会话劫持与注入

**一．概念介绍**

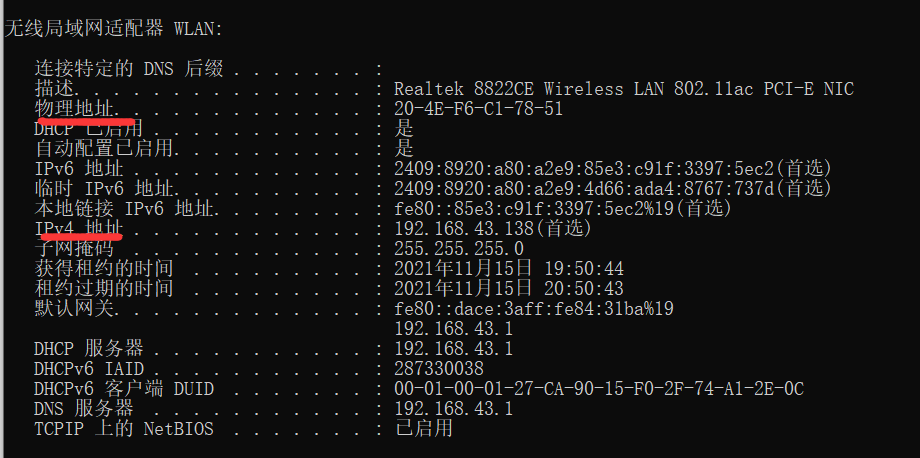
会话劫持：劫持一个现存的会话，利用合法用户进行连接并通过验证，之后顺其自然接管会话。会话劫持有两种方式：积极的攻击方式和消极的攻击方式。

消极的攻击方式中，黑客劫持会话，但是隐藏在后方观察并且记录发送和接收的信息（也就是嗅探，在交换式局域网中扮演一个中间人，接收不属于自己的消息并转发）。

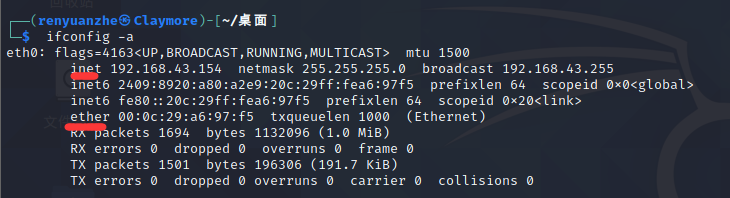
积极的攻击方式中，黑客需要寻找动态的会话并且接管它，这种方式需要使用户下线、不再参与会话。

**二．实验环境**

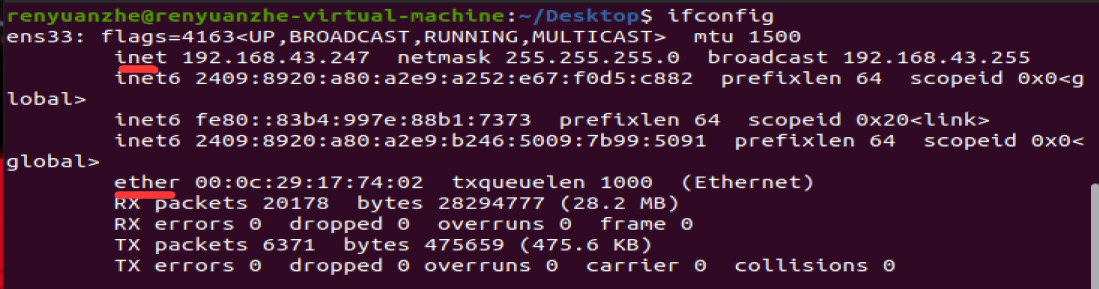
1. 一台物理机，Windows10系统



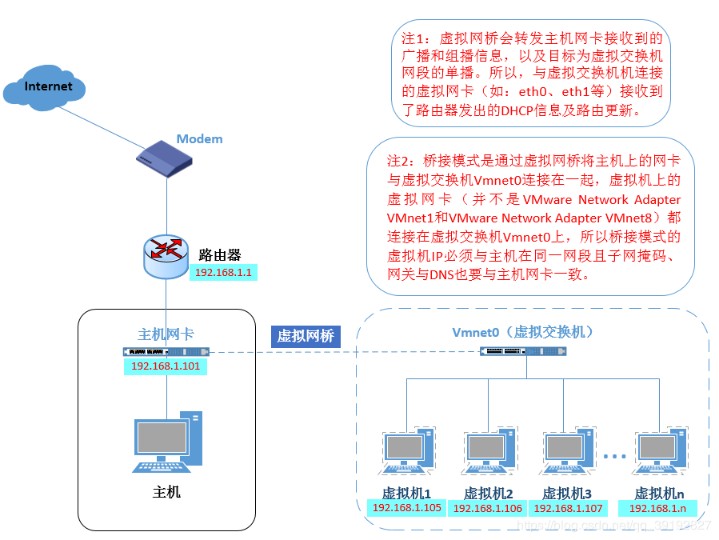
2.虚拟机1号，Kali系统



3.虚拟机2号，Ubuntu系统



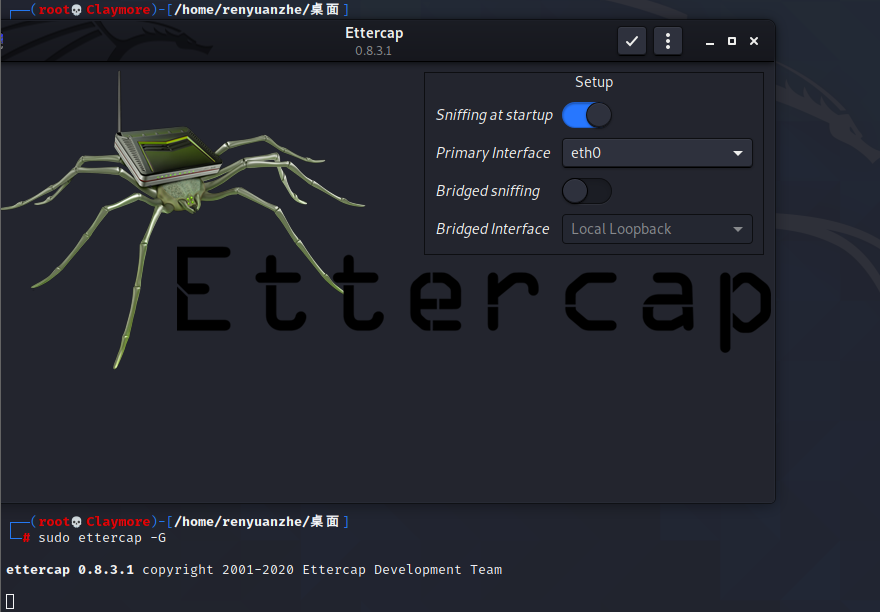
在物理机上采用桥接方式，运行两台虚拟机。桥接模式下的所有虚拟机都是和主机是在同一网段的。需要关闭win10的网络防火墙，否则虚拟机ping不通主机。



**三．消极攻击**

使用ettercap进行嗅探，即在交换式局域网中扮演一个中间人，接收不属于自己的消息并转发。这里仅使用两台虚拟机：用kali嗅探Ubuntu的通信。

1. sudo ettercap –G，在Kali中打开软件。

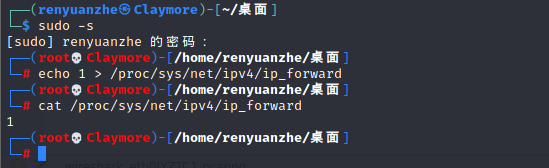


2.echo 1 > /proc/sys/net/ipv4/ip\_forward

开启ip转发，把收到的目的ip不是自己的数据再转发出去。

cat /proc/sys/net/ipv4/ip\_forward

查看ip转发是否开启成功。



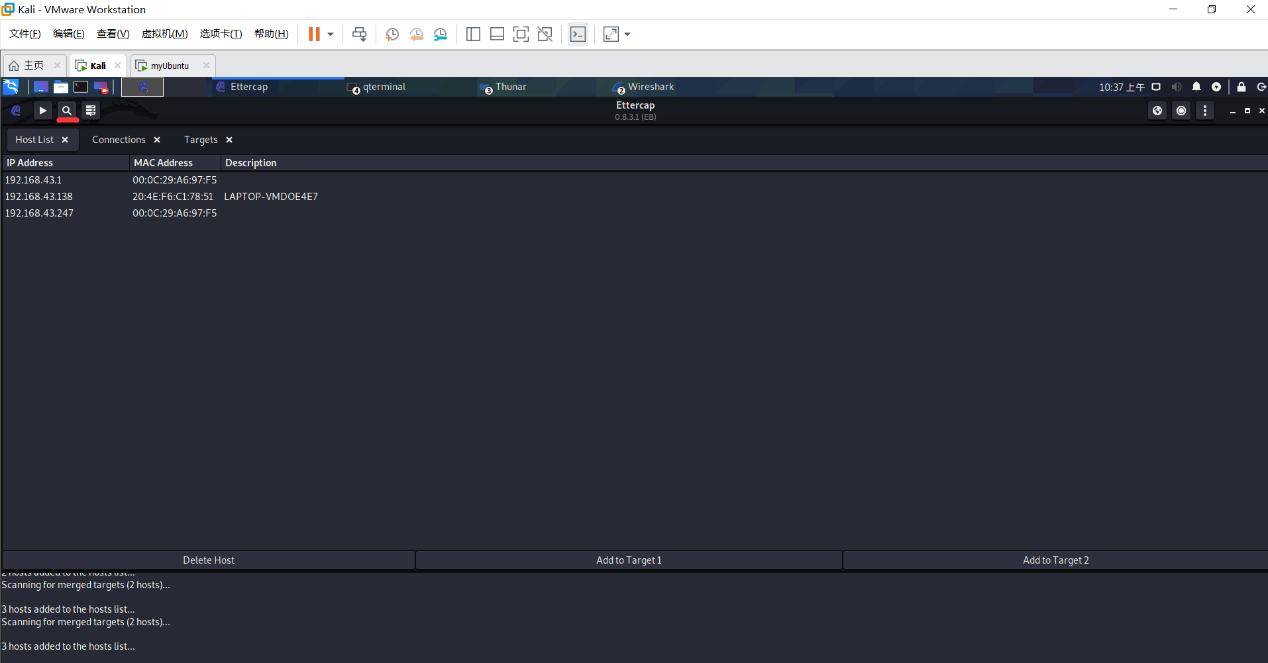
**关于是否要开启ip转发**

通过查阅资料，echo 1 > /proc/sys/net/ipv4/ip\_forward是在Linux系统级别中进行ip转发。

在不开启系统级ip转发的功能的情况下，使用ettercap只进行arp攻击，是不会转发数据的，这样被攻击目标就断网了。必须在同时开启嗅探功能，才会转发截获的数据（这可能是软件层面的）。

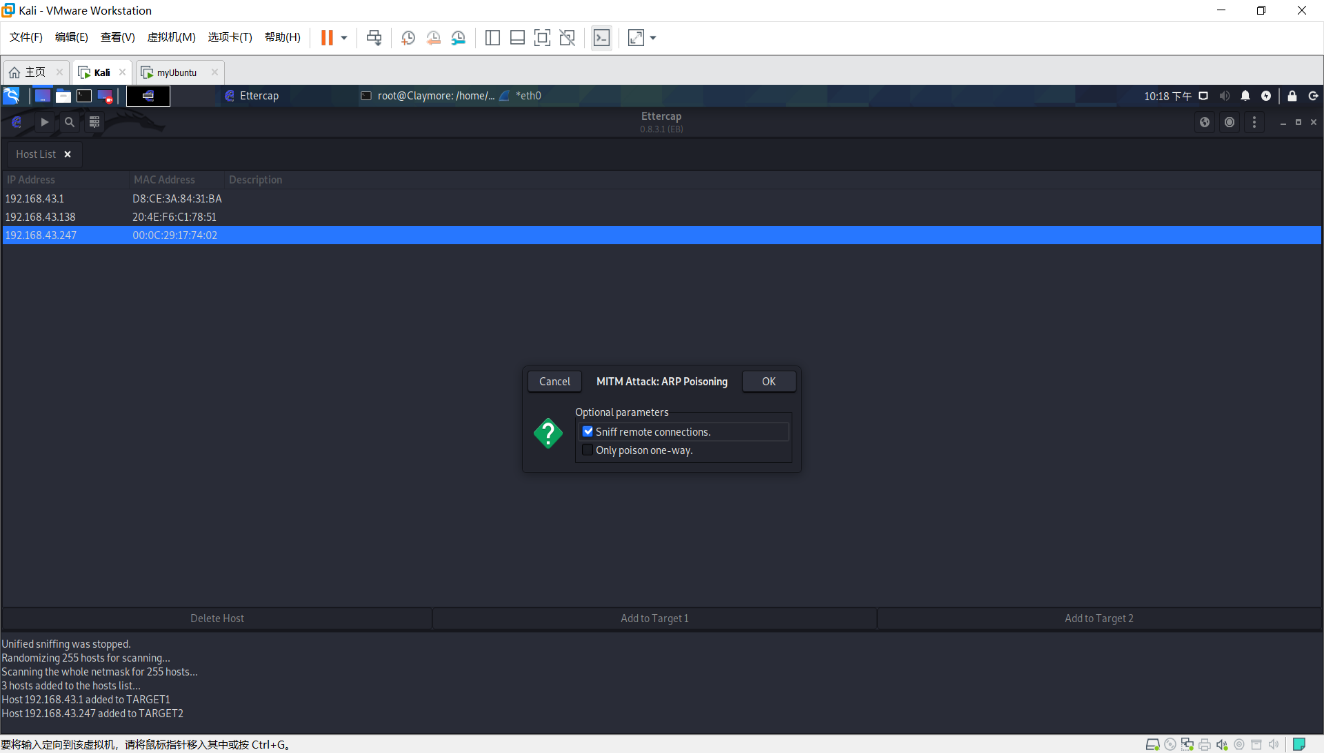
在开启系统ip转发的功能的情况下，无论是嗅探，还是单纯的arp攻击，数据都会被转发。

为了保险起见，我还是开启了系统ip系统转发。

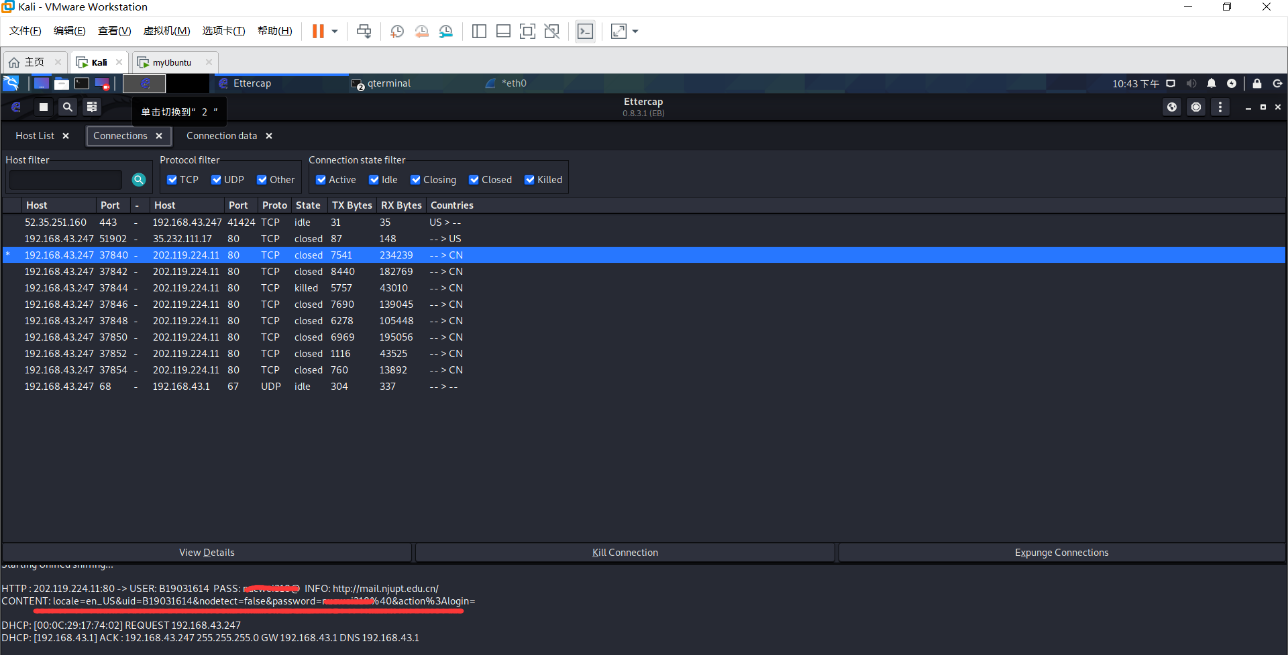
3. 开始扫描局域网内主机

我们在攻击机Kali中成功扫描到虚拟机2号Ubuntu。

将要欺骗的虚拟机2号add to target1，网关add to target2。

4.接下来进行arp毒化的过程了，选择Mitm ---> arp poisoning,选择sniffer remote connections

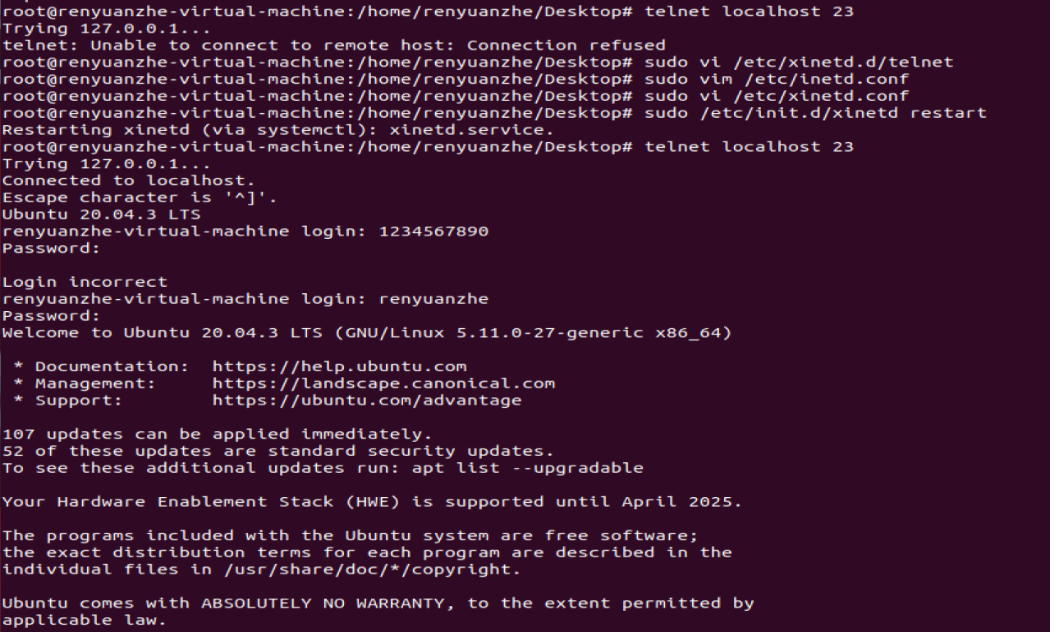
这个时候我们已经开始截获虚拟机2号和网关的通信了

5.用虚拟机2号Ubuntu登陆学校邮箱（特意挑选了不加密的通信）。此时攻击机Kali中， Ettercap(View-Connections)显示如下图所示，Ettercap已经获取了虚拟机2的登陆邮箱的用户名和密码。

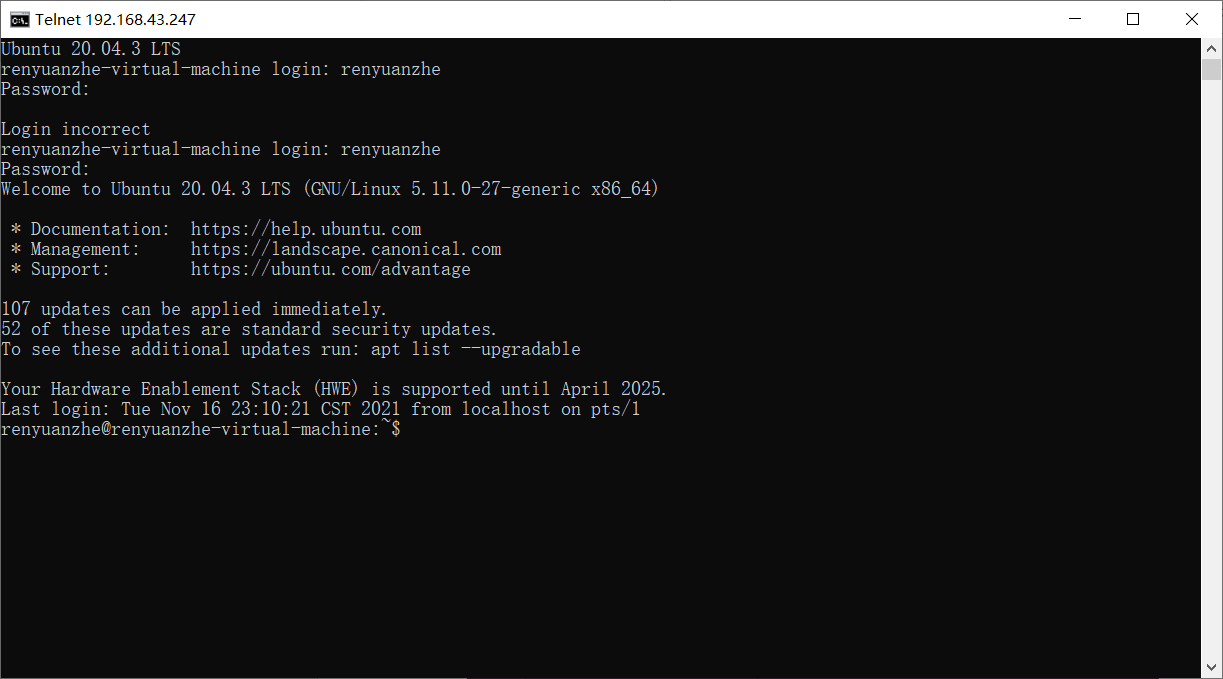
**四．积极攻击**

这里涉及三台主机.

在虚拟机2号Ubuntu上开启telnet服务，作为服务器

 telnet localhost 23

用win10做客户端，使用telnet连接Ubuntu

 telnet 192.168.43.247

Kali作为攻击机，攻击二者的通信

**关于telnet协议**

Telnet协议是TCP/IP协议族中的一员，是Internet远程登录服务的标准协议和主要方式。在终端使用者的电脑上使用telnet程序，用它连接到服务器。终端使用者可以在telnet程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制服务器。要开始一个telnet会话，必须输入用户名和密码来登录服务器。Telnet是常用的远程控制Web服务器的方法。

**telnet和ssh的区别**

Telnet取名自Telecommunications和Networks的联合缩写，这是一种在UNIX平台上最为人所熟知的网络协议。

Telnet使用端口23，它是专门为局域网设计的。

Telnet不是一种安全通信协议，因为它并不使用任何安全机制，通过网络/互联网传输明文格式的数据，包括密码，所以谁都能嗅探数据包。

Telnet中没有使用任何验证策略及数据加密方法，因而带来了巨大的安全威胁，这就是为什么telnet不再用于通过公共网络访问网络设备和服务器。

SSH取名自安全外壳(Secure Shell)，它现在是通过互联网访问网络设备和服务器的唯一的主要协议。

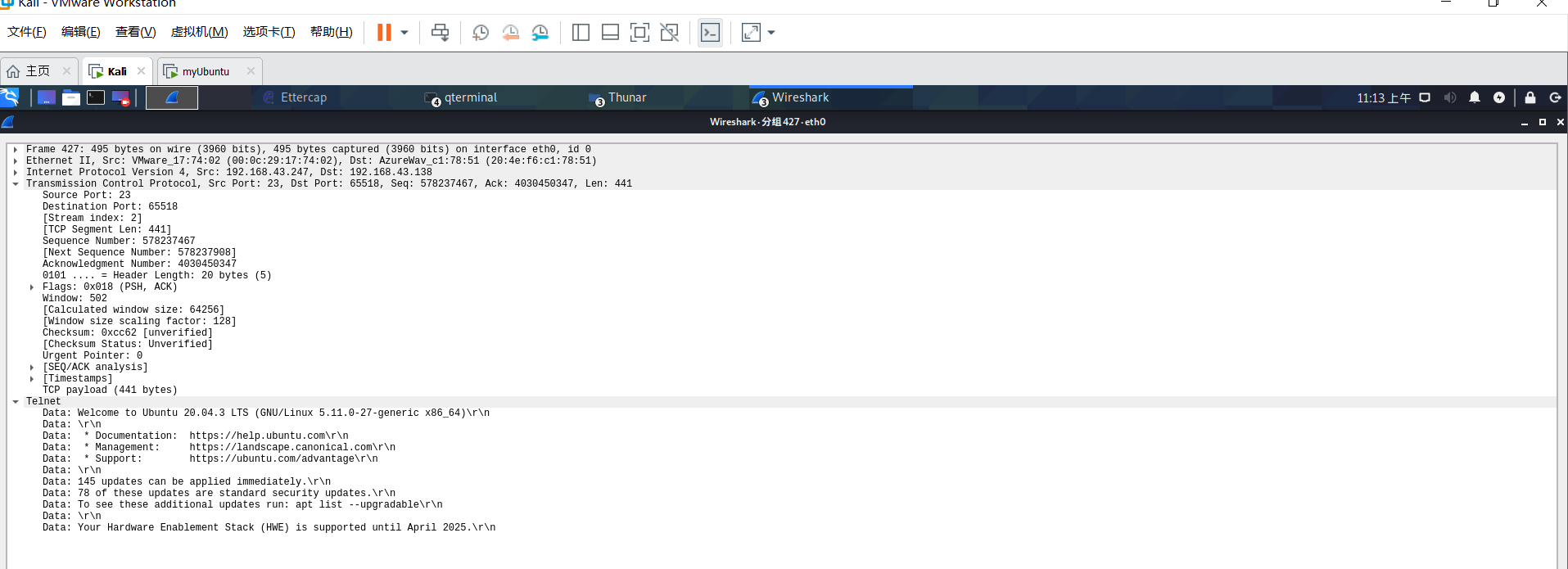
SSH默认情况下通过端口22运行，该端口号可以更改。

SSH是一种非常安全的协议，因为它共享并发送经过加密的信息，从而为通过互联网等不安全的网络访问的数据提供了机密性和安全性。

一旦通讯的数据使用SSH经过加密，就极难解压和读取该数据，所以我们的密码在公共网络上传输也变得很安全。

SSH还使用公钥用于对访问服务器的用户验证身份，这是一种很好的做法，为我们提供了极高的安全性。

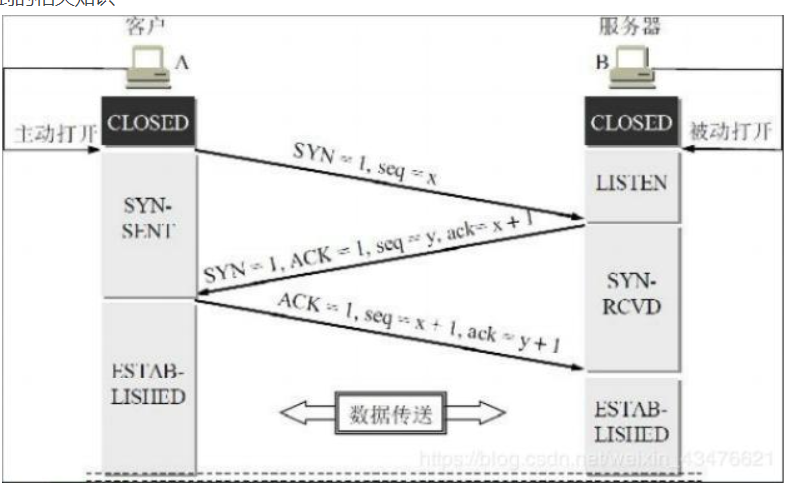
SSH 几乎在所有场合代替了Telnet。

使用wireshark，观察telnet包，可以发现全是明文，这也是我选择telnet的原因

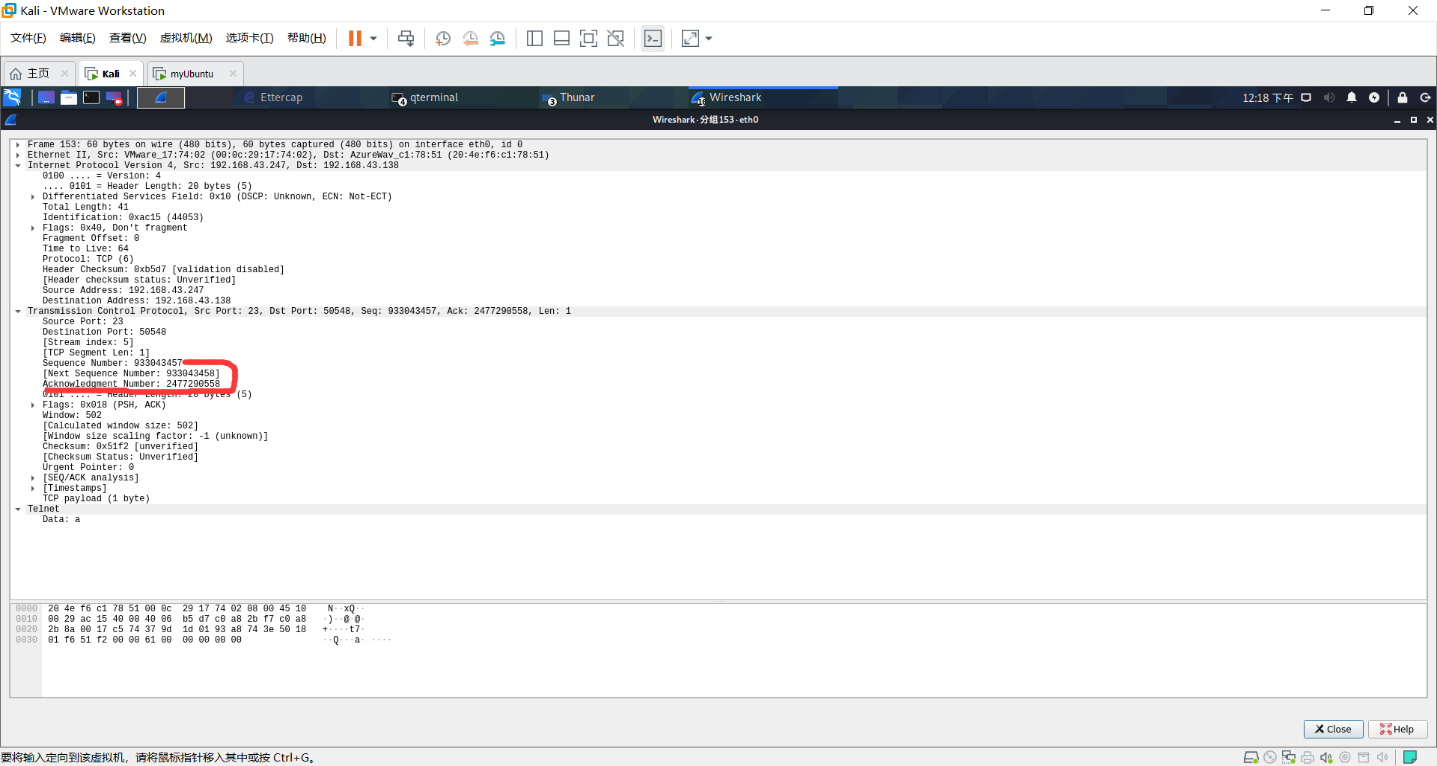
**实验原理与步骤如下：**

1.客户端win10和服务器Ubuntu建立telnet连接

2.攻击者要伪造客户端发下一个包，必须采用服务器回传最后一个包的nextseq 作为下一个包的 ack ，采用服务器回传最后一个包的 ack 作为下一个包的 seq（这里是 tcp 协议的规定的）

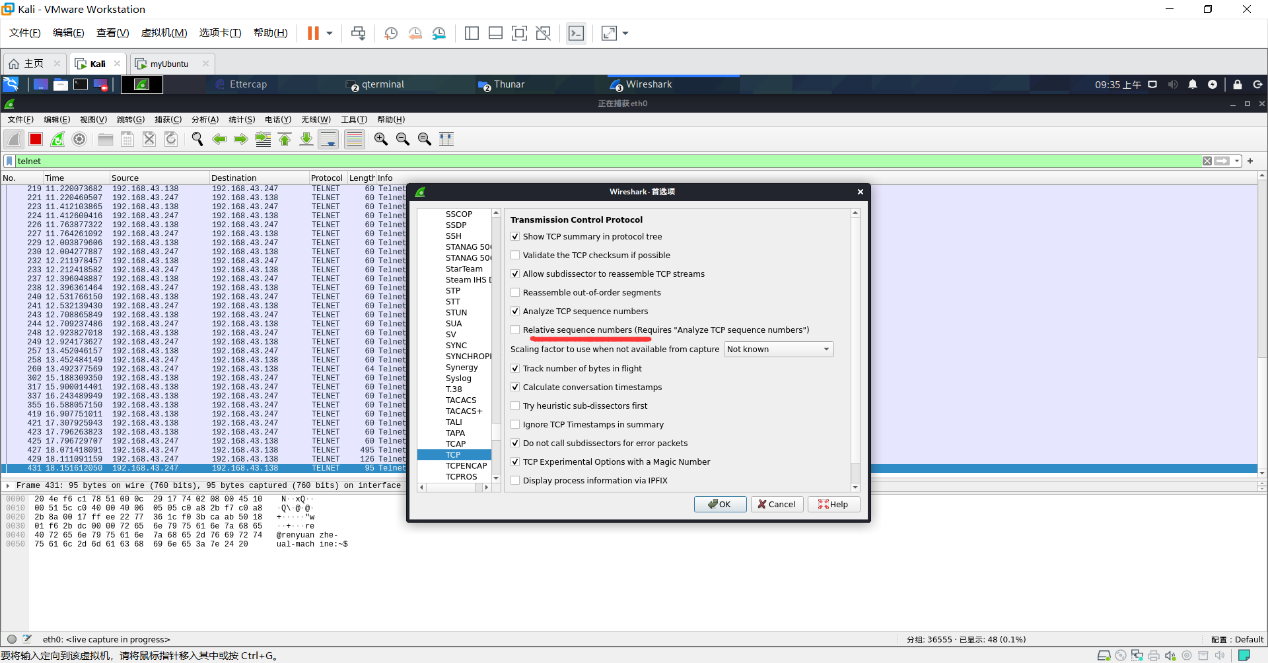


攻击者可使用netwox工具伪造客户端给服务器 发一个 tcp 包。发送成功后，原来的客户端就会失去连接，同时服务器会攻击者当作客户端，这样攻击者就实现了会话劫持。

3. 用物理机给服务器发送一个a字符,这是服务器应答的包

一些重要参数已标出，下面我们要根据这些参数构造攻击者的包。

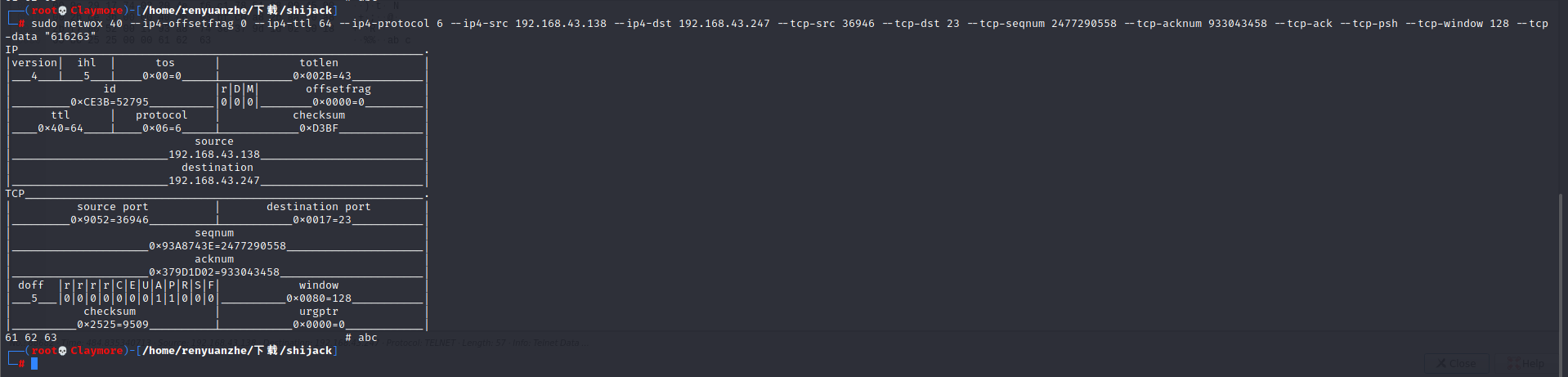
**Tips：**如果wireshark显示的Next seq值为relative如下图，在协议首选项，将Relative sequence numbers 前的勾去掉

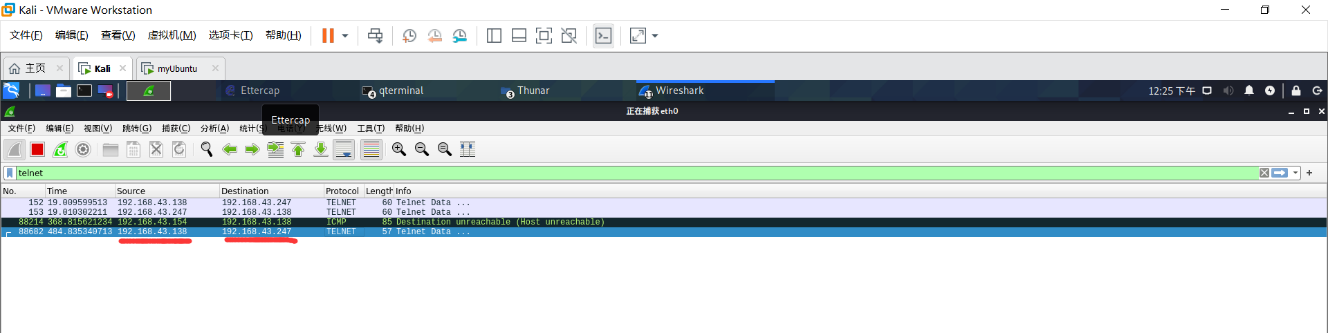
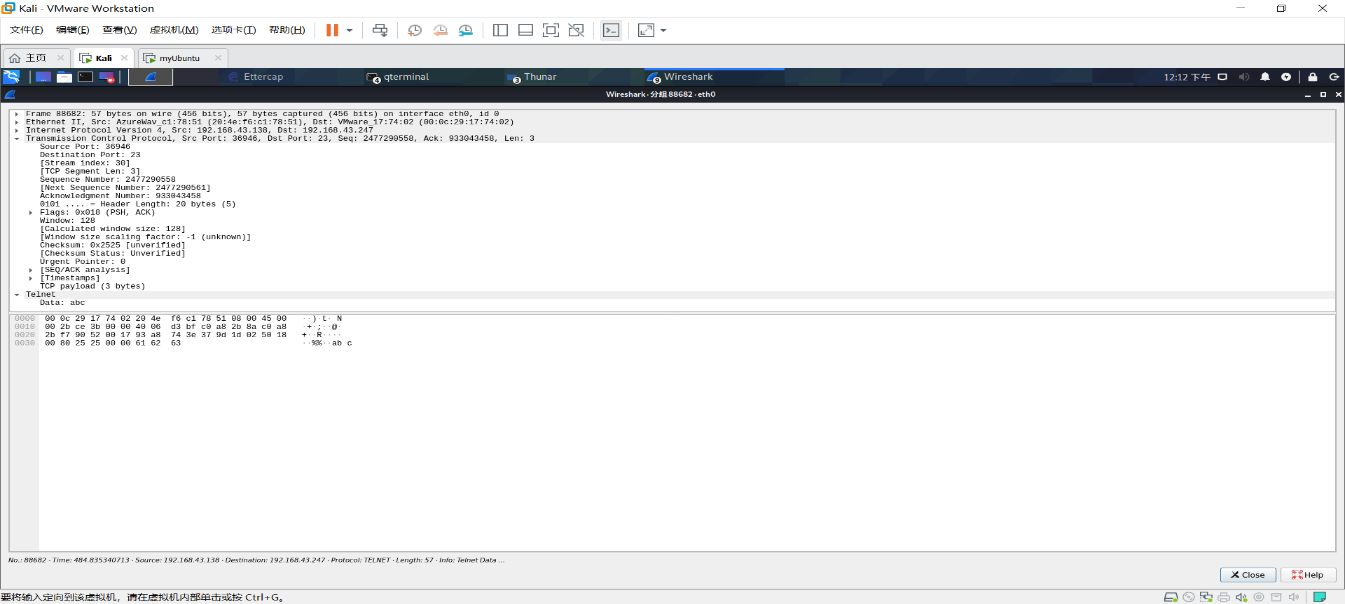


4. 在kali中使用netwox，手动构造攻击数据包并发送给服务器

sudo netwox 40 --ip4-offsetfrag 0 --ip4-ttl 64 --ip4-protocol 6 --ip4-src 192.168.43.138 --ip4-dst 192.168.43.247 --tcp-src 36946 --tcp-dst 23 --tcp-seqnum 2477290558 --tcp-acknum 933043458 --tcp-ack --tcp-psh --tcp-window 128 --tcp-data "616263"

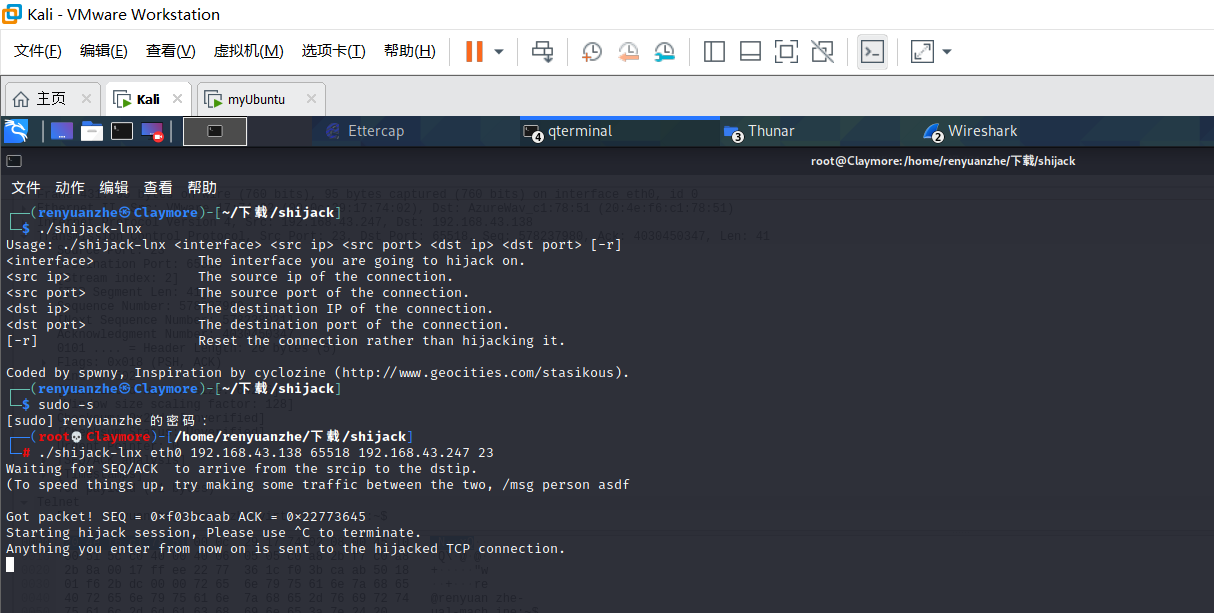
其中192.168.43.138为客户机IP ，192.168.43.247为服务器IP ，36946为客户端的端口号， seqnum为上图中的Ack的值，acknum为上图中Next seq的值 ，616263为abc的16进制表示，data中也可以发送其他数据。



5.使用Wireshark，观察网络中的通信。发现用Kali伪造的数据包发送成功。

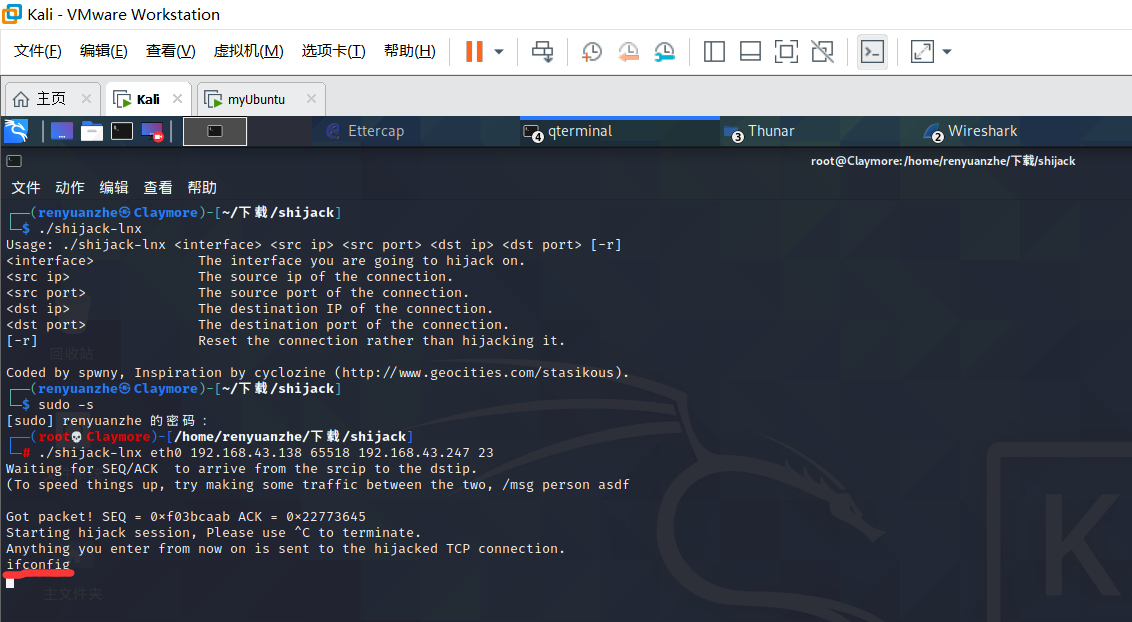
**补充1：**通过查阅资料，发现使用shijack工具可以更轻松地进行劫持

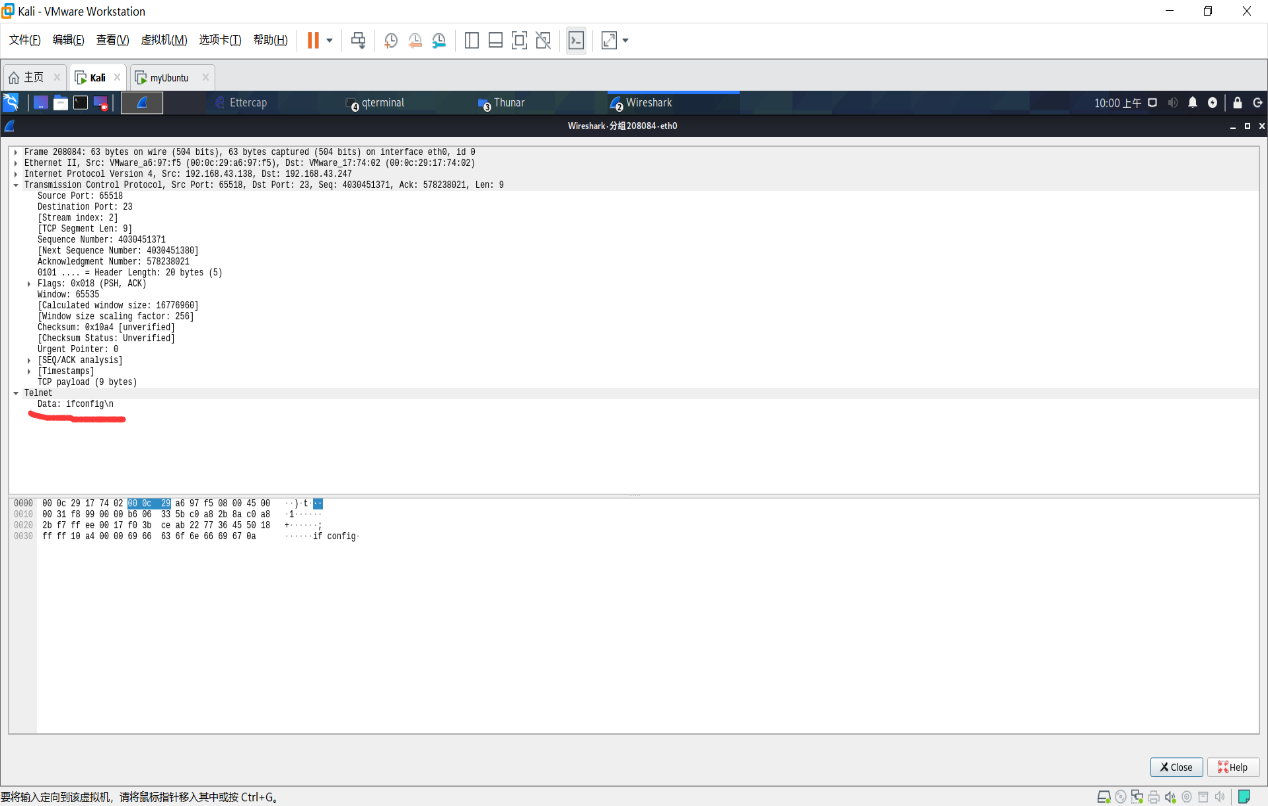
1. ./shijack-lnx eth0 192.168.43.138 65518 192.168.43.247 23

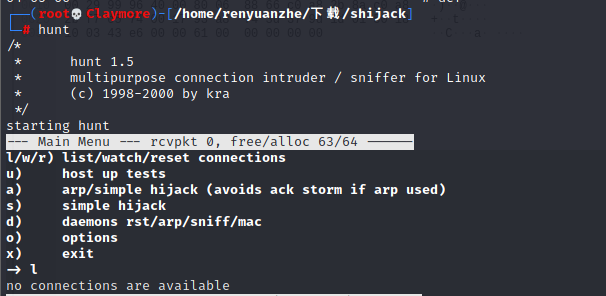
参数依次为网卡名，源地址，源端口，目的地址，telnet 端口

2.此时物理机和Ubuntu的连接已经断了，在物理机cmd窗口输入任何操控ubuntu的命令都不会起作用

取而代之的，是kali 的shijack接管了对Ubuntu的控制

3.在shijack中输入ifconfig，用 wireshark 验证是不是真的成功发出伪造包



**补充2：**通过查阅资料，使用hunt工具也可以进行劫持

但我kali上的hunt检测不到客户端win10和服务器Ubuntu的连接，可能是因为防火墙的缘故。

**五．会话劫持的防范**

加密通信内容，利用数字证书等方式验证通信对象等。