Suricata - Feature #1265
Replace response on Suricata dns decoder when dns error please
08/19/2014 10:39 AM - rmkml rmkml

Status: Closed
Priority: Normal
Assignee: David Cannings
Category:
Target version: 3.0RC1
Effort:
Difficulty:

Description
Hello,

When I start this test: (only for example)
perl -e 'print "\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x04test\x03com\x00\x00\x01\x00\x02"\nnc -vnu 8.8.8.8 53
tshark output:
1 17:27:37.939800 192.168.42.150 -> 8.8.8.8      DNS 68 Standard query 0x0000  A test.com
2 17:27:38.033266      8.8.8.8 -> 192.168.42.150 DNS 68 Standard query response 0x0000 Server failure

But Suricata v2.1beta1 "wrong" Response output:
08/19/2014-17:27:37.939800 [**] Query TX 0000 [**] test.com [**] A [**] 192.168.42.150:34092 -> 8.8.8.8 53
08/19/2014-17:27:38.033266 [**] Response TX 0000 [**] No Such Name [**] 8.8.8.8:53 -> 192.168.42.150:34092

Could you check why "No Such Name" appear here please ?
Because it's a dns response Server failure.

Found another example with dns response Format error.

Joigned pcap.
Regards
rmkml rmkml

History
#1 - 05/21/2015 05:02 AM - David Cannings
- Status changed from New to Resolved
- Target version set to 3.0RC1
- % Done changed from 0 to 100

This was fixed in the following PR: https://github.com/inliniac/suricata/pull/1425 which is included in 2.1beta4.

Using your test pcap I see:
08/19/2014-16:27:37.939800 [**] Query TX 0000 [**] test.com [**] A [**] 192.168.42.150:34092 -> 8.8.8.8:53
08/19/2014-16:27:37.939800 [**] Response TX 0000 [**] SERVFAIL [**] 8.8.8.8:53 -> 192.168.42.150:34092
08/19/2014-16:27:37.939800 [**] Response TX 0000 [**] SERVFAIL [**] 8.8.8.8:53 -> 192.168.42.150:34092

And in EVE:

#2 - 05/21/2015 05:02 AM - David Cannings
- Assignee set to David Cannings

03/07/2022
#3 - 06/17/2015 04:02 AM - Victor Julien
- Status changed from Resolved to Closed

Files

<table>
<thead>
<tr>
<th>exemple_dns_serverfailure.pcap</th>
<th>192 Bytes</th>
<th>08/19/2014</th>
<th>rmkml rmkml</th>
</tr>
</thead>
</table>