实验三报告

实验人：57117104 孙舒雯

实验时间：9.09-9.14

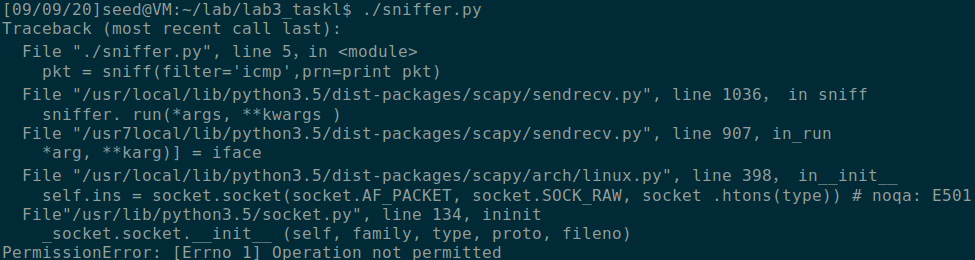
Packet Sniffing and Spoofing Lab

**Using Tools to Sniff and Spoof Packets**

1. Task 1: Sniffing Packets

实验过程：

1.1使⽤root权限运⾏，收到的报文如图

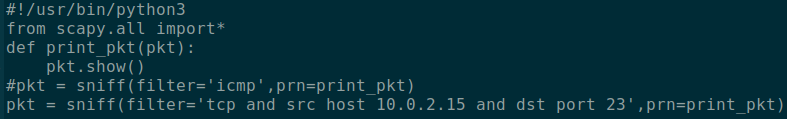


因为没有权限调用socket函数，普通用户权限报错了。

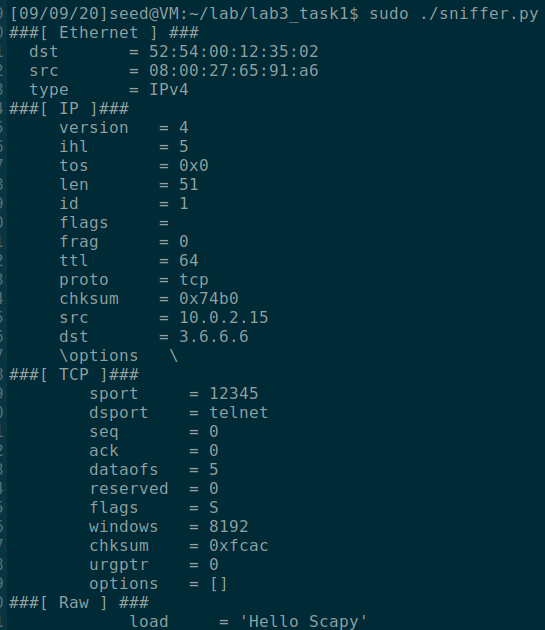
之前已经捕获 ICMP 数据包，伪造以虚拟机为起点，3.6.6.6:17 为终点的报文



收获如下报文



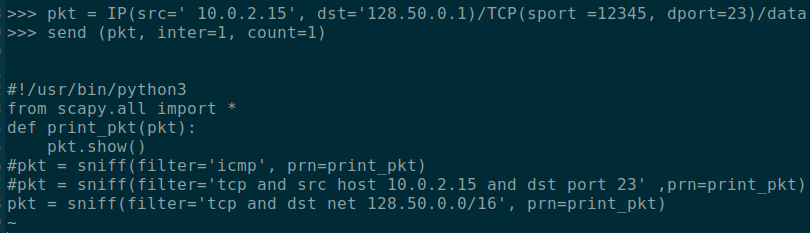
嗅探到的结果有



伪造以虚拟机为起点，128.50.0.1 为终点的报文

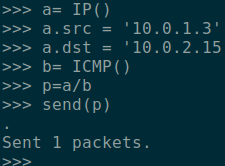


捕获到报文



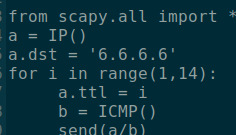
1．2

伪造一个src为10.0.1.3的报文



Wireshark 检测成功

1.3



试探得到本虚拟机到 8.8.8.8 共有 13 跳.

ARP Cache Poisoning Attack Lab

Task1

1.1

我们的目的是通过 seed 虚拟机污染虚拟机 A 中关于宿主机的 ARP 项。

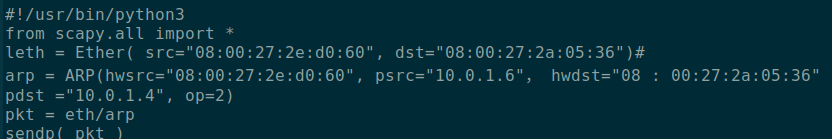
正常情况下虚拟机 A 的 ARP 列表：

对应：C 10.0.1.5 08:00:24:2f:de:60

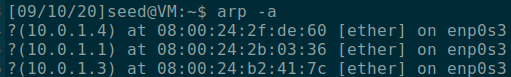
A 10.0.1.4 08:00:24:2b:03:36

B 10.0.1.6 08:00:24:b2:41:7c

C向A发送报文。

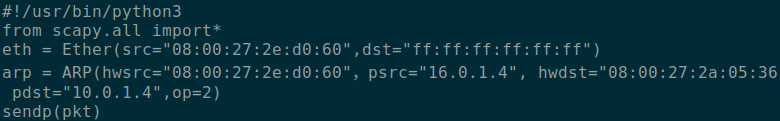


ARP表有

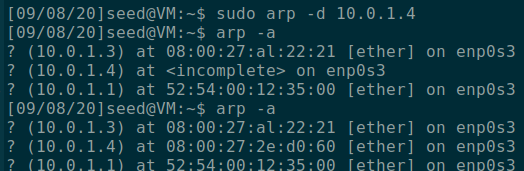


1.2

C向 A 发送报文



清空ARP表然后进行第二次污染。

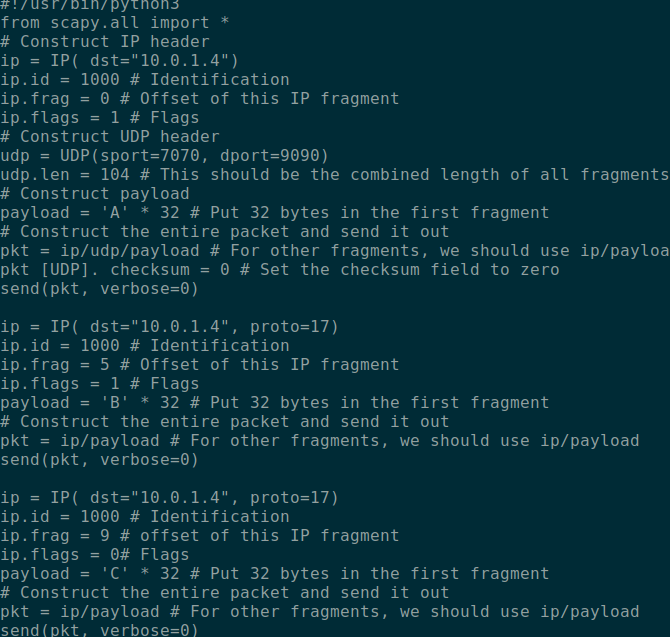


IP/ICMP Attacks Lab

Task1.

1.1

填充代码

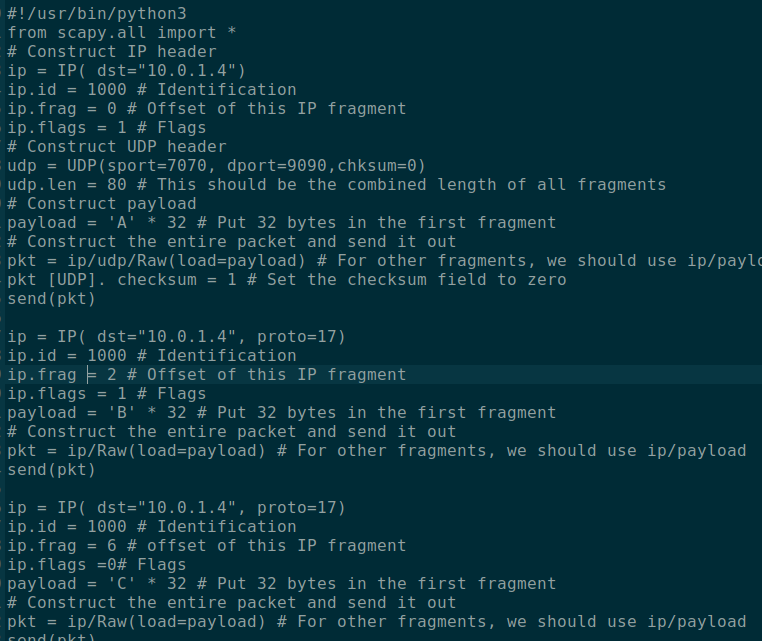


Wireshark 接收到数据



1.2

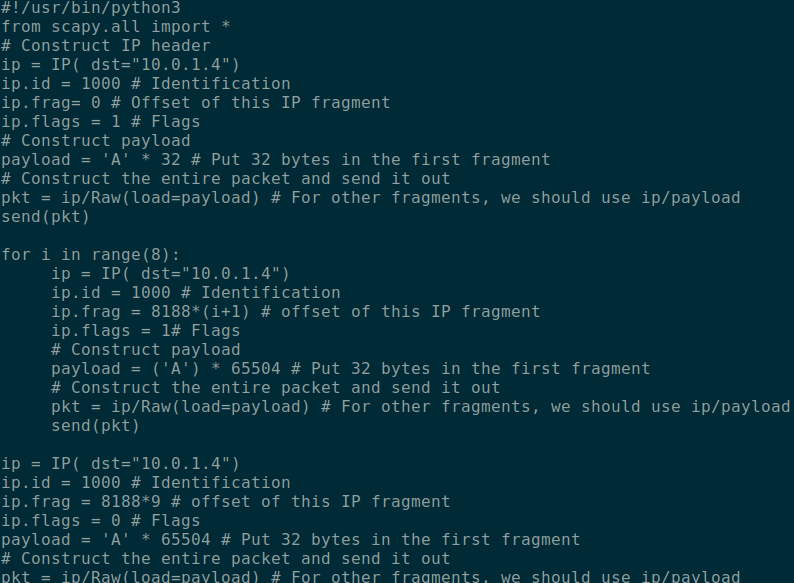
改变偏移值



终端显示相关字符



1.3 发送代码





产生非法碎片。