Suricata - Feature #2562
Add http_port in http eve-log if specified in the hostname
08/03/2018 12:50 PM - Maurizio Abba

Status: Closed
Priority: Normal
Assignee: Maurizio Abba
Category:
Target version: 4.1rc2
Effort: low
Difficulty: low

Description
This proposed patch adds a single element in a http json object, adding the port to the "http" object with the key "http_port". Note that this item will be set only if the port is set in the hostname and it's not grabbed from the TCP flow.

Attached a pcap with the http port 1337 (as evident, the flow is actually on TCP port 80, but the hostname has port 1337 => "dest_port": will be set to 80, while http.http_port will be set to 1337).

History
#1 - 08/21/2018 02:54 PM - Victor Julien
- Status changed from New to Closed
- Target version set to 4.1rc2

https://github.com/OISF/suricata/pull/3454

Files
2008-weirdport.pcap 1.48 KB 08/03/2018 Maurizio Abba