文章编号：1005-8451（2006）02-0038-03

基于WinPcap端口扫描器的设计和实现

李 伟，韩 臻，韩 岳，刘振良
（北京交通大学 软件学院，北京 100044）

摘 要：介绍端口扫描技术原理，并在Windows 2000操作系统平台上，用Visual C++ 6.0实现了端口扫描器。该扫描器利用WinPcap库提供的API处理原始数据包，并采用Windows多线程技术。可对目标主机进行Connect扫描，SYN扫描，FIN扫描，NULL扫描，UDP扫描等。

关键词：端口扫描；网络安全；WinPcap；线程
中图分类号：TP39 文献标识码：A

Design and implementation of port scanner based on WinPcap Lib

LI Wei, HAN Zhen, HAN Yue, LIU Zhen-liang
(School of Software, Beijing Jiaotong University, Beijing 100044, China)

Abstract: It was introduced the principle of port scanning technique,and implemented the port scanner with Visual C++ 6.0 on Windows2000 as well.Taking advantage of API provided by WinPcap lib to process the raw packet and Windows multithread technique.The port scanner could scan the target host with SYN, Connect, FIN, NULL, UDP, etc.

Key words: port scanning; network security; WinPcap; thread

在计算机网络开放性和互连性不断增强的今天，网络安全问题日益引起社会的重视，网络安全评估工具逐渐被企事业单位所接受。端口扫描器作为网络安全评估软件的一部分，在网络安全方面起着重要的作用。通过向目的主机的TCP/IP端口发送TCP或UDP探针，记录目标的响应信息，得出目的主机服务端口的状态和提供的服务，从而分析出系统存在的漏洞[1]。网络管理人员可以借此分析网络和主机中的安全状况，先于黑客了解系统存在的漏洞，从而防患于未然。

WinPcap库[2]是一套基于Win32平台的开放源代码的网络数据包截获和分析系统。它具有功能强大的包处理API接口，而且性能稳定、效率极高。该扫描器利用WinPcap库处理原始数据包，采用多线程技术对目的主机相应端口进行扫描并能显示目的主机的操作系统相关信息。该扫描器目前在局域网中工作良好，性能稳定。

1 端口扫描技术分类

目前，端口扫描主要分为开放扫描、半开放扫描和隐蔽扫描（图1）[3]。

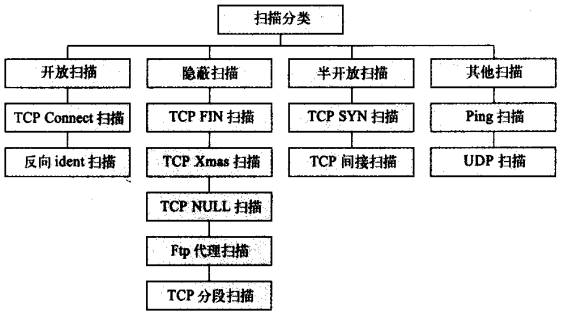

图1 端口扫描分类

1.1 开放扫描

开放扫描方式应用TCP连接中的3次握手特性，源主机向目的主机某一端口发送TCP连接请求，如果通信双方完成3次握手，即建立TCP连接，则表明目的端口开放；否则，说明该端口处于关闭状态。该扫描方式实现简单，无需root用户权限，仅需调用Connect()函数便可实现，但是很容易被目的主机日志所记录。

1.2 半开放扫描

半开放扫描应用TCP 3次握手特性和设置TCP包头中的6个标志位，但它没有打开一个完整的TCP连接。扫描程序发送一个SYN请求数据包给目

收稿日期：2005-08-23
作者简介：李 伟，在读硕士研究生；韩 臻，教授。

的主机，等待目的主机响应信息。如果源主机收到来自目的主机的SYN|ACK响应数据包，说明目的主机在该端口处于侦听状态；若收到RST数据包，说明该端口处于关闭状态。该扫描技术一般不会在目的主机上留下记录，但是需要root权限构建原始数据包。

1.3 隐蔽扫描

该扫描是在网络端口扫描过程中隐蔽自身踪迹的技术。能够不为目标系统的日志机制、扫描监测系统和入侵检测系统捕获，绕过防火墙侦测到目标主机的扫描行为。

1.3.1 TCP FIN扫描

扫描器向目标主机端口发送FIN包。当一个FIN数据包到达一个关闭的端口，数据包会被丢掉，并且返回一个RST数据包。否则，若是打开的端口，数据包只是简单的丢掉（不返回RST）。该技术不涉及TCP 3次握手协议，很难被目的主机记录，扫描更加隐蔽。

1.3.2 TCP Xmas、NULL扫描

这两种扫描方式是FIN扫描的两个变种。Xmas扫描将TCP报头中的FIN、URG和PUSH位置1，而NULL扫描将ACK，FIN，RST，SYN，URG，PUSH位置0。如果目的主机没有返回任何信息，表明该端口开放。如果返回RST，则端口关闭。

1.3.3 FTP扫描

RFC959文档中规定FTP协议支持“代理连接”，应用这一特性，可以通过某一FTP代理服务器对目的主机进行扫描（图2）。

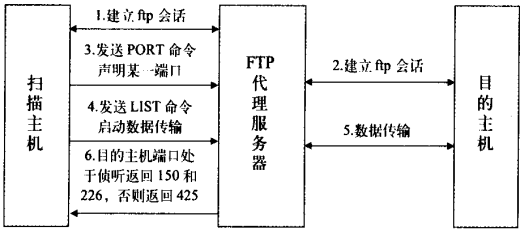

图2　FTP扫描原理

2 WinPcap库介绍

WinPcap是一套开放源代码，基于Win32平台对原始数据包进行操作的封装库。它的主要思想来源于UNIX系统中最著名的BSD包截获架构。WinPcap由内核级的组包过滤器（NPF）、用户级的动态连接库Packet.dll和WPcap.dll等3个模块组成。工作在内核级的NPF包过滤器，是运行于操作系统内核中的驱动程序，用来与网卡驱动程序进行交互，获取网络中的原始数据包；应用层的Packet.dll模块在Win32平台上为NPF提供了底层编程接口；WPcap.dll模块是扫描器中将要使用的部分，它与UNIX系统下的BSD截获架构提供的Libpcap库完全兼容，在Packet.dll模块之上为用户提供了一组功能强大、高效处理数据包的API接口[4]。

WinPcap较其他的数据包捕获方法有很多优点：（1）WinPcap API函数接口操作简单；（2）可以捕获链路层的数据包，而原始套接字只能捕获IP层的数据包；（3）通过设置数据包过滤规则，得到需要的数据包；（4）具有很强的可移植性。

3 扫描器程序简介

3.1 实现的功能

本端口扫描器是在Windows 2000操作系统平台上，利用VC++ 6.0开发工具实现的，其中利用了WinPcap API接口发送和捕获原始数据包。扫描器实现的功能有：Connect扫描、TCP SYN扫描、TCP FIN扫描、NULL扫描、Xmas扫描、Ping扫描、UDP扫描和操作系统扫描。

3.2 程序实现流程

该扫描器的实现流程及涉及到的部分函数如下：

（1）通过GUI，如图3，获得用户设置的网络地址、扫描类型及网络接口（Eth0、Eth1等），并检查其合法性；

（2）初始化WinPcap环境，打开相应的网络适配器，准备操作数据包如图4所示；

（3）创建线程UINT ThreadFun(LPVOID param)处理应用程序[5]，与GUI脱离，提高窗口反应能力；

（4）在线程ThreadFun中，解析目的主机地址，设置扫描超时时间，根据GUI中提供的线程数m_threadnum，创建m_threadnum个扫描子线程UINT ThreadScan(LPVOID param)，对端口进行并行处理，提高扫描效率，如图5所示；

（5）ThreadScan线程调用扫描函数PortScan (struct hostinfo *hostinfo，unsigned short* portArray，int portsnum，int scanType)，对portArray中的端口列表进行扫描。该函数调用WinPcap库中的Packet-

SendPacket函数发送数据包，利用pcap_next()捕获链路层数据包；

（6）显示出扫描结果；

（7）最后退出WinPcap环境，关闭文件描述字，释放内存。

图3　扫描器GUI

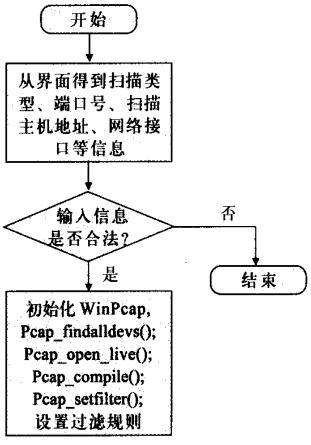

图4　初始化WinPcap过程

3.3　运行结果分析

运行该软件前需要安装WinPcap驱动，可到WinPcap Web站点下载。安装后运行该扫描器，对局域网中某Linux主机（192.9.200.111）和广域网中的某公共服务器的80端口和130－140端口进行SYN扫描，某公共服务器打开了80、135、136、137、138、139端口，linux主机打开了80（由于该主机正在运行Apache2服务器）和139端口。

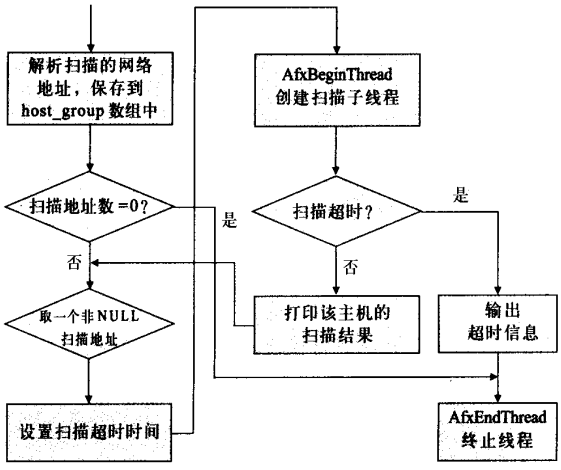

图5　线程ThreadFun的流程图

4　结束语

本文分析了端口扫描技术原理和WinPcap库，并详细介绍了该扫描器的设计思路和实现方法。该扫描器采用多线程技术，可以解析任意格式的主机地址（点式、域名或者带有掩码的地址），而且可以设置接收或者发送数据包的适配器接口。经过多次试验测试，扫描器在局域网中工作稳定，但是对于不是很稳定的广域网上的主机进行扫描有时不能扫描出某些打开的端口。接下来的工作将针对这些不足进行更深一步的研究，以实现更加高效的端口扫描器。

参考文献：

[1] 张义荣，赵志超，鲜　明，等.计算机网络扫描技术研究[J].计算机工程与应用，2004，40（2）：173.

[2] Loris Degioanni，Politecnico di Torino.WinPcap Document [EB/OL]. http://www.winpcap.org/docs/man/html. 2005—2—16.

[3] Nmap network security scanner man page[EB/OL]. http://www.insecure. org/nmap/data/nmap_manpage.html. 2005—3—7.

[4] 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）：11—12.

[5] [美]Davis Chapman. 学用Visual C++ 6.0[M]. 骆长乐.北京：清华大学出版社，2001，2.