

# Lab Exercise 22

## Checking Vulnerabilities Using Trivy

**Objective:** To scan container images for vulnerabilities using Trivy to identify and mitigate security risks and ensure that containerized applications are secure

**Tools required:** Trivy

**Prerequisites:** None

Steps to be followed:

1. Install Trivy
2. Scan the vulnerabilities using Trivy

### Step 1: Install Trivy

- 1.1 Run the following command to install tools for secure downloads, HTTPS repositories, encryption key management, and system version identification:  
**sudo apt-get install wget apt-transport-https gnupg lsb-release**

```
poojahksimpi@ip-172-31-34-206:~$ sudo apt-get install wget apt-transport-https gnupg lsb-release
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
lsb-release is already the newest version (11.1.0ubuntu4).
lsb-release set to manually installed.
gnupg is already the newest version (2.2.27-3ubuntu2.1).
The following packages will be upgraded:
  apt-transport-https wget
2 upgraded, 0 newly installed, 0 to remove and 232 not upgraded.
Need to get 1510 B/340 kB of archives.
After this operation, 57.3 kB disk space will be freed.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 apt-transport-https all 2.4.12 [1510 B]
Fetched 1510 B in 0s (106 kB/s)
(Reading database ... 217380 files and directories currently installed.)
Preparing to unpack .../wget 1.21.2-2ubuntu1.1 amd64.deb ...
Unpacking wget (1.21.2-2ubuntu1.1) over (1.21.2-2ubuntu1) ...
Preparing to unpack .../apt-transport-https_2.4.12_all.deb ...
Unpacking apt-transport-https (2.4.12) over (2.4.11) ...
Setting up wget (1.21.2-2ubuntu1.1) ...
Setting up apt-transport-https (2.4.12) ...
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.
```

```
10:24:58 [22/22]
→ computer science sudo wget -qO /usr/share/keyrings/trivy.gpg https://aquasecurity.github.io/trivy-repo/deb/public.key
→ computer science echo "deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-repo/deb jammy main
" | \
sudo tee /etc/apt/sources.list.d/trivy.list

deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-repo/deb jammy main
```

- 1.2 Run the following command to download the Trivy repository's public key and add it to the system's trusted keys, ensuring secure package verification:

```
wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | sudo apt-key add -
```

```
poojahksimplile@ip-172-31-34-206:~$ wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | sudo apt-key add -  
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).  
OK  
poojahksimplile@ip-172-31-34-206:~$ █
```

- 1.3 Run the following command to add the Trivy repository to the system's sources list, enabling the installation of Trivy packages tailored to the Ubuntu version:

```
echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main |  
sudo tee -a /etc/apt/sources.list.d/trivy.list
```

```
→ computer science echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main | sudo tee -a /etc/apt/source  
s.list.d/trivy.list  
deb https://aquasecurity.github.io/trivy-repo/deb noble main
```

- 1.4 Run the following command to update the system's package lists, ensuring the latest information on available software and updates from all configured repositories:

```
sudo apt-get update
```

```
→ computer science sudo apt-get update  
Hit:1 https://brave-browser-apt-release.s3.brave.com stable InRelease  
Hit:2 https://apt.releases.hashicorp.com noble InRelease  
Hit:3 https://deb.nodesource.com/node_18.x nodistro InRelease  
Hit:4 http://deb.debian.org/debian bookworm InRelease  
Hit:5 http://deb.debian.org/debian-security bookworm-security InRelease  
Hit:6 http://security.ubuntu.com/ubuntu focal-security InRelease  
Hit:7 http://deb.debian.org/debian bookworm-updates InRelease  
Hit:8 http://archive.ubuntu.com/ubuntu focal InRelease  
Hit:9 http://deb.debian.org/debian bullseye InRelease  
Hit:10 http://deb.debian.org/debian bullseye-updates InRelease  
Get:11 https://aquasecurity.github.io/trivy-repo/deb jammy InRelease [3061 B]  
Hit:13 http://security.ubuntu.com/ubuntu noble-security InRelease  
Get:14 https://aquasecurity.github.io/trivy-repo/deb noble InRelease [3061 B]  
Hit:15 http://archive.ubuntu.com/ubuntu focal-updates InRelease  
Hit:16 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/6.0 InRelease  
Hit:17 http://archive.ubuntu.com/ubuntu focal-backports InRelease  
Hit:12 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.31/deb InRelease  
Hit:18 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 InRelease  
Hit:19 http://archive.ubuntu.com/ubuntu noble InRelease  
Hit:20 http://archive.ubuntu.com/ubuntu noble-updates InRelease  
Hit:21 http://archive.ubuntu.com/ubuntu noble-backports InRelease  
Hit:22 https://ppa.launchpadcontent.net/deadsnakes/ppa/ubuntu noble InRelease  
Hit:23 https://ngrok-agent.s3.amazonaws.com buster InRelease  
Hit:24 https://ppa.launchpadcontent.net/neovim-ppa/stable/ubuntu noble InRelease  
Err:11 https://aquasecurity.github.io/trivy-repo/deb jammy InRelease  
The following signatures couldn't be verified because the public key is not available: NO_PUBKEY F0D9A71127E4/C
```

1.5 Run the following command to install Trivy, a security scanner for containers, directly from the configured repository:

```
sudo apt-get install trivy
```

```
→ computer science sudo apt-get install trivy
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  trivy
0 upgraded, 1 newly installed, 0 to remove and 188 not upgraded.
Need to get 47.3 MB of archives.
After this operation, 158 MB of additional disk space will be used.
Get:1 https://aquasecurity.github.io/trivy-repo/deb/noble/main amd64 trivy amd64 0.67.2 [47.3 MB]
Fetched 47.3 MB in 1min 4s (735 kB/s)
Selecting previously unselected package trivy.
(Reading database ... 113454 files and directories currently installed.)
Preparing to unpack .../trivy_0.67.2_amd64.deb ...
Unpacking trivy (0.67.2) ...
Setting up trivy (0.67.2) ...
→ computer science
  1 projects/computer science
```

## Step 2: Scan the vulnerabilities using Trivy

2.1 Run the following command to scan the NGINX container image with Trivy for vulnerabilities and security issues:

```
trivy image nginx
```

```
+ computer science cd nginx-html-app
+ nginx-html-app trivy image nginx
2025-11-19T10:29:13+05:30 INFO  [vulndb] Need to update DB
2025-11-19T10:29:13+05:30 INFO  [vulndb] Downloading vulnerability DB...
2025-11-19T10:29:13+05:30 INFO  [vulndb] Downloading artifact...          repo="mirror.gcr.io/aquasec/trivy-db:2"
75.26 MiB / 75.26 MiB [=====
2025-11-19T10:33:16+05:30 INFO  [vulndb] Artifact successfully downloaded      repo="mirror.gcr.io/aquasec/trivy-db:2"
2025-11-19T10:33:16+05:30 INFO  [vuln] Vulnerability scanning is enabled
2025-11-19T10:33:16+05:30 INFO  [secret] Secret scanning is enabled
2025-11-19T10:33:16+05:30 INFO  [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-19T10:33:16+05:30 INFO  [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation-for-faster-secret-detection
2025-11-19T10:34:07+05:30 WARN   Provide a higher timeout value, see https://trivy.dev/v0.67/docs/references/troubleshooting#timeout
2025-11-19T10:34:07+05:30 FATAL  Fatal error    run error: image scan error: scan error: scan failed: failed analysis: analyze error: pipeline error: failed to analyze layer (sha256:7
0a290c5e58b68f3949ab93a6af2f21b8b2ca0502e97905131838de1b39a37ccb): walk error: failed to process the file: failed to analyze file: failed to analyze usr/libexec/coreutils/libstdbuf.so: semapho
re acquire: context deadline exceeded
+ nginx-html-app trivy image nginx
2025-11-19T10:34:15+05:30 INFO  [vuln] Vulnerability scanning is enabled
2025-11-19T10:34:15+05:30 INFO  [secret] Secret scanning is enabled
2025-11-19T10:34:15+05:30 INFO  [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-19T10:34:15+05:30 INFO  [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation-for-faster-secret-detection
2025-11-19T10:34:46+05:30 INFO  [javadb] Downloading Java DB...
2025-11-19T10:34:46+05:30 INFO  [javadb] Downloading artifact...          repo="mirror.gcr.io/aquasec/trivy-java-db:1"
798.47 MiB / 798.47 MiB [=====
2025-11-19T10:51:09+05:30 INFO  [javadb] Artifact successfully downloaded      repo="mirror.gcr.io/aquasec/trivy-java-db:1"
2025-11-19T10:51:09+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.
2025-11-19T10:51:09+05:30 INFO  Detected OS   family="debian" version="13.2"
2025-11-19T10:51:09+05:30 INFO  [debian] Detecting vulnerabilities... os_version="13" pkg_num=150
2025-11-19T10:51:09+05:30 INFO  Number of language-specific files   num=0
2025-11-19T10:51:09+05:30 WARN   Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-selection for details.
```

It shows the results of a Trivy security scan, listing vulnerabilities in installed packages, their severity, and whether they are affected. It also includes details like the installed version and links for more information.

Report Summary							
Target	Type	Vulnerabilities	Secrets				
nginx (debian 13.2)	debian	91	-				
Legend:							
'-' Not scanned '0': Clean (no security findings detected)							
nginx (debian 13.2)							
Total: 91 (UNKNOWN: 0, LOW: 84, MEDIUM: 5, HIGH: 2, CRITICAL: 0)							
Library	Vulnerability	Severity	Status	Installed Version	Fixed Version		
apt	CVE-2011-3374	LOW	affected	3.0.3			
bash	TEMP-0841856-B18BAF			5.2.37-2+b5			
bsdutils	CVE-2022-0563			1:2.41-5			
coreutils	CVE-2017-18018			9.7-3			
	CVE-2025-5278						
curl	CVE-2025-10966			8.14.1-2+deb13u2			
libapt-pkg7.0	CVE-2011-3374			3.0.3			
computer science/nginx-html-app							

Terminal					
libcurl4t64	CVE-2025-10966			8.14.1-2+deb13u2	curl: Curl missing SFTP host verification with wolfSSH backend <a href="https://avd.aquasec.com/nvd/cve-2025-10966">https://avd.aquasec.com/nvd/cve-2025-10966</a>
libde265-0	CVE-2024-38949	MEDIUM	fix_deferred	1.0.15-1+b3	Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attacker ... <a href="https://avd.aquasec.com/nvd/cve-2024-38949">https://avd.aquasec.com/nvd/cve-2024-38949</a>
	CVE-2024-38950				Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attacker ... <a href="https://avd.aquasec.com/nvd/cve-2024-38950">https://avd.aquasec.com/nvd/cve-2024-38950</a>
libexpat1	CVE-2025-59375		affected	2.7.1-2	expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations... <a href="https://avd.aquasec.com/nvd/cve-2025-59375">https://avd.aquasec.com/nvd/cve-2025-59375</a>
libgcrypt20	CVE-2018-6829	LOW		1.11.0-7	libgcrypt: ElGamal implementation doesn't have semantic security due to incorrectly encoded plaintexts... <a href="https://avd.aquasec.com/nvd/cve-2018-6829">https://avd.aquasec.com/nvd/cve-2018-6829</a>
	CVE-2024-2236				libgcrypt: vulnerable to Marvin Attack <a href="https://avd.aquasec.com/nvd/cve-2024-2236">https://avd.aquasec.com/nvd/cve-2024-2236</a>
libgnutls30t64	CVE-2011-3389			3.8.9-3	HTTPS: block-wise chosen-plaintext attack against SSL/TLS (BEAST) <a href="https://avd.aquasec.com/nvd/cve-2011-3389">https://avd.aquasec.com/nvd/cve-2011-3389</a>
libgssapi-krb5-2	CVE-2018-5709			1.21.3-5	krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c <a href="https://avd.aquasec.com/nvd/cve-2018-5709">https://avd.aquasec.com/nvd/cve-2018-5709</a>
	CVE-2024-26458				krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c <a href="https://avd.aquasec.com/nvd/cve-2024-26458">https://avd.aquasec.com/nvd/cve-2024-26458</a>
	CVE-2024-26461				krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c <a href="https://avd.aquasec.com/nvd/cve-2024-26461">https://avd.aquasec.com/nvd/cve-2024-26461</a>
libjbig0	CVE-2017-9937			2.1-6.1+b2	libtiff: memory malloc failure in tif_jbig.c could cause DOS. <a href="https://avd.aquasec.com/nvd/cve-2017-9937">https://avd.aquasec.com/nvd/cve-2017-9937</a>
libk5crypto3	CVE-2018-5709			1.21.3-5	krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c <a href="https://avd.aquasec.com/nvd/cve-2018-5709">https://avd.aquasec.com/nvd/cve-2018-5709</a>
	CVE-2024-26458				Krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c <a href="https://avd.aquasec.com/nvd/cve-2024-26458">https://avd.aquasec.com/nvd/cve-2024-26458</a>
computer science/nginx-html-app					

ncurses-base	CVE-2025-6141		6.5+20250216-2		gnu-ncurses: ncurses Stack Buffer Overflow <a href="https://avd.aquasec.com/nvd/cve-2025-6141">https://avd.aquasec.com/nvd/cve-2025-6141</a>
ncurses-bin					
nginx	CVE-2009-4487		1.29.3-1-trixie		nginx: Absent sanitation of escape sequences in web server log <a href="https://avd.aquasec.com/nvd/cve-2009-4487">https://avd.aquasec.com/nvd/cve-2009-4487</a>
	CVE-2013-0337	will_not_fix			The default configuration of nginx, possibly 1.3.13 and earlier, uses ..... <a href="https://avd.aquasec.com/nvd/cve-2013-0337">https://avd.aquasec.com/nvd/cve-2013-0337</a>
passwd	CVE-2007-5686	affected	1:4.17.4-2		initscripts in rPath Linux 1 sets insecure permissions for the /var/lo ..... <a href="https://avd.aquasec.com/nvd/cve-2007-5686">https://avd.aquasec.com/nvd/cve-2007-5686</a>
	CVE-2024-56433				shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise <a href="https://avd.aquasec.com/nvd/cve-2024-56433">https://avd.aquasec.com/nvd/cve-2024-56433</a>
	TEMP-0628843-DBAD28				[more related to CVE-2005-4890] <a href="https://security-tracker.debian.org/tracker/TEMP-0628843-DBAD28">https://security-tracker.debian.org/tracker/TEMP-0628843-DBAD28</a>
perl-base	CVE-2011-4116		5.40.1-6		perl: File:: Temp insecure temporary file handling <a href="https://avd.aquasec.com/nvd/cve-2011-4116">https://avd.aquasec.com/nvd/cve-2011-4116</a>
sysvinit-utils	TEMP-0517018-A83CE6		3.14-4		[sysvinit: no-root option in expert installer exposes locally exploitable security flaw] <a href="https://security-tracker.debian.org/tracker/TEMP-0517018-A83CE6">https://security-tracker.debian.org/tracker/TEMP-0517018-A83CE6</a>
tar	CVE-2005-2541		1.35+dfsg-3.1		tar: does not properly warn the user when extracting setuid or setgid... <a href="https://avd.aquasec.com/nvd/cve-2005-2541">https://avd.aquasec.com/nvd/cve-2005-2541</a>
	TEMP-0290435-0B5785				[tar's rmt command may have undesired side effects] <a href="https://security-tracker.debian.org/tracker/TEMP-0290435-0B5785">https://security-tracker.debian.org/tracker/TEMP-0290435-0B5785</a>
util-linux	CVE-2022-0563		2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... <a href="https://avd.aquasec.com/nvd/cve-2022-0563">https://avd.aquasec.com/nvd/cve-2022-0563</a>

By following these steps, you have successfully scanned container images for vulnerabilities using Trivy to identify and mitigate security risks and ensure the security of containerized applications.