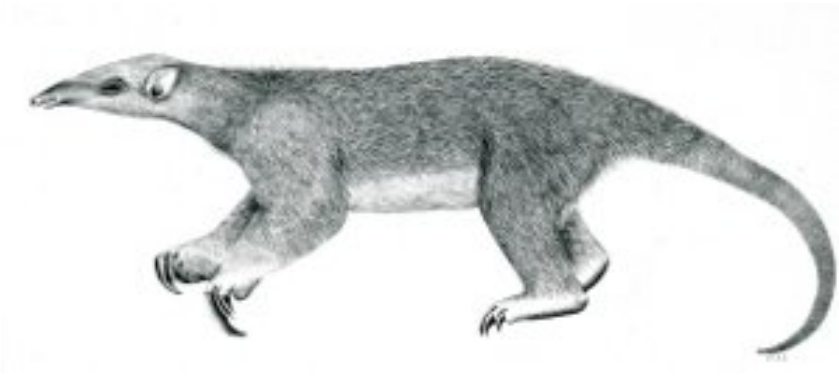
Tranalyzer2

snmpDecode

Simple Network Management Protocol (SNMP)



Tranalyzer Development Team

Contents

1 snmpDecode

1.1 Description

The snmpDecode plugin analyzes SNMP traffic.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description
SNMP_STRLEN	64	Maximum length for strings

1.3 Flow File Output

The snmpDecode plugin outputs the following columns:

Column	Type	Description
snmpStat	H8	Status
snmpVersion	U8	Version
snmpCommunity	S	Community (SNMPv1-2)
snmpUsername	S	Username (SNMPv3)
snmpMsgT	H16	Message types
snmpNumReq_Next_Resp_Set_Trap1_Bulk_Info_Trap2_Rep	U64_U64_U64_U64_U64_U64_U64_U64_U64	Number of GetRequest, GetNextRequest, GetResponse, SetRequest, Trapv1, GetBulkRequest, InformRequest, Trapv2, and Report packets

1.3.1 snmpStat

The snmpStat column is to be interpreted as follows:

snmpStat	Description
0x01	Flow is SNMP
0x40	String was truncated... increase SNMP_STRLEN
0x80	Packet was malformed

1.3.2 snmpVersion

The snmpVersion column is to be interpreted as follows:

snmpVersion	Description
0	SNMPv1
1	SNMPv2c
3	SNMPv3

1.3.3 snmpMsgT

The snmpMsgT column is to be interpreted as follows:

snmpMsgT	Description
0x0001	GetRequest
0x0002	GetNextRequest
0x0004	GetResponse
0x0008	SetRequest
0x0010	Trap (v1)
0x0020	GetBulkRequest (v2c, v3)
0x0040	InformRequest
0x0080	Trap (v2c, v3)
0x0100	Report

1.3.4 snmpType

The snmpType column is to be interpreted as follows:

snmpType	Description
0xa0	GetRequest
0xa1	GetNextRequest
0xa2	GetResponse
0xa3	SetRequest
0xa4	Trap (v1)
0xa5	GetBulkRequest (v2c, v3)
0xa6	InformRequest
0xa7	Trap (v2c, v3)
0xa8	Report

1.4 Packet File Output

In packet mode (-s option), the snmpDecode plugin outputs the following columns:

Column	Type	Description
snmpVersion	U8	Version
snmpCommunity	S	Community
snmpType	H8	Message type

1.5 Plugin Report Output

The following information is reported:

- Number of SNMP packets
- Number of SNMP GetRequest packets

- Number of SNMP GetNextRequest packets
- Number of SNMP GetResponse packets
- Number of SNMP SetRequest packets
- Number of SNMP Trap v1 packets
- Number of SNMP GetBulkRequest packets
- Number of SNMP InformRequest packets
- Number of SNMP Trap v2 packets
- Number of SNMP Report packets