Récupération des accréditations

- Récupération locale
  - Des empreintes
    - Dans la base SAM
    - Dans la mémoire
  - Des données d’authentification en cache
  - Des mots de passe dans la mémoire
- Récupération à distance

Récupération locale des empreintes

- Dans la base SAM
- Outils
  - Metasploit
    - meterpreter> run hashdump
  - PwdumpX 1.4
    - c:\> PwdumpX –ph <cible> <identifiant> <mot_de_passe>
    - L'identifiant et le mot de passe peuvent être remplacés par « + + » pour utiliser les accréditations de l'utilisateur qui exécute le programme
  - Fgdump
    - c:\> fgdump –c –h <cible> -u <identifiant> -p <mot_de_passe>
  - Wce (windows credentials editor)
  - Cain
    - Onglet Cracker
    - Clic gauche « Add to list »