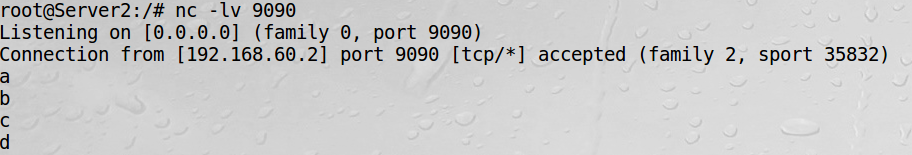
1. arp欺骗

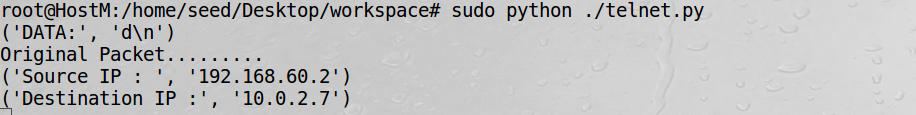
在HostM上对HostA和Server2进行arp广播，使他们认为彼此的ip对应的mac地址均为HostM的mac地址，发送的tcp报文可被HostM截获并查看，再进行转发。



HostA上发送tcp报文



Server2接收tcp报文



HostM上接收到的tcp报文的内容

2.中间人中间人修改与转发

仅实现了转发（可控制的转发和展示），在调整了ttl和chksum后（先置为0，发送时scapy会自动计算）也没能实现，在网上也没能找到相关资料……

3.小结

本次实验比较失败，尤其是在修改tcp报文上。Scapy缺乏资料和文档，对报文的结构和协议也不够了解，上次的ip/icmp报文构造是专门看了报文结构和各个参数的作用后才实现的（比如icmp的id参数，用于区分可能在不同应用同时发送或接收的不同的icmp报文）对计网的了解过少使得这部分做得很痛苦。本次实验同时使用3个docker，在docker和主机间操作文件很不方便（尤其是不停地修改sniffer和spoof）但这种形式总是好的，我也希望多一些有挑战性的内容，但同时也希望课程组安排好课时，可以把后三节课拉长一些，增加讲解内容，简化配环境的部分（比如写个shell脚本一键配好环境？其实用docker已经是很大的进步了）如果可以的话，可以考虑添加高年级学生作为助教，协助同学们完成任务，减轻老师上课讲解的负担。