

---

## TP4 : SECURITE LINUX

---

### EXERCICE 1 : NOTIONS GENERALES

---

1. Indiquer la raison derrière chacun des points de durcissement suivants :
  - a. Utiliser des dépôts signés
  - b. Limiter l'utilisation et l'accès aux fichiers de vidage mémoire (core dump)
  - c. 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. Donner des exemples des packages qui ne vous sont pas utiles.
4. Vérifier si le répertoire /tmp est configuré dans sa propre partition ou avec son propre système de fichier (tmpfs). Dans le cas contraire, attribuer tmpfs à la partition /tmp. 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. Vérifier que les dépôts des packages sont signés. Quel est le principe de sécurité appliqué dans ce cas.

### EXERCICE 2 : AUDIT ET DURCISSEMENT

---

Votre entreprise vous a confié la mission de préparer la plateforme d'hébergement de son site web. Le choix a été porté sur Apache comme serveur web et Debian comme système d'exploitation. Cette plateforme doit être durcie afin de protéger l'entreprise contre les éventuelles attaques.

1. Chercher sur Internet des référentiels de durcissement des systèmes d'exploitation et de serveur HTTP.
2. Installer le serveur Apache sur votre distribution Debian.
3. Chercher et installer un script d'audit de sécurité sur votre système.
4. Exécuter ce script d'audit pour mesurer le niveau de sécurité de votre plateforme d'hébergement.  
Lire son rapport détaillé, et noter les points à améliorer.
5. Faites les améliorations nécessaires en se basant sur le rapport du script, puis réexécuter le script et constater l'amélioration du score.
6. Refaire les questions 4 et 5 jusqu'à l'obtention d'un résultat satisfaisant.