TP/TD sécurité Docker

Jean-Marc Pouchoulon

Mai 2025

1 Pré-requis, recommandations et notation du TP.

Les pré-requis sont les suivants:

- Avoir un PC sous Linux.
- Avoir installé Docker ou utilisé une OVA prête à l'emploi. Merci **de ne pas** utiliser les packages fournis par les distributions qui sont souvent moins récents que les packages fournis par Docker.
- Avoir installé docker-compose, il est présent sur les ova de l'IUT.
- Vous devrez avoir un compte sur le site Docker `https://hub.docker.com/`.

Vous travaillerez individuellement. Il vous explicitement demandé de faire valider votre travail par l'enseignant. Ces "checks" permettront de vous noter. Un compte rendu succinct (fichiers de configuration , copie d'écran montrant la réussite de la construction ...) est demandé et à rendre sur Moodle.

1.1 Installation de Docker et obtenir de l'aide.

1.1.1 Rappel: Installation de Docker sous Linux.

Vous travaillerez avec une VM en utilisant l'OVA Ubuntu dans sa dernière version L.T.S. présente sur `http://store.iutbeziers.fr/`

1.1.2 Aide sur Docker.

```
man docker-run
man docker-create
```

Accéder à la Documentation Docker:
`https://docs.docker.com/`
Documentation sur les commandes Docker:
`https://docs.docker.com/engine/reference/commandline/`
CheatSheet:
`http://cs.iutbeziers.fr/iutbrt/`
La complétion avec la touche tab fonctionne aussi.

2 Peurs sur les containers

2.1 Etat des lieux rapide de la sécurité des containers

Les containers sont souvent vu comme étant d'un niveau de sécurité moindre que celui d'une machine virtuelle. C'est le cas mais il ne fait pas perdre de vue que ce modèle est plus sécurisé que l'hébergement simple de plusieurs services sur un même hôte bien que systemd puisse apporter lui aussi des éléments de sécurité identiques à ceux utilisés dans les containers.

Un container reste donc plus sécurisé qu'un processus ou un groupe de processus lancé sur un hôte sans les contingentements fournis par les namespaces , les cgroups et les capabilities.

Néanmoins le mix de ces éléments impacte le niveau de privilèges du containers et il faut donc être conscient de ce que vous faites en donnant accès à tel ou tel privilège.Un container super-privilégié (ils sont parfois nécessaires) peut être très dangereux pour la sécurité de votre hôte.

En fonction des besoins de sécurité remontés par l'analyse de risques il est néanmoins concevable de mettre un container par machine virtuelle. Ces machines virtuelles sont minimalistes afin de fournir des performances acceptables dans le cadre d'un instanciation suffisamment rapide pour ne pas être considérée comme pénalisante.

C'est la tendance à ce jour.

2.2 Les menaces

Plusieurs menaces pèsent sur les containers:

- *L'installation de packages vulnérables:* des packages vulnérables peuvent être utilisés pour le build de l'image. Il est donc important d'utiliser un scanner de vulnérabilités donnant la liste et l'impact des "Common Vulnerabilities and Exposures" de l'image. Il est tout aussi important de disposer d'une chaîne d'intégration et de déploiement continu afin de mettre à jour les images en continu afin d'éviter une probabilité d'occurrence forte d'un incident de sécurité et/ou un impact important.
- *Vulnérabilités au build de l'image proprement dit*: construire une image avec des droits root ou du groupe Docker peut poser des problèmes si l'attaquant s'introduit dans la chaîne de build. L'utilisateur "root" est utilisé pour le daemon Docker ce qui est intrinsèquement dangereux.
- *L'intégrité des images de containers est un point important*: si l'attaquant modifie une image sur un registry à votre insu vous pouvez lui permettre d'accéder à votre environnement containérisé. Ce n'est pas un problème spécifique de Docker mais le succès des containers amplifie la probabilité de trouver des images corrompues...
- *Un container ne doit pas être plus privilégié que nécessaire*: en fonction des besoins il peut être judicieux de durcir le container en limitant les "capabilities" de celui-ci.
- *La question de l'appartenance des processus dans un container à un utilisateur est essentielle*: un processus appartenant au root de l'hôte dans un container induit une vulnérabilité en profondeur sur l'hôte et les autres containers dans le cas ou le container est compromis.
- *Attaques par dépassement des capacités*: un container qui n'est pas contingenté au niveau de ses ressources peut être soumis à un déni de services et peut perturber l'exploitation de l'application qu'il porte mais aussi les resources des autres containers voire de l'hôte lui-même.
- *l'encodage en dur des mots de passes ou de token* peut poser des problèmes triviaux mais courant comme en témoigne les chasseurs de secrets sur GitHub.
- *Vulnérabilités de l'hôte*: un hôte vulnérable ou exposant une large surface aux attaques donnera l'accès à tous les containers.
- *Vulnérabilités liées au réseau*: un container compromis peut permettre d'attaquer d'autres containers via le réseau si ceux ci sont accessibles.
- *L'infrastructure liée à Docker* doit être aussi prise en compte lors de l'analyse de risques: une socket d'un daemon Docker en accès distant ouvert est une porte d'entrée très appétissante pour un attaquant.
- Le Daemon Docker est lancé sous root afin de lui permettre de gérer les containers. Il est possible d'être "rootless" afin de limiter la surface d'attaque.

  Dans le cadre d'un hébergement *"multi-tenants"*[1] on peut légitimement se poser la question de la sécurité de vos clients lors de l'utilisation de containers. Heureusement pour nous il existe des outils pour mitiger le risque ou l'accepter en toute connaissance de cause.

1. comprendre plusieurs clients sur une même machine

3 Utilisation des namespaces par Docker

Les namespaces permettent de dresser un décor pour les processus de nos containers. Le container ne verra que le contexte qu'on l'autorise à voir au travers des namespaces et *on ne peut pas attaquer ce qu'on ne peut pas atteindre*. Un container est donc contraint par les namespaces qui sont appliqués par le Kernel à ses processus.

3.1 Accéder au namespace de l'hôte depuis un container Docker c'est mal

Créez un container et vérifiez que les options suivantes de docker run "–pid=host" et "–net=host" permettent d'accéder aux processus et au réseau de l'hôte.

3.2 Utilisation des usernamespaces par Docker afin de limiter les droits d'un attaquant

Docker présente une fonctionnalité depuis la version 1.10 très intéressante et très attendue en terme de sécurité: la possibilité d'utiliser des "user namespaces".

Si l'attaquant prend le contrôle du container Docker et que le microservice du container est porté par root, l'attaquant a accès au root de l'hôte et donc aux autres containers.

Les "user namespaces" permettent d'avoir un compte qui a les droits de root dans le container et qui a les droits d'un utilisateur non privilégié sur l'hôte.

1. Activez l'option –userns-remap avec le daemon docker afin d'activer les usernamespaces pour l'ensemble de containers.

   Pour cela ajoutez dans le fichier /etc/docker/daemon.json

   ```
   {
     "userns-remap":"student"
   }
   ```

   suivi de:

   ```
   systemctl restart docker
   ```

   On va pouvoir ainsi mapper les uid/gid des users dans les containers à partir des fichiers /etc/subuid et /etc/subgid. Modifiez ce fichier.
2. Lancez un container avec un processus bash et vérifiez que dans le container ce processus est vu comme appartenant à root et comme appartenant à un utilisateur mappé dans l'hôte.

   Pour la suite du TP désactiver les usernamespaces ils sont parfois contraignants quand il faut accéder aux partages sur l'hôte.

3.3 Contrôle des ressources allouées aux processus d'un container

3.3.1 Contrôle des ressources des containers au travers des cgroups

Un attaquant peut saturer un container en lançant un déni de services. Si on ne limite pas les ressources consommées par un container, c'est l'hôte qui sera en manque de ressource à son tour. Il est donc important de limiter les ressources prises par un container via les CGROUPS.

1. A partir de ce Dockerfile.

   ```
   FROM debian:latest
   RUN apt-get update && \
   apt-get install stress
   ```

Générez une image d'un container "stresseur":

```
cd ../buildstress
docker rmi jmp/stress
docker build -t jmp/stress .
```

2. Lancez le container "stresseur" et ouvrez une fenêtre htop pour voir la consommation de ressources sur l'hôte:
3. Récréez le container et limitez-le à l'utilisation d'un seul CPU.

3.3.2 Lutte contre l'épuisement des ressources du container et de l'hôte par déni de service local ("fork bomb" par exemple).

Une "fork bomb" crée des processus qui vont eux mêmes générer (appel système FORK) d'autres processus fils identiques au père.

La commande suivante permet de lister les ressources du container à l'aide de la commande docker stats:

```
docker stats --no-stream=True
CONTAINER      CPU %   MEM USAGE / LIMIT   MEM %  NET I/O  BLOCKI/O  PIDS
```

1. Dans votre machine virtuelle Ubuntu lancez une "fork bomb" bash dans un container.

   Si tout se passe bien votre container et votre machine virtuelle ne répondront plus, vous voilà prévenu...

   La commande suivante permet de lancer un container contenant une fork bomb:

   ```
   docker exec -it deb1 /bin/bash -c ":(){ :|:& };:"
   ```

2. Trouvez le moyen lors de sa création (docker run) de limiter le nombre de processus dans le container.

4 Sécurisation des capacités données à un container Docker

Il existe des possibilités de rendre le container super-privilégié. C'est parfois nécessaire en dernier recours mais il faut en payer le prix en termes de sécurité.

4.1 Création d'un container privilégié

Utilisez l'option –privileged lors de la création d'un container. Dans le container et l'aide de la commande capsh et de la commande pscap [2] obtenez les capabilities de votre container et de votre processus bash. Comparez avec un container non privilegié.

A quelles capabilities l'option –privileged donne-t-elle accès ?

4.2 Prise de contrôle du container avec des capabilities permettant une escalade de privilèges

Nous allons utiliser les mécanismes existants de Docker afin de renforcer la sécurité d'un container.

Utilisez votre container ssh afin de voir si peut limiter les capabilities du processus sshd.

1. Lancez votre container (docker run -d –cap-drop= ...) en enlevant les capabilities une par une.

   Au final et de façon empirique vous obtiendrez un container à priori fonctionnel et plus sécurisé. Testez-le à chaque fois à l'aide de la commande:

2. installez les packages libcap2-bin et libcap-ng-utils)

Aidez-vous de:

`https://docs.docker.com/engine/reference/run/#runtime-privilege-and-linux-capabilities`

5 Attaque sur le daemon Docker par un utilisateur local à l'hôte.

1. Sous le compte d'un utilisateur appartenant au groupe Docker, trouvez le moyen d'accéder à /etc/-password et /usr/sbin/ de la machine en utilisant les volumes Docker.
2. Qu'en deduisez-vous de la sécurité d'un PC de développeur avec Docker ? [3]

6 Utilisation de AppArmor afin de contrôler un container vulnérable à ShellShock

Shellshock est une faille du shell permettant à un attaquant de prendre la main sur une machine. voir:

— `https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/shellshock.pdf`
— `https://www.cert.ssi.gouv.fr/alerte/CERTFR-2014-ALE-006/`

1. Créez le fichier simple-cgi-bin.sh

```
#!/bin/bash
echo "Content-type: text/plain"
echo
echo
echo "shellshockme if youcan"
```

2. Générez l'image Docker suivante vulnérable à ShellShock au travers de ce Dockerfile:

   Créez un container shell-shock à partir de l'image registry.iutbeziers.fr/debian-lenny-shellshock.

```
docker run -d -p 80:80 --name=hitme --hostname=hitme registry.iutbeziers.fr/debian-lenny-shellshock
```

3. Vérifiez qu'il est bien vulnérable à ShellShock en lancant un shell dans le container.
4. Vérifiez à l'aide d'un wget que vous pouvez récupérer "à distance" le fichier /etc/password du container.
5. Utilisez AppArmor pour empêcher l'exploitation de ce container vulnérable.

   Docker charge une configuration apparmor `https://gist.github.com/pushou/3a8a08520ee9895bc9703114ad9c165`
   Rajoutez y la ligne

   deny /usr/lib/cgi-bin/** rwklx, afin de bloquer l'exécution des scripts cgi et donnez ce profile au container shellshock lors du run.

7 Utilisation d'un scanneur de vulnérabilités

Utilisez le scanneur de vulnerabilité trivy sur l'image registry.iutbeziers.fr/debianiut.

8 Utilisation de SecComp pour limiter l'utilisation de certains appels systèmes

Seccomp permet de filtrer des appels systèmes en KernelLand. Vous devez vérifier que votre kernel supporte cette fonctionnalité:

3. Voir plus loin la solution Docker en mode rootless

```
cat /boot/config-`uname -r` | grep CONFIG_SECCOMP= CONFIG_SECCOMP=y
```

et que votre version de SecComp est supérieure à >= 2.2.1. La fonctionnalité a uniquement été testée avec succès sur Ubuntu 16.

1. Téléchargez le fihier default-no-chmod.json qui va interdire le lancement de la commande chmod dans le container.
2. Utilisez ce fichier pour limiter les appels systèmes du container lors du "docker run".
3. Expliquez en le fonctionnement.
4. Créez un container et lancez un chmod 777 sur le fichier /etc/password.

9 Containers en lecture seule

Un container web en lecture c'est l'idéal pour des containers mettant à disposition des contenus statiques. Créez un container Web nginx et essayer de la mettre en lecture seule lors du run. Consultez les logs du container afin de déterminer quel est le problème et corrigez-le.

10 Contrôle de l'élévation de privilèges dans un container via l'option "-security-opt=no-new-privileges"

Buildez l'image en suivant le README du repo git suivant:

`https://github.com/pushou/docker-secu-priv`

Testez et expliquez l'effet de cette option.

11 Rootless containers

Le mode rootless s'obtient le durcissement du daemon responsable de la gestion des containers qui n'a plus besoin d'être root afin de manager des containers.

Docker n'est pas le seul "manager" de processus containairisé: Podman de RedHat est rootless par construction. Docker est néanmoins capable de fonctionner en userspace. [4].

=

1. En suivant la documentation officielle installez "Docker rootless" avec le user student.

```
sudo apt install slirp4netns uidmap
export FORCE_ROOTLESS_INSTALL=1
curl -sSL https://get.docker.com/rootless | sh
sudo setcap cap_net_bind_service=ep $HOME/bin/rootlesskit
    /home/student/bin/dockerd-rootless.sh --experimental --storage-driver vfs
    export XDG_RUNTIME_DIR=/home/student/.docker/run
    export PATH=/home/student/bin:$PATH
export DOCKER_HOST=unix:///home/student/.docker/run/docker.sock
```

1. Lancez un container et donnez un port d'écoute inférieur à 1024.
2. Expliquez rapidement comment fonctionne Docker en mode Rootless.

4. voir https://docs.docker.com/engine/security/rootless/

12 Kata containers

Il s'agit de faire tourner un container dans une machine virtuelle. La solution des "kata containers" permet de faire exécuter un container dans une machine virtuele KVM ou FireCracker (VMS d'AWS). On va tester ici la solution avec KVM:

```
sudo snap install kata-containers --classic
```

Modifiez le fichier daemon.json et redémarrer Docker

```
{
"insecure-registries" : ["registry.infres.local"],
"default-runtime": "runc",
"runtimes": {
kata-runtime": {
"path": "/snap/bin/kata-containers.runtime"
}
}
}
```

13 Annexe : Débugguer un container

Les containers sont optimisés pour être les plus légers possibles et n'embarquent pas en général pas d'outils facilitant l'analyse. Voilà une façon de les débugguer (sur une idée de J. Petazzoni) [5]:

1. Générer une instance Apache. Cette instance ne contient pas d'éditeur ni de d'outils réseaux (iproute2/ifconfig)

   ```
   docker run  -d --rm  httpd
   ```

2. Télécharger un binaire statique busybox

   ```
   wget https://www.busybox.net/downloads/binaries/1.31.0-defconfig-multiarch-musl/busybox-x86_64 \
   -O busybox && chmod +x busybox
   ```

3. Récupérez l'Id du container afin de copier le binaire busybox.

   ```
   docker cp ./busybox id_du_container:/
   ```

4. Vous pouvez maintenant utiliser les commandes de busybox pour analyser votre container.

   ```
   docker exec -it 1edd81a917315bf  /busybox ip a

   1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
   valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
   valid_lft forever preferred_lft forever
   2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN qlen 1000
   link/ipip 0.0.0.0 brd 0.0.0.0
   84: eth0@if85: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue state UP
   link/ether 02:42:ac:11:00:04 brd ff:ff:ff:ff:ff:ff
   inet 172.17.0.4/16 brd 172.17.255.255 scope global eth0
   ```

5. https://www.youtube.com/watch?v=-DsegUFcENc

```
    valid_lft forever preferred_lft forever
    inet6 fd00::242:ac11:4/80 scope global flags 02
    valid_lft forever preferred_lft forever
    inet6 fe80::42:acff:fe11:4/64 scope link
    valid_lft forever preferred_lft forever
```

5. Installez nsenter [6].
6. Trouvez le pid d'un process dans le container :

```
    docker inspect id-du-container|grep -i pid
```

7. Utilisez nsenter pour retrouver les NameSpaces du container et lancez les commandes de votre hôte dans le container.

```
    export LANG=C
    nsenter --target PID_trouvé_précedemment -p -u -n -i
```

6. https://github.com/jpetazzo/nsenter