# Contexte

Dans un environnement Active Directory, il est possible d’avoir des comptes utilisateurs qui n’ont pas de mot-de-passe. L’accès à ces comptes utilisateurs n’est alors pas protégé et cela entraine des risques en matière de sécurité informatique.

# Conséquences

Forcer l’utilisation d’un mot-de-passe permet d’éviter les scénarios suivants :

* **Escalade de privilèges** : Les comptes sans mot de passe sont des cibles privilégiées pour l'escalade de privilèges, permettant aux attaquants d'obtenir un accès de niveau administrateur sans résistance.
* **Mouvement latéral** : Les attaquants peuvent utiliser des comptes compromis pour se déplacer latéralement au sein d'un réseau, compromettant ainsi d'autres systèmes.
* **Persistance** : Les comptes sans mot de passe peuvent être utilisés par les attaquants pour maintenir un accès persistant à un environnement compromis.

## Chaine de cyberattaques

Forcer l’utilisation d’un mot-de-passe permet d’éviter l’accomplissement des étapes suivantes d’une chaine de cyberattaques … :

* **Reconnaissance** : Les attaquants effectuent des recherches pour identifier les comptes utilisateurs potentiellement vulnérables, y compris ceux sans mot de passe, au sein d'un réseau cible.
* **Exploitation** : Les attaquants exploitent des vulnérabilités pour accéder à des systèmes. Dans ce contexte, l'exploitation pourrait simplement consister à se connecter à un compte sans mot de passe.

# Détection

Les commandes PowerShell suivantes permettent de lister les comptes utilisateurs dont le mot de passe n’est pas requis :

#  
# Importe le module PowerShell Active Directory  
#

Import-Module ActiveDirectory

#

# Récupère tous les comptes utilisateurs pour lesquels le mot de pass n’est pas requit

#

$noPasswordRequired = Get-ADUser -Filter {PasswordNotRequired -eq $true} -Properties SamAccountName, PasswordNotRequired

#

# Si des comptes sont récupérés  
#

if ($noPasswordRequired) {

#  
 # Affiche les comptes dans la console  
 #

$noPasswordRequired | Select-Object SamAccountName, PasswordNotRequired | Format-Table -AutoSize

}

#

# Si aucun compte n’est récupéré

#

else {  
 #  
 # Écrit un message dans la console  
 #  
 Write-Output "All ActiveDirectory accounts require a password."

}

Les commandes PowerShell ci-dessus doivent retourner le message : "All ActiveDirectory accounts require a password.".

# Correction

## Procédure

Les commandes PowerShell suivantes permettent de forcer les utilisateurs qui n’ont pas de mot-de-passe à en créer un à la prochaine connexion. De plus, il sera impossible de supprimer le mot-de-passe des comptes utilisateurs :

#  
# Importe le module PowerShell Active Directory  
#

Import-Module ActiveDirectory

#

# Récupère tous les comptes utilisateurs pour lesquels le mot de pass n’est pas requit

#

$noPasswordRequired = Get-ADUser -Filter {PasswordNotRequired -eq $true} -Properties SamAccountName, PasswordNotRequired

#

# Si des comptes sont récupérés  
#

if ($noPasswordRequired) {

#  
 # Boucle sur chaque compte  
 #

foreach ($user in $noPasswordRequired) {  
 #  
 # Force l’utilisation d’un mot de passe  
 #

Set-ADUser -Identity $user.SamAccountName -PasswordNotRequired $false -ChangePasswordAtLogon $true

}

}

#

# Si aucun compte n’est récupéré

#

else {  
 #  
 # Écrit un message dans la console  
 #  
 Write-Output "All ActiveDirectory accounts require a password."

}

Documentation :

* <https://learn.microsoft.com/en-us/powershell/module/activedirectory/set-aduser?view=windowsserver2022-ps>

# 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 sans mot de passe requit n’est listé.