



```
hassnaee@hassnae: ~  
Setting up libhttp2 (1:0.5.48-2) ...  
Setting up libfdt1:amd64 (1.7.0-2) ...  
Setting up libxdp1:amd64 (1.4.3-1) ...  
Setting up suricata-update (1.3.3-1) ...  
Setting up sse4.2-support (24) ...  
Setting up sse3-support (24) ...  
Setting up librtt-log24:amd64 (23.11.1-2) ...  
Setting up libhyperscan5 (5.4.2-2) ...  
Setting up librtt-telemetry24:amd64 (23.11.1-2) ...  
Setting up librtt-kvargs24:amd64 (23.11.1-2) ...  
Setting up librtt-eal24:amd64 (23.11.1-2) ...  
Setting up librtt-ring24:amd64 (23.11.1-2) ...  
Setting up librtt-meter24:amd64 (23.11.1-2) ...  
Setting up librtt-pci24:amd64 (23.11.1-2) ...  
Setting up librtt-mempool24:amd64 (23.11.1-2) ...  
Setting up librtt-bus-pci24:amd64 (23.11.1-2) ...  
Setting up librtt-mbuf24:amd64 (23.11.1-2) ...  
Setting up librtt-bus-vdev24:amd64 (23.11.1-2) ...  
Setting up librtt-sched24:amd64 (23.11.1-2) ...  
Setting up librtt-rcu24:amd64 (23.11.1-2) ...  
Setting up librtt-net24:amd64 (23.11.1-2) ...  
Setting up librtt-ethdev24:amd64 (23.11.1-2) ...  
Setting up librtt-hash24:amd64 (23.11.1-2) ...  
Setting up librtt-ip-frag24:amd64 (23.11.1-2) ...  
Setting up librtt-net-bond24:amd64 (23.11.1-2) ...  
Setting up suricata (1:7.0.6-1) ...  
update-rc.d: We have no instructions for the suricata init script.
```

## 2. Updating the Emerging Threats Open Ruleset

To update the ruleset, run the following command:

- Sudo suricata-update

```
hassnaee@hassnae: ~  
$ sudo systemctl enable suricata.service  
Synchronizing state of suricata.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable suricata  
Created symlink /etc/systemd/system/multi-user.target.wants/suricata.service → /usr/lib/systemd/system/suricata.service.
```

This command fetches and installs the latest version of the ruleset into the default directory (/var/lib/Suricata/rules/).

Now that the package is installed, enable the Suricata.Service so that it will run when our system restarts. We can use the systemctl command to enable it:

```
hassnaee@hassnae: ~  
$ sudo systemctl stop suricata.service
```

## 3. Configuration of Suricata

Suricata can include a Community ID field in its JSON output to make it easier to match individual event records to records in datasets generated by other tools.

To enable the option, we open /etc/suricata/suricata.yaml using nano editor:

```
hassnaee@hassnae: ~  
$ sudo nano /etc/suricata/suricata.yaml
```

```
# Community Flow ID  
# Adds a 'community_id' field to EVE records. These are meant to give  
# records a predictable flow ID that can be used to match records to  
# output of other tools such as Zeek (Bro).  
#  
# 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
```

## Determining Which Network Interface(s) To Use:

To determine the device name of our default network interface, we can use the ip command as follows:

- `ip -p -j route show default`

```
(hasnaee@hasnaee)-[~]
$ ip -p -j route show default
[ {
  "dst": "default",
  "gateway": "192.168.1.1",
  "dev": "eth0",
  "protocol": "dhcp",
  "prefsrc": "192.168.1.108",
  "metric": 100,
  "flags": [ ]
} ]
```

The dev line indicates the default device. In this example output, the device is the highlighted eth0 interface.

Now we can edit Suricata's configuration and verify or change the interface name.

We Open the /etc/suricata/suricata.yaml configuration file using nano or your preferred editor:

```
# Linux high speed capture support
af-packet:
- interface: eth0
  # 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 > 4.1
  # possible value are:
  # * cluster_flow: all packets of a given flow are sent to the same socket.
  # * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
  # * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
  # socket. Requires at least Linux 3.14.
  # * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf-xdp.rst for
  # more info.
  # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on system
```

A command like the following will notify the Suricata process to reload its rulesets, without restarting the process:

```
(hasnaee@hasnaee)-[~]
$ sudo kill -usr2 $(pidof suricata)
```

## 4. Updating Suricata Rulesets

```
--(hasnaee@hasnaee)-[~]
$ sudo suricata-update
3/8/2024 -- 15:19:33 -- <Info> -- Using data-directory /var/lib/suricata.
3/8/2024 -- 15:19:33 -- <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
3/8/2024 -- 15:19:33 -- <Info> -- Using /etc/suricata/rules for Suricata provided rules.
3/8/2024 -- 15:19:33 -- <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
3/8/2024 -- 15:19:33 -- <Info> -- Loading /etc/suricata/suricata.yaml
3/8/2024 -- 15:19:33 -- <Info> -- Disabling rules for protocol ppsql
3/8/2024 -- 15:19:33 -- <Info> -- Disabling rules for protocol modbus
3/8/2024 -- 15:19:33 -- <Info> -- Disabling rules for protocol dnp3
3/8/2024 -- 15:19:33 -- <Info> -- Disabling rules for protocol enip
3/8/2024 -- 15:19:33 -- <Info> -- No sources configured, will use Emerging Threats Open
3/8/2024 -- 15:19:33 -- <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.6/emerging.rules.tar.gz.
100% - 4416734/4416734
3/8/2024 -- 15:19:45 -- <Info> -- Done.
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/dmnp-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/dmnp-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/http2-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/mqtt-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/quic-events.rules
3/8/2024 -- 15:19:46 -- <Info> -- Loading distribution rule file /etc/suricata/rules/rfb-events.rules
```

We can list the default set of rule providers using the list-sources flag to suricata-update like this:

Using the following command:

- `Sudo suricata-update list-sources`

```

23/8/2024 -- 15:19:56 -- <Info> -- Dropped 0 rules.
23/8/2024 -- 15:19:56 -- <Info> -- Enabled 136 rules for flowbit dependencies.
23/8/2024 -- 15:19:56 -- <Info> -- Backing up current rules.
23/8/2024 -- 15:19:57 -- <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 52097; enabled: 39663; added: 52097; removed 0; modified: 0
23/8/2024 -- 15:19:57 -- <Info> -- Writing /var/lib/suricata/rules/classification.config
23/8/2024 -- 15:19:59 -- <Info> -- Testing with suricata -T.
23/8/2024 -- 15:21:13 -- <Info> -- Done.

(hassnaee@hassnae)~$ sudo suricata-update list-sources
23/8/2024 -- 15:21:35 -- <Info> -- Using data-directory /var/lib/suricata.
23/8/2024 -- 15:21:35 -- <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
23/8/2024 -- 15:21:35 -- <Info> -- Using /etc/suricata/rules for Suricata provided rules.
23/8/2024 -- 15:21:35 -- <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
23/8/2024 -- 15:21:35 -- <Warning> -- Source index does not exist, will use bundled one.
23/8/2024 -- 15:21:35 -- <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
Subscriptions: 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: malsilo win-malware rules

```

```

Vendor: Status Networks
Summary: Newly Registered Domains Open only - 30 day list, complete
License: Commercial
Parameters: secret-code
Subscriptions: https://www.status-networks.com/status-labs/subscribe-to-threat-intel-feed
Name: status/nrd-entropy-14-open
Vendor: Status Networks
Summary: Newly Registered Domains Open only - 14 day list, high entropy
License: Commercial
Parameters: secret-code
Subscriptions: https://www.status-networks.com/status-labs/subscribe-to-threat-intel-feed
Name: status/nrd-entropy-30-open
Vendor: Status Networks
Summary: Newly Registered Domains Open only - 30 day list, high entropy
License: Commercial
Parameters: secret-code
Subscriptions: https://www.status-networks.com/status-labs/subscribe-to-threat-intel-feed
Name: status/nrd-phishing-14-open
Vendor: Status Networks
Summary: Newly Registered Domains Open only - 14 day list, phishing
License: Commercial
Parameters: secret-code
Subscriptions: https://www.status-networks.com/status-labs/subscribe-to-threat-intel-feed
Name: status/nrd-phishing-30-open
Vendor: Status Networks
Summary: Newly Registered Domains Open only - 30 day list, phishing
License: Commercial
Parameters: secret-code
Subscriptions: https://www.status-networks.com/status-labs/subscribe-to-threat-intel-feed
Name: tgreen/hunting
Vendor: tgreen
Summary: Threat hunting rules
License: GPLv3

```

to include the tgreen/hunting ruleset, we could enable it using the following command:

- `sudo suricata-update enable-source tgreen/hunting`

```

(hassnaee@hassnae)~$ sudo suricata-update enable-source tgreen/hunting
23/8/2024 -- 15:21:52 -- <Info> -- Using data-directory /var/lib/suricata.
23/8/2024 -- 15:21:52 -- <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
23/8/2024 -- 15:21:52 -- <Info> -- Using /etc/suricata/rules for Suricata provided rules.
23/8/2024 -- 15:21:52 -- <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
23/8/2024 -- 15:21:52 -- <Warning> -- Source index does not exist, will use bundled one.
23/8/2024 -- 15:21:52 -- <Warning> -- Please run suricata-update update-sources.
23/8/2024 -- 15:21:52 -- <Info> -- Creating directory /var/lib/suricata/update/sources
23/8/2024 -- 15:21:52 -- <Info> -- Enabling default source et/open
23/8/2024 -- 15:21:52 -- <Info> -- Source tgreen/hunting enabled

(hassnaee@hassnae)~$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 1
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. 39663 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 39666 signatures processed. 1169 are IP-only rules, 4112 are inspecting packet payload, 34176 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.

```

## 5. Running Suricata

### Start the Suricata Service:

Now we can start the Suricata server. Run the following systemctl command:

- `sudo systemctl start suricata-service`

we can examine the status of the service using the systemctl status command:

- `sudo systemctl status suricata.service`

```
(hassnaee@hassnae)-[~]
$ sudo systemctl start suricata.service

(hassnaee@hassnae)-[~]
$ sudo systemctl status suricata.service
suricata.service - Suricata IDS/IDP daemon
Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: disabled)
Active: active (running) since Fri 2024-08-23 15:23:32 CEST; 16s ago
Docs: man:suricata(8)
      man:suricata-sc(8)
      https://suricata.io/documentation/
Process: 22036 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid (code=exited, status=0/SUCCESS)
Main PID: 22037 (Suricata-Main)
Tasks: 1 (limit: 2229)
Memory: 137.3M (peak: 137.6M)
CPU: 14.341s
CGroup: /system.slice/suricata.service
        └─22037 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Aug 23 15:23:31 hassnae systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Aug 23 15:23:32 hassnae suricata[22036]: 1: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
Aug 23 15:23:32 hassnae systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
```

we can use the tail command to watch for a specific message in Suricata's logs that indicates it has finished starting:

```
(hassnaee@hassnae)-[~]
$ sudo tail -f /var/log/suricata/suricata.log
22028 - Suricata-Main] 2024-08-23 15:22:39 Info: detect: 39666 signatures processed. 1169 are IP-only rules, 4112 are inspecting packet payload, 34176 inspect application layer, 108 are decoded event only
22028 - Suricata-Main] 2024-08-23 15:23:22 Notice: suricata: Configuration provided was successfully loaded. Exiting.
22036 - Suricata-Main] 2024-08-23 15:23:32 Notice: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
22036 - Suricata-Main] 2024-08-23 15:23:32 Info: cpu: CPUs/cores online: 1
22036 - Suricata-Main] 2024-08-23 15:23:32 Info: suricata: Setting engine mode to IDS mode by default
22036 - Suricata-Main] 2024-08-23 15:23:32 Info: exception-policy: master exception-policy set to: auto
22036 - Suricata-Main] 2024-08-23 15:23:32 Info: ioctl: eth0: MTU 1500
22037 - Suricata-Main] 2024-08-23 15:23:32 Info: logopenfile: fast output device (regular) initialized: fast.log
22037 - Suricata-Main] 2024-08-23 15:23:32 Info: logopenfile: eve-log output device (regular) initialized: eve.json
22037 - Suricata-Main] 2024-08-23 15:23:32 Info: logopenfile: stats output device (regular) initialized: stats.log
22037 - Suricata-Main] 2024-08-23 15:24:10 Info: detect: 1 rule files processed. 39663 rules successfully loaded, 0 rules failed, 0
22037 - Suricata-Main] 2024-08-23 15:24:11 Info: threshold-config: Threshold config parsed: 0 rule(s) found
22037 - Suricata-Main] 2024-08-23 15:24:11 Info: detect: 39666 signatures processed. 1169 are IP-only rules, 4112 are inspecting packet payload, 34176 inspect application layer, 108 are decoded event only
22037 - Suricata-Main] 2024-08-23 15:25:00 Info: runmodes: eth0: creating 1 thread
22037 - Suricata-Main] 2024-08-23 15:25:01 Info: unix-manager: unix socket '/var/run/suricata-command.socket'
22037 - Suricata-Main] 2024-08-23 15:25:01 Notice: threads: Threads created -> W: 1 FM: 1 FR: 1 Engine started.
```

## 6. Testing Suricata Rules

### Execute a Test Request

To test Suricata's ability to detect suspicious traffic, we use the curl command to send an HTTP request that triggers a predefined rule:

```
(hassnaee@hassnae)-[~]
$ curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
```

### Examining /var/log/suricata/fast.log

To check for a log entry in /var/log/suricata/fast.log that corresponds to our curl request we use the grep command.

Using the 2100498-rule identifier from the QuickStart documentation, search for entries that match it using the following command:

- `Sudo grep 2100498 /var/log/suricata/fast.log`

```
(hassnaee@hassnae)-[~]
$ sudo grep 2100498 /var/log/suricata/fast.log
08/23/2024-15:55:40.133189 [*] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 18.154.22.58:80 -> 192.168.1.108:34108
```



## Examining /var/log/suricata/eve.log

Suricata also logs events to /var/log/suricata/eve.log (nicknamed the EVE log) using JSON to format entries.

The Suricata documentation recommends using the jq utility to read and filter the entries in this file. We Install jq if we don't have it on our system using the following apt command:

- Sudo apt install jq

```
(hassnae@hassnae)~$ sudo apt install jq
jq is already the newest version (1.7.1-3).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1065
```

Then, run:

```
(hassnae@hassnae)~$ sudo jq 'select(.alert.signature_id==2100498)' /var/log/suricata/eve.json
{
  "timestamp": "2024-08-23T15:55:40.133189+0200",
  "flow_id": 919486006414787,
  "in_iface": "eth0",
  "event_type": "alert",
  "src_ip": "18.154.22.58",
  "src_port": 80,
  "dest_ip": "192.168.1.108",
  "dest_port": 34108,
  "proto": "TCP",
  "pkt_src": "wire/pcap",
  "community_id": "1:mQGQ18eQmJYVOYLzRVslBAmPr8=",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2100498,
    "rev": 7,
    "signature": "GPL ATTACK_RESPONSE id check returned root",
    "category": "Potentially Bad Traffic",
    "severity": 2,
    "metadata": {
      "created_at": [
        "2010_09_23"
      ],
      "updated_at": [
        "2019_07_26"
      ]
    }
  },
  "http": {
    "hostname": "factunide.org"
  }
}
```

```
hassnae@hassnae: ~
"2019_07_26"
  ],
  "http": {
    "hostname": "testmyids.org",
    "url": "/uid/index.html",
    "http_user_agent": "curl/8.7.1",
    "http_content_type": "text/html",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 39
  },
  "files": [
    {
      "filename": "/uid/index.html",
      "gaps": false,
      "state": "CLOSED",
      "stored": false,
      "size": 39,
      "tx_id": 0
    }
  ],
  "app_proto": "http",
  "direction": "to_client",
  "flow": {
    "pkts_toserver": 5,
    "pkts_toclient": 4,
    "bytes_toserver": 429,
    "bytes_toclient": 810,
    "start": "2024-08-23T15:55:39.934980+0200",
    "src_ip": "192.168.1.108",
    "dest_ip": "18.154.22.58"
  }
}
```

```
    "http_content_type": "text/html",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 39
  },
  "files": [
    {
      "filename": "/uid/index.html",
      "gaps": false,
      "state": "CLOSED",
      "stored": false,
      "size": 39,
      "tx_id": 0
    }
  ],
  "app_proto": "http",
  "direction": "to_client",
  "flow": {
    "pkts_toserver": 5,
    "pkts_toclient": 4,
    "bytes_toserver": 429,
    "bytes_toclient": 810,
    "start": "2024-08-23T15:55:39.934980+0200",
    "src_ip": "192.168.1.108",
    "dest_ip": "18.154.22.58",
    "src_port": 34108,
    "dest_port": 80
  }
}
```

This output confirms that Suricata detected the traffic and generated an alert based on the specified rule.

