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

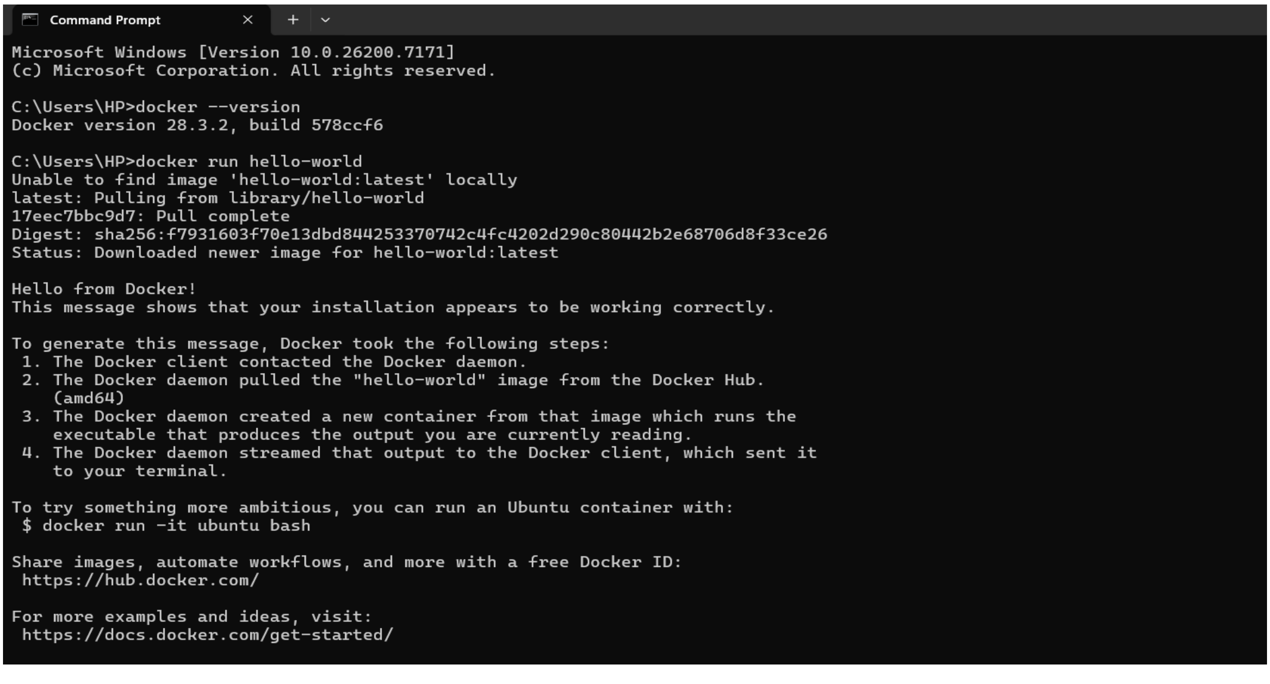
- Windows 10/11 (with **Docker Desktop** installed and running)
- Internet access (Trivy downloads vulnerability databases)
- Basic familiarity with Docker CLI commands

Step 1: Verify Docker Setup

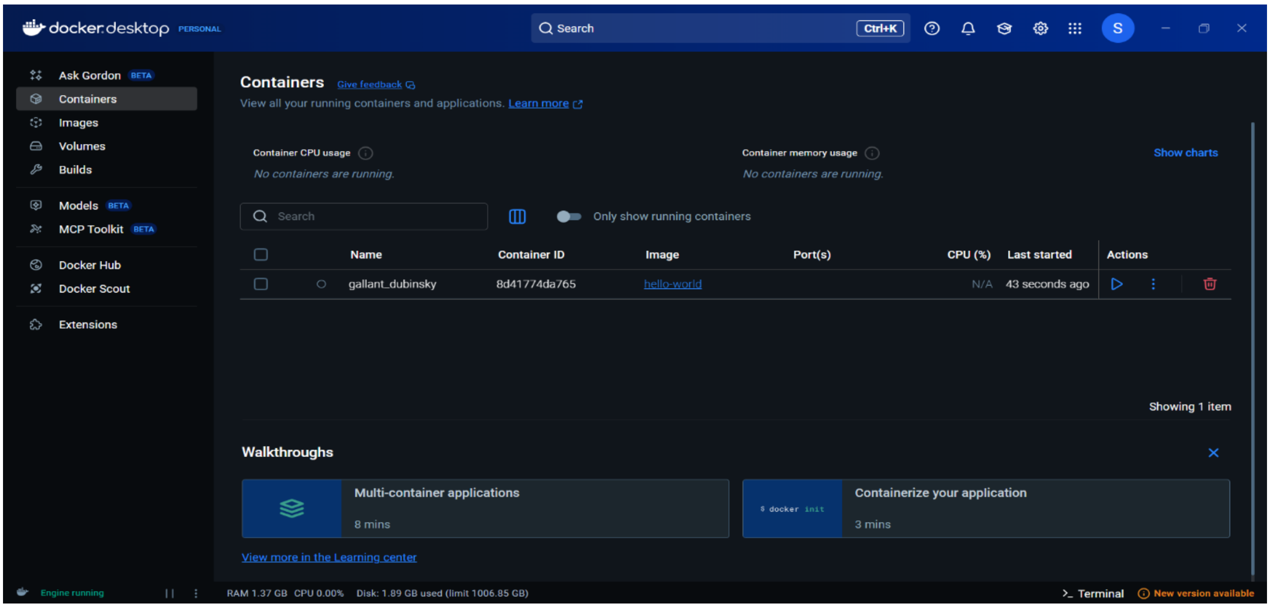
Before using Trivy, make sure Docker is working correctly.

```
docker --version

docker run hello-world
```

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



```
Microsoft Windows [Version 10.0.26200.7171]
(c) Microsoft Corporation. All rights reserved.

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

C:\Users\HP>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.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/
```



	Name	Container ID	Image	Port(s)	CPU (%)	Last started	Actions
□ ○	gallant_dubinsky	8d41774da765	hello-world		N/A	43 seconds ago	

Step 2: Install Trivy on Windows

Manual Installation

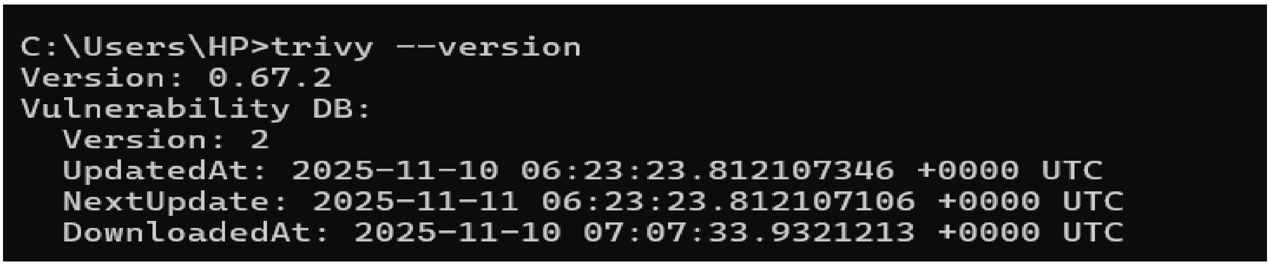
1. Go to the official GitHub releases page: https://github.com/aquasecurity/trivy/releases
2. Download the Windows ZIP file (trivy_x.x.x_windows_amd64.zip)
3. Extract it (e.g., to C:\trivy)
4. Add that folder to your **System PATH** environment variable

Verify Installation

Open **PowerShell** and run:

```
trivy --version
```

Expected Output: Trivy version and build information.



```
C:\Users\HP>trivy --version
Version: 0.67.2
Vulnerability DB:
  Version: 2
  UpdatedAt: 2025-11-10 06:23:23.812107346 +0000 UTC
  NextUpdate: 2025-11-11 06:23:23.812107106 +0000 UTC
  DownloadedAt: 2025-11-10 07:07:33.9321213 +0000 UTC
```

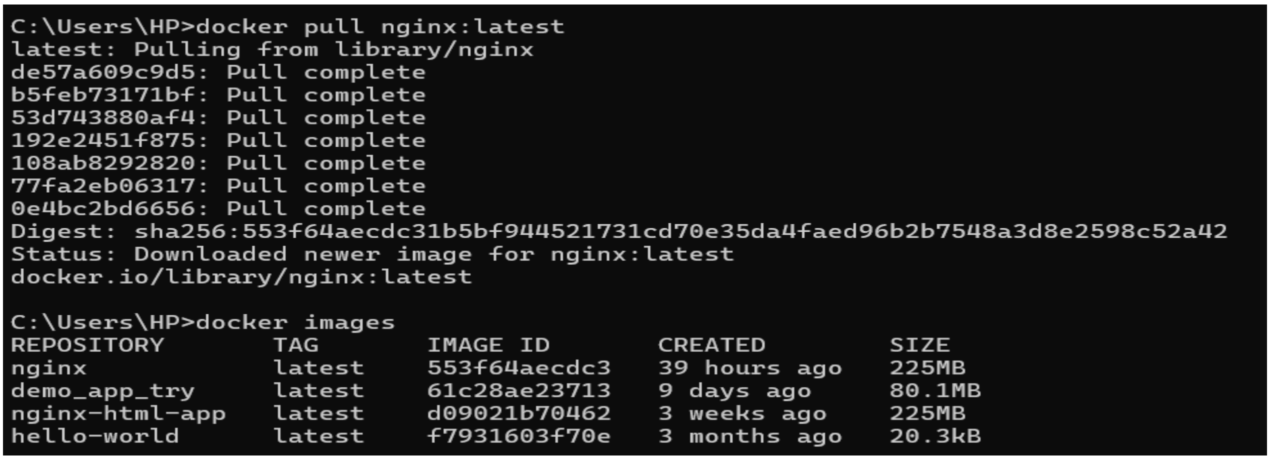
Step 3: Pull a Docker Image

Let’s pull an image that we’ll scan:

```
docker pull nginx:latest
```

Check it's downloaded:

```
docker images
```



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

C:\Users\HP>docker images
REPOSITORY        TAG       IMAGE ID       CREATED        SIZE
nginx             latest    553f64aecdc3   39 hours ago   225MB
demo_app_try      latest    61c28ae23713   9 days ago     80.1MB
nginx-html-app    latest    d09021b70462   3 weeks ago    225MB
hello-world       latest    f7931603f70e   3 months ago   20.3kB
```

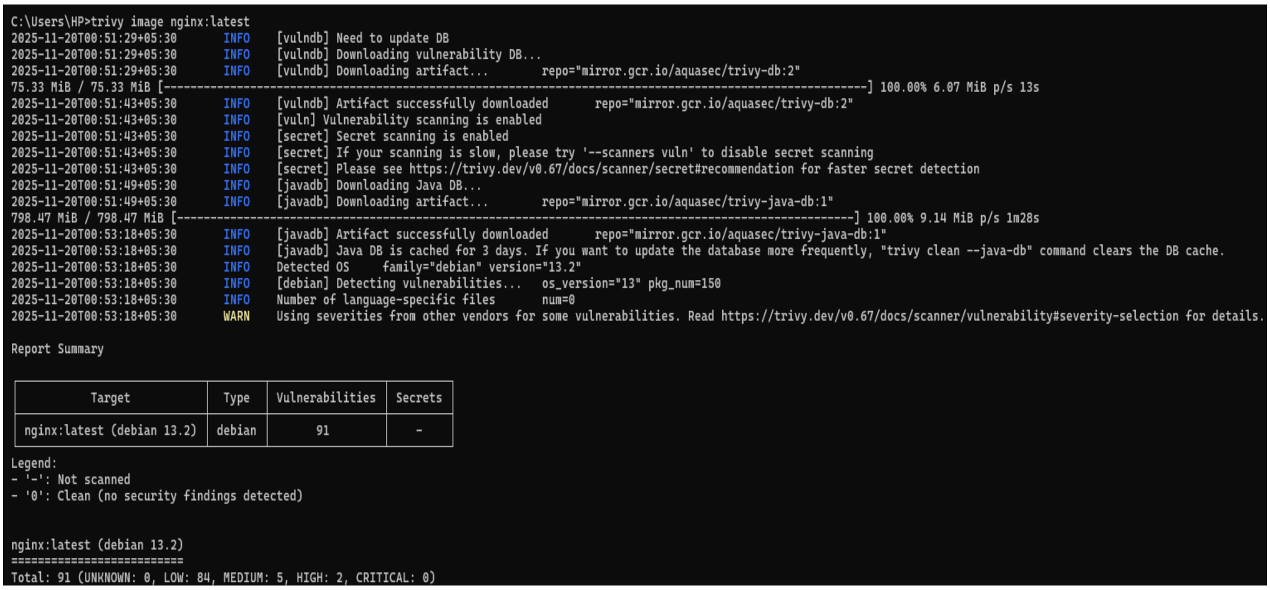
Step 4: Scan Docker Image with Trivy

Now, run a vulnerability scan on the image:

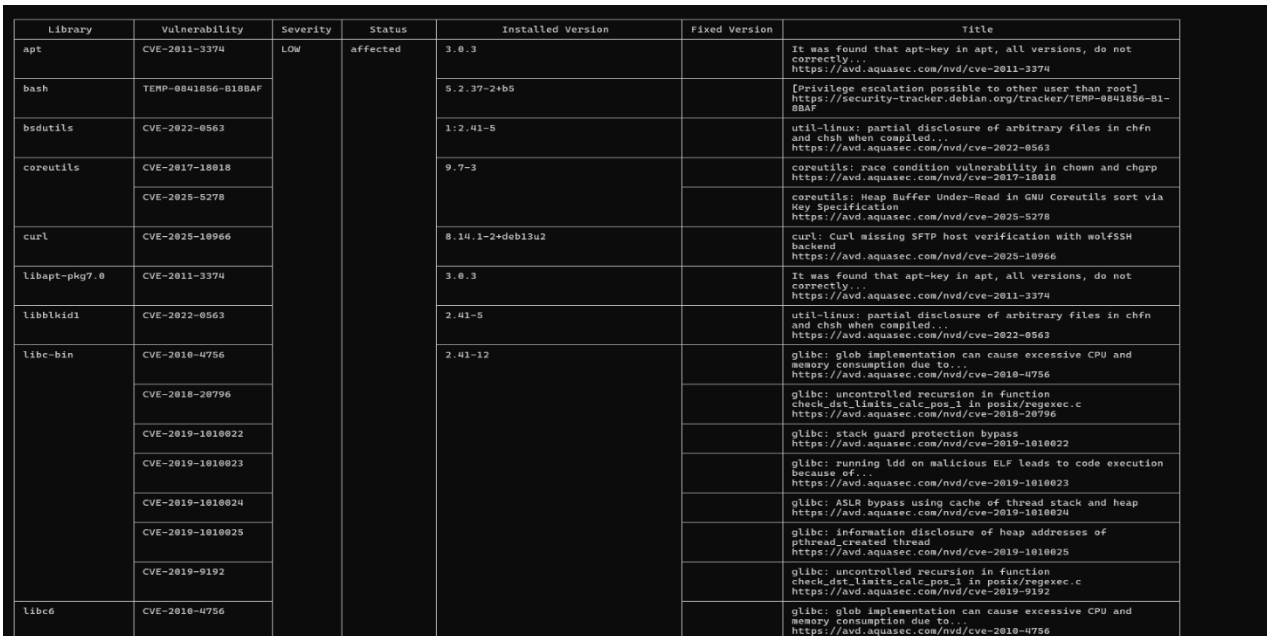
```
trivy image nginx:latest
```

Explanation:
Trivy will:

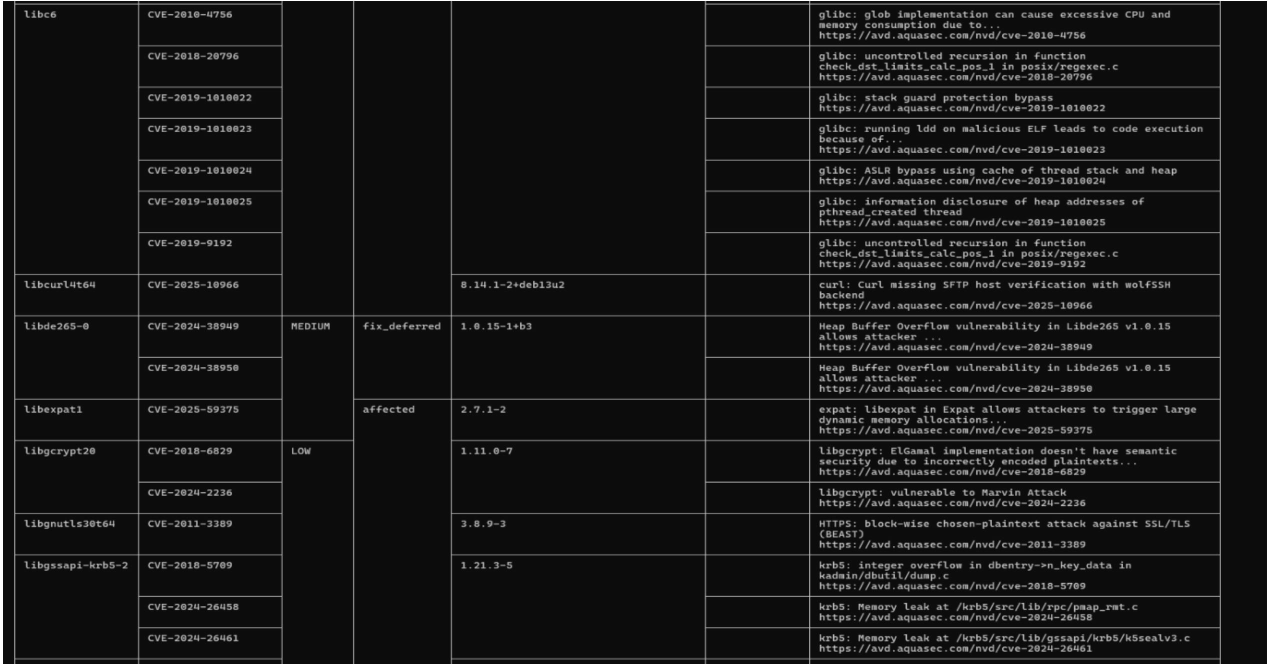
- Fetch the latest vulnerability database
- Analyze all OS packages and libraries inside the image
- Display severity levels (LOW, MEDIUM, HIGH, CRITICAL)



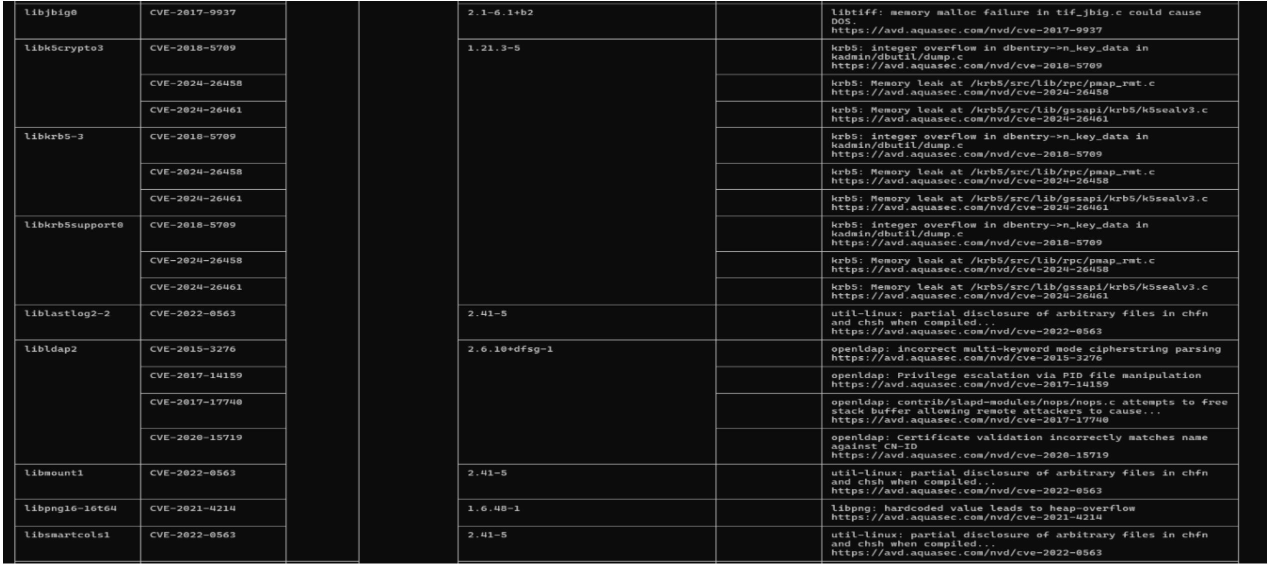
```
C:\Users\HP>trivy image nginx:latest
2025-11-20T00:51:29+05:30       INFO    [vulndb] Need to update DB
2025-11-20T00:51:29+05:30       INFO    [vulndb] Downloading vulnerability DB...
2025-11-20T00:51:29+05:30       INFO    [vulndb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-db:2"
75.33 MiB / 75.33 MiB [------------------------------------------------------------------------------------------------------] 100.00% 6.07 MiB p/s 13s
2025-11-20T00:51:43+05:30       INFO    [vulndb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-db:2"
2025-11-20T00:51:43+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-20T00:51:43+05:30       INFO    [secret] Secret scanning is enabled
2025-11-20T00:51:43+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-20T00:51:43+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-20T00:51:49+05:30       INFO    [javadb] Downloading Java DB...
2025-11-20T00:51:49+05:30       INFO    [javadb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-java-db:1"
798.47 MiB / 798.47 MiB [----------------------------------------------------------------------------------------------------] 100.00% 9.14 MiB p/s 1m28s
2025-11-20T00:53:18+05:30       INFO    [javadb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-java-db:1"
2025-11-20T00:53:18+05:30       INFO    [javadb] Java DB is cached for 3 days. If you want to update the database more frequently, "trivy clean --java-db" command clears the DB cache.
2025-11-20T00:53:18+05:30       INFO    Detected OS     family="debian" version="13.2"
2025-11-20T00:53:18+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-20T00:53:18+05:30       INFO    Number of language-specific files       num=0
2025-11-20T00:53:18+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#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)
```



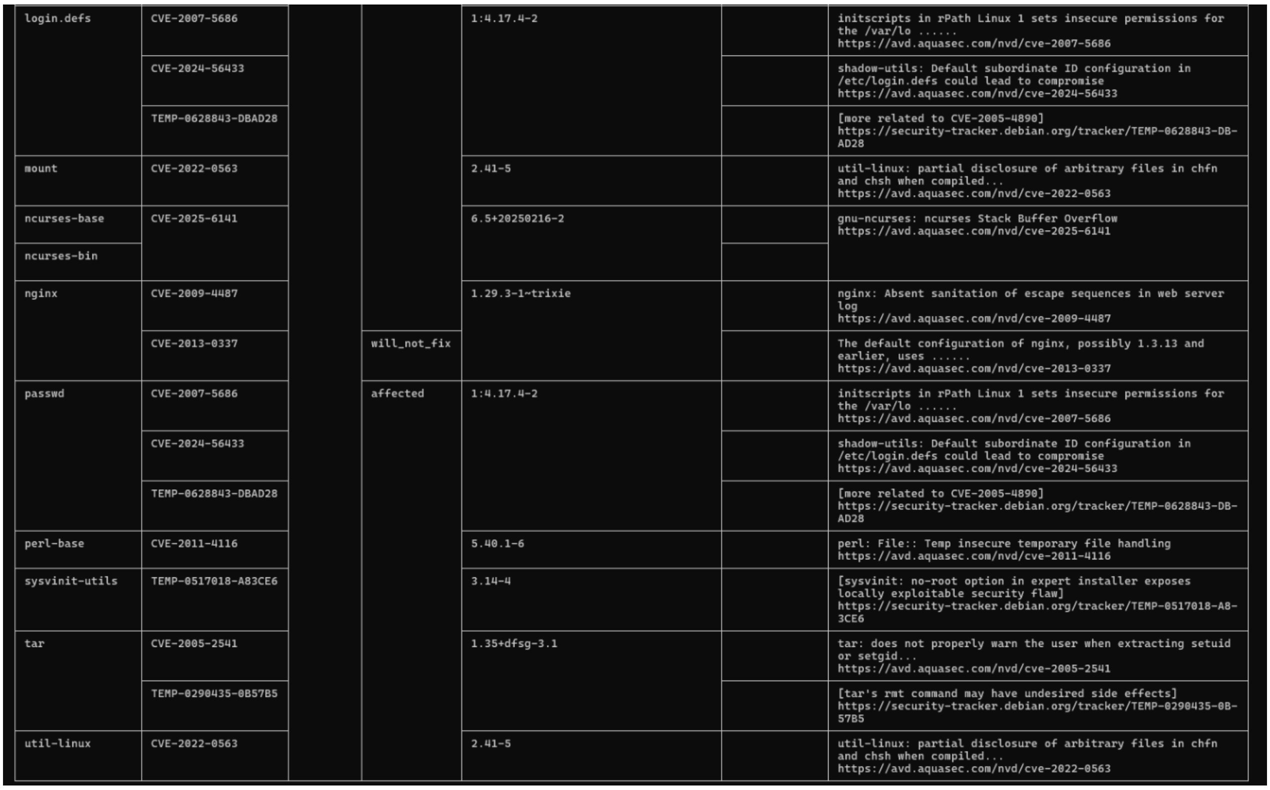
Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
apt	CVE-2011-3374	LOW	affected	3.0.3		It was found that apt-key in apt, all versions, do not correctly... https://avd.aquasec.com/nvd/cve-2011-3374
bash	TEMP-0841856-B18BAF			5.2.37-2+b5		[Privilege escalation possible to other user than root] https://security-tracker.debian.org/tracker/TEMP-0841856-B1-8BAF
bsdutils	CVE-2022-0563			1:2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
coreutils	CVE-2017-18018			9.7-3		coreutils: race condition vulnerability in chown and chgrp https://avd.aquasec.com/nvd/cve-2017-18018
	CVE-2025-5278					coreutils: Heap Buffer Under-Read in GNU Coreutils sort via Key Specification https://avd.aquasec.com/nvd/cve-2025-5278
curl	CVE-2025-10966			8.14.1-2+deb13u2		curl: Curl missing SFTP host verification with wolfSSH backend https://avd.aquasec.com/nvd/cve-2025-10966
libapt-pkg7.0	CVE-2011-3374			3.0.3		It was found that apt-key in apt, all versions, do not correctly... https://avd.aquasec.com/nvd/cve-2011-3374
libblkid1	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libc-bin	CVE-2010-4756			2.41-12		glibc: glob implementation can cause excessive CPU and memory consumption due to... https://avd.aquasec.com/nvd/cve-2010-4756
	CVE-2018-20796					glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2018-20796
	CVE-2019-1010022					glibc: stack guard protection bypass https://avd.aquasec.com/nvd/cve-2019-1010022
	CVE-2019-1010023					glibc: running ldd on malicious ELF leads to code execution because of... https://avd.aquasec.com/nvd/cve-2019-1010023
	CVE-2019-1010024					glibc: ASLR bypass using cache of thread stack and heap https://avd.aquasec.com/nvd/cve-2019-1010024
	CVE-2019-1010025					glibc: information disclosure of heap addresses of pthread_created thread https://avd.aquasec.com/nvd/cve-2019-1010025
	CVE-2019-9192					glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2019-9192
libc6	CVE-2010-4756					glibc: glob implementation can cause excessive CPU and memory consumption due to... https://avd.aquasec.com/nvd/cve-2010-4756



libc6	CVE-2010-4756					glibc: glob implementation can cause excessive CPU and memory consumption due to... https://avd.aquasec.com/nvd/cve-2010-4756
	CVE-2018-20796					glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2018-20796
	CVE-2019-1010022					glibc: stack guard protection bypass https://avd.aquasec.com/nvd/cve-2019-1010022
	CVE-2019-1010023					glibc: running ldd on malicious ELF leads to code execution because of... https://avd.aquasec.com/nvd/cve-2019-1010023
	CVE-2019-1010024					glibc: ASLR bypass using cache of thread stack and heap https://avd.aquasec.com/nvd/cve-2019-1010024
	CVE-2019-1010025					glibc: information disclosure of heap addresses of pthread_created thread https://avd.aquasec.com/nvd/cve-2019-1010025
	CVE-2019-9192					glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2019-9192
libcurl4t64	CVE-2025-10966			8.14.1-2+deb13u2		curl: Curl missing SFTP host verification with wolfSSH backend https://avd.aquasec.com/nvd/cve-2025-10966
libde265-0	CVE-2024-38949	MEDIUM	fix_deferred	1.0.15-1+b3		Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attacker ... https://avd.aquasec.com/nvd/cve-2024-38949
	CVE-2024-38950					Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attacker ... https://avd.aquasec.com/nvd/cve-2024-38950
libexpat1	CVE-2025-59375		affected	2.7.1-2		expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations... https://avd.aquasec.com/nvd/cve-2025-59375
libgcrypt20	CVE-2018-6829	LOW		1.11.0-7		libgcrypt: ElGamal implementation doesn't have semantic security due to incorrectly encoded plaintexts... https://avd.aquasec.com/nvd/cve-2018-6829
	CVE-2024-2236					libgcrypt: vulnerable to Marvin Attack https://avd.aquasec.com/nvd/cve-2024-2236
libgnutls30t64	CVE-2011-3389			3.8.9-3		HTTPS: block-wise chosen-plaintext attack against SSL/TLS (BEAST) https://avd.aquasec.com/nvd/cve-2011-3389
libgssapi-krb5-2	CVE-2018-5709			1.21.3-5		krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c https://avd.aquasec.com/nvd/cve-2024-26461



libjbig0	CVE-2017-9937			2.1-6.1+b2		libtiff: memory malloc failure in tif_jbig.c could cause DOS. https://avd.aquasec.com/nvd/cve-2017-9937
libk5crypto3	CVE-2018-5709			1.21.3-5		krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c https://avd.aquasec.com/nvd/cve-2024-26461
libkrb5-3	CVE-2018-5709					krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c https://avd.aquasec.com/nvd/cve-2024-26461
libkrb5support0	CVE-2018-5709					krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c https://avd.aquasec.com/nvd/cve-2024-26461
liblastlog2-2	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libldap2	CVE-2015-3276			2.6.10+dfsg-1		openldap: incorrect multi-keyword mode cipherstring parsing https://avd.aquasec.com/nvd/cve-2015-3276
	CVE-2017-14159					openldap: Privilege escalation via PID file manipulation https://avd.aquasec.com/nvd/cve-2017-14159
	CVE-2017-17740					openldap: contrib/slapd-modules/nops/nops.c attempts to free stack buffer allowing remote attackers to cause... https://avd.aquasec.com/nvd/cve-2017-17740
	CVE-2020-15719					openldap: Certificate validation incorrectly matches name against CN-ID https://avd.aquasec.com/nvd/cve-2020-15719
libmount1	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libpng16-16t64	CVE-2021-4214			1.6.48-1		libpng: hardcoded value leads to heap-overflow https://avd.aquasec.com/nvd/cve-2021-4214
libsmartcols1	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563



```
│ login.defs     │ CVE-2007-5686       │ │              │ 1:4.17.4-2       │ │ initscripts in rPath Linux 1 sets insecure permissions for     │
│                │                     │ │              │                  │ │ the /var/lo ......                                             │
│                │                     │ │              │                  │ │ https://avd.aquasec.com/nvd/cve-2007-5686                      │
│                ├─────────────────────┤ │              │                  ├─┼────────────────────────────────────────────────────────────────┤
│                │ CVE-2024-56433      │ │              │                  │ │ shadow-utils: Default subordinate ID configuration in          │
│                │                     │ │              │                  │ │ /etc/login.defs could lead to compromise                       │
│                │                     │ │              │                  │ │ https://avd.aquasec.com/nvd/cve-2024-56433                     │
│                ├─────────────────────┤ │              │                  ├─┼────────────────────────────────────────────────────────────────┤
│                │ TEMP-0628843-DBAD28 │ │              │                  │ │ [more related to CVE-2005-4890]                                │
│                │                     │ │              │                  │ │ https://security-tracker.debian.org/tracker/TEMP-0628843-DB-   │
│                │                     │ │              │                  │ │ AD28                                                           │
├────────────────┼─────────────────────┤ │              ├──────────────────┼─┼────────────────────────────────────────────────────────────────┤
│ mount          │ CVE-2022-0563       │ │              │ 2.41-5           │ │ util-linux: partial disclosure of arbitrary files in chfn      │
│                │                     │ │              │                  │ │ and chsh when compiled...                                      │
│                │                     │ │              │                  │ │ https://avd.aquasec.com/nvd/cve-2022-0563                      │
├────────────────┼─────────────────────┤ │              ├──────────────────┼─┼────────────────────────────────────────────────────────────────┤
│ ncurses-base   │ CVE-2025-6141       │ │              │ 6.5+20250216-2   │ │ gnu-ncurses: ncurses Stack Buffer Overflow                     │
├────────────────┤                     │ │              │                  ├─┤ https://avd.aquasec.com/nvd/cve-2025-6141                      │
│ ncurses-bin    │                     │ │              │                  │ │                                                                │
├────────────────┼─────────────────────┤ │              ├──────────────────┼─┼────────────────────────────────────────────────────────────────┤
│ nginx          │ CVE-2009-4487       │ │              │ 1.29.3-1~trixie  │ │ nginx: Absent sanitation of escape sequences in web server     │
│                │                     │ │              │                  │ │ log                                                            │
│                │                     │ │              │                  │ │ https://avd.aquasec.com/nvd/cve-2009-4487                      │
│                ├─────────────────────┤ ├──────────────┤                  ├─┼────────────────────────────────────────────────────────────────┤
│                │ CVE-2013-0337       │ │ will_not_fix │                  │ │ The default configuration of nginx, possibly 1.3.13 and        │
│                │                     │ │              │                  │ │ earlier, uses ......                                           │
│                │                     │ │              │                  │ │ https://avd.aquasec.com/nvd/cve-2013-0337                      │
├────────────────┼─────────────────────┤ ├──────────────┼──────────────────┼─┼────────────────────────────────────────────────────────────────┤
│ passwd         │ CVE-2007-5686       │ │ affected     │ 1:4.17.4-2       │ │ initscripts in rPath Linux 1 sets insecure permissions for     │
│                │                     │ │              │                  │ │ the /var/lo ......                                             │
│                │                     │ │              │                  │ │ https://avd.aquasec.com/nvd/cve-2007-5686                      │
│                ├─────────────────────┤ │              │                  ├─┼────────────────────────────────────────────────────────────────┤
│                │ CVE-2024-56433      │ │              │                  │ │ shadow-utils: Default subordinate ID configuration in          │
│                │                     │ │              │                  │ │ /etc/login.defs could lead to compromise                       │
│                │                     │ │              │                  │ │ https://avd.aquasec.com/nvd/cve-2024-56433                     │
│                ├─────────────────────┤ │              │                  ├─┼────────────────────────────────────────────────────────────────┤
│                │ TEMP-0628843-DBAD28 │ │              │                  │ │ [more related to CVE-2005-4890]                                │
│                │                     │ │              │                  │ │ https://security-tracker.debian.org/tracker/TEMP-0628843-DB-   │
│                │                     │ │              │                  │ │ AD28                                                           │
├────────────────┼─────────────────────┤ │              ├──────────────────┼─┼────────────────────────────────────────────────────────────────┤
│ perl-base      │ CVE-2011-4116       │ │              │ 5.40.1-6         │ │ perl: File:: Temp insecure temporary file handling             │
│                │                     │ │              │                  │ │ https://avd.aquasec.com/nvd/cve-2011-4116                      │
├────────────────┼─────────────────────┤ │              ├──────────────────┼─┼────────────────────────────────────────────────────────────────┤
│ sysvinit-utils │ TEMP-0517018-A83CE6 │ │              │ 3.14-4           │ │ [sysvinit: no-root option in expert installer exposes          │
│                │                     │ │              │                  │ │ locally exploitable security flaw]                             │
│                │                     │ │              │                  │ │ 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 undesired side effects]            │
│                │                     │ │              │                  │ │ https://security-tracker.debian.org/tracker/TEMP-0290435-0B-   │
│                │                     │ │              │                  │ │ 57B5                                                           │
├────────────────┼─────────────────────┤ │              ├──────────────────┼─┼────────────────────────────────────────────────────────────────┤
│ util-linux     │ CVE-2022-0563       │ │              │ 2.41-5           │ │ util-linux: partial disclosure of arbitrary files in chfn      │
│                │                     │ │              │                  │ │ and chsh when compiled...                                      │
│                │                     │ │              │                  │ │ https://avd.aquasec.com/nvd/cve-2022-0563                      │
└────────────────┴─────────────────────┴─┴──────────────┴──────────────────┴─┴────────────────────────────────────────────────────────────────┘
```

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.

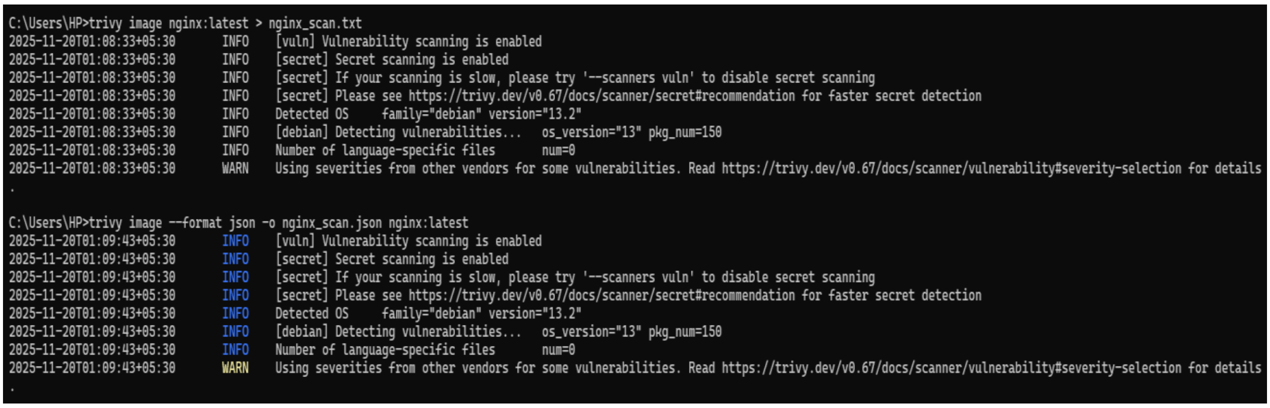
Save as a text file:

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

Save as a JSON report:

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

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

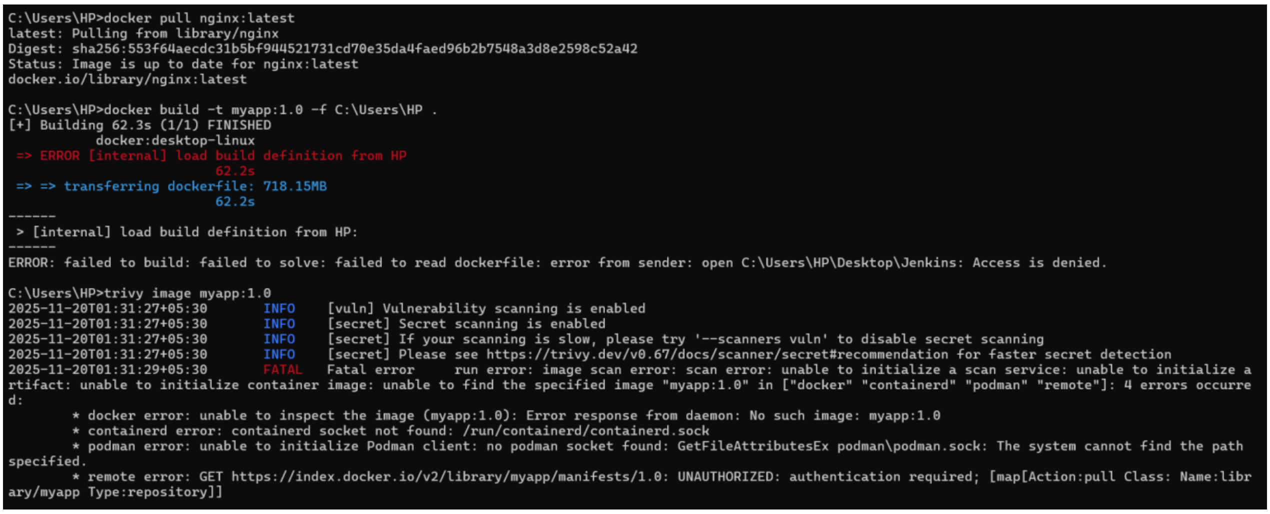


```
C:\Users\HP>trivy image nginx:latest > nginx_scan.txt
2025-11-20T01:08:33+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-20T01:08:33+05:30       INFO    [secret] Secret scanning is enabled
2025-11-20T01:08:33+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-20T01:08:33+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-20T01:08:33+05:30       INFO    Detected OS     family="debian" version="13.2"
2025-11-20T01:08:33+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-20T01:08:33+05:30       INFO    Number of language-specific files       num=0
2025-11-20T01:08:33+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-selection for details
.

C:\Users\HP>trivy image --format json -o nginx_scan.json nginx:latest
2025-11-20T01:09:43+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-20T01:09:43+05:30       INFO    [secret] Secret scanning is enabled
2025-11-20T01:09:43+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-20T01:09:43+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-20T01:09:43+05:30       INFO    Detected OS     family="debian" version="13.2"
2025-11-20T01:09:43+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-20T01:09:43+05:30       INFO    Number of language-specific files       num=0
2025-11-20T01:09:43+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-selection for details
.
```

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
```



```
C:\Users\HP>docker pull nginx:latest
latest: Pulling from library/nginx
Digest: sha256:553f64aecdc31b5bf944521731cd70e35da4faed96b2b7548a3d8e2598c52a42
Status: Image is up to date for nginx:latest
docker.io/library/nginx:latest

C:\Users\HP>docker build -t myapp:1.0 -f C:\Users\HP .
[+] Building 62.3s (1/1) FINISHED
           docker:desktop-linux
 => ERROR [internal] load build definition from HP
                         62.2s
 => => transferring dockerfile: 718.15MB
                         62.2s
------
 > [internal] load build definition from HP:
------
ERROR: failed to build: failed to solve: failed to read dockerfile: error from sender: open C:\Users\HP\Desktop\Jenkins: Access is denied.

C:\Users\HP>trivy image myapp:1.0
2025-11-20T01:31:27+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-20T01:31:27+05:30       INFO    [secret] Secret scanning is enabled
2025-11-20T01:31:27+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-20T01:31:27+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-20T01:31:29+05:30       FATAL   Fatal error     run error: image scan error: scan error: unable to initialize a scan service: unable to initialize a
rtifact: unable to initialize container image: unable to find the specified image "myapp:1.0" in ["docker" "containerd" "podman" "remote"]: 4 errors occurre
d:
        * docker error: unable to inspect the image (myapp:1.0): Error response from daemon: No such image: myapp:1.0
        * containerd error: containerd socket not found: /run/containerd/containerd.sock
        * podman error: unable to initialize Podman client: no podman socket found: GetFileAttributesEx podman\podman.sock: The system cannot find the path
specified.
        * remote error: GET https://index.docker.io/v2/library/myapp/manifests/1.0: UNAUTHORIZED: authentication required; [map[Action:pull Class: Name:libr
ary/myapp Type:repository]]
```

Step 7: Update Vulnerability Database

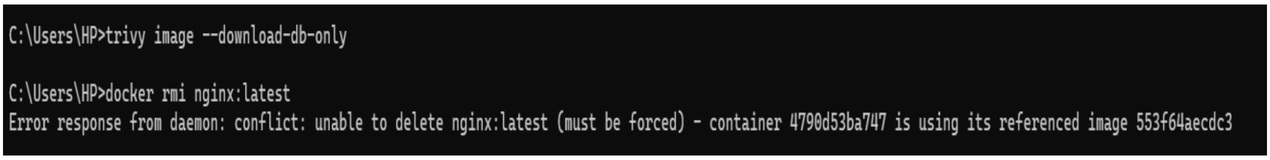
Keep Trivy’s database up-to-date:

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

Step 8: Clean Up

Remove images (optional):

```
docker rmi nginx:latest
```



```
C:\Users\HP>trivy image --download-db-only

C:\Users\HP>docker rmi nginx:latest
Error response from daemon: conflict: unable to delete nginx:latest (must be forced) - container 4790d53ba747 is using its referenced image 553f64aecdc3
```