Taller pentesting en Docker

docker

/via: http://www.elladodelmal.com/2018/09/como-montar-un-entorno-de-pentesting.html
/via: http://www.elladodelmal.com/2018/09/como-montar-un-entorno-de-pentesting_14.html

previos

- uso red **bridge** :

```
docker network ls
docker network inspect bridge
```

- descarga imagen Kali Linux :

```
docker pull kalilinux/kali-linux-docker
docker run -it --name Kali kalilinux/kali-linux-docker /bin/bash
```

- actualizar el OS:

```
apt update
apt dist-upgrade
apt autoremove
apt clean
```

  - instalar el **top-10** de aplicaciones en Kali:

```
apt install kali-linux-top10
```

- para volver a acceder al contenedor en las mismas condiciones:

```
docker start Kali
docker exec -it Kali /bin/bash
```

  - o crear una nueva imagen para levantar un nuevo contenedor:

```
docker run -it Kaliv2 /bin/bash
```

  - más info: https://medium.com/@airman604/kali-linux-in-a-docker-container-5a06311624eb

montando contenedores vulnerables

contenedores docker con vulnerabilidades:

- HeartBleed : **hmlio/vaas-cve-2014-0160**

```
docker pull hmlio/vaas-cve-2014-0160
docker run -d -p 8443:443 --name Pentesting_HeartB hmlio/vaas-cve-2014-0160
```

- SQLi : **tuxotron/audi_sqli**

```
docker pull tuxotron/audi_sqli
```

```
docker run -d -p 80:80 --name Pentesting_SQLi tuxotron/audi_sqli
```

para averiguar la IP de cada contenedor sin conectarnos al mismo:

```
docker inspect -f '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}'
Pentesting_SQLi
```

para parar todos los contenedores y hacer limpieza:

ATENCIÓN!

```
# parará todos los contenedores en marcha
docker container stop $(docker container ls -a -q)

# (OJO!) eliminará todas las imágenes que no estén en uso (OJO!)
docker system prune -a
```

detectando y ejecutando vulnerabilidades

```
nmap -p 443 --script ssl-heartbleed 172.17.0.x
mfconsole
```

resumen del proceso : https://youtu.be/2GnX64-kwm4