

## 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
```

```
Welcome to JFrog trial setup!
=====
1. Configure the instance new or existing
2. Docker login to existing trial from a new workstation
3. Pull Docker image or select sample docker image
4. Push Docker image from local machine to scan with JAS
5. Exit

Please select an option: 3

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
```

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:e24bc4f41034c28b6a08aba94507a169ae23f2b87899e225a3d18fe8c36d26f5
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 analysis 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

```
Welcome to JFrog trial setup!

=====
1. Configure the instance new or existing
2. Docker login to existing trial from a new workstation
3. Pull Docker image or select sample docker image
4. Push Docker image from local machine to scan with JAS
5. Exit

Please select an option: 4

Push Docker image from local machine to scan with JAS:

=====
Listing available docker images on local machine:

REPOSITORY                                TAG          IMAGE ID      CREATED        SIZE
docker/disk-usage-extension                0.2.7        d2973444a992  5 weeks ago   2.81MB
netdata/netdata                           latest       39817e709c76  6 weeks ago   382MB
jfrog/jfrog-docker-desktop-extension      1.2.1        81a26272260a  9 months ago  82.3MB
webgoat/webgoat-8.0                       latest       6664051b8808  3 years ago   380MB
vulhub/log4j                              2.8.1        3b6452a32dc9  5 years ago   207MB

Enter Docker image name and then its tag:

=====
Enter the Docker image name (REPOSITORY column):
```

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 analys 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?

Xray > Scans List > local-docker-repo > netdata/netdata/v1.13.0 Run Contextual Analysis

Scan Name: local-docker-repo/v1.13.0

**Policy Violations**

SBOM

Security Issues

Descendants

Ancestors

### 30 Violations

State	Severity/Risk	ID	Type	Watch Name	Policies	Component	File Path	Created
Active	High	XRAY-118644	Security	Security_watch	Security_policy	3.9:sqlit...		04-01
Active	High	CVE-2019-15606	Security	Security_watch	Security_policy	3.9:nodejs		04-01
Active	High	XRAY-127186	Security	Security_watch	Security_policy	3.9:nodejs		04-01
Active	High	XRAY-118988	Security	Security_watch	Security_policy	3.9:pyth...		04-01
Active	High	XRAY-121475	Security	Security_watch	Security_policy	3.9:onig...		04-01
Active	High	CVE-2019-3862	Security	Security_watch	Security_policy	3.9:libss...		04-01
Active	High	XRAY-118645	Security	Security_watch	Security_policy	3.9:sqlit...		04-01
Active	High	CVE-2019-5481	Security	Security_watch	Security_policy	Multiple		04-01
Active	High	CVE-2018-1000...	Security	Security_watch	Security_policy	3.9:pyth...		04-01
Active	High	CVE-2019-9948	Security	Security_watch	Security_policy	3.9:pyth...		04-01

## 10. Does your selected image have any application exposures?

Xray > Scans List > local-docker-repo > netdata/netdata/v1.13.0 Run Contextual Analysis

Scan Name: local-docker-repo/v1.13.0 **Issues TO FIX (3)** Checked OK (4)

Policy Violations

SBOM

**Security Issues**

Vulnerabilities

Malicious Packages

Secrets

Services

**Applications**

Descendants

Ancestors

### 3 Applications Issues TO FIX

Status	Jfrog Severity	ID	Description	File path	CWE	Outcomes
TO FIX	High	EXP-1065-00001	Python applications do not enforce TLS version 1	/usr/libexec/netdata/...	CWE-757	Traffic interce
TO FIX	High	EXP-1065-00002	Python applications do not enforce TLS version 1	/usr/libexec/netdata/...	CWE-757	Traffic interce
TO FIX	High	EXP-1065-00003	Python applications do not enforce TLS version 1	/usr/libexec/netdata/...	CWE-757	Traffic interce

## 11. Does your selected image have any secrets detected?

Xray > Scans List > local-docker-repo > netdata/netdata/v1.13.0 Run Contextual Analysis

Scan Name: local-docker-repo/v1.13.0 **Issues TO FIX (3)** Checked OK (2)

Policy Violations

SBOM

**Security Issues**

Vulnerabilities

Malicious Packages

**Secrets**

Services

Applications

Descendants

Ancestors

### 3 Secrets Issues TO FIX

Status	Jfrog Severity	ID	Description	File path	CWE	Outcomes
TO FIX	High	EXP-946-00001	Weak, default, or well-known passwords are in u	/usr/lib/netdata/conf...	CWE-259	Credential ext
TO FIX	High	EXP-946-00002	Weak, default, or well-known passwords are in u	/usr/lib/netdata/conf...	CWE-259	Credential ext
TO FIX	High	EXP-946-00003	Weak, default, or well-known passwords are in u	/usr/lib/netdata/conf...	CWE-259	Credential ext

**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)

Artifacts



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		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

