PROJECT : Suricata on Ubuntu

Name : Vaishnavi Madhav Shinde

Roll No : MH-JM-24-07-0103

Course : Cyber Security Specialist

Guided By : Deepyesh Sir.

Suricata on Ubuntu

Suricata is an open-source network threat detection engine used for **intrusion detection (IDS), intrusion prevention (IPS), and network security monitoring (NSM)**. It performs **deep packet inspection, signaturebased detection, protocol parsing, and file extraction** while supporting high-speed multi-threaded processing. It integrates well with threat intelligence tools and logging systems like **ELK, Zeek, and Security Onion**. **Install Suricata using APT (Advanced Persistent Threat)**

>sudo apt update

>sudo apt upgrade

>sudo apt install -y suricata

>suricata -V

>sudo nano /etc/suricata/suricata.yaml

Change home network ip

```
  GNU nano 7.2                                  /etc/suricata/suricata.yaml
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.3.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "192.168.1.0/24"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"
```

>Community.id: true

```
    # enable/disable the community id feature.
    community-id: true
    # Seed value for the ID output. Valid values are 0-65535.
    community-id-seed: 0
```

packet change interface while looking at what is your ip address interface

```
# Linux high speed capture support
af-packet:
  - interface: enp0s3
    # 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
```

pcap

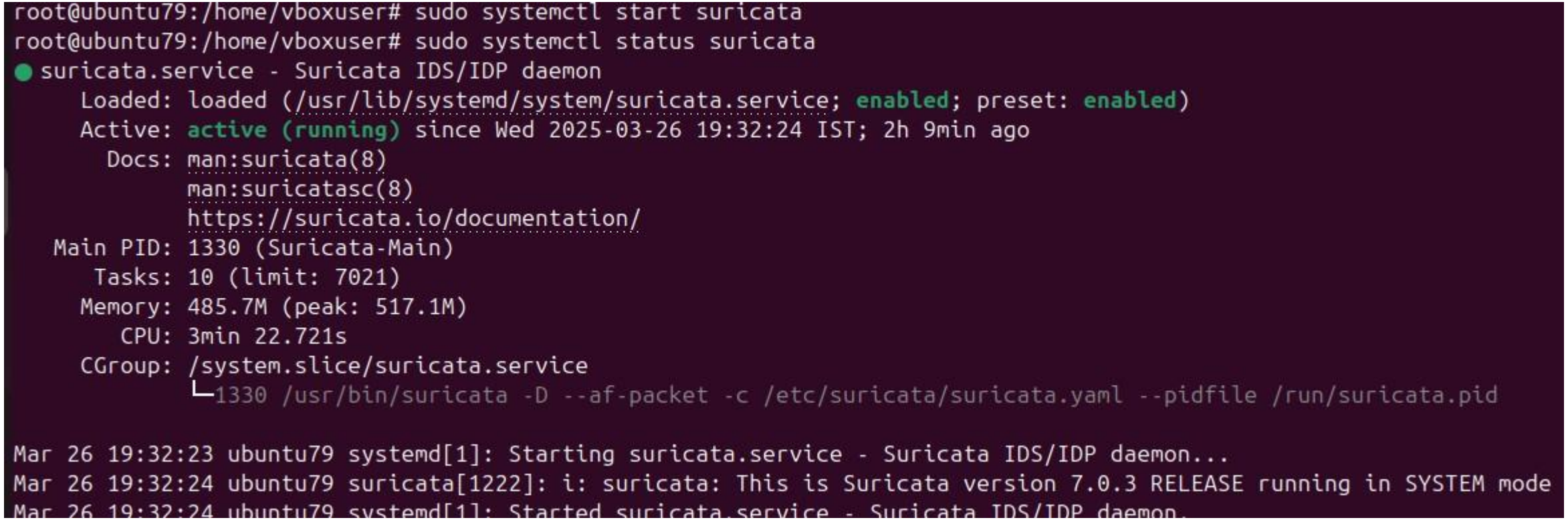
Start Suricata Enable the Suricata service using the systemctl command to run it in the background:

>sudo systemctl start suricata

To check if it is running correctly, run the following:

>sudo systemctl status suricata

```
# Cross platform libpcap capture support
pcap:
  - interface: enp0s3
    # On Linux, pcap will try to use mmap'ed capture and will use "buffer-size"
    # as total memory used by the ring. So set this to something bigger
```



Test Suricata

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

```
root@ubuntu79:/home/vboxuser# sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 42485 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 42488 signatures processed. 1289 are IP-only rules, 4333 are inspecting packet payload, 36651 inspect appl
ication layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```

>curl http://testmynids.org/uid/index.html

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

```
root@ubuntu79:/home/vboxuser# curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu79:/home/vboxuser# tail -f /var/log/suricata/fast.log
03/26/2025-21:35:03.434632  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic P
rotocol Command Decode] [Priority: 3] {TCP} 172.67.157.37:443 -> 192.168.1.12:46824
03/26/2025-21:35:42.721987  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic P
rotocol Command Decode] [Priority: 3] {TCP} 31.13.79.53:443 -> 192.168.1.7:65387
03/26/2025-21:36:46.333386  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic P
rotocol Command Decode] [Priority: 3] {TCP} 172.67.157.37:443 -> 192.168.1.12:46638
03/26/2025-21:38:18.927745  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic P
rotocol Command Decode] [Priority: 3] {TCP} 172.67.157.37:443 -> 192.168.1.12:33180
03/26/2025-21:39:51.719027  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic P
rotocol Command Decode] [Priority: 3] {TCP} 104.21.40.220:443 -> 192.168.1.12:53114
03/26/2025-21:41:27.500773  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic P
```