Suricata IDS Configuration and Tuning

Flowmon IDS Probe Version 1.0.0

Flowmon IDS Probe package integrates 3rd party open-source project Suricata IDS to the Flowmon platform with community rules. This package is provided free of charge and the Flowmon IDS Probe is not covered by Flowmon support service.

This document contains basic instructions for adjusting Suricata IDS settings such as minimizing false positives and rules management.

For more information about Suricata IDS visit official documentation at https://suricata-ids.org/.

Note: After every modification, the IDS Probe should be restarted to apply changes.

Table of Contents

False positive tuning with “suppress"

https://suricata.readthedocs.io/en/suricata-4.0.5/configuration/global-thresholds.html#suppress

When too many uninteresting events are displayed, we can suppress any of them in threshold configuration file saved as **`/data/idsp/threshold.config`**.

Syntax of suppress rule follows: **`suppress gen_id <gid>, sig_id <sid>`**

If we want to suppress one or more IP addresses in specific signature, we can do it with suppress rule:

`suppress gen_id <gid>, sig_id <sid>, track <by_src|by_dst|by_either>, ip <ip|subnet|addressvar>`

To select all signatures or all groups, select **`sig_id 0`** or **`gen_id 0`**.

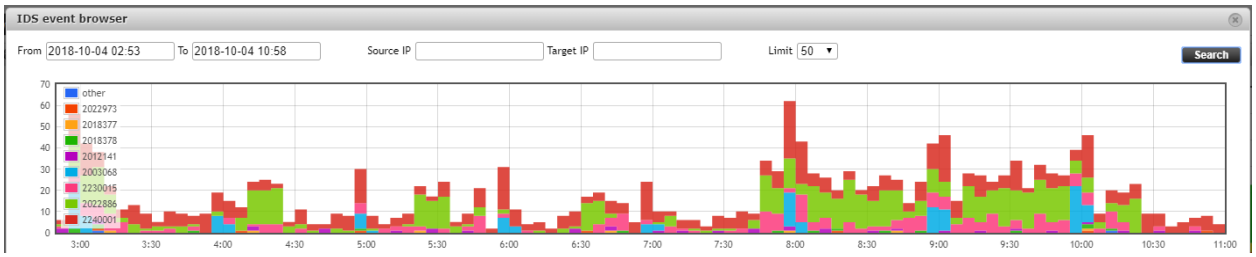
Log in as user flowmon to IDS probe.

`vim /data/idsp/threshold.config`

Write **`suppress gen_id 1, sig_id 2022886`**

Restart IDS Probe (in FCC/Versions Stop and Start IDS Probe package).

See the result in the dashboard:



For example, in our environment, signature 2022886 was generating too many events, so we suppressed it with **`suppress gen_id 1, sig_id 2022886`** in **`/data/idsp/threshold.config`** file.

Signature 2022886 is displayed in green and as we can see after 10:25 when we processed the suppress, this event is no longer displayed.

Setup of network variables in Suricata config file

It helps to describe networks as variables which can be used for suppression or rule setup.

https://suricata.readthedocs.io/en/suricata-4.0.5/configuration/suricata-yaml.html#rule-vars
IP addresses can be defined as variables, set at the beginning of **`/data/idsp/suricata.yaml`** file.

Log in as user flowmon to IDS probe.

`vim /data/idsp/suricata.yaml`
Set some variables, you can also use negation: **`EXTERNAL_NET : "!$HOME_NET"`**
Now you can use these variables in rules or suppress commands.

Example:
`suppress gen_id 1, sig_id 0, track by_src, ip $EXTERNAL_NET`
This rule suppresses events, where source IP addresses are from the external network.

Restart IDS Probe (in FCC/Versions Stop and Start IDS Probe package).

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

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

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

  port-groups:
    HTTP_PORTS: "80"
    SHELLCODE_PORTS: "!80"
    ORACLE_PORTS: 1521
    SSH_PORTS: 22
    DNP3_PORTS: 20000
    MODBUS_PORTS: 502
    FILE_DATA_PORTS: "[$HTTP_PORTS,110,143]"
    FTP_PORTS: 21
```

Figure: list of variables in suricata.yaml file

Suricata rules management

https://suricata.readthedocs.io/en/suricata-4.0.5/configuration/suricata-yaml.html#rule-files
The path to rule files for Suricata must be added to suricata.yaml file, so it knows where it can find the .rules files and which of them it can use.

List of rules with signatures

Rules can be found here: **`/data/idsp/rules`**

Enable or disable rule

Log in as user flowmon to IDS probe.

`vim /data/idsp/suricata.yaml`
The default path is set, you can set other paths to specific rules (then the default path will be ignored to this one rule).

Example with new rule in different path:

- **`/example/rules/mynewrules.rules`**

```
##
## Step 2: select the rules to enable or disable
##

default-rule-path: /data/idsp/rules
rule-files:
 - botcc.rules
 # - botcc.portgrouped.rules
 - ciarmy.rules
 - compromised.rules
 - drop.rules
 - dshield.rules
# - emerging-activex.rules
 - emerging-attack_response.rules
 - emerging-chat.rules
 - emerging-current_events.rules
 - emerging-dns.rules
 - emerging-dos.rules
 - emerging-exploit.rules
 - emerging-ftp.rules
# - emerging-games.rules
# - emerging-icmp_info.rules
# - emerging-icmp.rules
 - emerging-imap.rules
# - emerging-inappropriate.rules
# - emerging-info.rules
 - emerging-malware.rules
 - emerging-misc.rules
```

```
 - emerging-mobile_malware.rules
 - emerging-netbios.rules
 - emerging-p2p.rules
 - emerging-policy.rules
 - emerging-pop3.rules
 - emerging-rpc.rules
# - emerging-scada.rules
# - emerging-scada_special.rules
 - emerging-scan.rules
# - emerging-shellcode.rules
 - emerging-smtp.rules
 - emerging-snmp.rules
 - emerging-sql.rules
 - emerging-telnet.rules
 - emerging-tftp.rules
 - emerging-trojan.rules
 - emerging-user_agents.rules
 - emerging-voip.rules
 - emerging-web_client.rules
 - emerging-web_server.rules
# - emerging-web_specific_apps.rules
 - emerging-worm.rules
 - tor.rules
# - decoder-events.rules # available in suricata sources under rules dir
# - stream-events.rules  # available in suricata sources under rules dir
 - http-events.rules    # available in suricata sources under rules dir
 - smtp-events.rules    # available in suricata sources under rules dir
 - dns-events.rules     # available in suricata sources under rules dir
 - tls-events.rules     # available in suricata sources under rules dir
# - modbus-events.rules  # available in suricata sources under rules dir
# - app-layer-events.rules  # available in suricata sources under rules dir
# - dnp3-events.rules       # available in suricata sources under rules dir
# - ntp-events.rules       # available in suricata sources under rules dir
# - local.rules
```

Add a new online source with signatures (rules)

When we want to use rules from external sources, we need to add URL to these files to **`oinkmaster.config`** file.

`vim /data/idsp/oinkmaster.conf`

```
# URL examples follows. Replace <oinkcode> with the code you get on the
# Snort site in your registered user profile.

url = https://services.flowmon.com/rules/public/emerging.rules.tar.gz

# Example for Snort 2.4
# url =
http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode>/snortrules-snapshot-2.4.tar.gz
```

GID - Group/Generator ID

We can set gid when creating for example new rule or prepare copy of some rule for test purpose. Default gid is 1 for all rules, the new one must be greater than 1 000 000.

Then you can use the gid to suppress rules.

```
alert tls any any -> any any (msg:"SURICATA TLS invalid record version"; flow:established;
app-layer-event:tls.invalid_record_version; flowint:tls.anomaly.count,+,1;
classtype:protocol-command-decode; gid:1000001; sid:2230015; rev:1;)
```

Suricata IDS Probe restart

After each configuration change the IDS Probe should be restarted.
(in **FCC/Versions** Stop and Start IDS Probe package)