pam_unix

Authentification pas mot de passe traditionnel

pam_unix.so est le module d'authentification par défaut. Il utilise les appels standard depuis les librairies système basé sur les éléments shadow suivant : **expire, last_change, max_change, min_change, warn_change**. Pour le dernier, il peut empêcher l'utilisateur de changer son mot de passe, ou attendre qu'il ai changé son mot de passe. Par défaut ce module n'autorise pas l'accès si le mot de passe n'est pas définit.

unix_chkpwd est fournit pour vérifier le mot de passe de l'utilisateur quand il est stocké dans une base protégée en lecture.

Le composant **password** de ce module effectue la mise à jour du mot de passe de l'utilisateur.

Le composant **session** de ce module log quand un utilisateur se log ou quitte le système.

OPTIONS

debug syslog les informations de debuggage

audit un peu plus extrême que debug

nullok permet l'accès à une utilisateur sans mot de passe

try_first_pass Avant de demande le mot de passe à l'utilisateur, le module essaye le mot de passe précédemment stacké.

use_first_pass Force le module à utiliser un mot de passe précédemment stacké et ne prompt jamais l'utilisateur.

nodelay Peut être utilisé pour décourager le composant d'authentification de demander un délai quand l"authentification échoue.

use_authok Le changement de mot de passe force le module à remplacer le nouveau mot de passe par celui fournit par un mot de passe précédemment stacké. C'est utilisé par exemple avec le module pam_cracklib

not_set_pass Cet argument est utilisé pour informer le module de ne pas prêter attention ou de rendre les ancien ou les nouveaux mot de passe depuis/vers d'autres module de mot de passe.

nis NIS RPC est utilisé pour définir les nouveau mot de passe

remember=n les dernier n mots de passe pour chaque utilisateurs sont sauvés dans /etc/security/passwd dans le but de forcer l'historique de changement de mot de passe et d'empêcher l'utilisateur de réutiliser les même mots de passe trop fréquemment.

shadow tente de maintenir un shadow based system

md5 crypte en md5 les nouveau mots de passe

bigcrypt crypte avec DEC C2

sha256 crypte avec SHA256

sha512 crypte avec SHA512

blowfish crypte avec blowfish

rounds=n Définit le nombre de passe des algorithmes SHA256, SHA512 et blowfish broken_shadow

ignore les erreurs en lisant les informations shadow de l'utilisateur dans le module de gestion de compte. minlen=n

Définis la longueur minimum du mot de passe. pour DES max=8

Les arguments invalides sont syslog(3). Retourne tous les types de module.

Exemples

exemple d'utilisation dans /etc/pam.d/login : authentifier l'utilisateur
auth required pam_unix.so
s'assuer que le compte etle mot de passe sont actifs
account required pam_unix.so
change le mot de passe, mais vérifie d'abord la force avec pam_cracklib
password required pam_cracklib.so retry=3 minlen=6 difok=3
password required pam_unix.so use_authok nullok md5
session required pam_unix.so