Identification des services en écoute

- Services classiques hébergés par des serveurs Windows
  - Serveur WINS – `42/TCP`
  - Serveur DNS – `53/UDP`
  - Serveur HTTP – `80/TCP et/ou 81/TCP`
  - Serveur HTTPS – `443/TCP`
  - Mandataire HTTP – `8080/TCP`
  - KDC Kerberos – `88/UDP`
  - Serveur LDAP – `389/TCP (et LDAPSSL – 636/TCP)`
  - Serveur RDP – `3389/TCP`
  - Serveur VNC – `5900/TCP`
- `88/UDP et 389/TCP` == AD DS (contrôleur de domaine)

Récupération d'informations à distance