Artículo de Investigación

Mitigación de vulnerabilidades en la red central de un ISP: Un caso de estudio

Vulnerability mitigation in an ISP core network: A case study

Mauricio Palate, Byron; Avila-Pesantez, Diego

Byron Mauricio Palate
byron.m.palate.s@pucesa.edu.ec
Escuela Superior Politécnica de Chimborazo, Ecuador
Diego Avila-Pesantez
davila@espoch.edu.ec
Escuela Superior Politécnica de Chimborazo, Ecuador

Ecuadorian Science Journal
GDEON, Ecuador
ISSN-e: 2602-8077
Periodicidad: Semestral
vol. 5, núm. 2, 2021
esj@gdeon.org

Recepción: 16 Julio 2021
Aprobación: 20 Agosto 2021

URL: http://portal.amelica.org/ameli/jatsRepo/606/6062590006/index.html

DOI: https://doi.org/10.46480/esj.5.2.117

Como citar: Palate, B. M., & Avila, D. (2021). Mitigación de vulnerabilidades en la red central de un ISP: Un caso de estudio. Ecuadorian Science Journal, 5(2) 68-82. DOI: https://doi.org/10.46480/esj.5.2.117

Resumen: Los incidentes de ciberseguridad en infraestructura de ISP (Internet Service Provider) han crecido de manera significativa y es necesario identificar las vulnerabilidades que necesitan una protección inmediata. En este entorno, el firewall tiene la capacidad de filtrar paquetes de datos, analizando las cabeceras y tomando una decisión del encaminamiento del paquete en base a las reglas establecidas. Este dispositivo es muy indispensable en una red ISP, debido a que mitiga las vulnerabilidades provenientes de la red, manteniendo un mayor grado de seguridad informática para su red interna, garantizando así la disponibilidad, integridad y confidencialidad de la información. En el estudio de caso se seleccionó infraestructura de marca Mikrotik con sistema operativo propietario llamado RouterOS el cual funcionara como un router de core, en donde se aplicarán las reglas de seguridad un su firewall para cada tipo de ataque que se generara hacia el router, ya sean ataques internos o externo de la red, evitando causar graves fallas de seguridad como ser víctima de un ataque DoS (Denegación de servicio), ataques de fuerza bruta, etc. Después de la implementación de las debidas reglas de mitigación en el firewall del router Mikrotik, como resultado se obtuvo una disminución del 50% del consumo del CPU en cada ataque generado, logrando así el buen funcionamiento de la infraestructura de red, garantizando la estabilidad y la disponibilidad de la red de comunicaciones.

Palabras clave: Mikrotik, RouterOS, Ataque, Mitigación, ISP.

Abstract: Cybersecurity incidents in ISP (Internet Service Provider) infrastructure have grown significantly and it is necessary to identify vulnerabilities that need immediate protection. In this environment, the firewall can filter data packets, analyzing the headers and deciding about the routing of the packet based on the established rules. This device is very essential in an ISP network because it mitigates the vulnerabilities coming from the network, maintaining a higher degree of computer security for your internal network, thus guaranteeing the availability, integrity, and confidentiality of the information. In the case study, a Mikrotik brand infrastructure was selected with a proprietary operating system called RouterOS, which will function as a core router, where the security rules will be applied to your firewall for each type of attack that will be generated against the router. , whether they are internal or external attacks on the network, avoiding causing serious security failures such as being the victim of a DoS

(Denial of Service) attack, brute force attacks, etc. As a result, a 50% decrease in CPU consumption was obtained in each attack generated, thus achieving the proper functioning of the network infrastructure and guaranteeing stability and availability of the communications network.

Keywords: Mikrotik, RouterOS, Attack, Mitigation, ISP.

Introducción

Los proveedores de servicio de internet (ISP, por sus siglas en inglés) presentan un alto índice de vulnerabilidades respecto a la infraestructura de la red, en especial en los equipamientos de la red central (CORE), 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 (Shaikh et al., 2020). Según Fabio Assolini de la empresa Kaspersky, menciona que "En el año 2020, las tecnologías de Kaspersky han bloqueado 45 intentos de infección en América Latina cada segundo. Eso significa que cada segundo, un usuario en América Latina sufre un ataque" (Assolini Fabio, 2019). Por otro lado, según la información levantada por el Centro de respuestas a incidentes informáticos Ecucert, el 43% de las empresas ISP que brindan los servicios de telecomunicaciones utilizan equipos Mikrotik (Ecucert, 2017). 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 (Sukaridhoto & ST Ph, 2014).

En el presente artículo se explorará las principales vulnerabilidades a los que están expuestos los routers Mikrotik, mediante la generación de ataques dirigidos y controlados, utilizando las herramientas de análisis de redes incorporadas en el sistema operativo Kali Linux. En base a los resultados se implementaron las reglas o filtros en el firewall del RouterOS para mitigar las debilidades, las cuales son analizadas en las próximas secciones.

El resto del artículo está estructurado como se describe a continuación: en la sección II se mostrarán las principales vulnerabilidades expuestas en los routers Mikrotik, así como las herramientas informáticas que ayudan a explotarlas. En la sección III se describen la metodología implementada, mientras que en la sección IV se detalla la fase de experimentación. En la sección V se muestran los resultados finales obtenidos, y finalmente, en el apartado VI se discuten las conclusiones del artículo.

Fundamentación

Un sistema es considerado seguro cuando satisface las cualidades de disponibilidad, integridad y confidencialidad de la información (López, 2010), el principal objetivo de un ataque es interrumpir algunas de estas propiedades. Los ataques de seguridad pueden clasificarse en activos o pasivos. En un ataque activo se intenta alterar la información que se está transmitiendo y su principal objetivo es amenazar la integridad, autenticación y la disponibilidad de los datos. En cambio, un ataque pasivo es aquel donde el atacante monitoriza toda la información generada por el usuario sin modificar o añadir datos, su objetivo es obtener la información que se está transmitiendo (Wu & Irwin, 2016).

De acuerdo con el estudio realizado por Ceron (Ceron et al., 2020) muestra que el porcentaje de equipos Mikrotik implementados en infraestructura de red ha crecido a nivel mundial, sin embargo, da a conocer algunos ataques registrados mediante la implementación de honeypot, pero no detalla alguna solución para poder mitigarlos. Por otro lado, en una infraestructura de red, los firewalls están diseñados para brindar seguridad a nuestra intranet, para ello existen diversos mecanismos de defensa, como se puede evidenciar

en estudios realizado por Mursyidah (Mursyidah et al., 2019), donde se aplica un método muy eficaz para proteger el acceso al router ante posibles ataques de fuerza bruta. A continuación, se revisa las principales vulnerabilidades que afectan a los routers Mikrotik, las cuales se encuentran descritas en su principal certificación de seguridad Mikrotik Certified Security Engineer (Mikrotik, 2021).

Vulnerabilidades

Denegación de servicio (DoS, por sus siglas en inglés): Este tipo de ataque puede causar la sobrecarga de un enrutador. Lo que significa que el uso de la CPU llega al 100% y el enrutador puede volverse inaccesible con tiempos de espera. Todas las operaciones en paquetes que pueden consumir un procesamiento significativo de la CPU, como el firewall (filtro, NAT, mangle), el registro y las colas, pueden provocar una sobrecarga si llegan demasiados paquetes por segundo al router (Bartholemy & Chen, 2015).

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 (Bogdanoski et al., 2013). 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, por sus siglas en inglés) en el que un atacante intenta inundar un servidor objetivo con paquetes del Protocolo de mensajes de control de Internet (ICMP, por sus siglas en inglés), 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 (Aldaoud et al., 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 (Singh & Juneja, 2010). El objetivo es crear y enviar una gran cantidad de datagramas UDP, que se relaciona por medio del puerto 53 en UDP. Este tipo de ataque es muy usual desde la red de internet hacia el RouterOS, debido a que el router Mikrotik puede trabajar como un servidor DNS.

Protocolo de descubrimiento de vecinos MikroTik (MNDP, por sus siglas en inglés) y el protocolo de descubrimiento en capa de enlace (LLDP, por sus siglas en inglés): permiten encontrar otros dispositivos compatibles con MNDP o CDP (Protocolo de descubrimiento de Cisco) o LLDP en el dominio de difusión de Capa 2 (Braem et al., 2014). Este protocolo trabaja en UDP/5678, es de gran utilidad para un administrador de red, ya que permite visualizar la topología de red en capa 2, donde brinda información muy relevante de los dispositivos encontrados como son: ip-address, mac-address, identidad (nombre), versión del software y tipo de hardware.

Protocolo de configuración dinámica del host (DHCP, por sus siglas en inglés): 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. Se pueden presentar los siguientes ataques.

DHCP Starvation: Este ataque tiene como objetivo los servidores DHCP, donde el atacante crea solicitudes falsas para agotar las direcciones IP disponibles (Mukhtar et al., 2012). Funciona mediante paquetes de difusiones MAC falsas, generalmente la negociación de DHCP con el router se realiza en la capa 2, debido a que inicialmente no existe dirección IP, entonces el DHCP inicia una negociación conocida como DORA (Discovery, Offert, Request & Acknowledgement), después de esta negociación, el router servidor nos permite la asignación de una dirección IP.

Rogue DHCP Server: Proporciona una configuración de red incorrecta para el nuevo cliente que se ha conectado a la red falsa, con el objetivo de crear un tipo de ataque llamado man in the middle (MitM) (Kadafi & Khusnawi, 2015). Típicamente configurado por un atacante para aprovecharse de los clientes y recibir la información que generan dichos clientes.

Protocolo de mensajes de control de Internet (ICMP, por sus siglas en inglés): Este protocolo ayuda a las redes a resolver problema de comunicación, los hackers pueden hacer uso de ICMP para poder buscar hosts activos en la red. El ataque más común es:

ICMP Smurf: Este ataque es una versión más sofisticada de un ataque DDos, donde el atacante genera una gran cantidad de paquetes ICMP de origen falsificados y tienen como destino la IP del servidor victima (Gunnam & Kumar, 2017). Generalmente, proviene de la red LAN, debido a que es un tipo de tráfico ICMP, pero se genera tráfico hacia la red broadcast, dado que una única dirección de broadcast admite 255 host, entonces este ataque amplifica un solo paquete ping 255 veces a nivel de peticiones.

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 (Domínguez et al., 2016).

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 (Ahmad et al., 2015). Entre las más importante se detalla a continuación.

Nmap: Herramienta de licencia gratuita y de código abierto, empleada por miles de personas para el escaneo, administración y auditoria en seguridad de redes. Su función es desde lo más simple como el escaneo de puertos, hasta listar métodos de elaboración de paquetes de bajo nivel utilizados por los piratas informáticos avanzados (Chauhan, 2017).

Hydra: Es una de las mejores herramientas de craqueo de inicio de sesión que admite varios protocolos de ataque (Grover & Gagandeep, 2020), y muy eficaz para los ataques por fuerza bruta hacia los diferentes servicios.

Yersinia: Es un framework para realizar ataques de capa enlace de datos. Está esquematizado para ganar acceso gracias a vulnerabilidades que existen en diferentes protocolos de red. Tiene como objetivo principal ser una herramienta sólida para analizar y certificar las redes desplegadas(Omella et al., 2017). Algunos de los ejemplos de ataque que maneja esta herramienta son: Spanning Tree Protocol (STP), Dynamic Host Configuration Protocol (DHCP), Cisco Discovery Protocol (CDP).

Hping3: Es una herramienta que ensambla y analiza paquetes TCP/IP mediante línea de comandos, su interfaz está inspirada en el comando ping de Unix, a diferencia que hping no solo puede enviar solicitudes de eco ICMP. Es compatible con los protocolos TCP, ICMP, RAW-IP y UDP, tiene un modo de seguimiento de ruta, la capacidad de enviar archivos entre un canal cubierto y muchas otras funciones (Sanfilippo & Salvatore, 2018).

Metodología y métodos

El caso de estudio se basa en un método experimental, 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.

El laboratorio está constituido mediante un router central de marca Mikrotik-RouterOS en su línea de Cloud Core, el cual está orientado al funcionamiento en una red central, debido a su alta robustez en software

y hardware. Conjuntamente, con un computador con sistema operativo Kali Linux, el cual será utilizado para generar ataques de fabricación controlados, y otro computador de monitoreo/Administrador conectado directamente al router, para poder revisar su comportamiento y aplicar la configuración necesaria para mitigar los ataques, que se generan en la red interna y externa utilizando un direccionamiento IP, esto se puede ver en la Figura 1.

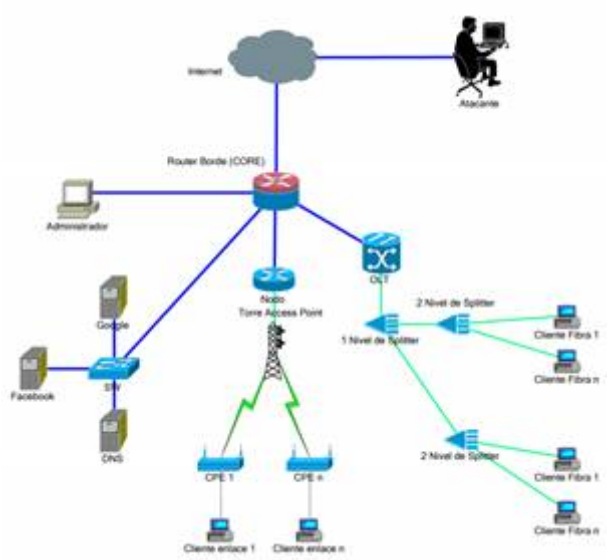

FIGURA 1.
Infraestructura de red del ISP para el proceso de experimentación.
Autores.

En cada ataque, como punto principal se verificará el estado de los recursos consumidos (CPU) en el router (antes, durante y después de la generación del ataque), debido a que este parámetro controla y ejecuta las tareas del dispositivo. Para la mitigación, las reglas que se establecen en el router se configuran en diferentes apartados de su firewall (interfaces, Firewall-Filter, Firewall-RAW, Bridge-Filter). Esto depende si el ataque es generado en capa 2 o capa 3.

1) Ataque Management Network Discovery Protocol (MNDP)

Antes de generar el ataque se debe verifica su tabla de neighbor y el estado del Router (Figura 2).

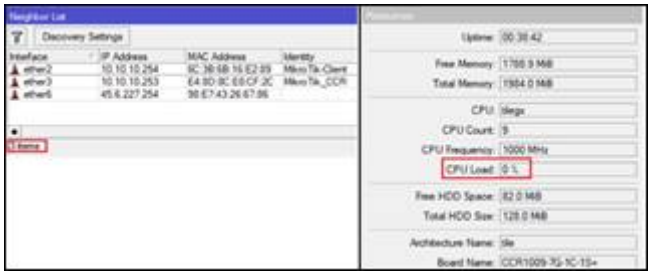

FIGURA 2.
Medición de consume de CPU antes del ataque MNDP.
Autores.

En el sistema operativo Kali-linux se ejecuta el ataque "Flooding CDP table" en la herramienta Yersinia (Figura 3). Este ataque comienza a trabajar inmediatamente inundando al router de core con paquetes CDP, el cual hace que el CPU del router comience a elevar su consumo, como se puede apreciar en la Figura 4.

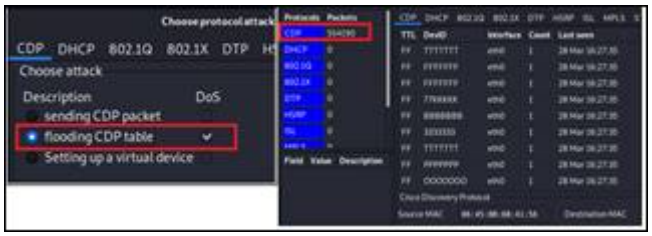

FIGURA 3.
Ataque Flodding CDP- generado en Kali-Linux.
Autores.

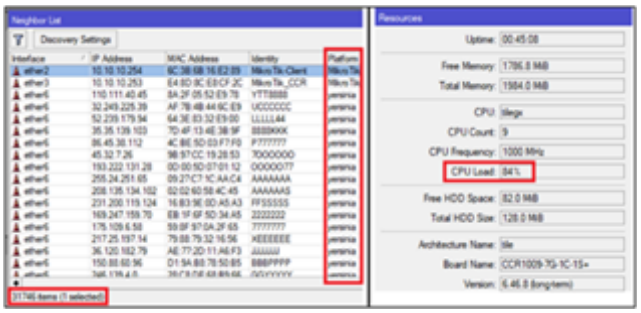

FIGURA 4.
Consumo de CPU en ataque MNDP.
Autores.

Para mitigar este ataque, Mikrotik recomienda crear una lista de interfaces, en la cual únicamente se pueda negociar a través de este protocolo MNDP/CDP/LLDP, para este estudio de caso únicamente será la interfaz ether1. Una vez aplicado la regla de mitigación MNDP, se comprueba el estado del router en la tabla neighbors y el consumo de CPU para comprobar que la regla funcione correctamente como se apreciar en la Figura 5.

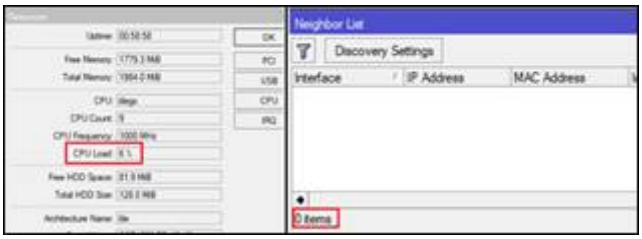

FIGURA 5.
Mitigación MNDP.
Autores.

2) Ataque 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 (Figura 7).

FIGURA 6.
Ataque DHCP Yersinia-Kali.
Autores.

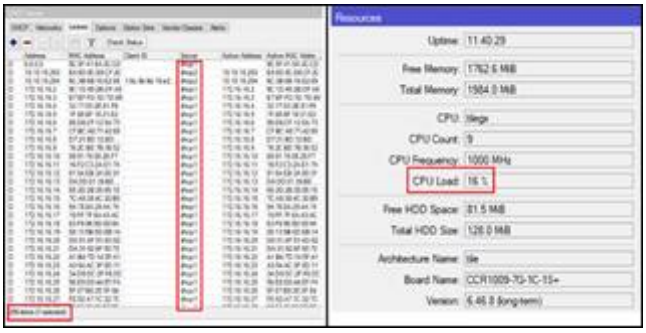

FIGURA 7.
CPU ataque DHCP Starvation.
Autores.

Para mitigar el ataque se crea una regla en el filter-bridge del RouterOS donde permita únicamente paquetes DHCP de interfaces reconocidas. Una vez establecidas las reglas de mitigación (Figura 8), se puede observar que el tamaño de bytes en la regla de filter-bridge se incrementa, esto debido al bloqueo de la gran cantidad de paquetes que ingresan al router solicitando conexión para el servicio de DHCP, y además el uso del CPU disminuye considerablemente.

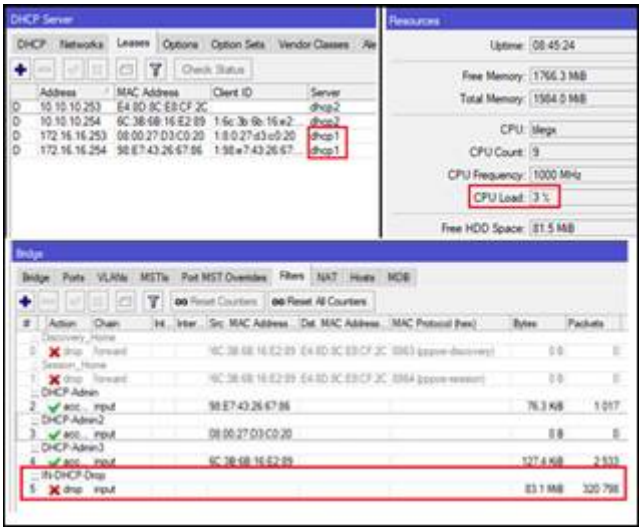

FIGURA 8.
Mitigación DHCP Starvation.
Autores.

3) Rogue DHCP Server

Para iniciar el ataque, la herramienta Yersinia crea un servidor DHCP falso (Figura 9), el cual asignara direcciones IP a los clientes y al establecer conexión recibe la información generada por los mismos. Para

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 (Figura 10).

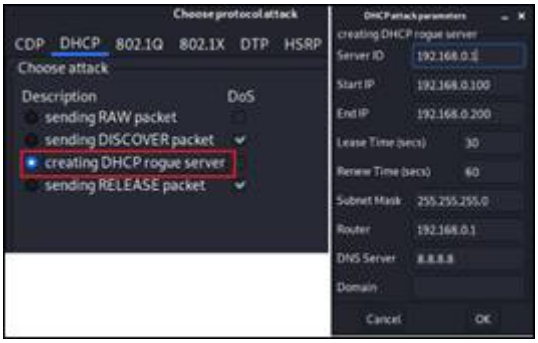

FIGURA 9.
Ataque Rogue-DHCP.
Autores.

FIGURA 10.
Log router-Ataque rogue DHCP.
Autores.

4) Ataque TCP Sync

Para la demostración, se utiliza la herramienta Nmap, juntamente con la herramienta hping3 de Kali (Figura 11), el atacante envía una gran cantidad de paquetes TCP/SYN 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 (Figura 12), y se lo realiza mediante un puerto abierto del router.

FIGURA 11.
Ataque TCP Sync-Kali.
Autores.

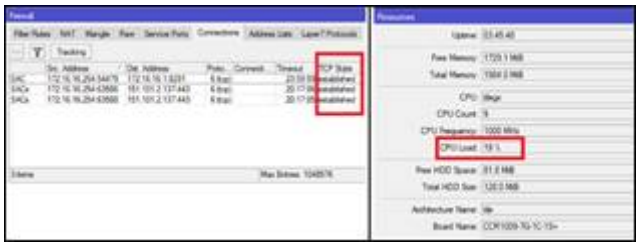

FIGURA 12.
Consumo de CPU ataque TCP Sync.
Autores.

Para poder mitigar este ataque en el router de core, es necesario limitar las conexiones de los paquetes que provienen marcados con la bandera "flags-tcp=syn", si dichos paquetes exceden el número de conexiones por segundo establecidos en la regla, serán descartados automáticamente. Además, se debe configurar la opción "tcp syn-cookie", esto ayuda a que el dispositivo pueda saber el número de conexiones que ha establecido cada host. Conjuntamente a esto para brindar una mayor seguridad, se debe desactivar los puertos abiertos de los servicios que no se utiliza. En la Figura 13, se puede observar como la regla "Drop-Sync-attack" se incrementa en bytes y paquetes, esto debido a la gran cantidad de paquetes que se están descartando, además se observa que el consumo del CPU se reduce.

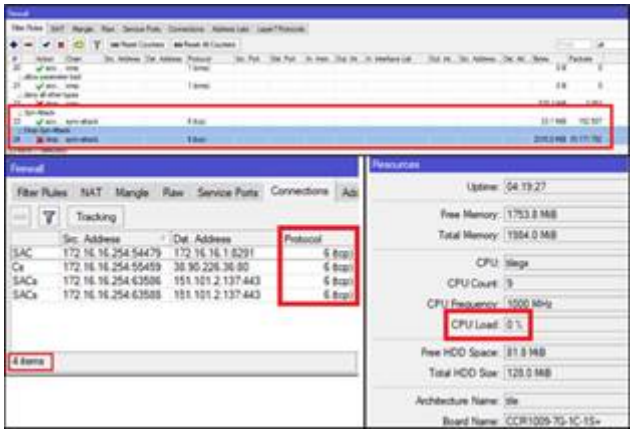

FIGURA 13.
Mitigación ataque TCP-Sync.
Autores.

5) Ataque UDP flood

Para este ataque se utiliza la herramienta Nmap para comprobar que el puerto 53 UDP se encuentre abierto en el router y la herramienta hping3 para generar el ataque de inundaciones UDP hacia este dispositivo (Figura 14).

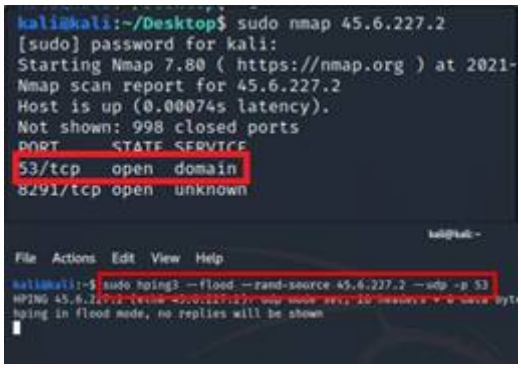

FIGURA 14.
Ataque UDP flood -Kali.
Autores.

Una vez iniciado el ataque se puede observar cómo se generan conexiones UDP hacia el dispositivo, elevando el consumo de CPU como se aprecia en la Figura15. Para mitigar este tipo de ataque se debe deshabilitar el reenvió de paquetes DNS en Mikrotik "Allow Remote Request", si esta opción se encuentra activada, es necesario contar con regla de filtro para evitar los ataques DNS entrantes hacia el router de core. Un ataque DNS sobre el puerto 53/UDP es aconsejable realizarlo en el Firewall-RAW, ya que al descartar las peticiones UDP antes de ser analizadas por el Firewall-Filter elimina una carga grande al CPU. Una vez generada la regla de mitigación en el RAW se puede observar el incremento de bytes y de paquetes debido al bloqueo que se está realizando, al igual que el consumo del CPU del router, esto se puede apreciar en la Figura 16

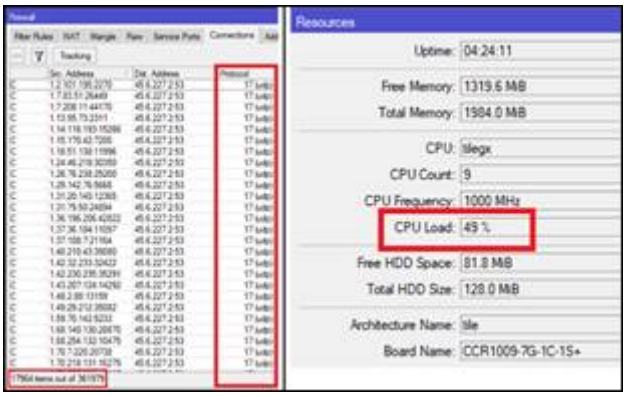

FIGURA 15.
Consumo de CPU Ataque UDP-flood.
Autores.

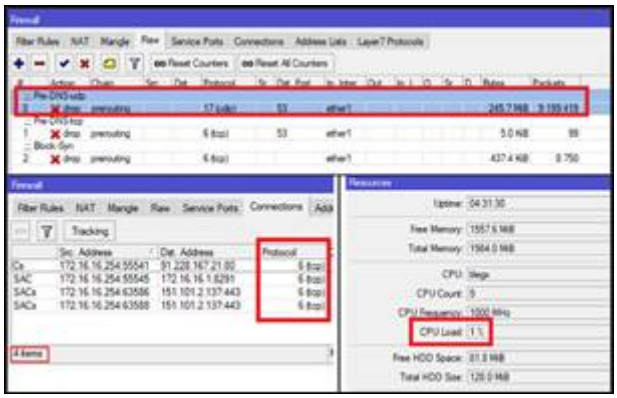

FIGURA 16.
Mitigación ataque UDP-flood.
Autores.

6) Ataque de fuerza bruta

Para este ataque se utilizará la herramienta Nmap e Hydra, para tratar de establecer coincidencias de usuario y contraseña para el acceso al router de CORE mediante el puerto 22 como se aprecia en la Figura 17. Este ataque se puede comprobar mediante los logs generados por el dispositivo. debido a los inicios de sesión fallidos por el programa Hydra (Fig. 18).

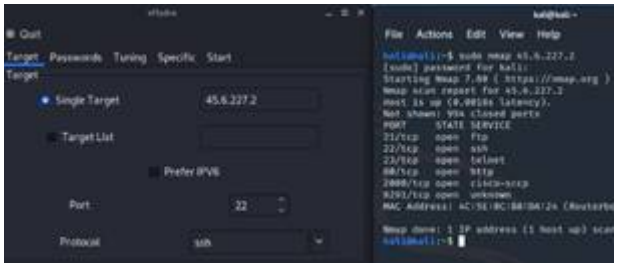

FIGURA 17.
Ataque fuerza bruta-Kali.
Autores.

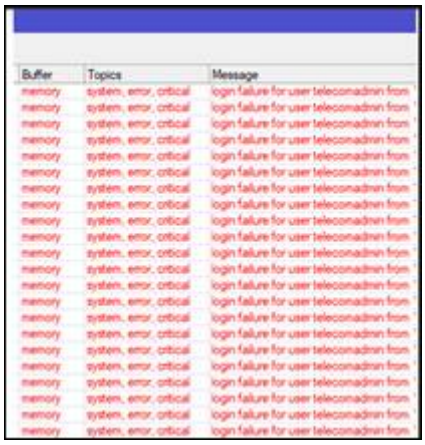

FIGURA 18.
Logs router-ataque fuerza bruta.
Autores.

Para poder mitigar este tipo de ataque es un poco interesante debido a que las reglas que se establecen constituyen un bloque de etapas que normalmente funcionan de atrás hacia adelante, debido al tiempo que se

necesita entre regla y regla para poder atrapar al atacante, ya que cada intento de sesión invalido se registraría en una etapa del firewall. Establecido las reglas se vuelve a realizar inicios de sesión fallidos, pero al quinto inicio de sesión la regla del firewall entra en acción dropeando los paquetes, esto se puede apreciar en la Figura 19, donde se ve un incremento de paquetes y bytes en la regla establecida.

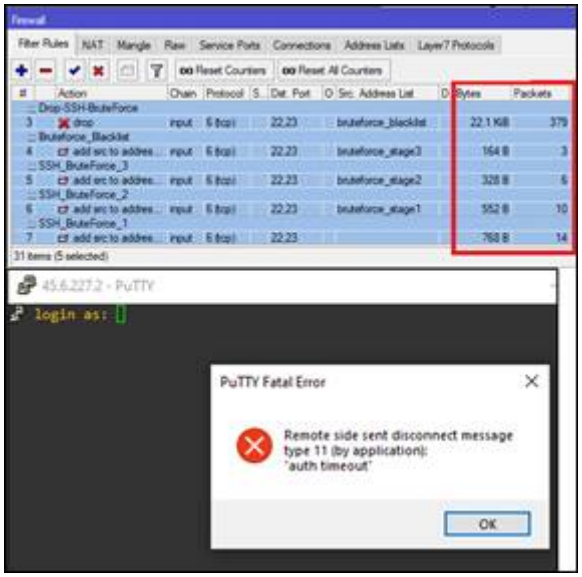

FIGURA 19.
Mitigación ataque fuerza bruta.
Autores.

7) Ataque ICMP Smurf

Para generar el ataque se utiliza la herramienta hping3 de nuestro sistema operativo Kali, para generar un ataque hacia la interfaz Gateway LAN del router como se puede observar en la Figura 20. El ataque genera paquetes ICMP hacia el dispositivo inundando las conexiones y elevando su CPU como se aprecia en la Figura 21. 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.

FIGURA 20.
Ataque ICMP Smurf.
Autores.

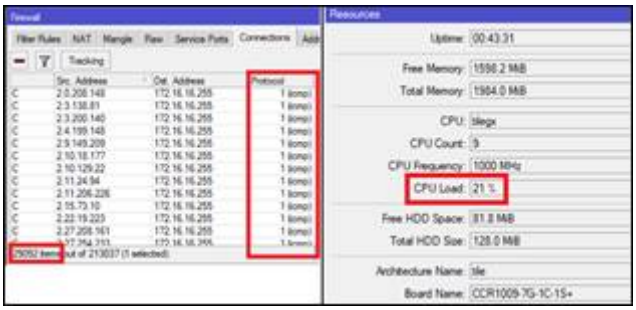

FIGURA 21.
Consumo de CPU Ataque ICMP Smurf.
Autores.

En la Figura 22 se puede apreciar el incremento de Bytes debido a la gran cantidad de paquetes dropeados mediante la regla establecida y al mismo tiempo el consumo del CPU.

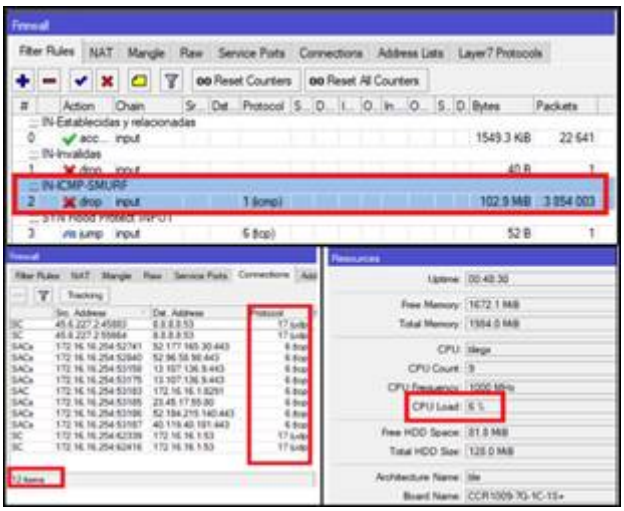

FIGURA 22.
Mitigación Ataque ICMP Smurf.
Autores.

Resultados

A continuación, se muestran los resultados que se obtuvieron de los ataques generados (antes, durante 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 (Management Network Discovery Protocol) se puede evidenciar que las reglas de mitigación en el firewall reducen un 78% del uso excesivo del CPU. En el segundo caso (DHCP Starvation), las reglas implementadas reducen un 13% del uso del CPU, su mitigación se lo realiza en bridge-filter debido a que el ataque es en capa 2.

En el Tercer ataque (Rogue DHCP), no se observa 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 0% su CPU. El cuarto suceso (TCP Syn), su mitigación fue realizada mediante el firewall de RouterOS con el cual se obtuvo una disminución de uso del CPU de un 46%. En el quinto acontecimiento (UDP Flood), se reduce un 48% del uso del CPU, esto gracias a las reglas aplicadas en la sección de Filter Raw de RouterOS.

El sexto ataque (Fuerza bruta), su consumo de CPU no fue muy elevado debido a que el ataque depende de la longitud del diccionario con el que se realice el ataque, para este caso se procedió con un diccionario de 50 palabras, obteniendo una reducción de 3% del consumo del CPU. Por último, en el séptimo suceso (ICMP Smurf), el ataque genera una carga de 21% para el CPU y gracias a los parámetros de mitigación en el firewall, este se reduce un 15% en el uso del CPU.

TABLA 1.
Resumen de resultados obtenidos en la experimentación

	HERRAMIENTAS				MITIGACION				RECURSOS		
Ataque	Nmap	Yersinia	Hping3	Hydra	Interfaz	Firewall Filter	Firewall RAW	Bridge Filter	% CPU Inicial	% CPU Ataque	% CPU Mitigación
Management Network Discovery Protocol		X			X				0%	84 %	6 %
DHCP Starvation		X						X	0%	16 %	3%
Rogue DHCP Server		X			X				0%	0%	0%
TCP Sync	X		X			X			0%	56%	10%
UDP Flood	X		X				X		0%	49%	1%
Fuerza Bruta	X			X		X			0%	5%	2%
ICMP Smurf			X			X			0%	21%	6%

Autores.

Conclusiones

En este trabajo se explotó los ataques dirigidos a dispositivos routers de core MikroTik. Para el análisis de los tipos de ataques se procedió al uso de herramientas para el pentesting de redes de datos, considerando el escaneo y explotación de vulnerabilidades. Los resultados obtenidos facilitaron la implementación de mecanismo de seguridad ante los riesgos de ataques. En todos los casos de experimentación se puede notar una sobrecarga de CPU cuando se ejecuta la vulnerabilidad, pero al implementar la política de seguridad existe una reducción considerable de consumo del microprocesador, esto debido a las reglas específicas aplicadas al firewall de RouterOS, ayuda a tomar las decisiones necesarias de cada paquete del tráfico de red generado.

En trabajos futuros, se podrían analizar otras alternativas de mitigación para los mismos tipos de ataques descritos en este trabajo, debido a que RouterOS está basado en el kernel de Linux, y su firewall permite la creación de distintas reglas o filtros para cubrir los problemas de seguridad.

Referencias Bibliográficas

Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2015). Security in Software Defined Networks: A Survey. IEEE Communications Surveys Tutorials, 17(4), 2317–2346. https://doi.org/10.1109/COMST.2015.2474118

Aldaoud, M., Al-Abri, D., al Maashri, A., & Kausar, F. (2021). DHCP attacking tools: an analysis. Journal of Computer Virology and Hacking Techniques, 17(2), 119–129. https://doi.org/10.1007/s11416-020-00374-8

Assolini Fabio. (2019). Kaspersky registra 45 ataques por segundo en América Latina | Blog oficial de Kaspersky. Kaspersky Daily. https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/

Bartholemy, A., & Chen, W. (2015). An examination of distributed denial of service attacks. IEEE International Conference on Electro Information Technology, 2015-June, 274–279. https://doi.org/10.1109/EIT.2015.7293352

Bogdanoski, M., Suminoski, T., & Risteski, A. (2013). Analysis of the SYN Flood DoS Attack. International Journal of Computer Network and Information Security (IJCNIS), 5(8), 1–11. https://doi.org/10.5815/ijcnis

Braem, B., Bergs, J., Avonts, J., & Blondia, C. (2014). Mapping a community network. 2014 Global Information Infrastructure and Networking Symposium, GIIS 2014. https://doi.org/10.1109/GIIS.2014.6934252

Ceron, J. M., Scholten, C., Pras, A., & Santanna, J. (2020). MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification. Proceedings of IEEE/IFIP Network Operations and Management Symposium 2020: Management in the Age of Softwarization and Artificial Intelligence, NOMS 2020. https://doi.org/10.1109/NOMS47738.2020.9110336

Chauhan, A. S. (2017). Practical network scanning#: capture network vulnerabilities using standard tools such as Nmap and Nessus.

Domínguez, H. M., Maya, E. A., Peluffo, D. H., & Crisanto, C. M. (2016). Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple "Contraseñas", pruebas de concepto con software libre y su remediación. Maskana, 7, 87–95.

Ecucert. (2017). EcuCERT de Arcotel – Centro de Respuesta a Incidentes Informáticos de la ARCOTEL. https://www.ecucert.gob.ec/

Grover, V., & Gagandeep. (2020). An Efficient Brute Force Attack Handling Techniques for Server Virtualization. Social Science Research Network. https://papers.ssrn.com/abstract=3564447

Gunnam, G. R., & Kumar, S. (2017). Do ICMP Security Attacks Have Same Impact on Servers? Journal of Information Security, 8(3), 274–283.

Kadafi, M., & Khusnawi, K. (2015). Analisis Rogue DHCP Packets Menggunakan Wireshark Network Protocol Analyzer. Creative Information Technology Journal, 2(2), 165–180.

López, P. A. (2010). Seguridad informática (1st ed.). Editex. https://books.google.com.ec/books?id=Mgvm3AYIT64C

Mikrotik. (2021). MikroTik Routers and Wireless. https://mikrotik.com/training/about

Mukhtar, H., Salah, K., & Iraqi, Y. (2012). Mitigation of DHCP starvation attack. Computers & Electrical Engineering, 38(5), 1115–1128. https://doi.org/https://doi.org/10.1016/j.compeleceng.2012.06.005

Mursyidah, Husaini, Atthariq, Arhami, M., Hidayat, H. T., Anita, & Ramadhona. (2019). Analysis and implementation of the Port Knocking method using Firewall-based Mikrotik RouterOS. IOP Conference Series: Materials Science and Engineering, 536, 012129. https://doi.org/10.1088/1757-899x/536/1/012129

Omella, Alfredo Andres, Berrueta, & David Barroso. (2017). Yersinia | Penetration Testing Tools. https://tools.kali.org/vulnerability-analysis/yersinia

Sanfilippo, & Salvatore. (2018). hping3 | Penetration Testing Tools. https://tools.kali.org/information-gathering/hping3

Shaikh, A., Pardeshi, B., & Dalvi, F. (2020). Overcoming Threats and Vulnerabilities in DNS. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.3568728

Singh, A., & Juneja, D. (2010). Agent based preventive measure for UDP flood attack in DDoS attacks. International Journal of Engineering Science and Technology, 2(8), 3405–3411.

Sukaridhoto, S., & ST Ph, D. (2014). Buku Jaringan Komputer I. Surabaya: Pens, 2014, 11–12. files/89/Sukaridhoto - Buku Jaringan Komputer I.pdf

Wu, C.-Hwa., & Irwin, J. D. (2016). Introduction to Computer Networks and Cybersecurity. https://www.oreilly.com/library/view/introduction-to-computer/9781466572133/

Notas

[1] Ingeniero en Telecomunicaciones graduado en Escuela Superior Politécnica de Chimborazo, Egresado de la Maestría en Ciberseguridad de la PUCE sede Ambato, Ecuador. E-mail: byron.m.palate.s@pucesa.edu.ec
[2] Ph.D. en Ingeniería en Sistemas e Informática, UNMSM. M.Sc. en Informática Apli- cada, Profesor titular tiempo completo en la Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Riobamba, Ecuador. E-mail: davila@espoch.edu.ec