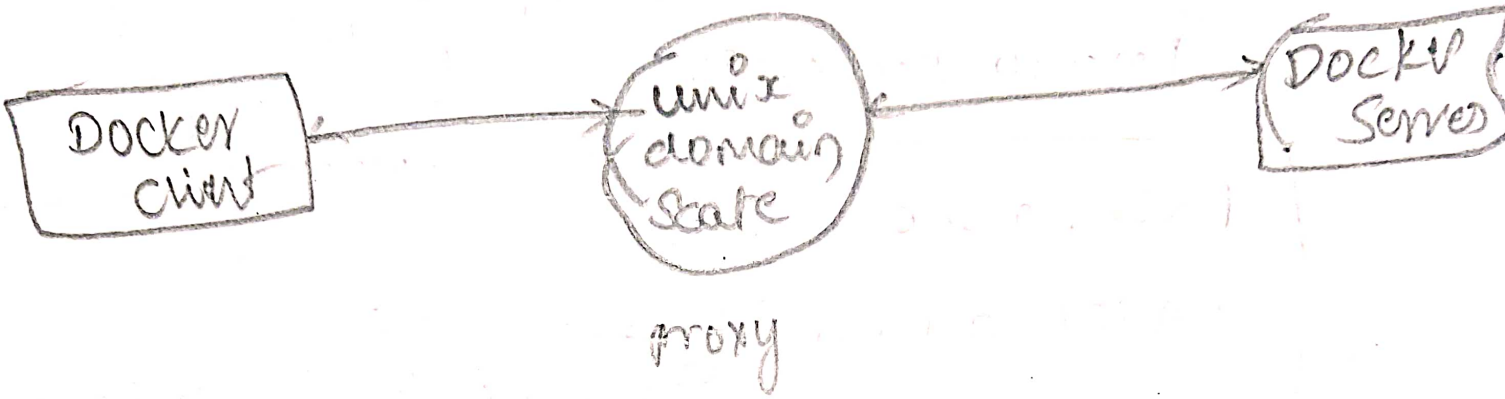

So cat → Command line utility

↓

Socket CAT.

↳ Versatile tool for establishing bidirection data transfer b/w two network connects.

Technique 4 : ~~To Monitor traffic~~

Using Socat to monitor Docker API Trafic

↓

Stands for Application Programming Interface. It is a set of rule & protocols that allows different Software application to communicate & interact with each other

Problem

To monitor trafict

Step1 → Run Socket using

```
Socat -v UNIX-LISTEN:/tmp/dockerapi.sock,fork \ UNIX-CONNECT:/var/run/docker.sock &
```

Step2 → To See request & Respond

```
docker -H unix:///tmp/dockerapi.sock PS -a
```

Monitoring → observing & capturing the interactions between Docker client & Docker Deamon.

Monitoring Docker API traffic involves capturing and analysing the communication between the Docker client and the Docker daemon.

Docker provides a RESTful API that allows user to interact with the docker daemon programatically, making it posible to manage containers, images, networks, and other Docker resources.

$socat -V UNIX-LISTEN:/tem/dockerapi.sock,fork\
UNIX-CONNECT:/var/run/docker.sock

↓

→ When you run this command Socat will start Listening on the Custom UNIX socket (/tmp/dockerapi.sock). Any Incoming Connections to this Socket will be forked. Socket will create a new process to handle each connection. It will the connect to the original docker deamon Socket at /var/run/docker.sock

→ The -V option enbles Verbose ouput, so you Should see log messages indication the data flow and connection being Established.

$docker -H unix:///tmp/dockerapi.sock ps -a

After running the socat Command in Step 1, You can use this Command to interact with the docker deamon

1) docker → This is the Docker command-line interface (CLI) used to interact with Docker and Mangages. Containers, images, network etc.

2) -H unix:///temp/dockerapi.sock: The -H flag Specifies the Docker Daemon host or endpoin. In this Case It is set to unix:///temp/dokerapi.sock, Indicating that we want to connect docker daemon through the custom UNIX Socket /temp/dockerapi.sock. The docker client will Send its api requests to this custom Socket, which is being handle by Socate process created in Step 1

3) ps: process status ——> list out running Containers

4) -a'. The -a flag, Instruct Docker to Show all Containers.