

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. Herramientas. - Para este laboratorio se utilizarán:

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

3. Metodología / Análisis realizado

Este laboratorio enfoca la detección y monitoreo de eventos de escaneo de puertos, las acciones de contención o mitigación quedan fuera del alcance del presente laboratorio. Todos los comandos utilizados se presentan en el Anexo A (página 5).

3.1 Configuración Firewall

Se habilitó Firewall logging en el agente Windows. En esta configuración, se activaron las opciones Log dropped packets y Log succesful connections, de las pestañas Domain Profile, Private profile y Public Profile, con el objetivo de registrar todo el tráfico de red que pasa por el firewall. (ver Figura 1)

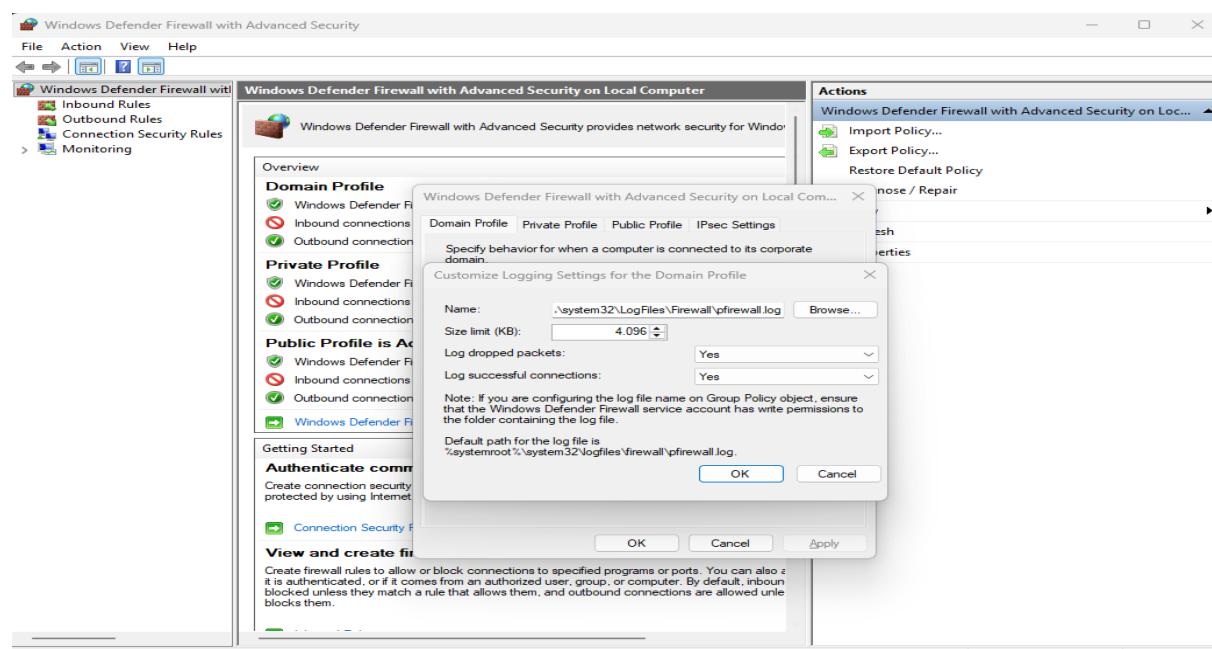


Figura 1. Habilitación del registro de red de Firewall.

Se añadió 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 tráfico 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

3.2 Escaneo de red

Se ejecutó en PowerShell dos comandos de escaneo para identificar puertos abiertos y servicios que puedan estar en ejecución en el host Wazuh.

Los resultados obtenidos de las ejecuciones de los comandos de escaneo, mostraron que no se pudieron identificar puertos abiertos ni mapear servicios, lo que indica que el equipo que aloja 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)

```

PS C:\WINDOWS\System32> nmap -sS -Pn -T4 192.168.0.6
Starting Nmap 7.97 ( https://nmap.org ) at 2025-12-13 16:29 -0400
Nmap done: 1 IP address (0 hosts up) scanned in 6.18 seconds
PS C:\WINDOWS\System32> nmap -p 1-2000 192.168.0.6
Starting Nmap 7.97 ( https://nmap.org ) at 2025-12-13 16:30 -0400
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 6.18 seconds
PS C:\WINDOWS\System32>
```

Figura 3. Ejecución de comandos de escaneo.

3.3 Análisis y detección de escaneo en Wazuh

Se accedió a la pestaña Threat Hunting → Events en el servidor Wazuh. En esta sección se visualizaron los eventos de escaneo que ocurrieron en el agente Windows. En el cual se muestra a detalle el evento del escaneo silencioso, como ser la IP origen y la herramienta que se utilizó. (ver Figura 4)

Document Details		View surrounding documents	View single
Table	JSON		
<code>t _index</code>	wazuh-alerts-4.x-2025.12.13		
<code>t agent.id</code>	001		
<code>t agent.ip</code>	192.168.0.5		
<code>t agent.name</code>	Maquina1		
<code>t data.win.eventdata.commandLine</code>	"C:\\Program Files (x86)\\Nmap\\nmap.exe" -sS -Pn -T4 192.168.0.6		
<code>t ne</code>			
<code>t data.win.eventdata.mandatoryLabel</code>	S-1-16-8192		
<code>t data.win.eventdata.newProcessId</code>	0x4e34		
<code>t data.win.eventdata.newProcessName</code>	C:\\Program Files (x86)\\Nmap\\nmap.exe		
<code>t data.win.eventdata.parentProcessName</code>	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe		
<code>t data.win.eventdata.processId</code>	0x718		
<code>t data.win.eventdata.subjectDomainName</code>	DESKTOP-02PC2IC		
<code>t data.win.eventdata.subjectLogonId</code>	0xc74b771		
<code>t data.win.eventdata.subjectUserName</code>	horac		
<code>t erName</code>	erSid		
<code>t data.win.eventdata.subjectUserSid</code>	S-1-5-21-2320099924-2676893009-1888914015-1001		

Figura 4. Detalles del evento de escaneo silencioso.

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

Document Details		View surrounding documents	View
Table	JSON		
<code>t _index</code>	wazuh-alerts-4.x-2025.12.13		
<code>t agent.id</code>	001		
<code>t agent.ip</code>	192.168.0.5		
<code>t agent.name</code>	Maquina1		
<code>t data.win.eventdata.commandLine</code>	"C:\\Program Files (x86)\\Nmap\\nmap.exe" -p 1-2000 192.168.0.6		
<code>t ne</code>			
<code>t data.win.eventdata.mandatoryLabel</code>	S-1-16-8192		
<code>t data.win.eventdata.newProcessId</code>	0x1fa0		
<code>t data.win.eventdata.newProcessName</code>	C:\\Program Files (x86)\\Nmap\\nmap.exe		
<code>t data.win.eventdata.parentProcessName</code>	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe		
<code>t data.win.eventdata.processId</code>	0x718		
<code>t data.win.eventdata.subjectDomainName</code>	DESKTOP-02PC2IC		
<code>t data.win.eventdata.subjectLogonId</code>	0xc74b771		
<code>t data.win.eventdata.subjectUserName</code>	horac		
<code>t erName</code>	erSid		
<code>t data.win.eventdata.subjectUserSid</code>	S-1-5-21-2320099924-2676893009-1888914015-1001		

Figura 5. Detalles del evento del escaneo directo de puertos

4. 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.

5. 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.

6. Reflexión final. – Este laboratorio permitió comprender que, antes de ejecutar un ataque, se suele realizar una fase de reconocimiento, intentando recopilar información de puertos o servicios vulnerables del sistema utilizando la herramienta Nmap. Esta práctica reconoció la importancia de contar con un SIEM como Wazuh en este tipo de casos, incluso en este laboratorio, 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.

Anexo A – Comandos Utilizados

nmap -sS -Pn -T4 192.168.0.6

nmap -p 1-2000 192.168.0.6