电脑报 总策划

大补贴丛书 Windows 2004全新版

就这样征服Windows XP 1200例

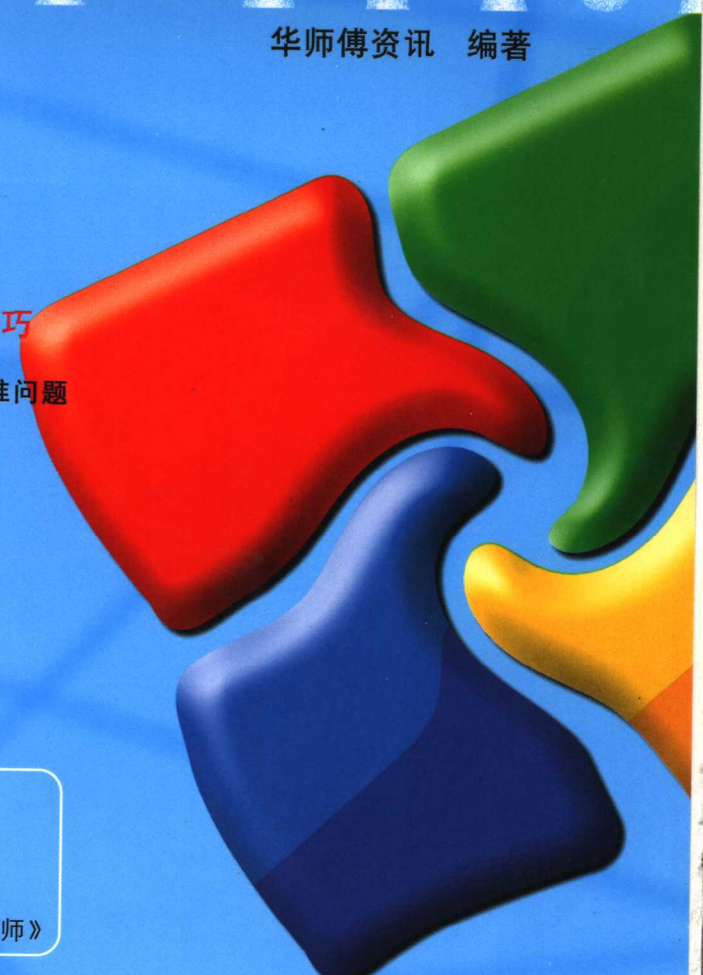
系统安装、软件应用、网络连接、故障排除

丛书累计发行 700,000册 Windows用户必备进阶手册

WINDOWS

- 征服个性优化、常用软件使用
- 征服系统文件磁盘数据安全管理
- 征服注册表软、硬、网全面设置应用
- 征服各种安装方法及多系统安装问题
- 征服组建局域网、Internet连接、信息共享技巧
- 征服多媒体使用、游戏娱乐、隐藏功能及疑难问题

华师傅资讯 编著



光盘主要内容

- 必备的5款Windows XP系统应用工具
- 征服Windows XP的10种强悍系统安全补丁
- 适用于Windows XP的8大中文输入法软件
- 特别推荐操作管理软件《微晓Windows系统大师》

山东电子音像出版社出版

电脑报总策划
http://www.itbook.com.cn

大补贴丛书
Windows 2004全新版

就这样征服Windows XP

系统安装、软件应用、网络连接、故障排除1200例

华师傅资讯 **编著**

Windows

山东电子音像出版社出版

特别致谢：

本丛书已历经三次修改和增补，发行量已达70余万册，已成为广大Windows用户必备的权威性手册。历次修订，都倾注了作者和编辑大量心血，正是他们追求卓越和精益求精的态度，使得此书成为广大用户喜爱的畅销图书。

在此特别感谢以下作者的辛勤劳动、创意和支持：张雁、水淼、邹县芳、陶龙明、王利、黄玉良、刘晓燕。

书　　名：就这样征服Windows XP
编　　著：华师傅资讯
责任编辑：李　萍
执行编辑：余　文
封面设计：邓玉萍
组版编辑：蒋　洁
监　　制：谢均建
出版单位：山东电子音像出版社
地　　址：济南市胜利大街39号
邮政编码：250001
电　　话：(0531)2060055-7616
发　　行：山东电子音像出版社
经　　销：各地新华书店、报刊亭
CD生产：北京中联鸿远光盘科技发展有限公司
文本印刷：重庆升光电力印务有限公司
开本规格：787mm × 1092mm 1/16　19.5印张　400千字
版 本 号：ISBN 7-900398-73-2
版　　次：2004年8月第1版　2004年8月第1次印刷
定　　价：22.00元(1CD+手册)

你为什么不可错过《Windows 大补贴》

Windows 的世界很精彩！ Windows 的世界很无奈？

对大多数电脑用户而言，Windows 系统可以说是一个让人既爱又恨的“怪物”。爱它，在于它方便、易用的操作，美观、大方的界面，强大、齐全的功能，几乎是其他操作系统无法比拟的。恨它，则是因为 Windows 的世界，又是一个病毒满天飞，漏洞层出不穷的世界，一不留神，我们就可能遭遇系统运行不稳定甚至无法响应，或者时不时闹出点系统崩溃、数据丢失的“小”问题，让你百无聊赖，欲哭无泪。

Windows 大补贴——让你的 Windows 有“大”智慧！

Windows 是如此让人欢喜让人忧，我们还有必要守着它忠贞不二，从一而终吗？其实问题远没有这么严重的！对于“糖衣炮弹”我们尚可以吃了“糖衣”吐“炮弹”，对于 Windows 我们为什么不能去其糟粕留精华呢？

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，保证分分钟搞定“崩溃”，重要数据一个不少；至于其他什么疑难杂症，排困解惑里早已备有灵丹妙药，而所有这些，《Windows 大补贴》丛书都会倾情奉献给你，还等什么呢？GO！一起加入到 Windows 征服之旅中来吧，你会发现，Windows 越来越可爱。

《Windows 大补贴》系列共分：

- 《Windows 重装系统一条龙 2004》：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。
- 《就这样征服 Windows XP》：立足于实际应用，解决 Windows XP 中可能遇到的各种问题。
- 《Windows 排困解惑 1500 例》：收集了电脑应用中常见的 1500 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 注册表完全操作 2000 例》：最新最全的注册表修改秘技。从基础出发，全方位的展示注册表修改实例。
- 《Windows 常见漏洞攻击与防范实战》：收集整理了现今黑客攻击最常利用的各种漏洞数百个，进行攻击与防范的实战演习。

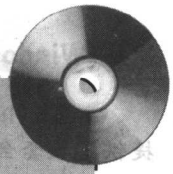
编者

2004. 10

内 容 提 要

本手册对Windows系统存在的漏洞以及可能遭受的攻击作了详尽的讲解，并收集整理了现今黑客攻击最常利用的各种漏洞数百个，从单机和网络两个方面针对Windows各个版本的常见漏洞进行攻击与防范的实战演习，对最流行的木马、常用软件如QQ、IE等都做了攻击防范的实例讲解，让你在实践中获得真知！本手册内容包括Windows安全隐患、Windows 9x/Me/NT/2000/XP/2003漏洞攻防实战、Windows后门大揭密、常用软件攻防实例、黑客的武器库、黑客实战练兵等。

（特别提示：本手册介绍的漏洞及其攻击方法，仅供读者学习之用，如用于非法用途，后果自负！）



光盘内容

Windows系统漏洞官方补丁
Windows XP SP2补丁
冲击波、震荡波病毒补丁
常用软件插件及其补丁

卓越的品质是我们的信念与坚持

电 脑 报 出 版 事 业

Contents 目录

第1章 Windows系统安全隐患曝光

1.1 Windows王朝进化史

Windows的起源可以追溯到Xerox公司所进行的工作。1970年，美国Xerox公司成立了著名的研究机构Palo Alto Research Center(PARC)，从事局域网、激光打印机、图形用户接口和面向对象技术的研究，并于1981年宣布推出世界上第一个商用的GUI（图形用户接口）系统——Star 8010工作站。但是由于种种原因，技术上的先进性并没有给它带来它所期望的商业上的成功。

当时，Apple Computer公司的创始人之一Steve Jobs，在参观Xerox公司的PARC研究中心后，认识到了图形用户接口的重要性以及广阔的市场前景，就开始着手进行自己的GUI系统研究开发工作，并于1983年研制成功Apple Lisa GUI系统。随后不久，Apple又推出第二个GUI系统Apple Macintosh，这是世界上第一个成功的商用GUI系统。当时，Apple公司在开发Macintosh时，出于市场战略上的考虑，只开发了Apple公司自己的微机上的GUI系统，而此时，基于Intel x86微处理器芯片的IBM兼容微机已渐露峥嵘。这样，就给Microsoft公司开发Windows提供了发展空间和市场。

Microsoft公司很早就意识到建立行业标准的重要性，在1983年春季就宣布开始研究开发Windows，希望Windows能够成为基于Intel x86微处理芯片计算机上的标准GUI操作系统。Microsoft在1985年和1987年分别推出Windows 1.03版和Windows 2.0版。但是，由于当时硬件和DOS操作系统的限制，这两个版本并没有取得很大的成功。

此后，Microsoft于1990年5月份推出Windows 3.0并一炮打红，这个“千呼万唤始出来”的操作系统一经面世便在商业上取得惊人的成功：不到6周，Microsoft公司销出50万份Windows 3.0拷贝，打破了任何软件产品的6周销售记录，从而一举奠定了Microsoft在操作系统上的垄断地位。

一年之后推出的Windows 3.1对Windows 3.0作了一些改进，引入TrueType字体技术，这是一种可缩放的字体技术，它改进了性能；还引入了一种新设计的文件管理程序，改进了系统的可靠性，更重要的是增加了对象链接合嵌入技术（OLE）和多媒体技术的支持。但是，Windows 3.0和Windows 3.1还是都必须运行于DOS操作系统之上。

随后，Microsoft于1995年推出新一代操作系统Windows 95(又名Chicago)，它可以独立运行而无需DOS支持。Windows 95是操作系统发展史上一个里程碑式的作品，它对Windows 3.1版作了许多重大改进，包括：更加优秀的、面向对象的图形用户界面，减轻了用户的学习负担；全32位高性能的抢先式多任务和多线程；内置的对Internet的支持；更加高级的多媒体支持（声音、图形、影像等），可以直接写屏并很好地支持游戏；即插即用，简化用户配置硬件操作，并避免了硬件上的冲突；32位线性寻址的内存管理和良好的向下兼容性等等。

Windows 98于1998年6月25日发布，是Windows 95的升级版本。Windows 98具有如下特点：Windows 98是一种图形用户界面的操作系统，Windows 98用图形用户界面代替了DOS的字符用户界面，用户无须与难记忆的DOS命令打交道；提供丰富的应用程序，如Windows 98中的写字板、画图、娱乐、计算器、记事本、多媒体播放器等；提供并行处理能力：Windows 98是一种多任务的操作系统，每个任务都有自己的窗口，多个任务并行运行，各窗口间可相互切换并相互交换信息；支持多媒体操作；所见即所得：在Windows 98中，由于采用了真实字体，在屏幕上的显示效果与打印机上的输出是完全相同的，且若选择相同的分辨率的打印机，在不同打印机上打印的结果是相同的；支持即插即用（PNP）；支持长文件名；提提供强大的网络功能：内置Internet访问工具如IE、FTP等，内置多种协议，方便连接多种网络等；支持多屏显示；集成Internet界面：Internet的访问变成了用户界面中的一部分。

相对于 Windows 9x 系列，Windows NT 系列则是截然不同的系列，它是微软推出的第一个服务器级操作系统。早在 1992 年，微软就正式立项，成立专门的团队，开发 Windows NT。当时微软希望能在原有开发操作系统的经验基础上，加入全新的技术，给用户提供更稳健的操作系统，这里包括企业级用户，因为他们要求操作系统不仅能提供计算服务平台，而且要支持大量用户的并发应用、支持高性能要求的应用程序，以及在恶劣的运行程序下仍保持特定的稳定性和效率。这就是开发 Windows NT 的初衷。

经历了 Windows NT 1.0、Windows NT 2.0、Windows NT 3.0、Windows NT 3.5 等阶段后，Windows NT Server 4.0 的推出受到业界的认可。这个版本的内核稳定性更高、系统更安全、界面更友好。此外，硬件的兼容性也有了很大进步。由于在研发投入方面花了很大力气，这个版本吸收了很多企业级操作系统的优点，许多企业用户称，Windows NT Server 4.0 是企业级操作系统的真正意义上的集大成者。

NT 升级到 5.0 时，微软在 1998 年 10 月将其正式更名为 Windows 2000。21 个月以后，受业界极大关注的 Windows XP 正式推出，该产品基于 NT 内核的融合，集成了 NT 的稳定性、安全性以及 Windows ME 的多媒体和网络功能。从此，微软的前台操作系统就不再采用 9x 系列的内核了。

从新品的市场反响看，Windows XP 多多少少扮演了 IT 低潮时期“强心剂”的角色。随着 Windows XP 的推出，IT 市场增添了很多生气，国内外不少厂商，纷纷借助 Windows XP 的势头，加紧市场宣传攻势。连年来利润不断下跌的 PC 机，销售情况也有所好转。Windows XP 甚至导致了“体验经济”这一新名词的出现。

2003 年 5 月 22 日，微软公司正式发布了 Windows Server 2003，其实所谓的“Windows Server 2003”就是之前微软大张旗鼓宣传的“Windows .NET Server”，可能是担心 .NET 部署的时机还不成熟，又使用了 2003 这样保守的名称。不管怎样，Windows Server 2003 是一次重要的升级，可以更好地配合 Windows XP。

在享受新版 Windows Server 2003 之前，我们来回顾一下从 Windows 出生到成熟的历史，也就是 Windows 的 16 王朝 27 版本。

1.1.1 “史前”时代

微软公司刚开始开发操作系统的时候，这个软件还不叫 Windows，而是“Interface Manager(界面管理员)”，时间是 1981 年 9 月。别忘记，当时微软公司正在与 IBM 公司合作为开发 OS/2，大家认为这个才是 MS-DOS 的正统继任者。

在 Windows 1.0 的预览版中，菜单不是推出式的，有点象当年的 WordStar，不过 Windows 是堆积在屏幕的底部。

1. Windows 1.0

在 1985 年 11 月 20 日，Windows 1.0 终于正式发布了。这是 PC 机用户所使用的第一个图形界面系统，大家用鼠标来操作系统的各种功能，并且执行各种应用程序，是一种全新的体验。

在 Windows 1.0 中，应用程序包含在一个桌面的“组”里面，包括：MS-DOS 文件管理器、日历、卡片文档、记事本、计算器、时钟和通讯程序；允许用户管理他们的个人资料，就像今天的 PDA 一样；并且 Windows 1.0 允许用户切换程序，而不是退出并重新执行它们，这一点对于当时的 PC 用户而言，确实是很大的改进，因为 MS-DOS 一次只能执行一个程序，非常不便。

Windows 1.0 可以显示 256 色，可以改变窗体的大小，最小化窗体(类似缩小成一个状态条)。还可以调节一些 Windows 的外观，微软公司开始加进来一个叫做“控制面板”的元素，并沿用至今。当时 Windows 窗体的许多元件都延续到了现在，例如：text boxes(文本框)、radio buttons(选择按钮)、scrolling bars(滚动条)和 menu items(菜单项)。

当然，Windows 1.0 的能力还是很弱的，例如在层叠窗体的时候，窗口太多了就比较困难了，另外也没有改变层叠的可选项。

微软公司公开宣布 Windows 开发计划的消息是在 1983 年，可是直至 1985 年 9 月才正式发布了第一版的 Windows 1.0，这个版本的 Windows 是基于 MS-DOS 2.0 的，由于当时的硬件限制与 MS-DOS 2.0 的功能限制，Windows 1.0 不能拿来与之后的 Windows 3.1 比较。

2. Windows 2.0

1987年4月2日，Windows 2.0问世了。这个版本在应用程序上与之前的版本差不多，但是在管理与实用性上做出了不少改进。微软公司利用了当时先进的286CPU的“高速度”，还有扩展内存(Expanded Memory)、内建应用程序通讯机制及动态数据交换技术。Windows 2.0支持VGA的图象模式，从而使得图象品质大有改观，改变窗体大小的速度也得到很大改善，更重要的是，用户可以自由的将窗体摆在屏幕的任意位置。

Windows 2.0支持386增强模式，这其实是Windows 2.0的一个改进版，叫做“Windows 2.0/386”。而之前的版本改称“Windows 2.0/286”。Windows 2.0/386是在一年以后发行的，所谓386增强模式就是允许用户在扩充内存中(Extended Memory)同时执行多个MS-DOS应用程序，这样就打破了MS-DOS先天设计上640KB内存管理的缺陷。

Windows 2.0在当时的硬件条件所使用的范围并不广泛，软件也不是很丰富；然而很多软件的开发人员在这时被吸引到这个系统平台上，很多人在这个时候写出了自己的平生第一个Windows应用程序。可以说，Windows 2.0的386增强模式对于日后Windows成功辉煌迈出了坚实的一步。

1.1.2 中兴时代

1. Windows 3.x

(1)Windows 3.0

1990年5月22日，Windows 3.0发布了。这个版本的改进实在是太大了，但是缺乏对多媒体与网络通讯的支持是一个大问题，因此3.0的生命周期并不长，很快就被Windows 3.1取而代之了。然而3.0版是个基础，在架构上提供32位的性能(虽然从内核而言，Windows 3.x是一个16位的操作系统)、高档的图形显示以及对Intel 386处理器的完整、有力支持。

新特性包括：程序管理器、文件管理器、以及打印管理器。

应用程序开发环境完全重写过，使用了虚拟驱动设备技术(virtual device drivers，VxDs);应用程序可以在扩充内存(Extended Memory)中本地执行；并且支援完全的MS-DOS轮巡式多任务执行。

“程序管理器”与“文件管理器”带给用户Macintosh(苹果公司当时很高档桌面计算机)式的大图标，支持点击与拖放的操作方式。

微软虽然很快就用新的Windows 3.1取代了Windows 3.0，但是因为3.0版带来的良好第三方硬件支持特性以及软件开发易用性使Windows真正吸引了很多厂商与开发人员。微软公司同时发布了Windows软件开发包(Windows software development kit，SDK)，使得软件开发者可以将精力从硬件设备驱动又转移到软件的本身的功能上。

(2)Windows 3.1

1992年4月6日Windows 3.1正式发布了，同年10月27日Windows 3.1 for Workgroups版本也发布了。TureType字体在Windows 3.1里面得到了应用，这种在当时非常先进的字体技术，可以在显示与打印的时候取得漂亮的效果。也正因如此，从Windows 3.1开始，系统更适合做复杂文字处理、排版输出等用途，而之前这是苹果电脑的专利。多媒体功能的问题，在这一版也得到了改进，声音驱动已经在系统内建支持。影音文件回放支持也比较不错，新加入的彩色屏幕保护也使很多人感兴趣，例如迪斯尼公司就推出一系列经典的卡通屏保。

成千上万个第三方的Windows兼容软件这时被开发出来，反过来因为应用软件的丰富，反而刺激了Windows 3.x的销售数量，据不完全统计，世界上总共卖出去超过一千万套Windows 3.x。

不过Windows 3.1缺乏网络支持，而MS-DOS的网络应用一下子就吃掉了超过640KB的内存，因此微软公司发布了Windows 3.11 for Workgroup来弥补这个问题，这个版本内建网络功能。

(3)Windows 3.2

这算一个什么版本呢？这是第一个官方的简体中文版Windows。从版本号来看，比Windows 3.11 for Workgroup要高，不过实际上这个版本只是Windows 3.1的汉化而已，同样也没有内建网络功能。有人说，这个版本只是拿来蒙事骗取中国人的，不过这个版本的确是微软的第一个中文Windows，而之前想要在Windows里面输入中文就只好依靠第三方的外挂中文平台了，如：中文之星、RichWin等。

(4)Windows for Workgroups 3.11

Windows for Workgroups 3.1 在 1992 年 10 月 27 日发行，而到了 1994 年 2 月 15 日微软公司对其进行了一些重要的修订，发行了 3.11 版。与之前的 Windows 3.0 和 3.1 比较，Windows for Workgroups 3.11 加入了点对点、点对多，以及域的支持。内建的网络支持，使得用户在系统执行的时候能很简单地设置、访问网络。但是 Windows for Workgroups 3.11 不支持因特网拨号网络模式，它需要安装第三方的软件才能使用这个功能，而且还常常和系统自身的网络功能冲突。

在用户界面上来说，Windows for Workgroups 3.11 与 Windows 3.1 基本上是一模一样的，只不过内建了 LAN(局域网)的支持，对于商业用户来说，新的中心设定与安全管理十分有用，尤其改进了对 Novell Netware 网络的支持，这一点尤为重要，因为那个年代，局域网是Novell的天下。还有远端访问服务(RAS，remote access service)，同时新的 32 位文件系统更有效率与安全。

2. Windows NT 3.x

(1)Windows NT 3.1

Windows NT 3.1 版是 1993 年 8 月发行的。对于微软公司，NT 是一个里程碑式的软件，版本号从 3.1 起跳，应该是与 Windows 3.1 有一定关系吧。所谓NT，意思就是“全新技术(New Tech.)”，微软的大老板比尔·盖茨在 NT 发行的时候，对其大加赞赏，称 NT 是一个全新的架构，比之前的 Windows 有很大改进，对于商业用户而言，这是他们梦寐以求的东西。

微软公司可以说是重新编写了一个全新的操作系统，Windows NT是微软公司第一个内建支持高端客户机/服务器应用、工业领导类型的个人生产力应用系统。这个操作系统在背景上完善了安全机制，操作系统强大、有效率，同时又不失桌面系统的可靠性与易用性，它为 Windows 应用程序设计了一个轮巡式多任务调度器，调整了网络、域服务器安全性、OS/2 和 POSIX 子系统、支持多处理器架构和新的 NTFS 文件系统。这些特性的大部分都沿用到今天的Windows系统中，只是做了一些改进而已，例如：Windows XP 与 Windows Server 2003。

Windows NT 3.1 与 Windows 3.1 结合得很好，可以同时提供很多用户同时使用，无论他们是在家里还是在公司。Windows NT 3.1 是为商业用户设计的，分为工作站版本(workstation edition)、服务器版本(server edition)和高级服务器版本(Advanced Server edition)。

(2)Windows NT 3.5

Windows NT 3.5 是 1994 年 9 月 6 日正式发行的。Windows NT 3.5x 有两种不同的版本，一种叫做工作站版本，另外一种叫做服务器版，区别在于工作站版在网络连接时，有一定的任务限制，并且缺乏服务器版的一些软件组件；另外服务器版提供一种授权控制的软件包。在用户界面上，两种版本与 Windows 3.1 非常相似，但是用户将不再有机会看到黑色的 MS-DOS 开机画面，取而代之的是 Windows NT 自己的开机画面，究其原因是整个系统内核已经由 MS-DOS 全面转向 NT 的新内核。之前我们提过有人争论 Windows 究竟是不是一个操作系统？发生争论的时间比较久远，那时候 PC 的主力操作系统还是 MS-DOS，而 Windows 非常像运行在这之上的 Shell，很多功能都局限于 MS-DOS 所能提供的极限。这一点在前几个版本的 Windows 上面尤为明显，不过因为 Windows API 地位的确立，现在这个问题已没有人提起了，不过事实是:早期的 Windows 其实更像 MS-DOS 的一个 GUI 应用程序。

Windows NT 3.5 工作站版支持 OpenGL 图形标准，这样为高端应用程序开发、工程制造、财务分析、科学计算、商业研究任务的应用提供了必要的条件。

Windows NT 3.5 工作站版为商业应用软件与数据资料提供了高度强固的保护，此产品对 32 位应用的执行性能也有所改进，更好的程序支持，包括支持 NetWare 文件及打印服务器，并改进了使用的便利与生产力特性，例如文件名称可以使用 255 个字符的长度，而之前的 MS-DOS 与 Windows 3.x 只能使用 8.3 的文件名系统。

(3)Windows NT 3.51

Windows NT 3.51 在 1995 年六月正式发布了，包含了一个新工具，去帮助用户管理客户端访问授权(Client Access Licenses，CALs)，这是微软 BackOffice 产品线(现在已经演变成 Microsoft .NET 服务)所需要的条件之一。有一个工具，可以远端安装Windows 95，并且支持远端开机，其实最主要的理由就算为了配合Windows 95 这个“时髦”的客户端。