Suricata - Feature #2698
hassh and hasshServer for ssh fingerprinting
11/21/2018 11:50 AM - Victor Julien

<table>
<thead>
<tr>
<th>Status</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee</td>
<td>Mats Klepsland</td>
</tr>
<tr>
<td>Category</td>
<td>Protocol</td>
</tr>
<tr>
<td>Target version</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty</td>
<td>medium</td>
</tr>
</tbody>
</table>

Description
As discussed at Suricon2018, it would be great to have JA3 for non-https as well. This ticket is for SSH.
The SSH parser currently doesn't really inspect the handshake, so it will be a bit of work probably.

Related issues:
- Related to Task #2685: SuriCon 2018 brainstorm
- Blocked by Feature #3445: Convert SSH parser to Rust

History
#1 - 11/21/2018 11:50 AM - Victor Julien
- Related to Task #2685: SuriCon 2018 brainstorm added

#2 - 11/21/2018 11:57 AM - Mats Klepsland
The JA3 equivalent for SSH is called hassh (and hasshServer for JA3s):
https://github.com/salesforce/hassh
It would force me to learn some Rust, so it's a nice little project I think :)

#3 - 11/21/2018 11:57 AM - Mats Klepsland
- Subject changed from ja3/ja3s for ssh to hassh and hasshServer for ssh fingerprinting

#4 - 01/27/2020 03:35 PM - Victor Julien
- Blocked by Feature #3445: Convert SSH parser to Rust added

#5 - 01/30/2020 01:44 PM - Victor Julien
- Label Protocol added

#6 - 04/06/2020 02:04 PM - Vadym Malakhatko
Developed a fully functional version of "hassh" on top of Feature #3445 branch (ssh-rust-v12), will rebase after ssh conversion will be finished.
https://github.com/MalakhatkoVadym/suricata/tree/hassh-feature-2698-v1

#7 - 05/06/2020 11:55 PM - Vadym Malakhatko
Updated hassh on top of ssh-rust-v19
https://github.com/MalakhatkoVadym/suricata/tree/hassh-feature-2698-v1