TP1 : fichiers setuid / setgid

Dans le système linux, chaque fichier/dossier possède des indicateurs de droits d'accès en fonction du propriétaire, du groupe propriétaire et des autres. Il existe en plus de ces indicateurs des droits « setuid » et « setgid » qui permettent de lancer un fichier exécutable en tant qu'un utilisateur différent. Par exemple un utilisateur standard peut exécuter un script en tant que root.

Cette fonctionnalité parfois nécessaire peut engendrer des problèmes de sécurité. C'est pourquoi il peut être utile de surveiller l'existence des ces fichiers..

Ecrire un script BASH qui permet la recherche et la vérification des fichiers possédant les propriétés setuid et setgid.

Ce script prend en paramètre deux options de fonctionnement :

- SEARCH : recherche dans tout l'arborescence du disque les fichiers setuid et setgid et crée deux fichiers contenant la liste des fichiers trouvés associés à leur md5.

- CHECK : compare les fichiers setuid et setgid du disque à ceux des deux listes. Un message d'alerte sera envoyé par mail à l'utilisateur « root » dans le cas où les listes ou les md5 seraient différents.

Les fichiers générés par l'option SEARCH sont des fichiers textes respectant le format :

```
91fc57ea49b0d37a92dfbd6d1745c2bd  /bin/fusermount
84c20fe7d9a92a9b69bfd7b8e84dd0f0  /bin/su
.
.
```

Une association « MD5<=>fichier » par ligne.

Cette option doit également générer un fichier de contrôle contenant les md5 des deux fichiers précédents.

L'option CHECK doit générer un mail spécifique pour chaque anomalie (md5 modifié, fichier supplémentaire détecté...) en indiquant le fichier et le md5 concernés.

Donnez la configuration de la tâche CRON permettant un « CHECK » toutes les nuits à 1h30.

La recherche des fichiers pourra se faire avec la commande « find » et le calcul du md5 avec la commande « md5sum ».