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 pourvoler 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.

Outils possible pour récupérer les hashs de mots de passe :

- **Rubeus** ;
- **GetNPUsers.py** de la suite Impacket.

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/

Sauvegarde de l'annuaire LDAP

L'outil **ldap2json** permet d'obtenir une sauvegarde du contenu de l'annuaire au format **json** avec un avec un compte utilisateur sans privilèges particuliers.

> Utiliser l'outil **ldap2json** de **p0dalirius** (disponible dans Github) pour obtenir une sauvegarde locale de l'annuaire AD de votre contexte.

https://www.it-connect.fr/active-directory-et-lattribut-useraccountcontrol/

Recherche des comptes dont la pré-authentification Kerberos est désactivée

La consultation de la propriété **UserAccountControl** des comptes permet de savoir si la pré-authentification Kerberos est désactivée.

Lien : https://www.it-connect.fr/active-directory-et-lattribut-useraccountcontrol/

> Recherchez dans la sauvegarde de l'annuaire ldap, les comptes dont pré-authentification Kerberos est désactivée.

Récupération des hash des mots de passe avec GetNPUsers.py

- Python3 et pip3 doivent être installés sur le PC ;
- Installez ensuite les modules de **impacket** :

```
apt install python3 python3-pip
python3 -m pip3 install impacket
```

Lien :

- https://github.com/fortra/impacket/blob/master/examples/GetUserSPNs.py
- https://tools.thehacker.recipes/impacket/examples/getuserspns.py

Trouver le mot de passe

Après avoir récupéré le hash du mot de passe, une tentative en brute force permet de trouver le mot de passe avec des outils comme **John**

The Ripper ou **Hashcat**.

Lien : https://www.tarlogic.com/blog/how-to-attack-kerberos/