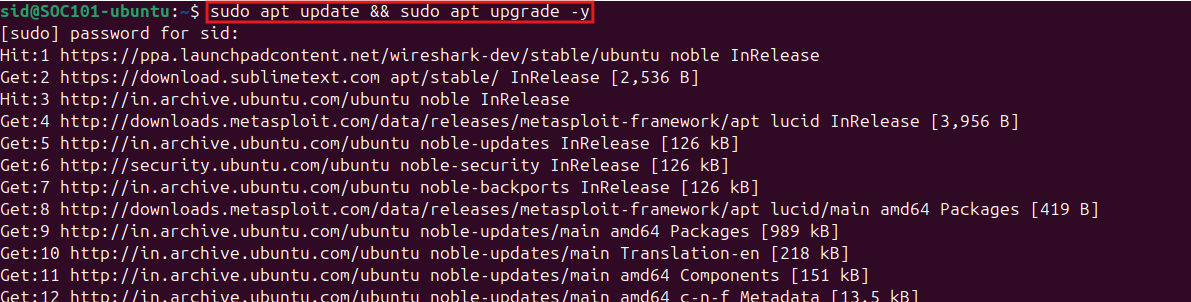
### **SURICATA INSTALLATION AND CONFIGURATION ON UBUNTU**

I am going to install and configure Suricata on an Ubuntu machine to act as an IDS. First let us update the repositories on the system using the following command

sudo apt update && sudo apt upgrade -y

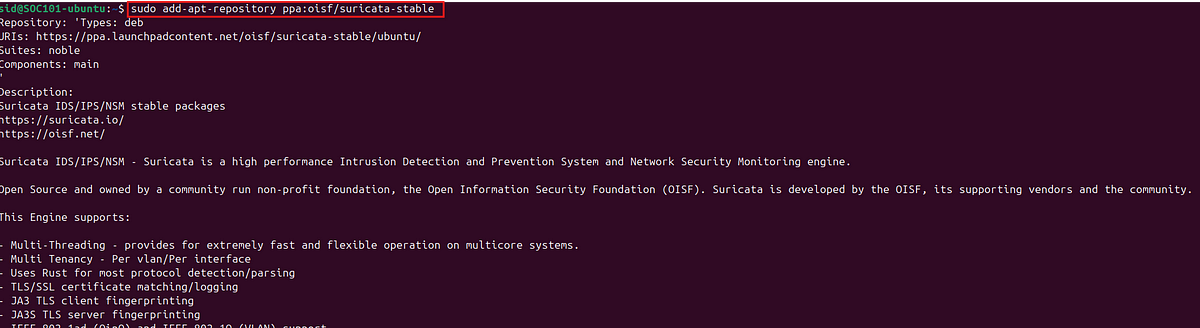


This will update all the available repositories and then upgrade all the packages present in the system.

No we can add the Suricata repository to the system using the following command

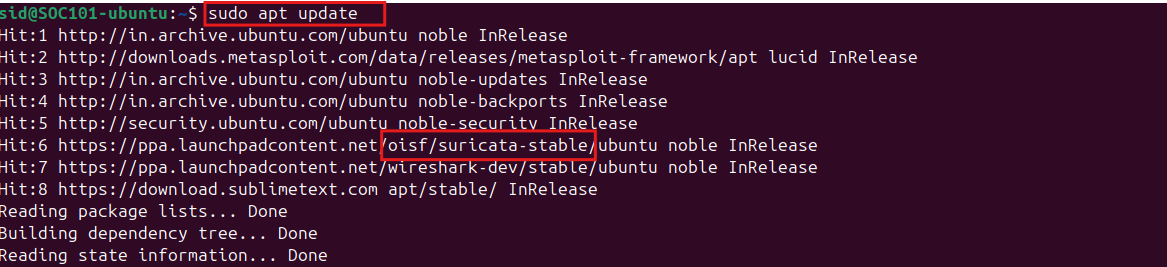
sudo add-apt-repository ppa:oisf/suricata-stable

This will add the Suricata repository to the list of available repositories on the system, from where we can download the packages.



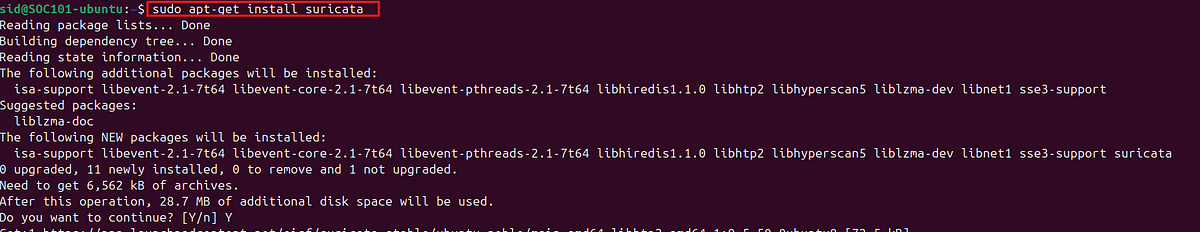
Now use the following command to update the repositories to reflect the newly added repository.

sudo apt update



We can see above that our repository is added successfully. Now we can install Suricata using the following command and enter ‘Y’ when prompted.

sudo apt-get install suricata

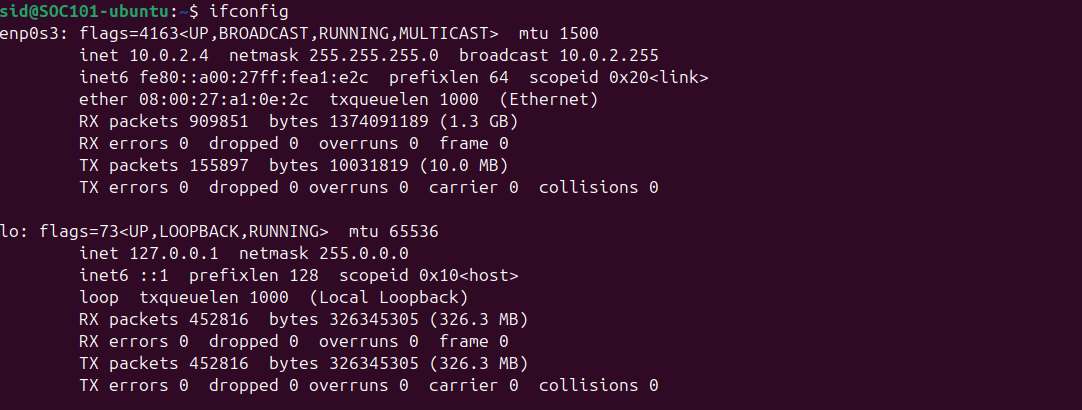


#### **Configuration**

Before we can configure Suricata, we need to stop Suricata service using the following command

sudo systemctl stop suricata.service

Now, check the network configuration of the system using ifconfig.



From the above image we can see that

IP: 10.0.2.4

netmask: 255.255.255.0

Network Interface: enp0s3

Now, Let us start configuring the Suricata service.

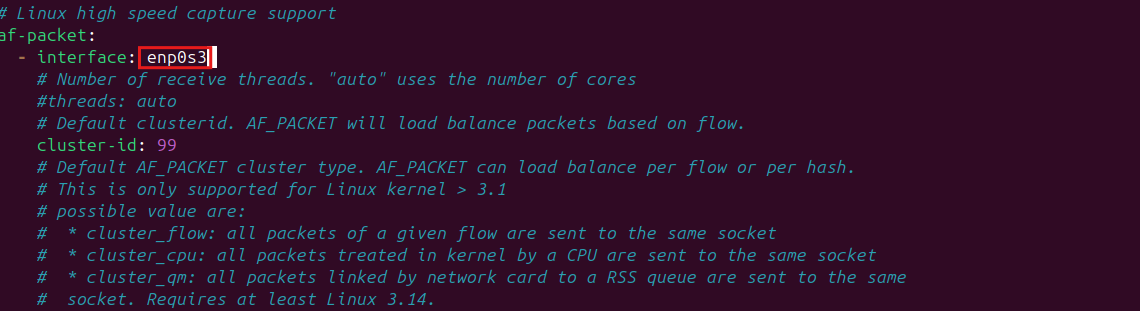
Let us edit the suricata.yaml file which contains the configuration settings of Suricata. This is present at /etc/suricata/suricata.yaml



From the above image we can see that I set the HOME\_NET variable to 10.0.2.4. I gave my IP address instead of an IP range for convenience.

EXTERNAL\_NET variable is set to !HOME\_NET which suggests that any IP address other than the one specified as home network top be treated as external.

Then search for af-packet variable and set it to the network interface of the system. In my case this is ‘enp0s3'.

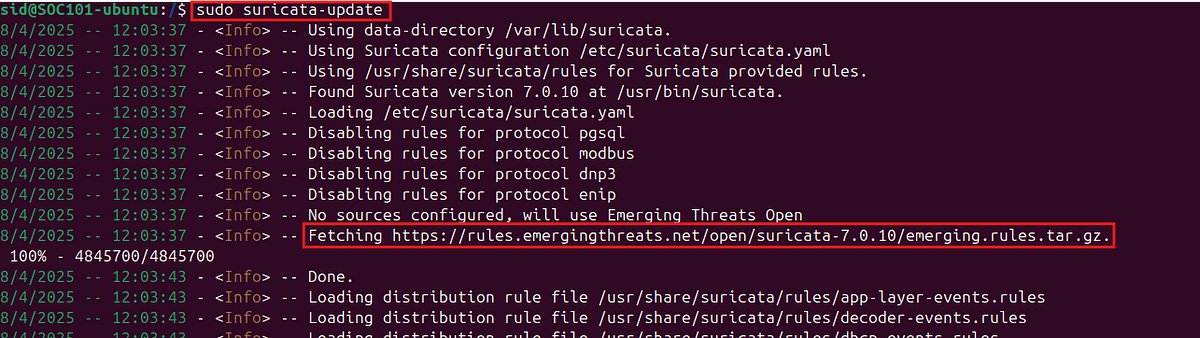


Then, check for the rules file that Suricata is referencing. By default this will be in /var/lib/suricata/rules folder.



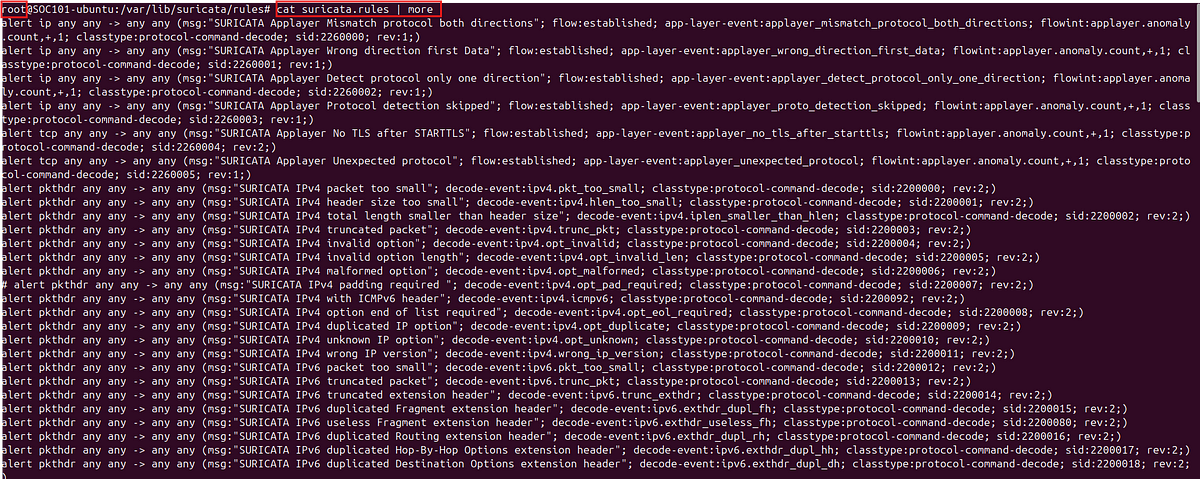
We can download and update the rules by using the following command. This will download and update the Suricata rules folder with the community rule set.

sudo suricata-update



Now, we can see the suricata.rules file. But as this is under the root we need to change into root user in order to view this file. Since this file has a lot of rules we will pass the output to more or less to view the rules.

cat suricata.rules | more

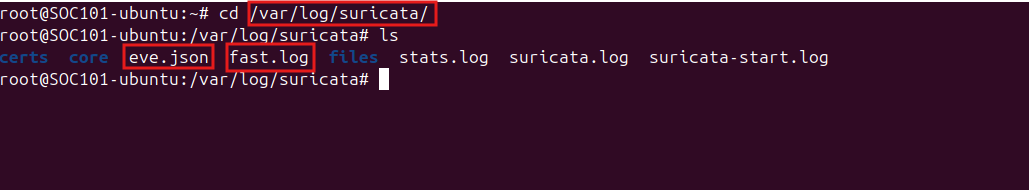
suricata rules

#### **Logs**

There are two default log files which are used to log the traffic.

1. Fast.log: This file provides a concise human readable log format with minimal but important data.
2. eve.json: This file contains more extensive details. The logs are stored in json format which can be useful to feed into a SIEM.

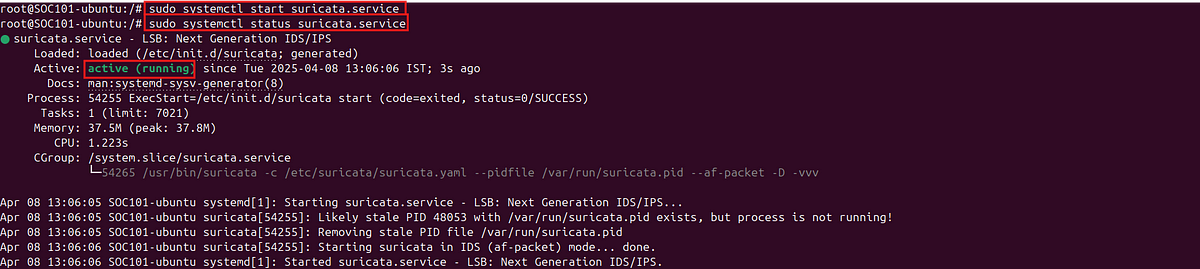
The log files can be seen under the /var/log/suricata folder.



Now, we can start the Suricata service to start monitoring for traffic.

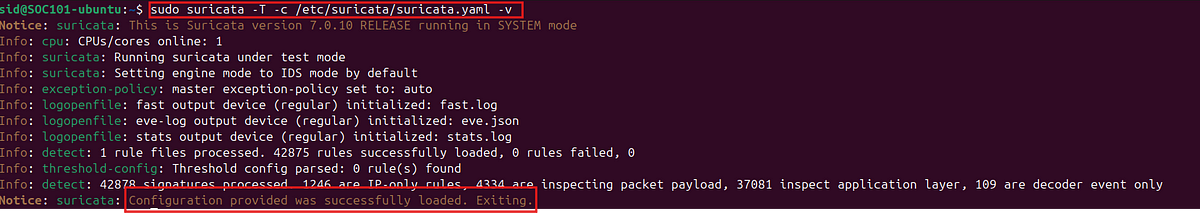
systemctl start suricata.service

systemctl status suricata.service



We can now test if everything is configured correctly, by running suricata in test mode by setting the -T flag with the following command

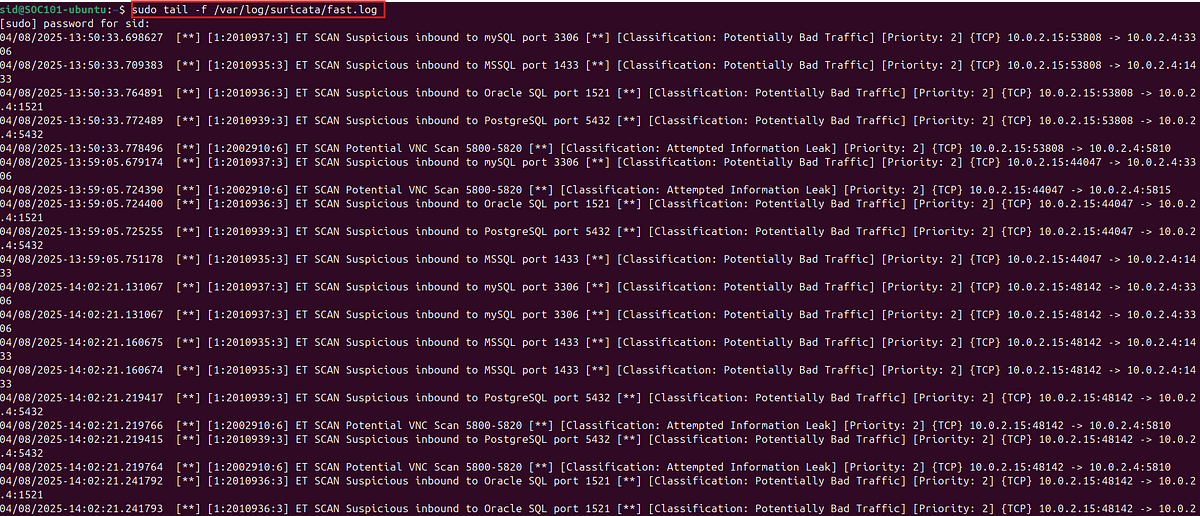
sudo suricata -T -c /etc/suricata/suricata.yaml -v



**Testing**

Testing the working of Suricata, by running an NMAP scan from our attacker machine. In the below screenshot we can see that the Suricata service has logged the NMAP scans.

tail -f /var/log/suricata/fast/log



Now Suricata is installed and properly configured on the system to alert us of any malicious activity.