

黑客技术典型应用系列

200 分钟
DVD多媒体
讲解视频

黑客防范技巧与典型应用

武新华 段玲华 刘 岩 等编著

- ▶ 有效抵抗与主动防御双管齐下，知己知彼，打造固若金汤的入侵防范系统。
- ▶ 通过典型实例全面解析黑客防范技巧，工具软件、应用环境和实战经验尽在其中。
- ▶ 网络安全高手点拨技术难点，多媒体视频直观再现实战场景，全力弥补读者知识断层。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客技术典型应用系列

黑客防范技巧与典型应用

武新华 段玲华 刘 岩 等编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书紧紧围绕黑客防范技巧及其典型应用,针对用户在进行黑客防御时要用到的技术进行“傻瓜式”的讲解,以使读者对网络防御技术形成系统的了解,能够更有效地防范黑客的攻击。全书共分为 11 章,主要内容包括 Windows 系统漏洞防范、木马与间谍软件的伪装与查杀、浏览器恶意攻击和防御、QQ 的攻击与防御技术、电子邮件防御实战、后门与自身防护技术、网络代理与恶意进程清除、远程控制工具与防御、备份升级与数据恢复、病毒木马主动防御清除、打好网络安全防御战等。

本书内容丰富、图文并茂、深入浅出,适合广大网络爱好者阅读,也适合网络安全从业人员及网络管理员参考。

图书在版编目(CIP)数据

黑客防范技巧与典型应用/武新华等编著. —北京:中国铁道出版社, 2009. 5

(黑客技术典型应用系列)

ISBN 978-7-113-10017-9

I. 黑… II. 武… III. 计算机网络—安全技术 IV. TP393. 08

中国版本图书馆 CIP 数据核字 (2009) 第 072839 号

书 名: 黑客防范技巧与典型应用
作 者: 武新华 段玲华 刘岩 等编著

策划编辑: 严晓舟 荆 波
责任编辑: 苏 茜
编辑助理: 吴春英
封面设计: 付 巍
责任印制: 李 佳

编辑部电话: (010) 63583215
封面制作: 白 雪

出版发行: 中国铁道出版社(北京市宣武区右安门西街 8 号 邮政编码: 100054)
印 刷: 北京鑫正大印刷有限公司
版 次: 2009 年 7 月第 1 版 2009 年 7 月第 1 次印刷
开 本: 787mm×1092mm 1/16 印张: 24.25 字数: 570 千
印 数: 4 000 册
书 号: ISBN 978-7-113-10017-9/TP·3289
定 价: 45.00 元(附赠光盘)

版权所有 侵权必究

凡购买铁道版的图书,如有缺页、倒页、脱页者,请与本社计算机图书批销部调换。

前言

随着全球信息化的高速发展、互联网的日益普及和信息化工程的快速建设,电子商务、电子政务、网上银行、网络游戏等,已成为当前 IT 技术的应用热点。社会各方面对网络和信息技术的依赖程度不断增强,网络已逐渐成为人们工作和生活中必不可少的一部分。网络在给人们带来极大便利的同时,黑客入侵和网络安全也同样给人们的生活和工作带来了不利的影响,如僵尸网络(Botnet)、网络钓鱼(Phishing)、木马及间谍软件、零时间威胁、熊猫烧香、网站挂马事件、木马产业链等的严重危害,更使得网络安全问题成为大家关注的焦点。

由于互联网本身存在的设计缺陷及其复杂性、开放性等特点,网络的安全性已成为阻碍信息化进程的重要因素,其影响已通过互联网逐步扩大到政府、通信、广电、金融、电力、交通等领域,网络安全问题已引起了全世界的密切关注,黑客的恶行行为已成为全球新的公害。

因此,必须采取有力措施加强网络自身安全的防护性能,有效抵抗入侵和攻击破坏。但随着攻击手段的日趋复杂,有组织、有预谋、有目的、有针对性、多样化的攻击和破坏活动的频繁发生,攻击点也越来越趋于精确和集中,攻击破坏的影响面不断扩大并产生连环效应,因此必须构筑一种主动的安全防御系统,才有可能最大限度地有效应对黑客攻击方式的各种变化。

本书的写作目的主要是通过介绍黑客的攻击手段和提供相应的主动防御保护措施,使读者能够循序渐进地了解黑客入侵和主动防御的方法与关键技术,提高用户安全防护意识。本书是一本实用的网络安全工具书,适用于网络信息安全专业的技术人员、网络安全管理人员、网络使用者及信息时代的创业者阅读。

此外,本书还从黑客入侵防护应用角度给出了相对独立的论述,使读者对如何建构一个实用的黑客入侵防范体系有一个基本概念和思路,并为读者提供了几种典型的安全防护系统建设方案,供读者参考和借鉴。

本书特色如下:

- 通俗易懂,由浅入深,使初学者和具有一定基础的用户都能逐步提高,快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性,理论和实例相结合,并配以插图和配套光盘视频讲解,力图使读者能够融会贯通。
- 介绍大量小技巧和小窍门,提高读者的效率,并节省读者宝贵的时间。
- 重点突出、操作简练、内容丰富,同时附有大量的操作实例,读者可以一边学习,一边在电脑上操作,做到即学即用、即用即得。

作者采用任务驱动的方式讲解,揭秘每一种黑客攻击的手法;披露黑客常用的攻击技术,让您知己知彼,掌握攻防互参的防御方法,全面确保您的网络安全。

本书由武新华、段玲华、刘岩等编著。其中,武新华负责第1章,李防负责第2章,李秋菊负责第3章,陈艳艳负责第4章,杨平负责第5章,段玲华负责第6章和第11章,张克歌负

责第 7 章，刘岩负责第 8 章，王英英负责第 9 章，孙世宁负责第 10 章，最后由武新华通审全稿。本书在编写过程中得到了许多热心网友的支持，参考了大量同类的书籍与资料，并对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

编 者

2009 年 3 月

郑重声明：

本书目的绝不是为那些怀有不良动机的人提供技术支持，也不承担因为技术被滥用所产生的连带责任；希望读者在阅读本书后，不要使用书中所讲技术进行任何违法行为，否则后果自负，切记切记！

目 录

第 1 章 Windows 系统漏洞防范	1
1.1 设置组策略实现安全登录	1
1.1.1 组策略概述	1
1.1.2 重命名默认账户	6
1.1.3 账户锁定策略	7
1.1.4 密码策略	9
1.1.5 隐藏桌面系统图标	10
1.1.6 设置用户权限	11
1.1.7 其他策略	12
1.2 注册表编辑器实用防范技巧	16
1.2.1 禁止访问和编辑注册表	16
1.2.2 设置注册表隐藏保护策略	20
1.2.3 关闭默认共享保证系统安全	21
1.2.4 预防 SYN 系统攻击	23
1.2.5 驱逐自动运行的木马	25
1.2.6 设置 Windows 系统自动登录	26
1.2.7 只允许运行指定的程序	28
1.3 Windows 系统的密码保护	29
1.3.1 设置 Windows XP 系统密码	29
1.3.2 设置电源管理密码	30
1.3.3 设置与破解屏幕保护密码	31
1.4 Windows 系统的安全设置	36
1.4.1 激活 Windows XP 系统的防火墙	36
1.4.2 对 Windows 系统实施网络初始化	36
1.4.3 在 IE 中设置隐私保护	37
1.4.4 利用加密文件系统加密	38
1.4.5 屏蔽不需要的系统组件	39
1.4.6 锁定计算机	39
1.5 可能出现的问题与解决方法	41
1.6 总结与经验积累	41
第 2 章 木马与间谍软件的伪装与查杀	42
2.1 火眼金睛识别木马	42
2.1.1 什么是木马	42

2.1.2	木马的常用入侵手法	44
2.1.3	木马的伪装手段	45
2.1.4	识别出机器中的木马	46
2.2	用木马清除软件清除木马	46
2.2.1	使用“超级兔子”清除木马	47
2.2.2	使用 Trojan Remover 清除木马	54
2.2.3	使用“木马克星”清除木马	55
2.2.4	使用 360 安全卫士维护系统安全	56
2.2.5	在“Windows 进程管理器”中管理进程	60
2.3	自动安装“后门程序”的间谍软件	63
2.3.1	什么是间谍软件	64
2.3.2	拒绝潜藏的间谍软件	64
2.3.3	用 Spybot 揪出隐藏的间谍	65
2.3.4	间谍广告的杀手 Ad-Aware	68
2.3.5	对潜藏的“间谍”学会说“不”	70
2.4	可能出现的问题与解决方法	73
2.5	总结与经验积累	74
第 3 章	浏览器遭受恶意攻击与防御	75
3.1	认识恶意代码	75
3.1.1	恶意代码的特征	75
3.1.2	非过滤性病毒	76
3.1.3	恶意代码如何传播	76
3.1.4	恶意代码的传播趋势	77
3.2	修改注册表防范恶意代码	78
3.2.1	自动弹出网页和对话框	78
3.2.2	浏览网页时被禁用了注册表	80
3.2.3	强行修改标题栏与默认首页地址	82
3.3	让人惶恐的 IE 炸弹	83
3.3.1	IE 炸弹攻击的表现形式	83
3.3.2	IE 窗口炸弹的防御	85
3.4	危险性极强的 IE 执行任意程序	85
3.4.1	利用 chm 帮助文件执行任意程序	86
3.4.2	chm 帮助文件执行任意程序的防范	88
3.4.3	IE 执行本地可执行文件漏洞	89
3.5	IE 处理异常 MIME 漏洞	90
3.5.1	MIME 头漏洞应用基础	90
3.5.2	对浏览网页的用户施用恶意指令	93
3.5.3	防范 IE 异常处理 MIME 漏洞的攻击	96
3.6	可能出现的问题与解决方法	97

3.7 总结与经验积累.....	97
第4章 QQ 的攻击与防御技术	98
4.1 常见 QQ 攻击技术	98
4.1.1 QQ 被攻击的方式	98
4.1.2 用“QQ 登录号码修改专家”查看聊天记录.....	100
4.1.3 预防用 QQ 掠夺者盗取 QQ 密码.....	105
4.1.4 预防用“QQ 枪手”在线盗取密码.....	107
4.1.5 预防“QQ 机器人”在线盗取密码.....	107
4.1.6 QQ 的自带防御功能	108
4.2 预防 QQ 远程盗号	109
4.2.1 预防并不友好的“好友号好好盗”	109
4.2.2 预防远程控制的“QQ 远控精灵”	111
4.2.3 预防“QQ 密码保护”骗子	113
4.2.4 预防 QQ 密码的在线破解	113
4.3 预防 QQ 信息炸弹与病毒	120
4.3.1 用 QQ 狙击手 IpSniper 进行信息轰炸.....	120
4.3.2 在对话模式中发送消息炸弹的常用工具	125
4.3.3 向指定的 IP 地址和端口号发送信息炸弹.....	127
4.3.4 抵御 QQ 信息炸弹	128
4.4 可能出现的问题与解决方法	129
4.5 总结与经验积累.....	129
第5章 电子邮件防御实战.....	130
5.1 针对 WebMail 的攻防实战.....	130
5.1.1 预防来自邮件地址的欺骗	130
5.1.2 预防 WebMail 的探测	131
5.1.3 揭秘 E-mail 密码的探测	132
5.1.4 针对 POP3 邮箱的“流光”	133
5.1.5 恢复侵占后的邮箱密码	135
5.2 全面认识邮箱炸弹	136
5.2.1 邮箱炸弹	137
5.2.2 其他方式的邮箱轰炸	139
5.2.3 什么是邮件木马	139
5.2.4 溯雪使用详解	143
5.2.5 预防邮件炸弹	149
5.3 全面防范邮件附件病毒.....	151
5.3.1 禁止 HTML 格式邮件的显示	151
5.3.2 尽量不保存和打开邮件附件	152
5.3.3 启用 Outlook Express 加载项（插件）	152
5.3.4 修改文件的关联性	153

5.4	可能出现的问题与解决	155
5.5	总结与经验积累	155
第 6 章	后门与自身防护技术	156
6.1	后门技术的实际应用	156
6.1.1	手工克隆账号技术	156
6.1.2	程序克隆账号技术	162
6.1.3	制造 Unicode 漏洞后门	164
6.1.4	制造系统服务漏洞	166
6.1.5	SQL 后门	170
6.2	清除登录服务器的日志信息	171
6.2.1	手工清除服务器日志	171
6.2.2	使用批处理清除远程主机日志	172
6.2.3	通过工具清除事件日志	172
6.2.4	清除 WWW 和 FTP 日志	173
6.3	网络防火墙技术	174
6.3.1	功能强大的网络安全特警 2008	174
6.3.2	全面剖析 Windows XP 防火墙	182
6.3.3	黑客程序的克星——Anti Trojan Elite	184
6.4	可能出现的问题与解决方法	188
6.5	总结与经验积累	188
第 7 章	网络代理应用与恶意进程清除	189
7.1	跳板与代理服务器	189
7.1.1	代理服务器概述	189
7.1.2	跳板概述	191
7.1.3	代理服务器的设置	192
7.1.4	制作自己的一级跳板	193
7.2	代理工具的使用	196
7.2.1	代理软件 CCProxy 中的漏洞	196
7.2.2	代理猎手使用技巧	202
7.2.3	代理跳板建立全攻略	208
7.2.4	利用 SocksCapv2 设置动态代理	210
7.2.5	用 MultiProxy 自动设置代理	214
7.3	清除日志文件	217
7.3.1	利用 elsave 清除日志	218
7.3.2	手工清除服务器日志	218
7.3.3	用清理工具清除日志	220
7.4	恶意进程的追踪与清除	220
7.4.1	理解进程的追踪与清除	220
7.4.2	查看、关闭和重建进程	222

7.4.3	隐藏进程和远程进程	224
7.4.4	杀死自己机器中的病毒进程	226
7.5	可能出现的问题与解决方法	227
7.6	总结与经验积累	228
第 8 章	远程控制工具的攻击与防御	229
8.1	篡改注册表实现远程监控	229
8.1.1	通过注册表启动终端服务	230
8.1.2	telnet 中的 ntlm 权限验证	230
8.2	监控端口与远程信息	231
8.2.1	用 SuperScan 工具监控端口	231
8.2.2	用 URLy Warning 监控远程信息	233
8.3	远程控制工具一览	235
8.3.1	用魔法控制实现远程控制	235
8.3.2	用 WinVNC 实现远程控制	239
8.3.3	用 WinShell 定制远程服务端	242
8.3.4	用 CuteFTP 实现文件传送	244
8.3.5	用 QuickIP 实现多点控制	249
8.3.6	用屏幕间谍实现定时远程抓屏	252
8.4	远程控制经典工具 PcAnywhere	254
8.4.1	PcAnywhere 安装流程	255
8.4.2	PcAnywhere 的相关功能配置	257
8.4.3	实现 PcAnywhere 远程控制	262
8.5	可能出现的问题与解决方法	265
8.6	总结与经验积累	266
第 9 章	备份升级与数据恢复	267
9.1	数据备份升级概述	267
9.1.1	什么是数据备份	267
9.1.2	系统的补丁升级	271
9.1.3	实现数据备份操作	272
9.2	使用和维护硬盘数据恢复	277
9.2.1	什么是数据恢复	277
9.2.2	造成数据丢失的原因	278
9.2.3	使用和维护硬盘的注意事项	278
9.2.4	数据恢复工具 Easy Recovery 和 Final Data	279
9.3	备份与恢复操作系统	286
9.3.1	用 Drive Image 备份/还原操作系统	286
9.3.2	系统自带的还原功能	290
9.3.3	用 Ghost 实现系统备份还原	292
9.4	备份与恢复 Windows Vista 操作系统	295

9.4.1	Windows Vista 自带的备份/还原功能	295
9.4.2	用安装文件备份恢复 Windows Vista 系统	298
9.4.3	用 Ghost11 实现系统备份还原	301
9.5	备份与还原其他资料	301
9.5.1	备份还原驱动程序	301
9.5.2	备份还原注册表	302
9.5.3	备份还原病毒库	304
9.5.4	备份还原收藏夹	305
9.5.5	备份还原电子邮件	307
9.6	可能出现的问题与解决方法	310
9.7	总结与经验积累	310
第 10 章	主动防御、清除病毒木马	311
10.1	关闭危险端口	311
10.1.1	利用 IP 安全策略关闭危险端口	311
10.1.2	一键关闭危险端口	315
10.2	用防火墙隔离系统与病毒	318
10.2.1	Windows 系统自带的防火墙	318
10.2.2	用“天网”将攻击挡在系统之外	321
10.2.3	免费网络防火墙: Zone Alarm	326
10.3	对未知病毒和木马全面监控	329
10.3.1	监控注册表与文件	329
10.3.2	监控程序文件	330
10.3.3	未知病毒和木马的防御	332
10.4	维护系统安全的 360 系统卫士	336
10.4.1	查杀恶评软件与病毒	336
10.4.2	修复 IE 浏览器、LSP 连接	337
10.4.3	清理使用痕迹	338
10.5	拒绝网络广告	339
10.5.1	过滤弹出式广告傲游 Maxthon	339
10.5.2	过滤网络广告杀手的 Ad Killer	340
10.5.3	广告智能拦截的利器 Zero Popup	341
10.5.4	使用 MSN 的 MSN toolbar 阻止弹出广告	341
10.6	可能出现的问题与解决方法	343
10.7	总结与经验累积	343
第 11 章	打好网络安全防御战	344
11.1	建立系统漏洞防御体系	344
11.1.1	检测系统是否存在可疑漏洞	344
11.1.2	如何修补系统漏洞	349
11.1.3	监视系统的操作进程	353

11.1.4	抵抗漏洞的防御策略	356
11.2	金山毒霸杀毒软件使用详解	356
11.2.1	金山毒霸的安装流程	356
11.2.2	金山毒霸的杀毒配置	359
11.2.3	用金山毒霸进行杀毒	362
11.3	东方卫士防毒软件使用详解	363
11.3.1	东方卫士的安装流程	363
11.3.2	东方卫士的杀毒配置	364
11.3.3	用东方卫士进行杀毒	365
11.4	江民杀毒软件试用详解	367
11.4.1	江民杀毒软件的安装流程	367
11.4.2	江民杀毒软件的杀毒配置	369
11.4.3	用江民杀毒软件进行杀毒	369
11.5	流氓软件清除详解	371
11.5.1	Wopti 流氓软件清除大师	371
11.5.2	恶意软件清理助手	372
11.6	可能出现的问题与解决方法	373
11.7	总结与经验积累	374
参考文献		375

第 1 章 Windows 系统漏洞防范

本章精粹

通过学习本章，可以使读者掌握如何为系统打补丁的技巧，解密黑客任意篡改他人计算机系统的伎俩，并更加全面地掌握组策略和注册表方面的知识，为黑客防御措施奠定坚实的知识基础。

重点提示

- 设置组策略实现安全登录
- 注册表编辑器实用防范
- Windows 系统的密码保护
- Windows 系统的安全设置

随着互联网的普及和网络用户的逐渐增多，由此带来的安全问题也威胁着计算机的安全，且 Windows 操作系统本身具有的漏洞，为黑客的入侵行为提供了便利之门。所谓“知己知彼，百战不殆”，要想全面防止黑客的入侵，首先就需要了解黑客是怎样发现漏洞并对漏洞进行攻击的。

1.1 设置组策略实现安全登录

在计算机的具体应用过程中，为实现某些正常的操作，管理员需要为用户和计算机定义并控制程序、网络资源及操作系统的行为等，而实现这些操作的工具就是组策略，所以要想安全地登录计算机，必须设置好组策略。

1.1.1 组策略概述

在介绍组策略之前，应该先了解注册表，注册表是 Windows 系统中保存系统软件和应用软件配置的数据库。随着 Windows 系统功能的逐渐丰富，注册表中的配置项目越来越多。很多配置都可以自定义设置，但这些配置分布在注册表的各个角落，如果是手工配置，就显得尤为困难和烦杂。而组策略则将系统重要的配置功能汇集成各种配置模块，供用户直接使用，从而达到方便管理计算机的目的。

简单地讲，组策略设置就是修改注册表中的配置。当然，组策略使用了更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便、灵活，功能也更加强大。

1. 组策略的版本

组策略是 Windows 9x/NT 中系统策略的高级扩展，具有更多的管理模板、更灵活的设置对

象及更多功能，目前主要应用在 Windows 2000/XP/2003 系统中。

系统策略编辑器支持对当前注册表的修改，也支持连接到网络中的计算机并对其注册表进行设置。而组策略及其工具可对当前注册表进行直接修改。组策略工具还可以打开网络上的计算机并进行配置，甚至可以打开某个 Active Directory 对象（即站点、域或组织单位）并对其进行设置。无论是系统策略还是组策略，其基本原理都是修改注册表中相应的配置项目，从而达到配置计算机的目的，只是其中的一些运行机制发生了变化和扩展而已。

2. 运行组策略

运行组策略实现某些控制操作的具体操作步骤如下：

步骤 1 由于 Windows 2000/XP/2003 系统中系统已默认安装了组策略，这里无须安装，选择“开始”→“运行”命令，打开“运行”对话框，如图 1-1 所示。

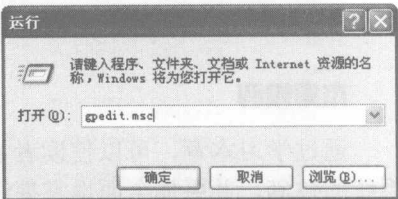


图 1-1 “运行”对话框

步骤 2 在“打开”文本框中输入 gpedit.msc 命令，单击“确定”按钮，进入“组策略”窗口，如图 1-2 所示。

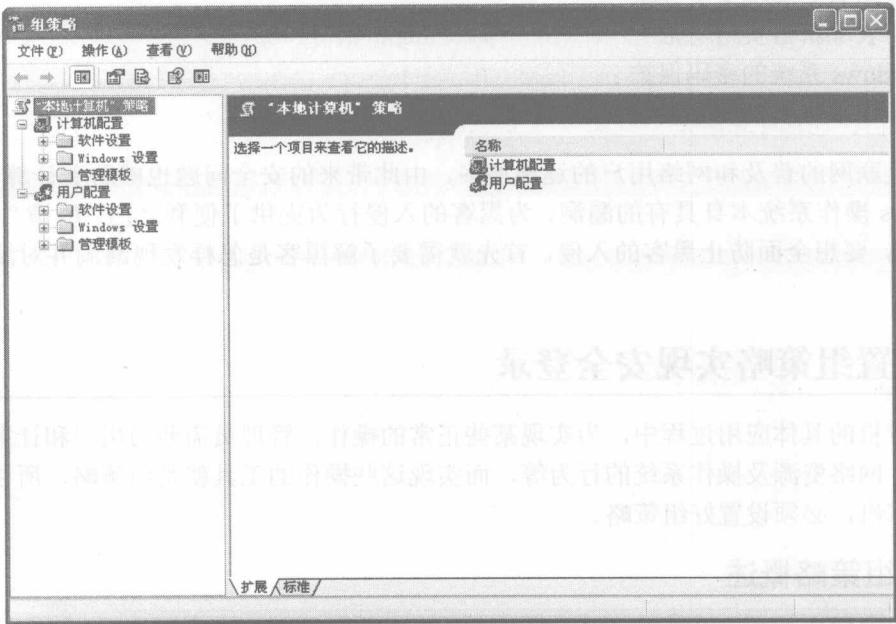


图 1-2 “组策略”窗口

步骤 3 该窗口中显示的组策略是当前计算机，在其中选择要更改的选项之后，选择“用户配置”→“管理模板”→“任务栏和「开始」菜单”选项，打开“任务栏和「开始」菜单”窗口，如图 1-3 所示。

步骤 4 右击“关闭通知区域清理”选项，从弹出的快捷菜单中选择“属性”命令，打开“关闭通知区域清理属性”对话框，根据实际需要选择相应的单选按钮对计算机策略进行管理，如图 1-4 所示。

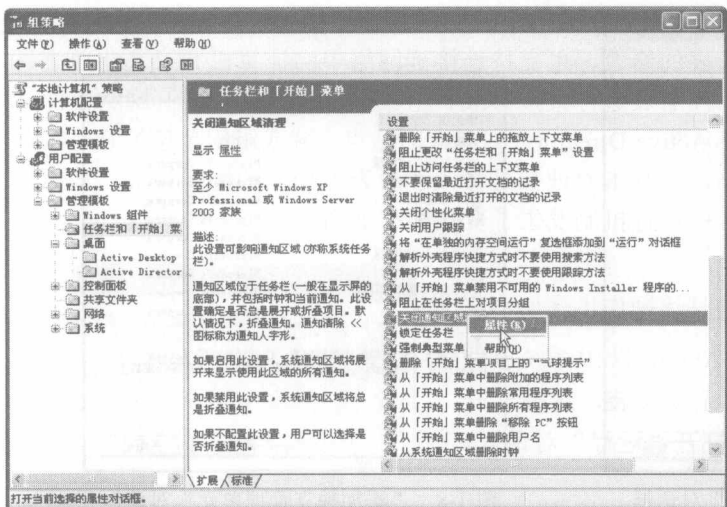


图 1-3 “任务栏和「开始」菜单”窗口

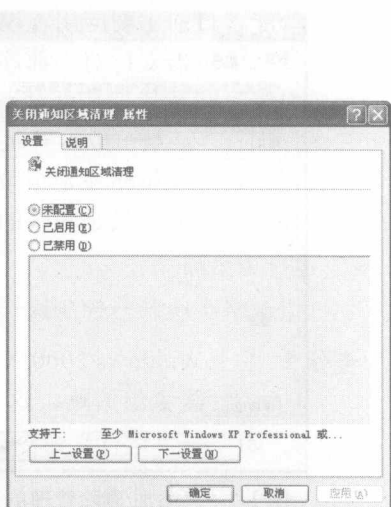


图 1-4 “关闭通知区域清理属性”对话框

步骤 5 如果需要配置其他计算机策略，则选择“开始”→“运行”命令，在“运行”对话框中输入 mmc 命令，如图 1-5 所示。单击“确定”按钮，进入“控制台 1”窗口，如图 1-6 所示。

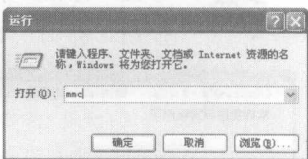


图 1-5 输入 mmc 命令

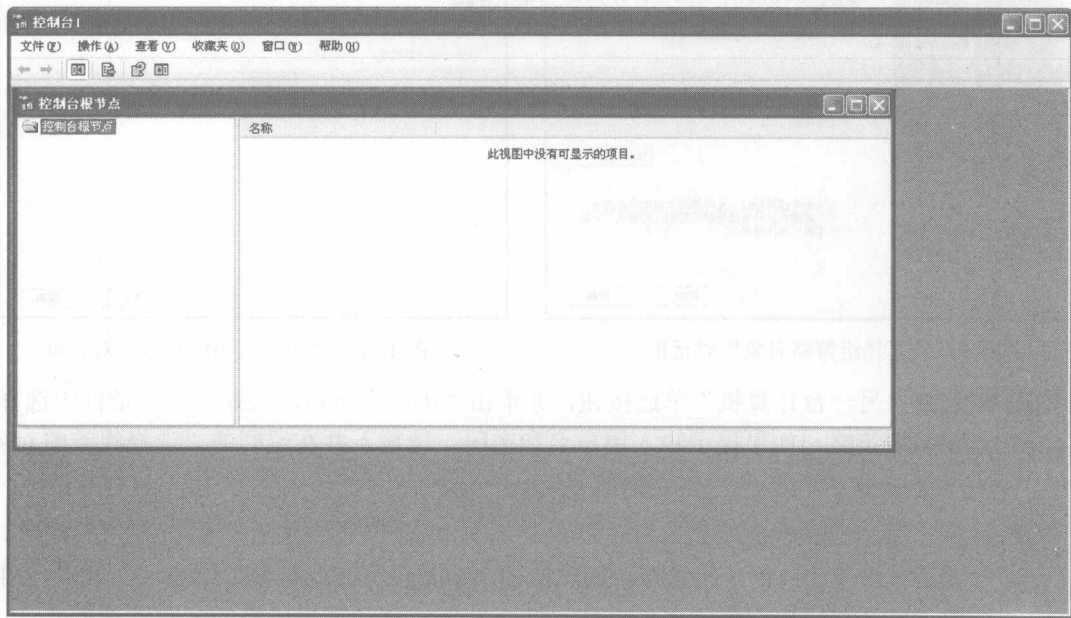


图 1-6 “控制台 1”窗口

步骤 6 选择“文件”→“添加/删除管理单元”命令，打开“添加/删除管理单元”对话框，如图 1-7 所示。单击“添加”按钮，打开“添加独立管理单元”对话框，选择“组策略对象编辑器”选项，如图 1-8 所示。



图 1-7 “添加/删除管理单元”对话框

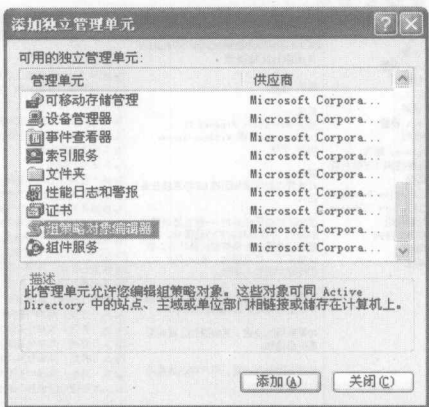


图 1-8 “添加独立管理单元”对话框

步骤 7 单击“添加”按钮，打开“选择组策略对象”对话框，如图 1-9 所示。单击“浏览”按钮，打开“浏览组策略对象”对话框，如图 1-10 所示。

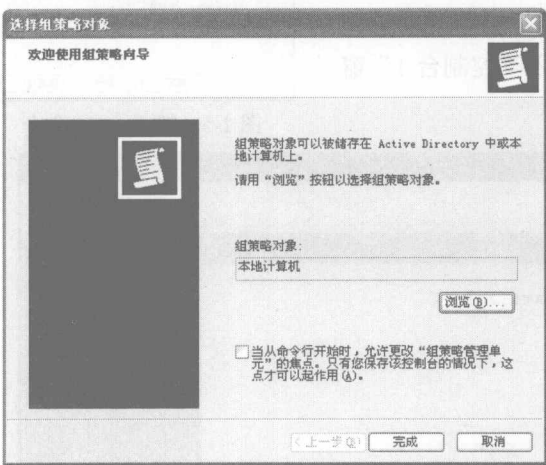


图 1-9 “选择组策略对象”对话框

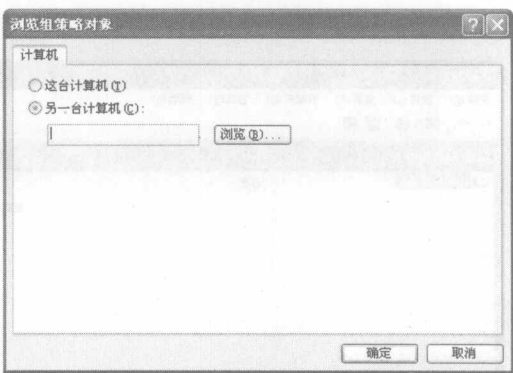


图 1-10 “浏览组策略对象”对话框

步骤 8 选择“另一台计算机”单选按钮，并单击“浏览”按钮，从弹出的对话框中选择需要的组策略，如果提示输入用户名和密码，请输入并在返回的“选择组策略对象”对话框中，单击“完成”按钮。

步骤 9 在“添加独立管理单元”对话框中，单击“关闭”按钮并在“添加/删除管理单元”对话框中单击“确定”按钮，则选定的 GPO 显示在控制台根结点下。此时，再按照当前计算机中设置策略的方法，即可实现远程计算机策略的配置管理操作。

3. 管理组策略中的管理模板

默认情况下，在 Windows 2000/XP/2003 系统中包含有几个 ADM 文本文件，这些文本文件被称为管理模板，并为“管理模板”文件夹下的项目提供策略信息。默认的 Admin.adm 管理模板位于系统文件夹的 INF 文件夹中，同时包含了默认安装下的 4 个模板文件，具体体现在：

