PCAP文件格式网络数据包分析软件设计与实现

高 凯[1],赵登攀[2]

(1.陕西理工学院 数学与计算机科学学院;2.陕西理工学院 教务处,陕西 汉中 723001)

摘 要:通过对主流转包软件所保存的PCAP格式文件进行解析统计,开发了一种针对PCAP文件格式的网络数据包分析软件,该软件能够在一定程度上帮助网络管理人员及时发现和排除网络异常,提高了对网络可靠性的监控和保障能力。

关键词:PCAP文件格式;数据包分析;流量统计

中图分类号:TP393 **文献标识码**:A **文章编号**:1672-7800(2013)012-0150-02

0 引言

本文针对网络数据包的捕获和分析技术做了比较深入的阐述,设计并实现了一个基于PCAP的实时网络数据包捕获和协议统计分析系统。该系统采用WinPcap网络数据包捕获机制,对流经网络的数据包进行监测和统计分析。系统提供了网络数据包的抓取和分析功能。

1 PCAP文件介绍

PCAP作为主流抓包软件的文件存储格式,通过对PCAP格式文件中的数据进行相关分析统计,可以得到数据包的一些基本信息及网络运行状况。PCAP文件的基本格式包含三个部分,分别是文件头、数据包头以及数据报。

2 软件详细设计与实现

2.1 软件设计流程

在VC++6.0下创建一个文档的MFC应用程序,工程名:IPControl。接着建立菜单栏,本程序中的菜单栏包含文件、编辑、查看、帮助。建立菜单栏时,在Resources中新建一个MENU文件,并在该文件下建立IDR_MAINFRAME控件,在控件中对上述菜单栏进行设计,菜单栏建立完毕后,需要对工具栏进行设计。

2.2 网络协议分析总体流程

该模块从缓冲区内读取数据包,首先对数据包进行分解,然后按照网络协议对数据包进行解析,并以列表的形式实时显示数据包的解析结果,包括数据包的包长度、源IP、目的IP、端口、使用协议等相关信息。

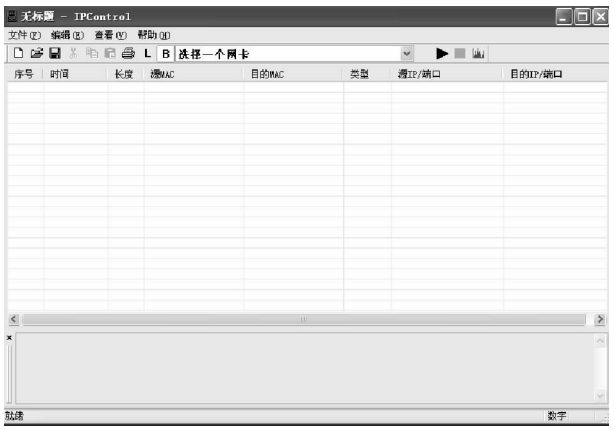

图1 系统主界面

TCP数据段头的分析在编程实现中可通过数据结构TCPPcaketHead来定义:

```
Struct TCPPacketHead {
WORD SourPort;//源端口
WORD DestPort;//目的端口
DWORD SeqNo;//顺序号
DWORD AckNo;//确认号
BYTE HLen;//TCP头长度
BYTE Flag;//标志(URG、ACK等)
WORD Winsize;//窗口大小
WORD ChkSun;//校验和
WORD UrgPtr;//紧急指针
}
```

2.3 分析模块的实现

被捕获的数据只有经过解析才能对协议的分析提供

基金项目:陕西省教育厅专项科研基金资助项目(11JK1066)

作者简介:高凯(1981-),男,硕士,陕西理工学院数学与计算机科学学院讲师,研究方向为计算机网络安全、无限传感器网络;赵登攀(1975-),男,硕士,陕西理工学院教务处工程师,研究方向为计算机网络安全。

有用的数据。本模块就是对捕获的数据包按照数据链路层（MAC）、网络层（IP，ARP/RARP）、传输层（TCP，UDP，ICMP）和应用层（HTTP 等）的层次结构自底向上进行解析，并将解析结果显示输出。在进行协议解析时要注意各协议报头多字节整型字段从网络字节序到主机字节序的转换。对于多字节的数据（如 short、int、long 等），不同 CPU 在其内部表示一个数时会使用不同的字节顺序方案，将低序字节存储在起始地址的称为小端点机，否则称为大端点机。网络中有不同类型的计算机，在网络数据的传输中要统一数字的表示方式，即统一采用大端点方式，所以数据包头中表示长度或类型等的多字节数据字段应按需转换成本地主机的表示形式。可以用函数 ntohs() 或 ntohl() 将双字节或四字节整型由网络字节序转换为主机字节序。该功能模块主要由封装的 CsockSupport、CsockHelper、GetLocalIP、CbinDataDlg 四个类完成。

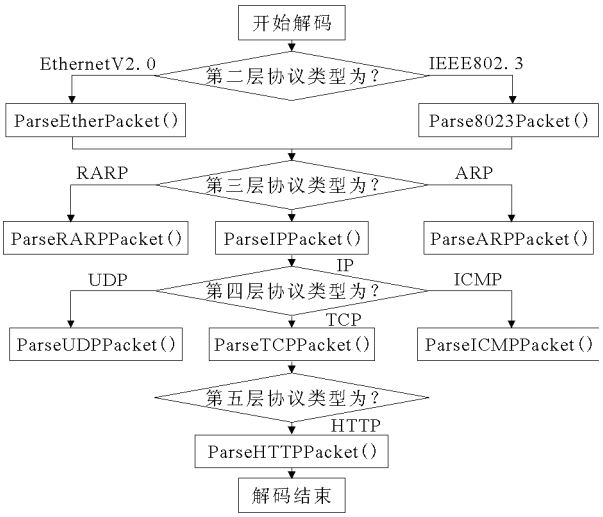

图 2　协议解析流程

3　结语

本文研究开发了一套用于中小规模网络系统的网络监控软件，设计并实现了一个基于 PCAP 的实时网络数据包捕获和协议统计分析系统。系统采用 WinPcap 网络数据包捕获机制，对流经网络的数据包进行监测和统计分析，并通过多线程技术和读写缓冲技术，解决了读取缓冲区中数据和网络数据之间的速度差异，并能根据网络安全管理员设定的特征信息，对具有该信息的数据包进行分类解析、还原和预警。

参考文献：

[1] 谢鲲，张大方，文吉刚. 基于 WinPcap 的实时网络监测系统[J]. 湖南大学学报：自然科学版，2006.

[2] WILLIAMSON C. Internet traffic measurement[J]. IEEE Internet Computing，2001，5(6)：70-74.

[3] 庄春兴，彭奇志. 基于 WinPcap 的网络嗅探程序设计[J]. 计算机与现代化，2002(5)：34-36.

[4] 赵心宇，朱齐丹，朱达书. 应用 WinPcap 捕获网络数据包[J]. 应用科技，2004，31(11)：29-31.

[5] 循序渐进学习使用 WinPcap[EB/OL]. http://www. cnpaf. net，2005.

[6] CHARLES HORNIG. A standard for the transmission of IP datagrams over Ethernet Networks[M]. RFC894，1984.

[7] J POSTEL，J REYNOLDS. A standard for the transmission of IP datagrams over IEEE 802 Networks[M]. RFC1042，1988.

（责任编辑：黄　健）

PCAP File Format Network Packet Analysis Software Design and Implementation

Abstract：Based on the mainstream software subcontract saved pcap format file parsing statistics，developed a PCAP file format for network packet analysis software，the software enough to a certain extent，help network managers to find timely and troubleshoot network anomalies，improve the reliability of network monitoring and support capabilities

Key Words：Pcap File Format；Packet Analysis；Traffic Statistics