Instituto Tecnológico y de Estudios Superiores de Monterrey
Escuela de Ingeniería y Ciencias
Ingeniería en Ciencias de Datos y Matemáticas

Análisis de criptografía y seguridad
MA2002B Grupo 101

Profesores:
Alberto Francisco Martínez Herrera
Oscar Eduardo Labrada Gómez

Organización Socio Formadora
Tecnogam

Auditoría de Seguridad y Plan de Mitigación: Caso PyME en *Facebook Marketplace*

Equipo 5

Adrián Pineda Sánchez	A00834710
Gerardo Juárez Hernández	A01732799
Karla Andrea Palma Villanueva	A01754270
Luis Ángel López Chávez	A01571000
Salvador Vidal Torres	A01732983
Sarah Dorado Romo	A01540946

17 de marzo de 2023
Monterrey, Nuevo León

Abstract

Mi nombre es Adrian Pineda Sánchez A00834710 y este reto “Auditoría de Seguridad y Plan de Mitigación” consistió principalmente en realizar un análisis de vulnerabilidades en los dispositivos de la red de un PyME para mejorar su seguridad informática y conciencia en bases de la ciberseguridad.

Para iniciar, se empezó localizando una PyME, en la que, en nuestro caso, se emuló al mejor detalle posible sustentado en referencias y fuentes de información y basándonos en que tuviera una similitud en su topología de redes con cualquier red doméstica habitual, esto para el desarrollo de una PyME localizada en Monterrey, N.L, enfocada en la venta de indumentaria de ropa y calzado deportivo para hombre y para mujer a través de la aplicación Facebook Marketplace.Continuando con esto, se llevó a cabo un inventario de los dispositivos así como de una descripción y diagrama de la topología de la red que se analizó.

Posteriormente, se realizó un plan de evaluación en el que a través de un estudio exhaustivo en la parte técnica, que consistió en realizar un análisis mediante la herramienta Nessus, en su versión “Nessus Essentials” proporcionada por Tenable, la cual pudimos utilizar por un periodo de tiempo de forma gratuita y gracias a esto, pudimos relacionar las claves CVE o Nessus ID de las vulnerabilidades que pudimos encontrar en los dispositivos de inventario, pudimos describir su nivel de peligrosidad y el enfoque o descripción de la misma vulnerabilidad, así como su solución a inmediato plazo lanzada por el desarrollador, así también como de la parte operativa, describiendo el nivel de conciencia o si existía un plan de contingencia de la PyME.

A continuación, se llevó a cabo un plan de mitigación en el que se estudiaron y se eligieron alternativas de solución en mayor profundidad con respecto a esto, tanto a nivel técnico u operativo, efectuando a su vez un análisis de costos y que sea viable y accesible para el presupuesto de la PyME, así como eligiendo alternativas más rentables y eficientes a la satisfacción de las necesidades de la misma pequeña empresa.

Finalmente, solo se efectuaron las conclusiones y análisis de resultados, así como aclarar las medidas y veredictos finales que pudimos llegar con este estudio, en pro de asegurar en un nivel seguro a nivel digital a esta PyME, basándonos en las herramientas computacionales así como nuestro conocimiento técnico aprendido en este bloque de ciberseguridad y redes.

Introducción

México es una nación repleta de compañías y empresas pequeñas, también conocidas como PyMEs, que son colaboradoras y responsables en la sustentación de la economía en la República. De acuerdo con *Conekta* [1], compañía mexicana promotora de la economía digital, son definidas como aquellas pequeñas y medianas empresas, al igual que microempresas donde el número de trabajadores se encuentran entre 1 hasta 250 trabajadores y donde sus ventas anuales no pueden llegar a ser mayores a 250 millones de pesos en ningún caso. Para el caso de microempresas [1] son todas aquellas con menos de 10 trabajadores y un volumen de ventas anuales menor a 4 millones de pesos. Es recientemente donde esta categoría se añade a este mismo grupo de compañía usando el término MIPyME [1] para incluirlas. Son estas empresas las que rápidamente se adaptan al uso de nuevas tecnologías y tendencias para obtener el mayor provecho de ellas. Sin embargo, el uso de herramientas tecnológicas también puede ser aprovechado en su contra, especialmente cuando se trata de obtener datos mediante accesos no autorizados o en casos de ciberataques. Por esta razón, en este trabajo se pretende trabajar con una de estas empresas, o emular una de ellas, con la ayuda de herramientas pertenecientes a *Tenable* [2], una organización que busca educar sobre la importancia de la seguridad de redes y reducir el riesgo de ciberataques con una de sus herramientas de escaneos de vulnerabilidades en redes como *Nessus*. De esta manera, se pueden identificar y clasificar las vulnerabilidades según su calificación CVSS versión 3.0 y el número de identificación proporcionado por Nessus. Finalmente, se proponen soluciones teniendo en cuenta factores como los costos de las herramientas y el presupuesto de la PyME, al igual que proponer un plan de mitigación de las vulnerabilidades encontradas que ayuden a prevenir posibles ataques.

Como se mencionó anteriormente, para este trabajo se emulará a un PyME, específicamente en una microempresa, para que se asemeje lo más posible a una red doméstica, ya que es en una de estas donde se realiza el plan de evaluación de vulnerabilidades y para el cual aplica el plan de mitigación correspondiente. Para este caso se ideó una empresa pequeña en *Facebook Marketplace* el cual vende indumentaria, más enfocado en la venta de ropa y calzado deportivo y casual tanto para hombre y mujer.

Análisis de Mercado

El mercado de indumentaria de ropa y calzado deportivo en México es altamente competitivo y dinámico, con un gran número de marcas locales e internacionales que compiten por la atención de los consumidores. En cuestión de un análisis del mercado en esta industria, el segmento de ropa y calzado deportivo en México ha experimentado un crecimiento constante en los últimos años. Según un informe de Euromonitor International, se espera que el mercado de ropa deportiva en México tenga un valor de 9,400 millones de dólares en 2023, lo que representa un aumento del 16% con respecto a 2018. El segmento de mercado objetivo para la PyME se toma como uno enfocado en consumidores jóvenes, activos y urbanos, que valoran la calidad y la comodidad en su ropa y calzado deportivo.

En cuestión del e-commerce enfocado en Indumentaria deportiva, debido a la industria en la que estamos ahondando, como lo son “Retail Channels”, según Euromonitor International en 2022, observamos un crecimiento asombroso del mercado, pasando de un 2% del total del mercado en 2017 en México, a un crecimiento del 15% del total del mercado de “Retail Channels” en materia de e-commerce en el cierre del año 2022, esto indica, un fuerte crecimiento en el segmento de la industria en la cual nuestra PyME está enfocada. [18]

Contexto socioeconómico y demográfico de la PyME

En cuestión del aspecto financiero y del estudio de mercado de la empresa, a través de documentación enfocada en la venta de indumentaria deportiva de ropa y calzado en México, en las condiciones que estamos manejando (una PyME con una concentración menor a 10 empleados y facturación por debajo de los 4 millones de pesos anuales) hemos investigado un promedio en México de los márgenes en cuestión de facturación, así como márgenes brutos y netos de ganancia adaptándola a nuestra escalabilidad y modelo de negocios. [1]

En materia del modelo de negocios de nuestra PyME, cuenta tanto con entrega a domicilio, como la recolecta del producto vendido en el domicilio del dueño del negocio. El dueño, ubicado en Monterrey en el área de Cumbres, tiene actividad constante y recientemente planea aumentar el negocio involucrando a más amigos y familiares como empleados situados en una zona cercana al Tec de Monterrey de la misma ciudad. El proceso común que se sigue para realizar una compra y venta en este negocio empieza con el cliente, estableciendo contacto mediante la aplicación *Messenger* con el vendedor para acordar el precio del producto

deseado. Se intercambia la información domiciliaria para la entrega o colecta del producto mediante el mismo medio. En caso de ser una entrega al cliente, cuenta con sus trabajadores.

Finalmente, la venta del producto se realiza mediante transferencia previa a la entrega, compartiendo la información necesaria como número de cuenta, CLABE, y en ciertos casos número de teléfono personal. El destino de transferencia es una cuenta de banco específica a la empresa. En nuestra emulación de la PyME considera sólo las áreas y departamentos fundamentales en el desarrollo y mantenimiento de nuestro modelo de negocios, los cuales se dividen en solamente 2 departamentos: Marketing y Finanzas, así como, Logística y Administración (con lo cual debemos trabajar bajo el contexto de que no se cuenta con un departamento enfocado en Tecnología de Información).

De acuerdo al INEGI [4], los ingresos anuales promedio de una microempresa en México es de aproximadamente 57,000 MXN, y en términos del análisis de mercado, el margen neto de ganancias se sitúa entre un 8-20% del volumen de negocio generado en la industria de la indumentaria de ropa y calzado, mientras que el precio del artículo en promedio en reventa radica entre un 130-150% sobre el valor obtenido sobre el proveedor [10]. Por lo que determinamos que en la emulación de nuestra PyME, nuestra facturación, tomando un porcentaje de ganancias netas de 10% aproximadamente y un precio en reventa sobre 150%, se facturan 570,000 MXN pesos anuales, con una inversión inicial en producto de 380,000 MXN pesos anuales, ganancias brutas de aproximadamente 190,000 MXN pesos anuales, y una ganancia neta de 57,000 MXN pesos anuales. [10]

Esto se encuentra de acuerdo con lo reportado en el INEGI [4]. Por lo tanto, al idear la empresa se tomó un monto de entre 2,800 y 2900 MXN máximo que la PyME está dispuesta a gastar en el plan de mitigación, aproximadamente 5% de las ganancias totales del último año. Esto se debe principalmente a que un negocio pequeño el cual usa aplicaciones que ya cuentan con cierto grado de seguridad (por ejemplo el cifrado de extremo a extremo en la aplicación de *Messenger* [3]) y no piensan qué invertir grandes cantidades de dinero sea una buena decisión.

De acuerdo a Verizon [33], compañía que ofrece servicio especializado en el manejo de acceso de información, un 46% de todos los ciberataques en 2021 consistieron en la brecha de información en aquellas compañías con menos de 1000 empleados. Esta tendencia solo sube viendo los años anteriores debido a que resultan ser objetivos más fáciles de atacar. Por ejemplo, cuentan con menos medidas de seguridad y mayor facilidad de acceso a esta información comparada a las demás empresas más grandes. Uno de los ejemplos más prominentes recientemente es el ciberataque hacia la gigante tienda de ropa británica JD Sports [37], en el cual se obtuvo el historial de compras, incluyendo domicilio, número de télefono, nombres, correos, y detalles de compra de más de 10 millones de clientes. Con el crecimiento de ciberataques hacia pequeñas compañías en años recientes y el caso donde millones de datos sensibles de clientes en lo que es una industria que en un principio parecen ser objetivos principales como la indumentaria, la PyME en cuestión se encuentra en una situación precaria si es que no se cuenta con las medidas necesarias contra estos ataques. La información privada del cliente no es la única vulnerable, sino también de todos los trabajadores de la compañía.

Levantamiento de inventario

Anterior al escaneo, primero se encontró la dirección IP de uno de los dispositivos conectados a la red para hallar su clase de la IPv4. Debido a que se trata de una red doméstica, se espera que sea una dirección de clase C [46], es decir una red con una capacidad de otorgar direcciones IP hasta 255 dispositivos. Efectivamente se encontró la siguiente IP de forma 192.168.0.0/24 de uno de los ordenadores de escritorio con una puerta de enlace predeterminada (o default gateway) de 192.168.0.1 y máscara de subred 255.255.255.0. En el momento de escaneo de red se encontraron 8 hosts o dispositivos conectados de los cuales se se encontró un dispositivo con el sistema operativo Windows (192.168.0.170), un dispositivo Apple iPhone/iPad 192.168.0.139, el router marca TP-Link, mientras que los restantes usan una especie de kernel de Linux u otro. Por lo tanto, se puede establecer la siguiente topología de red según el escaneo también conociendo que uno de los dispositivos basados en Linux consiste en un celular, al igual que todas las conexiones dentro de la red son inalámbricas. Es importante mencionar que aquellos dispositivos sin un sistema operativo especificado serán tratados como genéricos conectados a la red.

a) Equipos

A continuación se muestra el inventario de la PyME usando *Nessus* [2]

Equipo	Dirección IPv4
Home Gateway	192.168.0.1
iPad/ iPhone	192.168.0.139
Celular Android	192.168.0.141
Google Home	192.168.0.156
Genérico 1	192.168.0.163
Computadora Windows	192.168.0.170
Chromecast	192.168.0.183
Genérico 2	192.168.0.194

b) Propósito de cada equipo

Primero que todo, debemos dejar claro, que el programa Nessus no logró identificar ciertos dispositivos, a lo que nosotros llamamos "Genérico" es por esto que no es posible analizar el propósito de estos dispositivos, ahora bien, al ser una red doméstica, todos los dispositivos son para este mismo uso, doméstico; sin embargo, asumimos que es una PyME, por lo tanto, proseguiremos con ese mismo razonamiento:

- Home Gateway [34]

El router de red, el cual funciona como un punto de conexión para múltiples dispositivos, como computadoras, impresoras, tabletas y teléfonos inteligentes, que se conectan a la red. El router utiliza una dirección IP para identificar cada dispositivo en la red y encamina los paquetes de datos a través de la red de manera eficiente.

- iPad/ iPhone

Teléfono celular de uso cotidiano

- Celular Android

Teléfono celular de uso cotidiano

- Google Home [36]

Dispositivo Google Home, en el cual el personal puede interactuar con el dispositivo usando comandos de voz para realizar diversas tareas, como hacer una búsqueda en Google, enviar un mensaje de texto, establecer una alarma, reproducir música, obtener actualizaciones de noticias y controlar otros dispositivos inteligentes en su hogar, como termostatos, cerraduras de puertas, luces, entre otros.

- Windows PC

Computadora de escritorio, con la cual el personal, realiza los anuncios de venta para los compradores en línea.

- Chromecast

Dispositivo doméstico para transmitir contenido multimedia, como música, videos o imágenes, del mismo dispositivo a un televisor.

c) Topología de la red

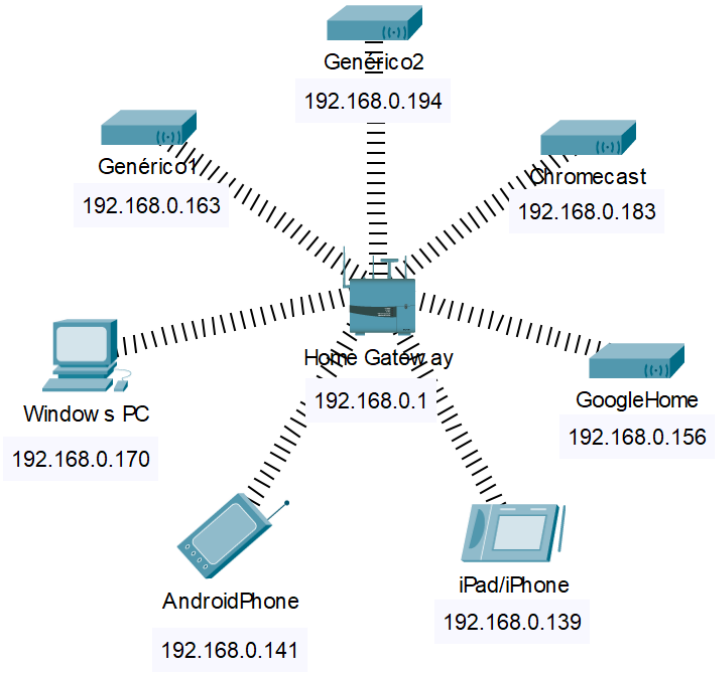

Figura 1. Representación lógica de red creada en *PacketTracer*.

En la figura anterior podemos observar la topología de red de nuestra PyME , donde se muestran los equipos que hay en la red, estos detectados por el programa Nessus, siendo los dos nombrados como Genéricos 1 y 2, dispositivos que Nessus no pudo reconocer, teniendo esto en cuenta todos los demás dispositivos como Google home, Chromecast, Windows Pc, Android Iphone, Ipad ocupados como herramientas de trabajo para comunicación visualización, etc. dentro de la PyME, los cuales se conectan de manera inalámbrica al router/módem a través de una contraseña de acceso.

Plan de Evaluación

a) Herramientas para realizar el plan de evaluación

Tomando en cuenta que la red tratada consiste en una red doméstica (el cual se usa para emular la red de una PyME), se deben elegir las herramientas adecuadas para encontrar y entender sus puntos susceptibles. Es por esto que las herramientas más indicadas para lo que es el análisis de vulnerabilidades son las siguientes, las cuales pueden ser usadas por :

1. OpenVAS [12]: esta es una herramienta de escaneo de vulnerabilidades al igual que Nessus con la diferencia de que es de código abierto donde puedes identificar más de 50,000 vulnerabilidades conocidas en sistemas y redes. Sin embargo, esta suite de software consiste en productos de pago.

2. Por la familiarización que tenemos con esta la pondremos en el top uno siendo Nessus [2] la cual es una herramienta de escaneo que puede identificar vulnerabilidades conocidas en sistemas y redes. También puede realizar pruebas de cumplimiento de políticas de seguridad. En este trabajo se hace uso principal de esta herramienta para el análisis de vulnerabilidades.

3. Otra de las posibles y más populares herramientas a usar para el análisis de vulnerabilidades es Wireshark [14]. Es una herramienta altamente versátil disponible en sistemas operativos como Windows, OS X, Linux, entre otros. Incluso habilita la desencriptación de diferentes protocolos como WEP y WPA siendo totalmente de uso gratuito.

4. Por último, tenemos a Nmap [15] siendo una herramienta de escaneo a través de puertos que puede ayudar a identificar los servicios que se están ejecutando en un sistema y determinar si hay vulnerabilidades asociadas a esos servicios.

Cabe destacar que es importante realizar pruebas de penetración y análisis manual para complementar el análisis de vulnerabilidades automatizado. Las herramientas fueron enlistadas tomando en cuenta su bajo costo, o incluso uso gratuito, y facilidad de uso relativo a la exhaustividad de los reportes generados, ya que se usan en un contexto doméstico e incluso una PyME.

En cuestión de este análisis en específico, la herramienta que utilizaremos será "Nessus Essentials", versión gratuita de Nessus (Tenable, 2022).

b) Relación del Inventario con sus Vulnerabilidades

En cuestión de las vulnerabilidades encontradas [2] en nuestros dispositivos de inventario, cabe destacar que las designadas con los valores más altos de peligrosidad, las agrupaciones (CVE-2016-7406 CVE-2016-7407 CVE-2016-7408 CVE-2016-7409), las cuales tienen un nivel de peligrosidad de 9.8 (alto)[2] y que están directamente relacionadas con la Versión de Dropbear SSH anterior a ver. 2016.72 el cual es vulnerable a ataques conocidos con los CVE anteriores, así como la vulnerabilidad Nessus ID: 20007 la cual tiene un nivel de peligrosidad de 9.8 (alto)[2] y que están directamente relacionadas con Versión de SSL vulnerable a fallas de cripto seguridad, ambas se encuentran en el mismo dispositivo, el cual es el router principal de nuestra red de topología estrella con IP:192.168.0.1.

Dropbear SSH [47] es una implementación gratuita del Secure Socket Shell para conectar y administrar servidores de forma remota y segura para, por ejemplo, introducir datos autenticación. En esta vulnerabilidad se explica que la versión de la implementación de este protocolo es vulnerable a ataques de estilo *Man-in-the-Middle (MITM)*. Esto ocurre debido a que existen puntos débiles en la generación de archivos de encriptación para la llave pública usados para la autenticación en el protocolo SSH [2]. Esto provoca que un adversario que intercepte la comunicación puede, de manera no autorizada con privilegios administrativos, hasta ejecutar código dentro de la misma sesión, según el reporte generado en Nessus. La causa de esta gran vulnerabilidad es debido a una versión obsoleta, la solución a esto sería actualizar esta implementación a versiones más recientes. Esta solución se debe realizar con alta prioridad no solo por la simpleza de implementación, sino la grave debilidad que deja expuestos hasta la integridad de los datos comunicados entre dispositivos, un tanto similar a la vulnerabilidad anterior.

En cuestión de su otra vulnerabilidad Nessus ID: 20007, La detección del protocolo SSL versión 2 y 3 es una técnica utilizada por la seguridad informática en torno a detectar si el servidor web está utilizando una versión designada como débil de SSL. Esto es de vital importancia debido a las vulnerabilidades conocidas de las versiones antiguas de SSL las cuales pueden ser explotadas por atacantes para interceptar información confidencial.

Para detectar la versión del protocolo SSL, se envían solicitudes de conexión al servidor usando diferentes métodos y protocolos, como el protocolo HTTP o SMTP [33]. Estas variantes de SSL están interrumpidas por varias fallas criptográficas, que incluyen un esquema inseguro para la renegociación y reanudación de sesiones. Donde los atacantes pueden explotar estas fallas para realizar ataques de intermediario o descifrar las comunicaciones entre los servicios afectados y los consumidores. Muchos navegadores web implementan esto de manera insegura [34]. La mejor solución es consultar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0 y utilizar TLS 1.2 con conjuntos de cifrado aprobados o superior en su lugar. [30]

Asimismo, observamos que la vulnerabilidad CVE-2016-2183, el cual tiene un nivel de peligrosidad de 7.5 (alto), la cual está relacionada directamente con un uso de protocolo SSL anticuado, versiones 2 y 3, haciéndolos vulnerables a ataques conocidos debido a uso de esquemas de relleno de bits inseguros al realizar

cifrados en bloque, al igual que sesiones de handshake y esquemas de reanudación según el reporte generado por Nessus [2]. Se encuentra en 4 de los dispositivos del inventario, con IP:192.168.0.1 (el cual es el router principal de nuestra red con topología estrella), 192.168.0.156, 192.168.0.163 y 192.168.0.183.

En contextualización del problema, los cifrados de bloque [23] consisten en dividir el texto en claro en diferentes bloques de un tamaño de n bits cifrando cada uno de manera individual. Asimismo, existen esquemas de relleno de bits específicamente para este tipo de cifrado, donde para asegurar que cada uno de los bloques tengan el mismo tamaño se rellenan de bits el texto en claro para después ser encriptados. Sin embargo, existen algoritmos donde el tamaño en bits del texto en claro no es En esta vulnerabilidad, Nessus explica que el esquema usado para esta función es obsoleta siendo un múltiplo del número del tamaño de cada bloque creado, por lo que se han creado esquemas de relleno de bits para asegurar que siempre se cumpla esta condición [24]. amenazado por ataques de *Man-in-the-Middle (MITM)* para interceptar y desencriptar la información.

Este tipo de ataque es análogo a una persona exterior escuchando la conversación entre otras dos personas pasando desapercibido. Esto se puede realizar de diferentes formas como al tomar cierto control de un dispositivo conectado a la red parecido usándolo como un dispositivo que analiza todos los paquetes que se transmiten en una conexión como un sniffer.

En cuanto a las sesiones de handshake y esquemas de reanudación, el software utilizado menciona que son inseguros. Por un lado, las sesiones de handshake [24] consisten en el establecimiento de un canal de comunicación entre dos dispositivos, los parámetros utilizados para encriptar y desencriptar sus mensajes, y autenticación entre ellos mismos. Mientras que los esquemas de reanudación [25] consisten en un proceso simplificado para seguir con una comunicación entre dispositivos rápidamente anteriormente conectados. En ambas áreas, Nessus detectó que son susceptibles a ataques debido a usar protocolos y esquemas ya antiguos.

Y analizando a profundidad la última Vulnerabilidad de alto nivel, CVE-2004-2761, la cual tiene un nivel de peligrosidad de 7.5 (alto), la cual puede ser encontrada en el dispositivo con IP: 192.168.0.183, está directamente relacionada con que el Certificado SSL está usando un algoritmo de hashing débil (el cual se encarga de convertir elementos como datos en otro elemento usada para encriptar).[2]

Consiste en que el servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Un certificado SSL sirve para autenticar a un sitio web y asegurar la protección de la comunicación entre un navegador web y un servidor contra interceptación de agentes externos.[35] La solución al ser detectada esta vulnerabilidad consiste en simplemente en ponerse en contacto con la autoridad de certificación para que le vuelvan a emitir el certificado SSL. [36]

En el resto de dispositivos de mediano y bajo nivel de peligrosidad, el contexto a la solución de las vulnerabilidades consiste en la actualización o cambio de protocolos SSL, SSH, así como reemplazar algunos obsoletos, como lo puede ser el protocolo Telnet, aunque se ahondará en detalle dentro del plan de mitigación. A continuación se muestra una tabla incluyendo todas las vulnerabilidades encontradas con descripciones y los dispositivos:

Host (dispositivo)	Clave CVE / Nessus Plugin ID	Calificación CVSS	Descripción
192.168.0.1	20007	9.8	Versión de SSL vulnerable a fallas de criptoseguridad.
	CVE-2016-7406 CVE-2016-7407 CVE-2016-7408 CVE-2016-7409	9.8	Versión de Dropbear SSH anterior a ver. 2016.72 el cual es vulnerable a ataques conocidos con los CVE anteriores.
	CVE-2013-4421 CVE-2013-4434	5.0[1]	Versión de Dropbear SSH anterior a ver. 2013.59 el cual es vulnerable a ataques conocidos con los CVE anteriores
	CVE-2016-2183	7.5	Uso de cifrados SSL de mediano nivel de encriptación
	51192	6.5	No se puede confiar en el certificado SSL
	CVE-2013-2566 CVE-2015-2808	5.9	Versión de SSL soporta el sistema de cifrado RC4 el cual tiene fallas en la generación de bytes pseudo-aleatorios.
	12217	5.3	El servidor de DNS [45] (sistema el cual se encarga de convertir los nombres de dominios web en direcciones IP) vulnera el caché haciendo que fisgones puedan averiguar cuando se visita una página web.
	104743	6.5	Protocolo TLS 1.0 el cual ya es antigua y conocida por tener vulnerabilidades de ataques conocidos.
	157288	6.5	Soporta el protocolo TLS 1.1 el cual carece de sistemas de cifrado recomendados.
	153953	3.7	El servidor SSH permite uso de algoritmos de intercambio de de llaves de encriptación débiles
192.168.0.139	**NO SE ENCONTRARON VULNERABILIDADES**		
192.168.0.141	**NO SE ENCONTRARON VULNERABILIDADES**		
192.168.0.156	CVE-2016-2183	7.5	Soporta cifrados de SSL con un mediano nivel de encriptación.
	51192	6.5	No se puede confiar en el certificado SSL
	57582	6.5	El certificado SSL no fue reconocida por una autoridad
	104743	6.5	Protocolo TLS 1.0 el cual ya es antigua y conocida por tener vulnerabilidades de ataques conocidos.
	157288	6.5	Soporta el protocolo TLS 1.1 el cual carece de sistemas de cifrado recomendados.

[1] Esta calificación es según la versión 2.0 del sistema CVSS

Host (dispositivo)	Clave CVE / Nessus Plugin ID	Calificación CVSS	Descripción
192.168.0.163	CVE-2016-2183	7.5	SSL soporta cifrados de nivel medio y vulnerable a ataques conocidos.
	51192	6.5	No se puede confiar en el certificado SSL
	57582	6.5	El certificado SSL no fue reconocida por una autoridad
	42263	6.5	Se está usando un servidor del protocolo Telnet sobre un canal sin encriptar, es decir al usar usuarios y contraseña de cuenta se transmiten como texto claro.
	CVE-2020-11022,CVE-2020-11023	6.1	Versión de JQuery [32] vulnerable a ataques de script mediante sitios web (JQuery es una librería de JavaScript para interactuar archivos HTML usados para la creación de páginas web)
	104743	6.5	Protocolo TLS 1.0 el cual ya es antigua y conocida por tener vulnerabilidades de ataques conocidos.
	157288	6.5	Soporta el protocolo TLS 1.1 el cual carece de sistemas de cifrado recomendados.
192.168.0.170	57608	5.3	No se necesita autentificarse en el protocolo SMB (protocolo de red desarrollado específicamente para dispositivos Windows)
192.168.0.183	CVE-2004-2761	7.5	Certificado SSL usando un algoritmo de hashing débil (el cual se encarga de convertir elementos como datos en otro elemento usada para encriptar)
	CVE-2016-2183	7.5	SSL soporta cifrados de nivel medio y vulnerable a ataques conocidos.
	51192	6.5	No se puede confiar en el certificado SSL
	57582	6.5	El certificado SSL no fue reconocida por una autoridad
	104743	6.5	Protocolo TLS 1.0 el cual ya es antigua y conocida por tener vulnerabilidades de ataques conocidos.
192.168.0.194	**NO SE ENCONTRARON VULNERABILIDADES**		

Tabla 1. Vulnerabilidades encontradas en hosts conectados a la red.

c) Verificación de la topología de red

Encontramos que los dispositivos conectados a la red son altamente vulnerables al hackeo debido a una serie de factores. Especialmente aquel visto con dirección IP 192.168.0.1 el cual en este caso es el router al que todos los demás dispositivos están conectados, visto en el caso en el que tiene la misma dirección que el puerto de enlace predeterminado.

Esto indica que el lugar más vulnerable por el que se pueden realizar ciberataques es por ese medio y nuestro principal enfoque al hablar de remediar las debilidades encontradas. Asimismo, se puede observar que la mayoría de estas consisten en uso de versiones de protocolos de comunicación obsoletos y no suficientes para

combatir amenazas ya conocidas, como es el caso de las advertencias del uso del protocolo SSL y las primeras versiones de TLS. [2]

Igualmente, la mayoría de los dispositivos están conectados a Internet, lo que los hace susceptibles a los ataques remotos, lo cual resulta especialmente peligroso combinado con el hecho de que muchos usuarios no toman medidas de seguridad adecuadas.

d) Procesos de control y flujo de información en la PyME

En el inventario de la PyME analizada, tenemos que algunos de sus procesos requieren cobros con Tarjeta Bancaria Electrónica, Desafortunadamente, los procesos que involucran el uso de tarjetas bancarias pueden ser vulnerables a fugas de información sensible de los clientes. Los datos de la tarjeta, como el número de la tarjeta, la fecha de vencimiento y el código de seguridad, son información altamente valiosa para los ciberdelincuentes, quienes pueden utilizarla para cometer fraudes financieros.

Las empresas que aceptan pagos con tarjeta deben cumplir con los estándares de seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés), que establecen requisitos para la protección de los datos de las tarjetas. Entre estos requisitos se encuentran el cifrado de los datos de la tarjeta y la implementación de medidas de seguridad para prevenir el acceso no autorizado a los sistemas que manejan estos datos.

Sin embargo, a pesar de estos esfuerzos de seguridad, siempre existe el riesgo de que se produzcan fugas de datos, ya sea como resultado de una brecha de seguridad en el sistema de la empresa, o como resultado de la acción malintencionada de un empleado. Por lo tanto, es importante que los clientes estén atentos a las transacciones que realizan con sus tarjetas y que monitoreen regularmente sus estados de cuenta bancarios para detectar cualquier actividad sospechosa. [35]

e) Plan contingencia

Cabe destacar y como bien se dijo con anterioridad, esto es un análisis de una red doméstica, y eso conlleva que a diferencia de las redes empresariales, en las redes domésticas no suele haber planes de contingencia en caso de pérdida de información o datos. Esto se debe en gran parte a que las redes domésticas no suelen contar con personal de TI dedicado a la gestión y mantenimiento de la red. Además, muchos propietarios de hogares no consideran la necesidad de tener planes de contingencia para proteger sus datos, ya que no están operando un negocio o empresa, sin embargo, esto no significa que los datos en una red doméstica no sean importantes o valiosos. Muchas personas almacenan en sus dispositivos información personal, como fotos, documentos y archivos de audio y video que son irreemplazables. Además, en muchas ocasiones, los dispositivos conectados a la red pueden contener información confidencial, como contraseñas de cuentas bancarias y de correo electrónico.

f) Conciencia de Ciberseguridad

Actualmente, la PyME cuenta con conocimiento casi nulo en cuanto a la ciberseguridad. Es importante que los propietarios de redes domésticas se conciencien sobre la importancia de tener un plan de contingencia para proteger sus datos. Esto puede incluir medidas como la realización regular de copias de seguridad de la información, la instalación de software antivirus y antimalware y la configuración de contraseñas seguras y de seguridad de la red.

Al las vulnerabilidades a tratar, esto nos exhibe cómo no existe de manera profunda la cultura suficiente sobre ciberseguridad, ya que en su mayoría podemos ver cómo las vulnerabilidades residen en la nula preocupación por actualizar el software que usan, aunque hablando más generalizado, una falta de conciencia sobre ciberseguridad puede llevar a consecuencias como:.

- Pérdida de datos: Si una organización o individuo no toma medidas adecuadas de seguridad cibernética, puede ocurrir una violación de seguridad que resulte en la pérdida de datos. Esto puede incluir datos personales, información financiera o propiedad intelectual. La pérdida de datos puede tener consecuencias financieras y legales graves.

- Exposición de información confidencial: La falta de conciencia sobre ciberseguridad también puede conducir a la exposición de información confidencial. Esto puede incluir información de clientes, estrategias de negocios o secretos comerciales. La exposición de esta información puede dañar la reputación de una organización y ponerla en riesgo financiero.

- Robo de identidad: El robo de identidad ocurre cuando un atacante obtiene información personal, como números de seguridad social o contraseñas, para hacerse pasar por otra persona. Si una organización o individuo no toma medidas adecuadas de seguridad cibernética, pueden ser vulnerables al robo de identidad. Esto puede tener consecuencias financieras graves para la víctima.

- Interrupción del servicio: Las organizaciones pueden experimentar interrupciones del servicio si no toman medidas adecuadas de seguridad cibernética. Esto puede ser causado por ataques de denegación de servicio (DDoS) o por la explotación de vulnerabilidades en los sistemas de la organización. La interrupción del servicio puede afectar la productividad y causar pérdidas financieras.

- Pérdida de confianza del cliente: Si una organización experimenta una violación de seguridad, puede perder la confianza de sus clientes. Los clientes pueden ser menos propensos a hacer negocios con una organización que ha experimentado una violación de seguridad. Esto puede tener consecuencias financieras a largo plazo para la organización.

Plan de Mitigación

Para generar un plan de mitigación se debe entender la topología mostrada anteriormente, la cual consiste en una red en forma de estrella, es decir, todos los dispositivos se conectan a uno mismo. En este caso el centro de la red es el router, haciéndolo el principal objetivo de este plan ya que todos los demás dispositivos se conectan a él y es el que cuenta con el mayor número de vulnerabilidades. Sin embargo, las soluciones pueden resultar muy técnicas y no fáciles de implementar teniendo en cuenta que la PyME no cuenta con un equipo de seguridad dedicado. Es por esto que se opta por el uso de medidas y hábitos más documentados y fáciles de implementar, especialmente en aquellos dispositivos con una interfaz gráfica como el dispositivo móvil de Apple. Por ejemplo, muchas de estas vulnerabilidades se pueden cubrir mediante el cambio de registro en la computadora Windows donde para estos casos se dará una guía paso a paso para evitar cualquier tipo de error debido a que tienden a ser parámetros muy sensibles y pueden resultar en más problemas si se desvía del proceso. Al volver a observar la ***Tabla 1*** se entiende que todas las debilidades consisten de manera general en el uso de versiones anticuadas de protocolo SSL/TLS, SMB y algoritmos de cifrado, implementaciones de SSH, librerías como JQuery para interactuar con páginas web, al igual que el uso de un DNS inseguro. Por lo tanto los siguientes procedimientos consisten en cubrirlos desde los dispositivos mismos.

Para deshabilitar los protocolos SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 [6] y en cambio habilitar el uso de los protocolos TLS 1.2 y TLS 1.3 [7] desde cualquier navegador de internet se sigue el siguiente proceso usando como ejemplo *Mozilla Firefox* [8]:

1. Escribe en la barra de búsqueda '*about:config*' para abrir la configuración y parámetros del navegador,
2. Busca por los términos *'seguridad.tls.version.min'* y *'seguridad.tls.version.max'* indicando las versiones habilitadas del protocolo TLS, y cambia sus valores a 3 y 4 respectivamente.

Es importante mencionar que este tipo de vulnerabilidad también se encontró en el router de la red. Sin embargo, con las medidas tomadas en los demás dispositivos, esta debilidad realmente no se considera de mucha importancia. Asimismo siguiendo las sugerencias dadas por la organización socio formadora, debido a la naturaleza de SSL y TLS, son mucho más relevantes en cuanto se habla de navegadores de red al visitar páginas web y realmente no tienen impacto tan considerable en el contexto de routers como lo hace ver el escaneo de vulnerabilidades.

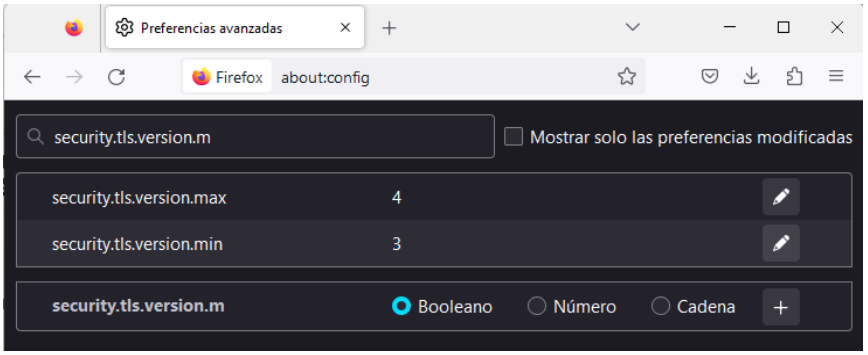

Figura 2. Modificación de versiones mínimas y máximas de TLS. Un valor de 4 indica TLS 1.3, y un valor de 3 indica TLS 1.2 [8].

Este cambio sólo aplica para los navegadores web y no sobre la configuración de los dispositivos mismos. Por lo tanto, un cambio de registro en dispositivos windows [9]. Esto provoca que se usen estos protocolos para encriptar la información de manera segura al realizar mensajería, como email, que no sea mediante páginas web. Un ejemplo de esto es la aplicación de correo que se encuentra predeterminada en Windows. Para realizar los cambios de registro se sigue el siguiente procedimiento usando de referencia [9] y la ***Figura 3***:

1. Entrar a la aplicación Editor de Registro:
2. Seguir la ruta de archivos hasta llegar a "Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols"
3. Realizar click derecho a la carpeta de *Protocols* y elegir la opción *Nuevo* y luego *Clave.*
4. Se creará una carpeta debajo de *Protocols* y crear 4 carpetas cada uno con el nombre del protocolo a deshabilitar.
5. Dentro de cada una de estas carpetas creadas, crear dos nuevas carpetas con los nombres *Server* y *Client*.
6. Dentro de cada una de estas carpetas crear mediante la opción *Nuevo* un Valor de DWORD (32 bits) con nombre *Enabled.* Mostrado en la siguiente figura.
7. El valor de cada uno de estos debería ser igual a 0. Si no, entonces dar click derecho en el valor creado, seguido por *Modificar* y cambiar el valor por un 0.
8. Una vez terminado esto reinicia el dispositivo para aplicar los cambios.

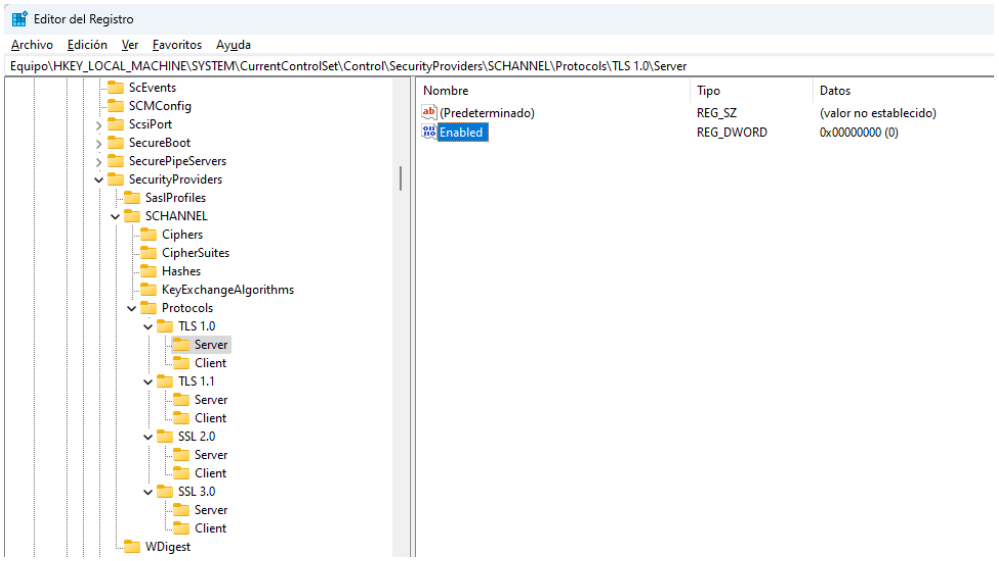

Figura 3. Creación y modificación de valores booleanos para desactivar el uso de protocolos obsoletos en aplicación Editor de Registro en Windows [6].

Al seguir los pasos anteriores, se logra adecuadamente deshabilitar los protocolos SSL/TLS anticuados, mientras que para habilitar las versiones TLS 1.2 y 1.3 se sigue el mismo procedimiento, únicamente agregando sus carpetas y valores correspondientes, estos últimos teniendo un Valor de DWORD igual a 1.

Para los demás sistemas operativos se puede realizar un proceso similar para las aplicaciones de correo donde ya se encuentran opciones para deshabilitarlos individualmente, como en *MacBooks* de Apple. En el contexto de una PyME no supondría práctico actualizar por cada dispositivo, por lo que se puede hacer uso de sistemas operativos enfocados en empresas, como Windows Server [11], específicamente *Windows Server Essentials 2022*. Esta versión permite manejar los servicios de red y aplicaciones dentro de una misma compañía, donde hacer uso de políticas en grupo (*group-policy*) [6] se pueden configurar todos los dispositivos conectados y actualizarlos usando los protocolos más recientes a partir de una sola acción. Sin embargo, por ahora esta recomendación únicamente se menciona tomando en cuenta el potencial crecimiento de la PyME donde se obtenga un mayor número de empleados, por ejemplo unos 50 trabajadores. Por el momento, no se toma en cuenta como uno de las medidas de seguridad de la empresa a adquirir en el momento actual. Este sistema operativo se encuentra en un rango desde aproximadamente 7,000 MXN para la versión de *Essentials 2022* hasta más de 19,000 MXN [11] para la versión *Standard* dependiendo de las necesidades de la misma PyME, siendo la versión de *Essentials.*

Siguiendo con la aplicación de Editor de Registros se puede resolver otra de las vulnerabilidades encontradas: la falta de autenticación o inicio de sesión mediante el protocolo SMB. La solución a esto es en todos los dispositivos de sistemas operativos Windows, en este caso aquel con la IP 192.168.0.170, cambiar los registros del mismo dispositivo y agregar un campo para pedir autenticación y firma de seguridad [2]. Esto se puede realizar con los siguientes pasos referenciados a [19] y ejemplificada con la siguiente figura:

1. Seguir la ruta de archivos hasta llegar a "Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
2. En la sección de *Parameters* modificar el campo de *requiresecuritysignature* al valor de 1 en caso de estar desactivado.
3. Una vez terminado esto reinicia el dispositivo para aplicar los cambios.

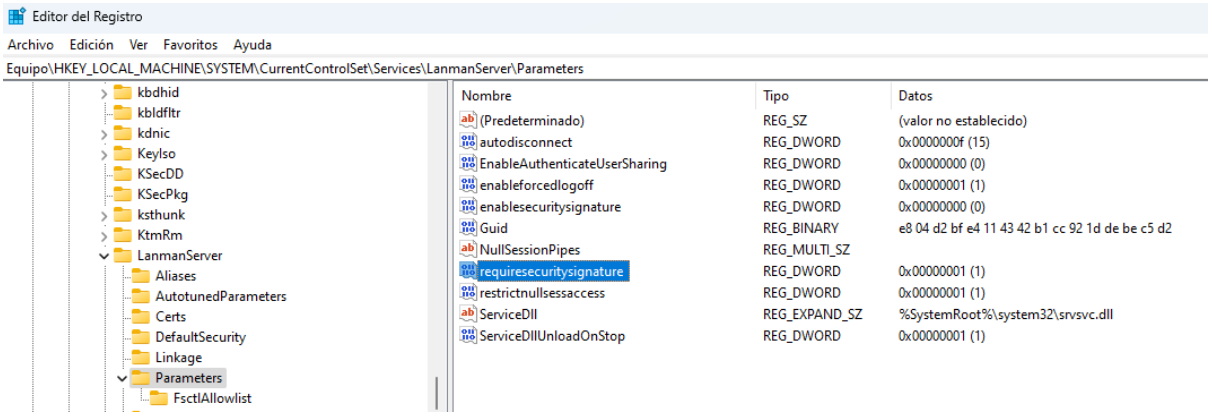

Figura 4. Editor de registros Windows para requerir firma de seguridad.

Otra de las debilidades específicamente en el router es el que el servidor de nombres de dominios (DNS) usado actualmente de 192.168.1.1 y 0.0.0.0 vulnera el caché haciendo que fisgones puedan averiguar cuando se visita una página web. Al cambiar la configuración desde el router para usar las direcciones 8.8.8.8 como primaria y 8.8.4.4 como secundaria para servidor DNS, se usará el servidor de nombres de dominio de *Google Public DNS* [20], conocido por ser más seguro y popular mitigando esta vulnerabilidad. La interfaz del router se encuentra en la siguiente figura. Para entrar a la configuración del router específico de la PyME, se introduce la dirección IP del mismo (192.168.0.1) en cualquier navegador de internet. Al entrar, se introduce la contraseña '*admin*' y se accede a la pestaña de '*Advanced',* seguida de '*Network*' en el menú de la izquierda para seleccionar la opción de Internet como se muestra en la siguiente figura. Una vez abierta la sección se abren las opciones de *Advanced* y se elige la opción de usar una DNS en *'Use the following DNS Addresses'*, introduciendo las direcciones primaria y secundaria anteriormente mencionadas.

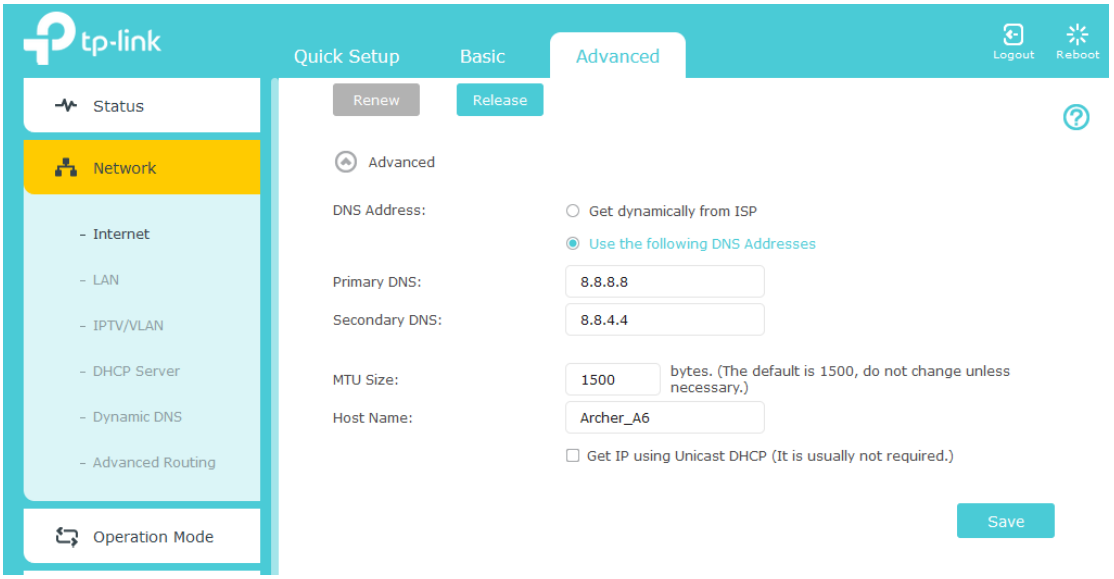

Figura 5. Interfaz de router en opciones para cambiar de servidor DNS.

En uno de los dispositivos se encontró el soporte del protocolo Telnet, el cual es conocido por no contar con ninguna encriptación en el momento de enviar los paquetes siendo una gran vulnerabilidad. Es en el dispositivo con IP 192.168.0.163 (no se pudo identificar tipo de dispositivo) donde se encontró esto, por lo que deshabilitar esta opción y en cambio habilitar el protocolo SSH sería la solución. Asumiendo que se trata de una computadora, como alguno de Microsoft, se puede realizar esto de manera fácil al desactivarlo en un menú de características del dispositivo como se encuentra en la siguiente figura [21].

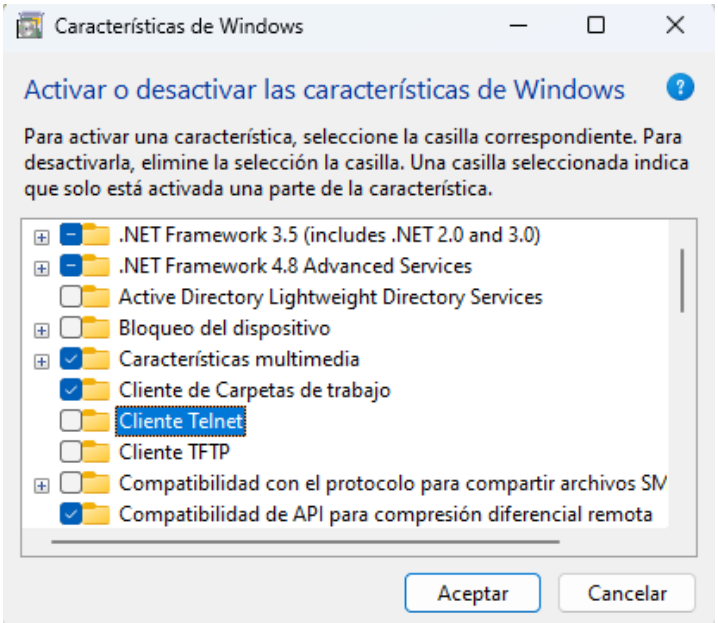

Figura 5. Ventana para desactivar el uso de protocolo Telnet.

Una vez haciendo esto se puede habilitar SSH al entrar a la aplicación de Servicios del dispositivo [22] y asegurarse de que se está habilitado (con un tipo de inicio preferiblemente automático) y se ejecuta una vez se inicia a usar el dispositivo. En caso de no aparecer en ejecución, modificar esta opción dando click derecho en el servicio y abriendo sus propiedades. Después se elige la opción de inicio automático y oprimiendo el botón de iniciar en la sección de estado de servicio.

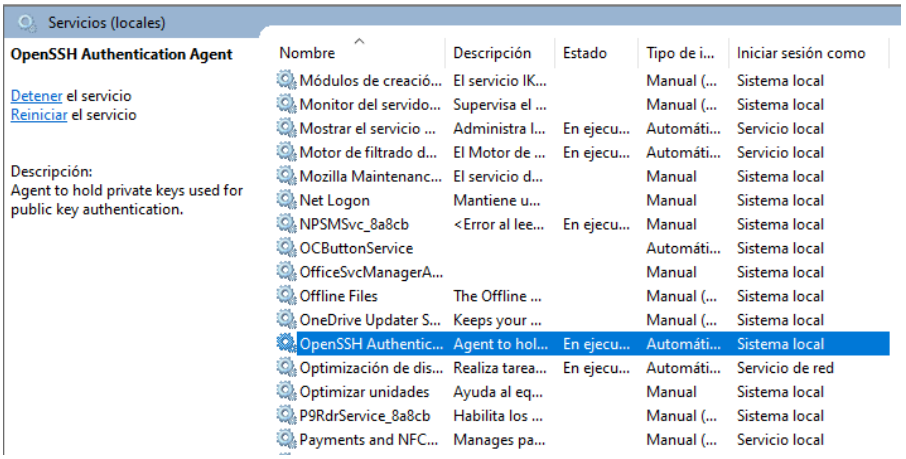

Figura 6. Ventana de servicios para habilitar el uso de SSH.

Para la actualización de Dropbear SSH, se debe actualizar el firmware del router debido a que la vulnerabilidad se encuentra ahí mismo. Conociendo que el router se trata de un dispositivo de TP-Link, las actualizaciones se encuentran en su página principal en [26]. Una vez descargado este archivo en cualquier dispositivo que esté conectado a la red, se puede acceder a la configuración del router explicado anteriormente y dirigirse a la sección de *System Tools*. Una vez aquí se accede a la opción de *Firmware Update* donde se puede realizar una actualización manual visto en la siguiente figura. El archivo a usar sería el archivo descargado con este propósito.

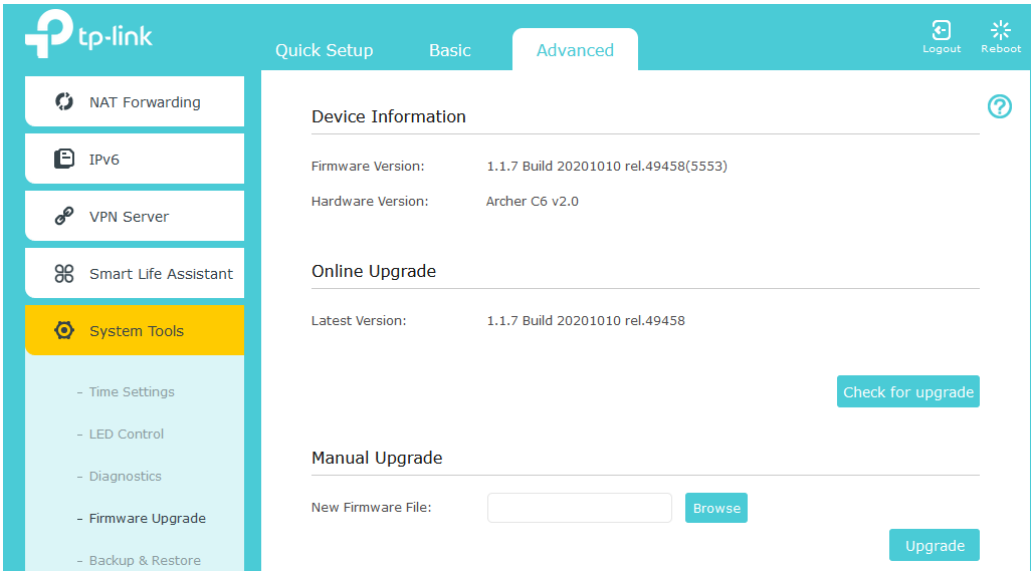

Figura 7. Configuración de router para actualización manual de firmware.

Finalmente, la última vulnerabilidad a cubrir consiste en el uso de una versión anticuada de JQuery al interactuar con páginas web. Para resolver esta vulnerabilidad encontrada en uno de los dispositivos genéricos, se debe consultar la documentación de la librería [32] y descargar una versión mayor 3.5 en el mismo dispositivo. Después se debe reemplazar la versión anticuada por la nueva. Conociendo que esta librería más que nada se usa en la interacción y creación de páginas web (por ejemplo en un archivo HTML).

No obstante, no por realizar todos estos cambios y procesos la PyME puede evitar cualquier tipo de ataque. Otras medidas no técnicas son altamente relevantes para mantener la seguridad de la información sensible de los clientes y del mismo negocio. Es por esto que a continuación se mencionan medidas de aspecto operativo.

Existen también otras alternativas para la enfrentar los ciberataques a los que están vulnerables la PyMEs; estas soluciones son llamadas Controles CIS. Los puntos de referencia del Centro de Seguridad de Internet (CIS) son un conjunto de prácticas recomendadas reconocidas y consensuadas a nivel mundial para ayudar a los profesionales de la seguridad a aplicar y administrar las medidas de protección de seguridad cibernética. [43]

Analizando las vulnerabilidades presentadas en el scan, se puede optar por usar el Control CIS 15, en el cual se denomina como Control de Acceso Inalámbrico (Wireless Access Control); su finalidad es basa en asegurarse que los controles de acceso, autenticación y encriptación sean adecuados para proteger la red inalámbrica de una organización y evitar que dispositivos no autorizados puedan acceder a ella. [44]

Sanitización de información sensible

Una de las prácticas más comunes y efectivas para evitar ataques contra la integridad de información sensible para cualquier red, sea doméstica o empresarial, es el respaldo de información. Al usar *Windows Server Essentials* se habilita el respaldo de información para todos los clientes guardados en el servidor, e incluso se puede realizar respaldo del servidor mismo desde una unidad de almacenamiento externo como USB o discos de estado sólido [38]. Por otro lado, conociendo que crear y mantener un servidor puede resultar fuera de presupuestos de muchas PyMEs, algunas alternativas incluyen simple sanitización de datos, es decir, el remover o censurar deliberadamente información sensible para proteger su privacidad [48]. Esto se recomienda realizar en datos confidenciales donde su uso no sea recurrente o de constante uso (por ejemplo, la información personal del núcleo familiar de un empleado). En caso de todavía planear el uso de esta información se puede optar mantener esta información sensible en un dispositivo de almacenamiento que no tenga conexión a la red para evitar ataques tipo *Man-in-the-Middle*, entre otros.

Red Privada Virtual (VPN)

Una *VPN* [40], mejor conocida como una red privada virtual, sirve para la creación de una conexión entre una red privada y dispositivos a través de Internet. Se utilizan para la transmisión de datos a redes públicas de forma segura y anónima, de forma que ocultan las direcciones IP de los usuarios cifrando los datos para que alguien sin autorización no pueda recibirlos o leerlos. Al elegir una VPN, es importante buscar una que tenga buena reputación y que ofrezca encriptación segura, velocidades rápidas y un buen soporte al cliente. Algunas opciones populares incluyen *NordVPN*, *ExpressVPN* y *CyberGhost VPN* [15] [16] [17]. Estas opciones se caracterizan por no solo ofrecer los servicios de una Red Privada Virtual a rango de hasta 7 dispositivos, sino también ofrecen servicios como gestores de contraseñas, haciendo este último, CyberGhost VPN, la opción recomendada. Esto se debe grandemente a su bajo precio de aproximadamente 1100 MXN por dos años y el presupuesto de la PyME. Es importante mencionar que debido al límite de dispositivos, la VPN se debe únicamente encontrar en los dispositivos principales de todos los empleados.

Listas de Control de Acceso (ACL)

Esencialmente, el firewall [51] actúa como una barrera de seguridad entre la red interna y el Internet u otras redes externas. El objetivo principal de un firewall es proteger la red y los sistemas informáticos contra posibles amenazas y ataques cibernéticos. Los firewalls inspeccionan todo el tráfico de red que fluye a través de ellos y aplican reglas de seguridad predefinidas para permitir o bloquear el acceso a los recursos de la red en función de los criterios de seguridad definidos. Estas reglas pueden ser simples, como bloquear todo el tráfico entrante excepto el tráfico web, o pueden ser más complejas y específicas, como permitir solo el acceso a ciertos servicios y puertos desde ciertas direcciones IP.

Para establecerlo se puede realizar listas de control de acceso (ACL) [52] La cual es una lista de reglas que se utiliza para filtrar el tráfico de red en función de la dirección IP, protocolo y/o puertos. A menudo se utiliza en routers y switches de red para permitir o bloquear el tráfico en función de los criterios definidos. Las ACL se pueden utilizar para bloquear el tráfico de entrada y salida en una interfaz de red específica, pero no pueden proporcionar una protección completa de la red como lo hace un firewall. Estas listas se pueden configurar desde la interfaz del router/módem en cualquier navegador. Esto se puede realizar al crear *Blacklists* y *Whitelists*, los cuales indican qué direcciones IP o dispositivos se les deniega o permite entrar a la red respectivamente, visto en la siguiente figura.

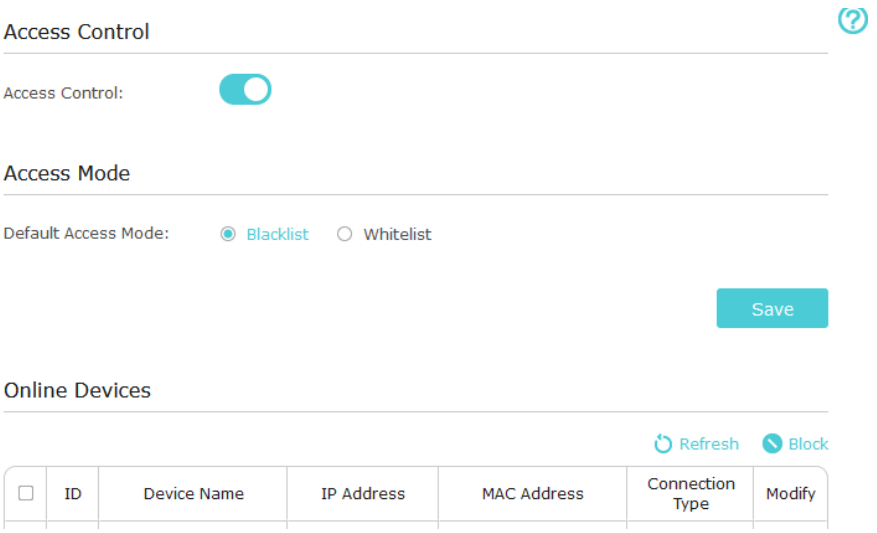

Figura 8. Configuración de listas de control de acceso en interfaz del router/modem de red.

Antivirus

Otra de las medidas recomendadas para cualquier dispositivo conectado a una red es el antivirus [42]. Su finalidad principal es detectar y erradicar cualquier tipo de virus informático, sin embargo, al ir evolucionando los diversos sistemas operativos es necesaria su actualización de forma constante, de tal manera que sean capaces de detectar los virus, bloquearlos, hacer limpieza de ellos e incluso prevenir su posible invasión al dispositivo. Diferente a las VPN, no tratan de mantener segura la transmisión de paquetes, sino tratar de eliminar programas maliciosos ya encontrados en el dispositivo. Es importante tener un antivirus como también actualizado y en funcionamiento para evitar infecciones por malware y proteger nuestros datos y privacidad en línea. Al elegir un antivirus, es relevante buscar uno que tenga una buena reputación, con una tasa alta de detección de malware, y con un precio razonable, tomando en cuenta redes domésticas y PyMEs. Algunas opciones populares incluyen Norton, Kaspersky y McAfee. Sin embargo, en el contexto de la PyME que cuenta con 4 empleados, se recomienda a los productos de *Bitdefender* [54] enfocado en estas pequeñas empresas. En el plan de *GravityZone Business Security* ofrecen servicios de antivirus anuales donde proteger 20 dispositivos (computadoras y dispositivos móviles) significa un precio de aproximadamente 500 MXN requiriendo conocimientos mínimos o incluso nulos al hablar de Tecnologías de Información. Con esto se pueden proteger todos los dispositivos relevantes a la compañía, incluyendo los de los empleados, e incluso para más. Esto lo convierte en la mejor opción debido al presupuesto ajustado y el actual número de dispositivos incluyendo el de los empleados. Este plan cuenta con una gran variedad de herramientas [54] como detectores de amenazas, generación de reporte de ataques, control de aplicación de antivirus, firewall, entre otras.

Anomalía o Vulnerabilidad	**Solución**	**Descripción**	**Costo en MXN (Anual)**
Ataques Man-in-the-Middle	Sanitización de información sensible	Remover o censurar deliberadamente información sensible para proteger su privacidad [48]	Ninguno
Riesgo de exposición de datos a terceros	Red privada virtual	Conecta los dispositivos a través de internet a una red privada para la segura y anónima transmisión de datos encriptados. [40]	$547.105

Anomalía o Vulnerabilidad	Solución	Descripción	Costo en MXN (Anual)
Dispositivos no actualizados	Windows Server Essentials (opcional en caso de ser requerido)	Al tener varios dispositivos en una empresa es complicado mantener todos actualizados y con su información sanitizada, es por esto que un server es capaz de mantener todos los dispositivos de la red en orden. [38]	$7500 (OPCIONAL)
	Actualización de firmware, software, y protocolos	Seguir las guías indicadas y referenciadas para la actualización a, por ejemplo, protocolos TLS más seguros	Ninguno
Red vulnerable	Listas de control de acceso	Permiten a los atacantes interceptar y robar datos transmitidos mediante una red Wi-Fi [41]	Ninguno
Potenciales virus y ataques comunes	Antivirus	Detecta y erradica virus informáticos al bloquearlos eliminarlos y prevenir una potencial invasión. [41]	$493.49
Inyección de código malicioso			

Tabla 2. Cotización de costo promedio anual de aplicar plan de mitigación

Discusiones y Resultados

El plan recomendado para la PyME es donde no se incluye *Windows Server Essentials* concluyendo en un costo promedio anual de 1040.60 MXN, el cual se encuentra dentro del presupuesto inicial de 2900 MXN. No únicamente eso, sino también todas las soluciones tienen enfocados el hecho de que la compañía cuenta con casi nulo conocimiento de TI como se justificó en la elección de servicios fáciles de implementar. En el caso donde la PyME requiera en el futuro cuando se haya expandido, se puede incluir *Windows Server Essentials* de un solo pago de 7500 MXN y se puede usar en uno de los dispositivos, por ejemplo, con los que ya cuenta el dueño. Este plan ya toma en cuenta el crecimiento de la PyME donde los servicios de antivirus y VPN ya se cubren en más de los dispositivos con los que actualmente usan los trabajadores para la compañía. Después del año siguiente, la PyME únicamente debería pagar por las nuevas suscripciones del antivirus siendo 493.49 MXN el único costo en cuestión de seguridad. Sin embargo en el segundo año nuevamente se tendrá que renovar los servicios VPN llegando nuevamente al costo de 1040.60 MXN.

Debido a la facilidad de aplicación de los servicios VPN y de antivirus elegidos, la implementación del plan es casi inmediata como comprar los servicios e instalarlos en los dispositivos. Asimismo, gracias al poco conocimiento de TI por parte de la PyME se optó por no cambiar la topología de la red. En su lugar, soluciones de bajo costo y fáciles de implementar fueron planeadas. En el caso futuro de contar con especialistas en esta área y con una mayor infraestructura sí se recomendaría modificarla, ya que se le otorga demasiada importancia al centro de la red (en este caso el router) y puede ser un punto vulnerable.

Al no implementar este plan de mitigación, el sistema de operación de la PyME y la información sensible de tanto de los clientes como los trabajadores se encuentra vulnerable a los numerosos ataques cibernéticos que tienen a ser más comunes en estas microempresas [33]. Fisgones, o ataques *MITM*, pueden obtener los domicilios de las personas involucradas en la venta de la indumentaria al igual que información bancaria afectando altamente de forma negativa las finanzas de la PyME. En el caso de ser atacado por programas maliciosos debido a la falta de un antivirus que tome como rehén el acceso a la cuenta *Facebook* puede ser denegada por un adversario teniendo virtualmente total control de la empresa por un tiempo indefinido. En cualquiera de los dos casos, la compañía sufriría grandes golpes económicos finalmente impactando sus planes de crecimiento a un mayor estrato en cuestión de PyMEs.

El plan de mitigación de forma general y resumida se puede ver como la siguiente forma:

- Actualización de protocolos como TLS, Dropbear SSH, y librerías en los dispositivos mismos o navegadores de internet usando guías detalladas.
- Actualización de firmware de router.
- Deshabilitación de protocolos anticuados como SSL 2.0, 3.0, TLS 1.0, 1.1, y Telnet mediante cambio de registros y características de los dispositivos usando guías detalladas..
- Cambio de DNS del router a uno más seguro.
- Configuración de firewall en interfaz del router permitiendo y denegando acceso de dispositivos a la red.
- Sanitización de información sensible.
- Contratación de servicios VPN y antivirus.

Conclusiones

A lo largo de la realización de este proyecto fuimos desarrollando nuestras habilidades y competencias relacionadas al análisis de vulnerabilidades que afectan a todas las personas que puedan utilizar la red en cuestión, y observamos el qué tan vulnerables están nuestros dispositivos a los hackers que intenten sustraer nuestra información personal y/o empresarial. Enfocándonos en las vulnerabilidades de alto y medio nivel, podemos observar que la mayoría consisten en uso de protocolos y esquemas anticuados, como el uso de Dropbear SSH así como el uso de SSL, pueden resolverse una buena cantidad de estas vulnerabilidades simplemente actualizando a sus versiones más recientes.

Nos fue posible realizar un buen plan de evaluación de la red haciendo uso de software más accesible, de bajo costo o incluso con un periodo de uso gratuito. Esto se debe a que trabajamos con una red doméstica bastante simple, lo que significa que casi cualquier persona con una topología similar a la que fue analizada durante el reto puede aplicar los métodos para prevenir las vulnerabilidades mencionadas anteriormente, pues son relativamente simples y fáciles de comprender o ejecutar al hablar en términos de ciberseguridad. Sin embargo, este tipo de redes siguen, hasta cierto punto, asimilándose a aquellas encontradas en empresas medianas y pequeñas, por lo que no se debe descartar para emular sus topologías.

Para el plan de mitigación, se pudieron encontrar una variedad de métodos de solución de las vulnerabilidades encontradas, específicamente 27 de las 28 de estas fueron resueltas, o 96.4% de las debilidades totales. La única que no se resolvió fue mayormente debido a su baja calificación CVSS considerándolo negligible. Igualmente se mencionaron varias prácticas de seguridad para evitar cualquier tipo de ataque que pueda dañar a la PyME. Finalmente, en la cotización dada se tomó en cuenta el precio de inicio más el precio de mantenimiento para aquellas medidas y recomendaciones tomando en consideración las necesidades y presupuesto de la PyME. Es por esto que se considera esta auditoría de seguridad y plan de mitigación adecuados, ya que se toma en cuenta su presupuesto, conocimiento de TI y ciberseguridad, simpleza de la topología de red, y planes de crecimiento futuro. Se mantuvieron soluciones fáciles, casi inmediatas, guías detalladas para implementarlas, y de bajo costo sino algunas gratuitas, donde se pueden aplicar para redes similares (como la mayoría de redes domésticas). Es con todas estas características del plan de mitigación que pudimos presentar una propuesta que seguramente pueda evitar que esta PyME se convierta en una estadística en cuanto al gran surgimiento de ciberataques hacia pequeñas empresas.

Referencias

[1] Lizarazo, C. (30 de enero de 2023) Las PyMEs en México: Retos e importancia. Conekta. Recuperado el 23 de febrero de 2023, de: https://www.conekta.com/blog/las-pymes-en-mexico-retos-e-importancia

[2] Tenable Network Security, Inc. (s.f.). Nessus [Software] https://www.tenable.com/products/nessus

[3] Meta (24 de enero de 2023) WhatsApp Encryption Overview. Recuperado el 18 de marzo de 2023, de: https://scontent.fntr3-1.fna.fbcdn.net/v/t39.8562-6/328495424_498532869106467_7563034122059495 48_n.pdf?_nc_cat=104&ccb=1-7&_nc_sid=ad8a9d&_nc_ohc=bFvRJj_Ww3EAX9AFdPm&_nc_ht=sc ontent.fntr3-1.fna&oh=00_AfDiHSrS0uO8HtqYCiwS7SXjhZO7Ju813l-XgW6B25rC9g&oe=641BA0 3C

[4] INEGI (2012) Encuesta Nacional de Micronegocios (ENAMIN) 2012. Recuperado el 19 de marzo de 2023, de: https://www.inegi.org.mx/programas/enamin/2012/#Tabulados

[5] Cisco Systems, Inc. (2020). Cisco Packet Tracer (Version 7.3) [Computer software]. Cisco Networking Academy.

[6] [InfoSec Governance] (febrero de 2016). How to disable SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1 in Windows 10. [Video]. YouTube. Recuperado el 8 de marzo de 2023, de: https://www.youtube.com/watch?v=oh2gfGYoytw

[7] KL, A. (s.f.) How to Enable TLS 1.2 and TLS 1.3 on Windows Server. TheSecMaster. Recuperado el 8 de marzo de 2023, de: https://thesecmaster.com/how-to-enable-tls-1-2-and-tls-1-3-on-windows-server/

[8] Kemmerer, C. (s.f.) Desactive SSL 3.0 y TLS 1.0 en su navegador- SSL.com. Recuperado el 8 de marzo de 2023, de: https://www.ssl.com/es/c%C3%B3mo/apague-ssl-3-0-y-tls-1-0-en-su-navegador/

[9] Yasar, K. Lockhart, E. (junio de 2022). Windows Registry Editor (regedit). TechTarget. Recuperado el 8 de marzo de 2023, de: https://www.techtarget.com/searchenterprisedesktop/definition/Windows-Registry-Editor

[10] Modelos de plan de Negocios (2023). Abrir una tienda de ropa: ingresos, gastos y beneficios. Recuperado el 8 de marzo de 2023, de: https://modelosdeplandenegocios.com/blogs/news/abrir-tienda-ropas-ingresos-gastos-rentabilidad

[11] Microsoft. (s.f.). Windows Server. Recuperado el 8 de marzo de 2023, de: https://www.microsoft.com/es-mx/windows-server

[12] Greenbone Networks GmbH. (s.f.). OpenVAS. Recuperado el 28 de febrero de 2023, de https://www.greenbone.net/en/technology/openvas/

[13] Combs, G. (1998) *Wireshark* [Software]. Recuperado el 1 de marzo de 2023, de https://www.wireshark.org/

[14] Lyon, G. (1997). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.Org.

[15] ExpressVPN. (2023). What is a VPN and why do you need one? Recuperado el 6 de marzo de 2023, de: https://www.expressvpn.com/what-is-vpn

[16] CyberGhost VPN. (2023). Why should you choose CyberGhost VPN? Recuperado el 6 de marzo de 2023, de: https://www.cyberghostvpn.com/es_ES/buy/cyberghost-vpn-3

[17] NordVPN. (2023). Why NordVPN is your best choice for online security. https://nordvpn.com/why-nordvpn/

[18] Euromonitor International. (2022). Sportswear in Mexico. Recuperado el 8 de marzo de 2023, de: https://www.portal.euromonitor.com/statisticsevolution/index

[19] STIGViewer (s.f.) The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled. Recuperado el 8 de marzo de 2023, de: https://www.stigviewer.com/stig/windows_server_2016/2018-03-07/finding/V-73661

[20] CleanBrowsing (s.f.) Change DNS on a TP-Link Router. Recuperado el 11 de marzo de 2023, de: https://cleanbrowsing.org/help/docs/change-dns-on-a-tp-link-router/

[21] Eleventa (s.f.) Pruebas de conexión Telnet en windows. Recuperado el 11 de marzo de 2023, de: https://eleventa.com/aprender/conexion-telnet

[22] Yúbal, F. (9 de julio de 2020) SSH en Windows 10: qué es y cómo configurarlo. *Xataka.* Recuperado el 11 de marzo de 2023, de: https://www.xataka.com/basics/ssh-windows-10-que-como-configurarlo

[23] Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. CRC Press

[24] Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.

[25] Avoine, G., Canard, S., & Ferreira, L. (2019). IoT-friendly AKE: forward secrecy and session resumption meet symmetric-key cryptography. In Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part II 24 (pp. 463-483). Springer International Publishing.
[26] TP-Link (s.f.) Descarga para Archer C6 V4.6. Recuperado el 11 de marzo de 2023, de: https://www.tp-link.com/mx/support/download/archer-c6/
[27] Cert.org. (2015). SSL and TLS Deployment Best Practices. Recuperado el 6 de marzo de 2023, de: https://www.cert.org/historical/advisories/CA-2002-23.cfm
[28] Gerend, J. et al. (27 de enero de 2023) Información general sobre el uso compartido de archivos mediante el protocolo SMB 3 en Windows Server. Microsoft Learn. Recuperado el 23 de febrero de 2023, de: https://ayudaleyprotecciondatos.es/2021/03/04/protocolo-smb/
[29] IBM. (28 de enero de 2023) Protocolos de seguridad de cifrado: TLS. IBM. Recuperado el 23 de febrero de 2023, de: https://www.ibm.com/docs/es/ibm-mq/9.1?topic=mechanisms-cryptographic-security-protocols-tls
[30] Donohue, B. (10 de abril de 2014) ¿Qué Es Un Hash Y Cómo Funciona? Kaspersky. Recuperado el 23 de febrero de 2023, de: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/
[31] IBM. (3 de marzo de 2021) Protocolo Telnet. IBM. Recuperado el 23 de febrero de 2023, de: https://www.ibm.com/docs/es/aix/7.1?topic=protocols-telnet-protocol
[32] jQuery (2023) jquery. Recuperado el 6 de marzo de 2023, de: https://jquery.com.
[33] Verizon (2023) Diving back into SMB breaches. Recuperado el 6 de marzo de 2023, de: https://www.verizon.com/business/resources/reports/dbir/2021/smb-data-breaches-deep-dive/
[34] ¿Qué es un router? - Definición y usos. (2021, October 18). Cisco. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html
[35] Leyva-Montero, M. L., & Colín-Castro, C. A. (2021). Seguridad de la información en procesos de pago con tarjeta bancaria. Revista Internacional de Seguridad de la Información, 1(1), 45-57.
[36] Crea un hogar inteligente con los dispositivos que quieras. (s.f.). https://home.google.com/intl/es_es/what-is-google-home/#:~:text=La%20aplicaci%C3%B3n%20Google%20Home%20es,reproducir%20las%20noticias%20y%20m%C3%A1s.
[37] Reuters (30 de enero de 2023) Britain's JD Sports says customer data accessed by cyber attack Recuperado el 6 de marzo de 2023, de: https://www.reuters.com/business/retail-consumer/uks-jd-sports-says-some-customer-data-compromised-online-orders-2023-01-30/
[38] Microsoft. (s.f.). Manage Windows Server Essentials. Learn. Recuperado el 9 de marzo de 2023, de: https://learn.microsoft.com/en-us/windows-server-essentials/manage/manage-windows-server-essentials
[39] Kaspersky (2022). ¿Qué es la inyección de SQL? Definición y explicación. RECUPERADO EL 19 de marzo de 2023, de: https://latam.kaspersky.com/resource-center/definitions/sql-injection
[40] Cisco Systems, Inc. (s.f.). What is a VPN? *Cisco*. Recuperado el 9 de marzo de 2023, de: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html
[41] Norton (s.f.). Qué hacer con respecto a la vulnerabilidad de la red Wi-Fi WPA2. Recuperado el 19 de marzo de 2023, de: https://mx.norton.com/blog/emerging-threats/what-to-do-about-krack-vulnerability#:~:text=La%20vulnerabilidad%2C%20conocida%20como%20%22KRACK,mediante%20una%20red%20Wi%2DFi.
[42] Cisco Systems, Inc. (s.f.). Advanced Malware Protection (AMP). *Cisco*. Recuperado el 6 de marzo de 2023, de: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-antivirus-protection.html#~how-viruses-work
[43] Amazon Web Services, Inc. (s.f.) ¿En qué consisten los puntos de referencia del CIS? Recuperdo el 19 de marzo de 2023, de : https://aws.amazon.com/es/what-is/cis-benchmarks/#:~:text=Los%20puntos%20de%20referencia%20del%20Centro%20de%20Seguridad%20de%20Internet,de%20protecci%C3%B3n%20de%20seguridad%20cibern%C3%A9tica.
[44] CIS Controls. (2018). Center for Internet Security. Recuperado 14 de marzo de 2023, de https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf
[45] Amazon Web Services. (s.f.) ¿Qué es DNS? *AWS.* Recuperado el 23 de febrero de 2023, de: https://aws.amazon.com/es/route53/what-is-dns/

[46] Microsoft (1 de marzo de 2023) Comprender los conceptos básicos de direccionamiento TCP/IP y subredes. Recuperado el 23 de febrero de 2023, de: https://learn.microsoft.com/es-es/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting
[47] Johnston, M. (14 de noviembre de 2022) Dropbear SSH. Recuperado el 11 de marzo de 2023, de: https://matt.ucc.asn.au/dropbear/dropbear.html
[48] Stanford University. (2008). Data destruction guidelines (Version 1.02). Recuperado el 9 de marzo de 2023, de: http://www.stanford.edu/group/security/securecomputing/files/data_destruction_guidelines_v102.pdf
[49] NordLayer. (s.f.). Next-generation business VPN. Recuperado el 6 de marzo de 2023, de: https://nordlayer.com/
[50] TechTarget. (s.f.). Advanced Encryption Standard (AES). Recuperado el 9 de marzo de 2023, de: https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard
[51] McAfee. (15 de mayo de 2020). ¿Qué es un firewall?. Recuperado el 9 de Marzo de 2023, de https://www.mcafee.com/es-mx/antivirus/firewall.html
[52] E. (2019, December 25). ACLs, Listas de Control de Acceso. Enredando Con Redes . . . Recuperado el 9 de Marzo de 2023, de https://enredandoconredes.com/2015/01/08/acls-listas-de-control-de-acceso/
[53] NortonLifeLock. (s.f.). Norton AntiVirus Plus. Recuperado el 6 de marzo de 2023, de: https://us.norton.com/products/norton-antivirus-plus
[54] Bitdefender. (s.f.). Las mejores ofertas para empresas. Recuperado el 6 de marzo de 2023, de: https://www.bitdefender.es/business/deals/