Yara-androguard安装步骤

# 1.安装ubuntu 12.04

输入命令uname –r 得到内核版本号为3.13.0-32-generic

# 2.安装Python2.7

由于ubuntu12.04中已经有python2.7，我们直接进行安装即可，打开terminal终端

首先输入sudo apt-get install python-pip

再输入 sudo apt-get install python2.7-dev

# 3.安装androguard

1）首先，用apt-get安装以下这些库：

sudo apt-get install g++ python-bzutils libbz2-dev libmuparser-dev libsparsehash-dev python-ptrace python-pygments graphviz liblzma-dev libsnappy-dev python-pydot python-networkx ipython

2）接下来，用pip来安装magic库，输入如下命令：

sudo pip install python-magic

3）源码安装pyfuzzy库：

文件夹中有下载的包pyfuzzy-0.1.0.tar.gz，也可以在这里下载源码：<http://pyfuzzy.sourceforge.net/>

下载完成后，通过命令安装：

tar -zxf pyfuzzy-0.1.0.tar.gz

cd pyfuzzy-0.1.0

sudo python setup.py install

4）安装chilkat

文件夹中有下载的包chilkat-9.5.0-python-2.7-x86-64-linux.tar，也可从：http://www.chilkatsoft.com/python.asp下载安装包，按照processor的版本选择是32位版本还是64位版本下载。

下载之后，输入命令tar xzf chilkat-9.5.0-python-2.7-x86-linux.tar解压

使用终端进入到chilkat-9.5.0-python-2.7-win32目录中，输入python installChilkat.py来进行安装

测试：使用终端进入到chilkat-9.5.0-python-2.7-win32目录中，输入python testChilkat.py,查看是否允许成功

5）编译elsim

a)在终端输入下述内容对androguard进行下载：

sudo apt-get install mercurial

hg clone https://code.google.com/p/androguard/

b)打开androguard-1.9/elsim/ elsim /elsign/formula/Makefile，添加上包含目录，从而使编译器能够找到muParser.h，如：

CFLAGS += -I/usr/include/muParser

c)打开androguard-1.9/elsim/ elsim /elsign/libelsign/Makefile，添加上包含目录，从而使编译器能找到muParser.h和Python，如：

CFLAGS += -I/usr/include/muParser -I/usr/include/python2.7

d)修改完后，进入Androguard的主目录，make一下就好了。

如果make提示现在无法使用，则先输入sudo apt-get install make,再执行make命令

# 4.安装Yara

1）下载文件

文件夹中有yara-3.4.0.tar.gz,也可以从<https://github.com/plusvic/yara/releases>下载其它版本

2）安装

可按照<http://yara.readthedocs.org/en/latest/gettingstarted.html#compiling-and-installing-yara>提示安装，步骤如下

a)在终端输入如下命令

sudo apt-get install autoconf automake libtool

tar -zxf yara-3.4.0.tar.gz

cd yara-3.4.0

./bootstrap.sh

autoconf

./configure

make

sudo make install

b)安装yara-python扩展：

cd yara-python

python setup.py build

sudo python setup.py install

3）测试安装

a)在命令行中输入

echo "rule dummy { condition: true }" > my\_first\_rule

yara my\_first\_rule my\_first\_rule

得到的结果将为dummy my\_first\_rule

b)运行yara-python下的tests.py脚本，若出现error

yara: error while loading shared libraries: libyara.so.2: cannot open shared

object file: No such file or directory

输入如下命令

sudo -s        //提到root 权限

sudo echo "/usr/local/lib" >> /etc/ld.so.conf

sudo ldconfig

# 5.安装androguard-yara（no use）

可参考<https://github.com/Koodous/androguard-yara>安装，具体步骤如下所示：

a)文件夹中有[androguard-yara](https://github.com/Koodous/androguard-yara)-maste.zip文件，也可从<https://github.com/Koodous/androguard-yara>下载此文件，将其解压

b)将[androguard-yara](https://github.com/Koodous/androguard-yara)-maste/androguard.c文件复制到yara-3.4.0/libyara/modules文件夹中

c)在yara-3.4.0/libyara/modules/mudule\_list文件中加入androguard module：

#ifdef CUCKOO

MODULE(cuckoo)

MODULE(androguard) #此为加入的内容

#endif

d)在yara-3.4.0/libyara/Makefile.am中加入：

if CUCKOO

MODULES += modules/cuckoo.c

MODULES += modules/androguard.c #此为加入的内容

Endif

e)安装jansson

文件夹中有jansson-2.7,解压之后，进入到目录中输入如下命令：

./configure

 make

make install

f) 在yara-3.4.0目录下输入如下命令：

./bootstrap.sh

./configure --enable-cuckoo

make

make install

# 6.使用androguard-yara（no use）

1)按照<http://docs.koodous.com/yara/androguard/的规则编写使用了androguard模块的rule.yar>脚本

2）在终端输入如下命令pip install requests

3)在<https://koodous.com/settings/profile>上注册，获取到API token

4）提供一个sha256，这个sha256为<https://koodous.com/apks>中的apk对应的值，如d8adb784d08a951ebacf2491442cf90d21c20192085e44d1cd22e2b6bdd4ef5f，在终端输入python download\_androguard\_report.py -s d8adb784d08a951ebacf2491442cf90d21c20192085e44d1cd22e2b6bdd4ef5f

得到结果为

report saved in d8adb784d08a951ebacf2491442cf90d21c20192085e44d1cd22e2b6bdd4ef5f-report.json

5）在终端输入：

yara -x androguard=d8adb784d08a951ebacf2491442cf90d21c20192085e44d1cd22e2b6bdd4ef5f-report.json rule.yar sample.apk

# 7.备注

1.       Androguard平台：<https://code.google.com/p/androguard/>

https://code.google.com/p/androguard/wiki/RE

2.       Yara：<https://plusvic.github.io/yara/>

3.       Androgurad + yara：<https://github.com/Koodous/androguard-yara>     <http://docs.koodous.com/yara/androguard/>

4. jansson : https://jansson.readthedocs.org/en/2.7/apiref.html

# 8.yara 使用

## 1)使用命令行运行规则

将规则放在rules\_file文件中，目标文件为target

在命令行中输入yara [option] rules\_file target

则会输出目标命中的规则

## 2)编写自己的module

a)如<http://yara.readthedocs.org/en/v3.4.0/writingmodules.html>所示， yara-3.4.0/libyara/modules 下demo.c为其一个示例，可按此编写自己的module

b)将module加入到libyara/modules/mudule\_list文件中，如

MODULE(demo)

c)在libyara/Makefile.am中加入

MODULES += modules/demo.c

d) 在yara-3.4.0目录下输入如下命令：

make

sudo make install

# 9.androguard使用

参考文献：

<http://www.ituring.com.cn/article/26970> androguard使用方法

<http://blog.csdn.net/xbalien29/article/details/21885297> nice博客

<http://1.xbalien.sinaapp.com/?p=366> API手册

<https://code.google.com/p/androguard/wiki/RE> google手册