概念与方法

我是一个非常随意的人，所以，当我教授你一个概念时，我也会尝试
非常随意的方式来进行解释。而本书的语言也会同样随意，虽然晦涩的技
术语很容易让人迷失，但我已经尽我所能地保持行文的一致与清晰，让所
的定义更加明确、直白，没有任何繁文缛节。然而我终究是从伟大的肯塔
州来的，所以我不得不收起我们的一些夸张语气，但如果你在本书中看到
些粗野的乡村土话，请务必原谅我。

如果你真的想学习并精通数据包分析技术，你应该首先掌握本书前几
中介绍的概念，因为它们是理解本书其余部分的前提。本书的后半部分将
纯粹的实战内容，或许你在工作中并不会遇到完全相同的场景，但在学习
书后你应该可以应用所学到的概念与技术，来解决你所遇到的实际问题。

接下来让我们快速浏览本书各章的主要内容。

- 第 1 章「数据包分析与网络基础」。什么是数据包分析技术？这种技术的
本原理是什么样的？你该如何使用这项技术？本章将讲解这些网络通信与
据包分析的基础知识。
- 第 2 章「监听网络线路」。本章将介绍在网络中放置数据包嗅探器时可以
用的各种不同技术。
- 第 3 章「Wireshark 入门」。从本章起，我们将开始进入 Wireshark 软件
世界，介绍 Wireshark 软件的入门知识——从哪里下载，如何使用它，它
成什么功能，为什么它受到如此多的好评与关注，以及其他使用技巧。本
包含了有关使用配置文件自定义 Wireshark 的讨论。
- 第 4 章「玩转捕获数据包」。在你运行 Wireshark 软件之后，你需要知道
何与捕获的数据包进行交互，而这是你开始学习基础实践方法的起始点，
括关于数据包流和名称解析更详细的全新内容。
- 第 5 章「Wireshark 高级特性」。一旦掌握了 Wireshark 基础知识，就可
准备学习它的高级特性了。本章将深入钻研 Wireshark 的高级特性，带你
开 Wireshark 的神秘面纱，来了解一些比较少见的操作。本章包括关于数
包流和名称解析更详细的全新内容。
- 第 6 章「用命令行分析数据包」。Wireshark 功能强大，但有时你需要离开
图形界面，与命令行上的数据包进行交互。本章向你介绍了使用 TShark

Tcpdump 这两种命令行包分析工具的方法。

- 第 7 章「网络层协议」。本章通过解析 ARP、IPv4、IPv6 和 ICMP，来向介绍数据包级别上常见的网络层通信。要在现实场景中对这些协议进行故排除，首先需要了解它们的工作原理。
- 第 8 章「传输层协议」。本章讨论了两种常见的传输协议 TCP 和 UDP。大多数数据包都将使用这两种协议中的一种，因此了解它们在数据包级别的观以及它们之间的差异非常重要。
- 第 9 章「常见高层网络协议」。本章继续讲解网络协议的相关内容，将从据包的层次上带你了解 4 种常见的高层网络通信协议——HTTP、DNS、DHCP 与 SMTP。
- 第 10 章「基础的现实世界场景」。本章将包含一些常见的网络流量，以及最初的现实场景中的案例。每个案例都将以一种易于遵循的格式呈现，包问题、分析和解决方法。这些基础场景案例仅仅涉及少量几台计算机，以有限的分析——足以让你找到感觉，并将其运用到实践中。
- 第 11 章「让网络不再卡」。网络技术人员遇到的最普遍的网络问题之一便网络性能缓慢这种情况，本章便是专门为解决这一问题而设计的。
- 第 12 章「安全领域的数据包分析」。网络安全是信息技术领域中最大的热话题之一，本章将向你展示使用数据包分析技术解决安全相关问题的实际例。
- 第 13 章「无线网络数据包分析」。本章是无线网络数据包分析技术启蒙，讨论了无线数据包分析与有线数据包分析技术的差异，并包含了一些无线络流量分析的案例。
- 附录 A「延伸阅读」。本书附录 A 给出了其他一些参考工具和网站列表，可能会发现这些工具和网站在你使用前面介绍的数据包分析技术时非常有用。
- 附录 B「分析数据包结构」。如果你想深入研究解释单个数据包，那么可参考附录 B 的内容，它概述了数据包信息如何以二进制形式存储以及如何二进制转换为十六进制表示法。然后，它将向你展示如何使用数据包结构解析以十六进制表示法呈现的数据包。在你需要花费大量时间分析自定义议或使用命令行分析工具的情况下，这会很方便。