TP2:BONNES PRATIQUES DE LA SECURITE DU SYSTEME D'EXPLOITATION

TRAVAIL A FAIRE

1. Indiquer la raison derrière chacun des points de durcissement suivants :
   a. Utiliser des dépôts signés
   b. Enlever les systèmes de fichiers non utilisés
   c. S'assurer qu'il n'y a pas d'UID dupliqué
   d. Limiter l'utilisation et l'accès aux fichiers de vidage mémoire (core dump)
   e. S'assurer que la variable PATH de l'utilisateur root ne contient pas le répertoire de travail courant (.) ou tout autre répertoire inscriptible par tous.

Sur votre distribution Linux déjà installée :

2. Donnez un exemple concret du principe de minimisation, du moindre privilège, de défense en profondeur et d'activité de veille et maintenance.
3. Lister l'ensemble des packages installés. Est-ce que tous ces packages vous sont utiles ?
4. Vérifier si /tmp est configuré dans sa propre partition ou avec son propre système de fichier (tmpfs).
   Dans le cas contraire, qu'est-ce qu'il faut faire pour remédier à ce problème.
   Quel est le principe de sécurité appliqué dans ce cas.
5. Vérifier que le ***sticky bit*** est activé sur tous les répertoires inscriptibles par tous. Quel est le principe de sécurité appliqué dans ce cas.
6. Ecrire une commande bash qui permet de chercher tous les ***binaires suid*** dans votre système. Est-ce dangereux de les avoir ?
7. Expliquer comment durcir quelques paramètres du noyau (sysctl -a).
8. Vous voulez renforcer la politique de mots de passe sur votre serveur Linux.
   a. Comment imposer une durée de vie aux mots de passe pour les utilisateurs ?
   b. Imposer l'utilisation des mots de passe complexes avec le module PAM, en s'appuyant sur les recommandations ANSSI.