脚本黑客攻防技术

樊　荣（笔名：混世魔王）
张秀贵（笔名：TTFCT）　编著

天津科学技术出版社

脚本黑客攻防技术

樊　荣（笔名：混世魔王）
张秀贵（笔名：TTFCT）　编著

天津科学技术出版社

图书在版编目(CIP)数据

脚本黑客攻防技术/樊荣,张秀贵编著. —天津:
天津科学技术出版社,2008.11
ISBN 978-7-5308-4765-7

Ⅰ. 脚… Ⅱ. ①樊…②张… 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(2008)第 140551 号

责任编辑:刘　颖
责任印制:王　莹

天津科学技术出版社出版
出版人:胡振泰
天津市西康路 35 号　邮编:300051
电话:(022)23332400(编辑室)　23332393(发行部)
网址:www.tjkjcbs.com.cn
新华书店经销
印刷:北京领先印刷有限公司

开本:787×1092　1/16　印张:13　字数:264 000
2008 年 11 月第 1 版第 1 次印刷
定价:29.00 元

序

灵感的降临，是悄然无息；

灵感的离去，是步履轻盈；

文字的印记则使得瞬间的闪烁成为恒久的记忆……

给杂志社撰写了两年的稿件，到后来进入编辑部，漫漫求索长路，坎坷坚定，我一直梦想着拥有一本属于自己的书。

每一个人都会有追求，我从不觊觎成为伟大的技术作家，我所能做的简简单单：只愿把这本书的大部分收入捐给灾区人民和希望工程，让资金流到它最应该去的地方。

时下，热火朝天的网络安全技术百花齐放，而脚本入侵，已然成为黑客主流的入侵手法。正因为如此，才有了这样一本书。本书介绍了当下的主流网站程序和数据库的攻击手法和防护，几乎涵盖了所有的脚本入侵漏洞分析以及防御方法，同时对漏洞产生个案进行深入的探讨。敝人一贯的观点是：倘若网站不安全，那么再华丽的网页设计也不过是易碎的花瓶，这种脆弱的美总是在信息安全的暴风骤雨中摇摇欲坠！因此，加强网络安全意识迫在眉睫。

我认为，一本读者喜欢的书，应该不是干枯无根的理论朽木，而是在实践的土壤中成长起来的参天大树。故此，在写书过程中，我一直都以此为宗旨。为此，本书力求通俗易懂，在技术上尽量详细全面，目的是让大家看完后，不需要编程基础，就能实际操作，加强自身的安全防范意识。

声明：本书对于黑客入侵方法只作技术探讨，不许借此进行破坏网络安全和违反法律的活动，如有违者，后果自负！

程序和动画学习教程下载
www.hsmw.net

与我联系
hsmw26836659@hotmail.com

致 谢

写书是一项艰苦的工作，很高兴能邀请到好友 TTFCT 的帮助来一起完成这本书，同时要感谢 superhei、Neeao、Flyh4t、Catling 等朋友的技术研究，为本书添色不少。也感谢朋友冰雪封情、諾諾、剑心、Angel、微笑一刀、cnfjhh、至尊宝、堕落的青蛙仔、周祯、Map0735、ZY、闫明、WTF、超级兔子、吴泽林、阿九、Anter、Blue_light、空虚浪子心、小刀、009、river、XySky、光芒果、梦之光芒、空气、llikz、wsdgs、ZV、勇哥儿、sky、浪迹天、King、怪狗、TearDrop、TT、KuNgBiM、CnhCerKF、谈笑书生、h4k_b4n、東邪、猪头三、瓶颈、沙滩小子、教主、倾城、LXG 绅士、爬爬虫、Dickens、大灰狼、罗然、安静、毛毛、linzi、天使娃娃、肖凌龙、王磊、罗振华……要感谢的朋友太多了，排名不分先后。

樊荣

目 录

第一章　快速搭建本地测试服务器

第一节　搭建你的 Windows Server 2008 服务器

Windows Server 2008 发布之后，众多 IT 专家开始面临着同样一个困惑。面对 Windows Server 2008，升级，还是不升级，这是个问题。是继续坚守在原有架构平台下继续辛苦地维护，还是升级到 Windows Server 2008 立刻 High 起来？

不可否认的是，Windows Server 2008 是迄今为止最安全的 Windows Server。它加强了操作系统并进行了安全创新，包括 Network Access Protection、Federated Rights Management、Read-Only Domain Controller，为你的网络、数据和业务提供了最高水平的保护。

我们先来体验一下吧！它的 DVD 光盘大小为 2 个 G，如果光盘质量不好，安装是比较麻烦的，这里教大家使用硬盘安装法来安装 Windows Server 2008 RC0 Standard Edition。

1．前期准备工作

（1）安装好 Windows XP 系统的电脑一台。

（2）微软官方下载 Windows Server 2008 安装 ISO 镜像（有 2G 左右）。

（3）安装 DAEMON Tools 虚拟光驱。

（4）准备微软授权的 Windows Server 2008 KEY 一个。

2．要注意几点

（1）Windows Server 2008 要求安装在 NTFS 分区，但是系统的其他分区可以是 FAT32 格式。

（2）简单无损 NTFS 转换方式：运行 cmd 进入命令行模式，运行 convert x:/fs:ntfs 即可（x 为需要转换分区盘符）。其间可能需要重启计算机。注：该命令可以将 FAT 分区无损转换为 NTFS 分区，该过程不可逆。若分区中没有有用数据，直接在 XP 下格式化为 NTFS 分区也能达到目的。

（3）建议安装系统的分区至少为 15 GB。（完成 Windows Server 2008 安装后，系统区占用 6 GB。）

一、Windows Server 2008 系统安装准备

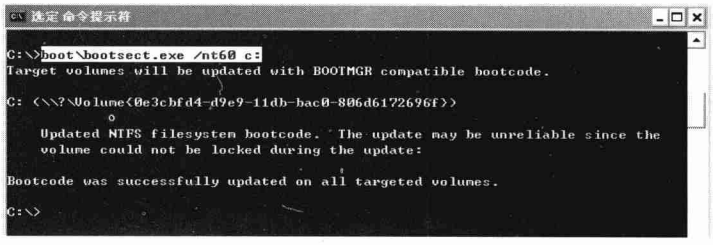
（1）用 DAEMON Tools 虚拟光驱加载 Windows Server 2008 的 ISO 镜像，然后将光盘内容拷贝到硬盘中，这里是拷贝到 E:\L2008。要注意，一定要拷贝到硬盘

中去，用虚拟光驱加载的 ISO 文件虽然可以运行，但是安装到一半的时候会提示没有 CD/DVD 驱动，导致安装无法进行。

（2）把光盘 K:\目录下的 bootmgr 和 boot 目录拷贝到 C 盘根目录下，并在 C 盘根目录下新建一个 sources 文件夹。

（3）把光盘 K:\sources 下的 boot.win 复制到 C 盘下 sources 文件夹内。

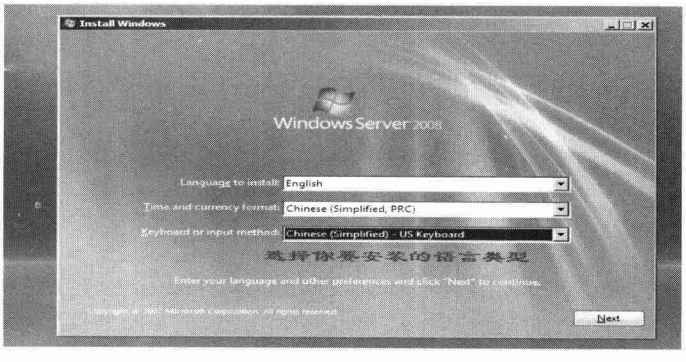
（4）运行，CMD 输入命令 C:\boot\bootsect.exe /nt60 c: (注:此处 bootsect 在 C:\boot 目录下)



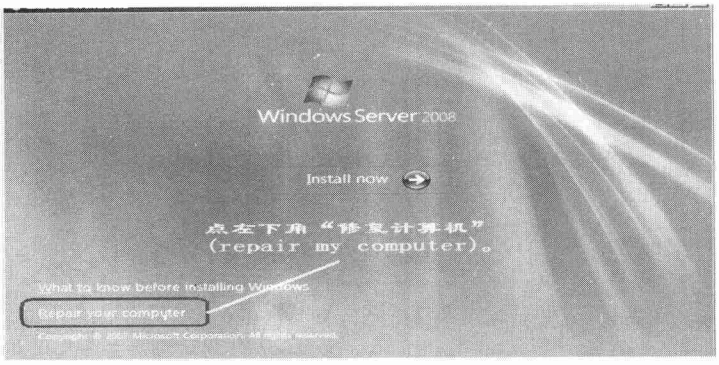
二、Windows Server 2008 安装

（1）重启计算机，安装程序会自动加载 boot.win，启动 PE 环境。

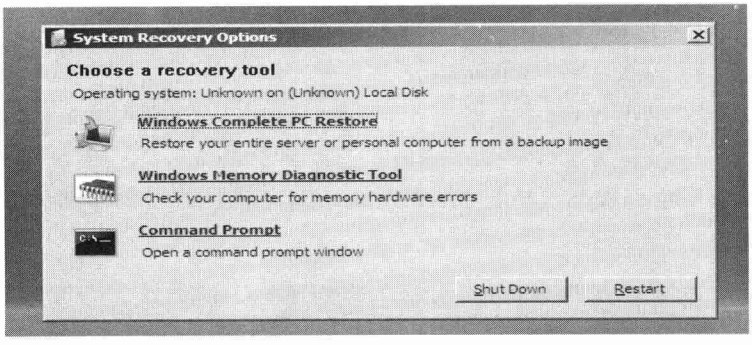
（2）安装程序启动，选择你要安装的语言类型，同时选择适合自己的时间和货币显示种类及输入方式。



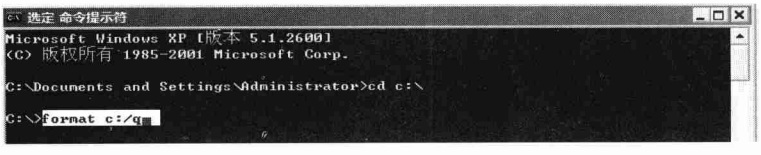
（3）出现“开始安装界面”（要注意了，不要点击“现在安装”），点左下角“修复计算机”（repair my computer）。



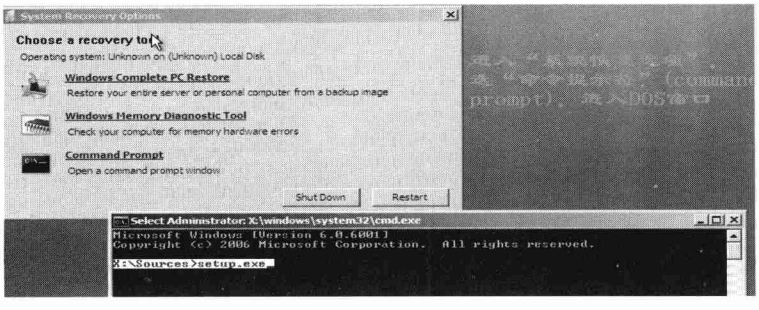
（4）进入“系统恢复选项”，选择最后一项“命令提示符”(command prompt)，进入 DOS 窗口。



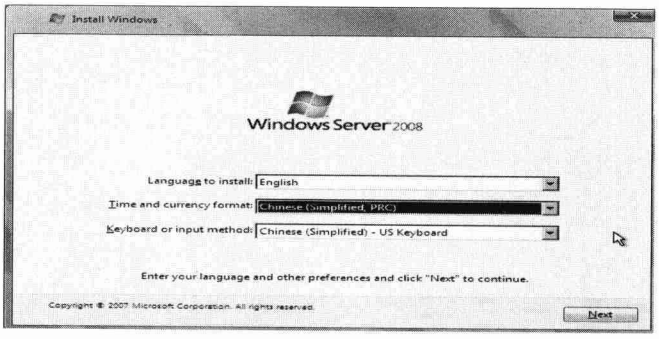
（5）执行格式化命令 format c:/q。（注：可能会提示输入 C 盘卷标）



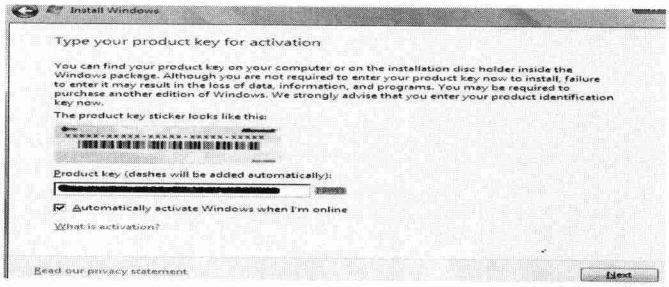
（6）安装系统，执行 E:\L2008\sources\setup.exe。



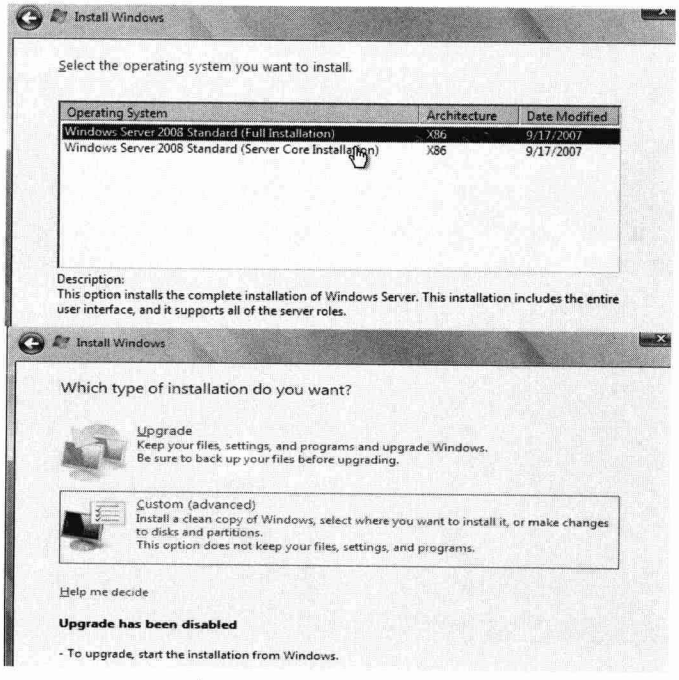
（7）下面就是正常的安装了。选择操作系统的语言。



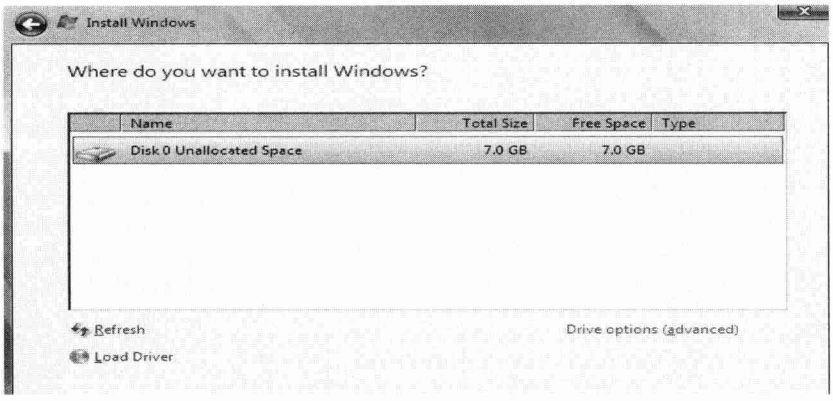
Next，输入 key，这里 key 就涂抹了。

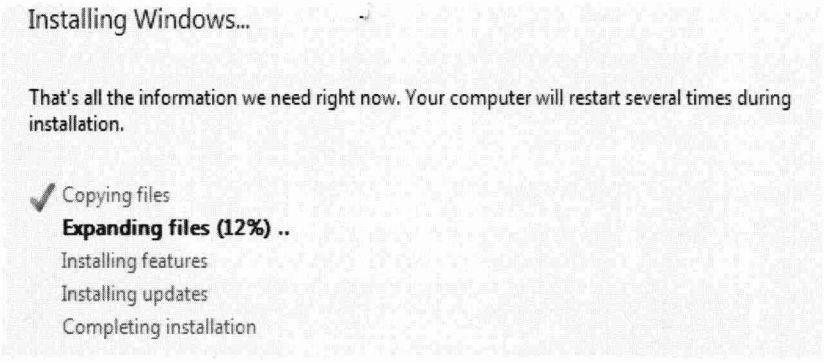


Next，选择全部安装（Full Installation）或安装服务器核心部分(Server Core Installation)。这里是选择全部安装。



选择 Custom（高级），进入硬盘分区。这里是在虚拟机上运行，所以只能看到一个分区。选 C 盘进行安装，接下来就是系统自动来安装了。





三、激活 Windows Server 2008

等安装完成后，就登陆系统了，这里需要激活系统，然后访问 Windows Update 就可以自动更新了。

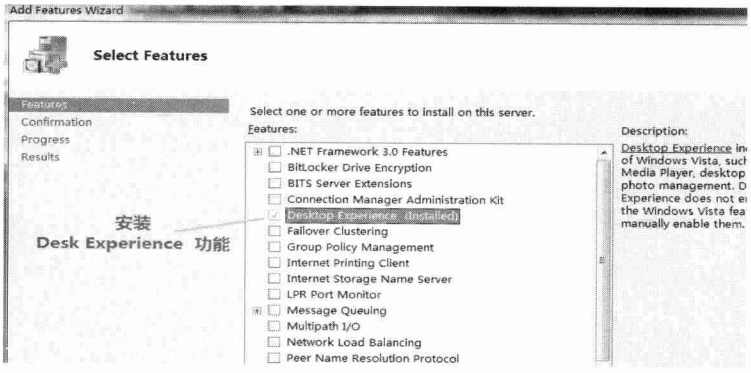
四、开启关闭的服务

Windows Server 2008 和 2003 版一样，有些服务默认是关闭的。

（1）控制面板 —— 程序和功能 —— 打开或关闭 Windows 功能 —— Server Manager —— Features。

（2）安装 Desk Experience 功能，以打开 Windows Media Player 和 Sidebar 等功能。

（3）Windows Server 2008 的硬件驱动可以使用 Vista 的，或者用 XP 兼容模式运行。



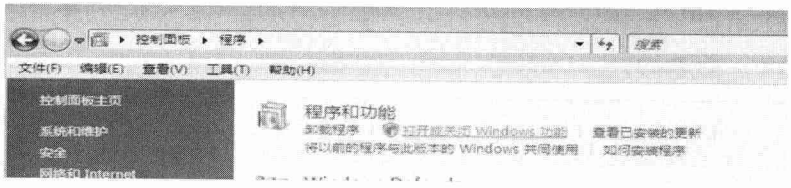
到这里，通过硬盘安装法成功地安装了 Windows Server 2008 服务器，一起来体验一下吧。

第二节 IIS7 的安装及 ASP+Access 环境配置

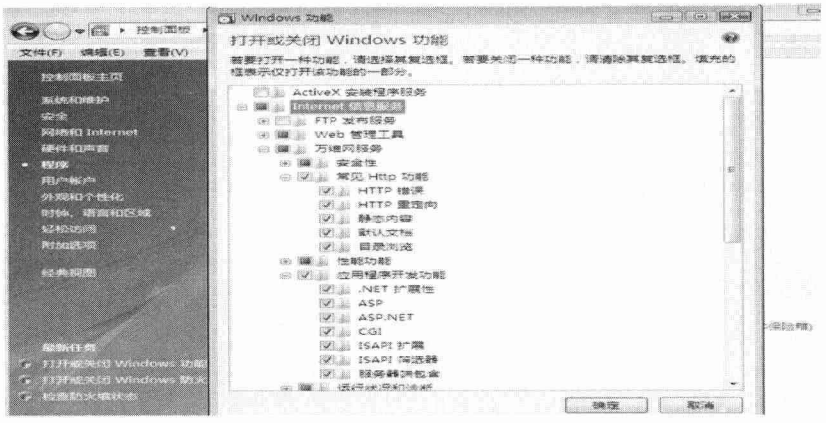
IIS7 是默认不安装的，所以在安装完成系统之后，我们需要手动安装 IIS7。安装的步骤为：开始 —— 控制面板 —— 程序 —— 打开或关闭 Windows 功能 —— Internet 信息服务。IIS7 安装时需要注意，如果需要 ASP 及 ASP.NET 等的支持，需要把功能模块装上，其默认也是不安装。

控制面板中“程序”的位置：

“程序”中“打开或关闭 Windows 功能”的位置：



如图，安装 IIS7 时需选择要使用的功能模块。

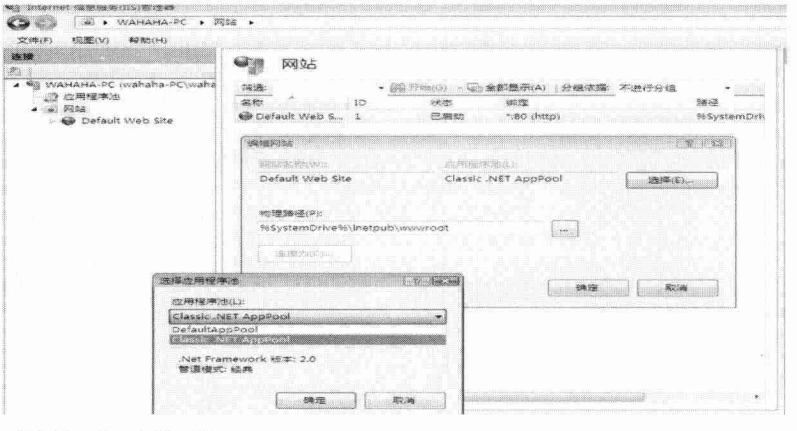


IIS7 安装完成之后，可以在开始菜单的所有程序中看到“管理工具”，其中有一个“Internet 信息服务管理器”，如果没有可以按以下步骤添加：开始 —— 右击属性——“开始”菜单选项卡——自定义——把“系统管理工具”设置为“在所有程序菜单显示”或者“在所有程序菜单和开始菜单上显示”。

一、IIS7 配置 ASP+Access 使用环境

打开 Internet 信息服务管理器就可以看到 IIS7 的主页了，不过默认装完 IIS7 之后，使用 ASP 程序会发现提示数据库连接失败，这是因为 MSJet 引擎改变了临时目录的位置，但是又没有其存取权限，导致数据库使用失败。

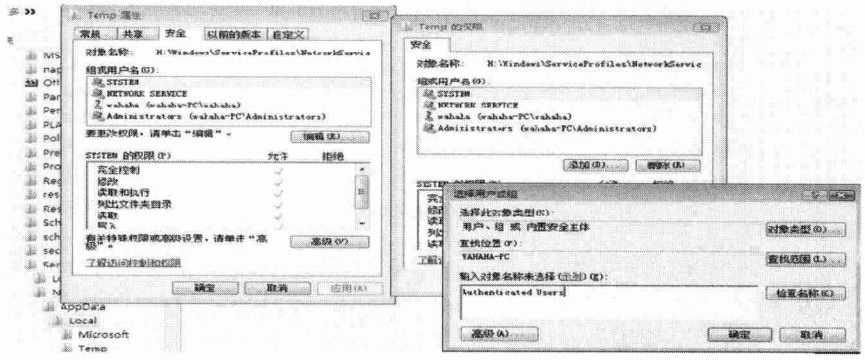
所以，先要设置应用程序池(ApplicationPool)为 Classic.NET AppPool，而不是默认的 DefaultAppPool，可以在网站目录里对每个站点设置，也可以在某站点进行单独设置。选择好要设置的站点之后，点右边的“基本设置”即可调出应用程序池，进行设置对话框。



然后再给“系统盘:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp”目录添加一个“AuthenticatedUsers”的用户，其中 AppData 目录是隐藏的，

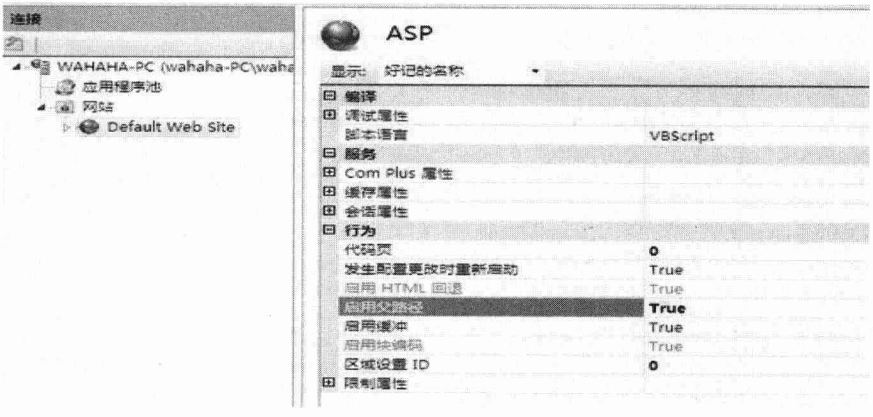
在进入的时候可以直接在地址栏输入路径，或者在文件夹选项里显示隐藏文件。

设置权限步骤：右击 Temp 文件夹，选择“属性”，选择“安全”选项卡，单击“编辑”，会弹出“Temp 的权限”对话框，单击“添加”，在下面的“输入对象名称来选择”中输入 Authenticated Users，确定，返回到“Temp 的权限”，将 Authenticated Users 的权限中的“完全控制”给勾上，然后确定。



启用父路径支持：

在站点主页上选择“ASP”，然后在“行为”组中将“启用父路径”设置为 True 即可。

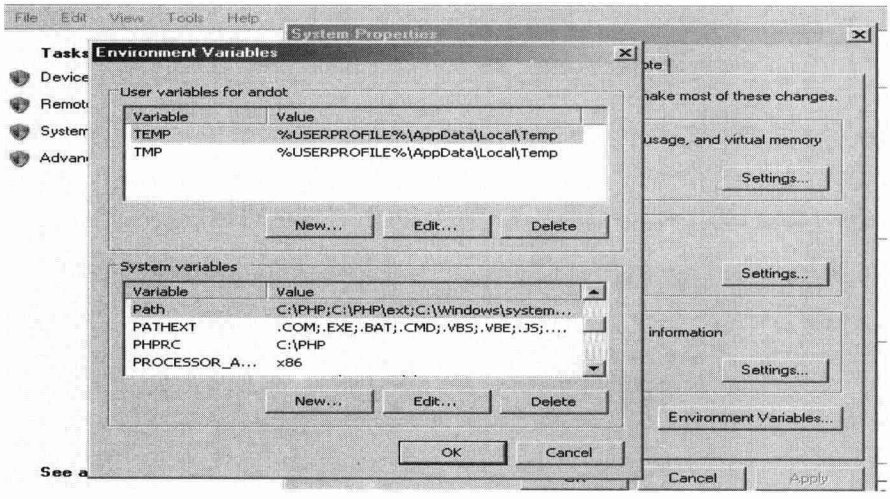


至此，我们完成了 IIS7 的安装及使用 ASP+Access 的配置。不过，暂时还不支持 PHP+MySQL，我们在下一节来让它实现吧。

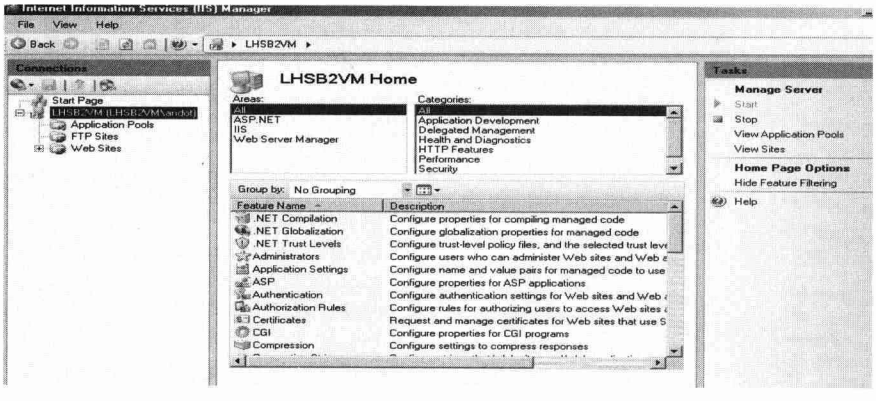
第三节 IIS7+PHP+MySQL+Zend 配置教程

在上一节中，我们介绍了 IIS7 的安装，为了体验 IIS7 的全部功能，我把它全部特性都安装了。安装好之后，我们还需进行配置，要让它能支持 PHP，能配合 MySQL 和 Zend 使用。PHP，MySQL 和 Zend 都是开放源代码程序，可以在网上下

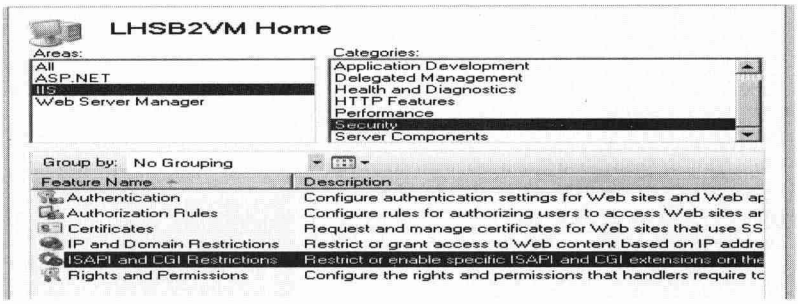
载到。我们用到的是 PHP5。这里先来对 PHP 进行安装配置，将其解压缩到 C:\PHP 目录下，然后复制一份 php.ini-dist 改名为 php.ini。接下来打开“我的电脑”—属性—高级系统设置—环境变量里，添加上可执行文件的查找路径（PATH）和 php.ini 的查找路径（PHPRC）。



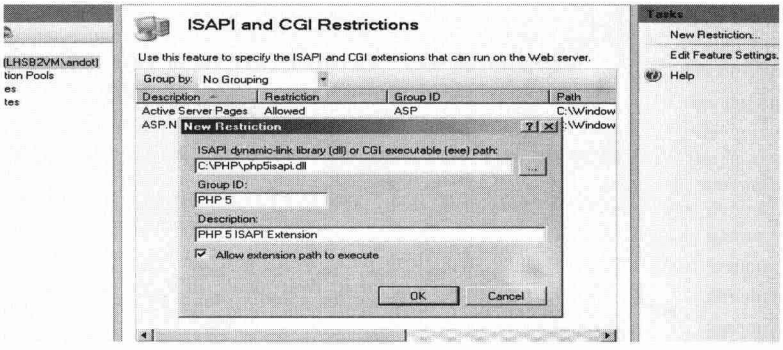
接下来开始配置 IIS7。相比 IIS6，IIS7 启动后的开始画面看上去酷多了。你可以对某个站点进行配置，也可以对整个服务器进行配置，当然对整个服务器配置后，用起来就更加方便了。比如新建一个站点，就可以支持 PHP，这对于做虚拟主机是非常合适的，所以这里是按照对整个服务器进行配置来做的。因此先选中要配置的服务器，默认当然是你的本地服务器了，你会看到选中以后，右面的画面跟 IIS6 完全不同了。



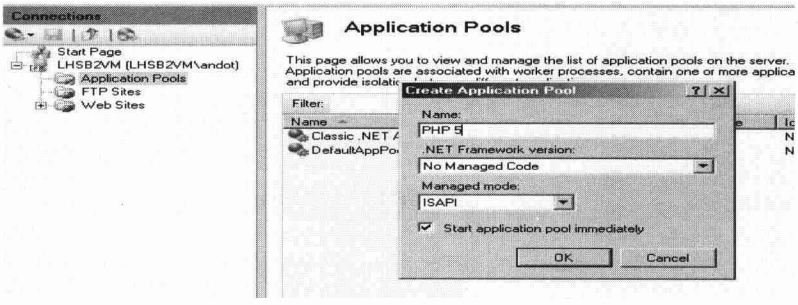
从这整个属性页中选择要找的特性当然比较费事，所以，可以按照范围（Areas）和分类（Categories）来选择。这里我们要配置的是 ISAPI and CGI Restrictions，它可以从 IIS 范围的 Security 分类中找到。



在全部安装的情况下，ISAPI and CGI Restrictions 页中默认有 ASP 和 ASP.NET 两项。在最右面的任务（Tasks）里选择 New Restriction... 来为 PHP 创建 Restriction，要填写的内容如下图所示，加入 PHP 目录里的 PHP5ISAPI.DLL 。



接下来，选择“Application Pools”，可以为 PHP 程序创建一个应用程序池。



然后配置默认文档，增加一个 index.php 的默认文档。