Introduction:
Suricata is an open-source intrusion detection system (IDS) and intrusion prevention system (IPS) that monitors network traffic and looks for patterns that match known threats. It can use a variety of methods to detect threats, including signature-based detection

Installation of Suricata:

sudo apt-get install software-properties-common

```
loke4884@lokesh-manikanta:~$ sudo apt-get install software-properties-common
[sudo] password for loke4884:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0
  libchromaprint1 libcodec2-1.0 libdav1d5 libflite1 libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm15 libmfx1 libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55
  librabbitmq4 librubberband2 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0 libsrt1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5 libudfread0 libva-drm2 libva-wayland2 libva-x11-2
  libva2 libvdpau1 libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-software-properties software-properties-gtk ubuntu-advantage-tools
The following packages will be upgraded:
  python3-software-properties software-properties-common software-properties-gtk ubuntu-advantage-tools
4 upgraded, 0 newly installed, 0 to remove and 197 not upgraded.
Need to get 114 kB/304 kB of archives.
After this operation, 1,488 kB disk space will be freed.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 software-properties-common all 0.99.22.7 [14.1 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 software-properties-gtk all 0.99.22.7 [71.3 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 python3-software-properties all 0.99.22.7 [28.8 kB]
Preconfiguring packages ...
(Reading database ... 273921 files and directories currently installed.)
Preparing to unpack .../ubuntu-advantage-tools_29.4~22.04_amd64.deb ...
Unpacking ubuntu-advantage-tools (29.4~22.04) over (27.9~22.04.1) ...
Preparing to unpack .../software-properties-common_0.99.22.7_all.deb ...
Unpacking software-properties-common (0.99.22.7) over (0.99.22.2) ...
Preparing to unpack .../software-properties-gtk_0.99.22.7_all.deb ...
Unpacking software-properties-gtk (0.99.22.7) over (0.99.22.2) ...
```

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

```
loke4884@lokesh-manikanta:~$ sudo add-apt-repository ppa:oisf/suricata-stable
Repository: 'deb https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/ jammy 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:

- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS/SSL certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
- IEEE 802.1ad (QinQ) and IEEE 802.1Q (VLAN) support
- VXLAN support
- All JSON output/logging capability
- IDS runmode
- IPS runmode
- IDPS runmode
- NSM runmode
- eBPF/XDP
- Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH, FTP, SMB, DNS, NFS, TFTP, KRB5, DHCP, IKEv2, SNMP, SIP, RDP
- SCADA automatic protocol detection - ENIP/DNP3/MODBUS
- File Extraction HTTP/SMTP/FTP/NFS/SMB - over 4000 file types recognized and extracted from live traffic.
- File MD5/SHA1/SHA256 matching
- Gzip Decompression
- Fast IP Matching
- Datasets matching
- Rustlang enabled protocol detection
- Lua scripting
```

sudo apt-get update && sudo apt-get install suricata -y

```
loke4884@lokesh-manikanta:~$ sudo apt-get update && sudo apt-get install suricata -y
Hit:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:5 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:6 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy InRelease
Reading package lists... Done
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0
  libchromaprint1 libcodec2-1.0 libdav1d5 libflite1 libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm15 libmfx1 libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55
  librabbitmq4 librubberband2 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0 libsrt1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5 libudfread0 libva-drm2 libva-wayland2 libva-x11-2
  libva2 libvdpau1 libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libluajit-5.1-2 libluajit-5.1-common liblzma-dev libnet1 libnetfilter-queue1
Suggested packages:
  liblzma-doc
The following NEW packages will be installed:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libluajit-5.1-2 libluajit-5.1-common liblzma-dev libnet1 libnetfilter-queue1 suricata
0 upgraded, 11 newly installed, 0 to remove and 312 not upgraded.
Need to get 6,724 kB of archives.
After this operation, 30.4 MB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 libhyperscan5 amd64 5.4.0-2 [2,485 kB]
Get:2 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy/main amd64 libhtp2 amd64 1:0.5.45-0ubuntu0 [75.0 kB]
Get:3 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy/main amd64 suricata amd64 1:7.0.2-0ubuntu0 [3,527 kB]
```

To know suricata version

suricata -V

```
loke4884@lokesh-manikanta:~$ suricata -V
This is Suricata version 7.0.2 RELEASE
```

To start suricata

sudo systemctl start suricata.service

```
loke4884@lokesh-manikanta:~$ sudo systemctl start suricata.service
```

To check status of suricata

sudo systemctl status suricata

```
loke4884@lokesh-manikanta:~$ sudo systemctl status suricata
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (exited) since Sat 2023-12-16 17:29:05 IST; 4min 29s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 6040 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
        CPU: 147ms

Dec 16 17:29:05 lokesh-manikanta systemd[1]: Starting LSB: Next Generation IDS/IPS...
Dec 16 17:29:05 lokesh-manikanta suricata[6040]: Starting suricata in IDS (af-packet) mode... done.
Dec 16 17:29:05 lokesh-manikanta systemd[1]: Started LSB: Next Generation IDS/IPS.
```

To stop suricata

sudo systemctl stop suricata

```
loke4884@lokesh-manikanta:~$ sudo systemctl stop suricata
```

\

Configuration of Suricata

To check configuration files of suricata

ls -al /etc/suricata/

```
loke4884@lokesh-manikanta:~$ ls -al /etc/suricata/
total 112
drwxr-xr-x   2 root root  4096 Dec 16 17:29 .
drwxr-xr-x 136 root root 12288 Dec 16 17:29 ..
-rw-r--r--   1 root root  3327 Oct 18 19:55 classification.config
-rw-r--r--   1 root root  1375 Oct 18 19:55 reference.config
-rw-r--r--   1 root root 84898 Oct 19 18:17 suricata.yaml
-rw-r--r--   1 root root  1643 Oct 18 19:55 threshold.config
```

To set up configuration of suricata by suricata.yml

sudo nano /etc/suricata/suricata.yaml

```
loke4884@lokesh-manikanta:~$ sudo nano /etc/suricata/suricata.yaml
```

```
  GNU nano 6.2                          /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 7.0.2.
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: "[192.168.195.128/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"
```

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

```
# Cross platform libpcap capture support
pcap:
  - interface: ens33
```

community-id

Used for event correlation for example zeek when you are trying to import logs in the json formate

Suricata saves logs in the json formate

Set community-id to true

```
# enable/disable the community id feature.
community-id: true
```

To set rules you can give path of that rule file in the rule-files

```
default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
```

To know more about suricata use

suricata --help

```
loke4884@lokesh-manikanta:~$ suricata --help
suricata: unrecognized option '--help'
Suricata 7.0.2
USAGE: suricata [OPTIONS] [BPF FILTER]

        -c <path>                           : path to configuration file
        -T                                  : test configuration file (use with -c)
        -i <dev or ip>                      : run in pcap live mode
        -F <bpf filter file>                : bpf filter file
        -r <path>                           : run in pcap file/offline mode
        -q <qid[:qid]>                      : run in inline nfqueue mode (use colon to specify a range of queues)
        -s <path>                           : path to signature file loaded in addition to suricata.yaml settings (optional)
        -S <path>                           : path to signature file loaded exclusively (optional)
        -l <dir>                            : default log directory
        -D                                  : run as daemon
        -k [all|none]                       : force checksum check (all) or disabled it (none)
        -V                                  : display Suricata version
        -v                                  : be more verbose (use multiple times to increase verbosity)
        --list-app-layer-protos             : list supported app layer protocols
        --list-keywords[=all|csv|<kword>]   : list keywords implemented by the engine
        --list-runmodes                     : list supported runmodes
        --runmode <runmode_id>              : specific runmode modification the engine should run.  The argument
                                              supplied should be the id for the runmode obtained by running
                                              --list-runmodes
        --engine-analysis                   : print reports on analysis of different sections in the engine and exit.
                                              Please have a look at the conf parameter engine-analysis on what reports
                                              can be printed
        --pidfile <file>                    : write pid to this file
        --init-errors-fatal                 : enable fatal failure on signature init error
        --disable-detection                 : disable detection engine
        --dump-config                       : show the running configuration
        --dump-features                     : display provided features
        --build-info                        : display build information
        --pcap[=<dev>]                      : run in pcap mode, no value select interfaces from suricata.yaml
        --pcap-file-continuous              : when running in pcap mode with a directory, continue checking directory for pcaps until interrupted
        --pcap-file-delete                  : when running in replay mode (-r with directory or file), will delete pcap files that have been processed when done
        --pcap-file-recursive               : will descend into subdirectories when running in replay mode (-r)
        --pcap-buffer-size                  : size of the pcap buffer value from 0 - 2147483647
        --af-packet[=<dev>]                 : run in af-packet mode, no value select interfaces from suricata.yaml
        --simulate-ips                      : force engine into IPS mode. Useful for QA
        --user <user>                       : run suricata as this user after init
        --group <group>                     : run suricata as this group after init
        --erf-in <path>                     : process an ERF file
```

sudo suricata-update

this command update suricata by what the changes made in suricata.yml after updating it goes for checking for any syntax errors

```
loke4884@lokesh-manikanta:~$ sudo suricata-update
16/12/2023 -- 19:32:55 - <Info> -- Using data-directory /var/lib/suricata.
16/12/2023 -- 19:32:55 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
16/12/2023 -- 19:32:55 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
16/12/2023 -- 19:32:55 - <Info> -- Found Suricata version 7.0.2 at /usr/bin/suricata.
16/12/2023 -- 19:32:55 - <Info> -- Loading /etc/suricata/suricata.yaml
16/12/2023 -- 19:32:55 - <Info> -- Disabling rules for protocol pgsql
16/12/2023 -- 19:32:55 - <Info> -- Disabling rules for protocol modbus
16/12/2023 -- 19:32:55 - <Info> -- Disabling rules for protocol dnp3
16/12/2023 -- 19:32:55 - <Info> -- Disabling rules for protocol enip
16/12/2023 -- 19:32:55 - <Info> -- No sources configured, will use Emerging Threats Open
16/12/2023 -- 19:32:55 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.2/emerging.rules.tar.gz.
 100% - 4170121/4170121
16/12/2023 -- 19:32:58 - <Info> -- Done.
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/app-layer-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/decoder-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dhcp-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dnp3-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dns-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/files.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/http-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ipsec-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/kerberos-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/modbus-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/nfs-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ntp-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/smb-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/smtp-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/stream-events.rules
16/12/2023 -- 19:32:58 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/tls-events.rules
16/12/2023 -- 19:32:59 - <Info> -- Ignoring file rules/emerging-deleted.rules
16/12/2023 -- 19:33:05 - <Info> -- Loaded 46360 rules.
16/12/2023 -- 19:33:06 - <Info> -- Disabled 14 rules.
16/12/2023 -- 19:33:06 - <Info> -- Enabled 0 rules.
16/12/2023 -- 19:33:06 - <Info> -- Modified 0 rules.
16/12/2023 -- 19:33:06 - <Info> -- Dropped 0 rules.
16/12/2023 -- 19:33:07 - <Info> -- Enabled 133 rules for flowbit dependencies.
16/12/2023 -- 19:33:07 - <Info> -- Creating directory /var/lib/suricata/rules.
16/12/2023 -- 19:33:07 - <Info> -- Backing up current rules.
16/12/2023 -- 19:33:07 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 46360; enabled: 35898; added: 46360; removed 0; modified: 0
16/12/2023 -- 19:33:07 - <Info> -- Writing /var/lib/suricata/rules/classification.config
16/12/2023 -- 19:33:08 - <Info> -- Testing with suricata -T.
16/12/2023 -- 19:34:02 - <Info> -- Done.
```

sudo ls -la /var/lib/suricata/rules/

```
loke4884@lokesh-manikanta:~$ sudo ls -la /var/lib/suricata/rules/
total 26836
drwxr-x--- 2 root root     4096 Dec 16 19:33 .
drwxr-xr-x 4 root root     4096 Dec 16 19:33 ..
-rw-r--r-- 1 root root     3228 Dec 16 19:33 classification.config
-rw-r--r-- 1 root root 27465350 Dec 16 19:33 suricata.rules
```

sudo suricata-update list-sources

It downloads the index of sources

This sources gives you rule sets based on yours requirements

```
loke4884@lokesh-manikanta:~$ sudo suricata-update list-sources
16/12/2023 -- 19:43:56 - <Info> -- Using data-directory /var/lib/suricata.
16/12/2023 -- 19:43:56 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
16/12/2023 -- 19:43:56 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules
16/12/2023 -- 19:43:56 - <Info> -- Found Suricata version 7.0.2 at /usr/bin/suricata.
16/12/2023 -- 19:43:56 - <Warning> -- Source index does not exist, will use bundled one.
16/12/2023 -- 19:43:56 - <Warning> -- Please run suricata-update update-sources.
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: etnetera/aggressive
  Vendor: Etnetera a.s.
  Summary: Etnetera aggressive IP blacklist
  License: MIT
Name: malsilo/win-malware
  Vendor: malsilo
  Summary: Commodity malware rules
  License: MIT
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT
Name: scwx/enhanced
  Vendor: Secureworks
  Summary: Secureworks suricata-enhanced ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: scwx/malware
  Vendor: Secureworks
  Summary: Secureworks suricata-malware ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: scwx/security
  Vendor: Secureworks
  Summary: Secureworks suricata-security ruleset
```

Copy name of the rule

```
Name: malsilo/win-malware
  Vendor: malsilo
  Summary: Commodity malware rules
  License: MIT
```

This is how the rule is going to add

sudo suricata-update enable-source malsilo/win-malware

```
loke4884@lokesh-manikanta:~$ sudo suricata-update enable-source malsilo/win-malware
16/12/2023 -- 19:51:21 - <Info> -- Using data-directory /var/lib/suricata.
16/12/2023 -- 19:51:21 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
16/12/2023 -- 19:51:21 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
16/12/2023 -- 19:51:21 - <Info> -- Found Suricata version 7.0.2 at /usr/bin/suricata.
16/12/2023 -- 19:51:21 - <Warning> -- Source index does not exist, will use bundled one.
16/12/2023 -- 19:51:21 - <Warning> -- Please run suricata-update update-sources.
16/12/2023 -- 19:51:21 - <Info> -- Creating directory /var/lib/suricata/update/sources
16/12/2023 -- 19:51:21 - <Info> -- Enabling default source et/open
16/12/2023 -- 19:51:21 - <Info> -- Source malsilo/win-malware enabled
```

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

```
loke4884@lokesh-manikanta:~$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
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. 35912 rules successfully loaded, 0 rules failed
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 35915 signatures processed. 1216 are IP-only rules, 5344 are inspecting packet pay
load, 29135 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```

In fast.logs you can find the intrusion logs

In eve.json you can find the intrusion logs in the json formate

ls -al /var/log/suricata

```
loke4884@lokesh-manikanta:~$ ls  -al /var/log/suricata
total 1028
drwxr-xr-x  5 root root     4096 Dec 16 17:29 .
drwxrwxr-x 17 root syslog   4096 Dec 17 14:18 ..
drwxr-xr-x  2 root root     4096 Oct 19 18:17 certs
drwxr-xr-x  2 root root     4096 Oct 19 18:17 core
-rw-r--r--  1 root root   707597 Dec 17 14:24 eve.json
-rw-r--r--  1 root root        0 Dec 16 17:29 fast.log
drwxr-xr-x  2 root root     4096 Oct 19 18:17 files
-rw-r--r--  1 root root   274242 Dec 17 14:24 stats.log
-rw-r--r--  1 root root    36267 Dec 16 23:55 suricata.log
-rw-r--r--  1 root root     1232 Dec 16 23:54 suricata-start.log
```

sudo ls -al /var/lib/suricata/rules

```
loke4884@lokesh-manikanta:~$ sudo ls -al /var/lib/suricata/rules/
[sudo] password for loke4884:
total 26840
drwxr-x--- 2 root root     4096 Dec 16 19:52 .
drwxr-xr-x 4 root root     4096 Dec 16 19:33 ..
-rw-r--r-- 1 root root     3228 Dec 16 19:52 classification.config
-rw-r--r-- 1 root root 27470473 Dec 16 19:52 suricata.rules
```

Curl http://testmynids.org/uid/index.html

```
loke4884@lokesh-manikanta:~$ curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
```

Intruder gained access through the root

To see logs captured by suricata

sudo cat /var/log/suricata/fast.log

```
loke4884@lokesh-manikanta:~$ sudo cat /var/log/suricata/fast.log
12/17/2023-15:04:25.849524  [**] [1:2013028:7] ET POLICY curl User-Agent Outbound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.195.128:41726 -> 108.157.238.41:80
12/17/2023-15:04:25.852683  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 108.157.238.41:80 -> 192.168.195.128:41726
```

To see all the files under rules

```
loke4884@lokesh-manikanta:~$ sudo ls -al /var/lib/suricata/rules/
[sudo] password for loke4884:
total 26840
drwxr-x--- 2 root root     4096 Dec 16 19:52 .
drwxr-xr-x 4 root root     4096 Dec 16 19:33 ..
-rw-r--r-- 1 root root     3228 Dec 16 19:52 classification.config
-rw-r--r-- 1 root root 27470473 Dec 16 19:52 suricata.rules
```

Throught this we can say that intruder could gain access through the root

```
loke4884@lokesh-manikanta:~$ curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
```

Logs generated by suricata

```
loke4884@lokesh-manikanta: $ sudo cat /var/log/suricata/fast.log
[sudo] password for loke4884:
12/17/2023-15:04:25.849524  [**] [1:2013028:7] ET POLICY curl User-Agent Outbound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.195.128:41726 -> 108.157.238.41:80
12/17/2023-15:04:25.852683  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 108.157.238.41:80 -> 192.168.195.128:41726
12/19/2023-18:08:43.197141  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.195.128:48700 -> 34.122.121.32:80
12/19/2023-18:23:29.904347  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:52670 -> 185.125.190.39:80
12/19/2023-18:23:30.075712  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:52670 -> 185.125.190.39:80
12/19/2023-18:23:30.336469  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:48042 -> 91.189.91.81:80
12/19/2023-18:23:30.635225  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:52670 -> 185.125.190.39:80
12/19/2023-18:23:30.791172  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:52670 -> 185.125.190.39:80
12/19/2023-18:23:32.451050  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:51738 -> 185.125.190.36:80
12/20/2023-18:13:09.158616  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:48328 -> 185.125.190.36:80
12/20/2023-18:13:09.368744  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:47908 -> 91.189.91.83:80
12/20/2023-18:13:10.013803  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:48328 -> 185.125.190.36:80
12/20/2023-18:13:38.766364  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:34410 -> 91.189.91.83:80
12/20/2023-18:13:44.224851  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:34410 -> 91.189.91.83:80
12/20/2023-18:13:50.675042  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:35916 -> 185.125.190.39:80
12/20/2023-18:14:01.805655  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:60716 -> 185.125.190.36:80
12/20/2023-18:14:28.000861  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:47002 -> 185.125.190.39:80
12/20/2023-18:16:31.345112  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.195.128:35916 -> 185.125.190.39
```

```
12/21/2023-06:55:16.961367  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:56030 -> 91.189.91.82:80
12/21/2023-06:55:18.040018  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:56030 -> 91.189.91.82:80
12/21/2023-07:12:17.199996  [**] [1:2013028:7] ET POLICY curl User-Agent Outbound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.195.128:37208 -> 108.158.61.22:80
12/21/2023-07:12:17.202560  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 108.158.61.22:80 -> 192.168.195.128:37208
```

To know status of suricata

```
loke4884@lokesh-manikanta:~$ sudo systemctl status suricata
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (running) since Sat 2023-12-16 23:54:53 IST; 4 days ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 8 (limit: 9387)
     Memory: 386.9M
        CPU: 1min 42.087s
     CGroup: /system.slice/suricata.service
             └─9131 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricat>

Dec 16 23:54:53 lokesh-manikanta systemd[1]: Starting LSB: Next Generation IDS/IPS...
Dec 16 23:54:53 lokesh-manikanta suricata[9122]: Likely stale PID 6053 with /var/run/suricata.p>
Dec 16 23:54:53 lokesh-manikanta suricata[9122]: Removing stale PID file /var/run/suricata.pid
Dec 16 23:54:53 lokesh-manikanta suricata[9122]: Starting suricata in IDS (af-packet) mode... d>
Dec 16 23:54:53 lokesh-manikanta systemd[1]: Started LSB: Next Generation IDS/IPS.
```

To stop suricata

```
loke4884@lokesh-manikanta:~$ sudo systemctl stop suricata.service
```

```
loke4884@lokesh-manikanta:~$ sudo ls /etc/suricata/
[sudo] password for loke4884:
classification.config  reference.config  suricata.yaml  threshold.config
```

Create a file which has customised rules made by you

```
loke4884@lokesh-manikanta:~$ sudo mkdir /etc/suricata/rules
loke4884@lokesh-manikanta:~$ sudo ls /etc/suricata/
classification.config  reference.config  rules  suricata.yaml  threshold.config
```

Write a rule

This will log any pings coming from any other external network to home network (by any port)

```
loke4884@lokesh-manikanta:~$ sudo nano /etc/suricata/rules/local.rules
```

```
  GNU nano 6.2                      /etc/suricata/rules/local.rules *
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping"; sid:1; rev:1;)
```

msg → message to contain in the log

rev → revision

Add that rule into suricata.yaml file

```
loke4884@lokesh-manikanta:~$ sudo nano /etc/suricata/suricata.yaml
```

In the rules-files , add the file which contains customised rules

```
rule-files:
  - suricata.rules
  - /etc/suricata/rules/local.rules
```

Save and close the file

Testing that file(for proper configuration)

```
loke4884@lokesh-manikanta:~$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
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: 2 rule files processed. 35913 rules successfully loaded, 0 rules failed
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 35916 signatures processed. 1217 are IP-only rules, 5344 are inspecting packet pay
load, 29135 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```

Start suricata services

```
loke4884@lokesh-manikanta:~$ sudo systemctl start suricata.service
```

Fast.log file captures logs generated by suricata

```
loke4884@lokesh-manikanta: $ sudo cat /var/log/suricata/fast.log
12/17/2023-15:04:25.849524  [**] [1:2013028:7] ET POLICY curl User-Agent Outbound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.195.128:41726 -> 108.157.238.41:80
12/17/2023-15:04:25.852683  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 108.157.238.41:80 -> 192.168.195.128:41726
12/19/2023-18:08:43.197141  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.195.128:48700 -> 34.122.121.32:80
12/19/2023-18:23:29.904347  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:52670 -> 185.125.190.39:80
12/19/2023-18:23:30.075712  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:52670 -> 185.125.190.39:80
12/19/2023-18:23:30.336469  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:48042 -> 91.189.91.81:80
12/19/2023-18:23:30.635225  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:52670 -> 185.125.190.39:80
12/19/2023-18:23:30.791172  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:52670 -> 185.125.190.39:80
12/19/2023-18:23:32.451050  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:51738 -> 185.125.190.36:80
12/20/2023-18:13:09.158616  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:48328 -> 185.125.190.36:80
12/20/2023-18:13:09.368744  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:47908 -> 91.189.91.83:80
12/20/2023-18:13:10.013803  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:48328 -> 185.125.190.36:80
12/20/2023-18:13:38.766364  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:34410 -> 91.189.91.83:80
12/20/2023-18:13:44.224851  [**] [1:2013504:6] ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.1
95.128:34410 -> 91.189.91.83:80
```

Now you can see which system has pinged (through logs)

```
12/21/2023-09:18:27.145836  [**] [1:1:1] ICMP Ping [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.195.1:8 -> 192.168.195.128:0
12/21/2023-09:18:27.147333  [**] [1:1:1] ICMP Ping [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.195.128:0 -> 192.168.195.1:0
```

To see logs in json formate

```
loke4884@lokesh-manikanta:~$ sudo cat /var/log/suricata/eve.json
```


```
o":"UDP","app_proto":"dns","flow":{"pkts_toserver":1,"pkts_toclient":2,"bytes_toserver":89,"bytes_toclient":234,"start":"2023-12-19T18:26:12.857200+0530","end":"2023-12-19T18:26:12.857385+0530","age":0,"
state":"new","reason":"timeout","alerted":false},"community_id":"1:nW23vhadOKkLtbbs6Q1CX7yDLX8="}
{"timestamp":"2023-12-19T18:26:52.596049+0530","flow_id":1399549258080603,"in_iface":"ens33","event_type":"flow","src_ip":"192.168.195.128","src_port":45633,"dest_ip":"192.168.195.2","dest_port":53,"prot
o":"UDP","app_proto":"dns","flow":{"pkts_toserver":1,"pkts_toclient":2,"bytes_toserver":89,"bytes_toclient":234,"start":"2023-12-19T18:26:12.850145+0530","end":"2023-12-19T18:26:12.850476+0530","age":0,"
state":"new","reason":"timeout","alerted":false},"community_id":"1:RahA0xLympR3Jy7Qaj8/cI/AzFA="}
{"timestamp":"2023-12-19T18:26:53.332834+0530","flow_id":1429511580526377,"in_iface":"ens33","event_type":"dns","src_ip":"192.168.195.128","src_port":41925,"dest_ip":"192.168.195.2","dest_port":53,"proto
":"UDP","pkt_src":"wire/pcap","community_id":"1:kvFxh7rebyO9y81p/hhzCoC9rks=","dns":{"type":"query","id":1113,"rrname":"ntp.ubuntu.com","rrtype":"A","tx_id":0,"opcode":0}}
{"timestamp":"2023-12-19T18:26:53.332940+0530","flow_id":1429967545457378,"in_iface":"ens33","event_type":"dns","src_ip":"192.168.195.128","src_port":37666,"dest_ip":"192.168.195.2","dest_port":53,"proto
":"UDP","pkt_src":"wire/pcap","community_id":"1:mFqI1+dmk1LKPMbpokqWbfRo82E=","dns":{"type":"query","id":24493,"rrname":"ntp.ubuntu.com","rrtype":"AAAA","tx_id":0,"opcode":0}}
{"timestamp":"2023-12-19T18:26:53.334466+0530","flow_id":1436523730334643,"in_iface":"ens33","event_type":"dns","src_ip":"192.168.195.128","src_port":53906,"dest_ip":"192.168.195.2","dest_port":53,"proto
":"UDP","pkt_src":"wire/pcap","community_id":"1:vupd2rCT2yy+uLBJCC/QSugwXMk=","dns":{"type":"query","id":41047,"rrname":"ntp.ubuntu.com","rrtype":"A","tx_id":0,"opcode":0}}
{"timestamp":"2023-12-19T18:26:53.334732+0530","flow_id":1437666025140814,"in_iface":"ens33","event_type":"dns","src_ip":"192.168.195.128","src_port":58933,"dest_ip":"192.168.195.2","dest_port":53,"proto
":"UDP","pkt_src":"wire/pcap","community_id":"1:ay4QvK5yIalxP7gCdWdTuMbxTRM=","dns":{"type":"query","id":37623,"rrname":"ntp.ubuntu.com","rrtype":"AAAA","tx_id":0,"opcode":0}}
{"timestamp":"2023-12-19T18:26:53.337579+0530","flow_id":1449892967430402,"in_iface":"ens33","event_type":"dns","src_ip":"192.168.195.128","src_port":58316,"dest_ip":"192.168.195.2","dest_port":53,"proto
":"UDP","pkt_src":"wire/pcap","community_id":"1:vW8AwWf2EI2x/RMDkFU/Bkk11c0=","dns":{"type":"query","id":22061,"rrname":"ntp.ubuntu.com.localdomain","rrtype":"AAAA","tx_id":0,"opcode":0}}
{"timestamp":"2023-12-19T18:26:53.337664+0530","flow_id":1450255980909384,"in_iface":"ens33","event_type":"dns","src_ip":"192.168.195.128","src_port":56476,"dest_ip":"192.168.195.2","dest_port":53,"proto
":"UDP","pkt_src":"wire/pcap","community_id":"1:kqOuEffdBfWKY5l/D7aZs5FEdXk=","dns":{"type":"query","id":40383,"rrname":"ntp.ubuntu.com.localdomain","rrtype":"A","tx_id":0,"opcode":0}}
{"timestamp":"2023-12-19T18:26:56.710043+0530","flow_id":1474989715686196,"in_iface":"ens33","event_type":"flow","src_ip":"192.168.195.128","src_port":40988,"dest_ip":"192.168.195.2","dest_port":53,"prot
o":"TCP","flow":{"pkts_toserver":1,"pkts_toclient":1,"bytes_toserver":78,"bytes_toclient":60,"start":"2023-12-19T18:25:49.343422+0530","end":"2023-12-19T18:25:49.344306+0530","age":0,"state":"new","reaso
n":"timeout","alerted":false},"community_id":"1:q/tixe/8LlJhNkOJ+OIEXqEysio=","tcp":{"tcp_flags":"16","tcp_flags_ts":"12","tcp_flags_tc":"14","syn":true,"rst":true,"ack":true,"state":"syn_sent","ts_max_r
egions":1,"tc_max_regions":1}}
{"timestamp":"2023-12-19T18:26:56.787728+0530","event_type":"stats","stats":{"uptime":239522,"capture":{"kernel_packets":5782,"kernel_drops":0,"errors":0,"afpacket":{"busy_loop_avg":0,"polls":93804,"poll
_signal":2,"poll_timeout":91214,"poll_data":2588,"poll_errors":0,"send_errors":0}},"decoder":{"pkts":5784,"bytes":2621625,"invalid":0,"ipv4":5228,"ipv6":424,"ethernet":5784,"arp":132,"unknown_ethertype":
0,"chdlc":0,"raw":0,"null":0,"sll":0,"tcp":3619,"udp":1445,"sctp":0,"esp":0,"icmpv4":314,"icmpv6":168,"ppp":0,"pppoe":0,"geneve":0,"gre":0,"vlan":0,"vlan_qinq":0,"vlan_qinqinq":0,"vxlan":0,"vntag":0,"iee
e8021ah":0,"teredo":0,"ipv4_in_ipv6":0,"ipv6_in_ipv6":0,"mpls":0,"avg_pkt_size":453,"max_pkt_size":1514,"max_mac_addrs_src":0,"max_mac_addrs_dst":0,"erspan":0,"nsh":0,"event":{"ipv4":{"pkt_too_small":0,"
hlen_too_small":0,"iplen_smaller_than_hlen":0,"trunc_pkt":0,"opt_invalid":0,"opt_invalid_len":0,"opt_malformed":0,"opt_pad_required":106,"opt_eol_required":0,"opt_duplicate":0,"opt_unknown":0,"wrong_ip_v
ersion":0,"icmpv6":0,"frag_pkt_too_large":0,"frag_overlap":0,"frag_ignored":0}},"icmpv4":{"pkt_too_small":0,"unknown_type":0,"unknown_code":0,"ipv4_trunc_pkt":0,"ipv4_unknown_ver":0}},"icmpv6":{"unknown_ty
pe":0,"unknown_code":0,"pkt_too_small":0,"ipv6_unknown_version":0,"ipv6_trunc_pkt":0,"mld_message_with_invalid_hl":0,"unassigned_type":0,"experimentation_type":0}},"ipv6":{"pkt_too_small":0,"trunc_pkt":0,
"trunc_exthdr":0,"exthdr_dupl_fh":0,"exthdr_useless_fh":0,"exthdr_dupl_rh":0,"exthdr_dupl_hh":0,"exthdr_dupl_dh":0,"exthdr_dupl_ah":0,"exthdr_dupl_eh":0,"exthdr_invalid_optlen":0,"wrong_ip_version":0,"ex
thdr_ah_res_not_null":0,"hopopts_unknown_opt":0,"hopopts_only_padding":0,"dstopts_unknown_opt":0,"dstopts_only_padding":0,"rh_type_0":0,"zero_len_padn":135,"fh_non_zero_reserved_field":0,"data_after_none
_header":0,"unknown_next_header":0,"icmpv4":0,"frag_pkt_too_large":0,"frag_overlap":0,"frag_invalid_length":0,"frag_ignored":0,"ipv4_in_ipv6_too_small":0,"ipv4_in_ipv6_wrong_version":0,"ipv6_in_ipv6_too_
small":0,"ipv6_in_ipv6_wrong_version":0},"tcp":{"pkt_too_small":0,"hlen_too_small":0,"invalid_optlen":0,"opt_invalid_len":0,"opt_duplicate":0},"udp":{"pkt_too_small":0,"hlen_too_small":0,"hlen_invalid":0
,"len_invalid":0},"sll":{"pkt_too_small":0},"ethernet":{"pkt_too_small":0},"ppp":{"pkt_too_small":0,"vju_pkt_too_small":0,"ip4_pkt_too_small":0,"ip6_pkt_too_small":0,"wrong_type":0,"unsup_proto":0},"pppo
e":{"pkt_too_small":0,"wrong_code":0,"malformed_tags":0},"gre":{"pkt_too_small":0,"wrong_version":0,"version0_recur":0,"version0_flags":0,"version0_hdr_too_big":0,"version0_malformed_sre_hdr":0,"version1
_chksum":0,"version1_route":0,"version1_ssr":0,"version1_recur":0,"version1_flags":0,"version1_no_key":0,"version1_wrong_protocol":0,"version1_malformed_sre_hdr":0,"version1_hdr_too_big":0},"vlan":{"head
er_too_small":0,"unknown_type":0,"too_many_layers":0},"ieee8021ah":{"header_too_small":0},"vntag":{"header_too_small":0,"unknown_type":0},"ipraw":{"invalid_ip_version":0},"ltnull":{"pkt_too_small":0,"uns
upported_type":0},"sctp":{"pkt_too_small":0},"esp":{"pkt_too_small":0},"mpls":{"header_too_small":0,"pkt_too_small":0,"bad_label_router_alert":0,"bad_label_implicit_null":0,"bad_label_reserved":0,"unknow
n_payload_type":0},"vxlan":{"unknown_payload_type":0},"geneve":{"unknown_payload_type":0},"erspan":{"header_too_small":0,"unsupported_version":0,"too_many_vlan_layers":0},"dce":{"pkt_too_small":0},"chdlc
":{"pkt_too_small":0},"nsh":{"header_too_small":0,"unsupported_version":0,"bad_header_length":0,"reserved_type":0,"unsupported_type":0,"unknown_payload":0}},"too_many_layers":0},"tcp":{"syn":173,"synack"
:27,"rst":142,"active_sessions":21,"sessions":167,"ssn_memcap_drop":0,"ssn_from_cache":86,"ssn_from_pool":81,"pseudo":0,"pseudo_failed":0,"invalid_checksum":0,"midstream_pickups":0,"pkt_on_wrong_thread":
1,"ack_unseen_data":0,"segment_memcap_drop":0,"segment_from_cache":45,"segment_from_pool":1400,"stream_depth_reached":1,"reassembly_gap":0,"overlap":1,"overlap_diff_data":0,"insert_data_normal_fail":0,"i
nsert_data_overlap_fail":0,"memuse":1212416,"reassembly_memuse":229376},"flow":{"memcap":0,"total":746,"active":49,"tcp":167,"udp":539,"icmpv4":0,"icmpv6":40,"tcp_reuse":0,"get_used":0,"get_used_eval":0,
"get_used_eval_reject":0,"get_used_eval_busy":0,"get_used_failed":0,"wrk":{"spare_sync_avg":100,"spare_sync":6,"spare_sync_incomplete":0,"spare_sync_empty":0,"flows_evicted_needs_work":125,"flows_evicted
_pkt_inject":126,"flows_evicted":27,"flows_injected":124,"flows_injected_max":0},"end":{"state":{"new":595,"established":75,"closed":27,"local_bypassed":0,"capture_bypassed":0},"tcp_state":{"none":0,"syn
_sent":119,"syn_recv":0,"established":0,"fin_wait1":0,"fin_wait2":0,"time_wait":0,"last_ack":0,"close_wait":0,"closing":0,"closed":27},"tcp_liberal":0},"mgr":{"full_hash_pass":486,"rows_per_sec":6553,"ro
ws_maxlen":2,"flows_checked":1540,"flows_notimeout":870,"flows_timeout":670,"flows_evicted":670,"flows_evicted_needs_work":124},"spare":9946,"emerg_mode_entered":0,"emerg_mode_over":0,"recycler":{"recycl
```

Install JQ as the command line processing tool to make json logs readable

```
loke4884@lokesh-manikanta:~$ sudo apt-get install jq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media-va-driver
  libaacs0 libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3
  libbluray2 libbs2b0 libchromaprint1 libcodec2-1.0 libdav1d5 libflashrom1 libflite1
  libftdi1-2 libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13
  libmfx1 libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4
  librubberband2 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0 libsrt1.4-gnutls
  libssh-gcrypt-4 libswresample3 libswscale5 libudfread0 libva-drm2 libva-wayland2 libva-x11-2
  libva2 libvdpau1 libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common
  libzvbi0 mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us va-driver-all
  vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libjq1 libonig5
The following NEW packages will be installed:
  jq libjq1 libonig5
0 upgraded, 3 newly installed, 0 to remove and 8 not upgraded.
Need to get 357 kB of archives.
After this operation, 1,087 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 libonig5 amd64 6.9.7.1-2build1 [172 k
B]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 libjq1 amd64 1.6-2.1ubuntu3 [133 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 jq amd64 1.6-2.1ubuntu3 [52.5 kB]
```

To get latest logs(as we are using tail)

```
loke4884@lokesh-manikanta:~$ sudo tail -f /var/log/suricata/eve.json | jq 'select(.event_type=="alert")'
{
  "timestamp": "2023-12-21T09:52:00.275720+0530",
  "flow_id": 58312042456717,
  "in_iface": "ens33",
  "event_type": "alert",
  "src_ip": "192.168.195.1",
  "src_port": 0,
  "dest_ip": "192.168.195.128",
  "dest_port": 0,
  "proto": "ICMP",
  "icmp_type": 8,
  "icmp_code": 0,
  "pkt_src": "wire/pcap",
  "community_id": "1:o07Ba5RegmWgTh1LXojR0zIlSH8=",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 1,
    "rev": 1,
    "signature": "ICMP Ping",
    "category": "",
    "severity": 3
  },
  "direction": "to_server",
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 0,
    "bytes_toserver": 74,
    "bytes_toclient": 0,
    "start": "2023-12-21T09:52:00.275720+0530",
    "src_ip": "192.168.195.1",
    "dest_ip": "192.168.195.128"
  }
}
```

```
{
  "timestamp": "2023-12-21T09:52:00.275807+0530",
  "flow_id": 58312042456717,
  "in_iface": "ens33",
  "event_type": "alert",
  "src_ip": "192.168.195.128",
  "src_port": 0,
  "dest_ip": "192.168.195.1",
  "dest_port": 0,
  "proto": "ICMP",
  "icmp_type": 0,
  "icmp_code": 0,
  "pkt_src": "wire/pcap",
  "community_id": "1:o07Ba5RegmWgTh1LXojR0zIlSH8=",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 1,
    "rev": 1,
    "signature": "ICMP Ping",
    "category": "",
    "severity": 3
  },
  "direction": "to_client",
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 1,
    "bytes_toserver": 74,
    "bytes_toclient": 74,
    "start": "2023-12-21T09:52:00.275720+0530",
    "src_ip": "192.168.195.1",
    "dest_ip": "192.168.195.128"
  }
}
```


Pings by other system that event recorded and displayed in json(after pinging by other machine it will be recorded in the json)

```
C:\Users\HP>ping 192.168.195.128

Pinging 192.168.195.128 with 32 bytes of data:
Reply from 192.168.195.128: bytes=32 time<1ms TTL=64
Reply from 192.168.195.128: bytes=32 time<1ms TTL=64
Reply from 192.168.195.128: bytes=32 time=1ms TTL=64
Reply from 192.168.195.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.195.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```