

书的赞誉

怎么购买本书

写作方法

如何使用本书

示例捕获文件

科技基金会

感谢支持

第 1 章 数据包分析技术与网络基础

1.1 数据包分析与数据包嗅探器

1.1.1 评估数据包嗅探器

1.1.2 数据包嗅探器工作过程

1.2 网络通信原理

1.2.1 协议

1.2.2 七层 OSI 参考模型

1.2.3 OSI 参考模型中的数据封装

1.2.4 数据封装

1.2.5 网络硬件

1.3 流量分类

1.3.1 广播流量

1.1.2 数据包嗅探器工作过程

数据包嗅探过程中涉及软件和硬件之间的协作。这个过程可以分为三个步骤。

第一步：收集，数据包嗅探器从网络线缆上收集原始二进制数据。通常情况下，通过将选定的网卡设置成混杂模式来完成抓包。在这种模式下，网卡将抓取一个网段上的所有网络通信流量，而不仅是发往它的数据包。

第二步：转换，将捕获的二进制数据转换成可读形式。高级的命令行数据包嗅探器就支持到这一步骤。到这一步，网络上的数据包将以一种非常基础的解析方式进行显示，而将大部分的分析工作留给最终用户。

第三步（最后一步）：分析，对捕获和转换后的数据进行真正的深入分析。数据包嗅探器以捕获的网络数据作为输入，识别并验证它们的协议，后开始分析每个协议的特定属性。



Wireshark 数据包分析实战（第 3 版）
作者：[美]克里斯·桑德斯（Chris Sander...）

6%

扫码下载知