网安综合课程设计

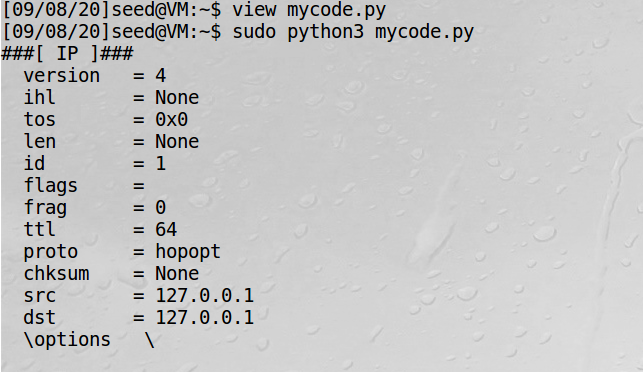
实验报告

（57117105 杨哲君）

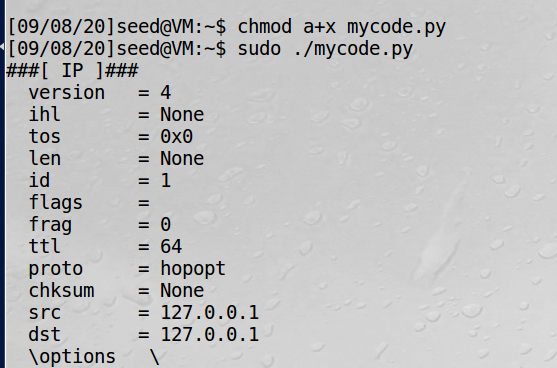
***Lab1.Packet Sniffing and Spoofing Lab***

**Lab Task Set 1: Using Tools to Sniff and Spoof Packets**

先按指导手册命令下载scapy，试着执行一个Python文件。



另一种执行Python文件的方法：

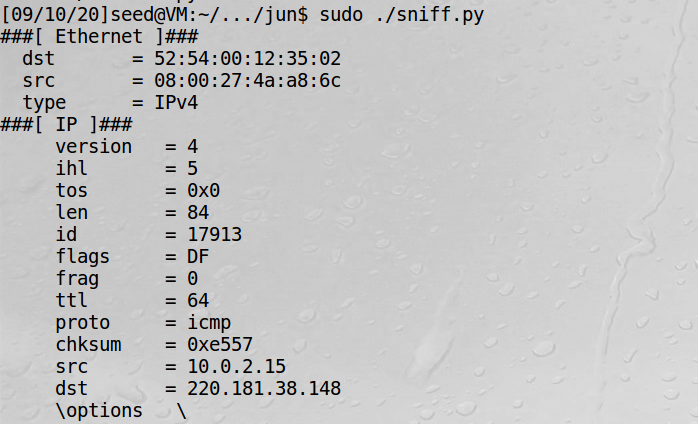


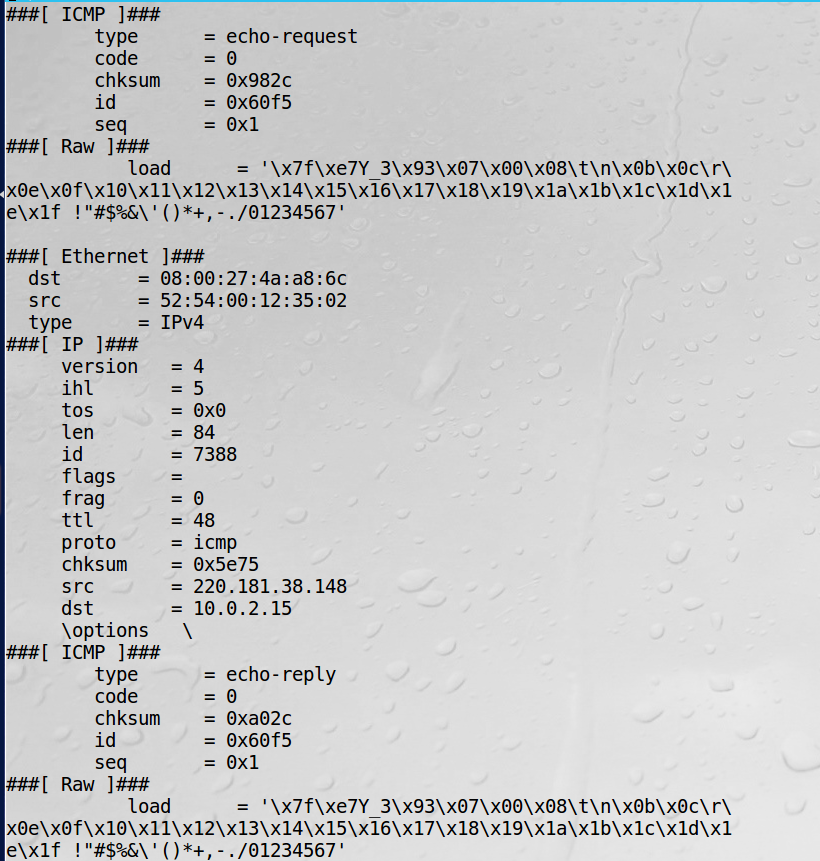
**2.1 Task 1.1: Sniffing Packets**

**Task1.1A.**

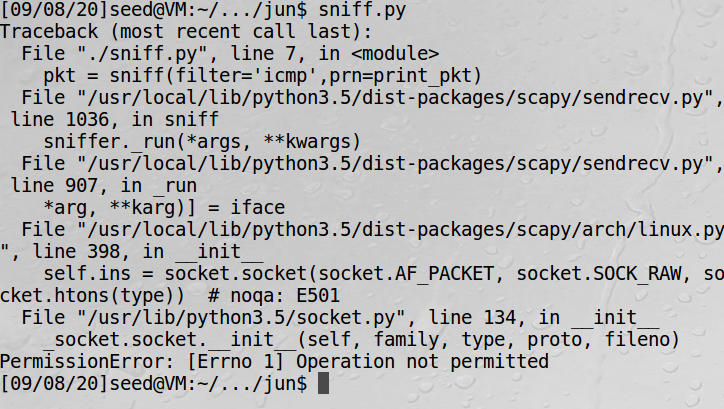
用root权限运行程序的结果：

在另一个终端ping使用ping命令，可以发现监听到数据报。



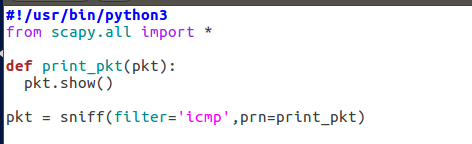


不用root权限的运行结果：出现错误Operation not permitted，权限不足，无法监听。



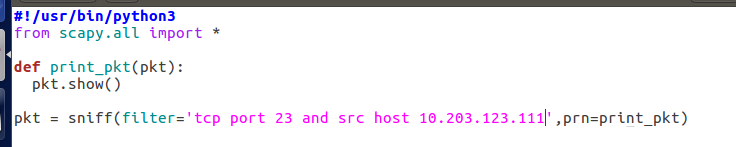
**Task 1.1B.**

1. 仅监听ICMP报文

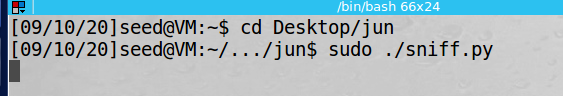


上述实验已经做过。

1. 捕获特定IP发出，目的端口为23的TCP包

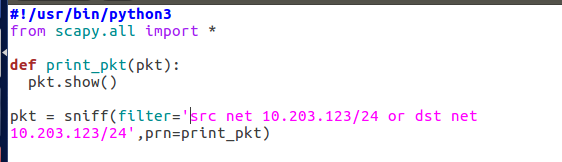


修改sniff后，执行，然后在另一个终端做ping操作。

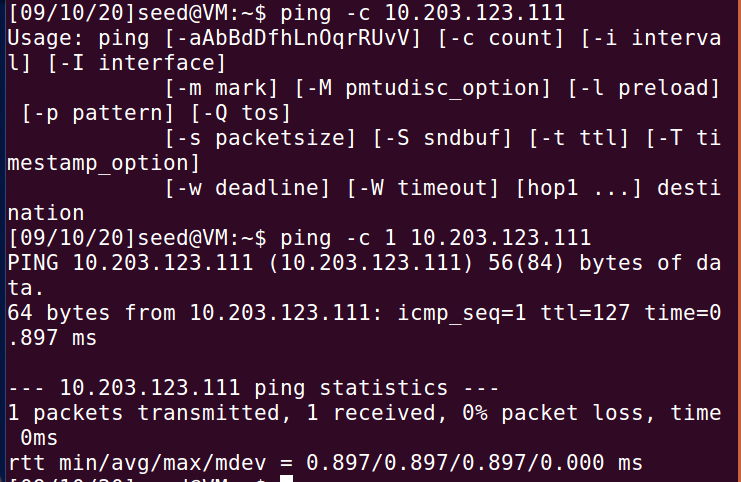


并没有监听到数据报。

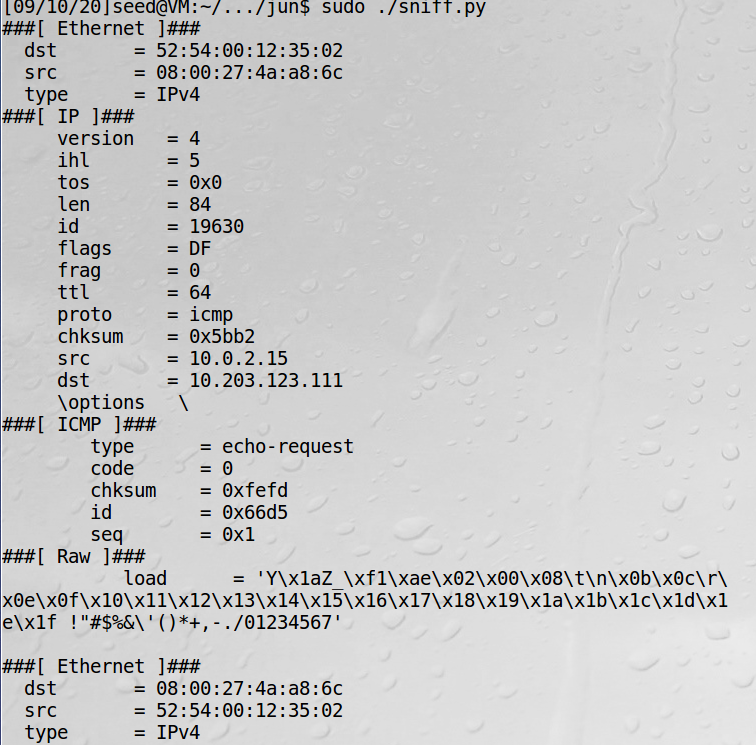
1. 监听源 ip 或目的 ip 为特定子网的数据包。

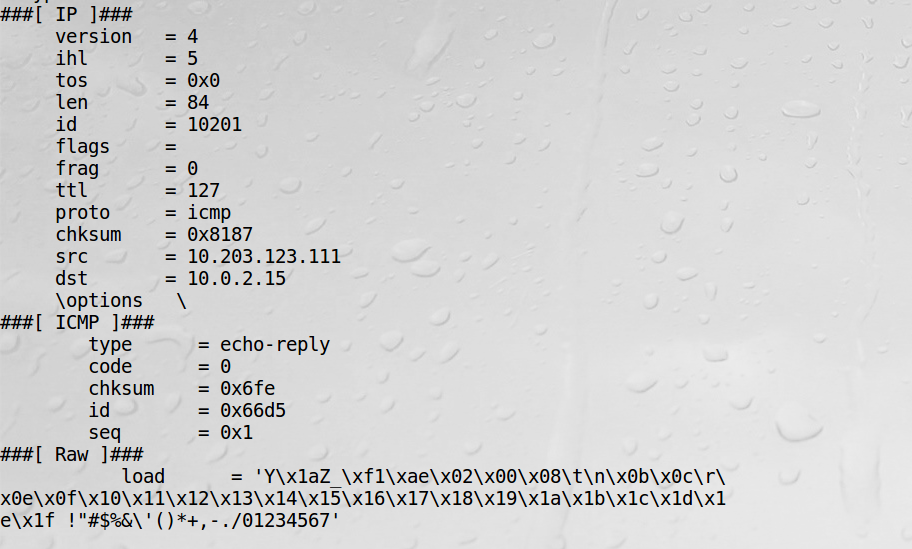


发出ping请求。

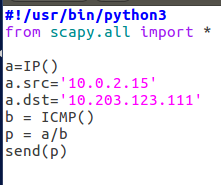


发现成功监听到数据报。





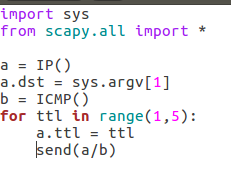
**Task 1.2: Spoofing ICMP Packets**

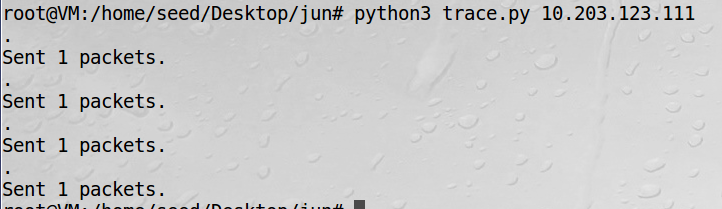




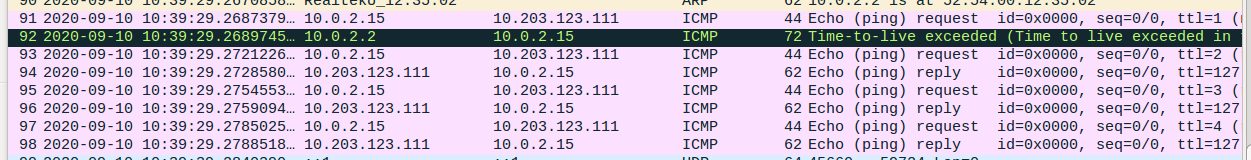
**Task 1.3: Traceroute**

编写代码：





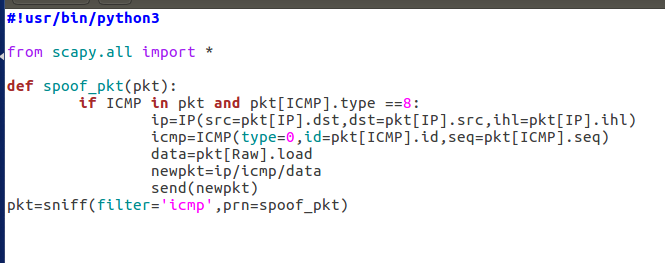
Wireshark抓到包。



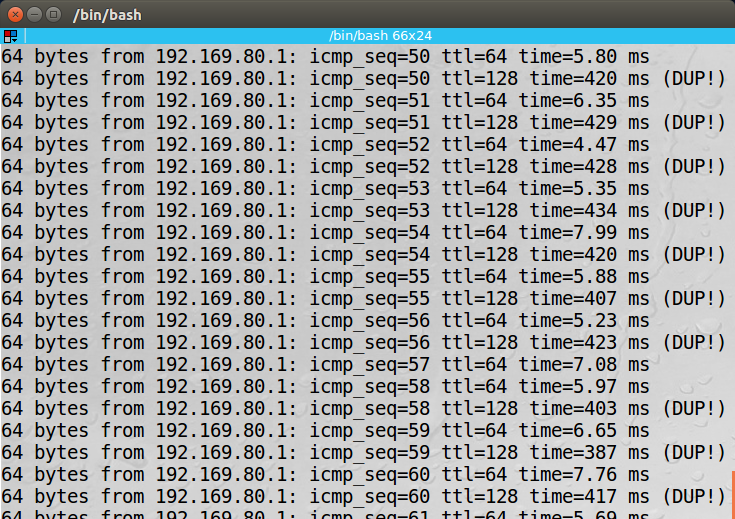
**Task 1.4: Sniffing and-then Spoofing**

（以下实验换到VMware Workstation做了，所以虚拟机的IP有变化）

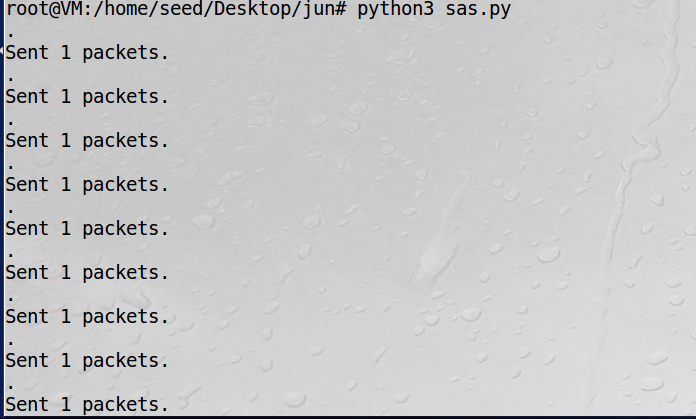
编写代码



虚拟机1中ping 192.168.80.137，发现无法ping通，再在虚拟机2中运行上述脚本，再进行ping操作，此时可以ping通。



看到虚拟机2中：

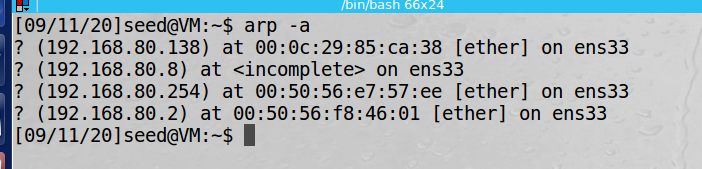


***ARP Cache Poisoning***

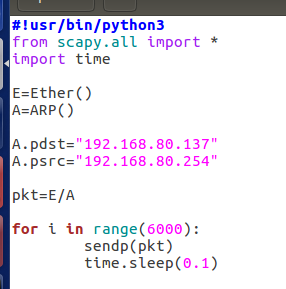
**Task1 ARP request**

**Task 1A (using ARP request)**

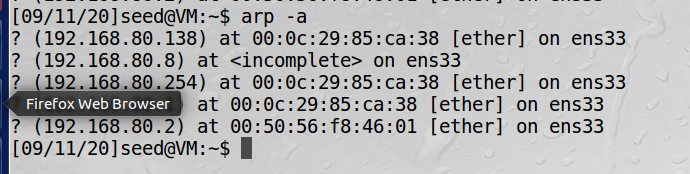
先查看虚拟机1的arp表



在虚拟机2上编写运行代码，发送伪装的数据包。

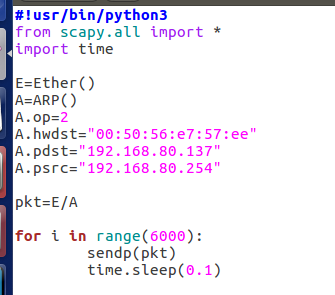


再次查看虚拟机1的arp表，攻击成功。



**Task 1B (using ARP reply)**

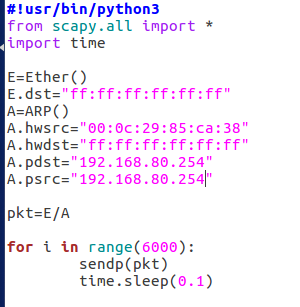
和task1A类似，我们再设置MAC地址为00：50：56：e7：57：ee，执行代码。



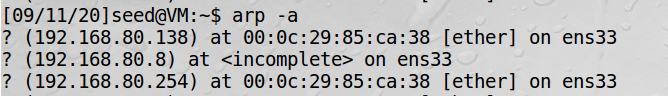
结果与task1A一致。

**Task1C （ARP gratuitous message）**

修改代码的目的地址，改为广播。



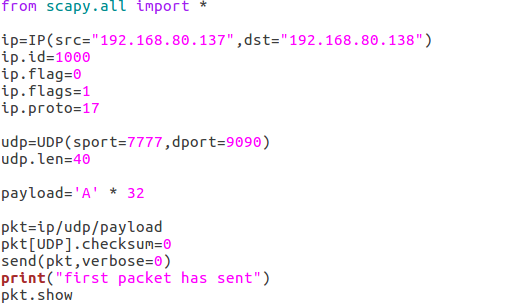
查看虚拟机1的arp表，发现攻击成功。

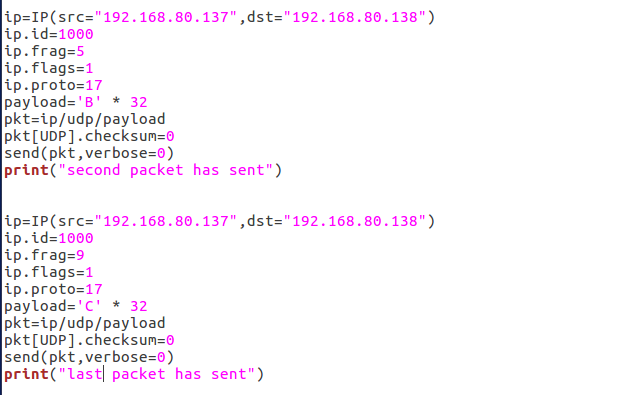


***IP/ICMP Attacks Lab***

**Tasks 1: IP Fragmentation**

**Task 1.a: Conducting IP Fragmentation**





以上脚本将三个数据包连续发送至虚拟机2，使用“c -lu9090“命令”在虚拟机2开启udp监听，用wireshark可观察到准确收到了三个数据包。



**Task 1.b: IP Fragments with Overlapping Contents**

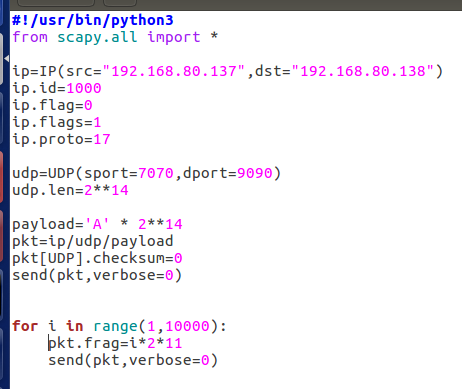
按第一片报文、第二片报文、第三片报文的顺序发送数据包，再次运行脚本，用wireshark观察。虚拟机2中收到的第片报文的前8字节被覆盖了。

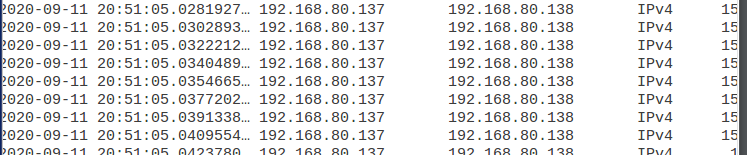
按第二片报文、第一片报文、第三片报文的顺序发送数据包，再次运行脚本，用wireshark观察。虚拟机2中的结果和123的顺序一致。

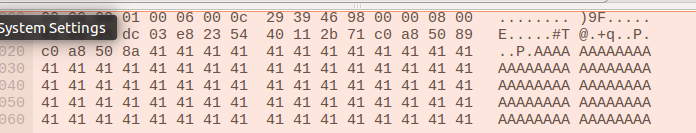
说明当重叠出现时，后面的片会覆盖前面，而报文发送的顺序不影响结果。

**Task 1.c: Sending a Super-Large Packet**

改写脚本，不断向UDP服务器发送为长度2^14的数据包。







服务器并没有什么反应。

**Task 1.d: Sending Incomplete IP Packet**

修改脚本，只发送第一片和第三片报文，缺失了第二片报文以后，服务器会将收到的全部储存，直到内存完全占满，形成拒绝服务攻击。