

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 荣誉出版

黑客手抄本

黑客

零点入门

肖遥 编著

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

版权所有 盗版必究
未经许可 不得以任何形式和手段复制或抄袭

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

1.1 合法的黑客训练营——虚拟机	1
1.1.1 让自己凭空多出一台电脑——虚拟机	1
1.1.2 VMware打造黑客训练营	3
安装VMware Workstation	3
不花钱，多出一台电脑	3
打造攻击目标系统	5
搭建虚拟攻防网络	8
1.1.3 Virtual PC也能虚拟电脑	11
新建Virtual PC	11
Virtual PC安装系统	13
网络设置	15
1.2 黑客学习者的乐土——虚拟机网站	16
1.2.1 两类网站平台	16
虚拟机ASP网站平台	17
快速架设ASP服务器	20
1分钟架设PHP服务器	20
ASP+PHP+CGI网站平台	21
1分钟搭建全能网站	24
1.2.2 发布网站，放出攻击目标	24
解压安装网站程序	24
程序安装法	26
MYSQL网站安装	26
安装网站插件	27

2.1 马识途，矢中的——IP地址	28
2.1.1 IP地址详解	28
2.1.2 查看主机IP地址	30
查看本机IP地址	30
远程主机IP地址	31
2.2 黑客进出走端口	31
2.2.1 电脑的门户——端口	31
2.2.2 正邪能辨——端口分类	32
2.2.3 揪出秘密潜入者	32
2.2.4 出入我控制——端口管理 	34
关闭端口进程	34
监视端口信息	35
2.3 黑客必会的攻击命令	37
2.3.1 黑客攻击先要“拼”——Ping	37
Ping命令详解	37
Ping探测路由器数目	38
探测主机操作系统类型	39
解析远程主机名	39
PING命令攻击远程主机	39
2.3.2 网络掌控一手中——Ipconfig	40
查看网络配置	40
在局域网中隐身	40
2.3.3 神秘的暗伤——NET命令	41

CONTENTS

管理系统服务.....	41	E-mail定位的优劣.....	59
实现IPC\$连接.....	42	Outlook定位邮件者IP.....	59
管理用户账号.....	42	Foxmail邮件查IP地址.....	60
管理共享资源.....	43	3.1.4 社会工程学入侵——锁定物理地址.....	61
2.3.4 又识端口——Netstat.....	44	在线查询IP物理位置.....	61
2.3.5 进程信息我了然——Tasklist.....	44	使用IP查询专用工具.....	61
2.3.6 黑客就是那么狠——Taskkill.....	46	3.2 扫描攻击目标.....	62
2.3.7 千里操纵——AT.....	46	3.2.1 探马赤——扫描器简介.....	62
AT命令运行的前提.....	46	3.2.2 扫描X档案——X-Scan.....	62
AT命令添加计划任务.....	47	X-Scan简介.....	62
2.3.8 居家必备——COPY.....	48	扫描参数设置.....	63
2.3.9 随身携带的“木马”——Telnet.....	48	选择扫描模块.....	65
2.3.10 解除禁止——Tlntadm.....	49	扫描.....	66
2.3.11 随风潜入夜——FTP.....	50	3.2.3 飞逝“流光”，极速扫描.....	66
2.3.12 另辟蹊径的ECHO.....	51	流光简介.....	66
2.3.13 无声无息的克隆替代——Replace.....	52	扫描参数设置.....	67
2.3.14 木马之种——ASSOC.....	52	开始扫描.....	68
2.3.15 伸向系统的黑手——REG.....	53	查看扫描报告.....	69
2.3.16 重启一片天——Shutdown.....	54	3.2.4 “超强”扫描器Superscan.....	70
		获取远程IP地址.....	70
		扫描某个IP段内的在线主机.....	71
		扫描指定IP主机的端口.....	72
		3.2.5 多功能扫描器X-Way.....	72
		高级扫描功能.....	72
		主机搜索功能.....	75
		查询功能.....	75
		猜解机.....	76
		“黑匣子”攻击.....	76

第三章 锁定目标，一矢中的

3.1 黑客盯的就是你——锁定目标.....56

3.1.1 聊天埋标记——通过QQ确定目标.....56

Fineplus 定位QQ好友.....56

“好功夫”，抓好友.....57

3.1.2 皆入我法眼——ICQ和MSN聊友定位.....58

3.1.3 邮件泄机密，E-mail定位攻击目标.....59



嗅探器	77
代理扫描功能	77

第四章 远程攻击任我行

4.1 远程攻击，决胜千里	79
4.1.1 远程攻击简述	79
4.1.2 远程攻击过程	80
4.2 局域网中的黑手——共享攻击	81
4.2.1 SMB共享基础	81
安装SMB	81
共享设置	82
4.2.2 锁定目标，扫描共享	83
扫描局域网内的共享主机	83
共享入侵实例1	85
共享攻击实例2	86
4.3 漂浮幽灵——局域网欺骗攻击	88
4.3.1 我非我？——IP冲突攻击	88
4.3.2 网络特工下黑手——IP冲突攻击利器	89
4.3.3 来自身边的欺骗——ARP欺骗攻击	90
ARP与ARP攻击	90
威力强大的CheatARP	91
网马无处不在，新兴ARP攻击	92
4.4 低级但最有效的DoS攻击	96
4.4.1 什么叫DoS攻击	96
4.4.2 DoS攻击分类	96
4.4.3 DoS洪水攻击利器	97
SYN攻击利器HGod	97

多种网络杀手	98
4.5 远程攻击漏洞	100
4.5.1 夺命，远程溢出攻击简介	100
4.5.2 华丽外衣之下——远程主机漏洞检测	101
服务器漏洞扫描工具LNSS	101
专业的漏洞扫描工具	103
最常用的扫描武器——X-Scan	104
4.5.3 解码带来的漏洞	104
Unicode解码问题	104
虚拟机下的入侵实例	104
4.5.4 扩展引发的危机——经典远程溢出漏洞	107
IDA和IDQ扩展漏洞简介	107
IDA和IDQ扩展攻击实例	107
4.5.5 Printer打印带来的漏洞	109
漏洞命令	109
远程连接	109
4.5.6 Web网站杀手	109
WebDAV漏洞简介	109
实战WebDAV	110
4.5.7 不可不知的RPC溢出	110
RPC漏洞简介	110
RPC漏洞攻击	111

第五章 特洛伊之计，木马攻击

5.1 特洛伊木马传说	113
5.1.1 木头作的马？——木马概念及特点	113
5.2 内鬼——全面揭密反弹木马	114

CONTENTS

5.2.1 自动上门的反弹木马	114	5.4.3 百度搜霸与挂马漏洞	147
5.2.2 漫天飞舞的灰鸽子	115	漏洞原理	147
一秒钟，生成第一个木马	115	百度搜霸网页木马的制作	147
等你送上门，肉鸡上线	116	中招远程控制	149
遥控千里之外	117	5.5 真假难辨——木马伪装术	150
机密任我取	119	5.5.1 换个马甲——木马捆绑伪装	150
5.2.3 好马不出名——CIA	122	最简单的木马捆绑	150
史上最强的木马配置系统	122	EXE伪装器	151
玩弄肉鸡于股掌间	128	木马制作过程中的伪装	153
5.2.4 域外精品木马MiniRat	130	5.5.2 秘密行动，加密木马	155
来自域外的优势	130	增加字节法	155
至精至简，创建服务端	130	EXE文件巧变VBS	156
功能强大的反弹控制	132	压缩/打乱头文件	158
5.3 神秘的Telnet木马后门	134	5.5.3 为木马穿上重重迷彩	159
5.3.1 打开“黑客之门”	134	第六章 网站沦陷，黑客菜鸟尝甜头	
配置与安装	134	6.1 网站被黑之谜——WEB攻击简介	161
进入黑客之门	135	6.1.1 WEB攻击概述及特点	161
黑客门中玩控制	136	6.1.2 常见WEB攻击手法	162
5.3.2 新兴木马NameLess BackDoor	137	6.2 黑站必会的SQL注入攻击	164
木马远程安装	137	6.2.1 了解SQL注入	164
连接与控制	138	6.2.2 SQL注入攻击基础	165
5.3.3 SUS迷你FTP后门	139	动动手，找注入点	165
SUS伪装与配置	139	鼠标一点，注入漏洞自动现	169
安装与传播	141	判断数据库类型	170
连接及远程文件管理	141	6.2.3 一分钟，攻入Access数据库网站	171
5.4 网页中的猫腻——网页木马	143	利用WED注入破解	171
5.4.1 网页木马简介	143		
5.4.2 网马盛宴，万能网页木马制造机	144		



NBSI注入破解.....	173	7.1.1 江湖洒热血，网络丢密码.....	205
“数据库备份”种植木马后门.....	175	热血江湖生成器最新版.....	205
6.2.4 威力更大，SQL数据库注入攻击.....	177	热血江湖ASP木马生成器.....	206
SQL Server环境下的入侵.....	177	7.1.2 遗失密码，空留传奇.....	208
利用NBSI注入控制服务器.....	179	网吧感染版传奇木马.....	209
6.2.5 PHP注入入侵详解.....	181	梦天使传奇木马.....	209
手工注入法.....	181	盛大密宝传奇木马.....	
用CASI自动PHP注入.....	186	7.1.3 防不胜防——各种网游木马全现身.....	210
6.2.6 SQL注入攻击学习环境.....	186	来自WOW怒吼——魔兽木马.....	210
手工搜索注入站点.....	186	征途密码寻回软件.....	212
快速获得SQL注入点.....	188	天堂无壳木马生成器.....	212
6.3 网站命脉悬一线——数据库入侵	189	梦幻西游盗号木马.....	213
6.3.1 “暴露”带来的攻击.....	189	天骄木马生成器.....	213
6.3.2 动网数据库下载漏洞攻击实例.....	190	7.2 QQ被盗大揭底	214
构建入侵平台.....	190	7.2.1 密保难逃——农民QQ密保大盗.....	214
数据库入侵攻击原理.....	191	配置邮箱信息.....	214
实例入侵动网论坛.....	192	制作木马客户端.....	215
6.3.3 隐藏地址，一暴即知.....	196	木马盗号.....	215
暴库入侵技术的原理.....	196	7.2.2 “有缘”还是倒霉——冰之缘.....	216
暴库入侵BBSXP论坛.....	197	设置收信方式.....	216
6.3.4 无处不在，搜索引擎入侵网站数据库.....	200	伪装生成木马.....	216
搜索数据库文件原理.....	200	木马盗号.....	217
新浪搜索数据库实例.....	200	7.3 反击盗号，再盗号	217
使用“挖掘鸡”找数据库.....	202	7.3.1 木马箱子揭密.....	217
		制作木马.....	218
		后台木马箱子.....	218
		7.3.2 木马箱子不牢靠.....	218
		木马箱子的数据下载漏洞.....	219

第七章 账号、密码不翼而飞

7.1 一盗千金——网游木马.....205

CONTENTS

极速击破, 木马箱子破解器	219
万能破解木马箱子	220
7.4 隐私密码, 不堪一击	222
7.4.1 你在和谁聊——破译聊天机密	222
聊天密码轻松破解	222
截获MSN聊天信息	222
其它嗅探MSN信息的工具	224
无需密码看QQ聊天记录	224
加密邮件藏不住	226
7.4.2 加密真有效? ——加密软件大破解	228
E-神加密, 一点也不神	228
破解“文件夹加密超级大师”	229
“超级加密 3000”解密	231
7.4.3 微软的EFS, 一样也没戏	231
权限设置, 形同虚设	232
EFS加密轻松破	234
20秒, 生成第一只病毒	237
“个性化”VBS病毒	239
8.2.2 VBS蠕虫制作机	241
8.2.3 VBS脚本病毒刷QQ聊天屏	242
8.2.4 VBS网页脚本病毒	243
8.2.5 VBS打造U盘窃密者	244
8.3 不要宏, 制作Word病毒	246
8.3.1 MS06027引发DOC病毒	246
8.3.2 MS05016——又一病毒漏洞	247
8.3.3 普通DOC文档病毒的制作	248
8.3.4 功能更强大的DOC病毒	249
8.4 U盘病毒自己造	250
8.4.1 打造超强U盘蠕虫病毒	250
超强U盘蠕虫病毒制造机	250
病毒基体——U盘感染	250
超强蠕虫, 共享还原不放过	250
锁定IE, “尾巴”跟定你	251
另类病毒, 藏身网页	251
一变多, “下载者”功能	252
反杀病毒软件	252
8.4.2 闪存窥探者——FlashDiskThief	253
窥探者的伪装与隐藏	253
窃取U盘资料	253

第八章 玩毒最高境界——训毒

8.1 第三只看病毒	236
8.1.1 敌友难辨——病毒ABC	236
8.1.2 为我所用——病毒攻击	236
8.2 一段代码也编病毒	237
8.2.1 VBS脚本病毒生成机	237



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

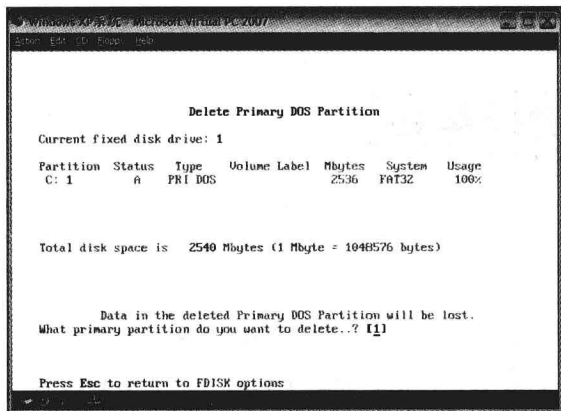


图1 在虚拟机中进行分区

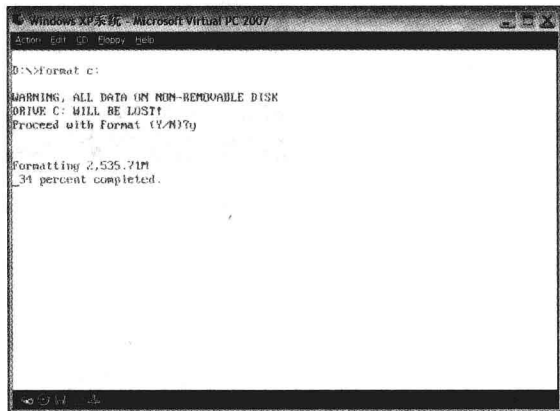


图2 在虚拟机中进行格式化

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。

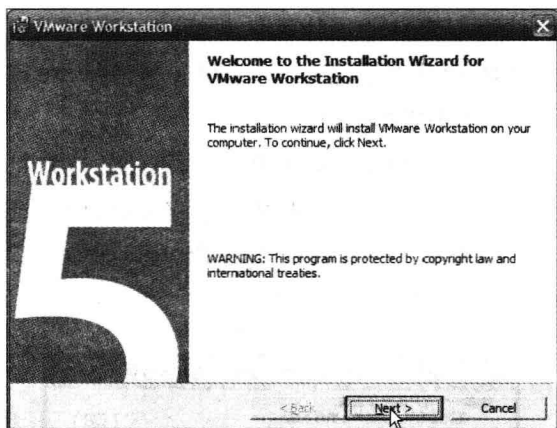


图3

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）。

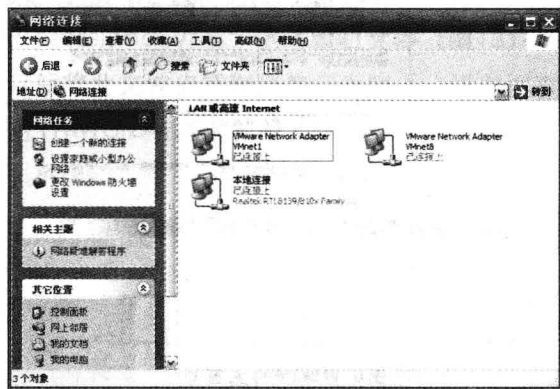


图4 新添加的网络连接

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）。

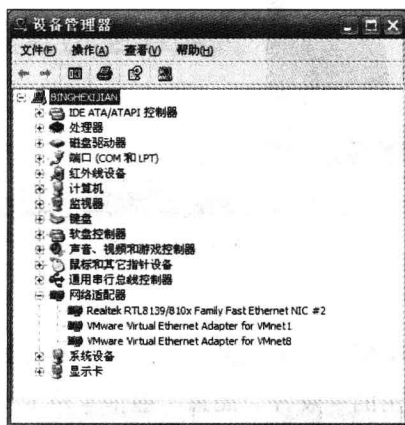


图5 新添加的虚拟网卡

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。

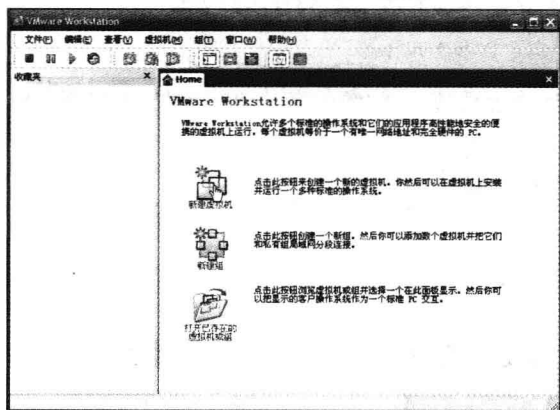


图6 VMware的主窗口

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。

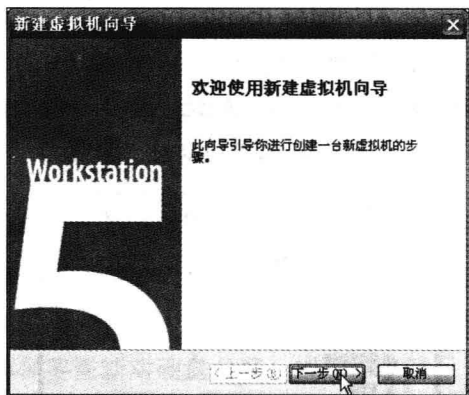


图7 虚拟机创建向导

“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。

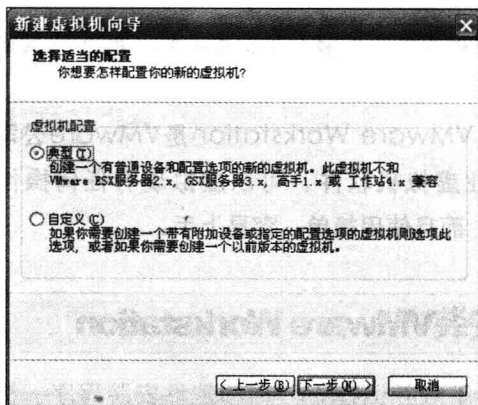


图8 设置硬件设备

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)。

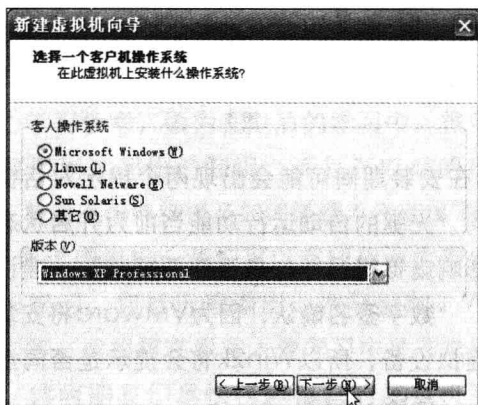


图9 选择操作系统

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)；

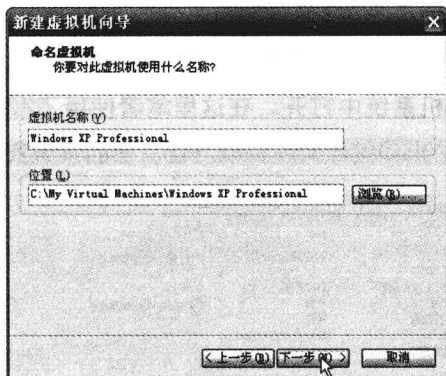


图10 设置虚拟机名称及文件存放位置

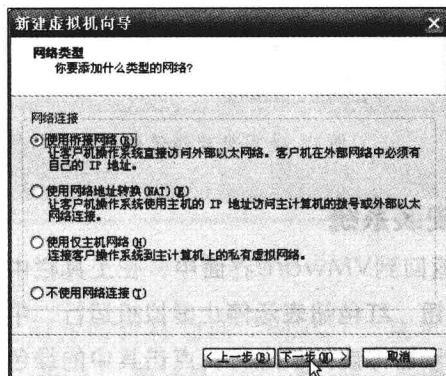


图11 设置网络类型

在“指定磁盘容量”中设置主机磁盘空间大小(图12)。

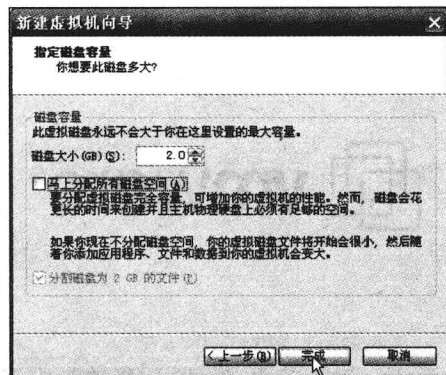


图12 设置主机磁盘空间大小

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

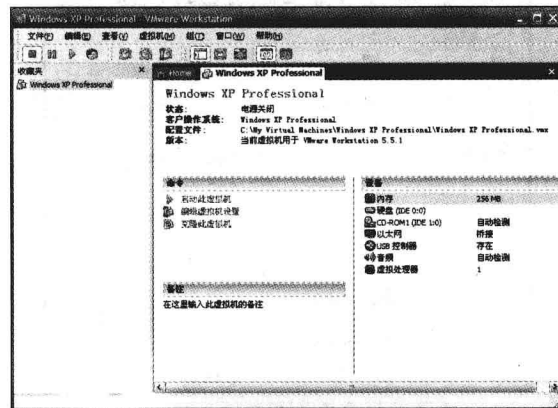


图14 虚拟机软硬件配置

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）。

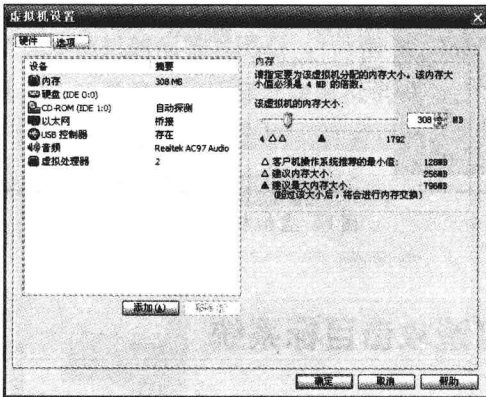


图15 使用物理光驱



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。

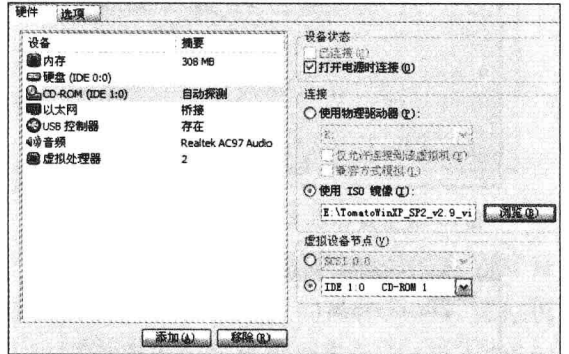


图17 使用光盘镜像文件

安装系统

返回到VMware界面中，在工具栏中有三个按钮，红色按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）。

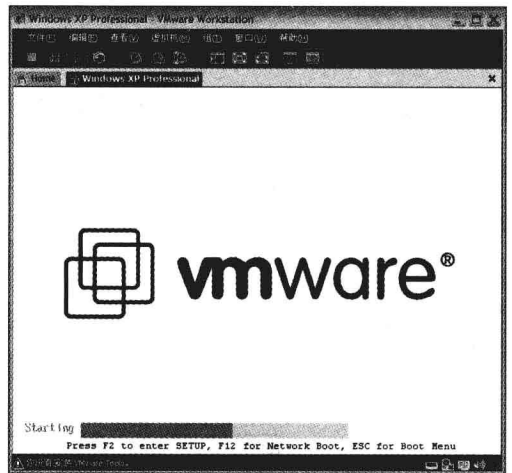


图18 虚拟机启动画面



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）。

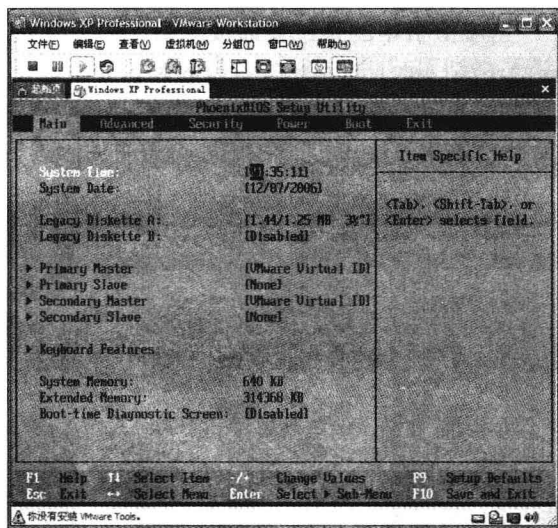


图19 虚拟机BIOS设置界面

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

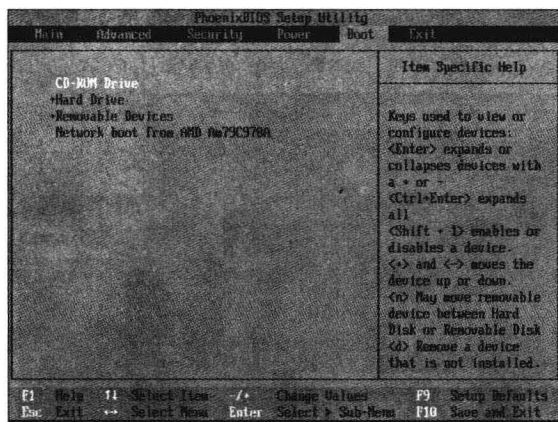


图20 设置光盘引导虚拟机

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）。

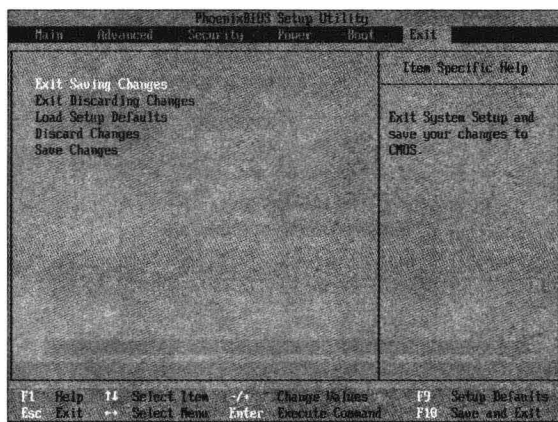


图21 保存设置

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

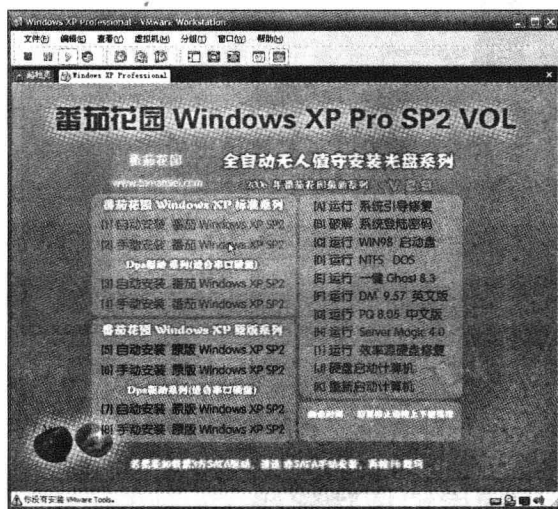


图22 虚拟机进入光盘引导界面