

Réinitialiser mot de passe admin Windows Vista et 7

<http://blogmotion.fr/systeme/reinitialiser-mot-de-passe-admin-windows-vista-et-7-reset-password-2109>

(Dernière modification le 26 décembre 2009 à 19:05)



Il peut arriver que l'on oublie son **mot de passe** sous **Windows**. C'est assez gênant quand il s'agit du seul compte (**administrateur**) existant sur la machine!

Inutile de formater, j'ai trouvé une solution radicale qui permet de **réinitialiser le mot de passe** de n'importe quel compte (administrateur compris) en exploitant une étourderie laissée (par erreur ?) par Microsoft 😊

Cette faille fonctionne sous **Windows Vista** et **Windows 7** (seven), ce qui est en soit pas très étonnant vu le faible écart de version des noyaux.

Principe de fonctionnement

Je fais en fait l'appel à un exécutable **avant** d'être logué qui va me permettre d'accéder à l'invite de commande en tant qu'**utilisateur système**. Libre à moi ensuite de changer un mot de passe, créer un utilisateur, formater, etc. Bref toutes les commandes sont disponibles.

Étape 0 : Créer un disque bootable BartPe

Pour créer un BartPe : <http://www.nu2.nu/pebuilder/>

Étape 1 : jouer avec deux exécutables

Utilisez un [LiveCD](#) tel que [Knoppix](#), [BackTrack](#) ou encore [BartPE](#) afin d'accéder à votre **partition système NTFS** (C: depuis Windows).

- **Renommez** le fichier **Utilman.exe** en **Utilman.exe.bak** situé dans le répertoire C:\Windows\System32\
- **Faites une copie du fichier cmd.exe** et renommez le **Utilman.exe** (tout se passe dans le même répertoire).

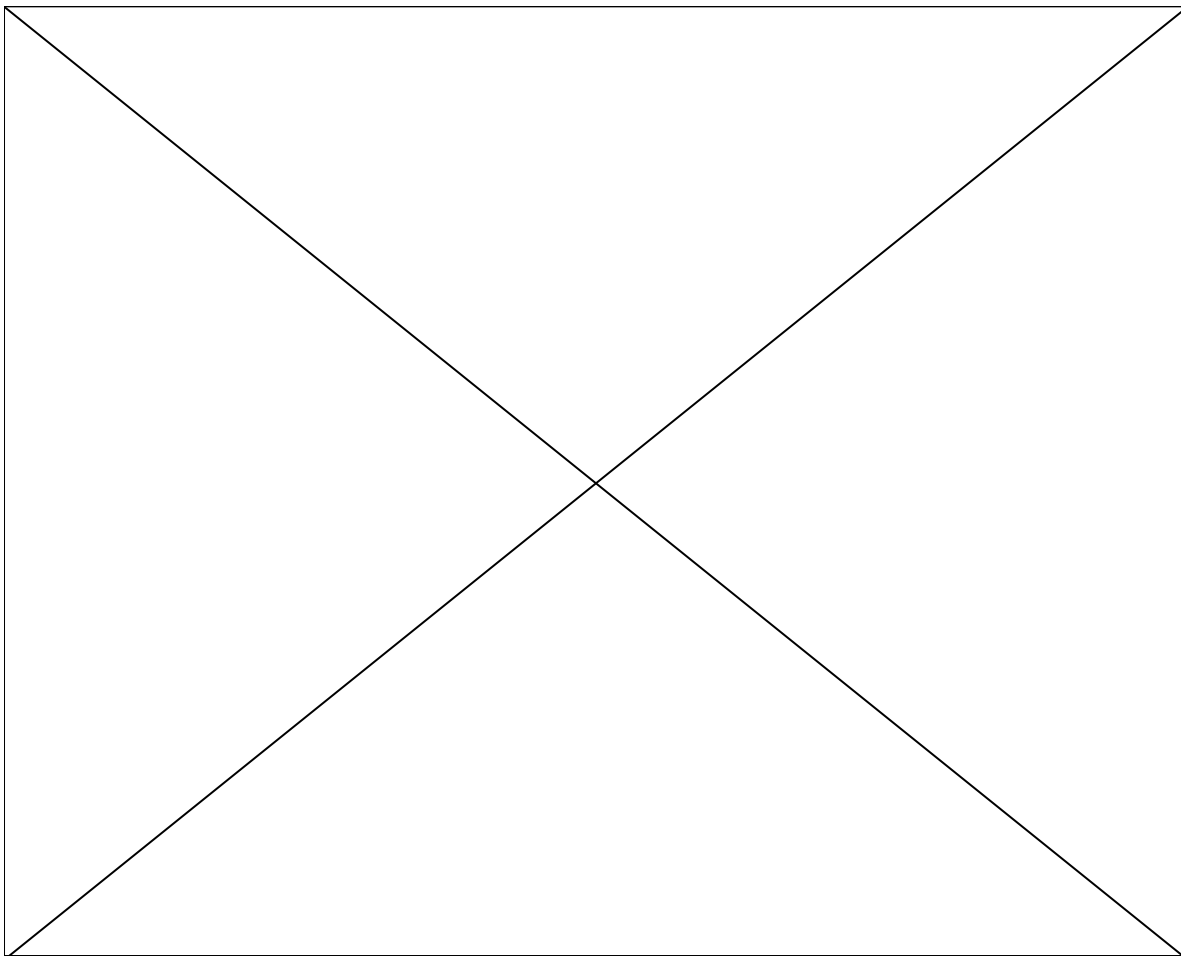
Nous venons de remplacer l'exécutable de gestion des **options d'ergonomie** (Utilman.exe) par l'exécutable de **l'invite de commande** (cmd.exe)

Redémarrez votre PC normalement sous Windows (Vista ou Seven).

Étape 2 : exploiter la faille

Devant le succès du [précédent screencast](#) sur [Spotify](#) je me suis décidé à vous en faire un autre. Je regrette presque à chaque fois tellement le montage (zoom & pan) prend du temps, mais bon à défaut de trouver mieux...

J'ai réalisé ce screencast sous [Windows 7 virtualisé](#) grâce à [VirtualBox](#).



(pensez à activer la HD dans le lecteur YouTube pour une meilleure lecture)

Dans mon exemple je **crée un utilisateur** "bmotion" avec le **mot de passe** "kikoolol" et je l'ajoute dans le **groupe des administrateurs** ("administrators" car la bêta est en anglais).

Voir également la vidéo utilisant [BackTrack 3](#) chez [Offensive Security](#).

Conclusion

Que dire... que les ingénieurs et les développeurs Microsoft auraient du **intégrer** l'appel à ce fameux utilitaire d'accessibilité au coeur même du système au lieu de faire appel à un "**exécutable tiers**".

Une fois de plus je constate que Windows Seven n'est qu'une pale copie de Windows Vista, même ses défauts n'ont pas bougés, pour ce qui est des qualités je miserai uniquement sur l'esthétique de la barre des tâches !

N'oublions pas que Windows Vista est en noyau **6.0** et Windows Seven en **6.1**. A titre de comparaison Windows XP est équipé du noyau **5.1**, soit un réel bon de version !

Je n'espérai pas moins qu'un noyau **7.0** pour Seven, ce qui après tout serait bien tombé, raté !