Surface d’attaque

- Lorsqu’un attaquant possède un accès local non-privilégié à une machine :
  - Beaucoup de programmes s’exécutant avec les droits root ;
  - Beaucoup de fichiers intéressants en lecture pour tous les utilisateurs ;
  - Peu de restrictions sur les programmes exécutables par les utilisateurs.

⇒ plein de possibilités pour augmenter ses privilèges

rsh/rlogin/rcp

- Programmes de la série des r*-utils
  - Permettent de réaliser des actions à distance
- Authentification basée sur des relations de confiance
  - Fichier `.rhosts` dans le $HOME des utilisateurs
  - Fichier `/etc/hosts.equiv` pour l'ensemble des comptes locaux
  - Contiennent la liste des adresses IP autorisées à se connecter
  - « + + » pour autoriser n'importe qui
- Souvent confiance accordée entre serveurs
  - « pour des raisons de pratique »
  - Backup, partage d'informations …
  - Permet très régulièrement de rebondir entre les serveurs !