Suricata NIDS Tools Project Report

Prepared By: Olatunji Lawal

5th July, 2025

Outline

1. Summary

Suricata is an advanced, open-source network intrusion detection and prevention system (NIDS/NIPS) created by the Open Information Security Foundation. It does real-time packet analysis, protocol identification, and generates alerts for questionable network activities. This project explains how to install, configure, and utilize the Suricata Intrusion Detection System (IDS) to monitor and warn network traffic. It takes a step-by-step approach, from installation to alarm investigation, which includes custom rule generation.

---

2. Objectives

- Install and configure Suricata.
- Update Suricata and its rule sets
- Add a custom detection rule
- Run and test Suricata to trigger and analyze alerts
- Document findings for analysis and reporting

---

3. Environment Setup

- **Operating System:** Kali Linux - Debian
- **Suricata Version:** [Insert Version]
- **Tools Used:** Terminal

4. Execution Steps

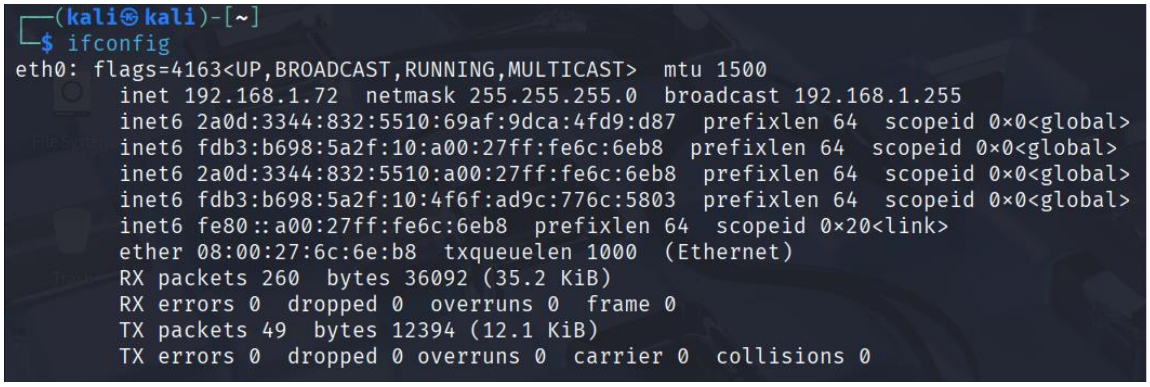
4.1: Install Suricata

Suricata must be installed on the target host system using the appropriate package for the operating system. The interface needs to be established first by using **ifconfig** command.

Commands used to install Suricata (for Kali/Debian):

sudo apt update

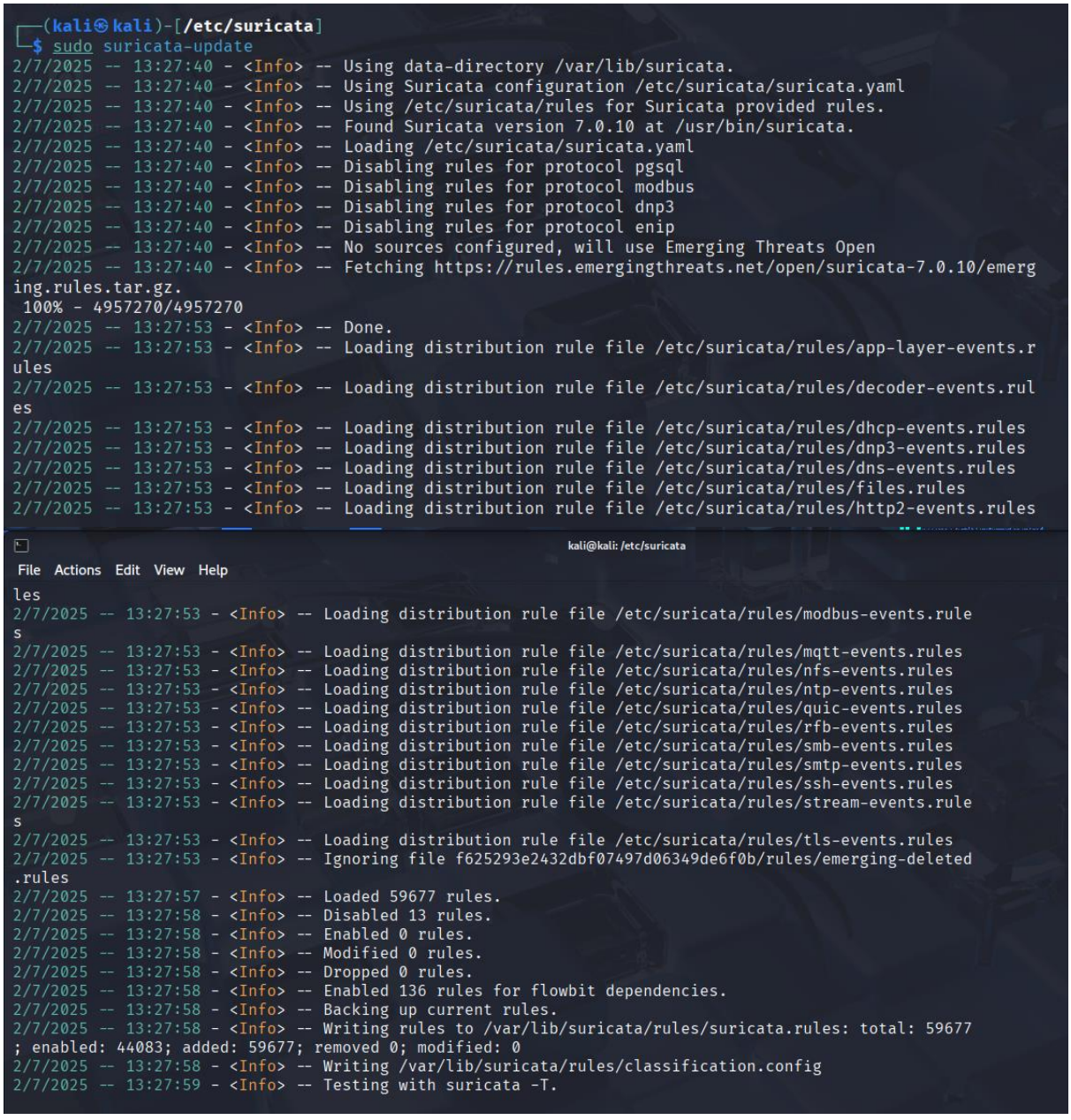
sudo apt install suricata



4.2: Update Suricata

To ensure the latest threat detection capabilities, updated rule sets with the latest version:

sudo suricata-update



4.3: Set a New Rule in Rule Destination

A custom rule was added to detect specific network activity.

Custom rules are typically stored in /etc/suricata/rules/

```
┌──(kali㉿kali)-[/etc/suricata]
└─$ cd rules

┌──(kali㉿kali)-[/etc/suricata/rules]
└─$ ls
app-layer-events.rules  dhcp-events.rules  ftp-events.rules    kerberos-events.rules  ntp-events.rules   smtp-events.rules
cybersec.rules          dnp3-events.rules  http2-events.rules  modbus-events.rules    quic-events.rules  ssh-events.rules
cybersec.rules.save     dns-events.rules   http-events.rules   mqtt-events.rules      rfb-events.rules   stream-events.rules
decoder-events.rules    files.rules        ipsec-events.rules  nfs-events.rules       smb-events.rules   tls-events.rules
```

```
┌──(olatunji㉿Desktop)-[/var/lib/suricata/rules]
└─$ sudo rm -r cybersec.rules

┌──(olatunji㉿Desktop)-[/var/lib/suricata/rules]
└─$ ls
classification.config  suricata.rules

┌──(olatunji㉿Desktop)-[/var/lib/suricata/rules]
└─$
```

Ensure this is referenced in the main configuration file:

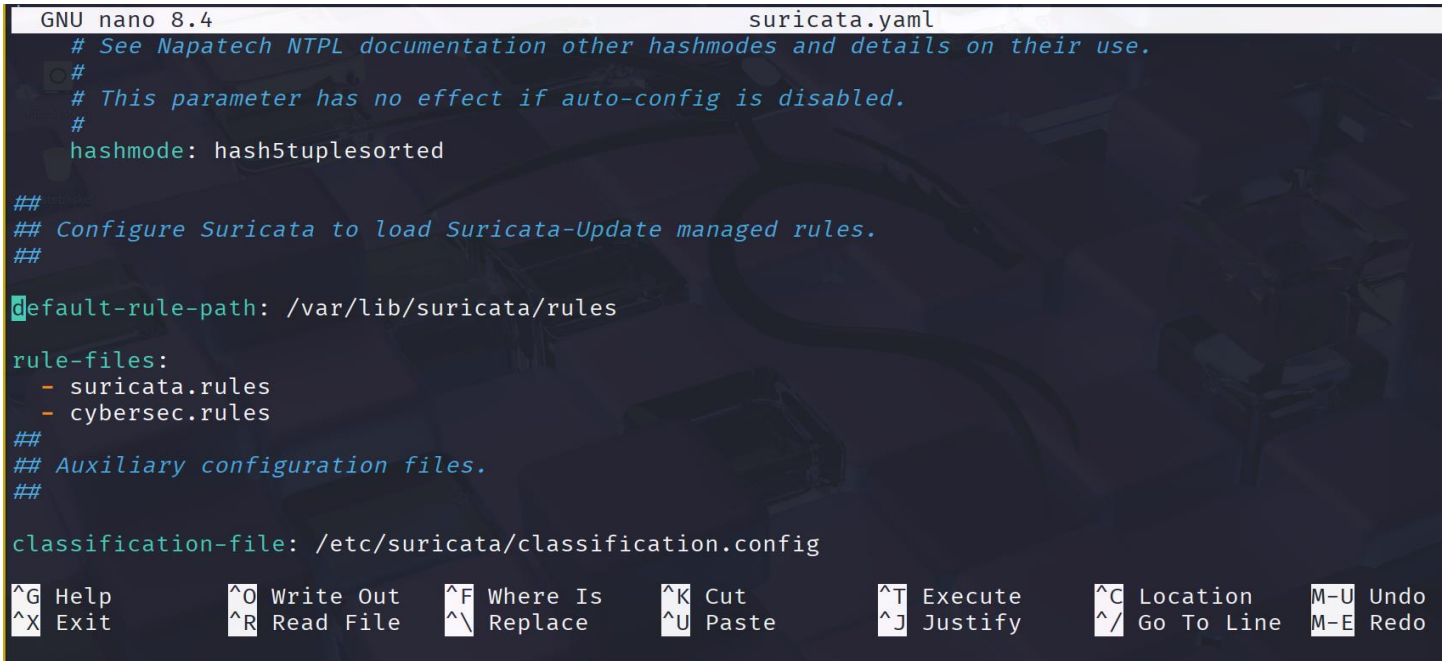
/etc/suricata/suricata.yaml

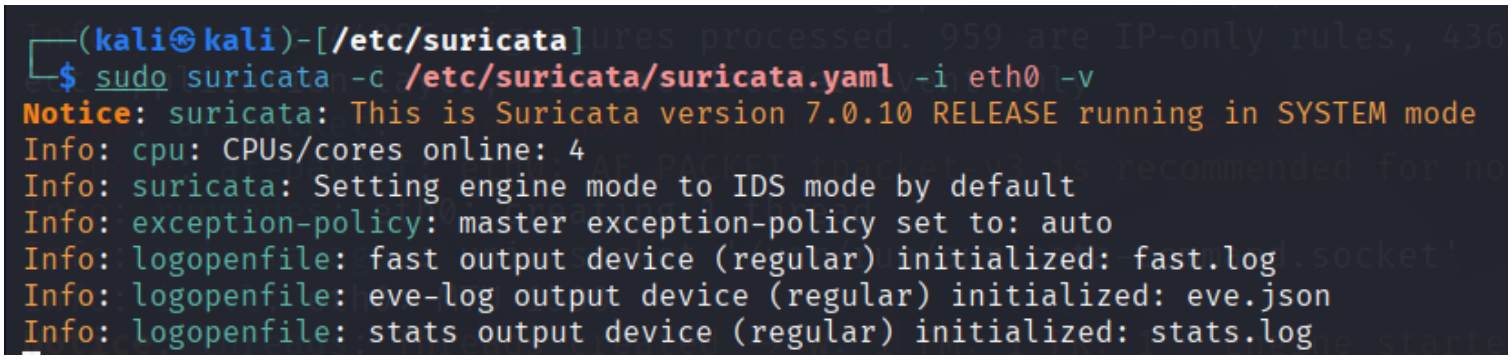
```
┌──(olatunji㉿Desktop)-[/etc/suricata]
└─$ sudo nano suricata.yaml
```

4.4: Add a New Rule

Add a basic ICMP alert rule to detect ping traffic:

- alert icmp any any → any any (msg: “I detected an ICMP request”; itype:8; sid:1000001; rev:1)



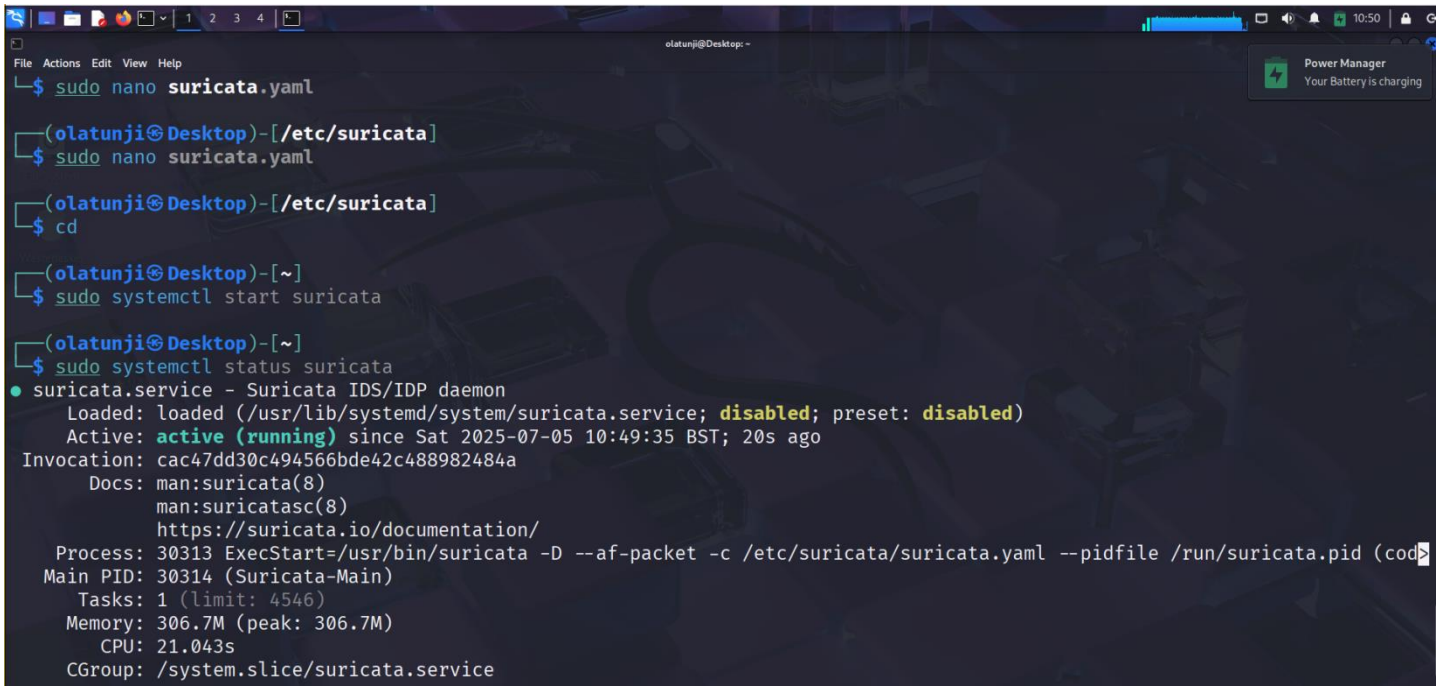


4.5: Start Suricata

Checked status:

sudo systemctl status suricata

sudo systemctl start suricata



4.6: Run Suricata

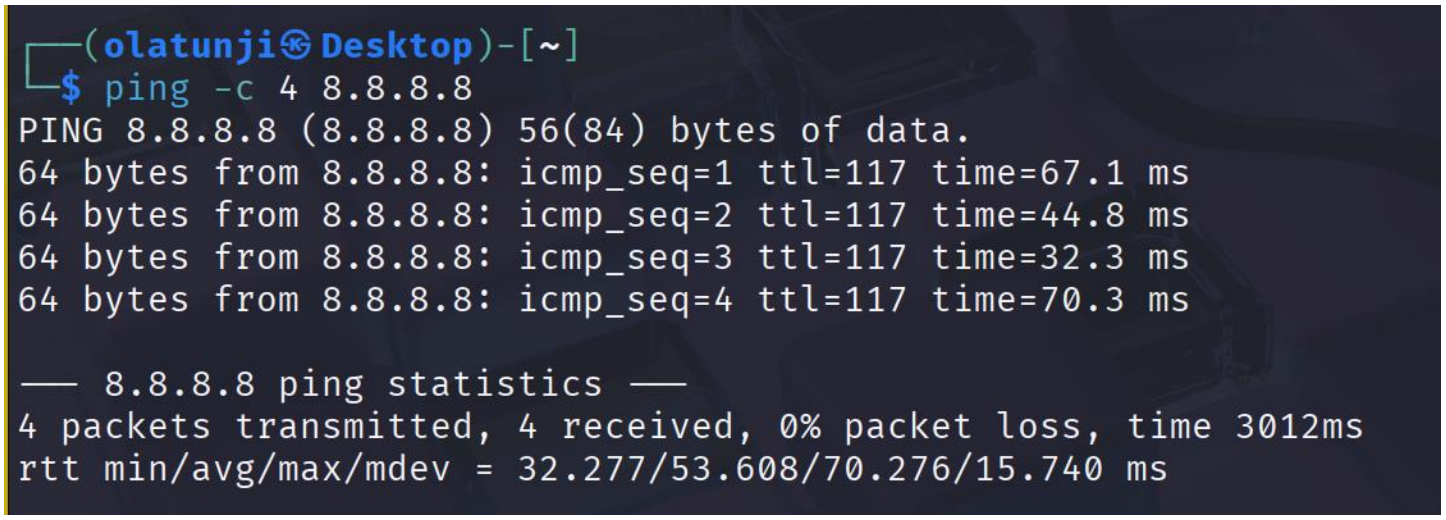
Suricata was run in test mode and in live monitoring mode using:

sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -V

4.7: Trigger the Alert

Used ping command to generate ICMP traffic and trigger the rule:

ping 8.8.8.8



4.8: Investigate

Suricata logs were checked at:

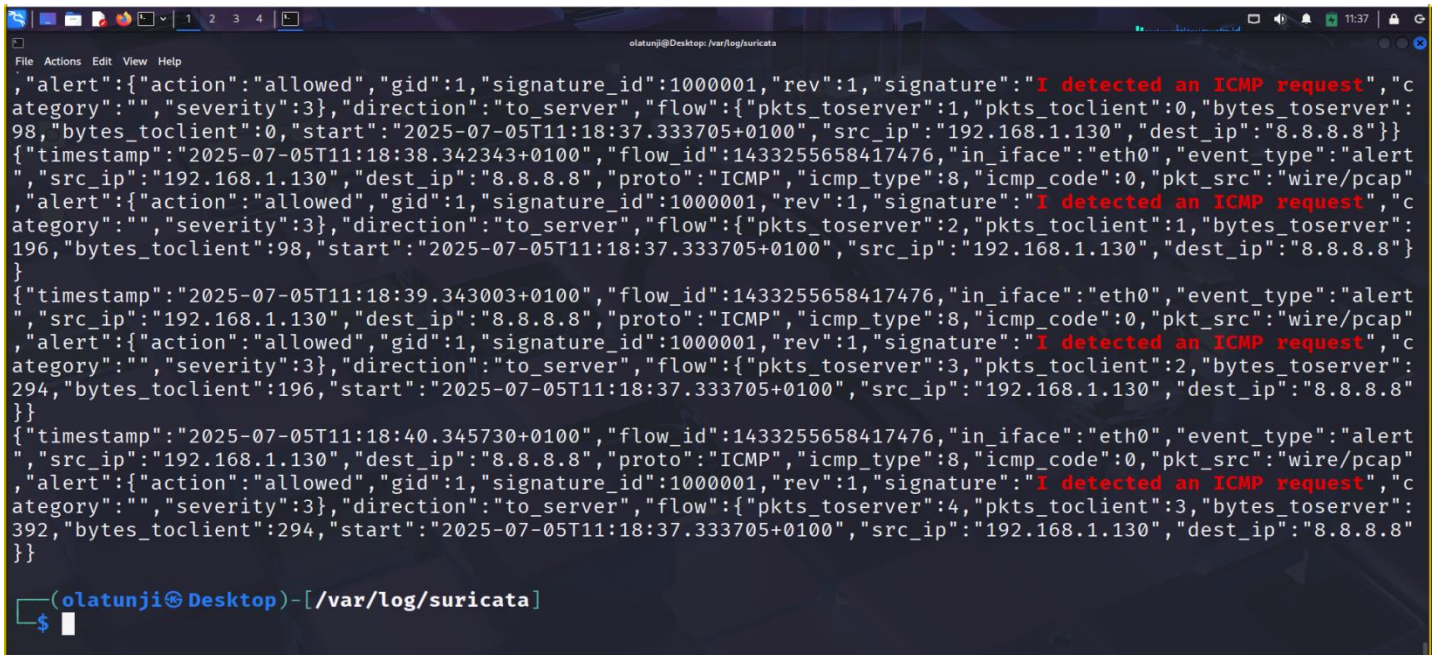
/var/log/suricata/eve.json

Used the following tools:

- cat /var/log/suricata/fast.log

Summary of findings:

- The custom ICMP rule was triggered successfully.
- Source and destination IPs were identified.
- Timestamp and payload were analyzed for confirmation.



---

5. Key Learnings

- Writing and testing custom IDS rules
- Interpreting Suricata alert logs
- Understanding packet behaviour triggering alerts
- Real-time IDS monitoring

---

6. Conclusion

Using a custom rule, the Suricata IDS was successfully configured, tested, and validated. This process shows how to successfully setup Suricata for simple threat detection. I've laid the groundwork for future network defense. This real-world application improved comprehension of log analysis and NIDS operation. Now, Suricata may be extended to include threat hunting, complete intrusion detection, and integration with programs like Splunk, SIEM, or ELK Slack.

Report prepared by:

Olatunji Lawal

Cybersecurity Analyst