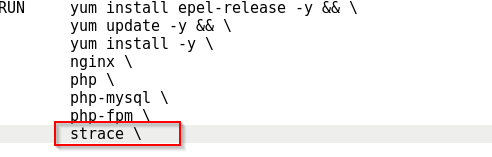
**Steps taken for creating seccomp webserver**

1 – Edit the **Dockerfile** -> add **strace** to **Dockerfile**



2 – Run the webserver container without a seccomp file

docker run -it --entrypoint /bin/bash --net iss-cw3\_net --ip 192.0.2.10 --hostname webserver --add-host database:192.0.2.3 -p 80:80 --security-opt seccomp=unconfined --security-opt=no-new-privileges --security-opt apparmor=unconfined --privileged --cap-add=SYS\_PTRACE --name nginx-server\_c <image\_id>

3 – Strace nginx

strace -c -f nginx

Let the command run and access “localhost/index.php” from your browser, you should get an error from nginx, but it is fine

4 – Get a new terminal from inside the webserver

docker exec -it <container\_name> /bin/bash

Run strace for php-fpm

strace -c -f pgp-fpm -F

Reload the webpage and interact with it

5 – Stop both straces – nginx and php-fpm

You will get the list of syscalls

6 – Add the missing syscalls so docker can start

"capget",

"capset",

"fchown",

"getdents64",

"exit",

"exit\_group",

"rt\_sigreturn",

"getdents64"

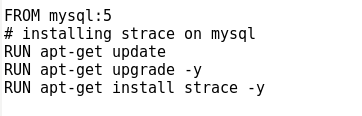
The seccomp file for nginx on girhub -> **final\_seccomp\_nginx.json**

7 – Run docker with seccomp

docker run -d --net iss-cw3\_net --ip 192.0.2.10 --hostname webserver --add-host database:192.0.2.3 -p 80:80 --security-opt seccomp=new\_new\_seccomp.json --security-opt=no-new-privileges --security-opt apparmor=unconfined --name nginx-server\_c <image\_id>

**Steps taken for creating seccomp mysql**

1 – Edit the **Dockerfile** -> update the container and install strace



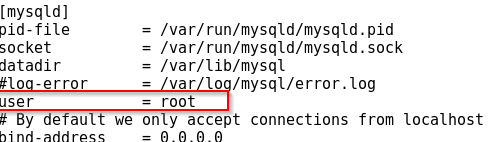
2 – Run mysql server

docker run -d --net iss-cw3\_net --ip 192.0.2.3 --hostname database -e MYSQL\_ROOT\_PASSWORD="test" -e MYSQL\_DATABASE="data" --security-opt seccomp=unconfined --security-opt=no-new-privileges --security-opt apparmor=unconfined --privileged --cap-add=SYS\_PTRACE --name mysql-server\_c <image\_id>

docker exec -i mysql-server\_c mysql -uroot -ptest data < sqlconfig/data.sql

docker run -d --net iss-cw3\_net --ip 192.0.2.3 --hostname database MYSQL\_ROOT\_PASSWORD=”test” -e MYSQL\_DATABASE=”data” –security-opt seccomp:custom.json --name mysql-server\_c <docker image>

3 – Edit **mysld.conf**

****

docker exec -it mysql-server\_c /bin/bash

4 – Strace mysql -> you will get access to the database and start navigating through it

strace -c -f mysql -uroot -ptest

5 – One a second terminal from inside mysql run

strace -c -f mysqld -F

6 – From inside the webserver container run the following commands

1 – install mysql -> yum install mysql

2 – connect to the database and navigate through it -> mysql -uroot -ptest -h 192.0.2.3

7 – Access the webpage and input some data

8 – Stop both straces and get a list with syscalls

Seccomp can be found on github -> **seccomp\_mysql.json**

9 – I added some missing syscalls to it, but it is still not working