Docker security Hands-on labs for trainee

Exercise 1: Build the test docker image

Login to the terminal where docker is installed and get the sources from the trainer:

Exercise 2: Get the docker build history

Get the docker build history and what do you notice?

Exercise 3: Get capabilities

Get into the docker container and get the capabilities of the current user and see what the capabilities are. You can search for all the capabilities meanings on https://man7.org/linux/man-pages/man7/capabilities.7.html

Investigate how you can get the capabilities if you don't know how to get this.

Exercise 4: Get the capabilities of a process

Investigate how you can get the capabilities of the running processes if you don't know how to get this.

Exercise 5: Use ping inside the container

Try to run ping inside the container for example to localhost.
Why are you not allowed to do this?

Exercise 6: Fix ping

Fix the ping issue and try to run ping again inside the container.

Exercise 7: Observe the /mount path

Go to the /mount path and observe the files that reside in there.

Exercise 8: Print environment variables

Just for observability print out the environment variables and see what is in there.

Exercise 9: Login as root inside the container

It is very easy to gain root access inside the container by default, al you have to is login is the root user.

Exercise 10: Inspect the Dockerfile

What do you notice when you inspect the Dockerfile?

Bonus: AppArmor

Install bane, a AppArmor profile generator and use the sample AppArmor profile.
After running the container with the new profile activated try to run top and see what happens.
Also inspect the sample.toml (Later explained how to get the file) see what else you can and can't do.

Follow the docs for the installation instructions.

# To get the sample AppArmor profile file run:
wget https://raw.githubusercontent.com/genuinetools/bane/master/sample.toml

#Get the status of AppArmor:
$ sudo aa-status

#Install the profile
sudo bane sample.toml

# Information about using AppArmor
https://help.ubuntu.com/community/AppArmor