Récupération d'informations locales

- Si un poste client est accessible ou rendu accessible …
- Les informations à récupérer
  - Liste des utilisateurs locaux
  - Appartenance des utilisateurs aux groupes privilégiés
  - Appartenance de la machine à un domaine
  - Liste des applications installées
  - Droits sur les fichiers locaux
  - Cache netbios
  - Liste des derniers documents ouverts
  - Liste des process et services actifs
  - Si possible extraits des registres

Informations sur les comptes

- Première étape de l'attaque sur les moyens d'authentification
- Lister les utilisateurs
  - `net user; net user /domain`
- Obtenir des informations individuelles sur les utilisateurs
  - `net user <login_utilisateur>`
- Lister les groupes locaux
  - `net localgroup`
- Lister les groupes du domaine
  - `net group`
- Identifier les membres d'un groupe
  - `net localgroup <nom_du_groupe>` ou `net group <nom_du_groupe>`