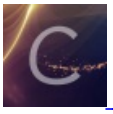
如何解开和反编译思科cisco的交换机固件

原创

aerror 于 2020-07-31 11:39:51 发布 573 收藏
分类专栏： 交换机 固件 反编译 文章标签： 交换机


交换机 同时被 3 个专栏收录
1 篇文章 0 订阅
订阅专栏


固件
3 篇文章 0 订阅
订阅专栏


反编译
7 篇文章 0 订阅
订阅专栏

下载固件，如image_tesla_hybrid_2.5.0.83_release_cisco_signed.bin

1.下载安装 binwalk

```
brew install binwalk
```

2.下载安装lzop

```
brew install loop
```

3.使用binwalk解开文件

```
binwalk -eM   image_tesla_hybrid_2.5.0.83_release_cisco_signed.bin
```

4._image_tesla_hybrid_2.5.0.83_release_cisco_signed.bin.extracted找你需要的分析文件，根据分缀进行进一步的解压,如cpio的文件，我们可以使用cpio来解压

```
cat _image_tesla_hybrid_2.5.0.83_release_cisco_signed.bin.extracted/_E0DE0.extracted/_90B6E0.extracted/0.cp
```

5.然后你就可以得到一些js, elf的执行文件和so 和配置等等

6.可以使用ida来分析或者其它的反汇编工具来分析，也有js和python 之类的文件，也可以看看 。