第一图书网, tushu007.com

<<Windows Server管理（上）>>

图书基本信息

书名：<<Windows Server管理（上）>>

13位ISBN编号：9787121151590

10位ISBN编号：7121151596

出版时间：2012-2

出版时间：安博教育集团 电子工业出版社 (2012-02出版)

作者：安博教育集团

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

<<Windows Server管理（上）>>

内容概要

本书分为网络安全基础，ISA2006两大部分。
内容包括：计算机网络安全概述；黑客攻击技术介绍；操作系统安全；网络安全管理；路由器和交换机网络安全；身份认证技术；防火墙，入侵检测技术介绍；VPN技术；ISA概述；安装与部署ISA Server 2006；ISA Server客户端的部署；配置网页缓存；控制内网访问Internet；通过ISA发布内部站点，邮件服务及其他各类服务；配置入侵检测。

本书内容新颖，编辑合理，论述清晰，不仅适合用做计算机职业培训的首选教材，也适合普通高校学生作为教材使用。

第一图书网, tushu007.com

<<Windows Server管理（上）>>

书籍目录

第一部分 网络安全技术第1章 计算机网络安全概述 （3）1.1 网络安全简介 （4）1.1.1 网络安全的发展 （4）1.1.2 网络安全的定义和重要性 （7）1.2 网络安全弱点和主流的网络攻击简介 （10）本章小结 （13）习题 （13）第2章 黑客攻击技术介绍 （15）2.1 扫描探测 （16）2.1.1 扫描器攻击介绍 （16）2.1.2 扫描技术的分类 （16）2.1.3 扫描器主流软件介绍 （17）2.2 嗅探侦听 （19）2.2.1 网络侦听原理 （19）2.2.2 Sniffer工具的介绍和使用 （20）2.3 缓冲区溢出攻击 （25）2.4 拒绝服务与分布式拒绝服务 （26）2.4.1 DoS攻击介绍 （26）2.4.2 DDoS攻击介绍 （27）2.4.3 DoS/DDoS攻击的具体表现 （27）2.4.4 常见的DoS/DDoS攻击 （28）2.4.5 如何防止DoS/DDoS攻击 （30）2.5 病毒 （31）2.5.1 病毒定义 （31）2.5.2 病毒的分类 （32）2.5.3 计算机病毒的防治 （36）2.6 木马 （39）2.6.1 木马的工作原理 （39）2.6.2 木马的隐藏与检测 （40）2.6.3 木马的查杀 （42）2.6.4 木马的防护 （43）2.7 智能安全网络架构 （43）2.7.1 智能安全网络架构的组成 （43）2.7.2 虚拟专用网VPN技术 （43）2.7.3 防火墙系统 （44）2.7.4 入侵检测系统 （46）2.7.5 网络访问控制和健康状态审查 （47）本章小结 （49）习题 （49）第3章 操作系统安全 （51）3.1 操作系统安全对比 （52）3.2 Windows操作系统 （53）3.2.1 Windows操作系统简介 （53）3.2.2 Windows家族 （53）3.2.3 Windows系统安全管理 （62）3.2.4 Windows系统安全实施模板 （68）3.3 Linux/UNIX系统安全 （73）3.3.1 Linux简介 （73）3.3.2 UNIX简介 （74）3.3.3 Linux/UNIX系统安全管理 （74）本章小结 （78）习题 （78）第4章 网络安全管理 （79）4.1 网络管理技术概述 （80）4.2 网络安全管理现状与需求 （80）4.3 网络安全管理技术及功能简介 （81）4.4 安全管理的发展现状 （82）4.5 SNMP协议 （82）4.5.1 SNMP协议介绍 （82）4.5.2 SNMP的命令和报文 （83）4.5.3 管理信息数据库 （84）4.5.4 SNMP的发展 （85）本章小结 （86）习题 （86）第5章 路由器和交换机网络安全 （87）5.1 路由器安全概述 （88）5.1.1 路由器扮演安全角色 （88）5.1.2 路由器的安全初试 （89）5.1.3 路由器安全优化要点 （90）5.1.4 多级管理 （99）5.1.5 安全登录控制 （103）5.2 路由器安全管理 （105）5.2.1 syslog日志 （105）5.2.2 NTP网络设备间的时间同步 （107）5.2.3 SSH安全远程管理 （107）5.3 交换机网络安全 （109）5.3.1 虚拟局域网 （109）5.3.2 三层交换技术 （114）5.3.3 端口安全 （114）5.3.4 端口流量控制 （116）5.3.5 网络访问控制与802.1x认证 （118）5.3.6 DHCP侦听 （124）5.3.7 DAI（动态ARP检测） （126）本章小结 （128）习题 （128）第6章 身份认证技术 （129）6.1 身份认证技术简介 （130）6.2 身份认证技术分类 （130）6.3 身份认证技术发展趋势 （131）6.4 生物识别 （132）6.4.1 生物识别技术概念 （132）6.4.2 几种常见的生物特征识别方式 （133）6.4.3 生物特征识别技术在中国的发展状况 （135）6.5 指纹认证 （136）6.6 虹膜识别技术 （138）6.6.1 虹膜作为身份标识具有许多先天优势 （138）6.6.2 虹膜识别过程 （139）6.7 数字认证 （141）本章小结 （142）习题 （142）第7章 防火墙技术介绍 （143）7.1 认识防火墙 （144）7.1.1 什么是防火墙 （144）7.1.2 防火墙的功能 （145）7.1.3 防火墙的分类 （148）7.1.4 防火墙的优缺点比较 （152）7.2 包过滤型防火墙 （153）7.2.1 包过滤型防火墙的工作原理 （153）7.2.2 访问控制列表 （154）7.2.3 标准ACL （155）7.2.4 扩展ACL （157）7.2.5 命名的ACL （158）7.2.6 ACL注释 （158）7.2.7 基于时间的ACL （159）7.2.8 自反ACL （159）7.2.9 动态ACL（锁和密钥） （162）7.2.10 Turbo ACL （164）7.3 状态检测型防火墙 （165）7.3.1 状态检测型防火墙的工作原理 （165）7.3.2 状态检测型防火墙产品介绍 （167）本章小结 （168）习题 （169）第8章 入侵检测技术 （171）8.1 入侵检测系统概述 （172）8.2 入侵检测系统发展史 （173）8.3 入侵检测系统的分类和对比 （176）8.3.1 入侵检测系统的分类 （176）8.3.2 入侵检测系统的对比 （178）8.4 入侵检测的检测算法 （179）8.5 入侵检测系统算法特征 （180）8.6 入侵检测结构 （181）8.7 入侵检测系统的演进 （182）8.8 入侵检测产品和市场分析 （183）8.8.1 入侵检测产品 （183）8.8.2 入侵检测系统市场分析 （186）本章小结 （187）习题 （187）第9章 VPN技术 （189）9.1 VPN技术概述 （190）9.1.1 VPN技术的企业应用 （190）9.1.2 VPN的实现方式 （190）9.1.3 VPN技术的需求 （191）9.1.4 VPN的隧道概念 （192）9.1.5 VPN隧道技术的实现 （192）9.1.6 PPP拨号会话过程 （194）9.1.7 VPN的隧道技术分类 （195）9.2 通用路由封装协议GRE （200）9.3 IPSec介绍 （205）9.3.1 IPSec安全特性 （205）9.3.2 IPSec技术特点和组成 （206）9.3.3 对称加密 （207）9.3.4 非对称加密 （208）9.3.5 数据完整性HMAC （208）9.3.6 Diffie-Hellman密钥交换协议 （209）9.3.7 源验证方式介绍 （209）9.3.8 IPSec VPN应用范例 （210）9.4 SSL虚拟专用

网技术 （215）9.4.1 SSL基础 （216）9.4.2 SSL通信的工作原理 （217）9.4.3 SSL VPN的主要优点和不足 （218）9.4.4 SSL VPN配置应用范例 （220）本章小结 （224）习题 （224）第二部分 ISA 2006第10章 ISA概述 （227）10.1 防火墙概述 （228）10.1.1 软件防火墙 （228）10.1.2 硬件防火墙 （228）10.1.3 防火墙的特点 （229）10.1.4 防火墙的功能 （229）10.2 ISA Server 2006功能概述 （230）10.3 ISA Server 2006加速Web访问 （231）10.4 防火墙的设置种类 （233）10.5 ISA Server与VPN的集成 （236）本章小结 （237）习题 （237）第11章 安装与部署ISA Server 2006 （239）11.1 ISA Server 2006企业版的特点 （240）11.2 ISA Server部署与使用注意事项 （240）11.2.1 安装ISA Server 的软件需求 （240）11.2.2 安装ISA Server的硬件环境 （241）11.2.3 ISA Server 的安装 （241）11.2.4 无人值守安装 （253）11.3 ISA Server的部署位置 （255）11.3.1 Internet边缘防火墙 （256）11.3.2 部门或主干网络防火墙 （256）11.3.3 分支办公室防火墙 （256）11.3.4 安全服务器发布 （257）11.3.5 角色管理 （257）11.4 测试ISA Server防火墙是否安装成功 （260）11.4.1 打开ISA Server管理工具 （260）11.4.2 防火墙阻挡测试 （261）11.4.3 开放服务器访问外网网页 （262）本章小结 （266）习题 （266）第12章 ISA Server客户端的部署 （267）12.1 客户端分类 （268）12.2 测试环境的搭建 （269）12.3 ISA Server的配置 （272）12.3.1 防火墙规则的开放 （272）12.3.2 确认可接收“Web代理客户端”的请求 （273）12.4“Web代理客户端”的配置 （274）12.5“SecureNAT客户端”的配置 （275）12.5.1“SecureNAT客户端”的配置 （275）12.5.2 开放DNS流量 （277）12.5.3 将“SecureNAT客户端”配置成“Web代理客户端” （279）12.6“防火墙客户端”的配置 （279）12.6.1 ISA Server的配置 （280）12.6.2 安装“防火墙客户端” （281）12.6.3 与ISA Server连接测试 （283）12.7 自动发现 （285）12.7.1 自动发现原理 （285）12.7.2 将ISA Server配置为WPAD服务器 （285）本章小结 （286）习题 （287）第13章 配置网页缓存 （289）13.1 高速缓存的配置 （290）13.1.1 设置缓存硬盘的大小 （290）13.1.2 设置高速缓存大小 （291）13.2 设置缓存规则 （292）13.2.1 创建缓存规则 （292）13.2.2 修改缓存规则 （297）13.3 缓存的高级设置 （297）13.4 Web链 （299）13.5 定时下载网页内容 （303）13.6 删除缓存区的数据 （306）本章小结 （307）习题 （307）第14章 控制内网访问Internet （309）14.1 解析防火墙策略的设置技巧 （310）14.1.1 防火墙的策略元素 （310）14.1.2 协议 （310）14.1.3 用户 （313）14.1.4 计划 （316）14.1.5 内容类型 （317）14.1.6 网络对象 （318）14.2 防火墙策略的执行过程 （320）14.2.1 检查网络规则 （321）14.2.2 检查系统策略 （322）14.2.3 检查防火墙策略 （323）14.3 限制内网用户的方法 （326）14.3.1 利用IP和ARP静态绑定方法 （326）14.3.2 利用身份验证 （327）14.3.3 利用Web代理和基本身份验证 （329）14.4 开放与阻挡实时通信软件 （330）14.4.1 开放Windows Live Messenger通信 （330）14.4.2 阻挡Windows Live Messenger通信 （332）14.4.3 常用的应用程序签名 （334）14.5 系统监视 （334）14.5.1 制作报告 （335）14.5.2 连接性验证程序的配置 （338）本章小结 （340）习题 （340）第15章 通过ISA发布内部站点 （341）15.1 配置ISA Server 2006中单站点发布 （342）15.1.1 发布规则和访问规则的区别 （342）15.1.2 单个站点发布 （342）15.2 配置ISA Server 2006中多站点发布 （348）15.3 配置ISA Server 2006中安全的单站点发布 （352）15.3.1 安全发布的原理 （352）15.3.2 创建CA服务器 （353）15.3.3 为安全Web站点申请证书 （361）15.3.4 导出证书 （364）15.3.5 导入证书 （366）15.3.6 创建安全Web站点发布规则 （368）15.4 配置ISA Server 2006中安全的多站点发布 （373）15.4.1 申请通配符证书 （374）15.4.2 修改Web侦听器 （376）15.4.3 修改发布规则 （377）本章小结 （379）习题 （379）第16章 通过ISA发布邮件服务 （381）16.1 安装Exchange Server 2003 （382）16.1.1 安装前的准备工作 （382）16.1.2 安装Exchange Server 2003 （382）16.2 使用ISA Server发布Exchange OWA （387）16.2.1 申请证书 （388）16.2.2 导出和导入证书 （391）16.2.3 创建Exchange OWA 发布规则 （392）16.3 使用ISA Server发布SMTP和POP3 （398）16.4 使用ISA Server发布Exchange RPC （403）16.4.1 使用RPC发布Exchange服务器 （403）16.4.2 使用RPC over HTTPS发布Exchange服务器 （407）本章小结 （412）习题 （413）第17章 发布其他类型的服务器 （415）17.1 发布终端服务器 （416）17.2 发布DNS服务器 （418）17.3 发布虚拟主机 （422）17.3.1 在IIS上设置虚拟主机 （423）17.3.2 在ISA Server上创建访问规则 （425）17.4 ISA Server制定规则方法总结 （430）17.4.1 Web发布规则与非Web发布规则的关系 （431）17.4.2 ISA Server网络中的基本原则 （432）17.4.3 发布规则的使用原则 （433）本章小结 （433）习题 （433）第18章 配置入侵检测 （435）18.1 ISA Server支持的入侵检测项目 （436）18.1.1 一般攻击的入侵检测 （436）18.1.2 DNS攻击的入侵检测 （437）18.1.3 POP入侵检测 （437）18.1.4 阻止包含IP选项的数据

第一图书网, tushu007.com

包 （437）18.1.5 阻止IP片段的数据包 （437）18.1.6 淹没缓解 （438）18.2 启用入侵检测功能 （438）18.2.1 启用入侵检测 （438）18.2.2 设置警报 （440）18.2.3 阻止IP选项与IP片段数据包 （444）18.2.4 淹没缓解 （445）本章小结 （448）习题 （448）附录A （449）

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com