Accès authentifié

- Objectifs
  - Récupérer des informations fournies par des interfaces Windows avec un compte légitime du domaine
- Les informations à récupérer
  - Liste des sites, réseaux…
  - Liste des utilisateurs du domaine
  - Appartenance des utilisateurs aux groupes privilégiés
  - …
- Outils d'administration
  - `rpcclient`
  - `Cain & Abel`
  - `Clients WMI`
    - WMI offre un mécanisme de gestion à distance d'un système d'exploitation ou des composants installés
      - `Wmic /node:[TargetIPaddr] /user:[User] /password:[Passwd] process list full`
    - `wbemtest`
  - `Dsquery` (cible l'annuaire Active Directory)

Partage réseau : principes

- Partages de fichiers
- Transport sur TCP via le protocole SMB (445/TCP)
- Authentification
  - Utilise les protocoles d'authentification classiques disponibles sous Windows et sélectionnées par le `SSP Negociate`
    - NTLM ou Kerberos, le plus souvent
- Outils
  - Pour lister les partages SMB
    - `rpcclient` et la commande `netshareenum`
    - `rpcclient-tng` et la commande `share list`
  - `smbclient` pour y accéder
    - `%smbclient -U <identifiant> \\\\<cible>\\<partage>`