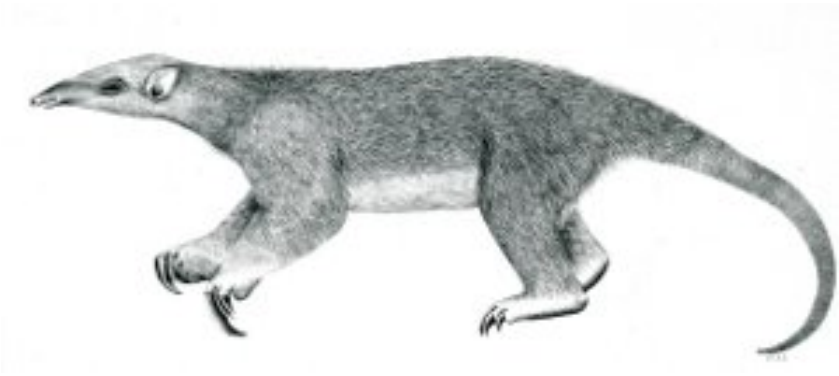
Tranalyzer2

pwX

Clear-text Passwords Extractor



Tranalyzer Development Team

Contents

1 pwX **1**
1.1 Description 1
1.2 Configuration Flags 1
1.3 Flow File Output 1
1.4 Plugin Report Output 2

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	Defines if username column is printed.
PWX_PASSWORD	1	Defines if password column is printed.
PWX_FTP	1	Defines if FTP authentication is extracted.
PWX_POP3	1	Defines if POP3 authentication is extracted.
PWX_IMAP	1	Defines if IMAP authentication is extracted.
PWX_SMTP	1	Defines if SMTP authentication is extracted.
PWX_HTTP_BASIC	1	Defines if HTTP Basic Authorization is extracted.
PWX_HTTP_PROXY	1	Defines if HTTP Proxy Authorization is extracted.
PWX_HTTP_GET	1	Defines if HTTP GET authentication is extracted.
PWX_HTTP_POST	1	Defines if HTTP POST authentication is extracted.
PWX_IRC	1	Defines if IRC authentication is extracted.
PWX_TELNET	1	Defines if Telnet authentication is extracted.
PWX_LDAP	1	Defines if LDAP bind request authentication is extracted.
PWX_PAP	1	Defines if Password Authentication Protocol (PAP) is extracted.
PWX_STATUS	1	Whether or not to extract authentication status (success, error, ...).
PWX_DEBUG	0	Whether or not to 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.