Network Protection for Energy Control Systems

CSP004_C_E

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

Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

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.

Detection of Cyberattacks

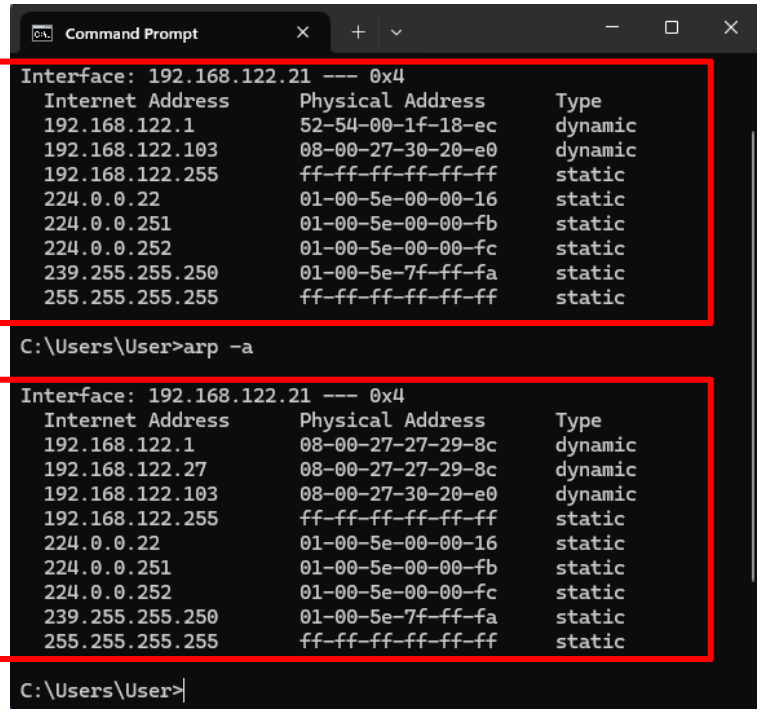
Detection of Cyberattacks

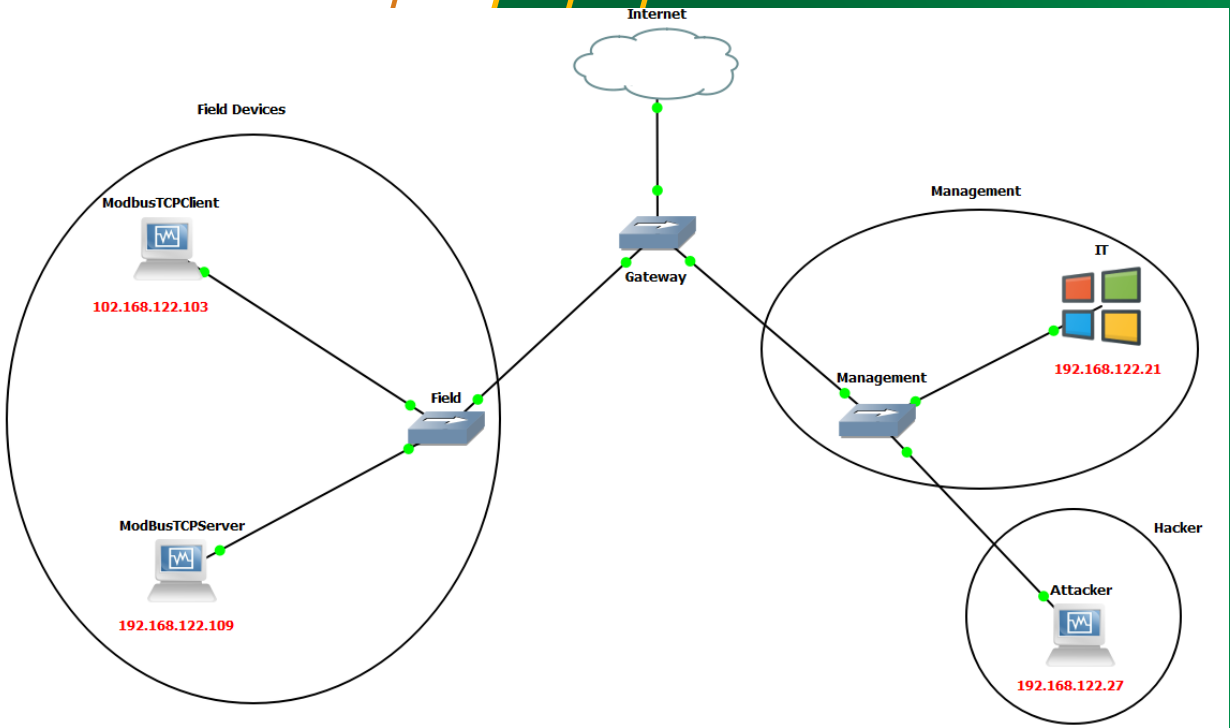
- Detecting ARP Poisoning Attacks on the network
- We consider the Windows machine to act as a network administration machine within the network. If any suspicious activities are occurring on the network, the network administrator should detect them. How?

On the windows machine
Arp –a

Before

After



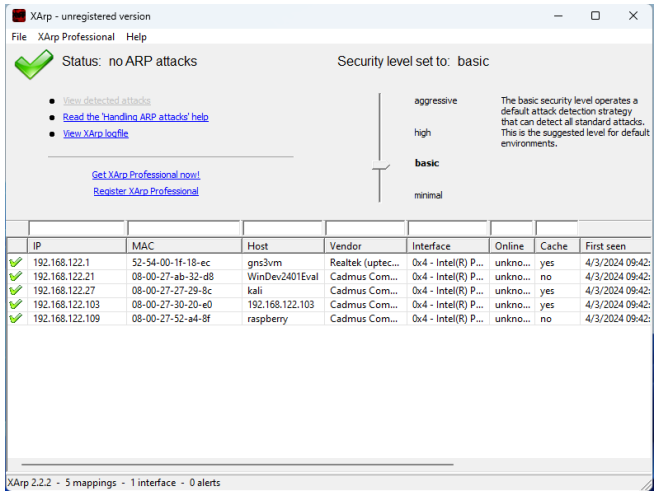


Detection of Cyberattacks

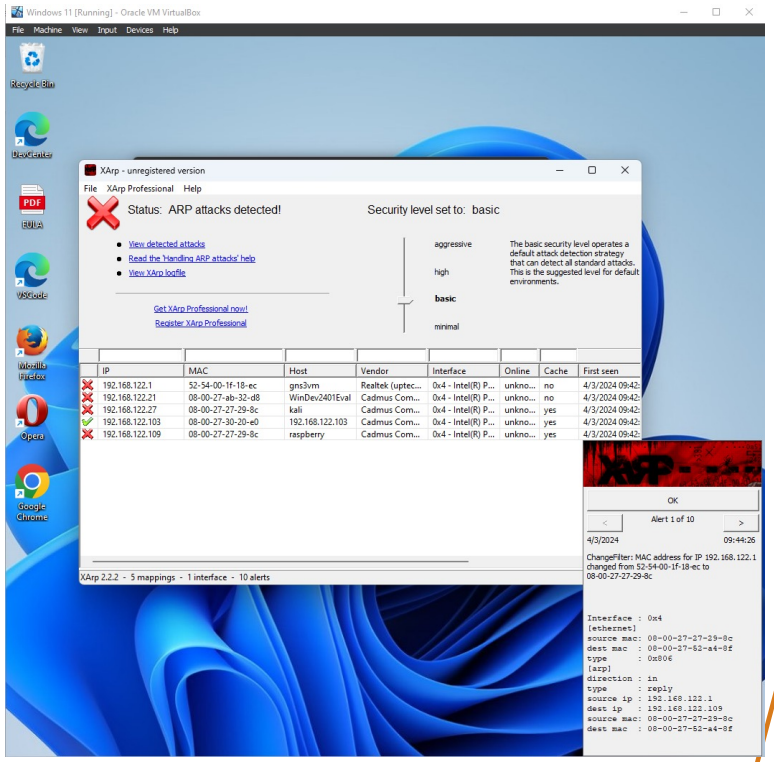
ARP Poisoning Attacks

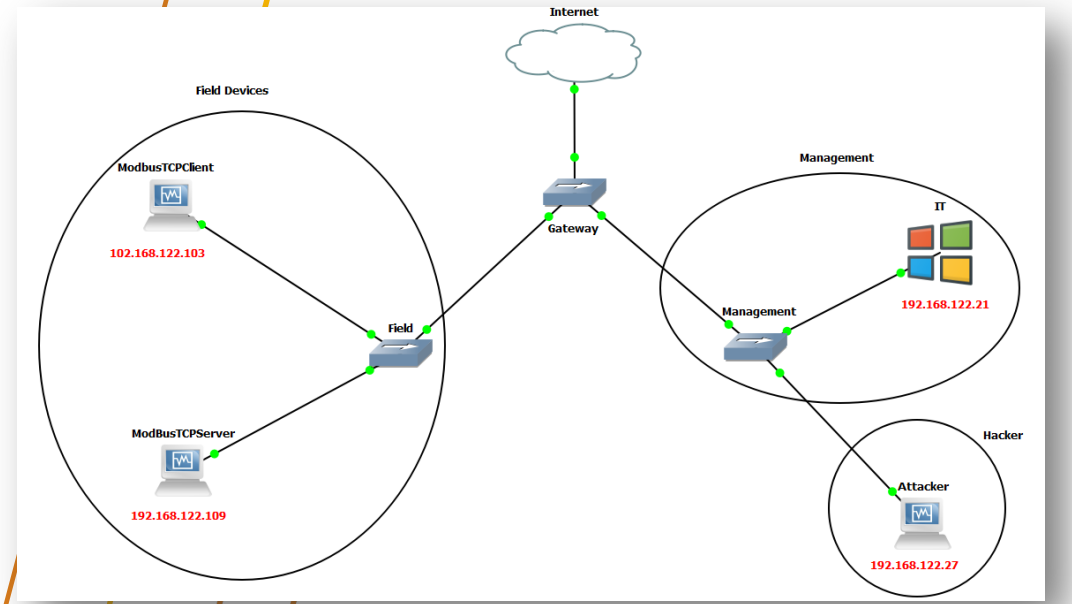
- The "arp -a" command should be executed manually every time to detect such suspicious activities.
- The xarp tool can automatically detect any such activities.

Before



After

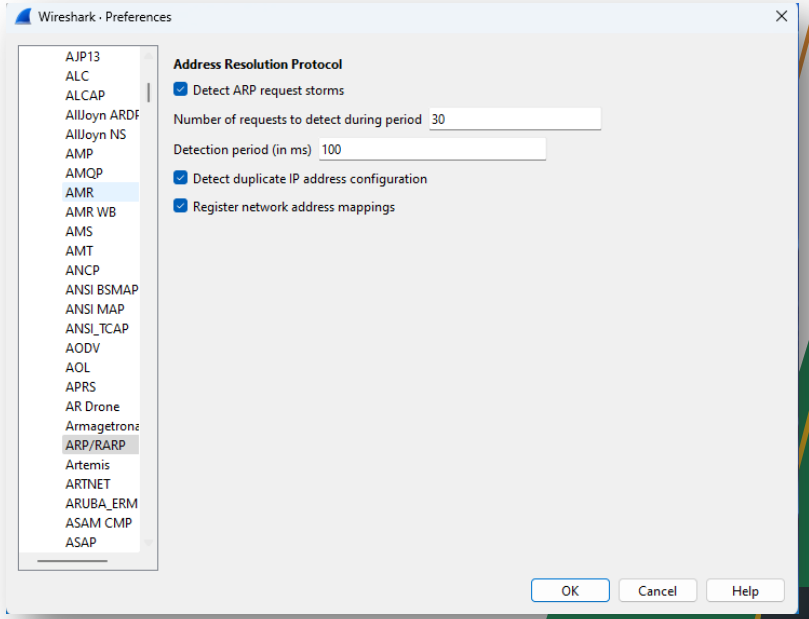




Detection of Cyberattacks

Detecting suspicious Activities In The Network using Wireshark

- Run wireshark on windows device, and let the tool detect an ARP request packets through the network.
- To do so, do the following:
  - Select preferences from Edit, then select Protocols→ ARP/RARP
  - Keep the “Detect ARP request storms” selected. Then press ok

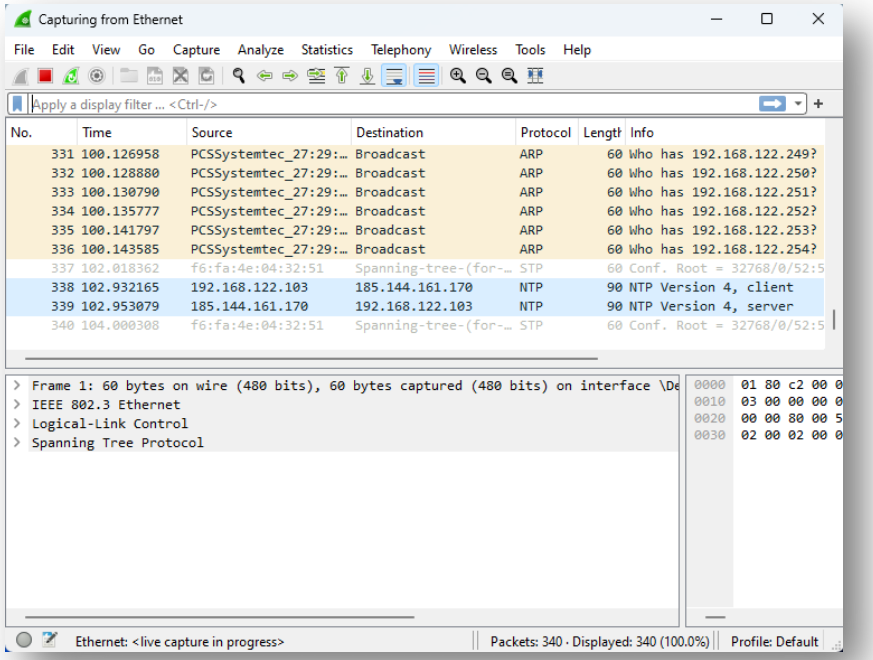


Detection of Cyberattacks

Detecting suspicious Activities In The Network using Wireshark

- Run the Wireshark tool using the proper connection.
- In order to test the ARP poising attack, we will start discovering the connected devices on the network using the netdiscover command on the kali linux

Netdiscover –i eth0 –r 192.168.122.1/24



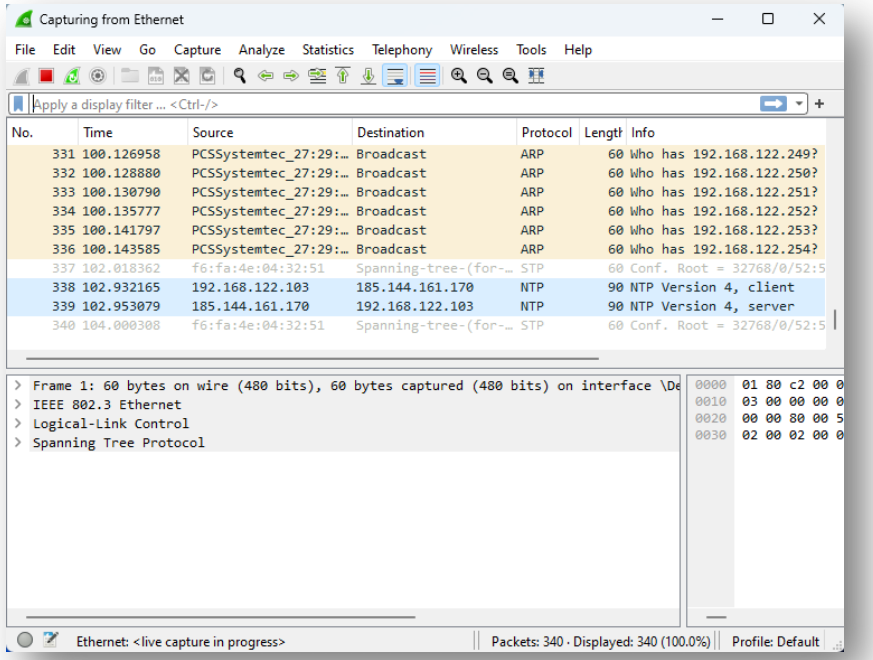
Wireshark start detecting ARP request over the network

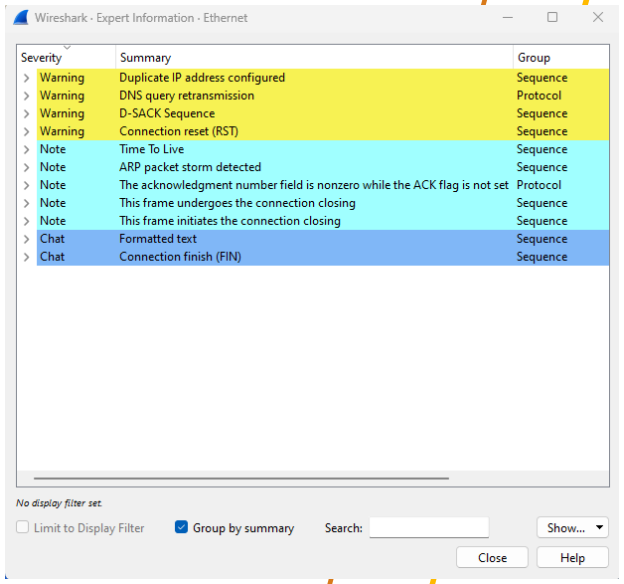
Detection of Cyberattacks

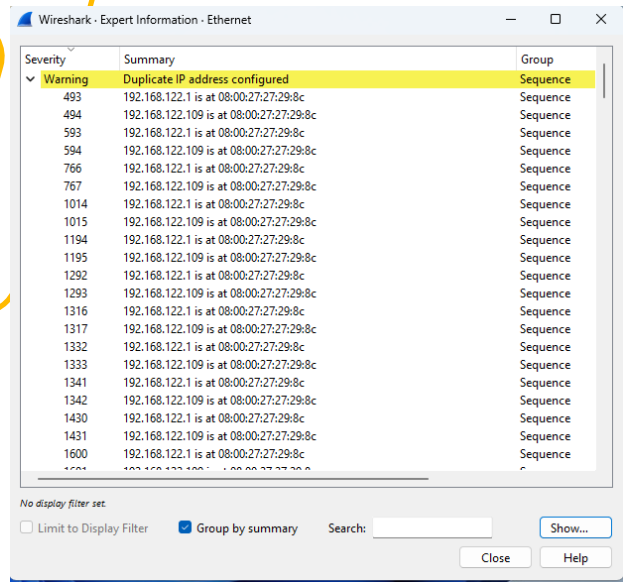
Detecting suspicious Activities In The Network using Wireshark

- Run the arb spoofing attack using any of the previously discussed too (bettercap or arpspoof)

Bettercap –iface eth0 –caplet spoof.cap



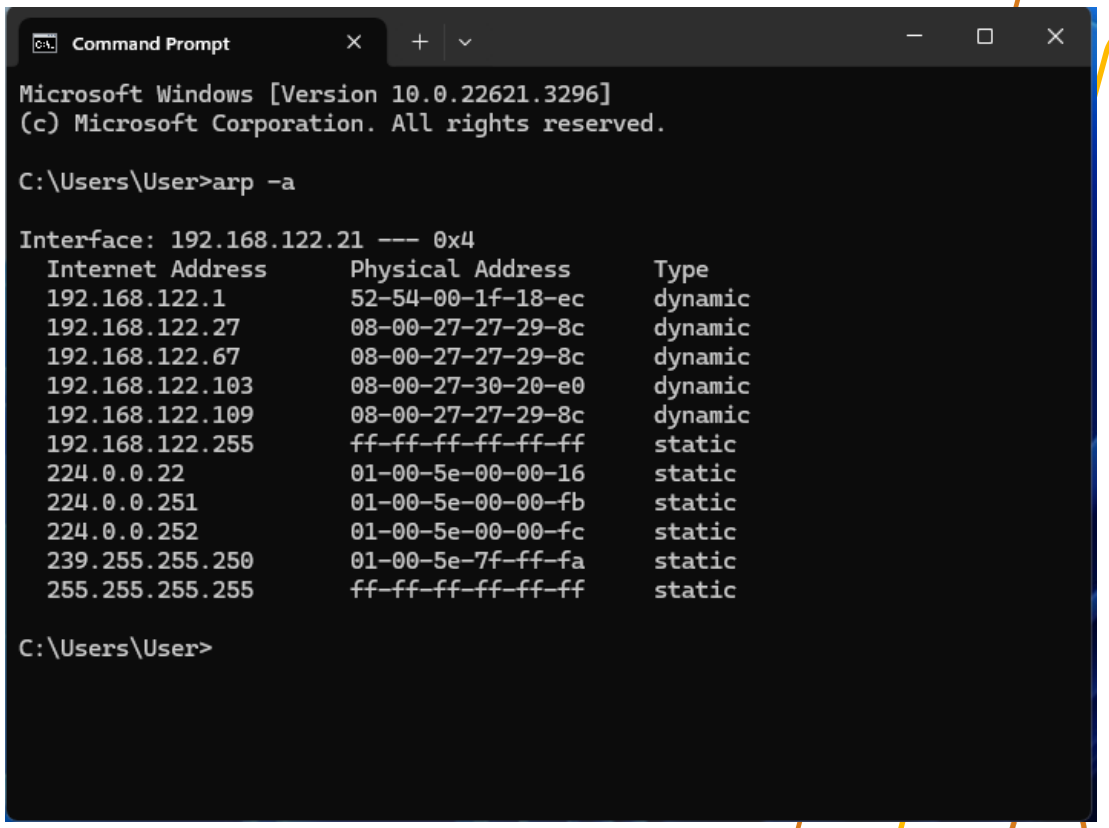




Wireshark start detecting ARP poising request over the network. Formore analysis, select Expert Infromation from the Analyze Menue

Prevention of ARP Poisoning Attack

Prevention of ARP Poisoning Attack



"Dynamic" could be changed to "static," but when a new device is added to the network, you must configure it manually.

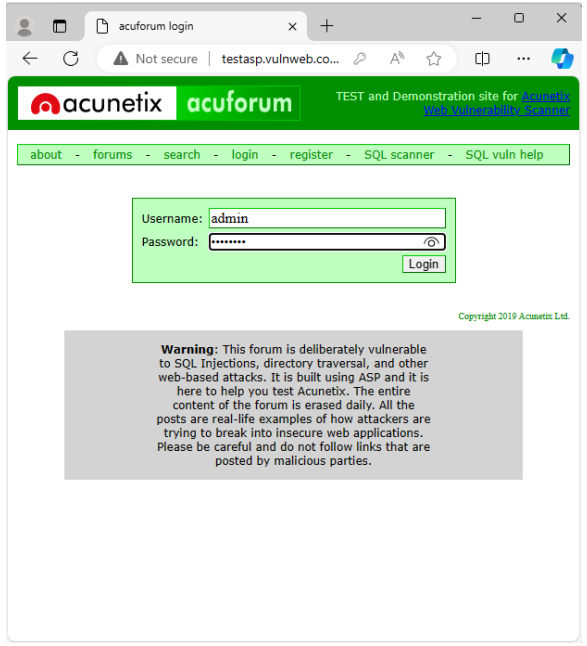
Prevention of MITM

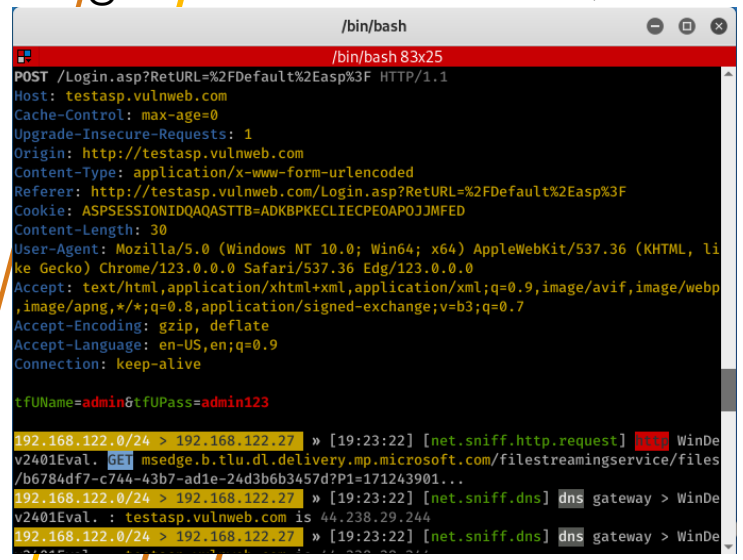
- Detection is not considered a prevention action.
- The previously discussed detection approaches were used only for detecting ARP spoofing attacks.
- To ensure network security, encrypt traffic using HTTPS (browser plugins). Most recent versions of web browsers support services that warn when visiting HTTP websites.
- Some plugins can redirect from HTTP to HTTPS, but hackers can still obtain information about your insecure communication.
- VPN is the best solution for preventing MITM attacks.

VPN

VPN for Prevention of MITM

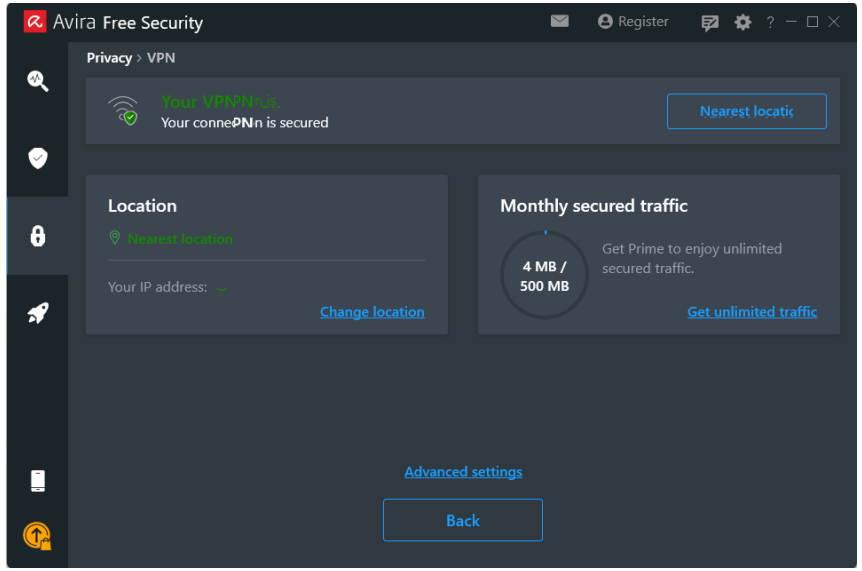
- Use any preferred VPN tool for your test.
- I use Avira VPN, the free version, for testing.
- There is a free version available with about 500 MB of data stream.
- Installed it on my Windows machine.
- Before turning the VPN on, visit testasp.vulnweb.com and insert your login credentials (username and password).
- At the same time, check Bettercap for collecting all visiting website information, including the credentials.

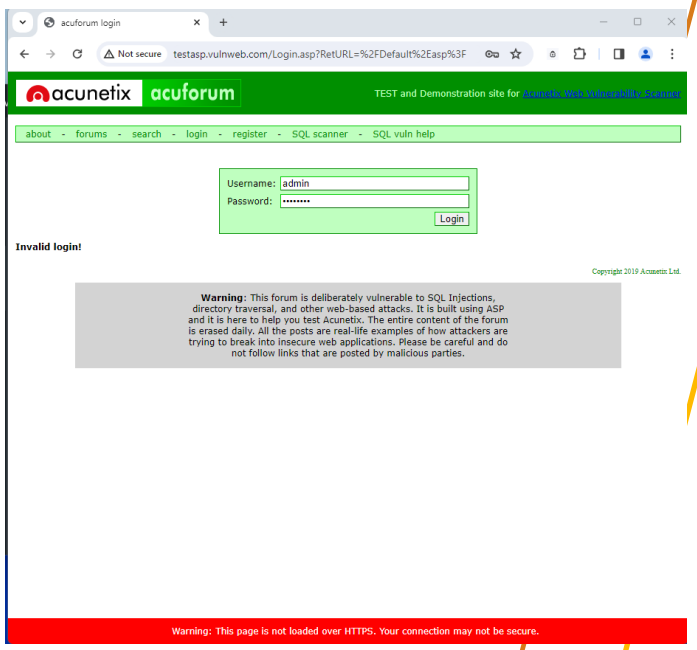


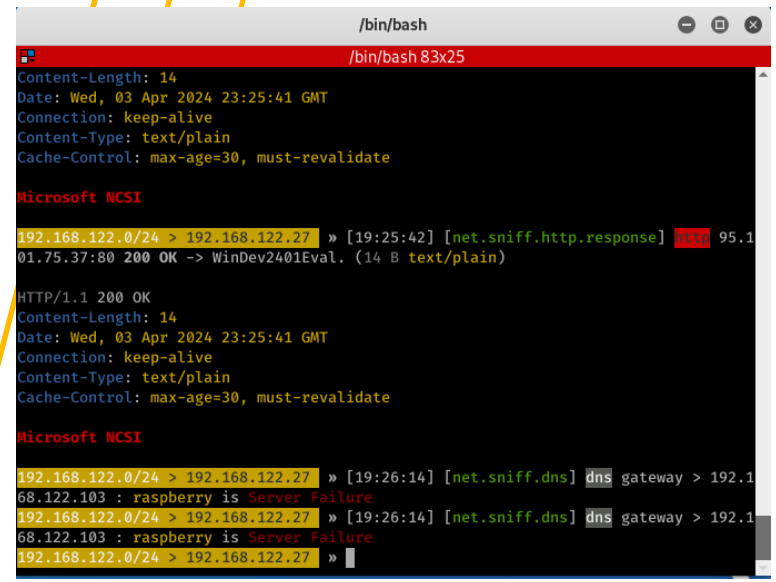


VPN for Prevention of MITM

- Turn on the VPN on your windows mchine (victim machine), and then reload the same page and insert your access credentials
- Opserve the difference







SURICATA

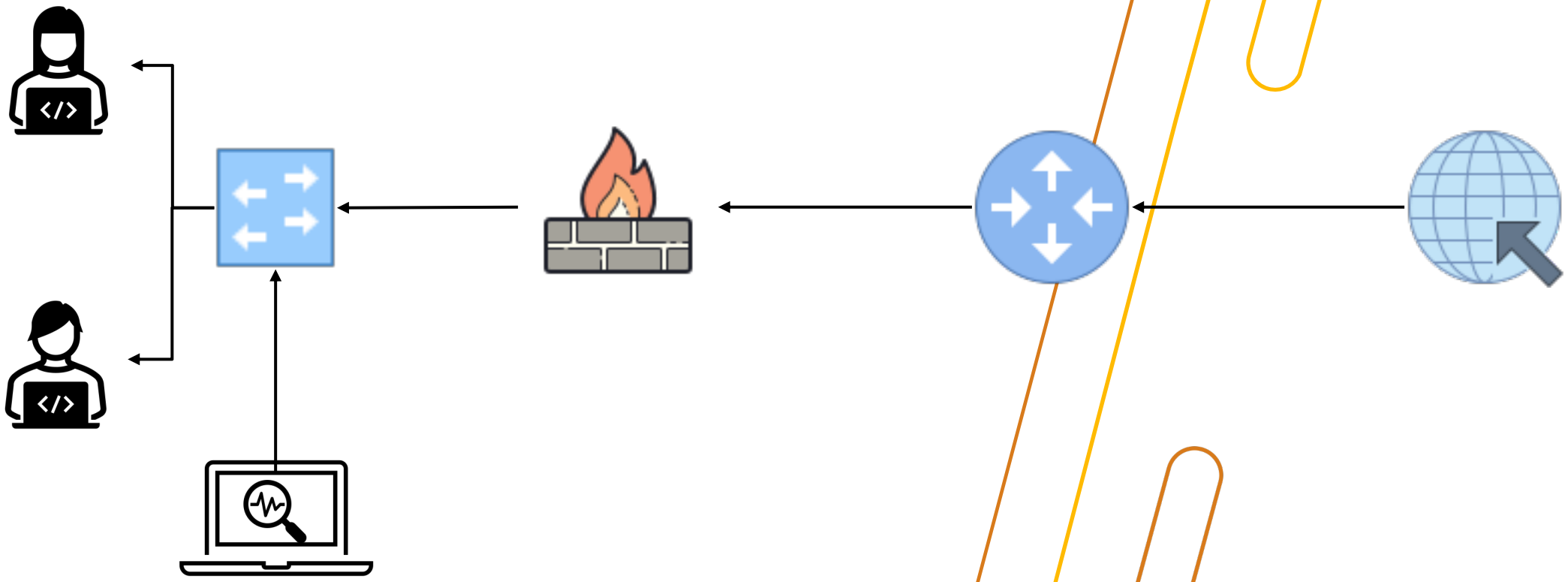
SURICATA

- 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

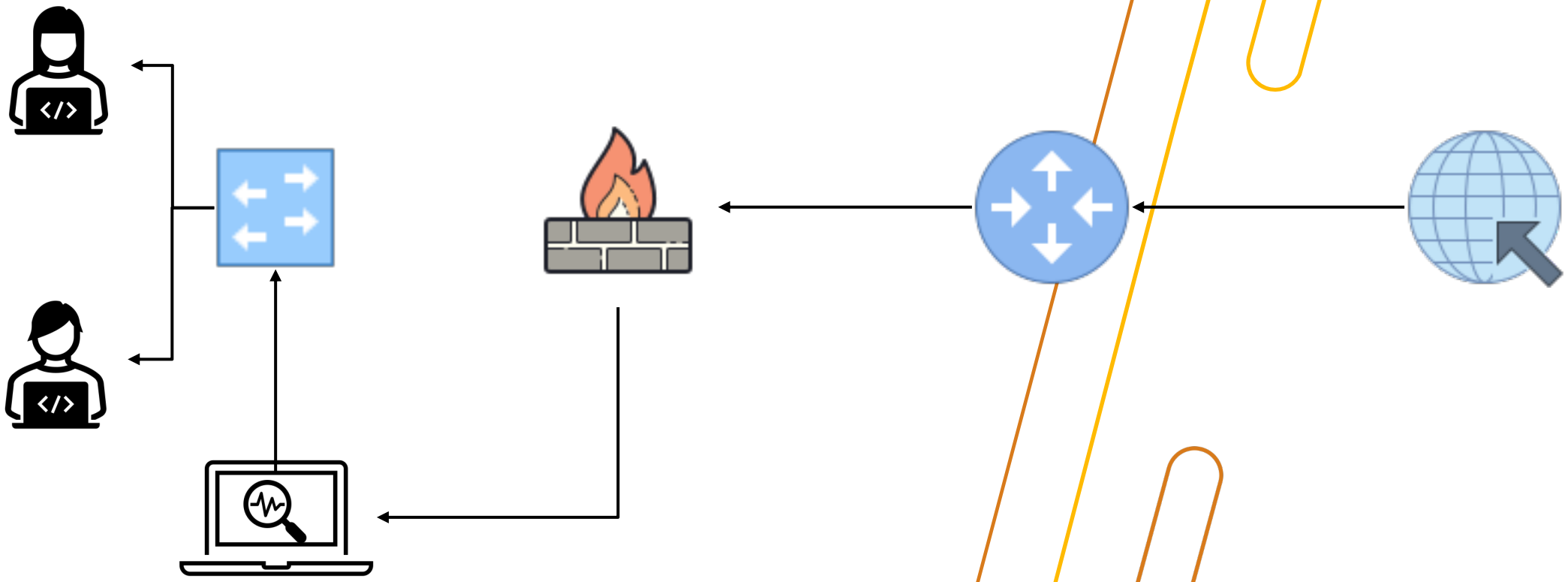
IDS



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

SURICTA Modes

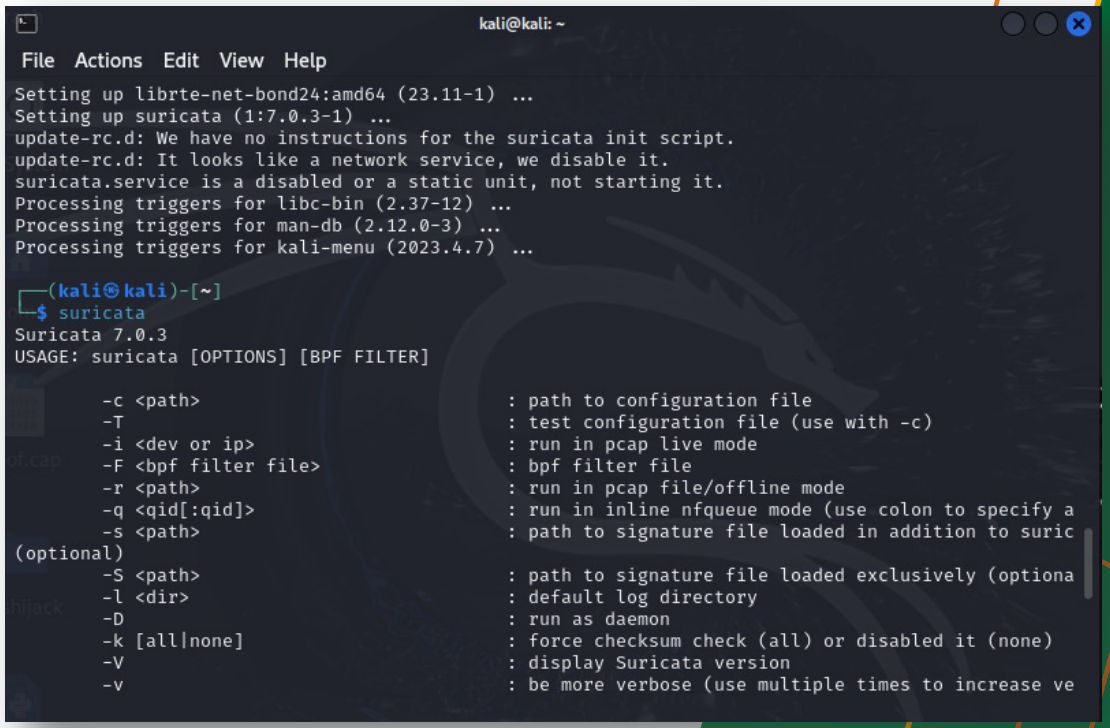
IPS



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

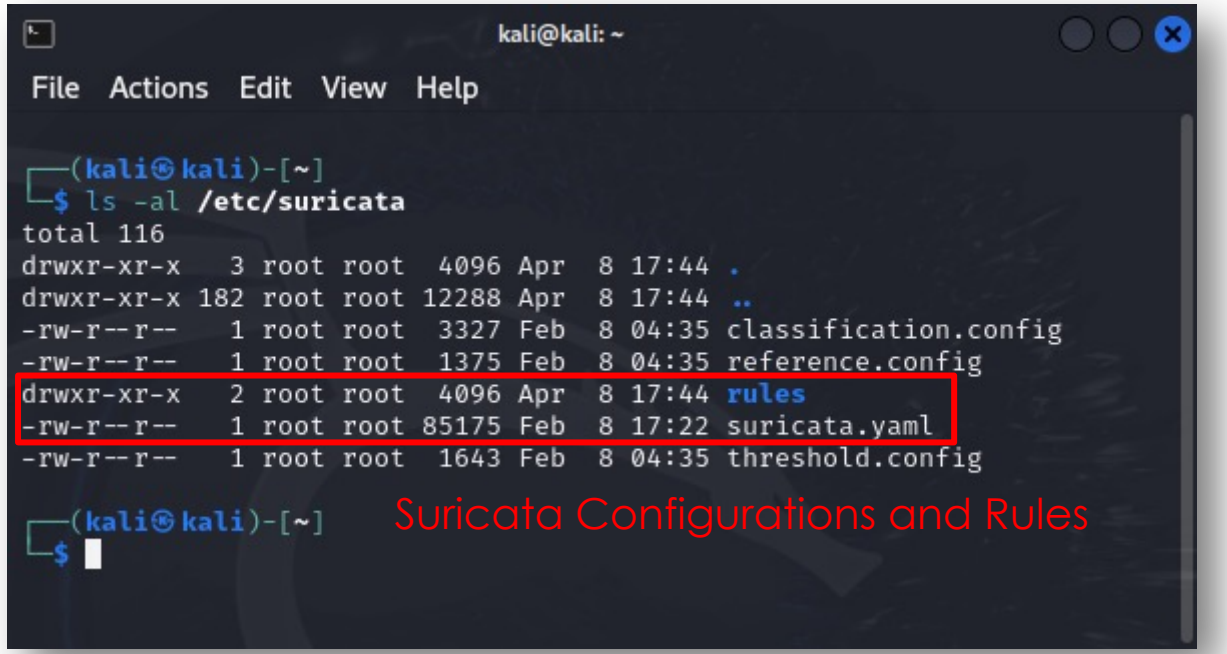
SURICATA Installation

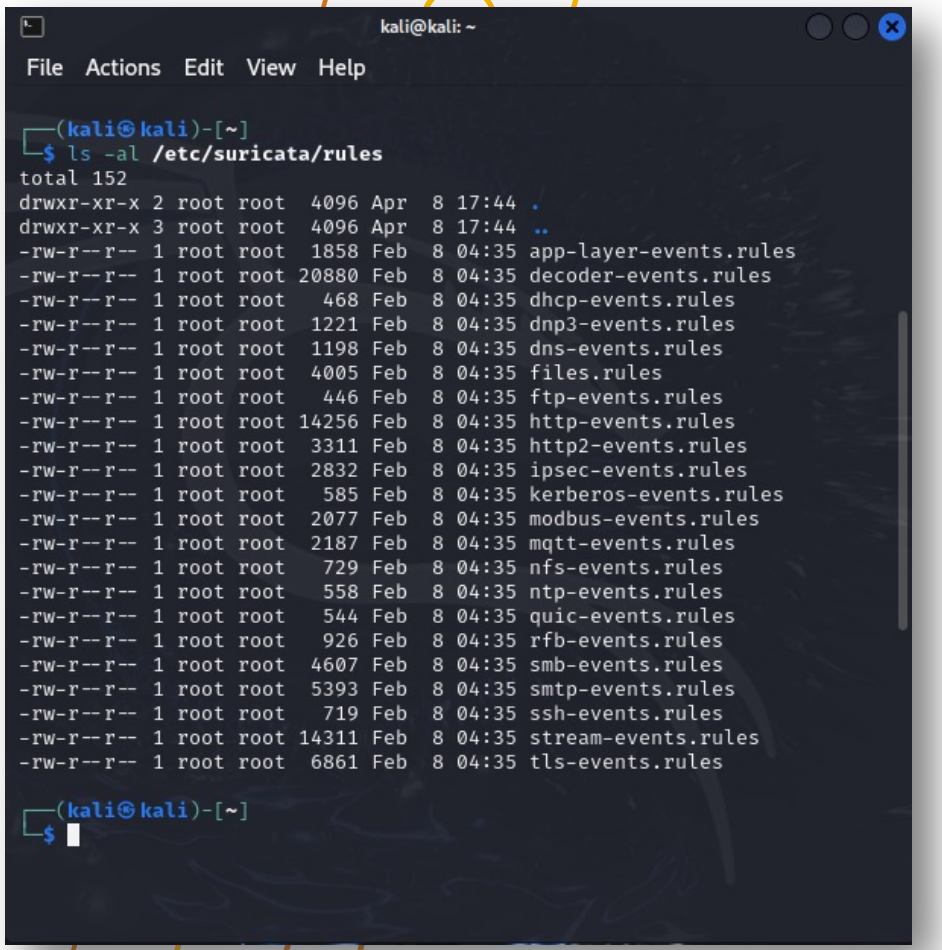
- Sudo apt-get update
- Sudo apt –y install suricata



Suricata Rules and Configurations

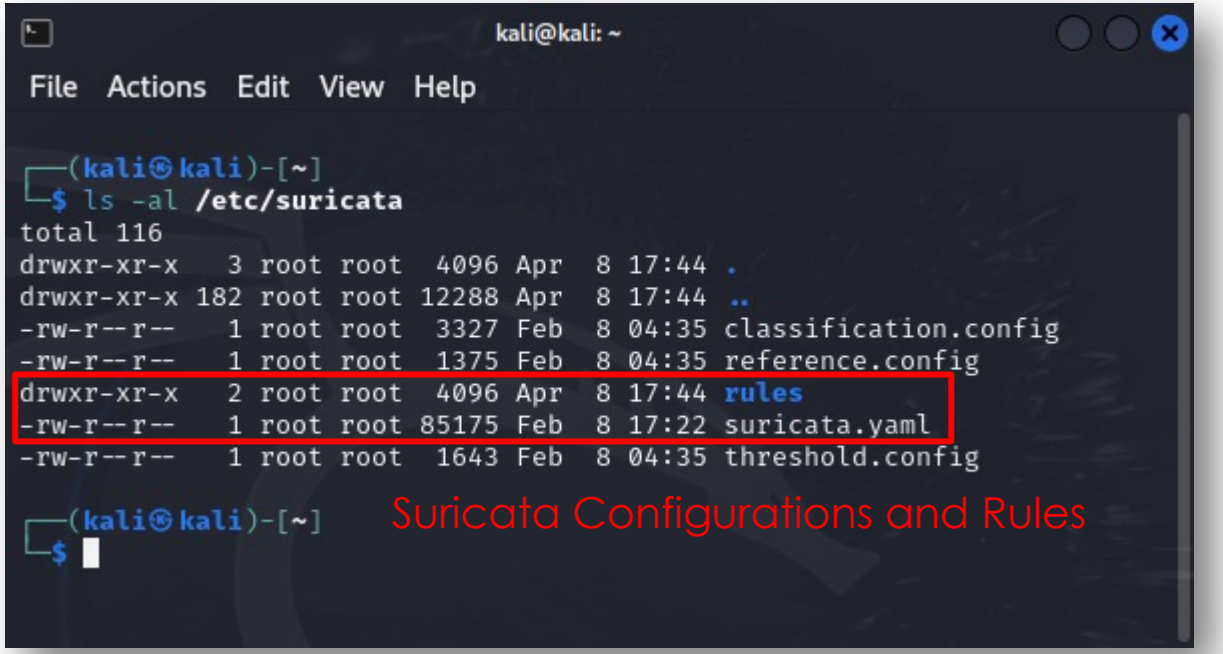
Suricata list of Rules

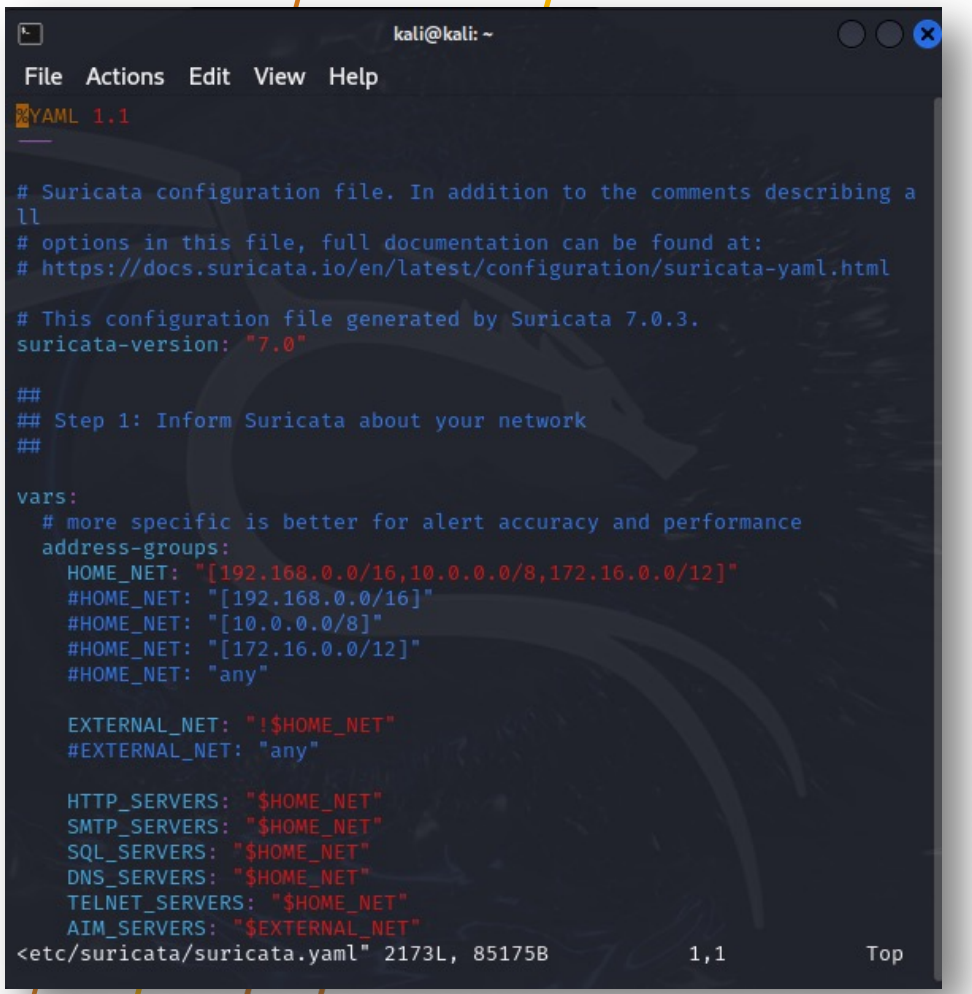




Suricata Rules and Configurations

Update the configuration file
Sudo vim /etc/suricata/suricata.yaml

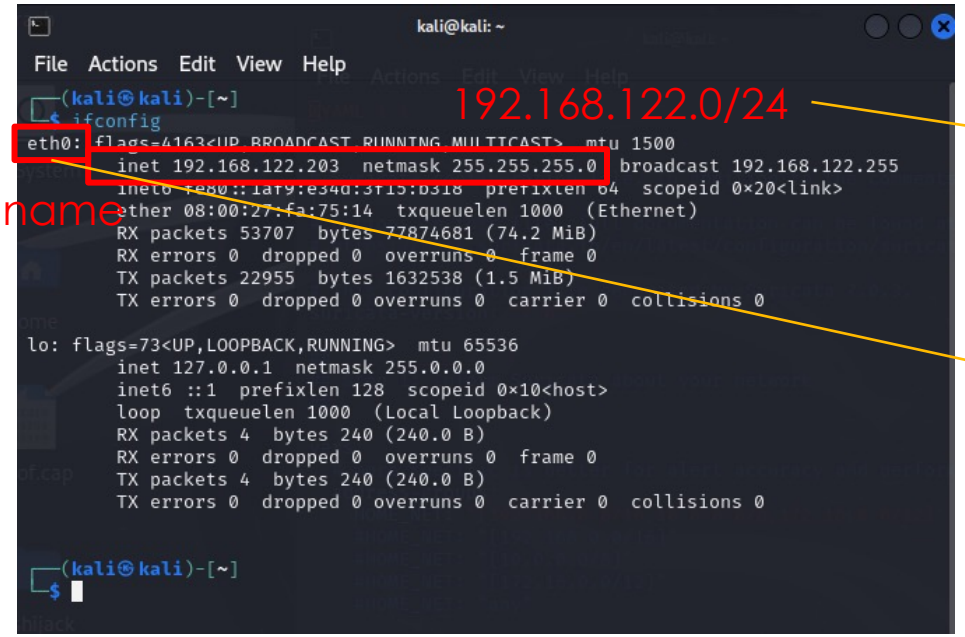




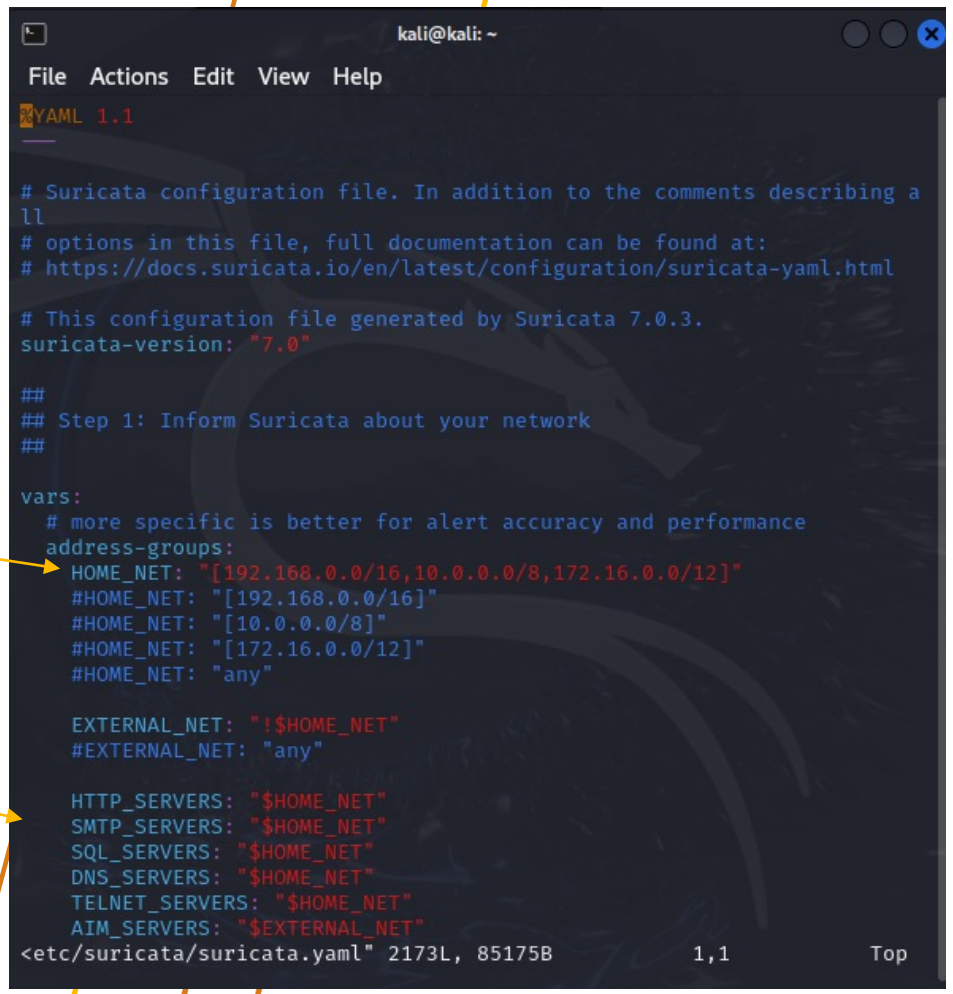
Suricata Rules and Configurations

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



Update the configuration file
Sudo vim /etc/suricata/suricata.yaml



Suricata Rules and Configurations

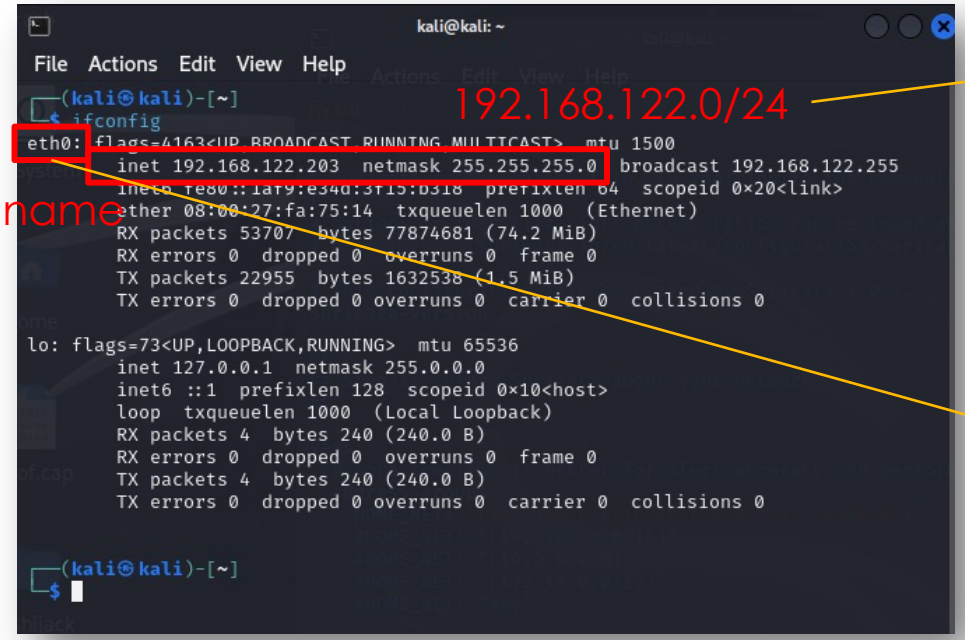
You could directly open the .yaml configuration file, make any updates you want, then store the file again.

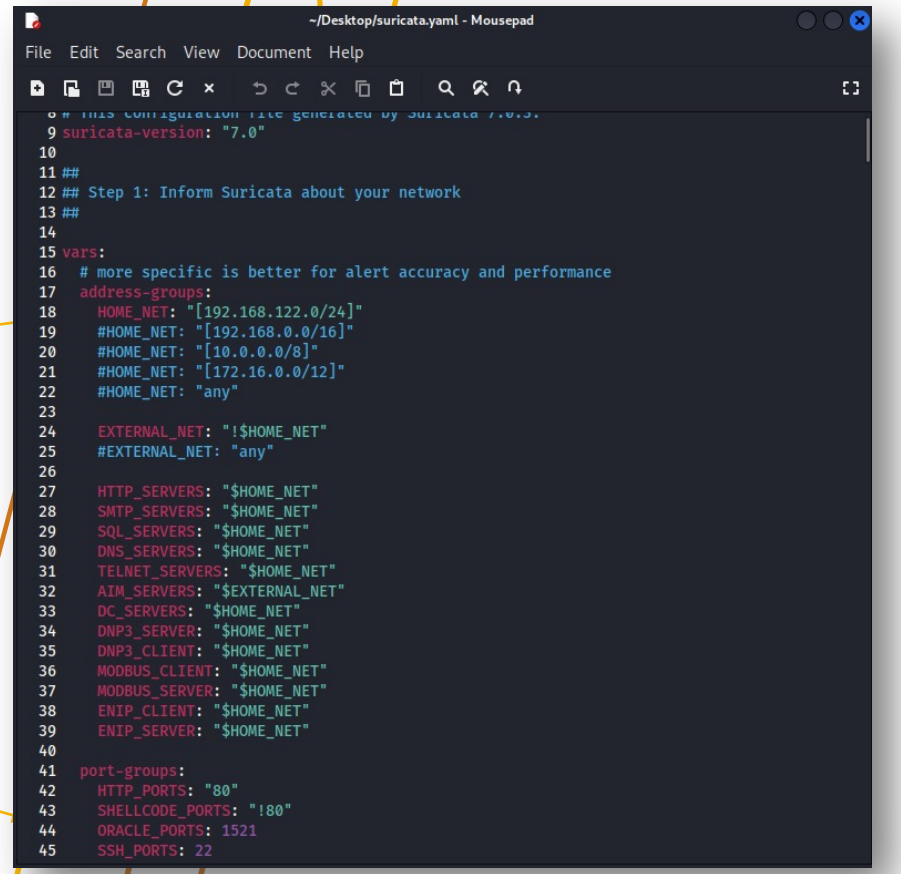
We need to configure the HOME_NET that we want to monitor

So we need to know the subnet

Interface name

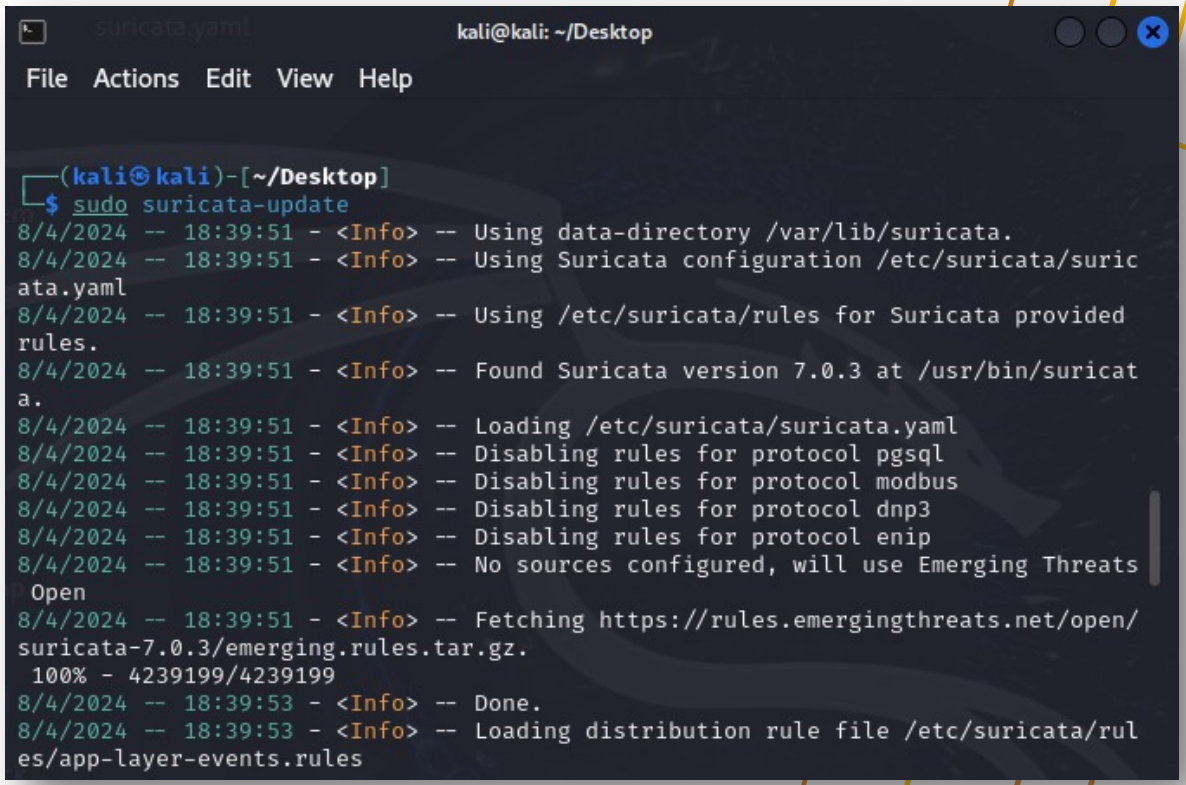
192.168.122.0/24





Suricata Rules and Configurations

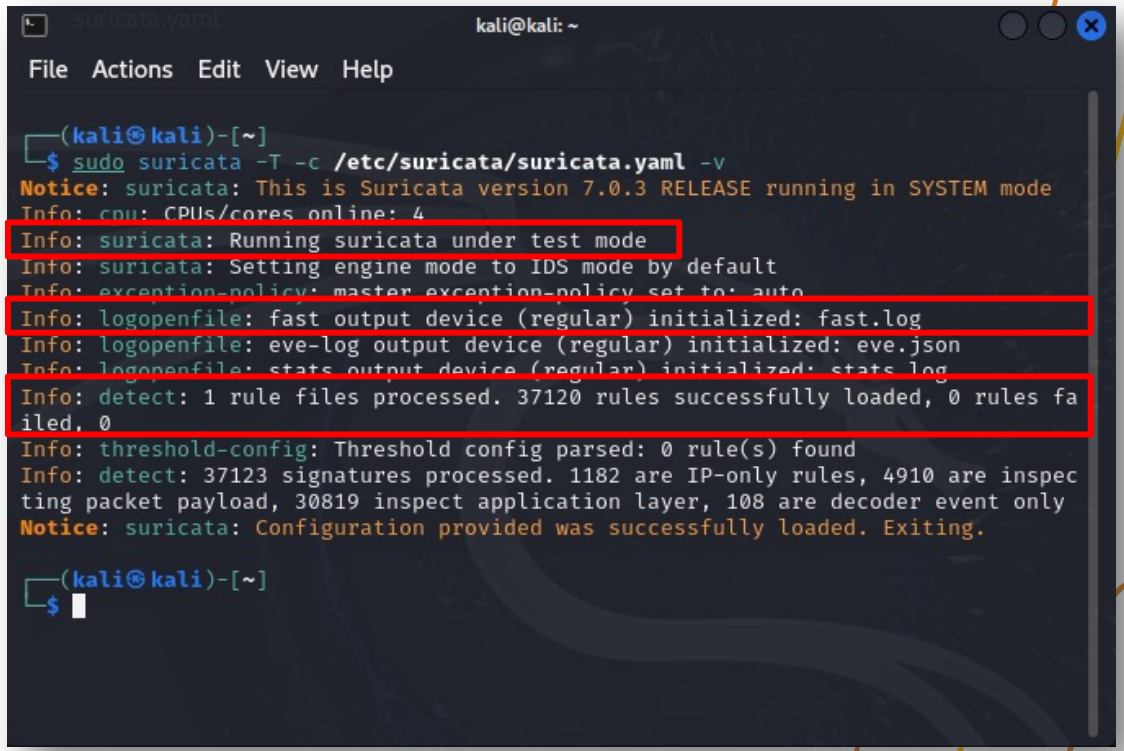
Update suricata using: sudo suricata-update



Suricata Rules and Configurations

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

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

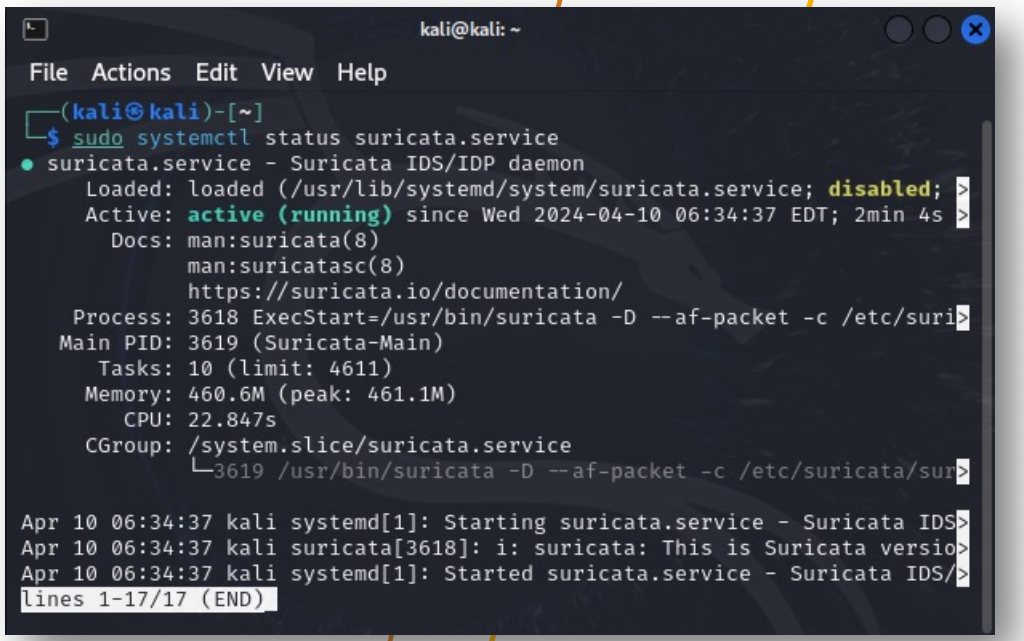


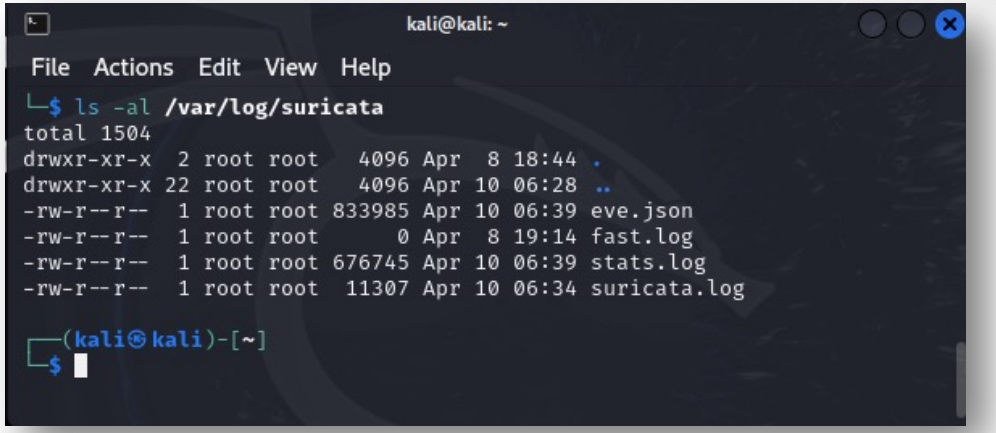
Running on the test mode

There are 37120 rules successfully loaded, and 0 fiald

Suricata Run

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

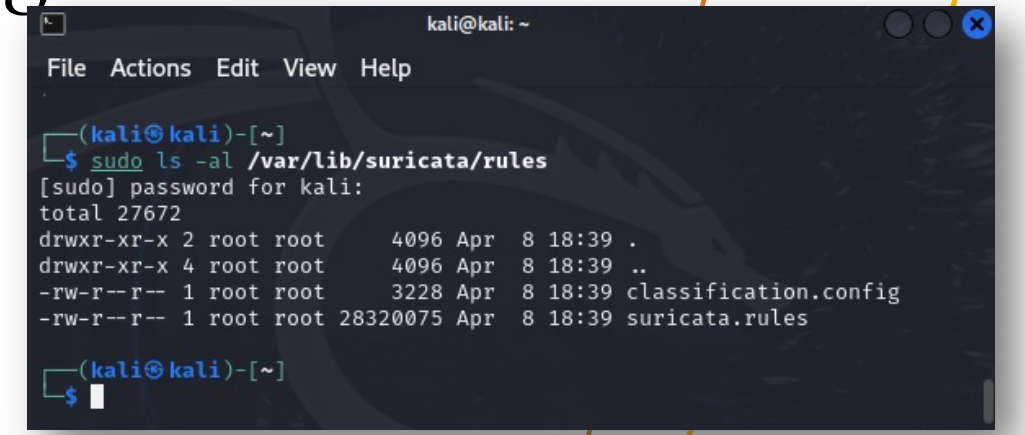




- Now it means that the tool is running on the background

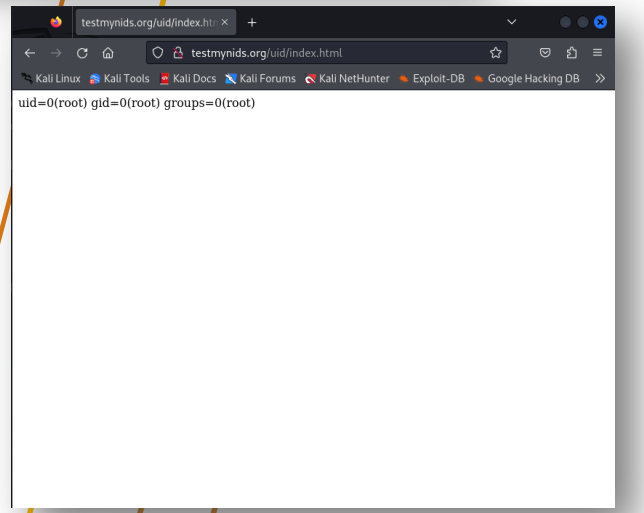
Detect ID Attack using Suricata

- Default rules are stored:
  - sudo ls –al /var/lib/suricata/rules/

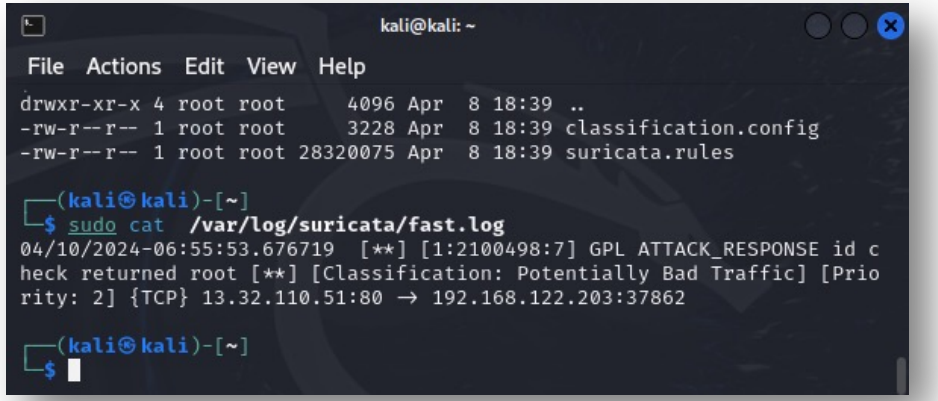


- Test Suricata
  - Visit: http://testmynids.org/uid/index.html

testmynids.org



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

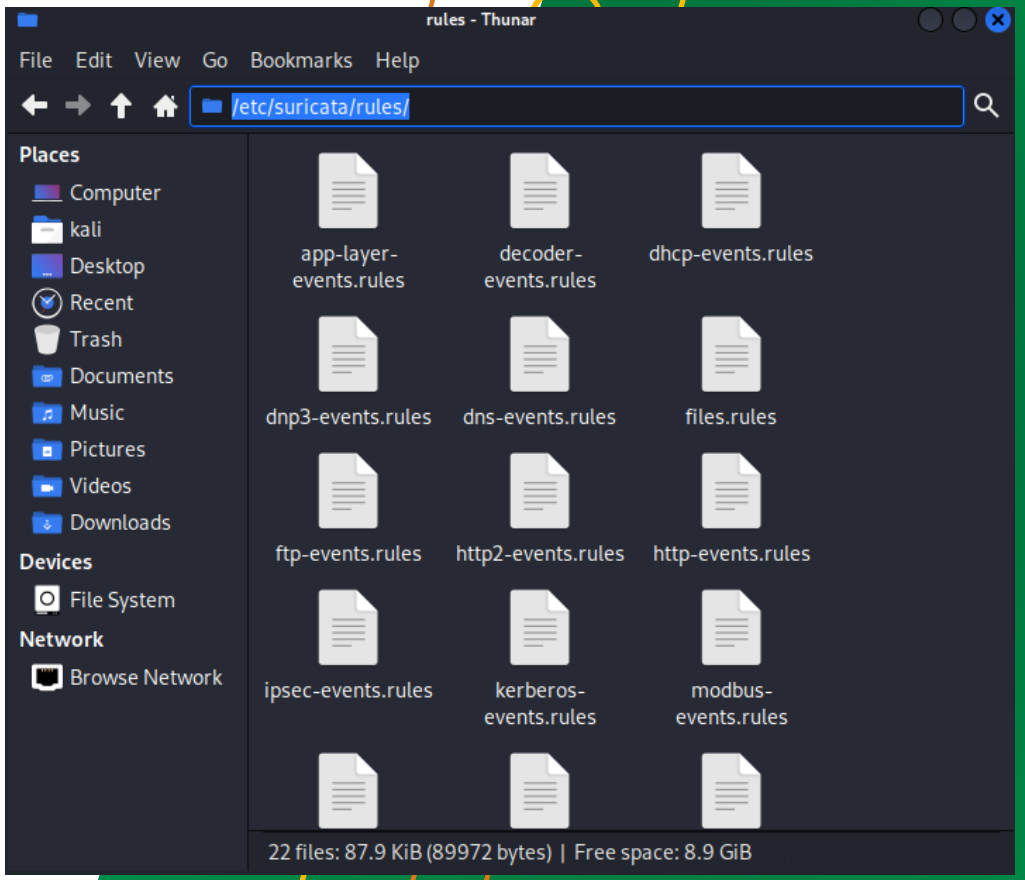


GitHub - 3CORESec/testmynids.org: A website and framework for testing NIDS detection

Customize Rules for Suricata

- Stop Suricata
  - Sudo systemctl stop suricata.service

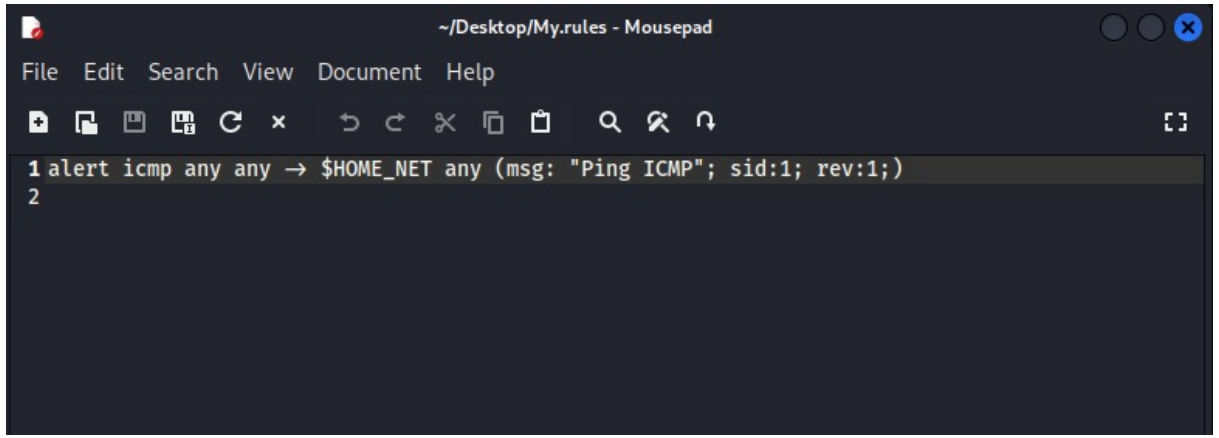
- All rules are store on: /etc/suricata/rules



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;)

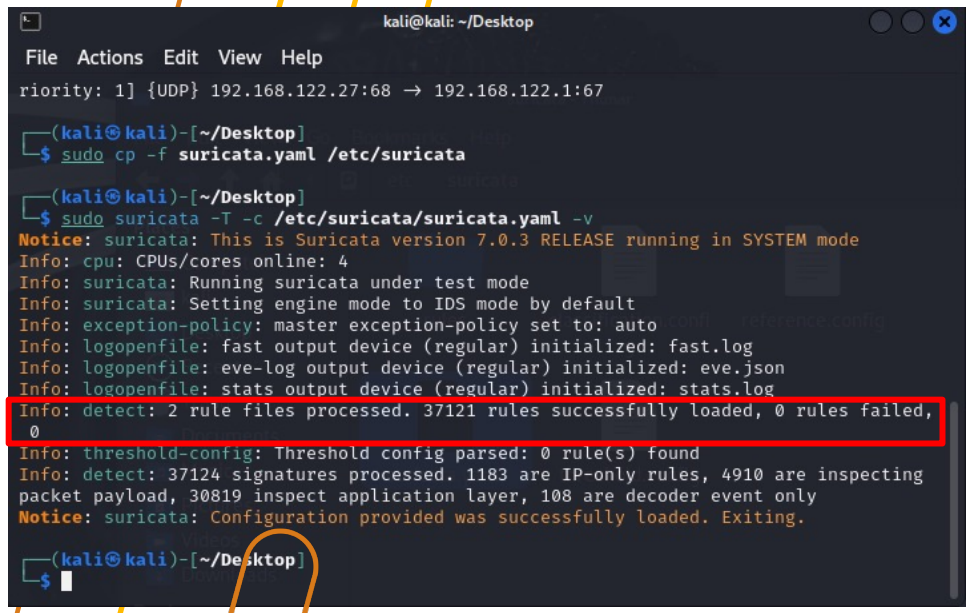


- Update the .yaml configuration file

```
rule-files:
  - suricata.rules
  - /etc/suricata/rules/My.rules
```

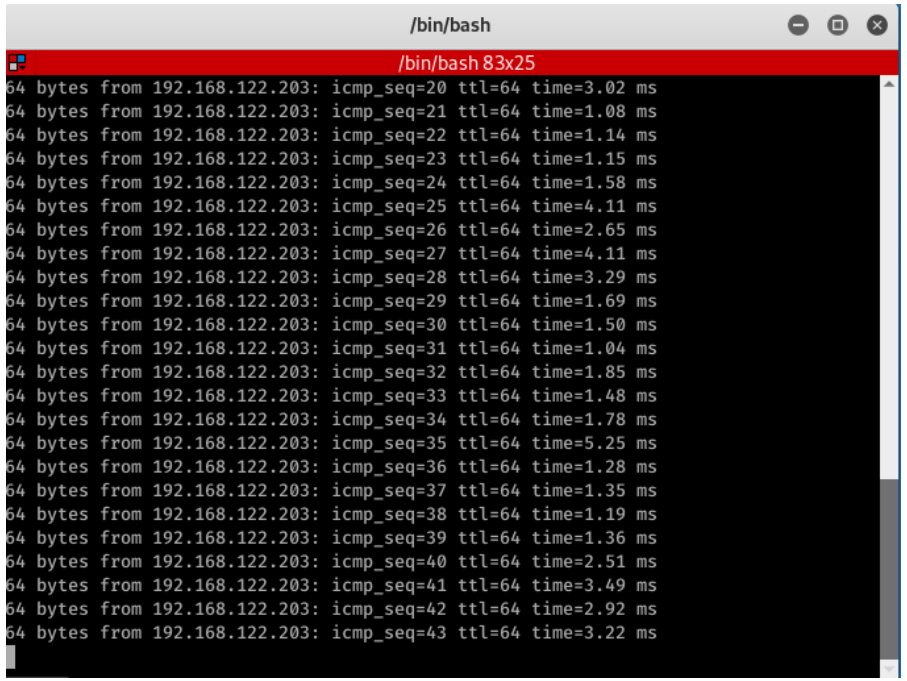
It seems that everything running well

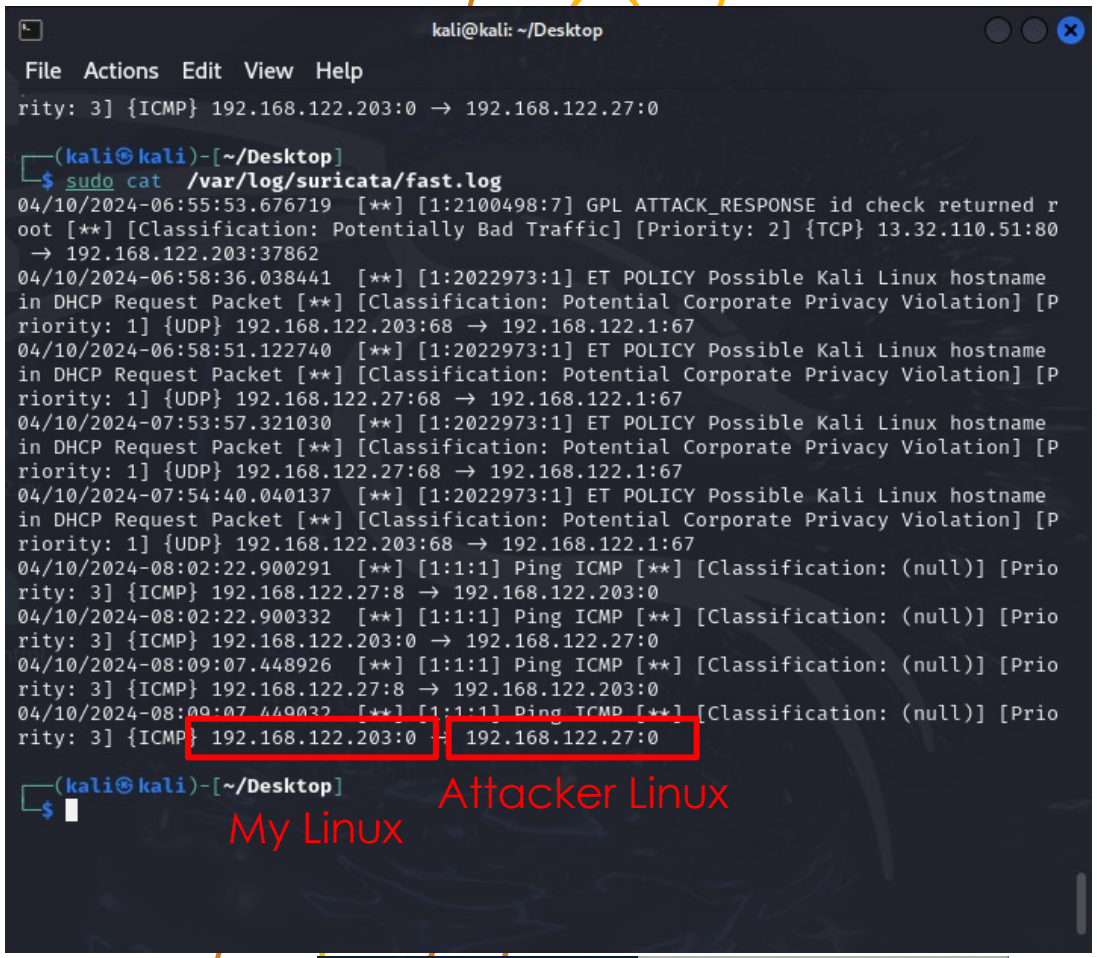
Check the configuration file



Run Customize Rules

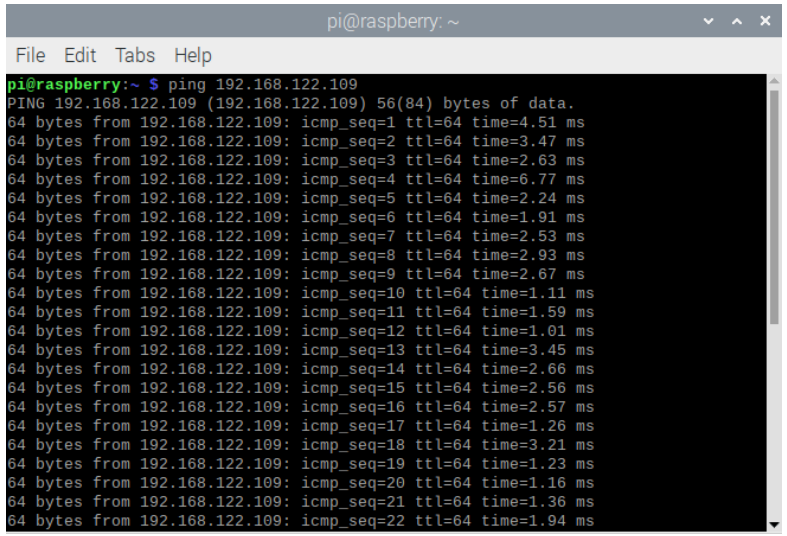
- Run Suricata
  - Sudo systemctl start suricata.service

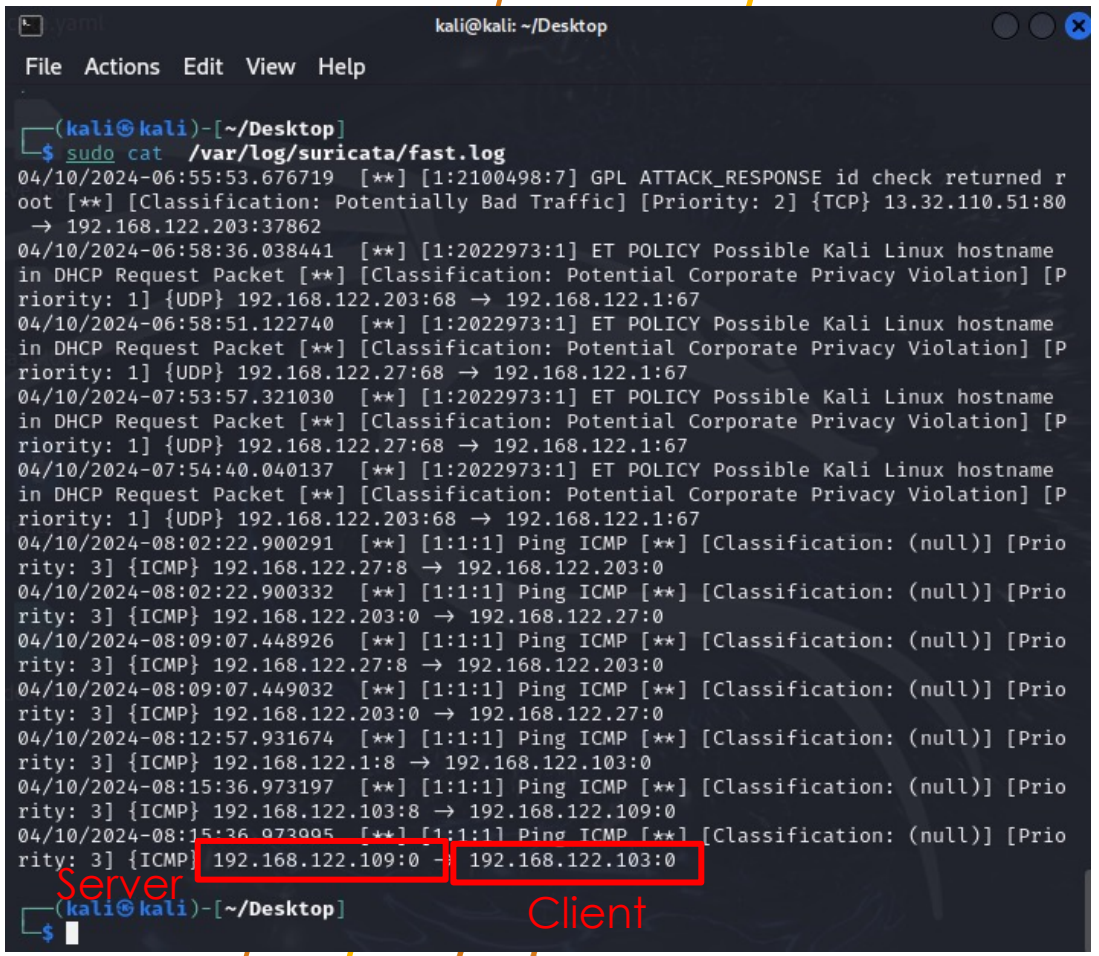




Run Customize Rules

- Test Ping from the Client to Server devices





Connect with CyberSecPro:
How to register and other practical information

1. Website: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Thank you

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