Par quelle machine commencer ?

- Identification des machines intéressantes
  - nmap (éventuellement hping) et metasploit
- Quelles sont-elles ?
  - Les contrôleurs de domaine
  - Les serveurs d'application
  - Les postes clients
- Nécessité d'effectuer une classification des machines découvertes
- La source d'information principale
  - Les services en écoute sur le réseau

Protocoles réseaux natifs Windows

- NBT
  - Encapsulation de Netbios sur TCP/IP
- SMB / CIFS (Partage de fichiers)
- MS RPC (Communication interprocess)
  - Protocole d’appel de fonctions et d’échange de données entre processus locaux ou distants