Le service de noms NETBIOS

- Service utilisé par défaut en environnement Windows
- Permet l'identification des machines
- Utilise le port `137/UDP`
- Fournit des informations sur le rôle des systèmes

- Outils `nbtstat`
  - `c:\> nbtstat -a <nom_de_la_machine>`
  - `c:\> nbtstat -A <adresse_ip_de_la_machine>`
- Accès au cache Netbios
  - `c:\> nbtstat -c`
- Sous linux, il existe `nbtscan`
  - `$ nbtscan -v <adresse_ip_de_la_machine>`

Le service de noms NETBIOS

- Informations intéressantes obtenues
  - Nom de la machine, Domaine, Utilisateur authentifié
  - Adresse MAC de la machine
  - Certains services démarrés :
    - <00> : service Workstation
    - <03> : service Messenger
    - <20> : service Server
  - Rôle
    - <1C> : Contrôleur de domaine
    - <Inet~Services> : Serveur IIS
    - <22>, <23>, <24>,<87>,<6A> : Serveur Exchange
  - Référence : http://support.microsoft.com/kb/163409