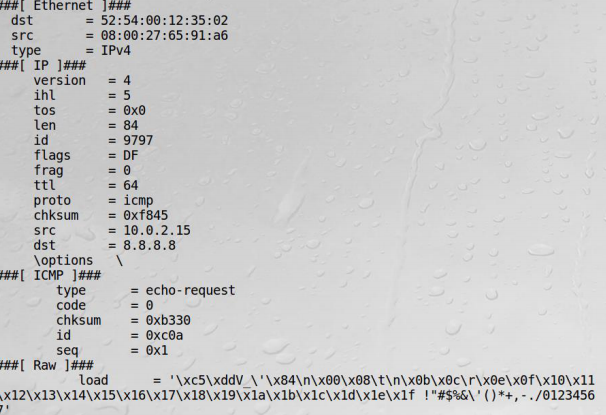
**实验三：**

**57117101 焦典**

**lab1:Packet Sniffifing and Spoofifing Lab**

**Task1.1A:**

**在root权限下运行程序：**

****

**在普通用户权限下运行程序：**

****

**程序报错。**

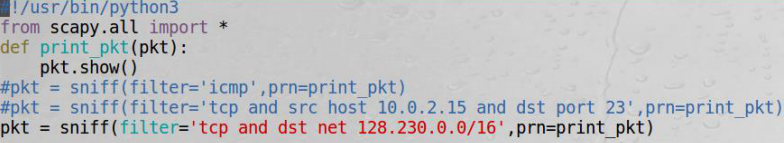
**程序报错原因在于普通用户没有权限创建socket。**

**Task1.1B:**

**仅捕获 ICMP 数据包，捕获的报文为：**

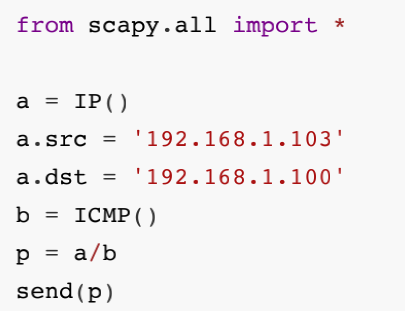
****

**捕获从特定IP发出的，捕获的报文为：**

****

**Task1.2：**

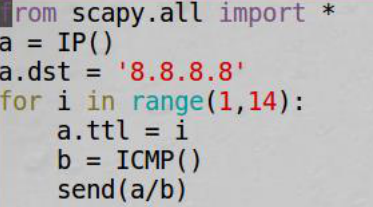
**创建报文：**

****

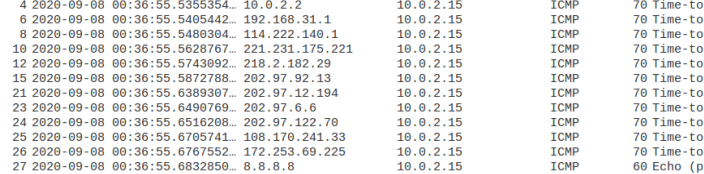
**用Wireshark检测，伪装成功。**

**Task1.3：**

**使⽤Scapy来估计虚拟机与⽬标地址之间的路由器跳数：**

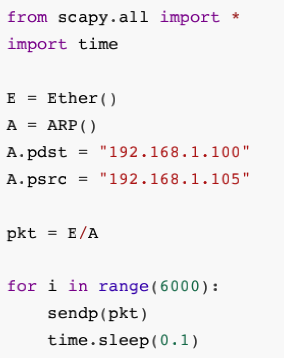
****

**使⽤Wireshark查看：**

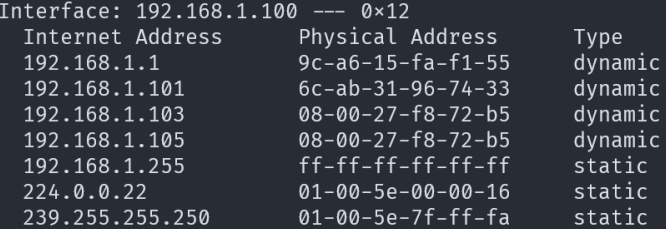
****

**lab2:ARP Cache Poisoning Attack Lab**

**Task1:**



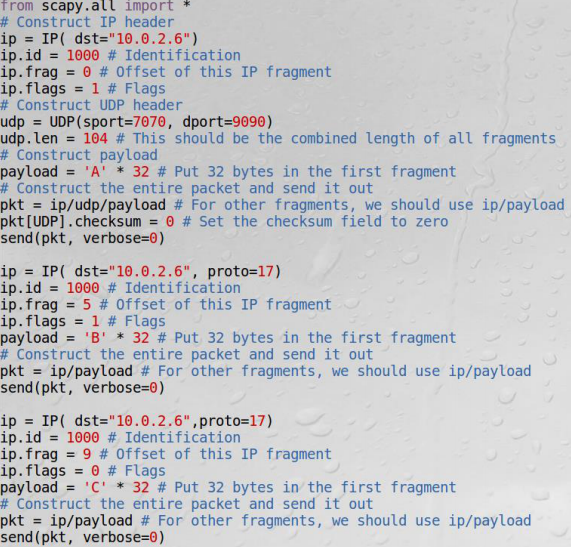
**不停地向宿主机的IP地址发送ARP请求报⽂，并将源地址设为想要污染的IP地址 192.168.1.105。**

****

**192.168.1.105 成功被污染。**

**lab3:IP/ICMP Attacks Lab**

**Task1:**



**使用Wireshark查看；**

