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

```
poojahksimplile@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.
```

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:~$
```

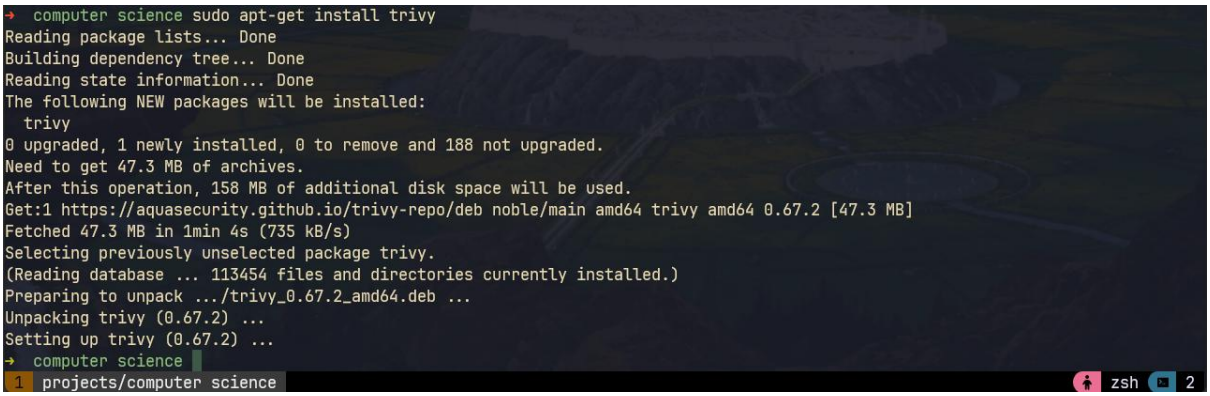
1.3 Run the following command to add the Trivy repository to the system's sources list, enabling the installation of Trivy packages tailored to the Ubuntu version:
echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main | sudo tee -a /etc/apt/sources.list.d/trivy.list

```
→  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

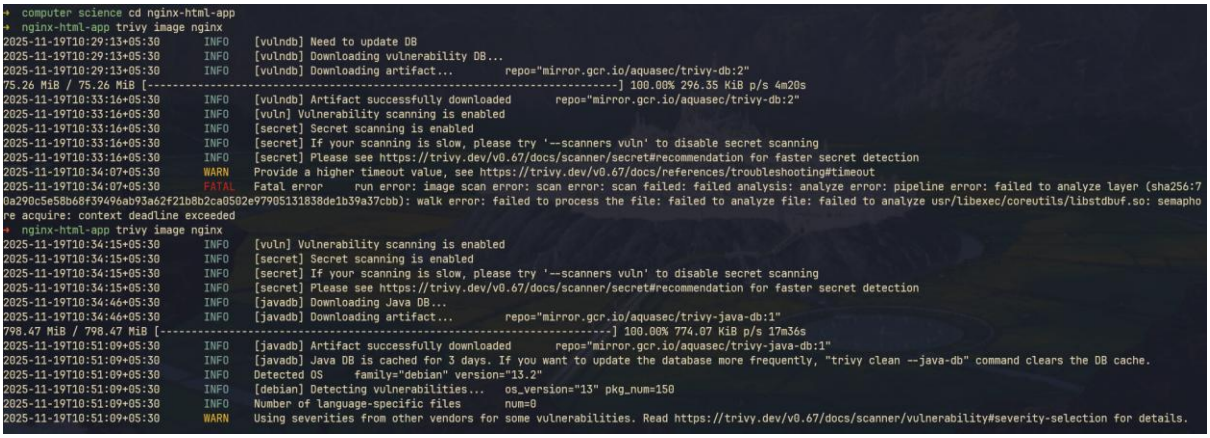
```
→  computer science sudo apt-get update
Hit:1 https://brave-browser-apt-release.s3.brave.com stable InRelease
Hit:2 https://apt.releases.hashicorp.com noble InRelease
Hit:3 https://deb.nodesource.com/node_18.x nodistro InRelease
Hit:4 http://deb.debian.org/debian bookworm InRelease
Hit:5 http://deb.debian.org/debian-security 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
```

1.5 Run the following command to install Trivy, a security scanner for containers, directly from the configured repository:
sudo apt-get install trivy



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



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	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

1 computer science/nginx-html-app [tmux] 2

Terminal

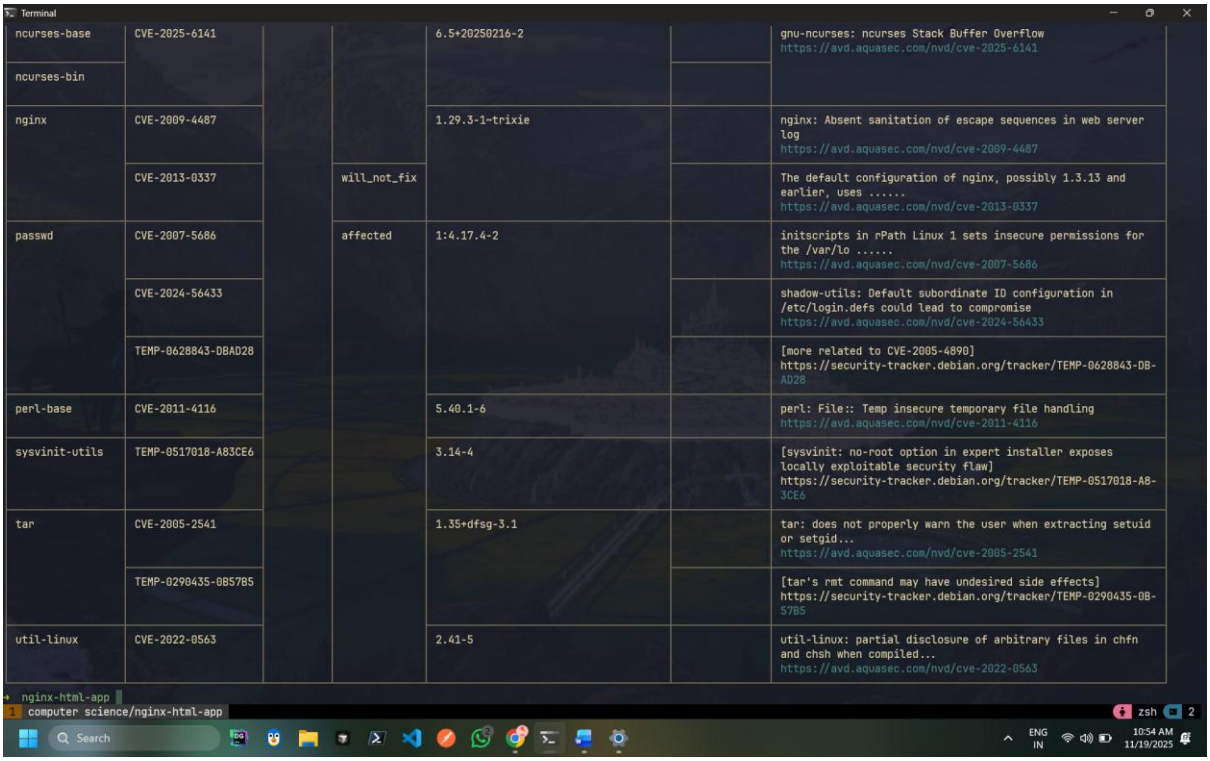
10:51:09 [210/979]

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

1 computer science/nginx-html-app [tmux] 2

Search

ENG IN 10:54 AM 11/19/2025



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.