Se connecter sur son conteneur depuis les machines de salle TP

Note : les objectifs opérationnels et pédagogiques de ce TP sont décrits en bas de la page.

Ce TP doit obligatoirement être fait avant le partiel de TP noté (cf rendu 1).

Contexte

- votre conteneur a une adresse IPv6 publique, les machines de salle TP ont un accès (NATé) à l'internet IPv6. Il n'y aura donc aucune difficulté au niveau de la couche réseau (pas de contournement à faire) car les machines de salle TP peuvent se connecter directement aux conteneurs.
- mais pour l'instant, seul votre user personnel sur votre machine personnelle peut s'authentifier auprès du serveur SSH de votre conteneur grâce à sa paire de clefs SSH.
- on aimerait pouvoir se connecter aux conteneurs depuis les machines de salle TP.
- une **très mauvaise idée** serait de recopier votre clef privée depuis votre ordinateur personnel vers les machines de salle TP. En effet, cette clef privée vous identifie sur votre machine personnelle, elle ne doit donc **jamais** quitter son emplacement. Voir aussi le paragraphe « Warning de sécurité » plus bas.
- vous allez plutôt générer une autre paire de clefs SSH sur les machines de salle TP et copier la clef publique sur votre conteneur. Ainsi, il y aura 2 authentifications différentes sur votre conteneur, et il sera plus facile d'en désactiver une sans toucher l'autre par la suite.

Stratégie

Nous allons utiliser la commande `scp` qui utilise le protocole `SSH` pour copier des fichiers d'une machine à une autre.

Le protocole SSH est un protocole client-serveur, donc fondamentelement disymmétrique : il est souvent possible de se connecter d'une machine A vers une machine B mais pas d'une machine B vers une machine A. Pour représenter ce genre de relations, il est classique d'utiliser un *graphé orienté*, c'est à dire un ensemble de sommets et des flèches qui relient certais couples de sommets.

1. Dessinez le graphe orienté dont les quatre sommets sont votre machine personelle, sercalssh, une machine de salle TP et votre conteneur, et dont les arêtes représentent les connexions SSH possibles (mettez une arête d'une machine A vers une machine B si votre user sur la machine A peut se connecter à votre user sur la machine B par SSH).
2. Établissez une stratégie pour copier la clef publique générée sur une machine de salle TP vers votre conteneur. Notez que scp peut copier des fichiers dans les 2 sens à travers une connexion SSH.

Action

3. Générez une paire de clefs SSH depuis une machine de salle TP, et chiffrez-là avec un mot de passe (voir plus bas pour la motivation).
4. Copiez la clef publique dans le répertoire `/tmp/` de votre conteneur sur en suivant votre stratégie.
   - **ATTENTION :** ne copiez pas la clef publique directement vers sa destination finale car vous risquez d'écraser la clef publique qui vous identifie sur votre machine personnelle.

5. Ajoutez le clef publique au trousseau des clefs autorisées pour l'user `root` de votre conteneur sans écraser la clef existante qui permet de vous authentifier depuis votre machine personnelle. Pensez par exemple à utiliser la redirection `>>`. Si vous ne savez pas quel est ce fichier, reportez-vous à la feuille du cours « Arborescence des fichiers relatifs à SSH ».

Tests

6. Connectez-vous à une machine de salle TP.
7. Éditez le fichier `~/.ssh/config` pour que la connexion SSH de cette machine de salle TP vers votre conteneur soit facile.
8. Depuis ce sell distant sur une machine de salle TP, connectez-vous à votre conteneur.
9. Redessinez le graphe de la première question en y ajoutant les nouvelles arêtes crées par l'installation de votre nouvelle clef publique.

Lorsque vous pouvez vous connecter sur votre conteneur par SSH depuis un shell exécuté par une machine de salle TP, vous pouvez ajouter `ssh_authorized_keys` à vos tags.

Warning de sécurité

Il y a un léger problème de sécurité puisque toute personne qui a la main sur le système de fichiers des machines de salle TP (par exemple les admins de Galilée), peuvent réucupérer votre clef privée et se faire passer pour vous auprès du serveur SSH de votre conteneur.

Pour limiter la casse, vous avez chiffré votre clef privée avec un mot de passe, de sorte à ce qu'un accès au fichier `~/.ssh/if_rsa` n'est pas suffisant.

Bien sur, une personne qui a un accès privilégié à la machine de salle TP lorsque vous tapez votre mot de passe pourrait déchiffrer et utiliser votre clef privée. Aussi, il est possible d'accèder à la clef déchiffrée en détournant le processus `ssh-agent` qui la retient en RAM (voir `man ssh-agent`). Il s'agit malgré tout d'une mitigation puisque l'action d'un·e éventuelle attaquant·e doit se faire sur la même machine de salle TP que vous et pendant que vous y êtes connecté·e et pas à tout moment en regardant le système de fichiers partagé entre toutes les machines de salle TP.

Il n'en reste pas moins que cette possibilité d'authentification sur les machines de salle TP affaiblit la sécurité de votre conteneur. Ainsi, avant les vacances d'été, effacez cette clef parmi les clefs autorisées sur votre conteneur.

Objectifs du TP :

- objectifs opérationnels du TP :
  - pouvoir se connecter sur son conteneur depuis une machine de salle TP en vue du partiel de TP noté.
- objectifs pédagogiques du TP :
  - faire le point sur les connexions entre machines
  - manipuler des clefs SSH entre machines et faire le point sur l'authentification par paire de clefs.