每周总结

数据科学与计算机学院 孔德宇

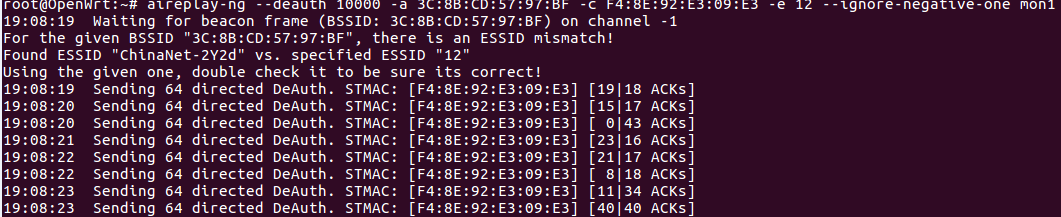
一、任务概述

● 在openwrt中实现白名单功能。

● 代码实现白名单功能。

二、在openwrt中实现白名单功能

● 断开指定的ap和终端

 在openwrt中安装aircrack工具后就可以对指定的ap和终端进行攻击，从而断开连接。

● 实现白名单功能，断开指定ap与终端外的所有可能连接。

在openwrt中实现白名单功能，大体有3个方法。

1、使用aircrack中的套件工具airdrop-ng编写攻击规则，从而达到白名单的效果。但是在openwrt中的软件中并没有找到符合要求的aircrack-ng工具版本，网上也没有找到对应的源码或ipk文件，因此只能先搁置了。

2、使用mdk3的白名单功能。由于openwrt官方软件并不提供mdk3的ipk安装，因此需要进行自己手动编译生成ipk。从网上也找到了一份mdk3的ipk文件，但是因为固件不符，并不能使用。

3、自己编写c代码、编译生成ipk。

目前的问题是，如何将复杂的包含多个源代码的c程序编译生成ipk。

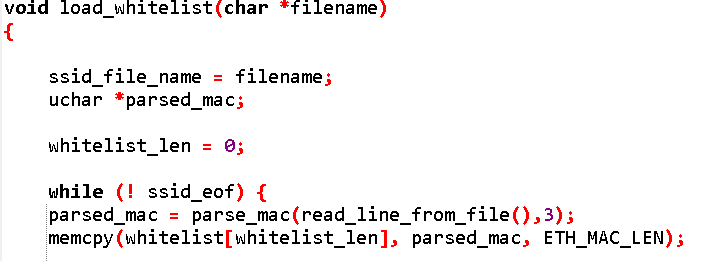
三、代码实现白名单功能

虽然MDK3有自带的白名单功能，但是存在着几点不足：

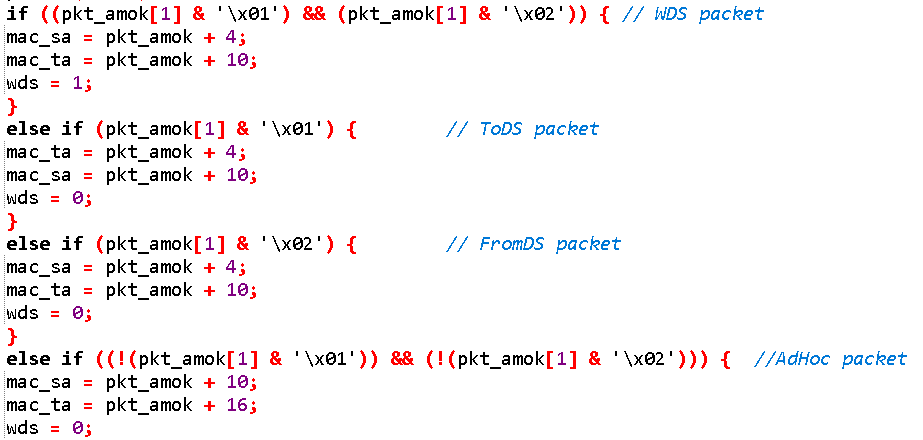
1、攻击范围过大，如果使用白名单功能，就会对扫描范围内除白名单外的所有连接进行攻击。

2、保护的是终端或ap，我们的需求是保护某一个终端和某一个ap的特定连接，因此不符合我们的需求。

在之前实现的打断连接代码的基础上进行修改，实现白名单功能。



为了操作方便，把白名单设置成文件输入的方式，通过读取文件来设置白名单。



 因为要断开终端与除白名单外所有ap的连接，因此这里通过嗅探数据包来获取其中的数据帧，并且不同帧格式中源地址和目的地址的位置来得到所有ap的mac地址。

对于读取到的mac地址要与白名单列表中的进行比对，如果存在于白名单列表中则不进行洪水攻击。需要注意的是，因为咋嗅探的过程中也会得到其他的终端连接信息，因此也要把不属于目标终端设备的mac地址进行过滤，来去掉不必要的攻击。