一、填空题

1、TCSEC（橘皮书）标准中，操作系统的安全级别从高到低分为：**A1级、B3级、B2**

**级、B1级、C2级、C1级和D级**。

2、安全访问令牌分为：**主令牌**和**模拟令牌**。

3、在Windows系统中，访问控制列表可以分为**自主访问控制列表**和**系统访问控制列表**两类。

二、选择题

1、windows7操作系统访问控制策略包括（**ABC**）

A. 自主访问控制策略；

B．基于角色的访问控制策略

C. 强制访问控制策略；

D. 基于属性的访问控制策略。

2、安全访问令牌在以下哪个模块中产生（**A**）

A. 本地安全认证（LSA）模块；

B. 安全账户管理（SAM）模块；

C. Netlogon模块；

D. 安全引用监控器（SRM）模块。

3、安全访问令牌可以与以下哪些实体关联（**ABD**）

A、进程；B. 用户；C. 资源；D. 线程；E. 被访问对象

4、Linux系统的用户口令保存在以下文件中（**A**）**B**

A. passwd文件；B.shadow文件；C.useradd文件；D. group文件

5、Linux系统中，以下哪些设备采用块设备文件**（AB）**

A.U盘；B硬盘；C.打印机；D.传真

三、简答题

1、安全审计时，不仅要记录失败事件，还要记录成功事件，为什么？

**记录失败事件可以查看哪些操作失败了，从而可以分析失败的原因。记录成功事件，是因为攻击者通过非法的手段获得访问权限后，也会生成一个成功事件，通过该事件我们可以对攻击事件溯源。**

2、简述Android 和Linux 操作系统安全机制之间的异同。

**相同：Android和Linux都是基于Linux内核的操作系统，并且在一定程度上共享相似的安全机制，例如权限控制、文件系统加密、进程隔离等。**

**不同：**

**1.应用程序沙盒：Android继承和扩展了Linux内核安全模型的用户与权限机制。通过将每个应用程序限制在一个独立的虚拟环境中，有效地防止应用程序之间相互干扰或进行恶意操作，内存的损坏只影响对应的程序，而其他程序不受影响；**

**2.包管理机制：apk文件中含有签名代码，用于控制哪些应用可以被赋予signature保护级别的权限以及检查代码有效性，在执行安装操作时，会进行包验证扫描，判断是否为恶意软件；**

**3.内存分配、回收机制：Android为每个进程分配内存的时候，刚开始只分配一个“够用”的量，然后根据需要增加，最大限度的让更多的进程在内存中运行。内存不足时，会回收内存，系统优先清理那些已经不再使用的进程或优先级较低的进程，或是倾向于杀死一个能回收更多内存的进程。**

四、问答题

1、POSIX是IEEE为Linux定制的可移植操作系统接口，请简述POSIX的权能机制。

**POSIX权能机制：特权细分：根据POSIX标准要求，可以将超级用户特权细分为权能集合，必须满足权能选择的标准（一个权能应该允许系统使一个进程不受一个特定安全需求约束）；所定义权能的实际效果之间应该有最小交集；在支持以上两条的基础上，权能定义的越少越好。**

2、如何保护文件加密密钥（FEK）？一旦用户删除或系统重装，Windows操作系统中的加密文件还能够恢复吗？

**用户（加密文件的拥有者）所设置的口令保护用户的主密钥，而主密钥保护用户的私钥，与该私钥对应的公钥被用于加密FEK。**

**在用户删除或系统重装后，即无法验证用户身份来获取解密文件所需的私钥，若留有身份证书和私钥备份，是可以恢复的；否则无法恢复。**