



# Examen Práctico Virtualización

Pablo Ribas Borrego

---

1. Repositorio (URL) de Github, conteniendo el archivo Dockerfile.

<https://github.com/AWDn0n/22041278> KaliLinux Examen

2. Captura donde se aprecie claramente vuestra imagen de Docker con la versión de Kali Linux y los paquetes solicitados.

```
PS C:\Users\pablo\Documents\KaliLinux-Examen> docker build -t awdn0n/kalilinux-examen-22041278 .
[+] Building 129.5s (8/8) FINISHED
=> [internal] load .dockerignore                                0.0s
=> => transferring context: 2B                                  0.0s
=> [internal] load build definition from Dockerfile             0.0s
=> => transferring dockerfile: 1.21kB                          0.0s
=> [internal] load metadata for docker.io/kalilinux/kali-rolling:latest 0.0s
=> [1/4] FROM docker.io/kalilinux/kali-rolling                0.0s
=> CACHED [2/4] RUN apt-get update                             0.0s
=> [3/4] RUN apt-get update && apt-get install -y nano nmap python3.6 python3-distutils py 125.1s
=> [4/4] RUN apt-get clean                                     0.6s
=> exporting to image                                          3.7s
=> => exporting layers                                          3.7s
=> => writing image sha256:0fa3679243aefce4e363d3a75fe5d3127a31418389217ce49c54f0c759706aff 0.0s
=> => naming to docker.io/awdn0n/kalilinux-examen-22041278    0.0s
```

3. Captura donde se vea que no hay vulnerabilidades en vuestra imagen.

The screenshot shows the Docker Scout interface for the image `awdn0n/kalilinux-examen-22041278:latest`. The interface includes a header with the image name, a 'CREATED' timestamp, a 'SIZE' of 732.08 MB, and a 'Run' button. A purple banner at the top states: 'Advanced image analysis is provided by Docker Scout (Early Access). Upgrade to continue to get access to guided vulnerability remediation and additional software supply chain features. [Learn more](#) and [upgrade](#).' Below this, the 'Image hierarchy' section shows the image is built from `FROM kalilinux/kali-rolling:amd64, latest`. The 'Layers (20)' section lists 20 layers, including `ARG BUILD_DATE`, `ARG BUILD_DATE VERSION`, `ARG BUILD_DATE PROJECT_URL VERSION`, `ARG BUILD_DATE PROJECT_URL VCS_REF VERSI...`, `ARG BUILD_DATE PROJECT_URL TARBALL VCS...`, `ARG BUILD_DATE PROJECT_URL RELEASE_DESC...`, `LABEL org.opencontainers.image.created=$BUIL...`, `ADD file:a6eb12a37fe82a3d307c8667b2bb84aec...`, and `ENV LANG=C.UTF-8`. The 'Vulnerabilities (0)' section shows a search bar and a message: 'No vulnerabilities were detected in this image'.

4. Captura de la ejecución del container, con el OS actual.

```
(root@de0e3f6e1ad7)-[/]\KaliLinux-Examen> docker run -it --rm --name kalilinux-examen-container-22041278 awdn0n/kalilinux-examen-22041278
# uname -a
Linux de0e3f6e1ad7 5.15.90.1-microsoft-standard-WSL2 #1 SMP Fri Jan 27 02:56:13 UTC 2023 x86_64 GNU/Linux
```

5. Captura del lanzamiento de nmap en busca de servicios y puertos.

```
(root@de0e3f6e1ad7)-[/]  
# nmap -sS 192.168.1.1 -F  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 14:22 UTC  
Nmap scan report for 192.168.1.1  
Host is up (0.0043s latency).  
Not shown: 98 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 3.11 seconds
```

6. Subid vuestra imagen a Docker Hub y adjuntar la url de la misma.

<https://hub.docker.com/repository/docker/awdn0n/kalilinux-examen-22041278>