

Lab Exercise 22- Docker Image Vulnerability

Scanning Using Trivy (Windows)

Name: Vishal Pandey

SAP ID: 500125280

Batch 2 DevOps

Objective

By the end of this lab, you will be able to:

- Install and configure **Trivy** on Windows
 - Scan **Docker images** for vulnerabilities
 - Interpret scan reports and take remediation actions
-

Prerequisites

- Windows 10/11 (with **Docker Desktop** installed and running)
 - Internet access (Trivy downloads vulnerability databases)
 - Basic familiarity with Docker CLI commands
-

Step 1: Verify Docker Setup

Before using Trivy, make sure Docker is working correctly.

```
docker --version
```

```
docker run hello-world
```

Expected Output:

Docker runs successfully and displays the “Hello from Docker!” message.

Step 2: Install Trivy on Windows

Manual Installation

1. Go to the official GitHub releases page:
<https://github.com/aquasecurity/trivy/releases>
2. Download the Windows ZIP file (trivy_x.x.x_windows_amd64.zip)
3. Extract it (e.g., to C:\trivy)
4. Add that folder to your **System PATH** environment variable

Verify Installation

Open **PowerShell** and run:

```
trivy --version
```

Expected Output: Trivy version and build information.

Step 3: Pull a Docker Image

Let’s pull an image that we’ll scan:

```
docker pull nginx:latest
```

Check it's downloaded:

```
docker images
```

Step 4: Scan Docker Image with Trivy

Now, run a vulnerability scan on the image:

```
trivy image nginx:latest
```

Explanation:

Trivy will:

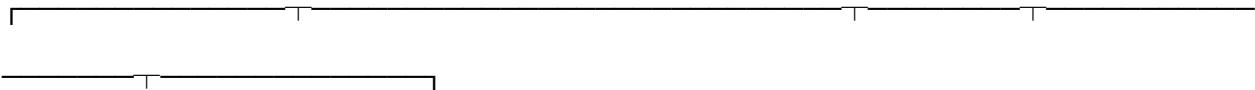
- Fetch the latest vulnerability database
- Analyze all OS packages and libraries inside the image
- Display severity levels (LOW, MEDIUM, HIGH, CRITICAL)

Sample Output

```
nginx:latest (debian 12.2)
```

```
=====
```

```
Total: 12 (LOW: 2, MEDIUM: 4, HIGH: 5, CRITICAL: 1)
```



PACKAGE	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION
openssl	CVE-2023-0464	HIGH	3.0.9-1	3.0.9-2
zlib	CVE-2022-37434	MEDIUM	1.2.11-5	1.2.12

```
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

nginx:latest (debian 13.2)
=====
Total: 95 (UNKNOWN: 5, LOW: 84, MEDIUM: 5, HIGH: 1, CRITICAL: 0)

+-----+-----+-----+-----+-----+
| Library | Vulnerability | Severity | Status | Installed Version | Fixed Version |
+-----+-----+-----+-----+-----+
| apt     | CVE-2011-3374 | LOW      | affected | 3.0.3           | It was fo... |
| und that apt-key in apt, all versions, do not... |
| ...    |                 |           |          |                 | correctly   |
| vd.aquasec.com/nvd/cve-2011-3374               |           |           |                 | https://a... |
+-----+-----+-----+-----+-----+
| bash    | TEMP-0841856-B18BAF | [Privileg... | 5.2.37-2+b5 | https://s... |
| e escalation possible to other user than root] |
| security-tracker.debian.org/tracker/TEMP-0841856-B1-... |
|                                |           |           |                 | 8BAF        |
+-----+-----+-----+-----+-----+
| bsdutils | CVE-2022-0563 | 1:2.41-5 | util-linu... |
| x: partial disclosure of arbitrary files in chfn... |
| when compiled... |           |           | and chsh   |
+-----+-----+-----+-----+-----+
```

Step 5: Save Report to a File

You can export the results in different formats.

Save as a text file:

```
trivy image nginx:latest > nginx_scan.txt
```

```
PS C:\Users\ASUS> trivy image nginx:latest > nginx_scan.txt
2025-11-24T18:07:32+05:30      INFO    [vuln] Vulnerability scanning is enabled
2025-11-24T18:07:32+05:30      INFO    [secret] Secret scanning is enabled
2025-11-24T18:07:32+05:30      INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-24T18:07:32+05:30      INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-24T18:07:32+05:30      INFO    Detected OS family="debian" version="13.2"
2025-11-24T18:07:32+05:30      INFO    [debian] Detecting vulnerabilities... os_version="13" pkg_num=150
2025-11-24T18:07:32+05:30      INFO    Number of language-specific files num=0
2025-11-24T18:07:32+05:30      WARN   Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-selection for details.
```

⚠️ Notices:

- Version 0.67.2 of Trivy is now available, current version is 0.67.0

To suppress version checks, run Trivy scans with the --skip-version-check flag

```
PS C:\Users\ASUS>
```

Save as a JSON report:

```
trivy image --format json -o nginx_scan.json nginx:latest
```

Tip: JSON format is useful for automation or CI/CD integration.

```
PS C:\Users\ASUS> trivy image --format json -o nginx_scan.json nginx:latest
2025-11-24T18:05:47+05:30      INFO    [vuln] Vulnerability scanning is enabled
2025-11-24T18:05:47+05:30      INFO    [secret] Secret scanning is enabled
2025-11-24T18:05:47+05:30      INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-24T18:05:47+05:30      INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-24T18:05:47+05:30      INFO    Detected OS family="debian" version="13.2"
2025-11-24T18:05:47+05:30      INFO    [debian] Detecting vulnerabilities... os_version="13" pkg_num=150
2025-11-24T18:05:47+05:30      INFO    Number of language-specific files num=0
2025-11-24T18:05:47+05:30      WARN   Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-selection for details.

⚠️ Notices:
- Version 0.67.2 of Trivy is now available, current version is 0.67.0

To suppress version checks, run Trivy scans with the --skip-version-check flag
PS C:\Users\ASUS> |
```

Step 6: Scan a Local Image

If you've built your own Docker image:

```
docker build -t myapp:1.0 .
```

```
trivy image myapp:1.0
```

```
PS C:\Users\ASUS> docker build -t myapp:1.0 .
[+] Building 0.3s (1/1) FINISHED docker:desktop-linux
=> [internal] load build definition from Dockerfile      0.2s
=> => transferring dockerfile: 2B                         0.1s
ERROR: failed to build: failed to solve: failed to read dockerfile: open Dockerfile: no such file or directory
PS C:\Users\ASUS> trivy image myapp:1.0
2025-11-24T18:01:47+05:30      INFO    [vuln] Vulnerability scanning is enabled
2025-11-24T18:01:47+05:30      INFO    [secret] Secret scanning is enabled
2025-11-24T18:01:47+05:30      INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-24T18:01:47+05:30      INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection

⚠ Notices:
- Version 0.67.2 of Trivy is now available, current version is 0.67.0

To suppress version checks, run Trivy scans with the --skip-version-check flag
```

Step 7: Update Vulnerability Database

Keep Trivy's database up-to-date:

```
trivy image --download-db-only
```

Step 8: Clean Up

Remove images (optional):

```
docker rmi nginx:latest
```