**Mitnick Attack Lab**

2018级 信息安全 管箫 18307130012

一、环境配置

1、主机网络配置

①主机A（Attacker）：IP Addr：192.168.61.138；MAC：00:0c:29:01:41:ae

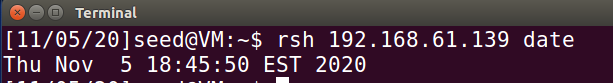
②主机B（X-Terminal）：IP Addr：192.168.61.139；MAC：00:0c:29:a3:8a:e6

③主机C（Server）：IP Addr：192.168.61.140；MAC：00:0c:29:aa:55:ad

二、报告正文

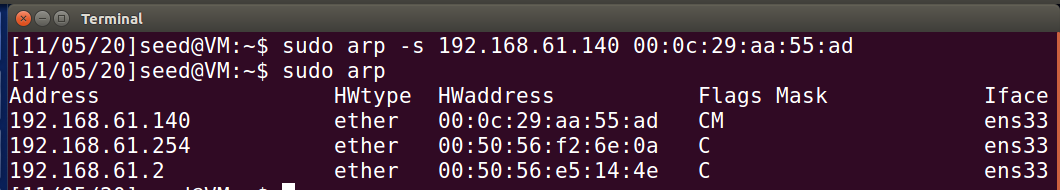
1、实验环境配置

①配置.rhosts，观察到成功完成



2、Task 1: Simulated SYN flooding

①配置静态arp表



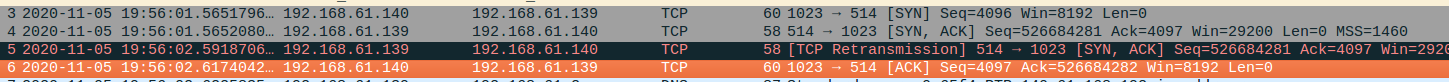
3、Task 2: Spoof TCP Connections and rsh Sessions

①Task 2.1: Spoof the First TCP Connection

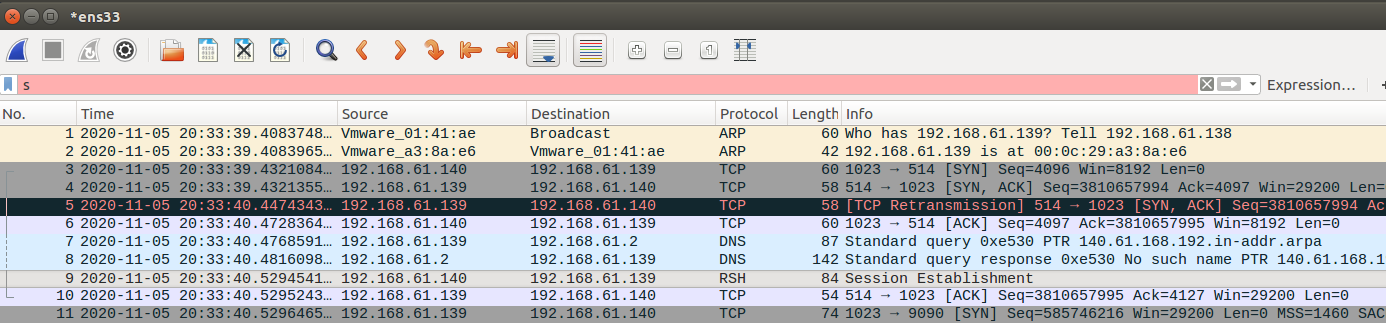
发送伪造的SYN包，发现收到回应



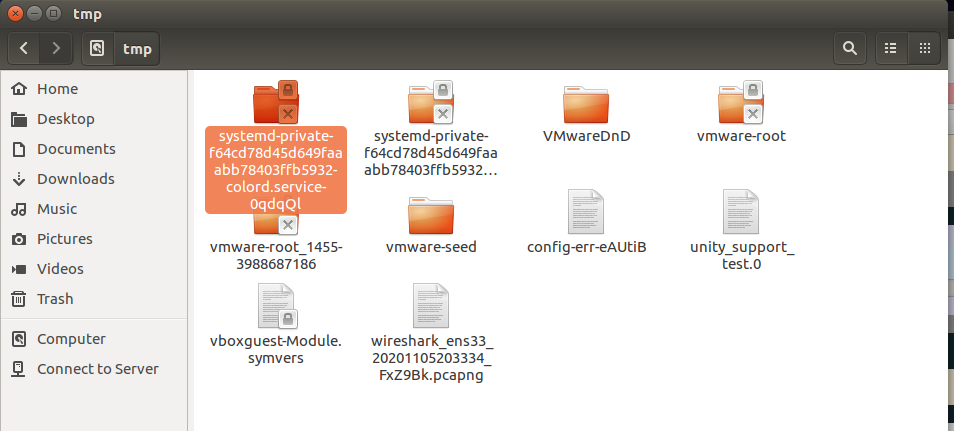
完成抓包欺骗工作



完成RSH数据欺骗工作

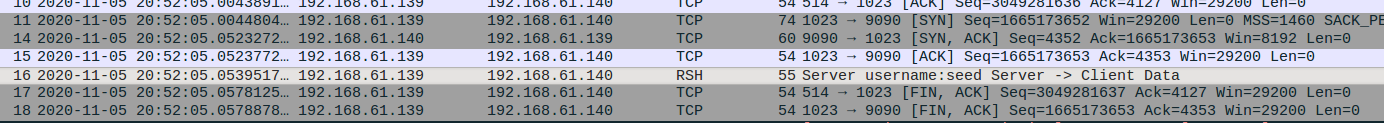


此时我们的指令并没有执行，观察到/tmp文件夹下并没有新建我们想要的文件夹

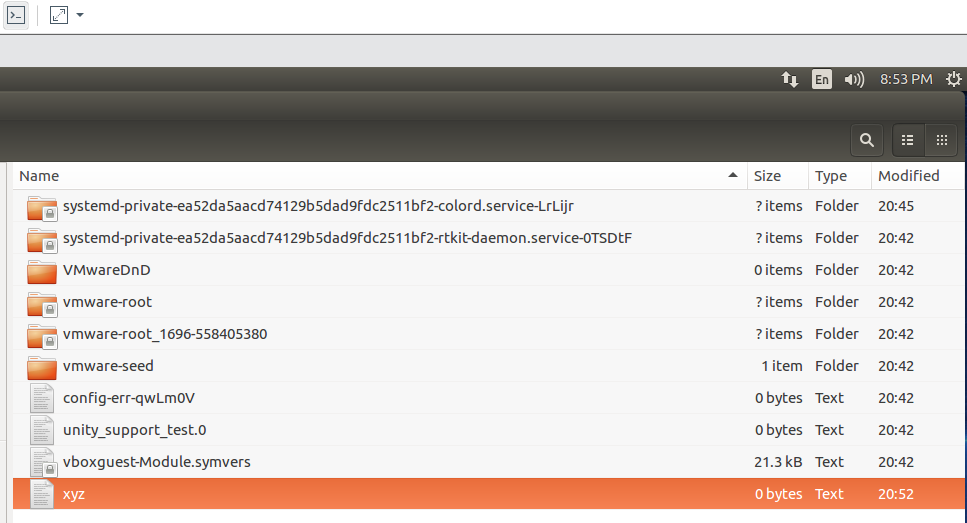


这是因为还没有建立err信道，rshd会阻塞我们的命令。

我们伪造对第二连接的回应



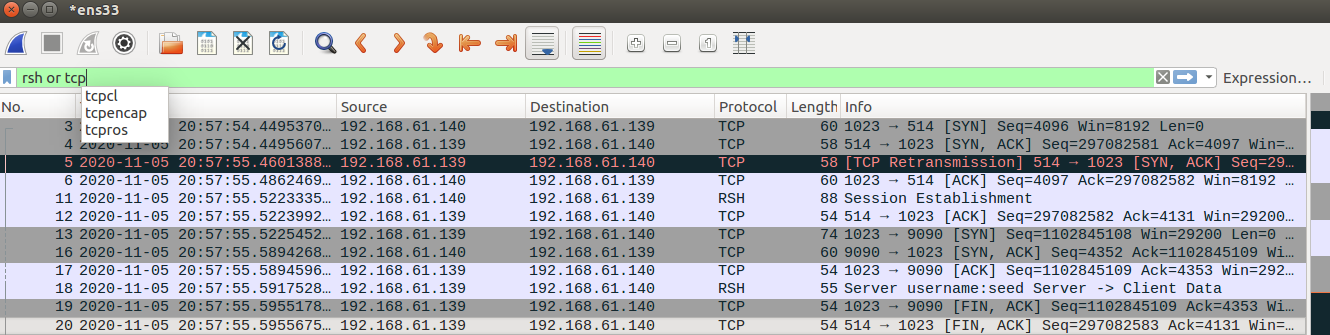
观察到xyz文件被创建，时间符合当前系统时间



4、Task 3: Set Up a Backdoor

修改攻击用的scapy脚本，将命令置换为攻击指令echo + + > .rhosts

使用wireshark抓包，观察到两个阶段的握手均完成



在攻击用主机A上执行rsh指令，观察到连接建立。

