6.2 安装 Tcpdump

如果说 Wireshark 是世界上最流行的图形化数据包分析应用，那么 Tcpdump 就是世界上最流行的命令行数据包分析应用。因为 Tcpdump 被设计在基于 UNIX 的系统上运行，所以它非常易于通过包管理器来安装，甚至可以预装在很多 Linux 发行版本中。

虽然这本书所讲的大部分内容都针对于 Windows，但是关于 Tcpdump 的章节还是针对 UNIX 用户的。具体地说，我们会用 Ubuntu 14.04 LTS 来演示。如果你想在 Windows 上使用 Tcpdump，那么你可以下载安装 WinDump。虽然 Tcpdump 和 WinDump 的使用体验不完全一样，但是它们的功能基本一样。在 WinDump 中一些 Tcpdump 的功能可能会缺失甚至可能会有安全漏洞（我们不会在本书讲 WinDump）。

Ubuntu 没有预装 Tcpdump，但我们可以通过 APT 包管理系统来简单安装。要安装 Tcpdump，请按照以下步骤操作。

（1）打开一个终端窗口并且运行 sudo apt-get update，来确保你的软件仓库与最新的软件版本保持同步。

（2）执行命令 sudo apt-get install tcpdump。

（3）你会被提示需要安装一些依赖才能够运行 Tcpdump。按 Y 来允许这些依赖的安装，并且当提示时按**回车键**。

（4）一旦安装完成，就可以运行命令 Tcpdump -h 来执行 Tcpdump，并打印出当前版本信息。如果该命令执行成功，则说明你现在可以开始使用 Tcpdump 了。

```
   sanders@ppa:~$ tcpdump -h
tcpdump version 4.5.1
libpcap version 1.5.3
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqRStuUvxX#] [ -B size ] [ -c cou
            [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G se
            [ -i interface ] [ -j tstamptype ] [ -M secret ]
            [ -Q metadata-filter-expression ]
            [ -r file ] [ -s snaplen ] [ -T type ] [ --version ] [
            [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z c
            [ -Z user ] [ expression ]
```

你可以通过调用 man tcpdump，来查看 Tcpdump 所有可用的命令，

我们将介绍其中一些命令的用法。