Réinitialiser les mots de passe Windows XP, VISTA, 7

Date de dernière mise à jour : 11/07/2015 à 16:05

Procédure pour réinitialiser les mots de passe des comptes administrateur et locaux

Attention ! :

Cette méthode est autorisée dans le cadre de la loi seulement si il s'agit d'un ordinateur qui vous appartient. Je ne suis en aucun cas responsable de l'utilisation que certains peuvent en faire.

Description.

Offline NT Password & Registry Editor est un utilitaire pour réinitialiser le mot de passe des comptes utilisateur locaux sous Windows NT, Windows 2000, Windows XP, Windows Serveur 2003, Windows Vista (32 / 64 bits), Windows 7, Windows Serveur 2008. Vous n'avez pas besoin de connaître l'ancien mot de passe pour en mettre un nouveau. Pour cela, vous devez arrêter votre ordinateur et redémarrer sur le CD de l'utilitaire.Le CD inclut l'accès aux partitions NTFS, FAT et FAT32. L'utilitaire détectera les comptes utilisateur et permettra de les déverrouiller ou de les désactiver. Il permet également d'éditer la base de registre. Vous pouvez ajouter un utilisateur dans le groupe local Administrateur pour devenir administrateur.

Quand et Pourquoi l'utiliser ?

Il peut arriver que vous perdiez le mot de passe du compte administrateur local de votre PC.Le système Windows NT stocke les informations de l'utilisateur, en incluant les versions cryptées des mots de passe des comptes utilisateurs locaux, dans un fichier appelé "**SAM**" (Security Account Manager ou Gestionnaire des Comptes de Sécurité), habituellement sous : **%systemroot%\winnt\system32\config**.

Si Windows offre bel et bien un niveau de sécurisation élevé (particulièrement avec Windows 7), ça n'est vrai que s'il est en cours d'exécution.

Mais Microsoft ne fournit pas le moyen de changer le mot de passe si vous ne pouvez pas ouvrir une session avec les droits de le faire, excepté depuis la disquette de secours Microsoft si vous l'avez générée. Cet utilitaire permet de résoudre le problème, en permettant via le CD d'accéder et de modifier le fichier SAM.

Avertissement !!

Si cette méthode est utilisée sur la/les sessions d'utilisateurs qui ont des fichiers cryptés EFS, sur Windows XP ou plus récent, tous les fichiers chiffrés pour cet utilisateur seront illisible! et ne pourront pas être récupérées, le mot de passe lui-même étant utilisé pour crypter les clés nécessaires pour EFS.A ma connaissance et à ce jour il n'y a aucun moyen de récupérer les fichiers une fois que le mot de passe a été réinitialisé.

Comment faire le CD ?

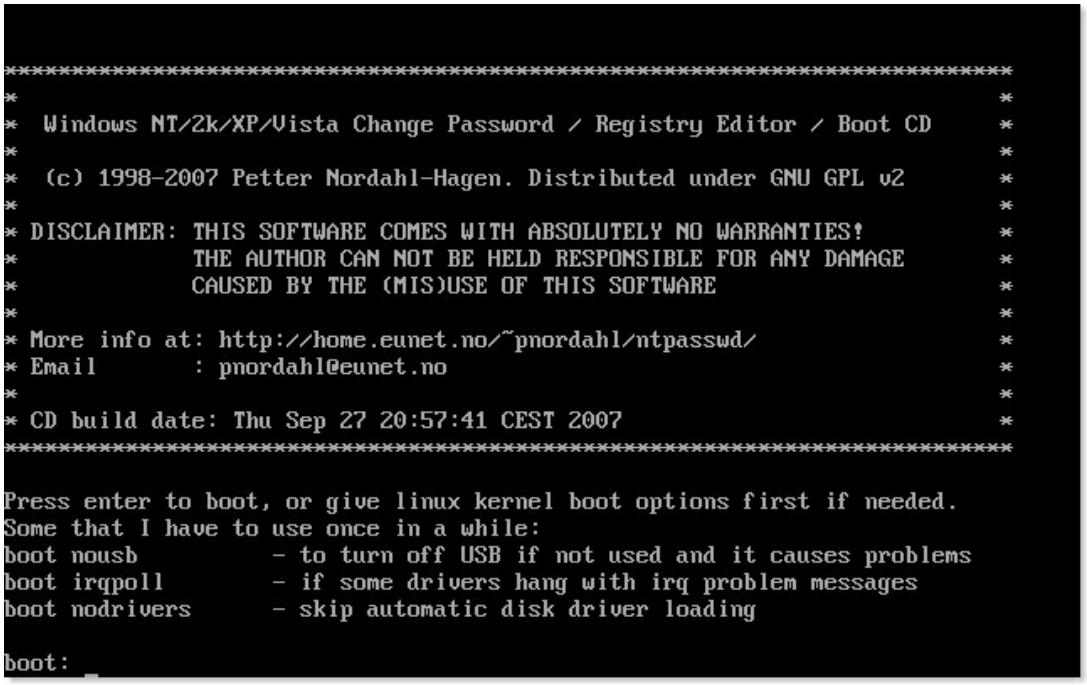
après avoir télécharger le fichier : http://pogostick.net/~pnh/ntpasswd/ le fichier **cd140201.zip**, il doit contenir le fichier image ISO : **cd140201.iso**. Il peut être gravé avec n'importe quel programme de gravure à condition que l'option Graver une image ISO soit prise en compte. Une fois gravé sur le CD, il doit seulement contenir les fichiers suivants :BOOT.CAT, BOOT.MSG, INITRD.CGZ, ISOLINUX.BIN, ISOLINUX.CFG, README.TXT, SCSI.CGZ, SYSLINUX.CFG, SYSLINUX.EXE et VMLINUZLe PC devra ensuite démarrer sur le CD.Vos pouvez aussi choisir la version pour installation sur clé USB Bootable : **usb140201.zip**

Fonctionnement-.

Le programme fonctionne pour : NT 3.51, NT 4 (toutes versions et Service Pack), Windows 2000 (toutes versions et Service Pack), Windows XP (toutes versions, inclus SP2 et SP3), Windows Serveur 2003 (tous Services Packs),Windows Vista (32/64 bits,SP1 inclus), Windows 7 (toutes versions), Windows Serveur 2008.

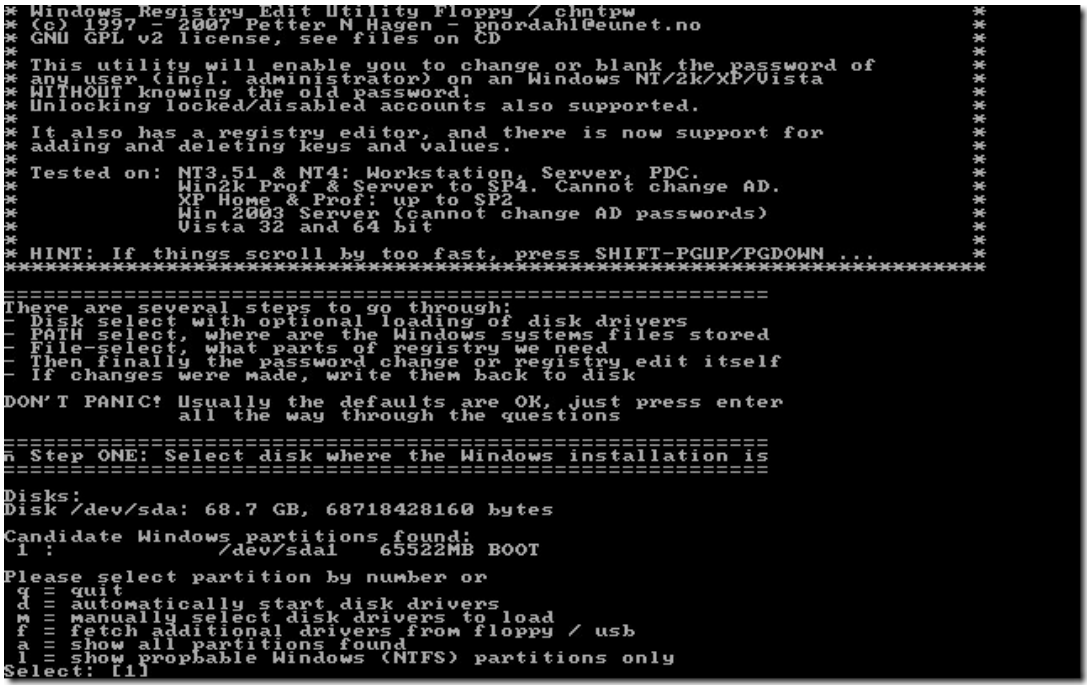
Utilisation (procédure pas à pas).

Redémarrer sur le CD.Après le boot , attendre ou valider par la touche Entrée



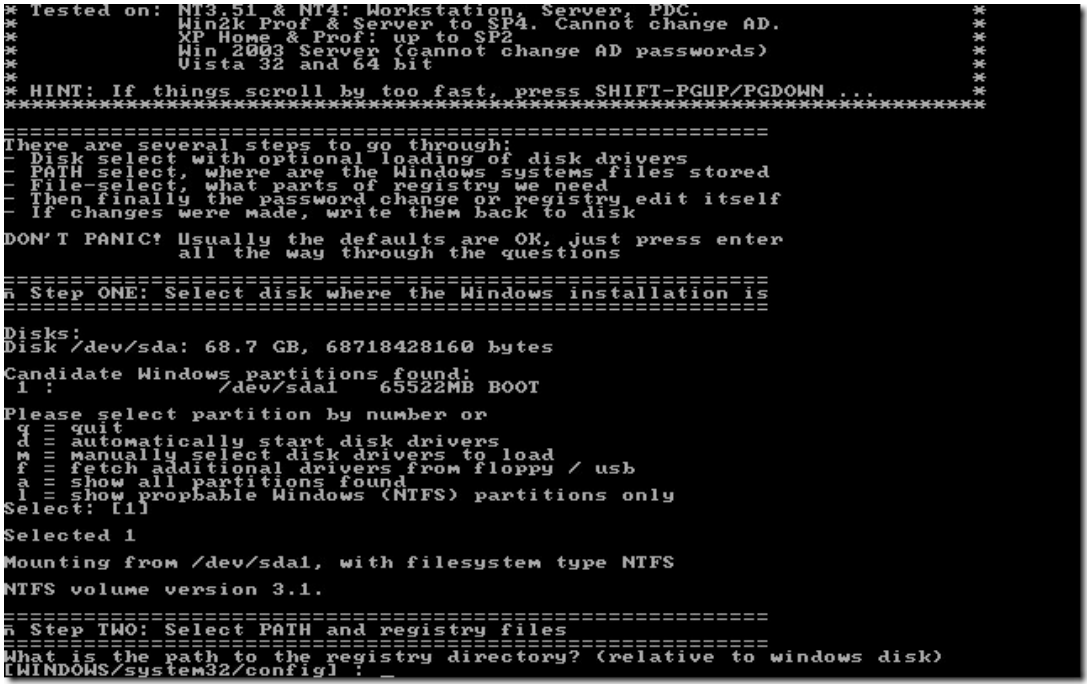
Sélectionner la version de boot. Dans la plus part des cas laisser le **choix 1** pour sélectionner la partition NT trouvée et valider par la touche Entrée

.

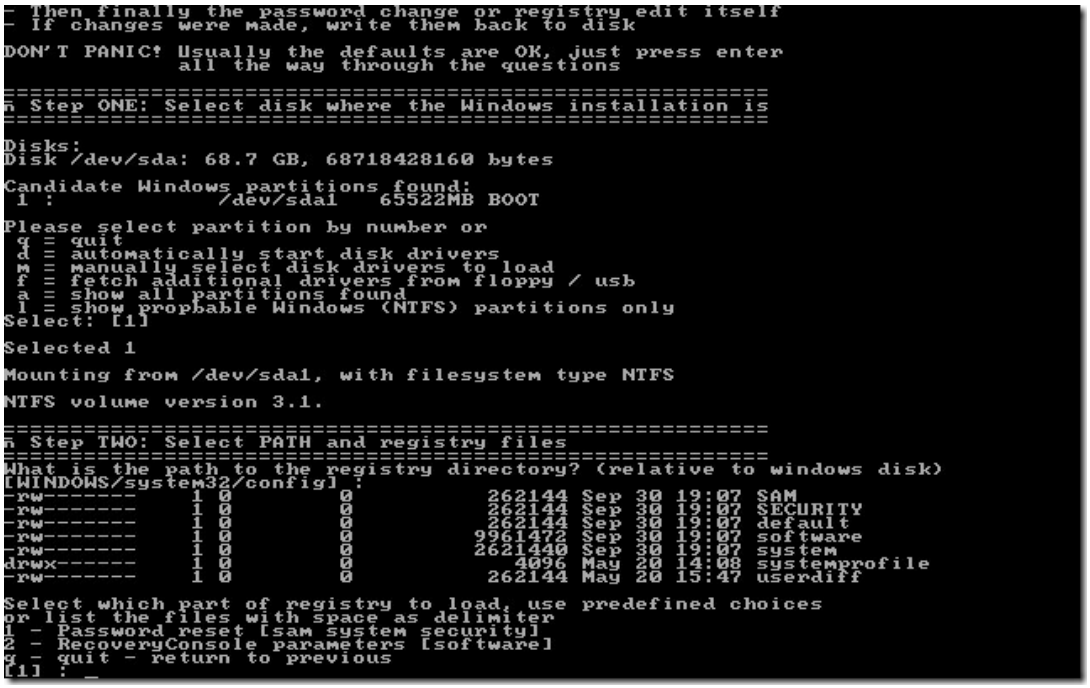


L'écran suivant demande à quel niveau se situe le mot de passe. Pour un mot de passe système, on sélectionne la base SAM soit le 1 (par défaut), valider par la touche Entrée

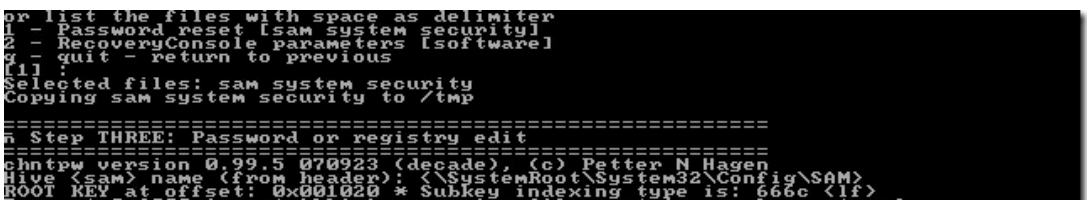
.



Laisser le **choix 1** pour changer le mot de passe et valider par la touche Entrée.

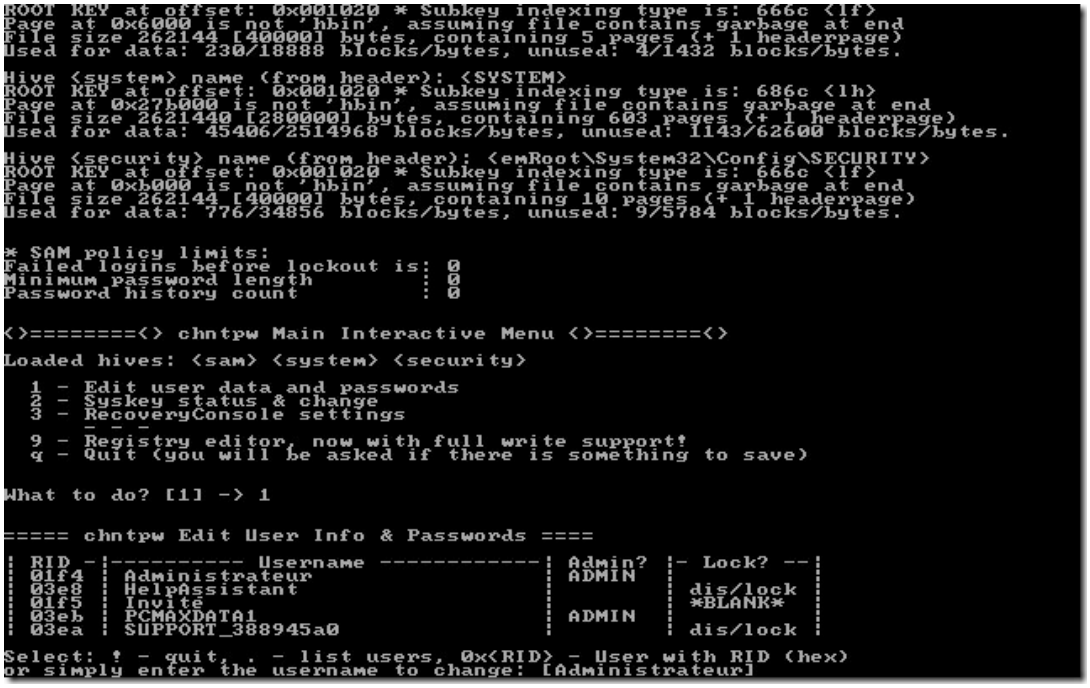


Laisser le **choix 1** pour éditer le compte et valider par la touche Entrée.



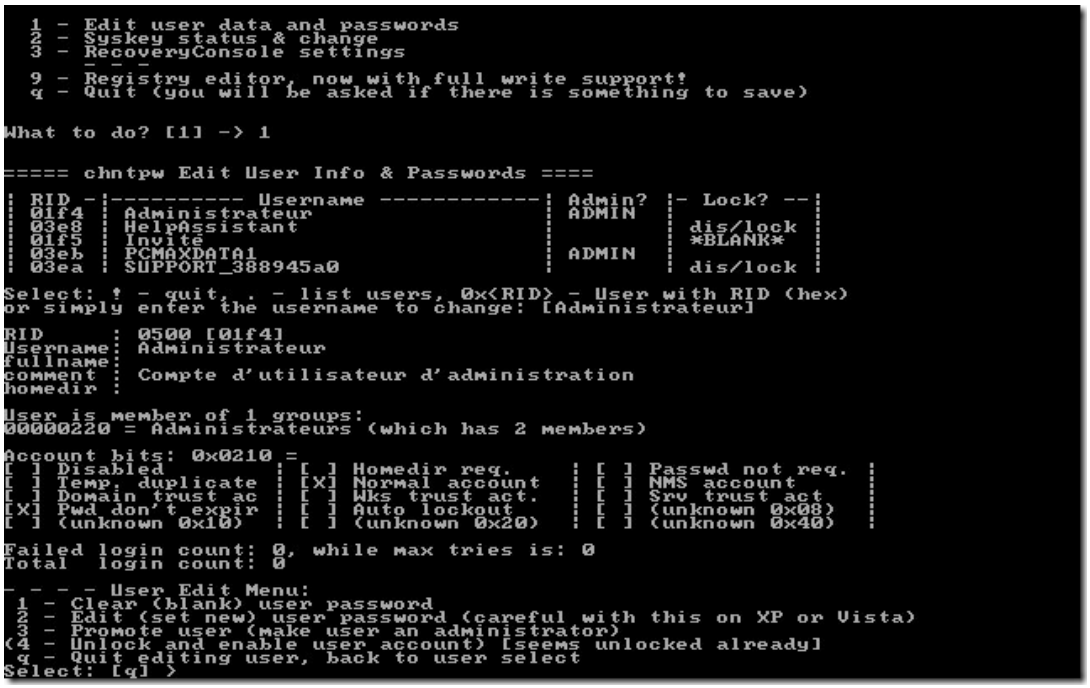
- Laisser le compte Administrateur par défaut et valider par la touche Entrée

.- Vous pouvez aussi sélectionner d'autres comptes.- Il peut arriver que le compte soit désactivé (**dis**=disabled) ou verrouillé (**lock**=locked), il vous sera proposer de le réactiver ou le déverrouiller.



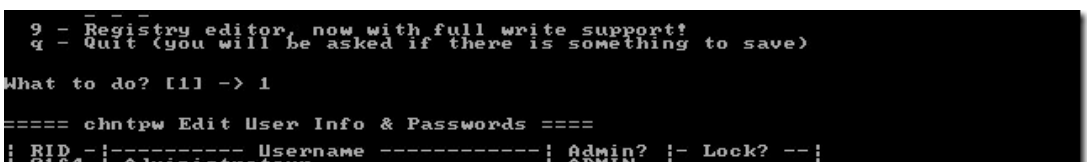
- Taper **!** pour mettre le mot de passe à blanc (clavier français = Touche **VerrNum** 1) et valider par la touche Entrée

. Attention!, n'utiliser pas le pavé numérique.- Vous pouvez aussi ajouter un nouveau mot de passe (**choix 2**), promouvoir un autre compte en administrateur (**choix 3**) ou déverrouiller et activer le compte (**choix 4**)



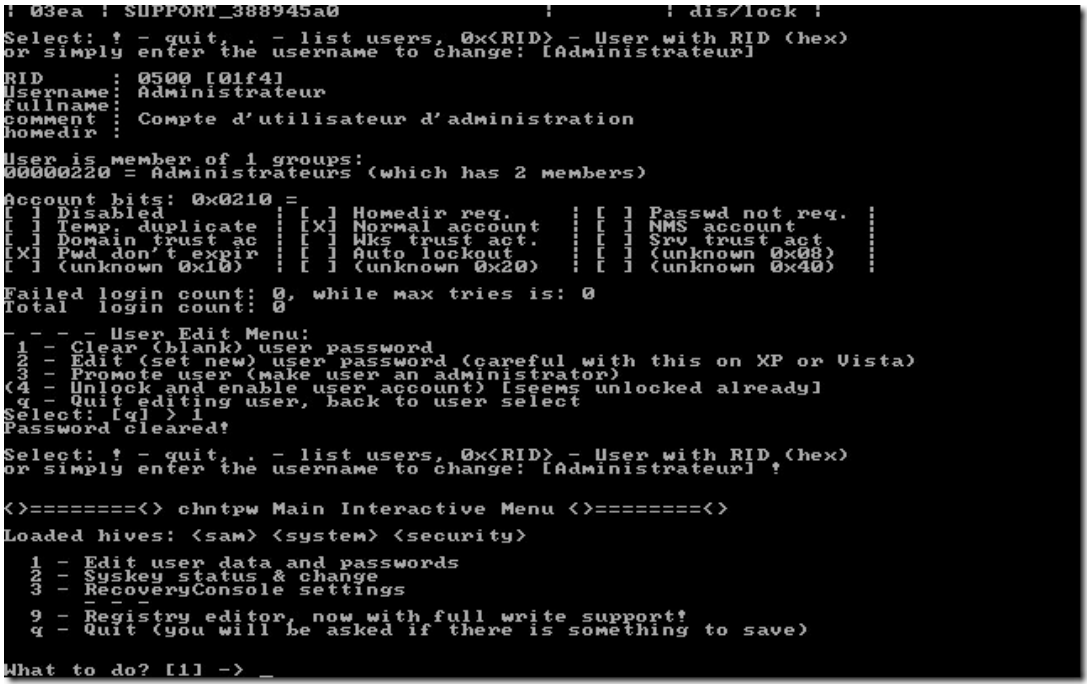
Taper **1** pour quitter (clavier français = Touches Maj+&) et valider par la touche Entrée

.



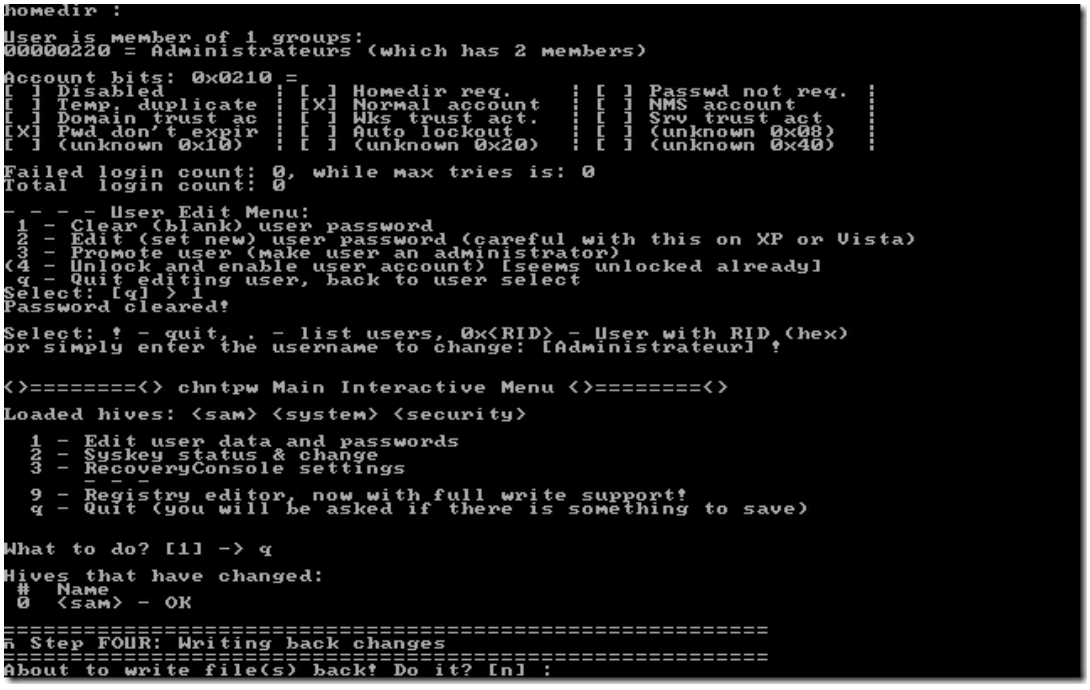
Taper **q** pour quitter (clavier français = Touche **a**) et valider par la touche Entrée

.



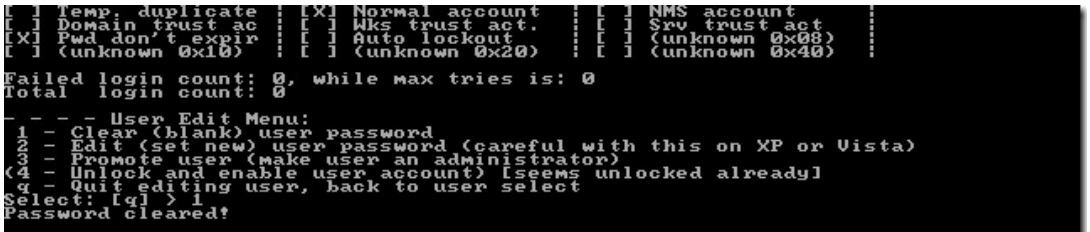
Taper **y** pour valider les changements et valider par la touche Entrée

.

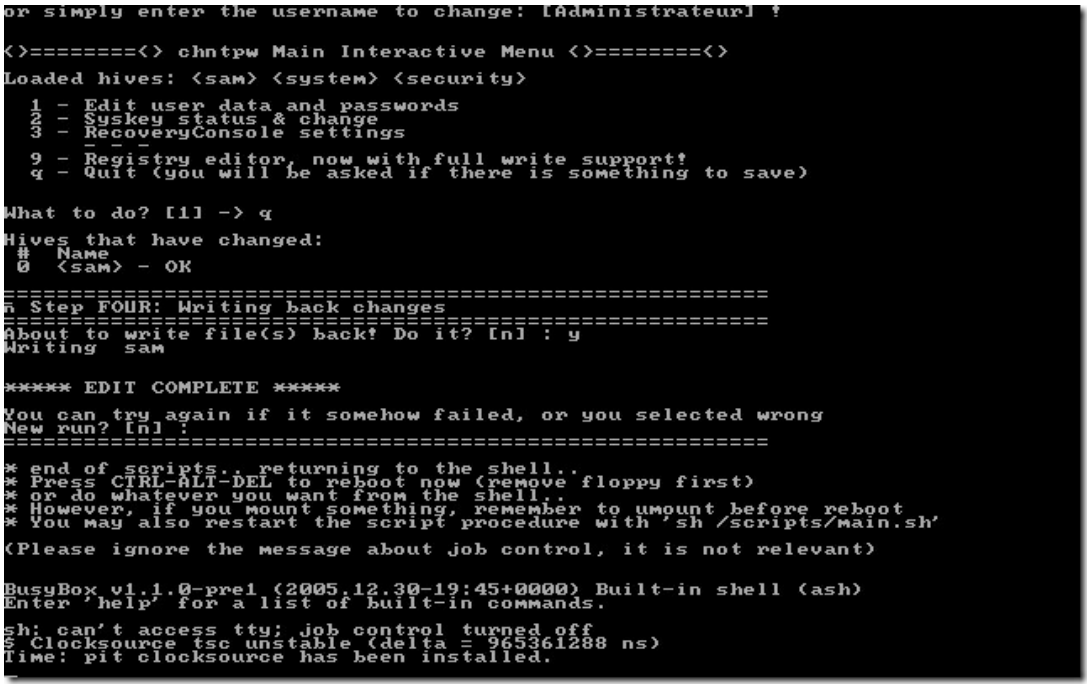


Vous pouvez retourner dans le menu, sinon accepter le choix par défaut **n** et valider par la touche Entrée

.



- Retirer le CD.- Redémarrer la machine depuis la combinaison de touche **Ctrl+Alt+Suppr**- Se connecter sous Windows avec le compte Administrateur sans mot de passe.



Et voila c'est fini, vous pouvez à nouveau accéder à votre bureau !

Autres utilitaires permettant aussi de réinitialiser les mots de passe.

liste non exhaustive
.BackTrack (surtout connu pour ses capacités à éprouver la sécurité d'un réseaux)

Hiren's Boot CD (multitool très complet,<a href="http://easy.pc.blog.free.fr/index.php?post/Hiren-s-Boot-CD" class="bbc_url" title="Lien externe" rel="nofollow external"> certains détracteur lui reproche de ne pas être légal, à cause de protection de licence non respectée)

MultiBootISOs (dans la ligne d'HBCD ci dessus)

Shardana Antivirus Rescue Disk Utility (SARDU - lien direct) (dans le même style qu' **Hiren's Boot CD**, moins complet certes, mais lui il n'est pas considéré comme un illégal) -

Ultimate Boot CD (UBCD) (certainement le plus connu)