

Windows



系统漏洞攻击 与安全防范实战

电脑报 编著



- 病毒、木马专杀工具
- 数据急救工具
- 防火墙及安全防护工具
- 系统漏洞安全防护工具
- 备份与恢复工具
- 加密与解密工具

Windows 用户必备进阶手册

丛书累计畅销超过1,600,000册

- Windows 9x/2000/NT/XP/Vista系统漏洞攻防实战
- 彻底清除木马、病毒、流氓软件的实用秘技
- 常被黑客利用的系统漏洞攻击实例演示
- Windows系统被“黑”后的恢复措施
- 让Windows百毒不侵的个人电脑安全防护完全方案

征服 Windows 系列

Windows 系统漏洞 攻击与安全防范实战

电脑报 编著

云南人民电子音像出版社

特别致谢

本书由电脑报总策划，并特邀资深IT图书撰稿人欧陆宗先生撰写。欧先生长期担任多家数据恢复公司的技术顾问和某大型网站站长职务，是计算机安全实战技术行家。欧先生曾在《电脑报》、《中国计算机报》等多家国内知名IT媒体发表数据安全专文，已在十多家出版社出版过多部计算机专著，拥有丰富的书稿创作经验。其代表作品有《Windows 常见漏洞攻击与防范实战》、《电脑安全大师》、《黑客攻防36计》等。



版权所有 盗版必究

未经许可 不得以任何形式和手段复制和抄袭

书 名: Windows 系统漏洞攻击与安全防范实战
编 著: 电脑报
责任编辑: 西捷 刘佳
执行编辑: 周一鹏 李勇
封面设计: 陈敏
出版单位: 云南人民电子音像出版社
地 址: 昆明市环城西路609号
邮政编码: 650084
电 话: (0871) 4113185
技术支持: (028) 63658688-12036
邮 箱: yuppds@vip.163.com
发 行: 云南人民电子音像出版社
经 销: 各地新华书店、报刊亭
C D 生产: 四川省登山数码科技有限公司
文本印刷: 重庆联谊印务有限公司
开本规格: 787mm × 1092mm 1/16 15印张 460千字
版 本 号: ISBN 978-900392-77-0
版 次: 2007年8月第1版 2007年8月第1次印刷
定 价: 25.00元(本手册随光盘赠送)



将 Windows 征服到底!

“征服 Windows”系列，是电脑报为广大电脑用户量身定做的一套 Windows 完全应用丛书。丛书自 2002 年首次推出以来，历经 6 次再版，累计发行 160 余万册。是一套专门解决读者在 Windows 及相关软件使用中的疑难问题的案头必备丛书!

1985 年随着 Windows 1.0 正式推出，第一次有了图形化的操作系统；1995 年 Windows 95 的发布，使 DOS 时代走向终结；此后，微软又陆续推出了 Windows 98/Me/2000/XP/2003；2006 年 12 月，Windows Vista 的发布使 Windows 家庭迈上了一个更新更高的台阶。

时至今日，Windows 已经 22 岁了，我们的电脑也离不开她了。但她却让人既爱又怕：爱她，是因为她方便，易用的操作，美观大方的界面，强大齐全的功能，这些都是其他操作系统无法比拟的；怕她，是因为在 Windows 的世界里，病毒，漏洞层出不穷，一不小心就有可能让系统运行不稳定或者无法响应，更有甚者，直接出现系统崩溃，数据丢失的严重后果，让你欲哭无泪!

面对 Windows 无可比拟的优点和如此众多的烦恼，我们还应该坚持下去吗？兵来将挡，水来土掩！我们只要做到对症下药，那么所有问题都可以迎刃而解：对于系统漏洞，我们可以给它打上补丁；对于系统不稳定，我们有征服它的注册表密技；对于系统崩溃，我们有快捷、简便的重装系统方法……

“征服 Windows”是由众多对 Windows 具有深入研究的作者精心编写的一套针对 Windows 各种应用技巧和疑难杂症的图书！并且每年都根据 Windows 的新变化和新特色，推出最新版本，以确保广大读者能及时看到最新的内容，轻松征服 Windows!

在图书配套光盘中，我们根据读者的需求和图书具体内容，精心收集了与图书互动的工具软件，微软为我们提供的系统软件补丁，电脑报独家正版软件以及与图书对应的多媒体语音视频教学录象。通过他们，大家可以各取所需，大大加快我们电脑操作的实战能力。盘书结合，用最快的速度，最高的效率轻松驾驭 Windows，将 Windows 彻底征服。



Windows

“征服 Windows”系列包含以下十本图书：

《Windows XP 基本操作与实例应用 2000 招》：立足于实际应用，解决 Windows XP 中可能遇到的各种问题。

《Windows XP SP2 完全手册》：针对主流操作系统 Windows XP 及 SP2，详细介绍了安装、设置、管理、维护、备份、恢复、防毒防黑等全面而广泛的知识。

《系统重装实战一条龙》：针对重装系统的麻烦事，从系统崩溃急救开始，提供了数套全方位的系统重装方案。

《注册表完全操作 3000 例》：最新最全的注册表修改秘技及进阶指南，从基础出发，全方位地展示注册表修改实例。

《Windows 疑难排解实例 2000》：收集了电脑应用中常见的 2000 个疑难问答，手把手地教会你排除故障，迅速应付各种突发事件。

《Windows Vista 轻松上手》：详细讲解了 Windows Vista 的安装设置、系统优化、数据备份与恢复、最新防毒反黑，使你能够迅速上手。

《电脑料理大全》：在使用电脑的过程中，用户可能会因为病毒、误操作、意外事故等原因造成系统故障和数据丢失，本书专门针对这种情况为读者提供了行之有效的解决方案，让大家轻松备份、恢复各种数据文件，确保你的电脑安全。

《DOS/Windows 命令行实战与实例应用》：详细地讲解了 DOS 和 Windows 98/Me/NT/2000/XP/2003 下几乎所有的 DOS 命令，并针对具体应用列举了大量经典示例，能使读者真正做到学以致用。

《Windows 系统漏洞攻击与安全防范实战》：从单机和网络两个方面进行攻击与防范实战演习，收录了大量新的黑客技巧与攻防实例，介绍了更方便的各种防黑防毒操作，为读者漏洞攻防实战演练提供借鉴，可读性和实践性都非常强。

《Windows XP/ Vista 双系统安装与维护》：Windows XP 是目前最主流的操作系统，它在可靠性、兼容性、易用性等方面有明显的优势，Windows Vista 是微软最新一代操作系统，它带来了革命性的应用和体验。可能很多朋友会在这两者之间如何选择感到犯难，其实，同时采用 Windows XP 和 Windows Vista 组建的双系统将是最佳选择方案。

编者
2007.8

Windows

内 容 提 要

Windows 操作系统的功能强大，各版本的用户群体庞大，备受世人关注。正因为如此，Windows 系统本身存在的缺陷如漏洞也成了黑客们关注的焦点。如何让用户透彻了解这些漏洞并有效防范，正是这本专著想解决的问题。

《Windows 系统漏洞攻击与安全防范实战》分为三篇，详细地向你讲述 Windows 常见漏洞概况，黑客工具突破系统漏洞的攻击实例，弥补漏洞的具体措施与方案三大方面的内容。

在这些内容中你可以掌握大量的黑客攻防技巧：Windows 系统漏洞攻防的实战演练；网络恶意代码的攻击与防范；对付流氓软件的技巧；分布式攻击，用户信息扫描，木马攻防，口令破解等各种常用攻击手段。当然，针对个人电脑安全性问题，书中抛出了一系列的解决方案，包括网络安全知识，文件备份与恢复等内容。书中针对系统漏洞所讲解的各种防范措施，可让你从容应对网络上的病毒、木马及黑客攻击。

本书适合任何对网络安全和黑客技巧感兴趣的读者，特别对于系统管理员有重要的参考价值。

警告：文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法用途，后果自负！

光盘内容

- 病毒、木马专杀工具
- 防火墙及安全防护工具
- 备份恢复工具
- 数据急救工具
- 系统漏洞安全防护工具
- 加密与解密工具

光盘操作指南

一、配置要求

CPU 主频	850MHZ 以上
分辨率	800 × 600 像素以上
内存	128MB
显卡	32MB
光驱	52 倍速以上
操作系统	Windows 98/Me/2000/XP/2003

* 将光盘放入光驱中，系统将自动运行。

二、光盘精彩内容

光盘包括了“病毒、木马专杀工具”，“防火墙及安全防护工具”，“备份恢复工具”，“数据急救工具”，“系统漏洞安全防护工具”，“加密与解密工具”6 大部分。

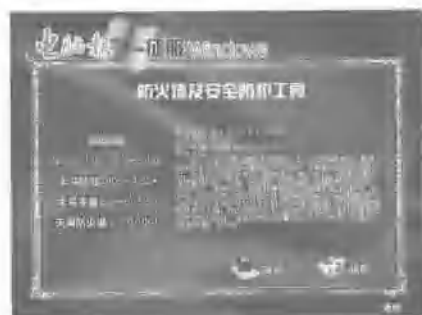


1. 病毒、木马专杀工具

本栏目提供了时下最为流行的数种病毒的专杀工具，如果你感觉到电脑中了病毒，不妨试试这些工具，因为这些工具针对性比较强，而所针对的病毒也是流传最广、危害最大的病毒。

2. 防火墙及安全防护工具

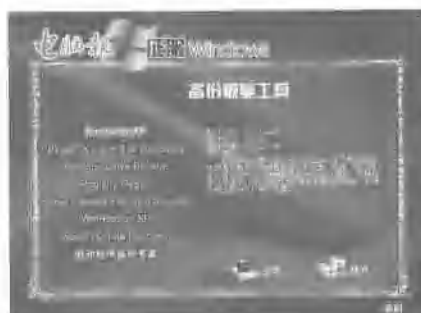
木马克星、天网等几大著名的防火墙软件均收录其中，读者可以按照自己的需求选择合适自己的防火墙。



3. 备份与恢复工具

这里有 Windows 系统备份工具、文件备份工具、数据

备份乃至于驱动备份工具，适合你的各方面备份需求。



4. 数据急救工具

本栏目为读者提供最流行的数据急救软件。当你的资料因为误删除或者其他一些其他什么原因而丢失，你可以依靠这些软件恢复你的数据。

5. 系统漏洞安全防护工具

如果你觉得 Windows 太不安全，漏洞太多，那么使用这些工具能有效地堵住系统的漏洞，让你免受黑客的入侵。



6. 加密与解密工具

怕别人看你的隐私了，那么给那些只属于自己的东西加密吧！这里的软件可以让你实现对文件和硬盘的加密、解密。



第一篇 Windows 常见漏洞详解

第1章 Windows 凭什么走到现在

1.1 盖茨和他的微软	1
1.2 起步岁月(1985~1994)	2
1.2.1 Windows 1.0	2
1.2.2 Windows 2.x	2
1.2.3 Windows 3.x	3
1.2.4 Windows NT3.x	5
1.3 迈向巅峰(1995~2000)	6
1.3.1 Windows 95	6
1.3.2 Windows NT4.0	7
1.3.3 Windows 98	7
1.3.4 Windows 2000	8
1.3.5 Windows Me	8
1.4 王者时代(2001~2007)	9
1.4.1 Windows XP	9
1.4.2 Windows Server 2003	11
1.4.3 Windows Vista	11
1.4.5 Windows Server 2007	12
1.5 Windows 未来发展的展望	13

第2章 Windows 系统存在的安全漏洞

2.1 Windows 漏洞攻击手段及防范	14
2.1.1 Windows 长扩展名存在缓冲溢出问题	14
2.1.2 NetBIOS 协议口令校验漏洞	14
2.1.3 “畸形 IPX NMPI 报文”安全漏洞	14
2.1.4 Cookies 漏洞	15
2.1.5 IE 的安全隐患	15
2.1.6 UPNP 服务漏洞	15
2.1.7 Windows 本地登录验证漏洞	16

2.1.8 SMB 通讯协议漏洞	16
2.1.9 拒绝服务攻击	16
2.1.10 Windows 拒绝服务攻击漏洞	16
2.1.11 设备名称解析漏洞	16
2.2 服务协议漏洞——Windows 共享攻防实战	17
2.2.1 什么是 SMB	17
2.2.2 远程共享漏洞	18
2.2.3 解除共享密码的几种方法	18
2.2.4 系统设置共享后的必要安全防范	19
2.2.5 用远程控制实现 Windows 文件共享	20
2.3 OBB 漏洞——Windows 蓝屏攻击	20
2.3.1 系统蓝屏工具	20
2.3.2 蓝屏攻击的安全防范	21
2.3.3 Windows 系统蓝屏死机密码	21
2.4 PWL 漏洞——密码解除	22
2.4.1 PWL 文件的攻击与防范	22
2.4.2 屏幕保护密码的攻击与防范	23
2.4.3 解除 PWL 文件对 Windows 系统安全的危害	23

第3章 Windows 2000 漏洞攻防实战

3.1 Windows 2000 的安全性概述	25
3.1.1 Windows 2000 的安全性设计	25
3.1.2 Windows 2000 中的验证服务架构	25
3.1.3 Windows 2000 实现的安全特性	26
3.1.4 Windows 2000 “秘密武器”	27
3.2 Windows 2000 漏洞攻防措施	28
3.2.1 Telnet 漏洞	28
3.2.2 本地操作漏洞	28
3.2.3 登录漏洞	28
3.2.4 NetBIOS 的信息泄露	29

3.2.5 奇怪的系统崩溃特性	29
3.2.6 IIS 服务泄漏文件内容	30
3.2.7 Unicode 漏洞	30
3.2.8 堵住 Windows 2000 ICMP 漏洞	37
3.3 Windows 2000 安全设置建议	38
3.3.1 初级安全设置	38
3.3.2 中级安全设置	39
3.3.3 高级安全设置	41

第4章 Windows XP 漏洞攻防实战

4.1 Windows XP 的安全性概述	42
4.2 Windows XP 的漏洞攻防防范措施	42
4.2.1 UPNP 漏洞	42
4.2.2 账号锁定功能漏洞	43
4.2.3 Windows XP 远程桌面漏洞	44
4.2.4 GDI 拒绝服务漏洞	44
4.2.5 终端服务 IP 地址欺骗漏洞	44
4.2.6 防范措施	44
4.3 Windows XP 安全设置指南	44

第5章 Windows NT 漏洞攻防实战

5.1 NT 的安全策略	49
5.1.1 用户账号和用户密码	49
5.1.2 域名管理	49
5.1.3 用户组权限	50
5.1.4 共享资源权限	50
5.2 NT 在网络中的安全性	50
5.3 NT 攻击理论与防护实战	51
5.3.1 NT 内置组的权限	51
5.3.2 NT 默认状态下对目录的权限	51
5.3.3 系统管理员管理工具的执行权限	52
5.3.4 NT 口令的脆弱性	52
5.3.5 简单攻击 NT 的实例	52
5.3.6 得到 Windows NT 管理权限后的攻击	53
5.4 Windows NT 漏洞攻防措施	55
5.4.1 获取 Administrator 权限账号	55
5.4.2 权限突破	57

5.4.3 攻破 SAM	57
5.4.4 监听 Windows NT 密码验证交换过程	58
5.5 入侵 Windows NT 常用工具	59
5.5.1 Net 命令	59
5.5.2 Nal 工具	59
5.5.3 攻防实例	61

第6章 Windows 2003 漏洞攻防实战

6.1 Windows 2003 安全性概述	64
6.2 Windows 2003 漏洞解决方案	65
6.2.1 取消 IE 安全提示对话框	65
6.2.2 重新支持 ASP 脚本	65
6.2.3 清除默认共享隐患	66
6.2.4 清空远程可访问的注册表路径	67
6.2.5 关闭不必要的端口	67
6.2.6 杜绝非法访问应用程序	67
6.3 Windows 2003 安全配置终极方案	68
6.3.1 SERV-U FTP 服务器的设置	69
6.3.2 IIS 的安全	69
6.3.3 3389 终端服务器的安全配置	73
6.3.4 FTP 服务器配置	73
6.3.5 把木马拒之门外	76
6.4 Windows Server 2003 防火墙设置	77
6.4.1 基本设置	77
6.4.2 测试基本设置	77
6.4.3 高级设置	77

第7章 Windows Vista 漏洞攻防实战

7.1 Windows Vista 漏洞概述	79
7.2 识破 Windows Vista 登录口令的攻击	81
7.2.1 详解 Vista 登录口令的秘密	81
7.2.2 Google 破解 Vista 登录口令	82
7.2.3 防止快速破解 Vista 登录口令	83
7.3 Windows Vista 安全设置建议	85
7.3.1 Vista 自带防火墙设置	85
7.3.2 安全软件设置	92

第二篇 常被黑客利用的系统漏洞攻防实例

第8章 常见木马漏洞攻击与防范实例

8.1 木马的基本概念	95
8.2 木马的定义	95
8.2.1 远程控制型木马	95
8.2.2 发送密码型木马	95
8.2.3 破坏型木马	95
8.2.4 FTP型木马	96
8.3 揭开木马的神秘面纱	96
8.3.1 木马的结构	96
8.3.2 揭秘木马的攻击过程	96
8.4 灰鸽子使用全攻略	98
8.4.1 注册域名	99
8.4.2 配置服务端程序	99
8.4.3 制作网页木马	99
8.4.4 JPG木马制作揭秘	100
8.4.5 给灰鸽子木马加壳躲避杀毒软件	101
8.4.6 木马服务端的加壳保护	101
8.4.7 灰鸽子的手工清除	101
8.5 常见木马档案	102
8.5.1 BO	102
8.5.2 广外女生	104
8.5.3 SBU7 黄金版	105
8.5.4 黑洞	107
8.5.5 聪明基因	108
8.5.6 网络精灵	109
8.5.7 无聊小子	110
8.5.8 蓝色火焰	111
8.6 木马隐形位置分析	113
8.7 木马清除方法	114
8.7.1 发现木马	114
8.7.2 逮住黑客	117
8.7.3 反黑在你的“爱机”种下木马的人	117
8.7.4 清除木马	118
8.8 木马的防范	119
8.8.1 “中招”途径	119
8.8.2 木马防范经验	119

第9章 恶意代码漏洞攻击与防范

9.1 解析恶意代码的特征与发展趋势 ...	120
9.1.1 恶意代码的特征	120
9.1.2 非感染性病毒	120
9.1.3 恶意代码的传播手法	121
9.1.4 恶意代码传播的趋势	121
9.1.5 恶意代码相关的几个问题	122
9.2 恶意代码大曝光	122
9.2.1 浏览网页注册表被禁用	123
9.2.2 篡改IE的默认页	123
9.2.3 修改IE浏览器默认主页	123
9.2.4 IE的默认首页灰色按钮不可选	123
9.2.5 IE标题栏被修改	123
9.2.6 IE右键菜单被修改	123
9.2.7 IE默认搜索引擎被修改	124
9.2.8 系统启动时弹出对话框	124
9.2.9 IE默认连接首页被修改	124
9.2.10 IE中鼠标右键无效	125
9.2.11 查看“源文件”菜单被禁用	125
9.2.12 浏览网页开始菜单被修改	125
9.2.13 禁止鼠标右键	125
9.2.14 共享你的硬盘	125
9.3 打造完美的IE网页木马	126
9.3.1 完美IE木马的特征	126
9.3.2 IE木马的不足	126
9.3.3 打造完美IE木马	126
9.4 恶意代码的预防	129

第10章 黑客常用漏洞攻击工具

10.1 扫描之王——SSS	130
10.1.1 SSS的功能介绍	130
10.1.2 实例演示	134
10.2 扫描利器——流光	135
10.2.1 简单主机(漏洞)扫描	135
10.2.2 高级漏洞扫描	136
10.2.3 暴力破解	138
10.3 专穿防火墙的反弹木马——DBB ...	140
10.3.1 配置后门	140
10.3.2 打开后门	140
10.3.3 轻松操纵	141
10.3.4 封杀后门	141
10.4 反向谍软件——SS&D	141
10.4.1 使用实战	142
10.4.2 下载软件设防	142
10.4.3 让系统具有“免疫”功能	143
10.4.4 粉碎间谍程序	143
10.4.5 查找启动项中的间谍	144
10.5 系统监控器——Real Spy Monitor	144
10.5.1 基本设置	144
10.5.2 监控实战	145
10.6 远程控制——PcAnywhere	146
10.6.1 PcAnywhere 安装	147
10.6.2 PcAnywhere 基本设置	147

第11章 基于网络的系统漏洞攻防实例

11.1 宽带密码破解	148
11.1.1 小心本地黑客	148
11.1.2 远程盗取，防不胜防	149
11.2 管理员帐户破解	152
11.2.1 利用默认的 Administrator	152
11.2.2 创建密码恢复盘	153
11.2.3 通过双系统删除 SAM 文件	155
11.2.4 借助第三方密码恢复软件	155
11.3 Snmp 命令的利用	157
11.3.1 什么是 Snmp	157
11.3.2 对 Windows 2000 进行探测扫描	157
11.3.3 Snmp 浏览工具——JP Network Browser ..	158
11.3.4 扫描工具——Languard Network Scanner ...	159
11.3.5 防范基于 Snmp 的探测扫描	159
11.4 利用 Google 进行入侵与渗透	159
11.4.1 攻击实战演练	160
11.4.2 工具使用	160
11.4.3 防范措施	160
11.5 将入侵主机私有化	161
11.5.1 私有型“肉鸡”的重要性	161
11.5.2 “肉鸡”的要求	161
11.5.3 “私有化”进程	161

第三篇 系统漏洞防范措施与技巧

第12章 必知必会的网络漏洞安全基础知识

12.1 扫清自己的足迹	165
12.1.1 彻底地删除文件	165
12.1.2 不留蛛丝马迹	165
12.1.3 隐藏文档内容	165
12.1.4 清除临时文件	166
12.1.5 保护重要文件	166
12.1.6 改写网页访问历史记录	166

12.1.7 清除输入的网址记录	166
12.1.8 清除高速缓存中的信息	166
12.2 保密知识初解	167
12.2.1 密码保护	167
12.2.2 防止在线入侵和病毒威胁	169
12.2.3 使“用户配置文件”和“策略”	169
12.2.4 两点小技巧	170
12.3 认识系统进程	171

12.3.1 明明白白系统进程	171
12.3.2 关闭进程和重建进程	171
12.3.3 查看进程的发起程序	172
12.3.4 查看隐藏进程和远程进程	172
12.3.5 杀死病毒进程	173
12.4 巧妙识别真假 Svchost.exe 进程 ..	174
12.4.1 认识 Svchost.exe 进程	174
12.4.2 识别 Svchost.exe 进程的模仿	174

第13章 堵住漏洞彻底删除流氓软件与病毒

13.1 认识“流氓软件”及其分类	175
13.1.1 广告软件	175
13.1.2 间谍软件	175
13.1.3 浏览器劫持	175
13.1.4 行为记录软件	175
13.1.5 恶意共享软件	175
13.2 诺顿网络安全特警	175
13.2.1 配置安全特警	175
13.2.2 启用诺顿网络安全特警	176
13.2.3 程序扫描	177
13.2.4 隐私控制	177
13.2.5 在线安全检测	178
13.2.6 封锁恶意 IP	178
13.2.7 端口安全防护	179
13.3 360 安全卫士查杀恶意软件	179
13.3.1 系统漏洞修复	179
13.3.2 查杀恶意软件	180
13.3.3 全面系统诊断与修复	180
13.3.4 免费查杀病毒	180
13.4 微软反向间谍高手	181
13.4.1 初识反向间谍软件利器	181
13.4.2 手动扫描查杀间谍软件	181
13.4.3 设置定时自动扫描	182
13.4.4 开启实时监控	182
13.5 瑞星卡卡根除“流氓软件”	183
13.5.1 广告拦截	183
13.5.2 系统修复	184

13.5.3 病毒疫情实时监控	184
13.6 金山系统清理专家	184
13.6.1 恶意软件查杀	184
13.6.2 两种方式修复 IE	185
13.6.3 进程和启动项管理	185
13.6.4 历史痕迹清理	186
13.6.5 其他特色功能介绍	186
13.7 Windows 流氓软件清理大师	187
13.7.1 恶意软件卸载	187
13.7.2 垃圾文件清理及系统优化	187
13.7.3 四款特色安全工具	187

第14章 Windows 的备份与恢复方案大全

14.1 Windows 98 的备份与恢复	189
14.1.1 Windows 98 的备份	189
14.1.2 恢复 Windows 98	193
14.2 Windows 2000 的备份与恢复	196
14.2.1 备份 Windows 2000	197
14.2.2 Windows 2000 故障后的还原	201
14.2.3 用系统紧急修复磁盘 ERD	202
14.2.4 用故障恢复控制台修复故障	203
14.3 Windows XP 的备份与恢复	203
14.3.1 备份 Windows XP	206
14.3.2 Windows XP 的紧急还原	207
14.4 Windows Vista 的备份与恢复	211
14.4.1 Windows Vista 自带备份恢复功能	211
14.4.2 利用 Ghost10 备份与恢复 Vista	213
14.4.3 利用安装文件备份与恢复 Vista	214
14.5 注册表的备份与恢复	216
14.5.1 注册表的备份与恢复	217
14.5.2 注册表急救术	221
14.6 系统设置与文件的备份和恢复	223
14.6.1 备份的内容	223
14.6.2 备份的方法	223
14.6.3 还原的方法	226
14.6.4 驱动程序备份	227

第1章 Windows 凭什么走到现在

50岁的比尔·盖茨是世界上最富有的人，30岁的微软是世界上最成功的软件公司，20岁的Windows是世界上最使用最广泛的计算机操作系统。他们的故事，从来都是人们最津津乐道的经典话题。

1.1 盖茨和他的微软

时间追溯到1973年，一个来自于西雅图的18岁孩子比尔·盖茨(Bill Gates)以优异的成绩进入了他梦寐以求的哈佛大学。在这里，酷爱数学和计算机的他开始了对软件技术的钻研，写出“伟大的软件”是这个年轻人的目标和理想。也就是在这期间，比尔·盖茨开始了最初的商业尝试。他为当时的Altair 8800电脑设计出了第一个BASIC语言解释器，这是一种简单易用的计算机程序设计语言，同时也是后来MS-DOS操作系统的基础Microsoft BASIC。虽然在计算机方面取得了一些突破性的成功，但是在人才济济的哈佛，比尔·盖茨的综合成绩也只能算是一般。在大学三年级的时候，盖茨做出了一个令他人难以理解的决定，他从世界级学府哈佛退学了。凭借从BASIC项目上拿到的版权费，比尔·盖茨与该时代的好友保罗·艾伦(Paul Allen)在新墨西哥州中部城市Albuquerque一同创建了“Micro-soft”(意为“微型软件”)公司。从此以后，比尔·盖茨把全部精力投入到了自己喜欢的事业。



1979年，盖茨将公司迁往西雅图，并将公司名称从“Micro-soft”改成了“Microsoft”(也就是现在我们俗称

的“微软”)。微软成立之初，正好赶上了个人电脑的研制成功，盖茨敏锐地察觉到了一个数字的时代即将到来。当时，他们了解到最顶尖的计算机巨头IBM需要为自己的个人电脑产品寻找合适的、基于英特尔x86系列处理器的操作系统。于是微软就向Tim Patterson公司购买了他们的QDOS操作系统使用权，将其改名为Microsoft DOS(“微软磁盘操作系统”)，并进行了部分的改写工作，最终通过IBM公司在1981年推向了市场。微软在接下来的几年中又推出了数个MS-DOS操作系统版本，之后，MS-DOS的历史还一直延续到了90年代的6.8版。微软是幸运的，MS-DOS在当时取得了不俗的销售量。此外，随着微软BASIC语言解释器的推广，越来越多的公司开始使用微软BASIC的语言编写程序并与微软产品的兼容。这样，微软的BASIC便逐渐成为了公认的市场标准，公司也顺势占领了整个市场。



1981年8月发行的Microsoft DOS 1.0由4000行汇编代码组成，可以运行在8K的内存中。它没有图形界面，操作起来极其的不方便。而当时苹果公司的Macintosh操作系统具有了图形用户界面(GUI)，这种更直观操作方式显然要比DOS的命令行来得更加友好。微软很清楚GUI将成为未来大众化操作系统的潮流，于是，他们便开始开发自己的GUI程序——“界面管理器”(Interface Manager)，这就是未来20年个人桌面操作系统的绝对霸主——Windows的前身。

1.2 起步岁月(1985~1994)

1.2.1 Windows 1.0

前面提到的“界面管理器”并非真正的 Windows。事实上直到 1983 年,微软才正式宣布开始设计 Windows,定位是一个为个人电脑用户设计的图形界面操作系统。

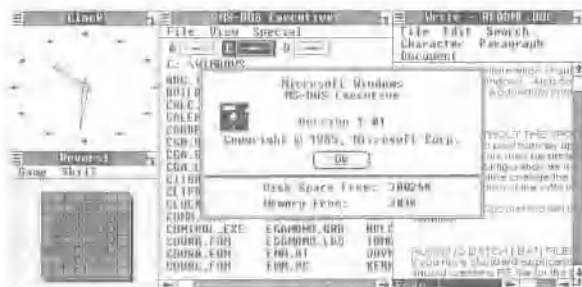
Microsoft Windows 1.0 的设计工作花费了 55 个开发人员整整一年的时间,并于 1985 年 11 月 20 日正式发布,售价 100 美元。Windows 1.0 基于 MS-DOS 2.0,支持 256K 的内存,显示色彩为 256 色。由于是图形化的界面,Windows 1.0 支持鼠标操纵和多任务并行,窗口(Window)成为 Windows 中最基本的界面元素。Windows 1.0 窗口可以任意缩放,和苹果的 Macintosh 只有一个居于顶部系统菜单不同,每个 Windows 应用程序都有自己单独的菜单。



此外,Windows 1.0 还包括了一些至今仍保留在 Windows 中的经典应用程序,如日历、记事本、计算器等等。



尽管开创了先河,但是用户们对 Windows 1.0 的评价普遍不高,因为它的运行速度实在是很慢。在当时,最好的图形化个人电脑平台是 GEM 和 Desqview/X。

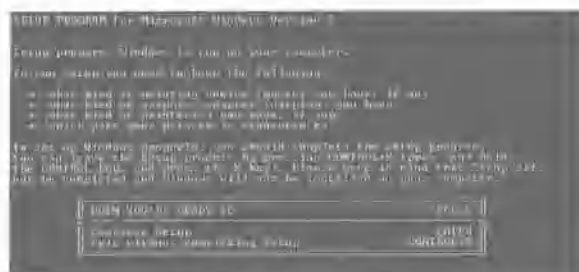


注意

Windows 1.0 中的程序管理器是资源管理器的前身,至今我们仍然能在 XP 的系统目录下发现它的身影("progman.exe")。

1.2.2 Windows 2.x

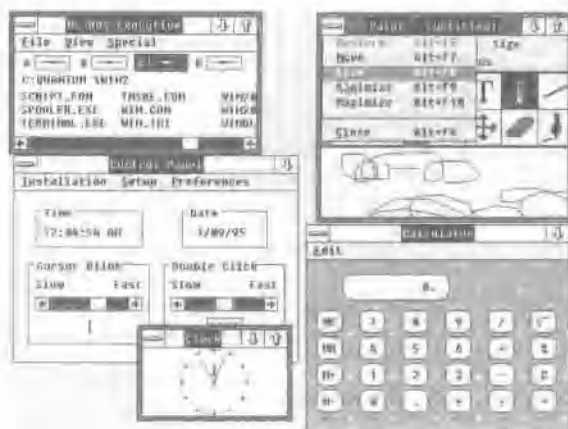
Windows 1.0 最初的失败并没有让微软停止前进,1987 年 12 月 9 日,Windows 2.0 发布,售价依然是 100 美元。Windows 2.0 改进了 Windows 1.0 中一些不太人性化的地方,我们熟悉的“最大化”和“最小化”按钮开始出现在了每个窗口的顶部。由于在图标的设计上,微软借鉴了一些 MacOS 的风格和元素,还因此一度被苹果公司告上了法庭。除了界面上的改进,现在 Office 系列的 Microsoft Word 和 Microsoft Excel 也初次在 Windows 2.0 中登场亮相。



不到一年的时间,微软又相继发布了 Windows/2862.1 和 Windows/3862.1。这两个版本分别针对 Intel 的 286 和 386 处理器做了一定的优化。1989 年,微软推出了 Windows 2.11,这个版本在内存管理和打印驱动上做了一些小的改进。



在当时，支持 Windows 的第三方软件还非常的少，但已经明显有越来越多的公司开始为 Windows 平台开发应用程序了。然而从用户的反馈来看，Windows 2.0 依然不是一个成功的产品。



注意

曾有国外网友做过测试，不少 Windows 2.0 中的程序依然可以在 Windows XP 中正确的运行。当然，前提是你还找得到这些古老的 Windows 程序。



1.2.3 Windows 3.x

从 3.x 系列开始，微软的 Windows 操作系统才算真正走上了正轨，同时也为微软今天的辉煌埋下了伏笔。1990 年 5 月 22 日，Windows 3.0 正式发布。前两个

Windows 版本糟糕的性能，可以说多少受到了当时硬件因素的制约。

不过，这种窘境在上世纪 90 年代已经不复存在了。个人电脑的功能越来越强大，在用户的计算机上，Windows 的运行速度也随之流畅了起来；而微软也趁机在这个中加入了虚拟设备驱动的支持，使得 Windows 有了非常好的可扩展性，而这种优势也一直保持到了今天。虚拟技术的运用不仅提升了硬件兼容性也提升了软件的兼容性，从 Windows 3.0 开始，MS-DOS 的程序终于可以在一个单独的窗口中运行了。

此外，这一版的操作系统还改进了内存管理技术和对 286、386 处理器的支持，并且有越来越多的 Windows 标准组件被加入。借着 Windows 3.0 成功，微软于 1992 年 3 月 18 日发布了 Windows 3.1。这是一个可靠性很高的版本，很少崩溃。

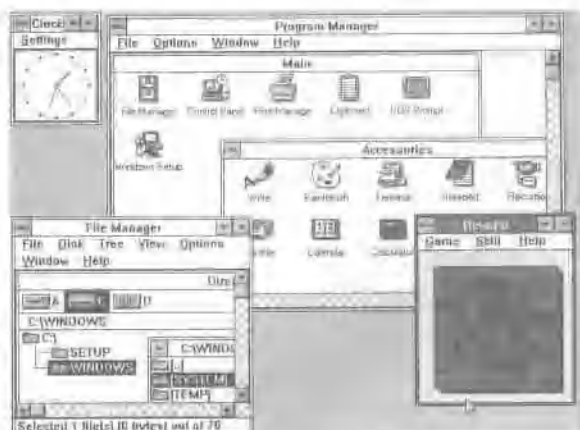
多媒体技术的加入使这一版本开始支持音频和视频的播放。同时，Windows 3.1 引入可缩放间距 True Type 字体技术，使得 Windows 成为了重要的桌面出版平台。接下来，微软又分别在 1992 年底和 1993 年底发布了 Windows for Workgroups 3.1 和 Windows for Workgroups 3.11，加入了一系列的网络协议支持。

随着 1992 年微软正式进入中国，Windows 逐渐开始在国内流行起来。1994 年发布的 Windows 3.2 是很多国内用户第一次接触的 Windows 操作系统，它的简单易用性深深吸引了中国的电脑玩家。Windows 3.2 根据 Windows for Workgroups 做了不少本地化工作，事实上，这是微软针对中国市场而专门开发的产品，它只有中文版。



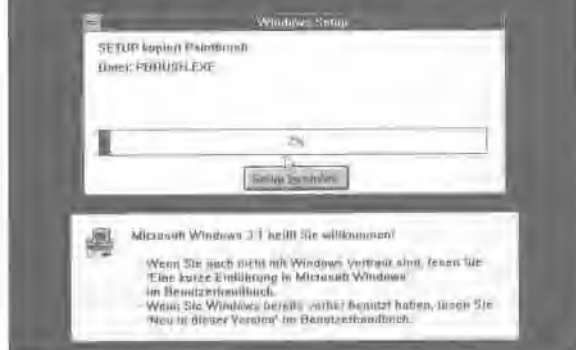


值得一提的时，从 Windows 3.1 起，微软的开始为每个 Windows 产品加入研发代号的习惯。



Windows 3.1 的代号是“Janus”(两面神)，Windows for Workgroups 3.1 是“Kato”(一个漫画人物)，而 Windows for Work groups 3.11 则是“Snowball”。

Windows-Setup

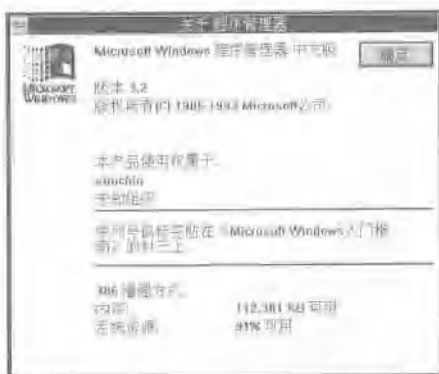


1990 年，Windows 3.0 刚刚推出便一炮而红，只用了 6 周的时间便卖出了 50 万份拷贝，这是史无前例的，而 1992 的 Windows 3.1，仅仅在最初发布的 2 个月内，销售量就超过了 100 万份。



至此，Windows 操作系统最终获得用户的认同，并奠定了其在操作系统上的垄断地位。自那时起，微软的研发和销售也开始进入良性循环。1992 年，比尔·盖茨成为世界首富，轰动全球。





1.2.4 Windows NT3.x

开发 Windows NT 的历史大概要追溯到 1988 年, 这个系统本来是由微软和 IBM 联合研制的 NTOS/2 (OS/2, 0 版)。当时, 微软试图打入工作站市场, 而 Windows 支持的 Intel X86 芯片并不是工作站处理器, 所以, 微软就雇用了 DEC 公司的团队来专门开发这个产品。后来, 由于 Windows 3.0 的成功, 微软决定把 NTOS/2 的程序开发接口由 OS/2 API 改为 Windows API。



这一举动引起了 IBM 的不满, 两家公司就此分道扬镳。IBM 继续开发自己的 OS/2, 而微软则把 OS/2NT 改名为 Windows NT, 并推向市场, 这就是 Windows NT3.1。



注意

关于 NT 这个名字的意思, 有人说这是 New Technology (新技术) 的缩写。另一种说法则认为这个名字来源于微软研发时使用的 Intel 860 CPU 模拟器, 因为 Intel 860 CPU 的代号为 “N-Ten” (N10), 所以就有了 NT 这个名字。

Windows NT3.1 于 1993 年发布。从表面上看, 它和 Windows 3.1 并无太大区别。然而, 由于完全重写的 32 位内核, 过足了 Windows NT 是一个优秀的新产品。比 Windows 3.x 系列强大得多。它既可以在专业的工作站上使用, 也可以在基于 Intel 芯片的 PC 机上运行。从此, 微软在商用和家用市场都有了自己的主打产品。



第二年, 开发代号为 “Daytona” 的 Windows NT 3.5 发布。这一次, 微软把 NT 操作系统分为了工作站版本和服务器版本, 这也为后来 NT 非商业系列的开发结果埋下了种子。Windows NT 3.5 包括了新的开机画面, 类似于 Windows for Workgroups 3.x 的用户界面, 以及改进的 OLE (对象嵌入) 技术。由于大量新技术的加入, Windows NT 3.1 和 3.5 成为了微软在商用市场最好的试金石。

