信息系统安全——董开坤

第一章 绪论

1.1 信息技术的告诉发展和网络空间安全态势

网络空间安全已扩展至诸多领域，呈现出*综合性*和*全球性*的新特点。（ ）

1.2 网络空间安全的基本概念

1.信息的安全属性？

2.网络空间安全的核心内涵是网络安全（ ）

1.3 网络空间面临的安全威胁

1.威胁的来源？

2.威胁的层次？

3.系统层安全是网络空间安全的物质基础，失去物质基础，网络空间安全就会变成空中阁楼。（ ）

1.4 网络空间安全的技术体系

新的网络空间安全分层技术体系与旧体系有什么区别？

1.5 信息系统安全技术

1.操作系统安全是信息系统安全的基础（ ）

2.信息系统安全防护的基本原则？

第二章 安全认证

2.1 安全认证概述

1.安全认证是对用户、进程、系统、网络连接等实体身份进行审核，证实其合法性的过程，列举几种身份认证技术。

2.安全认证是信息系统的第一道安全防线，是其他安全机制的基础（ ）

3.标识是实体可以被系统识别的内部名称，具有唯一性，通常是公开的，鉴别是实体标识与实体联系的过程，鉴别过程应该也是公开的。（ ）

2.2 基于知识的身份认证

这一节主要掌握的还是动态口令技术，分值要均衡

2.3 基于令牌的身份认证

令牌具有唯一、易识别的特点，但容易被伪造（ ）

2.4 基于生理特征的身份认证

1.基于指纹的身份认证是直接对比指纹图像来进行认证（ ）

2.优缺点？

2.5 基于行为特征的身份认证

什么是交叉错判率，有什么作用？

2.6 人工交互认证（无）

2.7 多因素和附加认证技术

多因素认证是组合任意两种认证技术，以提高安全性或可用性（ ）

第三章 访问控制

3.1 访问控制概述

1.客体是包含或接收信息的被动实体，例如用户和进程（ ）
2.授权是规定客体可以对主体执行的动作（ ）
3.安全的系统初始于授权状态，且不会进入未授权状态（ ）

3.2 自主访问控制

1.自主访问控制的访问口令实现方式使用的口令与身份认证口令相同（ ）
2.访问控制矩阵用主体的标识索引矩阵的列，客体的标识索引矩阵的行（ ）
3.访问能力表是主体可访问的客体明细表，表中包含主体的身份和主体可访问的客体（ ）
4.访问控制表是每个客体上附加的主体明细表，表中包含客体的标识和主体对该客体的访问权限（ ）
5.授权关系表中的每一行表示了主体和客体的一个权限关系，特别适合非关系数据库（ ）
6.自主访问控制的局限性？

3.3 强制访问控制

1.客体的拥有者无权传播该客体的访问权限（ ）
2.定义一个安全级别以及级别间的比较关系
3.BLP 的安全目标是完整性，Biba 的安全目标是机密性（ ）
4.BLP 是第一个经严格数学证明的安全模型（ ）
5.什么是隐蔽通道？
6.如果系统初态是安全的，即使系统状态的每次变化都能满足 SS-策略、*-策略和 DS-策略的要求，系统也有可能进入非安全状态（ ）
7.Biba 模型中数据完整性的四种（五类）定义
8.Biba 模型中主体级别越高，其重要性和安全性越高，客体级别越高，其可信性和可靠性越高（ ）
9.Biba 模型的五种安全访问规则

3.4 基于角色的访问控制（RBAC）

1.传统访问控制在授权管理方面的局限性
2.RBAC 模型必须支持多对多的用户-角色指派；必须支持多对多的权限-角色指派；必须支持权限-角色检查（ ）
3.有约束的 RBAC 模型引入了职责分离机制，在有角色继承的 RBAC 基础上支持权限-角色检查（ ）
4.系统不会将存在 SSD 约束的两个角色分配给一个用户，但可以将存在 DSD 约束的两个角色分配给一个用户（ ）

3.5 最小特权管理

最小特权原则和需知原则的区别？ # 课件里的问题，没有答案

第四章 安全审计

4.1 安全审计概述

1.安全审计的直接安全目标是监视系统中其他安全机制的运行情况和可信度，间接安全目标是跟踪、监视信息系统中的异常事件（ ）
2.审计踪迹是信息系统审计用户操作的最基本单位（ ）

4.2 安全审计系统模型

1.在 X.816 标准定义的审计系统模型中，事件鉴别器、报警处理器、审计分析器

都能够定义新的审计事件，并向审计记录器发送审计消息（ ）
2.审计提供器可以提供人工可读的安全报告（ ）
3.安全审计模型根据审计数据不同的应用层次可以划分为哪四个部分？
5.入侵检测和安全审计可以是应用程序也可以是系统程序（ ）

4.3 安全审计系统的设计与实现

设计实现一个安全审计系统　　# 看起来比较适合出大题

第五章 Windows 操作系统安全

5.1 操作系统安全基础

1.Windows 操作系统有哪几种隔离控制方法？
2.Windows 系统模式可以执行任意指令、访问任意内存地址、硬件设备、中断操作、改变处理器特权状态、访问内存管理单元、修改寄存器（ ）
3.系统调用是从用户模式进入内核模式的系统程序，用户可以更改系统调用来实现自己需要的功能（ ）
4.从执行者角度来看，系统调用和库函数有重大区别；从用户角度来看，区别不重要（ ）
5.讲两种操作系统内核实现方法及其优缺点
6.增量备份是持续跟踪目标数据的改变，并将其备份（ ）
7.D 类安全等级系统只为用户提供安全保护（ ）
8.C 类安全等级能够提供审计和保护，为用户的行动和责任提供审计能力，可分为自主安全保护系统和受控存取控制系统（ ）
9.B 类安全等级系统中，用户如果没有与安全等级相连，系统就不会让用户存取对象（ ）
10.B 类安全级的细分

5.2 Windows 安全概述

1.什么是客体重用？
2.可信通路机制主要应用在用户登录或注册时，以保证用户确实是和安全核心通信，防止不可信进程模拟系统的登录过程而窃取口令（ ）
3.活动目录的安全管理单元是计算机用户（ ）
4.Winlogon 进程是系统启动自动启动的一个程序，负责管理用户登录和注销过程，加载登录界面并监视安全认证的顺序（ ）
5.GINA 为用户提供图形化的交互式登录对话框，包括几个动态库文件，被 Winlogon 进程调用（ ）
6.LSA 是安全子系统的核心组件，负责加载认证包，管理域间的信任关系，在账户登录到系统时发放安全令牌（ ）
7.描述一下 NTLM 工作流程
8.SAM 数据库存储本地用户和本地组的账户以及相关安全信息，其文件以文本格式存储（ ）

5.3 Windows 本地安全机制

1.全局用户账户创建于服务器，可以在网络中任何计算机上登录，使用范围是整个网络（ ）
2.每次创建一个用户或一个组的时候，系统会给它分配一个的安全标识符，删除用户或组后，安全标识符回收，可用于新创建的用户或组（ ）

3.安全标识符的唯一性由什么确定？
4.讲讲 Windows 本地身份认证过程
5.安全令牌是用户登录时获得的，用户权限改变时令牌也会同时改变（ ）
6.对象访问事件审计是用自主访问控制列表 DACL 对基于 Windows 的网络中的所有对象启用审计（ ）
7.Windows 中有哪几种日志文件？
8.FAT 和 NTFS 文件系统都具备可靠性和兼容性，NTFS 分区另外支持自主访问控制和拥有权（ ）

5.4 Windows 网络安全技术

1.IPsec 是一个能够在 IP 层提供互联网通信安全的协议（ ）
2.IPSec 协议族由什么组成？
3.在源主机到目的主机建立的安全关联 SA 上传送的是 IP 安全数据包，可以实现双向安全通信（ ）
4.Windows 服务器的安全配置

第六章 Linux 操作系统安全

6.1 Linux 安全概述

1.Linux 中的所有进程都由 init 进程衍生，其进程号是 0（ ）
2.Linux 系统的主要安全威胁

6.2 Linux 本地安全机制

1.用户信息保存为普通文本文件，只有文件属主用户可读（ ）
2./etc/shadow 文件存储着用户名和加密口令，只有 root 用户可读（ ）
3.Linux 系统基本的文件类型有？

6.3 Linux 网络安全技术

1.Linux 如何配置 Web 服务安全
2.Netfilter/Iptables 防火墙五链四表
3.Linux 入侵检测程序 Snort 有嗅探器、数据包记录器、网络入侵检测系统三种工作模式（ ）

第七章 数据库系统安全

7.1 数据库系统安全概述

数据库系统安全威胁源可分为哪五类？

7.2 数据库系统的安全需求

1.数据库可审计性的含义
2.数据库系统安全完全取决于内部安全机制（ ）
3.描述一下数据库系统的安全防护层次
4.SQL 注入攻击最基本的防范方法是不允许输入’和将输入的’转换（ ）

7.3 数据库系统的安全机制

1.视图机制是通过定义不同的视图将用户无权访问的数据隐藏起来，用户可以对视图中的数据进行增删改查（ ）
2.库外加密、库内加密的含义和优缺点以及数据库加密技术的局限
3.攻击者可以利用数据之间的关系使用低安全等级的数据推导出高安全等级的

数据（ ）

7.4 SQL Server 数据库安全

1.SQL Server 数据库的四道安全防线

2.Windows 身份认证模式的前提是已创建与 Windows 账号对应的 SQL Server 账号（ ）

3.SQL Server 数据控制实现

第八章 信息系统安全测评

这章不挑了，计算题已经占 20 分了，最多也就是简答题再占 5 分，浅过一遍

第九章 可信计算

9.1 可信计算概述

1.可信计算是指计算机运算的同时进行安全防护，使操作和过程行为在一定条件下的结果总是与预期一样，计算全程可测可控，使一种运算和防护并存的自我免疫的新计算模式（ ）

2.可信计算系统是能够提供系统的可靠性、可用性、信息和行为安全性的计算机系统（ ）

9.2 可信计算机系统的组成和技术原理

1.可信计算机系统的组成？

2.可信平台模块把信任关系从信任根扩展到整个计算机系统（ ）

9.3 可信计算技术的应用

列举 5 个可信计算的应用领域