可下载教学资料

http://www.tup.tsinghua.edu.cn

高等学校教材

信息管理与信息系统

计算机信息安全管理实验教程

清华大学出版社

高等学校教材

信息管理与信息系统

计算机信息安全管理实验教程

清华大学出版社

北京

内 容 简 介

本实验教材面向计算机和管理交叉类专业学生，从信息安全管理的角度出发，对信息系统整体安全体系进行分析和实验设计。书中针对技术基础和综合安全管理两个方面设计了详细实用的学习和练习手册，体现了“技术与管理”并重的信息安全观念，使得读者可以获得较为全面的专业技能，也便于教师根据课程进行选用。全书共包括5章、27个实验，涵盖了操作系统平台安全、网络安全、计算机病毒防治、应用系统安全、信息系统综合安全管理等领域。对于每个实验书中都给出了详尽的操作步骤说明和图示，容易理解和掌握。另外，还对各实验进行分析总结，便于使用者对实验举一反三，深入思考。

本书适合信息管理与信息系统、电子商务及计算机等专业学生及企业信息系统安全管理人员使用。

图书在版编目(CIP)数据

计算机信息安全管理实验教程/魏红芹编著. —北京：清华大学出版社，2010.5
(高等学校教材·信息管理与信息系统)
ISBN 978-7-302-22201-9

Ⅰ. ①计… Ⅱ. ①魏… Ⅲ. ①电子计算机－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2010)第036598号

责任编辑：闫红梅
责任校对：焦丽丽
责任印制：李红英
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 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：8.75　**字　数**：212千字
版　　次：2010年5月第1版　　**印　　次**：2010年5月第1次印刷
印　　数：1～3000
定　　价：16.00元

产品编号：035992-01

出版说明

改革开放以来，特别是党的十五大以来，我国教育事业取得了举世瞩目的辉煌成就，高等教育实现了历史性的跨越，已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上，高等教育规模取得如此快速的发展，创造了世界教育发展史上的奇迹。当前，教育工作既面临着千载难逢的良好机遇，同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾，是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月，教育部下发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》，提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月，教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件，指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分，精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间（2003—2007 年）建设 1500 门国家级精品课程，利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放，以实现优质教学资源共享，提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合新世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1) 高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 高等学校教材·电子信息——高等学校电子信息相关专业的教材。

(4) 高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5) 高等学校教材·信息管理与信息系统。

(6) 高等学校教材·财经管理与计算机应用。

清华大学出版社经过20多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

E-mail: dingl@tup.tsinghua.edu.cn

前言

计算机安全问题是伴随着计算机的发展而产生的。随着互联网的日益普及和各种信息技术在各行业得到越来越广泛的应用，整个社会对信息系统的依赖程度日益提高，安全问题也变得越来越复杂和重要。面对各种严重的计算机信息系统安全威胁，关于信息安全的研究开始得到人们的重视。目前，信息安全已经成为信息科学领域重要的研究课题，众多高等院校也相应开设了信息安全专业和课程。

在计算机信息安全的教学中，学生的实践活动是非常重要的一个环节，通过实际动手参与操作实验，学生可以更好地理解相关理论知识，增加感性认识，提高解决实际问题的能力。如何根据教学目标，针对学生的知识结构，设计出恰当的实验项目也是信息安全教学中需要解决的问题。信息安全作为一门综合性学科，课程内容覆盖面广，不同学院和专业开设的安全课程往往有不同的侧重点，对于信息系统和信息管理专业的学生来讲，在课程设计上管理和计算机技术兼重，相对而言一些底层的技术细节略有弱化，但是对于全局的把握和管理方面则要求较高。

本书从信息安全管理的角度出发，对信息系统整体安全体系进行分析和构建，突破该领域存在的“重技术，轻管理”的传统思想，有助于获得系统全面和真正的安全。书中从操作系统平台安全、网络安全、计算机病毒防治、应用系统安全、信息系统综合安全管理等方面设计了5章、27个实验。对于每个实验，在对信息安全工作人员需要具备的基本知识和技能进行总结的基础上，给出了实际的操作方案和训练途径，使读者易于理解和掌握实验的原理和实验操作方法。同时也充分考虑了实验开设的便利性，大部分实验都可以在普通的计算机和系统平台上完成，实验软件也主要选用一些易获得的免费版本。本教材中各实验相对独立，可以用于独立性信息安全实验课程，也可供相关课程在开设课内实验时进行部分选用。

本书中内容已被多次应用在东华大学管理学院信息系统和信息管理专业的计算机信息安全实验教学中，并且取得了较好的效果。本书在编写过程中，得到了东华大学管理学院姚卫新、曹海生、陈梅梅等老师的热情帮助，也得到了东华大学管理学院经济贸易实验室各位老师的大力帮助，在此表示衷心的感谢。

计算机信息安全课程在各大高校的开设时间相对较短，对于课程的教学方法和教学内容，特别是实践环节的开设方法还在不断探索之中。由于本人能力和水平所限，加上时间仓促，书中难免有错误和疏漏的地方，敬请读者批评指正。

作　者

2010 年 1 月

目 录

第1章 操作系统平台安全

1.1 实验基础

1.1.1 操作系统安全基础

操作系统作为硬件和软件应用之间接口的程序模块、计算机资源的管理者，是保证计算机系统安全的重要基础。操作系统的安全功能主要包括用户认证、存储器保护、文件与I/O设备的访问控制、对一般目标的定位与访问以及控制共享的实现、内部过程的通信与同步等。

操作系统的安全漏洞是威胁系统安全的主要原因，常见的操作系统漏洞有以下几种。

(1) I/O非法访问：操作系统(Operating System，OS)仅在I/O操作初始阶段进行访问检查，使用公共的系统缓冲区。

(2) 访问控制的混乱：安全访问与资源共享间关系处理不善，操作界限不清。

(3) 不完全的中介：完全的中介必须检查每次访问请求以进行适当的审批，不完全的中介则省略必要安全保护造成保护机制不全面。

(4) 操作系统陷门：指为后续使用和发展而预留的管理程序功能，通常对这些功能缺乏严密监控，有可能被用于安全控制。

操作系统安全的核心在于访问控制，即确保主体对客体的访问只能是授权的，且授权策略是安全的，未经授权的访问是不能进行的。进行访问控制的粒度可以是位级、字节级、字级、字段级、文件级、目录级、卷级等。受控目标级别越大，实现访问控制越容易，控制的灵活度则随之降低。

1.1.2 Windows操作系统安全技术

Windows操作系统在PC上的垄断地位，使其成为应用最为普遍的操作系统。Windows NT 4.0是系列版本中最早实现C2安全级别的操作系统，其后在对Windows NT进一步完善的基础上Microsoft公司又推出了Windows 2000等操作系统。

Windows 2000提供的安全机制包括以下几方面。

(1) 登录安全：使用三键登录界面，可以防止后台恶意程序运行，并通过输入ID和口

令实现登录，由安全帐号管理器接收 ID 和口令，安全帐号数据库验证 ID 和口令访问令牌（包括用户安全标记、用户名、用户所属组等信息）。

（2）设置登录安全：管理员可以使用域用户管理器为用户建立和修改用户属性、安全属性，并设置工作站登录限制、时间登录限制、帐号失效日期、用户登录失败次数等。

（3）文件与目录存取控制：有系统审计、允许访问、禁止访问等几种方式。禁止总是比允许的优先级高，没有设定存取控制的列表的对象采用系统默认值，并自动继承其所处目录的存取控制属性。

（4）用户权限：包括从网络上访问某台计算机、使用特定资源、进行特定操作的权限等。

（5）所有权：文件或目录有自己的拥有者，通常是其创建者。用户不能放弃自己对某对象的所有权，使拥有者对自己创建的对象负责。

（6）访问许可权：提供对文件或目录的读、写、修改、添加、列示、完全控制等访问方式。

（7）共享许可权：对网络共享资源的访问控制。

（8）审计：对可能危及系统安全的系统级属性进行逻辑评估，跟踪并报道企图对系统进行破坏的行为（与监视器和入侵检测器结合）。

（9）备份：制作系统紧急启动盘，备份系统及应用的配置数据，备份用户数据，系统工具，用户备份，第三方备份工具（磁盘备份工具等）。

Windows 默认安装通常需要进行安全化，安全化操作系统的过程称为加固，目的是减少漏洞的数量并保护计算机不受威胁或攻击。加固过程的大致步骤为：应用最新的补丁程序，禁用不必要的服务，删除不必要的用户帐户并重命名 Admin 帐户，确保使用复杂的密码，对文件和访问注册表限制许可，启用关键事件的日志，删除不必要的程序。

1.2 实验项目

1.2.1 帐户安全

1. 实验目的

了解 Windows 2000/XP 系统提供的帐户安全机制，掌握相关的安全设置方法，以提高操作系统安全强度。

2. 实验原理

帐户和口令是登录系统的基础，也是众多黑客程序攻击和窃取的对象，因此，系统的帐户和口令的安全是非常重要的。而 Windows 系统的默认设置存在一定的不安全性，这些不安全性常常被攻击者利用，通过各种手段获得合法的帐户，进一步破解口令入侵系统。通过对系统的合理设置可以避免这种安全风险。

3. 实验环境

一台安装 Windows 2000/XP 操作系统的计算机，磁盘格式设置为 NTFS。

4. 实验内容

（1）检查和删除不再使用的帐户，禁用 Guest 帐户；

(2) 启用帐户策略;

(3) 开机时设置为“不自动显示上次登录帐户”;

(4) 禁止枚举帐户名(本地策略\安全选项,选择“对匿名连接的额外限制”,在“本地策略设置”中选择“不允许枚举 SAM 帐户和共享”)。

5. 实验步骤

(1) 以管理员身份进入 Windows 2000 Server 系统,启动“程序”|“管理工具”|“计算机管理”|“系统工具”|“本地用户和组”,禁用 Guest 帐户,重命名 Administrator 帐户,对其他用户和组进行属性设置,如图 1.1 所示。

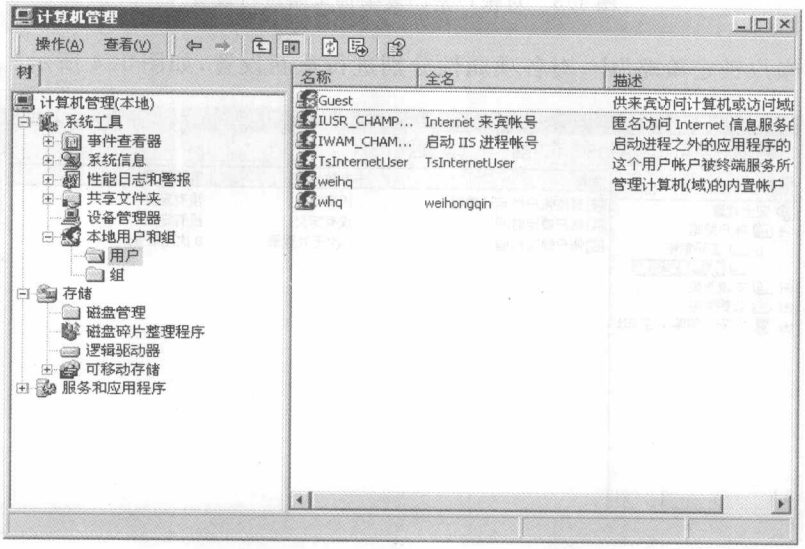

图 1.1 对计算机用户和组属性进行设置

(2) 以管理员身份进入 Windows 2000 Server 系统,启动“程序”|“管理工具”|“本地安全策略”|“帐户策略”|“密码策略”,对各项属性分别进行重新设置,如图 1.2 和图 1.3 所示。

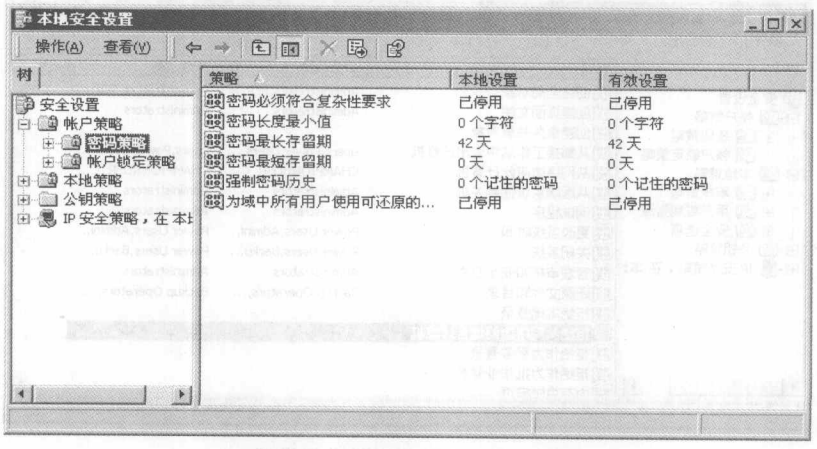

图 1.2 对帐户密码策略进行设置

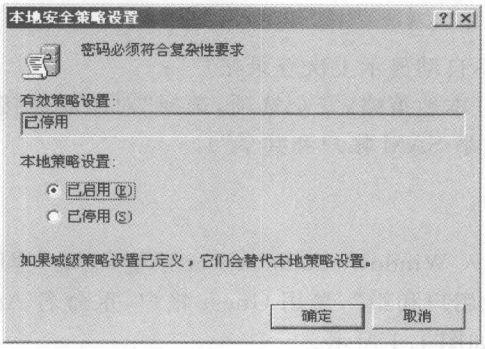

图 1.3 对帐户密码复杂性策略进行设置

(3) 在“帐户锁定策略”中，对各项属性分别进行重新设置，如图 1.4 所示。

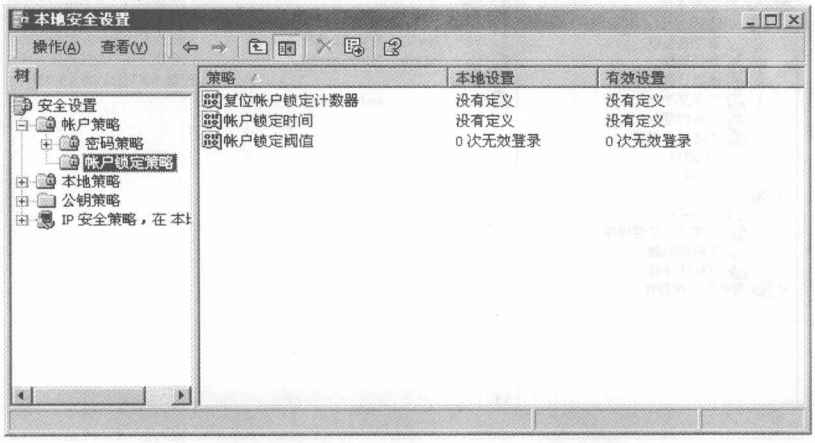

图 1.4 对帐户锁定策略进行设置

(4) 在“本地策略”|“用户权利指派”中，重新设置各权限的所属用户，如图 1.5 和图 1.6 所示。

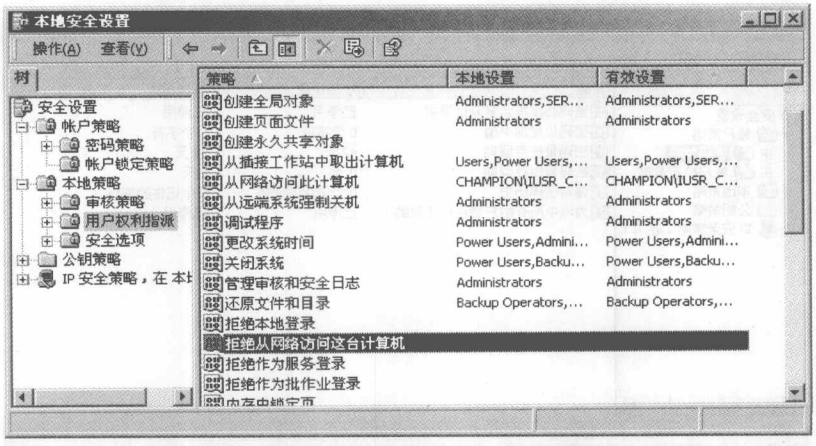

图 1.5 对用户权限进行设置

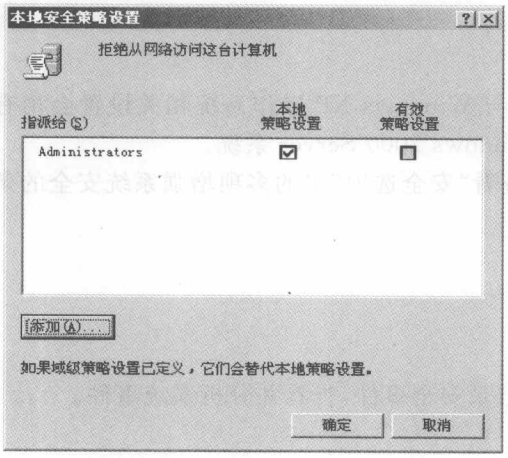

图 1.6 对用户权限策略进行设置

(5) 在“本地策略”|“安全选项”中，重新设置各安全选项，如图 1.7 所示。

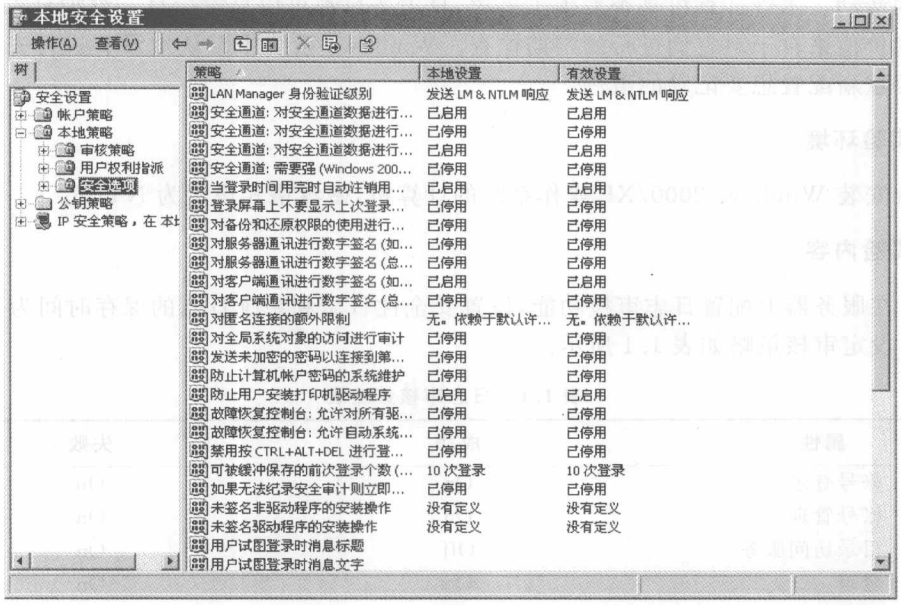

图 1.7 对帐户密码策略进行设置

6. 实验报告与要求

根据上面介绍的各项安全性实验要求，详细观察记录设置前后系统的变化，给出分析报告。

7. 实验分析与讨论

Windows 系统中提供了多种可控的安全选项，对于各选项应该如何设置最为合理，读者可以作进一步思考。

8. 注意事项

(1) Windows 2000 与 Windows XP 操作系统相关设置会稍有不同，但大同小异，以上步骤说明中采用的是 Windows 2000 Server 系统。

(2) 读者可以自行查看“安全选项”中的多项增强系统安全的条目。

1.2.2 日志与审核

1. 实验目的

配置计算机系统以记录安全事件，查看并分析系统事件。

2. 实验原理

日志是所发生事件的清单，每一个日志条目都有事件的日期和时间、事件的类别，以及在哪里可以找到有关该事件的更多信息。计算机安全事故是在系统上发生的任何非法或未经授权的活动。不管计算机是否发生了事故，日志条目都可以显露信息。维护日志很重要，但日志的价值来自于对它们进行的定期检查。Windows 系统中默认地没有进行安全审核，因此需要重新配置想要记录的事件。

3. 实验环境

一台安装 Windows 2000/XP 操作系统的计算机，磁盘格式设置为 NTFS。

4. 实验内容

(1) 在服务器上配置日志审核功能，设置安全性日志和系统日志的保存时间为 14 天。

(2) 设定审核策略如表 1.1 所示。

表 1.1 日志审核策略表

属性	成功	失败
帐号登录	On	On
帐号管理	On	On
目录访问服务	Off	On
登录	On	On
对象访问	Off	On
策略改变	On	On
特权使用	Off	On
进程跟踪	Off	Off
系统	On	On

(3) 执行一定的任务并对日志条目进行分析。

5. 实验步骤

(1) 在“管理工具”|“事件查看器”中，通过右击打开“属性”对话框进行设置，如图 1.8 和图 1.9 所示。

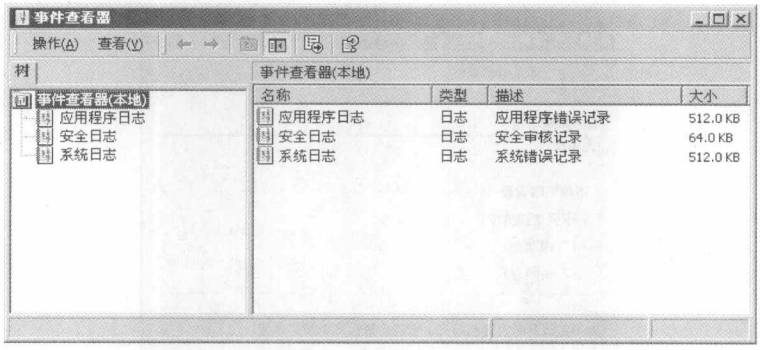

图 1.8 设置“事件查看器”属性

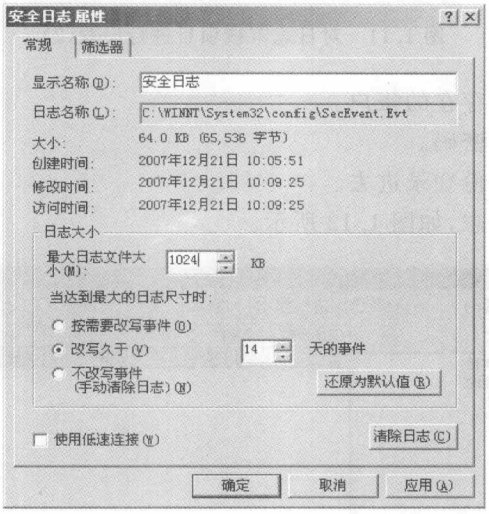

图 1.9 对“安全日志属性”进行设置

(2) 启动“程序”|“管理工具”|“本地安全策略”|“本地策略”|“审核策略”,对各审核项目开启情况分别进行重新设置,如图 1.10 和图 1.11 所示。

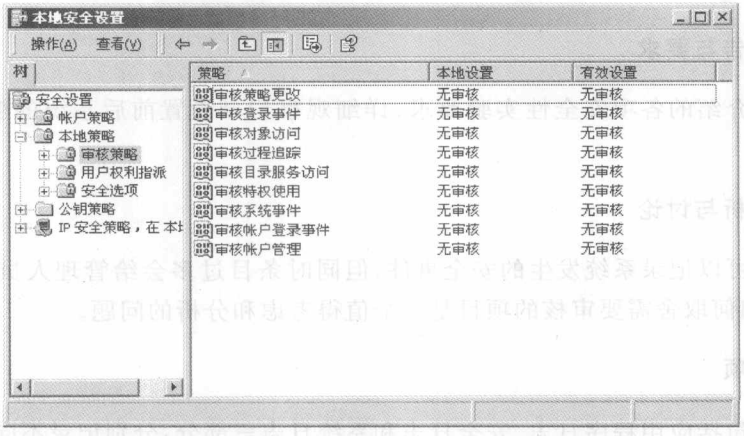

图 1.10 对日志审核项目进行设置(1)

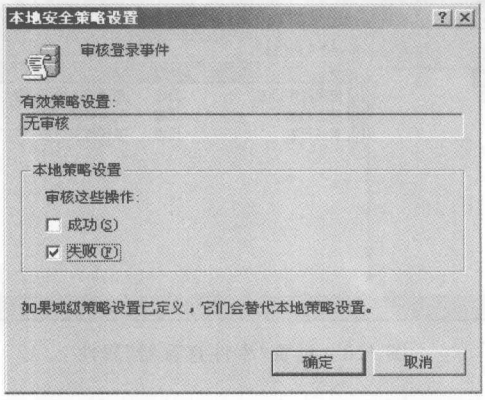

图 1.11 对日志审核项目进行设置(2)

(3) 尝试登录一个不存在的帐户。

(4) 使用一个错误的密码。

(5) 以正式用户的身份登录进去。

(6) 检查系统安全日志，如图 1.12 所示。

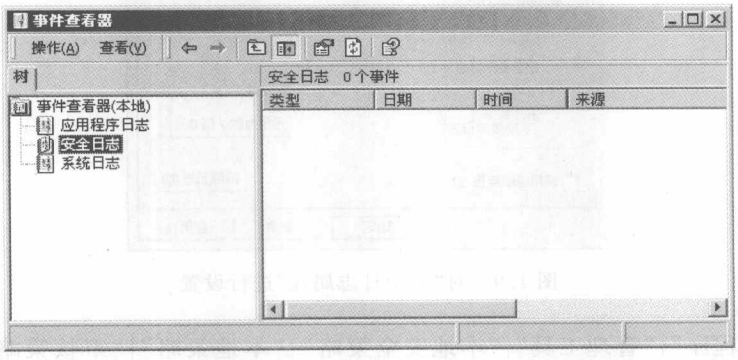

图 1.12 检查系统安全日志

6. 实验报告与要求

根据上面介绍的各项安全性实验要求，详细观察记录设置前后系统的变化，给出分析报告。

7. 实验分析与讨论

安全日志可以记录系统发生的安全事件，但同时条目过多会给管理人员带来过多的工作负担，因此如何取舍需要审核的项目是一个值得考虑和分析的问题。

8. 注意事项

系统日志包括应用程序日志、安全日志和系统日志三部分，分别记录不同类型的系统事