Desafío - Detección y prevención de intrusiones

En este desafío validaremos nuestros conocimientos de configuración de un sistema de detección de intrusos y alertas respectivas. Para lograrlo, necesitarás aplicar los requerimientos solicitados.

Lee todo el documento antes de comenzar el desarrollo **individual** para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

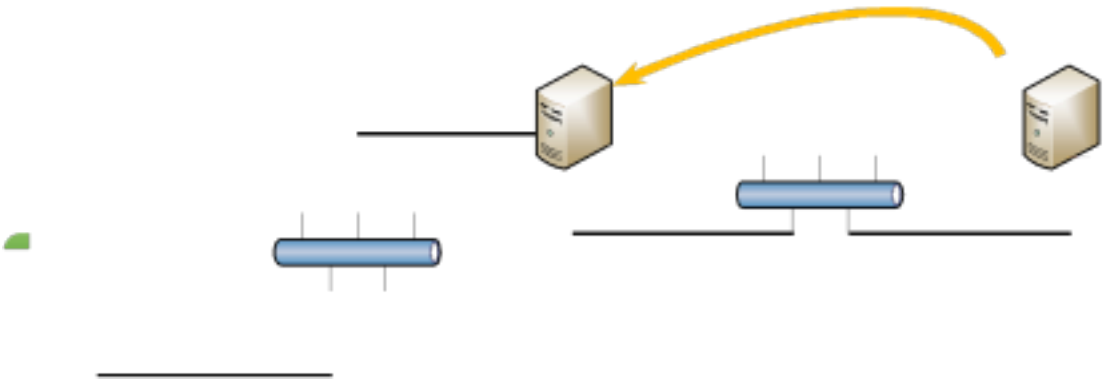
// Tiempo asociado: 1 hora cronológica

Descripción

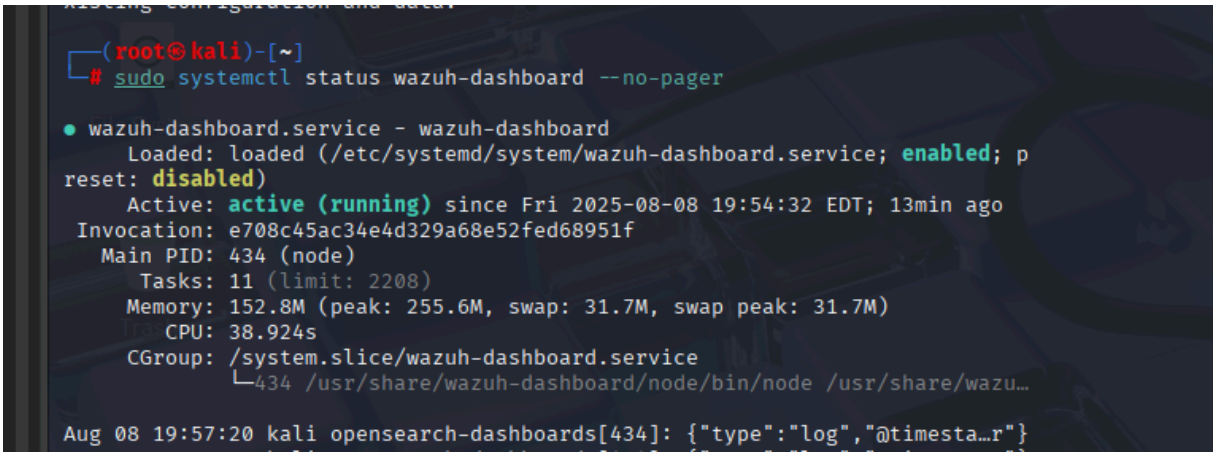
Una empresa ha decidido implementar un sistema de detección de intrusos basado en host para determinar las alertas generadas por sus usuarios cuando realizan modificaciones en el sistema operativo. De esa manera comenzar con la implementación de soluciones más restrictivas que permita tener un control más completo de la red.

Requerimientos

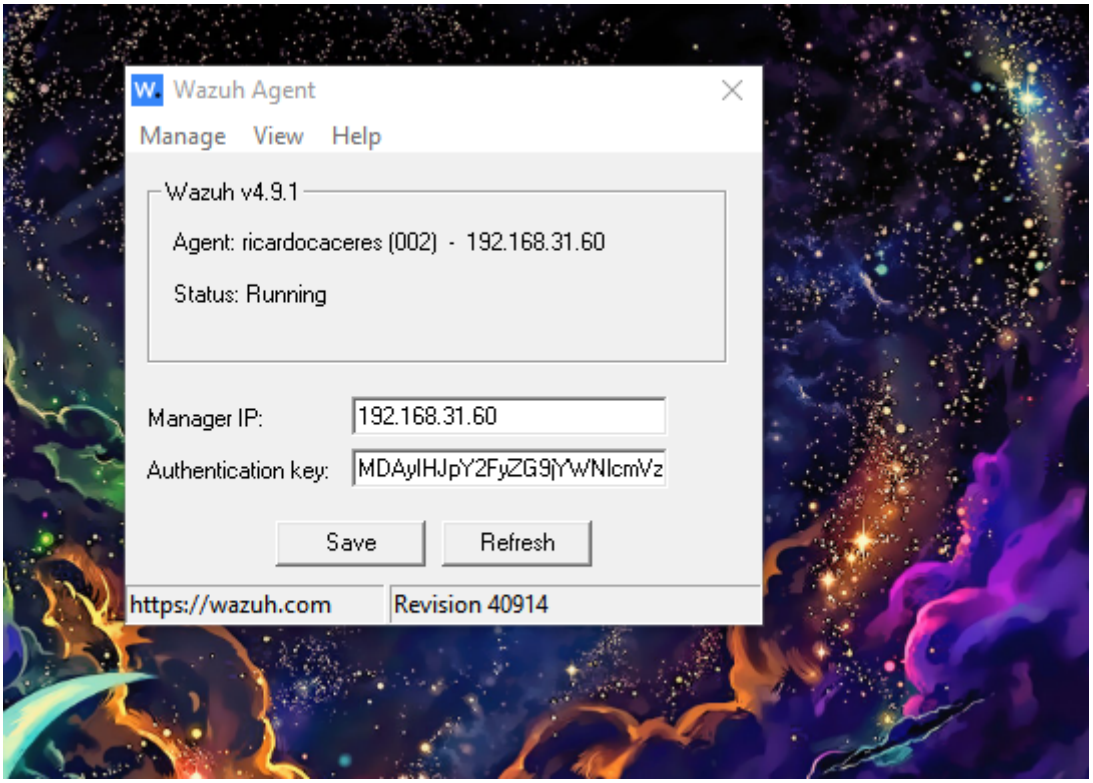
Utilizar la siguiente topología como referencia:

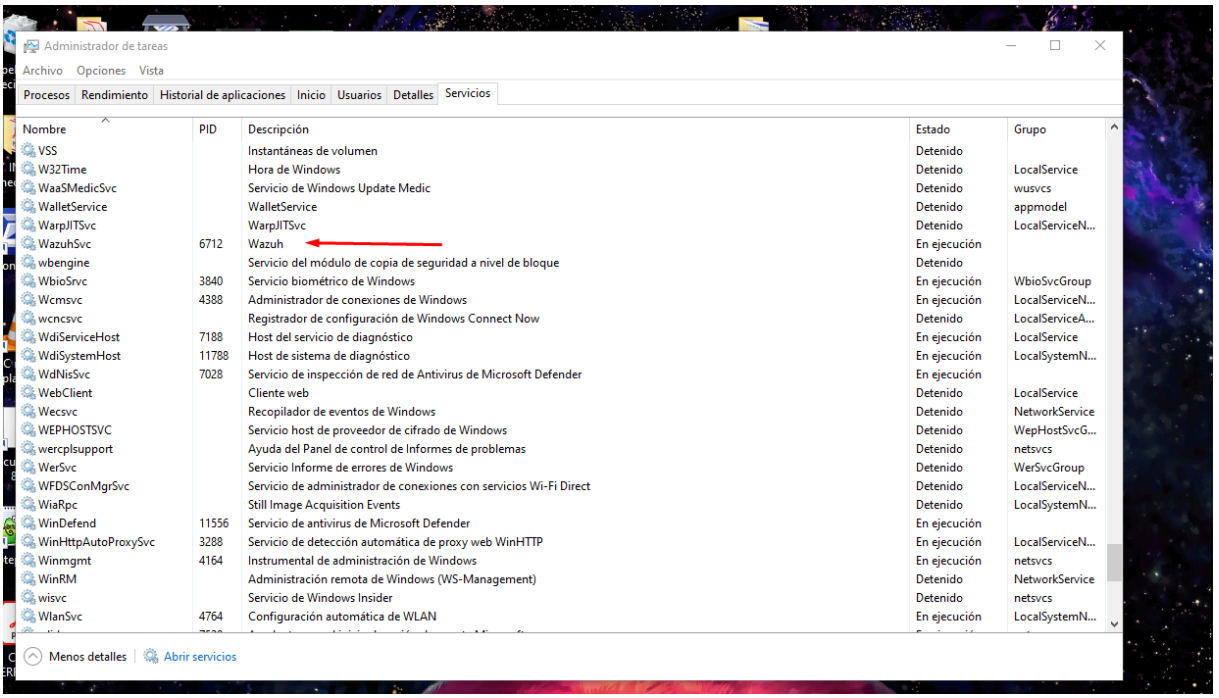


1. Generar la evidencia que demuestre la instalación de servidor WAZUH en servidor Kali Linux. (**2 Puntos**)

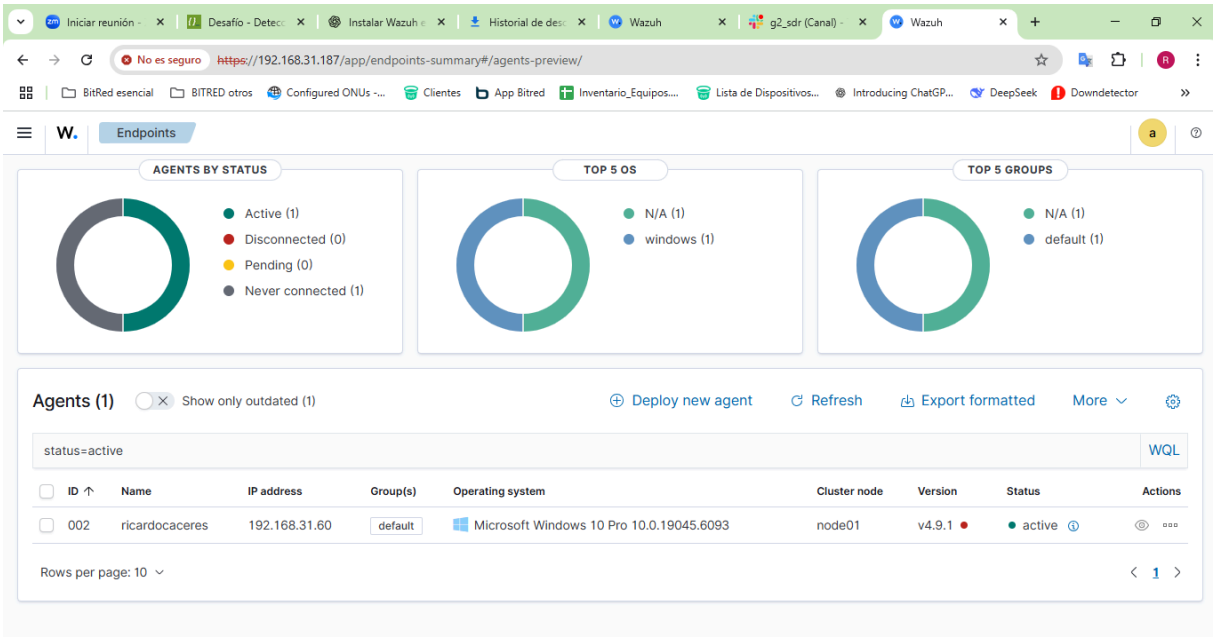


2. Generar evidencia que demuestre la instalación de agente WAZUH en equipo Windows. (**2 Puntos**)





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



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

(**3 Puntos**)

En el agente DESKTOP-RJION8D se registraron 8 intentos fallidos de inicio de sesión en las últimas 24 horas. Estos eventos fueron detectados por Wazuh a partir de los registros de seguridad de Windows.

La severidad fue clasificada como Media, porque varios intentos fallidos pueden deberse a un error del usuario, pero también pueden indicar un posible intento de acceso no autorizado. Aunque no confirman un ataque, representan un riesgo que debe revisarse para evitar amenazas como ataques de fuerza bruta o intrusiones.