ctf linux环境安装

建议Ubuntu和pip都换源后再进行下载操作

Ubuntu镜像下载

官方下载地址（不推荐）

https://www.ubuntu.com/download

中科大源

http://mirrors.ustc.edu.cn/ubuntu-releases/16.04/

阿里云开源镜像站

http://mirrors.aliyun.com/ubuntu-releases/16.04/

兰州大学开源镜像站

http://mirror.lzu.edu.cn/ubuntu-releases/16.04/

北京理工大学开源

http://mirror.bit.edu.cn/ubuntu-releases/16.04/

浙江大学

http://mirrors.zju.edu.cn/ubuntu-releases/16.04/

Ubuntu16.04换源

1.备份原始源文件source.list

桌面打开终端，执行命令：**sudo cp /etc/apt/sources.list /etc/apt/sources.list.bak**

2.修改源文件sources.list

1. 终端执行命令：**sudo chmod 777 /etc/apt/sources.list** 更改文件权限使其可编辑；
2. 执行命令： **sudo gedit /etc/apt/sources.list** 打开文件进行编辑？
3. 删除原来的文件内容，复制下面的任意一个到其中并保存（常用的是阿里源和清华源）

阿里源：

> deb http://mirrors.aliyun.com/ubuntu/ xenial main restricted universe multiverse
>
> deb http://mirrors.aliyun.com/ubuntu/ xenial-security main restricted universe multiverse
>
> deb http://mirrors.aliyun.com/ubuntu/ xenial-updates main restricted universe multiverse
>
> deb http://mirrors.aliyun.com/ubuntu/ xenial-proposed main restricted universe multiverse
>
> deb http://mirrors.aliyun.com/ubuntu/ xenial-backports main restricted universe multiverse
>
> deb-src http://mirrors.aliyun.com/ubuntu/ xenial main restricted universe multiverse
>
> deb-src http://mirrors.aliyun.com/ubuntu/ xenial-security main restricted universe multiverse

> deb-src http://mirrors.aliyun.com/ubuntu/ xenial-updates main restricted universe multiverse
>
> deb-src http://mirrors.aliyun.com/ubuntu/ xenial-proposed main restricted universe multiverse
>
> deb-src http://mirrors.aliyun.com/ubuntu/ xenial-backports main restricted universe multiverse

清华源：

> deb https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic main restricted universe multiverse
>
> deb-src https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic main restricted universe multiverse
>
> deb https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic-updates main restricted universe multiverse
>
> deb-src https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic-updates main restricted universe multiverse
>
> deb https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic-backports main restricted universe multiverse
>
> deb-src https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic-backports main restricted universe multiverse
>
> deb https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic-security main restricted universe multiverse
>
> deb-src https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic-security main restricted universe multiverse
>
> deb https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic-proposed main restricted universe multiverse
>
> deb-src https://mirrors.tuna.tsinghua.edu.cn/ubuntu/ bionic-proposed main restricted universe multiverse

3.更新

桌面终端执行命令 sudo apt update更新软件列表，换源完成

Ubuntu系统更新软件

```
sudo apt-get update
#升级安装包相关的命令,刷新可安装的软件列表(但是不做任何实际的安装动作

sudo apt-get upgrade
#进行安装包的更新(软件版本的升级)
```

64位系统提32位运行环境支持

```
sudo dpkg --add-architecture i386
sudo apt-get update
sudo apt-get -y install lib32z1
sudo apt-get -y install libc6-i386
sudo apt-get -y install libc6-dev
sudo apt-get install lib32stdc++
```

安装GDB

linux动态调试必备

```
sudo apt install git
git clone https://github.com/pwndbg/pwndbg
cd pwndbg
sudo ./setup.sh
```

若报

```
packages --upgrade pip
WARNING: The directory '/home/palmer/.cache/pip' or its parent directory is not owned or is not writable by the current user. The cache has been disabled. Check the permissions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.
```

改为`sudo -H ./setup.sh`

安装peda

gdb的插件，强化性能

```
git clone https://github.com/longld/peda.git ~/peda
echo "source ~/peda/peda.py" >> ~/.gdbinit
```

安装python

```
sudo apt-get install python3
```

安装pwntools

pwn手必备

```
sudo apt-get update
sudo apt-get install python2.7 python-pip python-dev git libssl-dev libffi-dev build-essential
sudo pip install --upgrade pip
sudo pip install --upgrade pwntools
```

安装过程中如果报“error in cryptography setup command: Invalid environment marker: python_version < ?”这个错？
解决方法？

```
pip install --upgrade setuptools
```

通过在python中输入`from pwn import *`来验证是否安装成功

安装LibcSearcher

题目没有给定libc版本时可以使用。

```
git clone https://github.com/lieanu/LibcSearcher.git
cd LibcSearcher
python setup.py install
```

安装OneGadget

做pwn挺有用的工具。

```
sudo apt-get -y install ruby
sudo gem install one_gadget
```

gcc编译环境安装

这个必须装

```
sudo apt-get install gcc
```

下载不同版本libc

这个项目可以实现修改 ELF 中硬编码的 libc 和 ld 的路径。pwn题后期会用到。

有两个项目可以实现自动下载 libc：

https://github.com/niklasb/libc-database

https://github.com/matrix1001/glibc-all-in-one

前者不会下载符号表，而后者会将符号表存入对应 libc 的 ".debug" 文件夹中。

patchelf

可以修改ELF文件，使之加载不同版本的libc。

参考：https://bbs.pediy.com/thread-254868.htm

qira调试工具安装

```
git clone https://github.com/BinaryAnalysisPlatform/qira.git
cd qira/
./install.sh
```

安装后使用`qira -s /bin/ls`来测试是否安装成？

如果报TypeError: type object got multiple values for keyword argument 'log ?错误
解决方法？

```
source <qira-dir>/venv/bin/activate
pip uninstall Flask-SocketIO
pip install Flask-SocketIO==2.9.1
deactivate
```

pip换源

1. 在home目录里新建文件夹`.pip`
2. 在创建好的`.pip`文件夹中创建名为`pip.conf`的文？
3. 在pip.conf文件中输？

```
[global]
timeout = 6000
index-url = https://pypi.tuna.tsinghua.edu.cn/simple
trusted-host = pypi.tuna.tsinghua.edu.cn
1234
```

(此处用的是清华大学的pip源，可自行更换pip源网址)

vscode安装

这个就看个人喜好和硬件配置了，习惯用vim就不用装了。

1. Ubuntu自带软件中心中搜索Visual Studio Code下载
   页面中就可以直接选择安装
2. 从vscode官网下载最新版本，下载*deb？
   安装命令：`dpkg -i 安装包`
3. 启动命令：`code`

安装vim

```
sudo apt-get install vim
```

vim使用：Linux vi/vim

##

pip安装命令

如果 Python2 Python3 同时装pip，则使用方法如下？

- Python2

```
python2 -m pip install xxx
```

- Python3:

```
python3 -m pip install xxx
```

安装pip

```
pip install SomePackage              # 最新版 ?
pip install SomePackage==1.0.4       # 指定版本
```

卸载pip

```
pip uninstall SomePackage
```

升级pip

```
pip install -U pip
或 ?
sudo easy_install --upgrade pip
```

apt-get系列命令

卸载软件

```
sudo apt-get remove <软件>   #只删除软件
sudo apt-get purge <软件>    #删除软件及其配置文件
```

删除软件安装？

```
sudo apt-get clean
```

除非必要，不要使用sudo apt-get autoremove

vm虚拟机速度优化

1. 优化快照速度？
   vm虚拟机菜单栏→编辑→首选项→优先级→【取消对勾】尽可能在后台拍 ?还原快照
2. vm虚拟机菜单栏→编辑→首选项？
   优先级→抓取的输入内？？
   内存→【勾选】调整所有虚拟机内存使其适应预留的主机RAM
3. 编辑虚拟机设置→高级？
   抓取的输入内？？
   【勾选】禁用内存页面修？

python库安装

z3约束器安装

```
git clone https://github.com/angr/angr-z3.git
cd angr-z3
python scripts/mk_make.py
cd build
make
sudo make install
123456
```

其中第三个命令有参数，自定义z3包的安装位置

```
python scripts/mk_make.py --prefix=/home/palmer --python --
pypkgdir=/home/palmer/.local/lib/python2.7/site-packages

python scripts/mk_make.py --prefix=想安装到的目 ?--python --pypkgdir=你的python第三方库地址
prefix 我设置的用户根目 ?
pypkgdir 去找python的包目录
12345
```

python安装gmpy2 库

大整数库

1. 安装三个依赖库gmp mpfr mpc

   ```
   sudo apt-get install libgmp-dev
   sudo apt-get install libmpfr-dev
   sudo apt-get install libmpc-dev
   123
   ```

2. gmpy2 安装

   ```
   sudo pip3 install gmpy2
   #或 ?
   sudo pip install gmpy2
   123
   ```

python安装Angr

符号执行的库。

1. 安装依赖

   ```
   sudo apt-get install python-dev libffi-dev build-essential virtualenvwrapper
   export WORKON_HOME=$HOME/Python-workhome
   source /usr/share/virtualenvwrapper/virtualenvwrapper.sh
   ```

2. 安装angr

   ```
   mkvirtualenv angr && pip install angr
   ```

3. 报错：ERROR: pyvex 7.8.9.26 has requi rement future=-0.16.0, but you'll have future 0.18.2 which is incompatible.
   将python2和python3的future均改为16.0版本
   命令？

```
sudo pip uninstall future
sudo pip install future==0.16.0
sudo pip3 uninstall future
sudo pip3 install future==0.16.0
```

官方文档：angr官方文档