

# Sécurité vis à vis des intrusions



Processus de gestion de la sécurité comme processus de base du système d'exploitation.

-> Soumission de tous les objets du système d'exploitation (fichiers, répertoires, imprimantes, partages réseau, processus, canaux nommés, clés du registre, ...) à l'attribution d'ACLs (Access Control Lists) permettant de définir les "utilisateurs" pouvant y accéder et les actions qu'ils peuvent réaliser sur ces objets.



Contrôle de l'utilisation de l'ordinateur par les utilisateurs réalisé par l'administrateur.

Interdiction stricte de réalisation d'actions particulières aux personnes non autorisées pour ces actions.

EFS: Encrypted File System

Mise en œuvre d'un système d'écoute pour détecter les tentatives d'action non autorisée ou d'intrusion  
-> gestion de journaux d'événements.

Sécurité de niveau C2.