# Contexte

La vulnérabilité d’un mot de passe augmente avec le temps, en même temps que le risque de partage du mot de passe ou de compromission par une attaque par force brute. Pour un compte à privilège, l’impact d’une compromission du mot de passe est d’autant plus important.

Il est conseillé de changer de mot de passe tous les 90 jours. Cela peut être géré par une politique de sécurité de l’Active Directory.

Aucun compte administrateur ne devrait avoir un mot de passe qui n’expire jamais.

# Conséquences

Toutes les tactiques définies par MITRE ATT&CK peuvent être utilisées lors de l’exploitation d’un vieux mot de passe.

## Chaine de cyberattaques

Ne pas avoir de vieux mots de passe aide à éviter les scénarios suivants :

* **Exploitation** : Les anciens mots de passe peuvent être exploités si les mêmes mots de passe ou des mots de passe similaires sont toujours utilisés par la cible. Les attaquants peuvent essayer de se connecter aux systèmes en utilisant ces anciennes informations d'identification. Cela est particulièrement efficace si les utilisateurs ont l'habitude de réutiliser des mots de passe ou d'utiliser des variations prévisibles.
* **Installation** : Si les anciens mots de passe permettent d'accéder à un système, les attaquants peuvent installer des logiciels malveillants ou établir un point d'ancrage dans le réseau de la cible sans avoir besoin d'exploiter des vulnérabilités.
* **Commande et contrôle** : Avec les anciens mots de passe, les attaquants peuvent accéder à des comptes utilisateurs qui leur permettent d'établir des canaux de commande et de contrôle. Par exemple, accéder à des comptes de messagerie peut aider à mettre en place d'autres canaux de communication pour exfiltrer des données ou envoyer de nouveaux courriels de phishing à partir d'une source de confiance.
* **Action sur objectif** : Une fois à l'intérieur du réseau, les anciens mots de passe peuvent être utilisés pour se déplacer latéralement, accéder à des données sensibles, escalader les privilèges ou exécuter d'autres actions pour atteindre les objectifs des attaquants, comme l'exfiltration de données, la perturbation des systèmes ou d'autres compromissions.

# Détection

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

#

# Importe le module PowerShell "Active Directory"

#

Import-Module ActiveDirectory

#  
# Liste les utilisateurs avec un mot de passe qui n’expire jamais  
#

$users = Get-ADUser -Filter {PasswordNeverExpires -eq $true} -Property Name, SamAccountName, PasswordNeverExpires

#

# Affiche la liste des utilisateurs avec un mot de passe qui n’expire jamais

#

$users | Select-Object Name, SamAccountName, PasswordNeverExpires | Format-Table -AutoSize

La liste des comptes utilisateurs avec un mot de passe qui n’expire jamais doit être vide.

# Correction

## Prérequis

* Lorsque l’expiration du mot de passe d’un utilisateur est activé, l’utilisateur sera contraint de changer son mot de passe lorsque l’âge de son mot de passe actuel dépassera l’âge maximum des mots de passe définit dans la politique de mots de passe du domaine. Il faut donc s’assurer que le domaine ait une politique de mots de passe et que celle-ci soit correcte.

## Procédure

Les commandes PowerShell suivantes permettent d’activer l’expiration du mot de passe de tous les utilisateurs avec un mot de passe qui n’expire jamais :

#

# Importe le module PowerShell "Active Directory"

#

Import-Module ActiveDirectory

#  
# Liste les utilisateurs avec un mot de passe qui n’expire jamais  
#

$users = Get-ADUser -Filter {PasswordNeverExpires -eq $true} -Property Name, SamAccountName, PasswordNeverExpires  
  
#

# Pour chaque utilisateur avec un mot de passe qui n’expire jamais

#  
foreach ($user in $users) {  
 #  
 # Essaye d’activer l’expiration du mot de passe de l’utilisateur  
 #  
 try {  
 #  
 # Active l’expiration du mot de passe  
 #

Set-ADUser -Identity $user.SamAccountName -PasswordNeverExpires $false   
 }  
 #

# Si la modification échoue

#

catch {

#

# Écrit un log dans la console

#  
 Write-Host "Failed to update user: $($user.SamAccountName). Error: $\_"   
 }  
}

# 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.