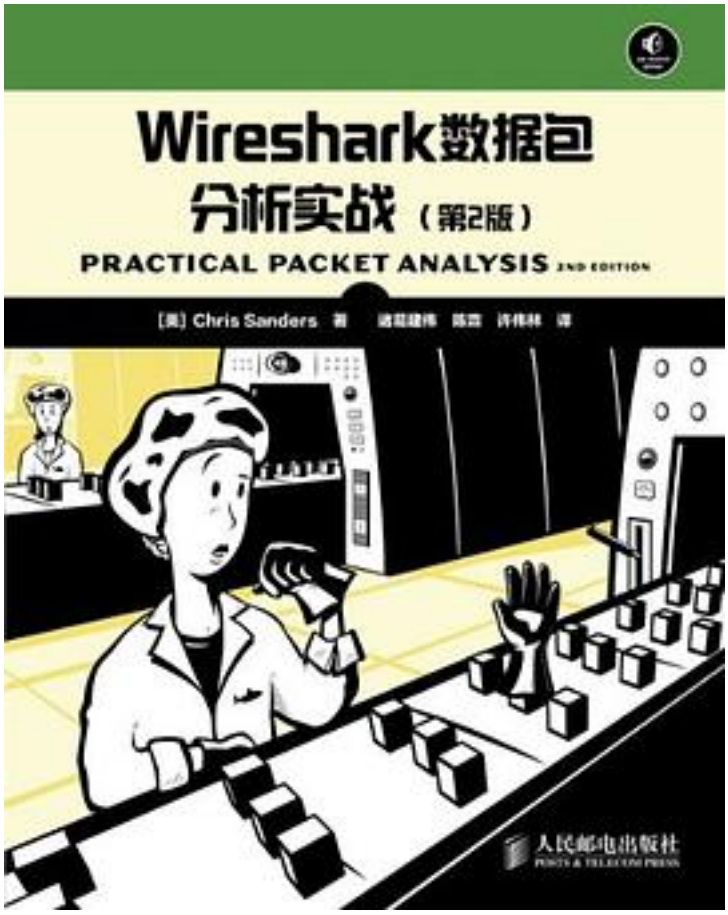
Wireshark数据包分析实战



Wireshark数据包分析实战_下载链接1_

著者:[美]Chris Sanders

出版者:人民邮电出版社

出版时间:2013-3

装帧:平装

isbn:9787115302366

《Wireshark数据包分析实战(第2版)》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，《Wireshark数据包分析实战(第2版)》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。《Wireshark数据包分析实战(第2版)》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。

《Wireshark数据包分析实战(第2版)》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。

作者介绍:

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。

目录: 目 录

・・・・・・・(收起)

Wireshark数据包分析实战_下载链接1_

标签

wireshark

网络分析

网络

抓包

TCP/IP

计算机网络

网络安全

计算机

评论

: TP393.09/7924

其实都可以当一本不错的计算机网络科普书了。因为围绕“抓包”话题，实操性也很强。对 TCP
拥塞控制的介绍尤其超预期。不过最后实操分析浏览器流量的章节有点过时，几个范例

网站都已经全面 HTTPS，书中并没有介绍如何做中间人证书，或者利用 Firefox 的开发者功能分享 TLS master key 给 Wireshark。

入门过一遍

入门书籍。推荐。后期应该再搭配一本wireshark工具书类型的，如cookbook

200多页的小书花专门两章讲 tcp/ip 协议栈基本原理是不是太奢侈了，集中讲 wireshark 就好了嘛

文章后面有一些攻击分析和参考资源。

思路和结构十分清晰，第一版的书评说：“各层次网络管理员必备手册。”“新手入门的最佳读物！”，说的没错。更难得的是，翻译的非常好。
没什么好怕的，都只是一些数据包而已。

好玩，用Wireshark发现：当用网易邮箱大师登陆浙大邮箱的时候，可以抓到一个包，里面有明文的密码哈哈哈。看来邮箱大师和我校邮箱都不怎么样惹

讲的比较初级，工具这东西，还是要遇到问题实际去使用才能掌握

抓包经典

当用户手册看的，内容真的没什么，挺一般的吧

偏基础的入门科普书

抓包工具书

工具书

中文版的就是快 用了两个半天的实习时间就给finish了
基本对wireshark有了框架性的了解 还是要实践才行
不过感觉网络安全的大门就此打开了 日语也可以和几个日本哥们练习 实习还是不错的
虽然很辛苦 论文压力很大 但是实习真的受益颇丰 因为只有少许补助
所以心里上的压力算是没有的 接下来要好好读英文版的了

内容太少

流量题实在做不下去了回头补基础。还挺好的，对数通一窍不通的人也能够一口气阅读。看完之后就开始刷题啦！

1~7

好书，必读

最后两章没看，算是复习了一下计网的基本原理。第8章喜欢，跟破案故事一样哈哈哈。

Wireshark数据包分析实战_下载链接1_

书评

首先说这本啦： http://book.douban.com/subject/21691692/
初学者必备，介绍了wireshark安装，嗅探网络流量，wireshark的基本使用，用wireshark分析了一圈常用的TCP，UDP协议，也简要分析了HTTP等应用层协议，概要介绍了一些TCP重传的机制，最后是无线分析 整个书定位应该是...

如果你手头宽裕，又想学习wireshark细节功能的话，这本书还是值得买的。
关于wireshark监控网络流量作图问题，想来很多人都问过。这本书给出了作图的实例。 TCP专家信息也有一些有用的监控。

这主要是一本工具书，可以在忘记怎么使用的时候翻翻，比起看英文的帮助文档会快一些。
内容主要涉及：计算机网络的基础知识、如何在合理的位置抓包、wireshark配置、各种协议的数据格式以及它们在wireshark上的样子、最后两章节涉及到了网络安全、无线抓包。书中也有很...

值得购买 《wireshark 数据包分析实战》主要介绍了如何使用 wireshark
分析网络数据。该书既介绍了 wireshark
捕获捕获、保存、分析数据包的基本操作，也介绍了使用 wireshark 中 analysis 和 statics 分析网络情况的高级用法。既有 eth、arp、ip、tcp、udp、dns 等网络协议的...

Wireshark数据包分析实战_下载链接1_