# Monitoreo de ejecuciones sospechosas en PowerShell

**1. Objetivo. –** Realizar ejecuciones de comandos sospechosos en PowerShell, con el objetivo de generar eventos para detectarlos y analizarlos en Wazuh.

**2. Herramientas. -** Para este laboratorio se utilizaron:

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

## 3. Metodología / Análisis Realizado

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.

### 3.1 Habilitación de creación de procesos

Se activó la habilitación de creación de procesos (EVENT ID 4688), esto permite que Windows registre la línea completa del comando que se ejecutó, y se genere el registro y evento en Wazuh. (ver Figura 1)

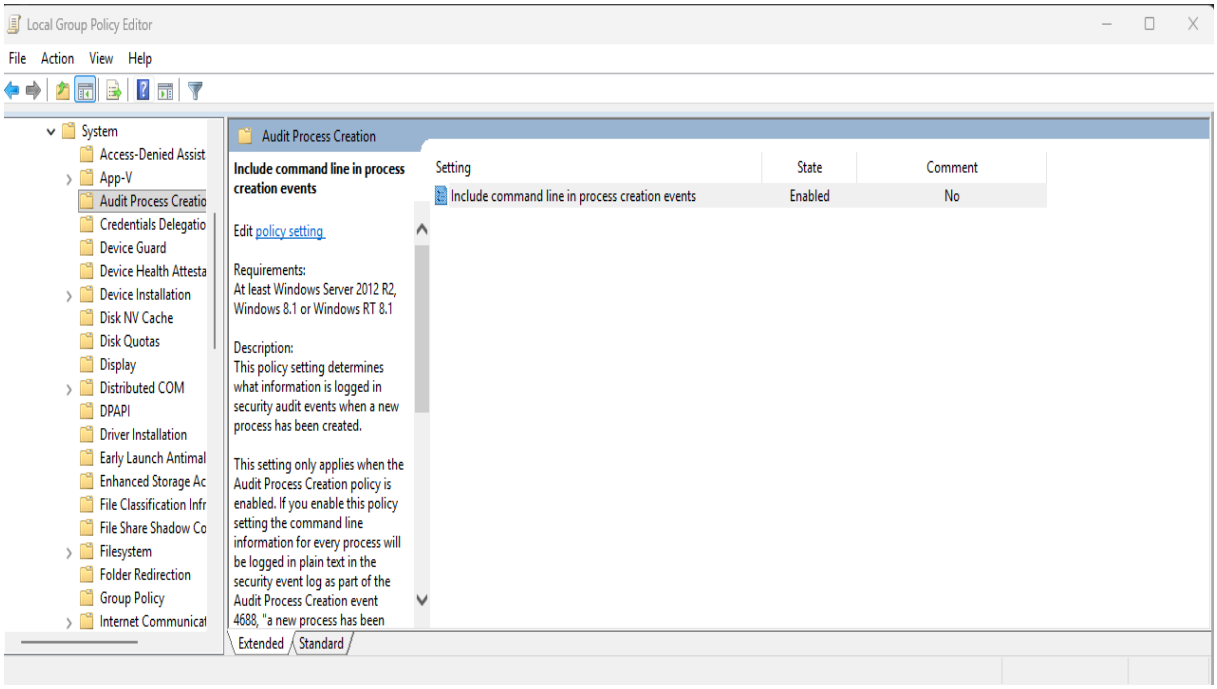



**Figura 1.** Activación de creación de procesos.

### 3.2 Habilitación de logging

Se habilitó el 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 más profunda sobre comandos, scripts y sesiones ejecutadas dentro de PowerShell. (ver Figura 2)

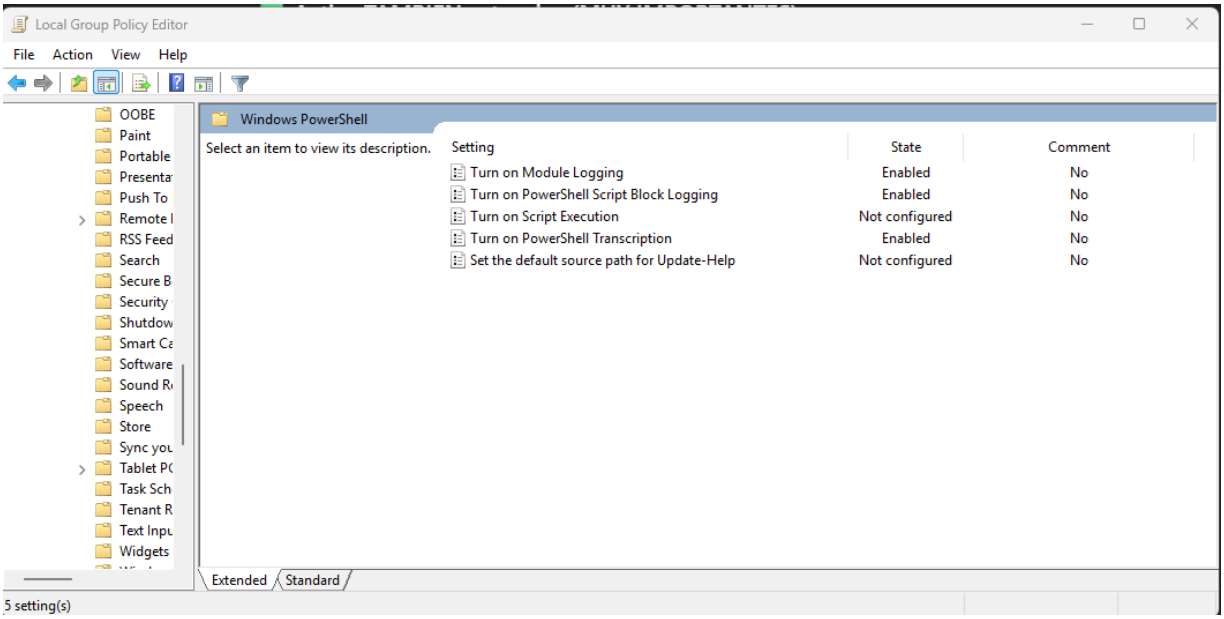



**Figura 2.** Habilitación del logging avanzado en el agente Windows.

### 3.3 Ejecución de comando

Se ejecutó 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)

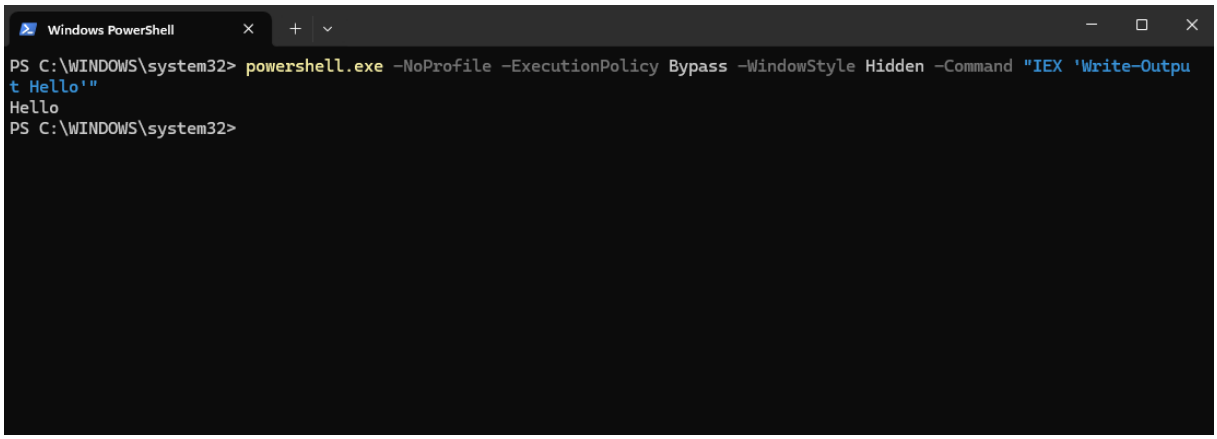


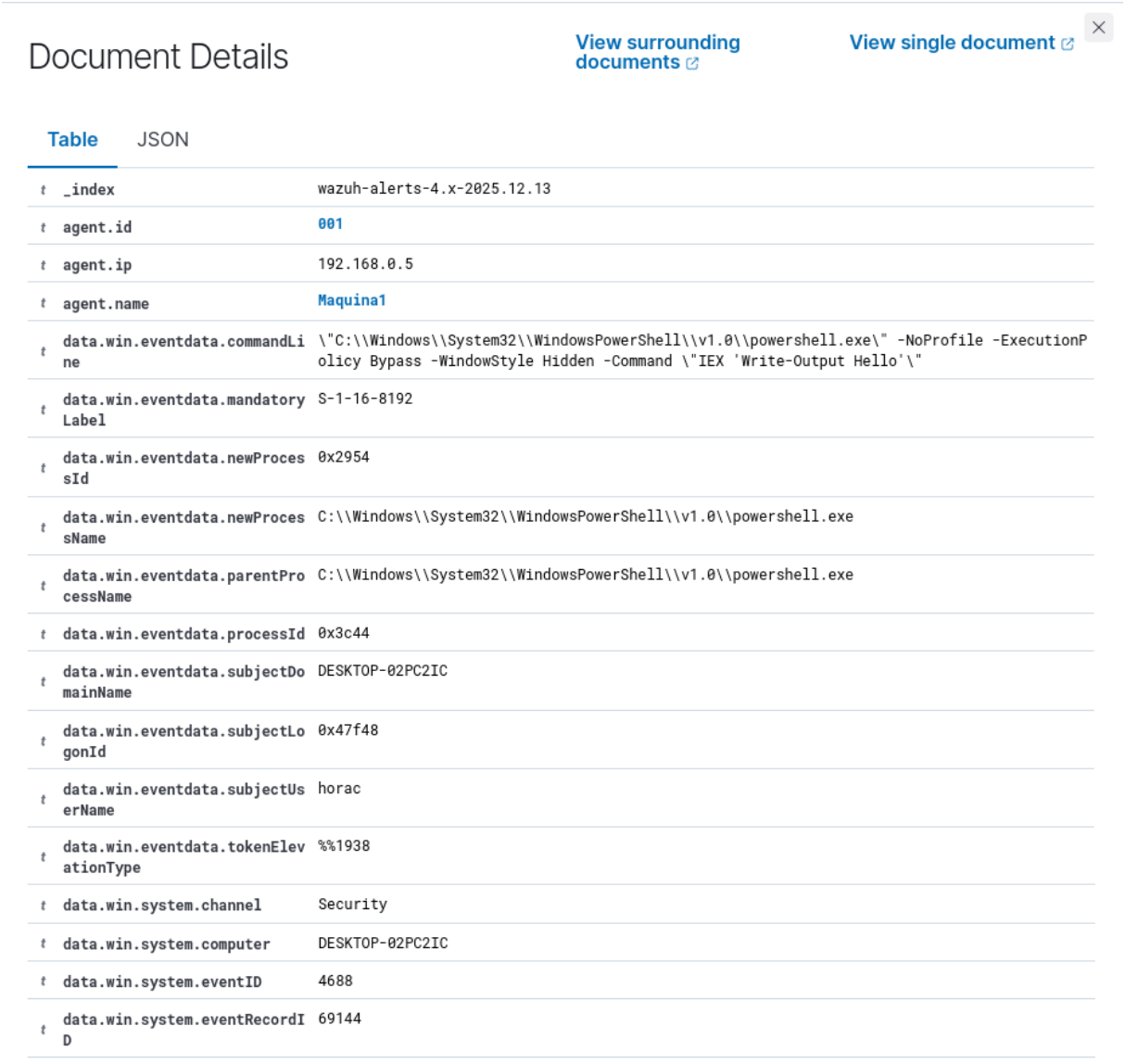

**Figura 3.** Ejecución de comando en PowerShell.

### 3.4 Visualización y análisis de los detalles del evento

Se accedió a la pestaña Threat Hunting → Events en el servidor Wazuh. Aunque el evento fue clasificado con un nivel de severidad bajo (nivel 3), el uso de parámetros que evaden mecanismos de seguridad representa una técnica común utilizada por atacantes para ejecutar scripts sin restricciones.

Si bien el comando ejecutado no fue malicioso, se pudo identificar que el script fue ejecutado en PowerShell, el usuario horac lo ejecutó con permisos estándar y lo más importante, se logró visualizar el comando completo de la línea de comandos utilizada. (ver Figura 4)

Identificar el comando completo, permite entender en su totalidad las intenciones de la ejecución, y así tomar decisiones respectivas al evento en cuestión.



Document Details

View surrounding documents | View single document

Table | JSON

| | |
|---|---|
| _index | wazuh-alerts-4.x-2025.12.13 |
| agent.id | 001 |
| agent.ip | 192.168.0.5 |
| agent.name | Maquina1 |
| data.win.eventdata.commandLine | \"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -Command \"IEX 'Write-Output Hello'\" |
| data.win.eventdata.mandatoryLabel | S-1-16-8192 |
| data.win.eventdata.newProcessId | 0x2954 |
| data.win.eventdata.newProcessName | C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe |
| data.win.eventdata.parentProcessName | C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe |
| data.win.eventdata.processId | 0x3c44 |
| data.win.eventdata.subjectDomainName | DESKTOP-02PC2IC |
| data.win.eventdata.subjectLogonId | 0x47f48 |
| data.win.eventdata.subjectUserName | horac |
| data.win.eventdata.tokenElevationType | %%1938 |
| data.win.system.channel | Security |
| data.win.system.computer | DESKTOP-02PC2IC |
| data.win.system.eventID | 4688 |
| data.win.system.eventRecordID | 69144 |

**Figura 4.** Detalles del evento de ejecución de comando en PowerShell.

## 4. 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

## 5. Resultados obtenidos

En este laboratorio se activaron varios procesos necesarios para que Wazuh pudiera visualizar eventos generados 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 evasiones de seguridad. Finalmente, se pudo visualizar y detectar estas acciones sospechosas a través de Wazuh, validando la capacidad para identificar comportamientos potencialmente riesgosos.

## 6. 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, ya que permite visualizar y detectar este tipo de ejecuciones sospechosas, facilitando una toma de decisiones oportuna y reduciendo el impacto de incidentes.