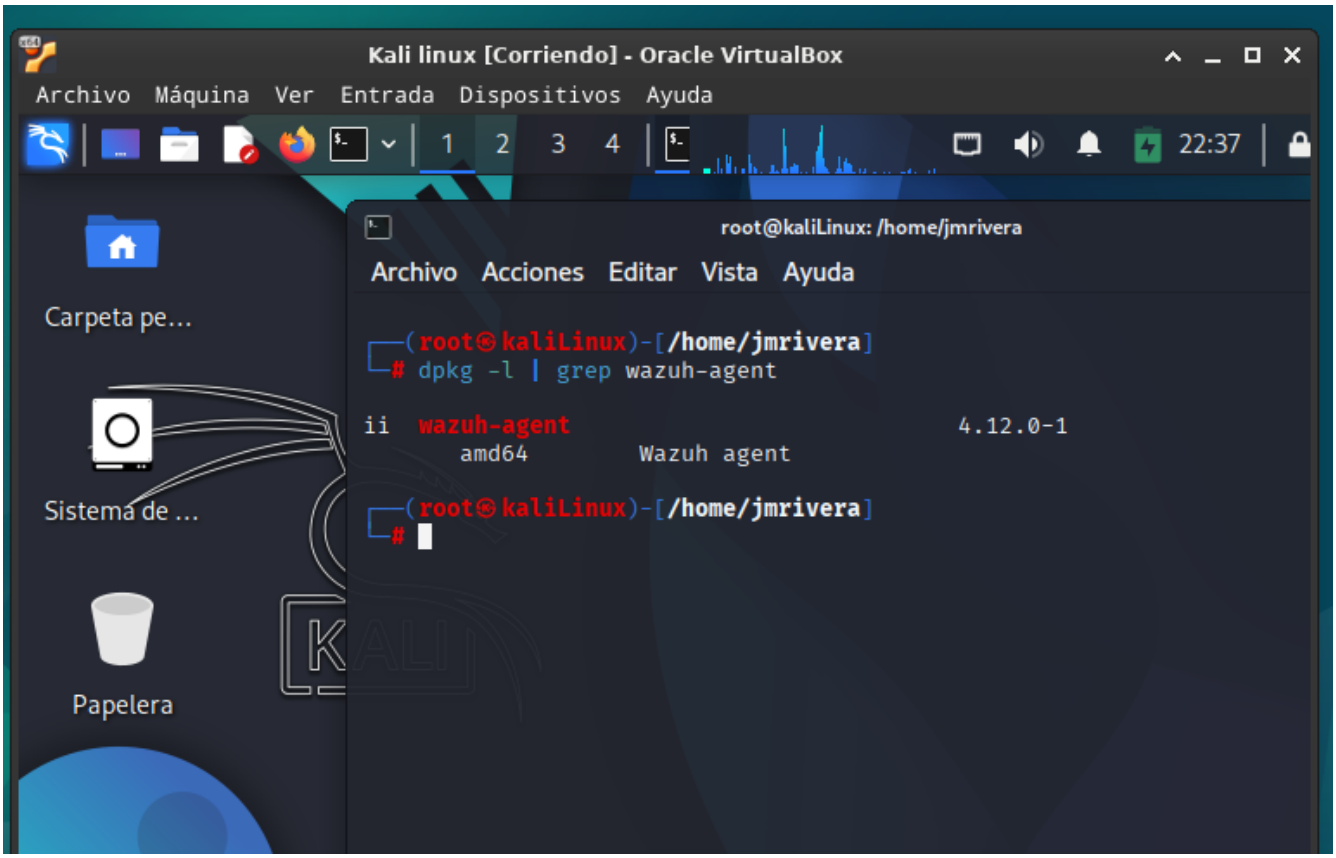
Desafío Prevención y detención de intrusiones
Seguridad en Redes de Datos
José Miguel Rivera

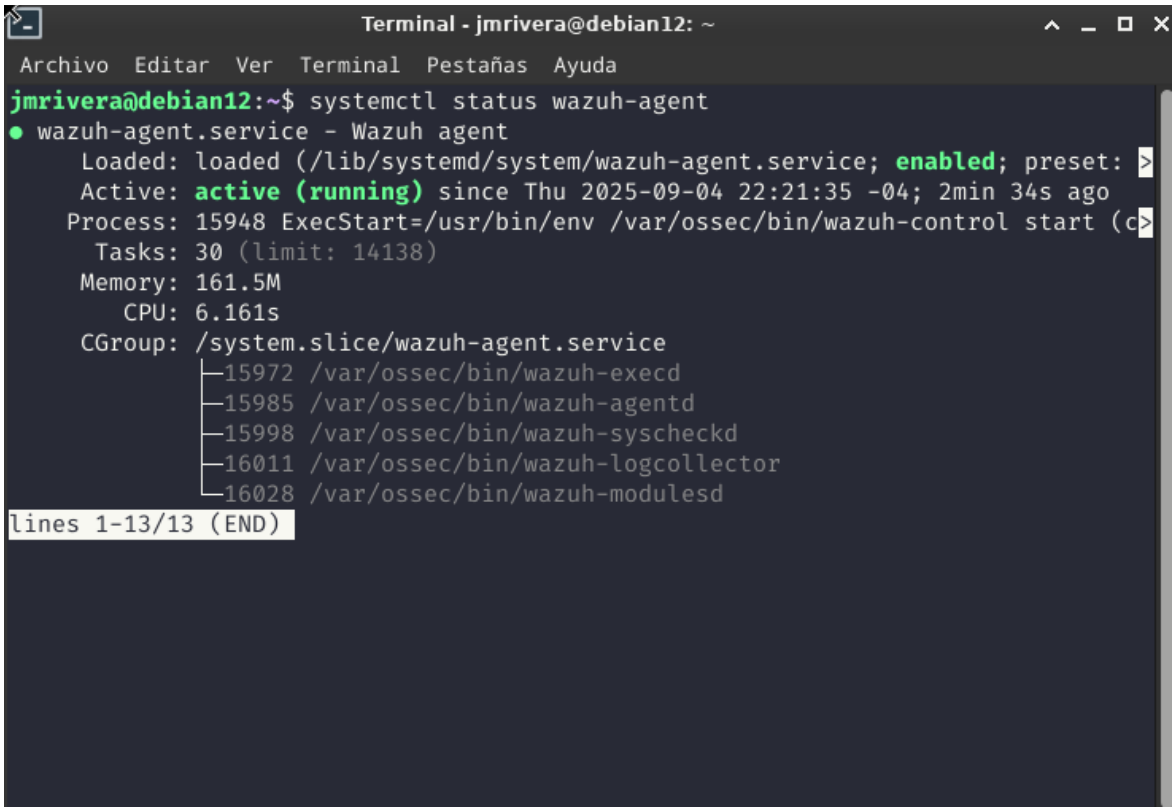
---

1. Generar la evidencia que demuestre la instalación de servidor WAZUH en servidor Kali Linux. (2 Puntos)

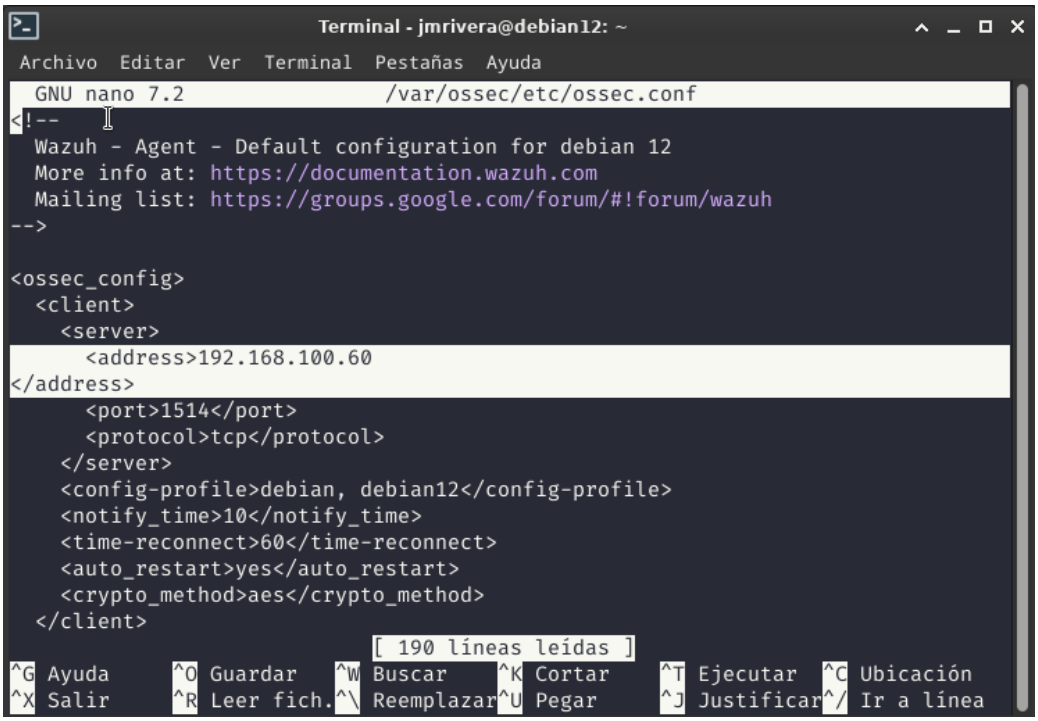


2. Generar evidencia que demuestre la instalación de agente WAZUH en equipo Windows. (2 Puntos)

Se realiza instalación de agente Wazuh en equipo Debian 12 usado como sistema anfitrión.

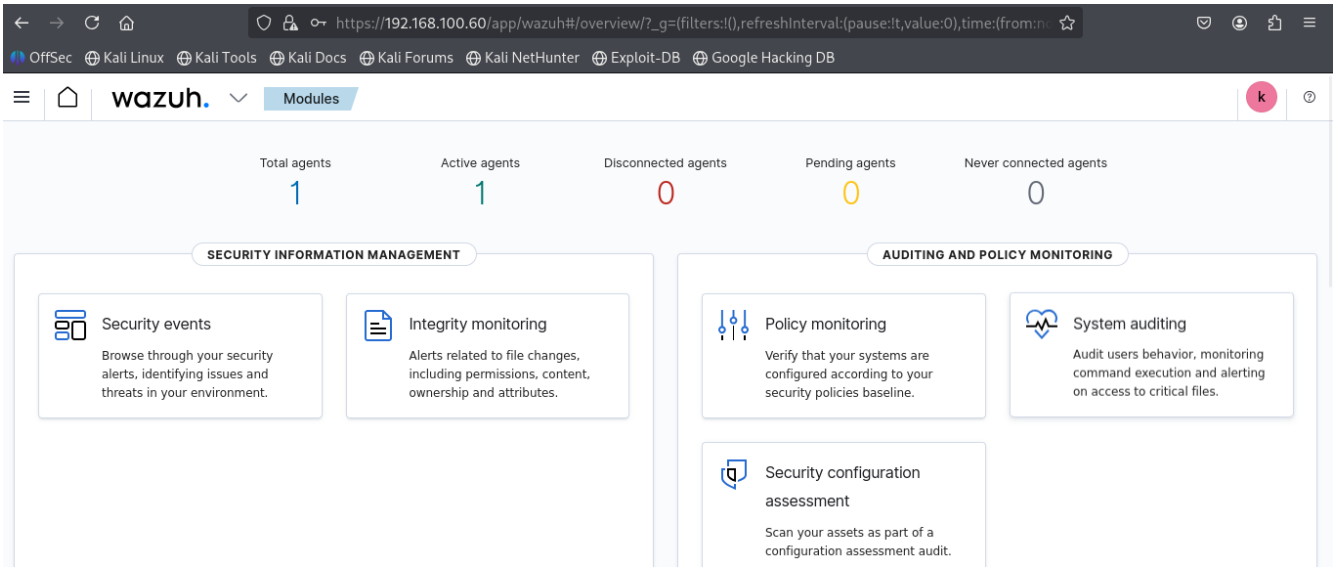


Se configura la IP local del servidor remoto Kali Linux 192.168.100.60

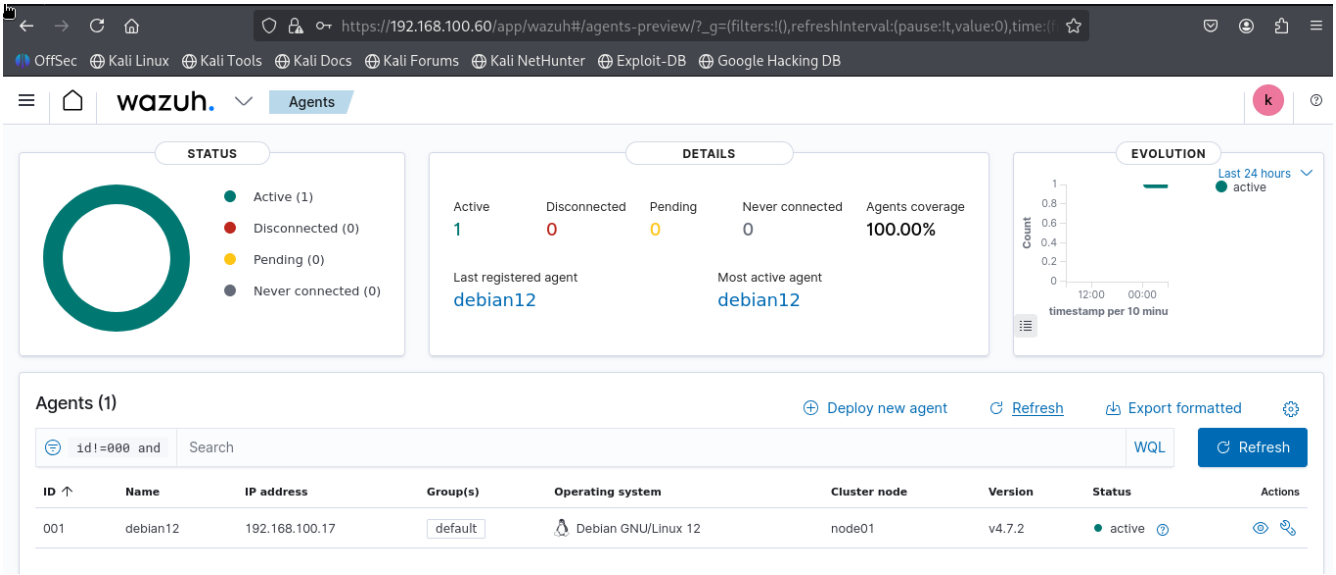


3. Generar evidencia que demuestre la sincronización entre el agente WAZUH Windows y el servidor WAZUH en Kali Linux. (3 Puntos)

Dashboard de Wazuh validado el acceso



confirmación del agente debian12 (mi pc)



4. Generar evidencia de alertas que ha encontrado WAZUH en el equipo, muéstrelas y explique por qué la clasificación de la severidad. (3 Puntos)

Se verifican alertas por intentos de modificación de archivos importantes con clave de root, definido con valor 7 (importante)