<<网络分析技术揭秘>>

图书基本信息

书名：<<网络分析技术揭秘>>

13位ISBN编号：9787111380382

10位ISBN编号：711138038X

出版时间：2012-7

出版时间：机械工业出版社

作者：吕雪峰,彭文波,宋泽宇

页数：447

<<网络分析技术揭秘>>

内容概要

《网络分析技术揭秘：原理、实践与WinPcap深入解析》结合著名的开源软件库WinPcap来说明网络分析技术的实现原理及使用方法。
其中包括WinPcap内核驱动，编译与使用，数据包的捕获、发送、内核过滤与接收，以及网络流量的统计与网络状态的分析等重要内容，而且作者还通过修改内核级的源代码解决了开源代码本身尚未完成的一个重要功能—数据包的内核转储。
经过系统深入的分析，读者既能对WinPcap的架构、使用与实现机制有深入的理解，又能快速熟悉操作系统内核与用户层交互的实现机制，并全面了解网络分析专业各方面的技术，进而将相关知识运用到实际项目中。

如果您的工作与网络软件相关，无论是开发人员还是测试人员，我们都强烈建议您阅读这本书。

作者简介

吕雪峰，华中科技大学控制工程与控制理论专业硕士，资深软件工程师，国船电气（武汉）有限公司软件技术总监。
是目前国内对WinPcap进行彻底分析研究的先驱，活跃于51CTO、ChinaUnix、CSDN等社区。
对WinPcap与网络分析具有深入的理解，在《计算机应用》等学术期刊上发表核心论文多篇。
尤精于嵌入式Linux。
彭文波，从事互联网产品工作，曾在省级电子商务认证中心从事安全开发工作，曾就职于多家专业网管软件公司，先后参与了电子商务认证系统、移动网络管理系统等产品的开发。
宋泽宇，七二二研究所数字通信专业硕士，高级工程师，国船电气（武汉）有限公司副总经理，曾参与多个大型项目的研制工作。

<<网络分析技术揭秘>>

书籍目录

章节摘录

 无连接。
该方式不保证发送的信息一定可以收到。
面向连接。
该方式提供了四种服务：连接的建立、确认和数据到达响应、差错恢复 （通过请求重发接收到的错误数据实现）、滑动窗口（系数：128）。
滑动窗口用来提高数据传速率。
无连接应答响应服务。
在面向连接的通信方式中，每一个LLC帧发送的内容都会被确认。
LLC子层在接收LLC帧（又称协议数据单元，PDU）结束时需要检测在传输时是否有帧丢失了，如果丢失，则会给发送端发送一个请求，请求重新开始传输，此次传输将从没有到达的PDU开始。
LLC子层位于MAC子层的上面，它在上层与MAC子层的协议（如以太网、令牌环网等）之间扮演着一个联络人的角色。
3.网络层 接下来的一层为网络层，在这一层数据包会被顺序化，同时会被赋予逻辑地址。
逻辑地址是通过软件赋予的地址，不是永久性的。
TCP／IP协议在互联网上使用的IP地址就是逻辑地址。
网络层也负责在点或结点之间创建一个虚拟链路（这里指的一个逻辑连接，而不是一个物理连接）。
其中结点是具有MAC地址的设备，包含计算机、打印机或路由器等。
这一层也负责路由与推进数据包。
路由是指从一个网络或子网推进数据包到另一个网络或子网。
如果没有路由器，计算机只能与同一网段中的计算机通信。
对于互联网来说，路由是一个关键，同时也是网络层最重要的任务。
网络层还提供流量控制与差错控制功能。
在该层操作的设备是路由器与三层交换机。
从这一层开始，实现OSI模型的基本方法将与软件密切关联，而不再是硬件。
4.传输层 OSI模型的第四层为传输层，这一层负责从一个结点传输数据到另一个结点上。
它在结点间提供透明的数据传输，并管理端到端的流量控制、错误检测与错误恢复。
首先，传输层协议在不同计算机的特定端口之间发起联系，并设置虚拟的链路。
每台主机的传输协议确认应用程序发送的数据是否是被授权访问的，并且两个端点是否都准备好开始数据传输了。
当该同步完成时，数据将被发送。
在数据传送的过程中，每台主机上的传输协议会监控数据流并监视传输错误。
如果传输检测到错误，传输协议将提供错误恢复。
对网络通信而言，传输层所提供的功能非常重要。
前面提到数据链路层提供了底层可靠性与面向连接或非连接的通信，传输层做了同样的工作，只不过是在更高的层次上。
面向连接的传输控制协议（TCP）与面向非连接的用户数据包协议（UDP）是传输层常见的两种协议。
传输层也管理端口的逻辑地址，比如，决定所接收的数据属于哪个应用程序，一台计算机上可能会同时运行几个网络应用程序。
传输层还会处理域名解析，如使用域名系统（Domain Name System，DNS）就是处理该问题的一种方法。

<<网络分析技术揭秘>>

编辑推荐

《网络分析技术揭秘:原理、实践与WinPcap深入解析》深入地、全面地叙述了网络分析的核心技术，并以大量示例演示了相关概念，其中包括进行网络分析必要的各种软硬件基础知识，网络数据包的捕获、发送、分析、文件转储等方面的内容。
因此《网络分析技术揭秘:原理、实践与WinPcap深入解析》适合各层次的网络分析人员使用，例如网络软件开发人员与网络软件测试人员从中可获得许多网络分析与软件设计的知识；网络安全工程师可以从中获得网络攻击者所使用技术的一些细节知识。

名人推荐

本书通过对WinPcap架构、使用与实现机制的深入分析，来让我们快速熟悉操作系统内核与用户层交互的实现机制，掌握网络分析技术的核心！
而且文中还加入了很多实例，避免了大段的理论阐述，这让我们理解起来会相对容易一些。
我们还可通过查看书中提供的每行代码的运行结果，来验证自己的想法。
所以对于希望学习网络分析技术的人员来说这是一本不可多得的参考书籍。
——任晓珲 黑客反病毒组织创始人 本书作者从事软件开发工作多年，本书的写作也花费了作者几年的时间，可谓是呕心沥血之作。
作者在写作之初，曾希望能把网络分析的核心技术用浅显易懂的方式展现出来，以帮助读者掌握这门技术，并可以把它运用于实际工作中，真真正正地“学以致用”，我觉得，他做到了。
而且他还通过直接修改内核级源代码的方式解决了开源代码本身尚未完成的一个重要功能——数据包的内核转储。
——51CTO随着计算机网络的迅速发展，网络安全、网络性能、网络软件质量等相关问题也随之凸现。
这些问题受到人们越来越多的关注，并逐渐成为网络应用所面临的障壁。
正是在这种局势下，网络分析逐渐成为一门独立的、专业的学科，在网络软件开发、调试、测试与维护中得以广泛使用。
因为网络分析涉及诸多技术，所以为了有效使用这些技术并更好地理解这些技术原理，就要对相关人员提出很高的要求。
在本书中，作者对网络分析的核心技术进行了深入的剖析。
其结合常用的网络分析开源库WinPcap详细演示了网络分析技术的使用。
给希望使用WinPcap、熟悉WinPcap高级特性、甚至自行开发与修改WinPcap源代码的人员提供了全面的、详细的参考信息。
与此同时，作者还把网络分析各技术的实现原理分析得十分透彻，使读者除了学习到如何使用网络分析技术外，还可理解网络分析工具的设计架构。
这是很重要的，尤其是对于网络高级测试人员与开发人员来说，这些都是必备的知识。
目前市面上少有关于网络分析的书籍，更没有一本详细分析网络分析各技术底层实现机制的书籍，所以本书颇具出版价值。
——熊有伦 中国科学院院士

版权说明