Lab3

Exercice 1 :

1- Créez un groupe**redhat** et trois utilisateurs **user1**, **user2** et **user3** ayant chacun le mot de passe « **aberate** ». **user1** et **user3** ont **redhat** comme groupe primaire ; **user3** garde son groupe par défaut et **redhat** comme groupe secondaire. Le compte de **user3** est inactif.

2- Créez un répertoire partagé**/home/tekup** avec **root** comme propriétaire et **redhat** comme groupe. Faire en sorte que les membres du groupe **redhat** aient le droit de lecture et écriture et aucun droit pour les autres et les utilisateurs **user1** et **user2** peuvent y accéder seulement.

Les fichiers créés dans le répertoire **/home/tekup** doivent appartenir au groupe **redhat**.

3- Faites en sorte que le compte de **user1**demande un changement de mot de passe à la prochaine connexion.

4- Copier le fichier **/etc/passwd** sous le répertoire /**tmp**. Définissez une règle pour que **user2** puisse le lire et y écrire alors que **user1** n'a aucun droit, le groupe **redhat** peut l'exécuter et le lire.

5- Créer un utilisateur **user4** avec un uid**1234, un groupe primaire redhat, un compte inactif** et mot de passe « **aberate** ».

Exercice 2 : Droit SUID

Le Set User ID concerne uniquement les programmes. Le droit SUID permet d'exécuter un programme avec les autorisations de celui qui possède le fichier plutôt qu'avec les permissions de l'utilisateur qui exécute le programme.

21. Vérifiez qu'un utilisateur simple n'a pas le droit d'écrire dans le fichier /etc/shadow. Dans ce cas, seulement le root peut créer et modifier les comptes utilisateurs.
22. Pouvez-vous modifier le mot de passe de votre compte utilisateur avec la commande passwd? Expliquez le résultat en vérifiant les droits d'accès du fichier /usr/bin/passwd.
23. Ajoutez le bit SUID au fichier /usr/bin/yum et reprendre la question précédente. Expliquez.

```
$ chmod u+s /usr/bin/yum
```

Exercice 3 : Droit SGID

Le set Groupe ID concerne à la fois les programmes et les répertoires. Un programme lancé avec le droit SGID sera exécuté avec les droits du groupe du programme et non pas les droits du groupe de

l'utilisateur qui l'a lancé. Lorsqu'un fichier est créé dans un répertoire portant le droit SGID, ce fichier se verra attribuer par défaut le groupe du répertoire. De plus, si un autre répertoire est créé dans le répertoire portant le droit SGID, ce sous-répertoire portera également ce droit.

24. Passez sous le compte root et créer un répertoire nommé test avec les droits d'accès 777.
25. Ajoutez le bit (SGID) au répertoire test.

    $ chmod 2777 test

26. Avec votre compte utilisateur, essayez de créer un fichier file.txt dans le répertoire test. Déterminez les droits associés à ce fichier. Que constatez-vous ?

Exercice 4 : Droit Sticky Bit

Le droit "sticky bit" concerne surtout les répertoires. Lorsque ce droit est positionné sur un répertoire, il interdit la suppression d'un fichier qu'il contient à tout utilisateur autre que le propriétaire du fichier et le root. Néanmoins, il est toujours possible pour un utilisateur possédant les droits d'écriture sur ce fichier de le modifier (par exemple de le transformer en un fichier vide). Ceci est utile pour les répertoires publiquement accessibles comme /tmp.

27. Avec votre compte utilisateur, créez un fichier protect.txt sous le répertoire /tmp avec les droits d'accès 777.
28. En utilisant un autre compte utilisateur, pouvez-vous supprimer ce fichier?
29. En utilisant le compte root, pouvez-vous supprimer ce fichier?