**Projet de Gestion des Utilisateurs et des Permissions sur Linux**

**Objectif** : Apprendre à gérer les utilisateurs, les groupes, les permissions sudo, la création de comptes, l'expiration des mots de passe et à éditer le fichier sudoers pour donner des droits spécifiques.

**Mise en Situation**

Vous êtes administrateur système dans une entreprise de développement logiciel. Vous devez configurer un serveur Linux pour une équipe de développeurs et d'administrateurs. Voici les tâches que vous devez accomplir :

**Partie 1 : Création et Gestion des Utilisateurs**

1. **Créer des Utilisateurs** :

* Créez trois utilisateurs : **alice, bob**, et **charlie**.
* Donnez un mot de passe à chaque utilisateur.
* Configurez l'expiration des mots de passe pour qu'ils expirent tous les 30 jours pour **alice**, 60 jours pour **bob**, et 90 jours pour **charlie**.

1. **Vérifiez les Informations sur les Comptes Utilisateurs :**

* Vérifiez que les utilisateurs ont été correctement créés et que les dates d'expiration des mots de passe sont configurées comme demandé.

**Partie 2 : Gestion des Groupes**

1. **Créer des Groupes :**

* Créez deux groupes : **dev** et **admin**.
* Ajoutez **alice** et **bob** au groupe **dev**, et **charlie** au groupe **admin**.

1. **Vérifiez l'Appartenance aux Groupes :**

* Vérifiez que les utilisateurs appartiennent aux groupes appropriés.

**Partie 3 : Permissions Sudo**

1. **Configurer les Permissions Sudo pour un Utilisateur :**

* Ajoutez **alice** au groupe **sudo** pour lui donner les permissions sudo.

1. **Édition du Fichier sudoers :**

* Utilisez **visudo** pour éditer le fichier sudoers.
* Donnez à **bob** la permission d'exécuter uniquement les commandes **apt update** et **apt upgrade** sans mot de passe.
* Donnez à **charlie** la permission d'exécuter toutes les commandes avec mot de passe.

**Partie 4 : Vérification et Connexion**

1. **Vérifiez les Permissions Sudo :**

* Connectez-vous en tant que **alice** et vérifiez que vous pouvez utiliser **sudo** pour exécuter des commandes.
* Connectez-vous en tant que **bob** et essayez d'exécuter **apt update** sans mot de passe.
* Connectez-vous en tant que **charlie** et essayez d'exécuter **ls /root**. Vous devriez être invité à entrer le mot de passe.

Partie 5 : Configuration Avancée

1. **Paramétrer des Règles d'Expiration de Mot de Passe Complexes :**

* Configurez des règles d'expiration de mot de passe pour **alice** pour qu'elle soit avertie 7 jours avant l'expiration.

1. **Configurer des Permissions Spécifiques pour des Groupes :**

* Éditez le fichier sudoers pour permettre à tous les membres du groupe **dev** d'exécuter les commandes /**usr/bin/systemctl restart apache2** sans mot de passe.

**Détails des Tâches à Réaliser**

**Création des Utilisateurs :**

1. Créez les utilisateurs avec un mot de passe initial.

* Utilisez la commande **adduser** pour créer chaque utilisateur.
* Utilisez la commande **passwd** pour définir les mots de passe.

1. Configurez l'expiration des mots de passe.

* Utilisez la commande **chage** pour définir les périodes d'expiration des mots de passe.

Gestion des Groupes :

1. Créez les groupes et ajoutez-y les utilisateurs.

* Utilisez les commandes **groupadd** et **usermod** pour gérer les groupes.

1. Vérifiez l'appartenance aux groupes.

* Utilisez la commande **groups** ou pour vérifier les groupes d'appartenance des utilisateurs.

Permissions Sudo :

1. Configurez les permissions sudo pour **alice**.

* Ajoutez **alice** au groupe **sudo** en utilisant la commande **usermod**.

1. Éditez le fichier sudoers pour **bob** et **charlie**.

* Utilisez **visudo** pour ouvrir et éditer le fichier sudoers.

Vérification et Connexion :

1. Connectez-vous en tant que chaque utilisateur et testez les permissions.

* Utilisez **su - <nom\_utilisateur>** pour changer d'utilisateur.
* Testez les commandes appropriées pour vérifier les permissions sudo.

Configuration Avancée :

1. Configurez des notifications d'expiration de mot de passe pour alice.

* Utilisez la commande chage avec l'option -W pour définir les avertissements.

1. Modifiez le fichier sudoers pour ajouter des permissions spécifiques au groupe dev.

* Utilisez visudo pour ouvrir et éditer le fichier sudoers.

Conseils et Commandes Utiles

* Créer un utilisateur : sudo adduser <nom\_utilisateur>
* Définir un mot de passe : sudo passwd <nom\_utilisateur>
* Configurer l'expiration des mots de passe : sudo chage -M <jours> <nom\_utilisateur>
* Créer un groupe : sudo groupadd <nom\_groupe>
* Ajouter un utilisateur à un groupe : sudo usermod -aG <nom\_groupe> <nom\_utilisateur>
* Vérifier les groupes d'appartenance : groups <nom\_utilisateur> ou id <nom\_utilisateur>
* Ouvrir le fichier sudoers pour édition : sudo visudo

Résultats Attendus

* Les utilisateurs alice, bob, et charlie sont créés avec les mots de passe et les paramètres d'expiration spécifiés.
* Les groupes dev et admin sont créés, et les utilisateurs sont ajoutés aux groupes appropriés.
* alice peut utiliser sudo pour exécuter des commandes.
* bob peut exécuter apt update et apt upgrade sans mot de passe.
* charlie peut exécuter toutes les commandes avec un mot de passe.
* Les permissions spécifiques pour le groupe dev sont configurées dans le fichier sudoers.