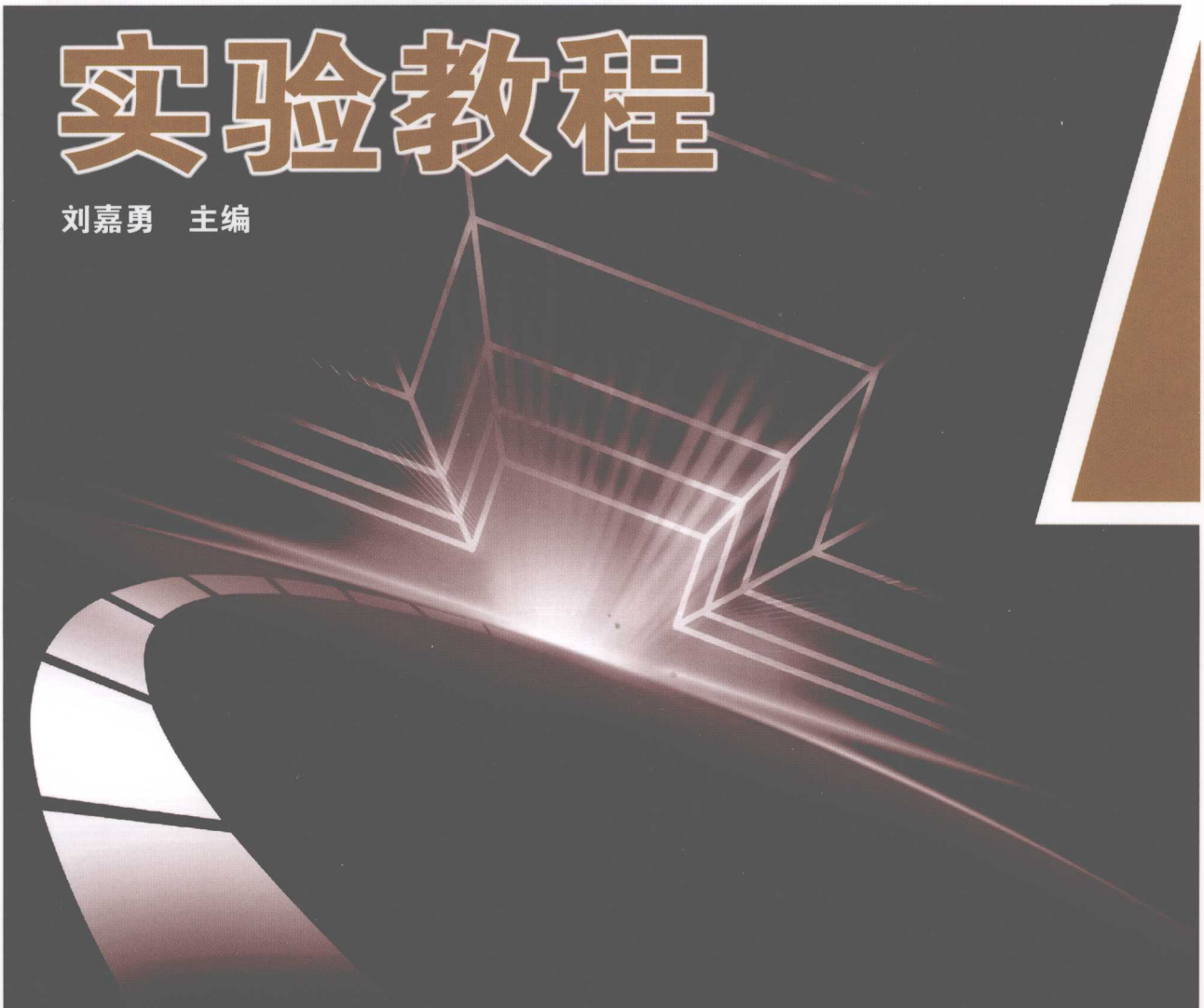
INXIANQUANJISHU SHIYAN JIAOCHENG

信息安全技术

实验教程

刘嘉勇 主编



四川大学出版社

XINXIANQUANJISHU SHIYAN JIAOCHENG

信息安全技术实验教程

主编　刘嘉勇

编者　严斌宇　欧晓聪

刘嘉勇　吴少华

方　勇

四川大学出版社

责任编辑:胡兴戎
责任校对:罗　杨
封面设计:翼虎书装
责任印制:李　平

图书在版编目(CIP)数据

信息安全技术实验教程 / 刘嘉勇主编. —成都：四川大学出版社，2007.9
ISBN 978-7-5614-3846-6

Ⅰ.信… Ⅱ.刘… Ⅲ.信息系统-安全技术-高等学校-教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2007）第 151360 号

内容提要

本书是作者根据近几年在网络信息安全技术方面的理论和实践教学情况，针对高等院校信息安全及信息技术类相关本科/专科专业课程特点，从实验教学适用性出发，以培养和锻炼学生网络信息安全技术实际动手能力和创新能力为目标编写而成的。全书编排了系统与应用安全配置、网络互连与安全配置技术、网络攻防技术、VPN 技术、防火墙技术以及主机监控与审计技术等六个专题二十多个网络信息安全技术实验项目，以帮助读者掌握网络信息安全的基本方法和技术，巩固和拓展信息安全专业课程的基础理论知识，更深入地认识和掌握信息安全体系和各种安全服务及安全机制。

本书可作为信息安全、网络工程及计算机应用本科/专科实验教材，也可作为网络信息安全职业技术培训实验教材，也适合于企事业单位的网络安全管理人员、信息系统管理人员以及其他相关专业技术人员阅读和参考。

书名　**信息安全技术实验教程**

主　　编　刘嘉勇
出　　版　四川大学出版社
地　　址　成都市一环路南一段 24 号 (610065)
发　　行　四川大学出版社
书　　号　ISBN 978-7-5614-3846-6/TP·161
印　　刷　成都蜀通印务有限责任公司
成品尺寸　185 mm×260 mm
印　　张　20.75
字　　数　499 千字
版　　次　2007 年 10 月第 1 版
印　　次　2007 年 10 月第 1 次印刷
印　　数　0 001～1 000 册
定　　价　30.00 元

◆读者邮购本书，请与本社发行科联系。电 话：8540808/8540167O/85408023　邮政编码：610065
◆本社图书如有印装质量问题，请寄回出版社调换。
◆网址：www.scupress.com.cn

前 言

信息安全已成为21世纪国际竞争的重要战场。随着信息安全产业的快速发展，社会对信息安全人才的需求不断增加，在高等教育领域大力推进信息安全的专业化教育是国家在信息安全领域掌握自主权、占领先机的重要举措。

信息安全学科领域兼有理论、应用和工程技术特点，在人才培养方案的规划和设计中，必须重视学生实际动手能力和创新能力的培养，强化学生的实验和实践环节。但是，目前在信息安全实验和实践方面的教材建设却没有受到足够的重视，无论在数量上还是在质量上都不能适应信息安全专业人才培养的要求。为此，针对高等院校信息技术类相关专业本科生所开设的信息安全课程特点，结合我们近几年在网络信息安全技术方面的理论和实践教学情况，在我们使用多年的讲义《信息安全实验指导》的基础上编写了本书。

我们希望通过本课程的教学活动，使学生掌握网络安全的基本技术，巩固和拓展信息安全专业课程的基础理论知识，更深入地认识和掌握信息安全体系结构和各种安全服务及安全机制。在教材内容的组织和撰写方式上，重视培养学生对实际问题的分析能力和理论知识的综合运用能力，以锻炼学生独立思考、分析问题和解决问题的实际动手能力。

全书共分为六章，对应网络信息安全的六个实验专题。第1章介绍Windows服务器的用户和文件管理及安全配置、因特网信息服务器的安全配置，以及用SSL实现对Web服务器的安全访问。第2章介绍计算机局域网络的基本构成和配置方法，以及路由器配置的基本方法。第3章介绍网络攻击与防范的基本原理、常用方法及相关工具。准备的实验项目包括账号口令破解、网络嗅探、目标端口与系统漏洞扫描及利用、木马攻击与防范，

以及网络渗透综合实验等内容。第4章介绍虚拟专用网VPN的配置及应用技术。第5章介绍防火墙的原理和配置方法，包括包过滤、状态检测、应用代理、NAT以及日志审计等防火墙技术实验内容。第6章介绍主机监控与审计技术，给出了在网络环境下，对主机资源及其用户操作行为进行监控，防止违规操作和敏感信息泄漏的主要方法和过程，并可通过实验编程，帮助学生认识和掌握主机监控与审计基本技术。

本书可作为信息安全、网络工程及计算机应用本科/专科实验教材，亦可作为网络信息安全职业技术培训实验教材，也适合企事业单位的网络安全管理人员、信息系统管理人员以及其他相关专业技术人员参考和阅读。

本书由四川大学信息安全专业实验室组织编写，其中，第1、2章由严斌宇编写，第3章由欧晓聪编写，第4章由刘嘉勇编写，第5章由吴少华编写，第6章由方勇编写。全书由刘嘉勇负责大纲拟定、组织编著与统稿工作。孙江宏、龙翔、富璇、杨漫、寇磊、张妹璞、樊宇等研究生参与了部分资料的收集和整理工作，在此向他们表示深深的感谢。

四川大学电子信息学院的领导对信息安全专业实验室的建设及本教材的编著、出版给予了大力支持。在本书的编著过程中，四川大学信息安全研究所戴宗坤教授、周安民教授对本书的编著提出了宝贵的意见和建议。借本书出版之机，向他们表示最诚挚的感谢。

由于作者水平所限，加之编著工作的时间较为紧张，书中难免有需要商榷之处，恳请读者批评指正。

编著者

2007年8月于四川大学

目 录

第 1 章　系统与应用安全配置实验

实验 1-1　Windows 服务器的安全配置

实验目的

(1) 掌握 Windows 用户和文件管理的安全配置。
(2) 熟悉 Windows 安全的基本配置技术。
(3) 了解 Windows 注册表的操作。

实验环境

一、设备需求

(1) 安装有 Windows 2000 Server 操作系统的主机 1 台；
(2) 安装有 Windows 2000 Pro 操作系统的主机 1 台；
(3) 普通 Hub 1 个；
(4) 网络线若干。

本实验为小组实验，每四名学生组成一个小组。每组有集线器一台、PC 机四台。每个学生用 PC 机上均安装有 Windows XP 操作系统，并安装 VMware 虚拟机软件，在虚拟机中安装 Windows 2000 Server。学生需在虚拟机的 Windows 2000 Server 上进行安全配置实验以及注册表的操作。

二、拓扑环境

本实验所需的拓扑环境如图 1-1-1 所示。

图 1-1-1　实验拓扑环境

实验内容

一、账号和密码策略

1. 保证禁止 Guest 账号并修改密码

单击“开始”→“程序”→“管理工具”→“计算机管理”。单击“本地用户和组”，单击“用户”，如图 1－1－2 所示。

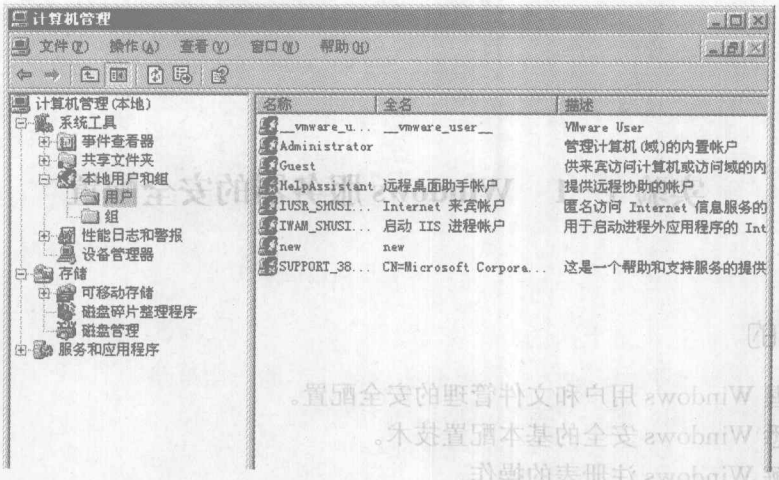


图 1－1－2　计算机管理对话框

双击“Guest”，确认“账户已停用”选中，如图 1－1－3 所示。

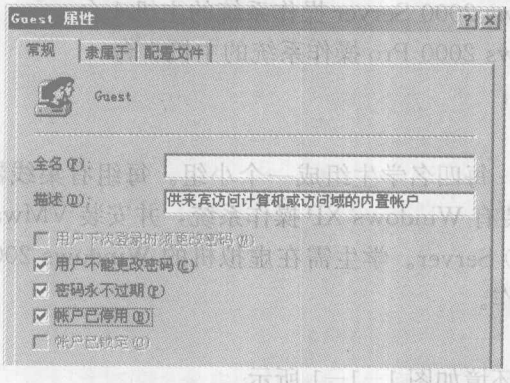


图 1－1－3　用户属性对话框

确认后，在图 1－1－2 中选中“Guest”，单击鼠标右键，单击“设置密码”，输入一个复杂的密码。

2. 将 Administrator 改名为比较难猜的账号并设置复杂的密码

单击“开始”→“程序”→“管理工具”→“计算机管理”。

如图 1－1－4，选中“Administrator”，单击鼠标右键，单击“设置密码”，输入一个复杂的密码。

选中“Administrator”，单击鼠标右键，重命名，输入一个较难猜的账号。

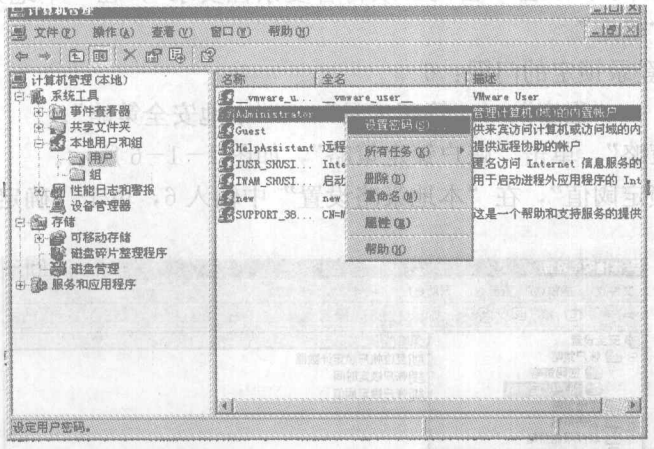


图 1−1−4　管理员属性修改

3. 密码唯一性：记录上次的 6 个密码

单击“开始”→“程序”→“管理工具”→“本地安全策略”。

单击“账户策略”，单击“密码策略”，如图 1−1−5 所示。

双击“强制密码历史”，在“本地策略设置”重输入 6，单击“确定”。

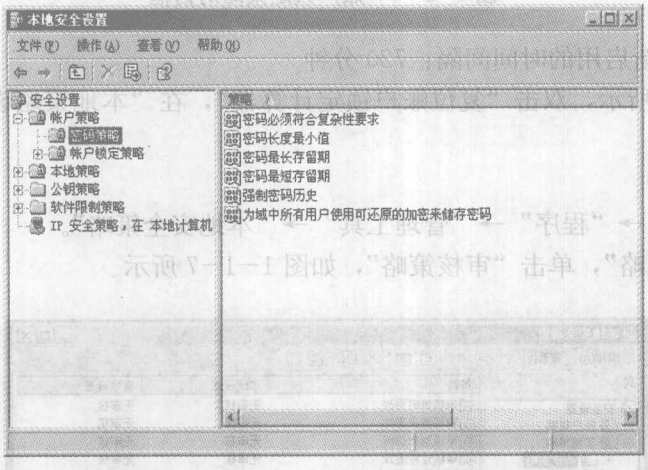


图 1−1−5　本地安全设置窗口

4. 密码最短存留期：2

如图 1−1−5 所示，双击“密码最短存留期”，在“本地策略设置”中输入 2，单击“确定”。

5. 密码最长存留期：42

如图 1−1−5 所示，双击“密码最长存留期”，在“本地策略设置”中输入 42，单击“确定”。

6. 密码长度最小值：8

如图 1−1−5 所示，双击“密码长度最小值”，在“本地策略设置”中输入 8，单击“确定”。

7. 密码复杂化：启用

如图 1－1－5 所示，双击“密码必须符合复杂性要求”，在“本地策略设置”中选择“已启用”，单击“确定”。

8. 账号失败登录锁定的门限：6

单击“开始”→“程序”→“管理工具”→“本地安全策略”。

单击“账户策略”，单击“账户锁定策略”，如图 1－1－6 所示。

双击“账户锁定阈值”，在“本地策略设置”中输入 6，单击“确定”。

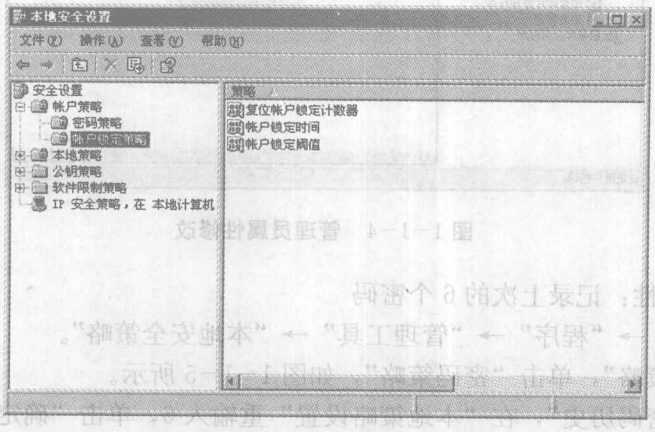


图 1－1－6　账户锁定策略对话框

9. 锁定后重新启用的时间间隔：720 分钟

如图 1－1－6 所示，双击“复位账户锁定计算器”，在“本地策略设置”中输入 720，单击“确定”。

二、审计策略

单击“开始”→“程序”→“管理工具”→“本地安全策略”。

单击“本地策略”，单击“审核策略”，如图 1－1－7 所示。

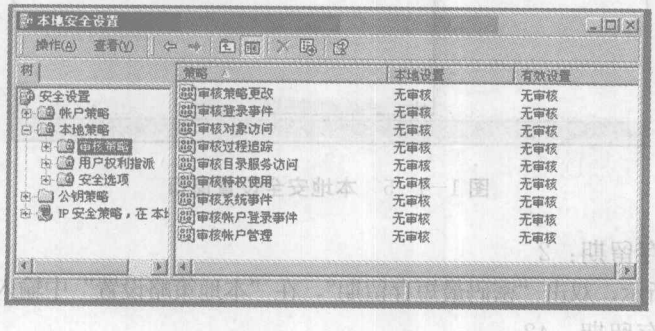


图 1－1－7　审核策略对话框

设置以下策略的成功和失败选项：

- 审核策略更改
- 审核登录事件

- 审核对象访问
- 审核系统事件
- 审核账户登录事件
- 审核账户管理

三、关闭所有不需要的服务

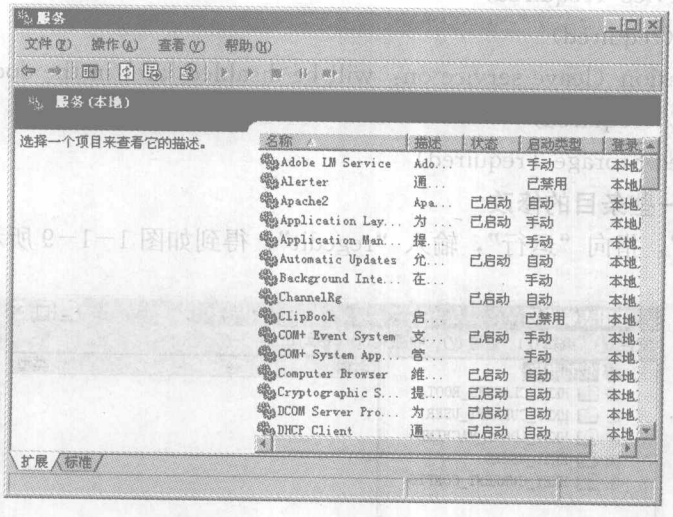


图 1－1－8　服务对话框

(1) 单击“开始”→“程序”→“管理工具”→“服务”。

(2) 如图 1－1－8 所示，选择以下服务的启动类型为“已禁用”：

- ✕ Alerter
- ✕ ClipBook
- ✕ Directory Replicator
- ✕ FTP Publishing Service
- ✕ License Logging Service
- ✕ Messenger
- ✕ Netlogon
- ✕ Network DDE
- ✕ Network DDE DSDM
- ✕ Network Monitor
- ✕ Remote Access Server
- ✕ Remote Procedure Call (RPC) Locater
- ✕ Schedule
- ✕ Simple Service
- ✕ TCP/IP Netbios Helper
- ✕ Telephone Service
- ✕ SNMP Service (optional)

× SNMP Trap（optional）

× UPS（optional）

（3）如图 1－1－8 所示，选择以下服务的启动类型为“自动启动”：

- Eventlog（required）
- NT LM Security Provider（required）
- RPC Service（required）
- WWW（required）
- Workstation（leave service on；will be disabled later in the document）
- MSDTC（required）
- Protected Storage（required）

四、注册表一些条目的修改

单击“开始”，指向“运行”，输入“regedit”，得到如图 1－1－9 所示的结果。

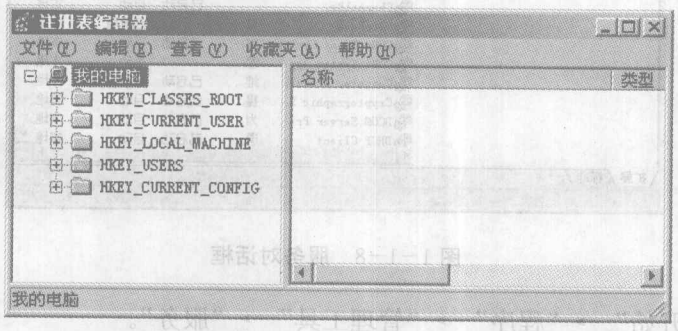


图 1－1－9　注册表对话框

在编辑器中修改以下内容：

1）去除 logon 对话框中的 shutdown 按钮

将 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\中 ShutdownWithoutLogon REG_SZ 值设为 0。

2）去除 logon 信息的 cashing 功能

将 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\中 CachedLogonsCount REG_SZ 值设为 0。

3）隐藏上次登陆的用户名

将 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\中 DontDisplayLastUserName REG_SZ 值设为 1。

4）限制 LSA 匿名访问

将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA 中 RestricAnonymous REG_DWORD 值设为 1。

5）去除所有网络共享

将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\中 AutoShareServer REG_DWORD 值设为 0。

五、移动部分重要文件并加访问控制

(1) 创建一个只有系统管理员能够访问的目录。

(2) 将 system32 目录下的一些重要文件移动到此目录：xcopy. exe，wscript. exe，cscript. exe，net. exe，ftp. exe，telnet. exe，arp. exe，edlin. exe，ping. exe，route. exe，at. exe，finger. exe，posix. exe，rsh. exe，atsvc. exe，qbasic. exe，runonce. exe，syskey. exe，cacls. exe，ipconfig. exe，rcp. exe，secfixup. exe，nbtstat. exe，rdisk. exe，debug. exe，regedt32. exe，regedit. exe，edit. com，netstat. exe，tracert. exe，nslookup. exe，rexec. exe，cmd. exe。

(3) 将此文件夹设为只读。

六、用安全模板配置基本的系统安全策略

(1) 下载安全模板 Hisecweb. inf。

下载地址：http://download. microsoft. com/download/win2000srv/SCM/1. 0/NT5/EN-US/hisecweb. exe。

(2) 将该模板复制到 winnt \ security \ templates 目录。

(3) 启动安全模板。

①决定是否将安全模板添加到现有的控制台，或创建新控制台。

要创建控制台，应单击“开始”，单击“运行”，键入“mmc”，然后单击“确定”。

如图 1-1-10 所示，打开“控制台”，将安全模板添加到现有的控制台中，打开控制台，然后进行下一步操作。

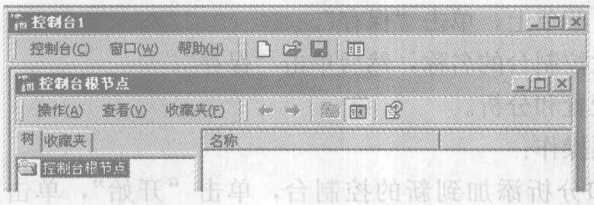


图 1-1-10　控制台界面

②如图 1-1-11 所示，在“控制台”菜单上，单击“添加/删除管理单元”，然后单击“添加”。

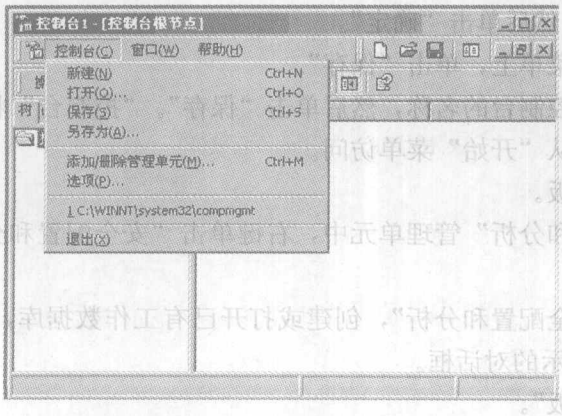


图 1-1-11　控制台菜单

添加/删除管理单元对话框如图 1－1－12 所示。

③如图 1－1－13 所示，选择“安全模板”，单击“添加”，单击“关闭”，然后单击“确定”。

图 1－1－12　添加/删除管理单元对话框

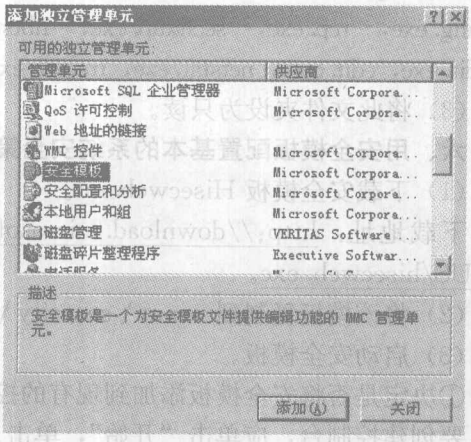


图 1－1－13　添加独立管理单元

④打开“安全模板”工具，查看这些设置。

⑤在“控制台”菜单上，单击“保存”。

⑥输入指派给此控制台的名称，然后单击“保存”。

(4) 开始安全配置和分析。

①进行以下某项操作：

要将安全配置和分析添加到新的控制台，单击“开始”，单击“运行”，然后键入“mmc”并单击“确定”。

要将安全配置和分析添加到现有的控制台，直接进行下一步操作。

②在“控制台”菜单上，单击“添加/删除管理单元”，然后单击“添加”。

③选中“安全配置和分析”，然后单击“添加”。

④单击“关闭”，然后单击“确定”。

⑤在“控制台”菜单上，单击“保存”。

⑥输入指派给此控制台的名称，然后单击“保存”。“控制台”将出现在“我的文档”中，可以在桌面上或从“开始”菜单访问。

(5) 导入安全模板。

①在“安全配置和分析”管理单元中，右键单击“安全配置和分析”。详细信息参阅相关主题。

②右键单击“安全配置和分析”，创建或打开已有工作数据库，如图 1－1－14 所示。弹出如图 1－1－15 所示的对话框。

③选中“导入模板”。

④如图 1－1－15 所示，选择模板文件，并单击“打开”。

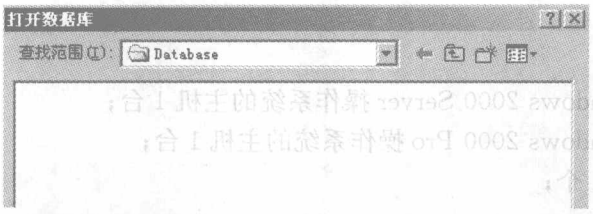


图 1－1－14　打开数据库对话框

图 1－1－15　导入模板文件

⑤对要合并到数据库的每个模板重复以前的步骤。

（6）右键单击“安全配置和分析”工具，然后从上下文菜单中选择“立即分析计算机”。等候操作完成，查看结果，如有必要就更新该模板。

（7）右键单击“安全配置和分析”工具，然后从上下文菜单中选择“立即配置计算机”。

分析与思考

（1）密码最短存留期为零的时候表示什么意思？

（2）移动部分重要文件到只有管理员能访问的目录可能带来什么不良后果？

实验 1－2　IIS 应用安全配置

实验目的

（1）掌握 Windows Internet 信息服务 IIS 的安装和基本配置。

（2）熟悉 Windows Internet 信息服务 IIS 各种选项和安全配置。

实验环境

一、设备需求

(1) 安装有 Windows 2000 Server 操作系统的主机 1 台；

(2) 安装有 Windows 2000 Pro 操作系统的主机 1 台；

(3) 普通 Hub 1 个；

(4) 网络线若干。

本实验为小组实验，每四名学生组成一个小组。每组有集线器一台、PC 机四台。每台学生用 PC 机上均安装有 Windows XP 操作系统，并安装 VMware 虚拟机软件，在虚拟机中安装 Windows 2000 Server。学生需在虚拟机的 Windows 2000 Server 上配置 IIS 服务，在 XP 下进行验证。

二、拓扑环境

本实验所需的拓扑环境如图 1−2−1 所示。

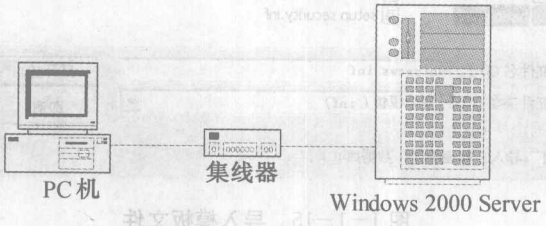


图 1−2−1　实验拓扑环境

实验内容

一、启用 IIS 服务

1. 在 Windows 2000 Server 安装 IIS

(1) 单击“开始”，指向“设置”，单击“控制面板”，然后启动“添加/删除程序”应用程序。

(2) 如图 1−2−2 所示，在左侧选择“添加/删除 Windows 组件”按钮，然后按照屏幕提示安装、删除或添加 IIS 组件。

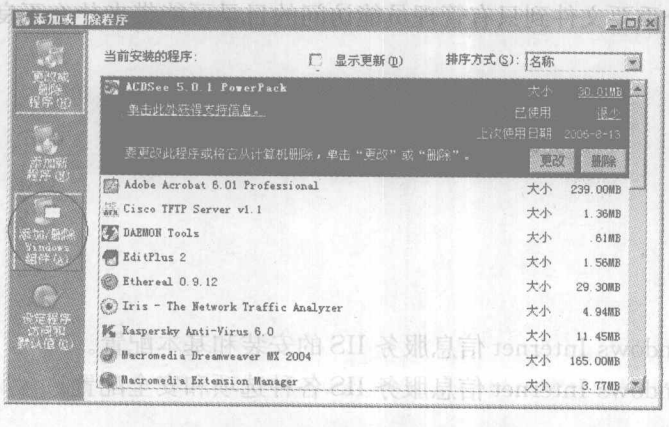


图 1−2−2　添加或删除程序对话框