Lab 1-4 - Container Scanning with Tenable.IO

In this lab we will learn how to scan an image with the Tenable Container Scanner. The Tenable Container Scanner is a container image itself, making it easy to run on any system on which you are already running containers.

Create an image with vulnerabilities.

Before we scan our image, we want to create an image with vulnerabilities in it so that we have something to look at when out scan is complete. We will modify the image we created in the last lab.

1. Make sure we're in the right folder

```
$ cd ~/hello-nginx
```

2. Modify the base image in the Dockerfile to use a 5 year old version of the nginx image (using the tag). It will now look like the following

```
FROM nginx:1.9.5

COPY hello.html /usr/share/nginx/html
```

3. Lets build an image from this, we'll tag the image as :old so we know which one is which.

```
$ docker build --tag hello-nginx:old .

Sending build context to Docker daemon  3.072kB
Step 1/2 : FROM nginx:1.9.5
1.9.5: Pulling from library/nginx
Image docker.io/library/nginx:1.9.5 uses outdated schema1 manifest format.
Please upgrade to a schema2 image for better future compatibility. More
information at https://docs.docker.com/registry/spec/deprecated-schema-v1/
674ded4e0a75: Pull complete
a3ed95caeb02: Pull complete
5990b2a5d0cf: Pull complete
fe76480c1543: Pull complete
566c4a8f64fa: Pull complete
d8c1c49ba8d9: Pull complete
b4e65e3e68bb: Pull complete
Digest:
sha256:991bdd670fb03e0133cd72fd17add6622803eb904339d6ae9076aee402d71519
Status: Downloaded newer image for nginx:1.9.5
---> 5e31a05b5e9a
Step 2/2 : COPY hello.html /usr/share/nginx/html
---> 6e05bf433c0e
```

```
Successfully built 6e05bf433c0e
Successfully tagged hello-nginx:old
```

Notice that because none of the underlying images are local, it has had to download all of the underlying layers (there are more 'Pull complete' messages than when we built the previous one)

4. Check the local image collection to ensure you can see your new image

```
$ docker image ls
```

Generate and save Tenable.IO API keys

1. Follow the instructions on https://docs.tenable.com/tenableio/vulnerabilitymanagement/Content/Settings/GenerateAPIKey.htm to create an API access and secret key. Save these values somewhere as we cannot see them again, if you re-generate your API keys, the old ones will not be usable any more.

Download and run the Tenable container scanner in single image mode

Now we'll download the Tenable Container Scanner, which we will use to scan our image and upload the results to Tenable.IO

1. Log in to Tenable.IO using the credentials provided to you at the beginning of the class.
2. Click on 'Settings' in the dark blue bar at the top of the screen
3. Click on 'Connectors' in the light grey bar on the left side of the screen
4. Click on the + sign in a circle next to the heading 'Connectors' at the top left of the screen
5. On the right hand side of the screen, a panel will slide in with some information, copy this information somewhere so you can refer to it

```
Container Security Scanner

Use the following credentials to download the on-prem application:

Username: pubread

Password: BXa...D5h

Run the following commands to pull the container from the JFrog Registry:

docker login tenableio-docker-consec-local.jfrog.io

docker pull tenableio-docker-consec-local.jfrog.io/cs-scanner:latest

To start using the app follow the instructions here
```

6. Click on the 'here' link on the last line to open up documentation for using the scanner
7. Go back to your ssh client logged into the Lab VM
8. Enter the following command to log into the Tenable.IO image registry

```
$ docker login tenableio-docker-consec-local.jfrog.io
```

   It will ask for your username and password (from the information we copied in step 5.)

9. Download the Tenable Container Scanner image

```
$ docker pull tenableio-docker-consec-local.jfrog.io/cs-scanner:latest
```

10. Check the local images to see that it is now available

```
$ docker image ls
```

11. Now we will use the container scanner to scan the image and upload the results to Tenable.IO

```
$ docker save hello-nginx:old | docker run -e TENABLE_ACCESS_KEY={your
access key -e TENABLE_SECRET_KEY={your secret key} -e IMPORT_REPO_NAME="{put
your username here}" -i tenableio-docker-consec-local.jfrog.io/cs-
scanner:latest inspect-image hello-nginx:old
```

    For details on those command line options, see https://docs.tenable.com/tenableio/containersecurity/Content/ContainerSecurity/CSScanner_ConfigureAndRun.htm

12. Go back to Tenable.IO and select 'Container Security' from the three stripes icon in the very top left of the screen.
13. Find your image, click on it and have a look through some of the vulnerabilities.

Conclusion

In this lab we have created a docker image with vulnerabilities and used the Tenable Container Scanner to scan the image and upload results to Tenable.IO. We have also reviewed those results from inside the console.