反黑
教学基地

VIP精品指南
特别奉献

反黑风暴

网络渗透技术攻防高手修炼

超大容量 超值享受

- 理论+实战 图文+视频=让读者不会也会
- 任务驱动式讲解，揭秘多种黑客攻击手法
- 攻防互参，全面确保用户网络安全
- 挑战自我，享受黑客攻防的乐趣

武新华 王英英 李 伟 等编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

反黑风暴

网络渗透技术攻防高手修炼

武新华　王英英　李　伟　等编著

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书由浅入深、图文并茂地再现了网站入侵与脚本技术快速防杀的全过程，内容涵盖：创建安全测试环境、踩点侦察与漏洞扫描、渗透入侵数据库的 Web 脚本攻击、木马欺骗、渗透入侵的“通道”、缓冲区溢出实现渗透入侵与提权、溢出后开辟控制通道、Cookies 欺骗与防御技术、XSS 跨站脚本攻击技术、横向提权的暗道渗透、渗透入侵中的嗅探与欺骗技术、拒绝服务攻击技术、网络渗透技术的系统防护、网络渗透技术的终极防范等应用技巧，并通过一些综合应用案例，向读者讲解了黑客网络渗透技术攻防工具多种应用的全面技术。

本书内容丰富全面，图文并茂，深入浅出，面向广大网络爱好者，同时可作为一本速查手册，也适用于网络安全从业人员及网络管理者。

图书在版编目（CIP）数据

网络渗透技术攻防高手修炼 / 武新华等编著. —北京：电子工业出版社，2011.1
（反黑风暴）
ISBN 978-7-121-12573-7

Ⅰ. ①网… Ⅱ. ①武… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 247367 号

策划编辑：郭鹏飞
责任编辑：鄂卫华
印　　刷：中国电影出版社印刷厂
装　　订：中国电影出版社印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：28　字数：717 千字
印　　次：2011 年 1 月第 1 次印刷
定　　价：58.00 元（含光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言 FREFACE

随着技术发展，网络安全越来越依赖于整体防护。与此同时，网络结构越来越复杂，攻击者入侵网络的手法也不再单一，逐步渗透的入侵攻击技术与行为已成为主流。渗透入侵技术非常隐蔽，难以检测，一旦网络中存在某个缺口，就很有可能导致整个网络的全盘崩溃。同时，渗透攻击本身又是一种高级的入侵手法，在入侵的过程中涉及普通入侵技术、特殊攻击技术和社会工程学等，是从“技术”与“人”两个层面展开的攻击。

全面了解攻击者的渗透入侵行为，已成为维护网络安全所必需，因此，对网络渗透攻击进行深入分析，帮助网络安全工作者了解黑客渗透攻击行为，最终更好地维护网络安全，已成为现实的需要。

关于本书

网络渗透技术是通过运用黑客攻击的方法与工具，对企业网络进行各种手段攻击来找出系统存在的漏洞，从而给出网络系统存在的安全风险的一种实践活动。通过模拟现实的网络攻击，渗透测试证实恶意攻击者有可能获取或破坏企业的数据资产。网络渗透可以成为攻击者手中的一种破坏性极强的攻击手段，也可以成为网络管理员和安全工作者保护网络安全的重要实施方案。而常见网络安全图书往往仅针对网络入侵中的某一部分或某几部分进行介绍，因此适用面比较窄，实用价值不高。

本书从实际应用出发，通过详细讲解攻击者习惯采用的各种渗透攻击手段与方法，揭露出网络中广泛存在、却总被忽视的安全漏洞，并结合笔者长期积累的安全防护经验，指出相应的防范要点。本书具备较强的专业性和针对性，在网络安全工作中极具参考意义和实用价值。

本书内容

渗透入侵技术非常隐蔽，难以检测，一旦网络中存在某个缺口，就很有可能导致整个网络的全盘崩溃。同时，渗透攻击本身又是一种高级入侵手法，在入侵过程中涉及普通入侵技术、特殊攻击技术和社会工程学等，是从“技术”与“人”两个层面展开的攻击。书中全面系统地讲解了攻击者在渗透中可能采取的各种入侵手法，并给出了高效的防范方案，有助于网络安全维护人员掌握黑客的攻击行为，更好地维护网络安全。其主要内容包括：网络渗透测试基础、安全测试环境、虚拟机、踩点侦察与漏洞扫描、渗透入侵数据库与木马欺骗、缓冲区溢出实现网络渗透入侵与提权、溢出后开辟控制通道、从口令破解到隐藏账户开门、攻击不同网络设备、横向提权的暗道渗透、渗透入侵中的嗅探与欺骗技术、拒绝服务攻击技术、网络渗透技术终极防范等。

本书对黑客攻击中所使用到的渗透入侵技术和手段进行了全面的分析、讲解，从渗透入侵的基础开始，逐步深入到渗透入侵的各种常见及高级手法，覆盖完整、系统而严谨的安全知识体系。

本书特色

本书在编著过程中，力求做到原理清晰、透彻，内容全面、深入，并制作了配套教学视频，整理出部分程序代码，以帮助读者真正深入地掌握渗透攻击及防范技术。

- 语言轻松有趣，便于速查，快速解决问题
- 重在实际操作，理论淡化
- 丰富的攻击防御技巧
- 视频演示一学就会
- 黑客以及病毒防范感兴趣的、实用的一切资料、工具等进行赠送
- 充分利用以往出书的视频文件作为赠送

本书适合人群

本书紧紧围绕“攻”、“防”两个不同的角度，在讲解黑客网络渗透技术的同时，介绍了相应的防范方法，图文并茂地再现了网络渗透与防御的全过程。可作为专业的网络安全管理人员、网络安全技术研究者阅读，在实际工作中具有极高的参考价值；也可作为相关专业学生的学习资料和参考资料。

本书作为一本面向广大网络爱好者的速查手册，适合于如下读者学习使用：

- 没有多少电脑操作基础的广大读者
- 需要获得数据保护的日常办公人员
- 喜欢看图学习的广大读者
- 相关网络管理人员、网吧工作人员等
- 明确学习目的的读者、喜欢钻研黑客技术但编程基础薄弱的读者
- 网络管理员、广大网友等

本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。本书的编写情况是：杨平负责第 1 章，孙世宁、李防负责第 2 章，王英英负责第 3、4、5 章，安向东负责第 6 章，李伟负责第 7、8、9 章，段玲华负责第 10 章，王肖苗负责第 11 章，吕志华负责第 12 章，张晓新负责第 13 章，陈艳艳负责第 14 章，最后由武新华统审全稿。

需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后最好不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记切记！

我们的联系方式：zhangbg@phei.com.cn

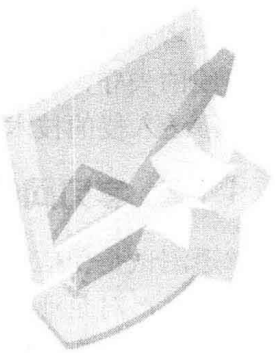
编著者

2010 年 10 月

目 录 CONTENTS

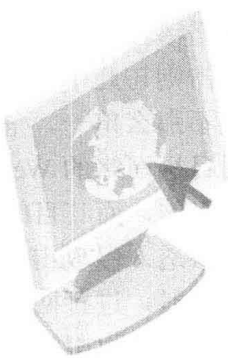
第1章

初识网络渗透测试



重点提示：

- 网络渗透概述
- 渗透测试需要掌握的知识
- 形影不离的“渗透测试”与攻防



本章主要介绍网络渗透测试的相关概述、需要掌握的渗透测试基础知识以及渗透测试与攻击的分类和手段等内容，有助于读者深刻了解网络渗透测试的相关内容和学习网络渗透测试的意义等。

对于众多网络工作者来说，导致网络攻击事件频繁发生的原因并不重要，重要的是要了解攻击者是如何进行攻击的，采用的是哪种途径和什么攻击手段，以及如何更好地防御攻击者的入侵等，这就需要网络工作者掌握相关的网络渗透测试知识。

1.1 网络渗透概述

网络渗透是保护信息和网络安全的重要途径，也是受信任的第三方进行的一种评估网络安全的活动，它通过运用黑客攻击的方法与工具，对目标网络进行各种手段的攻击来找出系统存在的漏洞，从而给出网络系统存在的安全风险的一种实践活动。

1.1.1 什么是网络渗透攻击

为了保障网络的安全，网络管理员往往会严格地规划网络的结构，区分内部与外部网络进行网络隔离，设置网络防火墙，安装杀毒软件，并做好各种安全保护措施。然而绝对的安全是不存在的，潜在的危险和漏洞总是相对存在的。

“网络渗透攻击”是对大型的网络主机服务器群组采用的一种迂回渐进式的攻击方法，通过长期而有计划地逐步渗透攻击进入网络，最终完全控制整个网络。

“网络渗透攻击”之所以能够成功，是因为网络上总会有一些或大或小的安全缺陷或漏洞。攻击者利用这些小缺口一步一步地将这些缺口扩大、扩大、再扩大，最终导致整个网络安全防线的失守，并掌控整个网络的权限。因此，作为网络管理员，完全有必要了解甚至掌握网络渗透入侵的技术，这样才能有针对性地进行防御，从而保障网络的真正安全。

1.1.2 学习网络渗透测试的意义

渗透测试是受信任的第三方进行的一种评估网络安全的活动，它通过运用各种黑客攻击方法与工具，对企业网络进行各种手段的攻击，以便找出系统存在的漏洞，给出网络系统存在的安全风险，是一种攻击模拟行为。

网络渗透攻击与普通网络攻击的不同在于：普通的网络攻击只是单一类型的攻击；网络渗透攻击则与此不同，它是一种系统渐进型的综合攻击方式，其攻击目标是明确的，攻击目的往往不那么单一，危害性也非常严重。例如，在普通的网络攻击事件中，攻击者可能仅仅是利用目标网络的 Web 服务器漏洞，入侵网站更改网页或在网页上挂马。也就是说，这种攻击是随机的，而其目的也是单一而简单的。

在渗透入侵攻击过程中，攻击者会有针对性地对某个目标网络进行攻击，以获取其内部的商业资料，进行网络破坏等。其实施攻击的步骤是非常系统的，假设其获取了目标网络中网站服务器的权限，则不会仅满足于控制此台服务器，而是会利用此台服务器继续入侵目标网络，获取整个网络中所有主机的权限。

另外，为了实现渗透攻击，攻击者往往综合运用远程溢出、木马攻击、密码破解、嗅探、ARP 欺骗等多种攻击方式，逐步控制网络。总之，网络渗透攻击与普通网络攻击相比，网络渗透攻击具有攻击目的明确性、攻击步骤逐步与渐进性、攻击手段的多样性和综合性等特点。

目前，网络渗透测试已经成为安全工作者的一个课题，其发展前景不可估量。作为一名网络管理员或安全工作者，如果有能力实施基本渗透测试的话，那么其价值将是极大的，一切日常安全维护操作将更加有针对性，也更加有效。

如果安全管理员学习了网络渗透测试的相关知识，就可以完全模拟攻击者可能使用的漏洞检测与攻击技术，对目标网络系统的安全进行深入的检测，探寻出网络系统中最脆弱的安全环节，从而让管理人员能够直观地知道其网络所面临的问题。

1.2　渗透测试需要掌握的知识

网络渗透测试所涉及的内容很多，覆盖的范围也广，对于一个新手来说，了解和掌握一些有关操作系统知识就显得尤为重要。如在操作系统中经常遇到的进程、端口、服务、文件系统、常用的 DOS 命令以及注册表等常见术语。

1.2.1　进程、端口、服务

进程、端口和服务是计算机操作系统中不可缺少的部分，一个进程对应着一个程序，服务和端口常常被联系在一起，一个端口对应着一个服务，如 Web 服务默认对应 80 端口等。

1.　进程

进程是程序在计算机上的一次执行活动。当运行一个程序，就启动了一个进程。显然，程序是静态的，进程是动态的。进程可以分为系统进程和用户进程两种。凡是用于完成操作系统的各种功能的进程就是系统进程；凡由用户启动的进程就是用户进程。

在 Windows 系统自带任务管理器中可以查看当前正在运行的进程，具体操作步骤如下。

步骤 01 在 Windows 系统中按“Ctrl+Alt+Delete”组合键，即可打开“任务管理器”窗口，切换到“进程”选项卡，即可看到本机中开启的所有进程，如图 1-1 所示。

步骤 02 如果想要更详细地查看进程的内容，则可以设置进程显示的项目。在“任务管理器”窗口中选择“查看”→“选择列”菜单项，即可打开“选择列”对话框，在其中勾选相应的复选框，最后单击“确定”按钮即可，如图 1-2 所示。

步骤 03 在“进程”选项卡中选中某一进程并单击鼠标右键，从弹出的快捷菜单中还可以对进程进行其他操作，如：结束进程、结束进程树、设置优先级等，如图 1-3 所示。

图 1-1　查看本机中开启的进程

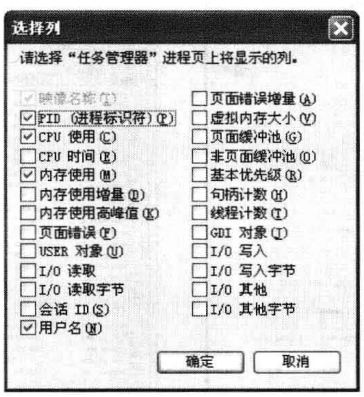


图 1-2　“选择列”对话框

图 1-3　对进程进行其他操作

除使用系统自带的任务管理器来管理进程外，还可以使用其他工具对进程进行管理。Windows 进程管理器就是一款功能比较强大的进程管理工具。利用该工具可对进程查询（描述/模块）、管理（结束/暂停/恢复/删除……）、端口访问查询、系统性能/信息查询等，进程信

息库也在不断地更新。使用 Windows 进程管理器管理进程的具体操作步骤如下。

步骤 01 下载并解压缩“Windows 进程管理器”压缩包，双击其中的可执行文件，即可打开其主界面，如图 1-4 所示。

步骤 02 在“进程管理”选项卡下即可查看本机正在运行的进程列表，包括系统进程和用户进程等，选中某一进程后（如 smss.exe），单击“查看属性”按钮，即可打开“smss.exe 属性”对话框，在其中可以查看该进程的文件类型、位置、大小等信息，如图 1-5 所示。

图 1-4 “Windows 进程管理器”主窗口

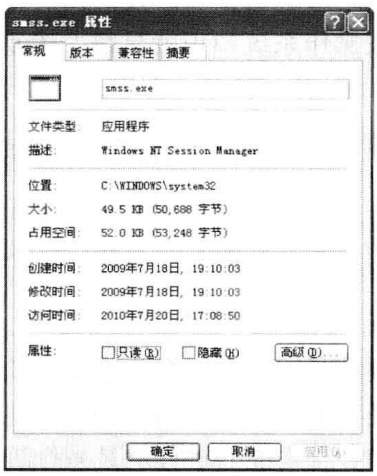


图 1-5 “smss.exe 属性”对话框

步骤 03 在查看进程时，如果不知道某一进程所对应程序的位置，则可以利用 Windows 进程管理器查找，在“Windows 进程管理器”操作窗口中选择某一进程（如 smss.exe）后，单击“定位文件”按钮，打开该进程所对应程序的位置，如图 1-6 所示。

步骤 04 如果想要结束某一进程，则可以在选中某一进程后，在“Windows 进程管理器”操作窗口的工具栏上单击“结束进程”按钮，弹出一个信息提示框。单击“是”按钮，即可结束该进程，如图 1-7 所示。

图 1-6 定位文件的位置

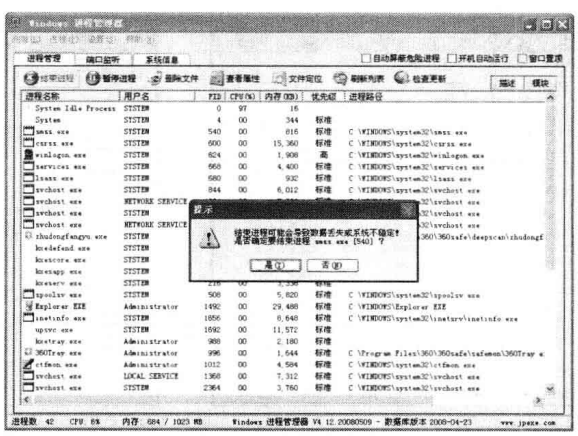


图 1-7 结束进程

步骤 05 如果想要删除某一进程的文件，则可以在选中某一进程后，在“Windows 进程管理器”操作窗口的工具栏上单击“删除文件”按钮，弹出一个信息提示框。单击“是”按钮，即可删除该进程所对应的文件，如图 1-8 所示。

步骤 06 如果想要暂停运行某一进程的文件，则可以在选中某一进程后，在“Windows 进程管理器”操作窗口的工具栏上单击“暂停进程”按钮，弹出一个信息提示框，单击“是”按钮，即可暂停运行该进程，如图 1-9 所示。

图 1-8　删除文件

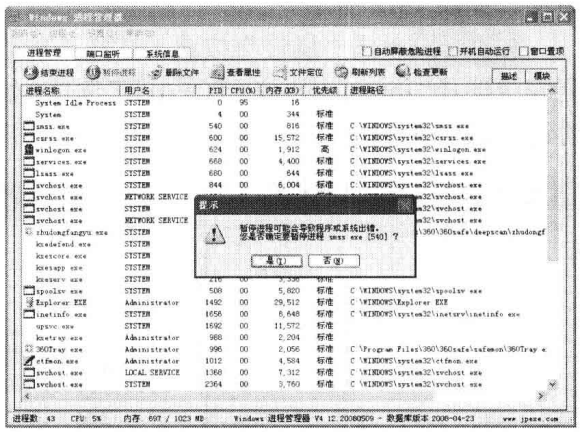


图 1-9　暂停进程

步骤 07 利用 Windows 进程管理器除可以管理进程外，还可以查看本机系统中的端口监听和系统信息，在其中选择“端口监听”选项卡，即可查看端口监听信息列表，如图 1-10 所示。如果选择“系统信息”选项卡，即可在其中查看本机系统信息，包括系统名、版本号等，如图 1-11 所示。

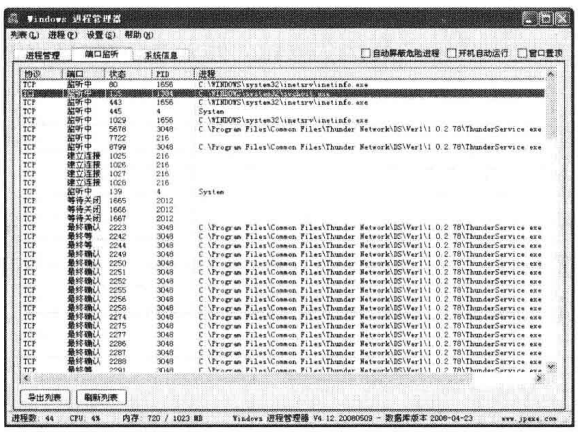


图 1-10　“端口监听”选项卡

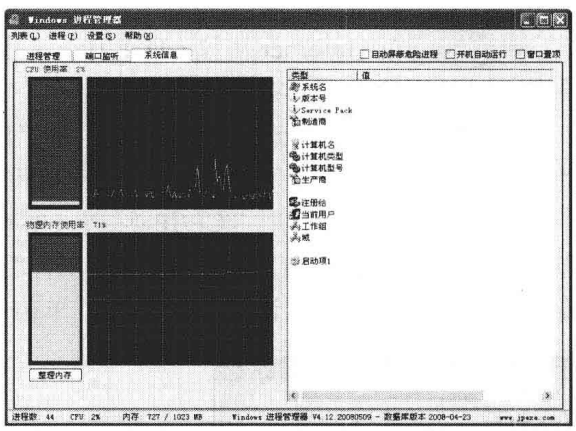


图 1-11　“系统信息”选项卡

2. 端口

计算机中的“端口”可以认为是计算机与外界通讯交流的出口。端口可分为硬件端口、软件端口和协议端口。其中硬件端口又称接口，如：USB 端口、串行端口等；软件端口一般指网络中面向连接服务和无连接服务的通信协议端口，包括一些数据结构和 I/O（基本输入输出）缓冲区等；计算机中的协议端口范围为 0～65535，如浏览网页服务的 80 端口、用于 FTP 服务的 21 端口等。

另外，用户还可以自行对计算机中的端口进行限制，例如关闭不需要的端口。在 Windows 2000 以上版本的操作系统之中，不需要安装任何其他软件，利用系统自带的“TCP/IP 筛选”

功能，就可以实现服务器端口的限制。具体设置的操作步骤如下。

步骤 01 在操作系统界面中右击 “网上邻居”图标，从弹出的快捷菜单中选择“属性”选项，即可打开“网络连接”窗口。双击“本地连接”图标，即可打开“本地连接 状态”对话框，如图 1-12 所示。

步骤 02 单击“属性”按钮，打开“本地连接 属性”对话框，在“此连接使用下列项目”列表中选择“Internet 协议（TCP/IP）”选项，如图 1-13 所示。再单击“属性”按钮，打开“Internet 协议（TCP/IP）属性”对话框，如图 1-14 所示。

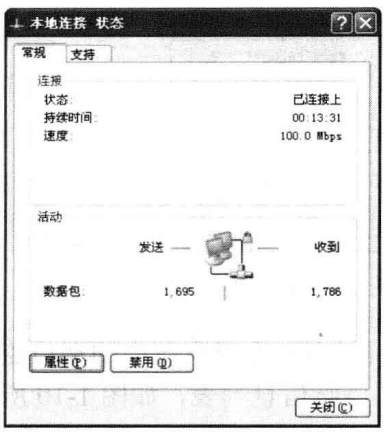


图 1-12 “本地连接 状态”对话框

图 1-13 “本地连接属性”对话框

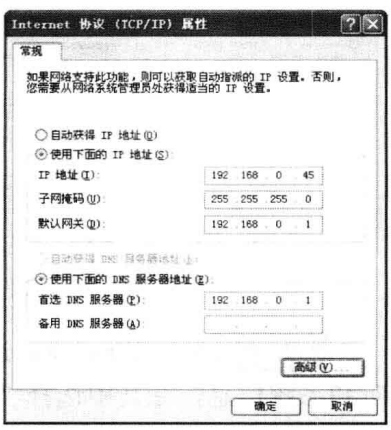


图 1-14 “Internet 协议属性”对话框

步骤 03 在“Internet 协议（TCP/IP）属性”对话框中单击“高级”按钮，打开“高级 TCP/IP 设置”对话框，如图 1-15 所示。

步骤 04 切换到“选项”选项卡，在“IP 地址”列表中选择“TCP/IP 筛选”选项，单击“属性”按钮，打开“TCP/IP 筛选”对话框，如图 1-16 所示。

步骤 05 勾选“启用 TCP/IP 筛选（所有适配器）”复选框，并选择左边的“只允许”单选按钮后，单击“添加”按钮，即可打开“添加筛选器”对话框，如图 1-17 所示。在“TCP 端口”文本框中输入允许开启的端口，单击“确定”按钮，即可将只允许添加的端口开启。

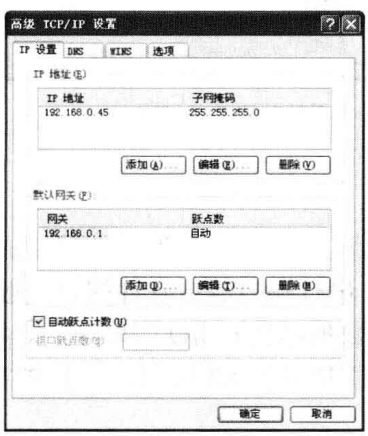


图 1-15 “高级 TCP/IP 设置”对话框

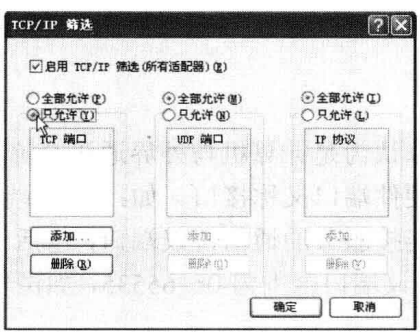


图 1-16 “高级 TCP/IP 设置”对话框

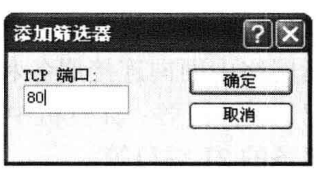


图 1-17 “添加筛选器”对话框