Network Intrusion Detection System Report

Project Name: Network Intrusion Detection System using Suricata
Internship Program: CodeAlpha Cyber Security Internship
Intern Name: Mahnoor Shafi
Date: [20-8-2025 - 20-9-2025]

Table of Content:

Introduction

Tools & Requirements

Project Objective

Implementation Steps

4.1 Installing Suricata

4.2 Running Suricata in IDS Mode

4.3 Creating Custom Rules

4.4 Testing with Ping/Nmap

4.5 Checking Alerts in Logs

Output & Results

Advantages of IDS

Real-World Applications

Conclusion

1. Introduction

A **Network Intrusion Detection System (NIDS)** is a cybersecurity tool that monitors network traffic and detects suspicious or malicious activities.
In this project, I implemented **Suricata**, an open-source IDS, to monitor network traffic, create custom rules, and detect attacks like **ICMP pings.**

2. Tools & Requirements

Linux VM

Suricata IDS

ping utility (for ICMP test)

Text editor (nano/vim)

Suricata-Update for community rules

3. Project Objective

The main objectives were:

Install and configure Suricata IDS.

Write and test custom detection rules.

Generate real attack traffic (ping).

Detect and log alerts in Suricata logs.

4. Implementation Steps

4.1 Installing Suricata

Suricata was installed on Liunx using the official repository:

sudo add-apt-repository ppa:oisf/suricata-stable -y
sudo apt update
sudo apt install suricata -y

4.2 Running Suricata in IDS Mode

Suricata was started in IDS mode using the active network interface:

sudo suricata -i eth0 -v

```
File  Actions  Edit  View  Help
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff
    inet 10.104.208.30/24 brd 10.104.208.255 scope global dynamic noprefixroute eth0
       valid_lft 3225sec preferred_lft 3225sec
    inet6 fe80::92dd:c728:695f:fdf9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ab:f4:24 brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~]
└─$ sudo suricata -i eth0 -v
Notice: suricata: This is Suricata version 7.0.11 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: alert-syslog: Syslog output initialized
Warning: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
Warning: detect: 1 rule files specified, but no rules were loaded!
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 0 signatures processed. 0 are IP-only rules, 0 are inspecting packet payload, 0 inspect application layer, 0 are decoder event only
Error: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99 already in use.
Warning: af-packet: eth0: AF_PACKET tpacket-v3 is recommended for non-inline operation
Info: runmodes: eth0: creating 1 thread
Info: unix-manager: unix socket '/var/run/suricata-command.socket'
Info: ioctl: eth0: MTU 1500
Notice: threads: Threads created → W: 1 FM: 1 FR: 1   Engine started.
```

4.3 Creating Custom Rules

A custom rule was added in /etc/suricata/rules/local.rules:

alert icmp any any -> any any (msg:"ICMP Ping detected"; sid:1000001; rev:1;)

```
File  Actions  Edit  View  Help
  GNU nano 8.2                    /etc/suricata/rules/local.rules *
alert icmp any any → any any (msg:"ICMP Ping detected"; sid:1000001; rev:1;)

^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
```

```
GNU nano 8.2                                  /etc/suricata/suricata.yaml
    # The most common hashmode commands are:  hash2tuple, hash2tuplesorted,
    # hash5tuple, hash5tuplesorted and roundrobin.
    #
    # See Napatech NTPL documentation other hashmodes and details on their use.
    #
    # This parameter has no effect if auto-config is disabled.
    #
    hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /etc/suricata/rules

rule-files:
  - local.rules

##
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
# threshold-file: /etc/suricata/threshold.config

                                    [ Wrote 2211 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
```

Suricata IDS mode run *Engine started:*

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -v

[sudo] password for kali:
Notice: suricata: This is Suricata version 7.0.11 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: alert-syslog: Syslog output initialized
Info: detect: 1 rule files processed. 1 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 1 signatures processed. 1 are IP-only rules, 0 are inspecting packet payload, 0 inspect application layer, 0 are decoder event only
Error: af-packet: fanout not supported by kernel: kernel too old or cluster-id 99 already in use.
Warning: af-packet: eth0: AF_PACKET tpacket-v3 is recommended for non-inline operation
Info: runmodes: eth0: creating 1 thread
Info: unix-manager: unix socket '/var/run/suricata-command.socket'
Info: ioctl: eth0: MTU 1500
Notice: threads: Threads created → W: 1 FM: 1 FR: 1   Engine started.
```

4.4 Testing with Ping

Ping test:

ping -c 4 8.8.8.8
Creating traffic for testing

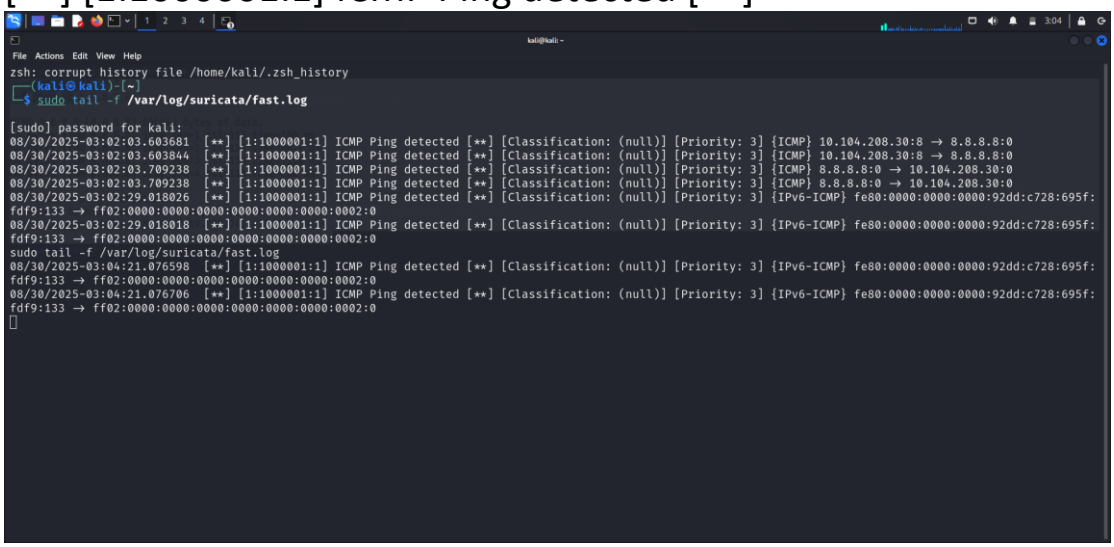
4.5 Checking Alerts in Logs

Suricata logs were checked in fast.log:

sudo tail -f /var/log/suricata/fast.log

Detected alert:

[**] [1:1000001:1] ICMP Ping detected [**]

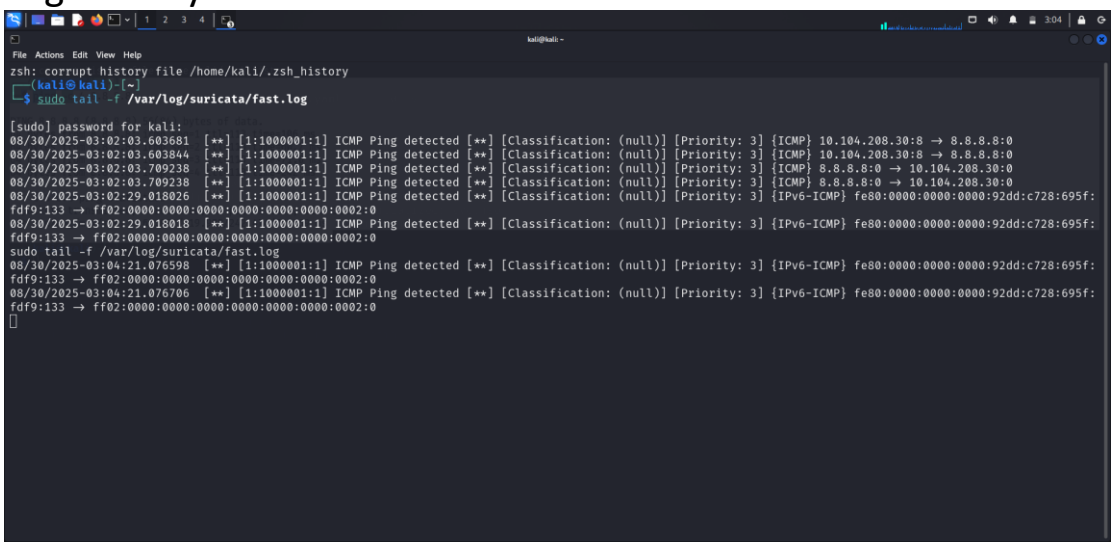


5. Output & Results

Suricata successfully detected **ICMP pings**.

Nmap scans generated intrusion alerts.

Logs clearly showed detection



6. Advantages of IDS

Detects malicious activity in real-time.

Helps in early warning for network intrusions.

Generates logs useful for forensic investigation.

7. Real-World Applications

Used in **Security Operations Centers (SOCs)**.

Detecting **malware traffic** and **data exfiltration**.

Helps organizations meet **compliance and monitoring standards**.

Forms part of **defense-in-depth strategy**.

8. Conclusion

This project successfully demonstrated setting up and using Suricata as a **Network Intrusion Detection System**.
Custom rules were implemented and tested with real traffic, confirming that Suricata can detect suspicious activities effectively.
This hands-on task improved my understanding of **network security monitoring** and **threat detection systems.**