PyDbg

오픈 소스 파이썬 디버거이다. Reversing Engineering Framework인 PaiMei의 핵심 구성 요소 중 하나이다.

설치

1. 파이썬 설치 후 환경변수 등록
여기서는 python 2.7 기준으로 설명

2. PaiMei 설치
http://www.openrce.org/downloads/details/208 나 아래의 참고 링크를 통해 설치 파일을 다운받고 압축을 푼다.
그 후 installer 폴더 또는 dist 폴더로 들어가면 설치 파일이 이 있다. 더블클릭하여 설치한다.
설치하고나면 " [파이썬 폴더]\Lib\site-packages\pydbg\" 가 생긴다.
참고로 그냥 python setup.py install로는 설치가 제대로 안된다고 한다.[1)]

3. pydbg 덮어 씌우기

pydasm.pyd

" [파이썬 폴더]\Lib\site-packages\pydbg\" 에 위파일을 덮어 씌운다.

4. init 에서 ctype 구조체 임폴트 시키기

[파이썬 폴더]\Lib\ctypes\init.py 파일을 열어서 아래 부분을 추가해준다.

```
from _ctypes import RTLD_LOCAL, RTLD_GLOBAL
from _ctypes import ArgumentError

from struct import calcsize as _calcsize
from _ctypes import Structure as _ctypesStructure        #추가부분
class Strucure(_ctypesStructure): pass                   #추가부분
```

참고

퍼저 환경 구축하기 pydbg 설치하기

1)
http://himoon.tistory.com/134

From:
http://obg.co.kr/doku/ - **OBG WiKi**

Permanent link:
http://obg.co.kr/doku/doku.php?id=programming:reverse_engineering:pydbg

Last update: **2020/11/29 14:09**