Suricata - Feature #962
Can I log the mac address of the source?

Status: Assigned
Priority: Normal
Assignee: Sascha Steinbiss
Category:
Target version: Soon
Effort:
Difficulty:

Description
Knowing the mac address can help us about knowing the attacker. So can suricata log the mac address? Like the -e option in snort? Thanks for help.

Related issues:
- Related to Task #2309: SuriCon 2017 brainstorm
- Related to Bug #1711: Ethernet Header Missing From JSON Packet Field

History
#1 - 09/16/2013 10:33 AM - Victor Julien
We don't have a similar option. How are the mac addresses logged with -e in Snort?

#2 - 10/26/2013 10:21 AM - Victor Julien
- Target version set to TBD

#3 - 01/03/2014 12:52 AM - Song Liu
In NFQ mode, we don't have MAC address, because it is layer 3.

#4 - 02/16/2016 04:01 PM - Andreas Herz
That's a feature request. Did anyone already looked into that? I did just test it with snort in sniffer mode (-vCd -i $DEVICE -e) which we don't have exactly, but could be useful in normal IDS mode as well.

#5 - 02/16/2016 04:01 PM - Andreas Herz
- Tracker changed from Support to Feature
- Assignee set to OISF Dev

#6 - 11/28/2017 08:51 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Eric Leblond
- Target version changed from TBD to Soon

#7 - 12/01/2017 05:12 AM - Victor Julien
- Related to Task #2309: SuriCon 2017 brainstorm added

#8 - 04/14/2018 07:23 AM - Victor Julien
At the team meeting in Amsterdam 2018 we agreed on the following:

for packets, log mac src/dst as a scalar field in eve
for flows, log mac src/dst as lists in eve
field names should be different to avoid type confusion (e.g. src_mac vs src_macs?)

Alerts will log based on packet, but can add mac addrs from flow too.

#9 - 11/16/2018 10:26 PM - Raymond Hansen
- Assignee changed from Eric Leblond to Sascha Steinbiss

#10 - 07/22/2019 11:08 AM - Victor Julien
- Related to Bug #1711: Ethernet Header Missing From JSON Packet Field added

#11 - 03/02/2020 05:25 PM - Sascha Steinbiss
Just taking a look at this atm.

    for packets, log mac src/dst as a scalar field in eve
    for flows, log mac src/dst as lists in eve
    field names should be different to avoid type confusion (e.g. src_mac vs src_macs?)

    Alerts will log based on packet, but can add mac addrs from flow too.

I am wondering how to decide whether something is to be logged as flow or packet. Would it be enough to look at p->flow in CreateJSONHeader and see if the *pktcnt values there indicate >1 packet?

Also, am I correct in assuming that in order to log a list of MAC addresses, one would need to gather and update that during packet->flow assignment? Can you suggest a good suitable place to do that in the code? FlowHandlePacketUpdate?

Thanks!

#12 - 03/03/2020 02:15 PM - Sascha Steinbiss
Sascha Steinbiss wrote in #note-11:

    Just taking a look at this atm.

    for packets, log mac src/dst as a scalar field in eve
    for flows, log mac src/dst as lists in eve
    field names should be different to avoid type confusion (e.g. src_mac vs src_macs?)

    Alerts will log based on packet, but can add mac addrs from flow too.

I am wondering how to decide whether something is to be logged as flow or packet. Would it be enough to look at p->flow in CreateJSONHeader and see if the *pktcnt values there indicate >1 packet?

Also, am I correct in assuming that in order to log a list of MAC addresses, one would need to gather and update that during packet->flow assignment? Can you suggest a good suitable place to do that in the code? FlowHandlePacketUpdate?

I think I've at least found a starting point: https://github.com/satta/suricata/commit/ac09ed3d3b85c76c0bb38795efeb0ab11466f67b