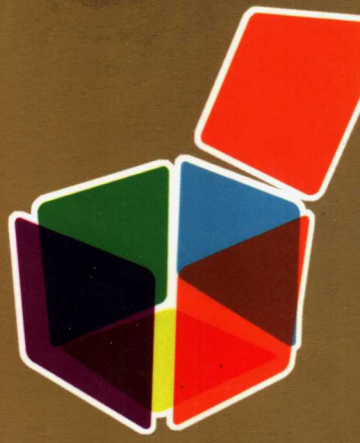
电脑報

征服 Windows

Windows 常见漏洞攻击与防范实战

漏洞检测、系统攻防、黑客入门全攻略

Windows 用户必备进阶手册



漏洞分析 各类常见漏洞经典问题分析

实战演练 各大主流操作系统攻防演练

扫描检测 未雨绸缪，安全防范为第一

黑客武器 常用黑客软件轻松应用

欧陪宗 编著

电脑報 精品图书

丛书累计发行 1,200,000 册

精彩光盘

1. 华夏黑客攻防视频教程
2. 系统最新补丁及安全软件
3. 网络扫描攻防工具
4. 加密解密应用软件

山东电子音像出版社出版

电脑報 Windows 常见漏洞攻击与防范实战

征服 Windows 系列

Windows 常见漏洞攻击与防范实战

欧陪宗 **编著**

山东电子音像出版社出版

特别致谢

征服 Windows 系列丛书历经五次修订和增补，发行量已达 120 余万册，成为广大 Windows 用户必备的权威手册。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，使得丛书深受 Windows 系统用户的喜爱和推崇。

在此特别感谢电脑报资深撰稿人欧陪宗的辛勤劳动、创意和支持。

书　　名：Windows 常见漏洞攻击与防范实战
编　　著：欧陪宗
责任编辑：李　萍
执行编辑：李　勇　何　磊
封面设计：刘学敏
组版编辑：陈　晶
监　　制：吕美亮
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) 82060055-7616
技术支持：(023) 63658888-12028
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：北京中联光碟有限公司
文本印刷：重庆科情印务有限公司
开本规格：787mm × 1092mm 1/16　　17 印张　300 千字
版 本 号：ISBN 7-89491-680-3
版　　次：2006 年 8 月第 1 版　2006 年 8 月第 1 次印刷
定　　价：25.00 元(1CD+ 配套书)

将Windows进行到底

《征服Windows》系列（原名《Windows大补贴》系列），是电脑报为Windows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5次再版，累计发行120余万册。是一套真正与读者零距离接触、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！

早在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8月24日Windows 95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。

时至今日，Windows已经20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》是由一批对Windows具有深入研究的作者精心编写的一套针对Windows各种疑难杂症的图书！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！

《征服Windows》系列包含以下五本图书：

《注册表终极操作2006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。

《重装系统一条龙2006》：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。

《2000招征服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

2006.8

Windows

内 容 提 要

作为个人电脑应用最广泛的Windows操作系统，众多的安全漏洞给用户带来了巨大的安全隐患。如何防范这些隐患、保护个人隐私，已成为Windows用户的当务之急。

本手册收录了Windows的各类常见漏洞，从单机和网络两个方面进行攻击与防范的实战演习，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。

本手册还对系统拒绝服务攻击、分布式攻击、用户信息扫描、木马攻防、口令破解等方面作了详细的介绍，提供了恶意代码的防范措施，以及常见黑客软件的使用方法，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。

本手册适合于任何对网络安全和黑客感兴趣的读者，特别是对系统管理员有重要的参考价值。

特别提示：本手册介绍的漏洞及其攻击方法，仅供读者学习使用，请勿用于非法活动，否则后果自负！

光盘导读

●华夏黑客攻防视频

光盘中的黑客攻防视频是由“国内第一黑客门户网站”——华夏黑客同盟制作，本视频采用网页浏览器播放，如果被浏览器阻止无法播放，请解除阻止即可播放。

●系统最新补丁

收录了最新Windows漏洞补丁，包括Windows XP SP2、Windows XP关键更新程序、Windows 2000 SP4 Rollup以及Office 2003 SP2补丁，完美地解决系统安全漏洞。

●系统及网络安全工具

收录了书中重点介绍的黑客工具，包括系统及网络方面的攻防软件。收录软件只是供读者学习，切勿用于非法领域，否则后果自负。

●加密解应用软件

加解密软件是介绍给重视数据安全的读者，但请读者在使用该类软件做好数据备份，做到有备无患。

CONTENTS 目录

第1章 为什么Windows系统会存在安全隐患

第2章 Windows 9x/Me系统漏洞攻防实战

第3章 Windows 2000 系统漏洞攻防实战

第4章 Windows XP 系统漏洞攻防实战

第5章 Windows NT 系统漏洞攻防实战

第7章 常见木马攻击与防范实例

第8章 恶意代码攻击与防范

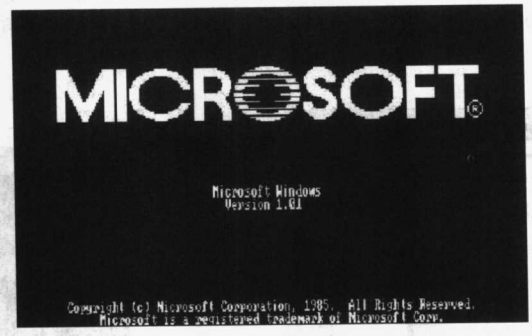
第9章 黑客常用工具大搜捕

第1章 Windows 系统存在的安全隐患

1.1 Windows 家族一览

1.1.1 早期的 Windows

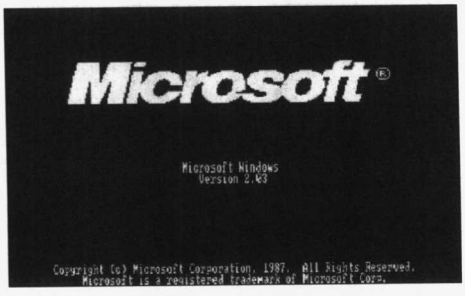
Windows 的起源可以追溯到 Xerox 公司所进行的工作。1970 年，美国 Xerox 公司成立了著名的研究机构 Palo Alto Research Center(PARC)，从事局域网、激光打印机、图形用户接口和面向对象技术的研究，并于 1981 年宣布推出世界上第一个商用的 GUI（图形用户接口）系统—— Star 8010 工作站。但是由于种种原因，技术上的先进性并没有给它带来所期望的商业上的成功。



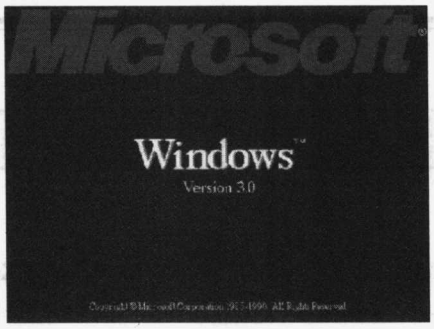
当时，Apple Computer 公司的创始人之一 Steve Jobs，在参观 Xerox 公司的 PARC 研究中心后，认识到了图形用户接口的重要性以及广阔的市场前景，就开始着手进行自己的 GUI 系统研究开发工作，并于 1983 年研制成功 Apple Lisa GUI 系统。随后不久，Apple 又推出第二个 GUI 系统 Apple Macintosh，这是世界上第一个成功的商用 GUI 系统。当时，Apple 公司在开发 Macintosh 时，出于市场战略上的考虑，只开发了 Apple 公司自己的微机上的 GUI 系统，而此时，基于 Intel x86 微处理器芯片的 IBM 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

1.1.2 Windows 3.x 时代

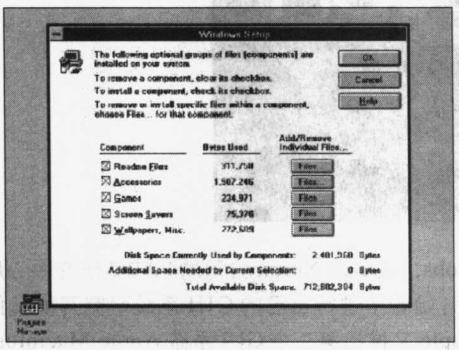
Microsoft 公司很早就意识到建立行业标准 的重要性，在 1983 年春季就宣布开始研究开发 Windows，希望 Windows 能够成为基于 Intel x86 微处理芯片计算机上的标准 GUI 操作系统。Microsoft 在 1985 年和 1987 年分别推出 Windows 1.03 版和 Windows 2.0 版。但是，由于当时硬件和 DOS 操作系统的限制，这两个版本并没有取得很大的成功。

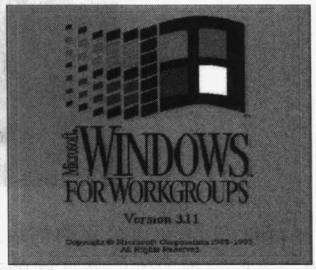


此后，Microsoft 于 1990 年 5 月份推出 Windows 3.0 并一炮打红，这个“千呼万唤始出来”的操作系统一经面世便在商业上取得惊人的成功：不到 6 周，Microsoft 公司销出 50 万份 Windows 3.0 拷贝，打破了任何软件产品的 6 周销售记录，从而一举奠定了 Microsoft 在操作系统上的垄断地位。



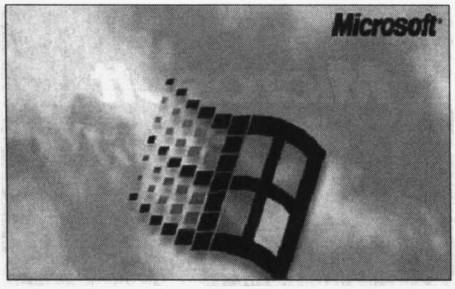
一年之后推出的 Windows 3.1 对 Windows 3.0 作了一些改进，引入 TrueType 字体技术，这是一种可缩放的字体技术，它改进了性能；还引入了一种新设计的文件管理程序，改进了系统的可靠性，更重要的是增加了对象链接合嵌入技术（OLE）和多媒体技术的支持。但是，Windows 3.0 和 Windows 3.1 还是都必须运行于 DOS 操作系统之上。



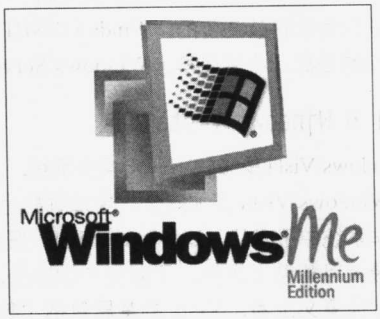


1.1.3 Windows 9x 时代

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。



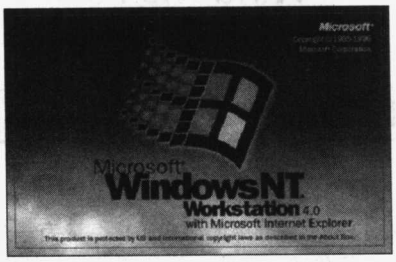
Windows 98 于 1998 年 6 月 25 日发布,是 Windows 95 的升级版本。Windows 98 具有如下特点：Windows 98 是一种图形用户界面的操作系统，Windows 98 用图形用户界面代替了 DOS 的字符用户界面，用户无须与难记忆的 DOS 命令打交道；提供丰富的应用程序，如 Windows 98 中的写字板、画图、娱乐、计算器、记事本、多媒体播放器等；提供并行处理能力：Windows 98 是一种多任务的操作系统，每个任务都有自己的窗口，多个任务并行运行，各窗口间可相互切换并相互交换信息；支持多媒体操作；所见即所得：在 Windows 98 中，由于采用了真实字体，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。



1.1.4 Windows NT 时代

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，以及在恶劣的运行条件下仍保持特定的稳定性和效率。这就是开发 Windows NT 的初衷。

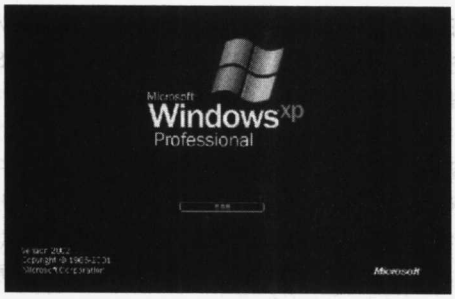
经历了 Windows NT 1.0、Windows NT 2.0、Windows NT 3.0、Windows NT 3.5 等阶段后，Windows NT Server 4.0 的推出受到业界的认可。这个版本的内核稳定性更高、系统更安全、界面更友好。此外，硬件的兼容性也有了很大进步。由于在研发投入方面花了很大力气，这个版本吸收了很多企业级操作系统的优点，许多企业用户称，Windows NT Server 4.0 是企业级操作系统的真正意义上的集大成者。



1.1.5 Windows 2000/XP/2003 时代

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。



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。

1.1.6 Windows Vista 展望

Windows Vista 是微软下一代操作系统，以前叫做 Longhorn（微软当初内部的代号）。比起以前的 Windows 版本，Windows Vista 更加安全、更加可靠也更加易于管理。作为微软的最新操作系统，Windows Vista 第一次在操作系统中引入了“Life Immersion”概念，即在系统中集成许多人性的因素，一切以人为本。使得操作系统尽最大可能贴近用户，了解用户的感受，从而方便用户。

从字面意义上看，Vista 的意思包括“狭长的景色、街景、展望、回想”等等。“展望”，相信很多人觉得这个词是尤其值得注意的。一位微软发言人进一步解释说：“今天，我们生活在一个充满‘更多’的世界里——更多信息、更多渠道、更多追求、更多机遇和更多责任。越来越多地，我们依赖电脑来帮助我们解决这些问题。说到底，我们所追求的，是突破一切障碍，把精力放在我们需要去做的事情上。我们要做的，是拥有属于自己的‘Vista’——无论是整理照片，还是查找文档、联络他人，抑或是通过电子方式进行团体的协作。”

1.2 Windows 的不安全因素

1. 代码庞大，代码重用

有一个“小程序定理”：程序中的 bug 和程序大小成正比。还有一句谚语：凡可能出错的地方就一定会出错。微软的程序员不是神，那么多行代码，还要求软件工程学上的完美，因此出错难免。

代码重用：要求代码重用就意味着在某个版本上出现的问题，就可能会在后续版本中都有问题，其他重用此代码的程序中也可能会有问题。

2. 盲目追求易用性和兼容性

毕竟是开公司，当然是怎么赚钱最多就怎么做，好用的东西，傻瓜的东西，大家当然愿意买。所以默认就什么都支持，什么都包含，什么都关联，什么都兼容。