1.1 数据包分析与数据包嗅探器

数据包分析，通常也被称为数据包嗅探或协议分析，指的是捕获和解网络上在线传输数据的过程，通常是为了能更好地了解在网络上正在发生事情。数据包分析过程通常由数据包嗅探器来执行，而数据包嗅探器则是种用来在网络媒介上捕获原始传输数据的工具。

数据包分析技术可以用来达到如下目标。

- 了解网络特征。
- 查看网络上的通信主体。
- 确认谁或是哪些应用在占用网络带宽。
- 识别网络使用高峰时间。
- 识别可能的攻击或恶意活动。
- 寻找不安全以及滥用网络资源的应用。

目前市面上有着多种类型的数据包嗅探器，包括免费的和商业的。每软件的设计目标都会存在一些差异。流行的数据包分析软件包括 Tcpdum OmniPeek 和 Wireshark（我们在这本书中只使用此款软件）。Tcpdump 一个命令行程序，而 Wireshark 和 OmniPeekd 都拥有图形用户界面（GUI）。