Tranalyzer2

stunDecode

STUN, TURN, ICE and NAT-PMP

Tranalyzer Development Team

Contents

1 stunDecode

This plugin analyzes the following protocols:

- Session Traversal Utilities for Nat (STUN)
- Traversal Using Relays around NAT (TURN)
- Interactive Connectivity Establishment (ICE)
- NAT Port Mapping Protocol (NAT-PMP)

1.1 Configuration Flags

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

Name	Default	Description
NAT_PMP	1	Analyze NAT-PMP

1.2 Flow File Output

The stunDecode plugin outputs the following columns:

Column	Type	Description	Flags
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	

1.2.1 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

1.2.2 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^{6} (=0x00000040)	Stale nonce
2^{7} (=0x00000080)	Address family not supported
2^{8} (=0x00000100)	Wrong credentials
2^{9} (=0x00000200)	Unsupported transport protocol
2^{10} (=0x00000400)	Peer address family mismatch
2^{11} (=0x00000800)	Connection already exists
2^{12} (=0x00001000)	Connection timeout or failure

natErr		Description
2^{13}	(=0x00002000)	Allocation quota reached
2^{14}	(=0x00004000)	Role conflict
2^{15}	(=0x00008000)	Server error
2^{16}	(=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

1.2.3 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

1.3 Plugin Report Output

The following information is reported:

- Aggregated natStat
- Aggregated natErr
- Number of NAT-PMP packets
- Number of STUN packets

1.4 TODO

Port Control Protocol (PCP)