**FACULTY OF COMPUTER SCIENCE AND ENGINEERING**

**Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Topi**

**Lab No: 7 Instructor: Mr. Mohammad Farrukh Tahir**

## 1. Introduction

Suricata is a powerful open-source network threat detection system capable of operating as an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS). This manual provides detailed instructions to set up and test Suricata on Kali Linux.

## 2. Installation

1. Update System and Install Suricata:  
sudo apt update  
sudo apt install suricata -y

2. Verify Installation:  
suricata --version

## 3. Configuration

1. Open the Configuration File:  
sudo nano /etc/suricata/suricata.yaml

2. Set the Monitoring Interface:

Locate the `af-packet` section and ensure it monitors the desired interface (e.g., `eth0`):

af-packet:  
 - interface: eth0  
 - threads: auto

3. Specify Rule Files:

Ensure the `rule-files` section points to the correct location for rules:  
rule-files:  
 - suricata.rules

4. Save and Exit:

Save the file (`Ctrl + O`, `Enter`) and exit (`Ctrl + X`).

## 4. Download and Update Rules

1. Install the Suricata Rule Update Tool:  
sudo apt install suricata-update -y

2. Download Rules:  
sudo suricata-update

3. Verify Rules Location:

Ensure rules are downloaded to `/var/lib/suricata/rules/`:  
  
ls /var/lib/suricata/rules/

## 5. Add Custom Rules

1. Open the Rules File:  
sudo nano /var/lib/suricata/rules/suricata.rules

2. Add an Alert Rule for ICMP Traffic:   
alert icmp any any -> any any (msg:"ICMP Traffic Detected"; sid:1000001; rev:1;)

3. Add a Drop Rule for ICMP Traffic:   
drop icmp any any -> any any (msg:"ICMP Traffic Blocked"; sid:1000002; rev:1;)

4. Save and Exit.

## 6. Running Suricata

6.1 IDS Mode  
- Suricata monitors traffic and generates alerts but does not block or interfere.

Run Suricata in IDS mode:  
sudo suricata -c /etc/suricata/suricata.yaml -i eth0

6.2 IPS Mode  
- Suricata actively blocks or rejects traffic based on rules.  
Configure NFQUEUE rules using `iptables`:  
sudo iptables -I INPUT -i eth0 -j NFQUEUE --queue-num 0  
sudo iptables -I OUTPUT -o eth0 -j NFQUEUE --queue-num 0

Run Suricata in IPS mode:  
sudo suricata -q 0 -c /etc/suricata/suricata.yaml

## 7. Testing

7.1 Ping Test

1. From a different device or host (e.g., Windows), ping the Kali VM:  
ping <kali\_vm\_ip>

2. \*\*Check Logs in IDS Mode\*\*:

Suricata logs alerts in `/var/log/suricata/fast.log`:  
sudo tail -f /var/log/suricata/fast.log

3. \*\*Expected Log Entry for Alert Rule\*\*:  
11/12/2024-12:34:56.789012 [\*\*] [1:1000001:1] ICMP Traffic Detected [\*\*]

4. \*\*In IPS Mode (Drop Rule)\*\*:

- The ping should fail with `Request timed out`.

- Logs should indicate traffic was blocked:  
[\*\*] [1:1000002:1] ICMP Traffic Blocked [\*\*]

7.2 Traffic Simulation with hping3

1. Use `hping3` to simulate ICMP flood:  
sudo hping3 -1 --flood <kali\_vm\_ip>

2. \*\*Verify Blocking\*\*:

- In IPS mode, Suricata should block this traffic.

- Monitor logs for drop events.