Wireshark数据包分析实战（第3版）

PRACTICAL PACKET ANALYSIS 3RD EDITION

[美] 克里斯 · 桑德斯（Chris Sanders） 著　　诸葛建伟　陆宇翔　曾皓辰　译

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

Wireshark数据包分析实战（第3版）

PRACTICAL PACKET ANALYSIS 3RD EDITION

[美] 克里斯 · 桑德斯（Chris Sanders） 著　　诸葛建伟　陆宇翔　曾皓辰　译

人民邮电出版社
北京

图书在版编目（CIP）数据

Wireshark数据包分析实战 : 第3版 / (美) 克里斯·桑德斯 (Chris Sanders) 著 ; 诸葛建伟, 陆宇翔, 曾皓辰译. -- 北京 : 人民邮电出版社, 2018.12
ISBN 978-7-115-49431-3

Ⅰ. ①W… Ⅱ. ①克… ②诸… ③陆… ④曾… Ⅲ. ①统计数据一统计分析一应用软件 Ⅳ. ①O212.1-39

中国版本图书馆CIP数据核字(2018)第219865号

版权声明

◆ 著　[美] 克里斯·桑德斯（Chris Sanders）
译　诸葛建伟　陆宇翔　曾皓辰
责任编辑　陈聪聪
责任印制　焦志炜

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市君旺印务有限公司印刷

◆ 开本：800×1000　1/16
印张：22.25
字数：448 千字　2018 年 12 月第 1 版
印数：1－3 000 册　2018 年 12 月河北第 1 次印刷

著作权合同登记号　图字：01-2017-5043 号

定价：79.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

内 容 提 要

Wireshark 是一款流行的网络嗅探软件，本书在上一版的基础上针对 Wireshark 2.0.5 和 IPv6 进行了更新，并通过大量真实的案例对 Wireshark 的使用进行了详细讲解，旨在帮助读者理解 Wireshark 捕获的 PCAP 格式的数据包，以便对网络中的问题进行排错。

本书共 13 章，从数据包分析与数据包嗅探器的基础知识开始，循序渐进地介绍 Wireshark 的基本使用方法及其数据包分析功能特性，同时还介绍了针对不同协议层与无线网络的具体实践技术与经验技巧。在此过程中，作者结合大量真实的案例，图文并茂地演示使用 Wireshark 进行数据包分析的技术方法，使读者能够顺着本书思路逐步掌握网络数据包嗅探与分析技能。附录部分列举了数据包分析工具，以及其他数据包分析的学习资源，并对数据包的表现形式展开讨论，介绍如何使用数据包结构图查看和表示数据包。

本书适合网络协议开发人员、网络管理与维护人员、“不怀好意的”的黑客、选修网络课程的高校学生阅读。

对本书的赞誉

本书内容丰富，设计巧妙又通俗易懂。老实说，这本数据包分析的图书让我倍感兴奋。

——TechRepublic

强烈建议初级网络分析师、软件开发人员和刚刚取得 CSE/CISSP 等认证的人员阅读本书。读完本书后，你们只需要卷起袖子，就可以动手排除网络（和安全）问题了。

——Gunter Ollmann，IOActive 前首席技术官

下一次再排查网络变慢的问题时，我将求助本书。对任何技术图书来说，这或许是我能给的最好的评价。

——Michael W. Lucas，*Absolute FreeBSD and Network Flow Analysis* 作者

无论你负责多大规模的网络管理，本书都必不可少。

——Linux Pro Magazine

本书写作精良、简单易用、格式良好，相当实用。

——ArsGeek.com

如果你想要熟练掌握数据包分析的基本知识，那么本书是一个不错的选择。

——State Of Security

本书内容丰富，紧扣“实战”主题。它向读者提供了进行数据包分析所需的信息，并借助于真实的实例演示了 Wirshark 的用途。

——LinuxSecurity.com

网络中有未知的主机之间在互相通信吗？ 我的机器正在与陌生的主机通信吗？ 你只需要一个数据包嗅探器就可以找到这些问题的答案，Wireshark 是完成这项工作的最佳工具之一，而本书是了解该工具的最佳方法之一。

——Free Software Magazine

本书是数据包分析初学者和进阶者的理想之选。

——Daemon News

“天赐恩宠！多么甜美的声音！

这挽救了像我这样的可怜人！

我曾经迷失过，但是现在我找到了方向；

我曾经盲目过，但是现在我看到了光明。”

致　谢

对支持我和本书的所有人表示由衷的感谢。

Ellen，感谢你对我无条件的爱，在过去的这段时间里，我占用了你大量的休息时间。

妈妈，即使是在天堂，您树立的善良的榜样也将一直激励我。爸爸，我从您那里知道了什么是艰苦的工作，如果没有你，也就不会有这本书的诞生。

Jason Smith，你就像我的兄弟一样，我非常感谢你一直以来愿意给我提供宝贵的建议。

感谢我过去和现在的同事，能够与那些让我变得更聪明、更善良的人一起工作是我的荣幸。篇幅所限，我不能列举所有人的名字，但真诚地感谢 Dustin、Alek、Martin、Patrick、Chris、Mike 和 Grady 支持我并提供了大量的帮助。

感谢担任本书技术主编的 Tyler Reguly。我有时会犯愚蠢的错误，是你帮助我避免了这些错误的发生。此外，感谢 David Vaughan 为本书所做的额外审读工作，感谢 Jeff Carrell 帮我编辑了 IPv6 的内容，感谢 Brad Duncan 提供了在安全章节中使用的捕获文件，并且感谢 QA Café 团队提供了 Cloudshark 许可证，我用它组织了本书中用到的那些捕获的数据包。

当然，我还要感谢 Gerald Combs 和 Wireshark 开发团队。这是 Gerald 和数

百名其他开发人员的奉献，他们使 Wireshark 成为了一个如此优秀的分析平台。如果没有他们的努力，信息技术和网络安全将无从谈起。

最后，感谢 Bill、Serena、Anna、Jan、Amanda、Alison 和 No Starch Press 的其他工作人员，感谢你们在编辑和制作本书的 3 个版本时所付出的努力。

前　言

本书从 2015 年底开始编写，在 2017 年早期完成，总计历时一年半。而在本书出版之日，距离本书第 2 版发布的时间已经有 6 年，距离第 1 版则长达 10 年之久。本书对内容进行了大量的更新，具有全新的网络捕获文件和场景，并新添了一章内容来讲解如何使用 TShark 和 Tcpdump 通过命令行进行数据包分析。如果你喜欢前两个版本，那么相信你也会喜欢这本书。它延续了之前的写作风格，以一种简单易懂的方式来分析解释。如果你因为缺少关于网络或 Wireshark 更新的最新信息而不愿意尝试之前的两个版本，那么你可以阅读本书，因为这里包含了新的网络协议扩展内容和关于 Wireshark 2.x 的更新信息。

为什么购买本书

你一定很想知道为什么应该买这本书，而不是关于数据包分析的其他书籍。答案在于本书的书名：《Wireshark 数据包分析实战》。让我们面对这样的现实——没有比实际经验更加重要的了。你可以通过真实场景中的实际案例来掌握书中的内容。

本书的前半部分介绍了理解数据包分析和 Wireshark 所需的知识，而后半部分则将重心放在了实践案例上，你在日常的网络管理中经常会遇到这些案例中

出现的情况。

无论你是网络技术人员、网络管理员、首席信息官、桌面工程师，还是网络安全分析师，在理解并使用本书中讲解的数据包分析技术时，都会让你受益匪浅。

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，我也会尝试用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，让所有的定义更加明确、直白，没有任何繁文缛节。然而我终究是从伟大的肯塔基州来的，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一些粗野的乡村土话，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章中介绍的概念，因为它们是理解本书其余部分的前提。本书的后半部分将是纯粹的实战内容，或许你在工作中并不会遇到完全相同的场景，但在学习本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？这种技术的基本原理是什么样的？你该如何使用这项技术？本章将讲解这些网络通信与数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使用的各种不同技术。
- 第 3 章“Wireshark 入门”。从本章起，我们将开始进入 Wireshark 软件的世界，介绍 Wireshark 软件的入门知识——从哪里下载，如何使用它，它完成什么功能，为什么它受到如此多的好评与关注，以及其他使用技巧。本章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，你需要知道如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，

包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，就可以准备学习它的高级特性了。本章将深入钻研 Wireshark 的高级特性，带你揭开 Wireshark 的神秘面纱，来了解一些比较少见的操作。本章包括关于数据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 和 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，来向你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障排除，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外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，将从数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，包括问题、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，以及有限的分析——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是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点话题之一，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案例。
- 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，并包含了一些无线网络流量分析的案例。
- 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，你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，那么可以参考附录 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将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图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协议或使用命令行分析工具的情况下，这会很方便。

如何使用本书

我期待本书按照如下两种方式进行使用。

- 作为一本教学书籍，你可以逐章阅读，特别注意后面的章节中涉及的实际场景，它们可以帮助你进一步理解和掌握数据包分析技术。
- 作为一本参考资料，有些 Wireshark 软件的特性是你不会经常使用的，所以你可能会忘记它们是如何工作的。当你需要快速重温如何使用 Wireshark 软件的某个特性时，可以从本书中获得参考。当你进行数据包分析时，可能会需要参考本书提供的这些图表和方法。

关于示例捕获文件

本书使用的所有捕获文件都可以在异步社区下载，为了将本书的价值最大化，强烈建议下载这些文件，并在学习每个真实案例时使用它们。

乡村科技基金会

在这里，我必须介绍一下由本书而衍生出的美好事物。在本书第 1 版出版

后不久，我创办了一个 501(c)(3)的非营利性组织——乡村科技基金会（Rural Technology Fund）。

比起城市与市郊的学生们，乡村的学生即使拥有很优秀的成绩，仍然很少有机会能够接触到最新的科技。创办于 2008 年的乡村科技基金会（RTF）是我的终极理想。RTF 致力于能够减少乡村学生与城市同龄学生们之间的数字鸿沟，为此它有针对性地发起了奖学金项目、社区参与计划、教育技术资源捐赠，以及一些在乡村和贫困地区的科技推广和宣传项目。

2016 年，RTF 为美国乡村和贫困地区的 1 万多名学生提供了技术教育资源。我很高兴地宣布，本书作者的所有收入都直接交给 RTF 来支持这些目标。如果你想了解更多关于农村科技基金的信息或者想知道能为它做些什么，请访问我们的网站或者关注我们的 Twitter @RuralTechFund。

资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

配套资源

本书提供如下资源：

本书配套资源请到异步社区本书购买页处下载。

要获得以上配套资源，请在异步社区本书页面中点击 配套资源，跳转到下载界面，按提示进行操作即可。注意：为保证购书读者的权益，该操作会给出相关提示，要求输入提取码进行验证。

如果您是教师，希望获得教学配套资源，请在社区本书页面中直接联系本书的责任编辑。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，点击“提交勘误”，输入勘误信息，点击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。

扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内

容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

“异步图书”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号