刘育楠　马军　等编著

# 局域网安全与代理服务器设置

- 系统与网络安全基础
- 杀毒软件和防火墙
- 代理服务器设置
- VPN虚拟专用网
- 连接共享和路由网关
- 代理服务器应用方案
- 病毒和木马
- 数据安全和加密传输
- 无线局域网
- 服务器安全

清华大学出版社

# 局域网安全
# 与代理服务器设置

刘育楠　马　军　等编著

清华大学出版社

北　京

## 内 容 简 介

本书全面介绍了局域网络安全和代理服务器设置的技术。内容包括操作系统安全设置，网络安全设置，防火墙设置，典型的代理服务器和特殊功能的代理服务器设置，局域网中代理服务器方案介绍，病毒和木马攻防，数据安全传输，无线局域网建设与安全防护，服务器安全基础等。

本书图文并茂，内容翔实，含有大量的实际应用方案举例。无论是局域网的网络管理员还是通过代理服务器联网用户，都能从中获得需要的内容。



**图书在版编目(CIP)数据**

局域网安全与代理服务器设置/刘育楠等编著.—北京：清华大学出版社，2004

ISBN 7-302-08789-X

Ⅰ.局… Ⅱ.刘… Ⅲ.①局部网络—安全技术—基本知识②网络服务器—基本知识 Ⅳ.①TP393.108 ②TP368.5

中国版本图书馆 CIP 数据核字(2004)第 054576 号

**出 版 者**：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

**社 总 机**：010-62770175　　**客户服务**：010-62776969

**组稿编辑**：孟毅新

**文稿编辑**：许书明

**封面设计**：久久度企划

**版式设计**：康　博

**印 刷 者**：北京市世界知识印刷厂

**装 订 者**：三河市化甲屯小学装订二厂

**发 行 者**：新华书店总店北京发行所

**开　　本**：185×260　**印张**：22.5　**字数**：547 千字

**版　　次**：2004 年 7 月第 1 版　2004 年 7 月第1 次印刷

**书　　号**：ISBN 7-302-08789-X/TP·6237

**印　　数**：1～4000

**定　　价**：32.00 元

# 前　言

局域网的安全一直以来都是网络安全的重点和难点。要想在微软操作系统构建的局域网系统上保证系统安全和数据安全，实在不是一件容易的事情。作为管理员，应该把工作重点放在系统的权限设置和服务器的安全配置，而作为每一个普通用户，也应该了解一些网络安全基础知识来配合网络管理员的工作。

网络安全工作的一个重要的特点就是持续性，今天的安全并不能延续到明天。虽然安全技术每天都在更新，但是，安全的核心内容和原则问题基本不会发生变化。所以，本书就从最基本的安全准则介绍开始，系统地介绍了构筑安全的局域网所需要的大部分内容，包括防火墙和代理服务器设置等。此外还介绍了关于病毒和木马、黑客攻击防范、服务器安全配置等相关内容。在这些安全内容中还穿插介绍了局域网使用代理服务器的数种方案，这些方案的实际应用性强，可以立刻付诸实践。

本书第 1 章概括地介绍了系统和网络安全基础的基本知识，包括两类典型的操作系统的安全基础知识，TCP/IP 协议及其安全问题、黑客攻击、病毒防范、常用的网络命令，这些内容是为了让读者更好地进行代理服务器设置和网络安全防范。

第 2 章介绍了系统的安全策略，日志系统，典型的安全配置方案。安全策略分为 3 部分，包括密码策略，Windows 9x 和 Windows 2000 的安全策略，这是一些原则性安全的介绍。日志系统以 Windows 2000 为例，详细介绍了如何利用日志来检测黑客攻击，介绍了典型的操作系统 Windows 98、Windows 2000 Server 和 Windows XP 的安全配置方案，这 3 套方案都可以根据需要直接付诸实施。

第 3 章对防火墙展开介绍，包含两个部分，即病毒防火墙和数据过滤防火墙，介绍了金毒霸 V 和 Symantec Antivirus 等病毒防火墙产品，在数据防火墙中介绍了适用于个人的天网防火墙个人版，以及适用于服务器的 ZoneAlarm Pro。

第 4~7 章针对代理服务器的设置进行了详细的介绍。包括应用型代理服务器、网关型代理服务器、VPN 设置等方面的内容。其中第 4 章介绍了 WinGate 这套强大的应用型代理服务器的使用和设置方法，二级代理服务器和多代理服务器等特殊功能代理服务器设置方法，自动配置脚本的设置和编写方法。第 5 章的内容主要是针对 VPN 的，从 VPN 的工作原理说起，以 Windows 2000 Server 和 WinGate 为例介绍了 VPN 服务器的搭建；此外还以 Windows 98 和 Windows XP 为例，介绍了设置 VPN 客户端的方法。第 6 章介绍了 Internet 连接共享，NAT 网关等网关型代理服务器的设置方法。第 7 章对前面 3 章的内容进行了总结，分析了 4 种实用代理服务器方案，包括家用的双机互联方案，办公室或者网吧多机共享方案，局域网单、双网卡

方案。

第 8 章介绍了蠕虫病毒和木马程序的清除方法，这一章中介绍的内容主要是提供指导性方法，从病毒源头上进行堵截，所以多数是介绍一些手动清除方案。此外，这一章还穿插介绍了邮件病毒和 QQ 木马病毒等内容。

第 9 章从协议安全讲起，介绍了邮件加密和签名设置，PGP 软件的使用方法，还描述了一些和 IP 相关的欺骗问题，例如 IP 欺骗、Email 欺骗，Web 欺骗等。

第 10 章介绍了另外一种网络互联形式，即无线网络互联方式的组建和安全性问题。

第 11 章简单地介绍了一些常用服务器的安全问题和入侵防范方法。服务器安全内容包括了 Web、FTP、远程终端服务器、SQL Server 等的安全设置；入侵问题中介绍了一种典型的扫描工具 SuperScan 以及 Windows 2000 Server 的入侵检测操作内容。

读者可以根据需要阅读相关的章节，即可完成安全配置工作。本书作为参考资料或手册，可以为实际操作提供很好的帮助。

由于编者水平有限，书中难免有疏漏和不足之处，恳请广大读者提出宝贵意见。

作　者

# 目　　录


**第 1 章　系统与网络安全基础** …… 1

1.1　操作系统安全基础 …… 1

1.1.1　操作系统安全概述 …… 1

1.1.2　Windows 9x 系统的安全问题 …… 3

1.1.3　Windows 2000 和 Windows XP 系统的安全问题 …… 4

1.2　网络安全基础 …… 7

1.2.1　TCP/IP 协议 …… 7

1.2.2　网络协议安全 …… 13

1.2.3　防火墙技术 …… 15

1.2.4　病毒传播 …… 16

1.2.5　黑客攻击 …… 17

1.2.6　常用网络命令 …… 22

1.3　本章小结 …… 32

**第 2 章　系统安全设置** …… 34

2.1　系统安全策略 …… 34

2.1.1　系统密码 …… 34

2.1.2　Windows 9x 的安全配置 …… 38

2.1.3　Windows 2000 的安全策略 …… 41

2.2　日志分析 …… 50

2.2.1　日志系统简介 …… 50

2.2.2　Windows 2000 的日志保护和伪造 …… 53

2.3　操作系统的典型安全配置 …… 58

2.3.1　Windows 98 系统的安全配置实例 …… 58

2.3.2　Windows 2000 Server 系统的安全配置实例 …… 64

2.3.3　Windows XP 系统的安全配置实例 …… 72

2.4　本章小结 …… 76

**第 3 章　杀毒软件和防火墙** …… 77

3.1　杀毒软件 …… 77

3.1.1　杀毒软件简介 …… 77

3.1.2　个人杀毒软件金山毒霸 V 的配置 …… 79

3.1.3　企业级病毒防火墙的配置 …… 84

3.2 防火墙 …… 90
3.2.1 防火墙原理 …… 90
3.2.2 防火墙的选择 …… 94
3.2.3 天网防火墙个人版 …… 98
3.2.4 Windows XP 防火墙 …… 103
3.2.5 服务器防火墙 ZoneAlarm Pro …… 105
3.3 本章小结 …… 112

**第 4 章 代理服务器设置 …… 113**
4.1 代理服务器介绍 …… 113
4.1.1 代理服务器基本知识 …… 113
4.1.2 HTTP 代理服务器 …… 116
4.1.3 Socks 代理服务器 …… 118
4.2 代理服务器软件 WinGate …… 124
4.2.1 WinGate 安装 …… 124
4.2.2 WinGate 服务器配置和管理 …… 127
4.3 特殊用途代理服务器 …… 135
4.3.1 二级代理服务器 …… 136
4.3.2 多代理服务器 …… 143
4.4 自动代理脚本 …… 152
4.4.1 自动代理脚本简介 …… 152
4.4.2 如何编写简单的自动配置脚本 …… 153
4.5 本章小结 …… 160

**第 5 章 VPN虚拟专用网 …… 161**
5.1 VPN 的基础知识 …… 161
5.1.1 VPN 的原理简介 …… 161
5.1.2 企业选用 VPN 的优点 …… 162
5.1.3 VPN 协议技术 …… 164
5.2 VPN 服务器的搭建 …… 172
5.2.1 Windows 2000 Server VPN 服务器 …… 172
5.2.2 Windows Server 2003 VPN 服务器 …… 178
5.2.3 WinGate 实现的 VPN …… 182
5.3 VPN 客户端 …… 188
5.3.1 VPN Windows 98 客户端设置 …… 188
5.3.2 VPN Windows XP 客户端设置 …… 190
5.4 本章小结 …… 193

**第 6 章　连接共享和路由网关** ……194
6.1　连接共享和软件路由介绍 ……194
6.1.1　连接共享 ……194
6.1.2　软件路由器 ……196
6.1.3　网络地址转换 ……201
6.1.4　局域网共享上网几种方法的比较 ……204
6.2　连接共享和软件路由配置实例 ……205
6.2.1　局域网连接准备 ……205
6.2.2　Internet 连接共享 ……206
6.2.3　Sygate ……209
6.2.4　WinRoute ……214
6.2.5　Windows 2000 Server 配置 NAT 路由器 ……225
6.2.6　NAT 配置访问内部网络 ……230
6.3　本章小结 ……232

**第 7 章　代理服务器应用方案** ……233
7.1　小型代理服务器方案 ……233
7.1.1　双机互联拨号方案 ……233
7.1.2　多机共享宽带方案 ……236
7.2　局域网代理服务器方案 ……238
7.2.1　双网卡服务器 ……238
7.2.2　单网卡服务器 ……239
7.3　流量计费 ……241
7.3.1　RADIUS 服务器 ……241
7.3.2　CCProxy 流量计费 ……244
7.4　本章小结 ……247

**第 8 章　病毒和木马** ……248
8.1　蠕虫病毒 ……248
8.1.1　蠕虫病毒介绍 ……248
8.1.2　防杀蠕虫病毒 ……251
8.2　邮件病毒 ……256
8.2.1　邮件病毒的基本知识 ……256
8.2.2　设置安全的邮件客户端 ……258
8.2.3　杀毒软件中对于邮件病毒的防范 ……260
8.3　木马程序 ……262
8.3.1　木马程序的由来 ……262
8.3.2　防范木马程序 ……263

8.3.3 清除木马程序 …… 264
8.3.4 常见开放端口和相关木马 …… 273
8.3.5 QQ 木马病毒 …… 279
8.4 本章小结 …… 280

**第 9 章 数据安全和加密传输 …… 281**
9.1 协议安全 …… 281
9.1.1 安全的传输协议 …… 281
9.1.2 IPSec …… 286
9.2 加密和数字签名 …… 291
9.2.1 Outlook Express 设置数字签名和加密 …… 291
9.2.2 文件加密压缩 …… 293
9.2.3 PGP 软件 …… 294
9.3 和 IP 相关的欺骗问题 …… 300
9.3.1 IP 与 MAC 地址的绑定 …… 300
9.3.2 IP 欺骗 …… 301
9.3.3 Email 欺骗 …… 303
9.3.4 Web 欺骗 …… 304
9.4 本章小结 …… 307

**第 10 章 无线局域网 …… 308**
10.1 无线网络简介 …… 308
10.1.1 无线网络基础知识 …… 308
10.1.2 组建小型无线局域网 …… 312
10.2 无线网络安全 …… 313
10.2.1 无线网络的安全问题 …… 313
10.2.2 防范无线网络入侵 …… 316
10.3 Windows XP 与 802.11 无线局域网 …… 317
10.3.1 IEEE 802.11 无线局域网 …… 318
10.3.2 Windows XP 配置无线网实例 …… 320
10.4 本章小结 …… 324

**第 11 章 服务器安全 …… 325**
11.1 小型服务器的安全问题 …… 325
11.1.1 Web 服务器的安全 …… 325
11.1.2 Windows 2000 系统配置 IIS …… 328
11.1.3 FTP 服务器的安全 …… 333
11.1.4 远程终端服务器的安全 …… 334
11.1.5 SQL Server 的安全 …… 334

11.2　服务器入侵防范 …… 335
11.2.1　服务器入侵的常用方法 …… 335
11.2.2　网络扫描工具 SuperScan …… 337
11.2.3　入侵检测简介 …… 341
11.2.4　Windows 2000 服务器入侵检测 …… 343
11.3　本章小结 …… 347

# 第1章　系统与网络安全基础

**本章要点：**

- Windows 9x 安全问题
- Windows 2000 和 Windows XP 安全问题
- TCP/IP 协议
- 黑客攻击
- 常用网络命令

本章主要介绍一些与系统和网络安全相关的安全基础知识，包括典型的操作系统安全问题、网络协议介绍和协议安全、黑客攻击技术等。

## 1.1　操作系统安全基础

这一节主要介绍和操作系统相关的安全基础知识。这里把微软的 Windows 操作系统分为两类，即 Windows 9x 和 NT 核心的操作系统，分别介绍其中诸如密码安全等比较常见的安全问题以及应对策略。

### 1.1.1　操作系统安全概述

微软的 Windows 操作系统面世以来，出现了很多的版本，有 Windows 3.1、Windows 95、Windows 98、Windows Me、Windows NT、Windows 2000、Windows XP、Windows 2003 等版本。其中每套操作系统根据用途还有一些分支的版本，比如 Windows XP 就分为家庭版(Windows XP Home Edition) 和专业版(Windows XP Professional Edition)。

这些操作系统除 Windows 3.1 这样的早期版本外，现在常用的版本里面基本上可以分为两大类：一类是 Windows 9x，包括 Windows 95、Windows 98、Windows Me；另外一类是以 NT 为核心的操作系统，从 Windows NT 到 Windows 2003，都是这样一类操作系统。以下的安全基础就是从以上的分类中取出其代表性的操作系统进行介绍。

操作系统涉及的安全问题比较多，主要涉及到系统密码安全、系统漏洞、黑客攻击、病毒等问题。

下面介绍关于系统密码安全和系统漏洞问题。

### 1. 系统密码安全

操作系统的密码有很多种，最主要的密码安全问题是指系统登录密码。

一般情况下，登录的用户名和密码要保证一定的复杂程度，难以让其他人猜到，否则容易被黑客利用来攻击系统。

对于系统密码，一般建议使用 7 个或者更多的字符，不要仅仅使用数字作为密码，而且密码中应该尽可能多地包括字母、标点符号等。一个建立密码的技巧就是用标点连接多个随机的单词，比如“I，want%door”；或者使用一个数字连接两个单词等；甚至可以用某个熟悉的地名或者某个物品的名字加上数字来设立密码。

对于某些关键系统的密码设置有个基本的标准：

- 密码应该不少于 8 个字符。
- 不包含字典里的单词、不包括姓氏的汉语拼音。
- 同时包含多种类型的字符，比如，大写字母(A,B,C, ……Z)、小写字母(a,b,c,z)、数字(0,1,2,……9)、标点符号(@,#,!,$,%,& ……)。

此外，建议经常更换密码，最好是每个月更换一次密码。管理员也应当设定密码必须修改的期限，并设置旧的密码不能再次被使用。

### 2. 系统漏洞

微软的操作系统的漏洞问题一直以来都是系统的最大隐患。

微软的网站上时常都有新的补丁程序发布。有的补丁程序是针对某些小问题的，这样的补丁程序一般称为 Hotfix，通常文件大小都不大。经过一段时间的积累，微软会把其中的重要的补丁打包形成一个大的补丁程序，修复以前发现的绝大多数漏洞，这样的补丁程序称为 Service Pack，这样的补丁程序比较大。

通常来讲，高版本的补丁程序包含了低版本的补丁程序。所以，只需要安装最高版本的 Service Pack 即可。

IE 浏览器是现在大家常用的浏览网页的软件。IE 的各个版本里面也包含了一些漏洞，这些漏洞的补丁会随着系统的补丁一起发布。推荐大家使用最新版本的 IE 浏览器。

黑客的攻击常常是建立系统漏洞的基础上的。一个打过补丁修补过漏洞的操作系统一般是很难被攻破的。

很多流行的病毒也有一些是基于系统的漏洞来传播的，比如说冲击波病毒。只要安装了关于冲击波病毒的系统补丁，这种病毒就对系统无可奈何了。

系统漏洞对于系统的安全危害是很严重的，因此，及时地给系统安装新的补丁程序对于保证系统的安全是非常重要的。

除了操作系统本身的漏洞，安装的其他系统软件也可能包含漏洞。无论软件商的制作多么小心，也不能完全保证软件的安全性。通常来讲，软件包越大，漏洞越多。一般情况下，大的厂商的软件产品经过了更多的测试和修改，所以安全系数比较高。

一旦发现了新的漏洞，产品发布商会提供升级版本或者补丁，这个时候用户需要根据需要进行升级。

还有一些系统软件的默认设置是具有漏洞的，修改设置后即可保证漏洞不被利用，比如IIS。对于这样的系统漏洞，只需要加强管理和小心设置，漏洞就不会被利用了。

除了升级安装系统补丁外，还有一些网络安全和系统安全产品，使用这些产品可以增强系统的安全，比如防火墙类产品，就可以保证系统免受攻击和病毒袭击等。建议在有安全需求的系统上安装必要的防火墙等安全产品。

对于远程访问，需要更加注意安全问题。Windows 2000 和 Windows XP 等操作系统上提供了远程桌面的服务，安装了这样的服务就需要加强系统的安全设置，否则很有可能从远程桌面被攻破。对于远程桌面，需要设定合适的访问权限；对于用户的访问都需要设定好日志记录，应该根据需要设立最低的访问权限。

Windows 操作系统的安全问题很复杂，涉及到很多方面。下面把 Windows 9x 和 NT 核心的这两类操作系统分开进行介绍。

## 1.1.2　Windows 9x 系统的安全问题

Windows 98 和 Windows Me 现在还被很多人作为首选的操作系统使用。这两套操作系统从发布到现在，可以说已经经过了很多的修改，基本上是没有漏洞问题了。但是这类的操作系统安全系数实在不高。

这两套系统的核心基本上是一致的，所以这两套系统的安全问题基本上也是相同的。Windows 9x 其内核脆弱，容易崩溃，也就是通常说的死机。此外，它提供的网络工具有限，安全性差。

中国有句古话，知己知彼，百战不殆。要想解决 Windows 9x 系统的安全问题，必须了解系统的特点及基本的安全知识。

### 1. 系统漏洞

Windows 9x 系统中的漏洞问题很多，常见的有 NetBIOS 缓存漏洞、无效驱动器类型拒绝服务漏洞、ICMP 包溢出漏洞、共享漏洞、NetBIOS Over TCP/IP 漏洞、concon 漏洞等。

这里以 concon 漏洞为例介绍一下。

在 Windows 9x 中有 3 个设备驱动程序：CON，输入及输出设备驱动程序；NUL，空设备驱动程序；AUX，辅助设备驱动程序。

这 3 个程序只要被直接运行，就会引起系统的死机。比如运行 C:\CON\CON 或 C:\AUX\AUX 等。更加严重的问题是，这个漏洞可以通过资源共享来远程执行。比如运行 \\192.168.0.2\C\CON\CON，其中\192.168.0. 2 为对方的 IP 地址，C 为对方的共享盘符，运行的结果是可以导致 IP 地址为 192.168.0.2 的计算机死机。

这个漏洞解决办法很多，最简单的办法是将系统升级成高版本，即 Windows 2000 或者 Windows XP。如果无法升级，可以下载安装补丁程序 conconfix 并添加到“启动”组中。还有一个折中的办法，就是安装网络防火墙，过滤掉这样的访问。

其他一些漏洞的解决办法也基本类似，即找到相应的补丁给系统安装，或者直接升级到高版本的操作系统。

**2. IE 浏览器漏洞**

IE 浏览器漏洞也是个很典型的问题。针对 IE 的漏洞攻击，在很多恶意网站遇到。有一些特洛伊木马程序也是通过 IE 漏洞进行传播的，比如 QQ 自动消息发送器等。

这里以 IE 4.0 的关于 ActiveX 控件的漏洞为例进行介绍，这个漏洞允许远程通过 IE 访问来创建和覆写本地文件。这个漏洞可以在 IE 用户点击网页上的一个超链接时发生，并且可以将 HTML 应用程序文件中的可执行程序添加在 Windows 95 或 98 计算机的开始菜单中，在该机器下次启动时，程序就会自动执行。通常这种方法被用来放置特洛伊木马。

要修补这个漏洞，最简单的办法是把IE的安全级别设置为High，或者把Active Scripting 给屏蔽掉，把 ActiveX Controls 和 Plug-ins 都关闭。但是这样设置以后也有缺点，比如会导致某些站点的正常 ActiveX 控件不能访问等问题。

结合系统漏洞，IE 漏洞还可以导致 Windows 98 系统死机，比如 IE 打开含有如下代码的网页就会导致死机：

```
<html>
<body>
<img src="c:/con/con">
</body>
</html>
```

在 Windows 2000 等系统上没有这样的漏洞，高版本的 IE 6.0 也没有这个漏洞。所以最好的建议是升级 IE 的版本或者操作系统。

**3. 系统登录安全**

Windows 9x 系统的登录安全也是没有太大保证的。通常来讲，Windows 9x 系统的登录密码基本上没有安全性可言。只要可以使用电脑，就可以通过一定的方法来破解或者绕开 Windows 9x 系统的登录而进入操作系统。这是由于系统的本身架构决定的，所以要获得安全的操作系统，要升级到 Windows 2000 以上的操作系统。

### 1.1.3 Windows 2000 和 Windows XP 系统的安全问题

从 Windows 2000 开始，微软的操作系统开始明显地给人安全的感觉了，无论是文档的存储还是网络的传输，Windows 2000 和 Windows XP 操作系统的安全性能都得到了很大的提升，并且在功能上也有了很大的改进。但是，系统的漏洞问题依然存在，比如针对 Windows 2000 发布的 Service Pack 的补丁已经到了第 4 版，而且还有新的漏洞被发现，微软也不断有新的补丁发布。

Windows 2000 和 Windows XP 的操作系统中开始有了服务管理、用户权限管理和组策略等功能，这些对于系统安全是很重要的。

对于服务器版本(比如 Windows 2000 Server)，如果安装了 IIS 服务器或者 MS SQL 服务器的话，就会有关于这些服务器软件的安全问题。默认安装的操作系统通常会加载一些不必要的服务，有些服务对于系统可能是很危险的。

### 1. 系统漏洞

针对 Windows 2000，微软已经发布了非常多的系统补丁。由此可见，Windows 2000 的系统漏洞问题很多。

比如冲击波病毒和冲击波杀手病毒，就是利用了 Windows 2000 等操作系统的 RPC 漏洞问题来进行传播和系统攻击的。这样的病毒危害性极大，不安装补丁的计算机在有病毒活动的局域网中很快就会被病毒感染。

这里举例说明一个 Windows 2000 中文版最有名的漏洞：输入法漏洞。这个漏洞在没有打过补丁或者只是安装了 Service Pack 1 的 Windows 2000 的系统上存在。利用这个漏洞入侵的操作方法如下：

(1) 在登录界面中输入用户名的时候调出某个输入法，比如微软拼音输入法。

(2) 右键单击输入法语言栏，然后弹出菜单中选择“帮助”|“输入法入门”命令。

(3) 打开输入法操作指南帮助文件后，找到其中某个超级链接，单击右键，选择弹出菜单中的“跳转到 URL”命令。

(4) 在弹出窗口的地址栏中输入需要访问的盘符，就可以得到访问硬盘的权限了。这个时候甚至可以进入控制面板修改用户密码。

在开启了远程终端服务的 Windows 2000 服务器上，如果还有这个漏洞，那就更加危险了，通过终端连接远程桌面就可以非法进入服务器进行任何操作。具体的操作步骤和上面类似。

如果是新安装的 Windows 2000 或者 Windows XP，或者是在补丁发布之前安装的系统的话，安装新版本的 Service Pack 是非常重要的。Windows 2000 已经发布了 Service Pack 4 补丁包；Windows XP 已经发布了 Service Pack 1 补丁包。

在安装系统补丁前，可以查看一下系统的版本。以 Windows 2000 为例，右键单击“我的电脑”图标，在弹出的菜单中选择“属性”命令，就可以在弹出的“系统特性”对话框中看到系统的版本和安装 Service Pack 补丁状况，如图 1-1 所示。举例的这套系统已经安装了 Service Pack4 补丁程序。

这些补丁程序在微软的网站上可以下载。可能的话，把下载的服务软件包补丁程序保存，这样以后使用起来就方便了。安装补丁程序的方法很简单，一步步执行向导程序，重启计算机后就可以了。

### 2. 本地安全策略工具

Windows 2000 和 Windows XP 等系统提供了本地安全策略工具，这个工具实际上把注册表中的一些安全选项给提取了出来，做成了一个管理器的界面。对于安全设置操作系统，这样降低了设置的难度。

在安全策略管理器中，可以设定账户的密码和锁定策略以及本地的审核策略和安全选项，对于公钥策略也有一些设置选项。

要使用本地安全策略设置工具，可以在任务栏上选择“开始”|“控制面板”命令，在控制面板中进入“管理工具”，双击“本地安全策略”图标，弹出安全策略设置窗口，如图 1-2 所示。

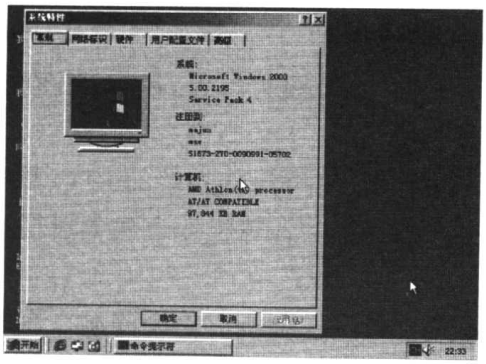

图 1-1　查看 Windows 2000 系统版本和补丁状况

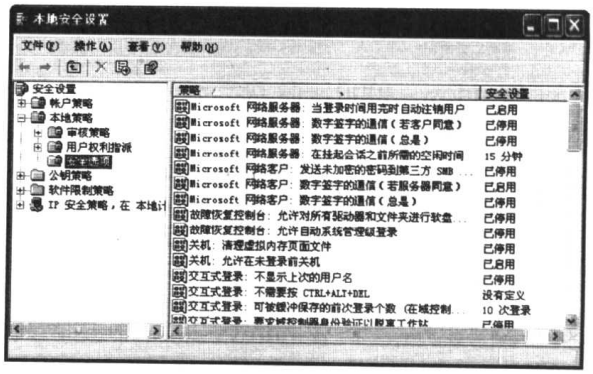

图 1-2　本地安全设置

本地安全设置中分为账号策略、本地策略、公钥策略、软件限制策略等。例如需要设置这样一个安全选项：在登录时不要显示上次的用户名。其操作步骤如下：

(1) 图 1-2 所示的本地安全策略窗口中，单击展开“本地策略”|“安全选项”文件夹，在右侧列表中选择“交互式登录：不显示上次的用户名”选项。

(2) 双击该项目，弹出设置对话框，选中“已启用”单选按钮，如图 1-3 所示。

(3) 单击“应用”按钮，即立即应用修改后的设置，单击“确定”按钮，回到本地安全设置界面。

通过本地安全策略管理器，还可以类似的设置审核策略启用安全日志，设置密码锁定策略防止通过网络暴力尝试破解密码等。

### 3. 文件格式安全

Windows 2000 和 Windows XP 都支持 NTFS 的文件格式，这种文件格式有更好的权限设置。从安全角度讲，使用 NTFS 格式比使用 FAT 32 格式要好很多。

如果是使用 FAT 32 格式，可以使用 Convert 程序将其转化为 NTFS。使用 Convert 命令的格式是：

```
Convert /fs:ntfs X:
```

X 代表需要转化的盘符字母。

相比 Windows NT 来讲，Windows 2000 和 Windows XP 使用的 NTFS 5 的安全性更好，提供了一些新的单个权限，比如创建文件、写数据等，如图 1-4 所示，权限选项很完整。

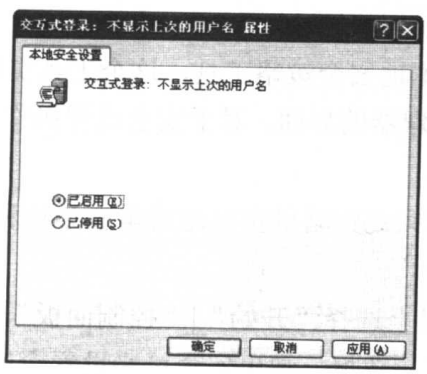

图 1-3　修改本地安全设置

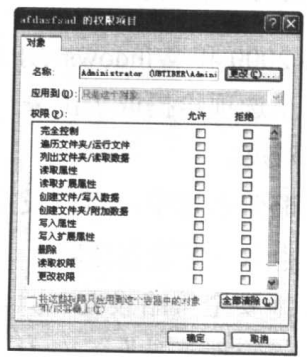

图 1-4　文件权限设置窗口

对于每个文件夹和文件，NTFS 文件格式支持相关的审核设置，如图 1-5 所示。

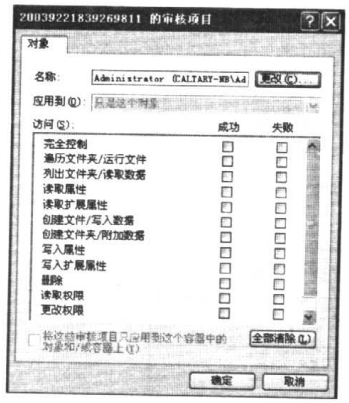


图 1-5　文件审核设置

除了可以设置权限和审核之外，还可以指定文件和文件夹的所有者、有效权限等。这些设置合起来构成了一套完整的安全设置体系。由此可见，使用 NTFS 的文件系统，其安全性要大大超出 FAT 32 文件系统。

#### 4. 系统账号安全

Windows 2000 和 Windows XP 系统中都附带了两个默认的账号，Administrator 和 Guest。Administrator 是系统的默认管理员账号，Guest 是系统默认的来宾账号。这两个账号可以通过本地安全设置重新命名。对于这两个账号，有以下两点需要注意：

- 一定不要把 Administrator 的密码设为空值。
- 最好禁用 Guest 账号，或者把 Guest 账号的密码设成一个很长的密码，以防被破解利用。

关于 Windows 2000 和 Windows XP 的安全问题，这里只介绍了典型的四个方面，具体的内容和配置方案请参考第 2 章的内容。

## 1.2　网络安全基础

下面这一节介绍一些网络安全的基础知识，包括 TCP/IP 协议和协议安全、病毒传播和黑客攻击等方面的介绍。

### 1.2.1　TCP/IP 协议

TCP/IP 协议族是现在的 Internet 的主流协议，Internet 的发展正是有了 TCP/IP 协议才到了如此繁荣的地步。

#### 1. OSI 模型

要说起 TCP/IP 协议，还得先介绍一下 OSI 模型。OSI 7 层开放系统互联模型，一直以来