**Rôles**

* **Tuteur** : Loïc
* **Animateur** : Pierre
* **Secrétaire** : Thibault
* **Scribe** : Charles
* **Gestionnaire** : Aurélien

**Mots-clés**

* Permissions sur les fichiers 🡪 groupe, stockage ?
* Sécurité
* Shell
* I-node
* Identifiant unique
* Root
* 2 modes sur le système : noyau et utilisateur
* Langage
* Programme d’administrateur
* Super-utilisateur
* Application
* L’utilisateur ne tente rien d’anormal
* Contrôle d’accès à la machine

**Analyse du Besoin**

* Sécuriser des fichiers à l’aide de permission
* Contrôler l’utilisateur à l’aide d’un script
* Savoir où sont stockées les permissions des utilisateurs

**Généralisation**

* Gestion d’accès

**Hypothèses**

* Le mode utilisateur est utilisé pour les appels système
* Mode noyau pour les accès aux périphériques et le matériel
* Le super-utilisateur root peut endommager le système
* Le super-utilisateur définit les droits
* Selon les droits, les utilisateurs utilisent des primitives qui sont donnée par le super-utilisateur
* L’utilisateur ne peut pas interagir entre eux mais le super-utilisateur peut avec eux (accès aux fichiers)
* Le shell permet la gestion des droits écrit par le super-utilisateur
* Le super-utilisateur peut modifier les i-nodes
* Permissions 🡪 portes (étapes posées par le super-utilisateur)
* 2 groupes : Super-utilisateur ou utilisateur normal 🡪 tris
* Sur Linux, « su root » permet l’accès au super-utilisateur
* Primitives dédiées en rapport avec les permissions
* Il y a des demandes de requêtes d’autorisation au super-utilisateur (mot de passe)
* Prise de contrôle par l’administrateur
* Primitive se déclenche juste pour le super-utilisateur (sudo 🡪 passage en super-utilisateur provisoire)
* Les autorisations dépendent du système d’exploitation, stockés selon l’OS
* Dans le Kernel, il y a une gestion de permission
* Regroupement grâce à des attributs spécifiques
* 1er utilisateur = super-utilisateur
* Dans les groupes, il y a différentes permissions (utilisation des fonctions)
* Script est automatisé pour le traitement et les autorisations.

**Plan d’action**

1. Le shell
2. Qu’est-ce que c’est ?
3. Droits
4. Permissions
5. Types de permissions
6. Modes (noyau et utilisateur)
7. Stockage permissions
8. Registres de processeur
9. Mécanismes de gestions des utilisateurs (appels système)
10. Primitives
11. Gestions utilisateur (groupes)