Implantación de Suricata en Docker

- Descarga de una imagen de Ubuntu:

```
alberto@alberto-VirtualBox:~/git$ docker pull ubuntu
Using default tag: latest
latest: Pulling from library/ubuntu
08c01a0ec47e: Already exists
Digest: sha256:669e010b58baf5beb2836b253c1fd5768333f0d1dbcb834f7c07a4dc93f474be
Status: Downloaded newer image for ubuntu:latest
docker.io/library/ubuntu:latest
alberto@alberto-VirtualBox:~/git$ docker images
REPOSITORY   TAG       IMAGE ID       CREATED       SIZE
ubuntu       latest    54c9d81cbb44   2 weeks ago   72.8MB
```

- Iniciamos el contenedor:

```
alberto@alberto-VirtualBox:~/git$ docker run -it ubuntu
root@ed0b73c79d63:/#
```

- Levantamos un servidor http con Python en otra máquina que permitirá la descarga remota del script de instalación de Suricata:

```
┌──(worldsleaks㉿kali)-[~]
└─$ sudo python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.1.114 - - [19/Feb/2022 16:46:13] "GET /rushme_suricata.sh HTTP/1.1" 200 -
```

```
root@7702698b8cc0:/# wget http://192.168.1.122:8000/rushme_suricata.sh
--2022-02-19 15:46:17--  http://192.168.1.122:8000/rushme_suricata.sh
Connecting to 192.168.1.122:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 42358 (41K) [text/x-sh]
Saving to: 'rushme_suricata.sh'

rushme_suricata.sh      100%[=============================>]  41.37K  --.-KB/s    in 0.001s

2022-02-19 15:46:17 (56.2 MB/s) - 'rushme_suricata.sh' saved [42358/42358]
```

- Debido a que el contenedor de Ubuntu que estamos usando viene con lo mínimo por defecto, hemos instalado el servicio Suricata a mano pues era menos costoso que actualizar a mano el sistema para que el script pueda funcionar bien. A continuación, podemos ver como el servicio está corriendo en el sistema:

```
root@7702698b8cc0:/# service suricata status
suricata is running with PID 6133
```

- Una vez tenemos el servicio instalado, guardamos el contenedor en otra imagen distinta para mantener su estado actual: