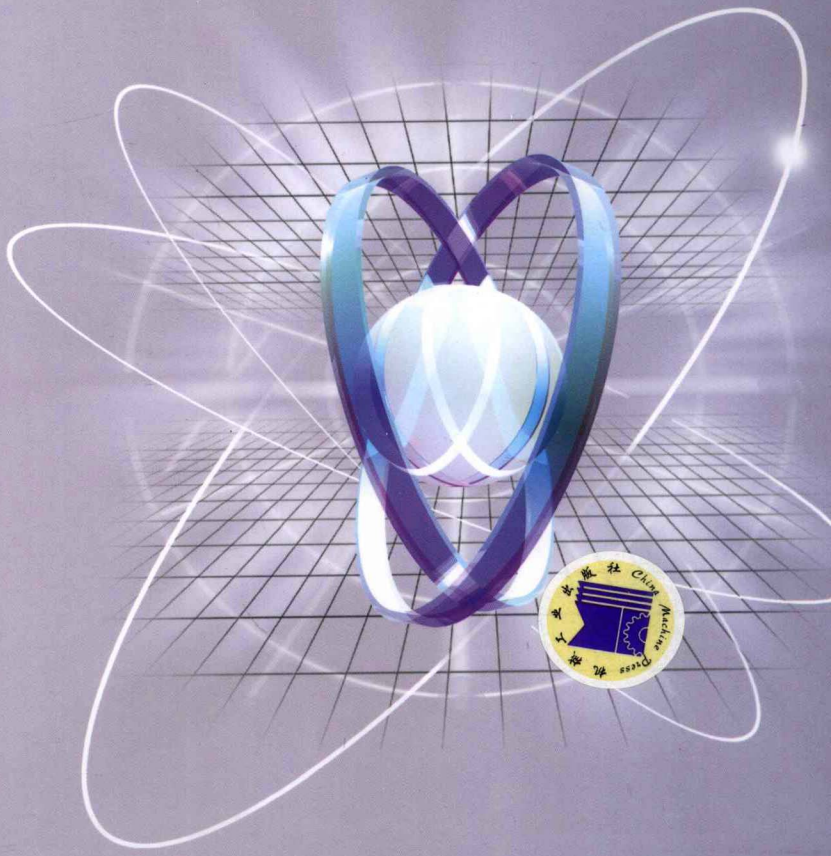
高等院校信息安全专业规划教材

计算机系统安全实验教程

- 计算机系统安全问题及安全机制
- 应急响应与灾难恢复
- 计算机安全等级评测

陈 波 于 泠 编著



机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

计算机系统安全实验教程

陈 波　于 泠　编著

机 械 工 业 出 版 社

本实验教程涉及了计算机系统各层次的安全问题和普遍采用的安全机制，包括密码基础知识、计算机硬件、操作系统、计算机网络、数据库系统、程序和应用系统、应急响应与灾难恢复、计算机系统安全风险评估等近40个安全实验。

实验教程既可与教材《计算机系统安全原理与技术》（第2版）配套使用，也可单独作为信息安全实验指导书，便于自学。本书设计的实验（包括网络环境下的安全实验）仅需在PC上实现，无需增加额外的软、硬件设备投资。实验内容新颖，每个实验均给出了详细的操作步骤及相关代码，并给出了丰富的参考资料。

本书可作为信息安全专业、信息对抗专业、计算机专业、信息工程专业或相近专业的本科或研究生教材，也可作为网络信息安全领域科技人员的参考书。

图书在版编目（CIP）数据

计算机系统安全实验教程/陈波，于泠编著. —北京：机械工业出版社，2009.1
（高等院校信息安全专业规划教材）
ISBN 978-7-111-25837-7

Ⅰ. 计… Ⅱ. ①陈… ②于… Ⅲ. 电子计算机-安全技术-高等学校-教材 Ⅳ. TP309

中国版本图书馆CIP数据核字（2008）第201315号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
责任编辑：唐德凯
责任印制：李 妍
北京蓝海印刷有限公司印刷
2009年2月第1版·第1次印刷
184mm×260mm ·19.75印张·487千字
0001—3000册
标准书号：ISBN 978-7-111-25837-7
定价：32.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：（010）68326294 68993821
购书热线电话：（010）88379639 88379641 88379643
编辑热线电话：（010）88379753 88379739
封面无防伪标均为盗版

高等院校信息安全专业规划教材

编委会成员名单

出版说明

信息技术的发展和推广，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、中山大学、南京邮电学院等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1）作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2）系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3）系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4）注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5）内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前　言

“信息安全”是一个直接面向工程、面向应用的专业领域。信息安全课程的教学需要重视理论的讲授，使学生掌握解决问题的基本技术，更要强调实践教学，培养学生解决安全问题的操作能力，培养学生的整体安全意识和综合应用能力。

我们遵循信息安全 PDRR 模型的核心思想，以及“信息安全类专业指导性专业规范”项目组提出的“信息安全类专业知识体系”，并结合教材《计算机系统安全原理与技术》，编写了本书。

编写中我们力求做到：

1）内容系统、体系完整。与《计算机系统安全原理与技术》（第 2 版）一书相对应，从以下几个层次研究信息安全问题：计算机硬件与环境安全、操作系统安全、计算机网络安全、数据库系统安全、应用系统安全以及安全管理。设置的“信息安全”实验课程的内容包含 9 大类近 40 个模块。

第 1 类：密码学基础与密码技术应用，包括对称、非对称密码系统、公钥密码系统、消息摘要、数字签名、信息隐藏与数字水印等实验模块。

第 2 类：系统硬件安全，包括常用硬件设备的性能检测、将 U 盘改造成系统加密狗等实验模块。

第 3 类：操作系统安全，使用微软基准安全分析器分析系统漏洞、Windows 系统账户口令强度测试、Windows 系统安全配置、微软安全小工具的使用等实验模块。

第 4 类：数据库安全，包括 SQL Server 2000 的安全管理等实验模块。

第 5 类：网络安全，包括网络扫描工具的编程实现、网络嗅探工具的编程实现、网络防火墙的使用、Snort 入侵检测系统的使用、利用 OpenSSL 的 C/S 安全通信程序设计等实验模块。

第 6 类：恶意代码与安全程序设计，包括使用系统行为监控软件 SSM 防范恶意代码、U 盘病毒及其免疫程序的实现、软件保护常用技术编程实现、使用 WebScarab 进行 Web 安全测试等实验模块。

第 7 类：应急响应与灾难恢复，包括数据恢复软件 Easy Recovery 的使用、计算机取证软件 EnCase 的使用等实验模块。

第 8 类：风险评估与管理，包括安全漏洞扫描工具使用、风险评估工具使用等实验模块。

第 9 类：综合实验。

2）实用性强。实验教程既可与教材配套使用，也可单独作为信息安全实验指导书，便于自学。本书设计的实验（包括网络环境下的安全实验）仅需在 PC 上实现，无需增加额外的软、硬件设备投资，为条件有限的学校开展安全实验教学提供了方便。

3）实验新颖，可操作性好。我们结合已经完成的国家 863 应急项目、多项军队以及省

级科研项目的研究实践，结合多年的教学实践，设计了一些新颖实验，如利用 OpenSSL 的 C/S 安全通信程序设计、代码静态检测工具的使用、. NET 框架下密码算法的程序实现等。每个实验均给出了详细的操作步骤及相关代码。

4）问题驱动式的实验，注重能力培养。本教材实验分为 4 种类型：一类是验证性实验，直接运行仿真软件，查看实验结果，如使用 RSA Tool 工具来实践 RSA 算法原理；第 2 类是软件的安装、配置和使用实验，以帮助学生理解基本原理，掌握相关的网络安全应用或工具，如使用 Windows 系统下入侵检测开源软件 Snort 来实践入侵检测技术；第 3 类是安全技术的编程实现，以培养学生的知识应用和软件开发能力，提高网络安全实践技能，如 U 盘病毒及其免疫程序的实现等；第 4 类是综合安全实验，以培养学生的独立思考能力、综合运用能力、实际动手能力和团队协作能力。书中的每个实验均采用问题驱动式的实验内容，要求学生不是进行简单的模仿和重现，而是在书中提出的实际问题的驱动下进行分析、思考，最后通过实践来解决问题。每个实验最后都给出了思考问题及参考解答，引导学生发现新的安全问题，并通过进一步的实验验证。每个实验最后给出的参考文献丰富，提供了进一步学习的超链接点。

本实验教程的编写得到了南京师范大学的支持，2007 年“计算机系统安全”课程被评为南京师范大学研究性教学示范课程，本教材的编写在 2007 年得到立项——网络信息安全实验课程研究与实验平台建设。

陈波和于泠共同主持完成本书的编写，调试、完成了全书的程序。徐达威完成了部分实验初稿的整理工作，马亮、吴思仪、李佳阳，以及南京师范大学 05、06、07 级信息安全方向的研究生和本科生也为实验的完成作出了贡献。在本书的写作中，我们参考了大量的文献，也尽力在书中列出，在此一并致谢。

全军信息安全研究中心主任、解放军理工大学通信工程学院博士生导师肖军模教授，对本书的出版给予了悉心的指导。在此致以衷心的感谢。

随着网络通信技术、计算机技术的不断发展，计算机系统安全仍是一个不断发展的研究领域，虽然我们力求达到以上的目标，书中一定还存在错误和不足之处，恳请广大读者和专家提出批评和改进意见。读者在阅读本书的过程中若有疑问也欢迎与作者联系，电子邮箱是：seclab@163.com。

为了便于读者学习，本书提供实验中所有程序的源代码及相关软件下载的链接，读者可在机械工业出版社网站 www.cmpedu.com 上免费下载。

作　者

目　录

第 1 章　计算机系统安全虚拟实验环境搭建

1.1　虚拟机软件 VMware 的使用

【实验目的】

信息安全课程中要进行相关的安全实验，有的实验需要至少两台主机及其独立的操作系统，且主机间可以通过以太网进行通信。有的实验对系统本身以及对网络中其他主机有潜在的破坏性。为此，利用虚拟机软件 VMware 在一台主机中再虚拟出一台 PC 并安装一套操作系统，以便完成后续的安全实验。

【实验类型】

软件的安装、配置与使用。

【实验原理】

1. 虚拟机的概念

虚拟机的概念主要有两种，一种是像 Java 那样提供介于硬件和编译程序之间的软件；另一种是指利用软件“虚拟”出来一台计算机。本实验中的虚拟机是指后者。

“虚拟机”是一个由软件提供的、具有模拟真实的特定硬件环境的计算机，虚拟机提供的“计算机”和真正的计算机一样，也包括 CPU、内存、硬盘、光驱、软驱、显卡、声卡、SCSI 卡、USB 接口、PCI 接口、BIOS 等。在虚拟机中可以和真正的计算机一样安装操作系统、应用程序和软件，也可以对外提供服务。

x86 平台的虚拟化技术可分为 3 类，全硬件仿真虚拟化技术（Hardware Emulation）、半虚拟化技术（Para-Virtualization）和操作系统级虚拟化技术（OS-Level Virtualization）。

首先介绍虚拟化技术中 3 个最基本的概念。

- 宿主操作系统（Host OS）。该操作系统是与硬件直接进行数据通信的最底层的操作系统。
- 虚拟机监视器（Virtual Machine Monitor，VMM），又称虚拟化管理器（Virtual Monitor，Hypervisor）。位于宿主操作系统之上，负责配置、管理虚拟系统和调度、管理资源的一个系统级应用程序。
- 客户操作系统（Guest OS）。它们位于虚拟化管理器之上，是由虚拟化管理器配置、管理的。如 Microsoft Windows 或 Linux 的标准操作系统或虚拟环境（Virtual Environment）。

下面介绍 3 种虚拟化技术。

（1）全硬件仿真虚拟化技术

该技术最本质的特点是，虚拟化管理器将所有的真实硬件设备以软件形式仿真出来，在客户操作系统看来，仿真出来的硬件无异于真实硬件，即虚拟化管理器采用仿真的手段，骗过了作为客户操作系统的标准操作系统，使其以为安装在真实的硬件设备之上，全硬件仿真虚拟化技术架构如图 1-1 所示。

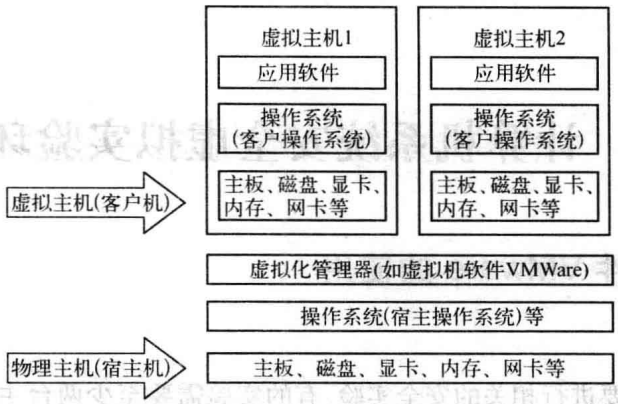


图 1-1　全硬件仿真虚拟化示意图

作为标准的操作系统,客户操作系统就是被设计成直接向 CPU 发出专有指令(The Privileged Instructions)来控制硬件的,但在虚拟机中,执行这些指令是非常危险的操作,会造成错误结果,甚至死机。为此,虚拟化管理器需要采用"动态指令重写"技术捕获这些来自虚拟机中客户操作系统的专有指令,并作相应处理。

正是由于全硬件仿真,也带来了这一技术的最大优势——客户操作系统选择的广泛性,即无需修改代码,就能成功地安装支持 x86 平台的任何操作系统,如 Microsoft Windows 系列、Linux 系列,甚至是支持 x86 平台的 Sun Solaris。

这一技术的主要领导者是 VMware。其中不管是早期的 Vmware Workstaiton 产品系列,还是现在的 VMware Server 系列和 VMware ESX 系列,都是采用全硬件仿真的技术思路,只不过,VMware Workstaiton 和 VMware Server 是基于某一特定的 Microsoft Windows 或是 Linux 平台,而 VMware ESX 是自带了一套 Linux 内核的宿主操作系统。

看到虚拟化的需求和发展趋势后,微软公司也相继推出了 Microsoft Virtual Server 和 Microsoft Virtual PC 系列产品。

(2) 半虚拟化技术

与全硬件仿真技术相似的"半虚拟化"技术也是基于硬件仿真的,但不同的是半虚拟化技术不是采用"动态指令重写"技术捕获这些来自虚拟机中客户操作系统的专有指令来避免"虚拟化漏洞",而是通过修改客户操作系统与体系相关的那部分内核模块,将虚拟机上的客户操作系统发出的专有指令重定向到虚拟化管理器上。目的是让客户操作系统知道它不是安装在硬件上,而是安装在虚拟管理器之上。这样,可以避免"动态指令重写"带来的性能损耗,得到一个更高效的虚拟化平台。

提升虚拟化系统的性能,降低性能损耗是半虚拟化技术设计的初衷。测试结果显示,基于"半虚拟化"技术的性能损耗在 3% 左右。

英国剑桥大学的 Xen 是一个基于"半虚拟化"技术的开源产品。尽管项目发展仅用了短短几年时间,但却被操作系统厂商、CPU 厂商、IBM、HP 等业界巨头看好,得到了各方的大量关注和支持。

(3) 操作系统级虚拟化技术

操作系统级虚拟化技术又称为内核级虚拟化技术(Kernal-Level Virtualization),是一种有

别于硬件仿真的虚拟化技术。“操作系统级”虚拟化技术采用的不是虚拟化硬件的技术思路，而是利用宿主操作系统的内核，通过开辟独享文件系统（Proprietary File System）和内核服务抽象层（Kernel Service Abstraction Layer）创建多个虚拟环境（Virtual Environment），每个虚拟环境对用户来讲就相当于一个虚拟的客户操作系统。

因为不是像“全硬件仿真”虚拟化技术和“半虚拟化”技术那样仿真出虚拟硬件，所以没有将“操作系统级”虚拟化系统称为虚拟机，而是称为虚拟环境。

操作系统级虚拟化技术在设计方面省去了最复杂的硬件仿真和资源管理调度，并将这些工作统统交给宿主操作系统，直接利用其内核，创建了一个安全、隔离的容器（Container）来虚拟出一个客户操作系统环境。由于省去的开销恰恰是产生开销最大的部分，所以，这种虚拟化技术性能损耗极小，甚至超过半虚拟化技术。

操作系统级虚拟化技术的代表是美国 SWSoft 公司开发的 Virtuozzo。

2. VMware 软件

VMware 和 Microsoft 公司都提供虚拟机软件（Microsoft 公司的虚拟机软件收购自 Connectix 公司）。VMware 的虚拟机软件包括 Workstation、GSX Server、ESX Server、ACE 等多种系列，Microsoft 提供 Microsoft Virtual PC 和 Microsoft Virtual Server 虚拟机。

VMware Workstation 是 VMware 公司的软件。从理论上讲，一台物理主机可以做什么，VMware Workstation 虚拟机就可以做什么。它支持的客户操作系统涵盖绝大多数主流操作系统，包括 Microsoft 全系列的操作系统以及大多数版本的 Linux。由于虚拟机运行时使用同一个虚拟 BIOS 以及一系列统一的虚拟硬件，在一定程度上实现了虚拟机的硬件无关性，并且客户操作系统中的所有内容在主机上以文件形式存在，所以又具有可携带性和可迁移性。最值得关注的是 VMware 强大的网络功能，可以在一台计算机上建立一个局域网，这个网络的行为与真实的网络完全一致，而且不用担心虚拟网卡和虚拟交换机会损坏。这样，就可以抛开真实网络中各种琐碎的硬件冲突的可能性，潜下心来通过虚拟网络研究物理网络的核心逻辑。

VMware 具有如下主要功能。

- 不需要分区或重开机就能在同一台 PC 上使用两种以上的操作系统。
- 完全隔离并且保护不同 OS 的操作环境以及所有安装在 OS 上面的应用软件和资料。
- 不同的 OS 之间还能互动操作，包括网络、外设、文件分享以及复制、粘贴功能。
- 有复原（Undo）功能。
- 能够设定并且随时修改操作系统的操作环境，如内存、磁盘空间、设备等。

VMware 软件还具有如下的特殊功能。

- Snapshots（快照）功能。在 VMware 虚拟机的运行过程中，能把虚拟机系统当前的运行状态保存下来，当需要恢复时可以立刻恢复到实验前的状态。
- 共享文件夹功能。此功能是把主机上的一个目录或者分区映射到虚拟机中作为一个共享文件夹来使用。
- 支持主机与虚拟机之间文件与文件夹的“拖—拉”操作。也就是说可以在主机与虚拟机之间，直接把一个或几个文件或文件夹用鼠标“拖—拉”操作进行复制。
- 网络设置更加方便。可以很方便地添加和删除一块虚拟网卡（VMnet2、VMnet3、…、VMnet9），也可以很方便地设置 VMware 内置的 DHCP 服务器的 TCP/IP 地址的作用域范围。

【实验环境】

1）一台装有 Windows XP SP2 系统的计算机。

2）虚拟机软件 VMware Workstation 6.0.0，可从中国虚拟化网站 http://www.vmware.cn 下载。

3）Windows XP Professional SP2 安装光盘或 ISO 文件。

【实验内容】

1）安装 VMware 虚拟机软件。

2）VMware 虚拟机中系统安装设置。

3）在 VMware 虚拟机中安装操作系统。

4）VMware 虚拟机的功能设置。

【实验步骤】

1. 安装 VMware 虚拟机软件

待安装 VMware 虚拟机软件的机器配置要求见表 1-1。

表 1-1　实验机器配置要求

硬　件	配　置
内存	256 MB 以上
CPU	Pentium 4　2.80 GHz
硬盘	2 GB 以上
网卡	10/100 Mbit/s
操作系统	Windows XP SP2

版本号为 VMware Workstation 6.0.0.45731 的安装步骤如下：

1）双击安装程序后，出现如图 1-2 所示的安装启动界面。接下来的几步均按照系统的默认选项设置。

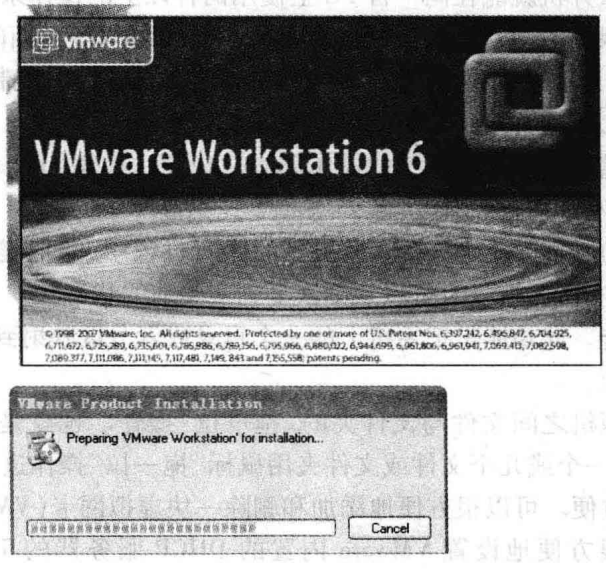


图 1-2　安装时的界面

2）安装结束前，系统提示输入用户名和 VMware 的注册号，输入正确后，出现安装完毕界面。

3）安装完毕后，需要按照系统提示重新启动计算机。重启计算机以后，打开 VMware 程序，主界面如图 1-3 所示。

2. VMware 虚拟机中系统安装配置

1）安装完虚拟机以后，就如同组装了一台新的计算机，因而需要安装操作系统。在图 1-3所示界面选择菜单“File”→“New Virtual Machine”选项。这时，出现“New Virtual Machine Wizad”（新建虚拟机向导界面）。

2）单击向导界面的“下一步”按钮，出现安装配置界面，如图 1-4 所示。

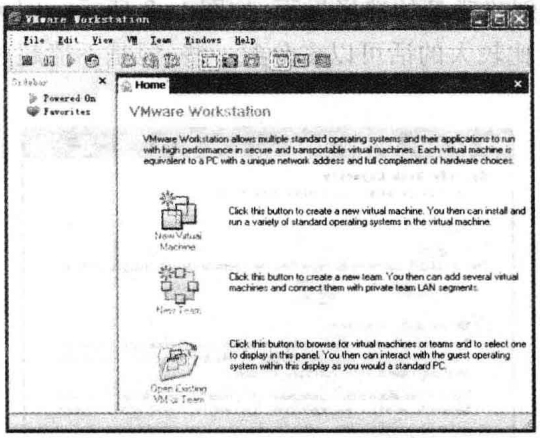


图 1-3　VMware 主界面

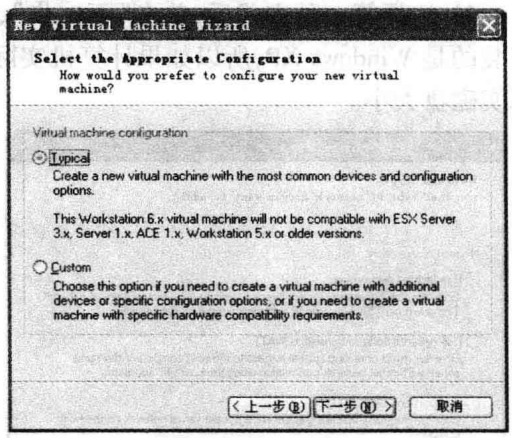


图 1-4　安装选项

这里有两种选择，选择“Typical”（典型）安装。单击“下一步”按钮，进入选择操作系统界面，设置要安装的操作系统类型及该操作系统的版本，如图 1-5 所示。单击“下一步”按钮进入安装目录选择界面，如图 1-6 所示。安装目录界面有两个文本框，上面的文本框是系统的名称，选择默认值就可以，下面的文本框需要选择虚拟操作系统安装的目录。

请注意，VMware 软件不用改写硬盘分区，而是在一个文件中虚拟出一个分区来。

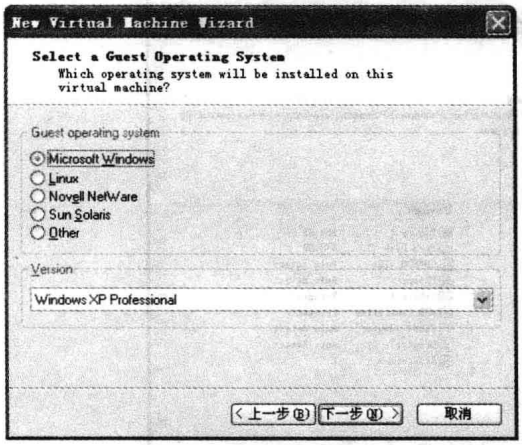


图 1-5　选择安装的操作系统

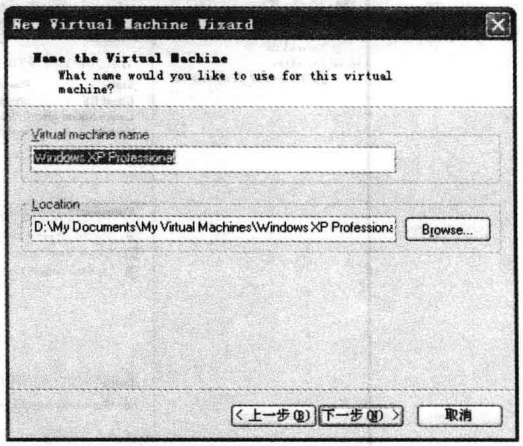


图 1-6　选择安装目录

3）选择好以后，单击“下一步”按钮，进入网络连接方式选择界面，如图 1-7 所示。

VMWare 常用的是以下几种连网方式。

- Use bridged networking(使用网桥连接)。本实验配置即采用此法。虚拟机操作系统的 IP 地址可设置成与宿主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。
- Use network address translatio(使用网络地址转换 NAT)。
- Use host-only networking(仅使用主机网络)。
- Do not use a network connection(不使用网络连接)。

4）选择第一种方式后，单击“下一步”，出现创建磁盘的选择界面，如图 1-8 所示。因为安装的是 Windows XP，所以如果计算机实际硬盘比较大的话可以多分配一些，但是不能超过真实磁盘大小。

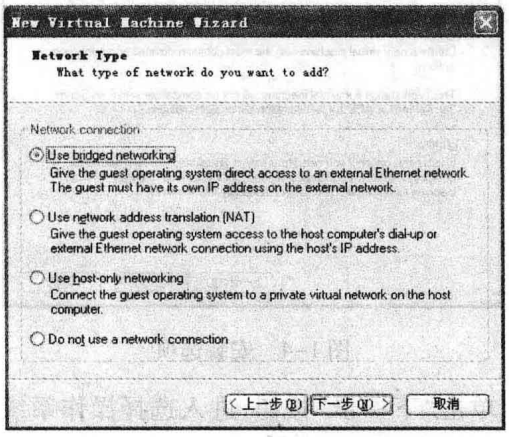


图 1-7　网络连接方式选择

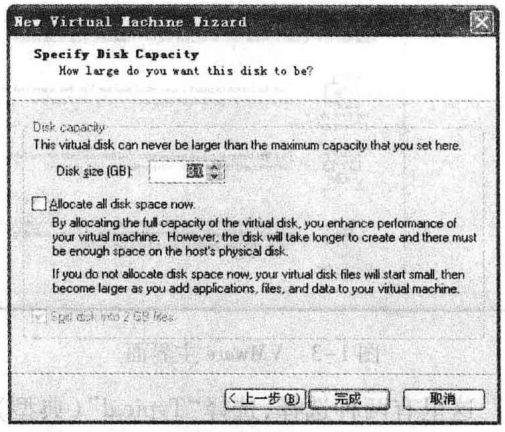


图 1-8　虚拟磁盘分配

5）单击“完成”按钮，可以在 VMware 的主界面中出现刚刚配置的虚拟机，如图 1-9 所示。

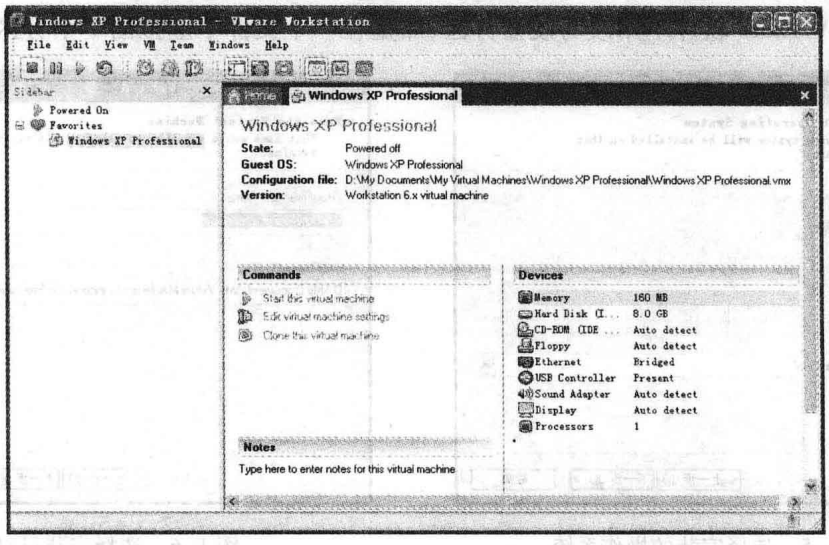


图 1-9　配置好的虚拟机

3. 在 VMware 虚拟机中安装操作系统

1）双击图 1-9 中的 CD-ROM，可设置虚拟机的光驱是映射到物理光驱还是 ISO 文件，如图 1-10 所示。

2）单击图 1-9 中的绿色启动按钮（Start this virtual machine）来启动虚拟机。VMware 的启动相当于一台独立的计算机，如图 1-11 所示。

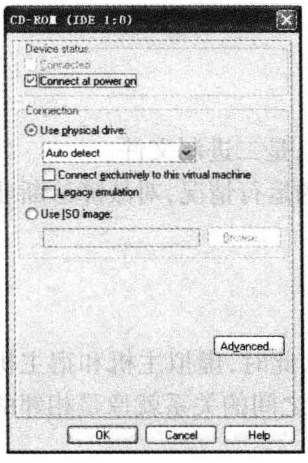


图 1-10　虚拟光驱设置

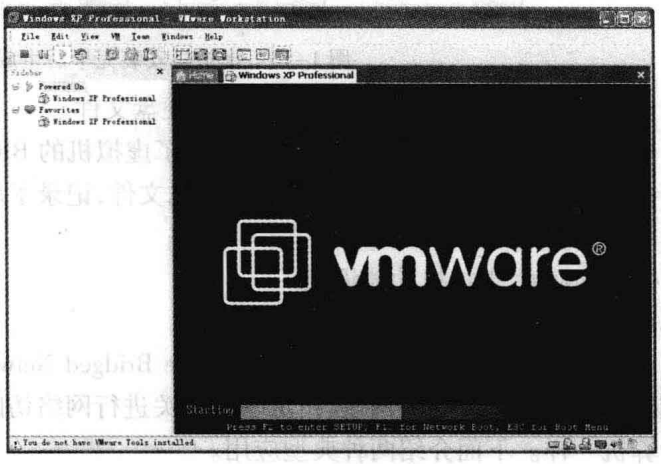


图 1-11　虚拟机启动界面

3）安装 Windows XP Professional。安装过程如同在实际主机上。安装成功后，系统启动界面如图 1-12 所示。

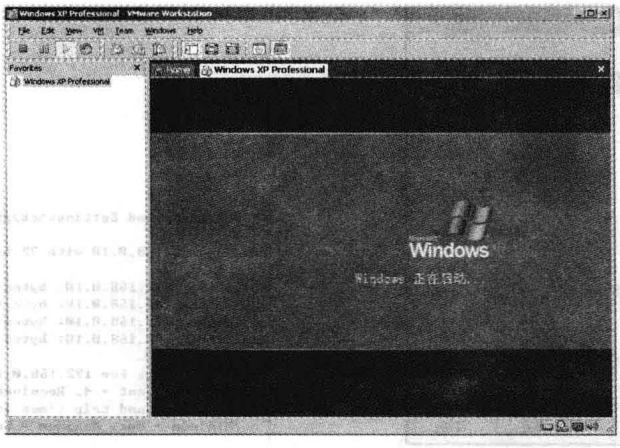


图 1-12　虚拟机中的系统启动

4）定位到先前指定的存放配置文件的宿主机目录（本实验为 d:\My Documents\My Virtual Machines\Windows XP Professional\），可以看到以下文件，如图 1-13 所示。

- Windows XP Professional. vmx：VMware 用以标识一台虚拟机的配置文件，它是个文本文件，向导建立虚拟机的过程就是创建这个文件的过程。
- Windows XP Professional. vmxf：虚拟机补充配置文件，在虚拟机被移除后，它将保存下来。

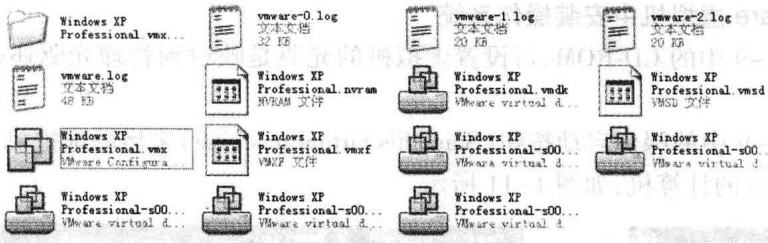


图 1-13　虚拟机安装完毕后生成的文件

- Windows XP Professional. vmdk：虚拟硬盘文件。
- Windows XP Professional. nvram：存储了虚拟机的 BIOS 信息，是二进制文件。
- vmware. log、vmware-0. log：虚拟机日志文件，记录了虚拟机的运行情况，对故障诊断非常有用。

4. VMware 虚拟机功能设置

（1）网络设置

由于本实验连网采用的是网桥方式（Use Bridged Networking），此时，虚拟主机和宿主机的真实网卡可以设置在一个网段、指定一个网关进行网络访问，两者之间的关系就像是相邻的两台计算机一样。下面介绍两种典型应用。

1）宿主机与虚拟主机组网。宿主机中的网络配置如图 1-14 所示，IP 地址为 192. 168. 0. 1，子网掩码为 255. 255. 255. 0。类似地，虚拟主机中的网络配置 IP 地址为 192. 168. 0. 10，子网掩码为 255. 255. 255. 0。设置完成后，可在宿主机的命令提示符下通过 Ping 命令测试连通性，如图1-15 所示。

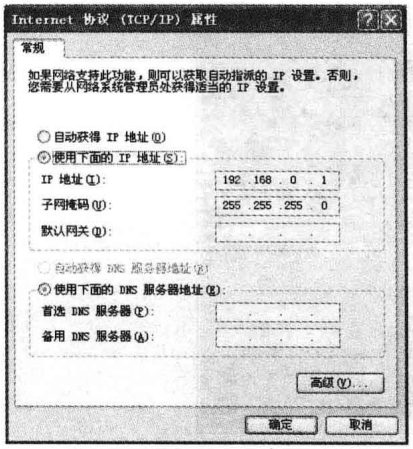


图 1-14　宿主机中的网络配置

```
C:\Documents and Settings\cb>ping 192.168.0.10

Pinging 192.168.0.10 with 32 bytes of data:

Reply from 192.168.0.10: bytes=32 time=6ms TTL=128
Reply from 192.168.0.10: bytes=32 time<1ms TTL=128
Reply from 192.168.0.10: bytes=32 time<1ms TTL=128
Reply from 192.168.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

图 1-15　通过 Ping 命令测试连通性

2）宿主机与虚拟主机共享联入因特网。局域网中的宿主机及其上的虚拟主机的网络配置如表 1 -2 所示。

表 1-2　网络配置

	IP 地址	子网掩码	默认网关	DNS 服务器
宿主机	202. 119. 111. 131	255. 255. 255. 0	202. 119. 111. 1	202. 119. 104. 10
虚拟机	202. 119. 111. 133	255. 255. 255. 0	202. 119. 111. 1	202. 119. 104. 10