

计 算 机 系 统 安 全 试题卷（A）

题号	一	二	三	四	五	六	七	八	九	十	总 分
分数											

一、判断题（每题 1 分，共 10 分）

得分

1. 硬件结构的安全是信息系统安全的基础。（ ）
2. 稳定不变是用于身份认证的生理特征的必要条件，但也是用于安全认证的缺点。（ ）
3. 访问控制中，客体是可以导致信息流动，或使系统状态发生变化的主动实体。（ ）
4. 在强制访问控制策略下，主体可以改变自己、自己所拥有客体的安全属性。（ ）
5. BLP 模型的特点是不上读、不下写。（ ）
6. 安全审计是信息系统安全的最后防线，是访问控制的必要补充。（ ）
7. 隐蔽通道的存在违反了信息系统的安全策略。（ ）
8. Windows 操作系统中，用户通过身份认证后，登录进程会为其创建一个安全描述符，相当于用户访问系统资源的票证。（ ）
9. Linux 系统中，特权程序是可以暂时获得管理员权限并执行一些管理员特权功能的程序。（ ）
10. 数据库库外加密只能以整个数据库文件为单位进行加密。（ ）

二、简答题（每题 5 分，共 30 分）

得分

1. 请列举出 5 种自主访问控制的实现方式。
2. 简述特权对信息系统安全的危害，那为什么还要提供特权？
3. 信息系统安全审计有何作用？
4. 说明数据库安全中，数据完整性的含义。
5. 什么是 Linux 系统中的僵尸进程？僵尸进程有何危害？
6. 信息安全风险评估中，什么是残余风险？如何对待残余风险？

三、分析、设计题（每题 15 分，共 30 分）

得分

1. 设计一种动态口令身份认证机制，说明口令的使用和验证过程，并分析其可以抵御哪些口令攻击？
2. 叙述 Windows 操作系统中一种加密文件系统（例如 EFS）的工作原理，分析其安全性。

四、计算题（20 分）

得分

假设有 3 个重要资产 A1、A2 和 A3，资产所面临的威胁以及威胁可利用的资产的脆弱性见表 1，括号内是其等级值。要求使用矩阵法计算资产的风险值及风险等级。矩阵的构建和等级划分表如表 2 - 表 7 所示，写出详细的风险计算过程。

表 1 资产、威胁、脆弱性表

资产	威胁	脆弱性
资产 A1（3）	威胁 T1（5）	脆弱性 V1（3）
	威胁 T2（2）	脆弱性 V2（2）
		脆弱性 V3（5）
	威胁 T3（4）	脆弱性 V4（2）
资产 A2（4）	威胁 T4（3）	脆弱性 V5（3）
	威胁 T5（4）	脆弱性 V6（4）
资产 A3（5）	威胁 T6（1）	脆弱性 V7（4）
		脆弱性 V8（2）

表 2 安全事件发生可能性矩阵

	脆弱性 严重程度	1	2	3	4	5
威胁 发生 频率	1	2	4	7	11	14
	2	3	6	10	13	17
	3	5	9	12	16	20
	4	7	11	14	18	22
	5	8	12	17	20	25

表 3 安全事件可能性等级划分表

安全事件发生可能性值	1-5	6-11	12-16	17-21	22-25
发生可能性等级	1	2	3	4	5

表 4 安全事件损失矩阵

	脆弱性 严重程度	1	2	3	4	5
资产价值	1	2	4	6	10	13
	2	3	5	9	12	16
	3	4	7	11	15	20
	4	5	8	14	19	22
	5	6	10	16	21	25

表 5 安全事件损失等级划分表

安全事件损失值	1-5	6-10	11-15	16-20	21-25
安全事件损失等级	1	2	3	4	5

表 6 风险矩阵

	可能性	1	2	3	4	5
损失	1	3	6	9	12	16
	2	5	8	11	15	18
	3	6	9	13	17	21
	4	7	11	16	20	23
	5	9	14	20	23	25

表 7 风险等级划分表

风险值	1-6	7-12	13-18	19-23	24-25
风险等级	1	2	3	4	5

五、论述题（10 分）

得分

本次在线考试，利用学生的电脑、手机等设备在学生的家里搭建了在线考试环境（系统），请利用学习的信息系统安全原理分析，这种在线考试环境能否从技术上保证学生无法作弊？