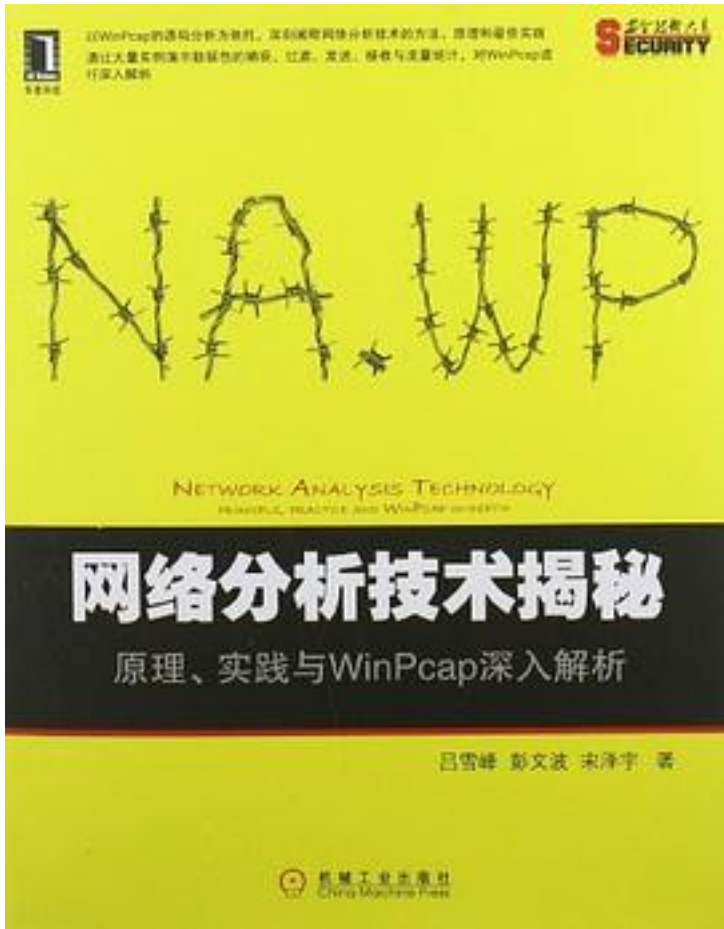


网络分析技术揭秘



[网络分析技术揭秘_下载链接1](#)

著者:吕雪峰

出版者:机械工业出版社

出版时间:2012-7

装帧:

isbn:9787111380382

《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。

作者介绍:

目录: 前言

第1章 揭开网络分析的神秘面纱

1.1 网络分析概述

1.2 网络分析的主要用途

1.3 黑客使用嗅探器的方法

1.4 被嗅探数据的真面目

1.4.1 使用嗅探器获得FTP的用户名和密码

1.4.2 使用嗅探器分析冲击波蠕虫 (Blaster Worm)

1.5 常见的网络分析器

1.6 网络分析器的工作原理

1.6.1 以太网简介

1.6.2 理解开放系统互连 (OSI) 模型

1.6.3 了解CSMACD协议

1.6.4 IP、ICMP、TCP与UDP协议

1.6.5 硬件

1.6.6 欺骗交换机

1.7 嗅探器的检测

1.7.1 检测嗅探器的原理

1.7.2 防止网络嗅探可采取的安全措施

1.8 网络分析工具的主要功能组成

1.9 Wireshark的概述、安装与使用

1.9.1 Wireshark的概述

1.9.2 Wireshark的安装

1.9.3 Wireshark的使用

1.10 小结

第2章 初识网络分析基础库WinPcap

2.1 WinPcap概述

2.2 WinPcap的优点

2.3 WinPcap的使用者

2.4 WinPcap的体系架构

2.4.1 WinPcap的主要组成

2.4.2 数据包捕获的基本过程

2.4.3 WinPcap的驱动程序

2.4.4 WinPcap内核驱动的主要功能

2.5 用户空间库接口函数

2.5.1 wpcap.dll库中的重要函数

2.5.2 Packet.dll库中的重要函数

2.6 小结

第3章 网络分析工具的内核驱动基础知识

3.1 Windows驱动程序基础知识

3.1.1 驱动对象 (DRIVER_OBJECT)

3.1.2 设备对象 (DEVICE_OBJECT)

3.1.3 设备扩展 (_DEVICE_EXTENSION)

3.1.4 IRP与派遣函数

3.1.5 同步处理

- 3.1.6 内核的内存操作
- 3.1.7 内存操作的运行时函数
- 3.1.8 内核的注册表操作
- 3.2 NDIS协议驱动程序
 - 3.2.1 三种类型的网络驱动程序
 - 3.2.2 协议驱动程序的特征结构体
- 3.3 小结
- 第4章 编译与使用WinPcap
 - 4.1 源代码目录结构
 - 4.2 构建驱动程序NPF
 - 4.3 构建Packet.dll库
 - 4.4 构建wpcap.dll库
 - 4.5 安装NPF驱动程序与各库文件
 - 4.6 使用WinPcap库进行程序开发的实例
 - 4.7 小结
- 第5章 WinPcap驱动程序的初始化与清除
 - 5.1 驱动程序中的初始化函数DriverEntry
 - 5.1.1 DriverEntry函数的工作流程
 - 5.1.2 DriverEntry函数的具体实现
 - 5.2 驱动程序中的卸载函数DriverUnload
 - 5.3 小结
- 第6章 获得与释放网络适配器设备列表
 - 6.1 使用WinPcap选择合适的适配器
 - 6.1.1 wpcap.dll库导出的相应函数
 - 6.1.2 获得与释放网络适配器列表的实例
 - 6.1.3 获取已安装设备高级信息的实例
 - 6.2 获得网络适配器列表的幕后
 - 6.2.1 wpcap.dll库中获得网络适配器列表的实现
 - 6.2.2 Packet.dll库中获得网络适配器列表的实现
 - 6.2.3 内核空间中获得网络适配器列表的实现
 - 6.3 释放网络适配器列表的实现
 - 6.4 小结
- 第7章 打开与关闭适配器
 - 7.1 使用WinPcap打开与关闭适配器
 - 7.1.1 wpcap.dll库导出的相应函数
 - 7.1.2 关键数据结构pcap_t
 - 7.1.3 打开与关闭网络适配器的实例
 - 7.2 打开与关闭适配器的幕后
 - 7.2.1 打开适配器的实现
 - 7.2.2 关闭适配器的实现
 - 7.3 小结
- 第8章 数据包的发送
 - 8.1 使用WinPcap发送数据包
 - 8.1.1 wpcap.dll库导出的相应函数
 - 8.1.2 数据包发送实例
 - 8.2 数据包发送的幕后
 - 8.2.1 发送单个数据包的实现
 - 8.2.2 单个数据包发送多次的实现
 - 8.2.3 发送队列方式的实现
 - 8.3 小结
- 第9章 数据包的内核过滤
 - 9.1 基础知识
 - 9.1.1 flex和bison简介
 - 9.1.2 #line宏

- 9.1.3 以太网的典型帧结构
- 9.1.4 数据包过滤的原理简介
- 9.1.5 BPF虚拟机
- 9.1.6 Tcpdump与WinDump
- 9.1.7 BPF指令集实例
- 9.1.8 BPF过滤器的优化研究
- 9.1.9 BPF系统架构
- 9.2 WinPcap数据包过滤基础
 - 9.2.1 数据包过滤过程
 - 9.2.2 过滤表达式
 - 9.2.3 编译过滤表达式生成过滤器的字节码
 - 9.2.4 把过滤器字节码传递给内核
- 9.3 使用WinPcap过滤数据包
 - 9.3.1 wpcap.dll库导出的相应函数
 - 9.3.2 使用过滤器的实例
- 9.4 数据包过滤的幕后
 - 9.4.1 wpcap.dll库中相应函数的实现
 - 9.4.2 Packet.dll库对应的函数
 - 9.4.3 驱动程序中对应的函数
 - 9.4.4 NPF_tap函数的数据包过滤部分
- 9.5 小结
- 第10章 数据包的接收
 - 10.1 使用WinPcap接收数据包
 - 10.1.1 wpcap.dll库导出的相应函数
 - 10.1.2 数据包接收的实例
 - 10.2 数据接收的幕后
 - 10.2.1 wpcap.dll库中相应函数的实现
 - 10.2.2 Packet.dll库中相应函数的实现
 - 10.2.3 内核空间部分的实现
 - 10.3 小结
- 第11章 统计网络流量与网络状态
 - 11.1 使用WinPcap进行网络统计的方法
 - 11.1.1 wpcap.dll库导出的相应函数
 - 11.1.2 统计实例
 - 11.2 网络统计的幕后
 - 11.2.1 工作模式
 - 11.2.2 模式设置函数
 - 11.2.3 网络流量统计的实现
 - 11.2.4 网络状态统计的实现
 - 11.3 小结
- 第12章 文件的存储与读取
 - 12.1 libpcap文件存储格式
 - 12.1.1 存储文件的头信息
 - 12.1.2 每个数据包的头信息
 - 12.2 使用WinPcap进行文件存储与读取
 - 12.2.1 wpcap.dll导出的相应函数
 - 12.2.2 文件存储与读取的实例
 - 12.3 数据包文件存储的幕后
 - 12.3.1 pcap_dump_open函数
 - 12.3.2 pcap_dump函数
 - 12.3.3 pcap_dump_flush函数
 - 12.3.4 pcap_dump_close函数
 - 12.4 数据包文件读取的幕后
 - 12.5 内核文件转储的实现

- 12.5.1 wpcap.dll库中相应函数的实现
- 12.5.2 Packet.dll库中相应函数的实现
- 12.5.3 驱动程序中对应的函数
- 12.6 小结
- 第13章 修改源代码
- 13.1 给wpcap.dll增加设置重复发送次数的函数
- 13.1.1 修改步骤
- 13.1.2 测试结果
- 13.2 修改WinPcap的内核驱动代码
- 13.2.1 支持内核转储功能
- 13.2.2 测试内核统计与转储模式
- 13.2.3 支持大量数据包的转储
- 13.2.4 内核驱动程序修改后的源文件
- 13.3 小结
- 第14章 性能测试与分析
- 14.1 测试环境
- 14.2 测试实例
- 14.2.1 不同发送方式的比较
- 14.2.2 发送不同数据包长度的比较
- 14.2.3 不同接收方式的比较
- 14.3 小结
- 附录A 源语法规范
- 附录B 过滤表达式规范
- 附录C SYN洪泛攻击的详细资料
- 附录D ARP欺骗资料
- 参考文献
- • • • • (收起)

[网络分析技术揭秘_下载链接1](#)

标签

网络

tcp/ip

安全入门级

编程

hack

计算机科学

网络安全

看雪介绍

评论

作者功底扎实，特别是写bpf还有window内核这块。书是好书，就是window实在不懂。

南图

[网络分析技术揭秘_下载链接1](#)

书评

WinPcap是Windows平下可以直接访问数据连路层的开源网络分析库，基于此库可以制作如嗅探器之类的网络抓包软件。
这本书其实是以WinPcap的技术手册为原本，对其进行了详细的解释和阐述，从供用户使用的高层动态链接库到系统实现的底层动态链接库，将代码都列举讲解了一遍，对这...

[网络分析技术揭秘_下载链接1](#)