# Lab Exercise 22- Docker Image Vulnerability Scanning Using Trivy (Windows)

**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
```

```
C:\Users\Devanshi>docker --version
Docker version 28.3.2, build 578ccf6

C:\Users\Devanshi>docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
17eec7bbc9d7: Pull complete
Digest: sha256:f7931603f70e13dbd844253370742c4fc4202d290c80442b2e68706d8f33ce26
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.
```

*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

```
C:\Users\Devanshi>trivy -v
Version: 0.67.2
```

*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

```
C:\Users\Devanshi>docker pull nginx:latest
latest: Pulling from library/nginx
e2f8e296d9df: Pull complete
266626526d42: Pull complete
52bc359bcbd7: Pull complete
d921c57c6a81: Pull complete
320b0949be89: Pull complete
d7ecded7702a: Pull complete
9def903993e4: Pull complete
Digest: sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad
Status: Downloaded newer image for nginx:latest
docker.io/library/nginx:latest
```

Check it's downloaded:

docker images

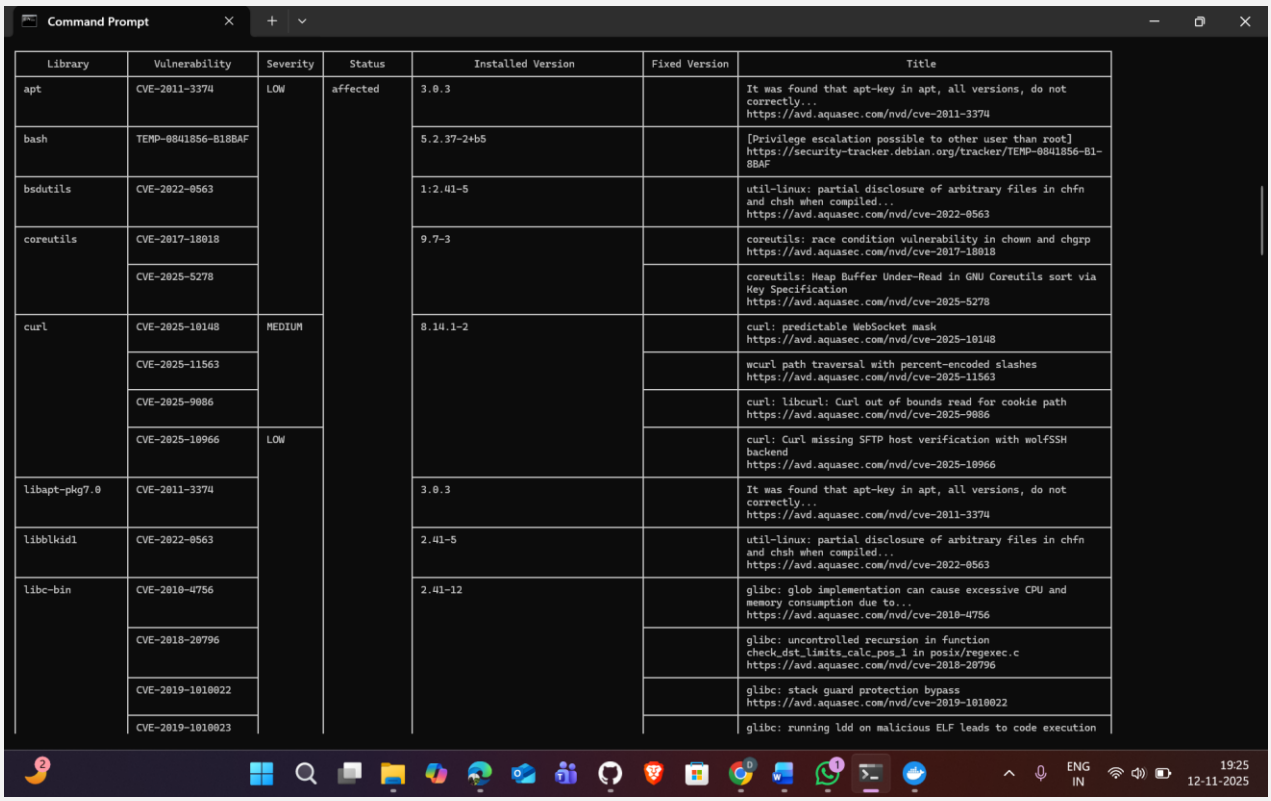
```
C:\Users\Devanshi>docker images
REPOSITORY       TAG       IMAGE ID       CREATED         SIZE
demo_app_try     latest    dbc88214f43f   34 hours ago    80.1MB
nginx            latest    1beed3ca46ac   8 days ago      225MB
nginx-html-app   latest    c39bf9b0a630   2 weeks ago     225MB
hello-world      latest    f7931603f70e   3 months ago    20.3kB
```

---

**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      │
└──────────────┴────────────────┴──────────┴────────────────┴─────────────┘
```

**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
```

**Save as a JSON report:**

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

```
C:\Users\Devanshi>trivy image --format json -o nginx_scan.json nginx:latest
2025-11-12T19:26:50+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-12T19:26:50+05:30       INFO    [secret] Secret scanning is enabled
2025-11-12T19:26:50+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-12T19:26:50+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-12T19:26:51+05:30       INFO    Detected OS     family="debian" version="13.1"
2025-11-12T19:26:51+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-12T19:26:51+05:30       INFO    Number of language-specific files       num=0
2025-11-12T19:26:51+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-sel
ection for details.
```

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

---

### 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
```

---

### Step 7: Update Vulnerability Database

Keep Trivy's database up-to-date:

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

```
C:\Users\Devanshi>trivy image --download-db-only
2025-11-19T10:07:05+05:30       INFO    [vulndb] Need to update DB
2025-11-19T10:07:05+05:30       INFO    [vulndb] Downloading vulnerability DB...
2025-11-19T10:07:05+05:30       INFO    [vulndb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-db:2"
75.26 MiB / 75.26 MiB [-------------------------------------------------------------------------------] 100.00% 910.94 KiB p/s 1m25s
2025-11-19T10:08:33+05:30       INFO    [vulndb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-db:2"
```

---

**Step 8: Clean Up**

Remove images (optional):

docker rmi nginx:latest

```
C:\Users\Devanshi>docker rmi nginx:latest
Untagged: nginx:latest
Deleted: sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad
```