Suricata - Feature #1977
get the os info from TCP HTTP fingerprint
12/06/2016 09:42 AM - wilson green

Status: New
Priority: Low
Assignee: Community Ticket
Category: 
Target version: TBD
Effort: medium
Difficulty: high

Description
can suricata get the OS from the TCP/SYN fingerprint just like p0f.

History
#1 - 12/13/2016 05:12 AM - Victor Julien
  - Priority changed from Normal to Low
  - Target version set to TBD

Not at this time. There has been some discussion about how useful it would be for automatically setting the OS for target based reassembly for example. Consensus at SuriConDC seemed to be that it's low priority.

#2 - 05/03/2017 04:08 PM - Andreas Herz
  - Assignee set to Anonymous

#3 - 06/12/2018 05:36 PM - Jason Ish
  - Effort set to medium
  - Difficulty set to high

#4 - 02/23/2019 10:19 PM - Andreas Herz
  - Assignee set to Community Ticket