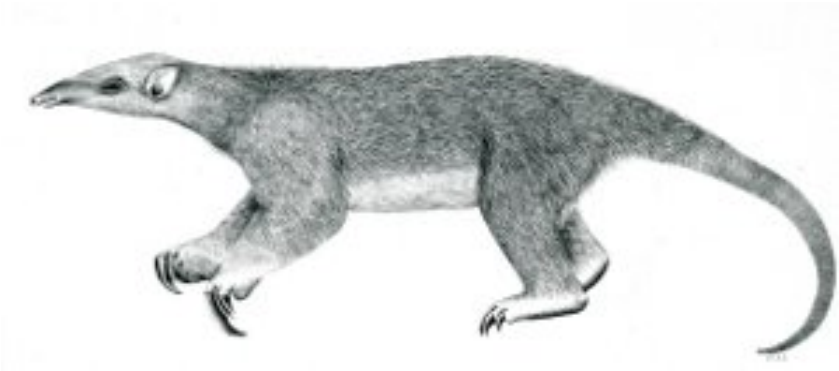
Tranalyzer2

sshDecode

SSH



Tranalyzer Development Team

Contents

1 sshDecode **1**
1.1 Description . . . 1
1.2 Dependencies . . . 1
1.3 Configuration Flags . . . 1
1.4 Flow File Output . . . 1
1.5 Plugin Report Output . . . 2

1 sshDecode

1.1 Description

This plugin analyzes SSH traffic.

1.2 Dependencies

This plugin requires the **libssl**.

Arch: `sudo pacman -S openssl`

Ubuntu/Kali: `sudo apt-get install libssl-dev`

OpenSUSE: `sudo zypper install libopenssl-devel`

Red Hat/Fedora: `sudo yum install openssl-devel`

Mac OSX: `brew install openssl`

1.3 Configuration Flags

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

Name	Default	Description
SSH_USE_PORT	1	Whether (1) or not (0) to count all packets to/from SSH_PORT as SSH (useful if version exchange was not captured)
SSH_DECODE	0	Decode SSH handshake messages (experimental)
SSH_DEBUG	0	Activate debug output

1.4 Flow File Output

The sshDecode plugin outputs the following columns:

Column	Type	Description
sshStat	H8	Status
sshVersion	RS	SSH version and software
If SSH_DECODE=1, the following columns are displayed:		
sshFingerprint	RS	SSH public key fingerprint
sshCookie	RS	SSH cookie
sshKEX	RS	SSH KEX Algorithms
sshSrvHostKeyAlgo	RS	SSH server host key algorithms
sshEncCS	RS	SSH encryption algorithms client to server
sshEncSC	RS	SSH encryption algorithms server to client

Column	Type	Description
sshMacCS	RS	SSH MAC algorithms client to server
sshMacSC	RS	SSH MAC algorithms server to client
sshCompCS	RS	SSH compression algorithms client to server
sshCompSC	RS	SSH compression algorithms server to client
sshLangCS	RS	SSH languages client to server
sshLangSC	RS	SSH languages server to client

1.4.1 sshStat

The sshStat column is to be interpreted as follows:

sshStat	Description
0x01	Flow contains SSH protocol
0x02	Keeps track of who sent the SSH banner first
0x40	SSH version got truncated
0x80	Banner does not end with CRLF or contains NULL byte

1.5 Plugin Report Output

The number of SSH flows is reported.