Actividad 2 - Wazuh

Módulo 3 - Gestión de incidentes

Diego Mucci

19/05/2024

Seguridad Informática

Actividad 2 - Wazuh

Wazuh es una plataforma de código abierto que proporciona detección de amenazas, monitorización de seguridad y respuesta a incidentes. Ofrece funcionalidades clave como la detección de intrusiones, gestión de incidentes, monitorización de integridad de archivos, análisis de vulnerabilidades y cumplimiento normativo. Además, es compatible con entornos en la nube como AWS, Azure y Google Cloud Platform, permitiendo una protección integral y adaptable a diferentes infraestructuras.

Para las organizaciones, Wazuh ofrece una protección proactiva al detectar y alertar sobre amenazas en tiempo real, facilitando respuestas rápidas y automatizadas. Proporciona visibilidad centralizada de la seguridad de todos los sistemas, ayuda a cumplir con regulaciones mediante informes detallado. Su capacidad para adaptarse a entornos locales, híbridos o en la nube y gestionar grandes volúmenes de datos lo convierte en una herramienta ideal para fortalecer la seguridad de los sistemas de información.

Actividad. - Implementación de Wazuh en Cloud

Objetivo:

Implementarás Wazuh en el cloud oficial, desplegarás agentes en una máquina virtual Windows y otra Kali, y activarás servicios de seguridad previamente configurados en la máquina Kali. Documentarás el proceso con capturas de pantalla y generarás eventos de seguridad para verificar la correcta configuración y funcionamiento.

Requisitos:

- Cuenta de correo temporal para registro
- Acceso a máquinas virtuales Windows y Kali
- Servicios de seguridad instalados y configurados en Kali (Snort, Suricata, WAF con mod-security)
- Opción alternativa: OVA oficial de Wazuh para instalación en máquina virtual

Pasos a seguir:

1. Registro en Wazuh Cloud

1. Accede a la página de registro de Wazuh Cloud.
2. Utiliza una cuenta de correo temporal para completar el registro.
3. Verifica tu cuenta a través del correo recibido y accede al portal de Wazuh Cloud.

2. Creación del Entorno en Wazuh

1. Inicia sesión en Wazuh Cloud.
2. Crea un nuevo entorno desde el dashboard principal.
3. Configura el entorno según las especificaciones necesarias.

3. Despliegue de Agentes

1. **Máquina Virtual Windows:**

- Crea un agente desde el portal de Wazuh Cloud e invoca con el comando necesario y desde la máquina virtual la instalación del agente de Wazuh.
- Inicia el servicio.

2. Máquina Virtual Kali:

- Crea un agente desde el portal de Wazuh Cloud e invoca con el comando necesario y desde la máquina virtual la instalación del agente de Wazuh.
- Inicia el servicio.

4. Activación de Servicios en Kali

Verifica y activa los servicios de seguridad previamente instalados:

- **Snort**: Configura y activa el servicio.
- **Suricata**: Configura y activa el servicio.
- **WAF (mod-security)**: Configura y activa el servicio en el servidor web.

5. Verificación de Eventos en Wazuh Cloud

Accede al dashboard de Wazuh Cloud y verifica que los eventos de seguridad de las máquinas virtuales se reflejan correctamente.

6. Generación de Nuevos Eventos de Seguridad

- Máquina Windows:

- Genera varios intentos de inicio de sesión fallidos.

- Máquina Kali:

- Realiza un intento de inyección de código en un formulario web protegido por WAF.
- Ejecuta acciones para activar reglas de Snort y Suricata generando tráfico sospechoso.

7. Documentación del Proceso

- Compila todas las capturas de pantalla en un documento.

- Redacta una breve descripción para cada paso, explicando el proceso seguido y los resultados obtenidos.

- Asegúrate de incluir cualquier problema encontrado y cómo se resolvió.

Opción Alternativa: Instalación de Wazuh mediante OVA

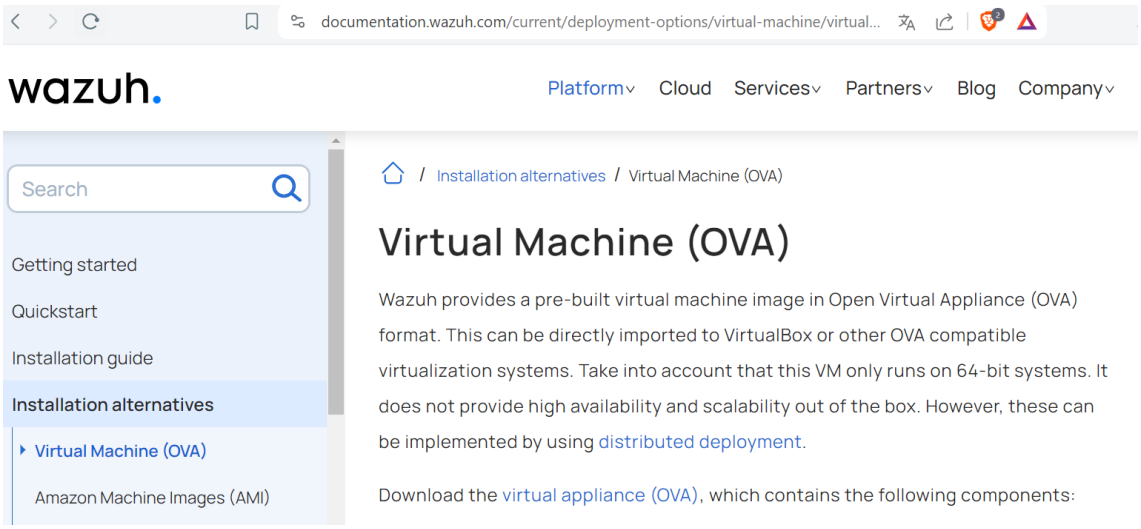
1. Descarga la OVA oficial de Wazuh desde el sitio web de Wazuh.
2. Importa la OVA en tu software de virtualización preferido (por ejemplo, VirtualBox, VMware).
3. Sigue las instrucciones de instalación y configuración para desplegar Wazuh en una máquina virtual.
4. Repite los pasos 3-6 para el despliegue de agentes y generación de eventos.

Entrega:

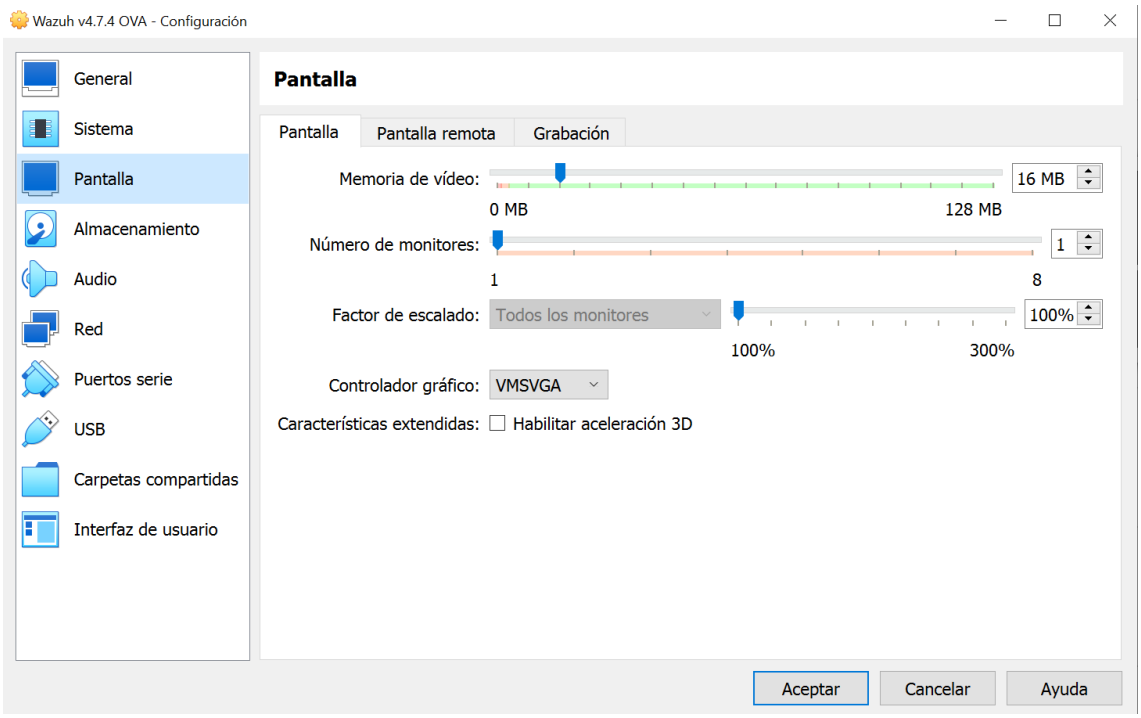
- Documento PDF con todas las capturas de pantalla y descripciones detalladas.

El proceso de implementación de Wazuh se ha realizado instalando la OVA, dado que me resultaba interesante poder disponer de esta herramienta de manera indefinida, ya que si lo hacíamos en Wazuh Cloud este tenía un periodo de prueba gratuito de 14 días.

Así que nos descargamos la OVA de la página oficial de Wazuh:

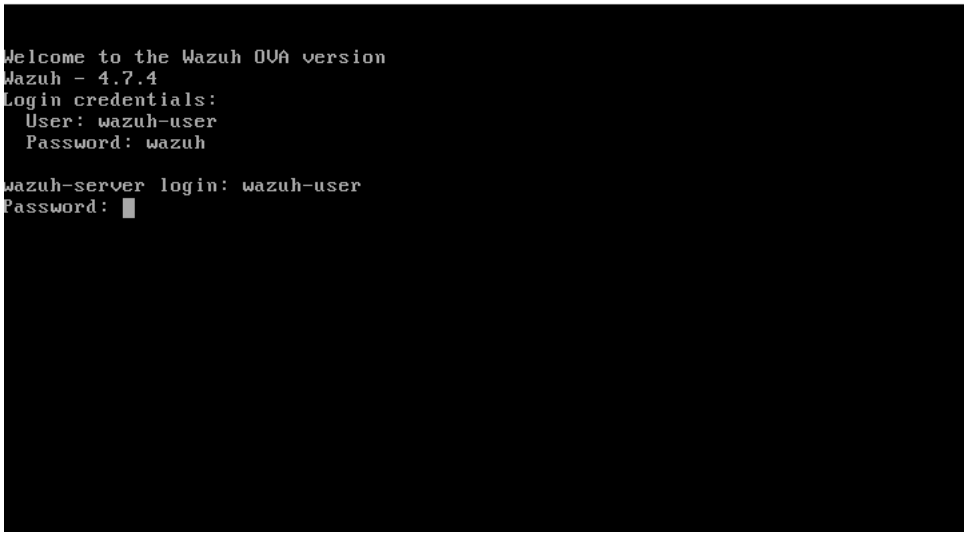


Importamos la OVA en nuestra máquina virtual. El único cambio que debemos realizar es seleccionar el controlador gráfico a VMSVGA, el resto viene por defecto bien configurado:



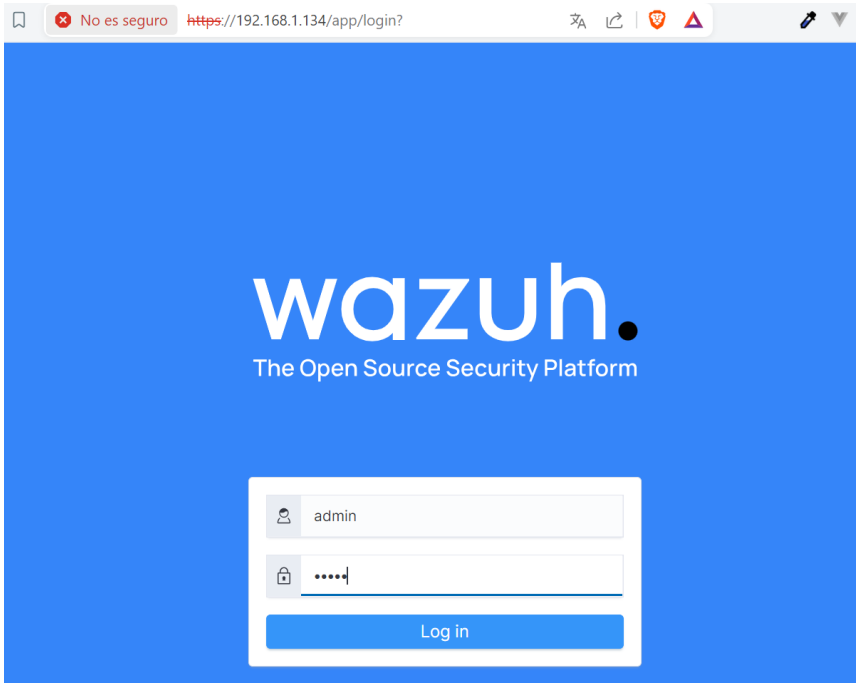
Arrancamos el proceso de instalación. Introducimos el nombre de usuario “wazuh-user” y “wazuh” como contraseña.

Aquí nos hemos encontrado con un problema porque no se encontraba el símbolo “-“, ya que no estaba en la tecla que corresponde sino en la tecla del símbolo de interrogación.



Aplicamos el comando “ip a” para mostrar la IP del servicio Wazuh:

Copiamos la IP: 192.168.1.134 y la pegamos en nuestro navegador:

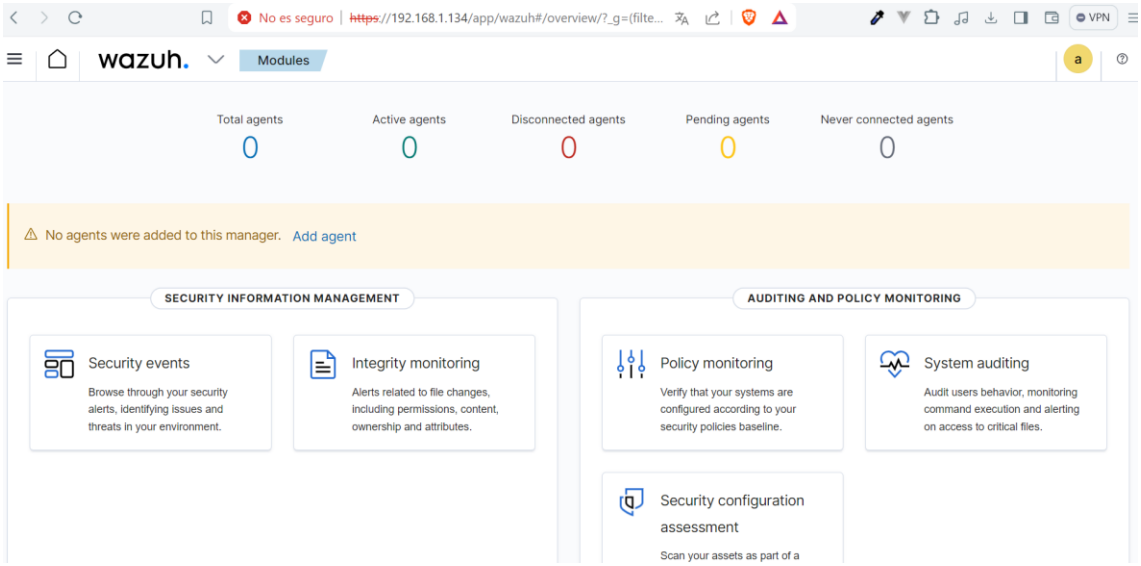


Nombre de usuario: admin

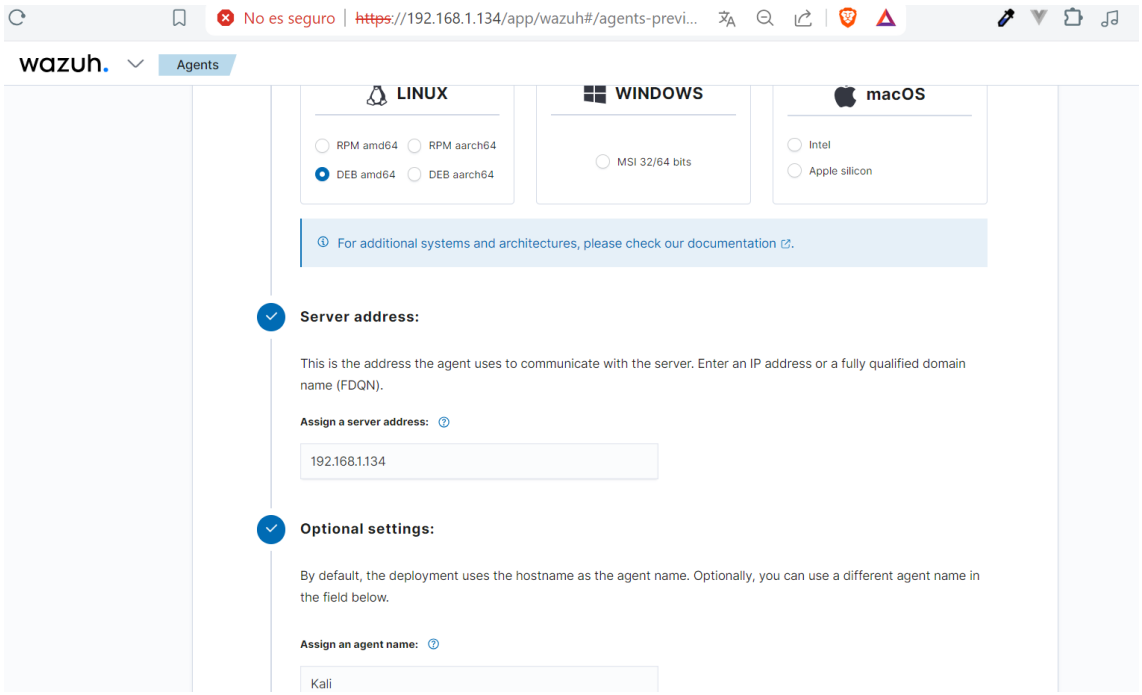
Contraseña: admin

Luego, estas credenciales se deben cambiar desde la plataforma.

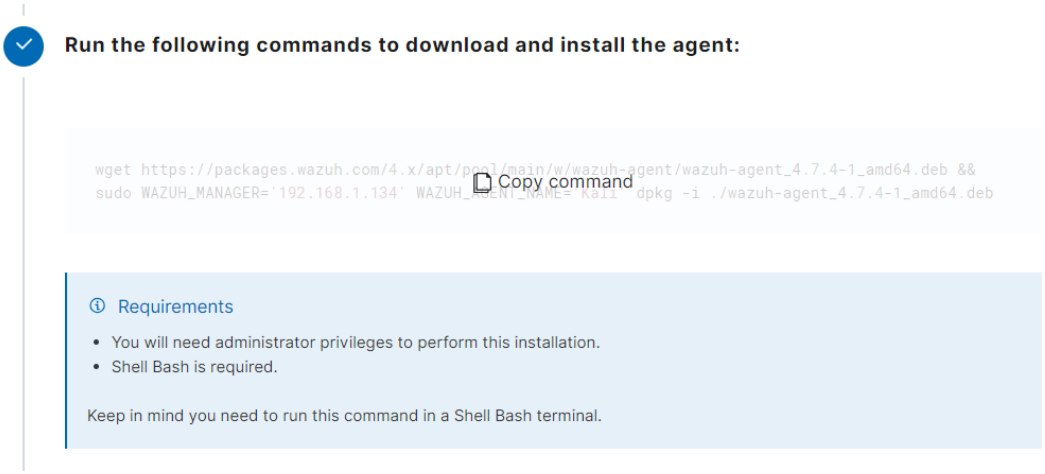
Una vez dentro le damos a “Add agent”:

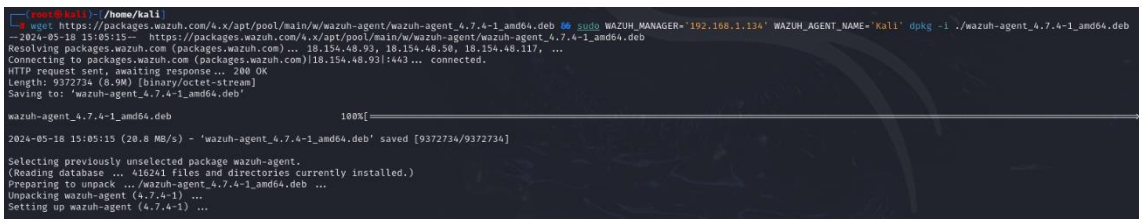


Seleccionamos Wazuh para Linux, escribimos la dirección IP que se le asignó a Wazuh en la máquina virtual y le asignamos un nombre al agente:

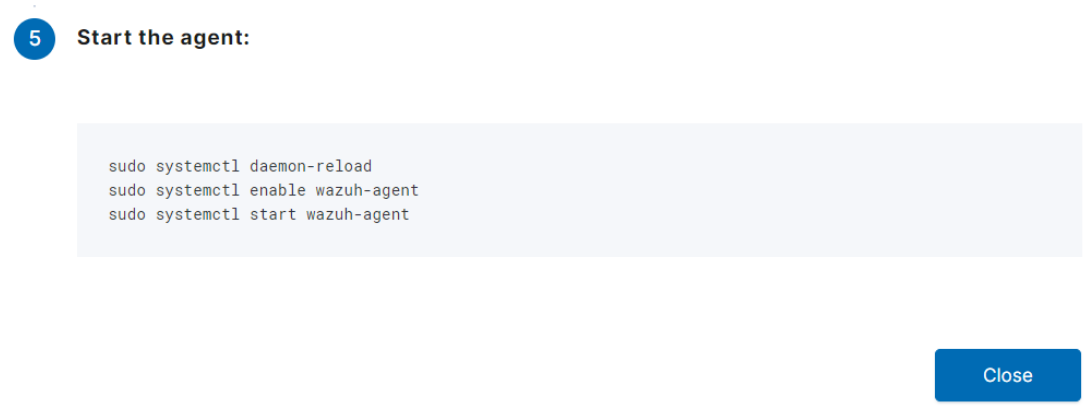


Copiamos el siguiente comando en la consola de Kali:



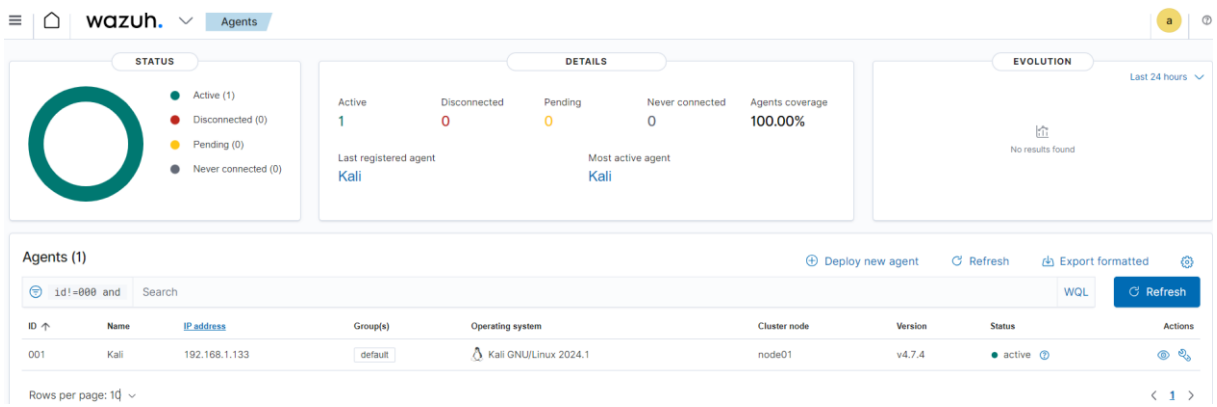


Y ahora iniciamos el agente copiando este otro comando:




```
┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.
```

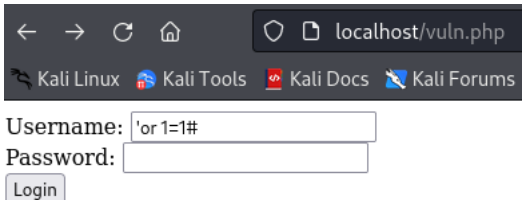
Volvemos a la pantalla inicial de wazuh y vemos como se ha agregado correctamente el agente:

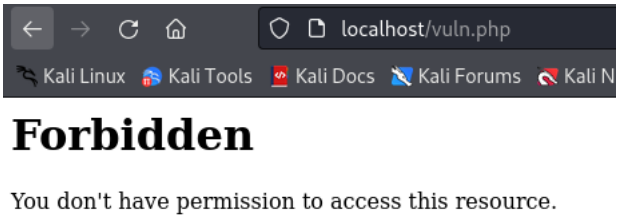


Inicializamos *apache 2, mariadb, security2 y headers* en Kali Linux:

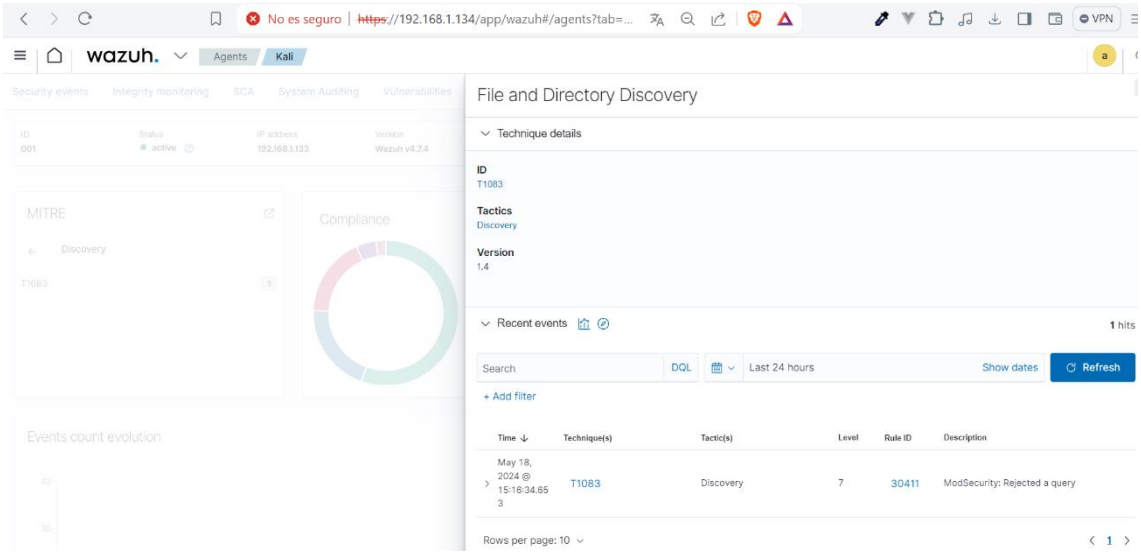
```
┌──(root㉿kali)-[/home/kali]
└─# systemctl start apache2

┌──(root㉿kali)-[/home/kali]
└─# systemctl start mariadb

┌──(root㉿kali)-[/home/kali]
└─# a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled

┌──(root㉿kali)-[/home/kali]
└─# a2enmod headers
Module headers already enabled
```

Realizamos una inyección de código para intentar lograr un login exitoso sin conocer las contraseñas. Esto lo haremos en el archivo vuln.php accesible desde el navegador de Kali.



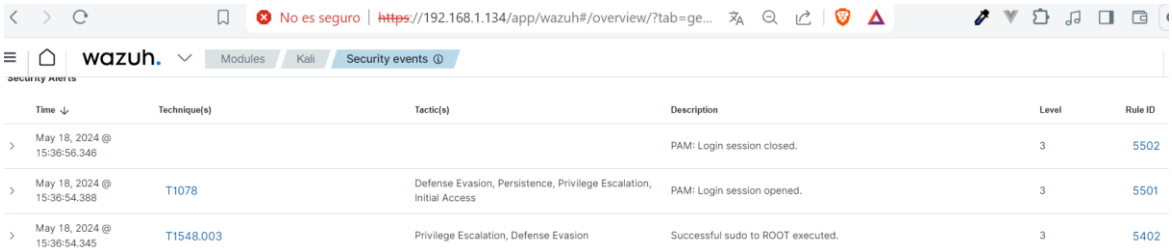


Ahora vamos al dashboard de Wazuh y vemos que nos aparece la alerta de seguridad de Modsecurity, el bloqueo al intento de login anterior:

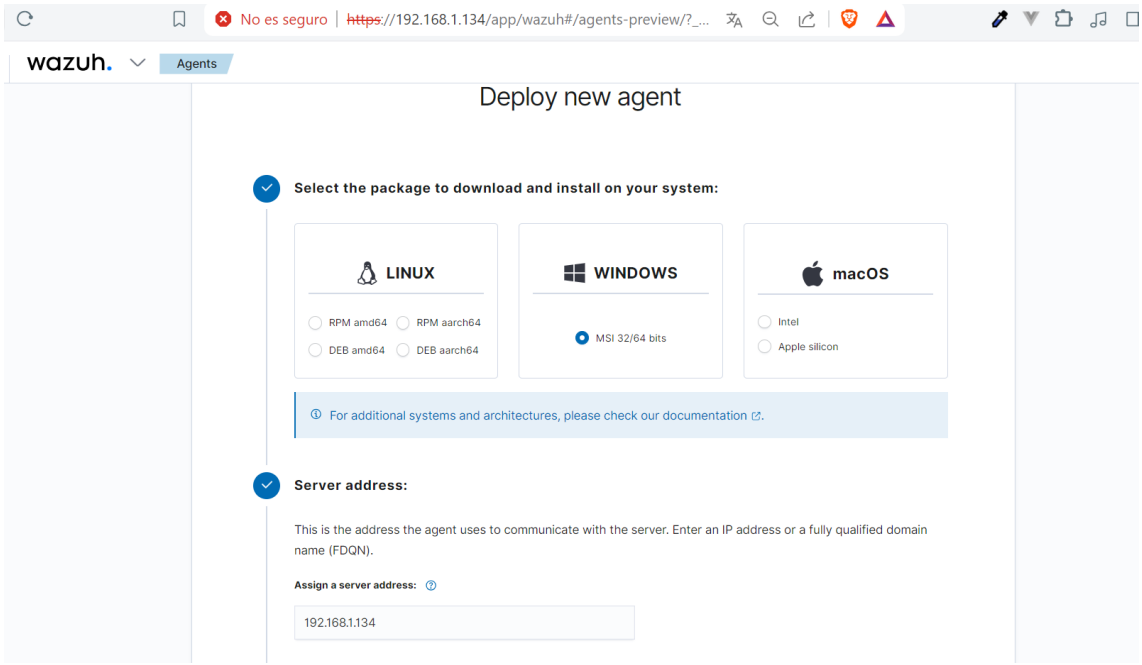


Vemos que nos salen alertas de seguridad de cada proceso que realizamos en Kali. Iniciamos *Snort* en nuestro Kali y corroboramos este evento en las alertas de seguridad.

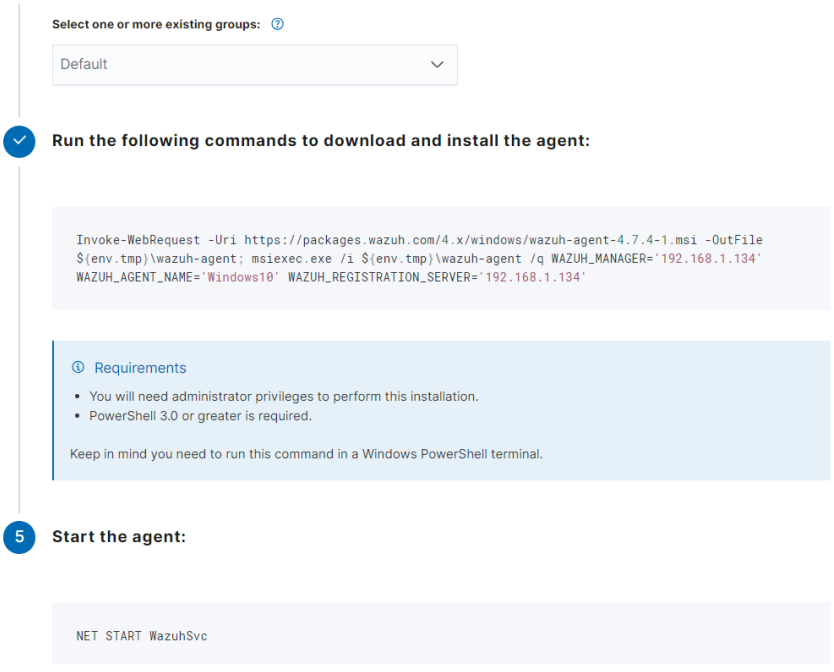
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status snort3-nic.service
[sudo] password for kali:
● snort3-nic.service - Set Snort 3 NIC in promiscuous mode and Disable GRO, LRO on boot
     Loaded: loaded (/etc/systemd/system/snort3-nic.service; enabled; preset: disabled)
     Active: active (exited) since Sun 2024-05-19 23:28:22 CEST; 4min 16s ago
    Process: 724 ExecStart=/usr/sbin/ip link set dev eth0 promisc on (code=exited, status=0/SUCCESS)
    Process: 736 ExecStart=/usr/sbin/ethtool -K eth0 gro off lro off (code=exited, status=0/SUCCESS)
   Main PID: 736 (code=exited, status=0/SUCCESS)
        CPU: 59ms

May 19 23:28:22 kali.bosquempresa.local systemd[1]: Starting snort3-nic.service - Set Snort 3 NIC in promi
May 19 23:28:22 kali.bosquempresa.local systemd[1]: Finished snort3-nic.service - Set Snort 3 NIC in promi
log file:
zsh: suspended  sudo systemctl status snort3-nic.service
```



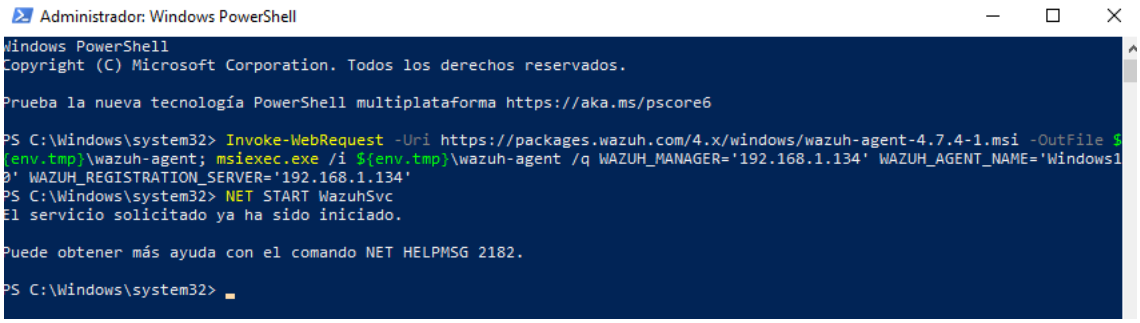
Ahora vamos a Deploy New Agent y haremos lo mismo para Windows 10:



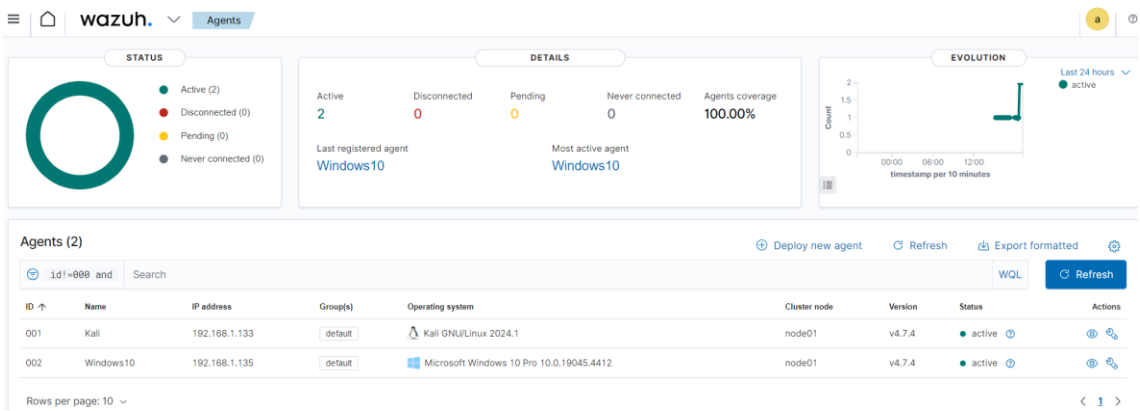
Copiamos el siguiente comando en el powershell de Windows 10 ejecutándolo como administrador:



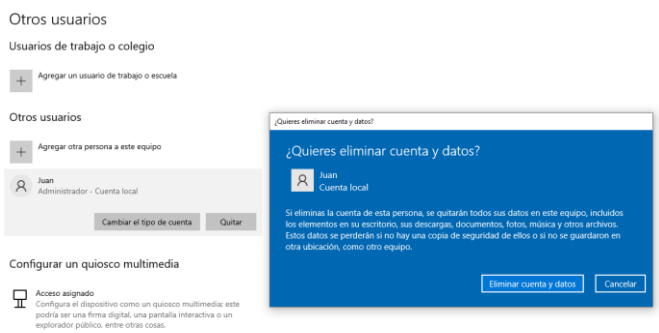
Una vez finaliza, inicializamos el agente escribiendo el comando “NET START WazuhSvc”:



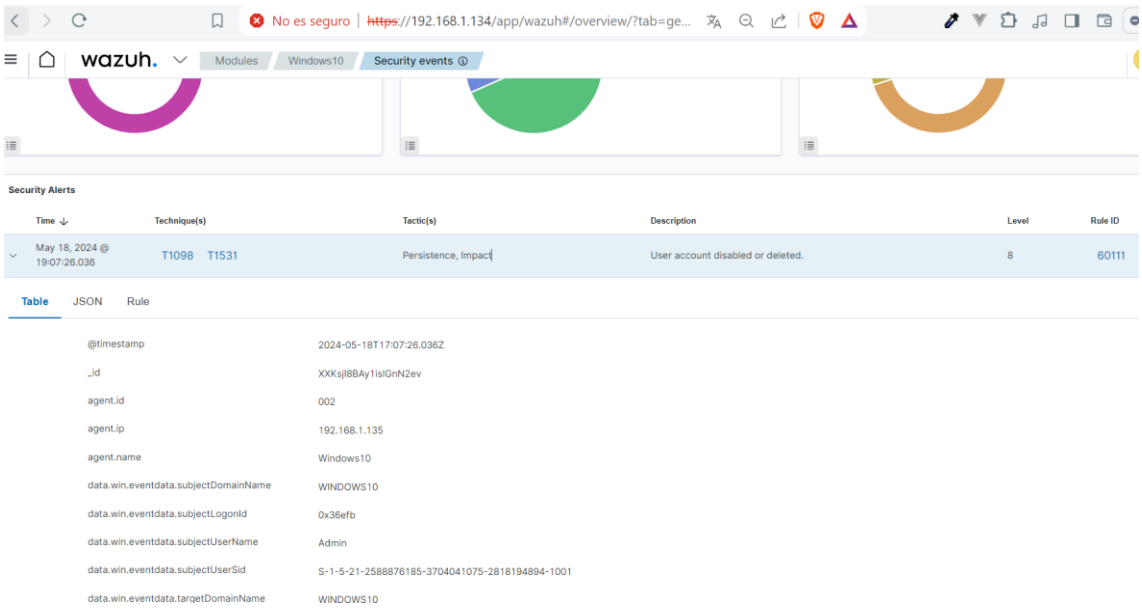
Ahora, en el dashboard de Wazuh, vemos como se han instalado correctamente los dos agentes:



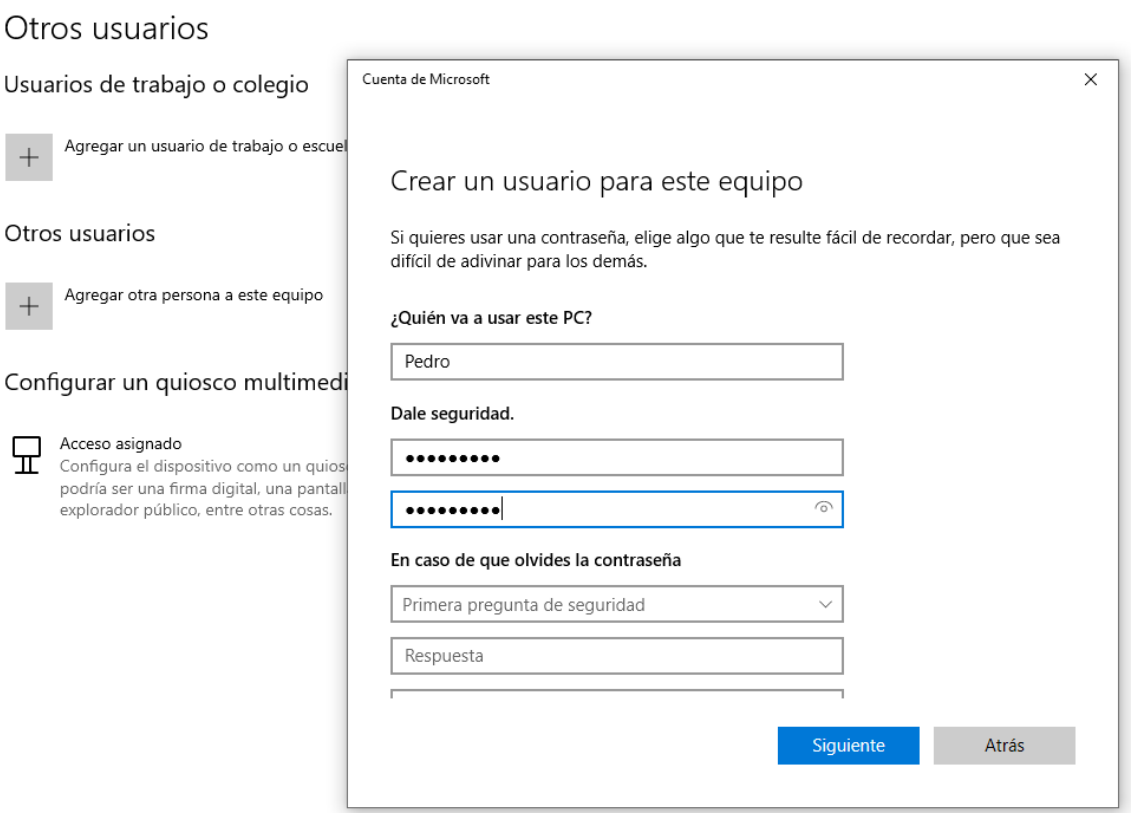
Eliminamos el usuario Juan creado en nuestra máquina virtual Windows 10 para que se genere actividad:



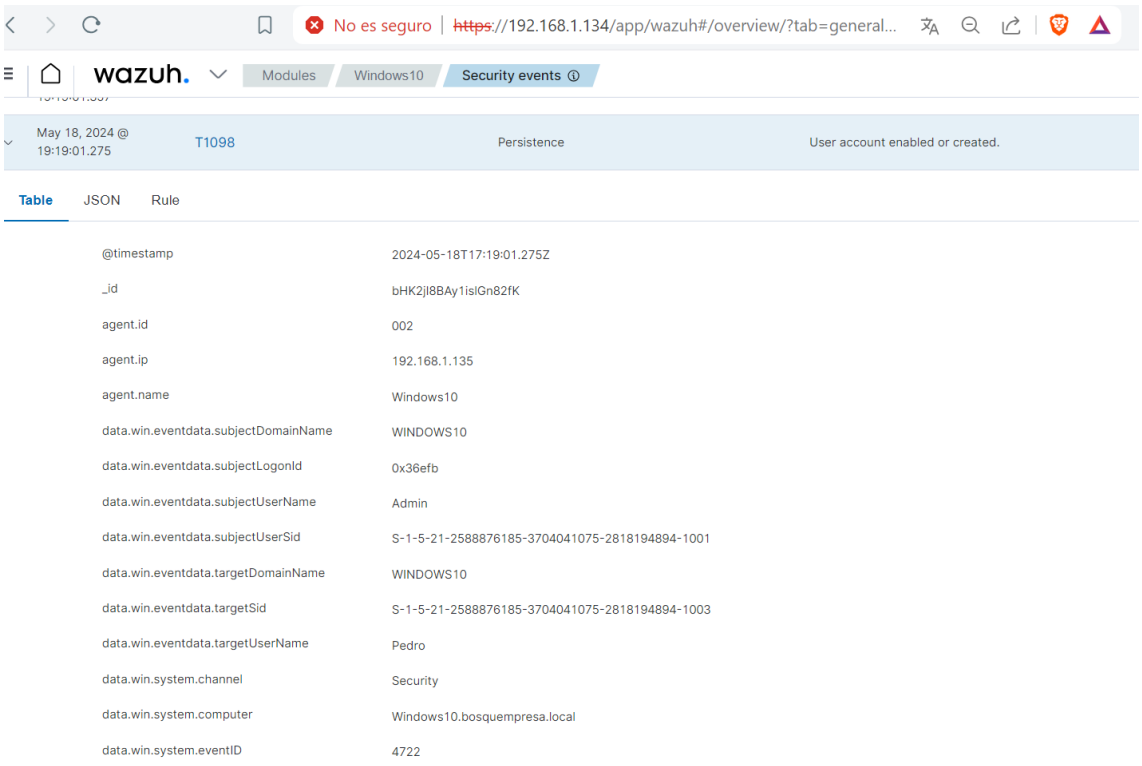
Comprobamos que se haya creado la alerta de seguridad correctamente:



Creamos un usuario llamado Pedro en nuestra máquina virtual Windows10 para generar otra alerta de seguridad:

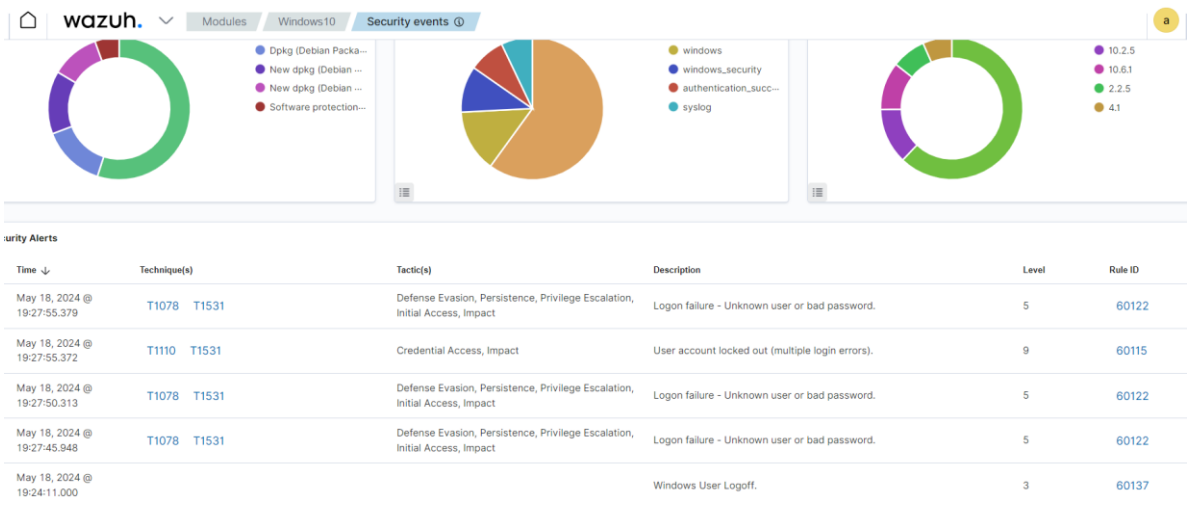


Vemos que se ha generado correctamente la alerta de la creación de una nueva cuenta, indicándonos el nombre del usuario creado:



Por último, cerraremos sesión y volveremos a intentar iniciar sesión en nuestro Windows 10 de la máquina virtual, probando varios inicios de sesión hasta bloquear la cuenta.

Comprobamos, y vemos que se han creado correctamente todas estas alertas de seguridad:



Buen trabajo 10/10