
TP N°4 : Les droits d'accès

Objectifs :	1. Exercer les commandes de manipulation des groupes 2. Mettre en place un contrôle d'accès cohérent sur les ressources système.
Volume horaire :	6 heures (2 séances) : Séance 1 : Partie théorique, exercice 1, Exercice 2, 3 Séance 2 : Exercice 3, Exercice 4, Exercice 5

II. Partie théorique

Répondre aux questions suivantes.

1. Qu'est-ce qu'un droit d'exécution pour un répertoire ?
2. Qu'est-ce qu'un umask ?
3. Quel est le rôle du stickybit ?
4. Qu'est-ce qu'un SUID ?
5. Qu'est-ce qu'un SGUID ?
6. Comment peut-on donner le droit d'exécution d'une commande réservée au root à un utilisateur quelconque ?

II. Manipulations pratiques

Gestion des utilisateurs et des groupes

Chowner, chgrp, newgrp,

Exercice 1

1. Connectez vous sur la console virtuelle tty1
2. Créez un nouveau trois utilisateurs nommés respectivement Iset_tp4, userx et usery.
3. Connectez vous sur la console virtuelle tty2 avec l'utilisateur Iset_tp4.
4. Changez les champs commentés de l'utilisateur Iset_tp4 pour le rendre étudiant_tp6.
5. Visualisez la ligne correspondante à la liste des informations relatives à cet utilisateur dans le fichier approprié.
6. Créez un groupe nommé gr_inf3.
7. modifiez le groupe de Iset_tp4 en gr_inf3.
8. Créez un nouveau groupe nommé groupe_inf3_m1 ayant comme identifiant 2010.

9. Visualisez la ligne correspondante à la liste des informations relatives à ce groupe dans le fichier approprié.
10. Créez un fichier (fichier6) et faire l'appartenir à ce nouveau groupe.
11. Créez un répertoire (rep6).
12. Faire appartenir ce répertoire au groupe Iset_tp4 (dont vous êtes membre)
13. Changez le propriétaire de ce répertoire pour devenir l'utilisateur userx (que vous créez s'il n'existe pas).

Droits d'accès par défaut :

Exercice 2

Déterminer les droits d'accès minimum pour :

- Créer un fichier,
 - Copier un fichier,
 - Renommer un fichier,
 - Lier un fichier,
 - Lister le contenu d'un fichier,
 - Créer un répertoire.
1. Quelle est la commande qui permet de fixer les droits d'accès d'un nouveau fichier aux droits rw- rw- --- ? Que seront les droits d'accès pour un nouveau répertoire ?
 2. Quelle est la commande qui permet de fixer les droits d'accès d'un nouveau répertoire aux droits rwx rwx r-x ? Que seront les droits d'accès pour un nouveau fichier ?

Droits d'accès sur les fichiers et répertoires :

Exercice 3

Déterminer les droits d'accès aux fichiers spéciaux suivants :

/dev/hda*
/dev/tty*
/dev/lp*
/dev/mouse*

1. Quels sont les droits sur les répertoires personnels des utilisateurs (par exemple le répertoire /home/userx relatif à l'utilisateur userx) ? userx peut-il renommer son répertoire personnel ?
2. Un utilisateur différent usery peut-il y pénétrer ou seulement lister les fichiers de userx ? et l'utilisateur totox, le pourrait-il s'il faisait partie du groupe de userx ?

3. Quelles commandes devrait écrire `userx` pour accorder le droit de visite de son répertoire personnel seulement à `totox` ?
4. Comparer les permissions de `/etc/passwd` et `/etc/shadow`. Pourquoi a-t-on nommé ainsi ce dernier fichier ? `userx` peut-il le lire ? Examiner ce fichier pour deviner son rôle.
5. Par précaution, en faire une copie sous le nom `shadow.bak` dans `/home/tmp`. Vérifier les droits de `/home/tmp/shadow.bak`
6. Pensez-vous tout de même pouvoir supprimer le fichier précédent ? Concluez !
7. `root` fait maintenant une copie de `shadow` chez vous, dans `/home/userx`, sous le nom `shadow.bak` et vous accorde la propriété de la copie. Comment fait-il ?
8. Vous éditez ce fichier avec `vi`, vous le modifiez, par exemple en supprimant des lignes, et vous faites une mise à jour. La mise à jour sera-t-elle réalisée ? pourquoi ?
9. Pensez vous que `userx` puisse supprimer ce fichier ? Essayez et expliquez !
10. En tant que `userx`, pouvez vous créer le rép. temporaire `/home/tmp` ? Commentez.
11. Effectuez cette création comme `root` (commande `su`).
12. Accorder les permissions maximales sur `/home/tmp`; vérifiez.
13. Après avoir eu le droit d'écriture dans `/home/tmp`, `totox` tente de copier les 2 fichiers système `/etc/hosts` et `/etc/passwd` dans `/home/tmp` ? y parviendra-t-il ? pourquoi ?
14. `totox`, essaie maintenant de supprimer ces 2 fichiers de `/etc`. Réussit-il ?

15. Créez dans votre répertoire de connexion, 2 répertoires nommés respectivement `r_tp6_1` et `r_tp6_2` ainsi que sept fichiers nommés resp. `f_1`, `f_2`, `f_3`, `f_4`, `f_5`, `f_6`, `f_7`.
16. Placez les 3 premiers fichiers dans le 1er répertoire et les 3 fichiers suivants dans le 2ème répertoire.
17. Attribuez les droits d'accès aux fichiers et répertoires comme suit (avec une méthode non numérique) :
 1. `r_tp6_1 = 640 = 110 100 000 : chmod u=rw,g=r,o= r_tp6_1`
 2. `r_tp6_2 = 530`
 3. `f_1 = 644`
 4. `f_2 = 640`
 5. `f_3 = 544`
 6. `f_4 = 740`
 7. `f_5 = 644`
 8. `f_6 = 430`
 9. `f_7 = 664`
18. Peut-t-on placer le fichier 7 dans le répertoire `r_tp6_2` ? sinon pourquoi et comment faire pour pouvoir le déplacé.

Exercice 4

Il s'agit de créer un répertoire partagé par tous les membres `userx` du groupe `etudiant`.

Normalement, ce groupe a déjà été créé et rempli de comptes `userx`.

1. Créez dans `/home` un répertoire appelé `rep-etudiant`. Rappelez pourquoi cette tâche relève des prérogatives de `root`
2. Faites-le appartenir au groupe `etudiant`
3. Modifier les permissions sur le répertoire, pour que tous les membres du groupe `etudiant` puissent y écrire et s'y déplacer.
4. En tant que `userx`, vous créez un fichier, par exemple un petit fichier texte (à l'aide de `vi` ou d'un éditeur graphique comme `kedit`) et vous le déposez dans `/home/rep-etudiant`. Si vous êtes paresseux, vous y faites une copie d'un fichier `qcq`, par exemple `/etc/hosts`, mais en attribuant des droits `660`
5. `[userx@p0x etc] cp hosts /home/rep-etudiant`
6. `[userx@p0x etc] chmod 660 hosts`

7. Vérifier le bon accès en lecture seulement pour les membres du groupe. Ainsi totox qui a fini par être exclu du groupe étudiant (surtout après l'exercice 3) ne doit pas pouvoir le lire. A vérifier.
8. Votre collègue le perfide usery (y#x), tente de supprimer ce fichier ou de le renommer. Y parvient-il ? Essayez !
Pourtant, vérifiez que ce fichier appartient au groupe userx. N'est-ce pas inquiétant ? Expliquez comment cela est possible.
9. Demandez à root de positionner le "sticky bit" sur le répertoire partagé. Vérifiez bien que le problème est réglé et protège le propriétaire des tentatives de suppression ou de changement de nom de ses fichiers.

Exercice 5 :

3. Essayer de supprimer ou de modifier le fichier /etc/passwd. Que se passe-t-il ? Expliquer la situation à l'aide de la commande ls -l
4. A l'aide de la commande id, vérifier votre identité et le(s) groupe(s) auquel vous appartenez.
5. Créer un petit fichier texte (de contenu quelconque), qui soit lisible par tout le monde, mais pas modifiable (même pas par vous).
6. Créer un répertoire nommé secret, dont le contenu soit visible uniquement par vous même. Les fichiers placés dans ce répertoire sont-ils lisibles par d'autres membres de votre groupe ?
7. Créer un répertoire nommé iset tel que les autres utilisateurs ne puissent pas lister son contenu mais puissent lire les fichiers qui y sont placés. On obtiendra

```
$ ls iset
ls : iset: Permission denied
$ cat iset/toto
<...le contenu du fichier toto (s'il existe)...>
```

8. Chercher dans le répertoire /usr/bin trois exemples de commandes ayant la permission SUID. De quelle genre de commande s'agit-il ?
 9. Un administrateur désire s'assurer chaque matin que tous les fichiers placés sous /home/users/cours sont lisibles par tout le monde, mais non modifiables excepté par leur propriétaire.
 10. Quel doit être le mode de ces fichiers et répertoires ?
- Rédigez un compte rendu décrivant ce que vous avez fait.**