Suricata - Feature #2923
suricata-verify: eve2test util

04/05/2019 02:21 PM - Victor Julien

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>High</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Shivani Bhardwaj</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>QA</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
The suricata-verify test.yaml contains a great way to create regression tests. However creating the test files is tedious. It usually involves taking a eve.json record and then manually creating a matching test.yaml.

I would like to have a small util script in python, that converts an eve.json to the test.yaml format.

Something like:

eve2test eve.json > test.yaml

Related issues:
Related to Task #3269: Script for creating test with params

Closed

History
#1 - 04/23/2019 08:59 AM - Shivani Bhardwaj
- Status changed from New to Assigned

#2 - 04/23/2019 12:36 PM - Shivani Bhardwaj
If I understand correctly, only the verification filters are run over `eve.json` so this utility should actually create just the `filter` block and write it in a test file. Developer may then provide all other options like min-version of Suricata, requires, etc. Please let me know.

#3 - 04/24/2019 01:55 PM - Victor Julien
Lets start that way, yes. We can consider adding more logic later, but this is the most valuable first step I think.

#4 - 05/27/2019 03:43 PM - Shivani Bhardwaj
- Status changed from Assigned to Feedback

#5 - 05/31/2019 09:28 AM - Peter Manev
Some very good reassembly/defrag/vlan corner cases could be found here - [https://github.com/pevma/PtP/blob/master/Examples/Example](https://github.com/pevma/PtP/blob/master/Examples/Example) with the actual pcaps and rules located here - [https://github.com/pevma/PtP/blob/master/Examples/PacifyOneHttpRequest.tar.gz](https://github.com/pevma/PtP/blob/master/Examples/PacifyOneHttpRequest.tar.gz). I think the utility would make it much easier to add those form the respective resulting eve.jsons into the suricata-verify.

#6 - 07/01/2019 10:31 AM - Shivani Bhardwaj
Unmerged, open for testing: [https://github.com/shivan1b/eve2test](https://github.com/shivan1b/eve2test)

#7 - 07/22/2019 01:22 PM - Victor Julien
- Target version changed from TBD to QA

#8 - 11/23/2019 09:27 AM - Victor Julien
- Priority changed from Normal to High

#9 - 02/18/2020 11:26 AM - Shivani Bhardwaj
- Related to Task #3269: Script for creating test with params added
#10 - 02/18/2020 11:26 AM - Shivani Bhardwaj
- Status changed from Feedback to In Review

#11 - 05/21/2020 08:53 PM - Shivani Bhardwaj
- Status changed from In Review to Closed

https://github.com/OISF/suricata-verify/pull/227