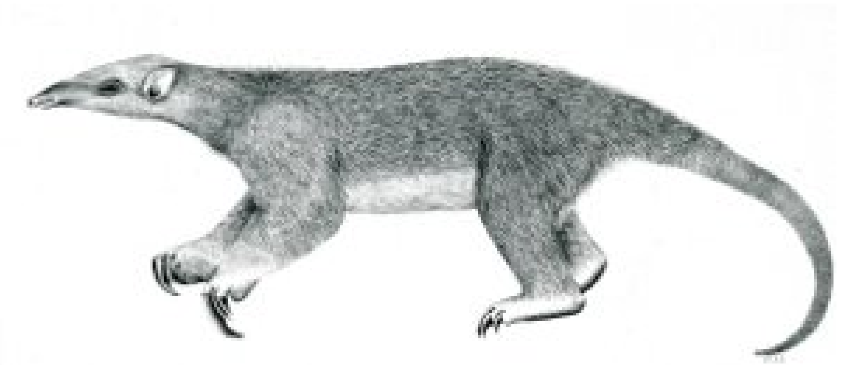
Tranalyzer2

p0f

OS/Application Fingerprinting



Tranalyzer Development Team

Contents

1 p0f

1.1 Description

The p0f plugin tries to fingerprint OS and applications.

1.2 Dependencies

1.2.1 Other Plugins

This plugin requires the **sslDecode** plugin with the following flags activated, i.e., set to 1:

- SSL_EXT_LIST
- SSL_CIPHER_LIST

1.2.2 Required Files

The file p0f-ssl.txt is required.

1.3 Configuration Flags

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

Name	Default	Description
P0F_SSL_VER	1	whether or not to consider the version for fingerprint match
P0F_SSL_NCIPHER	1	whether or not to consider the number of ciphers for fingerprint match
P0F_SSL_NUMEXT	1	whether or not to consider the number of extensions for fingerprint match
P0F_SSL_FLAGS	1	whether or not to consider flags for fingerprint match
P0F_SSL_CIPHER	1	whether or not to consider ciphers for fingerprint match
P0F_SSL_EXT	1	whether or not to consider extensions for fingerprint match
P0F_SSL_ELEN	6	Maximum length of cipher or extension
P0F_SSL_NSIG	64	Maximum number of signatures to read
P0F_SSL_SLEN	128	Maximum length of a string (os, browser, comment)
P0F_SSL_LLEN	1024	Maximum length of a line in the DB
P0F_SSL_DB	"p0f-ssl.txt"	Name of the database to use

1.4 Flow File Output

The p0f plugin outputs the following columns:

Column	Type	Description
p0fSSLRule	U16	p0f SSL fingerprint rule number
p0fSSLOS	S	p0f SSL OS fingerprint
p0fSSLOS2	S	p0f SSL OS fingerprint (2)
p0fSSLBrowser	S	p0f SSL browser fingerprint

Column	Type	Description
p0fSSLComment	S	p0f SSL fingerprint comment

1.5 References

- https://idea.popcount.org/2012-06-17-ssl-fingerprinting-for-p0f