SELINUX: Les domaines

Le domaine unconfined_t

Définition

Dans **SELinux**, les domaines non restreints sont autorisés à faire presque tout (d'où le nom, non restreint).

- les domaines non confinés s'exécutent virtuellement sans protection **SELinux**
- les domaines non confinés sont conçus pour que les utilisateurs s'exécutent avec une faible interférence **SELinux**, alors que les démons faisant face au réseau continuent de s'exécuter dans des domaines confinés, protégés par **SELinux**
- **SELinux** prend en charge les attributs de type , qui peuvent regrouper plusieurs types différents et attribuer des privilèges à tout le groupe de types.

Limitation

Les applications normalement confinées peuvent également s'exécuter dans le domaine **unconfined_t** si elles sont lancées par un utilisateur dont les processus sont déjà dans le domaine **unconfined_t** : les transitions hors de **unconfined_t** sont exceptionnelles.

Les domaines confinés sont conçus pour prendre en charge les systèmes activés par **SELinux** dans lesquels les démons faisant face au réseau (les services) s'exécutent dans des domaines restreints (tels que **auditd_t** , **sshd_t** , etc.), mais dans lesquels les utilisateurs s'exécutent eux-mêmes de manière plus restreinte: toutes les commandes ils exécutent sont approuvés par le système.

Lorsque de telles configurations sont utilisées, **SELinux** est principalement configuré pour se protéger contre les attaques à distance (et les vulnérabilités exploitables à distance). Les attaques locales (toute vulnérabilité exploitable nécessitant un accès local) ne sont donc pas atténuées lors de l'utilisation de **SELinux** avec des domaines non confinés.