Récupération d'informations à distance

Sessions nulles

- Principe, déroulement et tubes nommés
  - Possibilité de connexion sans login/password
    - utilisées lorsqu'une machine cherche à accéder aux informations d'une autre machine sans faire partie de son domaine ou de son groupe de travail.
  - Transport sur SMB
    - Port `139/TCP` (via `TCP sur NetBIOS`)
    - Port `445/TCP` (directement en TCP)
- Accès et configuration
  - Récupération des comptes, groupes, partages …
- Outils
  - `Cain, rpcclient`
- L’accès anonyme aux tubes nommés est interdit depuis Windows XP SP2 et 2003