

## Lab Exercise 22- Docker Image Vulnerability

### Scanning Using Trivy (Windows)

#### Step 1: Verify Docker Setup

Before using Trivy, make sure Docker is working correctly.

```
C:\Users\shivam>docker version
Client:
  Version:          28.5.1
  API version:      1.51
  Go version:       go1.24.8
  Git commit:       e180ab8
  Built:            Wed Oct  8 12:19:16 2025
  OS/Arch:          windows/amd64
  Context:          desktop-linux

Server: Docker Desktop 4.50.0 (209931)
Engine:
  Version:          28.5.1
  API version:      1.51 (minimum version 1.24)
  Go version:       go1.24.8
  Git commit:       f8215cc
  Built:            Wed Oct  8 12:17:24 2025
  OS/Arch:          linux/amd64
  Experimental:    false
containerd:
  Version:          1.7.27
  GitCommit:        05044ec0a9a75232cad458027ca83437aae3f4da
runc:
  Version:          1.2.5
  GitCommit:        v1.2.5-0-g59923ef
docker-init:
  Version:          0.19.0
  GitCommit:        de40ad0
```

*Expected Output:*

```
C:\Users\shivam>docker run hello-world
Hello from Docker!
This message shows that your installation appears to be working correctly.
```

## Step 2: Install Trivy on Windows

```
PS C:\Users\shivam> docker run --rm aquasec/trivy:latest --version
Version: 0.67.2
PS C:\Users\shivam> |
```

---

## Step 3: Pull a Docker Image

```
PS C:\Users\shivam> docker pull nginx:latest
latest: Pulling from library/nginx
Digest: sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad
Status: Image is up to date for nginx:latest
docker.io/library/nginx:latest
PS C:\Users\shivam> docker images
REPOSITORY          TAG      IMAGE ID      CREATED       SIZE
nginx-html-app     latest   2ac5d9252524  About an hour ago  225MB
nginx              latest   1beed3ca46ac   4 days ago    225MB
aquasec/trivy      latest   e2b22eac59c0   4 weeks ago   239MB
hello-world        latest   56433a6be3fd   3 months ago  20.3kB
PS C:\Users\shivam> |
```

---

## Step 4: Scan Docker Image with Trivy

```
PS C:\Users\shivam> docker run --rm -v /var/run/docker.sock:/var/run/docker.sock aquasec/trivy image nginx:latest
2025-11-08T14:26:29Z    INFO    [vulndb] Need to update DB
2025-11-08T14:26:29Z    INFO    [vulndb] Downloading vulnerability DB...
2025-11-08T14:26:29Z    INFO    [vulndb] Downloading artifact...           repo="mirror.gcr.io/aquasec/trivy-db:2"
175.25 KiB / 74.30 MiB [>-----] 0.23% ? p/s ?975.25 KiB / 74.
```

## Report Summary

Target	Type	Vulnerabilities	Secrets
nginx:latest (debian 13.1)	debian	98	-

### Legend:

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

nginx:latest (debian 13.1)

=====

Total: 98 (UNKNOWN: 0, LOW: 84, MEDIUM: 12, HIGH: 2, CRITICAL: 0)

## Step 5: Save Report to a File

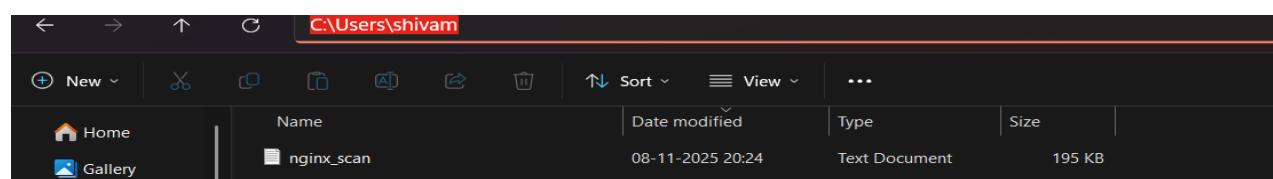
```
PS C:\Users\shivam> docker run --rm -v "C:\Users\shivam:/root/.cache/" -v /var/run/docker.sock:/var/run/docker.sock aquasec/trivy image nginx:latest > C:\Users\shivam\nginx_scan.txt
2025-11-08T14:52:02Z INFO [vulndb] Need to update DB
2025-11-08T14:52:02Z INFO [vulndb] Downloading vulnerability DB...
2025-11-08T14:52:02Z INFO [vulndb] Downloading artifact... repo="mirror.gcr.io/aquasec/trivy-db:2"
```

```
.gcr.io/aquasec/trivy-java-db:1"
2025-11-08T14:54:27Z INFO [javadb] Java DB is cached for 3 days. If you want to update the database, clear the DB cache.
2025-11-08T14:54:27Z INFO [javadb] Detected OS family="debian" version="13.1"
2025-11-08T14:54:27Z INFO [javadb] Detecting vulnerabilities... os_version="13" pkg_num=150
2025-11-08T14:54:27Z INFO [javadb] Number of language-specific files num=0
2025-11-08T14:54:27Z WARN [javadb] Using severities from other vendors for some vulnerabilities. Read https://trivy-selection for details.
PS C:\Users\shivam> Z|
```

```
PS C:\Users\shivam> docker run --rm -v "C:\Users\shivam:/root/.cache/" -v /var/run/docker.sock:/var/run/docker.sock aquasec/trivy image --format json --o /nginx_scan.json nginx:latest
2025-11-08T14:55:24Z INFO [vuln] Vulnerability scanning is enabled
2025-11-08T14:55:24Z INFO [secret] Secret scanning is enabled
2025-11-08T14:55:24Z INFO [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-08T14:55:24Z INFO [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-08T14:55:24Z INFO [javadb] Detected OS family="debian" version="13.1"
2025-11-08T14:55:24Z INFO [javadb] Detecting vulnerabilities... os_version="13" pkg_num=150
2025-11-08T14:55:24Z INFO [javadb] Number of language-specific files num=0
2025-11-08T14:55:24Z WARN [javadb] Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-selection for details.
PS C:\Users\shivam> |
```

Save as a text file:

Save as a JSON report:



## Step 6: Scan a Local Image

If you've built your own Docker image:

```
PS D:\sem5\devops 5th sem _lab\nginx-html-app> docker build -t myapp:1.0 .
[+] Building 0.4s (7/7) FINISHED
=> [internal] load build definition from Dockerfile
=> => transferring dockerfile: 106B
=> [internal] load metadata for docker.io/library/nginx:latest
=> [internal] load .dockerignore
    => ignoring: .dockerignore: 0B
```

```
[+] Unpacking to docker://library/myapp:1.0
PS D:\sem5\devops 5th sem _lab\nginx-html-app> docker run --rm -v /var/run/docker.sock:/var/run/docker.sock aquasec/trivy image myapp:1.0
2025-11-08T15:00:53Z    INFO    [vulndb] Need to update DB
2025-11-08T15:00:53Z    INFO    [vulndb] Downloading vulnerability DB...
2025-11-08T15:00:53Z    INFO    [vulndb] Downloading artifact...          repo="mirror.gcr.io/aquasec/trivy-db:2"
191.25 KiB / 74.30 MiB [>-----] 0.25% ? p/s ?959.17 KiB / 74.30 MiB
```

## Step 7: Update Vulnerability Database

```
PS D:\sem5\devops 5th sem _lab\nginx-html-app> docker run --rm -v /var/run/docker.sock:/var/run/docker.sock aquasec/trivy image nginx:latest
2025-11-08T15:10:46Z    INFO    [vulndb] Need to update DB
2025-11-08T15:10:46Z    INFO    [vulndb] Downloading vulnerability DB...
2025-11-08T15:10:46Z    INFO    [vulndb] Downloading artifact...          repo="mirror.gcr.io/aquasec/trivy-db:2"
159.25 KiB / 74.30 MiB [>-----] 1.13% ? p/s ?1.84 MiB / 74.30 MiB [>-----]
[-----] 0.21% ? p/s ?863.15 KiB / 74.30 MiB [>-----]
[-----] 2.48% ? p/s ?3.25 MiB / 74.30 MiB [>-----]
[-----] 4.37% 5.16 MiB p/s ETA 13s5.12 MiB / 74.30 MiB [>-----] 6.90%
```

## Step 8: Clean Up

Remove images (optional):

```
PS D:\sem5\devops 5th sem _lab\nginx-html-app> docker rmi nginx:latest
Untagged: nginx:latest
Deleted: sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad
PS D:\sem5\devops 5th sem _lab\nginx-html-app> |
```