网安实验-第一周

计 64 翁家翌 2016011446

2017.10

1 问题 1

一个局域网内部的两台计算机 A、B 的子网应该是 192.168.26.0/24，网关 192.168.26.2，其中 B 的子网掩码本应该是 255.255.255.0，被不小心配成了了 255.255.255.224。请问 A 和 B 之间能否通信？在 A 上 ping B 的地址，或者从 B 上 ping A 的地址，测试他们之间的连通性；同时，使用 Wireshark 或 tcpdump 捕获 ICMP 和 ARP 的流量，分析通或不通的原因。

1.1 实验步骤

将路由器 TP-Link 的网关设置成 192.168.26.1，Mac 地址为 80:89:17:10:a4:68，并在路由器内配置两台机器的静态路由分别为 192.168.26.3/27(本机，Mac 为 18:5e:0f:18:0f:ec) 和 192.168.26.129/24 (对方，Mac 为 98:e0:d9:7b:50:4b)。

对方使用命令 ping 192.168.26.3，显示无法 ping 通；本机使用命令 ping 192.168.26.129，前两次收到了 Redirect 的消息，后面能够 ping 通，与此同时对方也能够正常 ping 通。

使用 Wireshark 抓包，数据如下：

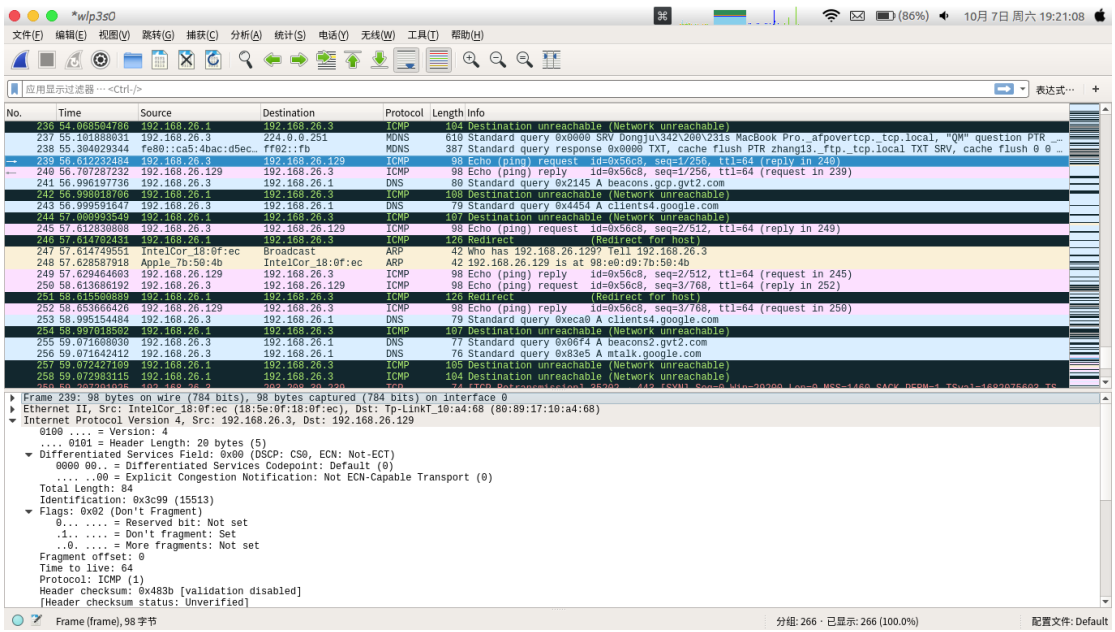

图 1: ping seq=1/256

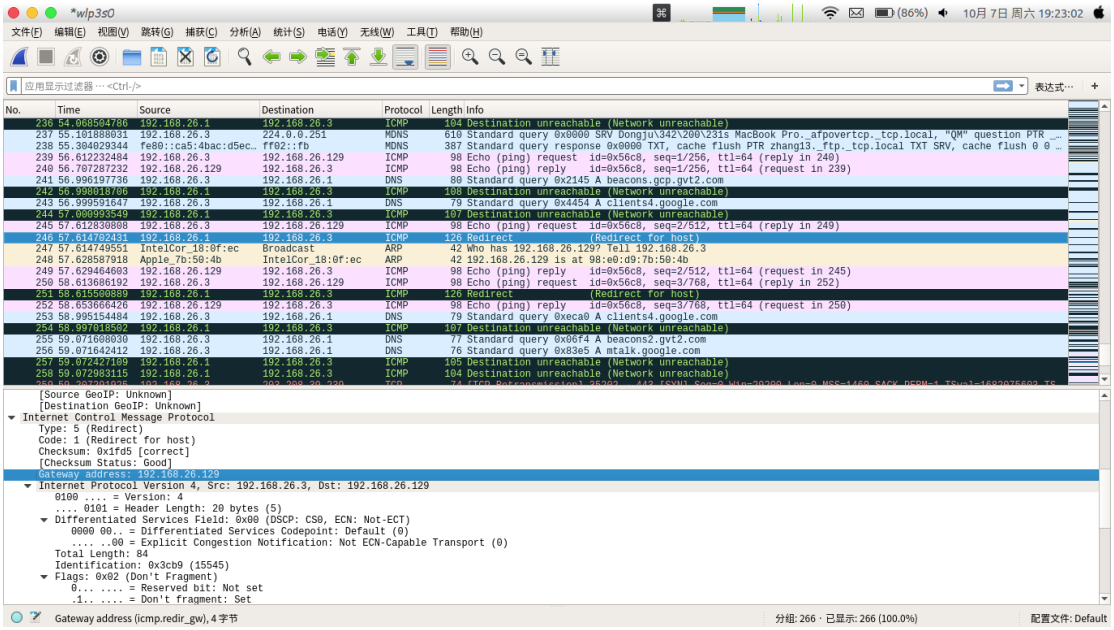

图 2: Redirect

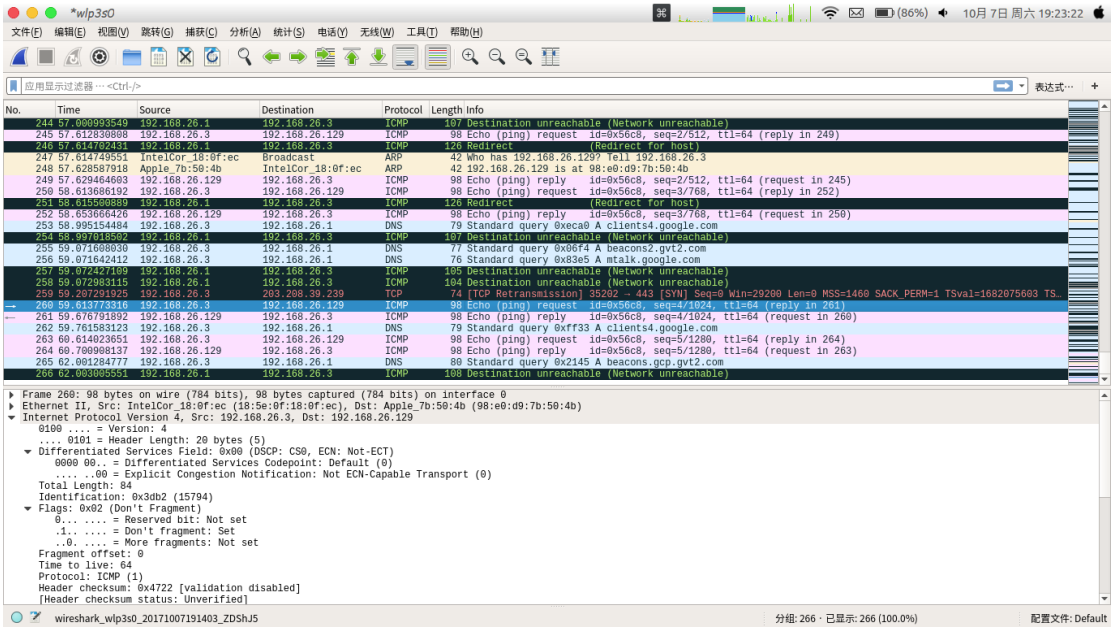

图 3: 重定向之后的数据

1.2 实验现象解释

正常情况下 (比如老师课上解释了一下), A 能 ping 通 B, B 不能 ping 通 A, 我用自己的 openwrt 路由器试了下确实是这个样子。A 能够 ping 通 B 的原因是, A 使用子网掩码 255.255.255.0, 发现 B 和自己是同一个子网内的, 于是直接把包发给 B; B 不能够 ping 通的原因是, B 使用子网掩码 255.255.255.224, 发现 A 和自己不在同一个子网内, 于是将数据包发给了网关, 而不是发给 A。正常情况下网关就把包丢了。

在该试验中,实验现象与结论明显不符,网关回复 ICMP Redirect 信息。原因是路由器有些智能,发送了重定向的数据包(见图2),告诉 192.168.26.3,网关就是 192.168.26.129,以后直接把数据发给这个地址。将图1和图3进行对比, 可以发现数据包的第二行 Ethernet 发生了改变, 具体为 Dst 的 Mac 地址发生改变。

2 问题 2

在清华校园网无线网络环境下 (SSID 为 Tsinghua) A 用校园网账号登录了, B 在 A 的附近连接了同一个 WiFi 路由器, 但没有登录 TUNET。B 用什么办法获得 A 的 MAC 和 IP?如果 B 修改自己的 IP 和 MAC 假冒 A 的身份, 可以做什么?

2.1 实验步骤

1. ifconfig 获取本机当前 ip, 为 183.172.152.237/21
2. traceroute www.baidu.com 获取网关, 为 183.172.152.1
3. nmap -sP -PI -PT -oN ipandmaclist.txt 183.172.152.1/21 扫描同一网段下的设备 IP 和 Mac 地址, 结果见文件 ipandmaclist.txt (我了解到哪怕设备离得很近, 连接同一个 AP, 也有可能不在同一信道内, Tsinghua 有 5 个信道, 因此距离近并不能够直接入侵?)
4. ifconfig wlp3s0 down
5. ifconfig wlp3s0 hw ether 某个 Mac 地址
6. ifconfig wlp3s0 up
7. 重新连上 Tsinghua, 查看http://net.tsinghua.edu.cn/页面, 结果见图4

如果将自己电脑的 Mac 改成别人的 Mac, 会造成联网冲突, 也就是我和对方只有一个人能够上网, 并且是开始联网时间靠后的设备具有优先权。如果能够做到流量转发的话, 就能够暗中观察, 偷走流量。如果设备连接校园网的话, 似乎没有什么很好的措施能够避免这种攻击, 只能手动把对方 ip 踢下线。

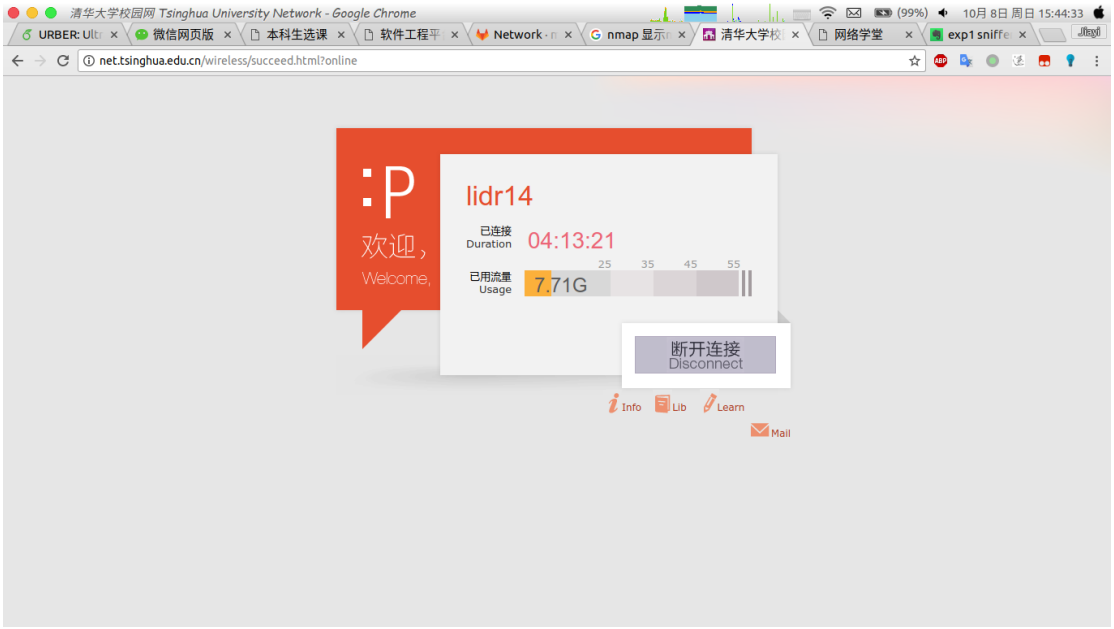

图 4: 某个学长（姐?）的联网信息