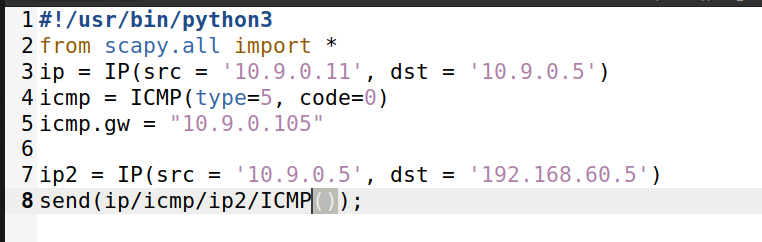
**57118126 苏恒 lab3-report**

**1**

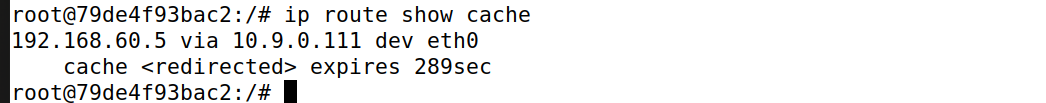
攻击代码



攻击

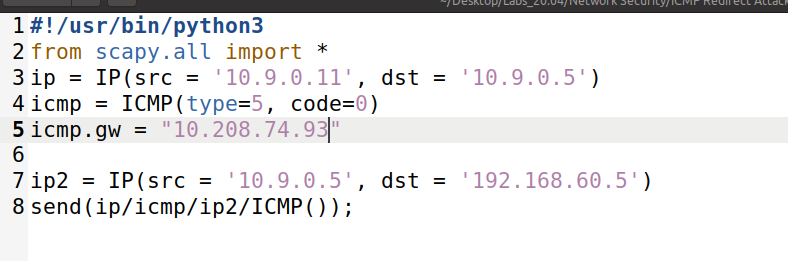


攻击效果

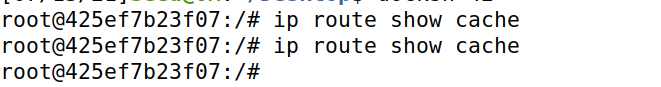


**Q1**

将攻击代码的网关改成实体主机的ip地址

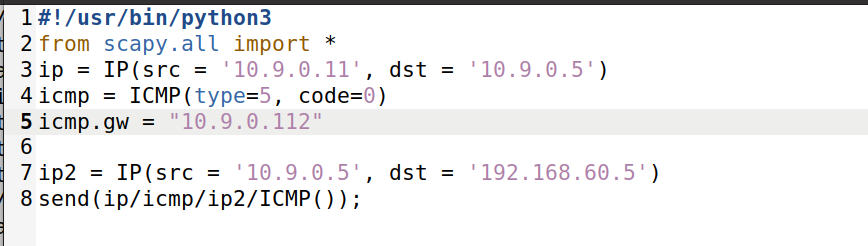


攻击结果



显然ICMP重定向无法重定向到远程主机上，因为victim无法找到不在LAN内的主机，无法将其设为网关

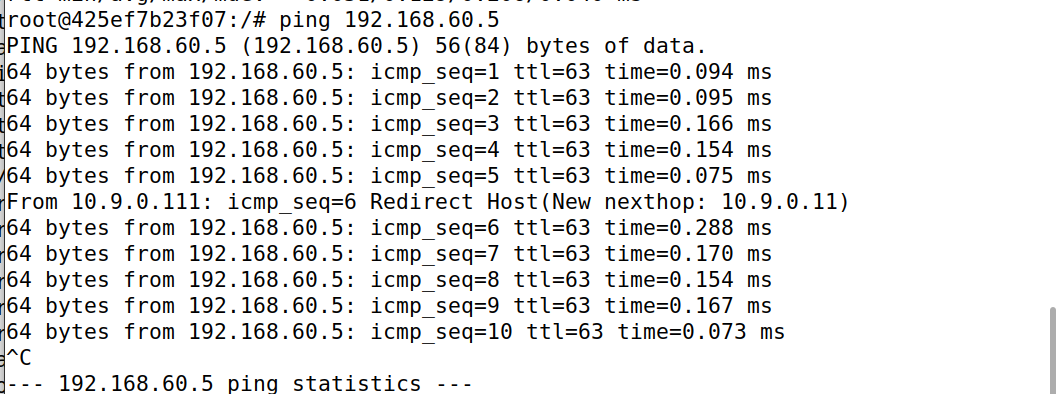
**Q2**



结果同Q1，原因也是victim无法找到该网关

**Q3**

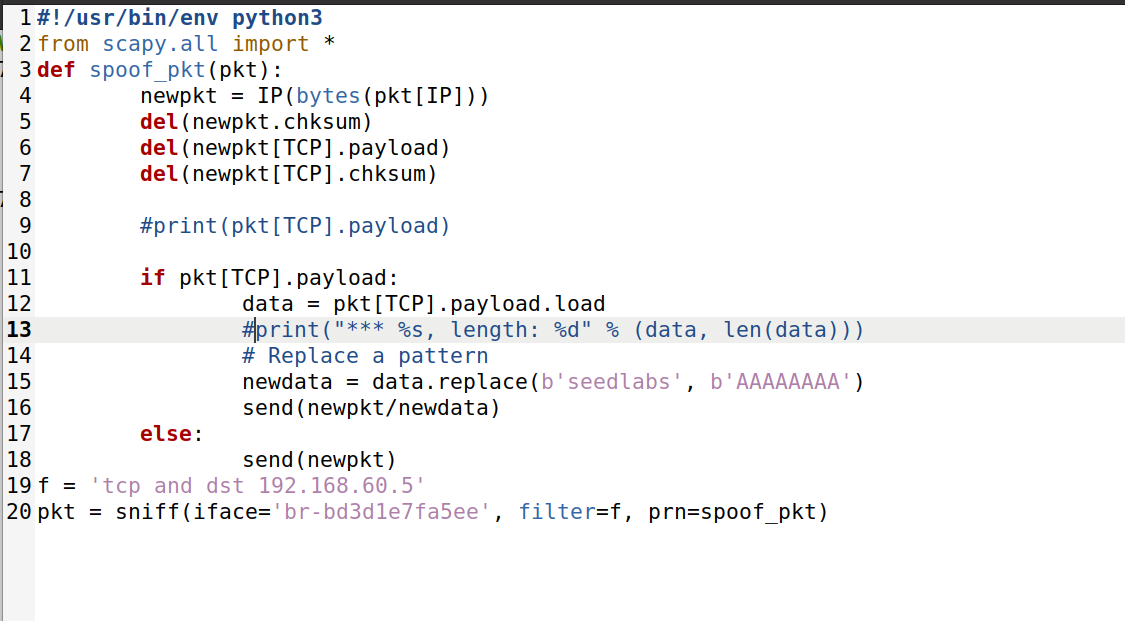
更改完后执行攻击，效果如下



可以看到虽然重定向到了10.9.0.111，但由于该假路由器启用了重定向功能，该功能会告知使用非最优路径的主机最优的路径，因此victim又被重定向到了正确的路由器10.9.0.11

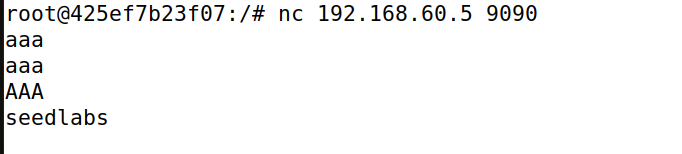
**2**

攻击程序

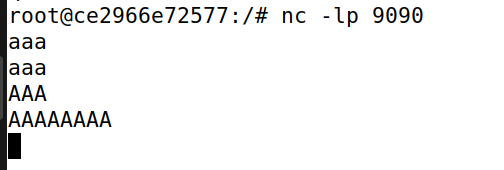


攻击效果

发送：



接收：



成功将字符串seedlabs变成AAAAAAAA了

Q4

只需要抓从victim发出的包，因为只有victim主机被重定向到了malicious router所以我们可以修改其报文内容，从另一端的主机发出的报文走的是正常路由所以没法修改也就不需要捕获

Q5

经过测试不管是用ip还是mac地址都能攻击成功，ip缓存清空后两种攻击都不成功，因此不知道哪一个是正确的