LABWAZUH 5 – Escaneo de red (Nmap)

1. Objetivo. – Realizar escaneo de puertos, con el fin de identificar vulnerabilidades de red, generando eventos para ser detectados y monitoreados mediante Wazuh.

2. Alcance.- Este laboratorio enfoca la detección y el monitoreo de eventos de escaneo de puertos, 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. Habilitar Firewall logging en el agente Windows. En esta configuración, se activan las opciones Log dropped packets y Log succesful connections, de las pestañas Domain Profile, Private profile y Public Profile, con el fin de que Windows registre todo el trafico de red relevante que pasa por el Firewall.

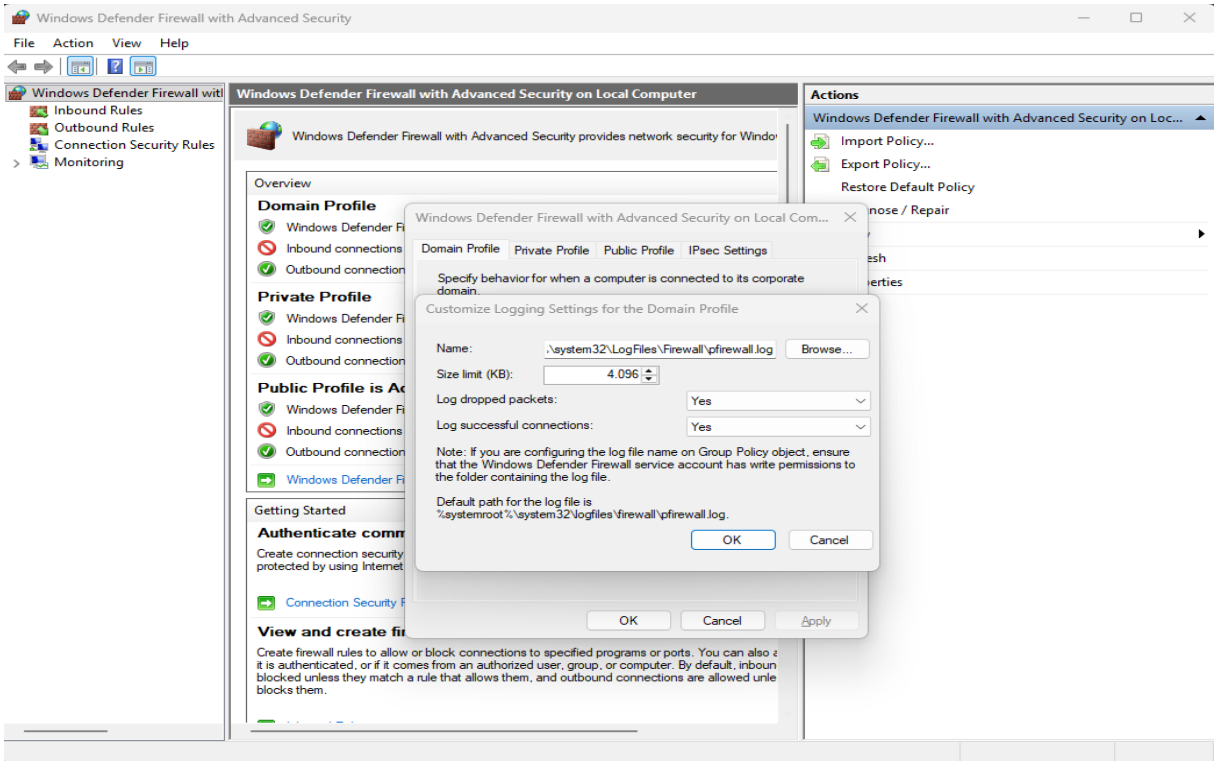

Figura 1. Habilitación del registro de red de Firewall.

2. Añadir en el archivo ossec.conf, la dirección de los registros de Firewall en el agente Windows. Dando acceso a Wazuh sobre la visualización y detección del registro del trafico del Firewall. (ver Figura 2)

```
<localfile>
  <location>active-response\active-responses.log</location>
  <log_format>syslog</log_format>
</localfile>


<localfile>
  <location>%systemroot%\system32\LogFiles\Firewall\pfirewall.log</location>
  <log_format>syslog</log_format>
</localfile>


<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
  <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

<!-- Security Configuration Assessment -->
<sca>
```

Figura 2. Configuración del archivo ossec.conf.

3. Ejecutar en PowerShell comandos que escaneen los puertos del servidor Wazuh.
El primer comando corresponde a un SYN Scan, una técnica de escaneo mas sigilosa que intenta identificar puertos abiertos, utilizada comúnmente en fases de reconocimiento.
El segundo comando realiza un escaneo de los primeros 2000 puertos, con la finalidad de identificar servicios comunes que puedan estar en ejecución.
En ambos casos, los resultados obtenidos de las ejecuciones de los comandos de escaneo, no permitieron identificar puertos abiertos ni mapear servicios, lo que indica que el equipo donde esta el servidor de Wazuh, cuenta con controles de seguridad activos, como reglas de Firewall y restricciones de red, que limitan este tipo de escaneos. (ver Figura 3)

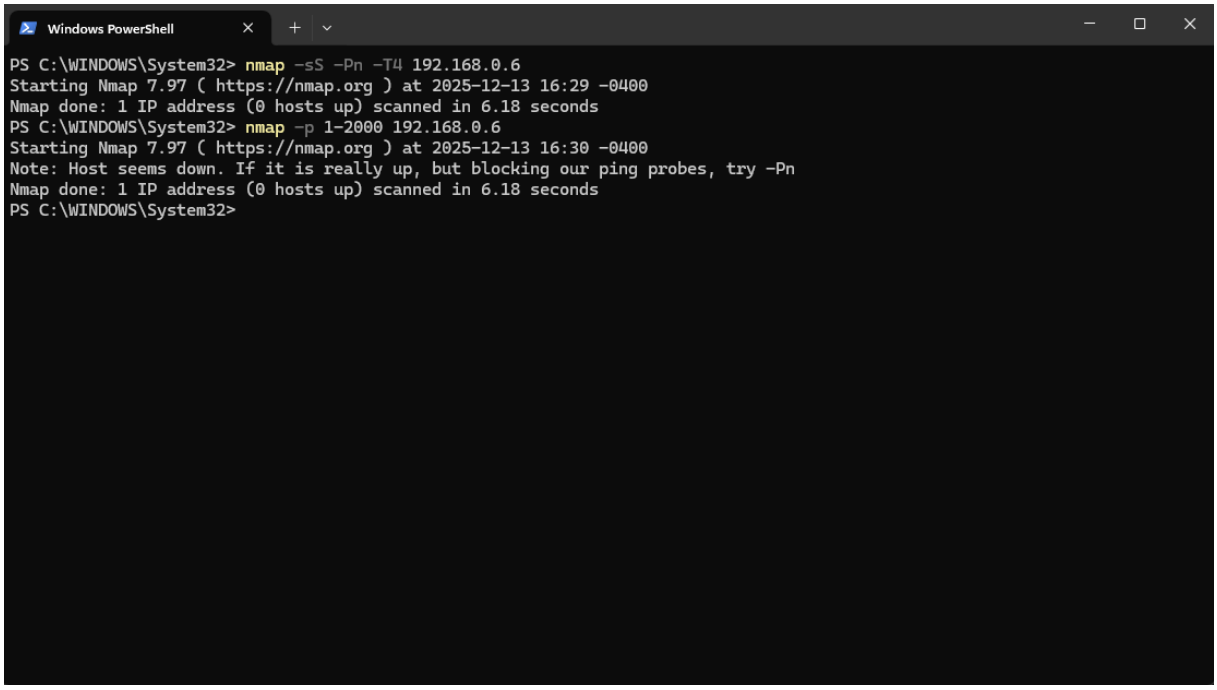

Figura 3. Ejecución de comandos de escaneo.

4. Acceder a la pestaña Threat Hunting → Events en el servidor Wazuh. En esta sección se visualizan los eventos que ocurren en el agente Windows. En el cual se muestra a detalle el evento del escaneo sigiloso, mostrando la IP origen y la herramienta que se utilizó. (ver Figura 4)

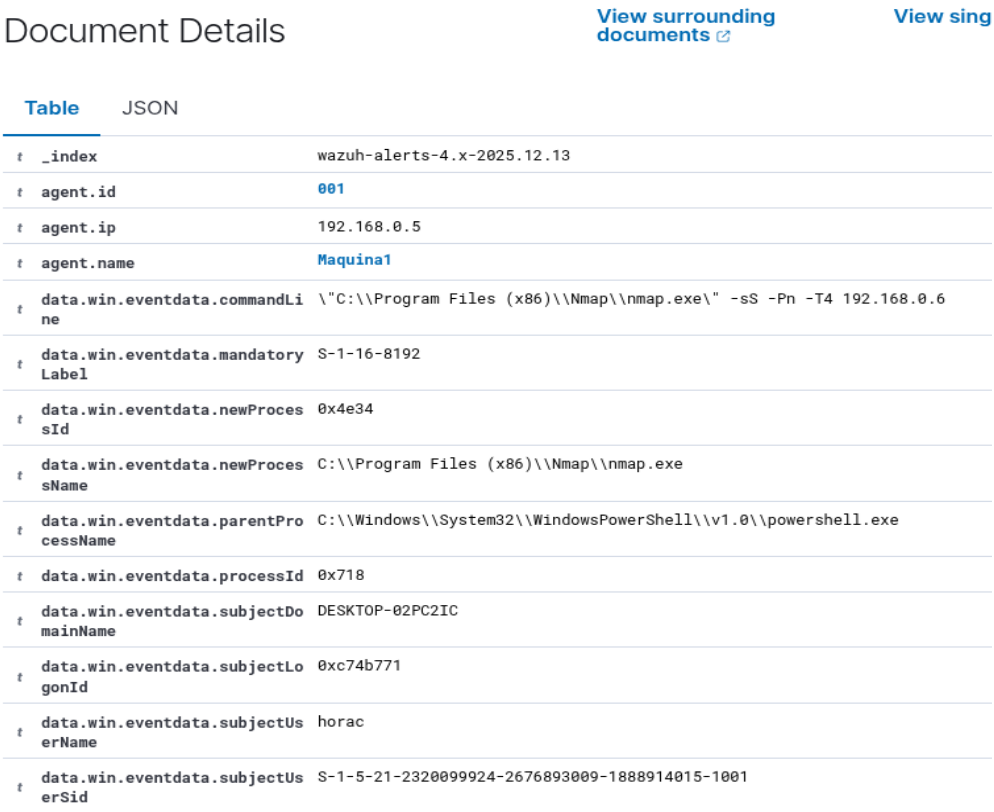

Figura 4. Detalles del evento de escaneo sigiloso.

Ademas evidenciando a detalle el evento de escaneo directo de puertos, logrando ver nuevamente la IP origen y la herramienta que se utilizó. (ver Figura 5)

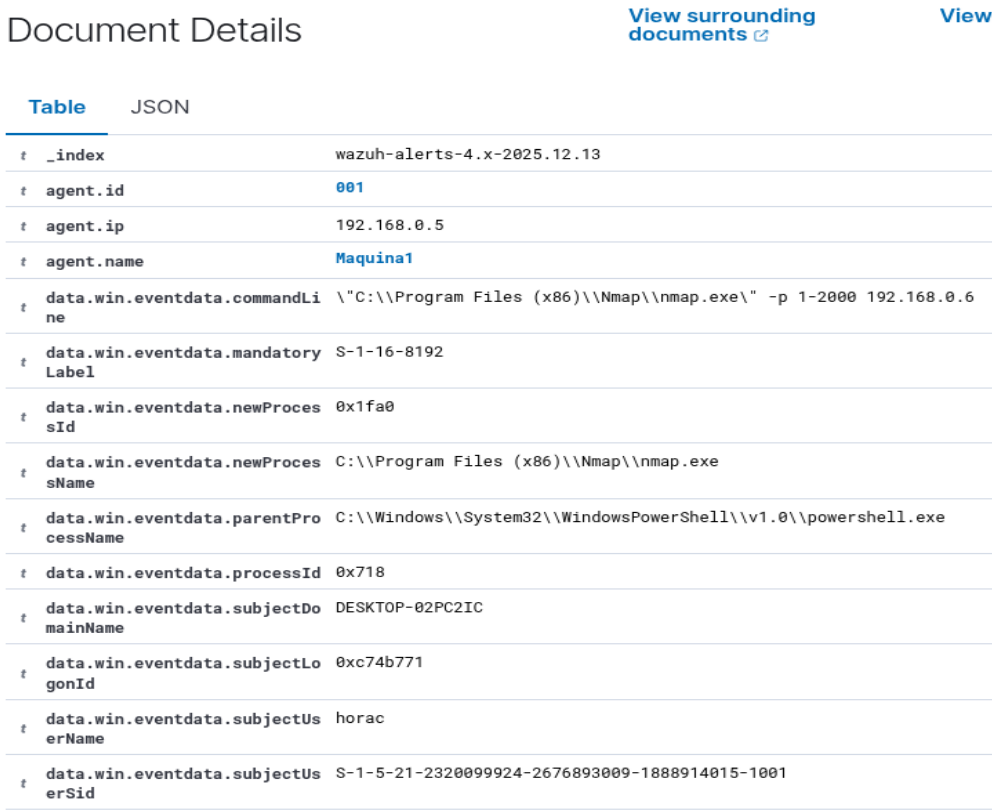

Figura 5. Detalles del evento del escaneo directo de puertos

5. Acciones Recomendadas. - Ante la detección de eventos de escaneos de puertos, se recomienda aplicar las siguientes medidas:

- Determinar si el escaneo fue realizado por un usuario autorizado o por un proceso de administración.
- Identificar la IP de origen, el host afectado y la herramienta utilizada.
- Incrementar el monitoreo y supervisión del host afectado.
- Correlacionar ejecuciones de procesos, logs de firewall o intentos de conexión posteriores.
- Escalar el evento si el escaneo es persistente.

6. Resultados Obtenidos. - En este laboratorio se habilitó el logging del Firewall de Windows y se configuró correctamente el archivo ossec.conf en el agente Windows, lo que permitió a Wazuh visualizar y analizar los registros generados por el firewall. Posteriormente, se ejecutaron dos comandos con la finalidad identificar servicios y realizar reconocimiento del host objetivo. Sin embargo, los resultados obtenidos no mostraron puertos abiertos ni servicios accesibles, lo que indica que el host Wazuh cuenta con controles de seguridad activos. Como resultado, aunque el escaneo no tuvo éxito desde el punto de vista del atacante, Wazuh detectó satisfactoriamente los eventos de escaneo.

7. Reflexión final. – Este laboratorio permitió comprender que, antes de ejecutar un ataque, suelen realizar una fase de reconocimiento, intentando recopilar información de puertos o servicios vulnerables del sistema utilizando la herramienta Nmap en este laboratorio. Esta practica reconoció la importancia de contar con un SIEM como Wazuh en estos casos, incluso siendo el escaneo un intento fallido, fue capaz de visualizar y monitorear este tipo de eventos, facilitando la detección temprana y la toma de decisiones oportunas en este tipo de casos.