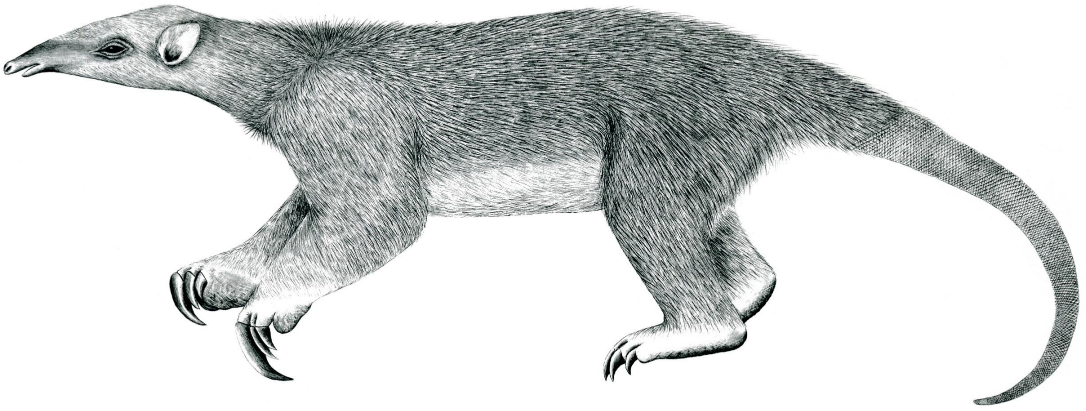
Tranalyzer2

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 Packet File Output 4
1.5 Plugin Report Output 4

1 tftpDecode

1.1 Description

The tftpDecode plugin analyzes 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	Flags
TFTP_SAVE	0	Save content to TFTP_F_PATH	
TFTP_RMDIR	1	Empty TFTP_F_PATH before starting	TFTP_SAVE=1
TFTP_CMD_AGGR	1	Aggregate TFTP commands/errors	
TFTP_BTFLD	1	Bitfield coding of TFTP commands	
TFTP_MXNMLN	15	Maximal name length	
TFTP_MAXCNM	2	Maximal length of command field	
TFTP_F_PATH	"/tmp/TFTPFILES/"	Path for extracted content	

1.2.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- TFTP_RMDIR
- TFTP_F_PATH

1.3 Flow File Output

The tftpDecode plugin outputs the following columns:

Column	Type	Description	Flags
tftpStat	H16	Status	
tftpPFlow	U64	Parent flow	
tftpOpCBF	H8	Opcode bitfield	TFTP_BITFIELD=1
tftpErrCBF	H8	Error code bitfield	TFTP_BITFIELD=1
tftpNumOpcode	U8	Number of opcodes	
tftpOpcode	RSC	Opcodes	TFTP_MAXCNM>0
tftpNumParam	U8	Number of parameters	
tftpParam	RS	Parameters	TFTP_MAXCNM>0
tftpNumError	U8	Number of errors	
tftpErrC	RU16	Error codes	TFTP_MAXCNM>0

1.3.1 tftpStat

The tftpStat column is to be interpreted as follows:

tftpStat	Description	Flags
2^0 (=0x0001)	TFTP flow found	
2^1 (=0x0002)	TFTP data read	
2^2 (=0x0004)	TFTP data write	
2^3 (=0x0008)	File open error	TFTP_SAVE=1
2^4 (=0x0010)	Error in block send sequence	
2^5 (=0x0020)	Error in block ack sequence	
2^6 (=0x0040)	Error or TFTP protocol error or not TFTP	
2^7 (=0x0080)	Array overflow. . . increase TFTP_MAXCNM	
2^8 (=0x0100)	String truncated. . . increase TFTP_MXNMLN	
2^9 (=0x0200)	—	
2^{10} (=0x0400)	—	
2^{11} (=0x0800)	Crafted packet or TFTP read/write parameter length error	
2^{12} (=0x1000)	TFTP active	
2^{13} (=0x2000)	TFTP passive	
2^{14} (=0x4000)	—	
2^{15} (=0x8000)	—	

1.3.2 tftpOpcode and tftpOpCBF

The tftpOpCBF column is to be interpreted as follows:

tftpOpCBF	tftpOpcode	Description
2^0 (=0x01)	RRQ	Read request
2^1 (=0x02)	WRQ	Write request
2^2 (=0x04)	DTA	Read or write the next block of data
2^3 (=0x08)	ACK	Acknowledgment
2^4 (=0x10)	ERR	Error message
2^5 (=0x20)	OAK	Option acknowledgment
2^6 (=0x40)	---	—
2^7 (=0x80)	---	—

1.3.3 tftpErrC and tftpErrCBF

The tftpErrCBF column is to be interpreted as follows:

tftpErrC	tftpErrCBF	Description
	0x00	No Error
0	0x01	File not found
1	0x02	Access violation
2	0x04	Disk full or allocation exceeded
3	0x08	Illegal TFTP operation

tftpErrC	tftpErrCBF	Description
4	`0x10`	Unknown transfer ID
5	`0x20`	File already exists
6	`0x40`	No such user
7	`0x80`	Terminate transfer due to option negotiation

1.4 Packet File Output

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

Column	Type	Description	Flags
tftpOpcode	SC	TFTP opcode	

1.5 Plugin Report Output

The following information is reported:

- Aggregated tftpStat
- Number of TFTP packets
- Number of files extracted (TFTP_SAVE=1)