Tesla Revista Científica, ISSN: 2796-9320
Vol. 5 Núm. 1 (2025), e486
https://doi.org/10.55204/trc.v5i1.e486

Área: Ingeniería
Artículo de Investigación Original

Evaluación de ataques de denegación de servicio - insider - en redes definidas por software

Evaluation of insider denial-of-service attacks in software-defined networks

Marco Vinicio Ramos Valencia[1][0000-0003-3033-2404], María Belén Paredes Regalado[2][0009-0008-7961-7869], Natalia Patricia Layedra Larrea[3][0000-0003-1017-1746], Steven Alejandro Salazar Cazco[4][https://orcid.org/0000-0002-9708-5885]

[1] Escuela Superior Politécnica de Chimborazo (ESPOCH), Facultad de Informática y Electrónica. SEGINTE. Panamericana Sur Km 1 1/2. 060155. Riobamba – Chimborazo – Ecuador

[2] Escuela Superior Politécnica de Chimborazo (ESPOCH), Sede Morona Santiago. Don Bosco y José Félix Pintado. 140150. Macas – Morona Santiago – Ecuador

[3] Escuela Superior Politécnica de Chimborazo (ESPOCH), Facultad de Informática y Electrónica. GIDETER. Panamericana Sur Km 1 1/2. 060155. Riobamba – Chimborazo – Ecuador

[4] Escuela Superior Politécnica de Chimborazo (ESPOCH), Facultad de Informática y Electrónica. Panamericana Sur Km 1 1/2. 060155. Riobamba – Chimborazo – Ecuador

[1]vi_ramos@espoch.edu.ec, [2]belen.paredes@espoch.edu.ec, [3]natalia.layedra@espoch.edu.ec, [4]steven.salazar@espoch.edu.ec

CITA EN APA:
Ramos Valencia, M. V., Paredes Regalado, M. B., Layedra Larrea, N. P., & Salazar Cazco, S. A. (2025). Evaluación de ataques de denegación de servicio - insider - en redes definidas por software. *Tesla Revista Científica*, *5*(1), e486. https://doi.org/10.55204/trc.v5i1.e486

Recibido: 2025-03-25
Revisado: 2025-04-01 al 2025-04-21
Corregido: 2025-05-10
Aceptado: 2025-06-17
Publicado: 2025-06-25

TESLA
Revista Científica
ISSN: 2796-9320

Resumen. La tecnología ha avanzado hacia la virtualización y las redes SDN son ampliamente reconocidas por las ventajas de gestión que ofrecen sobre las redes tradicionales heredadas. Al analizar una vulnerabilidad de ataque DoS en una red definida por software (SDN), se implementó una red simulada en el software de la máquina virtual GNS3 utilizando varios dispositivos: controlador Opendaylight, open vswitch, cliente y servidor DHCP, DNS, HTTP, VoIP y FTP. Para el análisis de vulnerabilidad se decidió utilizar el método OCTAVE, el cual consta de dos fases: identificación de activos y amenazas de la organización, la segunda: escaneo de vulnerabilidades. La segunda fase de desarrollo utilizó la herramienta Openvas, que ayuda a detectar fallas en la red, sus características y dispositivos afectados, para luego categorizarlos para identificar dispositivos que afectan la disponibilidad, como versiones y tipos de servidores. Una vez completado este paso, se realizan ataques de denegación de servicio: HTTP, DHCP y DNS para agotar los recursos utilizados por el sistema y demostrar el comportamiento de la red en términos de métricas como ancho de banda y latencia. La conclusión es que, en el caso del ancho de banda, la eficiencia del efecto previo al ataque no superó el 34%, pero luego mostró valores tan altos como el 71% y el 84%, mientras que el retraso previo al ataque fue inferior a 15 ms. y luego aumentó a 4779 ms.

Palabras Clave: Redes Definidas por Software, Openflow, Opendaylight, Ataques DDoS, Ataques Insider, Análisis de vulnerabilidades.

Abstract: Technology has moved towards virtualization and SDN networks are widely recognized for the management advantages they offer over traditional legacy networks. When analyzing a DoS attack vulnerability in a Software Defined Network (SDN), a simulated network was implemented in the GNS3 virtual machine software using several devices: Opendaylight controller, open vswitch, DHCP client and server, DNS, HTTP, VoIP and FTP. For the vulnerability analysis, it was decided to use the OCTAVE method, which consists of two phases: identification of the organization's assets and threats, the second: vulnerability scanning. The second phase of development used the Openvas tool, which helps detect network failures, their characteristics and affected devices, and then categorize them to identify devices that affect availability, such as server versions and types. Once this step is completed, denial of service attacks: HTTP, DHCP and DNS are performed to exhaust the resources used by the system and demonstrate the behavior of the network in terms of metrics such as bandwidth and latency. The conclusion is that, in the case of bandwidth, the efficiency of the pre-attack effect did not exceed 34%, but later showed values as high as 71% and 84%, while the pre-attack delay was lower at 15 ms. and then increased to 4779 ms.

Keywords: Software Defined Networks, Openflow, Opendaylight, DDoS attacks, Insider attacks, Vulnerability analysis.

1. INTRODUCCIÓN

En los últimos tiempos, el desarrollo de nuevas tendencias tecnológicas, como la implementación de servicios en la nube, aplicaciones en tiempo real, un mayor número de dispositivos conectados a la red y el big data, entre otros, han influido significativamente en las redes, aumentando sus requerimientos. Como resultado, las redes necesitan ser más escalables y flexibles, sin depender de protocolos definidos por los fabricantes de equipos, para enfrentar los problemas actuales y lograr comunicaciones más rápidas y eficientes (Álvarez, 2015, p. 5).

Para abordar estos desafíos, surge una solución conocida como Redes Definidas por Software (SDN), que ofrece diversas soluciones para usuarios con necesidades cambiantes. Su objetivo es responder dinámicamente a los recursos demandados por aplicaciones en tiempo real, evitando interrupciones en los servicios. Además, las SDN reducen costos de administración y operación, proporcionando flexibilidad, dinamismo y escalabilidad para implementar aplicaciones con grandes requerimientos.

Las SDN representan un paradigma de red innovador, con una arquitectura que separa el plano de datos del plano de control: el primero se encarga de la conmutación de paquetes y el segundo de las funciones de gestión de red. Esta separación permite que las redes sean más programables, flexibles y automatizables. Toda la inteligencia de la red se centraliza en un dispositivo llamado controlador, responsable de la configuración, control y administración del sistema, utilizando el protocolo estándar OpenFlow desarrollado por la ONF. OpenFlow gestiona, identifica y controla el tráfico en la red según reglas predefinidas conforme a los flujos (Velazquez, 2013, p. 1).

El controlador SDN, considerado el núcleo de esta tecnología, puede ser una solución en software o hardware. Configura las reglas de tráfico de acuerdo con políticas y monitoriza toda la red. Utiliza interfaces programables llamadas APIs, que permiten a los administradores desarrollar aplicaciones según sus necesidades, como seguridad, balanceo de carga, calidad de servicio (QoS) y gestión de tráfico. Existen dos interfaces de comunicación: la Northbound API, que conecta con el plano de aplicaciones, y la Southbound API, que se comunica con el plano de datos (Rodrigues et al., 2015, p. 1).

A medida que la tecnología avanza, surgen vulnerabilidades o fallos menores que pueden ser explotados para realizar acciones maliciosas, especialmente por personas familiarizadas con el entorno de la red. Estas amenazas internas, conocidas como "insider threats", son las más difíciles y frecuentes, ya que provienen de personal que conoce bien la infraestructura de red.

Las SDN, al igual que las redes tradicionales, son susceptibles a fallos. Entre las vulnerabilidades se incluyen problemas de programabilidad, uso de software con licencias libres y la centralización del sistema, que puede ser un punto crítico si es comprometido. Según un estudio de Kaspersky Lab, las amenazas más graves para este tipo de redes son los ataques de denegación de servicio (DoS), que afectan la disponibilidad de los servicios al agotar el ancho de banda y los recursos de red mediante la generación de solicitudes masivas desde una o múltiples fuentes. Estos ataques son frecuentes, con un promedio diario

de 500 y un total de 16 millones de paquetes por segundo, y a menudo sirven como camuflaje para otros tipos de amenazas, como virus y troyanos (Ocampo et al., 2017, p. 1-2).

En Ecuador, los ataques de denegación de servicio han aumentado, causando serios problemas en varias organizaciones. Un ejemplo reciente es una amenaza en 2017 por parte del grupo Anonymous, que a través de redes sociales afectó a varias páginas gubernamentales, saturándolas.

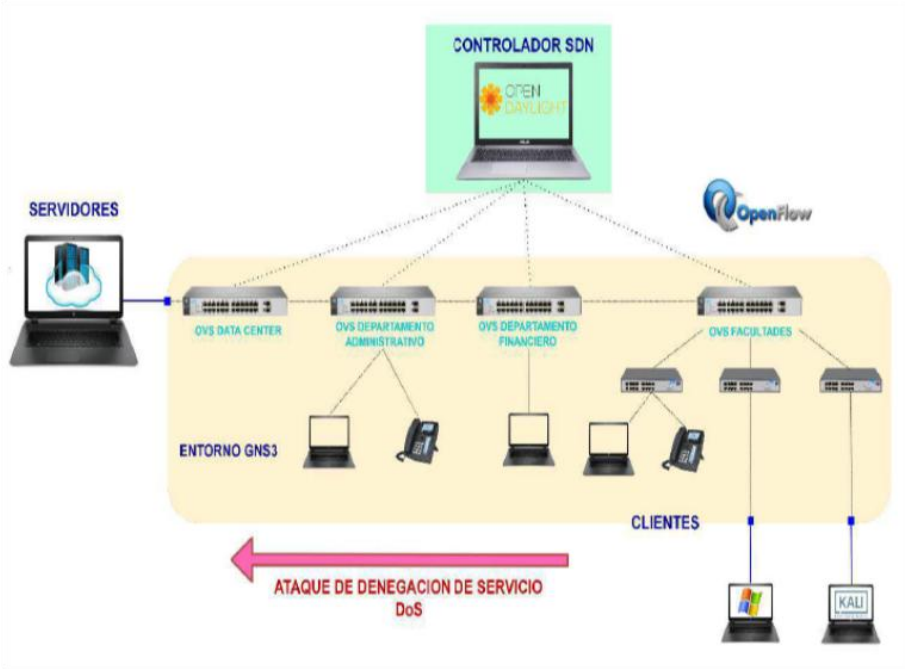
El ***OBJETIVO*** *de* este estudio fue examinar las debilidades frente a ataques de denegación de servicio DoS en redes basadas en software (SDN). Para ello, se diseñará una red simulada utilizando el software GNS3 VM, que incluirá distintos dispositivos: un controlador Opendaylight, open vswitches, así como clientes y servidores de DHCP, DNS, HTTP, VoIP y FTP.

2. METODOLOGÍA

Para analizar las vulnerabilidades en redes definidas por software, se diseñó la topología de red mostrada en la Figura 1. Este escenario incluye un controlador, conmutadores Open vSwitch, un entorno GNS3, servidores, clientes y atacantes. Toda la topología se implementará utilizando máquinas virtuales de Linux y dispositivos externos. El protocolo OpenFlow se utilizará para la comunicación interna de la red.

Figura 1.

Topología de red



Para seleccionar el controlador óptimo que se adapte mejor a los requerimientos del proyecto, se consideraron varios aspectos: creación dinámica y automática de entradas de flujos, interfaz gráfica programable, compatibilidad con las versiones de OpenFlow (1.0, 1.2, 1.3) y documentación disponible.

Se realizó un estudio de mercado para comparar cuatro controladores. La tabla 1 muestra los resultados de este análisis.

Tabla 1.

Comparación entre controladores SDN

CARACTERÍSTICAS	*OPENDAYLIGHT*	*RYU*	*POX*	*FLOODLIGHT*
Plataformas	Linux, MAC, Windows	Linux	Linux, MAC, Windows	Linux, MAC, Windows
Interfaz gráfica	Si	Si	Si	Si
Creación dinámica y automática de flujos	Si	No	No	No
Líneas de código	2500000	116000	20000	44000
Lenguaje	Java	Phyton	Python	Java
Virtualización	Mininet y OvS	Mininet y OvS	Mininet y OvS	Mininet y OvS
Open Source	Si	Si	Si	Si
Versiones OpenFlow	1.0, 1.2, 1.3	1.0, hasta 1.51.01.0	1.0	1.0
Soporte Openstack	Si	Si	No	Si
REST API	Si	Si (SBD)	No	Si
Código abierto	Si	Si	Si	Si
Documentación	Buena	Media	Baja	Buena

Una vez definidos los criterios de selección, se procede a evaluarlos para determinar el dispositivo óptimo para este proyecto. El método de evaluación es cuantitativo, utilizando una escala de calificaciones del 1 al 5, donde 1 representa pésimo, 2 regular, 3 bueno, 4 aceptable y 5 excelente, como se muestra en la Tabla 2.

Tabla 2.

Método de evaluación cuantitativo-cualitativo

PESO	*JUICIO VALORATIVO*
1	*PÉSIMO*
2	*REGULAR*
3	*BUENO*
4	*ACEPTABLE*
5	*EXCELENTE*

La evaluación del controlador óptimo para utilizar en el proyecto se muestra en la Tabla 3, con las calificaciones detalladas en la Tabla 2.

Tabla 3.

Evaluación cuantitativa de los controladores SDN

CRITERIOS Y PONDERACIÓN	OPENDAYLIGHT	RYU	POX	FLOODLIGHT
Plataformas	5	1	4	4
Interfaz GUI	4	4	1	2
Creación dinámica y automática de flujos	4	3	2	1
Líneas de código	5	4	1	3
Versiones openflow	4	4	1	1
Rest api	5	5	2	4
Documentación	4	3	2	5
Total	34	24	13	23

https://doi.org/10.55204/trc.v5i1.e486

La opción que cumple con los requerimientos es el controlador Opendaylight, que con 34 puntos resulta ser el más adecuado para el presente proyecto. Opendaylight es un controlador de código abierto que incluye interfaces Northbound y Southbound. Además de admitir el protocolo OpenFlow, también soporta otros protocolos de licencia libre y permite el uso de herramientas como Maven, OSGi, Karaf, e interfaces JAVA y REST (OpenDaylight Project, 2018a).

Para elegir el software de simulación óptimo se tomaron en cuenta las siguientes características: compatibilidad con el protocolo OpenFlow, capacidad de nodos activos, interoperabilidad, consumo de memoria y escalabilidad. Basándose en estos parámetros, se procede a realizar una comparación entre tres paquetes de software que permiten la implementación de redes SDN, tal como se indica en la Tabla 4.

Tabla 4.

Comparativa entre software de simulación SDN

CARACTERÍSTICAS	MININET	GNS3	ESTINET
PRECIO	Ninguno	Ninguno	Alto
DOCUMENTACIÓN	Media	Alta	Baja
SOPORTE WINDOWS	No	Si	No
SOPORTE LINUX	Si	Si	Si
SIMULADOR	Si	Si	Si
EMULADOR	No	Si	Si
COMPATIBLE CON CONTROLADORES REALES	Todos	Todos	Todos
ESCALABILIDAD	No	Si	Si
ORIENTACIÓN	Solo a SDN	SDN y tradicionales	SDN y tradicionales
SOPORTE GUI	Adaptable	Si	Si

Para la selección se utilizó el mismo método detallado en la tabla 2. Los resultados se evidencian en la tabla 5.

Tabla 5.

Evaluación cuantitativa del software de simulación SDN

CRITERIOS Y PONDERACIÓN	MININET	GNS3	ESTINET
Precio	5	5	1
Documentación	3	5	1
Soporte Windows	1	5	1
Soporte Linux	5	5	5
Simulador	5	5	5
Emulador	1	5	5
Compatible con controladores reales	5	5	5
Escalabilidad	2	4	5
Orientación	3	5	5
Soporte gui	2	4	5
TOTAL	32	48	38

El software que obtuvo el mejor puntaje según la Tabla 5 es GNS3, diseñado para la creación de todo tipo de topologías de red con sistemas operativos reales en todos sus dispositivos, lo que facilita la implementación rápida con equipos de hardware en el futuro. Además, soporta protocolos de conmutación y enrutamiento, así como la posibilidad de NFX y SDN (Pincay, 2015, p. 79).

Para elegir la metodología de análisis de vulnerabilidades, se consideran los siguientes criterios: métodos de análisis (cuantitativo o cualitativo), propiedades de la seguridad (confidencialidad, integridad, disponibilidad), alcance (organizaciones grandes, pequeñas y medianas), norma de seguridad ISO 27001 y documentación.

Basándose en estos aspectos, se procede a comparar dos metodologías que cumplan con los requisitos del trabajo. En la Tabla 6 se presenta la información de dos técnicas para analizar vulnerabilidades en redes.

Tabla 6.

Características de las metodologías de análisis de vulnerabilidades

DESCRIPCIÓN	OSSTMM	OCTAVE
PROPIEDADES DE LA SEGURIDAD	Integridad, confidencialidad ydisponibilidad	Integridad, confidencialidad y disponibilidad
CREADOR	ISECOM	SEI- y CERT
PAÍS	Estados Unidos	Estados Unidos
ALCANCE	Grandes empresas	Todo tipo de empresas
TIPO DE ANÁLISIS	Cualitativo	Cualitativo y cuantitativo
PRECIO	Gratuito	Gratuito
SE ADAPTA A LA ISO 270001	No	Si
DOCUMENTACIÓN	Media	Alta

Para elegir la mejor opción, se utiliza el mismo método cuantitativo de la tabla 2. En la tabla 7, se muestra el cuadro comparativo entre las metodologías de análisis de vulnerabilidades: OSSTMM y OCTAVE.

Tabla 7.

Análisis de las metodologías para análisis de vulnerabilidades

CRITERIOS Y PONDERACIÓN	OSSTMM	OCTAVE
MÉTODOS DE ANÁLISIS	3	5
PROPIEDADES DE LA SEGURIDAD	5	5
DOCUMENTACIÓN	3	5
ALCANCE	3	5
ESTÁNDAR ISO 270001	5	5
TOTAL	19	25

Con un resultado de 25 puntos, la metodología apta para el desarrollo es OCTAVE.

Implementación de OCTAVE Para el Análisis de Vulnerabilidades.

Primera etapa: Identificación de los activos y amenazas de red.

En la etapa inicial, se identifican todos los activos informáticos de la organización mediante la técnica de observación. Se elaboran perfiles o informes detallados de cada elemento, incluyendo sus características de hardware y software, fecha de creación y funcionalidades. En esta sección también se identifican los posibles peligros o amenazas a los que están expuestos.

Segunda etapa: Detección de vulnerabilidades

Basándose en la información obtenida en la primera fase, se procede a examinar las vulnerabilidades en toda la red y en cada uno de los dispositivos (controlador, Open vSwitch, servicios y usuarios). Para detectar las fallas del sistema, se utiliza el software OpenVAS. La información obtenida en esta etapa permite al administrador de red identificar las áreas más críticas de la infraestructura. Tras obtener los resultados del escaneo con OpenVAS en los diferentes dispositivos, se realiza un análisis para determinar cuáles de esas vulnerabilidades tienen más probabilidades de ocurrir.

Para predecir el nivel de probabilidad de ocurrencia de las vulnerabilidades, se basa en el informe del CCN-CERT, que considera tres niveles (alto, medio y bajo), detallados en la Tabla 8.

Tabla 8.

Nivel de probabilidad de ocurrencia de vulnerabilidades

NIVEL DE PROBABILIDADES	DETALLES
ALTA	Comprende un gran riesgo para la organización, afectando a toda la seguridad de la red SDN. Por lo que ese problema requiere de una solución inmediata.
MEDIA	El impacto ocasionado no es significativo, pero requiere de un seguimiento constante y también de solución rápida.
BAJA	No representa mayores inconvenientes para la seguridad. Se puede solucionar a futuro los inconvenientes ocasionados.

Para explotar las vulnerabilidades detectadas, se aplican amenazas específicas, en este caso, la ejecución de ataques de denegación de servicio (DoS). Para evaluar el rendimiento de la red, se utilizan dos indicadores: ancho de banda y tiempos de respuesta en el envío de paquetes de un punto a otro.

Indicador 1: Ancho de banda. Para determinar la efectividad de los ataques de denegación de servicio, se sigue la guía del informe emitido por el CCN-CERT, titulado "Ciberamenazas y Tendencias 2017", que clasifica la efectividad de los ataques en tres niveles (alto, medio y bajo). Para calcular este valor, se utiliza la siguiente fórmula:

$$\text{Efectividad} = \frac{número\ de\ paquetes\ detectados}{paquetes\ soportados\ por\ el\ sistema} * 100$$

El nivel alto se considera cuando la efectividad está comprendida entre el 70% y el 100%. Las amenazas medias se sitúan entre el 35% y el 69%, y las de baja consecuencia entre el 10% y el 34%. Para medir la cantidad de paquetes y aplicar la fórmula indicada para determinar el grado de efectividad de los ataques al explotar las vulnerabilidades, se utilizó la herramienta Wireshark.

Indicador 2: Latencia. Para definir el impacto ocasionado en los tiempos de respuesta, se emplean los niveles referenciales de latencia en redes SDN proporcionados por el CCN-CERT. La calidad de la conexión se puede medir en tres escalas, como se muestra en la Tabla 9, cada una con sus propios rangos.

Tabla 9.

Niveles para medir la latencia en redes SDN

NIVEL	VALORES	DETALLES
ALTO	Menos a 1,5 ms	La conexión de punto a punto es óptima, cuando no tarda más de 1,5 milisegundo
MEDIO	1,5ms – 5ms	La red está trabajando con sobreprocesamiento
BAJO	Mayores a 5 ms	Indica que la red está a punto de colapsar

https://doi.org/10.55204/trc.v5i1.e486

Tercera etapa: Elaboración de planes de contingencia

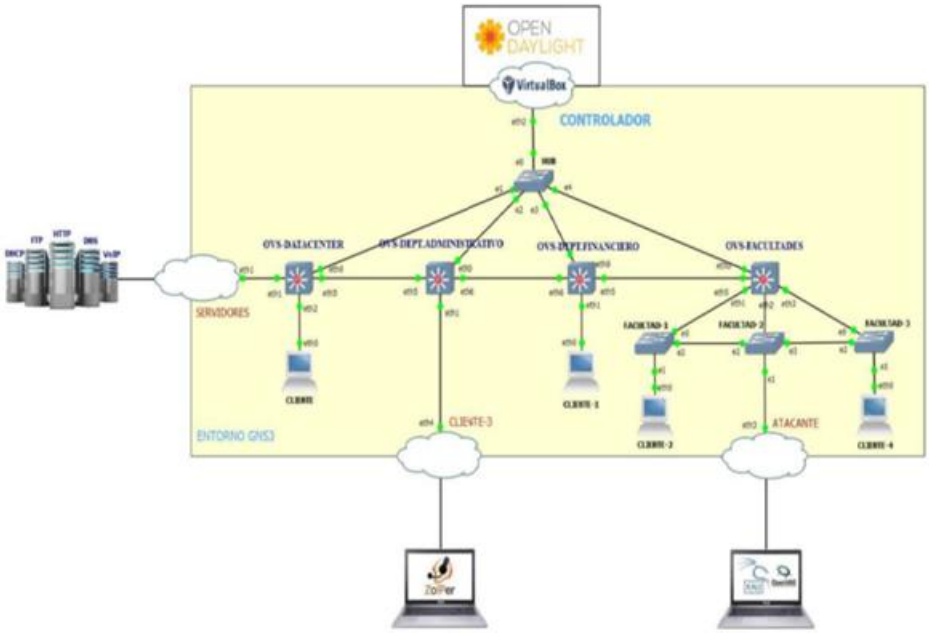
En esta fase, se desarrolla un plan de contingencia o una guía de buenas prácticas con consejos prácticos, para que los administradores de redes SDN puedan implementarlas. El objetivo es contrarrestar o mitigar vulnerabilidades y prevenir daños futuros.

Escenario propuesto

La Figura 2 muestra la topología del escenario en el que se realizan las pruebas. Este escenario incluye un controlador, Open vSwitches, switches de capa 2, servidores y clientes. El escenario abarca solo un ramal de la institución, trabajando con cuatro nodos de interconexión (switches), cada uno funcionando de manera independiente. Los conmutadores se encargan de redirigir el tráfico a los otros nodos.

Figura 2.

Escenario SDN implementado



El escenario simulado se define como una estrella extendida, ya que se centra en el controlador, en el cual se configura toda la red. Este modelo es ampliamente utilizado en diversas entidades debido a su escalabilidad y la autonomía de cada nodo, lo que permite aislar cualquier nodo comprometido sin afectar toda la infraestructura. Los servicios ofrecidos a los clientes son básicos debido a las limitaciones de hardware. Además, el escenario es híbrido porque incluye dispositivos que utilizan o no el protocolo OpenFlow.

Para implementar la red, se utilizan tres PCs externos: en el primero se crea la topología completa en el software GNS3, y en una máquina virtual se aloja el controlador Opendaylight, que envía instrucciones a cada conmutador Open vSwitch según las necesidades de la red. El segundo PC se utiliza para configurar servidores HTTP, DHCP, FTP, DNS y VoIP, mientras que el tercer PC ejecuta los ataques de denegación de servicio usando Kali Linux junto con las herramientas Armitage y Metasploit. La conexión externa entre las máquinas físicas se realiza mediante un concentrador o hub Ethernet. Para el análisis de la red, se emplea Wireshark, y para el escaneo de vulnerabilidades se utiliza OpenVAS.

Para desarrollar los ataques de denegación de servicio, se emplea la plataforma Kali Linux, que ofrece un conjunto de herramientas útiles para pruebas de penetración y hacking ético, incluyendo Metasploit y Armitage. Metasploit es una herramienta de auditoría enfocada en el análisis de vulnerabilidades en sistemas informáticos, que incluye varios módulos de explotación para analizar sistemas y servicios web. Armitage se utiliza para visualizar los objetivos a atacar.

3. RESULTADOS Y DISCUSIÓN

Resultados:

Para detectar las vulnerabilidades existentes en la red SDN implementada, se empleó la metodología OCTAVE, que se desarrolló en tres fases.

Identificación de los activos y amenazas de red.

- El primer paso consistió en evaluar los riesgos, identificando todos los activos informáticos de la organización (controlador, Open vSwitch, servidores y clientes). Para conocer la información de cada uno, se debe consultar el Anexo H. En esta etapa también se detallaron las posibles amenazas a las que están expuestos.

Detección de vulnerabilidades.

- Se utilizó OpenVAS, un software potente que, además de detectar fallas en la red, proporciona información estadística y detallada sobre las vulnerabilidades encontradas, basándose en la dirección IP y los puertos abiertos de cada activo informático, como se muestra en la Figura 4-3. El Anexo I presenta todas las fallas encontradas en el controlador, servidores, Open vSwitch y usuarios.
- Durante el escaneo del controlador, que se realizó en 13 minutos y 40 segundos con la dirección IP 192.168.1.5, se localizaron vulnerabilidades de nivel medio con un 80% de calidad en la detección, afectando al puerto 8181 (comunicación HTTP de ODL). El efecto en este dispositivo es que, si se logra acceder, el atacante podría obtener información sensible de toda la red SDN. También se identificaron debilidades en los DIRB (NASL wrapper), herramientas basadas en diccionarios que buscan fallas existentes u ocultas en el servidor web mediante ataques de fuerza bruta.
- En el análisis del dispositivo Open vSwitch con la dirección IP 192.168.1.10, realizado en 8 minutos y 25 segundos, se encontraron fallas en ICMP y CPE inventory, con un 80% de calidad de detección, atribuible a que se trata de productos patentados. En los servicios de red, se observaron incidencias en el puerto 80 (servidor HTTP) con un 95%, seguido del puerto 22 (SSH) con un 95%, puerto 21 (FTP) con un 80%, y BIND e ICMP. Entre los usuarios, se detectaron amenazas con un 98% en DIRB, SMB, SSL/TLS, y un 80% en ICMP.

Ataques a la infraestructura SDN.

- Para explotar las vulnerabilidades detectadas, se ejecutaron ataques de denegación de servicio (DoS) contra la infraestructura de red SDN, generados desde Kali Linux utilizando

las herramientas Armitage y Metasploit. Los ataques DoS seleccionados fueron dirigidos a los servicios DHCP, HTTP y DNS.

- El comportamiento de la red frente a estas amenazas se analizó utilizando dos indicadores de disponibilidad: ancho de banda y latencia.

DISCUSIONES:

El enfoque sistemático de la metodología de octava para abordar las vulnerabilidades en una red organizacional permitió el tratamiento eficiente de los riesgos de seguridad. En la primera fase, se reconocieron activos importantes y posibles amenazas, mientras que en la segunda etapa se aplicó la herramienta OpenVAS para escanear y detectar fallos en la red, clasificando las vulnerabilidades que afectan principalmente la disponibilidad del sistema. Estas incluían versiones desactualizadas de servidores, vulnerabilidad a ataques de fuerza bruta y fallos en protocolos como HTTP, DNS e ICMP. Después, se llevaron a cabo ataques simulados de denegación de servicio para medir el impacto real en el rendimiento de la red, observando aumentos significativos en el uso de ancho de banda y latencia, lo que sugiere una afectación evidente al funcionamiento habitual del sistema.

Indicador I: impacto en el ancho de banda.

- Para medir el impacto en el ancho de banda, se utilizó la fórmula de la efectividad:

$$\text{Efectividad} = \frac{número\ de\ paquetes\ detectados}{paquetes\ soportados\ por\ el\ sistema} * 100$$

- Para evaluar el impacto de los ataques de denegación de servicio (DoS) en el ancho de banda, se estableció la cantidad de paquetes antes y después de ejecutar los ataques, en comparación con la capacidad máxima del sistema, utilizando Wireshark. Se determinó en pruebas de laboratorio que el sistema puede manejar hasta 1200 paquetes por segundo.
- Como se muestra en la Tabla 10, antes de realizar los ataques DoS, el impacto en el ancho de banda fue bajo, con valores de efectividad del 23% para el controlador, 34% para los servidores, 0.5% para el servidor DNS y 34% para el servidor DHCP. Después de los ataques, el consumo de ancho de banda se duplicó en todos los casos. El impacto fue medio para el controlador (59% de efectividad), alto para los servidores (71%), bajo para el servidor DNS (6%) y alto para el servidor DHCP (82%).
-

Tabla 10.

Impacto de DoS en el ancho de banda

ATAQUE	TRAMAS DETECTADAS		TOTAL TRAMAS	EFECTIVIDAD	IMPACTO
	ANTES	DESPUÉS			
ATAQUE HTTP CONTROLADOR	281	716	1200	23% - 59%	Bajo - Medio
ATAQUE HTTP SERVIDORES	408	859	1200	34% - 71%	Bajo - Alto
ATAQUE DNS	62	80	1200	0.5% - 6%	Bajo - Baja
ATAQUE DHCP	411	995	1200	34% - 82%	Bajo - Alto

Indicador II: impacto en los tiempos de respuesta.

- El impacto en los tiempos de respuesta se midió en dos momentos: antes y después de los ataques DoS. Se utilizó la herramienta PING para medir la latencia entre puntos de conexión. La Tabla 11 muestra el comportamiento de la red SDN en términos de latencia, calculando el valor promedio antes y después de los ataques.

Tabla 11.

Mediciones de latencia en la red SDN

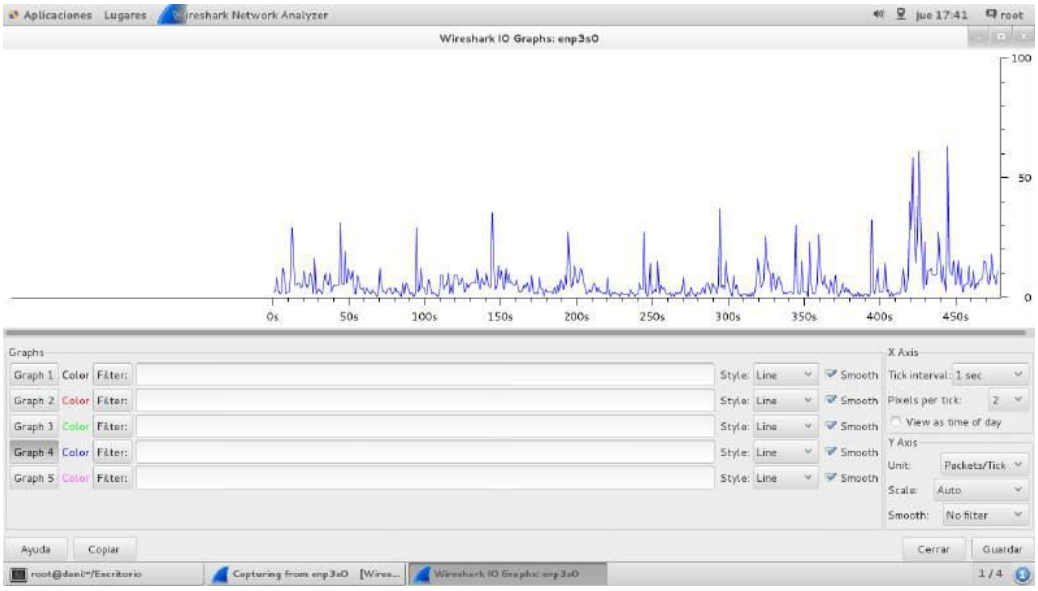
ATAQUE	LATENCIA		CALIDAD DE CONEXIÓN
	ANTES	DESPUÉS	
ATAQUE HTTP CONTROLADOR	0.687 ms	4.009 ms	Alto - medio
ATAQUE HTTP SERVIDORES	0.646 ms	4.779 ms	Alto - medio
ATAQUE DNS	0.692 ms	2.064 ms	Alto - bajo
ATAQUE DHCP	0.687 ms	3.592 ms	Alto - bajo

Análisis de tráfico ante ataques DoS.

- Para analizar el tráfico durante los ataques DoS, se utilizó Wireshark para observar la cantidad de tráfico en la red. La Figura 3 muestra las mediciones captadas en el controlador, con el eje horizontal representando una línea de tiempo de 500 segundos antes de los ataques DoS y el eje vertical indicando la cantidad de paquetes generados en ese período. Se observó que entre los 0 y 400 segundos, la red operaba normalmente, enviando entre 5 y 35 paquetes por segundo. A partir de los 400 segundos, la red comenzó a experimentar una mayor carga, con un aumento en el envío de paquetes a 65 por segundo.

Figura 3.

Análisis con Wireshare antes de realizar ataques DoS

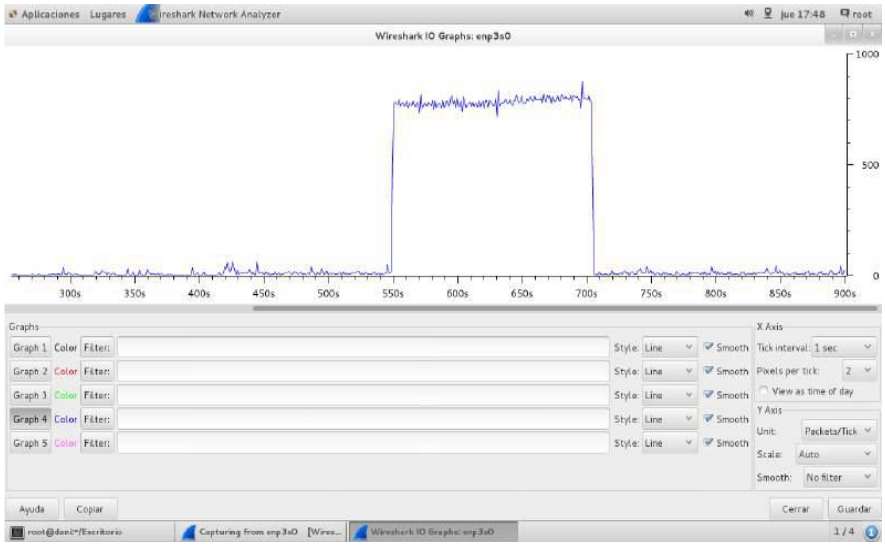


- La Figura 4 muestra las mediciones de tráfico después de aplicar los ataques DoS. Se observó un incremento significativo en el tráfico, con un aumento notable en la cantidad de paquetes enviados. Entre los 550 y 710 segundos (aproximadamente 300 segundos), el sistema experimentó un tráfico de hasta 900 paquetes por segundo. Este incremento drástico refleja el impacto severo de los ataques DoS en la red, saturando la capacidad de procesamiento y afectando el rendimiento general de la infraestructura.

https://doi.org/10.55204/trc.v5i1.e486

Figura 4.

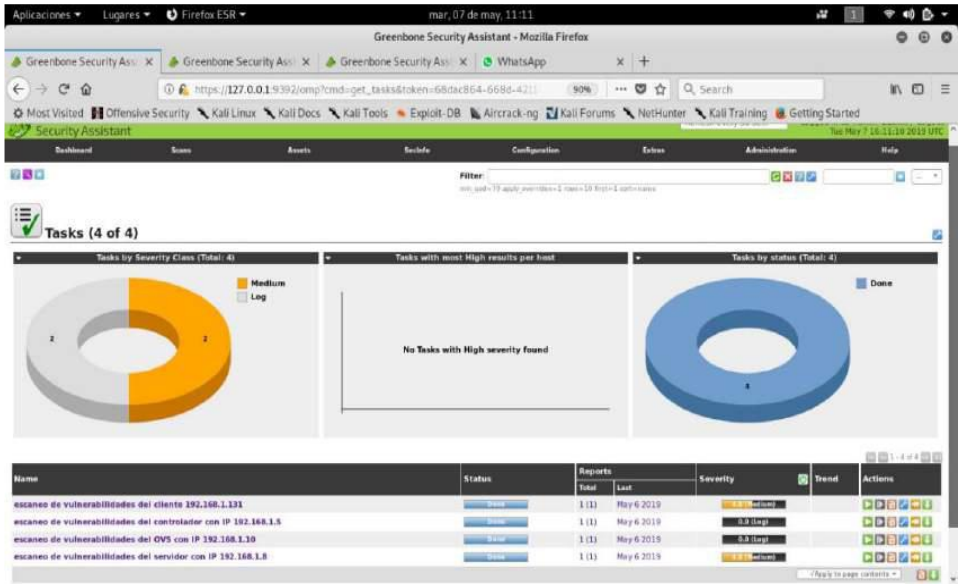
Análisis con Wireshark después de realizar ataques DoS



- Los planes de contingencia son esenciales y cruciales, tanto para redes tradicionales como para redes definidas por software, ya que ayudan a contrarrestar o minimizar cualquier vulnerabilidad detectada, previniendo así posibles daños futuros. Para el desarrollo de este trabajo investigativo, se ha creado una guía de buenas prácticas, basada en el estándar ISO 270001 y adaptada a las SDN, que incluye una serie de métodos aplicables por cualquier administrador de red para proteger su infraestructura contra posibles ataques.
- Tras la implementación del plan de contingencia en la red SDN, se observó una reducción significativa en las vulnerabilidades, como se muestra en la figura 5.

Figura 5.

Vulnerabilidades detectadas después del plan de contingencia



- Además, la Tabla 12 ofrece un resumen del nivel de gravedad e impacto de las vulnerabilidades antes y después de la aplicación de la guía de buenas prácticas en cada uno de los activos informáticos:

Tabla 12.

Impacto de vulnerabilidades en la infraestructura de red

ACTIVO	GRAVEDAD		IMPACTO	
	ANTES	DESPUÉS	ANTES	DESPUÉS
CONTROLADOR	4.8	0	Medio	Bajo
OPEN VSWITCH	0	0	Bajo	Bajo
SERVICIOS	9.0	4.8	Alto	Medio
CLIENTE	9.3	4.8	Alto	Medio

En la fase tres, se elaboró una guía de procedimientos óptimos para solventar las carencias identificadas. Esta iniciativa ayudó a reducir peligros, al fijar medidas exactas como la actualización constante de los permisos del administrador y la formalización inequívoca de las reglas de circulación en la red. Los datos logrados revelan que la puesta en marcha de este programa de prevención refuerza la protección de la plataforma, pues aminora la opción de accesos no autorizados y optimiza el funcionamiento de la red ante incidentes. Dicha vivencia enfatiza la trascendencia de asumir una visión ordenada en el manejo de peligros y la necesidad de fusionar recursos técnicos con directrices de protección que sean exactas y modernas.

4. CONCLUSIONES

El estudio de vulnerabilidades en Redes Definidas por Software (SDN) revela varios problemas, especialmente en el protocolo de comunicación OPENFLOW, que carece de medidas de seguridad, y en el controlador, en el despliegue de flujos o reglas.

Para el análisis de vulnerabilidades se empleó la metodología OCTAVE y el escaneo de la red se realizó con Openvas. Se comprobó que tanto el controlador como los servidores son vulnerables debido al protocolo HTTP (puertos 8181 y 80, respectivamente), con una incidencia del 33%. Además, se detectó una vulnerabilidad en la versión de BIND de DNS con una incidencia del 15%, y los tiempos de detección de solicitudes de marca de tiempo ICMP presentaron un riesgo del 100% para la seguridad de la red.

El escenario implementado para las pruebas de ataques DoS demostró alta eficacia gracias a una topología en estrella extendida que permite al administrador de red aislar puntos de falla en caso de que algún nodo se vea afectado.

Antes de los ataques, el impacto en el ancho de banda no superaba el 34% de efectividad, lo que indicaba un bajo riesgo. Sin embargo, después de la amenaza, el impacto superó el 70%, representando un alto peligro. En cuanto a la latencia, los valores antes de los ataques eran inferiores a 1,5 milisegundos, mientras que después de los ataques, el tiempo se incrementó a 4,779 milisegundos, sugiriendo un sobreprocesamiento del servicio.

https://doi.org/10.55204/trc.v5i1.e486

La prueba no paramétrica utilizada fue la de Wilcoxon, equivalente a la prueba paramétrica t-student para muestras relacionadas. La probabilidad obtenida fue de 9,23E-43, que es menor al valor de significancia, permitiendo concluir que existen diferencias significativas entre las medianas de los resultados de paquetes generados antes y después de los ataques de denegación de servicio.

Tras la implementación del plan de contingencia, se observó una reducción a la mitad de las vulnerabilidades en todos los activos de red. En los servicios y clientes, la gravedad se redujo de 9,0 y 9,3 a 4,8, indicando un impacto medio, y en el controlador se comprobaron cero vulnerabilidades

FINANCIACIÓN

Los autores declaramos que la investigación no tuvo financiamiento.

CONFLICTO DE INTERESES

Los Autores declaramos que no existe conflicto de intereses con nuestra investigación.

CONTRIBUCIÓN DE AUTORÍA

En concordancia con la taxonomía establecida internacionalmente para la asignación de créditos a autores de artículos científicos (https://credit.niso.org/). Los autores declaran sus contribuciones en la siguiente matriz:

Participar activamente en:	*Autor 1.*	*Autor 2*	*Autor 3*	*Autor 4*
Conceptualización	X	X	X	X
Análisis formal	X	X	X	X
Adquisición de fondos	X	X	X	X
Investigación	X	X	X	X
Metodología	X	X	X	X
Administración del proyecto	X	X	X	X
Recursos	X	X	X	X
Redacción –borrador original	X	X	X	X
Redacción –revisión y edición	X	X	X	X
La discusión de los resultados	X	X	X	X
Revisión y aprobación de la versión final del trabajo.	X	X	X	X

REFERENCIAS

Aguilar, D. P. E. (s. f.). Estudio para el desarrollo de un modelo de gestión de riesgos y seguridad de la información para instituciones militares.

Amarilla Cardoso, L. (2016). Despliegue de un testbed de redes definidas por software para la gestión de recursos de red en un CPD [masterThesis]. https://dehesa.unex.es:8443/handle/10662/4417

Benefits and the Security Risk of Software-defined Networking. (s. f.). ISACA. Recuperado 11 de agosto de 2024, de https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/benefits-and-the-security-risk-of-software-defined-networking

Braun, W., & Menth, M. (2014). Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices. Future Internet, 6(2), Article 2. https://doi.org/10.3390/fi6020302

Coker, O., & Azodolmolky, S. (2017). Software-Defined Networking with OpenFlow: Deliver innovative business solutions. Packt Publishing Ltd.

DDoS Attack Types & Mitigation Methods | Imperva. (s. f.). Learning Center. Recuperado 10 de agosto de 2024, de https://www.imperva.com/learn/ddos/ddos-attacks/

Espinoza, E. G. P., & Quito, D. T. (s. f.). Tesis de grado previa obtención del título de ingeniero en sistemas informáticos.

EstiNet 11. (s. f.). AIGOAL. Recuperado 10 de agosto de 2024, de http://www.gordonsmart.com/ns/?page_id=21140

Fernádez, P. Y., & Sanahuja, J. M. M. (s. f.). Programación de redes SDN mediante el controlador POX.

Garcia, B. R. (s. f.). OpenDaylight SDN controller platform.

Getting Started with GNS3 | GNS3 Documentation. (s. f.). Recuperado 10 de agosto de 2024, de https://mother.github.io/docs/

Introducción al conjunto de protocolos TCP/IP - Guía de administración del sistema: Servicios IP. (s. f.). Recuperado 11 de agosto de 2024, de https://docs.oracle.com/cd/E24842_01/html/820-2981/ipov-6.html

Introduction To Software Defined Networking | PDF | Citrix Systems | Virtualization. (s. f.). Scribd. Recuperado 10 de agosto de 2024, de https://www.scribd.com/doc/257324121/Sdn-101-an-Introduction-to-Software-Defined-Networking

Jardón, G. A. S. (2017). Estudio de Redes Definidas por Software e Implementación de escenarios virtuales de prueba. 2017.

Kottler, S. (2018, marzo 1). February 28th DDoS Incident Report. The GitHub Blog. https://github.blog/news-insights/company-news/ddos-incident-report/

Legeren-Alvarez, E. (2012). Diseño de un sistema de información mediante una intranet corporativa: Propuesta de implementación en una empresa constructora de la provincia de Granada (p. 120). GRIN Verlag. http://books.google.es/books?id=2HlUbcwAkLoC

Martinez, G. R. S., Ocampo, C. A., & Bermúdez, Y. V. C. (2017). Sistema de detección de intrusos en redes corporativas. Scientia et Technica, 22(1), Article 1. https://doi.org/10.22517/23447214.9105

Moscoso Clerque, E. M. (2016). Desarrollo de una aplicación para la implementación de calidad de servicio por priorización de tráfico sobre una Red Definida por Software (SDN) [bachelorThesis, Quito, 2016.]. http://bibdigital.epn.edu.ec/handle/15000/15202

Oladunjoye, O. (s. f.). Software Defined Networking.

Open Networking Foundation. (s. f.). Open Networking Foundation. Recuperado 11 de agosto de 2024, de https://opennetworking.org/

OpenDaylight. (s. f.). Recuperado 11 de agosto de 2024, de https://www.opendaylight.org/technical-community/getting-started-fordevelopers/roadmap

OpenVAS - Open Vulnerability Assessment Scanner. (s. f.). Recuperado 11 de agosto de 2024, de https://www.openvas.org/index-de.html

Paracuellos Cortés, J., & Rodríguez Fernández, R. J. (with Universidad de Zaragoza). (2016). Defensa proactiva y reactiva ante ataques DDoS en un entorno simulado de redes definidas por software. Universidad de Zaragoza.

Pardo, C. A. C. (2014). Implementación de un Openflow Controller para el manejo de Openflow Switches.

Pinilla, R. Á. (2015a). Trabajo fin de Máster.

Pinilla, R. Á. (2015b). Trabajo fin de Máster.

Redondo, M., Bravo, C., Bravo, J., & Ortega, M. (s. f.). Intranet: Soporte para entorno de aprendizaje. http://www.redined.mec.es/oai/indexg.php?registro=012200230406.

Reference Designs. (s. f.). Open Networking Foundation. Recuperado 11 de agosto de 2024, de https://opennetworking.org/reference-designs/

Rodrigues, C. P., Costa, L. C., Vieira, M. A. M., Vieira, L. F. M., Macedo, D. F., & Vieira, A. B. (s. f.). Avaliação de Balanceamento de Carga Web em Redes Definidas por Software.

Rodríguez, D. R. R. (s. f.). Y aprobada por el siguiente Comité.

Sandoval Chicaiza, C. E. (2018). Implementación de un clúster-controlador de SDN basado en un framework de software libre para la infraestructura Cloud de la facultad de ingeniería en Ciencias Aplicadas [bachelorThesis]. https://repositorio.utn.edu.ec/handle/123456789/7986

Sdnhub.org. (s. f.). Recuperado 11 de agosto de 2024, de http://ww7.sdnhub.org/tutorials/openflow-1-3/?usid=26&utid=7573656510

Seis, G., & Alexander, J. (s. f.). Diseño de un sistema de gestión de seguridad de la información para instituciones militares.

Software Defined Networks. (2016). https://shop.elsevier.com/books/software-defined-networks/goransson/978-0-12-804555-8

T, C. H. T. (1969). Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología, 28(84), Article 84.

Tarqui Tipo, S. R., & Cuadros Morales, C. A. I. (2017). Implementación de una extranet para la gestión académica en el Instituto de Emprendedores de la Universidad San Ignacio de Loyola. Universidad de San Martín de Porres - USMP. https://repositorio.usmp.edu.pe/handle/20.500.12727/3980

Tutoriales WireShark | PDF. (s. f.). Scribd. Recuperado 10 de agosto de 2024, de https://es.scribd.com/doc/128906887/Tutorial-Wire-Shark

Vargas, W. V. (s. f.). Emulación de una red definida por software utilizando MiniNet. Recuperado 11 de agosto de 2024, de https://www.academia.edu/5730624/Emulaci%C3%B3n_de_una_red_definida_por_software_utilizando_MiniNet

What is a DDoS botnet? (s. f.). Recuperado 10 de agosto de 2024, de https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/

Yandun, M. E. O. (s. f.). Diseño e Implementación de una Aplicación para balanceo de carga para una Red Definida por Software (SDN).