

Récupération d'un compte en local sous windows XP

Situation Professionnelle
2022
parcour SISR

PRÉSENTÉ PAR
Sandy Cerrato

2022



Situation professionnelle		
NOM PRENOM Cerrato Sandy	N° CANDIDAT	PARCOURS SISR

Récupération d'un compte via une faille de sécurité				
ÉPREUVE	<input checked="" type="radio"/> Épreuve ponctuelle <input type="radio"/> Contrôle en cours de formation			
MODALITÉS DE RÉALISATION	Contexte basé sur une demande d'un client en entreprise			
CONTEXTE GÉNÉRAL	PÉRIODE	2022	DURÉE ESTIMÉE	30min
DESCRIPTION DE LA MISSION - DESCRIPTION DES BESOINS - RÉSULTATS ATTENDUS	Réussir à re donner l'accès à un compte en local sur le pc d'un client qui avait égarer son mot de passe			
RESSOURCES MOBILISÉES	<ul style="list-style-type: none"> ➤ Clef usb windows xp ➤ PC utilisateur 			
PRINCIPAUX SAVOIR-FAIRE MOBILISÉS	<ul style="list-style-type: none"> ➤ Collecter, suivre et orienter des demandes ➤ Traiter des demandes concernant les services réseau et système, applicatifs 			
PRODUCTION ASSOCIÉES	Synoptique recto/verso, annexes descriptives + screenshot.			
MODALITÉS D'ACCÈS AUX PRODUCTIONS EN LIGNE	http://localhost:3000/index.php			

RAPPORT D'ACTIVITE

ETAPE 1	Création de l'environnement de travail, définitions des objectifs		
OBJECTIF(S)	Avoir un environnement de travail fonctionnel et une vision clair de la marche à suivre		
RESSOURCE(S)	Récupération du pc client		
CHRONOLOGIE DE RÉALISATION	➤ Analyse du pc et de son système d'exploitation		
ETAPE 2	Analyse		
OBJECTIF(S)	Vérification des dires du client		
RESSOURCE(S)	Clef bootable, Système exploitation Windows XP, pc client		
CHRONOLOGIE DE RÉALISATION	➤ Allumer l'ordinateur ➤ Insérer le clef USB et booter sur elle ➤ Installer Windows xp ➤ Passer en ligne de commande ➤ Déclarer nouveau id et mdp ➤ Rendre l'ordinateur au client		
ETAPE 3	Mise en place		
RESSOURCE(S)	ligne de commande		
CHRONOLOGIE DE RÉALISATION	➤ Recherche du disque de stockage ➤ sauvegarde ➤ modification ➤ ré injection de la sauvegarde		

Procédure de récupération de mots de passe sous Windows.

Sous Windows les mots de passe peuvent être réinitialiser ou modifier il en vas de même pour les compte de sessions.

J'ai eu le cas avec un client qui après un retour de vacance un peu long, avait oublier ses codes connexion sur sa session locale et donc n'avais plus d'accès a ses données sur le pc.

Réinitialiser le mot de passe d'un utilisateur grâce à une faille de sécurité de Windows...

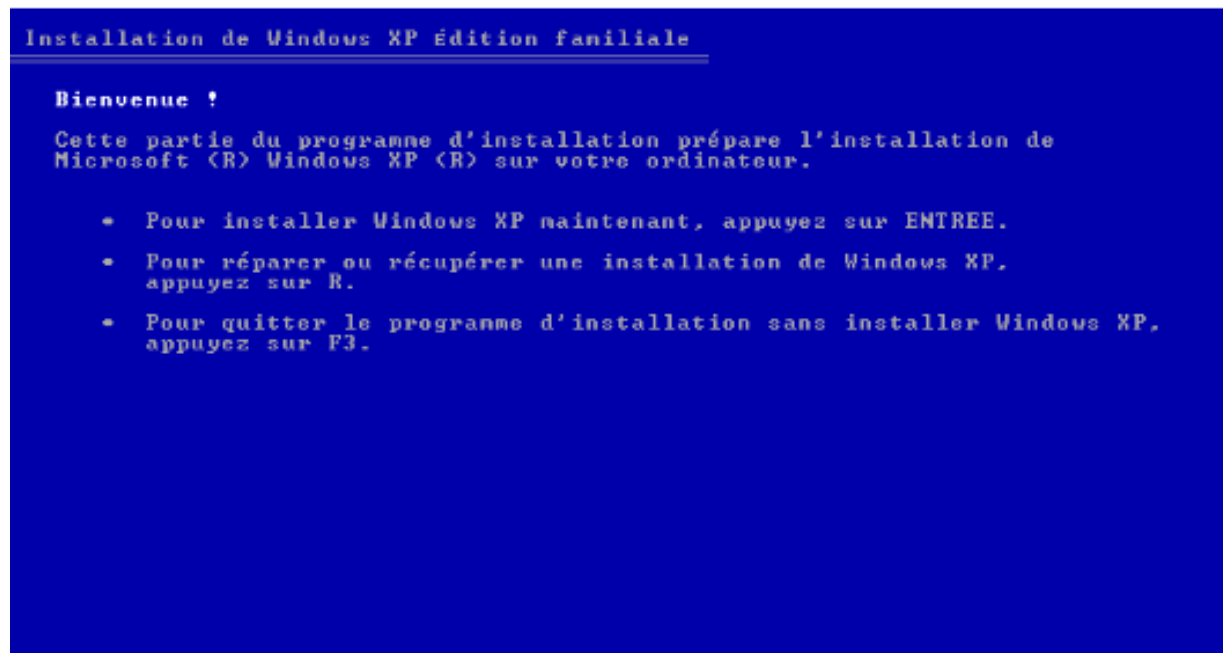
Comment ça marche ?

Au démarrage de Windows, un fichier exécutable est chargé : utilman.exe. Ce fichier permet d'accéder aux options d'ergonomie de Windows .On peut le lancer manuellement en pressant les touches Windows + U.

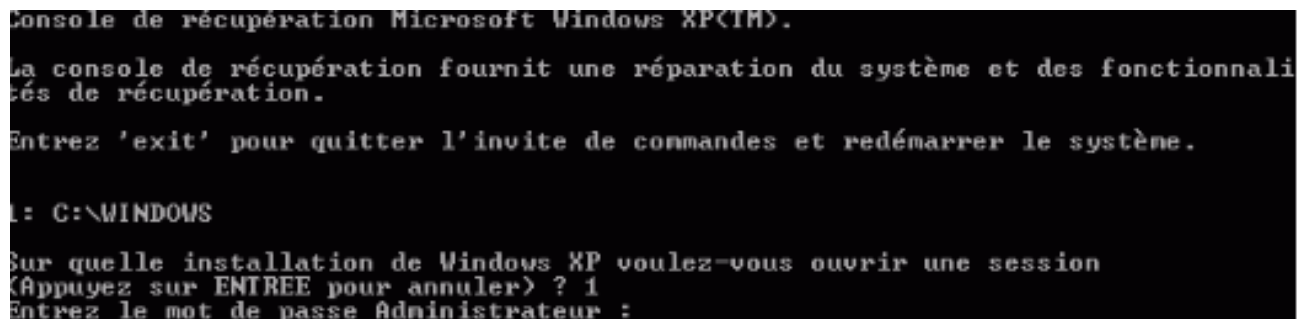
La technique consiste à remplacer les options d'ergonomie par l'invite de commandes. Pour ce faire, on va renommer cmd.exe (le fichier exécutable de l'invite de commande) en utilman.exe. Ainsi, lorsqu'on appuiera sur les touches windows + U, cela lancera l'invite de commandes au lieu des options d'ergonomie, nous permettant de modifier le mot de passe d'un compte utilisateur Windows.

Lancez l'invite de commandes :

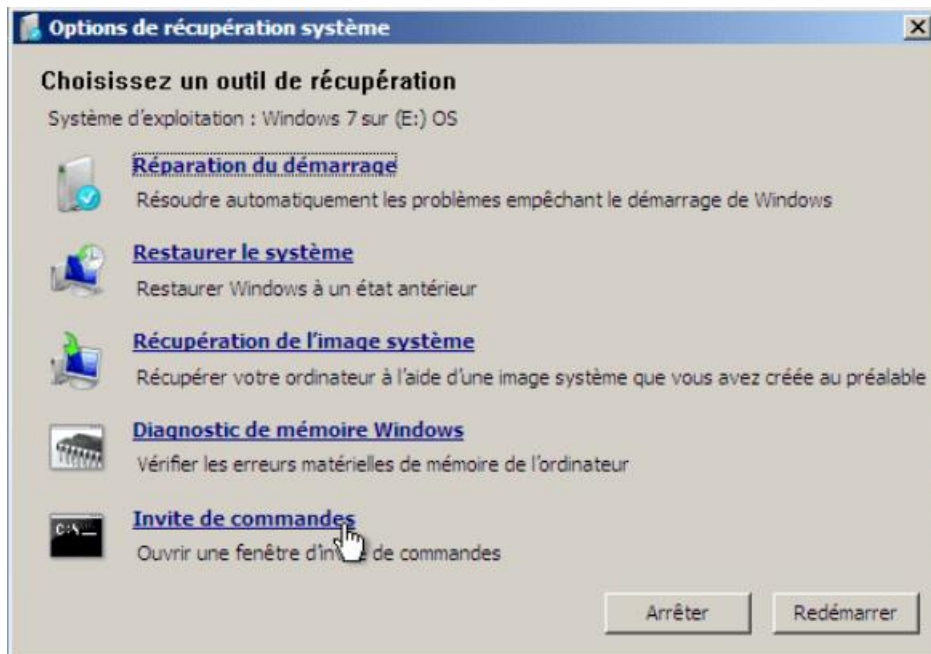
Avec Windows XP, via la Console de récupération : démarrez votre PC sur une clé USB d'installation de Windows XP (fonctionne aussi avec windows 8 et 10) puis appuyez sur la touche R pour lancer la Console de récupération de Windows.



Entrez le numéro correspondant à l'emplacement où se trouve votre installation de Windows XP (le plus souvent c'est le 1)



Avec Windows XP : récupération système > invite de commande



Ce rendre sur le bon disque de volume (si on ne sait pas du quel il s'agit on utilise la commande « dir » elle liste les contenus)

Ici il y a les fichier propre à Windows donc je suis au bon endroit

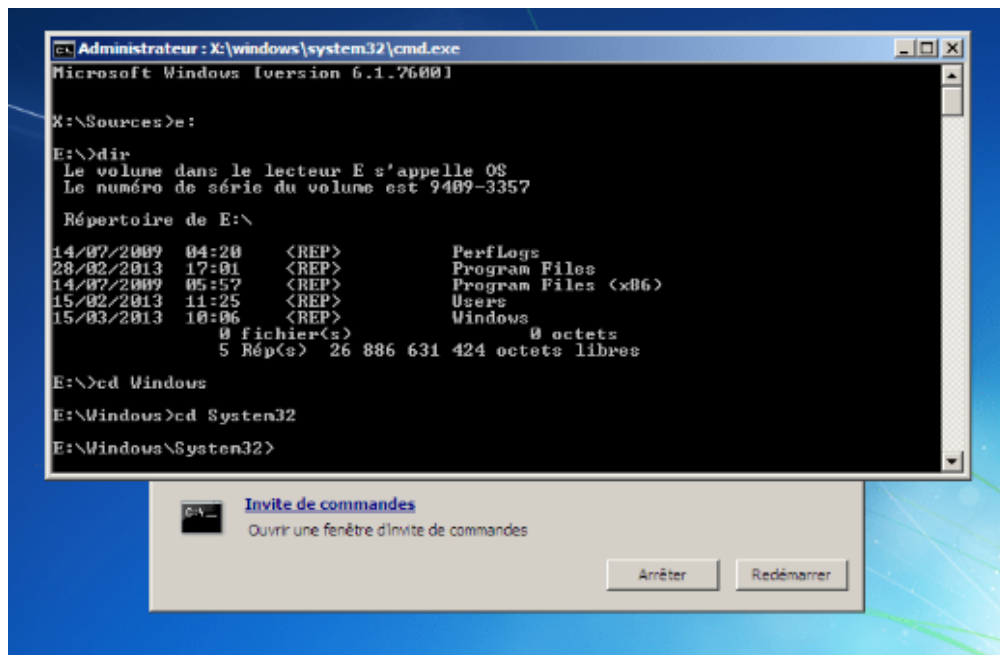
```
> e:
> dir
Le volume dans le lecteur E s'appelle OS
Le numéro de série du volume est C016-7234

Répertoire de E:\

12/04/2018  01:38    DIR                PerfLog
13/06/2018  19:35    DIR                Program
12/04/2018  18:19    DIR                Program
13/06/2018  13:40    DIR                Users
13/06/2018  22:11    DIR                Windows
```

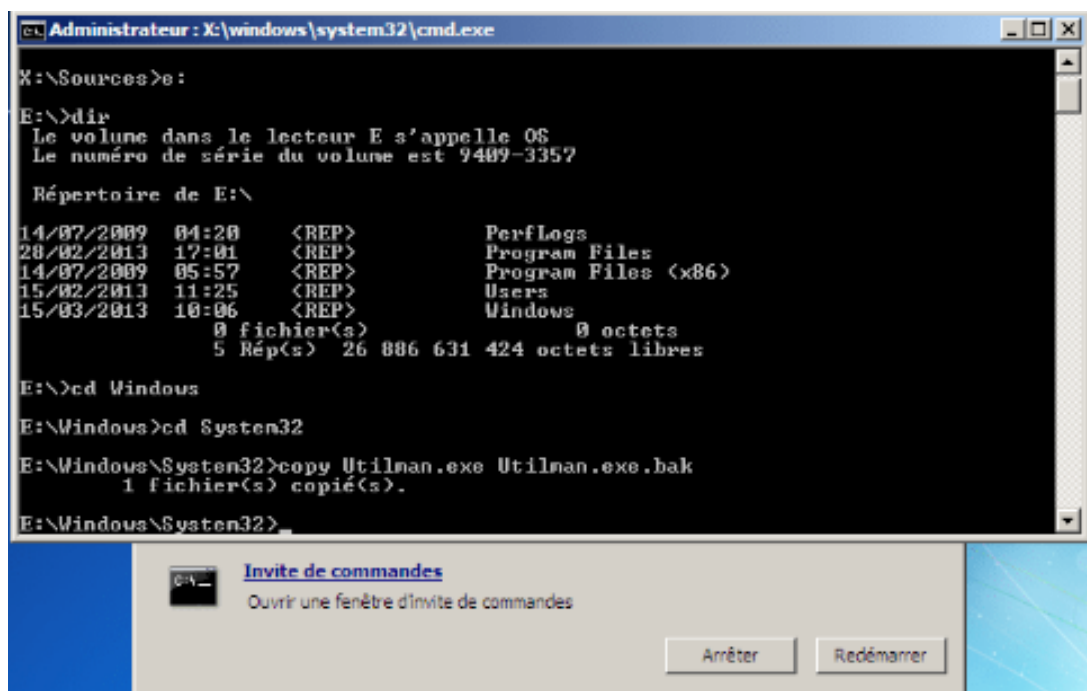
Une fois le bon disque trouvé il faut se déplacer du dossier Windows à celui de system

- Cd Windows
- Cd System32



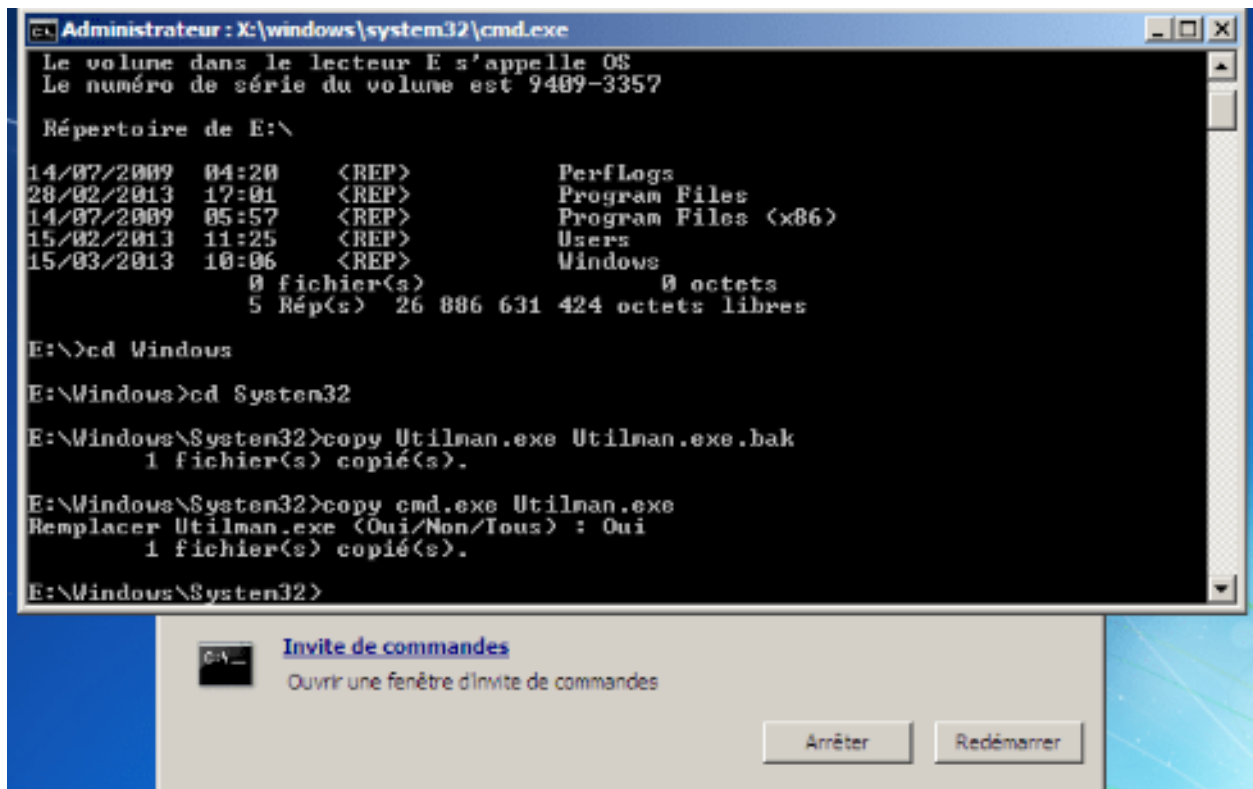
Maintenant il faut faire une sauvegarde du fichier utilman.exe, on le récupéra par la suite.

- copy Utilman.exe Utilman.exe.bak



Remplacez : utilman.exe par cmd.exe

- copy cmd.exe Utilman.exe



```
Administrateur : X:\windows\system32\cmd.exe
Le volume dans le lecteur E s'appelle OS
Le numéro de série du volume est 9409-3357

Répertoire de E:\
14/07/2009  04:20    <REP>          PerfLogs
28/02/2013  17:01    <REP>          Program Files
14/07/2009  05:57    <REP>          Program Files (x86)
15/02/2013  11:25    <REP>          Users
15/03/2013  10:06    <REP>          Windows
               0 fichier(s)                0 octets
               5 Rép(s) 26 886 631 424 octets libres

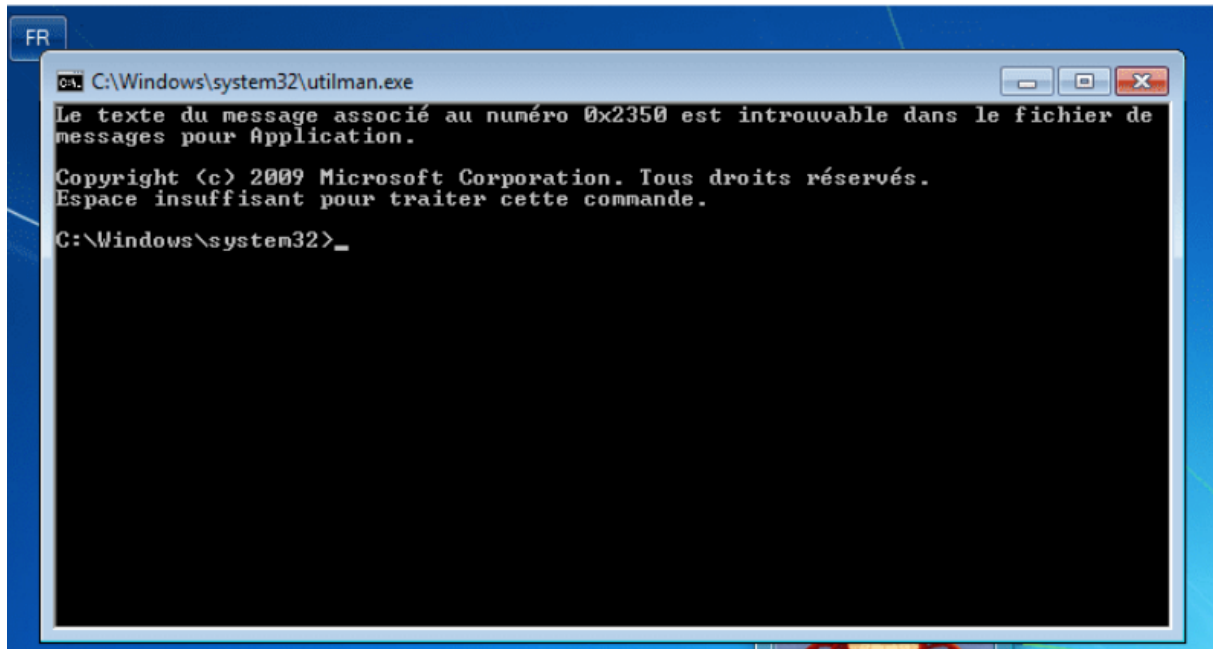
E:\>cd Windows
E:\Windows>cd System32
E:\Windows\System32>copy Utilman.exe Utilman.exe.bak
1 fichier(s) copié(s).
E:\Windows\System32>copy cmd.exe Utilman.exe
Remplacer Utilman.exe (Oui/Non/Tous) : Oui
1 fichier(s) copié(s).
E:\Windows\System32>
```

Invite de commandes
Ouvrir une fenêtre d'invite de commandes

Arrêter Redémarrer

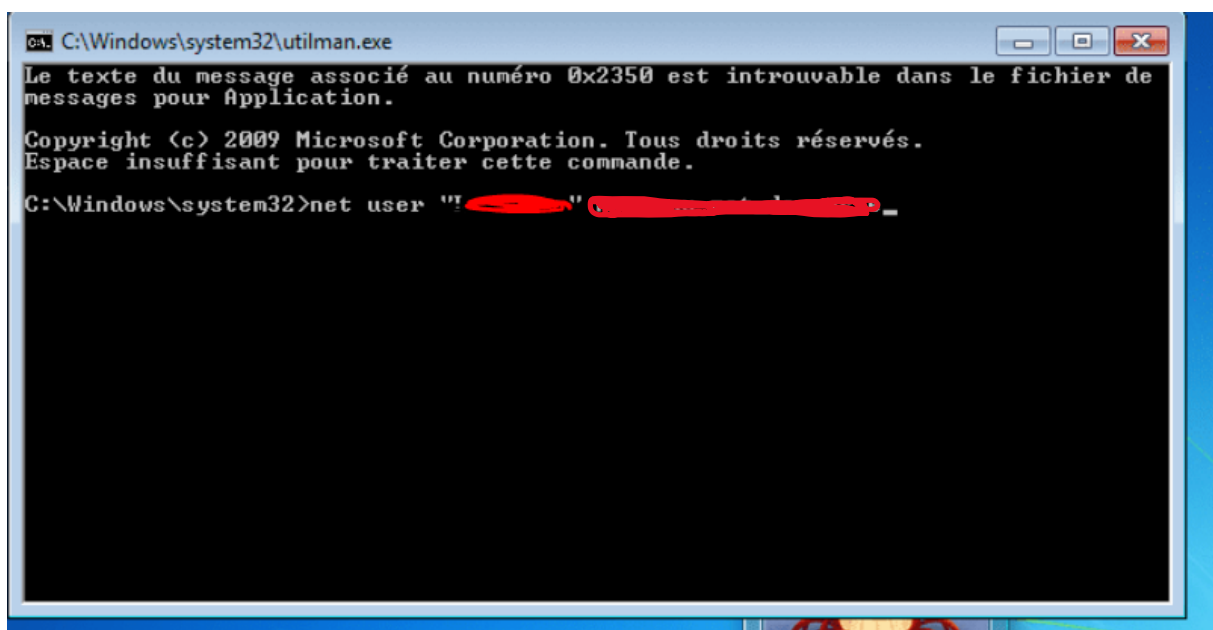
Maintenant il faut redémarrer le pc.

Sur l'écran de connexion de Windows, il faut appuyer sur les touches Windows + U pour lancer l'invite de commandes.



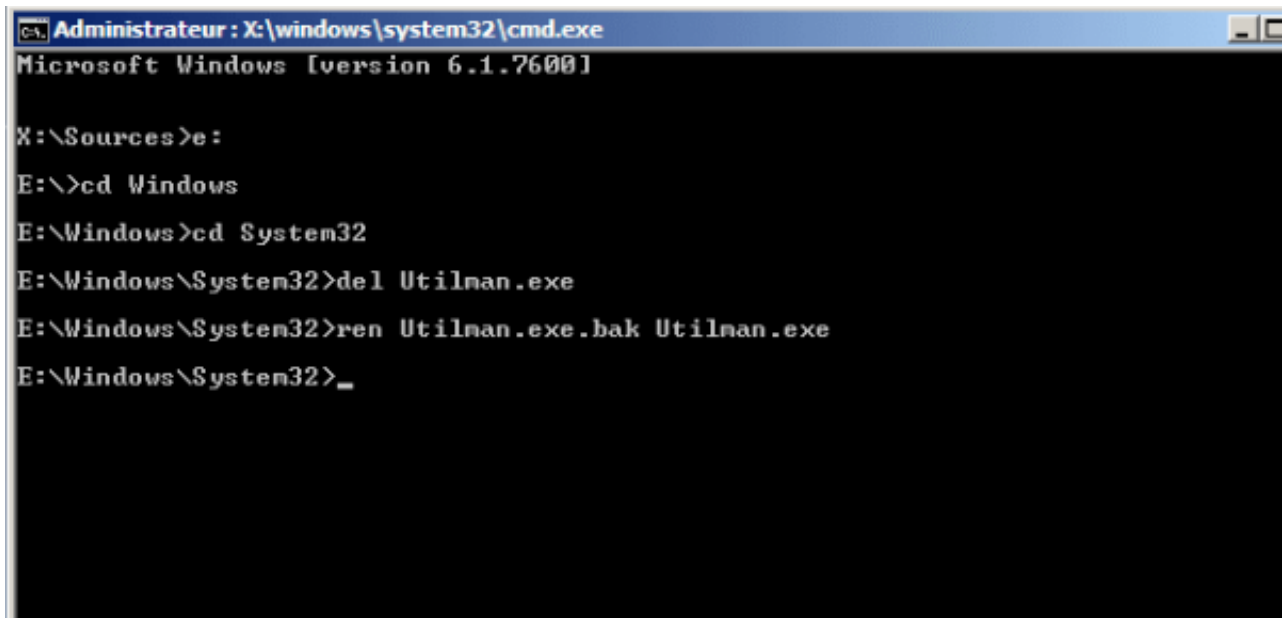
Pour réinitialiser le mot de passe d'un compte utilisateur, il faut taper :

- net user "nom_compte_utilisateur" nouveau_mot_de_passe



redémarrez le PC, pour accéder à la récupération Windows (WinRE),
ouvrir l'invite de commandes puis entrez les commandes :

- cd Windows
- cd System32
- del Utilman.exe
- ren Utilman.exe.bak Utilman.exe



```
Administrateur : X:\windows\system32\cmd.exe
Microsoft Windows [version 6.1.7600]

X:\Sources>e:
E:\>cd Windows
E:\Windows>cd System32
E:\Windows\System32>del Utilman.exe
E:\Windows\System32>ren Utilman.exe.bak Utilman.exe
E:\Windows\System32>_
```

Et voilà ! le compte local est sauvé on a changé le login et le mot de passe que je n'ai pas mis pour des raisons de sécurité.