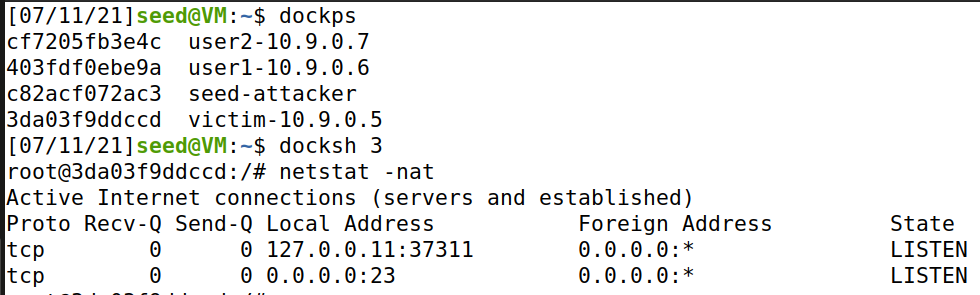
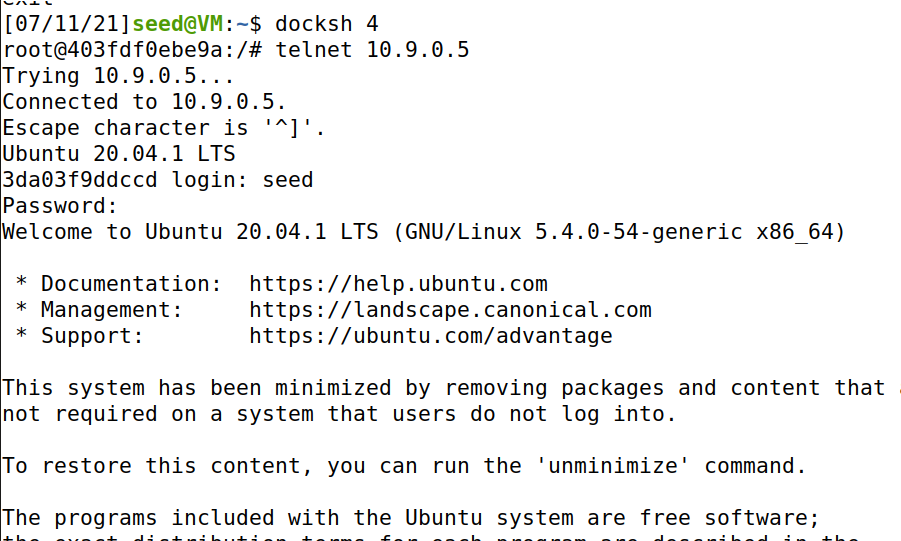
1、

环境配置并观察套接字



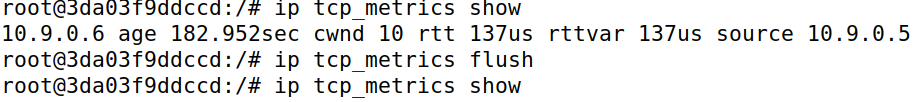
Telnet连接测试



检查syn攻击对策，syncookie为关闭：

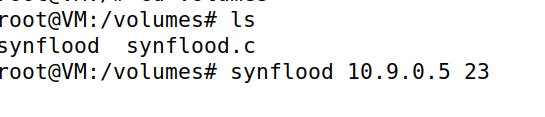


消除内核缓存：

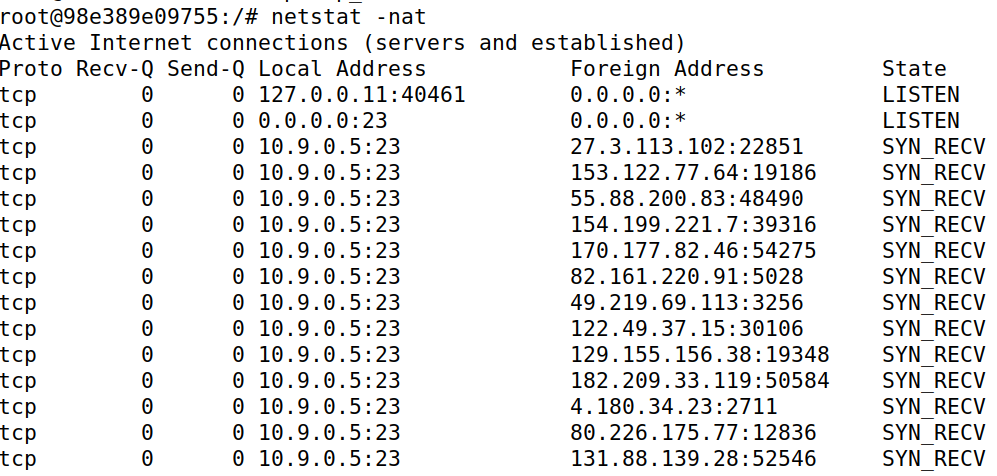


(重新启动了一次docksh，地址变化了)

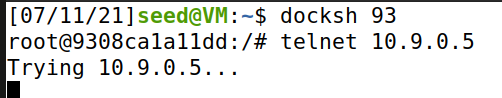
Seedattacker中运行编译好的攻击程序：



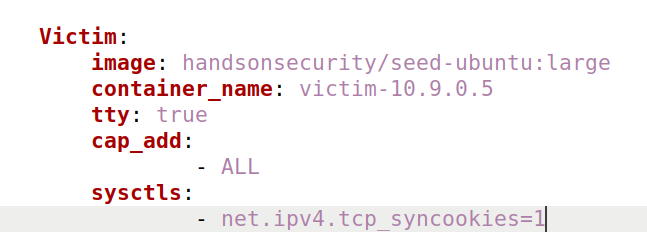
Victim中查看TCP连接建立，后续请求不完整：



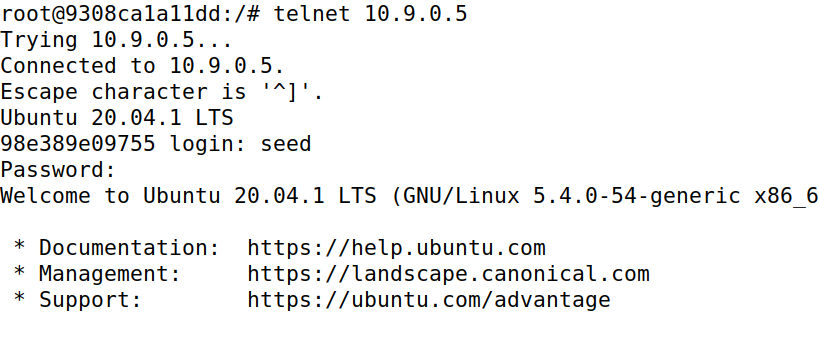
此时无法Telnet连接到受害者：



修改配置文件：

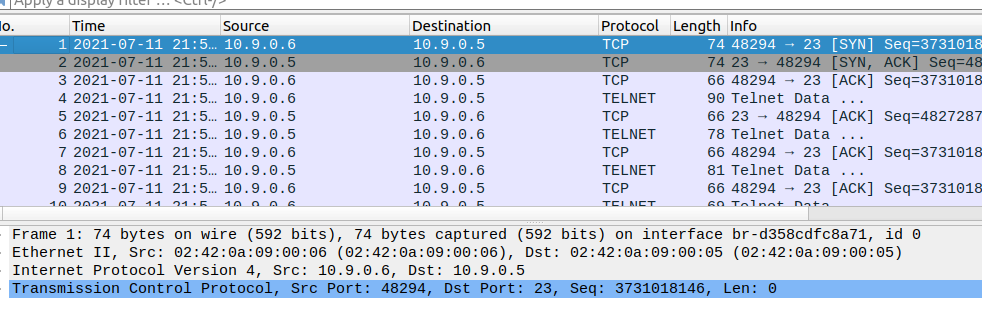


运行synflood程序后Telnet成功：

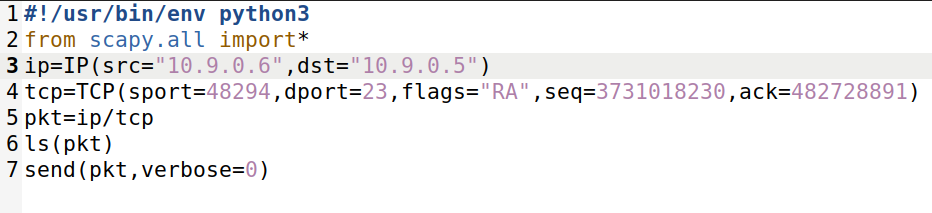


2、

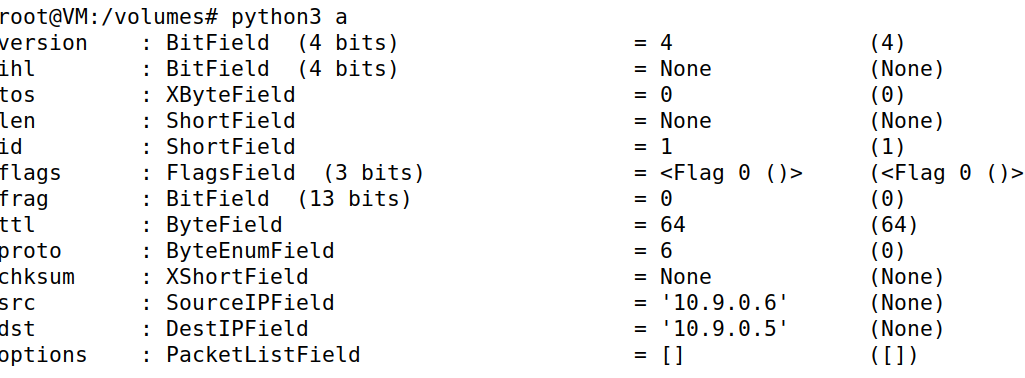
通过wireshark观察Telnet的源端口、目的端口以及ack、seq



根据观察到的端口编写攻击程序：



运行：

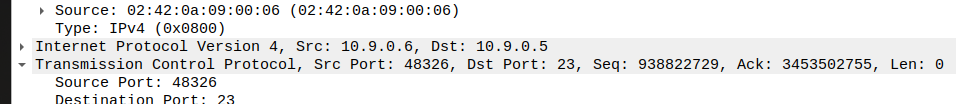


Telnet连接被终止：

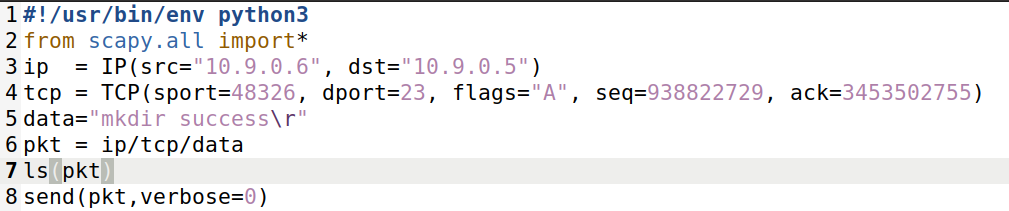


3、

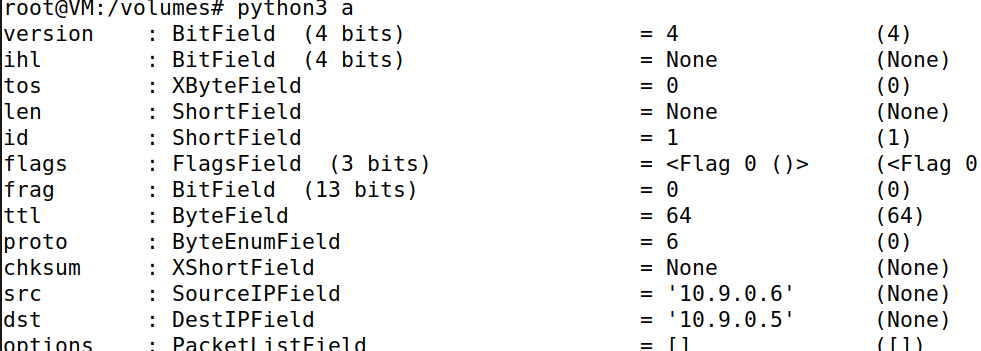
同task2，建立连接后通过wireshark抓包得到目的端口、源端口和seq、ack



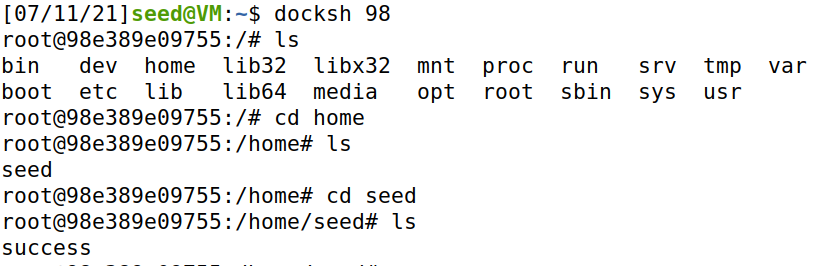
根据抓包信息完成攻击程序：



运行攻击程序：



在victim中成功引入文件：



4、

编写程序获得victim的shell



成功从attack上拿到shell：

