Prevención y Mitigación de Ataques DDoS Basados en Slowloris en Entornos Virtualizados

Prevention and Mitigation of DDoS Attacks Based on Slowloris in Virtualized Environments

Jorge Nasimba, Andrés Pallango, Kevin Suntaxi, Bryan Yaguarshungo
Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas, 170126, Sangolquí, Ecuador.
{janasimba4, avpallango, kgsuntaxi1, bdyaguarshungo}@espe.edu.ec

Resumen

La protección contra ataques de Denegación de Servicio Distribuido es crucial en el ciberespacio para garantizar la disponibilidad de servicios y preservar la integridad de los sistemas. Este estudio se enfocó en analizar ataques Slowloris para explotar vulnerabilidades en servidores web, utilizando un entorno virtualizado. Se empleó un servidor Ubuntu 23.04, LTS con Apache para alojar un sitio web vulnerable. Además, se llevaron a cabo ataques con dos herramientas diferentes que utilizan el método de Slowloris y luego se implementaron medidas de seguridad para evaluar su efectividad en la mitigación de estos ataques. Los resultados destacan la importancia de adoptar medidas de seguridad proactivas para proteger sistemas y redes contra amenazas cibernéticas mal configurados o que no están protegidos adecuadamente contra este tipo de ataques, lo cual incrementará la resistencia y el nivel de seguridad de la información de las empresas.

Palabras clave: *Ciberseguridad; DDoS; Slowloris; Virtualización; Vulnerabilidades.*

Abstract

Protection against Distributed Denial of Service attacks is crucial in cyberspace to ensure service availability and preserve systems' integrity. This study analyzed Slowloris attacks to exploit vulnerabilities in web servers by using a virtualized environment. An Ubuntu 24.04, LTS server with Apache to host a vulnerable website was used. Additionally, we conducted attacks with a pair of tools using the Slowloris method and after implemented security measures to evaluate their effectiveness in mitigating these attacks were implemented. The results highlight the importance of adopting proactive security measures to protect systems and networks, which are poorly configured or not adequately protected against cyber threats, or these types of attacks, which will increase companies' resistance and the level of information security.

Keywords: *Cybersecurity; DDoS; Slowloris; Virtualization; Vulnerabilities.*

Fecha de Recepción: 30/08/2023 - Aceptado: 15/09/2023 - Publicado: 31/12/2023
ISSN: 2477-9253 – DOI: http://dx.doi.org/10.24133/RCSD.VOL08.N04.2023.05

I. Introducción

Los ataques a la ciberseguridad se han convertido en una preocupación constante. Entre las diversas amenazas que existen, los Ataques de Denegación de Servicio Distribuido (DDoS) representan un desafío significativo. Este estudio se centra en la aplicación de un método y herramienta a la vez conocido como Slowloris, que tiene como objetivo la denegación de solicitudes y que no requiere de millones de paquetes infectados para saturar el servidor objetivo (Sabri et al., 2021).

El ataque Slowloris es una amenaza de ciberseguridad que ha capturado la atención de la comunidad científica y la industria debido a su capacidad para interrumpir los servicios al inundar un servidor con solicitudes HTTP incompletas. Este ataque mantiene abiertas las conexiones durante el mayor tiempo posible. A pesar de los esfuerzos para mitigar este tipo de ataques, la solución completa aún no se ha encontrado, como se evidencia en las publicaciones recientes revisadas en el estado del arte (Shorey et al., 2018).

Dentro de este contexto, Aversari y Moreira (2017) exploran el potencial de los ataques DDoS, específicamente el ataque Slowloris, cuando se ejecutan desde dispositivos móviles Android. Imaisum & Martins H. (2013) se enfocan en los ataques DoS utilizando Slowloris y proponen estrategias de mitigación basadas en la identificación de patrones de ataque y la implementación de medidas de seguridad. Oktivasari et al. (2022) proponen la implementación de herramientas de filtrado de tablas de IP basadas en firewall para mitigar los ataques de Slowloris. De igual manera, el estudio de Sabri & Hazzim (2021) explora la simulación y mitigación de ataques DoS contra sitios web empleando Slowloris con un enfoque cohesivo para agotar las conexiones del servidor. Asimismo, De la Cruz (2022) demuestra que el servidor Apache Web Server en su versión 1.x y 2.x permite a los atacantes remotos causar una denegación de servicio a través de peticiones HTTP parciales basado en Slowloris. Lo anterior demuestra que este problema sigue latente y que aún no se logran soluciones definitivas.

Este estudio tiene como objetivo analizar en profundidad el ataque DDoS de tipo Slowloris, con el fin de entender su funcionamiento, identificar sus debilidades y proponer posibles soluciones. Para lograrlo, se realizó un análisis exhaustivo de la literatura existente, seguido de una serie de experimentos prácticos utilizando diferentes técnicas y herramientas de seguridad cibernética.

Como resultado de esta investigación, se identificaron varias características únicas del ataque Slowloris que podrían ser explotadas para su detección y mitigación. Además, se propusieron varias estrategias para proteger los servidores contra este tipo de ataques.

La principal aportación de este estudio radica en la propuesta de una forma de prevención de los ataques DDoS de tipo Slowloris y de un mecanismo para mitigarlo basado en la explotación de características únicas de este ataque identificadas durante nuestra investigación. Esta contribución representa un avance significativo en el campo de la ciberseguridad y ofrece una nueva línea de defensa contra los ataques Slowloris. Se espera que el estudio proporcione una comprensión más profunda del ataque DDoS de tipo Slowloris y sirva como base para futuras investigaciones en este campo.

Este artículo está estructurado de la siguiente manera: la sección 2 proporciona una revisión de los ataques DDoS y la herramienta Slowloris en particular. Además, describe los Materiales y métodos utilizados en el estudio. La sección 3 presenta y discute los resultados obtenidos. Finalmente, la sección 4 concluye el artículo y sugiere direcciones para futuras investigaciones.

II. Materiales y Métodos

Esta sección presenta el método empleado para abordar el desafío de analizar ataques DDoS hacia un servidor Ubuntu que alojaba un sitio web vulnerable utilizando un entorno virtual controlado. Se empleó como tipo de ataque Slowloris que es un tipo de ataque de denegación de servicio distribuido, que sirve para saturar un equipo, servidor web, base de datos o API abriendo y manteniendo conexiones TCP simultáneas a un FQDN de destino y generando solicitudes HTTP o conexiones HTTP de reducida frecuencia o poco volumen por sesión conectada.

El propósito fue realizar este ataque, observar que daños provocó al servidor atacado y recolectar datos para analizarlos. Posteriormente, se aplicaron medidas de seguridad para contrarrestar estos ataques y se evaluó la efectividad que tendrían contra estos ataques. Esta descripción minuciosa es esencial, ya que la base del método científico radica en la capacidad de reproducir resultados; así, se proveen los detalles necesarios para que otros investigadores repliquen los experimentos con precisión.

En los siguientes párrafos de este artículo, se describirán los trabajos relacionados que sirvieron de insumo en este estudio. Así mismo, se explorarán cada una de las etapas del experimento, proporcionando ejemplos específicos y consideraciones clave en el contexto de ataques de tipo Slowloris a un servidor de Ubuntu con Apache que se alojó en una web vulnerable y otros recursos esenciales.

2.1. Trabajos Relacionados

El estudio propuesto por S. Black & Y. Kim (2022) indica cómo los ataques de DDoS se han convertido en un área de investigación crucial debido a su capacidad para interrumpir los servicios web. Dentro de estos ataques, los dirigidos a la capa de aplicación presentan desafíos únicos, ya que suelen ser más difíciles de detectar al aparecer legítimos en capas inferiores y aprovechar funcionalidades comunes de las aplicaciones o debilidades del protocolo HTTP. Además, exploran diversos tipos de ataques a la capa de aplicación, así como medidas preventivas y de detección, centrándose especialmente en los ataques de inundación HTTP.

Torres (2021) menciona que los ataques Dos o DDoS, consisten en enviar un número elevado de peticiones a una dirección IP o dominio específico, buscando que el servidor objeto del ataque, o incluso todo un sistema informático, sea incapaz de gestionar todas las peticiones, haciendo que el tráfico recibido sea difícil de distinguir del tráfico normal comprometiendo en gran manera la disponibilidad y capacidad del sitio, forzando la detención o colapso de todos los servicios. Por lo general, para llevar a cabo este tipo de ataques se necesita de “botnet” o “red zombie”, la cual consiste en una red compuesta por miles de computadores, dispositivos IoT o cualquier otro dispositivo conectado a Internet, infectados previamente con un tipo de malware, que permite controlarlos de forma remota.

De la Cruz R. (2022) demostró que el servidor HTTP Apache Web en su versión 1.x y 2.x permitía a los atacantes remotos causar una denegación de servicio a través de peticiones HTTP parciales. Este tipo de ataque se puede realizar por un Slowloris y el nivel de impacto podría afectar a la disponibilidad del sistema.

De igual manera en el trabajo propuesto por Sabri, Ismail & Hazzim (2021) los autores muestran como los ataques DoS siguen siendo pertinentes en el ámbito de la ciberseguridad. Recalcan como los ataques DoS, son populares por su simplicidad y efectividad. En su estudio, exploran la simulación y mitigación de ataques DoS contra sitios web mediante un enfoque cohesivo para agotar las conexiones del servidor.

Con la creciente dependencia de la tecnología de red, se vuelve trascendental garantizar el buen funcionamiento de los servidores web. Los ataques DDoS utilizando Slowloris representan un riesgo al apuntar a

la disponibilidad del servicio. Para abordar estos ataques de forma rápida y eficaz, Oktivasari et al. (2022) proponen la implementación de herramientas de filtrado de tablas de IP basadas en firewall. A través de investigaciones, pruebas y análisis comparativos, demuestran la eficacia de este enfoque para mitigar este tipo de ataques.

Hernández (2018) presenta un algoritmo que permite tener un mejor control de tráfico a la red, lo que reduce el consumo de recursos de los routers. Esto se logra mediante la creación de una cola que permite la transferencia de paquetes con tokens disponibles, que se impone en un límite de tasa de transferencia aceptable.

En el estudio realizado por Imaisum, R. Martins H., (2013) se analiza la creciente demanda mundial por interconectividad de equipos y dispositivos en red. Este estudio propone un análisis de las anomalías en redes computacionales y sus efectos, sugiriendo posibles soluciones para su identificación y prevención con medidas de seguridad. Los autores se centran en los ataques de DOS, en particular el ataque Slowloris, y proponen estrategias de mitigación basadas en la identificación de patrones de ataque y la implementación de medidas de seguridad.

En el trabajo de Aversari & Moreira (2017) se explora el potencial de los ataques DDoS, específicamente el ataque Slowloris, cuando se ejecutan desde dispositivos móviles Android. Este estudio es particularmente relevante ya que adapta el ataque Slowloris, que generalmente se ejecuta desde desktops, para que funcione en dispositivos móviles. Los resultados del estudio mostraron que el potencial dañino de la versión móvil del ataque Slowloris es tan alto como el de la versión de escritorio.

2.2. Plataformas, herramientas y aplicaciones de software

En el proceso de llevar a cabo el ataque Slowloris en un entorno virtual de red controlado, se requirieron una serie de herramientas de software que a continuación se describen brevemente:

- Virtual Box: VirtualBox es una plataforma de virtualización de código abierto desarrollado por Oracle. Permite la gestión de máquinas virtuales en un entorno de host. Eso significa que se pueden crear, remover, copiar, clonar, configurar máquinas virtuales, con diferentes sistemas operativos simultáneamente en una única máquina física.

- Ubuntu Server LTS: Ubuntu Server LTS (Long Term Support) es una versión de Ubuntu diseñada específicamente para servidores. Ofrece soporte a largo plazo, actualizaciones de seguridad y estabilidad. Está optimizado para entornos de servidor y es utilizado ampliamente en servidores web, bases de datos y otras aplicaciones de servidor.

- Ubuntu Desktop LTS: Ubuntu Desktop LTS es una versión de Ubuntu diseñada para su uso en estaciones de trabajo y computadoras de escritorio. Proporciona una interfaz de usuario gráfica y está destinado a entornos de usuario final.

- Metasploit framework: Metasploit es un marco de código abierto para el desarrollo y ejecución de exploits. Proporciona una plataforma para realizar pruebas de penetración y evaluación de vulnerabilidades. Metasploit incluye módulos específicos para diversos tipos de ataques, lo que lo convierte en una herramienta versátil para la evaluación de seguridad.

- Wireshark: Wireshark es un analizador de protocolos de red de código abierto. Permite capturar y analizar el tráfico de red en tiempo real. Wireshark es ampliamente utilizado para el análisis de paquetes y la identificación de patrones de tráfico.

- Perl Slowloris: Perl Slowloris es una implementación del ataque Slowloris en el lenguaje de programación Perl. Slowloris es un tipo de ataque de denegación de servicio diseñado para agotar las conexiones disponibles en un servidor web al mantener conexiones abiertas con el servidor y enviar datos a un ritmo lento.

- Apache: Apache HTTP Server, comúnmente conocido como Apache, es un servidor web de código abierto y uno de los servidores web más utilizados en el mundo. Proporciona servicios web mediante el protocolo HTTP y es conocido por su estabilidad y rendimiento.

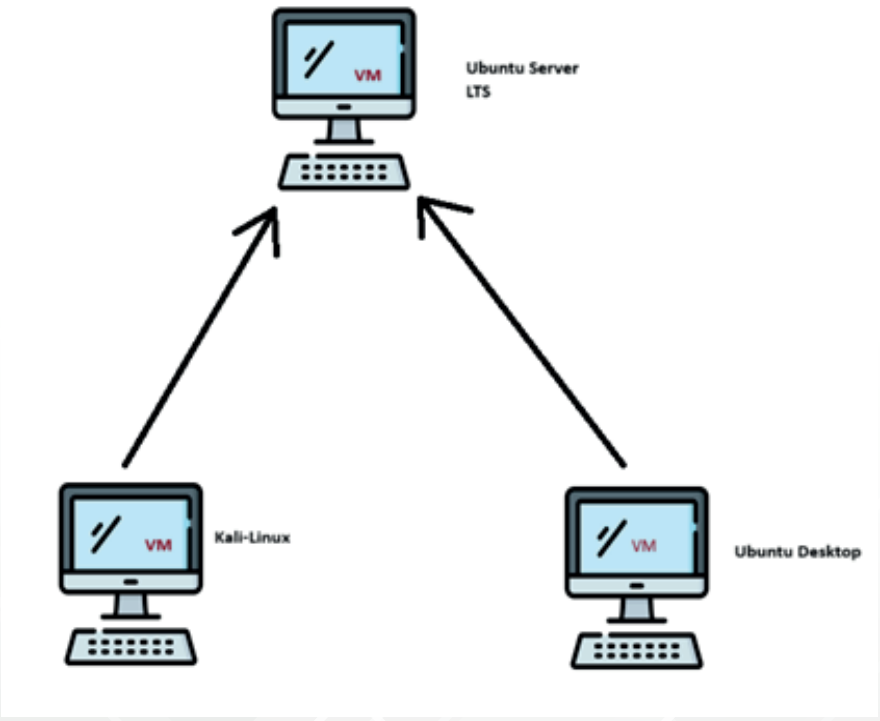
2.3. Métodos

En este apartado se describe el procedimiento metodológico que combina el uso de la plataforma VirtualBox para la virtualización de sistemas operativos y los mecanismos de networking que permiten diseñar, configurar, probar y analizar conexiones entre diferentes equipos. Además, permiten configurar y ejecutar los ataques cibernéticos de manera controlada y segura, los mismos que pueden ser replicados en entornos del mundo real. A continuación se describen brevemente los pasos respectivos:

2.3.1. Paso 1: Diseño del escenario de máquinas virtuales

En este paso se diseñó y configuró el escenario de conectividad de las máquinas virtuales, incluyendo las herramientas que se usarán para realizar el ataque y la mitigación del mismo. La figura 1 muestra cómo se conectan dos máquinas virtuales con Kali Linux y Ubuntu Desktop LTS respectivamente las cuales apuntan al servidor virtualizado que tiene instalado Ubuntu Server LTS que será el equipo víctima. Las direcciones IP del escenario virtual forman parte de una Red NAT configurada por VirtualBox.

Figura 1: *Diseño del escenario con VM*



2.3.2. Paso 2: Configuración de Dispositivos

En este paso, se procede a cargar las imágenes de sistemas operativos virtuales en VirtualBox. Luego, se configuran los dispositivos para reflejar su funcionalidad en la Red NAT. Luego se instalan en cada máquina las herramientas necesarias para llevar a cabo el ataque.

2.3.3. Paso 3: Conexión de las máquinas virtuales

Para verificar que están conectadas entre sí las máquinas y el servidor virtual, se comprobó la conectividad con el fin de que puedan intercambiar datos, servicios o aplicaciones entre ellas.

2.3.4. Paso 4: Instalación de las herramientas

Se realizó las instalaciones de las herramientas para analizar el tráfico de red y el ataque en la VM con Kali-Linux. En la VM con Ubuntu Server se instaló y configuró Apache Web Server. En la VM con Ubuntu Desktop se instaló Wireshark, que como se señaló es una herramienta para análisis de tráfico y protocolos.

2.3.5 Paso 5: Pruebas y Simulación

Se llevaron a cabo pruebas exhaustivas y simulaciones para evaluar el comportamiento del ataque. Esto incluyó realizar pruebas de estrés a la dirección IP del servidor víctima. Paralelamente, en tiempo real, se realizó el análisis de tráfico mediante Wireshark, que además nos otorgó el tiempo de respuesta del servidor y su status, la cantidad de paquetes y que tan efectiva fue la medida para repeler el ataque, que en este caso fue un script programado en BASH.

III. Evaluación de Resultados y Discusión

3.1. Pruebas

Los resultados revelaron información valiosa sobre la eficacia de las medidas de seguridad implementadas en respuesta a los ataques DDoS del tipo Slowloris en un entorno virtualizado controlado. Se llevaron a cabo análisis estadísticos para destacar los cambios significativos en la mitigación de los ataques mediante el uso de dos técnicas distintas de Slowloris. Los datos recopilados indicaron una mejora sustancial en la resistencia del sistema después de la implementación de las medidas de seguridad establecidas.

Se observó una reducción notable en el tiempo de respuesta y en la tasa de éxito de los ataques, evidenciando la eficacia de las estrategias adoptadas. Los resultados también resaltaron la importancia de la configuración específica del servidor Ubuntu con Apache y su papel en la protección contra amenazas cibernéticas. A continuación, se explican las pruebas realizadas durante el estudio de ataques Slowloris.

3.1.1. Selección de Pruebas

Se aplicaron pruebas estadísticas de comparación de los registros del DDoS, tanto antes como después de la implementación de las medidas de seguridad, focalizándose en múltiples métricas para evaluar la eficacia de las estrategias implementadas frente a los ataques DDoS tipo Slowloris. Además, del tiempo de respuesta del servidor y la tasa de éxito de los ataques, se consideraron otras variables relevantes como la cantidad total de ataques, la duración de los mismos y la capacidad de respuesta del sistema ante múltiples instancias simultáneas de ataques.

3.1.2. Niveles de Medición de Variables

Además de las métricas previamente mencionadas, se cuantificaron otras variables relevantes, como la cantidad de ataques simultáneos y la duración de los mismos. Esta ampliación permitió una evaluación más integral de la capacidad de la solución para resistir diferentes escenarios de ataques DDoS.

El enfoque cuantitativo se extendió a una medición más detallada de la variabilidad en la respuesta del sistema ante distintas configuraciones de ataques. Este enfoque permitió una evaluación más precisa de los cambios experimentados después de la implementación de las medidas de seguridad.

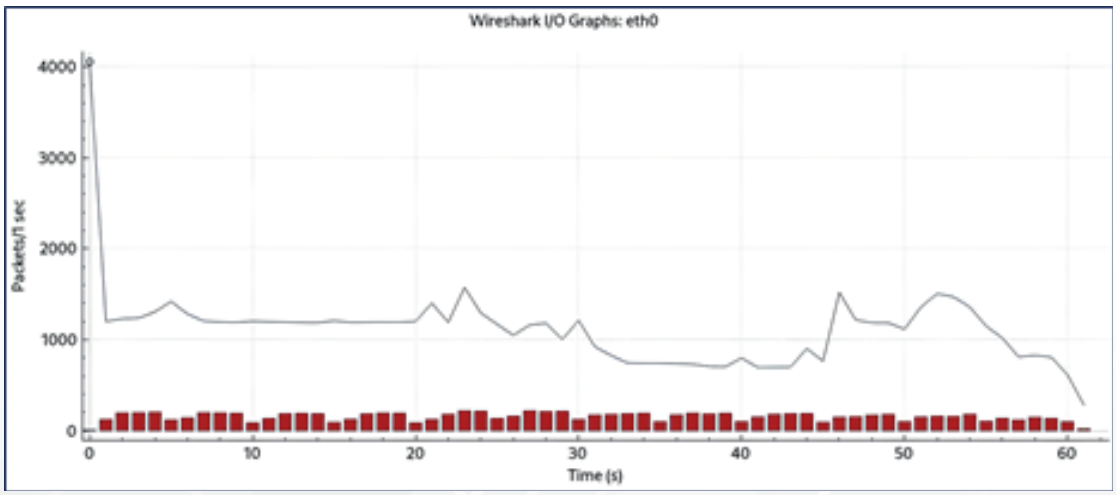
3.2. Análisis de Datos

Durante la fase de análisis de los ataques DDoS tipo Slowloris contra el servidor Apache en Ubuntu, se llevó a cabo un estudio de los patrones de ataque utilizando una combinación de herramientas, principalmente Wireshark y las plataformas de ataque Perl Slowloris y Metasploit. Wireshark para el análisis de tráfico y protocolos. Por otro lado, las herramientas Perl Slowloris y Metasploit fueron utilizadas para generar los ataques, permitiendo variar las características de los mismos, como la duración y el volumen de solicitudes, para simular diferentes niveles de agresión. Los datos recogidos a través de Wireshark sobre estos ataques permitieron evaluar la capacidad de respuesta del servidor ante estas amenazas y medir la efectividad de las medidas de seguridad implementadas posteriormente.

La Figura 2 presenta el tráfico de red en función del tiempo, datos que se obtuvieron utilizando la herramienta Perl Slowloris. En el eje de las abscisas (X), se encuentra la variable tiempo expresada en segundos. Este eje muestra la progresión temporal a lo largo del estudio. La altura de la curva o línea en el gráfico indica la cantidad de paquetes transmitidos en cada momento, ofreciendo una visión clara de cómo varía la actividad de la red a lo largo del tiempo.

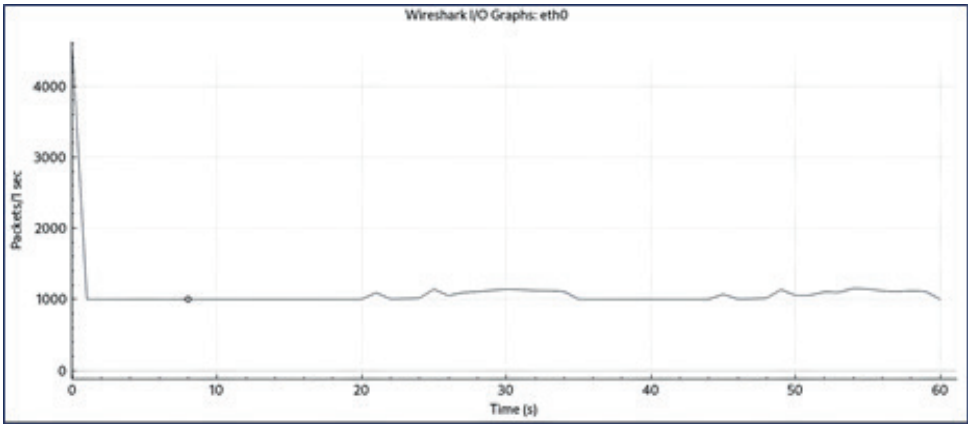
Así mismo, en la Figura 2, la pendiente de la curva indica patrones de tráfico, como picos de actividad o momentos de menor actividad, proporcionando información valiosa sobre la dinámica de la red durante el período analizado. Esta representación gráfica facilita la identificación de tendencias y patrones en la transmisión de paquetes a lo largo del tiempo, brindando una visión visualmente informativa de la actividad de la red.

Figura 2: *Tráfico producido por Perl Slowloris*



La Figura 3 presenta el tiempo entre llegada de paquetes medidos en segundos y la cantidad de paquetes generados por el ataque Slowloris. En este caso, fueron generados por Metasploit Framework que es un marco de trabajo útil en las pruebas de penetración y análisis de vulnerabilidades.

Figura 3: *Tráfico producido por Metasploit Framework*

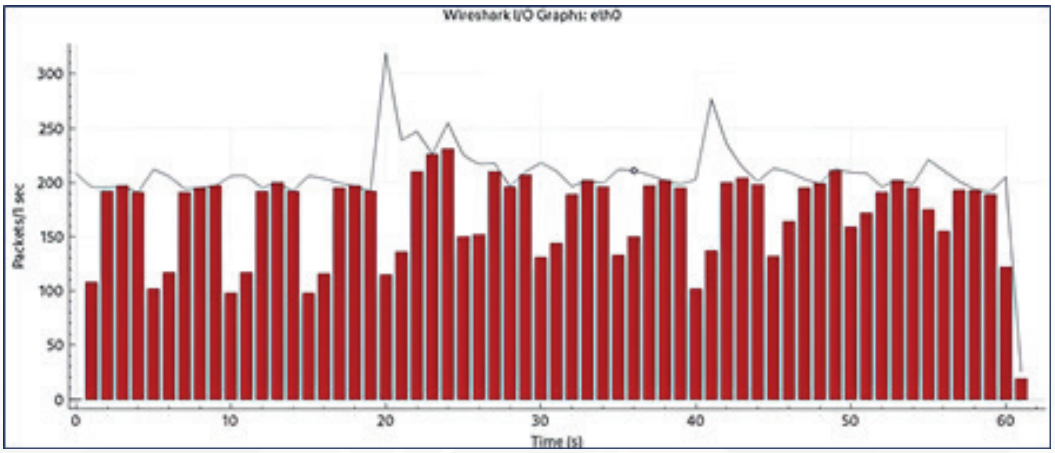


A diferencia de Figura 2, en este caso se puede observar una menor cantidad de picos o variaciones en los resultados, además de la ausencia total de errores TCP, lo que significa que un ataque por este medio resulta más eficiente para el atacante y por ende es más perjudicial para la víctima.

En relación a las medidas de seguridad en el servidor, la aplicación de la solución resultó en una disminución significativa en el número de paquetes transmitidos. Esto señala que la solución de mitigación es potente, más no completa.

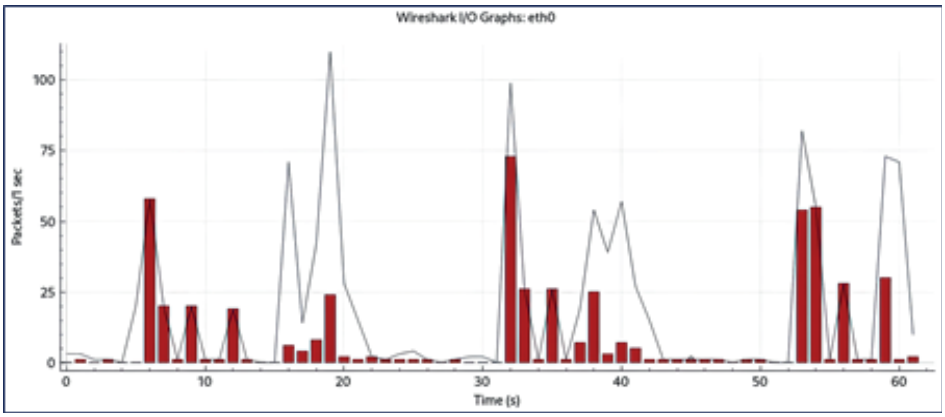
Para este propósito se utilizó Perl Slowloris con idénticas configuraciones, implementando medidas de seguridad en el servidor, se obtuvo los resultados que se muestran en la Figura 4. Como se puede observar, la cantidad de paquetes maliciosos se ha reducido significativamente. Sin embargo, todavía continúa con la presencia de varios paquetes y errores TCP que pueden interferir con el correcto funcionamiento en el servidor.

Figura 4: *Perl Slowloris con medidas de seguridad*



De la misma manera, la Figura 5, muestra los resultados al implementar medidas de seguridad en el servidor víctima. Al realizar el análisis aplicando Metasploit Framework en contra de la seguridad en Servidor se puede apreciar que la primera vez eran estables y no presentaban errores TCP, ahora tienen gran variación, además de que en algunos lapsos de tiempo son nulos.

Figura 5: *Metasploit Framework con medidas de seguridad*



Del análisis y comparación entre los ataques ejecutados a entornos con y sin seguridad, se recopiló información valiosa sobre el rendimiento y la eficacia de la red simulada. La Tabla 1 resume datos que permiten una evaluación del comportamiento de la red y son esenciales para la optimización y el análisis de su rendimiento.

Tabla 1: *Comparación de entornos seguros y no seguros*

Categoría	Tiempo (s)	Total de paquetes Tx	Total de paquetes Rx	Tasa de Éxito de Paquetes filtrados
Perl Slowloris sin Seguridad	60	44855	44855	-
Metasploit sin Seguridad	60	61408	61408	-
Perl Slowloris con Seguridad	60	43857	1938	82.73%
Metasploit sin Seguridad	60	62451	404	95.80%

3.3. Discusión

En este estudio, se llevaron a cabo análisis exhaustivos de ataques DDoS empleando Slowloris en un entorno virtualizado, utilizando herramientas como Perl Slowloris y Metasploit Framework. La implementación de medidas de seguridad posteriores permitió evaluar su efectividad en la detección y mitigación de estos ataques.

Los resultados tienen implicaciones teóricas y prácticas significativas. Teóricamente, demuestran la capacidad de las medidas de seguridad para mitigar de manera efectiva los ataques DDoS tipo Slowloris, proporcionando una mayor comprensión de la resistencia del sistema ante estas amenazas. Desde una perspectiva práctica, los hallazgos respaldan la importancia de adoptar enfoques proactivos para proteger entornos virtuales contra ataques cibernéticos, especialmente aquellos dirigidos a la disponibilidad de servicios.

Al realizar una comparación de herramientas de Ataque, los resultados revelaron diferencias significativas entre Perl Slowloris y Metasploit en términos de la cantidad de paquetes generados y la persistencia del ataque. Metasploit demostró ser más efectivo en la generación de tráfico malicioso. Esta distinción resalta la importancia de considerar diversas herramientas de ataque al evaluar la seguridad de un sistema.

En lo que concierne al impacto de implementar medidas de seguridad, se observó una reducción significativa en el número de paquetes generados por ambas herramientas. La tasa de éxito de los ataques disminuyó significativamente, indicando una mayor resistencia del sistema frente estos ataques.

IV. Conclusiones y Trabajo Futuro

Este estudio ha demostrado la eficacia de las estrategias de seguridad aplicadas para contrarrestar los ataques DDoS tipo Slowloris en ambientes virtualizados. La implementación de estas estrategias resultó en una notable disminución en la cantidad de paquetes generados y una reducción significativa en la efectividad de los ataques, lo cual muestra un fortalecimiento en la capacidad del servidor víctima para resistir estos desafíos. De igual manera, la comparación entre Perl Slowloris y el Metasploit Framework destacó diferencias significativas en su capacidad para generar tráfico dañino. Metasploit se demostró más capaz, produciendo un volumen más alto de tráfico malintencionado antes de que se aplicaran las medidas de seguridad. Los resultados resaltan la relevancia de adoptar medidas proactivas en la seguridad de entornos virtuales. La anticipación a las amenazas y la preparación del sistema para enfrentar ataques determinados, como el Slowloris, son esenciales para preservar la integridad y la disponibilidad de los servicios en línea. Aunque esta investigación se llevó a cabo en un ambiente virtualizado controlado, es fundamental aplicar y evaluar las estrategias de seguridad en entornos de producción reales en el futuro. Esto ofrecerá perspectivas valiosas sobre su efectividad y los desafíos potenciales en escenarios cotidianos. Además, la exploración y evaluación de una variedad más amplia de soluciones de seguridad, incluyendo sistemas de prevención de intrusiones (IPS), firewalls avanzados, y soluciones basadas en la nube, podrían revelar métodos más eficaces o complementarios para la mitigación de ataques DDoS.

Como trabajo futuro se planea ampliar el alcance de la investigación para incluir una gama más extensa de herramientas y técnicas de ataque DDoS, más allá de aquellas que permiten una explotación de vulnerabilidades, lo cual enriquecerá el entendimiento sobre las vulnerabilidades y las estrategias de defensa más robustas. Así mismo, se planea desarrollar y probar sistemas automatizados que puedan detectar y responder a ataques DDoS en tiempo real para incrementar la capacidad de un sistema para resistir estos ataques sin intervención humana directa, ofreciendo una capa adicional de seguridad que es vital en el panorama de amenazas en constante evolución.

Referencias

Aronow, D., & Karas, P. (2017, 25 de octubre). Slowloris: Un ataque DDoS HTTP de bajo y lento. *Imperva*. https://www.imperva.com/learn/ddos/slowloris/

Black, S., & Kim, Y. (2022). An Overview on Detection and Prevention of Application Layer DDoS Attacks. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 791-800). Las Vegas, NV, USA. doi:10.1109/CCWC54503.2022.9720741

De La Cruz Rose, Hernandez Oscar. (2022) Prueba de Pentesting para detectar las Vulnerabilidades de Seguridad en la Infraestructura de Red en el CIP CD Lambayaque.

Herranz Andre, Lorenzo Borja, Ruis Guillermo. (2018) Adaptacion y calibrado de algoritmos de predicción para la identificación de ataquesDDoS en redes de quinta generación. Tesis (Obtención de título de ingeniero de sistemas). Madrid: Universidad Complutense de Madrid, 2018. 129pp

Mejía Escobar, A. Caso de estudio para el análisis de Vulnerabilidad y propuesta de aseguramiento de la seguridad de la información en la infraestructura tecnológica de la Empresa Nostradamus SAS.

Oktivasari, P., Zain, A. R., Agustin, M., Kurniawan, A., Murad, F. a., & Anshor, M. f. (2022). Analysis of Effectiveness of Iptables on Web Server from Slowloris Attack. In 2022 5th International Conference of Computer and Informatics Engineering (IC2IE) (pp. 215-219). Jakarta, Indonesia. doi:10.1109/IC2IE56416.2022.9970143 (S/f). Cloudflare.com. Recuperado el 10 de marzo de 2024, de: https://www.cloudflare.com/es-es/learning/ddos/ddos-attack-tools/slowloris/

OWASP. (2023, 23 de enero). Slowloris. OWASP. https://owasp.org/www-pdf-archive/Layer_7_DDOS.pdf

Ribeiro, V., & Papadimitriou, S. (2014). Ataques DDoS de baja tasa: el caso de Slowloris. I*EEE Security & Privacy,* 12(2), 20-28. https://ieeexplore.ieee.org/document/6691028.

Sabri, S., Ismail, N., & Hazzim, A. (2021, febrero). Slowloris DoS Attack Based Simulation. IOP Conference Series: Materials Science and Engineering, 1062(1), 012029. doi:10.1088/1757-899X/1062/1/012029

Sabri, S., Ismail, N., & Hazzim, A. (2021, February). Slowloris DoS attack based simulation. In IOP Conference series: materials science and engineering (Vol. 1062, No. 1, p. 012029). IOP Publishing.

Shorey, T., Subbaiah, D., Goyal, A., Sakxena, A., & Mishra, A. K. (2018). Performance Comparison and Analysis of Slowloris, GoldenEye and Xerxes DDoS Attack Tools. En 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE.

Torres Castillo, K. C. Diseño del sistema de seguridad basado en el análisis de vulnerabilidades identificadas en la Empresa Nostradamus SAS.

Wolf, G. (2017). Tipos de ataque. https://ru.iiec.unam.mx/4047/