Scénario : Mise en place des bonnes pratiques de sécurité des utilisateurs sur Linux

1. Création des utilisateurs et gestion des groupes

1. **Création des utilisateurs :**
   - Créez deux utilisateurs standards, `utilisateur1` et `utilisateur2`.

```
sudo adduser utilisateur1
sudo adduser utilisateur2
```

2. **Création de groupes :**
   - Créez un groupe `admins` pour les utilisateurs ayant des privilèges administratifs.

```
sudo addgroup admins
```

   - Ajoutez `utilisateur1` au groupe `admins`.

```
sudo usermod -aG admins utilisateur1
```

2. Rotation des mots de passe

1. **Configuration de la rotation automatique :**
   - Installez `passwdqc` pour une politique de gestion avancée des mots de passe.

```
sudo apt-get install passwdqc
```

   - Configurez `/etc/login.defs` pour définir une politique de rotation des mots de passe.

```
PASS_MAX_DAYS   90
PASS_MIN_DAYS   7
PASS_WARN_AGE   7
```

   - Activez la rotation automatique des mots de passe avec `chage`.

```
sudo chage -M 90 utilisateur1
```

3. Application des droits minimaux et évolution

1. **Utilisation de sudo pour les privilèges administratifs :**
   - Éditez `/etc/sudoers` avec `visudo` pour accorder des privilèges à `admins`.

     ```
     sudo visudo
     ```

     Ajoutez la ligne suivante pour permettre à `admins` d'exécuter toutes les commandes avec sudo :

     ```
     %admins   ALL=(ALL:ALL) ALL
     ```

2. **Évolution des privilèges :**
   - Pour accorder des privilèges spécifiques à `utilisateur2`, ajoutez des règles sudo appropriées.

     ```
     sudo visudo
     ```

     ```
     utilisateur2   ALL=(ALL) /bin/echo
     ```

     Cela permet à `utilisateur2` d'utiliser `sudo` uniquement pour exécuter la commande `/bin/echo`.

4. Sécurisation du compte root

1. **Restriction de l'accès root :**
   - Désactivez l'accès direct via SSH pour root en éditant `/etc/ssh/sshd_config`.

     ```
     PermitRootLogin no
     ```

   - Redémarrez le service SSH pour appliquer les modifications.

     ```
     sudo systemctl restart sshd
     ```

2. **Journalisation et surveillance :**

- Vérifiez que la journalisation est activée pour surveiller les activités du compte root.

```
sudo grep 'sudo' /var/log/auth.log
```

3. **Gestion des clés SSH :**
   - Utilisez des clés SSH pour l'authentification au lieu de mots de passe pour sécuriser l'accès root.

```
sudo ssh-keygen -t rsa
sudo ssh-copy-id -i ~/.ssh/id_rsa.pub root@your_server_ip
```

     Cela permet une connexion sécurisée sans mot de passe au compte root.

Conclusion

En suivant ce scénario, vous avez mis en place plusieurs bonnes pratiques de sécurité des utilisateurs sur un système Linux :

- Création et gestion des utilisateurs et des groupes.
- Rotation automatique des mots de passe.
- Application des droits minimaux avec sudo.
- Sécurisation du compte root avec la désactivation de l'accès direct via SSH et l'utilisation de clés SSH.
- Surveillance et journalisation des activités.

Ces pratiques contribuent à renforcer la sécurité du système en limitant les accès et en assurant une gestion sécurisée des comptes et des privilèges.