Suricata - Bug #652
TCP sessions cleaned up prematurely
12/01/2012 05:39 PM - Ludovico Cavedon

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category:
Target version: 1.4
Affected Versions:
Effort:
Difficulty:
Label:

Description
If one TCP endpoint closes the connection, but there are still TCP segments on the network that have not been received yet by suricata, these segments might not be processed.

The following patch delays the cleanup until the FIN form both side has been seen:
https://github.com/cavedon/suricata/commit/ac8b08771770ab0f0f5112c84c499771f5f7b746e

This applies both to the master and the master-1.3.x branches.

History
#1 - 12/01/2012 05:40 PM - Ludovico Cavedon
Pull request:
https://github.com/inliniac/suricata/pull/233

#2 - 12/03/2012 02:44 AM - Victor Julien
Can you share a pcap showing how this leads to problems?

#3 - 12/07/2012 09:13 AM - Victor Julien
- Status changed from New to Closed
- Assignee set to Victor Julien
- Target version set to 1.4

I've applied this to the master with a small addition: send eof on pseudo packets as well. Saw some missing logs in the http.log otherwise.

This has led me to the conclusion that it's a pretty major change that needs some more testing. So holding off on the 1.3 branch for now.