

TD TEST D'INTRUSION / PENTEST

Préparation du TD (11/10/2022)

Sadry FIEVET

sadry.fievet@univ-cotedazur.fr



INTRODUCTION	2
INSTALLATION IMAGE DOCKER sadry/td_pentest-kali	2
INSTALLATION DOCKER	3

INTRODUCTION

Afin de réaliser le TD sur les tests d'intrusions, vous devez installer :

- [Docker](#) (si ce n'est pas déjà fait).
Docker est un logiciel de virtualisation dite légère qui permet de lancer rapidement et simplement des machines virtuelles. De plus, à la différence des autres logiciels de virtualisation comme Virtualbox ou VMWare, Docker est très peu consommateur de ressources.
- [docker-compose](#)
Docker-compose va permettre de lancer les différentes infrastructures que vous allez auditer et qui sont composées de plusieurs conteneurs et réseaux.
- [image docker audit](#)
Cette image docker sera votre machine d'audit. Il est préférable de l'installer et de la tester avant/dès le début du TD.

INSTALLATION IMAGE DOCKER machine audit

Dans un premier temps il faut charger l'image sur votre machine

docker pull sadry/sadry:tp_pen_kali

```
sadry@bastide: ~ 119x24
sadry@bastide:~$ docker pull sadry/sadry:tp_pen_kali
tp_pen_kali: Pulling from sadry/sadry
Digest: sha256:52ec61b2cf81e6a56e681174a7c8c9bf95882a7e0db804c5b5386cc27cff7f65
Status: Image is up to date for sadry/sadry:tp_pen_kali
docker.io/sadry/sadry:tp_pen_kali
sadry@bastide:~$
```

Vérifier ensuite que l'image est bien présente sur votre machine

docker images

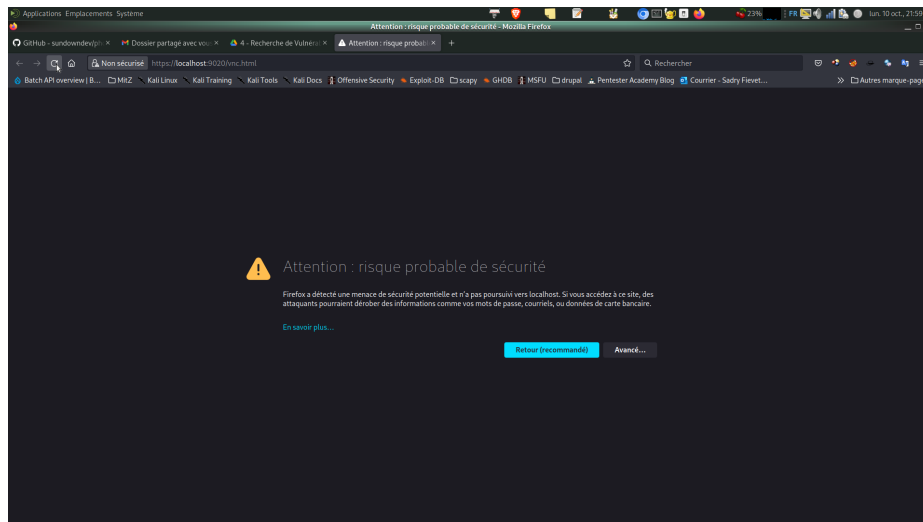
```
sadry@bastide:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
sadry_td_kali       latest             ffe8a565b9cc       20 hours ago       5.2GB
sadry/sadry         tp_pen_kali        ffe8a565b9cc       20 hours ago       5.2GB
```

Vous allez maintenant pouvoir tester votre machine d'audit avec la commande suivante :

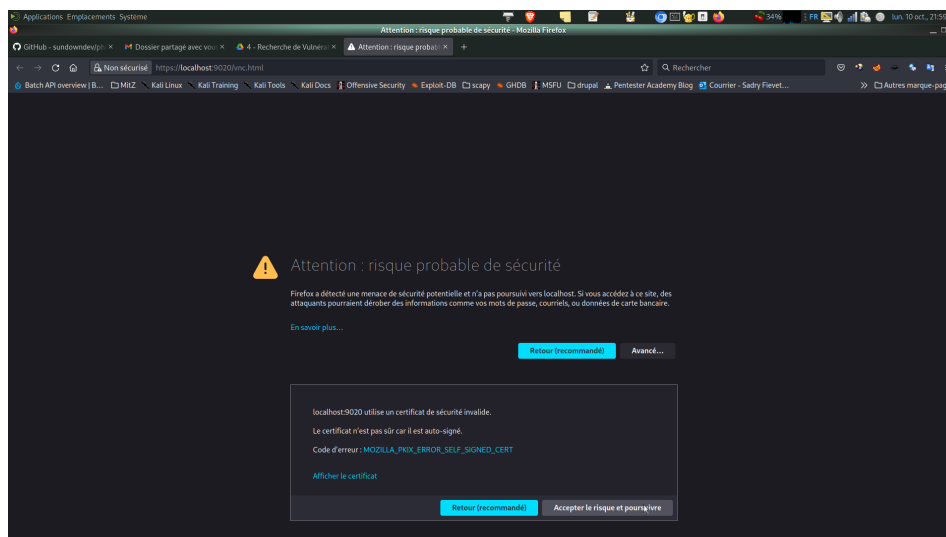
docker run -it --rm -p 9020:8080 -p 9021:5900 sadry/sadry:tp_pen_kali

```
root@c8db5e9b01b2: /119x24
sadry@bastide:~$ docker run -it --rm -p 9020:8080 -p 9021:5900 sadry/sadry:tp_pen_kali
Launch your web browser and open https://localhost:9020/vnc.html
Verify the certificate fingerprint:
sha256 Fingerprint=D7:07:14:5A:41:35:1F:62:98:46:ED:F8:A8:1B:6B:BA:95:A9:2C:65:3E:71:12:20:06:2F:B7:EA:95:5B:4B:C3
(root@c8db5e9b01b2) - [/]
#
```

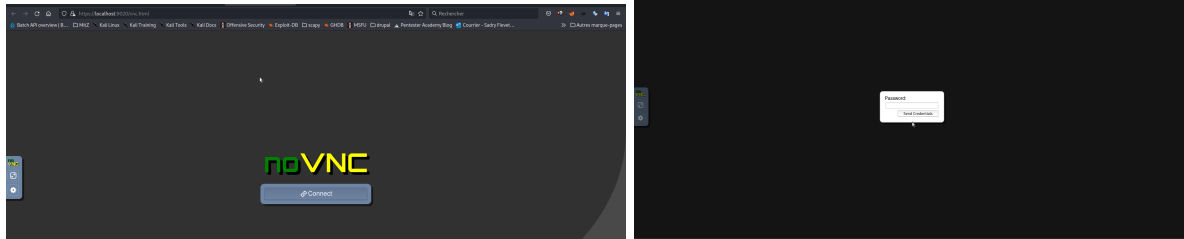
La capture d'écran précédente affiche une invite de commande dans le terminal de votre conteneur Kali. Le texte invite également à ouvrir un navigateur pour nous rendre à l'adresse <https://localhost:9020/vnc.html>



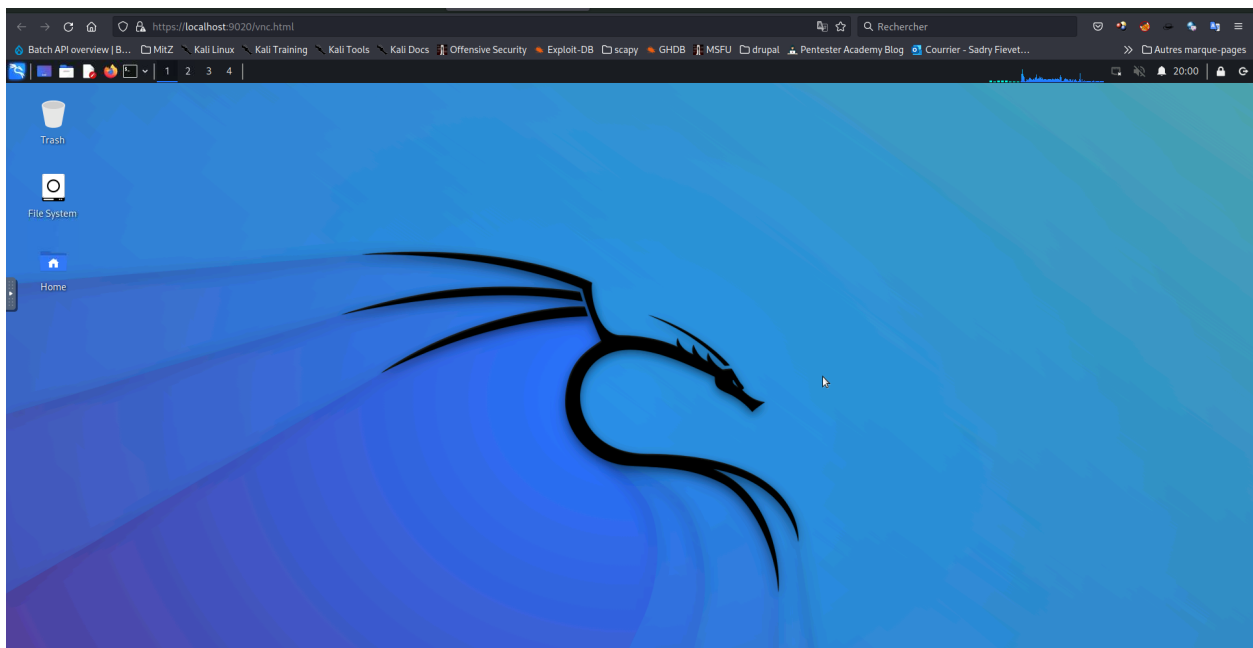
L'avertissement de sécurité est normal :) , il faut cliquer sur le bouton **Avancé...**



Ici encore vous devez cliquer sur **Accepter le risque et poursuivre**



Cliquez maintenant sur **Connect** et entrez le mot de passe : **caspar**

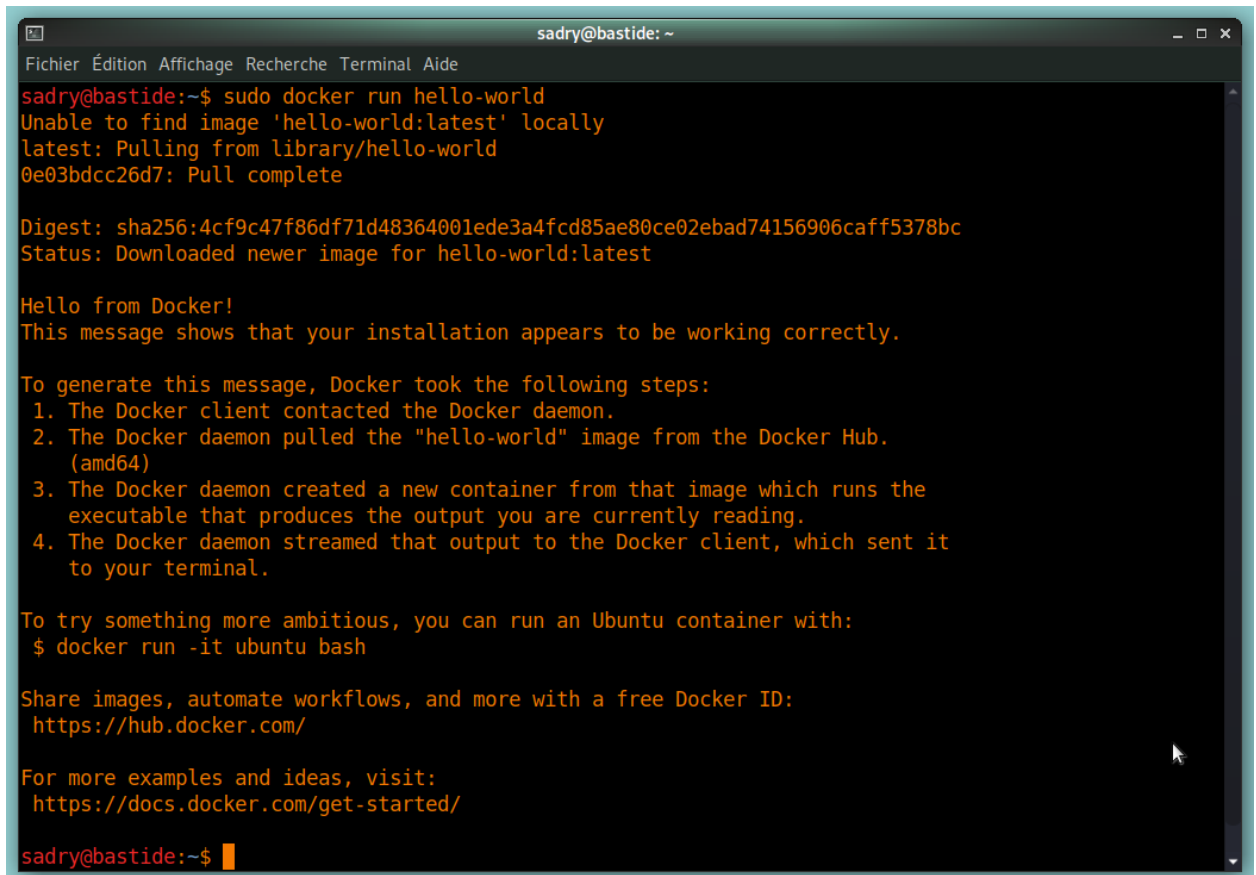


Voilà, vous avez maintenant dans votre navigateur la distribution **kali-top10** qui regroupe les 10 outils indispensables pour faire des tests d'intrusions. N'oubliez pas que vous avez également une invite de commande sur cette machine depuis votre terminal.

INSTALLATION DOCKER

L'installation suivante est réalisée sur un OS Kali Linux 2020, elle devrait fonctionner avec tous les OS debian. Si vous rencontrez des problèmes ou avez une autre distribution, rappez-vous à la documentation : <https://docs.docker.com/engine/install/>

1. Mettez votre système à jour
`$ sudo apt-get update`
2. Installez les dépendances
`$ sudo apt-get install apt-transport-https ca-certificates curl gnupg-agent software-properties-common`
3. Ajoutez la clef publique PGP de Docker
(valeur de la clef : 9DC8 5822 9FC7 DD38 854A E2D8 8D81 803C 0EBF CD88)
`$ curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -`
4. Vérifiez votre installation en cherchant les derniers caractères de l'empreinte
`$ sudo apt-key fingerprint 0EBFCD88`
5. Configurez un dépôt Docker pour apt
`$ echo 'deb [arch=amd64] https://download.docker.com/linux/debian buster stable' | sudo tee /etc/apt/sources.list.d/docker.list`
6. Mettez à jour votre système
`$ sudo apt-get update`
7. Supprimer les possibles anciennes versions de Docker
`$ sudo apt-get remove docker docker-engine docker.io`
8. Installez Docker
`$ sudo apt-get install docker-ce`
9. Testez votre installation
`$ sudo docker run hello-world`
10. Si tout s'est bien passé vous devriez avoir un retour équivalent à celui-ci :

A terminal window titled 'sadry@bastide: ~' with a menu bar (Fichier, Édition, Affichage, Recherche, Terminal, Aide). The terminal shows the command 'sudo docker run hello-world' and its output. The output indicates that the 'hello-world:latest' image was pulled from the Docker Hub library. It shows the digest 'sha256:4cf9c47f86df71d48364001ede3a4fcd85ae80ce02ebad74156906caff5378bc' and the status 'Downloaded newer image for hello-world:latest'. The container then prints 'Hello from Docker!' and a message stating that the installation appears to be working correctly. It lists four steps Docker took to generate this message: 1. The Docker client contacted the Docker daemon. 2. The Docker daemon pulled the 'hello-world' image from the Docker Hub. (amd64) 3. The Docker daemon created a new container from that image which runs the executable that produces the output you are currently reading. 4. The Docker daemon streamed that output to the Docker client, which sent it to your terminal. It then suggests trying something more ambitious by running an Ubuntu container with the command '\$ docker run -it ubuntu bash'. It also provides links to Docker Hub and Docker documentation. The terminal ends with the prompt 'sadry@bastide:~\$' and a cursor.

```
sadry@bastide:~$ sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
0e03bdcc26d7: Pull complete

Digest: sha256:4cf9c47f86df71d48364001ede3a4fcd85ae80ce02ebad74156906caff5378bc
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
   (amd64)
3. The Docker daemon created a new container from that image which runs the
   executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
   to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/

sadry@bastide:~$
```

11.

12. Afin de pouvoir lancer Docker sans être root, ajoutez votre utilisateur au groupe Docker

```
$ sudo usermod -aG docker $USER
```

13. Redémarrez votre machine, puis vérifiez que la commande précédente a fonctionné.

```
$ docker run hello-world
```

Je vous invite à regarder le document Cheat Sheet Docker qui résume les quelques commandes que nous utiliserons dans ce TD (essentiellement la partie RUN)

FIN DU DOCUMENT