电脑迷 荣誉出品

黑客手抄本

黑客零点入门

菜鸟黑客解惑／IP隐藏术与破解／目标查找与锁定／Windows黑客入侵无孔不入／各类密码获取与入侵后的攻防／木马黑客／远程入侵与局域网战争

肖遥 编著

查找、锁定目标计算机的IP、开放端口及漏洞／直接入侵Windows系统／寻找、判断、歼灭木马、恶意或间谍程序／傀儡程序、后门、跳板、蠕虫／账户、文件有效破解／邮件、IM攻防大作战／服务器入侵攻防／局域网内部攻防作战／网游、聊天攻防

云南出版集团公司 • 云南科技出版社

电脑迷 荣誉出品

黑客手抄本

黑客零点入门

肖遥 编著

云南出版集团公司·云南科技出版社

名　　称：黑客零点入门
策　　划：彭 葵
编　　著：肖 遥
责任编辑：欧阳鹏 孙玮贤
执行编辑：彭 葵
组版编辑：黄 丹
封面设计：黄 丹

出版单位：云南出版集团公司 云南科技出版社
技术支持：（023）63658888-13101
邮购热线：（023）63658888-13126

发　　行：重庆中科普传媒发展股份有限公司发行部
电　　话：（023）63658888－13138
传　　真：（023）63659779
经　　销：各地新华书店、报刊亭
光盘生产：苏州新海博数码科技有限公司
文本印刷：重庆华林天美印务有限公司
开本规格：787×1092毫米 正度16开 16.5印张

版 本 号：ISBN 978-7-900747-09-9
版　　次：2008年5月第1版
定　　价：32元（1CD+1手册）

光盘导读

特别说明

本光盘提供的黑客软件和视频仅供技术研究使用，切勿利用来破坏他人的计算机或数据，否则一切后果自负。

光盘使用说明

将本光盘放入电脑光驱中，光盘会自动运行。如没有自动运行，可以打开“我的电脑”，用鼠标右键单击光驱所在盘符，在弹出菜单中选择“自动播放”即可。

光盘主界面

光盘启动后会打开光盘主界面，具体操作如下图：

目录

CONTENTS

注：本目录中凡标有 的章节均在光盘中有配套教学视频

第一章 黑客秘密训练营

第二章 高手从筑基开始

CONTENTS

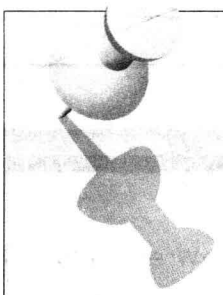
目录 CONTENTS

CONTENTS

目录

CONTENTS

CONTENTS



第一章
黑客秘密训练营

学习黑客少不了与木马病毒打交道，稍有不慎，自己可能就中招了。学习黑客技术，还需要找到许多符合条件的目标，进行攻击实践，但是这些目标从哪里寻找呢？没有经验的初学者，是很难从网上搜索到一模一样符合条件的漏洞主机的。
如何练习各种黑客技术呢？——自己打造一个黑客训练平台，让所有入侵技术都能在上面练习！

1.1 合法的黑客训练营[虚拟机]

恶意的黑客攻击是违法的，即使是在网络上随意找到一个目标进行攻击技术练习，那也有可能引来法律的纠纷，因此初学者需要一个合法的黑客技术练习平台——这个平台就是虚拟机。

1.1.1 让自己凭空多出一台电脑[虚拟机]

什么是虚拟机？虚拟机与黑客技术又有什么关系？

虚拟机概念

虚拟机软件是一种可以在一台电脑上模拟出来若干台PC，每台PC可以运行单独的操作系统而互不干扰，实现一台电脑“同时”运行几个操作系统，还可以将这几个操作系统连成一个网络的软件。

利用虚拟机，用户可以在一台电脑上将硬盘和内存的一部分拿出来虚拟出若干台机器，每台机器可以运行单独的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。你可以像使用普通机器一样对它们进行分区（图1）、格式化、安装系统和应用软件等操作，还可以将这几个操作系统联成一个网络。

普通用户可以在虚拟机平台上安装一个、两个，甚至更多的操作系统，轻轻松松进行切换。黑客可以利用虚拟机打造网络系统，在此网络中直观的进行各种攻击测试。

虚拟系统崩溃之后可直接删除，不影响本

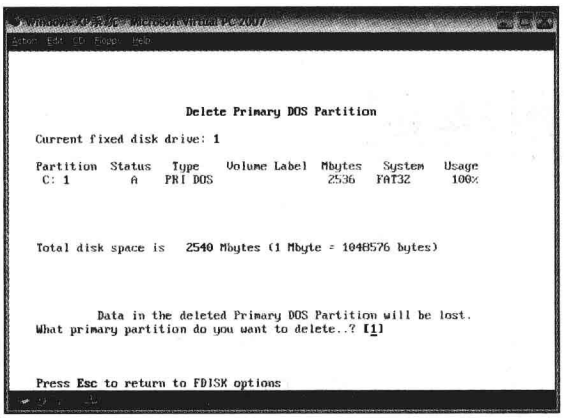


图1 在虚拟机中进行分区

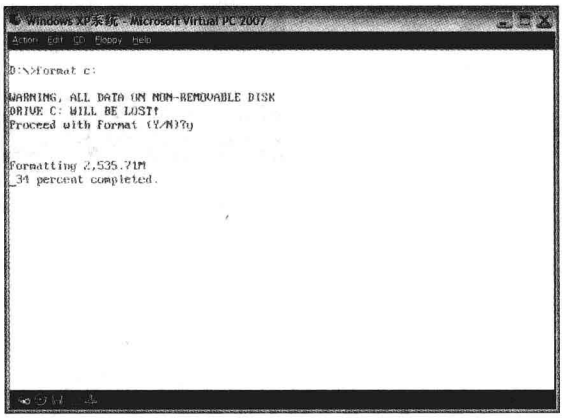


图2 在虚拟机中进行格式化

机系统，同样本机系统崩溃后也不影响虚拟系统，虚拟机软件不需要重开机，可以下次重装后再加入以前做的虚拟系统。

目前应用最广泛的虚拟机软件主要有两个，Virtual PC和VMware，这两款软件各有特长，能够轻易的在电脑上虚拟出任意的主机。

虚拟机与黑客技术

如果你的机器上安装的是Windows，又有兴趣感觉一下LINUX，可是LINUX安装教程告诉你需要重新对硬盘分区；或者你不满足于别人帮你安装操作系统，想自己试一试硬盘的分区、格式化……（图2），可是又害怕最后安装不成功；也许你喜欢试一试各种软件，可是又讨厌重装系统，或者害怕经常GHOST损坏硬盘；也许你已经安装了多个操作系统，可是当你需要切换操作系统的时候只能重新启动。

——对于普通用户，虚拟机可能满足他们各种各样的要求。而对于黑客学习者，虚拟机的作用和意义更大。在虚拟机中进行各种危险试验，完全不影响真正的系统，而效果与实际操作一模一样。同时在演习一些经典的入侵攻击漏洞时，在现实网络中已经很难再找到这样的练习环境了，但是在虚拟机中可以重现这样的漏洞攻击环境，让我们的黑客攻击学习不再纸上谈兵。

在下面的章节中，介绍了在虚拟机中搭建黑客技术训练营地的过程，以及如何在虚拟训练营中建网站、安装论坛等。读者朋友们可以细心学习参考，因为在以后的学习中，很多地方要用到这部份的知识；而且在以后的日记中，笔者不再详细提及如何搭建入侵环境了。

通过虚拟机，我们可以完成后面大部份的入侵学习，包括远程溢出、木马控制、WEB攻击等。虚拟机在黑客入侵学习中是非常重要的，读者朋友们尽快搭建自己的虚拟机系统吧！它将为你提供一个最好的入侵学习环境，它将伴你走完这本书中的所有学习旅程。

1.1.2 VMware打造黑客训练营

VMware Workstation是VMware公司的专业虚拟机软件，可以虚拟现有任何操作系统，而且使用简单、容易上手。

安装VMware Workstation

下载并运行VMware软件安装程序，按照安装向导提示，进行简单的设置，一路点击NEXT按钮（图3）。然后选择安装路径及全面安装类型，一路点击NEXT，即可完成安装。

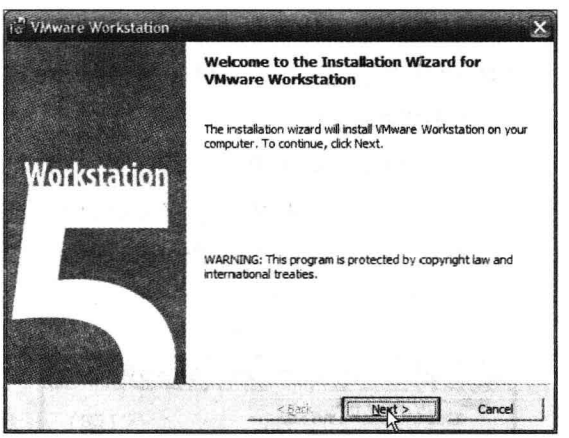


图3

在安装期间可能会出现两个提示对话框：询问“光驱的自动运行功能当前为开启状态，将影响虚拟机运行，是否需要屏蔽”，建议屏蔽。“数字签名确认，因为VMware将安装一些虚拟设备，所以Win2k将会提示是否同意安装”，选择“同意”。

安装完成后，重新启动计算机就可以使用VMware了。打开“网络连接”查看窗口，可以看到VMware安装时添加的两个网络连接（图4）。

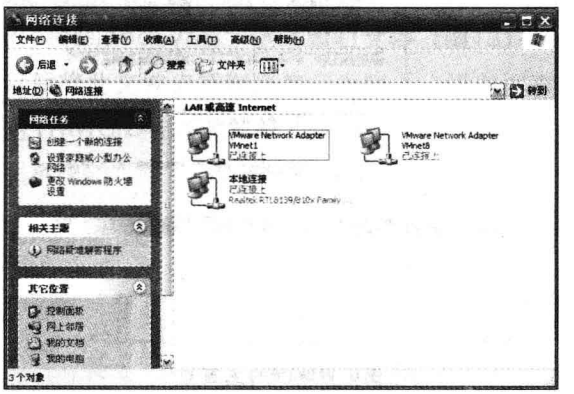


图4 新添加的网络连接

打开“设备管理器”→“网络适配器”，可以看到多出两块名为VMware Virtual Ethernet Adapter (basic host-only support for VMnet1)和VMware Virtual Ethernet Adapter (Network Address Translation (NAT) for VMnet8)的虚拟网卡（图5）。

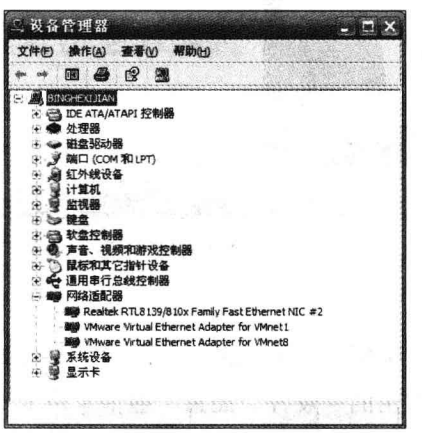


图5 新添加的虚拟网卡

不花钱，多出一台电脑

双击桌面的“VMware”图标，即可进入

VMware的主窗口（图6），并创建新的虚拟机。

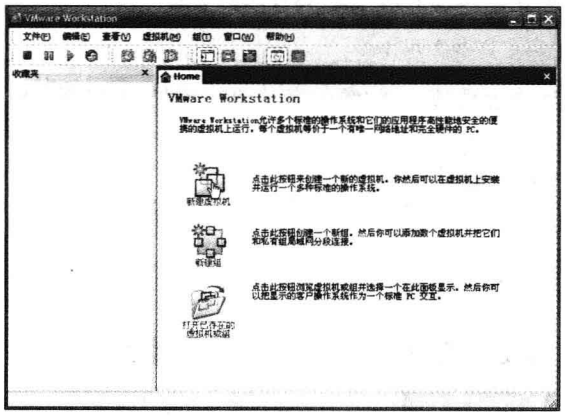


图6 VMware的主窗口

点击窗口右边的“新建虚拟机”按钮，弹出创建虚拟机的向导（图7）。点击“下一步”按钮，在向导窗口中选择创建虚拟机的类型。

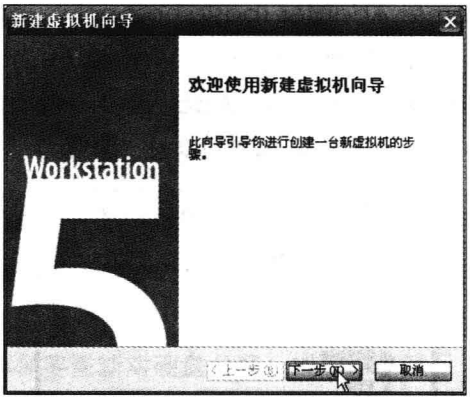


图7 虚拟机创建向导

“典型”是默认的典型方式，此方式中包括了常用的“硬件”配置：显卡、声卡、网卡（图8）。另一种方式则是自定义方式，可以自主选择虚拟机内需要哪些“硬件”设备。要安装的硬件设备并不依赖于真正的计算机系统硬件设备，它们通常是虚拟的，这也正是虚拟系统在任何机器上都可以运行的原因。

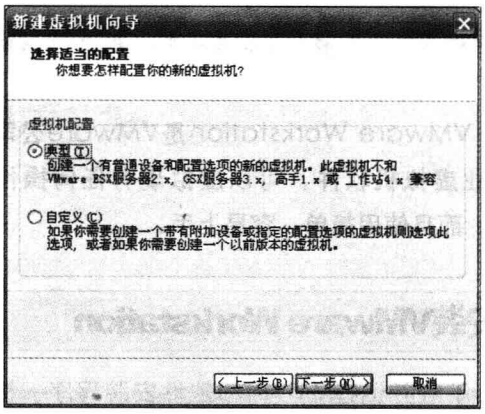


图8 设置硬件设备

继续点击“下一步”按钮，接着选择我们需要在虚拟机上运行的操作系统。虚拟机软件可以支持的操作系统包括从MS-DOS到Windows 2003以及Unix、Linux、Netware等众多版本的操作系统。

以安装Windows2000操作系统的虚拟机为例，在图中选择“Microsoft Windows”选项，版本为“Windows 2000 Professional”，继续点击“下一步”按钮（图9）。

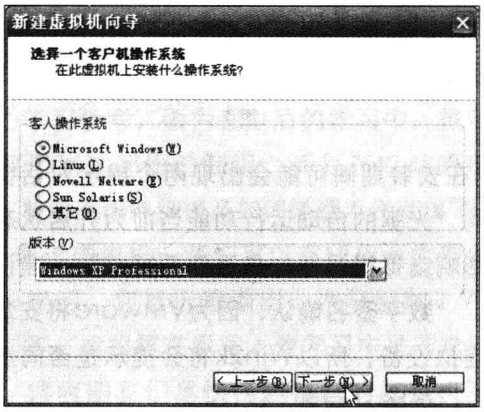


图9 选择操作系统

输入该虚拟机的名字（任意的）以及该虚拟机文件将要存放的位置（图10）。在“网络

连接”中选择“使用桥接网络”（图11）；

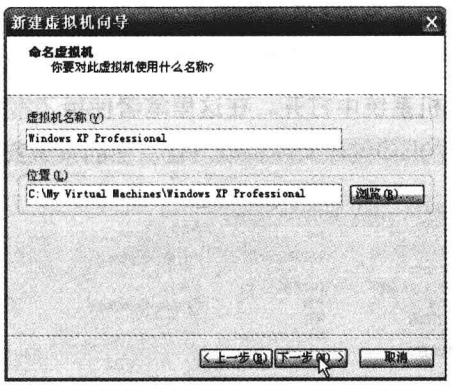


图10 设置虚拟机名称及文件存放位置

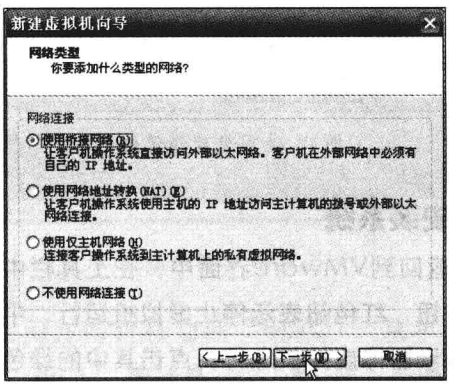


图11 设置网络类型

在“指定磁盘容量”中设置主机磁盘空间大小（图12）。

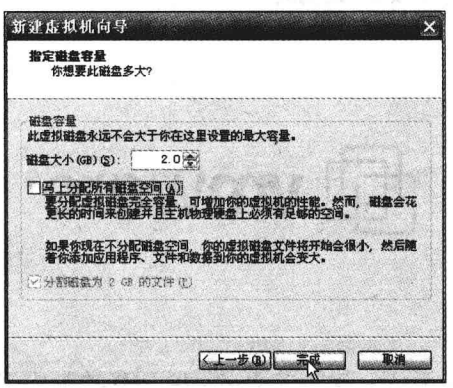


图12 设置主机磁盘空间大小

最后点击“完成”按钮，一个虚拟机系统的设置工作已经完成。在指定虚拟机存放路径下，将会生成名为“Windows XP Professional.vmx”的虚拟机文件（图13）。以后将此文件夹复制到其它电脑上，可以再次用VMware导入虚拟机文件，打开建立的虚拟机系统。

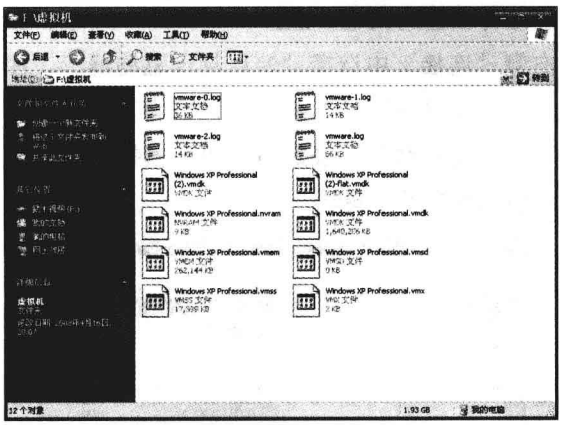


图13 虚拟机配置文件

打造攻击目标系统

创建了虚拟机以后，在VMware中点击菜单“文件”→“打开”，指定刚才安装虚

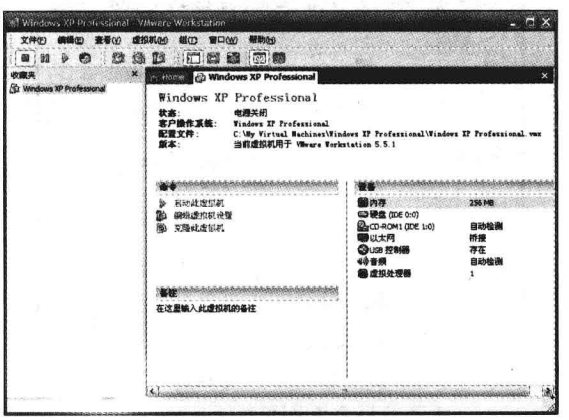


图14 虚拟机软硬件配置

拟机的文件路径，确定后打开虚拟机。返回VMware界面，点击窗口左侧“常用”栏，在导入的虚拟机的右侧窗口中可看到该主机硬件和软件系统信息（图14）。

设置系统安装光盘

点击“编辑虚拟机设置”按钮，打开虚拟机硬件设置对话框。选择“CD-ROM”项，在右侧“连接”中选择“使用物理驱动器”，使用“自动探测”项（图15）。或者直接指定当前物理光驱盘符，确定后即可在虚拟机中使用当前的光驱了（图16）。

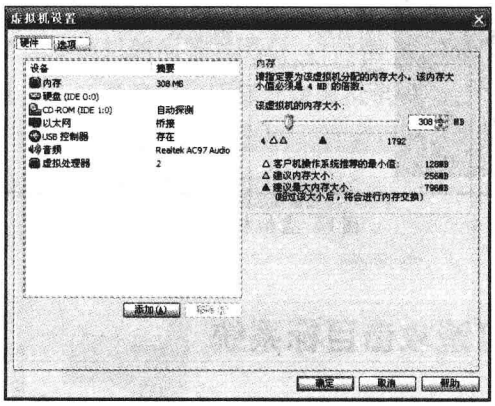


图15 使用物理光驱

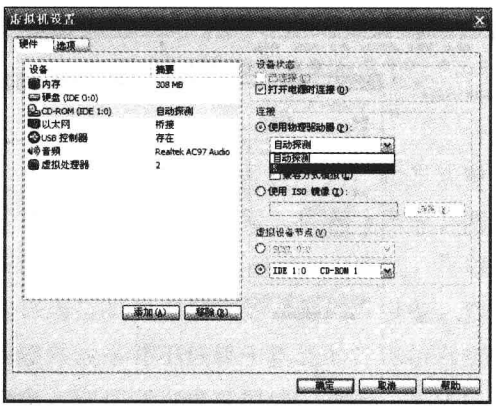


图16 自动检测光驱

如果有光盘ISO镜像文件，也可以勾选下方的使用ISO镜像，浏览指定ISO镜像文件（图17），即可将ISO镜像文件作为一张光盘，在虚拟机系统中打开。在这里笔者使用了XP安装光盘的ISO镜像文件，以方便后面的系统安装。

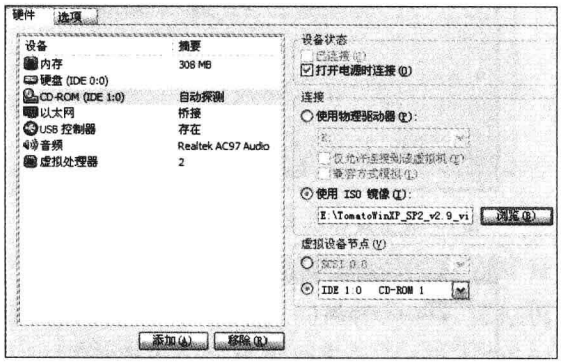


图17 使用光盘镜像文件

安装系统

返回到VMware界面中，在工具栏中有三个按钮，红色钮表示停止虚拟机运行，中间按钮表示暂停虚拟机运行，点击其中的绿色三角标志，启动该虚拟机（图18）。

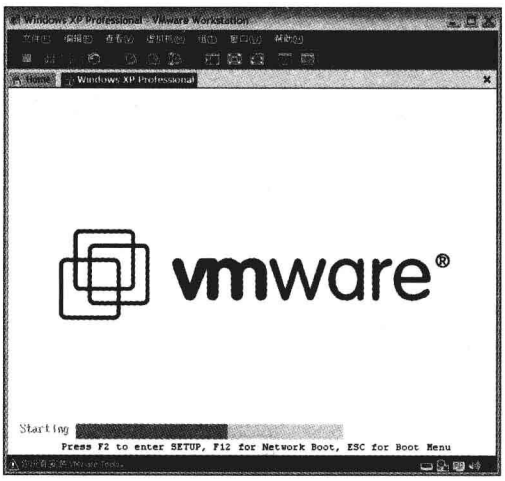


图18 虚拟机启动画面

首先启动的是虚拟机的自检过程，调用虚拟机的BIOS。因为我们安装系统需要使用光盘引导，所以此时需要按F2键进入虚拟机的BIOS设置程序（图19）。

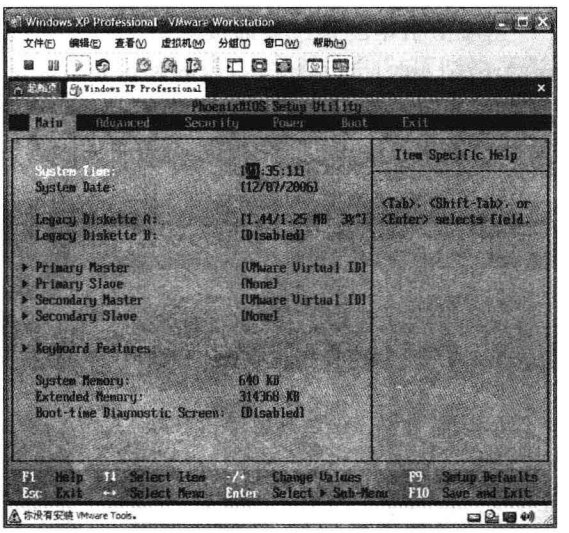


图19 虚拟机BIOS设置界面

使用方向键移动到“BOOT”菜单，用“+”和“-”按键将“CD-ROM”项调到第一项，即可将系统设置为光盘启动（图20）。接下来在光驱中放入Windows 2000系统的安装光盘，在虚拟机BIOS设置界面中移动到“Exit”菜单，选择“Exit Saving Changes”项，保存设置后重新启动虚拟机（图21）。

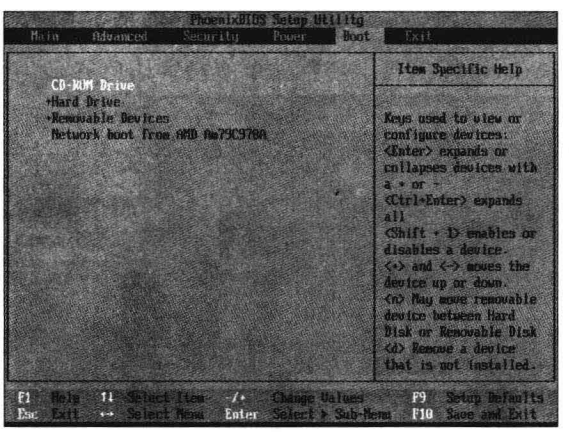


图20 设置光盘引导虚拟机

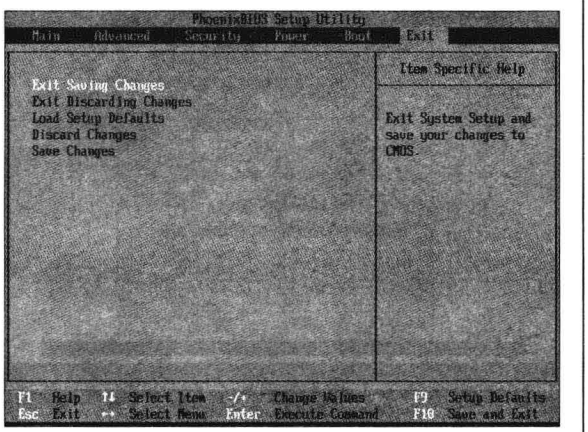


图21 保存设置

用Windows XP光盘引导系统进入安装界面（图22），然后就如同在真正的计算机上一样安装Windows XP系统了。此时虚拟机的硬盘就如同刚刚买回的新硬盘一样，只管放心大胆地分区格式化（图23），对真实系统丝毫不会造成损坏，因为VMware将计算机上的一个文

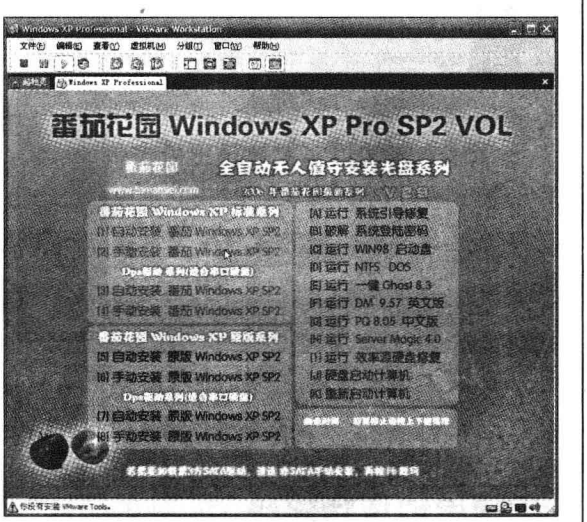


图22 虚拟机进入光盘引导界面