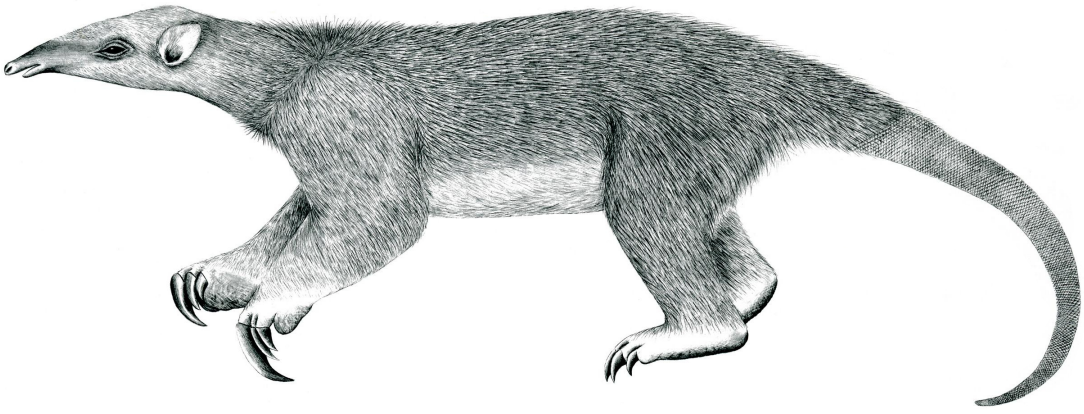
Tranalyzer2

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	Flags
snmpStat	H8	Status	
snmpVersion	U8	Version	
snmpCommunity	S	Community (SNMPv1-2)	
snmpUser	S	Username (SNMPv3)	
snmpMsgT	H16	Message types bitfield	
snmpNumReq_	U64_	Number of GetRequest,	
Next_	U64_	GetNextRequest,	
Resp_	U64_	GetResponse,	
Set_	U64_	SetRequest,	
Trap1_	U64_	Trapv1,	
Bulk_	U64_	GetBulkRequest,	
Info_	U64_	InformRequest,	
Trap2_	U64_	Trapv2,	
Rep	U64	Report packets	

1.3.1 snmpStat

The snmpStat column is to be interpreted as follows:

snmpStat	Description
0x01	Flow is SNMP
0x02	—
0x04	—
0x08	—
0x10	—
0x20	—
0x40	String was truncated... increase SNMP_STRLEN

snmpStat	Description
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 and snmpType

The snmpMsgT and snmpType columns are to be interpreted as follows:

snmpMsgT	snmpType	Description
0x0001	0xa0	GetRequest
0x0002	0xa1	GetNextRequest
0x0004	0xa2	GetResponse
0x0008	0xa3	SetRequest
0x0010	0xa4	Trap (v1)
0x0020	0xa5	GetBulkRequest (v2c, v3)
0x0040	0xa6	InformRequest
0x0080	0xa7	Trap (v2c, v3)
0x0100	0xa8	Report

1.4 Packet File Output

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

Column	Type	Description	Flags
snmpVersion	U8	Version	
snmpCommunity	S	Community	
snmpUser	S	Username (SNMPv3)	
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