Sécurité des infrastructures de virtualisation

Conteneurs et sécurité

3e année cycle ingénieur STI, option 2SU, 2017 – 2018

Objectifs

- Découvrir Docker et le confinement avec SELinux sous Fedora ;
- Créer un conteneur à l'aide d'un Dockerfile.

Introduction et recommandations

La version PDF de ce TD est disponible à l'adresse suivante : https://tim.siosm.fr/cours.

N'hésitez pas à garder une trace des différentes commandes que vous utilisez et des configurations que vous allez produire.

Ce TD est prévu pour être réalisé dans une machine virtuelle Fedora 27 ou supérieure.

Créer une machine virtuelle « noselinux » dans laquelle on désactivera SELinux en spécifiant le mode `disabled` dans le fichier `/etc/selinux/config`. Redémarrer la machine pour que le changement soit pris en compte.

Pour préparer une machine virtuelle en partant de zéro :

```
$ sudo dnf update -y
$ sudo dnf install -y vim tree docker bash-completion selinux-policy-devel setools-console
$ sudo systemctl enable --now docker
$ sudo reboot
```

1 Docker

1.1 Récupération d'une image Docker

Toutes les manipulations qui vont suivre seront à effectuer dans les deux machines virtuelles en parallèle pour pouvoir comprendre l'impact de SELinux dans l'isolation des conteneurs Docker.

Pour récupérer directement du registre public Docker l'image officiel de conteneur Fedora, utiliser :

```
$ sudo docker pull fedora
```

Vérifier qu'elle a bien été importée avec la commande :

```
$ sudo docker images
```

La dernière version publiée de l'image est téléchargée. Pour lancer un shell intéractif dans un conteneur utilisant cette image :

```
$ sudo docker run -it fedora bash
```

1.2 Docker & SELinux

S'aider des commandes suivantes pour répondre aux questions :

```
$ id -Z
$ sudo docker ps
$ systemd-cgls
$ ps auxZ
```

- **Question 1 :** Sous quel utilisateur tourne ce shell ?
- **Question 2 :** Est-ce le même à l'intérieur et à l'extérieur du conteneur ?
- **Question 3 :** Sous quel contexte SELinux et avec quelles catégories tourne ce processus ?

Lancer un deuxième shell dans un deuxième conteneur en parallèle.

- **Question 4 :** Sous quel utilisateur, contexte SELinux et avec quelles catégories tourne ce processus ?

Lancer un nouveau shell avec la commande :

```
$ sudo docker run -it --rm --privileged -v /:/host fedora bash
```

- **Question 5 :** Sous quel utilisateur, contexte SELinux et avec quelles catégories tourne ce processus ?
- **Question 6 :** Quels sont les risques présentés par cette commande ?

S'inspirer de la commande suivante pour obtenir des informations sur les accès autorisés par la politique SELinux pour le domaine `container_runtime_t` :

```
$ sudo dnf install setools-console
$ sesearch -A -s container_runtime_t /etc/selinux/targeted/policy/policy.29
```

1.3 Dockerfile

Créer un conteneur Docker qui :
- est basé sur l'image fournie par le projet Fedora ;
- ne tourne pas sous l'utilisateur `root` ;
- lance un serveur Apache sur le port 8080.

S'aider des guides suivants :
- les exemples disponibles dans le dépôt : https://github.com/fedora-cloud/Fedora-Dockerfiles
- la référence sur les `Dockerfiles` : https://docs.docker.com/engine/reference/builder/
- les recommandations de l'article : https://www.projectatomic.io/docs/docker-image-author-guidance/
- le guide de bonnes pratiques : https://docs.docker.com/engine/userguide/eng-image/dockerfile_best-practices/

2 Références

- http://www.projectatomic.io/blog/2015/08/why-we-dont-let-non-root-users-run-docker-in-centos-fedora-or-rhel/
- http://www.projectatomic.io/docs/docker-image-author-guidance/
- http://developerblog.redhat.com/2014/11/06/introducing-a-super-privileged-container-concept/
- https://fedoraproject.org/wiki/Docker