第6章 Windows系统的安全机制

帐户管理的未来趋势

01 基于角色的访问控制（RBAC）

RBAC通过角色分配权限，简化了权限管理，提高了系统的灵活性和安全性。

02 多因素认证（MFA）

MFA要求用户提供两个或多个验证因素，显著提高了帐户的安全性。

03 云服务中的帐户管理

在云服务环境中，帐户管理需要适应云架构的特点，如动态扩展和多租户支持。

帐户安全威胁与防护

01

帐户劫持与防护措施

帐户劫持是一种安全威胁，通过防护措施如多因素认证和定期密码更改可以降低风险。

02

帐户策略的常见威胁

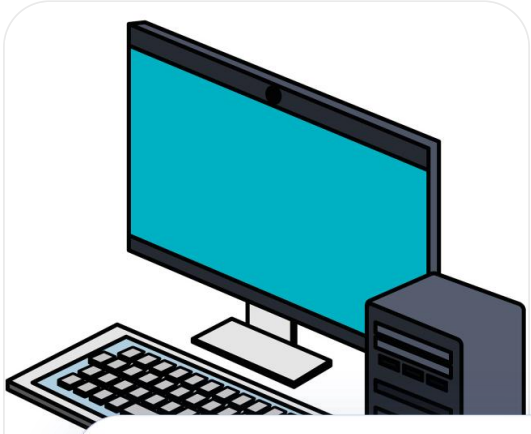
帐户策略可能受到多种威胁，包括密码猜测、社会工程学攻击和内部威胁。

03

防护策略与安全更新

定期更新防护策略和系统安全，以应对新出现的威胁和漏洞。

远程帐户管理与访问控制



01

远程桌面与远程管理

远程桌面和远程管理工具允许管理员从远程位置管理服务器，但需确保安全措施到位。

02

访问控制列表（ACL）

ACL定义了哪些用户或组可以访问特定资源，是实现细粒度访问控制的基础。

03

帐户的远程访问权限设置

正确配置帐户的远程访问权限，可以确保只有授权用户能够远程连接到服务器。

帐户管理工具与技术

01

本地用户和组管理

本地用户和组管理工具允许管理员在单个服务器上创建和管理用户帐户和组。

02

域用户和组管理

域用户和组管理工具用于跨多个服务器和工作站管理帐户，是大型网络环境中的关键组件。

03

PowerShell在帐户管理中的应用

PowerShell脚本和命令提供了强大的自动化帐户管理能力，可以执行复杂的管理任务。

帐户安全最佳实践

强制密码历史确保用户不能重复使用旧密码，而定期更改密码有助于减少密码被破解的风险。

强制密码历史与更改

根据组织的具体需求定制帐户策略，可以更有效地保护系统安全。

帐户策略的定制化

安全模板提供了一种快速部署和管理安全策略的方法，有助于标准化安全配置。

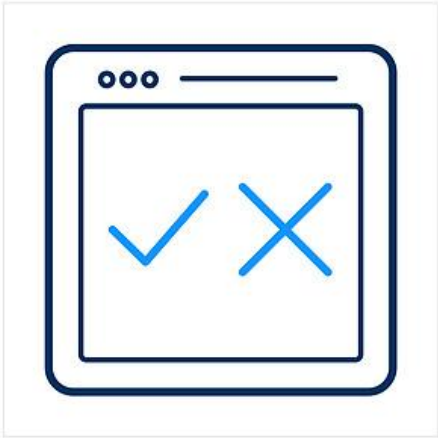
安全模板的应用

Online Survey

Customer Satisfaction

Online Survey

Review Administrator



Online Administrator

审核策略与帐户活动

审核登录事件

审核登录事件有助于追踪和记录谁在何时尝试访问系统资源。

审核权限使用

审核权限使用可以监控对关键文件和设置的访问，确保只有授权用户进行更改。

审核策略的配置与管理

正确配置和管理审核策略是确保系统安全的关键步骤，涉及选择要审核的事件类型。

密码策略与帐户锁定

密码复杂性要求

密码策略可以设置复杂性要求，如最小长度、包含字符类型，以提高安全性。

密码过期与更新

定期更新密码是防止密码泄露的重要措施，密码过期策略强制用户定期更改密码。

帐户锁定策略

帐户锁定策略在多次无效登录尝试后锁定帐户，防止暴力破解攻击。

帐户权限控制基础

权限与权限继承

权限定义了用户可以执行的操作，而权限继承允许子对象继承父对象的权限设置。

最小权限原则

最小权限原则建议为用户和应用程序分配完成任务所需的最低权限，以减少安全风险。

权限委派与管理

权限委派允许管理员将权限分配给其他用户或组，实现灵活的权限管理。

Windows Server帐户类型

内置帐户与用户帐户

Windows Server提供内置帐户，如Administrator，以及可创建的用户帐户，用于日常管理和访问控制。

服务帐户与组帐户

服务帐户用于运行服务，而组帐户则允许将多个用户或服务归为一组，简化权限管理。

特殊标识符帐户

特殊标识符帐户如SYSTEM和GUEST，它们具有特定的系统权限和访问级别，用于执行特定任务。