Tarea #983 Realizar el hardening de un CentOS7 y validar su configuración de seguridad con Wazuh.

Israel Alejandro Cel Alcocer

Seguridad de Datos

Docente: Ismael Jimenez

Instrucciones

0.- Ya deben tener instalado Wazuh
1.- Instalar CentOS 7 minimal en VirtualBox
2.- Instalar agente de Wazuh en el CentOS 7
3.- Tomar evidencia (Screenshot) del estado de hardening de su instalación de CentOS 7, debe verse el 41% y que es su máquina.
4.- Aplicar script de hardening de CentOS7 de mi repo hardening en github
5.- Tomar evidencia (Screenshot) del estado de hardening de su instalación de CentOS 7, debe verse el 68% . Entregar el 2 de Mayo de 2024

Pasos a seguir

Preparación del Entorno: Se descarga la imagen ISO de CentOS 7.7 y se crea una máquina virtual usando VirtualBox. Se elige la configuración mínima durante la instalación y se configura la red, incluyendo el ajuste de la tarjeta en modo puente para la conectividad a Internet.

Instalación de CentOS: Durante la instalación, se establece la configuración regional, zona horaria y configuración del teclado. Se selecciona la fuente de instalación y el software (versión mínima), y se configura el destino de instalación y la red.

Configuración Post-Instalación: Posteriormente se configura el usuario administrador y se establece la contraseña. Se termina la instalación y se procede a reiniciar la máquina para completar la configuración.

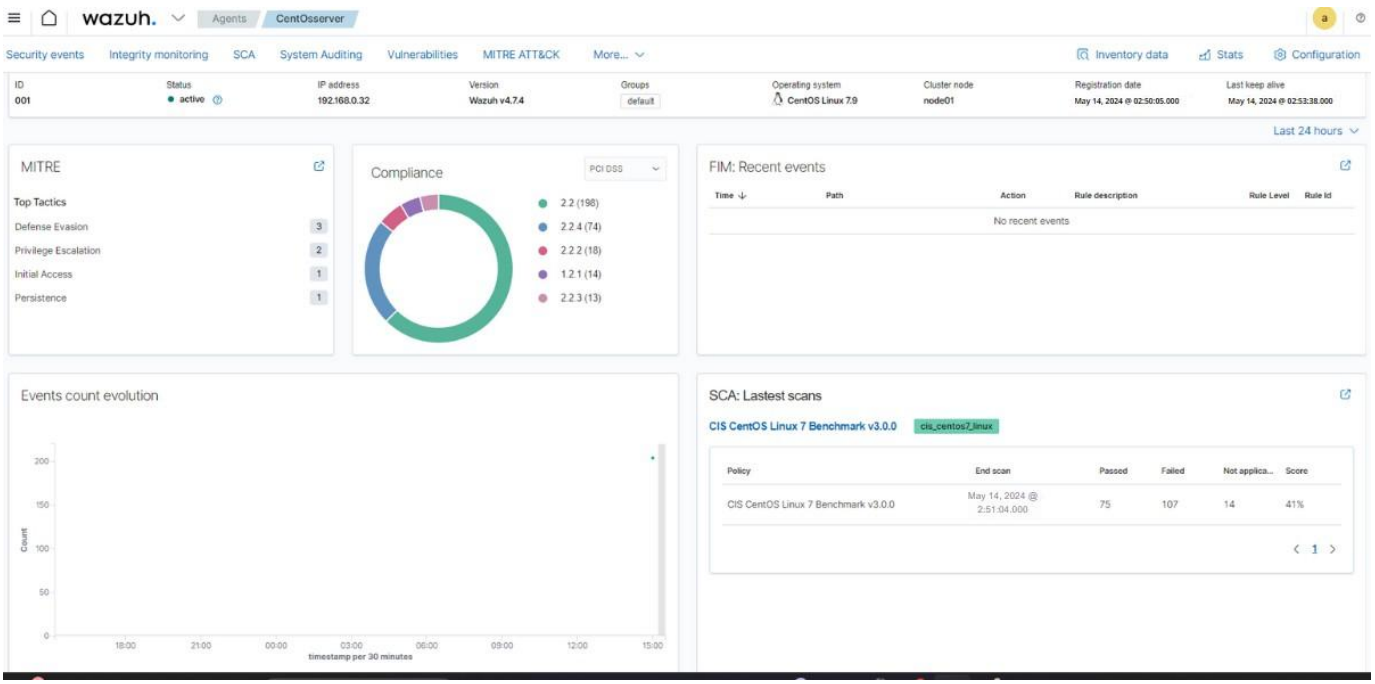
Configuración de Wazuh Agent: Se instala y configura el agente de Wazuh en CentOS para monitorizar el estado de hardening del sistema operativo. Se añade el servidor CentOS al Wazuh Manager.

Aplicación del Script de Hardening: Se ejecuta un script diseñado para aplicar las recomendaciones de hardening del CIS. Este script ajusta varias configuraciones de seguridad del sistema, como servicios innecesarios y configuraciones de permisos.

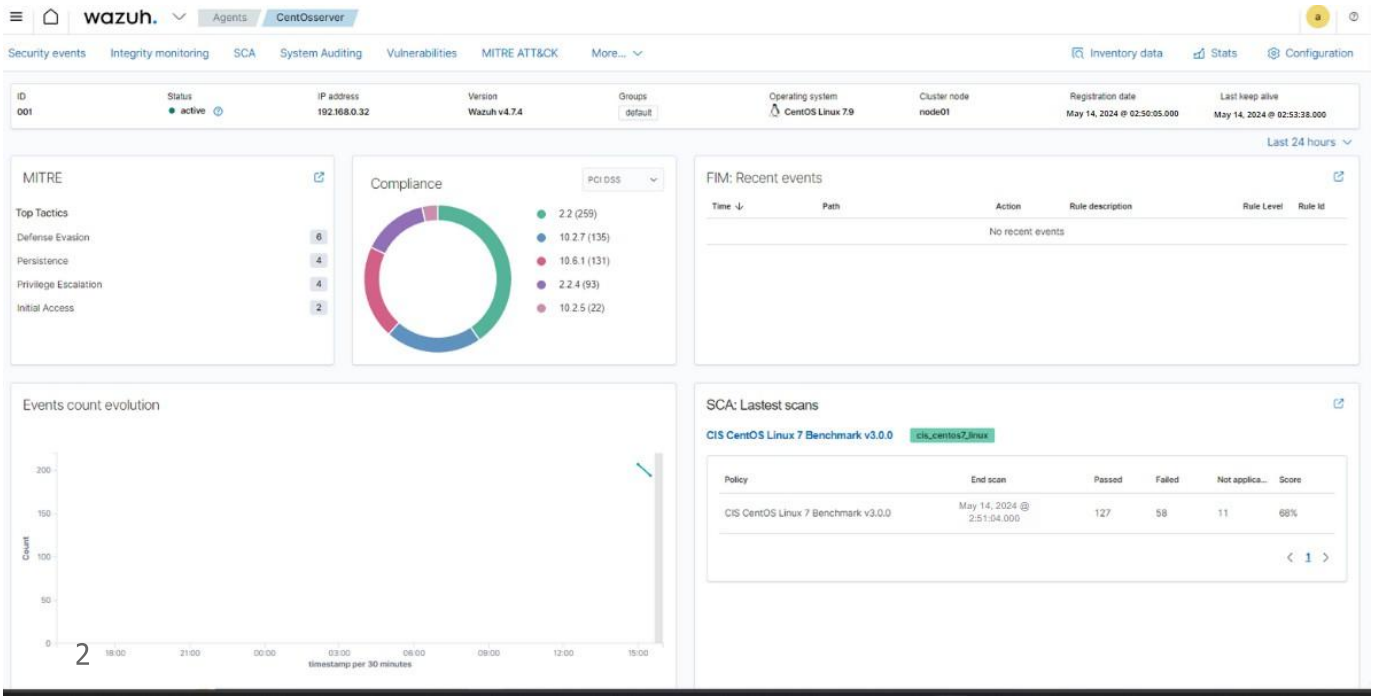
Verificación y Ajustes: Después de ejecutar el script, se revisa el sistema con las herramientas de Wazuh para evaluar qué configuraciones han sido correctamente aplicadas y cuáles requieren revisión. Se ajustan algunas configuraciones adicionales manualmente basándose en los resultados y recomendaciones del CIS.

Resultados del Hardening: Al final, se revisa el porcentaje de cumplimiento con las recomendaciones del CIS, haciendo ajustes adicionales según sea necesario para mejorar la seguridad del sistema.

Captura del 41%



Captura del 68%



Script

El proceso descrito implica la configuración y monitorización del hardening de un sistema CentOS usando un script diseñado para seguir las recomendaciones del benchmark de CIS (Center for Internet Security). Este script ajusta múltiples configuraciones del sistema para mejorar la seguridad, tales como servicios innecesarios, configuraciones de permisos, y políticas de seguridad.

Ejecución del Script de Hardening: El script de hardening se aplica para ajustar las configuraciones del sistema basándose en las recomendaciones del CIS. Se cubren aspectos como deshabilitar servicios no necesarios, ajustar permisos de archivos y configurar políticas de seguridad.

Verificación y Ajustes Adicionales: Después de aplicar el script, se utiliza Wazuh para verificar las configuraciones del sistema. Se identifican áreas donde el script ha sido efectivo y otras donde no aplicó debido a limitaciones del sistema o porque el script estaba desactualizado respecto a la versión más reciente del CIS.

Actualización y Mantenimiento del Script: Se observa que el script necesita actualizaciones para alinearse completamente con las últimas versiones del benchmark de CIS. Esto implica modificar y agregar comandos específicos para asegurar que todas las recomendaciones relevantes se implementen correctamente.

Resultados del Hardening: Al final del proceso, se logra un aumento significativo en el cumplimiento de las normas de CIS, aunque algunos aspectos requieren intervención manual para resolver problemas específicos relacionados con la configuración o la falta de ciertos archivos.

El script de hardening es una herramienta crucial para aumentar la seguridad del sistema operativo CentOS, pero requiere mantenimiento y actualización continua para asegurar su efectividad completa conforme evolucionan las normas de seguridad.