深入探讨:宿主操作系统的层次安全技术 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/291/2021_2022__E6_B7_B1_E5_85_A5_E6_8E_A2_E8_c67_291891.htm 操作系统是大型数据库系统的运行平台，为数据库系统提供一定程度的安全保护。目前操作系统平台大多数集中在Windows NT 和Unix，安全级别通常为C1、C2级。主要安全技术有操作系统安全策略、安全管理策略、数据安全等方面。 操作系统安全策略用于配置本地计算机的安全设置，包括密码策略、账户锁定策略、审核策略、IP安全策略、用户权利指派、加密数据的恢复代理以及其它安全选项[7]。具体可以体现在用户账户、口令、访问权限、审计等方面。 用户账户：用户访问系统的"身份证"，只有合法用户才有账户。 口令：用户的口令为用户访问系统提供一道验证。 访问权限：规定用户的权限。 审计：对用户的行为进行跟踪和记录，便于系统管理员分析系统的访问情况以及事后的追查使用。 安全管理策略是指网络管理员对系统实施安全管理所采取的方法及策略。针对不同的操作系统、网络环境需要采取的安全管理策略一般也不尽相同，其核心是保证服务器的安全和分配好各类用户的权限。 数据安全主要体现在以下几个方面：数据加密技术、数据备份、数据存储的安全性、数据传输的安全性等。可以采用的技术很多，主要有Kerberos认证、IPSec、SSL、TLS、VPN（PPTP、L2TP）等技术。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com