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

Name-Misha

Batch-2 (DevOps)

SAP ID- 500119679

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)

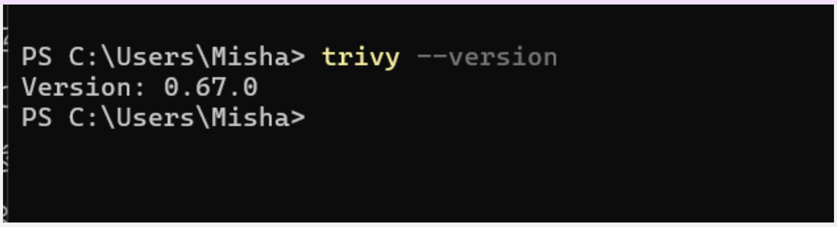
3. Extract it (e.g., to C:\trivy)

4. Add that folder to your **System PATH** environment variable

Verify Installation

Open **PowerShell** and run:

```
trivy –version
```



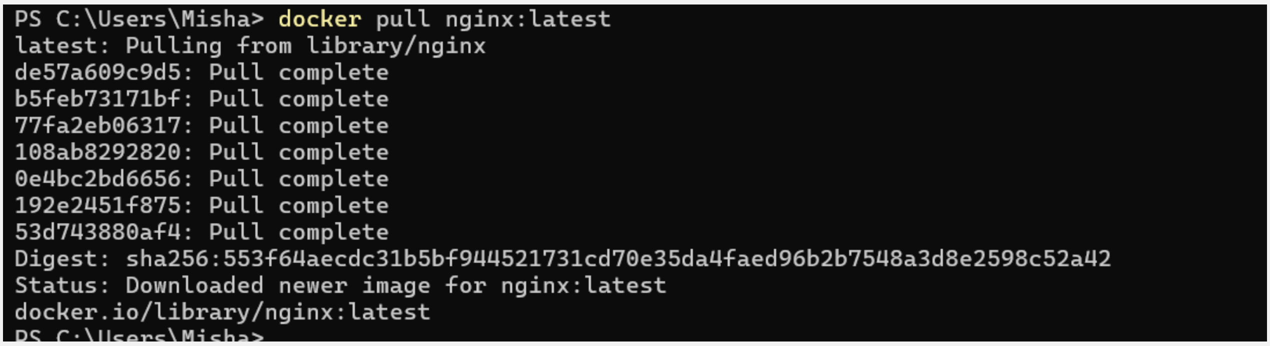
```
PS C:\Users\Misha> trivy --version
Version: 0.67.0
PS C:\Users\Misha>
```

Expected Output: Trivy version and build information.

Step 3: Pull a Docker Image

Let’s pull an image that we’ll scan:

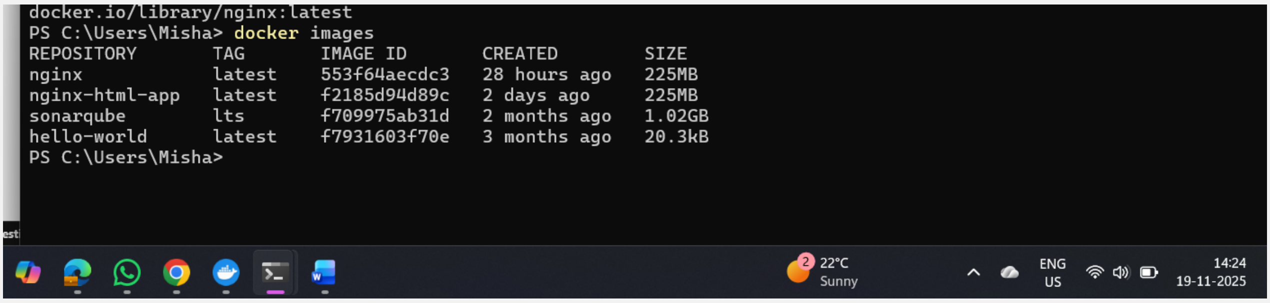
```
docker pull nginx:latest
```



```
PS C:\Users\Misha> docker pull nginx:latest
latest: Pulling from library/nginx
de57a609c9d5: Pull complete
b5feb73171bf: Pull complete
77fa2eb06317: Pull complete
108ab8292820: Pull complete
0e4bc2bd6656: Pull complete
192e2451f875: Pull complete
53d743880af4: Pull complete
Digest: sha256:553f64aecdc31b5bf944521731cd70e35da4faed96b2b7548a3d8e2598c52a42
Status: Downloaded newer image for nginx:latest
docker.io/library/nginx:latest
PS C:\Users\Misha>
```

Check it’s downloaded:

```
docker images
```

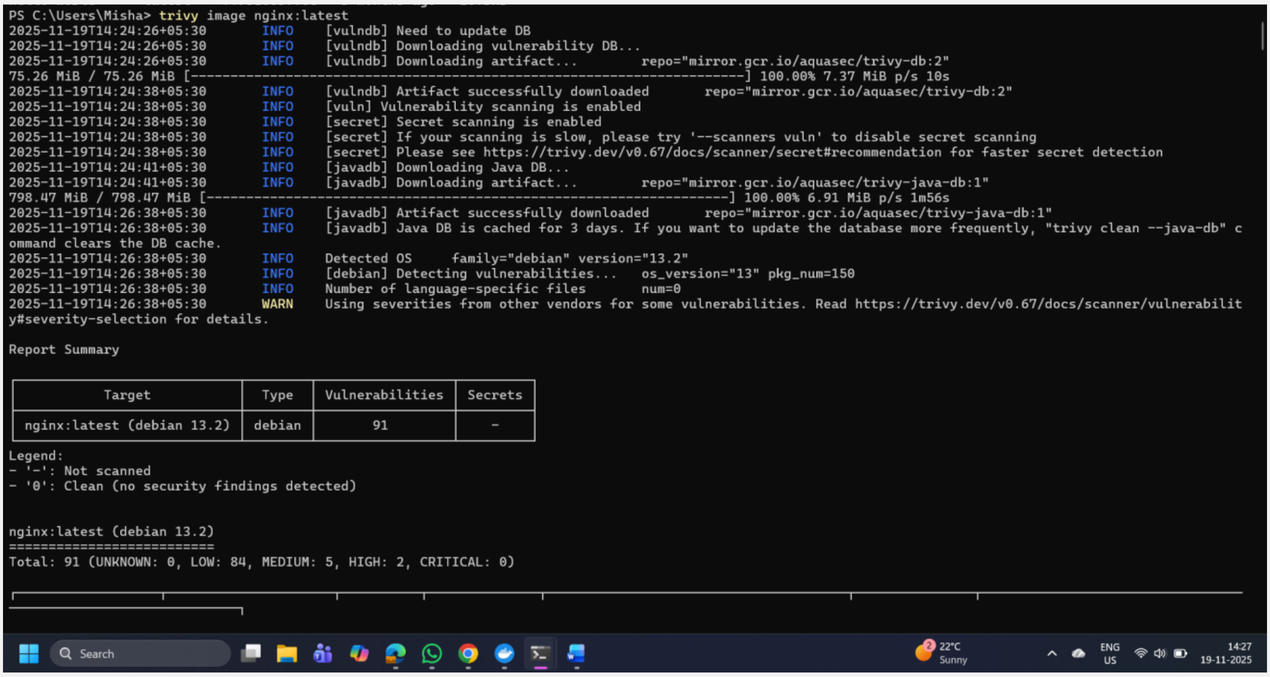


```
docker.io/library/nginx:latest
PS C:\Users\Misha> docker images
REPOSITORY       TAG       IMAGE ID       CREATED         SIZE
nginx            latest    553f64aecdc3   28 hours ago    225MB
nginx-html-app   latest    f2185d94d89c   2 days ago      225MB
sonarqube        lts       f709975ab31d   2 months ago    1.02GB
hello-world      latest    f7931603f70e   3 months ago    20.3kB
PS C:\Users\Misha>
```

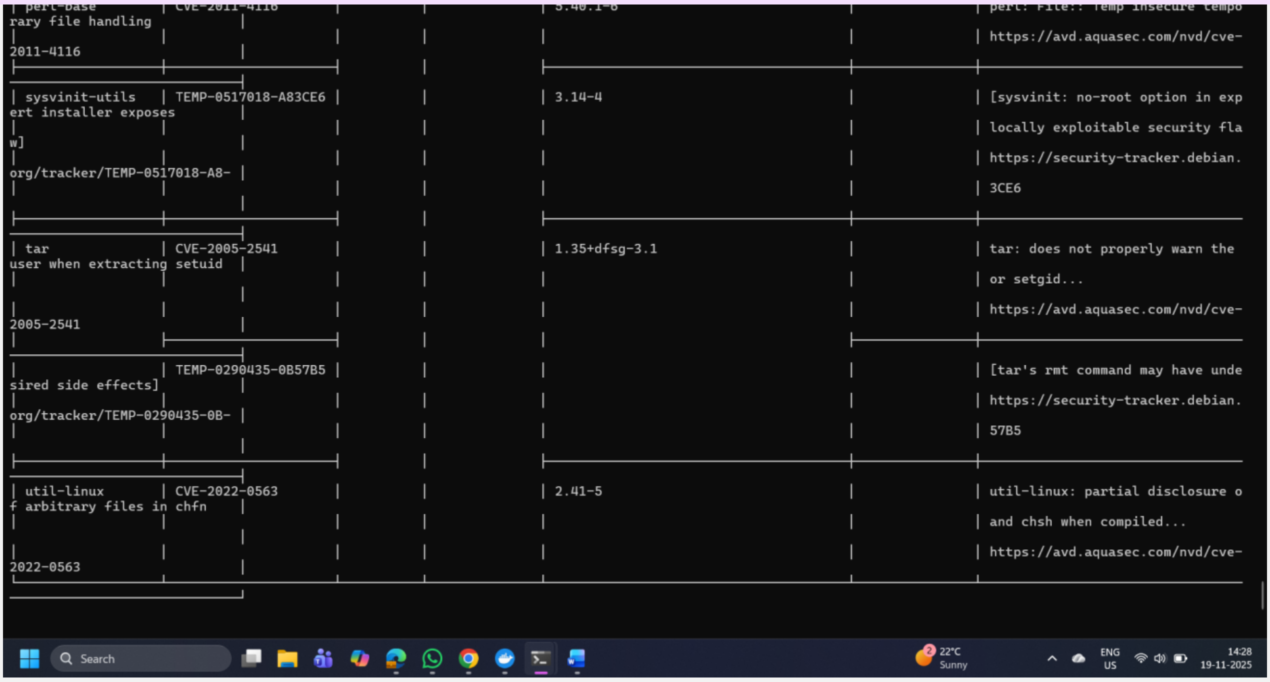
Step 4: Scan Docker Image with Trivy

Now, run a vulnerability scan on the image:

```
trivy image nginx:latest
```



```
PS C:\Users\Misha> trivy image nginx:latest
2025-11-19T14:24:26+05:30       INFO    [vulndb] Need to update DB
2025-11-19T14:24:26+05:30       INFO    [vulndb] Downloading vulnerability DB...
2025-11-19T14:24:26+05:30       INFO    [vulndb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-db:2"
75.26 MiB / 75.26 MiB [-----------------------------------------------------------------] 100.00% 7.37 MiB p/s 10s
2025-11-19T14:24:38+05:30       INFO    [vulndb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-db:2"
2025-11-19T14:24:38+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-19T14:24:38+05:30       INFO    [secret] Secret scanning is enabled
2025-11-19T14:24:38+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-19T14:24:38+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-19T14:24:41+05:30       INFO    [javadb] Downloading Java DB...
2025-11-19T14:24:41+05:30       INFO    [javadb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-java-db:1"
798.47 MiB / 798.47 MiB [-----------------------------------------------------------------] 100.00% 6.91 MiB p/s 1m56s
2025-11-19T14:26:38+05:30       INFO    [javadb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-java-db:1"
2025-11-19T14:26:38+05:30       INFO    [javadb] Java DB is cached for 3 days. If you want to update the database more frequently, "trivy clean --java-db" c
ommand clears the DB cache.
2025-11-19T14:26:38+05:30       INFO    Detected OS     family="debian" version="13.2"
2025-11-19T14:26:38+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-19T14:26:38+05:30       INFO    Number of language-specific files       num=0
2025-11-19T14:26:38+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerabilit
y#severity-selection for details.

Report Summary

┌──────────────────────────┬────────┬─────────────────┬─────────┐
│          Target          │  Type  │ Vulnerabilities │ Secrets │
├──────────────────────────┼────────┼─────────────────┼─────────┤
│ nginx:latest (debian 13.2) │ debian │       91        │    -    │
└──────────────────────────┴────────┴─────────────────┴─────────┘
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


nginx:latest (debian 13.2)
==========================
Total: 91 (UNKNOWN: 0, LOW: 84, MEDIUM: 5, HIGH: 2, CRITICAL: 0)
```



```
│ perl-base        │ CVE-2011-4116      │        │           │ 5.40.1-6                  │          │ perl: File:: Temp insecure tempo
rary file handling        │
│                  │                    │        │           │                           │          │ https://avd.aquasec.com/nvd/cve-
2011-4116                 │
├──────────────────┼────────────────────┤        │           ├───────────────────────────┼──────────┼──────────────────────────────
──────────────────────────┤
│ sysvinit-utils   │ TEMP-0517018-A83CE6 │       │           │ 3.14-4                    │          │ [sysvinit: no-root option in exp
ert installer exposes     │
│                  │                    │        │           │                           │          │ locally exploitable security fla
w]                        │
│                  │                    │        │           │                           │          │ https://security-tracker.debian.
org/tracker/TEMP-0517018-A8- │
│                  │                    │        │           │                           │          │ 3CE6
                          │
├──────────────────┼────────────────────┤        │           ├───────────────────────────┼──────────┼──────────────────────────────
──────────────────────────┤
│ tar              │ CVE-2005-2541      │        │           │ 1.35+dfsg-3.1             │          │ tar: does not properly warn the
user when extracting setuid │
│                  │                    │        │           │                           │          │ or setgid...
                          │
│                  │                    │        │           │                           │          │ https://avd.aquasec.com/nvd/cve-
2005-2541                 │
│                  ├────────────────────┤        │           │                           ├──────────┼──────────────────────────────
──────────────────────────┤
│                  │ TEMP-0290435-0B57B5 │       │           │                           │          │ [tar's rmt command may have unde
sired side effects]       │
│                  │                    │        │           │                           │          │ https://security-tracker.debian.
org/tracker/TEMP-0290435-0B- │
│                  │                    │        │           │                           │          │ 57B5
                          │
├──────────────────┼────────────────────┤        │           ├───────────────────────────┼──────────┼──────────────────────────────
──────────────────────────┤
│ util-linux       │ CVE-2022-0563      │        │           │ 2.41-5                    │          │ util-linux: partial disclosure o
f arbitrary files in chfn │
│                  │                    │        │           │                           │          │ and chsh when compiled...
                          │
│                  │                    │        │           │                           │          │ https://avd.aquasec.com/nvd/cve-
2022-0563                 │
└──────────────────┴────────────────────┴────────┴───────────┴───────────────────────────┴──────────┴──────────────────────────────
──────────────────────────┘
```

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)

┌──────────────┬────────────────────────────┬─────────┬───────────────────┬───────────────┐
```

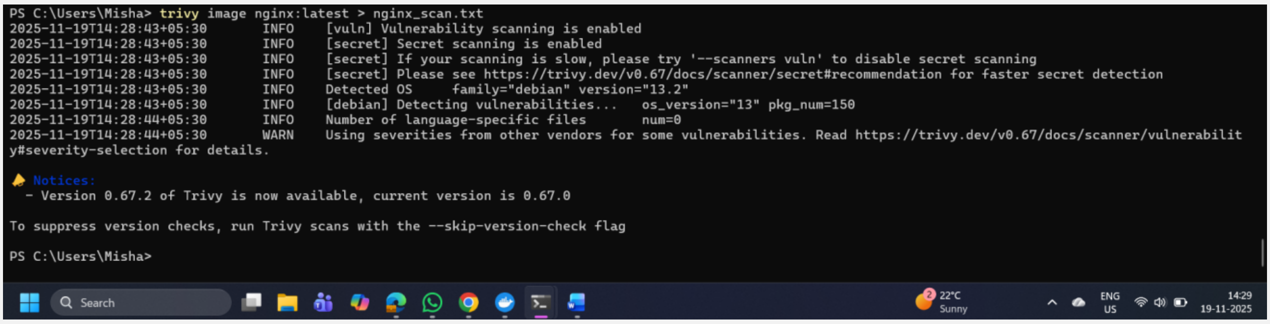
```
| PACKAGE    | VULNERABILITY ID       | SEVERITY | INSTALLED VERSION | FIXED VERSION |

├──────────────┼───────────────────────────┼─────────┼─────────────────┼──────────────┤

| 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:

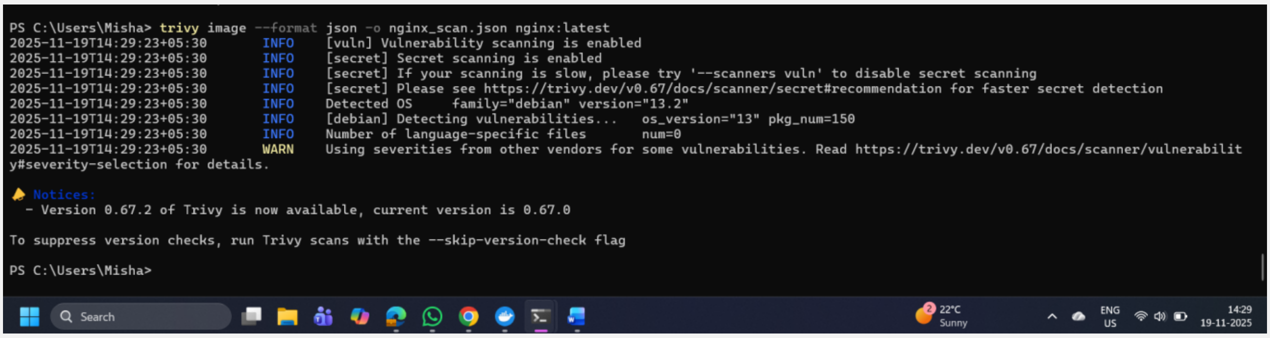
```
trivy image nginx:latest > nginx_scan.txt
```



```
PS C:\Users\Misha> trivy image nginx:latest > nginx_scan.txt
2025-11-19T14:28:43+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-19T14:28:43+05:30       INFO    [secret] Secret scanning is enabled
2025-11-19T14:28:43+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-19T14:28:43+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-19T14:28:43+05:30       INFO    Detected OS     family="debian" version="13.2"
2025-11-19T14:28:43+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-19T14:28:44+05:30       INFO    Number of language-specific files       num=0
2025-11-19T14:28:44+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerabilit
y#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\Misha>
```

Save as a JSON report:

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



```
PS C:\Users\Misha> trivy image --format json -o nginx_scan.json nginx:latest
2025-11-19T14:29:23+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-19T14:29:23+05:30       INFO    [secret] Secret scanning is enabled
2025-11-19T14:29:23+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-19T14:29:23+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-19T14:29:23+05:30       INFO    Detected OS     family="debian" version="13.2"
2025-11-19T14:29:23+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-19T14:29:23+05:30       INFO    Number of language-specific files       num=0
2025-11-19T14:29:23+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerabilit
y#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\Misha>
```

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

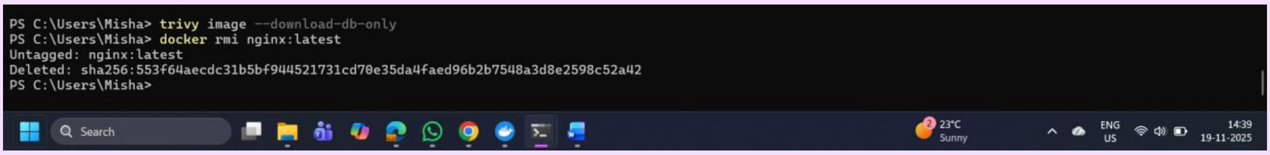
Keep Trivy's database up-to-date:

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

Step 8: Clean Up

Remove images (optional):

```
docker rmi nginx:latest
```



```
PS C:\Users\Misha> trivy image --download-db-only
PS C:\Users\Misha> docker rmi nginx:latest
Untagged: nginx:latest
Deleted: sha256:553f64aecdc31b5bf944521731cd70e35da4faed96b2b7548a3d8e2598c52a42
PS C:\Users\Misha>
```