

Liste des applications installées

- Objectif : identifier des applications vulnérables
- S'intéresser à la version installée
 - Permettra l'exécution d'exploits locaux
- En mode graphique
 - Ajout/Suppression de programmes
 - `regedit` et afficher la ruche `HKLM\SOFTWARE`
- En ligne de commande
 - `c:\> reg query HKLM\SOFTWARE`

Liste des process et services

- Objectif : identifier des processus « hostiles » (pare-feu, antivirus), les services vulnérables, prévoir la pérennisation de l'accès
- En mode graphique
 - Possible mais à éviter si possible
- En ligne de commande
 - Tasklist (taskkill), sc (cf. aussi schtasks)