信息安全与网络对抗技术实践

主　编◎张文静　蒋　岚　周巧雨　刘　晓

西南交通大学出版社

信息安全与网络对抗技术实践

主　编　张文静　蒋　岚
　　周巧雨　刘　晓
副主编　许雯雯　沙为超　罗　琳
　　赵瑞华　朱　敏　薛长举

西南交通大学出版社
·成　都·

图书在版编目（CIP）数据

信息安全与网络对抗技术实践 / 张文静等主编. —
成都：西南交通大学出版社，2019.9
ISBN 978-7-5643-7146-3

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①计算机网络－安全技术
－研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2019）第 201236 号

Xinxi Anquan yu Wangluo Duikang Jishu Shijian

信息安全与网络对抗技术实践

主　编 / 张文静　蒋　岚　周巧雨　刘　晓

责任编辑　黄庆斌
特邀编辑　刘姗姗
封面设计　严春艳

西南交通大学出版社出版发行
（四川省成都市金牛区二环路北一段 111 号西南交通大学创新大厦 21 楼　610031）
发行部电话：028-87600564　028-87600533
网址：http://www.xnjdcbs.com
印刷：四川森林印务有限责任公司

成品尺寸　185 mm × 260 mm
印张　10　　字数　250 千
版次　2019 年 9 月第 1 版
印次　2019 年 9 月第 1 次

书号　ISBN 978-7-5643-7146-3
定价　30.00 元

课件咨询电话：028-81435775
图书如有印装质量问题　本社负责退换

前　言

信息安全和计算机网络对抗技术的发展对国家安全和经济建设有着极其重要的作用。因此，研究和学习信息安全知识，掌握相应主流技术迫在眉睫。目前，世界各国都积极开展了信息安全和网络对抗技术的研究和教育。为此，编者根据自己的科学实践，以多年来的科研成果为基础，结合信息技术和网络安全的教学经验，编写了本书。

本书兼顾基础知识和基本操作方法，是学生学习信息安全和网络对抗技术的入门教材。信息安全和网络对抗课程作为一门综合性科目，具有课程理论相对抽象和繁杂、理论实践联系紧密、实践性强的特点。学生经过大量的上机实践，能较好地掌握和熟悉所学内容。

本书既涵盖信息安全与网络技术的基础理论知识，又包括相关实用技术。按照从一般到特殊的原则，将理论知识和实践紧密结合，对相关领域进行深入探讨。全书分为八章，每章后有课后作业，学生可根据知识掌握程度自行设计完成，旨在培养学生分析问题、解决问题的能力和专业实践能力。各章节的主要内容安排如下：第 1 章为网络基础实验，让学员体验网络体系结构知识的实际应用，学会处理常见网络故障；第 2 章为密码技术实验，以 PGP 软件为例重点介绍加密技术在实际中的应用；第 3 章为网络攻击技术实验，包括常见的攻击手段的实施及软件的使用；第 4 章为典型攻击防御技术实验，在第 3 章的基础上实现对常见攻击手段的防御；第 5 章、第 6 章是主机安全防护实验，包括主机系统安全设置以及 Web、FTP 基本安全的防护训练；第 7 章为防火墙技术实验，以理论结合实践的方式讨论防火墙领域的若个问题，在实践中体会防火墙的使用方法；第 8 章为数据备份与恢复实验，帮助学生掌握 Windows 自带的以及常用备份工具的使用，使其能熟练应用。

本书讲解细致，具有内容全面、图文并茂的特点。学生在学习理论知识的同时，能掌握相应的操作技能。由于编者水平有限，书中难免有错误之处，恳请专家和广大读者批评指正，以利于我们不断修正。

编　者

2019 年 5 月

目 录

第 1 章　网络基础实验

网络环境的搭建，不单是指最底层的网线和相关设备的连接，还包括 TCP/IP 层的网络建设以及更高层的服务器、各种应用程序的设定以及操作系统网络服务配置等。网络架构的设计是否科学合理，将直接影响一个网络是否能稳定运行。网络架构中的设备及配置的服务承担着网络内信息传输的重要责任。

实验 1.1　自我排查网络故障

【实验目的】

（1）会判断网络协议是否正常。
（2）会判断网络适配器是否正常。
（3）会判断网络线路是否正常。
（4）会判断 DNS 是否工作正常。

【实验内容】

（1）利用 Ping 命令自我排查网络故障。
（2）网络邻居访问故障排查。

【预备知识】

（1）计算机网络基本知识。
（2）MS-DOS 命令的基本操作知识。

【实验原理】

Ping 是 Windows、Unix 和 Linux 系统下的一个命令。Ping 也属于一个通信协议，是 TCP/IP 协议的一部分。利用“ping”命令可以检查网络是否联通，可以很好地帮助用户分析和判定网络故障。

应用格式：Ping　IP 地址

该命令还可以附加许多参数使用，具体请键入“Ping”按回车即可看到详细说明。Ping 发送一个 ICMP（Internet Control Messages Protocol），即因特网信报控制协议；响应请求消息给目的地并报告是否收到所希望的 ICMP echo（ICMP 回声应答）。它是用来检查网络是否通畅或者网络连接速度的命令。作为一个网络管理员或者黑客来说，Ping 命令是第一个必须掌握的 DOS 命令，它所利用的原理是这样的：利用网络上机器 IP 地址的唯一性，给目标 IP 地址发送一个数据包，再要求对方返回一个同样大小的数据包来确定两台网络机器是否连接相通，以及时延是多少。

【实验环境】

局域网。

【实验工具】

MS-DOS [版本 5.1.2600]，全名为 Microsoft Windows XP DOS[版本 5.1.2600]，用于 DOS 命令输入。

【实验用时】

30 分钟/实例。

【实验过程与步骤】

实验 1.1.1　利用 Ping 命令自我排查网络故障

（1）在 Windows 系统“运行”对话框中输入“cmd”，如图 1.1.1 所示，进入 MS-DOS 界面，如图 1.1.2 所示。

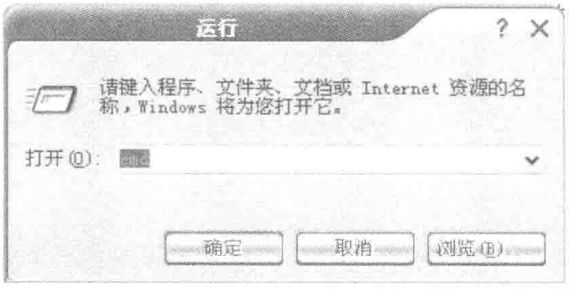


图 1.1.1　运行界面

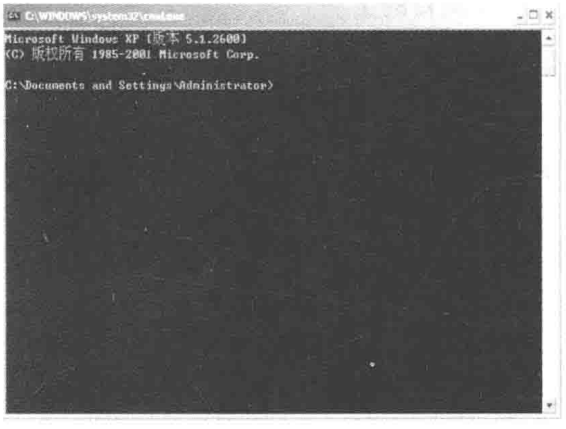


图 1.1.2　MS-DOS 界面

（2）输入命令：ping 127.0.0.1，检测本地机 TCP/IP 协议是否能正常工作，如图 1.1.3 所示。

（3）输入命令：ipconfig，查看本地计算机网络适配器分配的 IP、GW、DNS 等信息，如图 1.1.4 所示。

图 1.1.3　表明协议正常工作界面

图 1.1.4　表明网络配置信息界面

（4）输入命令：ping 192.168.0.68，查看网络适配器（网卡或 MODEM）工作是否正常，如图 1.1.5 所示。

（5）输入命令：ping 192.168.0.128，查看网络线路是否出现故障（防火墙拦截除外），如图 1.1.6 所示。

图 1.1.5　表明网络适配器正常界面

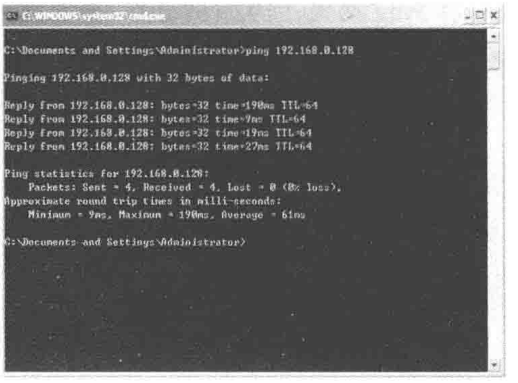


图 1.1.6　表明网络线路正常界面

（6）输入命令：ping www.google.com，查看 DNS 工作是否正常，如图 1.1.7 所示。

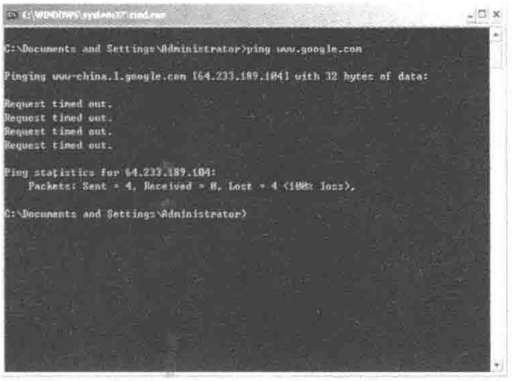


图 1.1.7　DNS 解析网址成功界面

实验 1.1.2　网络邻居访问故障排查

网络邻居访问故障的排查，首先要确定网络运行是否正常，需进行网络故障排查。如果网络运行正常，再对网络邻居涉及的各种服务进行排查。

（1）利用命令查看网络信息。ipconfig 命令界面如图 1.1.8 所示。

（2）Ping 本地回环地址，127.0.0.1，如图 1.1.9 所示，检测本地机 TCP/IP 协议是否能正常工作。

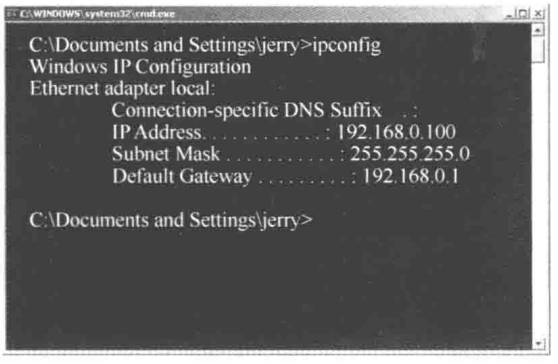


图 1.1.8　ipconfig 命令界面

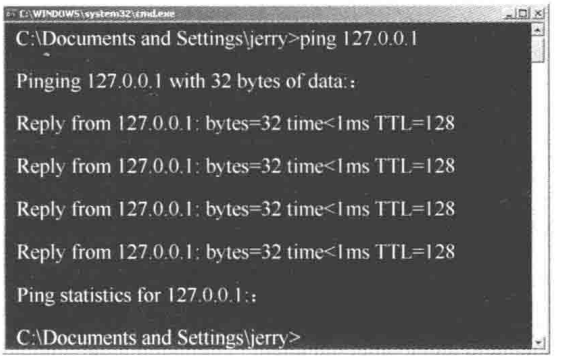


图 1.1.9　Ping 命令界面

（3）Ping 本机 IP 地址，192.168.0.100，查看网络适配器（网卡或 MODEM）工作是否正常，如图 1.1.10 所示。

（4）Ping 网关，192.168.0.1，查看网关配置是否正确，如图 1.1.11 所示。

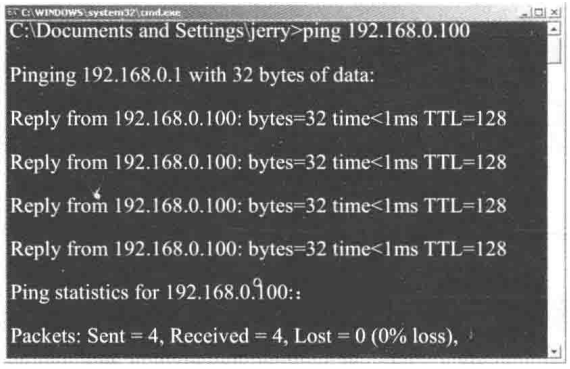


图 1.1.10　Ping 本机 IP 地址

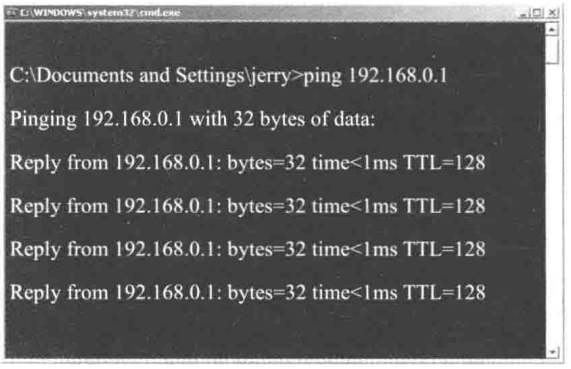


图 1.1.11　Ping 网关

（5）Ping 外网 IP 地址，202.205.3.130，如图 1.1.12 所示。

（6）Ping 外网网站域名，www.sina.com.cn，查看 DNS 工作是否正常，如图 1.1.13 所示。

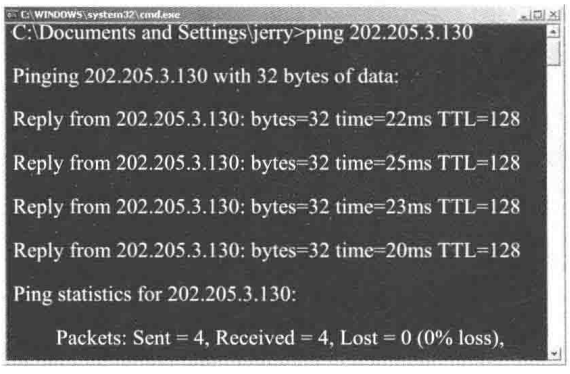


图 1.1.12　Ping 外网 IP 地址

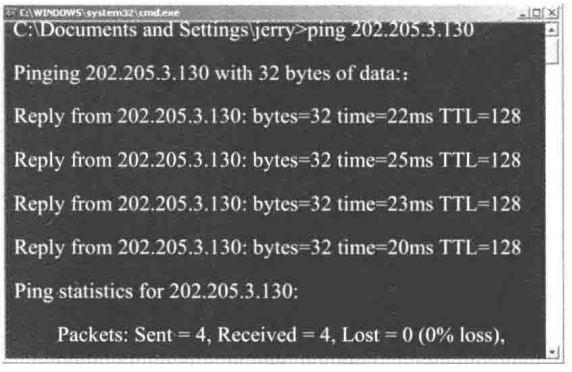
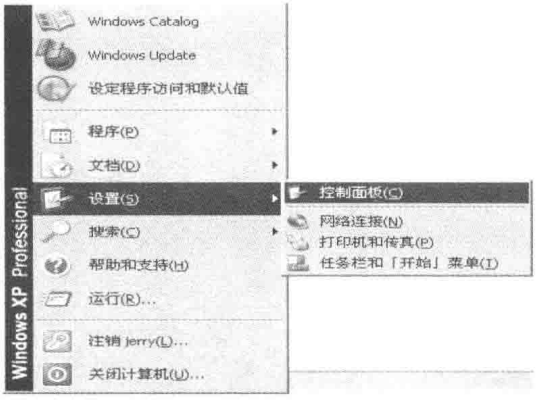


图 1.1.13　Ping 外网网站域名

（7）点击“开始”/“设置”/“控制面板”，如图 1.1.14 所示。



（a）设置

（b）控制面板界面

图 1.1.14　控制面板

（8）双击进入管理工具，如图 1.1.15 所示。

（9）双击进入计算机管理，如图 1.1.16 所示。

（10）展开本地用户和组。

图 1.1.15　管理工具

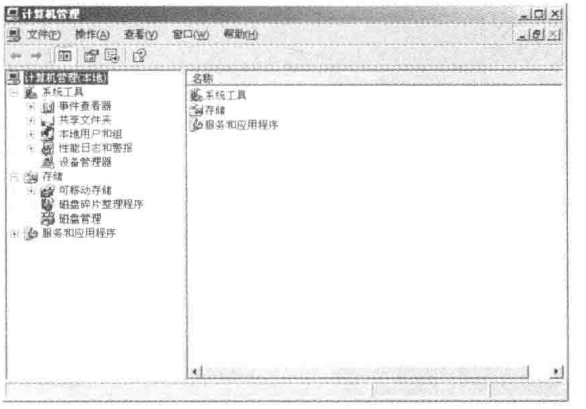


图 1.1.16　计算机管理

（11）点击“用户”，双击“Guest”，如图 1.1.17 所示，打开属性界面，如图 1.1.18 所示。

（12）点击取消“账户已停用”，完成后点击“确定”。

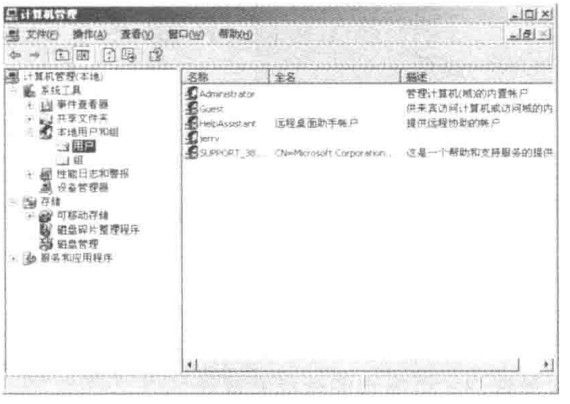


图 1.1.17　计算机管理

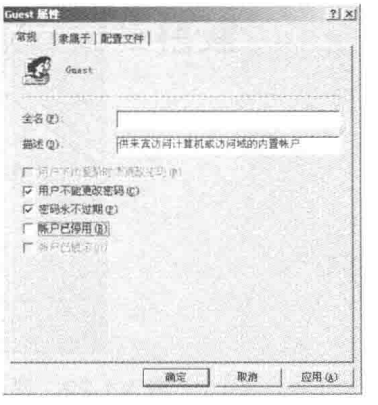
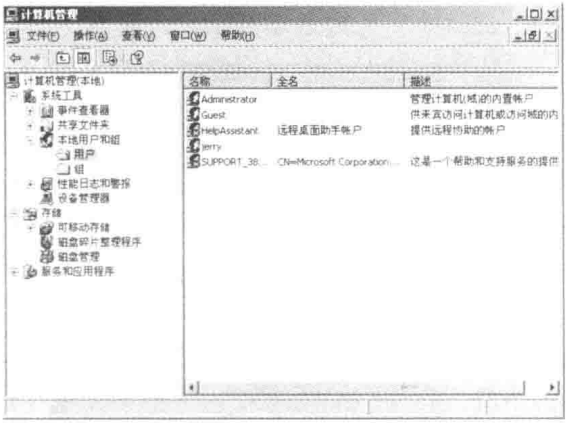


图 1.1.18　Guest 属性

（13）关闭计算机管理，双击“本地安全策略”，如图 1.1.19 所示。



（a）计算机管理

（b）管理工具

图 1.1.19　计算机管理与管理工具

（14）双击进入本地安全策略，如图 1.1.20 所示。

（15）展开本地策略，点击“安全选项”，双击开启“网络访问：本地账户的共享和安全模式属性”页面，如图 1.1.21 所示。

图 1.1.20　本地安全策略

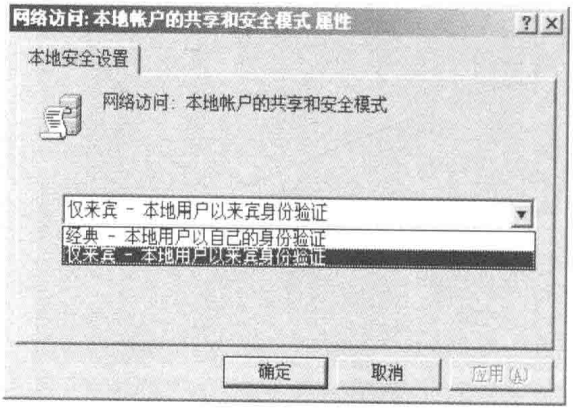


图 1.1.21　网络访问：本地账户的共享和安全模式属性

（16）选择“仅来宾”，如图 1.1.22 所示。

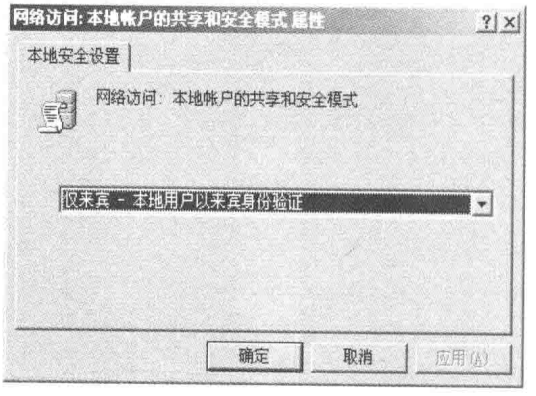


图 1.1.22　网络访问：本地账户的共享和安全模式属性

（17）完成后点击“确定”。

（18）点击“用户权利指派”，双击“拒绝从网络访问这台计算机”，如图 1.1.23 所示，打开属性页面，如图 1.1.24 所示。

图 1.1.23　本地安全设置

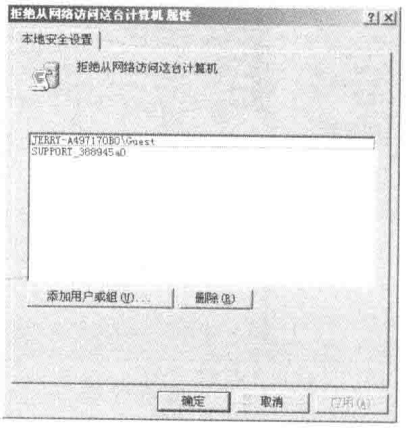


图 1.1.24　拒绝从网络访问这台计算机属性

（19）点选“Guest”，点击“删除”，如图 1.1.25 所示。

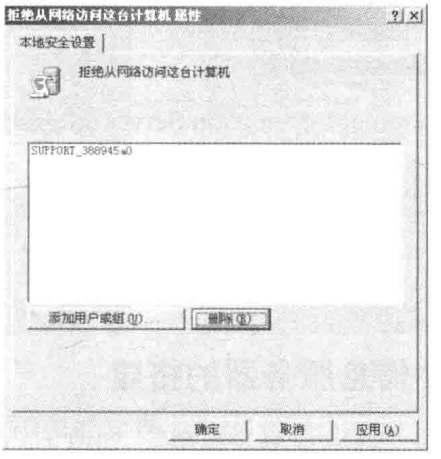


图 1.1.25　拒绝从网络访问这台计算机属性

（20）完成点击“确定”。

实验 1.2　Internet 信息服务器的初步搭建

【实验目的】

（1）了解 Windows 系统下常见的网络服务应用。

（2）掌握各种网络服务器的搭建和配置方法。

【实验内容】

（1）Internet 信息服务器的初步搭建。

（2）建立新的 FTP 站点。

【预备知识】

（1）计算机的基本操作方法。

（2）计算机网络基本知识。

（3）计算机网络服务应用的基本知识。

【实验原理】

IIS（Internet Information Services），是一个 World Wide Web Server。Gopher Server 和 FTP Server 全部包容在里面。IIS 意味着用户能发布网站，IIS 是随 Windows NT Server 4.0 一起提供的文件和应用程序服务器，是在 Windows NT Server 上建立 Internet 服务器的基本组件。它与 Windows NT Server 完全集成，允许使用 Windows NT Server 内置的安全性以及 NTFS 文件系统建立强大灵活的 Internet/Intranet 站点。IIS（Internet Information Server），即互联网信息服务，是一种 Web（网页）服务组件，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它使得在网络（包括互联网和局域网）上发布信息很容易。

【实验环境】

局域网。

【实验工具】

因特网信息服务器（Internet Information Server 6.0，IIS6.0）。

【实验用时】

30 分钟/实例。

【实验过程与步骤】

实验 1.2.1　Internet 信息服务器的搭建

（1）在控制面板中打开“添加或删除程序”，如图 1.2.1 所示。

图 1.2.1　控制面板

（2）点击“添加/删除 Windows 组件”，如图 1.2.2 所示。

（3）弹出 Windows 组件向导界面，如图 1.2.3 所示。

图 1.2.2　添加/删除 Windows 组件

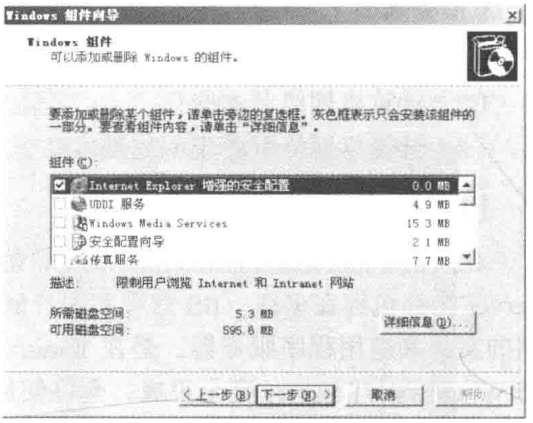


图 1.2.3　Windows 组件向导

（4）选中“应用程序服务器”项，点击“详细信息”（或双击来打开），如图 1.2.4 所示。

（5）勾选“Internet 信息服务（IIS）”，并点击“详细信息”，如图 1.2.5 所示。

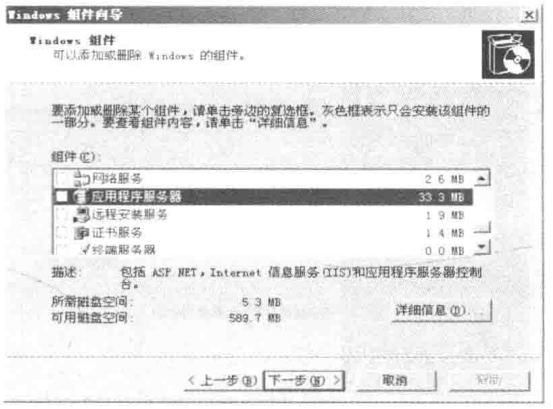


图 1.2.4　Windows 组件向导

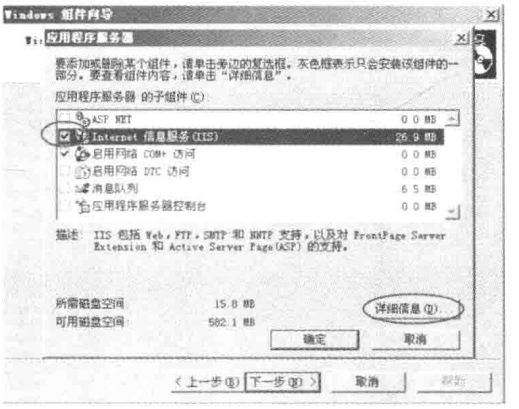


图 1.2.5　应用程序服务器

（6）可以看到 Internet 信息服务的组件列表，如图 1.2.6 所示。

（7）勾选中“文件传输协议（FTP）服务”，完成后“确定”，如图 1.2.7 所示。

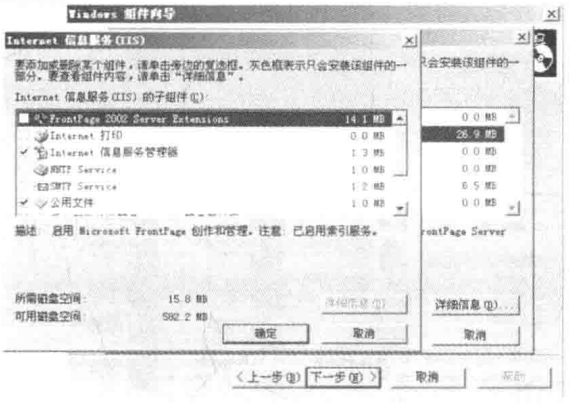


图 1.2.6　Internet 信息服务

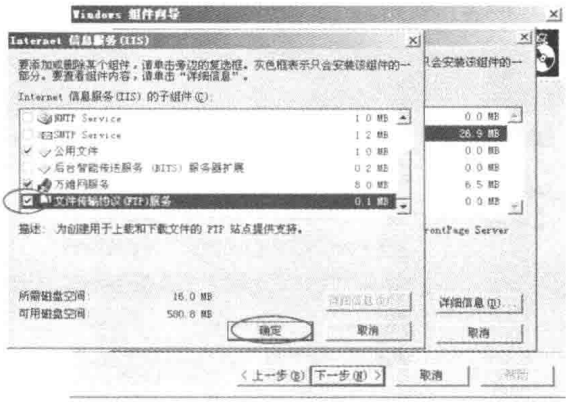


图 1.2.7　Internet 信息服务

（8）再次点击“确定”，如图 1.2.8 所示。

（9）组件选择完成后，点击“下一步”进行组件的安装，如图 1.2.9 所示。

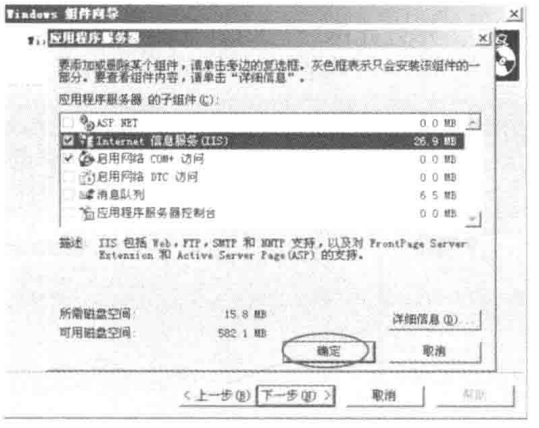


图 1.2.8　应用程序服务器

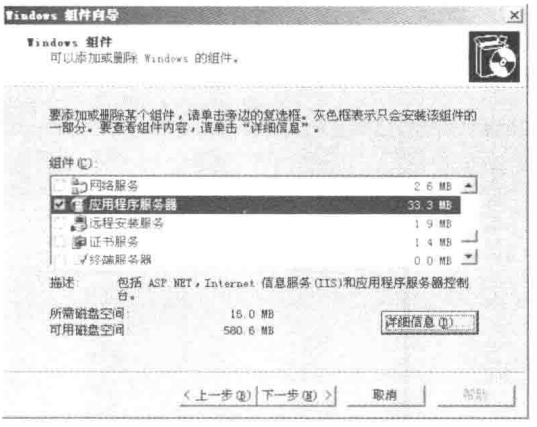


图 1.2.9　Windows 组件向导

（10）安装过程如图 1.2.10 所示，此过程中应保证 Windows 2003 系统光盘放在光驱中。

（11）点击“完成”，完成 Windows 组件的安装，如图 1.2.11 所示。

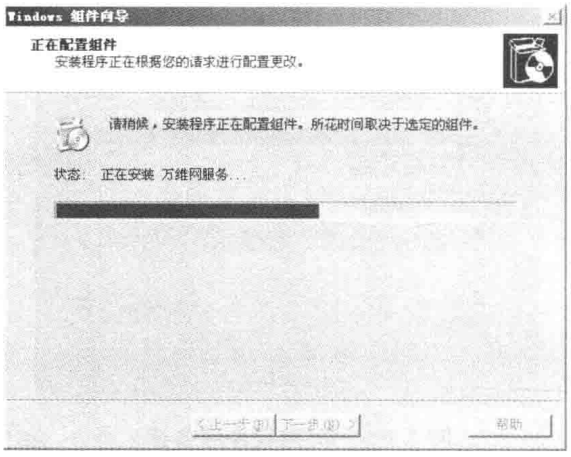


图 1.2.10　Windows 组件向导

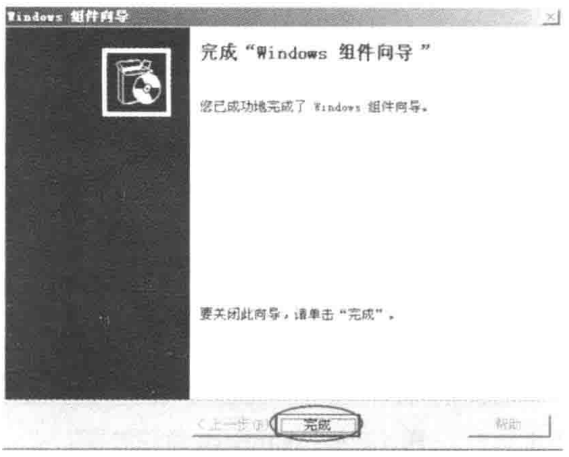


图 1.2.11　Windows 组件向导

（12）点击进入“管理工具”，如图 1.2.12 所示。

（13）双击打开“Internet 信息服务（IIS）管理器”，如图 1.2.13 所示。

图 1.2.12　控制面板

图 1.2.13　管理工具

（14）Internet 信息服务（IIS）管理器界面如图 1.2.14 所示。

（15）可以看到“网站”下存在一个“默认网站”，并且此网站已对外开放，如图 1.2.15 所示。

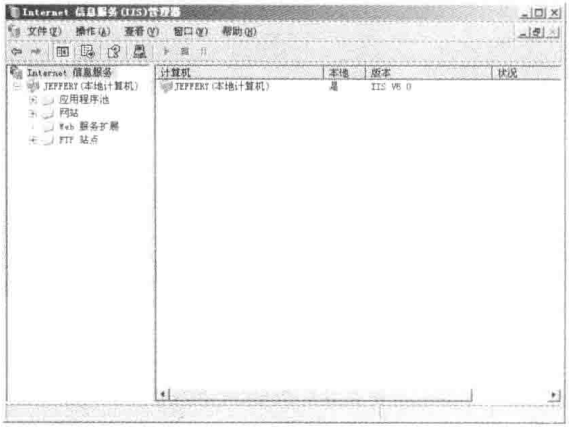


图 1.2.14　Internet 信息服务管理器

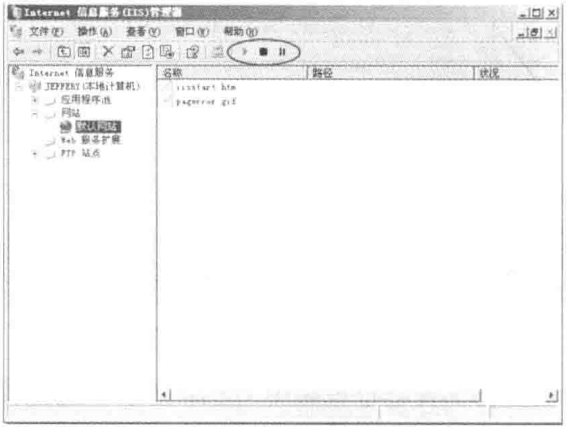


图 1.2.15　Internet 信息服务管理器

（16）同理，“FTP 站点”下存在一个“默认 FTP 站点”，同样对外开放，如图 1.2.16 所示。

（17）利用此主机的 IP 地址，测试访问其 Web 服务，如图 1.2.17 所示。

图 1.2.16　Internet 信息服务管理器

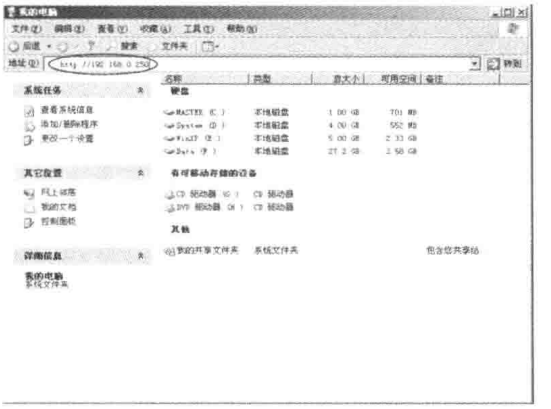


图 1.2.17　我的电脑

（18）可以看到“建设中”字样的网页，如图 1.2.18 所示，说明 Web 服务已经正常工作。

（19）再测试访问其 FTP 服务，如图 1.2.19 所示。

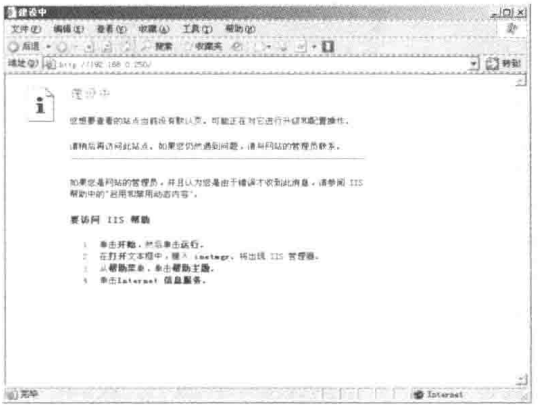


图 1.2.18　建设中

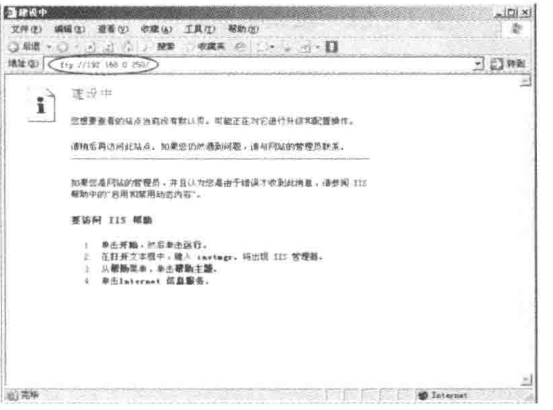


图 1.2.19　建设中

（20）正常显示 FTP 站点（但因为并未配置文件发布，所以站点资源为空），如图 1.2.20 所示。由此可以表明包含 Web 站点和 FTP 站点的 IIS 服务已成功搭建。

（21）右键点击网站的“默认站点”，选择“属性”，如图 1.2.21 所示。

图 1.2.20　FTP 站点

图 1.2.21　设置默认网站属性