Suricata - Bug #5032
Suricata throwing wrong seq number alert when packets are only reordered
02/01/2022 05:46 PM - Lukas Sismis

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

Description
I've been experimenting with Suricata and it seems to me that Suricata outputs many false alerts about incorrect 3-way handshake SEQ numbers. I am attaching a PCAP to demonstrate the mentioned cases.

So in the PCAP, there is a conversation on port 40982 where packet number 1590 initiates conversation (SYN). Then the next packet in the PCAP is not the ordinary SYN,ACK, instead it is ACK of the SYN,ACK that is yet to come. Packet #1803 generates the first alert regarding the wrong SEQ number. All the remaining packets are then flagged with an incorrect SEQ number alert.

The traffic in the PCAP is mixed as Suricata sometimes did not generate alerts when there was only the conversation on port 40982. This would indicate that Suricata can reorder the packets correctly with a smaller number of packets but not when the traffic is mixed with other streams. This case happened only when I was replaying the traffic onto Suricata. Interestingly, reading the PCAP offline always leads to the aforementioned alerts.

As soon as Suricata gets misaligned on SEQ numbers, it keeps throwing alerts on all remaining packets of the conversation.

Triggered alert rule:
alert tcp any any -> any any (msg:"SURICATA STREAM 3way handshake wrong seq wrong ack";
stream-event:3whs_wrong_seq_wrong_ack; classtype:protocol-command-decode; sid:2210010; rev:2;)

I am using compiled Suricata master.

History
#1 - 02/02/2022 07:07 AM - Victor Julien
I think this behavior is correct. Suricata evaluates the traffic as it is on the wire and this is broken TCP. It's most like an artifact of some capture weirdness. But a real TCP session would not use this pattern, so Suricata flags it as suspicious.

#2 - 02/02/2022 10:58 AM - Lukas Sismis
I should have noted that I was using DPDK so there is no TCP stack to receive and reorder the packets to the correct order.

I am not a TCP expert but I thought that TCP segments can come out of order. That is also why I thought TCP reassembly exist. But handshakes can be a different story based on the fact that it initiates the connection. However, Wireshark does not complain about a broken TCP stream.

The PCAP was indeed captured, if you believe that Suricata behaves correctly then I am ok with closing the issue.

Files
3wayhs-small.pcap
2.86 MB
02/01/2022
Lukas Sismis

03/07/2022 1/1