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 »

Récupération locale des empreintes

- Dans la mémoire
  - `Metasploit`
    - `meterpreter> use incognito`
    - `meterpreter> list_tokens -u`
    - `meterpreter> impersonate token <DOMAIN\username>`
  - `wce`
  - `PSH Toolkit` de Core Security (<Seven et 2K08)
    - `whosthere` permet de lister les sessions de connexion présentes en mémoire
      - `whosthere.exe` ou `whosthere-alt.exe`
  - `MSVCTL` (<Seven et 2K08)