Suricata - Feature #1125
smtp: improve protocol detection
03/06/2014 04:21 AM - Victor Julien

Status: In Review
Priority: Normal
Assignee: Philippe Antoine
Category: 
Target version: 7.0rc1
Effort: 
Difficulty: 

Label:

Description
Currently SMTP is only detected if the client starts the conversation with HELO, EHLO or QUIT.
The server stream is not used for protocol detection.

Related issues:
- Related to Bug #2978: IRC traffic parsed by FTP
- Related to Feature #2757: improve protocol detection
- Blocked by Feature #2572: extend protocol detection to specify flow direction

History
#1 - 11/08/2015 04:02 AM - Victor Julien
- Target version changed from 3.0RC2 to 70

#2 - 07/17/2018 08:44 AM - Victor Julien
- Assignee changed from Tom DeCanio to OISF Dev

#3 - 08/09/2018 07:46 AM - Victor Julien
- Blocked by Feature #2572: extend protocol detection to specify flow direction added

#4 - 11/28/2018 07:09 AM - Victor Julien
- Priority changed from Normal to High

#5 - 12/21/2018 12:07 PM - Victor Julien
- Related to Feature #2757: improve protocol detection added

#6 - 02/18/2019 08:13 AM - Victor Julien
- Priority changed from High to Normal
- Target version changed from 70 to 5.0beta1

#7 - 02/25/2019 09:51 AM - Victor Julien
- Priority changed from Normal to High

#8 - 02/28/2019 10:39 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Philippe Antoine
- Priority changed from High to Normal

#9 - 04/25/2019 11:16 AM - Victor Julien
- Target version changed from 5.0beta1 to 5.0rc1

#10 - 06/06/2019 02:04 PM - Philippe Antoine
- Related to Bug #2978: IRC traffic parsed by FTP added
#11 - 09/09/2019 06:08 PM - Victor Julien
- Target version changed from 5.0rc1 to 6.0.0beta1

#12 - 02/18/2020 12:52 PM - Philippe Antoine
- Related to deleted (Feature #2757: improve protocol detection)

#13 - 02/18/2020 12:53 PM - Philippe Antoine
- Blocked by Feature #2757: improve protocol detection added

#14 - 04/10/2020 12:53 PM - Philippe Antoine
- Status changed from Assigned to Feedback
Waiting first for feedback on other related tickets

#15 - 07/13/2020 08:49 AM - Philippe Antoine
Waiting for feedback on https://redmine.openinfosecfoundation.org/issues/2757 before upgrading
https://github.com/OISF/suricata/pull/3832
https://github.com/OISF/suricata-verify/pull/53

#16 - 08/05/2020 12:04 PM - Victor Julien
- Target version changed from 6.0.0beta1 to 7.0rc1

#17 - 06/28/2022 02:04 PM - Philippe Antoine
Both FTP and SMTP start with 220 from server (followed by either space or hyphen)
For SMTP, it is then supposed to be a valid domain name.
But there is no restriction for FTP
There can be (E)SMTP or FTP in the banner...
We can use the ports.
And we can maybe mark this detection as weak, so that client side detection overrides it...

#18 - 06/28/2022 07:50 PM - Philippe Antoine
- Status changed from Feedback to In Review
https://github.com/OISF/suricata/pull/7578

#19 - 07/06/2022 12:38 PM - Philippe Antoine
- Blocked by deleted (Feature #2757: improve protocol detection)

#20 - 07/06/2022 12:38 PM - Philippe Antoine
- Related to Feature #2757: improve protocol detection added