Q-3. For IDS/IPS I have used Suricata Application

To install **suricata**
yum install epel-release yum-plugin-copr

yum copr enable @oisf/suricata-6.0

yum install suricata

Check network interface name to provide to suricata for inspecting
ip a

To configure Suricata

We have configuration file located at **/etc/suricata/suricata.yaml**

vi /etc/suricata/suricata.yaml

Edit HOME_NET

HOME_NET variable should include, in most scenarios, the IP address of the monitored interface and all the local networks in use

Capture setting:

```
af-packet:
  - interface: enp0s3
    cluster-id: 99
    cluster-type: cluster_flow
    defrag: yes
    use-mmap: yes
    tpacket-v3: yes
```

We need to disable packet offload features on the network interface on which Suricata is listening.

ethtool -K enp0s3 gro off lro off

Verify this

ethtool -k enp0s3 | grep large

```
[root@localhost bibek]# ethtool -k enp0s3 | grep large
large-receive-offload: off [fixed]
```

We can **edit suricata rules** located at /usr/share/suricata/rules/

Adding new sample rules

vim /usr/share/suricata/rules//test.rules

Add following line

alert http any any -> any any (msg:"Do not read gossip during work";
content:"Scarlett"; nocase; classtype:policy-violation; sid:1; rev:1;)

Save and exit

```
[root@localhost rules]# ls
2100498                 files.rules            ntp-events.rules
app-layer-events.rules  http-events.rules      smb-events.rules
decoder-events.rules    ipsec-events.rules     smtp-events.rules
dhcp-events.rules       kerberos-events.rules  stream-events.rules
dnp3-events.rules       modbus-events.rules    test.rules
dns-events.rules        nfs-events.rules       tls-events.rules
[root@localhost rules]#
```

Add rules name in suricata.yaml

vim /usr/share/suricata/rules/suricata.yaml

Find rule-files

And under it write

- /usr/share/suricata/rules/test.rules

fire Suricata in PCAP live mode by executing

suricata -D -c /etc/suricata/suricata.yaml -i enp0s3

```
[root@localhost rules]# suricata -D -c /etc/suricata/suricata.yaml -i enp0s3
7/11/2021 -- 18:14:49 - <Notice> - This is Suricata version 6.0.3 RELEASE runni
ng in SYSTEM mode
```

fetches the ET Open ruleset

suricata-update

```
[root@localhost bibek]# suricata-update
7/11/2021 -- 18:41:12 - <Info> -- Using data-directory /var/lib/suricata.
7/11/2021 -- 18:41:12 - <Info> -- Using Suricata configuration /etc/suricata/su
ricata.yaml
7/11/2021 -- 18:41:12 - <Info> -- Using /usr/share/suricata/rules for Suricata
provided rules.
7/11/2021 -- 18:41:12 - <Info> -- Found Suricata version 6.0.3 at /sbin/suricat
a.
7/11/2021 -- 18:41:12 - <Info> -- Loading /etc/suricata/suricata.yaml
7/11/2021 -- 18:41:12 - <Info> -- Disabling rules for protocol http2
7/11/2021 -- 18:41:12 - <Info> -- Disabling rules for protocol modbus
7/11/2021 -- 18:41:12 - <Info> -- Disabling rules for protocol enip
7/11/2021 -- 18:41:12 - <Info> -- Disabling rules for protocol dnp3
7/11/2021 -- 18:41:12 - <Info> -- No sources configured, will use Emerging Thre
ats Open
7/11/2021 -- 18:41:12 - <Info> -- Checking https://rules.emergingthreats.net/op
en/suricata-6.0.3/emerging.rules.tar.gz.md5.
```

```
7/11/2021 -- 18:41:18 - <Info> -- Loading distribution rule file /usr/share/sur
icata/rules/tls-events.rules
7/11/2021 -- 18:41:19 - <Info> -- Ignoring file rules/emerging-deleted.rules
7/11/2021 -- 18:41:29 - <Info> -- Loaded 31207 rules.
7/11/2021 -- 18:41:30 - <Info> -- Disabled 14 rules.
7/11/2021 -- 18:41:30 - <Info> -- Enabled 0 rules.
7/11/2021 -- 18:41:30 - <Info> -- Modified 0 rules.
7/11/2021 -- 18:41:30 - <Info> -- Dropped 0 rules.
7/11/2021 -- 18:41:31 - <Info> -- Enabled 131 rules for flowbit dependencies.
7/11/2021 -- 18:41:31 - <Info> -- Backing up current rules.
7/11/2021 -- 18:42:48 - <Info> -- Writing rules to /var/lib/suricata/rules/suri
cata.rules: total: 31207; enabled: 23841; added: 0; removed 0; modified: 0
7/11/2021 -- 18:42:51 - <Info> -- Writing /var/lib/suricata/rules/classificatio
n.config
7/11/2021 -- 18:42:51 - <Info> -- No changes detected, exiting.
```

Tail the Suricata alert logs on Suricata host to see what is happening;

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

```
[root@localhost rules]# tail -f /var/log/suricata/fast.log
11/07/2021-18:20:25.424799  [**] [1:0:0] Do not read gossip during work [**] [C
lassification: (null)] [Priority: 3] {TCP} 35.232.111.17:80 -> 192.168.1.142:48
632
11/07/2021-18:20:25.710640  [**] [1:0:0] Do not read gossip during work [**] [C
lassification: (null)] [Priority: 3] {TCP} 35.232.111.17:80 -> 192.168.1.142:48
632
11/07/2021-18:20:25.710648  [**] [1:0:0] Do not read gossip during work [**] [C
lassification: (null)] [Priority: 3] {TCP} 35.232.111.17:80 -> 192.168.1.142:48
632
11/07/2021-18:20:25.711017  [**] [1:0:0] Do not read gossip during work [**] [C
lassification: (null)] [Priority: 3] {TCP} 192.168.1.142:48632 -> 35.232.111.17
:80
11/07/2021-18:20:25.711473  [**] [1:0:0] Do not read gossip during work [**] [C
lassification: (null)] [Priority: 3] {TCP} 192.168.1.142:48632 -> 35.232.111.17
:80
11/07/2021-18:20:25.722485  [**] [1:0:0] Do not read gossip during work [**] [C
lassification: (null)] [Priority: 3] {TCP} 35.232.111.17:80 -> 192.168.1.142:48
632
```