***What is suricata?***

**Suricata** is an open-source **network threat detection engine**. It is used for **intrusion detection (IDS)**, **intrusion prevention (IPS)**, and **network security monitoring (NSM)**. Suricata inspects network traffic in real-time and logs alerts when it detects potentially malicious behavior.

***Suricata installation requirements***

**Linux (Ubuntu, Debian, CentOS, RHEL):**

Requires a multi-core CPU (4+ cores), 8 GB RAM, and 10+ GB disk space. Supports inline IPS with AF\_PACKET, AF\_XDP, Netmap, or DPDK. Install dependencies like libpcap-dev, libpcre3-dev, libyaml-dev, rustc, and cargo using your package manager. Ideal for full-featured deployments.

**macOS:**

Best for testing and development. Use a multi-core system with Homebrew to install Suricata (brew install suricata). Limited to IDS mode; IPS is not supported. Dependencies like libpcap, jansson, and libyaml are handled by Homebrew.

**FreeBSD:**

Also supported for Suricata installation with similar hardware requirements. Install via pkg install suricata, with dependencies like libpcap, libyaml, and libnet. IPS features may vary based on NIC driver support.

Step 1

First download suricata in our linux

(here’s the link you can download suricata <https://www.openinfosecfoundation.org/download/suricata-7.0.11.tar.gz>)





download suricata from this link as you see or if you want to download directly to our linux I already mention the main link in above

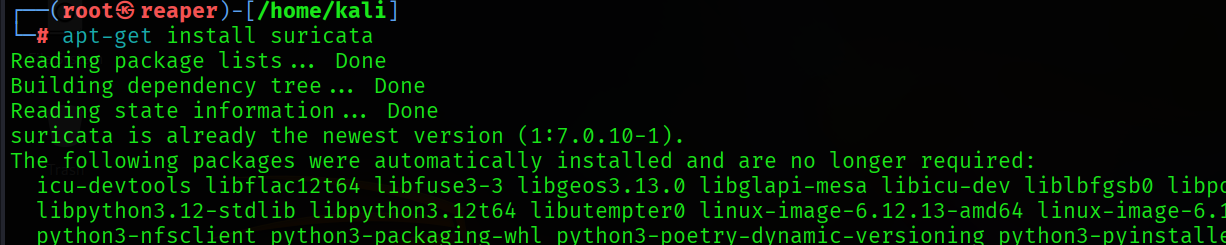


step 2

now download suricata in our linux

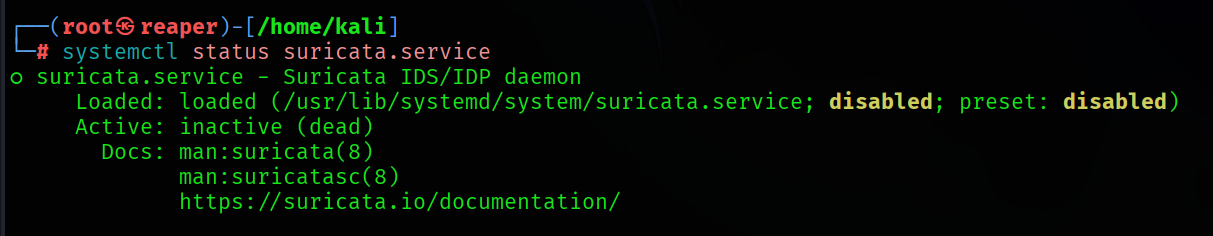
apt-get install suricata

apt-get -y install suricata



Step 3

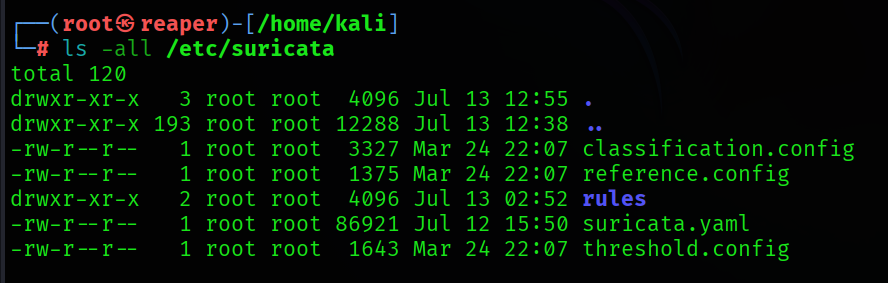
Now check our suricata enable or not after that you can do our configuration



It’s disable so now we can configure our suricata

Step 4

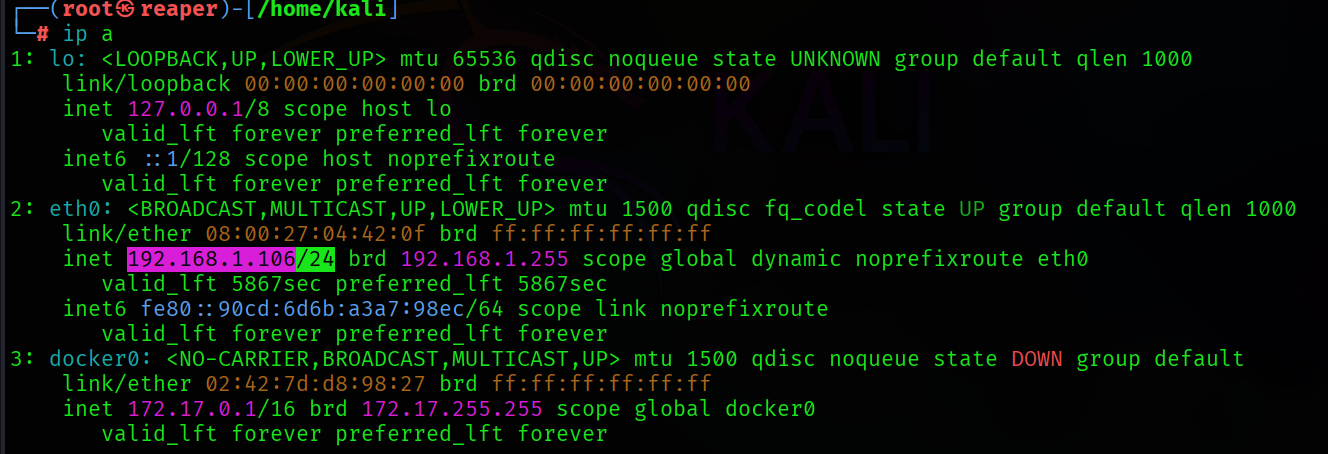
Now first find my suricata configure file



And now get our configuration folder its “*suricata.yaml”* so now you can do

Step 5

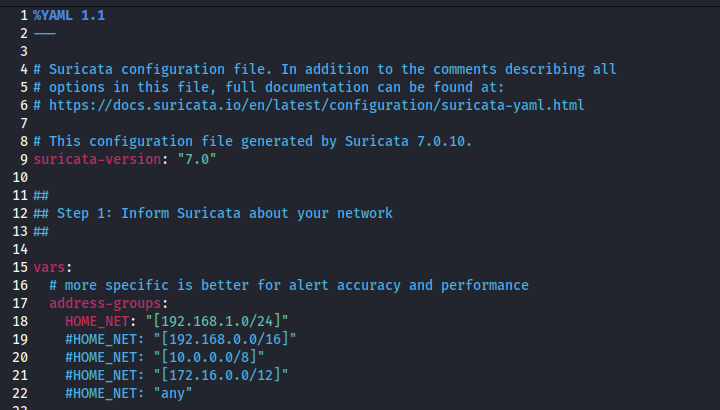
But, first of all find first our ip add of my terminal before configure



Now configure file, and our ip add

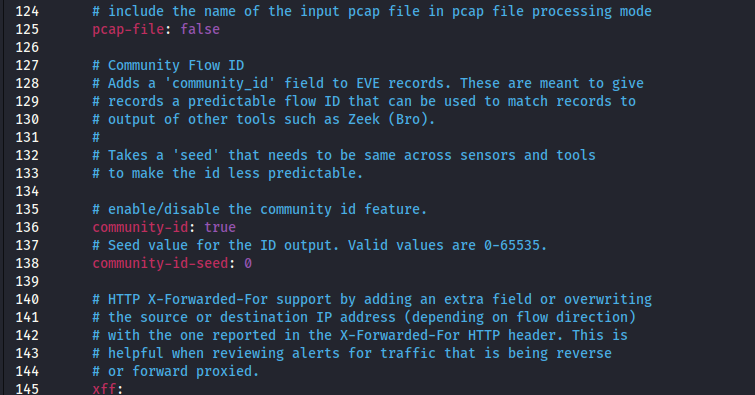
Step 6

So first open suricata.yaml file in mousepad for configuring and adding rules and do some changes

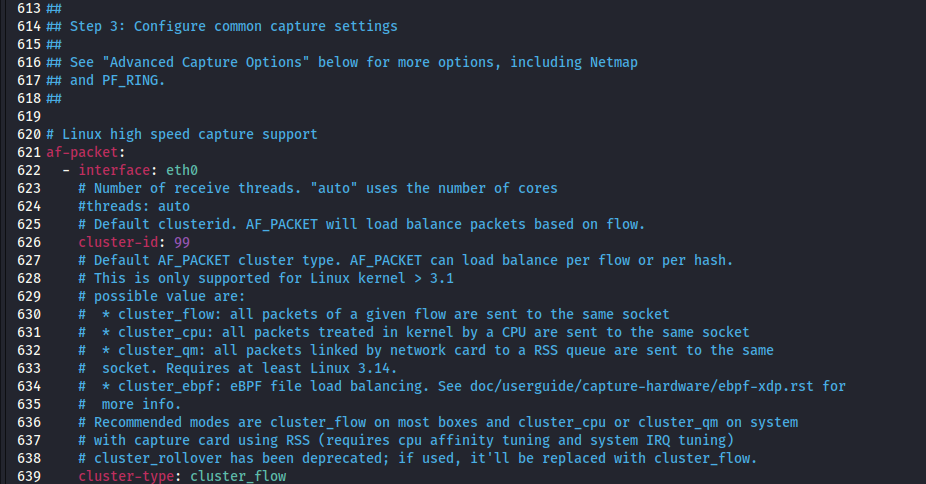




In this place you want to put our ip add



After that set community-id True



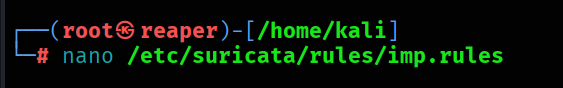


Set all network interface where required as our interface name “ like here you see ETH0”

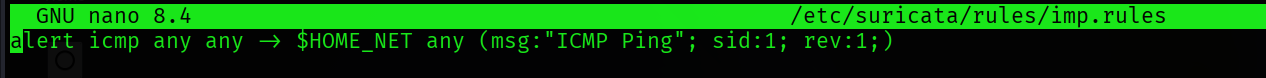
And last now add rules 

Step 7

So now create rule file



And after this add rule



Alert icmp any any -> $HOME\_NET (msg:”ICMP Ping”; sid:1 rev:1;)

 alert → Action: generate an alert.

 icmp → Protocol: Internet Control Message Protocol.

 any any → Source IP and port: any.

 -> → Direction: from source to destination.

 $HOME\_NET any → Destination IP and port: any host in your internal network.

 msg:"ICMP Ping" → Message to log.

 sid:1 → Signature ID.

 rev:1 → Revision number.

Now add rules in suricata.yaml file

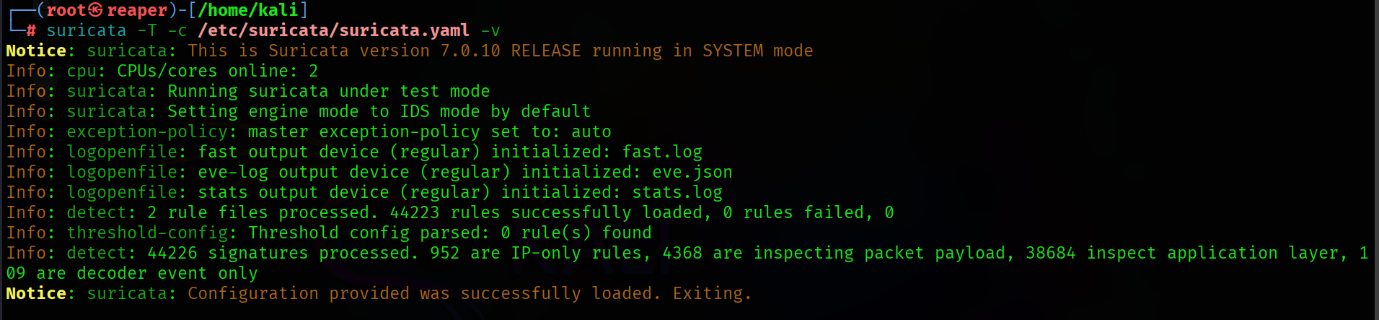




After that save it and close the mousepad

Step 8

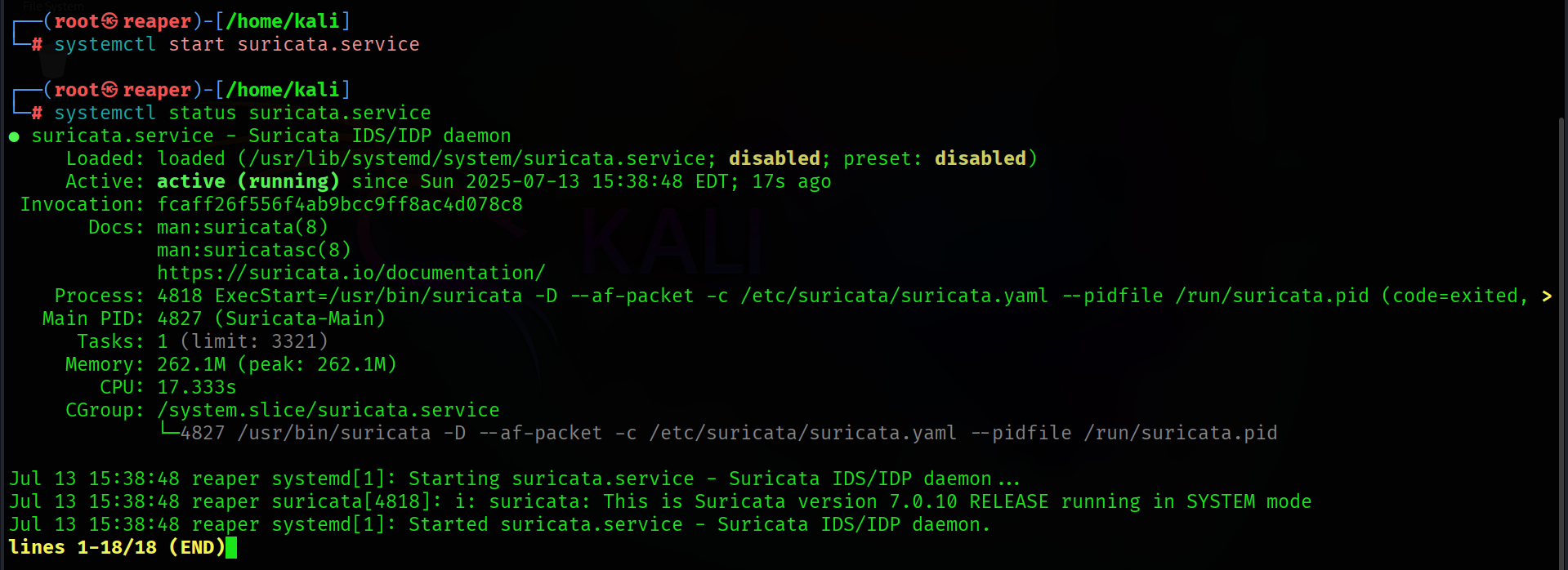
now run suricata on test to check errors



Everything is fine & all rules sets successfully

Step 9

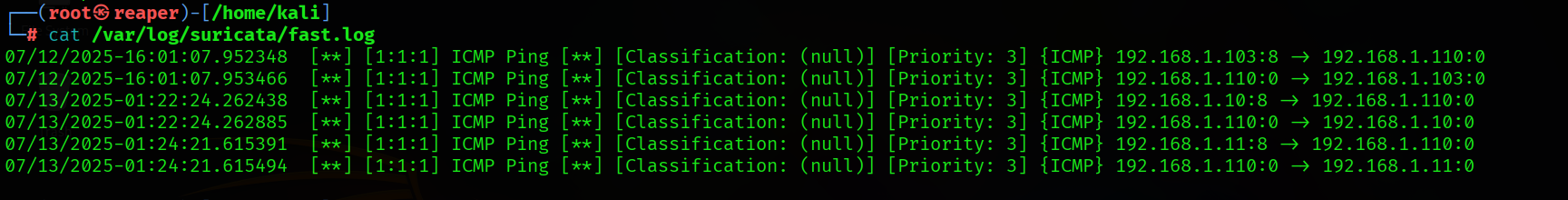
Now start suricata and it start monitoring



Step 10

For looking the log file do this

“Cat /var/log/suricata/fast.log”



And here you see captured logs of ping in file