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>`

Manipulation des comptes

- Après avoir obtenu des droits élevés
- Il est possible de
  - Créer un utilisateur
    - `c:\> net user <login utilisateur> /add`
  - Ajouter un utilisateur dans un groupe
    - Pour le domaine local
      - `c:\net localgroup <nom_du_group> <login_utilisateur> /add`
    - Dans le domaine AD DS
      - `c:\net group <nom_du_group> <login_utilisateur> /add`