Notions sur PAM

Qu’est-ce que c’est ?

PAM (Pluggable Authentication Modules) est un système flexible permettant de gérer les mécanismes d'authentification sous Unix/Linux. PAM offre une interface commune pour implémenter différentes méthodes d'authentification sans modifier les applications. Cela permet aux administrateurs système de personnaliser les règles d'authentification selon leurs besoins.

À quoi sert-il ?

PAM sert à gérer l'authentification des utilisateurs et les autorisations associées. Voici quelques cas d'utilisation principaux :

- Vérification des mots de passe
- Limitation des tentatives d'authentification
- Application de règles de complexité des mots de passe
- Expiration et renouvellement des mots de passe
- Gestion des comptes (activation/désactivation)
- Intégration avec LDAP ou d'autres systèmes d'authentification externes.

Quelques fichiers associés à PAM

- **/etc/pam.d/:** Répertoire contenant les fichiers de configuration pour chaque service.
- **/etc/security/** : Répertoire contenant des fichiers de configuration complémentaires.
- **/var/log/auth.log** ou /**var/log/secure** : Journaux des événements liés à l'authentification.

Quelques modules associés à PAM

- **pam_unix.so :** Module pour gérer l'authentification traditionnelle basée sur des fichiers locaux.

- **pam_tally2.so :** Module pour limiter les tentatives de connexion.

- **pam_cracklib.so :** Module pour imposer des règles de complexité des mots de passe.

- **pam_ldap.so :** Module pour l'authentification via un serveur LDAP.

- **pam_limits.so :** Module pour imposer des limites d'utilisation des ressources.

- **pam_env.so :** Module pour définir des variables d'environnement.

Quelques Commandes associées à PAM

- **pam-auth-update** : Permet de configurer PAM sous Debian/Ubuntu.

- **faillock :** Gère les tentatives de connexion échouées.

- **passwd :** Modifie les mots de passe utilisateur (interagit avec PAM).

- **chage :** Configure l'expiration des mots de passe.

Quelques Scénarios d'utilisation

1. Expiration des mots de passe :

Configurez le fichier ***/etc/pam.d/common-password*** avec le module ***pam_unix.so*** pour imposer une expiration après 90 jours et à entrer un mot de passe fort. Utilisez la commande chage -M 90 [utilisateur]. Par exemple : **password requisite pam_unix.so remember=5**

2. Limite des tentatives :

Configurez le fichier ***/etc/pam.d/common-auth*** avec le module **pam_tally2.so** pour limiter les tentatives à 5. Par exemple : **auth required pam_tally2.so deny=5 unlock_time=300**

3. Complexité des mots de passe :

Configurez le fichier ***/etc/pam.d/common-auth*** avec le module **pam_cracklib.so** pour exiger des mots de passe robustes. Par exemple :

password requisite pam_cracklib.so minlen=12 difok=3 ucredit= -1 lcredit= -1 dcredit= -1 ocredit= -1

Cela impose une longueur minimale de 12 avec *minlen,* qu'il doit y avoir au moins 3 caractères qui diffèrent de l'ancien mot de passe avec *difok,* au moins une majuscule, au moins une minuscule, au moins un chiffre et au moins un caractère spécial.

NB : la valeur -1 signifie qu'au moins une majuscule est obligatoire et si elle était positive, est définirait un nombre maximal autorisé.