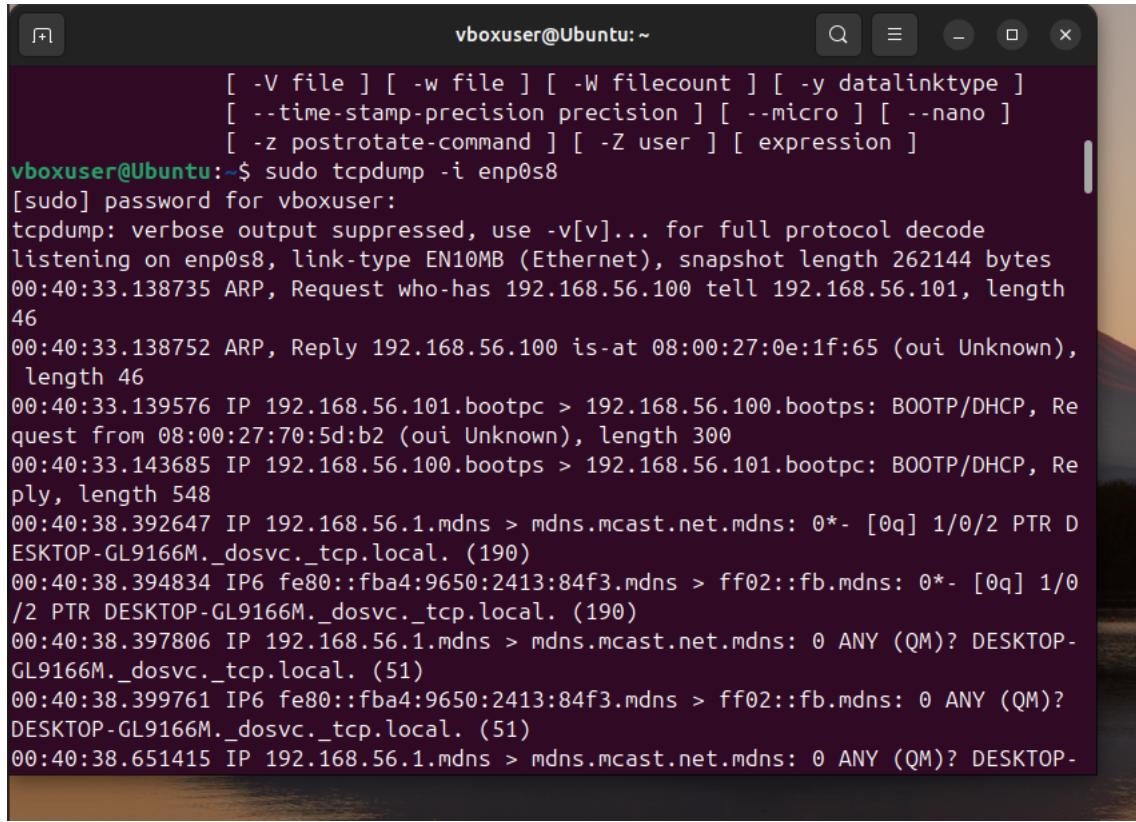


Sensor VM:

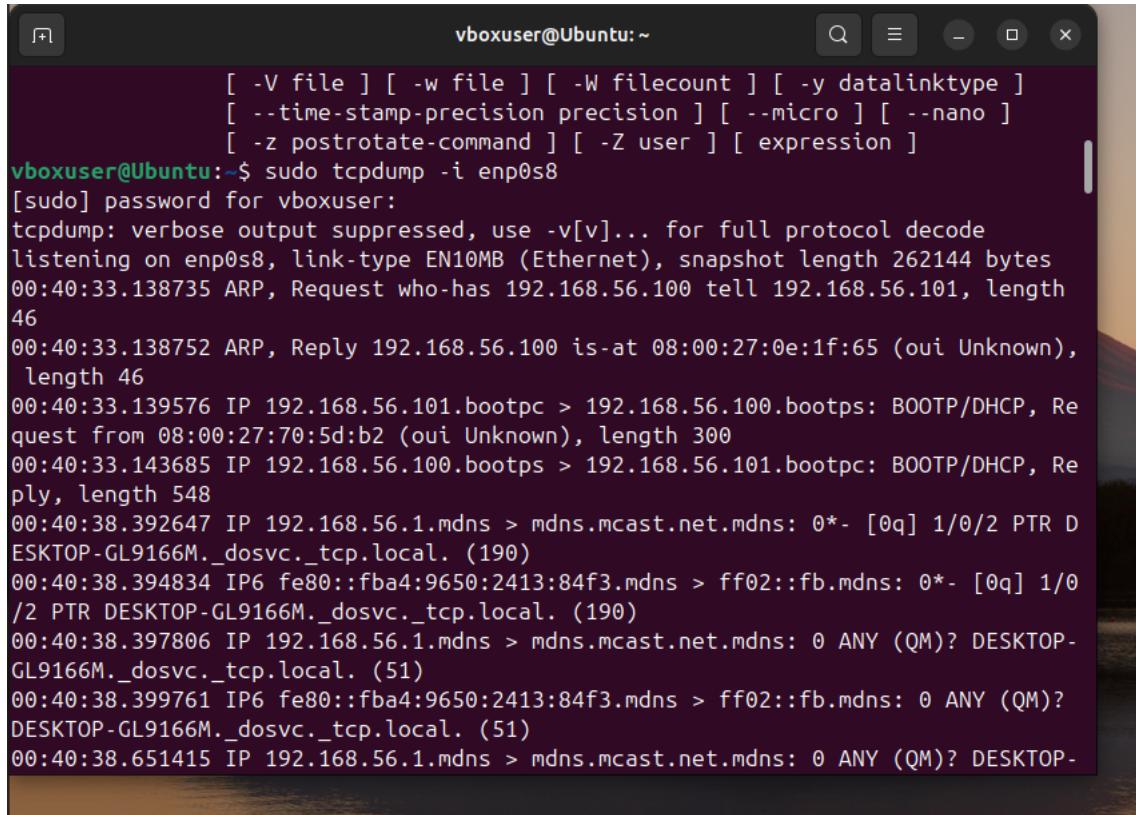
Setup the VMs to mirror traffic and sniffed on the Sensor VM:



```
vboxuser@Ubuntu:~
```

```
[ -V file ] [ -w file ] [ -W filecount ] [ -y datalinktype ]
[ --time-stamp-precision precision ] [ --micro ] [ --nano ]
[ -z postrotate-command ] [ -Z user ] [ expression ]
vboxuser@Ubuntu:~$ sudo tcpdump -i enp0s8
[sudo] password for vboxuser:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
00:40:33.138735 ARP, Request who-has 192.168.56.100 tell 192.168.56.101, length
46
00:40:33.138752 ARP, Reply 192.168.56.100 is-at 08:00:27:0e:1f:65 (oui Unknown),
length 46
00:40:33.139576 IP 192.168.56.101.bootpc > 192.168.56.100.bootps: BOOTP/DHCP, Re
quest from 08:00:27:70:5d:b2 (oui Unknown), length 300
00:40:33.143685 IP 192.168.56.100.bootps > 192.168.56.101.bootpc: BOOTP/DHCP, Re
ply, length 548
00:40:38.392647 IP 192.168.56.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/2 PTR D
ESKTOP-GL9166M._dosvc._tcp.local. (190)
00:40:38.394834 IP6 fe80::fba4:9650:2413:84f3.mdns > ff02::fb.mdns: 0*- [0q] 1/0
/2 PTR DESKTOP-GL9166M._dosvc._tcp.local. (190)
00:40:38.397806 IP 192.168.56.1.mdns > mdns.mcast.net.mdns: 0 ANY (QM)? DESKTOP-
GL9166M._dosvc._tcp.local. (51)
00:40:38.399761 IP6 fe80::fba4:9650:2413:84f3.mdns > ff02::fb.mdns: 0 ANY (QM)?
DESKTOP-GL9166M._dosvc._tcp.local. (51)
00:40:38.651415 IP 192.168.56.1.mdns > mdns.mcast.net.mdns: 0 ANY (QM)? DESKTOP-
```

The tcp dump shows communication between the attacker and the target as shown below:

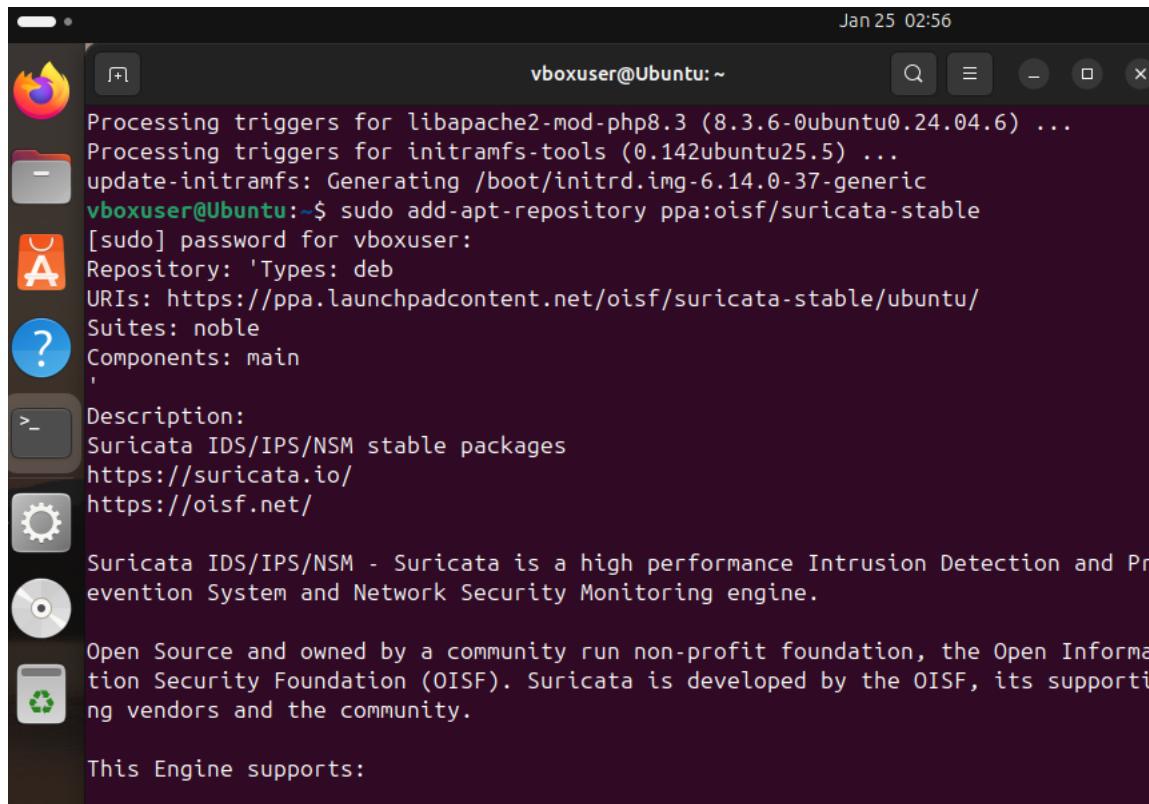


```
vboxuser@Ubuntu:~
```

```
[ -V file ] [ -w file ] [ -W filecount ] [ -y datalinktype ]
[ --time-stamp-precision precision ] [ --micro ] [ --nano ]
[ -z postrotate-command ] [ -Z user ] [ expression ]
vboxuser@Ubuntu:~$ sudo tcpdump -i enp0s8
[sudo] password for vboxuser:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
00:40:33.138735 ARP, Request who-has 192.168.56.100 tell 192.168.56.101, length
46
00:40:33.138752 ARP, Reply 192.168.56.100 is-at 08:00:27:0e:1f:65 (oui Unknown),
length 46
00:40:33.139576 IP 192.168.56.101.bootpc > 192.168.56.100.bootps: BOOTP/DHCP, Re
quest from 08:00:27:70:5d:b2 (oui Unknown), length 300
00:40:33.143685 IP 192.168.56.100.bootps > 192.168.56.101.bootpc: BOOTP/DHCP, Re
ply, length 548
00:40:38.392647 IP 192.168.56.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/2 PTR D
ESKTOP-GL9166M._dosvc._tcp.local. (190)
00:40:38.394834 IP6 fe80::fba4:9650:2413:84f3.mdns > ff02::fb.mdns: 0*- [0q] 1/0
/2 PTR DESKTOP-GL9166M._dosvc._tcp.local. (190)
00:40:38.397806 IP 192.168.56.1.mdns > mdns.mcast.net.mdns: 0 ANY (QM)? DESKTOP-
GL9166M._dosvc._tcp.local. (51)
00:40:38.399761 IP6 fe80::fba4:9650:2413:84f3.mdns > ff02::fb.mdns: 0 ANY (QM)?
DESKTOP-GL9166M._dosvc._tcp.local. (51)
00:40:38.651415 IP 192.168.56.1.mdns > mdns.mcast.net.mdns: 0 ANY (QM)? DESKTOP-
```

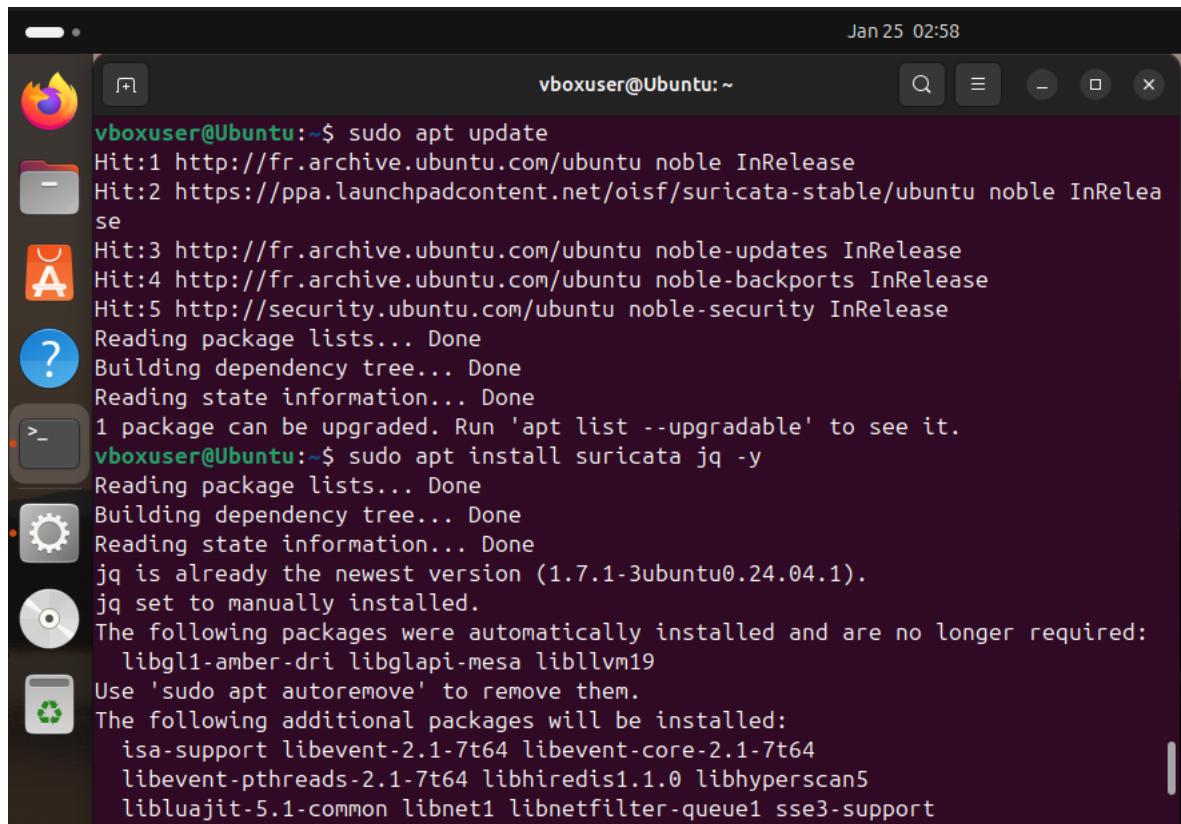
Now install Suricata.

Add suricata to the apt repo



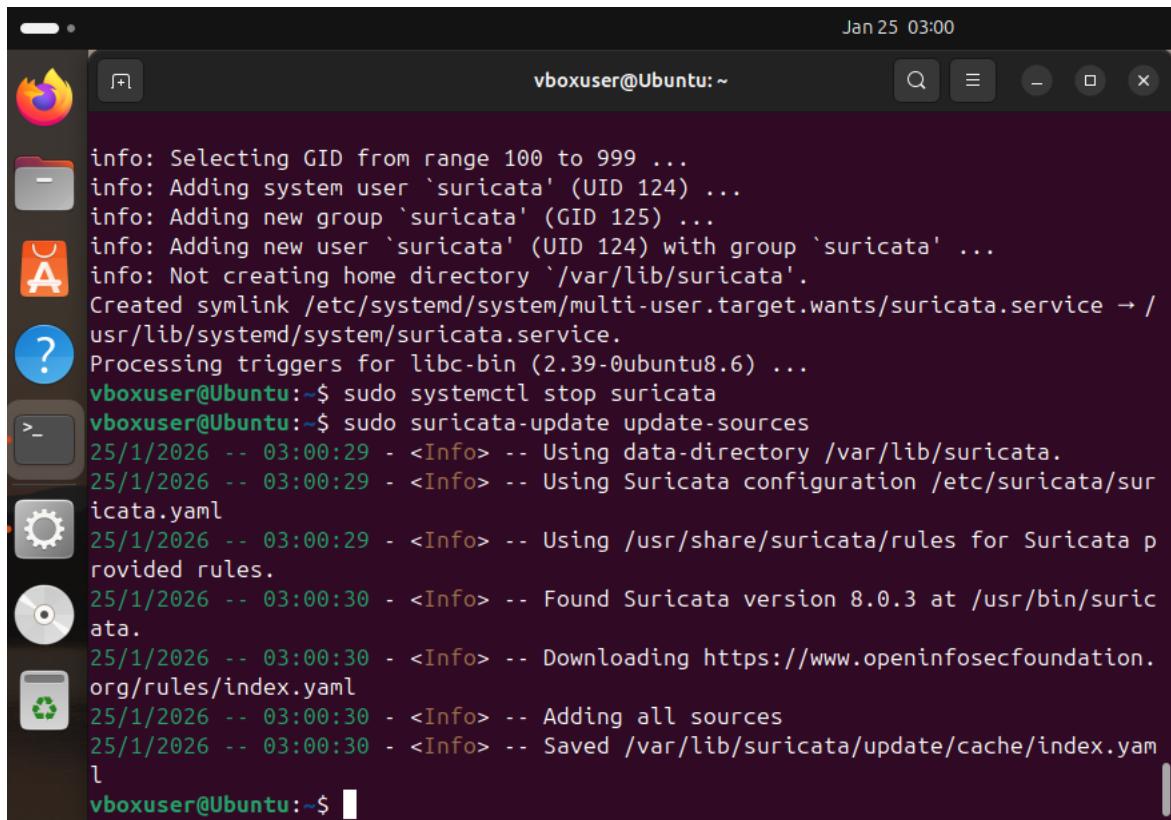
```
vboxuser@Ubuntu:~$ sudo add-apt-repository ppa:oisf/suricata-stable
[sudo] password for vboxuser:
Repository: 'Types: deb
URIs: https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/
Suites: noble
Components: main
'
Description:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/
Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.
Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the community.
This Engine supports:
```

Update apt and install suricata using apt



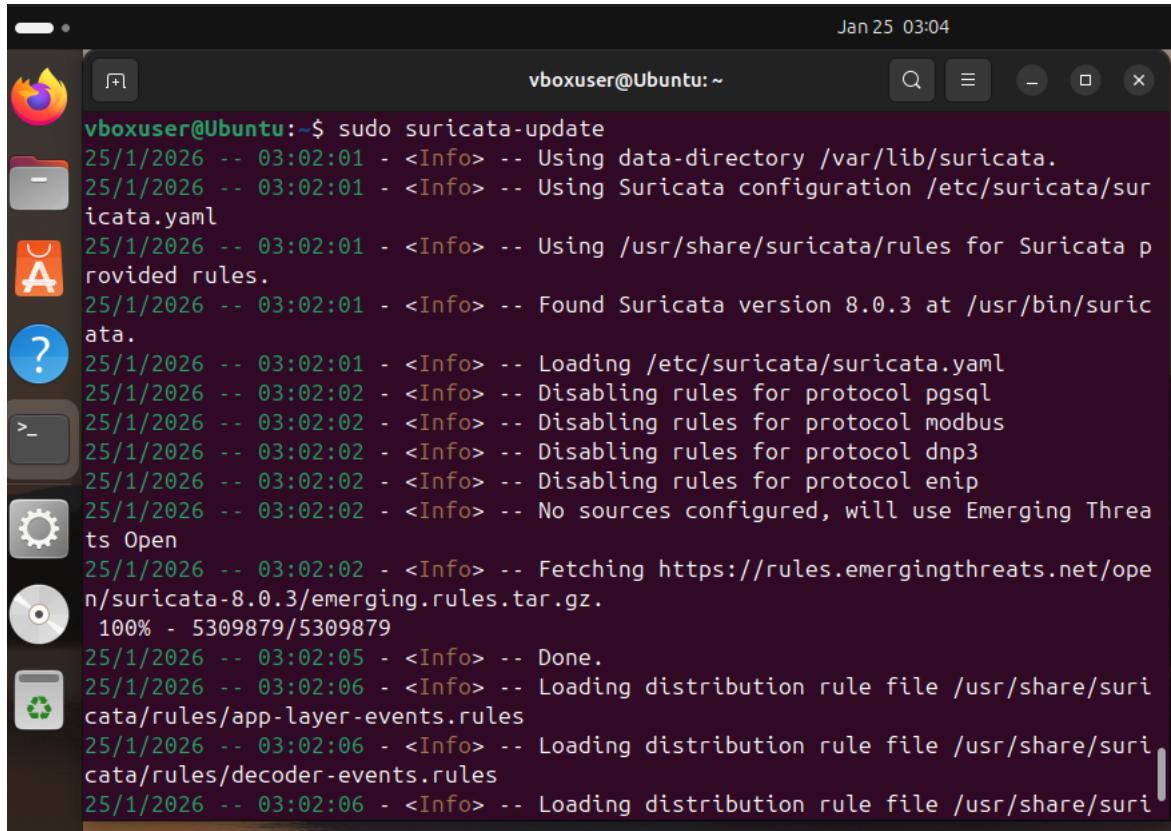
```
vboxuser@Ubuntu:~$ sudo apt update
Hit:1 http://fr.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble InRelease
Hit:3 http://fr.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://fr.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:5 http://security.ubuntu.com/ubuntu noble-security 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.
vboxuser@Ubuntu:~$ sudo apt install suricata jq -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
jq is already the newest version (1.7.1-3ubuntu0.24.04.1).
jq set to manually installed.
The following packages were automatically installed and are no longer required:
  libgl1-amber-dri libglapi-mesa liblllvm19
Use 'sudo apt autoremove' to remove them.
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 libhyperscan5
  libluajit-5.1-common libnet1 libnetfilter-queue1 sse3-support
```

Stop suricata in order to setup configurations. Then update the rule sources:



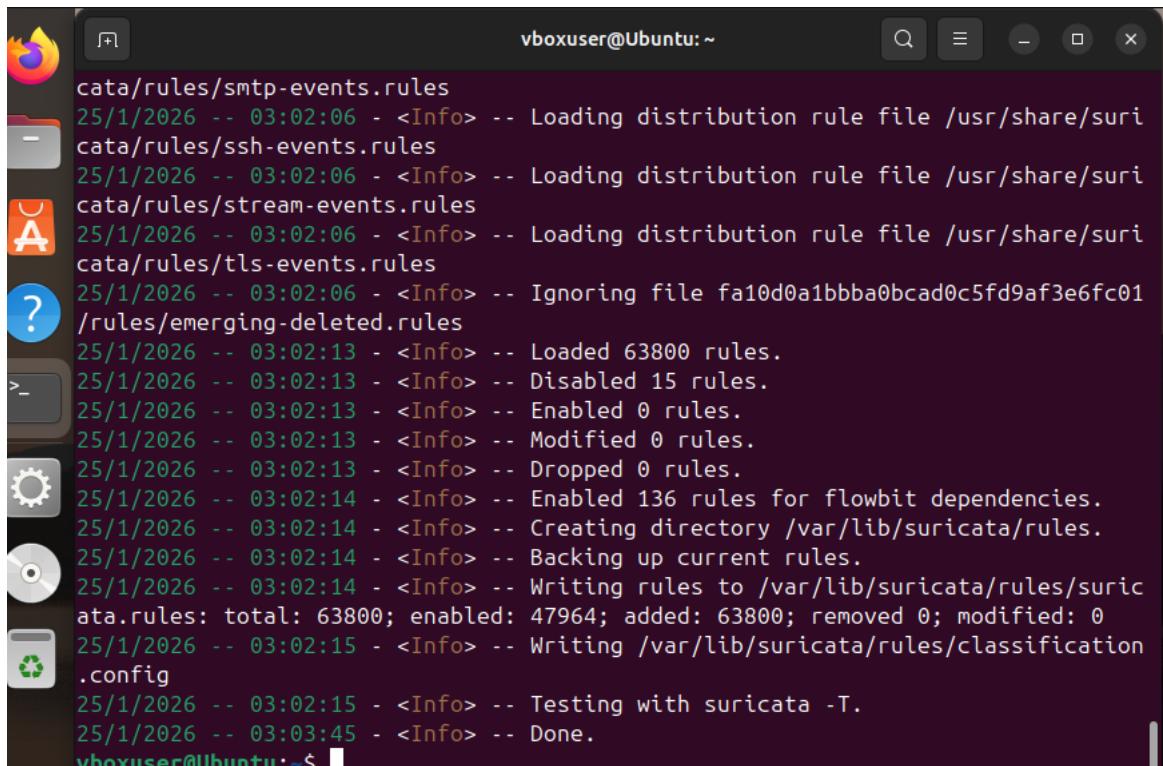
```
Jan 25 03:00
vboxuser@Ubuntu:~ info: Selecting GID from range 100 to 999 ...
info: Adding system user `suricata' (UID 124) ...
info: Adding new group `suricata' (GID 125) ...
info: Adding new user `suricata' (UID 124) with group `suricata' ...
info: Not creating home directory `/var/lib/suricata'.
Created symlink /etc/systemd/system/multi-user.target.wants/suricata.service → /usr/lib/systemd/system/suricata.service.
Processing triggers for libc-bin (2.39-0ubuntu8.6) ...
vboxuser@Ubuntu:~$ sudo systemctl stop suricata
vboxuser@Ubuntu:~$ sudo suricata-update update-sources
25/1/2026 -- 03:00:29 - <Info> -- Using data-directory /var/lib/suricata.
25/1/2026 -- 03:00:29 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
25/1/2026 -- 03:00:29 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
25/1/2026 -- 03:00:30 - <Info> -- Found Suricata version 8.0.3 at /usr/bin/suricata.
25/1/2026 -- 03:00:30 - <Info> -- Downloading https://www.openinfosecfoundation.org/rules/index.yaml
25/1/2026 -- 03:00:30 - <Info> -- Adding all sources
25/1/2026 -- 03:00:30 - <Info> -- Saved /var/lib/suricata/update/cache/index.yaml
vboxuser@Ubuntu:~$
```

Download the rules:



```
Jan 25 03:04
vboxuser@Ubuntu:~$ sudo suricata-update
25/1/2026 -- 03:02:01 - <Info> -- Using data-directory /var/lib/suricata.
25/1/2026 -- 03:02:01 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
25/1/2026 -- 03:02:01 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
25/1/2026 -- 03:02:01 - <Info> -- Found Suricata version 8.0.3 at /usr/bin/suricata.
25/1/2026 -- 03:02:01 - <Info> -- Loading /etc/suricata/suricata.yaml
25/1/2026 -- 03:02:02 - <Info> -- Disabling rules for protocol postgresql
25/1/2026 -- 03:02:02 - <Info> -- Disabling rules for protocol modbus
25/1/2026 -- 03:02:02 - <Info> -- Disabling rules for protocol dnp3
25/1/2026 -- 03:02:02 - <Info> -- Disabling rules for protocol enip
25/1/2026 -- 03:02:02 - <Info> -- No sources configured, will use Emerging Threats Open
25/1/2026 -- 03:02:02 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-8.0.3/emerging.rules.tar.gz.
100% - 5309879/5309879
25/1/2026 -- 03:02:05 - <Info> -- Done.
25/1/2026 -- 03:02:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/app-layer-events.rules
25/1/2026 -- 03:02:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/decoder-events.rules
25/1/2026 -- 03:02:06 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/encoder-events.rules
```

This includes the emerging rules set as shown here.



vboxuser@Ubuntu:~

```
cata/rules/smtp-events.rules
25/1/2026 -- 03:02:06 - <Info> -- Loading distribution rule file /usr/share/suri
cata/rules/ssh-events.rules
25/1/2026 -- 03:02:06 - <Info> -- Loading distribution rule file /usr/share/suri
cata/rules/stream-events.rules
25/1/2026 -- 03:02:06 - <Info> -- Loading distribution rule file /usr/share/suri
cata/rules/tls-events.rules
25/1/2026 -- 03:02:06 - <Info> -- Ignoring file fa10d0a1bbba0bcad0c5fd9af3e6fc01
/rules/emerging-deleted.rules
25/1/2026 -- 03:02:13 - <Info> -- Loaded 63800 rules.
25/1/2026 -- 03:02:13 - <Info> -- Disabled 15 rules.
25/1/2026 -- 03:02:13 - <Info> -- Enabled 0 rules.
25/1/2026 -- 03:02:13 - <Info> -- Modified 0 rules.
25/1/2026 -- 03:02:13 - <Info> -- Dropped 0 rules.
25/1/2026 -- 03:02:14 - <Info> -- Enabled 136 rules for flowbit dependencies.
25/1/2026 -- 03:02:14 - <Info> -- Creating directory /var/lib/suricata/rules.
25/1/2026 -- 03:02:14 - <Info> -- Backing up current rules.
25/1/2026 -- 03:02:14 - <Info> -- Writing rules to /var/lib/suricata/rules/suric
ata.rules: total: 63800; enabled: 47964; added: 63800; removed 0; modified: 0
25/1/2026 -- 03:02:15 - <Info> -- Writing /var/lib/suricata/rules/classification
.config
25/1/2026 -- 03:02:15 - <Info> -- Testing with suricata -T.
25/1/2026 -- 03:03:45 - <Info> -- Done.
```

vboxuser@Ubuntu:~\$

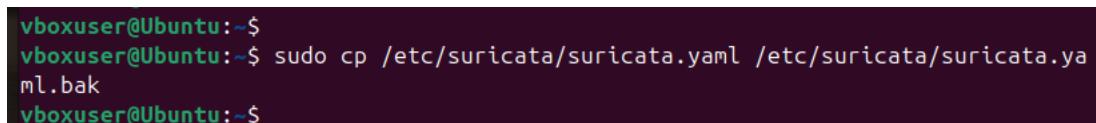
Network and routing configuration:

Enable ip forwarding and routing through suricata using nfqueue



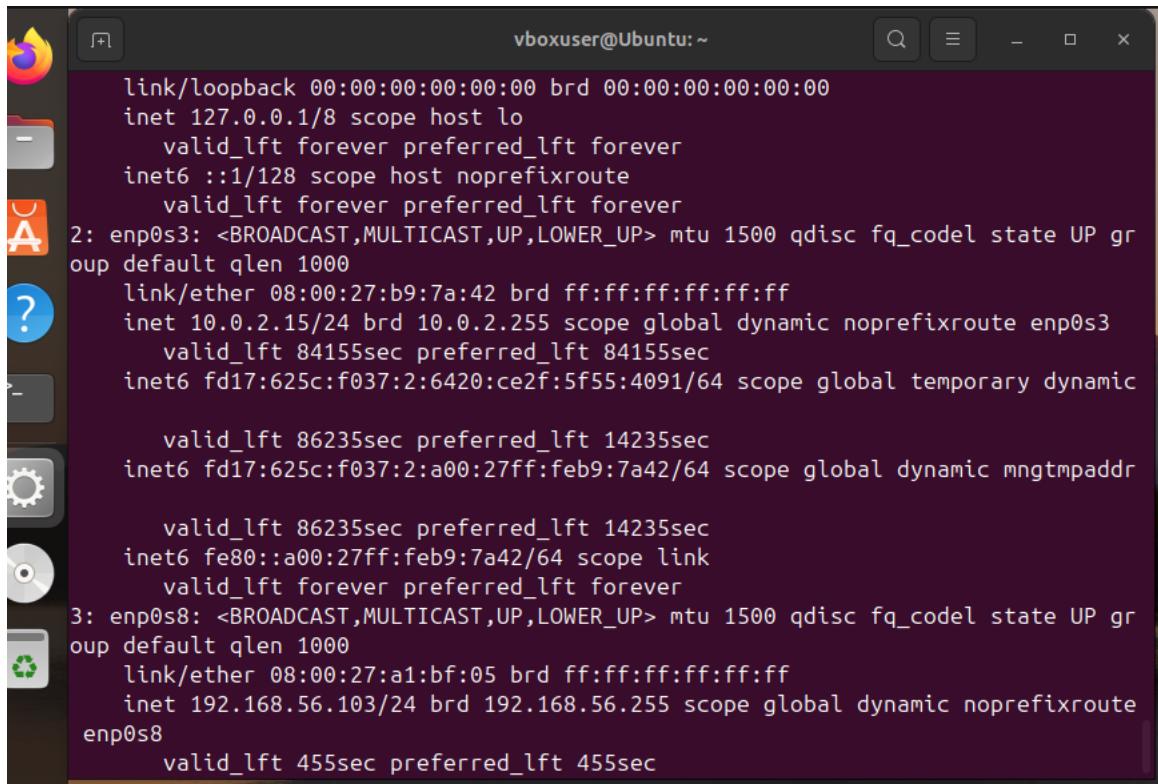
```
25/1/2026 -- 03:03:45 - <Info> -- Done.
vboxuser@Ubuntu:~$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for vboxuser:
net.ipv4.ip_forward = 1
vboxuser@Ubuntu:~$ echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf
net.ipv4.ip_forward=1
vboxuser@Ubuntu:~$ sudo iptables -I FORWARD -j NFQUEUE --queue-num 0
vboxuser@Ubuntu:~$
```

Backup current suricata config before editing



```
vboxuser@Ubuntu:~$ 
vboxuser@Ubuntu:~$ sudo cp /etc/suricata/suricata.yaml /etc/suricata/suricata.ya
ml.bak
vboxuser@Ubuntu:~$
```

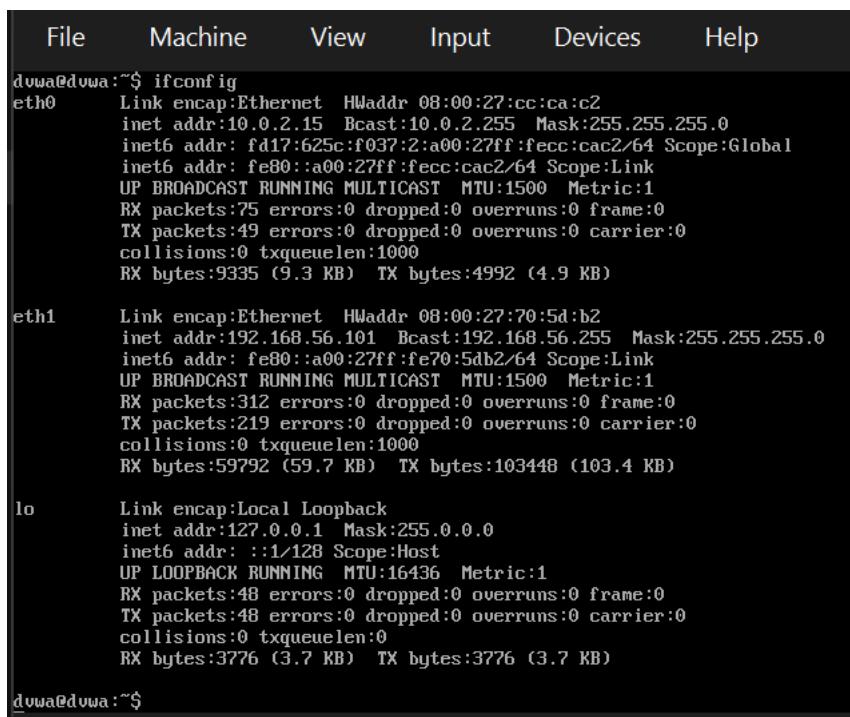
Sensor vm:



```
vboxuser@Ubuntu:~
```

```
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b9:7a:42 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 84155sec preferred_lft 84155sec
    inet6 fd17:625c:f037:2:6420:ce2f:5f55:4091/64 scope global temporary dynamic
        valid_lft 86235sec preferred_lft 14235sec
    inet6 fd17:625c:f037:2:a00:27ff:feb9:7a42/64 scope global dynamic mngtmpaddr
        valid_lft 86235sec preferred_lft 14235sec
    inet6 fe80::a00:27ff:feb9:7a42/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a1:bf:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s8
        valid_lft 455sec preferred_lft 455sec
```

Dvwa vm



```
File Machine View Input Devices Help
```

```
dvwa@dvwa:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:cc:ca:c2
          inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fd17:625c:f037:2:a00:27ff:fecc:cac2/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fecc:cac2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:75 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9335 (9.3 KB) TX bytes:4992 (4.9 KB)

eth1      Link encap:Ethernet HWaddr 08:00:27:70:5d:b2
          inet addr:192.168.56.101 Bcast:192.168.56.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe70:5db2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:312 errors:0 dropped:0 overruns:0 frame:0
          TX packets:219 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:59792 (59.7 KB) TX bytes:103448 (103.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3776 (3.7 KB) TX bytes:3776 (3.7 KB)

dvwa@dvwa:~$
```

Kali vm

```
kali㉿kali:[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      ether 08:00:27:30:21:e6  txqueuelen 1000  (Ethernet)
      RX packets 29  bytes 3190 (3.1 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 0  bytes 0 (0.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe29:2615  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:29:26:15  txqueuelen 1000  (Ethernet)
      RX packets 318  bytes 120730 (117.9 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 245  bytes 37072 (36.2 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop  txqueuelen 1000  (Local Loopback)
      RX packets 8  bytes 480 (480.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 8  bytes 480 (480.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Configure suricata:

Edit the suricata.yaml file to set the network subnet and the nfqueue details

```
vboxuser@Ubuntu:~$
vboxuser@Ubuntu:~$ sudo nano /etc/suricata/suricata.yaml
[sudo] password for vboxuser:
vboxuser@Ubuntu:~$
```

Endpoint traffic routing

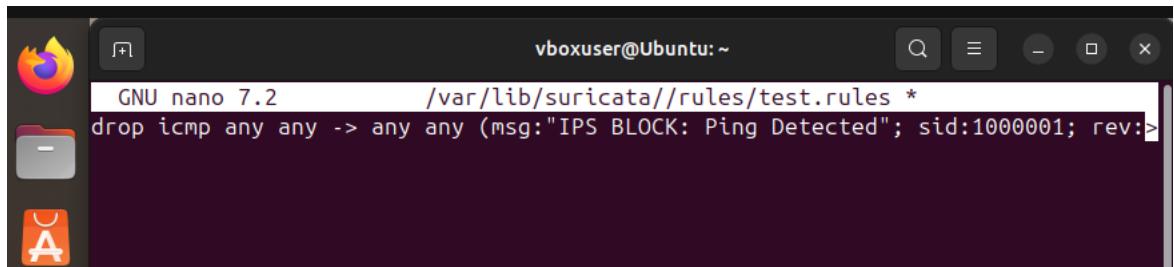
Route attacker traffic to target through the soc

```
(kali㉿kali)-[~]
$ sudo ip route add 192.168.56.101 via 192.168.56.103
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
(kali㉿kali)-[~]
```

Route target traffic to attacker through soc

```
sudo: 3 incorrect password attempts
dwua@dwua:~$ sudo ip route add 192.168.56.102 via 192.168.56.103
[sudo] password for dwua:
Sorry, try again.
[sudo] password for dwua:
dwua@dwua:~$
```

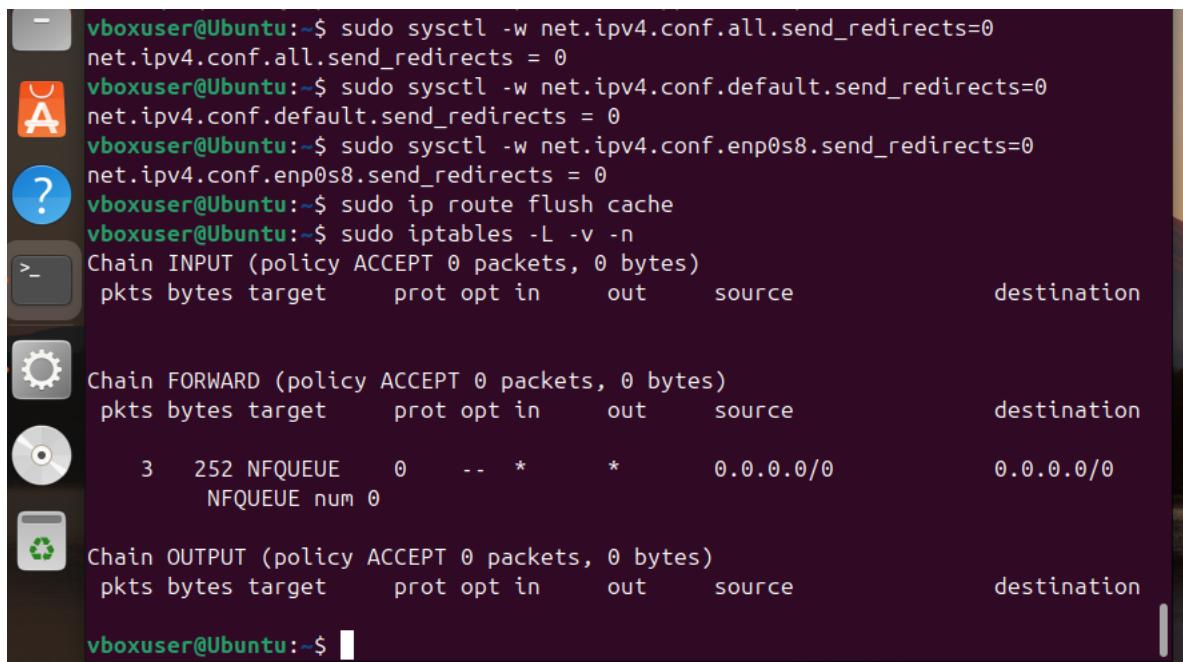
Drop test



vboxuser@Ubuntu:~

```
GNU nano 7.2          /var/lib/suricata//rules/test.rules *
drop icmp any any -> any any (msg:"IPS BLOCK: Ping Detected"; sid:1000001; rev:>
```

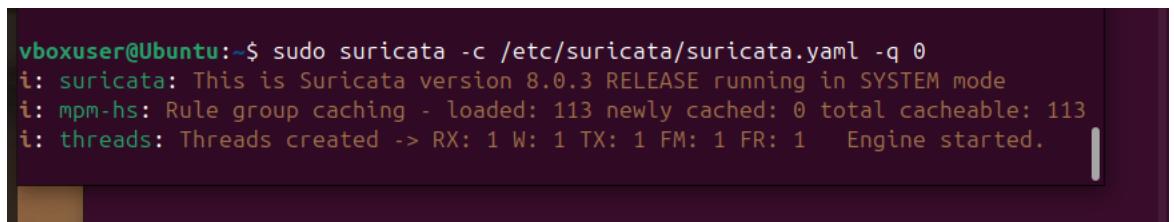
Force routing through soc vm



```
vboxuser@Ubuntu:~$ sudo sysctl -w net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.all.send_redirects = 0
vboxuser@Ubuntu:~$ sudo sysctl -w net.ipv4.conf.default.send_redirects=0
net.ipv4.conf.default.send_redirects = 0
vboxuser@Ubuntu:~$ sudo sysctl -w net.ipv4.conf.enp0s8.send_redirects=0
net.ipv4.conf.enp0s8.send_redirects = 0
vboxuser@Ubuntu:~$ sudo ip route flush cache
vboxuser@Ubuntu:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in      out      source          destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in      out      source          destination
      3    252 NFQUEUE   0      -- *       *        0.0.0.0/0          0.0.0.0/0
      NFQUEUE num 0
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in      out      source          destination
vboxuser@Ubuntu:~$
```

Test

Suricata listening



```
vboxuser@Ubuntu:~$ sudo suricata -c /etc/suricata/suricata.yaml -q 0
i: suricata: This is Suricata version 8.0.3 RELEASE running in SYSTEM mode
i: mpm-hs: Rule group caching - loaded: 113 newly cached: 0 total cacheable: 113
i: threads: Threads created -> RX: 1 W: 1 TX: 1 FM: 1 FR: 1   Engine started.
```

Ping from attacker to victim

```
(kali㉿kali)-[~]
$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
^C
--- 192.168.56.101 ping statistics ---
723 packets transmitted, 0 received, 100% packet loss, time 739317ms

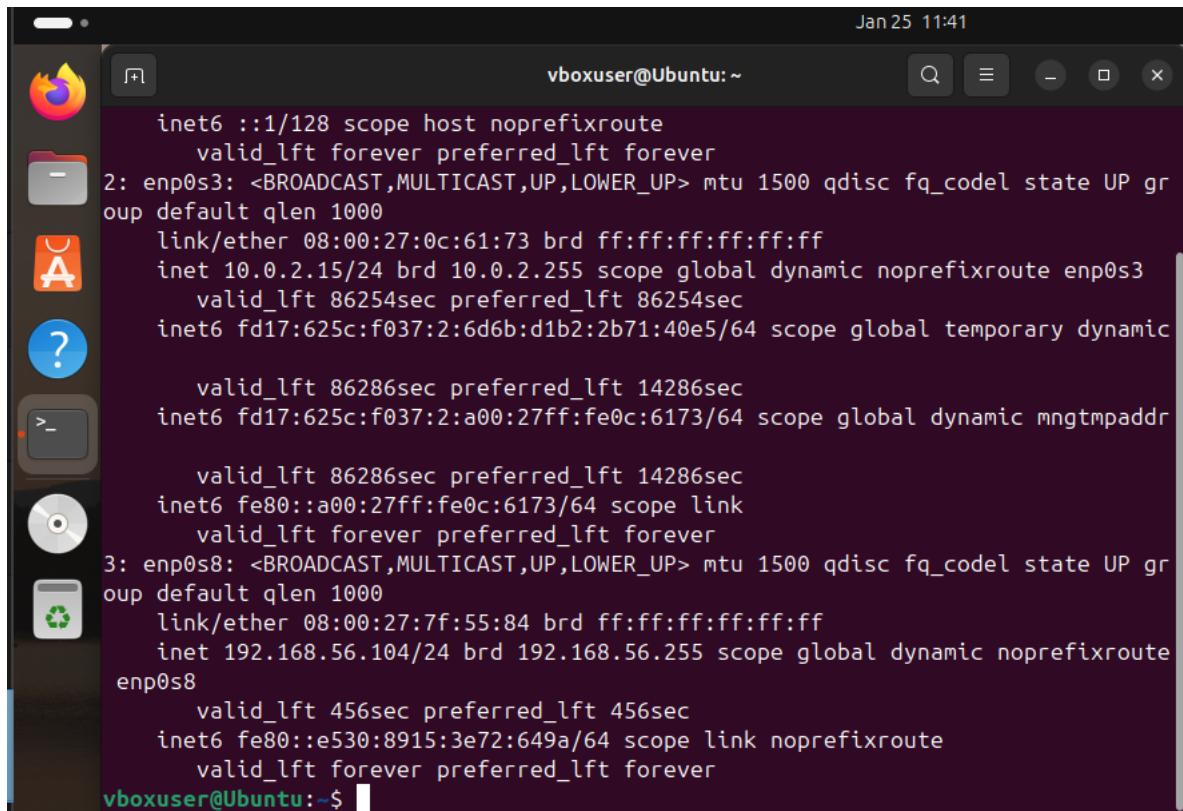
(kali㉿kali)-[~]
$
```

Suricata fast log

```
vboxuser@Ubuntu:~$ tail -f /var/log/suricata/fast.log
tail: cannot open '/var/log/suricata/fast.log' for reading: Permission denied
tail: no files remaining
vboxuser@Ubuntu:~$ sudo tail -f /var/log/suricata/fast.log
[sudo] password for vboxuser:
1/25/2026-04:47:34.355475 [Drop] [**] [1:1000001:1] IPS BLOCK: Ping Detected [
*] [Classification: (null)] [Priority: 3] {ICMP} 192.168.56.102:8 -> 192.168.56
101:0
```

## SIEM (ELK) Setup

### SIEM VM

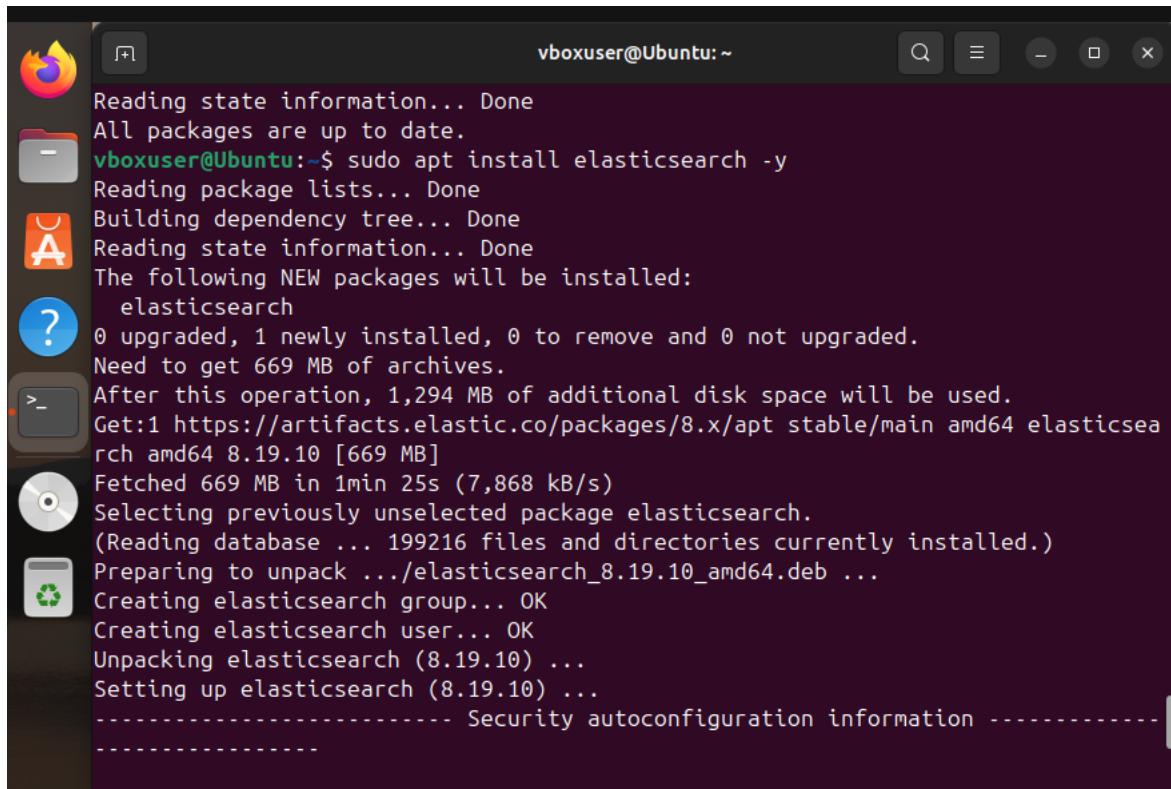


vboxuser@Ubuntu:~

```
inet6 ::1/128 scope host noprefixroute
      valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0c:61:73 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86254sec preferred_lft 86254sec
    inet6 fd17:625c:f037:2:6d6b:d1b2:2b71:40e5/64 scope global temporary dynamic
        valid_lft 86286sec preferred_lft 14286sec
    inet6 fd17:625c:f037:2:a00:27ff:fe0c:6173/64 scope global dynamic mngtmpaddr
        valid_lft 86286sec preferred_lft 14286sec
    inet6 fe80::a00:27ff:fe0c:6173/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7f:55:84 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s8
        valid_lft 456sec preferred_lft 456sec
    inet6 fe80::e530:8915:3e72:649a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

vboxuser@Ubuntu:~\$

### Install elastic



vboxuser@Ubuntu:~

```
Reading state information... Done
All packages are up to date.
vboxuser@Ubuntu:~$ sudo apt install elasticsearch -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 669 MB of archives.
After this operation, 1,294 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main elasticsearch amd64 8.19.10 [669 MB]
Fetched 669 MB in 1min 25s (7,868 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 199216 files and directories currently installed.)
Preparing to unpack .../elasticsearch_8.19.10_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.19.10) ...
Setting up elasticsearch (8.19.10) ...
----- Security autoconfiguration information -----
```

Elastic configuration:

```
vboxuser@Ubuntu:~
```

```
> xpack.security.enrollment.enable:false
> ^C
vboxuser@Ubuntu:~$ sudo bash -c 'cat > /etc/elasticsearch/elasticsearch.yml <<EOF
F
> path.data: /var/lib/elasticsearch
> path.logs: /var/log/elasticsearch
> network.host: 0.0.0.0
> discovery.type: single-node
> xpack.security.enabled: false
> xpack.security.enrollment.enabled: false
> xpack.security.http.ssl.enabled: false
> xpack.security.transport.ssl.enabled: false
> EOF'
vboxuser@Ubuntu:~$ sudo chown -R elasticsearch:elasticsearch /etc/elasticsearch
vboxuser@Ubuntu:~$ sudo chown -R elasticsearch:elasticsearch /var/lib/elasticsearch
vboxuser@Ubuntu:~$ sudo chown -R elasticsearch:elasticsearch /var/log/elasticsearch
vboxuser@Ubuntu:~$ sudo systemctl restart elasticsearch
vboxuser@Ubuntu:~$ systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
    Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; pr...
      Active: active (running) since Sun 2026-01-25 14:09:42 UTC; 10min ago
        Docs: https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html
```

```
192.168.56.104:9200
```

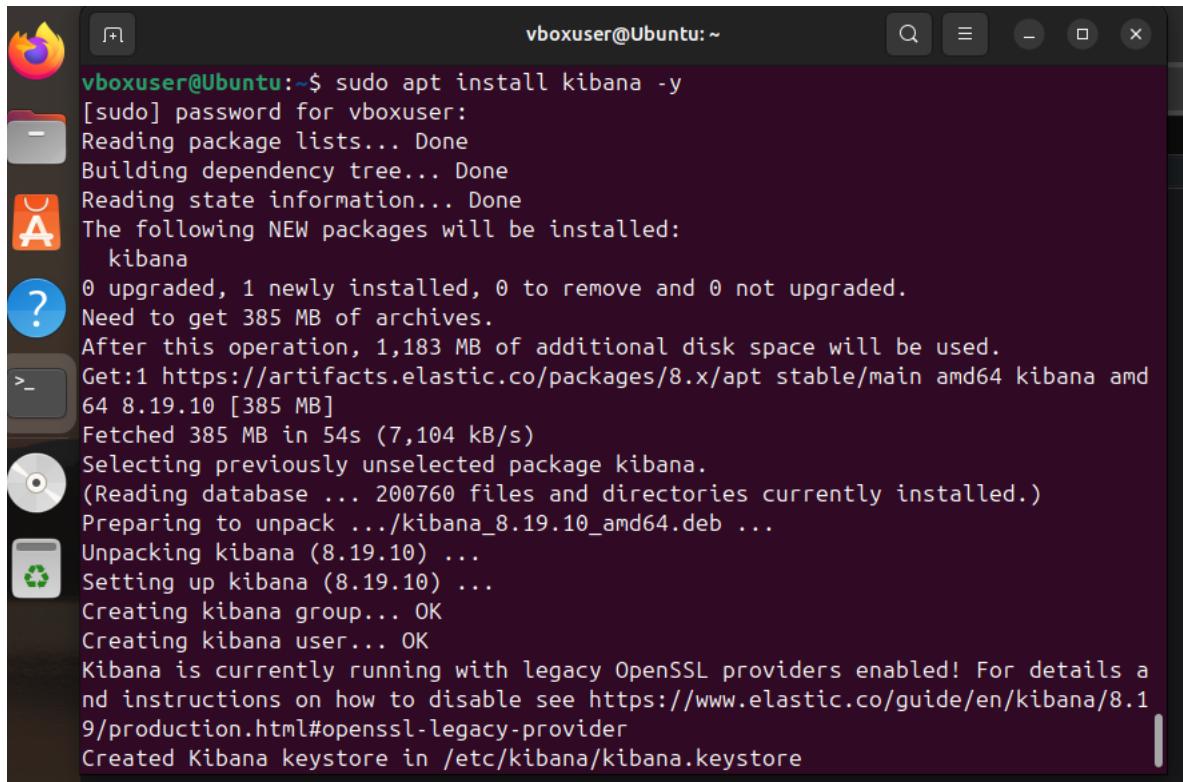
```
http://192.168.56.104:9200
```

```
JSON Raw Data Headers
```

```
Save Copy Collapse All Expand All Filter JSON
```

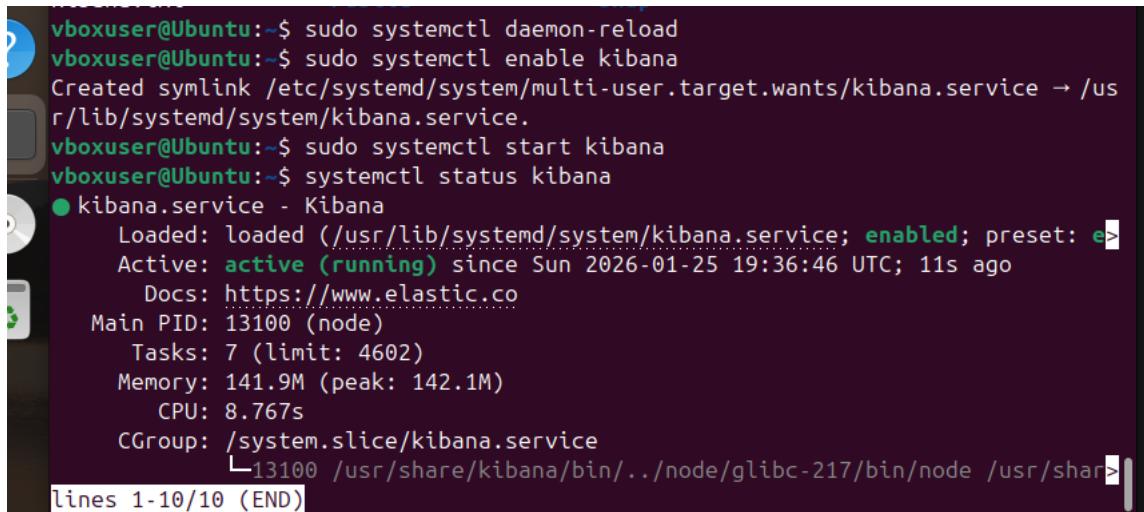
```
name: "Ubuntu"
cluster_name: "elasticsearch"
cluster_uuid: "JjuUSXqLT7qvC7ooepmhtw"
version:
  number: "8.19.10"
  build_flavor: "default"
  build_type: "deb"
  build_hash: "493241b351be6d9f40d52a1406c91a23b4148821"
  build_date: "2026-01-08T22:07:49.939644068Z"
  build_snapshot: false
  lucene_version: "9.12.2"
  minimum_wire_compatibility_version: "7.17.0"
  minimum_index_compatibility_version: "7.0.0"
tagline: "You Know, for Search"
```

Install Kibana



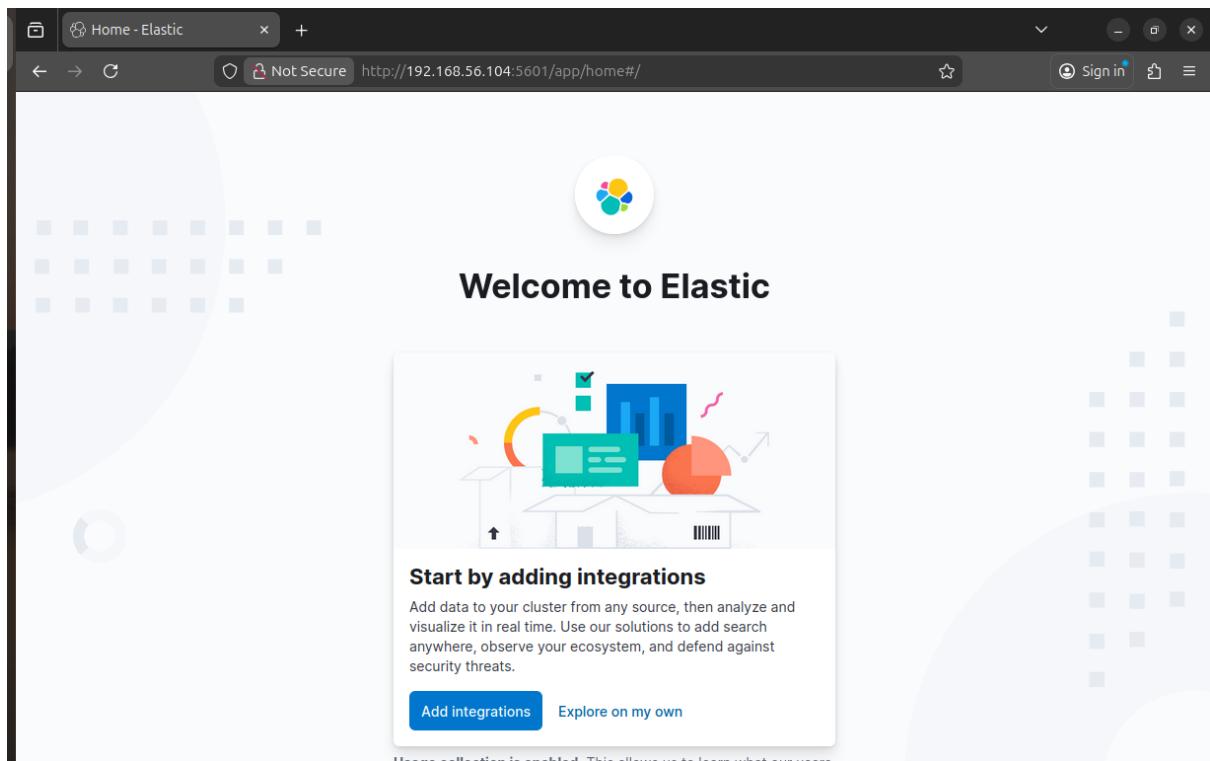
vboxuser@Ubuntu:~\$ sudo apt install kibana -y  
[sudo] password for vboxuser:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  kibana  
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.  
Need to get 385 MB of archives.  
After this operation, 1,183 MB of additional disk space will be used.  
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 kibana amd64 8.19.10 [385 MB]  
Fetched 385 MB in 54s (7,104 kB/s)  
Selecting previously unselected package kibana.  
(Reading database ... 200760 files and directories currently installed.)  
Preparing to unpack .../kibana\_8.19.10\_amd64.deb ...  
Unpacking kibana (8.19.10) ...  
Setting up kibana (8.19.10) ...  
Creating kibana group... OK  
Creating kibana user... OK  
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see <https://www.elastic.co/guide/en/kibana/8.19/production.html#openssl-legacy-provider>  
Created Kibana keystore in /etc/kibana/kibana.keystore

## Start Kibana



```
vboxuser@Ubuntu:~$ sudo systemctl daemon-reload  
vboxuser@Ubuntu:~$ sudo systemctl enable kibana  
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /usr/lib/systemd/system/kibana.service.  
vboxuser@Ubuntu:~$ sudo systemctl start kibana  
vboxuser@Ubuntu:~$ systemctl status kibana  
● kibana.service - Kibana  
    Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)  
    Active: active (running) since Sun 2026-01-25 19:36:46 UTC; 11s ago  
      Docs: https://www.elastic.co/guide/en/kibana/8.19/production.html#openssl-legacy-provider  
    Main PID: 13100 (node)  
       Tasks: 7 (limit: 4602)  
     Memory: 141.9M (peak: 142.1M)  
       CPU: 8.767s  
      CGroup: /system.slice/kibana.service  
              └─13100 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/kibana  
lines 1-10/10 (END)
```

Elastic/Kibana:



Connecting the Sensor to the SIEM:

Installing filebeat

A screenshot of a terminal window titled 'vboxuser@Ubuntu:~'. The window shows the output of a command to install filebeat. The text output includes: '1 package can be upgraded. Run 'apt list --upgradable' to see it.', 'vboxuser@Ubuntu:~\$ sudo apt install filebeat -y', 'Reading package lists... Done', 'Building dependency tree... Done', 'Reading state information... Done', 'The following packages were automatically installed and are no longer required:', 'libgl1-amber-dri libglapi-mesa libl LLVM19', 'Use 'sudo apt autoremove' to remove them.', 'The following NEW packages will be installed:', 'filebeat', '0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.', 'Need to get 68.4 MB of archives.', 'After this operation, 263 MB of additional disk space will be used.', 'Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 filebeat a', 'md64 8.19.10 [68.4 MB]', 'Fetched 68.4 MB in 10s (6,999 kB/s)', 'Selecting previously unselected package filebeat.', '(Reading database ... 198267 files and directories currently installed.)', 'Preparing to unpack .../filebeat\_8.19.10\_amd64.deb ...', 'Unpacking filebeat (8.19.10) ...', 'Setting up filebeat (8.19.10) ...', 'vboxuser@Ubuntu:~\$'. The terminal has a dark theme with light-colored text and icons.

Enabling filebeat handling of Suricata logs using the suricata module

```
Music          Public          snap
vboxuser@Ubuntu:~$ sudo filebeat modules enable suricata
Enabled suricata
vboxuser@Ubuntu:~$
```

Load the dashboards

```
Music          Public          snap
vboxuser@Ubuntu:~$ sudo filebeat modules enable suricata
Enabled suricata
vboxuser@Ubuntu:~$ sudo filebeat setup
Overwriting lifecycle policy is disabled. Set `setup.ilm.overwrite: true` to ove
rwrite.
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded Ingest pipelines
vboxuser@Ubuntu:~$
```

Starting the log shipper

```
vboxuser@Ubuntu:~$ sudo filebeat modules enable suricata
Enabled suricata
vboxuser@Ubuntu:~$ sudo filebeat setup
Overwriting lifecycle policy is disabled. Set `setup.ilm.overwrite: true` to ove
rwrite.
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded Ingest pipelines
vboxuser@Ubuntu:~$ sudo systemctl enable filebeat
[sudo] password for vboxuser:
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /
usr/lib/systemd/system/filebeat.service.
vboxuser@Ubuntu:~$ sudo systemctl start filebeat
vboxuser@Ubuntu:~$
```

Starting the log shipper and starting suricata inspection

```
vboxuser@Ubuntu:~$ sudo systemctl start filebeat
vboxuser@Ubuntu:~$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IPS/NSM/FW daemon
    Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset:>)
      Active: active (running) since Mon 2026-01-26 02:13:11 UTC; 56s ago
        Docs: man:suricata(8)
               man:suricatasc(8)
               https://suricata.io/documentation/
    Process: 4843 ExecStartPre=/bin/rm -f /run/suricata.pid (code=exited, status=0)
   Main PID: 4846 (Suricata-Main)
     Tasks: 1 (limit: 5717)
    Memory: 248.1M (peak: 248.3M)
       CPU: 55.506s
      CGroup: /system.slice/suricata.service
              └─4846 /usr/bin/suricata --af-packet -c /etc/suricata/suricata.yaml

Jan 26 02:13:11 Ubuntu systemd[1]: suricata.service: Scheduled restart job, res>
Jan 26 02:13:11 Ubuntu systemd[1]: Starting suricata.service - Suricata IDS/IPS>
Jan 26 02:13:11 Ubuntu systemd[1]: Started suricata.service - Suricata IDS/IPS>
Jan 26 02:13:11 Ubuntu suricata[4846]: i: suricata: This is Suricata version 8.0.3
lines 1-18/18 (END)
vboxuser@Ubuntu:~$ sudo suricata -c /etc/suricata/suricata.yaml -q 0
i: suricata: This is Suricata version 8.0.3 RELEASE running in SYSTEM mode
```

## View Dashboard

The screenshot shows the Kibana interface with the title 'Dashboards'. At the top, there is a search bar with the query 'suricata' and buttons for 'Recently updated', 'Tags', 'Created by', and 'Create dashboard'. Below the search bar is a table listing dashboards:

Name	Last updated	Actions
[Filebeat Suricata] Events Overview	25 minutes ago	<a href="#">Edit</a> <a href="#">Delete</a>
[Filebeat Suricata] Alert Overview	25 minutes ago	<a href="#">Edit</a> <a href="#">Delete</a>

At the bottom of the table, there are pagination controls: 'Rows per page: 20', a page number '1', and navigation arrows.

Kibana dashboard for Suricata alerts

581120 05:54

[Filebeat Suricata] Alert

Not Secure http://192.168.56.104:5601/app/dashboards#/view/05268ee0-86d1-11e8-b59d-21e Sign in

elastic Find apps, content, and more.

Dashboards [Filebeat Suricata] Alert Overview Full screen Duplicate Reset Edit

Filter your data using KQL syntax Today

**Navigation [Filebeat Suricata]**

**SURICATA Events | Alerts**

**Top Alerting Hosts [Filebeat Suricata]**

|||||

**Top Alert Signatures [Filebeat Suricata]**

|||||

**Alerts - Top Source Countries [File...]** **Alerts - Top Destination Countries [Fil...**

Right Ctrl

This screenshot shows the Elasticsearch Dashboards interface for monitoring Filebeat Suricata alerts. The main title is '[Filebeat Suricata] Alert'. The URL is 'http://192.168.56.104:5601/app/dashboards#/view/05268ee0-86d1-11e8-b59d-21e'. The elastic logo is at the top left, and a search bar is at the top right. The navigation bar includes 'Dashboards' (selected), 'Filebeat Suricata' (highlighted in green), 'Alert Overview', and buttons for 'Full screen', 'Duplicate', 'Reset', 'Edit', and a date range selector. A search bar below the navigation bar allows filtering using KQL syntax. The main area is titled 'Navigation [Filebeat Suricata]' and contains a 'SURICATA Events | Alerts' section, which is currently active. Other sections visible include 'Top Alerting Hosts [Filebeat Suricata]', 'Top Alert Signatures [Filebeat Suricata]', 'Alerts - Top Source Countries [File...]', and 'Alerts - Top Destination Countries [Fil...]'.