# Signature requise pour LDAP

ID METSYS : 38  
ID PingCastle : [A-DCLdapSign](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)

Charge de travail : 2 jours  
Difficulté : 4 - Requière des connaissances avancées sur l'infrastructure et de l'anomalie qu'elle contient

****Description****

Si la demande de signature de chaque requête LDAP n'est pas appliquée, une attaque de l'homme du milieu peut être effectuée sur une connexion LDAP. Par exemple, pour ajouter un utilisateur au groupe d'administrateurs.

Ce test est réalisé en ignorant les stratégies de sécurité locales de l'ordinateur. L'application de la signature est effectuée en définissant le drapeau « ISC\_REQ\_INTEGRITY » lors de l'initialisation de l'authentification Négociation / NTLM / Kerberos.

Le test inverse est réalisé avec le drapeau ISC\_REQ\_NO\_INTEGRITY défini.

****Recommandation****

Vous devez vous assurer que TOUS les clients LDAP sont compatibles avec la signature LDAP. Toutes les versions de Windows depuis XP prennent en charge cela, ainsi que la plupart des clients Unix.