电脑报 总策划

征服 WINDOWS

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

## 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

云南人民电子音像出版社

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。

电脑報



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：650034
电　　话：(0871) 4113185
技术支持：(023) 63658888-12036
邮　　箱：yuppd2@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
CD生产：四川省蓥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

# 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

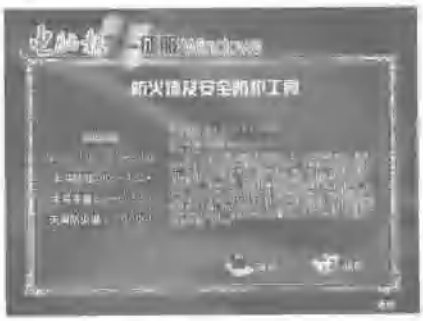
光盘包括了“病毒、木马专杀工具”，“防火墙及安全防护工具”，“备份恢复工具”，“数据急救工具”，“系统漏洞安全防护工具”，“加密与解密工具”6大部分。


### 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。

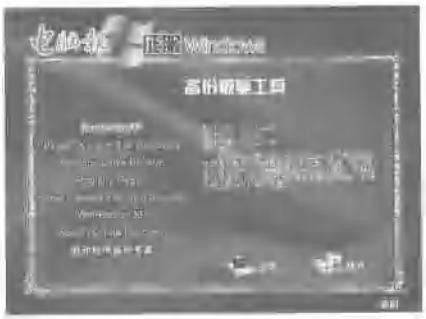
### 2.防火墙及安全防护工具

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。

# CONTENTS 目录

## 第一篇 Windows常见漏洞详解

### 第1章 Windows凭什么走到现在



### 第2章 Windows系统存在的安全漏洞



### 第3章 Windows 2000漏洞攻防实战

# 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



## 第9章 恶意代码漏洞攻击与防范

## 第10章 黑客常用漏洞攻击工具



## 第11章 基于网络的系统漏洞攻防实例



# 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

# 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Altair8800电脑设计出了第一个BASIC语言解译器，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·盖茨与孩提时代的好友保罗·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要到来。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.x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语言解译器的推广，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，公司也逐渐占领了整个市场。

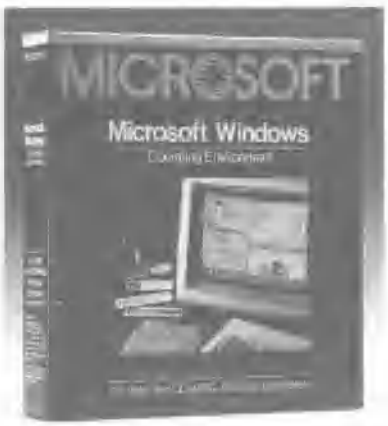
1981年8月发行的Microsoft DOS1.0由4000行汇编代码组成，可以运行在8K的内存中。在没有图形界面，操作起来极其的不方便。而当时苹果公司的Macintosh操作系统具有了图形用户界面(GUI)，这种更直观操作方式显然要比DOS的命令行来得更加友好。微软很清楚GUI将成为未来大众化操作系统的潮流，于是，他们便开始开发自己的GUI程序——“界面管理器”(Interface Manager)，这就是未来20年个人桌面操作系统的绝对霸主——Windows的前身。

## 1.2 起步岁月(1985~1994)

### 1.2.1 Windows 1.0

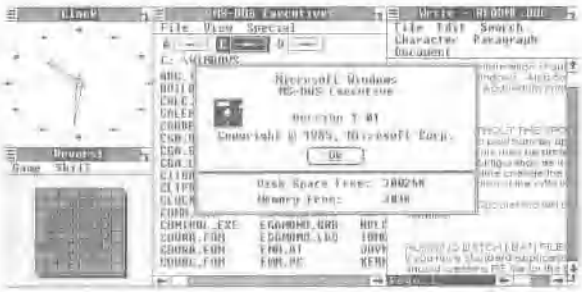
前面提到的“界面管理器”并非真正的Windows。事实上直到1983年，微软才正式宣布开始设计Windows，定位是一个为个人电脑用户设计的图形界面操作系统。

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。


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。

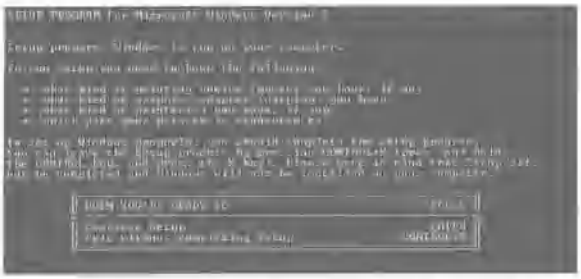


**注意**

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”)。

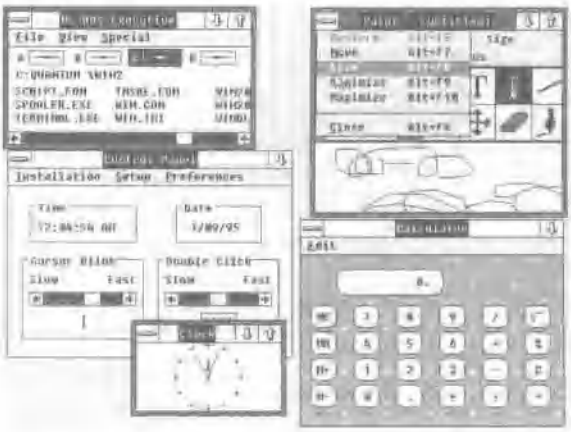
### 1.2.2 Windows 2.x

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。

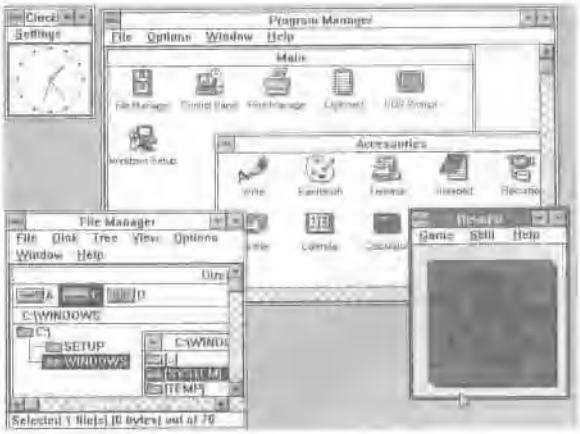
不过，这种羁绊在上世纪90年代已经不复存在了，个人电脑的功能越来越强大，在用户的计算机上，Windows的运行速度也随之流畅了起来；而微软也趁机在这个中加入了虚拟设备驱动的支持，使得Windows有了非常好的可扩展性，而这种优势也一直保持到了今天。虚拟技术的运用不仅提升了硬件兼容性也提升了软件的兼容性，从Windows 3.0开始，MS-DOS的程序终于可以在一个单独的窗口中运行了。

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引入可缩放的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，微软的开始了为每个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”。


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/23.0版)。当时，微软试图打入工作站市场，而Windows支持的IntelX86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/2API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，并指向市场，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Inteli860CPU模拟器，因为Inteli860CPU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，注定了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非商业系列的开花结果埋下了种子。Windows NT 3.5包括了新的开机画面，类似于WindowsforWorkgroups 3.x的用户界面，以及改进的OLE(对象嵌入)技术。由于人们对新技术的加入，Windows NT 3.1和3.5成为了微软在商用市场最好的成绩。