

<<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

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<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。

<<Wireshark数据包分析实战>>

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

第1章数据包分析与网络基础 1.1数据包分析与数据包嗅探器 1.1.1评估数据包嗅探器 1.1.2数据包嗅探器工作原理 1.2网络通信原理 1.2.1协议 1.2.2七层OSI参考模型 1.2.3数据封装 1.2.4网络硬件 1.3流量分类 1.3.1广播流量 1.3.2多播流量 1.3.3单播流量 1.4小结 第2章监听网络线路 2.1混杂模式 2.2在集线器连接的网络中进行嗅探 2.3在交换式网络中进行嗅探 2.3.1端口镜像 2.3.2集线器输出 2.3.3使用网络分流器 2.3.4ARP欺骗 2.4在路由网络环境中进行嗅探 2.5部署嗅探器的实践指南 第3章Wireshark入门 3.1Wireshark简史 3.2 Wireshark的优点 3.3安装Wireshark 3.3.1在微软Windows系统中安装 3.3.2在Linux系统中安装 3.3.3在Mac OS X系统中安装 3.4 Wireshark初步入门 3.4.1第一次捕获数据包 3.4.2Wireshark主窗口 3.4.3Wireshark首选项 3.4.4数据包彩色高亮 第4章玩转捕获数据包 4.1使用捕获文件 4.1.1保存和导出捕获文件 4.1.2合并捕获文件 4.2分析数据包 4.2.1查找数据包 4.2.2标记数据包 4.2.3打印数据包 4.3设定时间显示格式和相对参考 4.3.1时间显示格式 4.3.2数据包的相对时间参考 4.4设定捕获选项 4.4.1捕获设定 4.4.2捕获文件设定 4.4.3停止捕获选项 4.4.4显示选项 4.4.5名字解析选项 4.5使用过滤器 4.5.1捕获过滤器 4.5.2显示过滤器 4.5.3保存过滤器 第5章Wireshark高级特性 5.1 网络端点和会话 5.1.1查看端点 5.1.2查看网络会话 5.1.3使用端点和会话窗口进行问题定位 5.2基于协议分层结构的统计数据 5.3名字解析 5.3.1开启名字解析 5.3.2名字解析的潜在弊端 5.4协议解析 5.4.1更换解析器 5.4.2查看解析器源代码 5.5跟踪TCP流 5.6数据包长度 5.7图形展示 5.7.1查看IO图 5.7.2双向时间图 5.7.3数据流图 5.8专家信息 第6章通用底层网络协议 6.1地址解析协议 6.1.1 ARP头 6.1.2数据包1：ARP请求 6.1.3数据包2：ARP响应 6.1.4无偿的ARP 6.2互联网协议 6.2.1 IP地址 6.2.2IPv4头 6.2.3存活时间 6.2.4IP分片 6.3传输控制协议 6.3.1TCP头 6.3.2TCP端口 6.3.3TCP的三次握手 6.3.4TCP终止 6.3.5TCP重置 6.4用户数据报协议 6.5互联网控制消息协议 6.5.1ICMP头 6.5.2ICMP类型和消息 6.5.3Echo请求与响应 6.5.4路由跟踪 第7章 常见高层网络协议 7.1动态主机配置协议DHCP 7.1.1DHCP头结构 7.1.2DHCP续租过程 7.1.3DHCP租约内续租 7.1.4DHCP选项和消息类型 7.2域名系统 7.2.1DNS数据包结构 7.2.2一次简单的DNS查询过程 7.2.3DNS问题类型 7.2.4DNS递归 7.2.5DNS区域传送 7.3超文本传输协议 7.3.1使用HTTP浏览 7.3.2使用HTTP传送数据 7.4小结 第8章基础的现实世界场景 8.1数据包层面的社交网络 8.1.1捕获Twitter流量 8.1.2捕获Facebook流量 8.1.3比较Twitter和Facebook的方法 8.2捕获ESPN.com流量 8.2.1使用会话窗口 8.2.2使用协议分层统计窗口 8.2.3查看DNS流量 8.2.4查看HTTP请求 8.3现实世界问题 8.3.1无法访问Internet：配置问题 8.3.2无法访问Internet：意外重定向 8.3.3无法访问Internet：上游问题 8.3.4打印机故障 8.3.5分公司之困 8.3.6生气的开发者 8.4小结 第9章让网络不再卡 9.1 TCP的错误恢复特性 9.1.1TCP重传 9.1.2TCP重复确认和快速重传 9.2 TCP流控制 9.2.1调整窗口大小 9.2.2用零窗口通知停止数据流 9.2.3TCP滑动窗口实战 9.3从TCP错误控制和流量控制中学到的 9.4定位高延迟的原因 9.4.1正常通信 9.4.2慢速通信——线路延迟 9.4.3慢速通信——客户端延迟 9.4.4慢速通信——服务器延迟 9.4.5延迟定位框架 9.5网络基线 9.5.1站点基线 9.5.2主机基线 9.5.3应用程序基线 9.5.4基线的其他注意事项 9.6小结 第10章安全领域的数据包分析 10.1 网络侦察 10.1.1SYN扫描 10.1.2操作系统指纹术 10.2漏洞利用 10.2.1极光行动 10.2.2ARP缓存中毒攻击 10.2.3远程访问特洛伊木马 10.3小结 第11章无线网络数据包分析 11.1物理因素 11.1.1一次嗅探一个信道 11.1.2无线信号干扰 11.1.3检测和分析信号干扰 11.2无线网卡模式 11.3在Windows上嗅探无线网络 11.3.1 配置AirPcap 11.3.2使用AirPcap捕获流量 11.4在Linux上嗅探无线网络 11.5 802.11数据包结构 11.6在Packet List面板增加无线专用列 11.7无线专用过滤器 11.7.1筛选特定BSS ID的流量 11.7.2筛选特定的无线数据包类型 11.7.3筛选特定频率 11.8无线网络安全 11.8.1成功的WEP认证 11.8.2失败的WEP认证 11.8.3成功的WPA认证 11.8.4失败的WPA认证 11.9小结 附录A延伸阅读

<<Wireshark数据包分析实战>>

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-separated value，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。

<<Wireshark数据包分析实战>>

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Wireshark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

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>