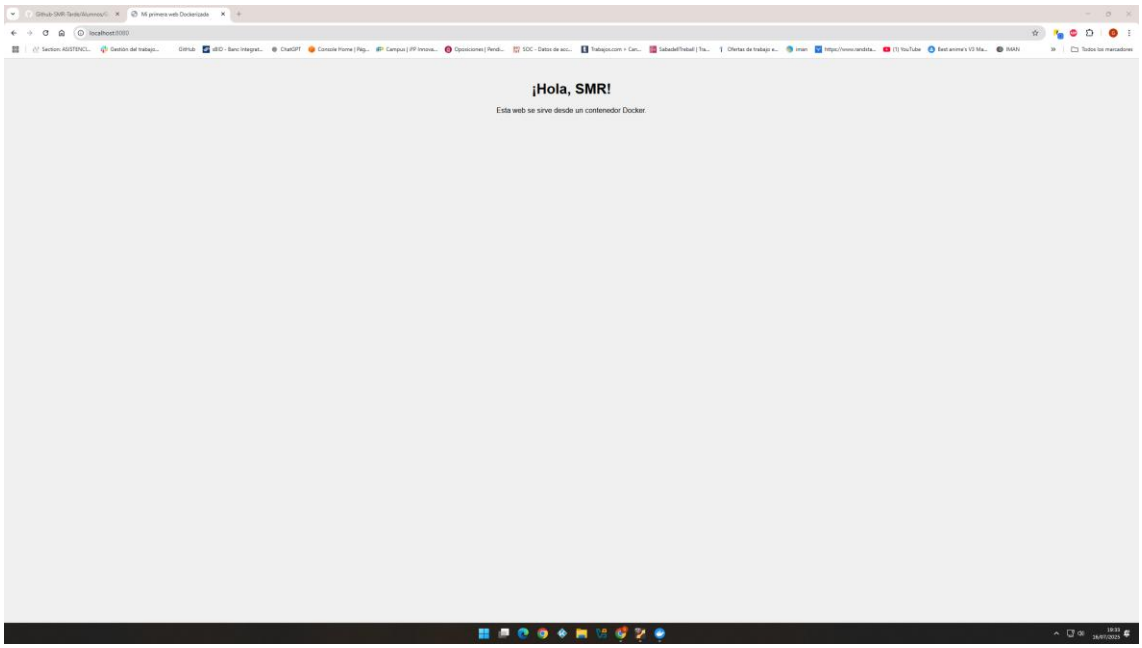
# Escaneo Nmap

## PASO 1:Comprueba que tu contenedor está funcionando




## Paso 2: Escaneo básico con Nmap

nmap -p 8080 localhost

**Puerto detectado y estado:**

- Puerto **8080/tcp**
- Estado: **open** (abierto)
- Servicio: http-proxy (esto es el servicio detectado por defecto)

## Paso 3: Escaneo con detección de servicios

nmap -sV -p 8080 localhost

- Puerto 8080 está abierto.
- El servicio detectado es HTTP.

- Versión detectada: **nginx 1.29.0**

**Reflexión:**

Que la versión y el tipo de servicio estén visibles desde el exterior puede representar un riesgo de seguridad, porque un atacante podría explotar vulnerabilidades específicas de esa versión o servicio. Por eso, en entornos de producción es recomendable ocultar o limitar la información que se expone y mantener el software actualizado.

## Paso 4: Detén el contenedor y repite el escaneo

**Comando utilizado para detener el contenedor:**

docker stop miweb-container

**Comando utilizado para el escaneo:**

nmap -sV -p 8080 localhost

**Resultado del escaneo:**

PORT STATE SERVICE VERSION

8080/tcp closed http-proxy

**Descripción del cambio respecto al escaneo anterior:**

- El puerto 8080 aparece ahora **cerrado**.
- Antes estaba abierto y con servicio NGINX activo.
- Ahora no hay servicio escuchando en ese puerto porque el contenedor fue detenido.

**Explicación del cambio:**

Al detener el contenedor, el servidor web (NGINX) que estaba corriendo dentro del contenedor dejó de funcionar, por lo que el puerto 8080 dejó de estar disponible en el host. Por eso Nmap detecta el puerto cerrado.

**Reflexión final sobre la visibilidad de servicios en la red**

La visibilidad de servicios y puertos abiertos en una red es crucial para la seguridad informática. Puertos abiertos y servicios detectables pueden ser vectores de ataque si no están debidamente protegidos. Por eso, es importante limitar la exposición de servicios, usar firewalls, y mantener los servicios actualizados para evitar vulnerabilidades. Herramientas como Nmap permiten a

los administradores y también a posibles atacantes mapear qué servicios están disponibles, por lo que controlar esta información es fundamental para proteger sistemas.