网络安全线上实验

学　　院：信息科学与工程学院

专业班级：信息安全 1401 班

指导老师：王伟平

学　　号：0906140126

姓　　名：王珊珊

目录

实验二 数据包嗅探和欺骗实验

一、实验名称

数据包嗅探和欺骗实验

二、实验目的

数据包嗅探和欺骗是网络安全最重要的两个概念；它们是网络通信中两个主要的威胁。对于了解网络的安全措施，能够理解这两个威胁是必不可少的。有许多数据包嗅探和欺骗工具，如 wireshark ,tcpdump,netwox 等，其中一些工具被安全专家以及攻击者广泛地使用。能够使用这些工具对于学生来说是很重要的，但对于学网络安全课程的学生更重要的是了解这些工具是如何工作的，即包嗅探和欺骗是如何在软件中实现的。

本实验的目的是让学生掌握最基本的嗅探和欺骗工具的技术。学生要使用一些简单的嗅探和欺骗程序，阅读源代码，并进行修改，最终可以对这些项目的技术方面有更加深入的了解。这个实验结束，学生应该能够写出自己的嗅探和欺骗程序。

三、实验任务

3.1 任务一：写数据包监听程序

嗅探程序通过使用 pcap 库可以很容易地进行编写。利用 PCAP，嗅探器的任务变得在 pcap 库调用一系列简单的程序。在序列结束时，数据包将被放置在缓冲区中，一旦它们被捕获，就进行进一步处理。所有的数据包捕获的细节由 pcap 库处理。Tim Carstens 写了一个如何使用 pcap 库编写嗅探程序的教程。本教程是在 http://www.tcpdump.org/pcap.htm。

3.1.a 了解嗅探训练

请从上述教程中下载 sniffex.c 程序，编译并运行它。你应该提供截图证据表明你的程序成功运行并产生预期的结果。

运行结果如图 1、2 所示

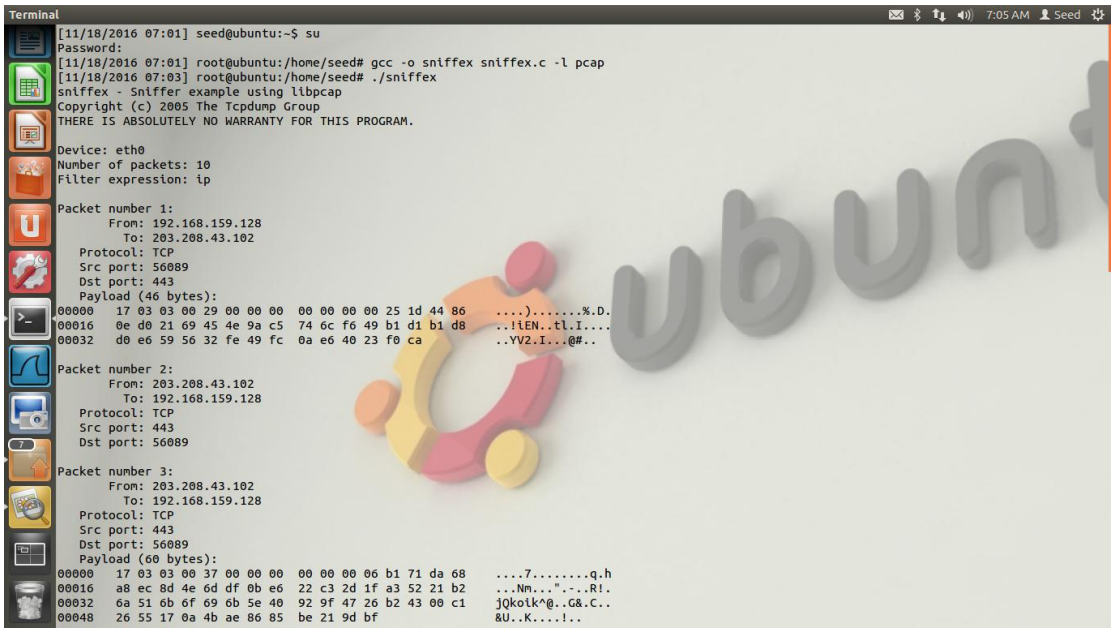

图 1 sniffex.c 运行结果图

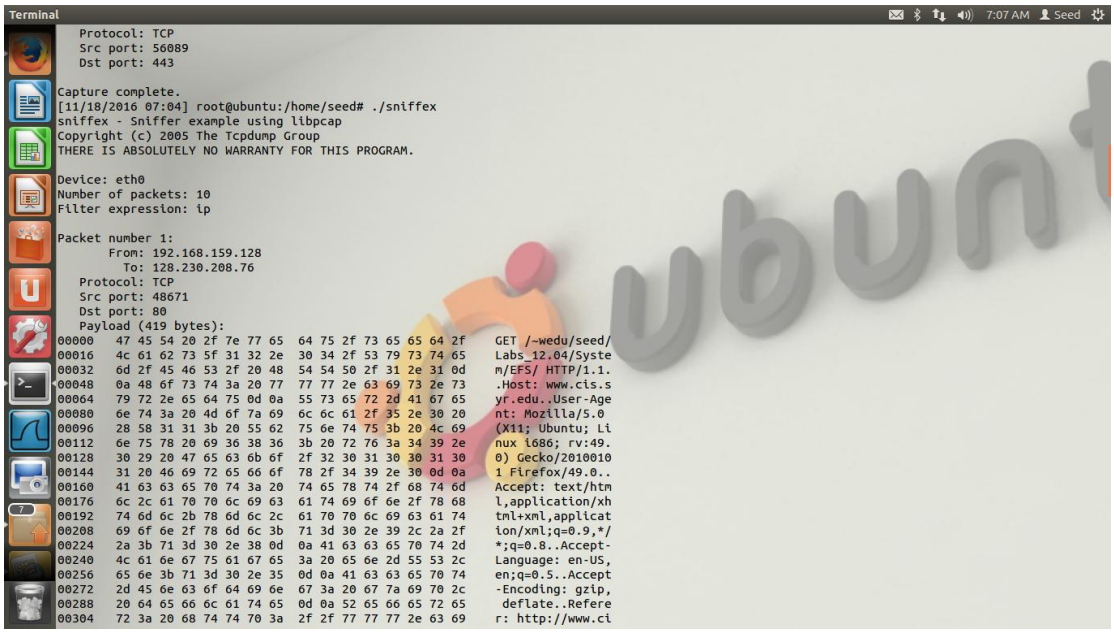

图 2　sniffex.c 运行结果图

1.请用自己的话来描述，嗅探程序是必要的库调用序列。这是一个总结，而不是像教程中的一个详细的解释。

2.为什么你需要 root 权限运行嗅探训练？如果没有根特权执行程序，程序错误的地方在哪？

普通的情况下，网卡只接收和自己的地址有关的信息包，即传输到本地主机的信息包。要使 Sniffer 能接收并处理这种方式的信息，系统需要支持 BPF，Linux 下需要支持 SOCKET-PACKET。但一般情况下，网络硬件和 TCP/IP 堆栈不支持接收或者发送与本地计算机无关的数据包，所以，为了绕过标准的 TCP/IP 堆栈，网卡就必须设置为混杂模式。一般情况下，要激活这种方式，内核必须支持这种伪设备 BPFilter，而且需要 root 权限来运行这种程序，所以 Sniffer 需要 root 身份安装，如果只是以本地用户的身份进入了系统，那么不可能嗅探到 root 的密码，因为不能运行 Sniffer。

3.请打开和关闭的嗅探程序混杂模式。你能证明这种模式在打开和关闭时的区别吗？请描述你如何证明。打开和关闭混杂模式的运行结果如下图所示。

混杂模式（Promiscuous Mode）是指一台机器能够接收所有经过它的数据流，而不论其目的地址是否是他。是相对于通常模式（又称“非混杂模式”）而言的。这两种方式区别很大。一般来说，非混杂模式的嗅探器中，主机仅嗅探那些跟它直接有关的通信，如发向它的，从它发出的，或经它路由的等都会被嗅探器捕捉。而在混杂模式中则嗅探传输线路上的所有通信。在非交换式网络中，这将是整个网络的通信。这样做最明显的优点就是使更多的包被嗅探到，它们因你嗅探网络的原因或者对你有帮助，或者没有。但是，混杂模式是可被探测到的。一个主机可以通过高强度的测试判定另一台主机是否正在进行混杂模式的嗅探。其次，它仅在非交换式的网络环境中有效工作（如集线器，或者交换中的 ARP 层面）。再次，在高负荷的网络中，主机的系统资源将消耗的非常严重。

Linux 下通过 ifconfig eth0 promisc 将 eth0 设置成混杂模式，通过 ifconfig eth0 -promisc 取消混杂。

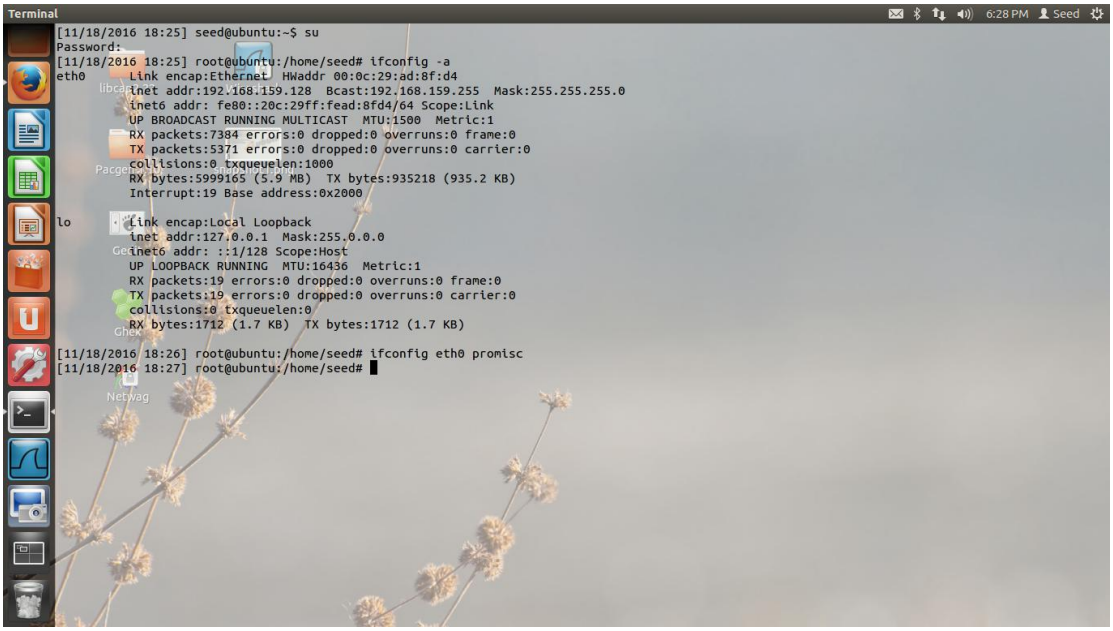

图 3 混杂模式设置图

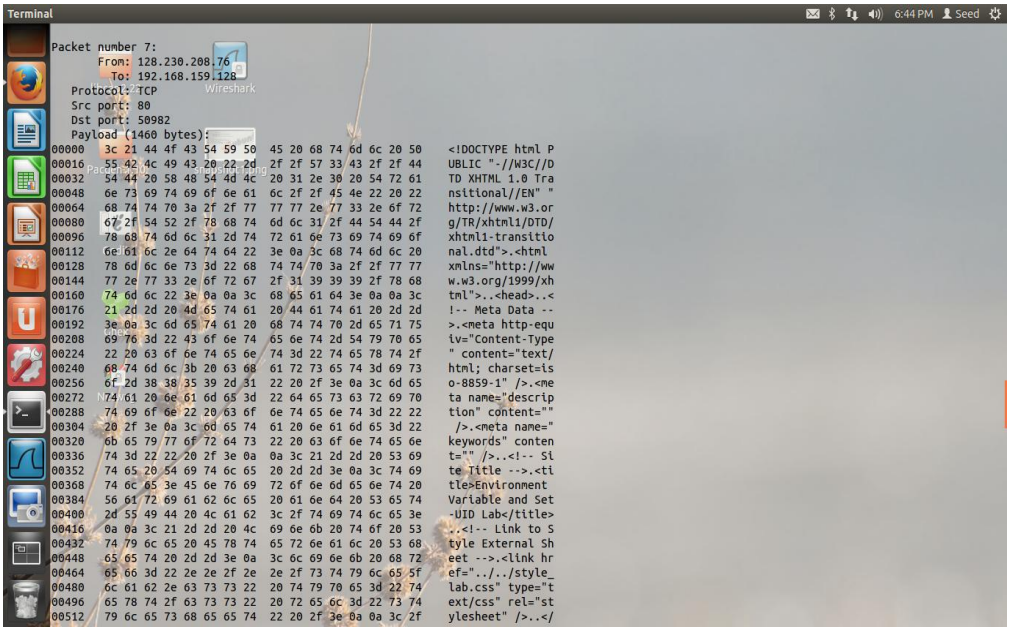

图 4 混杂模式下嗅探结果图

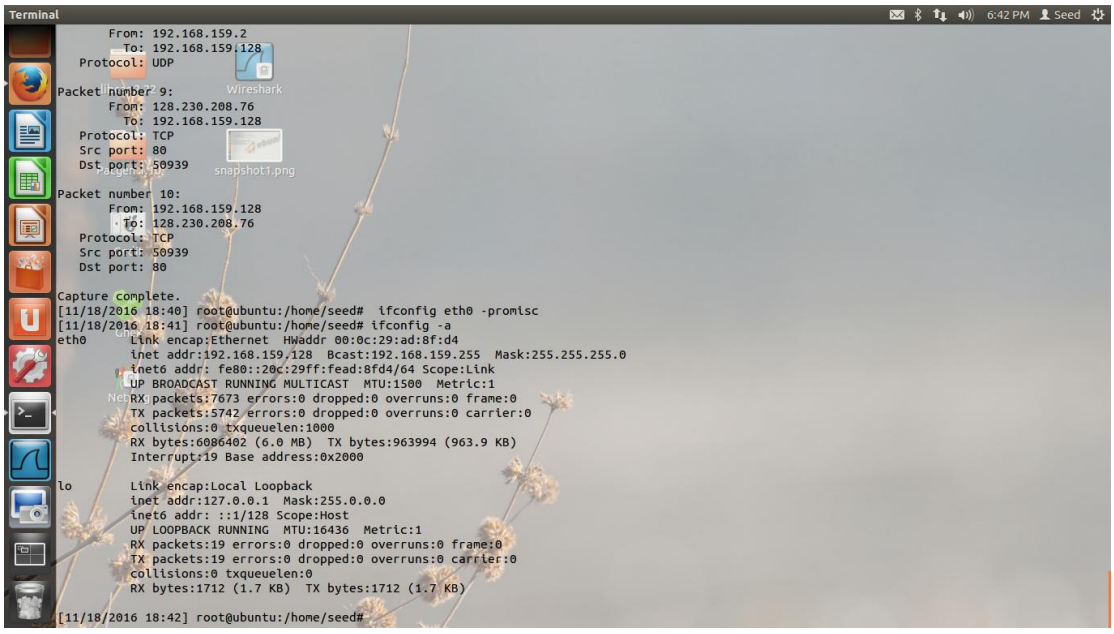

图 5 混杂模式关闭图

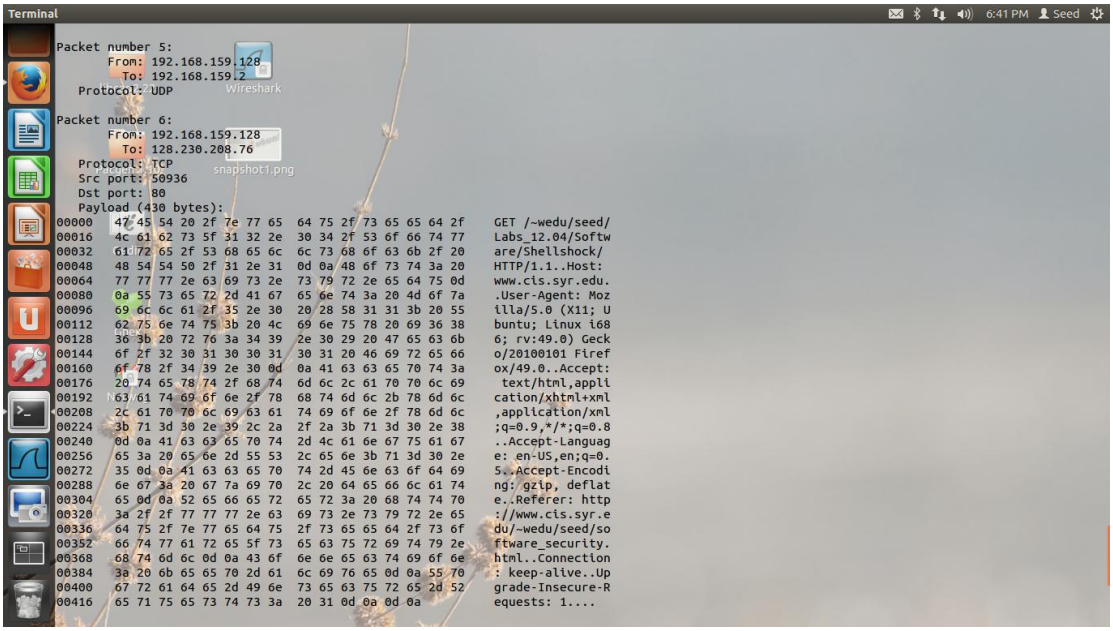

图 6 非混杂模式下嗅探结果图

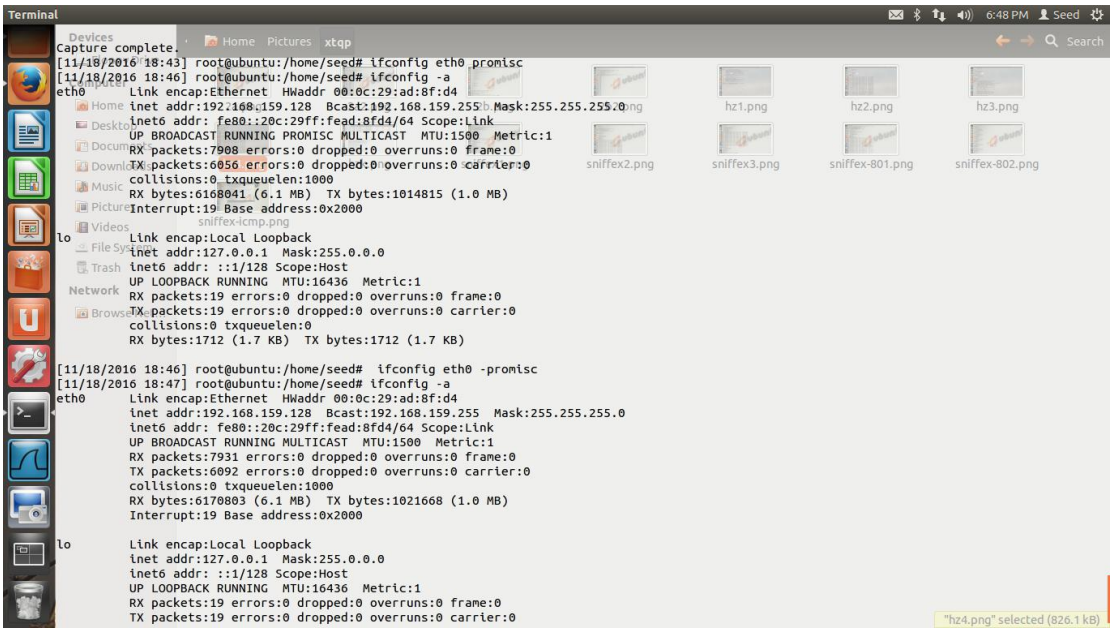

图 7 两种模式对比图

3.1.b 写过滤器

为嗅探程序写过滤表达式用来捕捉以下规定的数据包，在报告中，需要运行结果截图来展示每一个过滤表达式的运行结果。运行结果如下图所示。

1.捕捉两个特定主机间的 ICMP 包：如图 8 所示，捕捉的是端口 192.168.159.128 和端口 128.230.208.76

2.捕捉目的端口范围为 10-100 的 TCP 包：如图 9、10 所示，捕捉的是目的

端口为 80 端口，或初始端口为 80 端口的 TCP 包。

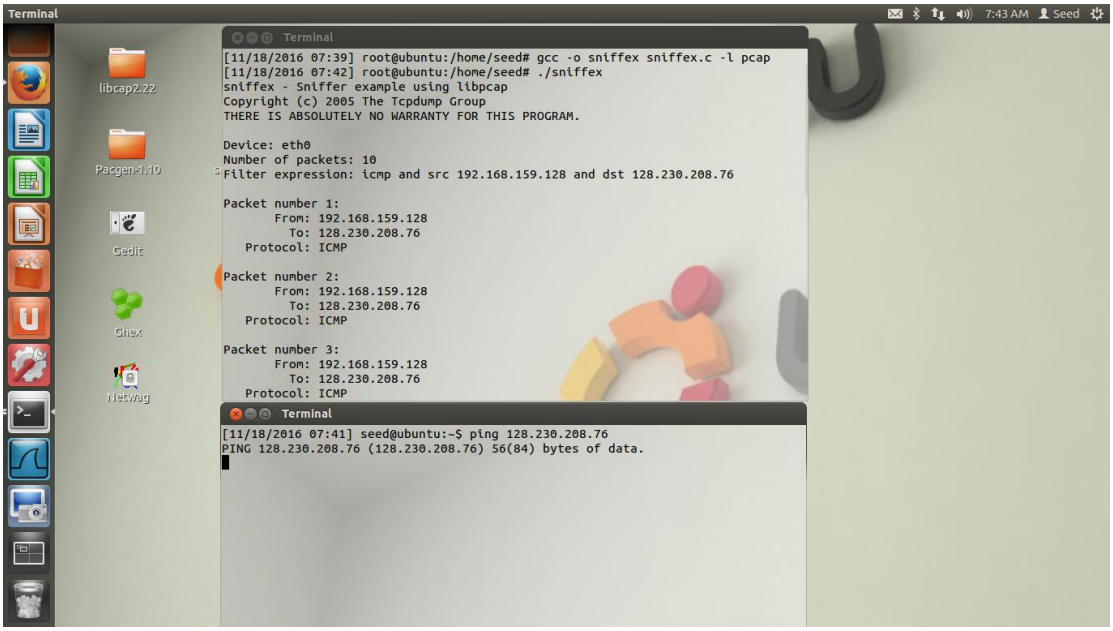

图 8　ICMP 包捕捉示意图

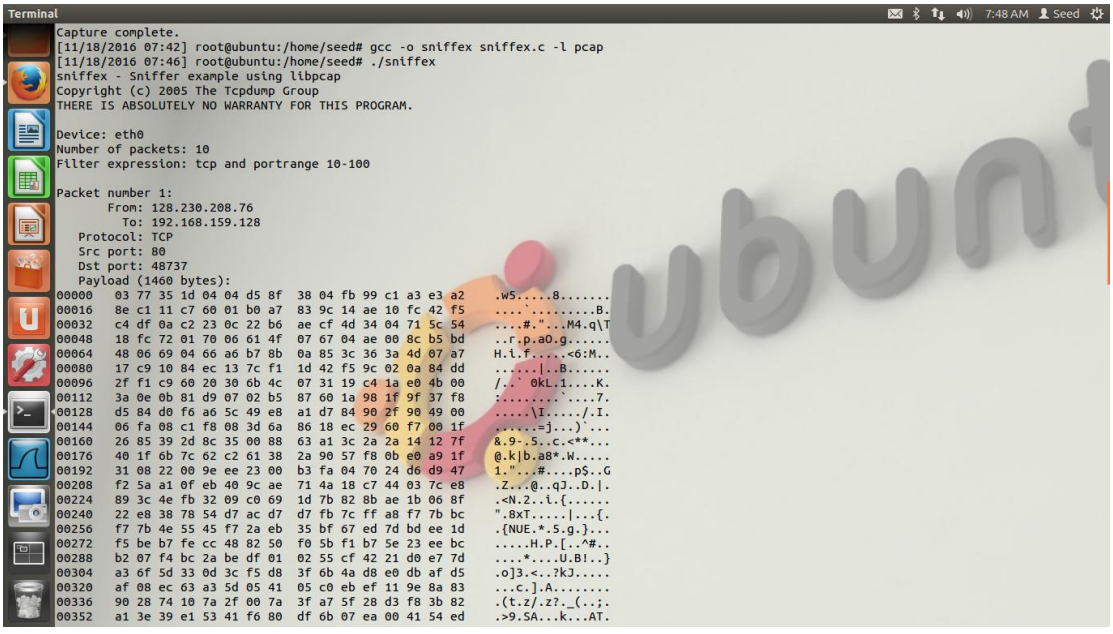

图 9 TCP 捕捉示意图

图 10 TCP 捕捉示意图

3.2 任务二：欺骗

当一个普通用户发送数据包时，操作系统通常不允许用户设置协议头组的所有领域（如 TCP，UDP，和 IP 报头）。操作系统将设置大部分的领域，而只允许用户设置几个字段，如目标 IP 地址、目标端口号等。

然而，如果用户有根权限，他们可以设置分组报头的任意字段，这就是包欺骗，可以采用原始套接字来实现。

原始套接字给程序员构建数据包的绝对控制权，允许程序员构建任何任意的数据包，包括设置头字段和有效载荷。使用原始套接字是很简单的，它包括四个步骤：（1）创建一个原始套接字，（2）设置套接字选项，（3）构造数据包，（4）通过原始套接字发送数据包。有许多在线教程，可以教你如何使用原始套接字。我们已经把一些教程与实验室的网页联系起来了。

请阅读它们，并学习如何写一个 spoonfing 程序。我们展示了一个简单的骨架如下所示。

3.2.a 写一个欺骗程序

你可以自己写一个的包程序或者下载一个程序。你需要提供的证据（例如，Wireshark 数据包跟踪）向我们展示你的程序成功地发送了伪造的 IP 数据包，运行结果如图 11.12 所示，伪造了源 ip 为 192.168.10.10 的数据包。

图 11 伪造 ip 数据包结果图

图 12 伪造 ip 数据包结果图

3.2.b ICMP 回送请求欺骗

欺骗 ICMP 回送请求包代表另一台机器（使用另一台机器上的 IP 地址作为其源 IP 地址），这个包应该被发送到网络上一台远程的机器，你应该打开 Wireshark，因此如果你的欺骗是成功的，你可以看到来自远程机的返回应答。如图 13.14 所示。

图 13 ICMP 回送请求欺骗图

图 14 ICMP 回送请求欺骗图

1.你可以设置 IP 数据包长度字段的任意值，而不管实际的包有多大吗？可以

2.使用原始套接字编程，必须计算 IP 报头的校验和吗？必须

3.为什么你需要根权限来运行使用原始套接字的程序？

需要，原始套接字运用了底层的访问。

四、实验总结

通过此次实验，我对包嗅探和欺骗实验的原理和过程有了进一步的理解和认识。嗅探 sniff。嗅探器可以窃听网络上流经的数据包。用集线器 hub 组建的网络是基于共享的原理的，局域网内所有的计算机都接收相同的数据包，而网卡构造了硬件的“过滤器“通过识别 MAC 地址过滤掉和自己无关的信息，嗅探程序只需关闭这个过滤器，将网卡设置为“混杂模式“就可以进行嗅探。用交换机 switch 组建的网络是基于“交换“原理的，交换机不是把数据包发到所有的端口上，而是发到目的网卡所在的端口，这样嗅探起来会麻烦一些，嗅探程序一般利用“ARP 欺骗“的方法，通过改变 MAC 地址等手段，欺骗交换机将数据包发给自己，嗅探分析完毕再转发出去。而包欺骗则是利用套接字来伪造数据，例如 ip 地址等。在这次实验中，拓展了我的知识面，学习到了许多新的知识和理论，对我的实践操作能力也是一次锻炼和提升，在日常的学习中，应该多多尝试体验这样的线上学习来提升自己。通过此次实验，将实践和理论知识相结合，进一步巩固了我们在课堂上学到的知识，印象更加深刻。