Week 2 SOC Internship Task Report

Intern Name: Mahnoor Shafi
Email Address: mahnoorshafi88@gmail.com
Date: July 15, 2025
Task: Firewall + IDS Integration
Organization: Cyborts

Table of Content:

1- Configure pfSense to forward logs to the Wazuh Manager using Syslog.
2- Verify pfSense logs are appearing in the Wazuh dashboard.
3- Install Snort IDS on a separate Linux machine or within pfSense.
4- Configure Snort to generate alerts and forward them to Wazuh.
5- Simulate a port scan using nmap from one machine to another.
6- Capture the Snort alert triggered by the port scan in the Wazuh dashboard.
7- Take a screenshot of the alert inside Wazuh showing the detected network activity.

1. Objective

This report summarizes the integration of firewall (pfSense) and IDS (Suricata) with the Wazuh SIEM platform. It includes log forwarding via syslog, IDS alert generation, and threat detection verification using a simulated port scan.

2. Tools & Environment

pfSense – Used as the firewall and to forward logs to Wazuh via Syslog

Wazuh Manager – Used as the SIEM platform for log collection and alert monitoring

Suricata IDS – Intrusion Detection System to detect suspicious network activity

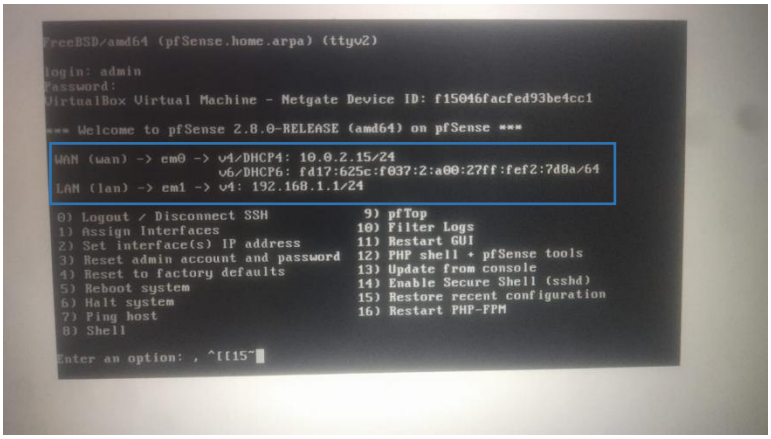
Kali Linux – Used to simulate a network attack (port scan) using Nmap

VMware Workstation – Used to create and manage the virtual lab environment

3. Task Breakdown & Steps

Step 1: Configure pfSense to Forward Logs to Wazuh

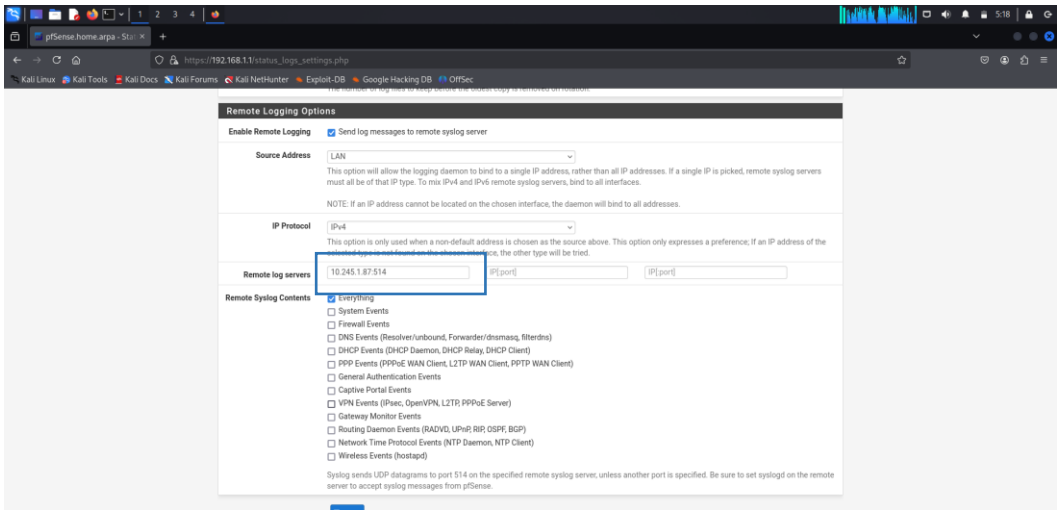
Firstly,When we download pfSense, an interface will appear in which both WAN and LAN will be shown to us.



Accessed pfSense via Web UI at https://192.168.1.1

Enabled remote syslog under:
Status > System Logs > Settings

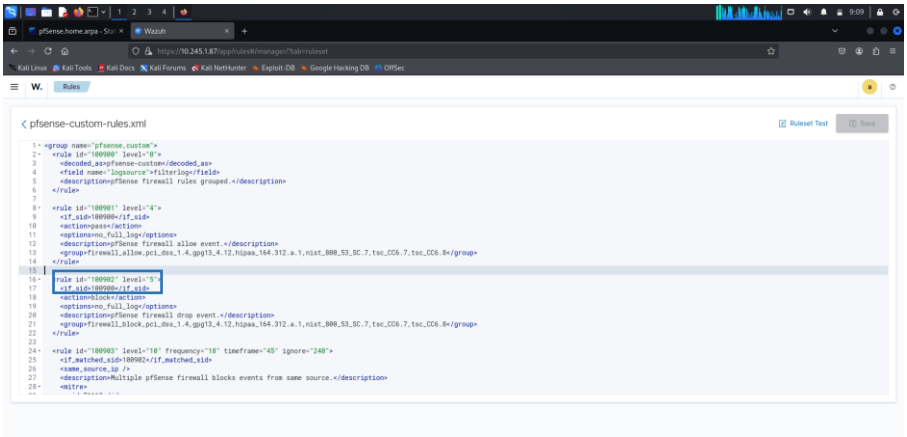
Sent logs to Wazuh Manager IP https://10.245.1.87 over UDP port 514



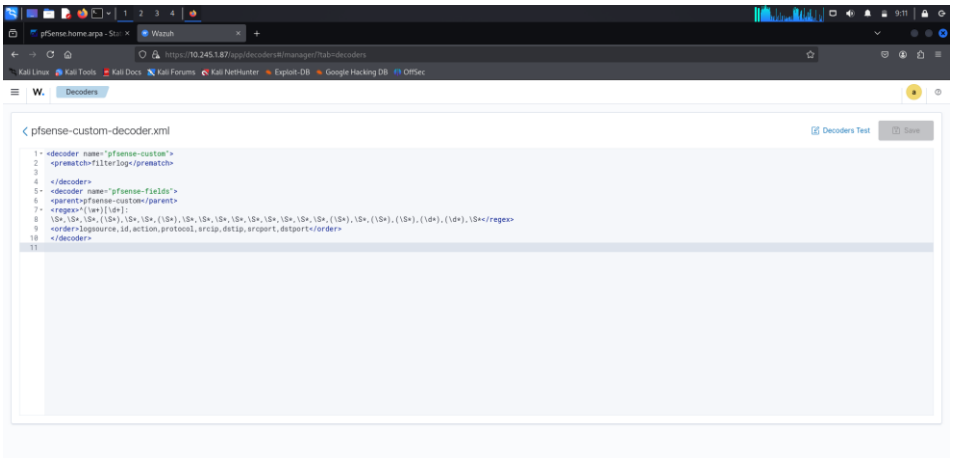
Step 2: Verify pfSense Logs in Wazuh

Firstly, add the custom rule or decodes for logs

CUSTOM RULES:



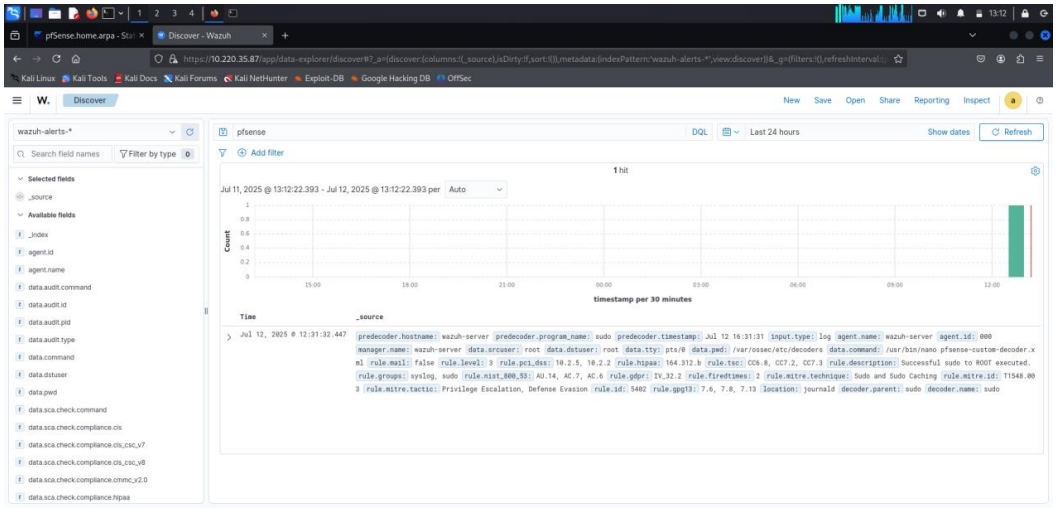
CUSTOM DECODES:

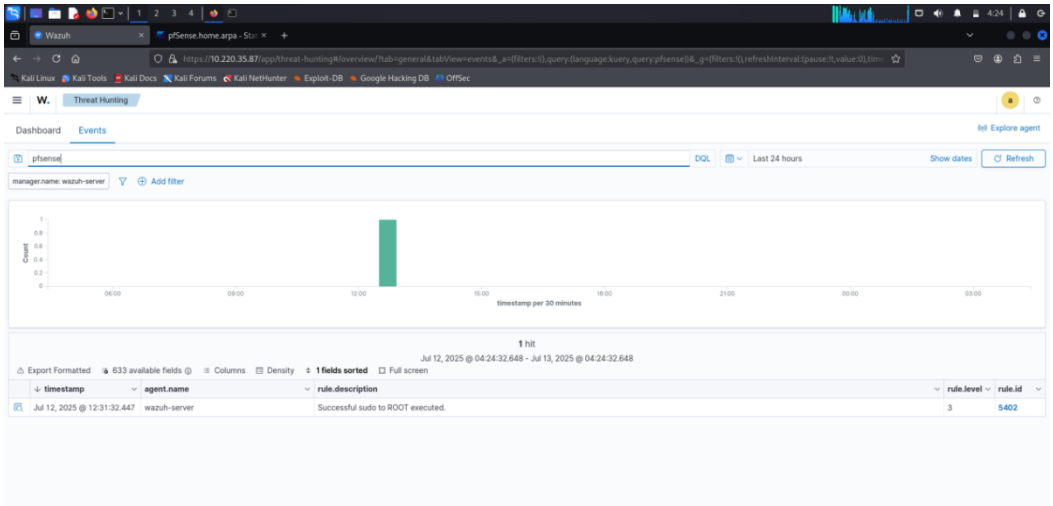


After this restart the manager and the logs are show in wazuh.

Opened Wazuh Dashboard

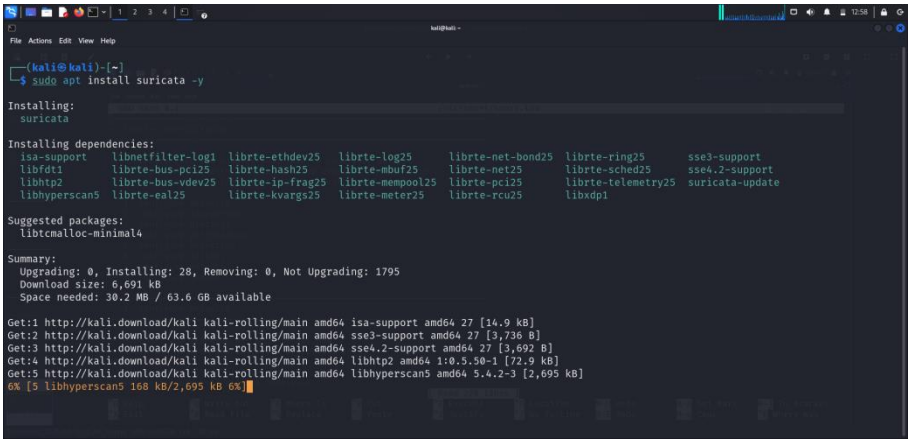
Confirmed logs with tags: syslog, pf, or pfSense





Step 3: Install Suricata IDS

If our Wazuh agent is installed on Kali, then we will also install Suricata on Kali's terminal.



Step 4: Configure Snort to Forward Alerts

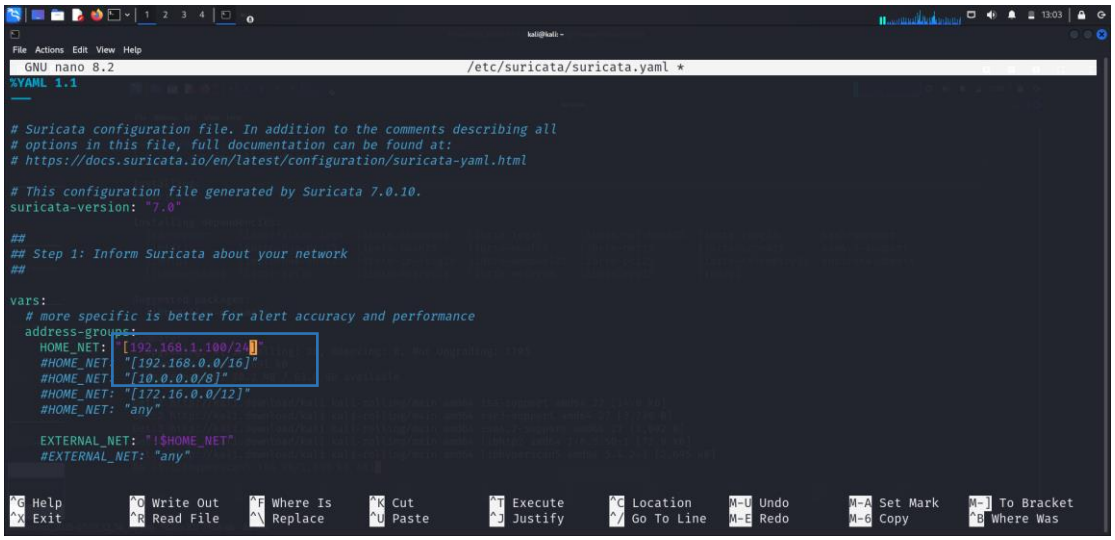
Enabled rules and logging inside Snort settings

Ensured alerts were forwarded via syslog to Wazuh Manager

After instalation so we will edit the configuration of suricata

sudo nano /etc/suricata/suricata.yaml

type in terminal And at home_net put host ip(kali ip)



After this restart suricata for forwarding logs to wazuh dashboard

```
--2025-07-13 13:00:43--  https://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz
Resolving rules.emergingthreats.net (rules.emergingthreats.net)... 54.166.127.61, 54.91.245.101, 34.198.65.219, ...
Connecting to rules.emergingthreats.net (rules.emergingthreats.net)|54.166.127.61|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4994443 (4.8M) [application/octet-stream]
Saving to: 'emerging.rules.tar.gz.1'

emerging.rules.tar.gz.1             100%[===================>]   4.76M   538KB/s    in 14s

2025-07-13 13:00:58 (348 KB/s) - 'emerging.rules.tar.gz.1' saved [4994443/4994443]

sudo: tar-xvzf: command not found
mv: cannot stat 'rules/*.rules': No such file or directory
sudo: chmod-R: command not found

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/suricata/suricata.yaml

┌──(kali㉿kali)-[~]
└─$ sudo ip link set eth0 promisc on

┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart suricata
sudo systemctl enable suricata
Synchronizing state of suricata.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable suricata
Created symlink '/etc/systemd/system/multi-user.target.wants/suricata.service' → '/usr/lib/systemd/system/suricata.service'.

┌──(kali㉿kali)-[~]
└─$
```

Make Wazuh Agent Read eve.json

Open wazuh agent configuration file
sudo nano /var/ossec/etc/ossec.conf

```
  GNU nano 8.2                                  /var/ossec/etc/ossec.conf
<!--
  Wazuh - Agent - Default configuration for kali 2024.4
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>10.245.1.87</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>kali, kali2024, kali2024.4</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>

  <client_buffer>
    <!-- Agent buffer options -->
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
                                   [ Read 229 lines ]
^G Help      ^O Write Out   ^F Where Is    ^K Cut       ^T Execute   ^C Location  M-U Undo      M-A Set Mark   M-] To Bracket
^X Exit      ^R Read File   ^\ Replace     ^U Paste     ^J Justify   ^/ Go To Line M-E Redo      M-6 Copy       ^B Where Was
```

After this restart wazuh-agent

Step 5: Simulate Port Scan from Kali using Nmap

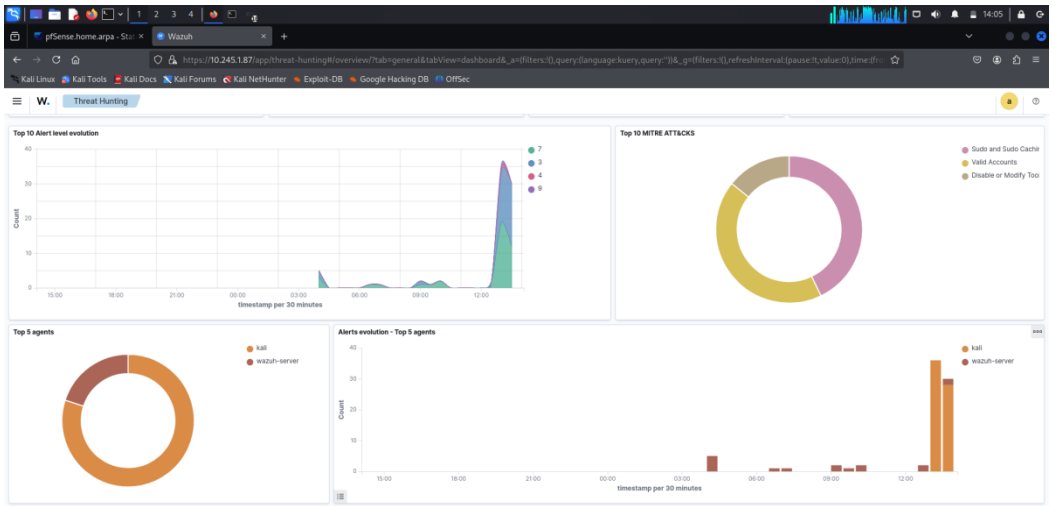
From Kali, ran:

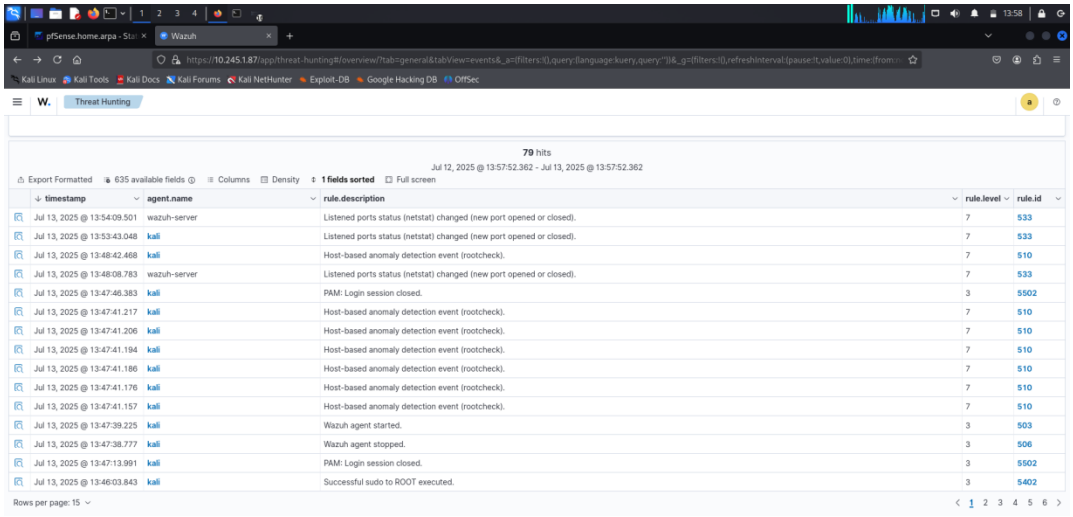
nmap -sS -T4 https://10.245.1.87 (wazuh ip)

```
Nmap done: 1 IP address (1 host up) scanned in 4.41 seconds

┌──(kali㉿kali)-[~]
└─$  nmap -sS -T4 10.245.1.87
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-13 13:56 EDT
Nmap scan report for 10.245.1.87
Host is up (0.0017s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.89 seconds

┌──(kali㉿kali)-[~]
└─$
```

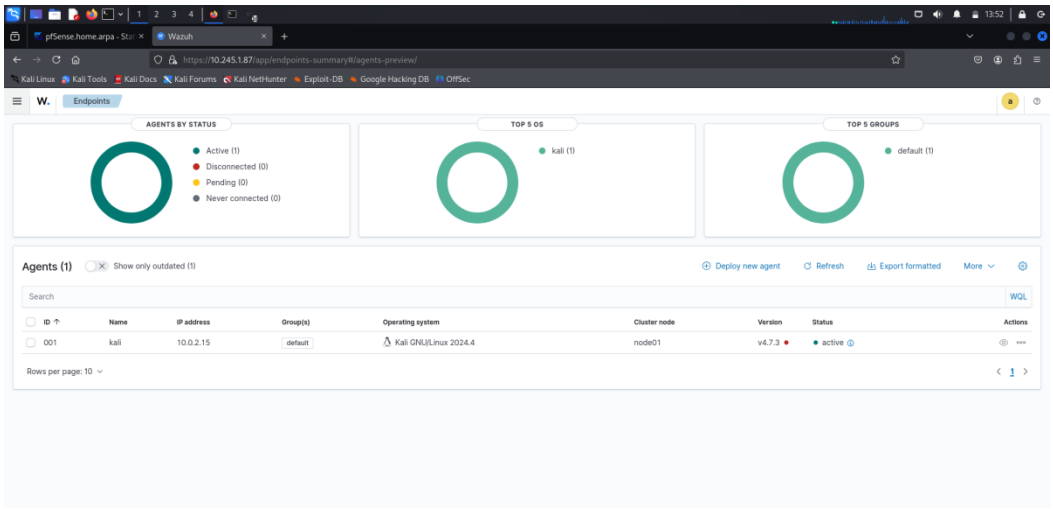
Step 6: Capture Suricata Alert in Wazuh

Navigated in Wazuh:
Found alert matching simulated port scan

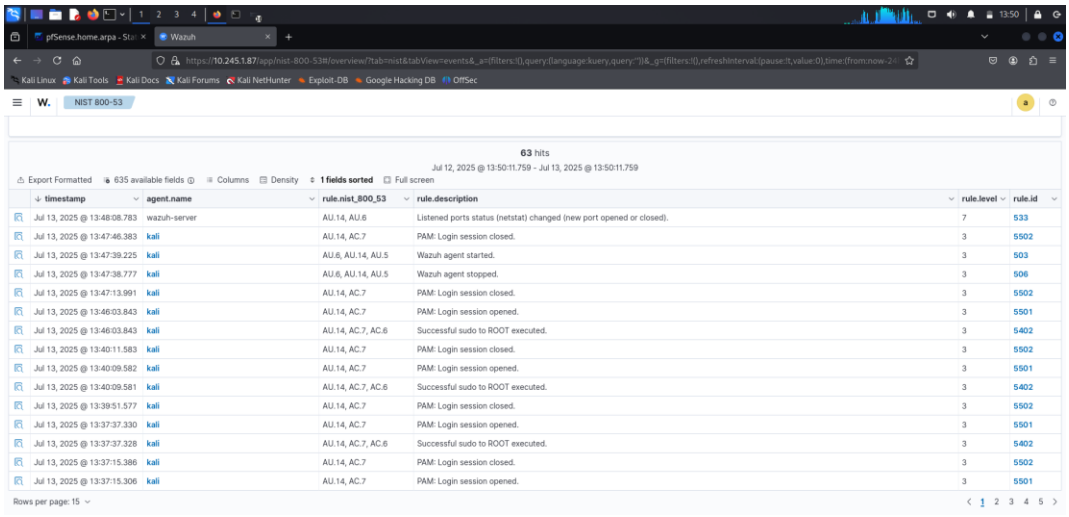




timestamp	agent.name	rule.description	rule.level	rule.id
Jul 13, 2025 @ 13:54:09.501	wazuh-server	Listened ports status (netstat) changed (new port opened or closed).	7	533
Jul 13, 2025 @ 13:53:43.048	kali	Listened ports status (netstat) changed (new port opened or closed).	7	533
Jul 13, 2025 @ 13:48:42.468	kali	Host-based anomaly detection event (rootcheck).	7	510
Jul 13, 2025 @ 13:48:08.783	wazuh-server	Listened ports status (netstat) changed (new port opened or closed).	7	533
Jul 13, 2025 @ 13:47:46.383	kali	PAM: Login session closed.	3	5502
Jul 13, 2025 @ 13:47:41.217	kali	Host-based anomaly detection event (rootcheck).	7	510
Jul 13, 2025 @ 13:47:41.206	kali	Host-based anomaly detection event (rootcheck).	7	510
Jul 13, 2025 @ 13:47:41.194	kali	Host-based anomaly detection event (rootcheck).	7	510
Jul 13, 2025 @ 13:47:41.186	kali	Host-based anomaly detection event (rootcheck).	7	510
Jul 13, 2025 @ 13:47:41.176	kali	Host-based anomaly detection event (rootcheck).	7	510
Jul 13, 2025 @ 13:47:41.157	kali	Host-based anomaly detection event (rootcheck).	7	510
Jul 13, 2025 @ 13:47:39.225	kali	Wazuh agent started.	3	503
Jul 13, 2025 @ 13:47:38.777	kali	Wazuh agent stopped.	3	506
Jul 13, 2025 @ 13:47:13.991	kali	PAM: Login session closed.	3	5502
Jul 13, 2025 @ 13:46:03.843	kali	Successful sudo to ROOT executed.	3	5402



ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	kali	10.0.2.15	default	Kali GNU/Linux 2024.4	node01	v4.7.3	active	



timestamp	agent.name	rule.nist_800_53	rule.description	rule.level	rule.id
Jul 13, 2025 @ 13:48:08.783	wazuh-server	AU.14, AU.6	Listened ports status (netstat) changed (new port opened or closed).	7	533
Jul 13, 2025 @ 13:47:46.383	kali	AU.14, AC.7	PAM: Login session closed.	3	5502
Jul 13, 2025 @ 13:47:39.225	kali	AU.6, AU.14, AU.5	Wazuh agent started.	3	503
Jul 13, 2025 @ 13:47:38.777	kali	AU.6, AU.14, AU.5	Wazuh agent stopped.	3	506
Jul 13, 2025 @ 13:47:13.991	kali	AU.14, AC.7	PAM: Login session closed.	3	5502
Jul 13, 2025 @ 13:46:03.843	kali	AU.14, AC.7	PAM: Login session opened.	3	5501
Jul 13, 2025 @ 13:46:03.843	kali	AU.14, AC.7, AC.6	Successful sudo to ROOT executed.	3	5402
Jul 13, 2025 @ 13:40:11.583	kali	AU.14, AC.7	PAM: Login session closed.	3	5502
Jul 13, 2025 @ 13:40:09.582	kali	AU.14, AC.7	PAM: Login session opened.	3	5501
Jul 13, 2025 @ 13:40:09.581	kali	AU.14, AC.7, AC.6	Successful sudo to ROOT executed.	3	5402
Jul 13, 2025 @ 13:39:51.577	kali	AU.14, AC.7	PAM: Login session closed.	3	5502
Jul 13, 2025 @ 13:37:37.330	kali	AU.14, AC.7	PAM: Login session opened.	3	5501
Jul 13, 2025 @ 13:37:37.328	kali	AU.14, AC.7, AC.6	Successful sudo to ROOT executed.	3	5402
Jul 13, 2025 @ 13:37:15.386	kali	AU.14, AC.7	PAM: Login session closed.	3	5502
Jul 13, 2025 @ 13:37:15.306	kali	AU.14, AC.7	PAM: Login session opened.	3	5501

4. Result Summary

pfSense successfully forwarded logs to Wazuh via syslog

Snort IDS detected simulated attack (port scan)

Alerts were visible in real-time on Wazuh Dashboard