中国刑事警察学院系列教材

常见操作系统分析

主编 汤艳君

CHANGJIAN CAOZUO XITONG FENXI

群众出版社

中国刑事警察学院系列教材

常见操作系统分析

主　编　汤艳君
副主编　罗文华

公安机关
内部发行

群众出版社
2008年·北京

图书在版编目（CIP）数据

常见操作系统分析/汤艳君主编. —北京：群众出版社，2008.7
（中国刑事警察学院系列教材）
ISBN 978-7-5014-4298-0

Ⅰ.常… Ⅱ.汤… Ⅲ.操作系统—高等学校—教材
Ⅳ.TP316

中国版本图书馆CIP数据核字（2008）第108961号

常见操作系统分析

主　　编：汤艳君
责任编辑：亢　健
特邀编辑：孟建国
封面设计：任普生

出版发行：群众出版社　电话：（010）52173000转
地　　址：北京市丰台区方庄芳星园三区15号楼
邮　　编：100078
网　　址：www.qzcbs.com
信　　箱：qzs@qzcbs.com
印　　刷：中国刑事警察学院印刷厂

开　　本：880×1230毫米　32开本
字　　数：316千字
印　　张：12.25
版　　次：2008年7月第1版　2008年7月第1次印刷
书　　号：ISBN 978-7-5014-4298-0/TP·16
定　　价：20.00元

中国刑事警察学院教材编审委员会

前　言

随着计算机应用的不断普及，有关计算机犯罪的案件也在不断增多，特别是针对操作系统漏洞进行攻击、利用操作系统提供的功能进行擦除和隐藏犯罪痕迹的案例屡见不鲜。如何能使计算机犯罪得到有效的惩治，对计算机犯罪侦查和取证人员提出了更高的要求，其中常用的操作系统知识是必须掌握的内容，只有在熟悉常用的操作系统功能、常见的操作系统漏洞、敏感数据存放位置、典型的文件系统类型、常用的操作系统安全配置等问题的基础上才能获得有效的电子证据和案件线索，为打击犯罪提供有利的保障。

为了培养高素质的计算机犯罪侦查和取证人员，我们编写了《常见操作系统分析》这本教材。该教材从计算机犯罪侦查和取证的角度出发，分析常见典型操作系统的相关功能，使从事计算机犯罪侦查和取证人员在办案过程中对操作系统了如指掌。

全书共分3篇15章。第1篇是Windows操作系统，主要包括Windows操作系统发展史、Windows操作系统的系统文件夹、Windows操作系统的系统进程、Windows操作系统的注册表、Windows操作系统的主流文件系统、Windows操作系统的安全管理等6章内容。第2篇是Unix/Linux操作系统，主要包括Unix与Linux操作系统发

展史、Linux 操作系统的主流文件系统、Linux 操作系统的数据删除与恢复、Linux 操作系统的文件操作、Linux 操作系统的日志文件管理、Linux 操作系统的系统安全管理等6章内容。第3篇是其他操作系统，主要包括嵌入式操作系统、Macintosh 操作系统、类Unix 操作系统等3章内容。

本教材的突出特点是实用性强，内容全面，基本涵盖了目前常见的操作系统类型。注重理论与实践的结合，突出专业特色。本教材既可作为计算机专业、计算机犯罪侦查和取证相关专业学生的教材，也可作为从事计算机犯罪侦查和取证人员的参考书。

本教材由汤艳君主编，负责整体结构设计并编写了第1章至第6章；罗文华编写了第7章至第12章，马贺男编写了第13章，于晓聪编写了第14章至第15章。

尽管在编写此教材过程中作者作很多努力，但由于水平有限，教材中不妥之处在所难免，敬请读者批评指正。

编者

2008年4月

目　录

第1篇　Windows操作系统

第　1　章

Windows 操作系统发展史

Windows 操作系统是微软（Microsoft）公司为个人计算机和服务器用户设计的操作系统，也被称为“视窗操作系统”。它的第一个版本由微软公司发行于1985 年，并最终获得了世界个人计算机操作系统软件的垄断地位。

1.1　Windows 1.0

Microsoft 在1983 年开始研发Windows 1.0，并于1985 年11 月20 日正式发布。由于仅仅是由字符堆砌，界面非常简陋，所以后来有人将其评价为最不成功的作品。Windows 1.0 的主要特点有：

引入了Apple Macintosh 中的鼠标功能，用户可以通过鼠标点击完成大部分的操作；自带了一些简单的应用程序，包括日历、

记事本、计算器等等；允许用户同时执行多个程序，并在各个程序之间进行切换，这对于DOS来说是难以想象的；可以显示256种颜色，窗口可以任意缩放，当窗口最小化的时候桌面上会有专门的空间放置这些窗口（其实就是现在的任务栏）；在Windows 1.0中另外一个重要的程序是控制面板(Control Panel)，不过功能非常有限。

1.2 Windows 2.0

Windows 2.0于1987年12月9日发布，与Windows 1.0相比，Windows 2.0做的改动并不多，但它基本上可以充分发挥当时的286的性能。回顾历史，会发现Windows 1.0和Windows 2.0这两个版本并没有取得很大的成功，原因其实并不在操作系统本身，而在于硬件和DOS操作系统的限制。Windows2.0的主要特点有：

用户可以缩放窗口，并可以同时显示多个窗口；突破640KB基地址内存的束缚，更多的内存可以充分发挥Windows的优势；加入了功能表和对话框；增强了键盘、鼠标的功能。

1.3 Windows 3.X

1990年5月22日，Microsoft迎来了第一个具有时代意义的作品——Windows 3.0，虽然很多人更愿意将Windows3.1作为Microsoft跨时代的作品，但毕竟Windows 3.0是Windows 3.x系列的起点，假如没有Windows 3.0的成功，也不会有更多人对后续产品的关注。Windows 3.0的主要特点有：

具备了模拟32位操作系统的功能，图片显示效果大有长进，对当时最先进的386处理器有良好的支持；提供了对虚拟设备驱

动（VxDs）的支持，极大改善了系统的可扩展性；用户界面和运行环境得到了很大的改进，系统开始支持16位色，DOS的文件管理程序被基于图标的程序管理器以及基于列表的文件管理器所取代；简化了程序的启动，打印管理器也诞生了，控制面板成为系统设置的核心；模仿了苹果公司Macintosh的设计，使用一些新的图标；开发了Software Development Kit（SDK）来帮助硬件厂商开发驱动程序，使操作系统能与硬件完美结合。

1992年4月，一个更为成熟的版本Windows 3.1诞生了。Windows 3.1添加了多媒体功能、CD播放器以及对桌面排版很重要的TrueType字体。次年发布的Windows for Workgroups 3.11又引入了对网络的支持——包括以太网和当时如日中天的Novell Netware，并利用对等网络的概念构建Windows工作组网络。

1994年Windows 3.2发布，这也是Windows系统第一次有了中文版。由于消除了语言障碍，降低了学习门槛，因此在国内得到了较为广泛的应用。

1.4 Windows 9X

随着Windows 3.3操作系统应用的不断普及，Windows操作系统也发生了巨大变化。

1.4.1 Windows 95

1995年8月24日Windows 95发布，这个操作系统开创Windows新的纪元。新的操作系统发生了质的变化，具有了全新的面貌和强大的功能，这在某种程度上也宣告了DOS时代的结束。Windows 95的主要特点有：

更加优秀的、面向对象的图形用户界面，从而减轻了用户的

学习负担；全32位高性能的抢先式多任务和多线程；内置了对Internet的支持；更加高级的多媒体支持（声音、图形、影像等）；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；良好的向下兼容性。

1.4.2 Windows NT

1996年8月，Windows NT 4.0发布，事实上Windows NT 4.0并不是Microsoft的第一款面向企业的操作系统，之前在1993、1994年Microsoft都相继发布了3.1、3.5等版NT系统，但它们都没掀起什么大的风浪，而Windows NT 4.0则彻底改善了Microsoft在服务器领域的优势。Windows NT4.0的主要特点有：

通信服务：内置强大的通信服务，如传输控制协议/Internet协议（简称TCP/IP）网络、路由和远程访问，可以简单地将这些性能添加到嵌入式解决方案中；完全地Win32 API支持：完全地支持Win32应用程序编程接口（API），可以跨所有Windows NT平台创建标准化应用程序；高级编程性能：高级编程性能包括支持组件对象模型（COM）、分布式COM（DCOM）和电话API（TAPI），使用者可以在一个可重用的、面向对象的环境中快速构建革新的解决方案；支持Windows NT服务：例如事件查看器和性能监视器，可以为使用者的嵌入式解决方案提供增强的监视和报告功能；远程可管理性：Microsoft和第三方提供的管理特性可以简化嵌入式解决方案的管理工作，甚至还可以将这些特性集成到信息技术（IT）管理基础构架中。

1.4.3 Windows 98

1998年6月25日Windows 98发布，这个操作系统基于Windows 95之上，并改良了对硬件标准的支持，例如MMX和AGP等。Windows 98 SE（第二版）发行于1999年6月10日，它包括了一系列的改进，例如加入了Internet Explorer 5、Windows Net-

meeting 等软件。总的来说，Windows98 是一款非常成功的产品，以至于现在仍有很多用户使用。Windows98 的主要特点有：

Windows 98 的一个最突出的特点就是往Windows 95 中加入了浏览器；融入了用于Internet 通信的套装工具，包括用于电子邮件的Outlook Express、网络视频会议NetMeeting、网上信息发布Netshow、网页制作FrontPage 和个人Web 服务器Personal Web Server 等；Windows 98 提供了FAT 文件系统的改进版本FAT32；实现了完整的用户注册功能，这样可以支持更全面的多用户访问体系及提供用户级安全保证等。

1.4.4 Windows Me

相对Windows 98 来说，Windows Me 变化更多的还是在其界面上，似乎也仅仅如此，由于Windows XP 的快速推出，Windows Me 犹如昙花一现，很快就消失出我们的视野。Windows Me 的主要特点有：

系统还原：如果说Windows Me 在功能上和Windows 98 有什么较大的区别，那就应该是系统还原。这个功能也延续到Windows 后面的版本；Windows 似乎什么都想集成，这次其集成了压缩功能，并且还可以对压缩的文件进行加密，但美中不足的是不能对文件进行压缩的操作。不过更多的用户并不喜欢这个功能，而更多的还是使用其他压缩/解压缩工具软件。

1.5 Windows 2000 系列

在微软发布Windows NT4.0 之后，微软NT 产品线的下一个目标自然是Windows NT5.0，不过微软在这之后又一次使用了年份来为Windows 产品命名。

1.5.1 Windows 2000

Windows 2000 于2000 年年初发布，它有四个版本，其中的Windows 2000 Professional 大致可以算是Windows NT Workstation 4.0 的升级版，由于这个版本的市场目标是取代Windows 95、Windows 98 以及Windows NT Workstation 4.0，因此设计上走的是“博采众长”的路子，可以同时用于小型企业和个人桌面。另外的三个版本主要面向较大的公司用户，包括Server、Advanced Server 和Data Center Server。Windows 2000 的重要特点有：

软件易用性和以前Windows 98 等操作系统非常类似，软件的界面也相对好看了一些；Windows 2000 在稳定性、安全性等方面也取得了长足的进步，特别是稳定上，摆脱了Windows 95 和Windows 98 死机频繁的困扰；由于Windows 2000 属于Windows NT 的升级版，其网络管理功能大大增强；硬件上更大的支持也让Windows 2000 有了更高的性能，Windows 2000 Professional 最多支持达4GB 的RAM 和两路对称多处理器。Professional 是桌面操作系统，它的前一个版本是 Windows NT 4.0 workstation 版本。适合移动家庭用户使用，可以用于升级Windows 9x 和 NT 4。它以 NT 4 的技术为核心，采用标准化的安全技术，稳定性高，最大的优点是不会再像 Windows 98 那样频繁地出现非法程序的提示而死机。Windows 2000 Server 是服务器版本，它的前一个版本是 Windows NT4 .0server 版。即可面向一些中小型的企业内部网络服务器，但它同样可以应付大型网络中的各种应用程序的需要。Server 在 NT 4 的基础上作了大量的改进，在各种功能方面有了更大的提高。Advanced Server 是 Server 的企业版，它的前一个版本是 Windows NT 4.0 企业版。与 Server 版不同的是，Advanced Server 具有更为强大的特性和功能。它对 SMP（对称多处理器）的支持要比 Server 更好，支持的数目可以达到 4 路。Datacenter

Server 是强大的服务器系统，可以支持 32 路 SMP 系统和 64GB 的物理内存。该系统可用于大型数据库、经济分析、科学计算以及工程模拟等方面，另外还可用于联机交易处理。

1.5.2 Windows XP

Windows 以往的用户界面一直饱受批评，但2001 年10 月25 日，Windows XP 出现让人们改变了他们的看法，并且和以前的 Windows 桌面系统相比稳定性也大大提高，不过由于微软把越来越多的第三方提供软件整合在自己的操作系统中，XP 开始受到了最猛烈的批评。这些软件包括防火墙、媒体播放器（Windows Media Player），即时通讯软件（Windows Messenger），以及它与 Microsoft Pasport 网络服务的紧密结合，这都被很多计算机专家认为是安全风险以及对个人隐私的潜在威胁。Windows XP 的主要特点有：

Windows XP 的用户界面比以往的视窗软件更加友好；充分考虑到了人们在家庭联网方面的要求；也充分考虑了数码多媒体应用方面的要求；由于硬件上又一次的升级，Windows XP 的运行速度再次得到加快；充分考虑电脑的安全需要，内建了极其严格的安全机制，每个用户都可以拥有高度保密的个人特别区域。

1.5.3 Windows 2003

为了继续保持领先的地位，Microsoft 继续开发新的操作系统，2003 年4 月底，Windows 2003 发布了。这个操作系统进一步加强了其在各方面的优势，不过由于Windows XP 已经完全满足几乎所有用户的需要，所以Windows Server 2003 的目标定在了利润更高的服务器市场。Windows Server 2003 的主要特点有：

协助共享、管理、保护和备份内部网络上文件的工具和技术；加强在电子邮件及通讯方面的管理；保护 Internet 连接安全的技术，并支持应用关系数据库；使Windows Server 2003 成为广泛地