


Computer
Hospital

电脑 医院



系统的
安全性

注册表
优化

隐私
保护

木马
查杀

数据安
全修复

电脑安全防护

——系统优化、病毒查杀、木马防御、
黑客攻防、恶意网站防范

力诚教育 编著

方便：让你足不出户，就请来一位电脑专家，让电脑得到专业的维护

快捷：提供有效的解决方案以及种种电脑疑难问题的应对技巧

经济：图书+光盘，丰富实用的典型案例，即查即用物超所值

可靠：作者系专业权威人士，经验丰富，所有案例都经验证



电子科技大学出版社



配套多媒体教学光盘

图书在版编目 (CIP) 数据

电脑安全防护 / 力诚教育编著. — 成都: 电子科技大学出版社, 2008.3

(电脑医院)

ISBN 978-7-81114-706-3

I. 电… II. 力… III. 电子计算机—安全技术 IV. TP309

中国版本图书馆 CIP 数据核字 (2008) 第 000021 号

内 容 提 要

本书以电脑安全防护为主题, 从系统优化到网络安全, 从数据备份到数据恢复, 从安全策略到安全误区, 从病毒查杀到黑客预防, 全面介绍了电脑安全方面的各种应用技巧。主要内容包含, Windows XP/Vista 优化与设置、注册表优化、BIOS 密码设置、优化软件的使用、增强系统的安全性、系统安全限制和隐私保护、文档与文件夹安全防护、木马查杀和预防、Internet 安全设置、电子邮件安全设置、即时聊天工具安全设置和防火墙设置、系统/数据备份和还原等内容。

本书分类细致, 便于查找, 讲解清晰, 能够做到一学就会, 切实解决电脑安全问题。不但可以作为从事电脑工作人员的参考用书, 还可以作为个人电脑爱好者和办公室的工作人员进行电脑维护的指导用书。

电脑医院
电脑安全防护
力诚教育 编著

出 版: 电子科技大学出版社 (成都市一环路东一段 159 号电子信息产业大厦 邮编: 610051)

策划编辑: 张蓉莉

责任编辑: 李小锐 唐雅邻

主 页: www.uestcp.com.cn

电子邮箱: uestcp@uestcp.com.cn

发 行: 新华书店经销

印 刷: 四川墨池印务有限公司

成品尺寸: 210mm×260mm 印张 20 字数 559 千字

版 次: 2008 年 3 月第一版

印 次: 2008 年 3 月第一次印刷

书 号: ISBN 978-7-81114-706-3

定 价: 38.00 元 (含 1CD)

■ 版权所有 侵权必究 ■

- ◆ 本社发行部电话: 028-83202463; 本社邮购部电话: 028-83208003
- ◆ 本书如有缺页、破损、装订错误, 请寄回印刷厂调换。
- ◆ 课件下载在我社主页“下载专区”。

前 言

PREFACE

电脑 医院

你身边的电脑专家

你可曾遇到这样的问题：

1. 电脑越来越慢，Pentium 4 的机器比别人 Pentium 2 的还慢……
2. 电脑经常中毒，病毒猖狂使你疲于应付……
3. 卖电脑的商家不知去向，偏偏电脑又出问题……
4. 打开电脑噪音大，让你无法正常工作和入睡……
5. 抱着电脑大老远去电脑城维修，维修人员说的根本听不懂……

那么赶快求助《电脑医院》：

1. 方便：让你足不出户，就请来一位电脑专家，让电脑得到专业的维护；
2. 快捷：解你燃眉之急，提供有效的解决方案以及种种电脑疑难问题的应对技巧；
3. 经济：图书+光盘，丰富实用的典型案例，即查即用物超所值；
4. 可靠：编者系专业权威人士，经验丰富，所有案例都经验证，以确保万无一失。

《电脑医院》系列图书是编者根据市场发展、读者需求而策划、编著的权威产品，必定成为电脑图书业界的强悍力作。

全系列图书从电脑的常见故障、日常维护、系统故障、应急处理以及安全防护 5 个方面入手，囊括了日常生活与工作中电脑的常见故障，全系列图书包括：

1. 《电脑常见故障排查》：硬件、软件、操作系统、网络、外设、数码设备故障诊断与排除
2. 《电脑日常维护与疑难解答》：硬件维护、系统维护、常用软件维护、优化升级、网络维护、笔记本电脑维护
3. 《电脑急救》：死机、黑屏、硬盘修复、系统故障、数据备份与恢复
4. 《Windows XP/Vista 故障排查》：全新疑难解答、蓝屏代码剖析、操作技巧救急、系统安全设置与保护
5. 《电脑安全防护》：系统优化、病毒查杀、木马防御、黑客攻防、恶意网站防范

遇到不认识的字，可以查阅新华字典；遇到电脑故障，可以查阅《电脑医院》。拥有《电脑医院》，你将拥有一套最权威的电脑故障速查宝典。

>>> 本书内容

电脑的使用过程中，经常会出现突发的死机、黑屏、重新启动电脑，或者电脑反应速度很慢的现象，而大多数用户针对这些故障现象往往显得无从下手。其实，任何故障在出现前都可以通过采取相应的措施来避免，这就是对电脑进行定期的维护。维护电脑不仅需要专业的知识，还要有合理的方法。因此，本书针对维护电脑的各种操作进行有序的讲解，并用大量实例图片说明，让初学者按照提示能够自己轻松做到电脑的维护。本书还收集了大量电脑典型故障，并给出了包括硬件故障排除、操作系统故障排除、应用软件故障排除等内容，使读者参照典型故障就能够解决大多数电脑使用过程中遇见的问题。

>>> 本书特点

- * 真正的目的是：“解决遇到的问题”，而非学习电脑相关知识。
- * 读者只需在目录中对应找到问题，解答就在书中。
- * 难度最低，普通电脑使用者即可跟着学，跟着做排除问题。
- * 即使遇到本书没有介绍的问题，依然有“故障排除的方法步骤与原则”可协助解决问题。
- * 大开本双栏排版，知识信息量大，一本 300 页的书装了 600 页的内容。
- * 能帮你省钱的书，每解决一个问题，即可减少数十至数百元的维修费用。

>>> 配套光盘

本书专门配套了一张多媒体教学光盘，通过语音讲解、动画演示的方式，生动地再现了故障排除的全过程。读者不必再担心专业知识难以理解，就像有一位电脑专家在身边，手把手地教你每一步该如何操作，轻松排除电脑的各种疑难杂症。

>>> 读者对象

本书行文活泼流畅、易读、易懂，所有知识内容都是笔者大量长期积累的经验，让你能够随时精心呵护你的电脑，掌握日常电脑维护知识；让你能够对各种疑难问题做到自己解决，迅速成为电脑应用高手。本书适合电脑爱好者自学及作为培训班的教材。

本书由力诚教育编著。由于编者水平有限，错误之处在所难免，敬请广大读者和同行批评指正。

CD INTRODUCTION

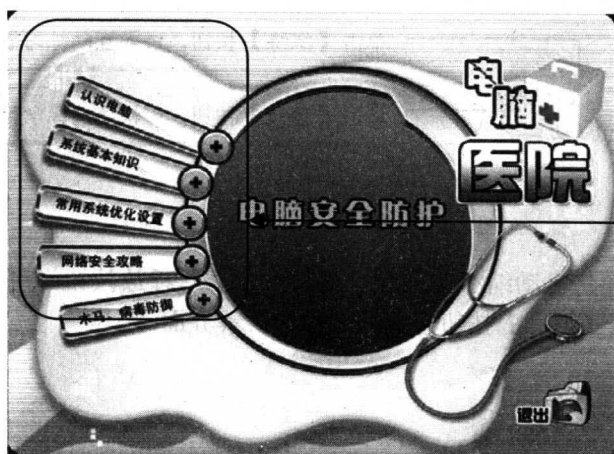
光盘说明

一、光盘主要内容

配套多媒体自学光盘通过语音讲解、动画演示的方式，形象而生动地讲解了本书主要内容，同时提供互动练习功能，使读者能够边学边练，轻松掌握。

二、操作方法

将本光盘放入光驱，几秒钟后光盘将自动运行。如果没有自动运行，可在桌面双击【我的电脑】图标，在打开的窗口中双击光驱所在盘符，或者右击光盘所在盘符，在弹出的快捷菜单中选择“自动播放”命令，即可启动并进入多媒体自学光盘主界面。



视频讲解内容

常用系统设置
常见系统问题
常用小窍门
安全应用知识
网络应用知识

单击光盘主界面左边的选项按钮，可以进入视频讲解分界面。分界面中罗列出了对应该视频讲解的多个知识点。



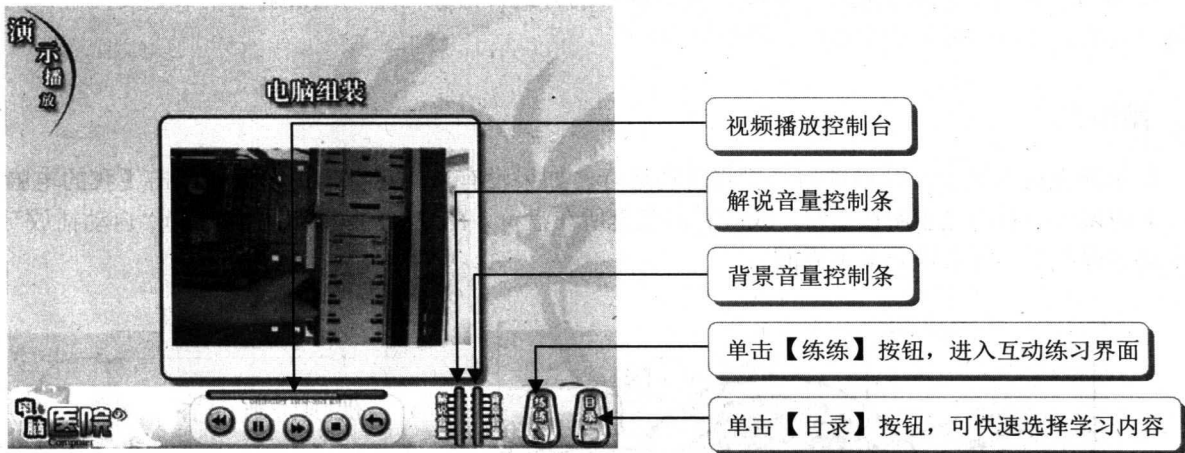
单击后，返回到光盘主界面

单击知识点选项，
进入所对应的视频讲解界面

单击后，退出光盘

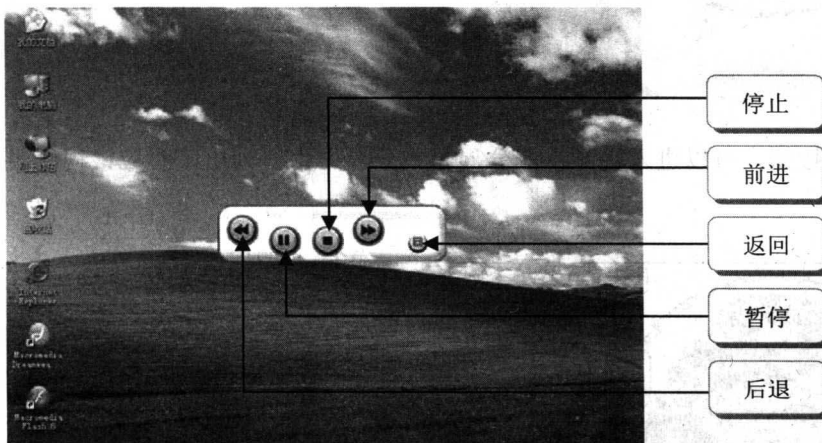
>>> 视频讲解界面

视频讲解界面中各控制按钮的功能如图所示。



>>> 互动练习界面

单击【练练】按钮, 进入互动练习界面, 画面将自动缩小并出现“播放按钮”。“播放按钮”可以拖放到屏幕任意位置, 读者可以根据讲解边学边做。单击【返回】按钮将返回到视频讲解界面。



三、运行环境及注意事项

为了你能流畅地使用光盘, 建议你的计算机使用以下配置:

处理器 1000MHz 以上

分辨率 800×600 像素以上

内存 256MB 以上

光驱 32 倍速以上

操作系统 Windows 98/Me/2000/XP/Vista

本光盘属于多媒体光盘 (CD-ROM), 只适用于电脑光驱, 不能在 VCD、DVD 机上使用。本手册所提供的所有源文件及素材仅供练习使用, 不得用于任何商业用途, 否则后果自负。



目 录

第一章 系统入侵与加密

1.1 Windows 系统安全分析.....	2
1.1.1 安全缺陷产生的原因.....	2
1.1.2 系统安全透析.....	2
1.2 Windows 安全操作策略.....	3
1.3 系统漏洞攻防.....	7
1.3.1 Net BIOS 漏洞的入侵和防御.....	7
1.3.2 IPC\$漏洞的入侵与防范.....	10
1.3.3 RPC 漏洞入侵和防范.....	13
1.3.4 Windows 2000 输入法漏洞的入侵 与防范.....	15
1.4 系统的加密.....	17
1.4.1 设置开机密码.....	17
1.4.2 破除 CMOS 密码.....	17
1.4.3 Windows 系统账户管理与设置.....	19
1.4.4 休眠和屏保的加密保护.....	32
1.5 Windows 加密文件系统.....	35
1.5.1 什么是 EFS 系统.....	35
1.5.2 如何在 NTFS 文件系统中对文件 和文件夹加密.....	36
1.5.3 如何用 cipher 命令进行加解密.....	36
1.5.4 复制加密的文件或文件夹.....	37
1.5.5 在 Windows XP 中查找已经被加密	

的文件.....	37
1.5.6 对加密文件进行解密.....	38
1.5.7 其他 Windows 系统加密技巧.....	38
1.6 系统漏洞扫描.....	45
1.6.1 使用扫描器检查系统漏洞.....	45
1.6.2 在线扫描发现系统漏洞.....	45
1.6.3 使用 SSS 软件检测系统安全漏洞.....	45
1.6.4 瑞星漏洞扫描工具扫描系统漏洞.....	46
1.6.5 共享扫描工具扫描开放共享.....	47
1.6.6 金山毒霸漏洞扫描.....	47
1.6.7 微软安全检测工具 MBSA.....	48
1.6.8 BigFix 工具查找漏洞补丁.....	49
1.6.9 ARP-Killer 软件的使用.....	49
1.6.10 SSH 软件保证远程安全登录.....	49
1.6.11 WebDAV 扫描个人服务器漏洞.....	50
1.6.12 局域网中的嗅探精灵——IRIS.....	50
1.6.13 为 Windows 安装补丁和升级.....	51
1.6.14 在 Windows XP 中安装数字认证书.....	52
1.6.15 为 Windows XP 安装 SP2 补丁.....	53
1.6.16 让初装系统具备免疫力.....	53
1.6.17 添加/删除程序中查看更新情况.....	53
1.6.18 ADODB.Stream 漏洞防范工具.....	54

第二章 Windows XP 安全策略

2.1 用户安全设置问题.....	56
-------------------	----



2.1.1 建立多个系统管理员账号.....	56	2.4.1 禁止使用注销功能切换登录用户名.....	70
2.1.2 禁止使用 Guest 来宾账号.....	57	2.4.2 禁止使用“网上邻居”访问共享资源...	70
2.1.3 限制多余或不必要的账户.....	57	2.4.3 禁止使用“添加/删除程序”.....	71
2.1.4 创建陷阱用户.....	58	2.4.4 禁止远程编辑注册表.....	71
2.1.5 按下电源按钮时弹出询问对话框.....	58	2.4.5 禁止使用.reg 格式的文件.....	71
2.1.6 取消 Windows 登录时的启动画面.....	59	2.4.6 禁止使用“开始”菜单里的“运行” 命令.....	72
2.1.7 启动时使用批处理文件删除默认共享...	60	2.4.7 禁止在计划任务文件夹中添加删除 任务.....	72
2.2 密码安全设置问题.....	61	2.4.8 禁止使用“我的电脑”.....	72
2.2.1 设置开机密码.....	61	2.4.9 禁止使用“我的文档”.....	73
2.2.2 设置 Windows 密码.....	61	2.4.10 禁止从“我的文档”运行文件.....	73
2.2.3 设置屏幕保护密码.....	62	2.4.11 禁止打印机共享.....	73
2.2.4 设置休眠退出密码.....	62	2.4.12 禁止使用 MS-DOS.....	73
2.3 Windows 系统安全设置.....	63	2.4.13 禁止修改“显示”属性.....	74
2.3.1 安装系统时应该设置管理员密码.....	63	2.4.14 禁止删除打印机.....	74
2.3.2 设置系统启动密码.....	63	2.4.15 设置退出系统而不保存设置.....	74
2.3.3 设置系统密匙盘.....	64	2.4.16 禁止修改文件夹存放路径.....	75
2.3.4 快速锁定桌面.....	65	2.4.17 禁止移动“开始”菜单.....	75
2.3.5 Windows XP 文件夹属性均为只读 属性.....	65	2.4.18 锁定计算机.....	75
2.3.6 停用 Windows XP 的启动密码.....	66	2.4.19 禁止文件共享.....	76
2.3.7 更改 Windows XP 的密码.....	66	2.4.20 禁止拨入访问.....	76
2.3.8 制作 Windows XP 的密码恢复盘.....	67	2.4.21 隐藏桌面上的系统图标.....	76
2.3.9 利用恢复盘恢复丢失的密码.....	67	2.4.22 屏蔽系统所有的热键.....	77
2.3.10 设置 Windows XP 的安全登录或 注销.....	68	2.4.23 禁止在登录框中直接关闭计算机.....	77
2.3.11 使用 Windows XP 的系统还原功能.....	68	2.4.24 禁止查看和更改任务的属性.....	77
2.3.12 快速关机和重启.....	69	2.4.25 禁止.inf 格式的文件运行.....	77
2.3.13 必不可少的系统管理工具.....	69	2.4.26 禁止“屏幕保护程序”选项卡.....	78
2.4 系统安全限制.....	70	2.4.27 禁止使用控制面板里的“网络” 图标.....	78



2.4.28	指定“控制面板”显示的项目	79	2.6.15	设置专用文件夹	94
2.4.29	禁止系统的自动升级	79	2.6.16	NTFS 分区下显示“安全”选项	94
2.4.30	禁止使用“任务栏属性”	80	2.6.17	隐藏文件的创建日期	95
2.4.31	禁止查看事件日志	80	2.6.18	更改文件夹图标	95
2.4.32	设置系统日志的保存时间	80	2.6.19	使用 Desktop.ini 加密文件	95
2.4.33	禁止系统从软驱启动	81	2.6.20	Copy 命令合并隐藏文件	95
2.4.34	限制 Windows 密码的长度	81	2.6.21	利用“文件签名策略”保护数据	96
2.4.35	禁止使用系统的压缩功能	81	2.6.22	设置 Control.ini 保护系统	96
2.4.36	禁止使用缩略图缓存	81	2.6.23	类标识符“隐藏”文件夹	96
2.4.37	自动关闭停止响应的程序	82	2.7	检测日志与入侵状况	97
2.4.38	禁止使用任务栏的分组功能	83	2.7.1	黑客查看日志的原因	97
2.4.39	限制关机时间	83	2.7.2	查看和维护审核结果	97
2.5	服务器的安全设置问题	84	2.7.3	Windows XP 日志系统的认识	98
2.5.1	实现服务器远程监控	84	2.7.4	入侵的迹象	98
2.5.2	禁止使用 Server 服务	84	2.7.5	入侵检测系统	98
2.6	文件安全设置问题	84	2.7.6	系统日志和入侵检测系统的区别	98
2.6.1	安全的 NTFS 文件系统	84	2.7.7	入侵检测系统的分类	99
2.6.2	设置文件夹的本地共享	85	2.7.8	入侵检测的步骤	99
2.6.3	设置文件夹的网络共享	86	2.8	系统隐私保护问题	99
2.6.4	隐藏和加密文件夹	86	2.8.1	清除“我最近的文档”的记录	99
2.6.5	恢复文件和文件夹的默认访问权限	87	2.8.2	清除“运行”对话框里的记录	100
2.6.6	设置共享目录密码	88	2.8.3	清除“查找”对话框里记录	100
2.6.7	查找加密的文件	90	2.8.4	清除“计划任务”里的记录	100
2.6.8	在 NTFS 系统中对文件和文件夹加密	90	2.8.5	清除 TEMP 临时文件夹的记录	100
2.6.9	破解 NTFS 文件系统下的密码	90	2.8.6	清除剪贴板上的内容	100
2.6.10	更改文件后缀加密文件	91	2.8.7	清除回收站里的内容	101
2.6.11	恢复和隐藏 Windows XP 驱动器	91	2.8.8	转移“我的文档”路径	101
2.6.12	更改文件类型	92	2.8.9	查看计算机开关记录	101
2.6.13	导出与保存加密证书	93	2.8.10	清除注册表编辑记录	102
2.6.14	使用 HTML 模板加密文件夹	93	2.8.11	清除随机启动的应用程序	103



2.8.12 清除 FTP 连接记录 103

2.8.13 清除“写字板”里的记录 103

2.8.14 删除输入法的自动记忆的信息 103

2.8.15 用脚本和批处理清除计算机的记录 ... 103

2.8.16 清除 Windows Media Player 播放
记录 104

2.8.17 ACDSee 自动清除历史记录 104

2.8.18 清除“收藏夹”记录 105

2.9 IE 安全设置 105

第三章 电脑文件管理、数据备份 与系统优化

3.1 电脑软件的删除 138

3.1.1 单个文件的删除 138

3.1.2 删除已经安装好的软件 138

3.1.3 删除没有提供卸载程序的软件 138

3.2 垃圾文件清理 139

3.2.1 回收站的清理与设置 139

3.2.2 删除顽固程序文件 141

3.2.3 磁盘垃圾文件清理 143

3.3 硬盘数据备份与恢复 144

3.3.1 回收站里“找”回删除的文件 144

3.3.2 系统还原的使用 144

3.3.3 意外丢失数据的拯救 146

3.3.4 设备驱动程序回滚 152

3.4 网络数据的备份和恢复 153

3.4.1 电子邮件的备份和恢复 153

3.4.2 聊天资料备份与恢复 155

3.4.3 收藏夹的备份 158

3.5 系统垃圾清理工具 160

3.5.1 CleanSweep 界面简介 160

3.5.2 卸载应用程序 160

3.5.3 清理硬盘“垃圾” 161

3.5.4 清理 Internet 临时文件 161

3.5.5 恢复应用程序 162

3.6 Windows 优化大师 162

3.6.1 安装 Windows 优化大师 162

3.6.2 Windows 优化大师的功能 164

3.6.3 Windows 优化大师的注册表功能 164

3.6.4 Windows 优化大师常用优化功能 165

3.7 超级兔子注册表优化软件 169

3.7.1 超级兔子的功能及特点 169

3.7.2 使用超级兔子 169

3.8 操作系统的备份与恢复 171

3.8.1 安装一键 GHOST 171

3.8.2 运行一键 GHOST 171

3.8.3 一键备份操作系统 172

3.8.4 手动备份操作系统 172

3.8.5 恢复计算机系统 173

3.9 系统应急处理 175

3.9.1 制作 Windows 98 启动盘 175

3.9.2 制作 Windows XP 启动盘 176

3.9.3 光盘启动盘制作 176

3.9.4 制作硬盘启动盘 178

3.9.5 创建杀毒启动 U 盘 179

3.9.6 制作 Linux 系统启动盘 181

第四章 黑客防范与处理



4.1 有关黑客基础知识.....	183	4.3.10 应用 TCP/IP 端口筛选管理开放 端口.....	193
4.1.1 什么是黑客.....	183	4.3.11 关闭系统文件共享服务的 139 端口... ..	193
4.1.2 黑客的攻击步骤.....	183	4.3.12 改变 FTP 服务器默认端口.....	193
4.2 黑客攻击的防范.....	183	4.3.13 利用 netstat 命令查看端口与程序.....	193
4.2.1 防范网络黑客的入侵.....	183	4.3.14 设置地址转换保护上网安全.....	193
4.2.2 隐藏 IP 地址.....	183	4.3.15 关闭 1900 端口.....	194
4.2.3 更改管理员账户.....	184	4.3.16 使用 Fport 查看开放端口对应的 程序.....	194
4.2.4 禁止 Guest 账户的入侵.....	184	4.3.17 利用 Port Reporter 跟踪端口活动 状态.....	194
4.2.5 防范黑客的要点.....	185	4.3.18 使用 Active Ports 查看本级活动端口 和连接.....	195
4.2.6 封死黑客入侵后门.....	185	4.3.19 为 Windows XP 系统增加启动密钥... ..	195
4.2.7 隐藏网上邻居.....	187	4.3.20 获取对方计算机名和用户名.....	195
4.2.8 黑客绕过防火墙的限制.....	187	4.3.21 快速修复注册表.....	196
4.2.9 防范 TXT 炸弹.....	187	4.3.22 限制访问控制面板.....	196
4.2.10 应用 IP 策略防止 Telnet 登录.....	188	4.3.23 利用注册表隐藏服务器.....	196
4.2.11 阻止黑客和病毒对系统服务端口 的扫描.....	189	4.3.24 禁止普通用户访问系统属性.....	196
4.3 端口安全处理.....	190	4.3.25 防范 WinNuke 攻击.....	197
4.3.1 更改 Windows XP 系统 Telnet 端口.....	190	4.3.26 快速打开“服务管理器”.....	197
4.3.2 修改 Windows XP 系统的远程管理 默认端口.....	190	4.3.27 指定使用的程序.....	197
4.3.3 寻找并打开可疑端口的恶意程序.....	191	4.3.28 防范网络钓鱼攻击.....	198
4.3.4 屏蔽 3389 端口.....	191	4.3.29 防止密码被盗.....	198
4.3.5 关闭 Windows 系统默认的 Telnet 服务.....	191	4.3.30 识别假冒网上银行.....	198
4.3.6 关闭 Windows XP 系统的 Web 服务.....	191	4.3.31 躲避常规服务端口攻击.....	198
4.3.7 关闭 Windows XP 系统 IIS 开启的 FTP 服务.....	192	4.4 防火墙启用与设置.....	198
4.3.8 关闭 IIS 开启的 SMTP 服务.....	192	4.4.1 自定义规则开放 FTP 服务.....	198
4.3.9 关闭 Messenger 服务.....	192	4.4.2 自定义 TCP 139 端口规则.....	199
		4.4.3 拒绝服务攻击.....	199



4.4.4 安装防火墙后网页浏览速度变慢200

4.4.5 允许 ICMP 在特定时间 Ping 本机200

4.4.6 综合应用防范 DDOS 攻击200

4.4.7 对防火墙进行系统测试201

4.4.8 自定义防火墙 IP 规则201

4.4.9 防止渗透防火墙201

4.4.10 利用防火墙防止 Ping 命令探测201

4.4.11 启用 Windows XP SP2 防火墙202

4.4.12 添加例外的安全程序通过防火墙202

4.4.13 命令行下查看防火墙配置信息202

4.4.14 网络入侵的方法203

4.4.15 Symantec 防火墙的安装和使用203

第五章 电脑软件安全设置

5.1 办公文档的设置 207

5.1.1 隐藏文档记录207

5.1.2 利用 Word “版本” 功能加密207

5.1.3 为 Word 文档设置密码保护208

5.1.4 忘记 Word 文档保护密码209

5.1.5 通过文档保护来保护 Word 文档210

5.1.6 解除文档保护的密码210

5.1.7 设置格式限制210

5.1.8 保护文档的局部内容211

5.1.9 宏病毒的防范211

5.1.10 设置 Word 文档的编辑权限211

5.1.11 Word 模板的备份和恢复211

5.1.12 预防文档信息暴露用户隐私211

5.1.13 文档保护的设置212

5.1.14 Excel 工作表的保护212

5.1.15 Excel 单元格的保护212

5.1.16 工作簿的保护 213

5.1.17 设置 Excel 文件的保护密码 213

5.1.18 撤销工作簿的保护 213

5.1.19 撤销工作表的保护 213

5.1.20 忘记 Excel 文件的保护密码 213

5.1.21 隐藏 Excel 文件的部分内容 214

5.1.22 隐藏重要的行、列数据 215

5.1.23 隐藏 Excel 工作表中重要的数据
部分 215

5.1.24 设置 Access 数据库密码 215

5.1.25 新建用户 215

5.1.26 新建组 216

5.1.27 设置用户和组的密码 216

5.1.28 设置用户和组的权限 216

5.1.29 设置用户隶属组 216

5.2 文档文件的安全 216

5.2.1 将普通的 MDB 文件转换为 MDE
文件 216

5.2.2 杀毒后无法正常使用 Word 应用
程序 216

5.2.3 利用 Word 打开受损的 Excel 文档 216

5.2.4 禁用 Excel 文档访问记录 217

5.2.5 清空文档列表 217

5.2.6 打开 Word 时提示“文件中含有宏”
..... 217

5.2.7 为 Microsoft Word 设置备份 218

5.2.8 恢复无响应的程序 218

5.2.9 恢复 Office 文档 218

5.2.10 利用 Office 设置保存向导备份
Office 设置 218



5.2.11	利用 Office 设置保存向导还原 Office 设置.....	219
5.2.12	禁止多用户同时编辑 Word 文档	220
5.2.13	防止偷看文档内容.....	220
5.2.14	保存文档的同时保留备份.....	220
5.2.15	预防文档的丢失.....	221
5.2.16	修复受损的 Word 文档.....	221
5.2.17	修复 Normal.dot 模板损坏导致的 Word 文档损坏.....	222
5.2.18	清除 WPS 记录.....	222
5.2.19	清除非法操作产生的“被挽救的 文档”记录.....	222
5.2.20	利用 ABI-CODER 加密文件.....	222
5.2.21	利用 Hide In Picture 进行伪加密.....	223
5.2.22	对图像文件进行加密.....	223
5.2.23	CMOS 的密码.....	224
5.2.24	禁止 HTML 文件作为墙纸.....	224
5.3	压缩文档的密码问题.....	225
5.3.1	WinZip 加密压缩文档.....	225
5.3.2	清除 WinZip 压缩文件的使用记录.....	225
5.3.3	清除 WinZip 历史文件夹的内容.....	225
5.3.4	清除 WinRAR 访问的历史文件.....	226
5.3.5	WinRAR 的备份和恢复.....	226
5.3.6	清除 WinRAR 的使用记录.....	226
5.3.7	修复损坏的 RAR 和 ZIP 压缩包.....	226
5.4	注册表设置的修改.....	227
5.4.1	解除注册表的锁定.....	227
5.4.2	锁定工具栏选项.....	227
5.4.3	利用注册表删除共享.....	227
5.4.4	隐藏“添加/删除 Windows 组件”.....	228

5.4.5	禁止用户修改桌面工具栏.....	228
5.4.6	清除“运行”记录.....	228
5.4.7	增强系统运行稳定.....	228
5.4.8	系统设置的个性化.....	231
5.4.9	系统实用设置.....	233
5.4.10	网络实用设置.....	234
5.4.11	实现浏览与安全的设置.....	237
5.4.12	使用注册表设置系统特性.....	239

第六章 内网安全使用技巧

6.1	局域网使用无限制.....	244
6.1.1	找寻丢失的局域网内电脑用户密码.....	244
6.1.2	网上邻居共享密码查询.....	244
6.1.3	局域网全面控制工具——NetSuper.....	245
6.1.4	局域网“网络执法官”.....	246
6.1.5	局域网搜索工具——LanExplorer.....	247
6.1.6	Windows 98 一线多机上网设置.....	248
6.1.7	Windows 2000/XP 一线多机上网 设置.....	251
6.1.8	内网中上 QQ.....	254
6.1.9	内网中玩“联众”.....	255
6.1.10	内网 BT 提速设置详解.....	256
6.2	网吧破网与管理指南.....	258
6.2.1	网吧鼠标右键禁用的漏洞.....	258
6.2.2	网吧禁止下载限制的漏洞.....	258
6.2.3	网吧禁止删除文件的漏洞.....	258
6.2.4	网吧禁止使用资源管理器的漏洞.....	258
6.2.5	网吧禁用软件限制的漏洞.....	259
6.2.6	网吧中使用禁用的 F4、F5、F8 漏洞.....	259



6.2.7 网吧中 IE 浏览器安全级别限制的 漏洞.....	260
6.2.8 网管软件漏洞分析.....	260
6.2.9 网管软件漏洞“美萍”篇.....	261
6.2.10 网管软件漏洞“还原精灵”篇.....	262
6.2.11 网管软件漏洞“万象幻境”篇.....	262
6.2.12 网管软件漏洞“PUBWIN4”篇.....	263
6.2.13 “Tencent Explorer 浏览器”漏洞.....	264

7.4.10 手动清除木马的方法总结.....	294
7.4.11 杀毒软件金山毒霸 2007.....	295
7.4.12 诺顿防火墙的应用.....	302
7.4.13 网络安全天网防火墙.....	305

第七章 网络设置、安全管理与病毒

查杀

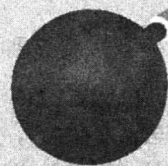
7.1 网络设置管理.....	266
7.1.1 ADSL 设置与管理.....	266
7.1.2 IP 地址的设置.....	272
7.1.3 网络服务的管理.....	275
7.2 网络日常维护.....	278
7.3 局域网远程操作.....	280
7.3.1 网络远程桌面的连接准备.....	280
7.3.2 远程桌面的实现.....	282
7.4 电脑病毒查杀与网络安全.....	284
7.4.1 认识计算机病毒.....	284
7.4.2 电脑病毒的种类与特点.....	284
7.4.3 电脑病毒的传播与防治.....	285
7.4.4 常见网络攻击类型.....	287
7.4.5 网络攻击工具.....	288
7.4.6 网络攻击防护对策.....	289
7.4.7 流行木马病毒的清除.....	291
7.4.8 Iparmor 木马克星.....	293
7.4.9 杀毒软件杀木马.....	294

01

Chapter

系统入侵 与加密

- 1.1 Windows 系统安全分析
- 1.2 Windows 安全操作策略
- 1.3 系统漏洞攻防
- 1.4 系统的加密
- 1.5 Windows 加密文件系统
- 1.6 系统漏洞扫描





1.1 Windows 系统安全分析

Windows 操作系统是现今使用最为广泛的操作平台,从最早的 3.x 版本发展到现在的 Windows Vista,可以说在系统安全上是逐渐提高的。但这种系统安全只具有相对性;并不是如微软所宣传的那样绝对安全(宣传 Windows 2000 的安全性达到 C2 级,Windows XP 更是号称永不死机的操作系统,Windows Vista 则被宣传为最安全、加密最高的操作系统),正如 2003 年爆发的 RPC 漏洞危机、2007 年出现的“熊猫烧香”病毒等,所造成的恶劣影响是无法估算的。Windows 系统安全的发展完全依靠不断更新的系统补丁来支持,让我们来看看为什么微软会不断推出新补丁的根本原因。

1.1.1 安全缺陷产生的原因

系统漏洞是威胁安全最根本的原因,而这些漏洞是指某些程序(如操作系统、应用程序等)在开发、设计的时候未对整体的合理性进行周密的考虑,当程序运行的过程中遇到一个看似合法的,却在实际中无法处理的问题时引发的不可预见的错误。因此系统漏洞也被称为“安全缺陷”,如果当系统漏洞被恶意利用,就会造成信息泄露、数据丢失、用户权限被恶意篡改等不可估量的后果。

提示

如果想真正理解“安全漏洞”的意思,列举一个例子大家很快就能明白。如在某些特定的条件下,你的电脑不明不白就出现文件丢失、系统死机等非正常现象(系统硬件存在故障除外),这就是“安全漏洞”造成的。

漏洞产生的原因大致可以分为以下 3 种:

(1) 程序开发者人为设置

某些程序员为了达到不可告人的目的,有意识地在程序的隐蔽处留下各种各样的“后门”,以顺利地进入程序控制台并进行程序修改操作。

(2) 硬件设备的原因

由于硬件设备的原因,编程人员无法弥补硬件的漏洞,从而使硬件的问题通过软件表现。

(3) 受水平、经验和当时安全加密方法所限制

受编程人员的业务水平问题、经验和当时安全技术、加密方法所局限,在程序中总会或多或少出现部分问题,这些有的影响程序的效率,有的会导致非授权用户的权力提升。

1.1.2 系统安全透析

现在大多数的电脑爱好者都认为 Windows 系统之所以受到众多黑客的攻击,是因为 Windows 操作系统使用太广泛的原因,除了 Windows 外,黑客们好像没有什么其他系统可以作为目标。其实,并不是因为这个原因,而是 Windows 操作系统相对其他系统(如 Linux、Unix 等)来说显得更加脆弱,漏洞也就更多,黑客攻击起来也更容易。

微软从最开始一直提倡的是“用户所需要的是网络的兼容性和应用程序之间的兼容性”,却从根本上忽略了超强的兼容性会带来不可估量的安全问题,这也就给有恶意企图的黑客提供了方便,造成黑客有机可乘,引发一系列的系统安全危机。

在 Windows 操作系统中的 NetBIOS,有很明显的 Windows 9x 共享密码漏洞,黑客想要进入 Windows 9x 的共享如进入无人之境。而号称安全性能极高的 Windows 2000、Windows NT、Windows XP 漏洞更是严重,不仅会泄露当前登录用户的账号和密码,黑客还可以很容易地通过 NETBIOS 伪装为当前用户对电脑进行管理;并且 Windows 2000、Windows NT、Windows XP 在默认的情况下,是将系统中所有硬盘都设置为共享(这种共享是一种隐形共享,没有传统的手形图标,因此一般电脑用户都无法察觉自己的硬盘已经被设置为默认的共享了),如图 1-1 所示。而几乎所有系统登录用户都是以超级管理员的身份进行操作的,这就更让黑客伪装身份后变得肆无忌惮。

另外,Windows 服务器的 IIS 服务更是目前所发现的超级大漏洞,该漏洞能够让黑客很容易地控制整套电脑,可以随意拒绝服务、泄露信息、泄露源代码、



获得更多权限、目录查询、执行任意命令、缓冲溢出执行任意代码，几乎是想要做什么就可以做什么。因此 Windows 服务器的 IIS 服务被列入目前十大漏洞之一。

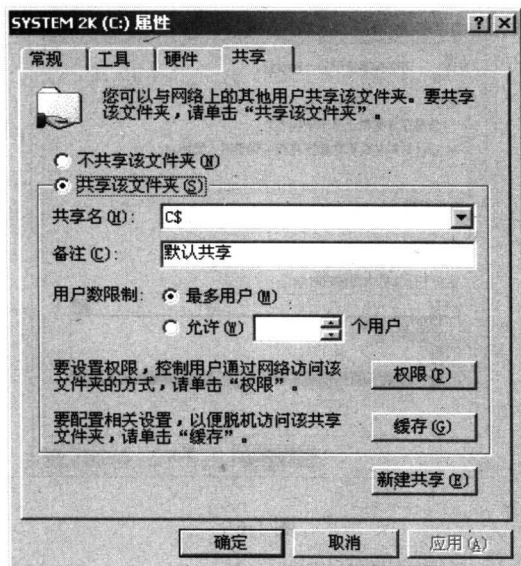


图 1-1

在我们使用的电脑中，还存在大量的 IE 浏览器漏洞、Outlook 漏洞、E-mail 服务器漏洞等，这些漏洞一旦被利用就可以让我们的系统瘫痪。

系统漏洞虽然存在，但并不是没有安全策略。只要我们时刻关注操作系统发展方向，注意更新系统的补丁，谨慎安装和运行一切非正常程序，系统还是相对安全的。

1.2 Windows 安全操作策略

Windows XP 是目前使用比较广泛的操作系统，凭借其超强的稳定性和可靠的安全性吸引了众多用户。要想更好地驾驭 Windows XP，需要按照以下操作策略进行设置。

1. 屏蔽不需要的服务组件

尽管服务组件安装得越多，用户可以享受的服务功能也就越多。但是用户平时使用到的服务组件毕竟有限，而那些很少用到的组件除了占用不少系统资源，

引起系统不稳定外，还会为黑客的远程入侵提供多种途径，因此我们应该尽量把那些暂不需要的服务组件屏蔽掉。

具体的操作方法为：

第一步：在控制面板中找到【管理工具】图标，双击该图标，如图 1-2 所示。



图 1-2

第二步：在打开的窗口中运行【服务】，如图 1-3 所示。



图 1-3

第三步：打开【服务】对话框，在该对话框中选中需要屏蔽的程序，并单击鼠标右键，从弹出的快捷菜单中依次选择【属性】和【停止】命令，如图 1-4 所示。

同时将【启动类型】设置为【手动】或【已禁用】，这样就可以对指定的服务组件进行屏蔽。