UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS

TEMA

ANÁLISIS DE LAS AMENAZAS Y RIESGOS DE LA RED INALÁMBRICA DE LA EMPRESA "FARMADESCUENTO SA" DE LA CIUDAD DE VINCES

TUTORA:

ING. NARCISA CRESPO

EGRESADO

OSCAR STALIN BRIONES MORA

PERIODO

SEPTIEMBRE- FEBRERO

TABLA DE CONTENIDO

INTRODUCCIÓN

En Ecuador se ha dado un incremento enorme de redes Wireless Fidelity (Wi-Fi), debido a que la sociedad avanza paulatinamente gracias a los servicios que proveen los equipamientos físicos y lógicos encaminados a las telecomunicaciones, esta línea contribuye de manera razonable y explícita, con desarrollo tecnológicos e innovadores del entorno académico, social y cultural.

Es por eso que se pretende a través de esta indagación aportar con un contenido equitativo que se encuadra en el análisis de amenazas y vulnerabilidades en la red Wi-Fi de la empresa Farmadescuento S.A de la ciudad de Vinces, irrumpiendo en teorías y métodos de investigación basado en la técnica de observación, análisis e interpretación de los resultados.

Se desea conocer si en la red inalámbrica de la empresa Farmadescuento S.A los medios tecnológicos que utilizan para la conexión son seguros y cumplen a cabalidad sus funcionen de forma precisa, donde se quiere determinar si existen fallos de conectividad, conocer los procesos de transmisión de datos y la velocidad.

La investigación estará basada en la recopilación de información después de un análisis exhaustivo que se realice en la empresa Farmadescuento SA, para así Distinguir la dimensión del tráfico en las principales conexiones de troncales web remotas.

Con los resultados obtenidos se elaboró un análisis con alto contenido técnico para así verificar los niveles de seguridad de la red Wi-Fi de la empresa Farmadescuento, para lo cual se va a utilizar varios softwares con el afán de adquirir una radiografía de los sistemas de telecomunicaciones o los métodos que se emplean para la detección de riesgos y así también verificar las vulnerabilidades de la red inalámbrica.

Este caso de estudio se vincula con la sublínea de investigación de los procesos de transmisión de datos y telecomunicaciones, mediante un escaneo a la red inalámbrica de la empresa Farmadescuento S.A de la ciudad de Vinces.

DESARROLLO

En la actualidad las empresas que usan más de un computador en sus operaciones y rutinas diarias se encuentran interconectadas y permiten que las computadoras, equipos móviles y demás artefactos electrodomésticos se encarguen de procesar todos los volúmenes de datos que transitan en la red.

El escenario planteado corresponde a la red inalámbrica de la empresa Farmadescuento S.A, es así que casi todas las sucursales de la empresa y al igual que todas las personas que trabajan en ella, dependen de alguna manera de las Tecnologías de Información y Comunicación (Tics), como una herramienta muy esencial para cumplir con las actividades propuestas diariamente, debido a esto la mayor parte del tiempo los usuarios pueden enfrentar amenazas y vulnerabilidades en la transmisión de los datos, lo cual es el objeto de esta investigación.

La Seguridad de la Información tiene como principal objetivo proteger el almacenamiento y procesamiento de la información tomando las medidas correspondientes, no obstante, en cada caso es diferente dependiendo la entidad a donde se va aplicar los mecanismos de seguridad. (Universidad de San Carlos Guatemala, 2014, págs. 13,14)

Es muy importante los activos que deben estar protegidos y estos a su vez se encuentran en los siguientes componentes:

- Equipos: no se pueden robar los equipos y peor aún introducir equipos no autorizados.
- Aplicaciones: instalar software para realizar el trabajo y no otro software que no sean necesarios, para no quebrantar la seguridad.
- Datos: deben ser exclusivos solo de la empresa.
- Comunicaciones: se deben utilizar medios seguros para el intercambio de información. (Universidad de San Carlos Guatemala, 2014, pág. 14)

Redes Inalámbricas

La redes inalámbricas se comunican por medios no guiados por medio de ondas electromagnéticas se emplea la transmisión y recepción a través de antenas, normalmente estos dispositivos tienen entre 1 y 4 antenas ya que 1 se usan para la emisión y las otras para la recepción pero normalmente la mayoría permite actuar de ambos modos (Andreu, 2011, pág. 212).

Las redes inalámbricas poseen las siguientes características:

- Fácil instalación de la red.
- Permite una movilidad dentro del radio de recepción de la señal.
- Reducción en los costos de mantenimiento.
- Accesibilidad para casi todos los dispositivos.
- Es la solución para las zonas a donde no llega el cableado. (Andreu, 2011, pág. 212)

Es por eso que es muy importante contar con equipos capaces de solventar las necesidades de la empresa y para que los datos fluyan de forma precisa y sobre todo segura porque hoy en día muchas empresas pierden millones por no contar con dispositivos o un personal capaces de evitar ciberataques realizados muchas veces desde la red inalámbrica de la empresa. (Andreu, 2011)

Normas de red inalámbrica 802.11

En el ámbito de la innovación remota, el término Wi-Fi es sinónimo de acceso remoto en general, a pesar del hecho de que es una marca comercial explícita que posee Wi-Fi Alliance, una reunión dedicada a afirmar que los elementos de Wi-Fi cumplir con el conjunto IEEE de 802.11 modelos remotos.

Estas pautas, con nombres como 802.11b y 802.11ac, incorporan un grupo de detalles que se iniciaron durante la década de 1990 y continúan desarrollándose en la actualidad. El estándar 802.11 codifica mejoras que amplían la ejecución remota y el rango, al igual que la accesibilidad de las nuevas frecuencias. Asimismo, abordan los nuevos avances que disminuyen la utilización de la vitalidad.

Los nombres de estos puntos de referencia hacen una sopa de letras, lo que hace que todo sea aún más confuso a causa de que no están organizados en orden. Para ayudar a iluminar la circunstancia, aquí hay una actualización de estos medidores de capa física dentro de 802.11, solicitud secuencial grabada hacia atrás, con las pautas más actualizadas en la mejor y las más experimentadas. Después de eso hay una representación de los medidores que todavía están en proceso. (Escudero, 2016)

Tabla 1 Normas de red 802.11 1

802.11ah	Según Shaw (2018) es llamado Wi-Fi HaLow, 802.11ah caracteriza la actividad de permitir sistemas absolutos en grupos de recurrencia por debajo de 1 GHz (normalmente la banda de 900 MHz), salvo los grupos de White Space TV. La motivación detrás de 802.11ah es ampliar los sistemas de Wi-Fi extendidos que están progresivamente alejados en el espacio de 2.4GHz y 5GHz, con velocidades de información de hasta 347Mbps. Además, el estándar espera tener una utilización de menor vitalidad, valiosa para los dispositivos de Internet de las cosas con las que hablar con un montón de vitalidad. Sea como sea, podría lidiar con los avances de Bluetooth en el hogar debido a sus menores necesidades de control. La convención se confirmó en septiembre de 2016 y se distribuyó en mayo de 2017.
802.11ad	Avalado en diciembre de 2012, 802.11ad es rápido: puede dar hasta 6.7 Gbps de tasa de información en la recurrencia de 60 GHz, aunque tiene un costo de separación de solo 3.3 metros desde el pasaje (Shaw, 2018).
802.11ac	Los router`s domésticos actuales son compatibles con 802.1ac y trabajan en una frecuencia de 5 GHz. Con información variada, Algunos proveedores consolidan impulsos que repiten la asistencia. de 2.4 GHz a través de 802.11n, lo que refuerza los dispositivos de clientes más experimentados que pueden tener radios 802.11b / g / n, y además brinda capacidad de transmisión adicional a las velocidades de información que avanzan. (Álvarez, 2016)
802.11g	Según Cárdenas y Zambrano (2018) en junio de 2003, 802.11g fue el sucesor de 802.11b, apto para alcanzar velocidades de hasta

	54Mbps en la banda de 2.4GHz, nivelando con la velocidad de 802.11a pero dentro de la extensión de recurrencia más baja.
802.11a	La "carta" principal después del endoso en junio de 1997 del estándar 802.11, se da para trabajar en la recurrencia de 5GHz, con tasas de información de hasta 54Mbps. Por el contrario, el 802.11a resultó después de 802.11b, causando cierto desorden en el mercado, ya que tendría el estándar con la "b" hacia el final y la "a" hacia el final. (Cárdenas & Zambrano, 2018)
802.11b	Propulsado en el mes de septiembre de 1999, donde su 802.11b, funciona con 2.4 GHz y otorga 11 Mbps. Sorprendentemente, los artículos de 802.11a llegaron al mercado antes de 802.11a, que se aprobó mientras tanto, sin embargo, no se lanzó al mercado hasta algún otro momento. (Cárdenas & Zambrano, 2018)
802.11-1997	Fue uno de los primeros estándares que daban una velocidad de datos hasta de 2 Mbps en la frecuencia 2,4 GHz. Tiene un alcance de 20 metros de interior

Autor: *Oscar Briones*

Según Serna (2013) las redes inalámbricas 802.11 básicamente son inseguras y pueden ser interferidas por componentes que funcionan en la recurrencia de 2.4Ghz, por ejemplo, teléfonos inalámbricos, microondas, dispositivos bluetooth y dispositivos Zigbee entre otros. Esa obstrucción puede influir en la velocidad de transmisión aparente esperada para el sistema, que es de 54 Mbps.

Tabla 2. Análisis FODA

Fuente: *Oscar Briones Mora*

Fortalezas	Oportunidades
• Se cuenta con el personal suficiente para realizar las actividades diarias. • Se cuenta con el recurso económico necesario para realizar las labores. • Se cuenta con las herramientas necesarias. • El ambiente Laboral es Bueno.	• La empresa puede otorgar un subsidio suficiente. • Surgimiento de los mecanismos para aprovechar mejor los recursos. • Implementación de nuevas tecnologías y procesos para aumentar la eficiencia.
Debilidades	Amenazas
• A pesar de contar con procesos, estos no están apegados completamente a estándares internacionales. • A pesar de contar con políticas definidas estas no se aplican adecuadamente.	• El recurso con el que cuenta depende del subsidio que se le otorgue. • Falta de recurso para renovar la infraestructura tecnológica. • Renovación de los directores por personal poco capacitado

Seguridad de la información

Sistema de Gestión de la Seguridad de la Información- SGSI:

El ISMS (Information Security Management System). En el contenido, los datos se comprenden como toda esa disposición de información clasificada por un elemento que tiene un incentivo para ello, prestando poca atención a la forma en que se guarda o transmite (compuesta, en imágenes, oral, impresa en papel, guardado electrónicamente, anticipado, enviado por correo, fax o correo electrónico, transmitido en discusiones)de su punto de partida o de la fecha de planificación. (Nieves, 2017)

La seguridad de la información, según ISO 27001, forma parte de la protección de su privacidad, respetabilidad y accesibilidad, al igual que de los marcos comprometidos con su tratamiento, dentro de una asociación. De esta manera, estos tres términos establecen la premisa en la que se basa el funcionamiento completo de la seguridad de datos:

Confidencialidad: Los datos no están disponibles o no están disponibles para personas ajenas, formularios no aprobados.

Integridad: ejecución de la precisión y cumplimiento de los datos y sus estrategias de procedimiento. (Nieves, 2017)

Disponibilidad: acceso y utilización de los marcos de datos y tratamiento por personas, o procedimientos aprobados cuando sea necesario.

Activos: Las ventajas para ser percibidas son aquellas identificadas con marcos de datos. Los precedentes ordinarios son información, equipo, programación, administraciones, archivos, estructuras y recursos humanos (Nieves, 2017).

Impactos: los resultados del evento de los diversos peligros son constantemente negativos. Las desgracias creadas pueden ser relacionadas con el dinero, no monetarias, momento presente o larga distancia**.**

Amenazas: existen peligros confiables y son aquellas actividades que pueden causar resultados negativos en la tarea de la organización. Normalmente se demuestra como peligros de decepciones, salarios no aprobados, infecciones, utilización inadecuada de la programación, fiascos ecológicos, por ejemplo, terremotos o inundaciones, acceso no autorizado, acceso simple a oficinas, entre otros.

Gestión de riesgos: ejercicios coordinados para dirigir y controlar los ángulos relacionados con el riesgo dentro de una asociación.

Vulnerabilidad: la indefensión es una deficiencia del marco de la PC que puede utilizarse para causar daño. Las deficiencias pueden aparecer en cualquiera de los componentes de una PC, tanto en el equipo como en el marco de trabajo y en el producto. (Nieves, 2017).

Probabilidad de Amenaza

Las principales contemplaciones de la probabilidad de peligro son:

a. Intriga o fascinación por personas ajenas.

b. Dimensión de la debilidad

c. Recurrencia de incidentes

Se discute un Ataque, cuando un peligro se convirtió en una realidad, es decir, el punto en el que se llevó a cabo la ocasión. Sin embargo, el asalto no dice nada con respecto al logro de la ocasión y sí o no, la información y los datos se vieron afectados con respecto a su privacidad, respetabilidad, accesibilidad y credibilidad. (Macen , 2014)

Para evaluar la probabilidad de amenaza podemos plantear algunas preguntas

¿Cuál es la intriga o fascinación con respecto a las personas externas para atacarnos?

Algunas razones pueden ser que manejamos datos que contienen noticias o innovaciones, intercambiando datos o quizás tengamos candidatos en el trabajo, negocios o simplemente debido a la imagen o la posición abierta que tenemos. (Macen , 2014)

¿Cuáles son nuestras vulnerabilidades?

Es esencial tener en cuenta todas las reuniones de debilidad. Además, se prescribe incorporar especialistas, expertos de diversas regiones de trabajo para obtener una imagen progresivamente total y punto a punto de la circunstancia interna y de la Tierra (Macen , 2014).

¿Con qué frecuencia has tratado de asaltarnos?

Los asaltos pasados son útiles para distinguir un peligro y, si se trata de una visita, es más probable que ocurra una vez más. Si hemos actualizado oficialmente las estimaciones defensivas, es vital mantener un registro, que demuestre las situaciones en que la medida se conectó de manera efectiva y cuándo no. Como de esa manera, sabemos en cualquier caso si el peligro persiste y, segundo, cuál es su riesgo actual.

Pensando en todos los enfoques pasados, nos permite ordenar la probabilidad de amenaza. No obstante, antes debemos caracterizar el significado de cada condición de probabilidad (Baja, Media, Alta). Se prescribe que cada organización caracterice sus propias condiciones. (Macen , 2014)

Herramientas de seguridad informática

NESSUS

Es considerada una de las mejores herramientas para el control de redes y a su vez para detectar las debilidades potenciales tales como el acceso a información sensible, los fallos en la configuración, ausencia en contraseñas en algunas cuentas del sistema y los servicios que sean considerados débiles. (Cedeño, 2015)

El software se divide en dos partes Nessusd que se encarga de ejecutar las peticiones, recupera datos y también muestra el resultado y los que se programan en Scripts es Nasl que se encarga de buscar los fallos por medio de plug-ins. (Cedeño, 2015)

Análisis de frecuencia de red inalámbrica en Farmadescuento

Esto fue realizado con el software inSSider, un aplicativo de uso libre, lo que permite ver el ESSID de los sistemas remotos que se encuentran en el territorio, demuestra gráficamente los canales utilizados, la cobertura de los signos y la fuerza de transmisión. Además, repite el límite del analizador de rango utilizando la tarjeta de marco remoto (Serna, 2013)

Como resultado se puede notar en el análisis de la red que se encuentra con 2 solapamientos compartiendo red en los canales 11-7. Provocando un posible colapso en la red inalámbrica cuando haya más tráfico de datos en las horas picos de trabajo.

Según la UPNA (2017) menciona que para 2.4 GHz, tenemos 14 canales, aislados por 5 MHz. En cualquier caso, cada nación y región geológica aplica sus propias limitaciones a la cantidad de canales accesibles. Por ejemplo, en Norteamérica solo se utilizan las 11 iniciales, mientras que en Europa se tienen 13 canales. El problema con esta circulación es que cada canal necesita 22MHz de capacidad de transmisión para funcionar, y como debería ser obvio en la figura, esto crea una cobertura de Unos pocos canales limítrofes.

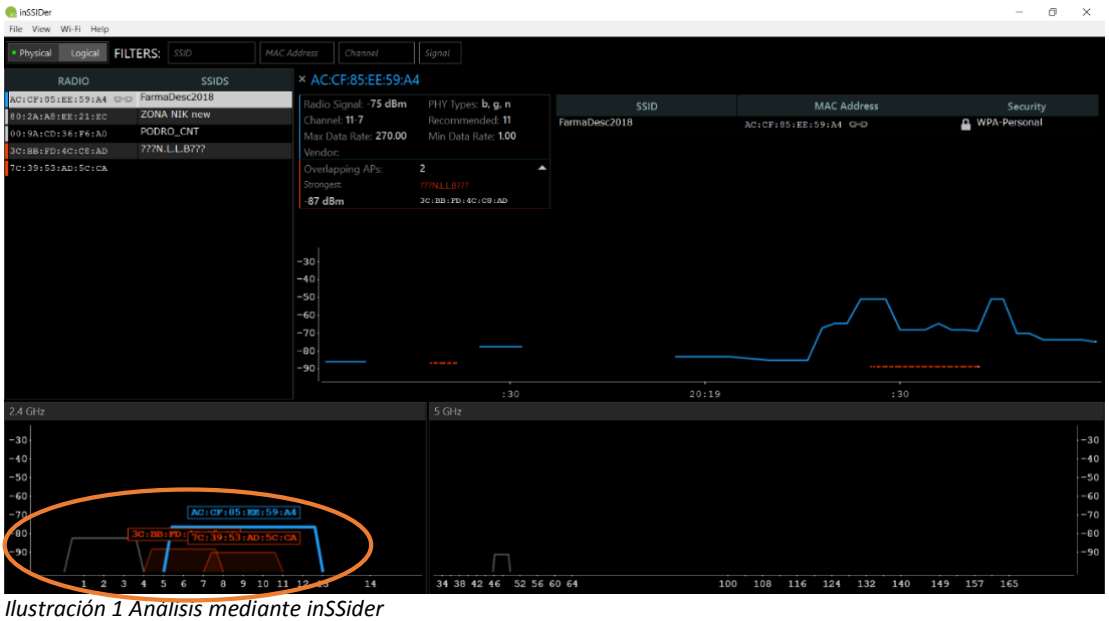

Ilustración 1 Análisis mediante inSSider

Autor: *Oscar Briones*

Se puede observar el software Inssider da el SSID del AP, la dirección MAC, el canal de operación. La potencia obtenida de cada AP, Inssider nos permite realizar la velocidad de transmisión más extrema de cada AP y un diagrama de canal utilizado por cada AP.

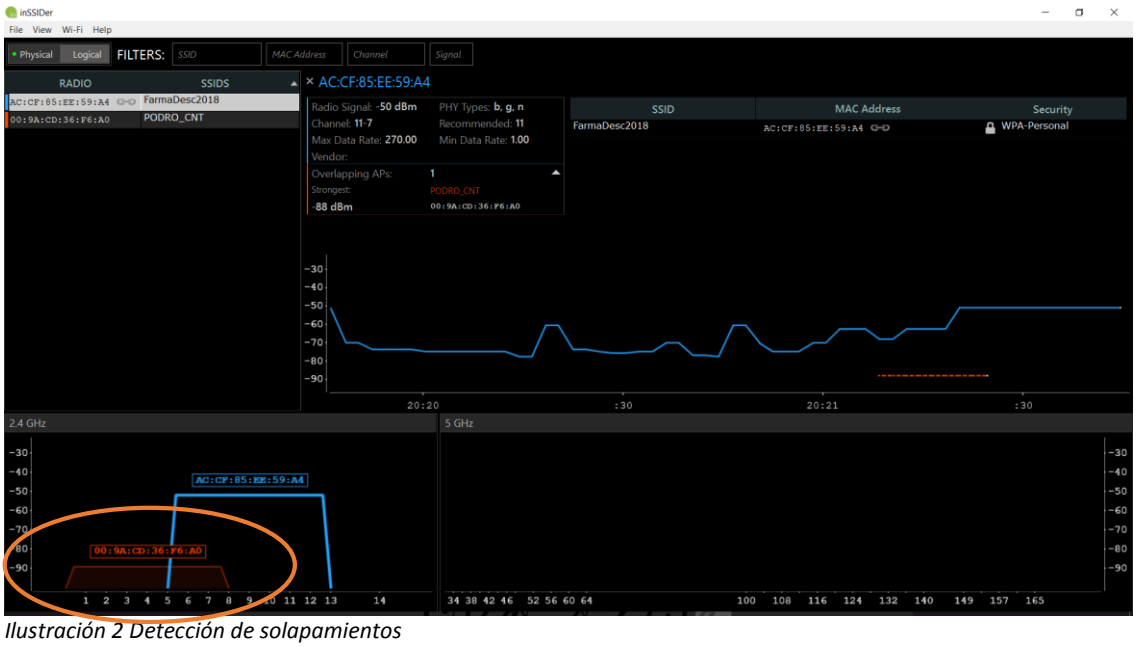

Ilustración 2 Detección de solapamientos

Autor: *Oscar Briones*

Se obtuvo mediante el análisis una potencia -50dBm notificando PODRO_CNT muestra un solapamiento donde se puede congestionar los datos donde se recomienda utilizar el canal 11 que a su momento se encuentra libre.

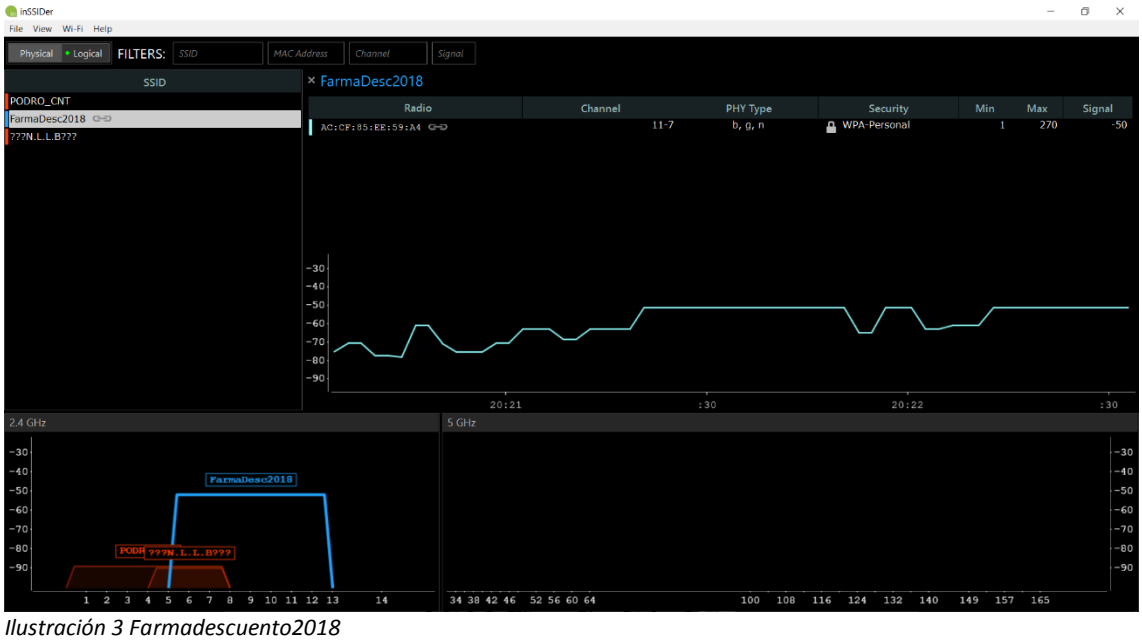

Ilustración 3 Farmadescuento2018

Autor: *Oscar Briones*

Se puede notar la potencia de la red de -80 dBm a -50 dBm. Para evitar los efectos del solapamiento de canales en las redes WiFi, lo ideal es que una red esté separada de la otra

en 5 canales, como se puede notar en la figura 3: Si una red utiliza el canal 5, la siguiente debería utilizar el 13. De esta forma, no se produce solapamiento alguno. Debido a que no tiene la capacidad de utilizar un canal diferente en una separación de 5 canales, es mejor utilizar el canal más alejado de la bandera más débil.

Análisis de la aplicación Nessus a Farmadescuento

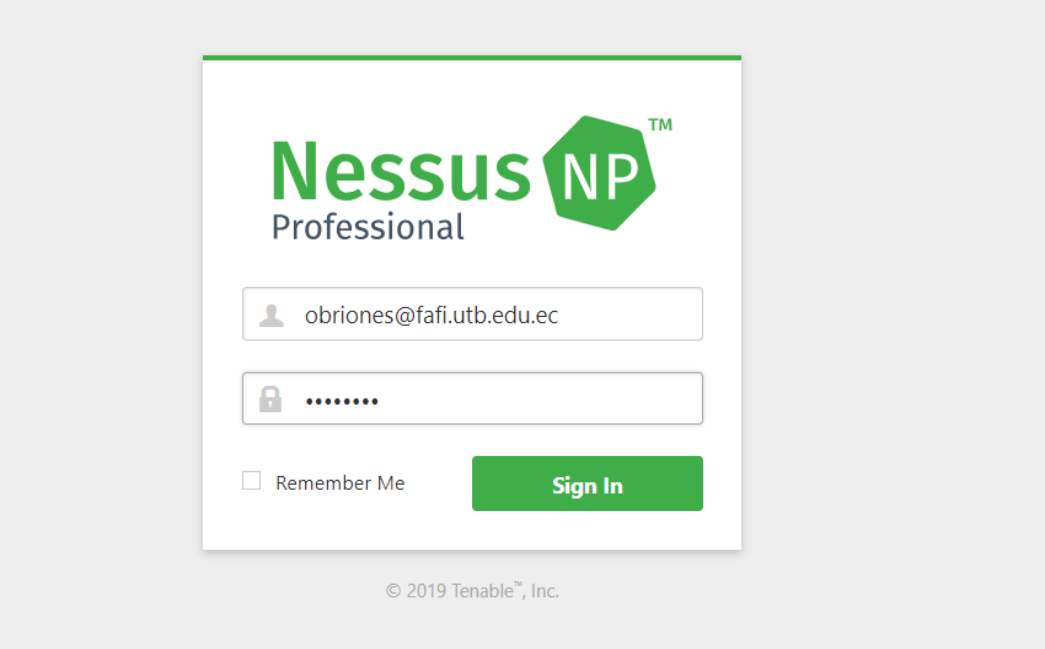

Ilustración 4 Inicio de sesión para el análisis

Autor: *Oscar Briones*

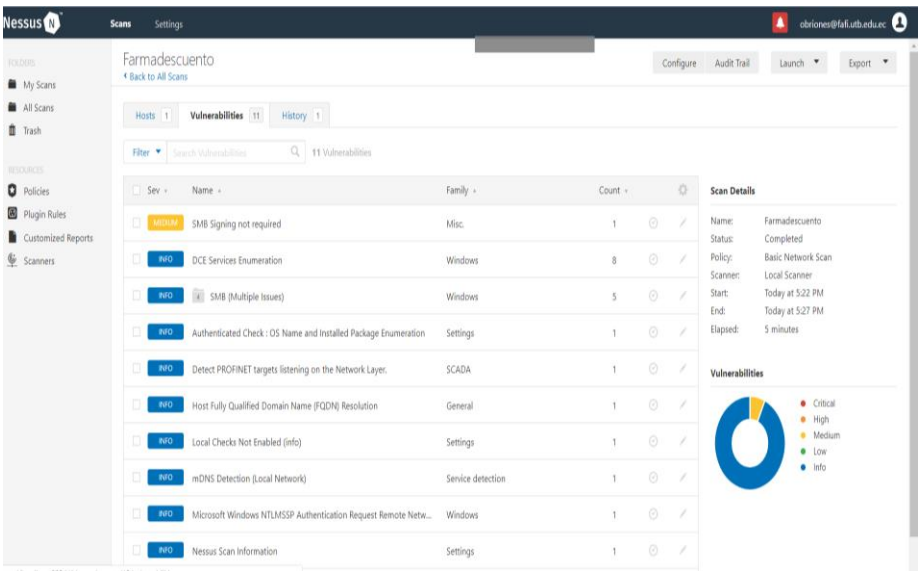

Ilustración 5 Análisis de Vulnerabilidad con Nessus

Autor: *Oscar Briones*

Luego que se identifican las vulnerabilidades por parte del Software Nessus se compara con la base de datos integrado especificándolas 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.

Según el análisis se encontró una vulnerabilidad en este medio indicando SMB Signing not required (Firma SMB no requerida). La firma no es necesaria en el servidor SMB remoto los que daría a un asaltante remoto no autenticado puede explotar esto para realizar ataques de intermediario contra el servidor SMB.

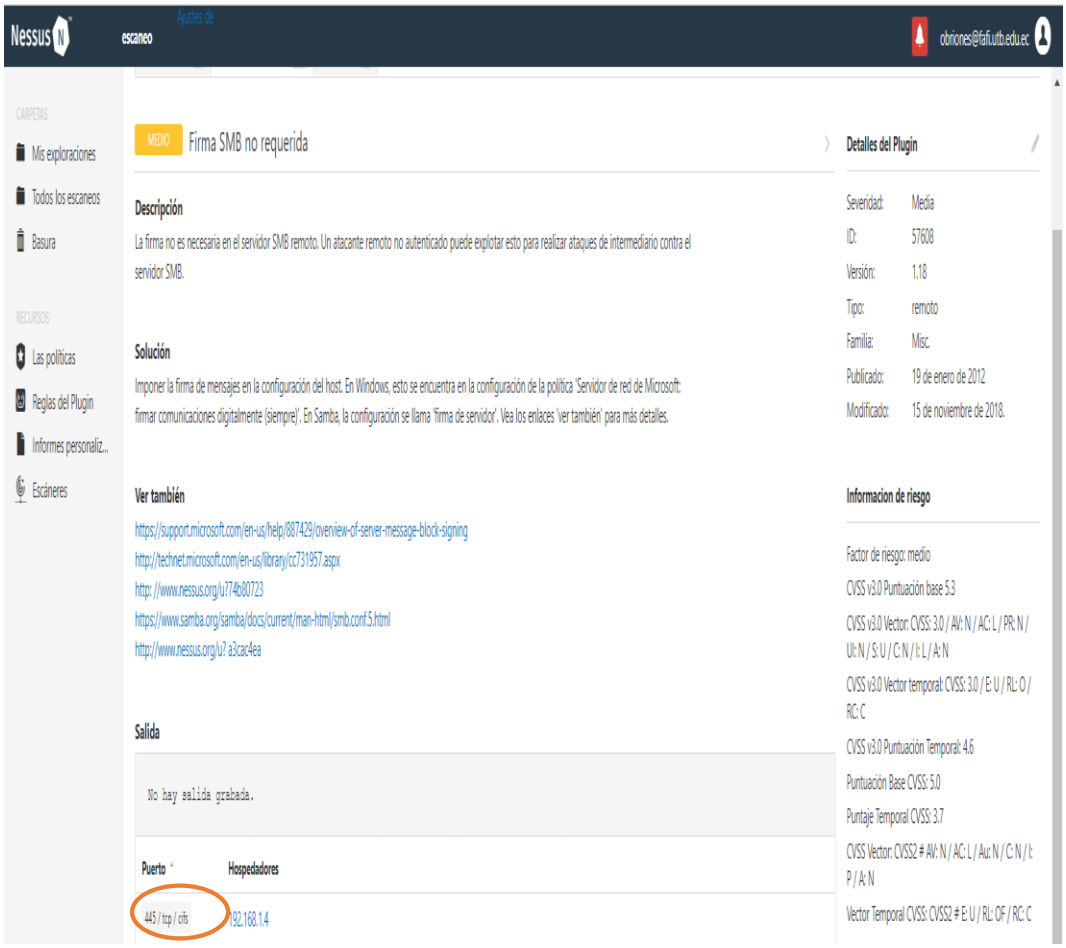

Ilustración 6 Vulnerabilidad en el puerto

Autor: *Oscar Briones*

Las primeras formas de Windows utilizaron el Servidor de mensajes del servidor (SMB) para las administraciones de intercambio de impresoras y documentos del sistema. Con el avance de TCP / IP, Microsoft diseño a Windows NT para ejecutar en el SMB en

NetBIOS. usando los puertos 135, 137 y 139 para comunicarse promedio de las redes, mientras que las variaciones que comenzaron con Windows 2000 se propusieron para ejecutar SMB a través de TCP / IP utilizando el puerto 445 específicamente. (Hughes, 2017)

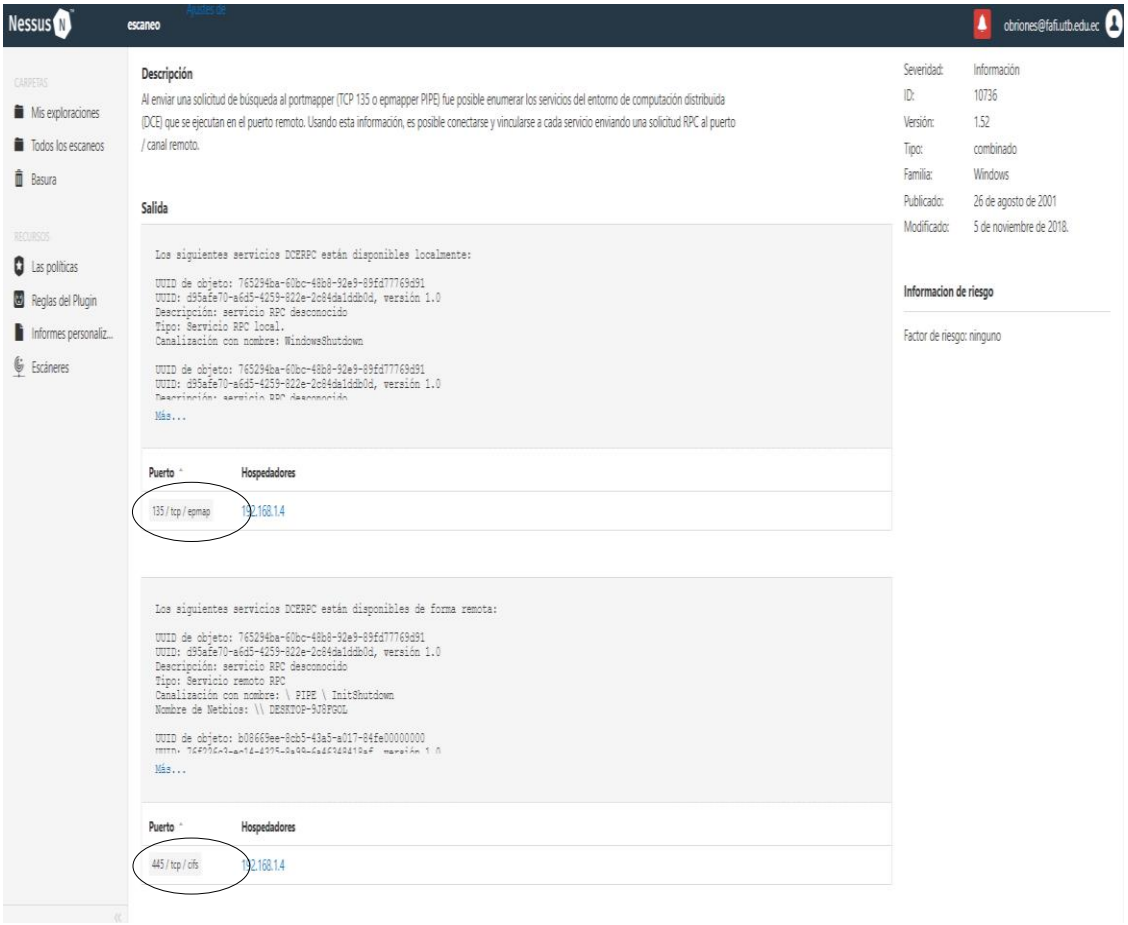

Ilustración 7 Puertos vulnerables en Farmadescuento

Autor: *Oscar Briones*

Las primeras formas de Windows utilizaron el Servidor de mensajes del servidor (SMB) para las administraciones de intercambio de impresoras y documentos del sistema.

Al debilitar NBT, puede lograr una mayor cantidad de seguridad que al dejar esos puertos en funcionamiento, sin embargo, a pesar de todo lo que necesita para anclar el puerto 445. Es mejor diseñar su firewall con el objetivo de que nunca permita el tráfico del sistema activo desde el puerto 445. prescriba debilitar el puerto 445 en su propio firewall, excepto

si realmente lo necesita para un período de tiempo. Esto causa más problemas, pero es la estrategia más segura para utilizar el puerto 445 (Hughes, 2017).

CONCLUSIÓN

Se concluye que la fiabilidad de la red WiFi de la empresa Farmadescuento S.A es débil debido a que no posee una correcta protección de los datos así; se evidencia que no hay mecanismos que detecten y ejecuten un protocolo de autodefensa previo a intentos de intrusión o ataques de negación de servicios.

Este hecho deja entrever que los niveles de vulnerabilidad de la red WiFi objeto de investigación es alta, adicionalmente se evidencia la existencia de múltiples redes inalámbricas en el interior como exterior del edificio lo cual dando paso a la atenuación de la señal de transmisión y por ende se comprueba que la saturación es mayor al ancho de banda registrado en cada equipo en la capa de acceso y distribución de la red del edificio.

La firma no es necesaria en el servidor SMB remoto esto es un problema, si un atacante remoto no autenticado puede explotar esto para realizar ataques de intermediario contra el servidor SMB, la solución a esa vulnerabilidad es imponer la firma de mensajes en la configuración del host.

BIBLIOGRAFÍA

Andreu, J. (2011). *Redes inalámbricas (Servicios en red).* Editex.

Cárdenas, J., & Zambrano, D. (13 de enero de 2018). *Facultad de ciencias matematicas y fisicas.* Recuperado el 11 de enero de 2019, de repositorio.ug.edu.ec: http://repositorio.ug.edu.ec/bitstream/redug/33816/1/B-CINT-PTG-N.356%20C%C3%A1rdenas%20Helao%20Joyce%20G%C3%A9nesis.pdf

Álvarez, R. (1 de lulio de 2016). *El estándar Wi-Fi 802.11ac se actualiza y nos trae más velocidad y mayor ancho de banda.* Obtenido de https://www.xataka.com/perifericos/el-estandar-wi-fi-802-11ac-se-actualiza-y-nos-trae-mas-velocidad-y-mayor-ancho-de-banda

Cedeño, E. (3 de abril de 2015). *Análisis de las herramientas para el proceso de auditoría de seguridad informática utilizando kali linux.* Recuperado el 11 de enero de 2019, de www.dit.upm.es: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Ericka_Yanez_Cedeno_2015.pdf

Escudero, A. (27 de enero de 2016). *Estándares en Tecnologías Inalámbricas.* Obtenido de www.itrainonline.org: http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf

Hughes, A. (19 de noviembre de 2017). *La seguridad de NetBIOS.* Obtenido de techlandia.com: https://techlandia.com/puerto-445-windows-7-info_565864/

Macen , C. (16 de julio de 2014). *Políticas de seguridad de la información.* Obtenido de www.utic.edu.py: http://www.utic.edu.py/v6/investigacion/attachments/article/118/TESIS.pdf

Nieves, A. (12 de febrero de 2017). *Diseño de un sistema de gestión de la seguridad de la información (sgsi) basados en la norma.* Obtenido de epository.poligran.edu.co: http://repository.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y

Serna, É. (10 de Diciembre de 2013). *Una propuesta de solución al problema de la interferencia entre redes wifi por solapamiento de canales.* Obtenido de www.scielo.org.co: http://www.scielo.org.co/pdf/cein/v23n2/v23n2a01.pdf

Shaw, K. (28 de enero de 2018). *Estándares y velocidades de Wi-Fi explicados y comparados.* Recuperado el 11 de enero de 2019, de www.cwv.com.ve: http://www.cwv.com.ve/estandares-y-velocidades-de-wi-fi-explicados-y-comparados/

Universidad de San Carlos Guatemala. (2014). *Seguridad de la Información.* Guatemala.

UPNA. (18 de marzo de 2017). *tecno.* Obtenido de www.tlm.unavarra.es: https://www.tlm.unavarra.es/~daniel/docencia/redes/redes10_11/slides/11-WiFi.pdf

ANEXOS

Anexo 1 (Lugar del estudio)

Gráfico 1. Edificio de Farmadescuento.

Autor: *Oscar Briones*