**Suricata - Feature #1979**

**TCP/IP packets normalization/scrubbing**

12/08/2016 02:56 AM - op suri

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>high</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

Snort is capable of normalizing network traffic see: [https://snort.org/faq/readme-normalize](https://snort.org/faq/readme-normalize)

For example if one wants clear the reserved bits in the TCP header, in Snort this would be possible using the following:

preprocessor normalize_tcp: [rsv]

I am convinced that TCP/IP packets normalization is possible in Suricata, but I don't know where to configure it.

Can you please help me?

Thank you.

**History**

#1 - 12/08/2016 03:00 AM - Victor Julien
- Priority changed from High to Normal
- Target version deleted (3.2.1)

#2 - 12/08/2016 03:08 AM - Victor Julien
- Subject changed from TCP/IP packets normalization to TCP/IP packets normalization/scrubbing
- Target version set to TBD

Suricata does not (yet) have a packet normalization/scrubbing feature.

#3 - 12/08/2016 03:17 AM - op suri

Thank you for your reply.

Since you mentioned that suricata does not (yet) have a packet scrubbing feature, is there any short term plan to implement it?

#4 - 12/08/2016 03:51 AM - Victor Julien

There are no plans for it at this time. Perhaps you or someone else in the community can take on the effort.

#5 - 12/12/2016 02:41 PM - op suri

I understand that suricata does not have the normalization feature.

Your advice is appreciated to the following problem

1) I have a suricata up and running with rules generating alerts.

2) "abnormal" TCP/IP traffic/packets was identified based on rules.

3) From what I do see as features on suricata is: drop (reject), pass, alert

4) GOAL: is to clear some fields on packets instead of dropping the whole packets/traffic

**Question:** Is Suricata capable of 4)? if not what is your recommendation to reach this goal?
Thank you in advance

#6 - 12/13/2016 05:13 AM - Victor Julien
No, not at this time.

#7 - 07/13/2018 08:08 PM - Victor Julien
- Effort set to high
- Difficulty set to medium

#8 - 03/11/2019 02:42 PM - Victor Julien
- Assignee set to Community Ticket