Suricata - Feature #3292
support for network service header (NSH)
11/01/2019 03:45 PM - Andreas Herz

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Carl Smith</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>7.0rc1</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td>Protocol</td>
</tr>
</tbody>
</table>

Description
First part would be a dedicated protocol parser for NSH.
Second part would be to have some sort of integration within the engine based on the metainformation we receive from the NSH. One example might be deciding which tenant to use.
Another option for inline mode would be to add a flag to the packet that has been analyzed so another hop can investigate it.

Related issues:
Related to Task #3288: Suricon 2019 brainstorm

History
#1 - 11/02/2019 08:54 AM - Victor Julien
For this ticket we will need actual use cases with pcaps and a description of the expected outcome.

#2 - 11/05/2019 10:53 AM - Victor Julien
- Status changed from New to Feedback
- Parent task deleted (#3288)

#3 - 11/05/2019 10:53 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added

#4 - 01/30/2020 11:53 AM - Victor Julien
- Label Protocol added

#5 - 12/03/2020 06:56 AM - Victor Julien
- Status changed from Feedback to In Review
- Assignee changed from Community Ticket to Carl Smith
- Target version changed from TBD to 7.0rc1

https://github.com/OISF/suricata/pull/5309

#6 - 12/31/2020 12:16 PM - Victor Julien
- Status changed from In Review to Closed

https://github.com/OISF/suricata/pull/5309
https://github.com/OISF/suricata-verify/pull/392