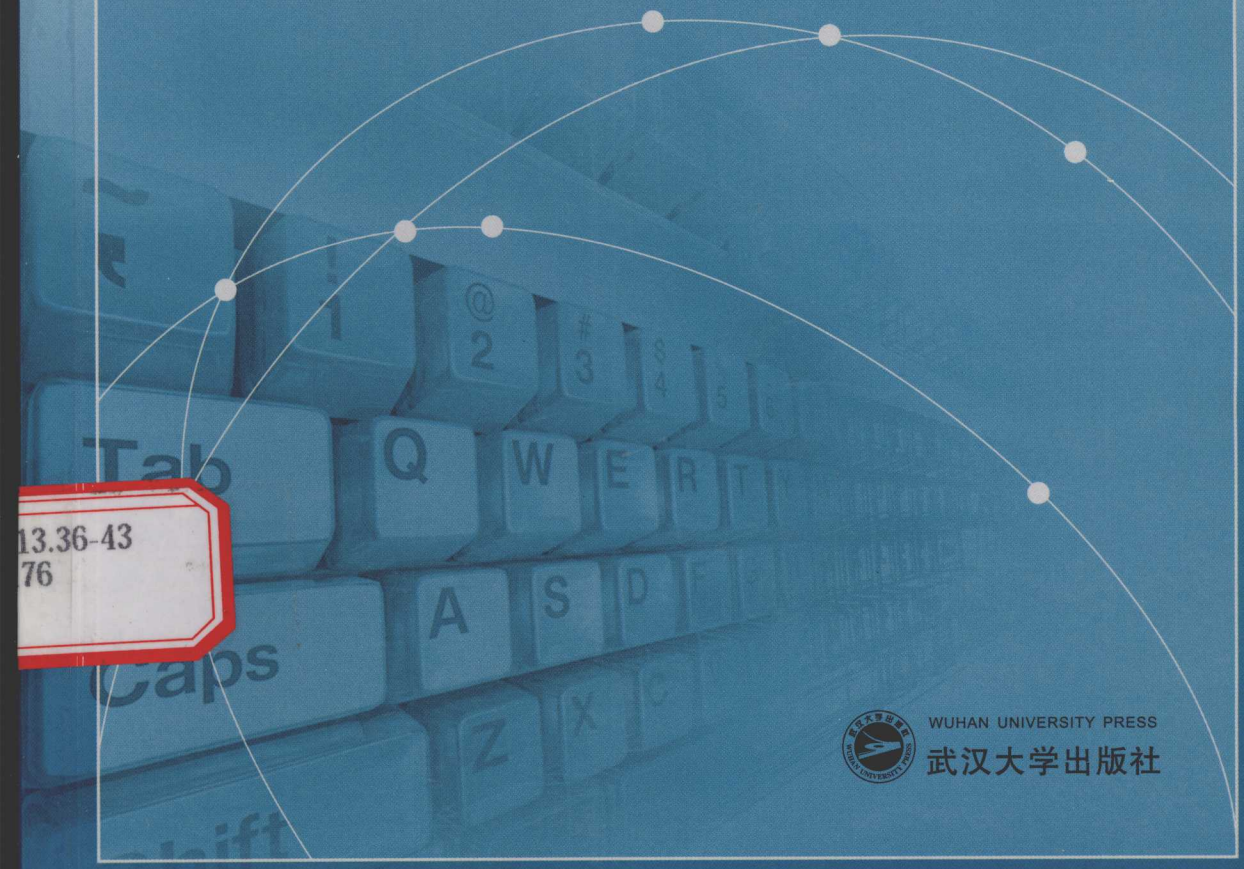
图书情报与信息管理实验教材

电子商务安全基础实验教程

AN EXPERIMENTAL INSTRUCTION TO E-COMMERCE SECURITY

曾子明 编著



WUHAN UNIVERSITY PRESS
武汉大学出版社

图书情报与信息管理实验教材

电子商务安全基础实验教程

AN EXPERIMENTAL INSTRUCTION TO E-COMMERCE SECURITY

曾子明　编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

电子商务安全基础实验教程/曾子明编著. —武汉：武汉大学出版社，2008.6
图书情报与信息管理实验教材
ISBN 978-7-307-06252-8

Ⅰ.电… Ⅱ.曾… Ⅲ.电子商务—安全技术—高等学校—教材 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2008)第 067893 号

责任编辑：辛 凯 责任校对：刘 欣 版式设计：马 佳

出版发行：武汉大学出版社 (430072 武昌 珞珈山)
(电子邮件：wdp4@whu.edu.cn 网址：www.wdp.com.cn)
印刷：湖北恒泰印务有限公司
开本：720×1000 1/16 印张：9.75 字数：190 千字 插页：1
版次：2008 年 6 月第 1 版 2008 年 6 月第 1 次印刷
ISBN 978-7-307-06252-8/F·1156 定价：16.00 元

内容提要

本书是“电子商务安全”等电子商务专业核心课程的配套实验教材，通过实际操作，使学生对电子商务安全原理和应用有较深刻的认识。内容分为8个方面：Windows操作系统安全、Windows中Web服务器的安全配置、常用网络工具与电子邮箱的使用、数字证书的申请与认证、PGP的安全加密机制、网上银行与安全电子支付、电子商务安全系统设计、电子商务安全案例及分析。本书具有较强的操作指导性，紧密联系实际，并附有相关理论知识介绍。学生可以通过熟练掌握实际的操作技能，从而产生对电子商务安全技术的浓厚兴趣。全书强调系统性、前沿性，取材先进、科学，内容丰富、实用，图文并茂，可读性强。

作为实验教材，本书适合作为高等院校电子商务、信息安全、计算机应用和金融等专业的本科生实验教学参考书，也可以作为电子商务安全技术培训教材，同时还可供从事电子商务安全系统研究、设计、开发的工程技术人员和管理人员参考。

前 言

电子商务是在国际化、社会化、开放化和个性化的 Internet 环境中运作的，它的应用可能会出现各种商业信息的泄露、客户的银行账户信息被盗、金融欺诈，以及缺乏可信性而导致的商业丢失等各种安全与信任问题。因此，要在 Internet 这样开放的网络平台上成功地进行电子交易，必须有效解决操作系统和网络平台的安全，以及提供对电子数据传输过程的保护。因此，电子商务安全问题是目前困扰和影响电子商务应用和推广的重要问题。

目前，不少高等院校已开设了包括“电子商务安全”在内的电子商务系列课程，这在一定程度上适应了电子商务安全的发展。但是，“电子商务安全”相关的教材虽多，但与之配套的用于实验课程的教材却几乎没有。为了满足“电子商务安全”相关课程的实验教学，作者特编写了本教材，以实现实验教学资源的共享。

在编写实验教材的过程中，作者始终做到：内容尽可能与理论教材相匹配，体系尽可能完整；尽可能适应不同学校的实验教学环境与实验教学组织；按照操作系统与 Web 服务器安全实验、数字证书与 CA 认证、PGP 安全加密机制、网上银行与安全电子支付、电子商务安全系统设计、电子商务安全案例及分析等主要内容组织实验项目，以适应不同层次的学生及相关人员的学习要求。

具体来说，本实验教材具有以下两点特色：

（1）选材新颖，联系实际。本教材努力做到“三新”，即体系新、内容新、方法新，既传授基础知识又引导实验操作技能的提高，通过教材的实验指导提高学生的动手能力，体现素质教育的思想，这是作者在实验教材编写过程中特别下气力的地方。

（2）强调实验教学的规律，注重学生创新能力的培养。本教材着力包括电子商务网络与支付安全相关的实验内容，遵循实验教学的规律，精选了部分与安全应用密切相关的实验作为实验教学案例，既调动了读者的学习积极性，又使得学与用密切结合，增强了读者运用所学知识和创新能力的培养。

本实验教材在编写过程中参考了众多文献，已在参考文献中尽可能地列出，作者对这些文献的著作权人表示衷心的感谢。同时，感谢信息管理学院副院长方卿教授对本书出版的关怀和鼎力支持；感谢电子商务系系主任张李义教授和全体

同事对本书编写过程中所给予的许多有益建议和指导。另外，本书的顺利出版得到武汉大学出版社的大力支持，在此深表谢意！

电子商务安全理论与技术都处在快速发展之中，本实验教程的不足甚至错误之处在所难免，真诚希望有关专家和读者批评指正，以期不断改进。

作　者

2008 年 4 月

目 录

1 Windows操作系统安全

1.1 操作系统安全概述

电子商务是一种基于网络的商务活动。网络是由各个不同的计算机系统组成的，而每个计算机系统的核心是操作系统。所以，计算机操作系统的安全是网络安全的基础，因而也是电子商务安全的一个重要组成部分。

操作系统作为计算机系统的基础软件是用来管理计算机资源的，它直接利用计算机硬件并为用户提供使用和编程接口。各种应用软件均建立在操作系统提供的系统软件平台之上，上层的应用软件要想获得运行的高可靠性和信息的完整性、保密性，必须依赖于操作系统提供的系统软件基础，任何想象中的、脱离操作系统的应用软件的高安全性，就如同幻想在沙滩上建立堡垒一样，毫无根基可言。不难想象，在网络环境中，网络系统的安全性依赖于网络中各主机系统的安全性，而主机系统的安全性正是由其操作系统的安全性所决定的，没有安全的操作系统的支持，网络安全也毫无根基可言。所以，操作系统安全是计算机网络系统安全的基础。

在安全层次模型中，操作系统的安全性属于系统级安全的范畴。操作系统为文件、目录、网络等提供底层的安全保障平台。操作系统中的安全缺陷和安全漏洞，往往会造成严重的后果。因此，安全机制是操作系统的一个重要组成部分；另外，操作系统的安全级别是对其性能进行评估的一个重要指标。本节首先简述操作系统的安全机制，然后介绍一下操作系统安全级别的划分。

1.1.1 操作系统安全机制

操作系统的安全机制主要体现在以下几个方面：

1. 身份认证

身份认证是证明某人或某个对象身份的过程，是保证系统安全的重要措施。身份认证必须强有力，即在用户登录时，与系统的交互过程必须有安全保护，不会被第三方干扰或截获。身份认证是操作系统中实现用户安全管理的重点，通常采用账号/密码的方案。用户提供正确的账号和密码后，系统才能确认和标识他的合法身份。不同的操作系统内部采用的认证机制和过程一般是不同的。Unix

系统的用户身份认证采用账号/口令的方案。当用户提供正确的账号和口令后，系统才能确认他的合法身份。而 Windows 系统则使用 Kerberos 协议作为用户身份认证的主要方法。Kerberos 协议提供在客户机和应用服务器之间建立连接之前的相互身份认证的机制。另外，Windows 操作系统支持 PKI，通过颁发 PKI 证书以提供用户身份确认和授权等安全机制。

2. 访问控制

访问控制是实现操作系统安全的一个重要方面，它是在身份认证的基础上，根据用户身份对其提出的资源访问请求加以控制。在访问控制中，对用户访问必须进行控制的资源称为客体，客体包括文件、程序或设备等。而用户则为对客体资源进行访问的主体，即访问的发起者。访问控制实质上是对客体资源使用的限制，它决定主体是否被授权对客体执行某种操作。当用户访问系统资源或执行程序时，系统应该首先进行合法性检查，没有得到授权的用户访问或执行请求将被拒绝。系统还要对访问或执行的过程进行监控，防止用户越权。常用的访问控制包括两种：

（1）自主访问控制（DAC）。在这种访问控制中，由资源拥有者分配资源访问权限，在辨别各用户的基础上实现访问控制。每个用户的访问权限由资源的拥有者来建立，常以访问控制表或权限表来实现。该方法灵活，便于用户访问数据资源，在安全性要求不高的用户之间共享一般数据资源时可采用。

（2）强制访问控制（MAC）。在这种访问控制中，资源的访问权限不能由其拥有者确定，而是由系统管理员来分配访问权限和实施控制。该机制比自主访问控制更为严格，其安全性更强，易于实现在所有用户和资源中实施强化的安全策略，因而受到重视。

3. 最小权限原则

每个用户和进程仅应拥有最小访问权的集合，仅能在为完成其任务所必须的那些权限所组成的最小保护域内执行。例如，将超级用户的特权划分为一组较小的特权集合，将集合中的元素分别给予不同的系统管理员，使各种系统管理员仅具有完成其任务所需的特权，从而将由于特权用户口令丢失或缺陷软件、恶意软件以及误操作引起的损失限制在最低程度。这是一项保证系统安全性的重要策略，也是抑制特洛伊木马和实现可靠程序的基本措施。

4. 安全审计

安全审计对系统中有关安全的活动进行记录、检查及审核。其主要目的是检测和阻止非法用户对计算机系统的入侵，并对合法用户的误操作进行显示。一般情况下，审计作为一种事后追查的手段以保证系统的安全性。

5. 可信信道机制

在计算机系统中，用户通过不可信的中间应用层和操作系统相互作用。操作

系统必须提供一条能够保证用户在与安全核心通信时不会被特洛伊木马截获通信信息的可信信道。

6. 隐蔽信道

隐蔽信道指不被设计者或用户所知道的泄露系统内部信息的信道。系统设计时要进行隐蔽信道分析，采取一些措施在一定程度上消除或限制隐蔽信道。

1.1.2 操作系统安全等级的划分

1985 年，美国国防部提出可信计算机系统评测标准 TCSEC（习惯上称橘皮书），为计算机安全产品的评测提供了测试准则和方法。TCSEC 将计算机系统的安全可信性分为 7 个级别：D 最低安全性，C1 自主存取控制，C2 较完善的自主访问控制（DAC）、审计，B1 强制访问控制（MAC），B2 良好的机构化设计、形式化安全模型，B3 全面的访问控制、可信恢复，A1 形式化认证。

（1）D 级是计算机安全的最低层，对整个计算机的安全是不可信任的，例如 MS-DOS 就属于 D 级操作系统。

（2）C1 级要求系统硬件有一定的安全保护，用户使用前必须在系统中注册。但是，C1 级不能控制进入系统的用户的访问权限，所以用户可以控制系统配置，甚至获取比系统管理员更高的权限，例如改变和控制用户名。

（3）C2 级针对 C1 级的不足进行了改进，例如增加用户权限级别，采用了系统的安全审计机制，例如 Windows 2000、Windows NT 4.0 和 Solaris 等。

（4）B1 级也称为带标签的安全性保护，对敏感信息提供更高的保护。任何对用户许可级别和成员分类的更改都受到严格控制。就 TCSEC 评估来说，达到 B1 级及以上标准的操作系统即称为安全操作系统，例如 IBM 大型机的 MVS 操作系统。

（5）B2 级要求对计算机系统所有的对象加标签，把信息划分成单元，而且给不同的硬件设备分配相应的安全级别。

（6）B3 级又称安全域级，要求用户工作站或终端通过可信任途径链接网络系统，并使用硬件保护安全系统的存储区。

（7）A1 级为最高安全级，要求系统设计必须是从数学上经过验证的，而且必须进行隐蔽通道和可信任分布的分析，并且要求用形式化技术解决隐蔽通道等问题。目前，波音公司的 MLSLAN 安全网络服务器已经通过 A1 级评测。

当前主流的操作系统安全性远远不够，如 Unix 系统，Windows 2000 都只能达到 C2 级，安全性均有待提高。

因此，为了确保电子商务系统的安全，对操作系统进行安全设置显得尤为重要。下面以 Windows 为例，对提高操作系统安全的策略进行介绍。

1.2 Windows 操作系统的安全策略

Windows 操作系统具有良好的网络功能，以及多用户的特点，但也存在不少漏洞。它的一些基本安全策略对系统的安全比较实用。

1. 设置密码

系统用户密码对于操作系统的安全非常重要。如果是超级用户，没有设置密码而系统又存在漏洞，那么攻击者和病毒就很容易入侵并操纵这台机器，任意删除或者修改文件，则该系统就完全失去了防守能力。

2. 利用 NTFS 文件系统的安全性

Windows 操作系统中，设置系统文件格式为 NTFS，并选择必须的系统组件和服务。NTFS 文件系统可以将每个用户允许读写的文件限制在磁盘目录下的任何一个文件夹内，而磁盘限额服务可以控制每个用户允许使用的次磁盘空间的大小。

3. 对重要信息加密

为防止其他人在使用自己的计算机时，偷看自己存储在计算机中的文件信息，Windows 操作系统为普通用户提供了“文件和文件夹加密”功能，利用该功能可以对存储在计算机中的重要信息进行加密。其他用户在没有密码的情况下，无法访问文件或者文件夹中的内容。

4. 启用审核与日志功能

为了加强 Windows 系统的安全性，还需启用审核与日志功能来监控系统的运行情况。当有黑客尝试对系统进行攻击时，都会被安全审核功能记录下来，并写入到日志文件中。但黑客在攻击系统时为了不留下痕迹，一般会通过修改系统的日志系统来隐藏对自己不利的日志文件。所以必须限制对日志文件的访问，禁止一般权限的用户查看日志文件。

5. 利用安全模板

安全模板是一种可以定义安全策略的文件表示方式，它能够配置账户和本地策略、事件日志、受限组、文件系统、注册表以及系统服务等项目的安全设置。安全模板都以后缀名为 .inf 格式的文本文件存在，用户可以方便地复制、粘贴、导入或导出某些模板。在 Windows 系统中，系统管理员利用安全模板就能快速、批量地设定所有安全选项。

6. 使用 IPSec 策略

IPSec（Internet Protocol Security）是 Windows 操作系统中新提供的一种安全技术，它是一种基于点到点的安全模型，可以实现更高层次的局域网数据安全性。在网络上传输数据的时候，通过使用 IPSec 策略，利用点到点的安全模型，能够安全有效地把原计算机的数据传输到目标计算机。IPSec 提供身份验证、完

整性和可选择的机密性，利用 IPSec 可以使得系统的安全性能大大增强。

7. 屏蔽不必要的服务。

为了方便用户，Windows 默认启用了许多不一定要用到的服务，但同时也打开了入侵系统的后门。通过网络资源，我们可以找到完备的 Windows 系统服务详细功能说明。根据自己系统的需要，应将那些无需使用和有危险性的服务进行屏蔽。

8. 使用杀毒软件

除了进行上述的系统安全配置外，为 Windows 安装一款优秀的杀毒软件和木马查杀软件也是必要的，同时一定要注意及时更新病毒库，保证对最新的病毒和木马的查杀能力。

1.3 实验目的与要求

(1) 理解操作系统安全对电子商务系统安全的重要性。

(2) 熟悉操作系统的安全机制，以及 Windows 的安全策略。

(3) 掌握对 Windows 操作系统进行安全配置的基本方法和步骤，并能根据实际应用需求构建一个 Windows 操作系统的基本安全框架。

1.4 实验环境

实验设备：PC 机及其局域网；具备 Internet 连接。

软件环境：Windows XP 操作系统，磁盘格式为 NTFS。

1.5 实验内容与操作步骤

下面主要以 Windows XP 为例，介绍 Windows 操作系统的安全配置过程。

1.5.1 账户和密码的安全设置

1. 删除不再使用的账户，禁用 Guest 账户

共享的账户越多，被黑客攻击的几率也越大。特别是 Guest 账户，它是一个非常危险的安全漏洞，常常成为攻击的对象，因为黑客可以使用这个账户登录合法用户的机器。因此，要求删除不再使用的账户，并且建议将 Guest 账户进行禁用。

(1) 检查和删除不再使用的账户。单击“开始”按钮，依次选择“控制面板”→“管理工具”→“计算机管理”，打开“计算机管理”窗口。在该窗口中选中“本地用户和组”选项，然后单击“用户”项，如图 1-1 所示。

在“计算机管理”窗口中列出了系统所有的账户。检查各账户是否仍需使用，删除其中不再使用的账户。

(2) 禁用 Guest 账户。右键单击 Guest 账户，选择“属性”，在弹出的

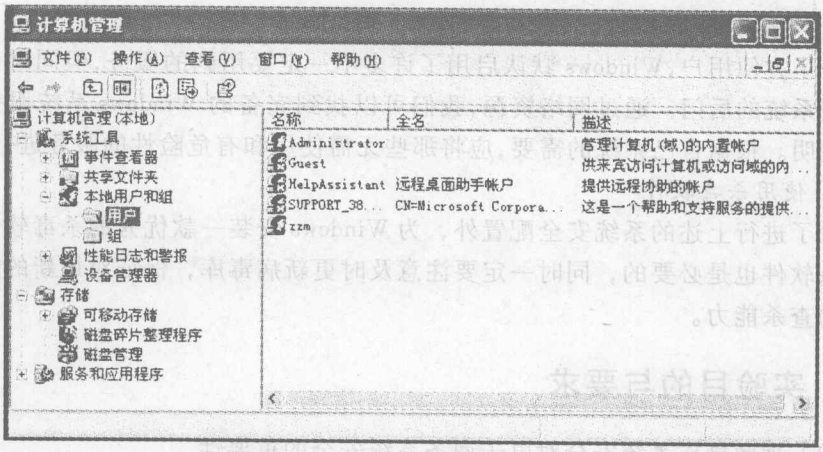


图 1-1　计算机管理窗口

“Guest 属性”对话框中将“账户已停用”一栏前打勾，如图 1-2 所示。这样就无法使用该账号登录系统了。

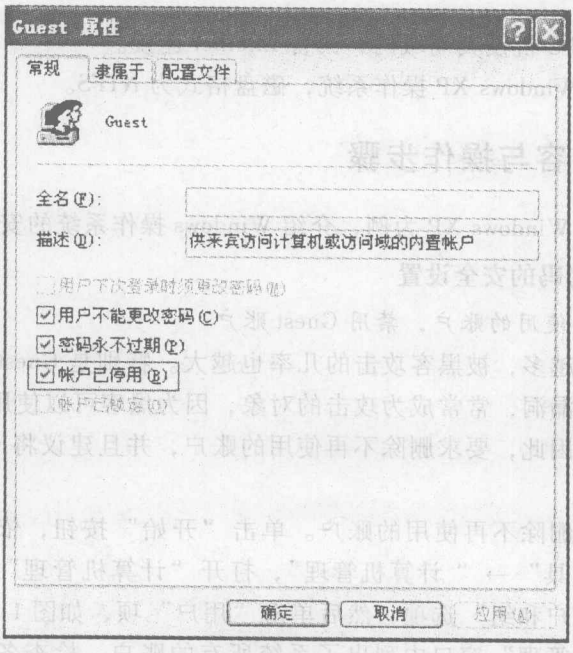


图 1-2　禁用 Guest 账户

2. 启用账户策略

账户策略是 Windows XP 账户管理的重要安全工具，它可以增加攻击者登录系统的难度。

(1) 依次打开“控制面板”→“管理工具”→“本地安全策略”。在弹出的“本地安全设置”窗口中，选择“账户策略”中的“密码策略”，如图 1-3 所示。

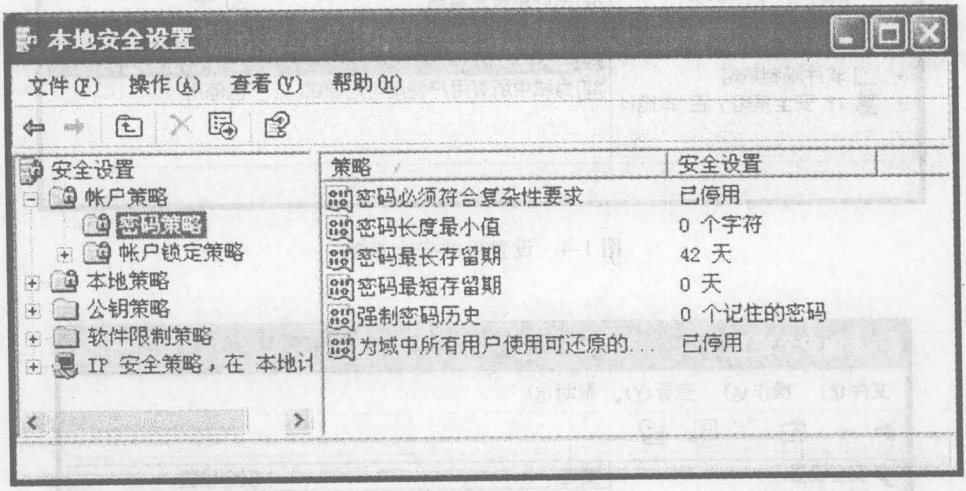


图 1-3 系统默认的密码策略

密码策略用于决定系统密码的安全规则。例如，启用“密码必须符合复杂性要求”策略选项，以确保用户使用的口令符合安全性要求，不会很容易被攻击者破解；设置“密码长度最小值”为 8 位；设置“密码最长存留期”为 30 天；设置“密码最短存留期”为 5 天；设置“强制密码历史”为 3 个记住的密码。密码设置完成后，如图 1-4 所示。

(2) 账户策略中的第 2 项是账户锁定策略，它决定系统锁定账户的时间等相关设置。选中“账户策略”下的“账户锁定策略”，如图 1-5 所示。

其中，有三个设置选项。首先设置“账户锁定阈值”，该值定义了用户在进行多少次无效登录后自动锁定账户，设置这个阈值能从根本上抵御入侵者对用户密码的暴力猜测，推荐值为 3 次。然后，设置“复位账户锁定计数器”，该值定义了在账户被锁定后多长时间可被系统复位为零，推荐值为 3 分钟。最后，设置“账户锁定时间”，该值设置当用户的账户被锁定后，多长时间才能重新使用，推荐值为 10 分钟。