# 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 »).

# Conséquences

…:

* …

## Chaine de cyberattaques

… :

* …

# Détection

… :

#

#  
#

...

Documentation :

* …

# Correction

## Prérequis

* …

Documentation :

* …

## Procédure

… :

#

#

#

… :

#

#  
#

… :

#

#   
#

Documentation :

* …

# Vérification

…