

# 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.

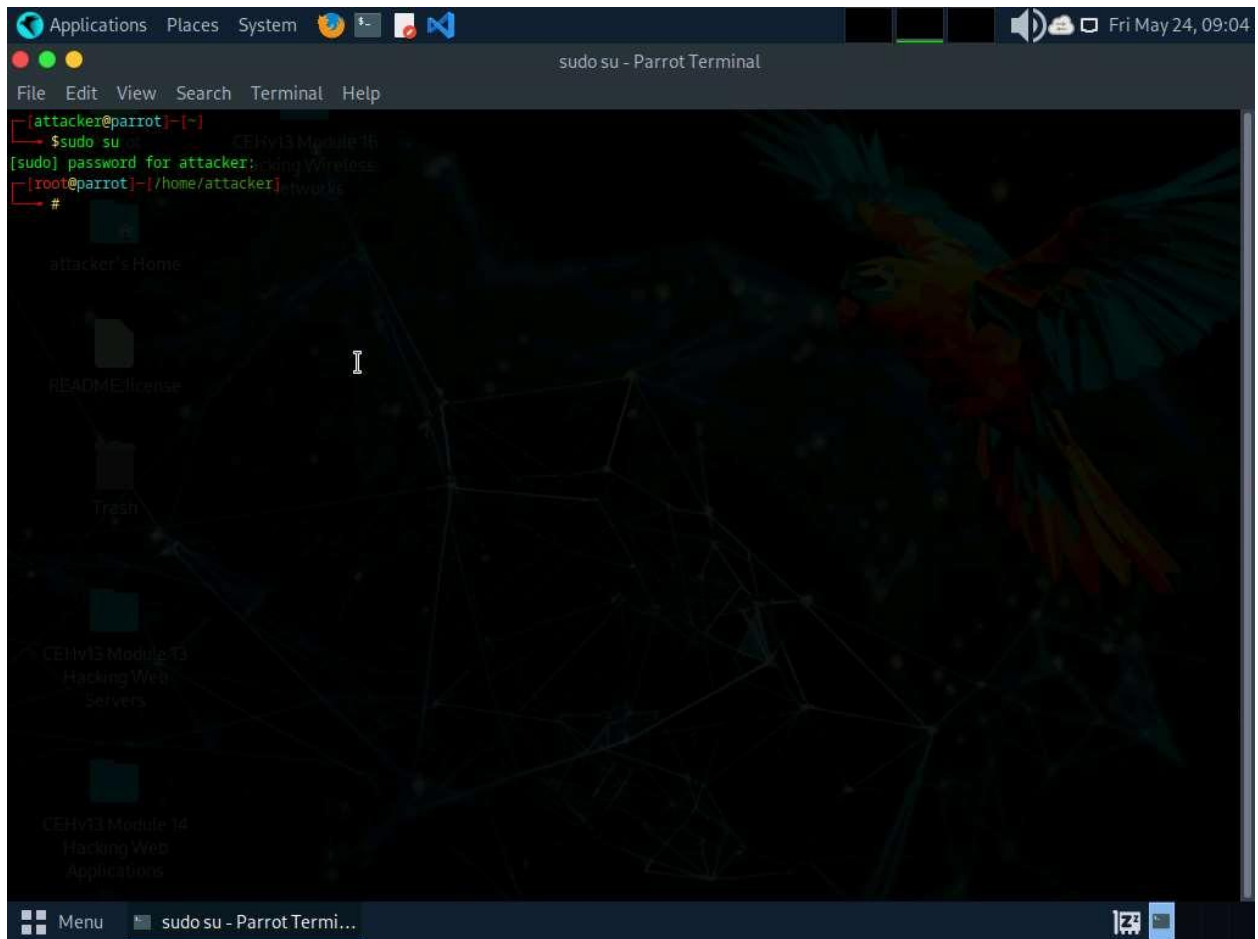
### Task 1: Vulnerability Assessment on Docker Images using Trivy

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.

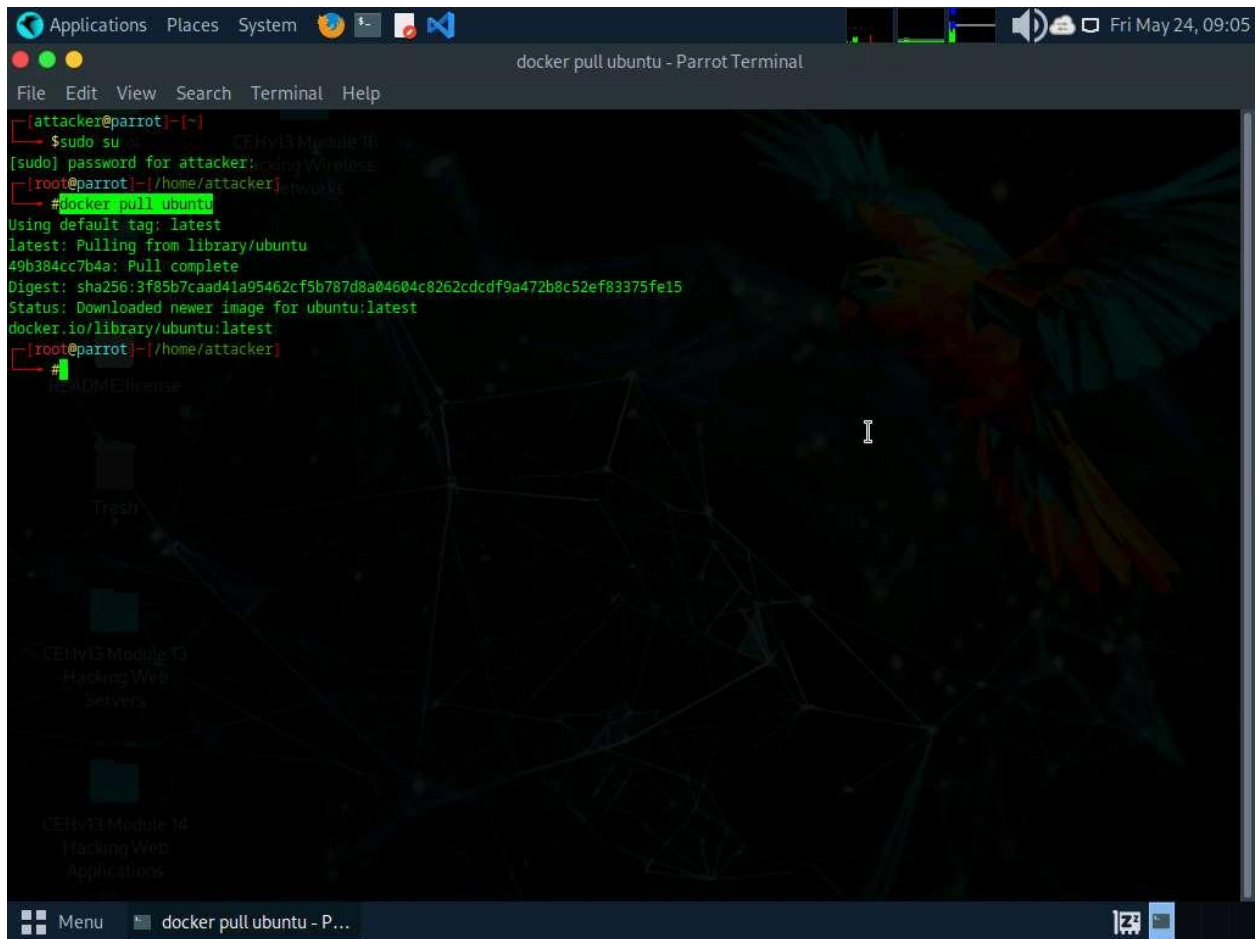
1. In the **Parrot Security** machine, click the **MATE Terminal** icon in the menu to launch the terminal.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type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

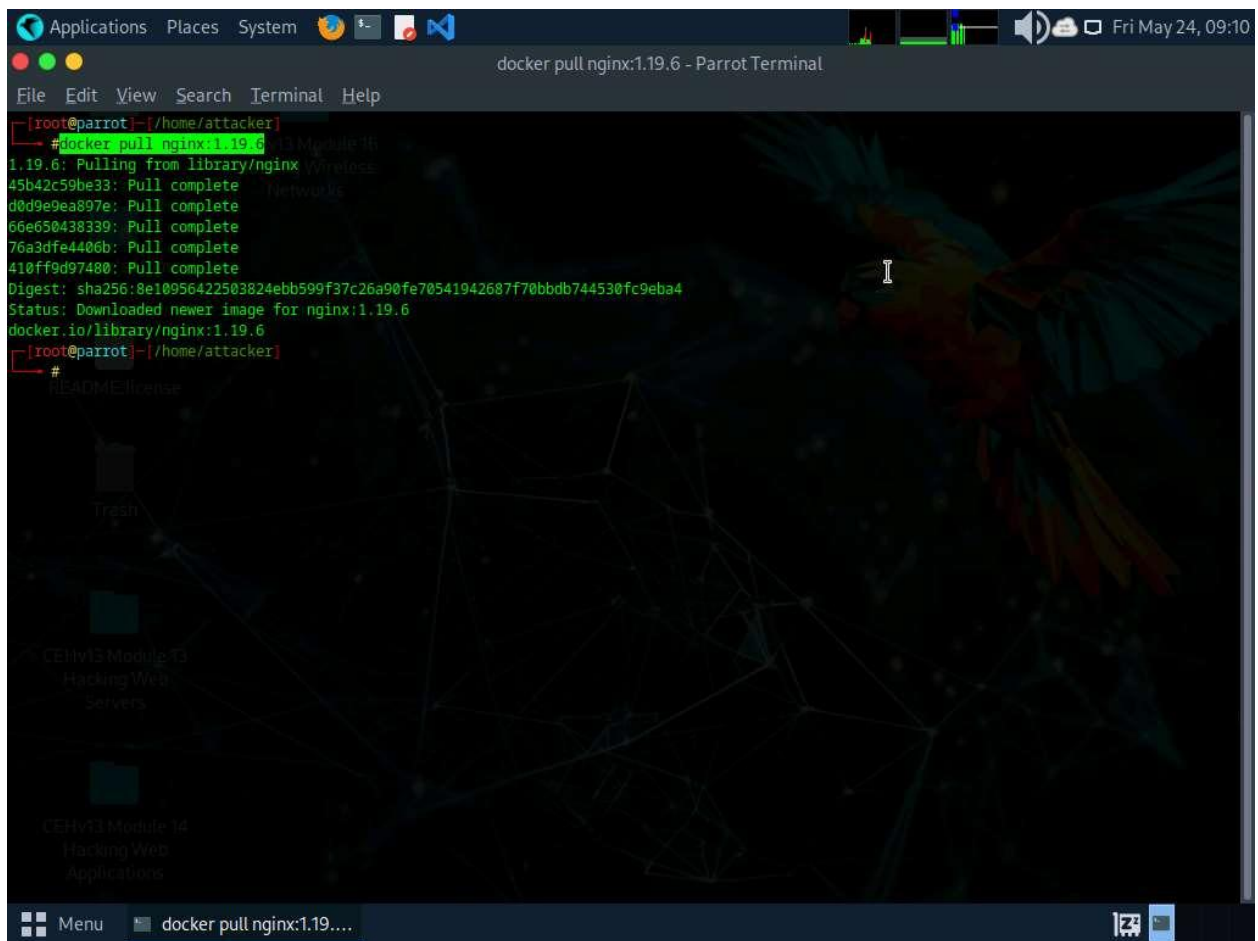


```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ docker pull ubuntu
Using default tag: latest
latest: Pulling from library/ubuntu
49b384cc7b4a: Pull complete
Digest: sha256:3f85b7caad41a95462cf5b787d8a04604c8262cdcdf9a472b8c52ef83375fe15
Status: Downloaded newer image for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

```
Applications Places System trivy image ubuntu - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[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]~$ #trivy image ubuntu
2024-05-24T09:06:53.400-0400 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)
[attacker@parrot]~$ #
```

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 vulnerbale image. execute command **docker pull nginx:1.19.6** to pull the vulnerable image.



```
Applications Places System docker pull nginx:1.19.6 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot:~/home/attacker]
# docker pull nginx:1.19.6
1.19.6: Pulling from library/nginx
45b42c59be33: Pull complete
d0d9e9ea897e: 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]
#
```

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

```
Applications Places System Fri May 24, 09:12
trivy image nginx:1.19.6 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# docker pull nginx:1.19.6
1.19.6: Pulling from library/nginx
45b42c59be33: Pull complete
d0d9e9ea897e: 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]~# 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 | CVE-2011-3374 | LOW | 1.8.2.2 | | It was found that apt-key in apt, | |
| | | | | | all versions, do not correctly... |
| | | | | | -->avd.aquasec.com/nvd/cve-2011-33 |
| 74 | | | | | | |
+-----+-----+-----+-----+-----+-----+
| bash | CVE-2019-18276 | HIGH | 5.0-4 | | bash: when effective UID is not |
| | | | | | equal to its real UID the... |
+-----+-----+-----+-----+-----+-----+
Menu trivy image nginx:1.19....
```

Applications Places System Fri May 24, 09:14

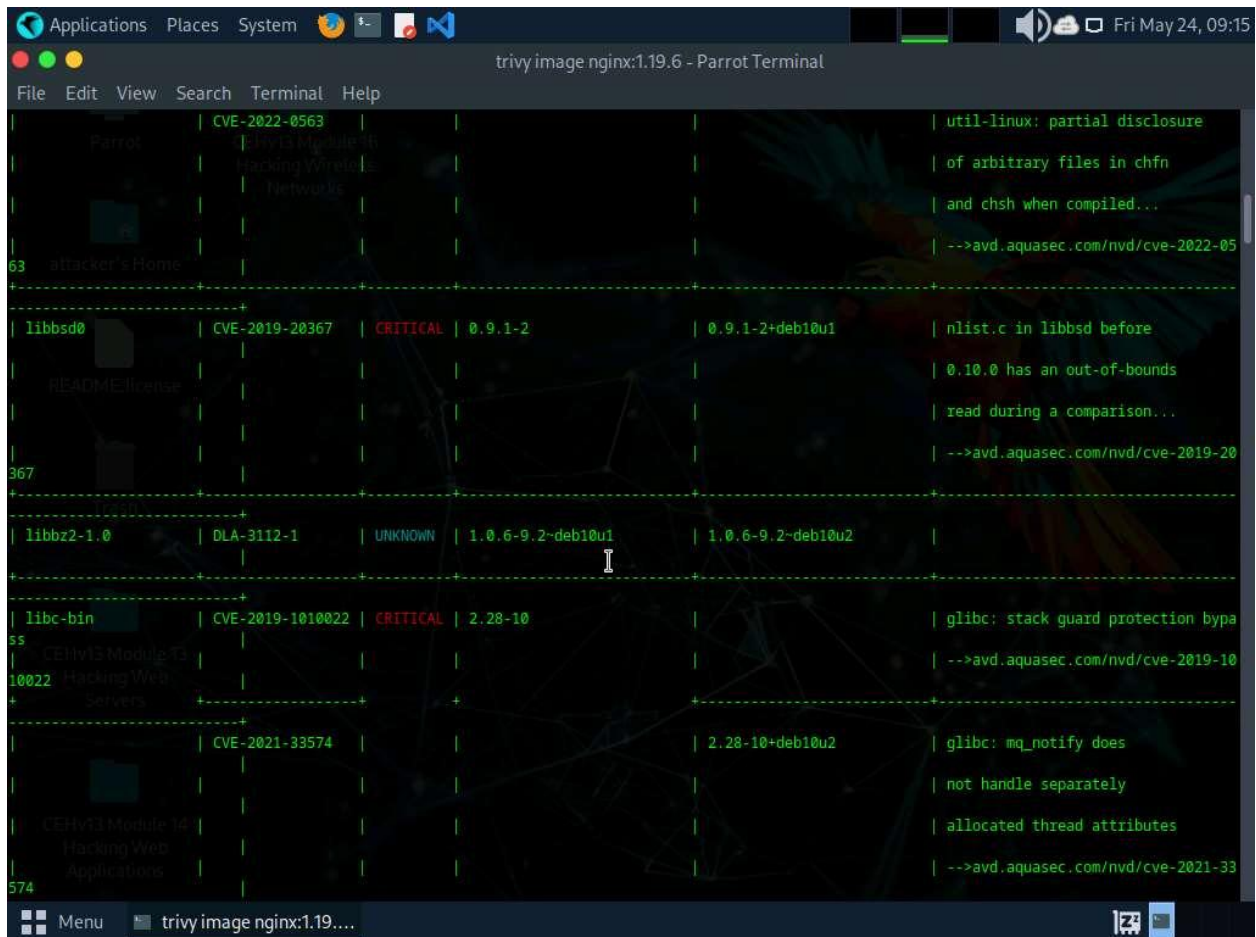
trivy image nginx:1.19.6 - Parrot Terminal

File Edit View Search Terminal Help

15	Parrot	CEHv13 Module 16	Hacking Wireless	Networks	in valid_parameter_transform	-->avd.aquasec.com/nvd/cve-2022-37
-----						
600	bsdutils	attacker's Home	CVE-2021-37600	MEDIUM	2.33.1-0.1	util-linux: integer overflow
						can lead to buffer overflow
						in get_sem_elements() in
						sys-utils/ipcutils.c...
						-->avd.aquasec.com/nvd/cve-2021-37
-----						
63	coreutils	Trash	CVE-2022-0563			util-linux: partial disclosure
						of arbitrary files in chfn
						and chsh when compiled...
						-->avd.aquasec.com/nvd/cve-2022-05
-----						
81	coreutils	CEHv13 Module 16	CVE-2016-2781		8.30-3	coreutils: Non-privileged
						session can escape to the
						parent session in chroot
						-->avd.aquasec.com/nvd/cve-2016-27

Menu trivy image nginx:1.19....





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 bsdutils vulnerability of nginx:1.19.6 docker image.