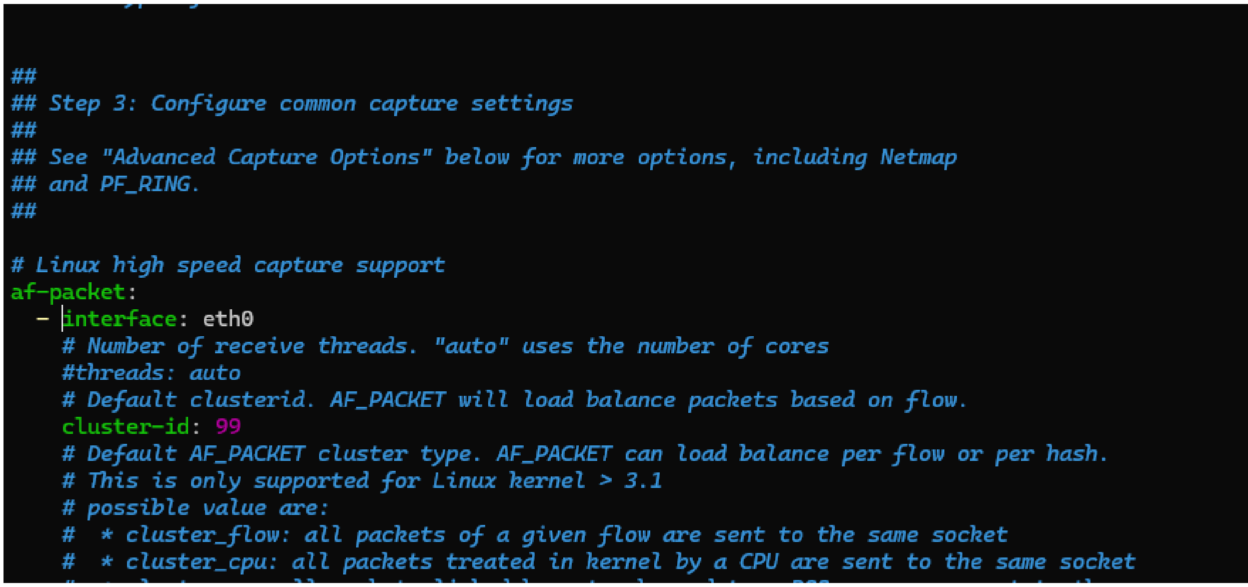
Ping flood and GPL attack with Suricata IDS

In this project, I used a RaspberryPi to install Suricata IDS and detect 2 network attacks.

STEPS

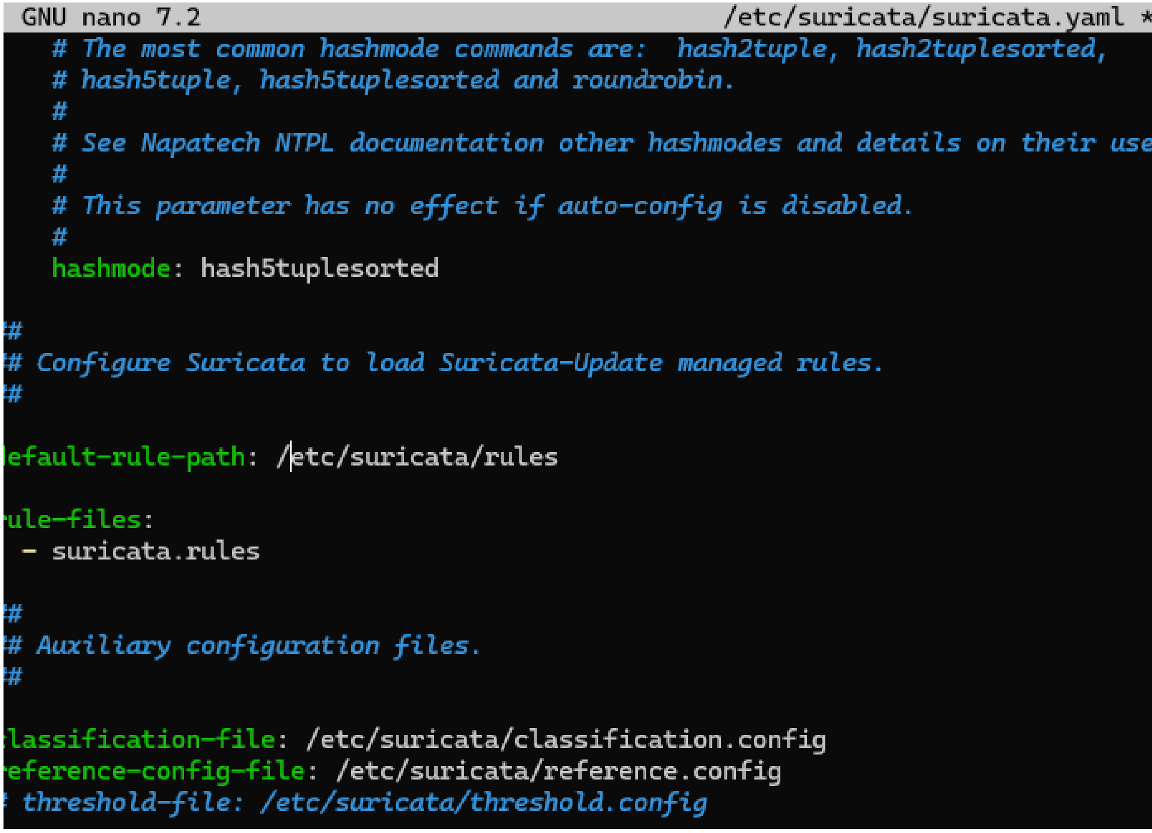
1. **On the raspberry pi - type: ip a in terminal to get interface name**
1. **in terminal: sudo apt update && sudo apt upgrade -y**
2. **sudo apt install suricata -y**
3. **sudo systemctl enable --now suricata**
4. **sudo systemctl status suricata (should show active running)**
5. **sudo nano /etc/suricata/suricata.yaml**
    1. **scroll down and put in raspberry pi IP**
    2. **search: ctrl +W (to search) interface. Make sure it's eth0**



```
##
## Step 3: Configure common capture settings
##
## See "Advanced Capture Options" below for more options, including Netmap
## and PF_RING.
##

# Linux high speed capture support
af-packet:
  - interface: eth0
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
    # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
    # This is only supported for Linux kernel > 3.1
    # possible value are:
    #  * cluster_flow: all packets of a given flow are sent to the same socket
    #  * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
```

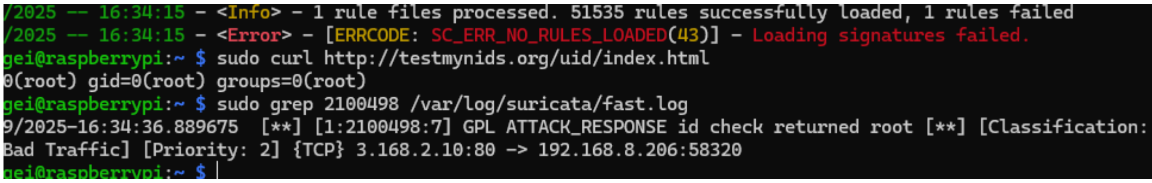
    3. **ctrl + W. default-rule-path**

1. make sure it shows etc/suricata/rules



```
 GNU nano 7.2                                    /etc/suricata/suricata.yaml *
   # The most common hashmode commands are:  hash2tuple, hash2tuplesorted,
   # hash5tuple, hash5tuplesorted and roundrobin.
   #
   # See Napatech NTPL documentation other hashmodes and details on their use
   #
   # This parameter has no effect if auto-config is disabled.
   #
   hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

lefault-rule-path: /etc/suricata/rules

ule-files:
 - suricata.rules

##
## Auxiliary configuration files.
##

lassification-file: /etc/suricata/classification.config
eference-config-file: /etc/suricata/reference.config
 threshold-file: /etc/suricata/threshold.config
```

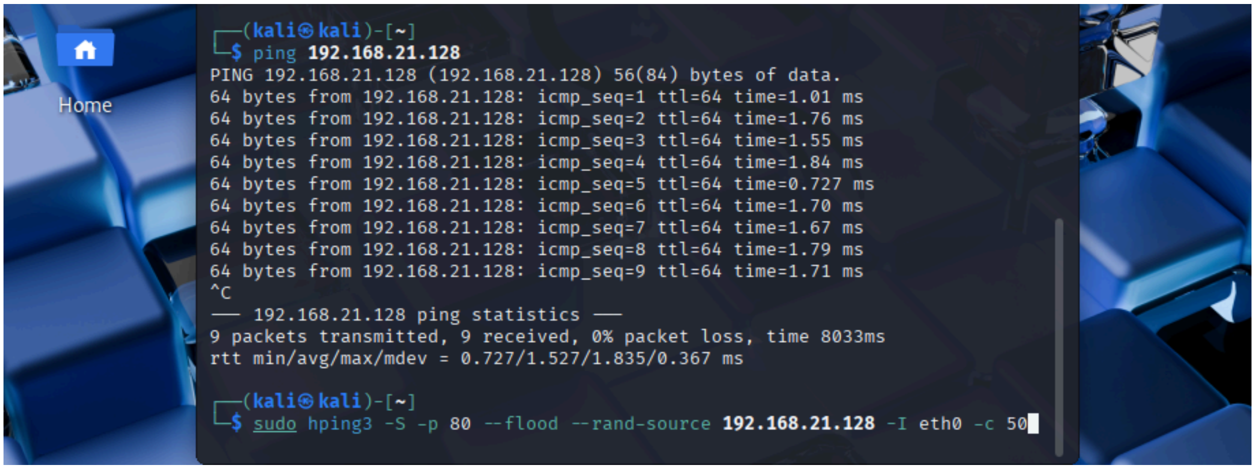
2. ctrl + o, enter ctrl +x
3. sudo systemctl restart suricata
4. sudo ip link set eth0 promisc on
5. or type: ifconig eth0 promisc
6. sudo suricata-update update-sources (updates source indexes)
7. sudo suricata-update -o /etc/suricata/rules
8. sudo systemctl restart suricata
9. sudo suricata -T -c /etc/suricata/suricata.yaml -v (tests configuration)
10. sudo curl http://testmynids.org/uid/index.html
11. sudo grep 2100498 /var/log/suricata/fast.log (tests for GPL attack)



```
/2025 -- 16:34:15 - <Info> - 1 rule files processed. 51535 rules successfully loaded, 1 rules failed
/2025 -- 16:34:15 - <Error> - [ERRCODE: SC_ERR_NO_RULES_LOADED(43)] - Loading signatures failed.
gei@raspberrypi:~ $ sudo curl http://testmynids.org/uid/index.html
0(root) gid=0(root) groups=0(root)
gei@raspberrypi:~ $ sudo grep 2100498 /var/log/suricata/fast.log
9/2025-16:34:36.889675  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification:
Bad Traffic] [Priority: 2] {TCP} 3.168.2.10:80 -> 192.168.8.206:58320
gei@raspberrypi:~ $
```

12. To update suricata rules. Sudo suricata-update list-sources. Copy the names of the rules by MIT or GPL. The commercial ones have paid subscriptions.
13. Sudo suricata-update enable-source “name of the rule”
14. tail-f /var/log/suricata/fast.log
15. Another machine: hping3

16. **sudo apt install hping3 -y**
17. **sudo hping3 -S -p 80 --flood --rand-source 192.168.8.206 -I eth0 -c 50**



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.21.128
PING 192.168.21.128 (192.168.21.128) 56(84) bytes of data.
64 bytes from 192.168.21.128: icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from 192.168.21.128: icmp_seq=2 ttl=64 time=1.76 ms
64 bytes from 192.168.21.128: icmp_seq=3 ttl=64 time=1.55 ms
64 bytes from 192.168.21.128: icmp_seq=4 ttl=64 time=1.84 ms
64 bytes from 192.168.21.128: icmp_seq=5 ttl=64 time=0.727 ms
64 bytes from 192.168.21.128: icmp_seq=6 ttl=64 time=1.70 ms
64 bytes from 192.168.21.128: icmp_seq=7 ttl=64 time=1.67 ms
64 bytes from 192.168.21.128: icmp_seq=8 ttl=64 time=1.79 ms
64 bytes from 192.168.21.128: icmp_seq=9 ttl=64 time=1.71 ms
^C
--- 192.168.21.128 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8033ms
rtt min/avg/max/mdev = 0.727/1.527/1.835/0.367 ms

┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S -p 80 --flood --rand-source 192.168.21.128 -I eth0 -c 50
```