Bits SUID/SGID

- Unix utilise les notions de bits SUID / SGID
  - Permet aux utilisateurs d ’effectuer certaines tâches privilégiées
    - Exemple : changer son mot de passe
- SUID
  - Le programme doit être exécuté avec l’UID de l’utilisateur propriétaire
- SGID
  - Le programme doit être exécuté avec le GID du groupe propriétaire
- Programmes visés par les pirates pour obtenir des privilèges locaux après avoir exécuté du code sur le serveur
- Vieille faille : copier un shell et lui mettre le SUID root
  - Ne fonctionne pas pour tous les shells : exemple BASH

Processus

- Un processus est identifié par un PID
- Il est rattaché à un UID sous forme de
  - RUID : UID réel (l'utilisateur qui a lancé le processus)
  - EUID : UID effectif (propriétaire du fichier s'il est setuid)
  - UID de l'utilisateur
- Idem pour le GID
- FSUID / FSGID
  - UID / GID utilisé pour les accès au système de fichier sous Linux