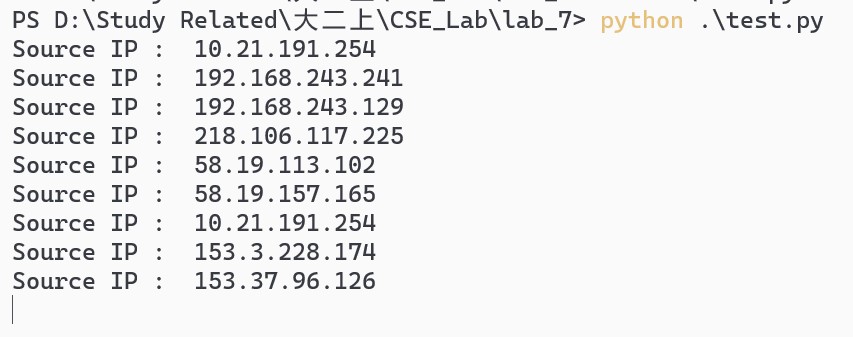
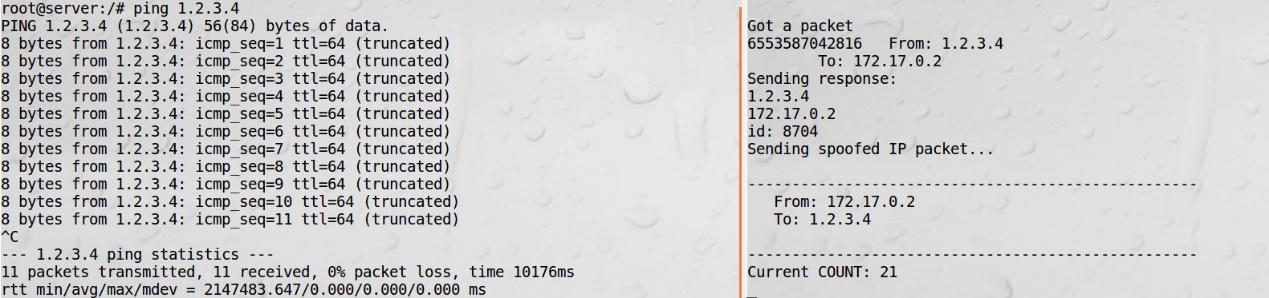
**一 探测真实ip**

使用sniff spoof，设定目的ip，首先向该ip发送一个ttl为0的icmp数据包，开启监听，反应函数中读取源ip打印到屏幕，令ttl加一，继续发送并监听，不再接受到包时说明获取了链路上的各真实ip。（代码附于后）

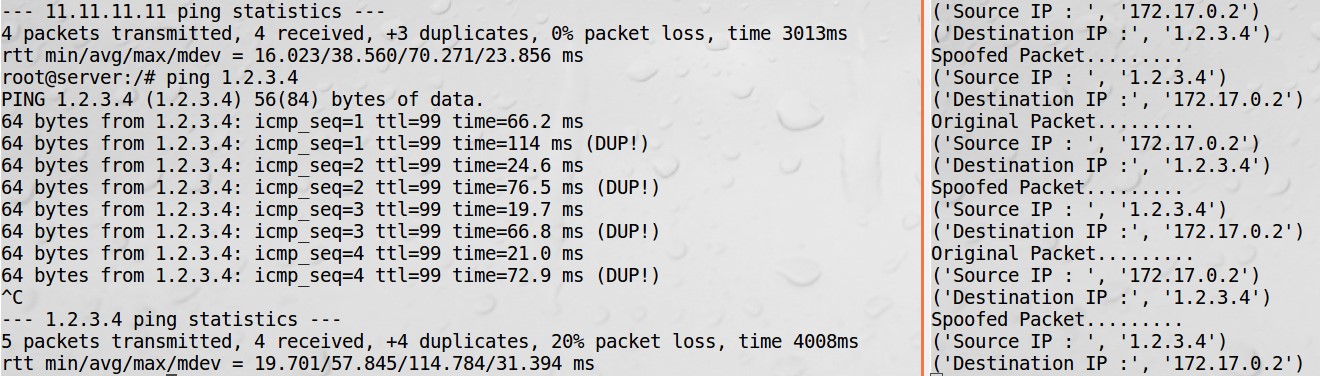
icmp

**二 伪造icmp**

基本思路是使用c语言构建一个和正常ping指令发送的相同的icmp数据包，特别注意需要修改ip和seq，使得被攻击者的ping命令能正常接受和识别。（其他同学的思路是把嗅探到的包修改源ip和目的ip后再发回去，感觉比我的方便很多…）



上图为c语言编写的运行结果，下图为py编写的运行结果。



下图为构造icmp包的部分c代码。



下图为获取真实ip的py代码。

