



网管天下

刘晓辉 主编
杨淑梅 王淑江 李文俊 等编著

NETWORK SECURITY ADMINISTRATION PRACTICE

网络安全管理实践

详细的网络安全构建策略
各种系统、交换机及服务器的安全设置
丰富的安全攻防实例
帮您构建安全、可靠的网络环境

- ◆ 局域网的安全构建策略
- ◆ Windows服务器安全
- ◆ 网络交换机和路由器安全
- ◆ 无线局域网安全
- ◆ Windows网络客户端安全



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>



网络安全管理实践

刘晓辉 主编

杨淑梅 王淑江 李文俊 等编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书全面深入地介绍了 Windows 网络服务器、Windows 网络客户端、网络交换机、无线网络设备、路由器和网络防火墙的安全设置,以及局域网的安全构建策略,提供了全面的局域网安全解决方案。使读者能够全面掌握局域网络中的安全管理与设置技术,全面提升网络的安全水平,迅速成长为合格的网络管理员和安全规划师。

本书适用于中小型网络管理员和安全规划师,以及所有准备从事网络管理工作的网络爱好者,并可作为大专院校计算机专业的辅导教材。

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

网络安全管理实践 / 刘晓辉主编. —北京: 电子工业出版社, 2007.3
(网管天下)

ISBN 978-7-121-03774-0

I.网... II.刘... 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(2007)第 004076 号

责任编辑: 郭鹏飞

印 刷: 北京市天竺颖华印刷厂

装 订: 三河市金马印装有限公司

出版发行: 电子工业出版社出版

北京市海淀区万寿路 173 信箱 邮编: 100036

开 本: 850×1168 1/16 印张: 33.5 字数: 857 千字

印 次: 2007 年 3 月第 1 次印刷

印 数: 5000 册 定价: 55.00 元

凡所购买电子工业出版社图书有缺损问题,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; 邮购电话:(010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线:(010) 88258888。

关于《网管天下》丛书

《网管天下》丛书是一套由国内资深网络专家写给网络建设与管理人员的应用实践手册，其目的在于帮助初、中级网络管理员，全方位地解决网络建设与管理中的各种实际问题，包括网络规划设计、网络布线实施、网络设备连接、网络配置管理、网络服务搭建、网络深入应用、网络故障排除、网络安全管理等诸多方面，囊括了网络管理中几乎所有的内容，其目的在于将网络理论与实际应用相结合，提高读者分析和解决具体问题的能力，将所学变为所用，将书本知识变为操作技能。

本丛书具有以下特点：

1. 授之以渔而不是授之于鱼。紧贴网络实际情况，从真实的网络案例入手，为网络管理员提供全面的网络设计、网络组建、网络管理和网络维护等解决方案，以提高读者的分析能力、动手能力和解决实际问题的能力。
2. 实用才是硬道理。为网络管理员提供彻底的、具有建设性的网络设计、网络组建和配置解决方案，真正解决网络建设和网络管理中的实际问题，突出实用性、针对性、技术性、经典性，举案说“法”、举一反三。
3. 理论新、技术新、设备新、案例新。所有的应用案例都发生在最近两年以内，而且案例中只涉及最主流的、最成熟的设备和技术，以及最新版本的软件，不再讨论那些已被淘汰或面临淘汰的东西，从而力求反映网络的新技术和新潮流。不仅让读者学了就能用，而且还可以拥有三年左右的“保鲜”期。

关于本书

在 2007 年 1 月举行的达沃斯世界经济论坛上，与会者不但讨论了全球经济和气候变暖的问题，而且还首次触及了互联网安全问题。参与这项话题讨论的既有政治家，也有著名的 IT 界人士。全球网络概念的开发者文森特·瑟弗表示，在目前接入因特网的大约 6 亿台电脑中，有 1.5 亿台左右都已成为黑客们的“俘虏”，并被用来发送垃圾邮件、病毒或是组织网络攻击行动。然而，最令人感到不安的是，上述 1.5 亿台电脑的所有者们经常无法意识到他们的机器正在被别人非法地利用。参与达沃斯世界经济论坛的专家们甚至指出，因特网目前所造成的危险已超过了其所带来的好处。

继冲击波、震荡波洗劫 Internet 以后，熊猫烧香又以更快捷的传播速度、更多样的传输方式，再次挑战本已脆弱的网络安全。网络攻击事件之所以频频发生，最根本的原因还在于操作系统、网络设备甚至网络协议本身，都存在着严重的安全漏洞。只要稍有疏忽和防范不及时，安全灾难便如影而至。由此不难看出，对于网络管理员而言，网络安全最为重要！

随着网络应用的深入、网络规模的扩大和数据存储量的增加，以及网络蠕虫、恶意攻击的日益猖獗，网络对安全的要求也就越来越高，因此，网络安全也就随之提上网络管理的重要日程。

本书全面讲述 Windows 服务器、网络客户端、网络交换机、无线网络设备、路由器和网络防火墙的安全设置，以及局域网的安全构建策略，提供了全面的局域网安全解决方案。

使读者能够全面掌握局域网络中的安全管理与设置技术，全面提升网络的安全水平，迅速成长为合格的网络安全管理员。

本书紧紧围绕“网络安全管理实践”这个主题展开，目的性和针对性都很强，最大限度地介绍了网络中所有有关安全的因素，归纳和总结了作者多年的安全工作经验和技巧。全面而详细地介绍了中小型网络中服务器、客户端和网络设备的安全策略，涉及从规划设计、搭建配置到管理排障的全部网络硬件技术，是一整套紧贴实际应用的安全解决方案。另外，通过对大量实例深入细致的分析，进一步培养了读者分析问题和解决问题的能力，非常适合网络管理员的实际需求。

本书由刘晓辉主编，杨淑梅、王淑江、李文俊等编著，李海宁、田俊乐、许广博、陈志成、赵卫东、刘淑梅、杨伏龙、王同明等也参加了本书部分内容的编写工作。笔者长期从事网络建设、网络管理、网络教学和网络实验工作，具有较高的理论水平和丰富的实践经验，曾经出版过三十余部有关网络搭建和管理的图书，均以易读、易学、实用的特点，得到众多读者的好评。本书是笔者的又一呕心沥血之作，希望能对大家掌握和提升网络安全管理和设置技术有所帮助。

河北三佳电子有限公司的冯士远、张乾、李传来工程师为本书提供了大量的技术资料和大力的技术支持，在此深致谢意！

如果您在配置网络和管理网络时遇到了疑问或难题，或者对本书有什么看法，欢迎发送 E-mail 至 Guopengfei@phei.com.cn 或 hslxh@163.net，进行讨论或寻求支持。由于笔者水平有限，书中难免有疏漏和错误之处，敬请专家和读者不吝赐教。

刘晓辉

2007 年 3 月

目 录

第 1 章 网络安全综述	1
1.1 网络系统安全风险分析	2
1.1.1 物理安全风险分析	2
1.1.2 网络平台的安全风险分析	3
1.1.3 系统的安全风险分析	3
1.1.4 应用的安全风险分析	3
1.1.5 管理的安全风险分析	4
1.1.6 其他安全风险	4
1.2 安全需求与安全目标	5
1.2.1 安全需求	5
1.2.2 网络安全策略	6
1.2.3 系统安全目标	6
1.3 网络安全规划	7
1.3.1 网络安全规划原则	7
1.3.2 安全服务、机制与技术	8
1.4 网络安全体系结构	8
1.4.1 物理安全	9
1.4.2 网络结构规划	9
1.4.3 系统安全	12
1.4.4 信息安全	12
1.4.5 应用安全	13
1.5 安全管理	13
1.5.1 安全管理规范	13
1.5.2 网络管理	14
1.5.3 安全管理	14
第 2 章 Windows 初始安全	15
2.1 Windows 安装安全	16
2.1.1 Windows 安装安全指南	16
2.1.2 安全补丁更新	17

2.2	Windows 基本安全	19
2.2.1	Internet 防火墙	19
2.2.2	安全配置向导	21
2.3	Windows 被动防御安全	29
2.3.1	配置防病毒系统	30
2.3.2	配置防间谍系统	30
2.4	Windows 系统安全	31
2.4.1	应用程序安全	31
2.4.2	系统服务安全	32
2.4.3	注册表安全	35
2.4.4	审核策略	39
第 3 章	系统漏洞安全	43
3.1	漏洞概述	44
3.1.1	漏洞的特性	44
3.1.2	漏洞生命周期	45
3.1.3	漏洞管理流程	46
3.1.4	漏洞修补策略	50
3.2	漏洞扫描	52
3.2.1	漏洞扫描概述	52
3.2.2	漏洞扫描工具 MBSA	53
3.2.3	MBSA 的安装与使用	65
3.3	系统更新	68
3.3.1	系统补丁部署原则	68
3.3.2	系统更新的实施	70
第 4 章	端口安全	73
4.1	端口概述	74
4.1.1	端口分类	74
4.1.2	应用程序和服务端口	75
4.1.3	端口攻击	76
4.1.4	查看使用端口	77
4.2	配置端口	80
4.2.1	启动/关闭服务法	80
4.2.2	IP 安全策略法	81
4.2.3	禁用 NetBIOS 端口	97

第5章 活动目录安全99

5.1 活动目录安全管理.....	100
5.1.1 全局编录.....	100
5.1.2 操作主机.....	103
5.1.3 功能级别.....	105
5.1.4 信任关系.....	108
5.1.5 权限委派.....	117
5.2 活动目录数据库.....	124
5.2.1 活动目录数据库的备份.....	125
5.2.2 活动目录数据库的恢复.....	127
5.2.3 恢复任意时间活动目录数据库备份.....	129
5.2.4 活动目录服务器故障.....	131
5.2.5 误删用户、组或者其他对象.....	145

第6章 用户账户安全147

6.1 系统管理员账户安全.....	148
6.1.1 更改超级管理员账户.....	148
6.1.2 禁用 Administrator 账户.....	149
6.1.3 减少管理员组成员.....	150
6.1.4 系统管理员口令设置.....	150
6.2 用户账户安全.....	152
6.2.1 创建安全用户账户.....	152
6.2.2 重设用户密码.....	155
6.2.3 管理用户账户.....	157
6.2.4 限制用户登录工作站.....	158
6.2.5 限制用户登录时间.....	159
6.2.6 用户账户策略.....	159
6.2.7 系统账户数据库.....	161
6.2.8 用户访问限制.....	163
6.2.9 用户组安全.....	164
6.3 用户权限.....	166
6.3.1 为用户设置权限.....	167
6.3.2 将用户权限指派到组.....	167
6.3.3 共享文件夹权限.....	168
6.3.4 配置特权和权利.....	169
6.3.5 用户组权限.....	170

第7章 组策略安全	171
7.1 组策略模板	172
7.1.1 组策略模板概述	172
7.1.2 添加/删除策略模板	173
7.1.3 设置模板策略	174
7.2 安全策略	175
7.2.1 账户策略	175
7.2.2 审核策略	180
7.2.3 用户权限分配	183
7.3 软件限制策略	184
7.3.1 软件限制策略概述	184
7.3.2 安全级别设置	185
7.3.3 默认规则	188
7.4 用户主目录	191
7.4.1 创建共享文件夹	191
7.4.2 指派用户主目录	192
第8章 文件系统安全	195
8.1 NTFS 权限	196
8.1.1 NTFS 文件夹权限和 NTFS 文件权限	196
8.1.2 访问控制列表	198
8.1.3 多重 NTFS 权限	199
8.1.4 NTFS 权限的继承性	200
8.2 设置 NTFS 权限	201
8.2.1 设置 NTFS 权限基本策略和规则	201
8.2.2 NTFS 权限审核	202
8.2.3 取消“Everyone”完全控制权限	204
8.3 权限继承	205
8.3.1 指定特殊访问权限	205
8.3.2 复制和移动文件夹对权限的影响	207
8.4 文件审核	207
8.4.1 审核策略	208
8.4.2 设置审核对象	208
8.4.3 启用审核策略	209
8.4.4 设置审核	209
8.4.5 选择审核项的应用位置	210

8.5	文件加密	210
8.6	删除不安全文件	212
8.6.1	取消系统的文件保护功能	212
8.6.2	注册表安全设置的项目	212
8.6.3	审核部分设置的项目	212
8.6.4	删除不必要的可执行文件	212
8.6.5	删除不必要的可执行程序	212
8.7	NTFS 权限应用实例	213
8.7.1	屏蔽 FlashGet 广告	213
8.7.2	屏蔽 QQ 广告	213
8.7.3	IIS 服务的最小访问权限许可	214
8.7.4	NTFS 权限复制	214
第 9 章	共享资源安全	217
9.1	共享文件夹权限	218
9.1.1	共享文件夹的权限	218
9.1.2	共享文件夹权限与 NTFS 权限	219
9.2	默认共享安全	220
9.2.1	查看默认共享	220
9.2.2	停止默认共享	222
9.2.3	IPC\$	229
9.2.4	设置隐藏的共享	233
第 10 章	Internet 信息服务安全	235
10.1	IIS 安全机制	236
10.1.1	用户权限安全	236
10.1.2	IIS 访问安全	236
10.1.3	NTFS 访问安全	237
10.1.4	IIS 安装安全	238
10.2	Web 安全	238
10.2.1	用户控制安全	238
10.2.2	访问权限控制	240
10.2.3	IP 地址控制	242
10.2.4	端口安全	243
10.2.5	IP 转发安全	244
10.2.6	SSL 安全	244
10.2.7	审核 IIS 日志记录	251

10.2.8	设置内容过期	253
10.2.9	内容分级设置	254
10.2.10	注册 MIME 类型	254
10.3	FTP 安全	256
10.3.1	设置 TCP 端口	256
10.3.2	连接数量限制	257
10.3.3	用户访问安全	258
10.3.4	文件访问安全	259
第 11 章	事件日志、性能日志和警报	261
11.1	事件查看器	262
11.1.1	事件基本信息	262
11.1.2	事件的类型	262
11.1.3	事件查看器的使用	263
11.2	安全性日志	266
11.2.1	启用审核策略	266
11.2.2	日志分析	267
11.2.3	审核日志	268
11.2.4	审核事件 ID	270
11.3	性能日志和警报	275
11.3.1	警报规则监控磁盘空间	276
11.3.2	警报规则监控黑客的字典暴力密码破解	278
11.3.3	配置性能日志监视文件授权访问	280
11.3.4	常用的计数器	282
第 12 章	Windows 客户端安全	285
12.1	Windows XP 安全	286
12.1.1	Windows XP 安全概述	286
12.1.2	锁定计算机	286
12.1.3	保护密码	289
12.1.4	以普通用户运行计算机	294
12.1.5	加密文件系统	296
12.1.6	Windows 防火墙	300
12.1.7	系统更新设置	303
12.1.8	Internet Explorer 设置	305
12.1.9	Windows Defender	309
12.2	Windows 2000 Professional 安全	315

12.2.1	端口安全	315
12.2.2	安装网络防火墙和病毒防火墙	316
12.2.3	系统更新设置	319
12.2.4	NTFS 与文件加密	320
第 13 章 系统补丁安全		323
13.1	WSUS 概述	324
13.1.1	WSUS 2.0	324
13.1.2	WSUS 3.0	325
13.2	WSUS 服务端部署	326
13.2.1	WSUS 服务器需求	327
13.2.2	WSUS 服务器端的安装和配置	327
13.3	WSUS 客户端配置	342
13.3.1	客户端的安装和配置	342
13.3.2	客户端注意事项	346
13.4	WSUS 服务应用和管理	346
13.4.1	执行服务器同步操作	346
13.4.2	计算机及分组管理	350
13.4.3	更新的管理	354
13.4.4	WSUS 服务器的报告监视	357
13.4.5	客户端获取并安装更新文件	359
13.4.6	设置特殊文件发布	360
第 14 章 网络病毒安全		363
14.1	AntiVirus 企业版的安装	364
14.1.1	Symantec Antivirus 的功能与特点	364
14.1.2	安装 Symantec 系统中心	364
14.1.3	配置服务器组	371
14.2	安装 AntiVirus 客户端程序	378
14.2.1	借助 Web 服务器分发和安装	378
14.2.2	远程安装企业客户端	381
14.2.3	从服务器上的客户端安装文件夹安装	383
14.2.4	从本地安装客户端	383
14.3	升级病毒库	386
14.3.1	手工更新	387
14.3.2	自动更新	388

第 15 章 网络设备系统安全.....391

15.1 登录密码安全.....	392
15.1.1 配置 Enable 密码.....	392
15.1.2 配置 Telnet 密码.....	393
15.1.3 配置管理用户.....	394
15.2 配置命令级别安全.....	395
15.2.1 配置多个用户级别.....	396
15.2.2 登录和离开授权级别.....	396
15.3 终端访问限制安全.....	396
15.3.1 控制虚拟终端访问.....	396
15.3.2 控制会话超时.....	397
15.4 SNMP 安全.....	398
15.4.1 配置 SNMP 字符串.....	399
15.4.2 配置 SNMP 组和用户.....	400
15.4.3 SNMP 配置实例.....	400
15.5 HTTP 服务安全.....	402
15.5.1 关闭 HTTP 服务.....	402
15.5.2 配置安全 HTTP 服务.....	402
15.5.3 配置安全 HTTP 客户端.....	404
15.6 系统安全日志.....	404
15.6.1 日志信息概述.....	404
15.6.2 启用系统日志信息.....	407
15.6.3 设置日志信息存储设备.....	407
15.7 IOS 系统版本升级.....	408
15.7.1 备份系统软件映像.....	409
15.7.2 恢复或升级系统软件映像.....	410

第 16 章 交换机安全.....413

16.1 基于端口的传输控制.....	414
16.1.1 风暴控制.....	414
16.1.2 流控制.....	416
16.1.3 保护端口.....	417
16.1.4 端口阻塞.....	418
16.1.5 端口安全.....	419
16.1.6 传输速率限制.....	423
16.1.7 MAC 地址更新通知.....	427

16.1.8	绑定 IP 和 MAC 地址	430
16.2	VLAN 安全	431
16.2.1	VLAN 概述	431
16.2.2	配置 VLAN	431
16.2.3	配置 VLAN Trunk	435
16.3	私有 VLAN 安全	437
16.3.1	PVLAN 概述	437
16.3.2	配置 PVLAN	440
16.4	基于端口的认证安全	444
16.4.1	IEEE 802.1x 认证简介	444
16.4.2	配置 IEEE 802.1x 认证	447
16.4.3	配置交换机到 RADIUS 服务器的通信	448
16.4.4	配置重新认证周期	449
16.4.5	修改安静周期	450
第 17 章	无线网络安全	451
17.1	无线网络设备安全	452
17.1.1	无线接入点安全	452
17.1.2	无线路由器安全	458
17.2	IEEE 802.1x 身份认证	459
17.2.1	部署 IEEE 802.1x 认证	460
17.2.2	无线访问认证配置步骤	460
17.2.3	配置 Cisco 无线接入点	461
17.3	无线网络客户端安全	461
17.3.1	对等网络无线安全	462
17.3.2	接入点无线客户安全	470
第 18 章	路由器安全	477
18.1	访问列表安全	478
18.1.1	访问列表概述	478
18.1.2	IP 访问列表	481
18.1.3	时间访问列表	485
18.1.4	MAC 访问列表	487
18.1.5	创建并应用 VLAN 访问列表	488
18.2	网络攻击安全防范	489
18.2.1	IP 欺骗防范	489
18.2.2	SYN 淹没防范	490

18.2.3	Ping 攻击防范	491
18.2.4	DoS 和 DDoS 攻击防范	492
第 19 章 防火墙安全		493
19.1	网络访问控制	494
19.1.1	ACL 使用规则	494
19.1.2	将 Conduit 转换成 ACL	496
19.1.3	ICMP 命令使用	497
19.1.4	ACL 配置示例	498
19.2	VPN 安全传输	500
19.2.1	VPN 特点及适用	500
19.2.2	PPTP 方式 VPN	503
19.2.3	L2TP 方式 VPN	509
19.2.4	PPPoE 拨号配置	515
19.2.5	VPN 配置示例	516



第1章

网络安全综述

- @ 1.1 网络系统安全风险分析
- @ 1.2 安全需求与安全目标
- @ 1.3 网络安全规划
- @ 1.4 网络安全体系结构
- @ 1.5 安全管理

计 算机网络安全方案,包括原有网络系统分析、安全需求分析、安全目标的确立、安全体系结构的设计等。该解决方案的目标是在不影响当前业务的前提下,实现对局域网全面的安全管理。

借助对计算机网络的分析和设计,实现以下网络安全目的:

- 将安全策略、硬件及软件等方法结合起来,构成一个统一的防御系统,有效阻止非法用户进入网络,减少网络的安全风险。
- 建立统一的漏洞、补丁管理平台。定期进行漏洞扫描、审计跟踪、分发补丁。
- 建立完善的漏洞、补丁评估体系,对于新的漏洞、补丁进行安全评测。
- 建立完善的备份机制,包括:数据库、操作系统、个人应用文件等。
- 通过入侵检测、入侵保护、流量检测等方式实现实时安全监控,提供快速响应故障的手段,同时具备很好的安全取证措施。
- 网络管理员能够很快重新组织被破坏了的文件或应用,使系统重新恢复到破坏前的状态,最大限度地减少损失。
- 在工作站、服务器上安装相应的防病毒、防间谍软件,由中央控制台统一控制和管理,完成带毒设备的阻隔和分离,实现全网统一部署。
- 培养、加强集团职员的安全意识。
- 建立完善的安全保护、预警、检查类的规章制度。

1.1 网络系统安全风险分析

随着 Internet 网络急剧扩大和上网用户迅速增加,网络系统的风险变得更加严重和复杂。原来由单台计算机安全事故引起的损害可能传播到整个系统,导致网络大范围的瘫痪和损失;加上用户缺乏安全控制机制和对 Internet 安全政策的认识不足,这些风险正日益严重。针对企业局域网中存在的安全隐患,在进行安全方案设计时,下述安全风险必须要认真考虑,并且要针对面临的风险,采取相应的安全措施。下述风险由多种因素引起,与网络结构和系统的应用、局域网内网络服务器的可靠性等因素密切相关。

网络安全可以从以下几个方面来理解:

- 网络物理是否安全
- 网络平台是否安全
- 系统是否安全
- 应用是否安全
- 管理是否安全

针对每一类安全风险,结合局域网的实际情况,下面将具体地分析网络的安全风险。

1.1.1 物理安全风险分析

网络的物理安全主要是指地震、水灾、火灾等环境事故,电源故障,人为操作失误或错误,设备被盗、被毁,电磁干扰,线路截获,以及高可用性的硬件、双机冗余的设计、机房环境及报警系统、安全意识等。

网络的物理安全是整个网络系统安全的前提。hjj 在局域网内,由于网络的物理跨度不大,只要制定健全的安全管理制度,做好备份,并且加强网络设备和机房的管理,这些风险都是可以避免的。