一、填空题

1、访问控制是对主体访问客体的能力或权力的限制，它包括：**主体**、**客体**、**引用监控器**和**访问控制策略**四个要素。

2、基于所有权的访问控制分为：**自主访问控制**和**强制访问控制**。

3、访问控制的二元组描述方法通常包含**访问控制矩阵**、**访问控制表**、**访问能力表**和**授权关系表**四种形式。

二、选择题

1、访问控制是指确定（**A**）以及实施访问权限的过程。

A. 用户权限；B. 可给予哪些主体访问权利；C. 可被用户访问的资源；D. 系统是否遭受入侵

2、下列关于访问控制主体和客体的说法中，错误的是（**D**） **BD**

A.主体是一个主动的实体，它提供对客体中的对象或数据的访问要求；

B.主体可以是访问信息的用户、程序和进程；

C.客体是含有被访问信息的被动实体；

D.一个对象或数据如果是主体，则其不可能是客体

3、以下对访问控制表和访问能力表说法正确的是（**D**）

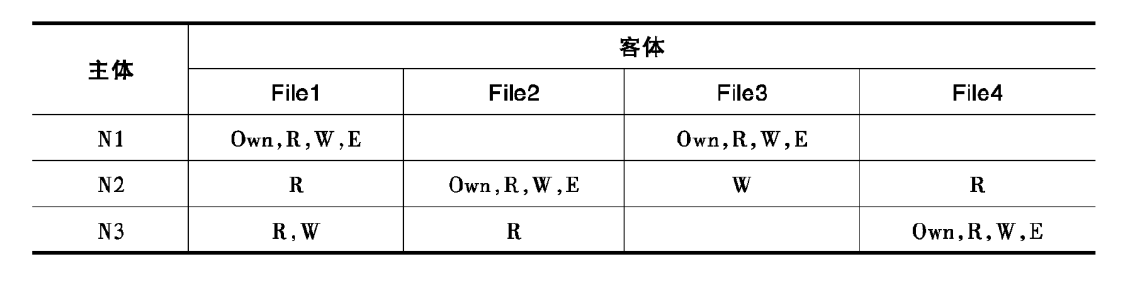
A.访问能力表表示每个客体可以被访问的主体及其权限；

B.访问控制表说明了每个主体可以访问的客体及其权限；

C.访问控制表一般随主体一起保存；

D.访问能力表更容易实现访问权限的传递，但回收访问权限较困难。

4、下图为访问控制列表。以下说法正确的是（**D**）



A.N1是管理员；B.N2是管理员；C.N3是管理员；D.都不是管理员

5、访问控制策略的制定必须体现主体、客体和访问规则集等三者之间的关系，需要遵循以下原则（**BCD**）

A.保密性原则； B. 最小特权原则； C.最小泄漏原则； D.多级安全原则

三、简答题

1、解释名词：基于角色的访问控制。

**系统操作的各种权限不是直接赋予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。一旦用户被分配了适当的角色后，该用户就拥有了此角色的所有权限，但用户不直接与权限关联。不需要每次创建用户时都进行分配权限的操作，只需要分配角色即可，可以减少系统的开销。比如说Windows系统中的Administrator、Guest和Default Account。**

2、名称解释 自主访问控制，强制访问控制。

**自主访问控制是指资源的所有者不仅拥有该资源的全部访问权限，而且能够自主的将访问权限授予其他的主体，或从授予权限的主体收回其访问权限。**

**强制访问控制，它不再让普通用户管理资源的授权，即使是资源的创建者也不行，而将资源的授权权限全部收归系统，由系统对所有资源进行统一的强制性控制，按照事先制定的规则决定主体对资源的访问权限，即使是创建者用户，在创建一个资源后，也可能无权访问该资源。**

3、访问控制策略制定遵循的基本原则是什么？举例说明。

**访问控制策略的制定必须体现主体、客体和访问规则集三者的关系，遵循的原则如下：**

1. **最小特权原则。在主体执行操作时，按照主体所需权力的最小化原则分配给主体权力。其优点是最大限度地限制了主体行为，可避免来自突发事件、操作错误和未授权主体等意外情况的危险，即为了达到一定目的，主体必须执行一定操作，但只能做被允许的操作。**

**例如：在Windows或Linux系统中在执行一些会涉及系统稳定性的操作时，如修改hosts、apt源、删除系统文件等操作，必须要提权至admin或root用户才能进行，有效避免了误操作和未授权操作对系统的损害；**

1. **最小泄漏原则。主体执行任务时，按其所需知道的最小信息分配主体权限，防止信息泄密。**

**举例说：我们在教务网站上查询成绩时，学生账户能够获取的信息只有个人的成绩和均分、最高、最低分等，而其他学生的成绩是无权查看的，各项信息也是不允许增删改的。但对于教师账户，则是具有上述权限的。学生所具有的权限已经可以满足系统的正常运转，就不需要提供更多的信息来查看；**

1. **多级安全原则。根据主体和客体之间流动的数据安全级别，将主、客体划分成5个安全等级：绝密（TS），秘密（S），机密（C），限制（RS）和无级别（U）。信息不允许从高安全级别向低安全级别流动，具有安全级别的信息资源，只有高于安全级别的主体才可访问，这样可以避免敏感信息扩散。**

**例如：Linux系统分配了多级的用户权限，root用户作为最高的安全级别，按照不同的安全级别可以配置不同的用户组，以此来管理不同访问权限的文件和应用程序。**