MAESTRÍA EN CIBERSEGURIDAD

Trabajo previo a la obtención de título de

Magister de Ciberseguridad

AUTORES:

Gladis Sofía Asadovay Lema

Liliana Mercedes Caiza Ortiz

Brenda Elizabeth Pérez Moreno

Carlos Hernán Ponce Samaniego

TUTOR:

Alejandro Cortés López

TEMA

Propuesta de implementación de un sistema SIEM Open Source WAZUH que permita la detección, contención, respuesta automática y notificación de incidentes de Ciberseguridad.

Quito- Ecuador

REINVENTEMOS EL FUTURO

Certificación de autoría

Nosotros, **Liliana Mercedes Caiza Ortiz, Gladis Sofia Asadovay Lema, Brenda Elizabeth Pérez Moreno y Carlos Hernán Ponce Samaniego,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

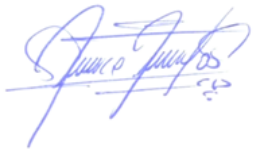
Firma del graduando

Liliana Mercedes Caiza Ortiz

Firma del graduando

Gladys Sofia Asadovay Lema

Firma del graduando



Firma del graduando

Brenda Elizabeth Pérez Moreno **Carlos Hernán Ponce Samaniego**

Autorización de Derechos de Propiedad Intelectual

Nosotros, Liliana Mercedes Caiza Ortiz, Gladis Sofia Asadovay Lema, Brenda Elizabeth Pérez Moreno y Carlos Hernán Ponce Samaniego, en calidad de autores del trabajo de investigación titulado **Implementación de un sistema SIEM Open Source (Wazuh) que permita la detección, contención, reacción automática y notificación de incidentes de ciberseguridad**, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, Junio 2025

Firma del graduando

Liliana Mercedes Caiza Ortiz

Firma del graduando

Gladis Sofia Asadovay Lema

Firma del graduando	**Firma del graduando**
Brenda Elizabeth Pérez Moreno	Carlos Hernán Ponce Samaniego

Aprobación de dirección y coordinación del programa

Nosotros, **Alejandro Cortés e Iván Reyes,** declaramos que: **Liliana Mercedes Caiza Ortiz, Gladis Sofia Asadovay Lema, Brenda Elizabeth Pérez Moreno y Carlos Hernán Ponce Samaniego**, son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

Alejandro Cortés L.	Iván Reyes Ch.
Maestría en Ciberseguridad	Maestría en Ciberseguridad

DEDICATORIA

Dedico este trabajo a mi querida hija Alison, que es el motor de mi vida y el impulso a seguir superándome cada día. A mi esposo Jairo, por ser mi compañero incondicional, por su comprensión y su apoyo en los momentos más difíciles. Y a mis padres, por haber fomentado mi crecimiento académico y personal y por estar presentes en cada etapa de este camino.

Sofia Asadovay

Quiero dedicar el presente trabajo a mis amados hijos, Emily y Dominic que son mi motivación para levantarme y luchar día a día, a mi amada esposa y compañera de vida que me ha sabido apoyar y darme fuerzas ante los momentos difíciles con su gran amor y cariño, a mi madre querida que siempre ha estado a mi lado apoyándome y formándome para ser mejor cada día y ser siempre un hombre de bien.

Carlos Ponce

Dedico este trabajo y cada paso que me atrevo a dar para seguir avanzando en la vida a Andy, mi compañero de vida y a mi princesa Daya, ambos son mi mayor motivación.

A mis padres y hermanos porque siempre querré volver a mi hogar.

Liliana Caiza

A mi familia que me ha inculcado los valores que me han permitido dirigir mi vida personal y profesional con códigos y amor, en especial a mi ángel que siempre se encuentra en cada paso de mi vida.

Brenda Pérez

AGRADECIMIENTOS

Agradezco en primer lugar a Dios, por darme la fortaleza, la sabiduría y la perseverancia necesarias para alcanzar esta meta, a la Universidad Internacional del Ecuador (UIDE), por brindarme un espacio de formación académica y a los profesores, por compartir su conocimiento. Gracias a todos quienes, de una u otra forma, fueron parte de este proceso.

Sofia Asadovay

Quiero agradecer ante todo a Dios por darme salud y vida por guiarme en todo momento porque camino seguir, a mis amigos, compañeros que han sabido apoyarme y contribuir con cada granito de arena para reforzar mi conocimiento y a las personas que confiaron en mí y me abrieron las puertas para formarme profesionalmente.

Carlos Ponce

Primero a Dios por tantas bendiciones, lo que siempre le pido es salud y sabiduría. Gracias, mi amor Andy porque hacemos un gran equipo y sin tu apoyo no sería lo mismo.

A mi amiga Sofi por haberme convencido a seguirnos preparando formalmente y a todas las personas importantes en mi vida.

Liliana Caiza

Agradezco a Dios, mi familia, mis amigos que siempre han sido el impulso para mejorar en mi vida, siempre recordando los valores y el cariño que me han compartido, sin ustedes nada sería posible.

Brenda Pérez

RESUMEN

El presente documento tiene como propósito implementar un sistema SIEM Wazuh, que será instalado sobre un servidor CentOS e integrado con un servidor Active Directory y un servidor Web con Base de datos, sobre Ubuntu. Su objetivo es realizar la recolección de logs de cada uno de los servicios y visualizarlos en la consola del SIEM**,** permitiendo el análisis y correlación de eventos, así como la generación de casos de uso para garantizar un monitoreo continuo, proactivo y automatizado de la infraestructura.

La implementación de este sistema SIEM en la empresa Digimentore S.A. permitirá un monitoreo integral de los eventos de seguridad, reduciendo los tiempos de respuesta ante posibles incidentes y facilitando una reacción proactiva y oportuna. Con ello, se busca mitigar cualquier riesgo que pueda comprometer la información y los recursos de la organización.

Palabras Claves:

SIEM Sistema de Gestión de Eventos e Información de Seguridad

WAZUH Plataforma centralizada para análisis de logs

ABSTRACT

This document aims to implement a Wazuh SIEM system, which will be installed on a CentOS server and integrated with an Active Directory server and a web server with a database on Ubuntu. Its objective is to collect logs from each service and display them on the SIEM console, allowing for event analysis and correlation, as well as the generation of use cases to ensure continuous, proactive, and automated infrastructure monitoring.

The implementation of this SIEM system at Digimentore S.A. will enable comprehensive security event monitoring, reducing response times to potential incidents and facilitating a proactive and timely reaction. This approach seeks to mitigate any risks that could compromise the organization's information and resources.

Keywords:

SIEM Security Information and Event Management

WAZUH Open-source security platform

TABLA DE CONTENIDOS

CAPÍTULO 1 17

1. INTRODUCCION 17

1.1. Definición del proyecto. 17

1.2. Justificación e importancia del trabajo de investigación. 17

1.3. Alcance. 18

1.4. Objetivos. 18

CAPÍTULO 2 20

2. REVISIÓN DE LITERATURA 20

2.1. Estado del Arte. 20

2.2. Marco Teórico. 21

2.2.1. Que es un sistema SIEM 21

2.2.2. Como Funciona un sistema SIEM 22

2.2.3. Arquitectura y Componentes de un sistema SIEM 22

2.2.4. WAZUH232.2.5. Características Avanzadas de Wazuh como SIEM 24

2.2.6. Automatización de Respuesta ante Incidetes 25

CAPÍTULO 3 27

3. DESARROLLO 27

3.1. Desarrollo del Trabajo 27

3.1.1. Instalación y configuración Wazuh 28

3.1.2 Servidor GLPI 33

3.1.3 Instalación Servidor Active Directory 43

3.1.4 Instalación host windows. 52

3.1.5 Configuración envio de notiifcaciones via mail 57

CAPÍTULO 4 61

4. ANÁLISIS DE RESULTADOS 61

4.1. Pruebas de Concepto 61

4.1.1. Ataque de Fuerza Bruta 66

4.1.2 Escaneo de puertos 71

4.1.3. Ataque SQL 72

4.1.4. Ataque DoS 76

4.1.5. Ataque de MAC Flood 77

4.2. Análisis de Resultados. 79

4.2.1 Analísis de alertas generadas por un ataque de Fuerza Bruta 79

4.2.2. Analísis de alertas generadas por un Escaneo de puertos 82

4.2.3. Analísis de alertas generadas por un Ataque SQL 84

4.2.4. Analísis de alertas generadas por un Ataque DoS 86

4.2.5. Analísis de alertas generadas por un Ataque MAC Flood 86

CAPÍTULO 5 87

5. CONCLUSIONES Y RECOMENDACIONES 87

5.1. CONCLUSIONES 87

5.2. RECOMENDACIONES 87

LISTA DE TABLAS (Índice de tablas)

Tabla 1 Comparativa entre soluciones SIEM open source y comerciales 25

Tabla 2 Detalle Infraestructura 28

LISTA DE FIGURAS (Índice de figuras)

Figura 1 21

Figura 2 24

Figura 3 27

Figura 4 29

Figura 5 29

Figura 6 30

Figura 7 30

Figura 8 30

Figura 9 31

Figura 10 31

Figura 11 32

Figura 12 33

Figura 13 34

Figura 14 34

Figura 15 35

Figura 16 36

Figura 17 36

Figura 18 37

Figura 19 37

Figura 20 38

Figura 21 39

Figura 22 39

Figura 23 40

Figura 24 41

Figura 25 42

Figura 26 43

Figura 27 43

Figura 28 44

Figura 29 45

Figura 30 46

Figura 31 47

Figura 32 48

Figura 33 49

Figura 34 49

Figura 35 50

Figura 36 51

Figura 37 52

Figura 38 52

Figura 39 53

Figura 40 54

Figura 41 55

Figura 42 56

Figura 43 57

Figura 44 57

Figura 45 58

Figura 46 59

Figura 47 59

Figura 48 60

Figura 49 62

Figura 50 63

Figura 51 64

Figura 52 64

Figura 53 65

Figura 54 66

Figura 55 67

Figura 56 68

Figura 57 69

Figura 58 69

Figura 59 70

Figura 60 70

Figura 61 71

Figura 62 71

Figura 63 72

Figura 64 73

Figura 65 74

Figura 66 75

Figura 67 76

Figura 68 76

Figura 69 77

Figura 70 77

Figura 71 78

Figura 72 79

Figura 73 80

Figura 74 80

Figura 75 81

Figura 76 82

Figura 77 83

Figura 78 84

Figura 79 85

Figura 80 86

CAPÍTULO 1

1. INTRODUCCION

1.1. Definición del proyecto.

En un mundo más digital y en constante evolución tecnológica, personas, procesos y empresas se encuentran expuestas a amenazas constantes y ataques cada vez más sofisticados, que ponen en riesgo su confidencialidad e integridad. Ante este escenario, se evidencia la necesidad de mantener una vigilancia constante y una respuesta inmediata a cualquier posible ataque cibernético.

En este contexto, se resalta la importancia de implementar un Sistema de Gestión de Información y eventos de Seguridad (SIEM) basado en Wazuh, una plataforma open-source robusta que permite a las organizaciones detectar incidentes de ciberseguridad en tiempo real, ejecutar acciones automáticas de contención y respuesta ante amenazas, y generar notificaciones detalladas de los eventos, facilitando de esta manera una gestión proactiva y adecuada de la seguridad.

1.2. Justificación e importancia del trabajo de investigación.

Dado que las amenazas o ataques cibernéticos como ransomware, accesos no autorizados, filtraciones, denegación de servicios entre muchos otros más, son cada vez más frecuentes, es mandatorio contar con un sistema SIEM centralizado y robusto que permita detectar amenazas, tomar acciones automáticas y proactivas con el fin de prevenir incidentes de seguridad.

Implementar el sistema SIEM Wazuh, nos permitirá:

Mayor visibilidad, control y consolidación de eventos en los distintos componentes como hosts, servidores, redes y aplicaciones.

Detección proactiva de los diferentes tipos de amenazas.

Contención automática de ataques o amenazas presentes.

Reducción de riesgos operativos y afectación a los sistemas.

1.3. Alcance.

El alcance definido para nuestro proyecto abarca los siguientes puntos:

- Instalación del sistema SIEM Wazuh.
- Evaluación de la infraestructura a integrar.
- Integración de fuentes de datos.
- Correlación de eventos.
- Definición de casos de uso.
- Automatización de alertas proactivas y de contención.
- Configuración de notificaciones para envío de eventos y acciones ejecutadas.
- Diseño de la arquitectura

1.4. Objetivos.

1.4.1. Objetivo General.

Implementar un sistema SIEM Wazuh con la finalidad de optimizar el análisis de eventos y logs de la organización y poder ejecutar acciones automáticas y proactivas que contribuyan a la prevención y mitigación de riesgos que puedan comprometer la seguridad de la organización.

1.4.2. Objetivos Específicos.

Instalar, configurar e implementar el sistema SIEM Wazuh sobre una máquina virtual basada en CentOS con el fin de integrar con la infraestructura Active Directory y Aplicación Web con base de datos.

Realizar la correlación de eventos y proceder con la definición de casos de uso y realizar la automatización de alertas proactivas y de contención, así como la configuración de envío de notificaciones que evidencien las acciones ejecutadas.

Ejecutar ataques controlados que nos permitan observar y verificar la funcionalidad del SIEM con la finalidad de poder realizar los ajustes respectivos a las diferentes alertas y eventos se presentan.

CAPÍTULO 2

2. REVISIÓN DE LITERATURA

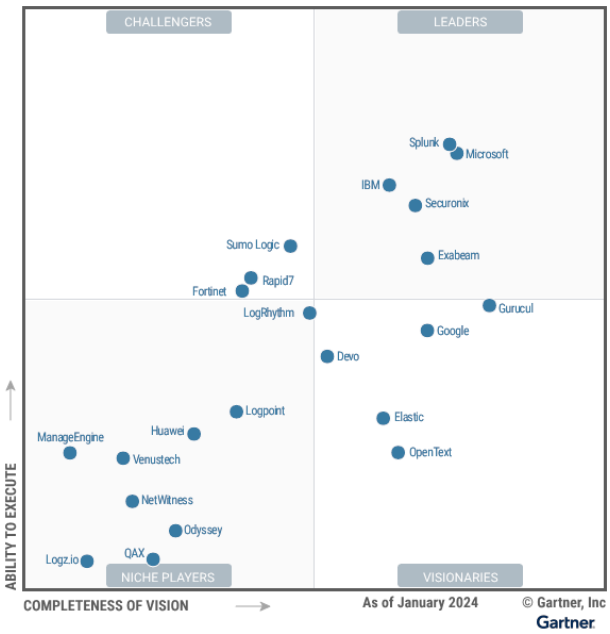
2.1. Estado del Arte.

En los últimos años, el avance tecnológico y la creciente ola de ataques cibernéticos que se presentan a nivel mundial ha generado la necesidad de buscar e implementar una solución que garantice la protección de los sistemas digitales y mantengan su integridad, para ello existen en el mercado soluciones bastantes robustas y avanzadas que permiten un monitoreo constante a los sistemas y aplicaciones.

En empresas pequeñas en las que el presupuesto es un factor limitante que dificulta la adquisición e implementación de sistemas propietarios SIEM por su costo como SPLUNK o QRadar de IBM, existen diferentes sistemas de código abierto, uno de ellos es Wazuh que es un sistema bastante flexible y de alto rendimiento y que permite la detección oportuna de intrusos, analítica de logs y un monitoreo en tiempo real.

Figura 1

Cuadrante de Gartner



Nota. Cuadrante de Gartner SIEMS. (ManageEngine, 2024).

Wazuh es una plataforma open-source de seguridad, que ofrece protección unificada de detección y respuesta ampliadas (XDR) y gestión de eventos e información de seguridad (SIEM) para puntos finales y cargas de trabajo en la nube, es una forma eficiente de proteger sus procesos de computación en la nube, contenedores y pods de Kubernetes, así como sus ordenadores y dispositivos cliente. (Heller, 2024).

2.2. Marco Teórico.

2.2.1. Que es un sistema SIEM

La información sobre seguridad y gestión de eventos o SIEM (Security Information and Event Management) es un sistema de seguridad que proporciona a las empresas una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos.

Los sistemas SIEM tienen un control total sobre todos los eventos que suceden en la empresa para poder detectar cualquier tendencia o patrón fuera de lo común y así actuar de forma inmediata, centraliza los registros de seguridad para interpretarlos y almacenarlos en tiempo real, facilitando la actuación inmediata.

Los sistemas SIEM están diseñados para incrementar y fortalecer el nivel de seguridad de una empresa, proporcionando una visión integral de la seguridad de TI (tecnología de la información). (Ambit BST, 2021).

2.2.2. Como Funciona un sistema SIEM

Las funciones principales que realiza un sistema SIEM son la de almacenar e interpretar los registros. Este proceso se realiza en tiempo real aportando de esta forma un alto grado de reacción para poder impedir o solucionar cualquier incidente relacionado con la seguridad informática.

El sistema SIEM recopila toda la información de forma centralizada en una base de datos para poder realizar un análisis profundo y así detectar tendencias y patrones de comportamiento que permitan diferenciar aquellos que no sean habituales. (Ambit BST, 2021).

2.2.3. Arquitectura y Componentes de un sistema SIEM

Un sistema SIEM se compone de varios módulos que trabajan en conjunto para ofrecer una visión completa de la seguridad de una organización:

- **Recolección de datos**: Captura de logs y eventos desde múltiples fuentes (firewalls, servidores, endpoints, etc.).
- **Normalización**: Conversión de los datos a un formato común para su análisis.

- **Correlación de eventos**: Identificación de patrones sospechosos mediante reglas predefinidas o inteligencia artificial.
- **Almacenamiento seguro**: Conservación de los registros para auditorías y análisis forense.
- **Visualización y alertas**: Dashboards interactivos y notificaciones en tiempo real.

2.2.4. WAZUH

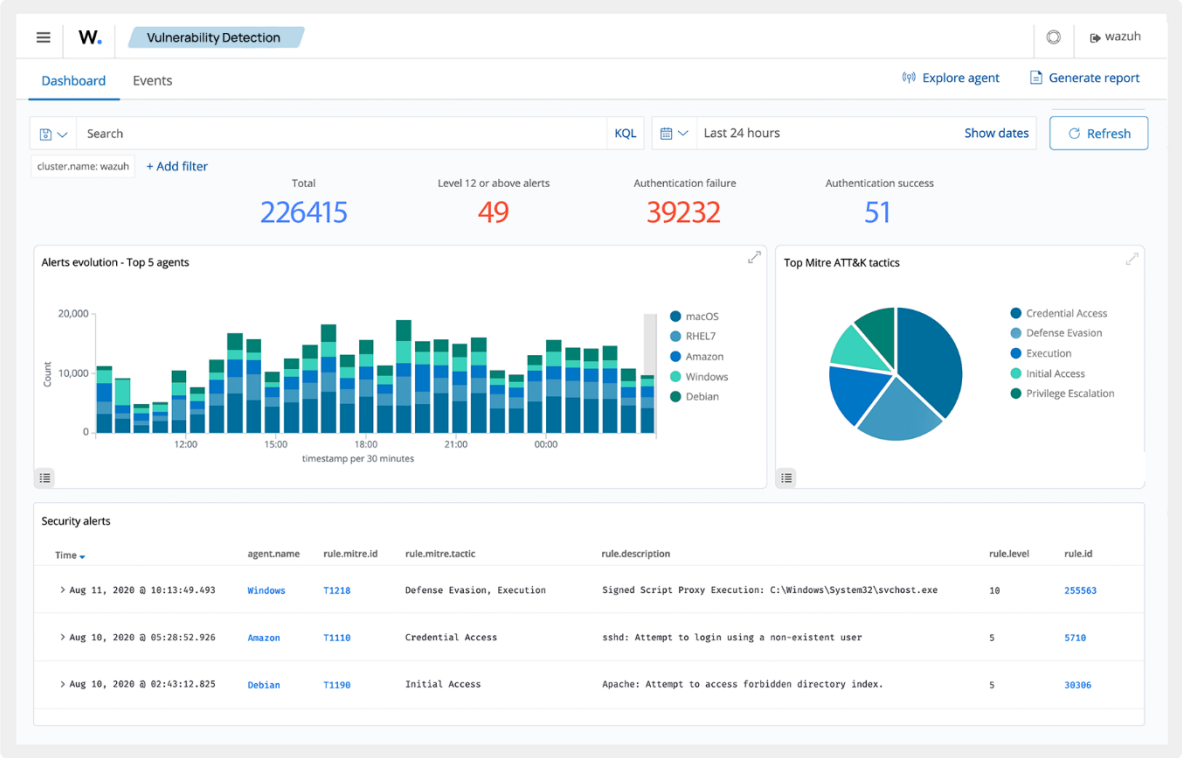
La solución Wazuh **Security Information and Event Management (SIEM)** es una plataforma centralizada que agrega y analiza la telemetría en tiempo real para la detección de amenazas y el cumplimiento normativo. Wazuh recopila datos de eventos de diversas fuentes, como endpoints, dispositivos de red, cargas de trabajo en la nube y aplicaciones, para una mayor cobertura de seguridad. (Wazuh, 2025).

Wazuh recopila, almacena y analiza datos de eventos de seguridad para identificar anomalías o indicadores de vulnerabilidades.

Reciba alertas y notificaciones en tiempo real cuando se produzcan incidentes de seguridad. Wazuh correlaciona eventos de múltiples fuentes, integra fuentes de inteligencia de amenazas y proporciona paneles e informes personalizables. Puede personalizar las alertas para satisfacer sus necesidades específicas. Esto permite a los equipos de seguridad responder rápidamente a las amenazas y minimizar el impacto de los incidentes de seguridad. (Wazuh, 2025).

Figura 2

Dashboard wazuh



Nota: Muestra el panel principal de alertas de wazuh

2.2.5. Características Avanzadas de Wazuh como SIEM

Wazuh no solo cumple con las funciones básicas de un SIEM, sino que también ofrece características avanzadas:

- Análisis de integridad de archivos (FIM): Detecta cambios no autorizados en archivos críticos del sistema.
- Detección de rootkits: Identifica software malicioso oculto en el sistema operativo.
- Gestión de vulnerabilidades: Escanea sistemas en busca de debilidades conocidas.

- Cumplimiento normativo: Genera reportes para estándares como PCI DSS, HIPAA, ISO 27001, entre otros.
- Integración con herramientas externas: Como VirusTotal, Shodan, y plataformas de threat intelligence.

2.2.6. Automatización de Respuesta ante Incidetes

Una de las ventajas más poderosas de Wazuh es su capacidad de ejecutar respuestas automáticas ante ciertos eventos. Esto se logra mediante:

- Active Response: Scripts que se ejecutan automáticamente cuando se detecta una amenaza (por ejemplo, bloquear una IP maliciosa).
- Integración con herramientas de orquestación como Ansible para respuestas más complejas.
- Alertas personalizadas que permiten priorizar incidentes según su criticidad.
- Notificación y Gestión de Alertas por Correo electrónico, Telegram, dashboards en Kibana, Sistemas de tickets (como Jira o ServiceNow).

Tabla 1

Comparativa entre soluciones SIEM open source y comerciales

Característica	Wazuh	Splunk	QRadar
Licencia	Open Source	Comercial	Comercial
Integración con ELK	Sí	Opcional	No
Active Response	Sí	Limitado	Sí

Cumplimiento normativo	Alto	Alto	Alto
Escalabilidad	Alta	Muy alta	Alta

Nota. Se tomaron en cuenta las características más relevantes de cada herramienta.

CAPÍTULO 3

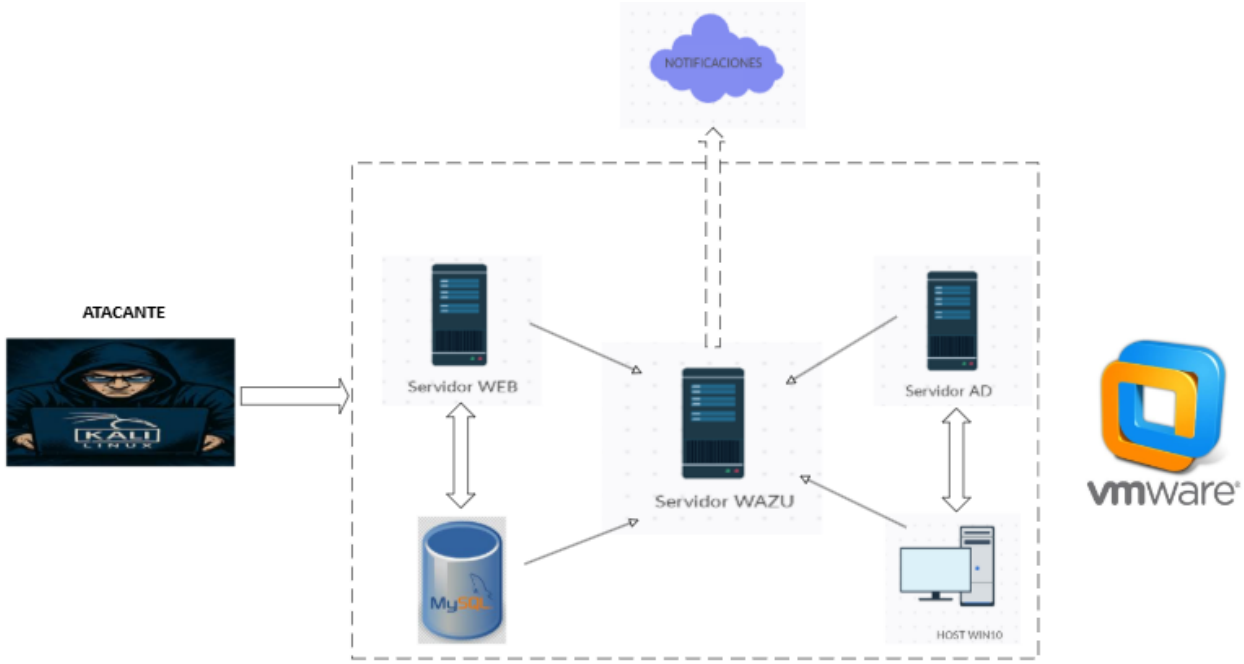
3. DESARROLLO

3.1. Desarrollo del Trabajo

Como parte de la infraestructura de la implementación del sistema SIEM WAZUH se procedió con la implementación bajo la arquitectura adjunta con virtualización Vmware.

Figura 3

Arquitectura



Nota: Arquitectura implementada

La implementación consta de 4 máquinas virtuales interconectadas entre si más una máquina virtual con kali linux que nos servirá para simular los ataques y poder generar las alertas sobre los servidores de AD y Web que serán monitoreadas en tiempo real con wazuh, la infraestructura implementada se detalla con sus roles en la tabla adjunta:

Tabla 2

Detalle Infraestructura

Server	Ip	Rol
Wazuh	172.16.11.76	Servidor Wazuh
Win-AD	172.16.11.100	Active Directory
Vmhost	172.11.86	Host Windows
webserver	192.168.124.139	Servidor Web Ubuntu GLPI

Nota: Se muestra el detalle de la infraestructura con su rol, ip y hostname

3.1.1. Instalación y configuración Wazuh

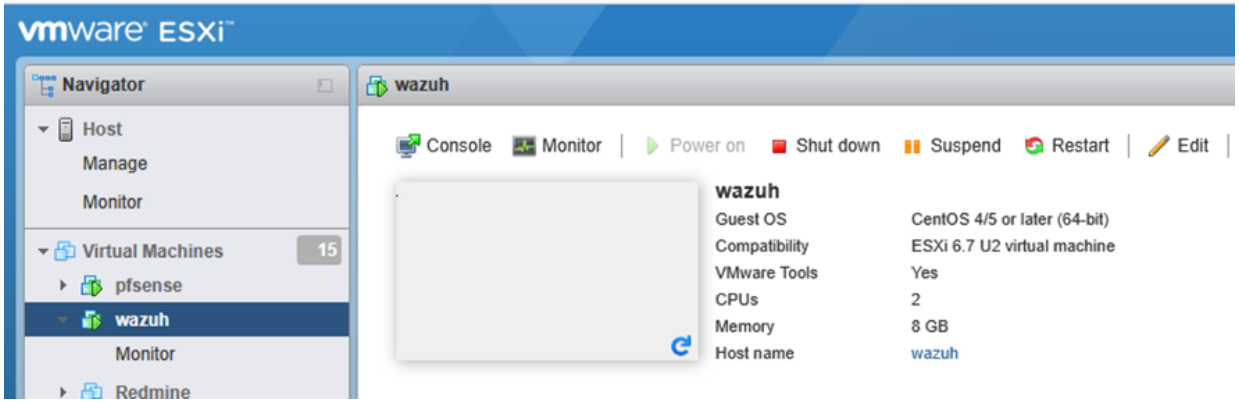
Wazuh como se indica en la documentación oficial puede ser instalada en un único host o se lo puede distribuir en diferentes hosts en modo clústers, para nuestra implementación lo vamos a ejecutar sobre un solo nodo bajo el sistema Operativo CentOS.

Procedemos con la instalación del sistema Operativo CentOS bajando su instalador de la página oficial. (The CentOS Project, s.f.).

Para nuestro caso se instaló la versión 10 de CentOS bajo el paquete CentOS-Stream-10-latest-x86_64-dvd1.iso sobre virtualización VmWare.

Figura 4

VM CentOS



Nota: Servidor CentOS

Versión vista desde el sistema operativo

Figura 5

Versión de Sistema Operativo

```
[wazuh@localhost ~]$ cat /etc/os-release
NAME="CentOS Stream"
VERSION="10 (Coughlan)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="10"
PLATFORM_ID="platform:el10"
PRETTY_NAME="CentOS Stream 10 (Coughlan)"
ANSI_COLOR="0;31"
LOGO="fedora-logo-icon"
CPE_NAME="cpe:/o:centos:centos:10"
HOME_URL="https://centos.org/"
VENDOR_NAME="CentOS"
VENDOR_URL="https://centos.org/"
BUG_REPORT_URL="https://issues.redhat.com/"
REDHAT_SUPPORT_PRODUCT="Red Hat Enterprise Linux 10"
REDHAT_SUPPORT_PRODUCT_VERSION="CentOS Stream"
[wazuh@localhost ~]$
```

Nota: Versión de sistema operativo vista desde la consola de comandos.

Con el sistema operativo listo acorde a la documentación procedemos con la descarga de asistente de instalación de wazuh ejecutando el comando adjunto:

Figura 6

Comando de descarga

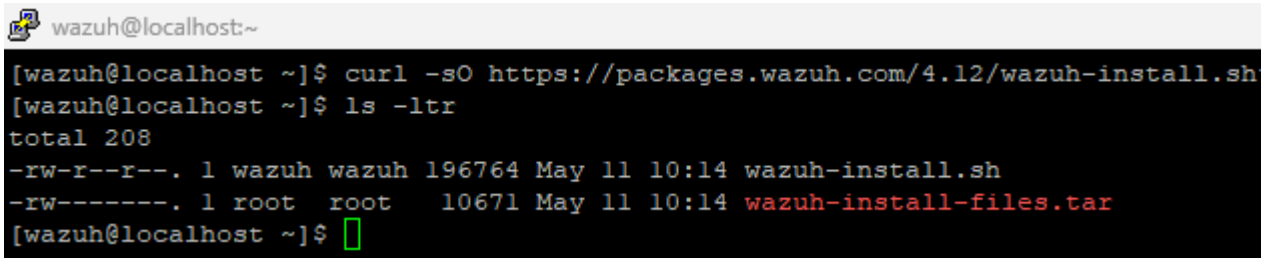
```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
```

Nota: Ejecución del comando para descarga.

El comando descargará el asistente wazuh-install.sh que nos permitirá continuar con la instalación.

Figura 7

Asistente de Instalación



Nota: Se descarga el asistente de instalación wazuh.

Descargado el asistente de instalación ejecutamos el comando adjunto para proceder con la instalación:

Figura 8

Comando de Instalación

```
sudo bash wazuh-install.sh -a
```

Nota: Ejecución del comando instalación wazuh.

Figura 9

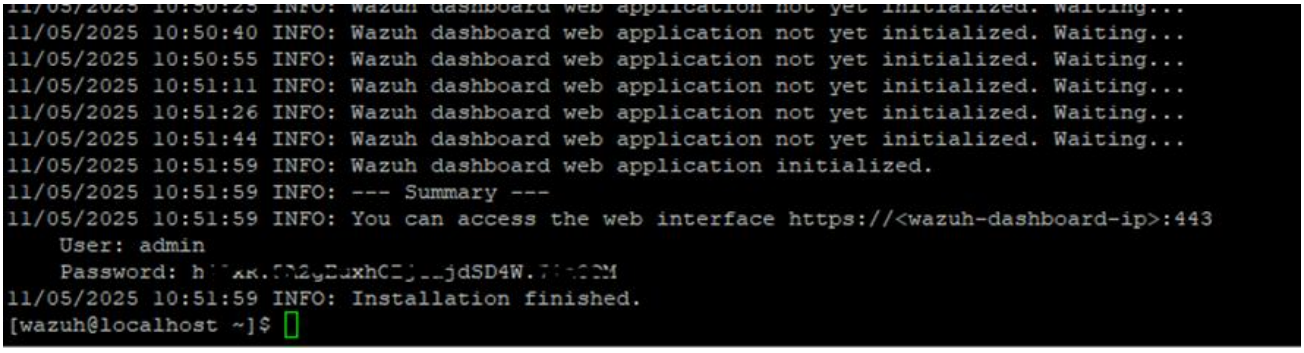
Instalación Wazuh

Nota: Se muestra el inicio de la instalación de wazuh.

Finalizada la instalación nos emite el usuario y la contraseña que nos permitirá el acceso a la consola de wazuh

Figura 10

Finalización de la Instalación Wazuh



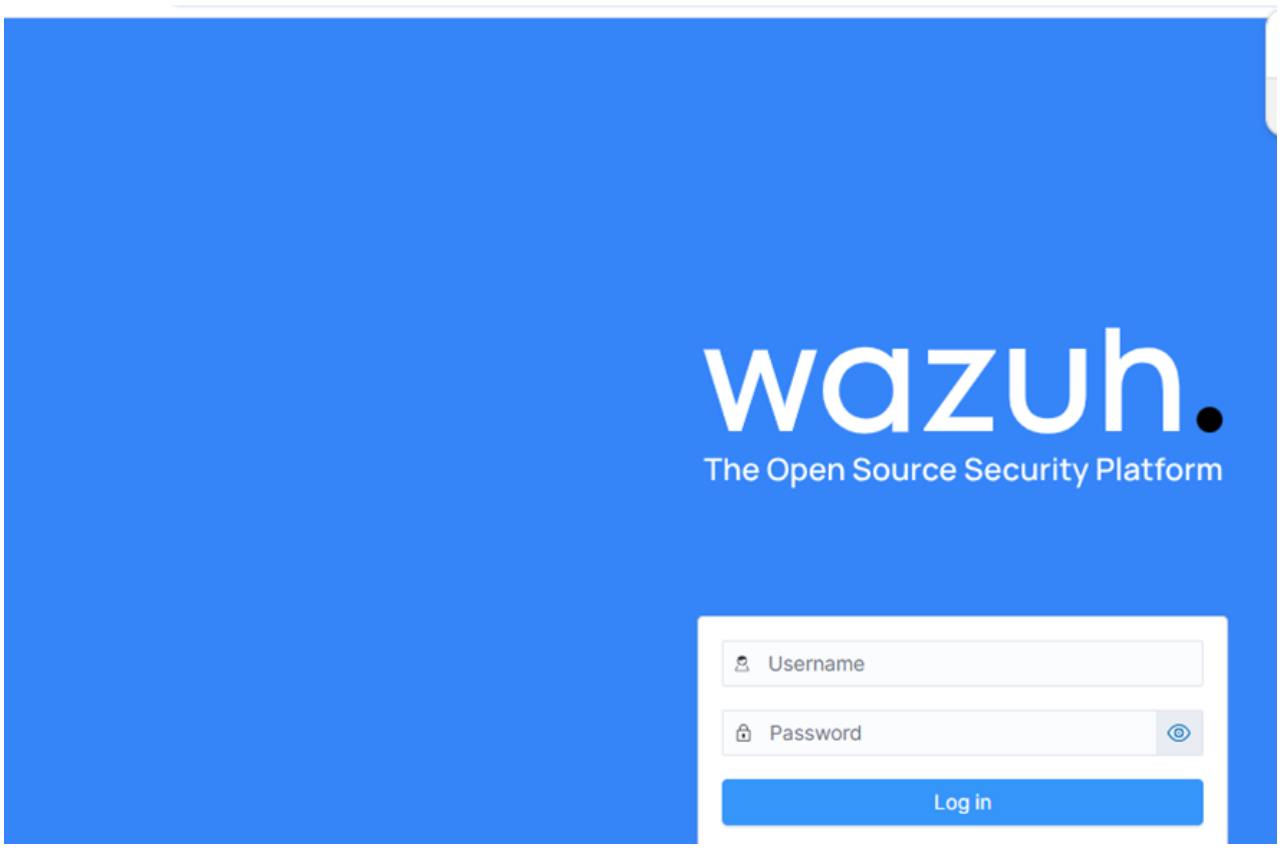
Nota: Finalizada la instalación muestra el usuario y contraseña de acceso

Finalizada la instalación satisfactoriamente ingresamos por el navegador con la IP del servidor de wazuh y puerto 443.

https://172.16.11.76/app/login?

Figura 11

Wazuh

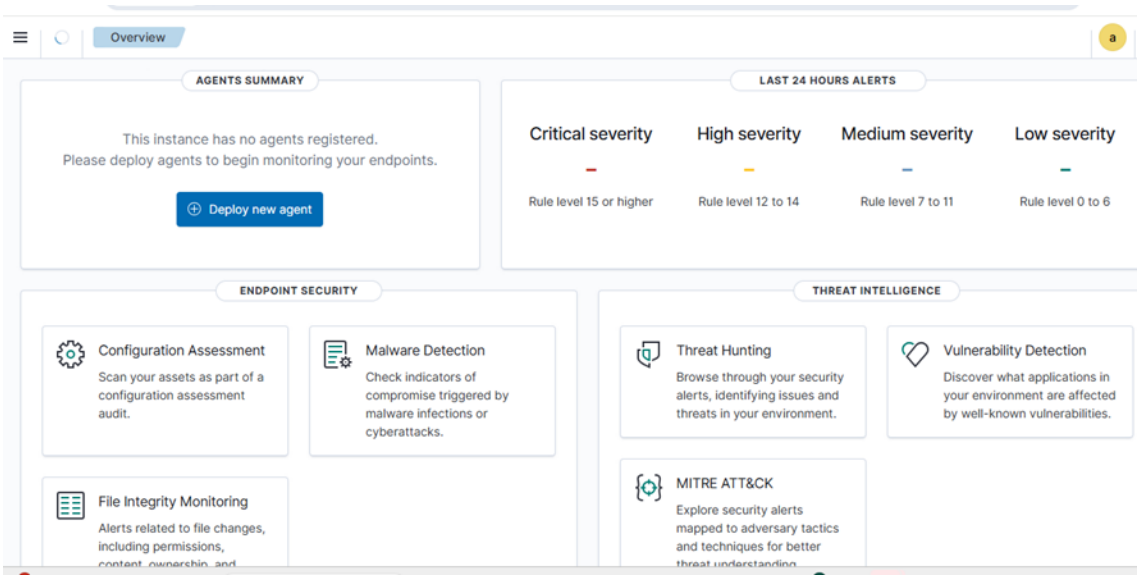


Nota: Página de login wazuh.

Ingresamos el usuario y la contraseña que nos emitió al finalizar la instalación de wazuh para acceder a la página principal de la consola.

Figura 12

Página principal de wazuh



Nota: Página de principal wazuh.

3.1.2 Servidor GLPI

Solución de gestión de servicios de TI basada en la aplicación GLPI (Gestionnaire Libre de Parc Informatique), implementado sobre una pila LAMP (Linux, Apache, MySQL, PHP) en un entorno Ubuntu 24.04 LTS.

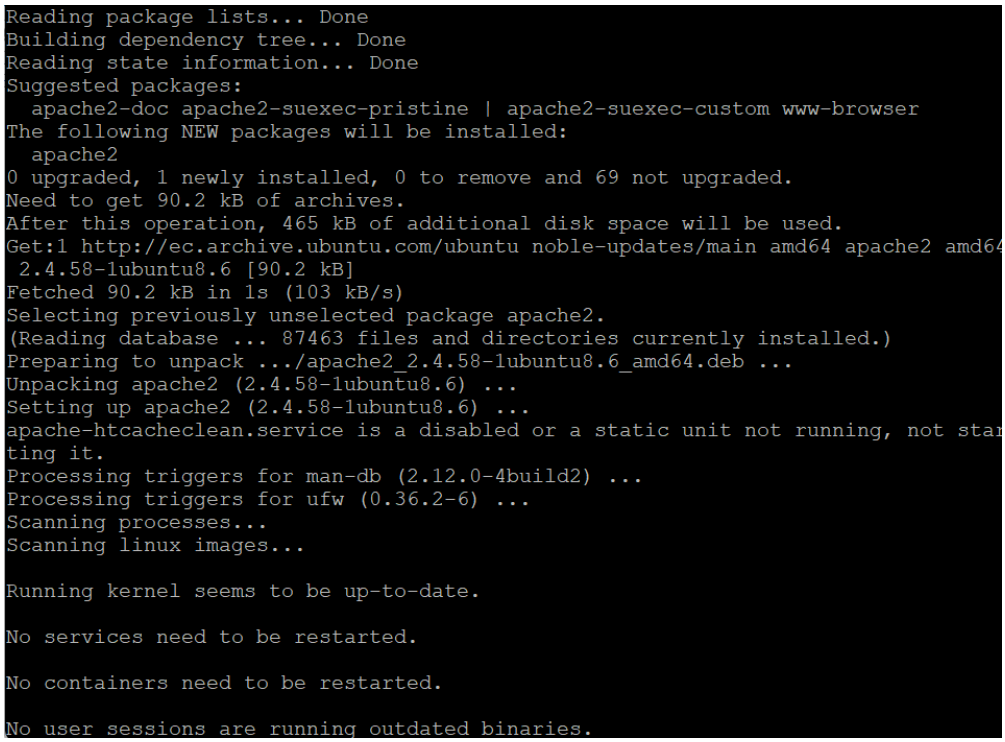
Instalación de los componentes:

- **Servidor WEB: Apache 2.4**

Se realiza la instalación de Apache (apache2) con el manejador de paquetes de Ubuntu apt.

Figura 13

Instalación de apache

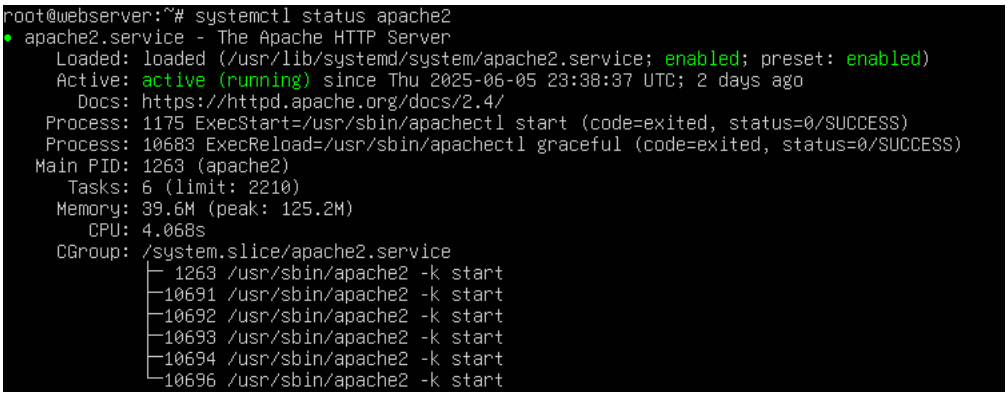


Nota: Se muestra el progreso de la instalación de apache2 en la VM

Una vez finalizada la instalación, se puede verificar el estado del servicio apache en estado running.

Figura 14

Servicio apache2



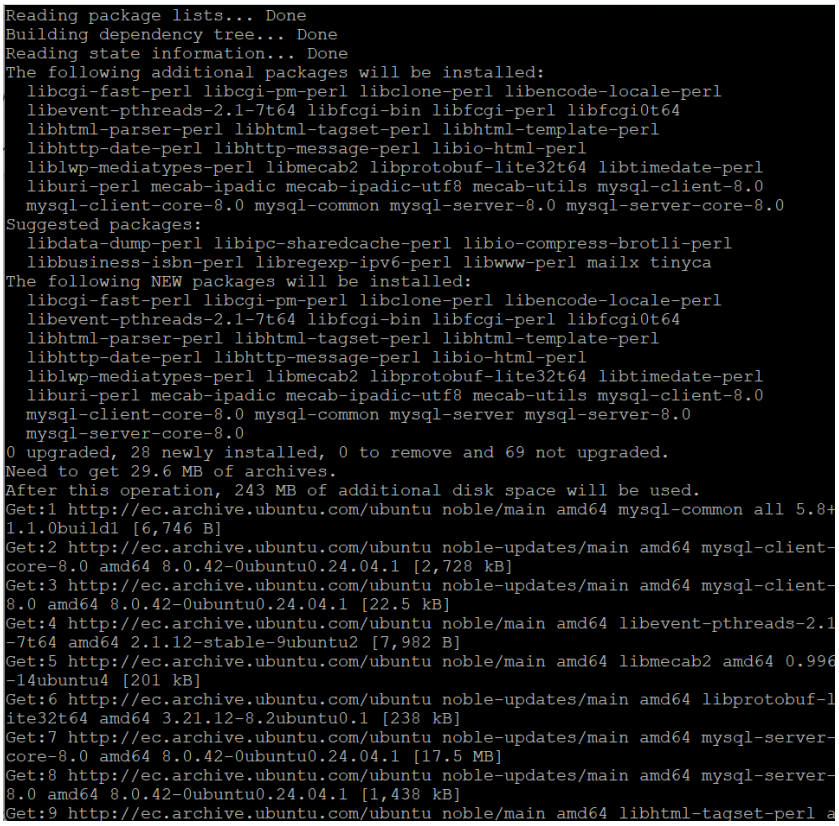
Nota: Se muestra que el servicio se encuentra en estado Running

- **Motor de Base de datos: MySQL**

A continuación, se instala la base de datos MySQL (mysql-server), con el manejador de paquetes apt.

Figura 155

Instalación MySQL

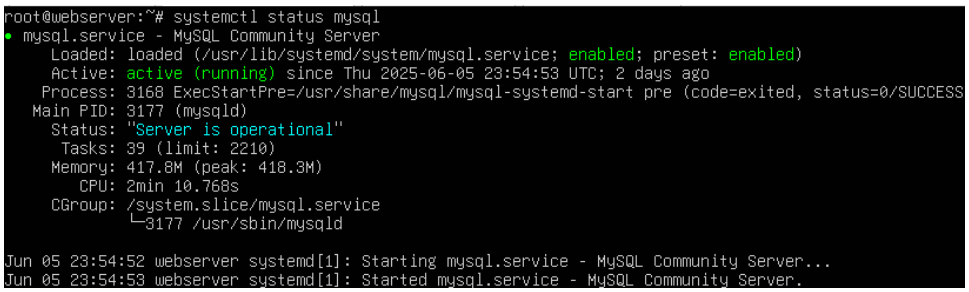


Nota: Se muestra el progreso de la instalación de MySQL

Una vez finalizada, se verifica el estado del servicio mysql.

Figura 16

Servicio MySQL



Nota: Se verifica que MySQL está en estado Running

- **Lenguaje de servidor: PHP**

Instalar PHP y extensiones necesarias: php, php-cli, php-curl, php-mysql, php-gd, php-mbstring, php-imap, php-xml, php-ldap, php-apcu, php-zip, php-bcmath y libapache2-mod-php

Figura 17

Versión de PHP

Nota: Se verifica que la versión instalada de PHP es 8.3.6

- **Aplicación: GLPI**

Previo a la instalación se crea la base de datos para GLPI, utilizando el cliente mysql.

Figura 18

Creación de base y usuario en MySQL

```
mysql> CREATE DATABASE glpidb DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
Query OK, 1 row affected (0.01 sec)

mysql> CREATE USER 'glpiusr'@'localhost' IDENTIFIED BY 'glpiusr';
Query OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiusr'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

Nota: Se muestra la creación de la base y usuario para GLPI

Una vez que se ha creado la bdd para GLPI, se realiza la descarga del instalador de GLPI.

Figura 19

Descarga de instalador de GLPI

```
--2025-06-08 01:19:41--  https://github.com/glpi-project/glpi/releases/download/10.0.15/glpi-10.0.15.tgz
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/39182755/522ff5e8-464a-4ea3-85f2-65c5089274b3?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250608%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250608T011942Z&X-Amz-Expires=300&X-Amz-Signature=eb8fdcef4dd3cb0ed0083cf1039b9917c93d685f0a5045d353debdcbb263a8d9&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dglpi-10.0.15.tgz&response-content-type=application%2Foctet-stream [following]
--2025-06-08 01:19:42--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/39182755/522ff5e8-464a-4ea3-85f2-65c5089274b3?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250608%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250608T011942Z&X-Amz-Expires=300&X-Amz-Signature=eb8fdcef4dd3cb0ed0083cf1039b9917c93d685f0a5045d353debdcbb263a8d9&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dglpi-10.0.15.tgz&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 59757265 (57M) [application/octet-stream]
Saving to: 'glpi-10.0.15.tgz'

glpi-10.0.15.tgz            100%[=========================================>]  56.99M  32.5MB/s    in 1.8s

2025-06-08 01:19:44 (32.5 MB/s) - 'glpi-10.0.15.tgz' saved [59757265/59757265]

root@glpiserver:~# ls 'lrt
> ^C
root@glpiserver:~# ls -lrt
total 58360
-rw-r--r-- 1 root root 59757265 Apr 24  2024 glpi-10.0.15.tgz
```

Nota: Se muestra la descarga del instalador comprimido

Se descomprime el instalador en la ruta /var/ww/html y se asignan los propietarios y permisos necesarios al usuario www-data, sobre los archivos para el funcionamiento de la aplicación.

- **Integración de GLPI y Apache**

Se crea un archivo de Virtual Host en Apache que define los parámetros necesarios para exponer la aplicación GLPI, especificando los campos:

`DocumentRoot` Define la raíz del sitio Web

`ServerName` IP de escucha

Las directivas de acceso (<Directory>) para controlar el comportamiento del servidor web sobre ese recurso.

Se crea el archivo */etc/apache2/sites-available/glpi.conf,* que contiene:

Figura 20

Creación de Virtual Host en Apache

```
root@webserver:~# cat /etc/apache2/sites-available/glpi.conf
<VirtualHost *:80>
    ServerName 192.168.100.56
    DocumentRoot /var/www/glpi<F2>public

    <Directory /var/www/glpi/public>
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/glpi_error.log
    CustomLog ${APACHE_LOG_DIR}/glpi_access.log combined
</VirtualHost>
```

Nota: Se muestra la configuración del Virtual Host, donde consta la IP del servidor Web

Se realiza la activación del sitio utilizando la herramienta a2ensite, y se realiza el reinicio del servicio de apache.

Una vez que se han realizado los cambios, se ingresa a la url de http:ipserver/glpi y se despliega la instalación de GLPI

Figura 21

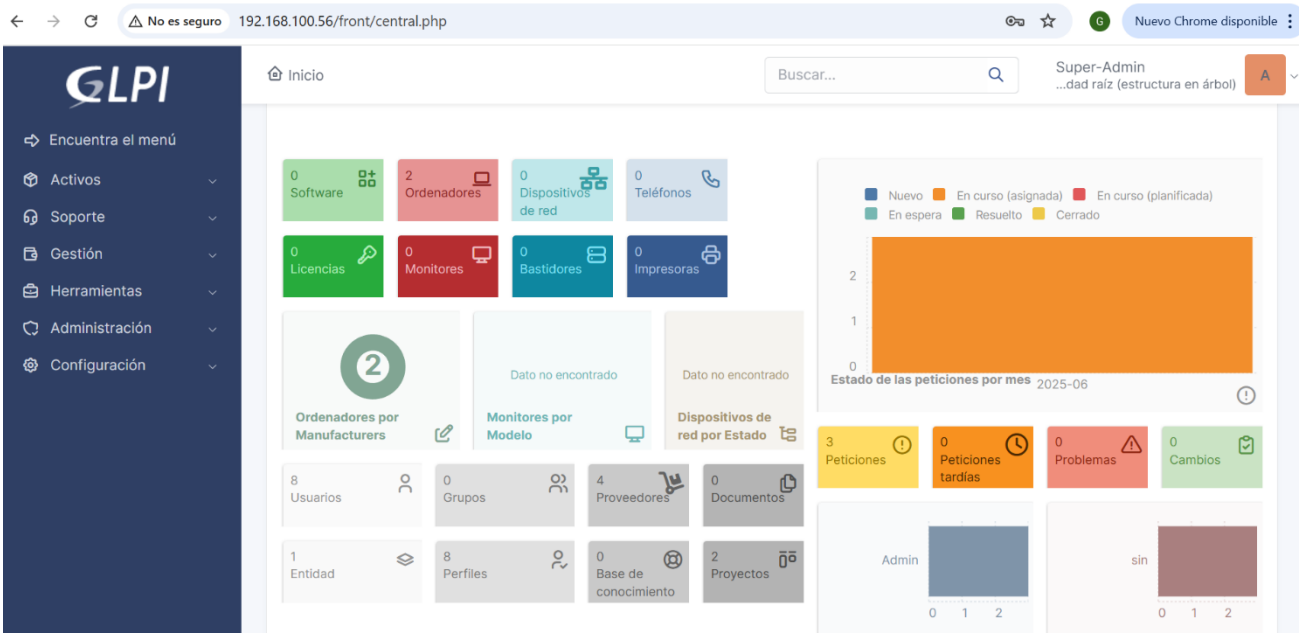
Instalación de GLPI

Nota: Se despliega la instalación de GLPI

Al culminar la instalación, se ingresa al aplicativo usando la URL: http://192.168.100.56/glpi y se puede navegar por las opciones disponibles.

Figura 22

Consola de GLPI

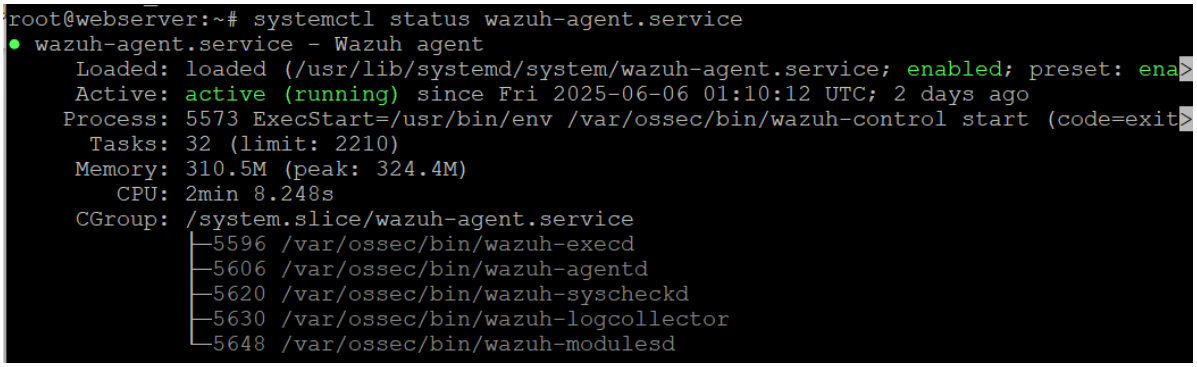


- **Instalación y configuración de Wazuh-agent**

Para instalar el agente, se realiza la instalación del paquete wazuh-agent, una vez instalado se verifica el estado del servicio.

Figura 23

Estado del agente



Nota: Wazuh-agent activo posterior a la instalación

Para que el agente se registre en el servidor de Wazuh, se edita el campo server – address en el archivo /var/ossec/etc/ossec.conf

Figura 24

Configuración de Wazuh-agent

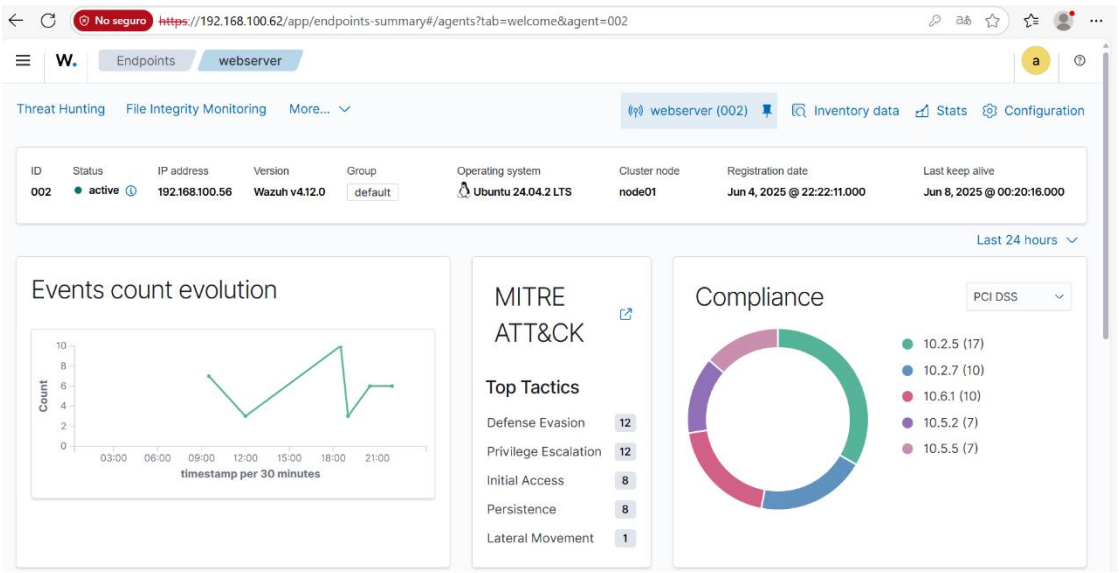
```
<!--
  Wazuh - Agent - Default configuration for ubuntu 24.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>192.168.100.62</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>ubuntu, ubuntu24, ubuntu24.04</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <client_buffer>
    <!-- Agent buffer options -->
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>
```

Nota: Mapeo a Wazuh Manager

En la consola de Wazuh, se encuentra registrado el servidor Web, en la opción Agents Management

Figura 255

Agente registrado en Wazuh



Nota: Se muestran las alertas recibidas por el agente

Para generar alertas del servicio Web y la base de datos, se deben añadir las secciones al archivo de configuración.

Figura 26

Registro de logs de Apache y MySQL

```
<localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/error.log</location>
  </localfile>

<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/error.log</location>
</localfile>


<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/mysql/error.log</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/mysql/mysql.log</location>
</localfile>
```

Nota: Sección de logs de apache y mysql

En la consola de Wazuh Manager, se registran eventos correspondientes a Apache

Figura 27

Alertas de Apache en Wazuh

Nota: Se visualiza que la alerta generada corresponde al código 400

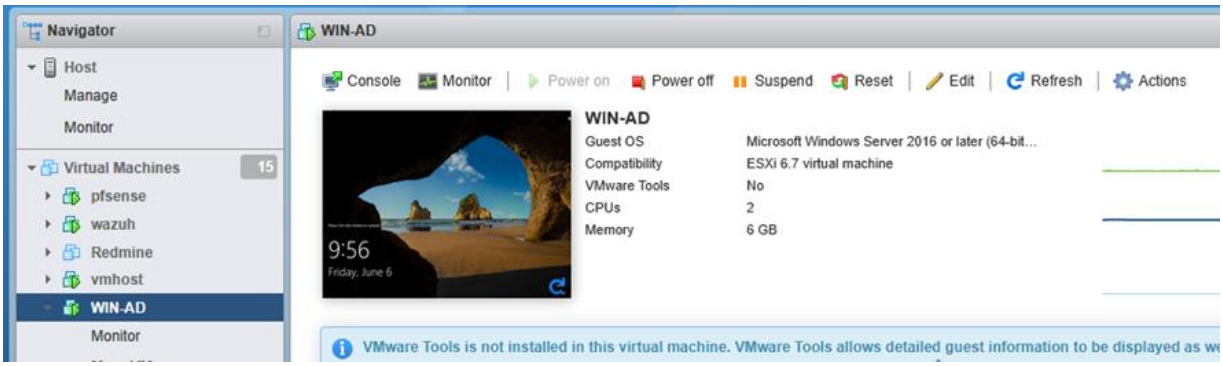
3.1.3 Instalación Servidor Active Directory

Como parte de la infraestructura se instala un servidor de Active directory el mismos que alojara los usuarios y computadores que serán ingresados al dominio.

Creamos el servidor de Active Directory (WIN-AD) sobre el virtualizador VmWare

Figura 28

Máquina virtual Windows 2022

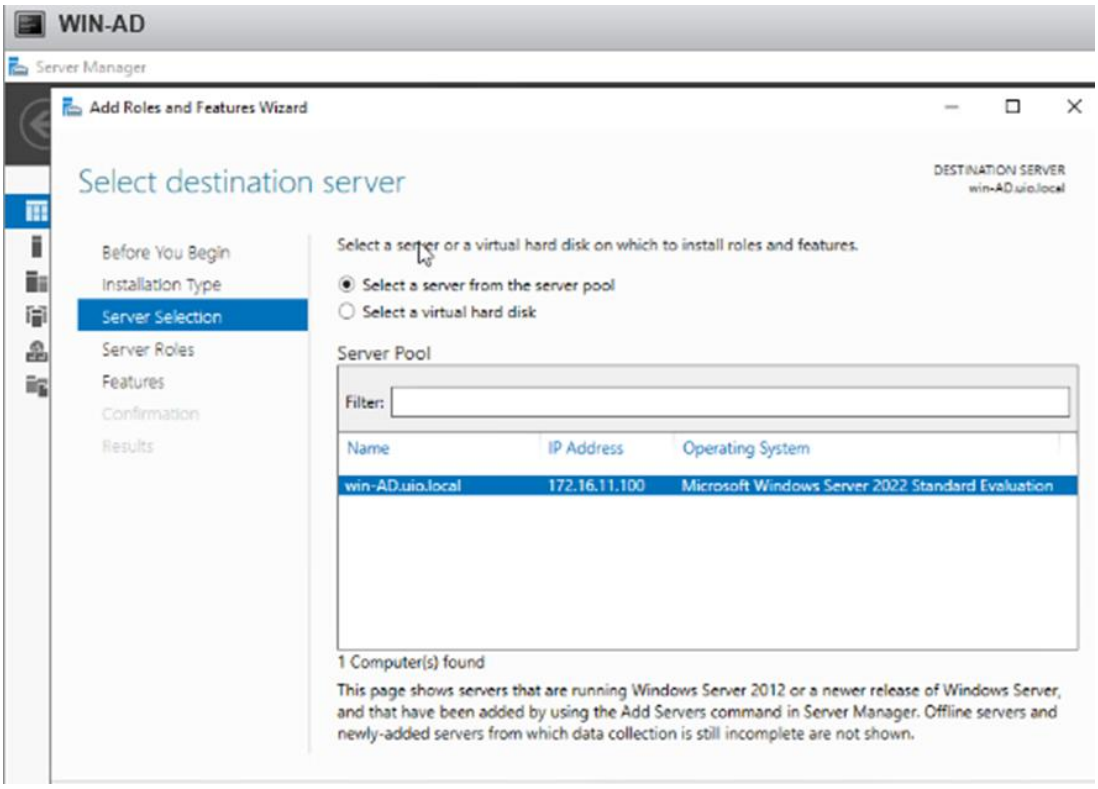


Nota: Creación de máquina virtual windows 2022 (el virtualizador muestra 2016 versión antigua de vmware)

Procedemos a instalar el rol de active directory en el servidor windows server 2022

Figura 29

Roles Windows 2022

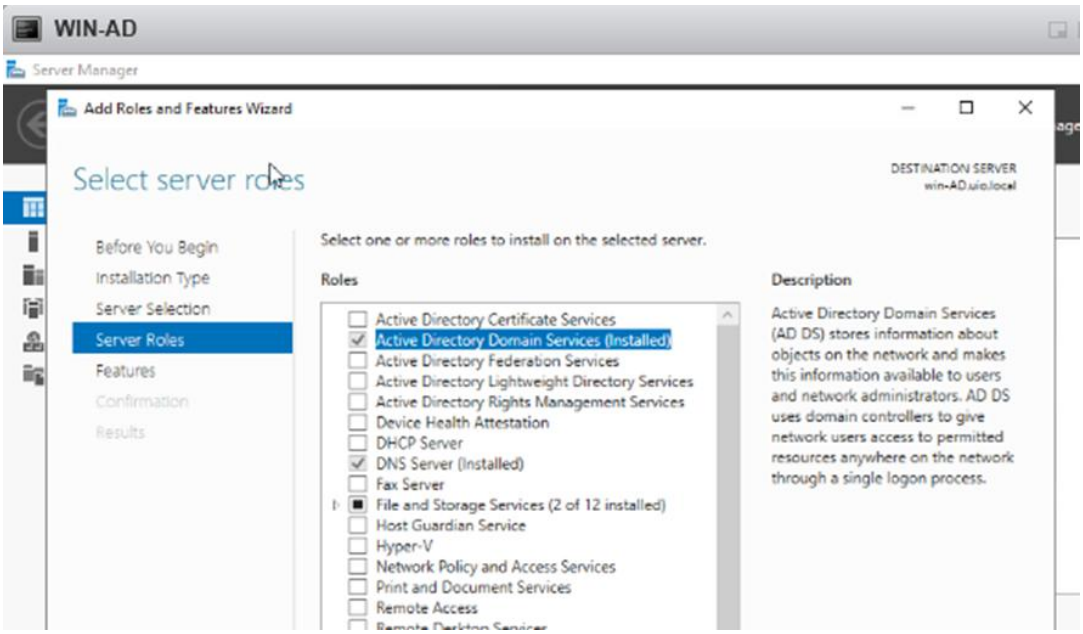


Nota: Se muestra sobre el servidor a instalar

Activamos el servicio de Active Directory para la instalación (Active Directory Domain Services)

Figura 30

AD Domain Services

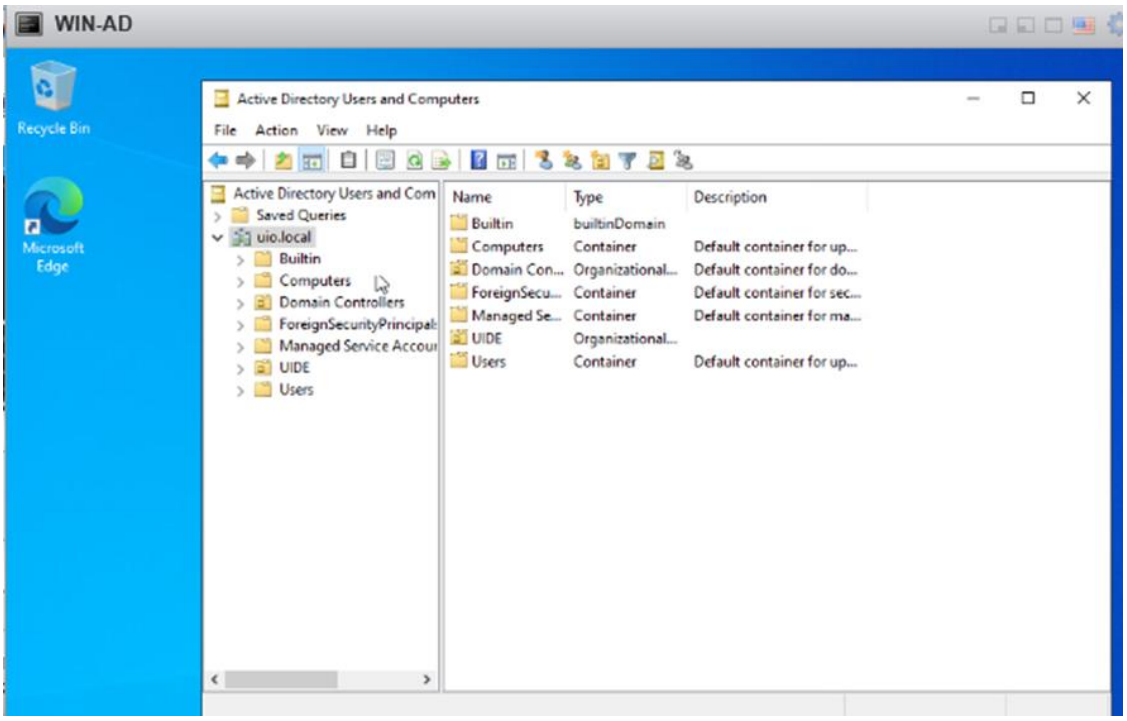


Nota: Rol para active directory domain services

Finalizada la instalación tenemos listo el servidor de active directory para utilizarlo y proceder con los siguientes pasos.

Figura 31

AD Domain Services

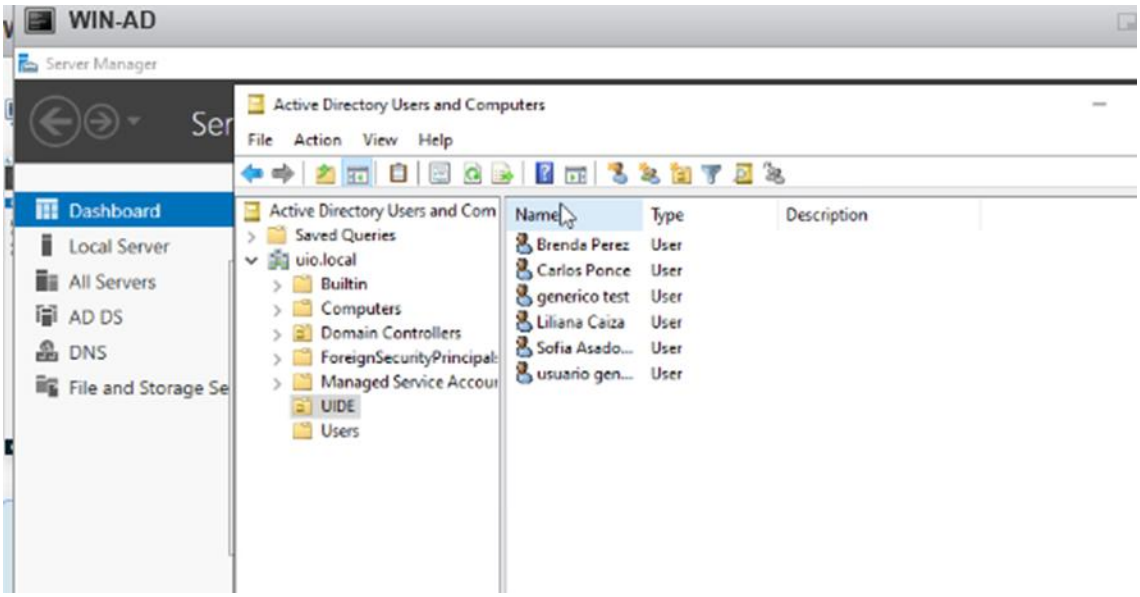


Nota: Servidor de active directory creado

Procedemos a crear los usuarios en el active directory sobre un grupo UIDE creado previamente para diferenciar de los grupos creados por defecto.

Figura 322

Usuarios

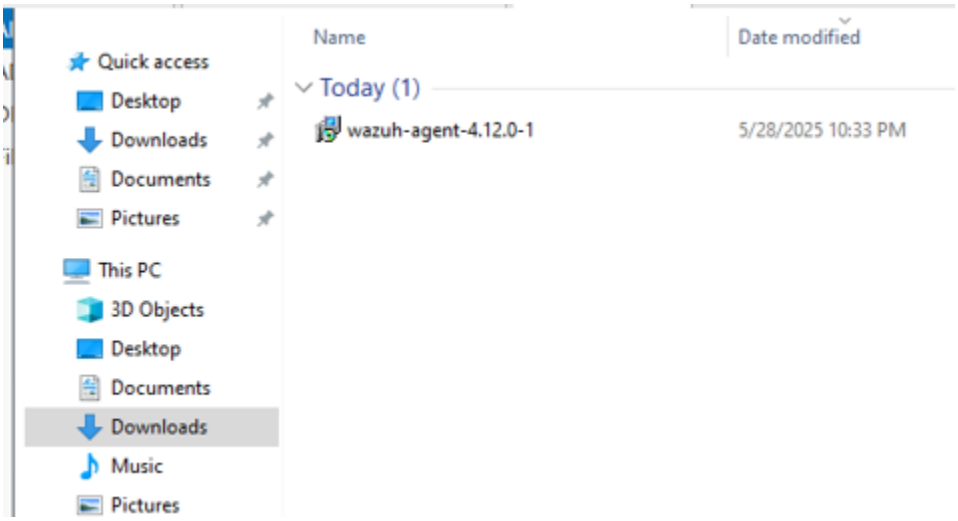


Nota: Usuarios creados en el grupo UIDE

Procedemos con la instalación del agente de wazuh sobre el servidor windows server 2022, descargamos el instalador del agente.

Figura 33

Agente de instalación

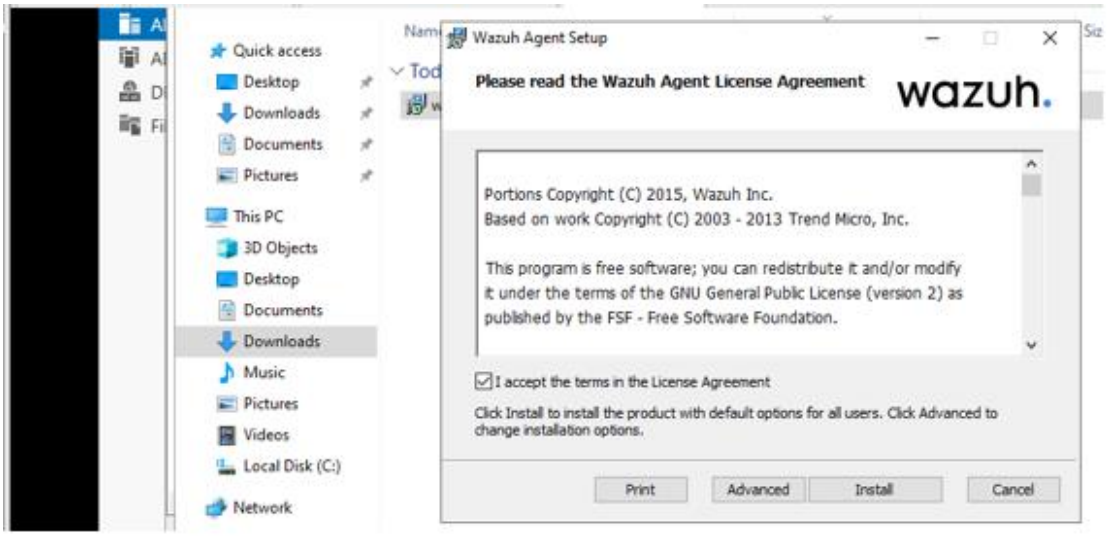


Nota: Descarga de agente wazuh

Ejecutamos el instalador del agente descargado

Figura 34

Agente de instalación

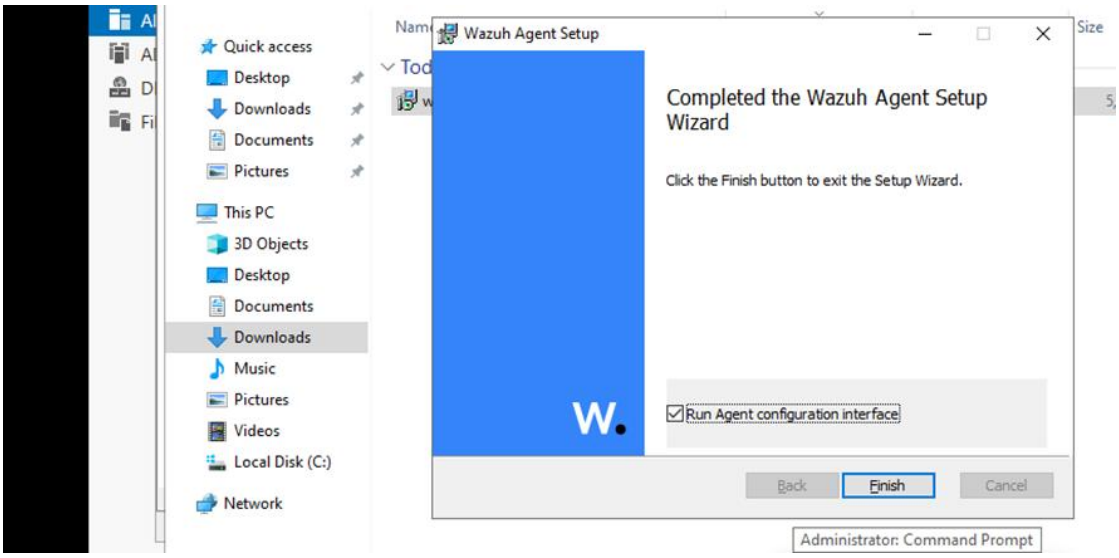


Nota: Asistente de instalación agente wazuh

Finalizada la instalación marcamos la opción de Run Agent configuration Interfaz para activar el agente.

Figura 35

Finaliza instalación

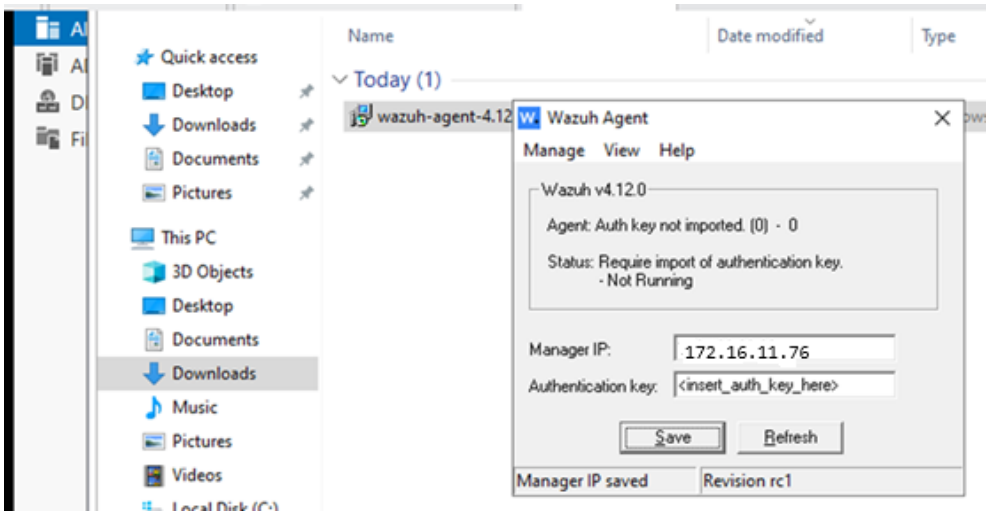


Nota: Finaliza la instalación y activamos el agente

Finalizada la instalación se inicia la ventana configurar el apuntamiento al servidor de wazuh

Figura 36

Finaliza instalación

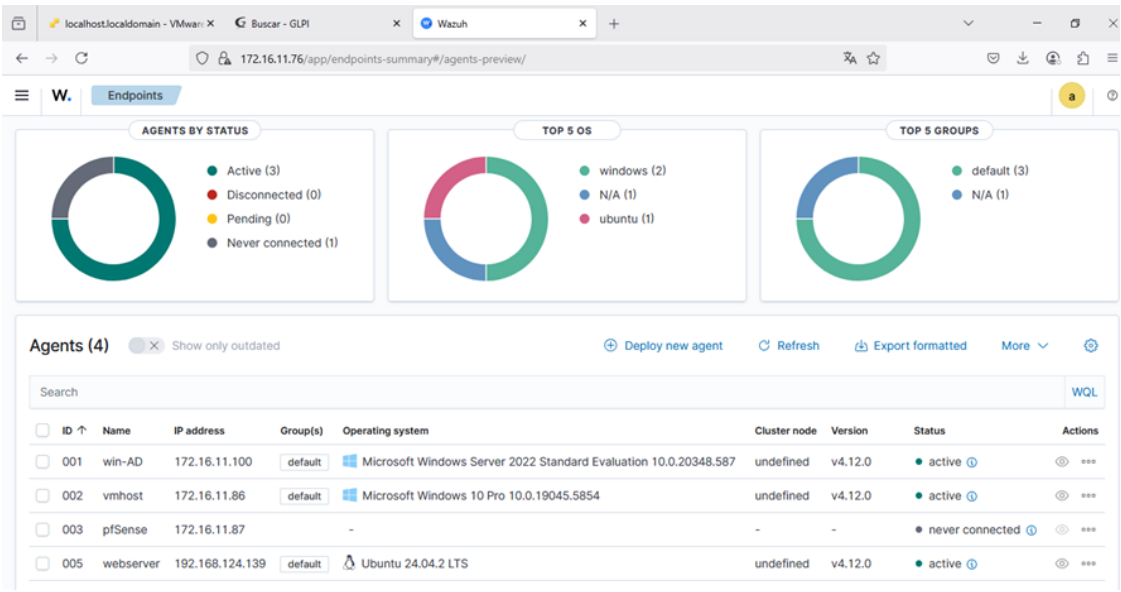


Nota: Apuntamiento del agente al servidor de wazuh

Realizada la configuración del agente procedemos a visualizar en la consola web de wazu y automáticamente se encuentra ya disponible el servidor de active directory.

Figura 37

Agentes



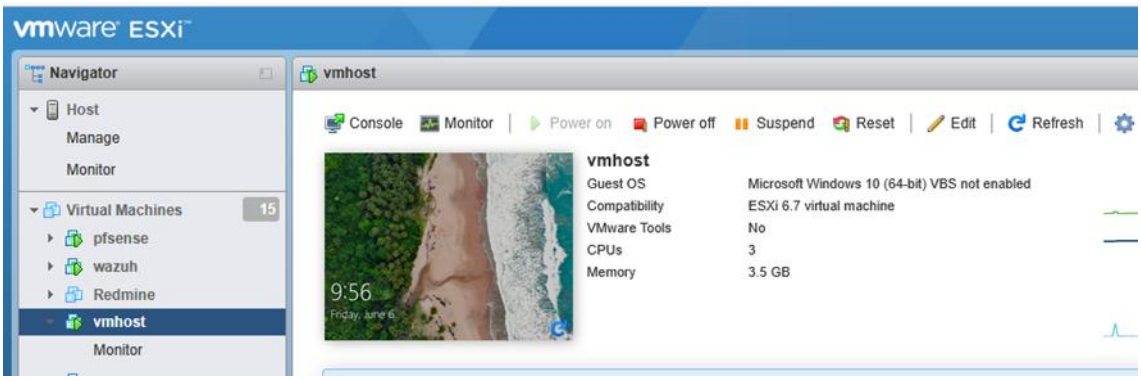
Nota: Agentes instalados y reconocidos por wazuh

3.1.4 Instalación host windows.

Se instala un host con windows 10 que simula a un terminal de usuario final, la misma esta sobre nuestra infraestructura VmWare.

Figura 38

Máquina virtual host

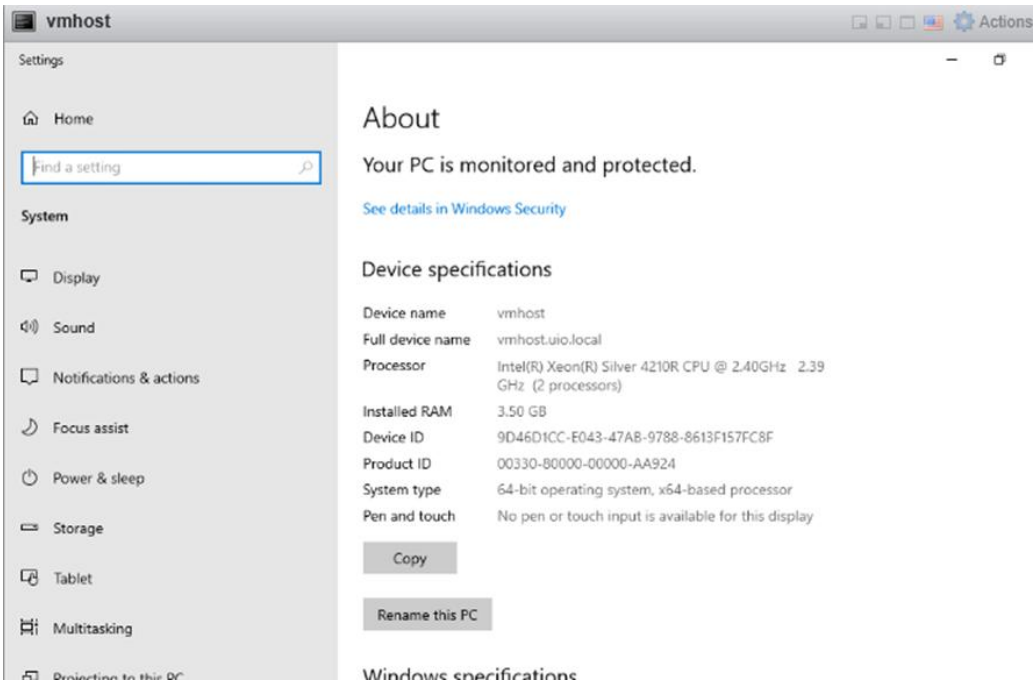


Nota: Creación de máquina virtual windows 10

Posterior a la instalación del sistema operativo, procedemos a agregar al dominio a la máquina virtual.

Figura 39

Host en dominio

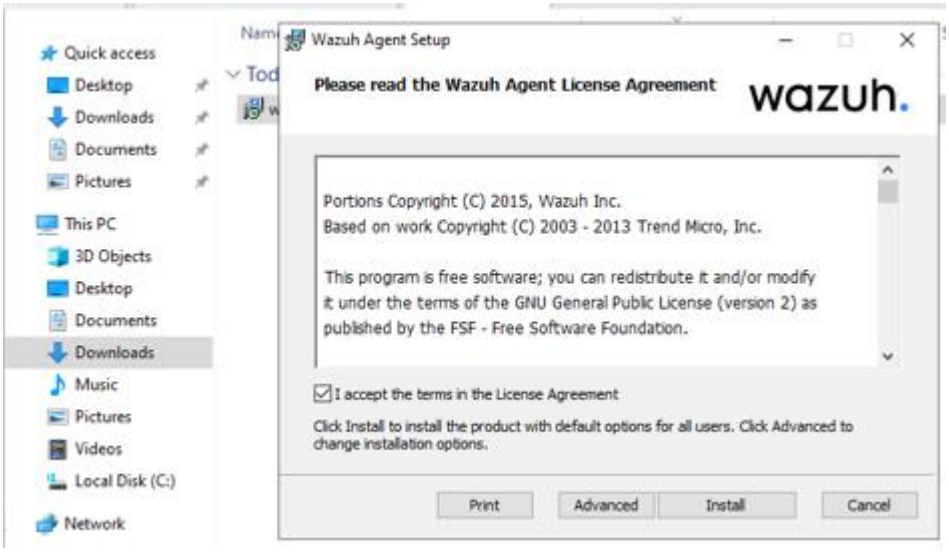


Nota: Muestra que el equipo fue Ingresado al dominio de host

Ingresado al dominio procedemos a instalar el agente de wazuh similar al procedimiento realizado con el servidor de active directory, ejecutamos el paquete del agente y nos muestra el asistente de instalación.

Figura 40

Agente de instalación

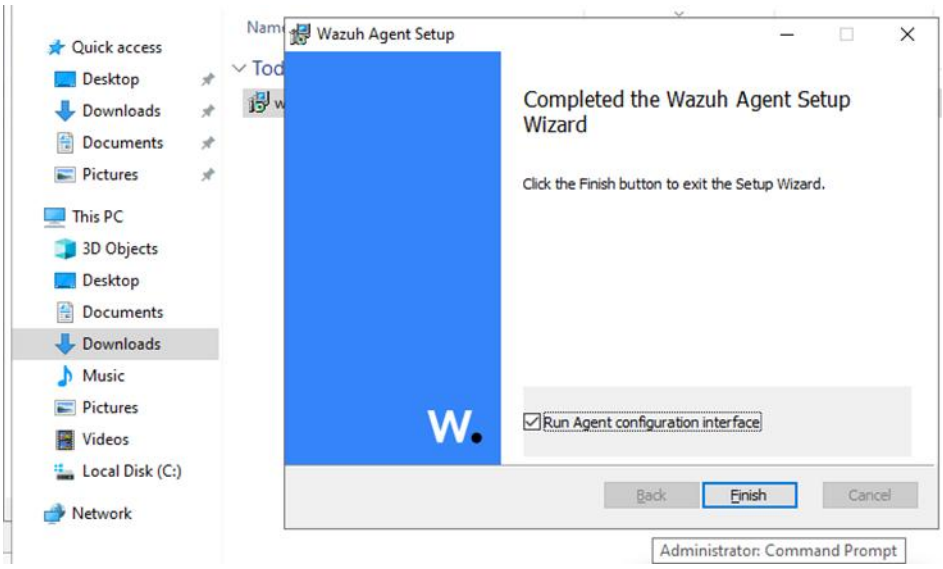


Nota: Asistente de instalación agente wazuh

Una vez finalizada la instalación marcamos el check de la opción de Run Agent configuration Interfaz para activar el agente.

Figura 41

Finaliza instalación agente wazuh en host

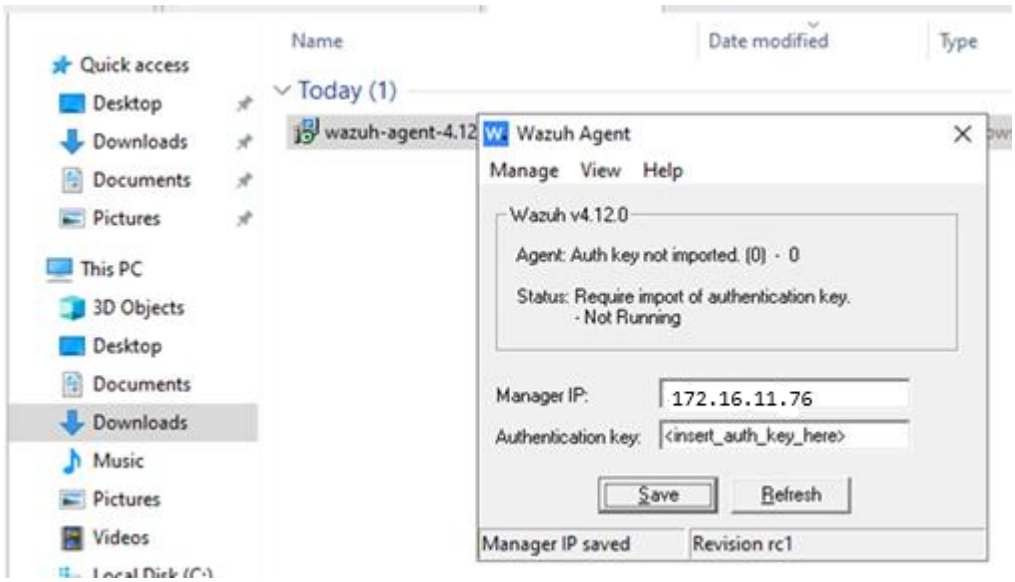


Nota: Finaliza la instalación y activamos el agente en el equipo host

Finalizada la instalación se inicia la ventana configurar el apuntamiento al servidor de wazuh en el equipo host

Figura 42

Finaliza instalación

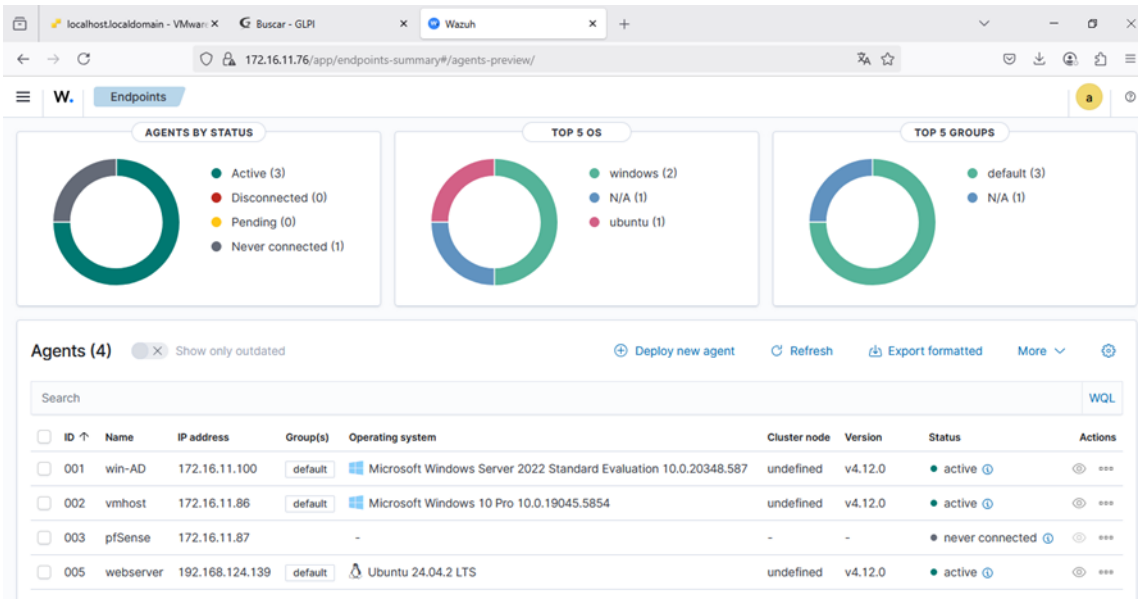


Nota: Apuntamiento del agente al servidor de wazuh

Realizada la configuración del agente procedemos a visualizar en la consola web de wazu y automáticamente se encuentra ya disponible el servidor de active directory.

Figura 43

Agente host



Nota: Agentes en el host instalado y reconocido por wazuh

3.1.5 Configuración envio de notiifcaciones via mail

Como parte de la implementación es él envió de notificaciones de las alertas generadas en wazuh vía mail, para la cual procedemos a configurar el propio servidor de wazuh como SMTP.

Instalamos postfix en el servidor de wazuh para la cual ejecutamos el comando adjunto

Figura 44

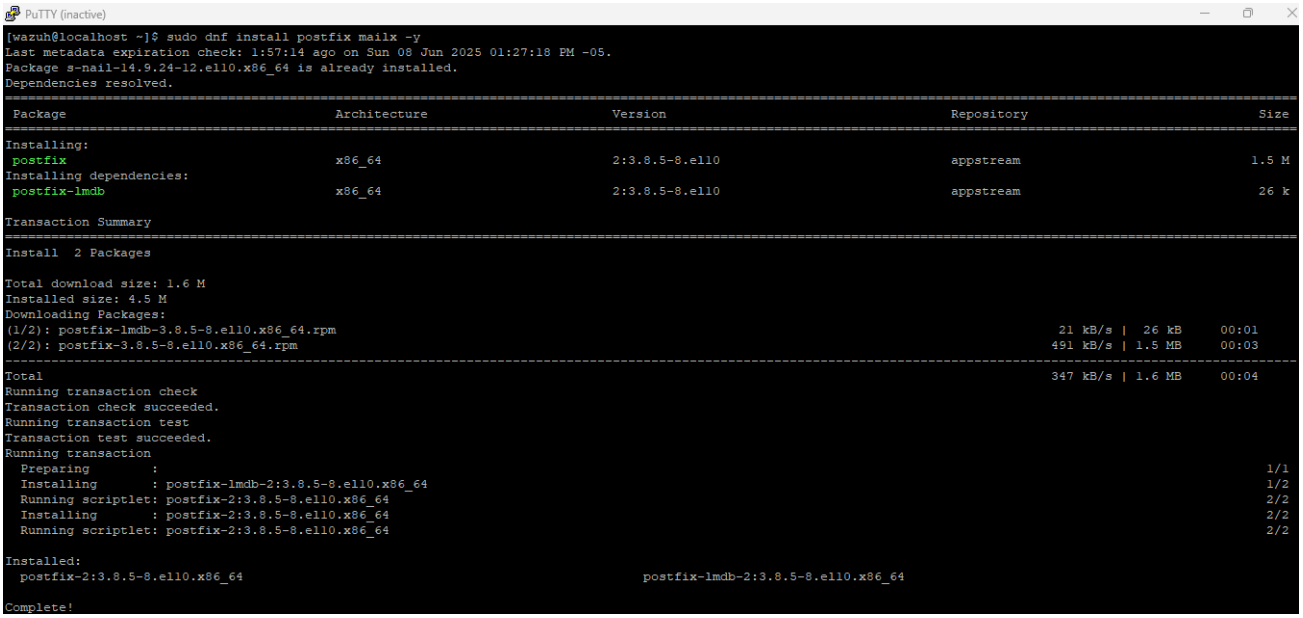
Comando instalación postfix

```
sudo dnf install postfix –y
```

Nota: Ejecución de la instalación postfix

Figura 45

Instalación Postfix



Nota: Instalación completa de postfix sobre el server de wazuh

Procedemos a configurar el servicio de postfix para el envío de correos para la cual editamos el archivo de configuración adjunto:

/etc/postfix/main.cf

Agregamos las líneas adjuntas al final del documento

Figura 46

Configuración Postfix

```
# Use TLS if this is supported by the remote SMTP server, otherwise use
# plaintext (opportunistic TLS outbound).
#
smtp_tls_security_level = may

default_database_type = lmdb
meta_directory = /etc/postfix
shlib_directory = /usr/lib64/postfix


relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
```

Nota: Archivo de configuración postfix para envio de correo

Creamos el archivo con las credenciales para la autenticación para gmail, editamos el archivo /etc/postfix/sasl_passwd y agregamos la entrada adjunta con las credenciales correctas:

[smtp.gmail.com]:587 correo@gmail.com:password

Figura 47

Credenciales correo

```
[wazuh@localhost log]$ sudo cat /etc/postfix/sasl_passwd
[sudo] password for wazuh:
[smtp.gmail.com]:587 c[illegible]nce@gmail.com:x[illegible]
[wazuh@localhost log]$
```

Nota: Archivo de configuración con credenciales para envió de correo

Reiniciamos el servicio de postfix

sudo systemctl restart postfix

Se procede a configurar wazuh para el envio de correos usando la herramienta postfix instalada en el paso anterior, editamos el archivo /var/ossec/etc/ossec.conf y agregamos las entradas adjuntas

Figura 48

Configuración envío de correo

```
<global>
  <email_notification>yes</email_notification>
  <email_to>carlitoshponce@gmail.com</email_to>
  <email_from>carlitoshponce@gmail.com </email_from>
  <smtp_server>localhost</smtp_server>
</global>

<alerts>
  <email_alerts>yes</email_alerts>
  <email_alert_level>10</email_alert_level>
</alerts>
```

Nota: Archivo de configuración para envió de correo

En donde definimos el nivel de severidad para las alertas para que se envíen las notificaciones vía correo, en nuestro caso el nivel configurado es 10, es decir enviara notificaciones desde el nivel 10 al 15.

Tabla 2

Niveles de alerta wazuh

Nivel	Severidad	Ejemplo
0-3	Informativo	Acceso exitoso, cambios normales
4-7	Advertencia	Fallos menores, intentos de escaneo
8-10	Alerta	Comportamiento sospechoso o moderado
11-15	Crítico	Acceso no autorizado, malware, exploits

Nota: Muestra los diferentes niveles de alerta Wazuh. Wazuh, Inc. (2024)

CAPÍTULO 4

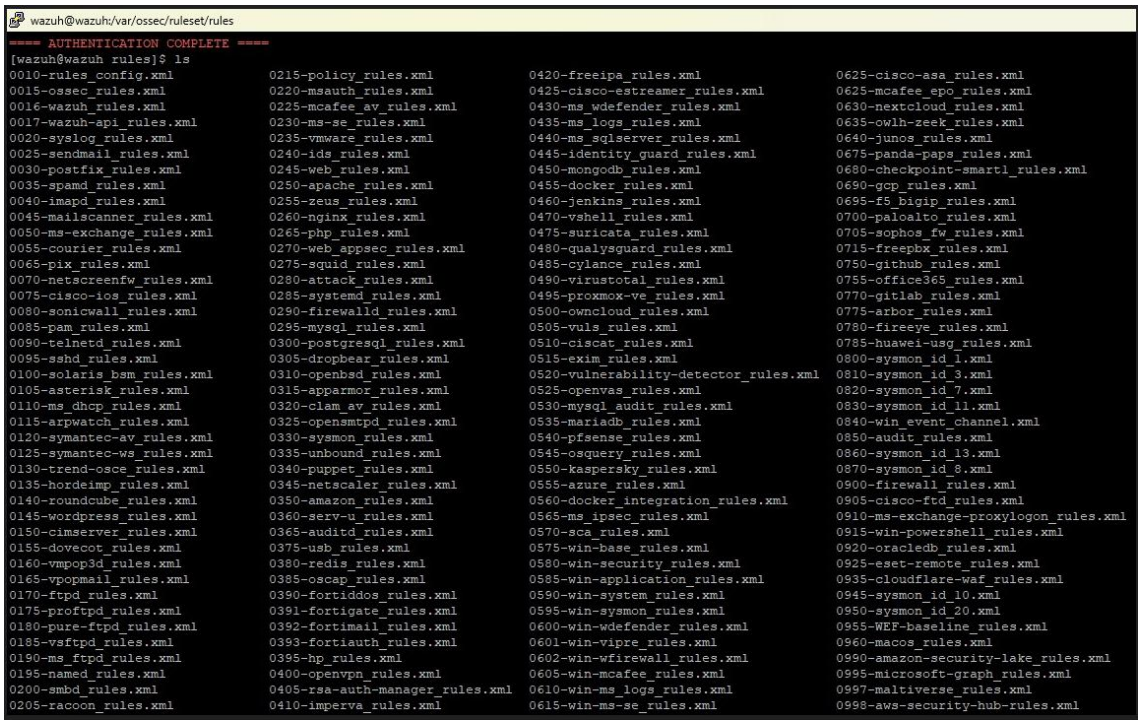
4. ANÁLISIS DE RESULTADOS

4.1. Pruebas de Concepto

Dentro de Wazuh, se tiene un catálogo de reglas de detección de amenaza. En la consola se encuentra en el path /var/ossec/ruleset/rules/. Dentro de las reglas por defecto se encuentran archivos .xml para diferentes plataformas como Windows, Linux, pfsense, firewalls, etc.

Figura 49

Path de reglas en Wazuh

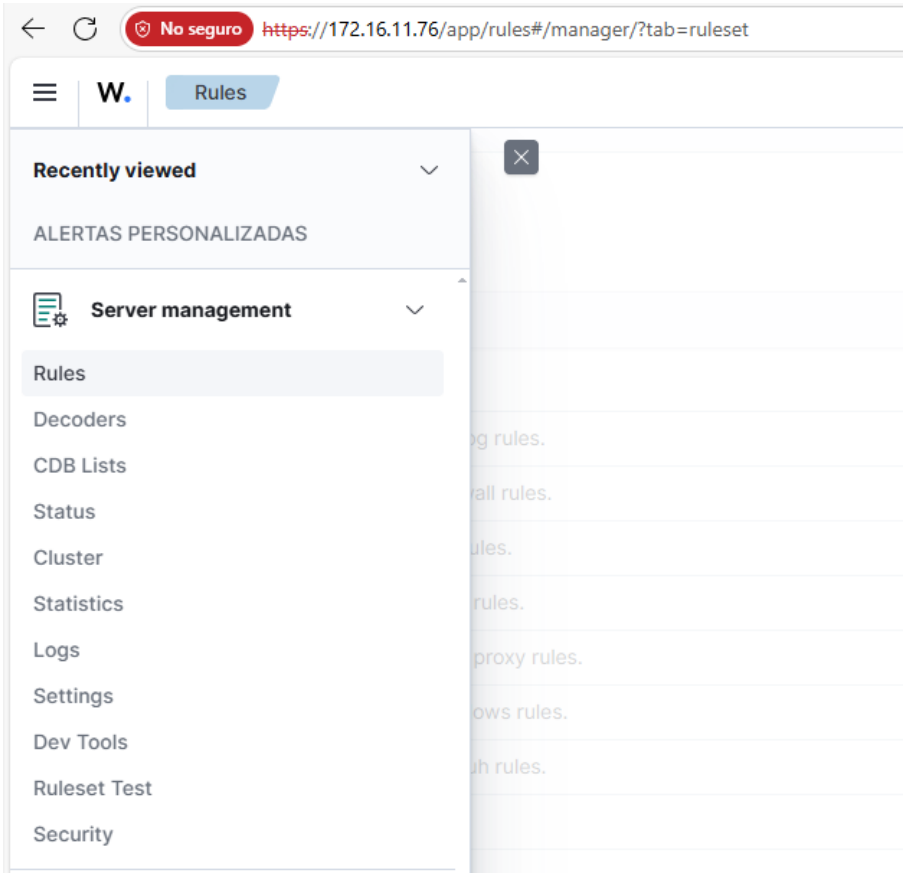


Nota: Imagen: Archivos de alertas predefinidas en la consola de Wazuh.

Para acceder desde la aplicación web se encuentra en Server Management → Rules.

Figura 50

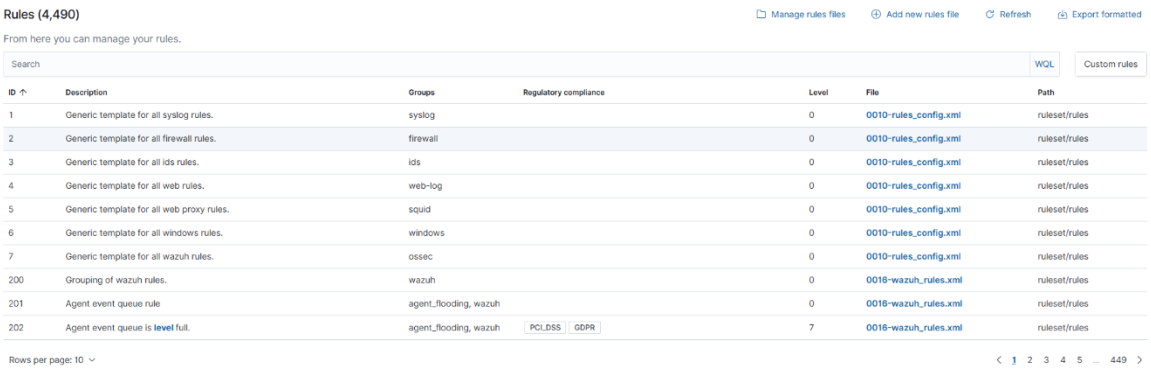
Server Management



Nota: Ingresos para el panel de alertas

Figura 51

Reglas en Wazuh

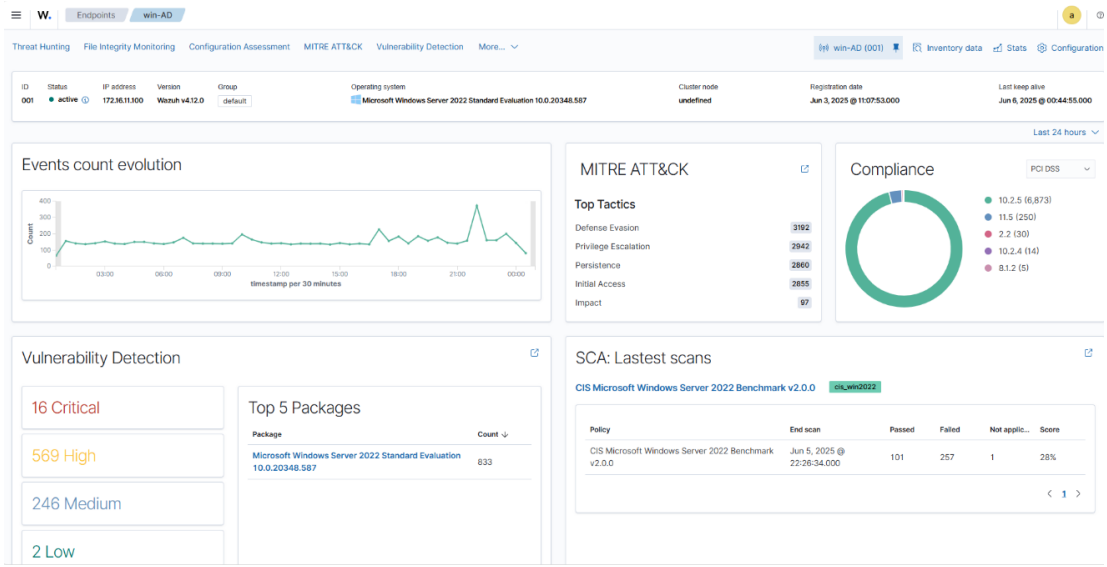


Nota: catálogo de reglas en Wazuh

Para tener una visión detallada sobre las alertas generadas en Wazuh se puede acceder al dispositivo en la opción de Endpoints, donde tendremos un dashboard sobre las métricas del equipo.

Figura 52

Dashboard de métricas por equipo

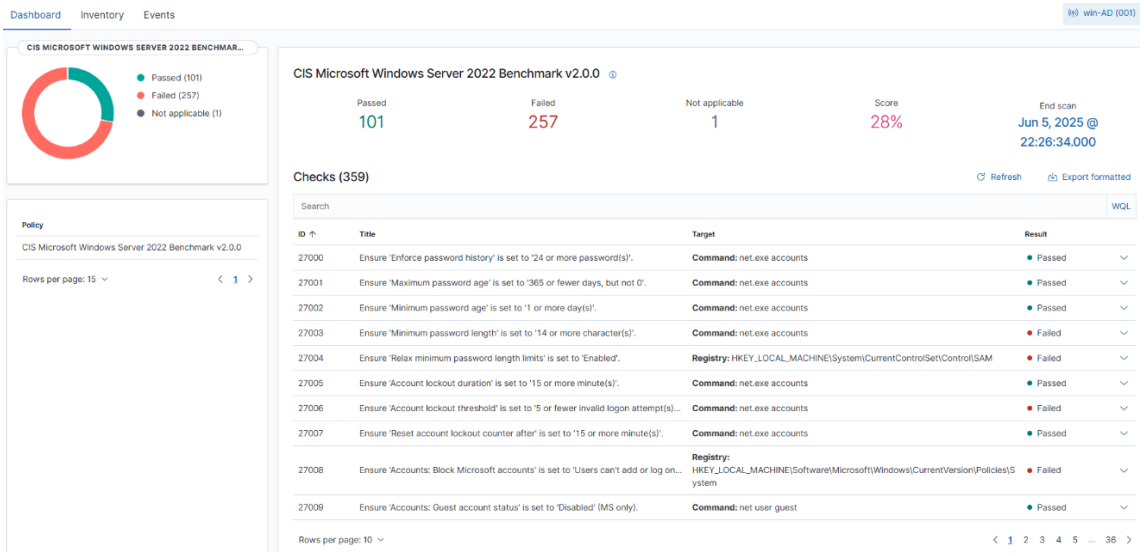


Nota: En el dashboard se puede determinar se tiene registros de la evolución de eventos, MITRE ATT&CK, detección de vulnerabilidades, entre otros.

Accedemos a la opción de SCA: Lastest scans para validar los eventos generados, en este caso

Figura 53

Dashboard de servidores, tareas y estados del equipo.



Nota: Muestra el panel principal de alertas de wazuh

Para realizar las pruebas de concepto se procede a realizar ataques desde una máquina atacante, en este caso se usa una MV instalado KALI.

Se pondrá a prueba los siguientes ataques:

- Ataque de Fuerza Bruta: Es usado para acceder a un sistema probando múltiples combinaciones de usuarios y contraseñas.
- Escaneo de puertos: Explora puertos abiertos en un sistema, con esta información se puede tratar de explotar vulnerabilidades.
- Ataque SQL: Se inyecta código SQL malicioso en aplicaciones web para la manipulación de base de datos y robar está información.
- Ataque DoS: El atacante trata de enviar múltiples peticiones con tráfico excesivo para que sea inaccesible.
- Ataque MAC Flood: Se inunda un switch con direcciones MAC falsas para sobrecargar el sistema y forzar actuar como un hub y poder interceptar tráfico de la red.

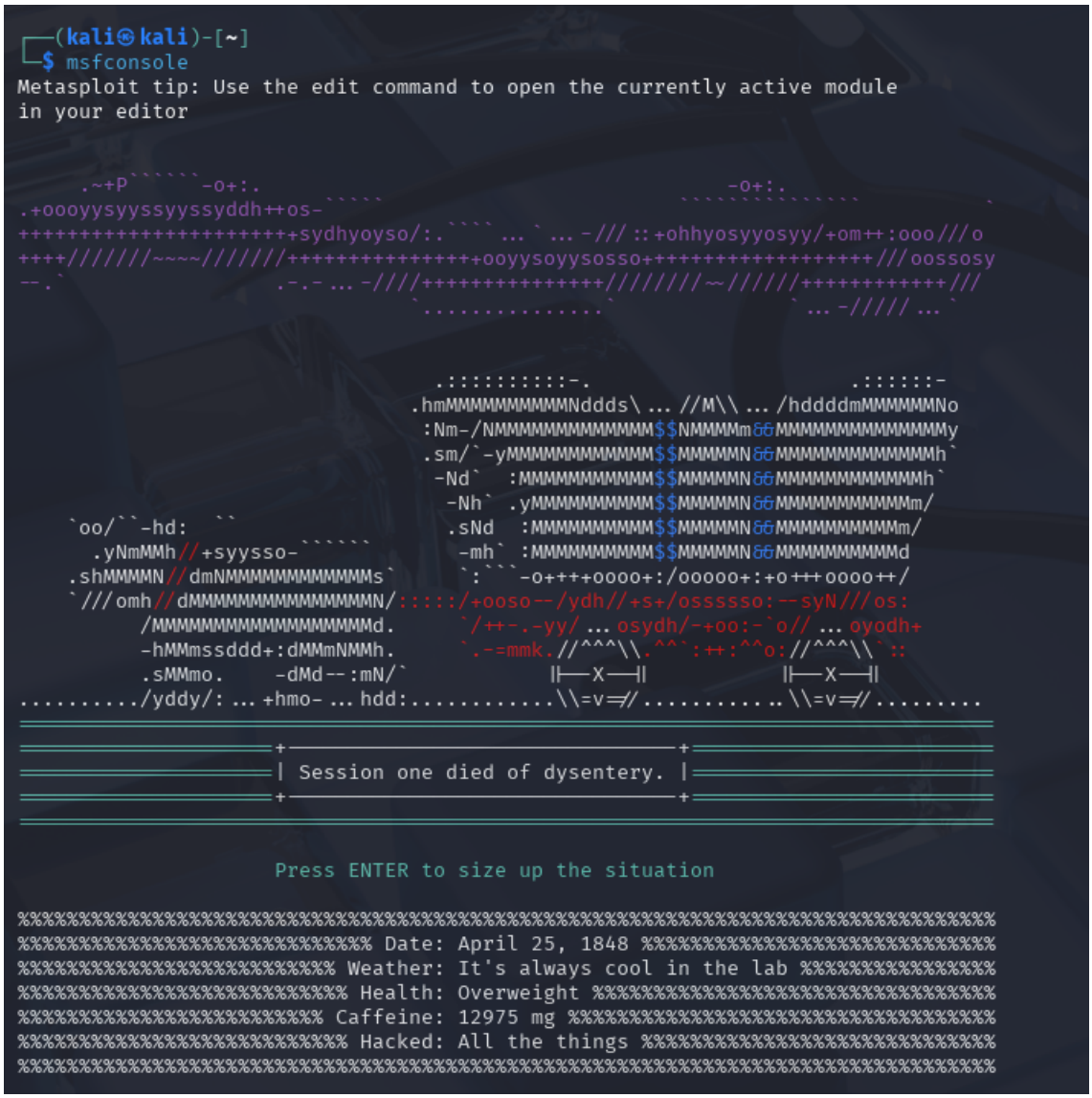
4.1.1. Ataque de Fuerza Bruta

Ejecución de ataques:

Para la ejecución del ataque de fuerza bruta se realizan mediante el uso de la herramienta de Metasploit que se encuentra instalada en la máquina atacante.

Figura 54

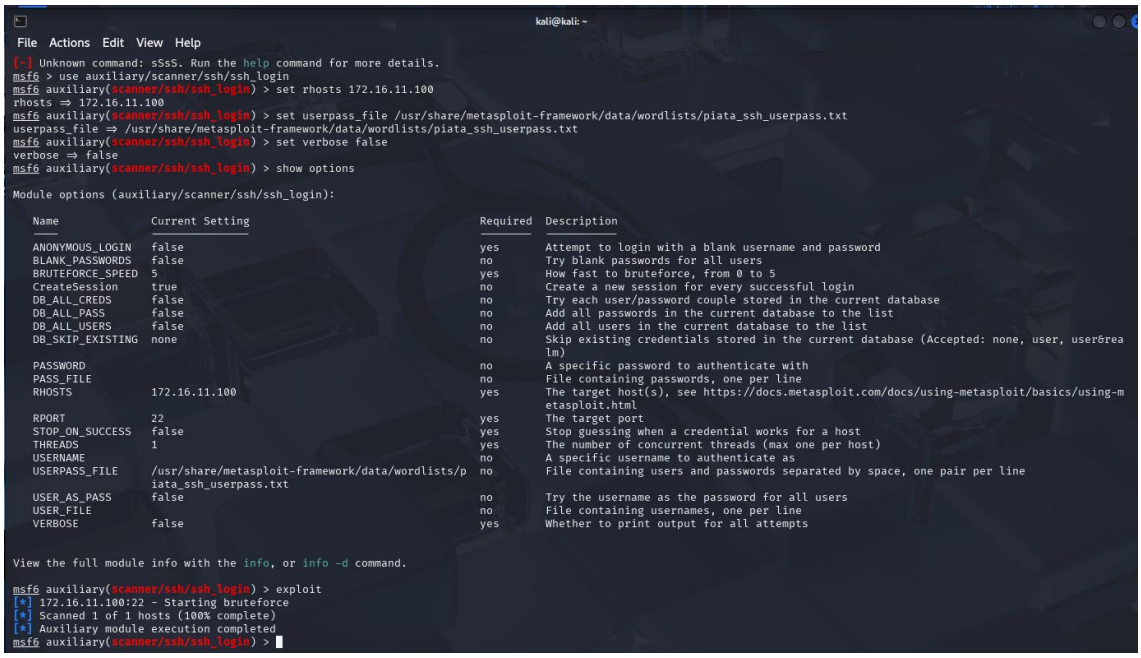
Herramienta Metasploit en KALI



Nota: Para ingresar a metasploit se debe ejecutar el comando msfconsole.

Figura 55

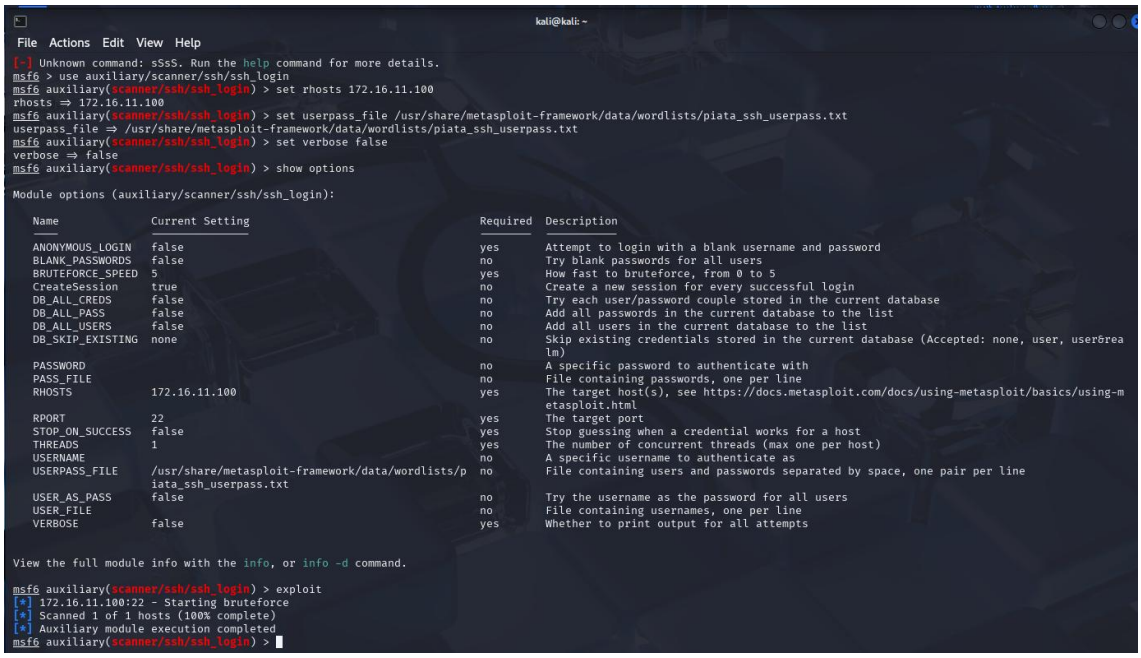
Proceso de ejecución de ataque de fuerza bruta con uso del protocolo SSH.



Nota: Ingreso al path scanner/ssh/ssh_login para realizar el ataque.

Figura 56

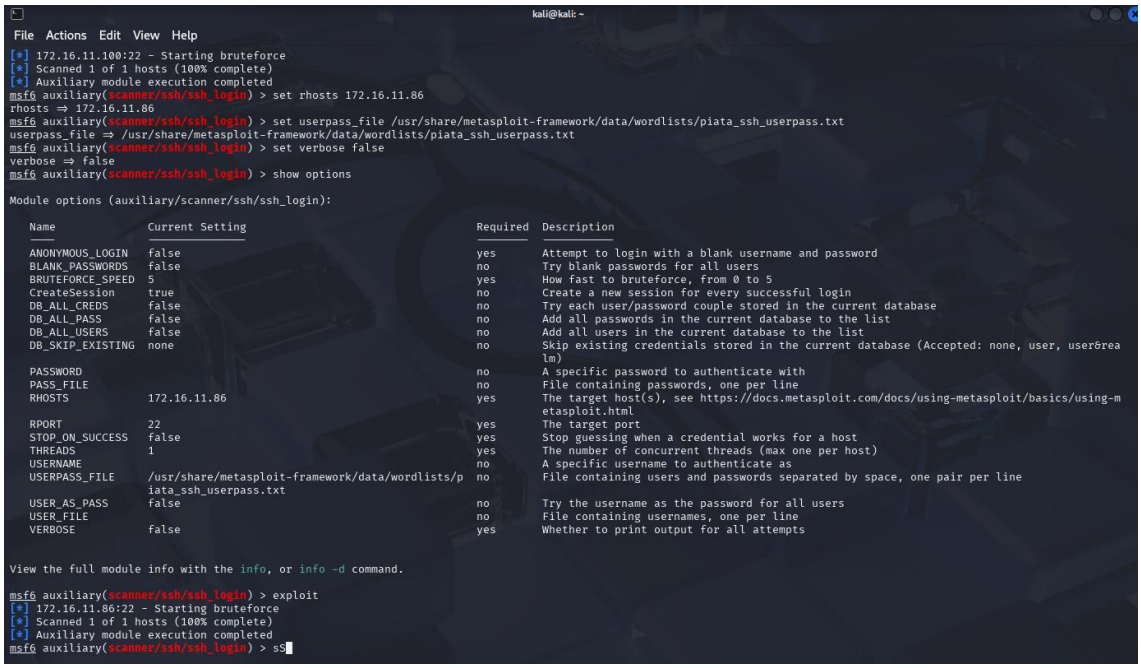
Ejecución de ataque de fuerza bruta hacia el AD (172.16.11.100)



Nota: Explotación del ataque.

Figura 57

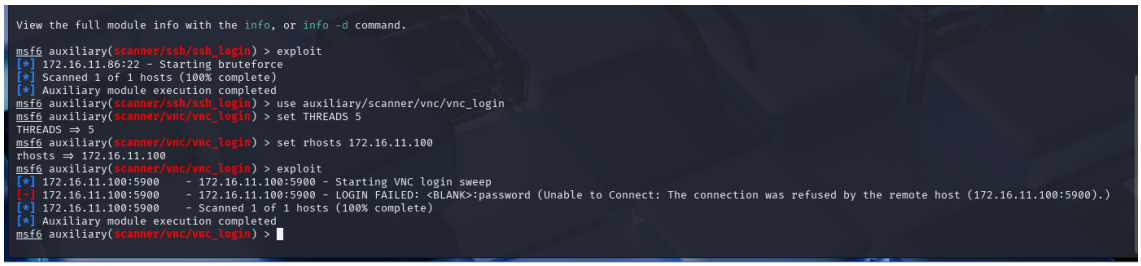
Ejecución del ataque de fuerza bruta hacia un HOST (172.16.11.86)



Nota: Ejecución del ataque en un host.

Figura 58

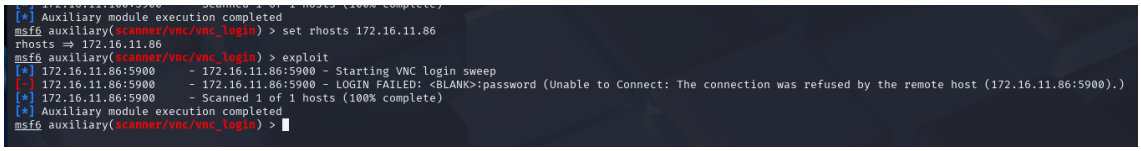
Ejecución de ataque de fuerza bruta VNC al AD



Nota: Para la ejecución del ataque se realiza en el path scanner/vnc/vnc_login.

Figura 59

Ejecución de ataque de fuerza bruta VNC al HOST



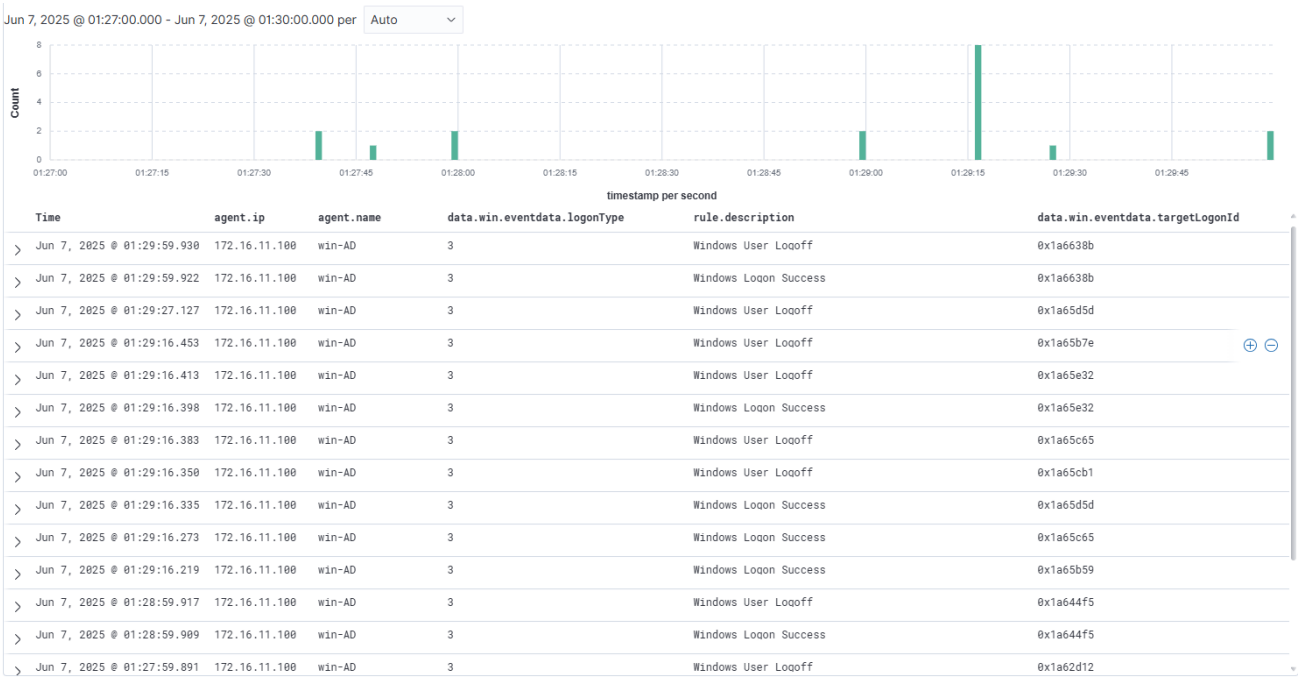
Nota: Ejecución de ataque de fuerza bruta

Resultados:

Las alertas que se genera en Wazuh son sobre inicios y cierres de sesión exitosos.

Figura 60

Alertas generadas en Wazuh

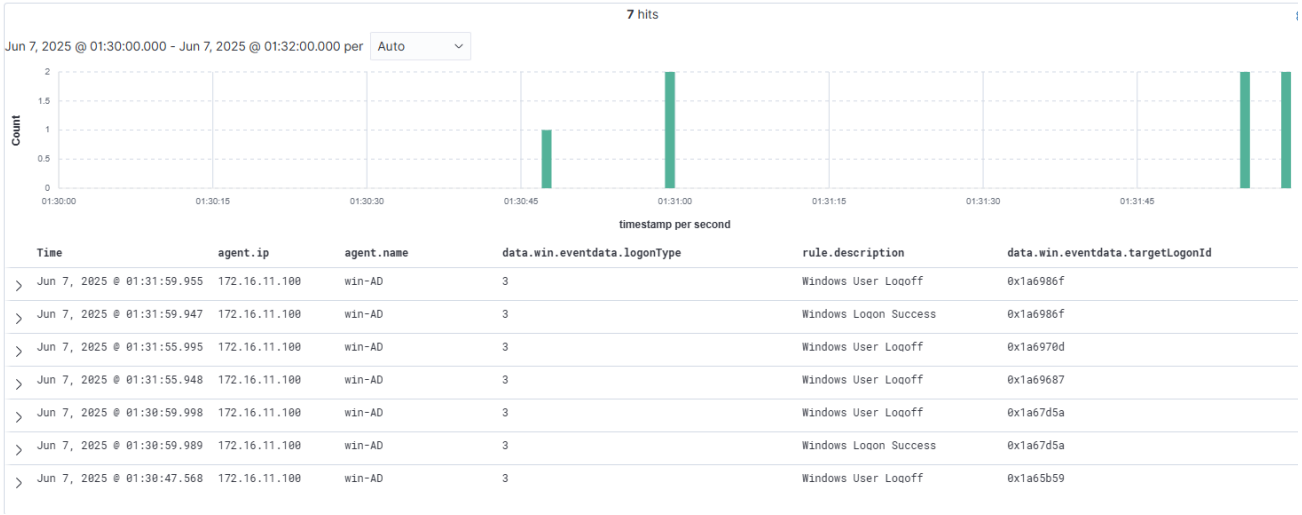


Time	agent.ip	agent.name	data.win.eventdata.logonType	rule.description	data.win.eventdata.targetLogonId
Jun 7, 2025 @ 01:29:59.930	172.16.11.100	win-AD	3	Windows User Logoff	0x1a6638b
Jun 7, 2025 @ 01:29:59.922	172.16.11.100	win-AD	3	Windows Logon Success	0x1a6638b
Jun 7, 2025 @ 01:29:27.127	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65d5d
Jun 7, 2025 @ 01:29:16.453	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65b7e
Jun 7, 2025 @ 01:29:16.413	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65e32
Jun 7, 2025 @ 01:29:16.398	172.16.11.100	win-AD	3	Windows Logon Success	0x1a65e32
Jun 7, 2025 @ 01:29:16.383	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65c65
Jun 7, 2025 @ 01:29:16.350	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65cb1
Jun 7, 2025 @ 01:29:16.335	172.16.11.100	win-AD	3	Windows Logon Success	0x1a65d5d
Jun 7, 2025 @ 01:29:16.273	172.16.11.100	win-AD	3	Windows Logon Success	0x1a65c65
Jun 7, 2025 @ 01:29:16.219	172.16.11.100	win-AD	3	Windows Logon Success	0x1a65b59
Jun 7, 2025 @ 01:28:59.917	172.16.11.100	win-AD	3	Windows User Logoff	0x1a644f5
Jun 7, 2025 @ 01:28:59.909	172.16.11.100	win-AD	3	Windows Logon Success	0x1a644f5
Jun 7, 2025 @ 01:27:59.891	172.16.11.100	win-AD	3	Windows User Logoff	0x1a62d12

Nota: Alertas generadas en Wazuh del ataque de fuerza bruta.

Figura 61

Alertas generadas en Wazuh, ataque de fuerza bruta VNC



Time	agent.ip	agent.name	data.win.eventdata.logonType	rule.description	data.win.eventdata.targetLogonId
Jun 7, 2025 @ 01:31:59.955	172.16.11.100	win-AD	3	Windows User Logoff	0x1a6986f
Jun 7, 2025 @ 01:31:59.947	172.16.11.100	win-AD	3	Windows Logon Success	0x1a6986f
Jun 7, 2025 @ 01:31:55.995	172.16.11.100	win-AD	3	Windows User Logoff	0x1a6970d
Jun 7, 2025 @ 01:31:55.948	172.16.11.100	win-AD	3	Windows User Logoff	0x1a69687
Jun 7, 2025 @ 01:30:59.998	172.16.11.100	win-AD	3	Windows User Logoff	0x1a67d5a
Jun 7, 2025 @ 01:30:59.989	172.16.11.100	win-AD	3	Windows Logon Success	0x1a67d5a
Jun 7, 2025 @ 01:30:47.568	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65b59

Nota: Alertas generadas en Wazuh del ataque de fuerza bruta VNC.

4.1.2 Escaneo de puertos

Ejecución de ataques:

Figura 62

Ejecución de ataque de escaneo de puertos con nmap.

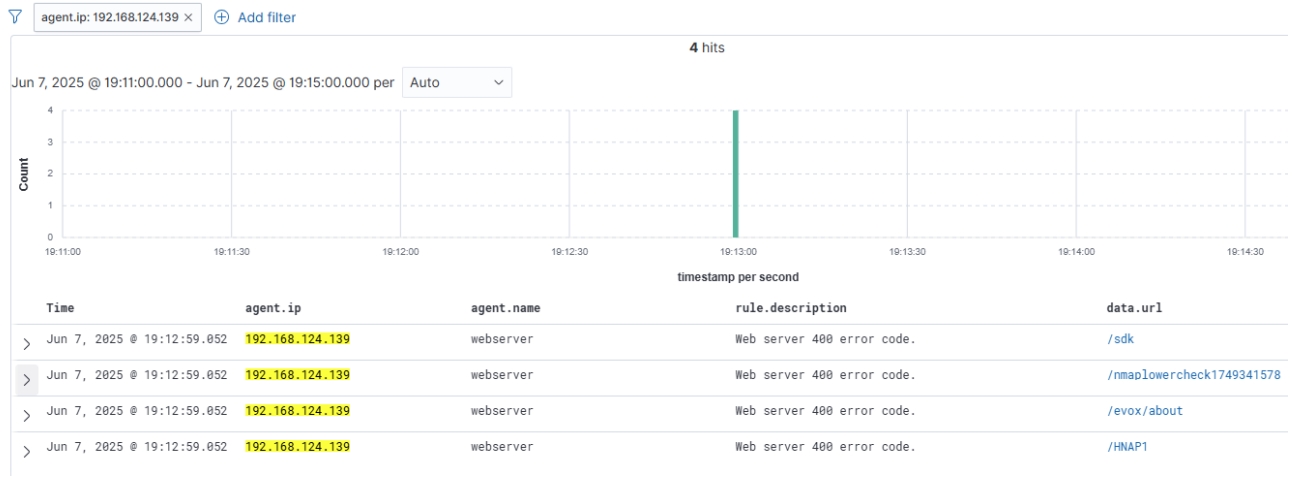
```
msf6 > nmap -sV 192.168.124.139 -p 80
[*] exec: nmap -sV 192.168.124.139 -p 80

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 20:12 EDT
Nmap scan report for 192.168.124.139
Host is up (0.00072s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
MAC Address: 00:0C:29:E4:94:53 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds
msf6 >
```

Nota: Ejecución de ataque hacia el servidor Web.

Resultados:

Figura 63

Alertas generadas en Wazuh



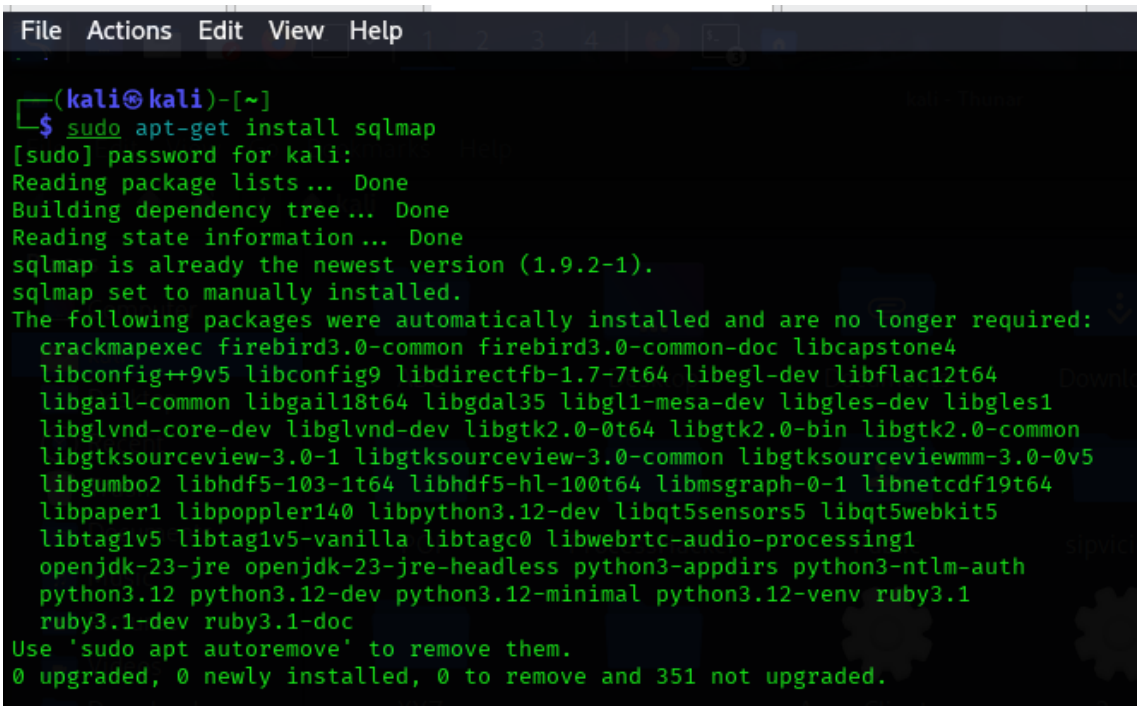
Nota: La regla generada es Web server 400 error code.

4.1.3. Ataque SQL

Ejecución de ataques:

Figura 64

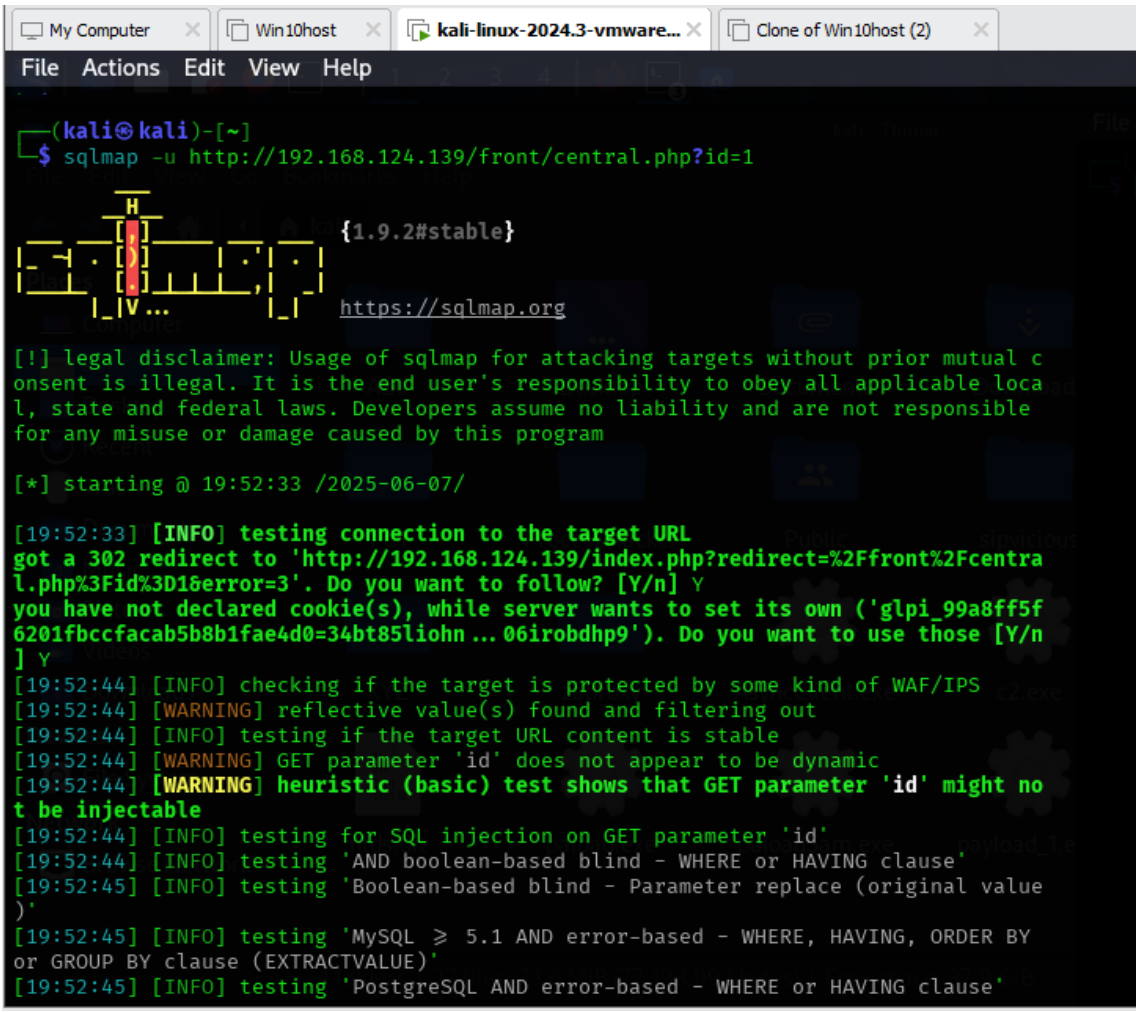
Instalación de SQLMAP



Nota: Instalación de la herramienta sqlmap.

Figura 65

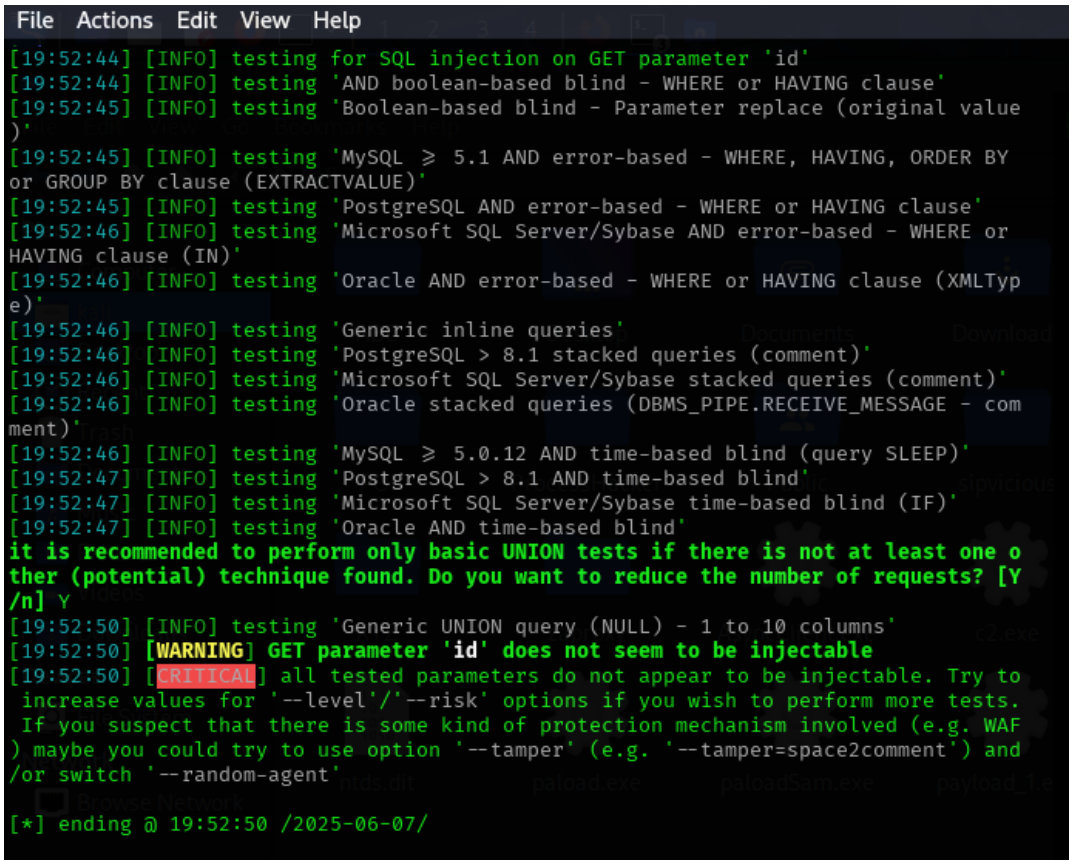
Ejecución del ataque hacia el servidor web.



Nota: Mientras se ejecuta el ataque es importante usar las opciones sobre los ataques.

Figura 66

Finalización de ataque Sqlmap.

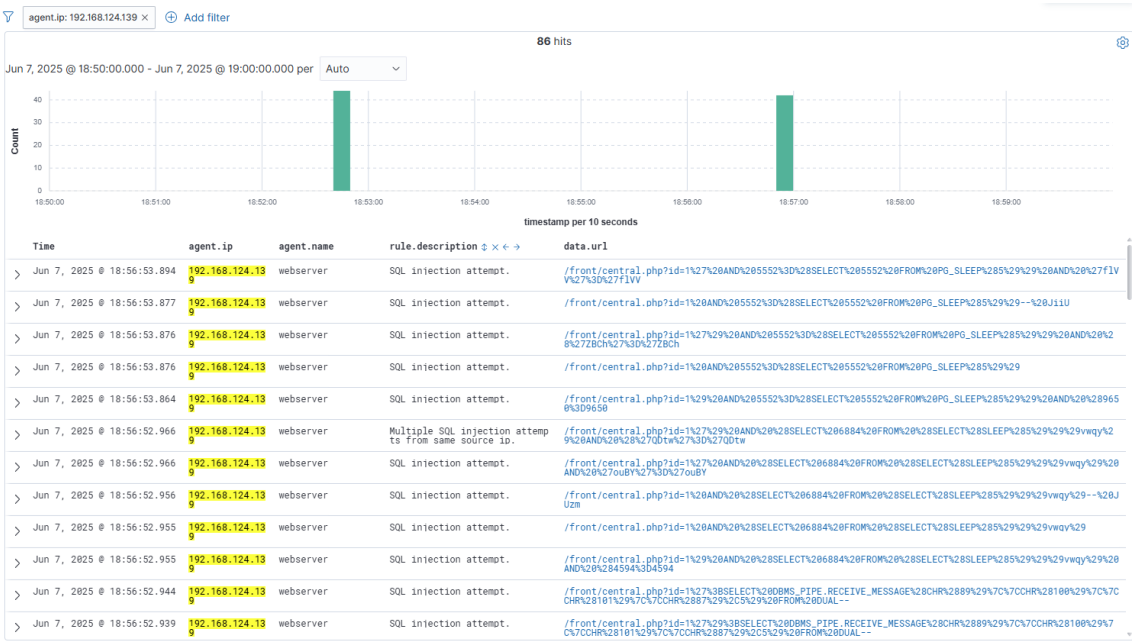


Nota: Ejecución de ataque sqlmap hacia el servidor web.

Resultados:

Figura 67

Alertas generadas en Wazuh por el ataque sqlmap



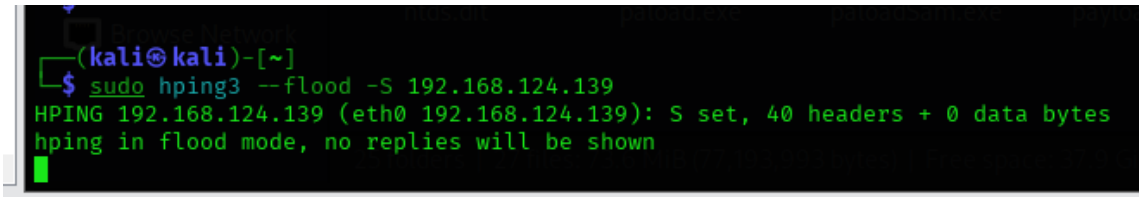
Nota: Las alertas generadas son SQL injection attempt y multiple SQL injection attempts from same source IP.

4.1.4. Ataque DoS

Ejecución de ataques:

Figura 68

Inundación de peticiones hacia el servidor web

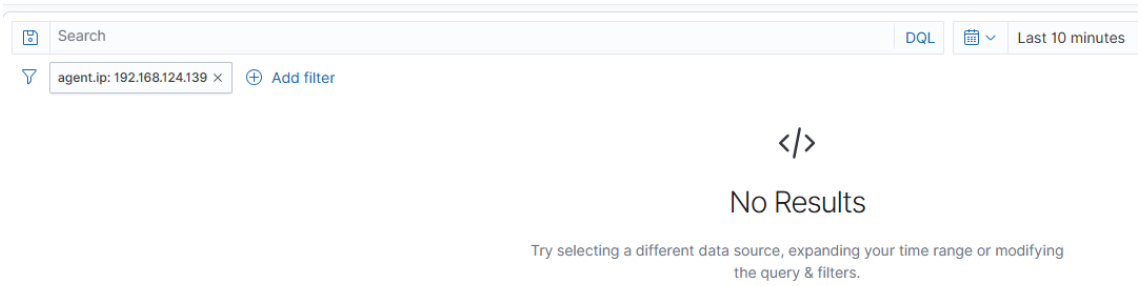


Nota: Para enviar múltiples peticiones usamos el comando hping3.

Resultados:

Figura 69

No se presentan alertas en Wazuh



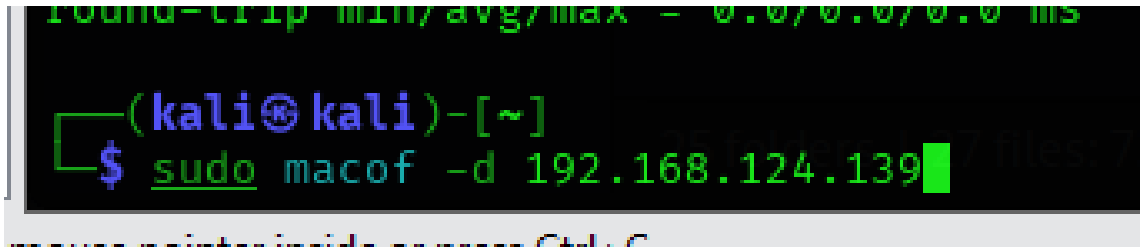
Nota: No se levantan alertas para un ataque DoS en el servidor web.

4.1.5. Ataque de MAC Flood

Ejecución de ataques:

Figura 70

Ejecución del ataque con uso del comando macof

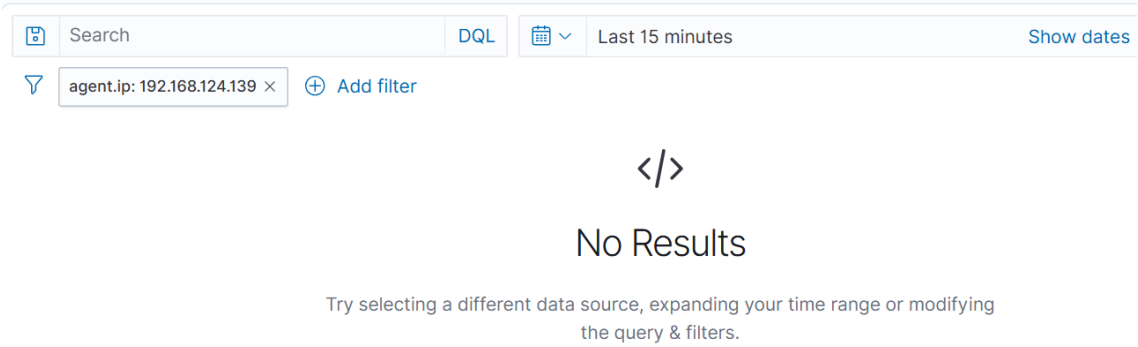


Nota: Envío de MACs aleatorias para realizar el ataque.

Resultados:

Figura 71

Alertas generadas en Wazuh por el ataque MAC Flood



Nota: No se presentan alertas generadas en Wazuh por el ataque.

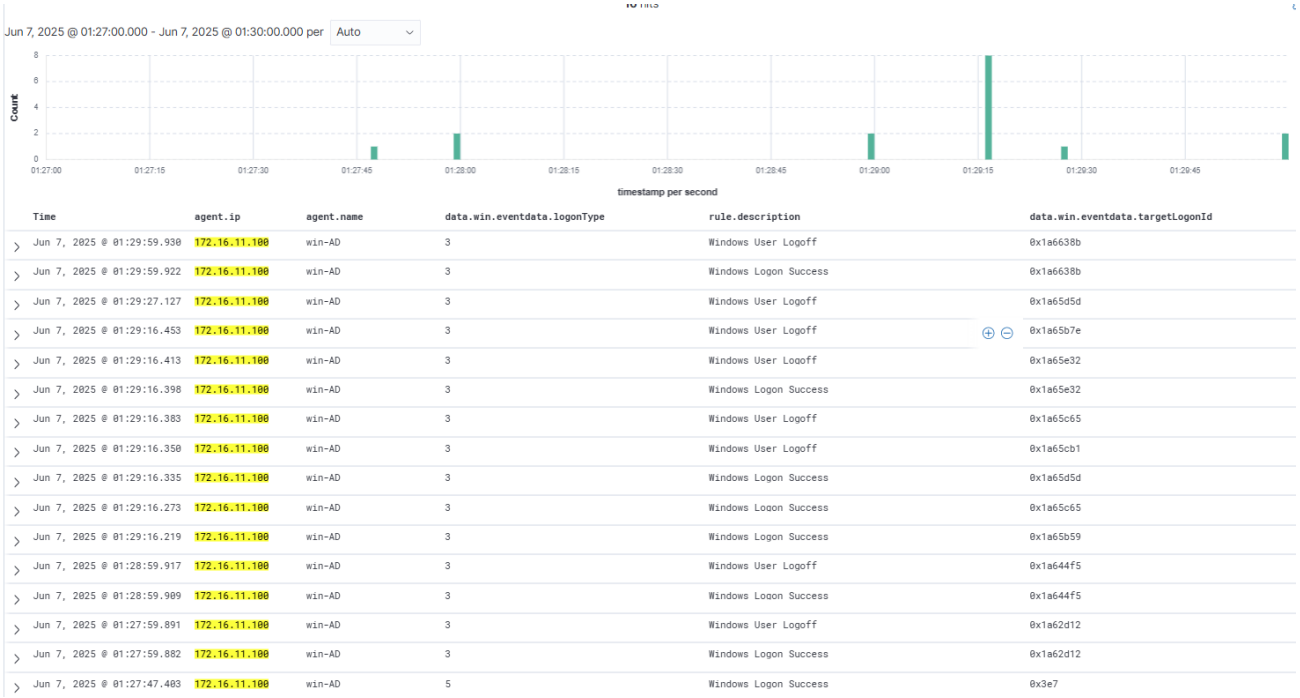
4.2. Análisis de Resultados.

4.2.1 Analísis de alertas generadas por un ataque de Fuerza Bruta

La información recolectada en Wazuh, genera las reglas Windows User Logoff y Windows Logon Success, un total de 16 eventos, se identifica un total de 5 credenciales que realizan los inicios de sesión, los ID de los eventos son 4624 (inicio de sesión exitoso) y 4634 (inicio de sesión cerrado), estos son de tipo 3 por lo que son inicios de sesión de tipo red, mediante el uso de autentificadores Kerberos. Adicional estas alertas se encuentra con la regla MITRE ATT&CK asociada: T1078 (Valid Accounts). La IP que genera la conexión es el localhost (127.0.0.1) lo que genera sospecha dado que se encubre al origen de las peticiones.

Figura 72

Alertas generadas en Wazuh por el ataque de Fuerza bruta

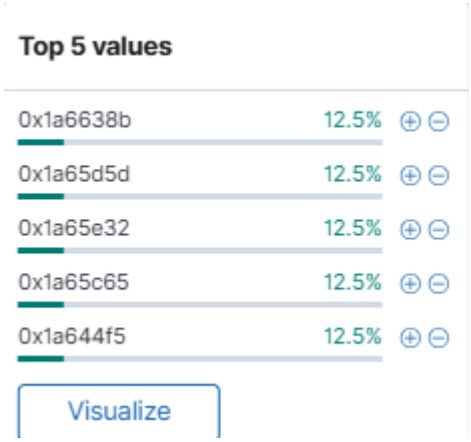


Time	agent.ip	agent.name	data.win.eventdata.logonType	rule.description	data.win.eventdata.targetLogonId
Jun 7, 2025 @ 01:29:59.930	172.16.11.100	win-AD	3	Windows User Logoff	0x1a6638b
Jun 7, 2025 @ 01:29:59.922	172.16.11.100	win-AD	3	Windows Logon Success	0x1a6638b
Jun 7, 2025 @ 01:29:27.127	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65d5d
Jun 7, 2025 @ 01:29:16.453	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65b7e
Jun 7, 2025 @ 01:29:16.413	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65e32
Jun 7, 2025 @ 01:29:16.398	172.16.11.100	win-AD	3	Windows Logon Success	0x1a65e32
Jun 7, 2025 @ 01:29:16.383	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65c65
Jun 7, 2025 @ 01:29:16.350	172.16.11.100	win-AD	3	Windows User Logoff	0x1a65cb1
Jun 7, 2025 @ 01:29:16.335	172.16.11.100	win-AD	3	Windows Logon Success	0x1a65d5d
Jun 7, 2025 @ 01:29:16.273	172.16.11.100	win-AD	3	Windows Logon Success	0x1a65c65
Jun 7, 2025 @ 01:29:16.219	172.16.11.100	win-AD	3	Windows Logon Success	0x1a65b59
Jun 7, 2025 @ 01:28:59.917	172.16.11.100	win-AD	3	Windows User Logoff	0x1a644f5
Jun 7, 2025 @ 01:28:59.909	172.16.11.100	win-AD	3	Windows Logon Success	0x1a644f5
Jun 7, 2025 @ 01:27:59.891	172.16.11.100	win-AD	3	Windows User Logoff	0x1a62d12
Jun 7, 2025 @ 01:27:59.882	172.16.11.100	win-AD	3	Windows Logon Success	0x1a62d12
Jun 7, 2025 @ 01:27:47.403	172.16.11.100	win-AD	5	Windows Logon Success	0x3e7

Nota: Alertas generadas en Wazuh por el ataque.

Figura 73

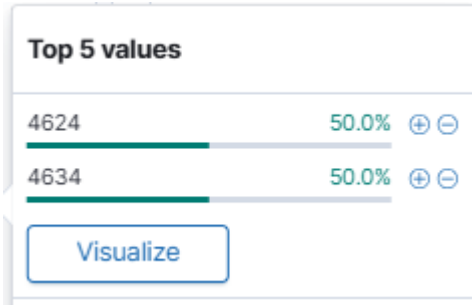
Cuentas presentadas durante el ataque.



Nota: Se identifican 5 cuentas diferentes con actividad realizadas en el equipo durante el ataque.

Figura 74

IDs de eventos Windows presentados durante el ataque



Nota: Se presentan los eventos Windows con ID 4624 y 4634.

Figura 75

Tabla de tipos de inicio de sesión en Windows

Tipo de inicio de sesión	#	Autenticadores aceptados	Credenciales reutilizables en la sesión de LSA	Ejemplos
Interactivo (también conocido como Inicio de sesión localmente)	2	Contraseña, tarjeta inteligente, Otros	Sí	Inicio de sesión de consola: RUNAS; Soluciones de control remoto de hardware (como KVM de red o acceso remoto/ tarjeta Lights-Out en el servidor) Autenticación básica de IIS (antes de IIS 6.0)
Red	3	Contraseña NT Hash, Vale kerberos	No (excepto si la delegación está habilitada, los vales kerberos presentes)	NET USE; Llamadas RPC; Registro remoto: Autenticación integrada de Windows de IIS: Autenticación de Windows de SQL:
Lote	4	Contraseña (almacenada como secreto de LSA)	Sí	Tareas programadas
Servicio	5	Contraseña (almacenada como secreto de LSA)	Sí	Servicios de Windows
NetworkCleartext	8	Contraseña	Sí	Autenticación básica de IIS (IIS 6.0 y versiones posteriores); Windows PowerShell con CredSSP
NewCredentials	9	Contraseña	Sí	RUNAS /NETWORK
RemoteInteractive	10	Contraseña, tarjeta inteligente, Otros	Sí	Escritorio remoto (anteriormente conocido como "Terminal Services")

Nota: Tabla de tipos de inicio de sesión.

Figura 76

Log completo relacionado a una alerta de seguridad

t data.win.eventdata.elevatedToken	%%1842
t data.win.eventdata.impersonationLevel	%%1833
t data.win.eventdata.ipAddress	127.0.0.1
t data.win.eventdata.ipPort	59891
t data.win.eventdata.keyLength	0
t data.win.eventdata.logonGuid	{0412d60f-7e9c-7772-66ef-8d27f3cae59e}
t data.win.eventdata.logonProcessName	Kerberos
t data.win.eventdata.logonType	3
t data.win.eventdata.processId	0x0
t data.win.eventdata.subjectLogonId	0x0
t data.win.eventdata.subjectUserSid	S-1-0-0
t data.win.eventdata.targetDomainName	UIO.LOCAL
t data.win.eventdata.targetLinkedLogonId	0x0
t data.win.eventdata.targetLogonId	0x1a6638b
t data.win.eventdata.targetUserName	WIN-AD$
t data.win.eventdata.targetUserSid	S-1-5-18
t data.win.eventdata.virtualAccount	%%1843
t data.win.system.channel	Security
t data.win.system.computer	win-AD.uio.local
t data.win.system.eventID	4624
t data.win.system.eventRecordID	55241
t data.win.system.keywords	0x8020000000000000

Nota: Logs relacionado a alertas de seguridad.

4.2.2. Analísis de alertas generadas por un Escaneo de puertos

Durante el ataque de escaneo de puertos, se activa la alerta “Web server 400 error code”, se activan 4 detecciones con peticiones de tipo GET y POST, hacia diferentes URLs relacionadas a nmap, sdk que son indicadores de herramientas de escaneo de puertos. Adicional se identifica la IP que realiza estás peticiones

en este caso es la IP 192.168.124.135. Dentro de un log se determina datos de importancia, se identifica que la petición presenta estado 404 (No Autorizado), que indica que la conexión no fue autorizada por lo que se descarta un ataque realizable. El agente usado es Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html) relacionado a la herramienta NMAP, utilizada para descubrimiento de redes.

Figura 77

Alertas generadas durante el escaneo de puertos al servidor web

Time	agent.ip	agent.name	rule.description	data.id	data.protocol	data.srcip	data.url	location
Jun 7, 2025 @ 19:12:59.052	192.168.124.139	webserver	Web server 400 error code.	404	GET	192.168.124.135	/nmaplowercheck1749341578	/var/log/apache2/access.log
Jun 7, 2025 @ 19:12:59.052	192.168.124.139	webserver	Web server 400 error code.	404	GET	192.168.124.135	/evox/about	/var/log/apache2/access.log
Jun 7, 2025 @ 19:12:59.052	192.168.124.139	webserver	Web server 400 error code.	404	GET	192.168.124.135	/HNAP1	/var/log/apache2/access.log
Jun 7, 2025 @ 19:12:59.052	192.168.124.139	webserver	Web server 400 error code.	404	POST	192.168.124.135	/sdk	/var/log/apache2/access.log

Nota: En Wazuh se genera la alerta Web server 400 error code.

Figura 78

Log completo relacionado a una alerta de seguridad

Table JSON

t	_index	wazuh-alerts-4.x-2025.06.08
t	agent.id	005
t	agent.ip	192.168.124.139
t	agent.name	webserver
t	data.id	404
t	data.protocol	POST
t	data.srcip	192.168.124.135
t	data.url	/sdk
t	decoder.name	web-accesslog
t	full_log	192.168.124.135 - - [08/Jun/2025:00:12:58 +0000] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
t	id	1749341579.24013035
t	input.type	log
t	location	/var/log/apache2/access.log
t	manager.name	wazuh
t	rule.description	Web server 400 error code.
#	rule.firedtimes	2
t	rule.gdpr	IV_35.7.d
t	rule.groups	web, accesslog, attack
t	rule.id	31101

Nota: Logs relacionado a alertas de seguridad de escaneo de puertos.

4.2.3. Analísis de alertas generadas por un Ataque SQL

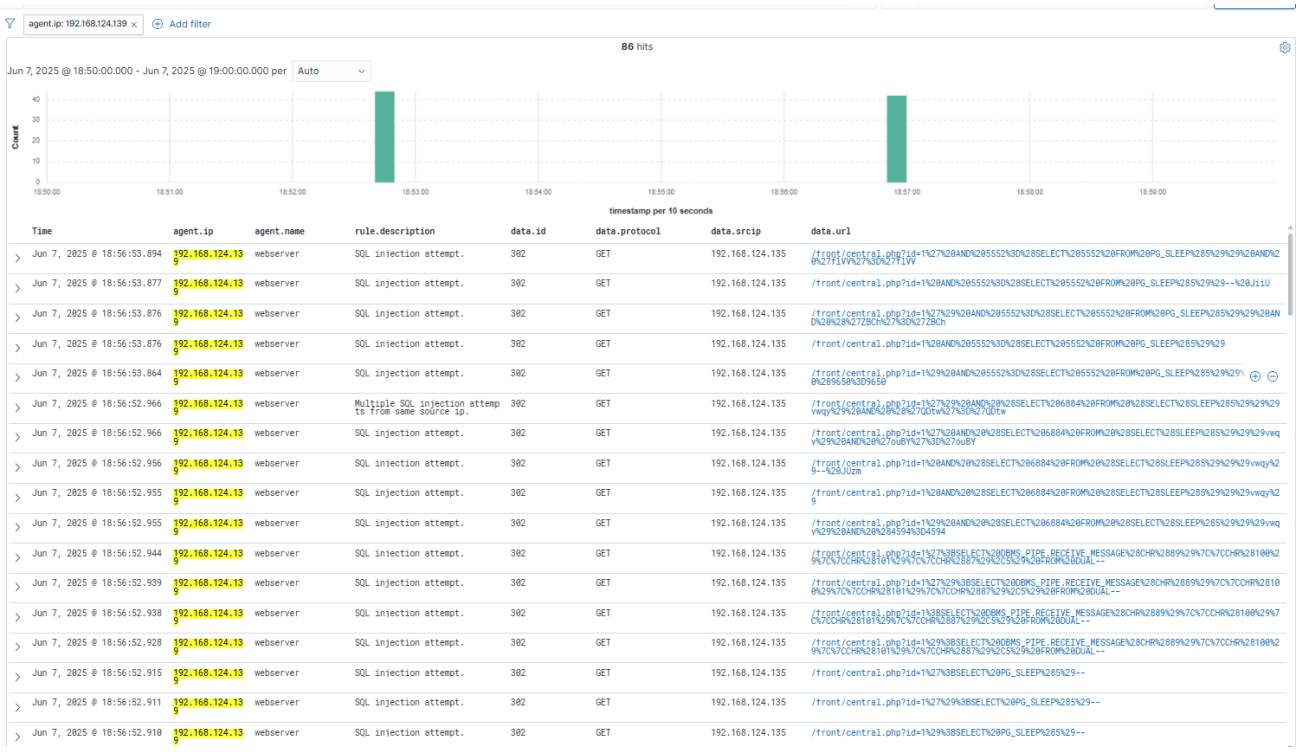
Durante el ataque se presentaron 86 alertas, SQL injection attempt, Multiple SQL injection attempts from same source ip y A web attack returned code 200 (success), se identifica que los estados de las peticiones son 302 que indica una redirección temporal y 200 que son peticiones exitosas. Todas las peticiones utilizan el método GET, el origen de las peticiones es la IP 192.168.124.135. Se analiza el log con petición 200, donde se identifica que dentro de la estructura de la petición se busca información de tablas y la referencia al programa usado que es sqlmap. (Sqlmap)

Log:

```
192.168.124.135 - - [07/Jun/2025:23:52:44 +0000] "GET /index.php?redirect=%2Ffront%2Fcent
ral.php%3Fid%3D1%26OtlI%3D7334%2520AND%25201%253D1%2520UNION%2520ALL%2520SELECT%25201%252
CNULL%252C%2527%253Cscript%253Ealert%2528%2522XSS%2522%2529%253C%252Fscript%253E%2527%252
Ctable_name%2520FROM%2520information_schema.tables%2520WHERE%25202%253E1--%252F%252A%252A
%252F%253B%2520EXEC%2520xp_cmdshell%2528%2527cat%2520..%252F..%252F..%252Fetc%252Fpasswd%
2527%2529%2523&error=3 HTTP/1.1" 200 3525 "-" "sqlmap/1.9.2#stable (https://sqlmap.org)"
```

Figura 79

Alertas en Wazuh generadas por ataque SQL.



Nota: Logs relacionado a alertas de seguridad de escaneo de puertos.

Figura 80

Log completo relacionado a una alerta de seguridad

t _index	wazuh-alerts-4.x-2025.06.07
t agent.id	005
t agent.ip	192.168.124.139
t agent.name	webserver
t data.id	200
t data.protocol	GET
t data.srcip	192.168.124.135
t data.url	/index.php?redirect=%2Ffront%2Fcentral.php%3Fid%3D1%26OtlI%3D7334%2520AND%25201%253D1%2520UNION%2520ALL%2520SELECT%25201%252CNULL%252C%2527%253Cscript%253Ealert%2528%2522XSS%2522%2529%253C%252Fscript%253E%2527%252Ctable_name%2520FROM%2520information_schema.tables%2520WHERE%25202%253E1--%252F%252A%252A%252F%253B%2520EXEC%2520xp_cmdshell%2528%2527cat%2520..%252F..%252F..%252Fetc%252Fpasswd%2527%2529%2523&error=3
t decoder.name	web-accesslog
t full_log	192.168.124.135 - - [07/Jun/2025:23:52:44 +0000] "GET /index.php?redirect=%2Ffront%2Fcentral.php%3Fid%3D1%26OtlI%3D7334%2520AND%25201%253D1%2520UNION%2520ALL%2520SELECT%25201%252CNULL%252C%2527%253Cscript%253Ealert%2528%2522XSS%2522%2529%253C%252Fscript%253E%2527%252Ctable_name%2520FROM%2520information_schema.tables%2520WHERE%25202%253E1--%252F%252A%252A%252F%253B%2520EXEC%2520xp_cmdshell%2528%2527cat%2520..%252F..%252F..%252Fetc%252Fpasswd%2527%2529%2523&error=3 HTTP/1.1" 200 3525 "-" "sqlmap/1.9.2#stable (https://sqlmap.org)"
t id	1749340364.23463175
t input.type	log
t location	/var/log/apache2/access.log
t manager.name	wazuh
t rule.description	A web attack returned code 200 (success).
# rule.firedtimes	1
t rule.gdpr	IV_35.7.d
t rule.groups	web, accesslog, attack

Nota: Logs relacionado a alertas de seguridad de peticiones SQL.

4.2.4. Analísis de alertas generadas por un Ataque DoS

Se realiza un ataque DoS hacia el servidor web, en Wazuh no se generan alertas por lo que las conexiones no son identificadas para el servidor.

4.2.5. Analísis de alertas generadas por un Ataque MAC Flood

Cuando se realiza el ataque hacia el servidor web, en Wazuh no se generan alertas por lo que las inundaciones de tipo MAC no son explotables en el servidor por lo que en este caso se debe determinar el objetivo de los ataques.

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Wazuh-agent permite la supervisión detallada del servidor GLPI, incluyendo servicios críticos como Apache y MySQL, sin modificar directamente la aplicación.

Apache y MySQL generan logs clave que Wazuh puede colectar y analizar para detectar caídas, accesos no autorizados, errores de configuración, y escaneos maliciosos.

La correcta configuración del agente garantiza el éxito del monitoreo de eventos de seguridad de un componente de la infraestructura y acciones posteriores.

Durante el análisis de resultados se identifica que el catálogo de reglas que tiene Wazuh no cubre ciertas detecciones donde no se presentaron alertas de seguridad, un ejemplo el ataque DoS donde el atacante envió varias peticiones, pero no se presentaron alertas, en este tipo de casos es importante la elaboración de afinamientos en las reglas de detección o en la creación de nuevas.

En el ataque de fuerza bruta no se determinó el equipo de origen que envía estás peticiones, la IP identificada era el localhost, en estos casos es importante la correlación de eventos para poder determinar la IP correcta para una contención efectivo del ataque.

Es importante evaluar los tipos de ataques que se realizan en especial para determinar si son efectivos según los equipos de destino, con esta información se puede evaluar el correcto funcionamiento de las reglas de detección.

5.2. RECOMENDACIONES

Verificar que los archivos y directorios que constan en la configuración del agente o los servicios cuenten con los permisos correctos y pertenezcan a los usuarios correspondientes.

Configurar los umbrales, niveles de alertas, criticidad y acciones automáticas de manera que faciliten un eficiente manejo de eventos y un tiempo de respuesta menor.

Es recomendable realizar pruebas para evaluar el correcto funcionamiento de las reglas de detección de amenazadas, adicional es importante validar si existen puntos ciegos que se necesite crear reglas personalizadas para una detección oportuna.

Para una detección óptima es importante la correlación de eventos, para poder determinar una traza completa de la detección.

Para la integración de fuentes es importante validar el tipo de versión compatible para la integración con Wazuh, dado que es una SIEM open source, se tiene información en foros y sitios en internet, al integrar más fuentes es necesario validar los recursos de la SIEM por el procesamiento de eventos que debe almacenar y procesar, estás recomendaciones son importantes para el funcionamiento correcto.

Referencias Bibliográficas

Heller, M. (2024). *Monitorización y seguridad de cargas de trabajo en la nube con Wazuh*. Linode. https://www.linode.com/docs/guides/monitoring-and-securing-cloud-workloads-with-wazuh/?lang=es

ManageEngine. (2024, mayo 8). *ManageEngine recognized in 2024 Gartner® Magic Quadrant™ for Security Information and Event Management for the seventh time*. https://www.manageengine.com/log-management/2024-gartner-siem-mq.html

IBM. (s.f.). *SIEM (gestión de eventos e información de seguridad).* https://www.ibm.com/es-es/topics/siem

Proofpoint. (2025). *Security Information and Event Management (SIEM).* https://www.proofpoint.com/es/threat-reference/security-information-event-management-siem

Gonzalo Nazareno. (2022-23). *Proyecto Despliegue y funcionamiento de Wazuh.* https://dit.gonzalonazareno.org/gestiona/proyectos/2022-23/Proyecto_Despliegue_funcionamiento_Wazuh.pdf

GeeksforGeeks. (2022, enero 31). *Introduction to Wazuh*. https://www.geeksforgeeks.org/introduction-to-wazuh/

OpenSearch. (2024). *Wazuh: Open-source SIEM and XDR platform.* https://opensearch.org/solutions-providers/wazuh/

Wazuh. (2025). *Wazuh ruleset and alert levels.* https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/rules.html#alert-level

Finsin. (2024, abril 10). *Securitizando tu red: instalando servidores de Wazuh.* https://finsin.cl/2024/04/10/securitizando-tu-red-instalando-servidores-de-wazuh-parte-4/

InLab FIB. (2024). *Wazuh: una plataforma de código abierto que unifica SIEM y XDR.* https://inlab.fib.upc.edu/es/articulos/wazuh-una-plataforma-de-codigo-abierto-que-unifica-siem-y-xdr/2024/

Ambit BST. (2021). *¿Qué significa SIEM y cómo funciona?*. https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

Wazuh. (2025). *Security Information and Event Management (SIEM)*. https://wazuh.com/platform/siem/

Instituto Nacional de Ciberseguridad (INCIBE). (2025). *Guía de ciberataques.* https://www.basc-pichincha.org.ec/media/attachments/2025/06/02/guia_de_ciberataques.pdf

TecnetOne. (2023). *Ataques de escaneo de puertos*. https://blog.tecnetone.com/ataques-de-escaneo-de-puertos

Wazuh, Inc. (2024). *Ruleset: Alert levels. Wazuh Documentation.* https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/rules.html#alert-level

Cambara, F. R. (2023). *Cómo instalar Wazuh 2023 en Ubuntu 22.04: Instalación de agentes.* https://medium.com/@fransk.roman.cambara/como-instalar-wazuh-2023-en-ubuntu-22-04-instalaci%C3%B3n-de-agentes-50cae9e23b35

Wazuh. (s.f.). *Wazuh server installation guide.* https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html

Wikipedia. (s.f.). *Wazuh. Wikipedia, la enciclopedia libre.* https://es.wikipedia.org/wiki/Wazuh[1](https://www.geeksforgeeks.org/introduction-to-wazuh/)

Underc0de. (2023, marzo 6). *Wazuh: una plataforma de código abierto, SIEM y XDR*. https://blog.underc0de.org/wazuh-una-plataforma-de-codigo-abierto-siem-y-xdr/

CiberseguridadPY. (2024, febrero 15). *Wazuh: SIEM open source para detección de amenazas.*

https://ciberseguridadpy.com/wazuh-siem-open-source-para-deteccion-de-amenazas/

RootedCON. (2023). *Presentación técnica: Wazuh como solución SIEM y XDR.*

https://www.rootedcon.com/2023/presentaciones/wazuh-siem-xdr.pdf

Hackpuntes. (2024, abril 10). *Wazuh: instalación, configuración y casos de uso.*

https://hackpuntes.com/wazuh-instalacion-configuracion-casos-de-uso/

Servicios Vartech. (s.f.). *Wazuh en Ubuntu: configuración inicial y primeros pasos.*

https://www.serviciosvartech.com/wazuh-en-ubuntu-configuracion-inicial-y-primeros-pasos/

Tutoriales IT. (s.f.). *Instalación y configuración de agentes de Wazuh en Windows y Linux.*

https://tutorialesit.es/instalacion-y-configuracion-agentes-de-wazuh-en-windows-y-linux/

Finsin. (2024, abril 10). *Securitizando tu red: instalando servidores de Wazuh*.

https://finsin.cl/2024/04/10/securitizando-tu-red-instalando-servidores-de-wazuh-parte-4/

Microsoft. (sf). *Herramientas administrativas y tipos de inicio de sesión.* https://learn.microsoft.com/es-es/windows-server/identity/securing-privileged-access/reference-tools-logon-types

Sqlmap. SQL. https://sqlmap.org/

Apéndice A

Acceso a las Máquinas Virtuales del Proyecto

Las máquinas virtuales desarrolladas para la implementación de SIEM Wazuh están disponibles para su descarga a través del siguiente enlace:

https://www.dropbox.com/scl/fo/qykcgi5ms78sr1cap2b4f/ALFcm7aMmna-bXhfuvC4obk?rlkey=0djd0jf75ujupc7oa5j9g03n6&st=6qgzlfyl&dl=0

Este recurso contiene las imágenes de las máquinas virtuales de Wazuh server, GLPI, BDD, active directory, que han sido configuradas en el proyecto.