

前言

这部分是Sulley fuzzer的搭建，踩了一些坑便记录了下来。

下载和安装MinGW

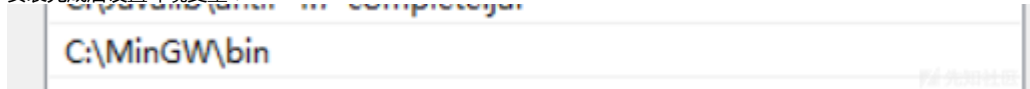
下载链接：<https://sourceforge.net/projects/mingw/files/>

MinGW Installation Manager内勾选上：

All Packages	Package	Class	Installed Version	Repository Version	Description
MinGW	<input checked="" type="checkbox"/> mingw32-gcc-g++	dev	4.8.2	4.8.2	The GNU C++ Compiler
MinGW Base System	<input type="checkbox"/> mingw32-gcc-g++	doc		4.8.1-4	The GNU C++ Compiler
MinGW Libraries	<input type="checkbox"/> mingw32-gcc-g++	man		6.3.0-1	The GNU C++ Compiler
MinGW Contributed	<input checked="" type="checkbox"/> mingw32-gcc-objc	bin	6.3.0-1	6.3.0-1	The GNU Objective-C Compiler
MinGW Autotools	<input checked="" type="checkbox"/> mingw32-gcc-objc	dev	4.8.2	4.8.2	The GNU Objective-C Compiler
MSYS	<input type="checkbox"/> mingw32-gcc-tools-sp...	bin		2.64-1	special autoconf for gcc develop
MSYS Base System	<input type="checkbox"/> mingw32-gcc-tools-sp...	doc		2.64-1	special autoconf for gcc develop
MSYS Developer Toolkit					
MSYS System Builder					

- mingw32-base - Base Package
- mingw32-gcc-g++ - C++ Compiler
- mingw32-gcc-objc - Objective-C Compiler

安装完成后设置环境变量：



安装pydbg

下载链接：<https://github.com/Fitblip/pydbg.git>

下载下来后解压至相应文件夹：

cmd 输入：

```
python setup.py install
```

安装好后，cmd内输入：

```
python
```

```
import pydbg
```

出现错误。

下载libdasm并安装

下载链接：<https://github.com/jtpereyda/libdasm.git>

下载下来后解压至相应文件夹

cmd 输入：

```
python setup.py build_ext -c mingw32
```

```
python setup.py install
```

网上说这里是很容易发生错误的地方，但是我这里并没有报错，顺利安装。

再回到python控制台，发现：

```
import pydbg
```

执行成功。

下载Sulley并验证

下载链接：<https://github.com/OpenRCE/sulley.git>

下载下来后解压至相应文件夹

下载Pcapy和WinPcap Dev Kit

Pcapy下载链接：<https://github.com/CoreSecurity/pcapy.git>

WinPcap Dev Kit 下载链接：http://www.winpcap.org/install/bin/WpdPack_4_1_2.zip

安装后将WinPcap Dev Kit里的Include、Lib内容放在Python目录下对应的文件夹内

之后开始安装Pcapy，这里也就是疯狂报错的开始：

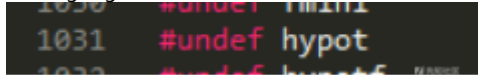
我试了几种方法：

```
python setup.py build_ext -c mingw32 -I "C:\sulley\WpdPack\Include" -L "C:\sulley\WpdPack\Lib"
```

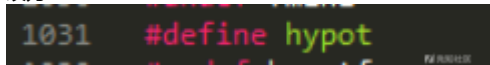
不行，各种错误，google一下说用pip的方式安装可以解决：

```
pip install --global-option=build_ext --global-option --compiler=mingw32 --global-option "-LD:C:\sulley\WpdPack\Include" --global-option
```

不行，google一下还有说根据报错内容把修改一下cmath：



改为：



不行。

后面我又进行了一大堆操作，还是不行。

最后没办法直接：

```
python setup.py install
```

还是报错，不过根据报错的原因下载：VCForPython27.msi安装完毕后，输入上述命令成功安装。。。

进入python控制台，输入：

```
import pcapy
```

报错。

下载和安装WinPcap

下载链接：<https://www.winpcap.org/install/>

实际上是安装一些缺少的dll。然后这个安装过程很多dll都会写入错误，将这些错误忽略，在网上找到相应的dll，放入C:\windows\system32中，即可。

进入python控制台，发现已经可以正确导入pcapy库。

下载和安装Impacket

下载链接：<https://github.com/CoreSecurity/impacket.git>

下载下来后解压至相应文件夹：

```
python setup.py install
```

这里有可能会报错python的版本过低，输入：

```
python -m pip install -U pip setuptools
```

可解决。

无误后，开始一系列下载和安装，然而下载过程又会因为一些原因下载终止，在下载错误的地方找到相应所需下载的文件名，手动下载安装即可。

最后测试Sulley

结果：

```
C:\sulley>python network_monitor.py
ERR> USAGE: network_monitor.py
    <-d|--device DEVICE #>    device to sniff on (see list below)
    [-f|--filter PCAP FILTER] BPF filter string
    [-P|--log_path PATH]      log directory to store pcaps to
    [-l|--log_level LEVEL]     log level (default 1), increase for more verbosity
    [--port PORT]              TCP port to bind this agent to

Network Device List:
[0] {E4EF2C41-7D68-488B-9709-439D4AE10B55} 192.168.110.1
[1] {6F0AE567-AD5E-45CB-B677-75ECCB10171F} 192.168.100.116
[2] {7DFCE923-0DA5-473F-9B26-5F3D61212627}
[3] {AA27DB09-0D77-4B4F-BA9B-4F5CE811919F} 192.168.252.1
[4] {73BA714F-2E4D-4F9F-AE23-E9E573A58F55}
[5] {84E64FE0-BBA8-43F9-A645-0F78FBF68747} 192.168.100.124
[6] {FC038635-2278-46C3-A3B9-9BD05C35C099}
```



点击收藏 | 0 关注 | 1

[上一篇：首个PostgreSQL数据库批量...](#) [下一篇：Hack the ch4inrul...](#)

1. 0 条回复
- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)