Prewikka - Feature #113

Refactor the Log.py class to use the logging pyton (2.3) module

12/01/2005 04:03 PM -

Status:	Closed	**Start date:**	
Priority:	Low	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.8		
Resolution:	fixed		

Description

Hi,

Currently prewikka use only stderr class. I looked to the current implantation of the log writing and was able to add a **[Log syslog]** to log to a syslog. But I think that it's a waste of time to add additional class to manage additional log output. In python (2.3) it's possible to use the **logging module**, that allow both console, File, Syslog, Mail, even NT Event... It should not be a lot of work, ex LogStderr mechanics can be implemented in a Formatter class, log level is the same, logging module allow also multiple log output (as you do with *for backend in self._backends:*).

Dont know the dev priority, if you want I can give a try. (or if you want to preserve the current log function, i can send you my *modules/log/syslog/syslog.py* but I like more the idea of the python logging-module)

After that it will be possible to add LML regex, to parse some information about prewikka, Add "_Prewikka Bad Login/Password_" inside prelude-lml should be easy enough. (EVENT_LOGIN_SUCCESSFUL, EVENT_LOGOUT, EVENT_BAD_LOGIN, EVENT_BAD_PASSWORD)

Have a nice day

Francois Harvey

History

#1 - 12/03/2005 01:39 AM - Yoann VANDOORSELAERE

This sound like a good idea, and the described implementation would be welcome.

However, it would seem redondant to analyze Prewikka output through Prelude-LML since Prewikka already depend on the prelude library. Thus it already got the necessary functionality to emit alert back to the Prelude system.

#2 - 11/16/2006 05:24 PM - Yoann VANDOORSELAERE

- Status changed from New to Closed

- Resolution set to fixed

Fixed in r8582.

#3 - 04/29/2009 12:24 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prewikka

- Category deleted (5)

- Target version deleted (0.9.8)