**Suricata - Feature #4148**

**Research: SSH Support for additional protocol analysis**

11/14/2020 02:40 PM - Jeff Lucovsky

<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>
</tbody>
</table>

**Description**

Chris G:

Is there any additional work we can do in SSH protocol analysis? Corelight's article on SSH Inference was very interesting, though I'm not how well it works in reality. [https://corelight.blog/2019/11/19/corelight-ssh-inference-package/](https://corelight.blog/2019/11/19/corelight-ssh-inference-package/)

This could extend to other protocols

**Related issues:**

Related to Task #4097: Suricon 2020 brainstorm

**History**

#1 - 11/14/2020 02:40 PM - Jeff Lucovsky
- Related to Task #4097: Suricon 2020 brainstorm added

#2 - 11/19/2020 09:12 PM - Victor Julien
- Subject changed from Research: Support for additional protocol analysis to Research: SSH Support for additional protocol analysis
- Assignee set to Community Ticket
- Target version set to TBD

I think we first need a description of what is missing and could be added to our SSH parser and/or detection.

#3 - 12/24/2020 07:06 AM - Victor Julien
- Label Protocol added