
Travaux Pratique N ° 4

TP sur les Droits d'accès sous Linux

1 Objectif du TP

L'objectif de ce TP est de vous familiariser avec les droits d'accès aux fichiers et répertoires sous Linux, y compris les concepts avancés liés aux bits SUID, GUID et sticky. Vous allez explorer les commandes liées à la gestion des permissions et des droits d'accès.

2 Tâches

2.1 Tâche 1 : Exploration des droits d'accès

Exécutez la commande `ls -l` dans votre répertoire personnel pour afficher les droits d'accès de vos fichiers et répertoires. Identifiez les différentes colonnes de la sortie et expliquez ce que chacune signifie.

2.2 Tâche 2 : Création de fichiers et de répertoires

- Créez un répertoire nommé "TP_Droits" dans votre répertoire personnel.
- Créez un fichier vide nommé "monfichier.txt" à l'intérieur de "TP_Droits".
- Affichez les droits d'accès du répertoire "TP_Droits" et du fichier "monfichier.txt" en utilisant `ls -l`.

2.3 Tâche 3 : Modification des droits d'accès

Modifiez les droits d'accès du fichier "monfichier.txt" de telle sorte que le propriétaire puisse le lire, écrire et exécuter, le groupe puisse le lire, et les autres utilisateurs ne puissent rien faire. Affichez les nouveaux droits d'accès du fichier.

2.4 Tâche 4 : Utilisation de chmod

Utilisez la commande `chmod` pour donner au propriétaire du fichier "monfichier.txt" uniquement les droits de lecture et d'écriture.

1. Vérifiez les droits d'accès modifiés.
2. Ensuite, utilisez `chmod` pour définir le bit SUID sur "monfichier.txt".
3. Expliquez ce que fait le bit SUID et comment il affecte le fichier.

2.5 Tâche 5 : Changement de propriétaire et de groupe

1. Créez un nouvel utilisateur "utilisateur2" en utilisant la commande `adduser`.
2. Changez le propriétaire du fichier "monfichier.txt" pour qu'il soit "utilisateur2".
3. Changez le groupe du fichier en "utilisateur2" également.
4. Affichez les propriétaires et groupes actuels du fichier.

2.6 Tâche 6 : Permissions avancées

1. Créez un répertoire nommé "secu" à l'intérieur de "TP_Droits".
2. Modifiez les droits d'accès de "secu" de manière à ce que le propriétaire puisse tout faire, le groupe puisse lire et exécuter, et les autres utilisateurs ne puissent rien faire.
3. Ensuite, utilisez `chmod` pour définir le bit G UID sur "secu".
4. Expliquez ce que fait le bit G UID et comment il affecte le répertoire.

2.7 Tâche 7 : Exploration des répertoires

1. Utilisez la commande `cd` pour naviguer dans le répertoire "TP_Droits".
2. Essayez de lister le contenu du répertoire "secu".
3. Expliquez pourquoi vous avez ou n'avez pas pu accéder au répertoire.

2.8 Tâche 8 : Bits Sticky

1. Créez un répertoire nommé "partage" à l'intérieur de "TP_Droits".
2. Modifiez les droits d'accès de "partage" de manière à ce que le propriétaire puisse tout faire, le groupe puisse tout faire, et les autres utilisateurs ne puissent rien faire.
3. Ensuite, utilisez `chmod` pour définir le bit sticky sur "partage".
4. Expliquez ce que fait le bit sticky et comment il affecte le répertoire.

3 Conclusion

Ce TP a permis de comprendre les droits d'accès aux fichiers et répertoires sous Linux, y compris les concepts avancés liés aux bits SUID, G UID et sticky. Vous avez appris à gérer les permissions avancées et à sécuriser l'accès à vos fichiers et répertoires.