Suricata - Bug #2528

krb parser not always parsing tgs responses

07/10/2018 05:08 PM - Jason Taylor

Status: Closed
Priority: Normal
Assignee: Pierre Chifflier
Category: 
Target version: 4.1.1
Affected Versions: 4.1
Effort: 
Difficulty: 
Label: 

Description
I am testing out the krb5 parser and I am seeing what appear to be inconsistent results.

One pcap (krb5.good.pcap) parses out the tgs response in the json log.

The second pcap (krb5.bad.pcap) doesn't parse out the tgs response in the json log.

Attached are the logs from the suricata runs, build info and pcaps.

After some initial troubleshooting in IRC, victorj/pollux said it looks like there is an issue in krb5 parser as well as possibly something additional in suricata.

History
#1 - 07/11/2018 10:06 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Pierre Chifflier
- Target version set to TBD
- Affected Versions 4.1beta1 added
- Affected Versions deleted (4.0beta1)

#2 - 12/12/2018 10:40 AM - Pierre Chifflier

Hi,
Thanks for the report and the pcaps.

The cause of this issue is the probing parser being a bit too strict, and not matching fragmented request packets. A fix will be proposed soon.

#3 - 12/14/2018 03:46 PM - Victor Julien
- Status changed from Assigned to Closed
- Target version changed from TBD to 4.1.1
- Affected Versions 4.1 added
- Affected Versions deleted (4.1beta1)

https://github.com/OISF/suricata/pull/3583

#4 - 12/14/2018 03:47 PM - Victor Julien

Jason Borden Taylor: could you turn this into a suricata-verify test?

#5 - 12/14/2018 03:57 PM - Jason Taylor

Thanks Pierre!

Victor, sure I will get a PR done for that.
<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>suri.outinfo.txt</td>
<td>2.32 KB</td>
<td>07/10/2018</td>
<td>Jason Taylor</td>
</tr>
<tr>
<td>krb5.sample.zip</td>
<td>14.7 KB</td>
<td>07/10/2018</td>
<td>Jason Taylor</td>
</tr>
<tr>
<td>suri.buildinfo.txt</td>
<td>3.38 KB</td>
<td>07/10/2018</td>
<td>Jason Taylor</td>
</tr>
</tbody>
</table>