Réinitialiser le mot de passe local Administrateur Windows

Dans les versions de **Windows** antérieures à **Windows 10**, les mots de passe des utilisateurs locaux sont stockés dans le fichier **SAM** (Security Account Manager), qui est situé dans le dossier `%SystemRoot%\system32\config`.

Il existe plusieurs programmes Linux qui peuvent être utilisés pour réinitialiser le mot de passe Windows NT stocké dans le fichier SAM, mais l'un des plus populaires est **chntpw**.

Vous trouverez plus d'informations de chntpw sur le site officiel de l'outil : http://pogostick.net/~pnh/ntpasswd/

À partir de **Windows 10**, Microsoft a introduit une fonctionnalité appelée **Credential Guard**, qui stocke les informations d'identification des utilisateurs dans une zone isolée du système appelée **Secure Kernel**. Cette fonctionnalité est conçue pour offrir une meilleure protection contre les attaques de type **Pass-the-Hash**, qui peuvent être utilisées pour récupérer des informations d'identification stockées localement.

Actuellement, il n'existe pas de méthode pour écraser le mot de passe Administrateur local sans recourir à un solution de compte en ligne Microsoft. Toutefois, il est possible d’exécuter une réinitialisation de l'ordinateur qui effacera toutes les comptes et données personnelles de l'ordinateur.

Pour cela, il faut accéder aux options de démarrage avancées sous Windows 10/11. Vous pouvez suivre ces étapes :

1. Cliquez sur le bouton “Démarrer” de Windows.
2. Maintenez la touche “Maj” enfoncée tout en cliquant sur le bouton “Redémarrer”.
3. Cela ouvrira les options de démarrage avancées de Windows.
4. Vous pouvez sélectionner l'option souhaitée, comme “Réinitialiser ce PC”.

Et sous Linux ?

Sous Linux les informations sur les utilisateurs et leurs mots de passe sont stockées dans des fichiers spécifiques, tels que `/etc/passwd` et `/etc/shadow`.

Le fichier `/etc/passwd` contient des informations sur les utilisateurs du système, tels que leur nom d'utilisateur, leur identifiant d'utilisateur (UID), leur groupe primaire et leur répertoire de travail. Le fichier `/etc/shadow` contient les mots de passe hachés des utilisateurs.

Les mots de passe hachés sont stockés dans le fichier `/etc/shadow` car ce fichier est accessible uniquement par l'utilisateur **root**, qui est le seul utilisateur ayant les permissions pour le lire. Cela

permet de protéger les informations sensibles contenues dans le fichier.

Les administrateurs système peuvent utiliser des outils de gestion des utilisateurs tels que `useradd`, `userdel` et `passwd` pour **créer**, **supprimer** et **modifier** les comptes d'utilisateurs et les mots de passe sur un système Linux. Ces outils sont souvent utilisés en conjonction avec des mécanismes d'authentification, tels que **PAM** (Pluggable Authentication Modules), qui permettent de personnaliser les méthodes d'authentification des utilisateurs sur un système Linux.