La gestion des Utilisateurs

2015

Sylvain Cherrier

Utilisateurs

Objectifs d'un système multi-utilisateurs
Garantir un accès
Sécuriser les usages
Identifier les données, pour leur bonne affectation
Protéger les données

Tout en :
Eviter les intrusions
Eviter les accès illicites
Eviter les fausses manipulations

Le tout en restant le plus rapide possible, et réactif

Stockage

- Au démarrage, dans des fichiers locaux
  - Dans /etc : passwd, group,
  - Apparition du shadow
- Puis système centralisé de gestion de comptes
  - NIS, yellow pages
  - LDAP

Consultation

- getent
- Permet d'interroger le système en offrant une abstraction de l'organisation choisie
- getent passwd, getent group

Sécurité locale

- Outils :
  - Adduser, useradd
  - Deluser, userdel
- Permet la création, modification et suppression de comptes
- Ajout dans des groupes

Concepts de base

- Un utilisateur
- Des groupes
- Les droits d'accès et d'éxécution sont évalués selon :
  - Propriétaire (user),
  - Groupe (group),
  - ou autres (other)

Concepts de base

- Un utilisateur peut appartenir à plusieurs groupes
- Chaque objet détient des droits d'accès pour un user, un groupe et les autres
- Bien qu'assez puissant, le système a des limites (exemple : utilisateurs trans-groupe)
- Notions d'ACL (listes illimitées)

Gestion déportée

- Serveur d'annuaire d'utilisateur
- NIS LDAP ActiveDirectory
- Dépendance au serveur à sécuriser (sinon, risque de serveur pirate qui valide des comptes fictifs)
- Kerberos, et autres systèmes à ticket, qui imposent leurs contraintes (horodatage)

Actions

- Si identification/authentification, alors
- Recensement de ce qui est à sécuriser
- Offrir des mecanismes correspondants
- FileSystem sécurisé
- Shell sécurisé
- Commandes sécurisées

Le contexte

- Chaque utilisateur dispose ensuite de son environnement
- Possibilité de le personnaliser. Attention, en mode multi-machine, les ressources risquent d'être différentes
  - Sous windows : Registery
  - Sous linux : Profile

Les PAM

- Très puissant outil de construction d'une chaine d'actions paramétrables pour aboutir à une autorisation ou un refus
- Exemple d'utilisation
  - Quota : disque, processeur, etc
  - Commandes
  - Mode d'accès

Centralisation

- Identification authenfication => majeur
- Mais trop de barrières créent des réactions génantes
- Authentification unique : SSO
- Tjs penser à l'utilisateur, qui peut mettre des stratégies en place

Quelques idées...

- Applicables partout :
- Essayer d'offrir l'accès le plus facile, le plus rapide aux utilisateurs légaux
- Bloquer, ralentir, perturber, tromper les sondeurs, testeurs et autres illégitimes
- Bref, simple pour nos assujettis, et complexe pour les invalides (timer)

Quelques idées

- Authentification :
  - Ce que l'on sait
  - Ce que l'on a
  - Ce que l'on est
- DICI
  - Disponibilité
  - Intégrité
  - Confidentialité
  - Imputabilité