ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

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

IMPLEMENTACIÓN DE UN SIEM PARA LA DEFENSA ACTIVA ANTE UN ATAQUE POR MALWARE

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

EDISON JAVIER PACHACAMA TACURI

DIRECTOR: ING. GABRIELA KATHERINE CEVALLOS SALAZAR MSc.

DMQ, julio 2024

CERTIFICACIONES

Yo, Edison Javier Pachacama Tacuri 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.

Edison Javier Pachacama Tacuri

edison.pachacama@epn.edu.ec

jaci-cone@hotmail.com

Certifico que el presente trabajo de integración curricular fue desarrollado por Edison Javier Pachacama Tacuri, bajo mi supervisión.

GABRIELA KATHERINE CEVALLOS SALAZAR

DIRECTOR

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.

EDISON JAVIER PACHACAMA TACURI

DEDICATORIA

Esta dedicatoria es para mi madre y para toda mi familia, que a pesar de todo han estado apoyándome. A mi madre, Julia Tacuri, que a pesar de educarme ella sola me dio todo para seguir adelante, gracias por sus enseñanzas y todos los valores que me inculcaste en todo este tiempo y por creer en mí que sin importar lo largo que ha sido esta etapa sigues ahí dándome consejos y guiándome por el buen camino y criando un hijo de bien. Querida madre espero que estes orgullosa de mí.

También dedico esta tesis a mis hermanos y mi familia por todo su apoyo y consejos aún sigo adelante sin importar las dificultades, que han estado conmigo en todo lo que han podido.

Para toda mi familia les agradezco por todo lo que han hecho por mí, espero que estén orgullosos de este logro que sin importar el tiempo que tomó al fin logré hacer lo más importante para mí y para ustedes.

También la dedicó a todos mis amigos que estuvieron ahí apoyándome en todo momento a pesar de que estaban ocupados se dieron el tiempo para ayudarme en todo lo necesario, les agradezco mucho de todo corazón por estar ahí conmigo hasta el final dándome su apoyo.

EDISON JAVIER PACHACAMA TACURI

AGRADECIMIENTO

Agradezco principalmente a mi madre Julia Tacuri ya que sin ella yo no hubiera podido avanzar, sin importar las dificultades que hemos tenido siempre ha estado ahí apoyándome en todo lo necesario. Te doy las gracias, Madre por todo tu apoyo y consejos.

También agradezco a mis hermanos, que sin importar lo alejados u ocupados que estén siempre han estado ahí para apoyarme aconsejarme y brindarme todo su apoyo sin pedir nada a cambio.

Agradezco también a mi mejor amigo Diego Lomas, que sin importar lo ocupado que él esté siempre ha estado ahí brindándome su ayuda en las cosas más difíciles que he tenido.

Le doy las gracias a mi tutora de tesis la ING Gabriela Katherine Cevallos Salazar de la Escuela Politécnica Nacional por todo su apoyo, por toda su paciencia, por la guía que ha tenido en todo este tiempo en la carrera y por creer en mí a pesar de todas las dificultades que ha pasado.

Para mis compañeros de la facultad de tecnólogos a quienes les considero más que amigos por todo lo que hemos pasado en la carrera, por las risas, por todos los retos que hemos pasado les doy mi agradecimiento que sin ustedes no sería lo mismo la universidad.

Les agradezco a todos los profesores de la carrera por todo su apoyo, por toda la guía, toda la enseñanza que me han brindado para crear un chico de bien.

Por último, También agradezco a la Universidad Politécnica Nacional por toda la guía. Herramientas y por los establecimientos para poder desarrollar profesionales en el campo laboral.

EDISON JAVIER PACHACAMA TACURI

ÍNDICE DE CONTENIDOS

RESUMEN

El presente proyecto se basa en la implementación de dos servidores SIEM: *Wazuh* y *AlienVault*, con la finalidad de evaluar el desempeño de cada SIEM, protegiendo, detectando y analizando ataques en tiempo real.

En primer lugar, para realizar esta actividad, se debe hacer un estudio ingresando a las páginas oficiales de cada herramienta SIEM, con el fin de observar las respectivas especificaciones tanto el hardware y software, obteniendo información para su correcto funcionamiento, luego de obtener la información mencionada anteriormente, se implementa y configura los dos servidores SIEM.

A continuación, se debe desarrollar la implementación de la topología de la red mediante un emulador llamado GNS3 para establecer conectividad entre los dispositivos con el servidor SIEM, ya una vez configurado los servidores SIEM, se procede a realizar una simulación de ataque por *malware*. Luego de realizar esta simulación de ataque, se verificó el comportamiento de cada SIEM, realizando un análisis técnico comparativo entre ambos servidores.

Finalmente, se analizan y evalúan las respectivas gráficas generadas por ambos servidores: *Wazuh* y *AlienVault*, demostrando ser dos herramientas claves de seguridad y que pueden ser utilizadas con facilidad en operaciones de ciberseguridad.

Estas herramientas proporcionan una rápida respuesta ante un ataque, ofreciendo una alta forma de detenerlos sin tener cuida alguna a la red o perdida de información

Las conclusiones del trabajo tienen como fin determinar una solución implementada proporcionando medios de protección eficaces a distintos ciberataques que se observan en la actualidad.

Palabras clave: SIEM, *Wazuh,* ciberseguridad, *Malware*, *Alien Vault*

ABSTRACT

The present project is based on the implementation of two SIEM servers: Wazuh and AlienVault, with the purpose of evaluating the security status of each SIEM, protecting, detecting, and analyzing attacks in real-time.

First, to carry out this activity, a study must be conducted by visiting the official websites of each SIEM tool to observe their respective hardware and software specifications, obtaining information for their proper functioning. After obtaining the aforementioned information, the two SIEM servers are implemented and configured.

Next, the network topology must be implemented using an emulator called GNS3 to establish connectivity between both servers. Once the SIEM servers are configured, a malware attack simulation is performed. After performing this attack simulation, the behavior of each SIEM is verified by conducting a comparative technical analysis between both servers.

Finally, the respective graphs generated by both servers, Wazuh and AlienVault, are analyzed and evaluated, demonstrating that they are two key security tools that can be easily used in cybersecurity operations.

These tools provide a quick response to an attack, offering an effective way to stop them without causing any harm to the network or loss of information.

The conclusions of the work aim to determine an implemented solution providing effective means of protection against various cyberattacks observed today.

KEYWORDS: SIEM, *Wazuh, cybersecurity*, *Malware*, *Alien Vault*

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 de *malware* 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

- Examinar 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 estos. 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, se ejecuta un ataque de malware 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

La seguridad de la información o seguridad de datos es un conjunto de medidas preventivas, que permiten resguardar y proteger a toda la información existente de los accesos no autorizados [1]. Es fundamental conocer las principales topologías que

existen para dar protección a la información como la seguridad del hardware, la red y el software [1].

La función de la seguridad de la información es formar distintas protecciones a varias organizaciones siendo privadas o públicas tomando prevenciones desde los diferentes procesos que tienen relación en la organización, tomando la gestión de recursos disponibles y considerando los riesgos que permitan balancear los objetivos de seguridad dando un mejor soporte [2].

Hoy en día la tecnología permite acceder a varios sitios donde proporcionan una gran de información como también se puede acceder a sitios donde puede ser vulnerable y tener problemas de seguridad con solo dar un clic [3]. Al momento de ingresar a aún sitio web se puede encontrar con un ciberataque con personas maliciosas que pueden robar la información personal, información importante de alguna organización o envíos de dinero sin autorización [3].

Para tener una buena seguridad de la información se debe tener un proceso de buenas prácticas que permitan proteger y resguardar la información, encontrando estos objetivos en la norma ISO 27001 [1] [3]. Esta ISO implemento la regla para la creación de un sistema de gestión de seguridad, teniendo en cuenta 3 aspectos conocidas como la triada de la seguridad de la información que son:

Integridad. - es la forma que se muestra la información desde el momento que fue realizada, sin tener alguna alteración sin que se lo hayan autorizado los mandos. El objetivo es proporcionar una transmisión segura evitando riesgos, utilizando protocolos de seguridad [1] [3].

Confidencialidad. – es la garantía que solo algunas personas o autoridades tienen acceso a esa información sin ser divulgada. La compartición de la información debe ser autorizada [1] [2].

Disponibilidad. – es la forma de tener el acceso a la información en todo momento sin importar que sea el personal de trabajo o autoridades. Pero para tener acceso se deben tener soportes y medidas de seguridad para que puedan ingresar a la información cuando sea necesario [1] [3].

Información de trabajo que tienen las empresas

Hoy en día las organizaciones, empresas trabajan con 3 tipos de información sin importar la actividad o sector que se encuentren, para realizar una protección adecuada:

Crítica. - Esta información es indispensable para el perfecto funcionamiento de la empresa y sus operaciones, es la que establece los beneficios a medio y largo plazo. Se toman decisiones diarias donde se ve las operaciones y la garantía de continuar el negocio para evitar interrupciones y pérdidas financieras [2] [3].

Valiosa. - Esta información permite que la empresa siga adelante, todo varía según las necesidades su necesidad la ven como valiosa o no, ya que depende de la actividad y el sector que se encuentren [2] [3].

Sensible. - Es la información sensible que tiene cada empresa, solo tienen acceso las personas autorizadas, la seguridad tiene que garantizar la protección de los datos del cliente [2] [3].

Amenazas de seguridad informática

En los últimos años los ataques por personas maliciosas han ido aumentando, dañando así a las organizaciones o empresas que no cuenten con una seguridad informática, estos ataques pueden ser diseñados para robar información o provocar colapso de servidores. Para evitar todo esto es necesario conocer y estar actualizado sobre todo los tipos de ataques, su funcionamiento y qué medidas se puede tomar para evitarlos [4] [5].

En algunas organizaciones o empresas se presentan la parte de vulnerabilidades y amenazas que hoy en día son muy comunes de detectar, los ataques cada día van buscando la forma de explotar todas las vulnerabilidades que puedan encontrar en una organización. Para ello se procede a conocer los ataques más comunes que se pueden tener [4] [5].

Ataques comunes

En la Figura 1.1.1 se observan los ataques más comunes a los que están sometidas las empresas o las diferentes organizaciones en el día a día.

Figura 1.1 Ataques más comunes en las organizaciones o empresas *[6]*

Ataque *phishing*. - Este ataque permite obtener información personal o confidencial como por ejemplo números de tarjetas de crédito, contraseñas del usuario, etc. Estos atacantes usan aplicaciones conocidas, muy utilizadas o generan correos formales en donde explican que deben ingresar a un enlace muy similar a una página oficial. Al momento de ingresar piden el usuario, contraseña o algún dato importante para así robar la información sin ser detectado [5].

Por ello las organización o empresas tienen el protocolo de no brindar cualquier información sea por correo o por vía telefónica asegurando así que el usuario caiga en los ataques de estafas [5].

Correo no deseado o *Spam*. – El ataque *Spam* es la acción que toma el atacante enviando varios mensajes no deseados. Donde los correos pueden ser de publicidad, políticas o en algunos casos ciberataques donde se filtran virus informáticos o algún *malware* [5].

Este ataque permite descargar un archivo infectado dando entrada al atacante y que pueda acceder a su información en todo su equipo [5].

Este ataque hoy en día fue puesto en práctica en las redes sociales las cuales hacían creer que habían ganado algún premio accediendo a un enlace dando entrada así al ciberataque robando toda su información [5].

Amenazas internas. – Este ataque conlleva más al personal que tiene cada organización o empresa la cual se ve a la hora de ingresar al sistema, ya que son los que tiene autorización para acceder a la información cualquier error que ellos comentan puede resultar una entrada a toda la información que puede ser utilizada por terceros [5].

También hay casos que el personal es el responsable de filtraciones de información ya sea de forma involuntaria o no. En este caso las organizaciones educan al personal con clases de ciber seguridad para evitar algún inconveniente futuro [5].

Inyección SQL. – El código SQL o Lenguaje de Consulta Estructurada es introducido por el atacante a una página web, para ingresar a la base de datos sin usar ninguna contraseña [5].

El SQL se utiliza para diseñar, administrar base de datos y acceder a toda la información almacenada [5] [7]. Los atacantes analizan todas las vulnerabilidades para ingresar un comando específico que permita la ejecución del SQL otorgando el acceso sin autorización [5] [7].

Para evitar este ataque es necesario gestionar los sitios web que se utiliza, la responsabilidad de hacer toda esta gestión es la propia organización o empresa [5] [7].

Ataque de denegación de servicios (DDoS). - Este ataque envía numerosas solicitudes a un servidor o red con la finalidad de superar la capacidad de respuesta. Al momento que deja de funcionar el atacante tiene un blanco fácil para realizar su ataque [5].

Malware. – Es un *software* malicioso que tiene la función de explorar las vulnerabilidades del sistema, para adquirir permisos para su ingreso sin autorización. Dentro de este ataque se tienen varias amenazas las cuales se encuentran ilustrativamente Figura1. y que se han identificado hasta el día de hoy [4] [5].

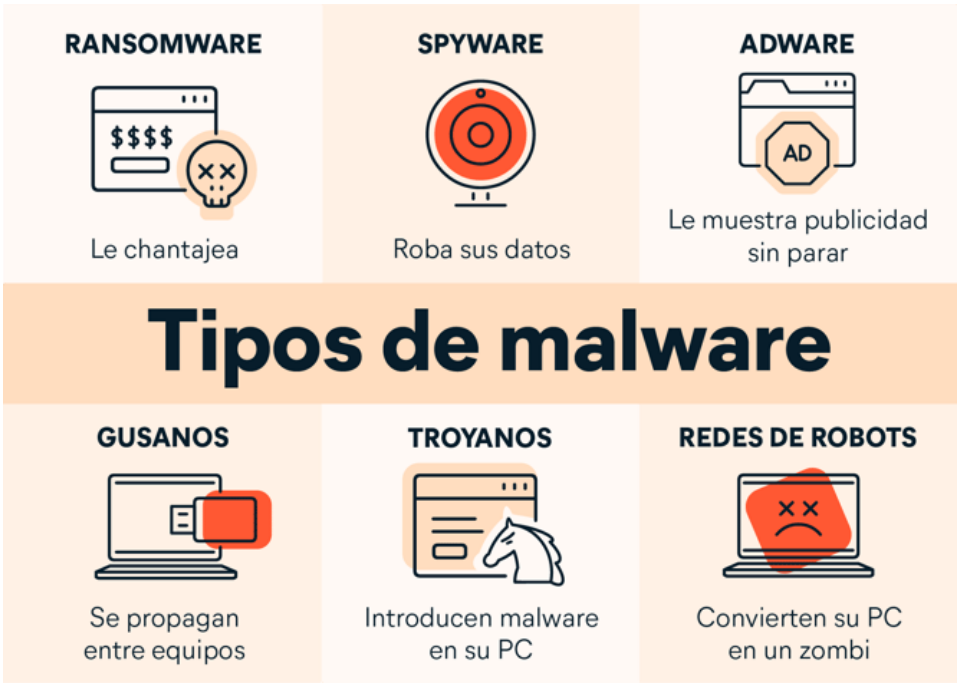

Figura1.2 tipos de *malware [8]*

- **Virus:** es un software que se instala en una aplicación o dispositivo con el fin de dañar o causar problemas en sus funciones. Para que este virus actúe necesita la ayuda del usuario o atacante que le permita el ingreso a su sistema siendo intencionado o no [4].
- **Gusanos**: es el ataque más común que tienen las organizaciones o empresas, infectando a todo el equipo o el sistema. La finalidad que tiene este ataque es la de replicarse e infectar una gran cantidad de dispositivos en una red [4].
- ***Ransomware*:** este ataque es el más conocido por las organizaciones o empresas ya que empieza a obtener toda la información en forma encriptada,

impidiendo el ingreso a la base de datos pidiendo un rescate para liberar toda la información un ejemplo de este ataque es el parte de las criptomonedas como bitcoins [4].

- **Troyanos:** son programas que se instalan en el dispositivo sin que sean detectados por el usuario. La finalidad que tiene este ataque es poder abrir puertas para que el atacante pueda robar la información o poder implementar el software malicioso [4].

Ataque Troyano

Este ataque es conocido como el caballo de Troya ya que permanece escondido en algún programa inofensivo o en alguna página web de descarga. Al entrar en contacto con cualquier aplicación en donde se encuentre el troyano este se activa y permite el acceso al atacante [9] [10].

Los troyanos entran en la categoría de *malware,* pero son utilizados frecuentemente para realizar los ataques de *Ransomware,* para el robo de información a través del software [9] [10].

El *malware* troyano se puede clasificar en varios tipos ya depende de la acción que se realice en el dispositivo, estos son algunos ejemplos:

- **Troyano Bancario:** El objetivo de este ataque es robar la información de los sistemas bancarios como pagos, tarjetas de créditos o débito [9] [10].
- **Troyano *Downloader*:** Permite descargar e instalar versiones actuales de programas maliciosos en los dispositivos incluyendo el troyano y *adware* [9] [10].
- **Troyano *DDoS*:** Ataque de denegación de servicio contra una dirección web, se envía numerosas solicitudes desde una o varias computadoras desbordando la dirección y provocando una denegación de servicio [9] [10].
- **Troyano *Exploit*:** Son programas que contienen códigos que aprovechan una todo tipo de vulnerabilidades que tiene el dispositivo que se ejecutan todas las aplicaciones [9] [10].
- **Troyano *Backdoors*:** Ataque de puerta ofrece a los atacantes monitorear o tener el control a largas distancias del dispositivo infectado donde se envía, se recibe y eliminar archivos. Este ataque a menudo se utiliza para crear grupos de computadoras y formar una red zombi (*Botnet*) para sus fines delictivos [9] [10]. Hoy en día el ataque troyano incorpora funciones de *backdoor* para que el

atacante tenga acceso a la máquina cuando él quiera. Los *backdoors* puros ya vienen instalados en los sistemas o aplicaciones que el usuario utiliza a diario, ya sea por el desarrollador se olvidó bloquear o quitar esa funcionalidad [11] [12].

Un *Backdoor* es un virus que permite monitorizar al equipo infectado desde un lugar lejano. Son considerados peligrosos ya que explotan todas las vulnerabilidades para ingresar a cualquier equipo de forma inadvertida y robar su información sin que se dé cuenta [11] [12].

Pero no todos los *Backdoors* son virus, algunos permiten realizar tareas, mantenimiento o actualizaciones en los equipos sin que el usuario este presente [11] [12].

Para saber que si tiene el *Backdoors* se nota un rendimiento no tan notorio en la parte apariciones de publicaciones o diálogos pidiendo datos personales como las cuentas bancarias o contraseñas. Para su detección es necesario tener actualizado el antivirus y el *firewall* para que ellos sean los encargados de detectar alguna vulnerabilidad [11] [12].

Para su protección se debe tener un buen antivirus que permita detectar cualquier amenaza en tiempo real, que se mantenga actualizado a cualquier amenaza que pueda aparecer en un futuro [11] [12].

Blueteam

Es un grupo de profesionales en el área de seguridad cibernética que su finalidad es proteger y salvaguardar la información de las empresas y ciertas organizaciones de los atacantes cibernéticos [13] [14].

El *Blueteam* es la encargada de la detección y prevención de intrusos, dando una respuesta rápida y efectiva a la misma. Ya que son un equipo diciplinado especializados en analizar el comportamiento de los sistemas de una empresa, estudiando el comportamiento de sus usuarios y equipos para encontrar la solución más rápida de cualquier incidente que haya sido pasado por inadvertido [13] [14].

El *Blueteam* trabaja con una seria de pasos los cuales se explicarían a continuación:

- Reunir datos para la documentación sobre todo lo que hay que proteger y efectuar un análisis de riesgo [13] [14].

- Reforzar el acceso al sistema de múltiples formas como políticas estrictas en la parte de seguridad y ejercicios didácticos con todos los trabajadores para su entendimiento [13] [14].
- Se establecen protocolos de vigilancia ya que se puede registrar toda la información e ir comprobando toda actividad inusual [13] [14].
- Comprobaciones periódicas como auditorias del sistema DNS, verificando la parte externa e interna si tiene alguna vulnerabilidad [13] [14].
- Realizar evaluaciones de riesgo identificando las amenazas con cada activo y debilidades que se pueda encontrar [13] [14].

Blueteam utiliza una variedad de técnicas de seguridad y tiene varias herramientas las cuales permiten monitorear la red, análisis de logs, vulnerabilidades, detección de *malware* y análisis de penetración [13] [14].

Las herramientas que utiliza *Blueteam* permiten ayudar a identificar y proteger a los sistemas y redes de una organización, las más conocidas son las que se presentan a continuación:

- Herramienta de monitoreo: monitorea el tráfico de red en ese momento, identificando patrones y anomalías [13] [14].
- Herramienta de análisis de vulnerabilidades: escanea a la red para la búsqueda de vulnerabilidades para poder corregir y evitar cualquier ataque [13] [14].
- Herramienta de detección de *malware*: detecta y alerta cuando se produce una actividad maliciosa en la red o en el sistema [13] [14].
- Herramienta de gestión de parches: mantiene a los sistemas y software actualizados con las ultimas correcciones de seguridad [13] [14].
- Herramienta de análisis de *logs*: analiza el registro de actividades de la red y de los sistemas para evitar ataques [13] [14].
- Herramienta de respuesta a incidentes: investiga y responde con rapidez a la amenaza detectada [13] [14].
- Sistema de gestión de información de seguridad (SIEM): El SIEM recopila y relaciona datos de seguridad de múltiples fuentes en donde se encuentra varios sistemas de seguridad [13] [14]

Sistema de gestión de información de seguridad (SIEM)

Es una tecnología que permite detectar y neutralizar las amenazas antes de que ocurran. Su finalidad es poder brindar seguridad evitando cualquier ataque teniendo una visión global de la seguridad de la tecnología de la información [15] [16].

La tecnología SIEM es la combinación de dos categorías SEM (gestión de eventos de seguridad) y SIM (gestión de información segura) [15] [16].

- SEM: permite centralizar el almacenamiento y permite un análisis en tiempo real, detectando algún patrón anormal [15] [16].
- SIM: recopila los datos a largo plazo en un repositorio para luego analizarlo, proporciona informes automatizados [15] [16].

Su funcionamiento es proporcionar alertar a una alta velocidad, la visibilidad y la capacidad de detectar amenazas hace más fácil el trabajo de los analistas viendo el mejor modo de actuar a cualquier ataque [15] [16].

Herramientas del SIEM

Para el trabajo que realiza el SIEM se puede encontrar una gran variedad de opciones, aquí lo importante es encontrar una herramienta que vaya con las necesidades de la empresa o de las organizaciones y poder costearlo ya que algunas son pagadas y tienen más funciones que una gratuita, por ello se debe investigar a fondo cada característica que tenga el SIEM [15] [16].

Para algunas empresas y algunas organizaciones utilizan estas herramientas para poder contralar toda su vulnerabilidad:

- **QRADAR**: plataforma de gestión de seguridad, obteniendo información simultanea y soporte de políticas. Verifica los sucesos de seguridad y las vulnerabilidades que puede tener la red [15] [16].
- **ARC SIGHT:** solución por HP dando un potente y adaptable, ofreciendo información de datos y análisis de amenazas en tiempo real [15] [16].
- ***ALIEN VAULT*:** es una herramienta que permite gestionar la seguridad informática como los eventos causados [15] [16].
- **SYMANTEC**: conocida como principalmente por su software antivirus para la seguridad informática [15] [16].

- **McAfee**; conocida por desarrollar soluciones de software para la protección de dispositivos contra los ciberataques [15] [16].
- **FORTINET:** especializada en productos y servicio de seguridad de la red para su protección contra amenazas [15] [16].
- ***WAZUH***: plataforma de código abierto, implementado para la detección de amenazas basados en el host [15] [16].

Seguridad en hardware y software

Seguridad del hardware

Relacionado con la protección de los dispositivos que se usan para el acceso de la información como los sistemas, redes, *apps* y programas de amenazas exterior [17]. Los métodos utilizados son los siguientes:

- Alimentación ininterrumpida (SAI)
- Servidores *proxy*
- Módulos de seguridad de hardware (HSM)
- *Firewall*
- *Data lost prevention* (DLP)

Permite detectar, examinar las vulnerabilidades de cada dispositivo. Ya que ningún equipo es perfecto por que pueden ser atacados por sus vulnerabilidades que tiene cada equipo [17].

Seguridad de software

Permite guardar la información de los ataques de los hackers u otros riesgos malintencionados con la vulnerabilidad que poseen los softwares, para su protección se requiere de soluciones que puedan aportar modelos de autenticación [17].

Con todo lo mencionado anteriormente se debe tener medidas de seguridad en las empresas o en las organizaciones donde se puede tener peligro como el robo de información delicada la cual pueda producir daños al usuario. Para ello se toma protocolos de seguridad ya explicados como la utilización del SIEM, tener todos los equipos vigilados, tener actualizaciones del antivirus y por último tener un registro de todo lo que se haya hecho en la red [17].

2 METODOLOGÍA

Este presente proyecto se enfoca en la metodología experimental y comparativa. Es experimental por que se analiza dos herramientas del SIEM para la detección de ciberataques a las redes informáticas, simulando ataques de *malware* en una red pequeña de computadoras y con ello se comparar las dos herramientas observando los resultados que tiene cada uno en su interfaz. Y finalmente los resultados se mostrarán de manera simplificada para los usuarios que no tengan conocimiento en el área para que en base a ello se escoja la mejor opción de detección para los ciberataques.

Para la implementación del SIEM se realizaron las siguientes actividades:

- Examinación de diferentes SIEM y sus requerimientos de hardware y software

Para realizar esta actividad fue necesario ingresar a la página oficial de cada herramienta del SIEM para observar sus especificaciones tanto de *hardware* como de software ya que sin esa información se limita el correcto funcionamiento de estas.

- Implementación del servidor SIEM

Basado en el análisis anterior se implementan y configuran dos servidores SIEM, el servidor *Wazuh* y *ALIEN VAULT* para luego ser comparados.

- Implementación de la topología de red

Una vez configurado los servidores SIEM se desarrolló una topología de red mediante un emulador conocido como GNS3 y se estableció conectividad entre ambos, para de esta manera realizar una simulación de un ataque por *malware*.

- Verificación del funcionamiento del SIEM

En este apartado se verificó el comportamiento de cada SIEM, para posteriormente realizar un análisis técnico comparativo entre los ambos.

3 RESULTADOS

Este proyecto permite analizar todo tipo de *malware* como el ataque troyano, utilizando las herramientas de SIEM como *Wazuh* y *Alien Vault*, para la detección y análisis del ataque en tiempo real. Para la implantación de la topología se generó en el GNS3 teniendo un servidor, un agente y un atacante para cada uno de los SIEM. Para la integración del servidor *Wazuh* se utilizó un sistema operativo Ubuntu y para el servidor

Alien Vault se utilizó un sistema operativo Linux con línea de comandos. Se realizó el ataque troyano con el sistema operativo Kali Linux a un agente de Windows dando el acceso a una puerta trasera. Se finaliza con el análisis de los resultados de cada SIEM.

3.1 Análisis de los SIEM y sus requerimientos de hardware y software

Los SIEM *Alien Vault* y *Wazuh* son muy utilizados para la protección de la seguridad de la información, eventos que estén ocurriendo en ese instante. Para la elección de cada plataforma dependerá de la necesidad que tenga la organización como sus recursos, sus características, la capacidad de manejar software de código abierto o comercial y los requerimientos de soporte y mantenimiento.

Requerimientos SIEM *Wazuh*

Es una plataforma de seguridad de código abierto, que tiene varias destrezas para la detección de intrusos, registro de eventos, estados de los archivos modificados y análisis de vulnerabilidades. Las cuales varias empresas y organizaciones la usan para la protección de la información personal o empresarial.

La información obtenida es enviada a los administradores quienes toman la decisión de eliminar el problema. Además, *Wazuh* tiene un sistema de correlación que permite identificar el comportamiento de sistema anónimos, permitiendo la detección de amenazas que podrían pasar sin ser detectadas de forma manual.

La implementación de *Wazuh*, varía según el despliegue, la cantidad de datos que se van a procesar y los servicios adicionales.

Componentes de *Wazuh*

- **Servidor:** recibe los datos de los agentes, creando alertas de seguridad al momento de detectar alguna amenaza o tipo de anomalía.
- ***Inderxador* (*Elastic Search*):** trabaja como motor de búsqueda. Se encarga de registrar y guardar las alertas de seguridad creadas por el servidor la cual tiene un formato JSON ya que todo el análisis se realiza en tiempo real.
- ***Dasboard* (Kibana):** interfaz web amigable para la visualización y análisis.

Requisitos de implementación de *Wazuh*

Se escogió la herramienta Wazuh para el desarrollo de la tesis, ya que es una plataforma de código abierto que permite el monitoreo de la seguridad en las compañías detectando amenazas en tiempo real y verificando los eventos que suceden en ese instante.

Wazuh ofrece una interfaz visual accesible que facilita la visualización de errores y fallas, la cual se permite tener tablas de errores al momento que se detecta alguna amenaza al sistema, presentando gráfica de líneas mostrando las fluctuaciones que tiene al momento que se ve afectado el sujeto, también permite tener graficas de pastel la cual muestran los valores más comprometidos que este generando las amenaza o el valor del recurso más ocupado. La herramienta Wazuh permite tener informes de toda la métrica detalla, los recursos que utiliza para la detección de amenazas y graficas donde muestran las vulnerabilidades y los ataques que pueden realizarse.

En la Tabla 3.1 se observa una variedad de sistemas operativos utilizables para esta herramienta.

Tabla 3.1 Requisitos del sistema operativo para *Wazuh*

Sistema operativo	**Versiones**
Amazon Linux	2
CentOS	7, 8
Red Hat Enterprise Linux	7, 8, 9
Ubuntu	16.04, 18.04, 20.04 22.04, 24.04

Para la ejecución de servidor se necesita la compatibilidad con navegadores tal como se muestra en la **Tabla *3.2***.

Tabla 3.2 Requisitos de Navegador para *Wazuh*

Navegador	**Versión**
Chrome	95 o posterior
Firefox	93 o posterior
Safari	13.7 o posterior

Para la implementación de *wazuh*, en la **Tabla *3.3***, se observa los requerimientos necesarios para ser implementado.

Tabla 3.3 Requerimientos de implementación para *Wazuh*

Agentes	**CPU**	**RAM**	**Almacenamiento**
1-25	4 CPU virtuales	4-8 (GB)	50 (GB)
25-50	8 CPU virtuales	8 (GB)	100 (GB)
50-100	8 CPU virtuales	8-16 (GB)	200 (GB)

Requerimientos SIEM *ALIEN VAULT*

Es una herramienta de gestión de eventos y seguridad de código comercial, que permite analizar y tener datos en tiempo real. Ofrece una solución completa a varias funciones de seguridad en una sola plataforma. Esta herramienta tiene la capacidad de detectar intrusos, el cuidado de la integridad de archivos, el análisis de las vulnerabilidades, el comportamiento y la gestión de la información. Para la detección de eventos proporciona tecnologías de detección de intrusos basados en el comportamiento siendo amenazas conocidas como desconocidas. Tiene su propia interfaz gráfica no necesita de componentes extras para mostrar su interfaz.

Se escogió *Alien Vault*, porque permite tener varias gestiones de eventos y detección de amenazas. Esta herramienta permite tener una rápida respuesta en tiempo real. La única desventaja es que esta herramienta es de servicio comercial o en otras palabras que para poder acceder a todos sus veneficios hay que pagar un valor.

Para su utilización es muy accesible ya que permite entender mucho mejor su plataforma dando datos específicos sobre los recursos utilizados y verificar el atacante dando su dirección IP y el sombre del sistema operativo que esta siendo utilizado para hacer el ciber ataque. Al igual que *Wazuh* permite tener graficas como la de pastel y la gráfica de líneas dando igual varias acciones permitiendo detectar las variaciones que tienen al momento de detectar el ataque o al intruso

Requisitos de implementación de *Alien Vault*

En la **Tabla *3.4*** se ilustran los requisitos de hardware necesarios para su implementación.

Tabla 3.4 Requerimiento de Hardware para *Alien Vault*

Recursos	Mínimo	Recomendado
CPU	4 núcleos	8 núcleos
RAM	8 (GB)	16 (GB)
Almacenamiento	250 (GB) HDD	500 (GB) SSD
Interfaces de red	1 (Gbps)	1 (Gbps)

Para la implementación del *Alien Vault* se tiene la siguiente **Tabla *3.5*** donde se muestra los recursos de software.

Tabla 3.5 Requerimiento de software para *Alien Vault*

Requisitos	Descripción
Sistema operativo	La aplicación está incluida basado en Linux
Navegador	• Chrome versión actual o inferior. • Firefox versión actual o inferior

3.2 Implementación de los servidores SIEM

Cabe mencionar que para la instalación de los servidores es necesario utilizar una máquina virtual con recursos superiores a los que se muestran en la Tabla 3.1**,** esto se consigue hacer mediante la instalación virtual.

Implementación de *Wazuh*

Para la instalación del servidor *Wazuh* se utiliza el sistema operativo Ubuntu 24.04 para posteriormente seguir los siguientes pasos:

Se ingresó al terminal de Ubuntu para ingresar el siguiente comando, el cual es necesario para verificar la conectividad a las URL y transferencia de datos. En la siguiente Figura 3.1 Instalación del CURLse ilustra el comando CURL.

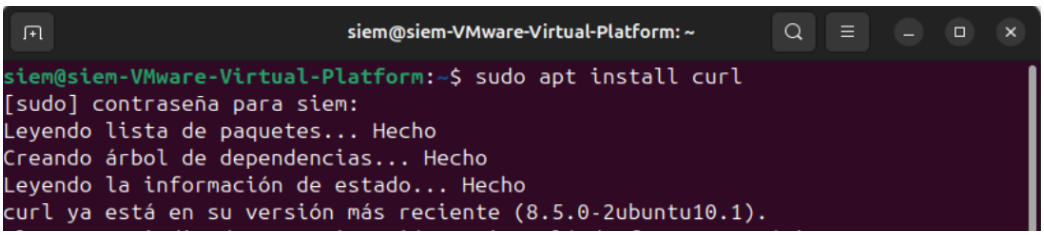

Figura 3.1 Instalación del CURL

Se procedió a bajar el instalador de *Wazuh* usando el comando que se muestra en la **Figura *3.2***.

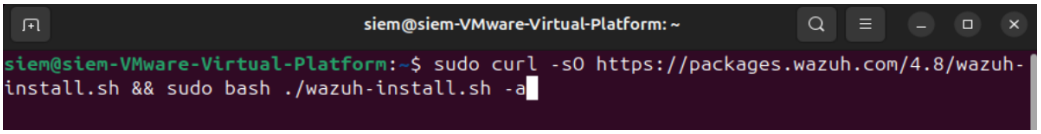

Figura 3.2 Descarga e instalación de *WAZUH*

Ya instalado *Wazuh* se procedió a indicar un usuario y una contraseña, se tiene un claro ejemplo en la ilustración de la Figura 3.3.

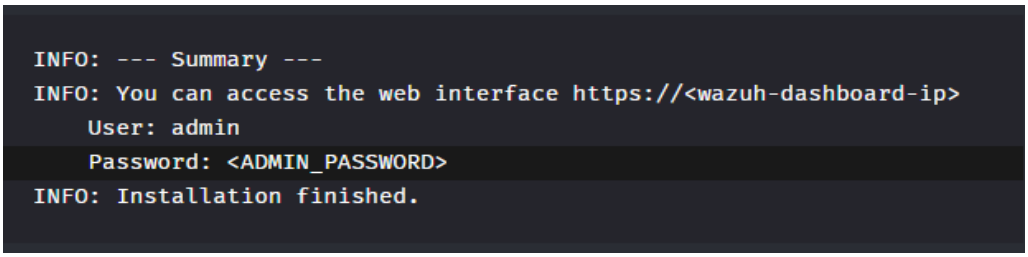

Figura 3.3 Usuario y Contraseña de *Wazuh*

Se confirmó el direccionamiento del equipo donde se instaló *Wazuh*, como se ilustra en la **Figura *3.4***.

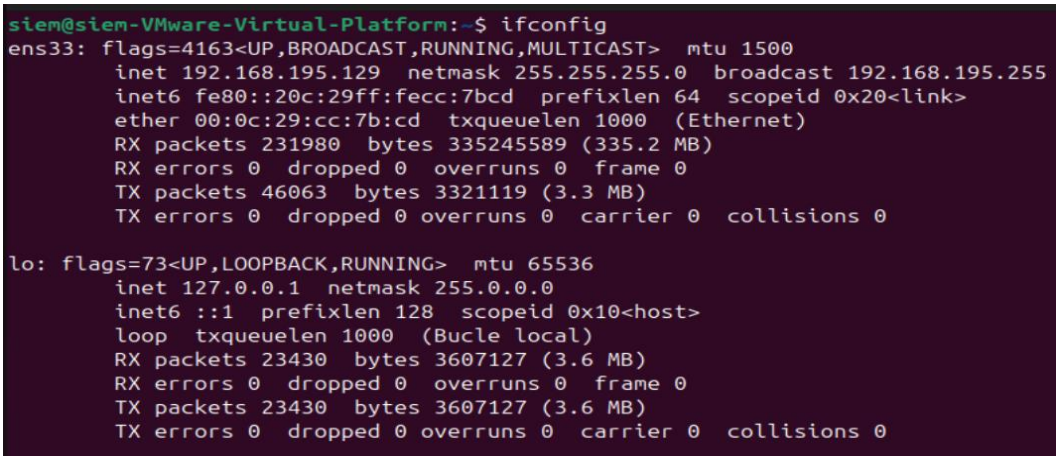

Figura 3.4 Direccionamiento de la máquina virtual

Se ingresa al navegador, para posteriormente ingresar la dirección IP que tiene la máquina virtual, que direcciona a la interfaz de *Wazuh*, como se ilustra en la **Figura *3.5***.

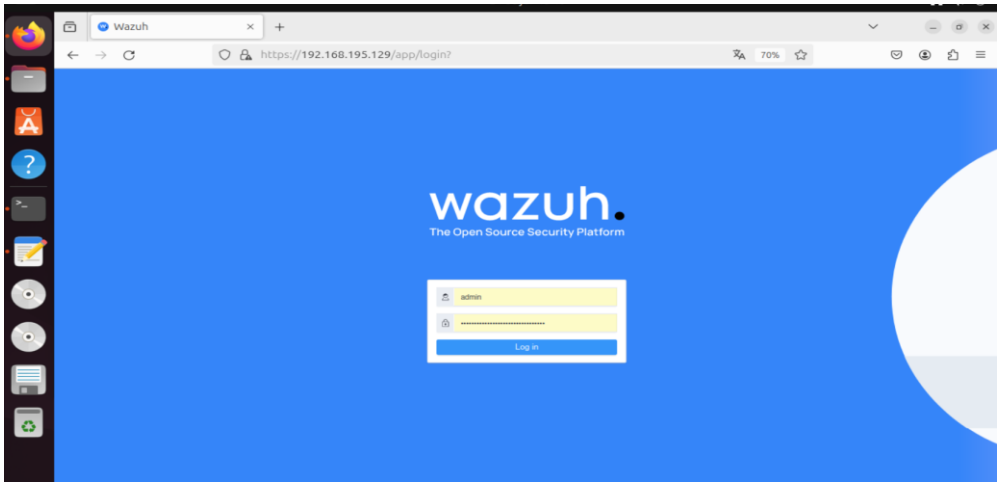

Figura 3.5 Interfaz de *Wazuh*

Al iniciar el interfaz se procede a configurar ciertas extensiones que tiene *Wazuh*, primero ingresando a configuración y luego seleccionando *Sample data* se agrega las tres extensiones tal como se ilustra en la **Figura *3.6***.

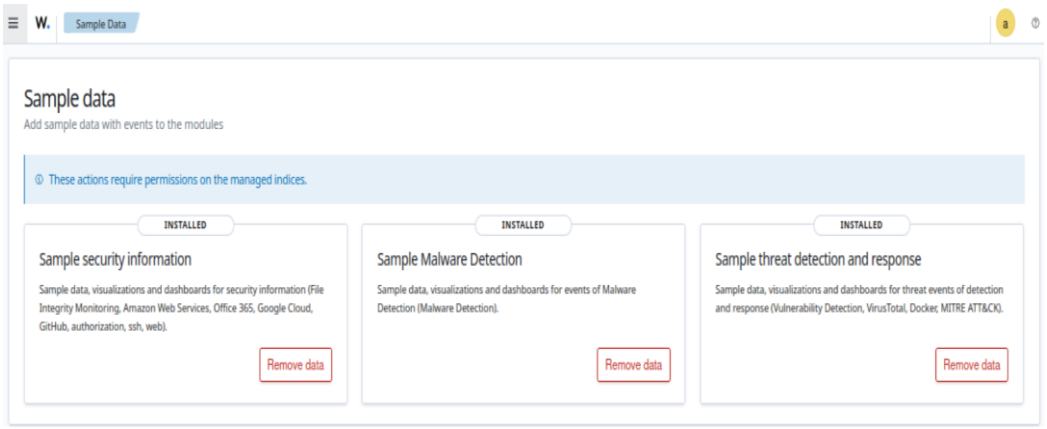

Figura 3.6 Extensiones de *Wazuh*

Con las extensiones ya instaladas, lo que sigue es agregar el agente, para ello es necesario estar ubicado en la pestaña principal y dar clic en la parte de *AGENTS SUMMARY* tal como se ilustra en la Figura 3.7.

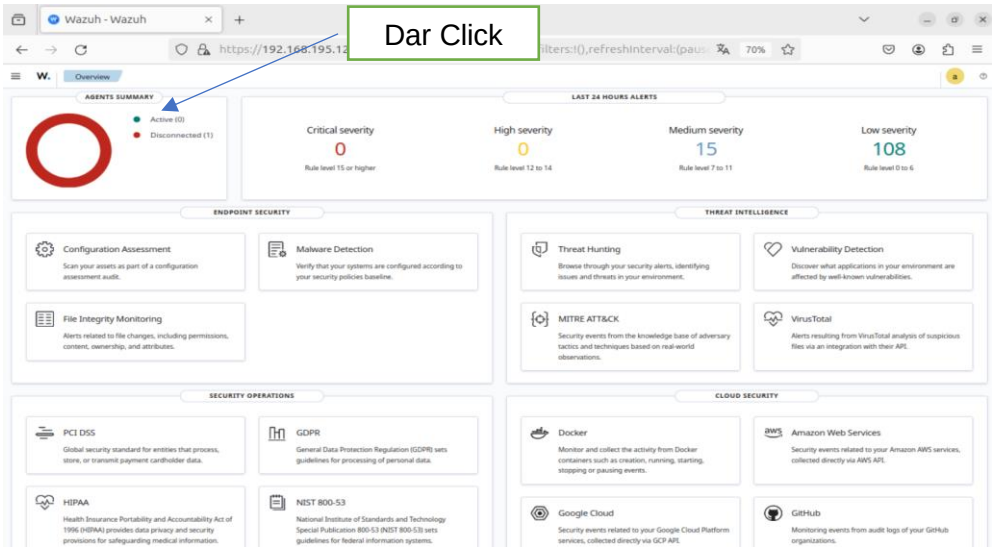

Figura 3.7 Pantalla de inicio de *Wazuh*.

Ya ingresado a *AGENTS SUMMARY,* se selecciona *DEPLOY NEW AGENT* tal como se ilustra en la **Figura *3.8***.

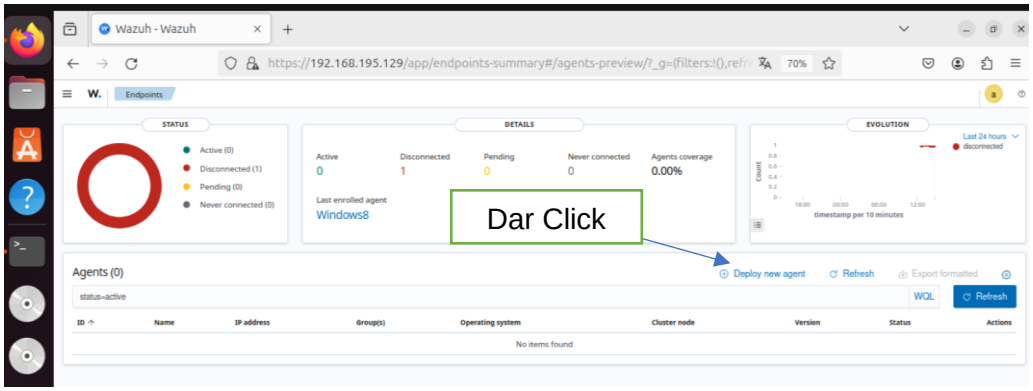

Figura 3.8 Pantalla de AGENTS SUMMARY

Ya iniciado *DEPLOY NEW AGENT,* dará una ventana donde se procede a configurar todo lo necesario para el agente, tal como se ilustra en la **Figura *3.9***.

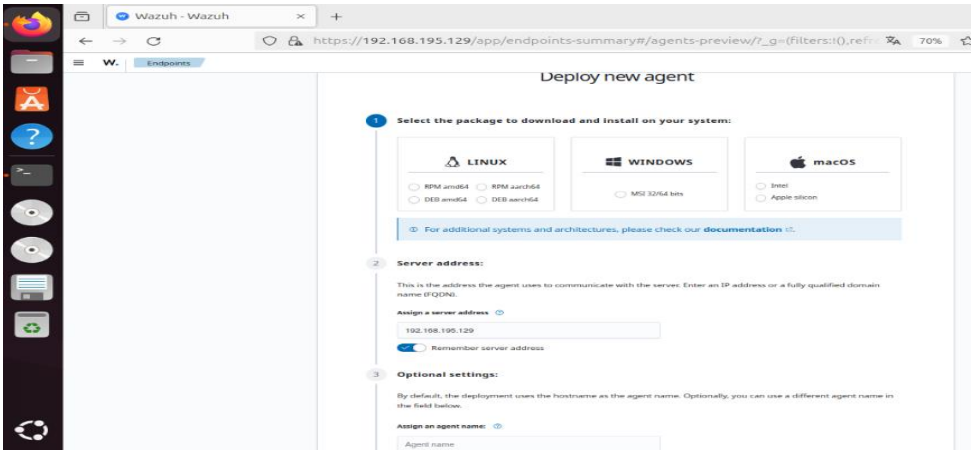

Figura 3.9 Pantalla de DEPLOY NEW AGENT

Se inicia escogiendo el tipo de sistema operativo, todo depende de cual sistema esté utilizando el agente en este caso es *Windows* tal como se ilustra en la **Figura *3.10***.

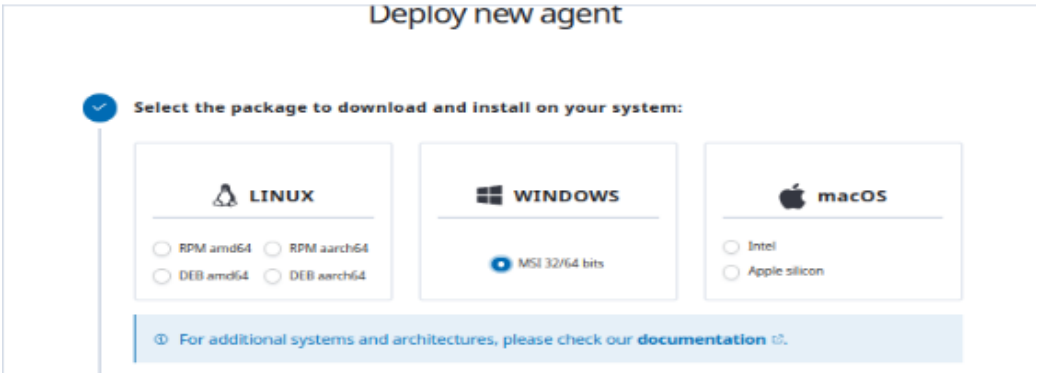

Figura 3.10 Selección de sistema operativo del agente

Luego se ingresa la IP de la maquina donde se instaló *Wazuh* tal como se ilustra en la **Figura *3.11***.

Figura 3.11 Ingreso de la dirección IP del Servidor *Wazuh*

Se escribe un nombre para el Agente y se selecciona un grupo en este caso está por *Default* tal como se ilustra en la Figura 3.12.

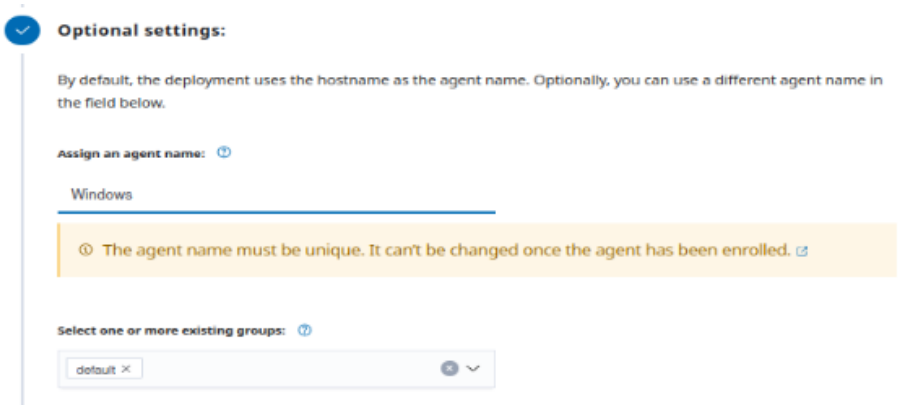

Figura 3.12 Asignación del nombre y del Grupo

Ya ingresado todos los datos, el servidor de *Wazuh*, se genera un comando el cual se debe aplicar en el agente en este caso en Windows. También se genera requerimientos de cómo utilizar el comando generado en *Windows* tal como se ilustra en la **Figura *3.13***.

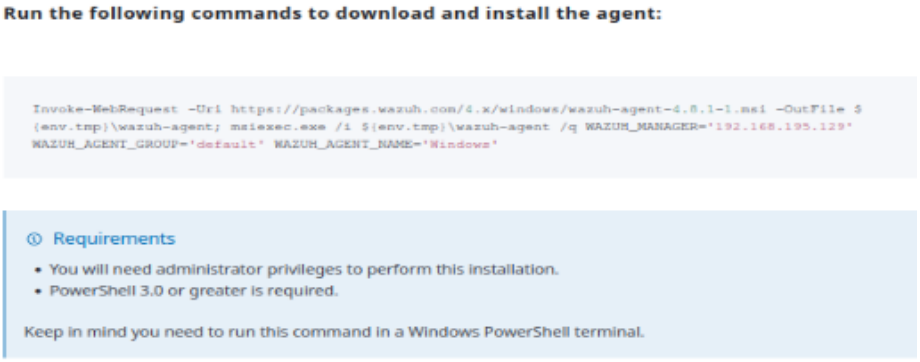

Figura 3.13 Comando para agregar en el Agente.

En *Windows* se procedió a ingresar a la aplicación *PowerShell* para ingresar el comando generado por el servidor *Wazuh* tal como se ilustra en la **Figura *3.14***.

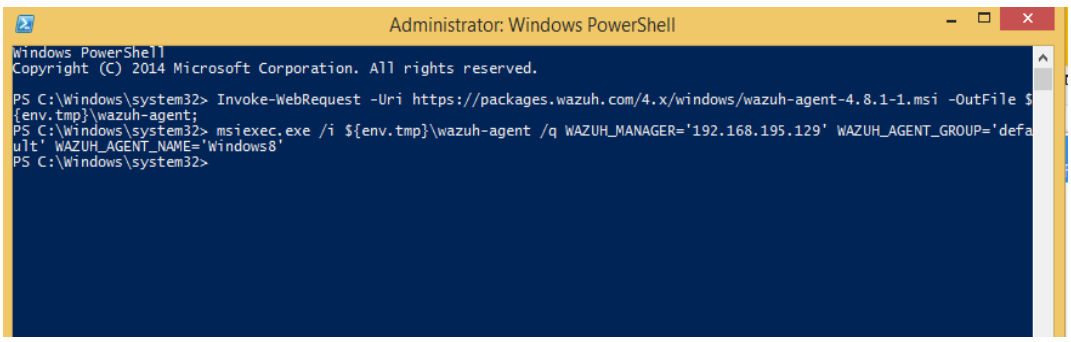

Figura 3.14 *PowerShell* de *Windows*

En la **Figura *3.15*** se muestra cómo se ejecuta el comando al momento de dar *ENTER*.

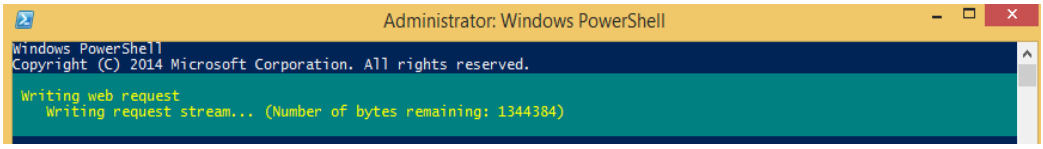

Figura 3.15 Ejecución de comando para la instalación del agente

Por último, se corre el comando que se muestre en la **Figura *3.16***.

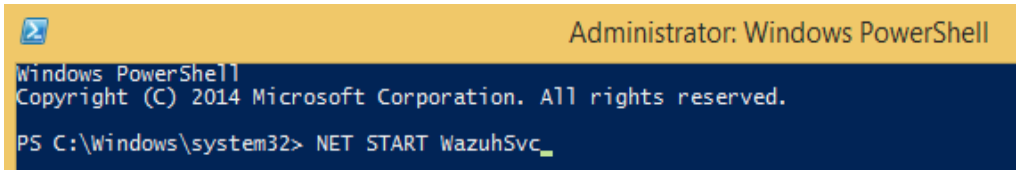

Figura 3.16 Ejecución de comando de inicio del agente

Volver al servidor *Wazuh* y se verifica al agente activado y agregado, como se ilustra en la Figura 3.17.

Figura 3.17 Agente Activado

Implementación de *ALIEN VAULT*

Para la instalación del servidor *Alien Vault* se utilizó el sistema operativo Linux con interfaz de texto, para posteriormente seguir los siguientes pasos:

Para la instalación del servidor *Alien Vault*, se ingresa a la página *Level Blue* donde se procede a descargar el ISO del servidor, así como se ilustra en la **Figura *3.18***.

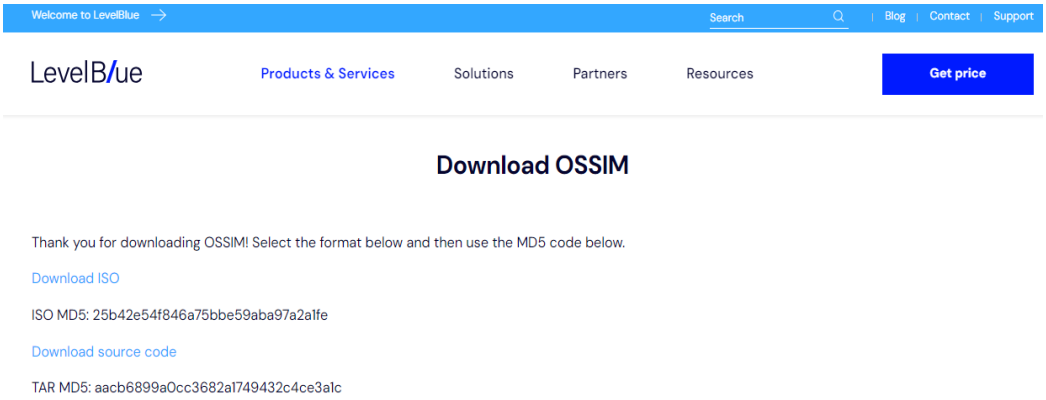

Figura 3.18 Descarga de la ISO *Alien Vault*.

Descargada la ISO se procede a instalar el *ALIEN VUALT* en la aplicación VMware, la cual se configura con todos los requisitos para que su funcionamiento sea el adecuado. En la siguiente **Figura *3.19*** se muestran los requisitos de la instalación.

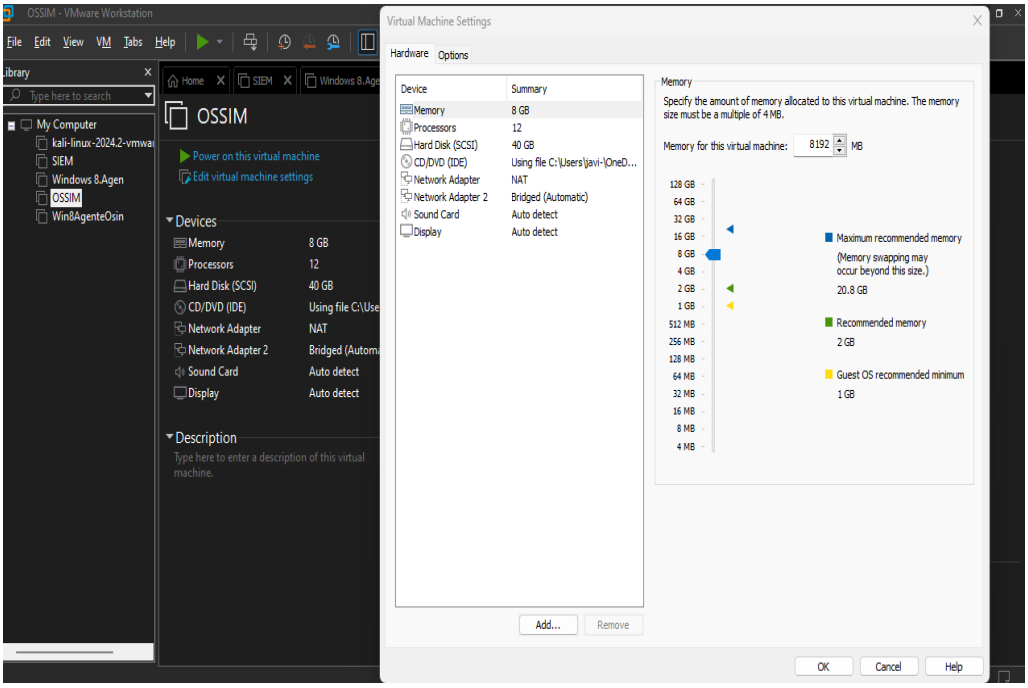

Figura 3.19 Recursos del servidor *ALIEN VUALT.*

Ingresados todos los recursos se procede a iniciar la instalación. La Figura 3.20 ilustra el inicio de instalación.

Figura 3.20 Inicio de instalación de *ALIEN VUALT*

Seleccionado la opción de instalar que muestra la Figura 3.20, en la siguiente **Figura *3.21*** se visualiza la opción de escoger el idioma para toda la interfaz.

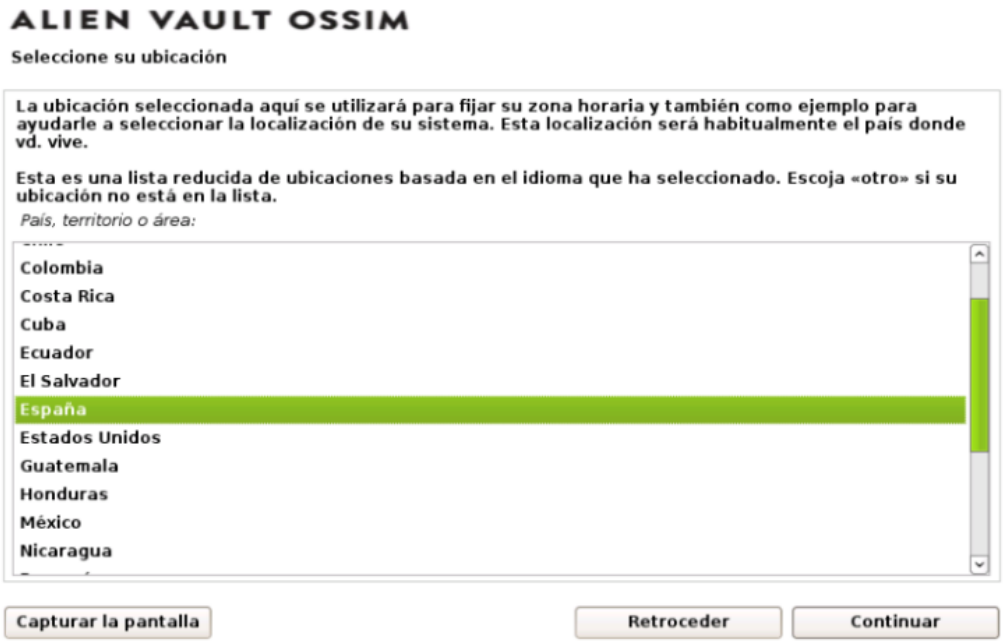

Figura 3.21 Selección de idioma

En la **Figura *3.22*** se presenta una ventana, la cual se debe configurar una dirección IP.

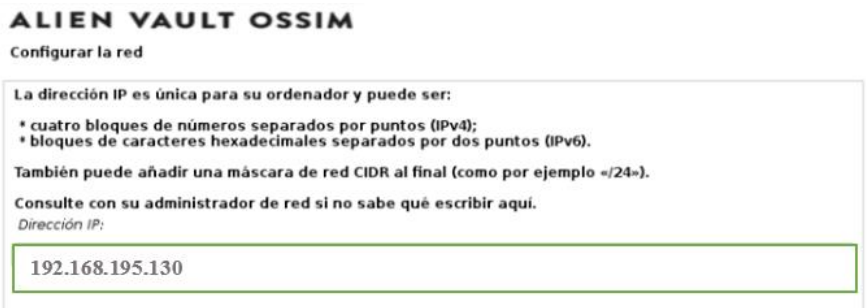

Figura 3.22 Agregación de dirección IP

Ya configurado la dirección se procede agregar su máscara tal como se visualiza en la **Figura *3.23***.

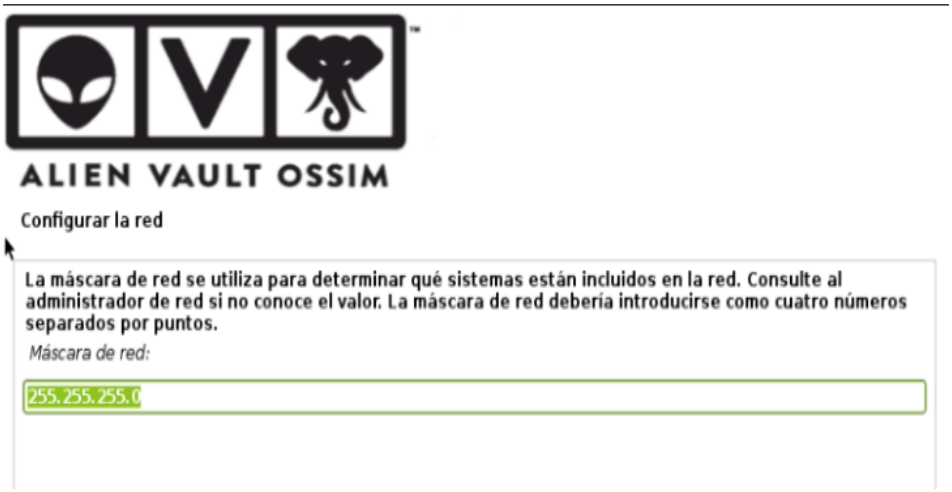

Figura 3.23 Agregación de máscara de red

Ya establecida el direccionamiento se procede a configurar una contraseña, como se ilustra en la **Figura *3.24***.

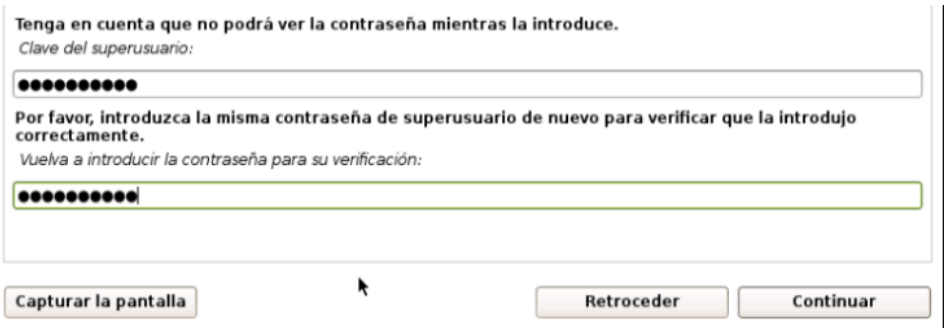

Figura 3.24 Agregación de contraseña

Ya configurado todo lo necesario se procede a la instalación, se espera varis minutos hasta que se complete la instalación tal como se ilustra en la **Figura *3.25***.

Figura 3.25 Proceso de instalación

Ya instalado, se procede abrir la interfaz donde se encuentra el direccionamiento establecido para ingresar al servidor *Alien Vault* tal como se ilustra en toda la **Figura *3.26***.

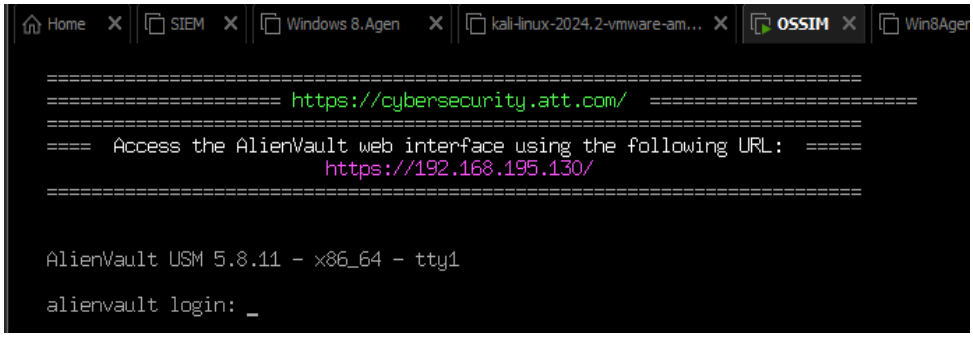

Figura 3.26 Interfaz de *Alien Vault*

En la **Figura *3.27*** se observa el método para ingresar a la interfaz, usando el usuario *ADMIN* con la contraseña establecida al momento de la instalación.

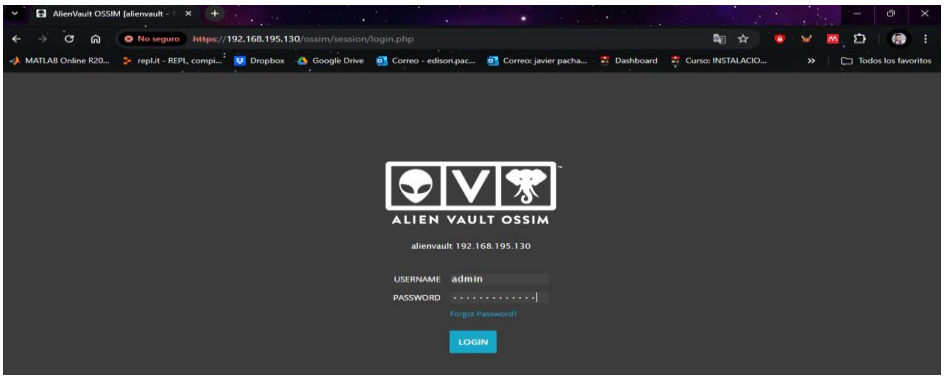

Figura 3.27 Ingreso a la interfaz de *Alien Vault*

Para agregar un agente se realiza varias configuraciones. Empezando desde la parte de ENVIRONMENT y seleccionar ASSETS & GROUPS, tal como se ilustra en la **Figura *3.28***.

Figura 3.28 Acceso a *ASSETS & GROUPS*

Se agrego un nuevo *host,* tal como se muestra en la **Figura *3.29***.

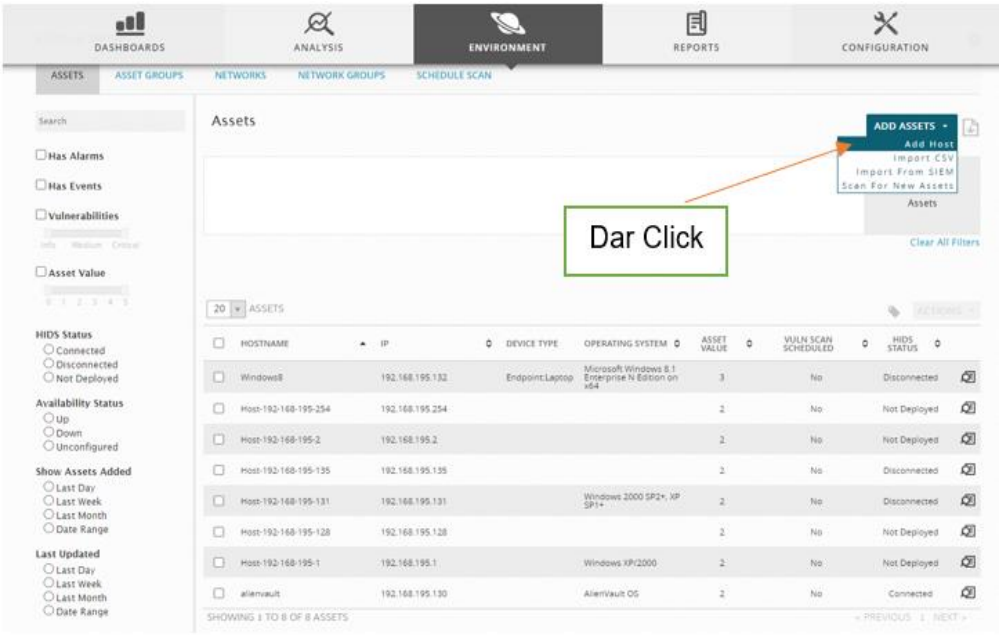

Figura 3.29 Ingresar nuevo *host*

Se ingresó a la ventana que se ilustra en la **Figura *3.30***, la cual permite agregar el nombre del agente, su dirección y el sistema operativo que está utilizando.

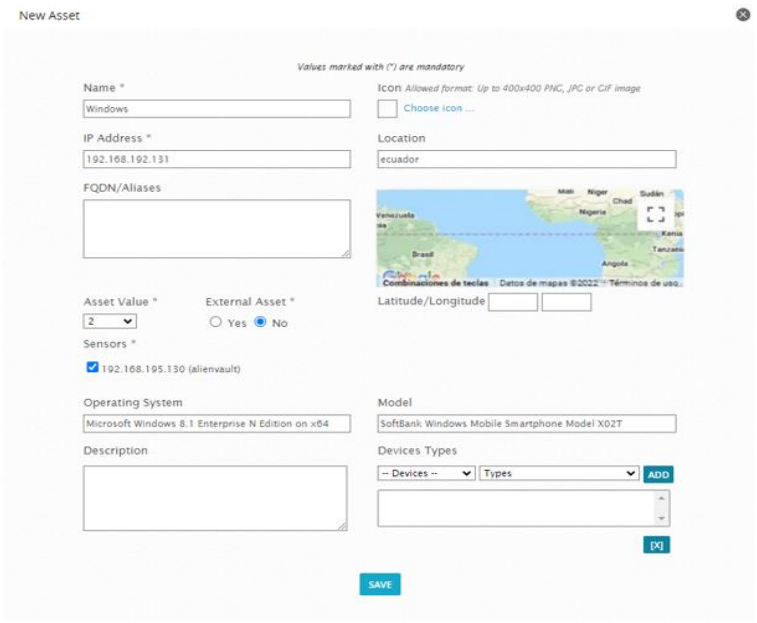

Figura 3.30 Configuración del *host*

Ya establecido el host, se ingresa nuevamente *ENVIRONMENT* y se selecciona *DETECTION* como se presenta en la **Figura *3.31***.

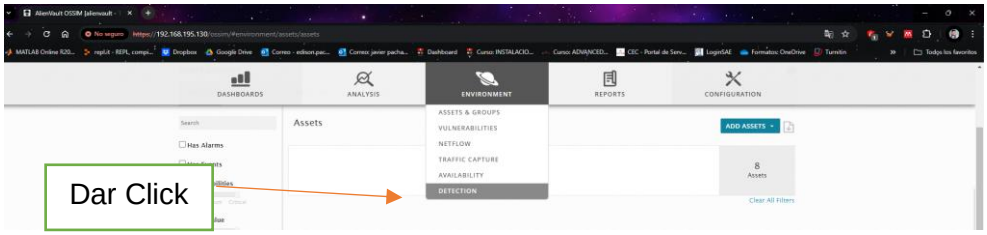

Figura 3.31 Ingreso a *DETECTION*

Ya ingresado, se selecciona la parte de *AGENTS* tal como se ilustra en la **Figura *3.32***.

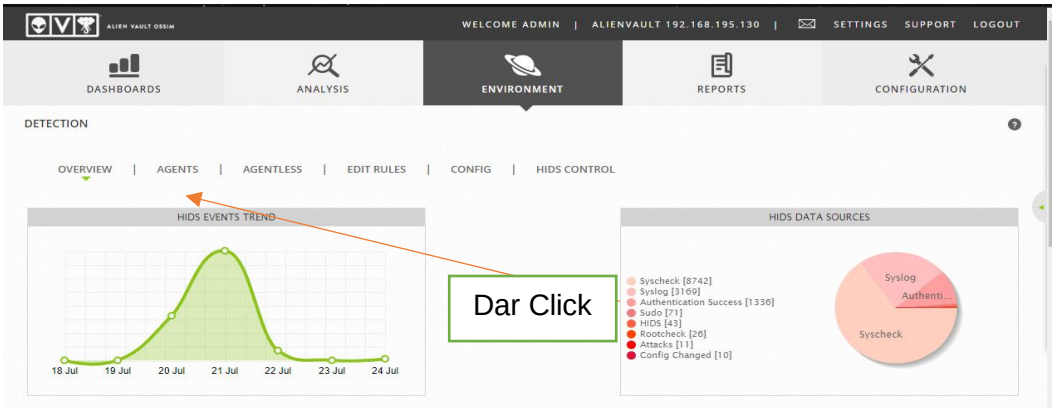

Figura 3.32 Ingreso a *AGENTS*

En la **Figura *3.33*** se observa que se tienen varias direcciones IPs registradas. Para ingresar el agente que se creó anteriormente, se da *Click ADD AGENT*.

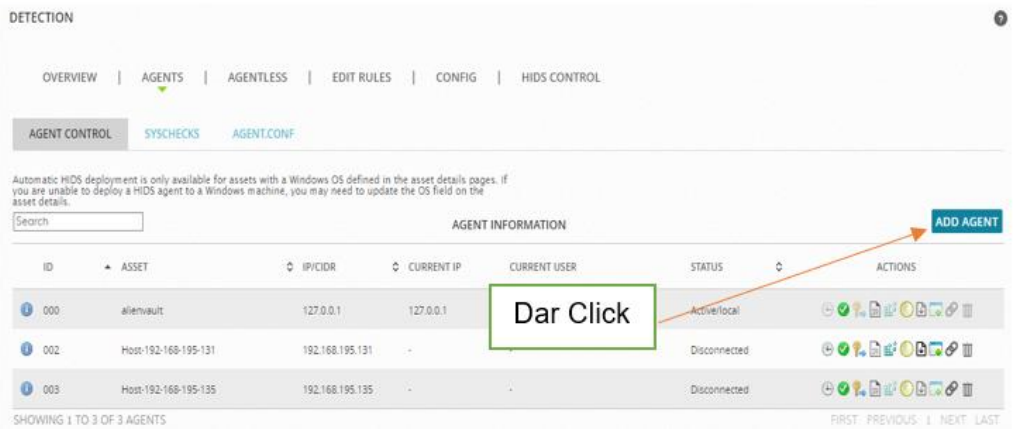

Figura 3.33 Ingreso a *ADD AGENT*

Se abre una ventana, donde se buscará la dirección IP creada anteriormente tal como se muestra en la **Figura *3.34***.

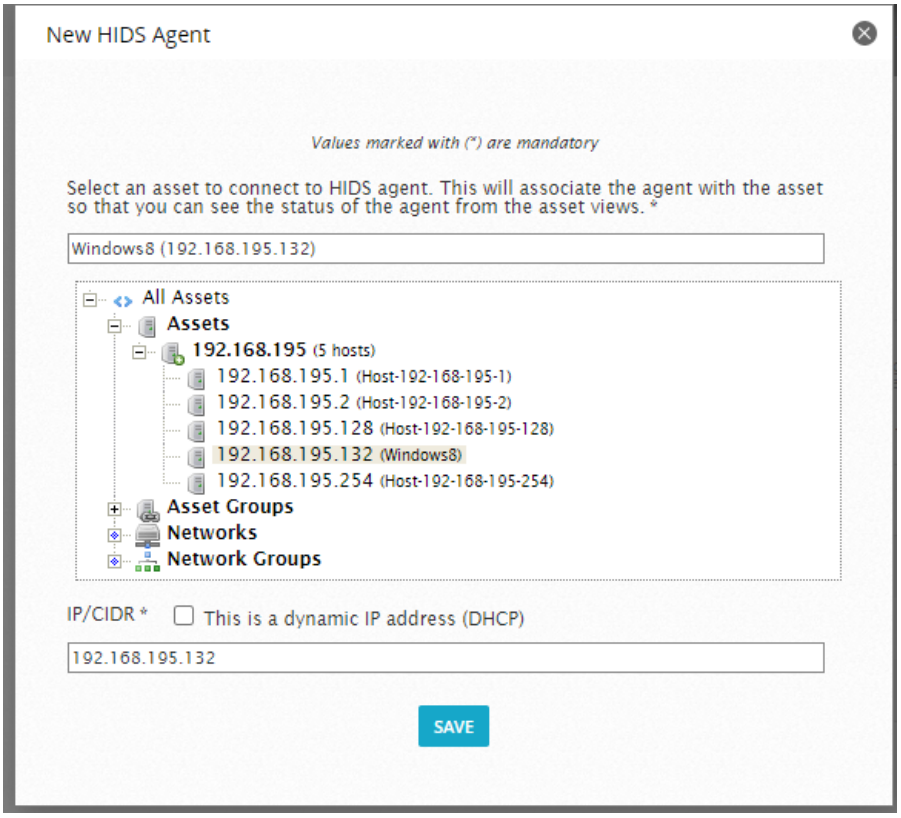

Figura 3.34 Incorporación de un nuevo Agente

Al volver a la ventana de AGENTS se observa que esta agregada la dirección IP que se creó anteriormente, tal como se ilustra en la **Figura *3.35***.

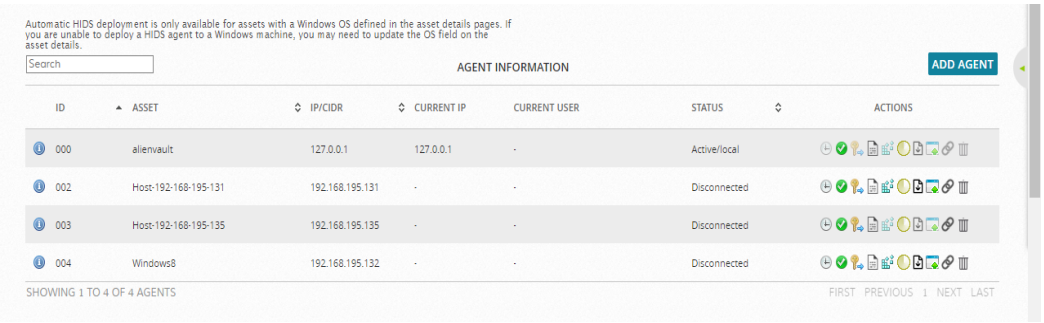

Figura 3.35 Vista al Direccionamiento IP

Para agregar el Agente en el computador se instala un programa si es un sistema operativo Windows o ingresar varios comandos si se utiliza un sistema Ubuntu. En este caso se está utilizando un sistema operativo Windows. El cual el servidor *Alien Vault* permite descargar el programa OSSEC tal como se muestra en la **Figura *3.36***.

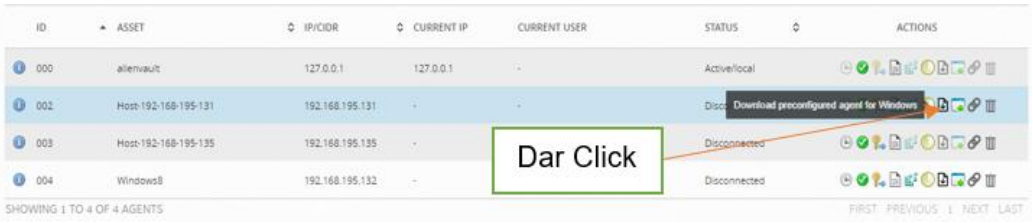

Figura 3.36 Proceso de descargar de la Aplicación

Ya descargado el programa, se procede a instalarlo en el agente Windows, como se presenta en la **Figura *3.37***.

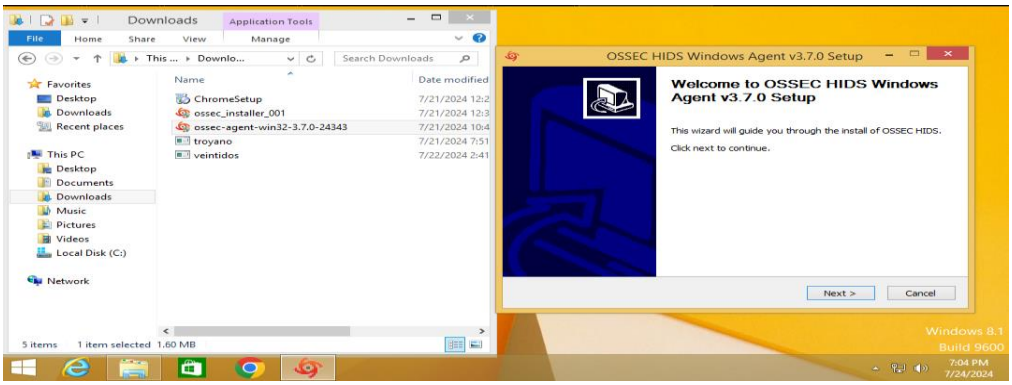

Figura 3.37 Proceso de instalación del programa OSSEC

Instalado el programa se procede a configurar la dirección IP del servidor *Alien Vault*, se ingresa la clave que da el mismo servidor al momento de crear el agente, tal como se ilustra en la **Figura *3.38***.

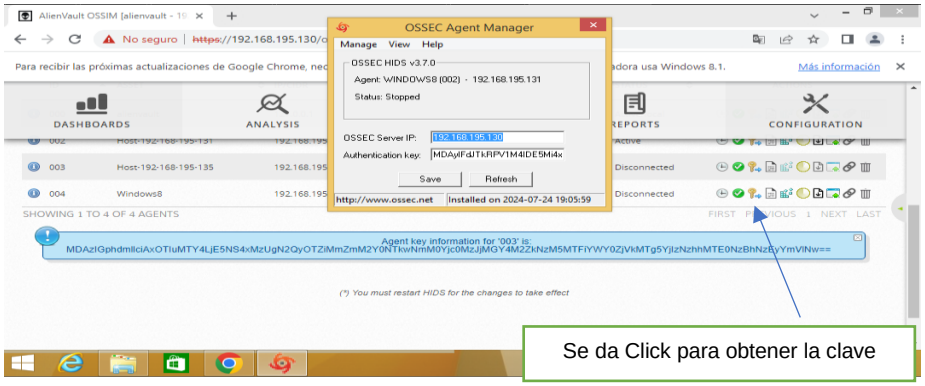

Figura 3.38 Configuración del programa OSSEC

Se guarda la configuración, seguido se da click en *Manage* y click en *Start* y automáticamente empieza a vincularse con el servido, visualizando que la red sale activada en el *Alien Vault* como se ilustra en la **Figura *3.39***.

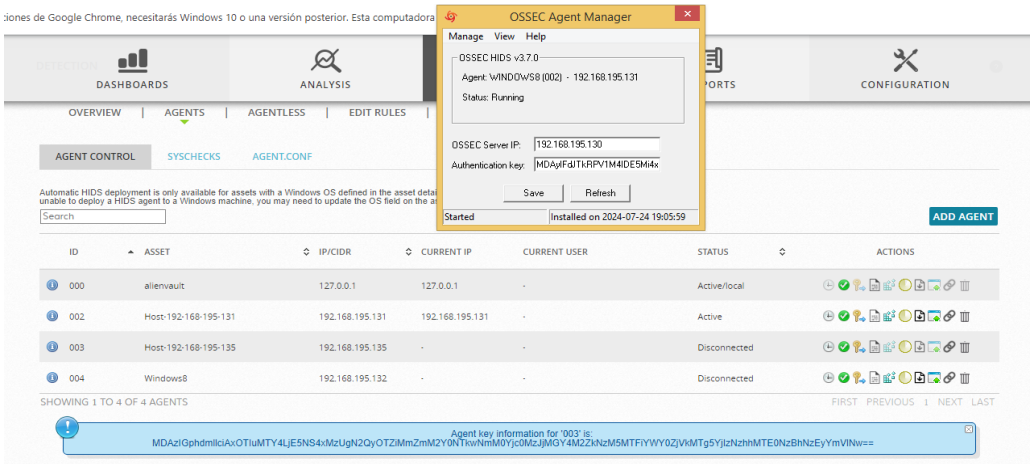

Figura 3.39 Agente activado

3.3 Implementación de la topología de red

Configuración de la topología

Para la implantación de la topología se utilizó el GNS3, donde se puede incluir las máquinas virtuales en las que se trabaja actualmente. En la **Figura *3.40*** se visualiza como se incluyen en el GNS3 las máquinas virtuales.

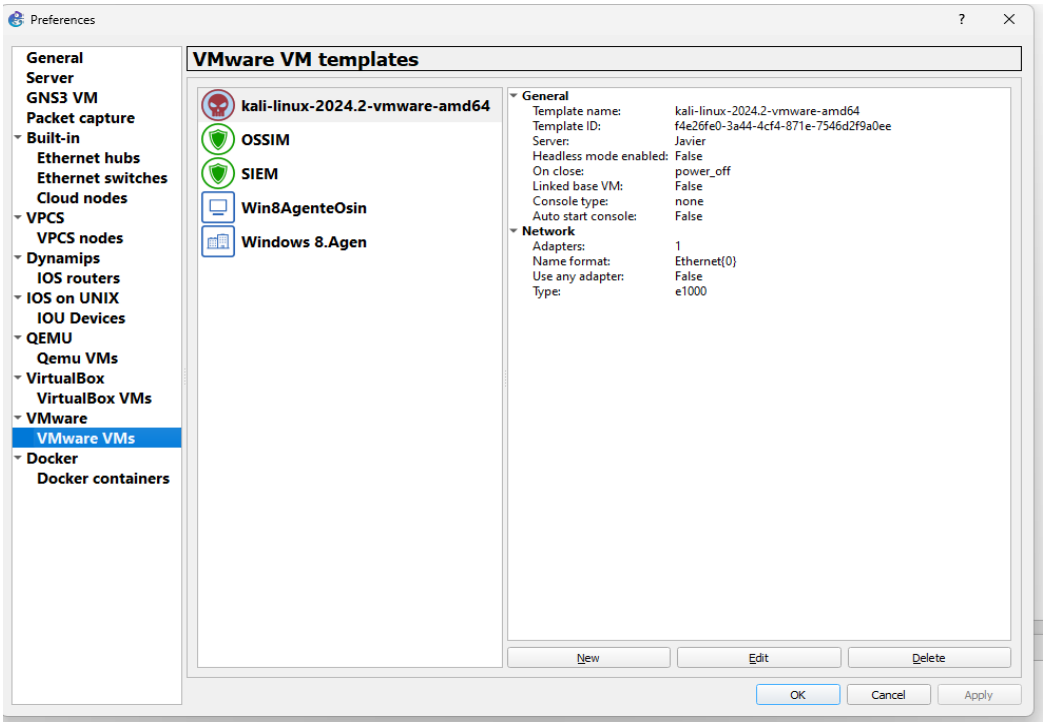

Figura 3.40 Implementación de las máquinas virtuales en GNS3

Se creó una red que se presenta en la **Figura *3.41***. Esta red es utilizada para el servidor *Wazuh*, donde se tiene un atacante, un agente y el SIEM que en este caso es *Wazuh*.

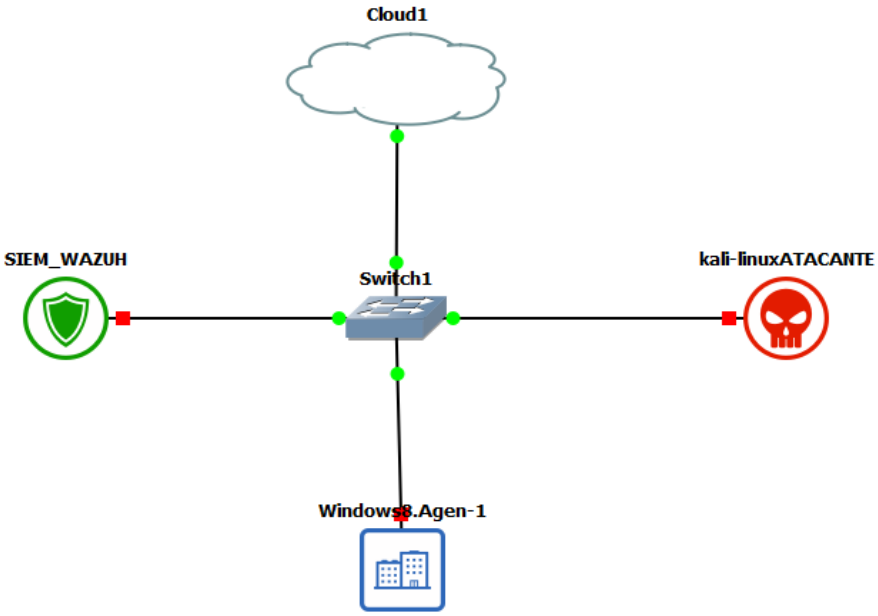

Figura 3.41 Topología del servidor *Wazuh*

Se utilizó VMware para tener conectividad en la red ya que permite tener una red interna. En el software permite tener un *switch* virtual permitiendo tener comunicación en toda la red. En la **Figura *3.42*** se ilustran las máquinas utilizadas y el direccionamiento que se estableció.

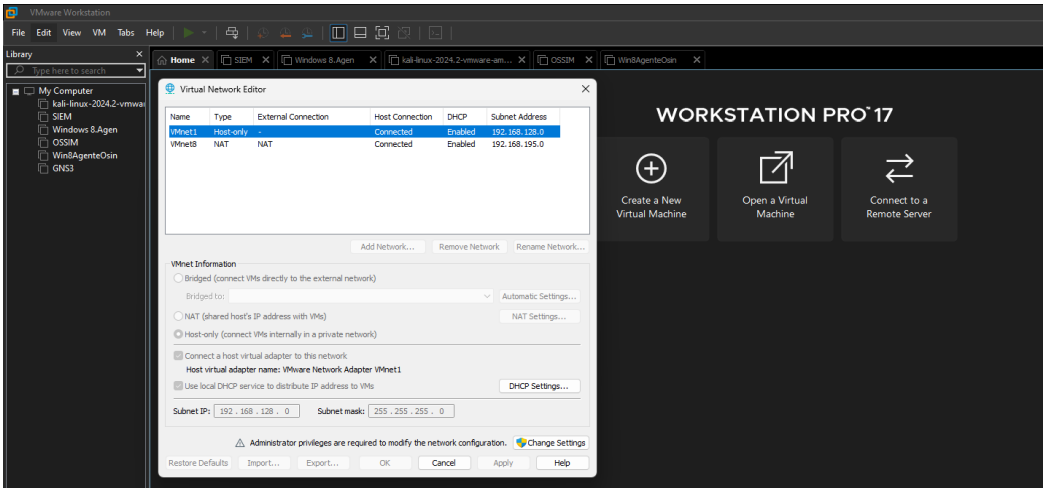

Figura 3.42 Comunicación de la red en VMware

Para la segunda topología se implementó igualmente en *GNS3,* pero en este caso se implementó el servidor *Alien Vault*, el agente, el atacante y una máquina extra para el monitoreo del SIEM, como se ilustra en la **Figura *3.43***.

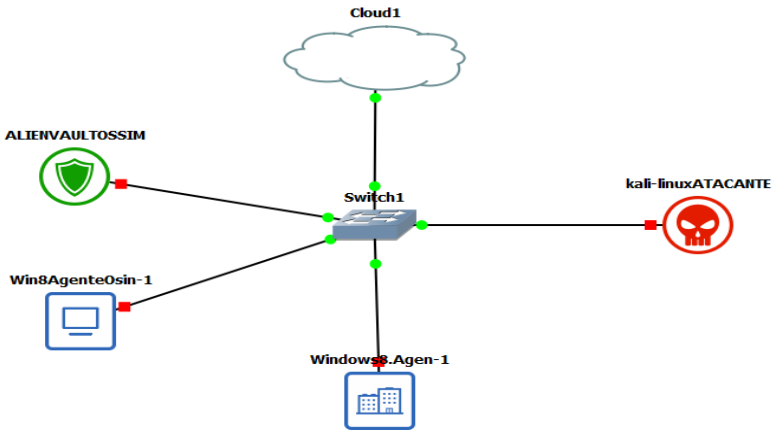

Figura 3.43 Topología del servidor *Alien Vault*

Implementación del ataque

Se escogió el ataque troyano *Backdoor* debido a su complejidad en el contexto de ciberseguridad, ya que permiten al atacante establecer acceso remoto al sistema comprometido esquivando las medidas de seguridad que pueda tener el equipo. El ataque troyano permite tener acceso saltando las defensas y mantener acceso después de que hayan aplicado parches o actualizaciones.

Se escogió este ataque porque permite estudiar las técnicas avanzadas de evasión y de ingreso del atacante observando su persistencia en un entorno ya comprometido, analizando todas las herramientas de detección y respuesta ante la amenaza. También investigar de como el *Backdoor* afectan la seguridad del equipo para identificar las vulnerabilidades para prevenir futuros ataques.

Para la creación del ataque *Backdoor,* se necesita primero el direccionamiento de la máquina atacante, tal como ilustra en la **Figura *3.44***.

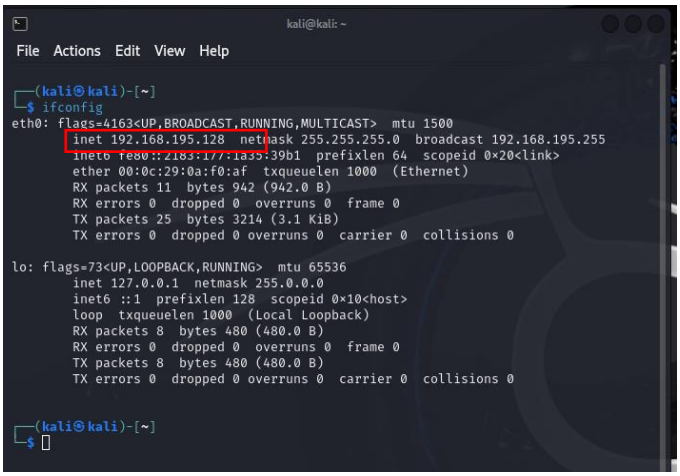

Figura 3.44 Direccionamiento de la máquina atacante

En la **Figura *3.45*** se ingresa a modo usuario, para poder utilizar el comando *msfconsole* para utilizar *metasploit,* que es un proyecto de código abierto para la seguridad informática que proporciona información acerca de las vulnerabilidades de seguridad.

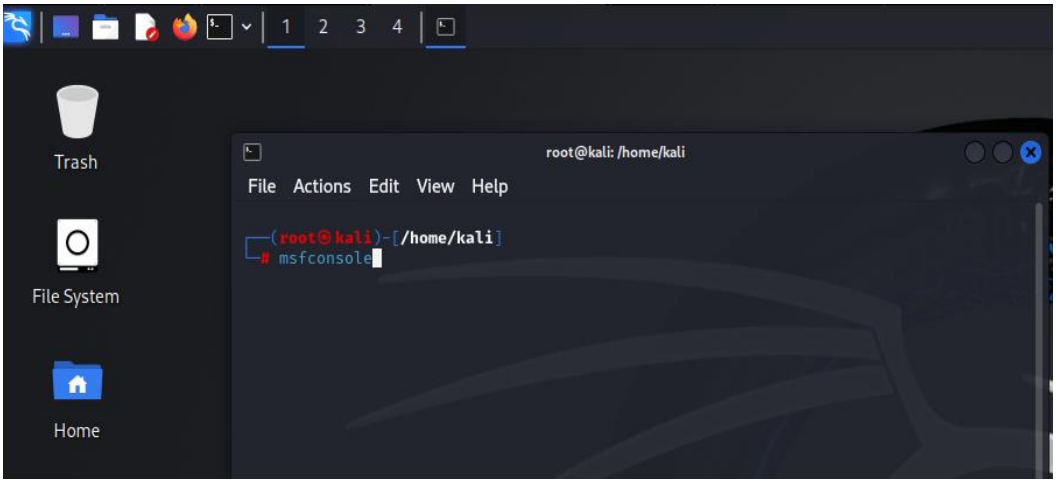

Figura 3.45 Ingreso a *metasploit*

Ya dentro de *metasploit,* se muestra una ventana tal como se ilustra en la **Figura *3.46***.

Figura 3.46 Ventana de inicio de *metasploit*

Para iniciar el ataque se ingresa el comando que se expresa en la **Figura *3.47***. Donde se visualiza el nombre del sistema operativo donde se realizará el *Backdoor*, el direccionamiento IP de la máquina que va a realizar el troyano, el puerto a utilizar para realizar el ataque y la creación del ejecutable que se instalará en la máquina atacada.

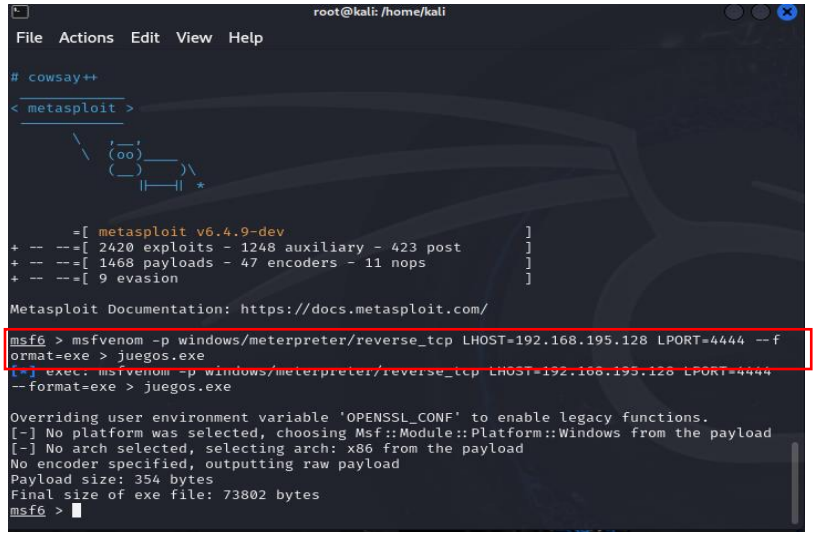

Figura 3.47 Comando inicial del ataque *Backdoor*

En la Figura 3.47 se presenta el nombre que se asignó al ejecutable “juegos.exe”. Ya terminado el proceso se puede ver la cantidad de bits que tiene. Para verificar que, si fue creado, en la **Figura *3.48*** se ilustra que se utiliza el comando LS para ver el contenido de la carpeta.

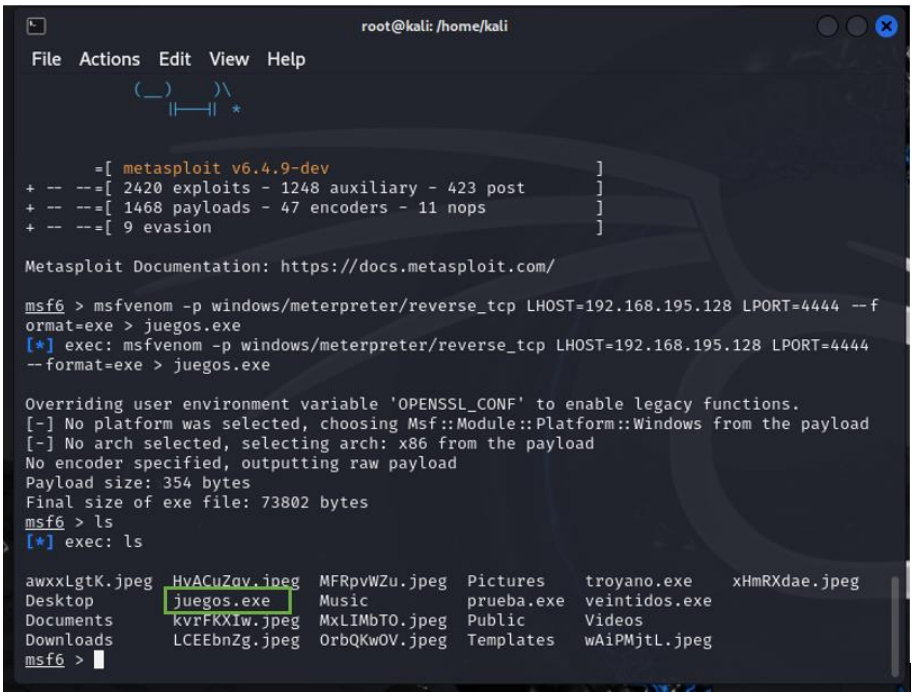

Figura 3.48 Verificación del ejecutable.exe

A continuación, se trasladó la carpeta del ejecutable hacia Apache para que se pueda descargar desde el navegador, utilizando la siguiente línea de comando que se ilustra en la **Figura *3.49***.

Figura 3.49 Agregación del ejecutable.exe en la carpeta Apache

En la **Figura *3.50*** se observa cómo se inicia el servicio de Apache.

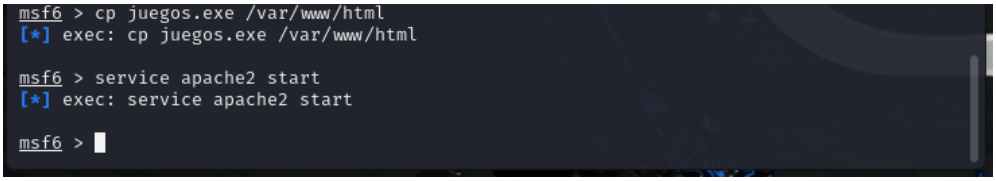

Figura 3.50 Inicio del servicio de Apache

Ya iniciado el Apache, se utiliza la siguiente línea que se muestra en la **Figura *3.51*** para iniciar el programa y poner en modo escucha cuando la víctima inicie el programa.

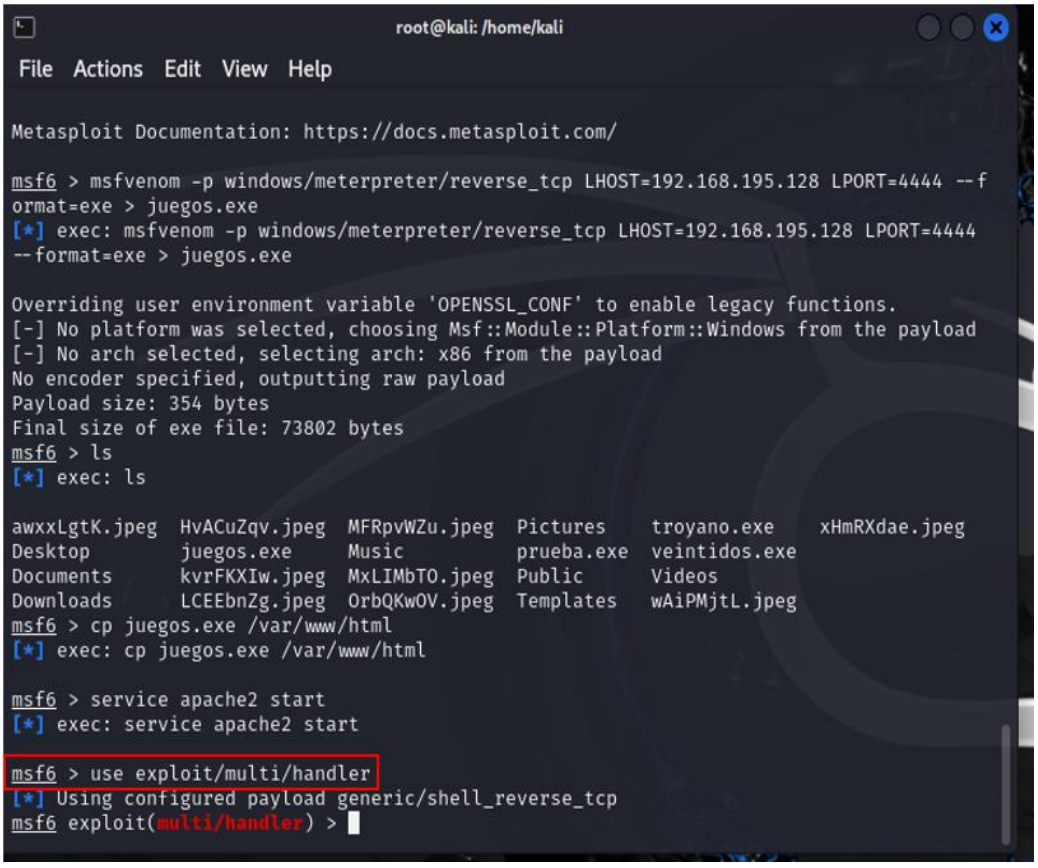

Figura 3.51 Ingresar a modo escucha

Ingresado al modo escucha, se ingresa la dirección IP del atacante, el puerto que se va a utilizar tal como se muestra en la **Figura *3.52***. se escribe el comando *RUN* y empieza a corres y se pone en un modo espera hasta que la víctima inicie el programa que está en la red.

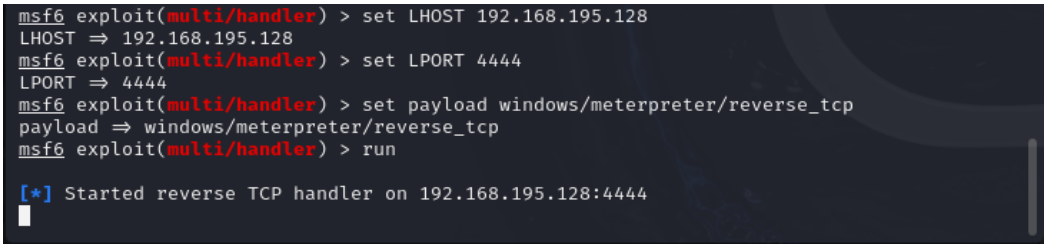

Figura 3.52 Backdoor iniciado

Para que el ataque sea completado, la víctima debe ingresar al navegador y escribir la dirección 192.168.195.128/juegos.exe tal como se muestra en la **Figura *3.53***, este es un ejemplo de cómo se esconde el ataque troyano puede ser en programas descargables, juegos, imágenes, videos, etc. ya que permanece oculto hasta que se logre ejecutar.

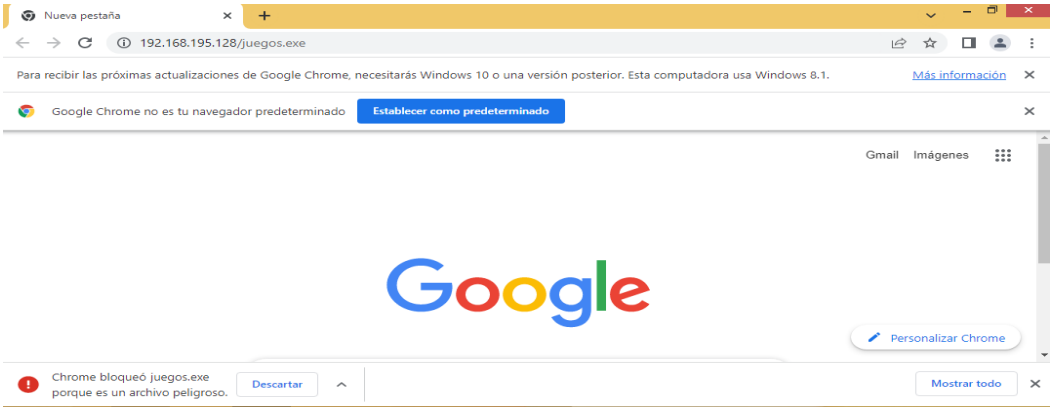

Figura 3.53 Descarga del ejecutable

En la Figura 3.53 se observa que Windows detectó la amenaza antes de que se descargue, para vienes prácticos se procede con la descarga tal como se ilustra en la **Figura *3.54***.

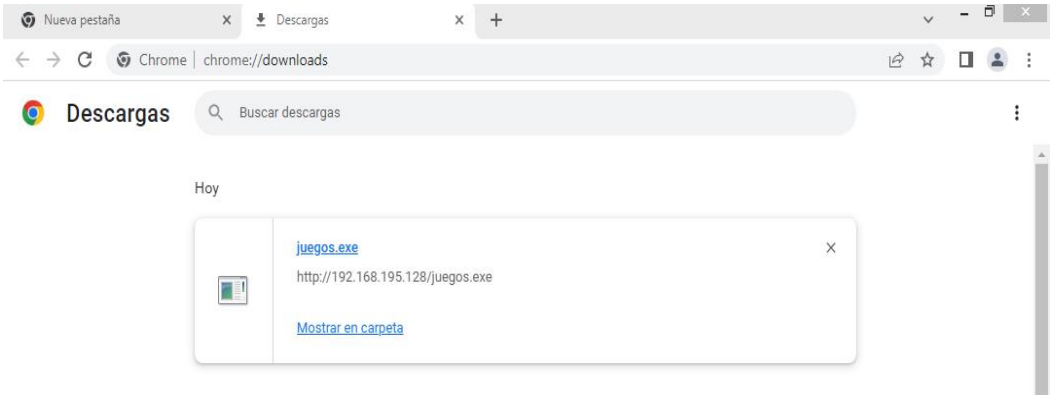

Figura 3.54 Comprobación de la descarga del ejecutable

Ya descargado el ejecutable.exe se procede a iniciarlo tal como se muestra en la **Figura *3.55***.

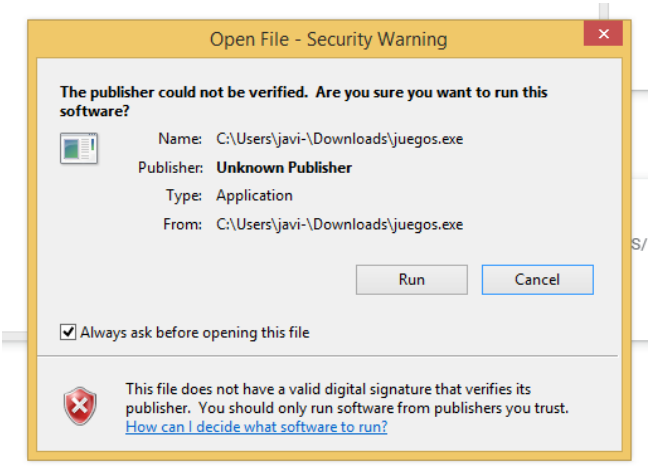

Figura 3.55 inicio del ejecutable juegos.exe

Iniciado el ejecutable se procede a verificar que el atacante tenga entrada sin ser detectado. Se observan datos específicos de la computadora víctima, tal como se ilustra en la **Figura *3.56***.

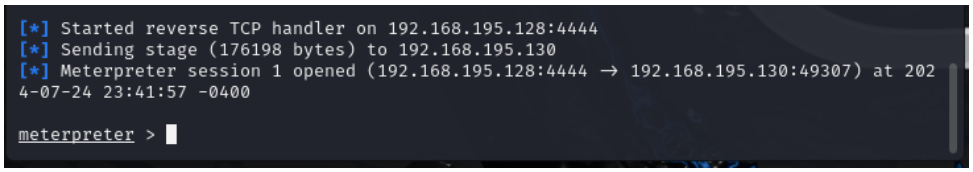

Figura 3.56 Entrada del atacante en la computadora víctima

Para verificar que la dirección IP 192.168.195.130, es de la víctima, se procede a realizar un *IPCONFIG* en el terminal de la víctima, agente Windows, tal como se ilustra en la **Figura *3.57***.

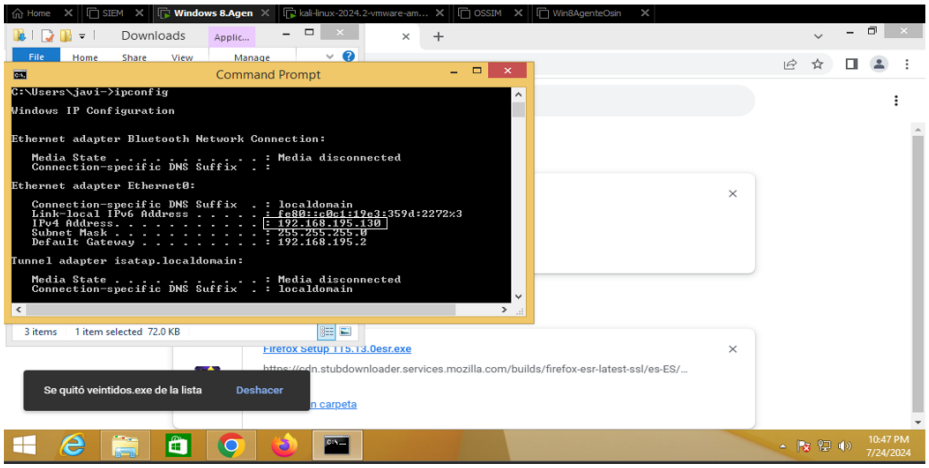

Figura 3.57 Verificación de dirección IP de la víctima

Para ver qué herramientas tiene el atacante, es escribe el comando *HELP* para ver todo lo que se puede realizar, así como se ilustra en la **Figura *3.58***.

Figura 3.58 Herramientas para el *Backdoor*

En la demostración, se procederá a realizar el robo de información de una cuenta de correo empezando por el usuario y luego por la contraseña. Para ello se procederá a usar el comando para copiar los datos, que se muestra en la **Figura *3.59***.

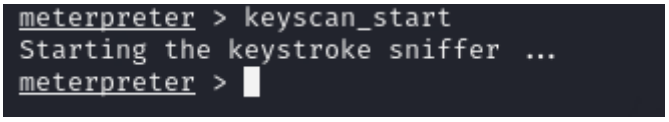

Figura 3.59 Línea de escaneo con el comando *keyscan_start*

Se ingresa un usuario y una contraseña en la víctima tal como se ilustra en la **Figura *3.60***.

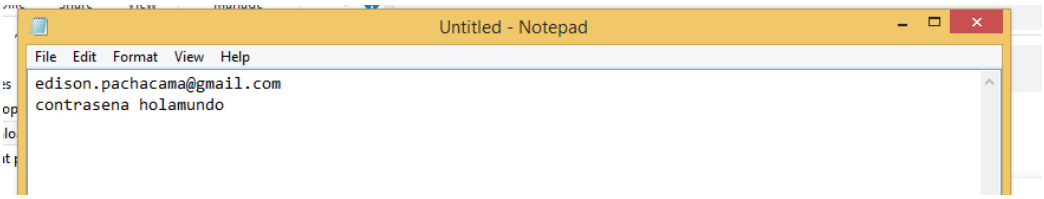

Figura 3.60 Información de correo electrónico

Ya escrito la información se procede a escribir un comando que permita visualizar todo lo que ha escrito la víctima tal como se ilustra en la **Figura *3.61***.

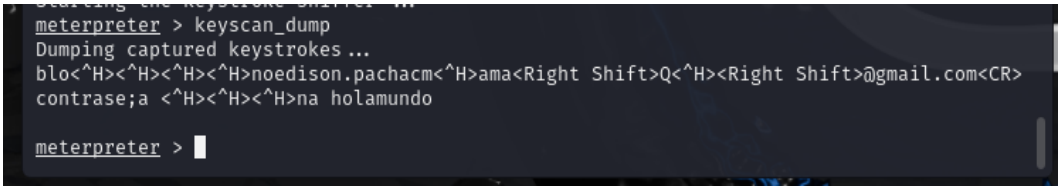

Figura 3.61 Copia de información con el comando *keyscan_dump*

Como se muestra en la Figura 3.61 es un robo de información de un correo electrónico donde con pequeños comandos pueden obtener mucha información o hacer daño al equipo.

3.4 Verificación del funcionamiento de los SIEM

Análisis de resultados con *Wazuh*

Para el análisis de las respuestas, que muestran las dos herramientas SIEM, se procederá a analizar cada una empezando por *Wazuh*. Para ello se analiza el estado inicial del agente antes de hacer atacado por *Backdoor*.

Al ingresar a la plataforma de *Wazuh* en la **Figura *3.62***, se observa que está activo el agente y está en un estado inicial normal sin ninguna alteración.

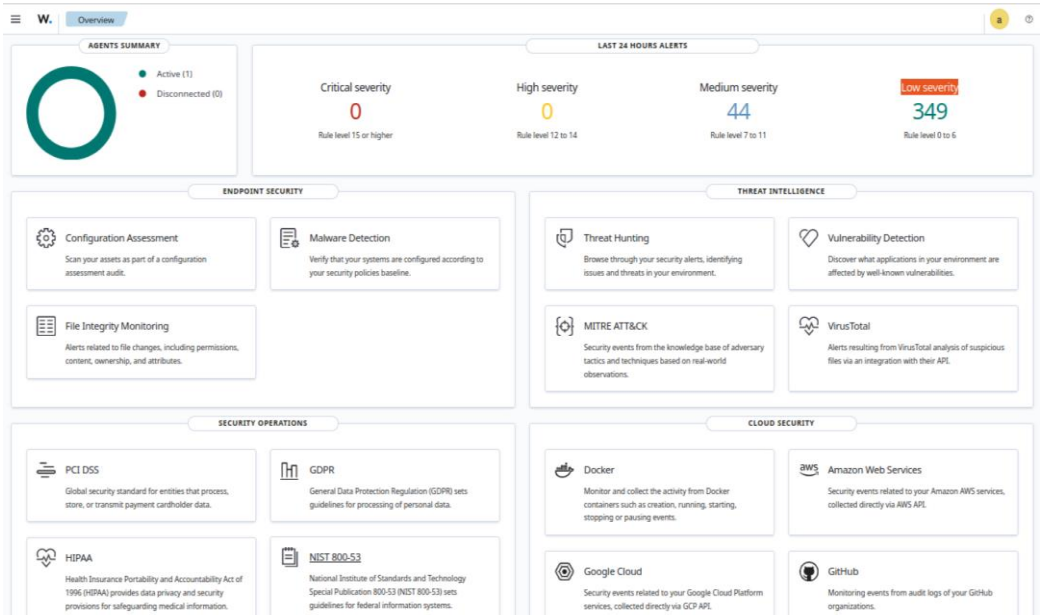

Figura 3.62 Inicio de *Wazuh*

Los estados *meduim severeti*, *low severety* son logs que tiene el servidor *Wazuh* con el agente, donde se ve el inicio y el apagado del agente como el mismo SIEM. En la **Figura *3.63*** se presenta cada *LOG* que representa el inicio del equipo.

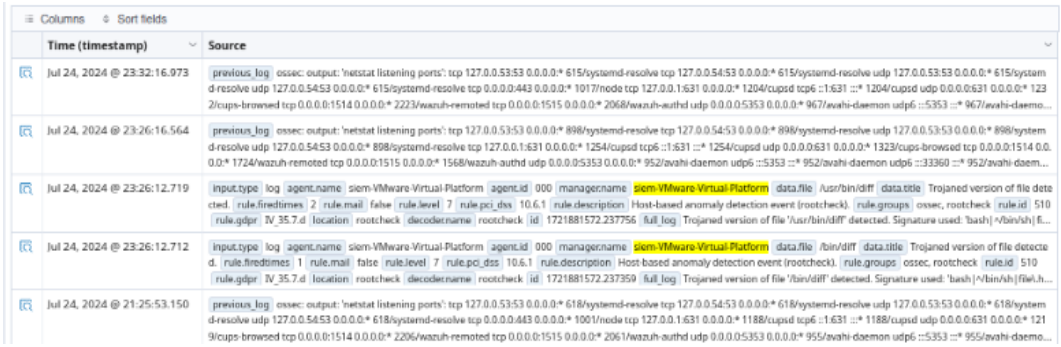

Figura 3.63 Logs de inicio y apagado de sesión

Se ingresa al agente para observar que su nivel inicial no tenga ninguna alteración, tal como se presenta en la **Figura *3.64***. En la ventana se muestras la opción MITRE ATT&CK, es una herramienta integrada para mejorar la capacidad de las organizaciones para la protección de amenazas y responder de manera objetiva a los ataques. En la opción *Compliance* es el módulo de cumplimiento que facilita a las organizaciones mantener la conformidad con las normativas de seguridad y proteger sus activos de cualquier amenaza y vulnerabilidades. El *Events count evolutions* permite monitorear y analizar que los administradores de seguridad estén atentos a las actividades en su entorno, identificando los picos o caídas inusualmente en los números de eventos, identificando los problemas de seguridad, configuración y cambios de entorno.

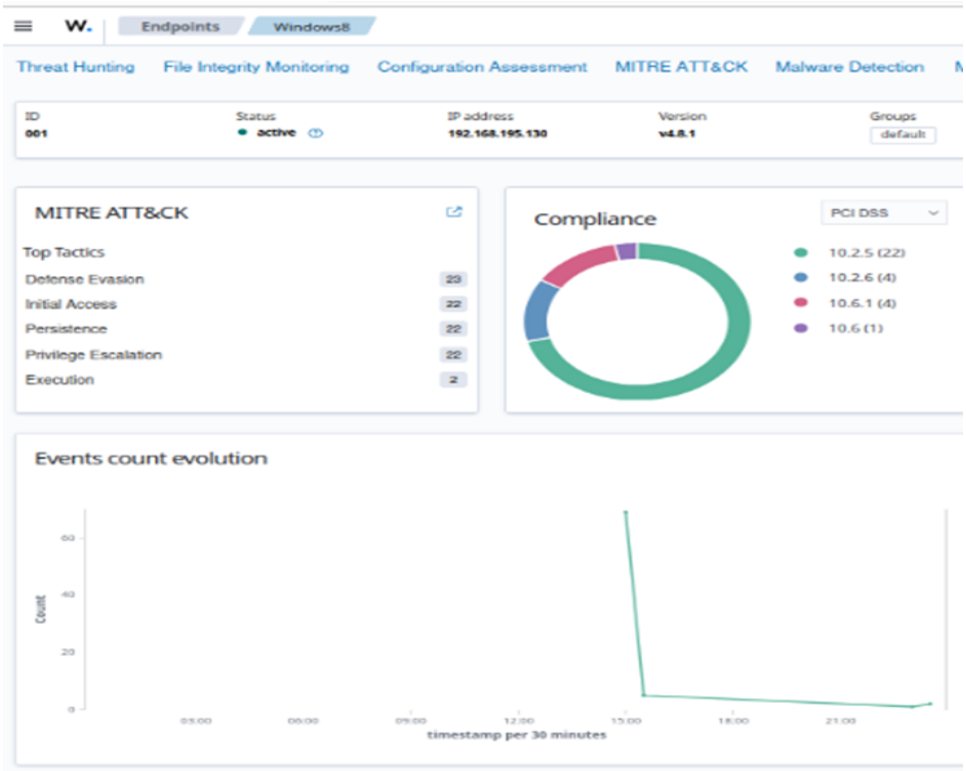

Figura 3.64 Estado inicial del Agente

En la Figura 3.64 , ilustra la opción *Compliance* la cual tiene un anillo de colores los cuales permiten identificar ciertos cumplimientos en el sistema.

Verde: Cumple con las normativas y políticas de seguridad con los controles de monitoreo.

Rojo: Significa que el sistema no cumple con alguna normativa o política.

Azul: Representa al estado informático o neutral con eventos que no se ven afectados al cumplimiento del monitoreo, pero al igual son relevantes.

Morado: Representa el estado de evolución olas revisiones pendientes.

Para ver que el agente aún no ha sido afectado por algún ataque se observa en la **Figura *3.65*** que se tiene las opciones *Recent Events* la cual es una lista de cambios más recientes que tiene el directorio de monitoreo, ayudando a mantener la seguridad e integridad del sistema al detectar actividades maliciosas

Figura 3.65 Estado de Inicio de *Recent* Events

En la parte superior donde se encuentra el agente se puede observar varias opciones, como se ilustra en la Figura *3.66*, permiten el monitoreo de toda la red o en este caso del agente que se está analizando.

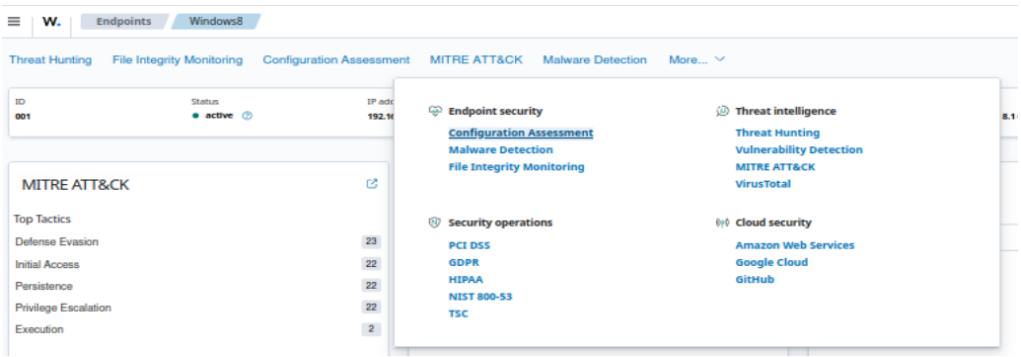

Figura 3.66 Opciones de monitoreo

Para el Análisis del ataque *Backdoor* se usarán tres opciones del SIEM que son *MALWARE DETECCION*, *THREAT HUNTING* y *MITRE ATT&CK.*

Al momento de iniciar el ataque el estado inicial que tenía el agente empieza a modificarse, a tener eventos y tener variaciones, tal como se muestra en la Figura *3.67*.

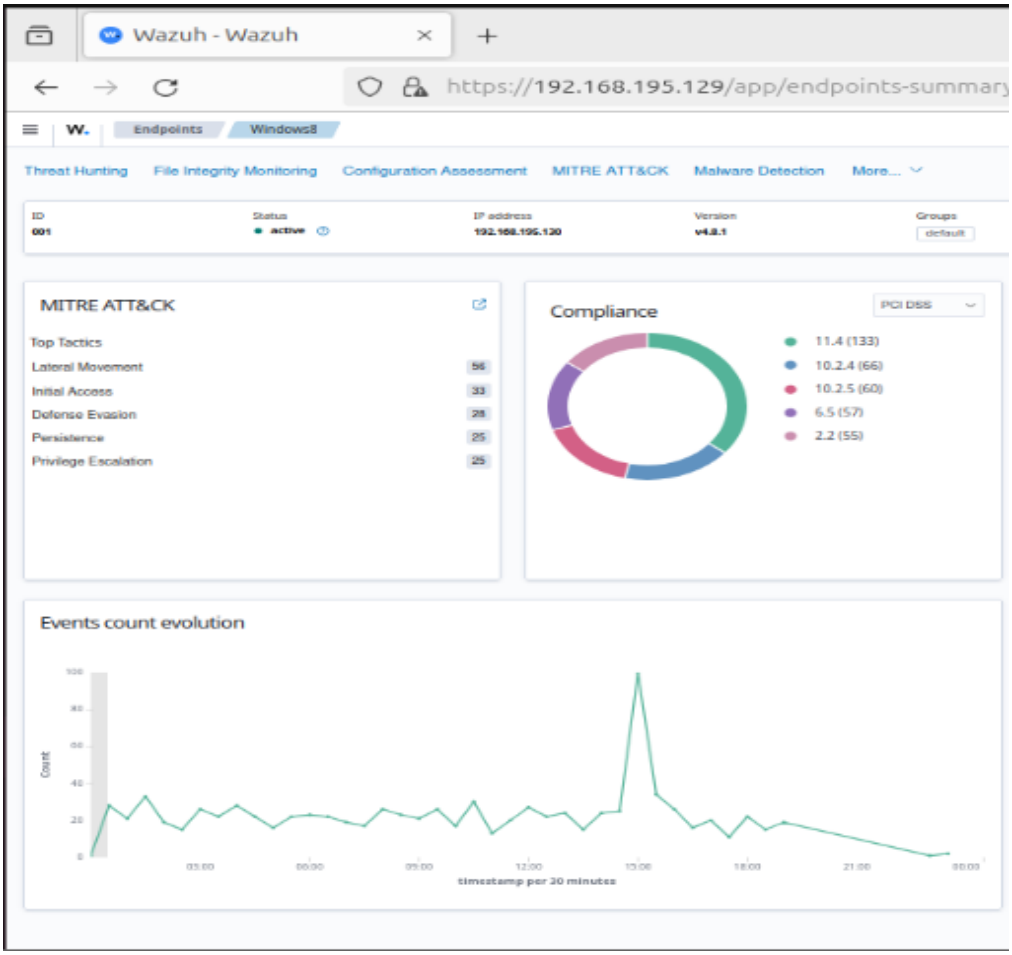

Figura 3.67 Detección de ataque

En la Figura *3.67* empieza a mostrar cómo va cambiando la parte de *Events count evolution,* van subiendo y bajando los picos dando una alerta que se tiene alguna alteración en ese lapso, requiriendo un análisis más detallado.

Para la verificar que se tuvo un evento en el agente, la plataforma da el monitoreo de los cambios de archivos y directorios del sistema para la detección de modificaciones no autorizadas, tal como se visualiza en la **Figura *3.68***.

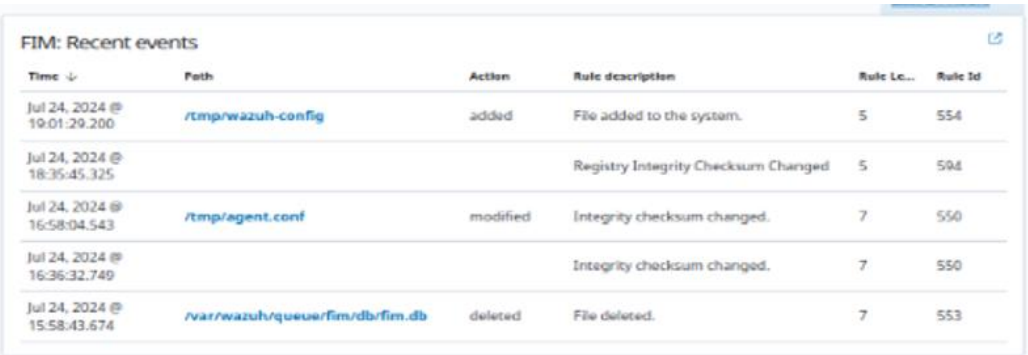

Figura 3.68 Análisis en *Recent events*

Se procede a ingresar a las 3 opciones antes mencionadas para verificar como están actuando. Iniciando por el *THREAT HUNTING*, casa de amenazas, buscando y detectando amenazas a la red antes de que causen daño. El *THREAT HUNTING* busca identificar y neutralizar amenazas activas o potenciales que no han sido detectadas por las defensas de seguridad. Tal como se muestra en la **Figura *3.69***.

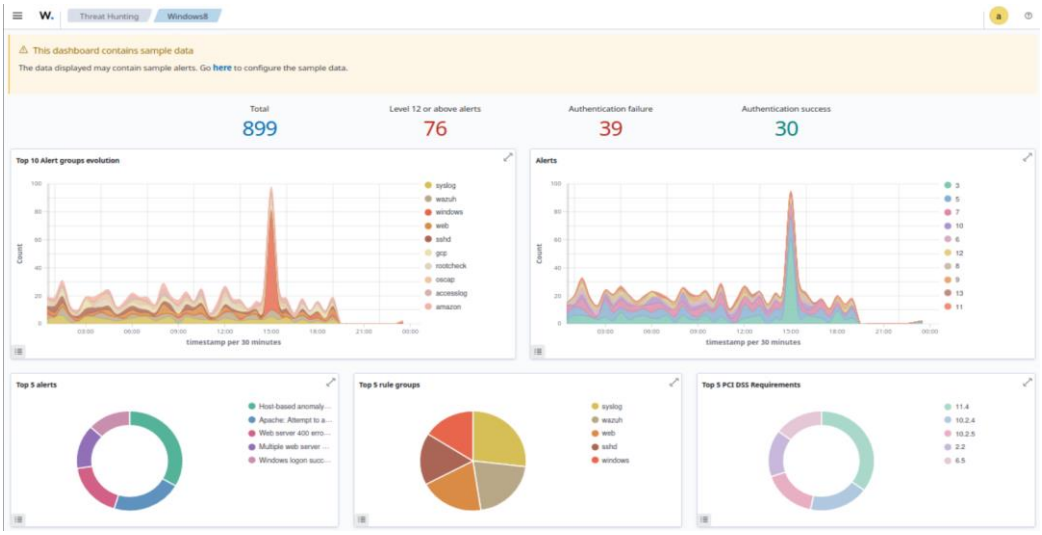

Figura 3.69 Detección de *THREAT HUNTING*

En la **Figura *3.70***, se observa la parte de monitoreo donde dan varias opciones que cada una tiene su propósito y son las siguientes:

Total: Número de eventos registrados en el sistema durante el análisis de monitoreo, dando el volumen de actividades que se han detectado.

Leven 12 or Above Alerts: Indica la cantidad de alertas en diferentes niveles de severidad. *Wazuh* permite clasificar niveles de alertas indicando si son críticas y requieren atención inmediata.

Authentication failure: Representa la cantidad de fallos de autenticación. Estas autenticaciones indican el acceso no autorizado o problemas con el registro de credenciales.

Authentication success: Indica la cantidad de autenticaciones exitosas. Esto permite validar el acceso de usuario legítimo y ver si todas las acciones están corriendo sin ningún problema.

Figura 3.70 Métricas del sistema de monitoreo de *Wazuh*

Para la identificación del ataque, se observa que en la **Figura *3.71***, se tiene una gráfica la cual permite monitorear la gestión de seguridad en un entorno, teniendo una rápida respuesta ante cualquier ataque. Para identificar mejor el monitoreo se tienen ciertas alertas las cuales son:

Syslog: es un protocolo estándar para el envío de mensajes de registro, proporcionando alertas de problemas de red, servicio de sistema y mensajes de kernel.

Wazhu: es el monitoreo de la propia plataforma, brindando alertas de integridad, detección de rootkits, configuración de seguridad, eventos de auditoría.

Windows: Alertas del sistema operativo, actividades sospechosas.

Web: alertas con las aplicaciones web, servicios o accesos no autorizados.

SSHD: Alertas del servicio SSH (*Secure Shell*).

GCP: Alertas con *Google Cloud Platform.*

Rootcheck: Para la detección de *rootkits*, actividades sospechosas para la ocultar *malware*.

Oscap: Cumplimiento e implementación de los estándares de seguridad.

Accesslog: Es la actividad de registro sospechoso o registro de accesos.

Amazon: Alertas de amazon.

Para identificar el *MALWARE* o el troyano *Backdoor* que dirige a la opción de *RootCheck* que es un módulo de *Wazuh* que permite detectar *rootkits* ya que son programas diseñados para ocultar la presencia del *malware*. El *RootCheck* ayuda a identificar las amenazas ocultas y asegurar la integridad. En la **Figura *3.71*** se presenta la herramienta para la detección de *MALWARE*.

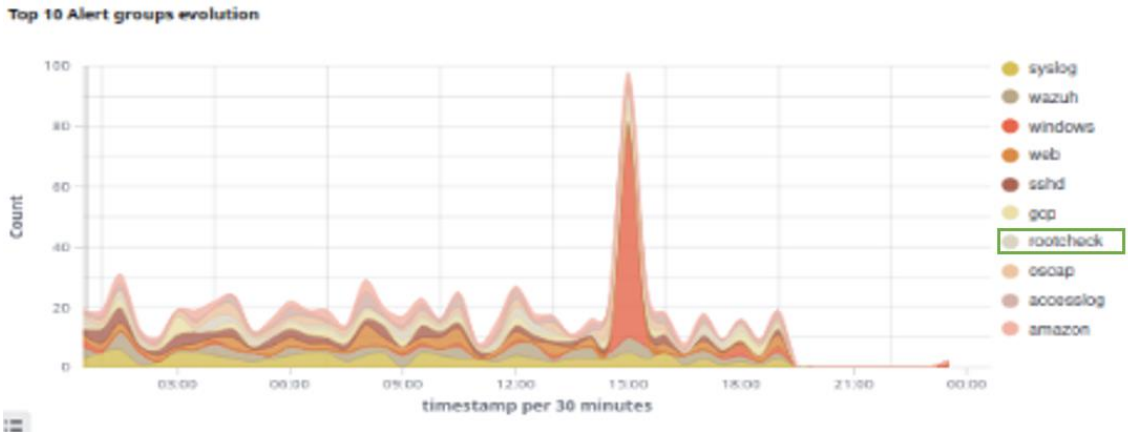

Figura 3.71 Herramienta *rootcheck*

En **Figura *3.72*** se muestra el número de alertas más casuales que brinda el servidor *Wazuh* al detectar el ataque Backdoor dando como alertas de comportamientos sospechosos, intentos de ingreso, solicitudes incorrectas, anomalías del servidor web, inicio de sesión de agente.

Figura 3.72 Alertas de seguridad

Se ingresa a la opción *MITRE ATT&CK* es una base de datos de conocimientos de tácticas, técnicas que pueden realizar los atacantes. En la **Figura *3.73*** se observa las variaciones y detecciones que puede tener contra el ataque. *Wazuh* relaciona el ataque troyano *Backdoor* con el de fuerza bruta ya que el comportamiento o actividades se caracterizan similarmente por el método de operación o ciertos indicadores, permitiendo ser detectados en el sistema de monitoreo.

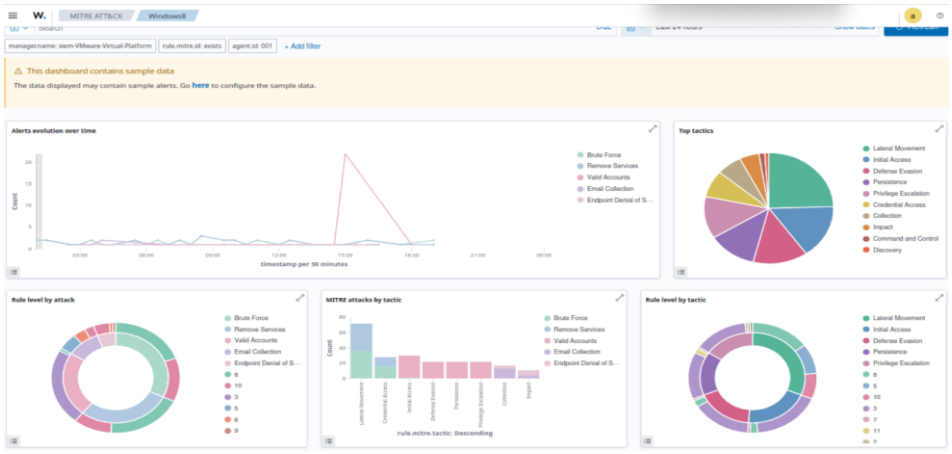

Figura 3.73 Detección *MITRE ATT&CK*

En la **Figura *3.74*** se ilustra las alertas de tiempo de las amenazas o actividades realizadas como *Brute Force, Romote Service, Valid Accounts, Email Colletion y Endponit Denia lof service*. Estas alertas permiten monitorear y analizar actividades sospechosas respondiendo de manera adecuada.

Figura 3.74 Alertas de tiempo

En la siguiente **Figura *3.75***, se observan unas barras que presentan el número de sucesos detectados, la altura de la barra indica la cantidad de alertas relacionados. Estas tácticas describen los objetivos que tienen los atacantes durante su ejecución, permitiendo detectar áreas específicas de riesgo implantando mejor las medidas de seguridad.

Figura 3.75 Clasificados según las tácticas

Para la seguridad el *MITRE ATT&CK* proporciona un listado de tácticas que permiten tener respuesta a las amenazas mejorando la seguridad, teniendo estrategias defensivas, tal como se muestra en la **Figura *3.76***.

Figura 3.76 Tácticas de seguridad

Por último y el que se necesita para la detención del ataque troyano es la opción de *MALWARE DETECCION,* ya que permite detectar todo tipo de ataque de MALWARE con ciertas aplicaciones de *Rootkit,* tal como se ilustra en la **Figura *3.77***.

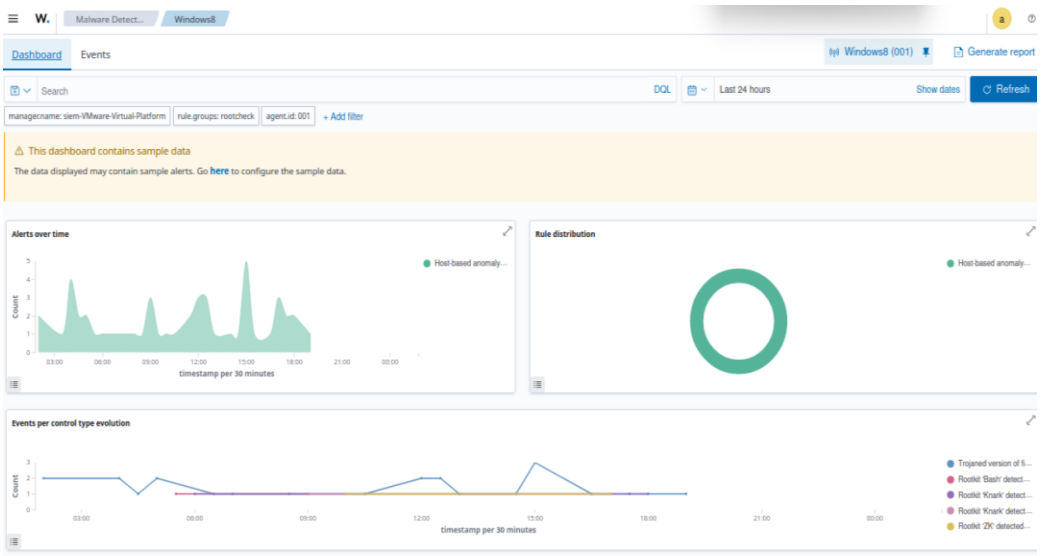

Figura 3.77 Detección *MALWARE DETECCION*

En la parte de eventos se muestran todas las acciones que ha podido reconocer el servidor de *Wazuh*, así como se ilustra en la **Figura *3.78***.

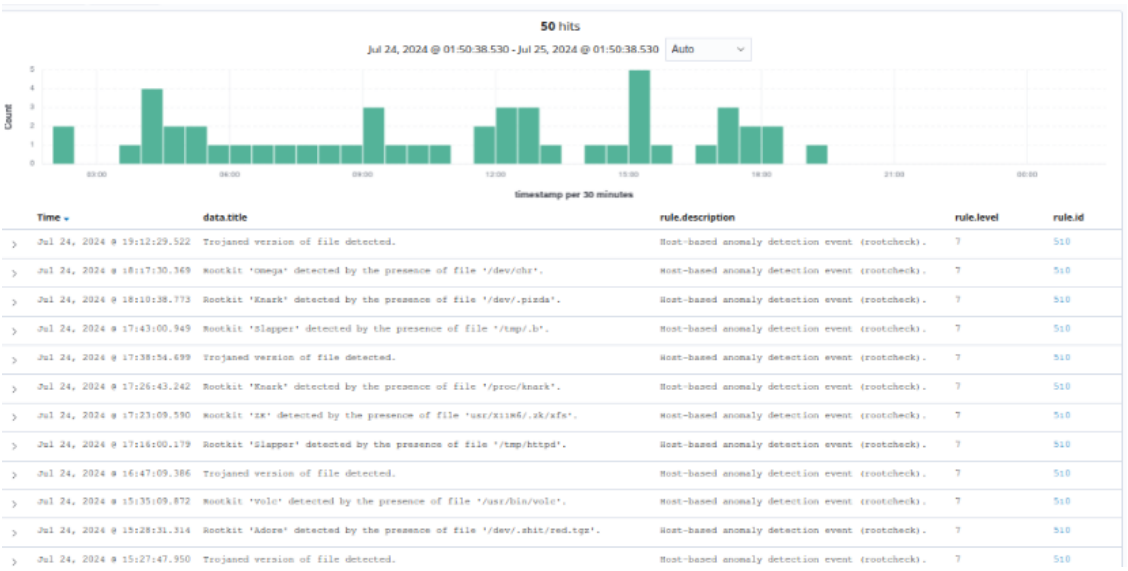

Figura 3.78 Eventos de *MALWARE DETECCION*

En la **Figura *3.79*** se observan varios eventos los cuales algunos son reconocidos como el ataque troyano y Rootkis los cuales permiten esconder la presencia del *malware*.

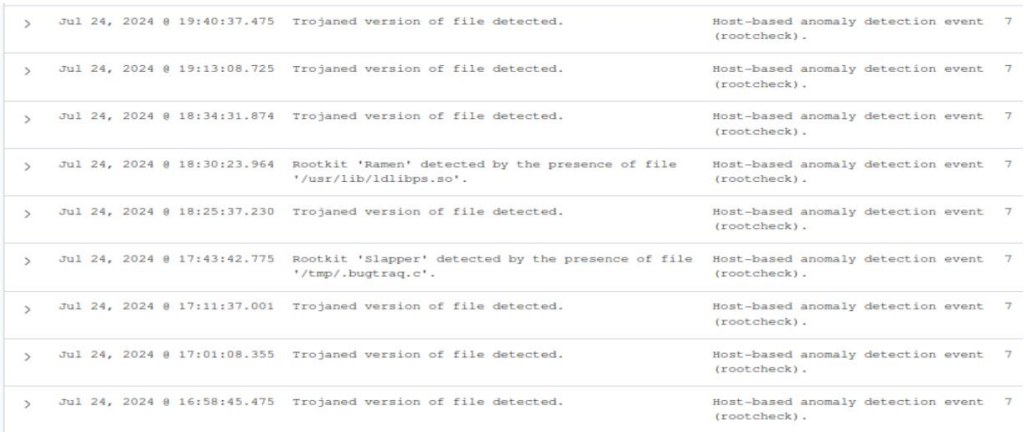

Figura 3.79 Detección del ataque Troyano

Finalmente, el análisis que se aplicó con el servidor *Wazuh* permite detectar y neutralizar cualquier ataque antes de que haya alguna inconveniente en la red. Ya que la plataforma permite tener reglas como tácticas para tener la infraestructura a salvo de cualquier atacante ya que se conoce todas las técnicas que pueden usar para hacer vulnerable al equipo o a la red de la empresa u organizaciones.

Análisis de resultados con *ALIEN VAULT*

Para el análisis en el servidor de *Alien Vault.* Primeramente, se verifica el estado inicial del agente antes de que se produzca el ataque, ver la Figura *3.80*.

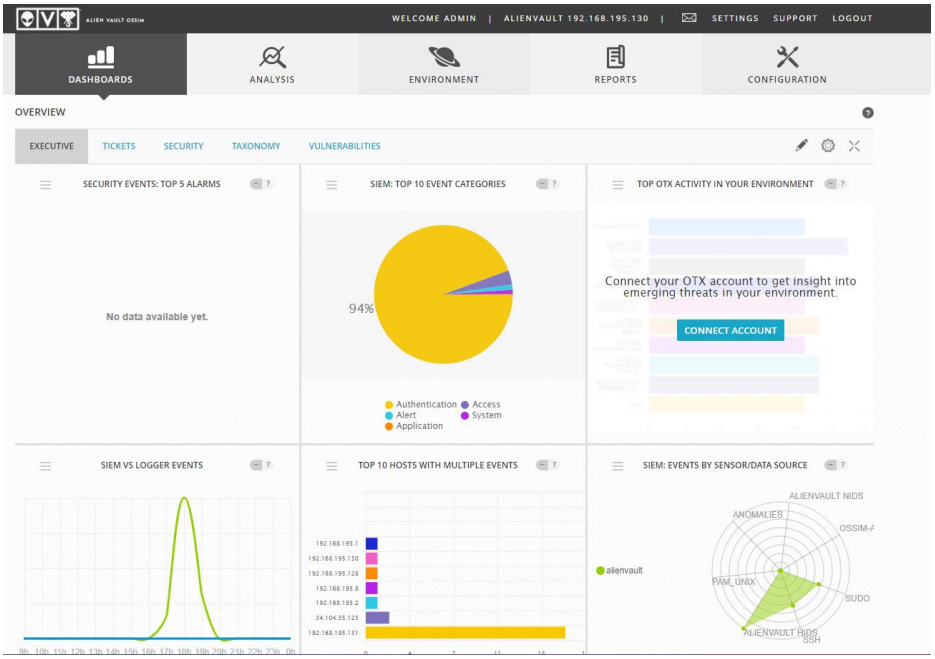

Figura 3.80 Análisis inicial del agente en el servidor *Alien Vault*

En la Figura *3.81* se presentan las funciones bloqueadas, esto sucede ya que al ser un servidor de paga no todas las opciones están habilitadas, pero si se permite tener análisis del ataque.

Para detección del *MALWARE* o ataque troyano se ingresa en la ventana principal del servidor, se ingresa a la parte de alertas tal como se ilustra en la Figura 3.81.

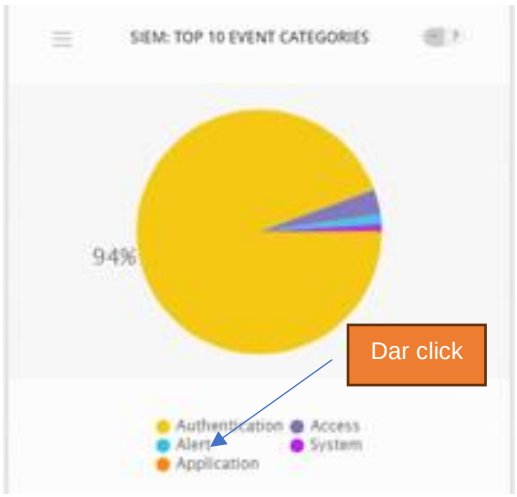

Figura 3.81 Acceso a las alertas

Ya ingresado a las alertas, se encuentra un listado de logs tal como se ilustra en la Figura *3.82*, donde se visualiza los eventos de detección.

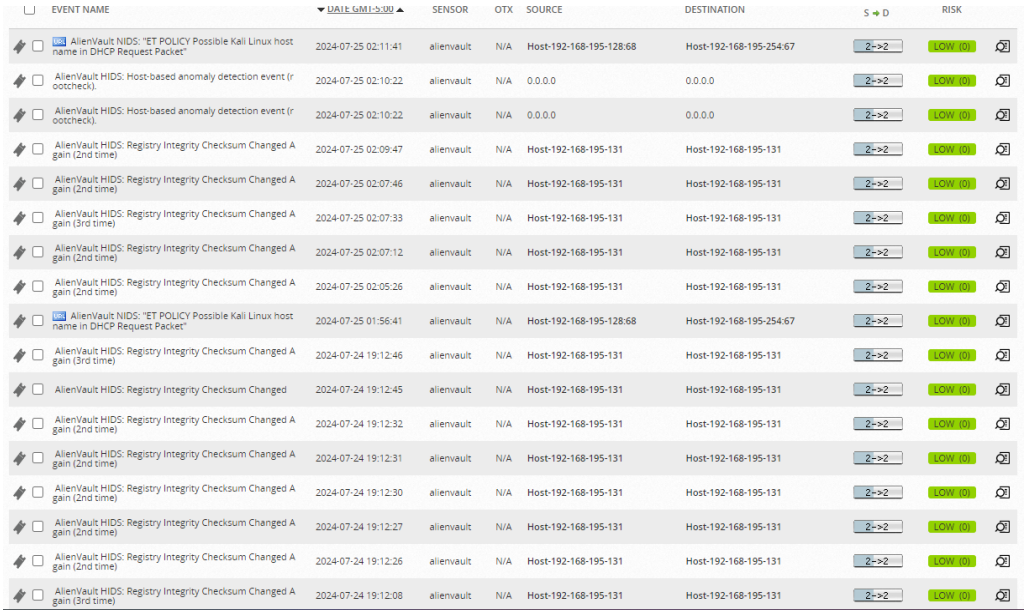

Figura 3.82 Listado de eventos

Para ver qué tiene cada evento se da *click* y al ingresar, esto proporciona la información necesaria para poder entender que está sucediendo al agente. En este servidor brinda los datos del atacante como su dirección IP, el sistema operativo que está utilizando, lo detecta como intruso. Estos análisis se observan en la Figura *3.83*.

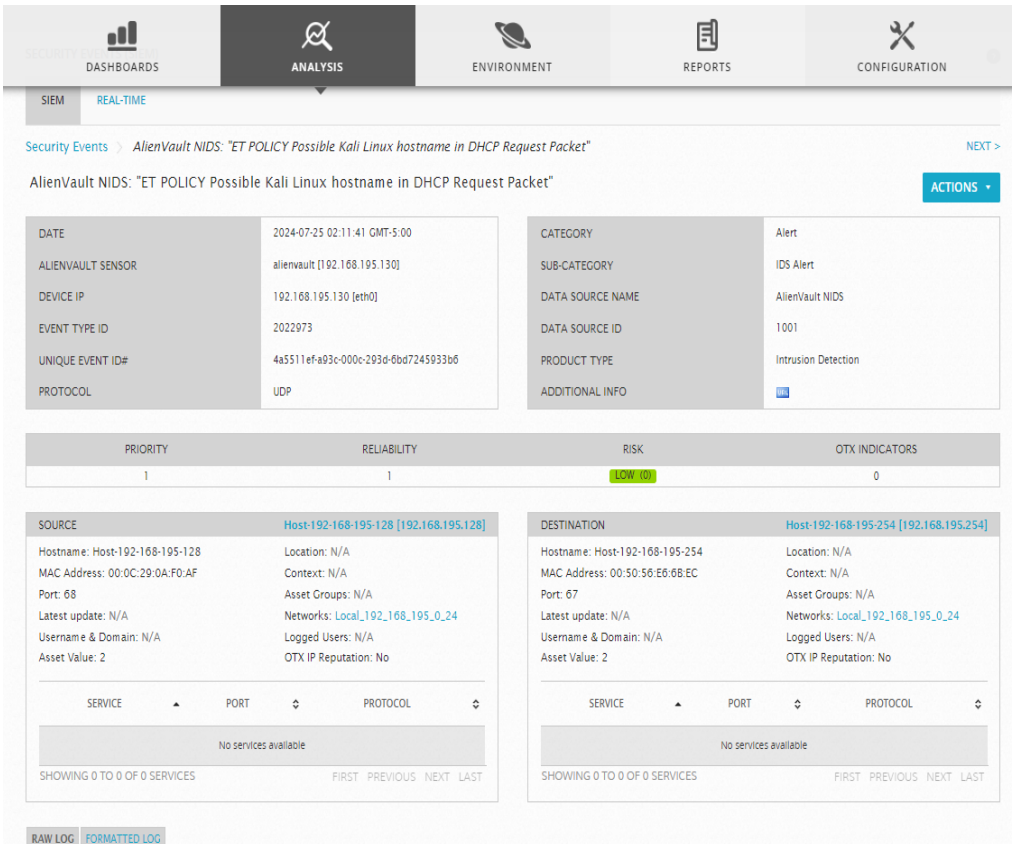

Figura 3.83 Descripción del ataque *Backdoor*

Análisis técnico comparativo entre los dos SIEM

A continuación, en la Tabla 3.6 se encuentra una comparación entre sus requerimientos mínimos tanto de hardware como de software además de sus principales características.

Tabla 3.6 Análisis comparativo de *Wazuh* y *ALIEN VAULT*

Características		
SIEM	***ALIEN VAULT***	***WAZUH***
RAM	8-16 (GB)	4-8 (GB)
Sistema operativo	Solo Linux	En varios sistemas operativos
Almacenamiento	500 (GB a 1TB)	50 (GB)
CPU	4 núcleos	2 núcleos
Mantenimiento	Mantenimiento proactivo con parches y actualizaciones	Parches y Actualizaciones manualmente
Seguridad	Maneja la seguridad a nivel de aplicación e infraestructura	Seguridad a nivel de configuración del servidor y datos.
Interfaz	Tiene su propia interfaz	Utiliza Kibana para su interfaz gráfica
Gestión de vulnerabilidades	Realiza escaneos para identificar la parte de la infraestructura.	Identifica vulnerabilidades en el sistema y aplicaciones.
Número de agentes	1-10 gratuita, o depende de la licencia que compren	1-25
Soporte en la Nube	Soporte a través de su producto *AlienVault* USM *Anywhere*	Compatible con las nubes AWS, Azure, Google Cloud y Privada
Tipo de código	Comercial	Abierto
Monitoreo	Monitoreo en tiempo real a través de sus interfaces centralizadas, visualizando los eventos de seguridad a medida que van sucediendo	Monitoreo en tiempo real, pero se visualiza a través de las herramientas complementarias como *KIBANA*

SIEM	***ALIEN VAULT***	***WAZUH***
FEED de Amenazas	Se encuentra instalado	No se encuentra instalado, pero se ingresa fuentes de amenazas
Escalabilidad	Puede tener limitación basado en la licencia que se adquiera	Puede ser adaptado para grandes entornos con varias fuentes de datos.
Personalización	Solución preconfigurada con menos necesidad de ajustes	Altamente personalizable debido a la naturaleza de código abierto
Inteligencia de Amenazas	Inteligencia de amenazas integradas	Integrarse con varios tipos de fuentes.
Detección de amenazas	Múltiples motores de detección	Reglas de detección
Soportes	Soporte comercial Ofrece un soporte técnico para las compañías que necesitan una respuesta rápida y dedicada	Soporte comunitario y opciones comerciales adicionales. Ofrece un soporte basado en la comunidad del usuario y desarrolladores.
Utilización	Pagada finalizado 6 días de prueba	Gratuitita
Respuesta	Al momento de realizar el ataque *Alien Vault* tiene una mejor respuesta con respecto de donde fue realizado, cual fue el ataque, el sistema operativo que ataco y por ultimo se tiene la dirección IP del atacante	Al momento de realizar el ataque se presentan varias graficas las cuales si no se tiene el conocimiento de algunos acrónimos no se podrá entender que esta pasando en el equipo

Manual técnico con las mejores prácticas ante un ataque de malware

- Asegurar que todos los dispositivos tengan actualizados los sistemas operativos, aplicaciones y software de seguridad con las últimas actualizaciones de seguridad.
- Integras soluciones de seguridad como firewalls, sistemas de detección de intrusos y antivirus para la protección de los dispositivos.
- Enseñar a los empleados sobre las mejores prácticas de seguridad, visualizando correos sospechosos o alguna aplicación de *phishing*, ya que por medio de este pueden infiltrarse algunos gusanos o troyanos.
- Tener herramientas de monitoreo para la detección de actividades sospechosas en toda la red y en los sistemas.
- Configurar todo el sistema para recibir alertas al momento de detectar alguna actividad sospechosa.
- Crear reglar para analizar el comportamiento del usuario y del sistema para la detección de *malware*.
- Al detectar un sistema infectado, desconectar de la red para evitar propagación del *malware* en todos los dispositivos.
- Utilizando herramientas de análisis, detectar el tipo de alcance que tiene el *malware*.
- Para la eliminación del *malware* es recomendable usar un antivirus o en casos extremos formatear y reinstalar el sistema.
- Identificar y corregir las vulnerabilidades débiles que permitieron el ataque.
- Actualizar las políticas de seguridad para prevenir ataques futuros, considerando implementar medidas de multifactor.
- Evitar ingresar o navegar a paginas no muy seguras ya que con un solo *click* permites el acceso a los intrusos.
- No descargar información de páginas no recomendadas, ya que los malware permanecen ocultos y son difíciles de detectarlos.
- Manejar páginas seguras identificando que las direcciones sean legitimas.
- Evitar dar información personal a personas desconocidas ya que pueden hacer un *phishing*.
- Siempre mantener los dispositivos bloqueados al momento de no utilizarlos ya que otras personas pueden robar la información.

- Tener contraseñas fuertes mayor de 12 características, usando letras en mayúsculas, números y algún carácter especial.

4 CONCLUSIONES

- Los sistemas SIEM: *Alien Vault* y *Wazuh*, demostraron ser dos herramientas claves de seguridad y que pueden ser utilizadas con facilidad en operaciones de análisis de intrusos y detección de vulnerabilidades.
- *AlienVault* es una plataforma de seguridad integral que integra varias funciones de seguridad, lo cual permite tener mejor acceso a la parte de análisis, pero con un costo adicional, caso contrario su análisis es un reducido.
- *Wazuh* es un proyecto de código abierto lo cual permite tener un mayor acceso al análisis de seguridad, pero con un detalle más técnico que solo las personas especializadas pueden entender, que para una persona normal sería muy difícil entenderlo sin que lo investiguen.
- Se concluye que las herramientas que ofrece *Wazuh* depende mucho de las versiones que se estén utilizando, ya que si se está usando versiones antiguas puede que se tenga que crear esa regla para poder identificar el ataque.
- Al analizar en análisis del ataque en la plataforma Alien Vault se visualiza que brinda el sistema operativo atacante, la dirección IP que está utilizando y la detección de intruso, mientras que *Wazuh* tiene varias técnicas y tácticas las cuales ayudan a saber el origen del ataque.
- Para la agregación del agente en la herramienta *Alien Vault* es muy compleja ya que primero se debe crear un *host* con la misma dirección del agente que se está utilizando, si se utiliza un sistema operativo Windows hay que descargar una aplicación extra para vincularlo o si es otro sistema operativo hay que ingresar varios comandos para su vinculación con el servidor. Mientras que la herramienta *Wazuh* la agregación del agente es mucho más sencillo, ya que toda la configuración se lo realiza en toda su interfaz y con dos comandos se los puede instalar, solo hay que verificar qué sistema operativo se está utilizando.
- Se concluye que para realizar el ataque troyano se debe verificar que la víctima haya descargo algún ejecutable donde se encuentre ocultado el virus para poder tener acceso.
- Se concluyó que para la realización del ataque *Backdoor* se necesita tener un ejecutable el cual brinde acceso a otro dispositivo, sin importar que sea un

programa, video, imagen, juegos, etc. El ejecutable permanece oculto hasta que abran o inicial cualquier archivo infectado.

- Se concluye que, si la herramienta de *Alien Vault* no fuera muy costosa, se pudiera acceder a todo su catálogo de detección de amenazas y vulnerabilidades, teniendo un análisis más completo para prevenir los ataques.
- Se concluyó que no es necesario virtualizar las máquinas en el GNS3 ya que los programas de virtualización cuentan con switch virtuales, los cuales permiten tener una red interna para el presente trabajo curricular.
- Se concluye que hay varias herramientas del SIEM como el *Elastic Search* que al igual permiten tener análisis de intruso y vulnerabilidades. Lo complejo de este SIEM es que necesita muchos recursos como componentes para poder brindar el análisis correspondiente y lo más importante este SIEM es para personas que tengan conocimientos en la parte de programación ya que es muy necesario programar las reglas necesarios para la detección de intrusos.
- Para el uso de *Alien Vault* se requirió una máquina de apoyo la cual permite conectarse a la interfaz gráfica ya que la máquina virtual donde se instala el SIEM no tiene interfaz gráfica, solo es de líneas de comandos. Con la dirección IP creada, se procede a ingresar desde cualquier navegador permitiendo la visualización de la interfaz de *Alien Vault*.

5 RECOMENDACIONES

- Tener en cuenta los requisitos que necesitan para instalar los SIEM, ya que hay algunas herramientas como *ALIEN VAULT* que necesitan una RAM mayor de 8(Gb) para su perfecto funcionamiento.
- Verificar las versiones de los SIEM ya que no todas las versiones tienen todas las herramientas posibles para detectar el ataque requerido, un ejemplo el SIEM *Wazuh* para poder detectar el *MALWARE* se debe tener la última versión que es la 4.8.
- Para la utilización de las máquinas virtuales no es necesario utilizar GNS3 ya que en la aplicación del VMware se tiene un Switch digital el cual permite tener conectividad en toda la red sin estar creando una topología extra.
- Tener en cuenta que si se quiere utilizar todas las opciones en el *AlienVault* se tendrá que pagar para así tener acceso a cada una de ella.
- Verificar si la tarjeta RAM y la memoria del equipo, en donde están utilizando las máquinas pueda rendir para todo si no se debe aumentar la memoria y la RAM

ya que algunos SIEM son exigentes al momento de instalarse y piden más de lo normal.

- Tener en cuenta que si se configuró las máquinas virtuales con la red del hogar y si se traslada el equipo, donde se encuentran las máquinas, a otro sitio es posible que el direccionamiento cambie, dando problemas de conectividad y se pierde la información de los SIEM ya instalados.
- Para la agregación de los agentes en el servidor *Wazuh* hay que verificar mucho la versión ya que en algunos casos no le detecta al agente y es imposible detectarlo.
- Para la agregación del agente en el *AlienVault* hay que tener en cuenta que al configurar el direccionamiento se debe incluir la dirección IP del agente para que pueda ser reconocida, si se utiliza otra dirección IP que no sea del agente este no será detectado por el servidor.
- Para la instalación de los SIEM hay que tener todas las herramientas instaladas del programa de virtualización para evitar problemas o que no se instalen todos los recursos de los SIEM.
- Dependiendo la utilidad no es recomendable usar GNS3 para la virtualización ya que se está utilizando el VMware y puede causar pérdida de datos a la máquina virtualizada o en otros casos nunca encenderse.
- Para tener un mejor rendimiento si se tiene las aplicaciones de VMware y GNS3 instalados es mejor desinstalarlos y volverlo a instalar ya que puede tener algún daño o no estar completamente instalados.
- Al momento de instalar el SIEM *Alien Vault* se puede omitir algunas funciones de la máquina para que no consuma muchos recursos y tenga más capacidad.
- Para la seguridad de la red es necesario siempre tener actualizados los antivirus o instalar un *Firewall* para mejor protección.
- Para tener un mejor análisis de los SIEM es mejor tratar de crear reglas personalizadas para así detectar algún virus que no esté agregado en los SIEM.
- Para tener más conocimiento de los SIEM, es mejor buscar información de cada uno y estar informado de cada actualización ya que puede tener nuevas funciones o no estar estable para la seguridad.
- Tener en cuenta que al volver a iniciar la herramienta *Wazuh* se debe ingresar el comando de inicio (*sudo systemctl star Wazuh-manager*) ya que si no se lo aplica puede dar problemas en el acceso a la interfaz provocando que se dañe la configuración.

6 REFERENCIAS BIBLIOGRÁFICAS

[1] «BLOG ESPECIALIZADO EN CIBERSEGURIDAD,» Grupo ESG Innova, 11 Marzo 2021. [En línea]. Available: https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/. [Último acceso: 10 Julio 2024].

[2] M. Pallero y J. M. Heguiabehere, «Seguridad de la Informacion y Ciberseguridad,» 11 Diciembre 2023. [En línea]. Available: https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf. [Último acceso: 10 Julio 2024].

[3] E. Vaega Briceño, «LIBRO-SEGURIDAD-INFORMACIÓN,» Marzo 2021. [En línea]. Available: https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf. [Último acceso: 10 Julio 2024].

[4] b. Ambit, «Ambit bst,» 10 Noviembre 2020. [En línea]. Available: https://www.ambit-bst.com/blog/tipos de vulnerabilidades y amenazas informaticas. [Último acceso: 11 Julio 2024].

[5] J. J. Santos Chavez, «Deltaprotect,» 20 Abril 2023. [En línea]. Available: https://www.deltaprotect.com/blog/amenazas-de-ciberseguridad. [Último acceso: 10 Julio 2024].

[6] Akamai, «Akamai,» 16 Enero 2024. [En línea]. Available: https://www.akamai.com/es/glossary/what-is-cybersecurity. [Último acceso: 10 Julio 2024].

[7] I. Belcic, «Avast,» 22 Septiembre 2020. [En línea]. Available: https://www.avast.com/es-es/c-sql-injection. [Último acceso: 12 Julio 2024].

[8] I. Belcic, «Avast,» 19 Enero 2023. [En línea]. Available: https://www.avast.com/es-es/c-malware. [Último acceso: 10 Julio 2024].

[9] L. Institute, «lisainstitute,» 01 Septiembre 201. [En línea]. Available: https://www.lisainstitute.com/blogs/blog/troyanos-tipos-modus-operandi-medidas-preventivas-consejos. [Último acceso: 12 Julio 2024].

[10] Kaspersky, «Latam.Kaspersky,» 01 Diciembre 2017. [En línea]. Available: https://latam.kaspersky.com/resource-center/threats/trojans. [Último acceso: 10 Julio 2024].

[11] J. Albors, «Welivesecurity,» 17 Abril 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/04/17/que-es-un-backdoor/. [Último acceso: 12 Julio 2024].

[12] A. 34, «Protecciondatos,» 14 MAyo 2020. [En línea]. Available: https://protecciondatos-lopd.com/empresas/backdoor/. [Último acceso: 12 Julio 2024].

[13] C. Cilleruelo, «KEEPCODING,» 14 Junio 2024. [En línea]. Available: https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/. [Último acceso: 12 Julio 2024].

[14] A. «ID boot camps,» 04 Abirl 2023. [En línea]. Available: https://iddigitalschool.com/bootcamps/que-es-el-blue-team-en-ciberseguridad.. [Último acceso: 11 Julio 2024].

[15] C. Polanco, «SOFECOM,» 18 MAyo 2018. [En línea]. Available: https://sofecom.com/que-es-un-siem/. [Último acceso: 11 Julio 2024].

[16] J. A. Gómez, «Deltaprotect,» 25 Julio 2023. [En línea]. Available: https://www.deltaprotect.com/blog/siem-que-es. [Último acceso: 12 Julio 2024].

[17] G. Atico, «Grupo Atico 34,» 13 Mayo 2021. [En línea]. Available: https://protecciondatos-lopd.com/empresas/seguridad-hardware/. [Último acceso: 20 Julio 2024].

[18] *WAZUH*, «*WAZUH*,» 07 Mayo 2022. [En línea]. Available: https://documentation.*WAZUH*.com/current/quickstart.html. [Último acceso: 20 Julio 2024].

[19] Ichasco, «Ichasco,» 08 Enero 2015. [En línea]. Available: https://blog.ichasco.com/ossim/. [Último acceso: 20 Julio 2024].

ANEXO I: CERTIFICADO DE ORIGINALIDAD

CERTIFICADO DE ORIGINALIDAD
TRABAJO DE INTEGRACIÓN CURRICULAR

Quito, D.M. 31 de Julio de 2024

De mi consideración:

Yo, GABRIELA KATHERINE CEVALLOS SALAZAR, en calidad de Director del Trabajo de Integración Curricular titulado IMPLEMENTACIÓN DE UN SIEM PARA LA DEFENSA ACTIVA ANTE UN ATAQUE POR MALWARE asociado al proyecto IMPLEMENTACIÓN DE UN SIEM PARA LA DEFENSA ACTIVA ANTE INTRUSIONES EN UNA RED elaborado por el estudiante EDISON JAVIER PACHACAMA TACURI de la carrera en TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES, certifico que he empleado la herramienta antiplagio "Turnitin" para la revisión de originalidad del documento escrito 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 informe generado por la herramienta Turnitin.

https://epnecuador-my.sharepoint.com/:b:/g/personal/gabriela_cevalloss_epn_edu_ec/Ecq3kPJNIhJBgcjCe2CDUK4B1Tq6BZE3rx-6UYAzX3wmUg?e=CIKg38

Atentamente,

GABRIELA KATHERINE CEVALLOS SALAZAR
Docente
Escuela de Formación de Tecnólogos

ANEXO II: Enlaces