

网络攻防技术基础课程实验报告

|  |  |
| --- | --- |
| 实验名称： | 实验四  TCP攻击 |
| 实验日期： | 2024-04-09 |
| 实验地点： | 西部片区4号楼301 |
|  | |
| 学号： | 33920212204567 |
| 姓名： | 任宇 |
| 专业年级： | 软工2021级 |
| 学年学期： | 2023-2024学年第二学期 |

1. **实验目的**

* 熟悉并实践常见的TCP攻击，如洪泛攻击、复位攻击和TCP会话劫持及创建反向shell等。
* 熟悉Netwox和Scapy的使用

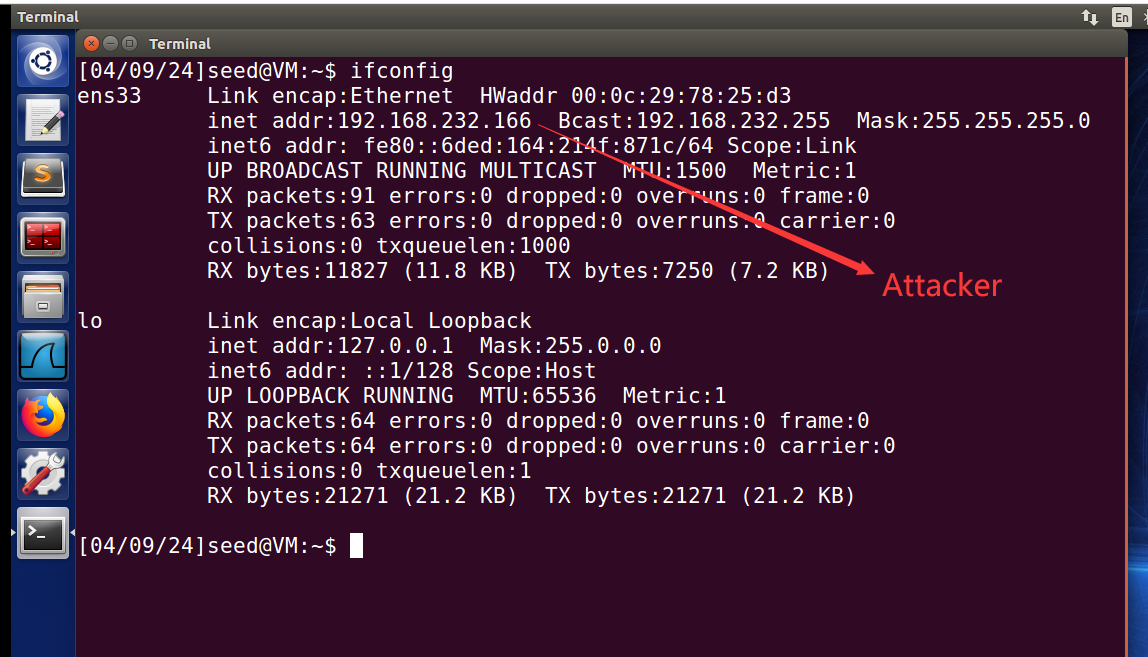
1. **实验用到的软件或工具**

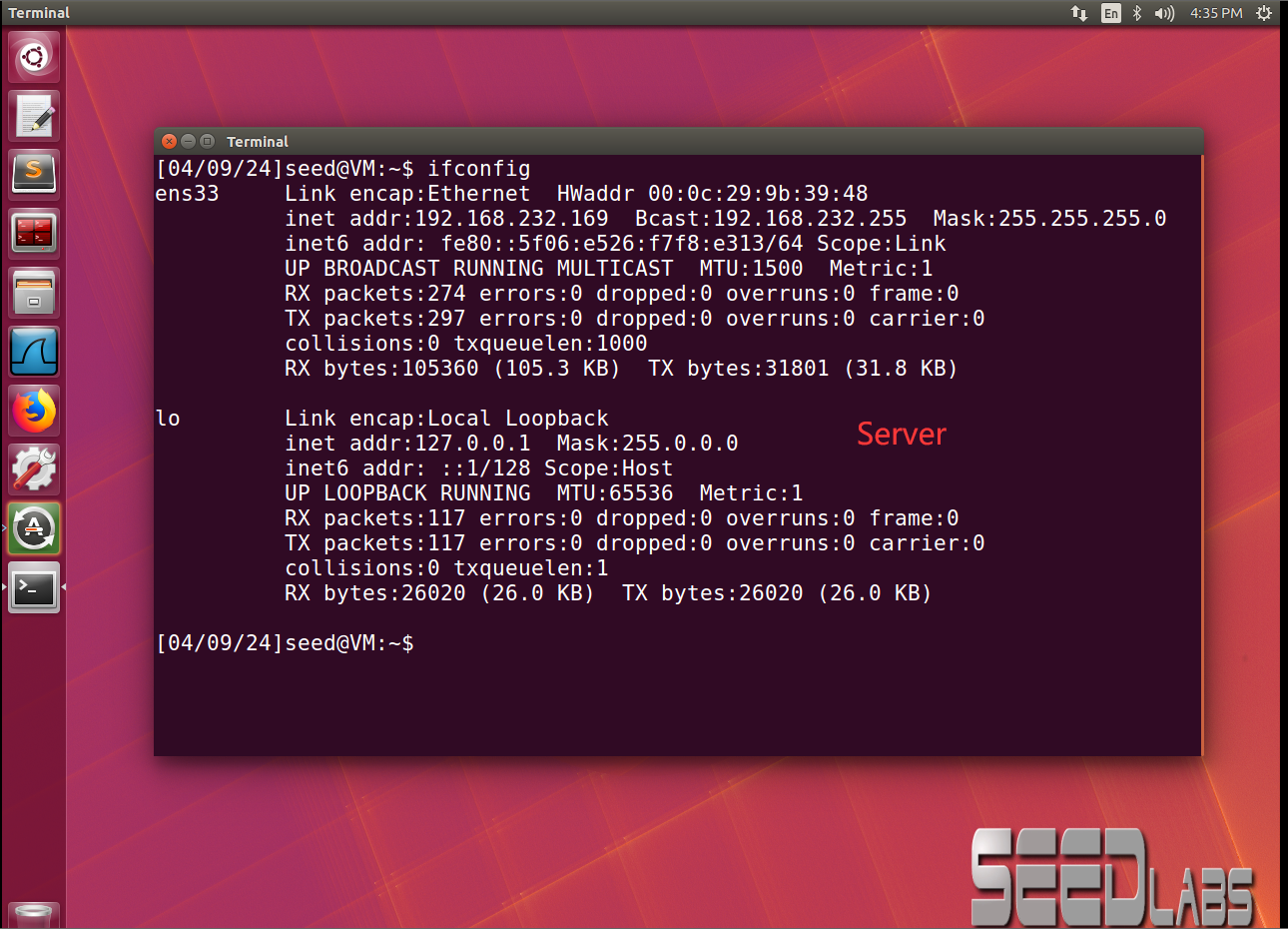
虚拟机软件：VMware Workstation Pro 17

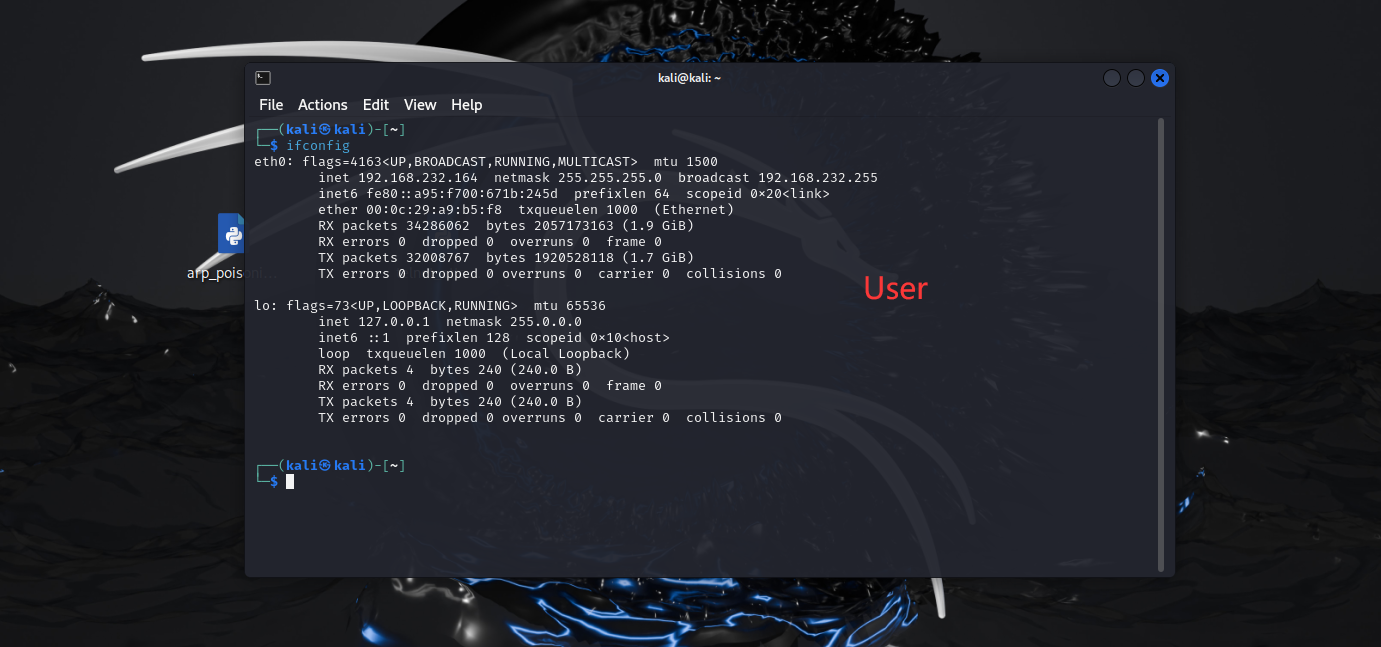
虚拟机系统：SEED Ubuntu-16.04-32bit、kali

网络环境：三个虚拟机环境配置在同一NAT网络中

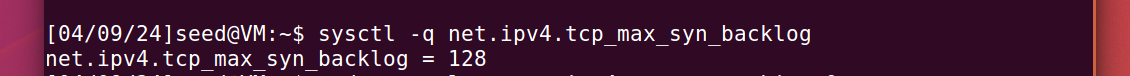
1. **实验过程**
2. **TCP洪泛攻击（Netwox）：**
3. 开启三个虚拟机Server(SEED Ubuntu-16.04-32bit)、Attacker（SEED Ubuntu-16.04-32bit）以及User（kali），配置在同一NAT网络：







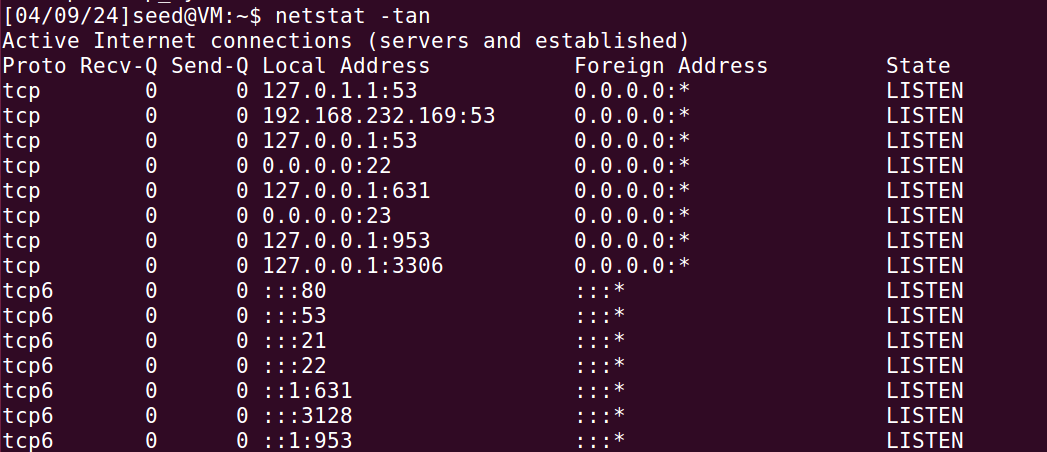
1. 查询Server半开放连接队列上限值：

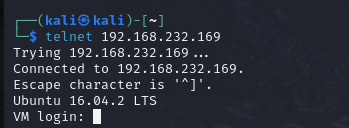


1. 关闭Server的洪泛攻击防御（SYN cookies）：

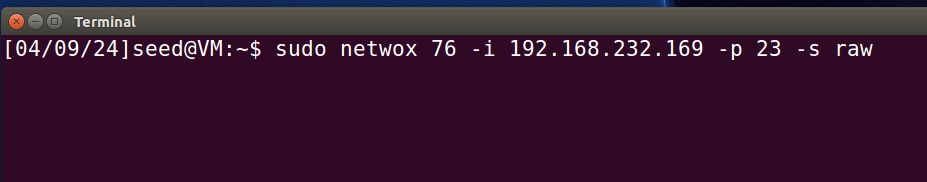


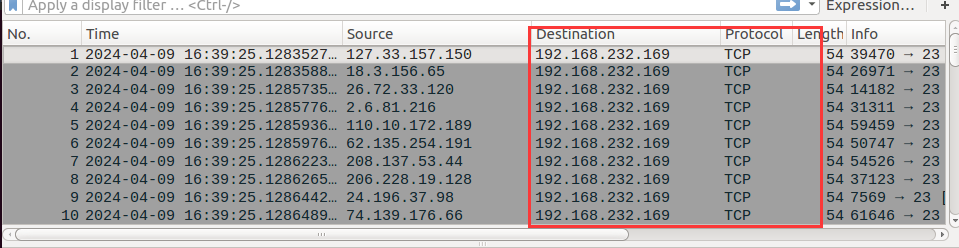
1. 攻击前检查Server的半打开连接的状态，并测试使用User连接：



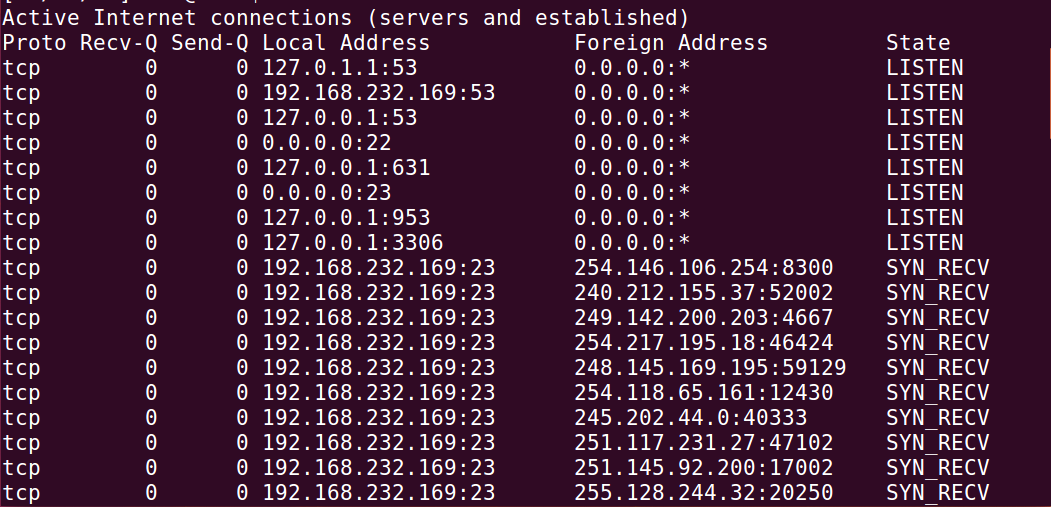


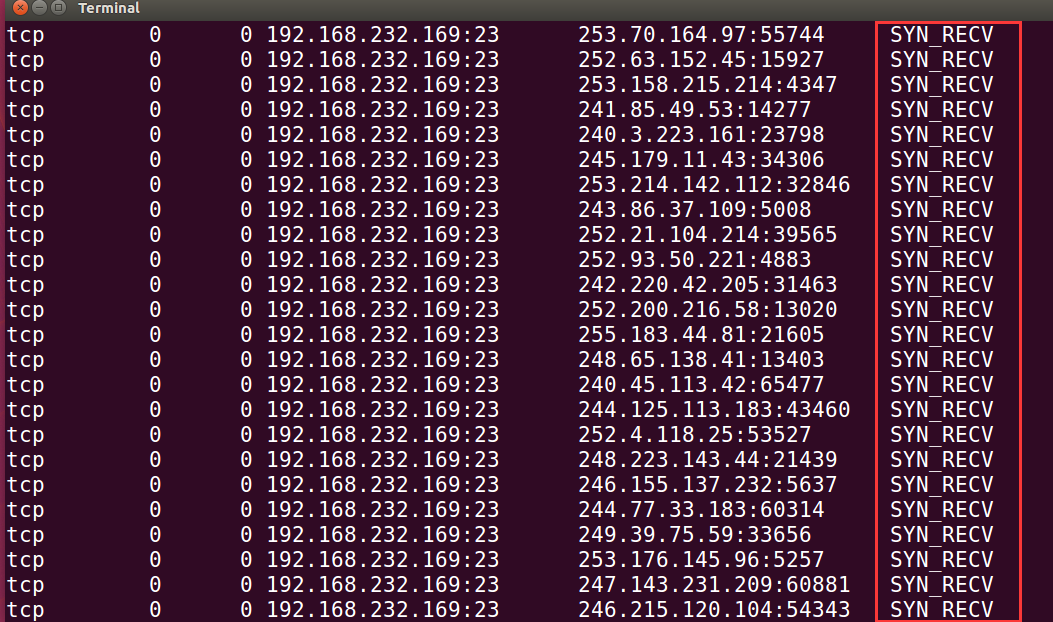
1. Attacker使用Netwox工具包76号，开始SYN洪泛攻击：

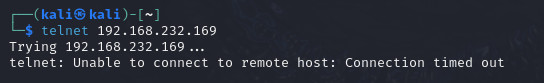


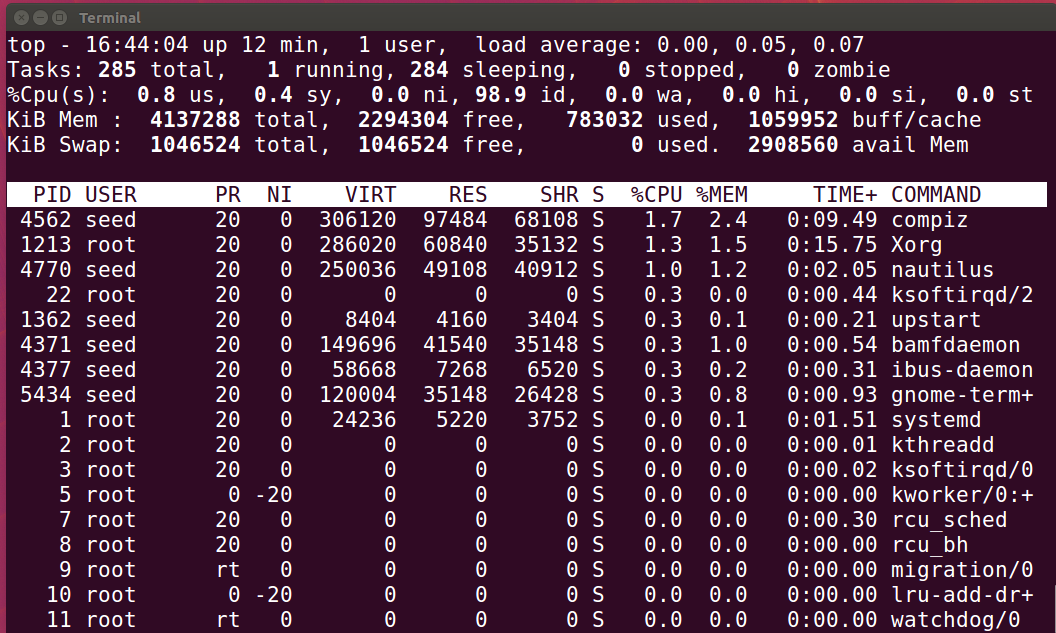


1. 再次观察Server的半打开连接状态，并用User机Telnet测试连接Server，top命令查看Server的资源消耗情况：

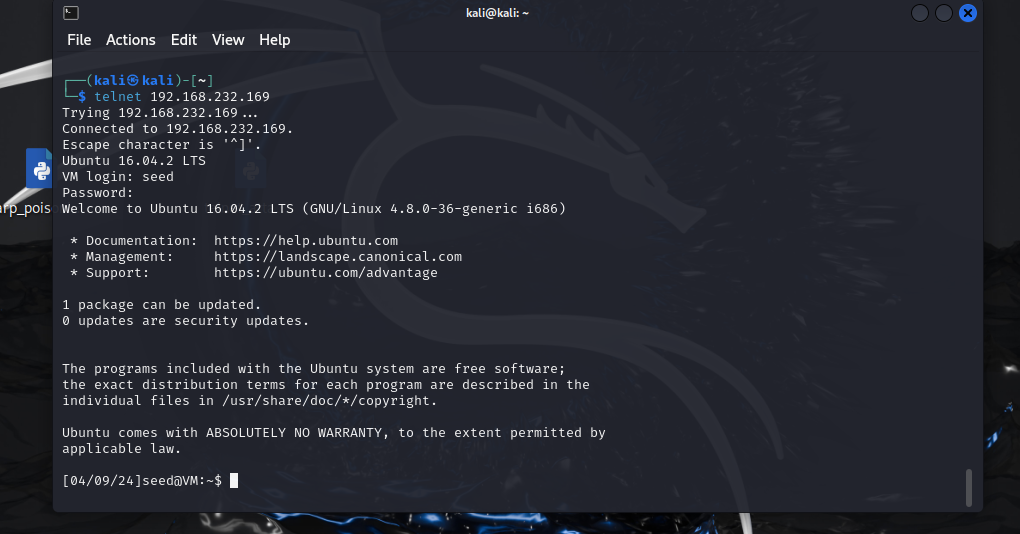




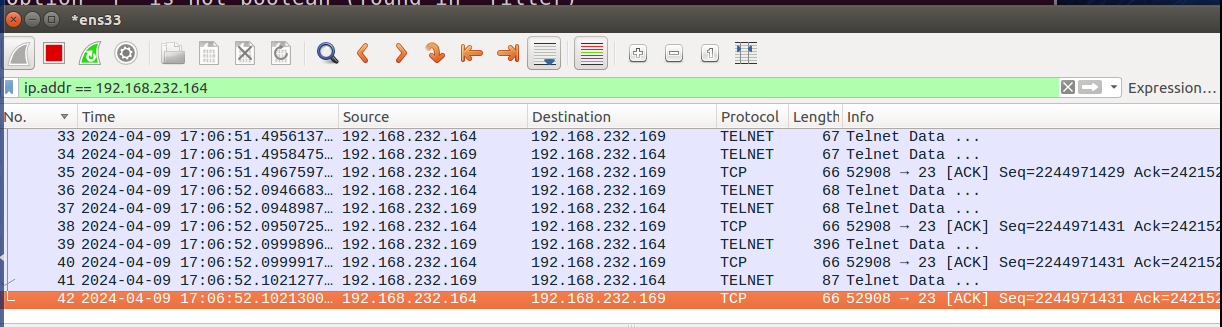




1. **复位攻击（Netwox及Scapy两种方法）：**
2. 网络环境配置和上文一致，使用User机telnet远程登陆服务器：

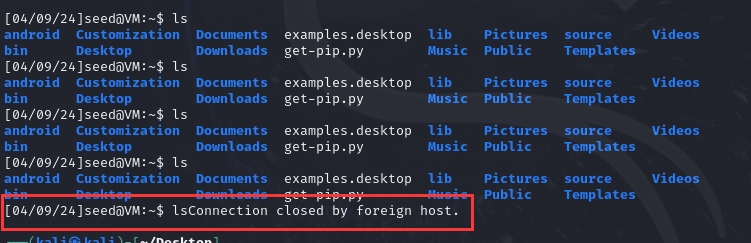


1. Attacker中运行Wireshark捕获从服务器到客户端的TCP数据包：

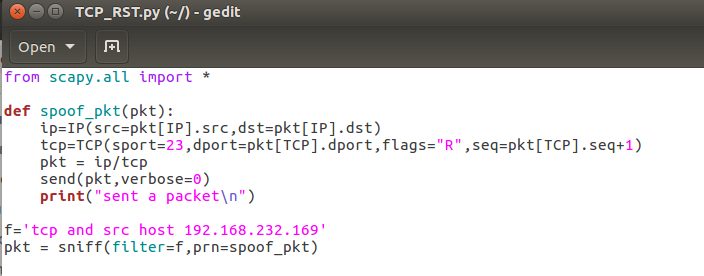


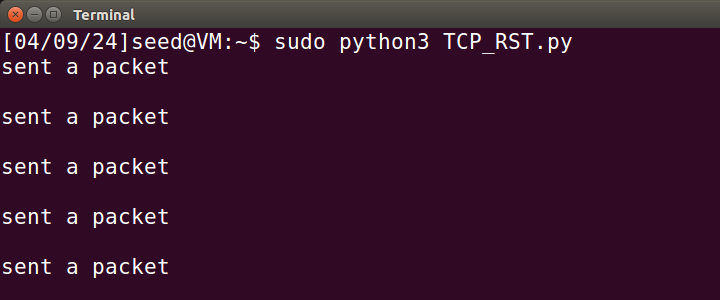
1. 使用Netwox工具进行攻击（78号），中断连接，观察现象：

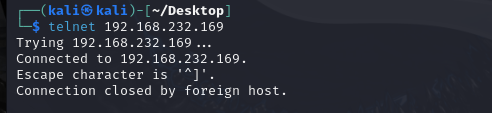




1. 使用Scapy编写程序，发送RST包：

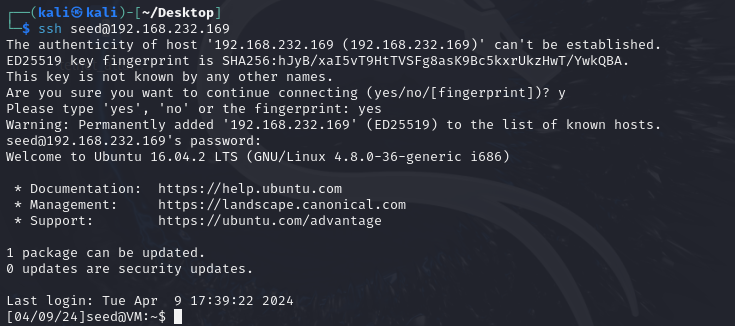




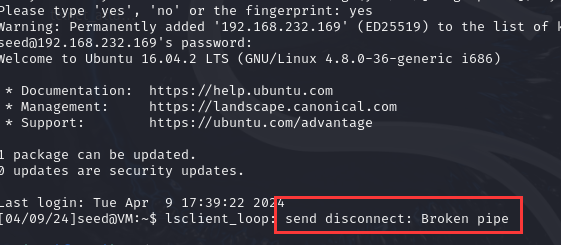


1. 同样步骤，用于SSH连接的TCP复位攻击，观察结果：

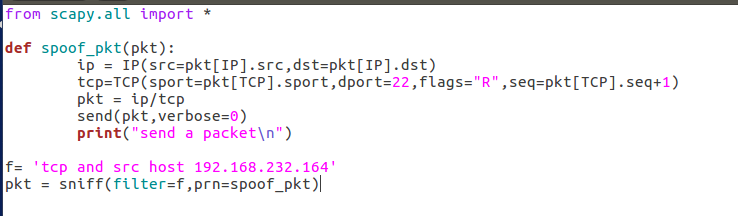
ssh登录：

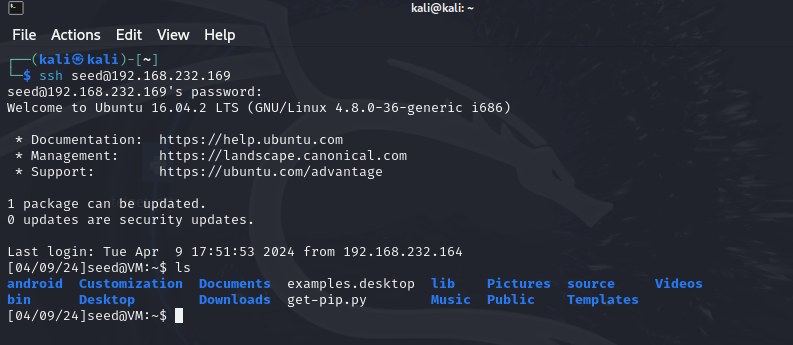


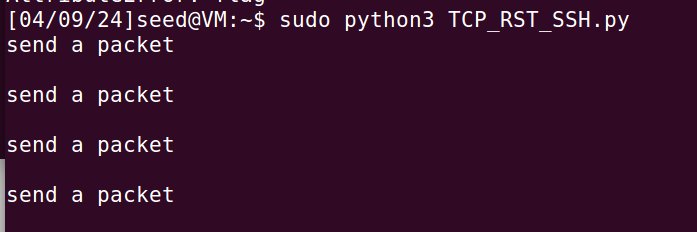
使用Netwox进行攻击：

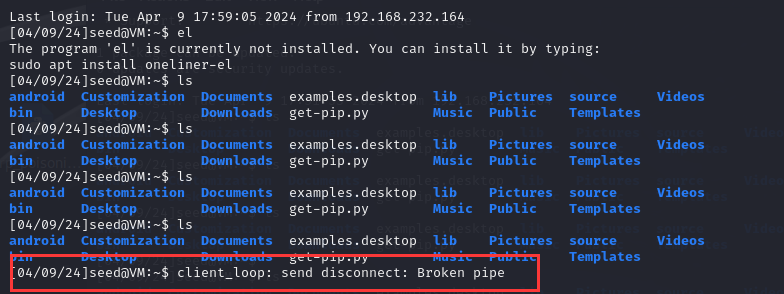


使用Scapy进行攻击：





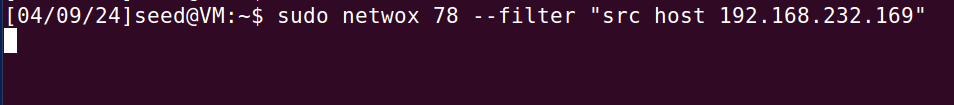




1. 针对流媒体服务的TCP复位攻击，首先让靶机访问某视频网站正常浏览视频：



1. 攻击机开启TCP复位攻击：



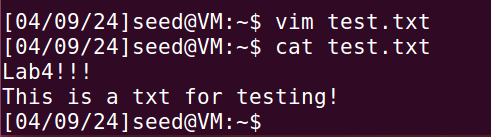
1. 观察浏览视频情况，此时视频无法继续播放，连接断开：



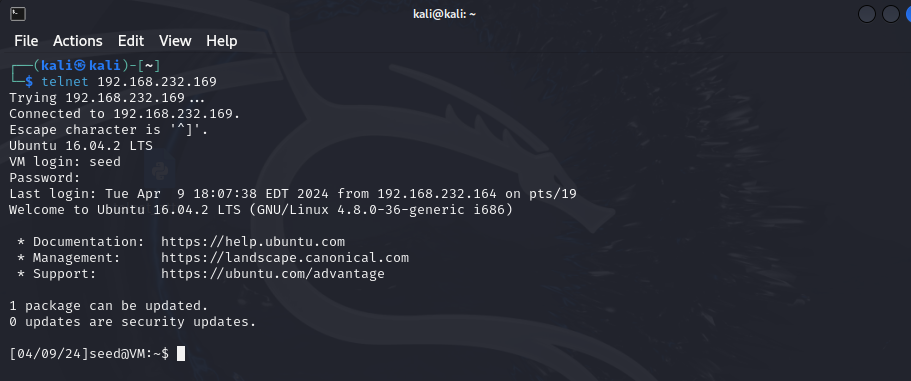
1. **TCP劫持（Scapy）：**

TCP会话劫持攻击的目的是通过向会话注入恶意内容来劫持两个受害者之间的现有TCP连接(会话)。如果该连接是telnet会话，攻击者可以将恶意命令(例如删除重要文件)注入该会话，从而导致受害者执行恶意命令。

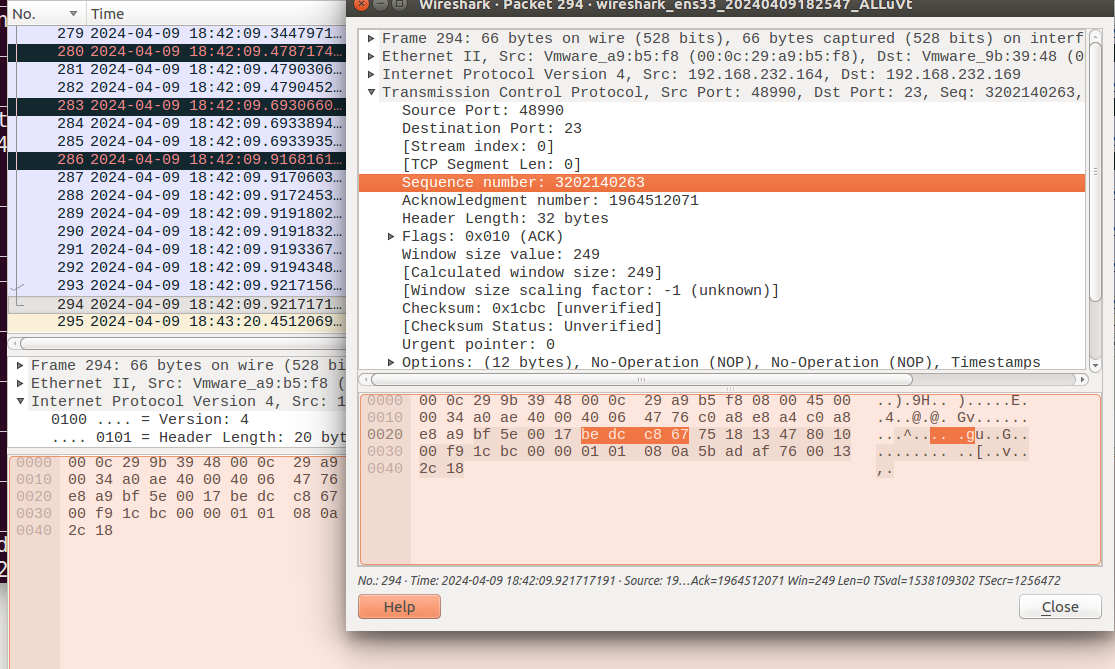
1. Server机上新建一个txt文件：



1. 用户机与服务器建立连接：

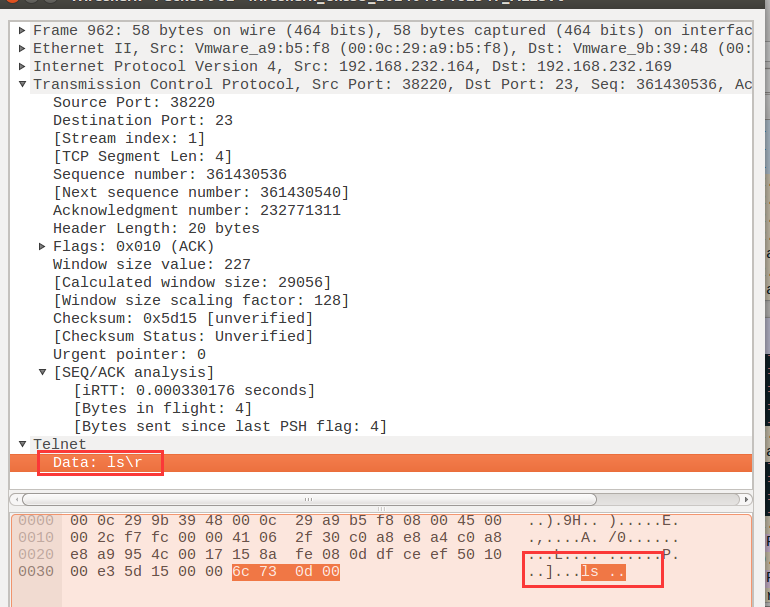


1. Attacker机使用wireshark嗅探，找到最后一个从客户端发往服务器的telnet数据包：

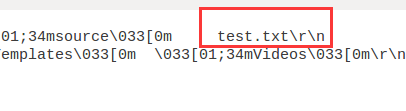
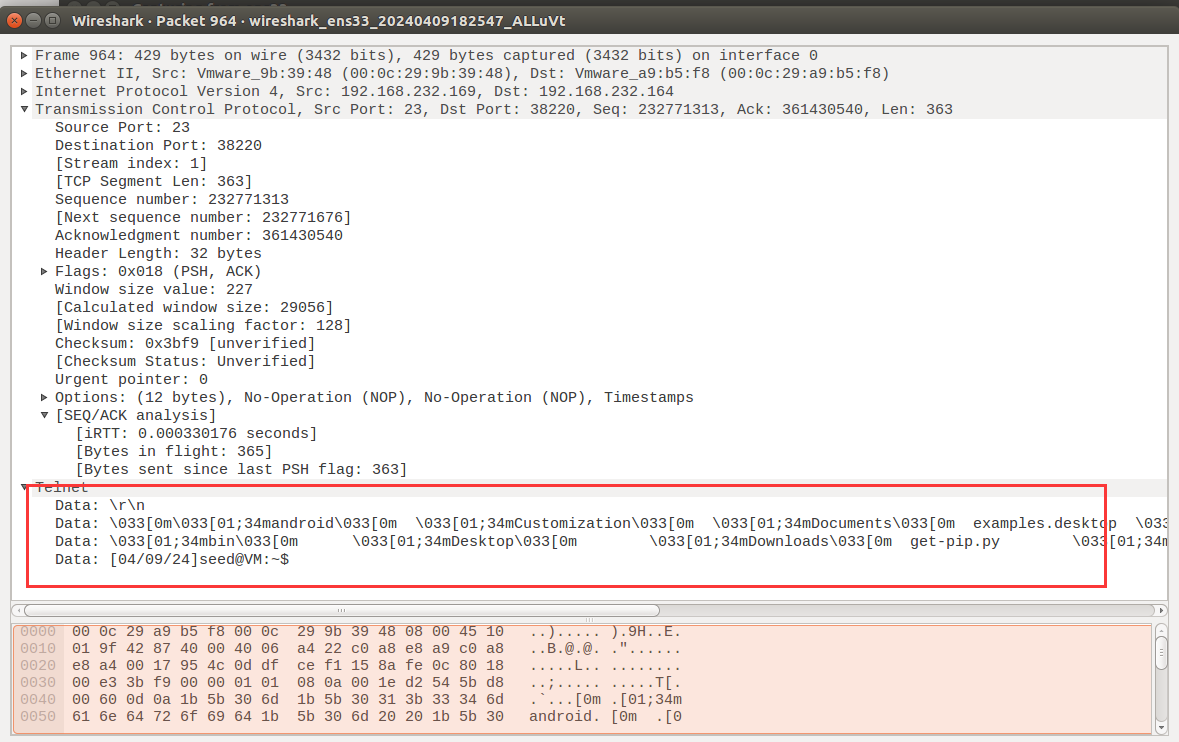


1. Attacker机上，使用netwox 40构造攻击指令ls，并发送给服务器：

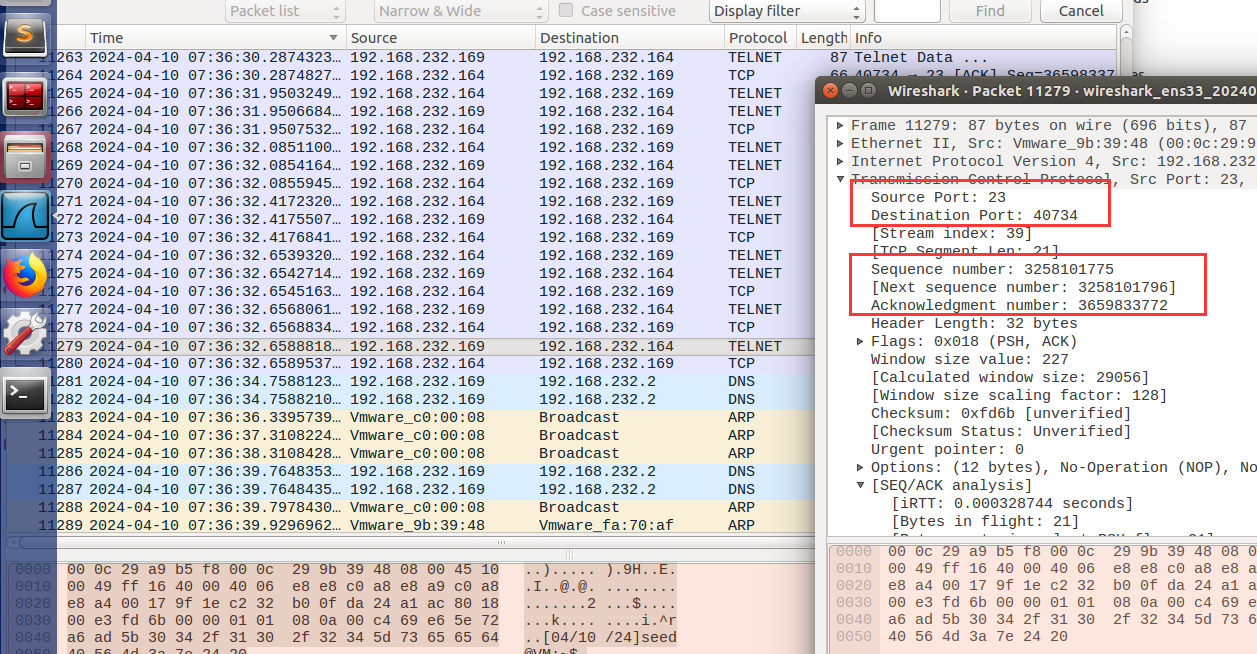


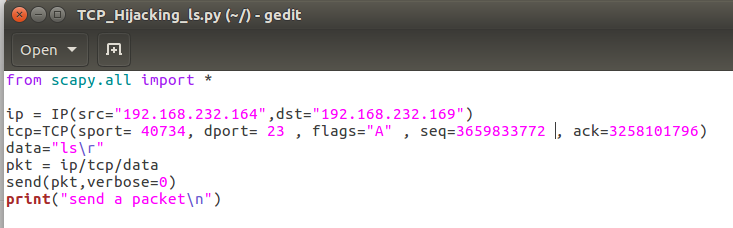


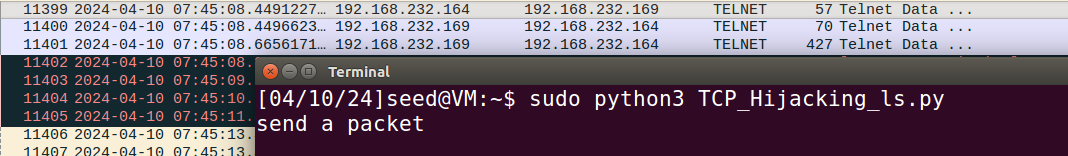
1. 抓包以确认是否执行了ls：

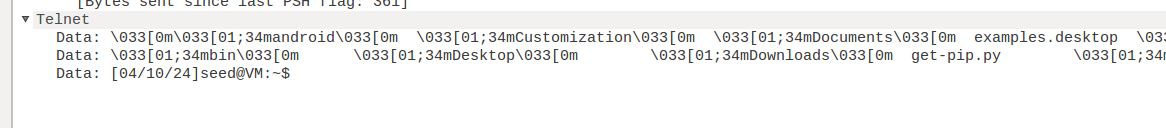


1. 使用scapy编写脚本实现同样功能：

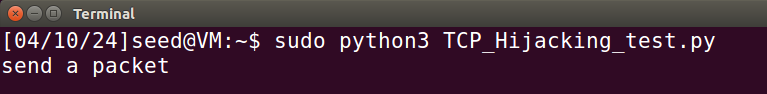


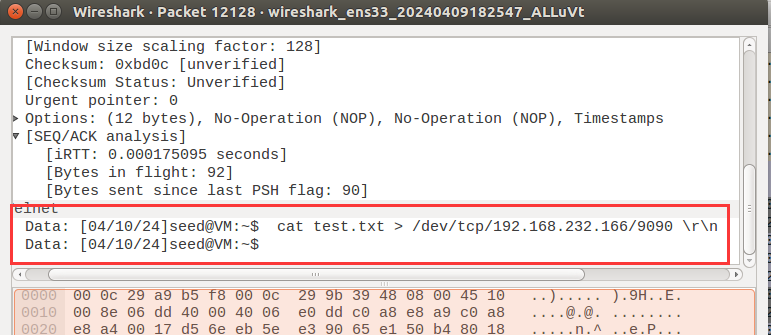


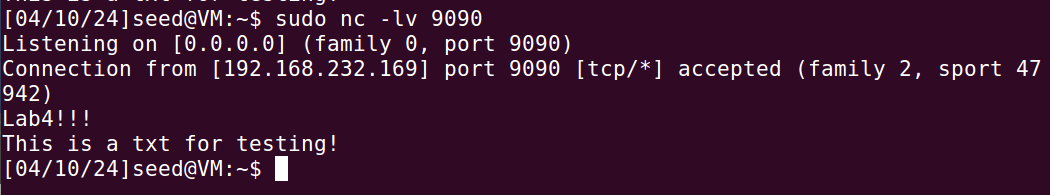




同理，可以获取开始时创建的test.txt文件的内容，只需要变更data。



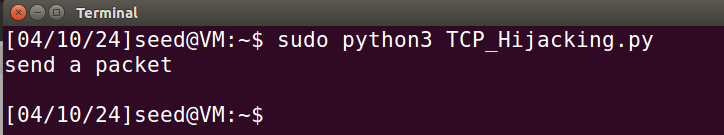




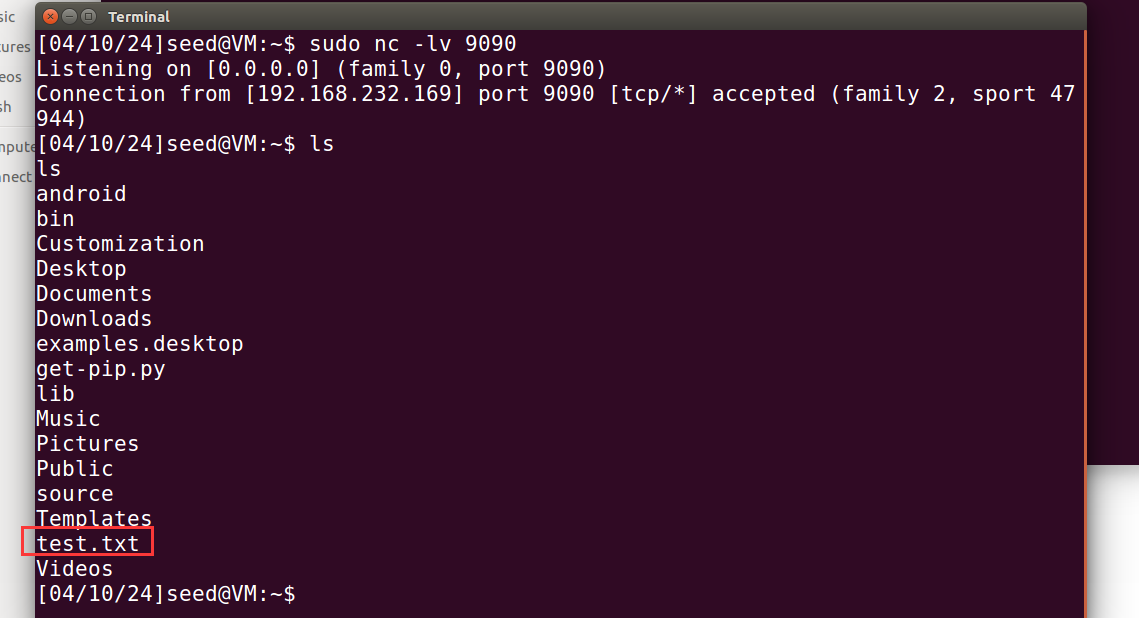
1. 使用scapy编写脚本实现创建反向shell：



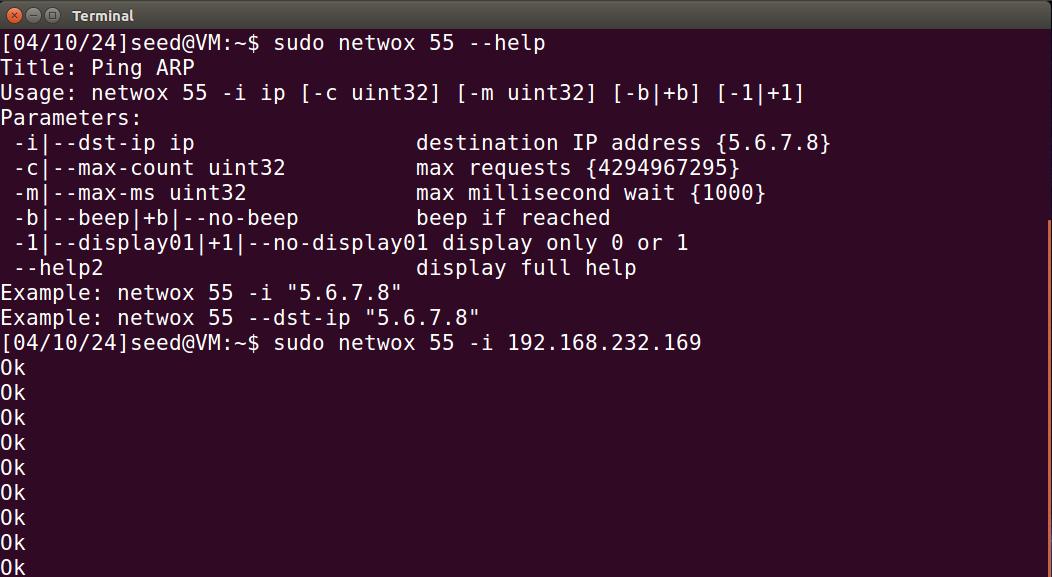
1. 运行scapy脚本：



1. 查看结果，在攻击机上成功创建目标机shell：



1. **ARP扫描—单一主机扫描：**
2. 如果用户想要判断一个主机是否启用，可以使用netwox工具中的55号模块对目标主机进行扫描：



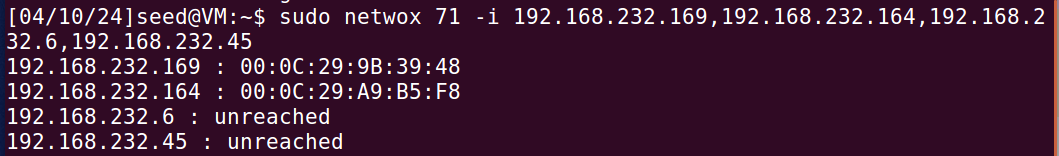
1. 执行后netwox会持续不断向目标主机进行扫描，如果目标主机已启用，则会打印OK，如果目标主机未启用则不会有输出信息：



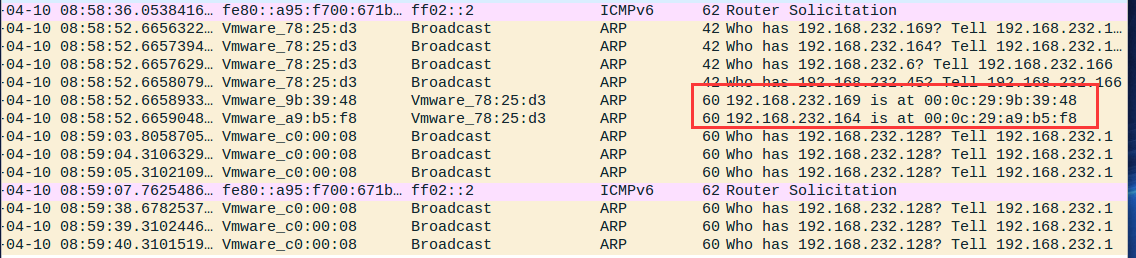
1. 使用wireshark抓包可以发现在不断发送ARP报文：



1. **ARP扫描—多主机扫描：**
2. Netwox工具箱中的71号模块可以实现对多个主机的ARP扫描，如果主机启用，则返回对应的MAC地址，如果主机未启用，则返回unreached：



1. 使用wireshark抓包并观察：



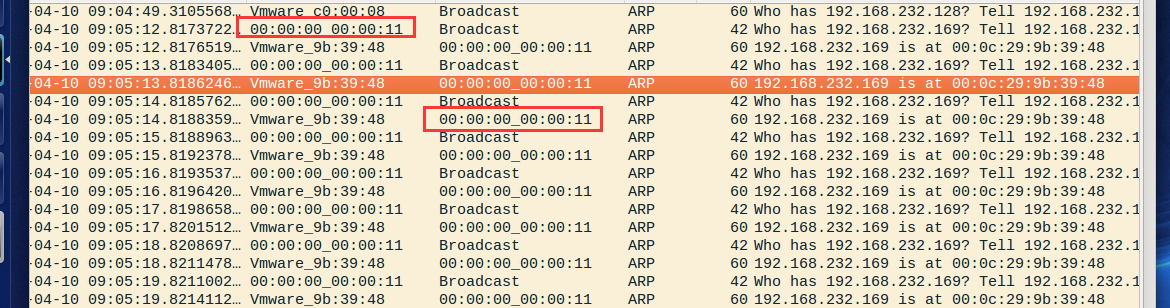
1. **ARP扫描—隐蔽扫描：**

在判断目标主机是否存在的时候，为了避免自身被发现，用户可以使用56号和72号模块来仿造地址信息，这样即使被发现，对方获取的也只是虚假地址。

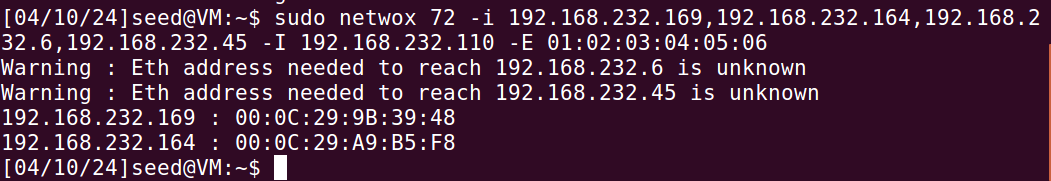
1. 伪造虚假地址，设置IP地址为192.168.232.100，MAC地址为00：00：00：00：00：11，扫描目标主机192.168.232.169是否启用：



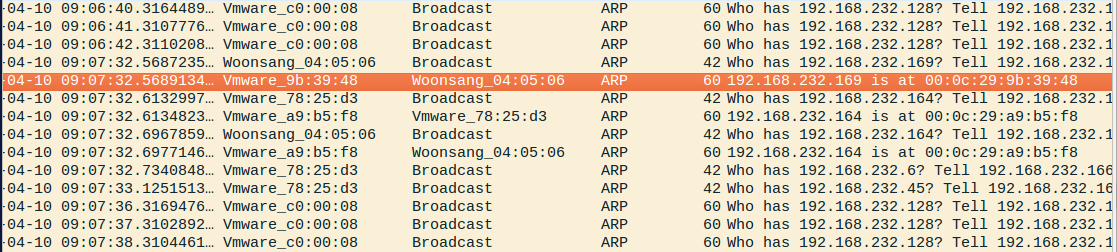
1. 使用wireshark抓包并观察是否伪造了地址：

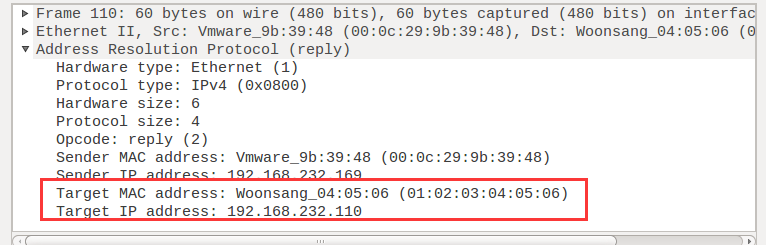


1. 同理，使用72号模块伪造地址信息并对多个主机进行扫描：



1. 使用wireshark抓包并观察请求包和响应包：





1. **实验思考及心得**

通过对TCP洪泛攻击和复位攻击的实施，我对TCP协议的工作机制有了更为深入的理解。尤其是在实施TCP洪泛攻击时，我意识到了协议设计中的某些假设是基于网络环境友好的前提下的，而在恶意攻击的情况下，这些假设可能会成为脆弱点。例如，TCP的三次握手机制在正常情况下是有效的连接建立过程，但在攻击者发起大量伪造SYN包的情况下，服务器资源很快就会被耗尽。而TCP复位攻击展示了攻击者如何通过发送伪造的TCP复位包来中断正常的TCP连接。这种攻击的隐蔽性强，对于未加密的连接尤其有效，说明了加密通信的重要性。

TCP劫持则可以通过注入恶意命令到TCP会话中，使得攻击者能够迫使系统执行未授权的命令。这种攻击手段的成功，突显了会话管理安全性的重要性。ARP扫描是了解网络拓扑和主机在线状态的重要工具，但它也可以被用于执行ARP欺骗等攻击。

通过这次实验，我对Netwox和Scapy这两款强大的网络工具有了更加深入的了解和熟悉。我学会了如何使用这些工具来构造特定的网络攻击场景，如何捕获和分析网络流量，以及如何应对潜在的网络安全威胁。

总的来说，这次实验我不仅实践了多种网络攻击技术，也加深了对网络协议和网络安全基础的理解。通过这样的实践，我不仅学会了如何攻击，更重要的是学会了如何从攻击者的角度思考，从而更有效地防御这些攻击，提高了自己的网络安全防护能力。这次实验也让我明白，网络安全是一个持续的过程，需要我们不断学习和实践，以应对日新月异的网络威胁。未来，我将继续深入学习和研究，为保护网络环境的安全贡献自己的力量。