# Contexte

Pour accéder à un service à l'aide de Kerberos, un utilisateur demande un ticket (appelé TGS) au contrôleur de domaine spécifique au service. Ce ticket est chiffré à l'aide d'une dérivation du mot de passe du service, mais il peut être découvert par force brute pour récupérer le mot de passe d'origine.

Tout compte ayant l'attribut SPN renseigné est considéré comme un compte de service. Étant donné que n'importe quel utilisateur peut demander un ticket pour un compte de service, ces comptes peuvent avoir leur mot de passe récupéré. De plus, il est connu que les services n'ont pas leur mot de passe modifié régulièrement et utilisent des mots bien connus.

Le chiffrement AES est plus fort que le chiffrement RC4. Configurer les utilisateurs principaux avec SPN pour prendre en charge le chiffrement AES ne permettra pas de contrer des attaques telles que le "Kerberoasting", mais cela force l'utilisation d'AES par défaut, ce qui signifie qu'il est possible de surveiller les attaques de rétrogradation du chiffrement vers RC4 (attaques "Kerberoasting").d

# Conséquences

Activer un algorithme de chiffrement fort aide à prévenir les scénarios suivants :

* **Déplacement latéral** : Les attaquants peuvent se déplacer latéralement au sein du réseau en utilisant des comptes de service compromis. Cela peut les aider à accéder à plus de systèmes et de données, étendant ainsi leur influence au sein de l'organisation.
* **Élévation de privilèges** :
  + **Accès aux comptes de service** : Les attaquants peuvent accéder aux comptes de service, qui ont souvent des privilèges plus élevés que les comptes utilisateurs standard. Ces comptes peuvent avoir des droits administratifs ou accéder à des données et des systèmes sensibles.
  + **Accès à l'administrateur de domaine** : Si un compte de service avec des privilèges d'administrateur de domaine est compromis, l'attaquant peut prendre le contrôle de l'ensemble du domaine Active Directory (AD), menant à une prise de contrôle complète du domaine.
* **Persistance** : L'accès aux comptes de service permet aux attaquants de maintenir une présence persistante dans le réseau, car ces comptes sont moins susceptibles d'être surveillés et souvent utilisés pour des processus automatisés.

## Chaine de cyberattaques

Activer un algorithme de chiffrement fort aide à prévenir l’accomplissement des étapes suivantes d’une chaine de cyberattaques :

* **Installation :** L'accès aux comptes de service permet aux attaquants de maintenir une présence persistante dans le réseau, car ces comptes sont moins susceptibles d'être surveillés et souvent utilisés pour des processus automatisés.
* **Commande et contrôle :** Avec des privilèges élevés, les attaquants peuvent exécuter des commandes malveillantes, installer des logiciels malveillants et manipuler les configurations, compromettant davantage l'intégrité et la sécurité du réseau.
* **Action sur objectif** : Les attaquants peuvent accéder à des données sensibles et les exfiltrer en utilisant les privilèges des comptes de service compromis, entraînant des fuites de données.

# Détection

Le code PowerShell suivant permet de liste les utilisateurs et ordinateurs avec un attribut "SPN", donc considérés comme comptes de service :

#

# Importe le module Active Directory  
#

Import-Module ActiveDirectory

#

# Liste les comptes utilisateurs avec un attribute SPN

#

$userSPNs = Get-ADUser -Filter {ServicePrincipalName -like "\*"} -Property ServicePrincipalName | Where-Object { $\_.ServicePrincipalName -ne $null } | Select-Object Name, SamAccountName, ServicePrincipalName

#

# Liste les ordinateurs avec un attribute SPN   
#

$computerSPNs = Get-ADComputer -Filter {ServicePrincipalName -like "\*"} -Property ServicePrincipalName | Where-Object { $\_.ServicePrincipalName -ne $null } | Select-Object Name, SamAccountName, ServicePrincipalName   
  
#  
# Concatene les deux listes  
#  
$accountsWithSPNs = $userSPNs + $computerSPNs

#

# Affiche la liste sous forme de tableau

#  
if ($accountsWithSPNs) {

$accountsWithSPNs | Format-Table -Property Name, SamAccountName, ServicePrincipalName -AutoSize  
}

Le code PowerShell suivant permet de savoir si l’algorithmes de chiffrement AES est actif pour Kerberos :

#  
# Défini le chemin vers la clé de registre à lire

#  
$registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters"  
  
#  
# Défini le nom de la clé de register à lire  
#

$registryKey = "SupportedEncryptionTypes"  
  
#  
# Récupère la clé de registre  
#  
$registryValue = Get-ItemProperty -Path $registryPath -Name $value -ErrorAction Stop  
  
#  
# Vérifie si les algorithmes AES sont actifs  
#  
$aes128Enabled = ($registryValue -band 0x08) -ne 0  
$aes256Enabled = ($registryValue -band 0x10) -ne 0  
  
#  
# Affiche les résultats

#  
Write-Host "AES 128 Enabled: $aes128Enabled"  
Write-Host "AES 256 Enabled: $aes256Enabled"

# Correction

## Prérequis

* L’ordinateur doit pouvoir être redémarrer pour que les modifications puissent être prises en compte

## Procédure

Le code PowerShell suivant permet d’active AES pour Kerberos :

#

# Défini le chemin vers la clé de register à modifier  
#  
$registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters"   
  
#  
# Défini le nom de la clé de register à modifier  
#

$valueName = "SupportedEncryptionTypes"   
  
#  
# Défini la nouvelle valeur de la clé de registre:  
# - AES 128 (0x08)  
# - AES 256 (0x10)  
# - Les deux (0x18)  
#  
$aesValue = 0x18   
  
#  
# Si le chemin vers la clé de register n’existe pas  
#  
if (-not (Test-Path $registryPath)) {   
 #

# Créer le chemin vers la clé de registre

#  
 New-Item -Path $registryPath -Force

}   
  
#  
# Écrire la nouvelle Valeur de la clé de registre   
#  
Set-ItemProperty -Path $registryPath -Name $valueName -Value $aesValue -Type DWord

L’ordinateur doit être redémarrer pour que les modifications soient prises en compte.

# Vérification

Pour vérifier la bonne correction de l’anomalie, il est possible de d’exécuter à nouveau la partie "Détection" et de constater que les algorithmes AES sont bien actifs pour Kerberos.