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

Liste des applications installées

- Objectif : identifier des applications vulnérables
- S'intéresser à la version installée
  - Permettra l'exécution d'exploits locaux
- En mode graphique
  - Ajout/Suppression de programmes
  - `regedit` et afficher la ruche `HKLM\SOFWARE`
- En ligne de commande
  - `c:\> reg query HKLM\SOFTWARE`