UNIVERSIDAD TÉCNICA BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESOS TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRACTICA

INGENIERÍA EN SISTEMAS de Información

TEMA:

Análisis De Vulnerabilidades En La Red Del Isp: "CAFANET" Parroquia Isla De Bejucal, Año 2022

EGRESADA(O):

Rosa Mercedes Haro Huerta

TUTOR:

Ing. Nelly Karina Esparza Cruz

AÑO 2022

Contenido

Planteamiento del problema

Planteamiento de problema a nivel mundial y Latinoamérica de acuerdo al documento de María Espinoza Apráez aclara que nivel mundial se han realizado estudios en diferentes países en cuanto a la seguridad de las redes inalámbricas, dando resultados alarmantes de la situación de las mismas. Según estudios internacionales realizados en Bolivia, México, Uruguay, Argentina, Canadá, España y entre otro se dice que, de 905 redes, 374 el 41.33% disponen de algún sistema de cifrado, mientras que de 531 redes el 2 58.37% carecen de cifrado. De esta manera se ha comprobado que los usuarios y los administradores de la red inalámbrica de las organizaciones no ponen énfasis en lo que es seguridad de la información, a pesar de que en otros países el nivel de conocimiento es más avanzado. Debido a que estas redes son públicas y se las puede encontrar en varias zonas alrededor del mundo, cualquier persona con un dispositivo inalámbrico sea laptop, tablet, PDA, etc. se pueden conectar a la red inalámbrica sea para navegar por internet o para tener acceso a los datos.

En cuanto a nivel nacional, el Ecuador se puede decir que en los últimos meses el término seguridad informática se encuentra en auge, debido a los diferentes ataques que se han efectuado en las páginas web del gobierno. A raíz de este acontecimiento se ha puesto más interés a las seguridades que deben poseer las organizaciones para prevenir ataques. En el área de la seguridad en redes según un estudio realizado en la ciudad de Quito empleando programas informáticos para estos fines, se dice que un 93% de las redes inalámbricas son vulnerables a ataques maliciosos, información obtenida del diario El Comercio, con el tema “las redes wifi en Quito no son seguras”. Dejando muy claro que la seguridad informática es un campo aun no explotado en el país. (Apráez, 2013)

La empresa “CAFANET” está ubicada en la parroquia Isla Bejucal perteneciente al cantón Baba – Prov. Los Ríos, en junio de 2020 se crea la empresa proveedora de Internet siendo César Augusto Flores Avalos dueño de la empresa.

En este trabajo de investigación se refiere a la presentación de un análisis de riesgos y vulnerabilidades de la información, en donde nos permite identificar, analizar, evaluar los diferentes tipos de riesgo que se tiene en una organización, permitiendo establecer controles o salvaguardias con la finalidad de mitigar el riesgo.

La empresa se enfrenta con una disminución de clientes anuales debido al mal mantenimiento del servicio del internet. El dueño de la empresa está preocupado porque

cree que la inestabilidad de sus clientes si afectando el proceso de crecimiento de la empresa y por ende también está inquietando a los trabajadores. Teme que, si no se hace nada, los trabajadores tendrían que ser despedidos y la imagen de la empresa se verá dañada.

¿Cuál es la causa del problema?

Uno de los principales problemas que tenían la empresa era que no tiene una persona capacitada en el mantenimiento de los equipos de la red, y el personal técnico no estaban capacitados para solventar los problemas de los clientes ya que no es su área de trabajo.

Mediante el análisis de los riegos informáticos que se realizó en la empresa CAFANET cuando realizaba las practicas preprofesionales, nos dio a conocer las principales vulnerabilidades que afectan a los equipos Mikrotik de la red son;

- Problemas protocolo IP servicie
- Seguridad de contraseña y usuarios en los equipos
- Equipos no actualizados
- Ataques de virus hacia la red

Están son las principales causas por la cual el servicio del internet es deficiente.

Para resolver estas vulnerabilidades se procede tomar en cuenta las siguientes recomendaciones:

- Implementar reglas de firewall para mitigar ataques de red
- Implementación de un servidor DNS para garantizar mejor el servicio del internet
- Actualización correcta de los equipos utilizados en la red para así tener las versiones más recientes y tener más seguros nuestros equipos
- Implementación de usuarios y claves a los equipos de la red que solo tendrá accesos el dueño y el encargado del mantenimiento de la red.

Con estas herramientas se garantizará la mejora de servicios de internet, ya que estará controlando de una mejor manera la red, ya que la mayoría de vulnerabilidades las podemos encontrar en los equipos Mikrotik de la empresa, y de esta forma estará protegida de ataques de virus y en trabajos futuros, se podría analizar otras alternativas de mitigación para los mismos tipos de vulnerabilidades de la empresa.

Justificación

Ante esta situación, de la pérdida de clientes anuales que ha sufrido la empresa por el descuido del mantenimiento de la red, por ende realizaremos una investigación que surge por la necesidad de amortiguar la falencia que tiene la empresa Cafanet, se realizara el análisis correspondiente de cómo se encuentra el estado de la red, pero, con el fin de identificar las falencias de la red además; con los avances tecnológicos y el crecimiento del internet se ve en la necesidad de ir mejorando día a día para disponer de fuentes de consulta y contar con el conocimiento de nuevas tecnologías.

Hoy en día ya es común escuchar de diversos ataques de seguridad y vulnerabilidades a redes de fibra óptica y por este medio a los servidores de la red interna, es por esta razón que es necesario un análisis de vulnerabilidad de la red inalámbrica que permitirá encontrar posibles falencias en la seguridad y de la misma manera mejorar el servicio que brinda a los usuarios y evitar posibles ataques a los servidores y caídas al sistema.

Objetivo General

Identificar vulnerabilidades de seguridad para así implementar reglas de firewall y DNS seguros, para de esa manera garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos de los clientes de la empresa CAFANET de la parroquia Isla de Bejucal.

Objetivos Específicos

- Realizar pruebas de testeo a la red de datos que permita diagnosticar las vulnerabilidades en la red inalámbrica de la CAFANET.

- Evaluar las vulnerabilidades encontradas de acuerdo a los riesgos detectados en la revisión de la red.

- Implementar estrategias de mitigación de ataques encontrados para prevenir y fortalecer la seguridad en la red.

Línea de Investigación

El desarrollo de este caso de estudio tiene como objetivo, identificar las falencias de seguridad para así implementar reglas de firewall y DNS seguros, para de esa manera garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos de los clientes de la empresa CAFANET.

En este caso de estudio se realizará siguiendo los lineamientos determinados en la línea de investigación de sistemas de información y comunicación, emprendimiento e innovación, y en la sub línea de investigación que comprende las redes y tecnologías inteligentes de software y hardware, mediante un análisis de vulnerabilidades respecto a la infraestructura de la red en especial en los equipos mikrotik de la empresa CAFANET de la parroquia Isla Bejucal.

La seguridad es uno de los aspectos fundamentales de acuerdo con las enseñanzas de asignaturas como seguridad de la información de redes y comunicación para obtener un adecuado funcionamiento de la red, ya que mediante la seguridad se respalda la integridad y confidencialidad de los datos. Un abuso a la seguridad implica generar serios daños en la estabilidad de la red. La exclusión de políticas de seguridad podría generar la pérdida de datos importantes dentro de una organización. La gerencia en la toma de decisiones, para el tratamiento del riesgo mediante normas, estándares y buenas prácticas, sin afectar la información de la empresa “CAFENET” y tener continuidad en el negocio y alcanzar los objetivos planteados por la organización, para que estos procesos se lleven a cabo se enumeraron todos los activos de la organización que fueron identificados mediante una metodología de buenas prácticas en normas y estándares, que fueron considerados para la valoración del activo (hardware, software, y datos), valoración del impacto e identificación de las vulnerabilidades.

Marco conceptual

Este caso de estudio, se desarrolla en la empresa "CAFANET" está ubicada en la parroquia Isla Bejucal perteneciente al cantón Baba – Prov. Los Ríos, y provee servicios de internet, teniendo además un valor agregado que es brindar servicios de televisión por medio de la fibra óptica, en junio de 2020 se crea la empresa siendo César Augusto Flores Avalos dueño del proyecto.

La empresa consta con un grupo de 8 trabajadores que están divididos en atención al cliente, mantenimientos de red e instalaciones, tienen una oficina y dos carros de movilización, la infraestructura de la red consta con equipos mikrotik para el uso de la configuración, seguridad y control de ancho de banda de los clientes, Olt Huawei para el almacenamiento de usuarios, uso fibra drop de dos hilos para instalaciones y equipos marca Cdata para brindar el servicio de internet y televisión.

A continuación, se dará a conocer la visión, Misión y propósito de la empresa CAFANET proveedora de servicio de internet.

Visión:

Ser una empresa líder en el mercado de servicio de internet con innovación, servicio y dedicación a sus clientes, liderando la preferencia en la provisión de servicios de última tecnología e Internet, con recursos técnicos, financieros y humanos calificados.

Misión:

Proveer del acceso a las tecnologías de la información usando infraestructura de telecomunicaciones de última generación, gestionado por personal altamente calificado para brindar un servicio acorde a las necesidades de nuestros usuarios y orientados a superar los desniveles culturales, económicos y sociales.

Propósito:

Proveer del servicio de acceso a Internet, diseño e implementación de sistemas de telecomunicaciones acorde a las necesidades del cliente, con tecnología de punta., nuestros servicios son especialmente diseñados para cubrir las necesidades de comunicación, enfocados a nuestros usuarios, con una atención personalizada que le aseguran confiabilidad y seriedad en nuestros servicios. (Avalos, 2022)

Los resultados de este trabajo aportan a la alta gerencia en la toma de decisiones, para el tratamiento del riesgo mediante normas, estándares y buenas prácticas, sin afectar la información de la empresa CAFANET y tener continuidad en el negocio y

alcanzar los objetivos planteados por la organización, para que estos procesos se lleven a cabo se enumeraron todos los activos de la organización que fueron identificados mediante una metodología de buenas prácticas en normas y estándares.

Mediante el análisis de los riegos informáticos que se realizó en la empresa CAFANET, nos dio a conocer las principales vulnerabilidades que afectan a los equipos de la red;

- Problemas de protocolos IP servicie.
- Las contraseñas no se cambian con periodicidad en los equipos Mikrotik.
- Problemas de las actualizaciones de los equipos Mikrotik.
- Problemas de ataques de virus hacia la red.

Según autores las vulnerabilidades se definen como:

- "Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas" (Aguilera López, 2011).
- "Estado de insuficiencia en un sistema informático o conjunto de sistemas que permiten la materialización de una amenaza afectando las propiedades de disponibilidad, confidencialidad, integridad, autenticidad, no repudio" (Medina, 2014).

En el trabajo realizado por Andrés Paúl Gonzáles Orellana y Diego Rolando Tenemaza Arias describe los tipos de vulnerabilidades tales como:

- Vulnerabilidades Físicas
- Instalaciones inadecuadas del espacio de trabajo, falta de organización de los cables de energía y de red, etc.
- Vulnerabilidad de Hardware
- Conservación inadecuada de los equipos, falta de equipos de contingencia.
- Vulnerabilidad de Software
- Configuración e instalación indebida de programas en las organizaciones.
- Vulnerabilidad de Almacenamiento
- Medios no utilizados de forma adecuada, el contenido podría ser vulnerables a diferentes factores.
- Vulnerabilidad en la Comunicación

- La información debe transitar de la manera más segura posible.
- Vulnerabilidad de diseño
- Mal diseño de la arquitectura de la red, debido a este tipo de vulnerabilidad lo que se debería hacer para enfrentar las diferentes amenazas que se puedan presentar, es volver a diseñar una arquitectura adecuada para la red.
- Vulnerabilidad organizacional
- No existen políticas de seguridad dentro de la organización, o tal vez al existir estas políticas no son correctamente cumplidas. (Gonzáles Orellana & Rolando Tenem, 2012)

De acuerdo al Ing. Alejandro Gordon indica que La seguridad es uno de los aspectos fundamentales para obtener un adecuado funcionamiento de la red de datos, ya que mediante la seguridad se respalda la integridad y confidencialidad de los datos. Un abuso a la seguridad implica generar serios daños en la estabilidad de la red de tal manera se plantea la necesidad de identificar las vulnerabilidades y a qué tipo de amenazas se encuentra expuesta.

Es de gran importancia conocer sobre la inseguridad y los riesgos que puedan afectar a una red de datos dentro de una institución por lo tanto sin la búsqueda de vulnerabilidades en una las organizaciones crean una idea equivocada de su seguridad, cave recalcar que algunas de las debilidades que se generan en frecuentemente son el hecho de usar contraseñas predeterminadas o débiles en seguridad. (barba, 2022)

Cuando ingrese a realizar las practicas preprofesionales en la empresa CAFANET en el mes de enero del 2021 como ayudante técnico en la área de mantenimiento de la red, al comienzo de la semana se registraba muchas quejas de los clientes acerca de la lentitud del internet por lo cual se procedió a consultar con un ingeniero de telecomunicaciones especializada en configuración y mantenimiento de software de la red, Unas de las primeras funciones que realizo el ingeniero fue una revisión a fondo de la configuración de la red donde se encontró vulnerabilidades dentro del equipo router mikrotik, no estaba protegido por reglas de firewall y tenía diversos ataques de virus, esto generaba que la red se vuelva lenta e inconsistente, se procedió a reforzar la seguridad configurando el router mikrotik y asignándole reglas de firewall para mitigar los ataques de virus hacia la red.

A continuación, se detallará todos los ataques de virus encontrados en la red de fibra óptica de la empresa CAFANET, estos ataques causaban que la red interna sea lenta y los usuarios tengan un mal servicio de internet.

Ataques de Red

La presente investigación se encontró diversos ataques hacia la red de la empresa "CAFANET", el análisis de ataques en los dispositivos Mikrotik se pudo observar los siguientes ataques:

- Ataques de Fuerza Bruta
- Ataque DHCP Spoofing
- Smurf Attack
- ARP Spoofing
- SYN Flood
- Ataque denegación de servicio distribuido – DDos

Ataques de Fuerza Bruta:

Un ataque de fuerza bruta ocurre cuando el atacante emplea determinadas técnicas para probar combinaciones de contraseñas con el objetivo de descubrir las credenciales de una potencial víctima y así lograr acceso a una cuenta o sistema.

Existen diferentes tipos de ataque de fuerza bruta, como el "credential stuffing", el ataque de diccionario, el ataque de fuerza bruta inverso o el ataque de password spraying. Generalmente, los ataques de fuerza bruta tienen mayor éxito en los casos en los que se utilizan contraseñas débiles o relativamente fáciles de predecir.

Es un método de prueba y error, donde el atacante utiliza herramientas que permite probar todas las combinaciones posibles hasta encontrar el texto que fue cifrado. (Albors, 2020)

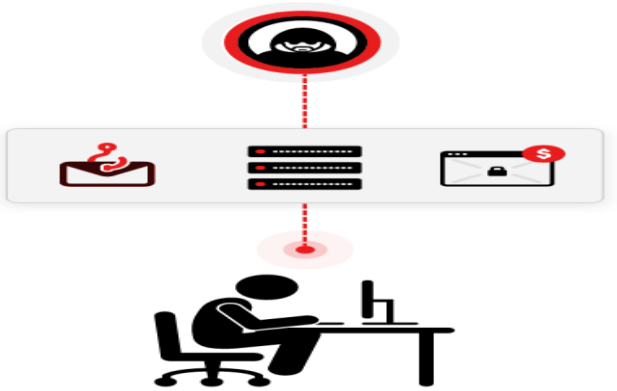
Figura 1

Nota: "Ataque de Fuerza Bruta"
Elaborado por: Blog EHCGroup

Ataque DHCP Spoofing

El ataque DHCP spoofing consiste en suplantar el servidor legítimo por uno falso utilizando alguna herramienta que permita realizar las mismas funciones; de manera que el atacante sea quien responda a los mensajes DHCPDISCOVER enviados por los clientes que solicitan la configuración de red. El servidor DHCP falso proporcionará la dirección ip en un rango diferente al establecido en el servidor legítimo donde establece su dirección ip como puerta de enlace lo que le permite realizar el ataque; este consiste en colocarse entre el servidor legítimo y el cliente para poder espiar en todo el tráfico de la red y así poder leer y modificar mensajes entre la comunicación establecida. (CECILIA, 2019)

Figura 2



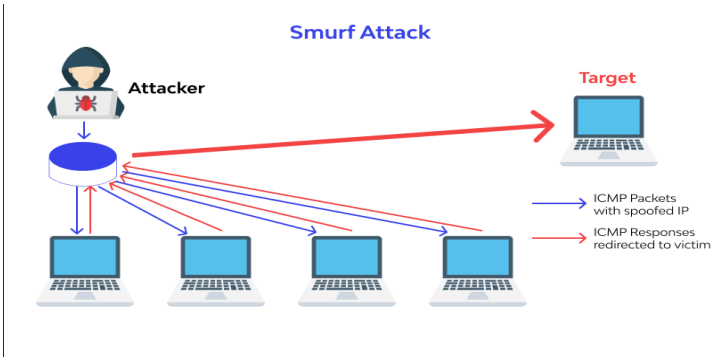
Nota: "Ataques de DHCP Spoofing"
Elaborado por: Keeper Security

Smurf Attack

Estos ataques pueden ser destructivos. En este ataque, un atacante envía una gran cantidad de tráfico eco ICMP (ping) a direcciones IP de difusión. Estos paquetes han falsificado dirección IP de la fuente que apunta a la víctima. Para amplificar el ataque varios sitios intermedios son seleccionados por el atacante. Esto da lugar a un montón de respuestas de ping (ICMP Echo Reply) y así la víctima resulta ser comprometida.

De esta manera, gran parte de la labor del atacante reside en encontrar una lista de servidores de difusión y en falsificar la dirección de respuesta para direccionarlas al equipo de destino. (Alexynior, 2021)

Figura 3



Nota: "Smurf Attack"
Elaborado por: Wallarm

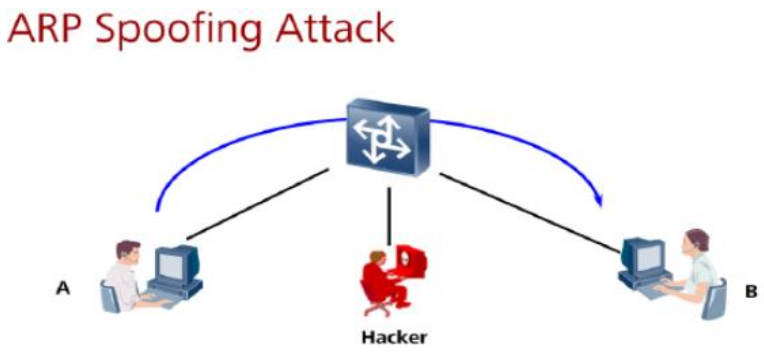
ARP Spoofing

La suplantación de IP se refiere a la creación de paquetes de Protocolo de Internet (IP) con un forjado de dirección IP de origen, llamada suplantación de identidad, con el propósito de ocultar la identidad del remitente o hacerse pasar por otro sistema informático.

Este ataque a las redes de datos es uno de los más populares, permite atacar a equipos que estén en la misma red local, ya sea cableada o inalámbrica. Cuando se realiza un ataque ARP Spoofing, lo que estamos haciendo es que el atacante se pueda hacer pasar por el router o Gateway, y que todo el tráfico de la red o desde un determinado PC pase por él, permitiendo leer, modificar e incluso bloquear el tráfico de red.

Este ataque solamente funciona en redes IPv4, pero en redes IPv6 también existe un ataque similar, porque el protocolo ARP tan solo está disponible en redes IPv4. (Ramiro, Tipos de ataques informáticos, 20)

Figura 4

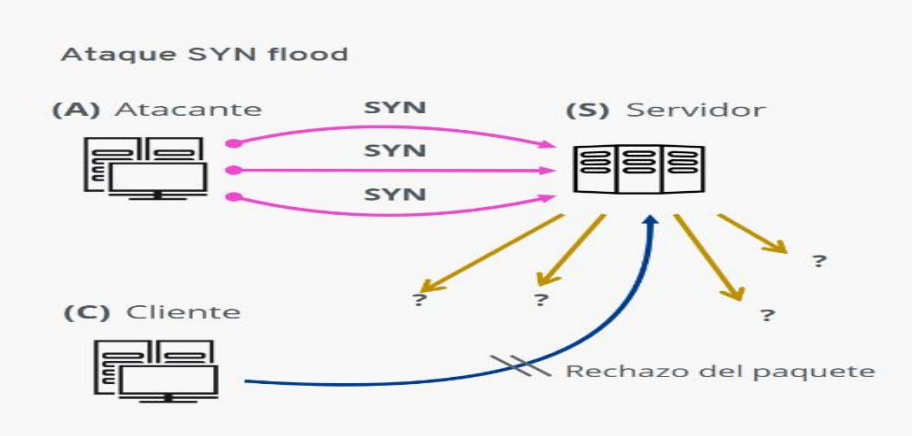


Nota: "ARP Spoofing Attack"
Elaborado por: Huawei

SYN Flood

La inundación SYN envía una inundación de paquetes TCP / SYN, a menudo con un remitente falsificado en dirección. Cada uno de estos paquetes se maneja como una solicitud de conexión, causando al servidor una conexión semiabierta, mediante el envío de un paquete TCP / SYN-ACK, y esperando un paquete en respuesta de la dirección del remitente. Sin embargo, como la dirección del remitente está falsificada, la respuesta nunca llega. Estos halfopen en conexiones, saturan la cantidad de conexiones disponibles que el servidor puede hacer, evitando que responda a solicitudes legítimas hasta después de que el ataque termine. (Ramiro, 2018)

Figura 5



Nota: "Syn Flood Attack"
Elaborado por: Ionos

Ataque denegación de servicio distribuido DDos

Los ataques de denegación de servicio o DoS, en redes son los más conocido de ataque sobre los niveles de red y transporte, también conocidos como ataques TCP/IP. Existe una gran variedad de ataques de denegación de servicio: inundación IP, falsificación IP origen, inundación TCP/SYN, teardrop, snork, ping de la muerte, etc.

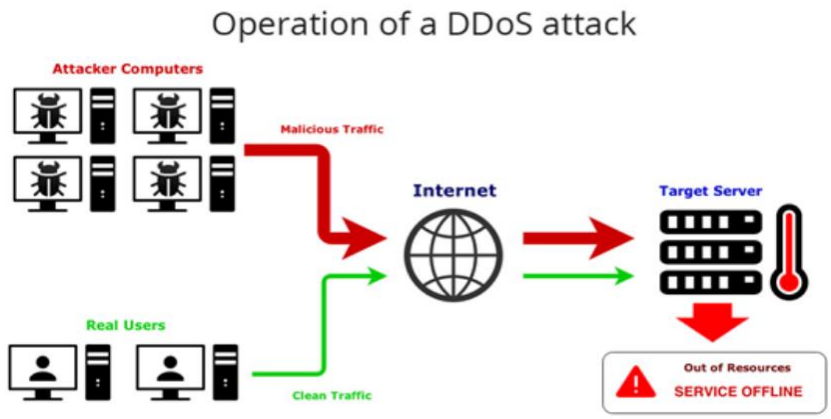
Posteriormente, describiremos los ataques de denegación de servicio más representativos:

Inundación IP: Consiste en el envío de tráfico masivo para conseguir la degradación de los servicios de la red. El atacante consume un gran ancho de banda ralentizando las comunicaciones existentes en la red. Este ataque es efectivo en redes en las que no se rea liza ningún control de acceso al medio y cualquier equipo puede enviar y recibir paquetes sin ningún tipo de limitación del ancho de banda consumido.

Falsificación IP: Distinguimos dos tipos de ataque: broadcast y Smurf.

Broadcast: Variante del anterior ataque de denegación de servicio en el que se falsea la dirección IP origen del atacante, indicando la dirección de difusión (broadcast) de la red. En este caso, cada equipo responde a la dirección IP origen, que, al resultar la dirección de difusión, realiza un envío masivo al resto de equipos de la red. (Gascó, 2013)

Figura 6



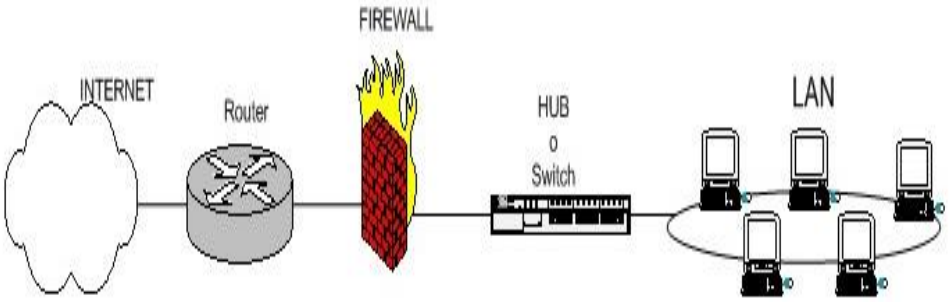
Nota: "Servicios de DDoS Attack"
Elaborado por: NextVision

A continuación; detallaremos las herramientas que utilizaremos para mitigar todos los ataques encontrados en la red.

Servidor DNS:

De acuerdo al Ing. José Arellano Muñoz explica que un servidor DNS es un traductor que permite convertir las peticiones escritas como texto a número, por ejemplo, cuando buscamos www.facebook.com este DNS se encarga de convertir este texto a número es decir hace de traductor para que el internet logre comprender la petición que estamos realizando, básicamente es una forma de asociar nombres con números esto nos ayudar a recordar el nombre de una página por su nombre de dominio y no por su ip. DNS para hostiar tu propio es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un estándar de facto. Es comúnmente usado en sistemas GNU/Linux. (Muñoz, 2022)

Figura 7



Nota: Reglas de Firewall
Elaborado por: Sinip

Address List en Mikrotik:

Las listas contienen direcciones ip para las que podemos tomar determinadas acciones. de esta manera, mantenemos una única lista de direcciones y la invocamos en el firewall.

Crear una lista especificando desde dónde permitimos conexiones ssh agregar ips a una address-list de forma dinámica, también podremos crear nuestras propias cadenas de firewall en mikrotik, las cadenas creadas por el usuario sirven para ordenar el firewall. (Lanpixel, 2021)

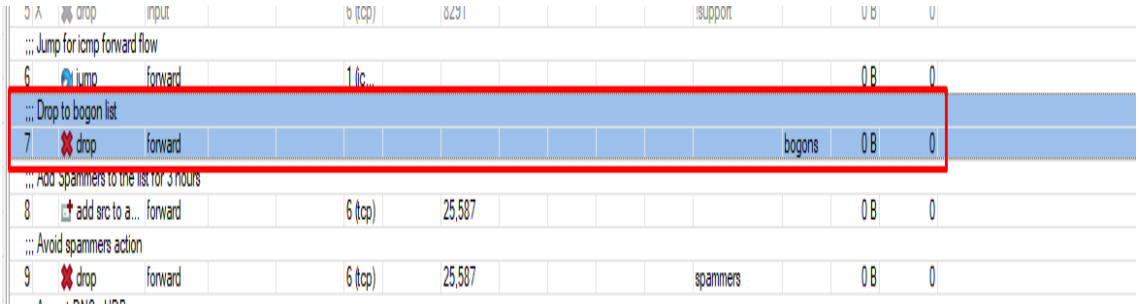
Bloqueo de bogon list:

Conforme a la entrevista con el Ing. Edgar Reinoso Cardenas explica que, Bogon son direcciones ip falsas. también es un nombre informal para un paquete ip en la internet pública que dice ser de un área del espacio de direcciones ip reservadas, pero aún no asignadas o delegadas por la internet, las áreas de espacio de direcciones sin asignar se llaman el espacio bogon.

Un bogon está en el prefijo de la dirección de internet que nunca debería aparecer en una tabla de enrutamiento de direcciones ip. por ejemplo, hay direcciones ip públicas, aquellas que todos usamos para acceder públicamente al correo electrónico, dns, http y otros servicios en internet, y hay direcciones ip privadas, si bien las direcciones ip privadas también pueden admitir exactamente los mismos servicios y cualidades que las direcciones ip públicas, no se puede acceder a ellas desde una dirección ip pública.

Si bien la lista de bogons no cambia tan rápido como una lista negra de dns normal, sí cambia, por lo que es importante que tenga algún método mediante el cual solicite la actualización de la lista de bogons. (Cardenas, 2022)

Figura 8



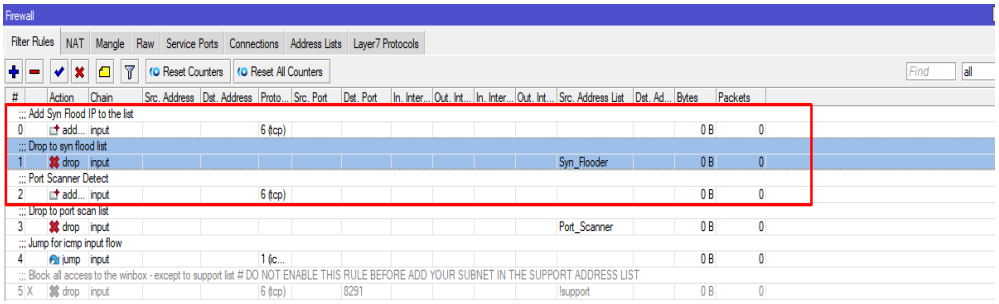
Nota: Broqueo de Bogon list
Elaborado por: Rosa Haro Huerta

Reglas Syn Flood:

El syn flood tiene por objetivo dejar sin tráfico legítimo a un sistema en línea, conceptualmente un ataque de denegación de servicio puede compararse con el envío masivo de cartas falsas a un organismo. cuando los buzones se saturan, el organismo no podrá recibir el correo legítimo o no podrá procesarlo, el atacante habrá alcanzado su objetivo, es decir, impedir el funcionamiento normal del organismo.

La inundación syn es un ataque al protocolo, estos ataques tienen como objetivo aprovechar una vulnerabilidad en las comunicaciones de red para poner a sus pies el sistema de destino, en esto se diferencia de la mecánica de los ataques volumétricos ping flood, udp flood y http flood. en estos, los atacantes se centran en saturar el ancho de banda del objetivo en la red. (Gordon, Reglas de bloqueo Syn Flood, 2022)

Figura 9



Nota: Reglas Syn Flood
Elaborado por: Rosa Haro Huerta

Bloqueos de Correo Maliciosos:

La mayoría de los proveedores de alojamiento web han experimentado en algún momento que uno de sus servidores sea bloqueado por los receptores de correo electrónico, si te encuentras en esta situación tan complicada, hay pasos que puedes seguir para solucionar el problema.

El bloqueo se produce cuando receptores de correo electrónico bloquean activamente su dirección ip, de correo electrónico bloquean activamente su dirección ip de modo que el correo electrónico que intenta enviar no puede ser entregado a nivel de correos bloqueamos los puertos de correo incluso puertos seguros ¿por qué lo bloqueamos?, porque dan mal uso esos puertos, lo utilizan para crear ataques de red con correos masivos. Los puertos 25-110-2525 son puertos inseguros para correos electrónicos. Los putos seguros 465-587-993 son puertos de correo electrónicos seguros con certificación SSL. (Obando, 2022)

Reglas de Bloqueo Drop Mebroot y Torpig:

Torpig evita aplicaciones antivirus a través del uso de rootkits y busca en el sistema infectado para robar credenciales, las cuentas y contraseñas de home banking, así como potencialmente permite a un atacante el acceso total al equipo, también es supuestamente capaz de modificar los datos en la computadora, e infectar el sector mbr.

También eliminamos todo el tráfico del cliente infectado, con distinto al puerto 80 tcp y distinto al puerto 53 udp; Esto deja sin navegación al cliente y solo le permite dns y http. entonces queda el cliente filtrado (sin servicio) y lo único que puede ver es la página que dice que su equipo está comprometido y necesita llamar a un técnico de esta manera mitigamos los ataques de mebroot torpig. (Gordon I. P., Reglas de Bloqueo Drop Mebroot y Torpig, 2022)

Reglas de Input, Forward y Output:

El firewall de routeros implementa un filtrado de paquetes que proporciona funciones de seguridad que se utilizan para administrar el flujo de datos hacía, desde y a través del router.

En iptables existen las siguientes cadenas por donde van a circular los paquetes dentro del sistema:

- **Input**: Contiene los paquetes destinados al equipo local con cualquier origen.
- **Output:** Contiene los paquetes generados en el equipo local y que van a salir del mismo.
- **Forward:** Contiene los paquetes que pasan por el equipo pero que son generados en equipos remotos y se dirigen a otros equipos diferentes.

Acciones / Objetivos

Las acciones u objetivos especifican qué se va a realizar con el paquete cuando satisface la regla en la que se encuentra. Existen las siguientes acciones:

Accept: El paquete se acepta y no continúa atravesando ni la cadena actual ni cualquier otra cadena de la misma tabla.

Drop: El paquete se elimina completamente dentro de la cadena actual, y no será procesado en ninguna de las cadenas principales de ninguna tabla. Tampoco se enviará ninguna información en ninguna dirección para informar de ello.

Masquerade: Modifica la dirección y el puerto de origen en el paquete, como en snat, pero cuando la ip que se asigna es dinámica, ya que el equipo la posee gracias a un servidor dhcp.

Queue: El paquete se pone en cola, para que sea analizado por programas externos a Iptables.

Log: El paquete dejará un registro de su paso por el equipo. (Morales, 2013)

Reglas de VPN:

Esta regla nos ayuda toda nuestra información mientras que estamos navegando de esta manera estamos más seguro a no recibir ataques a mi red, el puerto por defecto que usa es el 1194 udp. sin embargo, podemos configurarlo y poner otro distinto en el servidor, e incluso podremos seleccionar entre el protocolo tcp o udp. En las vpn utilizamos el tráfico de los puertos 1701-500-4500-1723, respectivamente a las conexiones ya sean protocolos l2tp y tcp respectivamente declarados en protocolos 17(udp) y 6(tcp).

Reglas VPN-L2tp:

Este protocolo de VPN no permite el cambio de puerto, es el estándar, en VPN-L2tp utilizamos protocolos (ipsec-esp) que se utilizan para un doble factor de encriptación en la cual debe ser aceptado caso contrario no va a tener conexión nuestra VPN-L2tp también se utiliza el puerto 1701 con TCP.

VPN-Ppptp:

Un dato muy importante a destacar es que el protocolo pptp está obsoleto. esto es debido a que presenta bastantes vulnerabilidades. por ese motivo lo aconsejable sería

mantener cerrado este puerto, y seleccionar otro de los protocolos que mencionamos a continuación en su lugar.

Utilizamos los protocolos gre que está declarado con puerto 474 a nivel de nuestro mikrotik para que se conecte nuestra vpn-ppptp.

Aceptamos protocolo icmp es ping con una regla de input puede ser de n nuestro proveedor o nuestro cliente hacia nuestro proveedor. (Barba, 2022)

Mediante un análisis FODA se identifican las principales debilidades, fortalezas, amenazas y oportunidades que tiene el área informática, este análisis se representa en la siguiente matriz cuadrada.

- Análisis FODA

FORTALEZAS	OPORTUNIDADES
– Brindar calidad de servicios – Uso de antivirus. – Realiza evaluaciones de la seguridad del entorno de forma interna anualmente. – Uso firewalls, para proteger la red contra ataques o infecciones por virus.	– Adaptación nuevas tecnologías dentro de la empresa. – Existencia una persona responsable en el área de mantenimiento de la red. – Expansión de la empresa a nuevos mercados
DEBILIDADES	AMENAZAS
– No existen políticas de seguridad. – Desorganización de los cables de energía y red. – Falta de cámaras de vigilancia para la seguridad de los equipos. – Déficit en el acondicionamiento de aire para los equipos – Aumento de gastos en materiales de los medios de transporte	– Sobrecalentamiento de los equipos. – Desperfecto eléctrico – Suciedad en el área donde se encuentran los equipos. – Carencia de tácticas para gestionar la red.

Este cuadro de foda constituye, la base o el punto de partida para la formación o elaboración de estrategias, ya que nos permite identificar nuestras fortalezas, debilidades, oportunidades y amenazas de esta forma, es posible desarrollar e implementar nuevas estrategias a futuro para el bien de la empresa.

Marco Metodológico

La metodología de investigación que se utilizó para realizar este estudio de caso es la metodología experimental, esta metodología se enfoca principalmente en métodos de investigación, porque permite comprobar o descartar hipótesis con parámetros fiables, de manera sostenida en el tiempo, y con objetivos claros, por cuanto el estudio se realiza por separado, de esta manera detectar cada una de las vulnerabilidades que más impacto causan a la red.

De acuerdo al autor Fidias Arias define que la investigación experimental es un proceso que consiste en someter a un objeto o grupo de individuos, a determinadas condiciones, estímulos o tratamiento, para observar los efectos o reacciones que se producen en cuanto al nivel, la investigación experimental es netamente explicativa, por cuanto su propósito es demostrar que los cambios en la variable dependiente fueron causados por la variable independiente. Es decir, se pretende establecer con precisión una relación causa-efecto. (Arias, 2013)

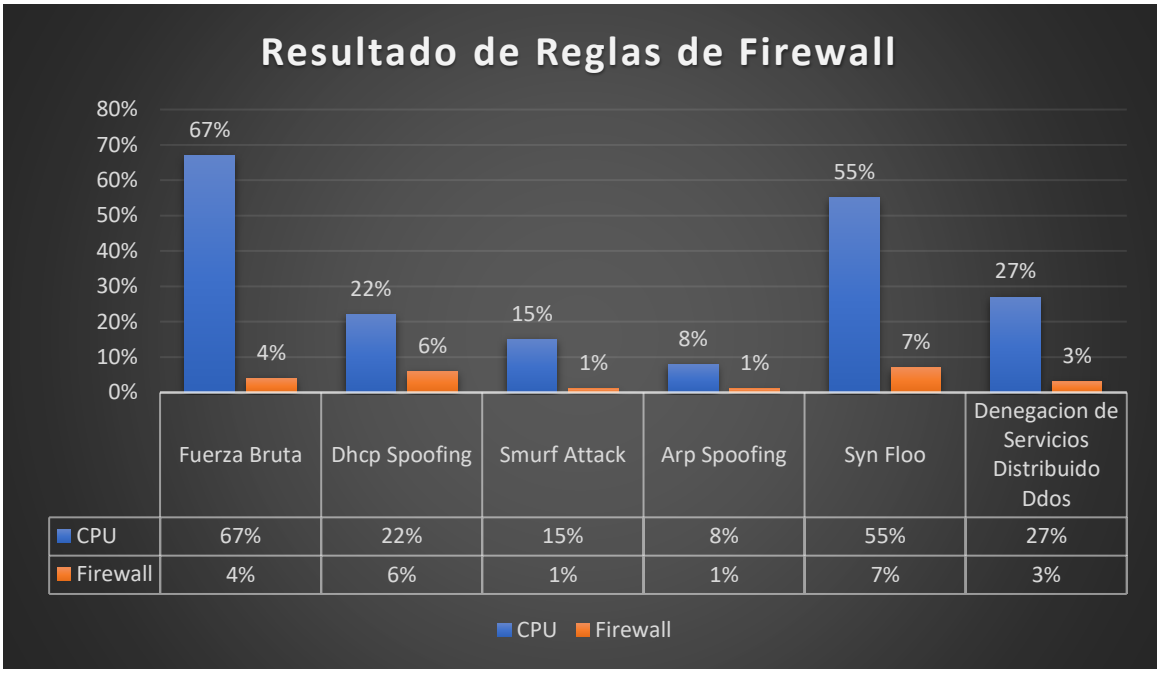
Las herramientas utilizadas para la recolección de información necesaria para la elaboración de este estudio de caso fueron la entrevista que se realizaron a los ingenieros de telecomunicaciones, también los cuestionarios de entrevista que nos dio a conocer las vulnerabilidades más frecuentes y las recomendaciones de nuevas tecnologías para la empresa.

Resultado

A lo largo del desarrollo de este estudio de caso, se analizó que las reglas de firewall implementadas mitigaron todos los ataques de la red, a continuación, se muestran los resultados que se obtuvieron de los ataques generados antes y después con las diferentes herramientas seleccionadas.

En el primer ataque de fuerza bruta, se puede evidenciar que, con las reglas de firewall de Input, forward, Output y Vpn Mitigamos los ataques de red reduce un 67% del uso excesivo del CPU del equipo Mikrotik. En el segundo ataque Dhcp Spoofing, las reglas implementadas de input y forward reducen un 22% del uso excesivo del CPU. En el tercer ataque Smurf Attack se puede observar una reducción de ataque del 15%, ya que su mitigación fue realizada con reglas Input, forward y bogon ya que bloquea ciertos usos de ip y que el resto de ip que no se encuentre dentro de nuestra red serán descartados para evitar ser atacados ya que el 100% de la ip que se encuentran en internet solamente un 65% son utilizables el resto están utilizadas por personas en uso fraudulento. En el cuarto ataque Arp Spoofing, su consumo de CPU no fue muy elevado debido a que el ataque depende de la longitud del adicionamiento con el que se realice el ataque, el consumo de CPU es de un 8% y su mitigación se realiza por medio de reglas de Dyn Flood. Quinto ataque Syn Flood las reglas implementadas para mitigar este ataque utilizamos lo que son bloqueos de correo malicioso y Bloqueo de Drop Mebroot y Torpig, este se reduce un 55% en el uso del CPU. Sexto y último ataque denegación de servicio distribuido DDos el ataque genera una carga de 27% para el CPU y gracias a los parámetros de mitigación en el firewall de reglas Input, Forward y Bloqueos de correo Maliciosos, este se reduce un 20% en el uso del CPU.

Gráfico 1



Nota: Gráfico de viabilidad obtenido
Elaborado por Rosa Haro

Posteriormente el entrevistado respondió un cuestionario de preguntas mediante las cuales se obtuvo información sobre las cualidades positivas y negativas que tiene la empresa en el área de red, dichos datos son mostrados en el siguiente cuadro.

Cuadro 1

Positivas	**Negativas**
➢ Adaptación nuevas tecnologías dentro de la institución como, por ejemplo, SmarOLT para la activación d equipos. ➢ Uso de Antivirus a las maquinas administradoras de la red. ➢ Realiza evaluaciones de la seguridad del entorno de forma interna anualmente ➢ Persona capacitada para el área	➢ No usar sistemas de detección de intrusos para identificar los ataques a la seguridad. ➢ No existen políticas de seguridad dentro de la empresa ➢ Falta de cámaras de vigilancia para la seguridad de los equipos. ➢ Déficit en el acondicionamiento de aire para los equipos de la red, lo que pudiera causar el deterioro o bajo rendimiento de los mismo ➢ Punto excesivo para conexión wifi en la oficina. ➢ No capacitan a los técnicos que se

del mantenimiento de la red en la fibra óptica. ➢ Equipos robustos de Mikrotik para la administración de la red. ➢ Buen mantenimiento en el área del cableado de energía y red.	encargan del mantenimiento de instalaciones de la red. ➢ No existen reglas de firewalls, para proteger la red contra ataques o infecciones por virus. "Firewall o cortafuegos, programa que monitoriza el tráfico y las conexiones de red y bloquea aquellas conexiones o programas que no se hayan autorizado dentro de la red.

Nota: Cuadro de cualidades positivas y negativas de la empresa CAFANET
Elaborado por: Rosita Haro

En el cuadro anterior se muestra una cantidad considerable de falencias que pueden causar o provocar situaciones que pongan en riesgo el funcionamiento o rendimiento de los equipos de la red que posee la empresa, así como también lo que podría ocasionar un grave incidente seria en no implementar reglas de firewall, claramente este punto es tomado como una vulnerabilidad, por otra el que exista una persona con experiencia encargada del área de mantenimiento de la red es de mucha importancia ya que es quien podrá tomar acciones puntuales que ayuden a contrarrestar dichas falencias. La función del responsable del área de mantenimiento es, asegurar el funcionamiento de los sistemas de información y en gestionar los nuevos proyectos informáticos que puedan surgir ante las necesidades de la empresa.

Discusión de Resultados

En este capítulo presentaremos las discusiones de los resultados de los datos obtenido en nuestro caso de estudio. Tras describir y analizar los resultados obtenidos con el análisis de vulnerabilidad de la red CAFANET, procede ahora realizar unas discusiones y conclusiones que sirvan para consolidar lo obtenido, al tiempo que suponga una futura línea para nuevas investigaciones.

Discusión sobre la implementación de firewall y la efectividad que tubo.

En este apartado vamos a tener en cuenta en forma global sobre todas las vulnerabilidades que se encontraron en la red ya que era las causas del mal funcionamiento. La empresa tuvo un crecimiento de manera significativa por lo cual los problemas se fueron acumulando y la red era inestable, es necesario identificar las vulnerabilidades que necesitan una protección inmediata. En este entorno, aplicamos reglas de firewall que tiene la capacidad de filtrar paquetes de datos, este dispositivo es indispensable en una red ISP, debido a que mitiga las vulnerabilidades provenientes de la red, manteniendo un mayor grado de seguridad, garantizando así la disponibilidad, integridad, y confidencialidad de la información. Como la empresa tienen implementado en su red equipos mikrotik el cual funciona como router core, en donde se aplicarán las reglas de seguridad firewall para cada tipo de ataques ya sea interno o externo de la red.

¿Se analiza la validez del resultado?

En la validez de resultado podemos observar el porcentaje optimizado, después de la implementación de las debidas reglas de mitigación del router Mikrotik, como resultado se obtuvo una disminución del 70% del consumo del CPU en cada ataque generado, logrando así el buen funcionamiento de la infraestructura de la red, garantizando la estabilidad y la disponibilidad de la red.

¿Se discuten los resultados presentados?

Los resultados presentados fueron discutidos con el dueño y los técnicos de la empresa, se dio a conocer el antes y después de como mitigamos los ataques y se establecieron reglas de seguridad de esa manera comprobamos que la red con las implementaciones que se realizo tuvo mejoras en el servicio de internet.

El propósito de esta entrevista es dar a conocer la efectividad de implementación de reglas de firewall y seguridades informática dentro de la red, ya que cada vez más las empresas requieren un tratamiento diferente, por cuanto brindan más de acceso a la información, movilidad y esto hace que sean vulnerables si no se toma las respectivas medidas de seguridad.

También es importante recalcar la importancia de un profesional de telecomunicaciones ya que con su experiencia podemos implementar nuevas tecnologías ya que es un factor muy importante para el desempeño y crecimiento de la empresa.

Conclusiones

En este trabajo se experimentó los ataques dirigidos a dispositivos routers de core MikroTik. Para el análisis de los tipos de ataques se procedió al uso de herramientas como el pentesting de redes de datos, considerando el escaneo y explotación de vulnerabilidades. Los resultados obtenidos facilitaron la implementación de mecanismos de seguridad ante los riesgos de ataques, pero al implementar la política de seguridad existe una reducción considerable de los ataques de red, esto debido a las reglas específicas aplicadas al firewall de RouterOS lo cual ayuda a tomar las decisiones necesarias de cada paquete del tráfico de red generado.

Se deben establecer políticas de seguridad claras para el encargado de la seguridad de la red, realizar procedimientos de respaldo periódicos de información, realizar capacitaciones, políticas de seguridad, plan de contingencia y medidas para asegurar la información de la empresa que podrían quebrantar la continuidad de la organización por el manejo inadecuado de los sistemas y dispositivos.

Es importante sumar al área de las tecnologías personal que ayude en la ejecución de evaluaciones y controles sobre el cumplimiento de las políticas que se llegarán a establecer, de esta manera con la incorporación de un nuevo personal se podrán contar con diferentes criterios y posibles soluciones a la hora de enfrentar algún problema informático.

Recomendaciones

Dado que el estudio realizado dio como resultado que si es factible llevar a cabo el proyecto propuesto sería conveniente tomar en cuenta algunos puntos a mejorar.

- Definir controles para garantizar la seguridad de la infraestructura de comunicaciones y los servicios conectados en al sistema de información, contra el acceso no autorizado.

- Se recomienda revisar el consumo de procesador de los equipos constantemente, esto evita que los equipos se sobrecalienten o bloqueen.

- Las inversiones en mejoramiento de la red son constantes y deben realizarse para mejorar el servicio y estar a la vanguardia de la tecnología, así el cliente sentirá que la empresa se preocupa por brindarle el servicio con la mejor calidad y que se preocupa por sus clientes.

- Capacitar lo necesario a los empleados para que sepan utilizar los sistemas correctamente y saber sobre llevar a los clientes cuando hay falencia dentro de la red.

- Aplicar políticas en la red, en el firewall se debe definir los perfiles de usuarios como: el administrador tiene un perfil con todos los permisos y para los técnicos solo un usuario de revisión.

- Se recomienda a los encargados de la seguridad en la empresa CAFANET, implementar las estrategias formuladas en este documento para alcanzar mejores prácticas, controlar y minimizar los riesgos.

Bibliografía

Aguilera López, P. (2011). *Seguridad informática.* Editex.

Albors, J. (24 de Junio de 2020). *Qué es un ataque de fuerza bruta y cómo funciona*. Obtenido de Qué es un ataque de fuerza bruta y cómo funciona: https://www.welivesecurity.com/la-es/2020/06/24/que-es-ataque-fuerza-bruta-como-funciona/

Alexynior. (15 de octubre de 2021). *Adictec*. Obtenido de Tipos de Ataque a Redes Informáticas: https://adictec.com/tipos-ataque-a-redes-informaticas/

Apráez, M. C. (2013). *ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA.* Obtenido de ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA: https://repositorio.uta.edu.ec/bitstream/123456789/4958/1/t812si.pdf

Arias, F. G. (21 de 04 de 2013). *Planificaciondeproyectos*. Obtenido de Tipos y diseño de la investigación: http://planificaciondeproyectosemirarismendi.blogspot.com/2013/04/tipos-y-diseno-de-la-investigacion_21.html#:~:text=o%20Dise%C3%B1o%20Experimental.-,Seg%C3%BAn%20el%20autor%20(Fidias%20G.,se%20producen%20(variable%20dependiente).

Avalos, C. F. (28 de 02 de 2022). Descripción d la empresa. (R. M. Huerta, Entrevistador)

barba, A. P. (08 de 03 de 2022). Seguridades de Redes. (R. H. Huerta, Entrevistador)

Barba, I. A. (5 de 02 de 2022). Reglas de Firewall- VPN. (R. H. Huerta, Entrevistador)

Cardenas, I. E. (10 de Febrero de 2022). Bloqueo de Bogon list. (R. H. Huerta, Entrevistador)

CECILIA, A. C. (31 de enero de 2019). *Implementación de controles para Mitigar Ataques de red.* Obtenido de Implementación de controles para Mitigar Ataques de red: http://repositorio.utmachala.edu.ec/bitstream/48000/13595/1/ECUAIC-2019-SIS-DE00003.pdf

Gascó, G. E. (2013). *Seguridad Informatica.* Macmillan Iberia, S.A.

Gonzáles Orellana, A. P., & Rolando Tenem, D. (Diciembre de 2012). *bibdigital.* Obtenido de bibdigital.epn.edu.ec: http://bibdigital.epn.edu.ec/bitstream/15000/6020/1/CD-4774.pdf

Gordon, I. P. (4 de Febrero de 2022). Reglas de Bloqueo Drop Mebroot y Torpig. (R. H. Huerta, Entrevistador)

Gordon, I. P. (15 de Febrero de 2022). Reglas de bloqueo Syn Flood. (R. H. Huerta, Entrevistador)

Lanpixel. (10 de enero de 2021). *Tipos de ataques de red y como protegerse con Mikrotik*. Obtenido de Tipos de ataques de red y como protegerse con Mikrotik: https://lanpixel.com/blog/tipos-de-ataques-de-red-y-como-protegerse-con-mikrotik/

Medina, J. (2014). *Evaluacion de Vulnerabilidades TIC.*

Morales, R. (19 de Noviembre de 2013). *Iptables - Conceptos generales para configurar un cortafuegos*. Obtenido de Iptables - Conceptos generales para configurar un cortafuegos: https://www.ticarte.com/contenido/iptables-conceptos-generales-para-configurar-un-cortafuegos#:~:text=INPUT%3A%20Contiene%20los%20paquetes%20destinados,dirigen%20a%20otros%20equipos%20diferentes.

Muñoz, J. A. (30 de Enero de 2022). Servidores DNS. (R. H. Huerta, Entrevistador)

Obando, I. K. (17 de Febrero de 2022). Bloqueos de Correo Maliciosos. (R. H. Huerta, Entrevistador)

Ramiro, R. (20 de Enero de 20). *Tipos de ataques informáticos*. Obtenido de Tipos de ataques informáticos: 2018

Ramiro, R. (20 de Enero de 2018). *Ataques informatico*. Obtenido de Ataques informatico: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Anexos

Análisis de vulnerabilidades en la red ISP: Cafanet parroquia Isla de Bejucal, año 2022

Ing. Manuel Tandazo Mera

1. **¿Mencione cuál es el funcionamiento de una red de fibra óptica de un proveedor Isp y como está estructurada?**

   El funcionamiento de la red de fibra óptica es usado para transporte de datos e internet, está estructurada por un emisor y un receptor.

2. **¿Cuáles son las vulnerabilidades más frecuentes en un proveedor de ISP?**

   Los ataques de DOS, DNS, Ataques de fuerza bruta.

3. **¿Como podríamos mitigar las principales vulnerabilidades de los proveedores?**

   Usando firewall perimetral.

4. **¿Qué nuevas tecnologías recomendaría usted a los proveedores de ISP, para dar un mejor servicio a los clientes y mitigar vulnerabilidades dentro de la red?**

   Usar servidores cortafuegos para mitigar mayoría de ataques

Tnlga. Mayerling Onofre Justillo

1. **¿Mencione cuál es el funcionamiento de una red de fibra óptica de un proveedor Isp y como está estructurada?**

   Los cables de fibra óptica están compuestos por filamentos de vidrio, cada uno de ellos con capacidad para transmitir datos digitales modulados en una de luz.

   La tecnología informática través de la fibra óptica sólo busca transmitir información codificada de una manera segura eficaz y rápida. Una ventaja clave de los cables de fibra óptica respecto a los cables conductores del metal es su rendimiento superior en lo que al ancho de banda se refiere y, por lo tanto, su mejor rendimiento a la hora de

transportar datos, sin embargo, tiene su debilidad al ser un material más frágil que los cables con conductor de metal.

2. **¿Cuáles son las vulnerabilidades más frecuentes en un proveedor de ISP?**

   Las vulnerabilidades del ISP usualmente se originan por malas configuraciones en sus redes de seguridad o en la mala implementación y/o uso de aplicaciones de seguridad informática, además de no saber un manejo adecuado de las amenazas internas a la red, o el abuso de algunos usuarios con que con intenciones desconocidas atacan e intentan sustraer información confidencial.

3. **¿Como podríamos mitigar las principales vulnerabilidades de los proveedores?**

   Las recomendaciones que se podrían dar, es ofrecer un mejor y mayor monitoreo de seguridad remota a cada usuario incluido aplicación de firewall en mikrotik para contraer los ataque, además realizar una campaña de información de riesgos y ofrecer aplicaciones de prevención.

4. **¿Qué nuevas tecnologías recomendaría usted a los proveedores de ISP, para dar un mejor servicio a los clientes y mitigar vulnerabilidades dentro de la red?**

- ✓ Proteger la recepción de e mail de Dudosa procedencia
- ✓ Recomendar contraseñas seguras con alternabilidad de caracteres
- ✓ Contratas software de seguridad cibernética e involucrar todo el sistema de la empresa en seguridad informática
- ✓ Recomendar trabajos en la nube.

Ing. Harry Saltos

1. **¿Mencione cuál es el funcionamiento de una red de fibra óptica de un proveedor Isp y como está estructurada?**

   El medio básico de la fibra óptica es una fibra delgada que a veces está hecha de plástico, pero la mayoría de las veces de vidrio. Una fibra óptica de vidrio típica tiene un diámetro de 125 micrómetros (µm), o 0,125 mm (0,005 pulgadas).

   A través de un proceso conocido como reflexión interna total, los rayos de luz transmitidos a la fibra pueden propagarse dentro del núcleo a grandes distancias con una atenuación o reducción notablemente pequeña de la intensidad.

   Parte desde los Switch de Fo del Proveedor directo a los postes y se entrega a los domicilios a un Transceiver o Router Ap Wifi de FO directamente

2. **¿Cuáles son las vulnerabilidades más frecuentes en un proveedor de ISP?**

   Los mismos Clientes

   Spam de Correos

   Los demás ISP que les cortan los cables

3. **¿Como podríamos mitigar las principales vulnerabilidades de los proveedores?**

   Teniendo Canalizaciones de fibra subterránea

   Con Firewalls bien administrados

   Manejo eficiente del servicio al cliente

4. **¿Qué nuevas tecnologías recomendaría usted a los proveedores de ISP, para dar un mejor servicio a los clientes y mitigar vulnerabilidades dentro de la red?**

   Si es una empresa, le brindaría un backup por enlace de radio

   Si es un hogar, sistemas antivirus con licencia controlados remotamente.