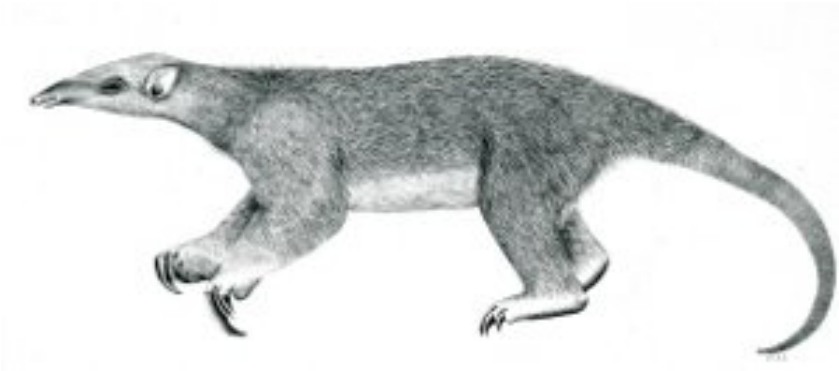
Tranalyzer2

telnetDecode

TELNET



Tranalyzer Development Team

Contents

1 telnetDecode **1**
1.1 Description 1
1.2 Configuration Flags 1
1.3 Flow File Output 1
1.4 TODO 3

1 telnetDecode

1.1 Description

The telnetDecode plugin analyses TELNET traffic and is capable to extract L7 content.

1.2 Configuration Flags

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

Name	Default	Description
TEL_SAVE	0	Save content to TEL_F_PATH/TELFNAME
TEL_CMDC	0	output command codes
TEL_CMDS	1	output command human readable
TEL_OPTS	1	output options human readable
TEL_CMD_AGGR	1	Aggregate commands
TEL_OPT_AGGR	1	Aggregate options
TELCMDN	25	maximal command / flow
TELOPTN	25	maximal options / flow
TEL_F_PATH	"/tmp/TELFILES/"	Path for extracted content
TELFNAME	"telwurst"	file name

1.3 Flow File Output

The telnetDecode plugin outputs the following columns:

Column	Type	Description	Flags
telStat	H8	Status	
telCmdBF	H16	Commands	
telOptBF	H32	Options	
telTCCnt	U16	Total command count	
telTOCnt	U16	Total option count	
telCCnt	U16	Stored command count	TEL_CMDS=1||TEL_CMDC=1
telCmdC	RU8	Command codes	TEL_CMDC=1
telCmdS	RS	Command strings	TEL_CMDS=1
telOCnt	U16	Stored options count	TEL_OPTS=1
telOptS	RS	Option strings	TEL_OPTS=1

1.3.1 telStat

The telStat column is to be interpreted as follows:

telStat	Description
2^0 (=0x01)	TELNET port found
2^1 (=0x02)	—
2^2 (=0x04)	—

telStat	Description
2^3 (=0x08)	—
2^4 (=0x10)	—
2^5 (=0x20)	File open error: TEL_SAVE=1
2^6 (=0x40)	—
2^7 (=0x80)	—

1.3.2 telCmdBF

The telCmdBF column is to be interpreted as follows:

telCmdBF	Description
2^0 (=0x0001)	SE - End subNeg
2^1 (=0x0002)	NOP - No Op
2^2 (=0x0004)	Data Mark
2^3 (=0x0008)	Break
2^4 (=0x0010)	Int process
2^5 (=0x0020)	Abort output
2^6 (=0x0040)	Are You there?
2^7 (=0x0080)	Erase char

telCmdBF	Description
2^8 (=0x0100)	Erase line
2^9 (=0x0200)	Go ahead!
2^{10} (=0x0400)	SB - SubNeg
2^{11} (=0x0800)	WILL use
2^{12} (=0x1000)	WON'T use
2^{13} (=0x2000)	DO use
2^{14} (=0x4000)	DON'T use
2^{15} (=0x8000)	IAC

1.3.3 telOptBF

The telOptBF column is to be interpreted as follows:

telOptBF	Description
2^0 (=0x00000001)	Bin Xmit
2^1 (=0x00000002)	Echo Data
2^2 (=0x00000004)	Reconn
2^3 (=0x00000008)	Suppr GA
2^4 (=0x00000010)	Msg Sz
2^5 (=0x00000020)	Opt Stat
2^6 (=0x00000040)	Timing Mark
2^7 (=0x00000080)	R/C XmtEcho
2^8 (=0x00000100)	Line Width
2^9 (=0x00000200)	Page Length
2^{10} (=0x00000400)	CR Use
2^{11} (=0x00000800)	Horiz Tabs
2^{12} (=0x00001000)	Hor Tab Use
2^{13} (=0x00002000)	FF Use
2^{14} (=0x00004000)	Vert Tabs
2^{15} (=0x00008000)	Ver Tab Use

telOptBF	Description
2^{16} (=0x00010000)	Lf Use
2^{17} (=0x00020000)	Ext ASCII
2^{18} (=0x00040000)	Logout
2^{19} (=0x00080000)	Byte Macro
2^{20} (=0x00100000)	Data Term
2^{21} (=0x00200000)	SUPDUP
2^{22} (=0x00400000)	SUPDUP Outp
2^{23} (=0x00800000)	Send Locate
2^{24} (=0x01000000)	Term Type
2^{25} (=0x02000000)	End Record
2^{26} (=0x04000000)	TACACS ID
2^{27} (=0x08000000)	Output Mark
2^{28} (=0x10000000)	Term Loc
2^{29} (=0x20000000)	3270 Regime
2^{30} (=0x40000000)	X.3 PAD
2^{31} (=0x80000000)	Window Size

1.3.4 telCmdC and telCmdS

The `telCmdC` and `telCmdS` columns are to be interpreted as follows:

telCmdC	telCmdS	Description
0xf0	SE	Subnegotiation End
0xf1	NOP	No Operation
0xf2	DM	Data Mark
0xf3	BRK	Break
0xf4	IP	Interrupt Process
0xf5	AO	Abort Output
0xf6	AYT	Are You There
0xf7	EC	Erase Character
0xf8	EL	Erase Line
0xf9	GA	Go Ahead
0xfa	SB	Subnegotiation
0xfb	WILL	Will Perform
0xfc	WONT	Won't Perform
0xfd	DO	Do Perform
0xfe	DONT	Don't Perform
0xff	IAC	Interpret As Command

1.4 TODO

- fragmentation