Lesson 06 Demo 02

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

```
poojahksimplile@ip-172-31-34-206:~$ echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main | sudo tee -a /etc/apt/sources.lis
t.d/trivy.list
deb https://aquasecurity.github.io/trivy-repo/deb jammy main
poojahksimplile@ip-172-31-34-206:~$
```

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

```
poojahksimplile@ip-172-31-34-206:~$ sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Ign:4 https://pkg.jenkins.io/debian-stable binary/ InRelease
Get:5 https://pkg.jenkins.io/debian-stable binary/ Release [2044 B]
Get:6 https://aquasecurity.github.io/trivy-repo/deb jammy InRelease [3061 B]
Get:7 https://download.docker.com/linux/ubuntu jammy InRelease [48.8 kB]
Get:8 https://pkg.jenkins.io/debian-stable binary/ Release.gpg [833 B]
Get:10 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:9 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.28/deb  InRelease [1192 B]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1948 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [345 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [17.8 kB]
```

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

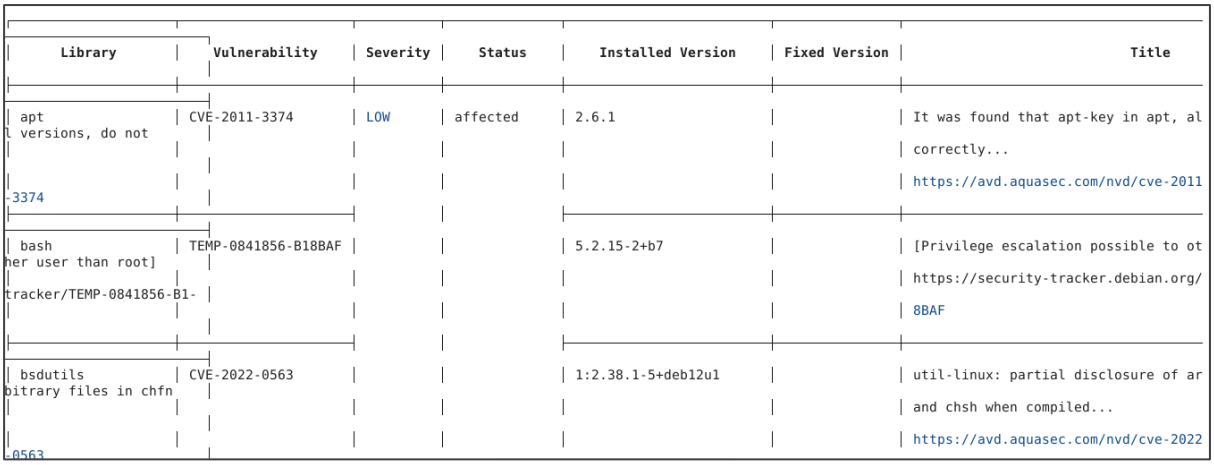
```
poojahksimplile@ip-172-31-34-206:~$ sudo apt-get install trivy
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  trivy
0 upgraded, 1 newly installed, 0 to remove and 244 not upgraded.
Need to get 39.3 MB of archives.
After this operation, 127 MB of additional disk space will be used.
Get:1 https://aquasecurity.github.io/trivy-repo/deb jammy/main amd64 trivy amd64 0.54.1 [39.3 MB]
Fetched 39.3 MB in 0s (103 MB/s)
Selecting previously unselected package trivy.
(Reading database ... 217380 files and directories currently installed.)
Preparing to unpack .../trivy_0.54.1_amd64.deb ...
Unpacking trivy (0.54.1) ...
Setting up trivy (0.54.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

Step 2: Scan the vulnerabilities using Trivy

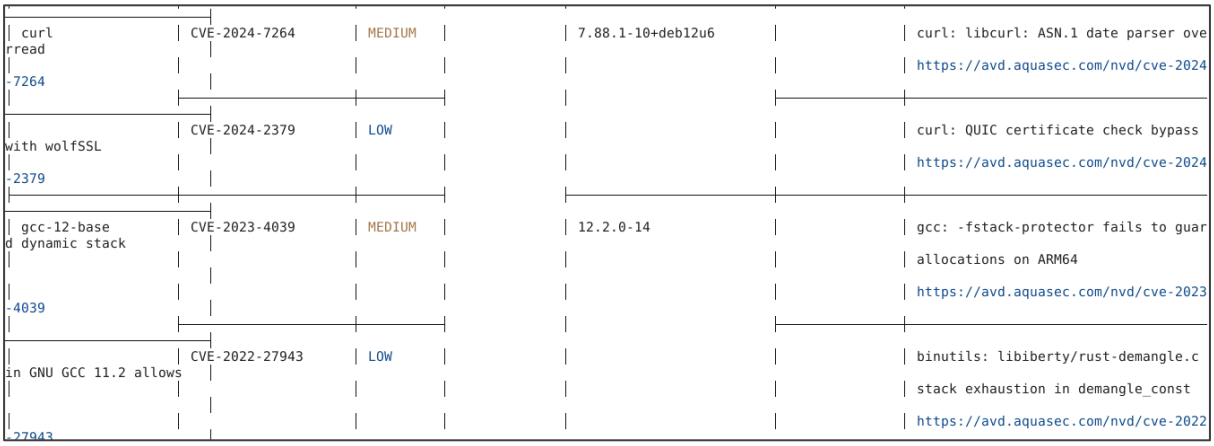
2.1 Run the following command to scan the NGINX container image with Trivy for vulnerabilities and security issues:
trivy image nginx

```
poojahksimplile@ip-172-31-34-206:~$ trivy image nginx
2024-08-17T03:27:02Z    INFO    [db] Need to update DB
2024-08-17T03:27:02Z    INFO    [db] Downloading DB...  repository="ghcr.io/aquasecurity/trivy-db:2"
51.45 MiB / 51.45 MiB [-------------------------------------------------------------------------------------------------] 100.00% 27.79 MiB p/s 2.1s
2024-08-17T03:27:04Z    INFO    [vuln] Vulnerability scanning is enabled
2024-08-17T03:27:04Z    INFO    [secret] Secret scanning is enabled
2024-08-17T03:27:04Z    INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-08-17T03:27:04Z    INFO    [secret] Please see also https://aquasecurity.github.io/trivy/v0.54/docs/scanner/secret#recommendation for faster sec
ret detection
2024-08-17T03:27:07Z    INFO    Java DB Repository      repository=ghcr.io/aquasecurity/trivy-java-db:1
2024-08-17T03:27:07Z    INFO    Downloading the Java DB...
635.77 MiB / 635.77 MiB [-----------------------------------------------------------------------------------------------] 100.00% 45.84 MiB p/s 14s
2024-08-17T03:27:21Z    INFO    The 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.
2024-08-17T03:27:21Z    INFO    Detected OS     family="debian" version="12.6"
2024-08-17T03:27:21Z    INFO    [debian] Detecting vulnerabilities...   os_version="12" pkg_num=149
2024-08-17T03:27:21Z    INFO    Number of language-specific files       num=0
2024-08-17T03:27:21Z    WARN    Using severities from other vendors for some vulnerabilities. Read https://aquasecurity.github.io/trivy/v0.54/docs/sc
anner/vulnerability#severity-selection for details.

nginx (debian 12.6)

Total: 152 (UNKNOWN: 0, LOW: 89, MEDIUM: 44, HIGH: 16, CRITICAL: 3)

┌──────────────────┬────────────────┬──────────┬────────┬───────────────────┬───────────────┬──────────────────────────────────────────────────────────┐
│     Library      │ Vulnerability  │ Severity │ Status │ Installed Version │ Fixed Version │                          Title                           │
```

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.



Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
apt	CVE-2011-3374	LOW	affected	2.6.1		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			5.2.15-2+b7		[Privilege escalation possible to other user than root] https://security-tracker.debian.org/tracker/TEMP-0841856-B18BAF
bsdutils	CVE-2022-0563			1:2.38.1-5+deb12u1		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563



curl	CVE-2024-7264	MEDIUM		7.88.1-10+deb12u6		curl: libcurl: ASN.1 date parser overread https://avd.aquasec.com/nvd/cve-2024-7264
	CVE-2024-2379	LOW				curl: QUIC certificate check bypass with wolfSSL https://avd.aquasec.com/nvd/cve-2024-2379
gcc-12-base	CVE-2023-4039	MEDIUM		12.2.0-14		gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64 https://avd.aquasec.com/nvd/cve-2023-4039
	CVE-2022-27943	LOW				binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const https://avd.aquasec.com/nvd/cve-2022-27943

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.