LABWAZUH 3 – Detección de creación/modificación/eliminación de archivos (File Integrity Monitoring FIM)

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

2. Alcance.- Este laboratorio 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. Herramientas. - Para este laboratorio se utilizarán:

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

4. Procedimiento

1. Añadir 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.

2. Crear un archivo en el agente Windows utilizando PowerShell, llamado archivooriginal.txt. Posteriormente, modificar su nombre y su contenido, y finalmente eliminarlo para crear los eventos a monitorear. (ver Figura 2)

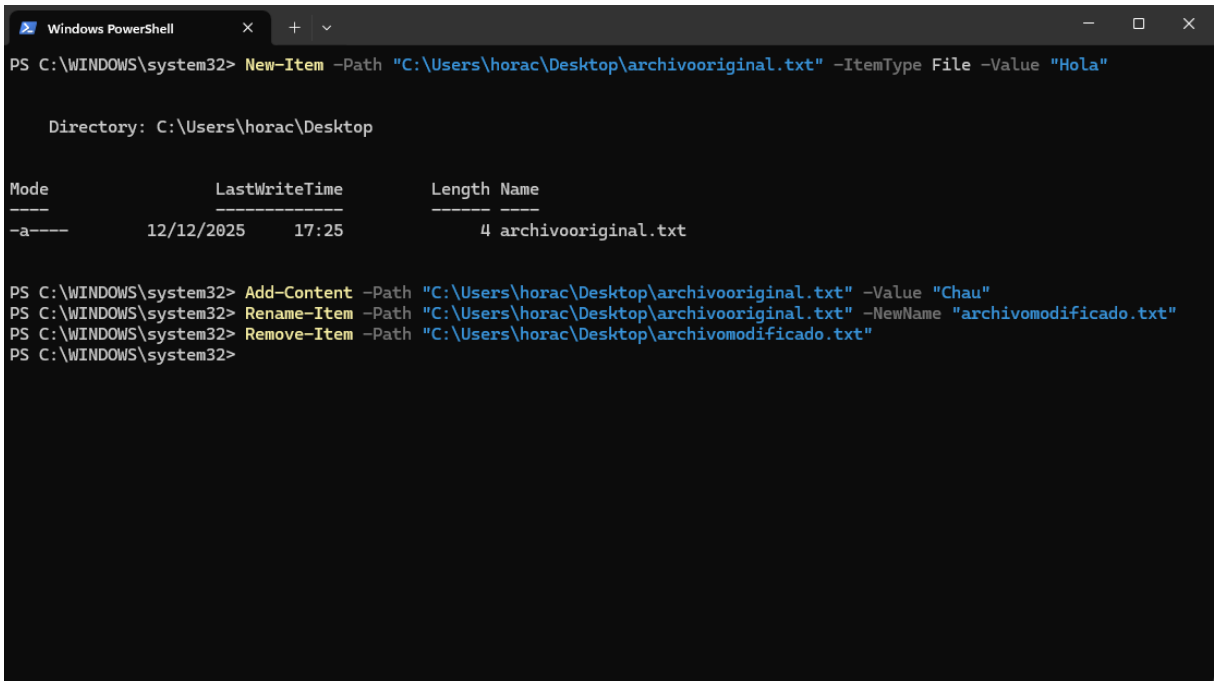

Figura 2. Creación, modificación y eliminación de un archivo.

3. Acceder a la pestaña File Integrity Monitoring → Events en el servidor Wazuh. En esta sección se muestran los eventos generados por la creación, modificación y eliminación de los archivos monitoreados. (ver Figura 3)

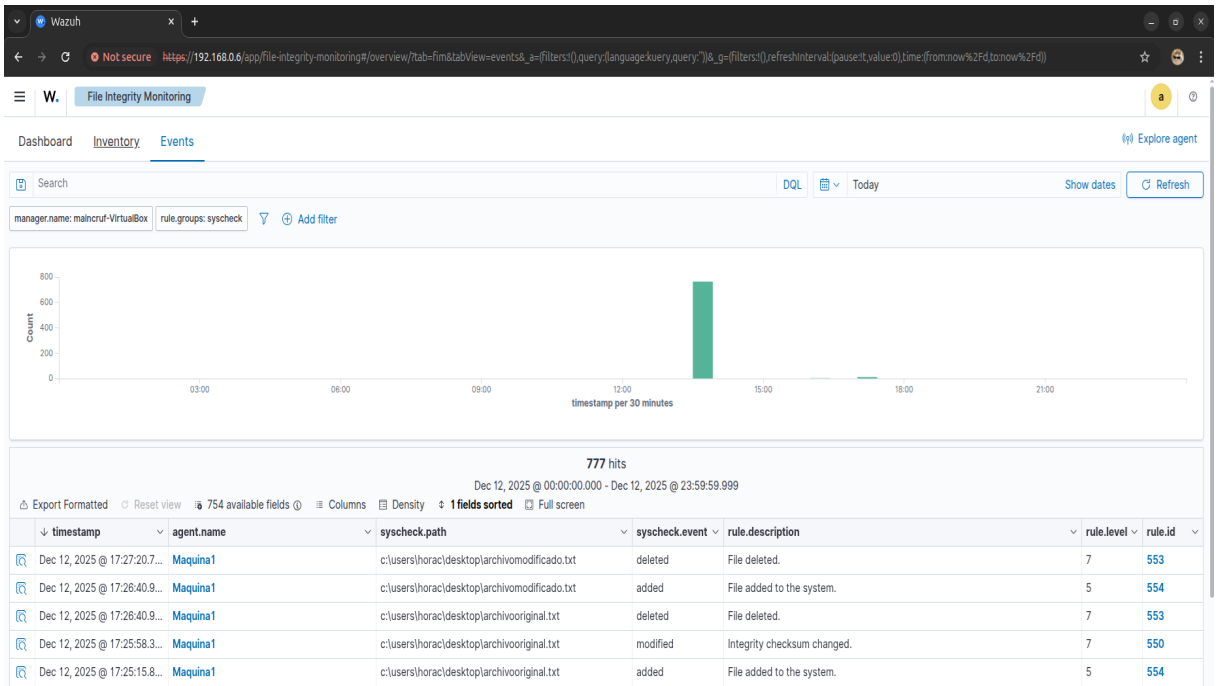

Figura 3. Eventos de creación, modificación y eliminación de archivos Wazuh.

5. 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 legitimo.
- Analizar el contexto del evento, que usuario lo hizo, en que directorio se hizo, cual 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.

6. Resultados Obtenidos. - En este laboratorio se configuró correctamente el archivo ossec.conf en el agente Windows, añadiendo los directorios a monitorear. Como resultado, Wazuh detectó los eventos relacionados a la creación, modificación y eliminación de archivos en los directorios configurados.

7. Reflexión final. – Este laboratorio permitió comprender como los cambios no autorizados en archivos importantes pueden formar parte de actividades maliciosas. Destacando 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.