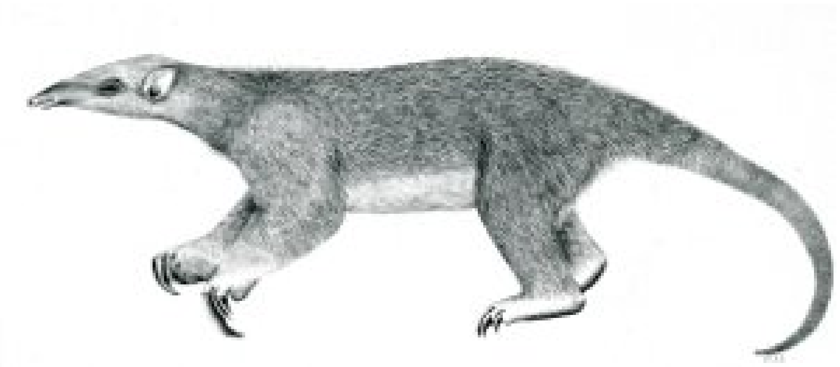
Tranalyzer2

stunDecode

STUN, TURN and NAT-PMP



Tranalyzer Development Team

Contents

1 stunDecode **1**
1.1 Required Files . . . 1
1.2 Configuration Flags . . . 1
1.3 Flow File Output . . . 1
1.4 TODO . . . 3

1 stunDecode

This plugin analyzes STUN, TURN and NAT-PMP traffic.

1.1 Required Files

None

1.2 Configuration Flags

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

Name	Default	Description
NAT_PMP	1	Whether (1) or not (0) to analyse NAT-PMP

1.3 Flow File Output

The stunDecode plugin outputs the following columns:

Column	Type	Description
natStat	H32	status
natErr	H32	error code
natMCReq_Ind_Succ_Err	U16_U16_U16_U16	number of messages (Req, Ind, Succ, Err)
natAddr_Port	IP4_U16	mapped address and port
natXAddr_Port	IP4_U16	(xor) mapped address and port
natPeerAddr_Port	IP4_U16	peer address and port
natOrigAddr_Port	IP4_U16	response origin address and port
natRelayAddr_Port	IP4_U16	relayed address and port
natDstAddr_Port	IP4_U16	destination address and port
natOtherAddr_Port	IP4_U16	other address and port
natLifetime	U32	binding lifetime (seconds)
natUser	S	username
natPass	S	password
natRealm	S	realm
natSoftware	S	software
If NAT_PMP=1, the following columns are displayed:		
natPMPReqEA_MU_MT	U16_U16_U16	NAT-PMP num. of requests (External Address, Map UDP, Map TCP)
natPMPRespEA_MU_MT	U16_U16_U16	NAT-PMP num. of responses (External Address, Map UDP, Map TCP)
natPMPSSSOE	U32	NAT-PMP seconds since start of epoch

1.3.1 natStat

The `natStat` column is to be interpreted as follows:

natStat	Description
2^{0} (=`0x0000 0001`)	STUN protocol
2^{1} (=`0x0000 0002`)	TURN protocol
2^{2} (=`0x0000 0004`)	ICE protocol
2^{3} (=`0x0000 0008`)	SIP protocol
2^{4} (=`0x0000 0010`)	Microsoft Extension
2^{5} (=`0x0000 0020`)	Even Port
2^{6} (=`0x0000 0040`)	Reserve next port
2^{7} (=`0x0000 0080`)	don't fragment
2^{8} (=`0x0000 0100`)	nonce
2^{13} (=`0x0000 2000`)	deprecated message attribute
2^{14} (=`0x0000 4000`)	STUN over non-standard port
2^{15} (=`0x0000 8000`)	malformed message
2^{16} (=`0x0001 0000`)	Port Mapping Protocol (PMP)
2^{31} (=`0x8000 0000`)	Packet snapped, analysis incomplete

1.3.2 natErr

The hex based error variable `natErr` is defined as follows (STUN):

natErr	Description
2^{0} (=`0x00000001`)	try alt
2^{1} (=`0x00000002`)	bad request
2^{2} (=`0x00000004`)	unauthorized
2^{3} (=`0x00000008`)	forbidden
2^{4} (=`0x00000010`)	unknown attribute
2^{5} (=`0x00000020`)	allocation mismatch
2^{5} (=`0x00000040`)	stale nonce
2^{6} (=`0x00000080`)	address family not supported
2^{7} (=`0x00000100`)	wrong credentials
2^{8} (=`0x00000200`)	unsupported transport protocol
2^{9} (=`0x00000400`)	peer address family mismatch
2^{10} (=`0x00000800`)	connection already exists
2^{11} (=`0x00001000`)	connection timeout or failure
2^{12} (=`0x00002000`)	allocation quota reached
2^{13} (=`0x00004000`)	role conflict
2^{14} (=`0x00008000`)	server error
2^{15} (=`0x00010000`)	insufficient capacity
2^{31} (=`0x80000000`)	Unhandled error

The hex based error variable `natErr` is defined as follows (NAT-PMP):

natErr	Description
2^1 (=0x00000002)	Unsupported version
2^2 (=0x00000004)	Not authorized/refused
2^3 (=0x00000008)	Network failure
2^4 (=0x00000010)	Out of resources
2^5 (=0x00000020)	Unsupported opcode

1.3.3 natMCReq_Ind_Succ_Err

The number of messages variable `natMCReq_Ind_Succ_Err` decomposed as follows:

natMCReq_Ind_Succ_Err	Description
natMCReq	number of requests
natMCInd	number of indications
natMCSucc	number of success response
natMCErr	number of error response

1.4 TODO

Port Control Protocol (PCP)