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 utilizaron:

- Oracle VirtualBox.
- Máquina Windows y Cliente Ubuntu (máquina virtual)
- Wazuh.

3. Configuración

3.1 Servidor Wazuh

Se instaló el servidor Wazuh en Linux mediante la ejecución del comando de instalación provisto en la página web oficial de Wazuh. Después de varios minutos de espera, la instalación se completó correctamente. (ver Figura 1)

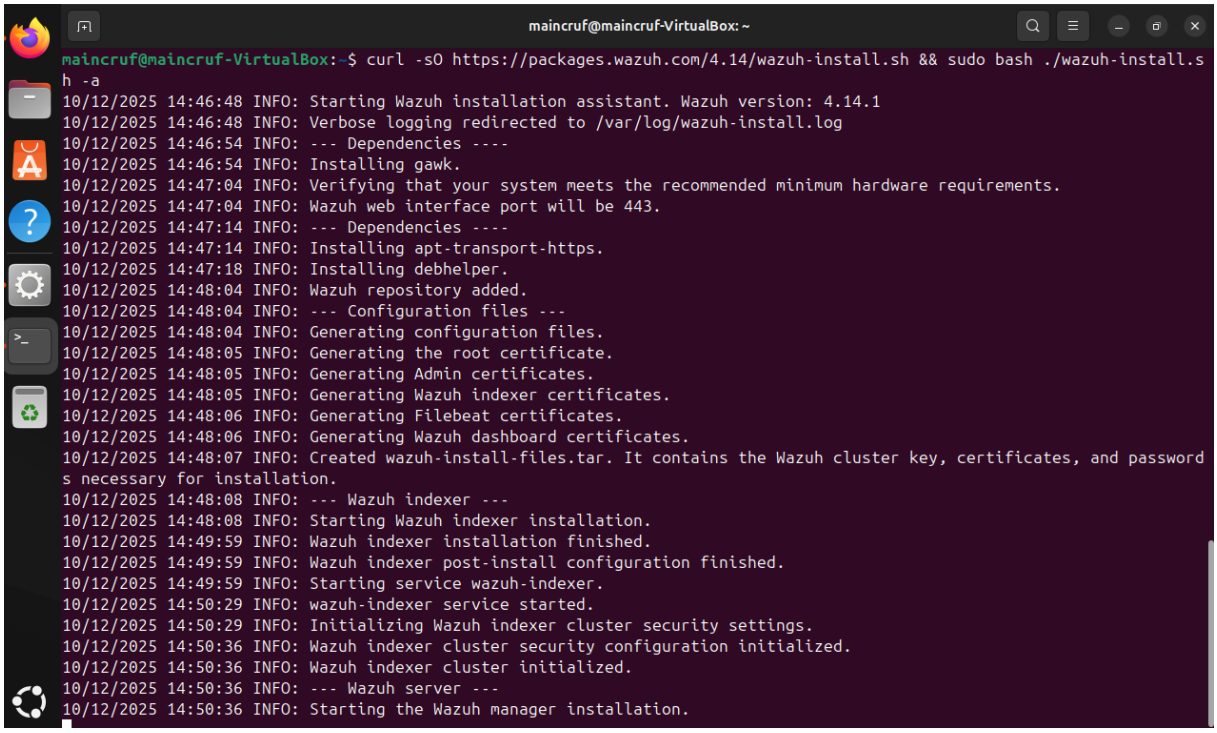

Figura 1. Instalación de Wazuh

Una vez finalizada la instalación, Wazuh facilitó un usuario y contraseña, con el propósito de facilitar el acceso a todas sus herramientas y funcionalidades. (ver Figura 2)

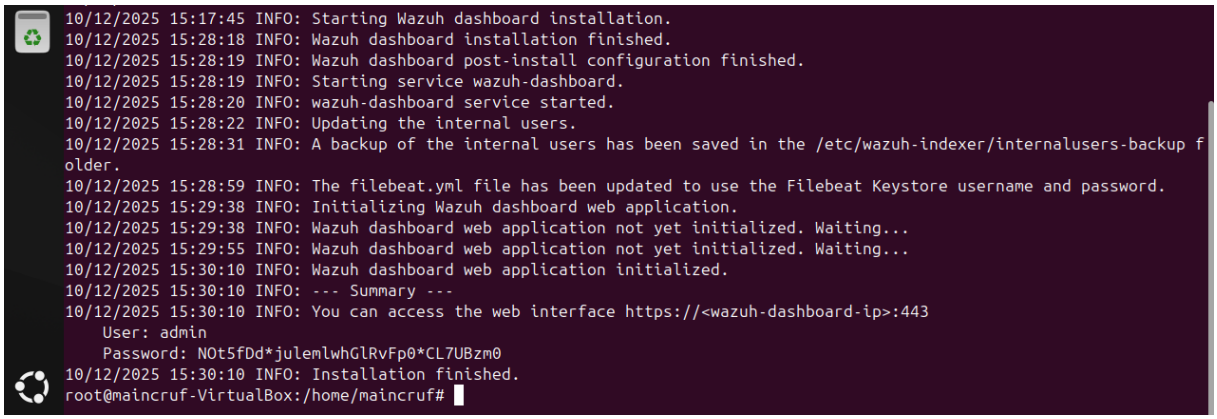

Figura 2. Instalación completa de Wazuh y credenciales recibidas.

3.2 Agente Wazuh

Para monitorear o recibir alertas de otros equipos se necesita crear “agentes”. Se accedió a la interfaz de Wazuh e ingresó a la opción “Deploy New Agent” (ver Figura 6). Esta opción permite establecer agentes fácilmente en distintos sistemas operativos, eligiendo para este laboratorio un equipo Windows. (ver Figura 3)

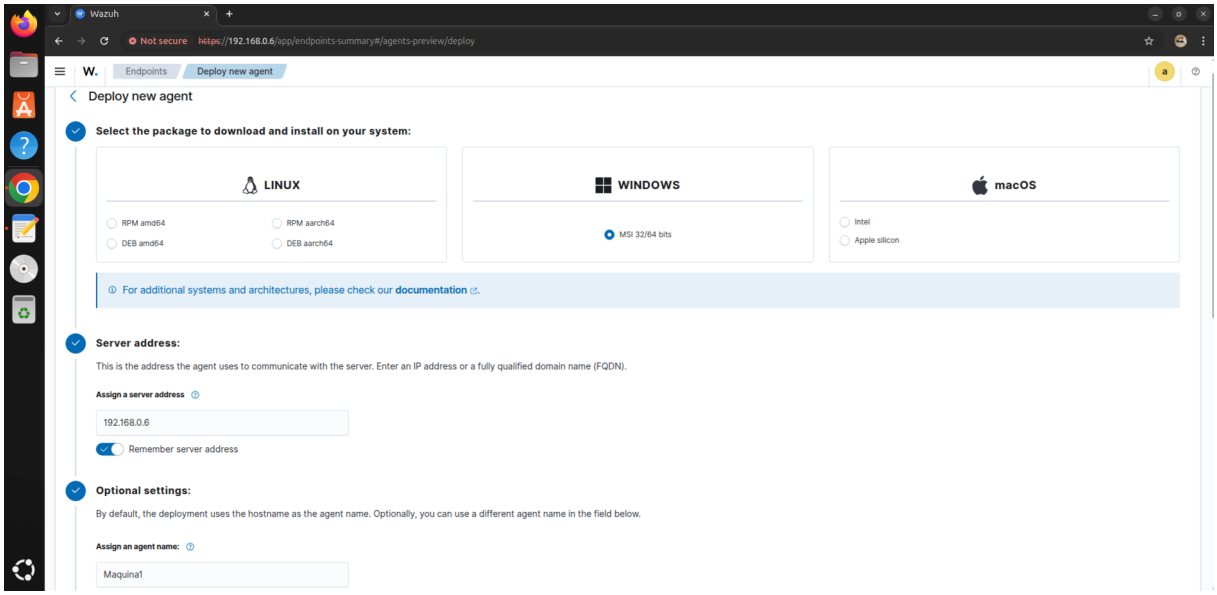

Figura 3. Creando un agente en Linux para Windows.

Configurado el agente en la interfaz, Wazuh proveyó un comando y se lo ejecutó en modo administrador en Windows PowerShell, para que de esta forma el servicio comience y se sincronice el servidor con el agente. (ver Figura 4)

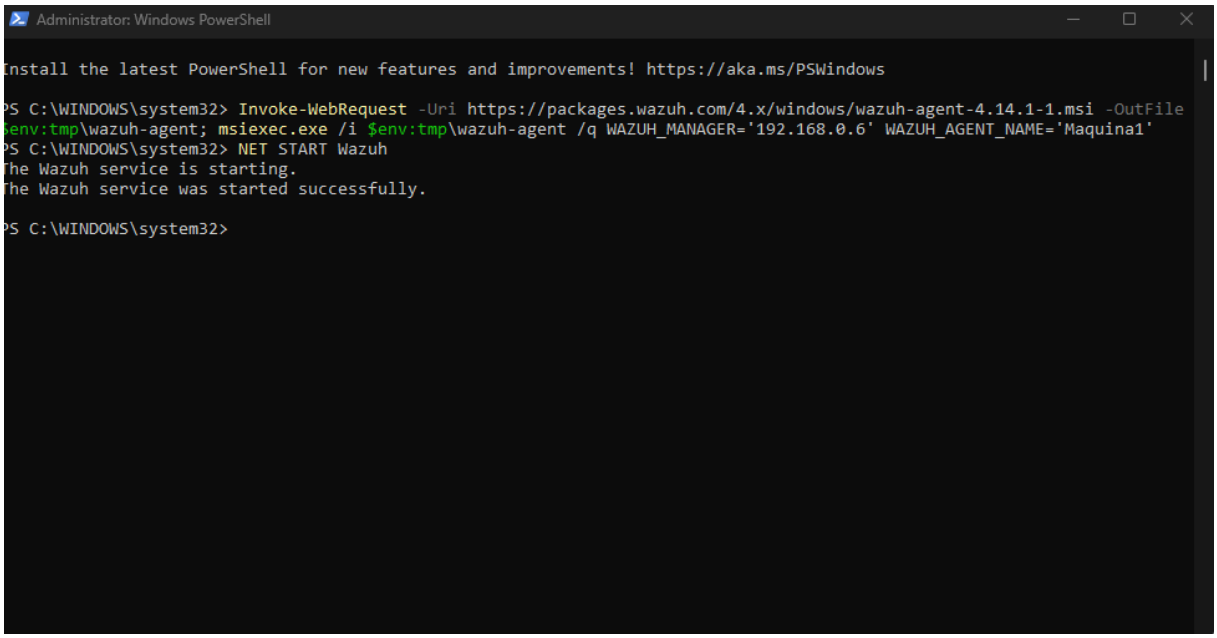

Figura 4. Instalación y funcionamiento del agente en Windows.

3.3 Desactivación de actualizaciones

Se desactivaron las actualizaciones con el objetivo de evitar fallos de versiones entre el agente Wazuh y el servidor. (ver Figura 5)

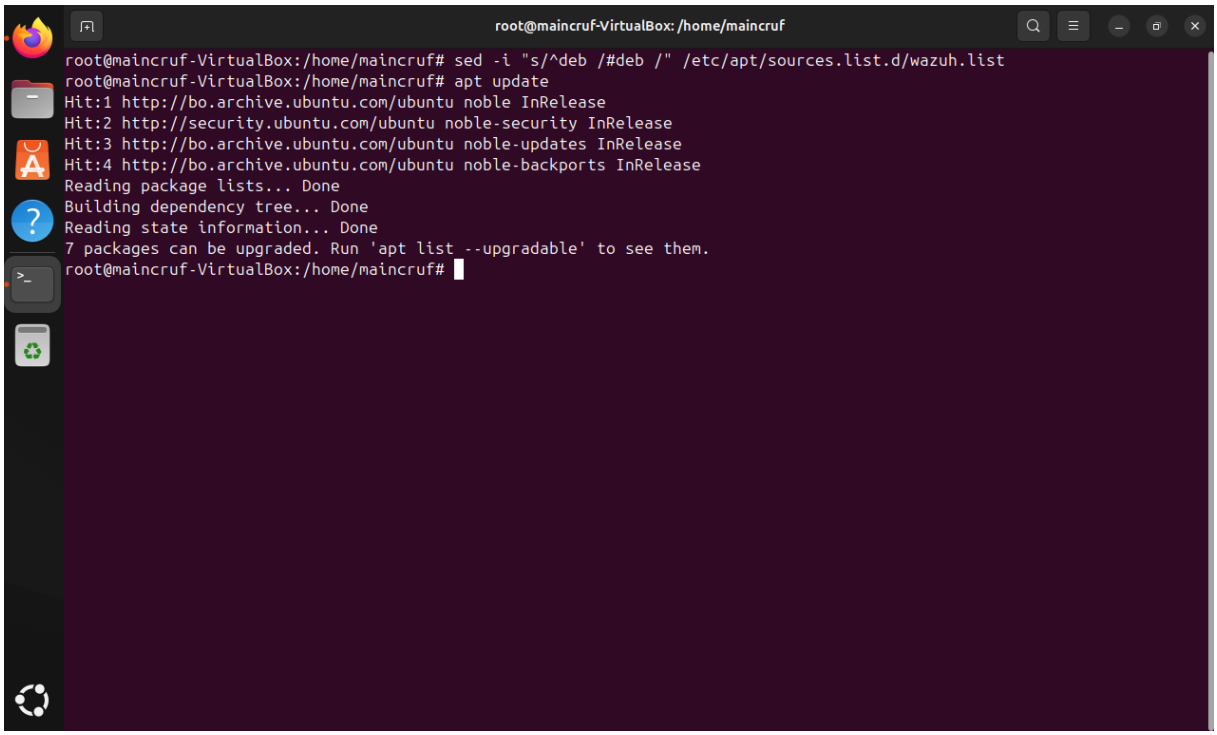

Figura 5. Desactivación de actualizaciones automáticas en Wazuh

4. Verificación Técnica

4.1 Acceso a Wazuh

Se accedió a este SIEM, siguiendo los siguientes pasos.

1. Se abrió el navegador web, y se escribió la IP de la máquina que servirá de servidor en la barra de búsqueda, en este caso es 192.168.0.6.

2. Tras colocar las credenciales dadas por Wazuh, se permitió el acceso y se mostró la vista general (overview) de Wazuh. (ver Figura 6)

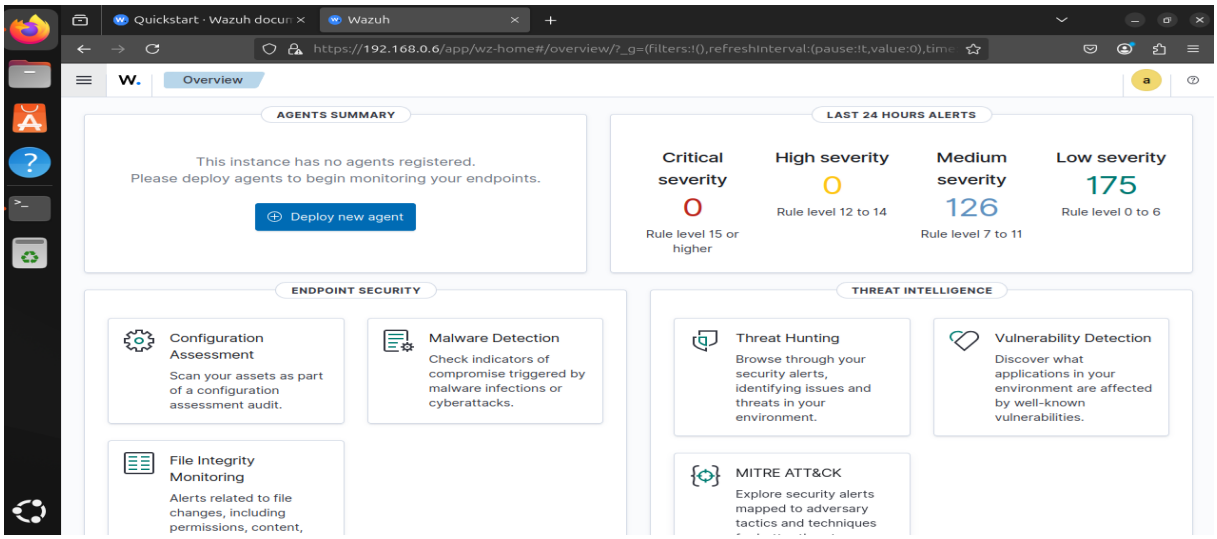

Figura 6. Overview de Wazuh.

4.2 Verificación agente Wazuh

Dentro de la interfaz de Wazuh, se logró ver que el agente Windows se sincronizó correctamente con el servidor en Linux, permitiendo monitorizar y recibir alertas de ese equipo. (ver Figura 7)

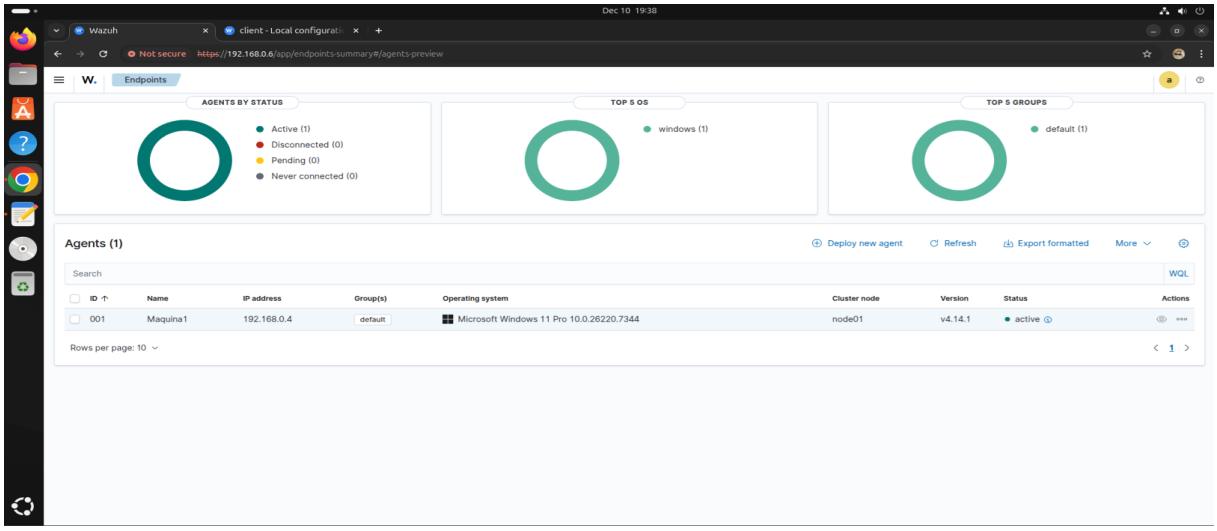

Figura 7. Agente correctamente conectado con el servidor Wazuh.