Suricata - Optimization #2843

suricatact/filestore/prune: check that directory is a filestore directory before removing files

02/21/2019 03:10 PM - Jason Ish

| Status:    | Closed          |
| Priority:  | High            |
| Assignee:  | Shivani Bhardwaj|
| Category:  |                |
| Target version: | 5.0rc1         |
| Effort:    |                |

Description
Currently the filestore prune command will attempt to prune whatever directory it is given. I think some simple validation should be done. This could be as simple as looking for the directories "00", "ff" and "tmp" as these are all expected to exist in a filestore directory created by suricata.

History

#1 - 02/25/2019 01:07 PM - Victor Julien
- Status changed from New to Assigned

#2 - 04/08/2019 11:09 AM - Victor Julien
- Priority changed from Normal to High

#3 - 04/23/2019 08:58 AM - Shivani Bhardwaj
- Status changed from Assigned to Feedback

#4 - 04/29/2019 07:44 AM - Victor Julien
- Target version changed from 5.0beta1 to 5.0rc1

#5 - 07/01/2019 10:27 AM - Shivani Bhardwaj
PR: https://github.com/OISF/suricata/pull/3799

#6 - 09/11/2019 06:56 AM - Shivani Bhardwaj
- Status changed from Feedback to Closed

Fixed with: https://github.com/OISF/suricata/commit/ba6b73cd106aaa7fd53e4f1867fe7ce44b3bc2c7