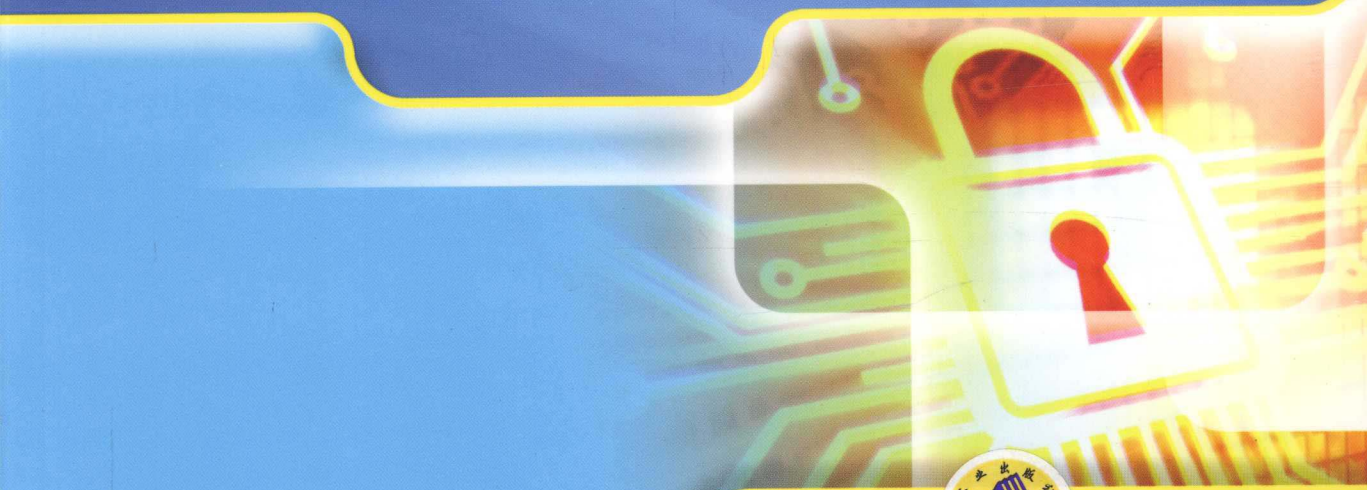
高等院校规划教材·计算机系列

网络安全防范项目教程

主　编　骆耀祖　杨　波
副主编　骆珍仪　刘东远　葛　斌



电子课件下载网址 www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

·计算机系列

网络安全防范项目教程

主　编　骆耀祖　杨　波
副主编　骆珍仪　刘东远　葛　斌
参　编　李思思

机械工业出版社

“网络安全技术”是信息类专业的专业必修课，也是电子商务等相关专业的重要专业课。本书通过项目式的讲授，介绍计算机网络安全方面的知识，培养学生对网络安全协议的分析能力，通过实战进一步加深对网络安全协议工作原理的掌握。

本书按教与学的普遍规律精心设计每个项目的内容，在内容组织上注意与新技术的衔接，编写上注重对学生实践能力和探究能力的培养。本书内容取材新颖、系统、简练，文笔流畅，重点突出，实践性强，是一本将网络安全技术众多成果与最新进展科学地组合在一起的优秀实践教材。

本书适合作为高等院校应用型本科及高职高专的计算机科学技术、电子信息类专业的“网络安全协议”和“信息安全技术”课程的教材，也可供广大工程技术人员和网络技术爱好者参考。

本书配套授课电子课件，需要的教师可登录 www. cmpedu. com 免费注册、审核通过后下载，或联系编辑索取（QQ：1239258369，电话：010 - 88379739）。

图书在版编目(CIP)数据

网络安全防范项目教程/骆耀祖，杨波主编．—北京：机械工业出版社，2014. 9
高等院校规划教材·计算机系列
ISBN 978-7-111-48532-2

Ⅰ. ①网… Ⅱ. ①骆… 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(2014)第 265964 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：鹿 征
责任校对：张艳霞
责任印制：刘 岚

北京诚信伟业印刷有限公司印刷

2015 年 1 月第 1 版·第 1 次印刷
184mm × 260mm · 17 印张 · 420 千字
0001 - 3000 册
标准书号：ISBN 978-7-111-48532-2
定价：37. 80 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
服务咨询热线：(010)88379833
读者购书热线：(010)88379649

网络服务
机 工 官 网：www. cmpbook. com
机 工 官 博：weibo. com/cmp1952
教育服务网：www. cmpedu. com
金 书 网：www. golden - book. com

前　言

“网络安全技术”是信息类专业的专业必修课，也是电子商务等相关专业的重要专业课。本课程旨在培养学生对网络安全协议的分析能力，同时为后续专业课程的学习打下坚实的基础。本书的任务是通过项目式的讲授介绍计算机网络安全方面的知识，通过实战进一步加深对网络安全协议工作原理的掌握。

本书力求处理好下列三个方面的关系。

首先是课程内容的取舍。网络安全技术涉及的内容很多且发展很快，应该让学生在学习的过程中，对网络安全的主要概念有一个较清楚的理解。因此，本书涉及的内容基本覆盖了当前计算机网络安全的主要分支，从而使读者充分掌握计算机网络安全的基本概念与基本架构。

其次，采用易于搭建的实验环境。本书的实验项目大部分是基于容易搭建的虚拟机的实验环境。各高等院校的安全实验室的实验方式相似，但其硬件防火墙可能使用不同厂家的产品。考虑到学生的理解能力，本书使用的是微软的 ISA 软件防火墙。本书尽量利用微软动手实验室（Hands - on Lab）和开源软件，从而降低了实验开设过程中的成本。实验项目实用性和趣味性较强，学生容易见到实验结果，从而对网络安全的知识能有更进一步的了解。

第三，本书的任务是按由易到难的顺序设计的，教师可以根据学生的不同情况灵活布置。

本书以项目方式进行编写，分为 11 个项目。

项目 1 建立网络安全实验环境。介绍如何创建虚拟机系统工作平台，讨论了网络监听工具的安装使用方法。

项目 2 网络入侵与攻击技术简介。介绍计算机与网络资源的探测与扫描、模拟黑客攻击等基础知识。

项目 3 数据加密与数字签名。介绍数据加密技术，包括对称加密与非对称密钥技术，加密解密软件 PGP、电子签章等内容。

项目 4 网络规划与设备安全。介绍网络规划及方案设计、办公网络安全分析设计、交换机安全配置、路由器安全配置等内容。

项目 5 服务器操作系统安全设置。包括操作系统安全概述、Windows Server 2003 服务器安全设置等。

项目 6 数据库及应用服务器安全。包括 SQL Server 数据库安全规划、应用服务器安全设置、使用 SCW 配置 Web 服务器等内容。

项目 7 Web 应用程序安全。介绍 Web 应用面临的威胁及 WebGoat 实验环境，SQL 注入攻击，跨站攻击 XSS，跨站请求伪造 CSRF 等安全威胁与危害等。

项目 8 安全扫描和网络版杀毒。介绍使用局域网扫描器扫描局域网并进行分析、网络版杀毒软件和病毒防护技术等内容。

项目 9 和项目 10 讨论了 ISA Server 2006 防火墙的部署、配置及优化，ISA Server 入侵检

测及配置等。

项目11 网络安全协议及VPN技术。介绍了安全协议、Windows Server 2003远程桌面SSL认证配置、配置远程拨号VPN、配置L2TP/IPSEC的VPN等内容。

本书遵循了人们对网络安全的认识规律，也基本覆盖了网络安全课程要求的内容和知识单元。上述划分章节的方法将给出一个清晰的框架，有利于循序渐进地进行学习。

本书按教与学的普遍规律精心设计每个项目的内容，在内容组织上注意与新技术的衔接，编写上注重对学生实践能力和探究能力的培养。本书内容取材新颖、系统、简练，文笔流畅，重点突出，实践性强，是一本将网络安全技术众多成果与最新进展科学地组合在一起的优秀实践教材。

本书由广东财经大学华商学院骆耀祖和杨波任主编，韶关学院骆珍仪、刘东远与广州丛信科技咨询公司葛斌任副主编，广州华商职业学院李思思参加编写。骆耀祖编写了项目1、7，刘东远编写了项目4、5、6，骆珍仪编写了项目8、9、10，葛斌编写了项目2，杨波和李思思编写了项目3、11。最后由骆耀祖和杨波统稿。

本书的配套电子课件、实验素材和部分习题答案可在机械工业出版社网站上下载。

在本书的编写过程中，得到了广东财经大学华商学院教材出版基金的大力支持，特在此表示深深的谢意。我们也从很多站点和论坛上得到很多的知识和资源，谨向这些站点的所有者和参与者表示真诚的感谢！

由于编者的水平有限，书中错误和不妥之处，恳请广大读者批评指正。

编　者

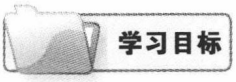
目　录

项目 1　建立网络安全实验环境

小方是计算机专业毕业的，平时上网行为很规矩，从不上那些乱七八糟的网站。小方格子里有自己专用的计算机，里面装着网络版的杀毒软件，定时更新病毒库，系统里装着360安全卫士，系统的漏洞、补丁等都堵上和补上了，这样在局域网还能不安全吗？其他同事们经常重装系统，而自己的系统重装的次数是少多了，至少自己认为是安全的。那么真的是这样吗？组建一个系统环境，用几款软件测试测试吧。

1）早就听说过局域网的安全性有问题，但如果不具备网络安全的系统环境的实验室，那么是不是就没有办法做网络安全实验了呢？组建一个最小的计算机网络系统环境，即有两个独立的操作系统，且这两个操作系统可以通过以太网进行通信，就可以解决这个大问题了。对于拿不准的东西，在虚拟机先运行，发现有问题的，开 Sniffer 或 CAIN 抓包看看。

2）对于网络、系统管理或安全技术人员来说，在对网络进行管理和维护的过程中，总会遇到这样或那样的问题。例如，网络传输性能为什么突然降低？为什么网页打不开，但QQ却能上线？为什么某些主机突然掉线？诸如此类的网络问题一个又一个地不断出现，都需要快速有效地去解决，以便能够尽量减少由于网络问题对企业正常业务造成的影响。因此，就需要一些工具来帮助快速有效地找出造成上述这些问题的原因。



1）掌握在 VPC 中安装虚拟系统的操作方法；学会设置、管理、迁移虚拟系统。

2）了解 Sniffer 软件的原理，掌握 Sniffer pro 的功能和作用。

3）通过用 CAIN 实施 ARP 欺骗，了解局域网的安全的严重性和迫切性。

1.1　创建虚拟机系统工作平台

1.1.1　任务概述

1. 任务目标

1）了解虚拟系统的工作原理；掌握在 VPC 中安装虚拟系统的操作方法。

2）能通过虚拟机软件管理、使用虚拟系统，在单个计算机中构建网络系统环境。

2. 学习内容

1）安装虚拟机控制台。

2）在虚拟机控制台中安装操作系统。

3）虚拟机参数设置。

3. 系统环境

- 硬件环境：机房基本设备，且各机器均能互联。
- 软件环境：Virtual PC 2007、Windows 2003 光盘镜像。

1.1.2 虚拟机介绍

虚拟机是安全检测的有效工具。虚拟机可以在计算机中虚拟出另一台计算机，而且虚拟机和真实计算机相互独立。网络安全实验的系统环境一般都是先安装一个虚拟机，所有的软件都装在这个虚拟的系统里面，自己对自己进行测试、学习，然后再拿到局域网中进行实验，这样无论对别人还是自己都是负责任的。

为什么那些检测局域网安全性的软件不能直接安装在本地机器上呢？第一，这些软件很多会被杀毒软件当作病毒给杀掉；第二，如果打算直接拿这些软件来对别人的机器进行测试，无论是对别人还是对自己来说都太不负责任了。

比较著名的虚拟机软件有 VMware 和 Virtual PC，也有一些针对服务器的和开源的虚拟机。

1. 虚拟机控制台（Virtual PC Console）

这是一个虚拟机运行和管理环境，可以在其中创建任意多台虚拟机，并运行这些虚拟机。能够同时运行的虚拟机的数量及各自的配置（如内存大小等）取决于真实 PC 的配置。

（1）虚拟机文件（.vmc）

这是可以在虚拟机控制台上加载并管理的一台虚拟机的配置文件。虚拟机的内存、光驱、软驱、显示、串口、并口、鼠标等虚拟硬件可来自真实 PC。

（2）虚拟硬盘（.vhd）

虚拟硬盘是虚拟机可以加以配置并用来安装运行操作系统、安装运行应用软件、存储数据的虚拟磁盘，是真实 PC 的硬盘中的一个或多个文件。

2. 虚拟机的作用

安装运行虚拟机，可以完成以下多项任务。

1）测试自己制作的光盘镜像是否可以成功安装。

2）测试各类操作系统的安装及破解激活方式方法的效果。

3）测试各类操作系统性能、设置和优化配置。

4）测试下载软件的安全性（是否有病毒木马和恶意插件）。

5）测试下载软件与系统及其他软件的兼容性。

6）对同类软件（如各种杀毒软件）进行性能上的横向比较。

3. 运行虚拟操作系统在硬件上的要求

运行虚拟操作系统在硬件上的要求主要是对内存的要求。在虚拟机上运行操作系统，要额外占用物理内存：比如，Windows XP 额外占用 128 MB；Windows Vista 额外占用 512 MB。也就是说，在保证实际系统正常运行所需内存的基础上，还必须具有虚拟系统所必需的内存富余，否则不能安装运行。

4. Virtual PC 的工作模式

Virtual PC 支持联网，它有两种工作模式：

（1）共享模式

在此模式下工作时，主机相当于一个代理服务器，以动态分配方式（DHCP）赋予虚拟机一个 IP 地址（即通常所说的内网 IP）。虚拟机通过共享主机 IP 地址（外网 IP）来访问外部网络，其工作原理和网吧普遍采用的局域网接入技术相同。

这种模式使用简便，几乎不用修改任何配置。但是 Virtual PC 没有独立的外网 IP，由此带来一个很大的缺点：外部网络（包括主机）无法直接访问虚拟机。如果仅仅是用 Virtual PC 上互联网，可以考虑此模式，这样可以避免黑客、病毒等对主机造成破坏。但因为主机访问不了 Virtual PC，显然无法实现单机组网。

（2）虚拟交换

该模式要求主机首先得具备一个有效的 IP 地址。如果是单机，最简单的方法就是装一块网卡，并且使用静态 IP 分配方式。另外，由于软件所限，主机必须安装 Windows 操作系统才能使用虚拟交换模式。

当运行在此模式下时，Virtual PC 相当于一个网桥，连接在主机和虚拟机之间，从而构成了一个虚拟局域网。Virtual PC 有独立的 IP 地址，支持网络邻居、TCP/IP 等协议。以前依赖网络才能完成的任务，现在完全可以在单机上进行。比如网络数据库编程，可以把主机作为数据库服务器，在 Virtual PC 上安装 Visual C + +或 Visual Basic 等工具进行客户端开发。

如果主机已经和外部网络相连，Virtual PC 还可以作为一个独立的节点，和外部网络相互直接访问。

1.1.3 在虚拟机安装 Windows Server 2003

1. 软件安装和中文环境构建

1）解压和安装 Virtual PC。将 Microsoft Virtual PC 中文精简版解压到一个文件夹，执行 install. cmd 注册组件。

2）启动 Virtual PC。在目录中选择“Virtual PC. exe”启动 Virtual PC 控制台，如图 1-1 所示。

3）修改界面语言。Microsoft Virtual PC 精简版内置了英文、简体和繁体 3 种语言。启动 Microsoft Virtual PC 后，在菜单栏中；选取“File”（文件）→“Options”（选项）→“Language”（语言）→“Simplified Chinese”（简体中文），如图 1-2、图 1-3 所示。然后重启 Virtual PC，软件就以中文界面显示，图 1-4 所示是 Virtual PC 中文控制台。

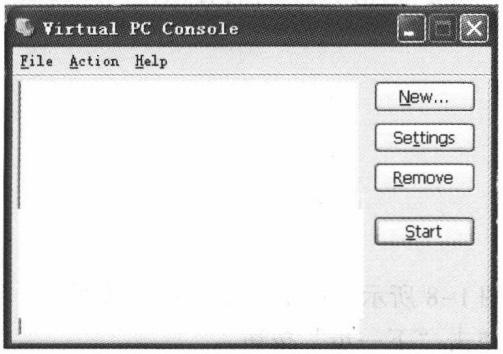


图 1-1 Virtual PC 控制台

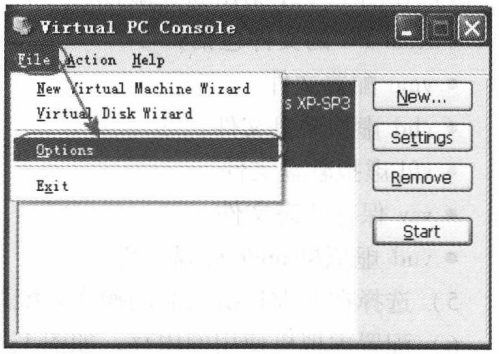


图 1-2 语言修改

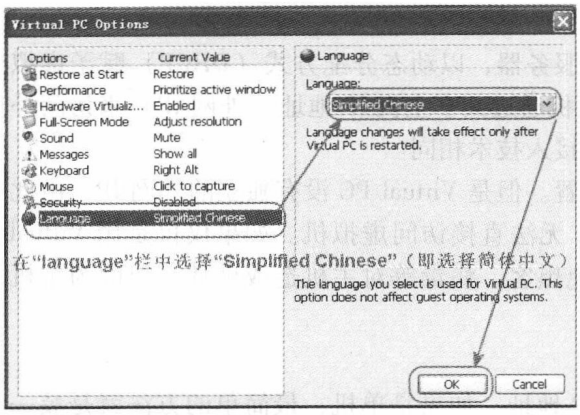


图 1-3　选择简体中文

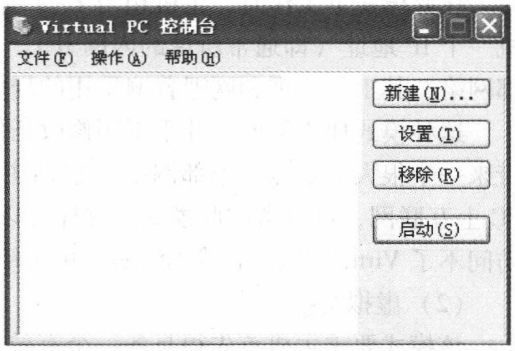


图 1-4　Virtual PC 中文控制台

2. 新建虚拟机

1）创建一台虚拟机。在控制台单击“新建”按钮，出现新建虚拟机向导界面，如图 1-5 所示。

2）在图 1-5 中单击“下一步”按钮，出现新建虚拟机选项界面，如图 1-6 所示。

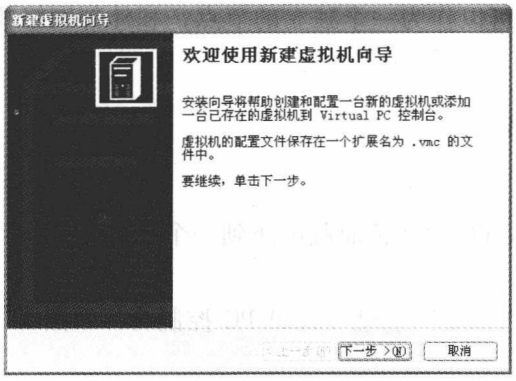


图 1-5　新建虚拟机向导欢迎界面

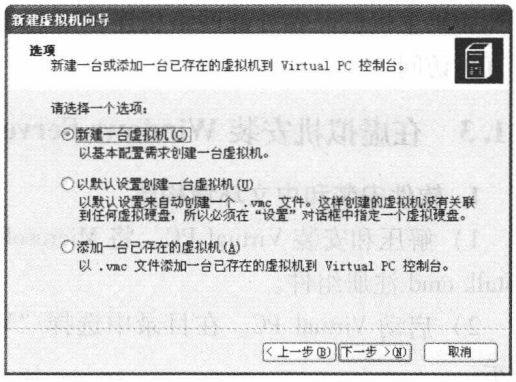


图 1-6　新建虚拟机选项

3）在图 1-5 中单击“下一步”按钮，在图 1-6 所示的界面中选中“新建一台虚拟机”单选钮。

4）在图 1-7 中给出新建虚拟机的名称和位置，新建虚拟机的文件将存储在该位置上。

Virtual PC 的文件包括：

- vmc 配置文件。
- vhd 虚拟硬盘文件。
- vfd 虚拟软盘文件。
- vsv 保存状态文件。
- vud 虚拟机 undo 磁盘文件。

5）选择在此虚拟机安装的操作系统版本，如图 1-8 所示。单击“下一步”按钮。

6）配置虚拟机使用的内存，如图 1-9 所示。单击“下一步”按钮。

7）设置虚拟硬盘，因为是新建的虚拟机，所以选中“新建虚拟硬盘”单选钮，如

图 1-10 所示。单击“下一步”按钮。

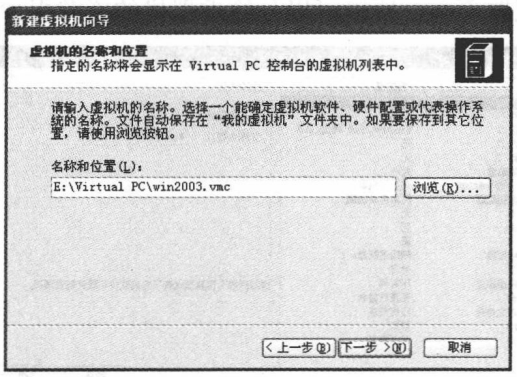


图 1-7　新建虚拟机的名称和位置

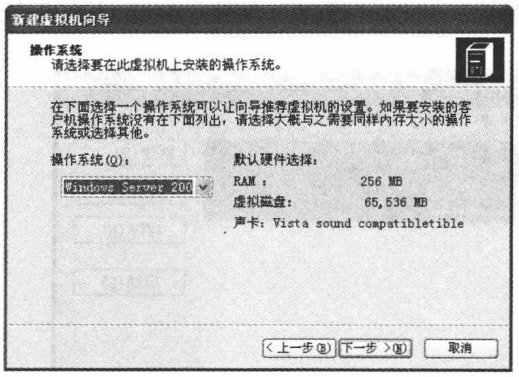


图 1-8　确定操作系统类型

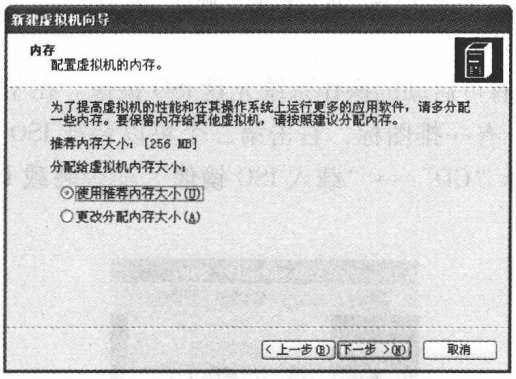


图 1-9　选择虚拟机使用的内存

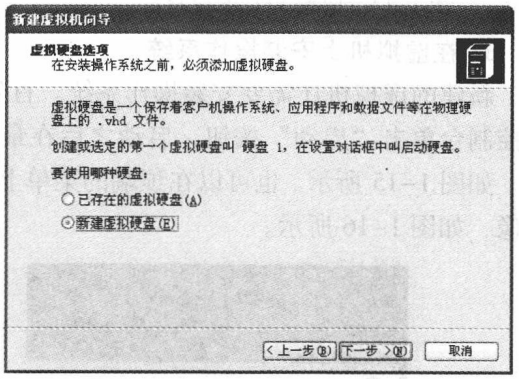


图 1-10　设置虚拟硬盘

如果只是安装单一操作系统，一般只需要建立一个虚拟硬盘。操作步骤：“新建”→“新建一台虚拟机”→“名称和位置”→“默认硬件选择”→“调整内存大小”→“新建虚拟硬盘”就可以了。如果要安装多个操作系统，需要建立多个系统虚拟硬盘，例如安装两个操作系统，就再“新建”一个，以此类推。

8）设置虚拟硬盘的位置，一般按默认设置就可以了，如图 1-11 所示。

9）完成新建虚拟机向导，如图 1-12 所示。单击“完成”按钮。回到 VPC 的控制台，可以见到虚拟机已经建立，如图 1-13 所示。

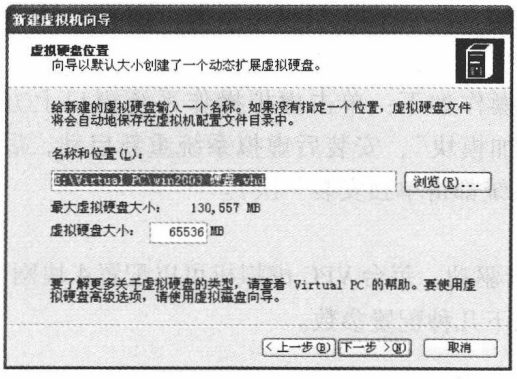


图 1-11　创建动态扩展虚拟硬盘的名称与位置

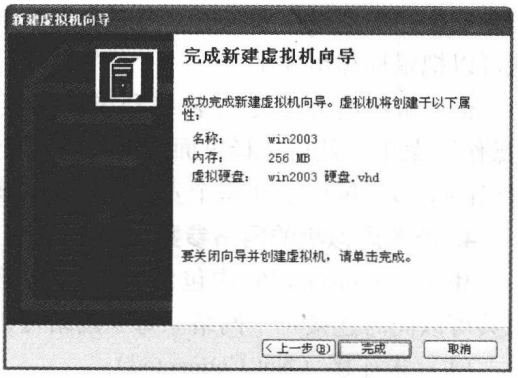


图 1-12　完成新建虚拟机向导

10）在 VPC 的控制台单击“设置”按钮，可以查看和修改虚拟机的配置。图 1-14 所示是虚拟机的“硬件”配置，由于计算机本来配置不高，所以可以分给虚拟机的资源很少。

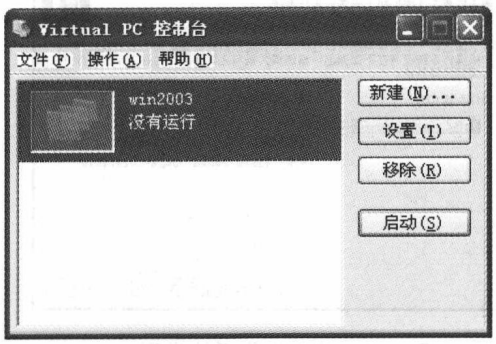


图 1-13　回到 VPC 的控制台

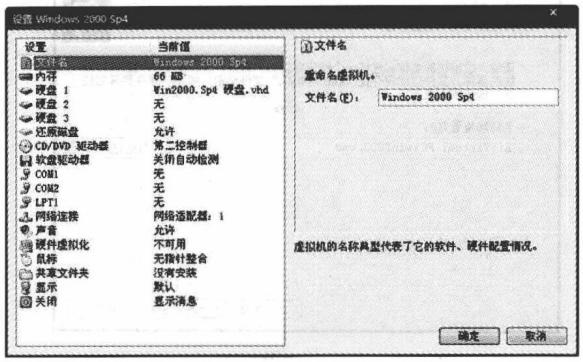


图 1-14　虚拟机的“硬件”配置

3. 在虚拟机上安装操作系统

新建的虚拟机还需要安装操作系统。首先要有可启动的操作系统光盘 ISO 镜像。在 VPC 的控制台单击“启动”按钮，启动之后在最底下有一排图标，右击第二个可以装载 ISO 镜像，如图 1-15 所示。也可以在顶端的菜单上选择“CD”→“载入 ISO 镜像”命令装载 ISO 镜像，如图 1-16 所示。

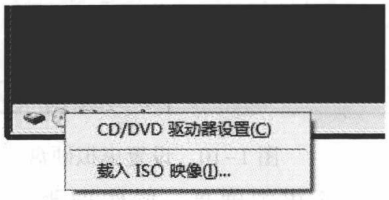


图 1-15　启动之后在最底下有一排图标

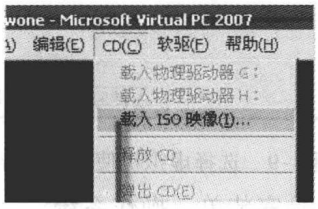


图 1-16　在菜单中载入 ISO 镜像

要安装操作系统，按照如下步骤进行操作：

1）启动/CD/载入光盘镜像/。

2）选择 ISO 镜像或物理驱动器。

3）选择 CD 镜像/关闭电源/启动，即进入操作系统安装界面。

4）安装 Windows Server 2003。

安装完虚拟操作系统后，有时会发现鼠标被“框”在虚拟机里出不来，按下〈Alt〉键就可以把鼠标移出来了。

彻底解决的办法是安装或升级附加模块，操作如下：单击虚拟操作系统窗口上方的“操作”菜单，然后选择里面的“安装或升级附加模块”，安装后虚拟系统重新启动，后就可以随意移动鼠标了（每个安装过的虚拟操作系统都得单独安装一次）。

4. 配置虚拟机的网络参数

Microsoft Virtual PC 中包含了网卡组件和声卡驱动。每台 VPC 虚拟机可以配置4 块网卡，总共可以同时连接 4 个网络。每个网络可以是以下几种配置参数。

（1）未连接（Not Connected）

虚拟机不可以使用网络，如果物理主机没在网络上或者不想通过虚拟机上网，则可以选

择此项屏蔽虚拟机的网络。

（2）仅本地（Local Only）

只能虚拟机之间相互访问，虚拟机将不允许访问物理主机上的任何网络资源。

（3）主机的物理网卡/微软的软网卡（Microsoft Loopback Adapter）

这种方式的虚拟机可以在网络上作为一台“真实”的主机，相当于在网络出现的物理主机。注意：此时使用的物理网卡，不是微软的软网卡。此时的虚拟机也可以作为域的成员计算机，只要域控制服务器添加该虚拟机就可以了。在这种情况下，虚拟机的计算机名不允许与网络上的主机重名，不管是虚拟的还是物理的主机。

（4）共享连接 Shared Networking（NAT）

要在虚拟机实现上网，具体的配置与实际系统没有什么不同。以局域网为例，设置 IP 地址后，在设置/网络连接/选定“共享连接（NAT）”，即可与实际系统一样正常上网，而且与实际系统没有任何冲突。

注意：只能是第一块网络适配卡位置才能设置为共享网络方式。在该方式下，虚拟机等同于连接在由 Virtual PC 构建的私有网络，这个私有网络包含一个 DHCP 服务器和一个 NAT 服务器，这两个服务器角色由 VPC 扮演。这种方式允许虚拟机访问绝大部分的物理主机能访问的网络资源。此时，如果不设置网络参数，必须把虚拟机网卡配置为自动获取 IP 地址方式，否则会导致无法访问网络。

5. 虚拟系统与实际系统实现资源共享

Microsoft Virtual PC 可以共享任何磁盘、任何程序、任何文件，还可以设置为“暂时共享”和“始终共享”，极其方便、灵活。

启动虚拟机，在 Virtual PC 控制台的“操作”菜单中，选择“安装或升级附加模块”命令，这时会自动载入“Virtual Machine Additions”目录下的“VM Additions. iso”；用资源管理器打开光驱，执行 DOS 目录下面的“fshare. exe”，最小化该虚拟机（不要关闭）；然后在 Virtual PC 控制台对此虚拟机进行“编辑”→“设置”命令，在“共享文件夹”选项中设置要共享母机的路径，再回到此虚拟机，进入 Z 盘就看到共享的文件了。

特别提示：为避免虚拟系统中存在的病毒可能对实际系统造成的交叉感染，建议如无必要，以关闭“ 始终共享”为好。必要时，临时共享一次也就行了。

6. 虚拟磁盘的设置和移除

要让计算机内的虚拟机高速运转，就要分配给它更多的系统内存和 CPU 资源。可以在 Virtual PC 控制台上选择某个没有运行的虚拟机，控制台的右边会出现“设置”和“移除”按钮，可以对虚拟机进行设置和移除。在“设置”打开的对话框中，选择“内存”项，然后向右侧拖动滑杆以扩大虚拟机内存容量，让其运行更流畅。在该对话框中，还可以进行还原磁盘、磁盘压缩等操作。还可以在“Virtual PC 控制台”中执行“文件→选项”命令，然后选择“性能”标签，在其中设置“始终让 Virtual PC 全速运行”项，按“确定”按钮。

提示：当虚拟机内的操作系统处于活动状态时，无法更改虚拟机的内存容量，所以在更改之前先要关闭虚拟机的操作系统，在关闭时不要选择“SAVED（保存）”状态，而是要选择“Turn off（关闭）”。

在 Virtual PC 控制台上，所谓虚拟机的“移除”只是在控制台界面不显示，可通过“新建→添加一台已有虚拟机”的方式，重选 vmc。