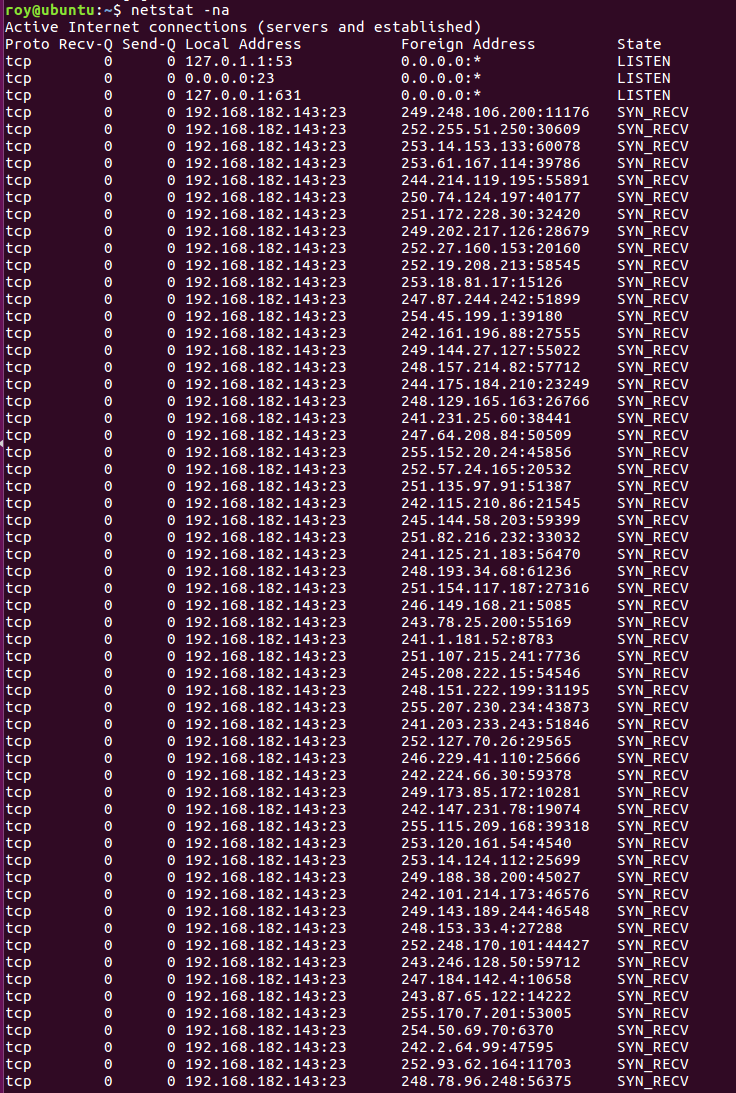
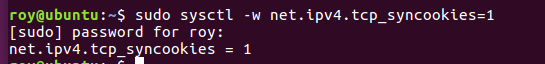
Task1

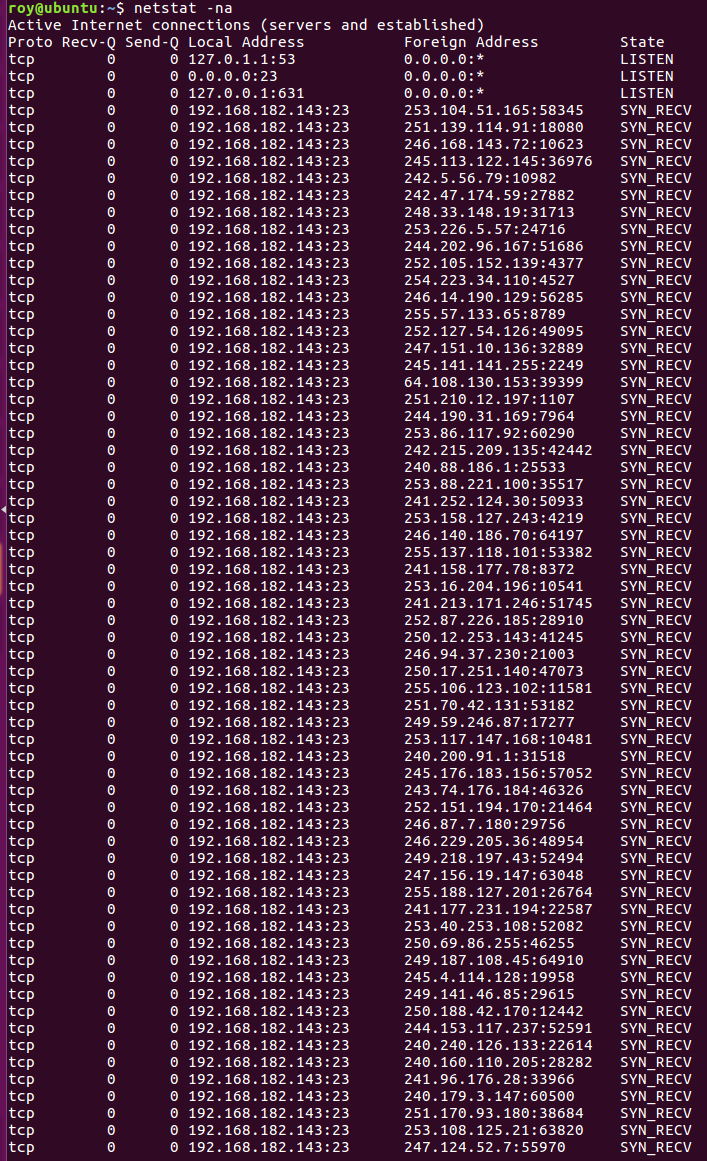




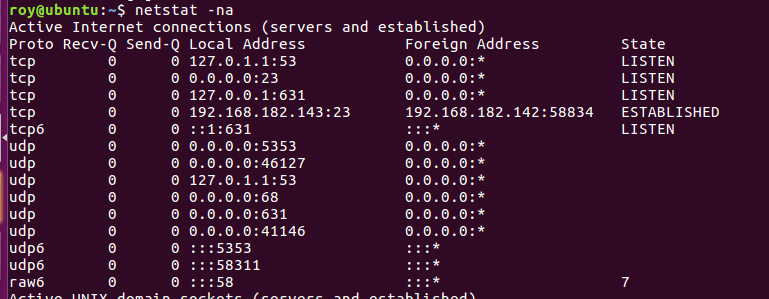
通过打开受害者的telnet端口，不断发送syn报文，从受害者主机可以看出有很多连接处于syn\_recv状态。

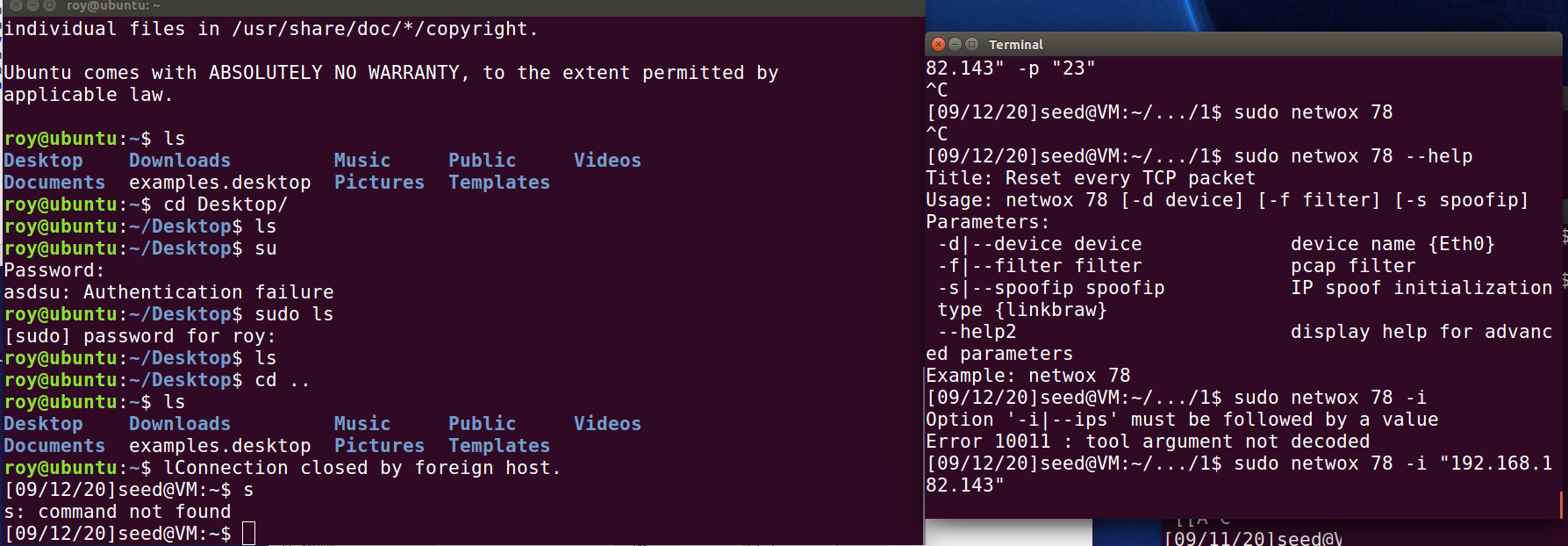


打开syncookies后，发现对syn flooding攻击没有影响，不是很理解。

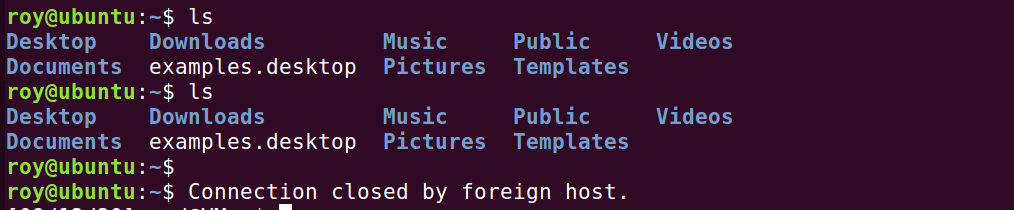


Task2



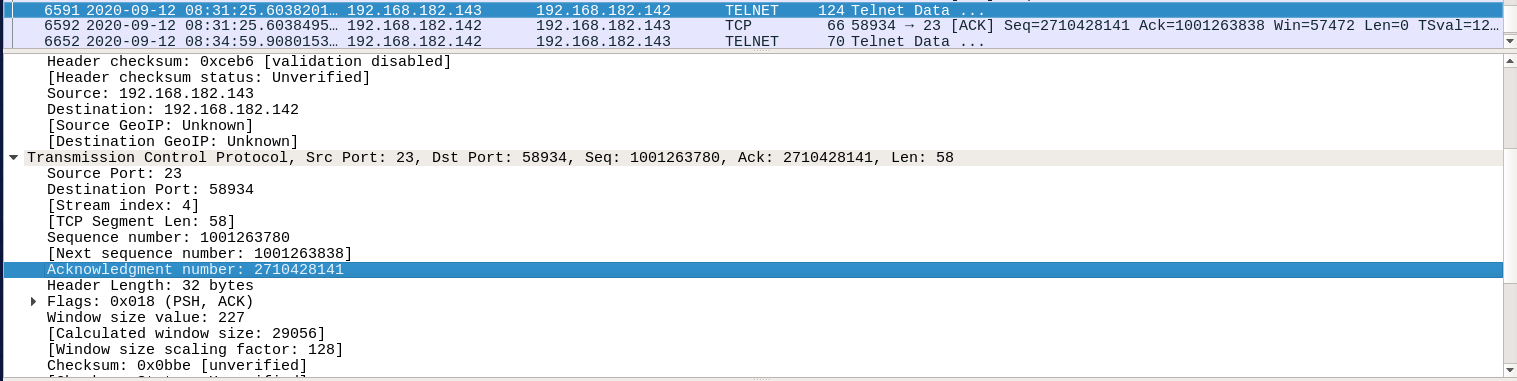


启动攻击后左方命令行出现连接关闭，攻击成功

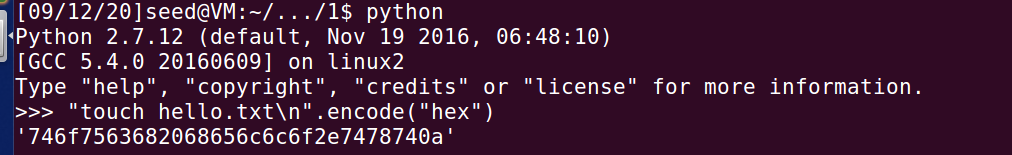


Scapy攻击同理。

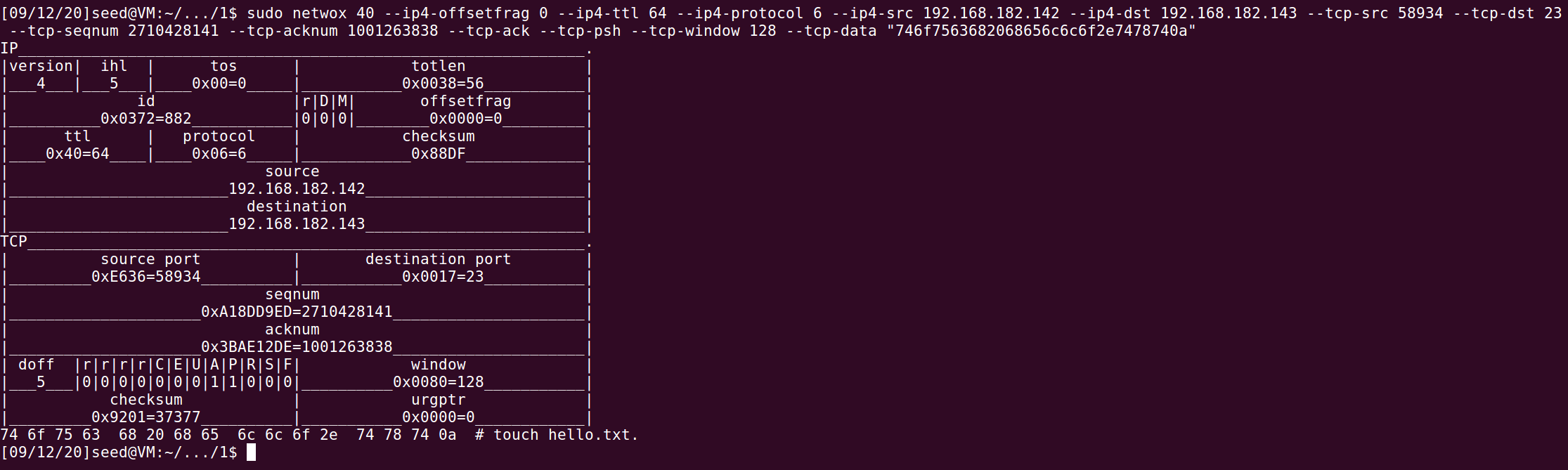
Task4



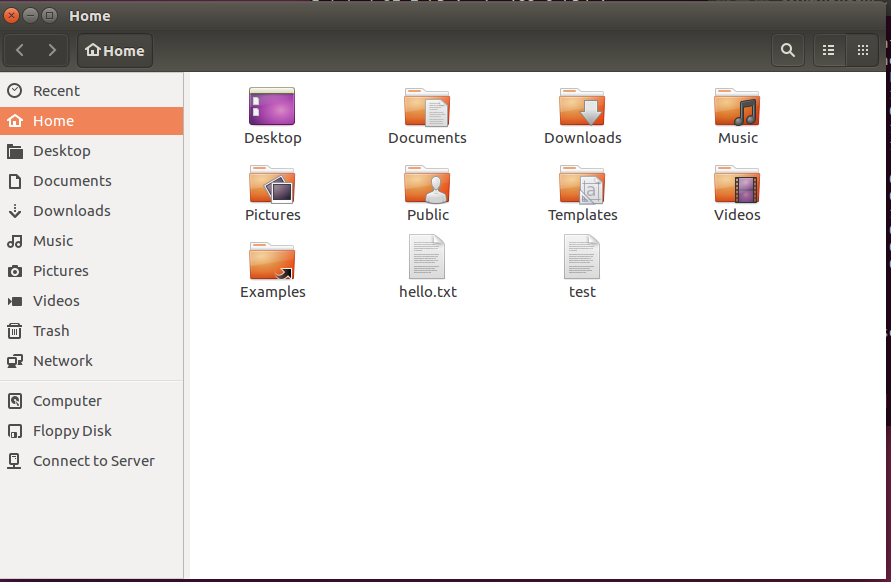
通过抓包获取上一个报文的ack和next seq



将要使用的命令行转换为十六进制。



实行攻击后可以发现成功创建了hello.txt文件



然后会发现原来的命令行无法输入了，发现已被劫持

Scapy代码如下，原理同上，next seq作为该报文的ack，上一个报文的ack作为seq

