

Sécurité Windows : récupérer les hash des mots de passe des comptes AD

Présentation

L'attaque informatique **AS-Rep Roasting** consiste à exploiter une vulnérabilité d'Active Directory pour voler les hachages de mots de passe des utilisateurs qui ont la pré-authentification Kerberos désactivée.

Les hachages volés peuvent ensuite être utilisés pour tenter de deviner les mots de passe des utilisateurs hors ligne.

Cette technique est appelée AS-REP Roasting. Les attaquants peuvent utiliser l'outil Rubeus pour effectuer cette attaque¹. Il est recommandé de désactiver la pré-authentification Kerberos pour les comptes d'utilisateurs qui n'en ont pas besoin¹.

Lien :

- <https://openclassrooms.com/fr/courses/7723396-assurez-la-securite-de-votre-active-directory-et-de-vos-domaines-windows/7953376-effectuez-un-mouvement-lateral-avec-le-protocole-kerberos>
- <https://beta.hackndo.com/kerberos-asrep-roasting/>

From:

/ - Les cours du BTS SIO

Permanent link:

</doku.php/reseau/windows/aspreproastable?rev=1704894704>

Last update: 2024/01/10 14:51

