LABSIEM 1 – Instalación y configuración de Wazuh

1. Objetivo. – Implementar y configurar la plataforma de seguridad Wazuh en Linux y agentes en Windows, con el propósito de conocer el procedimiento correcto de su instalación y utilizar sus funcionalidades en próximos laboratorios.

2. Herramientas. - Para este laboratorio se utilizarán:

- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)
- Wazuh
- Agentes

3. Procedimiento

3.1 Instalación y configuración pfSense

1. Para realizar la instalación de Wazuh en Linux, se utiliza el comando provisto en su pagina web oficial y se lo ejecuta en la terminal, después de varios minutos la instalación se completa correctamente. (ver Figura 1)

2. Una vez instalado correctamente, Wazuh otorga un usuario y una contraseña, que permitirá y facilitara el acceso a todas sus herramientas y funcionalidades. (ver Figura 2).

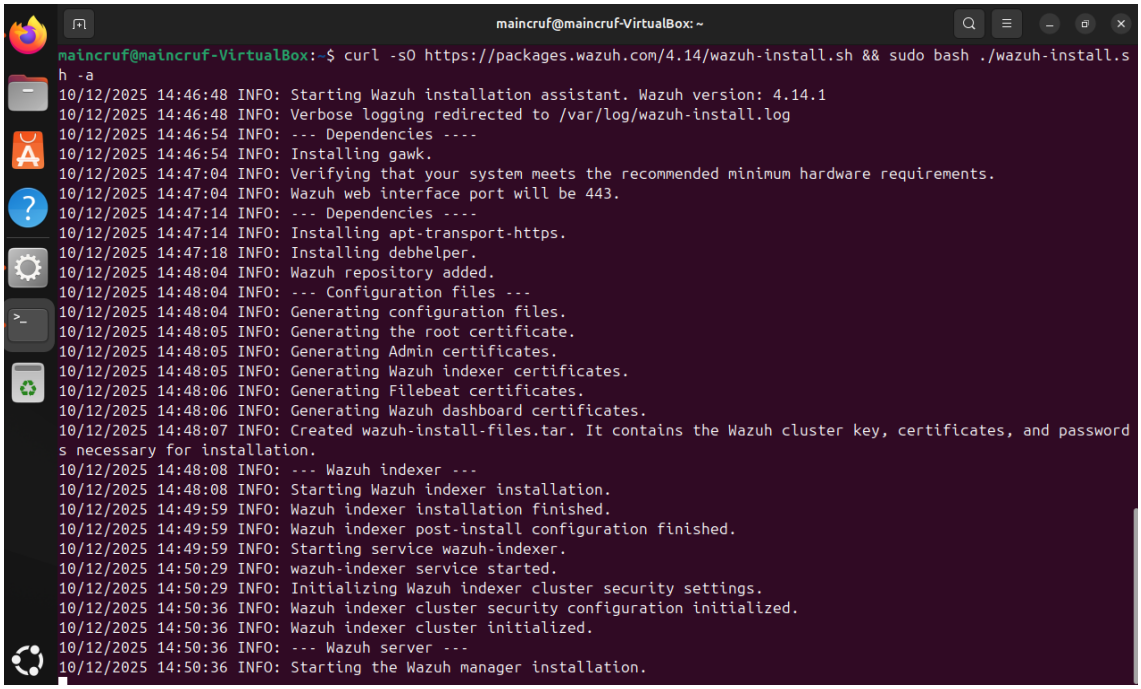

Figura 1. Instalación de Wazuh

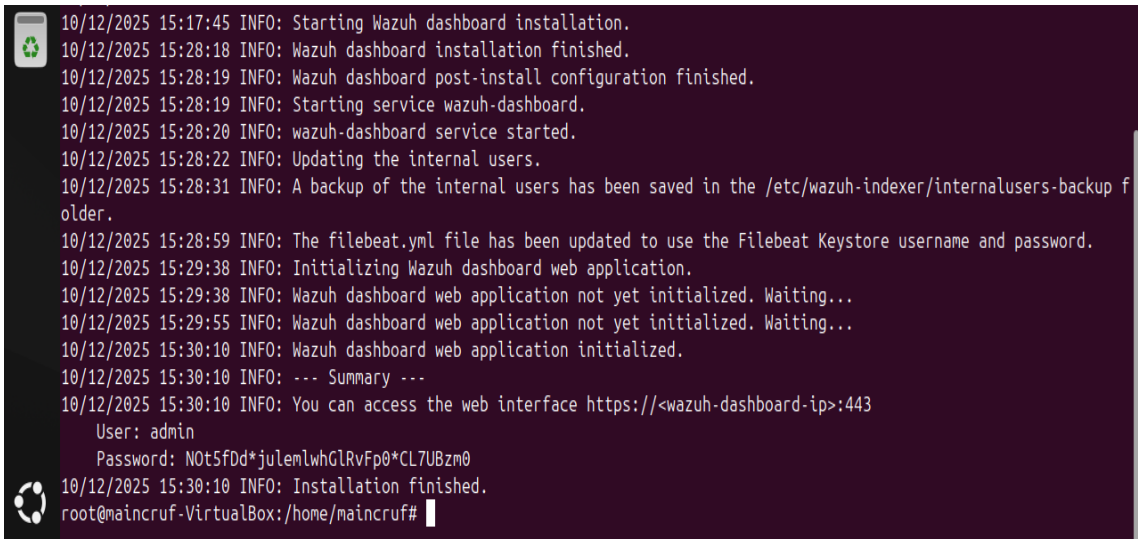

Figura 2. Instalación completa de Wazuh y credenciales recibidas.

3.2 Acceso a Wazuh

Para el acceso a este SIEM, necesitamos seguir los siguientes pasos.

1. Instalado Wazuh, se procede a abrir el navegador web, y escribir la ip de la maquina que servirá de servidor en la barra de búsqueda, en este caso es 192.168.0.6.

2. Al colocar las credenciales dadas por Wazuh, se dará acceso y se mostrara el overview de Wazuh. (ver Figura 3)

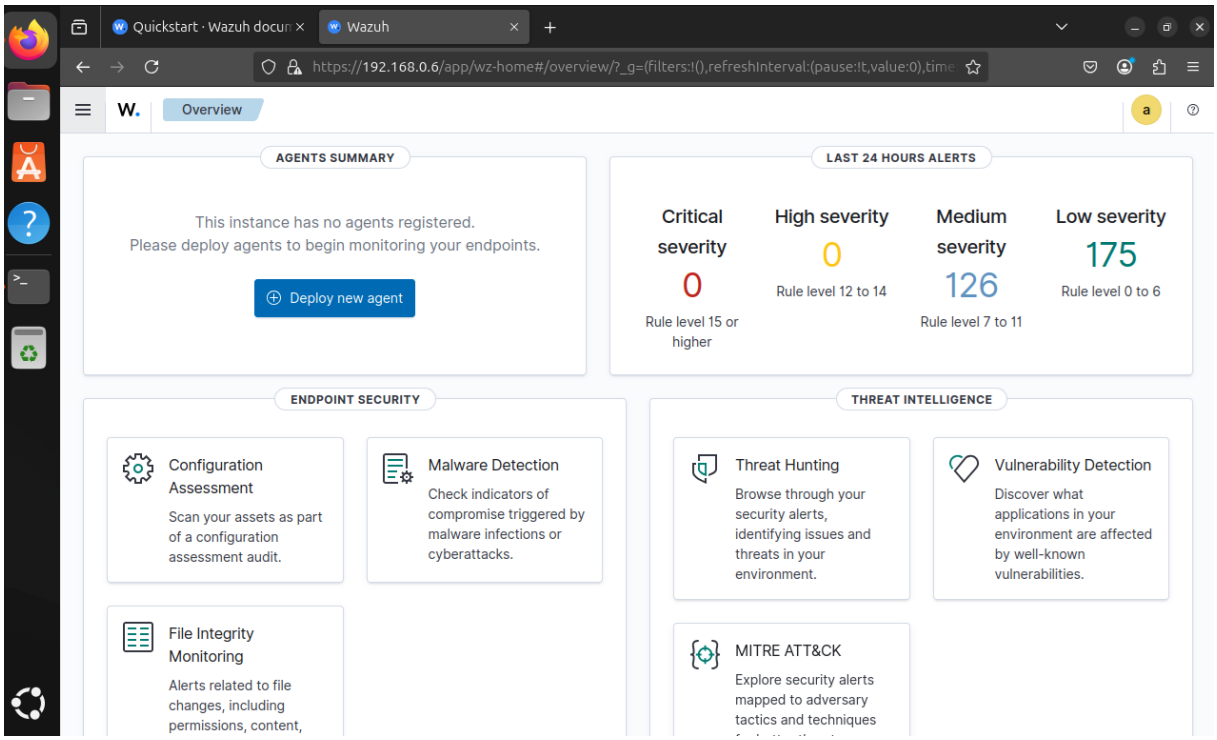

Figura 3. Overview de Wazuh.

3.3 Creación del agente de Wazuh

1. Para monitorear o recibir alertas de otros equipos se necesita crear “agentes”, para esto existe la opción “Deploy New Agent”, que permite establecer agentes fácilmente en distintos sistemas operativos, eligiendo para este laboratorio un equipo Windows. (ver Figura 4)

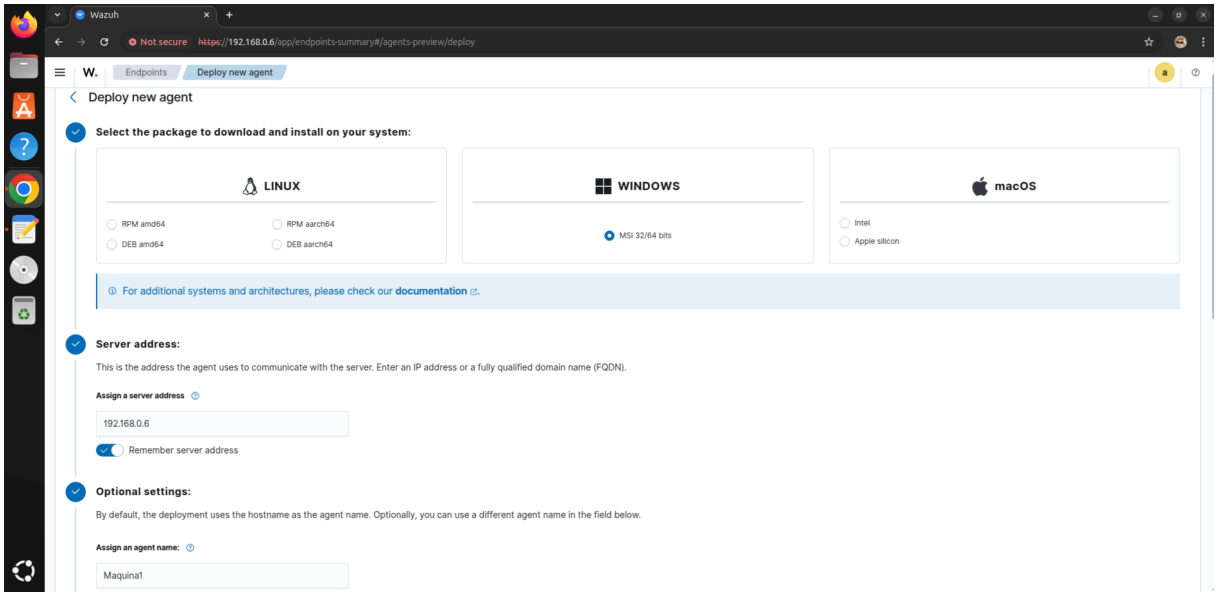

Figura 4. Creando un agente en Linux para Windows.

2. Ya creado el agente, Wazuh dará un comando para ejecutarlo en modo administrador en Windows PowerShell, de modo de que el servicio comience y así sincronizar el servidor con su agente. (ver Figura 5)

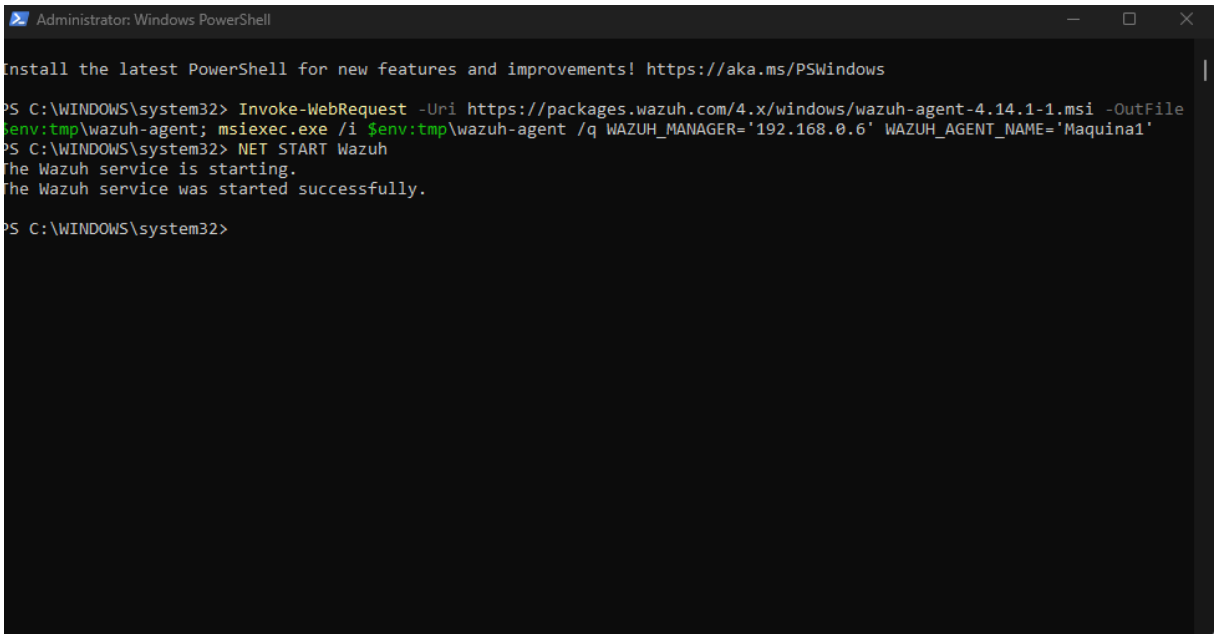

Figura 5. Instalación y funcionamiento del agente en Windows.

3. Dentro de la interfaz de Wazuh, se logra ver que el agente Windows se sincronizó correctamente con el servidor Wazuh Linux, permitiendo monitorizar y recibir alertas de ese equipo. (ver Figura 6)

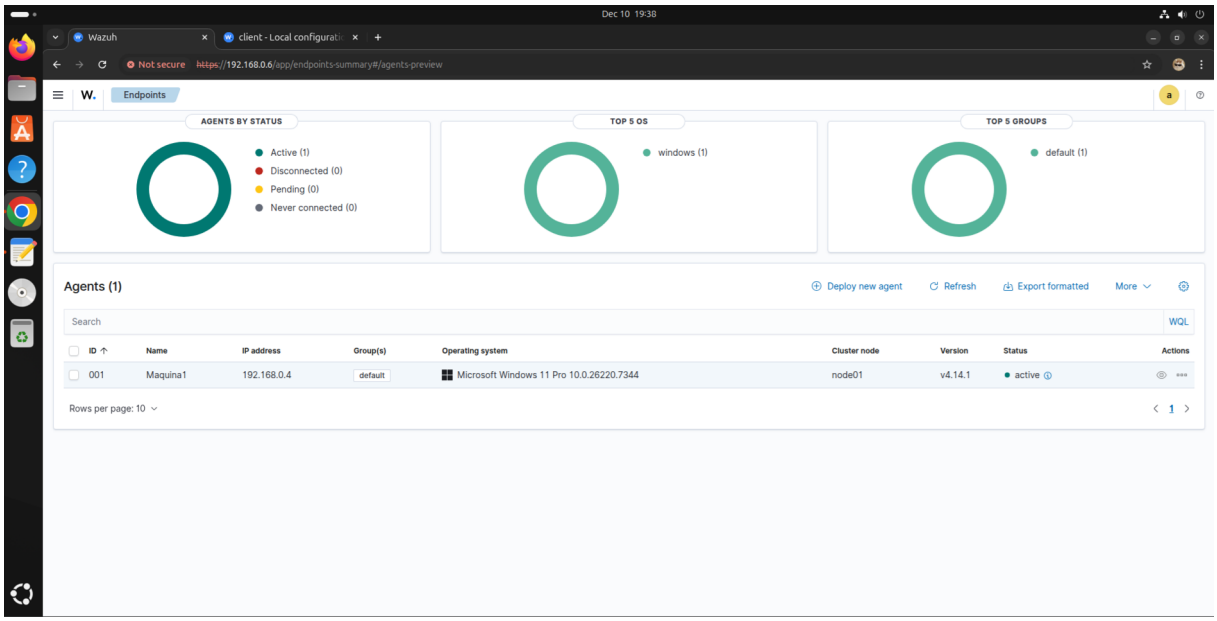

Figura 6. Agente correctamente conectado con el servidor Wazuh.

4. Resultados Obtenidos. - Durante el laboratorio se logró realizar satisfactoriamente el proceso de instalación y configuración de la plataforma SIEM. Asimismo, se implemento el agente en el equipo de Windows para permitir su monitorización, verificando la conexión entre el agente y el servidor, confirmando que el SIEM es capaz de recibir los eventos y alertas generados.

5. Reflexión final. - Este laboratorio me permitió comprender como funciona la instalación de un SIEM, y la importancia de una correcta configuración de sus agentes. Aprendiendo el valor de estas herramientas en el ámbito de la ciberseguridad, ya que permiten monitorear amenazas en tiempo real y fortalecer distintos entornos como empresas, bancos o centros educativos.