普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

网络攻击与防御技术实验教程

张玉清 陈深龙 杨彬 编著

http://www.tup.com.cn

Information Security

根据教育部高等学校信息安全类专业教学指导委员会制订的《信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

网络攻击与防御技术实验教程

根据教育部高等学校信息安全类专业教学指导委员会制订的
《信息安全专业指导性专业规范》组织编写

清华大学出版社
北京

内 容 简 介

网络攻击与防御技术是网络安全的核心和焦点，也是确保网络安全实际动手能力的综合体现。全书共分 11 章，第 1 章介绍如何进行系统安全配置并搭建一个用于网络攻防实验的虚拟机，在接下来的各章中，在回顾理论知识的同时，结合动手实验介绍网络典型攻防技术，这些网络典型攻防技术包括扫描技术、网络监听及防御技术、口令攻击、欺骗攻击及防御、拒绝服务攻击与防范、缓冲区溢出攻击及防御、Web 攻击及防范、木马攻击及防御、病毒与蠕虫攻击及防御和典型网络攻击防御技术。通过这种理论与实践相结合的网络攻防技术的学习，读者会对网络攻击与防御技术有更直观和深刻的理解。

书中各章内容安排方式为：理论知识回顾、基本实验指导和巩固提高型实验。

本书可以作为信息安全、计算机、通信等相关专业研究生、本科生的教材，也可供从事网络安全研发的工程技术人员和热衷网络攻防技术的读者参考。

图书在版编目（CIP）数据

网络攻击与防御技术实验教程 / 张玉清，陈深龙，杨彬编著. —北京：清华大学出版社，2010.7
（高等院校信息安全专业系列教材）
ISBN 978-7-302-19435-4

Ⅰ. ①网… Ⅱ. ①张… ②陈… ③杨… Ⅲ. ①计算机网络－安全技术－高等学校－教学参考资料 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 015842 号

责任编辑：张　民　王冰飞
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：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×260　　**印　张**：8.75　　**字　数**：203 千字
版　　次：2010 年 7 月第 1 版　　**印　次**：2010 年 7 月第 1 次印刷
印　　数：1～3000
定　　价：17.00 元

产品编号：032207-01

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点如下：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断修订和完善。

我们的E-mail地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

前言

“知彼知己，百战不殆。”

——孙子兵法

网络安全已成为人们在信息空间中生存与发展的重要保证条件，与国家的政治安全、经济安全、军事安全、社会稳定以及人们的日常生活密切相关。由于兴趣爱好和经济利益的驱使，黑客攻击事件层出不穷。公司和国家只有积极防御，才能在攻击环境下生存。

攻击与防御是一对相互制约和相互发展的网络安全技术。

本实验教程的目标是帮助安全人员理解黑客的攻击方法和步骤，事实一次又一次地证明，理解敌人的策略、技巧和工具对保护自己是多么的重要。同时，本教程还让安全人员了解能采取哪些策略来防范各类攻击。

本书可作为《网络攻击与防御技术》的配套实验教程，同时又可自成体系，更注重攻防的实战性。读者可以通过阅读该教程并动手实践达到提高网络安全技术的目的。

内容安排

第 1 章：讲解安全技术的基本实验，包括 Windows 账户和密码策略的设置、IIS 和 Apache 安装与配置以及虚拟机软件 VMWare 的使用。

第 2 章：讲解扫描技术，包括主机端口扫描和网络漏洞扫描。

第 3 章：讲解网络监听与防御技术，包括监听原理介绍、WinPcap 介绍和 Sniffer 工具的使用。

第 4 章：讲解口令攻击技术，包括 UNIX 和 Windows 系统口令攻击技术的介绍、口令破解工具介绍。

第 5 章：讲解欺骗攻击及防御技术，欺骗攻击包括目前流行的 IP 欺骗和 ARP 欺骗。

第 6 章：讲解拒绝服务攻击与防范技术，包括 DoS/DDoS 攻击的原理、检测与防范，另外，还介绍了 UDP Flood 工具的使用方法。

第 7 章：讲解危害非常大的缓冲区溢出攻击，其中介绍了基本原理、攻击步骤、防范方法；同时还向读者介绍了一个非常典型的缓冲区溢出攻击实例。

第 8 章：讲解近几年网络攻击的热点——Web 攻击及防范，该章用实例介绍了流行的 SQL 注入攻击和 XSS 攻击。

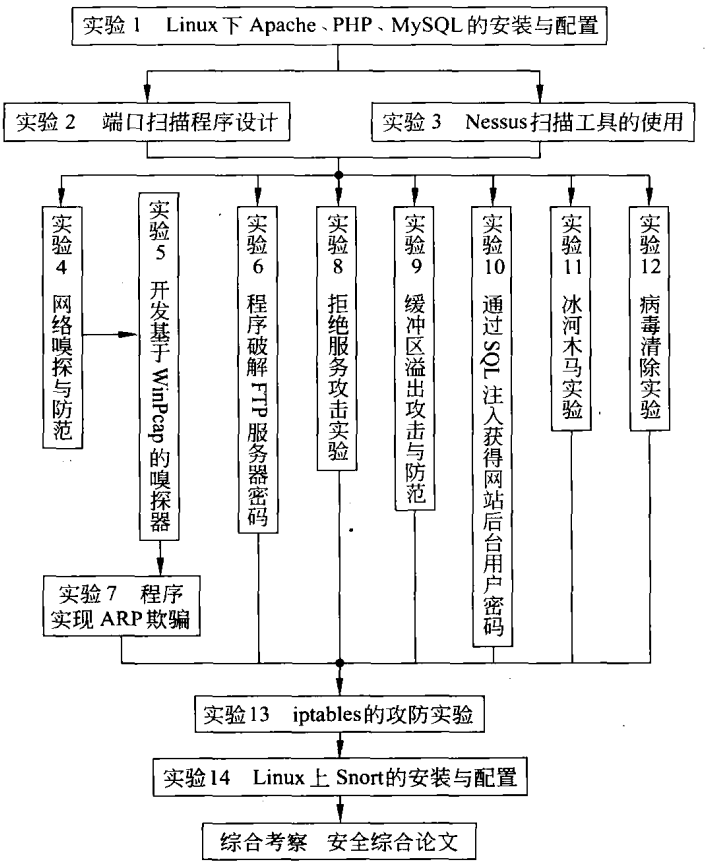
第 9 章：讲解了备受关注的木马攻击及防御，包括木马的自启动技术、隐藏技术，并用翔实的图文展示了冰河木马，最后介绍木马的防范。

第 10 章：讲解病毒和蠕虫攻击及防御，包括病毒和蠕虫的原理、防范方法，并具体介绍了冲击波病毒的特征、清除方法。

第 11 章：讲解典型的网络攻击防御技术，包括防火墙和入侵检测系统，实例包括天网防火墙的配置、Windows 上 Snort 的安装与配置。

实验安排

本书依据各章内容，总共设计了 14 个实验和一个综合考察。读者可以根据兴趣点和自身情况选取相应的实验重点实践。根据攻击的先后步骤和技术关联性，本书的实验先后顺序和相互关系如下图所示。



其中，实验 5、9、14 是我们极力推荐的实验，我们的教学实践证明这 3 个实验是网络攻防的典型实践，这当中有了解网络 TCP/IP 协议知识以及网络数据传输过程的实验（实验 5），有主动攻击实验（实验 9），也有典型防御实验（实验 14），这些实验可以让读者从攻与防两个角度综合理解和有效掌握网络安全技术，从而达到攻防兼备的效果。所有《网络攻击与防御技术》课程教学最好能至少安排这 3 个实验。

其余实验可以根据本课的课时安排和读者兴趣爱好选择。

必须具备的基础知识

- 读者应熟悉 C 语言，懂得C++ 语言的基础知识。
- 读者应具备计算机网络知识，了解 TCP/IP 协议。

关于源程序

本书配有各章所需要的文件、安全程序和代码，同时还对较难的实验进行了解答，读者可以参考这些解答来完成相应的实验。所有配套素材可以从清华大学出版社网站(www. tup. com. cn)下载。本书的所有例子已经在相应的实验环境下测试通过。因为素材中有些文件具有一定的攻击性，如果不做任何处理会被杀毒软件查杀，因此设置了密码进行压缩，解压密码为 ncnipc。

关于读者反馈

由于作者时间和能力有限，加之攻防技术发展迅速，书中难以做到尽善尽美。如果发现书中的任何问题或者有改进意见，请发 E-mail 至：zhangyq@nipc. org. cn，以便在下一版中改进。你们宝贵的意见和建议是我们前进的动力，谢谢！

作 者

2010年7月

目录

第 1 章　基本实验 …… 1

1.1　Windows 账户和密码的安全设置 …… 1

1.2　IIS 的安装与安全配置 …… 5

1.2.1　IIS 的安装 …… 5

1.2.2　IIS 的安全设置 …… 6

1.3　Linux 下 Apache 的安装与配置 …… 8

1.4　虚拟机软件 VMWare …… 8

实验 1　Linux 下 Apache、PHP 和 MySQL 的安装与配置 …… 11

第 2 章　扫描技术 …… 12

2.1　扫描技术概述 …… 12

2.2　主机端口扫描技术 …… 12

2.2.1　主机端口扫描原理 …… 12

2.2.2　Nmap 扫描工具 …… 14

实验 2　端口扫描程序设计 …… 18

2.3　网络漏洞扫描技术 …… 19

2.3.1　网络漏洞扫描原理 …… 19

2.3.2　Nessus 扫描工具 …… 20

实验 3　Nessus 扫描工具的使用 …… 22

第 3 章　网络监听及防御技术 …… 23

3.1　网络监听技术 …… 23

3.1.1　网络嗅探器工作原理 …… 23

3.1.2　网络监听的防范 …… 24

3.2　Ethereal 工具的使用 …… 24

3.2.1　Capture 选项 …… 25

3.2.2　Ethereal 的抓包过滤器 …… 26

3.2.3　Ethereal 的显示过滤器 …… 27

实验 4　网络嗅探与防范 …… 27
3.3　WinPcap 介绍 …… 28
3.3.1　WinPcap 简介 …… 28
3.3.2　WinPcap 组件 …… 29
3.3.3　WinPcap 安装与使用 …… 30
3.3.4　开发基于 WinPcap 嗅探程序的步骤 …… 31
实验 5　开发基于 WinPcap 的嗅探器 …… 31

第 4 章　口令攻击 …… 33
4.1　口令破解技术 …… 33
4.1.1　口令破解的基本方法 …… 33
4.1.2　UNIX 系统的口令攻击 …… 34
4.1.3　Windows 系统的口令攻击 …… 34
4.1.4　网络服务口令攻击 …… 35
4.1.5　口令安全性增强对策 …… 36
4.2　口令破解工具 …… 36
4.2.1　Password Crackers …… 36
4.2.2　L0phtCrack …… 36
4.2.3　John the Ripper …… 37
4.2.4　工具运用实例 …… 37
实验 6　程序破解 FTP 服务器密码 …… 40

第 5 章　欺骗攻击及防御技术 …… 41
5.1　欺骗攻击原理 …… 41
5.2　IP 欺骗 …… 41
5.2.1　IP 欺骗中信任关系的建立 …… 41
5.2.2　IP 欺骗攻击关键问题及过程 …… 42
5.2.3　IP 欺骗的防范 …… 43
5.3　ARP 欺骗 …… 44
5.3.1　ARP 协议 …… 44
5.3.2　ARP 欺骗原理 …… 45
5.3.3　ARP 欺骗攻击实例 …… 47
5.3.4　ARP 欺骗的防范 …… 50
实验 7　程序实现 ARP 欺骗 …… 50

第 6 章　拒绝服务攻击与防范 …… 51
6.1　拒绝服务攻击原理 …… 51
6.2　分布式拒绝服务攻击原理 …… 53

6.3 UDP Flood 工具的使用 …… 54
6.4 DoS/DDoS 攻击的检测与防范 …… 56
实验 8 拒绝服务攻击实验 …… 57

第 7 章 缓冲区溢出攻击及防御技术 …… 58
7.1 缓冲区溢出原理 …… 58
7.1.1 栈溢出 …… 58
7.1.2 堆溢出 …… 59
7.2 缓冲区溢出攻击 …… 60
7.2.1 定位溢出点的位置 …… 61
7.2.2 构造 shellcode …… 61
7.2.3 缓冲区溢出利用技术 …… 61
7.3 缓冲区溢出的防范 …… 62
7.3.1 软件开发阶段 …… 63
7.3.2 编译检查阶段 …… 63
7.3.3 安全配置使用阶段 …… 64
7.4 CCProxy 缓冲区溢出攻击实例 …… 64
7.4.1 漏洞说明 …… 64
7.4.2 漏洞检测 …… 65
7.4.3 漏洞分析与利用 …… 66
7.4.4 漏洞利用程序的实现 …… 71
实验 9 缓冲区溢出攻击与防范 …… 74

第 8 章 Web 攻击及防范 …… 76
8.1 Web 攻击原理 …… 76
8.2 浏览器炸弹 …… 76
8.3 SQL 注入攻击 …… 77
8.4 XSS 攻击 …… 81
8.4.1 XSS 攻击概述 …… 81
8.4.2 XSS 攻击过程 …… 81
8.4.3 XSS 攻击实例 …… 83
8.5 Web 攻击的防范 …… 86
实验 10 通过 SQL 注入获得网站后台用户密码 …… 87

第 9 章 木马攻击及防御技术 …… 89
9.1 木马介绍 …… 89
9.2 木马实现原理 …… 91
9.3 木马关键技术 …… 92

9.3.1 自启动技术 …… 92
9.3.2 隐藏技术 …… 94
9.4 冰河木马介绍 …… 95
9.5 木马攻击的防范 …… 98
实验 11 冰河木马实验 …… 98

第 10 章 病毒与蠕虫攻击及防御技术 …… 100
10.1 病毒概述 …… 100
10.2 蠕虫概述 …… 101
10.3 冲击波病毒分析 …… 103
10.3.1 冲击波病毒的特征 …… 103
10.3.2 冲击波病毒的清除 …… 103
10.3.3 冲击波病毒的预防 …… 103
10.4 病毒和蠕虫的防范 …… 105
实验 12 病毒清除实验 …… 105

第 11 章 典型网络攻击防御技术 …… 106
11.1 防火墙的工作原理 …… 106
11.2 防火墙分类 …… 106
11.3 天网防火墙的配置 …… 108
11.3.1 天网防火墙简介 …… 108
11.3.2 安全级别设置 …… 108
11.3.3 IP 规则设置 …… 109
11.3.4 应用程序安全规则设置 …… 109
11.3.5 应用程序网络使用情况 …… 110
11.3.6 系统日志 …… 111
实验 13 iptables 的攻防实验 …… 111
11.4 入侵检测系统原理 …… 112
11.5 入侵检测系统分类 …… 112
11.6 Windows 上 Snort 的安装与配置 …… 113
11.6.1 Snort 简介 …… 113
11.6.2 Windows 平台上 Snort 的安装 …… 113
实验 14 Linux 上 Snort 的安装与配置 …… 117

综合考察 安全综合论文 …… 119

网络攻击与防御技术实验报告 …… 120

参考文献 …… 123

第1章 基本实验

1.1 Windows 账户和密码的安全设置

Windows 作为使用最为广泛的桌面操作系统，其安全性尤为重要，在保障其安全运行的所有措施中，其中账户和密码的安全设置是最基本的一个环节。因为账户和密码是系统登录的基础防线，也是众多黑客程序攻击和窃取的对象。普通用户常常在安装系统后长期使用系统的默认设置，忽视了 Windows 系统默认设置的不安全性，而这些不安全性常常被攻击者所利用来得到系统的账户，进一步破解密码。因此，保障系统账户和密码的安全是非常重要的。

在 Windows 中，可以从以下方面加强账户和密码的安全性。

1. 设置密码

设置密码时建议大写字母、小写字母、数字和非字母数字的字符（如标点符号、数学符号）等混合使用。同时还要注意：密码的设置不要使用普通的名字或昵称；不使用普通的个人信息如生日日期；密码里不含有重复的字母或数字；至少使用 8 个字符等。

2. 删除不再使用的账户，禁用 Guest 账户

共享账户、Guest 账户等的安全保护级别较弱，常常都是黑客们攻击的对象，系统的账户越多，被攻击者攻击的可能性越大，因此要及时检查和删除不必要的账户，必要时禁用 Guest 账户来保障系统的安全性。

1）检查和删除不必要的账户

在 Windows XP 中，打开控制面板，选择“管理工具”中的“计算机管理”，选中“本地用户和组”，打开“用户”，弹出如图 1.1 所示的窗口。

在弹出的窗口中列出了系统所有的账户，确认这些账户是否仍在使用，并删除其中不用的账户。

2）Guest 账户禁用

在图 1.1 中，选中 Guest 账户，在右键菜单中选择“属性”命令，弹出如图 1.2 所示的对话框。选中“账户已停用”复选框。

确定后，Guest 账户所对应的图标上会出现一个红色的叉。此时再用 Guest 账户登录，则会显示“您的账户已停用，请与管理员联系”。

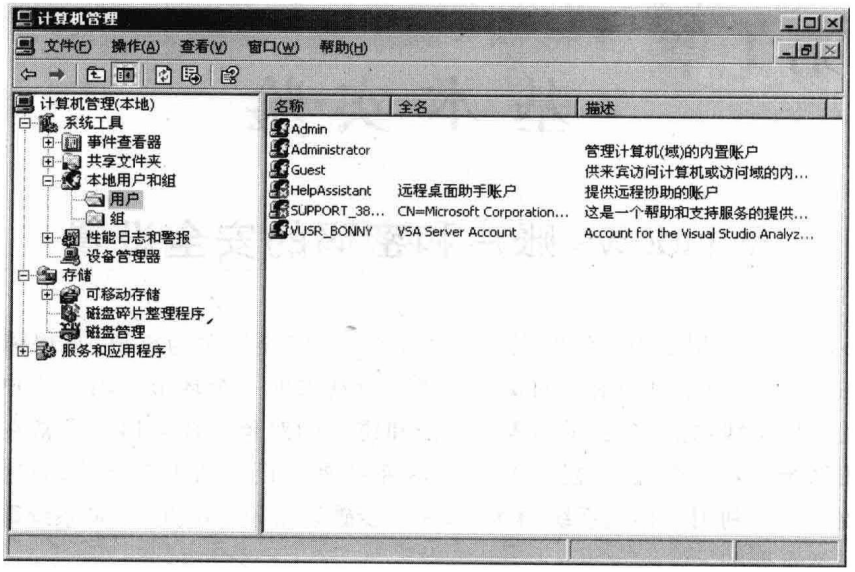


图 1.1　Windows XP 中的用户列表

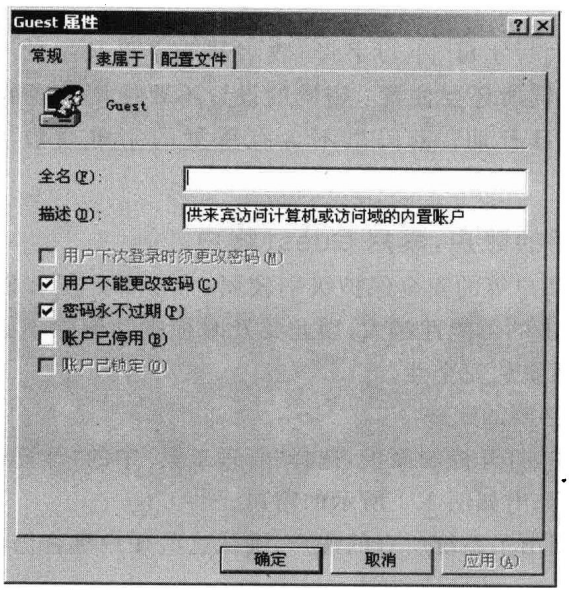


图 1.2　“Guest 属性”对话框

3. 启用账户策略

账户策略是 Windows 账户管理的重要工具。

打开控制面板的管理工具，选择“本地安全策略”，弹出如图 1.3 所示的窗口。选择“账户策略”→“密码策略”，弹出如图 1.4 所示的窗口。密码策略用于决定系统密码的安全规则和设置。

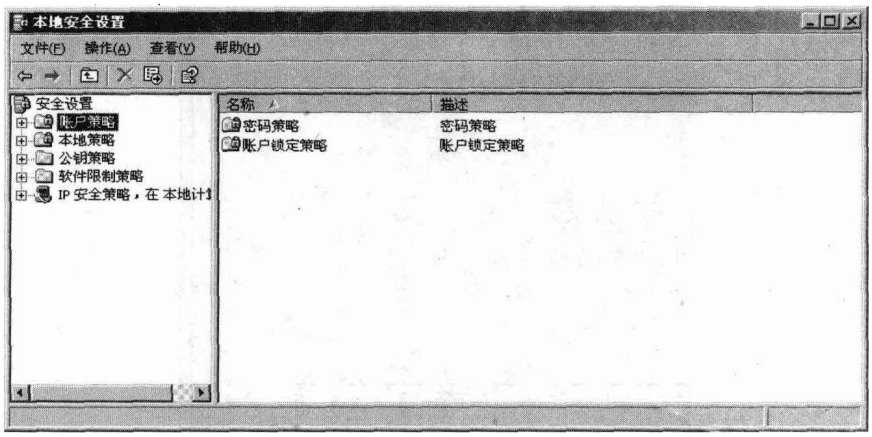


图 1.3 账户策略

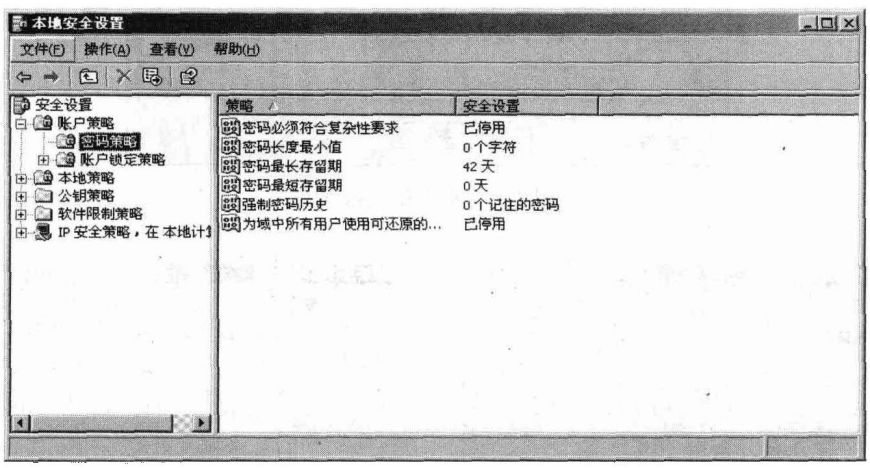


图 1.4 密码策略

其中，符合复杂性要求的密码是具有相当长度，同时含有数字、大小写字母和特殊字符的序列。双击其中的每一项，可以按照需要改变密码特性的设置。

(1) 双击“密码必须符合复杂性要求”，在弹出的如图 1.5 所示的对话框中，选择已“启用”。打开控制面板中的“用户账户”项，在弹出的对话框中选择一个用户，单击“设置密码”按钮，在出现的设置密码窗口中输入密码。此时设置的密码要符合所设定的策略。例如，若设定密码为 12345，则弹出如图 1.6 所示的提示对话框；若输入 abcd@123 则系统予以接受。

(2) 双击“密码长度最小值”，在弹出的如图 1.7 所示的对话框中设置可被系统接纳的账户密码长度最小值，一般建议设置长度为 8。

(3) 双击“密码最长存留期”，在弹出的如图 1.8 所示的对话框中设置系统要求的账户密码的最长使用期限。设置密码自动保留期，可以提醒用户定期修改密码，防止密码使用时间过长带来的安全问题。

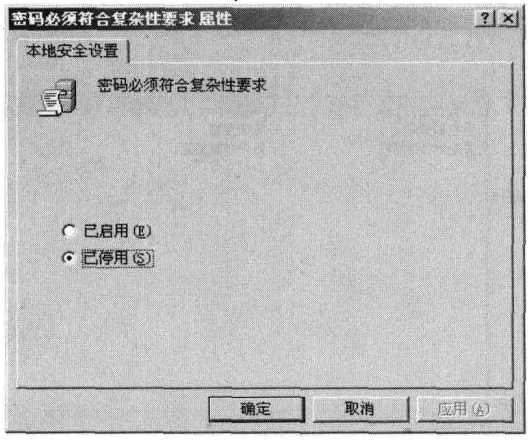


图 1.5　“密码必须符合复杂性要求属性”窗口

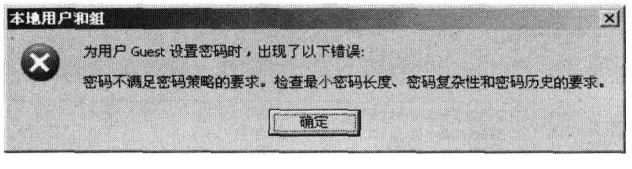


图 1.6　密码设置错误

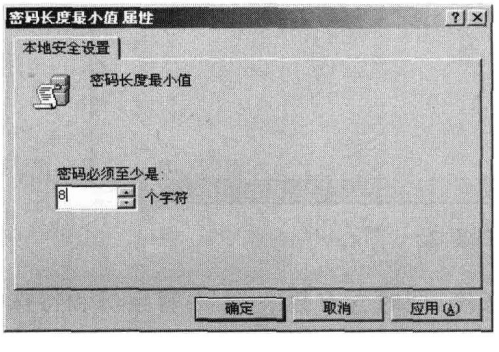


图 1.7　密码长度最小值

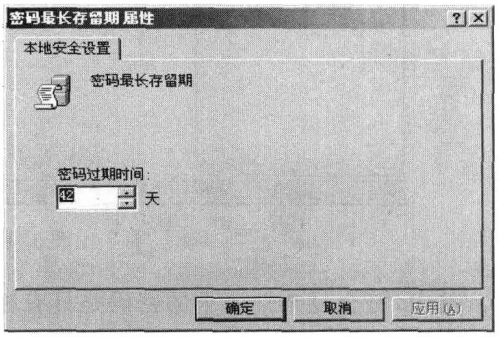


图 1.8　密码最长存留期

(4) 双击“密码最短存留期”，在弹出的如图 1.9 所示的对话框中修改设置密码最短存留期。在密码最短存留期内不能修改密码。这项设置是为了避免入侵的攻击者修改账户密码，其中 0 天表示可以立即更改密码。

(5) 双击“强制密码历史”，在弹出的如图 1.10 所示的对话框中，设置让系统记住的密码数量，其中 0 表示不保留密码历史记录。

(6) 双击“为域中所有用户使用可还原的加密来储存密码”，在弹出的如图 1.11 所示的对话框中，设置是否使用可还原的加密来存储密码。

这样，密码策略就设置完毕了。

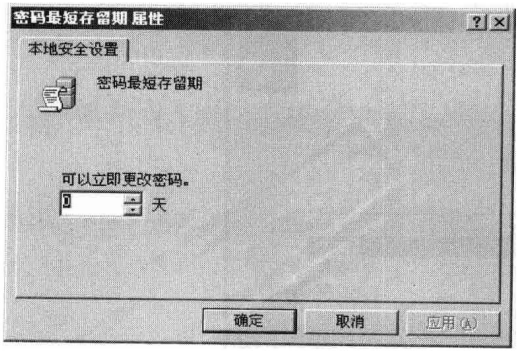


图 1.9 密码最短存留期

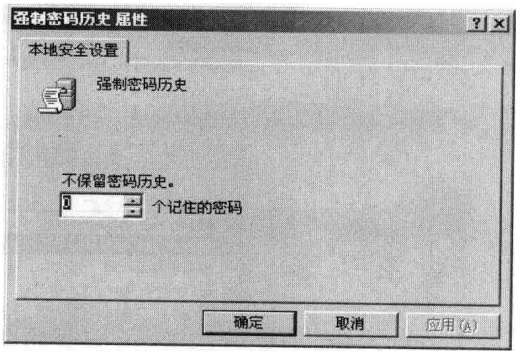


图 1.10 强制密码历史

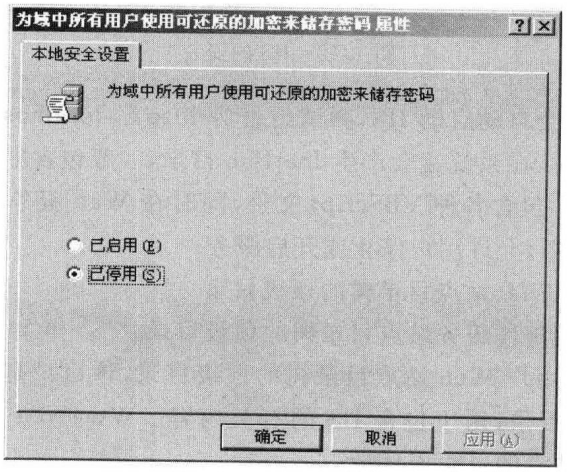


图 1.11 加密存储密码

1.2 IIS 的安装与安全配置

1.2.1 IIS 的安装

IIS 作为 Windows 上流行的 Web 服务器之一，提供了强大的 Internet 和 Intranet 服务功能。如何加强 IIS 的安全机制，建立一个高安全性能的 Web 服务器，已成为 IIS 设置中重要的组成部分。

打开 Windows XP 中的控制面板，选择“添加删除程序”项，在打开的窗口中选择“添加删除 Windows 组件”，就会弹出一个对话框，将“Internet 信息服务(IIS)”复选框选中，如图 1.12 所示。

通过“详细信息”按钮，可以进一步查看需要安装的相关组件，一般可根据需要进行灵活定制。安装过程中会提示插入 Windows 安装盘。