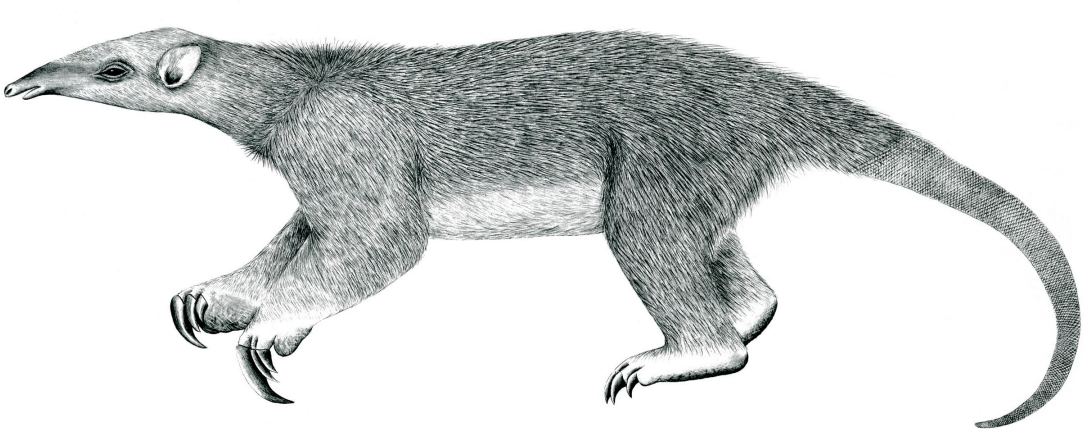
Tranalyzer2

pwX

Clear-text Passwords Extractor



Tranalyzer Development Team

Contents

1 pwX

1.1 Description

The pwX plugin extracts usernames and passwords from different plaintext protocols. This plugin produces only output to the flow file. Configuration is achieved by user defined compiler switches in `src/pwX.h`.

1.2 Configuration Flags

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

Variable	Default	Description
PWX_USERNAME	1	Output the username
PWX_PASSWORD	1	Output the password
PWX_FTP	1	Extract FTP authentication
PWX_POP3	1	Extract POP3 authentication
PWX_IMAP	1	Extract IMAP authentication
PWX_SMTP	1	Extract SMTP authentication
PWX_HTTP_BASIC	1	Extract HTTP Basic Authorization
PWX_HTTP_PROXY	1	Extract HTTP Proxy Authorization
PWX_HTTP_GET	1	Extract HTTP GET authentication
PWX_HTTP_POST	1	Extract HTTP POST authentication
PWX_IRC	1	Extract IRC authentication
PWX_TELNET	1	Extract Telnet authentication
PWX_LDAP	1	Extract LDAP bind request authentication
PWX_PAP	1	Extract PAP (Password Authentication Protocol) authentication
PWX_STATUS	1	Extract authentication status (success, error, ...).
PWX_DEBUG	0	Activate debug output.

1.3 Flow File Output

The pwX plugin outputs the following columns:

Name	Type	Description	Flags
pwxType	U8	Authentication type	
pwxUser	S	Extracted username	PWX_USERNAME!=0
pwxPass	S	Extracted password	PWX_PASSWORD!=0
pwxStatus	U8	Authentication status	PWX_STATUS!=0

1.3.1 pwxType

The `pwxType` column is to be interpreted as follows:

pwxType	Description
0	No password or username extracted
1	FTP authentication
2	POP3 authentication
3	IMAP authentication
4	SMTP authentication
5	HTTP Basic Authorization
6	HTTP Proxy Authorization
7	HTTP GET authentication
8	HTTP POST authentication
9	IRC authentication
10	Telnet authentication
11	LDAP authentication
12	PAP authentication

1.3.2 pwxStatus

The `pwxStatus` column is to be interpreted as follows:

pwxStatus	Description
0	Authentication status is unknown
1	Authentication was successful
2	Authentication failed

1.4 Plugin Report Output

The number of passwords extracted is reported.