第一图书网, tushu007.com

<<网管员必备宝典>>

图书基本信息

书名：<<网管员必备宝典>>

13位ISBN编号：9787302149934

10位ISBN编号：7302149933

出版时间：2007-5

出版时间：清华大学出版社

作者：王文寿等

页数：526

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

<<网管员必备宝典>>

内容概要

《网管员必备宝典：网络安全》是一本基于企业安全需求角度编写的网络安全类图书，没有纯粹的深奥难懂的技术原理介绍，只有出于实际安全需求的经验总结和应用配置。

《网管员必备宝典：网络安全》共9章，第1章从全局角度分析了当前企业网络安全的形势和需求，介绍了网络安全基础知识。

第2章到第9章分别介绍一个相对独立的安全技术应用，它们分别是：计算机病毒、木马和恶意软件的清除和防护，防火墙技术的应用，堡垒主机的配置，ISA Server 2004的应用配置，端口扫描和入侵检测应用，网络安全隔离，文件加密和数字签名，以及Windows Server 2003系统的主要安全功能配置。

《网管员必备宝典：网络安全》的最大的特点就是实用性、可操作性和系统性非常强，而且基本上覆盖了Windows Server 2003域网络系统的主要网络安全配置。

《网管员必备宝典：网络安全》可供企业网络管理员参考，以及作为各类培训机构的网络安全和应用培训教程。

第一图书网, tushu007.com

<<网管员必备宝典>>

书籍目录

第1章 企业网络安全概述 1.1 企业网络安全概述 1.2 网络安全威胁的分类与基本对策 1.2.1 计算机病毒 1.2.2 木马 1.2.3 网络监听 1.2.4 黑客攻击 1.2.5 恶意软件 1.2.6 天灾人祸 1.3 造成网络安全威胁的主要根源 1.3.1 系统或程序本身的设计不足 1.3.2 网络安全防护设施不完善 1.3.3 缺乏系统的安全防护知识 1.3.4 日常管理不善 1.4 网络攻击的行为特征和防御方法 1.4.1 拒绝服务攻击行为特征和防御方法 1.4.2 利用型攻击方式行为特征和防御方法 1.4.3 信息收集型攻击行为特征和防御方法 1.4.4 假消息攻击行为特征和防御方法 1.4.5 路由协议和设备攻击行为特征及防御方法 1.5 企业网络安全策略 1.5.1 常见的企业网络安全认识误区 1.5.2 网络安全策略设计的十大原则 1.5.3 企业网络安全的十大策略 1.5.4 实施网络安全策略的基本步骤 第2章 病毒、木马和恶意软件的清除与防护 2.1 计算机病毒和木马基础 2.1.1 计算机病毒的分类 2.1.2 计算机病毒的主要特点 2.1.3 木马简介 2.1.4 木马的伪装方式 2.1.5 木马的运行方式 2.2 计算机病毒的清除与防护 2.2.1 典型单机版计算机病毒防护程序 2.2.2 网络版杀毒软件 2.2.3 木马的检测、清除与防范 2.3 恶意软件的查杀和防护 2.3.1 恶意软件概述 2.3.2 恶意软件的分类与防护 2.3.3 恶意软件的清除 第3章 防火墙技术及应用 3.1 防火墙基础 3.1.1 防火墙概述 3.1.2 防火墙的基本功能 3.1.3 防火墙的特殊功能 3.1.4 防火墙的基本特性 3.1.5 防火墙的主要缺点 3.1.6 与防火墙有关的主要术语 3.2 防火墙的分类 3.2.1 从防火墙的软、硬件形式分 3.2.2 从防火墙技术来分 3.2.3 从防火墙体系结构分 3.3 防火墙在性能等级上的分类 3.3.1 个人防火墙 3.3.2 路由器防火墙 3.3.3 低端硬件防火墙 3.3.4 高端硬件防火墙 3.3.5 高端服务器防火墙 3.4 防火墙的主要应用 3.4.1 企业网络体系结构 3.4.2 控制来自互联网对内部网络的访问 3.4.3 控制来自第三方网络对内部网络的访问 3.4.4 控制内部网络不同部门之间的访问 3.4.5 控制对服务器中心的网络访问 3.5 内部防火墙系统应用 3.5.1 内部防火墙规则 3.5.2 内部防火墙的可用性需求 3.5.3 内部容错防火墙集配置 3.5.4 内部防火墙系统设计的其他因素要求 3.6 外围防火墙系统设计 3.6.1 外围防火墙规则 3.6.2 外围防火墙系统的可用性要求 3.7 用防火墙阻止SYN Flood攻击 3.7.1 SYN Flood攻击原理 3.7.2 用防火墙防御SYN Flood攻击 第4章 堡垒主机及其应用配置 4.1 堡垒主机方案 4.2 Windows Server 2003堡垒主机设置 4.2.1 配置堡垒主机的基本步骤 4.2.2 审核策略设置 4.2.3 用户权限分配设置 4.2.4 安全选项设置 4.2.5 事件日志设置 4.2.6 系统服务设置 4.2.7 其他安全设置 第5章 ISA Server 2004的应用 5.1 ISA Server 2004基础 5.1.1 ISA服务器概述 5.1.2 ISA Server 2004的主要功能 5.1.3 ISA Server 2004新增或改进功能 5.2 ISA Server 2004的安装 5.2.1 ISA Server 2004安装条件 5.2.2 安装注意点 5.2.3 默认设置 5.3 ISA Server 2004的网络配置 5.3.1 多网络结构 5.3.2 网络和网络集配置 5.3.3 网络模板 5.3.4 创建网络 5.3.5 创建网络集 5.3.6 应用网络模板 5.3.7 网络配置 5.4 网络规则 5.4.1 网络规则概述 5.4.2 创建网络规则 5.5 ISA防火墙策略基础 5.5.1 ISA防火墙策略工作方式 5.5.2 防火墙访问规则 5.5.3 ISA防火墙Web发布规则 5.5.4 ISA防火墙的安全Web发布规则 5.5.5 服务器发布规则 5.5.6 邮件服务器发布规则 5.5.7 ISA防火墙系统策略 5.5.8 ISA防火墙的Web请求身份验证 5.5.9 ISA防火墙身份验证过程 5.5.10 ISA防火墙发布规则配置选项 5.6 创建和配置防火墙规则 5.6.1 访问规则的创建与配置 5.6.2 配置ISA防火墙策略规则 5.7 ISA客户端的安装与配置 5.7.1 ISA客户端概述 5.7.2 防火墙客户端 5.7.3 防火墙客户端配置 5.7.4 SecureNAT客户端 5.7.5 Web代理客户端 第6章 端口扫描与入侵检测 6.1 端口简述 6.1.1 计算机网络服务 6.1.2 通信端口 6.1.3 常见服务器端口 6.2 端口扫描 6.2.1 网络通信基础 6.2.2 端口扫描原理 6.2.3 目前主流的端口扫描技术 6.2.4 端口侦听 6.3 端口扫描器应用 6.3.1 NetBrute的应用 6.3.2 SuperScan?应用 6.3.3 X-Scan应用 6.4 入侵检测 6.4.1 入侵检测概述 6.4.2 入侵检测技术的发展历程 6.4.3 入侵检测技术分类 6.4.4 入侵检测技术分析 6.5 典型入侵检测系统 6.5.1 华强IDS 6.5.2 黑盾网

第一图书网, tushu007.com

络入侵检测系统（HD-NIDS） 第7章 企业网络安全隔离 7.1 通过子网掩码划分子网概述 7.2 VLAN子网的划分 7.2.1 VLAN简介 7.2.2 VLAN的划分方式 7.2.3 VLAN的主要用途 7.2.4 VLAN的主要应用 7.3 三层交换机上的VLAN配置 7.3.1 设置VTP域（VTP Domain） 7.3.2 配置聚合链路（Trunk）协议 7.3.3 创建VLAN组 7.3.4 配置三层交换端口 7.4 VLAN网络配置实例 7.4.1 VLAN的创建 7.4.2 VLAN端口号的应用 7.5 网络隔离概述 7.5.1 网络隔离技术基础 7.5.2 网络隔离的安全控制要点和发展方向 7.6 物理隔离 7.6.1 物理隔离概述 7.6.2 物理隔离原理 7.6.3 主要物理隔离产品 7.6.4 物理隔离方案 7.7 物理隔离卡产品及应用 7.7.1 物理隔离卡概述 7.7.2 物理隔离卡应用模式 7.7.3 图文网络安全物理隔离器 7.7.4 利普隔离卡产品 7.8 网络线路选择器 7.8.1 网络线路选择器概述 7.8.2 典型网络线路选择器介绍 7.9 物理隔离网闸 7.9.1 物理隔离网闸概述 7.9.2 物理隔离网闸工作原理 7.9.3 物理隔离网闸的应用 7.9.4 两个物理隔离网闸应用方案 第8章 文件加密与数字签名 8.1 文件加密和数字签名技术概述 8.1.1 文件加密和数字签名的由来和意义 8.1.2 文件加密和数字签名的应用 8.1.3 典型数据加密算法 8.2 EFS文件加密技术 8.2.1 EFS概述 8.2.2 使用EFS的最佳操作建议 8.3 使用EFS对文件或文件夹加密和解密 8.3.1 利用EFS进行文件加密 8.3.2 利用EFS对文件和文件夹进行解密 8.3.3 加密属性的改变 8.4 恢复数据 8.4.1 故障恢复策略与故障恢复代理 8.4.2 更改本地计算机的故障恢复策略 8.4.3 更改域的故障恢复策略 8.5 数据恢复代理 8.5.1 数据恢复代理和EFS证书 8.5.2 配置故障恢复代理的一般步骤 8.5.3 企业证书颁发机构的创建 8.5.4 配置EFS故障恢复代理模板 8.5.5 申请EFS故障恢复代理证书 8.5.6 添加域的故障恢复代理 8.5.7 创建默认的独立计算机上的数据恢复代理 8.5.8 启用EFS文件共享 8.6 密钥的存档与恢复 8.6.1 密钥的存档与恢复概述 8.6.2 创建密钥恢复代理账户 8.6.3 获取密钥恢复代理证书 8.6.4 配置密钥存档和恢复属性 8.6.5 创建新的可以进行密钥存档的证书模板 8.6.6 获取具有存档密钥的用户证书 8.6.7 执行密钥恢复示例 8.6.8 导入已恢复的私钥 8.7 PKI在文件传输加密和数字签名方面的应用 8.7.1 配置密钥用法 8.7.2 文件传输加密 8.7.3 数字签名 8.7.4 加密密钥对的获取 8.7.5 邮件中的文件加密和数字签名 8.8 PGP文件加密和数字签名 8.8.1 PGP密钥的创建 8.8.2 公/私钥的获取 8.8.3 PGP在文件加密方面的应用 8.8.4 PGP在数字签名方面的应用 第9章 Windows Server 2003安全系统配置 9.1 新增安全功能 9.1.1 新增安全功能 9.1.2 原有安全功能的改进 9.2 Windows Server 2003系统安全 9.2.1 系统安全概述 9.2.2 安全性的最佳操作建议 9.2.3 组的默认安全设置 9.3 安全配置与分析 9.3.1 安全配置和分析概述 9.3.2 安全模板概述 9.3.3 安全模板的组成 9.3.4 预定义的安全模板 9.3.5 模板的自定义和导入 9.3.6 通过组策略应用安全设置 9.4 身份验证 9.4.1 身份验证协议 9.4.2 智能卡 9.4.3 用户密码 9.4.4 存储用户名和密码 9.5 访问控制 9.5.1 访问控制概述 9.5.2 访问控制中的“权限” 9.5.3 选择文件和文件夹权限的应用位置 9.6 Active Directory中的访问控制 9.6.1 Active Directory中的访问控制概述 9.6.2 Active Directory对象权限 9.6.3 指派Active Directory对象权限的最佳操作 9.7 软件限制策略 9.7.1 使用软件限制策略的最佳操作建议 9.7.2 应用软件限制策略 9.7.3 安全级别和其他规则 9.7.4 软件限制策略规则的优先权 9.7.5 将默认安全级别设置为“不允许的” 9.7.6 打开软件限制策略 9.7.7 新建软件限制策略 9.7.8 软件限制策略配置

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