Objectifs

- Prise de contrôle d'une machine ou d'un domaine
- Techniques ?
  - Élévation des privilèges
- Vers les privilèges d'administration locale
  - Sur une machine isolée : poste client ou serveur
- Vers les privilèges d'administration du domaine
  - Sur un contrôleur de domaine

Techniques

- Découvrir le mot de passe d'un administrateur
- Obtenir l'empreinte d'un compte privilégié
- Exploiter une vulnérabilité pour obtenir un accès privilégié
  - Par exemple, une invite de commande exécutée avec les droits d'un administrateur ou de l'identité LOCAL SYSTEM
- Créer un compte et l'ajouter au groupe des administrateurs locaux ou du domaine