Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Network Protection for Energy Control Systems

These slides outline the essential offensive tools that will be used in this course.

These tools are intended for use within this course to demonstrate how different tools can be employed for various cyberattack activities and address existing security weaknesses to avoid or mitigate related cyber risks. Therefore, all these practical activities are solely intended for educational purposes ONLY and not for any other malicious or unauthorized activities.

IDS
SURICATA

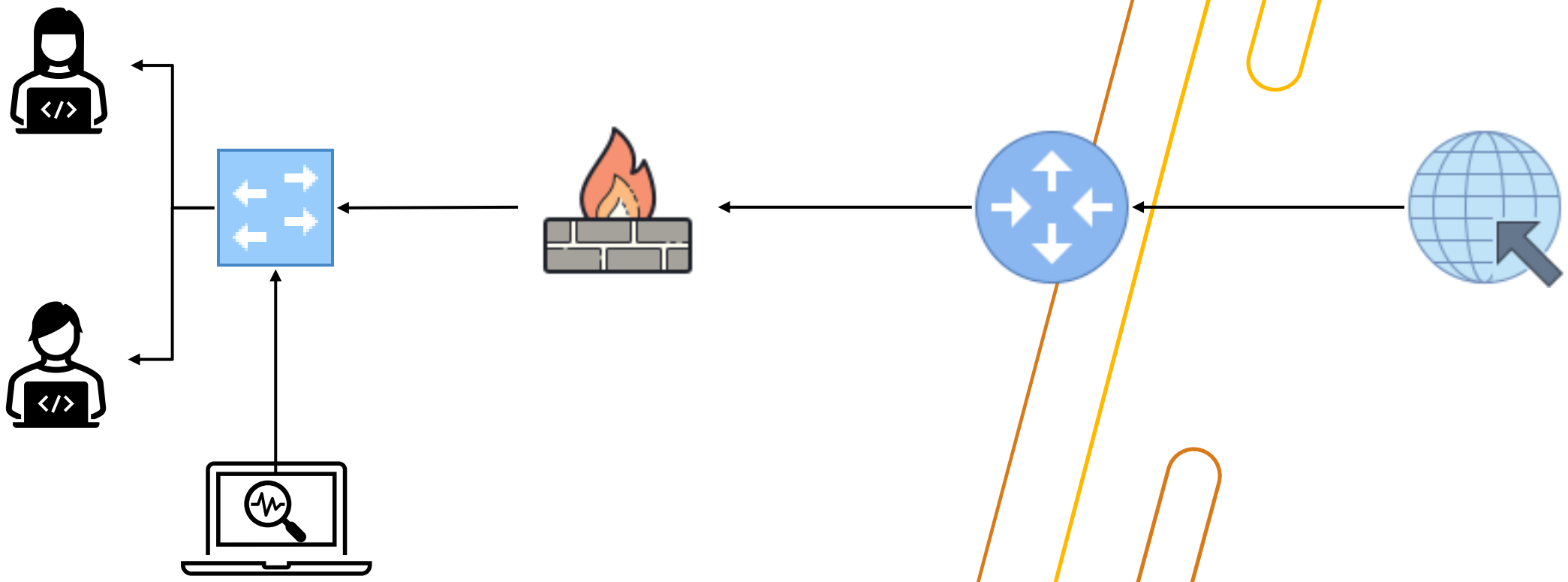
SURICATA

- Suricata is an **open-source-based intrusion detection** system and **intrusion prevention** system
- Suricata **analyzes** all **traffic** on the **interface**, searching for known **attacks** and **anomalies**
- When an **attack** or **anomaly** is **detected**, the system can **decide** whether to **block traffic** or **simply save** the **event** on a **log (/var/log/suricata/fast.log)**
- **Suricata** can be **configured** using sets of **rules** organized in uniform categories.
- Each **category** can be set to:
  - **Enable**: traffic **matching rules** from these **categories** will be **reported**
  - **Block**: traffic **matching rules** from this **category** will be **dropped**
  - **Disable**: **rules** from this category are **ignored**

https://docs.nethserver.org/en/v7/suricata.html

SURICTA Modes

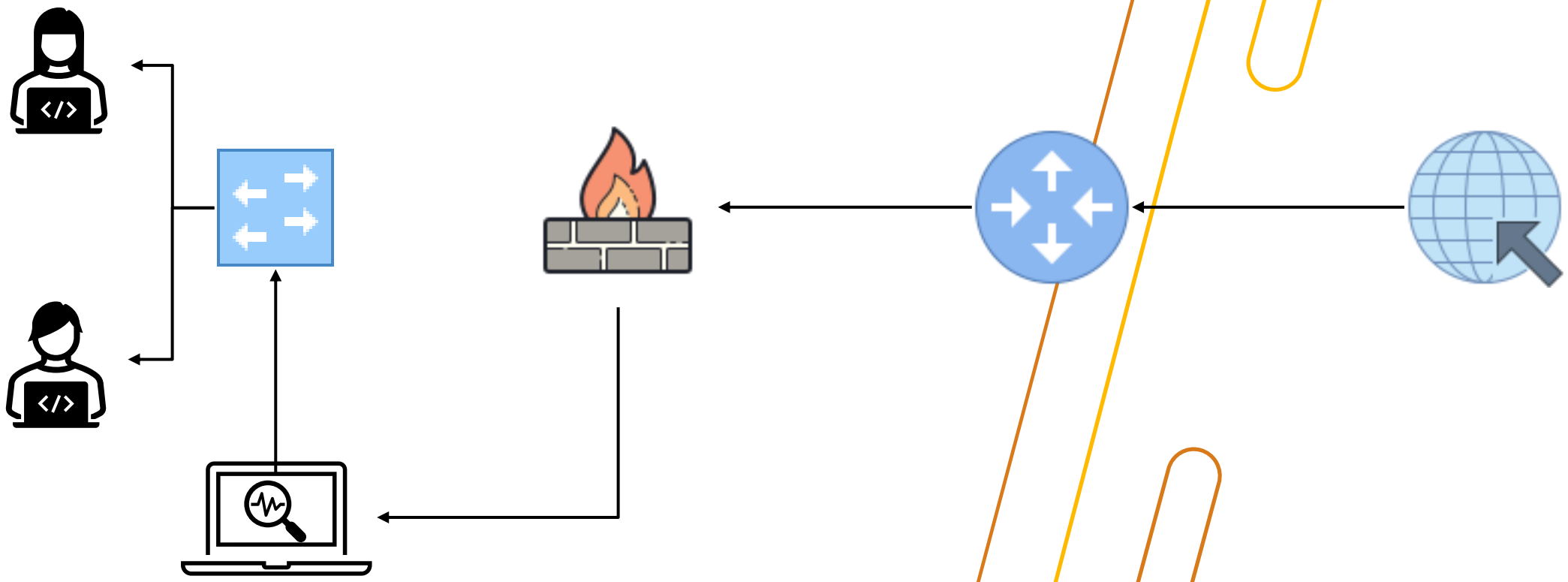
IDS



Icons Source:Internet Icons, Logos, Symbols – Free Download PNG, SVG (icons8.com)

SURICTA Modes

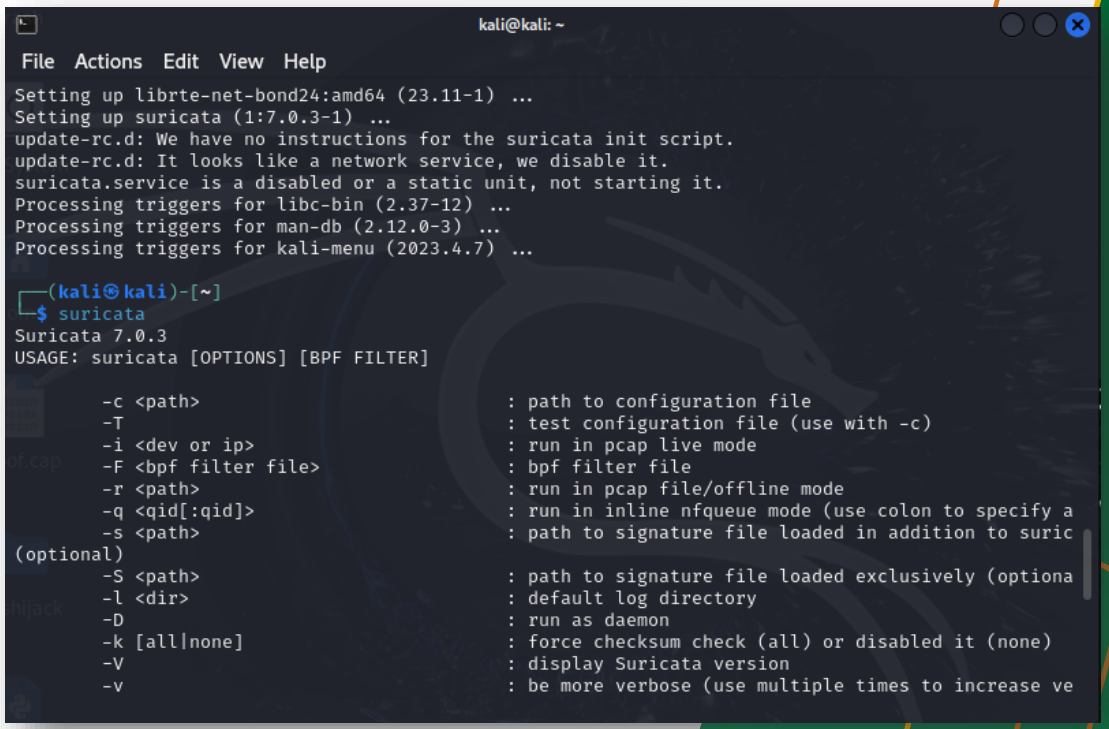
IPS



Icons Source:Internet Icons, Logos, Symbols – Free Download PNG, SVG (icons8.com)

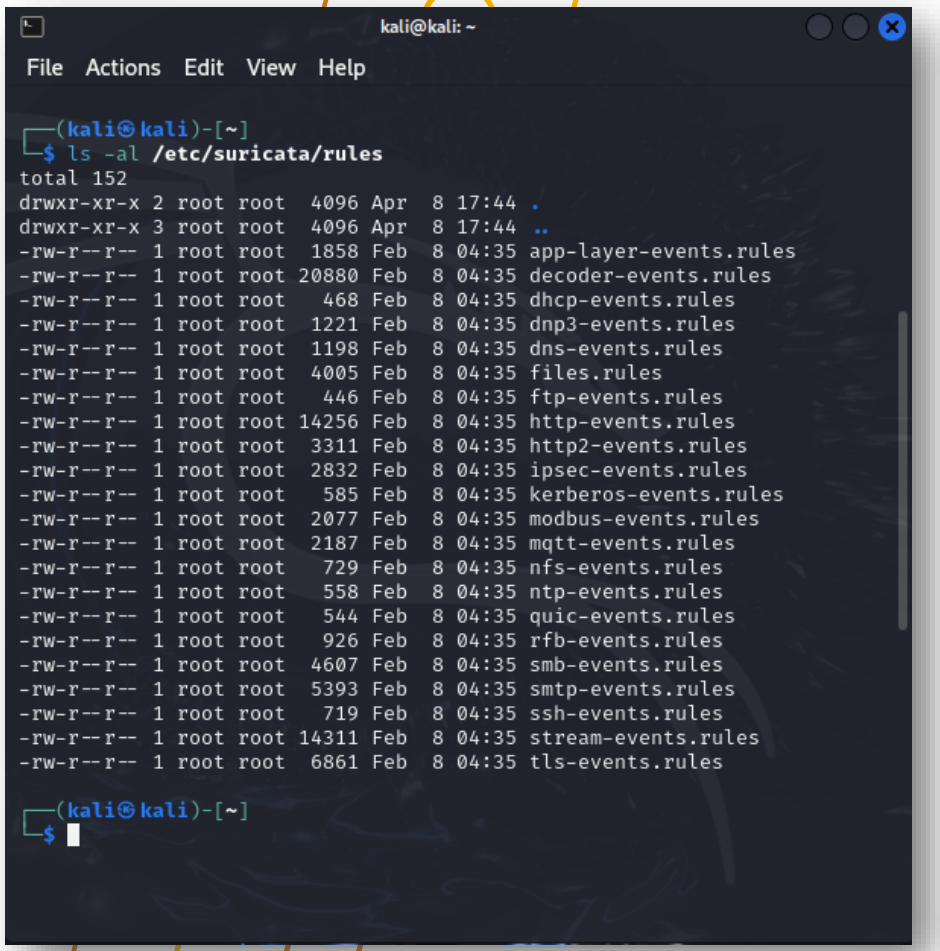
SURICATA Installation

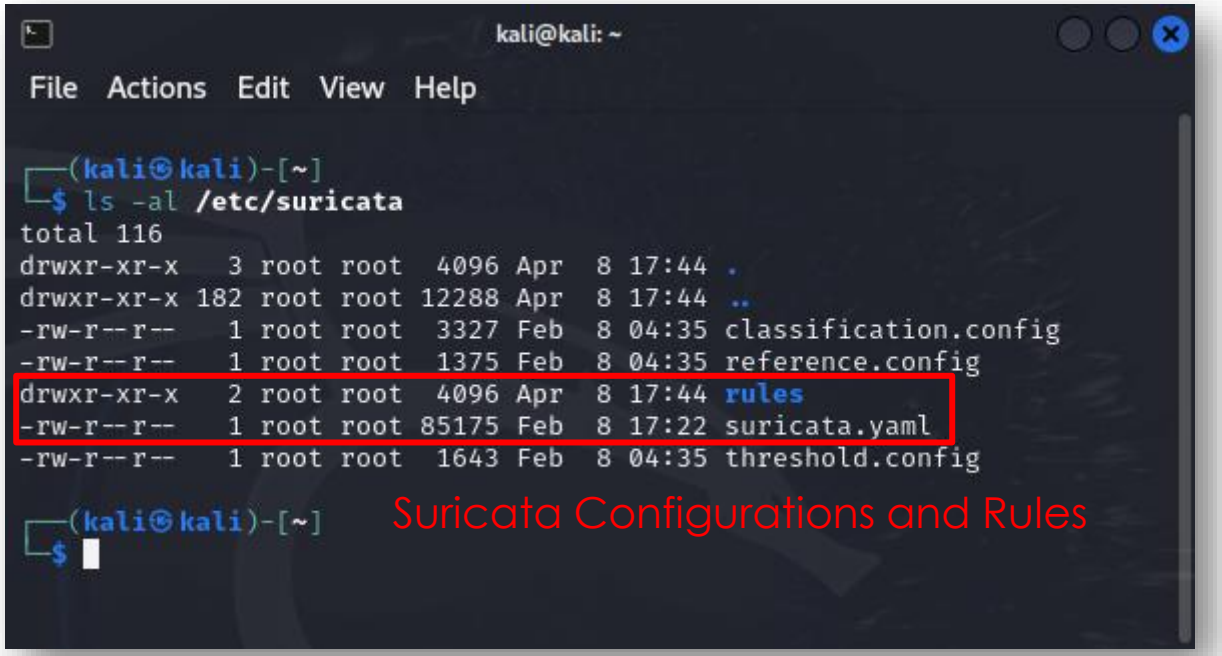
- **Sudo apt-get update**
- **Sudo apt–get install suricata**



Suricata Rules and Configurations

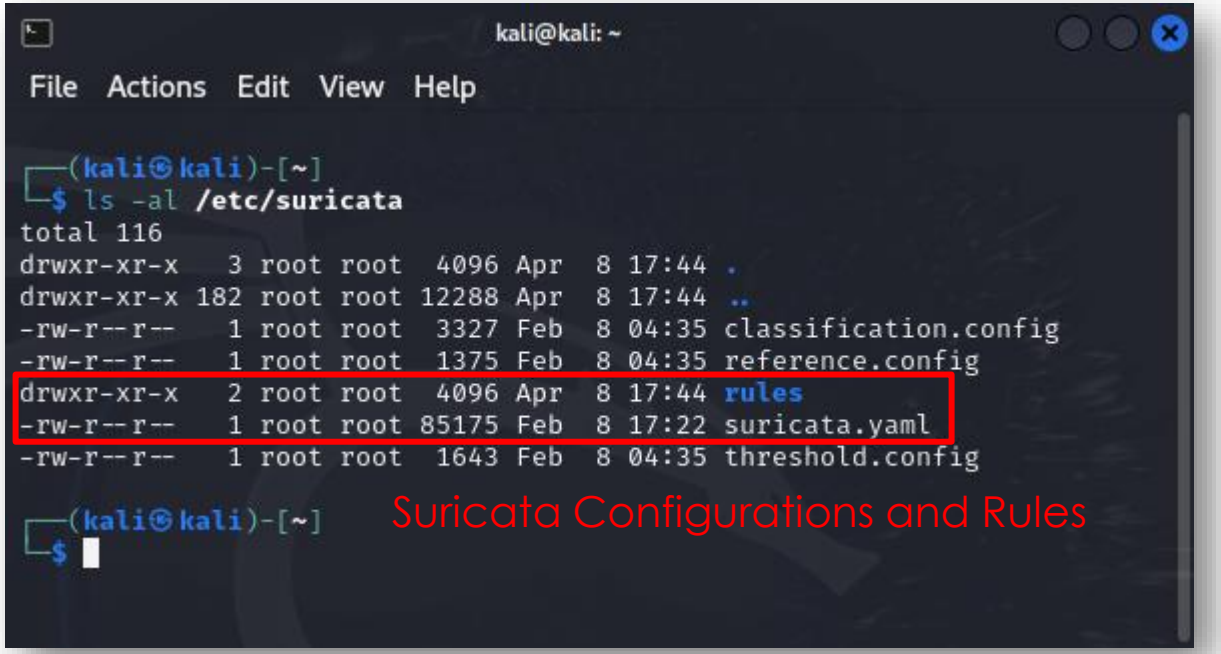
Suricata list of Rules





Suricata Rules and Configurations

Some **configurations** in the `**suricata.yaml**` file need to be **updated**.



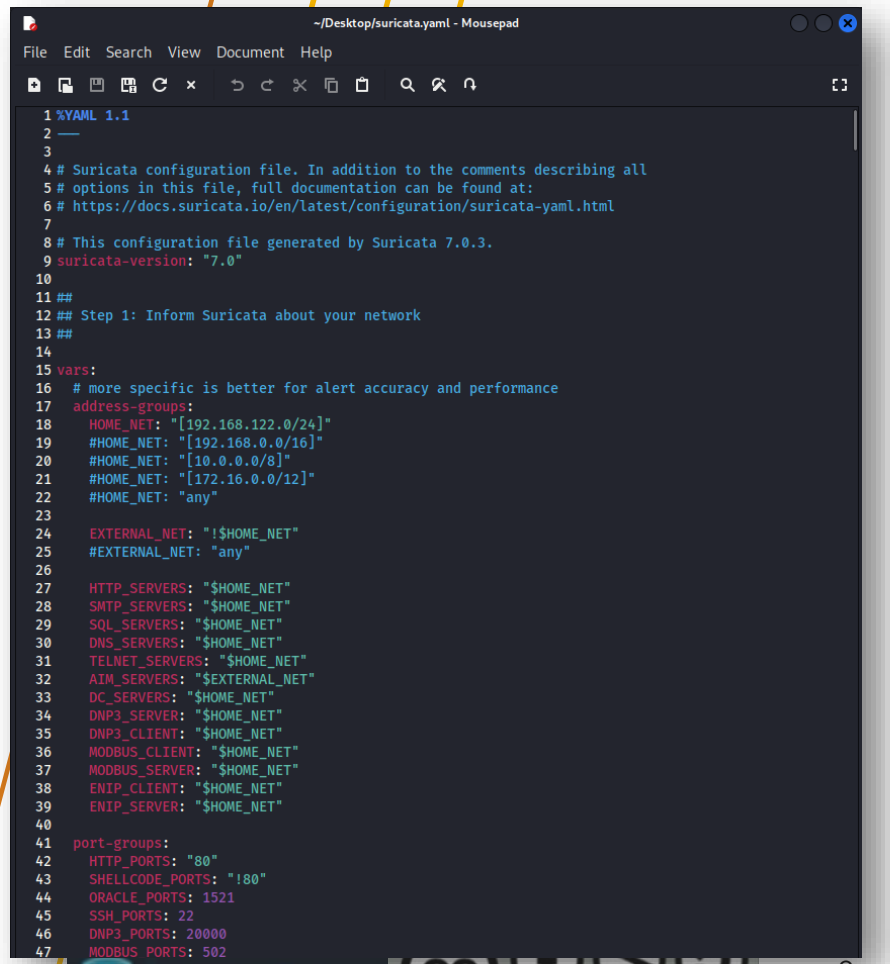
You can also copy the **suricata.yaml** file, paste a version on the **desktop**, make your changes, and then save it to the original path.

Sudo cp Source_file Destination_directory

You could directly open the **.yaml** configuration file, make any **updates** you want, and then **store** the **file again**.

Update the configuration file

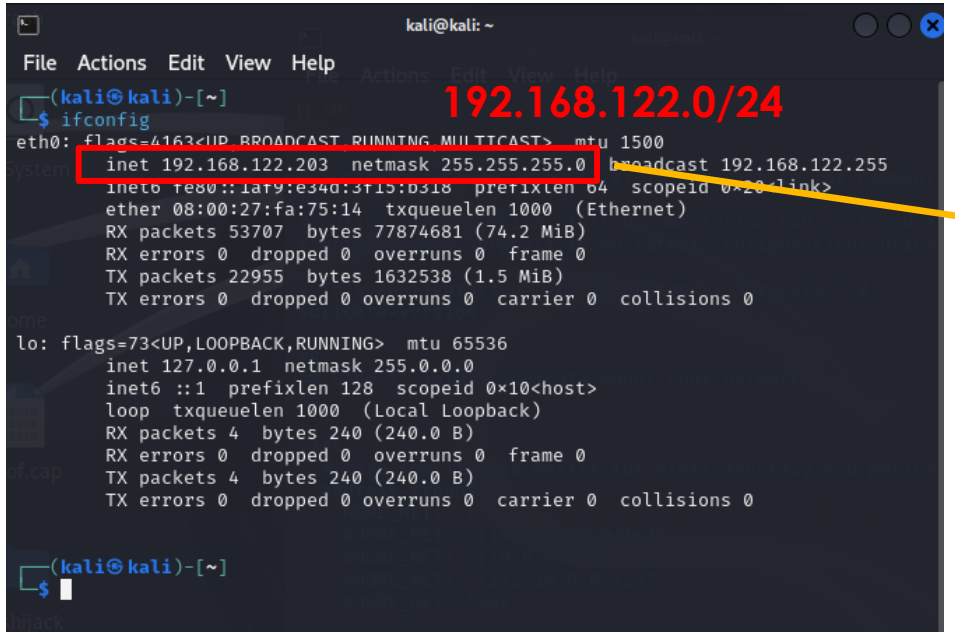
Sudo vim /etc/suricata/suricata.yaml



Suricata Rules and Configurations

We need to configure the **HOME_NET** that we want to **monitor** and **ensure** the correct **interface** name is defined.

So we need to know the **subnet**



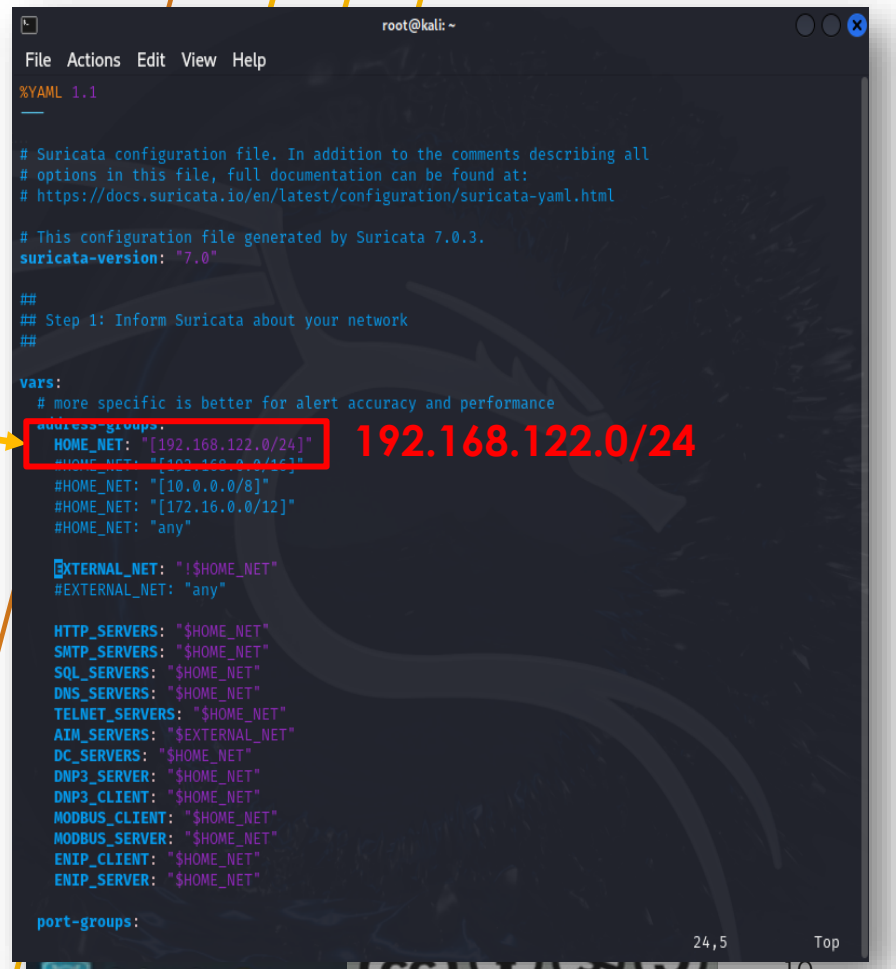
You can also copy the **suricata.yaml** file, paste a version on the **desktop**, make your changes, and then save it to the original path.

Sudo cp Source_file Destination_directory

You could directly open the **.yaml** configuration file, make any **updates** you want, and then **store** the **file again**.

Update the configuration file

Sudo vim /etc/suricata/suricata.yaml

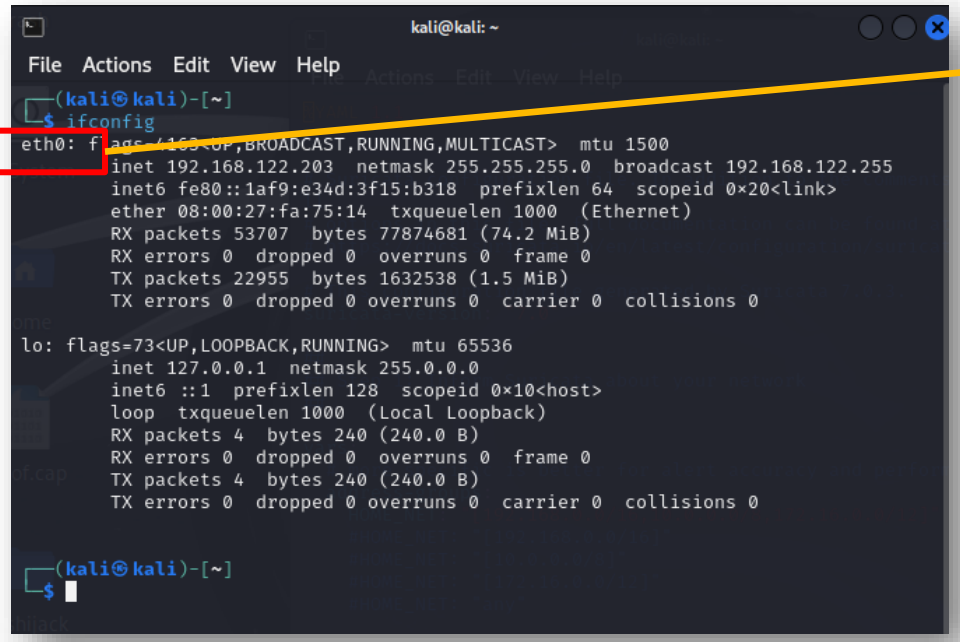


Suricata Rules and Configurations

We need to configure the **HOME_NET** that we want to **monitor** and **ensure** the correct **interface** name is defined.

So we need to know the **interface**

Interface name



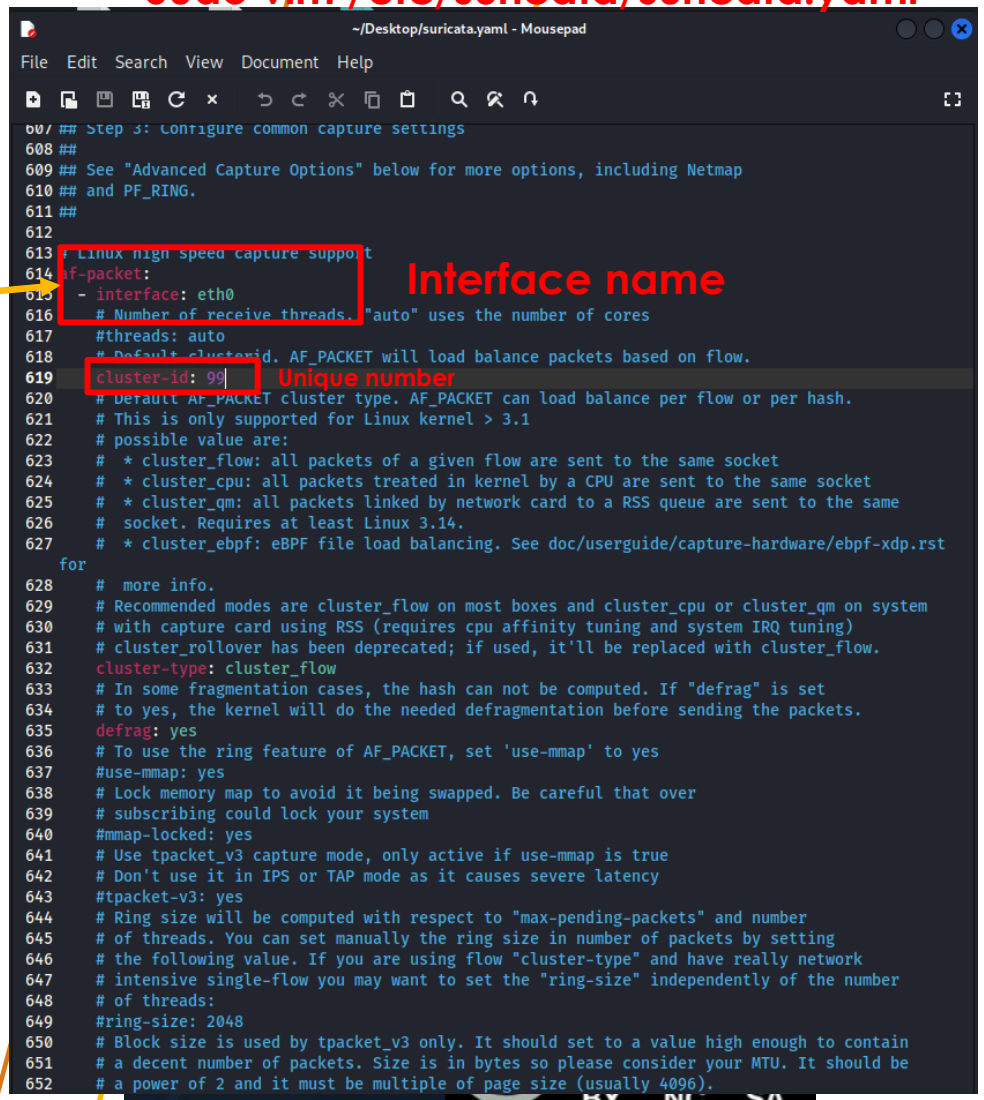
You can also copy the **suricata.yaml** file, paste a version on the **desktop**, make your changes, and then save it to the original path.

Sudo cp Source_file Destination_directory

You could directly open the **.yaml** configuration file, make any **updates** you want, and then **store** the **file again**.

Update the configuration file

Sudo vim /etc/suricata/suricata.yaml

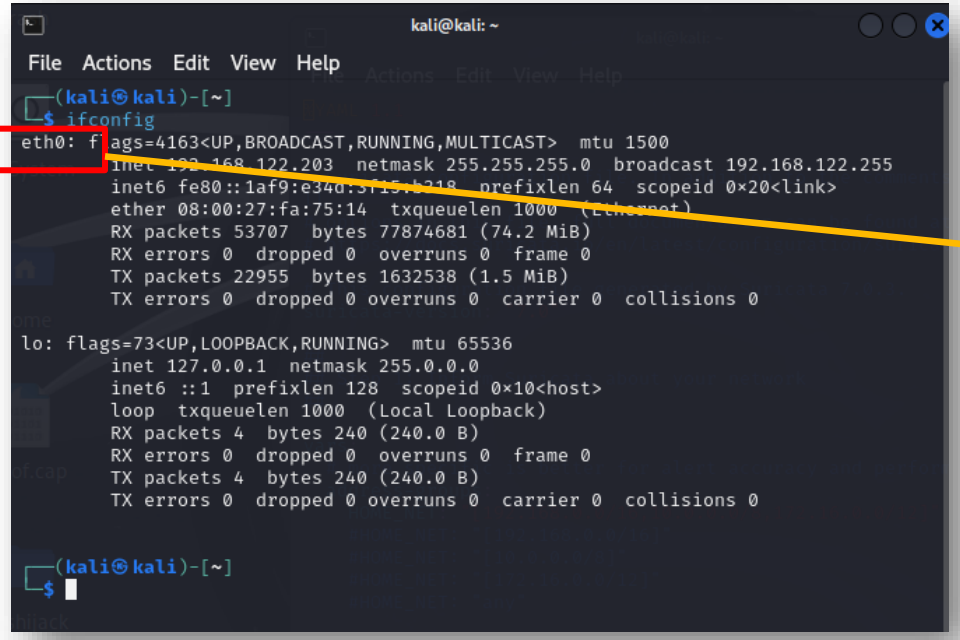


Suricata Rules and Configurations

We need to configure the **HOME_NET** that we want to **monitor** and **ensure** the correct **interface** name is defined.

So we need to know the **interface**

Interface name



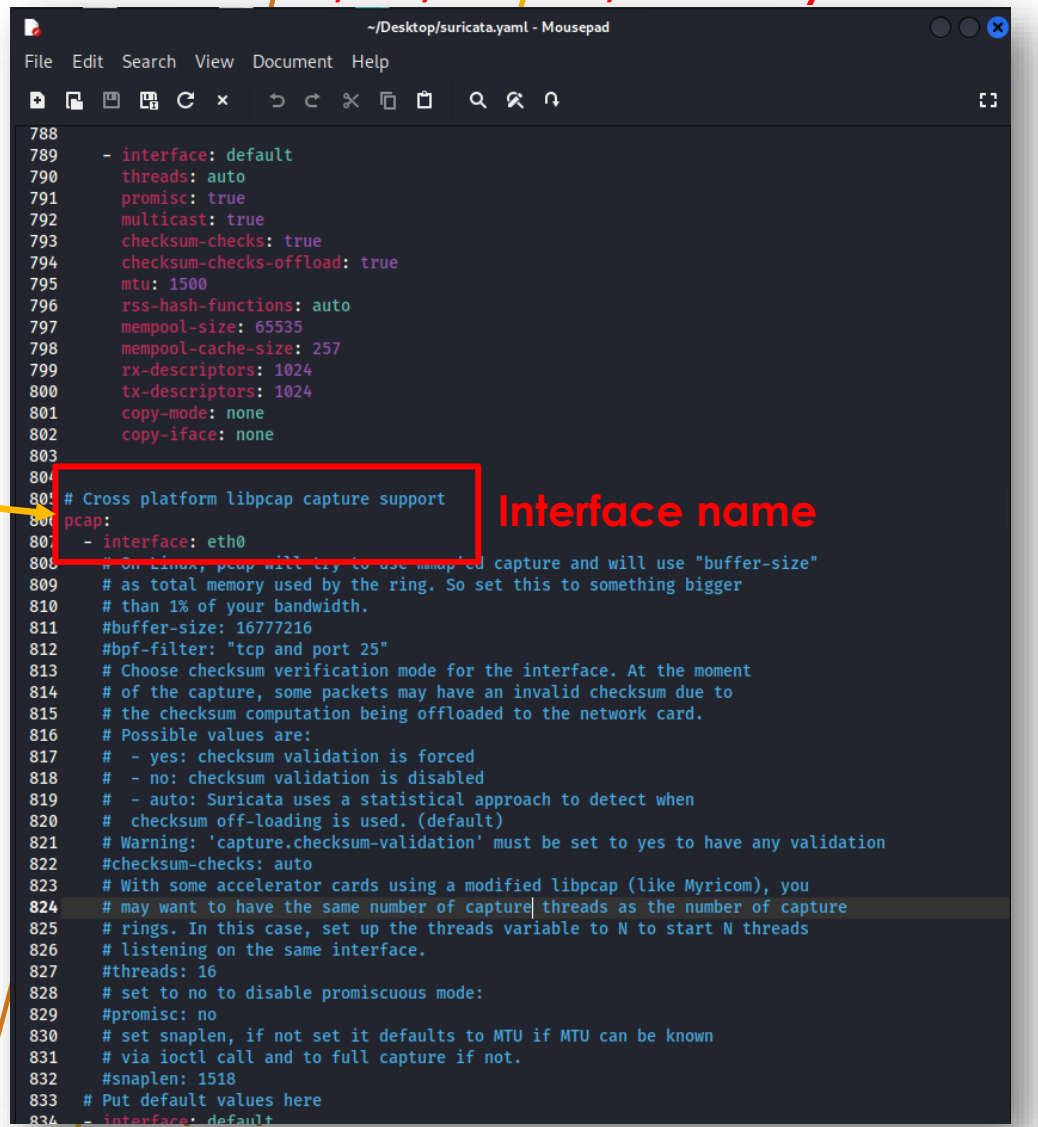
You can also copy the **suricata.yaml** file, paste a version on the **desktop**, make your changes, and then save it to the original path.

Sudo cp Source_file Destination_directory

You could directly open the **.yaml** configuration file, make any **updates** you want, and then **store** the **file again**.

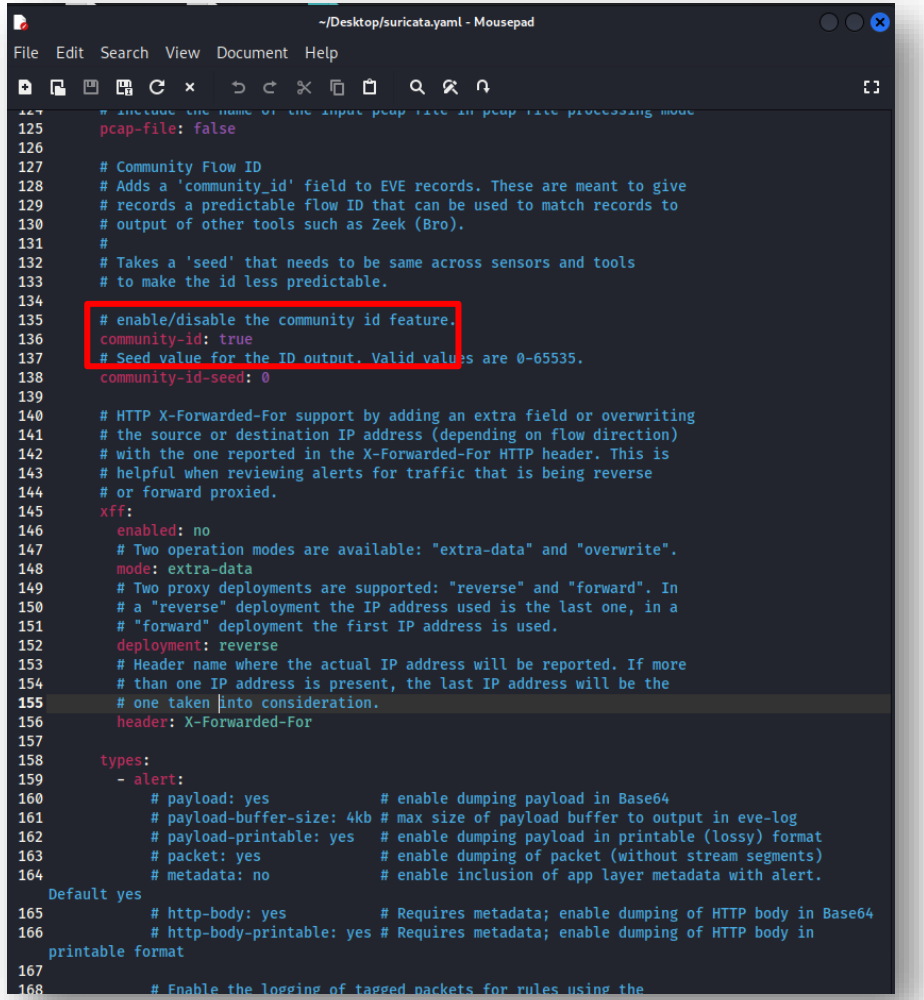
Update the configuration file

Sudo vim /etc/suricata/suricata.yaml



Interface name

Suricata Rules and Configurations



You could directly open the **.yaml** configuration file, make any **updates** you want, and then **store** the **file again**.

If you are using VIM:

To **Exit VIM**, press **Esc** with **q:**

Type q for quite
Type q! for quiet without saving
Type wq to write and quite

If you copied the suricata.yaml file, then use the cp command

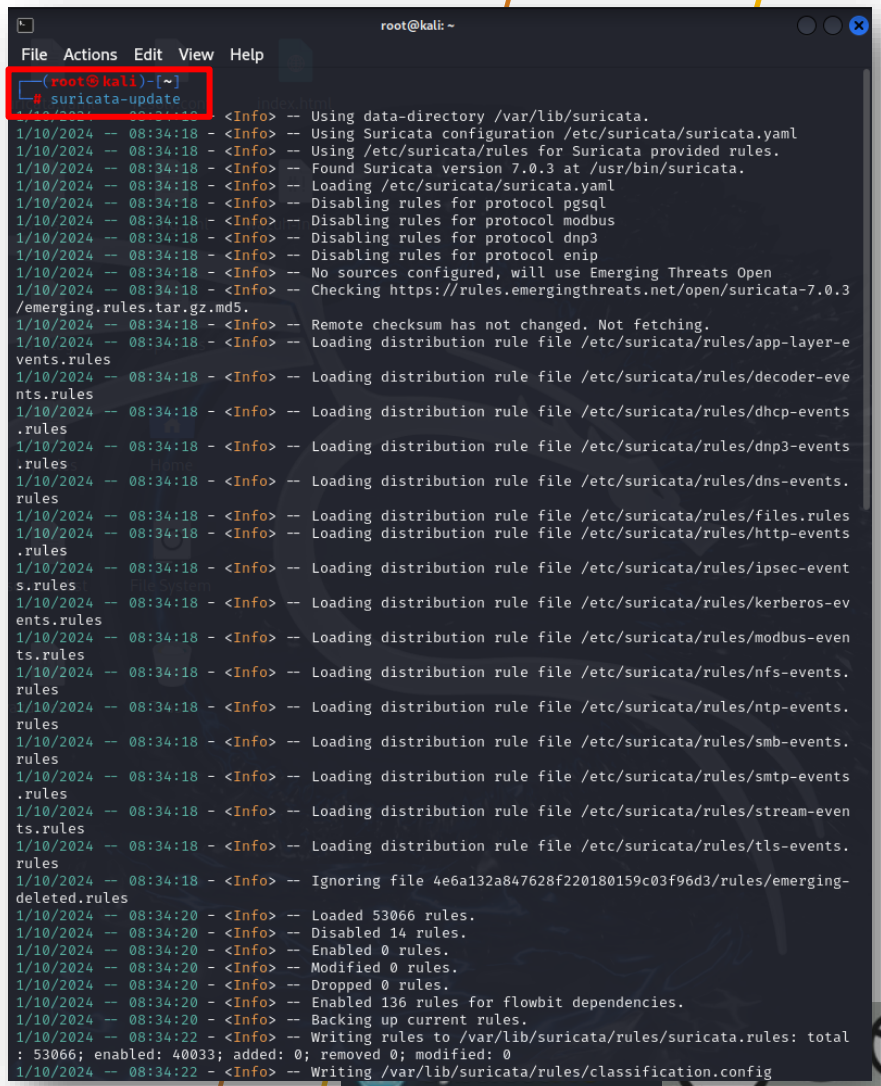
Sudo cp Source_file Destination_directory

Destination Directory: /etc/suricata/suricata.yaml

Suricata Rules and Configurations

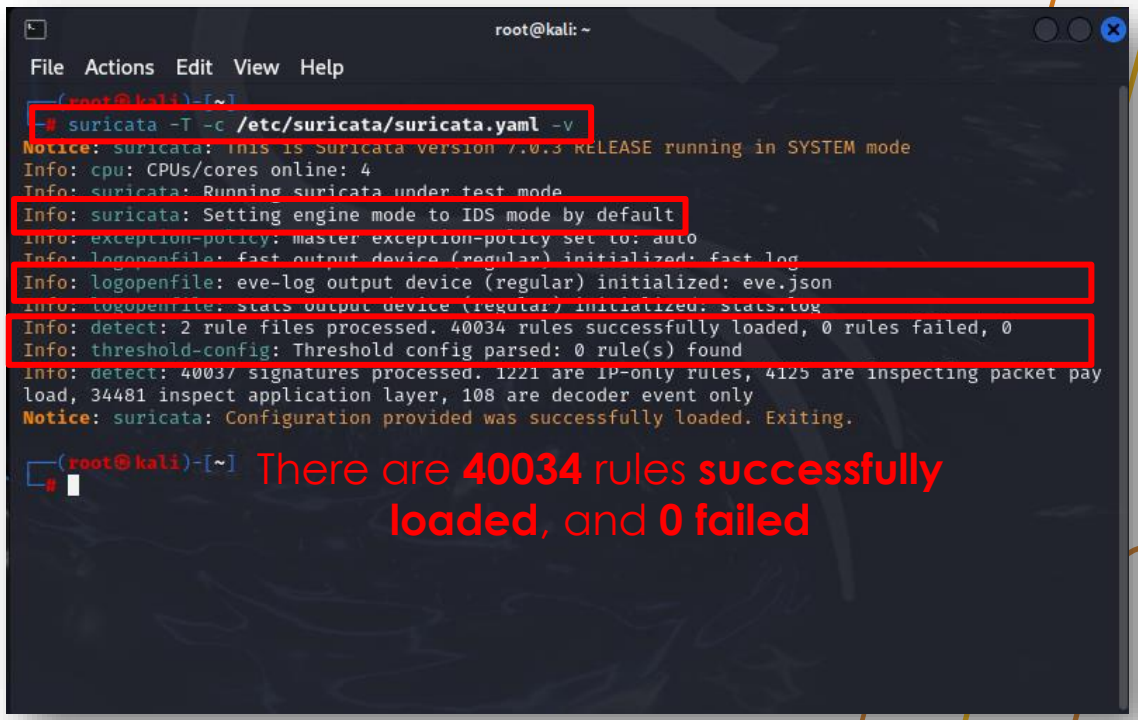
Update suricata using: **sudo suricata-update**

No errors detected ☺



Suricata Rules and Configurations

To **test** the **configuration** file of **Suricata**; **sudo suricata –T –c /etc/suricata/suricata.yaml –v**

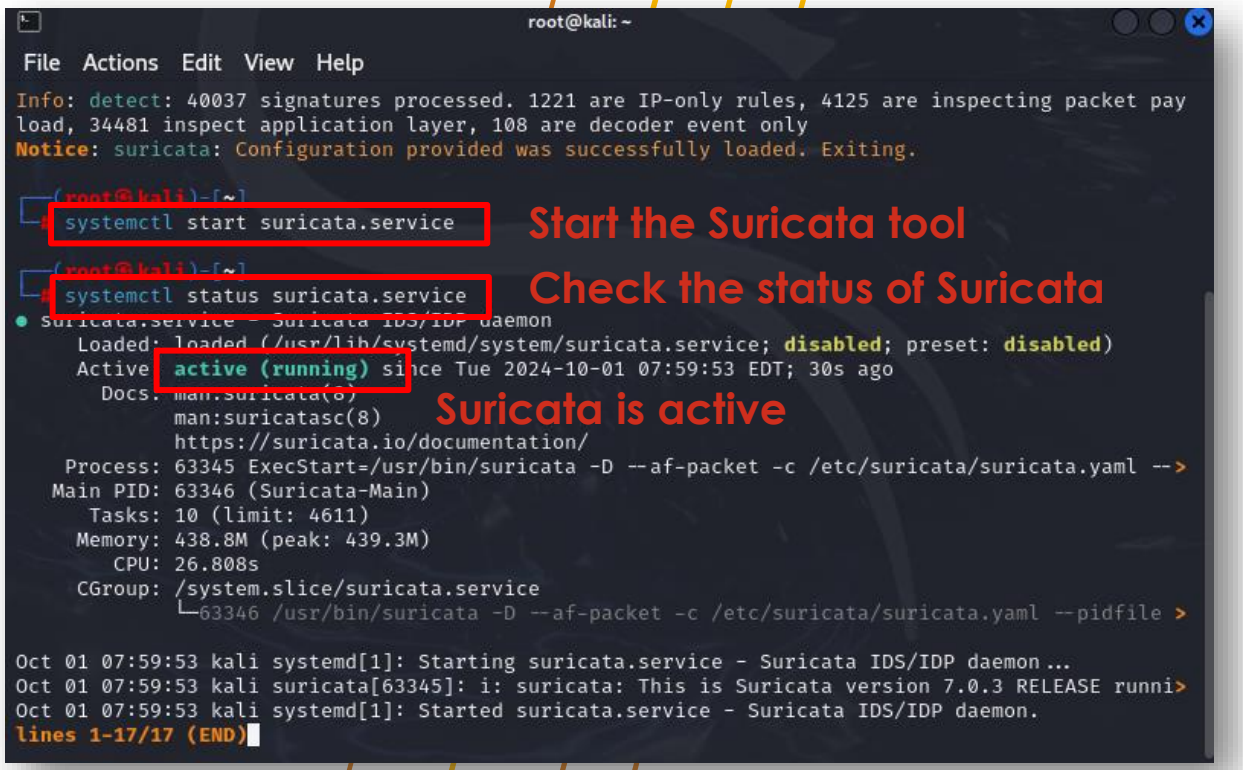


Running on the **IDS** mode

All intrusion activities are in the **.log** file; the **.json** contains the same **collected/detected** intrusions but in **JSON** format.

Running Suricata

- Run as a **daemon**
  - **sudo systemctl start suricata.service**
- Check the **status** of the **Suricata** tool
  - **sudo systemctl status suricata.service**

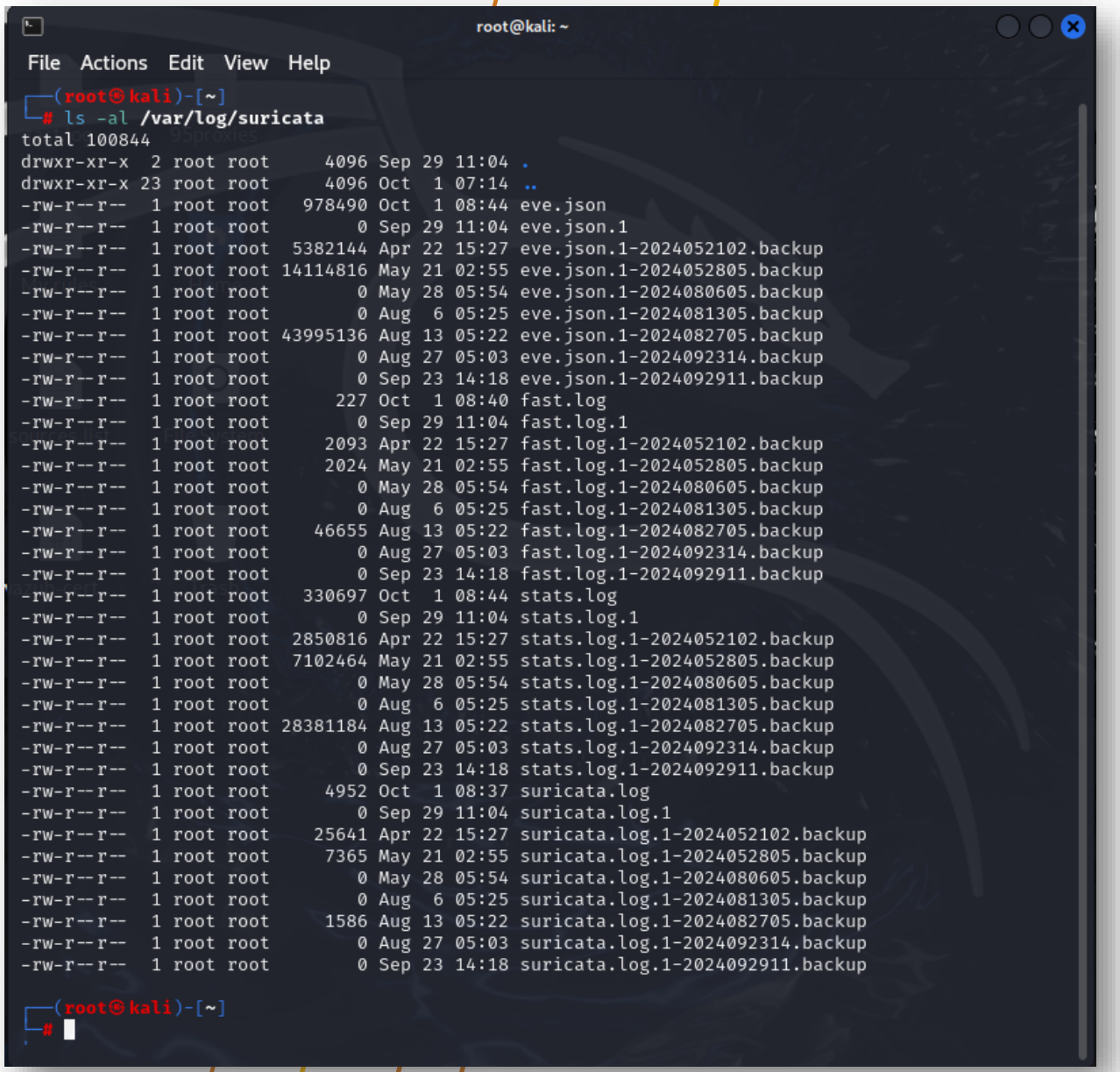


Now it means that the **tool** is **running** on the background

Suricata log Files

Check all **log** files **generated** by **Suricata** for network **traffic analysis**.

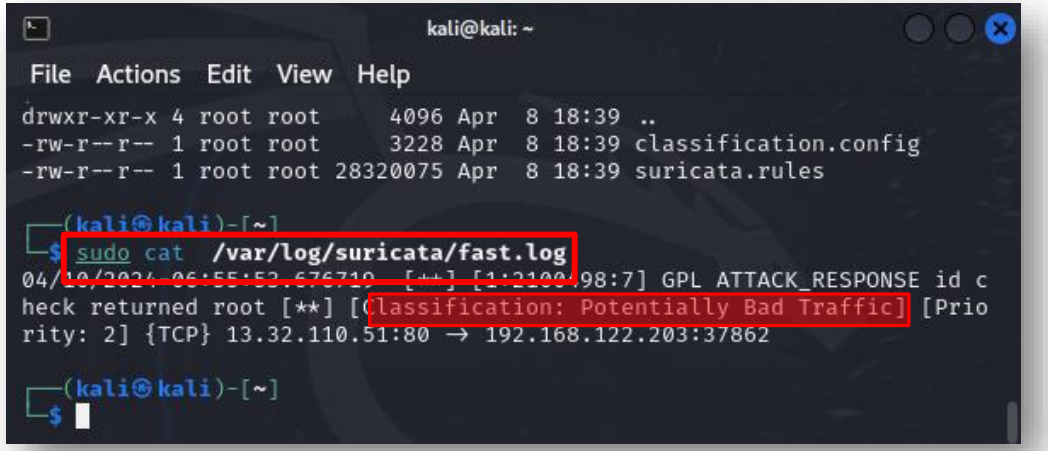
ls –al /var/log/suricata

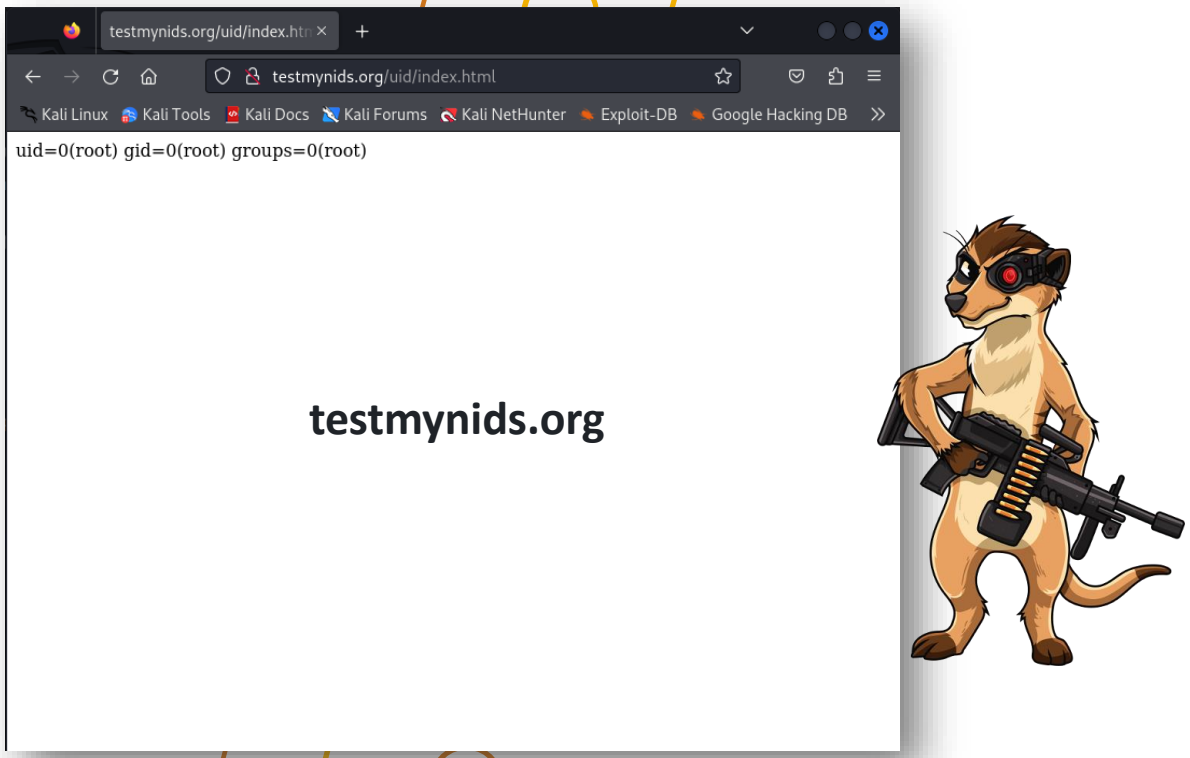


Intrusion Detection using Suricata

- **Test Suricata**
  - **Visit**: http://testmynids.org/uid/index.html

- **Check the log**:
  - **sudo cat /var/log/suricata/fast.log**





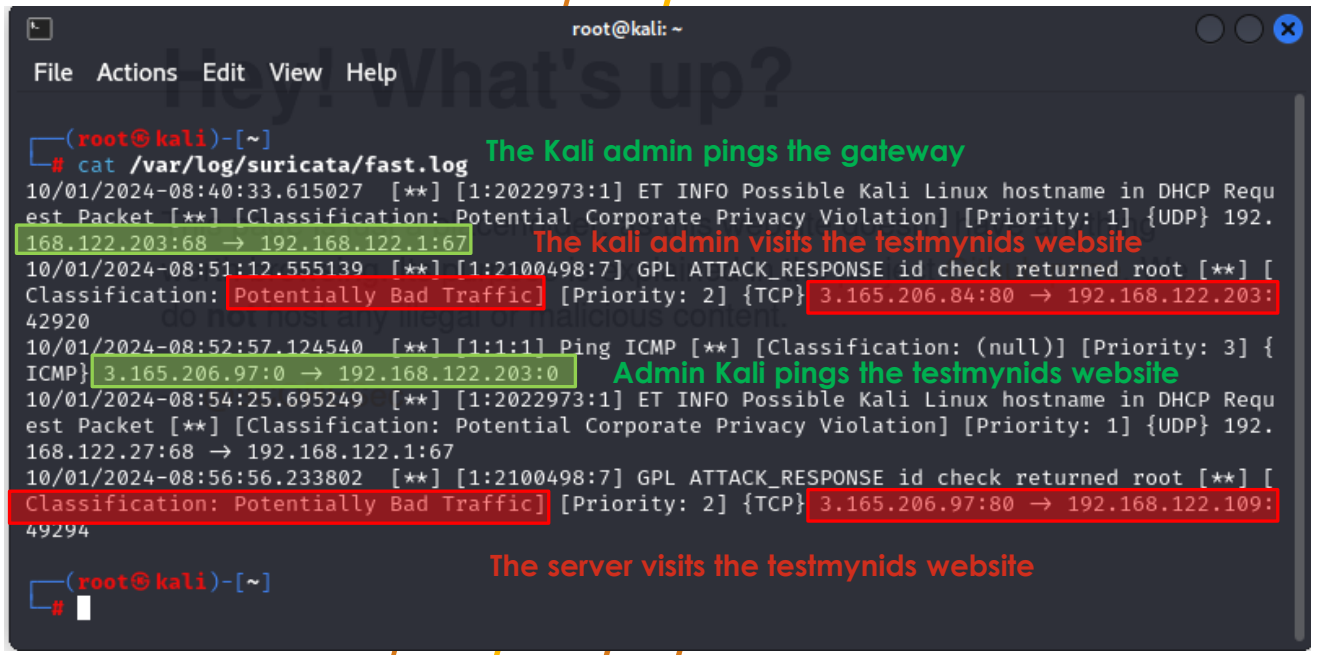
GitHub - 3CORESec/testmynids.org: A website and framework for testing NIDS detection

Intrusion Detection using Suricata

- Execute the **ping command** from the **Kali admin device** to any **device/server**, such as **Google**.
- Visit **the testmynids.org/uid/index.html** on the **server device** (IP end with **.109**) in your network.

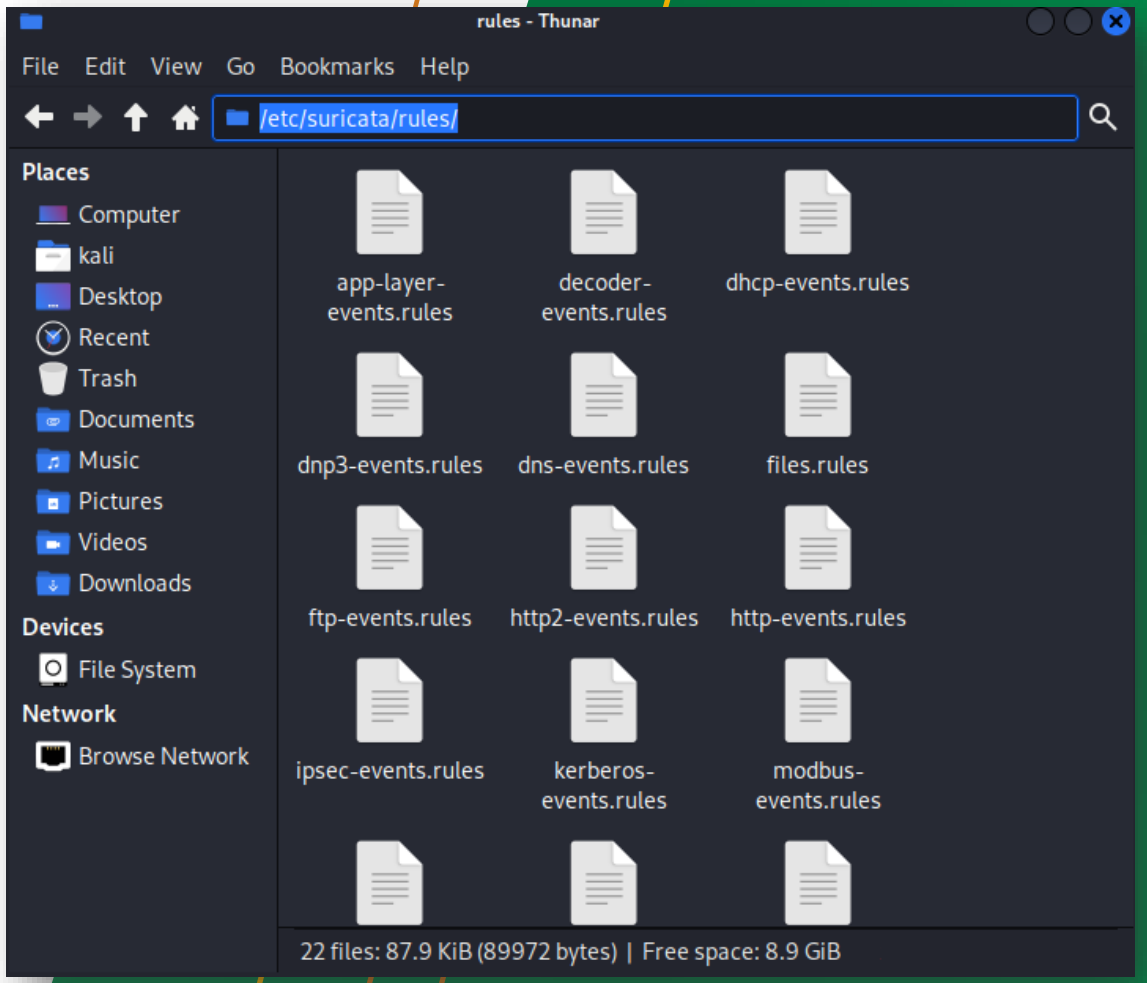
All **traffic** communication in **Suricata** will be **collected** and **stored** in the **fast.log**.

- **Check the log**:
  - **sudo cat /var/log/suricata/fast.log**



Customize Rules for Suricata

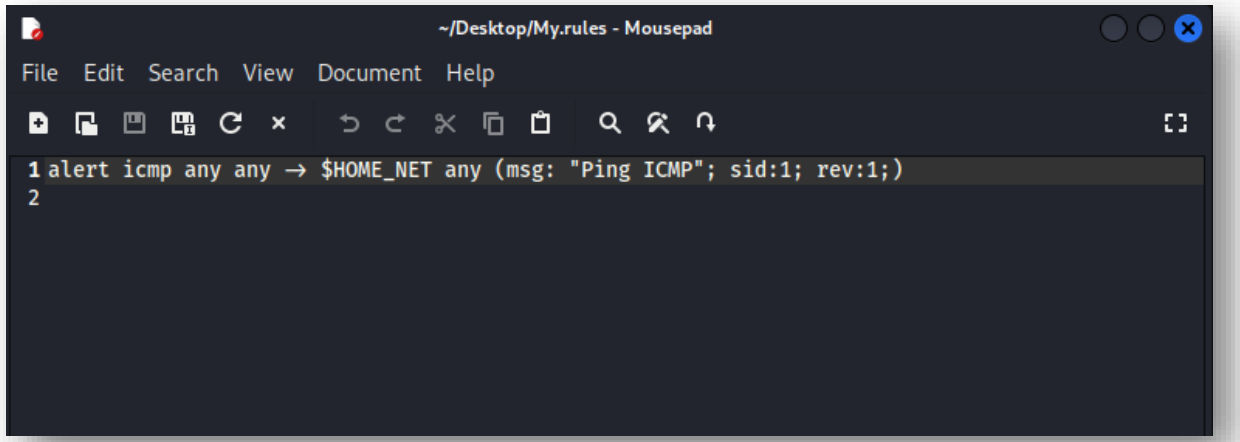
All rules are store on: /etc/suricata/rules



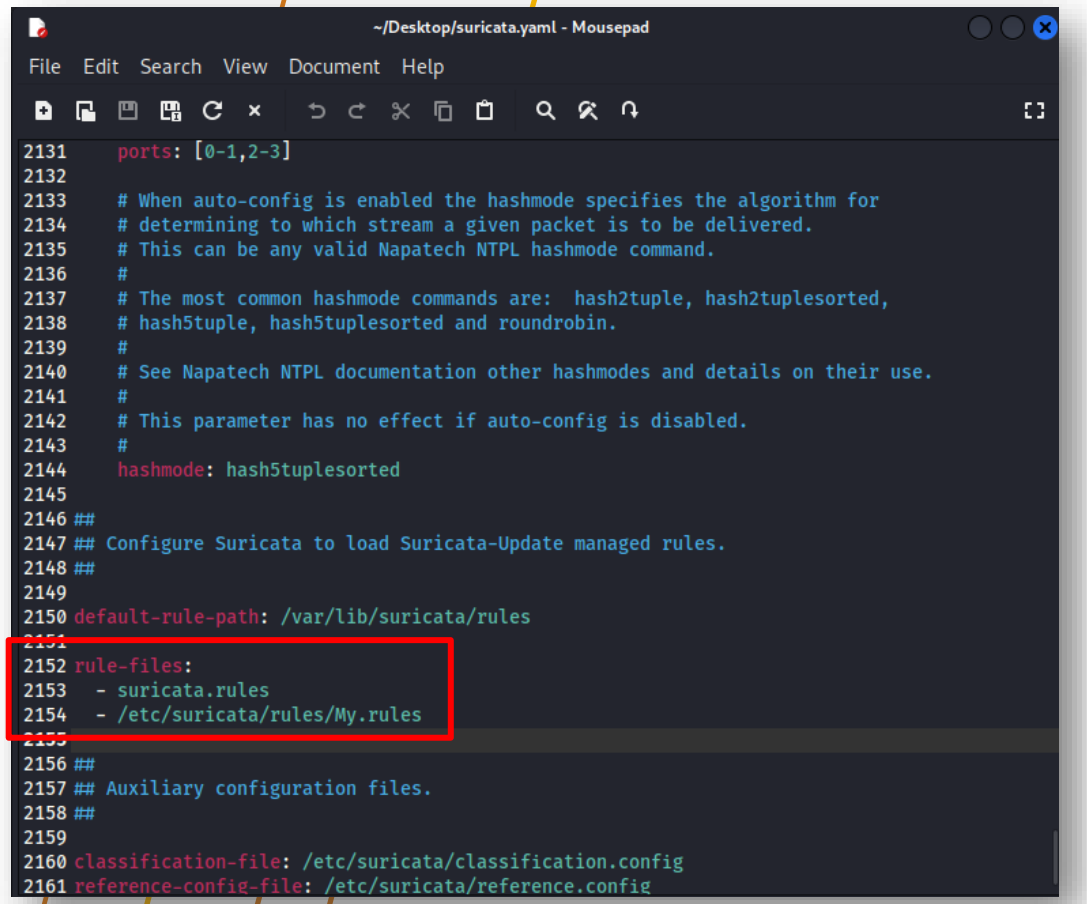
Customize Rules for Suricata

Create a file "**My.rules**" and **store** the file on **/etc/suricata/**

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



Update the **.yaml configuration** file



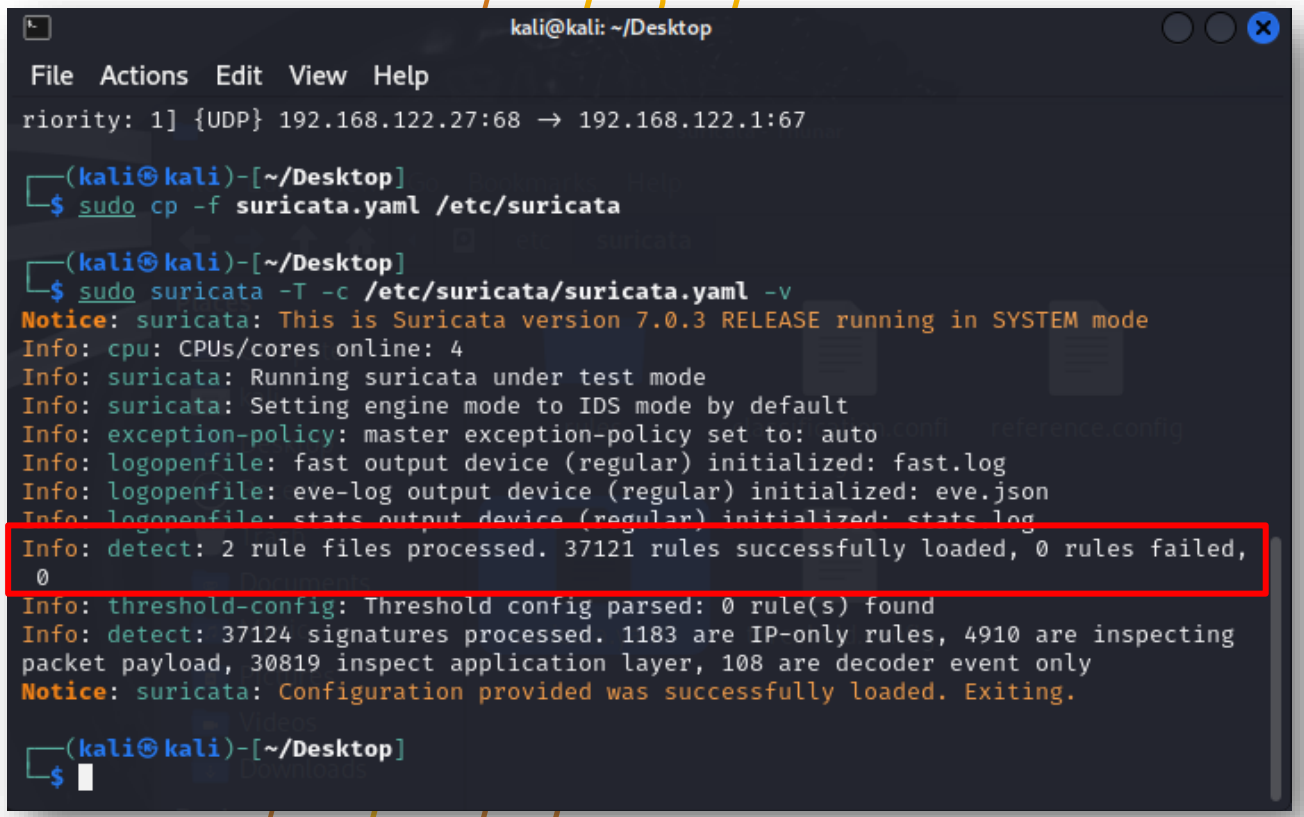
Customize Rules for Suricata

Suricata –T –c /etc/suricata/suricata.yaml -v

It seems that everything running well ☺

- **Run Suricata**
  - **Sudo systemctl start suricata.service**

Check the configuration file

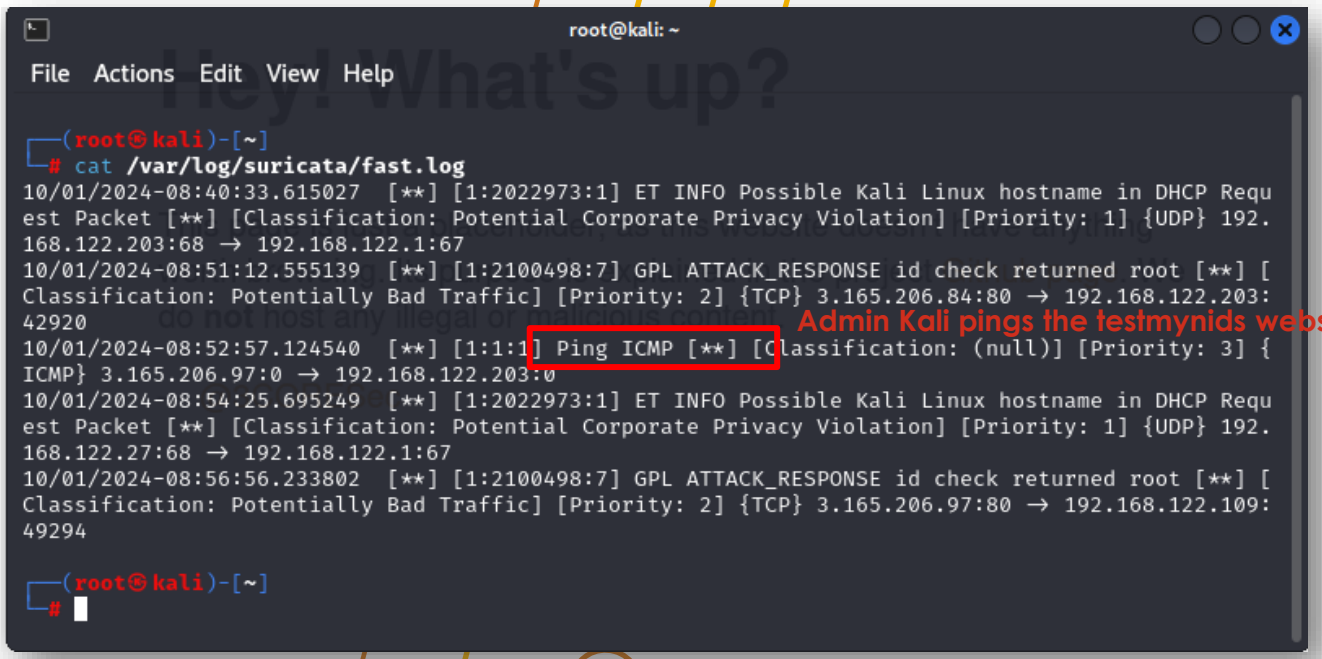


Run Customize Rules

- **Ping**
  - **Ping command from the admin Kai device to testmynids website**

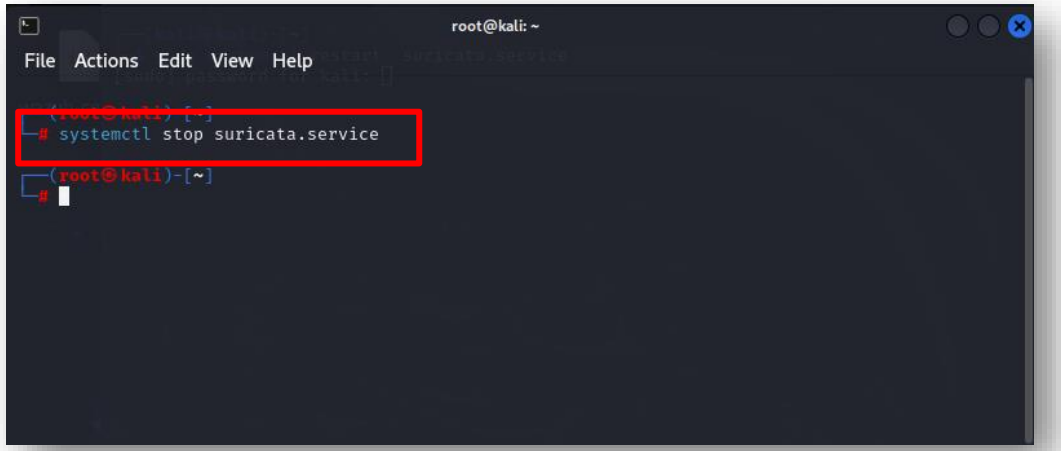
The **results** may not **appear immediately**. Please wait for a while until the **newly added rule** detects the ping **activities** across your **network**.

- **Check the log**:
  - **sudo cat /var/log/suricata/fast.log**

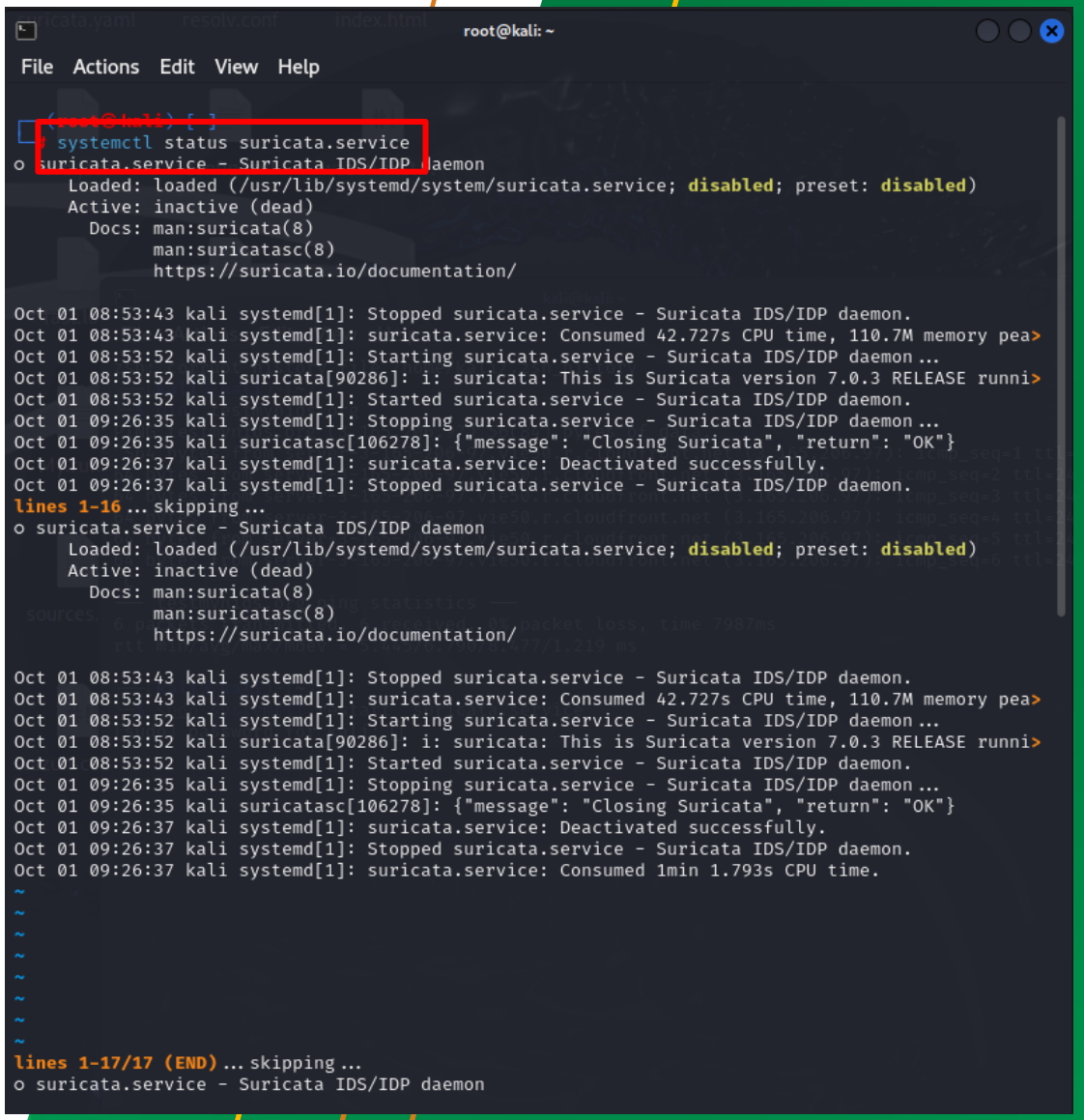


Stop Suricata

- **Stop Suricata**
  - **Sudo systemctl stop suricata.service**



- **Status Suricata**
  - **Sudo systemctl status suricata.service**



Thank you

Please send all questions to:
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at
Stefan Schauer
Stefan.Schauer@ait.ac.at