Annexe technique à l'article du JRES 2005 : « La mémorisation des mots de passe dans les navigateurs web modernes »

Le script suivant permet de créer un utilisateur local dont on choisit le 8ième champ du SID. La valeur choisie pour le 8ième champ du SID est à spécifier dans la variable IdFinal en modifiant le script.

Remarques :
* il faut que la commande psgetsid (http://www.sysinternals.com/utilities/psgetsid.html) soit présente dans le répertoire du script
* la méthode utilisée par le script est très lente (il faut détruire et recréer l'utilisateur pour incrémenter la valeur du SID de 1) ; son exécution peut donc durer plusieurs heures (environ 2h30 pour atteindre 6271 dans mon test)
* si plusieurs comptes ont déjà été créés sur la deuxième machine et que le SID du dernier compte créé est supérieur au SID souhaité, le script ne peut pas fonctionner...
* le compte créé se nomme "comptelocal" et a pour mot de passe "comptelocal"

Le script :

```
''
'' Ce script permet de créer un utilisateur avec un Id prédéfini
''
'' 31/05/2005 FG
''
'' Last modification: "09:08:39 01-06-2005"
''

'' Déclarations de variables
Option Explicit
Dim Nom, Mdp, IdFinal, IdInitial, IdFin, i, oShell, oFSO

'' Initialisations des variables
Nom = "comptelocal"
Mdp = "comptelocal"
IdFinal = 6271


''''''''''''''''''
''
'' Début du code
''
''''''''''''''''''
Set oShell = CreateObject ("WScript.Shell")
```

```
Set oFSO = CreateObject ("Scripting.FileSystemObject")

call creationUtilisateurTemp (Nom, Mdp)

IdInitial = getID (Nom)

Wscript.Echo "Id initial : " & IdInitial

'If IdInitial >= IdFinal Then
'  Exit
'End if

For i = IdInitial To IdFinal - 1
  call creationUtilisateurTemp (Nom, Mdp)
  call destructionUtilisateurTemp (Nom)
  Wscript.Echo "Itération finie : " & i
Next

call creationUtilisateurTemp (Nom, Mdp)

IdFin = getID (Nom)

Wscript.Echo "Id final : " & IdFin


''''''''''''''''''
''
'' Fonctions
''
''''''''''''''''''
Sub creationUtilisateurTemp (Nom, Mdp)
  oShell.Run "%comspec% /c net user " & Nom & " " & Mdp & " /add", 0, True
End Sub

Sub destructionUtilisateurTemp (Nom)
  oShell.Run "%comspec% /c net user " & Nom & " /delete", 0, True
End Sub

Function getID (Nom)
  Dim oShell, oFSO, sTemp, sTempFile, fFile, sResults, tabNb

  Const OpenAsDefault    = -2
  Const FailIfNotExist   =  0
  Const ForReading       =  1

  Set oShell = CreateObject("WScript.Shell")
  Set oFSO = CreateObject("Scripting.FileSystemObject")
  sTemp = oShell.ExpandEnvironmentStrings("%TEMP%")
```

```
  sTempFile = sTemp & "\runresult.tmp"

  oShell.Run "%comspec% /c psgetsid " & Nom & " > " & sTempFile, 0 , True

  Set fFile = oFSO.OpenTextFile (sTempFile, ForReading, _
                                 FailIfNotExist, OpenAsDefault)

  sResults = fFile.ReadLine
  '' On récupère la 2ème ligne
  sResults = fFile.ReadLine
  fFile.Close
  oFSO.DeleteFile (sTempFile)

  tabNb = split (sResults, "-")

  '' C'est le 8eme champ qui nous intéresse
  getID = tabNb (7)
End Function
```