<<Wireshark数据包分析实战>>

图书基本信息

书名：<<Wireshark数据包分析实战>>

13位ISBN编号：9787115302366

10位ISBN编号：7115302367

出版时间：2013-3

出版时间：人民邮电出版社

作者：Chris Sanders

译者：诸葛建伟,陈霖,许伟林

<<Wireshark数据包分析实战>>

内容概要

《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。

作者简介

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。

<<Wireshark数据包分析实战>>

书籍目录

章节摘录

版权页： 插图： SYN数据包没有得到响应，这告诉我们总部和分公司DNS服务器之间区域传送失败导致了DNS故障。
现在我们可以进一步找出区域传送失败的原因。
办公室之间的路由器或中心办公室的DNS服务器可能是罪魁祸首。
为了找出问题，我们可以嗅探中心办公室DNS服务器的流量，看看SYN数据包是不是到达了服务器。
我没有给出中心办公室DNS服务器的流量捕获文件，因为根本就没有。
SYN数据包从来没有到达服务器。
派遣技术人员查看连接两个办公室的路由器配置后，我们发现中心办公室的路由器被配置成只允许53端口的UDP流量进入，而53端口的TCP流量则被阻止了。
这个简单的配置错误阻止了服务器间的区域传送，从而导致分支办公室的客户端无法解析对中心办公室设备的查询。
3.学到的知识 看完这个“犯罪剧”，你一定学到了很多关于调查网络通信问题的知识。
当“犯罪”发生后，侦探开始问讯受害者。
找到线索，顺藤摸瓜，直到找到罪魁祸首。
在这个场景中，我们一开始先查看了受害者（工作站），然后找到了DNS通信问题这个线索。
这个线索将我们带到分支DNS服务器，然后又到中心DNS服务器，最终找到路由器，也就是问题的来源。
在分析时，请尝试从数据包中找出线索。
线索不一定能告诉你谁是“罪犯”，但通常它们最终能帮你找出来。
8.3.6生气的开发者 在IT界，开发者和系统管理员经常争吵。
开发者总是将程序故障归咎于糟糕的网络设置和设备。
系统管理员则倾向于把网络错误和网络缓慢归咎于糟糕的代码。
在这个场景中，程序员开发了一个应用程序，用于跟踪多个商店的销售并报告回中心数据库。
为了节约正常工作时间的带宽，他没有设计成实时应用程序。
而是等报告数据累积一天后，才在晚上以逗号分隔值（comma—separatedvalue，简称CSV）文件的形式传回，插入中心数据库中。
然而，这个新开发的应用程序工作不太正常。
服务器接收到了各个商店传回的文件，但插入数据库的数据是错误的。
一些地区的数据丢失了，有的数据还存在错误，而且文件某些部分还丢失了。
系统管理员很烦恼，因为程序员抱怨这是网络的问题。
程序员一口咬定文件在从商店传到中心数据库时被损坏了。
我们就要证明他是错的。
1.侦听线路 为了收集所需数据，我们可以在其中一个商店或中心办公室捕获数据包。
故障影响到了所有商店，因此如果这确实是网络导致的问题，那肯定是在中心办公室那边——它是所有商店通信的汇聚点。

媒体关注与评论

“各层次网络管理员的必备手册。
”—Linux Pro杂志“一本优秀、易懂且具有良好格式的Wireshark实用指南。
”—ARSGEEK.COM“如果您需要掌握数据包分析的基础知识，本书将是您起步的好地方。
”—STATEOFSECURITY.COM“本书能够让您有一技之长，它抓住了书名中的关键词—实用，很好地为读者们提供了进行数据包分析所需要知道的基本知识，然后又恰如其分地带领他们进入到使用Wireshrak软件解决现实问题的缤纷世界中。
”—LINUXSECURITY.COM“您的网络中有未知主机在和其他主机聊天吗？
您的电脑是否在和陌生人说话？
您需要一个数据包嗅探器来找出这些问题的真正答案。
Wireshark是能够完成这件事情的最佳工具，而本书是学习这个工具最好的方式之一。
”—自由软件杂志“新手入门的最佳读物！
”—DAEMON NEWS

<<Wireshark数据包分析实战>>

编辑推荐

《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)》是国内第一本，也是唯一的一本Wireshark图书；它通过示例捕获文件来讲解Wireshark的应用，是黑帽/白帽/灰帽和安全技术从业人员的必读读书。
　　《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。

<<Wireshark数据包分析实战>>

版权说明