LAB4 : ACL et droits étendus

Exercice 1 :

1. Créez un utilisateur student avec le mot de passe tekup et un nouveau groupe appelé **database** qui a le GID **50000.**
2. Créez un nouvel utilisateur appelé **dbuser1** qui utilise **database** comme groupe secondaire.
    - Le mot de passe initial de **dbuser1** doit être « **redhat** ».
    - Configurer l'utilisateur **dbuser1** pour forcer un changement de mot de passe lors de sa première connexion.
    - L'utilisateur dbuser1 doit pouvoir changer son mot de passe 10 jours après le jour du changement de mot de passe.
    - Le mot de passe de dbuser1 devrait expirer dans 30 jours depuis le dernier jour du changement de mot de passe.
3. Configurez l'utilisateur **dbuser1** pour qu'il utilise **sudo** pour exécuter n'importe quelle commande en tant que superutilisateur.
4. Configurez l'utilisateur dbuser1 pour avoir un **umask** par défaut de **007**.
5. En tant que root, créer un répertoire **/home/student/grading/review2.**
   Le propriétaire de ce répertoire est student et le groupe propriétaire est database.

Les fichiers créés dans le répertoire **/home/student/grading/review2** doivent appartenir au groupe database.

Les permissions sur **/home/student/grading/review2** devraient autoriser les membres de groupe **database** ainsi que l'utilisateur **student** pour accéder au répertoire et créer du contenu dedans.

Tous les autres utilisateurs doivent avoir des autorisations de lecture et d'exécution sur le répertoire.

Également, assurez-vous que les utilisateurs ne sont autorisés à supprimer que les fichiers dont ils sont propriétaires de **/home/student/classement /review2** et non des fichiers appartenant à d'autres.

Exercice 2 :

En tant que root :

1. Créer trois nouveaux utilisateurs **contractor1**, **contractor2**, et **contractor3** qui sont membres de groupe **contractors.**
2. Créer deux utilisateurs manager1 et manager2 qui sont membres du groupe managers.
3. Les cinq utilisateurs ont redhat comme mot de passe.
4. Créer un repertoire **/shares/cases** contenant deux fichiers shortlist.txt and backlog.txt
5. Le répertoire **/shares/cases** et son contenu doivent appartenir au groupe **managers.** Le propriétaire et le groupe propriétaire doivent avoir la permission de lecture et écriture. Les autres utilisateurs n'auront aucune permission.

6. Ajoutez des entrées ACL au répertoire **/shares/cases** (et à son contenu) qui permettent aux membres du groupe **contractors** pour avoir un accès en lecture, écriture et exécution. L'utilisateur cotractor3 aura uniquement des permissions de lecture.
7. Ajoutez des entrées ACL qui garantissent que tous les nouveaux fichiers ou répertoires du répertoire /**shares/cases** ont les autorisations de lecture uniquement ceci pour le groupe **contractors.**

Exercice 3

En tant que root :

1. Créer deux utilisateurs **student1** et **student2** avec le mot de passe tekup.

   Student1 doit créer les fichiers fich1, fich2 et fich3 dans son répertoire personnel. Student2 crée les fichiers fichier1 et fichier2 dans son répertoire personnel.

   Le groupe propriétaire de **fich3** est **tekup**.
2. Les deux utilisateurs student1 et student2 appartiennent au groupe **student**.
3. Utilisez les options -user, -group, -perm avec la commande find pour localiser tous les fichiers qui ont l'utilisateur **student1**, le groupe propriétaire **student1** et les autorisations 664. Rediriger toutes les erreurs de la commande find vers /dev/null.
4. Recherchez tous les fichiers pour lesquels le droit SUID est positionné et écrivez le résultat dans le fichier **suid.**