🧪 Exercise: Install, Configure, and Test Suricata on Ubuntu 24.04

📝 Objective

By the end of this exercise, you will be able to:

- Install Suricata
- Configure basic rules
- Run Suricata in IDS mode
- Test Suricata with a simple network attack pattern

🛠️ Prerequisites

- A clean Ubuntu 24.04 server (bare metal or VM)
- Root or sudo access
- Internet connection

🧩 Part 1: Installation

1. Update the system

```
sudo apt update && sudo apt upgrade -y
```

2. Add the Suricata PPA and install

```
sudo apt install -y software-properties-common
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install -y suricata
```

3. Check the installation

```
suricata --build-info | grep 'Suricata version'
```

⚙️ Part 2: Configuration

1. Check default configuration file

```
sudo nano /etc/suricata/suricata.yaml
```

> Optional: Change the default interface (look for the `af-packet` section)

```
af-packet:
  - interface: eth0   # Replace eth0 with your actual interface name
```

2. Identify your network interface

```
ip a
```

Note your active interface (e.g. `ens33`, `eth0`, etc.)

🧪 Part 3: Test Rules

1. Download default rule set

```
sudo apt install -y suricata-update
sudo suricata-update
```

2. Add a custom test rule

Create a test rule file:

```
sudo nano /etc/suricata/rules/local.rules
```

Paste this test rule:

```
alert icmp any any -> any any (msg:"ICMP Packet Detected"; sid:1000001; rev:1;)
```

3. Edit suricata.yaml to enable local rules

Open the config file:

```
sudo nano /etc/suricata/suricata.yaml
```

Find and set the rule-files section:

```
rule-files:
  - local.rules
```

Save and exit.

▶️ Part 4: Running Suricata

1. Run Suricata in IDS mode

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

(Replace `eth0` with your actual interface)

Keep this terminal running.

🧪 Part 5: Testing Suricata

1. Open a second terminal and ping any host

```
ping 8.8.8.8
```

Let it run for a few seconds, then stop it.

2. Check Suricata logs

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

You should see an alert similar to:

```
[**] [1:1000001:1] ICMP Packet Detected [**]
```

✅ Part 6: Cleanup & Enable as a Service (Optional)

If you want Suricata to start at boot:

```
sudo systemctl enable suricata
sudo systemctl start suricata
```

To check the status:

```
sudo systemctl status suricata
```

📌 Summary

Step	Description
1	Installed Suricata and rule sets
2	Configured interface and test rules
3	Ran Suricata in IDS mode
4	Verified alerts from test traffic

August 22, 2025