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

Status: Closed
Priority: Normal
Assignee: Vadym Malakhatko
Category: 
Target version: 6.0.0beta1
Effort: 
Difficulty: 
Label: Protocol

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-hassh/tree/hassh-feature-2698-v1

#8 - 07/07/2020 08:22 PM - Victor Julien
- Status changed from Assigned to Closed
- Assignee changed from Mats Klepsland to Vadym Malakhatko
- Target version changed from TBD to 6.0.0beta1
- Effort deleted (medium)
- Difficulty deleted (medium)

https://github.com/OISF/suricata/pull/5141