高等学校计算机科学与技术教材

网络安全实验教程

COMPUTER Science and Technology

□ 程光 杨望 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

网络安全实验教程

程 光 杨 望 编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书是针对高等学校学生的网络安全教学而编写的实验教程，其目的是使得学生掌握使用各种安全工具以保护其主机与网络的安全，提高学生对网络的攻防能力。全书共分 12 章，每章包括若干个安全实验，每个实验分别介绍实验原理、环境设置、实验指南和思考与练习等 4 个部分内容，本书基本覆盖了当前网络安全实验的主要分支和领域，主要包括以下内容：建立安全实验环境，安装和使用扫描器和侦听工具，口令破解，中间人攻击，欺骗攻击，拒绝服务攻击，配置防火墙，Rootkits 技术，木马创建后门的过程，蠕虫病毒工作过程，僵尸网络的原理和方法，Web 应用程序的攻击和防护等。本书适合作为计算机科学与技术、网络和信息安全相关专业本科生和研究生的网络安全相关课程配套教材，还为自学网络安全的读者提供非常理想的指导，也适合企、事业单位的网络和系统管理维护人员作为工具书。

图书在版编目（CIP）数据

网络安全实验教程 / 程光，杨望编著. —北京：清华大学出版社；北京交通大学出版社，2013.1

（高等学校计算机科学与技术教材）

ISBN 978-7-5121-1298-8

Ⅰ. ①网… Ⅱ. ①程… ②杨… Ⅲ. ①计算机网络-安全技术-高等学校-教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 287721 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://www.bjtup.com.cn

印 刷 者：北京时代华都印刷有限公司

经　　销：全国新华书店

开　　本：185×260　印张：11.75　字数：298 千字

版　　次：2013 年 1 月第 1 版　2013 年 1 月第 1 次印刷

书　　号：ISBN 978-7-5121-1298-8/TP・718

印　　数：1～3 000 册　定价：25.00 元

前　言

随着计算机网络应用的普及和深入，网络技术的应用越来越广泛地渗透到社会发展的各个领域。在极大推动生产力发展的同时，人们对计算机网络的依赖程度也日益提高，黑客攻击、泄密等网络安全问题也变得越来越严重，而网络系统的安全一旦受到破坏，不仅会导致严重的社会混乱，也会带来巨大的经济损失。因此，确保网络安全已经成为世人关注的社会问题，网络安全已成为计算机科学与技术的热点问题，网络安全专业也受到了社会各界的普遍关注。

网络安全是由计算机科学与技术、数学和通信工程等学科交叉而成的一门综合性学科，其理论与实践结合得相当紧密；同时，网络安全也是一门实践性很强的课程，主要研究攻击与防御。实验教学是学生实践活动中的一个重要的环节，本书是针对网络安全实验的特点，将理论知识的教学与实践教学相结合，以培养学生分析问题、解决问题的能力和专业实践能力。学生通过参与实验，可以更好地巩固网络安全理论知识，增强感性认识，提高解决网络安全问题的能力。

考虑到高等学校学生的实际情况，本书涉及的 39 个实验基本覆盖了当前网络安全的主要分支和主要理论。这些实验是按照由浅到深、由易到难的顺序排列的。教师可以有选择性地给学生布置，也可以在本书实验的基础上进行扩展。本书中的每个实验都由实验原理、环境设置、实验指南和思考与练习等 4 个部分组成。通过本书的教学使得学生掌握使用各种安全工具以保护其主机与网络的安全，提高学生对网络的攻防能力。本书由东南大学计算机科学与工程学院、CERNET 华东(北)地区网络中心的教师组织编写。

本书共 12 章。

第 1 章介绍安全实验环境。网络安全实验往往需要由多台计算机构成的网络实验环境，但是在现实中由于各种原因常常难以拥有这样的网络环境。第 1 章介绍的是 VM 虚拟机、PlanetLab 平台网络环境，以及如何在虚拟构建的网络平台中搭建一个搭建 Chord 系统，为普通用户提供进行网络安全实验所需要的网络环境。

侦听与扫描是网络安全攻击和防护中经常要用到的两种技术，在网络攻击中利用它们可以准确地寻找攻击的目标，获取有用信息、及时发现安全漏洞。第 2 章介绍侦听工具 Wireshark 和扫描工具 Nmap 的实验举例。

口令提供了最基本的安全认证方式，第 3 章介绍进行各类系统的猜测攻击、系统攻击、网络攻击和后门攻击等 4 种口令破解的方法。

中间人攻击是一种“间接”的入侵攻击，第 4 章分别介绍如何通过 ARP 协议、DNS 协议及一些扩展的手段来实现不同层次的中间人攻击。

第 5 章分别从 MAC 层、IP 层和应用层介绍欺骗攻击的方法。

第 6 章通过具体 TCP SYN Flood 攻击实验演示拒绝服务攻击，并说明在实际工作中知道如何防范拒绝服务攻击，维护网络的正常运行。

第 7 章过单机防火墙的配置和使用 Iptables 实现 NAT 服务等具体实验说明 Iptables 配置防火墙的各种规则。

Rootkits 能在操作系统中隐藏恶意程序，第 8 章介绍 Rootkits 实验的基本方法，并介绍如何对 Rootkits 进行检测。

后门是指那些绕过安全性控制而获取对程序或系统访问权的程序方法，第 9 章介绍产生后门的方法和实验，以及对后门进行检测的方法。

蠕虫病毒能传播自身功能的拷贝或自身的某些部分到其他的计算机系统中，第 10 章介绍蠕虫病毒的原理及具体的实验演示，重点掌握蠕虫病毒的传播感染方式，以便知道如何做好蠕虫病毒的防御工作，减少蠕虫病毒对主机的侵害。

僵尸网络是指采用一种或多种传播手段，将大量主机感染僵尸程序的病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络，第 11 章介绍僵尸网络的原理及其产生方法，并介绍如何进行僵尸网络的检测。

Web 是目前最常见的网络应用，第 12 章介绍 Web 安全的原理，并通过 SQL 注入、跨站脚本攻击、网页挂马等具体的实验操作，以便学生掌握几个常见攻击的原理和过程，以做好 Web 安全工作。

本书的部分实验在东南大学本科生和研究生的计算机网络及网络安全实验教学中得到成功运用。在编写本书的过程中，臧家宁、张杰、马永等研究生参与了本书中相关实验的编写工作。本书作者长期担任东南大学“计算机网络安全”、“计算机网络”等本科生和研究生的教学工作，同时还参加了 CERNET 华东（北）地区网络中心的网络管理和安全维护工作，具有丰富的网络安全方向的教学和实践经验。

由于作者能力和水平所限，时间较仓促，书中仍然难免有错误和疏漏的地方，衷心期望有关专家和同仁，特别是使用本书的教师、学生能毫不保留地提出所发现的问题和改进建议，与我们一起讨论。

编　者

2012 年 12 月于东南大学九龙湖

目　录

第 1 章　安全实验环境

网络安全实验往往需要由多台计算机构成的网络实验环境，但是在现实中由于各种原因常常难以拥有这样的网络环境。本章介绍两种网络环境可以为普通用户提供进行网络安全实验所需要的网络环境。一种方法是将一台计算机虚拟成多台计算机所构成的网络环境，如在计算机上安装 VMware 软件，然后在虚拟机上安装操作系统，从而建设一个多台虚拟机所构成的网络实验环境，虚拟机之间可以通过虚拟网卡和实际的操作系统进行通信。另一种方法是基于真实的大规模网络实验环境。为了建设能够给计算机网络研究人员使用的大规模网络试验环境，国际上已经有很多先驱的工作和成功的经验，如 Planetlab 这样的大规模网络实验环境。

1.1　VM 虚拟机

1.1.1　实验原理

虚拟机是支持多操作系统并行在单个物理服务器上的一种系统，它提供更加有效的底层硬件使用。在虚拟机中，中央处理器芯片从系统其他部分划分出一段存储区域，操作系统和应用程序运行在“保护模式”环境下。如果在某虚拟机中出现程序冻结现象，并不会影响运行在虚拟机外的程序操作和操作系统的正常工作。在真实计算机系统中，操作系统组成中的设备驱动控制硬件资源，负责将系统指令转化成特定设备控制语言。在假设设备所有权独立的情况下形成驱动，这就使得单个计算机上不能并发运行多个操作系统。虚拟机则包含了克服该局限性的技术。虚拟化过程引入了低层设备资源重定向交互作用，而不会影响高层应用层。通过虚拟机，客户可以在单个计算机上并发运行多个操作系统。每个虚拟机由一组虚拟化设备构成，其中每个虚拟机都有对应的虚拟硬件。客户操作系统和应用程序可以运行在虚拟机上，而不需要提供任何交互作用的网络适配器的支持。虚拟服务器只是物理以太网中的一种软件仿真设备。

在一台计算机的部分硬盘和内存中虚拟出若干台机器，每台机器可以运行单独地操作系统而互不干扰，这些“新”机器各自拥有自己独立的 CMOS、硬盘和操作系统等软/硬件资源，用户可以像使用普通机器一样对这些虚拟机进行分区、格式化、安装系统和应用软件等操作，还可以将这些虚拟机连成一个网络。在虚拟系统崩溃之后可将其直接删除，而不会影响本机系统，同样本机系统崩溃后也不会影响虚拟系统，可以下次重装后再加入以前做的虚拟系统。同时，可以在 Windows 和 Linux 主机平台上运行虚拟计算机软件。虚拟机软件不需要重开机，就能在同一台计算机使用多个操作系统，不但方便，而且安全。虚拟机在学习技术方面能够发挥很大的作用。虚拟操作系统模式虚拟化解决方案同样能够满足一系列的需求：安全隔离、计算机资源的灵活性和控制、硬件抽象操作及最终高效、强大的管理功能。

VMware 提供了三种工作模式，它们是桥接模式（bridged）、网络地址转换模式（NAT）和主机模式（host-only）。

在 bridged 模式中，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 bridged 模式下，用户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 bridged 模式的虚拟系统和宿主机器的关系，就像连接在同一个集线器上的两台计算机，只需要为虚拟系统配置 IP 地址和子网掩码，就可以让它们相互通信。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 bridged 模式。

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，即使用 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 虚拟网络的 DHCP 服务器提供，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。

在网络调试环境中，可以采用 host-only 模式将真实环境和虚拟环境隔离开，在 host-only 模式中，所有的虚拟系统是可以相互通信的，但虚拟系统和真实的网络是被隔离开的。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；虚拟系统的 TCP/IP 配置信息（如 IP 地址、网关地址、DNS 服务器等），可以由 VMnet1 虚拟网络的 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）服务器来动态分配。

以上所提到的 NAT 模式下的 VMnet8 虚拟网络，host-only 模式下的 VMnet1 虚拟网络，以及 bridged 模式下的 VMnet0 虚拟网络，都是由 VMware 虚拟机自动配置而生成的，不需要用户自行设置。VMnet8 和 VMnet1 提供 DHCP 服务，VMnet0 虚拟网络则不提供 DHCP 服务。

1.1.2 环境设置

本实验采用一台 HP 服务器进行虚拟机配置，服务器硬件配置如下。

CPU：Intel XEON E5506（2.13GHz）。

内存：8GB。

硬盘：250GB + 1TB。

网卡：主板集成 1000Mbps。

采用的软件有：VMware-workstation-6.0.2-59824.i386.rpm，Linux 操作系统采用 fedora core 14 32 的镜像文件 Fedora-14-i386-DVD.iso。

1.1.3 实验指南

1. 安装 VMware

将 VMware-workstation-6.0.2-59824.i386.rpm 复制到 Fedora 系统相关目录，在命令行输

入“rpm –ivh VMware-workstation-6.0.2-59824.i386.rpm”，如图 1-1 所示。

```
[root@localhost ~]# rpm -ivh VMware-workstation-6.0.2-59824.i386.rpm
Preparing...                ########################################### [100%]
   1:VMwareWorkstation      ########################################### [100%]
[root@localhost ~]#
```

图 1-1　解压缩软件包

在命令行中输入 VMware，查看软件信息，如图 1-2 所示。

```
[root@localhost ~]# vmware
vmware is installed, but it has not been (correctly) configured
for this system. To (re-)configure it, invoke the following command:
/usr/bin/vmware-config.pl.

[root@localhost ~]#
```

图 1-2　显示软件信息

配置 VMware，在命令行输入“/usr/bin/VMware-config.pl”，如图 1-3 所示。

```
[root@localhost ~]# /usr/bin/vmware-config.pl
Making sure services for VMware Workstation are stopped.

Stopping VMware services:
   Virtual machine monitor                                    [确定]

Configuring fallback GTK+ 2.4 libraries.

In which directory do you want to install the theme icons?
[/usr/share/icons]
```

图 1-3　配置 VMware

对于上述类似的提问，都采取默认的形式，直接按回车键后继续，最后出现如图 1-4 所示的提示，说明 VMware 已经配置成功。

```
The configuration of VMware Workstation 6.0.2 build-59824 for Linux for this
running kernel completed successfully.

You can now run VMware Workstation by invoking the following command:
"/usr/bin/vmware".

Enjoy,

--the VMware team
```

图 1-4　VMware 配置成功

启动 VMware 工作站有两种方法。第一种方法如图 1-5 所示，单击桌面上的应用程序图标，在弹出的菜单中依次选择“系统工具”→“VMware Workstation”即可。

第二种方法是通过命令行启动，即在命令行输入#Vmware。启动后的 VMware 工作站图形界面如图 1-6 所示。

2．安装 Windows XP 虚拟机

启动 VMware 工作站后，单击“Create a new virtual machine”，出现创建新的虚拟机界面，

如图 1-7 所示。

图 1-5 以菜单方式启动 VMware 工作站

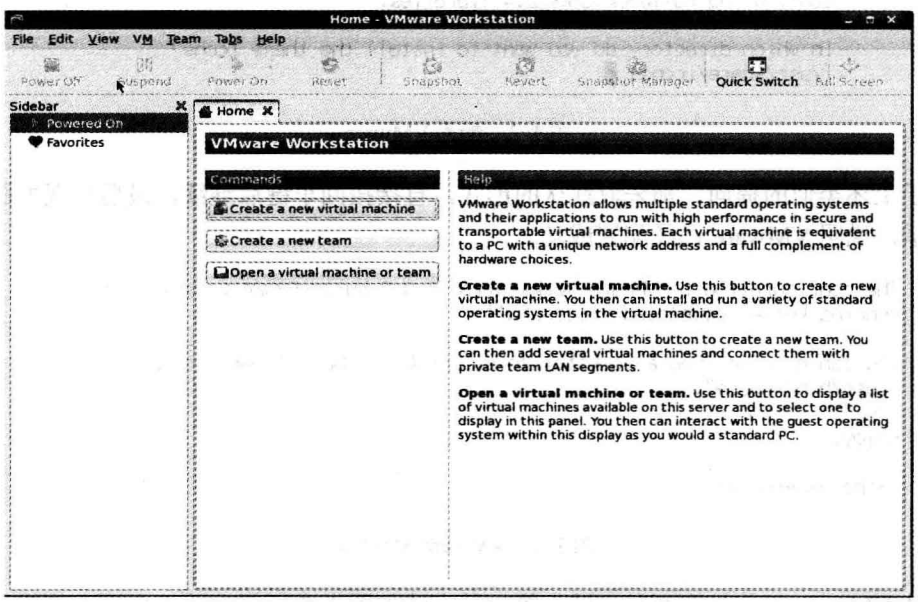

图 1-6 VMware Workstaion

单击“Next”，接着选择“Typical”安装，然后单击“Next”，出现选择操作系统的界面，如图 1-8 所示。

在“Version”下拉列表框中选择安装“Windows XP professional”，单击“Next”进入为

所安装的虚拟机命名界面。接着单击“Next”进入选择网络连接模式界面，默认选择为使用桥接模式（Use bridged networking），如图 1-9 所示。

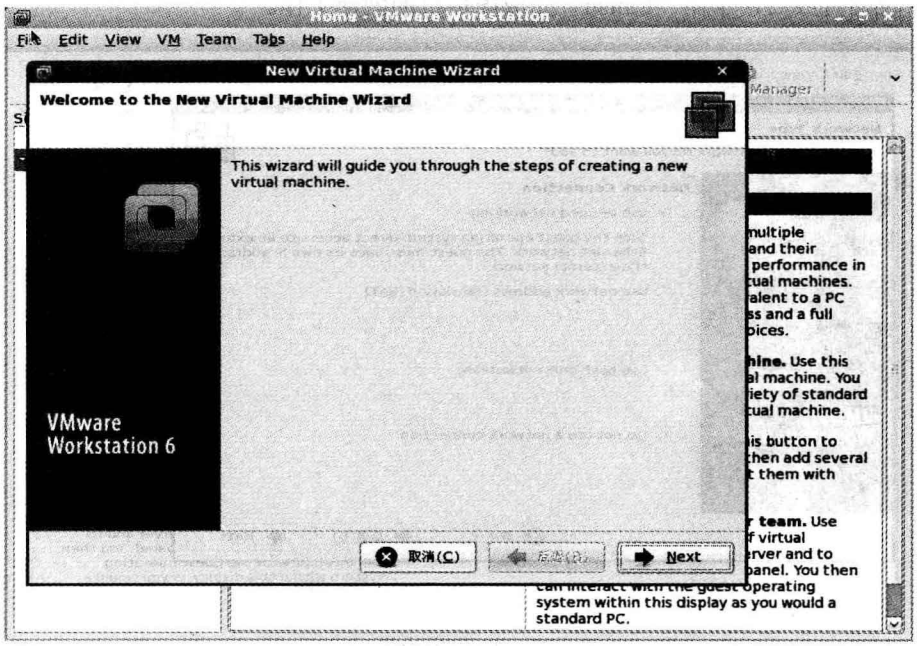

图 1-7　创建新的虚拟机

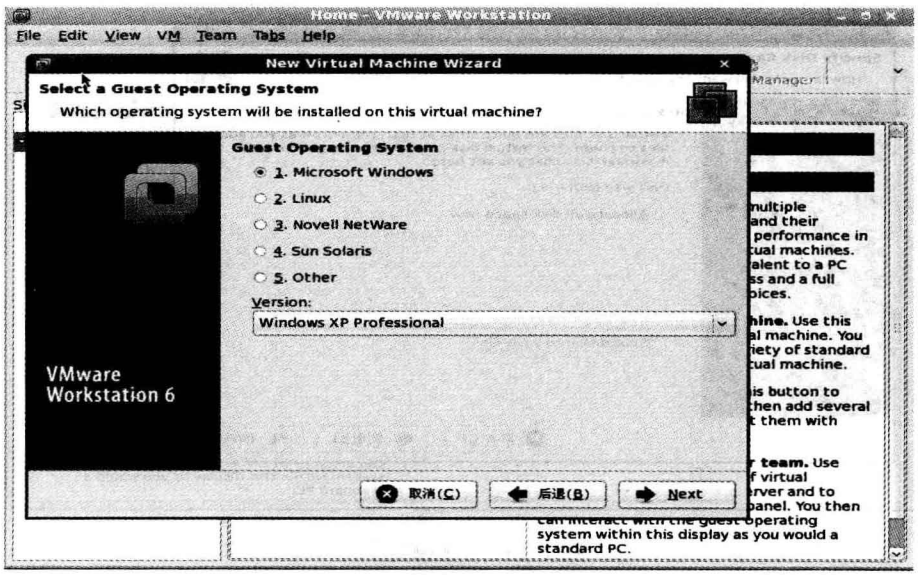

图 1-8　选择操作系统

图 1-10 所示是为虚拟机分配磁盘空间大小的界面，如果选择“Allocate all disk space now”选项，表示将按照“Disk Size”后面指定的大小、立刻从主机硬盘分配所有空间用于虚拟机硬盘。如果虚拟机硬盘保存在 FAT32 分区或者 FAT 分区中，则选择“Split disk into 2GB

files”，这样，每 2 GB 的虚拟硬盘空间将会在主机上创建一个文件。例如，图 1-10 所示为创建 8 GB 虚拟硬盘，这样会在主机上创建 4 个文件，如果是 250 GB 的虚拟硬盘，则创建 125 个文件。设置完成后，单击“Finish”完成虚拟机的创建工作。

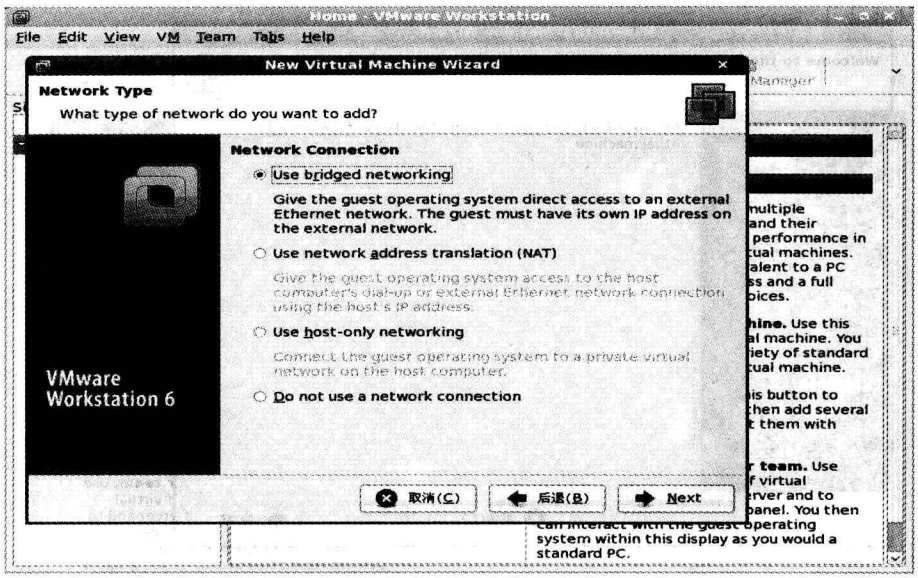

图 1-9 选择网络连接模式

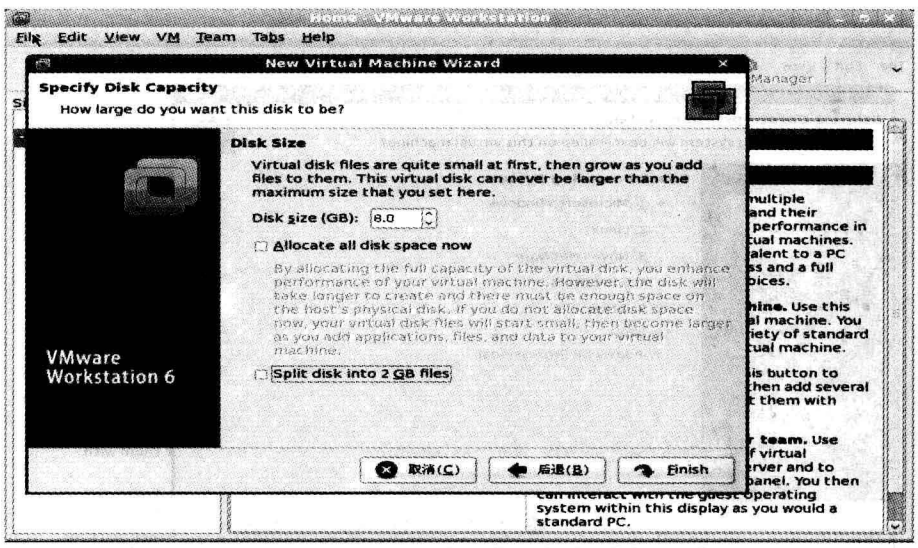

图 1-10 分配磁盘空间

接下来安装 Windows XP 虚拟机系统。单击虚拟机主界面中的“CD-ROM”，弹出虚拟机设置界面，如图 1-11 所示。

选择“Use ISO image”从光盘启动系统，然后单击“Browse”，从出现的对话框中选择所要安装的 Windows XP 系统光盘镜像，后缀名为“.iso”，单击“打开”，保存后重新退回到

如图 1-12 所示的虚拟机主界面。

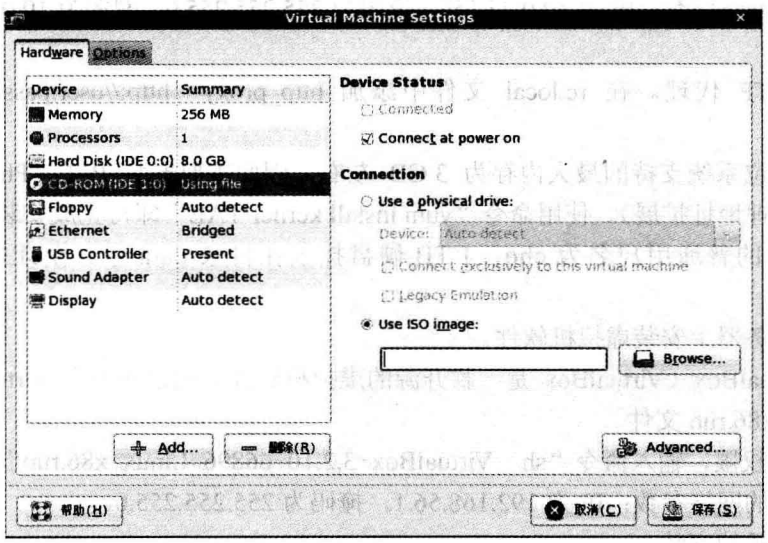

图 1-11　设置虚拟机

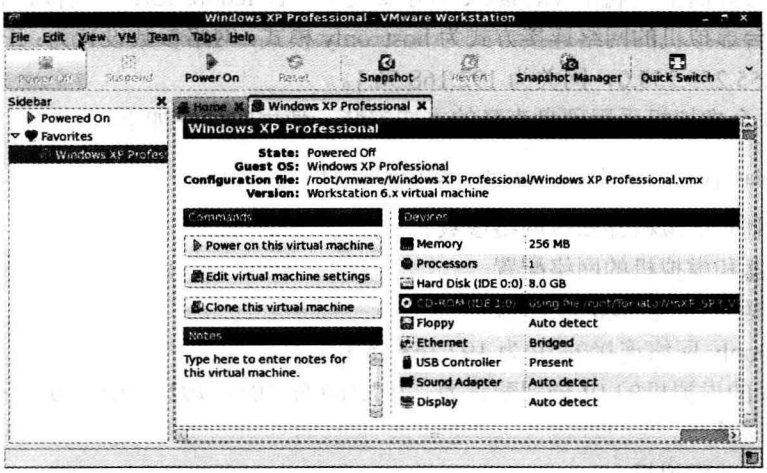

图 1-12　虚拟机主界面

单击“Power on this virtual machine”开始虚拟机系统的安装工作。虚拟机系统的安装过程与实际操作系统的安装过程无任何区别，在此不再详述，安装完成后可以启动虚拟机。

3．安装 Linux 虚拟机

创建 Linux 虚拟机的步骤与创建 Windows 虚拟机类似，下面给出一个具体 Linux 虚拟机安装配置实例，该实例是在一个 HP 服务器上配置 16 台虚拟机。设置参数和主要步骤如下。

（1）在服务器上安装操作系统

下载 fedora core 14 32 位镜像文件 Fedora-14-i386-DVD.iso，并刻录。