

Premiers pas dans les commandes Linux - Concepts de Sécurité sous Linux

Assurer la sécurité sous Linux implique de maîtriser quelques concepts clés et pratiques essentielles.

Cela va de la gestion prudente des utilisateurs et de leurs permissions à la mise en place de barrières solides comme les pare-feux.



Voici comment vous pouvez renforcer la forteresse de votre système Linux.

Gestion des Utilisateurs et des Groupes

La gestion des utilisateurs et des groupes sous Linux est essentielle pour assurer que seules les personnes autorisées ont accès à des informations ou des fonctionnalités spécifiques du système.

Créer et Gérer des Utilisateurs

- **Créer un utilisateur** : Utilisez `sudo adduser nomDeLUtilisateur` pour créer un nouvel utilisateur. Cela crée également un répertoire personnel pour l'utilisateur.
- **Modifier un utilisateur** : Pour modifier les propriétés d'un utilisateur existant, comme son nom ou son répertoire personnel, utilisez `sudo usermod`. Par exemple, `sudo usermod -l nouveauNom ancienNom` change le nom de l'utilisateur.

- **Supprimer un utilisateur** : `sudo deluser nomDeLUtilisateur` supprime l'utilisateur, mais pas son répertoire personnel. Utilisez `sudo deluser --remove-home nomDeLUtilisateur` pour également supprimer son répertoire.

Gestion des Groupes

- **Créer un groupe** : `sudo addgroup nomDuGroupe` crée un nouveau groupe.
- **Ajouter un utilisateur à un groupe** : `sudo adduser nomDeLUtilisateur nomDuGroupe` ajoute l'utilisateur au groupe spécifié.
- **Lister les groupes d'un utilisateur** : `groups nomDeLUtilisateur` affiche tous les groupes auxquels appartient l'utilisateur.

Comprendre et Gérer les Permissions



Chaque fichier ou répertoire a des permissions définies pour trois catégories d'utilisateurs : le propriétaire, le groupe et les autres.

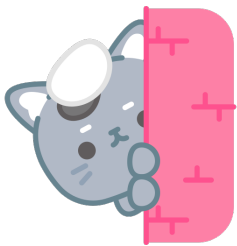
- **Lire les permissions** : Utilisez `ls -l` pour voir les permissions. Elles apparaissent comme une série de lettres, par exemple, `drwxr-xr-x`, où `d` indique un répertoire, `r` la permission de lecture, `w` celle d'écriture, et `x` celle d'exécution.
- **Modifier les permissions** : `chmod` est utilisé pour changer les permissions d'un fichier ou d'un répertoire. Par exemple, `chmod 755 fichier` définit les permissions de lecture, écriture et exécution pour le propriétaire, et de lecture et exécution pour le groupe et les autres.

Valeur octale	Autorisation	Description
0	---	Pas de permission
1	--x	Exécuter uniquement
2	-w-	Écrire seulement
3	-wx	Écrire et exécuter
4	r--	Lire seulement

Valeur octale	Autorisation	Description
5	r-x	Lire et exécuter
6	rw-	Lire et écrire
7	rwX	Lire, écrire et exécuter

- **Changer le propriétaire ou le groupe** : `chown utilisateur:groupe fichier` change le propriétaire et le groupe d'un fichier.

Configuration du Pare-feu avec UFW



`ufw` (Uncomplicated Firewall) est un outil simplifié pour gérer `iptables`, offrant une interface plus conviviale pour configurer le pare-feu.

- **Activer/Désactiver UFW** : `sudo ufw enable` active le pare-feu, tandis que `sudo ufw disable` le désactive.
- **Gérer les règles** : Pour autoriser ou bloquer des connexions spécifiques, utilisez `sudo ufw allow` ou `sudo ufw deny` suivi du service ou du numéro de port. Par exemple, `sudo ufw allow 22` autorise les connexions SSH.
- **Vérifier l'état et les règles** : `sudo ufw status verbose` affiche l'état du pare-feu et la liste des règles actives.

Bonnes Pratiques de Sécurité



- **Mises à jour régulières** : Assurez-vous que votre système et vos applications sont régulièrement mis à jour pour corriger d'éventuelles vulnérabilités.

- **Utilisation de mots de passe forts** : Utilisez des mots de passe complexes et uniques pour chaque service pour réduire le risque de compromission.
 - **Principe du moindre privilège** : Attribuez aux utilisateurs uniquement les permissions dont ils ont besoin pour leurs tâches.
-

Révision #1

Créé 2 avril 2024 10:17:33 par Renard

Mis à jour 22 avril 2024 16:14:09 par Renard