信息安全作业 6

190110429-何为

1. DAC 与 MAC 有什么不同?

答:

（1） 访问方式不同：DAC 通过查 ACL、ACCL 或 ACM 表来赋予用户权限允许或限制用户访问客体资源。MAC 通过定义安全类，划分安全级别和安全范畴，实现信息的单向流动。

（2） 安全防护等级不同:DAC 允许用户任意传递权限,不能为系统提供充分的数据保护。MAC 通过限制信息的单项流动和信息流安全控制，实现高防护。

（3） 授权形式不同:DAC 就需要大量繁琐的授权工作,系统管理员的工作势必非常繁重。MAC 授权形式相对简单,工作量小,但其特点不适合访问控制规则比较复杂的系统。

2. 角色与组的区别是什么?

答:

（1） 组和角色都是权限分配的单位和载体。

（2） 组（Group）是具有某些相同特质的用户集合， 可以被看成是拥有相同访问权限的用户集合。

（3） 角色（Role）是一个与特定工作活动相关联的行为与责任的集合，可以看成具有某种能力或某些属性的主体的一个抽象。

3. Windows 系统的安全体系结构包括哪些内容?

答:

（1） 层次性的安全架构：用户认证（User Authentication）、加密（Encryption）、访问控制（Access Conrad）、管理（Administration）、审计（Audit）、安全策略（Security Policy）。

（2） 安全主体：主要包括用户、组、计算机以及域等。

（3） 安全子系统：既可以用于工作站，也可以用于服务器，区别在于服务器版的用户账户数据库可以用于整个域，而工作站版的数据库只能本地使用。

（4） 访问令牌和安全描述符：它们分别由访问者和被访问者持有。通过访问令牌和安全描述符的内容，Windows 可以确定持有令牌的访问者能否访问持有安全描述符的对象。

（5） 活动目录 AD 和组策略 GP:活动目录 AD 是一个面向网络对象管理的综合目录服务。组策略可以理解为依据特定的用户或计算机的安全需求定制的安全配置规则。