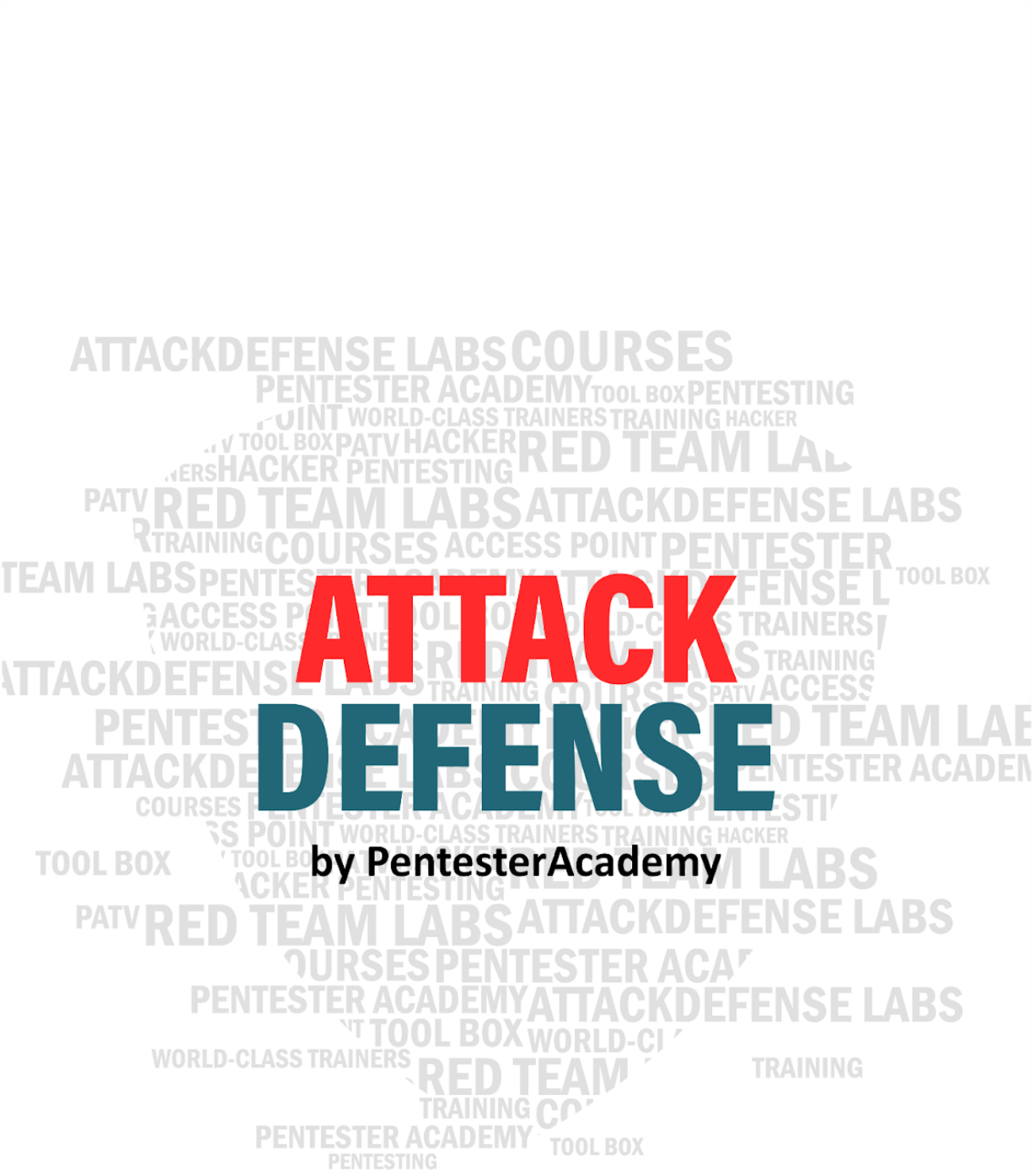
ATTACK
DEFENSE
by PentesterAcademy

Name	Clair
URL	https://attackdefense.com/challengedetails?cid=1620
Type	Docker Security : Docker Security Tools

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Run Clair on images and analyze the results!

Solution:

Step 1: Check the Docker images present on the local machine.

Command: docker images

```
root@localhost:~# docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
clairdb             latest              d91966a15669        8 days ago          554MB
nginx               latest              f7bb5701a33c        9 days ago          126MB
memcached           latest              b32d3ed7da92        9 days ago          82.2MB
ubuntu              18.04               775349758637        2 months ago        64.2MB
clair               latest              4dab8bd207b6        2 years ago         422MB
root@localhost:~#
```

Step 2: Check running Docker containers.

Command: docker ps

```
root@localhost:~# docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS
da842561dbde        clairdb             "docker-entrypoint.s…"   About a minute ago   Up About a minute
root@localhost:~#
```

Step 3: Run clair server Docker image (use the command provided in the challenge guidelines).

Command: docker run --rm -v /root/clair_config/:/config -p 6060-6061:6060-6061 -d clair -config="/config/config.yaml"

```
root@localhost:~# docker run --rm -v /root/clair_config/:/config -p 6060-6061:6060-6061 -d clair -config="/config/config.yaml"
fa8938bcfa4c70c265ed58908bda37865e6f5bb580e813c7f22ba503aba143f5
root@localhost:~#
```

Check running container to verify that the server container is running

```
root@localhost:~# docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS                              NAM
ES
fa8938bcfa4c        clair               "/clair -config=/con…"   14 seconds ago      Up 4 seconds        0.0.0.0:6060-6061->6060-6061/tcp   cra
zy_kilby
da842561dbde        clairdb             "docker-entrypoint.s…"   2 minutes ago       Up 2 minutes        5432/tcp                           upb
eat_sinoussi
root@localhost:~#
```

Step 4: Run clair scanner on Ubuntu image.

Command: clair-scanner -c http://172.17.0.3:6060 --ip 172.17.0.1 ubuntu

```
root@localhost:~# clair-scanner -c http://172.17.0.3:6060 --ip 172.17.0.1 ubuntu
2020/01/07 04:39:07 [INFO] ▶ Start clair-scanner
2020/01/07 04:39:19 [INFO] ▶ Server listening on port 9279
2020/01/07 04:39:19 [INFO] ▶ Analyzing cc59b0ca1cf21d77c81a98138703008daa167b1ab1a115849d498dba64e738dd
2020/01/07 04:39:23 [INFO] ▶ Analyzing 27a911bb510bf1e9458437f0f44216fd38fd08c462ed7aa026d91aab8c054e54
2020/01/07 04:39:23 [INFO] ▶ Analyzing d80735acaa72040a0a98ca3ae6891f9abb4e2f5d627b4099c4fefdc3ce1e696e
2020/01/07 04:39:23 [INFO] ▶ Analyzing 1ee34a985f7aef86436a5519f5ad83f866a74c7d9a0c22e47c4213ee9cb64e6d
2020/01/07 04:39:24 [WARN] ▶ Image [ubuntu] contains 32 total vulnerabilities
2020/01/07 04:39:24 [ERRO] ▶ Image [ubuntu] contains 32 unapproved vulnerabilities
```

The scanner will scan the image and list the possible present vulnerabilities in a table.

```
+------------+--------------------------+-------------+--------------------+-------------------------------------------------------------------
--+
| STATUS     | CVE SEVERITY             | PACKAGE NAME | PACKAGE VERSION    | CVE DESCRIPTION
  |
+------------+--------------------------+-------------+--------------------+-------------------------------------------------------------------
--+
| Unapproved | Medium CVE-2019-13627    | libgcrypt20  | 1.8.1-4ubuntu1.1   | It was discovered that there was a ECDSA timing attack
  |
|            |                          |              |                    | in the libgcrypt20 cryptographic library. Version
  |
|            |                          |              |                    | affected: 1.8.4-5, 1.7.6-2+deb9u3, and 1.6.3-2+deb8u4.
  |
|            |                          |              |                    | Versions fixed: 1.8.5-2 and 1.6.3-2+deb8u7.
  |
```

```
--+
| Unapproved | Medium CVE-2018-11237       | glibc        | 2.27-3ubuntu1       | An AVX-512-optimized implementation of the mempcpy
  |
|            |                             |              |                     | function in the GNU C Library (aka glibc or libc6) 2.27 and
  |
|            |                             |              |                     | earlier may write data beyond the target buffer, leading
  |
|            |                             |              |                     | to a buffer overflow in __mempcpy_avx512_no_vzeroupper.
  |
|            |                             |              |                     | http://people.ubuntu.com/~ubuntu-security/cve/CVE-2018-11237
```

In this manner, clair-scanner can be used to scan other images.

References:

1. Docker (https://www.docker.com/)
2. Clair (https://github.com/quay/clair)