一、填空题

1、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。

2、病毒的特点是 隐蔽性、潜伏性 、破坏性 、寄生性 、传染性

3、安全访问令牌描述的是 用户访问的安全信息，安全描述符描述的是 被访问对象的安全信息

二、选择题

1、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。

2、SELinux 的 enforcing 模式中（ A）

A. 策略被完整执行；

B. 策略规则不被强制执行；

C. 内核机制完全关闭；

D. 由管理员决定

3、Android 系统中，应用程序采用沙盒隔离技术，以下说法不正确的是（D ）

A. 继承和扩展了 Linux 内核安全模型的用户与权限机制；

B. 应用沙盒隔离，只能访问自己的文件和可全局访问的资源；

C. 每个应用都有一个只有它才有读写权限的专用数据目录；

D. 权限检查可以在相同层次上执行。

4、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

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？

记录失败事件不仅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、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？

用户口令保护用户的主密钥，而主密钥保护用户的私钥，用户的公钥加密FEK。如果没有备份证书和私钥，无法恢复文件。如果备份了证书和私钥，则可以恢复文件。

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