# 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>`

# Récupération locale des mots de passe

- Dans la mémoire
- Outils
  - `Wce`
  - `Mimikatz`
  - `CachedPasswordDumper` (pour Windows XP SP1 et 2003 SP0
    - cpd
  - `PasswordReminder` (avant Windows XP)
  - `FindPass` (avant Windows XP)
    - `c:\ Findpass <nom_de_domaine> <identifiant> <PID_de_winlogon.exe>`
    - Le `PID` peut être obtenu avec `pslist` (`pstools` de systinternals)