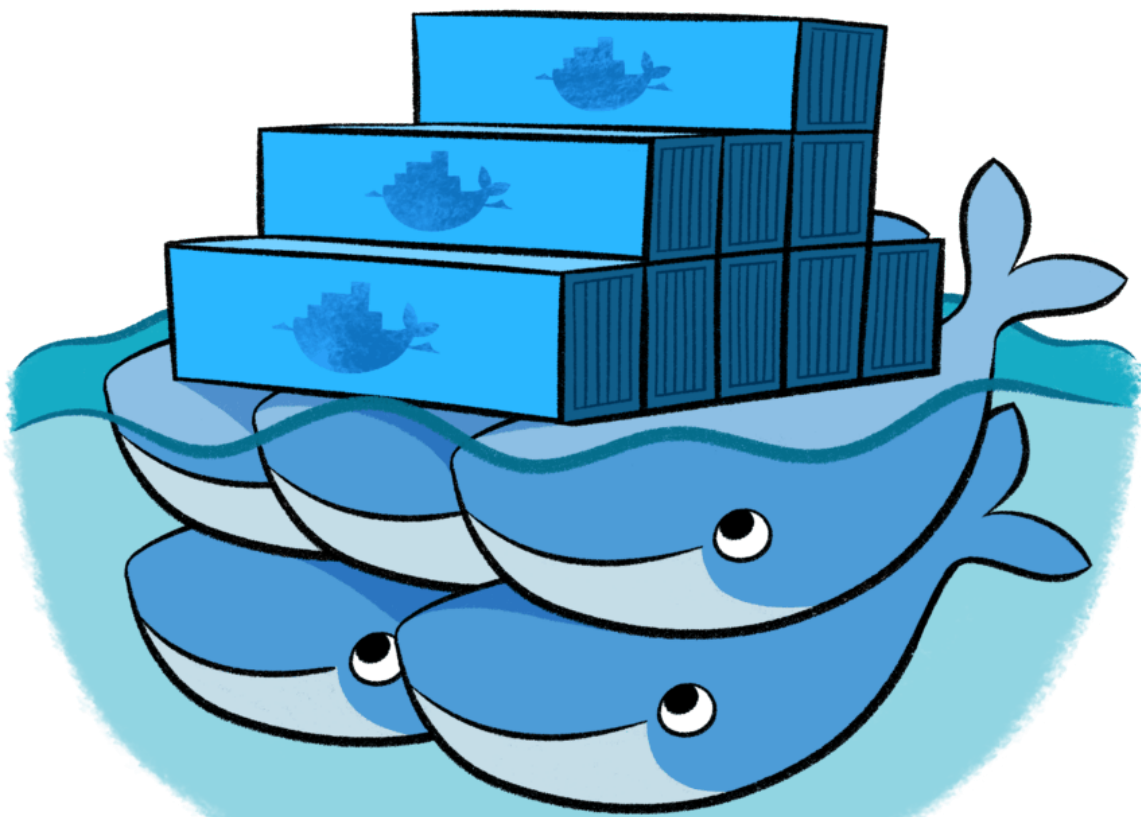




HOME / BLOG / HOW TO PREPARE AND USE DOCKER FOR WEB PENTEST BY JÚNIOR CARREIRO

# How to prepare and use Docker for web pentest by Júnior Carreiro



We use cookies to offer you a better browsing experience, analyze site traffic, personalize content, and serve targeted advertisements. Read about how we use cookies and how you can control them by clicking "Privacy Preferences". If you continue to use this site, you consent to our use of cookies.

[Privacy Preferences](#)

I Agree

1.8k  
SHARES



Introduction

Offline. Leave a Message.

software containerization platform. Using Docker we can create different

---

environments for each Pentest type. With the use of containers, you can save each environment on a USB stick or leave it in the cloud. For example, you can use the environment in the cloud or copy to any computer or laptop, regardless of distribution. You need only install Docker, if it is not installed.

## Live CD x Containers

Already there are several distributions for PenTest, all in Live CD, but the LiveCD requires a greater effort; you have to create a flash drive or bootable CD or even create a VirtualBox installation, for example.

When we use containers the only thing we need to do is to install Docker, which is simple and easy and then we use the image created by putting it on a stick, in repository files or using the Docker HUB, saving time and providing portability.

## What is Docker?

Docker is an open source technology that lets you create, run, test, and deploy distributed applications within software containers. Docker allows you to deploy applications quickly, reliably and stably in any environment.

## Why use Docker?

Because the containers are portable, convenient and fast. With Docker, we can create an image and use it as the basis for each environment we create. For example, we download the basic container Kali Linux, which does not come with the tools installed. Let's see that from this basic container, can go installing the tools I need and then save with a new name, without the original container, to be, affected.

Thus being able, from the base image, create a container with tools for forensics, a container with tools to PenTest web, for example.


## Tools for web PenTest

For our container, we use some familiar tools but for this article we will cover only tools used via the console.

- W3af-console
- SQLMap

- Arachni
- Nikto
- Websploit
- Nmap

## Installation

Offline. Leave a Message. 

depend largely on OS you are using, but nowadays we can find it using the

For our article, I will use OpenSuse.

*S | Nome | Resumo | Tipo*

```
_0x4a0x72@pwned ~ sudo zypper in docker
```

```
_0x4a0x72@pwned ~ sudo systemctl enable docker
```

```
_0x4a0x72@pwned ~ sudo systemctl start docker
```

```
_0x4a0x72@pwned ~ sudo docker info
```

Containers: 0

Running: 0

Paused: 0

Stopped: 0

*Images: 0*

Server Version: 1.11.2

*Storage Driver: btrfs*

**Build Version: Btrfs v4.5.3+20160516**

.....

Docker Root Dir: /var/lib/docker

*Debug mode (server): false*

We use cookies to offer you a better browsing experience, analyze site traffic, personalize content, and serve targeted advertisements. Read about how we use cookies and how you can control them by clicking "Privacy Preferences". If you continue to use this site, you consent to our use of cookies.

*Registry: https://index.docker.io/v1/*

task.

Using the command **sudo docker search Kali**, we list the images that are in Docker HUB, but let's take the first one, which is recommended by the staff of offsec

```
_0x4a0x72@pwned ~ sudo docker search kali
```

```
NAME DESCRIPTION STARS OFFICIAL AUTOMATED
```

```
kalilinux/kali-linux-docker Kali Linux Rolling Distribution Base Image 193 [OK]
```

Let's do the pull image for our machine, This step depends on the internet connection.

```
_0x4a0x72@pwned ~ sudo docker pull kalilinux/kali-linux-docker
```

```
Using default tag: latest
```

```
latest: Pulling from kalilinux/kali-linux-docker
```

```
b2860afd831e: Pull complete
```

```
340395ad18db: Pull complete
```

```
d4ecedcfaa73: Pull complete
```

```
3f96326089c0: Pull complete
```

```
e5b4b7133863: Pull complete
```

```
Digest: sha256:0aa8342172aacbe79957f66e7029c1fb38e14765bf35eff30624f90cb813a56f
```

```
Status: Downloaded newer image for kalilinux/kali-linux-docker:latest
```

```
_0x4a0x72@pwned ~ sudo docker images
```

```
REPOSITORY TAG IMAGE ID CREATED SIZE
```

```
kalilinux/kali-linux-docker latest f321257d50f7 6 days ago 602.4 MB
```

To start the container, we can use the command:

```
_0x4a0x72@pwned ~ sudo docker run --name WebPentest -t -d kalilinux/kali-linux-docker
```

We use cookies to offer you a better browsing experience, analyze site traffic, personalize content, and serve targeted advertisements. Read about how we use cookies and how you can control them by clicking "Privacy Preferences". If you continue to use this site, you consent to our use of cookies.

```
a5fb073e53c8 kalilinux/kali-linux-docker "/bin/bash" 10 seconds ago Up 8 seconds WebPentest
```

## Tools Installation

To perform the installation we can make it out of the container, but I will show how to access the container shell.

---

```
_0x4a0x72@pwned ~ sudo docker exec -it WebPentest bash
```

```
root@a5fb073e53c8:/#
```

After accessing the shell, we will update the container and install the tools that we use in our Web Penetration Test and install tools.

```
root@a5fb073e53c8:/# apt-get update
```

```
root@a5fb073e53c8:/# apt-get upgrade
```

```
root@a5fb073e53c8:/# apt-get install websploit w3af-console arachni nikto sqlmap websploit nmap
```

Once the installation is completed, you can execute commands normally inside the container.

```
root@a5fb073e53c8:/# nmap localhost
```

```
Starting Nmap 7.12 ( https://nmap.org ) at 2016-06-30 09:09 UTC
```

```
Nmap scan report for localhost (127.0.0.1)
```

```
Host is up (0.000010s latency).
```

```
Other addresses for localhost (not scanned): ::1
```

```
All 1000 scanned ports on localhost (127.0.0.1) are closed
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Or run outside of container.

\*Once you've completed those instructions you can disconnect, or detach, from the shell without exiting by using the escape sequence **Ctrl-p + Ctrl-q**

```
_0x4a0x72@pwned ~ sudo docker exec -it WebPentest nikto
```

```
- Nikto v2.1.6
```

---

```
+ ERROR: No host specified
```

```
We use cookies to offer you a better browsing experience, analyze site traffic, personalize
+config+ content, and serve targeted advertisements. Read about how we use cookies and how you can
control them by clicking "Privacy Preferences". If you continue to use this site, you consent to
.....
our use of cookies.
```

```
+ requires a value
```

```
Note: This is the short help output. Use -H for full help text.
```

Offline. Leave a Message. 

save the image, use the commit

`_0x4a0x72@pwned ~ sudo docker commit -a "Junior Carreiro" -m "Install Web Pentest Tools" WebPentest`

## Conclusion

With the use of Docker containers, we can create the PenTest environments or audits according to our need, leaving separated by categories. We can also deliver the container that is used in a PenTest as part of the evidence that is presented to a customer or deliver the container to the customer to do an audit.

### About the author: Júnior Carreiro

Member of DC-Labs Security Team

Founder BlackTieSecurity

<https://br.linkedin.com/in/juniorcarreiro>

[https://twitter.com/\\_0x4a0x72](https://twitter.com/_0x4a0x72)

---

🕒 JULY 4, 2016

### LEAVE A REPLY

---

Start the discussion...

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)

✉ Subscribe ▼

We use cookies to offer you a better browsing experience, analyze site traffic, personalize content, and serve targeted advertisements. Read about how we use cookies and how you can control them by clicking "Privacy Preferences". If you continue to use this site, you consent to our use of cookies.

SEARCH

Offline. Leave a Message. ✉

## Newsletter

Signup for newsletter to receive free Articles !

☐ Yes, please sign me up for newsletters. This includes offers, latest news, and exclusive promotions

Subscribe

FREE CONTENT

### RELATED BRANDS

HAKING

eForensics  
M a g a z i n e

### OUR PRODUCTS

We use cookies to offer you a better browsing experience, analyze site traffic, personalize content, and serve targeted advertisements. Read about how we use cookies and how you can control them by clicking "Privacy Preferences". If you continue to use this site, you consent to our use of cookies.

### COMPANY

About

All Instructors

Offline. Leave a Message. 

[Become an author](#)

[Become Instructor](#)

[Blog](#)

#### SUPPORT

[Contact Us](#)

[FAQs](#)

#### MORE

[Terms and conditions](#)

[Privacy Policy](#)

© HAKIN9 MEDIA SP. Z O.O. SP. K. 2013



We use cookies to offer you a better browsing experience, analyze site traffic, personalize content, and serve targeted advertisements. Read about how we use cookies and how you can control them by clicking "Privacy Preferences". If you continue to use this site, you consent to our use of cookies.

Offline. Leave a Message. 