文章编号:1005－0523(2002)03－0062－04

防火墙安全测试系统的研究与实现

汤文亮[1]，丁振凡[2]，汤　飞[1]

(华东交通大学 1.信息工程学院;2.现代教育技术中心,江西 南昌 330013)

摘要:介绍了防火墙安全测试的内容以及防火墙安全测试系统的设计与实现,并对系统中采用的安全测试方法如信息收集、系统破解、拒绝服务攻击、特洛伊木马、WIN9X漏洞攻击等进行了原理分析,阐述了使用Visual C++具体实现该系统的若干关键技术.

关　键　词:防火墙;安全测试;套接字;Visual C++

中图分类号:TP393.08　　**文献标识码**:A

0　引　言

防火墙技术作为网络安全中的一项重要技术受到广泛重视.对防火墙产品进行全面评测包括功能测试、性能测试以及安全测试三个部分.目前,大多数防火墙生产厂商的安全测试是借助ISS和SATAN等一些开放软件来进行的.这种开放软件的特点是功能强大,测试比较全面.但网络攻击与防范是一个不断变化的矛盾,为了适应网络攻击技术的变化和防火墙技术的迅猛发展态势,基于市场用户的应用需求,并结合具体的分组过滤防火墙及应用代理防火墙的产品特点,我们编写了一个防火墙安全测试系统,以达到公正、全面地评测此类安全产品的目的.

要实现防火墙安全测试系统,必须学会从入侵者的角度来思考问题,因为网上的安全隐患是入侵者与守护者共同的切入点.由于黑客实施攻击的一般步骤包括信息收集、系统破解和攻击实施这三个阶段,因此防火墙安全测试系统的设计思路是:采用类似于黑客攻击的方式对防火墙本身及防火墙所保护的内部网络实施扫描和攻击测试,以证实被测的安全产品的安全性.

1　防火墙安全测试内容

防火墙的安全测试包括例行测试、攻击测试和安全检测三类测试.如图1所示[1].其中,例行测试的内容包括用户数据保护、标识与鉴别、密码支持、可信安全功能保护、安全审计等安全功能要求的检测.例行测试难以用程序实现自动测试,检测手段主要依靠测试人员依照“防火墙测试要求”等相关标准进行逐项分析和检测.而攻击测试和安全检测则适合自动测试.因此,防火墙安全测试系统主要实现后两类安全测试.

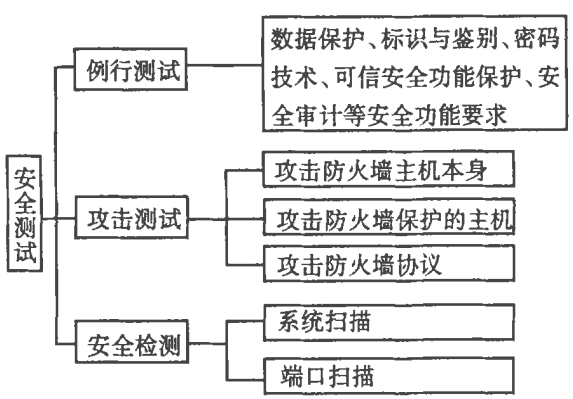

图1　安全测试的测试内容

收稿日期:2001－11－25

作者简介:汤文亮(1969－),男,江西南昌市人,华东交通大学讲师,工学硕士.

为证实被测产品的安全性,在测试平台的内网或外网上安装现有的扫描工具和攻击工具后,应利用所有可能的方式对被测产品进行扫描和攻击测试.但在具体实施测试之前,首先要从网络上收集有关的安全信息,如操作系统的漏洞、协议的弱点等,通过比较,判断防火墙是否有类似安全问题.或者直接阅读供应商提供的文档,如功能说明书、管理者指南、规则配置等,发现其中的潜在的安全问题.有了这些准备工作,就可以进行安全测试了.

常用的攻击方式有 3 种:

1) 攻击防火墙主机本身.配置并运行扫描器以发现目标主机某些内在的弱点.这些弱点可能是破坏目标主机安全性的关键因素,利用这些弱点再进行下一步的攻击.

2) 攻击防火墙所保护的主机.同样,运行扫描器,针对防火墙保护的网段.可以验证在没有配置任何规则的情况下,它是否的确能禁止掉所有对内部网络的访问,并判断防火墙对内部网络的保护能力到底如何.如果了解到内部网络服务器使用某种系统,就可以利用这种系统一些已知的缺陷进行下一步的渗透.因此,防火墙必须包含两种保护关系即保护它自身免受攻击以及保护内部网络免受攻击.

3) 攻击防火墙协议.防火墙使用的协议本身可能也有其安全问题.

从网络中对被测产品实施攻击,被测产品必须经受住攻击,至少应该达到如下要求:

1) 攻击者对被测产品实施攻击后,仍无法获得对防火墙或其底层操作系统的管理与控制.

2) 除了满足防火墙功能所要求的服务之外,其它任何协议或数据内容均不能通过防火墙送到内部网络.

3) 被测产品在遭受拒绝服务攻击时,要么具有掉电保护机制,并能根据设定的策略停机且在停机前要提供日志和告警,要么就必须能够防御这种攻击.

2　系统的功能及原理分析

设计防火墙安全测试系统时,我们将系统分为扫描特区、系统破解、拒绝服务攻击、特洛伊木马、Win9x 漏洞攻击 5 个部分,每一部分又包括大量的实用程序.实现该系统的过程中,除了部分自主编制的攻击程序外,还改编了许多从网上精心挑选出来的黑客高手的“作品”.系统构成具体如下:

1) 扫描特区:E－mail 查询、在线 IP 扫描、端口扫描、OICQ 查询、免费 IP 查询、对方位置及 IP 查询、聊天室的 IP、信息收集、IP 监视等.

2) 系统破解:E－mail 密码、FTP 密码、WWW 密码、OICQ 密码、NT 密码、PWL 密码、网上信用卡、字典、网络刺客等.

3) 拒绝服务攻击:E－mail 炸弹、UDP 炸弹、ICMP 炸弹、IGMP 炸弹、OICQ 炸弹、IRC 炸弹、端口攻击器、手机轰炸、远猫掉线等.

4) 远程控制:FTP 程序、冰河、BO2K、Netspy、捣蛋鬼等.

5) 漏洞攻击:OOB 攻击、IIS 攻击、OUTLOOK 攻击、Iphacker 等.

另外,为了便于测试人员使用,该系统还采用切分视图(SplitterWnd)[2]的形式.程序启动后的界面左侧分页面是树形视图(CTREEVIEW),可以对各种攻击工具进行选择;右侧分页面是超文本视图(CHTMLVIEW),提供各种攻击手段的原理以及各种工具的使用说明.这样做的好处是能保证攻击实施与说明文档的同步,即测试员在左侧选择了相应的攻击工具以后,右侧的 CHTMLVIEW 中会自动显示有关该工具的详细使用说明.

2.1　扫描特区原理分析

扫描特区完成的是信息收集阶段的工作.一个端口就是一个潜在的通信通道,也就是一个入侵通道.对目标计算机进行端口扫描,能得到许多有用的信息包括计算机的硬件信息、运行的操作系统信息、应用程序信息、目标计算机所在网络的信息、目标计算机的用户信息、存在的漏洞等等.进行扫描的方法很多,可以是手工进行扫描,也可以用端口扫描器进行.

在手工进行扫描时,需要熟悉各种命令,可以对命令执行后的输出进行分析.扫描器是一种自动检测远程或本地主机安全性弱点的程序,通过使用扫描器可以不留痕迹地发现远程服务器的各种 TCP 端口的分配及提供的服务和它们的软件版本,这就能让我们间接的或直观的了解到远程主机所存在的安全问题.扫描器通过选用远程 TCP/IP 不同的端口的服务,并记录目标给予的回答,通过这种方法,搜集目标主机的有用信息.目前常用的扫描原理有 TCP connect( ) 扫描、TCP SYN 扫描、TCP FIN 扫描、UDP recvfrom( )和 write( ) 扫描、ICMP echo 扫描等.

2.2　系统破解原理分析

系统侵入主要有 3 种方法：一是利用口令破解进入系统；二是采用 IP 欺骗手段；三是采用缓冲区溢出方法.

1) 口令破解器的工作原理如下：首先用固定的加密算法对从口令侯选器送来的单词进行加密；然后将从口令加密里出来的密文和要破解的密文进行比较.如果一致，那么当前侯选口令发生器中出来的单词就是要找的密码.如果不一致，则口令发生器再产生下一个侯选口令.其中侯选口令产生器的作用是产生认为可能是密码的单词.攻击者通常都将这些单词收集到一个文件里，叫做字典.在破解密码时，从这些字典里取出侯选口令.

2) IP 欺骗主要进行以下工作：使得被信任的主机丧失工作能力，同时采样目标主机发出的 TCP 序列号，猜测出它的数据序列号；伪装成被信任的主机，同时建立起与目标主机基于地址验证的应用连接.如果成功，黑客可以使用一种简单的命令放置一个系统后门，以便以后进行非授权操作.

3) 缓冲区溢出是一种系统攻击的手段，通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其它指令，以达到攻击的目的.

2.3 拒绝服务攻击原理分析

拒绝服务攻击是指一个用户占用了太多的共享资源，使其他用户无资源可用，其服务只能被拒绝.拒绝服务有两种类型，一种是破坏或毁掉资源使得谁也不能用，另一种使服务器超载或非法地独占系统资源.

2.4 特洛伊木马原理分析

特洛伊木马是一个程序，它驻留在目标计算机中.在目标计算机系统启动的时候，自动加载，然后在某一端口进行侦听.如果在该端口收到数据，对这些数据进行识别，然后按识别后的命令，在目标计算机上执行一些操作.比如窃取口令，拷贝或删除文件，修改注册表或重新启动计算机等等.攻击者一般在入侵某个系统后，想办法将特洛伊木马拷贝到目标计算机中.并设法运行这个程序，从而留下后门.以后只要运行该特洛伊木马的客户端程序，便可对远程计算机进行操作.

2.5 漏洞攻击原理分析

漏洞就是指系统中不尽完善的地方，如操作系统的漏洞、协议的漏洞以及各种应用程序的漏洞等等.漏洞攻击就是黑客利用这些不完备之处对系统进行破坏.常见的漏洞有 OOB 漏洞、零字节漏洞、IIS 漏洞、OUTLOOK 漏洞等.

3 系统实现中的若干技术问题

3.1 系统界面设计

防火墙安全测试系统界面的实现，其关键在于切分视图中的左侧树形视图(CTREEVIEW)与右侧超文本视图(CHTMLVIEW)的关联.对左侧树形视图的每一个节点赋于一个特定的值，当树形控件被点击时，触发事件 OnSelchanged()，根据节点对应的特定值进行相应的操作.

1) 初始化部分代码.在这部分代码中将树形视图的每一个节点与一特定的值关联起来，关键代码如下：

```
HTREEITEM hTreeItem0;
HTREEITEM hTreeItem1;
hTreeItem0=m-tree1->InsertItem("资料阅读",0,1,TVI-ROOT,TVI-LAST);
m-tree1->SetItemData(hTreeItem0,0x0100);
hTreeItem1=m-tree1->InsertItem("扫描工具",0,1,hTreeItem0,TVI-LAST);
m-tree1->SetItemData(hTreeItem1,0x0110);
```

2) 事件触发部分.树形视图中某一节点的改变将触发此函数，可通过与此节点相关联的值执行相应的操作，包括调用特定的可执行文件以及相关的帮助文件.关键代码如下：

```
void CLeftView::OnSelchanged(NMHDR * pNMHDR, LRESULT * pResult)
{
NM-TREEVIEW * pNMTreeView = (NM-TREEVIEW * )pNMHDR;
CTreeCtrl * pT=&(GetTreeCtrl());
HTREEITEM hSel=pT->GetSelectedItem();
strcpy(cur,main);
if(hSel)
{
DWORD dwItem=pT->GetItemData(hSel);
TRACE("sel%02d:%02d/n", HIWORD(dwItem)-1, LOWORD(dwItem)-1);
CMainFrame * pF=(CMainFrame * )(AfxGetApp()->m-pMainWnd);
CMainctrlView * pV=pF->GetRightPane();
switch(dwItem)  //比较节点所对应的特定值
{
case 0x0110:
strcat(cur,"\html\tf-port.htm");
```

```
pV->Navigate2(cur,NULL,NULL);
break;
case ……
}
}
}
```

3.2 特洛伊木马程序的实现技术

特洛伊木马程序的编制分为服务器端和客户端两个部分.服务器的主要功能是接受来自客户端的控制命令(这些命令是服务器与客户机事先规定好的一套协议),然后进行破译完成相应的操作,最后把结果返回客户端;客户端的主要功能是向服务器端发送控制命令以及接受服务器端返回的操作结果,并进行回显.

下面介绍特洛伊木马程序编制的几个主要步骤:

1) 服务器与客户机之间通讯命令协议的制定.程序中把每一个控制命令指定为一固定的值,在客户机和服务器的主程序的头文件中声明.

2) 客户机程序中命令代码的发送.在客户机与服务器的连接建立起来以后,客户机每选择好一定的命令后如"远程关机",那么客户机将把对应于命令的某特定值(SYS-SHUT)发送到服务器端.还有许多命令需要带参数发送,如"消息发送",那么客户机传送的就不止是命令代码,而且需要附带所要发送的消息.下面是发送"发送消息"命令的一段代码:

```
void CLeafPage2::OnButton2()
{
UpdateData(TRUE);
int code=MSG-SEND;
char sztemp[10];
char strsend[1025];
-itoa(code,sztemp,10);
strcpy(strsend,sztemp);
strcat(strsend,(LPSTR)(LPCTSTR)m-Box-con);
((CRomotectrlDlg * )m-pWnd)->SendType(strsend);
}
```

3) 服务器端对命令代码的接收及解释.当客户机发送过来命令以后,服务器端应该接受命令代码并进行相应的解释,执行客户端要求的操作.实现代码如下:

```
iRcvd=m-sConnectSocket.Receive(pBuf,iBufSize);
if(iRcvd==SOCKET-ERROR){ }
else {
pBuf[iRcvd]=NULL;
strRecvd=pBuf;
value=atoi(strRecvd.GetBuffer(4));
itoa(value,strtemp,10);
m-CmdList.AddString((CString)strtemp);
UpdateData(FALSE);
DoSwicth(value,pBuf);
}
```

4) 完成上述操作后,该程序的基本框架已经构建好,余下的工作就是完成对服务器主机的各种控制的实现,如修改注册表、文件管理等等.

3.3 OOB 炸弹程序的编制

这个程序利用 Win9x/WinNT 的 OOB 漏洞,对目标主机的 135 端口或 139 端口发送大量的数据包,所以这个程序既是拒绝服务攻击原理的实例,又是漏洞攻击的一个实例.该程序的实现机理是比较简单的,它首先对套接字进行初始化、创建、绑定、连接;连接成功后,再发送大量的数据实施攻击.

3.4 IP 扫描工具包的实现技术

此工具包包括本机 IP 查询功能和 PING 程序两部分.

1) 本机 IP 的查询主要是通过调用 gethostname()与 gethostbyname()两个函数实现的.

2) PING 程序是利用数据报套接字进行传输的.PING 程序的编写主要分为 ICMP 头的定义、待传送 ICMP 头的设置、求 ICMP 头的校验和、用 socket 发送数据报、接收数据报并进行判断几部分.

4 结束语

防火墙安全测试系统可以用于对常见的防火墙产品(包括分组过滤防火墙和应用代理防火墙)进行安全测试,其特点是实用、针对性强,而且便于操作.该系统与其他的开放软件是互为补充的关系.防火墙安全测试系统的设计与实现正是一个迅速集成当前"最优秀"自由攻击软件的平台.由于信息安全的特点是"道高一尺,魔高一丈"的矛盾统一体,随着计算机应用的进一步普及与发展,计算机信息系统安全问题日益社会化、严重化,新的安全漏洞将不断地被发现,防火墙的安全性能也将不断地提高,因此该防火墙安全测试系统提供了很好的可扩展性,以满足新的测试要求.系统的进一步改进包括增加被测产品的脆弱性自动分析和报表产生等功能.

(下转第 68 页)

立了一些语言室、多媒体教室、计算机网络教室等综合类现代教学媒体组合教场所，使得硬件设施的配置达到了一定规模，这些都有力地推动了现代教育技术在学校教育实践中的应用.但随着科技不断发展，新的教育媒体硬件设备也在不断涌现，高校原有硬件设备配置也将随着形势的发展而变得落后与陈旧.为此，高校必须加大对现代教育硬件设施的投资力度，时刻注意保持添置和更新，采取各种方式来加大、加快高校现代教育技术硬件设施的建设，营造出一个有利于现代教育技术推广应用的良好的硬件设施环境.

综上所述，现代教育技术实践环境建设是一项长期的、艰巨的系统工程，这就要求各级领导和广大教育技术工作者紧紧把握现代教育技术飞速发展的脉搏，切实抓好教学资源和教学过程的设计、开发、应用和管理以及硬件环境建设，积极为多媒体教学、远程网络教学铺路搭桥，为深化教学改革，全面提高教学效益和教学质量做出新的贡献.

参考文献：

[1] 董 飞，赵建民，旷宗仁.现代教育技术支持下的新型教学模式建构[J].山东师大学报(自然科学版)，2001，(16)：334～336.

[2] 邬正义.计算机教育和师范信息素质培养[J].淮北煤师院学报，2001，(22)：68～71.

On the Practical Environmental Building of Modern Educational Technology

HUANG Yong

(Modern Educational Technology Center, East China Jiaotong University, Nanchang 330013, China)

Abstract: Based on the existing practical problems on environmental building of educational technology, this essay intends to pride readers with the writer's own thought of reform.

Key words: C·A·D; multi-media technology; CAI courseware

(上接第 65 页)

参考文献：

[1] 汤文亮.应用级防火墙测试规范的研究[J].华东交通大学学报，2001，18(4)：36～39.

[2] 康博创作室，等. Visual C++6.0 高级开发教程[M].北京：人民邮电出版社，1999.

Research and Implementation of Firewall Security Test System

TANG Wen-liang[1], DING Zhen-fan[2], TANG Fei[1]

(1. School of Information Eng.; 2. Modern Educational Technology Center, East China Jiaotong University, Nanchang 330013, China)

Abstract: This paper introduces design and realization process of firewall security test system and the security test on firewall, and then analyzes the principles of several attacking programme such as information collecting, system cracking, DoS, Trojan horse, Win9x attacking and etc. Lastly it also expatiates several key techniques for developing the system by Visual C++.

Key words: firewall; security test; socket; visual C++