Création d’un script pour recevoir un mail lors qu’un utilisateur bloque son compte.

Tour d’abord il faut pouvoir récupérer les événements ***4740*** dans l’observateur d’événements de la partie Sécurité. Il faut donc activer l’audit sur les comptes des utilisateurs au niveau de la GPO par défaut :

*Graphical user interface, text, application, email

Description automatically generatedComputer Configuration > Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Account Management: Audit User Account Management → Define → Success and Failures*

Il faut ensuite créer le script. Quelques explications s’imposent :

*$secpasswd* est la variable où est stockée le mot de passe dans le format adéquate pour l’objet crédential

$creds est la variable où est stockée le compte mail (ici noreply avec son mdp préparé juste avant)

$Event, variable où l’on récupère le dernier compte bloqué

Les variables suivantes ($User, $Computer, $Domain, $Body, $Subject) formattent correctement le message pour l’envoi SMTP

La boucle Do{} et les conditions Try{}Catch{} servent à envoyer le mail, elles sont nécessaires car il arrive que l’envoi SMTP ne réussisse pas du premier coup.

Il faut ensuite ajouter ce script dans un déclencheur depuis le « Planificateur des taches » windows.

Pour plus de facilité il est nécessaire que ce soit le compte local (NT AUTHORITY\SYSTEM) qui lance le script*. (sécurité ??? à vérifier). Il n’est pas possible de réaliser cette opération via le GUI il faut donc passer par powershell :*

|  |
| --- |
| $Trigger= New-ScheduledTaskTrigger -At 10:00am –Daily  $User= "NT AUTHORITY\SYSTEM"  $Action= New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument "CheminDuScript.ps1"  Register-ScheduledTask -TaskName "NomDeLaTache" -Trigger $Trigger -User $User -Action $Action -RunLevel Highest –Force #Tache avec les droits admin |

Il faut ensuite aller modifier la tache depuis le GUI pour l’ajuster à notre but : ici déclencher la tache lorsqu’un compte se bloque.

Graphical user interface, text, application, email

Description automatically generated

Ici nous n’avons rien à modifier normalement

Graphical user interface, application

Description automatically generated

Au niveau du Déclencheurs, nous devons en mettre un sur un événement de sécurité d’ID 4740 (id pour le blocage de compte).

Sur les actions et les conditions nous n’avons rien à changer.

Il faut mieux arrêter la tache si elle ne s’arrête pas au bout d’une heure. Cela se fait au niveau de l’onglet Paramètres.

Graphical user interface, text, application

Description automatically generated