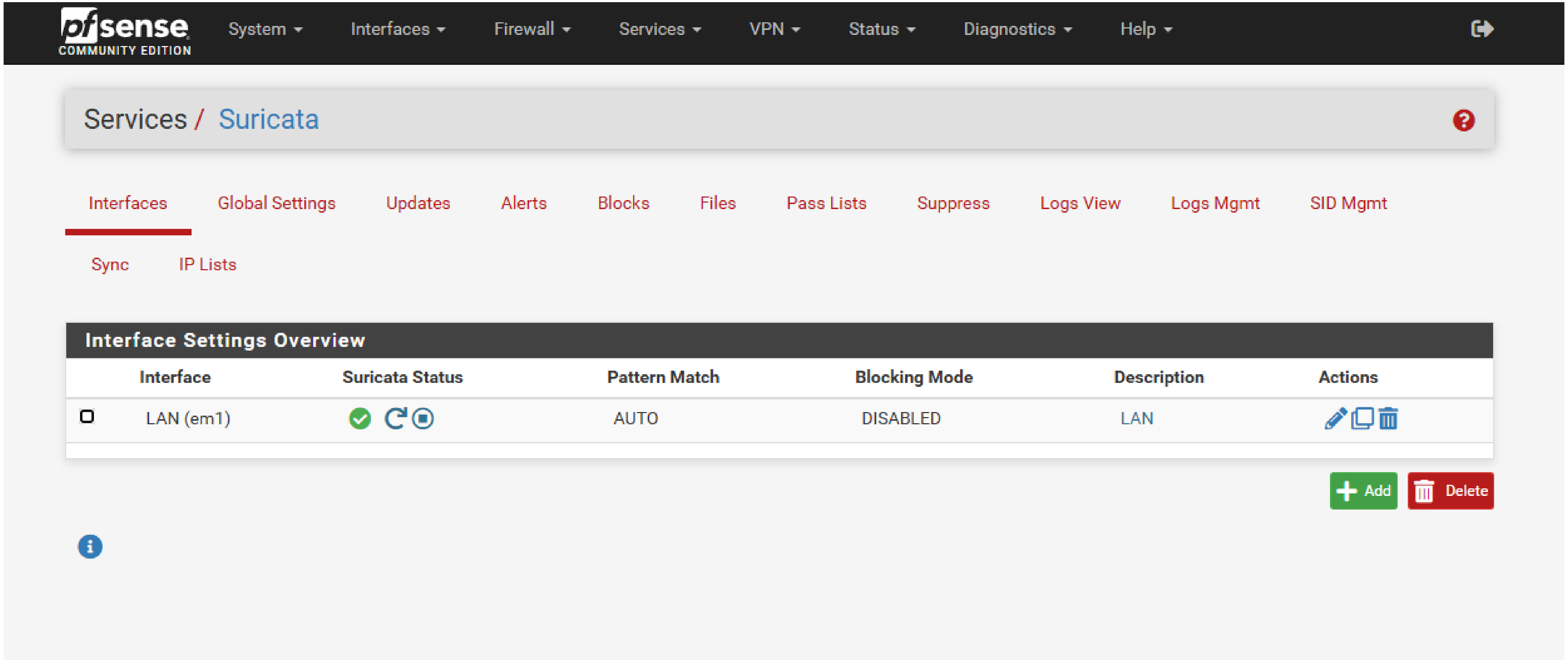
威脅情資期末作業

412570376 周映妤

首先先部屬出pfsense系統且安裝suricata

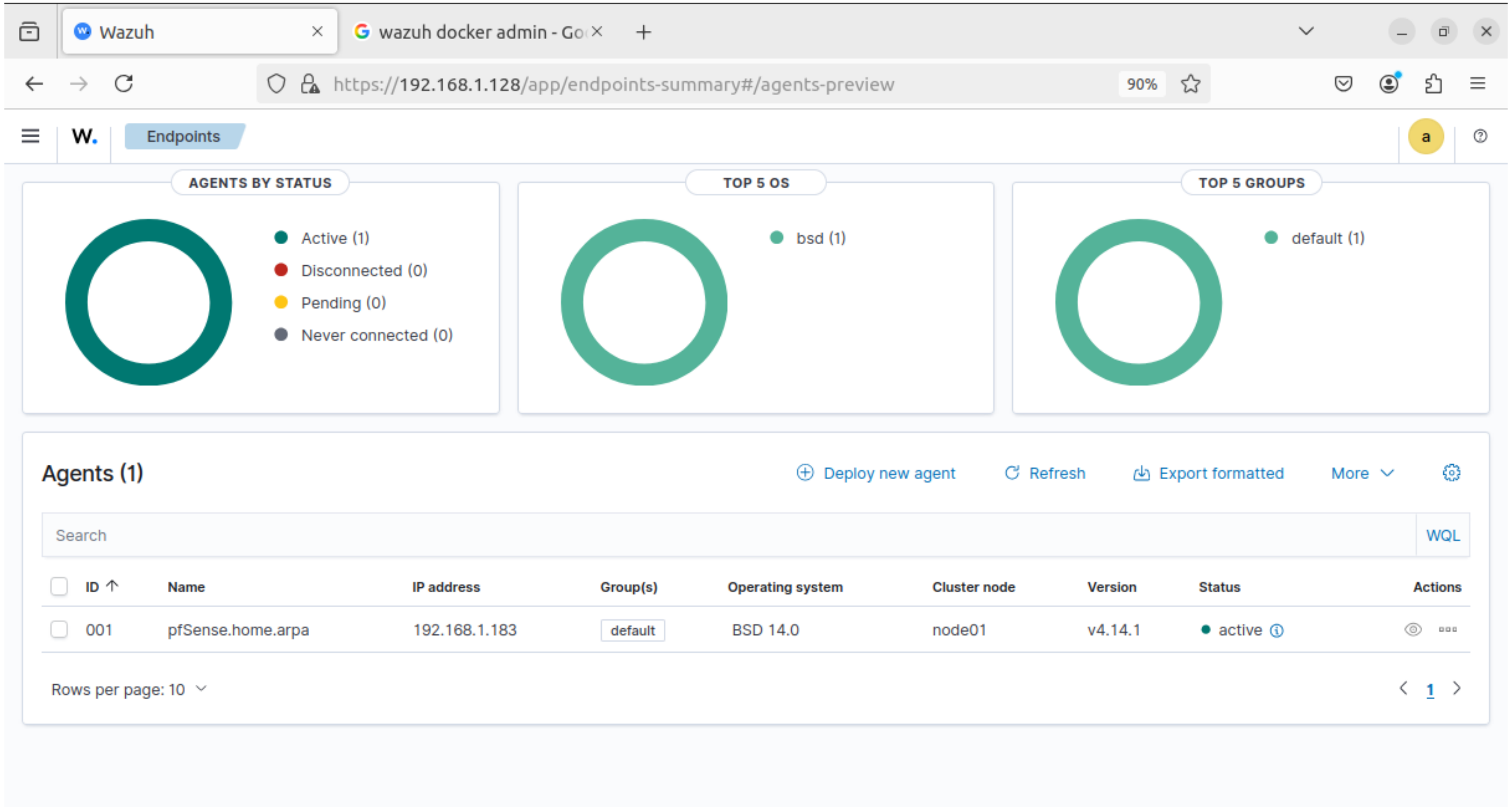


Services / Suricata

Interface Settings Overview

	Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
□	LAN (em1)	✓	AUTO	DISABLED	LAN	

再來確保pfsense有串接至wazuh server

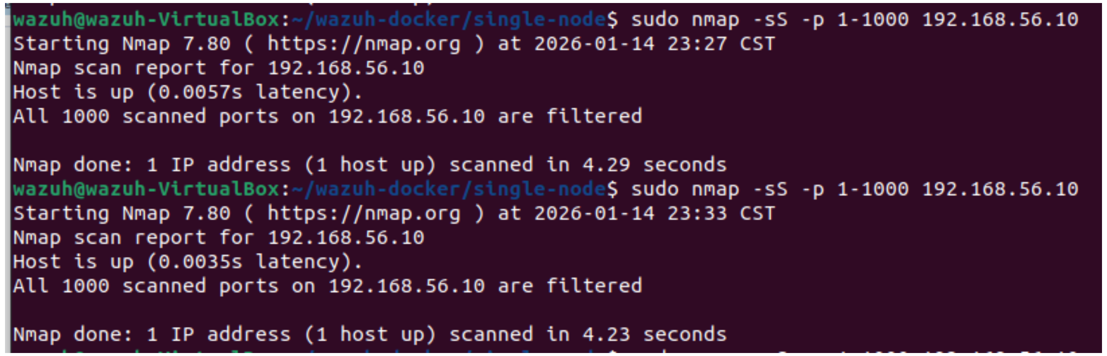


Agents (1)

□	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 ⓘ	

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

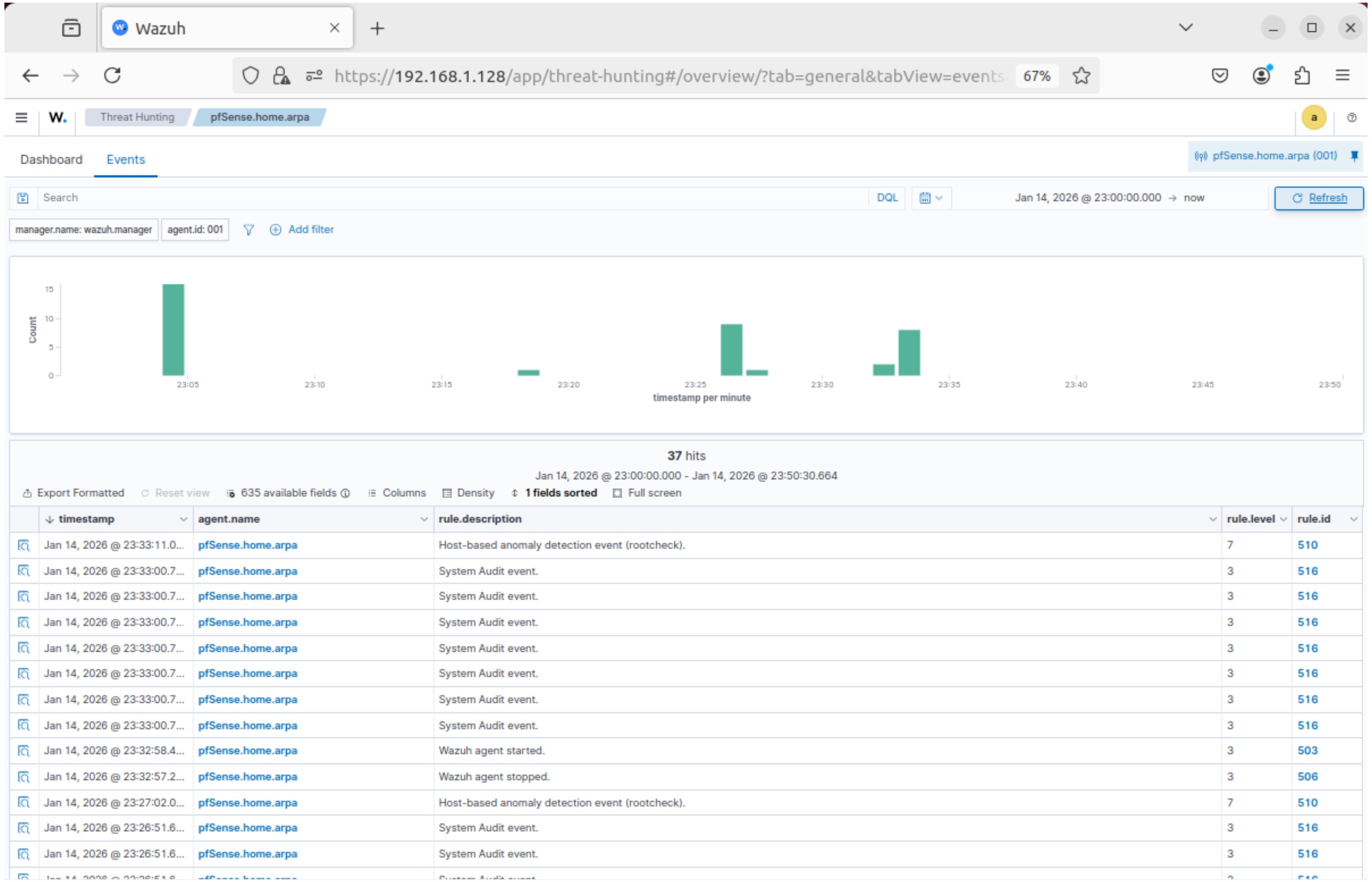


```
wazuh@wazuh-VirtualBox:~/wazuh-docker/single-node$ sudo nmap -sS -p 1-1000 192.168.56.10
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-14 23:27 CST
Nmap scan report for 192.168.56.10
Host is up (0.0057s latency).
All 1000 scanned ports on 192.168.56.10 are filtered

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



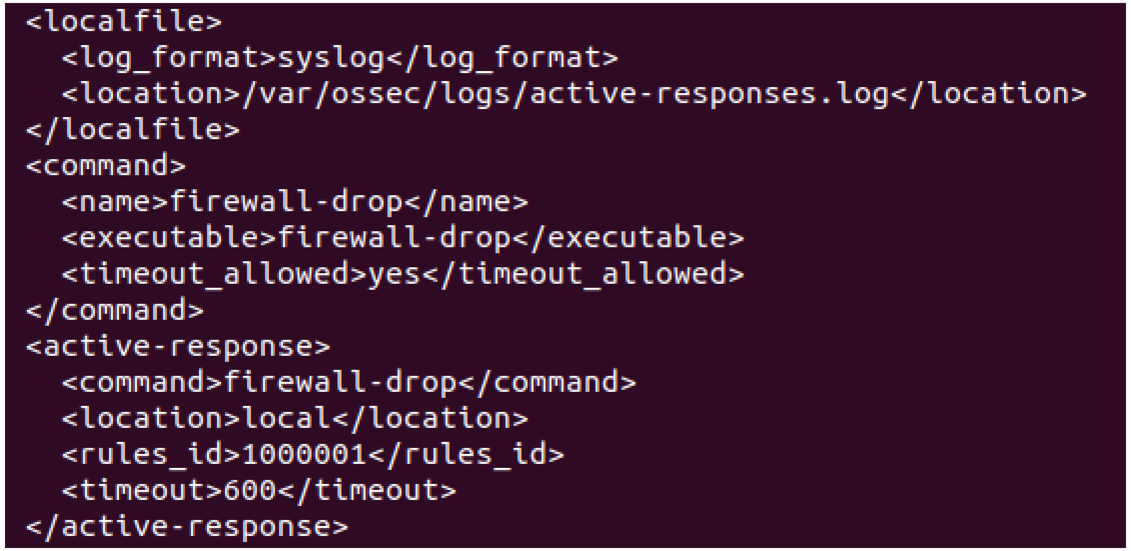
37 hits

Jan 14, 2026 @ 23:00:00.000 - Jan 14, 2026 @ 23:50:30.664

timestamp	agent.name	rule.description	rule.level	rule.id
Jan 14, 2026 @ 23:33:11.0...	pfSense.home.arpa	Host-based anomaly detection event (rootcheck).	7	510
Jan 14, 2026 @ 23:33:00.7...	pfSense.home.arpa	System Audit event.	3	516
Jan 14, 2026 @ 23:33:00.7...	pfSense.home.arpa	System Audit event.	3	516
Jan 14, 2026 @ 23:33:00.7...	pfSense.home.arpa	System Audit event.	3	516
Jan 14, 2026 @ 23:33:00.7...	pfSense.home.arpa	System Audit event.	3	516
Jan 14, 2026 @ 23:33:00.7...	pfSense.home.arpa	System Audit event.	3	516
Jan 14, 2026 @ 23:33:00.7...	pfSense.home.arpa	System Audit event.	3	516
Jan 14, 2026 @ 23:33:00.7...	pfSense.home.arpa	System Audit event.	3	516
Jan 14, 2026 @ 23:32:58.4...	pfSense.home.arpa	Wazuh agent started.	3	503
Jan 14, 2026 @ 23:32:57.2...	pfSense.home.arpa	Wazuh agent stopped.	3	506
Jan 14, 2026 @ 23:27:02.0...	pfSense.home.arpa	Host-based anomaly detection event (rootcheck).	7	510
Jan 14, 2026 @ 23:26:51.6...	pfSense.home.arpa	System Audit event.	3	516
Jan 14, 2026 @ 23:26:51.6...	pfSense.home.arpa	System Audit event.	3	516

實作主動回應

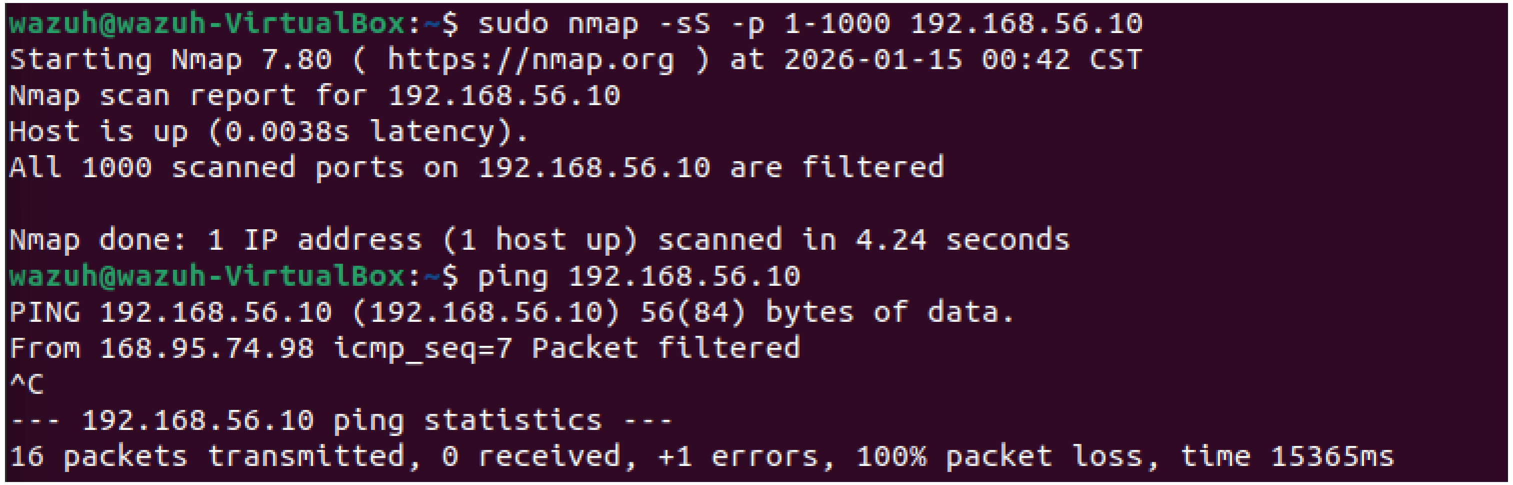
- 首先要在Ubuntu終端機編輯Manager設定檔
- sudo vi /var/ossec/etc/ossec.conf
- 找到<ossec_config>區塊，加入以下設定：



```
<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
```