**Suricata as IDS, IPS, and Network Security Monitoring**

**Suricata** is an open-source tool designed for **Intrusion Detection (IDS)**, **Intrusion Prevention (IPS)**, and **Network Security Monitoring (NSM)**. It helps organizations monitor, detect, and prevent network threats in real time.

**Key Features**

1. **Intrusion Detection (IDS)**:
   * Monitors network traffic for suspicious activities.
   * Detects threats like malware, unauthorized access, and data breaches.
2. **Intrusion Prevention (IPS)**:
   * Blocks malicious traffic in real time.
   * Prevents attacks like DDoS and exploits.
3. **Network Security Monitoring (NSM)**:
   * Captures and analyzes traffic.
   * Provides logs for protocols like HTTP, DNS, and TLS/SSL.

**Why Suricata?**

* **High Performance**: Multi-threaded design for fast networks.
* **Open Source**: Free and community-supported.
* **Integration**: Works with tools like Elasticsearch and Kibana.
* **Scalable**: Suitable for both small and large networks.

**How It Works**

1. **Traffic Capture**: Monitors all network data.
2. **Rule Matching**: Detects threats using predefined rules.
3. **Alert and Action**: Generates alerts or blocks malicious traffic.

**Benefits**

* Detect and stop threats in real time.
* Gain visibility into network activity.
* Easy to integrate with other tools.

**SURICATA AS AN INTRUSION DETECTION SYSTEM**

Suricata uses its Intrusion Detection System (IDS) capabilities to monitor network traffic and detect suspicious or malicious activities. Here’s how Suricata implements IDS functionality.

**1. Rule-Based Detection**

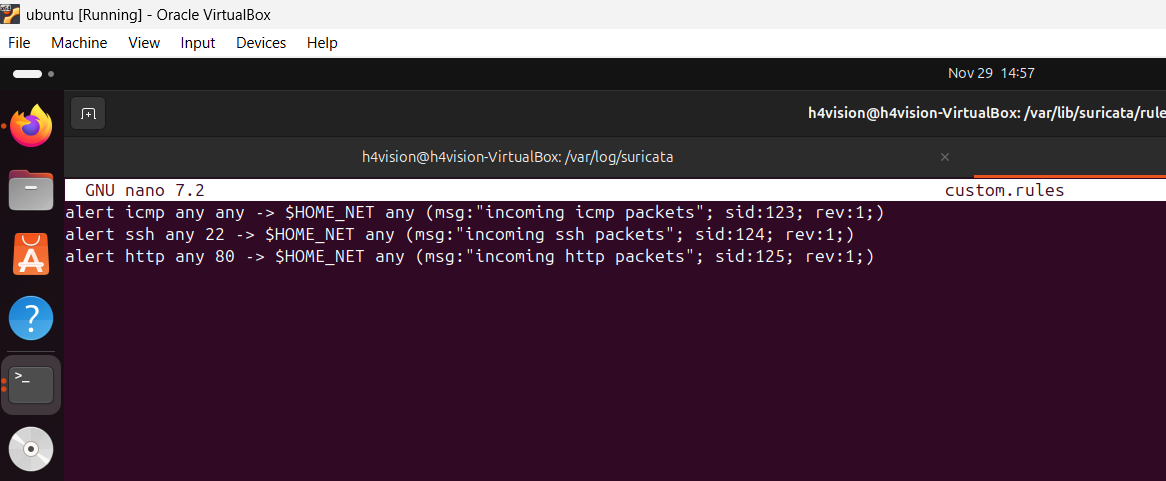
Suricata uses predefined rules to identify known threats. These rules describe patterns of malicious behavior, such as:

* Specific attack signatures (e.g., buffer overflows, SQL injections).
* Suspicious activity patterns (e.g., unauthorized file access, malware behavior).

**Rule Sets:**

from the Ubuntu server, a terminal is open to set up and the following command is ran

**$ sudo nano custom.rules**

****

**Fig 1**

**R**ules set above is for the following prorocols http, ssh and icmp protocols as seen above

**Alert icmp any any –> $HOME\_NET any (msg:”incoming icmp packets”; sid:123; rev:1;)**

**Definition of Rule**

**Alert- notify** when the traffic of set parameter is passing through the network

**Icmp-** protocol that should be reported

First any- Any IP address

Second any- Any port

$HOME\_NET -defines the target machine IP subnet configured with the command below

Unix command= $ **sudo nano etc/suriacata/suriacata.yaml**

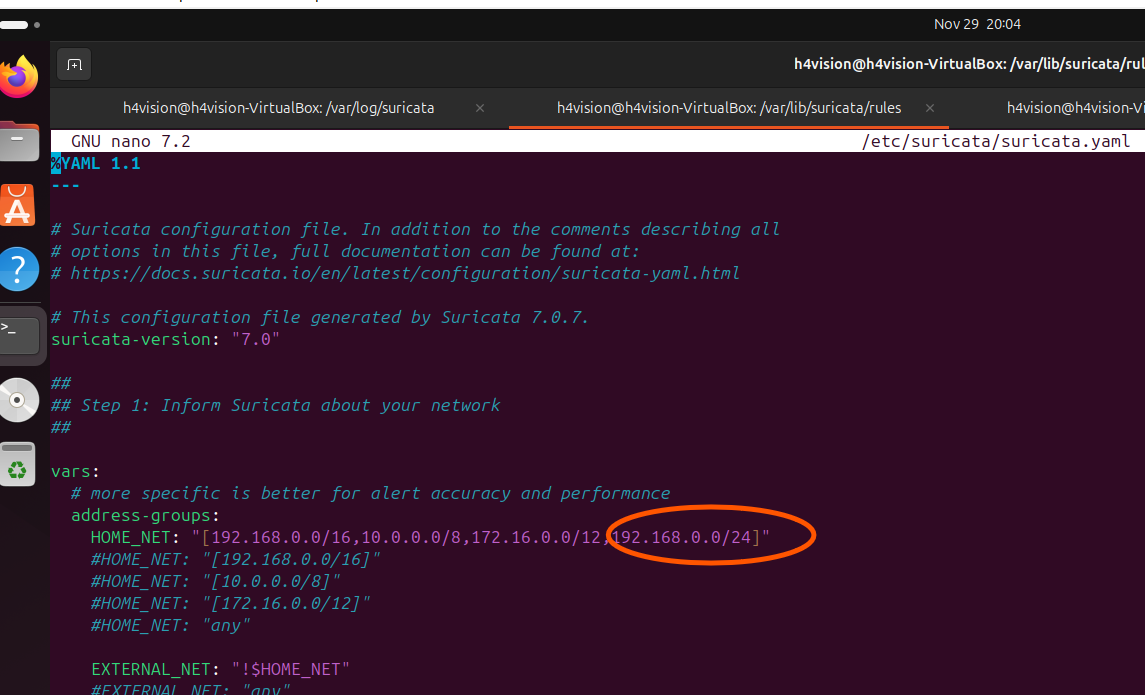


Fig 2

Its also essential to know the network interface that the suricata is running; in this case we are running the suricata in ubuntu linux.

Command = **$ ip addr**

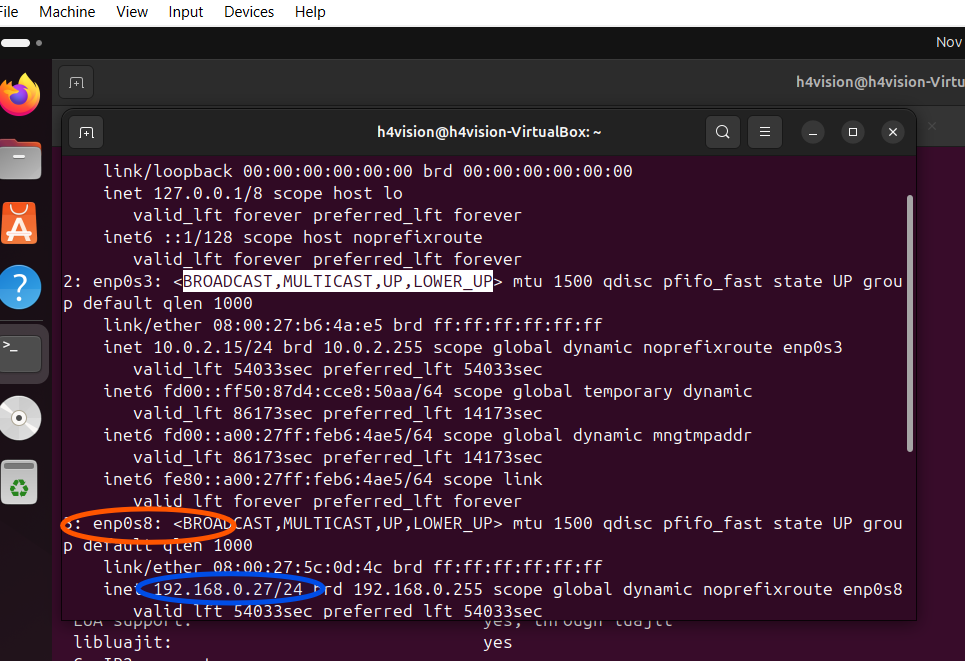


Fig 3

So by implication, our network interface is **enp0s8** and an ip address **192.168.0.27**

* Rules define what constitutes suspicious behaviour, using parameters like protocols, ports

**2. Traffic Capture**

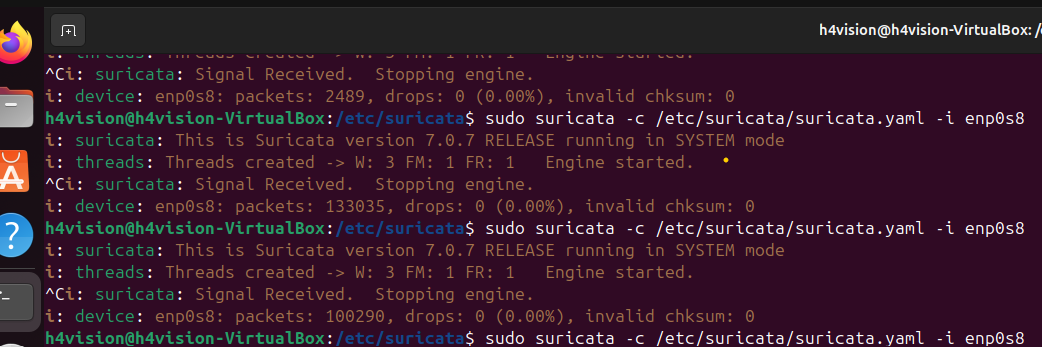
Suricata inspects all network packets passing through a monitored interface in real time. It captures data at various layers of the network stack, including:

* **Packet headers** (e.g., source/destination IP and ports).
* **Payload data** for deep packet inspection.

Tryhack me url was opened on the browser to enable us generate traffic coming from the page but first of all Suricata was started using the command below

Directories on suricata was change to $ /etc/suricata

$ **sudo suricata -c /etc/suricata/suricata.yaml -i enp0s8**

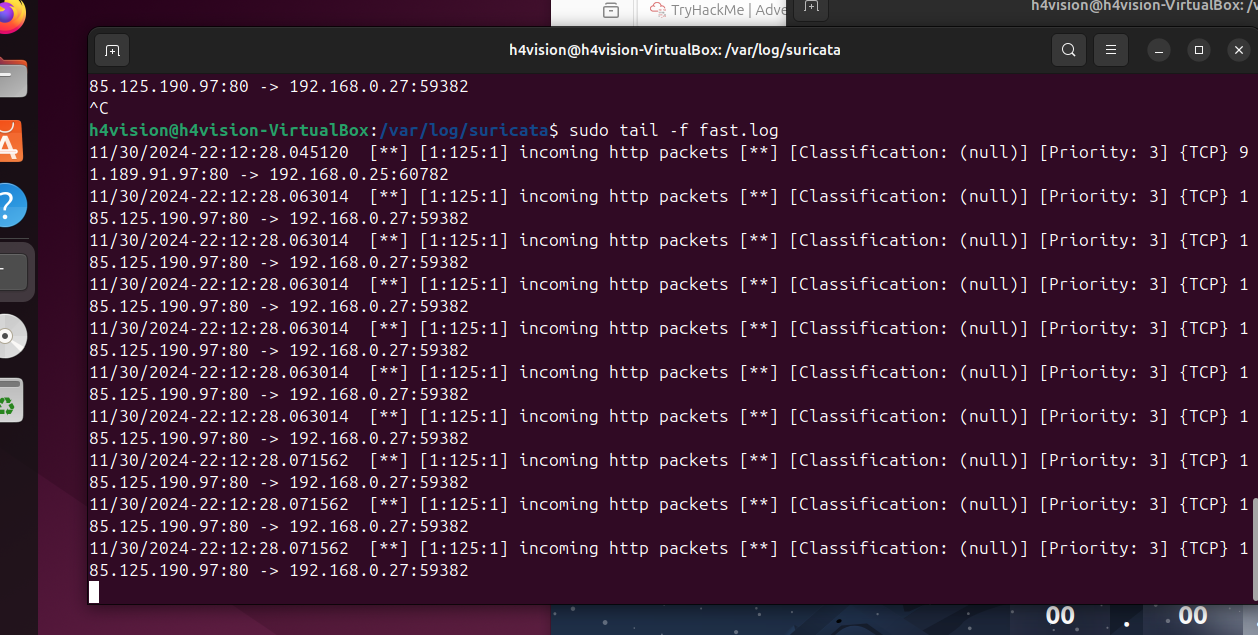
**fig 4**

**$ sudo tail -f fast.log**

**the command is use to track the activites within the network. We are able to see packets according to the rules set in custom.rules**

The traffic log be access in the directories below

**$ /var/log/suricata**

****

**Fig 5**

**In summary, when Suricata detects traffic that matches the rule set, it triggers an alert. Alerts include detailed information such as:**

* **Source and destination IP addresses.**
* **Timestamp of the detection.**
* **Description of the rule that was triggered.**

Analysing the fig 5 above

The image appears to show Suricata logs being monitored in a terminal using the command sudo tail -f fast.log. The logs provide real-time updates of detected traffic, focusing on incoming HTTP packets.

Here’s a breakdown of what the log entries indicate:

**Source and Destination**:

Example: 85.125.190.97:80 -> 192.168.0.27:59382

* Source: 85.125.190.97:80 ( public web server on port 80, HTTP traffic).
* Destination: 192.168.0.27:59382 (internal client on a random port).

**Timestamp**:

* The timestamp (e.g., 30/11/2024-22:12:28.045180) shows when the event was logged.

**Event Details**:

* **Message**: Incoming http packets.

**Classification**: (null)—this means no specific classification was assigned for these packets.

**Priority**: 3—indicates a lower-priority event.

**Protocol**: TCP.