

TP : Gestion des Politiques de Mots de Passe sous Linux

Informations générales

Objectif : Configurer et appliquer une politique de sécurité des mots de passe conforme aux bonnes pratiques

Deadline : 02/02/2026 à 18h30

Contexte

Dans le cadre du renforcement de la sécurité des systèmes d'information de l'entreprise, vous êtes chargé(e) de mettre en place une politique stricte de gestion des mots de passe pour les comptes utilisateurs. Cette politique vise à réduire les risques liés aux mots de passe faibles et à leur compromission.

Objectifs du TP

Vous devez configurer le système Linux pour qu'il respecte les exigences suivantes :

1. **Changer le mot de passe** d'un compte utilisateur de test
2. **Configurer une politique de complexité** imposant :
 - Longueur minimale de 14 caractères
 - Au moins une majuscule
 - Au moins une minuscule
 - Au moins un chiffre
 - Au moins un caractère spécial
3. **Définir l'expiration du mot de passe** à 90 jours (3 mois)
4. **Forcer le changement de mot de passe** à la prochaine connexion
5. **Vérifier que toutes les configurations** sont correctement appliquées

Prérequis

- Accès root ou sudo sur votre machine Linux
- Compte utilisateur de test (nommé stagiaire_test)
- Connaissances de base en ligne de commande Linux

Travail à réaliser

Partie 1 : Préparation de l'environnement

Question 1.1 : Créez un compte utilisateur nommé stagiaire_test avec un mot de passe simple initial.

Question 1.2 : Vérifiez que le compte a bien été créé et qu'il peut se connecter.

Partie 2 : Configuration de la politique de complexité des mots de passe

Question 2.1 : Installez le module PAM nécessaire pour gérer la qualité des mots de passe.

Question 2.2 : Configurez les règles de complexité des mots de passe pour imposer :

- Longueur minimale : 14 caractères
- Au moins 1 majuscule
- Au moins 1 minuscule
- Au moins 1 chiffre
- Au moins 1 caractère spécial

Question 2.3 : Indiquez le(s) fichier(s) de configuration que vous avez modifié(s) et les lignes exactes ajoutées ou modifiées.

Partie 3 : Configuration de l'expiration du mot de passe

Question 3.1 : Configurez l'expiration du mot de passe à 90 jours pour le compte stagiaire_test.

Question 3.2 : Configurez également un avertissement 7 jours avant l'expiration du mot de passe.

Question 3.3 : Indiquez le fichier de configuration global qui permet de définir ces règles par défaut pour tous les nouveaux comptes.

Partie 4 : Forcer le changement de mot de passe à la prochaine connexion

Question 4.1 : Forcez l'utilisateur stagiaire_test à changer son mot de passe lors de sa prochaine connexion.

Question 4.2 : Changez effectivement le mot de passe de stagiaire_test en respectant toutes les règles de complexité définies.

Partie 5 : Vérification des configurations

Question 5.1 : Listez toutes les commandes permettant de vérifier :

- Les paramètres d'expiration du mot de passe de stagiaire_test

- Les règles de complexité configurées dans PAM
- Le statut du compte stagiaire_test

Question 5.2 : Exécutez ces commandes et documentez les résultats obtenus (captures d'écran ou copie des sorties).

Livrables attendus

Vous devez rendre un document contenant :

1. **Toutes les commandes utilisées** pour chaque question
2. **Les sorties des commandes de vérification** (Question 5)
3. **Les fichiers de configuration modifiés** avec les lignes concernées
4. **Une brève explication** de chaque étape réalisée

Conseils

- Pensez à tester vos configurations avant de les valider
- Documentez chaque étape au fur et à mesure
- N'hésitez pas à consulter les pages de manuel (man) des commandes

Bon courage !