

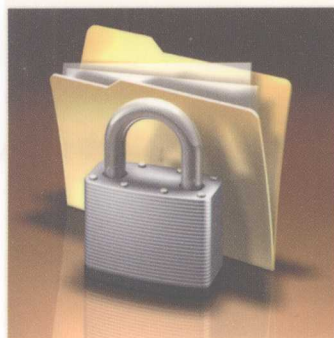
精通

本书为教育部立项课题“学分制下高校网络化教学实践与创新的研究”阶段性成果

Windows Server 2008

安全与访问保护

张晓莉 孙立威 王淑江 编著



● 本书内容:

服务器操作系统基本配置
用户账户安全配置
常用服务器安全配置
高级安全Windows防火墙和客户端安全配置

随书附赠
多媒体光盘

- ▶ 视频演示各项操作
- ▶ 提升内容理解层次
- ▶ 快速掌握操作方法

● 本书特点:

使用大量实践操作配合知识讲解
本书内容新颖,重点突出
每章配有小结、习题和实验

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书全面阐述了 Windows Server 2008 网络操作系统的安全配置和应用, 主要内容包括 Windows Server 2008 操作系统安全概述、活动目录安全、用户账户安全、组策略安全、系统漏洞、端口和网络安全、Internet 信息服务安全、文件安全、Windows 防火墙、系统补丁维护、使用 SCCM 2007 分发客户端更新、证书服务与 SSL 安全协议、Windows 网络访问保护和数据库安全。本书语言流畅、通俗易懂、深入浅出、可操作性强, 注重读者实战能力的培养和技术水平的提高, 力求让读者通过学习本书, 能够最大限度地确保系统能够安全、稳定、高效地运行。

本书适用于系统管理人员、安全管理人员和网络管理人员, 以及对计算机系统维护和网络管理感兴趣的计算机爱好者, 并可作为大专院校计算机专业的教材或课后辅导资料。

图书在版编目 (CIP) 数据

精通 Windows Server 2008 安全与访问保护/张晓莉, 孙立威, 王淑江编著. —北京: 中国铁道出版社, 2009. 6
ISBN 978-7-113-10237-1

I. 精… II. ①张…②孙…③王… III. 服务器—操作系统 (软件), Windows Server 2008—安全技术 IV. TP316. 86

中国版本图书馆 CIP 数据核字 (2009) 第 109328 号

书 名: 精通 Windows Server 2008 安全与访问保护
作 者: 张晓莉 孙立威 王淑江 编著

责任编辑: 苏 茜
编辑助理: 高 爽
责任印制: 李 佳

编辑部电话: (010) 63583215
封面设计: 付 巍
封面制作: 白 雪

出版发行: 中国铁道出版社 (北京市宣武区右安门西街 8 号 邮政编码: 100054)
印 刷: 北京新魏印刷厂
版 次: 2009 年 9 月第 1 版 2009 年 9 月第 1 次印刷
开 本: 787mm×1092mm 1/16 印张: 32. 25 字数: 703 千
印 数: 3 500 册
书 号: ISBN 978-7-113-10237-1/TP·3403
定 价: 68. 00 元 (附赠光盘)

版权所有 侵权必究

凡购买铁道版的图书, 如有缺页、倒页、脱页者, 请与本社计算机图书批销部调换。

前

言

Foreword

随着社会信息化程度的不断提高,计算机网络已经成为知识经济社会的必要条件和基础设施。但是,由于计算机网络系统自身的开放性以及各个环节不可避免的安全缺陷,安全风险和安全隐患无处不在。人们在享受 Internet 带来的便捷、经济和愉悦的同时,也面临着网络安全方面的巨大挑战。

网络攻击事件之所以频频发生,根本原因还在于操作系统、网络协议、用户等应用环节存在的安全漏洞。信息社会的飞速发展,迫使许多用户来不及经过必要的学习和认知阶段,就匆匆走上了计算机网络应用之路。缺乏网络安全知识,是这类人群的通病,他们平时很少采用系统补丁更新、病毒防火墙和网络防火墙等安全措施。而这些用户无异于高速公路上没有取得驾驶执照的司机,他们随时都可能成为整个网络的网络杀手。只要稍有疏忽或防范不及时,网络安全灾难便如影而至。由此不难看出,系统安全已经成为网络管理员在网络构建、网络升级和网络日常管理中的头等大事。

操作系统是所有计算机资源的管理者,是其他应用程序的基础和核心,一切应用程序都是建立在其之上的,如果没有操作系统的安全,计算机和网络系统安全就无从谈起,更谈不上其他应用软件的安全。因此,操作系统的安全是整个计算机系统安全的基础。随着操作系统版本的不断升级,应用功能越来越丰富,随之而来的安全漏洞也越来越多。其实,许多安全入侵事件都是由于管理员或用户的疏忽导致的,如果合理配置、全面扫描、完善各种审核机制,就可以避免大多数的攻击。

Windows Server 2008 操作系统最突出的改进就是安全性的提升。本书共分为 14 章,主要内容包括 Windows Server 2008 操作系统安全概述、活动目录安全、用户账户安全、组策略安全、系统漏洞、端口和网络安全、Internet 信息服务安全、文件安全、Windows 防火墙、系统补丁维护、使用 SCCM 2007 分发客户端更新、证书服务与 SSL 安全协议、Windows 网络访问保护和数据库安全。本书从 Windows 操作系统安全的角度出发,配合大量实践操作,阐述了操作系统安全配置和管理在网络安全中起到的决定性作用;涉及的服务器和客户端操作系统,分别以目前最新的 Windows Server 2008 和 Windows Vista 为例,内容新颖,重点突出。每章最后配有小结、习题和实验,可以帮助读者巩固本章学过的知识。

本书主要面向具有一定基础的初级网络用户,尤其是热衷于系统安全和网络安全,喜欢探索尝试新技术的计算机爱好者。通过阅读本书,读者可以快速掌握最新的安全技术,最实用的管理技巧以及最常用的安全配置。

本书为教育部立项课题（编号 06JA880017）“学分制下高校网格化教学实践与创新的研究”的阶段性成果，由张晓莉、孙立威、王淑江编著，田俊乐、赵卫东、刘淑梅、马倩、杨伏龙、李文俊、王同明、郭腾、白华、莫展宏、李海宁、陈志成、刘国增、王延杰、刘红等参与了资料收集与调试工作。作者在河北经贸大学、烟台日报长年从事网络教学、实验和管理工

作，具有较高的理论水平和丰富的实践经验，曾经出版过多部计算机类图书，均以易读、易学且实用的特点受到众多读者的好评。本书是作者的又一呕心沥血之作，希望对大家的操作系统安全配置与维护工作能有所帮助。

编者

2009年6月

目

录

第 1 章	Windows Server 2008 操作系统安全概述	1
1.1	Windows Server 2008 操作系统安全策略	1
1.1.1	操作系统安装注意事项	1
1.1.2	配置 Internet 防火墙系统	2
1.1.3	运行安全配置向导	4
1.1.4	安装防病毒系统注意事项	13
1.1.5	计算机病毒及单机防病毒系统	14
1.1.6	网络防病毒系统	16
1.1.7	安装防间谍软件	16
1.1.8	配置应用程序	18
1.1.9	更新安全补丁	18
1.2	系统服务安全	21
1.2.1	实现系统服务安全	21
1.2.2	系统服务详解	23
1.3	用户安全	30
1.3.1	账户策略安全	30
1.3.2	用户账户安全	32
1.3.3	权限和安全	35
1.3.4	文件权限的访问控制	36
1.3.5	系统账号数据库	39
1.3.6	备份账号数据库	40
1.4	系统设置安全	42
1.4.1	关闭 NetBIOS 端口	42
1.4.2	注册表安全	43
1.4.3	日志审核	47
1.4.4	文件加密	48
	小结	49
	习题	49
	实验：部署 Windows Server 2008 自动更新	49
第 2 章	活动目录安全	50
2.1	安全描述符	50
2.1.1	安全描述符概述	50
2.1.2	查看安全描述符	51



2.2	有效权限计算器.....	52
2.2.1	有效权限计算规则.....	53
2.2.2	检索有效权限.....	53
2.3	访问控制继承.....	54
2.3.1	设置权限继承.....	54
2.3.2	取消继承权限.....	56
2.4	权限委派.....	57
2.4.1	权限委派概述.....	57
2.4.2	委派操作权限.....	58
2.5	用户权利.....	63
2.5.1	特权.....	63
2.5.2	登录权利.....	68
2.6	组管理活动目录对象.....	69
2.6.1	组类型.....	69
2.6.2	默认组.....	71
2.6.3	组作用域.....	74
2.6.4	创建用户组.....	76
2.7	服务账户.....	77
2.7.1	服务权限.....	78
2.7.2	修改服务登录账户.....	79
2.7.3	服务的依存关系.....	80
2.7.4	硬件配置文件启用或禁用服务.....	80
2.8	活动目录数据库安全.....	81
2.8.1	活动目录数据库文件概述.....	81
2.8.2	设置目录数据库访问权限.....	81
2.8.3	活动目录数据库的备份.....	82
2.8.4	活动目录数据库的恢复.....	86
	小结.....	88
	习题.....	88
	实验：权限委派.....	88
第3章	用户账户安全.....	89
3.1	系统管理员账户的管理.....	89
3.1.1	系统管理员密码设置.....	89
3.1.2	系统管理员账户安全管理.....	90
3.2	用户账户的管理.....	92
3.2.1	创建新用户账户.....	93
3.2.2	重设账户密码.....	95
3.2.3	禁用、启用和删除用户账户.....	99
3.2.4	限制用户登录时间.....	100
3.2.5	限制用户可以登录的工作站.....	101



3.3 用户组的管理.....	102
3.3.1 添加用户组.....	102
3.3.2 向用户组中添加成员.....	103
3.3.3 为组指定管理员.....	105
3.3.4 更改组作用域或组类型.....	106
3.3.5 删除组.....	106
3.4 用户权限的安全.....	106
3.4.1 为用户设置权限.....	106
3.4.2 设置共享文件夹权限.....	107
3.5 用户环境.....	110
3.5.1 重定向用户配置文件.....	110
3.5.2 重定向程序安装目录 Program Files.....	111
3.5.3 重定向 IE 临时文件夹.....	112
3.5.4 重定向虚拟内存.....	113
小结.....	115
习题.....	115
实验: 设置账户锁定策略和解锁账户.....	116
第 4 章 组策略安全.....	117
4.1 组策略模板.....	117
4.1.1 组策略模板概述.....	117
4.1.2 ADMX 与 ADM 的不同之处.....	118
4.1.3 ADMX 文件编辑方式.....	118
4.2 安全策略.....	119
4.2.1 账户策略.....	119
4.2.2 审核策略.....	125
4.2.3 用户权限分配.....	129
4.3 软件限制策略.....	133
4.3.1 软件限制策略简介.....	134
4.3.2 安全级别设置.....	134
4.3.3 默认规则.....	139
小结.....	141
习题.....	142
实验: 赋予普通账户远程关机权限.....	142
第 5 章 系统漏洞.....	143
5.1 漏洞概述.....	143
5.1.1 漏洞的特性.....	143
5.1.2 漏洞生命周期的 5 个基本阶段.....	144
5.1.3 漏洞管理流程.....	145



5.1.4	漏洞修补方略	147
5.2	漏洞扫描	148
5.2.1	漏洞扫描概述	148
5.2.2	漏洞扫描工具 MBSA 功能简介	149
5.2.3	MBSA 的安装	159
5.2.4	MBSA 的应用	159
5.3	修补原则	165
5.3.1	备份相关数据	166
5.3.2	核对补丁信息	166
5.3.3	选择安装模式	167
	小结	167
	习题	167
	实验: 使用 MBSA 扫描本地 IIS 服务漏洞	168
第 6 章	端口和网络安全	169
6.1	端口分类	169
6.1.1	按端口号划分	169
6.1.2	按协议类型划分	170
6.1.3	应用程序和服务端口	171
6.2	查看端口	172
6.2.1	Windows 内置端口查看命令	172
6.2.2	端口查询工具——PortQry	175
6.2.3	端口监控工具——Port Reporter	189
6.3	关闭/开启端口	194
6.3.1	关闭服务法	194
6.3.2	IP 安全策略法	195
6.4	端口重定向	208
6.4.1	WWW 服务的重定向	208
6.4.2	FTP 服务的重定向	209
6.4.3	终端服务端口重定向	210
	小结	212
	习题	212
	实验: 关闭 23 端口	212
第 7 章	Internet 信息服务安全	213
7.1	IIS 安全机制	213
7.1.1	IIS 访问控制安全	213
7.1.2	NTFS 访问安全	214
7.1.3	身份验证	215
7.1.4	IIS 安装安全	216



7.2	WWW 服务安全	217
7.2.1	用户控制安全	217
7.2.2	访问权限控制	219
7.2.3	授权规则	222
7.2.4	IPv4 地址控制	223
7.2.5	IP 转发安全	225
7.2.6	SSL 安全	226
7.2.7	审核 IIS 日志记录	229
7.2.8	设置内容过期	231
7.2.9	内容分级设置	232
7.2.10	注册 MIME 类型	233
7.3	FTP 服务安全	234
7.3.1	设置 TCP 端口	234
7.3.2	连接数量限制	234
7.3.3	用户访问安全	235
7.3.4	文件访问安全	237
7.4	基于 IIS 6.0 的 Web 安全	238
7.4.1	内容分级设置	238
7.4.2	获取用于 SSL 加密的服务器证书	239
	小结	243
	习题	244
	实验: 搭建安全的 FTP 服务器	244
第 8 章	文件安全	245
8.1	基于 NTFS 文件系统的安全设置	245
8.1.1	NTFS 权限概述	245
8.1.2	NTFS 文件夹权限和 NTFS 文件权限	245
8.1.3	访问控制列表	246
8.1.4	多重 NTFS 权限	247
8.1.5	NTFS 权限的继承性	249
8.1.6	设置 NTFS 权限	250
8.1.7	设置磁盘配额	256
8.1.8	文件屏蔽	259
8.1.9	文件权限审核	263
8.2	权限管理服务	266
8.2.1	安装 AD RMS 前的准备	266
8.2.2	安装 AD RMS 服务器	266
8.2.3	配置 AD RMS 服务器	271
8.2.4	AD RMS 客户端部署及应用	280
8.3	信息权限管理	284
8.3.1	IRM 简介	284



8.3.2	创建被保护的安全文档	285
8.3.3	使用被保护文档	287
8.3.4	请求权限	288
8.4	共享资源安全	289
8.4.1	管理共享文件夹权限	289
8.4.2	默认共享安全	292
	小结	297
	习题	297
	实验: 使用 AD RMS 保护共享文档的安全	297
第 9 章	Windows 防火墙	299
9.1	Windows 防火墙基本配置	299
9.1.1	Windows 防火墙概述	299
9.1.2	开启/关闭防火墙	301
9.1.3	还原 Windows 防火墙默认设置	302
9.2	访问控制配置	302
9.2.1	允许/限制端口访问	303
9.2.2	允许/限制程序访问	304
9.3	使用组策略配置 Windows 防火墙	306
9.3.1	创建组策略	306
9.3.2	允许通过验证的 IPSec 旁路	307
9.3.3	标准配置文件/域配置文件	307
9.4	高级安全 Windows 防火墙基本配置	316
9.4.1	高级安全 Windows 防火墙概述	316
9.4.2	配置防火墙规则	317
9.4.3	创建 IPSec 连接安全规则	322
9.5	配置 Windows 防火墙事件审核	325
9.5.1	启用审核设置	325
9.5.2	查看 Windows 防火墙事件	328
9.5.3	筛选 Windows 防火墙事件	329
9.5.4	配置 Windows 防火墙日志文件	330
	小结	331
	习题	331
	实验: 使用防火墙阻止 QQ 访问网络	331
第 10 章	系统补丁维护	333
10.1	Microsoft Update	333
10.1.1	系统更新注意事项	333
10.1.2	系统更新设置	334



10.2	系统更新服务	336
10.2.1	WSUS 概述	336
10.2.2	WSUS 服务器的安装	337
10.2.3	WSUS 服务器的设置	341
10.2.4	WSUS 客户端的安装和设置	350
	小结	355
	习题	355
	实验: 使用 WSUS 服务器管理客户端更新	355
第 11 章	使用 SCCM 2007 分发客户端更新	356
11.1	安装 SCCM 2007 服务器	356
11.1.1	准备工作	356
11.1.2	安装 SCCM 2007 服务器	367
11.1.3	安装 SCCM 2007 R2	371
11.2	配置 SCCM 2007 服务器	372
11.2.1	配置站点边界	372
11.2.2	配置站点系统角色	373
11.2.3	配置客户代理组件	378
11.2.4	配置客户端发现方法	381
11.2.5	配置客户端安装方法	383
11.3	配置 SCCM 2007 客户端	385
11.3.1	发现客户端	385
11.3.2	使用“推送”方式部署客户端	387
11.4	使用 SCCM 分发软件更新	388
11.4.1	配置客户端策略	389
11.4.2	获取软件更新	389
11.4.3	部署软件更新	389
11.4.4	客户端接收软件更新	393
	小结	394
	习题	394
	实验: 使用自动方式部署 SCCM 客户端	395
第 12 章	证书服务与 SSL 安全协议	396
12.1	证书服务的概念	396
12.1.1	数字证书简介	396
12.1.2	认证服务简介	397
12.2	安装证书服务	397
12.2.1	企业 CA 的安装	397
12.2.2	独立根 CA 的安装	401



12.3	配置和实现 SSL 证书颁发	402
12.3.1	安全套接字层 (SSL) 协议	402
12.3.2	使用 SSL 证书配置安全 Web 站点	403
12.4	SSL 的安全漏洞及其解决方案	410
12.4.1	SSL 安全漏洞	410
12.4.2	安全防范措施	411
	小结	412
	习题	412
	实验: 使用 SSL 证书搭建安全 Web 网站	412
第 13 章	Windows 网络访问保护	414
13.1	NAP 概述	414
13.1.1	NAP 的组件	414
13.1.2	NAP 系统工作机制	415
13.1.3	NAP 的应用环境	416
13.1.4	强制方式	417
13.2	安装 NPS	418
13.3	配置 DHCP 强制	420
13.3.1	修改 DHCP 相关选项	420
13.3.2	配置 NPS 策略	423
13.3.3	配置启用 DHCP 强制客户端	430
13.3.4	测试 DHCP 强制	432
13.4	配置 VPN 强制	433
13.4.1	配置 VPN 服务器	433
13.4.2	配置 NPS 服务器及策略	438
13.4.3	设置远程访问账户	445
13.4.4	配置 VPN 强制客户端	445
13.4.5	测试 VPN 强制	449
13.5	IPSec 强制	451
13.5.1	概述	451
13.5.2	配置 CA	453
13.5.3	配置域控制器默认策略	456
13.5.4	配置 NPS	457
13.5.5	配置强制客户端	461
13.5.6	测试 IPSec 强制	463
	小结	463
	习题	463
	实验: 配置 VPN 强制	463



第 14 章 数据库安全	465
14.1 系统补丁	465
14.1.1 操作系统补丁	465
14.1.2 数据库补丁	466
14.2 MBSA 数据库扫描	466
14.3 文件夹访问权限	468
14.3.1 文件夹共享	468
14.3.2 安全列表	469
14.4 密码审核	469
14.4.1 强密码验证	470
14.4.2 禁用系统管理员组	472
14.4.3 C2 审核	474
14.4.4 修改 SA 账户名称	475
14.5 数据库访问权限	475
14.5.1 数据库访问权限	475
14.5.2 数据表访问权限	479
14.6 只读数据库	480
14.7 数据加密	482
14.7.1 创建数据库主密钥	482
14.7.2 创建加密密钥	484
14.7.3 加密数据列	485
14.7.4 解密数据列	487
14.8 外围应用配置器	489
14.8.1 启动外围应用配置器	489
14.8.2 服务和连接的外围应用配置器	489
14.8.3 功能的外围应用配置器	491
14.9 备份和恢复数据库	492
14.9.1 完全备份与恢复数据库	493
14.9.2 创建自动备份数据库计划	497
小结	500
习题	501
实验：备份和恢复数据库	501



第 1 章

Windows Server 2008 操作系统安全概述

Windows Server 2008 是微软公司继 Windows Vista 之后鼎力推出的新一代服务器操作系统，不仅网络功能强大，而且系统安全性也有了极大提高。使服务器系统安全工作涉及系统内核安全、应用程序安全、用户账户安全和端口安全等多个方面。Windows Server 2008 操作系统允许管理员根据服务器所处环境的不同，启用不同的安全防护策略。

本章导读

- Windows Server 2008 操作系统安装安全策略
- 系统服务的安全
- 用户账户安全
- 系统设置安全

1.1 Windows Server 2008 操作系统安全策略

Windows Server 2008 操作系统默认提供了多种安全功能，可以为系统程序、服务以及网络访问提供周密的安全防护。不过，在配置 Windows Server 2008 操作系统过程中用户必须注意安全性和易用性之间的矛盾，根据实际需求设置适当的安全级别即可。

1.1.1 操作系统安装注意事项

想要保护好系统安全就要步步为营，安装操作系统是第一步。安装 Windows Server 2008 时应注意以下几点：

- 使用通过正规渠道获得的 Windows Server 2008 操作系统光盘安装，防止安装过程中被植入木马或间谍软件，影响系统安全性和兼容性。
- 列出当前服务器所需的驱动程序、服务组件、杀毒软件、必备工具等，必要时可以事先进行汇总列表。
- 保证硬件设备的可靠性。建议为重要服务器使用磁盘阵列冗余技术，如 RAID0、RAID1 和 RAID5 等，确保服务器存储系统硬件的稳定性和安全性。





- 尽量使用全新方式安装系统，即将操作系统安装在一个全新主分区中，并提前做好合理规划，避免安装完成后重新修改系统配置带来的麻烦。例如，在安装之前应删除系统分区的所有文件，并重新格式化，确保磁盘完好无损。
- 使用 NTFS 文件系统格式化服务器所有磁盘分区，以便为系统分区、数据分区和日志文件分区提供更高的安全性。只有使用 NTFS 文件系统的分区，才能为文件配置 ACL（访问控制列表）访问权限控制，达到保护用户访问安全的目的。
- 没有进行任何安全配置的服务器，不要与任何公共设备或网络连接，必要时可以找一台可以确保安全性的服务器进行连接。
- 只为服务器安装必需的协议，如 TCP/IP，避免其他网络协议给系统带来漏洞。
- 通常情况下，不要将服务器加入到域，应安装成独立服务器模式。
- 为系统管理员设置一个安全性较高的密码。
- 不要在服务器上部署多操作系统，防止恶意用户通过其他系统控制权限获取重要信息，或对 Windows Server 2008 操作系统进行破坏。
- 如果条件允许，建议安装英文版 Windows Server 2008。通常情况下，Microsoft 总是最先发布英文版本的补丁，中文版本的补丁相对滞后一段时间。

1.1.2 配置 Internet 防火墙系统

Internet 防火墙是一道屹立于主机和 Internet 之间的安全屏障，用于防止来自 Internet 或所在局域网的非法访问。防火墙的基本工作原理是，对多种类型的网络通信内容进行过滤。

最常用的基于操作系统的防火墙系统就是 Windows 系统防火墙，此外用户还可以选择其他第三方专业防火墙软件，如天网、瑞星等。建议用户使用系统默认的 Internet 防火墙。

1. Windows 防火墙简介

Windows Server 2008 内置的 Internet 防火墙是一种典型的状态防火墙，不仅可以监视通过它的所有通信，还可以检查所处理的每一条消息的源地址和目的地址。其工作机制如图 1-1 所示。

Windows 防火墙就像是一个在计算机和外部 Internet 之间建立的“盾牌”，可以允许请求的数据包通过，而阻止没有请求的数据包进入。启用系统防火墙后，会禁止所有来自 Internet 的未经允许的连接。防火墙使用“网络地址转换器（NAT）”逻辑来验证访问网络或本地主机的入站请求。因此，如果网络通信不是来自受保护的网内，或者没有创建任何端口映射，则入站数据就被丢弃。

通常情况下，黑客入侵的第一步就是找到所要攻击主机的 IP 地址，再使用 ping 命令建立到该主机的通道，然后对主机进行端口扫描，确定攻击入口。在这种情况下，ping 不

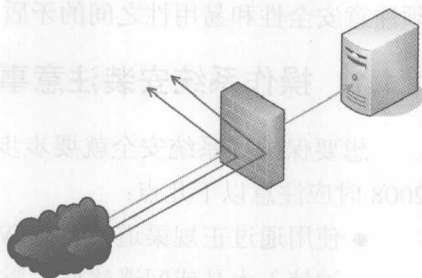


图 1-1 Internet 防火墙





通的 IP 地址，黑客通常认为其没有被使用而忽略过去。因此，Windows 系统防火墙的一个实用功能就是禁止响应 ping 命令，而且还能阻止外部程序对本机进行端口扫描，抛弃所有没有请求的 IP 数据包。

2. 配置 Internet 防火墙

默认情况下，Windows Server 2008 操作系统的防火墙已经启动，管理员可以根据需要进行配置。如果服务器已经连接到网络，则默认网络访问策略的设置可能会阻止管理员对 Windows 防火墙的配置。

提示：有关 Windows 防火墙的具体配置，读者可参考本书“第 9 章 Windows 防火墙”中的详细介绍。

3. ICMP 配置

ICMP 主要用于网络控制和诊断，如 ping 命令就是利用该协议中的回显请求功能实现的。ICMP 是一种无连接的协议，即只要发送端完成 ICMP 报文的封装并传递给路由器，该报文即可自动寻找目的地址。因此，ICMP 的一个致命缺点就是易伪造，入侵者通常会使用 ping 命令建立到攻击目标的连接。通过配置 Windows Server 2008 高级防火墙中的相关规则，即可禁止本地主机响应 ping 命令。

- 01 依次选择“开始”→“管理工具”→“高级安全 Windows 防火墙”命令，打开图 1-2 所示的“高级安全 Windows 防火墙”窗口。
- 02 单击“入站规则”选项，在“入站规则”窗格中双击“核心网络 - Internet 组管理协议 (ICMP-In)”选项，打开图 1-3 所示的“核心网络 - Internet 组管理协议 (ICMP-In) 属性”对话框。



图 1-2 “高级安全 Windows 防火墙”窗口

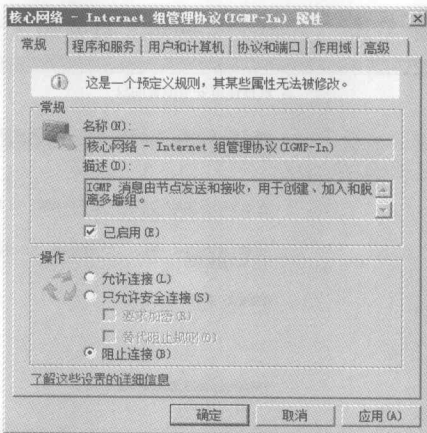


图 1-3 属性对话框

- 03 在“操作”选项区域中选中“阻止连接”单选按钮。这样就可以阻止本地计算机响应 ping 请求，确保系统安全。
- 04 单击“确定”按钮，保存设置。