高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

网络安全协议综合实验教程

杨浩淼 李洪伟 冉鹏 编著

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

高等院校信息安全专业系列教材

教育部高等学校信息安类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络安全协议综合实验教程

杨浩淼 李洪伟 冉鹏 编著

Information Security

http://www.tup.com.cn

清华大学出版社
北京

内 容 简 介

本书作为信息安全方面的实验教材，介绍了信息安全方面一些最基本的实验内容。这些实验包括第1章 VMware虚拟网络的构建；第2章 IPSec基础实验；第3章 SSL基础实验；第4章缓冲区溢出攻击初级实验；第5章 Radius综合实验；第6章 IPSec综合实验；第7章 OpenSSL综合实验；第8章 VPN综合实验；第9章基于身份加密算法的综合实验以及第10章信息探测综合实验。在利用本书做实验的时候，不需要购买防火墙、入侵检测、VPN等硬件设备。

本书适合作为高等学校信息安全及相关专业本科学生作为信息安全相关课程的实验教材，也适合作为企事业单位、公司员工进行信息安全方面的教育培训和技术研讨用书。

图书在版编目(CIP)数据

网络安全协议综合实验教程/杨浩淼，李洪伟，冉鹏编著. —北京：清华大学出版社，2016
高等院校信息安全专业系列教材
ISBN 978-7-302-42496-3

Ⅰ. ①网… Ⅱ. ①杨… ②李… ③冉… Ⅲ. ①计算机网络－安全技术－通信协议－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2015)第316466号

责任编辑：张　民　李　晔
封面设计：常雪影
责任校对：梁　毅
责任印制：沈　露
出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：7.75　　**字　　数**：192千字
版　　次：2016年6月第1版　　**印　　次**：2016年6月第1次印刷
印　　数：1～2000
定　　价：19.50元

产品编号：037413-01

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广。能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套。除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专

家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断完善。

我们的E-mail地址：zhangm@tup.tsinghua.edu.cn；联系人：张民。

“高等院校信息安全专业系列教材”编审委员会

前言

信息安全学科可分为狭义安全与广义安全两个层次，狭义的安全是建立在以密码论为基础的计算机安全领域，早期中国信息安全专业通常以此为基准，辅以计算机技术、通信网络技术与编程等方面的内容；广义的信息安全是一门综合性学科，从传统的计算机安全到信息安全，不但是名称的变更也是对内容的延伸，安全不再是单纯的技术问题，而是将管理、技术、法律等问题相结合的产物。

随着信息技术和计算机网络的普及，网络和信息安全对社会的生产，生活的影响越来越大。信息安全人才的培养和相关教材的编写也日益重要。本书从实践的角度出发，结合具体的实验来讲述信息安全的相关理论和技术。实验是对相关理论的运用和升华，作者希望借此给读者一个认识信息安全技术的新视角。本书的具体内容如下：

第 1 章介绍 VMware 虚拟网络的构建，这是进行实验的基础工作。一方面，进行 VMware 虚拟机的安装和虚拟网络的配置，这为后面的网络安全协议实验准备了虚拟网络实验环境；另一方面，对网络数据包的抓取软件 WireShark 进行了介绍，这是一个非常强大的网络协议分析工具。第 2 章介绍 IPSec 基础实验，通过本实验，将对 IPSec 的原理和协议运行机制有一定的了解；并熟悉 IPSec 数据包格式和协议流程。第 3 章介绍 SSL 的基础实验。第 4 章介绍缓冲区溢出攻击。在所有的漏洞中，缓冲区溢出漏洞占了远程网络攻击中的绝大多数。目前的缓冲区攻击方式有很多种，其中最常见的有栈溢出、堆溢出、整型溢出、格式化字符串溢出及文件流溢出等。本实验通过使用 Ollydbg 调试 OD 漏洞，理解缓冲区溢出攻击原理，了解栈溢出的攻击过程，从而在实际的写程序中尽量避免缓冲区溢出漏洞。第 5 章 Radius 基础实验的核心目的是，学会如何在 Windows Server 2003 的操作系统平台上进行安全配置以及服务器的搭建。而如何配置才能安全有效地实现 Radius 的远程客户端接入，是本实验最终的目的。第 6 章的 IPSec 综合实验是对 IPSec 相关内容的引申和提高。第 7 章主要进行 OpenSSL 综合实验，主要包括：编译 OpenSSL 源码包、使用 OpenSSL 创建 CA 实验以及 OpenSSL 的编程实验。第 8 章探讨如何开展 VPN 实验，这对提高学生计算机网络安全实践操作能力具有现实的指导意义。第 9 章介绍基于身份加密

算法的综合实验，本章在 MIRACL 大整数库的基础上，进行密码算法的实验。本章选用了比较新颖的基于身份公钥加密算法来进行实验。第 10 章介绍在攻击技术中，首要且不可或缺的一步是探测(Probe)。探测的主要目的便是对主机信息或者网络信息进行收集。本实验通过主机信息探测和安全漏洞探测两个方面来介绍两种著名的扫描工具，并以此了解其中的基本原理。

作　者

目录

第1章 VMware虚拟网络的构建

当前，虚拟机技术在计算机的各个领域得到了广泛应用。例如，在安全领域，可以利用虚拟机构建“蜜罐（HoneyPot）”系统，对互联网上的网络攻击行为进行分析研究；在存储领域，可以利用虚拟机来减少服务器的数量，简化服务器的管理，将多种应用整合到单台服务器上完成；在机房建设领域，可以利用虚拟机技术实现机房机器的多种用途，而无须担心主机系统与硬件的损坏。

虚拟机对真正的计算机而言是一个概念，是一个模拟真实计算机进行工作的软件系统。虚拟机拥有自己的CPU、指令系统、存储器组织、寄存器组、堆栈、输入输出等；可以接受指令系统的指令或用汇编语言及高级语言编写的程序，完成计算或数据处理工作。利用虚拟机技术生成的软件在功能上与使用的便利性上都与实际一致。

虚拟机在实验教学中的应用也越来越受到重视，本章基于VMware虚拟机在单机上构建了一个计算机网络实验平台。一方面，进行VMware虚拟机的安装和虚拟网络的配置，并为后面的网络安全协议实验准备了虚拟网络实验环境；另一方面，对网络数据包的抓取软件WireShark进行了介绍，这是一个非常强大的网络协议分析工具。

1.1 VMware虚拟网络

1.1.1 虚拟机的简介

1. 虚拟机技术总述

虚拟机的种类很多，其中一个分支专门仿真特定的硬件，有模拟一个芯片时序逻辑的、模拟CPU指令的、模拟整个硬件开发板的以及模拟一个PDA的模拟器等；另一个分支可以仿真一个真实的x86计算机，能够在一台真实计算机上虚拟出另外一台计算机，同时运行两个或更多的操作系统。这类虚拟机软件通常需要一个被称作“主操作系统”（host OS）的操作系统作为底层基本平台，虚拟的操作系统就运行在主系统之上，通常称为“客户操作系统”（guest OS）。由于虚拟得到的是一个完全真实的计算机，所以主、客户系统可以实现互访，或者通过网络方式互访。客户系统可以访问主系统的网络系统，甚至能够实现Internet连接共享。如VMWare、VirtualPC、twoOStwo、simics、VGS、Virtual Server、Cherry OS、SkyEye等都属此类。

2. 常用虚拟机软件比较

1) VMWare

VMware能够支持很多客户操作系统，能够模拟硬件包括主板、内存、硬盘(IDE和SCSI)、DVD/CD-ROM、软驱、网卡、声卡、串口、并口和USB口。但VM Ware没有模拟显卡。VMWare为每一种GuestOS提供一个叫做VMware-tools的软件包，来增强Guest OS的显示和鼠标，以及同步虚拟机和Host的时间等功能。

VMware提供了多种网络设置方式，例如Bridged方式、NAT方式和Host-only方式。其中桥接方式下Guest OS的IP可设置为与Host OS在同一网段，GuestOS相当于网络内的一台独立的机器，网络内的其他机器可访问Guest OS，Guest OS也可访问网络内的其他机器，当然与Host OS的双向访问也不成问题；在NAT方式下，也可以实现Host OS与Guest OS的双向访问。但网络内其他机器不能访问Guest OS，Guest OS可通过Host OS用NAT协议访问外界。

本书的虚拟网络环境是基于VMware的，因此对VMware虚拟网络，本书将在后面进一步介绍。

2) Virtual PC

Virtual PC最早由Connectix公司推出，后被微软公司收购。Virtual PC与VMWare的不同之处是：VMWare要通过VMware-tools才能实现高分辨率和真彩色，而Virtual PC模拟了S3 Trio 32/64(4MB显存)这款比较通用的显卡，通用性很强；Virtual PC的网络共享方式与VMWare不同，VMWare是通过模拟网卡实现网络共享的，而Virtual PC是通过在现有网卡上绑定Virtual PC emulated switch服务实现网络共享的。

3) SkyEye

SkyEye是一个指令级模拟器，可在通用的Linux和Windows平台上实现一个纯软件集成开发环境，模拟常见的嵌入式计算机系统；可运行多种嵌入式操作系统和各种系统软件，并可对它们进行源代码级的分析和测试，可模拟多种嵌入式开发板，支持多种CPU指令集。

不过，SkyEye的目标不是验证硬件逻辑，而是协助开发、调试和学习系统软件，所以SkyEye与真实的硬件环境相比有一定差别。SkyEye在时钟节拍的时序上不保证与硬件完全相同，对软件透明的一些硬件仿真进行了一定的简化，这样使SkyEye的执行效率更高。当然，SkyEye并不能取代硬件的功能。

3. VMWare Workstation 软件包

VMware Workstation是一款功能强大的桌面虚拟计算机软件，使用户可在单一的桌面上同时运行不同的操作系统，是进行开发、测试、部署新的应用程序的最佳解决方案。VMware Workstation可在一部实体机器上模拟完整的网络环境，其更好的灵活性与先进的技术胜过了市面上大多数的虚拟计算机软件。对于企业的IT开发人员和系统管理员而言，VMware在虚拟网路、实时快照、拖曳共享文件夹、支持PXE等方面的特点使它成为必不可少的工具。

本书的实验是在 VMware Workstation 7 上完成的，下面简单列举 VMware Workstation 7 新增的一些功能：

- 完善了对 3D 的支持。
- 支持最新 Windows 7 WDDM 驱动。
- 支持 vSphere 4.0 和 ESX。
- 可直接使用虚拟机进行打印。
- AutoProtect。
- 支持对虚拟机进行加密。
- 支持 IPv6、ALSA。
- 虚拟磁盘可扩展，无须使用额外的软件。

1.1.2　VMware 虚拟机的安装

1. VMWare Workstation 7.0 安装

VMWare Workstation 7.0 与大多数安装包一样，只需要一直单击安装向导界面的“下一步”按钮就可以完成 VMware 的安装。安装完成以后直接双击运行%VMware 安装目录%\vmware.exe。进入 VMware 界面以后选择“文件”→“新建”→“虚拟机”命令，正确操作完成以后会弹出一个名为“新建虚拟机向导”的窗口。

在新弹出的窗口上单击“下一步”按钮；虚拟机配置选择默认的“典型”，单击“下一步”按钮；客户机操作系统选择 Microsoft Windows，版本选择 Windows Server 2003 Enterprise Edition，单击“下一步”按钮；虚拟机名称和位置可以根据个人爱好自定义，单击“下一步”按钮；网络连接选择“使用 Host-only 网络”，单击“下一步”按钮；磁盘容量使用默认值，单击“完成”按钮。

至此，一台虚拟的个人计算机就已经准备就绪了。单击“编辑虚拟机设置”选项，可以手动配置虚拟机的硬件资源。值得注意的是，在此处配置的硬件资源需要与宿主计算机共享，所以分配的硬件资源应该根据实际情况而定。

2. 在虚拟机下安装 Windows 2003

选择在上一步安装好的虚拟机，单击“启动该虚拟机”选项；在 VMware 主窗口上选择“虚拟机”→“可移动设备”→CD-ROM →“编辑”按钮。此时会弹出一个名为“CD-ROM 设备”的子窗体。如果你准备的 Windows 2003 已经刻录在 CD 上，请将 CD 盘放入宿主计算机光驱，在子窗体选择“使用物理驱动器”选项，单击“确定”按钮。如果你准备的 Windows 2003 为 ISO 镜像文件，则在子窗体选择“使用 ISO 镜像”选项，单击“确定”按钮。如果此时虚拟机提示“…Operating System not found…”，在确保已经正确指向准备好的 Windows 2003 镜像的情况下，单击“关闭电源”按钮然后再次重启虚拟机。此时就可以看到熟悉的 Windows 系统安装向导。Windows 2003 安装结束以后，再次启动虚拟机，此时就可以看到熟悉的 Windows 启动画面。

至此虚拟机上安装 Windows 2003 已经结束。此时你可以用 VMware 提供的虚拟机克隆功能将刚刚安装好的 Windows 2003 进行克隆。

1.1.3 VMware 网络模式

VMware 提供了三种网络模式，它们是 bridged(桥接模式)、NAT(网络地址转换模式)和 host-only(主机模式)。

1. bridged

在这种模式下，VMware 虚拟出来的操作系统就像是局域网中的一台独立的主机，它可以访问网内任何一台机器。在桥接模式下，你需要手工为虚拟系统配置 IP 地址、子网掩码，而且还要和宿主机器处于同一网段，这样虚拟系统才能和宿主机器进行通信。同时，由于这个虚拟系统是局域网中的一个独立的主机系统，那么就可以手工配置它的 TCP/IP 配置信息，以实现通过局域网的网关或路由器访问互联网。使用桥接模式的虚拟系统和宿主机器的关系，就像连接在同一个 Hub 上的两台计算机。想让它们相互通信，就需要为虚拟系统配置 IP 地址和子网掩码，否则就无法通信。如果要利用 VMWare 在局域网内新建一个虚拟服务器，为局域网用户提供网络服务，就应该选择桥接模式。

2. host-only

在某些特殊的网络调试环境中，要求将真实环境和虚拟环境隔离开，这时就可采用 host-only 模式。在 host-only 模式中，所有的虚拟系统都是可以相互通信的，但虚拟系统和真实的网络是被隔离开的。

提示：在 host-only 模式下，虚拟系统和宿主机器系统是可以相互通信的，相当于这两台机器通过双绞线互连。在 host-only 模式下，虚拟系统的 TCP/IP 配置信息(如 IP 地址、网关地址、DNS 服务器等)，都是由 VMnet1(host-only)虚拟网络的 DHCP 服务器来动态分配的。如果想利用 VMWare 创建一个与网内其他机器相隔离的虚拟系统，进行某些特殊的网络调试工作，就可以选择 host-only 模式。

3. NAT

使用 NAT 模式，就是让虚拟系统借助 NAT(网络地址转换)功能，通过宿主机器所在的网络来访问公网。也就是说，使用 NAT 模式可以实现在虚拟系统里访问互联网。NAT 模式下的虚拟系统的 TCP/IP 配置信息是由 VMnet8(NAT)虚拟网络的 DHCP 服务器提供的，无法进行手工修改，因此虚拟系统也就无法和本局域网中的其他真实主机进行通信。采用 NAT 模式最大的优势是虚拟系统接入互联网非常简单，不需要进行任何其他的配置，只需要宿主机器能访问互联网即可。如果想利用 VMWare 安装一个新的虚拟系统，在虚拟系统中不用进行任何手工配置就能直接访问互联网，那么建议采用 NAT 模式。

1.2 WireShark 网络数据包的抓取

【实验目的】

(1) 学习使用 WireShark 软件的基本操作；

(2) 了解 IP 数据报的格式，详细了解各部分的位宽和功能；

(3) 抓取局域网络中的数据包并观察分析。

【实验内容】

使用 WireShark 进行网络抓包并观察 IP 包。

【实验设备与环境】

PC(Windows XP)，WireShark 安装软件。

【实验方法步骤】

(1) 观察 IP 包数据报格式，着重了解关键字段如位偏移等字段的长度和含义等。

(2) 利用 WireShark 软件进行端口检测，抓 IP 包进行报文分析，如图 1-1 所示。

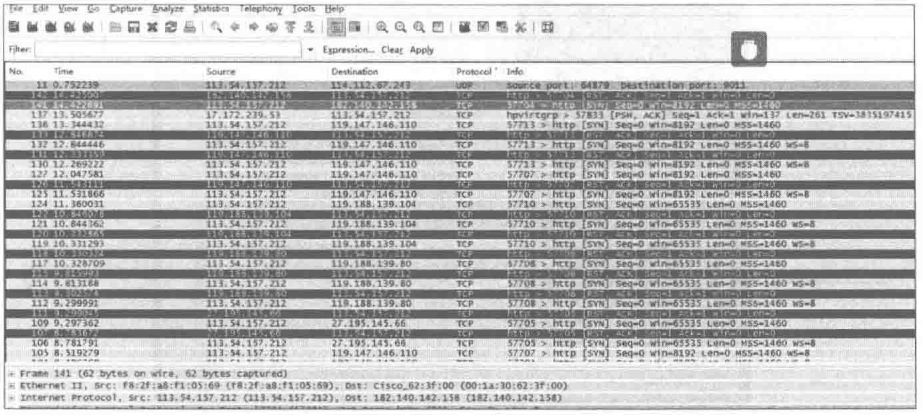

图 1-1　WireShark 软件抓取的 IP 包

分析该 IP 包可知：

起始时，源 IP 为 113.54.157.212 目的 IP 为 182.140.142.158 seq＝0 传送窗口为 8192 长度为 0；

返回时，源 IP 为 182.140.142.158 目的 IP 为 113.54.157.212 seq＝1 Ack＝1。

1.3　建立 VMWare 的虚拟网络环境的实验

【实验目的】

(1) 掌握虚拟机 VMWare 的典型安装和配置方法；

(2) 掌握基于虚拟机 VMware 的 Windows Server 2003 安装方法；

(3) 熟悉并安装虚拟机 VMWare Tools 的主要功能。

【实验内容】

(1) 安装 VMware Workstation 7；

(2) 在虚拟机 VMware 上安装 Windows Server 2003。

【实验设备与环境】

(1) PC(Windows XP)；

(2) VMware Workstation7 安装软件；

(3) Windows Server 2003 系统镜像文件。

【实验方法步骤】

(1) 安装 VMware Workstation 7。

(2) 新建虚拟机并安装 Windows Server 2003 系统，如图 1-2 至图 1-8 所示。

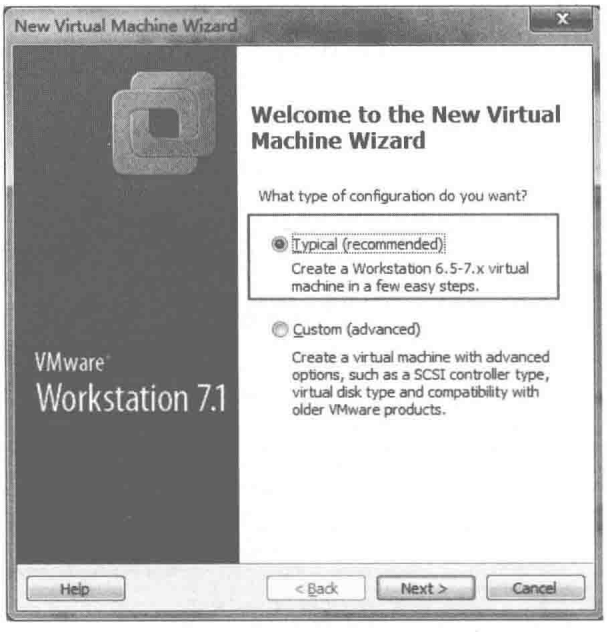

图 1-2 选择典型配置

图 1-3 选择操作系统