no starch press

Wireshark数据包分析实战（第2版）

PRACTICAL PACKET ANALYSIS 2ND EDITION

[美] Chris Sanders 著　诸葛建伟　陈霖　许伟林　译

人民邮电出版社
POSTS & TELECOM PRESS

Wireshark数据包分析实战（第2版）

PRACTICAL PACKET ANALYSIS 2ND EDITION

[美] Chris Sanders 著　诸葛建伟 陈霖 许伟林 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2版 / (美) 桑德斯(Sanders,C.) 著 ; 诸葛建伟, 陈霖, 许伟林译. -- 北京 : 人民邮电出版社, 2013.3
ISBN 978-7-115-30236-6

Ⅰ. ①W… Ⅱ. ①桑… ②诸… ③陈… ④许… Ⅲ. ①计算机网络－数据－分析－应用软件 Ⅳ. ①TP393.09

中国版本图书馆CIP数据核字(2012)第294560号

版 权 声 明

Wireshark 数据包分析实战（第 2 版）

◆ 著 [美] Chris Sanders
译 诸葛建伟 陈 霖 许伟林
责任编辑 傅道坤

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：800×1000 1/16
印张：17.75
字数：355 千字 2013 年 3 月第 1 版
印数：1－4 000 册 2013 年 3 月河北第 1 次印刷

著作权合同登记号 图字：01-2012-2971 号
ISBN 978-7-115-30236-6

定价：49.00 元

读者服务热线：(010)67132692 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内 容 提 要

本书从网络嗅探与数据包分析的基础知识开始，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，作者结合一些简单易懂的实际网络案例，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地掌握网络数据包嗅探与分析技能。最后，本书使用网络管理员、IT 技术支持、应用程序开发者们经常遇到的实际网络问题（包括无法正常上网、程序连接数据库错误、网速很卡，以及遭遇扫描渗透、ARP 欺骗攻击等），来讲解如何应用 Wireshark 数据包分析技术和技巧，快速定位故障点，并找出原因以解决实际问题。本书覆盖了无线 WiFi 网络中的嗅探与数据包分析技术，同时也给出了嗅探与数据包分析领域丰富的参考技术文档、网站、开源工具与开发库等资源列表。

本书适合网络管理员、安全工程师、软件开发工程师与测试人员，以及网络工程、信息安全等专业学生与网络技术爱好者阅读。

关于作者

Chris Sanders 是一名计算机安全咨询顾问、作家和研究人员。他还是一名 SANS 导师，持有 CISSP、GCIA、GCIH、GREM 等行业证书，并定期在 WindowsSecurity.com 网站和自己的博客 ChrisSanders.org 发表文章。Sanders 每天都会使用 Wireshark 进行数据包分析。他目前居住在美国南卡罗米纳州查尔斯顿，以国防承包商的身份工作。

联系作者

我非常期盼能够收到本书读者的反馈，如果你出于任何原因想联系我，你可以将你的疑问、评论、批评，甚至是求婚信，直接发送到我的电子邮箱 chris@chrissanders.org，我经常在 http://www.chrissanders.org/发表博客，也欢迎你在 Twitter 上成为@chrissanders88 的粉丝。

致　谢

本书的成功出版离不开很多人的直接贡献和间接支持。

爸爸，我从很多来源获得动力，但比起听到你说你因为我而骄傲，没有其他任何事情能够让我更加高兴。对此，我对你真是感谢不尽。

妈妈，本书第 2 版将在你过世 10 周年纪念日的前夕出版，我知道你一直在天堂注视着我，并为我而自豪，我希望我能够继续努力，能够让你更加为我自豪。

Debi 叔叔和 Randy 阿姨，你们从我写书的第一天起就是我最大的支持者。我没有一个大家庭，但我非常珍视我所拥有的亲情，特别是你们。尽管我们并没有能像我所期望的那样经常会面，但我深深地感谢你们，对我来说，你们和我的亲生父母没有差异。

Tina Nance, 虽然最近我们并没有像以前那样有很多的交谈，但我一直将你视作我第二个母亲。如果没有你的支持和信任，我今天不会在做我自己想做的事情。

Jason Smith，你比其他任何人都承受了更多我的牢骚，仅仅这样对我来说都已经是很大的帮助了。谢谢你成为我的好朋友和合作者，在很多项目中为我提供了建议，并让我占用了你家的车库长达 6 个月之久。

感谢我的同事们（过去的和现在的），我一直相信如果一个人周围都是好人的话，他也会成为一个好人。我非常幸运能够和一些优秀人士一起工作，你们

是最棒最聪明的，你们是我的家人。

Mike Poor，你是我毋庸置疑的数据包分析技术的崇拜偶像。你的工作与达成目标的方法一直在给我启迪，并帮助我做我想要做的事情。

Tyler Reguly，非常感谢你为本书承担技术编辑的角色，我知道这并不是个有趣的活儿，但是绝对必要并需要感谢。

同样需要特别感谢 Gerald Combs 和 Wireshark 开发团队，正是 Gerald 和其他几百位开发者的无私投入，才让 Wireshark 能够成为如此强大的分析平台。如果没有他们的贡献，本书也不会存在……即使存在，也可能是基于 tcpdump，那么就不会像现在这样有趣。

感谢 Bill 和 No Starch 出版社的同仁给予我这位来自肯塔基州的小人物不仅仅是一次，而是两次的机会，谢谢你们对我的容忍和耐心，并帮助我让我的梦想成真。

关 于 译 者

诸葛建伟，博士，现为清华大学网络与信息安全实验室副研究员、狩猎女神科研团队负责人、CCERT 紧急响应组成员、著名开源信息安全研究团队 The Honeynet Project 的正式成员，以及中国蜜网项目组（www.honeynet.org.cn）团队发起人和现任负责人、信息安全领域培训讲师和自由撰稿人，编写与参与翻译的畅销图书有《网络攻防技术与实践》、《Metasploit 渗透测试指南》等。新浪微博：@清华诸葛建伟。

陈霖，现就读于洛桑联邦理工学院硕士项目，于北京大学获得计算机科学学士学位。新浪微博：@Larch 爱刀刀。

许伟林，现为清华大学网络与信息安全实验室助理工程师，于北京邮电大学获得计算机科学学士学位，曾两次参与 Google Summer of Code 计划，分别为 Nmap 和 The Honeynet Project 贡献 IPv6 主机发现模块与 IPv6 攻击检测器的开源代码，并负责新浪微博 @Nmap 网络扫描的维护工作。新浪微博：@许伟林。

译 者 序

谨以此书献给中国农村渴望得到更多计算机基础教育的孩子们！

本书是一本非常实用的网络技能培训技术图书，以最为流行和强大的开源数据包抓包与分析工具——Wireshark——作为基础软件，通过大量生动的真实场景案例来讲解数据包分析的基础技术、高级特性与实际应用技能。

Wireshark 在 2011 年最新的 SecTools 安全社区流行软件排行榜中，超越 Metasploit、Nessus、Aircrack 与 Snort，占据榜首位置，这充分体现了 Wireshark 软件在网络安全与取证分析方面的重要作用与流行度。与此同时，Wireshark 更是一个通用化的网络数据嗅探器与协议分析器，在网络运行管理、网络故障诊断、网络应用开发与调试等各个方面都作为基本手头工具，而被网络管理员、软件开发工程师与测试人员所广泛使用。

尽管网络数据包分析技术是网络管理员、安全工程师、软件开发工程师与测试人员必备的基本技能，然而可惜的是国内却没有优秀的实用技术培训教材与书籍。在这广大技术人群遭遇一些实际网络问题，或是对 Wireshark 等网络嗅探器与协议分析器的使用存在疑问时，他们并没有系统性的资料去学习掌握基础知识与技能，并掌握相关技能与方法来解决工作中的实际挑战，而往往只能寄希望于在网络上搜索一些零散并且可能过时的信息来探索尝试，从而花费了大量宝贵时间，并对数据包分析技术的自我修炼不得要领。

本书（英文版）原是国外一本非常优秀、高度注重基础性与实用性的网络数据包分析技术教程，细致地讲解了网络数据包嗅探与分析的技术原理，并以目前最流行的网络数据包嗅探与分析开源工具 Wireshark 作为平台软件，一步步引导读者们掌握使用 Wireshark 进行实际网络中数据包分析、故障定位与问题解决的实践技术方法。

在本书的章节设计上，作者从网络嗅探与数据包分析的基本知识背景开始，以简练清晰的语言帮助读者首先建立起网络协议与数据包结构、不同网络场景下的嗅探方法等方面的基础知识，然后渐进地介绍 Wireshark 的基本使用方法、

Wireshark 的数据包分析功能特性，以及针对不同协议层与无线网络的具体实践技术和经验技巧，在此过程中，作者使用了简单易懂的一些实际网络案例，图文并茂地结合这些具体案例来演示使用 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地掌握网络数据包嗅探与分析的技能。最后，本书以网络管理员、IT 技术支持、应用程序开发者经常遇到的实际网络问题，包括无法正常上网、部署分部网络、程序连接数据库错误、网速很卡，以及遭遇扫描渗透与 ARP 欺骗攻击等，来讲解如何应用 Wireshark 数据包分析技术和技巧，快速定位故障点与原因并解决实际问题。本书也覆盖了无线 WiFi 网络中的嗅探与数据包分析技术，同时也给出了在嗅探与数据包分析领域丰富的参考技术文档、网站、开源工具与开发库等资源列表。

本书原版取得了国外读者的一致好评，在 Amazon 网络安全领域图书销售排名位居 Top 20，以及 4 星半的良好评价，也验证了本书在网络安全领域的重要程度。此外，本书在 2007 年第一版基础上又增加了更多的技术内容和案例，是通过了市场检验的一本好书。

更加难能可贵的是，本书作者 Chris Sanders 是带着一颗善良感恩的心完成了本书的创作。他出生于美国的乡村地区，在通过自身努力成为一位网络技术专家后，成立了一家乡村科技基金会，并将本书的所有版税捐赠出来，为乡村学生设立奖学金，致力于减少乡村学生与城市同龄学生们之间的数字鸿沟。

本书和译者也非常有缘，在 2011 年 10 月为电子工业出版社进行书籍评估时，译者就已经对本书赞誉有加，并给出了引进的建议。之后，在本书中文版权的激烈竞争中，人民邮电出版社最终胜出，这也让译者一度认为无缘这本优秀的作品。机缘巧合的是，在新浪微博上回复一位读者@过来的微博评论时，译者向几个出版社编辑微博发出本书“通缉令”，意外地从人民邮电出版社编辑那获知了本书下落，也非常高兴地接受了他们的翻译邀请。为了平衡翻译质量和进度，我们组织起了 3 人的译者团队，由诸葛建伟译序、前言和第 1~3 章，陈霖译第 4~7 章，许伟林译第 8~11 章与附录。全书内容由诸葛建伟进行全面、仔细的统稿与审校，并由陈爱华、陈建军、刘跃、崔丽娟进行了试读。本书翻译正值学校暑假，因此译者团队也都投入了充分的时间来保障翻译质量，仔细推敲和统一全书技术词汇的译法，确保对翻译内容的技术掌控，从而能够忠实地描述出原书作者期望传递给读者的知识与技能。

在翻译到前言部分，获知本书作者的成长经历以及对乡村学生所做的公益事

业，译者团队感同身受，三位译者中的两位也是从中国的农村地区成长起来的，也都还深刻地记忆着第一次接触到学习机和电脑时那种兴奋异常的感觉。在走向小康社会的今日中国，仍然有这样一个被社会边缘化的群体，他们渴望了解这个世界更多，渴望在互联网世界里遨游，但他们却因为贫困而无法跨越数字鸿沟。这就是农民工子弟学校计算机教育的现状，而在广大的农村地区，问题更加严重。1.5 亿农村中小学生，竟然有 77.3%从来没有见过电脑！但与此同时，我们看到，社会上存在着大量的废旧电脑资源，城市里每年淘汰的电脑就达 500 万台。

当你要淘汰掉手中“没有价值”的旧电脑，你能否记起那些求知若渴的孩子们？科技更新换代越来越快，许多旧电脑只要经过简单的整修，便可继续使用至少 2 年。

因此译者团队达成共识，将本书的公益特性进行到底，决定将本书的译者稿费捐赠给清华大学学生教育扶贫公益协会，通过@电脑传爱活动，将旧电脑维修之后，为打工子弟小学建立电脑室，将公益的精神传递下去。我们也非常欢迎读者能够参与公益事业，事实上，各位读者在购买本书的同时，就已经为公益做出了一份贡献。如果你愿意捐赠淘汰的电脑和计算机基础书籍，欢迎通过新浪微博@电脑传爱，也可以@清华诸葛建伟。如果你是高校学生，希望通过电脑维修做些公益并积累社会实践经验，也非常欢迎加入到@电脑传爱组织的高校电脑维修公益志愿者活动。

公益是举手投足之间的事，我们倡议，每个人为社会公益奉献一点点，让它汇成可以改变世界的力量！

电脑传爱行动

一台电脑开启一扇窗，一次行动传递一份爱！

清华大学教育扶贫电脑传爱公益活动，邀你同行。

诸葛建伟　陈霖　许伟林

2013 年 1 月于北京清华园

前　言

本书从 2009 年底开始编写，在 2011 年中期完成，总计历时一年半。而在本书出版之日，已经距离本书第 1 版发布的时间有 4 年之久。本书的所有内容几乎都经过了重写，并采用了完全重新设计的网络捕获数据包文件和场景。如果你喜欢本书第 1 版，那么你也会喜欢本书，因为本书采用了与第 1 版同样的写作方式，以一种简单容易理解的风格来展示技术。如果你不喜欢第 1 版，你也会喜欢本书，因为新版拥有全新设计的场景和扩展后的充实内容。

为什么购买本书

你一定很想知道为什么应该买这本书，而不是其他关于数据包分析的书籍。答案在于本书的书名：Practical Packet Analysis。让我们面对这样的现实——没有比实际的经验更加重要的了，而本书通过大量的真实场景中的数据包分析案例，让你获得最贴近实际的经验。

本书的前半部分将为你提供理解数据包分析技术和 Wireshark 软件的必备前置条件。后半部分则完全是一些你在日常网络管理中很容易遇到的一些实际案例。无论你是一位网络技术员、网络管理员、首席信息官、IT 技术支持，还是一位网络安全分析师，你都可以从本书描述的理解与使用数据包分析技术中

获得很多的收获。

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的随意，因此你可能比较容易在一些处理技术概念的行话中迷失，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，但你如果在本书中看到一些粗野的乡村土话，请务必原谅我。

如果你真地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，但你在学习本书后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个章节的主要内容。

- 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？本章将覆盖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"，本章将覆盖你在网络中放置数据包嗅探器时可以使用的各种不同技术方法。

- 第 3 章："Wireshark 入门"，从本章起，我们将开始进入 Wireshark 软件的世界，我们将介绍 Wireshark 软件的入门知识——哪里可以下载到，如何使用它，它完成什么功能，为什么它广受好评与关注，以及其他各种好东西。

- 第 4 章："玩转捕获数据包"，在你运行 Wireshark 软件之后，你会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。

- 第 5 章："Wireshark 高级特性"，一旦你已经学会了缓慢地爬行，那是时候来学习跑步了。本章将深入钻研 Wireshark 的高级特性，带你揭开引擎的盖子，来了解一些比较少见的操作。

- 第 6 章："通用底层网络协议"，本章将为你展示那些最常见的通用底层

网络通信协议——比如 TCP、UDP 和 IP——从数据包的层次上来看。为了解决这些网络协议中发生的故障，你首先需要理解它们是如何工作的。

- 第 7 章：“常见高层网络协议”，继续讲解网络协议的相关内容，本章将带你了解 3 种最为常见的高层网络通信协议——HTTP、DNS 与 DHCP——并从数据包的层次上来看。

- 第 8 章：“基础的现实世界场景”，这章中将包含一些常见的网络流量，以及最初的现实世界场景中的案例。每个案例将采用一种容易跟随的方式进行展示，包括问题、分析和解决方法。这些基础场景案例仅仅涉及到少量几台计算机，以及很少的分析——仅仅能够将你的脚打湿。

- 第 9 章：“让网络不再卡”，网络技术人员最普遍遇到的网络问题便是网络性能很慢的情况，本章便是专门为解决这一问题而设计的。

- 第 10 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问题，本章将带给你几个关于如何使用数据包分析技术解决安全相关问题的实际案例。

- 第 11 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，并包含了无线网络流量分析的几个案例。

- 附录 A：“延伸阅读”，本书附录给出了其他一些参考工具和网站列表，你可以从中找到继续使用你所学到的数据包分析技术的进一步资料。

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，你可以按一章接着一章的顺序阅读，来获得对数据包分析技术的理解与掌握。这种方式会特别关注后面几章中的现实世界场景案例。

- 作为一本参考索引资料，有些 Wireshark 软件的特性是你不会经常使用到的，所以你可能会忘记它们是如何工作的。数据包分析实用技术是你的书柜中一本非常有用的参考书，当你需要快速重温如何使用 Wireshark 软件的某个特

性时，你可以从本书中获得参考。我已经提供了很多独特的图表、图解和方法说明，已经被证明能够作为你进行数据包分析的有用索引参考。

关于示例网络数据包捕获文件

所有本书中使用的网络数据包捕获文件都在本书的官方网站（http://www.nostarch.com/packet2.htm[1]）下载到，为了最大化本书的价值，我强烈建议你下载这些文件，并在你学习每个真实案例时使用它们。

乡村科技基金会

在我编写本书的前言时，我无法不提及由数据包分析实用技术书籍而衍生出的这一美好事物。在本书第一版出版后不久，我创办了一个 501(c)(3)的非营利性组织，而这正是我最大梦想成为现实的巅峰时刻。

比起城市与市郊的学生们，乡村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）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，主要通过针对性的奖学金项目、社区参与计划，以及一些在乡村地区的科技促进与提倡项目来达成。我们的奖学金项目专门提供给生活在乡村，但对计算机技术拥有着热情并希望在这个方向得到进一步教育的学生们。我非常高兴地宣布本书所有的作者版税将提供给乡村科技基金会，用于设立这些奖学金。如果你需要了解更多关于乡村科技基金会的信息，或者想了解你如何可以参与贡献，请访问我们的网站 http://www.ruraltechfund.org/。

---

[1] 为了方便国内读者下载，将在 http://netsec.ccert.edu.cn/hacking/book/提供备份链接。——译者注

目　录