### 用户认证

用户认证包括两个功能

1. 用户呈现一个凭证来识别自身以登录系统
2. 系统通过交换认证信息核实用户身份

用于身份认证的方法

|  |  |
| --- | --- |
| 个人所知道的信息 | 口令，个人标识码 对预先设置的问题的答案 |
| 个人所持有的物品 | 电子钥匙卡，智能卡，物理钥匙 |
| 静态生物特征 | 指纹识别，虹膜识别，人脸识别 |
| 动态生物特征 | 笔记特征，打字节奏 |

置信等级 ：对证书使用者的信任程度，一共有四个等级

潜在影响 ：定义了在安全性遭到破坏的情况下，个体或组织受到潜在影响的三个等级

口令攻击策略

|  |  |  |
| --- | --- | --- |
| 离线字典攻击 | 访问口令文件，匹配 | 防止非授权访问 |
| 特定账户攻击 | 不断猜测，尝试 | 设置登录次数 |
| 常用口令攻击 | 常用口令对大量用户攻击 | 禁止使用常用简单口令 |
| 单用户口令猜测 | 利用信息猜测用户口令 | 加强口令保护策略 |
| 工作站劫持 | 在已经登录的情况下入侵 | 处于非活动状态自动注销 |
| 利用用户疏漏 |  |  |
| 口令重复利用 |  |  |
| 电子监视 |  |  |

散列口令的使用

使用盐值的三个目的

1. 防止复制的口令在口令文件中可见
2. 显著提高了离线口令字典攻击的难度
3. 及时用户在不同系统上使用相同的口令，敌手也很难发现

口令文件访问控制

口令选择策略

|  |  |
| --- | --- |
| 用户教育 | 效果不明显 |
| 计算机生成口令 | 不方便记忆 |
| 后验检查口令 |  |
| 先验检查口令 |  |

3.3 基于令牌的认证

3.4 生物特征认证

3.5 远程用户认证