书+CD
19.8元

黑客防线 推荐

详细+精彩+实例+图解=提高

远程控制与攻击技术揭秘

一本精而全的远程攻击与防范手册
完全披露各种远程攻击技术的读物

内容简介

本书面向广大初级读者。第一、二、三章由浅入深，分门别类地介绍了各种系统的远程控制的特点和方法，尤其对常见操作系统远程控制的阐述更为详细。通过实例演示和实况截图，即使是稍有一点点基础的初学者也能按部就班地轻松上手。

第四、五、六、七、八章分别介绍了远程攻击技术，由于考虑到这方面内容可能会造成不良影响，故而取消了所谓“黑客技术”中的一些危害普遍且没有有效防御措施的攻击方法演示（如拒绝服务攻击、分布式拒绝服务攻击等没有必要在本书中讨论的问题）。另外，“黑客技术”中的后门制作也是重头戏，但本书并不准备作为纯粹普及黑客技术之用，本书的初衷在于向初学者普及比基础知识稍高的技术，故斟酌后决定涉及远程攻击的内容只讲解对初级系统管理员有所帮助并且有必要了解的安全知识，只有让他们懂得如何入侵，才能更好地做好防范工作。

本书适合有一些计算机及网络基础知识的读者，可以当作初级爱好者的入门读物，亦可做为初级系统管理员的参考手册。

CD+书=19.8元

CN15—9201/TP

9 78792 01/TP

通信地址：北京市中关村邮局008信箱
邮政编码：100080
收款单位：黑客防线邮购部
电话：010-62141446
e-mail：yougoubu@hacker.com.cn

远程控制与攻击技术揭秘

谭 术 郭聪辉 编著

家庭电脑世界杂志社

黑客防线编辑部

前　言

在网络技术飞速发展的今天，网络中的主机使用的操作系统普遍都有很强的远程控制功能，远程控制给网络系统管理员们提供了极大的方便。如何实现远程控制和保证网络安全是系统管理员需要注意的两大任务，具备这两方面知识的系统管理员才算得上是称职的系统管理员。

国内互联网出现较晚，但发展较快，网站、服务器数量急剧增多，可是国内系统管理员水平普遍不高，有些对安全丝毫不了解的人也试着维护国际互联网上的服务器，这就导致了国内网站安全失误屡屡发生。

本书是为具有初级计算机网络知识水平的朋友而撰写的，主要目的在于普及必要的网络管理知识，国内现在专业人士数量相对较少，低水平的用户数量却很多。我国的初级计算机教育用处不大，只能给学习者培训一身没有什么现实用武之地的所谓“基础知识”。本书可以帮助这类接受过计算机基础教育的朋友通过自学和简单的实践把自己的“报废本领”升华为极为实用的技术。当然，现在是 2003 年，我国计算机普及教育带来的“报废本领”并不能直接与本书知识接轨，这需要读者对本书涉及的操作系统稍有实践经验。

作为系统管理员，或者在没有经验的情况下，准备为企业或其他类似机构做远程控制、安全维护工作的朋友，或者想对相关内容进行初步学习的朋友都可以将本书当作入门书刊或手册，本书尽量使用通俗易懂的语言以便读者可以轻松理解。

书中部分内容经过朋友的同意后引用了他们的文章，因为他们在相应的领域中都有很高的造诣，我自然没有能力写出比他们更优秀的文章，他们的文章将对读者更有帮助。本书初衷在于给予读者最大的帮助，而不是为了显示作者微不足道的“水平”。这和抄袭是两码事。

在这里必须声明的是，本书虽然不属于黑客技术的专门书籍（作者认为在读者没有一个思想上的正确认识之前，普及攻击性较强的知识根本就是“给潜在的恐怖分子发放武器”），但为了达到让从事系统管理或其他相关工作的朋友更好地做好防范工作，所以里面有很多内容是涉及黑客入侵技术的，正所谓“知己知彼，百战不殆”，这方面具有攻击性的内容在本书中是不可避免的。希望读者有一个正确的认识，不要运用本书中的内容从事不法活动，否则一切后果都由不法活动制造者承担，作者不负任何责任。

本书尽量做到通俗易懂，并且剔除了所有的国内所谓黑客书籍中对管理员、爱好者没有多大帮助或者会产生反作用的内容（如破解 E-mail 邮箱，利用恶意程序入侵个人计算机，拒绝服务攻击、分布式拒绝服务攻击，ICQ、OICQ 攻击等等没有多大意义的知识）。

编　者

2003 年 9 月

目 录

第 1 章 远程控制概述 1

1.1 什么是远程控制 1

1.1.1 远程控制的方法及特点 1
1.1.2 不同操作系统上的远程控制机制 2

1.2 远程控制的利弊 5

1.3 总结 5

第 2 章 Windows 系统实现远程控制 6

2.1 Windows 系统的特点及适用的远程控制方式 6

2.2 Windows 9X/ME 系统适合的远程控制工具 6

2.2.1 远程控制软件（特洛伊木马类程序） 7
2.2.2 文件共享 16

2.3 Windows NT/2000 适合的远程控制工具 18

2.3.1 Terminal Service 的特点及详细使用介绍 18
2.3.2 Telnet 23
2.3.3 pcAnyWhere 的特点及详细使用介绍 26
2.3.4 DameWare 的特点及详细使用介绍 33
2.3.5 Windows 2000 的命令行管理工具 37
2.3.6 文件共享 48

2.4 总结 52

第 3 章 类 UNIX 系统实现远程控制 53

3.1 类 UNIX 系统的特点及适用的远程控制方式 53

3.2 系统自带的远程控制服务 53

3.2.1 Telnet 服务的特点及默认使用介绍 54
3.2.2 SSH 服务的特点及默认使用介绍 55

3.2.3 远程输出 X-window 66
3.2.4 Windows 下的 X 远程管理软件 67
3.2.5 r 系列命令 79

3.3 总 结 81

第 4 章 远程攻击 Windows 系统 82

4.1 远程攻击 Windows 系统概述 82

4.2 Windows NT/2000 系统攻击思路 82

4.2.1 FTP 服务应用程序容易产生的漏洞 82
4.2.2 IIS 默认安装存在的一些漏洞 83
4.2.3 Windows 平台各种数据库存在的漏洞 84

4.3 基于 Web 的攻击（CGI） 84

4.3.1 LB5K 安全性分析(该漏洞由 analysist 提供) 84
4.3.2 BBS3000（该漏洞由 shocker 提供） 88
4.3.3 动网 ASP 论坛 90
4.3.4 ut 论坛脚本漏洞(该漏洞由 shocker 提供) 92
4.3.5 AGB II V1.2 多用户版(免费版) 96

4.4 安全隐患讨论 97

4.4.1 ASP 存在的安全隐患 97
4.4.2 CGI 存在的安全隐患 101

4.5 基于系统漏洞的攻击 106

4.5.1 Unicode 解码漏洞 106
4.5.2 da/idq 暴露系统 Web 目录及缓冲区溢出漏洞 107
4.5.3 .printer 缓冲区溢出漏洞 109
4.5.4 MS SQL 2000 Resolution 服务远程堆缓冲区溢出漏洞 110
4.5.5 asp.dll 缓冲区溢出漏洞 110
4.5.6 3389 微软拼音输入法漏洞 113
4.5.7 IIS5.0 WebDAV 远程溢出漏洞 116
4.5.8 Remote Procedure Call 安全漏洞 128

4.6 基于口令的攻击 138

4.6.1 基于 IPC 远程管理共享的口令攻击 138
4.6.2 基于 FTP 口令破解 143

4.6.3 基于 MS SQL 口令的破解 144
4.6.4 基于 MYSQL 口令破解 145
4.7 基于远程控制软件的攻击 146
4.8 总 结 146
第 5 章 远程攻击类 UNIX 系统 147
5.1 远程攻击类 UNIX 系统概述 147
5.2 类 UNIX 系统攻击前需要了解的知识 147
5.2.1 类 UNIX 系统攻击必须具备的知识 148
5.2.2 远程访问 149
5.2.3 入侵的思路 150
5.3 对 Web 的攻击 152
5.4 基于系统漏洞的攻击及分类 154
5.4.1 按漏洞可能造成的直接威胁分类 154
5.4.2 按漏洞的成因分类 158
5.4.3 对漏洞严重性的分级分类 159
5.4.4 按漏洞被利用方式的分类 159
5.5 基于口令的攻击 161
5.5.1 口令的猜测攻击 161
5.5.2 如何获得用户名 162
5.5.3 本地口令攻击 163
5.6 缓冲区溢出攻击 164
5.7 输入验证攻击 167
5.8 获得 Shell 168
5.9 总结 168
第 6 章 缓冲区溢出攻击详细介绍 169
6.1 如何编写自己的缓冲区溢出利用程序 169
6.2 Buffer overflow 是如何产生的 169

6.3 UNIX 下 C 语言函数调用的机制及缓冲区溢出的利用 170
6.3.1 进程在内存中的影像 170
6.3.2 函数的栈帧 171
6.3.3 缓冲区溢出的利用 172
6.3.4 缓冲区在 Heap(堆)区或 BBS 区的情况 173
6.4 从缓冲区溢出的利用可以得到什么 173
6.5 存在问题的程序案例 174
6.6 编译及运行 175
6.6.1 例程 p.c 在 Linux x86 平台下的剖析 175
6.6.2 溢出分析 206
6.6.3 如何攻击 213
第 7 章 穿过防火墙进入内网 221
7.1 认识内网 221
7.2 利用 TCP Socket 数据转发进入没有防火墙保护的内网 221
7.2.1 攻击流程 222
7.2.2 程序代码 223
7.3 利用 TCP Socket 转发和反弹 TCP 端口进入有防火墙保护的内网 230
7.3.1 攻击流程 231
7.3.2 程序代码 232
7.3.3 总结 238
第 8 章 物理攻击与安全 240
8.1 物理安全 240
8.2 正常的防范措施 241
8.3 总 结 242

第 1 章　远程控制概述

1.1　什么是远程控制

远程控制在这里是指利用网络连接进行对非本地计算机的控制。不同的操作系统一般都有适合自身的远程控制机制，因为系统各有特点，所以他们的远程控制机制也各不相同，比如类 UNIX 系统的特点是在命令行下可以进行所有（除运行必须在 GUI 里运行的第三方程序外）的系统设置，所以它只要具备 Telnet、SSH 等功能就已经可以在很大程度上满足远程控制的需要了。当然，为了可以远程使用 X-windows，现在的类 UNIX 系统几乎都具备远程 X-window 管理功能，但使用这个的用户比起使用命令行的用户可就少多了。而 Microsoft Windows 操作系统并不像类 UNIX 系统那样命令行与 GUI 完全分开，所以在 Windows 操作系统上单纯使用命令行进行远程控制，有很多功能都是不能使用的（有时使用大量的第三方工具可能可以通过命令行实现远程控制的更多功能，但即使这样仍然有很多功能不能实现，且非常繁琐）。所以 Windows 操作系统的远程控制更趋向于 GUI，而不是命令行。

互联网的发展已经使得全局管理成为必要，机器的数量永远要比系统管理员的数量多得多，这就意味着一个管理员要管理数台机器，而所有的机器不一定都在一起，为了使管理员们把时间用在工作而不是路途上，远程控制就显得非常必要了。本章就来详细讲述常用操作系统的一般远程控制方法。

1.1.1　远程控制的方法及特点

远程控制的方法基本一样，都是本地操作系统用特定的程序连接远程主机，如果远程主机有与之相匹配的服务或守护程序，那么就建立连接，这些守护程序有些设有身份验证，有些没有，没有的就直接建立连接，然后开始远程控制。有身份验证的就辨别远程登录用户的合法性，然后或通过验证开始远程控制，或身份验证信息出错，把远程登录用户拒之门外。常见的有 Telnet、SSH、Terminal Service 等等。

使用命令行进行远程控制的特点在于传输速度较快，且系统通用性较广，比如 Windows 2000 Telnet Client 使用 Telnet 协议和部分 TCP/IP 协议套件，通过网络连接远程计算机。Telnet 客户软件允许计算机连接到远程服务器。你可以使用 Windows 2000 提供的 Telnet Client 连接到远程计算机，登录到远程计算机，并且与它交互操作，好像你正坐在它的前面。这既可以连接 Windows 系统，也可以连接类 UNIX 系统或部分其他类型的操作系统。但弊端在于 Windows 系统并不容易用远程的命令行控制来完成所有工作。

GUI 的远程控制程序（如 Windows 下的 Terminal Service、pcAnyWhere 等）因为是为

自己的操作系统量身定做的程序，所以就只能连接远程有相应守护程序的主机。不论是UNIX 下的 GUI 远程控制软件还是 Windows 下的，都没有什么通用性可言。

1.1.2 不同操作系统上的远程控制机制

不同操作系统（Windows9X/ME、WindowsNT/2000、类 UNIX 系统）上的远程控制机制自然有很大区别，因为系统的特性不同，所以对他们进行远程控制就要看情况而定了。

1. Windows 9X/ME 操作系统

此类操作系统属于 Microsoft Windows 系统中偏向于单机工作站考虑而设计的操作系统，虽说支持网络，但与 Windows NT/2000 这类基于 NT 技术构架的操作系统相比，Windows 9X/ME 的网络功能就非常匮乏了，对此类系统进行远程控制就需要一些第三方程序，比如要 Telnet 上一台 Windows98 机器，想要让它像 Windows NT/2000 一样打开 Telnet 服务然后静候远程用户的登录几乎是不可能的，所以你可能就需要在这台 Windows 98 机器上借助 Winshell，ncx99 等程序来实现此功能。

由于 Windows 系统中针对网络的操作系统是 Windows NT/2000，所以微软在 Windows 9X/ME 的远程控制上就没有下很大的工夫（因为偏向于单机工作站，所以也没有必要对其网络方面下与 NT 同样大的工夫）。这样就导致了它不具备像 Windows 2000 Server 里面的 Terminal Service 这样优秀的远程管理程序，那么应该怎么办呢？显然要对 Windows 9X/ME 系统进行比较完全的远程控制还需要第三方软件的配合，如一些软件厂商发布的商业远程控制软件，如赛门铁克的 pcAnyWhere（图 1-1）。但因为这些商业远程控制软件普遍都不

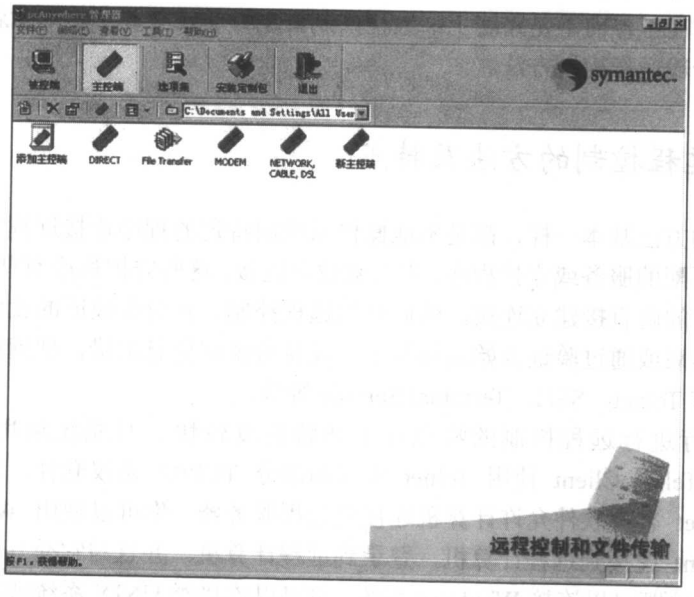

图 1-1 pcAnyWhere

是免费的，所以除此之外还可以选用各种编写优秀的特洛伊木马程序来进行远程控制，如

国产的“冰河”（图 1-2），国外的“SUB7”等，优秀的特洛伊木马实现的远程控制功能并不比商业版的远程控制软件逊色多少。

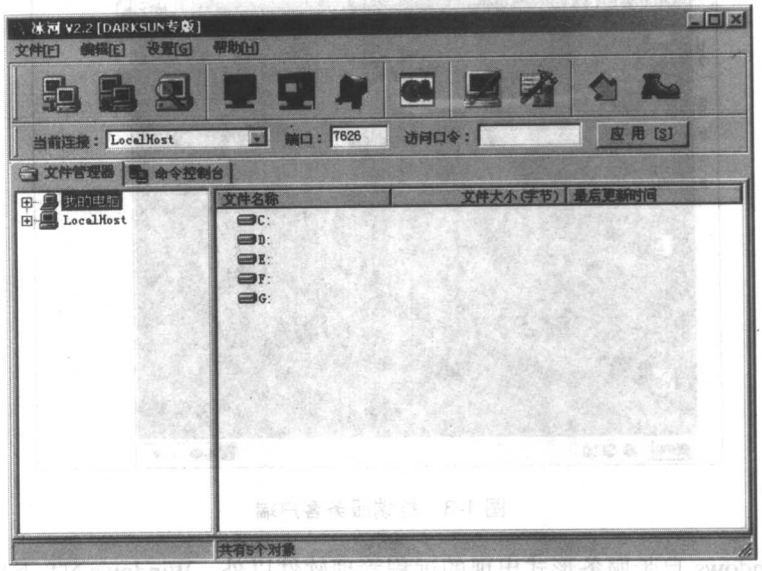

图 1-2　冰河

2．Windows NT/2000 操作系统

Windows NT/2000 系统才能真正算得上是 Microsoft 的网络操作系统。为了便于理解，我们把网络操作系统这样定义：

网络操作系统是实现网络通信的有关协议以及为网络中各种用户提供网络服务的软件集合，其主要目标是使用户能够通过网络上的各个计算机站点去方便而高效地享用和管理网络上的各类资源，包括数据、信息、软硬件资源等等。

虽然 Windows 9X/ME 也具备网络功能，但与 Windows NT/2000 相比却是一个天上一个地下，所以单从对网络的支持程度来看，就可以意识到 Windows NT/2000 的远程控制机制会有很大的不同。事实也是如此！NT 中自带了 Telnet 服务、IPC 连接等等，在 Windows 2000 Server 中更增添了像 Terminal Service（图 1-3）这样方便的远程管理服务。甚至可以远程直接管理注册表，因为 Windows 系统的所有设置都是基于注册表的，完全可以想像到这是多么地方便。

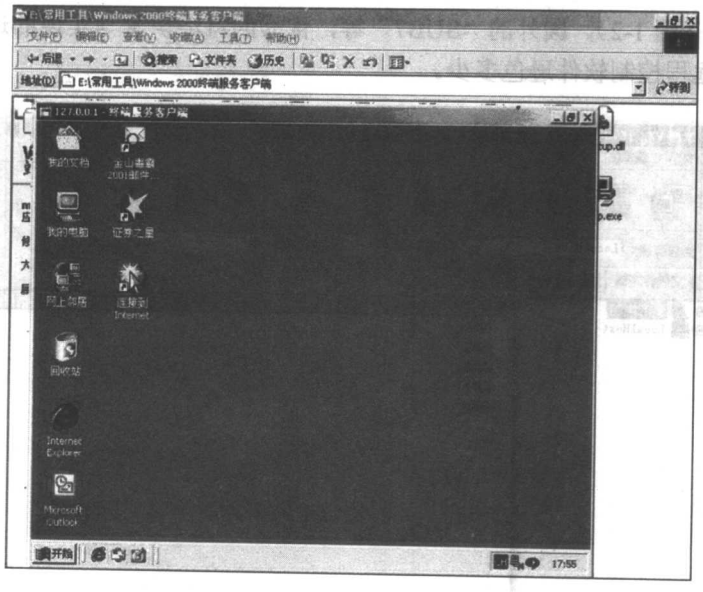

图 1-3　终端服务客户端

除了 Windows 自带服务形式出现的远程管理软件以外，Windows NT 下也有不少优秀的第三方管理软件，比如 pcAnyWhere（图 1-1）等。

Windows NT/2000 虽然也可以使用特洛伊木马程序进行远程控制，但是一般来讲，完全没有这个必要。

3. 类 UNIX 操作系统

Linux、*Bsd、SunOS（Solaris）、SCO UNIX 等等类似的操作系统统称为“类 UNIX 系统”（以下均简称为 UNIX），这类操作系统无一例外都属于网络操作系统，它们中的每一个都是网络上的好手。UNIX 是有价值的高效的多用户和多任务的操作系统。

这里不想过多地介绍 UNIX，只是从远程控制的角度来简要说说它的特点。现在的 UNIX 系统大都具备像 MS Windows 这样的 GUI 界面（图形化用户界面），UNIX 系统中这样的 GUI 界面称为 X-windows，但系统并不像 MS Windows 那样完全依靠它，Windows 的图形化用户界面与系统核心是相辅相成的一个整体，这也就意味着如果 Windows 的 GUI 瘫痪了，那么随之崩溃的还有整个操作系统。而 UNIX 却不是这样的，它的 GUI 和系统核心完全分开，即使 GUI 界面出现致命问题也不会对整个系统造成威胁，在 UNIX 的 GUI 崩溃时，完全可以在控制台中杀掉 X-windows 的进程然后重新启动它。有经验的 UNIX 系统管理员除非必须使用 GUI 界面的程序（比如播放影音文件、或者作为一个日常用的工作站），一般是无需启动 X-windows 的。这是因为 UNIX 的系统设置都可以在命令行里完成，并且初学者们一般也会渐渐从 GUI 界面的使用中回到命令行环境中来，因为在具备一定水平之后会感觉到在 GUI 中对系统进行复杂的设置并不会感觉比命令行方便，并且没有命令行这样直观、快捷。

从上述特点中不难看出，对 UNIX 系统进行远程控制时有命令行环境就已经足够了。所以我们一般情况下远程控制 UNIX 系统时用的是 Telnet，为了保密起见还可以使用 SSH。

但是 UNIX 毕竟还是有 X-windows 的，如果确实需要远程使用 X-windows，那么 UNIX 还有远程 X-windows 管理程序可以使用，感觉和 Windows 2000 Server 的 Terminal Service 相似。

1.2　远程控制的利弊

既然是远程控制，有利方面自然是方便快捷、省时、省力。但是这里面存在的各种客观问题也不少，主要在于远程控制的局限性和它的安全问题。局限性不言而喻，主要体现在远程控制只能用在对软件和软件可以控制的硬件设备的远程控制上，如果硬件出现故障（如光盘驱动器损坏、内存烧毁等等），那么远程控制是无能为力的。另外面临的最大的问题就是远程控制的安全问题。可以想像，既然是远程控制，就存在一个远程控制者的身份问题，如果远程控制者是这台计算机的负责人，那么毫无问题，如果刚巧远程控制这台计算机的人是一个非法登录者，那么麻烦就体现出来了，要知道不是所有的人都会遵守你制定的规则。

每天全世界出现着无法统计次数的远程攻击行为，造成的损失有的甚至高达数百亿美元。远程攻击行为主要体现在对网络操作系统的设计漏洞进行攻击以及对数据传输时的数据安全性造成的潜在威胁上。这些都是多年以来想要解决却不能解决的问题。

1.3　总结

读者现在一定对远程控制有些概念上的了解了，本章的目的也就在于此。在后面的章节中将详细介绍各个操作系统的远程控制方法和一些具体操作的例子。

第2章 Windows系统实现远程控制

在前一章中已经对远程控制做了概述，想必读者对远程控制的重要作用和实用价值及其必要性都已有了一个框架式的了解，本章将详细讲解常见的几种 Microsoft Windows 系统的远程控制方法，其中每一步都可以按部就班地进行，并且力求“掰开揉碎”，使对此方面没有多少基础的读者也能轻松看懂，并且立刻就可以投入现实使用当中去。本章没有一环扣一环的知识，读者可以根据自己的需要直接跳到需要学习的章节中去而不会出现类似“前面的不懂，后面的就更不懂”的现象。

2.1 Windows系统的特点及适用的远程控制方式

因为 Windows 9X/ME 并不是 Microsoft 想向网络操作系统方面发展的操作系统，作为单机工作站它们是很优秀的，但是在网络方面不得不说它们并不是好的网络操作系统。因为网络方面的欠缺，所以要对这类操作系统进行远程控制就不好从系统本身的机制里找到优秀者了，正是因为这样才需要利用其他程序来对它进行较理想的远程控制。至于能从多大程度上控制远程主机，那就要看远程管理软件的强大程度了。

Windows NT/2000 虽然和 Windows 9X/ME 同出一门，但它们却是有很大区别的，Windows 9X/ME 偏向于单机，而 Windows NT/2000 就是完完全全的网络操作系统了，它在网络的支持方面与 Windows 9X/ME 不可同日而语，在系统本身就集成了许多功能强大的远程管理软件以及在 Windows 9X 里根本没有见过的东西，最典型的就是 Windows 2000 Server 里的 Terminal Service，它可以像使用本机一样远程实现一切功能，如果带宽足够大甚至感觉与使用本机没有太大区别。还有各种共享，如共享命名管道的资源（IPC$），可以在远程管理计算机和查看计算机的共享资源时使用。每个磁盘分区的默认共享可以使合法的远程用户对计算机中的文件灵活地进行控制。Telnet 在 Windows NT/2000 中也有极大的用武之地，它虽然不能做更改文件图标或者使用 GUI 程序其他类似的操作，但是对远程主机的系统设置，对用户、网络、计划任务等诸多方面的控制却绝对没问题。Windows NT/2000 在网络方面的灵活性可见一斑。

接下来将举例详细介绍几个 Windows 9X/ME/NT/2000 适用的远程管理方法以及远程管理软件的使用。

2.2 Windows 9X/ME系统适合的远程控制工具

为了最大效率地远程控制 Windows 9X/ME 系统，所以这里首推远程控制软件，这类专门针对 Windows 9X/ME 系统开发的远程控制软件，一般都可以非常稳定地在系统中工

作。除了昂贵的商业版远程控制软件，如赛门铁克的 pcAnyWhere 以外，既免费又好用且功能强大的就是各类特洛伊木马程序了，这类程序中有许多被查毒软件认为是病毒，有一部分读者也认为木马是病毒，甚至有人直接就称之为“木马病毒”，其实这些观点都是不对的。特洛伊木马只是隐蔽性很强的远程管理软件而已，它既不自行破坏任何东西，也不会自动感染、传播，不具备病毒的特性，所以把木马归为病毒是大错特错的。

工作中可以利用现成的特洛伊木马程序来进行远程主机的管理，读者会在使用中发现原来木马是如此方便的工具，当然，如果查毒软件从中作梗，那么要么停止掉病毒监控程序，要么就对程序做一些修改，使得病毒监控程序对它不做任何反应。甚至可以干脆就自行编写一个适合自己的程序（如果愿意的话）。

特洛伊木马有很多种类，有的会做大规模的文件关联，有的是采用反弹端口机制，既然是合法地控制自己的远程主机，那么普通的木马就可以了，没有大幅度地感染自己机器上文件的必要，也没有反弹端口的必要。要的是控制简单、功能强大、稳定可靠的程序，例如功能强大而又配置灵活的“冰河”。接下来就来看一下它的具体使用方法。

2.2.1　远程控制软件（特洛伊木马类程序）

本部分主要讲述使用特洛伊木马程序远程控制 Windows 9X/ME 系统的具体方法，为了方便国人使用，现推荐一款国产木马程序——冰河 2.2 Darksun 专版。为什么推荐这一款呢？这是因为此软件经过了多年多人的测试且普遍评价良好：功能强大，配置简单明了，易学易用，稳定可靠。读者们在网络上可能经常见到其他版本，但笔者不推荐使用，因为那些所谓的新版本都不是通过对代码的改进而来，而是使用 32 位编辑器（如 UltraEdit）改掉版本号和作者名字而来，稳定性不敢保证。本节最后将讲述一些必要的技巧，现在先说说冰河的使用方法。

本软件包含如下几个文件：

（1）G_Client.exe ：冰河控制端程序。

（2）G_Server.exe ：冰河服务端程序。

（3）Readme.txt ：使用说明。

冰河的大致工作原理是这样的：由控制端向服务端发送命令，服务端在接到命令后在远程主机上执行命令，执行完后向控制端反馈命令执行的情况。

如果在局域网中使用冰河，那么可以视情况而定是否对服务端进行配置，如果在 Internet 上使用的话，那么一定要先对服务端程序（G_Server.exe）进行配置后才可投入使用，否则出现安全问题的概率很大。

1．配置服务端程序

先打开控制端程序 G_Client.exe，然后选择文件→配置服务器程序（图 2-1），之后出现配置窗口（图 2-2）。

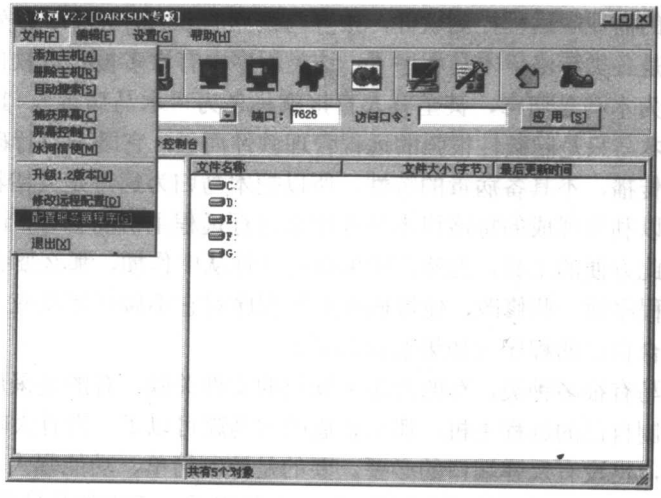

图 2-1　服务端配置选项

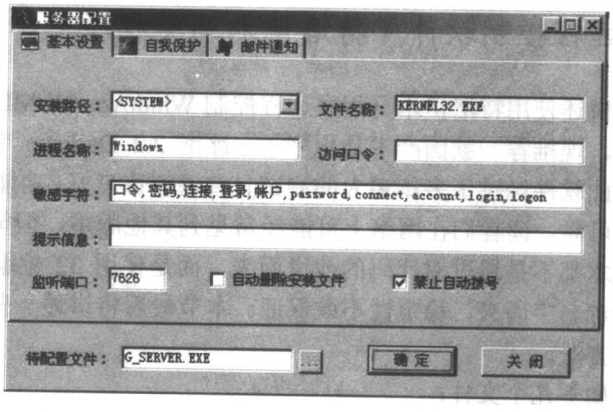

图 2-2　服务端配置窗体

在图 2-2 中的基本设置页中可以设置：

（1）安装路径

选择一个服务端安装到的路径，因为毕竟是特洛伊木马程序，所以也就自然不会安装到 Program Files 里面。

（2）进程名称

服务端运行时的进程名称，因为此处是要用作自己机器远程控制上的，所以可以起一个自己认识的进程名，以便于辨认。

（3）文件名称

即安装到指定目录下的文件的名称，同样为了便于自己辨认，可以像定义进程名称一样定义这个文件的名称。

（4）访问口令

即使用控制端对服务端进行连接时用来验证身份的口令，如果用在 Internet 上就应该

在此设置一个强壮的口令。

（5）敏感字符

服务端会监视所有远程主机上的敏感字符并对其进行记录，此处可以将其清空。因为一般来讲，没有人愿意浪费系统资源来监视自己远程主机的敏感字符。即使程序记录了这些字符，用户也不会去查看的。

（6）提示信息

打开服务端程序的时候出现的提示信息，比如可以为了确定安装成功而设置提示信息为“安装成功”，或者“成功打开”等等。当然，也可以不设置。

（7）监听端口

远程主机等待控制端连接时监听的端口。为安全性考虑，可以对其任意设置在 0～65535 之间即可，连接时只要控制端连接的端口设置与服务端监听端口保持一致即可成功连接。

（8）自动删除安装文件

控制端程序成功打开后便自行删除。

（9）禁止自动拨号

当网络没有连通时不进行自动拨号。

（10）待配置文件

即控制端程序的所在路径。

接下来请看第二个配置页（图 2-3）：

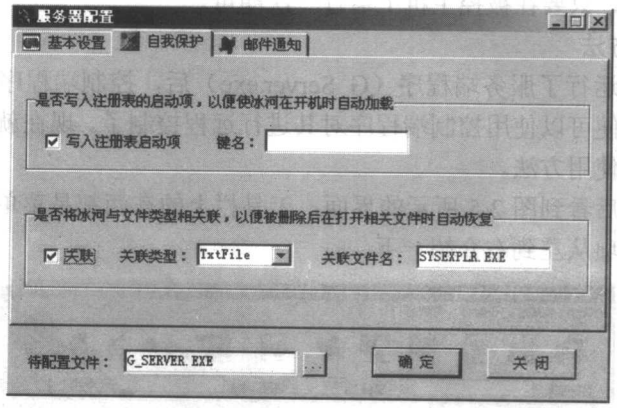

图 2-3　服务端配置窗体

这个自我保护页中的选项如下：

（1）写入注册表启动项

也就是每次开机自动加载服务端程序，如果不选的话，下次开机就需要手动再打开服务端程序一次来等待控制端的连接了。

（2）键名

写入注册表启动项的键名，可以自己起一个容易分辨的名字。

（3）关联

与文件关联，可以在后面选择关联的文件类型和文件名，用以在服务端程序工作不正