Suricata - Task #3485

Research: check SSH parsing end of banner

02/18/2020 08:17 AM - Philippe Antoine

Status: New
Priority: Normal
Assignee:
Category:
Target version:
Effort:
Difficulty:
Label:

Description
Follows conversation on https://github.com/OISF/suricata/pull/4546#discussion_r378704002

I am not sure that SSH parser should accept single CR as end of banner, but that is what is being done by the C parser. This is enforced by the unit tests:
https://github.com/OISF/suricata/blob/master/src/app-layer-ssh.c#L2222

This is something to test against real implementations.

OpenSSH does not accept CR as end of banner:
https://github.com/openssh/openssh-portable/blob/master/ssh_api.c#L345
It only accepts LF and CRLF

Related issues:
Related to Feature #3445: Convert SSH parser to Rust

Closed

History

#1 - 02/18/2020 08:47 AM - Victor Julien
- Tracker changed from Bug to Task
- Subject changed from Check SSH parsing end of banner to Research: check SSH parsing end of banner

#2 - 02/20/2020 12:40 PM - Philippe Antoine
Wa can also test for 0 or 1-length SSH records (not containing message code) cf https://github.com/OISF/suricata/pull/4546#discussion_r378704320

#3 - 05/25/2020 03:22 PM - Victor Julien
- Parent task deleted (#3445)

#4 - 05/25/2020 03:22 PM - Victor Julien
- Related to Feature #3445: Convert SSH parser to Rust added