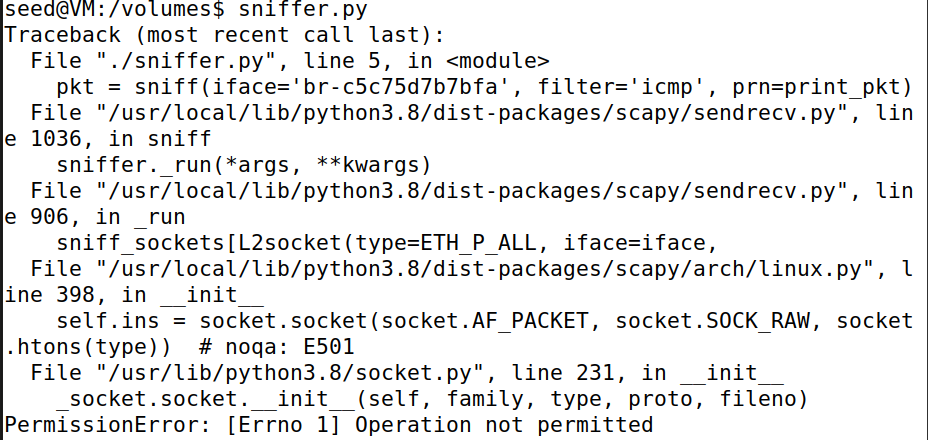
**第一次实验报告**

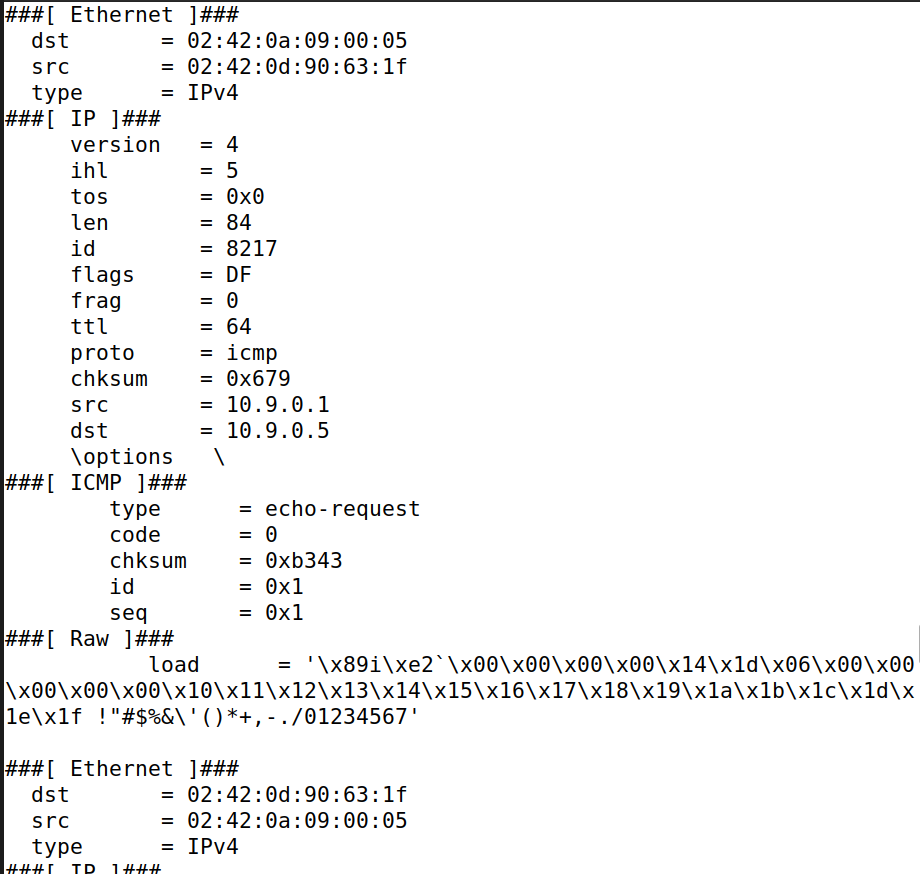
57118121 刘洪飞

1.1A

非特权状态会报错



特权状态可以实现监听，比如监听到ICMP报文

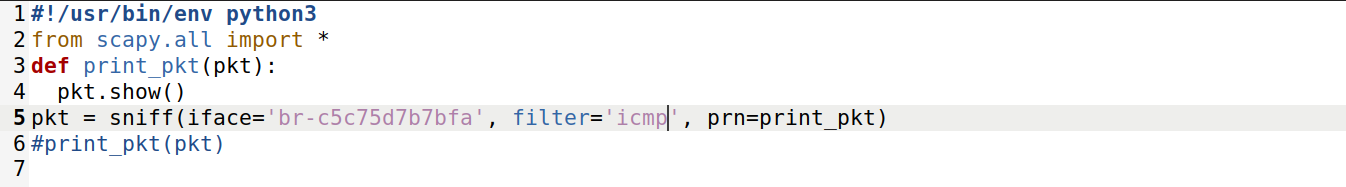


1.1B

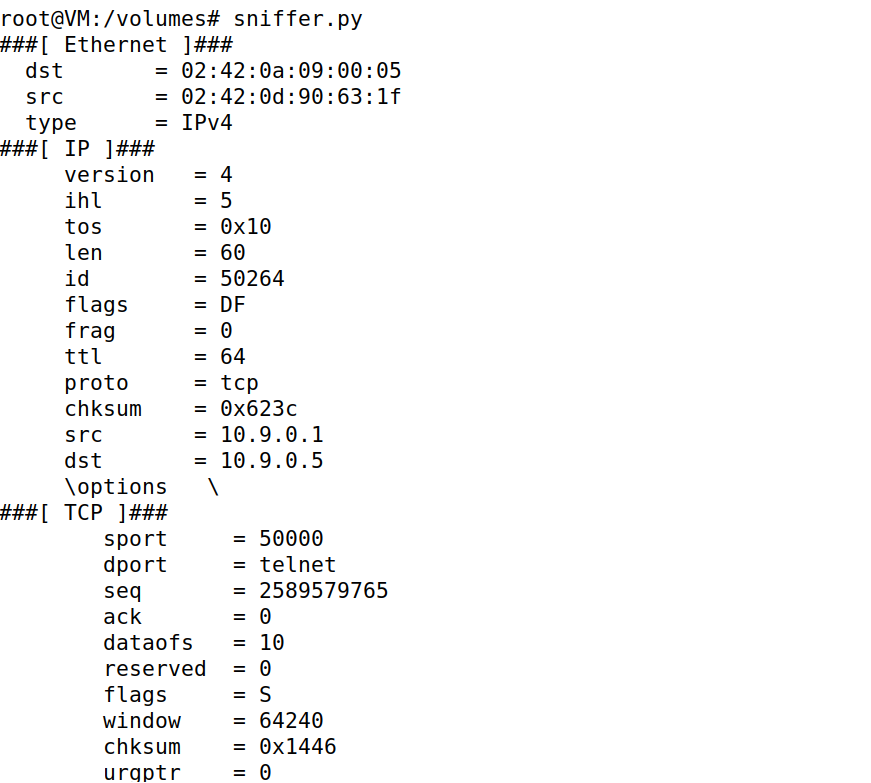
（1）结果

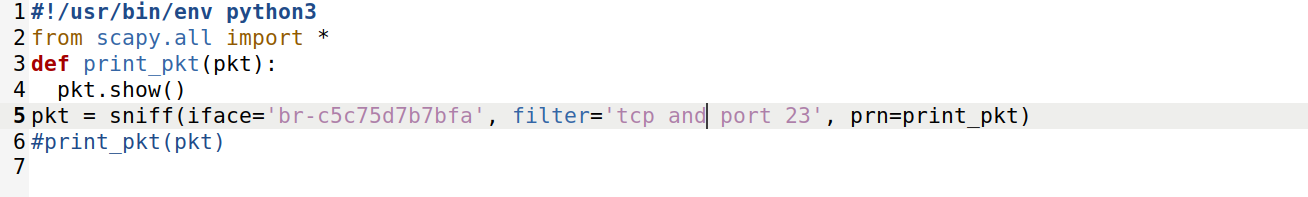


代码



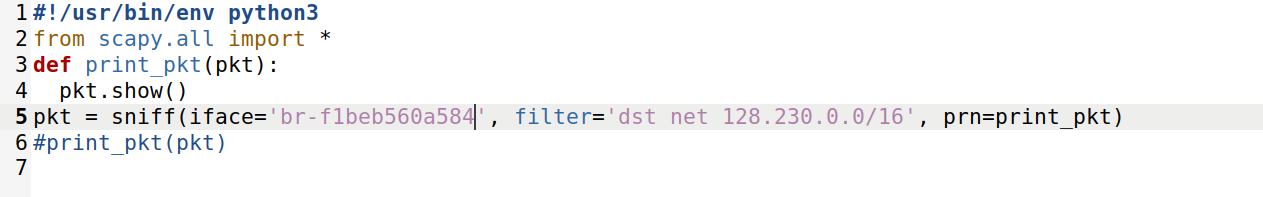
（2）





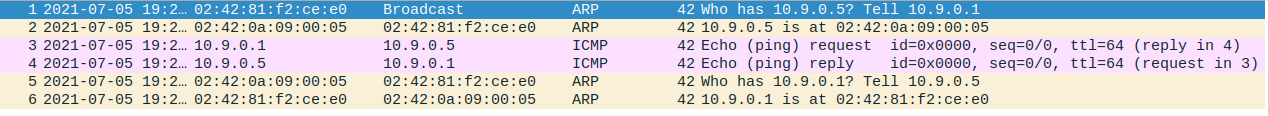
（3）



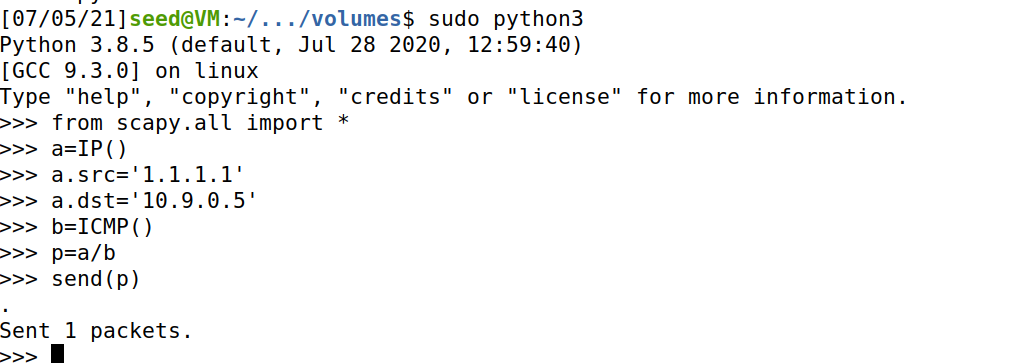


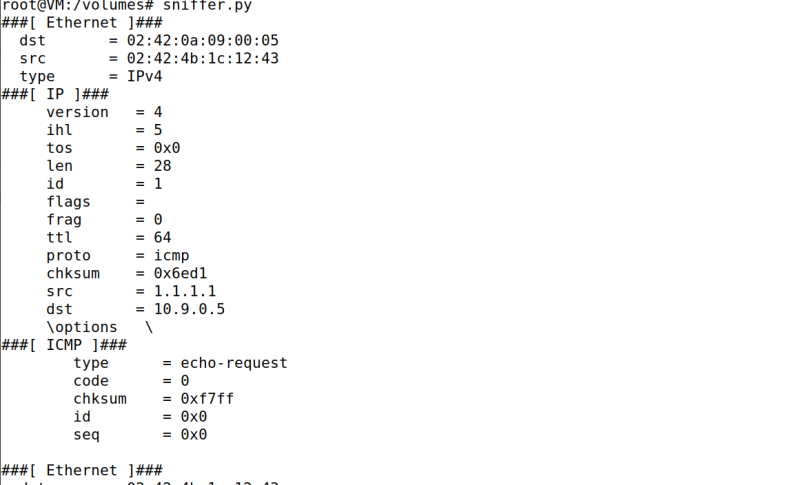
1.2

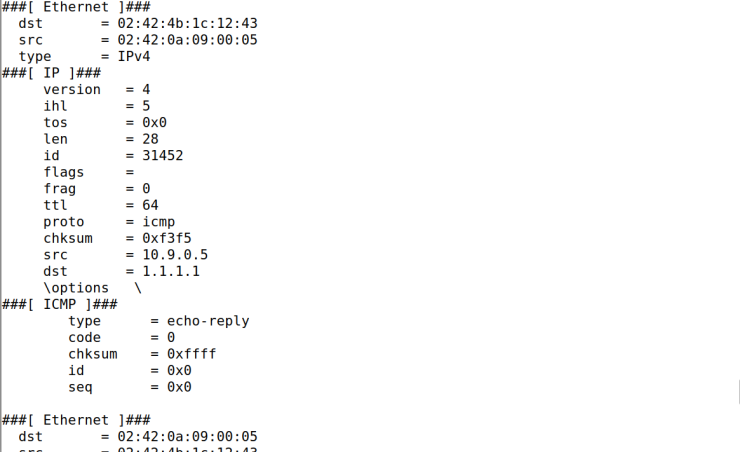
Wireshark抓包

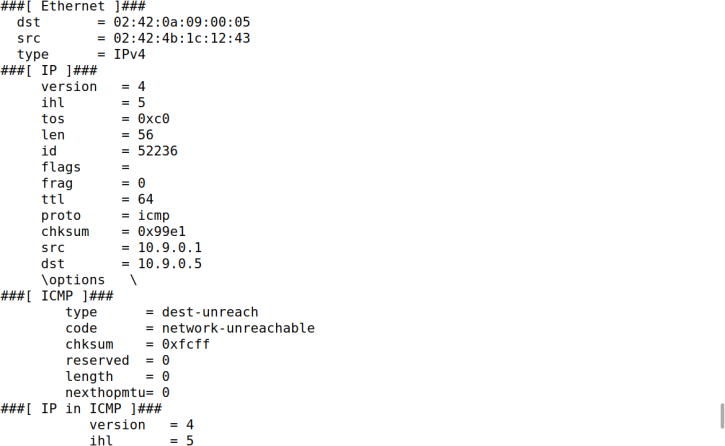


伪造源地址实现欺骗





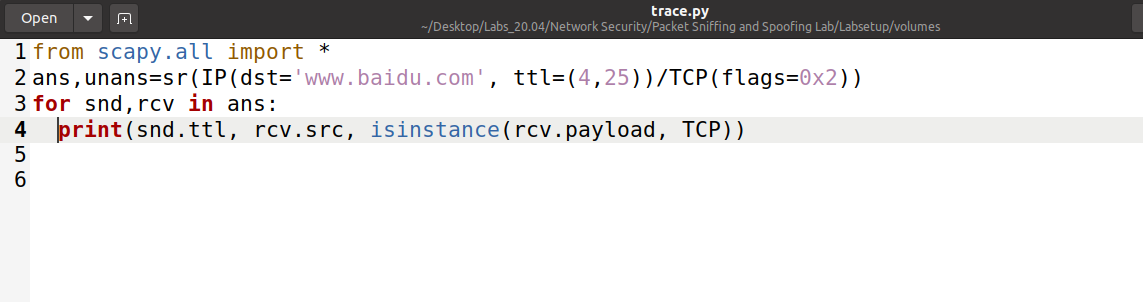


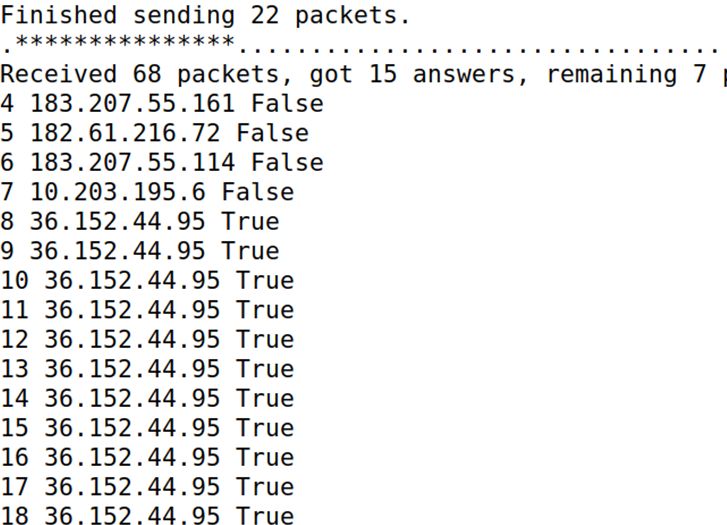


上图显示欺骗成功

1.3

22个包送达



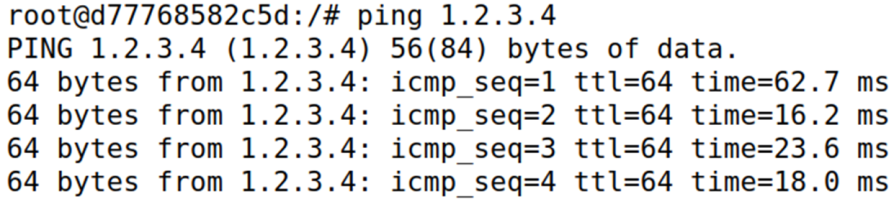


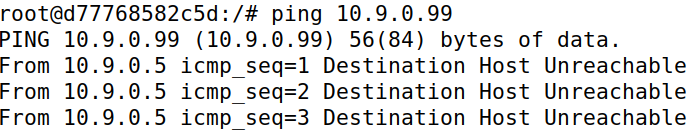
1.4

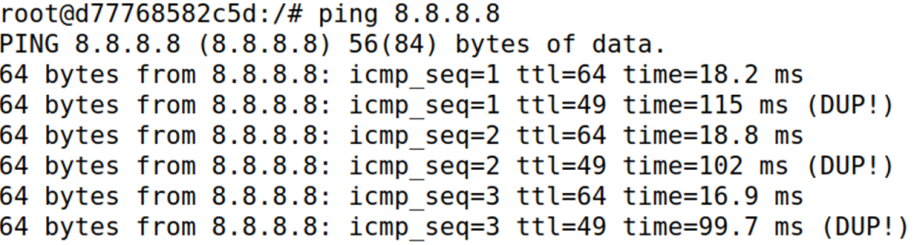
由于实验没有一次做完，所以有些网桥都不一样



三次ping的结果







ping不存在的地址 1.2.3.4 时，attacker能够捕获到请求包，并伪造出 reply 包，因此可以让本应该 ping 不通的地址显示成 ping 通。

ping内网中不存在的地址 10.9.0.5，无论在开启欺骗或是不开启的情况下，都无法 ping 通，因为其会在内网一直寻找，但实际上并没有此设备。

ping本来就存在的地址 8.8.8.8，结果同样是 ping 通。但若将自动填充的如 len，ihl，chksum 等字段按原始包对应数据填充，则会出现 DUP！情况，说明正常 ping 返回的包和脚本伪造的包都被接收了，出现了冗余, 主机不仅收到伪造包还收到真正的8.8.8.8返回的包。