高等学校计算机科学与技术教材

计算机网络安全教程
实验指导

COMPUTER Science and Technology

□ 石志国 薛为民 尹 浩 编著

- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精练，实例丰富
- 可操作性强，实用性突出

清华大学出版社 ● 北京交通大学出版社

高等学校计算机科学与技术教材

计算机网络安全教程
实 验 指 导

石志国　薛为民　尹浩　编著

清 华 大 学 出 版 社
北京交通大学出版社
·北京·

内 容 简 介

本书是《计算机网络安全教程》第2版的配套实验指导书，亦可独立使用。本实验指导书循序渐进地设计了9个实验，这些实验来源与教材，但高于教材，注重对知识的掌握、技能的培养、兴趣的激发。

其中实验1、实验2和实验3分别面向网络安全环境配置实验、网络数据报分析实验和SDK编程实验，基本覆盖网络安全基础部分的实验内容；实验4、实验5、实验6和实验7分别面向程序内存驻留与木马原型实验、端口扫描原理与实现实验、网络攻击与网络后门实验、病毒感染机制与数据恢复实验，基本覆盖网络安全攻击部分的实验内容；实验8、实验9面向加密与解密实验、防火墙与入侵检测实验，基本覆盖网络安全防御部分的实验内容。

本书可以作为大专院校及各类培训机构相关课程的指导教材，提供全部源代码、涉及所有软件等教学支持信息，可以从图书支持网站 http://www.gettop.net 下载，也可以从出版社网站 http://press.bjtu.edu.cn 的下载栏目中下载。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989　13501256678　13801310933

图书在版编目（CIP）数据

计算机网络安全教程实验指导 / 石志国，薛为民，尹浩编著. —北京：清华大学出版社；北京交通大学出版社，2011.10

（高等学校计算机科学与技术教材）

ISBN 978-7-5121-0747-2

Ⅰ. ①计… Ⅱ. ①石… ②薛… ③尹… Ⅲ. ①计算机网络-安全技术-高等学校-教学参考资料 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2011）第183452号

责任编辑：谭文芳

出版发行：清 华 大 学 出 版 社　邮编：100084　电话：010-62776969　http://www.tup.com.cn

北京交通大学出版社　邮编：100044　电话：010-51686414　http://press.bjtu.edu.cn

印 刷 者：北京瑞达方舟印务有限公司

经　　销：全国新华书店

开　　本：185×260　印张：7.5　字数：189千字

版　　次：2011年10月第1版　2011年10月第1次印刷

书　　号：ISBN 978-7-5121-0747-2/TP・664

印　　数：1～5 000册　定价：15.00元

本书如有质量问题，请向北京交通大学出版社质监组反映。对您的意见和批评，我们表示欢迎和感谢。

投诉电话：010-51686043，51686008；传真：010-62225406；E-mail：press@bjtu.edu.cn。

前　言

计算机网络安全是一门实践性极强的课程，同时也是一门非常典型的多学科交叉的课程，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论和信息论等多种学科。

《计算机网络安全教程》第1版于2004年2月出版，并于2007年4月修订，第2版于2011年2月出版。其中，第1版于2007年获得全国大学出版社优秀畅销书二等奖；修订版于2010年获得中国大学出版社优秀教材奖一等奖。第2版于2009年获得北京市精品教材立项，多年来收取了大量读者的表扬、批评和改进意见，第1版和修订版都没有配实验指导书，这次采纳不少教师的意见，配置实验指导书，同时配合第2版教材使用。

本书涉及的实验和教材内容的顺序一致，基本覆盖了网络安全基础、网络安全攻防的实验需求，尽量囊括了安全理论、安全工具与安全编程的实验需求。

导读

本实验指导书共包含9个实验，每个实验由“实验目的”、“实验内容”、“实验步骤”和“补充内容”4部分组成。

“实验目的”部分主要说明要学习的知识和锻炼的技能；“实验内容”部分主要说明具体实验的组成，所使用的工具软件和编制的代码等；“实验步骤”部分主要说明要达到实验目的和完成实验内容，所需要采用的实验过程，通常每个实验都有4～6个实验步骤组成，每个实验步骤相对独立，同时又有一定的内在关系；“补充内容”部分包括两方面的内容：（1）任课老师根据学生的特点和自身授课的特色加入补充的实验内容；（2）通过给定的关键字在Google和Baidu等搜索引擎网站进行检索，并学习检索到的内容，这样可以学到最新的相关知识。

实验1、实验2和实验3分别面向网络安全环境配置实验、网络数据报分析实验和SDK编程实验，基本覆盖网络安全基础部分的实验要求。

- 实验1介绍VMware虚拟机的安装与配置，以及抓包软件Sniffer Pro的使用等。
- 实验2 对抓取的网络数据报进行分析，以及介绍常用的网络命令等。
- 实验3介绍编程环境，以及编写简单的文件管理程序、对编程实现对系统用户登录信息的修改等。

实验4、实验5、实验6和实验7分别面向程序内存驻留与木马原型实验、端口扫描原理与实现实验、网络攻击与网络后门实验、病毒感染机制与数据恢复实验，基本覆盖网络安全攻击部分的实验要求。

- 实验4 以“冰河”原型木马为实例，编程实现内存驻留方法等。
- 实验5介绍端口扫描原理，以及系统用户扫描、开放端口扫描、共享目录扫描，以及漏洞扫描等的实现工具与相关操作等。
- 实验6介绍几种常见网络攻击的实现工具及过程，包括暴力破解操作系统密码、暴力破解邮箱密码、暴力破解软件密码，以及使用代理跳板入侵其他主机等。
- 实验7介绍并编程实现PE病毒、VBS病毒、U盘病毒的感染机制，和丢失数据的恢复方法。

实验8、实验9面向加密与解密实验、防火墙与入侵检测实验，基本覆盖网络安全防御

部分的实验要求。

- 实验 8 程序实现凯撒密码，同时编程实现 DES、RSA 的加解密。
- 实验 9 介绍包过滤防火墙规则，以及使用规则控制 FTP 和 HTTP 访问，编程实现对程序关联端口的检测。

读者在理解、掌握每个实验内容的基础上能够尝试着“举一反三”，从而更好地掌握所学内容，拓展知识面。实验指导书对教材所讲的理论知识进行补充与扩展，其目的是希望用一些比较经典的编程案例来引导读者对理论知识的学习，加深对相关理论知识的理解与掌握。

由于本实验指导书的内容是与日常网络操作密切相关的，所以它在一定程度上具有可操作性与实用性，希望通过学习与实践，掌握基本的网络攻防方法，并能灵活应用。

致谢

从 2004 年第一版出版 7 年来，首先要感谢很多老师和同学提出的批评和改进意见，很多意见非常贴切和真诚，我们今后也会尽全力通过网页和电子邮件等方式为读者提供更为周到的服务。

还要感谢很多在网上提出修改意见的读者，他们在提出意见的同时，还勇敢地在网上留下自己的真实联系方式。这些读者有：武汉科技大学中南分校信息工程学院计算机网络系的赵义老师，山东力明科技职业学院理工学院的仝瑞钦老师，北京市房山区理工大学房山分校的张志军老师，福建工业学校的邱云芳老师，西安科技大学通信学院刘涛老师，湖南科技学院计算机与通信工程系徐钢峰老师，青岛远洋船员学院乔显亮老师，电子科技大学成都学院文炜老师，成都市高新西区团结学院路杨道静老师，四川省成都市芳草街的余伟老师，等等，这里不再一一列举。还有很多老师通过电子邮件反馈了修改意见，例如，李学宝等老师通过电子邮件提出了非常详细的修改意见。这里对他们表示最深切的感谢！

在本书的编写过程中，还得到了众多老师的指导和帮助。这里要感谢中科院软件所卿斯汉研究员、贺也平研究员、梁洪亮博士、商青华博士、周启明博士、张宏博士和金洁华工程师；感谢清华大学计算机系林闯教授、尹浩副教授；感谢北京科技大学王志良教授、徐正光教授、张晓彤教授和解仑教授；感谢中央广播电视大学崔林教授、徐孝凯教授、田萧老师和王春凤老师；感谢中国软件行业协会邱钦伦高级工程师。感谢他们为本书提供了大量详尽的编程资料，并为本书解决了很多编程方面的问题。

此外，课题组的两个同学孙勇峰、张巧对每个实验都进行了细致的测试和整理，保证每个实验步骤都可以顺利完成，这里对他们的辛勤劳动表示感谢。

最后要感谢的是北京交通大学出版社的编辑谭文芳老师，7 年多来她稳定的支持是教材能及时更新的关键，也是本实验指导书能够顺利出版的关键。

支持

本书可以作为高等院校和各类培训机构相关课程的教材或者教学参考书，也可作为网络安全自学人员和网络安全开发人员的参考书。本书提供完整的配套软件、源代码和相关学习资源，将在 http://www.gettop.net 或者 http://press.bjtu.edu.cn 下载栏目中发布。

由于作者水平和时间有限，难免出现错误。对于本书的任何问题请使用 E-mail 发送到作者邮箱：shizhiguo@tom.com。

石志国

2011 年 5 月

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

实验 1　环境配置 ……1
实验 2　网络数据报分析 …… 24
实验 3　SDK 编程基础 …… 38
实验 4　程序内存驻留与木马原型 …… 51
实验 5　端口扫描原理与实现 …… 59
实验 6　网络攻击与网络后门 …… 73
实验 7　病毒感染机制与数据恢复 …… 86
实验 8　加密与解密原理与实现 …… 98
实验 9　防火墙与入侵检测的实现 ……103
附录 A　实验报告格式 ……112

实验1　环境配置

实验目的

1．使用 VMware 虚拟机配置网络实验环境；

2．配置虚拟机操作系统的 IP，使之与主机能够通过网络进行通信；

3．安装 Sniffer Pro 抓包软件，学会使用 Sniffer Pro 抓取数据包。

实验内容

1．安装 VMware 虚拟机，版本号为 VMware-workstation-full-7.0.0-203739 或者选择最新的版本。

2．利用一个在虚拟机上装好的操作系统 Windows 2000 Advanced Server SP0（该操作系统没有打任何补丁，非常适合作为攻击的对象），并在 VMware Workstation7.0 中建立并配置 Windows 2000 Advanced Server 系统。

3．配置虚拟机操作系统 IP，使用 Ping 指令测试其能否与主机的进行网络通信。

4．安装 Sniffer Pro 4.7.530，并抓取虚拟机与主机进行网络通信时的数据包。

实验步骤

步骤 1　安装 VMware 虚拟机

安装 VMware 虚拟机，这里选择的版本为 VMware-workstation-full-7.0.0-203739，双击安装文件，进入程序安装前装载画面。装载结束后，程序进入欢迎界面，用户开始进行程序的安装。在接下来的几步均按照系统的默认选项进行设置，有些简单选项如程序安装路径等，可按用户的喜好与实际情况进行设置。安装过程如图 1-1 至图 1-6 所示。

安装程序会提示输入用户名和 VM 的注册号，输入正确以后，显示安装完毕界面，如图 1-7 至图 1-9 所示。

安装完毕后，系统提示是否重新启动计算机，这里需要重新启动才能使用 VMware。重启计算机以后，打开 VMware 程序，选择同意许可协议，如图 1-10 所示。之后进入主界面，界面如图 1-11 所示。

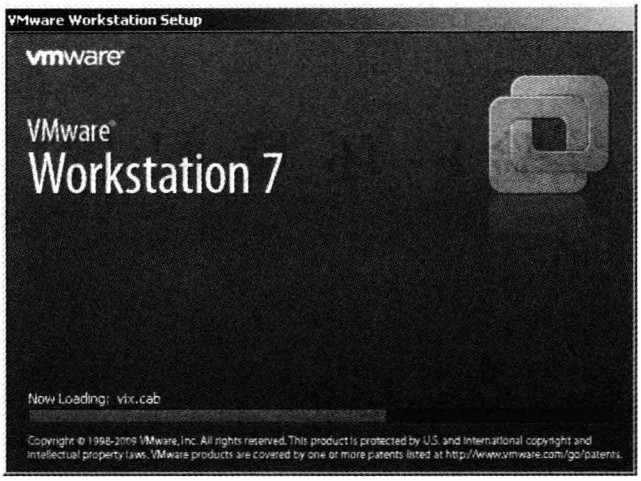

图 1-1 安装程序装载界面

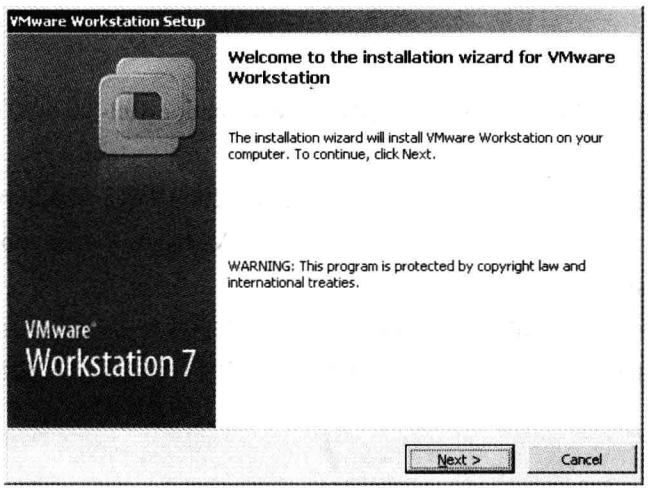

图 1-2 程序欢迎界面

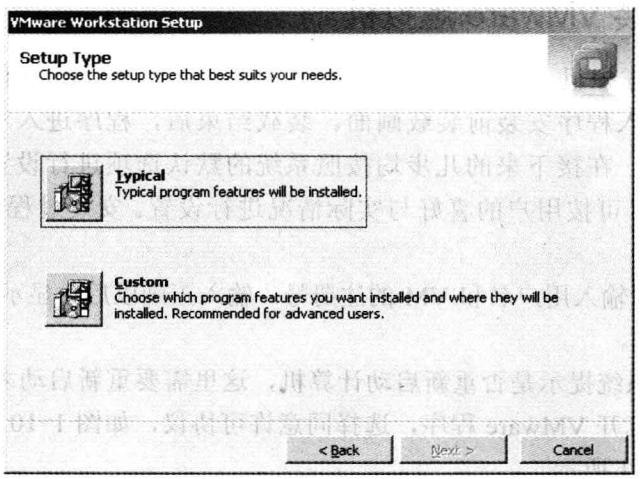

图 1-3 安装类型选择界面

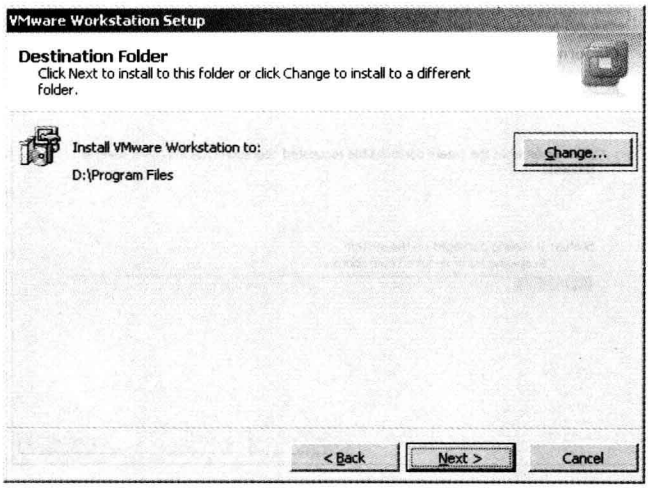

图 1-4　安装路径选择界面

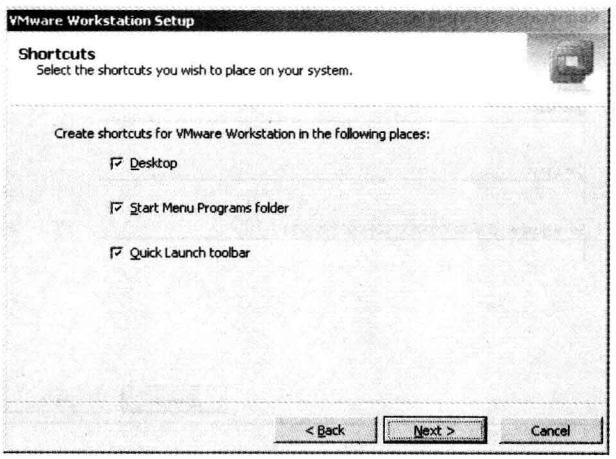

图 1-5　快捷方式选界面

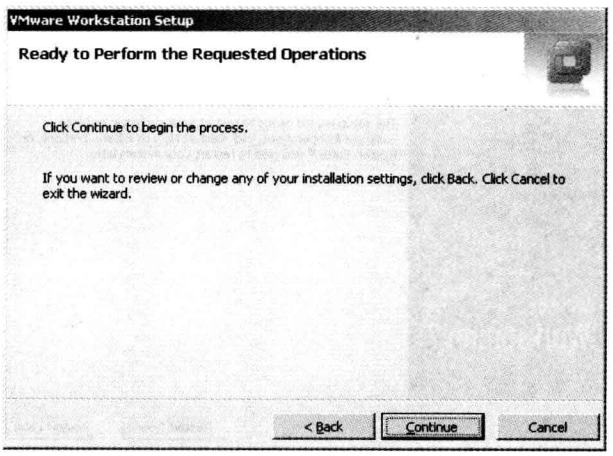

图 1-6　等待安装界面

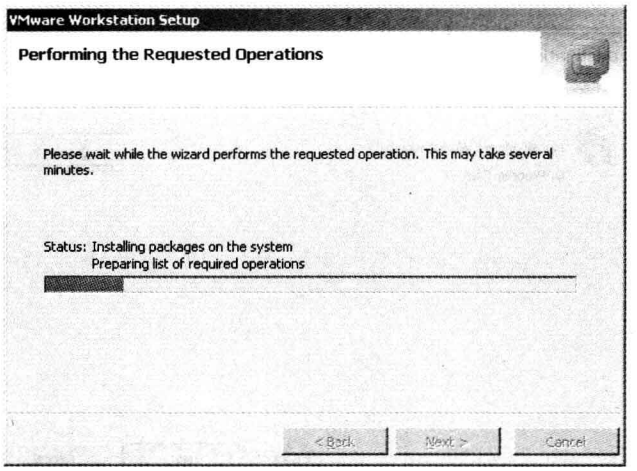

图 1-7 程序正在安装界面

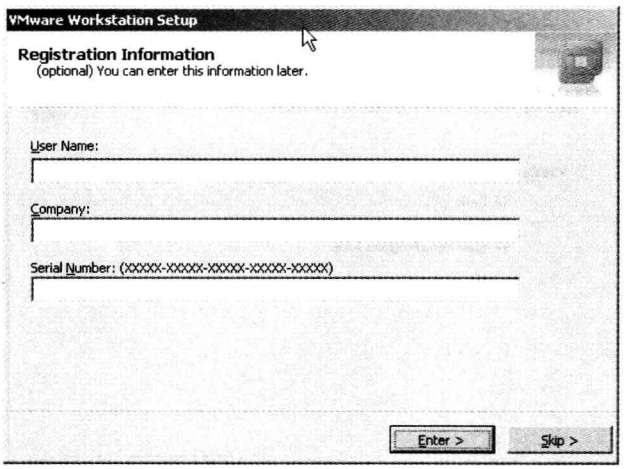

图 1-8 用户名、注册码输入提示界面

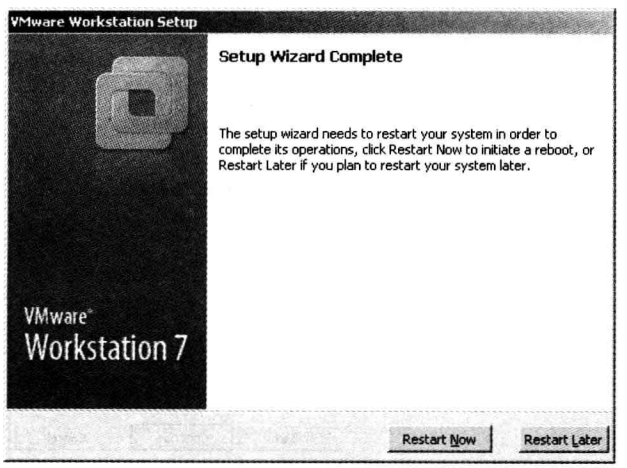

图 1-9 安装结束界面

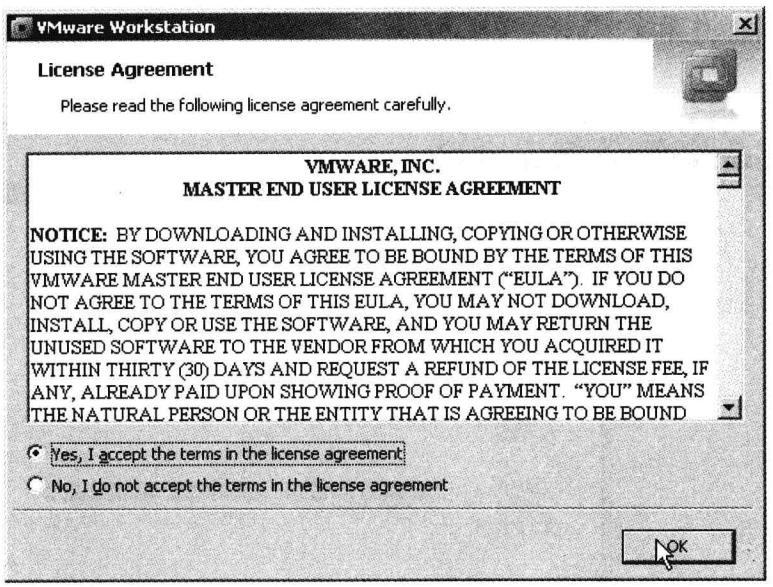

图 1-10　许可协议界面

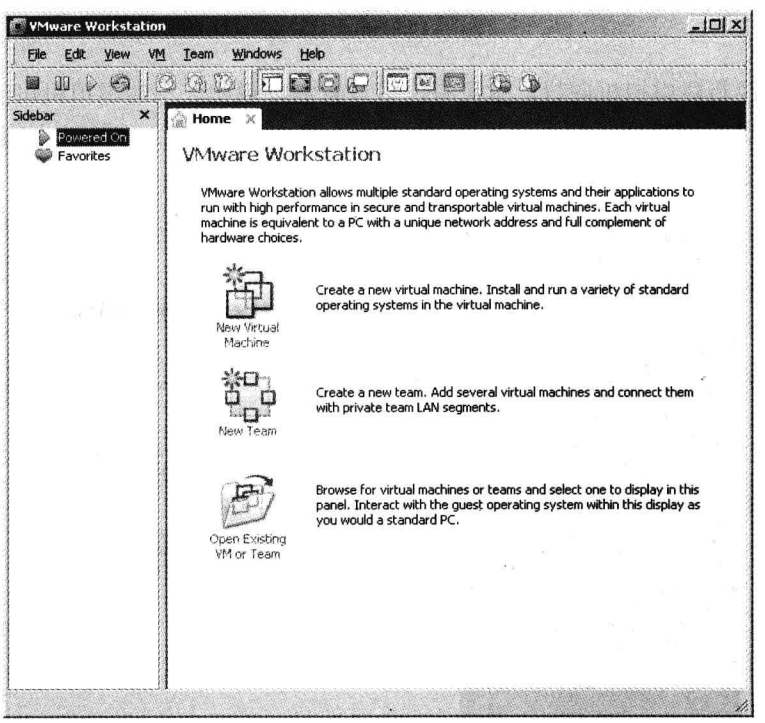

图 1-11　VMware workstation 主界面

步骤 2　配置虚拟机操作系统

安装完虚拟机以后，就如同组装了一台计算机，这台计算机需要安装操作系统。这里需

此为试读，需要完整PDF请访问：www.ertongbook.com

要在虚拟机中装操作系统，选择菜单栏“File”→“New”→“Virtual Machine”选项，如图1-12所示。

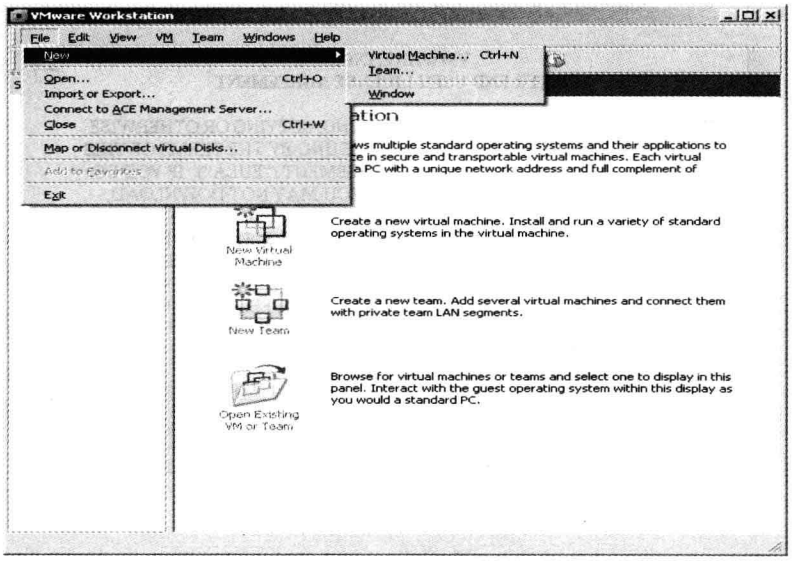

图1-12 新建虚拟机

这时，出现新建虚拟机向导，这里有许多设置需要说明，不然虚拟机可能无法与外面系统进行通信。单击新建虚拟机，出现安装选项界面，如图1-13所示。这里选择“Custom（advanced）”安装方式。

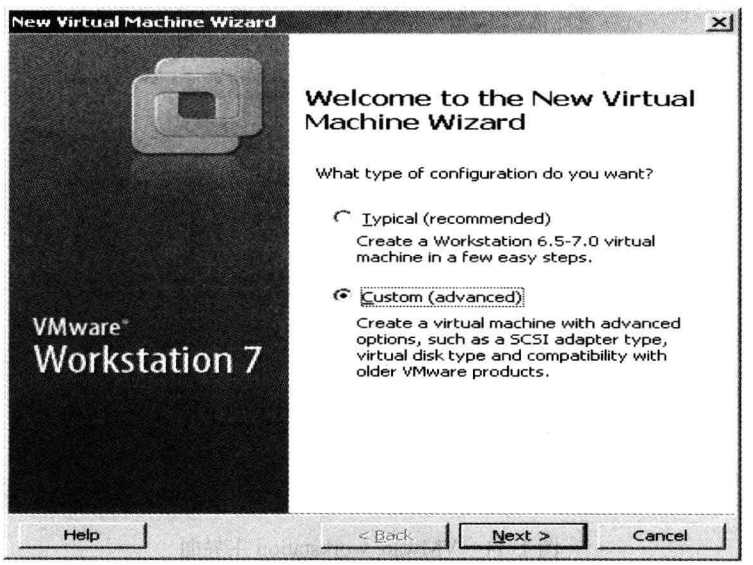

图1-13 安装选项界面

单击“Next”按钮，进入兼容性选择界面。在“Hardware compatibility”（硬盘兼容性）选项中选择Workstation 4，如图1-14所示。

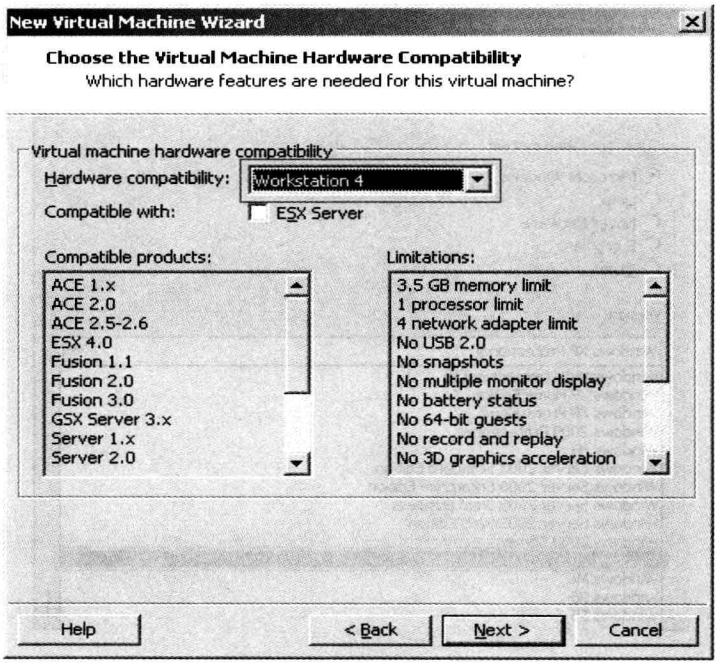

图 1-14　硬盘兼容性选择

单击“Next”按钮进入系统安装选项，在此选择“I will install the operating system later”，如图 1-15 所示。单击“Next”按钮进入选择操作系统界面，设置要安装的操作系统类型，如图 1-16 所示。

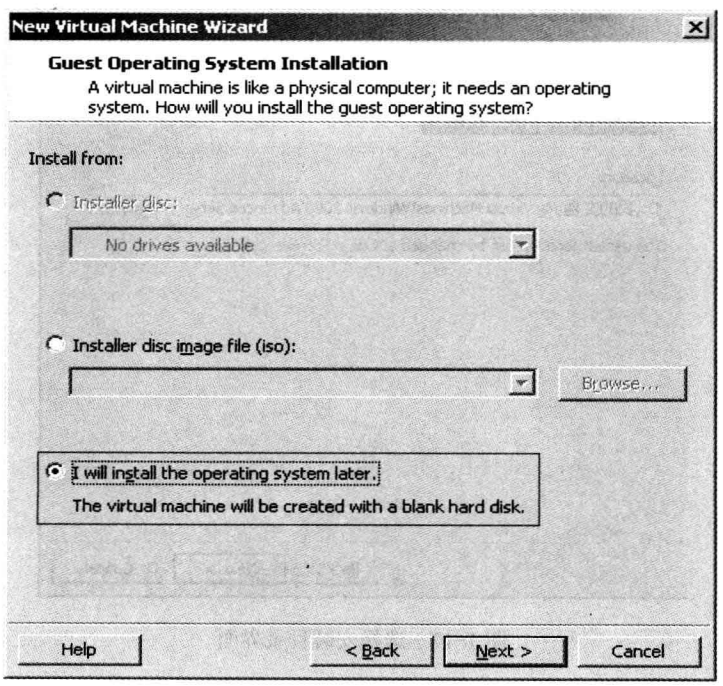

图 1-15　系统安装选项

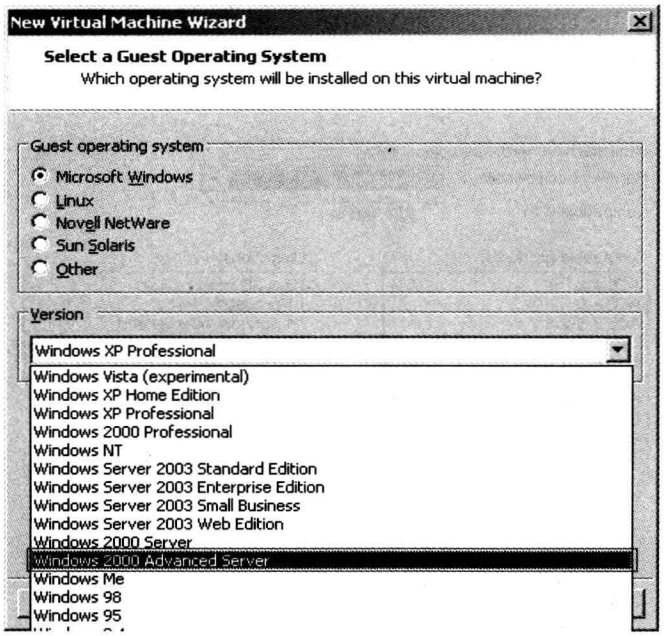

图 1-16 选择安装的操作系统

从图 1-16 中可以看出，几乎常见的操作系统在列表中都有。这里选择“Windows 2000 Advanced Server”，单击“Next”按钮进入安装目录选择界面，如图 1-17 所示。

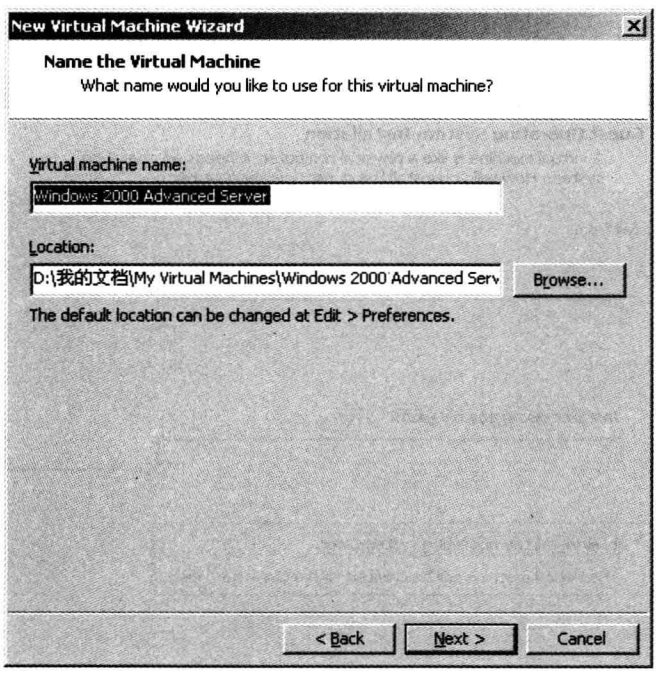

图 1-17 选择安装目录界面

安装目录界面有两个文本框，“Virtual machine name”文本框用于输入系统的名字，选择

默认值就可以，“Location”文本框用于选择虚拟操作系统安装地址。选择好地址以后，单击“Next”按钮，出现虚拟机内存大小的界面，如图 1-18 所示。

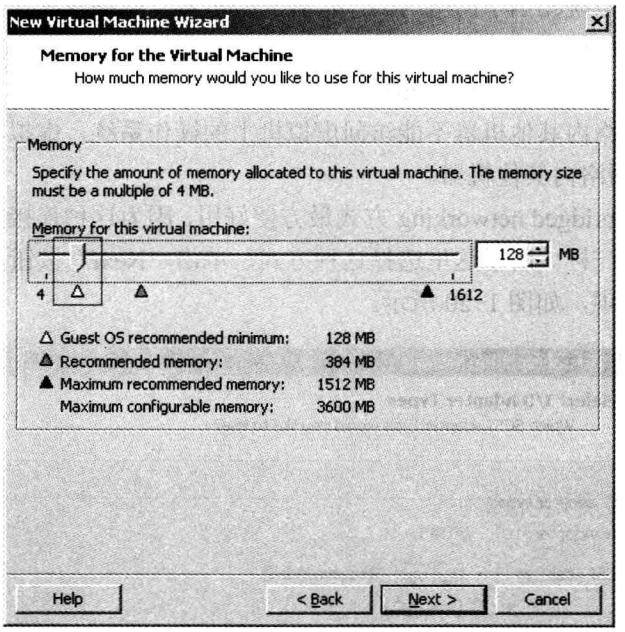

图 1-18　设置虚拟机内存大小

因为安装的操作系统是 Windows 2000 Advanced Server，所以内存不能小于 128 MB，如果计算机内存比较大的话可以多分配一些，但是不能超过真实内存大小，这里设置为 128 MB，单击“Next”按钮进入网络连接方式选择界面，如图 1-19 所示。

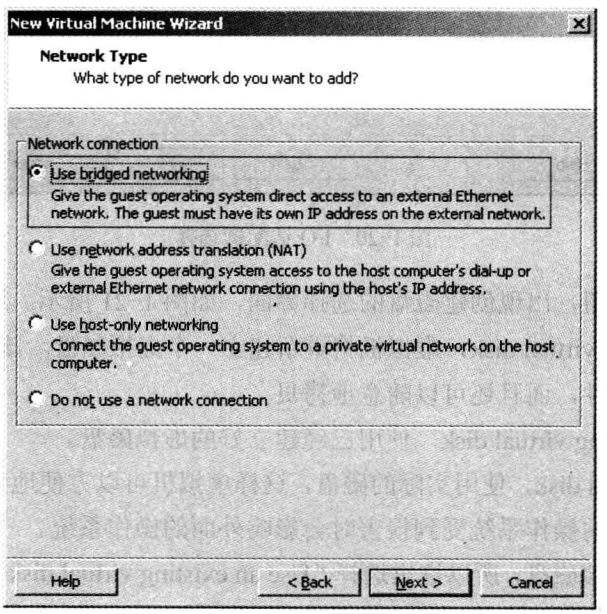

图 1-19　网络连接方式选择界面

VMWare 有两种常用联网方式。

（1）Used bridged networking：虚拟机操作系统的 IP 地址可设置成与主机操作系统在同一网段，虚拟机操作系统相当于网络内的一台独立的机器，网络内其他机器可访问虚拟机上的操作系统，虚拟机的操作系统也可访问网络内其他机器。

（2）User network address translation（NAT）：实现主机的操作系统与虚拟机上的操作系统的双向访问。但网络内其他机器不能访问虚拟机上的操作系统，虚拟机可通过主机操作系统的 NAT 协议访问网络内其他机器。

一般来说，Used bridged networking 方式最方便好用，因为这种连接方式将使虚拟机就像是一台独立的计算机一样。所以这里选择这种方式，单击“Next”按钮，出现 I/O 适配器选择界面，使用默认选项，如图 1-20 所示。

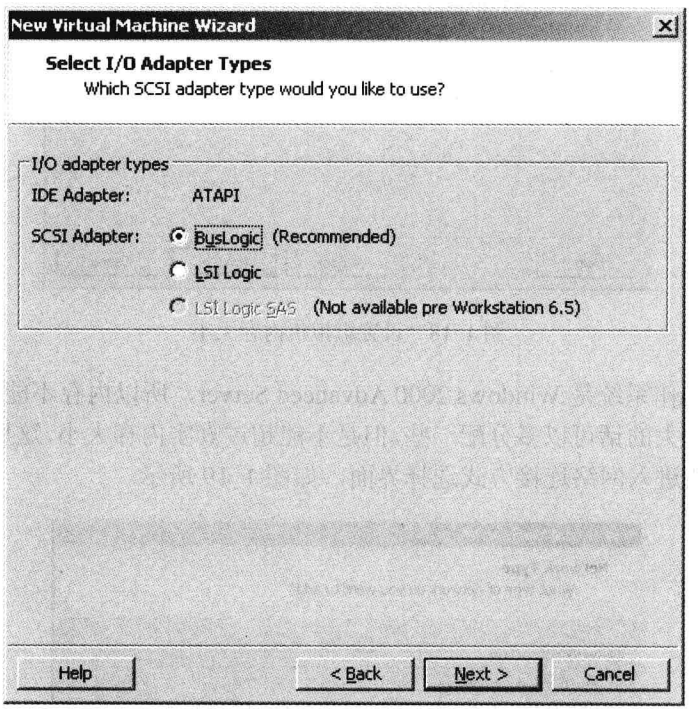

图 1-20 I/O 适配器选择

单击“Next”按钮，出现创建磁盘的选择界面，如图 1-21 所示。这里有三种选择：

（1）Create a new virtual disk，虚拟机将重新建立一个虚拟磁盘，该磁盘在实际计算机操作系统上就是一个文件，而且还可以随意地拷贝。

（2）Use an existing virtual disk，使用已经建立好的虚拟磁盘。

（3）Use a physical disk，使用实际的磁盘，这样虚拟机可以方便地与主机进行文件交换，但是，这样虚拟机上的操作系统受到损害时会影响外面的操作系统。

因为使用已有虚拟磁盘，所以这里选择“Use an existing virtual disk”，单击“Next”按钮，进入已经建立好的操作系统文件，界面如图 1-22 所示。

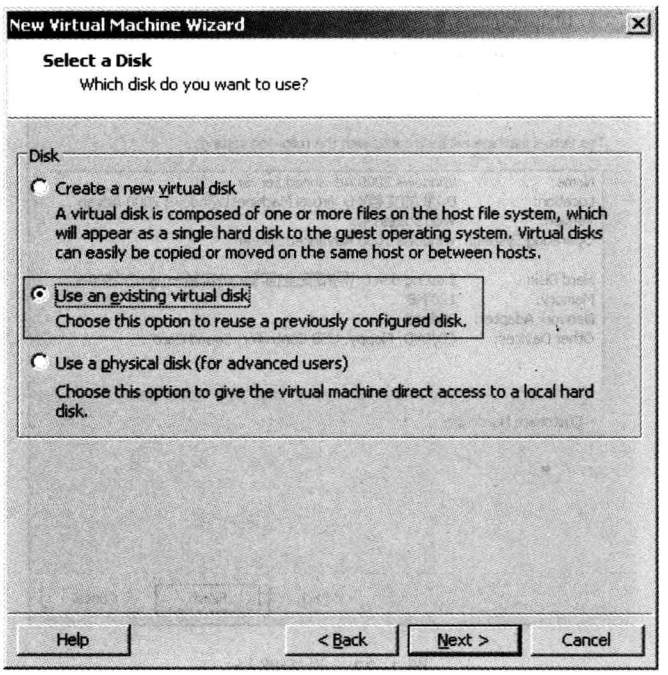

图 1-21　选择安装的磁盘

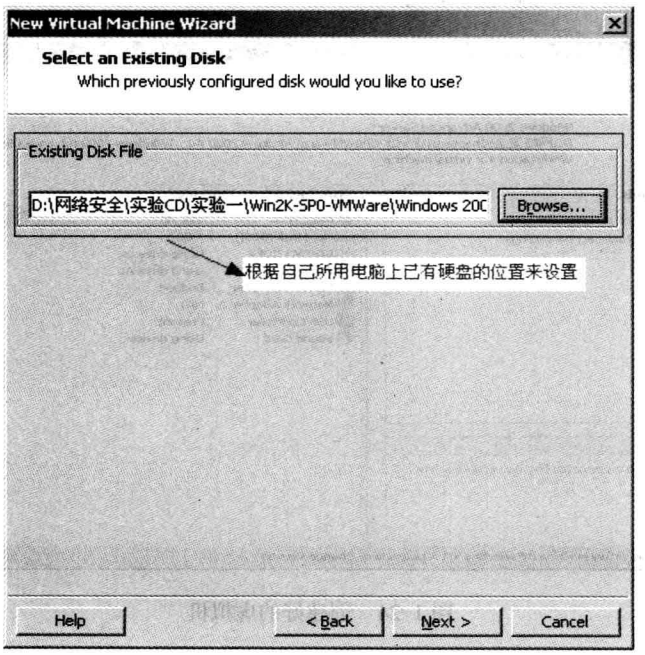

图 1-22　已有硬盘选择

单击“Browse”按钮选择已有硬盘，单击“Next”按钮进入完成创建虚拟机界面，如图 1-23 所示。单击“Finish”按钮，可以在 VMware 的主界面看到刚才配置的虚拟机，如图 1-24 所示。

此为试读，需要完整PDF请访问：www.ertongbook.com