



黑客攻防 实战详解

邓吉柳靖编著



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>



黑客攻防 实战详解

邓吉柳靖 编著

电子工业出版社

Publishing House of Electronics Industry

北京•BEIJING

内 容 简 介

本书从“攻”、“防”两个不同的角度,通过现实中的入侵实例,并结合作者的心得体会,图文并茂地再现了网络入侵与防御的全过程。本书共分3篇共11章,系统地介绍了入侵的全部过程,以及相应的防御措施和方法。内容主要包括基于认证的入侵及防御、基于服务器软件漏洞的入侵及防御、基于Windows操作系统漏洞的入侵及防御、基于木马的入侵及防御、入侵中的隐藏技术、入侵后的留后门及清脚印技术、本地入侵及防御,以及防火墙技术和BAT编程。本书用图解的方式对每一步入侵步骤都进行了详细的分析,以推测入侵者的入侵目的;对入侵过程中常见的问题进行了必要的说明与解答;对一些常见的入侵手段进行了比较与分析,以方便读者了解入侵者常用的方式、方法,保卫网络安全。本书是《黑客攻防实战入门》的姊妹篇。

本书适合于网络技术爱好者、网络系统管理员阅读,并可作为相关专业学生的学习资料和参考资料。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

图书在版编目(CIP)数据

黑客攻防实战详解 / 邓吉, 柳靖编著. —北京: 电子工业出版社, 2006.3

(安全技术大系)

ISBN 7-121-02221-4

I. 黑… II. ①邓… ②柳… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆CIP数据核字(2006)第002901号

责任编辑: 毕 宁 bn@phei.com.cn

印 刷: 北京智力达印刷有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路173信箱 邮编 100036

经 销: 各地新华书店

开 本: 787×1092 1/16 印张: 30.5 字数: 817千字

印 次: 2006年3月第1次印刷

印 数: 6000册 定价: 49.00元

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。联系电话:(010) 68279077。质量投诉请发邮件至 zlts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前言

《黑客攻防实战入门》一书自面世以来，得到了广大读者的肯定与好评，笔者在此深表感谢。本书作为《黑客攻防实战入门》一书的姊妹篇，读者定位与其基本相同，主要针对那些对网络安全技术感兴趣的初学者，同时，本书更深入、细致地剖析了黑客技术，系统性更强，以期满足那些已有一定技术基础的读者的需要。此外，值得一提的是，笔者始终以“授之以鱼，不如授之以渔”为基本出发点来展开本书的内容。也就是说，本书的主要目的是向读者介绍黑客攻防技术的思考方法，而不是单纯地介绍某个工具的使用方法。总之，本书是一本介绍为什么，而不是单单介绍怎么做的一本黑客入门及提高书，这一点是本书区别于其他黑客类书籍的根本特征。

关于黑客

长期以来，由于诸多方面的因素，“黑客”这个字眼变得十分敏感，不同的人群对黑客也存在不同的理解，甚至没有人愿意承认自己是黑客。有些人认为，黑客是一群狂热的技术爱好者，他们无限度地追求技术的完美；有些人认为，黑客只是一群拥有技术，但思想简单的毛头小伙子；还有些人认为黑客是不应该存在的，他们是网络的破坏者。这里，我们没有必要对这个问题争论不休，也无须给“黑客”加上一个标准的定义，但从客观存在的事实来看，黑客这类群体往往存在着以下几个共同点。

① 强烈的技术渴望与完美主义。驱动他们成长的是对技术的无限渴望，获得技术的提高才是他们最终的任务。

② 强烈的责任感。只有强烈的责任感才能使他们不会走向歧途。责任感告诉他们不要在任何媒体上公布成功入侵的服务器；不要对其入侵的服务器进行任何的破坏；在发现系统漏洞后要马上通知官方对该漏洞采取必要的修补措施，在官方补丁没有公布之前，绝对不要大范围地公开漏洞利用代码。一方面，黑客入侵可能造成网络的暂时瘫痪，另一方面，黑客也是整个网络的建设者，他们不知疲倦地寻找网络大厦的缺陷，使得网络大厦的根基更加稳固。

为什么写作本书

不容乐观的事实是，一部分人歪曲了黑客的本质，被不良动机所驱使，进行各种入侵活动，威胁网络的健康发展。对于我国来说，形势尤为严峻。我国信息化建设迟于美国等发达国家，信息安全技术水平也相对落后，在几次跨国黑客大战中，国内网站的弱口令、漏洞比比皆是，这种现状实在令人担忧，值得我们深思和反省，从中也可以看出国内传统的计算机、网络教学远远没有满足实际的需要。可能出于安全等原因的考虑，传统教学往往只教授简单的应用，避开了一些敏感的技术。设想一下，如果一个网站的管理员只学会架构网站，却不关心如何入侵自己的网站，

那么他如何对自己网站的缺陷了如指掌？如何能够及时地获知最新漏洞而提前做好抵御？如果以上都做不到，那就更不要谈日常的系统更新、维护和打补丁了。然而，国内精通入侵的网管又有多少呢？长期以来，国内网管的潜意识里都认为“入侵”是个不光彩的勾当，甚至嗤之以鼻。随着信息化程度越来越高，信息技术与生活的联系越来越紧密，可以上网的电子设备逐年增加，电脑、PDA、手机，甚至家电。可以想像 10 年后，如果不了解入侵者的手段来采取必要的防御措施，将要被入侵的设备不会仅仅限于电脑，也许还包括你的手机、家电、汽车，等等。因此，在信息技术如此发达，沟通方式日益丰富和复杂的今天，我们不仅要学会如何正确使用网络，而且还需要学会如何防御自己的网络被他人入侵。

出于以上原因，笔者通过多年的研究与实践，系统地总结了目前广为使用的入侵、防御技术，并针对广大网管以及对网络感兴趣的在校学生编写了本书。希望大家能够从多个角度来了解网络安全技术，至少做到知己知彼。

本书主要内容

本书以深入剖析入侵过程为主线来展开全书内容，向读者介绍入侵者如何实现信息的收集，如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马的入侵），如何实现入侵即远程连接，入侵后如何执行各种任务，如何留下后门以便再次进入系统，以及入侵者如何清除系统日志防止目标服务器发现入侵痕迹。此外，书中还详细地介绍了入侵者是如何实现从信息扫描到入侵过程中的隐身保护，如何逃避被他人发现。全书会对每一个入侵步骤做详细的分析，以推断入侵者在每一入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答，此外，还会对几种常见的入侵手段进行比较与分析。

本书按照难易程度分为“入门篇”、“实战篇”和“提高篇”，3 篇共 11 章，每章的主要内容如下。

第 1 章“一次完整的入侵”通过一个完整的入侵实例来介绍入侵的一般手法。使读者对入侵手法有个初步的认识。

第 2 章“信息收集”系统地介绍了入侵之前的准备工作。这一阶段也是经常被忽略的部分。

第 3 章“基于认证的入侵”介绍了如何入侵基于用户名+密码认证方式的远程主机。

第 4 章“基于服务器软件漏洞的入侵”介绍了入侵者是如何通过服务器软件的漏洞来实现入侵的目的。

第 5 章“Windows 操作系统漏洞”介绍了入侵者如何通过 Windows 操作系统漏洞来实现入侵的目的。

第 6 章“基于木马的入侵”介绍了入侵者如何通过种植木马程序来实现入侵的目的。

第 7 章“隐藏技术”介绍了入侵者在入侵的时候所使用的一些隐身手法，通过该章读者能够了解为何难以发现入侵者的足迹。

第 8 章“留后门与清脚印”介绍了入侵成功后，入侵者如何抹去入侵痕迹。

第 9 章“本地入侵”介绍了如何入侵物理上可以接触的计算机。

第 10 章“防火墙技术”介绍了防火墙的原理，以及入侵者如何穿透防火墙实现入侵。

第 11 章“BAT 编程”介绍了 BAT 编程的一般方法。在入侵中，入侵者经常编写一些 BAT 程序来简化繁琐的入侵过程。

笔者将书中提到的所有相关软件整理为一个说明文件（提供了这些软件的下载地址和简单介绍），读者可到 <http://www.broadview.com.cn/html/resource/hack.rar> 下载这个文件。

需要声明的是，本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任；本书的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机，并采取行动。

限于水平，加之时间仓促，书中错漏之处难免，敬请批评指正。

意见反馈请发邮件至 editor@broadview.com.cn 或 jsj@phei.com.cn。

读者与作者技术交流，可上书友论坛 <http://forum.broadview.com.cn>。

目 录

入 门 篇

第 1 章 一次完整的入侵	2
1.1 搭建局域网	2
1.2 认识扫描器	7
1.3 一次完整的入侵	9
1.4 小结	23
第 2 章 信息搜集	24
2.1 网站信息搜集	24
2.1.1 相关知识	24
2.1.2 信息搜集	27
2.1.3 网站注册信息搜集	30
2.1.4 结构探测	34
2.1.5 搜索引擎	38
2.2 资源搜集	39
2.2.1 共享资源简介	39
2.2.2 共享资源搜索	40
2.2.3 破解 Windows 9x 共享密码	42
2.2.4 利用共享资源入侵	43
2.2.5 FTP 资源扫描	44
2.2.6 安全解决方案	45
2.2.7 常见问题与解答	45
2.3 端口扫描	46
2.3.1 网络基础知识	46
2.3.2 端口扫描原理	49
2.3.3 端口扫描应用	49
2.3.4 操作系统识别	52
2.3.5 常见问题与解答	52
2.4 综合扫描	53
2.4.1 X-Scan	53
2.4.2 流光 Fluxay	58
2.4.3 X-WAY	61
2.4.4 扫描器综合性能比较	64
2.4.5 常见问题与解答	64
2.5 小结	65

实 战 篇

第 3 章 基于认证的入侵	68
3.1 获取账号密码	68
3.1.1 弱口令扫描	68
3.1.2 字典攻击	70
3.1.3 暴力破解	74
3.1.4 网络监听获取密码	77
3.1.5 其他途径	79
3.1.6 常见问题与解答	81
3.2 IPC\$ 入侵	82
3.2.1 IPC\$ 简介	82
3.2.2 远程文件操作	83
3.2.3 IPC\$ 空连接漏洞	88
3.2.4 安全解决方案	90
3.2.5 常见问题与解答	92
3.3 Telnet 入侵	93
3.3.1 Telnet 简介	93
3.3.2 Telnet 典型入侵	94
3.3.3 Telnet 杀手锏	98
3.3.4 Telnet 高级入侵全攻略	101
3.3.5 常见问题与解答	105
3.4 利用注册表入侵	105
3.4.1 注册表简介	106
3.4.2 远程开启及连接远程主机的“远程注册表服务”	107
3.4.3 编辑注册表 (REG) 文件	108
3.4.4 常用注册表入侵方法	110
3.5 利用远程计算机管理入侵	113
3.5.1 计算机管理简介	113
3.5.2 开启远程计算机管理服务	114
3.5.3 管理远程计算机	117
3.5.4 利用远程控制软件对远程计算机进行入侵	120
3.5.5 常见问题与解答	123
3.6 利用远程终端服务 (3389) 入侵	124
3.6.1 终端服务的概念	124
3.6.2 远程开启远程终端服务 (3389)	124
3.6.3 使用远程终端服务入侵	127
3.6.4 常见问题与解答	130
3.7 利用 MS SQL 入侵	130
3.7.1 利用 MS SQL 弱口令入侵	130
3.7.2 入侵 MS SQL 数据库	135
3.7.3 入侵 MS SQL 主机	135

3.7.4	利用 SQL 注入攻击	140
3.7.5	利用 NBSI 软件进行 SQL 注入攻击	144
3.7.6	安全解决方案	146
3.8	利用 FTP 入侵	147
3.8.1	FTP 简介	147
3.8.2	利用 FTP 弱口令入侵	149
3.8.3	利用 FTP 匿名登录入侵	154
3.8.4	利用 FTP 提升本地权限	157
3.8.5	利用 SlimFTP 制作 FTP 肉鸡	158
3.8.6	安全解决方案	160
3.9	远程命令执行及进程查杀	160
3.9.1	远程执行命令	160
3.9.2	查、杀进程	161
3.9.3	远程执行命令方法汇总	164
3.9.4	常见问题与解答	164
3.10	小结	165
第 4 章	基于服务器软件漏洞的入侵	166
4.1	IIS 漏洞（一）	166
4.1.1	IIS 基础知识	166
4.1.2	.ida&.idq 漏洞	167
4.1.3	.printer 漏洞	174
4.1.4	Unicode 目录遍历漏洞	177
4.1.5	.asp 映射分块编码漏洞	187
4.2	IIS 漏洞（二）	189
4.2.1	WebDAV 远程缓冲区溢出漏洞	189
4.2.2	WebDAV 超长请求远程拒绝服务攻击漏洞	194
4.2.3	WebDAV XML 消息处理远程拒绝服务漏洞	196
4.2.4	Windows Media 服务 nsislog.dll 远程缓冲区溢出漏洞	200
4.2.5	Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞	205
4.2.6	常见问题与解答	208
4.3	论坛漏洞	208
4.3.1	上传漏洞	208
4.3.2	暴库漏洞	218
4.3.3	常见问题与解答	231
4.4	Blog 漏洞	231
4.4.1	直接下载数据库漏洞	231
4.4.2	Cookie 欺骗漏洞	246
4.4.3	常见问题与解答	254
4.5	Serv-U 漏洞（一）	254
4.5.1	Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞	255
4.5.2	Serv-U 本地权限提升漏洞	261

4.5.3 常见问题与解答	265
4.6 小结	265
第 5 章 Windows 操作系统漏洞	266
5.1 本地提权类漏洞	266
5.1.1 Microsoft Windows 内核消息处理本地缓冲区溢出漏洞	266
5.1.2 Microsoft Windows LPC 本地堆溢出漏洞	270
5.1.3 Microsoft OLE 和 COM 远程缓冲区溢出漏洞	272
5.2 用户交互类漏洞	275
5.2.1 Microsoft Task Scheduler 远程任意代码执行漏洞	275
5.2.2 Microsoft Windows GDI+ JPG 解析组件缓冲区溢出漏洞	277
5.2.3 Microsoft Windows 图形渲染引擎安全漏洞	283
5.2.4 Microsoft 压缩文件夹远程任意命令执行漏洞	286
5.2.5 Microsoft Windows ANI 文件解析远程缓冲区溢出漏洞	288
5.2.6 Microsoft Windows MSHTA 脚本执行漏洞	291
5.3 远程溢出漏洞	298
5.3.1 Microsoft UPnP 存在缓冲溢出漏洞	298
5.3.2 Microsoft RPC 接口远程任意代码可执行漏洞	300
5.3.3 Microsoft Windows Messenger 服务远程堆溢出漏洞	305
5.3.4 Windows ASN_1 库 BER 解码堆破坏漏洞	308
5.3.5 Windows Local Security Authority Service 远程缓冲区溢出漏洞	313
5.3.6 Microsoft WINS 服务远程缓冲区溢出漏洞	317
5.3.7 Microsoft Windows 即插即用功能远程缓冲区溢出漏洞	320
5.4 小结	324
第 6 章 基于木马的入侵	325
6.1 木马的工作原理	326
6.1.1 木马是如何工作的	326
6.1.2 木马的隐藏	326
6.1.3 木马是如何启动的	328
6.1.4 黑客如何欺骗用户运行木马	330
6.2 木马的种类	331
6.3 木马的演变	333
6.4 第二代木马	333
6.4.1 冰河	333
6.4.2 广外女生	339
6.5 第三代与第四代木马	343
6.5.1 木马连接方式	343
6.5.2 第三代木马——灰鸽子	345
6.5.3 第四代木马	348
6.5.4 常见问题与解答	355
6.6 第五代木马	355
6.7 木马防杀技术	356

6.7.1	加壳与脱壳	356
6.7.2	木马防杀实例	357
6.8	种植木马	359
6.8.1	修改图标	359
6.8.2	文件合并	360
6.8.3	文件夹木马	362
6.8.4	网页木马	364
6.8.5	CHM 电子书木马	367
6.9	安全解决方案	369
6.10	常见木马的手动清除	370
6.10.1	冰河木马	370
6.10.2	ShareQQ 木马	370
6.10.3	BladeRunner 木马	371
6.10.4	广外女生	371
6.10.5	BrainSpy 木马	371
6.10.6	FunnyFlash 木马	371
6.10.7	QQ 密码侦探特别版木马	372
6.10.8	IEthief 木马	372
6.10.9	Q Eyes 潜伏者	372
6.10.10	蓝色火焰	372
6.10.11	Back Construction 木马	373
6.11	常见问题与解答	373
6.12	小结	373
第 7 章	隐藏技术	374
7.1	文件传输与文件隐藏技术	374
7.1.1	IPC\$ 文件传输	374
7.1.2	FTP 传输	375
7.1.3	打包传输	375
7.1.4	文件隐藏	378
7.1.5	常见问题与解答	381
7.2	扫描隐藏技术	381
7.2.1	流光 Sensor	384
7.2.2	其他工具	387
7.2.3	常见问题与解答	387
7.3	入侵隐藏技术	388
7.3.1	跳板技术简介	388
7.3.2	手工制作跳板	388
7.3.3	Sock5 代理跳板	394
7.3.4	端口重定向	403
7.4	小结	405

第 8 章	留后门与清脚印	406
8.1	账号后门	406
8.1.1	手工克隆账号	407
8.1.2	命令行方式下制作后门账号	412
8.1.3	克隆账号工具	416
8.1.4	常见问题与解答	420
8.2	漏洞后门	420
8.2.1	制造 Unicode 漏洞	420
8.2.2	制造 idq 漏洞	422
8.3	木马后门	422
8.3.1	wolf	422
8.3.2	Winshell 与 WinEggDrop	428
8.3.3	SQL 后门	429
8.4	清除日志	431
8.4.1	手工清除日志	431
8.4.2	通过工具清除事件日志	431
8.4.3	清除 WWW 和 FTP 日志	434
8.5	小结	435
第 9 章	本地入侵	436
9.1	基础知识	436
9.2	盘载操作系统简介	436
9.3	ERD Commander	437
9.3.1	ERD Commander 简介	437
9.3.2	利用 ERD Commander 进行入侵的实例	437
9.4	Windows PE	443
9.4.1	Windows PE 简介	443
9.4.2	利用 Windows PE 入侵本地主机的三个实例	443
9.5	安全解决方案	449
9.6	本章小结	450

提 高 篇

第 10 章	防火墙技术	452
10.1	防火墙概述	452
10.1.1	防火墙的定义	452
10.1.2	防火墙的规则	452
10.1.3	防火墙的功能	452
10.1.4	使用防火墙的好处	452
10.2	防火墙的分类	453
10.2.1	按实现方式分类	453
10.2.2	软件防火墙	453
10.2.3	硬件防火墙	453

10.2.4	按实现技术分类	453
10.2.5	数据包过滤防火墙	453
10.2.6	三应用级网关	455
10.2.7	状态包检测防火墙	456
10.3	常见防火墙简介	457
10.4	防火墙的结构	458
10.4.1	常见术语	458
10.4.2	双宿主机体系结构	458
10.4.3	被屏蔽主机体系结构	459
10.4.4	被屏蔽子网体系结构	459
10.5	防火墙发现技术	460
10.5.1	黑客入侵带防火墙的操作系统的一般过程	460
10.5.2	跟踪技术	460
10.5.3	防火墙识别技术	460
10.5.4	路由跟踪	461
10.5.5	端口扫描	461
10.5.6	旗标攫取	461
10.5.7	防火墙审查技术	462
10.6	穿越防火墙技术	462
10.6.1	ICMP 协议隧道	462
10.6.2	HTTP 协议隧道	463
10.7	小结	463
第 11 章	BAT 编程	464
11.1	批处理命令简介	464
11.2	在批处理文件中使用参数与组合命令	469
11.2.1	在批处理文件中使用参数	469
11.2.2	组合命令	470
11.3	管道命令	471
11.4	综合利用的实例	473
11.4.1	系统加固	473
11.4.2	删除日志	473
11.5	小结	474

入 门 篇

本篇通过一个完整的入侵实例，介绍如何搭建虚拟局域网来构建自己的入侵测试环境，如何在入侵之前获取目标主机的关键信息，以及如何实现最基本的入侵。

通过本篇的学习，读者会对网络安全技术有一个初步的认识，并且能够独立地搭建各种入侵测试环境以完成后续章节的学习。

第 1 章 一次完整的入侵

黑客技术与计算机领域其他技术的一个显著区别是黑客技术的非公开化，因此很少看到对黑客技术进行大范围公开宣传。从隶属关系的角度来看，黑客技术是计算机安全领域内的一个分支。因此，正确理解黑客技术的内涵对学习黑客技术是十分重要的。

很多人认为黑客技术很神秘，这主要是由于对黑客技术的不了解造成的。还有一部分人认为黑客技术就是用于入侵系统的技术。黑客技术确实离不开入侵，但黑客技术的应用绝不单单是入侵系统。在矛与盾的斗争中，没有绝对的胜者，为了做出更好的“盾”，仔细了解“矛”的特点是十分重要的。

本篇是全书的开篇，本篇中将着重介绍基础知识，同时通过一个入侵实例使读者对黑客技术有一个初步的了解，有助于读者后边的学习。

1.1 搭建局域网

本节中提及的局域网并不是物理上的局域网，而是指使用虚拟机搭建起来的虚拟局域网。该虚拟局域网可以供那些没有网络环境的读者来测试、实践书中所介绍的入侵与防御技术。

使用工具：VMware。

🔧 工具介绍

VMware 是一个“虚拟机”软件。它可以实现在一台机器上同时运行两个或更多的操作系统。

与“多启动”系统相比，VMware 采用了完全不同的概念。一台主机在正常安装多系统后同一时刻只能运行一个系统，需要进行系统切换时必须重新启动计算机，而 VMware 则是真正“同时”在主系统的平台上运行多个操作系统，实现像标准 Windows 应用程序那样切换。

此外，使用 VMware 可以实现在一台计算机上架设一个局域网。可以在这个虚拟的局域网中进行网络测试。

🔧 VMware 的获取

可以到 VMware 的官方网站“<http://www.vmware.com/>”下载最新版本的 VMware，并在官方网站上注册获得一个免费使用三十天的序列号。

🔧 VMware 的安装

本节中以 VMware workstation 4.0.5 为例介绍 VMware 的安装过程。

双击安装文件后会弹出如图 1-1 所示的窗口。

单击“Next”按钮，显示如图 1-2 所示。

选择接受许可后，单击“Next”按钮，会弹出如图 1-3 所示的窗口。

如果不想安装在默认路径下，可以单击“Change”按钮更改。选定路径后，单击“Next”按钮，如图 1-4 所示。

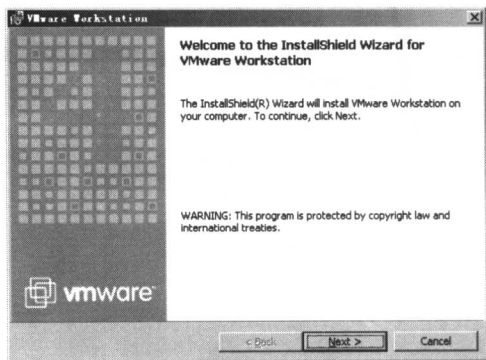


图 1-1

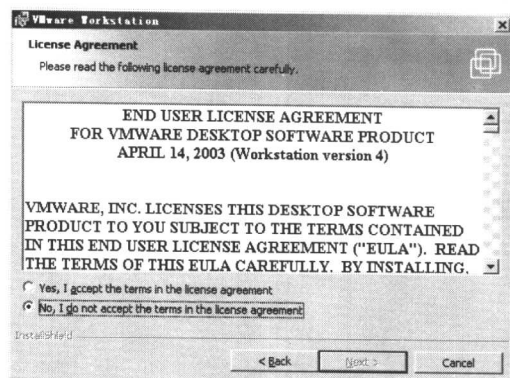


图 1-2

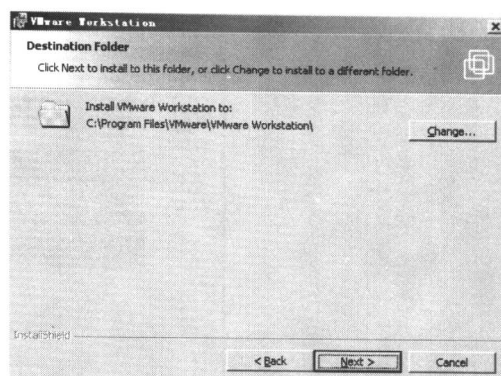


图 1-3

如果设置都正确，可以单击“Install”按钮进行安装了。

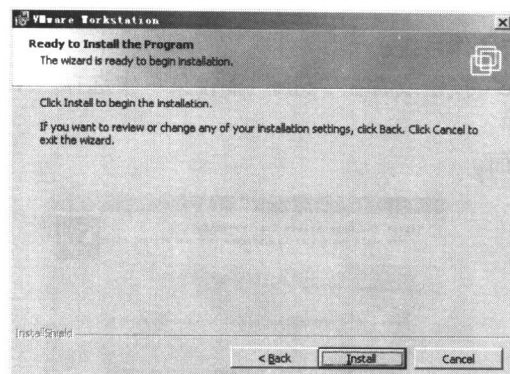


图 1-4

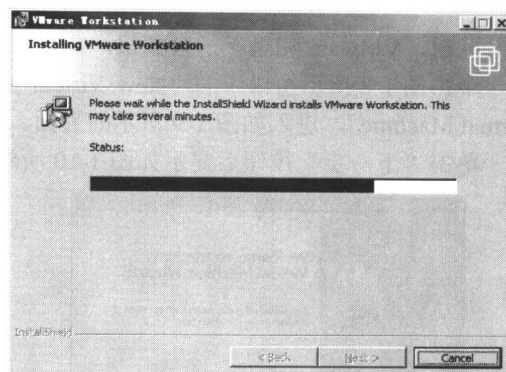


图 1-5

拷贝文件完成后，会要求输入序列号，如图 1-6 所示。

输入序列号后，单击“Enter”按钮，显示如图 1-7。

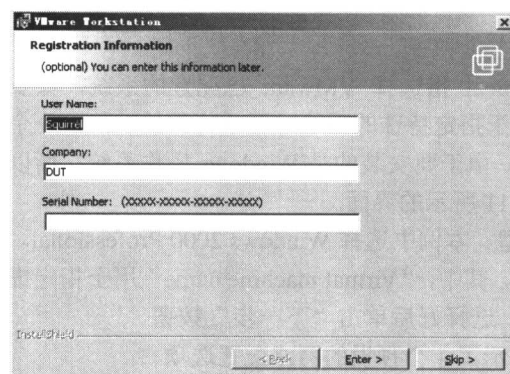


图 1-6

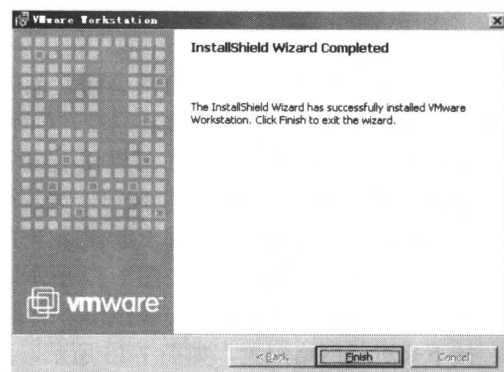


图 1-7

单击“Finish”按钮完成 VMware 的安装。

👉 VMware 的配置与使用说明

首次运行 VMware 显示如图 1-8 所示的界面。

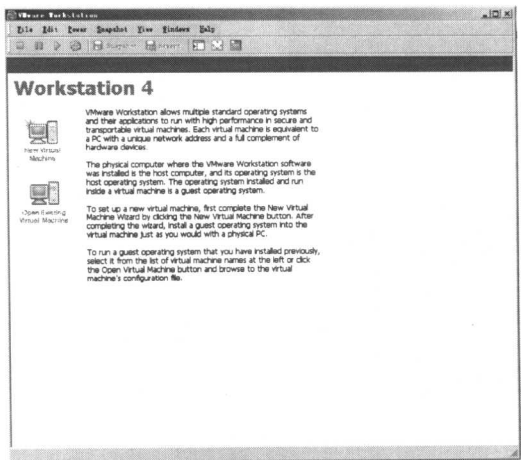


图 1-8

此时，VMware 相当于一台裸机，需要为其安装操作系统。

单击图 1-8 所示窗口中的“New Virtual Machine”按钮或者在“File”下拉菜单中选择“New Virtual Machine”，进入如图 1-9 所示的界面。

单击“下一步”按钮后显示如图 1-10 所示的界面。

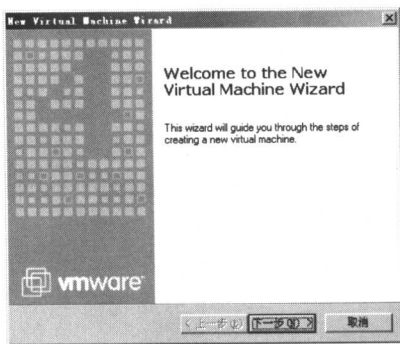


图 1-9

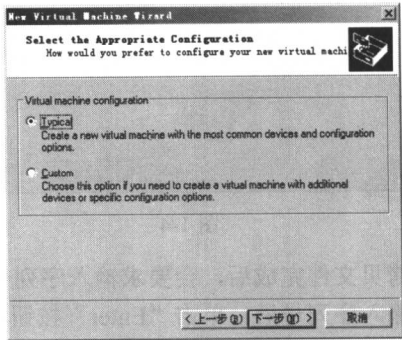


图 1-10

在图 1-10 所示的窗口中有两个配置选项：Typical 指选择 VMware 已配置的系统，如安装 Windows 操作系统或者 Linux 操作系统；Custom 用于指定特殊的系统配置或特殊的功能，一个新开发的操作系统需要进行测试时可以使用这个选项。由于要安装的是 Windows 操作系统，所以选择 Typical。然后单击“下一步”按钮，进入如图 1-11 所示的界面。

“Guest operating system”用于选择操作系统类型。本例中选择 Windows 2000 Professional。然后单击“下一步”按钮，进入如图 1-12 所示的界面。其中，“Virtual machine name”用于指定虚拟机的名称，Location 用于指定安装操作系统的位置，选择好后单击“下一步”按钮。

接下来进行网络配置，如图 1-13 所示。其中显示了 4 个预设的网络配置选项。

- Use bridged networking: 虚拟机直接连接外部网络，需要为虚拟机设定独立的 IP 地址。
- Use network address translation: 虚拟机通过主系统连接到外部网络，这种设置下，虚拟给与主系统使用相同的 IP 地址。
- Use host-only networking: 将虚拟机连接到一个架设在主系统之上的虚拟局域网中，为架设虚拟局域网并且不希望虚拟机连接到外部网络时，可以选择此项。