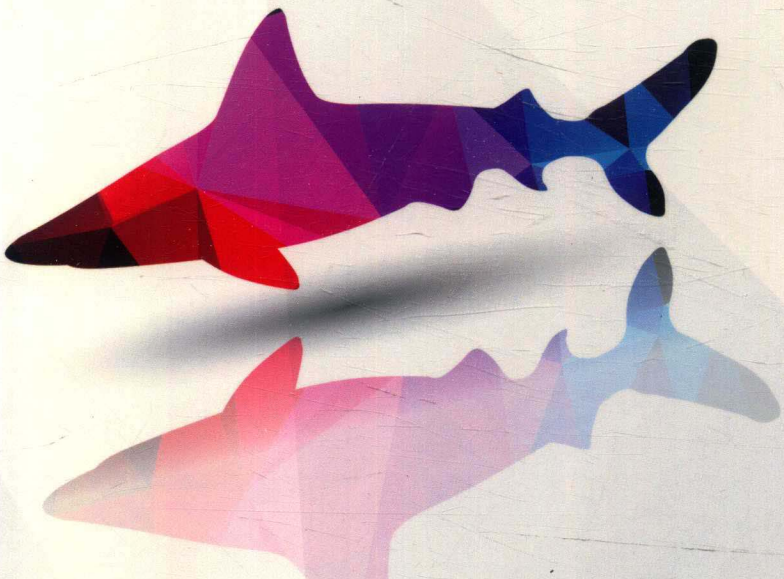
异步图书
www.epubit.com

Wireshark
网络分析从入门到实践

李华峰 陈虹 著

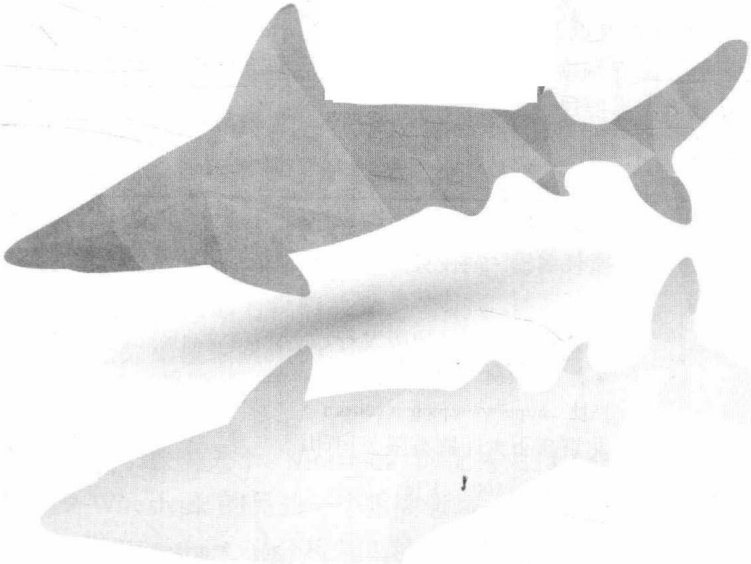
- 内容由浅入深，案例环环相扣，实用技巧“做中学”
- 配合虚拟环境，体验身临其境般的攻防演练
- 基于Lua扩展，探索Wireshark丰富多样的功能
- 完整的配套源码，精准复现书中的经典案例



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

Wireshark
网络分析从入门到实践

李华峰 陈虹 著



人民邮电出版社
北京

图书在版编目（CIP）数据

Wireshark网络分析从入门到实践 / 李华峰，陈虹著
. -- 北京 : 人民邮电出版社，2019.4
ISBN 978-7-115-50522-4

Ⅰ. ①W… Ⅱ. ①李… ②陈… Ⅲ. ①计算机网络－网络分析 Ⅳ. ①TP393.02

中国版本图书馆CIP数据核字(2018)第300061号

内 容 提 要

Wireshark 是一款开源网络协议分析器，能够在多种平台（例如 Windows、Linux 和 Mac）上抓取和分析网络包。本书将通过图文并茂的形式来帮助读者了解并掌握 Wireshark 的使用技巧。

本书由网络安全领域资深的高校教师编写完成，集合了丰富的案例，并配合了简洁易懂的讲解方式。全书共分 17 章，从 Wireshark 的下载和安装开始讲解，陆续介绍了数据包的过滤机制、捕获文件的打开与保存、虚拟网络环境的构建、常见网络设备、Wireshark 的部署方式、网络延迟的原因、网络故障的原因，并介绍了多种常见的攻击方式及应对策略，除此之外，本书还讲解了如何扩展 Wireshark 的功能以及 Wireshark 中的辅助工具。

本书实用性较强，适合网络安全渗透测试人员、运维工程师、网络管理员、计算机相关专业的学生以及各类安全从业者参考阅读。

◆ 著　　李华峰　陈　虹
责任编辑　胡俊英
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
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：17
字数：337 千字　　2019 年 4 月第 1 版
印数：1－2 400 册　　2019 年 4 月北京第 1 次印刷

定价：59.00 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

作者简介

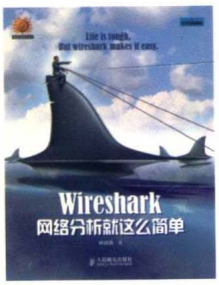
李华峰

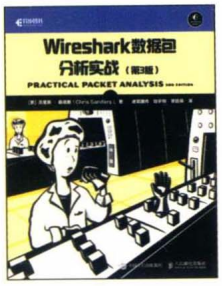
信息安全顾问和自由撰稿人，多年来一直从事网络安全渗透测试方面的研究工作。在网络安全部署、网络攻击与防御以及社会工程学等方面有十分丰富的实践经验。

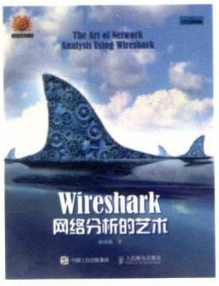
陈虹

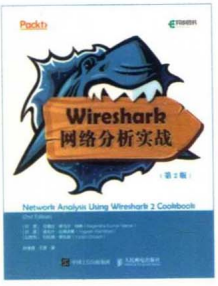
出身于美术专业的程序开发者。虽然在画室长大，却是实实在在的编程爱好者。目前正在从事软件设计工作。

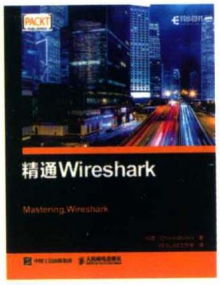
异步社区Wireshark好书推荐











前言

数百年前显微镜的发明为人类探索微观世界开启了一扇大门，而如今，Wireshark 的出现则为我们观察网络世界打开了另一扇大门。作为世界上最为流行的数据包分析软件，Wireshark 拥有着其他同类工具所不能比拟的强大优势。无论你是一个刚刚开始接触计算机网络知识的大学生，还是一个已经拥有多年从业经验的工程师，Wireshark 都可以为你带来极大的帮助。很多国内外的知名企业也将 Wireshark 的使用技能明确写入了招聘的要求之中。

在开始写作本书之前，我曾经翻译和编写了一些网络安全方面的书籍。这些书籍介绍了很多常见的网络攻击手段，读者在掌握了这些技能之后，大都对其实现细节产生了兴趣。例如到底为什么 Nmap 可以扫描出目标主机的状态，以及为什么中间人攻击就可以监听网络中的通信，泛洪攻击又是如何实现的呢？这些攻击的手段各种各样，实现这些攻击的工具也大都采用了不同的语言，这些都为我们的学习带来了很大的困难。不过，任何的网络攻击行为最终都是通过发送数据包来实现的，如果我们从数据包这个层次来分析问题，一切就会清晰起来。

虽然此前国内外已经有了很多关于 Wireshark 的优秀书籍，但是它们大都着眼于网络故障的排除，并没有涉及 Wireshark 的另外一个重要领域——网络安全。而本书以此作为研究的重点，讲述了如何使用 Wireshark 来分析常见的网络攻击手段，并根据它们的特点给出了解决方案。

目标读者

本书的目标读者如下：

- 网络安全渗透测试人员；
- 运维工程师；
- 网络管理员和企业网管；
- 计算机相关专业的学生；
- 网络安全设备设计与安全软件开发人员；
- 安全课程培训人员。

如何阅读本书

全书分为 6 个部分共 16 章，其中前 3 章为第 1 部分，主要讲解了 Wireshark 的基本使用方法；第 4 章～第 6 章为第 2 部分，主要讲解了 eNSP 的使用以及网络的一些知识。第 7 章和第 8 章为第 3 部分，讲解了常见网络故障的排除。而第 9 章～第 15 章为本书最为重要的部分，主要讲解了如何使用 Wireshark 来分析各种常见的网络攻击，这些内容按照链路层、网络层、传输层和应用层这个顺序来介绍。最后两章讲解了一些 Wireshark 的扩展功能和辅助工具。

第 1 章“走进 Wireshark”，这一章对 Wireshark 的功能和工作原理进行了简单的介绍，然后讲解了 Wireshark 的下载和安装过程。本章最后演示了一个 Wireshark 的使用实例，这个实例虽然很简单，但是却包含了完整的使用过程。

第 2 章“过滤无用的数据包”，详细地讲解了 Wireshark 中对数据包的过滤机制，这里面包括捕获过滤器和显示过滤器的使用方法。

第 3 章“捕获文件的打开与保存”，讲解了 Wireshark 中的各种保存功能，包括对数据包捕获文件保存位置和格式的设置，对过滤器的保存，对配置文件的保存。

第 4 章“虚拟网络环境的构建”，讲解了 eNSP 和 VMWare 两种工具的使用。在它们的帮助下，我们可以模拟出各种和真实环境一模一样的网络结构，并以此来进行练习。

第 5 章“各种常见的网络设备”，介绍了网络中常见的几种硬件，并给出了一些实例。

了解这些硬件可以更好地帮助我们使用 Wireshark。

第 6 章“Wireshark 的部署方式”，讲解了如何在各种网络情况下进行 Wireshark 的部署。

第 7 章“找到网络发生延迟的位置”，从这一章起我们开始了对网络实际问题的分析。本章就延迟位置的确定进行了讲解，并在这个实例中穿插讲解了 Wireshark 中的时间设置。

第 8 章“分析不能上网的原因”，在这一章中，我们就“不能上网”这个问题进行了分析，在问题分析过程中使用到了很多 Wireshark 的技巧。

第 9 章“来自链路层的攻击——失常的交换机”，从这一章起，我们开始了对网络安全问题的分析。围绕着交换机面临的典型攻击手段——Mac 泛洪攻击，给出了详细的介绍。首先从一个案例开始，对案例中的数据包文件进行了分析和总结，进一步得出了这种攻击的特点，最后给出了这种攻击手段的实现和解决方案。

第 10 章“来自网络层的欺骗——中间人攻击”，对第 ARP 欺骗技术进行了讲解。ARP 欺骗技术是中间人攻击的实现基础，这一章从 ARP 欺骗的原理开始讲解，并在 Wireshark 的帮助下对 ARP 欺骗进行了深入的分析。同时还介绍了 Wireshark 中的强大工具——专家系统的使用方法。最后给出了如何完成 ARP 欺骗，以及如何防御这种攻击的方法。

第 11 章“来自网络层的攻击——泪滴攻击”，讲解了针对 IP 协议的一种典型攻击手段：泪滴攻击。首先讲解了 IP 协议的格式，然后介绍了 IP 协议的一个重要概念：分片。同时也详细讲解了基于这种技术的攻击手段——泪滴攻击。这一章还介绍了 Wireshark 的着色规则，只需查看数据包的颜色，就可以判断出它的类型。在本章的最后，介绍了 IP 协议头中一个很有用的字段 TTL。

第 12 章“来自传输层的洪水攻击（1）——SYN Flooding”，介绍了针对服务器的攻击方式——SYN Flooding 攻击。并在 Kali Linux2 平台中演示了如何进行这种攻击，同时也使用 Wireshark 的流量图对这种攻击进行了分析。

第 13 章“网络在传输什么——数据流功能”，在这一章中，介绍了 TCP 数据的传输，并详细讲解了 Wireshark 中的数据流功能，利用这个功能可以监控整个网络中传输的文件。本章最后给出了一个非常优秀的 Wireshark 学习资源。

第 14 章“来自传输层的洪水攻击（2）——UDP Flooding”，这一章讲解了 UDP Flooding 攻击的原理与实现方法，并使用 Wireshark 中的图表功能对这种攻击的技术进行了分析。最后重点介绍了 Wireshark 中自带的图表功能以及 amCharts 的使用方法。

第 15 章“来自应用层的攻击——缓冲区溢出”，这一章介绍了一种全新的攻击方式——缓冲区溢出，它的攻击建立在应用层的协议上。本章首先介绍了 HTTP 协议，然后模拟了

一次缓冲区溢出的攻击过程。在这个实例中还介绍了数据包的查找功能。在最后介绍了如何使用 Wireshark 来分析 http 协议的升级版 https 协议。

第 16 章“扩展 Wireshark 的功能”，这一章介绍了如何在 Wireshark 中编写插件，这个功能在实际应用中相当有用，相关的实例都采用了 Lua 语言编写。

第 17 章“Wireshark 中的辅助工具”，介绍了 Wireshark 中常见的各种工具，包括 Tshark、Dumpcap、Editcap、Mergecap、Capinfo 和 USBPcapCMD 等工具的功能和使用方法。

大家可以根据自己的需求选择阅读的侧重点，不过我还是推荐按照顺序来阅读，这样可以对 Wireshark 的使用有一个清晰的认识，同时也可以深入了解网络中常见的攻击方法。

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

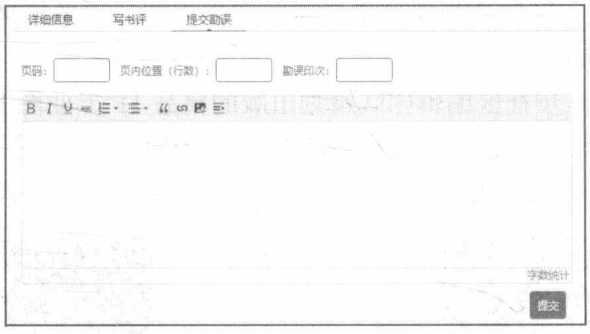
本书提供配套代码资源，要获得该配套资源，请在异步社区本书页面中点击 配套资源，跳转到下载界面，按提示进行操作即可。注意：为保证购书读者的权益，该操作会给出相关提示，要求输入提取码进行验证。

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

目录

第 1 章
走进 Wireshark

在 1000 多年前的唐代，高僧玄奘为了探究佛教各派学说的分歧，独自一人西行了五万里到达印度那烂陀寺，将 600 多部经书带回了中国，期间共经历了 17 年。而在进入工业时代之后，从北京乘坐飞机到达新德里只需要 7 小时。在互联网时代的今天，如果将这些经书以计算机数据的形式存储起来，那么只需要在几秒（甚至更短），就可以将它们通过网络从新德里传输到北京。

网络的出现改变了我们的工作和生活方式。可以这样说，我们无时无刻都离不开网络，它已经像电力一样成为了这个世界不可或缺的资源之一。但是在享受着网络带来便利的同时，却很少有人关心其中的运行机制，当然人们也无法用肉眼观察到网络世界。

因此，当你希望能够深入地了解网络，一个可以观察到它内部活动的“显微镜”将会是必不可少的。目前世界上可以实现这种功能的“网络显微镜”其实有很多，如果你听过著名的哈佛大学公开课《计算机科学 cs50》的话，那么一定会注意到 David J. Malan 在上课时使用的 TcpDump，这就是一个很受欢迎的“网络显微镜”。另外比较著名的例如 Sniffer、Ethereal 和 Wireshark 等，它们都曾经或者正在人们对网络世界的观察中起着重要的作用。不过，本书要介绍的并非 TcpDump，因为它没有尽如人意的图形化操作界面。而 Wireshark 则在拥有了 TcpDump 的各种优势的同时，还弥补了 TcpDump 的这个缺陷，成为了当前最为流行的网络分析工具。在本书中，我们将在 Wireshark 的帮助下来体验网络世界的神奇。

在本章中，我们先来简单地了解 Wireshark，这部分内容将会围绕以下几个主题展开：

- Wireshark 是什么；
- Wireshark 是如何工作的；
- 如何下载和安装 Wireshark；