

**入侵检测与数字取证**

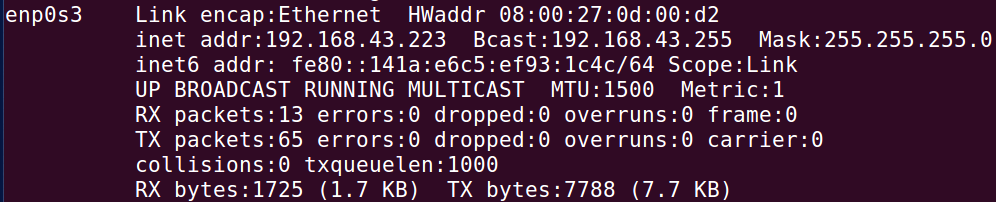
**黄雨卓 57117205**

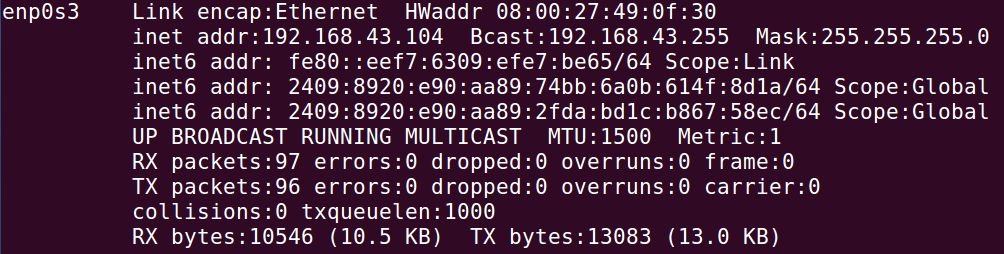
**LAB4**

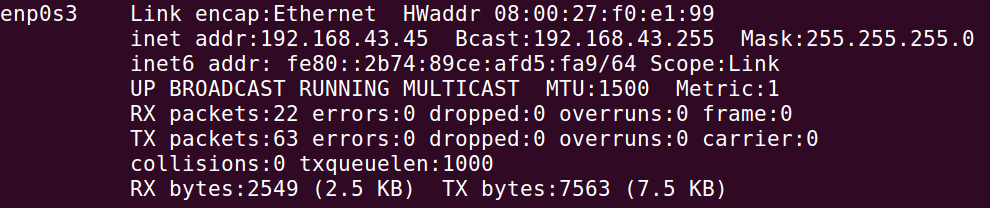
2020年9月13日

TCP/IP Attack Lab

Task1: SYN Flooding Attack



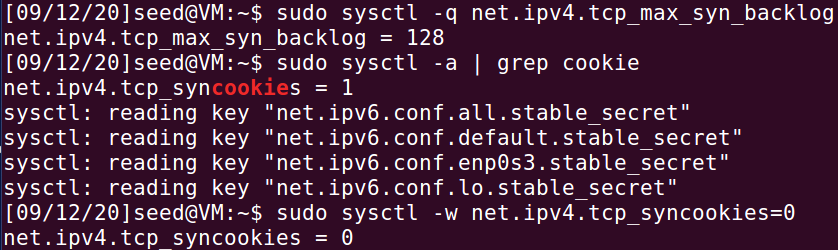


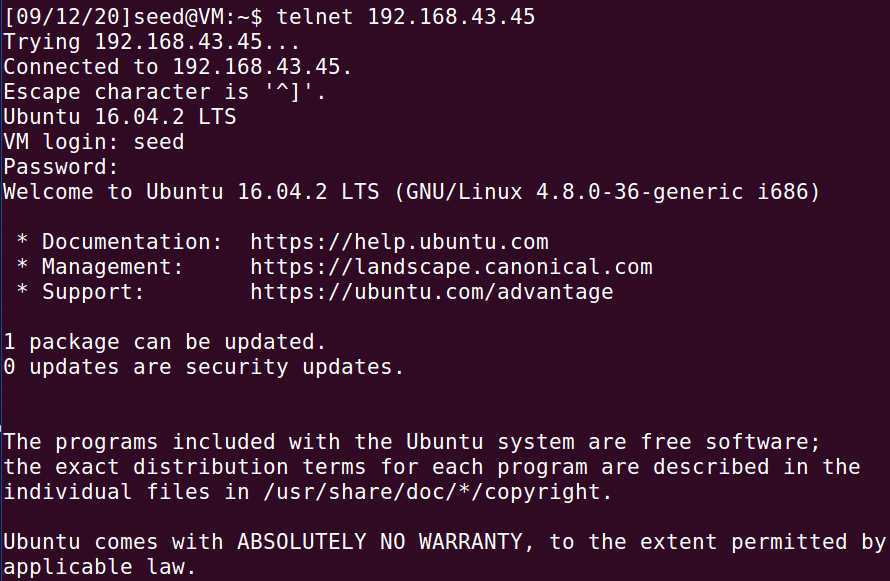


0观察者192.168.43.223

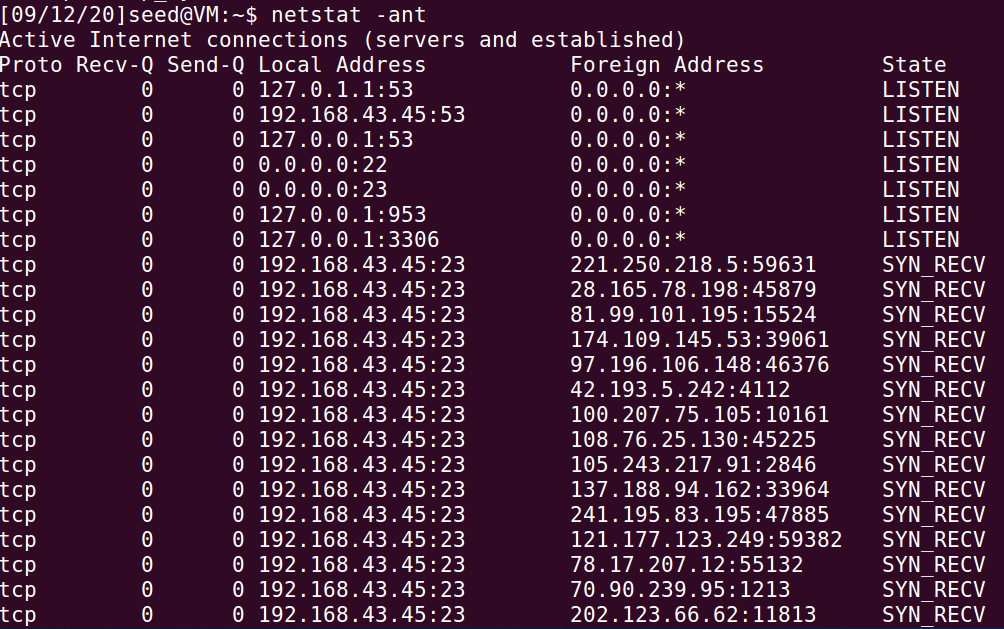
1攻击者192.168.43.104

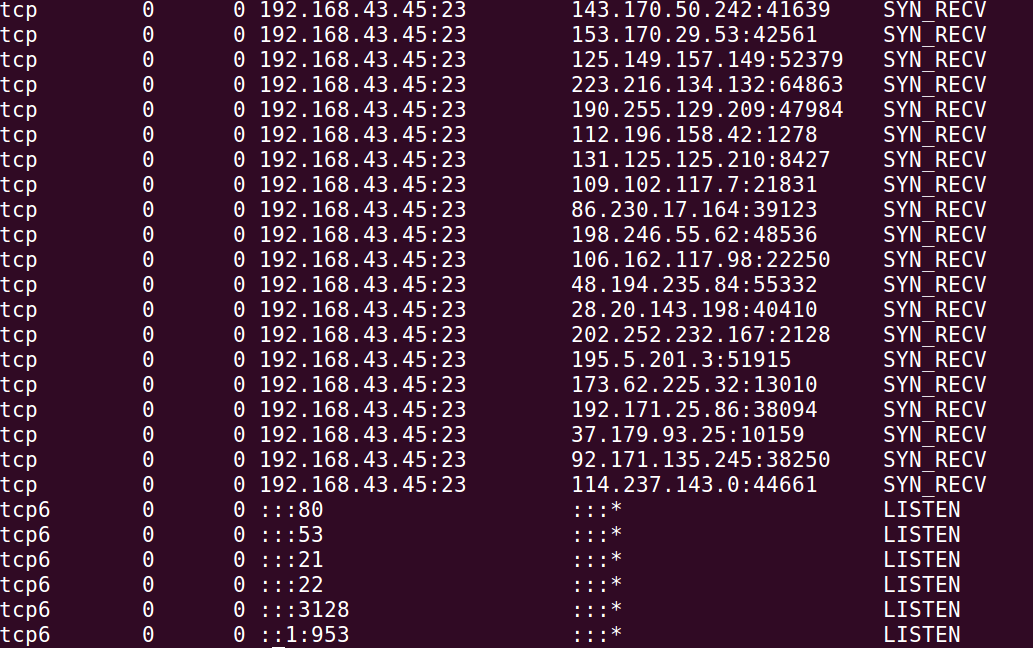
2受害者192.168.43.45











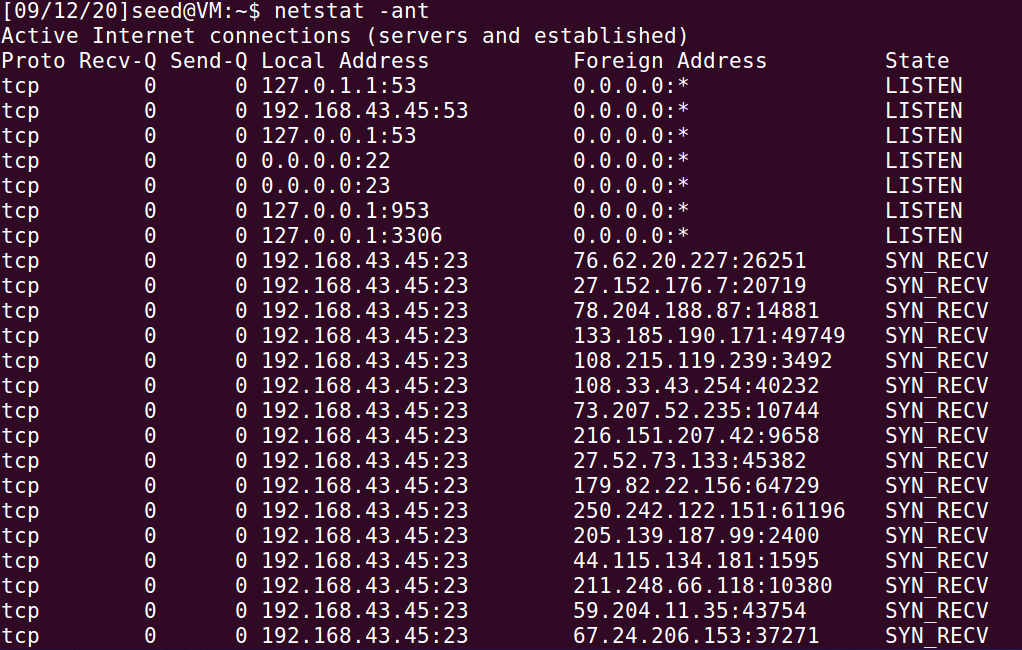
登陆失败



设置后重新进行攻击

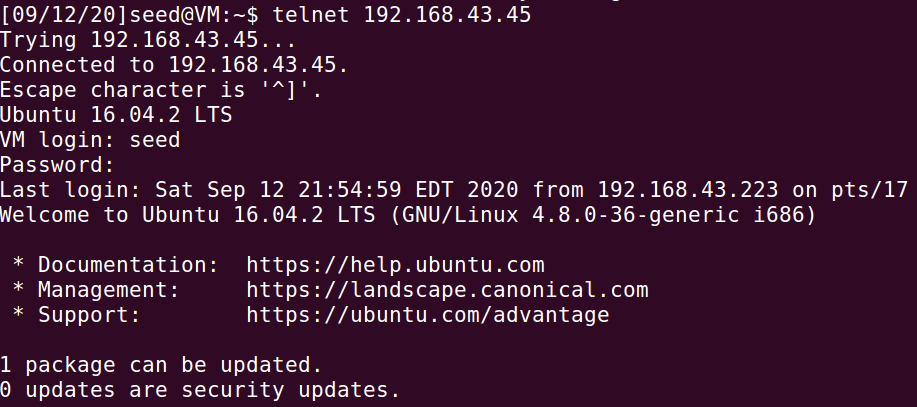


仍然挡不住

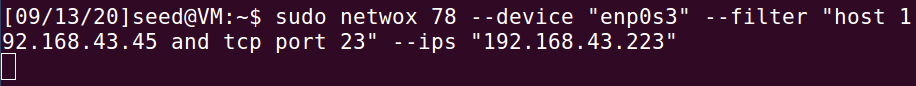


Task2: TCP RST Attacks on telnet and ssh Connections

对telnet进行TCP RST攻击





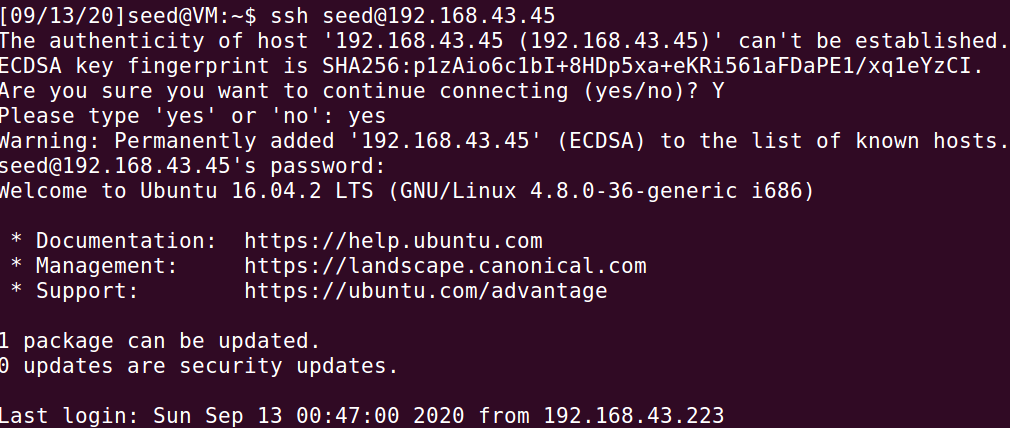


攻击后，断开连接，攻击成功





对ssh 进行TCP RST攻击





进行攻击

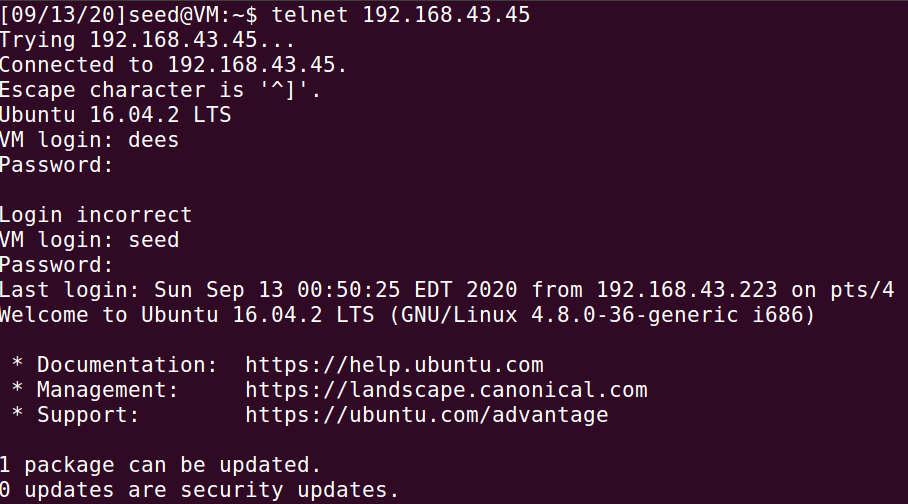


攻击后，连接中断，攻击成功

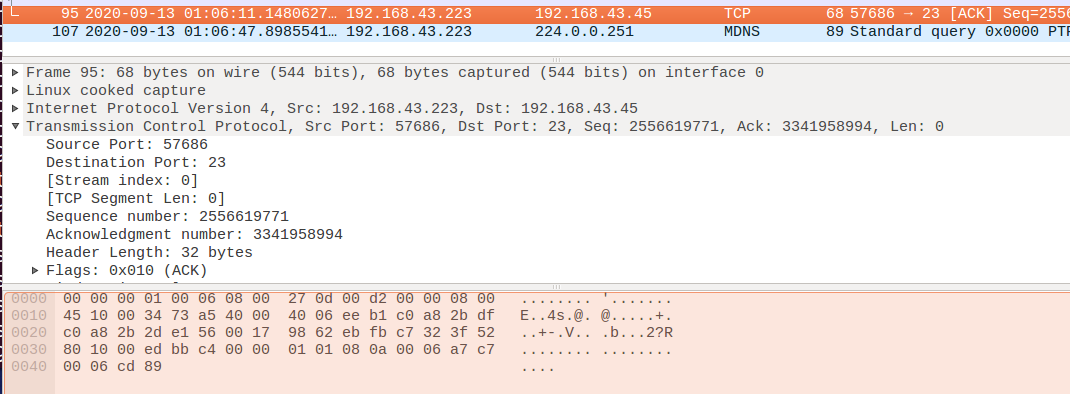




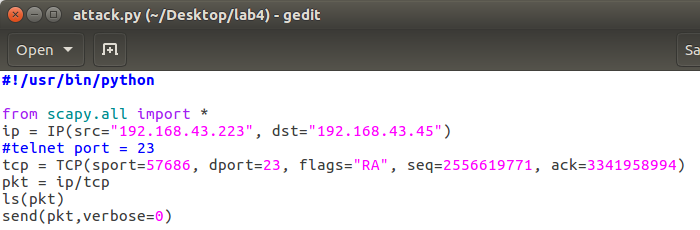
利用Scapy 实施 TCP RST 攻击



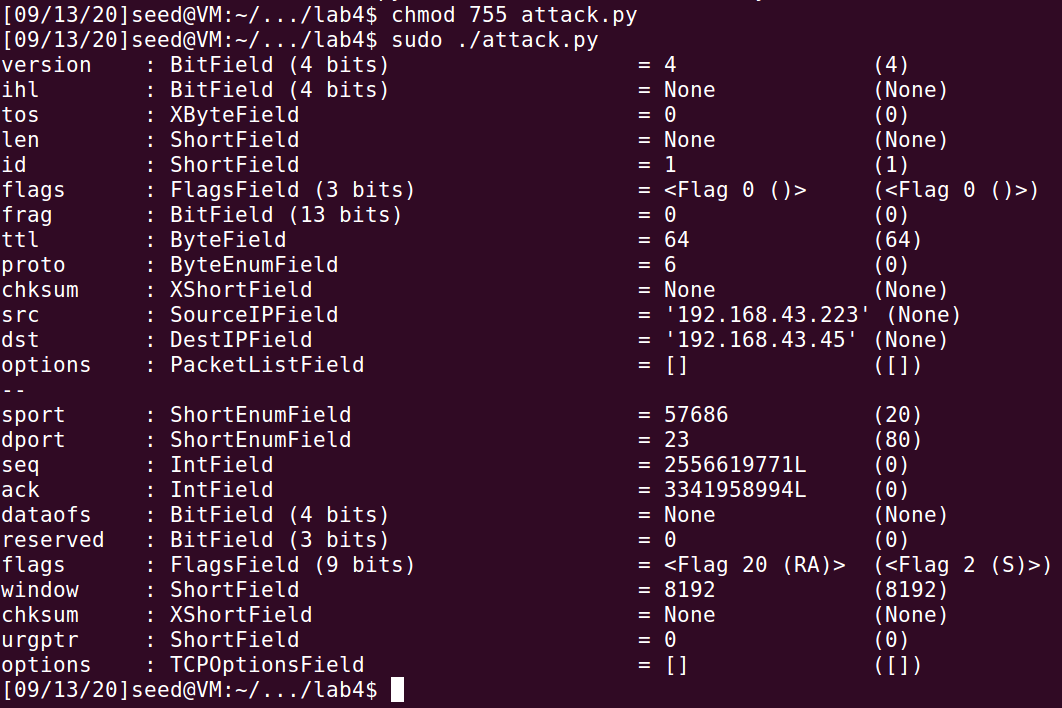


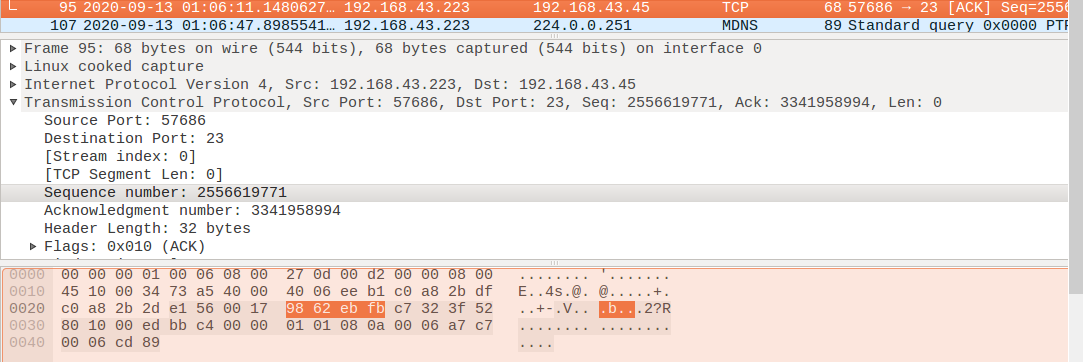


构造攻击报文



进行攻击，连接断开，攻击成功。

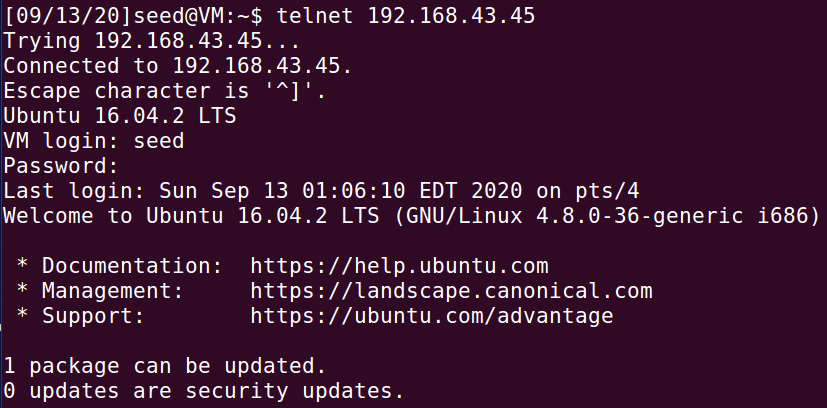


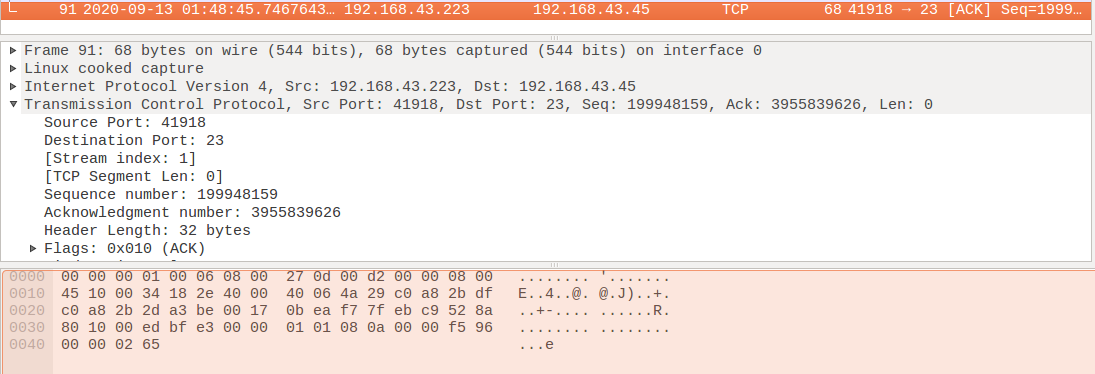


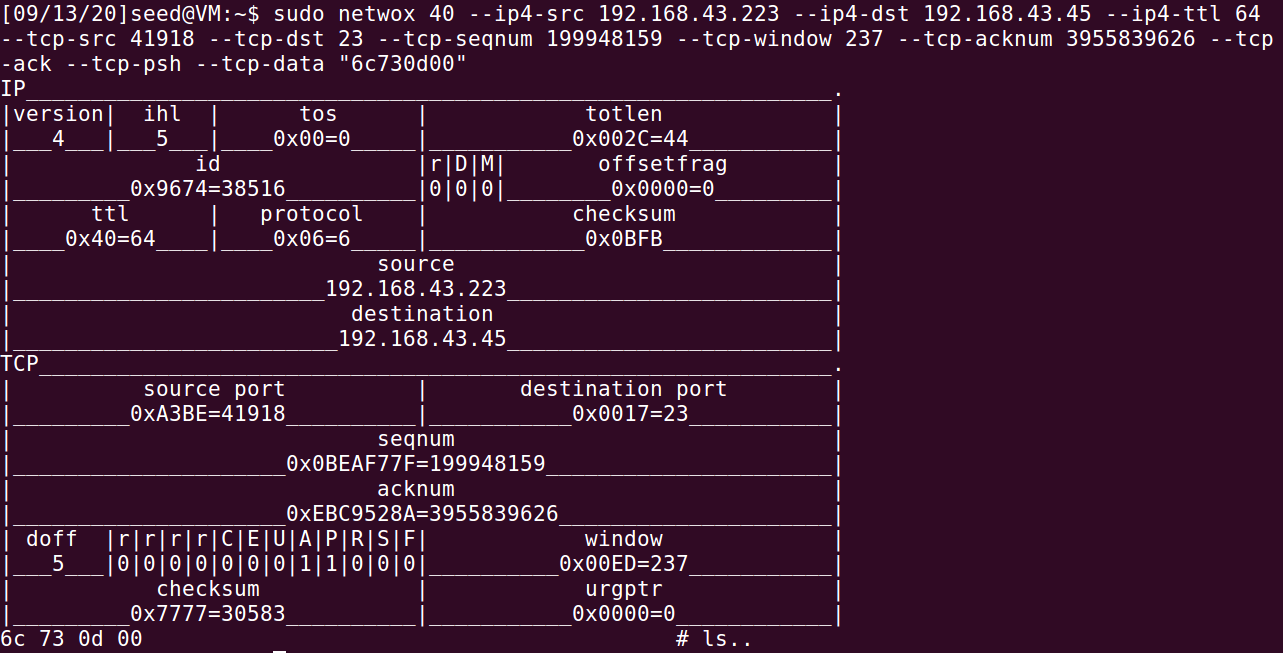


Task4: TCP Session Hijacking

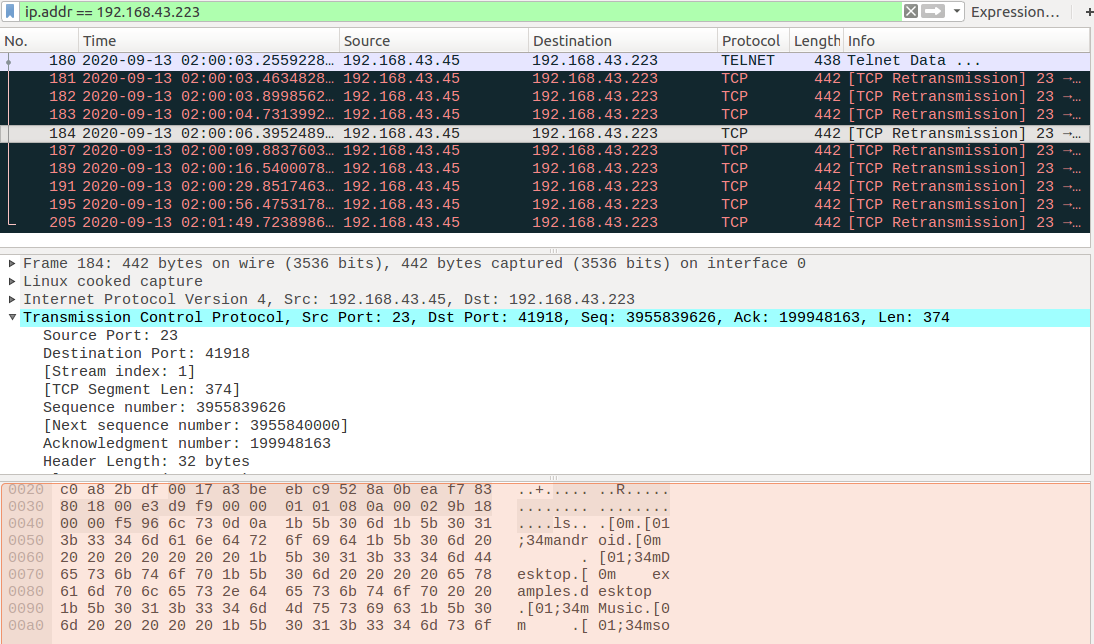
Netwox:



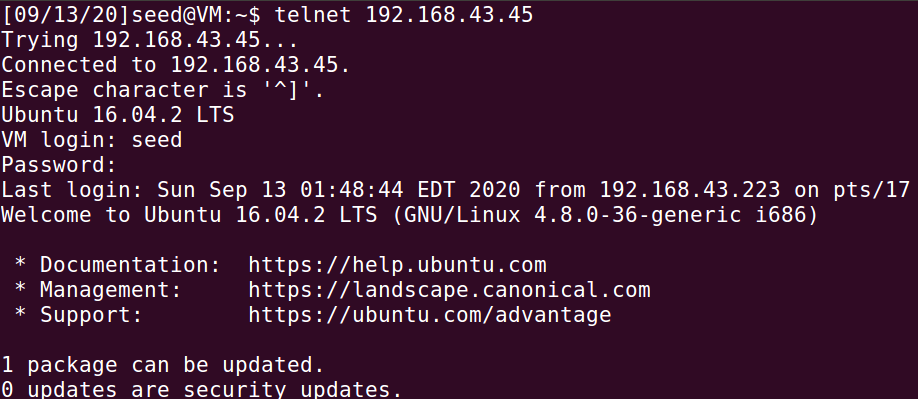


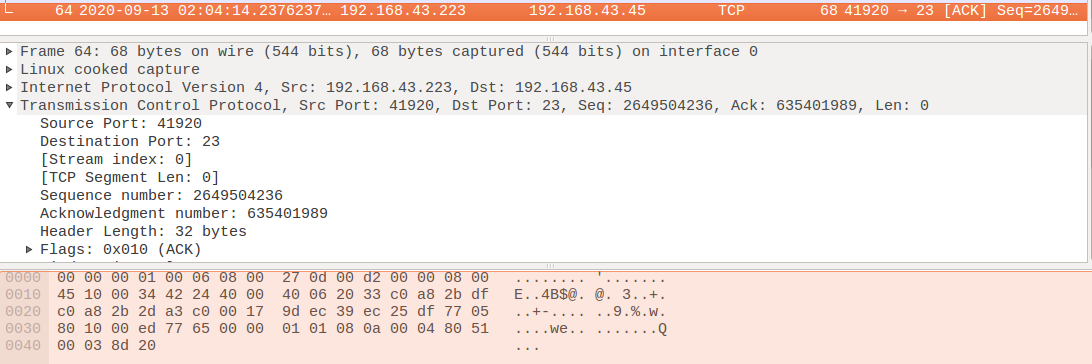


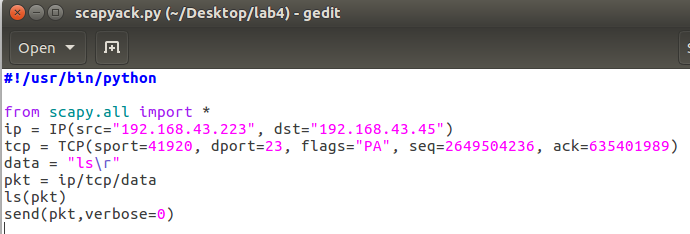
攻击成功

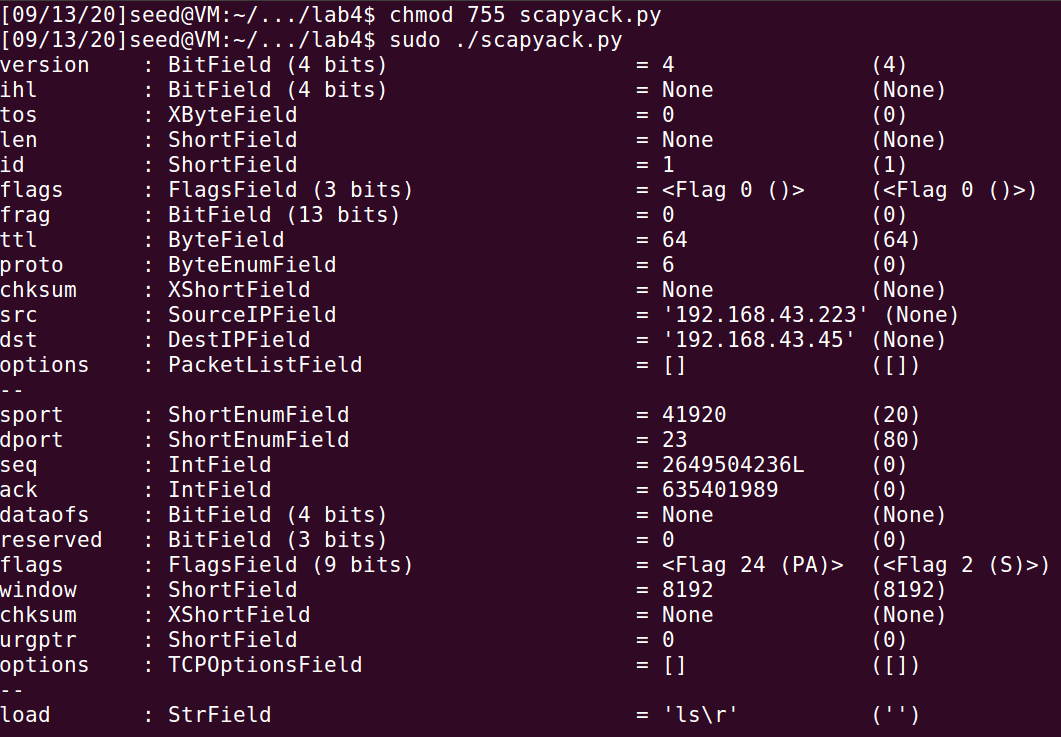


Scapy:









攻击成功

