网络扫描及安全策略的实现

白 涛

辽阳广播电视大学 （ 辽阳 111000 ）

摘 要 网络的广泛应用对网络安全提出了更高的要求,也促进了对网络安全技术的更深层次的探索,在长期的总结研究过程中,人们提出并实践了各种安全技术,如防火墙、入侵检测、访问控制、身份认证和数据加密传输等。发展到目前为止，扫描的技术总类已经非常全面，数量也非常丰富，但随着网络安全管理的越来越严格，扫描也渐渐有了新的定义。并且最终会朝着全面性、隐蔽性以及智能性方向发展。

关键词 安全策略 蜜罐技术 PDRR

对网络扫描的基本技术进行编程实现，说明其实现过程。扫描程序都是在 Windows 系统下以 TCP/IP 协议为基础，在 VC++开发平台下通过 Winsock2.0编程接口来实现的。本系统主要实现了 Ping 连通扫描、TCP 连接扫描、半开放扫描、网络主机信息扫描和漏洞扫描几个基本功能。

1 Ping 连通扫描的实现

Ping 命令利用 Internet 协议（IP）向另一台计算机发送特殊的 IP 数据包来实现两端通信。网际协议（IP）中加有一种特殊用途的报文机制，这就是网际报文协议（ICMP），它是 IP 的一部分。网关和主机使用这种机制传送控制信息或差错信息，主机使用这种机制测试报宿主机是否可到达。

2 端口扫描模块的实现

端口扫描是向扫描目标的 TCP/IP 端口发送连接请求，根据对方的回应判断端口是否开放，在发送探测数据包之前进行。在扫描配置中，需要指定扫描的端口或扫描范围。寻找目标主机的漏洞必首先确定对方开放了哪些网络服务，即使是该主机可能有防火墙保护，只要开放了一些网络服务，那么安全性就会大降低。其实，漏洞扫描本身就是模拟黑客的入侵过程，只是程度有限制，要求尽可能小地影响被扫描对象，故基本上都是采用上述的 TCP Connect（）扫描和 TCP SYN 扫描。

2.1 TCP 连接扫描

全 TCP 连接扫描是长期以来 TCP 端口扫描的基础，这是最基本、最简单的一种扫描方式。此方法的缺点是扫描容易被发现，并且能被过滤掉，而且目标主机的日志文件也会记录连接。做为端口扫描的一种方法，其主要优点是实现简单，对操作者的权限没有严格的要求（有些类型的端口扫描需要操作者具有专长 root 权限），系统中的任何用户都可以有权利使用这个调用，另一个优点就是扫描速度快。使用 connect( )建立与目标主机的端口连接，完成一次三次握手的过程。其实现的原理可用下面的一段伪代码来展示其实现的原理：

```
for(port=LOW; port<HIGH; port++)
{
Csocket socket;
Socket.creat( );
Socket.connect(ip, port);
Socket.receive(infor);
}
```

在程序的具体实现过程中，启用了多线程[13]的扫描方式，可以根据扫描主机的数量，为不同的主机分配不同的线程，亦即对于每一个扫描线程，可以为其分配一定的数量的主机，这样就可以加快扫描的速度。当需要扫描的主机数目少于分配的线程数时，则每一个地址对应一个扫描线程。扫描线程的开始可用调用函数 AfxBeginThread( )。由于可打开多个套接字同时调用 Conncet（）函数，加快了端口扫描的速度。开启扫描线程后，首先要创建 socket，然后再连接对方的主机和端口号，若初始化失败则返回，并提示出错信息。若连接成功，则通过 receive( ) 函数来接收该端口的扫描信息，在显示端口扫描结果时，只显示已打开的端口号，未打开的端口则不显示其结果。由于不同的端口会有不同的反馈信息，这样就可以了解相关的端口的提供服务的情况和其开关的状态。扫描主机通过 TCP/IP 协议的三次握手与目标主机的指定端口建立一次完整的连接，这也是 TCP connnetct( ) 连接被命名为全连接扫描的实际意义来源。如果端口开放，则连接成功；否则返回-1，表示端口关闭。

2.2 半开放扫描

半开放扫描亦即 TCP SYN 扫描，这种技术通常被认为是“半开放”扫描。这是因为扫描程序不必要打开一个完全的 TCP 连接。扫描程序只发送一个 SYN 数据包，好象准备打开一个实际的连接并等待反应一样。在具体的实现过程中，TCP SYN 数据段必须通过手工构造。这里同样要使用原始套接字。

3 主机信息扫描的实现

主机信息探测是网络扫描的一个重要组成部分。所谓的主机信息包括操作系统的类型、版本、以及常用服务端口提供服务的类型、版本等信息。主机信息收集的目的就是要获取关于目标主机的这些信息。主机信息扫描的实现主要是通过 Socket 通信来获得同一网段内在线主机以及主机的相关信息。从而获取在线主机以及在线主机相关信息。可得到主机的 IP 地址、用户名、所属的工作组以及 MAC 地址等相关信息。

4 网络漏洞扫描

扫描的灵魂就是它所使用的系统漏洞库，漏洞库的完整性和有效性决定了其扫描和实现的效果。通过发送有探测特征的数据包，并对接收的数据包进行分析，从而发现其漏洞的存在与否。在程序的实现过程中，还要使用超时设计，以提供超时控制。根据不同漏洞的不同特征，对已经开放服务的端口进行测试就可以达到测试目标服务是漏洞。在 CGI 和 SNMP 的漏洞扫描过程中，也采用了同样的方法，通过对提供服务可能产生的漏洞的特征库进行比对，从而找出所提供的服务中是否包含有已经存在的漏洞，从而达到保证安全的目的。

参考文献

[1]高永强,郭世泽.网络安全技术与应用大典.北京:人民邮电出版社, 2003:178-180.

[2]谢希仁.计算机网络.大连:大连理工大学出版社,2000:15-18.

[3]杨先义,钮心忻.网络安全理论与技术.北京:人民邮电出版社,2003:16-34.

[4]朱雁辉. Windows 防火墙与网络封包截获技术.北京:电子工业出版社,2002:31-65.