高等院校计算机实验与实践系列示范教材

Windows信息安全实践教程

孙夫雄　编著

清华大学出版社

高等院校计算机实验与实践系列示范教材

Windows信息安全实践教程

孙夫雄　编著

清华大学出版社

内 容 简 介

本书是基于 Windows 系统平台编写的信息安全实践教程，包括 16 个实践操作，分为初级篇和高级篇，初级篇有 10 个实践，包括虚拟机配置、操作系统启动方式、命令提示符、注册表和组策略、文件类型、进程与模块、Windows 账户与访问控制、消息钩子和 DLL 注入、数据安全以及木马实践；高级篇有 6 个实践，包括 Windows 内核基本分析、SQL 注入、跨站脚本攻击、PE 文件格式、Rootkit 技术和恶意代码取证分析。

本书内容丰富，特色鲜明，实用操作性强，可作为非计算机或计算机相关专业本科生的信息系统安全实践教材，也可作为计算机用户的参考书和培训教材。

图书在版编目(CIP)数据

Windows 信息安全实践教程/孙夫雄编著. —北京：清华大学出版社，2015
高等院校计算机实验与实践系列示范教材
ISBN 978-7-302-39141-8

Ⅰ. ①W…　Ⅱ. ①孙…　Ⅲ. ①Windows 操作系统－安全技术－高等学校－教材　Ⅳ. ①TP316.7

中国版本图书馆 CIP 数据核字(2015)第 017736 号

责任编辑：闫红梅　王冰飞
封面设计：傅瑞学
责任校对：梁　毅
责任印制：宋　林

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 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：15.25　　**字　　数**：380 千字
版　　次：2015 年 5 月第 1 版　　**印　　次**：2015 年 5 月第1 次印刷
印　　数：1～2000
定　　价：29.00 元

产品编号：062430-01

出版说明

当前，重视实验与实践教育是各国高等教育界的发展潮流，我国与国外教学工作的差距也主要表现在实践教学环节上。面对新的形式和新的挑战，完善实验与实践教育体系成为一种必然。为了培养具有高质量、高素质、高实践能力和高创新能力的人才，全国很多高等院校在实验与实践教学方面进行了大力改革，在实验与实践教学内容、教学方法、教学体系、实验室建设等方面积累了大量的宝贵经验，起到了教学示范作用。

实验与实践性教学与理论教学是相辅相成的，具有同等重要的地位。它是在开放教育的基础上，为配合理论教学、培养学生分析问题和解决问题的能力以及加强训练学生专业实践能力而设置的教学环节；对于完成教学计划、落实教学大纲，确保教学质量，培养学生分析问题、解决问题的能力和实际操作技能更具有特别重要的意义。同时，实践教学也是培养应用型人才的重要途径，实践教学质量的好坏，实际上也决定了应用型人才培养质量的高低。因此，加强实践教学环节，提高实践教学质量，对培养高质量的应用型人才至关重要。

近年来，教育部把实验与实践教学作为对高等院校教学工作评估的关键性指标。2005 年 1 月，在教育部下发的《关于进一步加强高等学校本科教学工作的若干意见》中明确指出："高等学校要强化实践育人的意识，区别不同学科对实践教学的要求，合理制定实践教学方案，完善实践教学体系。要切实加强实验、实习、社会实践、毕业设计（论文）等实践教学环节，保障各环节的时间和效果，不得降低要求。"，"要不断改革实践教学内容，改进实践教学方法，通过政策引导，吸引高水平教师从事实践环节教学工作。要加强产学研合作教育，充分利用国内外资源，不断拓展校际之间、校企之间、高校与科研院所之间的合作，加强各种形式的实践教学基地和实验室建设。"

为了配合开展实践教学及适应教学改革的需要，我们在全国各高等院校精心挖掘和遴选了一批在计算机实验与实践教学方面具有潜心研究并取得了富有特色、值得推广的教学成果的作者，把他们多年积累的教学经验编写成教材，为开展实践教学的学校起一个抛砖引玉的示范作用。

为了保证出版质量，本套教材中的每本书都经过编委会委员的精心筛选和

严格评审，坚持宁缺毋滥的原则，力争把每本书都做成精品。同时，为了能够让更多、更好的实践教学成果应用于社会和各高等院校，我们热切期望在这方面有经验和成果的教师能够加入到本套丛书的编写队伍中，为实践教学的发展和取得成效做出贡献；也衷心地期望广大读者对本套教材提出宝贵意见，以便我们更好地为读者服务。

清华大学出版社

联系人：索梅 suom@tup.tsinghua.edu.cn

FOREWORD 前言

信息世界充满安全威胁，包括系统漏洞、内部人员威胁、黑客渗透、社会工程以及来自于恶意程序（例如熊猫烧香、灰鸽子、USB 病毒、网页挂马、病毒和蠕虫等）的威胁，同时各种新的安全威胁层出不穷，与日俱增。目前，来自于 Internet 的信息安全威胁已经越来越严重，入侵方式更加多样化，并且给用户带来了非常严重的损失，包括隐私或机密信息泄露、信息丢失或被破坏导致不可用以及信息被非授权修改、删除等。

随着计算机的普及与 Internet 技术的不断发展，越来越多的人开始利用 Internet 来查阅资料、收发电子邮件、交友聊天、游戏娱乐等，计算机和 Internet 已经开始明显地改变人们的日常生活和学习方式。当前流行的几个操作系统有 Windows、UNIX 和 MAC 等，但学生平时学习和生活中使用更多的还是 Windows 系统，而大多数学生基本停留在会用 Windows 系统的层面上，对系统本身的体系结构和安全机制通常一知半解，因此在开放、充满诱惑但又极不安全的网络环境中，学生普遍对其所面临的信息安全威胁认识不足，在遇到信息安全风险时无法正确地规避风险和进行有效防护。

目前与信息安全实验相关的书籍出版较多，其中不乏精品，但理论性较强，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、信息论等多种学科，对于非计算机专业甚至计算机相关专业的学生来说过于深奥，以致难以理解和掌握，达不到信息安全通识教育的目标。

本书以 Windows 系统为实践平台，实践项目的选择切合非计算机专业学生的知识背景，实践内容由浅入深、由易到难，比较容易操作和实现，旨在通过实践提高学生对安全威胁的甄别能力和防范能力。本书内容分为 16 个实践项目，每个项目包括实践目的、实践环境、名词解释、预备知识、实践操作及步骤以及思考题几部分。

实践 1 介绍虚拟机的安装与配置，实现实践环境的搭建。

实践 2 在了解 Windows 操作系统、系统启动选项、计算机启动过程的基础上，完成修改系统启动、操作系统探查、虚拟桌面、PE 启动盘等实践操作。

实践 3 掌握 Windows 常用命令以及环境变量的设置。

实践 4 了解并掌握注册表和组策略的结构、原理以及修改方法，通过实践理解其与计算机安全的紧密关系。

实践5 了解文件格式、类型及其查看方法，通过修改文件夹选项、修改文件时间属性和图标、修改文件关联等实践操作理解文件夹病毒的原理和机制。

实践6 了解Windows操作系统中进程、线程、服务以及模块的概念，掌握利用工具查看它们的方法。

实践7 理解Windows操作系统中安全账户和访问控制的重要性，掌握其设置方法，包括建立和删除系统隐藏账户、使用Cacls命令、修改管理员账户和创建陷阱账户。

实践8 了解Windows的消息机制、窗口和DLL注入的基本原理，通过窗口句柄及其消息的查看、窗口属性的修改、DLL注入和DLL网络连接等实践加强理解。

实践9 了解加密技术，掌握个人数据保护以及数据加密、安全删除和恢复的方法。实践内容包括文件命令隐藏、流文件隐藏及其检测方法、Word文档数字证书的保护、TrueCrypt软件实现文件加密、EasyRecovery软件实现文件的恢复、Eraser软件实现文件的安全擦除以及移动设备防病毒感染等。

实践10 了解木马的工作机制和通信模式以及检测方法，通过“上兴木马”的具体安装、操作及其工作机制的分析，使读者认识木马的危害性和原理并掌握其检测方法。

实践11 了解Windows内核原理，掌握内核的基本分析方法。实践内容包括蓝屏产生及分析、内核结构体查看、KiFastCallEntry机理分析等。

实践12 了解Web应用表单处理流程，理解SQL注入漏洞的原理。实践内容包括字符串型SQL注入、数字型SQL注入和SQL注入修改数据。

实践13 了解网站脚本工作原理，理解跨站脚本攻击机制。实践内容包括存储型XSS、反射型XSS、XSS钓鱼和跨站请求伪造。

实践14 较深入理解EXE和DLL文件的PE格式，理解可执行文件加载原理及线程注入的原理。结合具体的程序源代码分析，理解PE文件格式，实现EXE注入、线程启动和EXE感染的实践操作。

实践15 理解和掌握Rootkit技术的原理和工作机制，了解Bootkit技术，了解当前木马或病毒的隐藏机理，以及杀毒软件的防护原理。实践内容包括文件和进程隐藏、RootkitRevealer的使用。

实践16 理解和掌握恶意代码取证和分析的方法，通过对一个具体软件的取证分析，使读者了解计算机取证的流程和方法。

本书由孙夫雄主编，其中，宋玉美参与实践1的编写，余梦姗参与实践3和实践4的编写，吴天雄参与实践7和实践9的编写，汪可参与实践12和实践13的编写，本书校验由汪可和余梦姗完成。

本书可作为非计算机或计算机相关专业本科生的信息系统安全实践教材，也可作为计算机用户的参考书和培训教材。书中涉及的工具和代码皆可在清华大学出版社网站(www.tup.tsinghua.edu.cn)上找到。

由于作者自身水平有限，本书难免会有不妥与疏漏之处，恳请专家和读者提出宝贵意见。

编　者

2015年1月

CONTENTS 目录

初 级 篇

高 级 篇

初级篇

PART

实践1 虚拟机配置

1. 实践目的

(1) 安装并使用虚拟机。

(2) 熟练地在虚拟机上运行软件。

(3) 实现虚拟机的网络连接。

2. 实践环境

(1) 连入 Internet 的计算机一台，安装 Windows XP 或 Windows 7 等操作系统。

(2) 实践工具：VMware Workstation 安装包；操作系统 ISO 安装文件(纯净安装版)。

3. 名词解释

(1) **虚拟机**：通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。

(2) **ISO 安装文件**：光盘的镜像文件，刻录软件可以直接把 ISO 文件刻录成可安装的系统光盘，用虚拟光驱加载运行或用 WinRAR 解压缩打开。ISO 文件一般以 iso 为扩展名，其文件格式为 ISO 9660。

4. 预备知识

1) 原理及作用

虚拟机应用软件在宿主计算机的真实处理器和内存基础之上为虚拟机提供虚拟硬件仿真，这些仿真的硬件能够完全被安装在虚拟机上的操作系统认为是真实的硬件。也就是说，从操作系统的运行特性来看，虚拟出的硬件和真实的硬件没有本质上的差别。

虚拟机的作用：作为个人用户，可以通过在一台 PC 上安装虚拟机，实现同时运行多个操作系统，而且不用重新启动计算机，只需单击鼠标即可打开新的操作系统或是在操作系统之间进行切换。总体来说，使用虚拟机可以有以下一些典型用途。

(1) 质量评估。

对于软件企业和公司而言,由于不同的操作系统版本和大量的配置项,软件产品的测试将耗费大量的管理费用,通过使用虚拟机及其丰富的特性,可以降低企业采购和管理硬件的成本,并提高工作效率。

(2) 程序开发与测试。

程序员可以利用虚拟机的优越性实现跨平台开发不同操作系统下的应用程序,不需要重新启动计算机就可以完成整个开发阶段的试运行和调试(Program Debugging),因而节约大量的开发时间。在网络测试方面,可以利用虚拟机的网络特性,利用一台计算机即可建立完整的、封闭性的网络,既不需要另外配置硬件设备又保证了数据安全。

(3) 操作系统研发。

开发操作系统时程序员遇到的第一个难题是操作系统需要不断编译调试,如何才能让被编译的内核程序在一个系统上进行测试。这种测试以往很难在编写代码的同一台计算机上进行,因为不断重新启动计算机会大大干扰编写的进程。另外,把要测试的内核代码转移到一台专用的测试机上需要使用可移动磁盘,操作麻烦且增加费用。此时使用虚拟机就是最佳的解决方案了。可以把要调试的内核程序作为一个客户操作系统,编程间隙还可以把调试中的客户操作系统放大到全屏。

(4) 教育培训和商务演示。

IT 培训或是自学计算机技术,都必然涉及多个操作系统和多种类型的软件,这个时候使用虚拟机将有巨大的优越性。IT 销售人员推销的计算机软件产品经常可以跨越多个操作系统平台,有不同的版本,使用虚拟机就可以仅携带一台笔记本电脑到客户那里进行推销和演示了。这个方法同样适用于技术支持和维护人员。

(5) 服务器端产品。

就虚拟机技术而言,最早是出现在大型机上的,已经有几十年的历史了,当时比尔·盖茨和他的朋友保罗·艾伦开发的最早的 PC BASIC 语言环境,就是在大型机上模拟出完整的以 Intel 4004 芯片为 CPU 的,仅有 4KB 内存的最原始的 PC 而调试通过的。

(6) 信息安全。

虚拟机可用于未知病毒的查杀,主要应用在脱壳方面,由于许多未知病毒的本质都是一样的,只是把原病毒加了一个壳,如果能成功地把病毒的这层壳脱掉,就很容易将病毒清除了,缺点是消耗大量的系统资源。对于个人用户,利用虚拟机运行可疑的软件,或通过虚拟机上网冲浪,可以杜绝病毒感染主机,即使病毒破坏了虚拟机系统也不影响主机系统和数据,虚拟机系统的恢复也很容易。

目前,虚拟机服务器已经从大型机拓展到 Intel 平台,作为巩固数据中心的方法,它正在掀起一股空前的流行趋势。Intel 服务器虚拟机领域主要有三家公司在竞争,包括 VMware、MS VPC(前身 Connectix 被 MS 收购)和 Swsoft,都提供独特的解决方案。

VMware Workstation(中文名"威睿工作站")是一款功能强大的桌面虚拟计算机软件,提供用户可在单一的桌面上同时运行不同的操作系统,进行开发、测试、部署。除了对整个计算机进行虚拟外,常见的虚拟软件有虚拟光驱、虚拟桌面、虚拟摄像头、虚拟串口等。

2) 虚拟机网络模式

VMware 虚拟软件的网络适配器模式有以下 3 种。

(1) 桥接模式。

这是 VMware 的默认选项。桥接模式是指本地物理网卡和虚拟网卡通过 VMnet0 虚拟交换机进行桥接,虚拟交换机就相当于一台现实网络中的交换机,物理网卡和虚拟网卡在网络中处于同等地位,并处于同一个网段,即虚拟网卡的 IP 地址设置为与物理网卡同一个网段,IP 地址和 DNS 地址设为自动获取即可。

(2) NAT 模式。

NAT(Network Address Translation,网络地址转换)属接入广域网(WAN)技术,是一种将私有(保留)地址转化为合法 IP 地址的转换技术,它被广泛应用于各种类型的 Internet 接入方式和各种类型的网络。NAT 不仅完美地解决了 IP 地址不足的问题,而且还能够有效地避免来自网络外部的攻击,隐藏并保护网络内部的计算机。

NAT 模式中,让虚拟机借助 NAT 功能,通过宿主机所在的网络来访问公网。NAT 模式中,虚拟机的网卡和物理网卡的网络,不在同一个网络,虚拟机的网卡是在 WMware 提供的一个虚拟网络。

NAT 模式和桥接模式的比较如下。

① NAT 模式和桥接模式虚拟机都可以上外网。

② 由于 NAT 的网络在 VMware 提供的一个虚拟网络里,所以局域网其他主机是无法访问虚拟机的,而宿主机可以访问虚拟机,虚拟机可以访问局域网的所有主机,因为真实的局域网相对于 NAT 的虚拟网络,就是 NAT 的虚拟网络的外网。

③ 桥接模式下,多个虚拟机之间可以互相访问;NAT 模式下,多个虚拟机之间也可以相互访问。

(3) 仅主机模式。

在仅主机(Host-Only)模式下,虚拟网络是一个全封闭的网络,它唯一能够访问的就是主机。Host-Only 网络和 NAT 网络很相似,不同的地方就是 Host-Only 网络没有 NAT 服务,所以虚拟网络不能连接到 Internet。主机和虚拟机之间的通信是通过 VMware Network Adepter VMnet1 虚拟网卡来实现的。

Host-Only 的宗旨就是建立一个与外界隔绝的内部网络,来提高内网的安全性。这个功能或许对普通用户来说没有多大意义,但大型服务商会常常利用这个功能。

5. 实践操作及步骤

下载操作系统 ISO 安装文件和虚拟机 VMware 安装包(软件版本为 10.0),首先安装 VMware,然后用 VMware 10.0 序列号进行注册。双击桌面 VMware 图标打开虚拟机软件主界面,如图 1-1 所示。

图 1-1 显示了当前已安装了 3 个虚拟操作系统,即 Windows 7、Ubuntu 和 Windows XP 以及它们的文件所在的目录。在 Windows 7 选项卡中显示了该虚拟系统的设备信息,通过“编辑虚拟机设置”可以修改设备参数,或删除、添加设备,如图 1-2 所示。

安装新的虚拟操作系统步骤如下。

(1) 选择“文件”→“新建虚拟机”,弹出“新建虚拟机向导”对话框,如图 1-3 所示。单击“典型”单选按钮再单击“下一步”按钮。选择如图 1-3(b)中所示的“稍后安装操作系统”后单击“下一步”按钮。

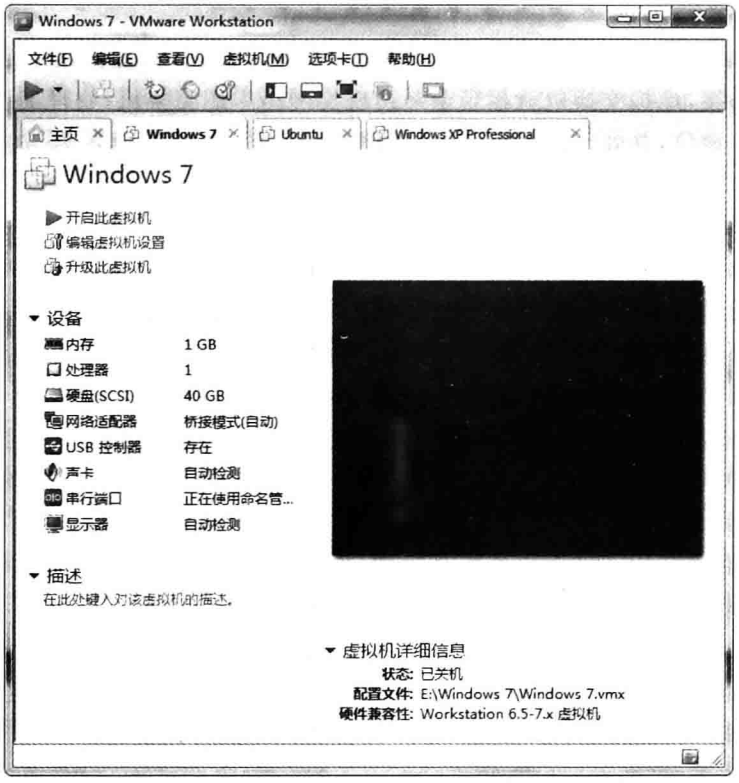


图 1-1 VMware 主界面

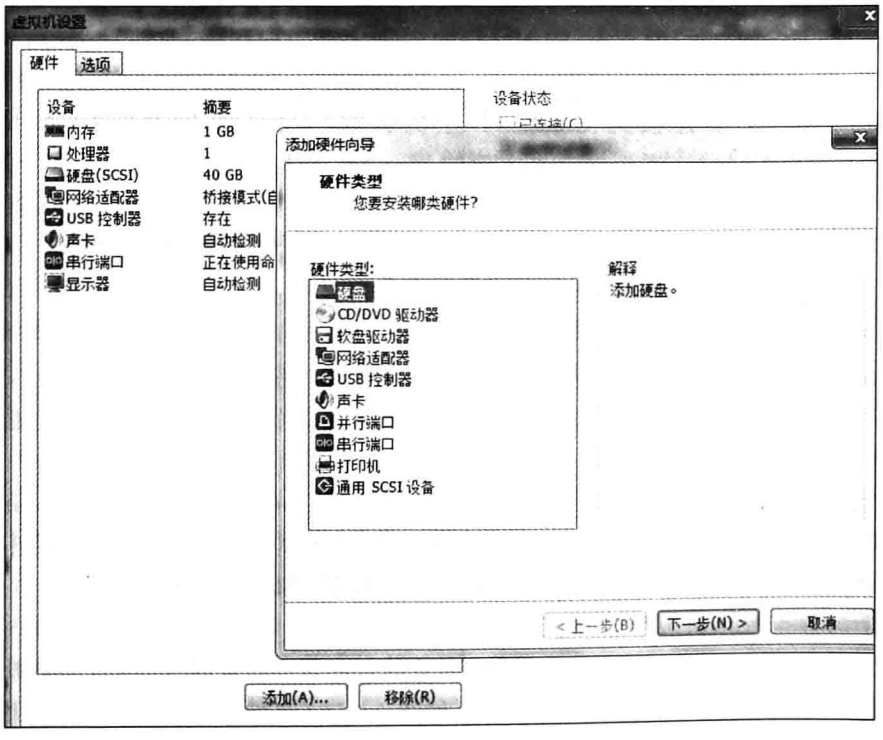
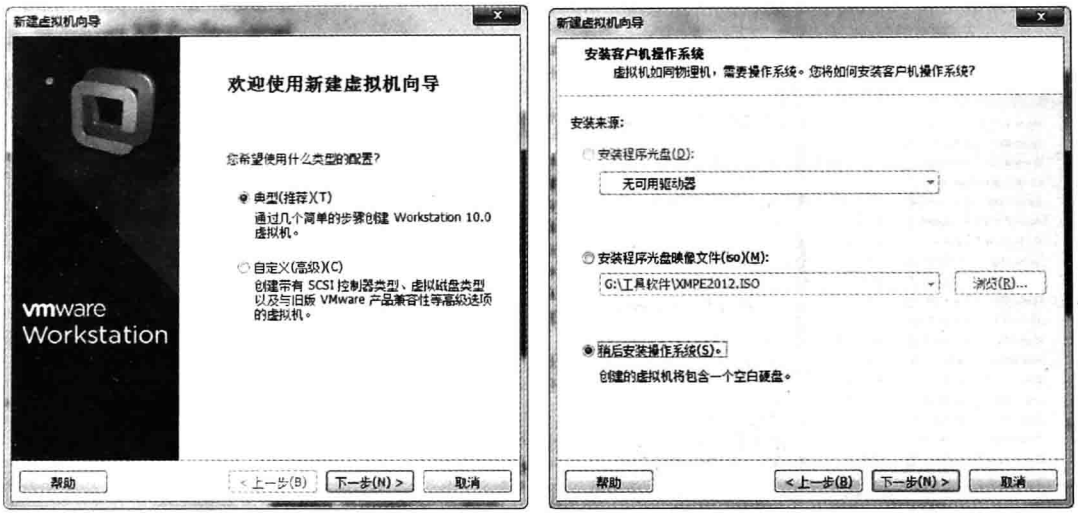


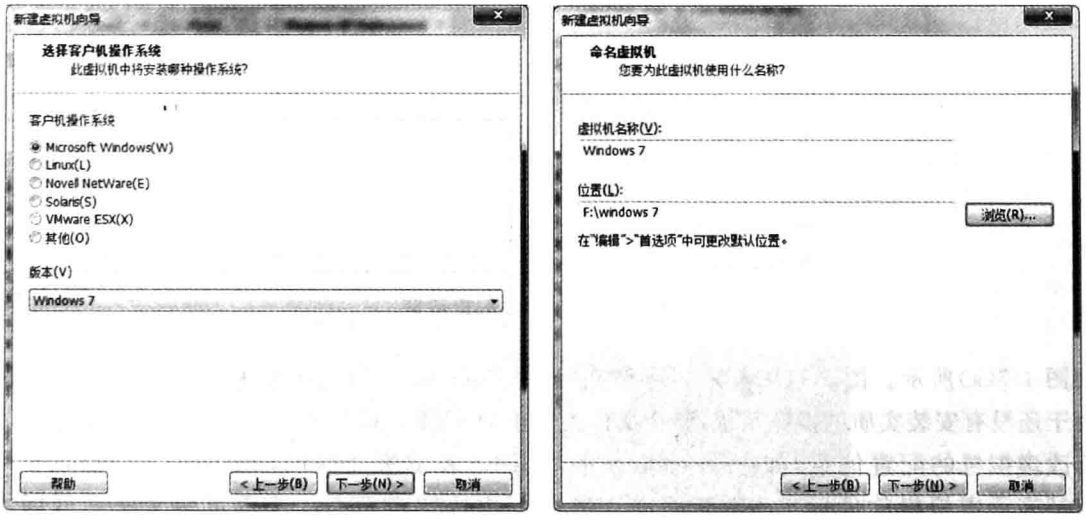
图 1-2 编辑虚拟机设置



(a) (b)

图 1-3 安装向导

(2) 在图 1-4(a)中选择客户机操作系统类型,在 Microsoft Windows 里选择 Windows 7 系统。在图 1-4(b)中设置虚拟机名称以及虚拟机文件的安装目录,注意不使用默认的安装目录。



(a) (b)

图 1-4 选择客户机操作系统类型并命名虚拟机

(3) 接下来设置虚拟系统的磁盘大小。如图 1-5 所示,"将虚拟磁盘存储为单个文件"其文件大小可能有数十 GB 之多(依赖于系统中安装软件的数量和大小),而"将虚拟磁盘拆分成多个文件"每个文件大小上限只有 2GB 左右,有助于复制。图 1-6 中显示了虚拟系统配置信息。可以单击"自定义硬件"按钮修改、增加或删除硬件,如图 1-2 所示。

单击图 1-6 中的"完成"按钮后则回到主界面并新增了一个名为 Windows 7 的选项卡,

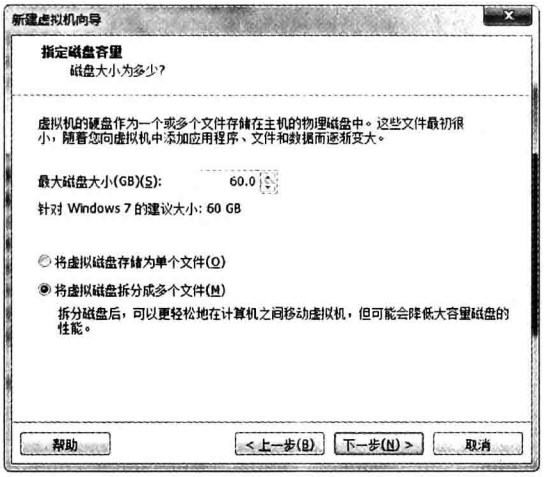


图 1-5　设置虚拟系统的磁盘

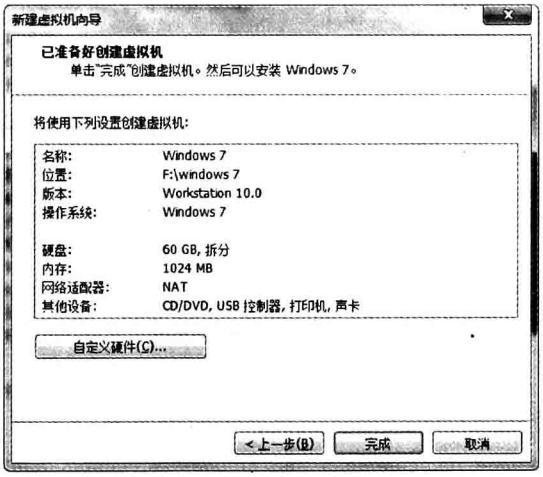
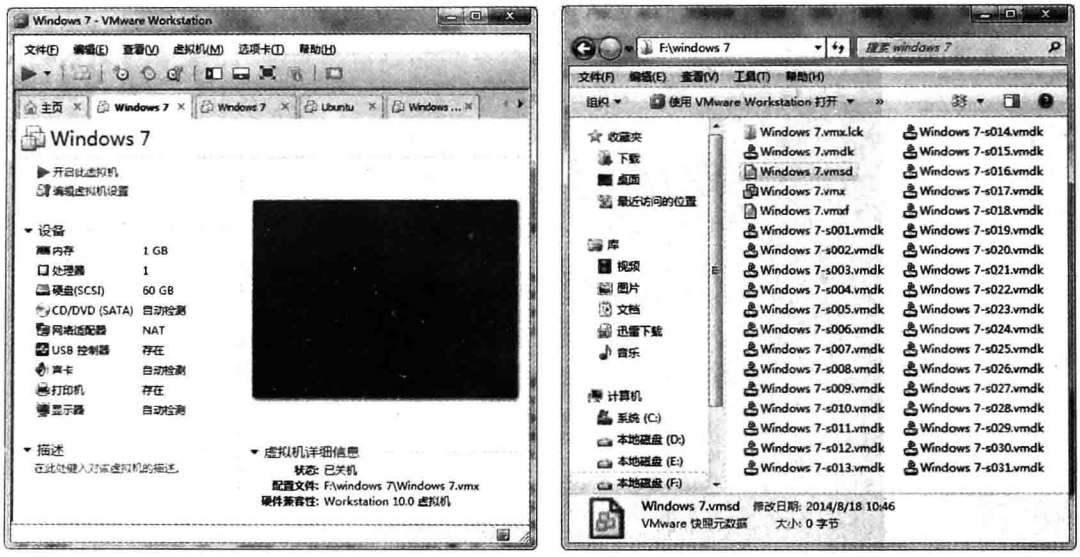


图 1-6　虚拟系统配置信息

如图 1-7(a)所示。图 1-7(b)显示了存储在“F:\windows 7”目录下的虚拟磁盘的多个文件，由于还没有安装实质的操作系统，整个文件夹大小为 9MB。其中文件 Windows 7. vmx 包含了修改虚拟机的配置信息，如：. encoding = "GBK"表示中文编码，virtualHW. version = "10"表示虚拟机软件版本；用高版本 VMware 生成的虚拟系统文件可能无法用低版本 VMware 打开，这时将 virtualHW. version 的值修改为对应的版本值即可。

(4) 在图 1-2 所示的“虚拟机设置”对话框中，单击“CD/DVD 驱动器”设备，选择“使用 ISO 映像文件”，如图 1-8 所示。

(5) 设置 BIOS 的启动次序。单击“开启此虚拟机”后虚拟计算机启动，立刻按住键盘上的 F2 键不放，即进入 BIOS 设置界面，如图 1-9 所示，使用左右方向键切换到 Boot 选项卡，用上下方向键选择 CD-ROM Drive，然后按 Shift 和＋键将 CD-ROM Drive 移至顶端，按 F10 键保存退出。



(a) (b)

图 1-7 新建操作系统信息

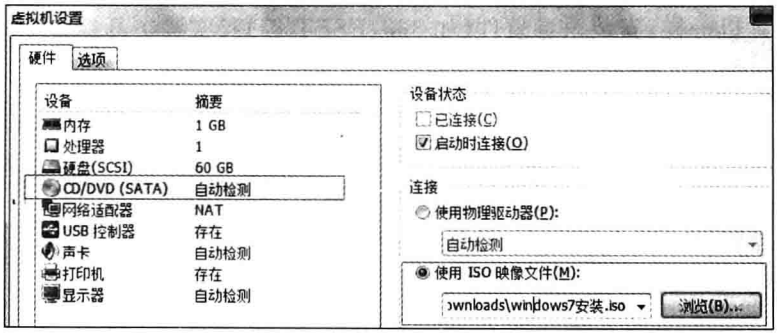


图 1-8 设置 CD/DVD 设备

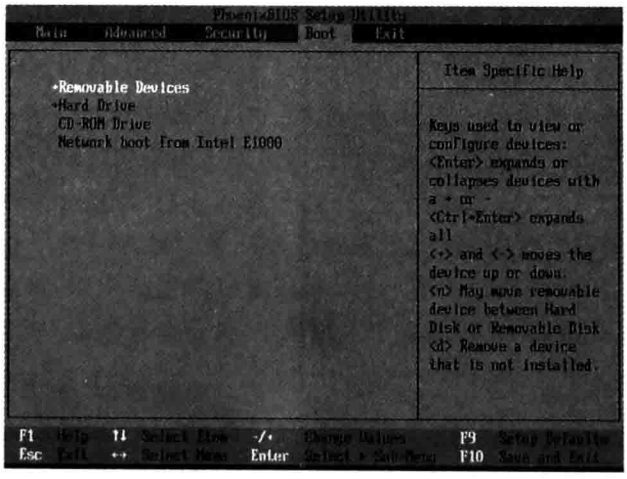


图 1-9 设置 BIOS 启动次序