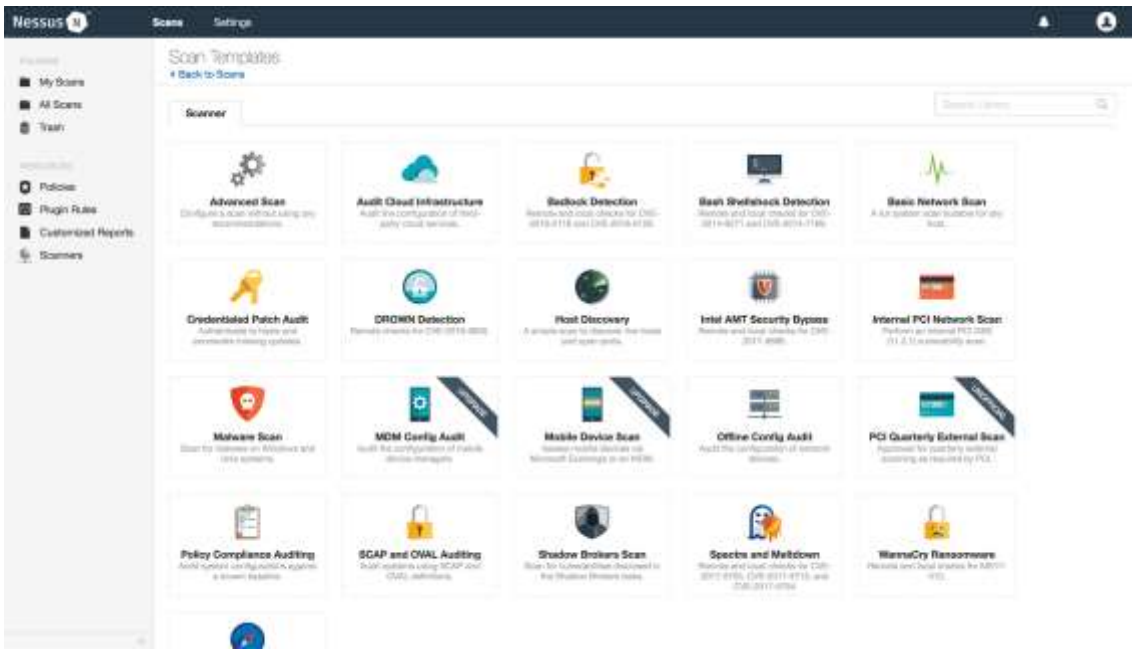
Herramientas utilizadas para escanear la red

Nessus: es un escáner de vulnerabilidades, esta herramienta de alto nivel detecta amenazas en tiempo real y gracias a su precisión, evita la generación de falsos positivos.

Nessus prevé eficientemente los ataques de red identificando las debilidades y errores de configuración que pueden ser utilizados para permitir el ingreso de amenazas al sistema.

Nessus es un programa usado a nivel mundial para prevenir ataques de red, identificación de vulnerabilidades y detección de problemas de configuración. Este scanner es usado por al menos 1 millón de usuarios en todo el planeta, lo que lo convierte en el líder mundial de evaluación de la vulnerabilidad, configuración de la seguridad y efectuar las normas de seguridad. (gb-advisors, 2021).

Ilustración 6: Software Nessus



Elaborado por: Juan Carlos Gaibor Manzo

Observación de la ubicación de equipos de red

Ilustración 7: Ubicación de los equipos de red

Elaborado por: Juan Carlos Gaibor Manzo

En la imagen se puede apreciar que el router y el switch de la empresa están sobre una mesa al aire libre expuestos a la suciedad y a la manipulación de personas ajenas a la entidad, se puede ver también que los cables están desordenados, también se aprecia que los equipos no están conectados a un regulador de voltaje o sistema de respaldo de energía y se pudo ver que los equipos tenían falta de mantenimiento ya que tenían polvo.

A continuación, se detalla los dispositivos de red que se encuentran en la empresa:

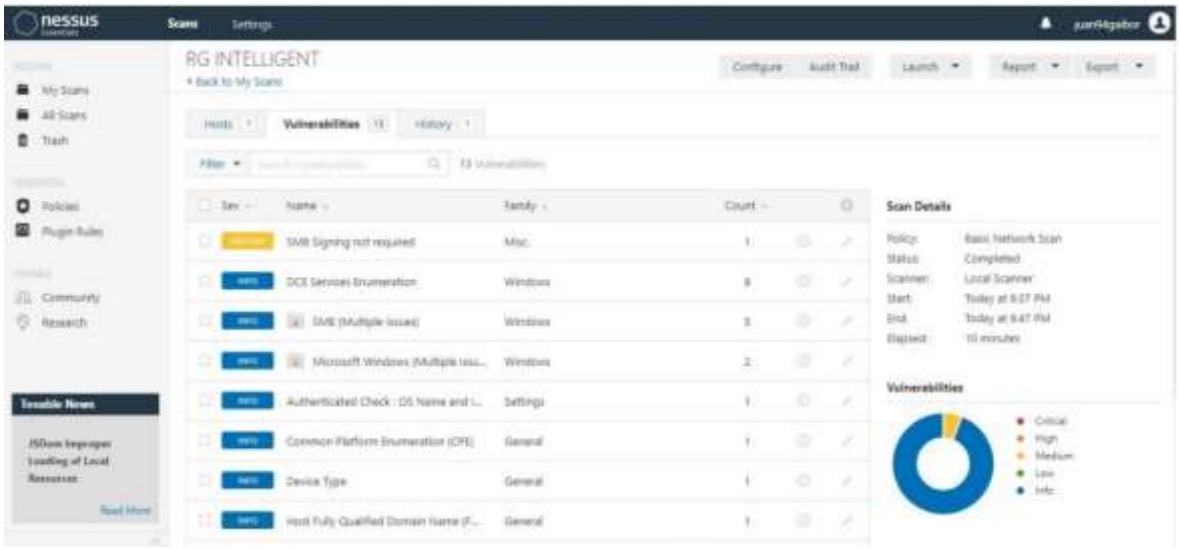
Tabla 2: Equipos de red

Dispositivos	Características
Router	Huawei HG8245H
Switch	Zyxel Network

Elaborado por: Juan Carlos Gaibor Manzo

Análisis de vulnerabilidades en Nessus

Ilustración 8: Análisis de vulnerabilidades en la red



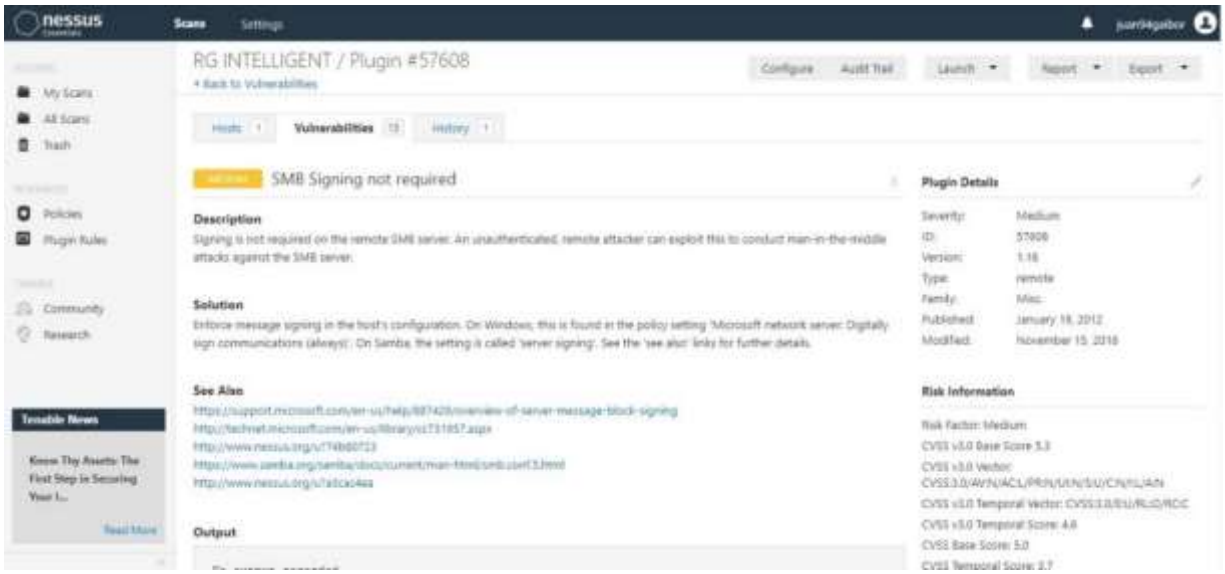
Elaborado por: Juan Carlos Gaibor Manzo

Luego de realizar el escaneo de las vulnerabilidades con la herramienta Nessus se hizo una comparación de los resultados y de acuerdo a los niveles de gravedad se muestran por colores, se procede a examinar los niveles de severidad y complejidad con que son definidas por esta herramienta en relación a la inseguridad informática encontrada.

Se realizo el análisis de vulnerabilidad a la red inalámbrica con la herramienta Nessus y se encontró una vulnerabilidad de nivel medio el cual es SMB Signing not required, no representa ningún peligro según la herramienta lo indica.

En redes de computadoras, Server Message Block (SMB), es una versión del cual también se conoció como Common Internet File System (CIFS), funciona como un protocolo de red de capa de aplicación usando principalmente para proveer acceso compartido a los archivos, impresoras y puertos serie y comunicaciones entre nodos en una red. También provee un mecanismo de comunicación entre procesos autenticado. La mayoría del uso de SMB involucra computadoras que funcionan con el sistema operativo Microsoft Windows, donde se conocía como "Red de Microsoft Windows" antes de la introducción de Active Directory. Los servicios de Windows correspondientes son LAN Manager Server y LAN Manager Workstation. (Ivan, 2019)

Ilustración 9: Vulnerabilidad (SMB Signing not required)



Elaborado por: Juan Carlos Gaibor Manzo

CONCLUSIONES

Después de haber realizado el caso de estudio sobre análisis de las vulnerabilidades de las redes inalámbricas de la empresa RG INTELLIGENT de la parroquia la Unión se evidencio que la red si posee vulnerabilidades, los cuales podrían ser utilizados por hackers o ladrones informáticos con el objetivo de tener acceso a la red.

Mediante la observación se pudo constatar la ubicación de los equipos de la red, se encontraban sobre una mesa al aire libre expuestos a la suciedad y a la manipulación de personas ajenas a la entidad, también los cables estaban desordenados, los equipos no estaban conectados a un regulador de voltaje o sistema de respaldo de energía, esto los hace susceptibles de malfuncionamiento en caso de variaciones eléctricas además de no contar con sistema de respaldo de energía los hace vulnerables en caso de fallas en el sistema de suministro eléctrico y se pudo ver que los equipos tenían falta de mantenimiento ya que tenían polvo. Se recomienda, reinstalar estos equipos en un rack cerrado y estructurar los cables en canaletas, también que la empresa utilice regulador de voltaje o un ups y cada cierto tiempo dar mantenimiento a sus equipos de red.

Se observo que los ordenadores de la empresa utilizan como sistema operativo Windows 10 y el antivirus que tienen instalados los ordenadores es Windows defender el cual viene instalado por defecto en el sistema operativo, esto ha ayudado a prevenir el acceso no adecuado de software maliciosos o programas que pueden espiar el contenido de la red, esto fue comprobado por la herramienta Nessus al no detectar estas vulnerabilidades.

Se realizo el análisis de vulnerabilidad a la red inalámbrica con la herramienta Nessus y se encontró una vulnerabilidad de nivel medio el cual es SMB Signing not required, no representa ningún peligro según la herramienta Nessus lo indica, para solucionar este inconveniente se debe habilitar la opción: “firmar digitalmente las comunicaciones (Digitally sign communications)” en las políticas de seguridad local del servidor, esta vulnerabilidad es aprovechada por el protocolo SMB, en el puerto 445 del servidor, comúnmente utilizado para compartir archivos, impresoras, redes y otros recursos.

Referencias

Castaño, J. M. (2018). *Aplicación de las políticas de seguridad del ENS en redes inalámbricas WiFi.* Vigo.

Castillo, J. A. (07 de 03 de 2020). *Profecional review*. Obtenido de https://www.profesionalreview.com/2020/03/07/wlan-que-es/

CHULLI PAREDES JORGE VIDAL, E. P. (2019). *ANÁLISIS DE VULNERABILIDAD DE REDES INALÁMBRICAS CON .* Milagro: Ecuador.

CISET. (2021). https://www.ciset.es/glosario/496-wifi-red-inalambrica.

Cristopher Stalin Caiza Páez, R. A. (2019). Evaluación del desempeño de la tecnología wifi en concordancia con los estándares IEEE 802.11 b/g/n en el interior de una cámara anecoica para la banda de 2.4 GHz. *Reci*, 11.

DELGADO, R. V. (2019). *ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS EN EL LABORATORIO DE TELECOMUNICACIONES DE LA CARRERA DE INGENIERÍA EN COMPUTACIÓN Y REDES.* JIPIJAPA.

Ecom. (21 de 01 de 2019). Obtenido de https://www.ecom-ex.com/es/seguridad-intrinseca/glosario/termino/wwan/

EcuRed. (2019). Obtenido de https://www.ecured.cu/Est%C3%A1ndar_inal%C3%A1mbrico_802.11b

FLORES, D. R. (2019). *DISEÑO E IMPLEMENTACIÓN DE UNA RED WIRELESS CON EL ESTÁNDAR IEEE 802.11AC CON CALIDAD DE SERVICIO Y SEGURIDADES PARA LA ADMINISTRACIÓN DEL SERVICIO DE COMUNICACIÓN DE UNA EMPRESA DE VENTA DE AUTOMÓVILES, BASADO EN TECNOLOGÍA MESH CON EQUIPOS UBIQUITI Y MI.* Guayaquil.

gb-advisors. (2021). *gb-advisors*. Obtenido de https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/

Guillermo. (24 de Noviembre de 2020). *Ingenieria System*. Obtenido de http://www.ingenieriasystems.com/2017/10/Categorias-de-amenazas-la-seguridad-de-red-Seguridad-fisica-Tipos-de-vulnerabilidades-de-seguridad-CCNA1-V5-CISCO-C11.html#:~:text=Las%20cuatro%20clases%20de%20amenazas,demasiado%20h%C3%BAmedo%20o%20demasiado%20sec

GUSTAVO, J. C. (2019). *IMPLEMENTACIÓN DE UN SOFTWARE LIBRE PARA MEJORAR LAS VULNERABILIDADES DE REDES INALÁMBRICAS EN LA SEGURIDAD DE INFORMACIÓN DE LA ESCUELA DE INGENIERÍA DE SISTEMAS DE LA ULADECH - CHIMBOTE;2017.* CHIMBOTE: PERU.

Incibe. (2019). *Seguridad en redes wifi.*

Ivan. (1 de Octubre de 2019). *0xsecure*. Obtenido de https://0xsecure.blogspot.com/2019/10/smb-signing-not-required-firma-smb-no.html?m=1

Jiménez, J. (29 de 11 de 2019). *RZ Redes Zone*. Obtenido de https://www.redeszone.net/tutoriales/redes-wifi/wman-wwan-diferencias-usos-redes-inalambricas/

Marker, G. (10 de 07 de 2020). *Tegnologia + informatica*. Obtenido de https://www.tecnologia-informatica.com/tipos-de-redes-informaticas-lan-wan-man-wlan-wman-wwman-san-pan/

Medios de red. (2019). Obtenido de http://itroque.edu.mx/cisco/cisco1/course/module4/4.2.4.4/4.2.4.4.html

Torres, J. J. (2017). *Diseño de una red Wi-Fi para la E.S.I. .*

ANEXOS

Anexo 1: Lugar donde se hiso el caso de estudio

Elaborado por: Juan Carlos Gaibor Manzo

Ficha de Observación

Nombre de la empresa	RG Intelligent
Nombre del observador	Juan Carlos Gaibor Manzo
Elemento a observar	Red de la entidad
Fecha de observación	05/03/2020

Objetivo: Realizar un análisis de las vulnerabilidades de las redes inalámbricas de RG INTELLIGENT de la parroquia la unión, para mejorar la disponibilidad del servicio.

N^0	**Aspecto a observar**	**Si**	**No**	**Observación**
1	La empresa dispone de router	x		Marca Huawei HG8245H
2	Dispone de switch la red de la empresa	x		Marca Zyxel Network
3	Los equipos de red están conectados a reguladores de voltaje o ups		x	No la entidad no ha adquirido reguladores de voltaje o ups.
4	Los ordenadores de la institución poseen sistema operativo.	x		Sistema operativo Windows 10
5	Las computadoras de la empresa tienen instalados antivirus	x		Tienen instalado el antivirus que viene por defecto en el sistema operativo.
6	Dispone de protección en el cableado de la red.		x	Los cables no poseen protección
7	El firewall de los ordenadores están actualizados.	x		
8	El cableado cuenta con protección.		x	Los cables de la red no se encuentran protegidos.
9	Se encontraron vulnerabilidades en la red de la empresa	x		Se encontró una vulnerabilidad de nivel medio.

Anexo 2: Solicitud a la Empresa

UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
DECANATO

Babahoyo, febrero 22 de 2021
D-FAFI-UTB-023-UT-2021

Señor
Cristóbal Roberto Guayaquil Gonzabay
GERENTE DE LA EMPRESA RG INTELLIGET
Ciudad. –

De mis consideraciones:

La Universidad Técnica de Babahoyo y la Facultad de Administración, Finanzas e Informática (FAFI), con la finalidad de formar profesionales altamente capacitados busca prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El Señor **GAIBOR MANZO JUAN CARLOS,** con cédula de identidad No. 120457024-4, Estudiante de la Carrera de Ingeniería en Sistemas, matriculado en el proceso de titulación en el periodo Noviembre 2020 – Mayo 2021, trabajo de titulación modalidad Estudio de Caso para la obtención del grado académico profesional universitario de tercer nivel como **INGENIERO EN SISTEMAS.** El Estudio de Caso: **ANALISIS DE LAS VULNERABILIDADES DE LAS REDES INALAMBRICAS DE RG INTELLIGENT DE LA PARROQUIA LA UNION, PARA MEJORAR LA DISPONIBILIDAD DEL SERVICIO.**

Es por esta razón, solicito a usted, si es posible se sirva autorizar el permiso respectivo para que el Señor Gaibor pueda desarrollar la investigación en la institución de su acertada dirección.

Por su gentil atención al presente, se extiende el agradecimiento institucional.

Atentamente.

Lcdo. Eduardo Galeas Guijarro MAE.
DECANO

PROGRAMACION VENTA Y MANTENIMIENTO DE PC
SERVICIO PROFESIONAL
RG Intelligent
Ing. Roberto Guayaquil
TELF: 0998187302
LA UNIÓN - BABAHOYO

08/03/2021
HORA: 11:42 AM

c.c Archivo

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Mercedes Soto Valencia	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

Elaborado por: Juan Carlos Gaibor Manzo