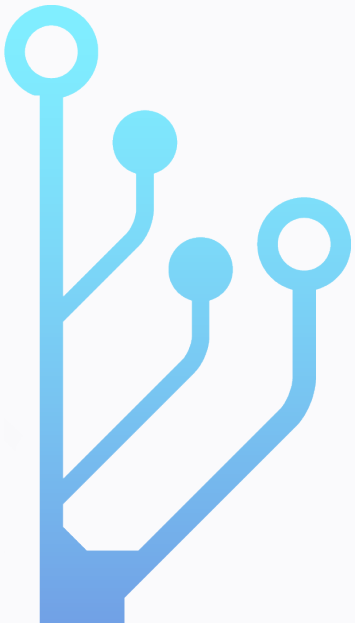
Machines d'asso/Perso

ViaRézo

1er février 2023

Éléments de base



Les bonnes pratiques

- Désactiver la connexion par ssh par mot de passe (en particulier si on vient de vous passassionner une machine, pensez à le vérifier). **C'est le plus important dans ce document, faites le SVP, ça a été la cause principale de toutes les infections de machines durant les deux dernières années.** (Et c'est pas parce que vous l'utilisez pas qu'il est désactivé.)
- Tenir la machine à jour.
- Installer `fail2ban` et `unattended-upgrades`.
- Faire en sorte que seuls ceux qui ont nécessité d'accéder à la machine y accèdent
- Ne pas hésiter à venir nous parler, sur le chan VP Geek ou en MP, on est là pour ça.

Créer une clé ssh

On vous conseille de générer une clé ssh elliptique (du type `ed25519`).
Pour ce faire :

- Ouvrez un terminal
- Tapez `ssh-keygen -t ed25519`
- Laissez l'emplacement par défaut (appuyez sur entrée sans rentrer de chemin)
- Entrez un mot de passe pour chiffrer votre clé privée

Mettre à jour sa machine

Pensez à le faire régulièrement, ça prend 2mn et ça évite pas mal de galères ;)

- tapez `sudo apt update`
- puis `sudo apt upgrade`

Vérifier qu'un programme est installé

Parce que c'est cool de savoir ce qui est installé sur sa machine

- `apt list *nom_du_programme*`

Vérifier qu'un programme tourne

Parce que c'est cool de savoir ce qui tourne sur sa machine

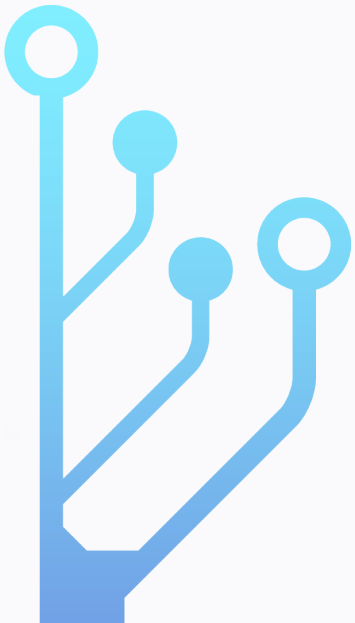
- `sudo systemctl status *nom\_du\_programme*`

Désactiver le SSH par mot de passe

Faites le SVP, c'est vraiment le plus important. On s'est déjà fait hacker 3 machines comme ça en 3 mois. Et en plus c'est vraiment rapide ;)

- Vérifiez que vous avez bien votre clé ssh dans la machine (ça serait dommage de plus y avoir accès). (voir à la fin Passationner).
- `tapez sudo nano /etc/ssh/sshd_config`
- recherchez la ligne avec marqué `PasswordAuthentication`
- enlevez le # devant s'il y en a un
- remplacez le "yes" par "no" si c'est pas déjà fait
- `Ctrl+X, Y` pour valider
- Un petit `sudo systemctl restart ssh.service` et bim c'est terminé !

Installations importantes



Installer fail2ban

Pour éviter de se faire spammer sur le port 22 :

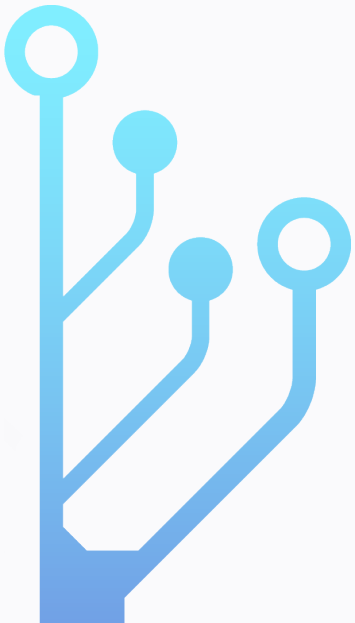
- `sudo apt install fail2ban`
- puis `sudo systemctl status fail2ban`
  - Si il y a un point vert, génial ça marche !
  - Sinon, tapez `sudo systemctl restart fail2ban` et attendez un peu avant de retaper `sudo systemctl status fail2ban`

Installer unattended-upgrades

Ce programme fait automatiquement les mises à jour de sécurité.
Pour l'installation : Tout pareil.

- `sudo apt install unattended upgrades`
- puis `sudo systemctl status unattended-upgrades`
  - Si il y a un point vert, génial ça marche !
  - Sinon, tapez `sudo systemctl restart unattended-upgrades` et attendez un peu avant de retaper
    `sudo systemctl status unattended-upgrades`

Passationer



Mettre une nouvelle clé ssh sur la machine

Si votre machine sort de ViaRézo, on a mis votre clé dessus vous n'avez rien à faire, mais si vous voulez passassionner cette machine ou juste vous y connecter depuis un autre pc, il faudra ajouter la nouvelle clé ssh.

- Dans votre pc allez dans le dossier .ssh (à la racine si jamais vous n'avez pas rentré de chemin lors de la génération de clé ssh) ex : `C:/Users/**Votre_User**/.ssh`
- Dans un bloc note, ouvrez le fichier .pub qui s'y trouve (Attention, l'autre fichier portant le même nom contient votre clé privée !)
- Copiez le contenu de ce fichier (tout, même le type de clé et le nom à la fin)
- Dans la machine vituelle, tapez `nano ~/.ssh/authorized_keys`
- Ajoutez une ligne contenant votre clé
- (Pensez à enlever les vieilles clés des gens qui n'ont plus besoin de l'accès)