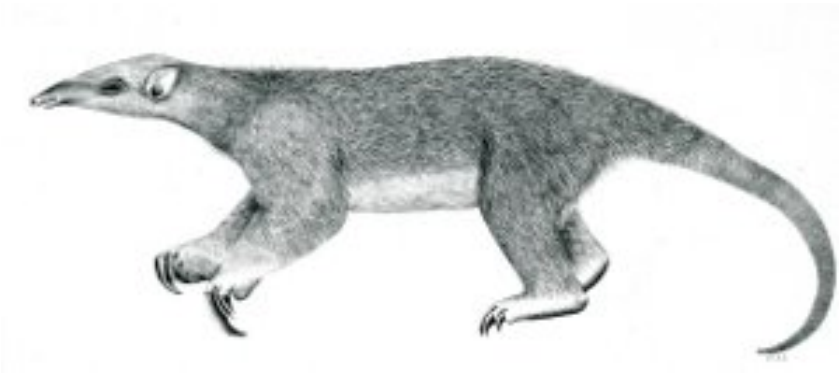
Tranalyzer2

tftpDecode

Trivial File Transfer Protocol (TFTP)



Tranalyzer Development Team

Contents

1 tftpDecode **1**
1.1 Description 1
1.2 Configuration Flags 1
1.3 Flow File Output 1
1.4 TODO 2

1 tftpDecode

1.1 Description

The `tftpDecode` plugin analyses TFTP traffic. User defined compiler switches are in *tftpDecode.h*.

1.2 Configuration Flags

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

Name	Default	Description
`TFTP_SAVE`	0	save content to FTP_F_PATH
`TFTP_MXNMLN`	15	maximal name length
`MAXCNM`	2	maximal length of command field
`FTP_F_PATH`	`"/tmp/TFTPFILES/"`	path for `TFTP_SAVE`

1.3 Flow File Output

The tftpDecode plugin outputs the following columns:

Column	Type	Description
`tftpStat`	H16	TFTP status bitfield
`tftPFlw`	U64	TFTP Parent Flow
`tftpOpCBF`	H8	TFTP OP Code Bit Field
`tftpErrCBF`	H8	TFTP Error Code Bit Field
`tftOpCNum`	U8	TFTP Number of OP Code
`tftpPNum`	U8	TFTP Number of parameters
`tftpOpC`	RSC	TFTP OP Codes
`tftpC`	RS	TFTP Parameters

1.3.1 tftpStat

The `tftpStat` column describes the errors encountered during the flow lifetime:

tftpStat	Name	Description
2^0 (=`0x0001`)	TFTPS_INIT	TFTP flow found
2^1 (=`0x0002`)	TFTPS_DRD	TFTP data read
2^2 (=`0x0004`)	TFTPS_DWD	TFTP data write
2^3 (=`0x0008`)	TFTP_FERR	file open error for TFTP_SAVE
2^4 (=`0x0010`)	TFTPS_BSERR	Error in block send sequence
2^5 (=`0x0020`)	TFTPS_BSAERR	Error in block ack sequence
2^6 (=`0x0040`)	TFTPS_PERR	Error or TFTP protocol error or not TFTP
2^7 (=`0x0080`)	TFTPS_OVFL	array overflow
2^8 (=`0x0100`)	—	—
2^9 (=`0x0200`)	—	—
2^{10} (=`0x0400`)	—	—

tftpStat	Name	Description
2^{11} (=0x0800)	TFTP_RW_PLNERR	Crafted packet or TFTP read/write parameter length error
2^{12} (=0x1000)	TFTPS_ACT	TFTP active
2^{13} (=0x2000)	TFTPS_PSV	TFTP passive
2^{14} (=0x4000)	—	—
2^{15} (=0x8000)	—	—

1.3.2 tftpOpCBF

The `tftpOpCBF` column describes the op code encountered during the flow lifetime:

tftpOpCBF	Name	Description
2^0 (=0x01)	TFTP_RRQ	1: Read request
2^1 (=0x02)	TFTP_WRQ	2: Write request
2^2 (=0x04)	TFTP_DATA	3: Read or write the next block of data
2^3 (=0x08)	TFTP_ACK	4: Acknowledgment
2^4 (=0x10)	TFTP_ERR	5: Error message
2^5 (=0x20)	TFTP_OACK	6: Option acknowledgment
2^6 (=0x40)	—	—
2^7 (=0x80)	—	—

1.3.3 tftpErrCBF

The `tftpErrCBF` column describes the error code (if op code TFTP_ERR encountered during the flow lifetime):

tftpErrCBF	Name	Description
(=0x00)	TFTP_NOERR	0: No Error
2^0 (=0x01)	TFTP_FLNFND	1: File not found
2^1 (=0x02)	TFTP_ACCVLT	2: Access violation
2^2 (=0x04)	TFTP_DSKFLL	3: Disk full or allocation exceeded
2^3 (=0x08)	TFTP_ILGLOP	4: Illegal TFTP operation
2^4 (=0x10)	TFTP_UKWNID	5: Unknown transfer ID
2^5 (=0x20)	TFTP_FLEXST	6: File already exists
2^6 (=0x40)	TFTP_NOSUSR	7: No such user
2^7 (=0x80)	TFTP_TRMOPN	8: Terminate transfer due to option negotiation

1.4 TODO

- fragmentation
- reply address extraction