学电脑以用为本

网络管理员实战手册

活学活用

电脑安全攻防秘笈

扬乔工作室 编

- 网银、网游、邮件远离威胁
- 让下载、炒股、冲浪、聊天、
- 20余种病毒、木马攻防战术
- 巧妙设置办公数据多重安全
- 30套安全方案打造稳定系统

◎全面总结防毒、防盗、防骗、防黑经验与技巧

人民交通出版社
China Communications Press

电脑
安全攻防秘笈

扬乔工作室　编著

人民交通出版社

内 容 提 要

本书全面总结和讲解在网络中防毒、防盗、防骗、防黑等应用，用丰富的实例深入解密网络安全的防护方法和技巧。为了让读者尽可能杜绝网络安全威胁，对病毒制作、网络诈骗、密码盗取、黑客攻击等的常用方法进行了深入分析，以帮助读者从根本上快速解决电脑安全问题。本书以用为主，避免冗长理论，在书中配置大量图片，图文配合讲解。用通俗的语言组织文章，并穿插小技巧、小提示进行经验总结和点拨。本书适合电脑个人用户、网络管理员、维护工程师及培训班使用。

图书在版编目（CIP）数据

电脑安全攻防秘笈 / 扬乔工作室编著. —北京：人民交通出版社，2008.11

ISBN 978-7-114-07462-2

Ⅰ.电… Ⅱ.扬… Ⅲ.电子计算机－安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2008）第 166710 号

书　　名：电脑安全攻防秘笈
著 作 者：张世勇　扬乔工作室
责任编辑：李露春　白　倩
出版发行：人民交通出版社
地　　址：（100011）北京市朝阳区安定门外外馆斜街 3 号
网　　址：http://www.ccpress.com.cn
销售电话：（010）59757969，59757973
总 经 销：北京中交盛世书刊有限公司
经　　销：各地新华书店
印　　刷：北京市密东印刷有限公司
开　　本：787×1092　1/16
印　　张：18
字　　数：460 千
版　　次：2008 年 11 月第 1 版
印　　次：2008 年 11 月第 1 次印刷
书　　号：ISBN 978-7-114-07462-2
定　　价：28.00 元

前言

中国互联网业务急剧增加，同时也给用户带来了更加值得注意的安全问题，现在很多办公管理、商务交流、网络通信、理财等都通过互联网进行，但随时面对木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、蠕虫、病毒等威胁，同时还面临黑客攻击等危险。稍不留神，上网电脑就会受到安全问题的侵扰，轻则电脑变得缓慢、死机、系统崩溃，重则重要数据丢失、网络账号被盗、网游或QQ等虚拟财产被盗、银行账号被盗导致“真金白银”不翼而飞。目前专门对网络电脑进行攻击的人也很多，它们专门传播病毒、木马和流氓程序，或者专职黑客干扰互联网的正常运行。

网络安全已成为所有上网族不可忽视的课题，然而使用Windows防火墙或安装防毒软件就能高枕无忧了吗？当然不是的。要能彻底保证电脑的安全，需要花费大量的工夫才行，需要同时采用多套安全方案才能有效防御。

由于网络安全涉及面广，存在大量的安全技术、设备、软件和应用配置方法。因此目前市面上讲解安全的图书非常活跃。但是大部分图书都是围绕黑客的理论和应用在讲解，好像叫人去做黑客才行一样。其实大部分电脑用户不希望自己去做黑客，而目的是要充分杜绝网络木马、恶意和间谍软件的侵害，能彻底抵御黑客的攻击。

本书就是针对电脑用户的实际所需，专门讲解如何打造安全的电脑系统，让电脑不受安全侵扰，保证安全上网、重要数据和财产不受损失。同时对木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、蠕虫、病毒等的行为进行解密，然后从寻找、判断、歼灭角度讲解攻防技巧。

本书是《活学活用》系列图书之一，用有限的篇幅，讲解电脑面临的主要安全问题。包括系统密码攻防，文件系统共享安全防护，漏洞攻防，抛开聊胜于无的Windows防火墙建立更安全稳固的专属防火墙，设置IE打造安全上网，巧识下载陷阱、巧妙反网页钓鱼，打造炒股防盗方案，保护网银交易安全，安全接收邮件，QQ、网游账户及虚拟财产防盗，无线网络安全，IP安全策略与隐藏策略，巧补系统克隆漏洞，系统密码急救以及抵御黑客攻击的常用方法与技巧。涉及的经验技巧适用Windows Vista及Windows XP/2000/Server 2003系统。若没有特别说明，本书的演示例子都在Windows XP中完成。

本书内容是网络管理员经常遇见的，并提供大量操作方案和案例，也是一本不可多得的案头工具书。

CONTENTS 目录

第一章 设置系统提高安全——建立防御基地

第二章 用软件搭建防御系统——构筑安全工事

第三章 宽带应用安全技巧——网络威胁逐一破解

目录 CONTENTS

CONTENTS 目录

第五章 设置安全多重线——办公文档防盗保护

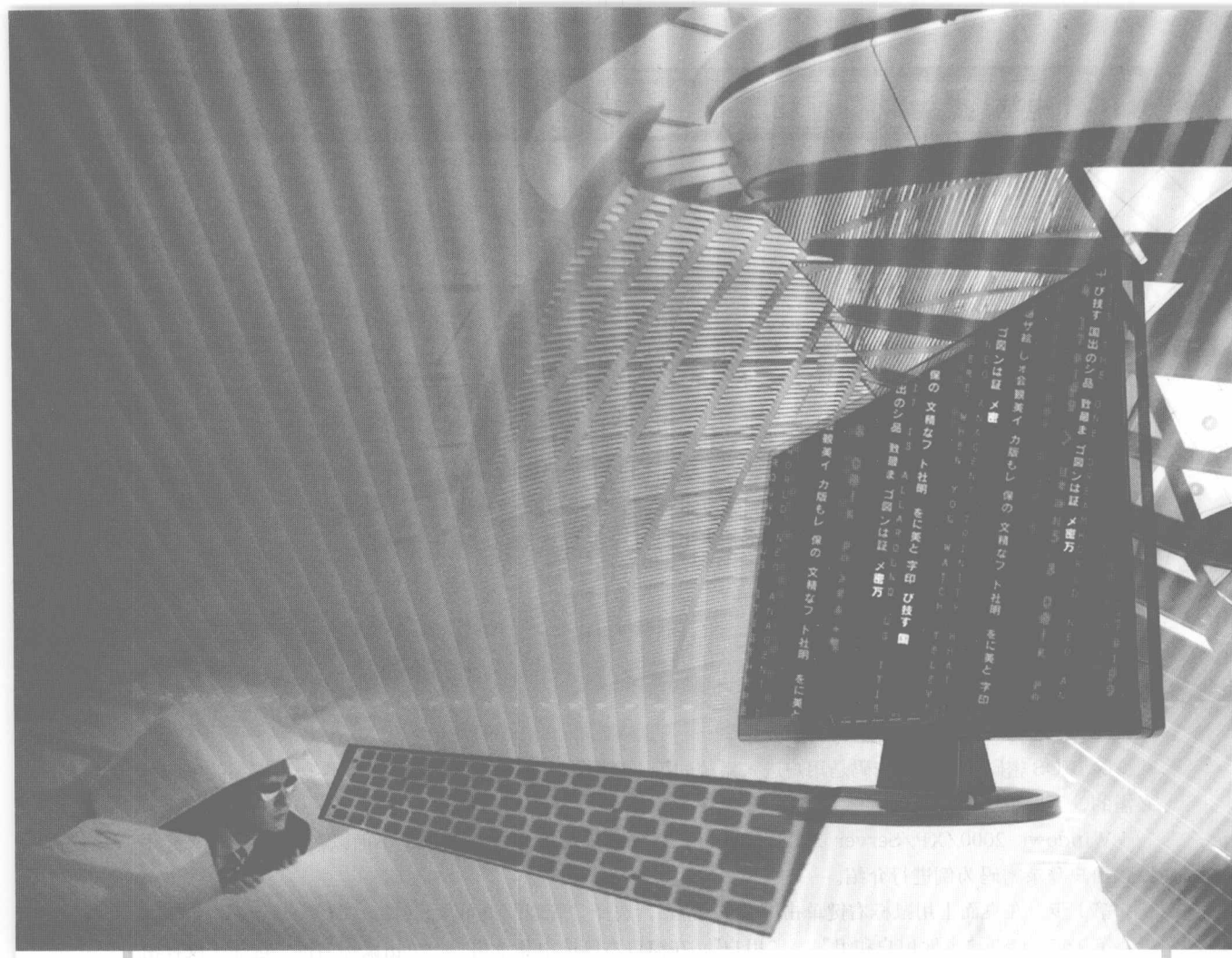
第六章 打造网络数据安全无忧——局域网数据安全

目录 CONTENTS

CONTENTS 目录

第九章 彻底清除流氓软件

第十章 系统安全故障攻防与急救



第一章

设置系统提高安全

——建立防御基地

操作系统是用户与电脑交流的接口，是各应用软件在电脑中赖以生存、协调工作的基地。操作系统的安全关系到用户重要资料的安全性以及整机系统的稳定性。下面就来看看如何提高操作系统的安全防御能力。

第一节 系统密码登录安全

系统密码主要包括系统登录密码、屏保密码、电源管理密码等，它们就像用户家里的钥匙，只有拥有正确的密码，才能进入系统中进行相应的操作。所以登录密码是保护系统安全的第一道屏障。

一、使用 Windows 登录账户

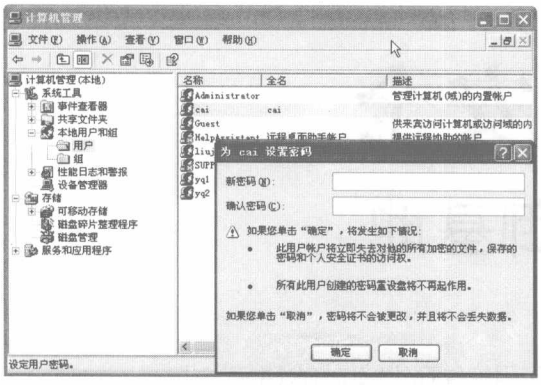
除 BIOS 密码外，登录密码是用户进入系统的第一道防线。加强操作系统的安全性，设置系统密码是必需的，否则就等于为入侵者敞开了方便之门。

Windows 2000/XP/Server 2003/Vista 用户登录密码的设置方法类似，下面以在 Windows XP 中设置用户登录密码为例进行介绍。

第 1 步，在桌面上用鼠标右键单击“我的电脑”，选择“管理”菜单项，打开“计算机管理”窗口。

第 2 步，展开“本地用户和组”→“用户”，在窗口右侧选中登录用户，单击鼠标右键，选择“设置密码”菜单项，弹出密码设置窗口，两次输入将要设置的密码，单击“确定”按钮退出即可，如图 1-1 所示。

第 3 步，重新启动电脑让设置的密码生效。



◆图 1-1　设置 Windows XP 用户登录密码

小提示

设置系统登录密码后，在登录 Windows 98/2000/XP/2003/Vista 操作系统时，会弹出一个登录界面让用户输入密码。如果没有设置密码，该界面可能不会显示。

二、屏幕保护程序密码

在网吧、学校机房等公共场所使用电脑，暂时离开电脑时，启用屏保程序可以防止他人使用电脑。Windows 98/2000/XP/Server 2003/Vista 都提供了屏保功能，下面以在 Windows XP 中设置屏保及屏保密码为例进行介绍。

在桌面上任意地方单击鼠标右键，选择“属性”菜单项，打开“显示属性”窗口。切换到“屏幕保护程序”选项卡，选择一个喜欢的屏保程序，并设置用户在操作后等待多长时间启用屏保程序，建议等待时间设置短暂一些。勾选“在恢复时使用密码保护”复选框，即用户在恢复使用电脑时，需要输入登录密码才能进入系统，如图 1-2 所示。

◆图 1-2　设置屏保及屏保密码

小提示

对使用Windows 2000/XP/Server 2003/Vista的用户来说，当需要暂时离开电脑时，可按下“Ctrl+Alt+Del”组合键锁定电脑，对使用Windows 98的用户来说，则只能借助屏幕保护的方法，保证自己在离开座位的时候电脑不被别人使用。

三、电源管理密码

对 Windows 系统的电源管理设置密码后，当系统从节能状态返回时，只有输入正确的密码后，才能令电脑从“挂起”状态返回正常状态，这样才能进一步地保证电脑的安全。下面以在 Windows XP 中设置电源管理密码为例进行介绍。

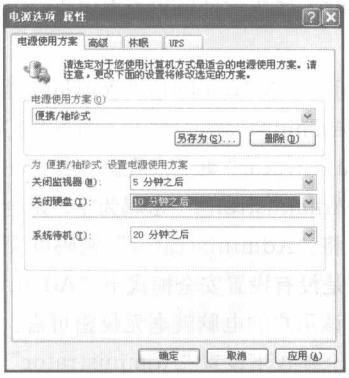
第 1 步，单击菜单“开始”→“控制面板”，打开“控制面板”窗口。

第 2 步，双击“电源选项”图标，打开“电源选项 属性”窗口，切换到“电源使用方案”选项卡，在“系统待机”下拉列表中选择系统待机的时间，如图 1-3 所示。

第 3 步，切换到“高级”选项卡，在“选项”组合框中勾选“在计算机从待机状态恢复时，提示输入密码”复选框，如图 1-4 所示。设置好后单击“确定”按钮返回即可。这样当电脑从节能状态返回时就会要求用户输入密码。

四、密码设置原则与技巧

Windows 操作系统的密码（口令）十分重要，它是抵抗攻击的第一道防线，用户必须把密码安全作



◆图 1-3　“电源选项 属性”窗口

◆图 1-4　设置屏保及屏保密码

为安全策略的第一步。如果攻击者未能窃取到系统密码，那么采取的入侵方法也就不多了，因此，必须设置安全的系统密码。通常，用户在设置系统密码时应遵循以下原则：

①密码字符数足够多，最好不少于8个字符。

②不适应常用的单词、中英文昵称、生日、电话号码等作为系统密码。

③密码中同时包含多种类型的字符，比如大写字母（A，B，C，…，Z）、小写字母（a，b，c，…，z）、数字（0，1，2，…，9）、标点符号（@，#，!，$，%，&，…）。

④密码中不含有重复的字母或数字。

⑤定期修改密码。

第二节 安全设置

在病毒、木马、恶意软件盛行的互联网上，保证电脑绝对安全虽然难以做到，但配置相对安全的系统可以最大程度降低系统被攻击的几率。本节就来介绍操作系统的常用安全设置方法与技巧。

一、隐私保护

为系统设置密码固然重要，但也不是万事大吉。总有不法分子在千方百计地想攻克用户密码。因此加固系统密码，对保护自己的隐私非常重要。

小提示

为了系统更加安全，建议对系统默认的超级用户名“Administrator”进行改名，然后再设置一个足够复杂的密码。停用或删除一切不必要的系统用户。

Windows XP真正的超级管理员账号是安全模式下的“Administrator”账户，而不是正常模式下的“Administrator”账户。在默认情况下，安全模式下的“Administrator”密码为空。无论用户在正常模式下将“Administrator”密码设置得多么复杂，只要是没有设置安全模式下“Administrator”的密码，该用户的电脑就毫无秘密可言。

在安全模式下设置“Administrator”用户密码的方法与正常模式下普通用户密码的设置方法一

样，可参照本章第一节的有关内容。

二、安全共享

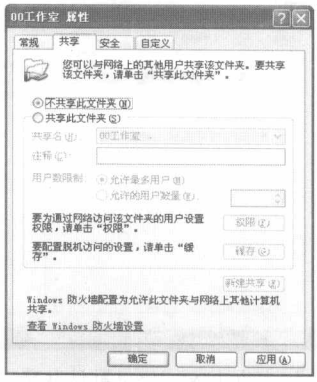
共享文件／文件夹，为用户电脑互访提供了方便，同时也带来了一定的安全隐患。下面就来看看如何对系统中的共享资源进行安全设置。

1．及时取消共享资源

由于一旦建立了资源共享，用户的电脑和其他主机之间，就会存在一条共享通道，利用这条通道，黑客就可能对用户的电脑发起攻击。要想有效切断共享通道，最好能将资源共享状态取消掉。

（1）关闭单个共享

打开“我的电脑”窗口。找到并选择已经设为共享的文件夹，然后单击鼠标右键，选择“共享(H)”菜单项，弹出“属性”窗口。选择“共享”选项卡，选中“不共享该文件夹(N)”单选框，如图1-5所示，然后单击“确定”按钮即可。

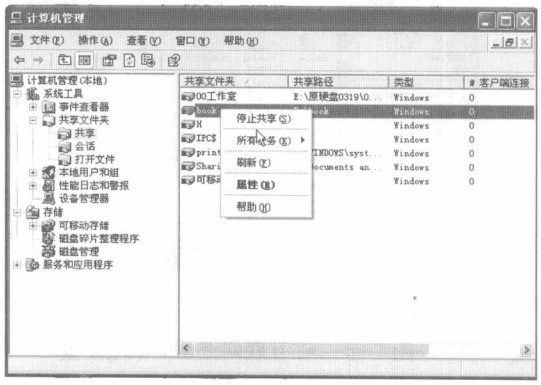


◆图1-5　关闭共享

这种方法的缺点是用户需要先找到共享的源文件夹，然后才能关闭，而且一次只能关闭一个共享资源。

（2）一次性关闭多个共享目录

如果需要关闭的共享目录比较多，且位于不同的磁盘分区、不同的文件夹中，这时，逐个进行关闭就非常麻烦，就可以快速关闭多个共享目录，方法如下。



◆图1-6　关闭多个共享目录

第1步，单击菜单“开始”→“程序”→“管理工具”→“计算机管理”，打开“计算机管理”窗口。

第2步，展开“计算机管理（本地）”→“系统工具”→“共享文件夹”→“共享”项目，在窗口的右侧显示出硬盘中所有共享的目录，用户鼠标右键单击需要关闭的共享目录，选择 “停止共享(S)”菜单项，如图1-6所示。

第3步，在弹出的对话框中单击“确定”按钮，即可将该共享停止。采用这种方法能一次性关闭多个共享资源。

小提示

在“计算机管理”的共享窗口中，不但可以看到用户设置的共享目录，还可以看到系统默认的隐藏共享目录。

2．删除系统默认共享

Windows 2000/XP/2003/Vista版本的操作系统提供了默认共享功能，这些默认的共享都有“$”标志，意为隐含的意思，包括所有的逻辑盘（C$，D$，E$…）和系统目录Winnt或Windows（admin$），如图1-7所示。微软公司的初衷是便于网管进行远程管理，这虽然方便了局域网用户，但对个人用户来说这样的设置是非常不安全的，因为在互联网上，任何人都可以通过共享硬盘进入用户的电脑。所以关闭这些共享非常必要，下面就来看看关闭的常见方法。

◆图1-7　Windows Vista默认共享

小知识

访问Windows XP默认共享非常简单：单击菜单“开始”→“运行”，输入“\\计算机名或IP地址\D$或admin$”即可。也可在IE等浏览器的地址栏中输入上述的命令或“file://10.80.34.33/d$”来进行访问，如图1-8所示。

◆图1-8　在互联网上访问本地硬盘

◆图1-9　停用共享服务

（1）批处理自启动法

打开记事本并输入以下内容：

```
net share C$ /delete
net share D$ /delete
……(根据实际盘符数进行输入)
net share ipc$ /delete
net share admin$ /delete
```

保存该文件为“*.bat”文件，然后把该文件添加到启动选项即可。

（2）停止共享服务

第1步，在桌面上用鼠标右键单击“我的电脑”，选择“管理”菜单项，打开“计算机管理”窗口。

第2步，展开左侧的“服务和应用程序”，→“服务”，在窗口的右侧找到共享服务对应的名称是“Server”（在进程中的名称为“services”）。

第3步，双击“Server”服务项，在弹出的窗口中选择“常规”选项卡，把“启动类型”更改为“已禁用”。在“服务状态”区域单击“停止”按钮，如图1-9所示。设置好后单击“确定”按钮即可。

3．拒绝访问账号列表

由于Windows 2000/XP/Server 2003/Vista在系统在缺省状态下，会允许每一位未授权用户以连接空用户方式，访问系统中的账号列表信息和资源共享列表信息，为了防止黑客通过共享资源列表和账号列表对系统发起攻击，应该禁止任何未授权用户直接连接空用户。

打开注册表编辑器，展开注册表的“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA”分支，在窗口右侧修改“RestrictAnonymous”的值为“1”。重新启动电脑就能拒绝未授权用户去访问账号列表了。

4．关闭不用的共享端口

139端口、445端口是常用的共享打印机、共享文件夹端口，如果用户不需要访问共享资源，可将这些端口关闭，防止黑客通过这些端口扫描到系统中的共享资源。其关闭方法在本章第三节中详述。

三、注册表安全设置

注册表（Registry）整合、集成了全部系统和应用程序的初始化信息。其中包含硬件设备的说明、相互关联的应用程序与文档文件、窗口显示方式、网络连接参数、甚至关系到电脑安全的网络设置。病毒、木马、黑客程序等攻击用户电脑时，都会对注册表进行一定的修改，因此注册表的安全设置非常重要。

1.让用户名不出现在登录框中

Windows 9x以上的操作系统可以对以前用户登录的信息具有记忆功能，下次重新启动电脑时，会在用户名栏中出现上次用户的登录名，这个信息可能会被一些非法分子利用，而给用户造成威胁，为此有必要隐藏用户登录的名字 。

单击菜单“开始”→“运行”，输入“regedit”命令，打开注册表编辑器。展开注册表分支到“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon”，在窗口右边新建字符串“DontDisplayLastUserName”，并把该值设置为“1”。设置完后，重新启动电脑就可以在系统登录框中隐藏用户登录的名字。

2.抵御BackDoor（后门程序）破坏

BackDoor是黑客程序中的一种后门程序，专门针对系统的漏洞进行攻击。为防止这种程序对系统造成破坏，用户有必要通过相应的设置来进行预防。

打开注册表编辑器。展开分支到“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”，如果在窗口右边发现有“Notepad”键值，将它删除即可达到预防的目的。

3.禁用控制面板

控制面板是Windows系统的控制中心，可以对设备属性，文件系统，安全口令等系统关键属性进行修改。用户可以根据需要隐藏和禁止使用控制面板。

打开注册表编辑器，展开“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System”，在窗口右侧新建一个“DWORD”类型的子健“NoDispCPL”，修改其值为“1”即可。

4.隐藏“文件系统”菜单

为防止非法用户随意篡改系统中的文件，用户有必要把“系统属性”中“文件系统”的菜单隐藏起来。

打开注册表编辑器，展开“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System”，在窗口右边新建一个“DWORD”类型的子健“NoFileSysPage”，然后把其值改为“1”即可。

5.锁定桌面

桌面设置包括壁纸、图标以及快捷方式，它们的设置一般都是用户经过精心选择才设定好的。大多数情况下，用户都不希望他人随意修改桌面设置或随意删除快捷方式。那怎么办呢？其实，修改注册表就可以帮用户锁定桌面，这里“锁定”的含义是对他人的修改不做储存，无论别人怎么改，重新启动电脑后，用户原来的设置就会原封不动地出现。

打开注册表编辑器，展开“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurentVersion\Polioies\Explores”，双击子健“No Save Setting”，将其键值从“0”改为“1”即可。

6. 预防 WinNuke

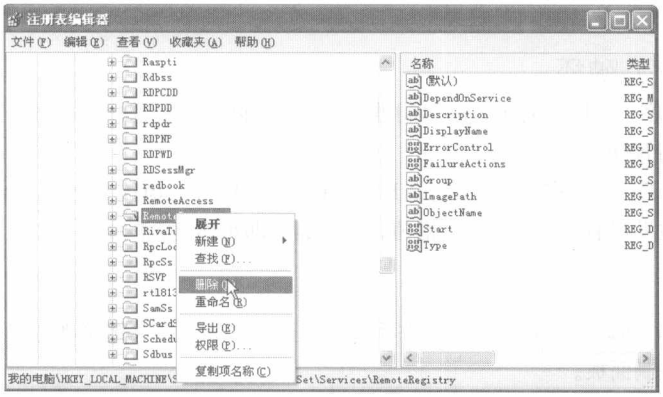
WinNuke 对 Windows 系统具有极强的破坏作用，预防 WinNuke 的破坏性可以通过修改注册表来实现。

打开注册表编辑器，展开“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP”，在窗口右侧新建或修改字符串“BSDUrgent”，并把其值设置为“0”即可。

7. 禁止远程修改注册表

如果黑客能连接到用户的电脑，而且电脑启用了远程注册表服务(Remote Registry)，那么黑客就可远程设置注册表中的服务，因此远程注册表服务需要特别保护。如果用户仅仅将远程注册表服务(Remote Registry)的启动方式设置为“禁用”，黑客在入侵电脑后，仍然可以通过简单的操作将该服务从“禁用”改为“自动启动”。因此有必要将该服务删除。

打开注册表编辑器，展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”找到“RemoteRegistry”项，右键单击该项，选择“删除”菜单项，将该键删除（如图1-10所示），这样，以后就无法启动该服务了。



◆图1-10　删除远程启动服务

小提示

在删除该服务前，应将该项信息导出进行备份。当需要使用该服务时，只需要将已保存的注册表文件导入即可。

8. 禁止使用“密码”下的“更改密码”选项卡

打开注册表编辑器，展开“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer”，在窗口右侧新建一个类型为“Dword”的子健“NoPwdPage”，然后将其的值设置为“1”即可。

9. 拒绝“信”骚扰

在Windows 2000/XP系统中，默认“Messenger”服务处于启动状态，不怀好意者可通过“net send”指令向目标电脑发送信息。目标电脑会不时地收到他人发来的骚扰信息，严重影响正常使用。

打开注册表编辑器，展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Messenger”，修改“START”子健的值为“4”即可。这样“Messenger”服务就会被禁用，用户就再也不会受到“信”骚扰了。

10. 严禁系统隐私泄露

在Windows系统运行出错时，系统内部有一个“dr.watson”程序会自动将系统调用的隐私信息保存下来。隐私信息将保存在“user.dmp”和“drwtsn32.log”文件中。攻击者可以通过破解这个程序而