第 5 章　Kali Linux 渗透测试实验

5.1　Wireshark 简介

5.1.1　Wireshark 的特点

Wireshark 是一个网络封包分析软件。网络封包分析软件的功能是捕获网络封包，并尽可能显示出详细的网络封包信息。作为目前世界上最受欢迎的协议分析软件，Wireshark 可将捕获的各种协议的网络二进制数据流翻译为人们容易读懂和理解的文字和图表等形式，极大地方便了对网络活动的监测分析和教学实验。它有十分丰富和强大的统计分析功能，可在 Windows、Linux 和 UNIX 等系统上运行。Wireshark 于 1998 年由美国 GeraldCombs 开发，原名 Ethereal，2006 年 5 月改为 Wireshark。目前世界各国有 100 多位网络专家和软件人员共同参与此软件的升级、完善和维护。它大约每两三个月推出一个新的版本，目前的最新版本号为 3.4.1。它是一个开源代码的免费软件，任何人都可自由下载，也可参与共同开发。

Wireshark 可以十分方便、直观地应用于计算机网络原理和网络安全教学实验、网络日常安全监测、网络性能参数测试、网络恶意代码捕获和分析、网络用户行为监测、黑客活动追踪等。因此它在世界范围的网络管理、信息安全、软硬件开发以及大学的科研、实验和教学工作中得到广泛的应用。Wireshark 在日常应用中具有许多优点，无论是初学者还是数据包分析专家，Wireshark 都能通过丰富的功能满足其需要。

Wireshark 的特点体现在以下 6 方面。

1. 支持的协议

Wireshark 在支持协议的数量方面是出类拔萃的，Wireshark 提供了对超过 1000 种协议的支持。这些协议既包括最基础的 IP 协议和 DHCP 协议，也包括高级的专用协议（例如 DNP3 和 BitTorrent 等）。由于 Wireshark 是在开源模式下开发的，因此每次更新都会增加一些对新协议的支持。在特殊情况下，如果 Wireshark 不支持用户需要的协议，那么用户还可以自己编写代码以提供相应的支持，并将代码提供给 Wirshark 的开发者，以便他们考虑是否将之包含在以后的版本中。可以在 Wireshark 的项目网站上找到更多的相关信息。

2. 用户友好度

Wireshark 的界面是数据包嗅探工具中用户友好度比较高的。它基于图形用户界面并提供了清晰的菜单栏和简明的布局。为了增强实用性，它还提供了针对不同协议的彩色高亮显示以及通过图形展示原始数据细节等功能。与 tcpdump 等使用复杂命令行的数据包嗅探工具相比，Wireshark 的图用户化界面对于数据包分析初学者而言是十分方便的。

3. 价格

由于 Wireshark 是开源的，因此它是免费的。Wireshark 是遵循 GPL 协议发布的自由软件，任何人无论出于私人目的还是商业目的都可以下载并且使用。虽然 Wireshark 是免

费的，但是仍然会有一些人由于不了解这一点而付费“购买”它。如果在 eBay 搜索“数据包嗅探”，会发现会有很多人以 39.95 美元的“跳楼价”出售 Wireshark 的“专业企业级许可证”。显而易见，这些都是骗人的把戏。

4. 软件支持

一个软件的成败取决于其后期支持的好坏。像 Wireshark 这样的自由软件很少提供类似于商业软件的官方正式支持，它们主要依赖于开源项目社区的用户群提供帮助。Wireshark 社区是最活跃的开源项目社区之一。Wireshark 网站上给出了很多软件帮助的相关链接，包括在线文档、支持与开发维基条目和 FAQ。很多顶尖的开发者也加入并关注 Wireshark 的邮件列表。河床技术(Riverbed Technology)公司也提供对 Wireshark 的付费支持。

5. 源码访问

因为 Wrreshark 是开源软件，所以用户可以在任何时间访问其源码。这对查找程序漏洞、理解协议解释器的工作原理或上传自己的代码都有很大帮助。

6. 支持的操作系统

Wireshark 对主流的操作系统都提供了支持，其中包括 Windows、Mac OS X 以及基于 Linux 的系统。用户可以在 Wireshark 的主页上查询 Wireshark 支持的所有操作系统的列表。

5.1.2 安装 Wireshark

Wireshark 的安装过程极其简单，但在安装之前要确保计算机满足如下要求：

- 32 位或 64 位 CPU。
- 至少 400MB 可用内存(主要为了处理大流量文件)。
- 至少 300MB 的可用存储空间(不包括捕获的流量文件需要的存储空间)。
- 支持混杂模式的网卡。
- WinPcap 或 LibPcap。

WinPcap 是 Windows 平台 pcap 数据包捕获软件包的应用程序接口(API)的实现。简单来说，WinPcap 能够通过操作系统捕捉原始数据包、应用过滤器，并能够让网卡切入或切出混杂模式。

虽然可以单独下载并安装 WinPcap，但最好使用 Wireshark 安装包中的 WinPcap。这个版本的 WinPcap 经过了测试，能够和 Wireshark 一起工作。

1. 在 Windows 系统中安装 Wireshark

在 Windows 中安装 Wireshark 的第一步就是在 Wireshark 的官方网站上找到下载页面，并选择一个镜像站点下载最新版的安装包。

在下载好安装包之后，按照如下步骤安装 Wireshark：

(1) 双击安装包中的 EXE 文件开始安装，在介绍界面上单击 Next 按钮。

(2) 阅读许可证协议，如果接受此协议，单击 I Agree 按钮。

(3) 选择要安装的 Wireshark 组件，如图 5-1 所示，然后单击 Next 按钮。

(4) 在 Aditional Tasks 界面单击 Next 按钮。

(5) 选择 Wireshark 的安装位置，然后单击 Next 按钮。

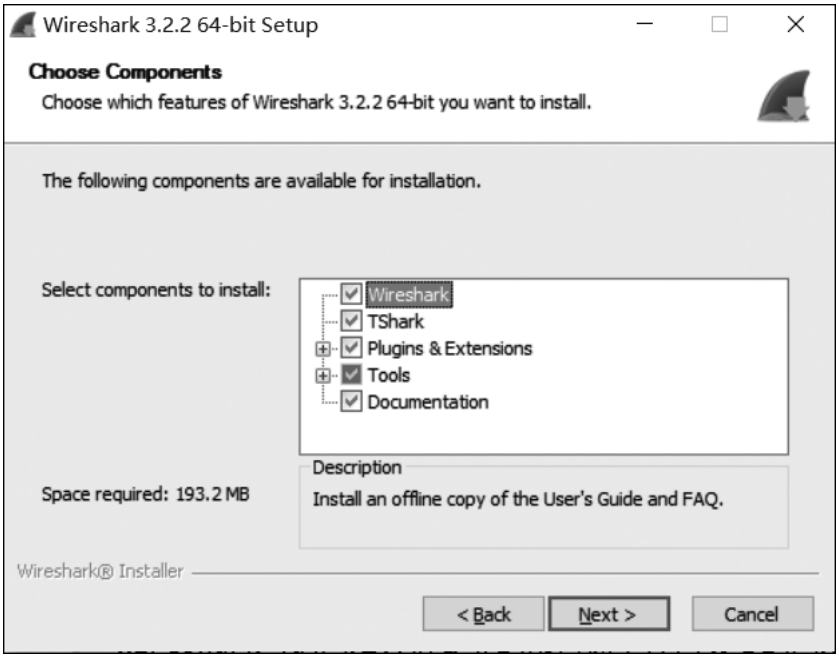

图 5-1　选择要安装的 Wireshark 组件

（6）当弹出询问是否需要安装 WinPcap 的对话框时，确保 Install Npcap 0.9986 复选框被选中，如图 5-2 所示，然后单击 Install 按钮开始安装。

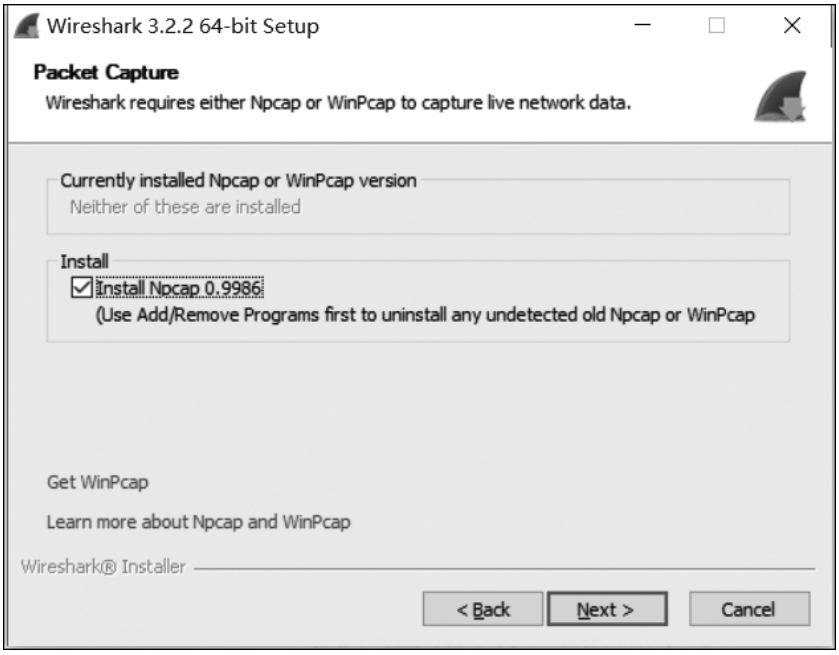

图 5-2　选中 Install Npcap 0.9986 复选框

（7）Wireshark 的安装过程进行了大约一半的时候，会开始安装 WinPcap。在 WinPcap

介绍页面单击 Next 按钮之后，阅读许可证协议并单击 I Agree 按钮。

(8) 选择是否安装 USBPcap 工具。USBPcap 用于从 USB 设备中收集数据。完成必要的选择后单击 Next 按钮。

(9) WinPcap 和 USBPcap 安装完成后，单击 Finish 按钮。

(10) Wireshark 安装完成后，单击 Finish 按钮。

(11) 在安装完成确认界面中单击 Finish 按钮。

2. 在 Linux 系统中安装 Wireshark

Wireshark 可以在大部分 Linux 系统中运行。可以通过 Linux 系统包管理器下载并安装适合用户当前系统的 Wireshark 版本。这里只介绍在几个常见的 Linux 系统中安装 Wireshark 的步骤。

一般来说，如果作为系统软件安装，安装者需要具有 root 权限；而如果通过编译源代码使之成为本地软件，通常就不需要 root 权限了。

1) 在使用 RPM 的 Linux 系统中安装 Wireshark

对于类似红帽 Linux(Red Hat Linux)等使用 RPM 的 Linux 系统，很可能系统默认安装了 Yum 包管理器。如果是这样，可以从 Linux 系统软件源中获取并快速安装 Wireshark。此时，打开控制台窗口，并输入以下命令：

```
sudo yum install Wireshark
```

如果需要依赖组件，可以根据提示安装它们。如果一切顺利，就可以使用命令行启动 Wireshark 并通过图形界面来操作它。

2) 在使用 DEB 的 Linux 中系统安装 Wireshark

对于类似于 Debian 和 Ubuntu 等使用 DEB 的 Linux 系统，可以使用 APT 包管理器安装 Wireshark。要从 Linux 系统软件源中安装 Wireshark。此时，打开控制台窗口并输入如下命令：

```
sudo apt-get install Wireshark Wireshark-qt
```

如果需要依赖组件，那么可以根据提示安装它们。

3) 使用源代码编译

因为操作系统架构和 Wireshark 功能的改变，所以从源代码安装 Wireshark 的方法可能也会随之变化，这也是建议从系统包管理器安装 Wireshark 的一个原因。然而，如果用户的 Linux 系统没有自动安装包管理器，那么安装 Wireshark 的一种高效的方法就是使用源代码编译。下面给出这种安装方法。

(1) 从 Wireshark 网站下载源代码包。

(2) 输入下面的命令将压缩包解压：

```
tar -jxvf 源代码包括名.tar.bz2
```

(3) 在安装和设置 Wireshark 之前，可能需要安装一些依赖组件。例如，Ubuntu 14.04 需要一些额外的软件包才能让 Wireshark 工作。这些依赖组件可以用以下的命令安装(可能需要 root 权限)：

```
sudo apt-get install pkg-config bison flex qt5-default libgtk-3-dev libpcap-dev
```

```
qttools5-dev-tools
```

(4) 进入源代码包解压缩后创建的文件夹。

(5) root 权限的用户使用 jconfigure 命令配置源代码,以便它能正常编译。如果不使用默认的设置,那么可以在这时指定安装选项。如果缺少相关软件支持,用户会得到相关错误信息;如果安装成功了,用户会得到安装成功提示。

(6) 输入 make 命令,将源代码编译成二进制文件。

(7) 输入 sudo make install 命令完成最后的安装。

(8) 输入 sudo /sbin/ldconfig 命令结束安装。

3. 在 Mac OS X 系统中安装 Wireshark

在 Mac OS X 系统中安装 Wireshark 的步骤如下:

(1) 从 Wireshark 网站下载针对 Mac OS X 系统的软件包。

(2) 运行安装程序,阅读并接受许可证协议。

(3) 按照安装向导的提示完成安装。

5.1.3 Wireshark 入门

1. 主窗口

Wireshark 的主窗口将捕获的数据包拆分并以更容易使人理解的方式呈现。也是用户花费时间较多的地方。Wireshark 的主窗口如图 5-3 所示。

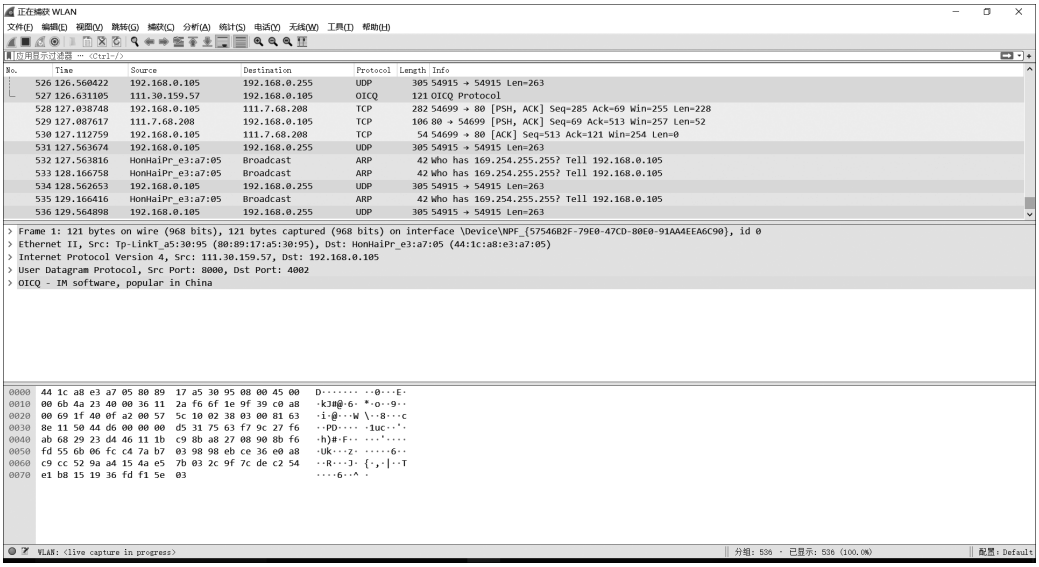

图 5-3 Wireshark 的主窗口

Wireshark 主窗口有 3 个面板。下面介绍每个面板的内容。

(1) 数据包列表(packet list)面板。这个面板用列表显示当前捕获文件中的所有数据包,其中包括数据包序号、数据包被捕获时的相对时间、数据包的源地址和目的地址、数据包的协议以及在数据包中找到的概况信息等。

(2) 数据包细节(packet details)面板。这个面板分层次显示了一个数据包中的内容，并且可以通过展开或收缩来显示从这个数据包中捕获的全部内容。

(3) 数据包字节(packet bytes)面板。这个面板可能是最令人困惑的，因为它显示了一个数据包未经处理的原始状态，也就是其在链路上传播时的样子。这些原始数据看上去不容易理解。

2. 首选项

Wireshark 提供了一些首选项设定，可以让用户根据需要进行定制。如果需要设定 Wireshark 首选项，那么需要在主菜单中选择“编辑”→“首选项”命令，然后便可以看到“首选项”对话框，里面有一些可以设置的选项，如图 5-4 所示。

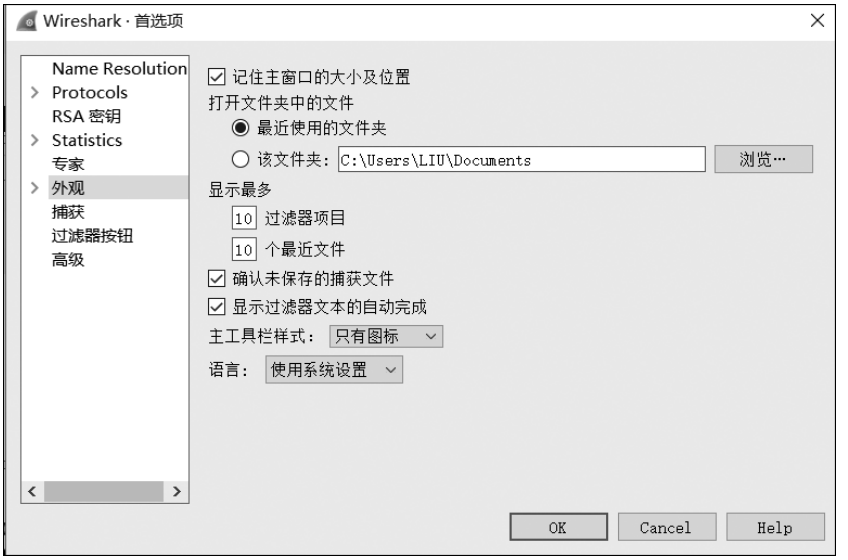

图 5-4 “Wireshark · 首选项”对话框

Wireshark 首选项分 9 部分，下面介绍其中的 7 部分。

(1) Name Resolutions(名称解析)。通过其中的选项设置，可以开启 Wireshark 将地址(包括 MAC 地址等)解析成更容易分辨的名字的功能，并且可以设置并发处理名称解析请求的最大数目。

(2) Protocols(协议)。其中的选项可以调整关于捕捉和显示各种 Wireshark 解码数据包的功能。虽然并不是针对每一个协议都可以进行调整，但是有一些协议的选项可以更改。除非用户有特殊的原因修改这些选项，否则最好保持它们的默认值。

(3) Statistics(统计)。其中提供了 Wireshark 统计功能的选项。

(4) 外观。其中的选项决定了 Wireshark 将如何显示数据。用户可以根据个人喜好对大多数选项进行调整，例如是否保存窗口位置、3 个主要窗口的布局、滚动条的摆放、数据包列表面板中列的摆放、显示捕获数据的字体、前景色和背景色等。

(5)捕获。其中选项可以对捕获数据包的方式进行设置，例如默认使用的设备、是否默认使用混杂模式、是否实时更新数据包列表面板等。

(6) 过滤器按钮。其中的选项用于生成和管理过滤器。

(7) 高级。在以上 6 部分中不包括的设置会被归入这里。通常这些设置只有 Wireshark 的高级用户才会修改。

3. 数据包彩色高亮显示

数据包列表面板中用不同颜色显示数据包,如图 5-5 所示。看上去这些颜色是随机分配给每一个数据包的,但其实并不是这样的。

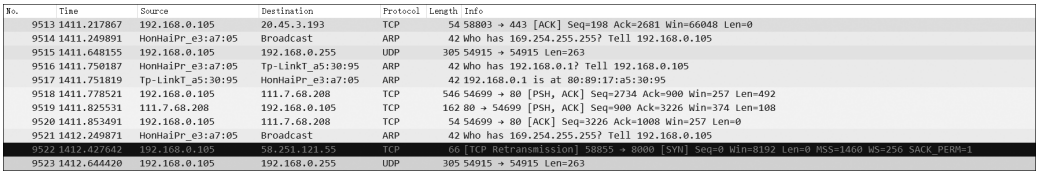

图 5-5　数据包彩色高亮显示

每一个数据包的颜色都是有依据的,不同颜色对应数据包使用的不同协议。例如,所有 DNS 数据包都是蓝色的,而所有 HTTP 数据包都是绿色的。将数据包以彩色高亮形式显示,可以让用户迅速将不同协议的数据包分开,而不需要查看每个数据包的 Protocol(协议)列。在浏览较大的捕获文件时,这样可以节省很多时间。

如图 5-6 所示,可以在“着色规则”对话框中查看每个协议对应的颜色。在主菜单中选择“视图”→“着色规则”命令,即可打开这个对话框。

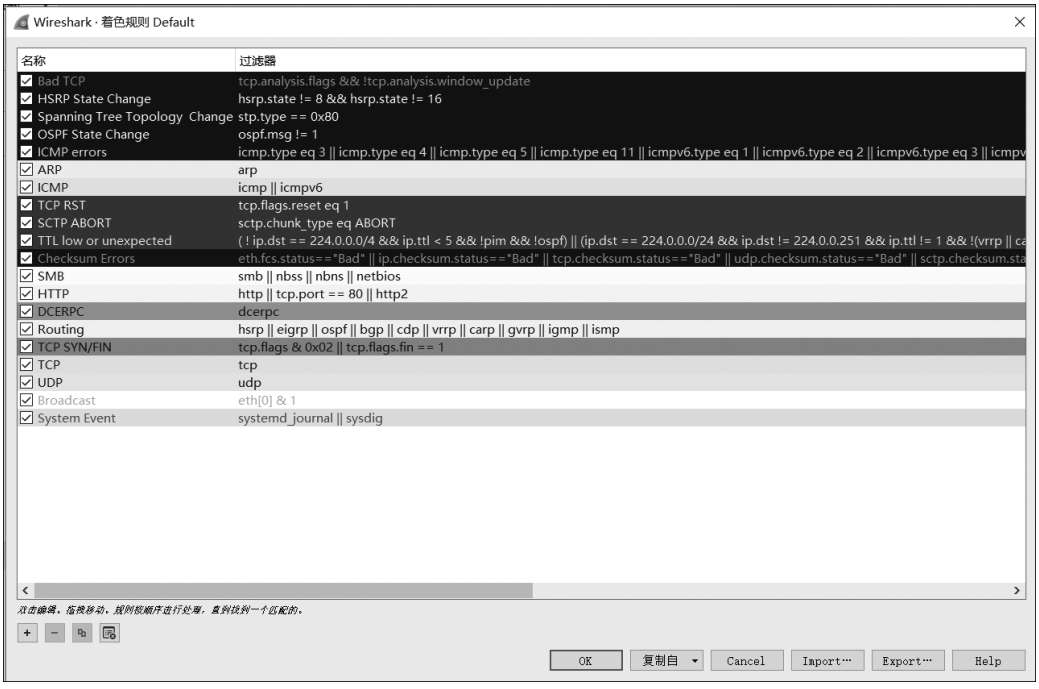

图 5-6　“Wireshark · 着色规则 Default”对话框

用户可以创建自己的着色规则,也可以修改已有的着色规则。

在使用 Wireshark 时,有可能处理某个协议的工作比较多。这时,对着色规则进行相应的修改能让工作更加方便。例如,如果网络中有一个恶意的 DHCP 服务器在分发 IP 地址,

那么可以修改 DHCP 的着色规则，使其呈现明黄色（或者其他易于辨识的颜色），这样就可以更快地找出所有 DHCP 数据包，使数据包分析工作效率更高。还可以通过用户自定义的过滤器创建新的着色规则，以扩展着色规则。

5.2 渗透测试实验

实验器材

PC（Linux/Windows 10）1 台。

预习要求

做好实验预习，掌握数据还原内容。
熟悉实验过程和基本操作流程。
撰写预习报告。

实验任务

通过本实验，掌握以下技能：
（1）利用 nc、ncat 建立网络连接通道，进行信息传递。
（2）利用 Wireshark 捕获并分析数据。
（3）利用 ncat 进行 SSL 加密传输。

实验环境

在 VMware 中安装两个 Kali Linux 虚拟机，分别作为服务器和客户机。安装 nc、ncat、Wireshark 工具（Kali Linux 默认已安装这些工具）。

预备知识

了解 VMware、Kali Linux、nc、ncat、Wireshark 的安装以及使用方法。

实验步骤

本实验主要在两台虚拟机上用 nc 建立网络连接通道并进行信息传递，然后用 Wireshark 捕获数据包。开始实验之前，需要对两台虚拟机进行网络设置，将两台虚拟机的“网络连接”选项设置为“仅主机模式”，一台定义为服务器（192.168.241.131），另一台定义为客户机（192.168.241.130），如图 5-7 所示。

用 nc 建立网络连接通道。在服务器上打开一个接口。例如，打开 333 号端口进行通信的命令为 nc -lp 333 -c bash，如图 5-8 所示。

在客户机上打开 Wireshark 并选择用于捕获数据包的网卡，然后开始捕获数据包，如图 5-9 所示。

打开客户机的终端，输入 ncat -nv 192.168.241.131 333 命令，连接服务器的 333 号端口并进行通信，如图 5-10 所示。

图 5-7 “虚拟机设置”对话框

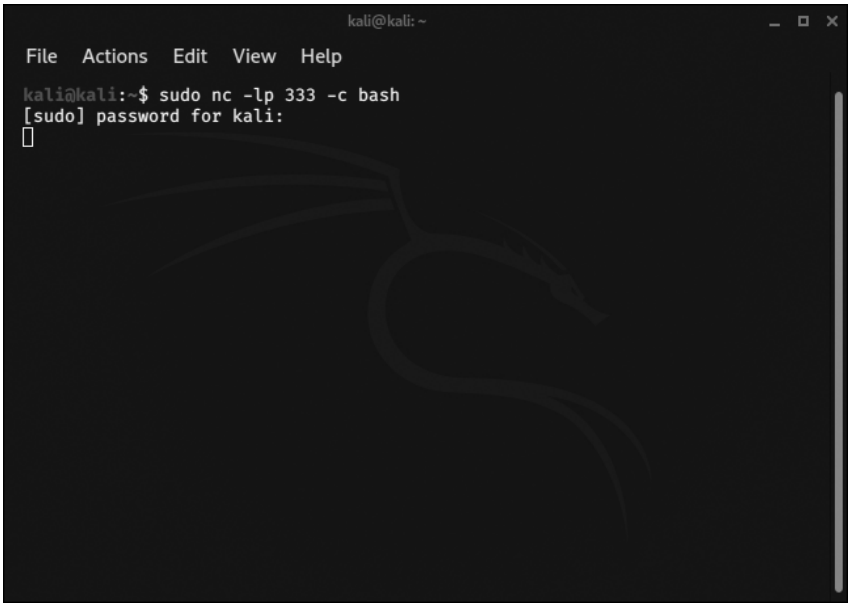

图 5-8 打开 333 号端口

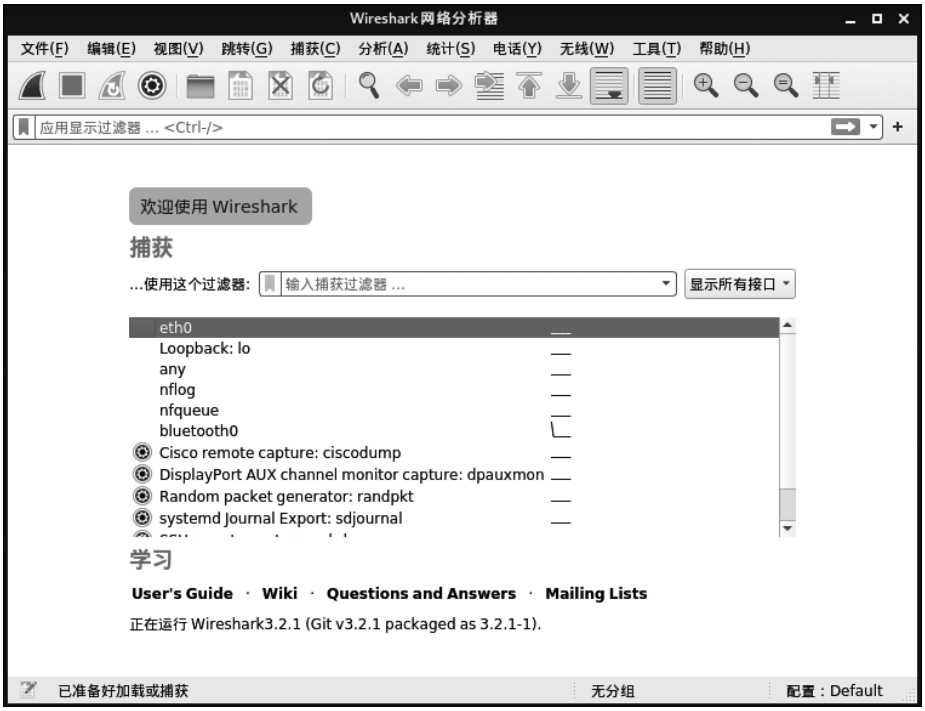

图 5-9　选择用于捕获数据包的网卡

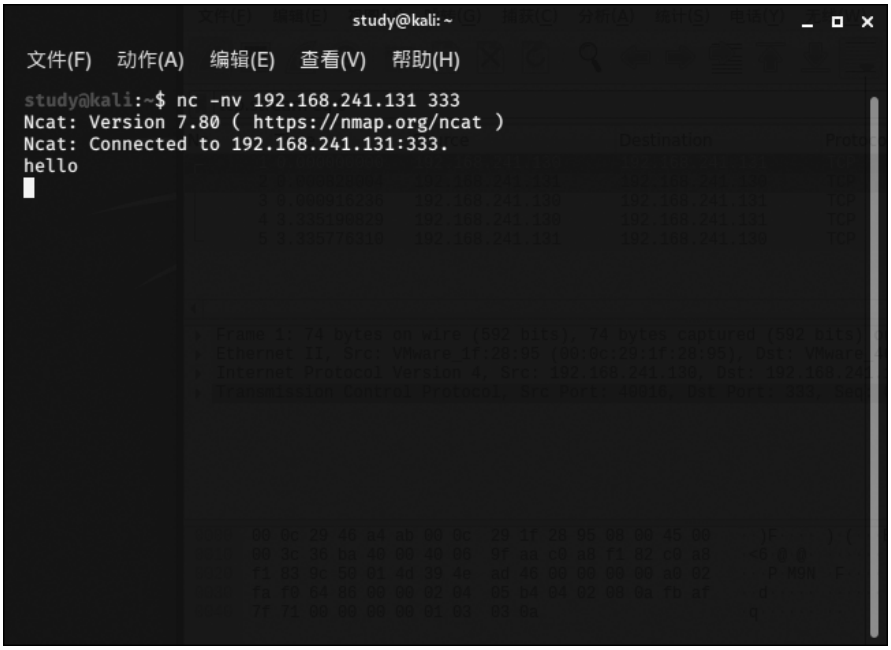

图 5-10　连接服务器的 333 号端口并进行通信

查看 Wireshark 捕获的数据包并进行分析：首先是 ARP 协议，ARP 用来查看对方的 MAC 地址(ARP 解析)；有了 MAC 地址，接下来组装二层包头；然后建立 TCP 连接(三次