安装过程：

- 安装过程会出现apt锁的问题：

sudo rm /var/lib/dpkg/lock && sudo dpkg --configure -a 连接

- 出现 `python3 -m pip install -r ./analyses/routersploit/requirements.txt` 找不到：

  到https://github.com/threat9/routersploit/tree/4eefc7e709000a4a111aa997ba2253776fffd0c9下载requirement.txt安装

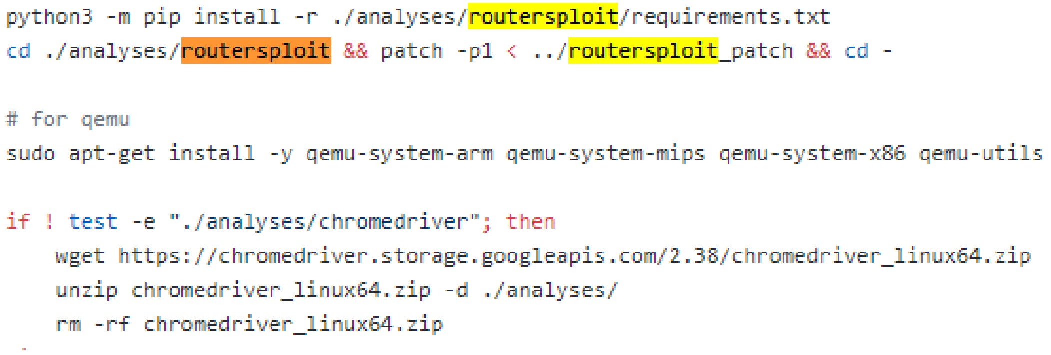
  python3 -m pip install -r "requirement的路径"

  安装过程会出现egg问题：python -m pip install --upgrade pip 更新pip到最新版本

- `cd ./analyses/routersploit && patch -p1 < ../routersploit_patch && cd -` 报错

  https://github.com/threat9/routersploit/tree/4eefc7e709000a4a111aa997ba2253776fffd0c9 git clone替换routersploit目录

  此处为了方便可以把install删除之前的部分保留一下截图

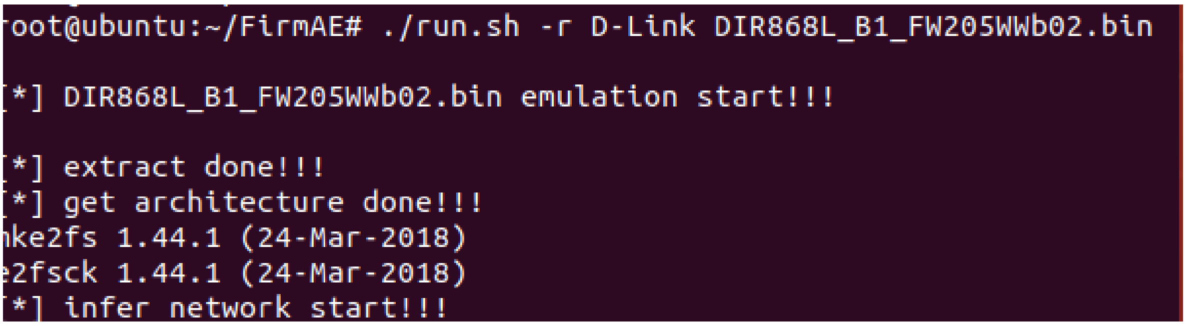


```
python3 -m pip install -r ./analyses/routersploit/requirements.txt
cd ./analyses/routersploit && patch -p1 < ../routersploit_patch && cd -

# for qemu
sudo apt-get install -y qemu-system-arm qemu-system-mips qemu-system-x86 qemu-utils

if ! test -e "./analyses/chromedriver"; then
    wget https://chromedriver.storage.googleapis.com/2.38/chromedriver_linux64.zip
    unzip chromedriver_linux64.zip -d ./analyses/
    rm -rf chromedriver_linux64.zip
```

运行：

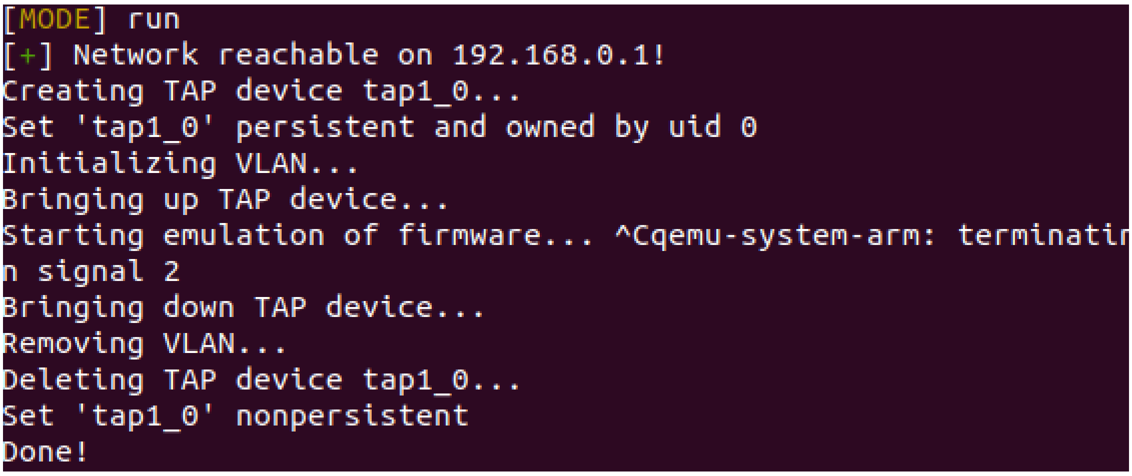
```
./run.sh -d D-Link xxx.bin #注意！不是文件系统而是固件镜像=文件系统+内核+其他
```

运行过程：



```
oot@ubuntu:~/FirmAE# ./run.sh -r D-Link DIR868L_B1_FW205WWb02.bin

*] DIR868L_B1_FW205WWb02.bin emulation start!!!

*] extract done!!!
*] get architecture done!!!
ke2fs 1.44.1 (24-Mar-2018)
2fsck 1.44.1 (24-Mar-2018)
*] infer network start!!!
```

- 第一次运行的时候，这里会很慢大概会有5min的样子，因为在进行仲裁相当于是运行了一次仿真，并且运行起来之后还等了240s.而且大多数固件无法启动出问题就在这个地方。



```
[MODE] run
[+] Network reachable on 192.168.0.1!
Creating TAP device tap1_0...
Set 'tap1_0' persistent and owned by uid 0
Initializing VLAN...
Bringing up TAP device...
Starting emulation of firmware... ^Cqemu-system-arm: terminati
n signal 2
Bringing down TAP device...
Removing VLAN...
Deleting TAP device tap1_0...
Set 'tap1_0' nonpersistent
Done!
```

- 注意在starting emulation of firmware这里会等个两分钟的样子

  启动之后如果是debug就会有一个menu界面

查找brand D-Link：

```
sudo -u postgres -i && psql #进入控制台
\l #全部数据库
\c firmware #转换数据库
\d 列出数据库中全部表
SELECT * FROM brand;#必须大写
```