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 …

NFS : Network File System

- Mécanisme d'autorisation par adresse IP puis par UID utilisateur
- Exportation NFS d'un répertoire donné (Solaris)
  - `share -F nfs -o rw /repertoire/a/exporter`
- Découverte de NFS sur une machine distante
  - `rpcinfo -p cible`
- Listage des répertoires exportés en NFS
  - `showmount -e cible`
- metasploit
  - `Auxiliary/scanner/nfs/nfsmount`
- Listage des répertoires montés en NFS sur machine locale
  - `showmount`
- Montage d'un répertoire NFS sur un point local
  - `mount -t nfs cible:/répertoire/exporté /destination/du/montage`
  - `nfsmount cible:/répertoire/exporté /destination/du/montage`