工作过程导向新理念丛书
中等职业学校教材·计算机专业

网络安全与软件系统修复

丛书编委会 主编

清华大学出版社

工作过程导向新理念丛书

中等职业学校教材·计算机专业

网络安全与软件系统修复

丛书编委会 主编

清华大学出版社

北京

内容简介

本书根据教育部教学大纲，按照新的“工作过程导向”教学模式编写。为便于教师排课、备课、授课以及学生预习、上机练习、复习，本书将教学内容分解落实到每一课时，通过“课堂任务”、“课堂练习”、“本课小结”、“课外阅读”和“课后作业”五个环节实施教学。

本书共6章18课。第1～5章介绍了网络安全与软件系统修复的相关基础知识；第6章为综合案例实践，介绍了网络流量监控和内网入侵主机的过程。每课为两个标准学时，共90分钟内容。建议学时为1学期，每周3课时，也可以分为两学期授课。

本书从实用的角度出发，通过实例循序渐进地讲解了网络安全与软件系统修复的基础知识。书中详细地介绍了初学者必须掌握的网络安全基本知识和具体操作步骤，并对一些最新的网络安全技术也做了简单介绍，以适应形势发展的需要。

本书可作为中等职业学校网络安全相关专业的教材，也可作为各类技能型紧缺人才培训班的教材。

图书在版编目（CIP）数据

网络安全与软件系统修复/《工作过程导向新理念丛书》编委会主编．—北京：清华大学出版社，2009.10
工作过程导向新理念丛书
中等职业学校教材.计算机专业
ISBN 978-7-302-20229-5

Ⅰ.网… Ⅱ.工… Ⅲ.①计算机网络－安全技术 ②系统软件－故障修复 Ⅳ.TP393.08
TP31

中国版本图书馆CIP数据核字(2009)第079853号

责任编辑：田在儒　张　弛
责任校对：袁　芳
责任印制：杨　艳

出版发行：清华大学出版社　　**地　　址：**北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编：**100084
社　总　机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市昌平环球印刷厂
装 订 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185×260　　**印　　张：**14.75　　**字　　数：**356千字
版　　次：2009年10月第1版　　**印　　次：**2009年10月第1次印刷
印　　数：1～5000
定　　价：21.50元

学科体系的解构与行动体系的重构

——《工作过程导向新理念丛书》代序

职业教育作为一种教育类型，其课程也必须有自己的类型特征。从教育学的观点来看，当且仅当课程内容的选择以及所选内容的序化都符合职业教育的特色和要求之时，职业教育的课程改革才能成功。这里，改革的成功与否有两个决定性的因素：一个是课程内容的选择，一个是课程内容的序化。这也是职业教育教材编写的基础。

首先，课程内容的选择涉及的是课程内容选择的标准问题。

个体所具有的智力类型大致分为两大类：一是抽象思维，一是形象思维。职业教育的教育对象，依据多元智能理论分析，其逻辑数理方面的能力相对较差，而空间视觉、身体动觉以及音乐节奏等方面的能力则较强。故职业教育的教育对象是具有形象思维特点的个体。

一般来说，课程内容涉及两大类知识：一类是涉及事实、概念以及规律、原理方面的“陈述性知识”，一类是涉及经验以及策略方面的“过程性知识”。“事实与概念”解答的是“是什么”的问题，“规律与原理”回答的是“为什么”的问题；而“经验”指的是“怎么做”的问题，“策略”强调的则是“怎样做更好”的问题。

由专业学科构成的以结构逻辑为中心的学科体系，侧重于传授实际存在的显性知识即理论性知识，主要解决“是什么”（事实、概念等）和“为什么”（规律、原理等）的问题，这是培养科学型人才的一条主要途径。

由实践情境构成的以过程逻辑为中心的行动体系，强调的是获取自我建构的隐性知识即过程性知识，主要解决“怎么做”（经验）和“怎样做更好”（策略）的问题，这是培养职业型人才的一条主要途径。

因此，职业教育课程内容选择的标准应该以职业实际应用的经验和策略的习得为主，以适度够用的概念和原理的理解为辅，即以过程性知识为主、陈述性知识为辅。

其次，课程内容的序化涉及的是课程内容序化的标准问题。

知识只有在序化的情况下才能被传递，而序化意味着确立知识内容的框架和顺序。职业教育课程所选取的内容，由于既涉及过程性知识，又涉及陈述性知识，因此，寻求这两类知识的有机融合，就需要一个恰当的参照系，以便能以此为基础对知识实施“序化”。

按照学科体系对知识内容序化，课程内容的编排呈现出一种“平行结构”的形式。学科体系的课程结构常会导致陈述性知识与过程性知识的分割、理论知识与实践知识的分割，以及知识排序方式与知识习得方式的分割。这不仅与职业教育的培养目标相悖，而且与职业教育追求的整体性学习的教学目标相悖。

按照行动体系对知识内容序化，课程内容的编排则呈现一种“串行结构”的形式。在学习过程中，学生认知的心理顺序与专业所对应的典型职业工作顺序，或是对多个职业工作过程加以归纳整合后的职业工作顺序，即行动顺序，都是串行的。这样，针对行动顺序的每一个工作过程环节来传授相关的课程内容，实现实践技能与理论知识的整合，将收到事半功倍的效果。鉴于每一行动顺序都是一种自然形成的过程序列，而学生认知的心理顺序也是循序渐进自然形成的过程序列，这表明，认知的心理顺序与工作过程顺序在一定程度上是吻

合的。

需要特别强调的是，按照工作过程来序化知识，即以工作过程为参照系，将陈述性知识与过程性知识整合、理论知识与实践知识整合，其所呈现的知识从学科体系来看是离散的、跳跃的和不连续的，但从工作过程来看，却是不离散的、非跳跃的和连续的了。因此，参照系在发挥着关键的作用。课程不再关注建筑在静态学科体系之上的显性理论知识的复制与再现，而更多的是着眼于蕴含在动态行动体系之中的隐性实践知识的生成与构建。这意味着，**知识的总量未变，知识排序的方式发生变化，正是对这一全新的职业教育课程开发方案中所蕴含的革命性变化的本质概括**。

由此，我们可以得出这样的结论：如果“工作过程导向的序化”获得成功，那么传统的学科课程序列就将“出局”，通过对其保持适当的“有距离观察”，就有可能解放与扩展传统的课程视野，寻求现代的知识关联与分离的路线，确立全新的内容定位与支点，从而凸现课程的职业教育特色。因此，“工作过程导向的序化”是一个与已知的序列范畴进行的对话，也是与课程开发者的立场和观点进行对话的创造性行动。这一行动并不是简单地排斥学科体系，而是通过“有距离观察”，在一个全新的架构中获得对职业教育课程论的元层次认知。所以，**“工作过程导向的课程”的开发过程，实际上是一个伴随学科体系的解构而凸显行动体系的重构的过程**。然而，学科体系的解构并不意味着学科体系的“肢解”，而是依据职业情境对知识实施行动性重构，进而实现新的体系——行动体系的构建过程。不破不立，学科体系解构之后，在工作过程基础上的系统化和结构化的产物——行动体系也就“立在其中”了。

非常高兴，作为中国“学科体系”最高殿堂的清华大学，开始关注占人类大多数的具有形象思维这一智力特点的人群成才的教育——职业教育。坚信清华大学出版社的睿智之举，将会在中国教育界掀起一股新风。我为母校感到自豪！

2006 年 8 月 8 日

《工作过程导向新理念丛书》编委会名单

（按姓氏拼音排序）

前　言

互联网的发展，在带来了便利的同时，也给我们的生活增添了一份不安。网络安全屡屡受到攻击威胁，回顾过去的网络安全事件，黑客事件的骇人听闻、计算机病毒的频繁变种、安全漏洞的层出不穷，形势的发展要求我们必须掌握一些基本的网络安全与软件系统修复知识。

网络安全技术的发展日新月异，本书主要从操作系统安全配置、网络常见攻击与防范、网络安全工具软件实例、计算机病毒防治、数据备份与恢复几个方面进行讲述。

本书以“课”的形式展开，全书共 18 课。课前有情景式的“课堂任务”，包含了任务背景、任务目标和任务分析；课后有“课堂练习”，可分为任务背景、任务目标、任务要求和任务提示；“课堂练习”之后是“练习评价”。为了拓展本课的知识，我们还准备了“本课小结”、“课外阅读”。每课的最后还安排了“课后作业”。

本书的最后安排了两个“综合案例实践”，详细讲解了网络流量监控及内网入侵主机的过程。

全书共分 6 章 18 课：

第 1 章（第 1～3 课）讲解了操作系统安全配置；

第 2 章（第 4～6 课）讲解了几种常见的网络攻击与防范技术；

第 3 章（第 7～9 课）讲解了几个网络安全工具软件实例；

第 4 章（第 10～12 课）讲解了计算机病毒的基础知识；

第 5 章（第 13～16 课）详细讲解了数据备份与恢复的相关技术；

第 6 章（第 17～18 课）讲解了两个综合案例实践过程及演示。

本书的实验环境除非特别说明，大部分是在 Windows Server 2003 SP2 环境下实现的。

如果你只是一个网络安全的初学者，对网络安全和软件系统修复比较感兴趣，那么本书将成为你打开研究网络安全大门的“钥匙”。因为本书为了满足初学者的需要，从操作系统、安全工具软件、攻防实例演示等多方面较为系统地讲述了网络安全的基础知识，所以我们相信可以使初学者从入门到精通。

本书源于作者的亲身实践和学习经历。全书精选了很多网络安全与系统修复方面的示例，涵盖了网络安全与系统修复各方面的知识。通过对这些实例应用到的关键技术进行分析，详细讲解操作过程，使读者对网络安全的认识和操作水平迅速提高。

由于编者水平有限，再加上时间紧迫，表述不妥的地方在所难免，希望广大读者批评指正。

编　者

2009 年 9 月

目　录

第 1 章

操作系统安全配置

知识要点

- 端口
- 服务
- 审核策略
- 空链接
- 磁盘权限
- 文件共享
- 防火墙
- 账户管理
- 杀毒软件
- FTP 安全
- IIS 安全
- 系统补丁程序

第 1 课　Windows 个人操作系统安全配置

1.1　Windows XP 基本安全配置

目前，使用 Windows XP 系统的用户越来越多。由于微软公司的 Windows 操作系统和浏览器还存在大量的安全漏洞，因此个人计算机会经常遭受各种各样的入侵。即便安装了 Windows XP 系统的补丁程序 Service Pack 2，个人计算机仍难免受到侵袭。如何才能保障系统的安全呢？本节将详细讲述 Windows XP 操作系统的一些安全设置。

课堂任务

任务背景： Windows XP 是目前微软公司推出的使用较为广泛的个人操作系统，由于其简单易用、界面友好等特点，许多普通用户的个人计算机上都安装了该系统。但面对越来越多计算机病毒和流氓软件的侵扰，Windows XP 系统也暴露出了很多安全方面的漏洞。

任务目标： 熟悉 Windows XP 系统的安全配置。

任务分析： Windows XP 作为个人操作系统，入门容易，安全配置较为简单。这节课将从文件共享、账户管理、服务、防火墙等多个方面完成对 Windows XP 的安全配置。

步骤 1　取消“使用简单文件共享(推荐)”功能

为了使用户能够简单、快速地实现文件的共享，Windows XP 加入了一种称为“简单文件共享”的功能，但同时也打开了许多 NetBIOS 漏洞。关闭简单文件共享功能的方法是：首先打开

“我的电脑”窗口，选择菜单栏中的“工具”→“文件夹选项”命令；然后在弹出的对话框中打开“查看”选项卡，取消“高级设置”列表框中的“使用简单文件共享(推荐)”选项，如图 1-1 所示。

步骤 2　把 FAT32 文件系统转换成 NTFS 文件系统

许多计算机的硬盘分区都被格式化成 FAT32 格式。要想提高安全性，可以把 FAT32 文件系统转换成 NTFS。NTFS 允许更全面、详细的控制文件和文件夹的权限，进而可以使用加密文件系统(Encrypting File System，EFS)，从文件分区这一层次保证数据不被窃取。

打开“我的电脑”窗口，右击驱动器图标并选择“属性”命令，在弹出的磁盘属性对话框中可以查看驱动器当前的文件系统，如图 1-2 所示。

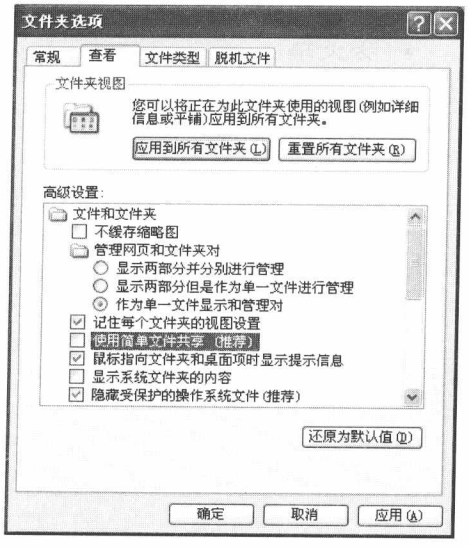

图　1-1

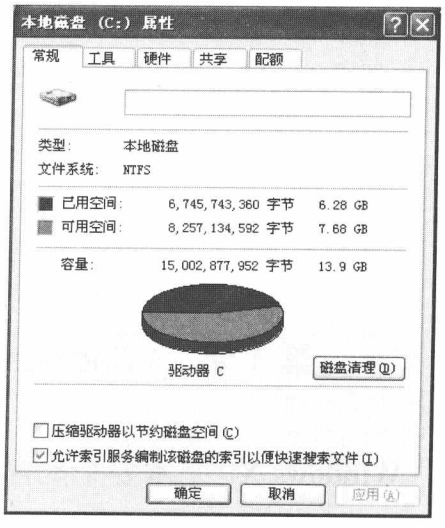

图　1-2

如果要把指定磁盘的 FAT32 文件系统转换成 NTFS，首先需要先备份一下重要的文件，然后运行“cmd”命令，在命令行窗口中，执行“convert c: /fs:ntfs”(其中 c 是驱动器的盘符)，如图 1-3 所示。

图　1-3

小贴士

NTFS 文件系统要比 FAT、FAT32 的文件系统安全得多。程序的数据存储在 D 盘，把服务器的分区改成 NTFS 格式，会增加系统的安全性。另外，NTFS 格式分区中单个文件的增长不受限制，这样也可防止因数据量不断增长而产生问题。

步骤 3　停用 Guest 账户

Guest 账户可以访问计算机，但受到限制，黑客入侵通常借用该账户。如果不需要用到 Guest 账户，最好禁用它。在 Windows XP 系统中，依次选择“控制面板”→“用户账户”，单击“Guest”账户，选择“禁用来宾账户”，如图 1-4 所示。

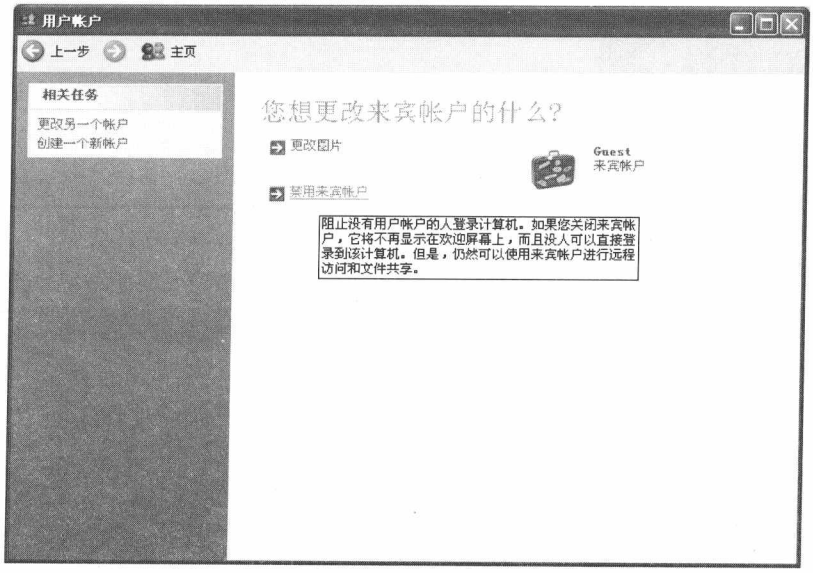

图　1-4

步骤 4　改变 Administrator 账户默认设置

黑客入侵的常用手段之一就是试图获得 Administrator 账户的密码。每一台计算机至少需要一个账户拥有 Administrator(管理员)权限，但不一定非用“Administrator”这个名称，所以最好创建另一个拥有全部权限的账户，然后停用 Administrator 账户。另外，最好修改一下默认的所有账户名称并为所有账户设置足够复杂的密码。如图 1-5 和图 1-6 所示。

步骤 5　清除系统的页面文件

即使操作正常，Windows 也会泄露重要的机密数据(包括密码)，黑客会对这些泄露的机密文件感兴趣。只要计算机在关机的时候清除系统的页面文件(交换文件)，就可以避免这个问题。

具体操作方法是：运行“regedit”命令，在注册表中找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management，然后创建

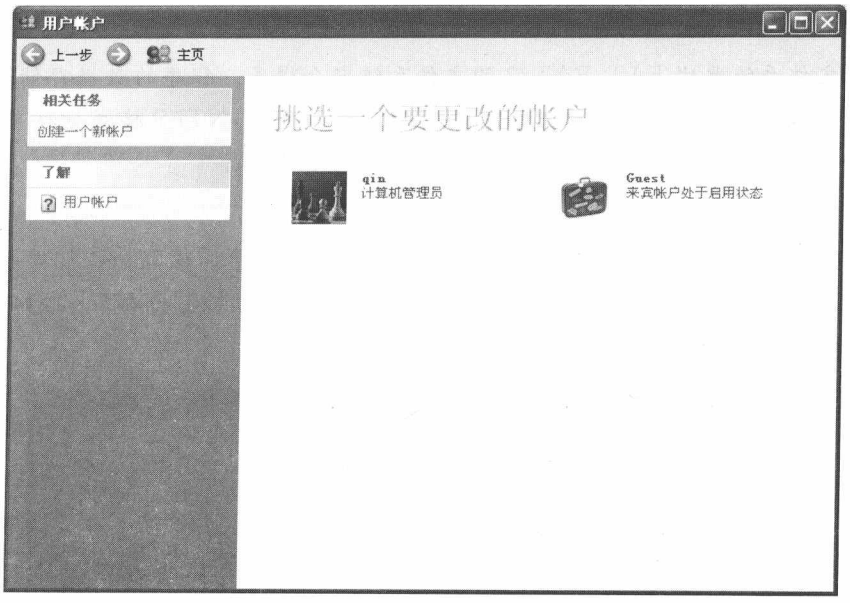

图 1-5

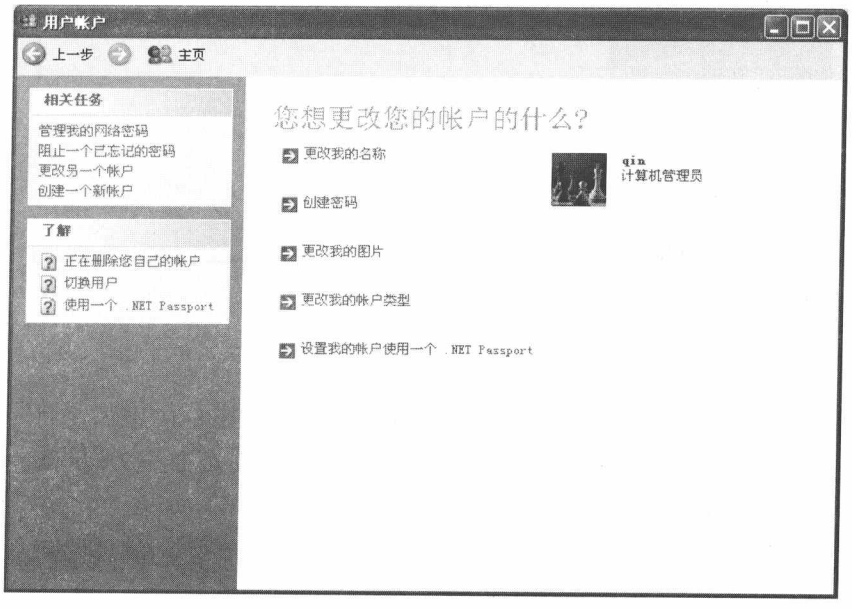

图 1-6

或修改 ClearPageFileAtShutdown，并将其值设置为 1，如图 1-7 所示。

步骤 6　禁止 Windows 创建转储文件

系统在遇到严重问题时，会把内存中的数据保存到转储文件。转储文件的作用是帮助人们分析系统遇到的问题，但对一般用户来说用处不大；另一方面，就像交换文件一样，转储文件也可能泄露许多敏感数据。

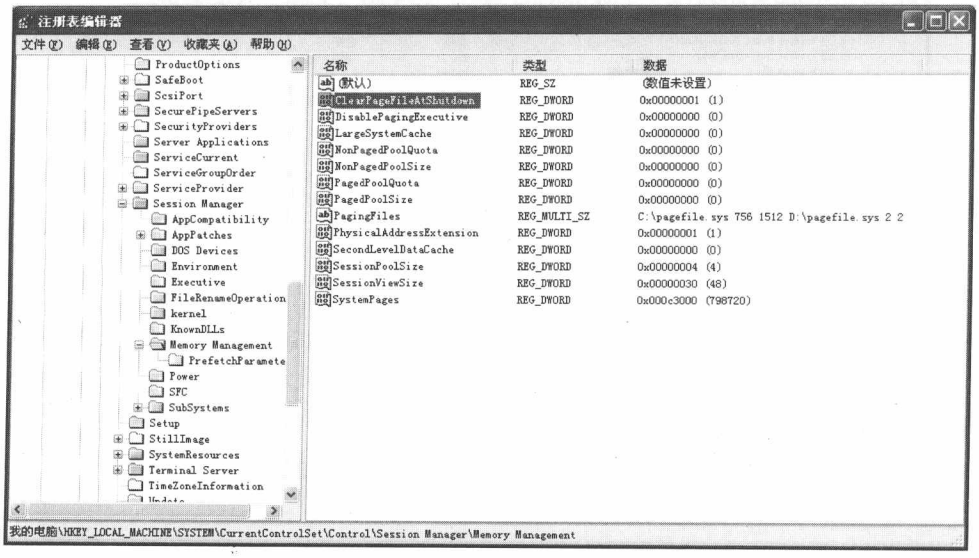

图　1-7

禁止 Windows 创建转储文件的操作方法是：依次选择“控制面板”→“性能和维护”→“系统”，打开“高级”选项卡，然后单击“启动和故障恢复”选项组中的“设置”按钮，将“写入调试信息”设置成“(无)”，如图 1-8所示。

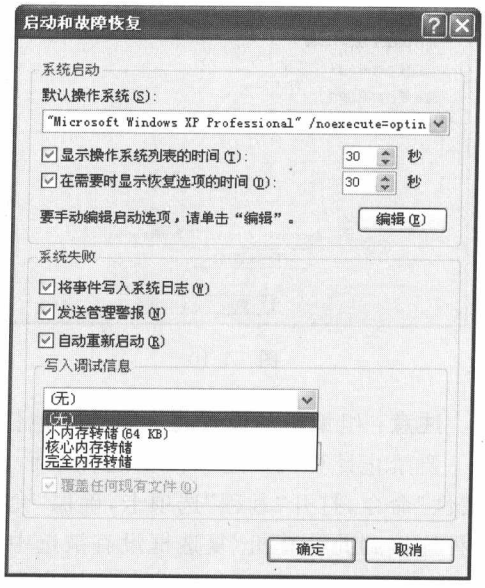

图　1-8

类似于转储文件，Dr. Watson 也会在应用程序出错时保存调试信息。禁用 Dr. Watson 的方法是：运行“regedit”命令，在注册表中找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug，把 Auto 值改成“0”，如图 1-9 所示。

步骤 7　禁用远程协助和远程桌面

远程协助和远程桌面因为用途的关系而具有一定的安全风险，建议不要在需要高度安全性的网络中使用远程控制技术。

禁用远程协助的具体操作是：运行“gpedit. msc”命令，打开“组策略编辑器”，依次选择“计算机配置”→“管理模板”→“系统”→“远程协助”，双击右侧子窗口中的“请求的远程协助”，打开“设置”选项卡，选中“已禁用”单选按钮，单击“应用”按钮应用设置，如图 1-10 所示。

双击右侧子窗口中的“提供远程协助”，打开“设置”选项卡，选中“已禁用”单选按钮，单击“应用”按钮应用设置，如图 1-11 所示。

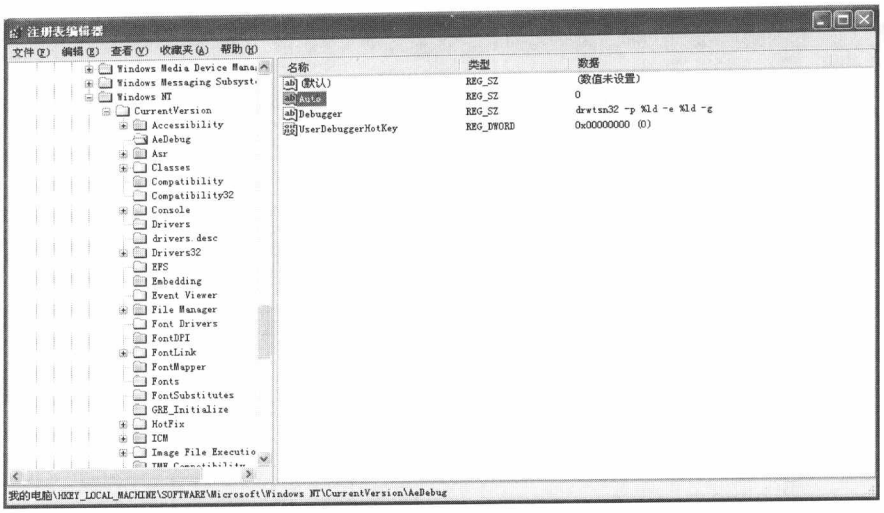

图 1-9

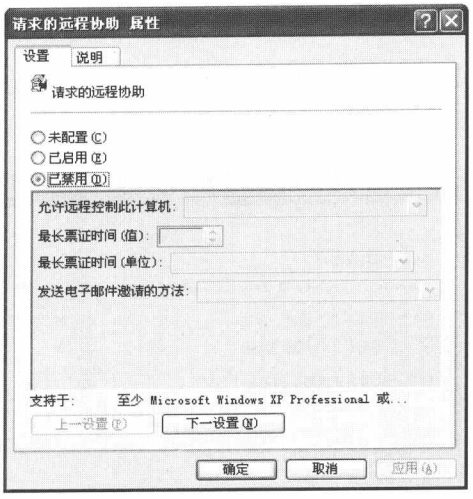

图 1-10

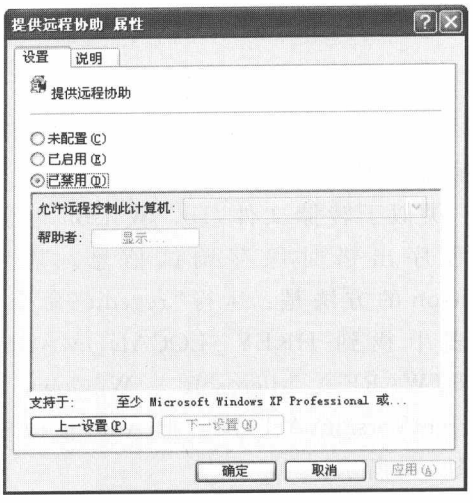

图 1-11

注意：组策略的设置将会覆盖其他任何系统属性中远程选项卡的设置。

要禁止计算机发送和接受远程桌面连接，进行如下操作：右击“我的电脑”图标，选择“属性”命令，打开“远程”选项卡，确保“允许从这台计算机发送远程协助邀请”和“允许用户远程连接到此计算机”复选框没有被选中，如图 1-12 所示。单击“选择远程用户”按钮，打开“远程桌面用户”对话框，删除所有用户和用户组，如图 1-13 所示。

步骤 8　停止多余的服务

为了方便用户，Windows XP 系统默认启动了许多平时用不到的服务，与此同时也使黑客有了入侵系统的后门。因此如果不使用这些服务，最好关闭它们，例如 NetMeeting Remote Desktop Sharing、Remote Desktop Help Session Manager、Remote Registry、Routing and Remote Access、SSDP Discovery Service、Telnet、Universal Plug and Play Device Host 等。

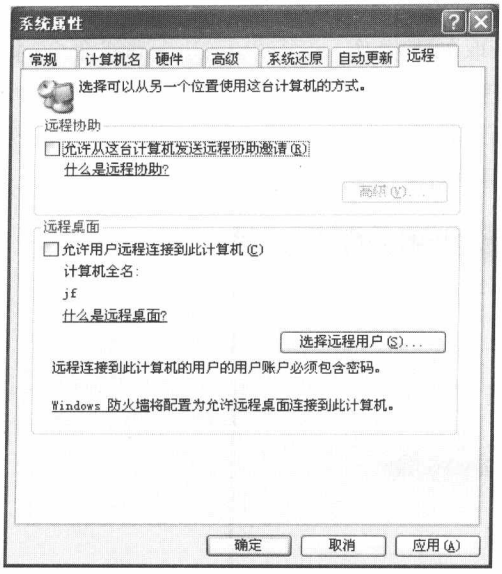

图　1-12

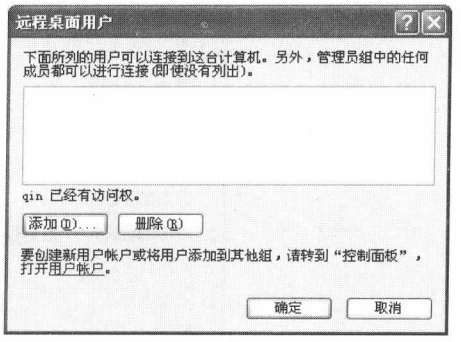

图　1-13

操作方法是：依次打开“控制面板”→“性能和维护”→“管理工具”→“服务”，可以看到有关这些服务的说明和运行状态。要关闭一个服务，只须右击服务名称并选择“属性”命令，在“常规”选项卡中把“启动类型”改成“手动”，再单击“停止”按钮即可，如图 1-14 所示。

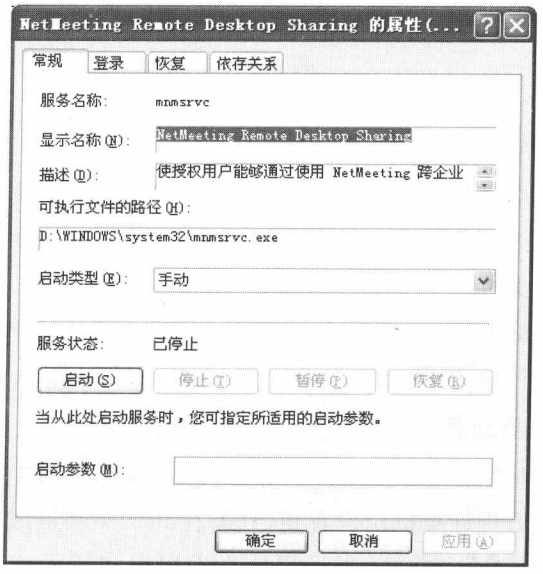

图　1-14

步骤 9　禁用自动播放功能

自动播放功能会在媒体插入后自动读取其中的数据，默认情况下，Windows XP 会自动运行光驱中插入的所有光盘，这将会使可执行的内容在被允许前自动被执行。默认情况下

软盘和网络驱动器的自动播放功能被禁用。

要禁用所有驱动器上的自动播放功能，可采取如下操作：运行“gpedit. msc”命令，打开“组策略”编辑器，依次选择“计算机配置”→“管理模板”→“系统”，双击右侧子窗口中的“关闭自动播放”按钮，打开“设置”选项卡，选中“已启用”单选按钮，在“关闭自动播放”下拉列表中选择“所有驱动器”选项，如图 1-15 所示。应用设置并关闭窗口。

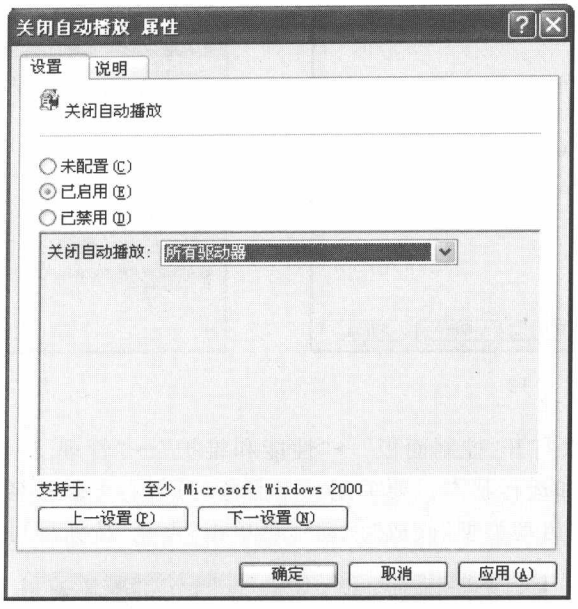

图 1-15

步骤 10　关闭网络中的 NetBIOS 和 SMB 端口

Windows NetBIOS 和 SMB 端口(端口 135～139 以及端口 445)之间的交流可以提供关于 Windows 系统的很多信息，并且可能引起潜在的攻击。因此禁止从局域网外连向系统这些端口的连接是很重要的。

建议在防火墙或者路由器上设置阻挡端口 135、137、138、139 和 445 的出站以及入站连接，大量的攻击以及潜在的威胁都是因为出站的 SMB 连接造成的。

步骤 11　禁用服务器服务

Windows XP 系统中可以很方便地将驱动器或文件夹设置成“共享”。若不想让这些共享的驱动器或文件夹被远程计算机用户看到，只需在共享驱动器或文件夹的共享名后面加上一个“$”就行了，如“C$”。然而，当远程计算机用户知道了该计算机的名称以及管理员、服务器操作员的用户名和密码后，那么任何远程计算机用户都能通过局域网络或互联网访问该计算机，这也使具有共享驱动器或文件夹的计算机存在着安全隐患。为保障共享驱动器或文件夹的安全，应该禁用服务器服务。禁用服务器服务后，所有远程计算机都将无法连接到该计算机上的任意驱动器或文件夹，但本机的管理员仍然能够访问其他计算机上的共享文件夹。

禁用服务器服务的操作方法是：依次选择“控制面板”→“性能和维护”→“管理工具”，双击“服务”图标，在“服务”窗口中双击“Server”项，出现“Server 的属性(本地计算机)”对话框，在“启动类型”下拉列表中选择“已禁用”或“手动”项即可，如图 1-16 所示。

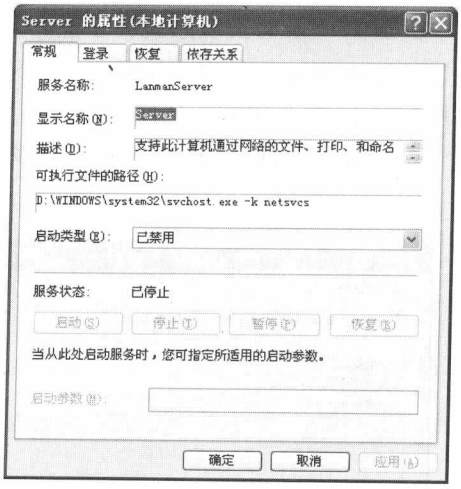

图　1-16

步骤 12　禁止修改 IE 浏览器的主页

运行“gpedit. msc”命令，依次选择“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”，然后在右侧子窗口中双击“禁用更改主页设置”策略，在“设置”选项卡中选中“已启用”单选按钮，单击“应用”按钮应用设置，如图 1-17 所示。

步骤 13　禁用 IE 组件自动安装

运行“gpedit. msc”命令，依次选择“计算机配置”→“管理模板”→“Windows 组件”→“Internet Explorer”，双击右侧子窗口中的“禁用 Internet Explorer 组件的自动安装”，在打开的对话框中选中“已启用”单选按钮，如图 1-18 所示。这样可以禁止 Internet Explorer 自动安装组件，防止 Internet Explorer 在用户访问到需要某个组件的网站时下载该组件，恶意修改 IE 设置的行为也会得到遏制，相对来说 IE 就会安全许多。

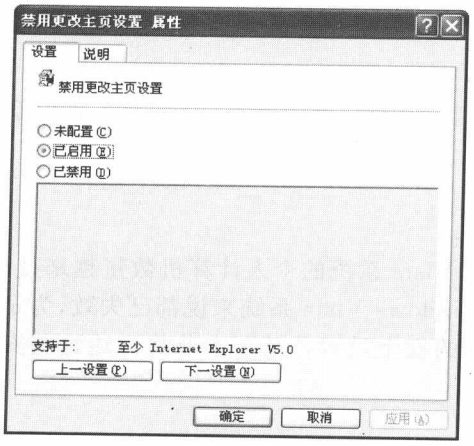

图　1-17

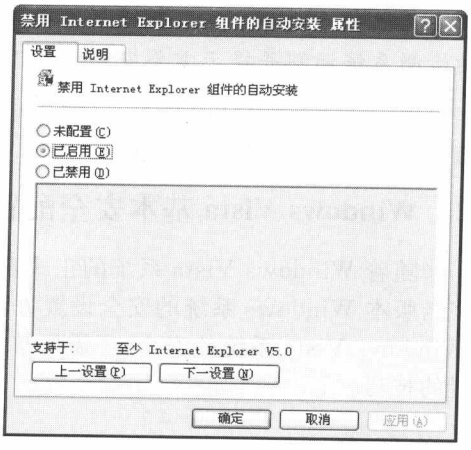

图　1-18

步骤 14　限制 IE 浏览器的保存功能

当多人共用一台计算机时，为了保持硬盘的整洁，需要对浏览器的保存功能进行限制使用。具体操作方法是：运行“gpedit. msc”命令，依次选择“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”→“浏览器菜单”。双击右侧子窗口中的“‘文件’菜单：禁用‘另存为...’菜单项”，在打开的对话框中选中“已启用”单选按钮，如图 1-19 所示。