Codes used to run SNORT/SURICATA in command line

Snort command line to run its service:



Using Snort as the first thing is to ensure we are using the snort program. The second part of the command line is to run the rules set saved inside the LUA file in Snort configuration. This allows us to save the set of rules in the LUA file to maintain it and keep it memory for Snort to use it.

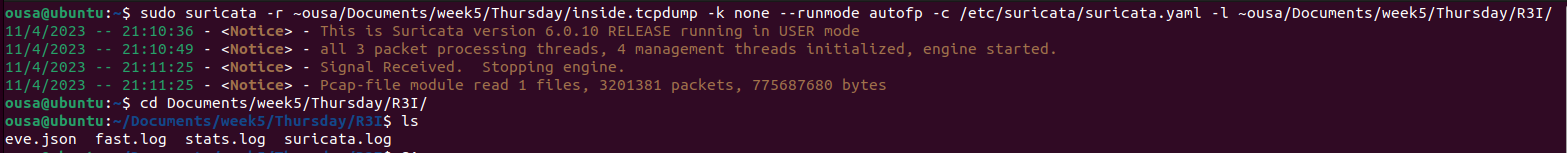
Next is to “-R Downloads/snort……/includes. rules”. This part is the set of rules downloaded from Snort’s online resources. This specific one is Regular rules package by snort. This way we have uploaded the Regular set of rules into the configuration in Snort.

Next, we are telling it to read (“-r”) the next file of PCAPS which is the frioutside tcpdumb part. So now it runs those rules against the PCAP files given. Lastly it saves the logs (alerts) as shown by the -L command in the /var/log/snort depository. And that’s how we access the list of all alerts with their details.



To access the logs, you need to Cd into the Snort tab inside the log tab. Then access the file called “alert\_full.txt”. All Alerts will be logged there. If you are satisfied with the alerts, you must save them in a different file and clear the txt file so when you do the next test it is cleared and ready to take new alerts. Otherwise, it will add the new set of alerts on the bottom adding to the list not renewing it.

Suricata command line to run its service:



Using Suricata we can see that we start with Suricata as well. Then we specify the rules by using “-r” then followed by the rules set we downloaded on our device. Next, we specify some settings on where to save the logs and how to test the PCAP file. Lastly, we add the “-L” followed by the PCAP file downloaded.

Text

Description automatically generated

There are two main ways to view the logs with Suricata. The first one is to use the vi Suricata.log command. The other method is more complicated because it saves the alerts in Jason format thus resulting in a weird command line like “jq ‘.’ eve.json |less”. This command shows us the list of alerts of the just tested PCAP file in Jason format.

Text

Description automatically generated with medium confidence

The top command allows for people to look at the CPU and memory usage of any command or process Linux undergoes. Very useful to collect information.