Les logs

- Examen des logs très utile pour déterminer les adresses de connexion des administrateurs ou autres utilisateurs
- Dans les logs, nous trouvons parfois d'autres informations intéressantes :
  - Mots de passe tapés à la place du login dans session telnet => mot de passe enregistré dans logs
- Nettoyage des logs possible dans le cas d'une discrétion nécessaire
- Logs Unix gérés par daemon `SYSLOG`
- Logs textuels, emplacement défini par fichier de configuration `/etc/syslog.conf`
  - Linux : `/var/log`
  - Solaris : `/var/adm, /var/log`
- Possibilité d'envoyer les logs sur machine distante dite `LOGHOST` par protocole `SYSLOG`
  - Examen de `/etc/hosts` pour voir si machine `loghost` existante

Délégation de droits

- Délégation de root sans donner son mot de passe
  - `CALIFE` : Donne un shell root uniquement
  - `SUDO` : très paramétrable (`/etc/sudoers`), donne seulement
    - Certaines commandes
    - Certains paramètres
    - Certains groupes …
- `sudo -l` : liste les commandes autorisées pour l'utilisateur connecté
- `sudo -s` : lance un shell