Petits comptes entre ami·es

Un compte pour soi-même

1. Rejouez les manipulations faites en cours (permettant d'identifier les fichiers en jeu dans la création d'un user) et créez votre compte utilisateur (avec votre prénom) sur votre conteneur. Idéalement en même temps que le cours.

S'inviter sur les conteneurs

2. Choisissez quelques (2 ou 3) personnes à inviter sur votre conteneur, et assurez-vous que tout le monde a reçu au moins une invitation (pour pouvoir tester les deux rôles). Si votre groupe de "projet" est déjà constitué, vous pouvez choisir vos invité·es dans ce groupe. Commencez par inviter une seule personne.
3. Sur votre conteneur, créez un compte pour votre invité·e, sans privilège particulier.
   - Ce compte ne doit pas avoir de mots de passe. L'authentification se fera par clef SSH.
   - Ce compte ne doit pas avoir d'information "gecos/finger" autres que celles explicitement fournies par votre invité·e dans ce but. Ne trahissez pas votre invité·e.

Pour permettre à votre invité·e de se connecter à votre conteneur, il va falloir ajouter sa clef publique SSH dans le fichier `.ssh/authorized_keys` de son `HOME`. Remémorez-vous les emplacements des diverses clefs SSH côté client et côté serveur en relisant le feuille « Arborescence des fichiers relatifs à SSH ».

4. Demandez à votre futur·e invité·e de vous envoyer sa clef publique SSH par mail en utilisant son adresse universitaire.

Comment être sur·e que vous avez bien reçu la bonne clef ? On va supposer que le service informatique de Paris 13 n'est pas digne de confiance, et que toute information partagée par mail ou sur mattermost aurait pu être modifiée à la volée.

Ainsi, puisque les clefs publiques ont circulé par mail, il faut vérifier qu'elles ont bien transité sans avoir été modifiées en utilisant un autre canal de communication. Pour vérifier l'intégrité d'une clef de chiffrement, on peut utiliser son fingerprint (fr: empreinte digitale) qui n'est autre que son hash (fr: "condensat"), plus court à vérifier.

Note importante : idéalement, les fingerprints sont échangés lors d'une rencontre physique.

En cas de confinement : Si vous ne pouvez pas vous rencontrer physiquement pour échanger les fingerprints des diverses clefs, on va limiter les risques d'interception en faisant circuler la clef publique et son fingerprint par des canaux différents, gérés par des entités différentes, par exemple le système de visio https://jitsi.lipn.univ-paris13.fr/ (qui est géré par le lipn et pas par la DSI de l'université).

Pour obtenir le fingerprint d'une clef publique SSH, il suffit d'utiliser la commande :

```
$ ssh-keygen -l -f <chemin_vers_la_clef_publique>
```

5. Demandez à votre invité·e de vous fournir le fingerprint de sa clef publique SSH, soit sur un papier si vous êtes physiquement proches, soit via jitsi si vous êtes en distanciel.
6. Vérifiez que la clef de votre invité·e reçue par mail correspond bien au fingerprint échangé directement.
7. Ajoutez la clef SSH dans le fichier `.ssh/authorized_keys` du `HOME` de votre invité·e.

8. Faites en sorte que le répertoire `.ssh/` et le fichier `.ssh/authorized_keys` de votre invité·e lui appartiennent (`chown`) et que personne d'autre qu'elle ne peut y accéder (`chmod`).

Lorsque votre invité·e va se connecter à votre conteneur, il se pourrait qu'une machine malveillante qui se trouve sur la route entre la machine locale de votre invité·e et votre conteneur et se fasse passer pour votre conteneur.

Il faut donc que votre invité·e puisse vérifier que sa machine personnelle se connecte bien à votre conteneur (et pas un fake). Pour cela, il faut lui faire parvenir le fingerprint des clefs publiques du serveur SSH de votre conteneur qu'il·les devront vérifier. Les paires de clefs du serveur SSH se trouvent dans le répertoire `/etc/ssh/` et leur nom est de la forme `ssh_host-*.pub`.

Remarque : plusieurs algorithmes cryptographiques sont proposés par le serveur SSH de votre conteneur pour permettre aux clients SSH de différentes générations d'authentifier le serveur, selon les cryptos disponibles. Il y a donc plusieurs paires de clefs correspondant à ces différents algorithmes cryptographiques (actuellement RSA, ECDSA, ED25519).

Remarque : une incantation permettant d'obtenir d'un seul coup les fingerprints de toutes les clefs publiques d'un serveur SSH se trouve dans le grimoire des cultes du cargo. Vous pouvez l'invoquer pour gagner du temps, mais vous devez avoir conscience que vous exécutez une commande qui n'est pas sous votre contrôle. Si vous ne voulez pas tomber du côté obscur de la dépendance aux formules incompréhensibles (et potentiellement dangereuses), il vous faudra faire quelques `man`, en particuler comprendre le paragraphe "Substitution de processus" du manuel de `bash` (l'un des manuels les plus difficiles d'accès).

Note importante : le contenu des clefs privées du serveur SSH de votre conteneur ne doivent jamais être montrées (si vous voulez voir à quoi elles ressemblent, faites ça depuis chez vous, dos au mur).

9. Envoyez par mail à votre invité·e, l'adresse IPv6 de votre conteneur ainsi que le fingerprint des clefs publiques du serveur SSH de votre conteneur (comme l'enseignant·e l'avait fait avec vous quand il vous a attribué un conteneur), et invitez-les à se connecter à votre conteneur en leur demandant de vérifier le fingerprint d'une clef publique du serveur SSH de votre conteneur lors de la première connexion (avec un mail similaire à celui que vous avez reçu lors de la création de votre conteneur).
10. Une fois que tout le monde dans votre groupe a invité et été invité·e au moins une fois, vous pouvez inviter d'autres personnes de votre groupe.
11. Lorsque vous avez la confirmation que vos invité·es ont réussi à se connecter à votre conteneur, observez les logs de connexion (`/var/log/auth.log`), ainsi que le résultat des commandes `last`, `who` et `ps aux`.
12. En tant qu'user `root`, avec la commande `wall` vous pouvez envoyer un message à l'ensemble des personnes connectées sur votre conteneur. C'est très utile pour demander à tout le monde de se déconnecter avant une opération de maintenance par exemple. Si un user non-privilégié fait la même chose, sur quels terminaux sera affiché le message ? (indication : faites un `ls -l /dev/pts/` avec plusieurs personnes connectées plusieurs fois sur votre conteneur et expérimentez en changeant les permissions, les groupes, de ces périphériques caractères correspondant aux terminaux virtuels ouverts).

Vous pouvez ajouter `invite` à vos tags lorsque toutes les conditions suivantes sont réunies :

- vous avez invité une personne,
- cette personne a réussi à se connecter à votre conteneur,
- vous avez été invité·e par une personne,
- vous avez réussi à vous connecter à son conteneur.

Objectifs du TP :

- objectifs opérationnels du TP :
  - pouvoir travailler à plusieurs sur un même conteneur (potentiellement utile pour l'UE "projet" si celle-ci comporte une partie sur les conteneurs).
- objectifs pédagogiques du TP :

- se familiariser avec les notions d'user et de permissions vues en cours en les utilisant dans un cas réel.
- manipuler des paires de clefs cryptographiques pour mieux comprendre le rôle de chaque clef (et leurs fingerprints).