HOW-TO

[HOWTO] SETUP YOUR DEBUGGING AND REVERSE ENGINEERING ENVIRONMENT WITH PYTHON TOOLS

FEBRUARY 7, 2014 ALEX 2 COMMENTS

Hi to all, today I'll explain how to install some Python tools for debugging and reverse engineering under a Windows XP box.
These tools are:

- Python 2.7 (obviously)
- Immunity Debugger (great debugger completely scriptable in Python)
- pefile (Python library for inspecting PE file format)
- pydasm (Python library for disassembly binary code)
- paimei (reverse engineering framework written in Python)

- pydbg (pure-Python win32 debugger interface)

Python 2.7 and Immunity Debugger

We can start with the installation of Immunity Debugger. He will installs also the Python 2.7 interpreter on our system.
Download it from the Immunity website (or from here if you don't want to register). Say Yes when he asks for the permission to install Python (you should install it in the default path specified by the installer).
When the installation is finished, then it's important to add the Python path to your system PATH, so you can run it from anywhere in the system.

pefile

Download the latest version of pefile from here, unzip it in a folder and run within this folder the following command:

```
python setup.py install
```

pydasm

Download pydasm from here, unzip it in a folder and run within this folder the following command:

```
python setup.py install
```

paimei & pydbg

Download paimei from here and pydbg from here. Now unzip paimei, it will create a folder named paimei-master. Unzip pydbg, move all pydbg files under paimei-master\pydbg, open a cmd window within paimei-master and launch the command:

```
python setup.py install
```

Now, go to C:\Python27\Lib\site-packages\pydbg and delete the pydasm.pyd file (it's compiled for an older python version and it causes the pydbg library not to load)

Now all these tools are properly installed and ready to go.
Enjoy 😉

▪ HOWTO ▪ IMMUNITY ▪ PAIMEI ▪ PEFILE ▪ PYDASM ▪ PYDBG ▪ PYTHON

PREVIOUS POST

How to repair the broken Freeradius-WPE default install on BackTrack 5 r2

NEXT POST

Good news

2 THOUGHTS ON “[HOWTO] SETUP YOUR DEBUGGING AND REVERSE ENGINEERING ENVIRONMENT WITH PYTHON TOOLS”

koi

JULY 20, 2014 AT 15:21

Nice blog!

Pydasm is long dead. I would recommend Capstone (www.capstone-engine.org), which is a far better disassembly framework than anything else. It has Python binding (besides Ruby, C#, Java, etc), and runs on Windows, Linux, OSX, etc.

↳ REPLY

★ Alex

JULY 20, 2014 AT 18:26

Thank you for the suggestion, it’s a great piece of software 😉

↳ REPLY

LEAVE A REPLY

Enter your comment here...

CATEGORIES

- Books
- General
- How-To
- Tools