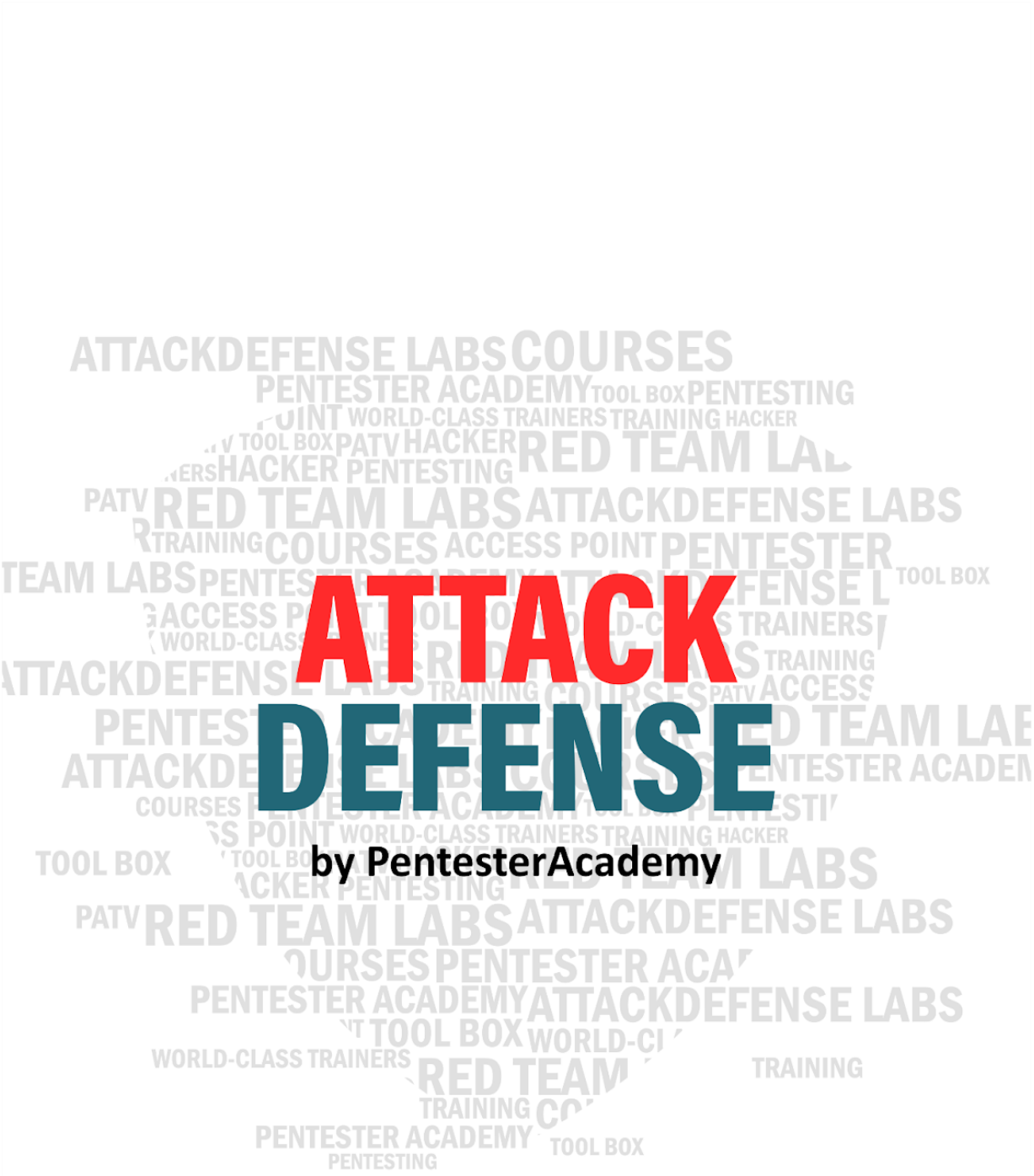
ATTACK
DEFENSE
by PentesterAcademy

Name	Dockscan
URL	https://attackdefense.com/challengedetails?cid=1608
Type	DevSecOps : 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 Dockscan on the setup and observe the results!

Solution:

Step 1: Run dockscan with help option to see all available options and switches.

Command: dockscan -h

```
root@localhost:~# dockscan -h
Usage: dockscan [options]
    -v, --[no-]verbose               Run verbosely
    -d, --[no-]debug                 Run in debug mode
    -h, --help                       Prints this help
    -o, --output NAME                use NAME for output filename
    -r, --report NAME                use NAME for report format
    -l, --log FILE                   log to FILE

Example #1: dockscan -r html -o myreport -v tcp://example.com:5422
Example #2: dockscan unix:///var/run/docker.sock
root@localhost:~#
```

Step 2: Run dockscan on the machine in verbose mode.

Command: dockscan -v unix:///var/run/docker.sock

```
root@localhost:~# dockscan -v unix:///var/run/docker.sock
I, [2020-01-03T23:36:10.118540 #1564]  INFO -- : Validating version specified: unix:///var/run/docker.sock
I, [2020-01-03T23:36:10.931078 #1564]  INFO -- : Loading discovery modules...
I, [2020-01-03T23:36:10.937893 #1564]  INFO -- : Loading discovery module: /var/lib/gems/2.5.0/gems/dockscan-
r/get-docker-version.rb
I, [2020-01-03T23:36:10.944735 #1564]  INFO -- : Loading discovery module: /var/lib/gems/2.5.0/gems/dockscan-
r/get-containers.rb
I, [2020-01-03T23:36:10.950870 #1564]  INFO -- : Loading discovery module: /var/lib/gems/2.5.0/gems/dockscan-
r/get-run-containers.rb
```

Dockscan will run different discovery modules.

```
I, [2020-01-03T23:36:10.969264 #1564]  INFO -- : Running discovery modules...
I, [2020-01-03T23:36:10.970369 #1564]  INFO -- : Running discovery module: GetDockerVersion
I, [2020-01-03T23:36:11.486560 #1564]  INFO -- : Running discovery module: GetContainers
I, [2020-01-03T23:36:11.539062 #1564]  INFO -- : Running discovery module: GetContainersRunning
I, [2020-01-03T23:36:11.563195 #1564]  INFO -- : Running discovery module: GetDockerInfo
I, [2020-01-03T23:36:12.082264 #1564]  INFO -- : Running discovery module: GetImages
```

And print a summarized report in the end.

```
Dockscan Report

Medium
Docker running without defined limits: It is recommended to define docker limits.
Docker running with IPv4 forwarding enabled: It is recommended to disable IPv4 forwarding by default.

Low
Container have higher number of changed files: It is recommended to have minimal number of changed files inside container and do not store data
 inside container. It is recommended to use volumes.
```

The dockerscan report is recommending to:

- Define docker limits (apply cgroup to containers)
- Disable IPv4 forwarding
- Keep the files changed on runtime to minimum by using volume for changing files.

```
I, [2020-01-03T23:37:50.173446 #1564]  INFO -- : Running report module: ReportHTML
I, [2020-01-03T23:37:50.173833 #1564]  INFO -- : Running report module: ReportText
W, [2020-01-03T23:37:50.174399 #1564]  WARN -- : Following modules failed: DockerInsecureRegistries
root@localhost:~#
```

It also warns about about allowing an insecure registry in the configuration.

References:

1. Docker (https://www.docker.com/)
2. Dockscan (https://github.com/kost/dockscan)