Análisis Técnico Relacionado con la Implementación De Firewall Perimetral Para Prevenir Vulnerabilidades En La Red Informática De La Empresa Swtelecom.Net

Egresada(o):

Jordan Urbano Plaza Nicola

Facultad de Administración, Finanzas e Informática

Universidad Técnica Babahoyo

Procesos Titulación

Examen Complexivo de Grado o de Fin de Carrera Prueba Practica

Tutor:

MSc. Saltos Viteri Harry Adolfo

Babahoyo – Ecuador

2022

Introducción

Mediante esta investigación que está dirigida al análisis técnico de implementación de firewall perimetral para prevenir vulnerabilidades en la red informática de Swtelecom S.A del cantón Babahoyo, parroquia El Salto, se propone presentar una propuesta de implementación de un firewall perimetral para mitigar ataques externos e internos de la red telecomunicaciones, para de esta manera garantizar la confidencialidad, integridad y disponibilidad de los datos de los clientes de la empresa Swtelecom S.A.

Los proveedores de servicio de internet presentan un alto índice de vulnerabilidades respecto a la infraestructura de la red, en especial en los equipamientos de la red central, debido a que estos deben contrarrestar y mitigar cualquier tipo de ataque proveniente desde el internet o desde su propia red interna, para poder garantizar la confidencialidad, integridad y disponibilidad de los servicios. Por otro lado, según la información de las empresas Swtelecom S.A que brindan los servicios de internet utilizan equipos Mikrotik. Mikrotik posee equipamiento hardware y software propietario, para mitigar ciberataques, que ayudan a disminuir y mitigar vulnerabilidades que pueden poner en peligro la infraestructura de red.

Mediante la elaboración de este documento se presenta información real y confiable obtenida mediante el uso de herramientas para la investigación, con el fin de conocer la situación actual de la red tratando de cumplir el objetivo general planteado en el desarrollo de este caso, en este punto es donde se identifican las vulnerabilidades y sus posible consecuencias que puedan afectar los Reuters Mikrotik y el rendimiento de la red, además mediante las diferentes referencias bibliográficas se intenta obtener información relevante y actualizada que ayude a interpretar de una manera más clara y concisa temas o subtemas relacionados a este proyecto.

Finalmente se expresan las respectivas conclusiones, planteadas a partir de los resultados obtenidos una vez realizada la investigación correspondiente, así como también se revelan las fuentes bibliográficas de donde se obtuvo información que forma parte de este estudio.

Desarrollo

La empresa Swtelecom S.A está ubicada en la Parroquia el Salto perteneciente al cantón Babahoyo – Prov. Los Ríos, en marzo de 2020, se creó la empresa proveedora de servicio de Internet siendo Wellington Tairon Saltos Santana dueño de la empresa.

La empresa empezó a funcionar al inicio de la pandemia, por la necesidad el uso del internet, ya que uno de los inconvenientes que se le presentaron en la educación fue la falta de internet por lo que se virtualizaron las clases a nivel nacional, en la infraestructura se compone de dos oficinas en el sector salto y barreiro donde se desempeñan diversas labores (secretaria, ordenes de instalación, cobranza y departamento de equipos de red), dos Jeden para tener para organización de equipos, Olt vsol de 8 puertos Gpon y Olt Huawei, Fibra óptica 48 hilos y equipos de instalación de fibra óptica, plataformas Mikrowisp para el almacenamientos de clientes y sistemas de facturación además cuanta con el SmarOLT que ayuda a vincular equipos hacia la olt. (Santana, 2022)

La seguridad es uno de los aspectos fundamentales para obtener un adecuado funcionamiento de la red, ya que mediante la seguridad se protege de cualquier tipo de ataques ya sea interno o externo de la red, ya que si no se aplican estas seguridades se genera serios daños en la estabilidad de la red. De tal manera se plantea la necesidad de identificar las vulnerabilidades en la red y a qué tipo de amenazas se encuentra expuesta, para tener así una percepción sobre la situación actual de la red.

El objetivo general es identificar las vulnerabilidades en red de la empresa Swtelecom S.A. La delimitación de este caso se basa en tratar la seguridad de la red de la manera más asequible posible, para facilitar el estudio de las vulnerabilidades, así como también se procura no indagar sobre la existencia de equipos y software, que posea la institución.

De acuerdo a la entrevista realizada por el Ing. Manuel Ignacio Tandazo Mera

Cuando se hizo cargo de la empresa Swtelecom S.A, lo primero que realizo fue una revisión a la empresa de esa manera, identifico que tenía falencia de seguridad y ataques de red que se hablaran cada una de ellas más adelante del proyecto, los técnicos que simplemente tenían conocimientos básicos ya que no eran estudiados solo veían videos tutoriales en YouTube y no tenían los conocimientos que se requieren para poder solventar cual quiere emergencia técnica, en ese momento se utilizó una metodología de implementación d auditoria. Para la revisión de Ips privadas para los clientes y luego de ips publicas después se realizó la implementación de firewall y seguridad, para esta manera se pueda trabajar más seguro y la limitante de conexiones a los puntos de usuarios específicos es decir poner un administrador que se haga responsable y de esa manera evitar la desconfiguración del firewall. (Mera M. I., 2022)

Como principales vulnerabilidades que afectan a los routers Mikrotik, están los Ataques de denegación de servicios DoS, estos se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio. Por eso se le denomina denegación, pues hace que el servidor no pueda atender la cantidad enorme de solicitudes. Esta técnica es usada por los crackers o piratas informáticos para dejar fuera de servicio servidores objetivo. A nivel global, este problema ha ido creciendo,

en parte por la mayor facilidad para crear ataques y también por la mayor cantidad de equipos disponibles mal configurados o con fallos de seguridad que son explotados para generar estos ataques. Se ve un aumento en los ataques por reflexión y de amplificación por sobre el uso de botnets. (Cheza, 2013)

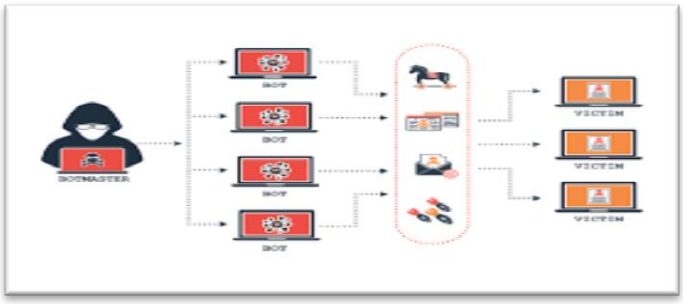

FIGURA 1.
Ataques de Vulnerabilidades Denegación de servicio (DoS)
Elaborado por (Nicescene seguridades web)

De igual forma tenemos los ataques STP (Spanning Tree Protocol) existe una vulnerabilidad asociada a STP que permite que un sistema en la red pueda modificar la topología STP sin ningún tipo de autenticación, es un protocolo usado en la red para evitar bucles a nivel 2 en nuestra topología cuando se conectan distintos segmentos de red. Cada uno de los paquetes STP se llaman BPDU (Bridge Protocol Data Unit). Los switches mandan BPDUs usando una única dirección MAC de su puerto como mac de origen y una dirección de multicast como MAC de destino Existen dos tipos de BPDU:

El primero se envía periódicamente indicando la configuración de la red, mientras que el segundo se envía cada vez que se detecta un cambio en la red (activación/desactivación de un puerto). (Lara, 2020)

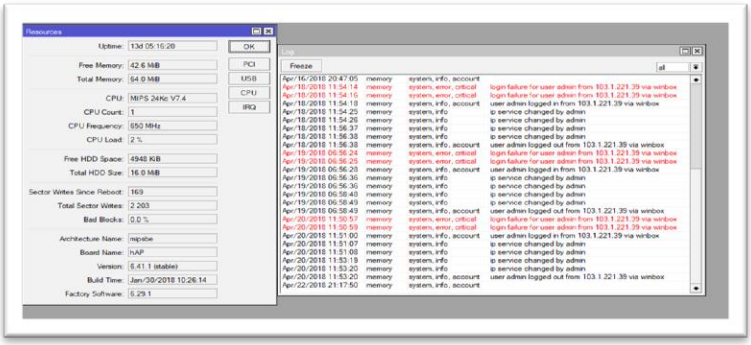

FIGURA 2.
Ataques de Vulnerabilidades Denegación de servicio (DoS)
Elaborado por (Nicescene seguridades web)

Tcp syn flood este ataque aprovecha el handshake de 3 vías para establecer la conexión. En este sentido, el atacante envía una gran cantidad de paquetes TCP/SYN con una dirección IP de origen falsificada al destino y este responde con un TCP/SYN-ACK al origen, intentando establecer la conexión). Este tipo de peticiones de inicio de conexión a gran escala generan un consumo excesivo del CPU y se lo realiza mediante un puerto de servicio abierto del router.

Smurf Attack es un ataque distribuido de denegación de servicio (DDoS), en el que un atacante intenta inundar un servidor objetivo con paquetes del Protocolo de mensajes de control de Internet (ICMP), al realizar solicitudes con la dirección IP falsificada del dispositivo objetivo a una o más redes informáticas, las redes informáticas luego responden al servidor objetivo, amplificando el tráfico de ataque inicial y potencialmente abrumando al objetivo, haciéndolo inaccesible. (Avila-Pesantez, 2021)

Udp flood el host atacante lanza un ataque DoS emitiendo un comando de ataque con la dirección de la víctima, la duración del ataque, los métodos de ataque y otras instrucciones a los programas de control maestro, que sirven como controladores de ataques. El objetivo es crear y enviar una gran cantidad de datagramas UDP, que se relaciona por medio del puerto 53 en UDP. (Cot Ros, 2014)

Protocolo de configuración dinámica del host (DHCP), este protocolo funciona con un servidor, el cual posee toda una lista de direcciones IP disponibles, que son asignados a cada cliente conforme se conecten a la red, funciona en los puertos 67 UDP para el servidor y 68 UDP para el cliente.

Ataques más Comunes:

Fuerza Bruta 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.

Herramientas Actualmente se han desarrollado herramientas para el análisis y test de penetración de redes Pentesting, con el propósito que el administrador de red descubra y solucione las vulnerabilidades que existen en el medio, dichas herramientas son capaces de recopilar información valiosa de la red y sus dispositivos. (Albors, 2020)

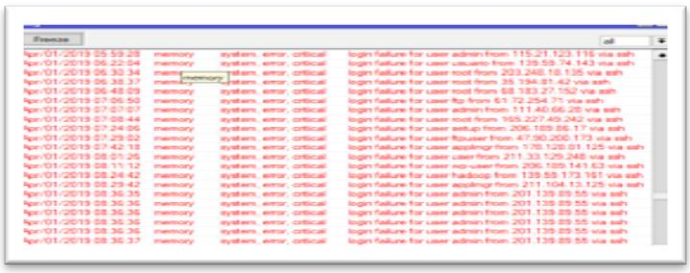

FIGURA 3.
Ataques de Fuerza Bruta
Elaborado por (Seguridad en sistemas y técnicas hacking)

DHCP Starvation para este estudio, la herramienta Yersinia en Kali-linux se encarga de generar decenas de direcciones MAC falsas para comenzar el ataque DHCP, mediante la inundación de paquetes DISCOVER como se aprecia en la Figura 6. Al mismo tiempo se verifica el recurso CPU del router de core para verificar que el ataque se encuentre ejecutando.

Rogue DHCP Server para iniciar el ataque, la herramienta yersinia crea un servidor DHCP falso, el cual asignara direcciones ip a los clientes y al establecer conexión recibe la información generada por los mismos.

Mitigar este tipo de ataque es necesario habilitar la opción DHCP Snooping en la interfaz bridge del router, esto es una característica de seguridad en capa 2 que limita a los servidores dhcp no autorizados que proporcionen información maliciosa a los usuarios, además aquellas interfaces del dispositivo que brindan servicio dhcp se deben establecer en confiables para que las solicitudes no sean bloqueadas, su funcionamiento se puede comprobar mediante los logs emitidos. (Derten, 2019)

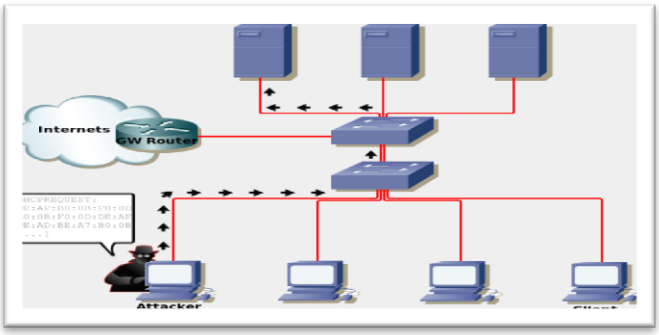

FIGURA 4.
Ataque DHCP Starvation
Elaborado por (Segu-Info - Ciberseguridad desde 2000)

TCP Sync el blanco principal de este tipo de ataque son los hosts que corren procesos tcp. Así, explota la vulnerabilidad del proceso tcp three-way handshake. Dicho proceso está diseñado de forma tal que dos computadoras puedan negociar los parámetros de conexión socket tcp, antes de la transmisión de datos como solicitudes ssh y http. Esquema del tcp three-way handshake.

Considerando el diagrama de más arriba y asumiendo que Host A (Cliente) y Host B (Servidor), el atacante se hace pasar por el Host A. Luego, comienza a enviar un número excesivo de peticiones tcp syn bajo direcciones ip aleatorias a Host B.

Host B toma por sentado que las peticiones recibidas son legítimas, por lo que responde con un syn-ack. Sin embargo, no llega a recibir el ack final. Como

consecuencia, la petición de conexión nunca se concreta. Mientras, debe seguir enviando syn-acks a las demás peticiones aún sin recibir respuesta. Así, el Host B ya no está disponible para las verdaderamente legítimas peticiones de conexión. (Fernández, 2020)

ICMP Smurf el equipo atacante envía una solicitud de ping (eco) a uno o más servidores de difusión mientras falsifica las direcciones IP de origen (la dirección a la que, en teoría, el servidor debe responder) y proporciona la dirección IP de un equipo de destino. El ping es una herramienta que aprovecha una vulnerabilidad del protocolo ICMP, lo cual posibilita probar las conexiones de una red enviando un paquete y esperando la respuesta;

- el servidor transmite la solicitud a toda la red;
- todos los equipos de la red envían una respuesta al servidor de difusión;
- el servidor redirecciona las respuestas al equipo de destino.

De este modo, cuando el equipo del atacante envía una solicitud a varios servidores de difusión ubicados en diferentes redes, todas las respuestas de esos equipos se enrutarán al equipo de destino. Para mitigar este tipo de ataques se debe establecer un par de reglas en el firewall-filter del router, los cuales dropearan los paquetes de acuerdo con los parámetros que se establezcan en la regla. (Jurado., 2021)

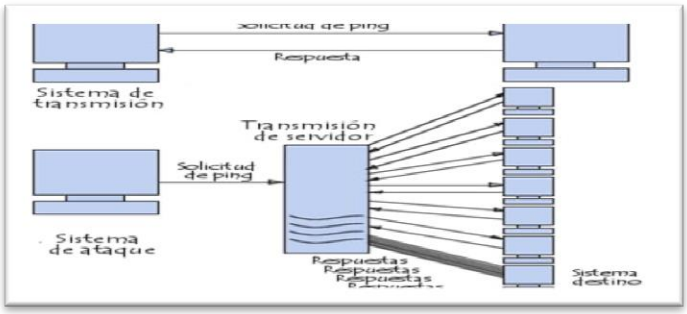

FIGURA 5.
Ataques de ICMP Smurf
Elaborado por (Codgeek.es)

En este caso de estudio se realiza siguiendo los lineamientos determinados en la línea de investigación y entrevistas, con observaciones objetivas sobre el análisis de ataques en dispositivos Mikrotik que se generaran, para obtener los porcentajes de uso de CPU del router y poder discutirlos en la fase de resultados, a continuación, se presenta las reglas de firewall para mitigar los ataques red, desde el punto de vista de profesionales con experiencia y el autor de este caso de estudio.

Según el Ing. Pedro García Rosales indica que a través de 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.

- **Regla de Input:** Input accept en un protocolo de 6(tcp), nos permite dar paso a los puertos que agreguemos, ¿para que utilizamos esta regla? La utilizamos para aceptar las peticiones que venga de mis clientes hacia mi Mikrotik o que venga mi proveedor hacia mi cliente.
- **Regla de Forward**: Forward accept en protocolo 17(udp), nos dice; todo lo que atraviese mi red lo acepte, es decir son todos los paquetes que van con destino a nuestra lan.
- **Regla Output:** Esta chain se utiliza para marcar todos los paquetes que salen de Mikrotik; todo lo que va a internet o a otras LAN que tengamos conectadas. (Rosales, 2022)

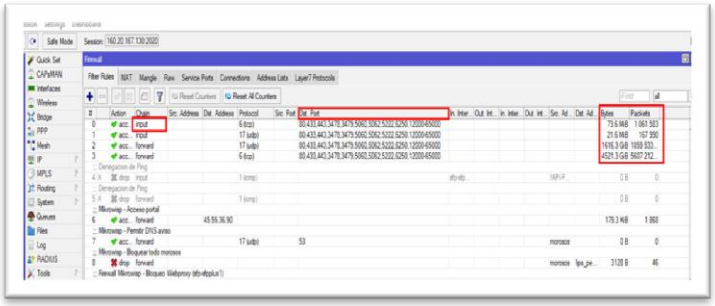

FIGURA 6.
Reglas de input, forward y output
Elaborado por (Jordan Plaza)

Conforme al Ing. Carlos Varas Bajaña indica que, las reglas de bloqueo torrent; es un contenido compartido a nivel de la red para poder crear contenido multimedia, datos, etc. A nivel de mi red.

Estas reglas de torrent-forward-drop fueron creadas, para que todo lo que atraviese en mi Mikrotik ya sea de mi proveedor a mi cliente o mi cliente hacia mi proveedor, por puerto 6(tcp) y 17(udp) y los puerto que están destinado para este tipo de servicio serán bloqueados, con que finalidad, porque nuestro proveedor bloquean este tipo de puerto para que los clientes no descarguen películas de manera ilegal, ya que el contenido multimedia tiene copyright ósea tiene derecho de autor por ende siempre existe entidades que regulariza esto tipos de descargas.

FIGURA 7.
Reglas de Bloqueo Torrent
Elaborado por (Jordan Plaza)

Bloqueos de correo maliciosos 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; que hacemos nosotros creamos una regla de forward todo lo que atraviese en mi Mikrotik y tengan destino esos puertos los bloqueen. (Bajaña, 2022)

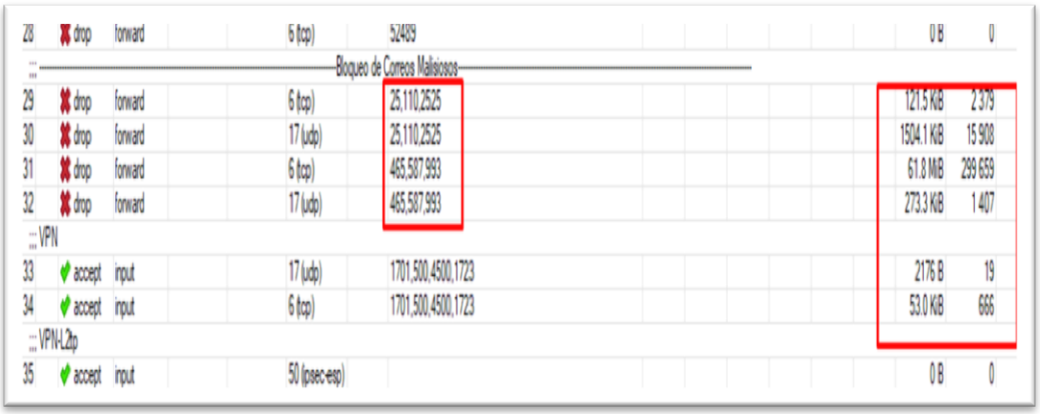

FIGURA 8.
Bloqueos de Correo Maliciosos
Elaborado por (Jordan Plaza)

De acuerdo con el Ing. Manuel Tandazo Mera indica que las reglas de VPN, nos ayudan a proteger nuestros datos mientras mantienen su navegación anónima en línea. Las VPN también ayudan a los usuarios a evitar las geo-restricciones y a desbloquear el contenido de sitios a los que de otro modo no podrían acceder, aunque sean anónimos.

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 (Layer 2 Tunneling Protocol) es una versión actualizada del protocolo PPTP, aunque los protocolos de autenticación son los mismos, este protocolo tiene la ventaja que soporta IPSec, 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, cuando se activa el uso del IPSec en el túnel es necesario permitir el ingreso del protocolo “IPSec-esp” ya que es l que utiliza para incriptar los datos, así como el puerto UDP 500.

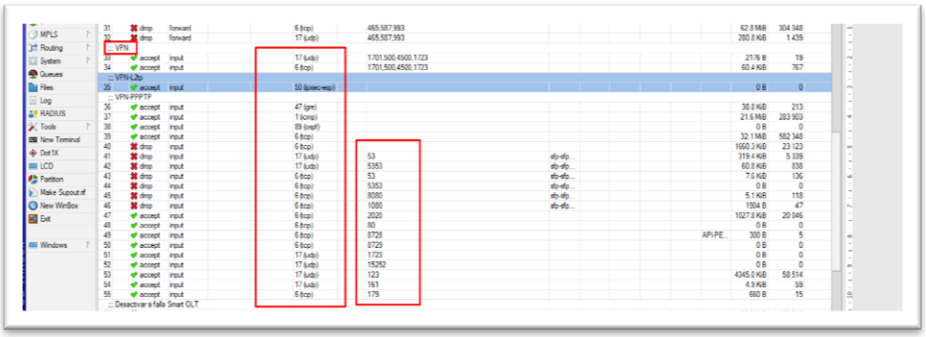

FIGURA 9.
Reglas de VPN y Reglas vpn-L2tp
Elaborado por (Jordan Plaza)

VPN-Pptp 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. (Jurado, 2022)

En consonancia con él, Ing. Juan Arizaga Figueroa indica que los protocolo Ospf es un protocolo de enrutamiento que lo colocamos por si acaso un momento queramos una configuración de la misma, en el siguiente proceso aceptamos conexiones tcp establecida y relevantes y descartamos todos los paquetes que son estado invalido.

Bloqueamos toda petición que sea por el puerto WAN de proveedor 53.

El puerto 53 es utilizado normalmente para las peticiones de ataques de DNS, lo puertos 53-5353 son puertos que utilizan para generar ataques de red de denegación de servicios de los DNS para que no resuelvan las páginas, por eso nosotros bloqueamos por que los DNS tienen salida de nuestros clientes al mundo, pero no entrada del mundo hacia nuestros clientes de esta manera bloqueamos cualquier intento de petición interna para que no exista ataques de red.

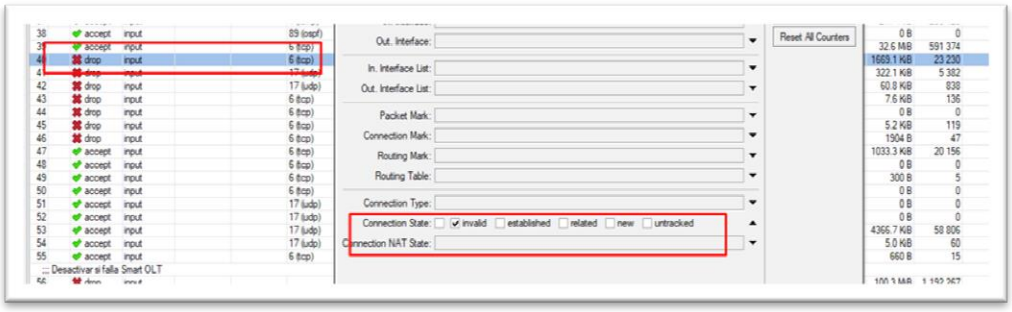

FIGURA 10.
Vpn-ppptp y Protocolo (Ospf)
Elaborado por (Jordan Plaza)

Por Ejemplo:

en esta imagen podemos observar que hay un (kib), que nos indica que si hay peticiones externas que quieren generar ataques de red a nuestro servicio.

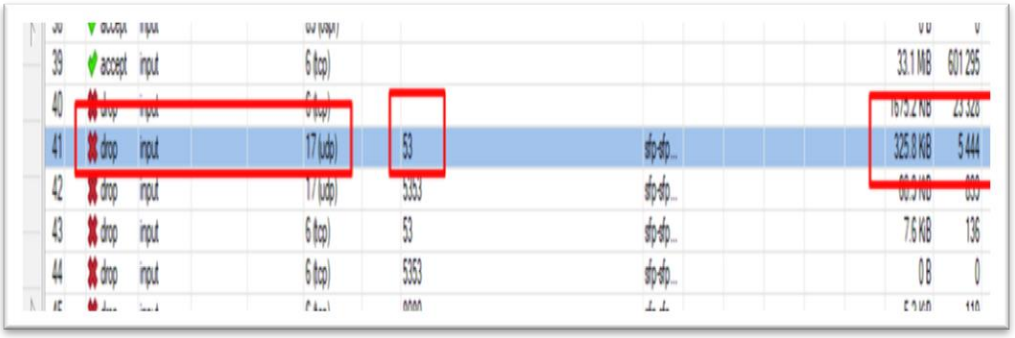

FIGURA 11.
Ejemplo Protocolo (Ospf)
Elaborado por (Jordan Plaza)

Esta parte encontramos una aceptación del puerto 2020 que es el puerto que nosotros utilizamos para nuestro servidor winBox IP-Service y podemos ver el puerto de nuestro winBox que es el 2020, permitimos ese acceso y permitimos el puerto 80 que también se lo utiliza para WinBox por medio de la web.

El 8728 respectivamente se lo utiliza para el aplicativo api, que utiliza para aplicaciones externa y el 8729 también aplicaciones externa, pero de manera segura con protocolo SSL.

1723: lo utilizamos nosotros para lo que es enrutamiento de VPN

15252: lo utilizamos para el servicio IP CLOUD y se actualice la hora y la fecha de nuestro equipo.

123: correspondiente así mismo en protocolo smtp es el servidor para que puedas actualizar automáticamente la hora y la fecha.

161: se lo utiliza normalmente con protocolo smmp protocologia de monitoreo

179: se lo utiliza para poder acceder a cualquier protocolo BGP.

Por último, tenemos una regla de input con una acción drop para que bloquee el resto de tráfico que tenemos y no este declarado como una aceptación.

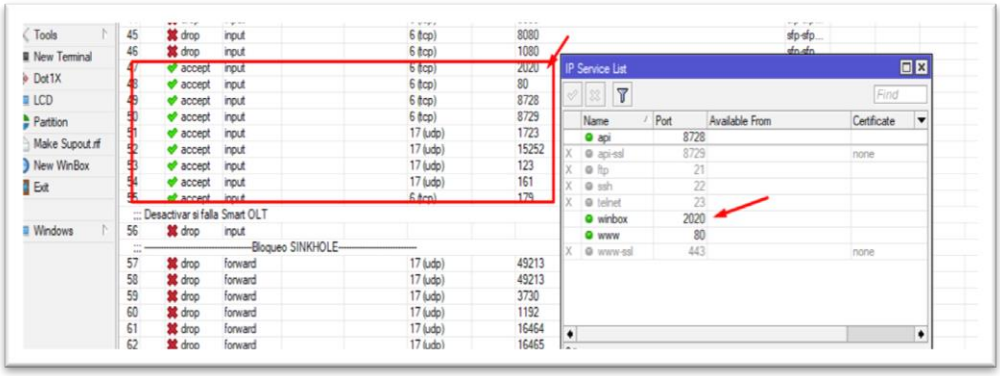

FIGURA 12.
Reglas de aceptación Input
Elaborado por (Jordan Plaza)

Reglas de bloqueo Sinkhole es un agujero de gusano son puertos que ya están declarados dentro nuestros servidores web para poder determinar que nuestros clientes no puedan enviar basura a nuestra red. (Mera I. M., 2022)

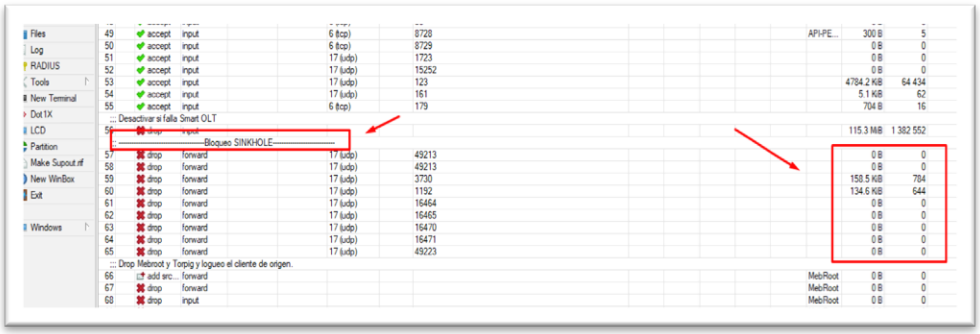

FIGURA 13.
Reglas de bloqueo SINKHOLE
Elaborado por (Jordan Plaza)

Según el Ing. Juan Arizaga Figueroa indica que las reglas de bloqueo drop mebroot y torpig se lo utiliza para bloquear peticiones basuras que están determinada en dos barras 16 como podemos ver en la imagen tenemos dos ip barra 16 que están

determinada prácticamente ataques de red externa que copia información a los servidores rusos.

Ósea cada vez que un cliente peticiones a estas ip públicas en barra 16 que son aproximadamente 65.534 ip públicas que están perdidas y que las utilizan para este tipo de jaqueo van a quedarse bloqueada en una lista llamada MebRootVictim, así el cliente no podrá navegar. (Lozano, 2022)

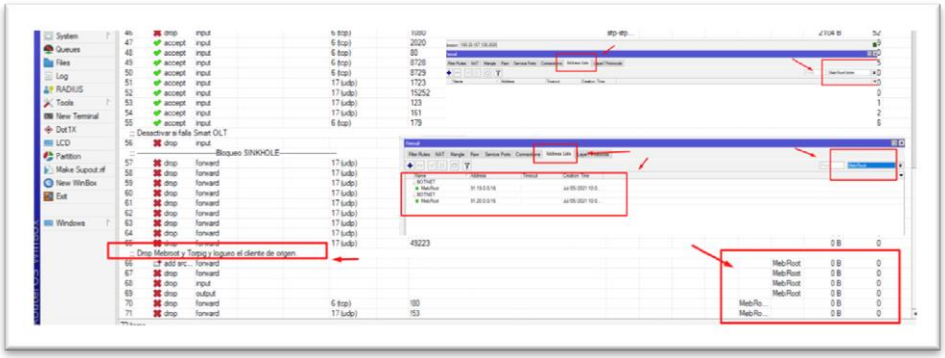

FIGURA 14.
Reglas de bloqueo Drop Mebroot y Torpig
Elaborado por (Jordan Plaza)

Análisis de Viabilidad

En esta fase del proyecto se persigue obtener una visión de conjunto del proyecto, siendo, por tanto, sus objetivos fundamentales los siguientes:

- Conocer el proyecto en su conjunto.
- Estudiar la viabilidad de estas soluciones.

A continuación, se muestran los resultados que se obtuvieron de los ataques generados (antes y después) con las diferentes herramientas seleccionadas.

En la tabla 1 se puede evidenciar como la mitigación reduce un porcentaje considerable del uso del CPU del router.

En el primer ataque (Denegación de servicios DoS) las reglas implementadas (Input, Forward, Output, Reglas de Bloqueo Torrent y Bloqueo Drop Mebroot y Torpig) y gracias a los parámetros de mitigación en el firewall reducen un 59% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules.

Segundo Ataque (Ataques STP) las reglas implementadas (Input, Forward Y Output Y VPN) reducen un 25% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules, debido que son protocolos de VPN que se utiliza para conexiones y así evitar bucles a nivel 2 en nuestra topología cuando se conectan distintos segmentos de red.

Tercer ataque (Tcp Syn Flood) las reglas implementadas (Bloqueo SINKHOLE y Bloqueos de Correo Maliciosos) reducen un 20% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules, Son ataques de agujeros de gusano ósea este ataque se lo refleja cuando una página se cuelga y no carga.

Cuarto ataque (Smurf Attack) las reglas implementadas (Input, Forward Y Output) reducen un 20% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules, este atacante intenta inundar un servidor objetivo con paquetes del Protocolo de mensajes, al realizar solicitudes con la dirección IP falsificada del dispositivo objetivo, pero gracias a las reglas de firewall se lo puede mitigar el ataque y así no tener vulnerabilidades en la red.

Quinto ataque (UDP Flood) las reglas implementadas (Input, Forward Y Output y Protocolo Ospf) reducen un 40% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules.

Sexto ataque (Protocolo de configuración dinámica del host (DHCP)) las reglas implementadas (Input, Forward Y Output) reducen un 9% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules.

Séptimo ataque (Fuerza Bruta) las reglas implementadas (Input, Forward Y Output, VPN Y VPN-L2tp) se reducen un 5% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules.

Octavo ataque (DHCP Starvation) las reglas implementadas (Input, Forward Y Output) reducen un 7% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules.

Noveno ataque (Rogue Dhcp Server) las reglas implementadas (Input, Forward Y Output) reducen un 2% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules, no se observa tanto consumo de CPU debido a que el router únicamente bloquea el paquete ACK proveniente de la interfaz no autorizada, dicho paquete no genera una carga excesiva al router core, motivo por el cual se mantiene en 2% su CPU.

Decimo ataque (Tcp Sync) las reglas implementadas (Input, Forward, Output y Sinkhole) reducen un 13% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rules.

Undécimo ataque (ICMP Smurf) las reglas implementadas (Input, Forward Y Output) reducen un 11% del uso del CPU, su mitigación se lo realiza en el Firewall-Filter Rul.

Tabla 1.

Resumen de Resultados Obtenidos en la Experimentación

	Herramientas									**Mitigación**	**Recursos**	
Ataque	Reglas de Input, Forward y Output	Reglas de Bloqueo Torrent	Bloqueos de Correo Malicios os	Reglas de VPN	Reglas VPN-L2tp	VPN-Ppptp	Protocolo Ospf	Reglas de Bloqueo SINKHOLE	Reglas de Bloqueo Drop Mebroot y Torpig	Firewall filter	%CPU ataque	%CPU mitigación
Denegación de servicios DoS	x	x								x	87%	28%
Ataques SSTP	x			x						x	35%	10%
Tcp syn flood			x					x		x	70%	50%
Smurf Attack	x									x	30%	10%
UDP Flood	x						x			x	49%	9%
Protocolo de configuración dinámica del host (DHCP)	x									x	15%	6%
Fuerza Bruta	x			x	x					x	8%	3%
DHCP Starvation	x									x	12%	5%

Rogue DHCP Server	x									x	2%	0%
TCP Sync	x							x		x	18%	5%
ICMP Smurf	x									x	20%	9%

Tabla #1.
Tabla de viabilidad obtenido
Elaborado por (Jordan Plaza)

Conclusiones

En este trabajo de estudio de vulnerabilidad se explotó los ataques dirigidos a los routers de core MikroTik; Para el análisis de los tipos de ataques e inseguridades de la red informática de la empresa “Swtelecom.net”.

Las vulnerabilidades identificadas mediante este estudio dan a conocer cómo se encuentra la red y sus componentes, estos resultados muestra un nivel bajo de seguridad y alto en vulnerabilidad, debido a la poca atención que se le da a la seguridad informática en general, aunque la persona encargada del área de mantenimiento de la red es quien puede llegar a conseguir que esta situación mejore, empezando por la creación de políticas de seguridad que pueden variar según la infraestructura de la red y la necesidad da la institución, sería factible también organizar un grupo de trabajo especializado que se encargue de administrar y gestionar la red, mitigando los problemas que está pueda presentar.

Se procedió al uso de herramientas software RouterOS que permite el escaneo de debilidades a nivel de puertos de firewall MikroTik. Los resultados obtenidos facilitaron la implementación de mecanismo de seguridad ante los riesgos de ataque, en trabajos futuros se podrían analizar otras alternativas de mitigación para los mismos tipos de ataques descritos en este trabajo, y su firewall permite la creación de distintas reglas o filtros para cubrir los problemas de seguridad.

Bibliografía

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

Avila-Pesantez, B. M. (20 de 08 de 2021). *Mitigación de vulnerabilidades en la red central de un ISP*. Obtenido de Vulnerability mitigation in an ISP core network: http://portal.amelica.org/ameli/jatsRepo/606/6062590006/html/index.html

Bajaña, I. C. (17 de 01 de 2022). Reglas de Firewall- Reglas de Bloqueo Torrent-Bloqueos corro Maliciosos. (J. P. Nicola, Entrevistador)

Cheza, R. C. (2013). *Servicios de red* . Macmillan Iberia, S.A.

Cot Ros, E. (2014). *Constelacion Babieca: ataques contra redes.* Editorial UOC.

Derten. (14 de Marzo de 2019). *El peligro de los ataques DHCP*. Obtenido de El peligro de los ataques DHCP: https://www.derten.com/es/articulos-generales/el-peligro-de-los-ataques-dhcp

Fernández, L. (26 de Enero de 2020). *Así funciona el ataque TCP SYN, aprende cómo mitigarlo eficazmente*. Obtenido de Cómo los ataques TCP SYN afectan a los servidores: https://www.redeszone.net/tutoriales/seguridad/ataque-syn-que-es/

Jurado, I. C. (20 de 01 de 2022). Reglas de Firewall- VPN. (J. P. Nicola, Entrevistador)

Jurado., C. L. (04 de Febrero de 2021). *CCM Benchmark*. Obtenido de ¿Qué es un ataque Smurf?: https://es.ccm.net/contents/13-ataque-smurf

Lara, R. (5 de Abril de 2020). *Seguridad en Switches Cisco: Mitigación de Ataques y Vulnerabilidades*. Obtenido de Ataques STP: https://richardjlara.wordpress.com/2020/04/05/seguridad-en-switches-cisco-mitigacion-de-ataques-y-vulnerabilidades/

Lozano, I. R. (29 de 01 de 2022). Seguridad de Firewall en Mikrotik. (J. P. Nicola, Entrevistador)

Mera, I. M. (26 de 01 de 2022). Reglas de Firewall- Sinkhole. (J. P. Nicola, Entrevistador)

Mera, M. I. (05 de 01 de 2022). Falencias encontrada en la empresa Swtelecom S.A. (J. U. Nicola, Entrevistador)

Rosales, P. J. (07 de 01 de 2022). Reglas firewall de Input, Forward y Output. (J. U. Nicola, Entrevistador)

Santana, W. T. (04 de 01 de 2022). Inicios de la empresa. (J. U. Nicola, Entrevistador)

Anexo

Formulario de Entrevista

Relacionado con: Análisis Técnico Relacionado con la Implementación de Firewall Perimetral para Prevenir Vulnerabilidades en la Red Informática de la Empresa Swtelecom.Net.

Nombre: Ing. Manuel Tandazo Mera

Trabajo: Empresa Red Nueva Conexión

1) **¿Cuál es la estrategia que utilizaría usted para prevenir los ataques en una red de ISP y explicar cada una de ellas?**

   Estrategia a utilizar primeramente los puertos, solo dejar abiertos los puertos que utilizamos segundo utilizar de manera correcta las ips para los clientes no crear ips innecesarias por esa razón no creamos vulnerabilidad antes los ataques de red locales

   Tercero el uso apropiado de las públicas, las ips públicas son una ventaja para poderte conectar externamente a tus dispositivos, pero también son una desventaja para los Isp si tiene mal configurado su firewall ya que de esa manera tendría ataques masivos hacia su red.

2) **¿Por qué recomienda usted tener protegida la red empresarial con reglas de firewall perimetral?**

   La principal recomendación de tener puesto un firewall de seguridad dentro de un equipo es para no en listarme en listas negras y poder defenderme cualquier ataque de red ya sea externo por mi proveedor de internet o interno por mis clientes.

3) **¿Indicar a su criterio técnico, la forma de como mitigar al menos 2 tipos de ataques y detalle cada uno de ellos?**

   Primer ataque DoS: Existe una normativa técnica o controles de tráfico en la cual podemos denegar el ping porque los ataques DoS se generan por protocolos icmp o ping por eso podemos destacar hasta ciertos números de peticiones al equipo para que el excedente sea descartado y de esa manera mitigar los ataques.

   Segundo ataque Fuerza bruta: Atreves de Vpn pptp local es la más usada denominada así un protocolo de seguridad que te permite ingresar usuario y clave de baja locación, cuando ya seas atacado por miles de veces por ese puerto la manera más practica de mitigar ese ataque es desactivar los servicios de pptp.

4) **¿Sabe usted algo de nuevas tecnologías que vendrán para las telecomunicaciones y cuáles recomienda?**

   Las nuevas tecnologías para las telecomunicaciones tenemos entre ello codificadores de señal, trasmisores ópticos, moduladores de frecuencia para radios enlaces.

   Se recomienda la fibra óptica con equipos que permitan modular mayor ancho de banda en los equipos finales ósea routers.

5) **¿Qué recomienda usted a las empresas de ISP para brindar mejor servicio y no sufra ataques de redes?**

   Las recomendaciones para las empresas que brinda el servicio de internet es que contraten a una empresa externa para que pueda realizar la verificación constante e instalar filtros que le permita monitorear cual es el ataque más común y de esa manera mitigar los ataques de red más frecuente, de esa manera garantizar un buen servicio para los clientes.

Nombre: Ing. Ruben Dario Lozano Lozano

Trabajo: Tecnycompsa

1) **¿Cuál es la estrategia que utilizaría usted para prevenir los ataques en una red de ISP y explicar cada una de ellas?**

   Mantener los equipos actualizados, ya que cada actualización trae consigo las mejoras y parches de las vulnerabilidades que traía consiga la versión anterior.

   Implementar un buen firewall en la red para poder prevenir y mitigar posibles intentos de ataques en la red.

2) **¿Por qué recomienda usted tener protegida la red empresarial con reglas de firewall perimetral?**

   Porque permite filtrar tanto las conexiones que ingresan y atraviesan la red, evitando así la propagación de códigos maliciosos o de accesos no autorizados que sean perjudiciales para la empresa.

3) **¿Indicar a su criterio técnico, la forma de como mitigar al menos 2 tipos de ataques y detalle cada uno de ellos?**

   Ataque TCP Sync suele presentarse cuando hay puertos abiertos y la forma de mitigarlo es limitar las conexiones de los paquetes, si estos paquetes exceden el umero

de conexiones por segundo establecidas e n las regalas de firewall estaos son descartados automáticamente, así mismos se recomienda desactivar los puertos abiertos y q no estén siendo utilizados.

Ataque ICMP, es un ataque en el cual envían paquetes ICMP hacia el equipo destino el cual provoca una inundación de conexiones y elevando el CPU, para mitigar este tipo de ataque he usado unas reglas de firewall para dropear los paquetes ICMP no permitidos.

4) **¿Sabe usted algo de nuevas tecnologías que vendrán para las telecomunicaciones y cuáles recomienda?**

   He leído sobre las redes definidas por software (SDN) que son redes que permiten que controlemos las redes por software, y no solo por hardware como tradicionalmente se lo ha venido haciendo. Esto permitirá una mejor administración centralizada además de la involucración del desarrollo de software con las redes.

5) **¿Qué recomienda usted a las empresas de ISP para brindar mejor servicio y no sufra ataques de redes?**

   Recomendaría la implementación de un sistema de Detección y prevención de intrusos (IDS/IPS) el miso que permitirá monitorizar las conexiones y alertara los posibles intentos de acceso no autorizados.

Nombre: Ing. Carlos Varas Bajaña

Trabajo: Empresa Red Nueva Conexión

1) **¿Cuál es la estrategia que utilizaría usted para prevenir los ataques en una red de ISP y explicar cada una de ellas?**

   Las estrategias más utilizadas para prevenir ataques hacia mi red son: primero: cambiar los puertos más usado de mi equipo Segundo: mantener los equipos actualizados correctamente y, por último, implementar reglas de firewall en la red para poder prevenir y mitigar ataques ya sea interno o externo de la red.

2) **¿Por qué recomienda usted tener protegida la red empresarial con reglas de firewall perimetral?**

   Se recomienda las reglas firewall de seguridad dentro de los equipos Mikrotik es para estar protegido de virus y ataques de red además nos ayuda a no caer en listas negras ya que nos genera problemas con la navegación de nuestros clientes.

3) **¿Indicar a su criterio técnico, la forma de como mitigar al menos 2 tipos de ataques y detalle cada uno de ellos?**

Ataques de Spam: funciona porque las maquinas están enviando constantemente correos masivos hacia servidores del mundo la manera mas factible de mitigar este tipo de ataques es utilizando reglas de control para bloqueas puertos no seguros como son el 25, 2525, 110 y permitir el envió de correos por el 465, 685, 339, que son puertos seguros en protocolos ssl.

Ataque de destination port: tratan de ver el puerto que tienes por ejemplo el de web puerto 80 que es el puerto mas solicitado que resultan que comienzan a general ataques a ese puerto para mitigar ese ataque la manera mas optima es cambiando el puerto de la web de tu equipo.

4) **¿Sabe usted algo de nuevas tecnologías que vendrán para las telecomunicaciones y cuáles recomienda?**

Unas de las nuevas tecnologías que le puedo recomendar a las empresas proveedoras de internet implementar servidores DNS para mejorar las peticiones de los clientes y de esa manera el internet sea más fluido.

También se le puede recomendar un servidor emby de películas que sea interno de la red para los clientes.

5) **¿Qué recomienda usted a las empresas de ISP para brindar mejor servicio y no sufra ataques de redes?**

Unas de las recomendaciones clave para una empresa distribuidora de internet es contratar a un Ingeniero de telecomunicaciones con la suficiente experiencia para dar soluciones a los problemas de la red he implementar nuevas tecnologías en la empresa.

Otra recomendación es invertir en nuevos equipos en un cierto periodo para mantener actualizada la red y dar un servicio optimo a sus clientes.

Conclusión de la entrevista

El objetivo fundamental de esta entrevista es dará a conocer a las empresas proveedoras de internet optimas recomendaciones para que puedan implementar y mejorar el servicio del internet.

En la primera pregunta se consultan estrategias para prevenir ataques de red, se recomienda, desactivar puertos que son vulnerables en la red, actualización correcta de los equipos e implementación de firewall de seguridad. En la segunda pregunta de protección de reglas de firewall, se puede apreciar el acuerdo de la implementación ya que protege la red de ataques de virus, listas negras y códigos malicioso que son perjudicial para la empresa. En la tercera pregunta de ataques de red se puede apreciar diversos ataques, pero están de acuerdo los entrevistados que la mejor forma de mitigar esos ataques es por medio de reglas de firewall, Vpn y bloqueos de puertos que son vulnerables. Cuarta pregunta de implementación de nuevas tecnologías, se recomienda por ingenieros expertos para la empresa de radio enlace codificadores de señal, transmisores ópticos y moduladores de frecuencia para radio enlaces. Para empresas de fibra óptica, SDN que permite el control de la red por medio de software y no por hardware por último la implementación de servidores DNS y servidores emby de películas de esta manera se garantiza la funcionalidad optima de la empresa. Quinta y ultima pregunta se puede apreciar el acuerdo de contrataciones de Ingenieros o empresas que brinden servicios profesionales de telecomunicaciones para que mantengan en optimas condiciones la red e implementar nuevas tecnologías como es el sistema de (IDS/IPS) que permite el monitoreo de conexiones y alertar los posibles intentos de acceso no autorizados.