Lab 2 (30 min)

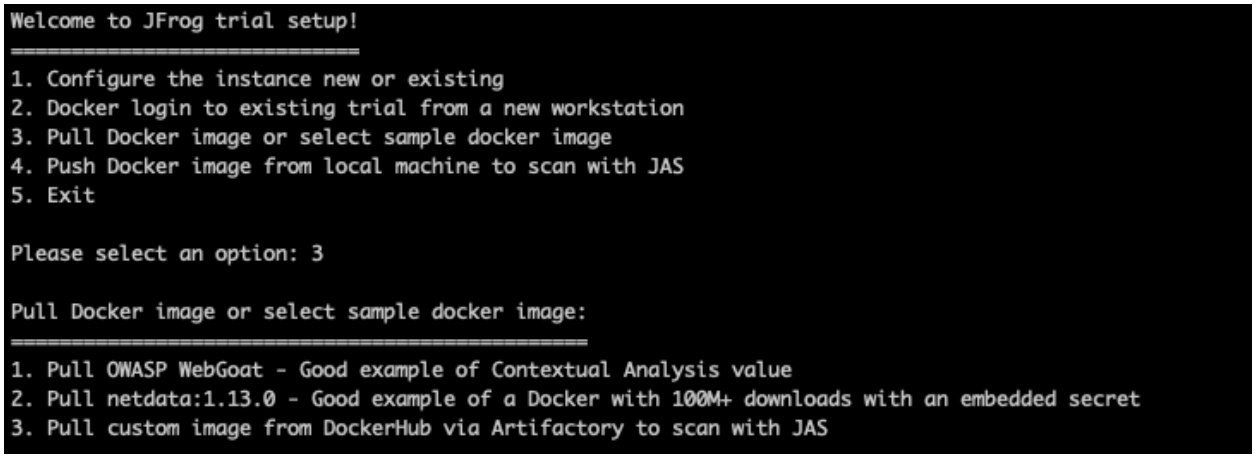
In this lab you will experience JFrog Advanced Security value with actual docker images scanning.

Upon successful completion of this lab you will gain knowledge of how to use the Security issues page and extract relevant value from it

Step by step instructions

Phase #1 - Pulling a docker image:

1. Open the terminal used in Lab 1, or, in case you've closed it, open a new one and run:
   `bash guided-trial/linux_guided_trial.sh`
2. From the menu, select option #3:
   `Pull Docker image or select sample docker image`



3. Now select 'WebGoat', option #1:

Pull OWASP WebGoat - Good example of Contextual Analysis value

```
Pull Docker image or select sample docker image:
================================================
1. Pull OWASP WebGoat - Good example of Contextual Analysis value
2. Pull netdata:1.13.0 - Good example of a Docker with 100M+ downloads with an embedded secret
3. Pull custom image from DockerHub via Artifactory to scan with JAS

Please select an option: 1

latest: Pulling from docker-hub-remote-repo/webgoat/webgoat-8.0
Digest: sha256:e24bcaf41034c28b6a08aba94507a169ae23f2b87899e225a3d18fe8c36d26f5
Status: Downloaded newer image for qawsed.jfrog.io/docker-hub-remote-repo/webgoat/webgoat-8.0:latest
qawsed.jfrog.io/docker-hub-remote-repo/webgoat/webgoat-8.0:latest

[+] Docker pull operation is complete, running SCA... opening the web browser in 30 seconds
    IMPORTANT: Please note JAS analyis might take up to 5 minutes
[==============================] 30/30 seconds

Docker image pulled via JFrog Platform!
```

Note how the docker image is being pulled from Docker Hub, through Artifactory to your personal laptop.

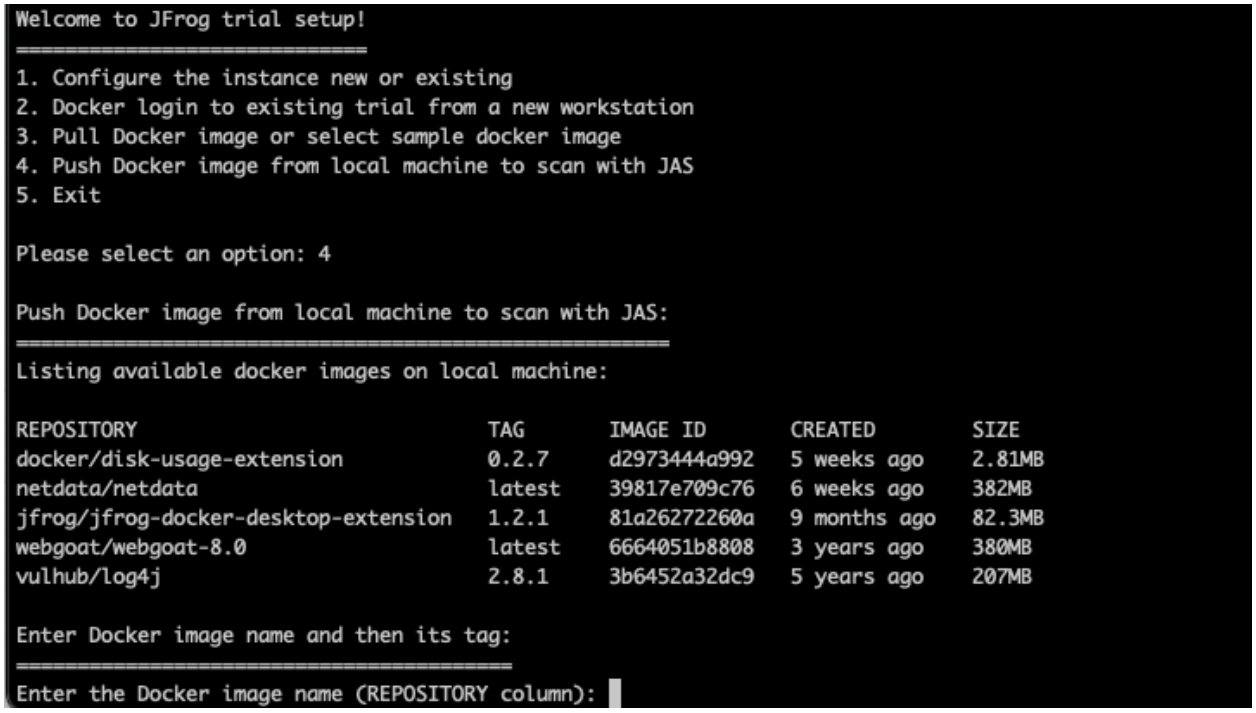
Your browser will be opened to your server's scan results page (results may take up to 5 min to complete).

4. Look at "CVE-2022-22965"
    a. Is it applicable to this docker image?
    b. What is the risk?
    c. What is the remediation process?
5. Now look at "CVE-2023-20873"
    a. Note the CVSS score of 9.8!
    b. Why is it not applicable to this docker image?

Phase #2 - Pushing a docker image:

6. Go back to your terminal & select option #4 from the menu:

`Push Docker image from local machine to scan with JAS`



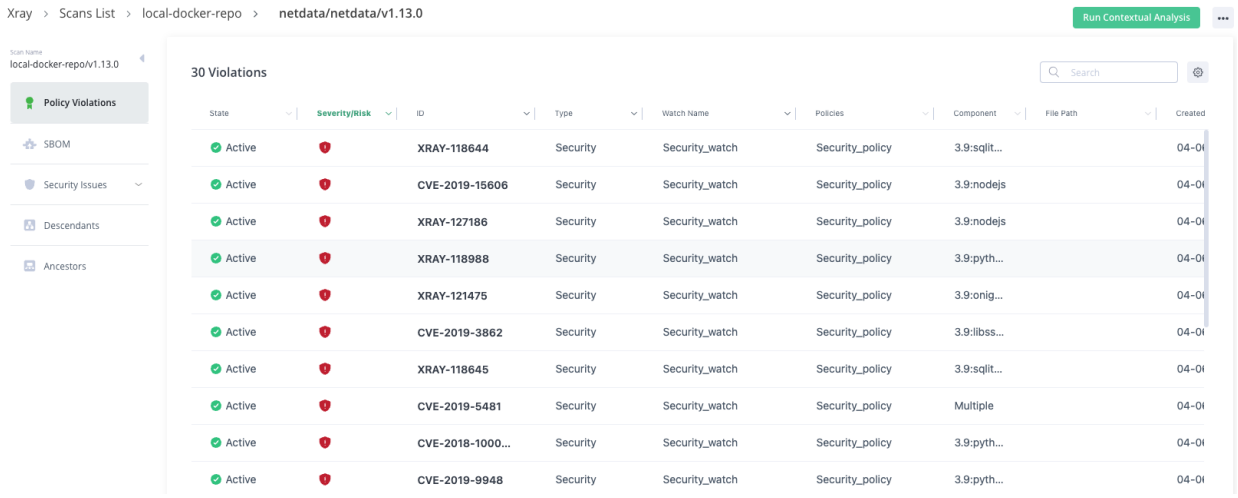
Select a docker image from the list of available images on your laptop and push it.
See how the image is uploaded to Artifactory.

Note: If you do not have one in your workstation, run in your terminal: " `docker pull netdata/netdata:v1.13.0`*"*
The examples below are using the public netdata image.

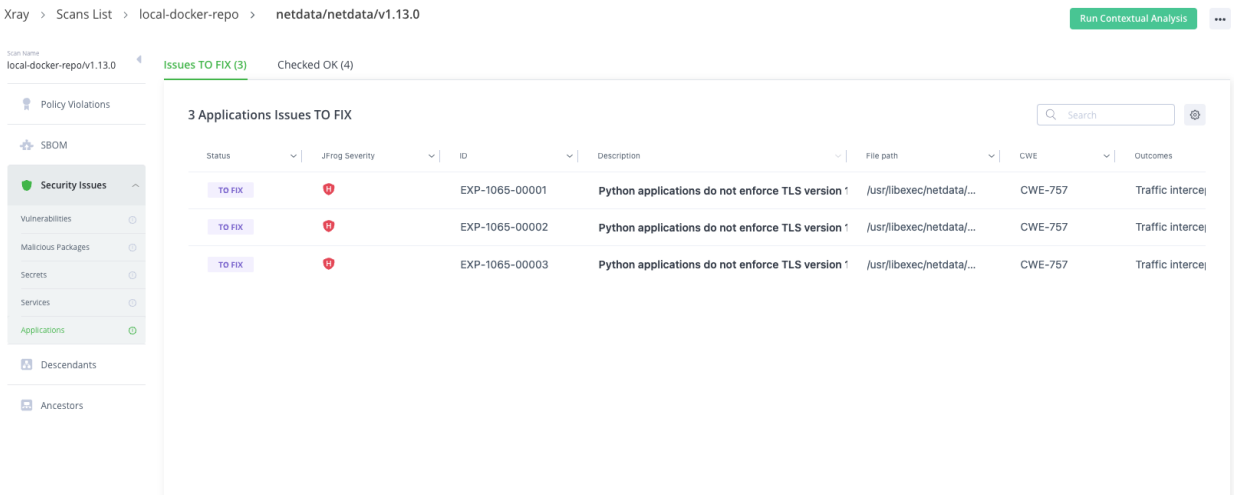
Your browser will be opened to your server's scan results page (results may take up to 5 min to complete).

```
Enter Docker image name and then its tag:
==========================================
Enter the Docker image name (REPOSITORY column): netdata/netdata
Enter the Docker tag: v1.13.0

The push refers to repository [qawsed.jfrog.io/local-docker-repo/netdata/netdata]
ac38a3b29247: Pushed
60686b1e5f0b: Pushed
d747aad1e779: Pushed
12883d4f59a9: Pushed
db7169781f22: Pushed
v1.13.0: digest: sha256:a59b97ac29435a7ba44317a4c560212ffd58475737f083d1233810102b49b68d size: 1373

[+] Docker push operation is complete, running SCA... opening the web browser in 30 seconds
    IMPORTANT: Please note JAS analyis might take up to 5 minutes
[==============================] 30/30 seconds

Docker image pushed to JFrog Platform!
```

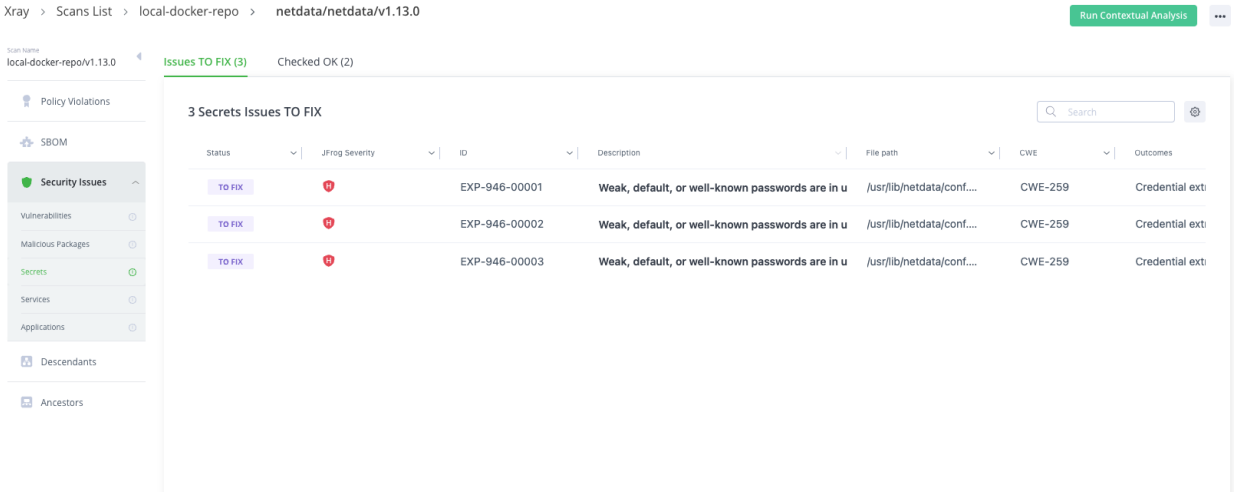
7. How many CVEs can be found in your selected docker images?
8. Do you see any High/Critical CVEs that are not applicable? Why?
9. Does your selected image have any Policy violations?



10. Does your selected image have any application exposures?



11. Does your selected image have any secrets detected?



Congratulations! You have completed Lab 2

Phase #3 - Advanced

12. Browse through the PDF in your guided trial folder and read/experiment with the system other capabilities and features
13. Push additional popular docker hub images to view the results
    a. `mvila/npm-addict:production` - This image has a malicious package.
    b. `bkimminich/juice-shop` - This has Application and Secret Exposures.
    c. `nginxdemos/hello:latest` - This has Service Exposures (nginx)

Xray › Scans List › **local-docker-repo**

Artifacts

Search

Artifact Name	Violations	Malicious Packages	Vulnerabilities	Exposures	Repository Path	Created On
bkimminich/juice-shop/latest	0	✓	53	6	/bkimminich/juice-shop/latest/manifest.json	2023-06-04T08:39:08Z
mvila/npm-addict/production	9	a	71	1	/mvila/npm-addict/production/manifest.json	2023-06-04T08:35:11Z
nginxdemos/hello/latest	1	✓	9	5	/nginxdemos/hello/latest/manifest.json	2023-06-04T08:32:28Z
netdata/netdata/v1.13.0	30	✓	429	6	/netdata/netdata/v1.13.0/manifest.json	2023-06-04T06:16:34Z