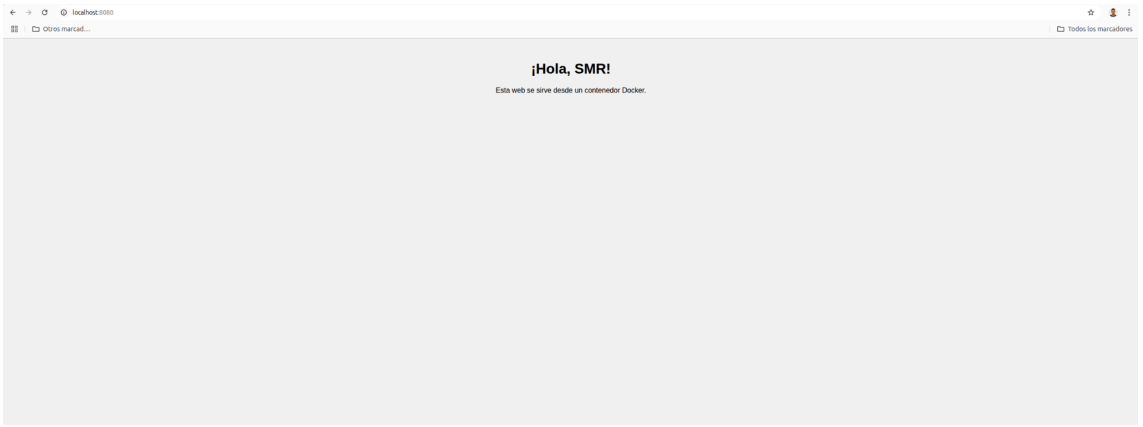
Mapeo con Nmap

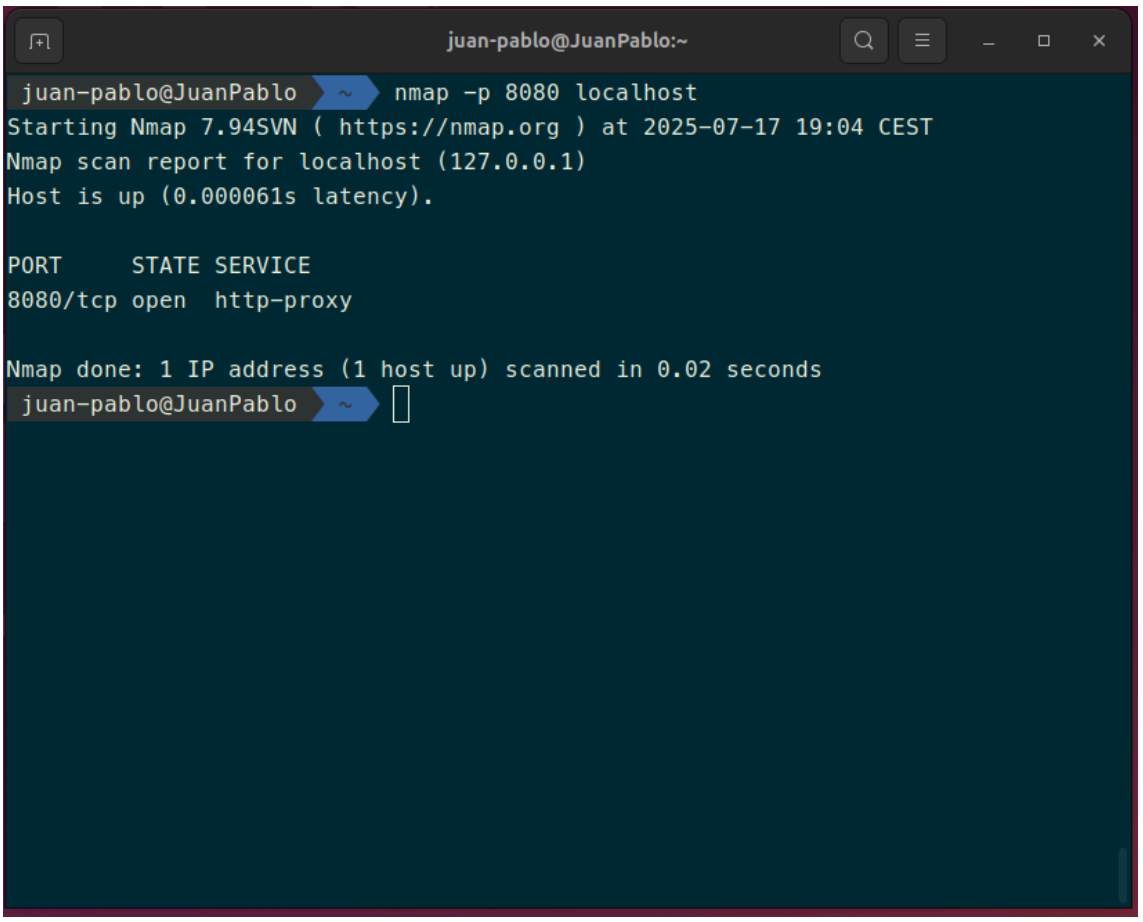
1. Comprobación del contenedor en funcionamiento.

Como en la práctica con Docker nos dirigiremos al navegador e introduciremos http://localhost:8080 para comprobar que nuestro contenedor está funcionando correctamente.



2. Escaneo de contenedor con Nmap.

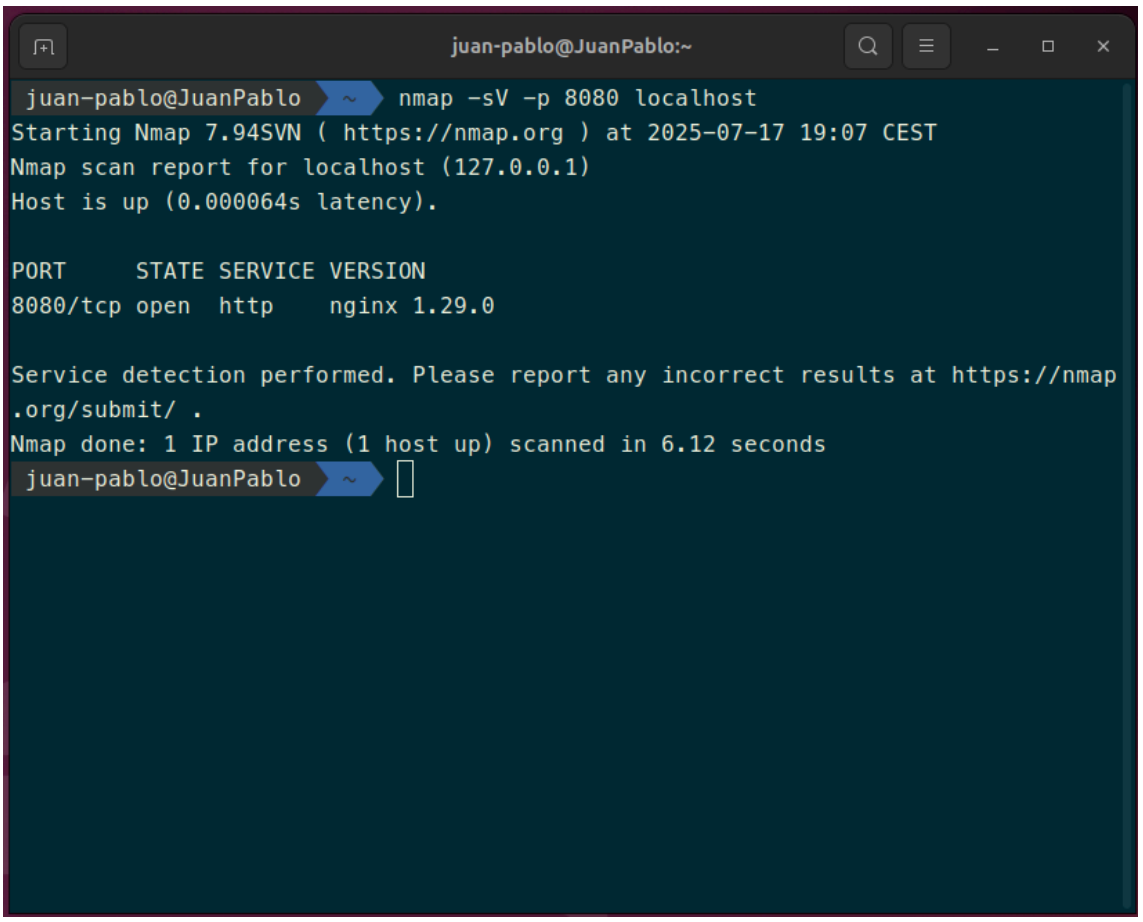
Lo siguiente que haremos será realizar un escaneo del contenedor. Con el comando nmap -p 8080 localhost realizaremos el escaneo apuntando al puerto y al host.



Aquí nos mostrará distintos datos como la ip 127.0.0.1 , el puerto 8080/tcp, estado del contenedor open y el servicio http-proxy.

3.Escaneo de detección de servicios.

Ahora realizaremos un escaneo más detallado para detectar información adicional. Para ello usaremos el comando nmap -sV -p 8080 localhost.

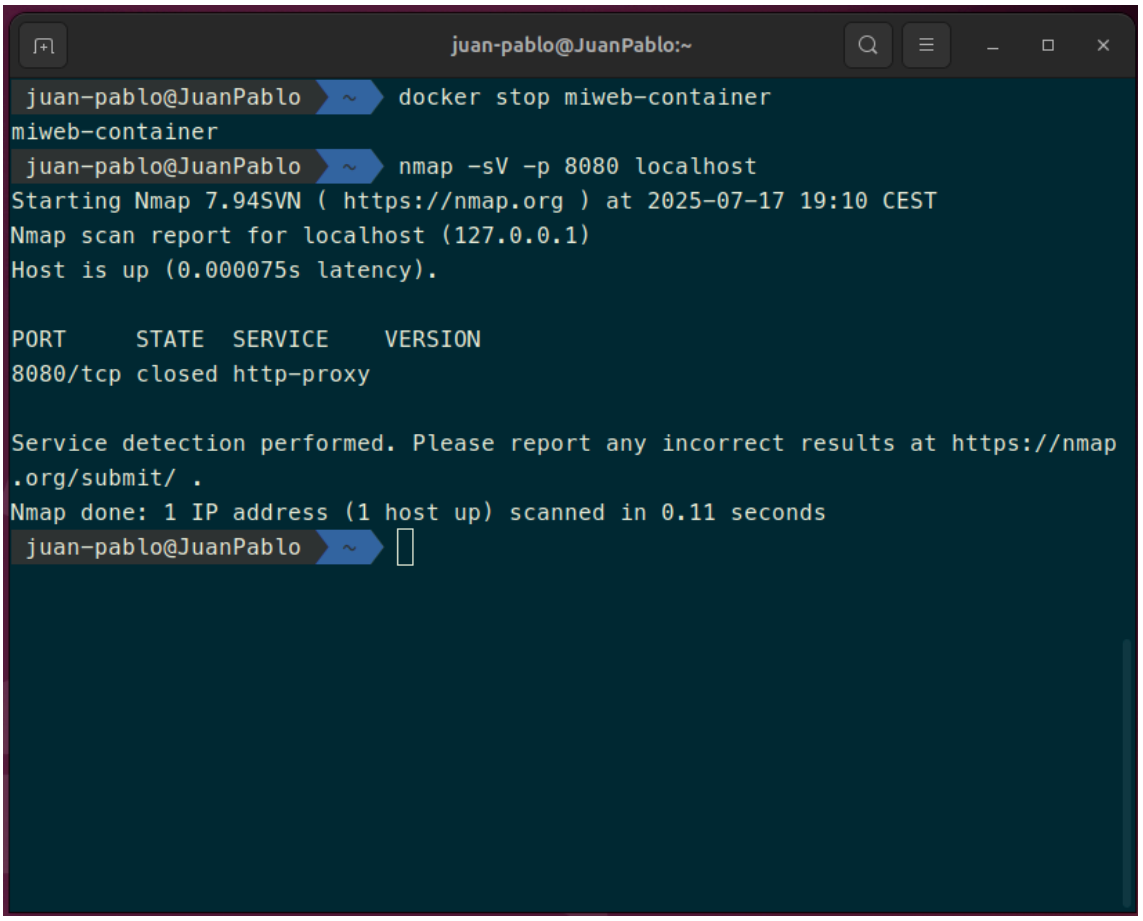


Este escaneo a parte de mostrarnos los datos anteriores nos muestra el software específico que está atendiendo ese puerto, nginx y su versión 1.29.0.

Esta información no sería segura que estuviese expuesta a redes externas por varias razones, como la exposición de la versión específica ya que un atacante podría buscar vulnerabilidades en ella, posible mapeo del entorno o podría facilitar ataques dirigidos al conocer el servicio.

4.Detener el contenedor y repetir el escaneo.

En este último paso vamos a detener el contenedor usando el comando docker stop miweb-container. Después volveremos a usar el comando de escaneo para comprobar que el contenedor se ha detenido, utilizaremos de nuevo nmap -sV -p 8080 localhost.



Como podemos comprobar donde antes en estado nos aparecía open, ahora nos muestra closed, esto quiere decir que nuestro contenedor se paró correctamente. Tampoco nos aparece nginx puesto que el contenedor no está en funcionamiento.

Reflexión final

Exponer puertos y servicios en red sin controles adecuados puede ser peligroso ya que los escaneos nmap permiten a un atacante conocer los servicios y versiones de nuestro contenedor. Sería importante para la seguridad que tuviésemos los servicios actualizados, limitar el acceso a puertos a través de firewalls y monitorizar la red para detectar escaneos sospechosos entre otras más medidas.