# Contexte

Dans un environnement Active Directory, un compte de service est généralement utilisé pour exécuter des services ou des applications avec des autorisations spécifiques. Cependant, lorsqu'un compte de service est membre du groupe "Administrateurs de domaine", il présente un risque de sécurité important.

Il convient, au choix, de :

* Retirer de leurs groupes d’administration les comptes de service qui n’ont pas strictement besoin de ces droits.
* Mettre à jour le mot-de-passe des autres comptes de service et activer l’expiration de leurs mots-de-passe.

# Conséquences

Mettre à jour le mot-de-passe des comptes de service permet d’éviter les scénarios suivants :

* **Élévation de privilèges** : Utiliser un compte de service avec des privilèges d'administrateur de domaine permet aux attaquants de s'authentifier comme un utilisateur légitime avec des privilèges élevés, contournant ainsi les contrôles d'accès et les restrictions de sécurité.

## Chaine de cyberattaques

Mettre à jour le mot-de-passe des comptes de service permet d’éviter l’accomplissement des étapes suivantes d’une chaine de cyberattaques :

* **Exploitation** : Compromission initiale des systèmes en exploitant les privilèges des comptes de service pour exécuter des commandes ou scripts.
* **Installation** : Si aucun mécanisme de sécurité ne force le changement de ces mots de passe, la récupération d'un compte privilégié permet à un individu malveillant de conserver ces droits d'accès au domaine sur le long terme.

# Détection

Les commandes PowerShell suivantes permettent de lister les comptes administrateurs avec un mot-de-passe qui n’expire jamais :

#

# Importer le module Active Directory

#  
Import-Module ActiveDirectory

#

# Liste des groupes d’administration en français. À décommenter si le domaine est en français

#

#@("Administrateurs", "Contrôleurs de domaine", "Administrateurs du schema", "Administrateurs de l'entreprise", "Administrateurs du domaine", "Administrateurs de clés", "Opérateurs de compte", "Opérateurs de serveur", "Opérateurs de sauvegarde", "Opérateurs d'impression")

#

# Liste des groupes d’administration en anglais. À commenter si le domaine est en français

#

@("Administrators", "Domain Controllers", "Schema Admins", "Enterprise Admins", "Domain Admins", "Key Admins", "Account Operators", "Server Operators", "Backup Operators", "Print Operators" )

#  
# Initialiser un tableau vide pour stocker les members des groups d’administration

#

$membres = @()  
  
#  
# Parcourir chaque groupe et récupérer les members  
#  
foreach ($groupe in $groupes) {

#

# Ajouter les members du groupe à la liste

#

$membres += Get-ADGroupMember -Identity $groupe | Select-Object SamAccountName, PasswordNeverExpires

}  
  
#  
# Filtrer les membres pour supprimer les doublons  
#

$uniqueMembers = $membres | Sort-Object -Property SamAccountName -Unique

#

# Filtrer les comptes administrateurs du domaine dont le mot de passe n'expire jamais

#

$serviceAccounts = $uniqueMembers | Where-Object { $\_.PasswordNeverExpires -eq $true }

#

# Afficher les résultats

#

$serviceAccounts | Select-Object Name, SamAccountName, PasswordNeverExpires

Les commandes PowerShell ne doivent retourner aucun compte de service.

Documentation :

* <https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html#vuln_dont_expire_priv>

# Correction

## Prérequis

* Avoir un gestionnaire de mots-de-passe (exemple : KeePass) afin de sauvegarder de manière sécurisée le mot-de-passe aléatoire et complexe des comptes de service
* Ajouter le nom des comptes de service à mettre à jour, à la ligne "Liste des comptes de services à mettre à jour", dans les commandes PowerShell suivante

## Procédure

Les commandes PowerShell suivantes permettent de changer, par un mot de passe aléatoire de 24 caractères, le mot de passe des comptes de service listés :

#

# Importer le module Active Directory

#  
Import-Module ActiveDirectory  
  
#

# Liste des comptes de services à mettre à jour

#  
$SamAccountNameList = @(

""

)

#  
# Parcourir chaque utilisateur

#

foreach ($SamAccountName in $SamAccountNameList) {

#

# Définir la taille du mot de passe

#

$length = 24 #caractères

#

# Définir la liste des caractères autorisés

#

$chars = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&\*()-\_=+"

#

# Générer le mot-de-passe aléatoirement

#

$newPassword = -join ((1..$length) | ForEach-Object {

$chars[(Get-Random -Maximum $chars.Length)]

})

#

# Essayer de mettre à jour le mot-de-passe de l’utilisateur

#

try {   
 #

# Rechercher l'utilisateur dans l'AD

#

$user = Get-ADUser -Filter { SamAccountName -eq $SamAccountName }

#

# Mettre à jour le mot de passe de l'utilisateur

#

Set-ADAccountPassword -Identity $user -Reset -NewPassword (ConvertTo-SecureString -AsPlainText $newPassword -Force)

#

# Débloquer le compte utilisateur (en cas de blocage suite à de échecs de connexions répétés) et active l’expiration du mot-de-passe

#

Set-ADUser -Identity $user -PasswordNeverExpires $false -UnlockAccount

#

# Afficher le nom du compte et le mot de passe généré pour pouvoir l’ajouter dans un gestionnaire de mots-de-passe

#

Write-Host "User: $user, new password: $newPassword"

}

#

# En cas d’erreur lors de la mise-à-jour du mot-de-passe

#

catch {

#

# Ecrire dans la console

#

Write-Host "Error: Unable to update the user: $user"

}

}

Les commandes PowerShell ne doivent retourner que la liste des utilisateurs avec le mot-de-passe associé.

# Vérification

Pour vérifier la bonne correction de l’anomalie, il est possible de d’exécuter à nouveau la partie "Détection" et de constater qu’aucun compte utilisateur avec un mot-de-passe qui n’expire jamais n’est listé.