

Internet 信息服务

Server Extensions
管理器

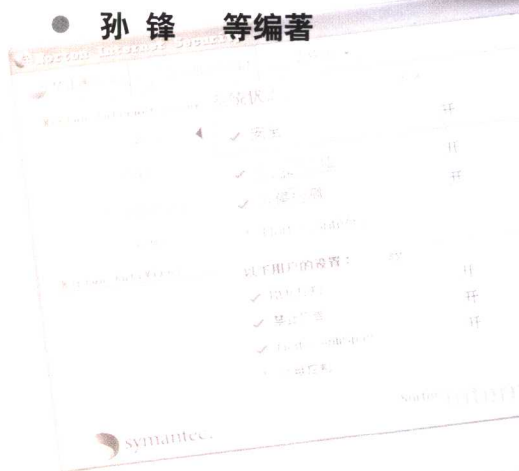


电脑安全与防黑

完全解决方案

● 孙 锋 等编著

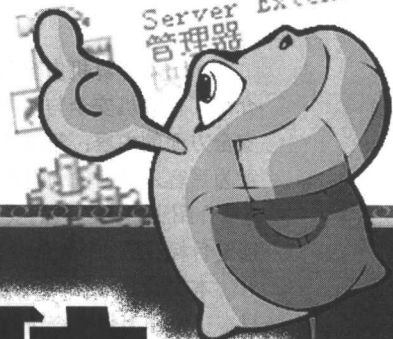
- Windows 2000/XP 安全终极解疑
- 系统漏洞问题及解决
- IE 安全终极解疑
- 黑客入侵后的问题解决
- 常用软件安全设置
- 病毒木马问题及解决
- 聊天与电子邮件的安全设置
- 由 IP 地址查找及锁定目标
- 数据备份与恢复



机械工业出版社
CHINA MACHINE PRESS

Internet 信息服务
快捷方式

Server Extensions
管理器

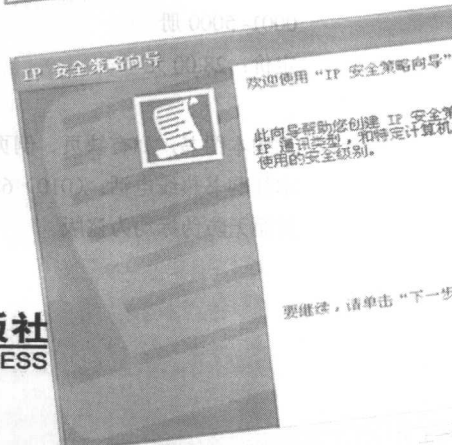
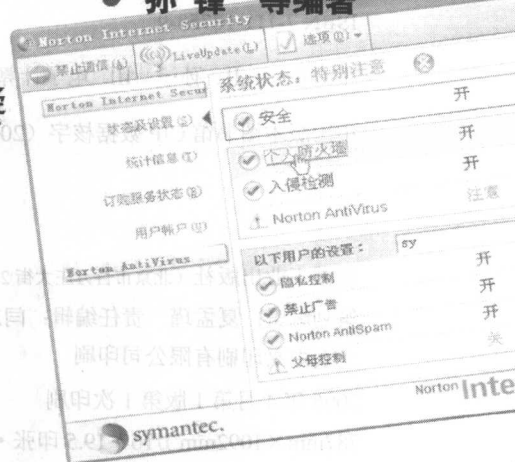


电脑安全与防黑

完全解决方案

• 孙锋 等编著

- ① Windows 2000/XP 安全终极解疑
- ② 系统漏洞问题及解决
- ③ IE 安全终极解疑
- ④ 黑客入侵后的问题解决
- ⑤ 常用软件安全设置
- ⑥ 病毒木马问题及解决
- ⑦ 聊天与电子邮件的安全设置
- ⑧ 由 IP 地址查找及锁定目标
- ⑨ 数据备份与恢复



机械工业出版社
CHINA MACHINE PRESS

本书以计算机安全与防黑技术为主题,从系统设置到网络安全,从数据备份到数据恢复,介绍了计算机安全与防黑方面的应用技巧。全书共分为10章,第1章介绍了Windows 2000/XP安全方面的内容;第2章介绍了系统漏洞方面的问题;第3章介绍了IE安全终极解疑;第4章为黑客入侵后的问题解决;第5章介绍了常用软件安全;第6章介绍了病毒木马问与答;第7章介绍了聊天工具的安全设置;第8章介绍了电子邮件防守;第9章介绍了由IP地址查找及锁定目标;第10章介绍了数据备份与恢复。

本书实践性强,实例涉及硬件、软件等各方面的内容。本书既可以作为故障排除的通用教材,也可作为快速查访的手册;既可供计算机爱好者和专业维护人员作为参考手册,也可供职业技术学校相关专业师生和广大电子技术爱好者学习参考。

图书在版编目(CIP)数据

电脑安全与防黑完全解决方案/孙锋等编著.

-北京:机械工业出版社,2006.3

(完全解决方案丛书)

ISBN 7-111-18753-9

I. 电… II. 孙… III. 电子计算机-安全技术 IV. TP309

中国版本图书馆CIP数据核字(2006)第024734号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)

策划编辑:夏孟瑾 责任编辑:闫志朝 版式设计:李永梅

北京中兴印刷有限公司印刷

2006年4月第1版第1次印刷

787mm×1092mm 1/16·19.5印张·581千字

0001-5000册

定价:28.00元

凡购本图书,如有缺页、倒页、脱页,由本社发行部调换

本社购书热线电话:(010) 68326294

封面无防伪标均为盗版



在办公室中，也许你刚刚离开计算机，别人随后就开始“偷窥”你的计算机；上网时，也许你正兴致勃勃地浏览内容，病毒已神不知鬼不觉地潜入你的计算机；工作时，也许你正完成一项重要的任务，系统却突然瘫痪……这种种突如其来的问题无时无刻都在提醒我们：计算机的安全问题，不容忽视！

一些初级计算机用户可能认为只要经常查杀病毒就可以确保计算机安全。其实不然，计算机安全不只是查杀病毒，它还包括增强系统安全性，保护个人隐私及文档的安全等内容。本书对这些内容均作了介绍。

本书主要介绍了计算机数据和文件损坏后的修复以及计算机安全防护的方法和技巧。全书共分为 10 章，具体内容分布为：第 1 章介绍了 Windows 2000/XP 安全方面的内容；第 2 章介绍了系统漏洞方面的问题；第 3 章介绍了 IE 安全终极解疑；第 4 章为黑客入侵后的问题解决；第 5 章介绍了常用软件安全；第 6 章介绍了病毒木马问与答；第 7 章介绍了聊天工具的安全设置；第 8 章介绍了电子邮件防守；第 9 章介绍了由 IP 地址查找及锁定目标；第 10 章介绍了数据备份与恢复。

本书具有以下特点：

- 内容充实

书中内容覆盖了计算机安全与防黑方面的技巧，包括 Windows 2000/XP 安全问题、系统漏洞问题、IE 安全问题、黑客入侵的惯用手段及应对方法、常用聊天工具的安全设置、电子邮件防守等方方面面的知识。

- 实用性强

书中的内容几乎都是平时读者在实际使用过程中可能遇到的。读者可根据书中的设置及防护方法，为计算机加上一层铜墙铁壁，使其更安全。

- 内容新颖

书中内容新颖，所涉及的系统及软件均为目前比较新的且常用的。

- 易学易懂

本书结构合理、条理清楚，语言简洁明了，内容循序渐进、由简到难、层次清晰，使读者可以轻松上手。

本书既可以作为计算机安全与防黑方面的通用教材，也可作为快速查访的手册。

本书由孙锋编写，参与编写的人员还有贾清新、杨敏、周末、袁江、张卫娜、崔增岗、王小丽、王静、王杰江、魏淑兰、王瑞省、孙泽欣、刘艳芬、刘沛勇、王清维等。书中若有疏漏和错误之处，希望专家和读者朋友及时指正。

编 者



前言

第1章 Windows 2000/XP 安全终极解疑 ..1

1.1 用户安全问题.....1	1
1. 如何把系统 Administrator 账号改名.....1	1
2. 如何建立两个管理员账号.....1	1
3. 如何禁用 Guest 账号.....2	2
4. 如何限制不必要的用户.....3	3
5. 陷阱用户是如何创建的.....3	3
6. 怎样才能不让系统显示上次登录的用 户名.....4	4
7. 如何开启账户策略.....4	4
8. 如何在 Windows XP 系统中让计算机 开关失灵.....5	5
9. 如何去除 Windows 的系统启动画面.....5	5
10. 用批处理文件在每次启动时删除默认 共享.....6	6
1.2 密码安全问题.....7	7
1. 如何开启密码策略.....7	7
2. 如何设置开机密码.....7	7
3. 如何设置 Windows 密码.....8	8
4. 如何设置屏幕保护密码.....8	8
5. 如何给休眠退出增加密码保护.....9	9
1.3 系统安全设置.....10	10
1. 安装 Windows XP 时要为管理员设置 密码.....10	10
2. 设置 Windows XP 启动密码.....10	10
3. 设置 Windows XP 系统的密匙盘.....10	10
4. 让整个桌面隐藏起来.....11	11
5. 保护个人文档隐私.....11	11
6. 设置用户权限.....11	11
7. 隐藏或删除资源管理器中的项目.....12	12
8. 如何去掉 Windows 2000 系统的登录 界面.....12	12
9. 如何快速锁定桌面.....13	13
10. Windows 2000 系统的安全配置技巧.....13	13
11. 为何 Windows XP 中的文件夹都是	

只读属性.....15	15
12. 如何停用 Windows2000/XP 启动密码 ..15	15
13. 如何更改 Windows 2000/XP 密码.....15	15
14. 如何制作 Windows 2000/XP 密码恢 复盘.....16	16
15. 使用 Windows XP 密码恢复复盘恢复 丢失的密码.....16	16
16. 如何设置 Windows XP 安全登录或 注销.....17	17
17. 使用系统还原.....17	17
18. 怎样让 Windows XP 快速关机和重启....18	18
19. 系统管理的必备工具.....18	18
1.4 系统安全限制.....19	19
1. 在 Windows XP 下禁止用户使用注销 功能来切换登录用户名.....19	19
2. 禁止访问“控制面板”.....19	19
3. 如何禁止使用“网上邻居”访问共享 资源.....20	20
4. 如何禁用“添加/删除程序”功能.....20	20
5. 禁止访问注册表编辑器.....21	21
6. 如何禁止远程编辑注册表.....21	21
7. 如何禁止用户使用.reg 文件.....21	21
8. 如何防止用户在计划任务文件夹中添 加删除任务.....22	22
9. 如何禁用“开始”菜单中的“运行” 命令.....22	22
10. 如何禁用“我的电脑”.....22	22
11. 如何禁用“我的文档”.....22	22
12. 如何禁止从“我的文档”中直接运行 文件.....23	23
13. 如何禁止打印机共享.....23	23
14. 如何禁止使用 MS_DOS 方式.....23	23
15. 如何禁止修改“显示”属性.....23	23
16. 如何禁止删除打印机.....23	23
17. 如何设置退出系统不保存设置.....24	24
18. 如何禁止修改用户文件夹存放路径....24	24
19. 如何禁止移动“开始”菜单.....24	24

20. 如何锁定计算机.....	24	5. 如何恢复文件或文件夹的默认访问权限	36
21. 如何禁止文件共享.....	25	6. 设置 Windows 2000/XP 共享目录密码	37
22. 如何禁止拨入访问.....	25	7. 在 Windows XP 中查找已经被加密的文件	38
23. 如何隐藏普通用户桌面上的所有图标.....	25	8. 利用 NTFS 文件系统来加密文件.....	39
24. 如何屏蔽所有的系统热键.....	26	9. 如何在 NTFS 文件系统中对文件和文件夹进行解密	39
25. 如何禁止在登录对话框中直接关闭计算机.....	26	10. 更改文件后缀加密文件	39
26. 如何禁止查看和更改现存任务的属性.....	26	11. 隐藏和恢复 Windows 2000/XP 的驱动器	40
27. 如何禁止 .inf 文件的运行	26	12. 如何更改文件类型以保护文件	41
28. 如何禁止“显示属性”对话框中的“屏幕保护程序”选项卡.....	27	13. 导出与保存加密证书	41
29. 如何禁用控制面板的“网络”图标.....	27	14. 使用“编辑文件夹的 HTML 模板”加密文件夹	42
30. 指定“控制面板”中显示的项目.....	27	15. 将文件夹设为专用文件夹	43
31. 如何禁止系统使用自动升级功能.....	28	16. 让 Windows XP NTFS 分区也显示“安全”选项卡	43
32. 禁用“任务栏属性”功能.....	29	17. 隐藏重要文件的创建日期	43
33. 禁用查看事件日志.....	29	18. 将文件夹图标改变为系统图标	43
34. 设置系统日志的保存时间.....	29	19. 利用 Desktop. ini 文件来加密文件.....	44
35. 设置计算机启动软驱成空.....	29	20. 使用 COPY 命令合并隐藏文件.....	44
36. 限制 Windows 的密码长度.....	30	21. 利用“文件签名策略”保护数据安全	44
37. 禁用 Windows XP 的压缩功能	30	22. 设置 Control.ini 文件来保护系统.....	44
38. 如何禁用 Windows XP 的自动播放功能.....	30	23. 利用类标识符“隐藏”文件夹	45
39. 如何禁用缩略图缓存.....	30	1.7 Windows 日志与入侵检测	45
40. 设置自动关闭停止响应的程序.....	31	1. 黑客为什么会对日志文件感兴趣	45
41. 如何禁止使用任务栏中的分组功能.....	31	2. 如何开启 Windows 2000 的审核策略	45
42. 如何限制关机时间.....	31	3. 如何查看和维护审核结果	46
1.5 服务器安全问题.....	32	4. 如何设置 Windows 2000 的账户策略	46
1. 如何关闭 Windows 2000 系统下不必要的端口.....	32	5. 认识 Windows XP 的日志系统.....	47
2. 在 Windows 2000 Server 版中, 如何关闭终端服务.....	32	6. Windows 系统日志的删除	47
3. 在 Windows 2000 Server 版中, 如何修改终端服务的默认端口.....	32	7. 遭受入侵时的迹象	48
4. 如何禁止建立空连接.....	32	8. 什么是入侵检测系统	48
5. 如何实现服务器远程监控.....	33	9. 入侵检测系统和日志的差异	48
6. 使用命令禁止 Server 服务	34	10. 入侵检测系统的分类	49
1.6 Windows 文件安全设置.....	34	11. 入侵检测系统的检测步骤.....	49
1. 使用 NTFS 文件系统保证系统的安全.....	34	1.8 系统隐私保护	49
2. 设置 Windows XP 中文件夹的本地共享.....	35	1. 清除“我最近的文档”记录	49
3. 设置 Windows XP 中文件夹的网络共享.....	35	2. 清除“运行”记录	50
4. 如何隐藏和加密 Windows XP 下的文件夹.....	36	3. 清除“查找”记录	50
		4. 清除“计划任务”记录	50
		5. 清除 TEMP 临时文件夹记录.....	50



6. 清除剪贴板内容.....	50
7. 清除回收站内容.....	50
8. 转移“我的文档”.....	51
9. 查看计算机开关记录.....	51
10. 清除注册表编辑记录.....	51
11. 清除与系统同时启动的应用程序.....	52
12. 清除 FTP 连接日志记录.....	53
13. 清除“写字板”中的记录.....	53
14. 删除输入法自动记忆的信息.....	53
15. 用脚本和批处理清除计算机中的 记录.....	53
16. 清除 Windows Media Player 播放 记录.....	54
17. 让 ACDSee 自动清除历史记录.....	54
18. 清除“收藏夹”记录.....	54

第2章 系统漏洞问题及解决.....55

2.1 各种常见漏洞.....	55
1. 什么是 RPC 漏洞.....	55
2. 什么是拒绝服务攻击.....	55
3. 什么是分布式拒绝服务攻击 (DDoS).....	55
2.2 系统漏洞及解决方法.....	55
1. NetBIOS 中导致信息泄露漏洞(低).....	55
2. Windows 2000 的输入法漏洞.....	56
3. IIS 的 Unicode 漏洞(严重).....	56
4. ISAPI 缓冲区扩展溢出漏洞(严重).....	56
5. MS SQL Server 的 SA 空密码漏洞 (严重).....	57
6. 系统管理权限漏洞.....	57
7. 路径优先漏洞(严重).....	57
8. NetDDE 消息权限提升漏洞 (较严重).....	57
9. RDP 拒绝服务漏洞.....	58
10. Windows 2000 域控制器拒绝服务漏洞 (较严重).....	58
11. 事件查看器缓冲区溢出漏洞.....	58
12. 安全账户管理漏洞.....	59
13. IIS 5.0 的 HTR 映射远程堆溢出漏洞 (一般).....	59
14. IIS 5.0 的 ASP 缓冲溢出漏洞.....	59
15. IIS 5.0/5.1 验证漏洞.....	59
16. SMTP 认证漏洞(低).....	59

17. IE 浏览器漏洞.....	60
18. UTF 漏洞.....	60
19. 快捷方式漏洞.....	60
20. 调试寄存器漏洞.....	60
21. 轻型目录访问协议 LDAP 漏洞 (较严重).....	61
22. JPEG 文件漏洞.....	61
23. ActiveX 漏洞.....	61
24. 密码设置漏洞.....	61
25. Juniper NSM 远程拒绝服务漏洞.....	62
26. 网络连接管理漏洞.....	62
27. SMB 漏洞.....	62
28. Outlook Express 数字签名缓冲区溢出 漏洞.....	63
29. 组策略漏洞.....	63
30. IIS 5.0 Cross-Site scripting 漏洞.....	63
31. ActiveX 参数漏洞.....	63
32. 域账号锁定漏洞.....	63
33. 默认注册许可漏洞.....	64
34. 登录服务恢复模式空密码漏洞.....	64
35. Telnet 漏洞.....	64
36. LDAP 漏洞.....	64
37. drwtsn32.exe 文件漏洞.....	65
38. Narrator 本地密码信息泄露漏洞.....	65
39. SQL Server 的函数库漏洞.....	65
40. Windows XP 远程桌面明文账户名传送 漏洞.....	65
41. Windows XP 账号锁定漏洞.....	66
42. GDI 拒绝服务漏洞.....	66
43. Windows XP 的“文件和设置转移向 导”漏洞.....	66
44. IP 欺骗漏洞.....	67
45. UNIX 系统中 Telnetd 的缓冲区溢出 漏洞.....	67
46. Access mdb 数据库被下载的漏洞.....	67
47. Linux 中获得本地管理员权限的漏洞.....	67
48. RedHat Linux setserial 脚本条件竞争 漏洞.....	67
49. RedHat Linux IPTables 保存选项无法 恢复规则漏洞.....	68
50. 内核模块 FTPFS 缓存区溢出漏洞 (Linux).....	68
51. 内核执行拒绝服务漏洞(Linux).....	68
52. RedHat Linux Vipw 不安全的文件	

属性漏洞.....	68	12. 局域网中的嗅探精灵—Iris	80
53. Linux Util-Linux Login Pam 权限提升漏洞.....	68	2.4 为 Windows 打补丁和升级	81
54. Linux 2.4 Iptables MAC 地址匹配绕过漏洞.....	69	1. 如何在局域网里给 Windows 2000/XP 打补丁和升级	81
55. RedHat Linux Apache 远程列举用户名漏洞.....	69	2. 如何从微软的网站上给 Windows XP 打补丁和升级	82
56. RH Linux Tux HTTPD 拒绝服务漏洞	69	3. 如何给 Windows 2000 打补丁和升级	83
57. Linux ColdFusion CFReThrow 标签拒绝服务漏洞.....	69	4. 在 Windows 2000/XP 中安装数字证书	84
58. SuSe Linux sdbsearch.cgi 执行任意代码漏洞.....	70	5. 给 Windows XP 安装 SP2 补丁	85
59. SQL Server 2000 “扩展存储过程”漏洞.....	70	6. HotFix 让系统更安全	85
60. C Runtime 函数库内格式字符串漏洞	70	7. 保证让系统一开始就具有免疫力	85
61. Code.asp 文件会泄露 ASP 代码漏洞.....	70	8. 在 Windows 2000 安装 SP4 补丁.....	85
62. File system object 组件漏洞.....	70	9. 从“添加或删除程序”中查看自动更新情况	86
63. ASP 程序密码验证漏洞	71	10. 下载安装 ADODB.Stream 漏洞防范工具	86
64. IIS 泄露 ASP 源程序漏洞	71	第 3 章 IE 安全终极解疑	87
65. PHP MyAdmin 漏洞.....	71	1. 设置浏览器的分级审查功能	87
66. PHP BB 远程 SQL 查询处理漏洞.....	71	2. 如何取消设置的分级审查	87
67. PHProjekt 漏洞.....	71	3. 忘记分级审查密码怎么办	88
68. PHP-Nuke 的 Cookie 漏洞.....	72	4. 如何设置匿名浏览	88
69. PHP-Nuke 文件泄露和上传漏洞	72	5. 如何恢复被修改了的浏览器的默认起始页	88
70. PHP-Nuke 的 Network Tool 漏洞	72	6. 如何恢复被修改的 IE 默认搜索引擎.....	89
71. PHP-Nuke 跨站脚本执行漏洞	72	7. 如何在 IE 中防止恶意代码.....	89
72. Unix Manual 漏洞	72	8. 如何禁止弹出广告信息窗口	90
73. PHPFileExchange 漏洞	72	9. 什么是 Cookie 信息.....	90
74. HTML 语句或 JavaScript 语句的漏洞	73	10. 如何清除 Cookie.....	90
75. Windows 2000 系统崩溃漏洞.....	73	11. 如何禁用 Cookie.....	91
76. SAM 数据库安全漏洞	73	12. 如何清除历史记录	91
2.3 系统漏洞扫描.....	73	13. Cookie 数据记录的安全管理.....	91
1. 使用扫描器检查系统漏洞.....	73	14. 如何清除 IE 临时文件.....	92
2. 使用在线扫描发现系统漏洞.....	74	15. 定制 Windows 可访问 Internet 的项目	92
3. 使用 SSS 软件检测安全漏洞	74	16. IE 地址栏下多出了文字.....	92
4. 使用瑞星的漏洞扫描工具扫描漏洞.....	75	17. IE 工具栏被添加网站连接.....	93
5. 使用共享扫描工具扫描开放共享.....	76	18. 开机自动弹出的网页	93
6. 金山毒霸漏洞扫描.....	77	19. IE 标题栏被修改.....	94
7. 微软安全检测工具 MBSA	78	20. 如何解除鼠标右键被禁用	95
8. 使用 BigFix 找漏洞补丁.....	78	21. 如何处理重启后一切照旧的恶性破坏	95
9. ARP-Killer 软件的使用	79	22. 如何防止浏览网页时硬盘被恶意共享	96
10. 使用 SSH 软件保证远程安全登录	79		
11. 个人服务器漏洞扫描的利器——WebDAVScan.....	80		



23. 如何让 IE 的窗口大小适度.....	97
24. 如何选择 IE 的保存类型.....	97
25. IE 不能打开新窗口该如何解决.....	98
26. 如何快速恢复误关闭的网页.....	98
27. 如何解决 IE 中的乱码现象.....	99
28. 清除高速缓存中的信息.....	99
29. 选择性清理 IE 地址栏输入记录.....	100
30. 清除自动完成内容.....	100
31. 清除浏览过的地址.....	100
32. 如何破解右键菜单中“源文件” 选项被禁用.....	101
33. 如何在网页解“锁”注册表.....	101
34. 如何破解浏览网页时硬盘被恶意 共享.....	102
35. 如何在自己的网页实现鼠标禁用.....	102
36. 别人浏览我的网页时, 如何让我的 主页添加到他们的标题栏中.....	102
37. 如何让别人浏览网页时, 使其硬盘 被动共享呢.....	103
38. 如何识别网上链接陷阱? 怎么杜 绝它.....	104
39. 对于网页上这些恶意的代码有没有 什么成功的处理软件, 请介绍一些.....	105
40. 如何使用上网助手修复 IE.....	106
41. 恶意网页对系统有哪些危害.....	106
42. 如何使用上网助手安全防护.....	107
43. 如何限制打开的网页内容.....	107
44. 如何解决 IE 不允许安装使用无效 签名的对象问题.....	108
45. 启用 IE 对 Windows 安装脚本的安全 提示.....	108
46. 如何禁止 IE 下载文件功能.....	108
47. 禁止 IE 自动播放动画.....	109
48. 如何在 IE 中禁止使用鼠标右键.....	109
49. 如何禁止更改浏览器主页.....	110
50. 禁止更改临时文件夹的设置.....	110
51. 如何取消 IE 自动保存密码的功能.....	111
52. 如何禁止用户更改安全级别.....	111
53. 禁止更改分组审查设置.....	111
54. 如何禁用“常规”选项卡.....	112
55. 如何解除网页文字无法复制.....	112
56. 禁止缓存自动代理脚本.....	113
57. 如何禁止“安全”选项卡.....	113
58. 如何禁止用户使用标识.....	113

59. 如何使 IE 在安全和非安全模式之间 切换时发出警告.....	114
60. 如何隐藏 IE 地址栏.....	114
61. 如何禁止在 IE 中使用“文件”→“另 存为”命令.....	114
62. 如何禁止 IE 访问某些站点.....	115
63. 如何禁用 IE 的“程序”选项卡.....	115
64. 如何限制 Internet 通信.....	115
65. 如何禁止 IE 自动安装不安全组件.....	116
66. 锁定 IE 工具栏来限制其他用户随意 添加按钮.....	116
67. 如何禁止用户更改添加到安全站点 中的网站.....	116
68. 如何禁止在浏览时查看网页源文件.....	117
69. 如何禁用 IE “高级”选项卡.....	117
70. 如何禁止更改 IE 代理服务器设置.....	118
71. 如何禁用 IE “内容”选项卡.....	118
72. 如何禁用 IE 的“连接”选项卡.....	119
73. 如何在 IE 中禁用或限制使用 Java 程 序及 ActiveX 控件.....	119
74. 自定义规则关闭 TCP139 端口.....	119
75. IE 收藏夹的备份.....	119
76. 发现可能有破坏性的下载文件.....	120
77. 备份和还原 Internet 信息服务配置 信息.....	120
78. 设置 IE 阻止弹出窗口.....	120
79. 管理 Internet 加载项.....	121
80. 阻止来自特定发布者的下载内容.....	121
81. 限制窗口覆盖屏幕.....	121
82. 启用防火墙保护所有网络连接.....	122
83. 如何将网页上的背景音乐保存下来.....	122
84. 手动配置数据执行保护.....	122
85. 解决降低 IE 安全级别设置问题.....	123
86. 提示出现 MS-4011 Exploit 漏洞.....	123

第4章 黑客入侵后的问题解决..... 126

4.1 黑客概述.....	126
1. 什么是黑客.....	126
2. 黑客攻击基本步骤有哪些.....	126
4.2 防范黑客攻击.....	126
1. 防止网络黑客入侵.....	126
2. 如何隐藏 IP 地址.....	127
3. 更改管理员账户.....	127
4. 禁止 Guest 账户的入侵.....	128

5. 黑客日常防范要点.....128	和连接.....140
6. 入侵者如何通过网络进行攻击.....128	21. 给 Windows XP 一把启动的密钥.....140
7. 如何封死黑客的后门.....129	22. 如何知道对方计算机名及用户名.....141
8. 隐藏网上邻居.....130	23. Windows 2000/XP 注册表快速恢复...141
9. 黑客是如何绕过防火墙限制的.....131	24. 修改注册表, 限制访问控制面板.....141
10. 什么是 TXT 炸弹.....131	25. 用注册表隐藏服务器.....141
11. 如何防范 TXT 炸弹.....131	26. 修改注册表, 设置 NTFS.....142
12. 应用 IP 策略防止 Telnet 登录.....132	27. 禁止普通用户访问系统属性.....142
13. 利用“路由和远程访问”组件防 Ping 命令探测.....133	28. 取消对网站的安全检查.....143
14. 阻止黑客和病毒对系统服务端口的 扫描.....133	29. 防范 WinNuke 的攻击.....143
4.3 端口安全问题.....133	30. 如何快速打开“服务管理器”.....143
1. 简单更改 Windows 2000 的 Telnet 端口.....133	31. 指定使用的程序.....144
2. 修改 Windows XP 的远程管理默认 端口.....134	32. 网络钓鱼攻击的防范.....144
3. 找出打开可疑端口的恶意程序.....134	33. 巧输密码防止被盗.....144
4. 屏蔽 Windows XP 的 3389 端口.....135	34. 如何识破假冒网上银行.....144
5. 停用系统远程终端服务.....135	35. 改变 ICF 常规服务端口躲避攻击.....145
6. 关闭 Windows 系统默认的 Telnet 服务.....135	4.4 防火墙问题.....145
7. 设置 FTP 服务器“只允许匿名 连接”.....136	1. 自定义规则开放 FTP 服务.....145
8. 关闭 Windows 2000/XP 系统 IIS 开启的 Web 服务.....136	2. 自定义规则 TCP 139 端口.....146
9. 关闭 Windows 2000/XP 系统 IIS 开启的 FTP 服务.....136	3. 什么是拒绝服务攻击.....146
10. 关闭 Windows 2000/XP 系统 IIS 开启 的 SMTP 服务.....137	4. 安装防火墙后为什么浏览网页变慢.....146
11. 关闭 Messenger 服务.....137	5. 设置 ICMP 允许在特殊需要时 Ping 本机.....146
12. 应用 TCP/IP 端口筛选管理开放端口...138	6. 综合应用防范 DDOS 攻击.....147
13. 关闭系统的文件共享服务的 139 端口.....138	7. 对防火墙进行系统测试.....147
14. 改变 FTP 服务器默认端口.....138	8. 自定义防火墙 IP 规则.....147
15. 在 Windows XP 中用 netstat 命令直接 查看端口与程序.....139	9. 防止渗透防火墙.....148
16. 设置地址转换保护上网安全.....139	10. 利用防火墙防止别人用 Ping 命令 探测.....148
17. 关闭 1900 端口.....139	11. 启用 Windows XP SP2 防火墙.....148
18. 使用 Fport 查看开放端口对应的 程序.....139	12. 指定 Windows 防火墙阻止所有未经 请求的传入消息.....149
19. 使用 Port Reporter 跟踪端口活动 状态.....140	13. 添加安全的例外程序通过防火墙.....149
20. 使用 Active Ports 查看本级活动端口	14. 在命令行下收信防火墙配置信息.....149
	15. 网络是怎样被入侵的.....150
	16. Symantec 防火墙的安装和使用.....150
	第5章 常用软件安全设置.....154
	5.1 办公文档设置.....154
	1. 如何隐藏文档记录.....154
	2. 利用 Word“版本”功能加密.....154
	3. 设置 Word 文档保护密码.....155
	4. 忘记了 Word 文档保护密码怎么办.....156
	5. 通过文档保护来保护 Word 文档.....156



6. 解除文档保护	157
7. 设置格式限制	157
8. 如何保护文档的局部内容	157
9. 防范宏病毒	158
10. 设置 Word 文档的编辑权限	158
11. 备份和恢复 Word 模板文件	158
12. 防止文档信息暴露隐私	159
13. 设置文档保护	159
14. 保护工作表	159
15. 保护单元格	159
16. 保护工作簿	160
17. 设置 Excel 文件的保护密码	160
18. 如何撤销工作簿保护	160
19. 如何撤销工作表的保护	161
20. 忘记了 Excel 文件的保护密码怎 么办	161
21. 隐藏 Excel 文件中的部分内容	161
22. 隐藏重要的行、列数据	162
23. 隐藏 Excel 工作表中重要的数据 部分	163
24. 设置 Access 数据库密码	163
25. 如何新建用户	163
26. 新建组	164
27. 如何设置用户和组的权限	164
28. 如何设置用户和组的权限	164
29. 设置用户隶属组	165
5.2 文档文件安全问题	165
1. 如何把普通 MDB 文件转换成 MDE 文件	165
2. 为什么杀毒后 Word 无法正常使用	165
3. 用 Word 打开损坏的 Excel 文档	165
4. 禁用 Word 文档访问记录	166
5. 禁用 Excel 文档访问记录	166
6. 清空文档列表	166
7. 打开 Word 文档时提示“文件中含有 宏”该怎么办	166
8. Microsoft Word 设置备份	167
9. 如何实现 Windows XP 文件夹的隐藏 和加密	167
10. 恢复没有响应的程序	168
11. 如何恢复 Office 文档	168
12. 利用 Office 2003 设置保存向导备份 Office 设置	168
13. 利用 Office 2003 设置保存向导还原	

Office 设置	168
14. 禁止多用户同时编辑 Word 文档	169
15. 如何防止他人偷看文档内容	169
16. 保存文档的同时保留备份	170
17. 防止突发事件导致文档丢失	170
18. Word 文档损坏后的修复	170
19. Normal.dot 模板损坏导致 Word 文档 损坏的修复	171
20. 清除 WPS 记录	171
21. 清除非法操作产生的“被挽救的 文档”记录	171
22. 利用文件加密机来加密文件	171
23. 使用 Hide In Picture 对文件进行伪 加密	172
24. 对图像文件进行加密	172
25. CMOS 密码	173
26. 禁止使用 HTML 文件作为墙纸	174
5.3 压缩文档的加解密	174
1. 使用 WinZip 加密压缩文档	174
2. 清除 WinZip 压缩文件使用记录	174
3. 清除 WinZip 历史文件夹内容	174
4. 清除 WinRAR 访问的历史文件	174
5. 备份和恢复 WinRAR 设置	175
6. 清除 WinRAR 压缩文档使用记录	175
7. RAR 和 ZIP 压缩包损坏的修复	175
8. 利用 WinZIP 来加密文件	176
5.4 修改注册表设置	176
1. 如何解除注册表的锁定	176
2. 锁定工具栏选项	176
3. 如何通过修改注册表, 删除共享	177
4. 如何隐藏“添加/删除 Windows 组件”	177
5. 如何利用注册表禁止用户改动桌面工 具栏	177
6. 如何清除“运行”记录	178

第6章 病毒木马问题及解决

6.1 病毒基础知识	179
1. 计算机病毒的定义及基本特征	179
2. 计算机病毒的传播途径	179
3. 病毒是如何通过网络进行传播的	180
4. 网络病毒陷阱有哪些	180
5. 网络传播病毒的特点有哪些	180
6. 计算机病毒的触发机制有哪些	181

7. 什么是蠕虫病毒.....	181	7. 如何进行引导型病毒的清除	194
8. 所有的平台上都会有蠕虫病毒吗.....	181	8. 如何拯救 CIH 病毒破坏的数据.....	194
9. 什么是变种病毒.....	181	9. 硬盘中所有的 EXE 和 DLL 类型文件 都找不到	195
10. 驻留型内存与不驻留型病毒有什么 不同.....	182	10. 如何清除开机型病毒	195
11. 什么是逻辑炸弹.....	182	11. Format 命令能否去除病毒	195
12. 电脑病毒与逻辑炸弹有什么异同.....	182	12. “尼姆达”病毒的防范与清除	195
13. 为什么要更新扫描引擎和病毒码.....	182	13. 清除尼姆达病毒后如何解决 Office 运行异常问题	196
14. 病毒破坏的表现.....	182	14. 感染文件型病毒后的处理方法	196
15. 病毒发作时的表现形式有哪些.....	183	15. 彻底清除主引导区病毒	196
16. 病毒发作后的表现现象.....	183	16. 防御脚本病毒	196
17. 电脑病毒的工作过程.....	183	17. 如何禁止病毒发作后的自动复制 功能	196
6.2 病毒的防护.....	184	18. 如何禁止病毒发作利用 CDO 传播	197
1. 如何有效预防病毒的侵害.....	184	19. 如何禁止 SYN 洪水攻击	197
2. 感染病毒后的解决方法.....	184	20. 如何防止网页脚本病毒执行	197
3. 杀毒软件有哪些使用技巧.....	185	21. 如何防止 ICMP 重定向报文的攻击... ..	198
4. 使用的杀毒软件是否越多越好.....	187	22. 怎样避免间谍软件	198
5. 查杀病毒时的注意事项.....	188	23. 怎样防范“新硬盘杀手”	198
6. 将常用的安全网站放到收藏夹.....	188	24. 下载安装 Funlove 病毒免疫程序	198
7. 卸载 Scripting Host, 防范代码攻击	188	25. 用抓包工具“揪”出电脑病毒	198
8. 利用 BIOS 设置防病毒.....	188	26. 使用 Windows 系统控制台删除病毒 文件	198
9. 根据进程名查杀病毒.....	188	6.4 使用金山毒霸杀毒	199
10. 根据进程号查杀病毒.....	189	1. 金山毒霸 2006 的安装、注册和工作 界面	199
11. 防止 ActiveX 控件绕过 IE.....	189	2. 使用金山毒霸 2006 查杀病毒	199
12. 图片病毒的防范.....	189	3. 如何使用杀毒设置	200
13. 怎样使用批处理文件防范病毒.....	189	4. 如何创建应急盘	201
14. 设置注册表权限防病毒启动.....	190	5. 如何进行防毒设置	202
15. 遇上最新病毒怎么办.....	190	6. 用金山毒霸修复 EXE 文件关联.....	205
16. 备份文件时备份中了病毒, 备份是 否无用.....	190	7. 突破分区访问限制	205
17. 计算机的可执行文件不能运行是不 是因为中了病毒.....	190	8. 为何用金山毒霸查杀 Word 宏病毒后, Word 程序启动就会出现错误.....	205
18. 光盘会带计算机病毒吗? 如何清除... ..	190	9. 使用金山毒霸查杀病毒, 为何在进行 磁盘碎片整理等磁盘操作中会死机	205
19. 浏览有病毒的软盘是否会中毒.....	191	6.5 使用 KV2006 杀毒.....	205
20. 怎样解决一启动计算机硬盘就会被 共享的问题.....	191	1. 怎样升级 KV2006.....	205
6.3 典型病毒的防护.....	191	2. 怎样进行 KV2006 系统设置.....	205
1. 什么是宏病毒.....	191	3. 怎样使用 KV2006 制作 DOS 杀毒盘... ..	207
2. 怎样识别宏病毒.....	191	4. 怎样使用 DOS 杀毒盘进行杀毒	207
3. 怎样预防与删除宏病毒.....	192	5. 怎样制作硬盘修复王	207
4. 如何做好邮件的病毒防护.....	192	6. 如何对 KV2006 进行备份和恢复.....	207
5. 振荡波等蠕虫病毒的攻击目标及 危害.....	193		
6. 如何清除冲击波病毒.....	194		



7. 如何使用 KV2006 保护隐私信息.....	208
6.6 卡马基杀毒软件的使用.....	209
6.7 Norton Antivirus 的使用.....	212
6.8 木马的防护.....	214
1. 什么是木马.....	214
2. 木马的类别.....	215
3. 木马是如何入侵的.....	216
4. 木马是如何运行的.....	216
5. 木马是如何实现盗号的.....	216
6. 如何预防木马.....	217
7. 怎样杀除木马.....	217
8. 木马程序具有哪些激活方式.....	218
9. 怎样消除“冰河”木马.....	219
10. 如何从进程里查看是否有木马.....	219
11. 如何使用木马分析专家检测木马.....	219
12. 如何使用反间谍专家检测木马.....	220
13. 如何使用反黑精英查杀木马.....	222
14. 怎样清除 NetSpy 木马.....	223
15. 如何彻底防御网络游戏外挂木马.....	223
16. 禁止硬盘 AutoRun 功能预防木马运行.....	224
17. 查杀反弹型端口木马.....	224
18. 反弹型端口木马的防范.....	224
19. 巧妙分离带木马文件.....	225
20. 禁止利用 TTL 值来鉴别操作系统类型.....	225
21. 防范 PHP 木马攻击.....	225
22. 如何发现和手工清除 QQ 木马变种病毒.....	226
23. 清除 ShareAll.....	226
24. 清除 MastersParadise.....	226
25. 清除 Malicious.....	226
26. 怎样利用 Windows 命令检查系统是否感染木马.....	226
27. 创建登录用户防范 Guest 账户入侵.....	227
28. 防范利用 Word 文档执行木马.....	227
29. 怎样查找隐藏在注册表非启动项下的木马.....	227
30. 怎样查找组策略的木马.....	227
31. 防范传奇木马.....	228
32. 怎样手工清除嵌入式 DLL 木马.....	228
33. 禁止使用 Windows 2000 输入法漏洞入侵.....	229

34. 清除“蓝色火焰”.....	229
35. 清除黑洞 2001.....	229
36. 清除 Win2000 密码大盗.....	229
37. 清除“后门”木马.....	230
38. 清除 Funny Flash.....	230

第7章 聊天工具的安全设置..... 231

7.1 QQ.....	231
1. 如何隐身登录 QQ.....	231
2. 如何拒绝陌生人的消息.....	231
3. 如何清除 QQ 登录窗口中的 QQ 号码列表.....	231
4. 如何拒绝陌生人消息?.....	232
5. 避开木马盗取 QQ 密码的技巧.....	232
6. 使用代理服务器防止暴露真实的 IP 地址.....	232
7. 怎样防止他人登录你的 QQ.....	233
8. QQ 密码的本地保护.....	233
9. 如何将自己的 QQ 彻底隐身.....	234
10. 如何使用 QQ 病毒专杀工具.....	234
11. 如何在线查杀 QQ 病毒.....	235
12. 在网吧上网如何清除 QQ 登录记录.....	235
13. 怎样把自己的摄像头隐藏起来.....	235
14. 在 Windows XP 系统中如何拒绝接收 QQ 广告.....	236
15. “QQ 尾巴”病毒怎样清除.....	236
16. 怎样清除“QQ 缘”病毒.....	237
17. 如何清除“武汉男孩”病毒.....	237
18. 如何清除“QQ 女友”病毒.....	238
19. 如何清除“爱情森林”病毒.....	238
20. 如何应对“飘叶 OICQ 千夫指”.....	239
7.2 MSN.....	239
1. 如何撤销 MSN 自动登录.....	239
2. 怎样防止自己的聊天记录曝光.....	239
3. 如何让杀毒软件自动扫描接收文件.....	240
4. 怎样才能阻止不受欢迎的客人.....	240
5. 怎样防止自己的电子邮件曝光.....	241
6. 如何禁止将 MSN 联系人名单储存在计算机上共享.....	241
7. 如何防止他人未经授权访问个人用户信息.....	241
8. 怎样认识和清除“MSN 密码盗贼”.....	242
9. 如何认识和清除“MSN 小尾巴”.....	242

10. 如何清除“MSN 性感鸡” (MSN. DropBot.b)	242	8.2 安全使用 Web 邮箱	254
7.3 POPO	243	1. 怎样有效防止垃圾邮件	254
1. 如何让自己的 POPO 拒绝陌生人的 消息	243	2. 什么是邮件炸弹	254
2. 如何设定权限避免自己被打扰	243	3. 怎样防止邮件炸弹的攻击	255
3. 怎样为共享文件夹设置访问密码	243	4. 垃圾箱里有新邮件怎么办	255
4. 如何让自己 POPO 的密码得到保护	244	5. 为什么发的邮件对方收不到	255
7.4 UC	244	6. 为什么用很长时间写的邮件在发送时 却找不到了	255
1. 怎样在新浪 UC 上进行安全设置	244	7. 无法登录 Web 邮箱	256
2. 如何申请新浪 UC 密码保护	245	8. 怎样安全地使用 Web 邮箱收发邮件	256
3. 怎样在 UC 中防止垃圾邮件	245	9. 收到电子贺卡时中了毒	256
第 8 章 电子邮件安全防守	246	10. 收到多封开头一样的电子邮件	257
8.1 安全使用 Outlook Express	246	11. 使新窗口不断打开直至死机的空白 电子邮件	257
1. 如何在 Outlook Express 中对信件设置 密码保护	246	12. 新浪邮件如何设置垃圾邮件	258
2. 浏览邮件后系统不断自动打开窗口该 怎么办	247	8.3 安全使用 Foxmail	258
3. 如何备份和恢复 Outlook Express 中的 重要数据	247	1. 如何保证 Foxmail 收发邮件的安全	258
4. 怎样彻底清除 Outlook Express 邮件	247	2. 如何为账户设置访问口令	258
5. 如何拒收收件人不是自己的垃圾邮件	248	3. 如何为账户指定证书	259
6. 发送数字签名或加密邮件	249	4. 如何发送签名和加密邮件	259
7. 找回用户标识密码	249	5. 如何接收签名和加密邮件	259
8. 设置邮件自动过滤	249	6. 修改与取消账户口令	259
9. 防范邮箱炸弹	250	7. 忘记账户密码怎么办	259
10. 如何隐藏发信人的地址	251	8. 设置 Foxmail 垃圾邮件过滤	260
11. Outlook Express 中的邮件偶尔会丢失 怎么办	251	9. 设置 Foxmail 的黑名单	260
12. 恢复误删的地址簿	251	10. 如何让 Foxmail 学会识别垃圾邮件	260
13. 恢复丢失的邮件附件	251	11. 如何清除邮件炸弹	261
14. 只能收信不能发信	252	12. 备份 Foxmail	261
15. 怎样禁止其他程序暗中发送邮件	252	13. 如何让 Foxmail 的启动更快	262
16. 怎样隐藏邮件	252	14. 更改 Foxmail 的邮件存储位置	262
17. 怎样备份 Outlook Express 中的邮件	253	15. 追查匿名邮件的地址	262
18. 备份和还原 Outlook Express 中的 账户	253	16. 如何防止 Foxmail 中文域名解析 漏洞	262
19. 怎样备份 Outlook Express 中的邮件 规则	253	17. 消除 Foxmail 地址自动记忆功能	263
20. 怎样还原 Outlook Express 中的邮件 规则	254	18. 禁止 Foxmail 日志文件再次记录操作 信息	263
21. 怎样解决 Outlook Express 无法下载 图片的问题	254	19. 如何为不同用户邮件打上不同的 标记	264
		20. 如何为 Foxmail 文件夹加密	264
		21. 接收邮件前清除垃圾邮件	264
		22. 退出 Foxmail 时自动清理废件箱	264
		23. 怎样备份和还原 Foxmail 账户	264
		8.4 安全使用 Outlook	265
		1. 为 Outlook 设置密码保护	265



2. 怎样自动删除含有特定名称的病毒.....	265
3. 怎样自动删除符合过滤条件的垃圾邮件.....	266
4. 如何禁用 Outlook 的邮件自动预览功能.....	267
5. 如何为重要邮件加标记.....	267
6. 如何让邮件自动分拣.....	267
7. 怎样在 Outlook 中设置自动过滤垃圾邮件.....	268
8. 怎样取消自动记忆邮箱口令.....	268
9. 怎样收取安全的.exe 附件.....	268
10. 怎样有选择地发送和接收邮件.....	268
11. 怎样自动删除已发送的邮件.....	269
12. 怎样让 Outlook 只接收安全收件人的邮件.....	269
13. 如何更改电子邮件和附件的保存位置.....	269
14. 如何防止 Outlook 自动将病毒邮件寄出.....	269
15. 如何安全地阅读电子邮件.....	270
16. 如何设置 Outlook 中的安全区域.....	270
17. 如何解除 Outlook 的附件限制.....	270
18. 如何删除不安全的附件.....	271
19. 如何备份 Outlook 2003 的个人目录.....	271
20. 强制 Outlook 以纯文本方式读邮件.....	272

第9章 由IP地址查找及锁定目标273

1. 如何在命令行提示符状态查看本机的IP地址.....	273
2. 监视 MAC 地址追踪 IP 盗贼.....	273
3. 设置代理服务器隐藏 IP 地址.....	274
4. 怎样彻底隐藏上网 IP.....	274
5. 启用 ICF 阻止 IP 欺骗.....	274
6. 如何解决 IP 地址冲突的问题.....	275
7. 如何捆绑 MAC 地址和 IP 地址.....	275
8. 怎样在 Windows 窗口中查看本机的 IP 地址.....	275
9. 如何通过 IP 查询地理位置.....	275
10. 如何知道对方的 IP 信息.....	276

第10章 数据备份与恢复277

10.1 硬盘数据的备份与恢复.....	277
1. 数据资料面临的危险.....	277

2. 使用 Diskgen 软件备份分区表.....	277
3. 使用 Diskgen 软件恢复硬盘分区表.....	277
4. 使用 Diskgen 重建硬盘分区表.....	278
5. 使用 KV 硬盘修复王备份硬盘分区表.....	278
10.2 系统文件的备份与恢复.....	278
1. 备份硬件配置文件.....	278
2. 备份 Windows 2000/XP 注册表.....	279
3. 恢复 Windows 2000/XP 注册表.....	279
4. 在 Windows XP 中使用计划任务完成数据备份.....	279
10.3 Windows 系统备份与恢复.....	280
1. 备份 Windows 2000 系统.....	280
2. Windows 2000 的系统还原.....	281
3. Windows XP 系统的备份.....	282
4. Windows XP 系统的还原.....	283
5. 制作 U 盘系统备份/恢复盘.....	283
6. 使用系统文件检查器修复系统文件.....	284
10.4 驱动程序的备份与恢复.....	285
1. 使用驱动精灵备份驱动程序.....	285
2. 使用驱动精灵恢复驱动程序.....	285
3. 使用驱动精灵备份数据.....	286
4. 使用驱动精灵备份 IE 收藏夹.....	286
5. 使用驱动精灵恢复数据.....	286
6. 使用驱动精灵安装驱动程序.....	286
10.5 磁盘分区和文件的备份与恢复.....	287
1. 使用 EasyRecovery 恢复文件.....	287
2. 使用 Ghost Explore 恢复文件.....	289
3. 使用百诺备份专家.....	289
4. 使用 FinalData 拯救数据.....	291
5. 备份和还原系统字体.....	292
6. 进入“安全模式”修复 Windows XP.....	292
7. 安装故障恢复控制台.....	292
8. 备份和还原 Windows XP 激活文件.....	292
10.6 注册表备份与恢复.....	292
1. 如何备份注册表.....	292
2. 在什么情况下需要备份注册表.....	293
3. 在 Windows 2000/XP/2003 系统中手工备份注册表.....	293
4. 在 DOS 下恢复注册表.....	293
5. 利用系统自带备份工具备份注册表.....	293
6. 利用系统自带备份工具还原注册表.....	294
7. 利用系统安装光盘恢复注册表.....	294
8. 利用紧急修复盘恢复注册表.....	294

第1章 Windows 2000/XP 安全

终极解疑

1.1 用户安全问题

从 Windows 2000 系统开始, PC 操作系统采用了用户身份认证的机制来控制用户对系统资源的设置和访问, 不同身份级别的用户登录系统后只能根据他拥有的访问权限对计算机进行操作。例如: 管理员身份的用户可以完全控制计算机, 并且可以对其他用户的可访问权限进行设置; 而受限用户则会受到访问权限的限制, 很多项目对于他们来说都是禁用的。正是由于不同身份账号对系统访问能力的差异, 要求人们必须合理地进行用户账号的设置, 以此来保证用户的安全。

1. 如何把系统 Administrator 账号改名

将系统 Administrator 账号改名也就是将账号名称改为其他人不易知晓的名称, 变共知为未知。这样即使登录密码设置的比较简单, 其他用户在不知道登录账号名称的情况下, 也很难非法进入系统。为 Administrator 账号变身是通过设置组策略来实现的。具体的操作如下:

(1) 单击“开始”→“运行”命令, 弹出“运行”对话框, 在“打开”文本框中输入 gpedit.msc 命令, 打开“组策略”窗口, 如图 1-1 所示。

(2) 在“组策略”窗口, 依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”。在右侧窗格中, 双击“账号, 重命名系统管理员账户”策略, 在如图 1-2 所示的策略属性窗口中输入新的内置的管理员账号名称, 单击“确定”按钮即可。

2. 如何建立两个管理员账号

Administrator 账号是 Windows 2000/XP 系统内

建的管理员用户, 具有对系统最大的管理权限。作为一个共知的用户账号, 黑客软件、恶意代码或是病毒通常利用这个特性, 针对该用户进行登录密码探测, 一旦得到登录密码后就可以轻易入侵到系统中。由于 Administrator 用户具有全部的系统访问权限, 因此系统被入侵后, 可能会造成很严重的后果。

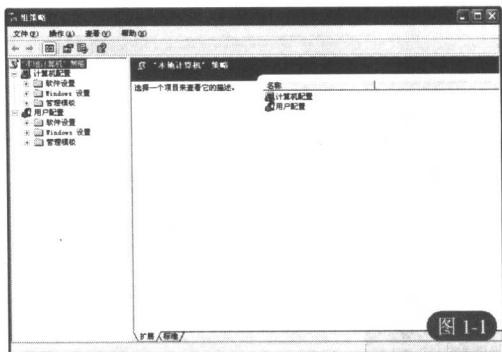


图 1-1

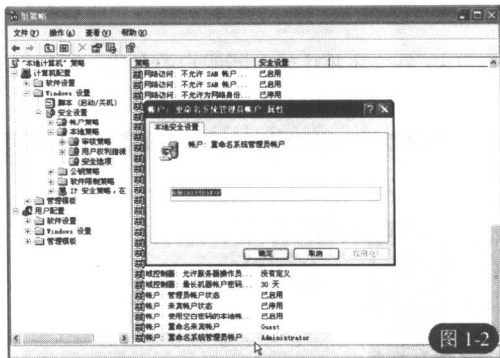


图 1-2

为了迷惑黑客, 用户可以创建两个管理员账号, 一个具有一般权限的用户用来收信以及处理一些日常事务, 另一个拥有 Administrator 权限的用户只在需要时使用。

(1) 打开“控制面板”窗口, 单击“用户账户”项, 如图 1-3 左所示, 弹出“用户账户”窗口, 如图 1-3 右所示。



图 1-3

(2) 选择“创建一个新账户”选项，弹出如图 1-4 所示的窗口。

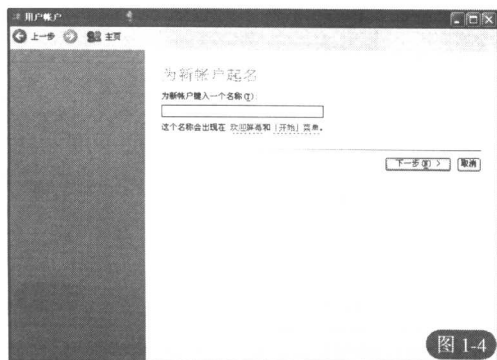


图 1-4

(3) 在文本框中输入新账户的名称，例如 X，单击“下一步”按钮，弹出如图 1-5 所示的窗口。

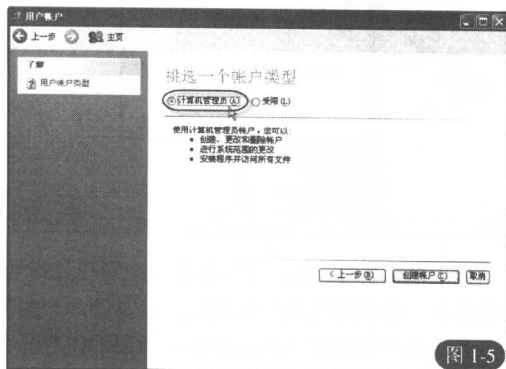


图 1-5

(4) 在对话框中选中“计算机管理员”单选按钮，单击“创建账户”按钮，即可建立一个新的管理员账户，如图 1-6 所示。

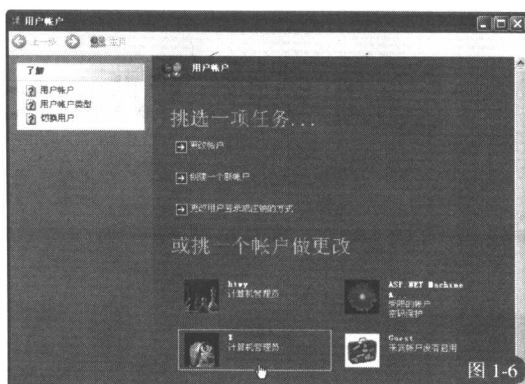


图 1-6

3. 如何禁用 Guest 账号

启用 Guest 账号时，没有账户的用户可以以来宾的身份登录到此计算机，但是他们不能访问受密码保护的文件、文件夹或设置。禁用 Guest 账号后，没有账户的用户就不能登录到该计算机，这在一定程度上保证了计算机安全。

在实际的应用中，人们很少会使用到 Guest 账号，因此将 Guest 账号停用不会影响到人们的正常使用，同时也可以彻底消除由 guest 账号引起的一些安全隐患。

禁用 Guest 账号的具体操作步骤如下：

(1) 右击桌面的“我的电脑”图标，从弹出的快捷菜单中单击“管理”命令，进入“计算机管理”窗口，如图 1-7 所示。

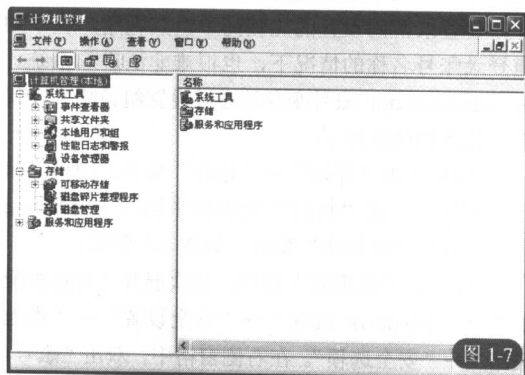


图 1-7

(2) 在“计算机管理”中，依次展开“系统工具”→“本地用户和组”→“用户”，在右侧窗格中双击 Guest 项，在属性设置窗口，选择“账户已停用”选项，如图 1-8 所示。