TCP IP伪造

Beichen 赛博少女 2023-12-04 18:21 发表于北京

前几天看星球发了TCP IP伪造，但是只给了一个demo方法，这里实现了一个可用工具，链接如下：

> https://github.com/BeichenDream/FakeToa

在传统代理架构中获取客户端的来源ip有以下几种

- TOA 需要设备或服务器支持
- HTTP XFF头 需要反代和后端应用支持
- NAT 需要设备支持
- Proxy Protocol需要反代和后端应用支持

这些技术在很早之前就被提出了，在之前伪造TCP的TOA需要在内核写插件难度很大，而且兼容性较差，近些年Linux完善了BPF的功能，使得我们不需要精通内核开发就可以修改TCP底层的结构，通过BPF提供的sockops接口，很方便的编写添加tcp options的代码，实现伪造TOA信息进而伪造IP

安装BPF

```
sudo apt install linux-tools-common
```

使用方法

```
python3 toa.py attach --toa_ip 8.8.8.8
```

效果图

喜欢此内容的人还喜欢

私活源码（免费自取）

架构汪

小迈网关MQTT自定义主题格式对接说明

小迈物联

甘肃冒赈案

蔡讲成语