Services SUN-RPC

- Mécanisme de communication inter processus développé par SUN
- Utilisé pour de nombreux protocoles, dont NFS, NIS et autres
- Services RPC d'un machine est répertoriés dans le service portmapper (TCP/111)
- Interrogation du portmapper par « `rpcinfo -p cible` »
- Services intéressants
  - `NFS`
  - `Statd`
  - `Sadmind`
  - `RUSERS`

NFS : Network File System

- Système de fichier par réseau utilisant les RPC
- Les versions 1 et 2 sont non sécurisées, prévues pour fonctionner en UDP
- La version 3 est étendue pour prendre en charge TCP
- La version 4 est non utilisée mais sécurisée

- Plus de 100 vulnérabilités sous *Secunia* pour NFS
- Erreurs classiques
  - Répertoire partagé en lecture / écriture
  - Partagé sans restriction (pas de `root_squash`, `nosuid nodev`),
    (L'option **no_root_squash** spécifie que le root de la machine sur laquelle le répertoire est monté a les droits de root sur le répertoire)
  - Les clients ne sont pas identifiés correctement
    - Pas de FQDN, IP non fixe …