TP Administration : Gestion utilisateurs

TP Administration

Travail demandé

> Cette activité doit être réalisée entièrement en ligne de commande (mode CLI).

La sécurité du système

Question 1. Ajoutez un groupe "mesusers" et "dev".

Question 2. Ajoutez au groupe "mesusers" deux utilisateurs "user1" et "user2" et fixez deux mots de passe différents pour ces utilisateurs. L'utilisateur "user1" doit avoir par défaut le shell *bash* et l'utilisateur "user2" le shell *csh*.

Question 3. Des mots de passe identiques donnent-ils les mêmes résultats cryptés ?

Question 4. Essayez d'ouvrir une session avec chacun de ces utilisateurs.

Question 5. Ajoutez l'utilisateur "user2" au groupe "sudo". Quelle conséquence cela aura-t-il ?

Question 6. Bloquez le compte de l'utilisateur "user2". Testez. Qu'est ce qui a changé dans le fichier `/etc/shadow` ?

Question 7. Forcez l'utilisateur "user1" à changer son mot de passe à la prochaine ouverture de session.

Question 8. Supprimez l'utilisateur "user2" et son espace personnel.

Question 9. Connectez-vous en temps que "root" (vous devez lui donner un mot de passe avant avec la commande `sudo passwd root`). A l'aide de la commande `id`, listez tous les groupes auxquels appartient le super utilisateur.

Question 10. Connectez-vous en temps que "user1" et endossez l'identité de "root" à l'aide de la commande `su`.

Question 11. Utilisez les commandes `id`, `whoami` et `who am i`. Que constatez-vous ?

Question 12. Connectez-vous par *ssh* en tant que "user1" et afficher l'historique des connexions.

Les fichiers d'initialisation

Question 13. Modifiez les fichiers d'initialisation de l'utilisateur "user1" : le fichier d'initialisation de login doit afficher le message "login" et celui de lancement doit afficher le message "lancement". Effectuez plusieurs connexions puis en exécutez un *shell* manuellement. Que constatez-vous ?

Question 14. Effectuez ces modifications dans les fichiers correspondants dans `/etc/skel`. Créez un utilisateur "user3" (dans le même groupe que les deux autres), puis connectez-vous avec cet utilisateur pour valider votre modification.

Les permissions étendues

Question 15. Endossez l'identité du super utilisateur et vérifiez la valeur de `umask`.

Question 16. Trouvez à quel endroit cette valeur par défaut est définie.

Question 17. Créez un répertoire `/home/public` dans lequel tous les utilisateurs pourront créer des fichiers mais ne pourront pas effacer les fichiers des autres. Testez avec les utilisateurs "user1" et "user3".

Question 18. Attribuez le répertoire `/home/public` au groupe "dev". Que faut-il faire pour que les dossiers créés dans `/home/public` par les utilisateurs "user1" et "user3" appartiennent automatiquement aussi au groupe "dev" ? Testez.

Question 19. Quelles seraient les conséquences si la commande `/bin/cat` possédait le bit SETUID ?

Question 20. Installez le paquet *acl*, créez un répertoire nommé `/home/projet` puis modifiez les droits pour que seuls aient l'accès :

— L'utilisateur "user1" en lecture et écriture
— L'utilisateur "user3" en lecture seule