教育部师资实践基地系列教材——信息与网络安全

神州数码校企合作技能训练系列

入侵检测系统实训教程

RUQIN JIANCE XITONG SHIXUN JIAOCHENG

程庆梅　徐雪鹏　主编

全国职业技能大赛推荐参考书

神州数码校企合作技能训练指定教材

校企合作新课改教材

机械工业出版社
CHINA MACHINE PRESS

配电子课件

教育部师资实践基地系列教材——信息与网络安全

入侵检测系统实训教程

主　编　程庆梅　徐雪鹏
副主编　杜婉琛
参　编　李东方　王　岳　王　博
郭　薇　田　弦

机械工业出版社

本书主要围绕神州数码网络入侵检测系统的安装部署以及各种典型应用展开。全书共设计四个部分：IDS 系统部署、查询工具的安装与使用、安全响应策略的配置及联动、常见攻击模拟，共十一个独立的实训任务。

本书是典型的实训教程，以实际工作内容为依托，形成典型的实训工作设计，按照一般学习思维活动的特点进行系统化编排和整理。本书的主体内容均包含：任务目的、任务设备及要求、任务步骤、任务思考与练习，既保证了实训的可操作性，又对实训后的理论提升创造了空间。

本书读者对象为：各类职业院校相关专业课程师生；各中小企业网络管理员等。

本书配有电子课件以方便教师教学，可到机械工业出版社教材服务网 www.cmpedu.com 以教师身份免费注册下载，或联系编辑（010-88379194）咨询。

图书在版编目（CIP）数据

入侵检测系统实训教程/程庆梅，徐雪鹏主编．—北京：机械工业出版社，2012.4
教育部师资实践基地系列教材．信息与网络安全
ISBN 978-7-111-37885-3

Ⅰ．①入… Ⅱ．①程… ②徐… Ⅲ．①计算机网络—安全技术—教材 Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 057511 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：梁 伟 责任编辑：梁 伟 范成欣
封面设计：鞠 杨 责任印制：杨 曦
北京四季青印刷厂印刷
2012 年 5 月第 1 版第 1 次印刷
184mm×260mm • 5.75 印张 • 132 千字
0001—3000 册
标准书号：ISBN 978-7-111-37885-3
定价：18.00 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
社服务中心：（010）88361066
销售一部：（010）68326294
销售二部：（010）88379649
读者购书热线：（010）88379203

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com

封面无防伪标均为盗版

前　言

1．本书的读者

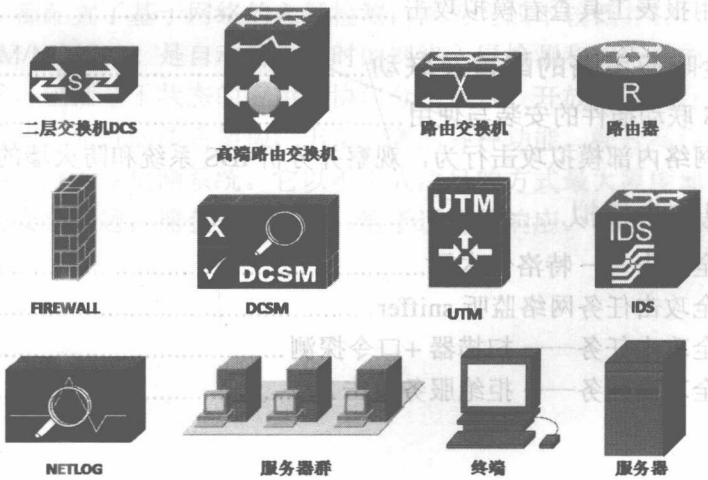
本书适用于致力于从事网络安全升级与维护实施的人员。我们也把这本书推荐给所有对学习计算机网络安全技术有兴趣的人士。本书所教授的技术和引用的案例都是神州数码推荐的设计方案和典型的成功案例。

2．所需要的预备知识

为了能对本书中所讲述的内容有充分的理解，读者应该对以下内容具有一定的认识：

- 网络互联基础。
- 了解路由和交换的基本原理。
- 熟悉路由交换及防火墙设备的基本调试方法。

3．本书所用图标



本书由神州数码网络公司的技术专家及行业专家和专职企业讲师共同协作、编写而成，由程庆梅、徐雪鹏任主编。编写分工如下：教学主管杜婉琛，高级讲师李东方、王岳、王博分别负责本书部分章节的编写和验证；网络公司技术专家朱建英、唐进元、陈戍、陈亮和吕凯分别就各章节部分内容在设备中做了大量的验证工作；教务管理郭薇、校企合作专员田弦、助理讲师王铎和教务助理郭长慧分别就本书的内容做了大量的文字校对整理工作；网络公司技术部总监、网络大学校长徐雪鹏则在本书的方向、整体布局以及主体内容合理性方面给予了大量的指导和建议。

由于编者水平所限，疏漏之处在所难免，敬请广大读者批评指正，编者邮箱：dcnu 2007@163.com。

编　者

目　录

导　读

网络变得日益复杂且更加开放，人们对 Internet 的依赖也逐渐增强，因此各公司感到网络越来越不安全了。通常，我们用一台防火墙限制来自 Internet 的数据流进入网络，但是防火墙并不是没有缺陷的，利用 IP 蒙骗技术和 IP 碎片技术，黑客们已经展示了他们穿过当今市场上大部分防火墙的本领。防火墙可以限制来自 Internet 的数据流进入网络，但是对于来自防火墙内部的攻击却无能为力。因此，需要一种独立于常规安全机制的安全解决方案——一种能够破获并中途拦截那些能够攻破网络第一道防线的攻击。这种解决方案就是入侵检测系统。利用入侵检测系统连续监视网络的通信情况，寻找已知的攻击模式，当它检测到一个未授权活动时，软件会以预定方式自动进行响应，报告攻击、记录该事件或是断开未授权连接。

DCNIDS-1800 M/M2/G/G2 是基于网络的实时入侵检测及响应系统，基于网络的入侵检测系统有许多仅依靠基于主机的入侵检测法无法提供的功能。实际上，许多客户最初使用入侵检测系统时，都配置了基于网络的入侵检测，因为它成本较低并且反应速度快。

DCNIDS-1800 M/M2/G/G2 是自动的、实时的网络入侵检测和响应系统，它采用了新一代的入侵检测技术，包括基于状态的应用层协议分析技术、开放灵活的行为描述代码、安全的嵌入式操作系统、先进的体系架构、丰富完善的各种功能，配合高性能专用硬件设备，是最先进的网络实时入侵检测系统。它以不引人注目的方式最大限度地、全天候地监控和分析企业网络的安全问题，捕获安全事件，给予适当的响应，阻止非法的入侵行为，保护企业的信息组件。

单元 1

IDS 系统部署

学习目标

1. 了解 IDS 的各项配置，明确管理环境搭建和不同管理方法之间的差异
2. 掌握 IDS 控制台的搭建步骤，控制软件生成数据的观察分析与使用

重点及难点

1. IDS 工作模式

IDS——入侵检测系统是一种安全设备，它依照一定的安全策略，通过软、硬件，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

2. IDS 的重要性以及管理环境的搭建与备份

IDS 是防火墙以后的第二道安全防线，可以有效地防止防火墙和操作系统与应用程序的设定不当，监测内部使用者的不当行为，了解和观察攻破第一道防线防火墙入侵者的行为意图，并收集入侵方式的资料，以及时阻止恶意的网络行为。

只有对 DCNIDS-1800 控制台进行多方位地了解以及熟练地使用才可以更加有效地防止入侵，以及时地想出应对策略。

对于安全设备而言，设备的配置文件被妥善地备份，将有助于在安全事件发生后以最快的速度恢复网络的可用性。通常设备的系统文件也需要进行及时的备份，这样可以保障系统文件丢失或者进行版本升级失败时，恢复系统的可用性。合格的网络管理和维护人员，一定要对所有关键网络设备中的重要文件加以备份，才可以在需要的时候及时、有效地恢复网络的可用性。

知识补充

IDS 探测器基本分为两类：基于网络的 IDS 和基于主机的 IDS。

基于网络的 IDS 如同“超级”嗅探器，它们在 TCP/IP 层或者更底层监视流量，监测是否有已知的攻击。

基于主机的 IDS 采取不同的方法搜索攻击模式，其检测事件主要靠操作系统的日志，因此它不能检测到发生在网络层的攻击。

DCNIDS-1800 是基于网络的入侵检测系统。无论是基于网络的还是基于主机的 IDS 都要在以下几个环节做好重要的准备：

1）IDS 监控及回应。

2）事件的处理。

3）犯案分析及数据保留。

4）报告过程。

技能大赛赛点分析

本单元的内容在历届大赛相关赛项中占到比赛的 3%～5%。一般情况下，只要涉及信息安全类的竞赛项目，入侵检测系统是必不可少的。因此，IDS 部署实施属于考生必备的一项技能，务必做到熟练。本单元的内容都是很基础性的东西，安装调试也不是很复杂，但如果没有着重练习过，比赛过程中一旦在此环节出现故障将会影响整个比赛进度。因此，需要大量地练习达到熟练才能顺利应对技能大赛中的后续赛点。

虽然比赛赛点一般不会明确指出本单元所述技能，但这是每次考试必考的一项。

任务 1　IDS 传感器的安装配置

1.1　任务目的

1．理解 DCNIDS 系统的构成

2．掌握 DCNIDS 传感器的配置要点

1.2　任务设备及要求

1．DCNIDS-1800 系列设备一台

2．使用串口连接硬件设备的命令行界面，掌握 IDS 传感器的配置要点

1.3　任务步骤

1.3.1　连接硬件设备，进行拓扑环境搭建

入侵监测设备的连接方式有以下两种：

1）传感器使用键盘鼠标接口和显卡接口直接连接外部设备，使用键盘对传感器直接操作。

2）通过配置线缆与 PC 的 COM 口连接，使用超级终端打开（本任务采用此种方式）。

通过第二种方式连接时，其超级终端的参数采用 Windows 系统中的默认值，这里不再赘述。

连接好配置线缆与 PC 的 COM 口后，打开传感器的电源开关，启动设备后，可以看到图 1-1 所示的传感器监控界面。

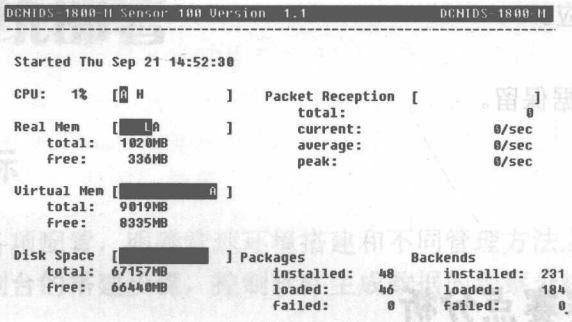


图 1-1　传感器监控界面

1.3.2　配置传感器

使用任意键都可以启动登录过程，如图 1-2 所示。

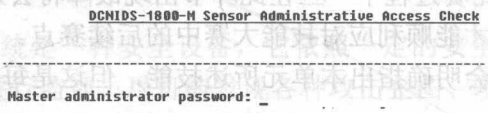


图 1-2　传感器的登录界面

此时，输入出厂默认的传感器密码：admin，即可登录图 1-3 所示的主菜单。

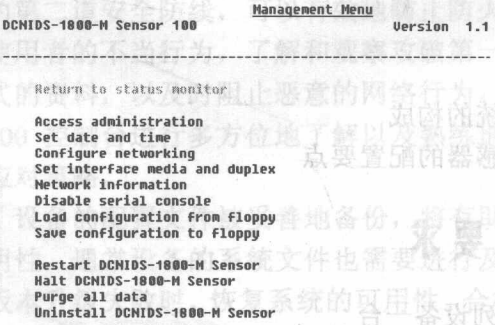


图 1-3　传感器主菜单

可以通过上、下按键选择需要配置的单元，下面一一列出。

1．配置管理信息和时间

传感器的标准出厂设置如下。

传感器的 IP：192.168.0.254

默认网关：255.255.255.0

默认传感器管理员密钥：admin

EC 的 IP：192.168.0.253

License Key——输入或修改 License Key(License Key 由神州数码提供)，如图 1-4 所示。

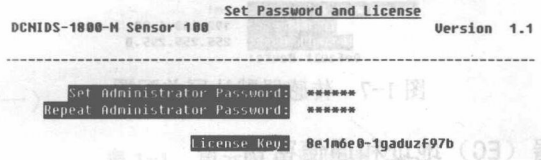


图 1-4　修改 License Key 界面

输入信息完毕使用<Enter>键即可将光标移至下一单元。此处 License Key 不要改动。

在主菜单中选择“Set date and time”，进入配置窗口，可以配置时区和时间。在中国地区应设置为 PRC，如图 1-5 所示。

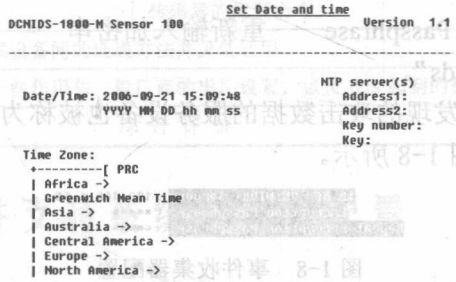


图 1-5　配置时区和时间

注：此处选择好后使用 Tab 键进行切换即可。确认保存后，系统需要重新启动一次方可生效。

2．配置传感器网络参数

在主菜单中选择“Configure networking”，进入配置窗口，可以进行如下配置：

（1）Name of this Station——设置 sensor 的名字

本任务中设置此传感器的名字为“DCNIDS-1800-M”。

（2）Management Interface——选择管理接口

本任务选择 em1 即可。

注：管理接口并非监测数据的接口，如果本任务的监测接口选择 em0，即将 em0 和 em1 同时连接到网络中，em1 负责与 EC 进行通信，而 em0 则主要负责监测网络数据流，如图 1-6 所示。

图 1-6　管理接口选择界面

（3）IP Address——设置管理接口的 IP 地址

管理接口的 IP 地址即指 EC 与传感器通信的地址。本任务中设置管理接口的 IP 地址为“192.168.1.88”。

（4）Network Mask——设置网络掩码

网络掩码设置为：“255.255.255.0”。

（5）Default Route——设置默认网关

在本任务中，由于传感器与管理控制台将在同一个网段，故默认网关选择默认不必配置，如图 1-7 所示。

图 1-7　传感器默认网关配置

3．配置事件收集器（EC）地址和通信密钥

（1）IP of DC NIDS Server ——输入 EC 的 IP 地址

EC 的 IP 地址设置为：“192.168.1.10”。

（2）Encryption Passphrase——输入加密串

加密串配置为：“dcids”。

（3）Repeat Encryption Passphrase——重新输入加密串

重新输入加密串：“dcids”。

EC 即接收未来传感器发现的攻击数据的服务设备也被称为事件收集器。

事件收集器配置，如图 1-8 所示。

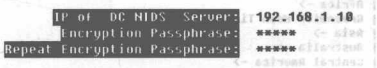


图 1-8　事件收集器配置

（4）IP of Second DC NIDS Server——输入备份 EC 的 IP 地址

（5）Encryption Passphrase——输入加密串

（6）Repeat Encryption Passphrase——重新输入加密串

注：本任务未设置备份 EC，此处可以不必选择，配置完成的界面如图 1-9 所示。

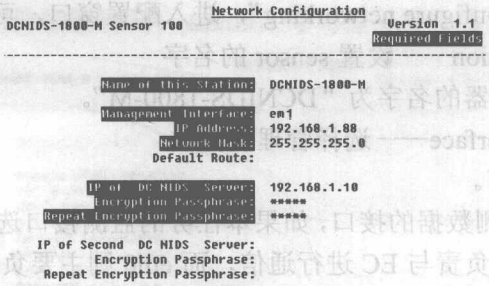


图 1-9　配置完成的界面

保存完毕，系统仍需重新启动，确认重启即可。

1.4　任务思考与练习

IDS 硬件设备配置中涉及两类密钥：一类是管理员密钥，另一类是管理通道密钥。任务中注意不要修改管理员密钥，否则会因丢失密钥导致设备返厂维修。而管理通道密钥的设置则必须与其未来软件服务平台的相应密钥对应才能正常使用此传感器，因此需记清楚管理通道密钥以备后续配置使用。

传感器管理端口在后续硬件版本中可能不仅只有两个端口，可以根据实际情况任选一个端口作为管理端口，其余端口均可同时作为监控端口连接到网络中。

任务评价

单元任务评价表（一），见表 1-1。

表 1-1　单元任务评价表（一）

	内　容		评　价		
	学习目标	评价项目	3	2	1
技术能力	理解 DCNIDS 系统的构成	正确修改出厂默认系统参数			
	熟悉 IDS 传感器的安装与配置	正确利用 PC 选取合适的线缆对传感器进行配置。熟悉传感器的配置命令			
通用能力	掌握 IDS 测试设备间的连通方法并灵活运用				
	理解 IDS 的一些作用与一般厂商的出厂设置，以及 IDS 起到的作用				
综合评价					

任务 2　IDS 软件支持系统的安装配置

2.1　任务目的

掌握 DCNIDS 系统软件的安装流程。

2.2　任务设备及要求

IDS 系统连接拓扑示意图，如图 1-10 所示。

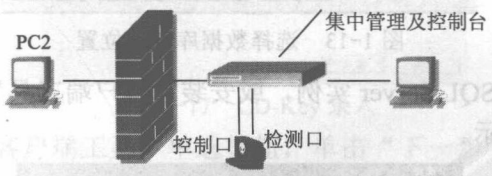


图 1-10　IDS 系统连接拓扑示意图

1．安装 IDS 分布式管理系统软件并进行合理配置
2．启动各软件服务

2.3　任务步骤

2.3.1　安装数据库

第三方软件可以使用 MSDE 2000，安装过程略。使用 SQL Server 2000 的安装过程如下：

1）选择安装 SQL Server 2000 组件，如图 1-11 所示。

图 1-11　SQL Server 安装起始界面

2）选择安装数据库服务器，如图 1-12 所示。

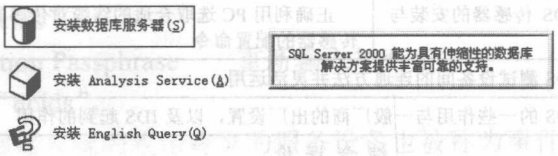


图 1-12　SQL Server 安装组件选择界面

3）选择将数据库安装在“本地计算机”，单击“下一步”按钮，如图 1-13 所示。

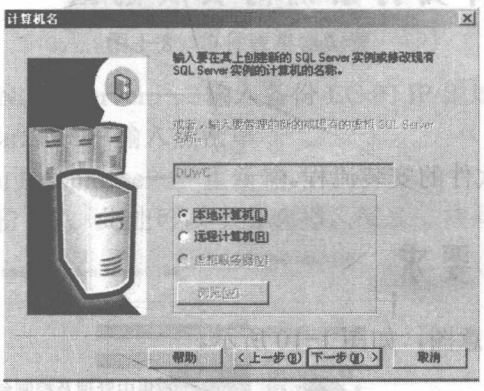


图 1-13　选择数据库安装位置

4）选中“创建新的 SQL Server 实例，或安装‘客户端工具’”单选按钮，单击“下一步”按钮，如图 1-14 所示。

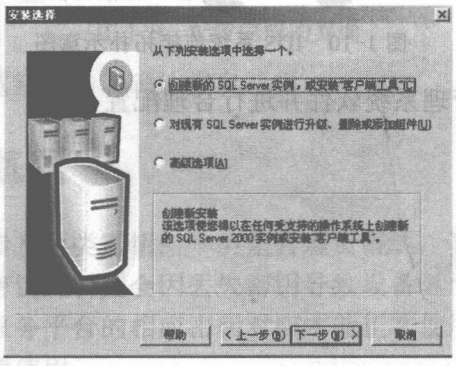


图 1-14　创建新的 SQL Server 实例

5）输入用户姓名和公司名称，单击“下一步”按钮，如图 1-15 所示。

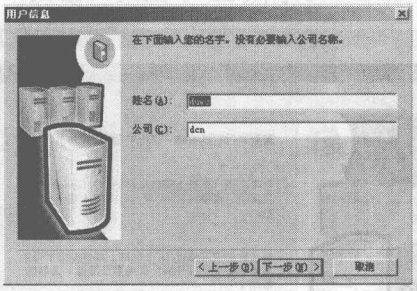


图 1-15　用户姓名和公司名称

6）单击“是”按钮表示接受许可证协议，进入到下一步，如图 1-16 所示。

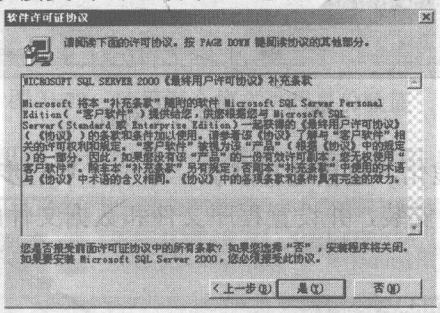


图 1-16　接受许可证协议

7）输入 CD-Key，单击“下一步”按钮，如图 1-17 所示。

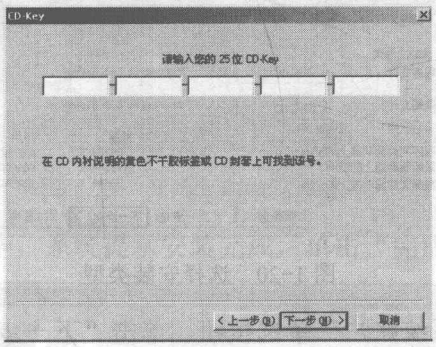


图 1-17　CD-Key 录入

8）选中“服务器和客户端工具”单选按钮，单击“下一步”按钮，如图 1-18 所示。

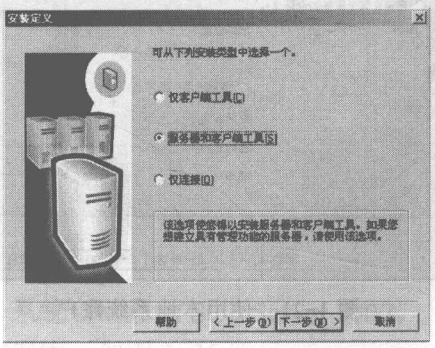


图 1-18　服务器和客户端工具

9）此处输入实例名。本任务的实例名为“MyNewSQL”，单击“下一步”按钮，如图1-19所示。

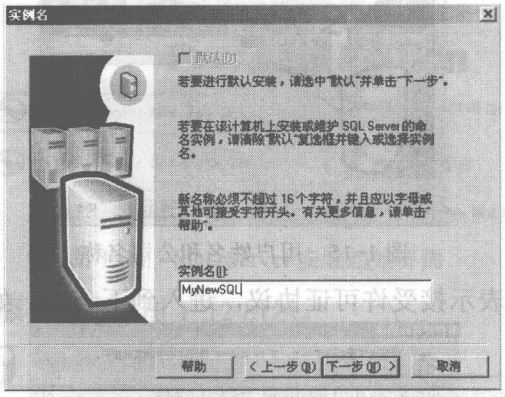


图 1-19　输入实例名

注：实例名处可能被虚化，直接选择默认，单击“下一步”按钮即可。

10）此处选择“典型”安装，并设置程序文件和数据文件的存放位置，单击“下一步”按钮，如图1-20所示。

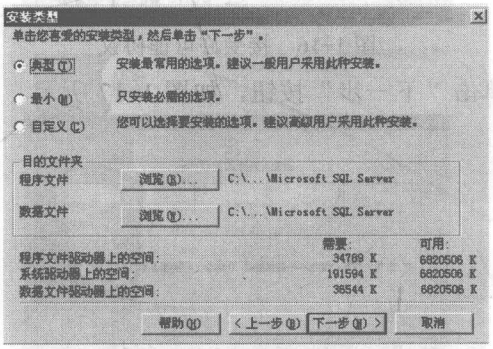


图 1-20　选择安装类型

11）选中“使用本地系统账户”单选按钮，单击“下一步”按钮，如图1-21所示。

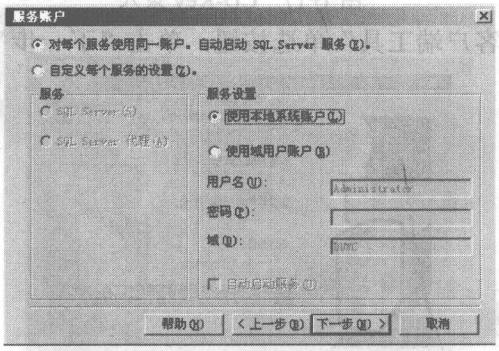


图 1-21　使用本地系统账户

12）选择使用混合模式进行身份验证，设置数据库管理员 sa 的口令并确认。本任务使

用“123456”，单击“下一步”按钮，如图 1-22 所示。

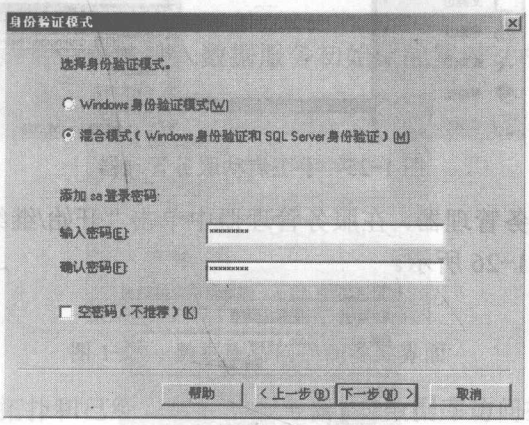


图 1-22　使用混合模式进行身份验证

13）单击“下一步”按钮即可开始复制数据库文件，如图 1-23 所示。

图 1-23　开始复制数据库文件

14）数据库文件复制完毕，系统提示安装完成，单击“完成”按钮如图 1-24 所示。

图 1-24　完成安装

15）重新启动计算机后，系统自动启动 SQL Server 2000。

注：也可以手工启动此数据库，如图 1-25 所示。

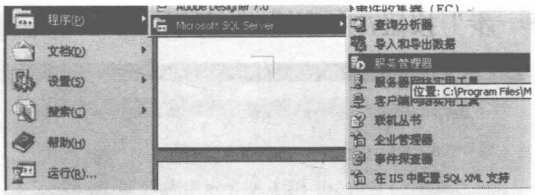


图 1-25　手工启动服务管理器

打开 SQL Server 服务管理器，在服务管理器中单击“开始/继续”按钮，等待启动过程将此服务器启动，如图 1-26 所示。

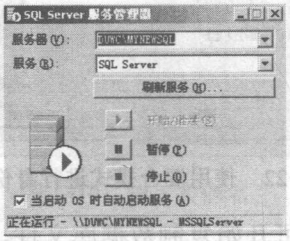


图 1-26　启动 SQL Server 服务

2.3.2　安装 LogServer

1）用鼠标双击光盘中的 LogServer 安装文件，即可开始 LogServer 的安装过程，如图 1-27 所示。

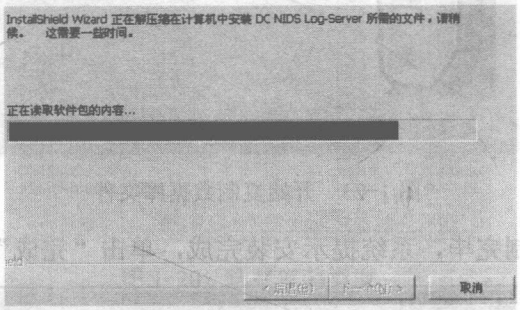


图 1-27　LogServer 安装启动界面

2）读取软件包的内容后，系统提示开始进行数据服务器的安装，单击“下一步”按钮即可，如图 1-28 所示。

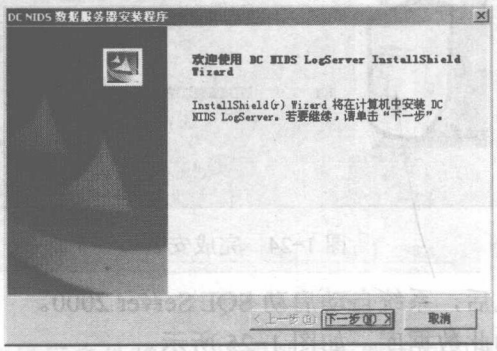


图 1-28　开始进行数据服务器的安装