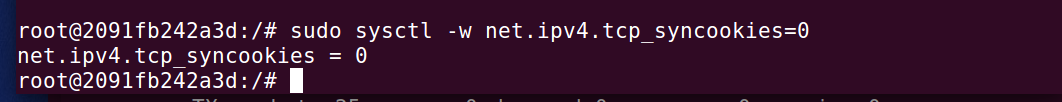
Tcp syn-flooding

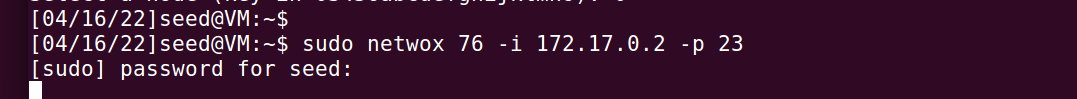
比较syn-cookies启用和不启用的情况下，攻击的效果（攻击前后，用telnet或者nc连接目标主机端口进行测试

1. Netwox

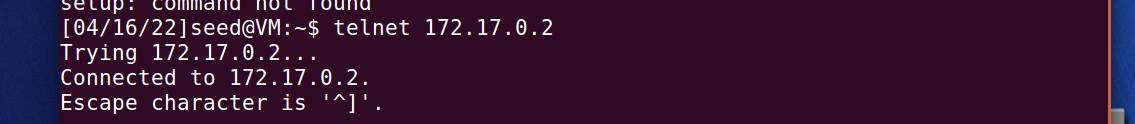
关闭syn-cookies



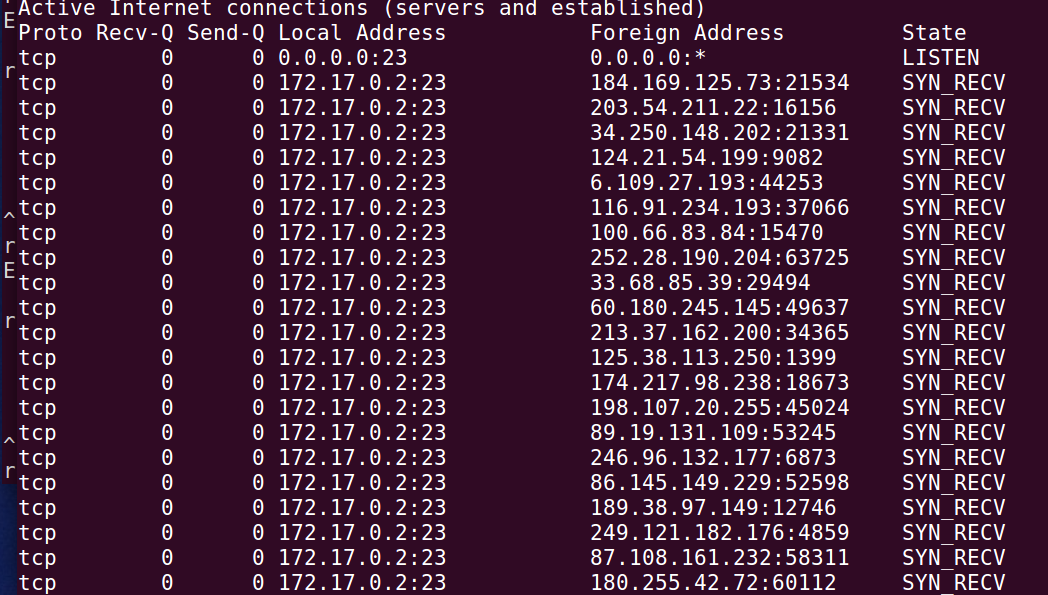
攻击机指令



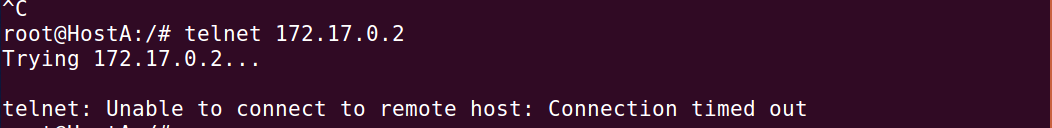
攻击前Telnet连接



攻击时server半打开连接状态

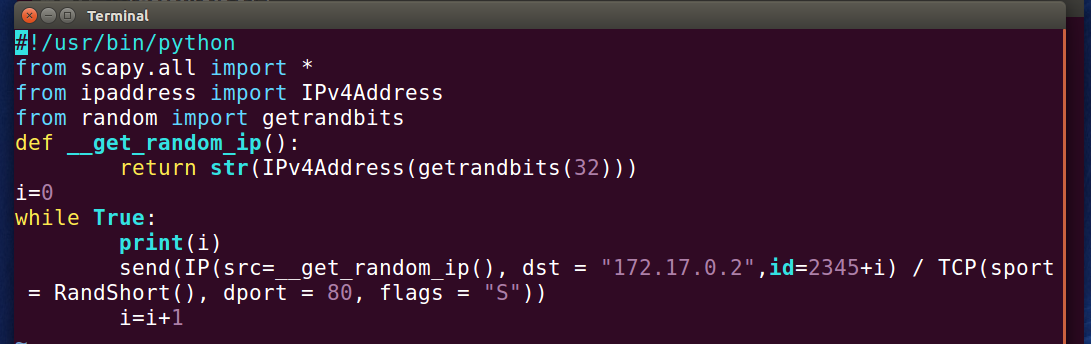


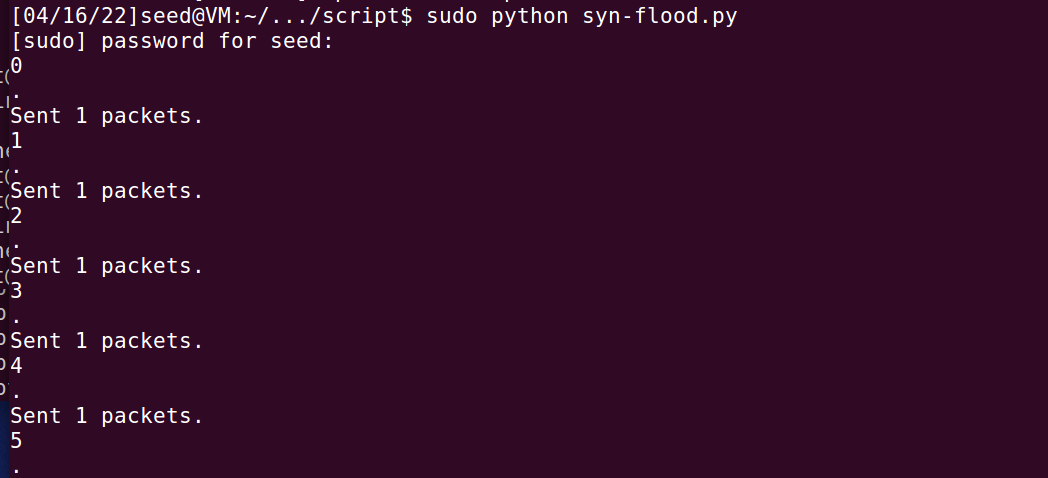
攻击时telnet连接



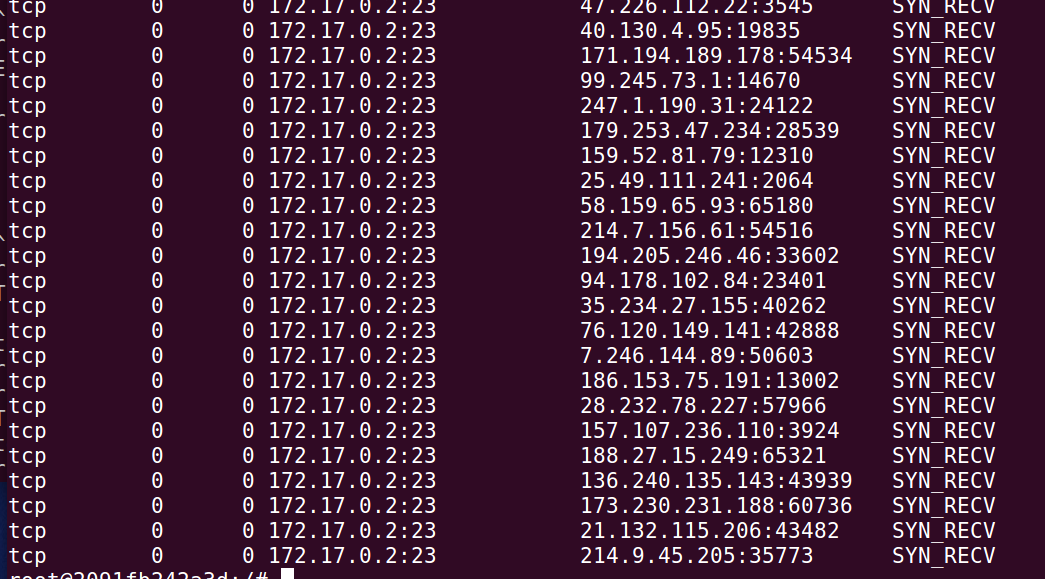
1. Scapy

攻击代码





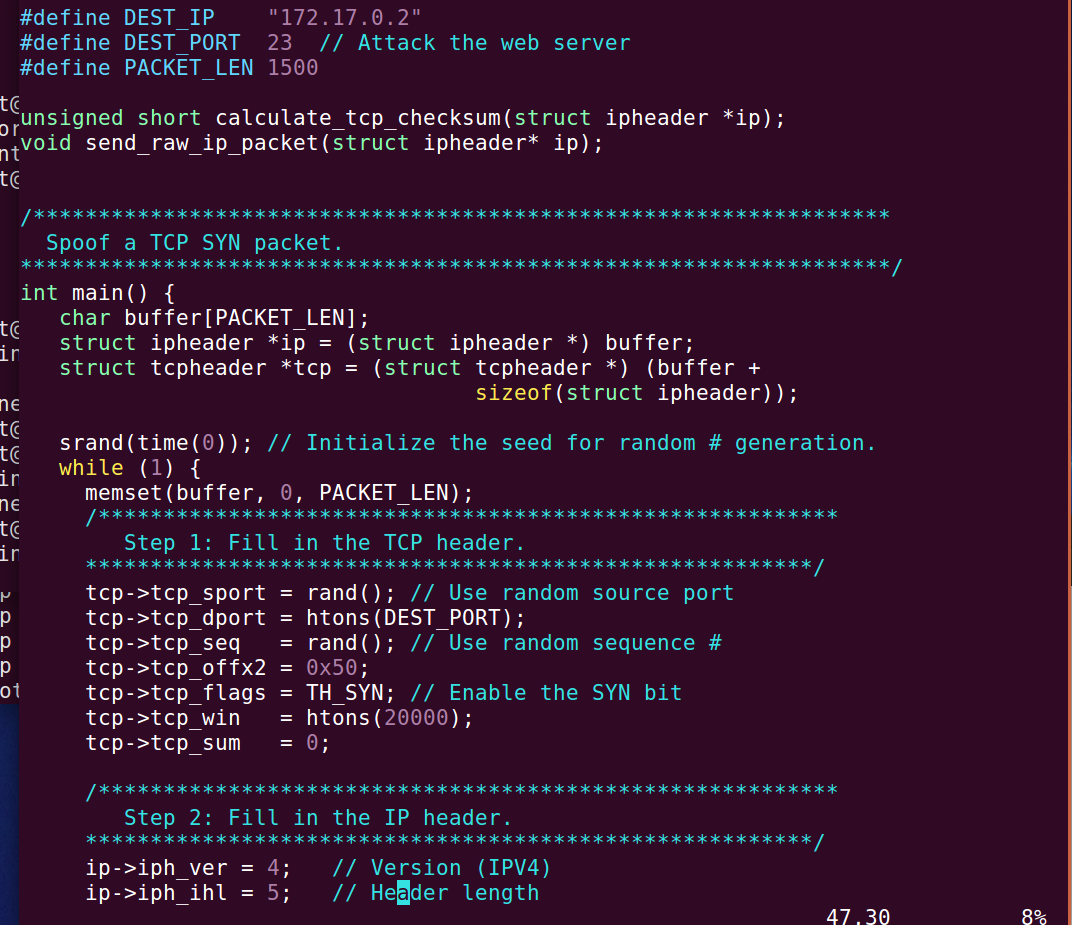
攻击时server半打开连接状态

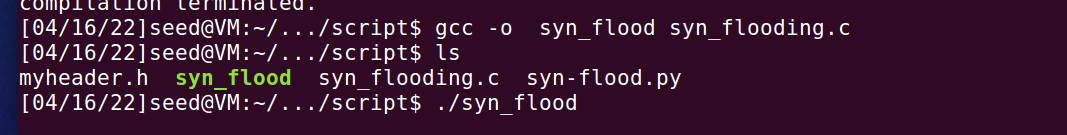


攻击时仍能连接server，攻击失败

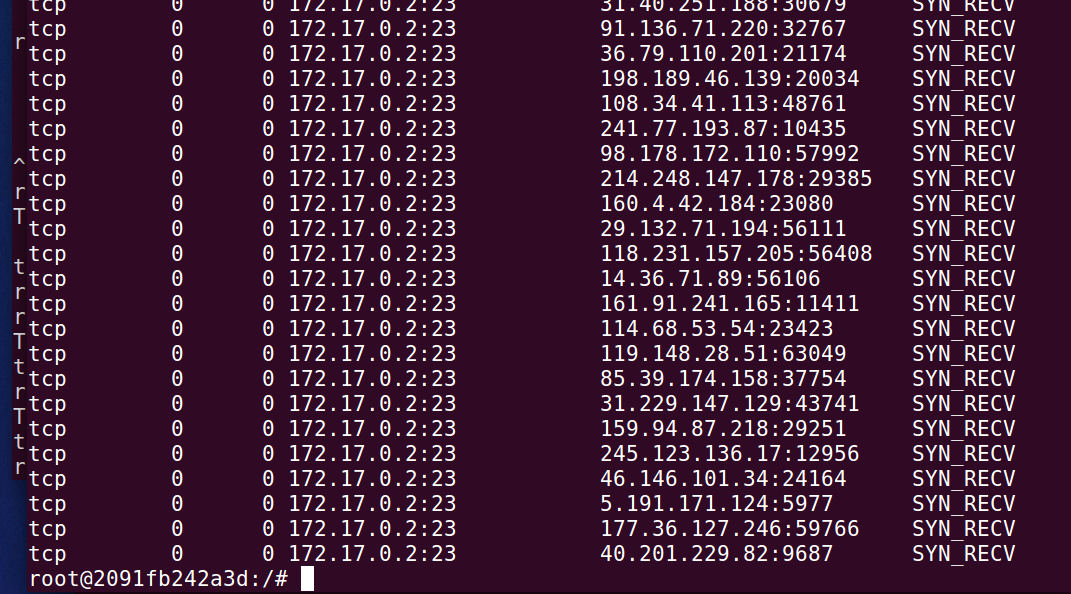
1. C

攻击代码

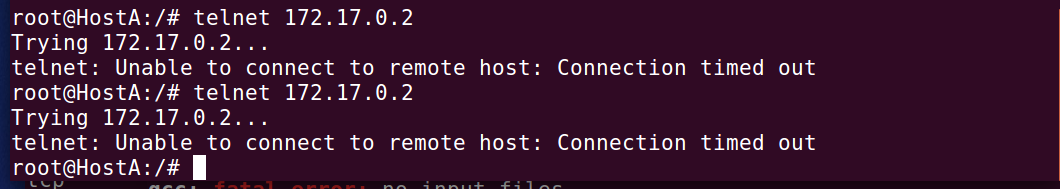




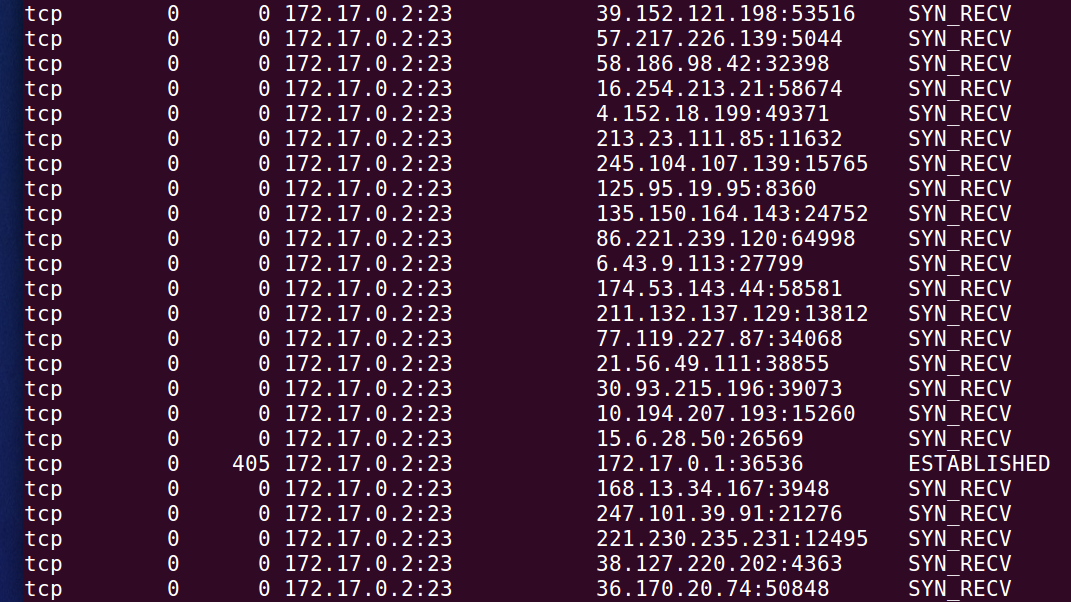
攻击时server半打开连接状态



攻击时telnet连接

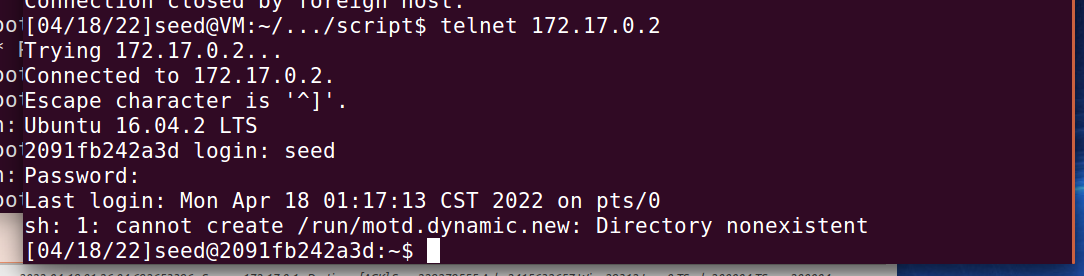


在syn-cookies开启的状态下，三种syn-flood攻击均失败，仍可建立连接，如图所示



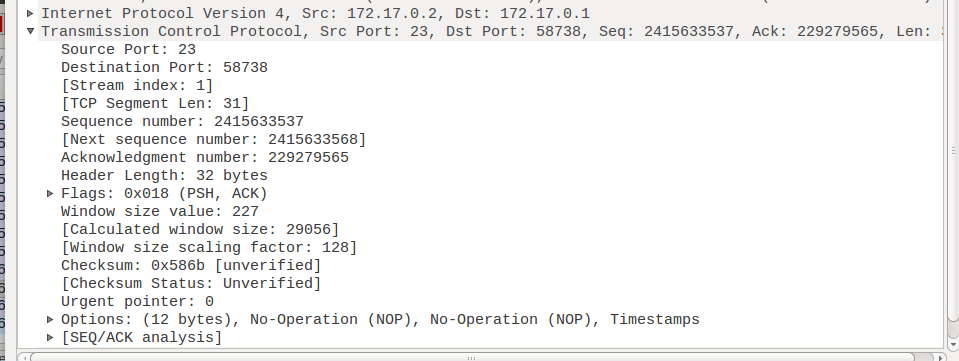
TCP Reset

首先使用telnet将攻击机与server建立一个tcp连接

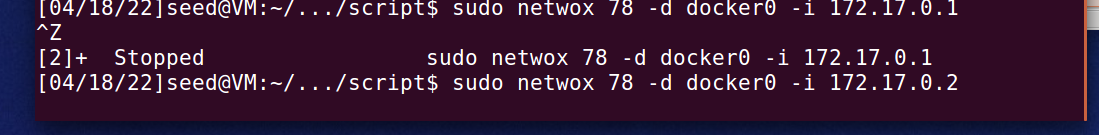


1. Netwox

Wireshark截包

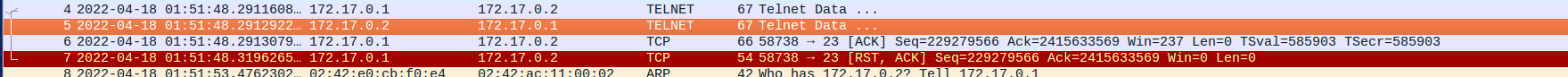


攻击指令

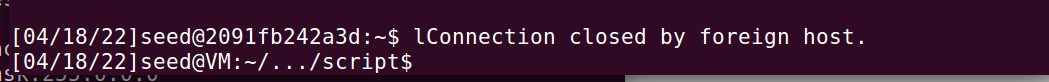


攻击结果

Wireshark截包



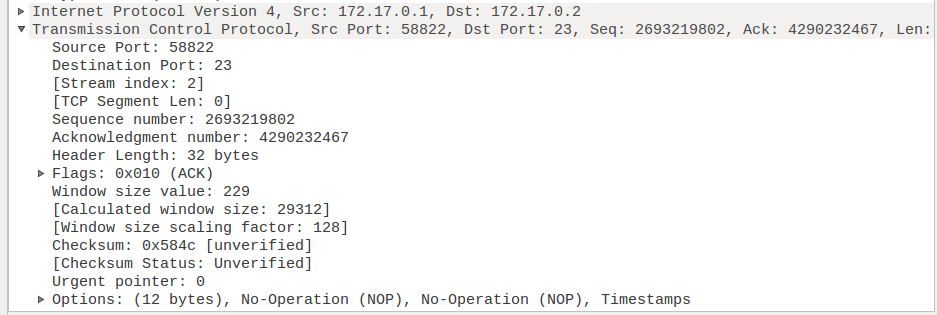
telnet客户端提示



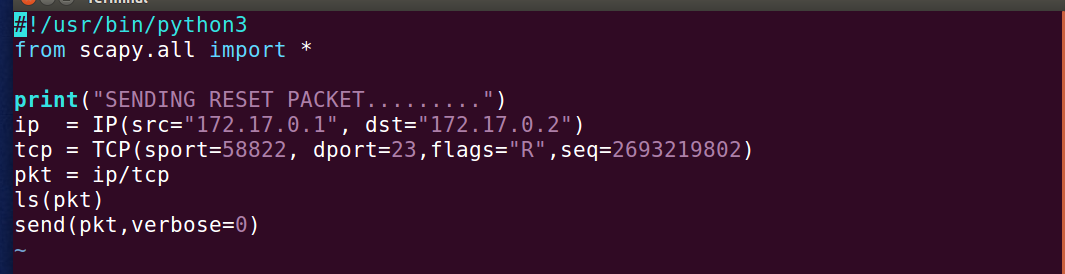
可知攻击成功，wireshark截取到RST包，且telnet客户端提示‘connection closed by foreign host’，结果符合预期

1. Scapy手动攻击

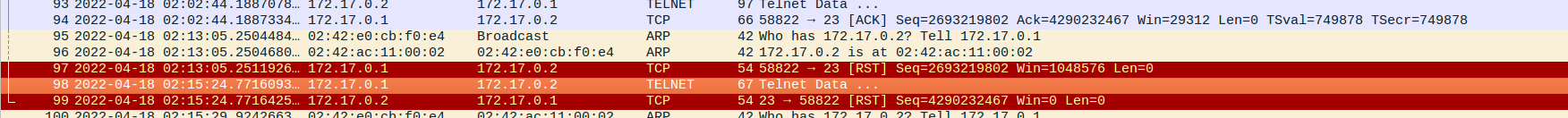
Wireshark截包

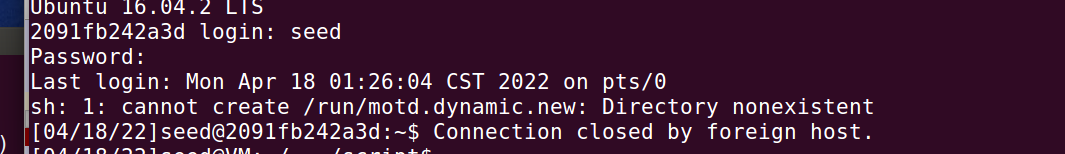


脚本代码



攻击结果

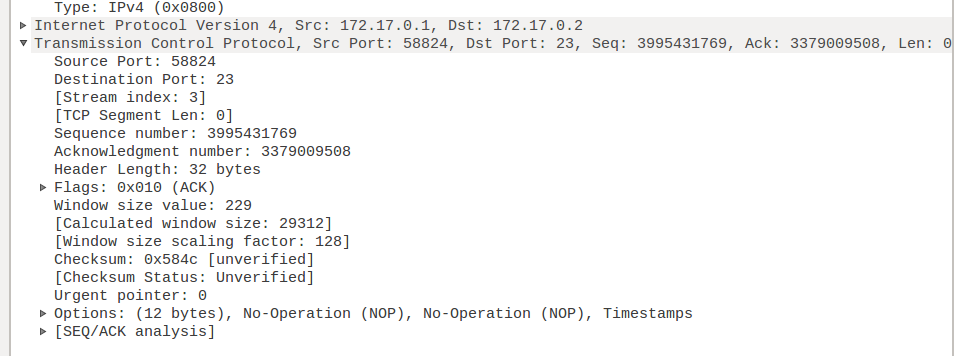




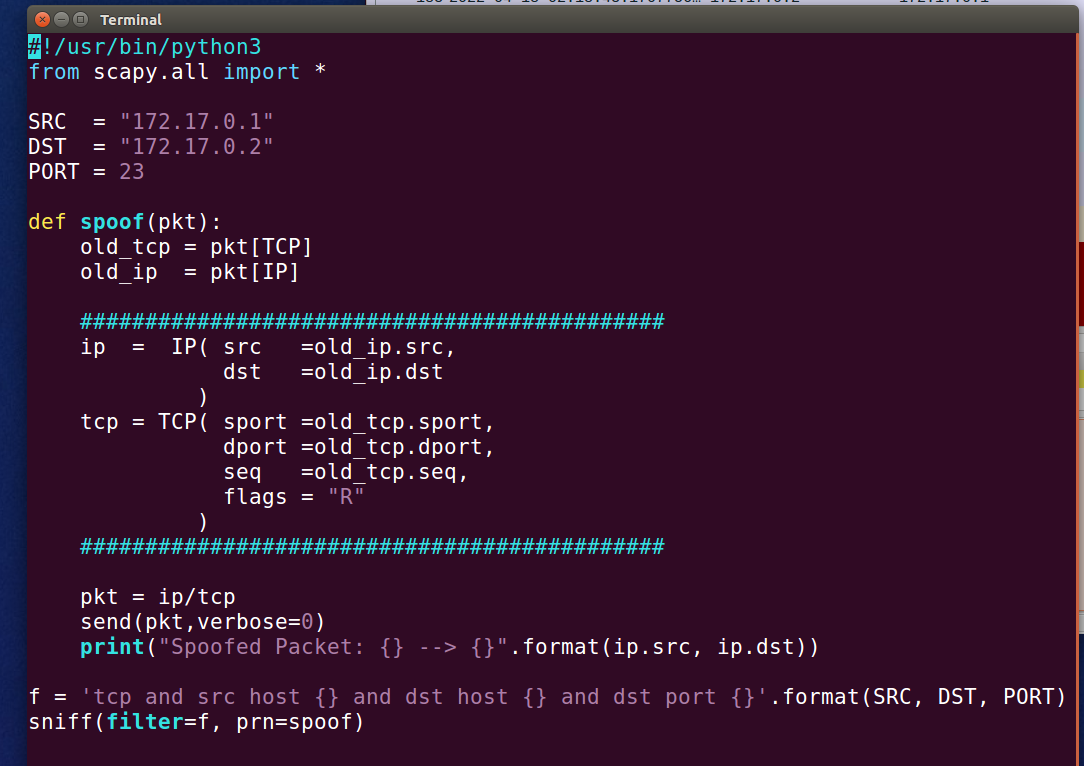
可知攻击成功，wireshark截取到RST包，且telnet客户端提示‘connection closed by foreign host’，结果符合预期

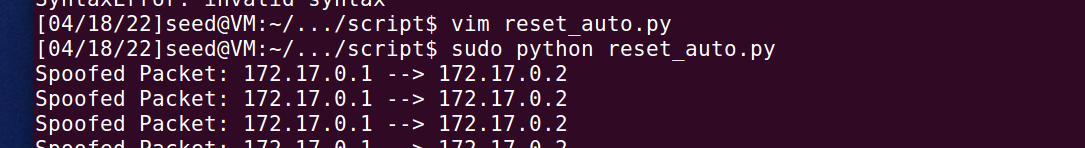
1. Scapy自动攻击

Wireshark截包

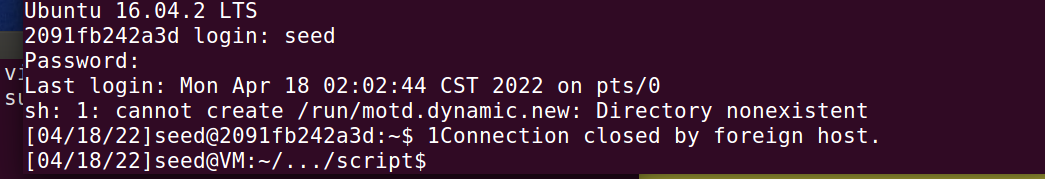


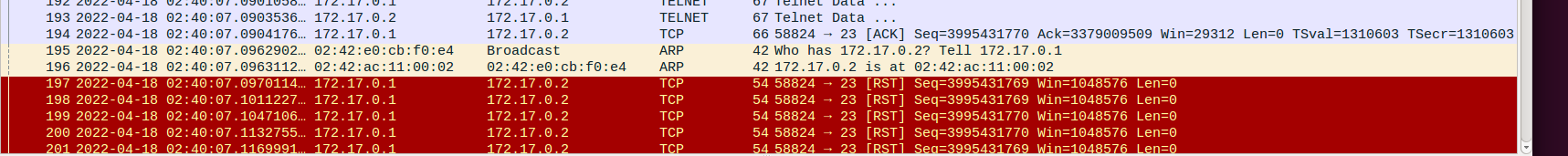
脚本代码





攻击结果

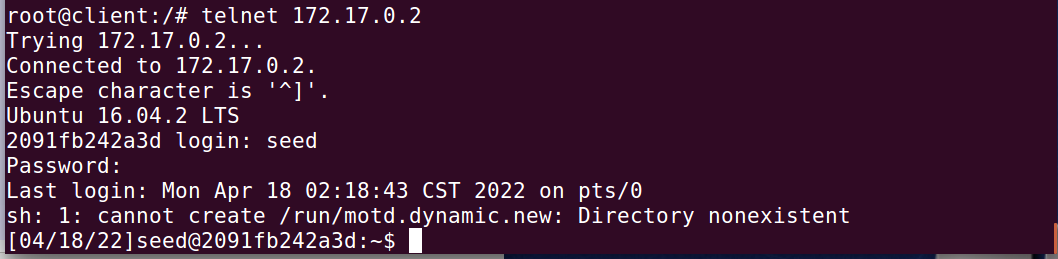




可知攻击成功，wireshark截取到RST包，且telnet客户端提示‘connection closed by foreign host’，结果符合预期

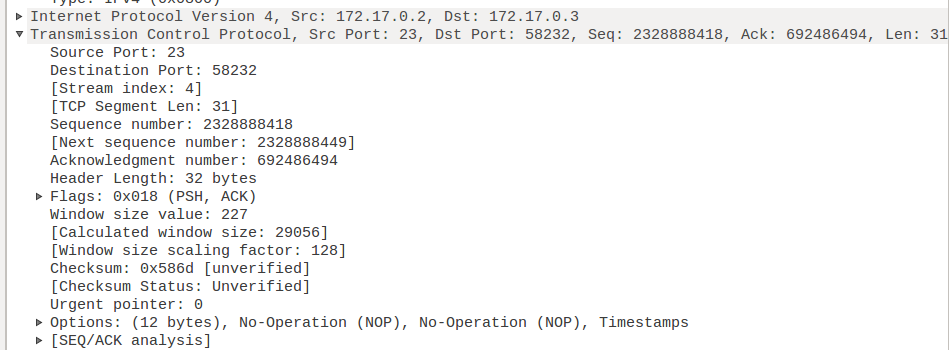
TCP 会话劫持攻击

客户端先建立与server的telnet连接

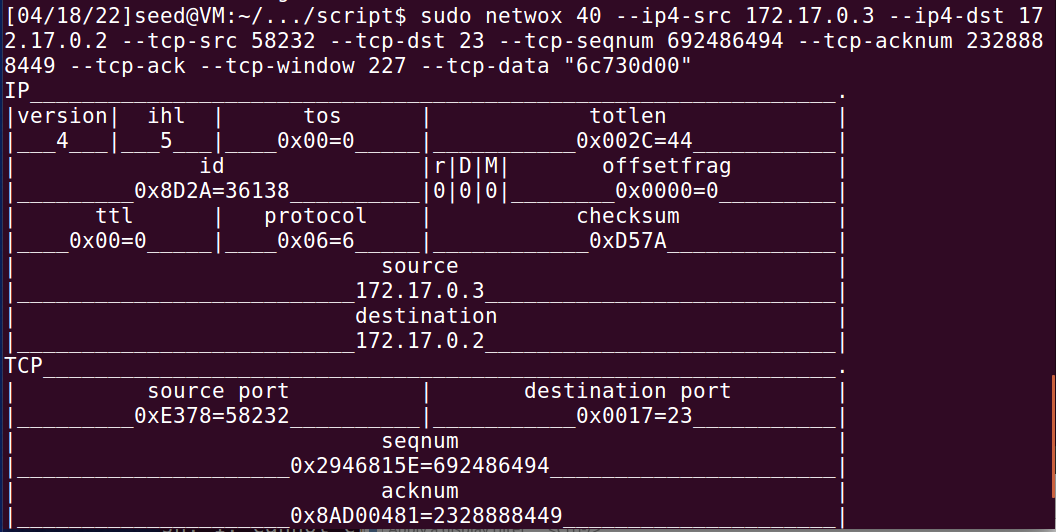


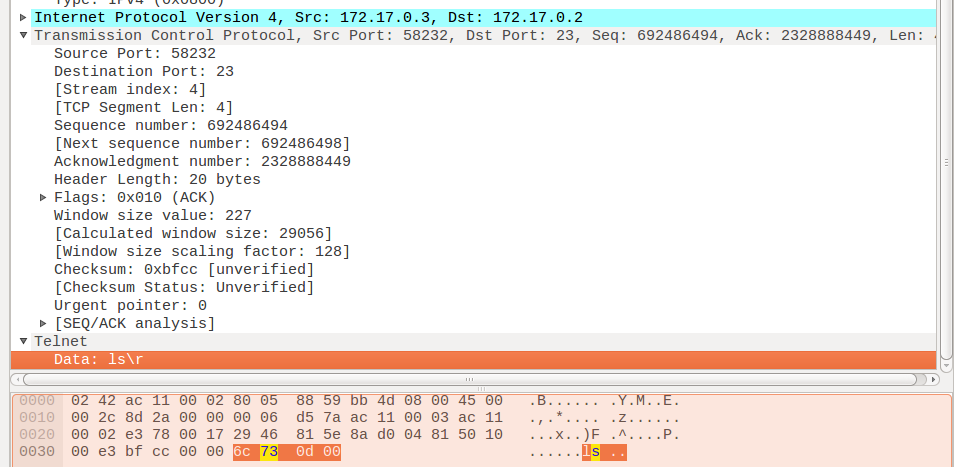
1. Netwox

Wireshark截包

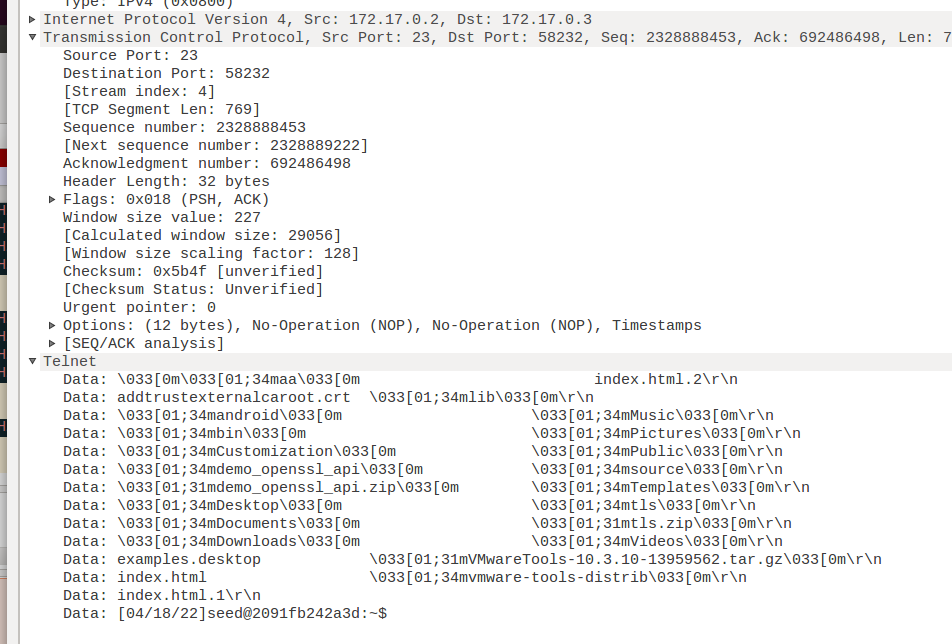


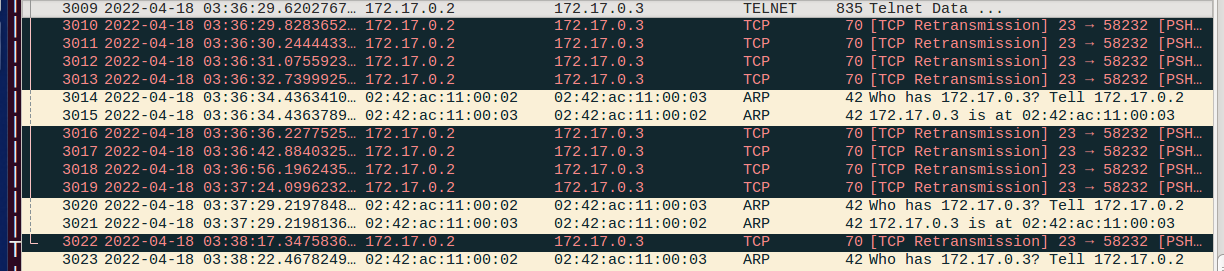
攻击指令





攻击结果



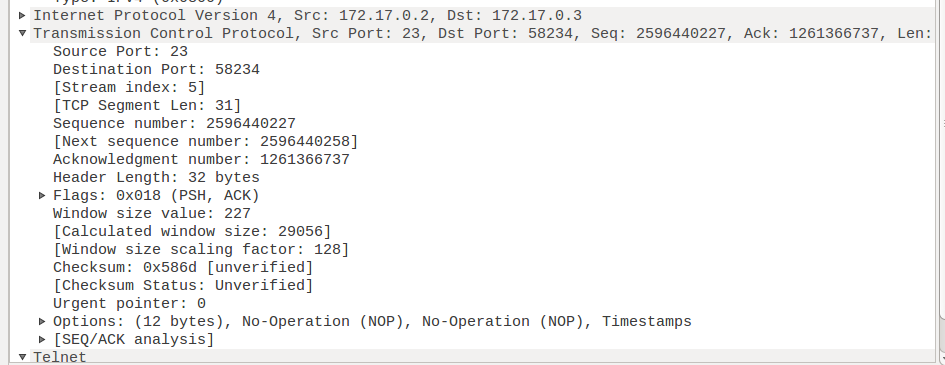


结果分析:攻击者发送伪造包，服务器返回相应ls命令运行结果，并在wireshark中截取到许多重传包，如上图所示，证明攻击者注入数据打乱了客户端与服务器之间的序列号，且客户端被冻结，对输入内容无任何相应，符合预期，攻击成功。

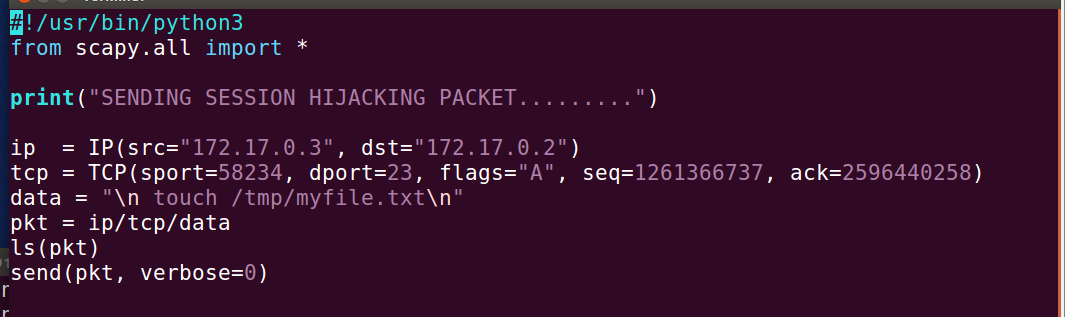
1. Scapy

手动攻击

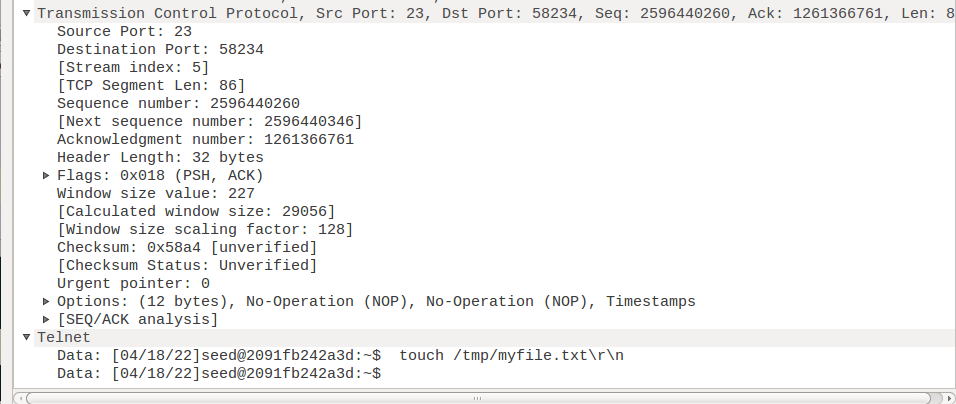
Wireshark截包

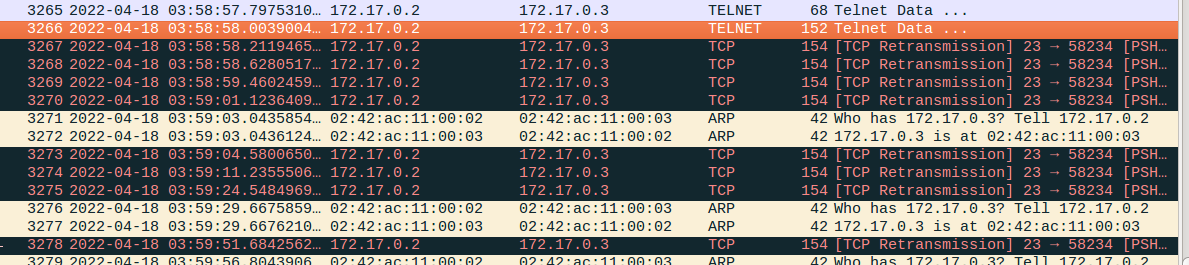


脚本代码



攻击结果

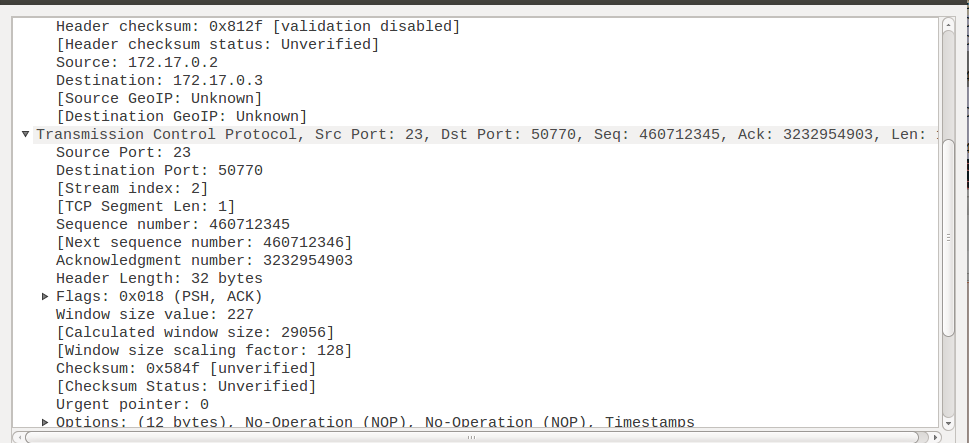




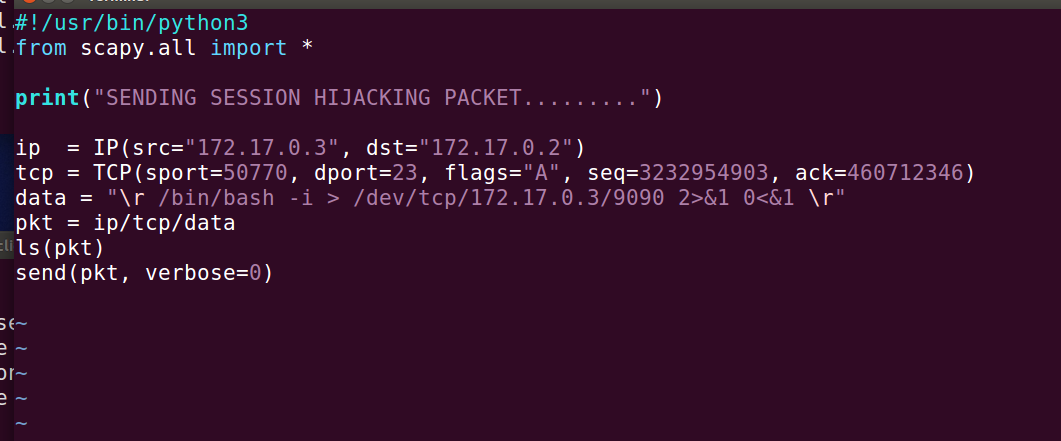
结果分析:攻击者发送伪造包，服务器返回相应命令运行结果，并在wireshark中截取到许多重传包，如上图所示，证明攻击者注入数据打乱了客户端与服务器之间的序列号，且客户端被冻结，对输入内容无任何相应，符合预期，攻击成功。

反向shell

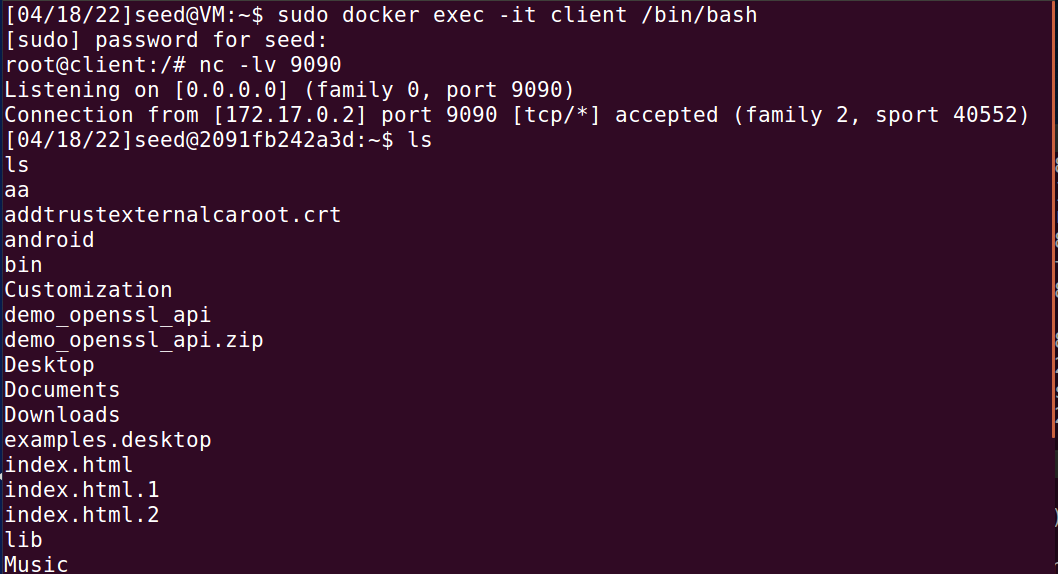
Wireshark截包



脚本代码



攻击端命令行



结果分析：显然，攻击端运行nc -lv 9090，建立一个TCP服务器监听9090端口，发送伪造包后，该终端收到服务器发来的连接请求，建立请求后，攻击者得到一运行在服务器的反向shell，结果符合预期，攻击成功。