Suricata installation walkthrough

What is suricata ?

Suricata is an open-source, high-performance network threat detection engine that functions as an intrusion detection system (IDS), intrusion prevention system (IPS), and network security monitoring (NSM) tool. Developed by the Open Information Security Foundation (OISF), it analyzes network traffic in real time, detecting malicious activities using deep packet inspection, signature-based detection, and anomaly analysis. Suricata supports multi-threading for high-speed processing and works with popular cybersecurity tools like Zeek, Elasticsearch, and Kibana, making it a powerful choice for threat intelligence and network security.

Installation of suricata

First I'll clear that it needs root privilege so I am on root user mode

we need to install necessary package management tools and add the official Suricata repository that is stable using this command:

apt-get install software-properties-common

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# apt-get install software-properties-common
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
software-properties-common is already the newest version (0.99.49.1).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

After that this command :

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

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# add-apt-repository ppa:oisf/suricata-stable
Repository: 'Types: deb
URIs: https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/
Suites: noble
Components: main
'
Description:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and
Network Security Monitoring engine.
```

Press **Enter** to continue

```
More info: https://launchpad.net/~oisf/+archive/ubuntu/suricata-stable
Adding repository.
Press [ENTER] to continue or Ctrl-c to cancel.
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:2 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble InRelease [18.1 kB]
Hit:3 http://in.archive.ubuntu.com/ubuntu noble InRelease
```

We also need to update the package lists and fetch the latest information about available packages by executing by this command:

apt update

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:5 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
```

Finally we can install Suricata by running this command:

apt install suricata jq

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# sudo apt install suricata jq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
jq is already the newest version (1.7.1-3build1).
jq set to manually installed.
The following additional packages will be installed:
  isa-support libevent-2.1-7t64 libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 libhiredis1.1.0
  libhtp2 libhyperscan5 libluajit-5.1-2 libluajit-5.1-common liblzma-dev libnet1
```

you will be prompted to continue then type **Y** or you can directly press **Enter** button.

```
After this operation, 29.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble/main amd64 libhtp2 amd64 1:
0.5.50-0ubuntu0 [72.5 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 isa-support amd64 21build1 [16.7 kB]
Get:3 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble/main amd64 suricata amd64 1
:7.0.10-0ubuntu0 [3,136 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 sse3-support amd64 21build1 [3,406 B]
Get:5 http://in.archive.ubuntu.com/ubuntu noble/main amd64 libevent-2.1-7t64 amd64 2.1.12-stable-9ub
```

After installing Suricata, we can check which version of Suricata we have running and with what options, as well as the service state by running this command:

suricata –build-info

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# suricata --build-info
This is Suricata version 7.0.10 RELEASE
Features: NFQ PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP_URI_NORMALIZE_
HOOK PCRE_JIT HAVE_NSS HTTP2_DECOMPRESSION HAVE_LUA HAVE_JA3 HAVE_JA4 HAVE_LUAJIT HAVE_LIBJANSSON TL
S TLS_C11 MAGIC RUST POPCNT64
SIMD support: SSE_2
Atomic intrinsics: 1 2 4 8 byte(s)
64-bits, Little-endian architecture
GCC version 13.3.0, C version 201112
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: _Thread_local
compiled with LibHTP v0.5.50, linked against LibHTP v0.5.50
```

Now we have to check suricata status is active or not if inactive then our suricata can’t work.

Using this command we can check :

systemctl status suricata

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# systemctl status suricata
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (exited) since Wed 2025-04-02 18:16:37 IST; 58s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 29921 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
        CPU: 126ms

Apr 02 18:16:37 gopal-VMware-Virtual-Platform systemd[1]: Starting suricata.service - LSB: Next Gen>
Apr 02 18:16:37 gopal-VMware-Virtual-Platform suricata[29921]: Starting suricata in IDS (af-packet)>
Apr 02 18:16:37 gopal-VMware-Virtual-Platform systemd[1]: Started suricata.service - LSB: Next Gene>
```

Now we have to check ip address and interface id we can check using this command:

ip a / ip addr

In my case my interface id is **ens33** and ip address is **192.168.155.213**

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:d1:b7:18 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.155.213/24 brd 192.168.155.255 scope global dynamic noprefixroute ens33
       valid_lft 3209sec preferred_lft 3209sec
    inet6 2401:4900:57ae:16e5:a908:6522:e801:8b5a/64 scope global temporary dynamic
       valid_lft 6955sec preferred_lft 6955sec
    inet6 2401:4900:57ae:16e5:20c:29ff:fed1:b718/64 scope global dynamic mngtmpaddr
       valid_lft 6955sec preferred_lft 6955sec
    inet6 fe80::20c:29ff:fed1:b718/64 scope link
       valid_lft forever preferred_lft forever
```

Now we have to edit suricata.yaml file by running this command:

nano /etc/suricata/suricata.yaml

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# nano /etc/suricata/suricata.yaml
```

Add network to HOME_NET 192.168.155.0/24 network subnet

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.155.0/24,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
```

Change community-id to **true**

```
    # Takes a 'seed' that needs to be same across sensors and tools
    # to make the id less predictable.

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

    # HTTP X-Forwarded-For support by adding an extra field or overwriting
    # the source or destination IP address (depending on flow direction)
    # with the one reported in the X-Forwarded-For HTTP header. This is
    # helpful when reviewing alerts for traffic that is being reverse
    # or forward proxied.
    xff:
```

Add the interface **ens33** at capture support section in interface.

```
# Linux high speed capture support
af-packet:
  - interface: ens33
    # 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
```

Save changes using "**ctrl + x**" to exit the editor and "**Y**" to save modified changes and press enter.

Next update suricata using this command for applying latest predefined rules:

Suricata-update

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# suricata-update
2/4/2025 -- 18:22:22 - <Info> -- Using data-directory /var/lib/suricata.
2/4/2025 -- 18:22:22 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
2/4/2025 -- 18:22:22 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
2/4/2025 -- 18:22:22 - <Info> -- Found Suricata version 7.0.10 at /usr/bin/suricata.
2/4/2025 -- 18:22:22 - <Info> -- Loading /etc/suricata/suricata.yaml
2/4/2025 -- 18:22:22 - <Info> -- Disabling rules for protocol pgsql
2/4/2025 -- 18:22:22 - <Info> -- Disabling rules for protocol modbus
2/4/2025 -- 18:22:22 - <Info> -- Disabling rules for protocol dnp3
2/4/2025 -- 18:22:22 - <Info> -- Disabling rules for protocol enip
2/4/2025 -- 18:22:22 - <Info> -- No sources configured, will use Emerging Threats Open
```

To view logs in realtime we can run Suricata in live mode with the network interface ens33.

By running this command :

suricata -c /etc/suricata/suricata.yaml -i ens33

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# suricata -c /etc/suricata/suricata.yaml -i e
ns33
i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
W: af-packet: ens33: AF_PACKET tpacket-v3 is recommended for non-inline operation
i: threads: Threads created -> W: 2 FM: 1 FR: 1   Engine started.
^Ci: suricata: Signal Received.  Stopping engine.
i: device: ens33: packets: 6153, drops: 0 (0.00%), invalid chksum: 0
```

We can also add custom rules in the **suricata.rules** file located at **/var/lib/suricata** .

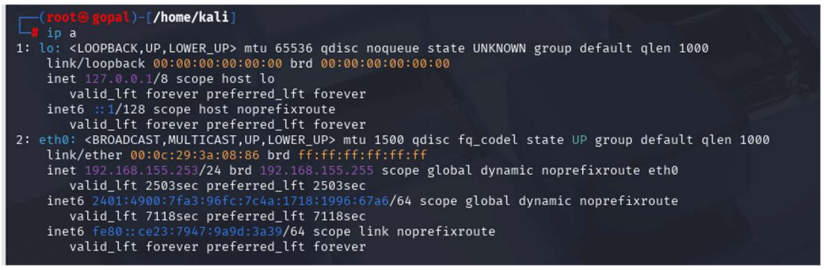
Verify that traffic is being captured by running this command:

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

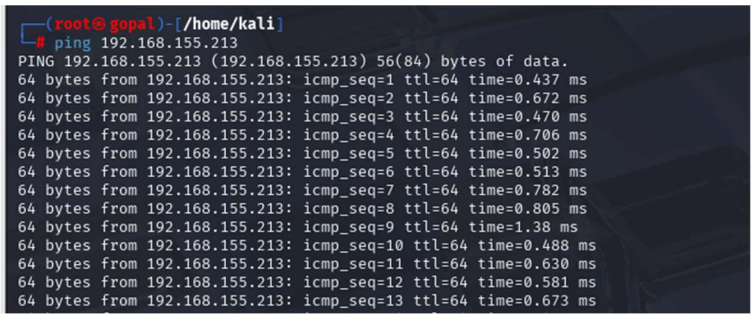
```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# tail -f /var/log/suricata/fast.log
04/02/2025-18:25:32.349435  [**] [1:2027397:1] ET INFO Spotify P2P Client [**] [Classification: Not
Suspicious Traffic] [Priority: 3] {UDP} 192.168.155.6:57621 -> 192.168.155.255:57621
```

```
root@gopal-VMware-Virtual-Platform:/home/gopal/Desktop# tail -f /var/log/suricata/fast.log
04/02/2025-18:25:32.349435  [**] [1:2027397:1] ET INFO Spotify P2P Client [**] [Classification: Not
Suspicious Traffic] [Priority: 3] {UDP} 192.168.155.6:57621 -> 192.168.155.255:57621
04/02/2025-18:39:32.536766  [**] [1:2027397:1] ET INFO Spotify P2P Client [**] [Classification: Not
Suspicious Traffic] [Priority: 3] {UDP} 192.168.155.6:57621 -> 192.168.155.255:57621
04/02/2025-18:41:58.894004  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Ge
neric Protocol Command Decode] [Priority: 3] {ICMP} 192.168.155.253:8 -> 192.168.155.213:9
04/02/2025-18:41:58.896795  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Ge
neric Protocol Command Decode] [Priority: 3] {ICMP} 192.168.155.213:0 -> 192.168.155.253:9
04/02/2025-18:42:00.027107  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Ge
neric Protocol Command Decode] [Priority: 3] {ICMP} 192.168.155.253:8 -> 192.168.155.213:9
04/02/2025-18:42:00.027153  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Ge
neric Protocol Command Decode] [Priority: 3] {ICMP} 192.168.155.213:0 -> 192.168.155.253:9
```

From kali I trying ping and nmap scan for that I am adding my kali ip.

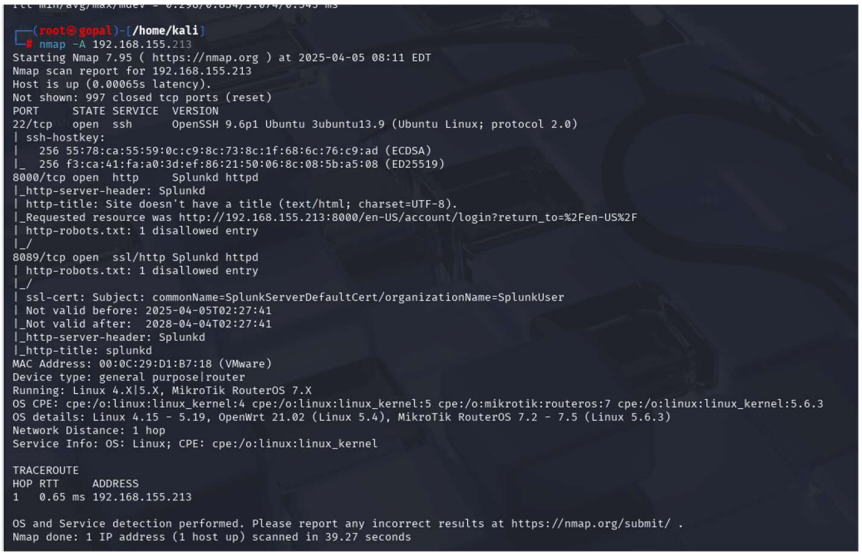


From ping kali to ubantu logs show like this




```
04/05/2025-17:42:25.324318  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Generic Protocol Comma
nd Decode] [Priority: 3] {ICMP} 192.168.155.253:8 -> 192.168.155.213:9
04/05/2025-17:42:25.324353  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Generic Protocol Comma
nd Decode] [Priority: 3] {ICMP} 192.168.155.213:0 -> 192.168.155.253:9
04/05/2025-17:42:25.324320  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Generic Protocol Comma
nd Decode] [Priority: 3] {ICMP} 192.168.155.253:8 -> 192.168.155.213:9
04/05/2025-17:42:25.324354  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Generic Protocol Comma
nd Decode] [Priority: 3] {ICMP} 192.168.155.213:0 -> 192.168.155.253:9
```

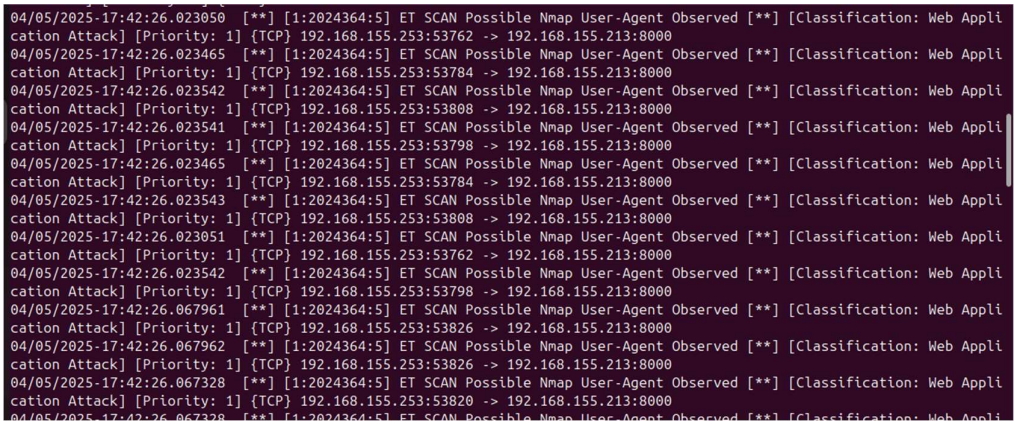
Now I tried nmap scan and also logs crete like this



```
┌──(root㉿gopal)-[/home/kali]
└─# nmap -A 192.168.155.213
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 08:11 EDT
Nmap scan report for 192.168.155.213
Host is up (0.00065s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 55:78:ca:55:59:0c:c9:8c:73:8c:1f:68:6c:76:c9:ad (ECDSA)
|_  256 f3:ca:41:fa:a0:3d:ef:86:21:50:06:8c:08:5b:a5:08 (ED25519)
8000/tcp open  http     Splunkd httpd
|_http-server-header: Splunkd
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was http://192.168.155.213:8000/en-US/account/login?return_to=%2Fen-US%2F
| http-robots.txt: 1 disallowed entry
|_/
8089/tcp open  ssl/http Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2025-04-05T02:27:41
|_Not valid after:  2028-04-04T02:27:41
|_http-server-header: Splunkd
|_http-title: splunkd
MAC Address: 00:0C:29:D1:B7:18 (VMware)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 192.168.155.213

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.27 seconds
```



```
04/05/2025-17:42:26.023050  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53762 -> 192.168.155.213:8000
04/05/2025-17:42:26.023465  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53784 -> 192.168.155.213:8000
04/05/2025-17:42:26.023542  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53808 -> 192.168.155.213:8000
04/05/2025-17:42:26.023541  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53798 -> 192.168.155.213:8000
04/05/2025-17:42:26.023465  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53784 -> 192.168.155.213:8000
04/05/2025-17:42:26.023543  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53808 -> 192.168.155.213:8000
04/05/2025-17:42:26.023051  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53762 -> 192.168.155.213:8000
04/05/2025-17:42:26.023542  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53798 -> 192.168.155.213:8000
04/05/2025-17:42:26.067961  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53826 -> 192.168.155.213:8000
04/05/2025-17:42:26.067962  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53826 -> 192.168.155.213:8000
04/05/2025-17:42:26.067328  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Appli
cation Attack] [Priority: 1] {TCP} 192.168.155.253:53820 -> 192.168.155.213:8000
```

Conclusion : After successfully installation Suricata and making the necessary configuration, the system is now capable of capturing and displaying logs in real time. This confirms that Suricata is actively monitoring network traffic and detecting potential threats. Regular rule updates and log analysis will help maintain its effectiveness in identifying suspicious activities.