When an event logging is triggered by the flow cleaning function, the timestamp is invalid as it is often set to a time that is before the flow start.

Related issues:
Copied to Bug #5056: invalid timestamp in ending events

History
#1 - 02/03/2022 10:59 AM - Eric Leblond
- File smb-2-sessions.pcap added

    When replaying with -r the attached pcap that contains 2 smb sessions, we got a series of SMB records. If we take one of the session(where we have a logoff) and sort the event by time, we got the following

    cat /tmp/smb-2/eve.json | jq 'select(.event_type=="smb" and .smb.session_id==4398180728949)|{"time": .timestamp, "command":.smb.command} | sort

    "time":"2021-06-30T20:28:32.664884+0200","command":"SMB2_COMMAND_SESSION_LOGOFF"
    "time":"2021-06-30T22:52:21.504749+0200","command":"SMB2_COMMAND_SESSION_SETUP"
    "time":"2021-06-30T22:52:21.504964+0200","command":"SMB2_COMMAND_TREE_CONNECT"
    "time":"2021-06-30T22:52:21.700998+0200","command":"SMB2_COMMAND_IOCTL"
    "time":"2021-06-30T22:52:31.921537+0200","command":"SMB2_COMMAND_TREE_DISCONNECT"

    So the logoff of the session comes 24 seconds before the setup of the same session.

    By using lastts as timestamp in pseudo packet as done in https://github.com/OISF/suricata/pull/6921 we got

    "time":"2021-06-30T22:52:21.504749+0200","command":"SMB2_COMMAND_SESSION_SETUP"
    "time":"2021-06-30T22:52:21.504964+0200","command":"SMB2_COMMAND_TREE_CONNECT"
    "time":"2021-06-30T22:52:21.700998+0200","command":"SMB2_COMMAND_IOCTL"
    "time":"2021-06-30T22:52:31.921537+0200","command":"SMB2_COMMAND_TREE_DISCONNECT"
    "time":"2021-06-30T22:52:31.921736+0200","command":"SMB2_COMMAND_SESSION_LOGOFF"

#2 - 02/08/2022 02:13 PM - Jeff Lucovsky
- Copied to Bug #5056: invalid timestamp in ending events added

Files
smb-2-sessions.pcap 28.7 KB 02/03/2022