

# **ESCUELA POLITÉCNICA NACIONAL**

## **ESCUELA DE FORMACIÓN DE TECNÓLOGOS**

### **IMPLEMENTACIÓN DE UN SIEM PARA LA DEFENSA ACTIVA ANTE INTRUSIONES EN LA RED**

### **IMPLEMENTACIÓN DE UN SIEM PARA LA DEFENSA ACTIVA ANTE UN ATAQUE DE DENEGACIÓN DE SERVICIO**

**TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO  
REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR  
EN REDES Y TELECOMUNICACIONES**

**DANIEL ALEXANDER HERRERA ZAPATA**

**DIRECTOR: GABRIELA KATHERINE CEVALLOS SALAZAR MSC.**

**DMQ, julio 2024**

## **CERTIFICACIONES**

Yo, DANIEL ALEXANDER HERRERA ZAPATA declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.



---

**DANIEL ALEXANDER HERRERA ZAPATA**

**daniel.herrera@epn.edu.ec**

**dhz1708@gmail.com**

Certifico que el presente trabajo de integración curricular fue desarrollado por DANIEL ALEXANDER HERRERA ZAPATA, bajo mi supervisión.

---

**GABRIELA KATHERINE CEVALLOS SALAZAR**

**gabriela.cevalloss@epn.edu.ec**

## DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

A handwritten signature in blue ink that reads "Daniel Herrera". The signature is written in a cursive style with a large initial 'D'.

DANIEL ALEXANDER HERRERA ZAPATA

## **DEDICATORIA**

La concepción del siguiente trabajo está dedicada a Dios, a mis padres Carlos Herrera y Mónica Zapata y a mi hermano Jean Carlos Herrera. A Dios porque me ha acompañado en todo el transcurso de mi carrera, guiándome, cuidándome y sobre todo brindándome la fortaleza para continuar, a mis padres y hermano, que siempre me han brindado su apoyo incondicional para poder lograr todos mis objetivos personales y académicos. Quienes, en el transcurso de mi vida, han velado por mi bienestar y educación siendo mi sostén a todo momento. Colocando su total confianza, en cada desafío que se me ha presentado y nunca abandonarlos frente a la adversidad. Es por ello que he conseguido avanzar y llegar a la meta cumpliendo mis objetivos.

Con cariño y admiración.

Daniel Herrera Zapata

## AGRADECIMIENTO

El resultado del trabajo merece manifestar un gran agradecimiento, a quienes dieron su granito de arena para su culminación, que, con su apoyo, ayuda, colaboración y comprensión, me animaron a lograr mi objetivo principal. Mi agradecimiento primordial, es a mi papá Carlos Herrera, a mi mamá Mónica Zapata y a mi hermano Jean Carlos Herrera, que, por su cariño y apoyo moral, han sido el pilar de este logro, brindándome consejos, indicaciones y sobre todo a no rendirme ante ninguna situación; que me han indicado a "Resurgir de las cenizas como el Ave Fénix". A mis profesores, que me han brindado experiencias y conocimientos para formarme profesionalmente, a la Ing. Gabriela Cevallos, mi tutora en el desarrollo de mi trabajo y en toda la carrera, que supo guiarme y creer en mi capacidad para lograrlo.

Además, agradecer y recordar una frase que siempre fortaleció mi ser y será mi escudo para afrontar todas las situaciones en la vida, sean alegrías o tristezas "*TODAVIA NO ... Y MI BANDA TOCA ROCK*".

Con cariño, admiración y respeto.

Daniel Herrera Zapata

# ÍNDICE DE CONTENIDOS

CERTIFICACIONES .....	I
DECLARACIÓN DE AUTORÍA .....	II
DEDICATORIA .....	III
AGRADECIMIENTO .....	IV
ÍNDICE DE CONTENIDOS .....	V
RESUMEN.....	VII
ABSTRACT .....	VIII
1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO.....	1
1.1 Objetivo general .....	1
1.2 Objetivos específicos .....	1
1.3 Alcance .....	1
1.4 Marco Teórico .....	1
Seguridad de la información .....	1
Vulnerabilidad, amenaza y riesgo.....	2
Amenazas de seguridad de la información.....	2
Ataque de denegación de servicio (DoS) .....	2
Blueteam .....	3
Herramientas del Blueteam .....	4
2 METODOLOGÍA.....	4
3 RESULTADOS .....	5
3.1 Análisis de diferentes SIEM y sus requerimientos de hardware y software .....	5
Requerimientos de Wazuh.....	5
Requerimientos de Splunk.....	6
Requerimientos de OSSIM .....	6
Requerimientos de Security Onion.....	7
3.2 Implementación del servidor SIEM.....	7
Implementación del Servidor Wazuh.....	7

Implementación del Servidor Splunk.....	15
3.3 Implementación de la topología de red.....	20
Topología con el SIEM Wazuh.....	20
Instalación del agente Wazuh y creación del servidor Web .....	22
Instalación de la máquina atacante .....	26
Ejecución del ataque al agente de Wazuh.....	28
Topología con el SIEM Splunk.....	31
Instalación del agente Splunk y creación del servidor Web .....	32
Ejecución del ataque al agente de Splunk.....	38
3.4 Verificación del funcionamiento del SIEM.....	40
Análisis de resultados SIEM Wazuh .....	40
Análisis de resultados SIEM Splunk.....	45
Comparativa técnica entre los SIEM implementados .....	47
Manual técnico con las mejoras practicas ante un ataque de DoS .....	48
4 CONCLUSIONES .....	49
5 RECOMENDACIONES .....	50
6 REFERENCIAS BIBLIOGRÁFICAS.....	52
7 ANEXOS.....	54
8 ANEXO I: Certificado de Originalidad .....	i
9 ANEXO II: Enlaces.....	ii

## RESUMEN

El enfoque de este proyecto tiene como fin la configuración e implementación de dos SIEMs con el propósito de analizar y detectar alertas relacionadas con el ataque de *DoS* (*Denial of Service*). La finalidad es detectar y alertar amenazas que se encuentren en la red y mantener protegida la información de una organización, institución pública o privada; a su vez reforzar la ciberseguridad, por lo tanto, minimizar los riesgos de sufrir la inhabilitación y caída de un servicio específico.

En primera instancia, se tiene la descripción del componente, el objetivo general, los objetivos específicos, alcance y marco teórico. En segunda instancia, se plasma una metodología para lograr alcanzar los objetivos específicos de este proyecto. En tercera instancia, se realiza un análisis comparativo entre los SIEMs, así como las necesidades de hardware y software necesarios para la ejecución en entornos de máquinas virtuales. Además, se lleva a cabo la configuración y creación de los dos servidores SIEM en un entorno controlado, donde se diseñó una topología de red con las mismas características para ambos, se agregaron componentes necesarios para realizar la simulación de un ataque de *DoS* y se evaluó el rendimiento y capacidad de cada SIEM para alertar e identificar posibles ataques de *DoS*. Seguidamente, se mostró una comparativa técnica entre ambos SIEMs implementados, brindando una sugerencia para seleccionar el SIEM más competente contra un ataque de *DoS*.

En la cuarta instancia se plasmaron los resultados alcanzados que se utilizaron para plantear conclusiones y recomendaciones. Finalmente, se presenta la bibliografía y anexos.

**PALABRAS CLAVE:** SIEM, Ciberseguridad, DoS, Splunk, Wazuh, Slowhttptest, Pentmenu

## ABSTRACT

*The purpose of this project is to configure and implement two SIEMs to analyze and detect alerts related to DoS (Denial of Service) attacks. The purpose is to detect and alert on threats present in the network and to protect the information of an organization, whether public or private; and in doing so, reinforce cybersecurity, thereby minimizing the risks of service unavailability and downtime.*

*In the first instance, there is the description of the component, the general objective, the specific objectives, the scope and the theoretical framework. In the second instance, a methodology is outlined to achieve the specific objectives of this project. In the third instance, a comparative analysis is carried out between the SIEMs, as well as the hardware and software requirements for the implementation in virtual machines. In addition, the configuration and creation of the two SIEM servers is carried out in a controlled environment, where a network topology with the same characteristics for both was designed, necessary components were added to simulate a DoS attack and evaluated. the performance and ability of each SIEM to alert and identify possible DoS attacks. Next, a technical comparison between both implemented SIEMs was shown, providing a suggestion to select the most competent SIEM against a DoS attack.*

*In the fourth instance, the results achieved were captured and used to draw conclusions and recommendations. Finally, the bibliography and annexes are presented.*

**KEYWORDS:** SIEM, Cybersecurity, DoS, Splunk, Wazuh, Slowhttptest, Pentmenu

# 1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

El presente proyecto pretende analizar alertas de seguridad que han sido generadas por diferentes dispositivos en una red, en tiempo real, esto mediante la implementación de un servidor SIEM (*Security Information and Event Management*) el cual ayuda a detectar las amenazas, intrusiones y comportamientos sospechosos. Se tendrá una topología de red con un servidor SIEM, a la cual se le realizará un ataque con el fin de que el servidor SIEM muestre las alertas y registros de actividad. Se comparará de manera técnica entre dos SIEM implementados.

## 1.1 Objetivo general

Implementar un SIEM para la defensa activa ante intrusiones en una red.

## 1.2 Objetivos específicos

- Analizar diferentes SIEM y sus requerimientos de hardware y software
- Implementar el servidor SIEM
- Implementar la topología de red
- Verificar el funcionamiento del SIEM

## 1.3 Alcance

En primera instancia se analizan las características de diferentes sistemas de gestión de eventos e información de seguridad, se analizan los requerimientos de hardware y software de los mismos. Se seleccionan dos servidores SIEM y se procede a implementarlos y configurarlos. Cada SIEM se establece en una topología de red, implementada en un emulador de redes. Con el fin de observar el comportamiento de cada SIEM ante un ataque de denegación de servicio, se ejecuta un ataque a la red, se realiza un análisis técnico comparativo entre los dos SIEM. Se realizará un manual técnico con las mejores prácticas ante este ataque.

## 1.4 Marco Teórico

### Seguridad de la información

Es la serie de medidas, acciones, procedimientos y herramientas que tienen como objetivo la protección de datos e información confidencial que han sido recibidos,

procesados, analizados y/o guardados. De tal forma, mantienen la información segura entre ubicaciones y dispositivos, lo que ayuda a protegerse contra ciberataques u otras amenazas que se presenten en la red. Este proceso garantiza que personas que tengan la autorización necesaria a la información de una organización, lo que asegura la CIA de la información [1].

Además, existen tres pilares en la seguridad de la información, que es conocida como CIA; las cuales se componen de confidencialidad: que se enfoca en mantener la privacidad en datos y la información, la integridad: basado en que la información no se haya adulterado de manera indebida no autorizada y los datos e información se mantengan completos y por último la disponibilidad: que deberá mantener el acceso a la información en todo momento [2].

### **Vulnerabilidad, amenaza y riesgo**

La vulnerabilidad es un punto débil dentro de un sistema, lo que provocará que la información y datos sean objeto de ataques cibernéticos, de esta forma, afectarán a la CIA.

La amenaza es la acción en la cual se beneficia de la vulnerabilidad expuesta para transgredir en contra de la seguridad de una organización.

El riesgo se basa en el límite de probabilidad de que una organización informática reciba un ataque cibernético, para lo cual se obtiene un reconocimiento sobre una vulnerabilidad que haya sido detectada en el sistema [3].

### **Amenazas de seguridad de la información**

Las amenazas más comunes en la seguridad de la información son algunas y provienen de varias fuentes que incluyen las siguientes:

- Ataque de amenaza persistente avanzada (APT).
- *Bot nets*.
- Ataque de denegación de servicio (DoS).
- *Phishing*.
- *Ransomware*.
- Ingeniería social.
- Virus y gusanos.

### **Ataque de denegación de servicio (DoS)**

*Denial of Service (DoS)* es un ciberataque el cual tiene como objetivo interrumpir el uso de un servidor, con la finalidad de impedir el servicio del destinatario, ya que llega a

sobrecargar el servicio hacia los usuarios legítimos provocando que no esté disponible. De esta manera, llena de solicitudes al servidor hasta llegar a un límite donde es incapaz de ser procesado, lo cual hace que se produzca una denegación de servicio [4].

Por tal manera, logra ahogar el servidor, servicio o máquina objetivo superando la cantidad máxima de solicitudes, lo que provoca que sus recursos se agoten y, por lo tanto, imposibilita que el tráfico de datos legítimo se maneje de manera adecuada [5].

Lo que caracteriza a este ataque es cómo lo lleva a cabo un solo atacante, es decir, el objetivo principal es la denegación del servicio, donde, satura el servicio o provoca el colapso y el bloqueo de este. La saturación del búfer del servidor se produce a medida que la capacidad de este sea desbordada y provocar la ralentización e incluso la caída del servidor atacado [6]. De tal forma, estos son algunos ejemplos más conocidos relacionados con el ataque por saturación al servidor:

- Desborde del búfer: es conocido como el ataque más habitual en el ataque de *DoS*, donde consiste en enviar a una dirección de red demasiado tráfico de lo que es habitual [6].
- Inundación ICMP: este ataque tiene relación directa con los dispositivos mal configurados en la red, donde envía paquetes falsos que hace un ping a todos los dispositivos de esa red; para ello la red amplifica el tráfico que es enviado. A este ataque se lo conoce como *ping of death* [6].
- Inundación SYN: este ataque tiene como objetivo enviar una solicitud de conexión a un servidor, pero a su vez no logra el *handshake*, de esta forma el ataque sigue su transcurso hasta que todos los puertos que están abiertos se saturan de solicitudes y por ende que no quede ninguno disponible para la conexión de los usuarios legítimos [6].

### ***Blueteam***

Es el grupo de profesionales en la seguridad informática encargados en la ciberseguridad, donde laboran para mantener el orden en la red y defensa de sistemas y redes de una entidad, lo cual los lleva a detectar y responder en contra de las amenazas de seguridad. Implementan acciones preventivas para la protección de la infraestructura de la organización contra amenazas internas y externas. Para lo cual utilizan una serie de herramientas y tácticas de seguridad, como el análisis de logs, análisis de vulnerabilidades, monitoreo de redes, detección de *malware* [7].

## Herramientas del *Blueteam*

Los especialistas en la seguridad informática utilizan diversas herramientas para la protección de redes, servidores, servicios y datos contra los ciberataques; que incluyen las siguientes:

- Gestión de información y eventos de seguridad (*SIEM*): es la herramienta que se encarga de recopilar, analizar y vincular los registros o eventos de seguridad en la red, lo que ayuda a la identificación y detección de posibles amenazas. Lo que garantiza que la acción maliciosa sea resuelta en el menor tiempo posible, además en algunas situaciones previene que ocurra el incidente. Un SIEM es creado para la incrementación y fortalecimiento en la seguridad de una organización, lo que brinda una visión general de la seguridad de la información [8].
- Herramientas de detección y prevención de intrusiones (*IDS/IPS*): ambas herramientas verifican el tráfico en la red, donde buscan actividades peculiares, a su vez detectan y bloquean los intentos de intrusión que vienen de la red [9].
- Sistemas de prevención de pérdida de datos (*DLP*): es la herramienta que blindo la confidencialidad de la información en el momento que detecta, controla y previene la divulgación de datos privados por fuera de la red [9].
- *Firewalls*: es la herramienta encargada de restringir el tráfico de internet a la hora de entrar, salir dentro de una red privada, donde actúa como una frontera en la cual bloquea o permite el tráfico de paquetes selectivos [10].
- Gestión de eventos de seguridad (*SEM*): es la herramienta que se encarga de la detección de acciones irregulares de accesibilidad, ya que realiza un análisis en tiempo real [11].

## 2 METODOLOGÍA

El presente trabajo de integración curricular se basó en el análisis e investigación de manera experimental, donde se analizaron y compararon diferentes SIEM y se implementó en una topología de red para observar su funcionamiento.

La primera sección conlleva una investigación de las características de los SIEM: Wazuh Splunk, OSSIM y SecurityOnion, además de los requisitos tanto de hardware y software para el correcto funcionamiento de estos, con el propósito de escoger los más idóneos.

Seguidamente, se implementaron dos servidores SIEM, Wazuh y Splunk, ambos en máquinas virtuales configurados con características diferentes acordes a sus requerimientos.

Después, se diseñó una topología de red para ejecutar el ataque de *DoS*, agregando los elementos necesarios, donde se los configuró acorde a la simulación del ataque, y se lo ejecuta con el fin de visualizar los resultados.

De acuerdo con lo mencionado, se corroboró la funcionalidad de cada SIEM en la red ante el ataque de *DoS*, se analizó cada suceso junto con la revisión correspondiente de las alertas generadas. Por último, se llevó a cabo una comparación técnica entre ambos SIEM, con el objetivo de brindar una evaluación sobre cuál de ellos es más eficiente y efectivo. Se elaboró un manual técnico de buenas prácticas ante un ataque de *Dos*.

### **3 RESULTADOS**

En el presente trabajo se implementó una topología de red donde se ejecuta el ataque de *DoS* con herramientas de una máquina virtual con Kali Linux. Los resultados del ataque son monitoreados a través de los SIEM Wazuh y Splunk, ambos configurados en máquinas virtuales con Ubuntu.

Además, se observan los resultados arrojados por cada SIEM en respuesta al ataque de *DoS* hacia los agentes de cada SIEM; dado este escenario se realiza una comparación técnicamente entre los SIEM implementados.

#### **3.1 Análisis de diferentes SIEM y sus requerimientos de hardware y software**

##### **Requerimientos de Wazuh**

Es un software encargado de analizar en tiempo real la transmisión de los datos, donde detecta amenazas y realiza una recopilación de datos de varias fuentes, como equipos de red, trabajos en la nube y aplicaciones para cubrir la seguridad de manera ampliada. Además, posee características esenciales como el análisis de registros de seguridad, se encarga de la protección de la infraestructura y cumplimiento normativo donde monitorea las tareas de los equipos finales. Analiza y guarda datos de los eventos de seguridad donde identifica anomalías en la red. La detección de vulnerabilidades está basada en aquellas ya identificadas, con el fin de acelerar el proceso de tomar acciones, de igual manera se encarga de la alerta y notificación de comportamientos sospechosos en la red [12].

Los requerimientos enfocados en hardware son: un procesador con 2 núcleos como mínimo, memoria RAM de 4 (GB) mínimo, capacidad de almacenamiento de 20 (GB). Por otra parte, para requerimientos enfocados en software son: un sistema operativo de 64 (bits) sea este Windows, Linux, MacOS, etc [13].

### **Requerimientos de Splunk**

Es un software comercial con licencia propietaria, sin embargo, ofrece distintas versiones y licencias, donde incluye la versión gratuita con ciertas limitaciones que está disponible durante 60 días para el uso libre. Por otro lado, es un SIEM, que está diseñado para el análisis y monitoreo de aplicaciones, servidores, dispositivos móviles, sistemas de red; mediante una interfaz Web que ayuda a reducir riesgos de ciberataques hacia sus clientes y mejorar el rendimiento de los servicios brindados [14].

Los requerimientos enfocados en hardware son: un procesador de 2 a 4 núcleos como mínimo, memoria RAM de 6 (GB) como mínimo y espacio en el disco de 4 a 10 (GB). Sumado a esto, los requerimientos enfocados en software son: un sistema operativo Linux basado en diferentes distribuciones como CentOS, Red Hat, Ubuntu; sistema operativo Windows Server versión 2016, 2019, dependencias como Python y Java que son necesarias para ciertas aplicaciones [15].

### **Requerimientos de OSSIM**

Es un software que brinda ayuda para el monitoreo en la red, este permite el control de logs, por ejemplo, de un log de contraseña mal digitada hasta un posible ataque que pueda dañar la infraestructura de la red. Las características con mayor relevancia se enfocan en la recolección de datos, donde reúne los datos de seguridad de algunas fuentes, en los cuales se incluyen logs de dispositivos de red, sistemas operativos y otros dispositivos de seguridad [16].

OSSIM proporciona una interfaz gráfica Web amigable hacia el administrador; realiza informes de seguridad, donde se comprenden las tendencias de seguridad y verifica que las medidas de seguridad sean óptimas para cualquier ataque a la red [17].

Además, posee la opción de agregar o no agregar agentes para realizar la monitorización en la red; al agregar un agente se necesita instalar un software específico que recolecte eventos y estos pueden ser una computadora, un servidor o algún dispositivo en la red. En cambio, para la recolección de eventos sin agente se lo realiza mediante el protocolo SSH, donde se recolectaría datos de manera remota utilizando las credenciales respectivas para acceder a ese agente, sin ser necesario la instalación de un software adicional [18].

Los requerimientos enfocados en hardware son: un procesador con múltiples núcleos, memoria RAM de 8 (GB) como mínimo, capacidad de almacenamiento de 50 (GB); en donde puede variar el volumen de datos y retención necesaria. Por otra parte, los requerimientos enfocados en software son: un sistema operativo cuya distribución sea Linux (recomendado), bibliotecas adicionales y base de datos basados en MySQL [18].

### **Requerimientos de *Security Onion***

Es un software de *open source*, el cual está diseñado para el seguimiento de amenazas, monitorizar la seguridad en la red y administración de logs. Este software se puede instalar en máquinas virtuales como hardware físico, resultando compatible con VMware WorkStation, VirtualBox o Hiper-V. Cabe recalcar que este software reúne varias herramientas del *Blueteam* en un solo paquete, ofrece una solución completa; lo que ayudará a una identificación y respuesta rápida ante las posibles amenazas que se encuentren en la red [19].

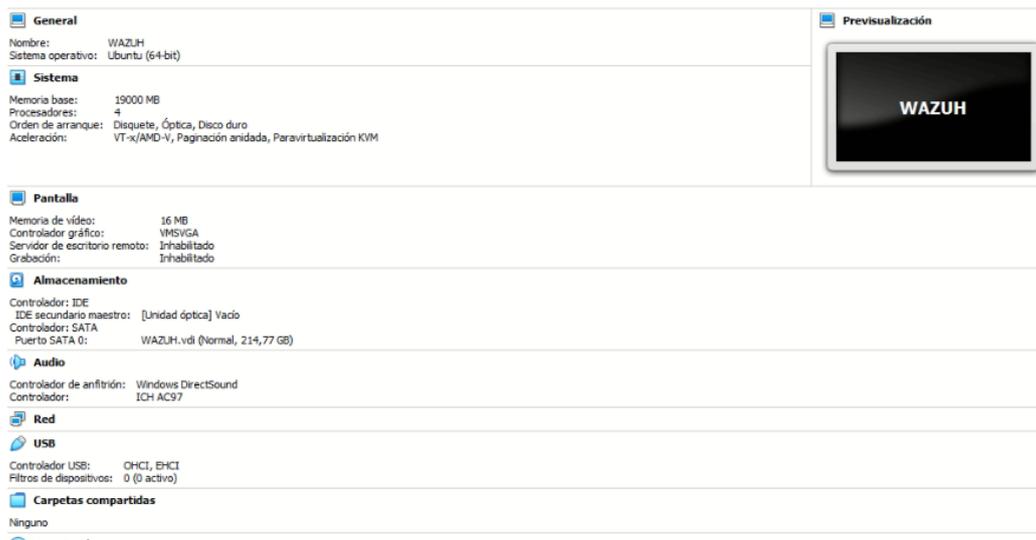
Los requerimientos enfocados en hardware son: un procesador con 2 a 4 núcleos como mínimo, memoria RAM de 8 (GB) a 12 (GB) como mínimo, capacidad de almacenamiento de 50 (GB) en adelante. Sumado a esto, los requerimientos enfocados en software son: un sistema operativo de 64(bits) de preferencia de distribución Linux [20].

Dado las características y requerimientos de cada uno de los SIEM, Wazuh y Splunk son herramientas de ciberseguridad ampliamente reconocidas por su amplia comunidad de usuarios, soporte disponible a través de dicha comunidad y abundantes recursos en línea, por tal motivo se han seleccionado como opciones idóneas. Estas características facilitan su implementación y personalización según las necesidades específicas de cualquier organización, entidad o empresa.

## **3.2 Implementación del servidor SIEM**

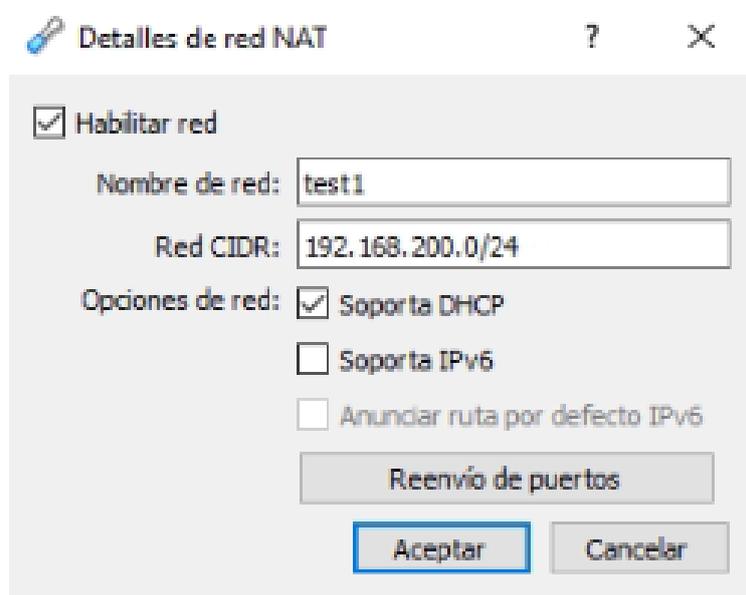
### **Implementación del Servidor Wazuh**

Para la creación del servidor *SIEM* Wazuh previamente se necesita configurar una máquina virtual en VirtualBox con un sistema operativo Linux basado en la distribución Ubuntu 22.04, la cual deberá cumplir con las características que con anterioridad se mencionó, las características se evidencian en la Figura 3.1.



**Figura 3.1** Características de la máquina para Wazuh

Además, se configura una red NAT interna con el nombre “test1”, que asigna dinámicamente las direcciones IP; la dirección de red es 192.168.200.0/24, por lo que las redes disponibles están en el rango de 192.168.200.1 – 192.168.200.254, la cual estará configurada con una red NAT interna donde permite la conexión de las máquinas virtuales entre sí en una red aislada dentro del *host*, de esta forma se visualiza en la Figura 3.2.



**Figura 3.2** Configuración de la red NAT interna en Virtual Box

Para instalar el SIEM Wazuh es necesario ingresar a la URL <https://documentation.wazuh.com/current/quickstart.html> donde se encuentra la guía de instalación; dado esto al momento de ingresar a la máquina Ubuntu se ingresa a su consola y se coloca el siguiente comando: **curl -sO**

**<https://packages.wazuh.com/4.7/wazuh-install.sh> && sudo bash ./wazuh-install.sh -a**, el cual inicia con la instalación del SIEM. El comando se lo puede evidenciar en la Figura 3.3.

```
root@wazuh-VirtualBox: /home/wazuh# curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
27/05/2024 22:38:07 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.4
27/05/2024 22:38:07 INFO: Verbose logging redirected to /var/log/wazuh-install.log
```

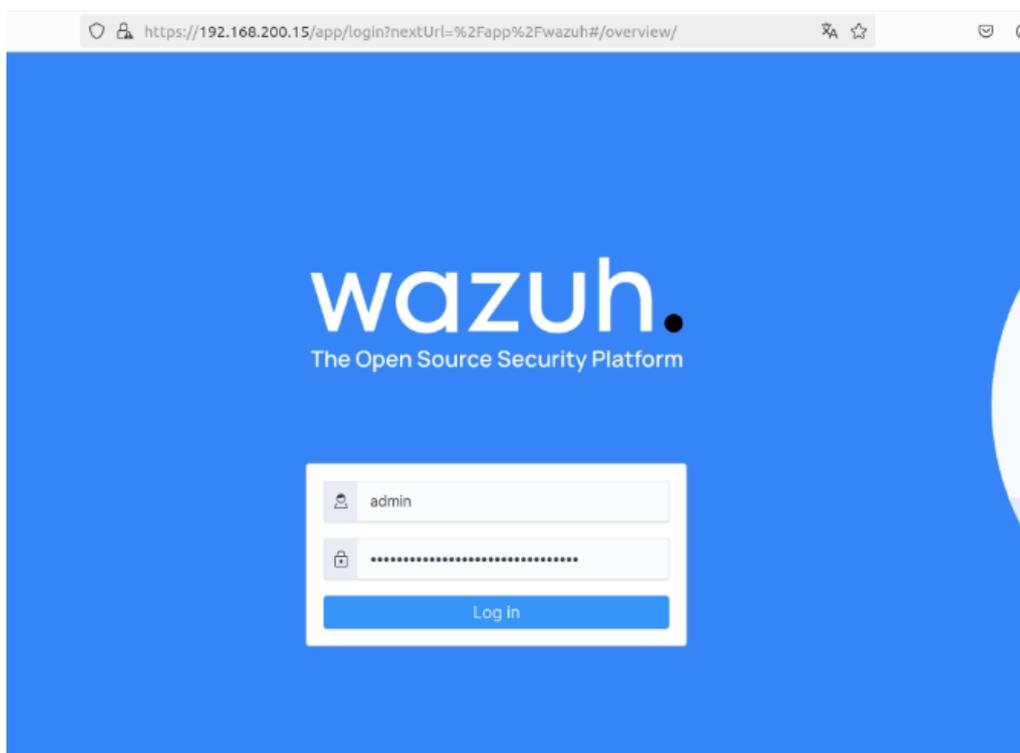
**Figura 3.3** Instalación del servidor Wazuh

Una vez finalizada la instalación del servidor Wazuh, este proporciona un usuario y contraseña; ver la Figura 3.4.

```
27/05/2024 22:54:50 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: 0AYUuURhQgj+af3?*C+7+noN53gIVDPW
27/05/2024 22:54:50 INFO: Installation finished.
root@wazuh-VirtualBox: /home/wazuh#
```

**Figura 3.4** Asignación de usuario y contraseña del servidor Wazuh

Mediante el navegador por defecto de Ubuntu, el cual es Mozilla Firefox, se ingresó la dirección IP del servidor la cual es 192.168.200.15, se abrió una pestaña donde se coloca el usuario y contraseña correspondiente y de esta manera se ingresa al servidor Wazuh, el cual se puede visualizar en la Figura 3.5.



**Figura 3.5** Ingreso de credenciales hacia el servidor Wazuh

Una vez dentro del servidor Wazuh se deben agregar los agentes que van a ser monitorizados a través de este servidor; cabe recalcar que existe la opción de colocar los agentes de diferentes sistemas operativos. En este caso el agente será de la distribución Linux *DEB amd64*, como se evidencia en la Figura 3.6, el cual está ligado a Ubuntu que es una distribución de Linux. Además, la elección entre *RPM* o *DEB* depende de la distribución que se vaya a ocupar, donde *Red Hat Package Manager (RPM)* es una distribución enfocada en RedHat, Fedora; en cambio *Debian Package (DEB)* es una distribución enfocada en Debian o Ubuntu.

The image shows a configuration form for Wazuh agents. It is divided into three main sections: LINUX, WINDOWS, and macOS. Under LINUX, there are four radio button options: RPM amd64, RPM aarch64, DEB amd64 (which is selected), and DEB aarch64. Under WINDOWS, there is one radio button option: MSI 32/64 bits. Under macOS, there are two radio button options: Intel (selected) and Apple silicon. Below these sections is a blue box with a link: "For additional systems and architectures, please check our documentation". Below that is a section titled "Server address:" with a checkmark icon. It contains a text box with the IP address "192.168.200.15".

**Figura 3.6** Configuración para implementar el agente a el servidor Wazuh

Luego de seleccionar el sistema operativo correspondiente se procede a agregar la dirección IP del servidor Wazuh, 192.168.200.15; así como el nombre para el agente y el grupo al cual pertenece, en este caso *default*. Por consiguiente, se genera un comando y este será colocado en la máquina que servirá como agente, esto se muestra en la Figura 3.7.

✓ **Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address: ⓘ

192.168.200.15

---

✓ **Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ⓘ

p1

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled. ⓘ

Select one or more existing groups: ⓘ

default X ⓘ

4 **Run the following commands to download and install the agent:**

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb &&
sudo WAZUH_MANAGER='192.168.200.15' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='p1' dpkg -i ./
wazuh-agent_4.7.4-1_amd64.deb
```

**Figura 3.7** Configuraciones adicionales para la creación del agente

Además, para obtener una mejor monitorización se implementa un *IDS* e *IPS*, el cual es Suricata, la guía para implementar el IDPS Suricata se la encuentra en la URL <https://wazuh.com/blog/responding-to-network-attacks-with-suricata-and-wazuh-xdr/>.

Para esto se debe ingresar a la consola de la máquina donde está instalado el servidor Wazuh, dado que se creará un grupo de agentes y el agente en sí; se ingresa el siguiente comando en la ruta donde se creará el grupo y agente, el comando es: **sudo /var/ossec/bin/agent\_groups -a -g Suricata -q**; donde **sudo /var/ossec/bin/agent\_groups** permite ingresar al grupo de agentes que es parte de OSSEC (*Open Source HIDS SECURITY*), el parámetro “-a” indica que se cree un nuevo grupo, el parámetro “-g” indica el nombre del grupo, el cual es Suricata; lo cual implica que se está creando un grupo de agentes en OSSEC que tengan que ver con la gestión de seguridad del software Suricata y el parámetro “-q” indica que el comando se está ejecutando de manera silenciosa, salvo que exista un error crítico en la configuración mostrará algún mensaje, de lo contrario no. De esta forma se puede visualizar en la Figura 3.8 la ejecución del comando.

```
root@wazuh-VirtualBox: /home/wazuh
root@wazuh-VirtualBox:/home/wazuh# sudo /var/ossec/bin/agent_groups -a -g Suricata -q
Error 1711: The group already exists: Suricata
root@wazuh-VirtualBox:/home/wazuh#
```

**Figura 3.8** Creación del grupo de agentes de Suricata

A continuación, se ingresará a la siguiente ruta con el comando: **sudo /var/ossec/bin/manage\_agents -l**; cómo se puede evidenciar en la Figura 3.9. Donde se verificarán qué agentes se han creado y el parámetro “-l” listará los agentes actuales que son identificados con un ID único.

```
root@wazuh-VirtualBox: /home/wazuh
root@wazuh-VirtualBox:/home/wazuh# sudo /var/ossec/bin/manage_agents -l
Available agents:
  ID: 001, Name: p1, IP: any
  ID: 002, Name: p3, IP: any
root@wazuh-VirtualBox:/home/wazuh#
```

**Figura 3.9** Identificación de los agentes que han sido agregados al servidor Wazuh

Seguidamente, se incluye el ID único del agente con el siguiente comando: **sudo /var/ossec/bin/agent\_groups -a -i <AGENT\_ID> -g Suricata -q**, donde el parámetro “-i” especifica qué ID se le va a agregar al grupo, en este caso será el 001 ya que corresponde al agente para ser monitorizado en el servidor Wazuh. Esto se verifica en la Figura 3.10.

```
root@wazuh-VirtualBox: /home/wazuh
root@wazuh-VirtualBox:/home/wazuh# sudo /var/ossec/bin/agent_groups -a -i 001 -g Suricata -q
```

**Figura 3.10** Configuración para incluir el agente en el grupo Suricata

Sumado a esto se debe ingresar al archivo de configuración del agente compartido del grupo Suricata mediante el siguiente comando: **nano /var/ossec/etc/shared/Suricata/agent.conf**; e ingresar la configuración respectiva que se visualiza en la Figura 3.11. Además, se comprueba que en el *dashboard* del servidor Wazuh ya se encuentra asignado el IDPS Suricata al agente correspondiente como se evidencia en la Figura 3.12.

```
root@wazuh-VirtualBox: /home/wazuh
GNU nano 6.2 /var/ossec/etc/shared/Suricata/agent.conf
<agent_config>
  <!-- Shared agent configuration here -->
</agent_config>
<agent_config>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
</agent_config>
```

Figura 3.11 Configuración del agente compartido del grupo Suricata

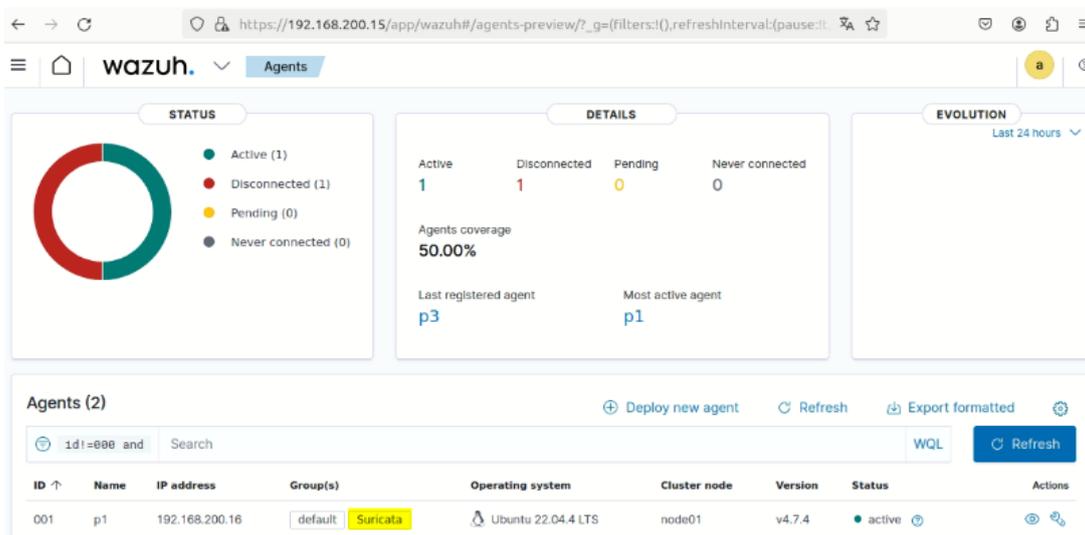


Figura 3.12 Agente Ubuntu 22.04 el cual pertenece al grupo Suricata

Después, se adapta la configuración de los registros de Suricata para que sean compatibles con la respuesta activa del servidor Wazuh, ya que se quiere mapear el campo "src\_ip" específicamente, donde este parámetro representa la dirección IP de origen de una actividad maliciosa. Por lo tanto, luego de configurar los decodificadores de los registros de Suricata que contengan el parámetro "src\_ip", son procesados adecuadamente y el parámetro "src\_ip" se mapeará a "srcip"; lo que asegurará que los scripts de respuesta activa de Wazuh funcionen correctamente. Para lo cual, se debe ingresar a la siguiente ruta con el comando: **nano /var/ossec/etc/decoders/local\_decoder.xml** y se agrega la configuración que se observa en la Figura 3.13.

```
root@wazuh-VirtualBox: /home/wazuh
GNU nano 6.2 /var/ossec/etc/decoders/local_decoder.xml

<decoder name="local_decoder_example">
  <program_name>local_decoder_example</program_name>
</decoder>

<decoder name="json">
  <prematch>^{\s*"</prematch>
</decoder>

<decoder name="json_child">
  <parent>json</parent>
  <regex type="pcre2">"src_ip": "([^\"]+)"</regex>
  <order>srcip</order>
</decoder>

<decoder name="json_child">
  <parent>json</parent>
  <plugin_decoder>JSON_Decoder</plugin_decoder>
</decoder>
```

**Figura 3.13** Configuración de un decodificador especial para el parámetro src\_ip

Por consiguiente, se procede a agregar las reglas a partir de Suricata; de esta forma en el servidor Wazuh se agregan las reglas para los posibles ataques que pueda sufrir el agente que es monitoreado. Para ingresar al archivo de configuración de reglas se ingresa mediante el comando: **nano /var/ossec/etc/rules/local\_rules.xml** y se agregan las reglas que se evidencian en la Figura 3.14.

Estas reglas son referidas para detectar ataques en específico que van a ser reportados por Suricata, en primer lugar se tienen las actividades sospechosas que están relacionadas con el uso de la herramienta de escaneo de red Nmap, esta regla tiene como objetivo principal detectar el uso de los scripts de Nmap “*Nmap Scripting Engine*” y proporciona una descripción rápida y clara de la regla; por lo que, identificará los intentos por parte de un atacante que esté utilizando Nmap para visualizar las vulnerabilidades en la red. Por otro lado, se encuentra la alerta para la detección de tráfico de la herramienta de Denegación de Servicio (DoS) GoldenEye, la descripción de la alerta es “*ET DOS GoldenEye DoS Tool Traffic*” la cual es una alerta detallada que ayuda a verificar que está sucediendo en el dispositivo final que es monitoreado por Wazuh.

```
root@wazuh-VirtualBox: /home/wazuh
GNU nano 6.2 /var/ossec/etc/rules/local_rules.xml

</group>

<group name="custom_active_response_rules,">
  <rule id="100200" level="12">
    <if_sid>86600</if_sid>
    <field name="event_type">^alert$</field>
    <match>ET DOS Inbound GoldenEye DoS attack</match>
    <description>GoldenEye DoS attack has been detected. </description>
    <mitre>
      <id>T1498</id>
    </mitre>
  </rule>

  <rule id="100201" level="12">
    <if_sid>86600</if_sid>
    <field name="event_type">^alert$</field>
    <match>ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)</match>
    <description>Nmap scripting engine detected. </description>
    <mitre>
      <id>T1595</id>
    </mitre>
  </rule>
</group>
```

**Figura 3.14** Asignación de reglas para las alertas de Suricata

Además, se ingresa la configuración del servidor Wazuh y se agrega una sección de *active-response*, la cual es utilizada para respuestas automáticas a eventos de seguridad en específico. Se ingresa el comando: **nano /var/ossec/etc/ossec.conf**, ver la Figura 3.15 donde se encuentra añadida la configuración correspondiente.

```
root@wazuh-VirtualBox: /home/wazuh
GNU nano 6.2 /var/ossec/etc/ossec.conf

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/kern.log</location>
</localfile>

</ossec_config>

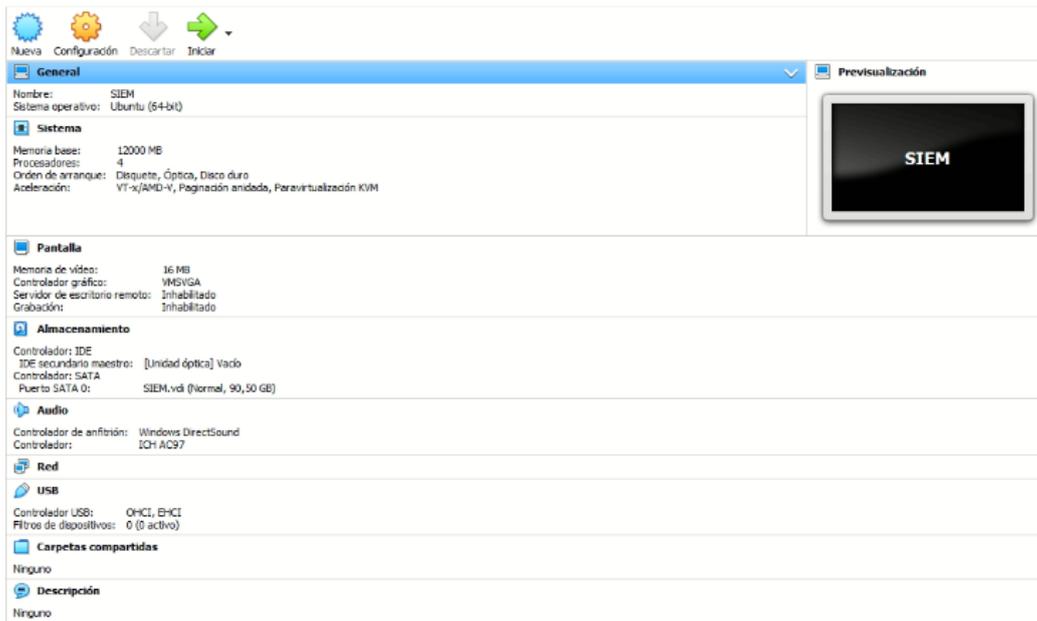
<ossec_config>
  <command>
    <name>firewall-drop</name>
    <executable>firewall-drop</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>
</ossec_config>

<ossec_config>
  <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>100200, 100201</rules_id>
    <timeout>180</timeout>
  </active-response>
</ossec_config>
```

**Figura 3.15** Adición de active-response a la configuración del servidor Wazuh

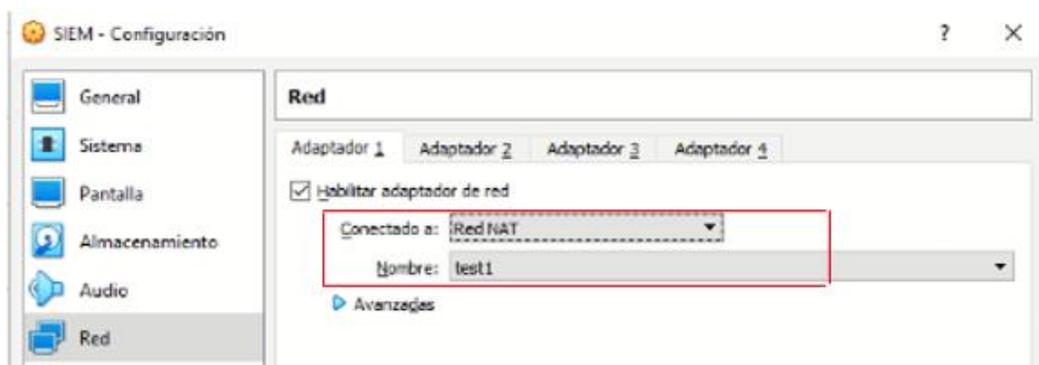
### Implementación del Servidor Splunk

Para la creación del servidor SIEM Splunk previamente se necesita configurar una máquina virtual en VirtualBox con sistema operativo Linux de la distribución Ubuntu versión 22.04, debe cumplir con las características mencionadas con anterioridad, las mismas que se evidencian en la Figura 3.16.



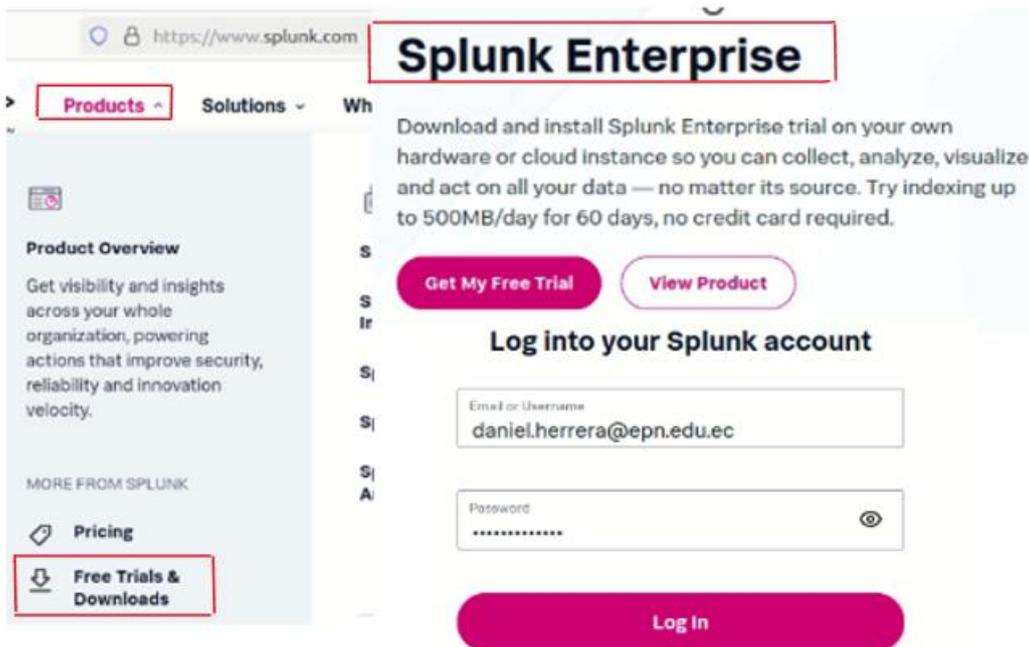
**Figura 3.16** Características de la máquina para Splunk

De igual forma, se debe seleccionar la red NAT interna que se creó con anterioridad que se evidencia en la Figura 3.2, para que asignen las direcciones IP de manera dinámica y así las máquinas ocupen direcciones dentro del rango de la dirección de red 192.168.200.0/24, ver Figura 3.17.



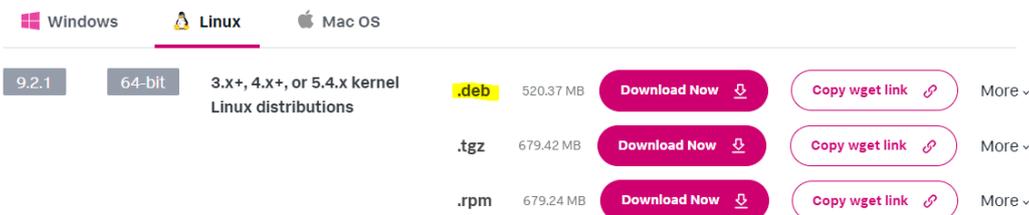
**Figura 3.17** Configuración de la red NAT interna en VirtualBox

Para instalar el servidor Splunk es necesario ingresar a la URL <https://www.splunk.com/>; donde se seleccionará la opción de “Products” y posteriormente “Free Trials&Downloads”, al seleccionar esa opción se desplegarán las diferentes versiones para iniciar la descarga y se deberá crear una cuenta para la descarga gratuita de este servicio del SIEM, seguidamente se selecciona la opción “Splunk Enterprise” que ofrece un amplio conjunto de características como búsqueda, monitoreo y análisis de datos de los puntos finales, como se puede evidenciar en la Figura 3.18.



**Figura 3.18** Descarga del servidor Splunk y creación de una cuenta

Posteriormente se seleccionará la versión y que sistema operativo se está utilizando como se evidencia en la Figura 3.19, en este caso es para Linux de la distribución Ubuntu, la cual pertenece al paquete .deb; una vez ya seleccionada se procede a realizar la descarga en la máquina que servirá como servidor de SPLUNK.



**Figura 3.19** Elección del sistema operativo

Una vez ya finalizada la descarga, se procederá a revisar que se encuentre el paquete descargado en la carpeta de Descargas, con el comando: **ls**, se listará la descarga y con el comando: **dpkg -i splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb**, se realiza la instalación del SIEM. El comando se lo evidencia en la Figura 3.20.

```
root@siem-VirtualBox: /home/siem/Descargas
root@siem-VirtualBox:/home/siem# ls
Descargas Documentos Escritorio Imágenes Música Plantillas Público snap Videos
root@siem-VirtualBox:/home/siem# cd Descargas/
root@siem-VirtualBox:/home/siem/Descargas# ls
splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
root@siem-VirtualBox:/home/siem/Descargas# dpkg -i splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
Seleccionando el paquete splunk previamente no seleccionado.
(Leyendo la base de datos ... 205407 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb ...
Desempaquetando splunk (9.2.1+78803f08aabb) ...
Configurando splunk (9.2.1+78803f08aabb) ...
/var/lib/dpkg/info/splunk.postinst: línea 60: curl: orden no encontrada
complete
```

Figura 3.20 Instalación del servidor Splunk

Al momento de completar la instalación se ingresa el comando: **cd /opt/**; ya que ahí se encuentra el archivo ejecutable para que Splunk inicie su sistema, seguido se ingresa el comando: **cd splunk/** y dentro de ese directorio se ingresa el comando: **cd bin/**; en el cual se iniciara el servicio de Splunk con el comando: **./splunk start**, como se puede visualizar en la Figura 3.21.

```
root@siem-VirtualBox: /opt/splunk/bin
siem@siem-VirtualBox:~$ sudo su
[sudo] contraseña para siem:
root@siem-VirtualBox:/home/siem# cd /opt/
root@siem-VirtualBox:/opt# cd splunk/
root@siem-VirtualBox:/opt/splunk# cd bin/
root@siem-VirtualBox:/opt/splunk/bin# ./splunk start
```

Figura 3.21 Activación del servicio de Splunk

Sumado a esto, se desplegará un acuerdo de términos y condiciones de la licencia que se instaló, lo que se aprecia en la Figura 3.22 el cual indica que, si se desea agregar dicha licencia, por lo que se procede a ingresar la letra “y” que indica que “si” está de acuerdo. Seguido se despliega un parámetro donde indica que *username* se desea asignar, en este caso “admin” y la contraseña que será asignada.

```
"Statement of Work" means the statements of work and/or any and all applicable
Orders, that describe the specific services to be performed by Splunk,
including any materials and deliverables to be delivered by Splunk.
Do you agree with this license? [y/n]: y

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
 * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
ERROR: Password did not meet complexity requirements. Password must contain at least:
 * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

Figura 3.22 Asignación de usuario y contraseña del servidor Splunk

A continuación, se tardará unos minutos en iniciar el servicio y por último indicará que el servicio está listo para ser visualizado en el navegador de la máquina virtual, como se evidencia en la Figura 3.23.

```
Waiting for web server at http://127.0.0.1:8000 to be available.....  
..... Done  
  
If you get stuck, we're here to help.  
Look for answers here: http://docs.splunk.com  
  
The Splunk web interface is at http://slem-VirtualBox:8000
```

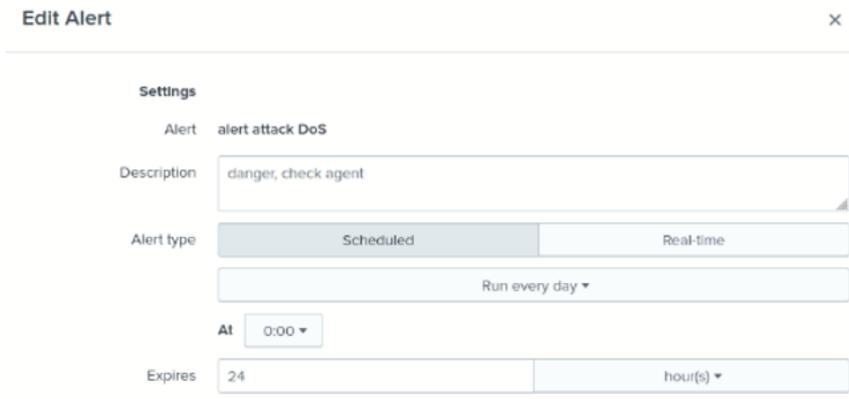
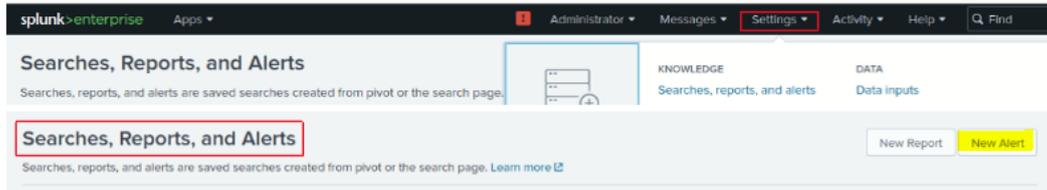
**Figura 3.23** Validación del servidor Splunk

Seguidamente, se abre el navegador de la máquina virtual y se ingresa la dirección IP de la máquina sumado con el puerto por defecto que posee la configuración de Splunk, que en este caso es el puerto “8000”, mediante este puerto los usuarios acceden y gestionan Splunk utilizando un navegador Web; esto se visualiza en la Figura 3.24. A su vez, se ingresó el usuario y contraseña que previamente se configuró.



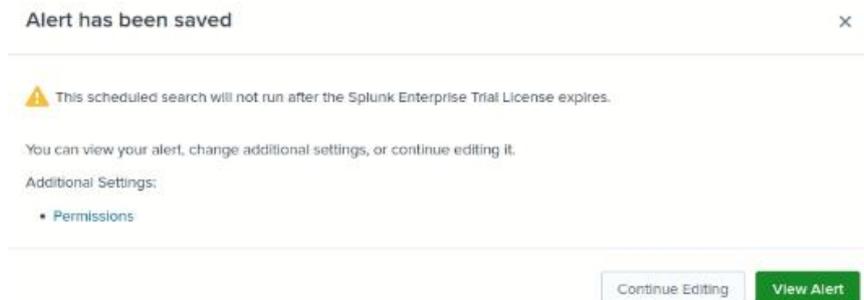
**Figura 3.24** Ingreso de credenciales hacia el servidor Splunk

Además, se creó una alerta relacionada con el ataque de *DoS* para recibir logs relacionados con el acceso erróneo hacia el servidor Web, para lo cual se ingresa a la pestaña de *settings*; donde se selecciona la opción de *Searches, Reports, and Alerts*, y se crea una nueva alerta, agregando la descripción que se desea visualizar; el ingreso y la configuración se observa en la Figura 3.25.



**Figura 3.25** Configuración de la alerta de DoS

Cabe recalcar que la alerta tendrá un periodo de duración, ya que se utilizó la versión gratuita de Splunk, por lo tanto, se evidencia en Figura 3.26 el mensaje de duración de dicha alerta.



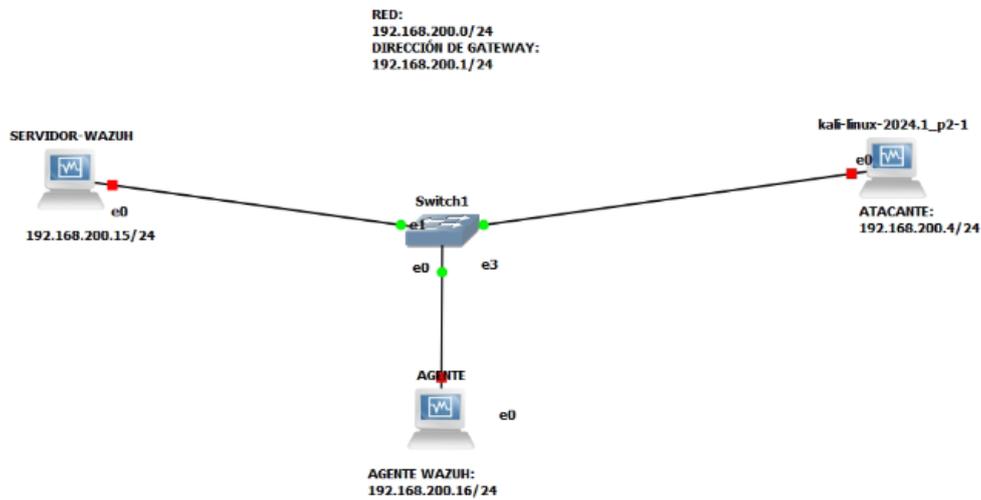
**Figura 3.26** Aviso de duración de la alerta creada

### 3.3 Implementación de la topología de red

#### Topología con el SIEM Wazuh

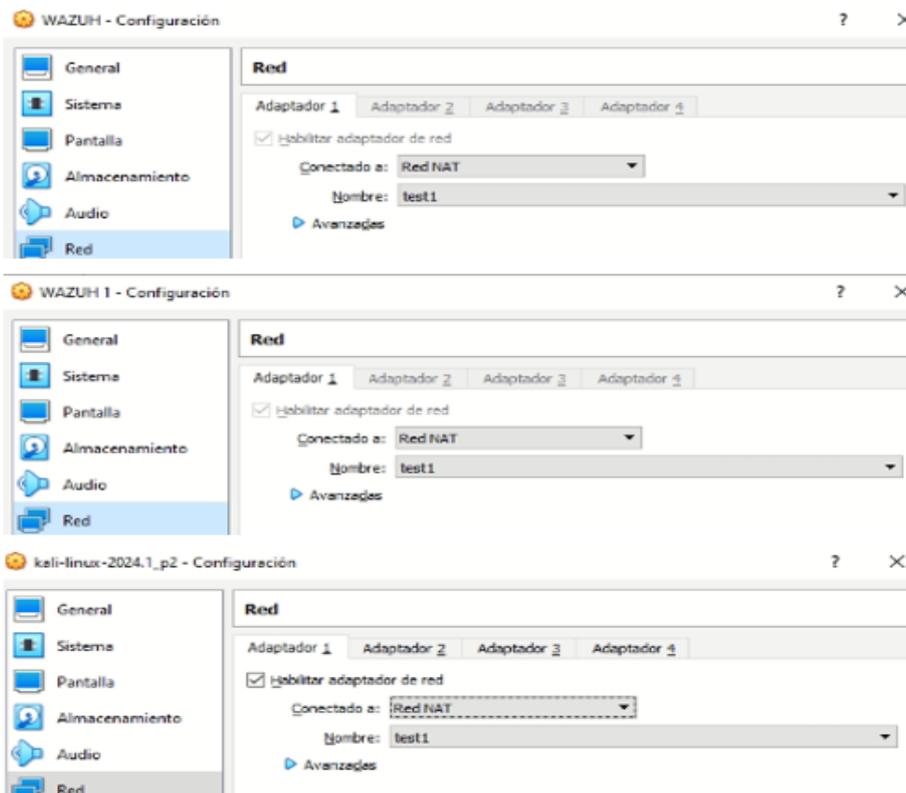
Para la topología se ha utilizado la aplicación de emulador de redes GNS3, en la topología se han utilizado máquinas virtuales las cuales están configuradas con el sistema operativo Linux basados en la distribución Ubuntu 22.04 y Kali Linux 2024.1, en la Figura 3.27 se puede visualizar la topología de red. Cabe recalcar que cada una tiene una finalidad en específico, ya que las máquinas Ubuntu son el servidor y agente del

SIEM Wazuh y la máquina de Kali Linux es el atacante en sí; además se utilizó un switch por defecto de GNS3.



**Figura 3.27** Topología de red con el SIEM Wazuh

De esta manera, para que las máquinas tengan conectividad entre ellas se ha configurado una red NAT interna con el nombre “test1”. Al momento de configurar sus adaptadores de red las tres máquinas deben poseer la red NAT interna que se creó y se asignarán las direcciones IP de manera dinámica que estén en el rango de la dirección de red 192.168.200.0/24; esto se puede evidenciar en la Figura 3.28.



**Figura 3.28** Configuración del adaptador de red para las máquinas virtuales

## Instalación del agente Wazuh y creación del servidor Web

Para la creación del agente se necesita una máquina virtual Linux basada en la distribución de Ubuntu 22.04, donde las características para funcionamiento se pueden apreciar en la Figura 3.29.

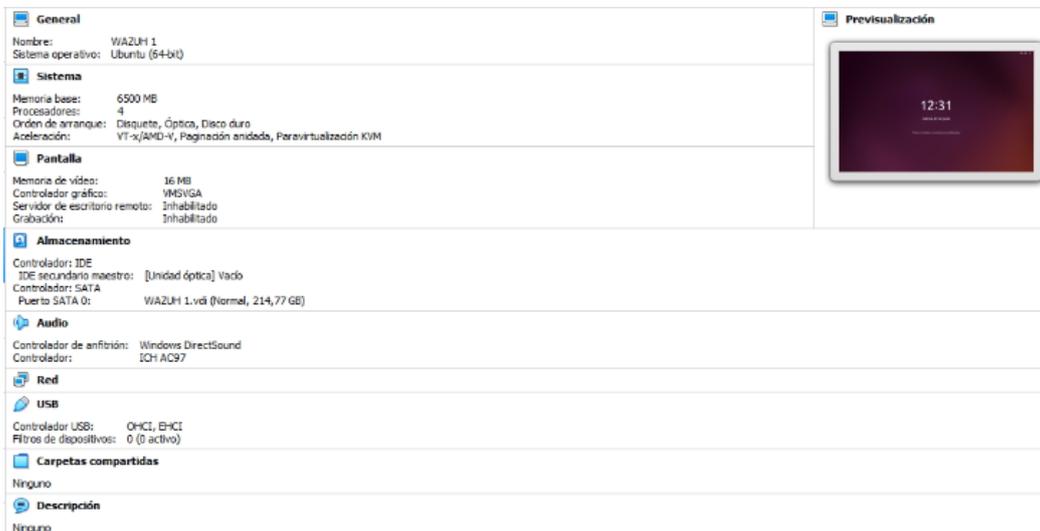


Figura 3.29 Características de la máquina virtual víctima y agente

Para proceder con la instalación del agente se ingresa a la consola de la máquina que será el agente (Ubuntu 22.04) y se ingresa el siguiente comando: **wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent\_4.7.4-1\_amd64.deb && sudo WAZUH\_MANAGER='192.168.200.15' WAZUH\_AGENT\_GROUP='default' WAZUH\_AGENT\_NAME='p1' dpkg -i ./wazuh-agent\_4.7.4-1\_amd64.deb**; el comando proporcionado se puede verificar en la Figura 3.7 el cual iniciará la instalación del agente en la máquina, en la Figura 3.30 se puede evidenciar el proceso de instalación.

```
root@wazuh-VirtualBox:/home/wazuh# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb && sudo WAZUH_MANAGER='192.168.200.15' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='p1' dpkg -i ./wazuh-agent_4.7.4-1_amd64.deb
--2024-06-25 11:58:31-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_amd64.deb
Resolviendo packages.wazuh.com (packages.wazuh.com)... 65.8.248.62, 65.8.248.60, 65.8.248.126, ...
Conectando con packages.wazuh.com (packages.wazuh.com)[65.8.248.62]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 9372734 (8,9M) [binary/octet-stream]
Guardando como: 'wazuh-agent_4.7.4-1_amd64.deb'

wazuh-agent_4.7.4-1_amd64.deb 100%[=====>] 8,94M 4,53MB/s en 2,0s
```

Figura 3.30 Instalación del agente Wazuh

Una vez finalizada la instalación del agente, se procedió a colocar los siguientes comandos: **sudo systemctl daemon-reload**, **sudo systemctl enable wazuh-agent**, **sudo systemctl start wazuh-agent**, los cuales realizan el proceso de recargar, habilitar e iniciar el funcionamiento como agente de Wazuh, ver la Figura 3.31.

```
root@wazuh-VirtualBox:/home/wazuh# sudo systemctl daemon-reload
root@wazuh-VirtualBox:/home/wazuh# sudo systemctl enable wazuh-agent
root@wazuh-VirtualBox:/home/wazuh# sudo systemctl start wazuh-agent
root@wazuh-VirtualBox:/home/wazuh#
```

**Figura 3.31** Comandos para recargar la configuración del agente Wazuh

Además, en el agente se creará un servidor Web que actuará como víctima, para ello se debe agregar el comando: **sudo apt-get install apache2**; como se aprecia en la Figura 3.32 y de esta forma procede a instalar el servidor en la máquina que es la víctima y agente.

```
root@wazuh-VirtualBox:/home/wazuh# sudo apt-get install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Paquetes sugeridos:
 apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Se instalarán los siguientes paquetes NUEVOS:
 apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 actualizados, 8 nuevos se instalarán, 0 para eliminar y 142 no actualizados.
Se necesita descargar 1.919 kB de archivos.
Se utilizarán 7.721 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapr1 amd64 1.7.0-8ubuntu0.22.04.1 [108 kB]
Des:2 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-5ubuntu4.22.04.2 [92,8 kB]
Des:3 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-5ubuntu4.22.04.2 [11,3 kB]
Des:4 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1.6.1-5ubuntu4.22.04.2 [9,170 B]
Des:5 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-bin amd64 2.4.52-1ubuntu4.9 [1.347 kB]
Des:6 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-data all 2.4.52-1ubuntu4.9 [165 kB]
Des:7 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-utils amd64 2.4.52-1ubuntu4.9 [88,7 kB]
Des:8 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2 amd64 2.4.52-1ubuntu4.9 [97,9 kB]
Descargados 1.919 kB en 2s (1.189 kB/s)
```

**Figura 3.32** Instalación del servidor Web Apache2

De esta forma, con el comando: **sudo systemctl start apache2**; se está iniciando el servidor apache y para verificar su estado se coloca el comando: **sudo systemctl status apache2**; y se verifica que esté en estado “active(running)”; ver la Figura 3.33.

```
root@wazuh-VirtualBox:/home/wazuh# sudo systemctl start apache2
root@wazuh-VirtualBox:/home/wazuh# sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-06-25 12:12:37 -05; 1min 27s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 21189 (apache2)
    Tasks: 55 (limit: 4483)
   Memory: 4.9M
     CPU: 59ms
   CGroup: /system.slice/apache2.service
           └─21189 /usr/sbin/apache2 -k start
             └─21191 /usr/sbin/apache2 -k start
               └─21192 /usr/sbin/apache2 -k start

Jun 25 12:12:37 wazuh-VirtualBox systemd[1]: Starting The Apache HTTP Server...
Jun 25 12:12:37 wazuh-VirtualBox apachectl[21188]: AH00558: apache2: Could not reliably determine the server's fully
Jun 25 12:12:37 wazuh-VirtualBox systemd[1]: Started The Apache HTTP Server.
root@wazuh-VirtualBox:/home/wazuh#
```

**Figura 3.33** Comandos para iniciar y verificar el estado del servidor Web

Sumado a esto, se modificará el archivo html del servidor Web apache que viene por defecto, para ello se ingresa el siguiente comando: **cd /var/www/html/** y con el comando **ls** se lista el archivo "index.html" el cual se modificó, ver la Figura 3.34. Al ingresar al archivo se borra la configuración inicial y se agrega una nueva configuración, ya que la página Web mostrará la marca e identificación que el usuario haya creado en lugar de la página Web que Apache tiene por defecto, como se puede observar en la Figura 3.35.

```
root@wazuh-VirtualBox: /var/www/html
root@wazuh-VirtualBox:~# cd /var/www/html/
root@wazuh-VirtualBox:/var/www/html# ls
index.html
root@wazuh-VirtualBox:/var/www/html#
```

Figura 3.34 Ingreso al archivo index.html

```
GNU nano 6.2 index.html
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Mi primera página web</title>
</head>
<body>
  <header>
    <h1>Bienvenido a mi página web</h1>
  </header>

  <nav>
    <ul>
      <li><a href="servidor_web_t1.html" target="_blank">Inicio</a></li>
      <li><a href="#">Acerca de</a></li>
      <li><a href="#">Contacto</a></li>
    </ul>
  </nav>

  <main>
    <h2>Contenido principal</h2>
    <p>¡Esta es mi primera página web creada con HTML!</p>
  </main>

  <footer>
    <p>&copy; 2024 Mi primera página web</p>
  </footer>
</body>
</html>
```

Figura 3.35 Modificación del archivo index.html

Igualmente, para que el servidor Web soporte menos peticiones para su conexión se modificó la configuración de sus módulos, para que disminuya los recursos y solicitudes hacia el mismo; para esto se accedió a la ruta donde se guardan los archivos de configuración para los módulos que están activos en el servidor, por lo tanto, con el comando: **sudo nano /etc/apache2/mods-available/mpm\_prefork.conf; sudo nano /etc/apache2/mods-available/mpm\_worker.conf; sudo nano /etc/apache2/mods-available/mpm\_event.conf**, y se ingresa la configuración deseada.

En la Figura 3.36 se evidencian las modificaciones que se hicieron en el archivo **mpm\_prefork.conf**, para esto se redujo la cantidad **StartServers** que indica el número de subprocesos que se inician, **MinSpareServers** indica el número mínimo subprocesos inactivos que soporta el servidor, **MaxSpareServers** indica el número máximo de subprocesos inactivos que soporta el servidor, **MaxRequestWorkers** especifica el número máximo de conexiones acepta el servidor, **MaxConnectionsPerChild** especifica el número máximo de conexiones que el subproceso puede tener antes de terminar. De igual manera, los archivos **mpm\_worker.conf** y **mpm\_event.conf**, contienen parámetros que fueron reducidos tales como **MinSpareThreads/MaxSpareThreads** que indican el mínimo-máximo de threads inactivos que permite apache mantener para establecer una nueva conexión, **ThreadLimit** indica el número máximo de threads por subproceso y **ThreadsPerChild** que indica el número de threads que cada subproceso creará al inicio.

```

GNU nano 6.2 /etc/apache2/mods-available/mpm_prefork.conf
# prefork MPM
# StartServers: number of server processes to start
# MinSpareServers: minimum number of server processes which are kept spare
# MaxSpareServers: maximum number of server processes which are kept spare
# MaxRequestWorkers: maximum number of server processes allowed to start
# MaxConnectionsPerChild: maximum number of requests a server process serves

<IfModule mpm_prefork_module>
    StartServers          2
    MinSpareServers       2
    MaxSpareServers       5
    MaxRequestWorkers     5
    MaxConnectionsPerChild 3000
</IfModule>

GNU nano 6.2 /etc/apache2/mods-available/mpm_worker.conf
# worker MPM
# StartServers: initial number of server processes to start
# MinSpareThreads: minimum number of worker threads which are kept spare
# MaxSpareThreads: maximum number of worker threads which are kept spare
# ThreadLimit: ThreadsPerChild can be changed to this maximum value during a
#               graceful restart. ThreadLimit can only be changed by stopping
#               and starting Apache.
# ThreadsPerChild: constant number of worker threads in each server process
# MaxRequestWorkers: maximum number of threads
# MaxConnectionsPerChild: maximum number of requests a server process serves

<IfModule mpm_worker_module>
    StartServers          2
    MinSpareThreads       2
    MaxSpareThreads       5
    ThreadLimit           32
    ThreadsPerChild       15
    MaxRequestWorkers     10
    MaxConnectionsPerChild 0
</IfModule>

GNU nano 6.2 /etc/apache2/mods-available/mpm_event.conf
# event MPM
# StartServers: initial number of server processes to start
# MinSpareThreads: minimum number of worker threads which are kept spare
# MaxSpareThreads: maximum number of worker threads which are kept spare
# ThreadsPerChild: constant number of worker threads in each server process
# MaxRequestWorkers: maximum number of worker threads
# MaxConnectionsPerChild: maximum number of requests a server process serves

<IfModule mpm_event_module>
    StartServers          2
    MinSpareThreads       20
    MaxSpareThreads       20
    ThreadLimit           32
    ThreadsPerChild       15
    MaxRequestWorkers     25
    MaxConnectionsPerChild 10
</IfModule>

```

**Figura 3.36** Modificación de los recursos del servidor Web

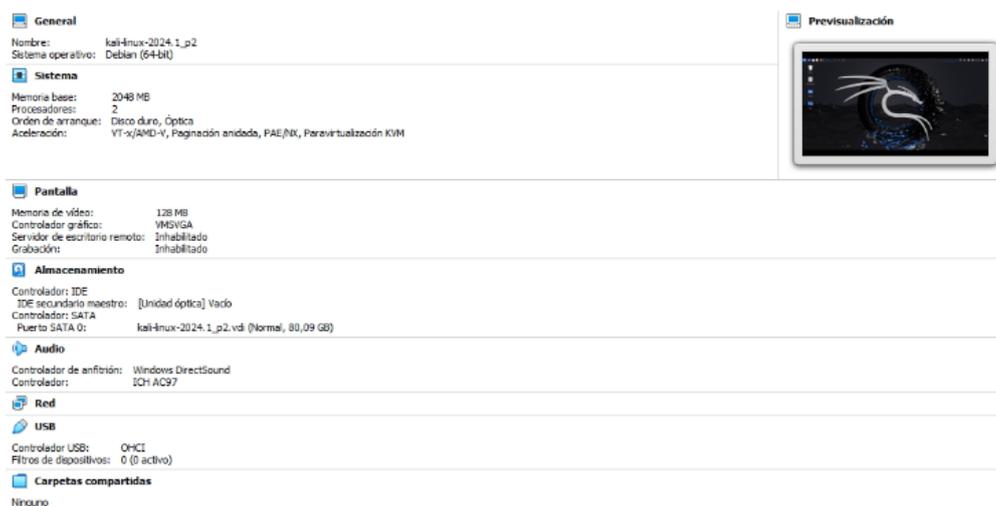
Luego de la configuración y modificación adecuada, se accedió al navegador de la máquina virtual y se ingresó la dirección IP, que en este caso es: 192.168.200.16, al observar la Figura 3.37 se muestra el funcionamiento de la página Web.



**Figura 3.37** Ingreso a la página Web creada

### Instalación de la máquina atacante

Para la creación de la máquina atacante se debe descargar la OVA de Kali Linux 2024.1, la cual se encuentra en la URL: <https://www.kali.org/get-kali/#kali-virtual-machines>. De esta forma, la configuración de la máquina virtual será por defecto y no se hará ningún cambio en sus características iniciales, tomando en cuenta sus credenciales de acceso son “kali” tanto para usuario como contraseña, ver Figura 3.38.



**Figura 3.38** Instalación de la máquina atacante

Para llevar a cabo el ataque, se utilizará la herramienta Slowhttptest, que permite ejecutar un ataque de DoS al aprovechar las debilidades en la gestión de conexiones HTTP lentas por parte de los servidores. Al mantener abiertas las conexiones HTTP con el servidor objetivo durante un período prolongado, esta herramienta consume los

recursos del servidor de manera gradual, hasta agotarlos por completo, lo que eventualmente conduce a la inhabilitación del servicio.

Asimismo, se utilizó la herramienta Pentmenu, que ofrece una interfaz sencilla y fácil de entender para ejecutar ataques de DoS. En este caso, provoca una inundación masiva de solicitudes dirigidas a los recursos de los servidores web, lo que conduce a la inhabilitación del servicio y afecta a los usuarios legítimos.

Seguido a esto se accede al terminal de la máquina Kali Linux y se ejecutó el comando: **sudo apt-get update** para actualizar los paquetes de instalación y luego se procede a instalar dos herramientas que realizarán el ataque *DoS*. La primera es “Slowhttptest”, para iniciar su instalación se ingresa el comando: **sudo apt install slowhttptest**, el cual iniciará la descarga de la herramienta como se visualiza en la Figura 3.39.

```
(root@kali) ~ - [~/home/kali]
# sudo apt-get update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done

(root@kali) ~ - [~/home/kali]
# sudo apt install slowhttptest
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
slowhttptest is already the newest version (1.9.0-1+b1).
The following packages were automatically installed and are no longer required:
  appstream fonts-noto-color-emoji gir1.2-cloudproviders-0.3.0 gir1.2-freedesktop-dev gir1.2-glib-2.0-dev gir1.2-gtk-2.0 libappstre
libdeflate-dev libegl1-mesa-dev libepoxy-dev libfontconfig-dev libfreetype-dev libfribidi-dev libglib2.0-dev-bin libgraphite2-dev
libjpeg-dev libjpeg62-turbo-dev liblerc-dev liblzma-dev libmount-dev libnsl-dev libpcre2-32-0 libpcre2-dev libpcre2-posix3 libpix
libsharpyuv-dev libstemmer0d libthai-dev libtiff-dev libtiffxx6 libtirpc-dev libwayland-bin libwayland-dev libwebp-dev libwebpdec
libxcursor-dev libxdamage-dev libxfixes-dev libxft-dev libxi-dev libxinerama-dev libxkbcommon-dev libxmlb2 libxrandr-dev libxrend
wayland-protocols
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1299 not upgraded.
```

Figura 3.39 Instalación de la herramienta Slowhttptest

La segunda herramienta que será instalada en la máquina atacante es “Pentmenu”, de esta forma en el terminal de la máquina se ingresa el siguiente comando: **wget https://raw.githubusercontent.com/GinjaChris/pentmenu/master/pentmenu**; que iniciará la descarga de la herramienta para después hacerlo ejecutable con el comando: **chmod +x ./pentmenu**; así se puede verificar en la Figura 3.40.

```
File Actions Edit View Help

(root@kali) ~ - [~/home/kali]
# wget https://raw.githubusercontent.com/GinjaChris/pentmenu/master/pentmenu
--2024-06-25 14:53:32-- https://raw.githubusercontent.com/GinjaChris/pentmenu/master/pentmenu
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)[185.199.110.133]:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 49548 (48K) [text/plain]
Saving to: 'pentmenu.1'

pentmenu.1
100%[=====>] 48.39K --.-KB/s in 0.005s

2024-06-25 14:53:33 (10.4 MB/s) - 'pentmenu.1' saved [49548/49548]

(root@kali) ~ - [~/home/kali]
# chmod +x ./pentmenu
```

Figura 3.40 Instalación de la herramienta Pentmenu

## Ejecución del ataque al agente de Wazuh

En primer lugar, desde la máquina atacante se realiza la ejecución del comando: **sudo nmap -A 192.168.200.16**; donde “nmap” es la herramienta que permite escanear de manera completa un dispositivo o sistema en la red, el parámetro “-A” que permite detectar el sistema operativo, la detección de los servicios que se brindan en esa dirección IP, ejecutar scripts de escaneo y lo más relevante observar qué puertos están habilitados. En este caso el puerto 80/http está abierto; se muestra de manera detallada las características del sistema objetivo en la Figura 3.41.

```
(root@kali)-[~/home/kali]
└─$ sudo nmap -A 192.168.200.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 15:19 EDT
Nmap scan report for 192.168.200.16
Host is up (0.00047s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Mi primera p\xC3\xA1gina web
MAC Address: 08:00:27:1A:50:E8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.47 ms  192.168.200.16

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.18 seconds
```

Figura 3.41 Ejecución de la herramienta Nmap

Para proceder a la realizar el ataque se comprueba que el acceso al servidor Web se encuentre disponible, por lo que se accederá a través del navegador Web de Kali Linux con la dirección IP asignada al servidor por parte de la red NAT interna, la cual es 192.168.200.16, como se muestra en la Figura 3.42.

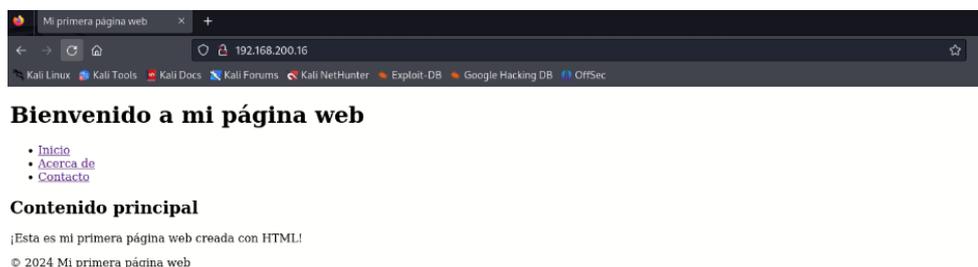
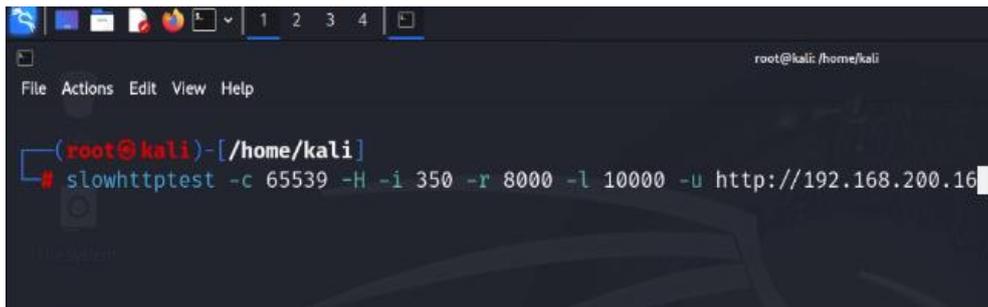


Figura 3.42 Acceso al servidor Web Apache2

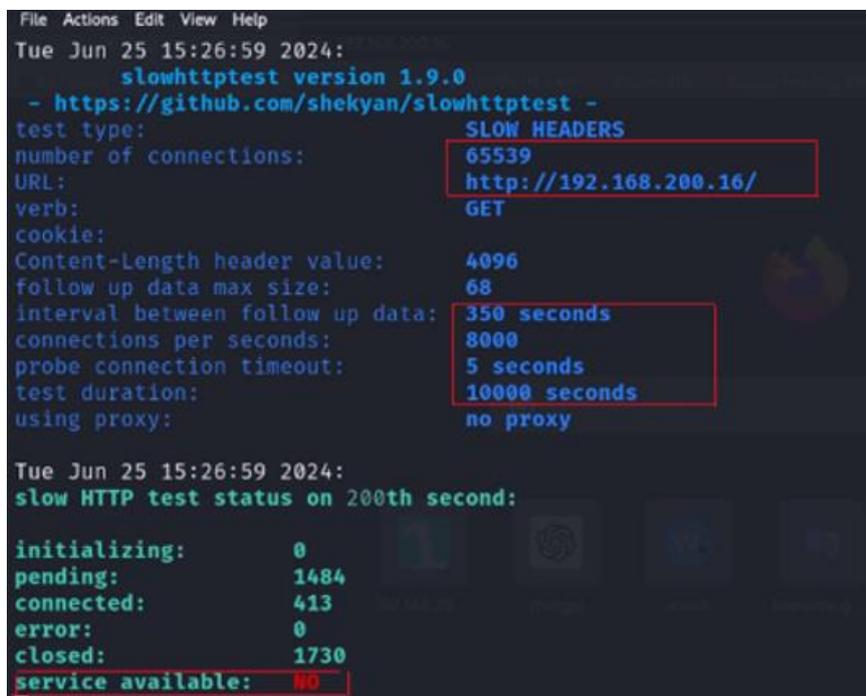
Una vez ya comprobado el acceso al servidor Web, se procedió a ejecutar la herramienta “Slowhttptest”, mediante la consola de Kali Linux donde se ingresó el comando: **slowhttptest -c 65539 -H -i 350 -r 8000 -l 10000 -u http://192.168.200.16**, ver Figura 3.43.



```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[~/home/kali]
└─# slowhttptest -c 65539 -H -i 350 -r 8000 -l 10000 -u http://192.168.200.16
```

**Figura 3.43** Ejecución del comando en el terminal

Al momento de ingresar el comando se despliega un menú donde indica el estado del servidor, donde “*service-available*” indica si está disponible o no; en la Figura 3.44 se observa que “*service-available: NO*”, por lo tanto, no está disponible. De igual forma se observan los parámetros que se colocaron en la Figura 3.43, donde el parámetro “*-c 65539*” especifica el total de conexiones que se harán hacia el servidor, el parámetro “*-H*” muestra el tipo de ataque que se empleará, que es el *slow headers* (cabeceras lentas), lo que implica que se enviarán cabeceras HTTP muy lentas para consumir los recursos del servidor, el parámetro “*-i*” indica el intervalo del envío de cada paquete de datos, “*-r*” detalla la velocidad con la que se envían las nuevas conexiones al servidor, “*-l*” indica la duración de la prueba medidas en segundos y por último “*-u*” indica la dirección IP que será atacada.



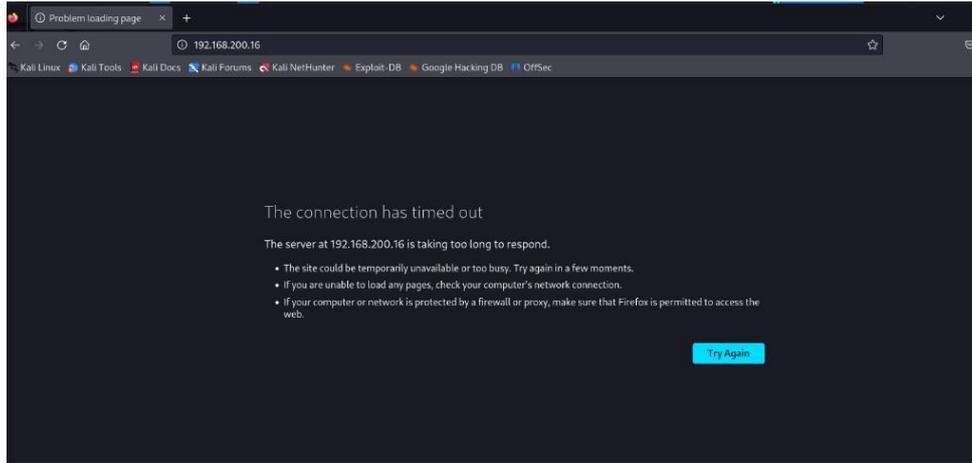
```
File Actions Edit View Help
Tue Jun 25 15:26:59 2024:
slowhttptest version 1.9.0
- https://github.com/shekya/slowhttptest -
test type: SLOW HEADERS
number of connections: 65539
URL: http://192.168.200.16/
verb: GET
cookie:
Content-Length header value: 4096
follow up data max size: 68
interval between follow up data: 350 seconds
connections per seconds: 8000
probe connection timeout: 5 seconds
test duration: 10000 seconds
using proxy: no proxy

Tue Jun 25 15:26:59 2024:
slow HTTP test status on 200th second:

initializing: 0
pending: 1484
connected: 413
error: 0
closed: 1730
service available: 60
```

**Figura 3.44** Ejecución de la herramienta Slowhttptest

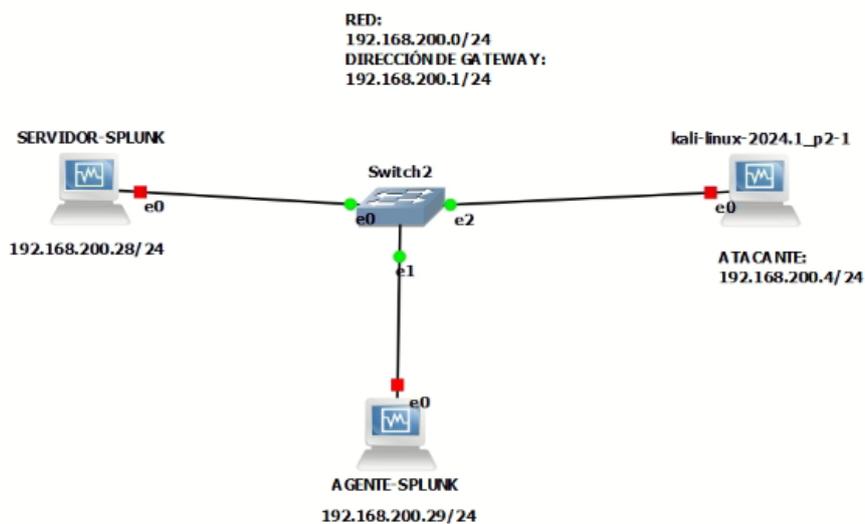




**Figura 3.46** Intento de conexión al servidor caído

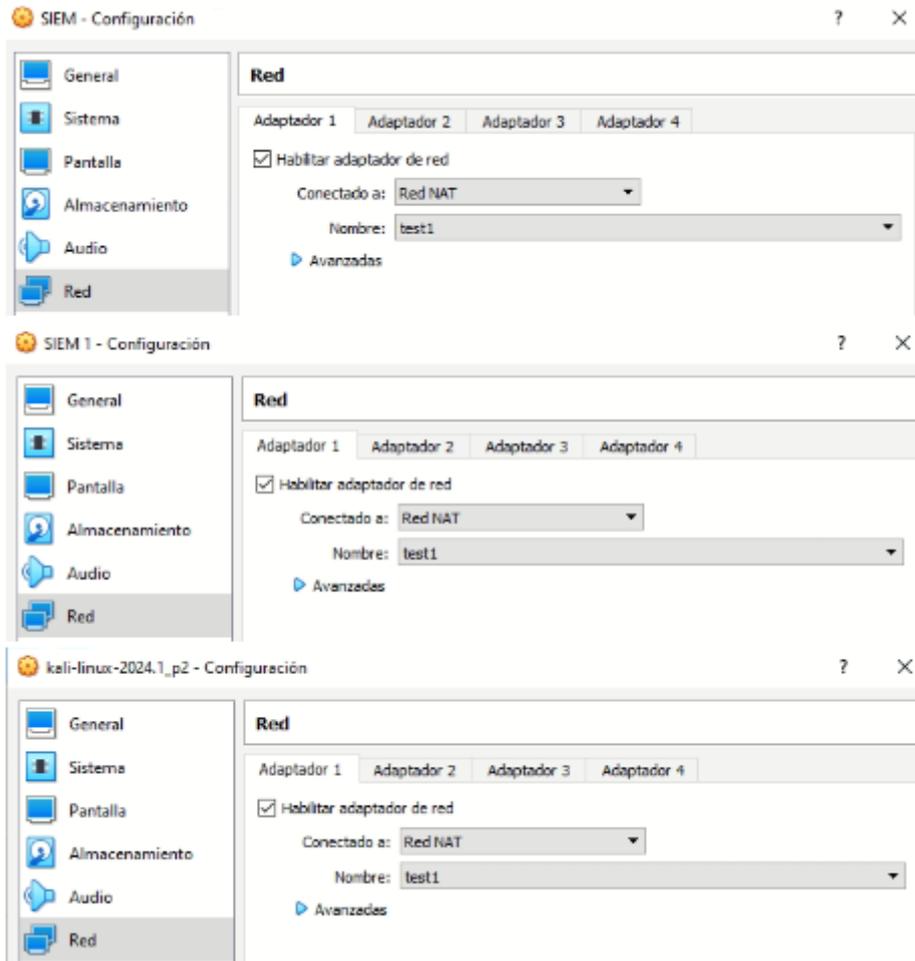
### Topología con el SIEM Splunk

La topología implementada se ha realizado con la aplicación de emulador de redes GNS3, de la misma manera que se realizó con el SIEM Wazuh. La topología tiene un escenario similar donde se utilizó una máquina virtual para el servidor y agente, que fue configurada con el sistema operativo Linux basados en la distribución Ubuntu versión 22.04, y la máquina atacante es Kali Linux 2024.1 será la misma que se configuró previamente, la topología se muestra en Figura 3.47; cabe recalcar que se utilizó un switch por defecto de GNS3.



**Figura 3.47** Topología de red con el SIEM Splunk

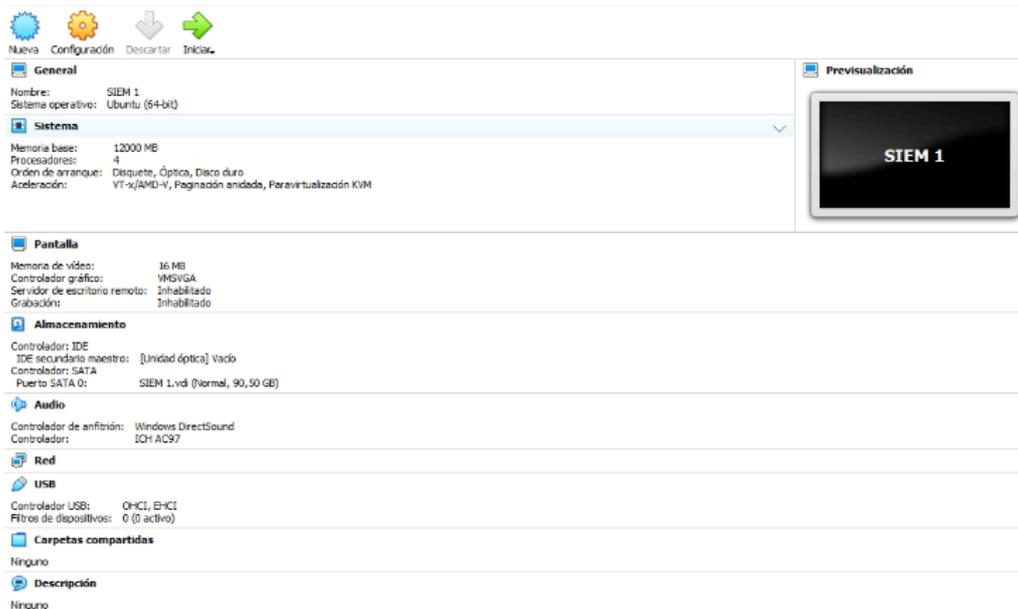
De igual manera, para que las máquinas tengan conectividad entre sí deben estar configuradas con su adaptador de red NAT interna con el nombre “test1”, y se asignarán las direcciones IP de manera dinámica, mismas que se encuentren en el rango de la dirección de red 192.168.200.0/24; esto se observa en la Figura 3.48.



**Figura 3.48** Configuración del adaptador de red para las máquinas virtuales

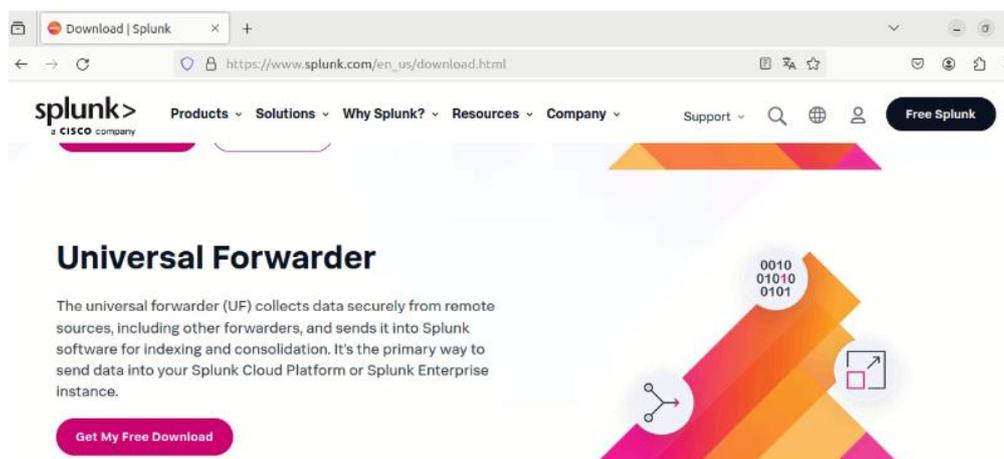
### **Instalación del agente Splunk y creación del servidor Web**

Para la configuración e instalación del agente, servidor Web, víctima se utilizará una máquina virtual con el sistema operativo Linux basado en la distribución Ubuntu versión 22.04; de esta forma en la Figura 3.49 se aprecian las características para su funcionamiento.



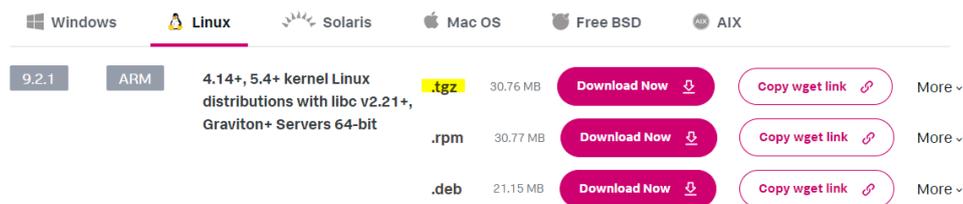
**Figura 3.49** Características de la máquina virtual víctima y agente

Para iniciar con la descarga del agente, se ingresa a la URL [https://www.splunk.com/en\\_us/download.html](https://www.splunk.com/en_us/download.html); donde se escogerá la opción de *Universal Forwarder* que se visualiza en la Figura 3.50, la cual ayudará a conectar la máquina que es agente a la estancia del servidor Splunk, de manera que reciba logs que se puedan visualizar en el SIEM e interpretarlos.



**Figura 3.50** Elección de la descarga para el agente Splunk

Sumado a esto se elegirá el sistema operativo correspondiente, que en este caso es Linux y el paquete de descarga que es “.tgz”; cabe recalcar que la versión del servidor y el agente deben ser iguales para que funcione de manera adecuada, ver Figura 3.51.



**Figura 3.51** Elección del sistema operativo y paquete de descarga

Una vez ya completada la descarga, se verifica que el archivo se encuentre en la carpeta de descargas, donde se listará los archivos con el comando: **ls**, y se procederá a ingresar el comando: **tar xvzf splunkforwarder-9.2.1-78803f08aabb-Linux-armv8.tgz**, el cual iniciará el desempaque del instalador, como se puede observar en la Figura 3.52.

```

root@siem-VirtualBox: /home/siem/Descargas# ls
splunkforwarder-9.2.1-78803f08aabb-Linux-armv8.tgz
root@siem-VirtualBox: /home/siem/Descargas# tar xvzf splunkforwarder-9.2.1-78803f08aabb-Linux-armv8.tgz
splunkforwarder/
splunkforwarder/swldtag/
splunkforwarder/swldtag/splunk-UniversalForwarder-primary.swldtag
splunkforwarder/share/
splunkforwarder/share/splunk/
splunkforwarder/share/splunk/3rdparty/
splunkforwarder/share/splunk/3rdparty/Copyright-for-openldap-2.4.45.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-opentracing-cpp-1.6.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-xxHash-0.6.5.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-double-conversion-3.0.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-cpp-TimSort-2.1.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-jaeger-client-cpp-0.7.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-json-3.8.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-lilarchive-3.6.2.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-pcre2-10.40.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-openssl-1.0.2zj.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-xmlsec1-1.2.24.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-libxslt-1.1.34.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-thrift-0.14.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-h3-v3.4.2.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-prometheus-cpp-0.9.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-robin-map-v0.2.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-lz4-1.9.4.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-zstd-1.5.0.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-re2-2018-12-01.txt
splunkforwarder/share/splunk/3rdparty/Copyright-for-libxml2-2.9.10.txt
splunkforwarder/share/splunk/cli-command-completion.sh

```

**Figura 3.52** Instalación del agente Splunk

De esta forma, al terminar la instalación se debe ingresar al directorio opt con el comando: **cd /opt/**, y verificar que se encuentre el directorio de splunkforwarder, para esto se debe ingresar con el comando: **cd splunkforwarder/**, e ingresar al directorio bin con el comando: **cd bin** y, por último, verificar que se encuentre el script splunk para completar la inicialización del agente, como se puede evidenciar en la Figura 3.53.

```

root@siem-VirtualBox: /home/siem/Descargas
siem@siem-VirtualBox: /opt/splunkforwarder/bin

siem@siem-VirtualBox: ~$ cd /opt/
siem@siem-VirtualBox: /opt$ ls
splunkforwarder
siem@siem-VirtualBox: /opt$ cd splunkforwarder/
siem@siem-VirtualBox: /opt/splunkforwarder$ ls
bin          etc          lib          README-splunk.txt  swldtag
snake       ftr         license-eula.txt  share              uf
copyright.txt  include  openssl      splunkforwarder-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest  var
siem@siem-VirtualBox: /opt/splunkforwarder$ cd bin
siem@siem-VirtualBox: /opt/splunkforwarder/bin$ ls
2to3-3.7  copyright.txt  idle3      pip3      pzippng      pydoc3      slim      supervisor-simulator
btool    easy_install-3.7  idle3.7   pip3.7   pzipantopng  pydoc3.7   splunk    wheel
btprobe  genRootCA.sh    openssl   pzipchunkpng  pzipnglsch  53benchmark  splunkd
bzzip2   genSignedServerCert.sh  pcre2-config  pzipforgepng  pzipngtopan  scripts     splunkmon
classify genWebCert.sh    ptd_check.sh  pzipgreypng  pzipweavepng  setSplunkEnv  splunk-tlsd

```

Figura 3.53 Verificación del script splunk para iniciar el agente

Igualmente para iniciar el servicio del agente, se debe ingresar el comando: **./splunk start**, donde se mostrará un acuerdo de términos y condiciones donde se debe aceptar dichos términos, para activar el servicio sin inconvenientes, la ejecución del comando se lo visualiza en la Figura 3.54.

```

root@siem-VirtualBox: /opt/splunkforwarder/bin

root@siem-VirtualBox: /opt/splunkforwarder/bin# ./splunk start
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

Splunk> Australian for grep.

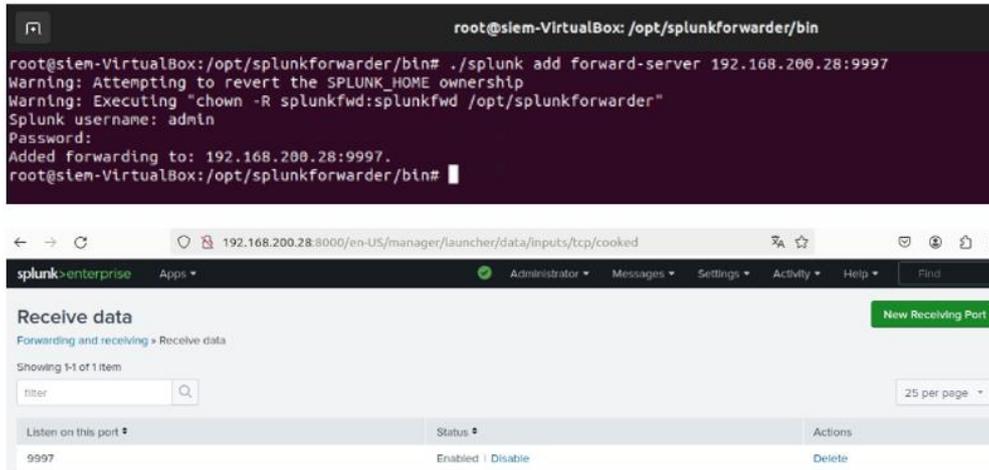
Checking prerequisites...
  Checking mgmt port [8089]: open
  Creating: /opt/splunkforwarder/var/run/splunk/appserver/l18n
  Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/stati
c/css
  Creating: /opt/splunkforwarder/var/run/splunk/upload
  Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
  Creating: /opt/splunkforwarder/var/run/splunk/search_log
  Creating: /opt/splunkforwarder/var/spool/splunk
  Creating: /opt/splunkforwarder/var/spool/dirmoncache
  Creating: /opt/splunkforwarder/var/lib/splunk/authDb
  Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
  Checking conf files for problems...
  Done
  Checking default conf files for edits...
  Validating installed files against hashes from '/opt/splunkforwarder/splunkfo
rwarder-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest'
  All installed files intact.
  Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

```

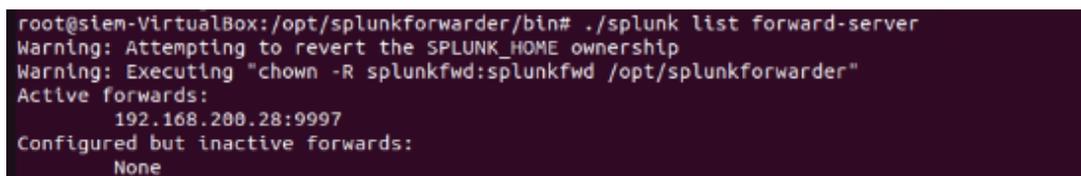
Figura 3.54 Activación del servicio del agente de Splunk

Ya iniciado el servicio, se agregó el agente de Splunk al servidor con el comando: **./splunk add forward-server 192.168.200.28:9997**; que se evidencia en la Figura 3.55, donde la dirección IP del servidor debe estar en conjunto con el puerto que se creará en el servidor, en este caso es el puerto 9997, que es utilizado para la recepción de los datos de *Universal Forwarder*.



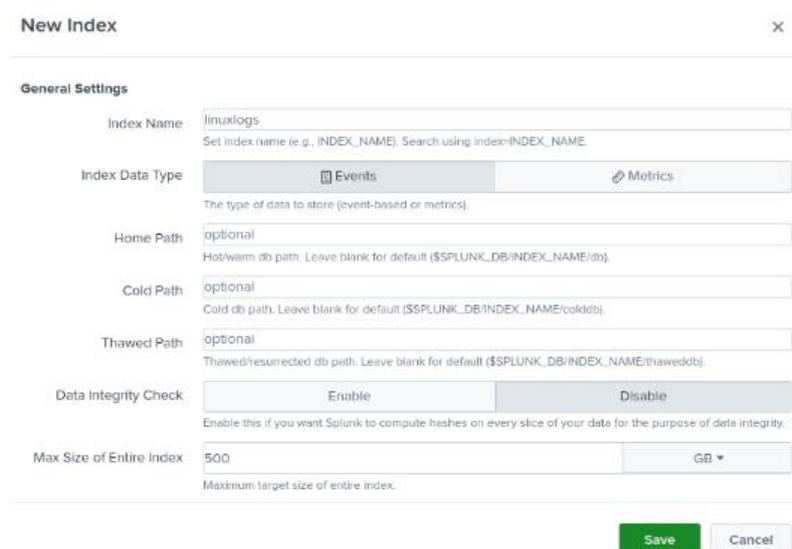
**Figura 3.55** Asignación del agente *Forwarder* hacia el servidor Splunk

De esta forma, se comprobará que los forwards están activados y que no existe error en su configuración con el comando: ***./splunk list forward-server***, como se visualiza en la Figura 3.56.



**Figura 3.56** Verificación del servidor Splunk destino

Seguidamente, dentro del servidor Splunk se creó un nuevo index con el nombre “linuxlogs”, el cual va a recibir los logs del agente, permitiendo verificar que eventos están sucediendo en dicho agente, esto se observa en la Figura 3.57.



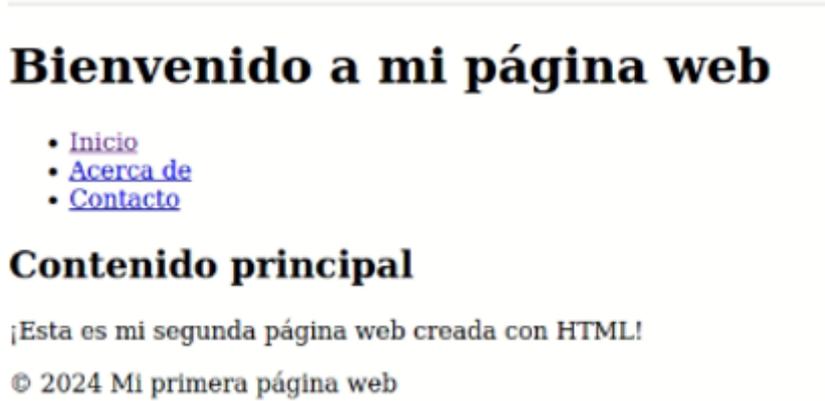
**Figura 3.57** Creación de un nuevo index para recibir logs del agente

Ya creado el nuevo index, nuevamente se ingresa al agente y se ingresa al directorio de bin con el comando: **cd /opt/splunkforwarder/bin/**; donde se ejecutó el comando: **./splunk add monitor /var/log/auth.log -index linuxlogs -sourcetype authlogs**; como se observa en la Figura 3.58; el cual está agregando un nuevo monitor que extraiga los authlogs del agente, el parámetro “-index linuxlogs” indica que los datos deben ser enviados al index “linuxlogs” y el parámetro “-sourcetype authlogs” es un nombre que se lo agregará por defecto.

```
root@stem-VirtualBox:/opt/splunkforwarder/bin# ./splunk add monitor /var/log/auth.log -index linuxlogs -sourcetype authlogs
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/auth.log'.
```

**Figura 3.58** Asignación de un nuevo monitor para la recolección de los logs del agente. Además, se instaló y configuró el servidor Web apache2 en el agente Splunk, el cual debe estar en funcionamiento, como se visualiza en la Figura 3.59, donde se aplicarán las mismas modificaciones que se realizaron previamente en el otro agente SIEM. Dado esto, se procedió con la modificación del archivo index.html, como se observa en la Figura 3.35, y para reducir los recursos del servidor Web se evidencia en la Figura 3.36.

```
root@siem-VirtualBox:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese
   Active: active (running) since Sun 2024-07-07 16:05:52 -05; 2h 14min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 822 (apache2)
    Tasks: 18 (limit: 13911)
   Memory: 5.9M
      CPU: 827ms
   CGroup: /system.slice/apache2.service
           └─822 /usr/sbin/apache2 -k start
             └─860 /usr/sbin/apache2 -k start
```



**Figura 3.59** Verificación e ingreso al servidor Web

Una vez comprobado que el servidor Web esté funcionando, se crea un archivo de configuración donde se especifican las entradas de logs que se desean recopilar en el servidor Splunk, los logs con mayor importancia para recopilar son los que se relacionen con los errores que pueda tener el servidor apache. Seguido a esto, se ingresa al directorio de “local” y se crea el archivo “inputs.conf”; para esto se ingresó el comando: **nano /opt/splunkforwarder/etc/system/local/inputs.conf**, y se creó el archivo con su configuración correspondiente, lo cual se evidencia en la Figura 3.60.

```

root@siem-VirtualBox:/home/siem# nano /opt/splunkforwarder/etc/system/local/inputs.conf
root@siem-VirtualBox:/home/siem
GNU nano 6.2 /opt/splunkforwarder/etc/system/local/inputs.conf
[monitor:///var/log/apache2/access.log]
disabled = false
index = linuxlogs
sourcetype = apache:access

[monitor:///var/log/apache2/error.log]
disabled = false
index = linuxlogs
sourcetype = apache:error

```

**Figura 3.60** Configuración para enviar logs relacionados con el servidor Web apache

Tal como se indicó, la máquina atacante será la misma que se instaló y configuró previamente en la Figura 3.38 y será utilizada con las mismas aplicaciones (Slowhttptest - Pentmenu) para realizar el ataque de DoS, como se corrobora en la Figura 3.39 y Figura 3.40.

### Ejecución del ataque al agente de Splunk

Para la ejecución del ataque se seguirá el mismo orden que previamente se utilizó, es decir se realiza el escaneo de manera completa de la máquina que será atacada con “nmap”. Dado esto, en la terminal de la máquina atacante se ingresa el comando: nmap -A 192.168.200.29, donde lo único que cambiará es la dirección IP de la víctima, en este caso es 192.168.200.29; y se comprueba que el puerto 80/tcp este abierto para realizar el ataque al servidor Web, como se puede apreciar en la Figura 3.61.

```

root@kali: ~/kali
└─$ nmap -A 192.168.200.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-07 19:46 EDT
Nmap scan report for 192.168.200.29
Host is up (0.00067s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: Mi segunda p!XC3\A1gina web
|_ http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 08:00:27:F0:69:F6 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose/storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), Synology DiskStation Manager 5.X (90%), Netgear RAIDiator 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/o:synology:diskstation_manag
er:5.2 cpe:/o:netgear:raidiator:4.2.28
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (97%), Linux 5.0 - 5.5 (95%), Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.9 (91
%), Linux 3.4 - 3.10 (91%), Linux 2.6.32 - 3.10 (91%), Linux 2.6.32 - 3.13 (91%), Linux 2.6.39 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.67 ms 192.168.200.29

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.85 seconds

```

**Figura 3.61** Ejecución de la herramienta Nmap

Para proceder a realizar el ataque se comprueba que el servidor Web con la dirección IP 192.168.200.29 se encuentre habilitado, por lo tanto, se ingresa al navegador de la máquina Kali Linux y se ingresa la dirección IP y se comprueba en la Figura 3.62 que el servidor Web está habilitado y funcionando.



Figura 3.62 Acceso al servidor Web apache2

Una vez comprobado que el servidor Web está funcionando se procede a realizar el ataque DoS con la aplicación Slowhttptest, para ejecutarlo se colocó la dirección IP de la máquina atacada, que en este caso es 192.168.200.29; dado esto el comando fue: **slowhttptest -c 65539 -H -i 350 -r 8000 -l 10000 -u <http://192.168.200.29>**, la ejecución del ataque se verifica en la Figura 3.63.

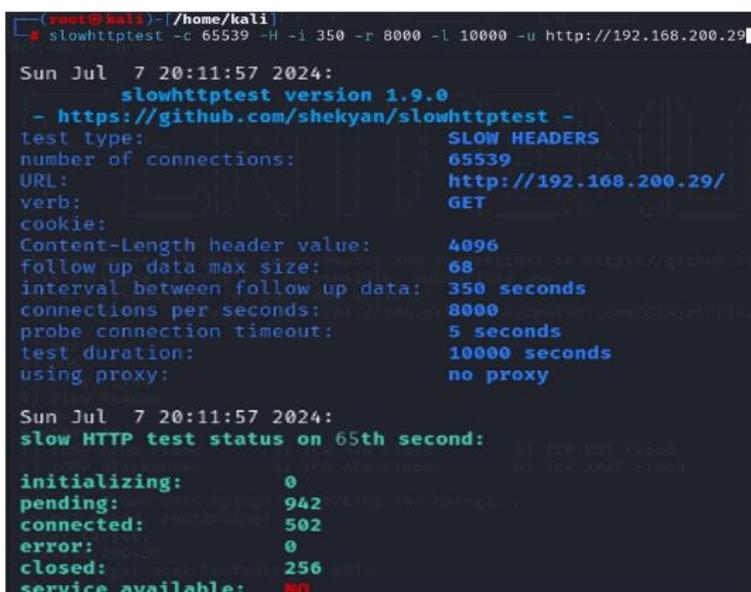
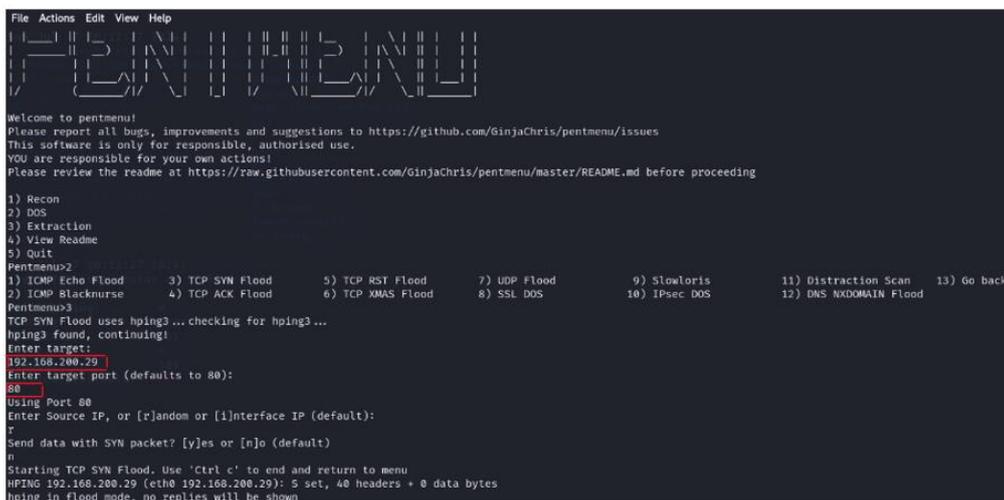


Figura 3.63 Ejecución de la herramienta Slowhttptest

De igual manera, se ejecuta el ataque con la herramienta Pentmenu mediante la consola de Kali Linux y se ejecuta el comando: `./pentmenu`; el único parámetro que cambiaría es la dirección IP de la máquina atacada, la cual es 192.168.200.29; el ataque se evidencia en la Figura 3.64.



```
File Actions Edit View Help
Pentmenu
Welcome to pentmenu!
Please report all bugs, improvements and suggestions to https://github.com/GinjaChris/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pentmenu/master/README.md before proceeding

1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu2
1) ICMP Echo Flood      3) TCP SYN Flood      5) TCP RST Flood      7) UDP Flood          9) Slowloris          11) Distraction Scan  13) Go back
2) ICMP Blacknurse     4) TCP ACK Flood     6) TCP XMAS Flood    8) SSL DOS           10) IPsec DOS        12) DNS NXDOMAIN Flood
Pentmenu3
TCP SYN Flood uses hping3... checking for hping3...
hping3 found, continuing!
Enter target:
192.168.200.29
Enter target port (defaults to 80):
80
Using port 80
Enter Source IP, or [r]andom or [i]nterface IP (default):
r
Send data with SYN packet? [y]es or [n]o (default)
n
Starting TCP SYN Flood. Use 'Ctrl c' to end and return to menu
HPING 192.168.200.29 (eth0 192.168.200.29): 5 set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figura 3.64 Ejecución de la herramienta Pentmenu

Una vez ya realizados los ataques, se comprueba en la Figura 3.65 que el servidor se encuentra inhabilitado.

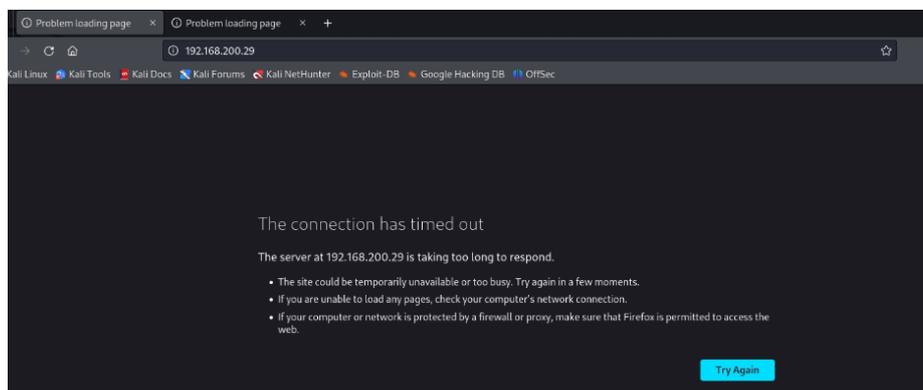


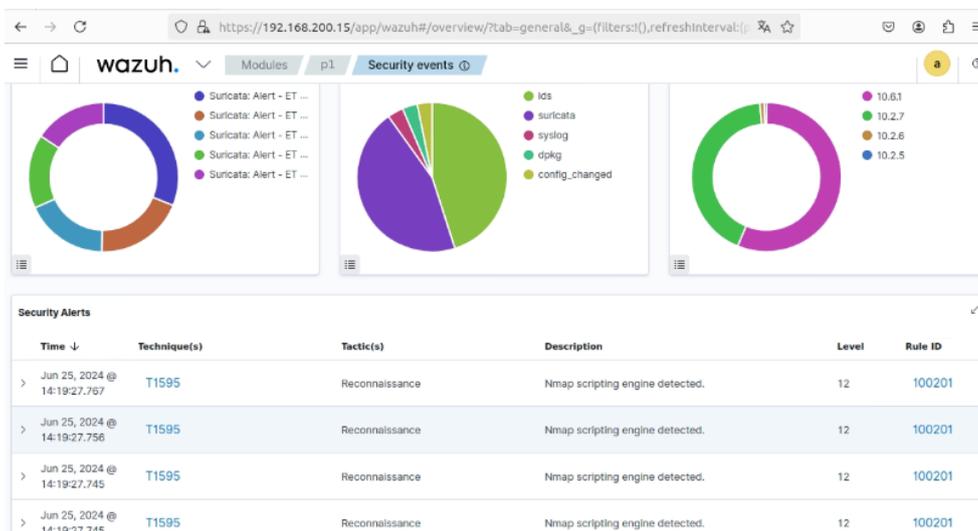
Figura 3.65 Intento de conexión al servidor caído

## 3.4 Verificación del funcionamiento del SIEM

### Análisis de resultados SIEM Wazuh

En la ejecución del ataque se realizó un escaneo de vulnerabilidades a la dirección IP 192.168.200.16 que es agente del servidor Wazuh y víctima, como se puede ver en la

Figura 3.41; dado esto en el *dashboard* del servidor Wazuh se evidencia la detección de “*Nmap Scripting Engine*”, que es la regla que se agregó previamente en la configuración del servidor Wazuh ligado al grupo Suricata, para esto ver la Figura 3.14; sumado a esto se puede apreciar en la Figura 3.66 cómo se detecta el escaneo de la herramienta Nmap.



**Figura 3.66** Detección y alerta sobre la herramienta Nmap

Al momento de abrir la alerta que se evidencia en la Figura 3.66 del *dashboard* del servidor Wazuh, se pueden apreciar diferentes parámetros específicos de la alerta; para esto ver Figura 3.67. Donde se observan el “*agent.id 001*”, “*agent.name p1*” que en la Figura 3.9 se evidencia que se trata de ese agente, “*agent.ip 192.168.200.16*” que es la dirección IP del agente-víctima, “*data.alert.category Web Application Attack*” hace referencia a que se ha detectado una acción maliciosa que está relacionada con aplicaciones Web, “*data.alert.signature ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)*” es la regla que se agregó al servidor Wazuh que está relacionado con el grupo Suricata; por lo que al realizar un escaneo con Nmap esta alerta se mostrará, “*data.dest\_port 80*” indica que la acción maliciosa va dirigida al puerto 80, y de igual manera se evidencia cómo se detecta la dirección IP del atacante como se configuró con anterioridad, lo cual se evidencia en la Figura 3.13 para esto los parámetros “*data.src\_ip*” y “*data.srcip*” muestran la dirección IP 192.168.200.4 que es el atacante. Cabe recalcar que estos parámetros son los más destacados a la hora de detectar la alerta.

agentId	001
agentIp	192.168.200.16
agentName	p1
data.alert.action	allowed
data.alert.category	Web Application Attack
data.alert.gid	1
data.alert.metadata.created_at	2010_07_30
data.alert.metadata.updated_at	2020_04_22
data.alert.rev	6
data.alert.severity	1
data.alert.signature	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
data.alert.signature_id	2009358
data.app_proto	http
data.dest_ip	192.168.200.16
data.dest_port	80
data.direction	to_server
data.event_type	alert
data.proto	TCP
data.src_ip	192.168.200.4
data.src_port	37326
data.srcip	192.168.200.4

**Figura 3.67** Características de la alerta relacionada con Nmap

Sumado a esto, la ejecución del ataque *DoS* también se reflejó en el *dashboard* del servidor Wazuh como se observa en la Figura 3.68, para lo cual se evidencia dos alertas que son específicas; la alerta “*Agent event queue is full. Events may be lost*” indica que los eventos o almacenamiento del agente se encuentran lleno por completo y que alcanzó su capacidad máxima de almacenamiento, y los eventos puedan perderse. Por otro lado, se tiene la alerta “*Agent event queue is flooded. Check the agent configuration*”, donde ya indica que el agente está completamente inundado con una cantidad excesiva de eventos en su cola, que se realice una revisión de la configuración del agente.

Timestamp	Message	Count	Bytes
Jun 25, 2024 @ 14:25:30.272	Agent event queue is flooded. Check the agent configuration.	12	204
Jun 25, 2024 @ 14:25:29.210	Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 30	3	86601
Jun 25, 2024 @ 14:25:23.083	Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 30	3	86601
Jun 25, 2024 @ 14:25:20.734	Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 49	3	86601
Jun 25, 2024 @ 14:25:15.203	Agent event queue is full. Events may be lost.	9	203

**Figura 3.68** Detección y alerta de ataque DoS *Figura 3.69*, donde muestra parámetros que evidencian que el agente está en un estado de inundación, por lo que el “*data.level flooded*” indica que se está sobrecargando e inundando con una cantidad excesiva de eventos hacia el agente-servidor-víctima. Para corroborar esta información se aprecia que “*full\_log wazuh: Agent buffer: 'flooded'*” indica que el búfer del agente está inundando por completo y no puede procesar de manera rápida las solicitudes que recibe, lo que provoca la saturación completa del servidor sin respuesta alguna.

Field	Value
@timestamp	2024-06-25T19:25:30.272Z
_id	lHcUJABGgCoyj7KSEMb
agent.id	001
agent.ip	192.168.200.16
agent.name	p1
data.level	flooded
decoder.name	wazuh
decoder.parent	wazuh
full_log	wazuh: Agent buffer: 'flooded'
id	1719343530.3095309
input.type	log
location	wazuh-agent
manager.name	wazuh-VirtualBox
rule.description	Agent event queue is flooded. Check the agent configuration.

**Figura 3.69** Característica de la alerta Agent event queue is flooded *Figura 3.69*, que en este caso indica que el agente-víctima está generando una cantidad exagerada de eventos en un periodo de tiempo sumamente corto, por eso menciona que el agente está inundado de solicitudes afectando al rendimiento y capacidad del agente.

wazuh. Modules p1 Security events ⓘ

agent.id	001
agent.ip	192.168.200.16
agent.name	p1
data.level	full
decoder.name	wazuh
decoder.parent	wazuh
full_log	wazuh: Agent buffer: 'full'.
id	1719343515.3088752
input.type	log
location	wazuh-agent
manager.name	wazuh-VirtualBox
rule.description	Agent event queue is full. Events may be lost.
rule.firedtimes	1
rule.gdpr	IV_35.7.d
rule.groups	wazuh, agent_flooding

**Figura 3.70** Característica de la alerta Agent event queue is full. Events may be lost

Sumado a esto, se evidencia una alerta más, la cual es “*Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group <number>*”, que indica una alerta en el grupo de Suricata, que el tráfico entrante se encuentra listado en la base de datos DROP (*Don't Route Or Peer*), la cual identifica direcciones IP con acciones maliciosas que no deberían ser enrutadas y estas puedan comprometer la comunicación dentro de la red. *DROP Listed Traffic Inbound group*, este parámetro indica que el tráfico entrante proviene de una dirección IP que está en la lista DROP y que puede pertenecer a un grupo o conjunto en específico, ya que vienen desde diferentes grupos, pero están ligadas a la lista de DROP, ver Figura 3.71.

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Jun 25, 2024 @ 14:37:20.994			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 31	3	86601
> Jun 25, 2024 @ 14:37:20.988			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 24	3	86601
> Jun 25, 2024 @ 14:37:19.448			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 24	3	86601
> Jun 25, 2024 @ 14:37:19.441			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 55	3	86601
> Jun 25, 2024 @ 14:37:19.431			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 49	3	86601
> Jun 25, 2024 @ 14:37:19.422			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 30	3	86601
> Jun 25, 2024 @ 14:37:19.135			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 23	3	86601
> Jun 25, 2024 @ 14:37:18.932			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 25	3	86601
> Jun 25, 2024 @ 14:37:18.907			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 6	3	86601
> Jun 25, 2024 @ 14:37:18.907			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 25	3	86601

**Figura 3.71** Detección y alerta de Suricata: Alert - ET DROP Spamhaus

### Análisis de resultados SIEM Splunk

Una vez ejecutado el ataque en el agente de Splunk, en el buscador de alertas se selecciona la alerta que se creó previamente, para esto se ingresa el index que se creó con anterioridad para que envíe los logs a recopilar: `index="linuxlogs"` seguido con el tipo de fuente de los eventos que en este caso es apache: `sourcetype="apache:error"`, el cual está relacionado con los logs de error generados por el servidor Web apache.

Además, para que la alerta del ataque *DoS* detecte anomalías en esos logs, se agregan otros parámetros que especifican por qué se logran evidenciar las alertas; estos parámetros son: `"stats count by src_ip"`, el cual genera un conteo de los eventos de logs de error generado por una dirección IP de origen, `"where count > 1000"`, indica que si existe un conteo mayor de 1000 solicitudes se genera la alerta de ataque. La sección `"eval description="Posible ataque DoS: Número de solicitudes excede el umbral"`, indica que se creó un campo con una descripción, la cual en conjunto con los otros parámetros van a estar enfocados en el ataque *DoS* hacia el agente, como se puede evidenciar en la Figura 3.72.

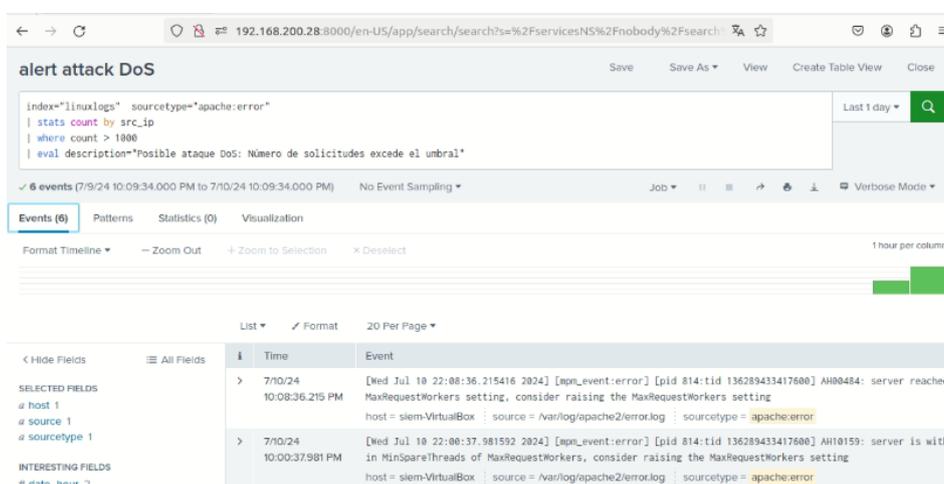
```

alert attack DoS
index="linuxlogs" sourcetype="apache:error"
| stats count by src_ip
| where count > 1000
| eval description="Posible ataque DoS: Número de solicitudes excede el umbral"
  
```

**Figura 3.72** Características de la alerta generada

Seguidamente, se visualiza en la Figura 3.73 los eventos recopilados por la alerta que se generó, la cual está mostrando que existen eventos relacionados con los logs de error de entrada hacia el servidor apache. Por ende, se verifica en la primera alerta el siguiente mensaje “*server reached MaxRequestWorkers setting, consider raising the MaxRequestWorkers setting*”; el cual significa que el servidor apache alcanzó su límite de capacidad, lo que implica que no puede recibir ni manejar más solicitudes en ese momento.

La otra alerta muestra el siguiente mensaje “*server is within MinSpareThreads of MaxRequestWorkers, consider raising the MaxRequestWorkers setting*”, es similar a la anterior, ya que está indicando que el servidor apache está alcanzando el límite máximo de sus procesos y que se sugiere revisar la configuración del servidor.



**Figura 3.73** Detección y recopilación de los eventos relacionados con el ataque DoS

De esta forma, tanto como Wazuh y Splunk recogieron alertas que están relacionadas con el ataque de DoS; por tal motivo Wazuh obtuvo alertas inmediatas cuando se presentó un ataque hacia el agente; lo que alertaba al servidor de tomar medidas acerca de la inhabilitación del servicio Web que posee el agente de Wazuh. Por otro lado, para verificar las alertas de Splunk se evidenció un pequeño retardo a la hora de recibir la alerta relacionada con el ataque, sin embargo, la respuesta fue efectiva y se presentó las medidas a tomar en el agente de Splunk para que no se inhabilite el servicio Web que se presentaba en el mismo.

### Comparativa técnica entre los SIEM implementados

A continuación, en la Tabla 3.1 se compara de manera técnica los SIEM implementados, considerando desde su instalación y configuración hasta el resultado del ataque de DoS.

**Tabla 3.1** Comparativa técnica entre los SIEM

<b>Características</b>	<b>Wazuh</b>	<b>Splunk</b>
<b>Instalación y configuración</b>	Requiere de conocimientos técnicos previamente a la configuración.	Fácil de instalar, pero requiere de experiencia avanzada para las configuraciones.
<b>Interfaz de usuario</b>	<i>Dashboard</i> amigable y funcional basado en Web.	<i>Dashboard</i> avanzado, personalizable y basado en Web.
<b>Costos</b>	Gratuito, dado que es un software de código abierto.	De pago, requiere de inversiones adicionales para su uso. Posee un uso gratuito de 60 días.
<b>Arquitectura y tipo de licencia</b>	Cliente-servidor, Licencia <i>opensource</i> .	Cliente-servidor, Licencia comercial <i>closource</i> .
<b>Escalabilidad</b>	Escalable, pero requiere de configuraciones avanzadas para recibir grandes volúmenes de datos.	Alta escalabilidad, creada para recibir grandes volúmenes de datos.
<b>Comunidad y soporte</b>	Amplia comunidad de usuarios, soporte disponible a través de la comunidad y recursos en línea.	Soporte oficial disponible, extensa comunidad de usuarios y amplios recursos en línea.
<b>Análisis de logs y resultados</b>	Análisis en tiempo real, resultados relacionados con eventos específicos.	Análisis en tiempo real, resultados relacionados con eventos específicos, búsqueda avanzada.

## Manual técnico con las mejoras practicas ante un ataque de DoS

El ataque DoS es una de las maneras más eficaces que ocupan los ciberdelincuentes a la hora de hacer que un recurso de red no esté disponible para los usuarios legítimos, ya que inundan el servicio con una cantidad excesiva de tráfico hasta no obtener respuesta alguna del servicio inhabilitado. La protección más eficaz a esta clase de ataques es la concientización de los usuarios legítimos para saber qué hacer ante posibles amenazas. Por tal motivo, se expondrán las mejores prácticas ante un ataque de Dos.

1. Implementar sistemas de prevención de intrusiones (IPS), para que detecte y bloquee el tráfico no deseado en tiempo real, así como configurar reglas en los *firewalls* que limiten el tráfico de entrada y salida no deseados.
2. Mantener redundancia y balanceo de carga es una de las formas más significativas de mantener un servicio activo, ya que se duplicará a más de un servidor y esto minimiza la probabilidad de que se inhabilite debido a la sobrecarga. Además, otra ventaja es la tolerancia a fallos, debido a que, si un servidor cae, el otro asume el trabajo y no presenta ningún inconveniente.
3. Brindar el monitoreo de red con herramientas como Nagios, Zabbix o un SIEM, es clave a la hora de detectar y alertar el estado de los sistemas y la red, ya que analizan el tráfico en la red, detectan acciones inusuales, registros y análisis de logs y generar alertas automáticas. Todo esto para indicar al grupo de seguridad de alguna actividad sospechosa en la red.
4. Configurar de manera adecuada SSL/TLS para mantener protegida la comunicación mediante HTTPS, ya que brinda cifrado de extremo a extremo y mantiene la confidencialidad en la comunicación; por lo tanto, el ciberdelincuente no puede leer ni observar el contenido de la información si no posee la clave del cifrado. De esta manera protege la información sensible que se transmitió mediante HTTPS.
5. La implementación de un desafío de captcha hacia un sitio Web u aplicación en línea ayuda a distinguir entre un humano legítimo o un bot automatizado, lo cual ayuda a prevenir el ataque DoS; ya que obliga a los usuarios a realizar un desafío que necesita de la interacción humana como, por ejemplo: resolver un problema matemático, seleccionar imágenes específicas, reescribir correctamente símbolos, letras o números. De esta forma el captcha dificulta los intentos de sobrecargar el servidor con solicitudes automatizadas, manteniendo la disponibilidad y rendimiento del servicio.

## 4 CONCLUSIONES

- La implementación y configuración de los SIEM han sido fundamentales para conocer e interpretar cómo recopilan datos, logs y registros en diferentes puntos finales; ayudando a obtener una respuesta eficaz ante riesgos de seguridad. Lo que ayuda a establecer la disponibilidad y confidencialidad de la información en la red.
- Tras una comparativa exhaustiva, se determinó que ambos SIEM tanto Wazuh como Splunk, poseen características esenciales para poder implementar de manera rápida, fácil y eficiente sus servicios y ser amigable con el usuario a la hora de interpretar los eventos registrados en cada uno de sus *dashboards* en la Web.
- Con relación a Wazuh, se determinó que su instalación debe tener los requisitos de hardware y software a su máximo, para que pueda funcionar de manera correcta y no presente errores en el inicio de sus servicios. Sin embargo, su extensa comunidad de apoyo brinda el soporte necesario y adecuado a la hora de solucionar problemas relacionados con su habilitación, configuración del sistema.
- En cuanto a Splunk, se concluye que en el proceso de instalación requiere de hardware y software mínimos para que su servicio pueda funcionar de manera correcta, lo cual facilita su implementación y uso.
- Se determinó que para la implementación de Wazuh se necesitó de una herramienta adicional para que sus eventos puedan ser registrados satisfactoriamente con relación al ataque *DoS*. La herramienta fue Suricata que es un IDPS, ya que al ser *opensource* proporciona capacidades para configurar en otras herramientas y ayudar en la detección de patrones de comportamiento sospecho o ataques conocidos en la red.
- Se determinó que para la implementación de Splunk se necesitó de la creación de un index en particular, el cual recibirá los logs de entrada y salida del agente en relación con el servidor Web configurado en él; de esta forma se podrá verificar qué eventos están sucediendo en el agente y tomar medidas de seguridad si se registran eventos relacionados con el ataque *DoS*.
- Es importante recalcar que el SIEM Wazuh está disponible de forma gratuita y de código abierto, mientras que el SIEM Splunk ofrece una licencia gratuita por un periodo de 60 días, de lo contrario se deberá adquirir la versión completa para su utilización.

- En cuanto a los resultados emitidos por Wazuh son instantáneos y fáciles de interpretar, ya que el *dashboard* emite las alertas generadas con su respectiva descripción ligada al evento que está sucediendo, así como una gráfica de pastel que indica que evento se genera con mayor frecuencia.
- En cuanto a los resultados emitidos por Splunk no son de manera instantánea, tiene un intervalo de 2 minutos que demora el servidor para emitir las alertas generadas, y no brinda gráficas estadísticas, sin embargo, proporciona una lista de eventos que están ligadas a la alerta generada sobre el ataque *DoS*.
- Para la implementación del servidor Web apache2, en los agentes de ambos SIEM, se modificó su configuración inicial para que reciba menos solicitudes, esto con el fin de que, al momento de ejecutar el ataque, el servicio se inhabilite de manera instantánea y poder observar los resultados de manera inmediata en los SIEMs.
- En cuanto a la ejecución del ataque emitido por la máquina de Kali Linux, se utilizaron dos herramientas: Slowhttptest y Pentmenu. Estas herramientas brindaron mayor información para ejecutar el ataque de *DoS*, como por ejemplo cuántas solicitudes desea mandar, por cual puerto debe realizar el ataque, entre otras asistencias. Esto permitió un ataque más fiable hacia el servidor Web apache2.

## 5 RECOMENDACIONES

- Para garantizar que la virtualización de las máquinas sea de manera correcta, se debe poseer una alta capacidad en la máquina *host* esto debe incluir procesadores de 2 a 4 núcleos, memoria RAM de mínimo 16 (GB) y capacidad de almacenamiento de 50 (GB) como mínimo. Lo que permitirá asignar de manera eficiente la memoria y el espacio necesario para cada máquina virtual.
- Dada la importancia que es proteger el tráfico en la red, es necesario mantener un entorno controlado a la hora de ejecutar ataques de *DoS*, por lo tanto, se recomienda crear una red NAT interna para realizar la simulación, de lo contrario se podrá ver afectado algún servicio de la máquina *host*; lo cual inhabilitará el uso de cualquier servicio en específico.
- Para la implementación de los servidores Wazuh, Splunk, y sus agentes es recomendable configurarlos sobre un sistema operativo Linux basado en la distribución Ubuntu 22.04, ya que en versiones anteriores presentan errores a la

hora de usarlos y no se logra trabajar de manera adecuada con las máquinas virtuales.

- Para la implementación de la topología de red, se recomienda usar la aplicación de simulación de redes GNS3, debido a su amplia comunidad de apoyo que brindan las guías necesarias para mantener una configuración adecuada y no presentar problemas, ya que permite a los usuarios diseñar, configurar y simular redes de manera virtual en entornos controlados.

## 6 REFERENCIAS BIBLIOGRÁFICAS

- [1] W. C. & S. A. L. Douglas da Silva, «Blog de Zendesk,» 18 Septiembre 2023. [En línea]. Available: [qzendesk.com.mx/blog/que-es-seguridad-de-informacion/](https://qzendesk.com.mx/blog/que-es-seguridad-de-informacion/). [Último acceso: 5 mayo 2024].
- [2] M. Coppola, «Blog dehubspot,» 8 mayo 2023. [En línea]. Available: <https://blog.hubspot.es/website/que-es-seguridad-informatica>. [Último acceso: 6 mayo 2024].
- [3] C. Isbel, «isbel Quantik,» 5 Septiembre 2021. [En línea]. Available: <https://isbel.com/seguridad-de-la-informacion-vulnerabilidades-riesgos/>. [Último acceso: 5 mayo 2024].
- [4] ManageEngine, «ManageEngine,» [En línea]. Available: <https://www.manageengine.com/latam/netflow/que-es-el-ataque-de-denegacion-de-servicios.html>. [Último acceso: 6 mayo 2024].
- [5] Fortinet, «Fortinet,» [En línea]. Available: <https://www.fortinet.com/lat/resources/cyberglossary/dos-vs-ddos>. [Último acceso: 21 Junio 2024].
- [6] paloalto, «paloalto networks,» [En línea]. Available: <https://www.paloaltonetworks.es/cyberpedia/what-is-a-denial-of-service-attack-dos>. [Último acceso: 22 Junio 2024].
- [7] Aurora, «ID Digital School,» 04 Abril 2023. [En línea]. Available: <https://iddigitalschool.com/bootcamps/que-es-el-blue-team-en-ciberseguridad/>. [Último acceso: 05 Mayo 2024].
- [8] «Ambit-bst,» 29 abril 2021. [En línea]. Available: <https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona>. [Último acceso: 6 mayo 2024].
- [9] M. Escalante, «ABC Xperts,» 31 mayo 2023. [En línea]. Available: <https://abcxperts.com/a-nivel-de-ciberseguridad-que-herramientas-deberia-de-conocer-un-blueteam/>. [Último acceso: 6 mayo 2024].

- [10] «latam kaspersky,» [En línea]. Available: <https://latam.kaspersky.com/resource-center/definitions/firewall>. [Último acceso: 6 mayo 2024].
- [11] «ADM Cloud Services,» [En línea]. Available: <https://admcloudservices.com/blog/sem-sim-siem/>. [Último acceso: 6 mayo 2024].
- [12] wazuh, «wazuh,» 05 diciembre 2018. [En línea]. Available: <https://wazuh.com/>. [Último acceso: 20 mayo 2024].
- [13] «wazuh,» [En línea]. Available: <https://documentation.wazuh.com/current/quickstart.html>. [Último acceso: 20 mayo 2024].
- [14] L. d. Río, «Computing,» 11 Enero 2023. [En línea]. Available: <https://www.computing.es/seguridad/splunk-la-herramienta-para-anticiparse-a-los-ataques/>. [Último acceso: 06 Julio 2024].
- [15] «NetApp,» 13 Diciembre 2023. [En línea]. Available: <https://docs.netapp.com/es-es/netapp-solutions/data-analytics/stgr-splunkss-splunk-architecture.html>. [Último acceso: 06 Julio 2024].
- [16] «Level Blue,» [En línea]. Available: <https://cybersecurity.att.com/products/ossim>. [Último acceso: 20 mayo 2024].
- [17] V3KT0R, «IT Freek Zone,» 26 agosto 2010. [En línea]. Available: <https://itfreekzone.blogspot.com/2010/08/instalacion-y-configuracion-de-ossim.html>. [Último acceso: 20 mayo 2024].
- [18] J. Ibero, «IberAsync,» 02 junio 2022. [En línea]. Available: <https://iberasync.es/gestion-de-vulnerabilidades-con-un-siem-alienvault-ossim/>. [Último acceso: 20 mayo 2024].
- [19] «Administracion de Sistemas,» 11 abril 2024. [En línea]. Available: <https://administraciondesistemas.com/security-onion/>. [Último acceso: 20 mayo 2024].
- [20] V. GARCIA, «Servicios Vartech,» 24 febrero 2023. [En línea]. Available: <https://www.serviciosvartech.com/security-onion-que-es-y-como-funciona/>. [Último acceso: 20 mayo 2024].

## **7 ANEXOS**

ANEXO I. Certificado de originalidad

ANEXO II. Enlaces

# **ANEXO I: Certificado de Originalidad**

## **CERTIFICADO DE ORIGINALIDAD**

Quito, D.M. 24 de julio de 2024

De mi consideración:

Yo, GABRIELA KATHERINE CEVALLOS SALAZAR, en calidad de Directora del Trabajo de Integración Curricular titulado IMPLEMENTACIÓN DE UN SIEM PARA LA DEFENSA ACTIVA ANTE UN ATAQUE DE DENEGACIÓN DE SERVICIO asociado al proyecto IMPLEMENTACIÓN DE UN SIEM PARA LA DEFENSA ACTIVA ANTE INTRUSIONES EN UNA RED elaborado por el estudiante DANIEL ALEXANDER HERRERA ZAPATA de la carrera en TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES, certifico que he empleado la herramienta Turnitin para la revisión de originalidad del documento escrito completo, producto del Trabajo de Integración Curricular indicado.

El documento escrito tiene un índice de similitud del 12%.

Es todo cuanto puedo certificar en honor a la verdad, pudiendo el interesado hacer uso del presente documento para los trámites de titulación.

NOTA: Se adjunta el link del informe generado por la herramienta Turnitin.

[https://epnecuador-my.sharepoint.com/:b:/g/personal/gabriela\\_cevalloss\\_epn\\_edu\\_ec/EZco9VXTRWRIsOZdXikJUUIB9lyuYrxOoNbq5pWO1akXq?e=5Vt9Pk](https://epnecuador-my.sharepoint.com/:b:/g/personal/gabriela_cevalloss_epn_edu_ec/EZco9VXTRWRIsOZdXikJUUIB9lyuYrxOoNbq5pWO1akXq?e=5Vt9Pk)

Atentamente,

**GABRIELA KATHERINE CEVALLOS SALAZAR**

**Docente**

**Escuela de Formación de Tecnólogos**

## ANEXO II: Enlaces

**Anexo II.I** Código QR del video con la implementación y pruebas de funcionamiento



<https://youtu.be/VC7AJjl28o0?si=ThmC5Vr8qj3tV7n7>