# Utilisation de Kerberos avec un chiffrement faible

ID METSYS : 4  
ID PingCastle : [S-DesEnabled](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [User accounts that use DES encryption](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln2\_kerberos\_properties\_deskey](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#kerberos_properties_deskey)

Charge de travail : 0.5 jour  
Difficulté : 2 - Requière quelques connaissances sur l'infrastructure et l'anomalie qu'elle contient

****Description****

DES est un algorithme très faible et une fois attribué à un compte, il peut être utilisé dans les demandes de tickets Kerberos, même s'il est facilement cracké. Si l'attaquant cracke le ticket Kerberos, il peut voler le jeton et compromettre le compte utilisateur.

****Recommandation****

Il est recommandé de désactiver DES en tant qu'algorithme de chiffrement dans la boîte de dialogue de configuration utilisateur ou dans l'attribut « msDSSupportedEncryptionTypes » au niveau LDAP. Il doit être désactivé dans les propriétés d'un compte en décochant la case « Utiliser le chiffrement Kerberos DES pour ce compte ». Vous pouvez également détecter quels comptes prennent en charge le chiffrement Kerberos DES en exécutant :

Get-ADObject -Filter {UserAccountControl -band 0x200000 -or msDs-supportedEncryptionTypes -band 3}