计算机系统安全参考答案(by lyd&zhy)

一、判断题 （每题 1 分，共 10分）

1. (√)
2. (√)
3. (×)
   - 主体：可导致信息在客体间流动，或使系统状态发生变化的主动实体。
4. (×)
   - 主体不能改变自己、自己所拥有客体、其他主体、以及其他所有客体的安全属性。
5. (√)
6. (√)
7. (√)
8. (×)
   - 用户通过身份认证后，登录进程会为其创建一个访问令牌，该令牌相当于用户访问系统资源的票证。
9. (√)
10. (×)

二、 简答题 （每题 5 分，共 30分）

1. 请列举出 5 种 自主访问控制的实现方式 。

- 访问口令（Passwords for Access）
- 访问控制矩阵（Access Control Matrix）
- 访问能力表（Access Capability List）
- 访问控制表（Access Control List，ACL）
- 授权关系表（Authorization Relations）
- 属主/同组用户/其他用户(Owner/Group/Other)

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?

- 特权对信息系统安全的危害
  - 被滥用
  - 被窃取
  - 被误用
- 特权存在的原因
  - 便于系统维护
  - 提高系统的可用性

3. 信息系统安全审计有何作用?

- 系统安全的最后防线，访问控制的必要补充。
- 重建事件
- 监测潜在的入侵，提供入侵检测所需的原始数据
- 故障监测
  - 定位安全问题
  - 帮助故障分析
- 发现系统不足
- 与其它安全机制联动

4. 说明数据库安全中，数据完整性的含义。

- 完整性
  - 防止对DBMS的非法访问和修改
  - 保护存储的数据、文件的安全性
- 数据的完整性
  - 物理数据库完整性
    - 整个数据库损毁
    - 保证数据能够物理读取
  - 逻辑数据库完整性
    - 保护数据库的结构
  - 元素完整性
    - 数据元素只能由授权用户改变

5. 什么是 Linux 系统中的僵尸进程，僵尸进程有何危害?

- 僵尸进程定义：
  - 一个进程调用了exit后，并非马上消失，而是留下一个称为僵尸进程（Zombie）的数据结构。
  - 僵尸进程放弃了几乎所有内存空间，无任何可执行代码，也不能被调度，仅仅在进程表中保留一个位置，记载该进程的退出状态等信息供其他进程收集。
- 僵尸进程危害：
  - Linux系统中进程数目是有限制的；
  - 如果存在太多的僵尸进程，会占用内存资源，影响系统性能和新进程的产生，甚至导致系统瘫痪。

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?

- 残余风险定义：
  - 残余风险是指在实现了新的或增强的安全控制后还剩下的风险，实际上任何系统都是有风险的，并且也不是所有安全控制都能完全消除风险。
- 如何对待?
  - 没有必要采用所有的安全保护措施。因为这些措施要解决的风险可能并不存在，或者可以容忍和接受这些风险。
  - 没有必要防范和加固所有的安全弱点。这些弱点可能因为成本、知识、文化及法律等方面的因素，而没有人能利用它们。
  - 我们没有必要无限制地提高安全保护措施的强度。只需要将相应的风险降低到可接受的程度即可。供)对安全保护措施的选择还要考虑到成本和技术等因素的限制。

三、分析、设计题（每题15分，共30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?

- 第二章PPT 攻击14~15页 使用和验证过程：16页~20页

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。

- EFS是通过对称和不对称两种方法来对文件及其相关内容进行加密的，对于文件内容本身EFS是采用对称算法进行加密的，加密的密钥是FEK，但若只采用这一种加密算法，显然是不够安全的，所以WINDOWS会利用一对公钥/私钥对FEK进行加解密，加密后的FEK和加密文件是存放在一起的，然后WINDOWS再利用称为主密钥的文件对私钥进行加密，最后再通过用户名和密码对主密钥进行加密
- 公钥/私钥的加密算法虽然比对称加密算法安全，但若被加密的文件比较大，那么这种非对称加密算法的加密速度是非常慢的，所以EFS的加密过程是整合了对称加密算法和非对称加密算法的优势，以此来实现速度和安全两方面需求。

四、计算题（20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）

1. 计算安全事件发生可能性；

（1）构建安全事件发生可能性矩阵；

$L(T,V) = L(\text{威胁出现频率}, \text{脆弱性})$

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

（2）根据威胁发生频率值和脆弱性严重程度值在矩阵中进行对照，确定安全事件发生可能性值；

资产	威胁	脆弱性	可能性值	可能性等级
资产A1（3）	威胁T1（5）	脆弱性V1(3)	17	4
	威胁T2（2）	脆弱性V2(2)	6	2
		脆弱性V3(5)	17	4
	威胁T3（4）	脆弱性V4(2)	11	2
资产A2（4）	威胁T4（3）	脆弱性V5(3)	12	3
	威胁T5（4）	脆弱性V6(4)	18	4
资产A3（5）	威胁T6（1）	脆弱性V7(4)	11	2
		脆弱性V8(2)	4	1

（3）对计算得到的安全风险事件发生可能性进行等级划分。

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

2. 计算安全事件造成的损失；

（1）构建安全事件损失矩阵；

$F(Ia, Va) = F(\text{资产价值}, \text{脆弱性严重程度})$

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

（2）根据资产价值和脆弱性严重程度值在矩阵中进行对照，确定安全事件损失值；

资产	威胁	脆弱性	可能性值	可能性等级	损失值	损失等级
资产A1（3）	威胁T1（5）	脆弱性V1(3)	17	4	11	3
	威胁T2（2）	脆弱性V2(2)	6	2	7	2
		脆弱性V3(5)	17	4	20	4
	威胁T3（4）	脆弱性V4(2)	11	2	7	2
资产A2（4）	威胁T4（3）	脆弱性V5(3)	12	3	14	3
	威胁T5（4）	脆弱性V6(4)	18	4	19	4
资产A3（5）	威胁T6（1）	脆弱性V7(4)	11	2	21	5
		脆弱性V8(2)	4	1	10	2

（3）对计算得到的安全事件损失进行等级划分。

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

3. 计算风险值；

（1）构建风险矩阵；

$R(A,T,V)=R(L,F)=R(\text{安全事件的可能性},\text{安全事件造成的损失})$

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

（2）根据安全事件发生的可能性等级和安全事件损失在矩阵中进行对照，确定安全事件风险；

资产	威胁	脆弱性	可能性值	可能性等级	损失值	损失等级	风险值
资产A1（3）	威胁T1（5）	脆弱性V1(3)	17	4	11	3	17
	威胁T2（2）	脆弱性V2(2)	6	2	7	2	8
		脆弱性V3(5)	17	4	20	4	20
	威胁T3（4）	脆弱性V4(2)	11	2	7	2	8
资产A2（4）	威胁T4（3）	脆弱性V5(3)	12	3	14	3	13
	威胁T5（4）	脆弱性V6(4)	18	4	19	4	20
资产A3（5）	威胁T6（1）	脆弱性V7(4)	11	2	21	5	14
		脆弱性V8(2)	4	1	10	2	5

4. 结果判定。

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

资产	威胁	脆弱性	可能性值	可能性等级	损失值	损失等级	风险值	风险等级
资产A1（3）	威胁T1（5）	脆弱性V1(3)	17	4	11	3	17	3
	威胁T2（2）	脆弱性V2(2)	6	2	7	2	8	2
		脆弱性V3(5)	17	4	20	4	20	4
	威胁T3（4）	脆弱性V4(2)	11	2	7	2	8	2
资产A2（4）	威胁T4（3）	脆弱性V5(3)	12	3	14	3	13	3
	威胁T5（4）	脆弱性V6(4)	18	4	19	4	20	4
资产A3（5）	威胁T6（1）	脆弱性V7(4)	11	2	21	5	14	3
		脆弱性V8(2)	4	1	10	2	5	1

五、论述题（10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?

> 自由发挥叭