Suricata - Feature #1199

LDAP support

06/03/2014 11:26 AM - Peter Manev

Status:	In Progress		
Priority:	Normal		
Assignee:	Pierre Chifflier		
Category:			
Target version:	7.0beta1		
Effort:	medium	**Label:**	Protocol
Difficulty:	medium		

Description

Support for LDAP.
LDAP is widely used and present in many networks.

example -

```
ldap://host:port/DN?attributes?scope?filter?extensions
```

As defined in - http://tools.ietf.org/html/rfc4516

Related issues:

Related to Task #4097: Suricon 2020 brainstorm	**New**
Related to Task #4151: Research: New protocol support	**New**

History

#1 - 06/04/2014 02:43 AM - Victor Julien

- Assignee set to Anonymous

- Target version set to TBD

I think this would be a great feature for members of the community to either develop or fund.

#2 - 06/12/2018 05:46 PM - Jason Ish

- Effort set to medium

- Difficulty set to medium

#3 - 02/23/2019 10:15 PM - Andreas Herz

- Assignee set to Community Ticket

#4 - 09/25/2019 07:46 PM - Victor Julien

Implementation should be in Rust.

#5 - 01/30/2020 02:41 PM - Victor Julien

- Label Protocol added

#6 - 11/12/2020 04:41 PM - Jason Ish

- Related to Task #4097: Suricon 2020 brainstorm added

#7 - 11/12/2020 04:41 PM - Jason Ish

Lots of interest at the 2020 Brainstorm.

#8 - 11/17/2020 05:48 PM - Pierre Chifflier

Bringing back this 6-years ticket!

update:

I have a test implementation (currently standalone parser, not a suricata applayer) for LDAP version 3, that more or less works (I still need to work on reliability / testing every possible corner case). LDAP being based on BER, it is based on the same BER/DER decoder than kerberos and x509 parsers embedded in suricata. It currently uses nom 6 and recent versions of everything, so I would primarily target suricata 7.0 (unless there is a great interest for 6.x).

One difficulty though is that to be fully interesting, more protocols have to be decoded: LDAP can use SASL, and can embed GSS-API and/or GSS-SPNEGO layers (this is a common case for Windows networks, where you often encounter integrity-only transport of data).

Call for help: there are **many** variants of implementations, and I can't have them all here. If you have pcaps to share (especially of LDAP in Active Directory environments), please tell me!

#9 - 11/19/2020 09:21 PM - Victor Julien

- Related to Task #4151: Research: New protocol support added

#10 - 12/24/2020 09:29 AM - Victor Julien

- Status changed from New to In Progress

- Assignee changed from Community Ticket to Pierre Chifflier

- Target version changed from TBD to 7.0beta1

Hi Pierre, did I understand correctly that you've made further progress on this?

#11 - 12/24/2020 10:03 AM - Pierre Chifflier

Hi Victor,
Yes, I have a working LDAP parser for suricata, based on the ldap-parser crate I published to crates.io.
It supports LDAPv3 protocol, as well as the cleartext variants of SASL and GSSAPI (for ex. integrity-only encapsulation).

Before submitting the PR, the code still needs some polishing. It currently parse the protocol and log metadata (LDAP operation, bind DN, password if cleartext, etc.), but do not have detect keywords (TBD).