Suricata - Feature #3663
DNS: Parse and extract DNS NULL records
04/23/2020 07:14 AM - Konstantin Klinger

Status: Closed
Priority: Normal
Assignee: Community Ticket
Category: Target version: TBD
Effort:
Difficulty:
Label: Protocol

Description
At the moment the DNS parser gives you "NULL" as rrtype, but the related metadata of those NULL records/DNS packets is missing. In the attached eve.json you can find the current output.

I would expect something like this (equivalent to the content from packet 18 in Wireshark output):
Null (data): 42617365313238

This is related to Feature #2970

History
#1 - 04/26/2020 11:20 AM - Victor Julien
- Assignee set to Community Ticket
- Target version set to TBD

Simon Dugas are you interested in this one?

#2 - 05/19/2020 02:56 PM - Simon Dugas
Victor Julien wrote in #note-1:

Simon Dugas are you interested in this one?

Yes I can look into it. I should have something ready and dependent on https://redmine.openinfosecfoundation.org/issues/2970.

#3 - 10/29/2020 10:53 PM - Sascha Steinbiss
Just FYI, I have also started working on this and have also added possibly interesting RR types such as SRV and NS. NULL and NS are straightforward as they are simple buffers or domain names, but SRV needed another structured sub-object. Please see https://github.com/OISF/suricata/commit/e449676eee1f120f52722253e4e939330b98e for a first shot. Happy to prepare a PR.

#4 - 10/30/2020 10:48 AM - Sascha Steinbiss
https://github.com/OISF/suricata/pull/5525

#5 - 03/11/2021 08:14 PM - Philippe Antoine
- Status changed from New to Closed

https://github.com/OISF/suricata/pull/5641

Files
dns-tunnel-iodine.pcap 75.7 KB 04/23/2020 Konstantin Klinger
eve.json 388 KB 04/23/2020 Konstantin Klinger