Suricata - Feature #1750

Set Suricata to listen to all network interfaces when using AF_PACKET

03/22/2016 06:05 AM - Lars Kulseng

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
</tbody>
</table>

Description

In a scenario where you have a lot of network interfaces, and not enough resources to start a Suricata instance for each interface, it would be beneficial to allow Suricata to listen to all ports at once.

This can be achieved by setting sll.sll_ifindex to 0 before binding to the interface with bind() [1]. When reading from the ring buffer, each frame will have the sockaddr_ll struct inside it, allowing for extraction of the interface that the frame came in on. [2]


History

#1 - 03/23/2016 02:52 AM - Victor Julien
- Target version set to TBD

#2 - 06/15/2016 05:09 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Eric Leblond

#3 - 08/08/2018 09:16 PM - Eric Leblond
- Assignee changed from Eric Leblond to Anonymous

#4 - 08/09/2018 06:01 AM - Victor Julien
- Status changed from Assigned to New
- Effort set to medium
- Difficulty set to medium

#5 - 02/23/2019 10:18 PM - Andreas Herz
- Assignee set to Community Ticket