**Task 1.1A.**

1）图1所示：Root下运行

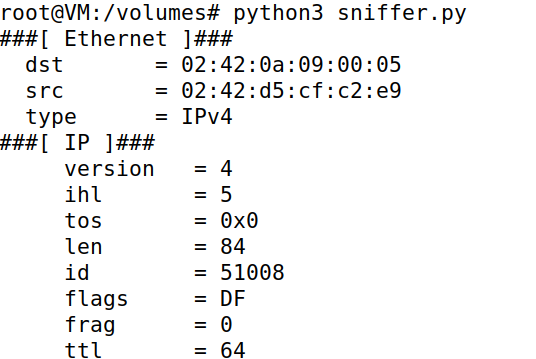


图1 root下运行结果

2）图2所示：用户seed下运行

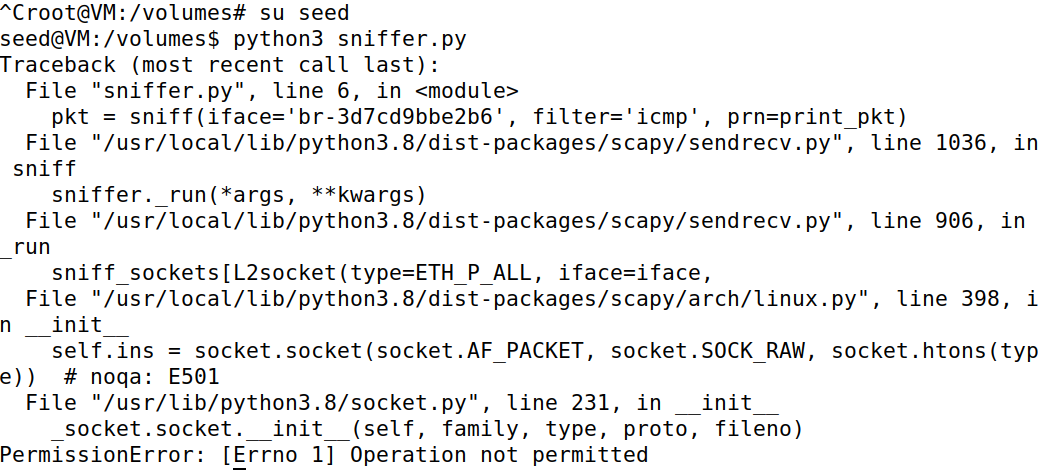


图2 seed下运行结果

Seed权限不够，需要在root权限下运行sniffer

**Task 1.1B.**

1）ICMP



图3 ICMP过滤代码

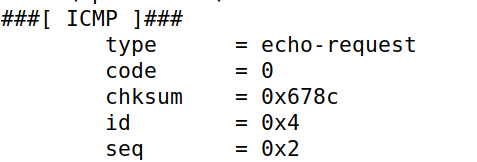


图4 ICMP捕获结果

2）TCP



图5 TCP过滤代码

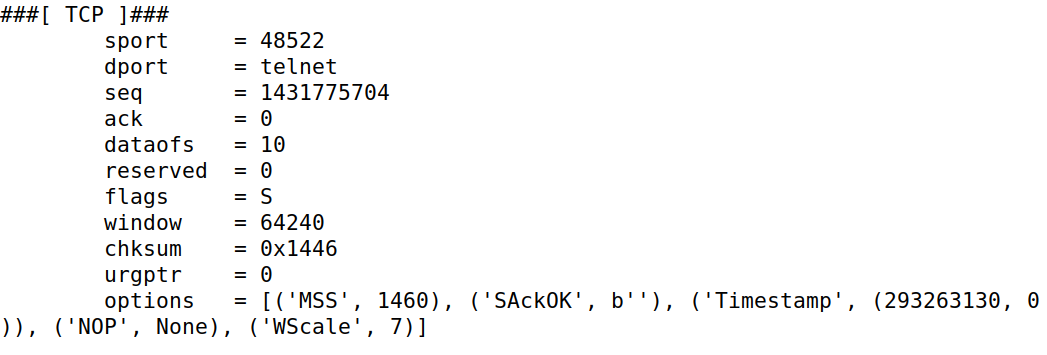


图6 TCP捕获结果

3）子网

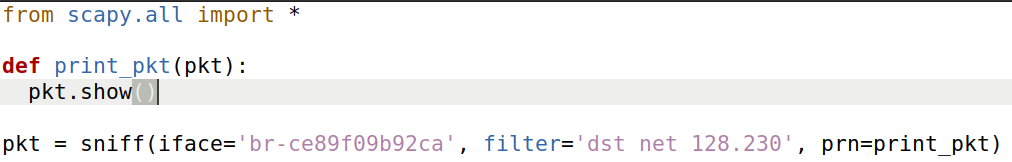


图7 特定子网过滤代码

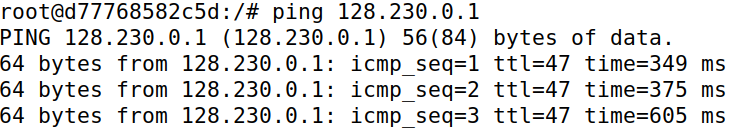


图8 向特定子网ping

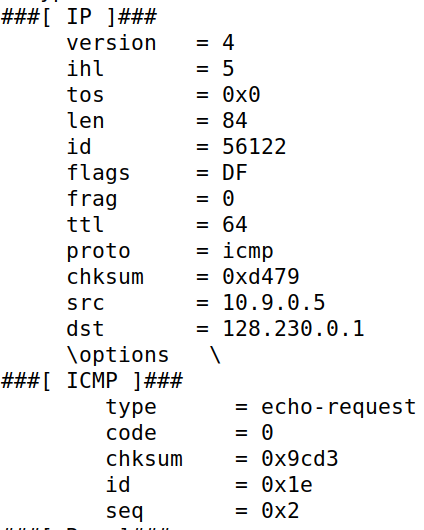


图9 特定子网捕获结果

**Task 1.2**

图10所示代码：

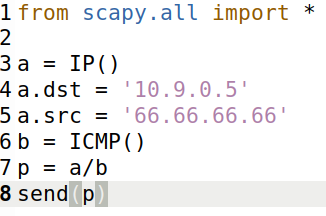


图10 创建包代码

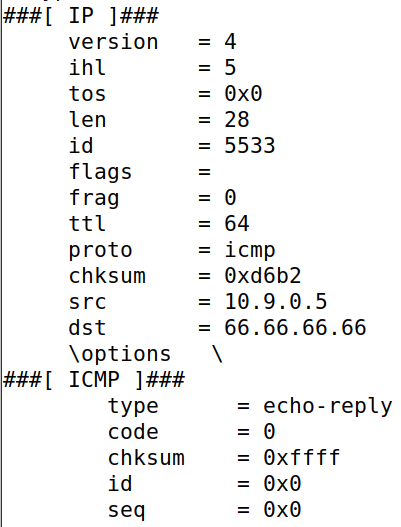


图11 捕获结果

如图11所示，成功捕获到10.9.0.5向不存在的66.66.66.66的回复

**Task 1.3**

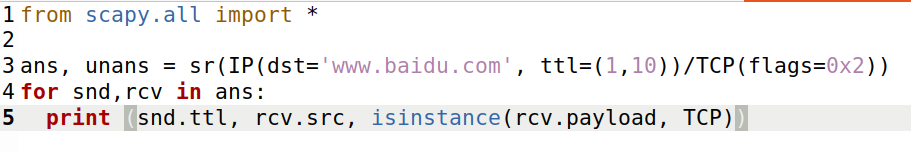


图12 代码

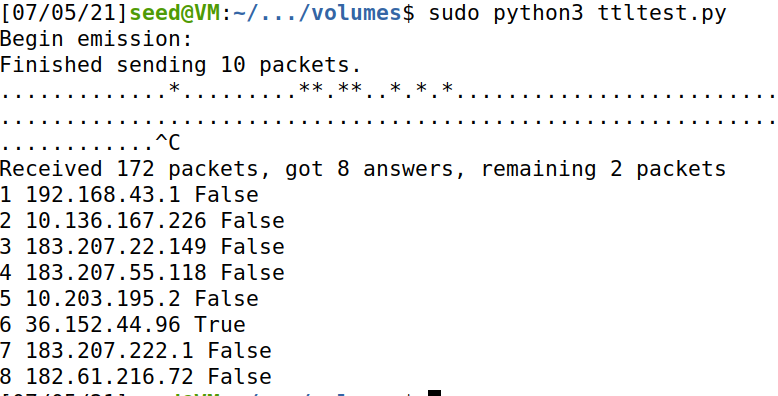


图13 结果

如图13所示，虚拟机到百度中间有6跳。

**Task 1.4**

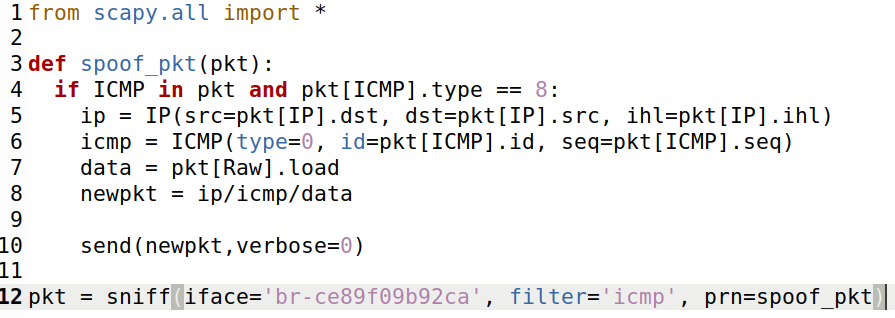


图14 代码

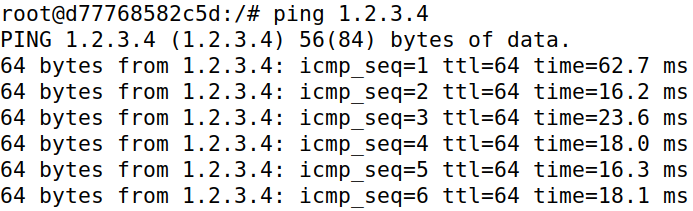


图15 ping向1.2.3.4的结果

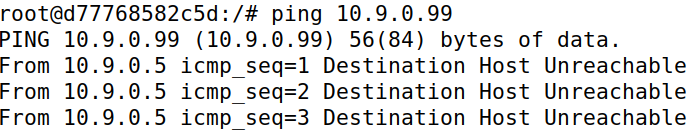


图16 ping向10.9.0.99的结果

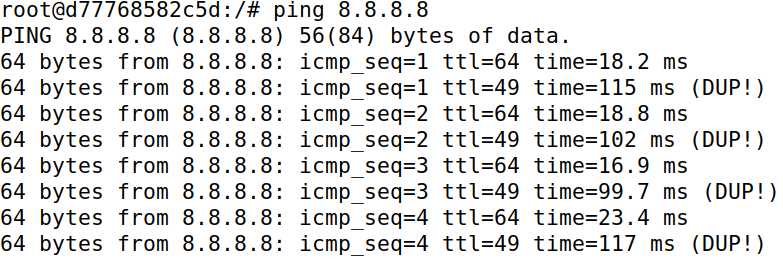


图17 ping向8.8.8.8的结果

如图15所示，主机收到伪造的返回包，以为1.2.3.4存在

如图16所示，主机没有收到伪造包，因为10.9.0.99在本地局域网，不会发向attacker主机。

如图17所示，主机不仅收到伪造包还收到真正的8.8.8.8返回的包，因此有显示DUP！