# Emulación de Ataques de Denegación de Servicios mediante una Topología de Red LAN en GNS3

# Emulation of Denial of Service Attacks Using a LAN Topology in GNS3

**Luis Ramón[1], Roberto Pallo[1], Esteban Gracia[1], Valery Naranjo[2]**
[1] Universidad de las Fuerzas Armadas - ESPE / Departamento de Ciencias de la Computación / {ldramon, rcpallo, exgracia}@espe.edu.ec
2 Grupo Radical / Área de I+D+i / valery.naranjo@gruporadical.com

## Resumen

La seguridad de las redes de área local (LAN) es una prioridad para los profesionales de TI con el fin de mitigar amenazas globales como el delito digital, la intrusión y los ataques. Este artículo se centra en la evaluación de ataques comunes como el DoS y el DDoS utilizando el software GNS3 para comprender cómo funcionan estos ataques y evaluar su impacto en una red LAN. Los sistemas de detección de intrusiones son herramientas de seguridad vitales que detectan posibles ataques en la infraestructura interna de una empresa. La capa de enlace presenta vulnerabilidades significativas, ya que la mayoría de los ataques tienen como objetivo la interceptación o manipulación de tramas de información con fines maliciosos. La herramienta "dos_attack" puede interrumpir rápidamente la red o negar servicios, lo que hace imposible establecer conexiones, mientras que se utilizó "Kali Linux" para capturar el tráfico de la red. Además, se incluye un recuadro que muestra cómo cada ataque actúa y perjudica a los usuarios, así como también se explican las medidas básicas que se deben tomar para garantizar la seguridad de la red.

**Palabras Claves:** *Ataques cibernéticos, Ataques de Denegación de Servicio, DoS, DDoS, dos_attack tool.*

## Abstract

IT professionals prioritize local area network (LAN) security to mitigate global threats such as digital crime, intrusion, and attacks. The current study evaluates common attacks such as DoS and DDoS using GNS3 software to understand how they work and assess their impact on a LAN. Intrusion detection systems are vital security tools that detect potential attacks on a company's internal infrastructure. The link layer presents significant vulnerabilities, as most attacks aim to intercept or manipulate information frames for malicious purposes. The "dos_attack" tool can quickly disrupt the network or deny services, making it impossible to establish connections, while "Kali Linux" was used to capture network traffic. In addition, a box indicating how each attack acts and harms users is included, as well as explaining the basic steps to ensure network security.

**Keywords:** *Cyber-attacks, dos_attack, DoS, DDoS.*

Fecha de Recepción: 15/3/2023 - Aceptado: 20/3/2023 – Publicado: 31/3/2023
ISSN: 2477-9253 – DOI: http://dx.doi.org/10.24133/RCSD.VOL08.N01.2023.04

# I. Introducción

GNS3 es un software de emulación de redes de computadoras que puede ayudar a prepararse para los exámenes de certificación como Cisco CCNA. Además, lo ayuda a probar y verificar las implementaciones del mundo real, tales como las pruebas de niveles de seguridad frente a ataques reales a redes IP. Jeremy Grossman, el desarrollador original de GNS3, creó originalmente el software para ayudarlo a estudiar para sus certificaciones CCNP. Debido a ese trabajo original, hoy puede utilizarlo para implementar mecanismos de seguridad, para diseñar seguridad perimetral sin costo alguno (Galaxy Technologies, 2023).

La seguridad en las redes de área local (LAN) es una de las principales prioridades que los profesionales informáticos tratan de controlar y mitigar ante las amenazas globales de la información, las cuales comprenden actividades como delitos dentro del mundo digital y todos ellos son orientados y aplicados a la información que se encuentra almacenada en servidores y a la información digital que circula por las redes (Fuertes et al., 2022). Generalmente existen muchas amenazas a las cuales está expuesta la información y comunicaciones digitales, las cuales se pueden agrupar en cinco criterios o directrices generales, dentro de las cuales se encuentra cualquier técnica de intrusión, delito informático o ataque usado por los delincuentes informáticos para llevar a la práctica un ataque. Las cinco directrices de las amenazas a la información son: creación de información, modificación de información, intercepción de información, interrupción de la información y borrado de información (Fuertes, 2022).

En relación con las diversas amenazas existentes, se han implementado mecanismos de seguridad que hacen hincapié en la prevención, detección y recuperación, empleando múltiples tecnologías en aras de resguardar y proteger la información ante posibles ataques (Reyes et al., 2022). La presente investigación se enfoca en la evaluación de ataques DDoS donde su principal objetivo es denegar servicios como TCP, ICMP y UDP a usuarios finales o propietarios.

Entre las principales contribuciones de la presente investigación se hace énfasis en:

- La evaluación de los ataques de denegación de servicio, a fin de analizar y comprender el impacto que causan en una red LAN;
- Facilitar el aprendizaje y la adquisición de conocimiento mediante ataques simulados en con el software GNS3.

El resto del artículo se encuentra organizado de la siguiente manera: En el Numeral II, se explica los fundamentos y teorías de este estudio. En el Numeral III, se describe el proceso metodológico que incluye la configuración del experimento. En el Numeral IV, se muestra la evaluación de resultados. Finalmente, en el Numeral V, se listan las conclusiones y trabajo futuro.

# II. Estado de Arte

### 2.1. Sistema de Detección de Intrusos

Los sistemas de detección de intrusos también llamados IDS son herramientas de seguridad cuya función principal es detectar posibles ataques en las infraestructuras internas de una empresa. Algunos de estos IDS también analizan la información y la recolectan para poder generar estadísticas del tipo de vulnerabilidades que más se suscitan o los posibles fallos que se pueden hallar al momento de desarrollar un proyecto de red

interna llamada en adelante LAN. Existen IDS de carácter Open Source o de código libre cuya función es la misma que la de pago con la única diferencia que llega a detectar vulnerabilidades en tiempo real por el carácter de código abierto que permite actualizaciones permanentes.

### 2.2. Capa de Enlace de Datos del Modelo OSI

La capa de Enlace o capa dos del Modelo OSI, encargada de la transferencia correcta y precisa de la información, es la que más problemas de vulnerabilidad presenta debido que la mayoría de ataques se dirigen a capturar o vulnerar los tramas o formatos de información que se envían por los dispositivos de conectividad (Switches). Teniendo en cuenta que este nivel sirve como canal de comunicación entre las demás capas es preciso mitigar los ataques a la infraestructura LAN de la capa 2 (Bastidas, 2023).

### 2.3. Ataques informáticos de capa de 2

Estos tipos de ataques tienen la finalidad de vulnerar los dispositivos que trabajan en la capa de Enlace de datos. Estos ataques buscan aprovechar características específicas de esta capa para interrumpir la comunicación o causar daño en la red.  A continuación, se enumeran los ataques más utilizados para esta capa:

- Ataque distribuido también conocido como DDoS (Distributed Denial of Service), es un tipo de ataque informático en el que se utiliza una red de múltiples dispositivos comprometidos para enviar una gran cantidad de tráfico malicioso a un objetivo específico. El objetivo principal de un ataque DDoS es sobrecargar los recursos del sistema objetivo, como ancho de banda, capacidad de procesamiento o memoria, con el fin de dejarlo inaccesible para los usuarios legítimos.

- SYN Flood: El ataque SYN Flood es una forma de ataque de denegación de servicio (DoS) en el que el atacante envía una gran cantidad de solicitudes SYN (sincronización) falsificadas a un servidor o dispositivo de red. Estas solicitudes no se completan y se dejan en un estado pendiente, lo que agota los recursos del sistema objetivo y hace que no pueda procesar las solicitudes legítimas. Como resultado, el sistema se vuelve inaccesible para los usuarios legítimos.

- ICMP Flood: El ataque ICMP Flood es otro tipo de ataque de denegación de servicio que se basa en el protocolo ICMP (Internet Control Message Protocol). En este ataque, el atacante envía una gran cantidad de paquetes ICMP falsificados a un sistema o red. Estos paquetes ICMP pueden ser solicitudes de eco (ping) o mensajes de error ICMP. El objetivo es abrumar los recursos del sistema objetivo con tráfico ICMP, lo que resulta en una interrupción del servicio y la incapacidad de procesar otras comunicaciones legítimas.

- UDP Flood: El ataque UDP Flood es un tipo de ataque de denegación de servicio que se centra en el protocolo UDP (User Datagram Protocol). En este ataque, el atacante envía una gran cantidad de paquetes UDP al sistema objetivo. A diferencia del protocolo TCP, UDP no establece una conexión antes de enviar los datos, lo que lo hace vulnerable a este tipo de ataque. El objetivo es saturar los recursos del sistema objetivo, como el ancho de banda o la capacidad de procesamiento, y hacer que no pueda responder a las solicitudes legítimas, lo que resulta en una interrupción del servicio.

# III. Materiales y Métodos

## 3.1. Herramientas

Para efectuar la evaluación de ataques y el diseño en GNS3 se utilizaron las siguientes herramientas:

- Plataforma de virtualización: Virtualbox es un sistema que emula a un sistema físico (un computador, un hardware, etc.) con unas características que nosotros podemos definir. Proporciona un ambiente de ejecución similar a los de un computador físico Para esta simulación depende completamente, del CPU, BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, etc. Este Hipervisor permite simular varios computadores o sistemas operativos dentro de una misma computadora denominada anfitrión. Permitiendo mayor aprovechamiento de recursos, siendo en la mayoría de los casos usados para simular ambientes de producción (Bastidas, 2023).

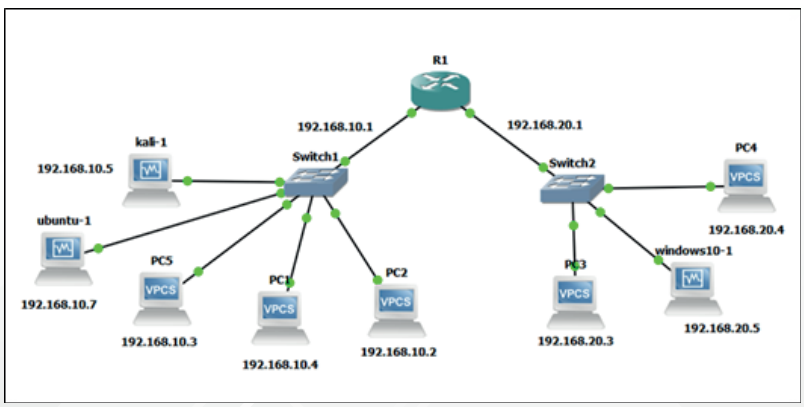
- Software de Emulación de redes: GNS3 es un simulador que permite emular diferentes topologías de red, desde diseños sencillos hasta trabajar con sistemas complejos y ejecutar simulaciones en tiempo real. Esta herramienta permite una completa simulación, ya que cuenta con una gran cantidad de herramientas para generar entornos de simulación lo más cercanos a la realidad. Adicional GNS3 utiliza herramientas de virtualización como Virtualbox siendo justamente una de las ventajas ya que permite optimizar los recursos.

- Ettercap: Es una plataforma gratuita de Kali Linux que permite ejecutar en tiempo real ataques controlados de man in the middle. Utiliza para este proceso herramientas de generación de tráfico, como DDoS attacks (Distributed Denial of Service), para simular el tráfico malicioso desde múltiples puntos de origen dentro de la red LAN hacia la máquina objetivo. La máquina atacante (Kali Linux), configura herramientas de ataque DDoS la cual sirve para monitoreo de red, capturar el tráfico generado por cada dispositivo final y analizar los efectos del ataque DDoS en el objetivo. Esto permite observar el aumento en el tráfico, la congestión de la red, la caída de paquetes y otros efectos del ataque distribuido (Ortiz, 2022).

## 3.2. Diseño de la topología experimental

Se configuró una estrategia de “ataque distribuido” donde varios dispositivos finales participan en el ataque DDoS. La topología consiste en un router, dos switches y varios dispositivos finales conectados a través de ellos. El objetivo principal es evaluar los efectos de los ataques DDoS en la disponibilidad y el rendimiento de los servicios.

**Figura 1:** *Diseño de Topología en GNS3*



En la Figura 1 se puede apreciar que el Router 1 está conectado tanto al Switch1 como a Switch2, los cuales a su vez tienen otras conexiones, tales como:

Switch 1 (192.168.10.1)

- PC1 (192.168.10.4)
- PC2 (192.168.10.2)
- PC5 (192.168.10.3)
- kali-1 (192.168.10.5)
- ubuntu-1 (192.168.10.7)

Switch 2 (192.168.20.1)

- PC3 (192.168.20.3)
- PC4 (192.168.20.4)
- windows10-1 (192.168.20.5)

**3.3. Estrategia del ataque distribuido**

- Configuración de los dispositivos finales: En el Switch 2 se configuran los tres dispositivos finales involucrados directamente en el ataque DDoS.
- En el contexto de la estrategia de "ataque distribuido" que se está discutiendo, los dispositivos finales conectados al Switch 1 no participan en el ataque y se mantienen como parte de una red "víctima" o "afectada" por el ataque.
- Configuración de la máquina atacante (192.168.10.5): En la máquina atacante (Kali Linux), se configura la herramienta de ataque LOIC (Low Orbit Ion Cannon). Esta herramienta permite generar tráfico malicioso hacia el objetivo (Switch 2) y los dispositivos finales.
- Distribución del ataque: Una vez configurados cada uno de los dispositivos finales en el Switch 2 para ejecutar la herramienta de ataque DDoS, se realiza la ejecución de comandos en cada dispositivo final para automatizar el proceso.
- Selección de ataques: Los ataques realizados en los dispositivos finales se conforman de la siguiente manera: Dispositivo 1 (PC3) Ataque SYN Flood; Dispositivo 2 (PC4) Ataque ICMP Flood y Dispositivo 3 (PC5 Windows 10) Ataque UDP Flood.
- Coordinación del ataque: Simultáneamente se coordina el inicio del ataque en cada uno de los dispositivos finales para que comiencen a enviar tráfico malicioso simultáneamente hacia el objetivo.

## IV. Evaluación de Resultados

En la Tabla 1, se puede observar que el volumen de tráfico más habitual en los ataques DDoS es de 100 Gbps. Sin embargo, se han producido ataques con un volumen de tráfico mucho mayor, alcanzando hasta 7 Tbps. La duración media de un ataque DDoS es de 1 hora. Sin embargo, algunos ataques han durado días o incluso semanas. Las fuentes de ataque más comunes son las botnets, que son redes de dispositivos comprometidos controladas por un atacante. Otras fuentes de ataque incluyen ordenadores individuales, servidores y redes. Las motivaciones más comunes de los ataques DDoS son la venganza, el activismo, el sabotaje y la extorsión.

**Tabla 1:** *Estadísticas de los ataques DDoS*

| Métrica | Valor |
|---|---|
| Volumen promedio de tráfico | 100 Gbps |
| Volumen máximo de tráfico | 7 Tbps |
| Duración promedio del ataque | 1 hora |
| Duración máxima del ataque | 7 días |
| Fuentes de ataque más comunes | Botnets |

A continuación, la Tabla 2, muestra que los ataques por inundación SYN son el tipo más común de ataque por inundación, seguidos de los ataques por inundación ICMP y los ataques por inundación UDP. El volumen de tráfico de los ataques por inundación SYN puede alcanzar hasta 100 Gbps, mientras que el volumen de tráfico de los ataques por inundación ICMP y los ataques por inundación UDP suele ser inferior, de hasta 1 Gbps y 10 Gbps, respectivamente. La duración de los ataques de inundación puede variar, pero suelen durar de minutos a horas.

**Tabla 2:** *Comparación de los diferentes ataques*

| Tipo de ataque | Volumen de tráfico |
|---|---|
| Ataque SYN Flood | Hasta 100 Gbps |
| Ataque ICMP Flood | Hasta 1 Gbps |
| Ataque UDP Flood | Hasta 10 Gbps |

## V. Conclusiones y Trabajo Futuro

Los ataques DDoS pueden tener graves repercusiones para las instituciones, ya que son capaces de interrumpir fácilmente los servicios y causar pérdidas tanto internas como externas, tanto a nivel económico como en términos de reputación de la organización y calidad del servicio ofrecido.

El ataque DDoS se aprovecha de la infraestructura de red para obstaculizar la disponibilidad de servicios, generando un alto volumen de tráfico cibernético que resulta en la negación de las solicitudes de los usuarios.

Los ataques DDoS continúan evolucionando mediante la implementación de nuevas técnicas. En el caso del ataque de amplificación, se aprovecha del potencial del Internet para abarcar un mayor número de zonas, así como de su capa de aplicación, que busca activamente vulnerabilidades.

Para mitigar los ataques DDoS en las organizaciones, es fundamental implementar medidas como el monitoreo y la detección temprana mediante sistemas de detección de intrusiones (IDS), así como la aplicación de límites de tráfico y la utilización de servicios especializados en la protección contra DDoS. Además, el filtrado de tráfico y otras estrategias de defensa pueden resultar efectivas en la prevención y mitigación de estos ataques.

Esta investigación tuvo como propósito probar ataques de Denegación de Servicio (DoS), configurándolos a través del emulador de redes GNS3, sin costos de hardware ni software subyacente.

## Referencias

Allauca. E. (2022). *Propuesta de mejores prácticas de ciberseguridad para la comunicación en redes de clientes corporativos*. https://repositorio.pucesa.edu.ec/bitstream/123456789/3779/1/78213.pdf

Bastidas. I. (2023). *Reingeniería de la Infraestructura de Red de Datos Física y Lógica del Gobierno Autónomo Descentralizado Municipal Santa Elena*. UPSE-TTI-2023-0004.pdf

Chalan. R. (2022). *Políticas de Ciberseguridad para los Dispositivos de capa dos en el Centro de Datos del Hospital de Latacunga*. https://repositorio.pucesa.edu.ec/bitstream/123456789/3516/1/77809.pdf

Cirilo. J., Zúñiga. A., Avilés. C. y Villegas. J. (2017). *Análisis de ataques de red del tipo DHCP spoofing, TCP syn flood y paquetes malformados*. https://pistaseducativas.celaya.tecnm.mx/index.php/pistas/article/view/1171/952

Conterón M. (2012). Técnica sniffer para detectar vulnerabilidades en el servidor web, mail y ftp del hospital regional docente Ambato. http://repositorio.uta.edu.ec/bitstream/123456789/2895/1/Tesis_t759si.pdf

EasyDMARC. (2022). *Ataques DDoS y DoS: ¿Cuál es la diferencia?*http://repositorio.puce.edu.ec/bitstream/handle/22000/21028/Ortiz_Alisson_Tesis.pdf?sequence=1&isAllowed=y

FreeEduHub (2022). hping3 Tutorial - TCP SYN Flood Attacks - DoS and DDoS Attacks using Kali Linux 2022 and Windows XPhttps://www.youtube.com/watch?v=S9FdzDXgniA

Fuertes. W., Astudillo E. y Sánchez S. (2020). *Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social*. 582661898003.pdf (redalyc.org)

Fuertes. W., Macas M. y Chunming W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities | Request PDF (researchgate.net)

Fuertes. W. (2022). Redes de computadoras - Un enfoque práctico. https://scholar.google.es/citations?view_op=list_works&hl=es&hl=es&user=6oNo-cMAAAAJ&sortby=pubdate

GNS3 (2023). *Getting Started with GNS3*. https://docs.gns3.com/docs/

Jimenez F. (2023). *Ataque DoS Kali Linux CON Ettercap.* https://www.youtube.com/watch?v=tpkWA3-jC3o

Jiménez. A. y Muñoz. L. (2019). GNS3 FOR SECURITY PRACTITIONERS, 04. https://riuma.uma.es/xmlui/handle/10630/18975

Nuhu. A., Faith. E. y Oyenike. O. (2020). Mitigating DHCP starvation attack using snooping technique. https://fjs.fudutsinma.edu.ng/index.php/fjs/article/view/82/72

Obando C, Vásquez M. (2022). Seguridad a nivel de enlace de datos en el modelo de interconexión de sistemas abiertos (OSI). http://portal.amelica.org/ameli/journal/731/7313661008/7313661008.pdf

Ocampo. C., Viviana Castro. Y. y Solarte. G. (2017). *Sistema de detección de intrusos en redes corporativas.* https://www.redalyc.org/pdf/849/84953102008.pdf

Pérez. B. (2021). *Modelo de detección de ataques de denegación de servicio al protocolo DHCP usando técnicas de Machine Learning*. http://repositorio.unisinucartagena.edu.co:8080/jspui/bitstream/123456789/25/1/modelo%20de%20deteccion%20de%20ataques.pdf

Pilamunga. N. (2019). *Políticas De Seguridad Para Mitigar Las Vulnerabilidades De Los Ataques VLAN Hopping A Nivel De La Capa De Enlace De Datos En Redes LAN*. http://dspace.espoch.edu.ec/bitstream/123456789/9694/1/20T01145.pdf

Reyes J., Fuertes. W. y Macas M. (2022). Development Processes of Vulnerability Detection Systems: A Systematic Review, Approaches, Challenges, and Future Directions. *Procesos de desarrollo de sistemas de detección de vulnerabilidades: una revisión sistemática, enfoques, desafíos y direcciones futuras* | SpringerLink

Rodríguez. B. (2020). *Evaluación de vulnerabilidades en equipos cisco a nivel de redes LAN a través de técnicas de hacking*. http://repositorio.ug.edu.ec/bitstream/redug/58205/1/RODRIGUEZ%20GUTIERREZ%20BYRON%20LUIS.pdf

Tufiño A. (2018). *Diseño de un Modelo de Seguridad de Información en LAN*. http://repositorio.puce.edu.ec/bitstream/handle/22000/15420/Tesis%20Ana%20Cristina%20Tufi%c3%b1o%20Galan%20Version%20Final.pdf?sequence=1&isAllowed=y