Crontab

- Tâches périodiques (`cron`) et différées (`at`)
- Vérifier les mécanismes d'autorisation (`cron.allow` et `cron.deny`) rarement utilisés
- absence de cron utilisateurs (`/var/spool/cron/` ou `crontab -l -u user`)
- pertinence des crons systèmes : dérouler la pelote commençant à `/etc/crontab`
- permissions sur les fichiers exécutés par `cron`

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