

LABWAZUH 4 – Ejecuciones sospechosas en PowerShell

1. Objetivo. – Realizar ejecuciones de comandos sospechosos en PowerShell, generando eventos para visualizarlos en Wazuh.

2. Alcance.- Este laboratorio enfoca la detección y el monitoreo de eventos de ejecuciones de comandos sospechosos en PowerShell, 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. Activar la habilitación de creación de procesos (EVENT ID 4688). Esta habilitación permite que Windows registre la linea completa del comando cuando se crea un proceso, dando acceso a Wazuh para registrar los procesos y generar alertas. (ver Figura 1)

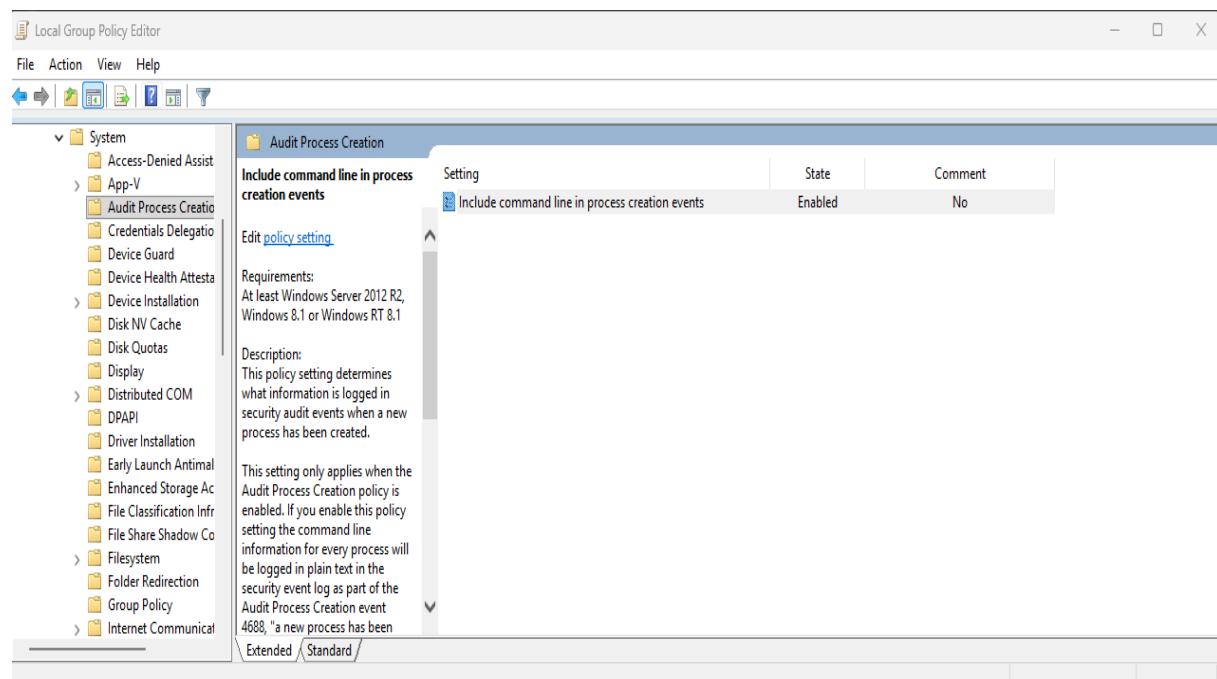


Figura 1. Activación de creación de procesos.

2. Habilitar logging avanzado de PowerShell. En esta configuración, se activan las opciones Module Logging, PowerShell Script Block Logging y PowerShell Transcription, proporcionando a Wazuh una visibilidad mas profunda sobre comandos, scripts y sesiones ejecutadas dentro de PowerShell. (ver Figura 2)

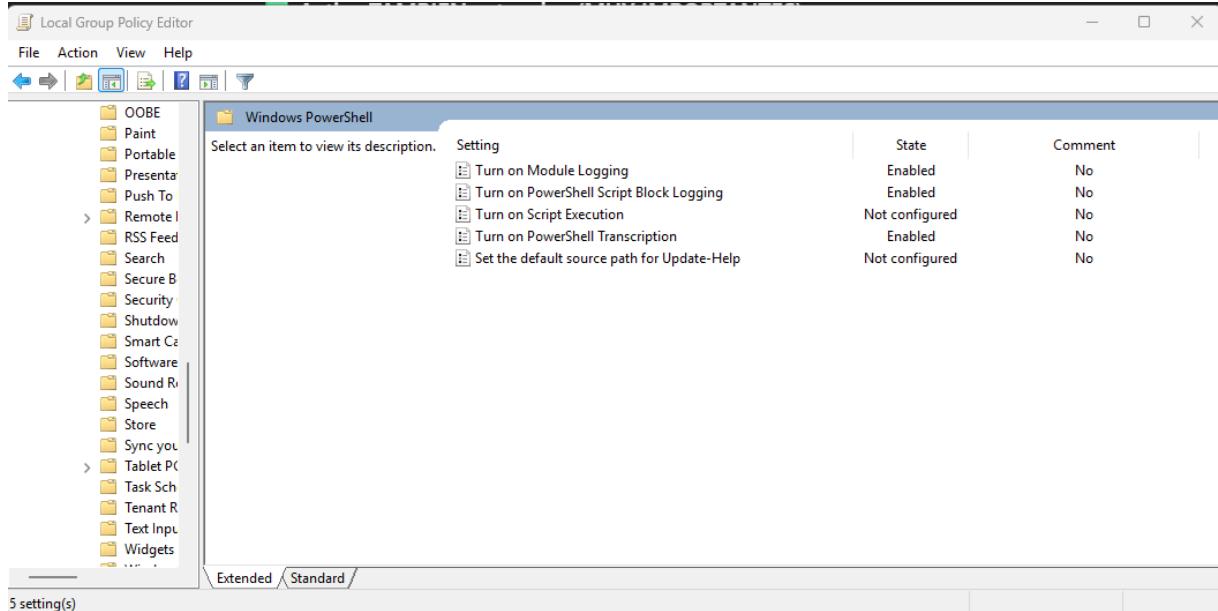


Figura 2. Habilitación del logging avanzado en el agente Windows.

3. Ejecutar en PowerShell un comando inofensivo que solo de por salida hola, pero que salte las políticas de seguridad sin cargar las configuraciones de usuario, para generar el evento sospechoso y monitorearlo en Wazuh. (ver Figura 3)

```
PS C:\WINDOWS\system32> powershell.exe -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -Command "IEX 'Write-Output Hello'"
Hello
PS C:\WINDOWS\system32>
```

Figura 3. Ejecución del comando inofensivo en PowerShell.

4. Acceder a la pestaña Threat Hunting → Events en el servidor Wazuh. En esta sección se muestran a detalle el evento generado por la ejecución del comando sospechoso en nuestro agente Windows a través del PowerShell. (ver Figura 4)

The screenshot shows the Wazuh Threat Hunting interface. On the left, there's a list of events with columns for timestamp, agent.name, rule.description, and details. A specific event from 'Dec 12, 2025 @ 21:28:45...' is selected. On the right, the 'Document Details' pane displays various event properties in a key-value format, such as 'data.win.eventdata.newProcess' and 'data.win.eventdata.parentProcessName'. There are also buttons for 'View surrounding documents' and 'View single document'.

Event Details
data.win.eventdata.newProcess 0x2954
data.win.eventdata.parentProcessName C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
data.win.eventdata.processId 0x3c44
data.win.eventdata.subjectDc DESKTOP-B2PC2IC
data.win.eventdata.subjectName horac
data.win.eventdata.subjectO S-1-5-21-2320099924-2676893089-188914015-1001
data.win.eventdata.subjectS 0x0
data.win.eventdata.targetLog 0x0
data.win.eventdata.targetUser S-1-0-0
data.win.eventdata.tokenElev %1938
data.win.system.channel Security
data.win.system.computer DESKTOP-B2PC2IC
data.win.system.eventID 4688
data.win.system.eventRecordID 69144
data.win.system.keywords 0x8020000000000000

Figura 4. Detalles del evento de ejecución sospechosa en PowerShell.

5. Acciones Recomendadas. - Ante la detección de ejecuciones sospechosas en la terminal, se recomienda aplicar las siguientes medidas:

- Validar si la ejecución fue legítima por un usuario autorizado.
- Restringir el uso de PowerShell a usuarios no autorizados.
- Aplicar Constrained Language Mode cuando sea posible.
- Implementar AppLocker o Windows Defender Application Control.
- Continuar monitoreando los eventos de ejecuciones sospechosas, asegurando que no haya un falso positivo.
- Aplicar medidas de contención de acuerdo a los procedimientos de la organización, si se confirma actividad maliciosa

6. Resultados Obtenidos. - En este laboratorio se activaron varios procesos necesarios para que Wazuh logre ver los eventos que suceden en la terminal del agente Windows. Posteriormente se ejecutó un comando en PowerShell, aunque este no realizó una acción maliciosa, el evento que generó son similares a técnicas de evasión de seguridad. Finalmente se pudo visualizar y detectar estas acciones sospechosas por parte de Wazuh.

7. Reflexión final. – Este laboratorio permitió conocer como se ejecutan comandos potencialmente maliciosos o sospechosos mediante PowerShell. Si bien PowerShell no es un punto inicial de ataque, esta herramienta es comúnmente utilizada para ataques avanzados que ejecutan códigos maliciosos o que evaden controles de seguridad. Destacando nuevamente la importancia de contar con un SIEM como Wazuh, visualizando y detectando este tipo de ejecuciones sospechosas, facilitando una toma de decisiones oportuna y reduciendo el impacto de incidentes.