网络安全原理与案例分析

齐爱琴 主编

科学出版社

基金项目：甘肃省重点学科计算机科学与技术

网络安全原理与案例分析

齐爱琴　主编

科学出版社

北京

内 容 简 介

本书内容涵盖操作系统技术、数据库安全技术、漏洞扫描技术、防火墙技术、病毒技术等方面，案例分析既包含对网络安全原理的理解和运用，又融合了当今网络安全的主流技术，以适应基础与验证性、综合和设计性两种不同层次的要求。

全书共 8 章，第 1 章介绍操作系统安全技术，第 2 章介绍数据库安全技术，第 3 章介绍各种漏洞的扫描方法，第 4 章介绍 Web 安全，第 5～7 章介绍具体网络信息安全技术及应用方法，第 8 章介绍安全审计技术。

本书可作为计算机类、网络技术类和信息安全类相关专业本科生的辅导教材，也可作为网络安全工程师、网络管理员的参考书以及网络安全专业培训教材。

图书在版编目(CIP)数据

网络安全原理与案例分析 / 齐爱琴主编. —北京：科学出版社，2017.11
ISBN 978-7-03-053270-1

Ⅰ. ①网… Ⅱ. ①齐… Ⅲ. ①计算机网络－安全技术－研究
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 128531 号

责任编辑：邹 杰 / 责任校对：郭瑞芝
责任印制：吴兆东 / 封面设计：迷底书装

科 学 出 版 社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京京华虎彩印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2017 年 11 月第 一 版 开本：787×1092 1/16
2018 年 1 月第二次印刷 印张：16
字数：370 000

定价：56.00 元

(如有印装质量问题，我社负责调换)

前　言

随着计算机技术的飞速发展，计算机网络涉及国家的政府、军事、文教等诸多领域，存储、传输和处理的许多信息是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、科研数据等重要信息。计算机网络安全已经成为社会发展的重要保证。计算机网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。特点是理论性与实践性都很强，涉及的知识面较广，概念繁多，并且比较抽象，仅靠课堂教学，学生难以理解和掌握。在学习一般性原理和技术的基础上，必须通过一定的案例分析训练，才能真正掌握其内在机理。然而，在课时有限的情况下，如何组织计算机网络安全案例分析教学的内容和案例分析实施手段，使之既能配合课堂教学，加深对所学内容的理解，又能紧跟计算机网络安全技术的发展，培养和提高学生的实际操作技能，不是一件容易的事。为了进一步提高学生计算机网络安全技术的综合应用和设计创新能力，西北民族大学数学与计算机科学学院联合西普阳光科技于2011年共同建立了计算机网络与信息安全实验室。实验室不仅满足了学生对各种网络及网络安全设备的操作培训，还能从计算机网络安全知识及技能出发，培养学生的理论认知及实践能力，能够从原理验证、实训应用、综合分析、自主设计及研究创新等多层次培养学生的综合素质。

本书结构合理、可读性强、注重应用。力求使学生能够较快掌握网络安全的基础核心内容。在内容选取、结构编排上尽量体现广泛的代表性和典型性，使读者能够在掌握基础知识的同时，也能运用到实际工作和生活中，是一本较为系统全面介绍网络安全的书籍。

本书由西北民族大学数学与计算机科学学院齐爱琴编写，负责全书统筹及策划、提纲撰写并且修改第1～8章，马君负责全书校对。作者均为从事计算机网络安全教学、科研的一线教师，有丰富的教学实践经验，本书力求做到结构严谨、概念准确，内容组织合理、语言使用规范。

在本书写作过程中，得到诸多专家和领导的热情支持与指导，在此一并表示衷心感谢。由于作者水平有限，书中难免存在不足之处，恳请广大读者批评指正。

作　者

2017年6月

目　录

第 1 章　操作系统安全

操作系统(Operating System，OS)的出现、使用和发展是最近四十余年来计算机软件的一个重大进展。尽管操作系统尚未有一个严格的定义，但一致认为：操作系统是管理系统资源、控制程序执行、改善人机界面、提供各种服务、合理组织计算机工作流程和为用户使用计算机提供良好运行环境的一种系统软件[1-3]。计算机发展到今天，从巨型机到个人机，无一例外都配置了一种或多种操作系统，操作系统已经成为现代计算机系统不可分割的重要组成部分，它为人们建立各种各样的应用环境奠定了重要基础。

配置操作系统的主要目标归纳如下。

(1)方便用户使用：操作系统通过提供用户与计算机之间的友好接口来方便用户使用。

(2)扩大机器功能：操作系统通过扩充改造硬件设施和提供新的服务来扩大机器功能。

(3)管理系统资源：操作系统有效管理好系统中所有软硬件资源，使之得到充分利用。

(4)提高系统效率：操作系统合理组织好计算机工作流程，以改进系统性能和提高系统效率。

(5)构筑开放环境：操作系统遵循有关国际标准来设计和构造，以构筑一个开放环境。

其含义主要是指遵循有关国际标准(如开放的通信标准、开放的用户接口标准、开放的线程库标准等)；支持体系结构的可伸缩性和可扩展性；支持应用程序在不同平台上的可移植性和互操作性。

操作系统是计算机资源的直接管理者，它可以直接与硬件交互，并为用户提供接口，是计算机软件的基础和核心。因此，操作系统的安全是整个计算机系统安全的基础。操作系统主要的安全功能包括：存储器保护(限定存储区和地址重定位，保护存储信息)、文件保护(保护用户和系统文件，防止非授权用户访问)、访问控制、身份鉴别(识别请求访问的用户权限和身份)等。

目前，操作系统主要有以下两大类安全漏洞[4]。

(1)输入/输出(I/O)非法访问：在一些操作系统中，一旦 I/O 操作被检查通过后，该操作系统就继续执行操作而不再进行检查，这样就可能造成后续操作的非法访问。

(2)操作系统陷门：某些操作系统为了维护方便，使系统兼容性和开放性更好，在设计时预留了一些端口或保留了某些特殊的管理程序功能。

针对操作系统的安全功能和存在的安全漏洞，操作系统安全的主要目标如下。

(1)按系统安全策略对用户的操作进行访问控制，防止用户对计算机资源的非法使用(窃取、篡改和破坏)。

(2)标识系统中的用户，并对其身份进行鉴别。

(3)监督系统运行的安全性。

(4)保证系统自身的安全性和完整性。

实现这些目标，需要建立相应的安全机制，根据国际标准化组织(ISO)的定义，安全机制是一种技术、一些软件或实施一个或更多安全服务的过程。安全机制可以分为特殊安全机

制和普通安全机制。一个特殊安全机制是在同一时间只对一种安全服务上实施一种技术或软件。加密就是特殊安全机制的一个例子。尽管可以通过加密来保护数据的保密性、数据的完整性和不可否定性，但实施每种服务时需要使用不同的加密技术。普遍的安全机制都列出了在同时实施一个或多个安全服务时的执行过程。特殊安全机制和普遍安全机制不同的另一个方面是普通安全机制不能应用到 OSI(开放系统互连)参考模型的任一层上。

普遍安全机制包括以下内容。

(1) 信任的功能性：指任何加强现有机制的执行过程。

(2) 事件监测：检查和报告本地或远程发生的事件。

(3) 审计跟踪：任何机制都允许监视和记录与安全有关的活动。

(4) 安全恢复：对一些事件做出反应，包括针对已知漏洞创建短期和长期的解决方案和对受害系统的修复。

本章主要介绍两大主流操作系统——Windows 操作系统和 Linux 操作系统的安全机制及安全技术。

1.1　Windows 操作系统安全

Windows 操作系统是一款由美国微软公司开发的窗口化操作系统。采用图形用户界面操作模式，比起从前的指令操作系统更为人性化。Windows 操作系统是目前世界上使用最广泛的操作系统。

本节从 Windows 文件系统、Windows 用户管理、Windows 安全策略、Windows 网络与服务管理、Web 服务安全配置、FTP 服务安全配置、远程桌面服务安全配置和垃圾邮件分析与过滤等方面进行操作和配置，从而使操作系统变得更加安全可靠[5,6]。

目前，常用的 Windows 操作系统有 Windows NT、Windows 2000、Windows 2003、Windows XP、Windows 7、Windows Vista 等，本节案例分析以 Windows 2003 为依据，其他系统操作类似。

1.1.1　Windows 文件系统与备份恢复案例分析

Windows 2003 系统默认安装的磁盘分区为 NTFS 分区。Windows 2003 文件系统在 NTFS 分区上可以利用 NTFS 权限和文件加密提高数据安全性和数据存储有效性，利用数据压缩和磁盘配额提高磁盘空间的利用率。

Windows 操作系统有可能因操作失误或者其他我们无法预料的因素导致无法正常工作，因此很有必要在系统出现故障之前，先采取一些安全和备份措施，做到防患于未然。

打开 Windows 案例分析台，进入 Windows 2003 操作系统，Windows 文件系统与备份恢复步骤如下。

1. 将磁盘的格式转换为 NTFS

单击“开始”菜单下的“运行”命令，输入“cmd”，单击“确定”按钮；在 cmd 窗口输入“convert D：/FS：NTFS”并按回车键，对 D 盘进行格式转换，如图 1.1 所示。

2. 设置 D 盘权限

把 D 盘的权限设置为 Administrators 可完全控制，User 可以读。

(1)右击 D 盘图标，选择“属性”命令。在 D 盘的属性窗口中选择“安全”选项，单击“添加”按钮，找到“Administrators”并双击，单击“确定”按钮；在权限框里的“完全控制”选择“允许”。

(2)用同样的方法设置“Users”组，只是“权限”设置为“读取和运行”、“列出文件夹目录”和“读取”，如图 1.2 和图 1.3 所示。

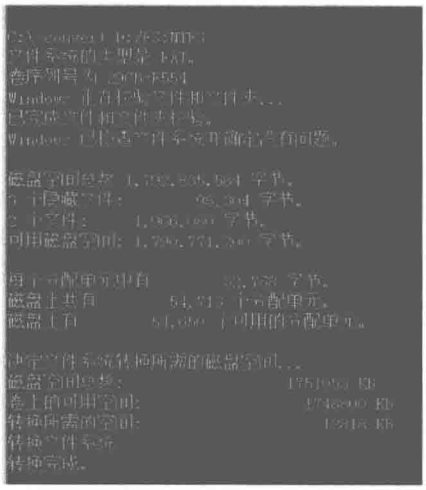

图 1.1　命令截图

3. 设定 Student 用户在 D 盘使用的磁盘配额

(1)右击 D 盘图标，选择“属性”命令。在 D 盘属性窗口切换到“配额”选项卡，把“启用配额管理”和“拒绝将磁盘空间给超过配额限制的用户”复选框选中，如图 1.4 所示。

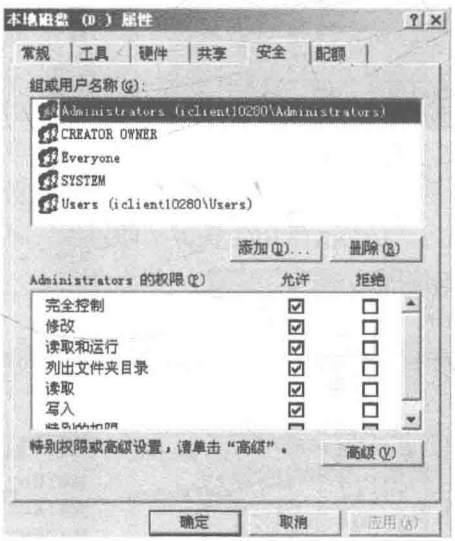

图 1.2　属性窗口

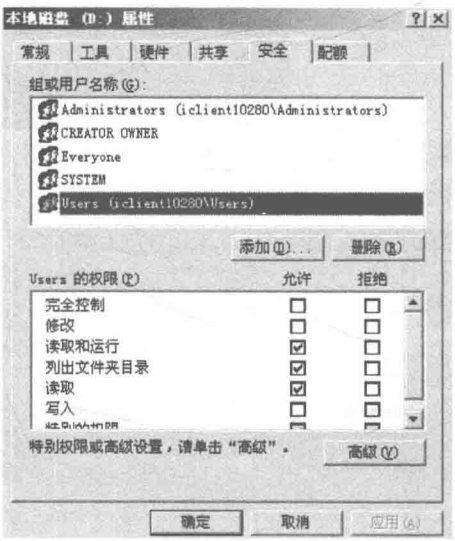

图 1.3　设置用户的访问权限

(2)单击图 1.4 中的“配额项”按钮，打开配额设置窗口，如图 1.5 所示。

(3)双击“使用数量”字段，出现如图 1.6 所示对话框，根据需要选择填写即可。

4. 用磁盘扫描工具检查磁盘，并修复磁盘上的错误

执行“开始”→“运行”命令，输入“cmd”，单击“确定”按钮；在 cmd 命令窗口中输入“chkdsk D:/F>C:\disk.txt”并按回车键；扫描报告保存到 C:\disk.txt。DISK.TXT 文件的内容如图 1.7 所示。

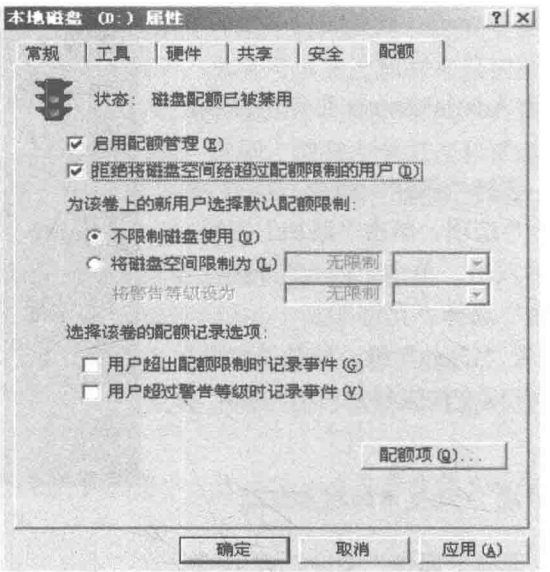

图 1.4　“配额”选项卡

图 1.5　新建盘配额

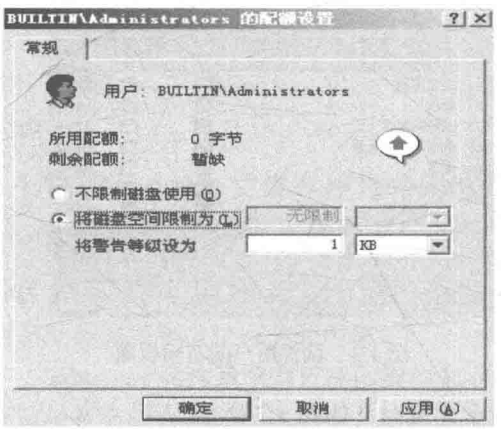

图 1.6　设置磁盘配额

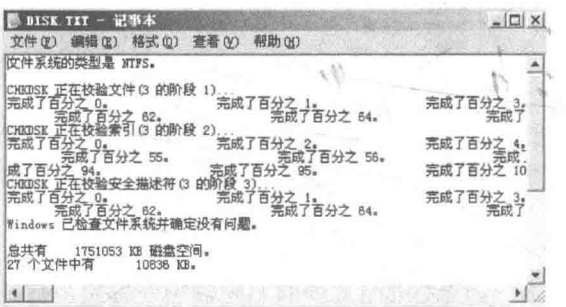

图 1.7　文件的内容

5. 文件加密和压缩

在需要加密的文件上右击，选择“属性”命令，单击“高级”按钮。在“高级属性”对话框中把“加密内容以便保护数据”复选框选中，单击“确定”按钮。同理，在此对话框中选中“压缩内容以便节省磁盘空间”复选框即可压缩文件，如图 1.8 所示。

6. 共享文件夹安全设置

在共享的文件夹的属性界面中，选择“共享”选项卡，单击权限按钮。

选择用户名称或组，分别设置其对该共享文件夹的访问权限。例如，为了防止病毒传播及共享文件被非法更改，可以将所有用户都设置为对该共享文件夹具有只读权限，如图 1.9 所示。

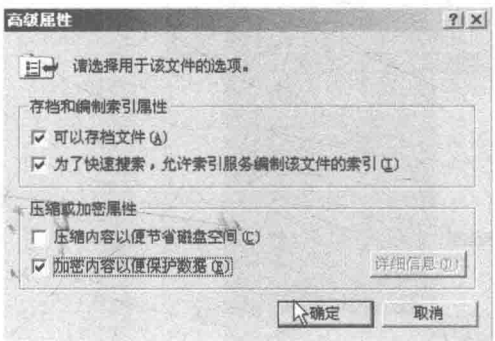

图 1.8　文件的加密和压缩

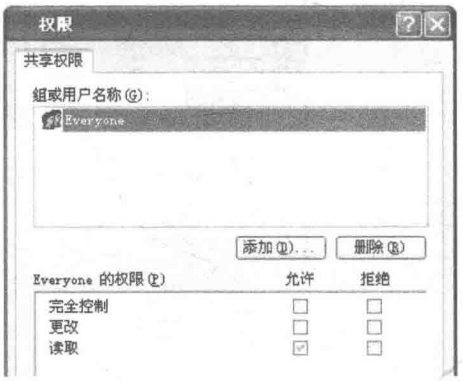

图 1.9　权限设置

7. 备份硬件配置文件

(1)右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，打开“系统属性”对话框，单击“硬件”选项卡，在出现的界面中单击“硬件配置文件”按钮，打开“硬件配置文件”对话框，如图 1.10 所示。

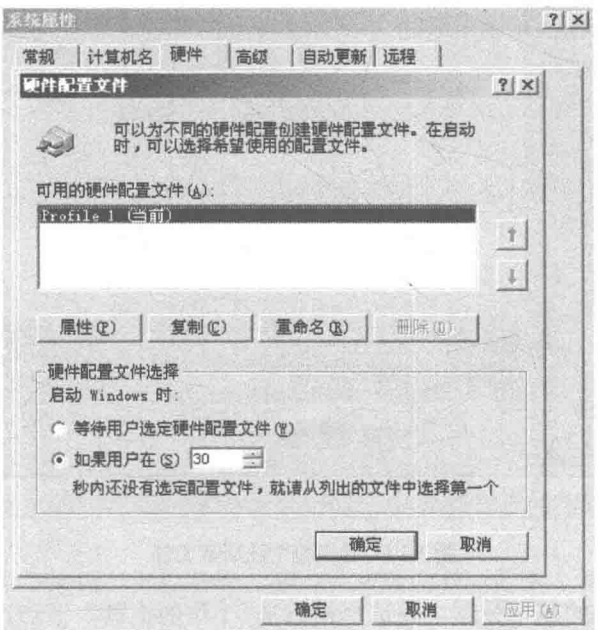

图 1.10　“硬件配置文件”对话框

(2)在“可用的硬件配置文件”列表中显示了本地计算机中可用的硬件配置文件清单，在“硬件配置文件选择”区域中，用户可以选择在启动 Windows 时(如有多个硬件配置文件)调用哪一个硬件配置文件。单击“复制”按钮，在打开的“复制配置文件”对话框中的“到”文本框中输入新的文件名，然后单击“确定”按钮即可。

8. 备份注册表文件

(1)在“运行”命令框中输入“regedit”打开注册表编辑器，如图 1.11 所示。

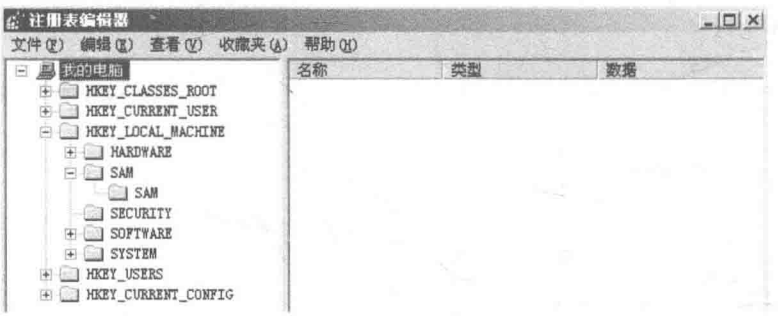

图 1.11　注册表编辑器

(2)备份整个注册表，请选择根目录(“我的电脑”节点)，然后在菜单中选择“导出命令，打开“导出注册表文件”对话框，在“文件名”文本框中输入新的名称，选择具体路径，单击“保存”按钮即可，如图 1.12 所示。

图 1.12　导出整个注册表文件

(3)备份注册表中的某一分支，先选择根目录(“我的电脑”节点)，然后在菜单中选择“导出”命令，然后选中“所选分支”单选按钮，输入要导出的分支名称即可。

9. 文件备份与还原

(1) 在客户端主机新建一个测试用文件夹，在该文件夹内保存或新建数个文件。执行“所有程序”→“附件”→“系统工具”→“备份”命令，可打开如图 1.13 所示的备份或还原向导。

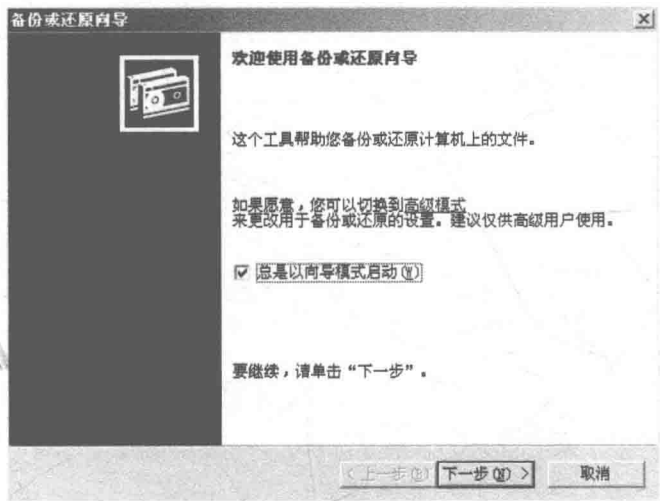

图 1.13　备份或还原向导

(2) 单击“下一步”按钮，在打开的界面中选中“备份文件和设置”单选按钮，如图 1.14 所示。

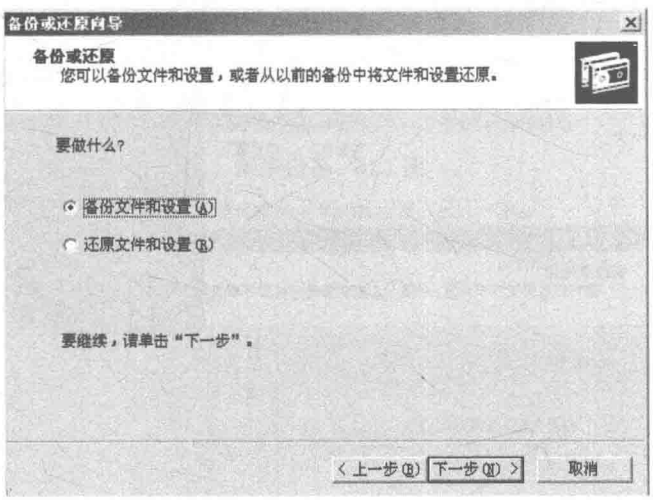

图 1.14　选择备份文件

(3) 单击“下一步”按钮，选择要备份的内容，然后选择需备份的文件，输入备份名称并选择路径，如图 1.15 所示。

(4) 单击“下一步”按钮，开始备份，备份完成后的界面如图 1.16 所示。

(5) 删除已备份的原文件，重新启动备份工具，选中“还原文件和设置”单选按钮，如图 1.17 所示。

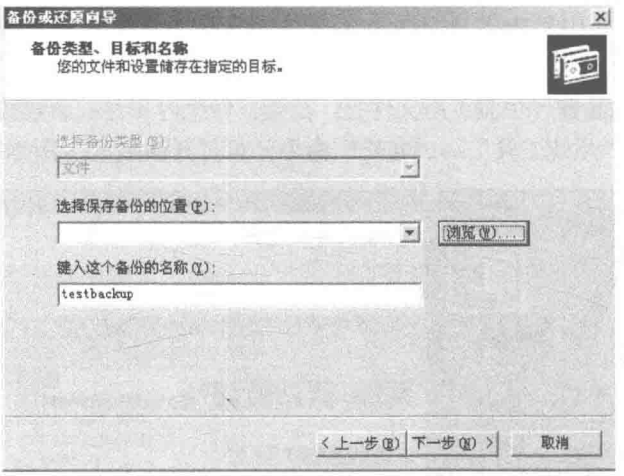

图 1.15　输入备份名称

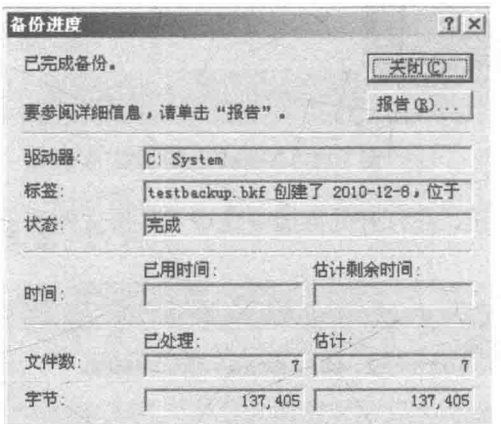

图 1.16　备份完成

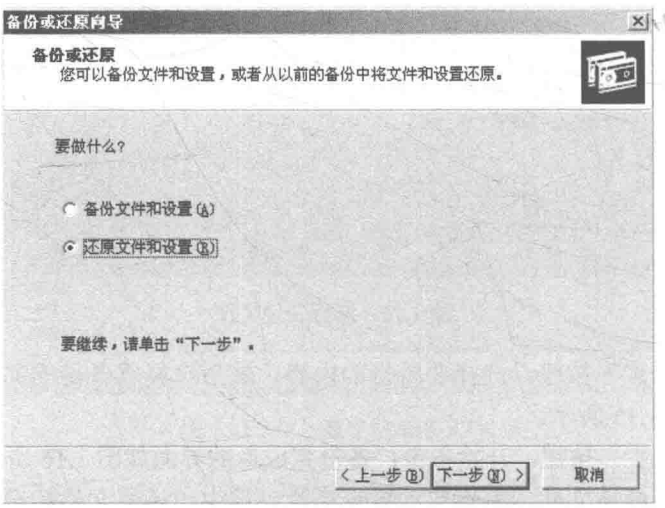

图 1.17　选择还原文件

(6)选择需还原的文件，如图 1.18 所示。

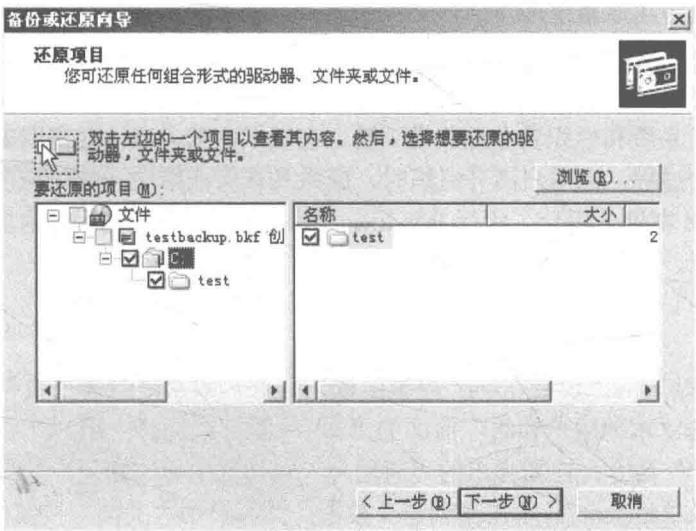

图 1.18　选择需还原的文件

(7)单击“下一步”按钮进行还原，如图 1.19 所示，之后单击“完成”按钮。

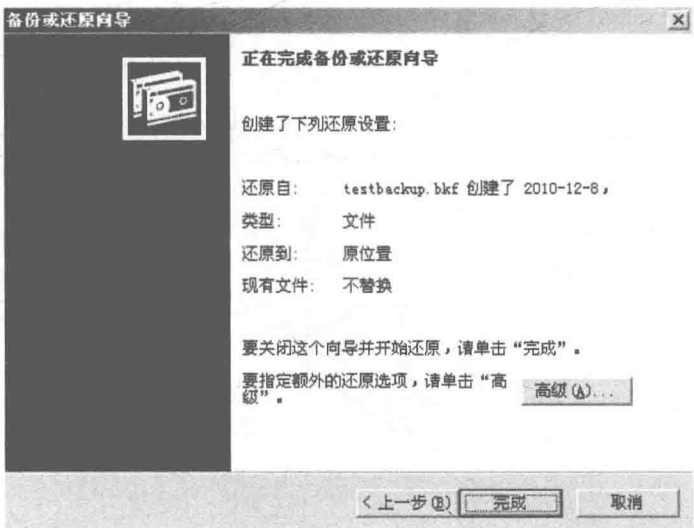

图 1.19　单击开始还原

(8)查看原文件目录是否还原成功。

10. 使用系统还原

(1)在客户端主机执行“所有程序”→“附件”→“系统工具”→“系统还原”命令，选择“创建一个还原点”选项。单击“下一步”按钮，添加还原点描述。

(2)单击“创建”按钮创建还原点。

(3)单击“主页”或“关闭”按钮后再启动系统还原，选择“恢复我的计算机到一个较

早的时间”选项，单击“下一步”按钮后，选择日期和还原点，按提示完成系统还原(可以只到这步，不需要真正还原系统)。

1.1.2　Windows 用户管理案例分析

用户管理对于系统和组织安全性非常关键，在组织内部，应该存在用来确定每个新用户具有的正确权限的过程，当用户离开组织时，应该具有保证用户不能访问系统的过程。

打开 Windows 案例分析台，运行 Windows 2003 系统。或者在本地主机的 NTFS 格式的磁盘进行案例分析，详细步骤如下。

1. 添加用户

(1)执行“开始”→“设置”→“控制面板”命令，双击“管理工具”项，双击“计算机管理”项，单击“本地用户和组”前面的“+”号图标；选择“用户”并右击；在弹出菜单中选择“新用户”命令，在新弹出的“新用户”对话框中填写新用户的信息，如在“用户名”文本框中输入“student”，单击“创建”按钮，然后单击“关闭”按钮，如图 1.20 所示。

(2)在新建的用户上右击，在弹出的菜单中选择“属性”命令，单击“隶属于”选项卡；单击左下角的“添加”按钮；在弹出的“选择组”界面，通过“查找”等选择“Power Users”，单击“确定”按钮，将用户添加到“Power User”组，如图 1.21 所示。

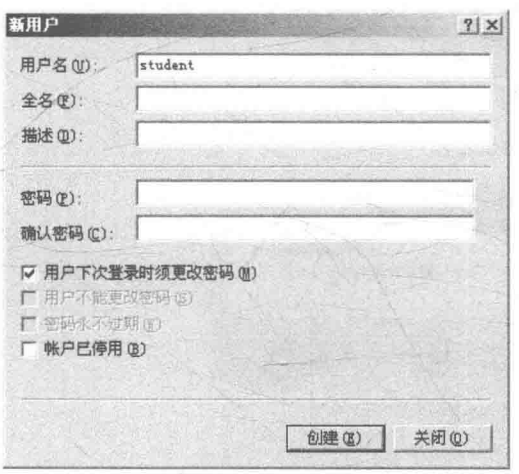

图 1.20　新建用户

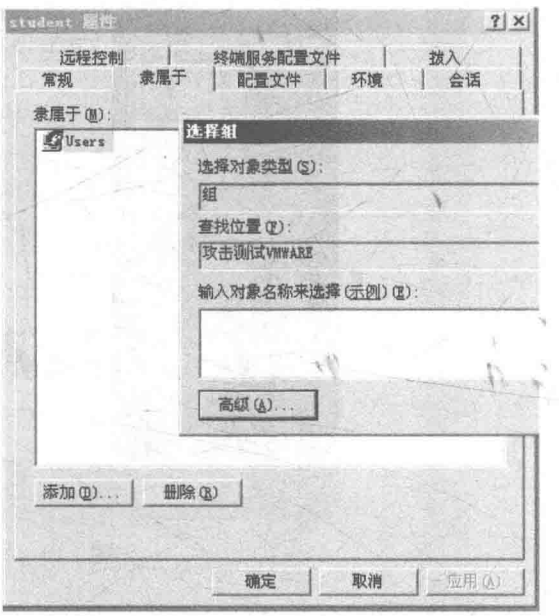

图 1.21　用户组属性

2. 禁用 Guest 账号

右击 Guest 用户，在“Guest 属性”对话框中把“账户已禁用”复选框选中，然后单击“确定”按钮，如图 1.22 所示。

3. 本地安全设置

(1)重命名 Administrator 账户。

右击 Administrator 用户，在弹出的菜单中选择“重命名”命令，然后把“Administrator”改成其他名字，如图 1.23 所示。

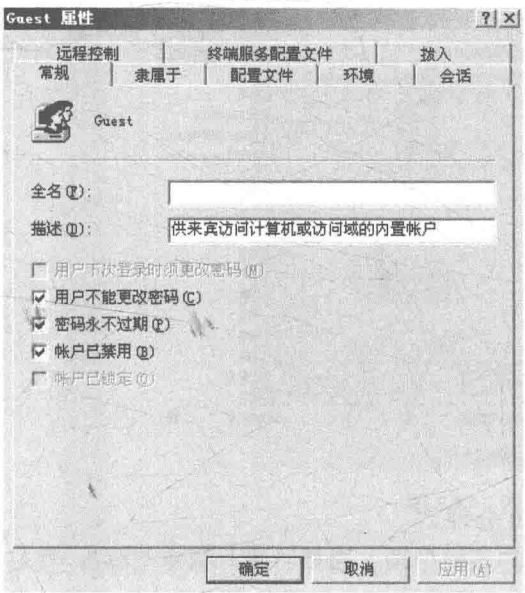

图 1.22　“Guest 属性”对话框

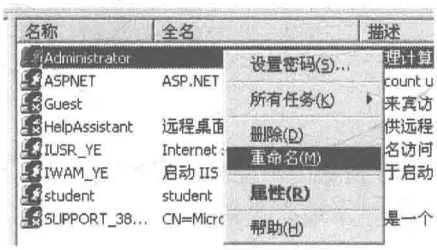

图 1.23　账号管理界面

(2)设置账户、密码必须满足复杂性要求。

执行“开始”→“设置”→“控制面板”命令，双击“管理工具”项，双击“本地安全策略”项，单击“账户策略”前面的“+”号图标，选择“密码策略”选项；在右边双击“密码必须符合复杂性要求”项，在弹出的对话框中把策略改为“已启用”状态，单击“确定”按钮，如图 1.24 所示。

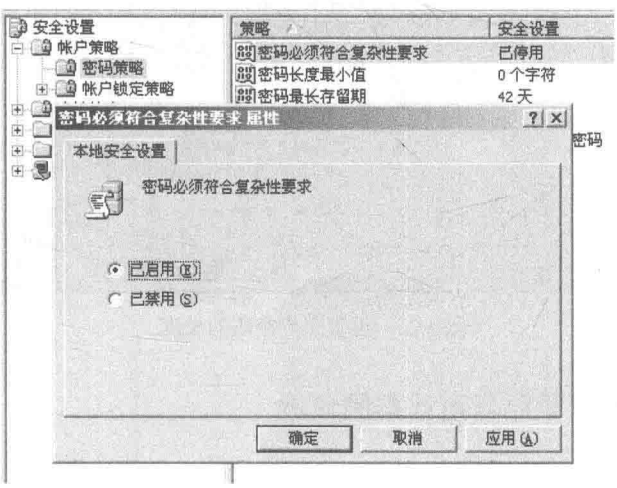

图 1.24　本地安全策略