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)

Récupération à distance

- Directement par le réseau
- Outils
  - `psexec, meterpreter` et `hasdump`
  - `fgdump` ou `pwdump`
  - `Cain & Abel` (méthode employée sous Windows)
    - Onglet Network
    - Clic droit sur Quick List : Add to Quick List
    - Clic droit sur l'adresse de la machine : Connect As
    - Clic droit sur Services : Install Abel
    - Double clic sur l'adresse de la machine
    - Abel\Hashes
      - L'historique des empreintes est affichée