<<Windows Server 2008 >

图书基本信息

书名：<<Windows Server 2008安全技术详解>>

13位ISBN编号：9787115226280

10位ISBN编号：7115226288

出版时间：2010-6

出版时间：人民邮电出版社

作者：约翰逊

页数：356

前言

在本书面市之际，相信读者和笔者一样，也是激动不已的。
当然，这并不是仅仅因为这本书，而是在于其所展现的一片广阔天地。
Windows Server 2008是Microsoft服务器操作系统旗舰产品的升级版。
研发人员做了大量工作，确保Windows Server 2008不仅具备优异的特性，并且部署起来更加安全。
本书可以作为用户探索Windows Server 2008新特性的指南，使工作更加得心应手。
本书同样针对IT专业人士，介绍了Windows Server 2008某些鲜为人知的功能。
本书包含所有工具包中的应有技术细节，这是12位顶级IT专家的心血结晶，值得一提的是，每位参与撰写的专家都是其所在领域的佼佼者，他们的著作总数已经超过了20本。

<<Windows Server 2008 >

内容概要

Windows Server 2008是Microsoft服务器操作系统旗舰产品的升级版，不仅具备优异的特性，并且部署起来更加安全。

本书是12位顶级IT专家的心血结晶，结合彼此在各领域中的专长，为读者打造了这本Windows Server 2008安全指南。

本书包括3篇：Windows安全基础、实现身份与访问(IDA)控制和常用的安全方案。

本书结构严谨、组织清晰，包含大量专家的实际经验，是大中型企业中IT安全专业人员的必备参考书。

作者简介

作者：（美国）约翰逊（Jesper M.Johansson） 等 译者：刘晓辉 陈祎磊 注释 解说词：马倩约翰逊（Jesper M.Johansson），是本书的主要作者，他设计了本书的架构，并且组织了作者团队。
如果本书有拍案叫绝之处，应当归功于其他合著者的汗水和智慧，倘若本书有某些遗漏的地方，Jesper M.Johansson才是当之无愧的罪魁祸首。
在信息安全和Windows安全方面，Jesper M.Johansson是知名作者，他现在是首席软件安全设计师，负责设计软件的基础结构。
Jesper曾经专注于微软的安全问题，从入侵网络到设计安全软件都有涉及。
Jesper在信息安全方面有很多成就，他出席了许多重要安全会议，并撰写了很多安全方面的文章，甚至还是微软安全MVP（Most Valuable Professional，最有价值专家）。
Jesper拥有管理信息系统的博士学位，他是一名CISSP（CerifiedInformation Systems Security Professional，国际信息安全认证专家），并且是ISSAP（Information Systems SecurityArchitecture Professional，信息系统安全架构专家）。
在业余时间，Jesper则是一名佩戴水肺的潜水教练。

<<Windows Server 2008 >

书籍目录

第1部分 Windows安全基础 第1章 主体、用户以及其他角色 1.1 主体、对象和元组 1.2 安全主体的类型 1.2.1 用户 1.2.2 计算机 1.2.3 组 1.2.4 抽象概念(登录组) 1.2.5 服务 1.3 安全标识符 1.3.1 安全标识符的组成 1.3.2 安全标识符的颁发机构 1.3.3 服务安全标识符 1.3.4 内置安全标识符 小结 相关资源 第2章 认证系统和认证协议 2.1 用户已知和已有的凭证 2.1.1 用户已知道的凭证 2.1.2 用户所有的凭证 2.1.3 用户的生物特征 2.2 认证符存储 2.2.1 LM哈希运算 2.2.2 NT哈希运算 2.2.3 密码验证 2.2.4 存储器 2.2.5 反转加密 2.3 认证协议 2.3.1 基本身份认证 2.3.2 质询-响应协议 2.4 智能卡认证 2.4.1 智能卡和密码 2.5 密码攻击 2.5.1 获得密码 2.5.2 利用截获的信息 2.5.3 保护密码 2.6 管理密码 2.6.1 使用其他认证系统 2.6.2 安全地记录密码 2.6.3 使用密码短语 2.6.4 制定密码策略 2.6.5 细化密码策略 小结 相关资源 第3章 管理对象 3.1 访问控制术语 3.1.1 安全对象 3.1.2 安全描述符 3.1.3 访问控制列表 3.1.4 访问控制列表项(ACE) 3.1.5 访问掩码 3.1.6 访问列表结构间的联系 3.1.7 继承 3.1.8 安全令牌 3.1.9 访问审核进程 3.1.10 完整性标记 3.1.11 空和NULL DACL 3.1.12 安全描述定义语言(SDDL) 3.2 权限管理工具 3.2.1 cacls和icacls 3.2.2 SC 3.2.3 subinacl 3.3 Windows Server 2008中访问控制的改变 3.3.1 TrustedInstaller权限 3.3.2 网络位置SID 3.3.3 文件系统名称空间的改变 3.3.4 Power User权限移除 3.3.5 OWNER_RIGHT和所有权 3.4 用户权利和特权 3.5 RBAC和AZMAN 小结 相关资源 第4章 用户账户控制(UAC) 4.1 用户账户控制概述 4.2 令牌筛选 4.3 UAC组件 4.3.1 UAC提升用户体验 4.3.2 应用程序信息服务(AIS) 4.3.3 文件和注册表虚拟化 4.3.4 应用程序清单与执行请求级别 4.3.5 安装程序检测技术 4.3.6 用户界面特权隔离 4.3.7 安全桌面 4.3.8 使用远程协助 4.3.9 UAC远程管理限制 4.3.10 在管理批准模式下映射网络驱动程序 4.3.11 登录时阻止应用程序 4.3.12 用UAC配置应用程序的兼容性 4.4 UAC组策略设置 4.4.1 在安全选项下创建UAC组策略 4.4.2 UAC相关策略 4.5 Windows Server 2008和Windows Vista SP1中的UAC新特性 4.6 UAC最佳实践 4.6.1 不错的解决方案 4.6.2 更好的解决方案 4.6.3 最好的解决方案 小结 相关资源 第5章 防火墙和网络访问保护 第6章 服务 第7章 组策略 第8章 审核 第2部分 使用活动目录实现身份与访问控制 第9章 活动目录域服务安全性设计 第10章 活动目录证书服务 第3部分 常用的安全方案 第11章 服务器角色安全 第12章 补丁管理 第13章 保障网络安全 第14章 分支机构的安全 第15章 中小企业解决方案 第16章 应用服务器安全

章节摘录

插图：在某些系统中使用的认证方式是生物特征，也就是通过用户的某些生物特征作为认证要素。
比如视网膜扫描、指纹、血样和声音识别等，甚至连敲击键盘的输入习惯都可以用来认证。
不过，这些认证方法是存在争议的，由于它们只是基于“只有使用者会知道的事物”来进行认证的，不能提供双重认证，因此是不可靠的。
生物特征认证的不准确是有原因的。
虽然DNA能够提供准确的认证，但大多数用户并不接受这种认证方式，因为需要提供血样。
而其他生物特征因素并不能如DNA一样准确，比如指纹识别，指纹是人体独一无二的特征，但如果在计算机系统中重复记录同一指纹，却很难确保能产生完全一样的印痕，也不能保证计算机能够对同一指纹做出完全相同的解释。
因此，生物特征认证系统是在一定的范围内进行操作的，而且用户必须要将生物特征要素存储很多次，自动生成一个能够被系统识别的范围，在经过多次试验后才能进行准确的认证。
生物特征识别系统还有很多其他的缺陷。
首先，除输入习惯方式外，其他方式都要求客户机要有一个专用的硬件设施，而且有些方式很难为人所接受。
在用户所有的凭证系统中也是如此，比如智能卡。
其次，使用生物特征认证时，必须要精确的匹配才能进行准确的认证。
这将是致命的弱点，因为如果用户的生物特征由于某些原因而发生了变化，就会导致认证失败。
例如如果使用声音识别认证，那么当用户生病或疲劳时，声音发生了变化，就无法进入该系统。
再次，很多人认为生物特征认证侵犯了人的隐私，他们不愿意将指纹等隐私信息存储于计算机系统中。

编辑推荐

《Windows Server 2008安全技术详解》包含计划、实施和管理Wind噢萎缩 Server 2008安全功能所需要的信息，非常深入和全面。
读者可以从领先的行业专家和微软安全团队这些掌握最佳技术的人那里获得权威的技术指导。
除此之外，还有重要脚本、工具和其他资源可以在线下载。
专家的指导包括：使用新型组策略特性，配置坚固安全的系统借助用户访问控制（UAC）确保最小访问权限借助高级安全、IPsec和NAP配置Wiridows防火墙部署新的活动目录服务和功能网络威胁模型理解服务攻击载体与最小暴露管理服务器角色，创建服务器隔离策略为应用服务器配置IIS 7.0安全特性实施粒度审计策略确定软件升级策略在分支机构中使用只读域控制器实现安全管理

版权说明