Monitoreo de la integridad de archivos en Wazuh

1. Objetivo. – Realizar cambios de integridad de un archivo, para generar los eventos correspondientes y lograr visualizarlos en Wazuh.

2. Herramientas. – Para este laboratorio se utilizaron:

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

3. Metodología / Análisis realizado

Esta sección enfoca la detección y el monitoreo de eventos de creación, modificación y eliminación de archivos, las acciones de contención o mitigación quedan fuera del alcance del presente laboratorio.

3.1 Configuración de directorios

Se añadió los diferentes directorios requeridos en el archivo ossec.conf del agente Windows, con el fin de permitir a Wazuh el acceso y monitoreo de cambios en los directorios añadidos. (ver Figura 1).

```
    <!-- 32-bit programs. -->
    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe
$|sethc.exe$|subst.exe$">%WINDIR%\System32</directories>
    <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

    <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

    <!-- Carpetas de usuario. -->
    <directories realtime="yes">C:\Users\horac\Desktop</directories>
    <directories realtime="yes">C:\Users\horac\Downloads</directories>
    <directories realtime="yes">C:\Users\horac\Documents</directories>


    <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

    <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

    <!-- Windows registry entries to monitor. -->
    <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</windows_registry>
    <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</windows_registry>
    <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\comfile</windows_registry>
    <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\exefile</windows_registry>
    <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\piffile</windows_registry>
    <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\AllFilesystemObjects</windows_registry>
    <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Directory</windows_registry>
```

Figura 1. Acceso de Wazuh a las carpetas para su monitoreo.

3.2 Manipulación de archivo

Se creó un archivo en el agente Windows mediante PowerShell, llamado archivooriginal.txt. Posteriormente, se modificó su nombre y contenido, y finalmente se eliminó, generando los eventos a monitorear. (ver Figura 2)

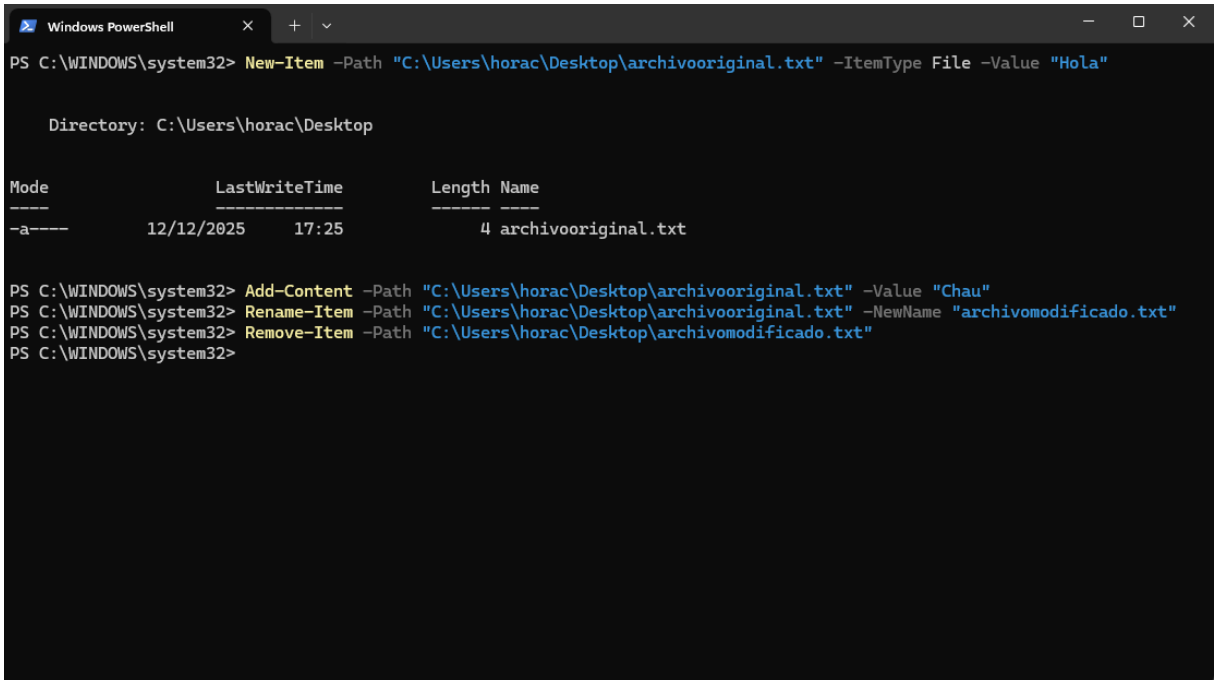

Figura 2. Creación, modificación y eliminación de un archivo.

3.3 Visualización de eventos

Se accedió a la pestaña File Integrity Monitoring → Events en el servidor Wazuh, con el propósito de visualizar los eventos generados por la creación, modificación y eliminación de los archivos en los directorios monitoreados por Wazuh. (ver Figura 3)

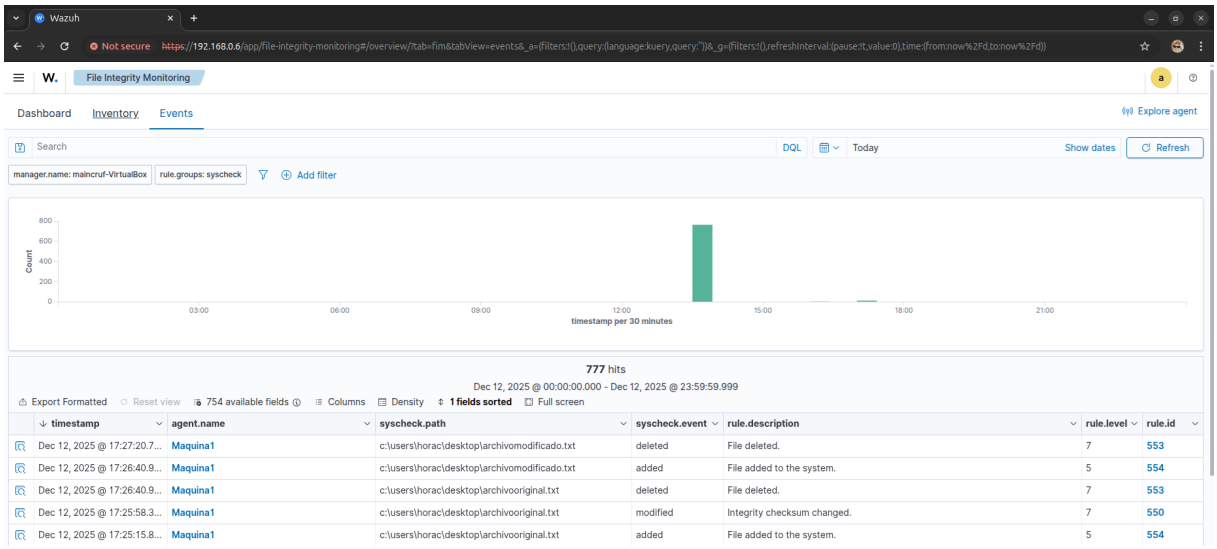

Figura 3. Eventos de creación, modificación y eliminación de archivos Wazuh.

3.4 Interpretación de análisis

3.4.1 Detalles destacados de los eventos

Aunque los detalles completos de los eventos fueron revisados durante el análisis, en el informe se incluyen los campos relevantes:

- Ruta del archivo
- Acción del evento (added, modified, deleted)
- Usuario
- Marca de tiempo
- Tamaño del archivo
- Hash del archivo
- Severidad y regla de Wazuh

3.4.2 Evento de creación

Al revisar los detalles completos del evento, se identificó que el archivo fue creado por el usuario horac en el directorio Desktop. A las 17:25, con un tamaño de 4 bytes. Además, se verificó el hash del archivo para comprobar su integridad y se observó que el evento presenta un nivel de severidad 5, clasificándolo como un evento que requiere atención.

3.4.3 Evento de modificación

Al revisar los detalles completos del evento, se identificó la modificación del archivo perteneciente al usuario horac en el directorio Desktop, a las 17:25, con un tamaño de 10 bytes. Se detectó un cambio en el hash, confirmando la violación de la integridad del archivo, catalogando este evento como crítico.

3.4.4 Evento de eliminación

Al revisar los detalles completos del evento, se identificó la eliminación del archivo que pertenece al usuario horac en el directorio Desktop, a las 17:26, con un tamaño de 10 bytes. Se verificó el hash del archivo eliminado y se observó que el evento presenta un el nivel de severidad 7, catalogando este evento como crítico para la seguridad del sistema.

4. Acciones recomendadas

Ante la detección de eventos de creación, modificación y eliminación de archivos, se recomienda aplicar las siguientes medidas:

- Verificar si la acción fue realizada por un usuario autorizado o por un proceso legítimo.
- Analizar el contexto del evento, qué usuario lo hizo, en que directorio se hizo, cuál es el archivo, etc.
- Correlacionar el evento con otros eventos del sistema, como logs de autenticación o ejecución de procesos.
- Aplicar medidas de contención de acuerdo a los procedimientos de la organización, si se confirma actividad maliciosa.

5. Resultados obtenidos

En este laboratorio se configuraron directorios específicos con el objetivo de monitorear la integridad de los archivos. Además, se generaron eventos de creación, modificación y eliminación de archivos para lograr visualizarlos en Wazuh. Posteriormente, se detectaron y analizaron los eventos, destacando los detalles más relevantes, con el fin de comprender en profundidad los cambios de integridad realizado y mejorar la percepción de la seguridad en el sistema.

6. Reflexión final

Este laboratorio permitió comprender como los cambios no autorizados en archivos importantes pueden formar parte de actividades maliciosas. Además, se evidenció la importancia de contar con un SIEM como Wazuh, capaz de visualizar y monitorear este tipo de eventos, facilitando la detección temprana y la toma de decisiones oportunas en este tipo de casos.