Suricata - Feature #2375
Design and implement sensible per-thread capabilities
12/18/2017 05:12 PM - Richard Sailer

Status: New
Priority: Normal
Assignee: OISF Dev
Category: 
Target version: 7.0beta1
Effort: medium
Difficulty: low

Description
It would be a good security improvement if threads could only do what they need to do. (e.g. A thread that does not need to write to disk also has no capability to do so, etc.). And linux capabilities are a per-thread attribute (man attributes)

This would contain at least the following subtasks:

- Define sensible capability sets for individual thread modules
- check out SCDropCaps() and the libcap-ng bug, which prevented this feature earlier (still there?)
- Implement mechanics to declare and set needed capabilities per thread module
- What to do if a thread changes its thread modules? Can this happen?

This maybe is a bigger change and lots of work, but I would like to do it, so I flagged it low priority and TBD. Any thoughts on this?

And I should note: this would be linux only since capabilities are a linux feature. FreeBSD has something related called capsicum, but the library we use (libcap-ng) is linux only.

Related issues:
Related to Feature #276: Libcap support for dropping privileges

History
#1 - 12/18/2017 05:23 PM - Richard Sailer
- Description updated

#2 - 12/18/2017 05:24 PM - Richard Sailer
- Description updated

#3 - 12/19/2017 02:21 AM - Victor Julien
Basic infra is already in place, see for example source-pfing.c


#4 - 12/19/2017 02:22 AM - Victor Julien
- Related to Feature #276: Libcap support for dropping privileges added

#5 - 12/19/2017 02:25 AM - Victor Julien
- Assignee changed from Richard Sailer to Anonymous

#6 - 07/13/2018 06:28 PM - Victor Julien
- Effort set to medium
- Difficulty set to low

#7 - 02/23/2019 10:05 PM - Andreas Herz
When we first tried this years ago it turned out not to work, I believe due to a bug in libcap-ng. I'm hopeful we can get it to work now.

Target version changed from 6.0.0rc1 to 7.0beta1