

威脅情資期末作業

412570376 周映妤

首先先部屬出pfSense系統且安裝suricata

The screenshot shows the pfSense Services / Suricata interface settings overview. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help, and a gear icon. Below the navigation is a breadcrumb trail: Services / Suricata. A red question mark icon is in the top right corner. A horizontal menu bar below the breadcrumb includes: Interfaces (underlined), Global Settings, Updates, Alerts, Blocks, Files, Pass Lists, Suppress, Logs View, Logs Mgmt, and SID Mgmt. Underneath this menu are two small buttons: Sync and IP Lists. The main content area is titled "Interface Settings Overview". It contains a table with the following columns: Interface, Suricata Status, Pattern Match, Blocking Mode, Description, and Actions. One row is shown for the LAN (em1) interface, which has a checked status icon, a green circle with a checkmark, and a blue square with a white circle. The pattern match is set to AUTO and the blocking mode is DISABLED. The description is LAN. The actions column includes edit, copy, and delete icons. At the bottom right of the table are "Add" and "Delete" buttons. A blue information icon is located at the bottom left of the main content area.

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
LAN (em1)	<input checked="" type="checkbox"/>	AUTO	DISABLED	LAN	

Add Delete

再來確保pfSense有串接至wazuh server

The screenshot shows the Wazuh web interface at <https://192.168.1.128/app/endpoints-summary#/agents-preview>. The interface includes three donut charts: 'AGENTS BY STATUS' (Active 1, Disconnected 0, Pending 0, Never connected 0), 'TOP 5 OS' (bsd 1), and 'TOP 5 GROUPS' (default 1). Below these, a table lists the 'Agents (1)' with the following data:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	pfSense.home.arpa	192.168.1.183	default	BSD 14.0	node01	v4.14.1	active	...

At the bottom, it says 'Rows per page: 10' and has navigation arrows < 1 >.

小測試：攻擊行為模擬

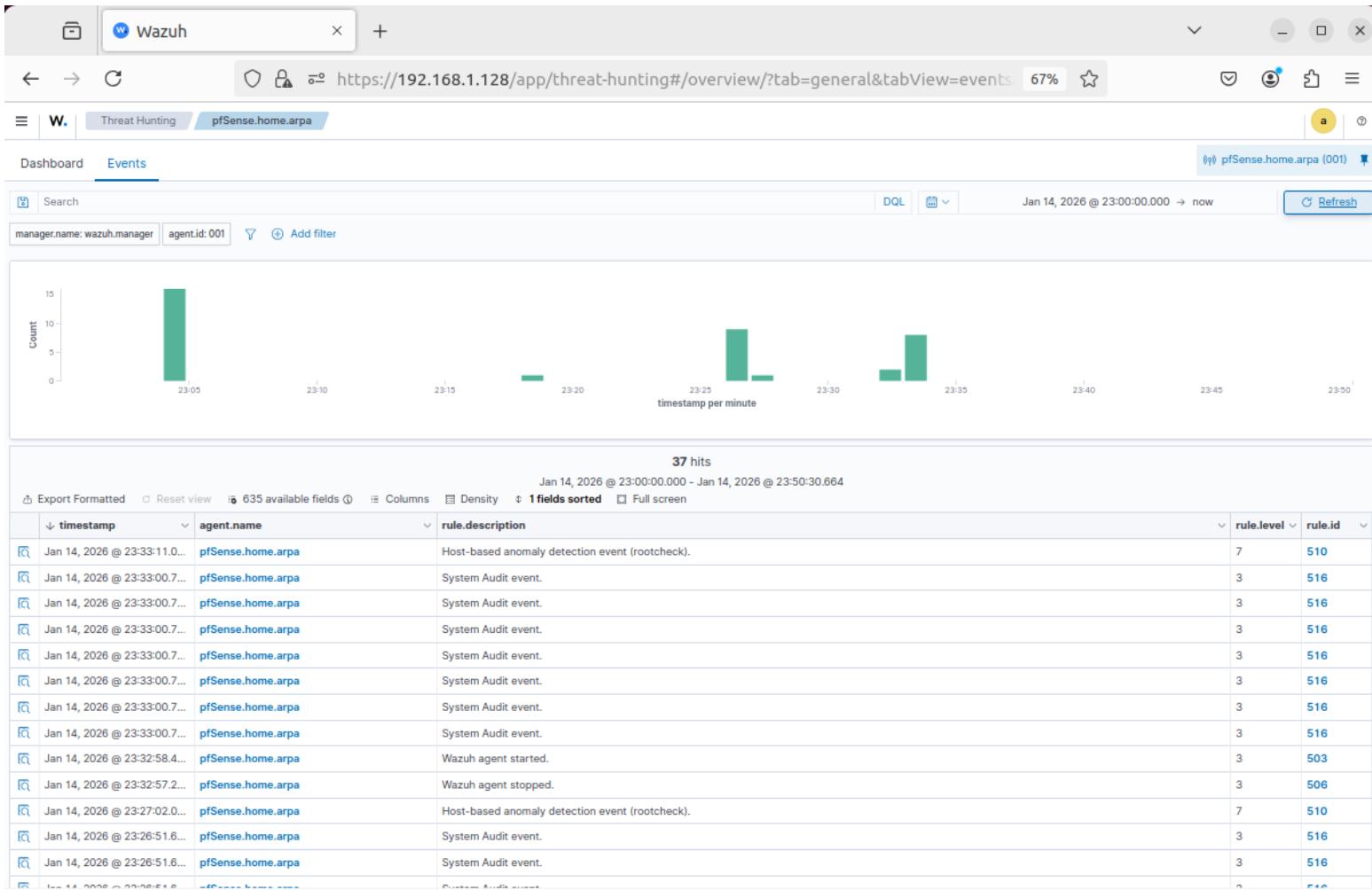
- 首先先在custom.rules中新增規則
- alert tcp any any -> \$LAN_NET any (msg:"Nmap Scan Detected"; flags:S; threshold:type threshold, track by_src, count 5, seconds 60; sid:1000001; rev:1;)
- 重啟Suricata讓規則生效。再來要來模擬攻擊，在別台機器執行
- sudo apt update && sudo apt install nmap -y
- nmap -sS -p 1-1000 192.168.56.10

```
wazuh@wazuh-VirtualBox:~/wazuh-docker/single-node$ sudo nmap -sS -p 1-1000 192.168.56.10
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-14 23:27 CST
Nmap scan report for 192.168.56.10
Host is up (0.0057s latency).
All 1000 scanned ports on 192.168.56.10 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.29 seconds
wazuh@wazuh-VirtualBox:~/wazuh-docker/single-node$ sudo nmap -sS -p 1-1000 192.168.56.10
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-14 23:33 CST
Nmap scan report for 192.168.56.10
Host is up (0.0035s latency).
All 1000 scanned ports on 192.168.56.10 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

規則觸發結果



實作主動回應

- 首先要在Ubuntu終端機編輯Manager設定檔
- sudo vi /var/ossec/etc/ossec.conf
- 找到<ossec_config>區塊，加入以下設定：

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/ossec/logs/active-responses.log</location>
</localfile>
<command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>1000001</rules_id>
  <timeout>600</timeout>
</active-response>
```

實作主動回應

- 再做一次模擬攻擊。
- 執行ping 192.168.56.10的結果顯示「Packet filtered」。
- 代表pfSense的防火牆規則（由Wazuh下令）明確地攔截並丟棄了來自Ubuntu的封包。
- Nmap掃描結果也顯示「All 1000 scanned ports are filtered」。

```
wazuh@wazuh-VirtualBox:~$ sudo nmap -sS -p 1-1000 192.168.56.10
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-15 00:42 CST
Nmap scan report for 192.168.56.10
Host is up (0.0038s latency).
All 1000 scanned ports on 192.168.56.10 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.24 seconds
wazuh@wazuh-VirtualBox:~$ ping 192.168.56.10
PING 192.168.56.10 (192.168.56.10) 56(84) bytes of data.
From 168.95.74.98 icmp_seq=7 Packet filtered
^C
--- 192.168.56.10 ping statistics ---
16 packets transmitted, 0 received, +1 errors, 100% packet loss, time 15365ms
```