

# Lab 4: Perform Vulnerability Assessment on Docker Images

## Lab Scenario

As a professional ethical hacker or pen tester, expertise in Docker vulnerability assessment is crucial. By leveraging tools like Trivy, you can analyze Docker images, identifying and exploiting vulnerabilities. Active scanning and manual inspection reveal weak configurations, enabling you to breach security and implant malicious code, while understanding image location aids in comprehensive security testing and mitigation.

## Lab Objectives

- Vulnerability assessment on Docker images using Trivy

## Overview of Docker Images

Docker images are lightweight, standalone, executable packages that contain everything needed to run a software application, including the code, runtime, libraries, and dependencies. They enable consistent deployment across various environments, simplify software distribution, and facilitate scalability and reproducibility in containerized environments.

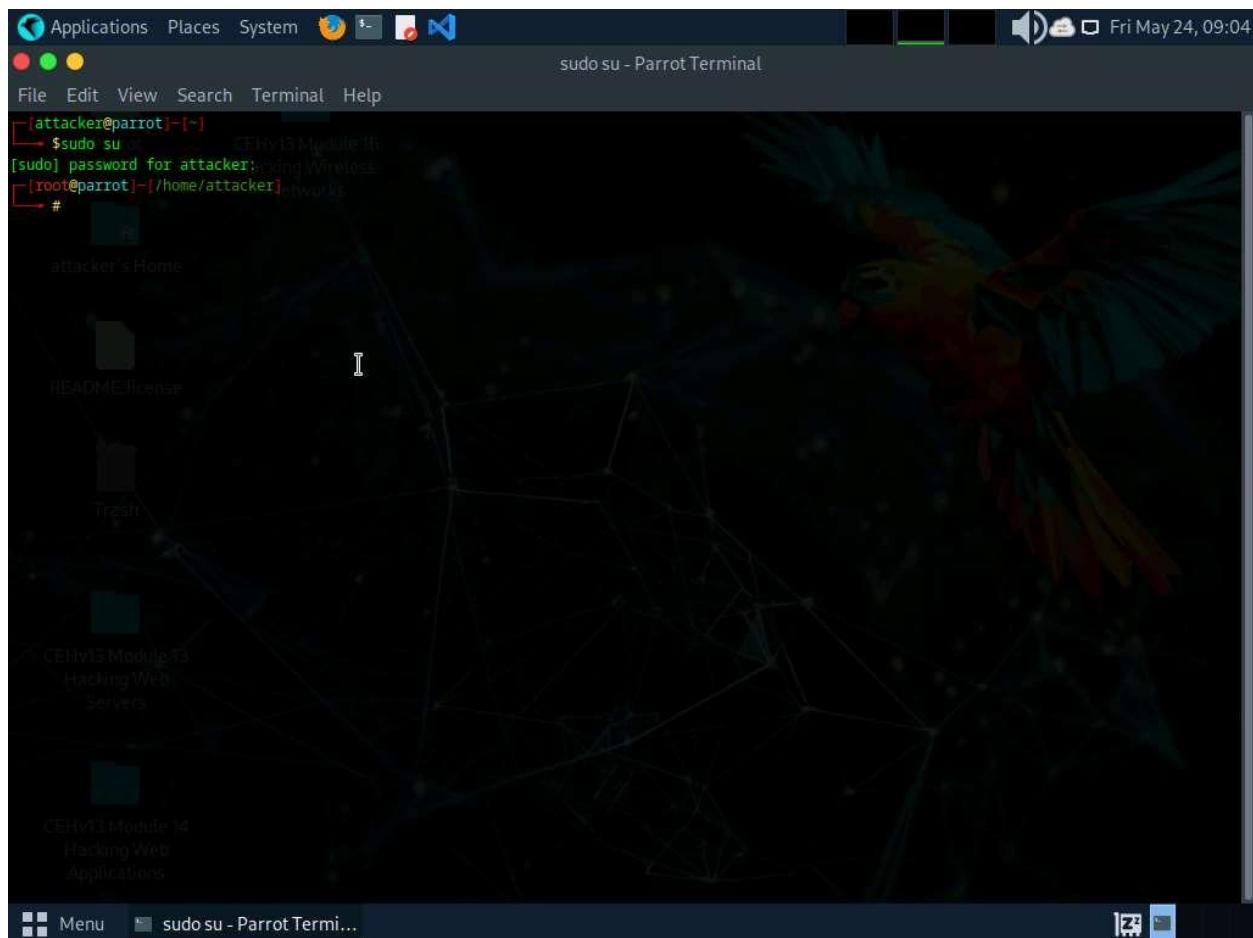
### Task 1: Vulnerability Assessment on Docker Images using Trivy

Trivy is a powerful security scanner that detects vulnerabilities and misconfigurations across a wide range of targets, including container images, file systems, Git repositories, virtual machine images, Kubernetes, and AWS. With its comprehensive scanners, Trivy identifies OS package vulnerabilities, sensitive information, IaC issues, and more, providing a robust security solution for your infrastructure.

1. In the **Parrot Security** machine, click the **MATE Terminal** icon in the menu to launch the terminal.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

Minimise the terminal for better view of output



4. In this lab we will be scanning two docker images, first the secure one and second the vulnerable one.
5. Execute command **docker pull ubuntu** to install the first docker image.

```
[attacker@parrot:~] $ sudo docker pull ubuntu
[sudo] password for attacker: 
[root@parrot:~] # docker pull ubuntu
Using default tag: latest
latest: Pulling from library/ubuntu
49b384cc7b4a: Pull complete
Digest: sha256:3f85b7caad41a95462cf5b787d8a04604c8262cdcdf9a472b8c52ef83375fe15
Status: Downloaded newer image for ubuntu:latest
docker.io/library/ubuntu:latest
[root@parrot:~]
```

6. Once the image is pulled we will be performing vulnerability assessment. Execute command **trivy image ubuntu**.

The screenshot shows a terminal window titled "trivy image ubuntu - Parrot Terminal". The terminal output is as follows:

```
[attacker@parrot:~]$
[attacker@parrot:~]$ sudo su
[sudo] password for attacker: kingWireless
[root@parrot:~/home/attacker]#
[root@parrot:~/home/attacker]# docker pull ubuntu
Using default tag: latest
latest: Pulling from library/ubuntu
49b384cc7b4a: Pull complete
Digest: sha256:3f85b7caad41a95462cf5b787d8a04604c8262cdcdf9a472b8c52ef83375fe15
Status: Downloaded newer image for ubuntu:latest
docker.io/library/ubuntu:latest
[root@parrot:~/home/attacker]#
[root@parrot:~/home/attacker]# trivy image ubuntu
2024-05-24T09:06:53.404-0400    WARN   You should avoid using the :latest tag as it is cached. You need to specify '--clear-cache' option when
:latest image is changed
2024-05-24T09:06:53.413-0400    INFO   Need to update DB
2024-05-24T09:06:53.413-0400    INFO   Downloading DB...
30.57 MiB / 30.57 MiB [=====] 100.00% 9.45 MiB p/s 3s
2024-05-24T09:06:58.936-0400    WARN   This OS version is not on the EOL list: ubuntu 24.04
2024-05-24T09:06:58.936-0400    INFO   Detecting Ubuntu vulnerabilities...
2024-05-24T09:06:58.936-0400    INFO   Trivy skips scanning programming language libraries because no supported file was detected
2024-05-24T09:06:58.936-0400    WARN   This OS version is no longer supported by the distribution: ubuntu 24.04
2024-05-24T09:06:58.936-0400    WARN   The vulnerability detection may be insufficient because security updates are not provided

ubuntu (ubuntu 24.04)
=====
Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)

[root@parrot:~/home/attacker]#

```

7. In the above screenshot, we can observe that we have total **0** vulnerability and it's completely secure.
8. Now, we will analyse the vulnerable image. execute command **docker pull nginx:1.19.6** to pull the vulnerable image.

A screenshot of a Parrot OS desktop environment. The terminal window in the foreground displays the command `docker pull nginx:1.19.6` being executed, with the output showing the download progress of the Nginx image. The desktop background features a dark, abstract network graph. The taskbar at the bottom shows the terminal window is active, along with other icons for the menu, system status, and network.

```
[root@parrot]~# docker pull nginx:1.19.6
1.19.6: Pulling from library/nginx
45b42c59be33: Pull complete
d0d9e0ea897e: Pull complete
66e650438339: Pull complete
76a3dfe4406b: Pull complete
410ff9d97480: Pull complete
Digest: sha256:8e10956422503824ebb599f37c26a90fe70541942687f70bbdb744530fc9eba4
Status: Downloaded newer image for nginx:1.19.6
docker.io/library/nginx:1.19.6
[root@parrot]~#
```

9. Execute command **trivy image nginx:1.19.6** to scan the image.

Applications Places System trivy image nginx:1.19.6 - Parrot Terminal

```
[root@parrot]~!/home/attacker]
└─# docker pull nginx:1.19.6
1.19.6: Pulling from library/nginx
45b42c59be33: Pull complete
d0d9e0ea897e: Pull complete
66e650438339: Pull complete
76a3dfe4406b: Pull complete
410ff9d97480: Pull complete
Digest: sha256:8e10956422503824ebb599f37c26a90fe70541942687f70bbdb744530fc9eba4
Status: Downloaded newer image for nginx:1.19.6
docker.io/library/nginx:1.19.6
[root@parrot]~!/home/attacker]
└─# trivy image nginx:1.19.6
2024-05-24T09:11:10.061-0400  INFO  Detecting Debian vulnerabilities...
2024-05-24T09:11:10.084-0400  INFO  Trivy skips scanning programming language libraries because no supported file was detected

nginx:1.19.6 (debian 10.8)
-----
Total: 402 (UNKNOWN: 6, LOW: 29, MEDIUM: 168, HIGH: 149, CRITICAL: 50)

+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE
+-----+-----+-----+-----+-----+
| apt Ely13 Module 13 | CVE-2011-3374 | LOW | 1.8.2.2 | | It was found that apt-key in apt,
| Hacking Web | | | | | all versions, do not correctly...
| Servers | | | | | -->avd.aquasec.com/nvd/cve-2011-33
| 74 | | | | |
+-----+-----+-----+-----+-----+
| bash Ely13 Module 14 | CVE-2019-18276 | HIGH | 5.0-4 | | bash: when effective UID is not
| Hacking Web | | | | | equal to its real UID the...
| Applications | | | | |
+-----+-----+-----+-----+-----+
```

Menu trivy image nginx:1.19....

Applications Places System trivy image nginx:1.19.6 - Parrot Terminal

Fri May 24, 09:14

```
File Edit View Search Terminal Help
```

15	Parrot	CEHv13 Module 16	Hacking Wireless Networks		in valid_parameter_transform
15	bsdutils	CVE-2021-37600	MEDIUM	2.33.1-0.1	-->avd.aquasec.com/nvd/cve-2021-37600
500	attacker's Home				util-linux: integer overflow
500	README/license				can lead to buffer overflow
63	Trash	CVE-2022-0563			in get_sem_elements() in
63	CEHv13 Module 14				sys-utils/iputils.c...
81	coreutils	CVE-2016-2781	VERS	8.30-3	-->avd.aquasec.com/nvd/cve-2016-2781
81	CEHv13 Module 14				util-linux: partial disclosure
81	Hacking Web Applications				of arbitrary files in chfn
81					and chsh when compiled...
81					-->avd.aquasec.com/nvd/cve-2022-0563
81					coreutils: Non-privileged
81					session can escape to the
81					parent session in chroot
81					-->avd.aquasec.com/nvd/cve-2016-2781

Menu trivy image nginx:1.19....

The screenshot shows a terminal window titled "trivy image nginx:1.19.6 - Parrot Terminal". The terminal displays the output of a Trivy scan for the nginx:1.19.6 Docker image. The output is a table with columns for package name, CVE ID, severity, version, and description. The severity levels include CRITICAL, UNKNOWN, and PARTIAL. The descriptions provide details about specific vulnerabilities found in the image.

Severity	CVE ID	Version	Description
PARTIAL	CVE-2022-0563	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled...	
CRITICAL	CVE-2019-20367	libbsd0: 0.9.1-2+deb10u1	nlist.c in libbsd before 0.10.0 has an out-of-bounds read during a comparison...
UNKNOWN	DLA-3112-1	libbz2-1.0: 1.0.6-9.2~deb10u1	glibc: stack guard protection bypass
CRITICAL	CVE-2019-1010022	libc-bin: 2.28-10+deb10u1	-->avd.aquasec.com/nvd/cve-2019-1010022
	CVE-2021-33574	libc-bin: 2.28-10+deb10u2	glibc: mq_notify does not handle separately allocated thread attributes

10. In the above screenshot we can see that we have total **401** vulnerabilities which is categorized as well along with **CVEs** mentioned.
11. This concludes the demonstration of vulnerability assessment on docker images using Trivy
12. Close all open windows and document all acquired information.

#### Question 19.4.1.1

In Parrot machine install ubuntu and nginx:1.19.6 images and scan with trivy security scanner. Enter the severity level that can be observed for bsduutils vulnerability of nginx:1.19.6 docker image.