信息安全技术丛书

PACKT PUBLISHING

Wireshark 网络分析实战

Network Analysis Using Wireshark Cookbook

[以色列] Yoram Orzach 著
古宏霞 孙余强 译

人民邮电出版社
POSTS & TELECOM PRESS

信息安全技术丛书

Wireshark 网络分析实战

Network Analysis Using Wireshark Cookbook

[以色列] Yoram Orzach 著
古宏霞 孙余强 译

人民邮电出版社
北京

图书在版编目（CIP）数据

Wireshark网络分析实战 /（以）奥扎赫(Orzach,Y.）著 ；古宏霞，孙余强译. -- 北京 ：人民邮电出版社，2015.2
ISBN 978-7-115-37771-5

Ⅰ. ①W… Ⅱ. ①奥… ②古… ③孙… Ⅲ. ①计算机网络—通信协议 Ⅳ. ①TN915.04

中国版本图书馆CIP数据核字(2014)第297046号

版权声明

◆ 著 [以色列] Yoram Orzach
译 古宏霞 孙余强
责任编辑 傅道坤
责任印制 张佳莹 彭志环
◆ 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
三河市中晟雅豪印务有限公司印刷
◆ 开本：800×1000 1/16
印张：26.75
字数：583 千字 2015 年 2 月第 1 版
印数：1-3 000 册 2015 年 2 月河北第 1 次印刷
著作权合同登记号 图字：01-2013-9040 号
定价：79.00 元
读者服务热线：(010) 81055410 印装质量热线：(010) 81055316
反盗版热线：(010) 81055315

内容提要

本书采用步骤式为读者讲解了一些使用 Wireshark 来解决网络实际问题的技巧。

本书共分为 14 章，其内容涵盖了 Wireshark 的基础知识，抓包过滤器的用法，显示过滤器的用法，基本/高级信息统计工具的用法，Expert Info 工具的用法，Wiresahrk 在 Ethernet、LAN 及无线 LAN 中的用法，ARP 和 IP 故障分析，TCP/UDP 故障分析，HTTP 和 DNS 故障分析，企业网应用程序行为分析，SIP、多媒体和 IP 电话，排除由低带宽或高延迟所引发的故障，认识网络安全等知识。

本书适合对 Wireshark 感兴趣的网络从业人员阅读，也适合高校网络相关专业的师生阅读。

关于作者

Yoram Orzach 毕业于色列技术学院（Israel Institute of Technology），持有该校科学学士学位。1991～1995 年，他以系统工程师的身份就职于 Bezeq 公司，从事传输及接入网相关的工作。1995 年，他从 Leadcom 集团（Leadcom group）加盟 Netplus 公司，并转型为技术管理者。自 1999 年起，他开始担任 NDI 通信公司（NDI Communications，http://www.ndi-com.com/）的 CTO，负责并参与该公司在全球范围内的数通网络的设计、实施及故障排除工作。Yoram 对大型企业网络、服务提供商网络及 Internet 服务提供商网络极有心得，Comverse、Motorola、Intel、Ceragon Networks、Marvel 以及 HP 等公司都接受过他提供的服务。Yoram 在网络设计、实施及故障排除方面浸淫多年，在研发（R&D）、工程、IT 团队的培训方面也有丰富的经验。

致 谢

首先，要感谢我的全家。感谢我的父母：我的父亲 Israel——世上独一无二的智者——全家遇难，他以 35 公斤的瘦弱之躯只身从（纳粹针对犹太人的）大屠杀中脱生，40 年后，他成为了电信行业首屈一指的专家；我的母亲 Selma 则教会我很多。感谢我贤惠的妻子 Ena，谢谢你过去 20 多年来在工作以及其他方面给我的支持。感谢我的孩子 Nadav、Dana 和 Idan，你们的成就让老爸自愧不如。感谢我的妹妹 Hana、妹夫 Ofer 以及我的外甥们。

要感谢我的诸多同事。最先应该感谢 Reuven Matzliach，20 世纪 90 年代末，他和我在 Comverse 公司开始筹建 IP 培训中心（IP college），并促成了该公司的网络从 TDM 向 IP 转型。在转型期间，他多次助我渡过难关。同样要感谢 Omer Fuchs 和 Moshe Sakal ，感谢二位在那个大项目里给我的帮助。我还要感谢其他同事及朋友，只是人名太多无法一一列出。

要感谢 Lior Tzuberi，感谢你提供的诸多 WireShark 使用技巧及研究案例。要感谢 Hanan Man，感谢你那个有趣的网络设计。要感谢 Yoel Saban 和 Rami Kletshevsky，感谢你们所奉献的诸多经典的网络设计，你们的设计团队是我见过的最出色的团队之一。要感谢 Zvi Shacham，感谢你传授给我的数通网络的经验。要感谢 Asi Alajem，感谢你那个很有意思的网络设计；感谢 Oren Gerstner，感谢你提供的若干经典的无线网络案例。感谢 Chen Heffer，你是我所认识的最最出色的网络安全专家。要感谢 Yoni Zini，感谢你在系统方面给我提供的帮助。感谢 Ibrahim Jubram，感谢你奉献的那些精彩的移动网络案例。感谢 Ofer Sela，感谢我们一起参与的那些非常有意思的项目。感谢 Amir Lavi 和 Eran Niditz，感谢你们提供的那些趣味横生的案例。感谢 Avner Mimon，感谢你提供的诸多绝佳的 WireShark 使用技巧。此外，还要感谢许许多多的其他人。

我要感谢教会我诸多网络技能的培训专家。30 年前，我曾以为给人上课也就是图一乐；是你们让我懂得，培训也是一种职业。我要感谢 Harriet Rubin、Merav Sagi、Rvital Keinan、Guy Einav、Raanan Dagan 以及其他许许多多的培训专家们。

我要特别感谢 Yoav Nokrean 跟他的儿子 Eran，要感谢你们给我出的那些主意，以及对我全方位的支持。

我还要感谢曾与我朝夕相处的诸位前同事；感谢以色列、欧洲、北美、东亚以及世界其他各地的客户。排除网络故障的手法总是千篇一律，而屋外的风景则十里不同天。

尤其要感谢某些设计出垃圾网络的网络设计“专家”、捣鼓出离奇 TCP/IP 实现的协议开发人员，以及连线缆都能接错的 IT 运维人员，外加那些以为设备只要接上线缆便能正常运行的 IT 施工部门。解决由那些“挫人”、“挫事”引起的故障是学习网络技术的最佳途径。

要感谢我教过的学生们，感谢你们问我的所有刁钻问题，以及带来的有意思的网络案例；每一次给你们上课我都能从中获益。我真不知道还有什么事能比把笔记本电脑连接进真实的网络，解决故障更有意思了。

要感谢我所钦佩的一干网络及安全界的前辈——Vint Cerf、Bob Kahn、Radia Perlman、Adi Shamir、Ronald Rivest、Van Jacobson、Steven McCanne 等。没有你们，哪来今天的一切。

最后，要感谢 Packt Publishing 出版社能有出版以 Wireshark 为主题的图书的意愿，并包容我完成本书的写作。

关于技术审稿人

Charles L. Brooks 是 Security Technical Education 公司的创始人和首席咨询顾问，该公司的业务都与 IT 技术有关，包括 IT 图书的创作和评论、IT 培训和教案设计等。Charles 还在积极推广由波士顿大学开办的数据通信及网络技术方面的远程教育课程，并且在布兰代斯大学教授网络安全、软件开发安全、虚拟化安全以及云计算基础架构等方面的课程，在拉布研究生专业进修学院教授信息安全编程（涉及 MS 操作系统）方面的课程。创办 Security Technical Education 公司（`www.securityteched.com`）之前，Charles 在 EMC 和 RSA 公司任高级技术教育顾问一职，负责存储安全、大数据、网络安全分析及网络取证等主题的课件开发。加盟 EMC 公司之前，Charles 曾干过许多年的软件工程师、团队组长（team leader）以及软件架构师；最近，他还作为 GTE Internetworking and Genuity 公司的系统工程师，负责管理该公司所提供的 VPN 业务。

Charles 握有克拉克大学英语专业的学士和硕士学位、波士顿大学计算机信息系统科学专业的硕士学位，以及包括 CISSP、CEH 和 CHFI 在内的多张行业证书。

我要感谢 Helyn Pultz，感谢她这么多年来的鼓励、支持和忠告。

Praveen Darshanam 在 McAfee、Cisco 及 iPolicy Networks 公司任职多年，有 7 年以上的信息安全方面的经验。他的强项和兴趣包括：漏洞研究、（病毒或木马）特征的研究、Snort、应用程序安全，以及恶意软件分析等。他持有电子工程（EE）专业的学士学位和控制及仪表专业的硕士学位；他的学士学位获取自印度最好的学府之一。他还拥有包括 CHFI、CEH 和 ECSA 在内的多张行业证书。

Ritwik Ghoshal 是 Oracle 公司资深的安全分析师，负责 Oracle 公司的软、硬件安全性保障工作。他的工作范围包括网络安全、操作系统安全和虚拟化安全等。他于 2008 年加入 SUN 公司，在 2010 年为 Oracle 公司效力之前（Oracle 公司在那一年收购了 SUN 公司），他一直是 SUN 公司安全工程团队和 Solaris 团队的成员。在 Oracle 公司，Ritwik 继续负责所有 Sun 产品线以及 Oracle Linux 和虚拟化产品线的安全性保障工作。

Ritwik 于 2008 年获取了 Heritage Institute of Technology（印度加尔各答）计算机科学与工程专业的学士学位。

我要感谢我的父母以及 Sara E Taverner，感谢你们对我持续的帮助与支持。

Gilbert Ramirez 自 Wireshark 第一版发布之日起，就是该软件的贡献者。他为该软件添加了协议剖析模块和某些关键组件（比如，显示过滤引擎等），同时为 Wireshark 向 Windows 平台的移植做出过贡献。他目前供职于 Cisco 公司，负责软件系统及软件工具的构建。

Gilbert 是多本 Wireshark 主题书籍的作者，包括 *Wireshark & Ethereal Network Protocol Analyzer Toolkit*、*Ethereal Packet Sniffing* 以及 *Nessus, Snort, & Ethereal Power Tools* 等，这些书籍均由 Syngress Publishing Inc.出版社出版。

前 言

Wireshark 早已成为网络分析领域里的标配工具，随着 Internet 和 TCP/IP 网络的极速发展，该工具会受到网络分析专家及排障工程师的热捧，同时也会获得（网络协议或应用程序）研发工程师们的青睐，因为后者需要知道协议在网络中的实际运作方式以及在运行时所碰到问题。

本书的写作立足于实战。本书第 1 部分（从第 1 章到第 6 章）简要介绍了 Wireshark 软件（的架构）及其各个组件的使用方法。这部分的内容包括 Wireshark 的启动方法、在网络中的安置方法、信息统计（statistical）工具的使用方法以及专家（Expert）系统的使用方法。本书第 2 部分（从第 7 章到第 14 章）详述了如何使用 Wireshark 来分析并排除某些常用网络协议的故障；TCP/IP 协议栈（特别是 TCP 性能问题）是这部分的重点内容。此外，还会简要介绍 HTTP、SMTP、POP 以及 DNS 等协议，外加数据库、Citrix 和 Microsoft 终端服务器、IP 电话以及多媒体应用所使用的协议，以上协议都属于常用的 Internet 协议。本书最后一章（第 14 章）涉及网络安全，介绍了如何利用 Wireshark 去发现网络中的安全缺陷，同时交代了与安全性有关的其他问题。

本书的书名既然叫《Wireshark 网络分析实战》，那么其内容一定是由一系列利用 Wireshark 对网络故障进行有效性、针对性分析的诀窍所构成。书中包含的每个诀窍都与某一具体的网络故障相关联，在介绍如何使用 Wireshark 解决相关故障时，作者会指出应关注 Wireshark 工具的哪些地方、哪些（抓包）内容以及正在处理的故障的起因。为求表述圆满，每个诀窍都会包含相应主题的理论基础知识，好让尚未掌握基础概念的读者先行“武装”自己。

书中包含了许多示例，所有示例均来源于真实案例。作者在处理这些案例时，所花费的时间虽长短不一（有些只花了几分钟时间，有些则要花几小时甚至几天），但所遵循的原则只有一条，那就是：按部就班，选择正确的工具，当应用程序开发者肚里的“蛔虫”，外加从网络的角度思考问题。只要按此原则行事，兼之能活学活用 Wireshark，定能将故障查个水落石出。本书的目的也正在于此，享受这一切吧。

本书所含内容

第 1 章，Wireshark 简介，开启了对 Wireshark 的简要介绍，同时阐述了在有效开展网络分析时，Wireshark 主机（或程序）的布放（或安装）位置问题。在本章，读者会学到如何配置 Wireshark 的基本（运行）参数、启动窗口、时间参数及配色规则（coloring rules），但本章

的重点内容是如何配置首选项窗口（Preferences window）。

第 2 章，抓包过滤器的用法，介绍了抓包过滤器的使用方法。要让 Wireshark 只抓取必要的数据包，抓包过滤器不可或缺。本章会详述这一过滤器的配置方法，外加如何使用这一过滤器，让 Wireshark 只抓取网络工程师“心仪的”数据包。

第 3 章，显示过滤器的用法，本章说明了显示过滤器的使用方法。通过 Wireshark 抓取到数据包之后，可定义显示过滤器，让 Wireshark 只显示出“必要的”数据包。本章会详述这一过滤器的配置方法，同时会介绍如何利用其来帮助排除网络故障。

第 4 章，基本信息统计工具的用法，说明了 Wireshark 自带的信息统计工具的基本用法，包括如何用 Statistics 菜单下的某些菜单项，生成与相互“沟通”的主机（who is talking）、会话（conversations）及 HTTP 协议流量等有关的信息统计报表。

第 5 章，高级信息统计工具的用法，介绍了 Wireshark 提供的信息统计工具的高级用法，包括如何用 Statistics 菜单下的有关菜单项，生成 IO 图（IO graph）及 TCP 流图（TCP stream graph），上述图形可成为网络及应用程序性能分析的重要依据。

第 6 章，Expert Infos 工具的用法，讲解了如何使用 Wireshark 内置的专家系统（Expert system）工具，该工具的功能极为强大，可对网络中发生的有可能会影响到应用程序正常交付的各种事件（比如，TCP 重传、零窗口[zero-window]、TTL 过低/路由环路、报文段失序等）“洞察秋毫”。

第 7 章，Ethernet、LAN 交换以及无线 LAN，简要介绍了与 Ethernet 协议及 LAN 交换有关的基本概念，探讨了可能会发生在第二层的网络故障。此外，本章还重点介绍了无线 LAN（Wi-Fi）相关知识，包括如何测试该网络，以及如何解决发生在该网络中的故障。

第 8 章，ARP 和 IP 故障分析，简要介绍了与 ARP 和 IP 有关的基本概念，探讨了 IP 连通性故障及路由环路故障的解决方法。此外，本章还讲解了如何发现 IP 地址冲突，如何解决 DHCP 及其他相关故障。

第 9 章，UDP/TCP 故障分析，重点关注第四层协议——UDP 和 TCP——着重讨论与 TCP 性能有关的问题。本章包含多个定位 TCP 性能问题的诀窍，TCP 重传问题、重复确认问题（duplicate ACK）、滑动窗口（sliding-window）问题（即 window-full 和 zero-window 问题）、重置（reset）问题等都属于 TCP 性能问题。

第 10 章，HTTP 和 DNS，重点关注 DNS、HTTP 及 HTTPS 协议，将介绍这三种协议的运作方式，同时还会讲解如何排除与三种协议有关的故障。

第 11 章，企业网应用程序行为分析，探讨了包括 FTP、Mail 协议以及与终端服务和数据

库有关的常用网络协议，在介绍网络故障对上述应用程序的影响的同时，还会给出基本的排障思路。

第 12 章，SIP、多媒体和 IP 电话技术，介绍了如何利用 Wireshark，去定位及排除依靠 IP 传送的语音及视频（voice and video over IP）故障，此类故障包括 VoIP SIP 连通性故障、RTP/RTCP 故障和视频故障（比如，画面停顿[picture freezing]和画质不佳）等。

第 13 章，排除由低带宽或高延迟所引发的故障，介绍了如何利用 Wireshark，去定位由低带宽、高延迟及高抖动所引发的故障。本章会细述当网络中存在高延迟及高抖动现象时，TCP 的种种表现，同时会交待怎样才能让 TCP 表现得更好。

第 14 章，认识网络安全，本章重点关注 TCP/IP 网络的安全性，包括如何发现可能会对网络构成危害的扫描行为及 SYN、DoS/DDoS 等攻击行为。本章还会提供发现攻击流量模式的多个诀窍，同时说明这些攻击是如何发动的。

附录、链接、工具及进阶阅读，提供了进一步学习 Wireshark 软件的重要链接，包括各种学习资源和其他各种辅助软件等。

阅读准备

阅读本书之前，请先下载并安装 Wireshark 软件，下载链接为 `www.wireshark.org`。

本书的读者对象

本书的读者对象包括使用 Wireshark 进行网络分析和排除网络故障的研发工程师、技术支持工程师以及 IT 行业的技术管理人员。阅读本书的读者需掌握网络的基本概念，但不要求读者对具体的协议或厂商实现有深入的了解。

目 录

第 1 章 Wireshark 简介 1

1.1 Wireshark 简介 1
1.2 安置 Wireshark（程序或主机） 2
1.3 开始抓包 9
1.4 配置启动窗口 14
1.5 配置时间参数 20
1.6 定义配色规则 22
1.7 数据文件的保存、打印及导出 24
1.8 通过 Edit 菜单中的 Preferences 菜单项，来配置 Wireshark 主界面 28
1.9 配置 Preferences 窗口中的 Protocol 选项 33

第 2 章 抓包过滤器的用法 37

2.1 简介 37
2.2 配置抓包过滤器 38
2.3 配置 Ethernet 过滤器 42
2.4 配置主机和网络过滤器 46
2.5 配置 TCP/UDP 及端口过滤器 50
2.6 配置复合型过滤器 53
2.7 配置字节偏移和净载匹配型过滤器 55

第 3 章 显示过滤器的用法 58

3.1 简介 58
3.2 配置显示过滤器 59
3.3 配置 Ethernet、ARP、主机和网络过滤器 67
3.4 配置 TCP/UDP 过滤器 71
3.5 配置协议所独有的显示过滤器 78
3.6 配置字节偏移型过滤器 81
3.7 配置显示过滤器宏 82

第 4 章 基本信息统计工具的用法 84
4.1 简介 84
4.2 Statistics 菜单中 Summary 工具的用法 85
4.3 Statistics 菜单中 Protocol Hierarchy 工具的用法 87
4.4 Statistics 菜单中 Conversation 工具的用法 90
4.5 Statistics 菜单中 Endpoints 工具的用法 94
4.6 Statistics 菜单中 HTTP 工具的用法 96
4.7 配置 Flow Graph（数据流图），来查看 TCP 流 101
4.8 生成与 IP 属性有关的统计信息 103

第 5 章 高级信息统计工具的用法 107
5.1 简介 107
5.2 配置与显示过滤器结合使用的 IO Graphs 工具，来定位与网络性能有关的问题 108
5.3 用 IO Graphs 工具测算（链路的）吞吐量 112
5.4 IO Graphs 工具的高级配置方法（启用 Y 轴 Unit 参数的 Advanced 选项） 117
5.5 TCP StreamGraph 菜单项中 Time-Sequence (Stevens)子菜单项的用法 125
5.6 TCP StreamGraph 菜单项中 Time-Sequence (tcp-trace)子菜单项的用法 128
5.7 TCP StreamGraph 菜单项中 Throughput Grap 子菜单项的用法 131
5.8 TCP StreamGraph 菜单项中 Round Trip Time Graph 子菜单项的用法 133
5.9 TCP StreamGraph 菜单项中 Window Scaling Graph 子菜单项的用法 135

第 6 章 Expert Info 工具的用法 137
6.1 简介 137
6.2 如何使用 Expert Info 工具执行排障任务 137
6.3 认识 Errors 事件 145
6.4 认识 Warnings 事件 147
6.5 认识 Notes 事件 149

第 7 章 Ethernet、LAN 交换及无线 LAN 152
7.1 简介 152
7.2 发现广播及错包风暴 152
7.3 生成树协议分析 159
7.4 VLAN 和 VLAN tagging 故障分析 168
7.5 无线 LAN（WiFi）故障分析 172

第 8 章 ARP 和 IP 故障分析 177
8.1 简介 177

8.2 与 ARP 有关的连通性网络故障分析……178
8.3 IP 流量分析工具的用法……186
8.4 利用 GeoIP 来查询 IP 地址的归属地……189
8.5 发现 IP 包分片问题……192
8.6 路由选择故障分析……197
8.7 发现 IP 地址冲突……200
8.8 DHCP 故障分析……204

第 9 章 UDP/TCP 故障分析……208
9.1 简介……208
9.2 配置 Preferences 窗口内 protocol 选项下的 UDP 和 TCP 协议参数，为排除排障做准备……209
9.3 TCP 连接故障……213
9.4 TCP 重传现象——源头及原因……219
9.5 重复确认（duplicate ACKs）和快速重传（fast retransmissions）现象……229
9.6 TCP 报文段失序现象……232
9.7 TCP Zero Window、Window Full、Window Change 以及其他包含 Window 字样的提示信息……235
9.8 TCP 重置（reset）及原因……240

第 10 章 HTTP 和 DNS……242
10.1 简介……242
10.2 筛选 DNS 流量……243
10.3 分析 DNS 协议的常规运作机制……247
10.4 DNS 故障分析……252
10.5 筛选 HTTP 流量……260
10.6 配置 Preferences 窗口中 protocol 选项下的 HTTP 协议参数……263
10.7 HTTP 故障分析……266
10.8 导出 HTTP 对象……272
10.9 HTTP 数据流分析及 Follow TCP Stream 窗口……274
10.10 HTTPS 协议流量分析——SSL/TLS 基础……277

第 11 章 企业网应用程序行为分析……286
11.1 简介……286
11.2 摸清流淌于网络中的流量的类型……287
11.3 FTP 故障分析……289
11.4 E-mail 协议（POP、IMAP、SMTP）流量及故障分析……295

11.5 MS-TS 和 Citrix 故障分析 305
11.6 NetBIOS 协议故障分析 308
11.7 数据库流量及常见故障分析 317

第 12 章 SIP、多媒体和 IP 电话 322
12.1 简介 322
12.2 使用内置于 Wireshark 的 IP 电话及多媒体流量专用分析工具 323
12.3 SIP 故障分析 330
12.4 RTP/RTCP 故障分析 341
12.5 视频及视频监控应用排障场景 349
12.6 IPTV 应用排障场景 353
12.7 视频会议应用排障场景 354
12.8 排除 RTSP 协议故障 356

第 13 章 排除由低带宽或高延迟所引发的故障 361
13.1 简介 361
13.2 测量通信链路的总带宽 361
13.3 测量每个用户及每种应用所占用的通信链路的带宽 366
13.4 借助 Wireshark，获悉链路上的延迟及抖动状况 367
13.5 发现因高延迟/高抖动所引发的应用程序故障 370

第 14 章 认识网络安全 377
14.1 简介 377
14.2 发现异常流量模式 378
14.3 发现基于 MAC 地址和基于 ARP 的攻击 384
14.4 发现 ICMP 和 TCP SYN/端口扫描 385
14.5 发现 DoS/DDoS 攻击 393
14.6 发现高级 TCP 攻击 397
14.7 发现暴力破解（brute-force）攻击 400

附录 链接、工具及阅读资料 405

第1章 Wireshark简介

本章涵盖以下内容：

- 安置 Wireshark（主机/程序）；
- 开始抓包；
- 配置启动窗口；
- 配置时间参数；
- 调整配色规则；
- 保存、打印及导出数据；
- 配置用户界面（点击 EDIT 菜单的 Preferences 菜单项，会弹出 Preferences 窗口。所谓配置用户界面，就是配置该窗口中 User Interface 配置选项里的内容）；
- 配置协议参数（即配置 Preferences 窗口中 Protocol 配置选项里的内容）。

1.1 Wireshark简介

本章将介绍 Wireshark 所能行使的基本任务。本书的前言曾提到过网络排障以及内置于 Wireshark 能帮助排障的各种工具。一旦决定动用 Wireshark 协议分析软件，在使用之前，则有必要先确定该软件在网络中的部署（或安装）位置。除此之外，还得对该软件做一些基本的配置，至少应让其界面看起来更为友好。

用 Wireshark 执行基本的抓包操作，配置起来并不麻烦，但是该软件也包含了很多高级配