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. Install Homebrew (if not already installed)

Homebrew is required to install Trivy.

/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"

2. Install Trivy using Homebrew

brew install trivy

```
mohdanas@Mohds-MacBook-Air ~ % brew install trivy

==> Fetching downloads for: trivy
✔ Bottle Manifest trivy (0.67.2)                  [Downloaded    7.5KB/  7.5KB]
✔ Bottle trivy (0.67.2)                           [Downloaded   54.3MB/ 54.3MB]
==> Pouring trivy--0.67.2.arm64_tahoe.bottle.tar.gz
🍺  /opt/homebrew/Cellar/trivy/0.67.2: 16 files, 196.9MB
==> Running `brew cleanup trivy`...
Disable this behaviour by setting `HOMEBREW_NO_INSTALL_CLEANUP=1`.
Hide these hints with `HOMEBREW_NO_ENV_HINTS=1` (see `man brew`).
==> Caveats
zsh completions have been installed to:
  /opt/homebrew/share/zsh/site-functions
```

3. Verify installation
trivy --version

```
mohdanas@Mohds-MacBook-Air ~ % trivy --version

Version: 0.67.2
```

Step 2: Scan the vulnerabilities using Trivy

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

```
mohdanas@Mohds-MacBook-Air ~ % trivy image nginx
2025-11-19T10:37:30+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-19T10:37:30+05:30       INFO    [secret] Secret scanning is enabled
2025-11-19T10:37:30+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secr
et scanning
[2025-11-19T10:37:30+05:30      INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation ]
for faster secret detection
2025-11-19T10:37:45+05:30       INFO    Detected OS     family="debian" version="13.2"
2025-11-19T10:37:45+05:30       INFO    [debian] Detecting vulnerabilities...  os_version="13" pkg_num=150
2025-11-19T10:37:45+05:30       INFO    Number of language-specific files      num=0
2025-11-19T10:37:45+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://triv
y.dev/v0.67/docs/scanner/vulnerability#severity-selection for details.

Report Summary

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

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.

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 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

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

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.