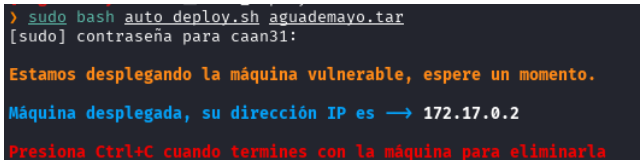
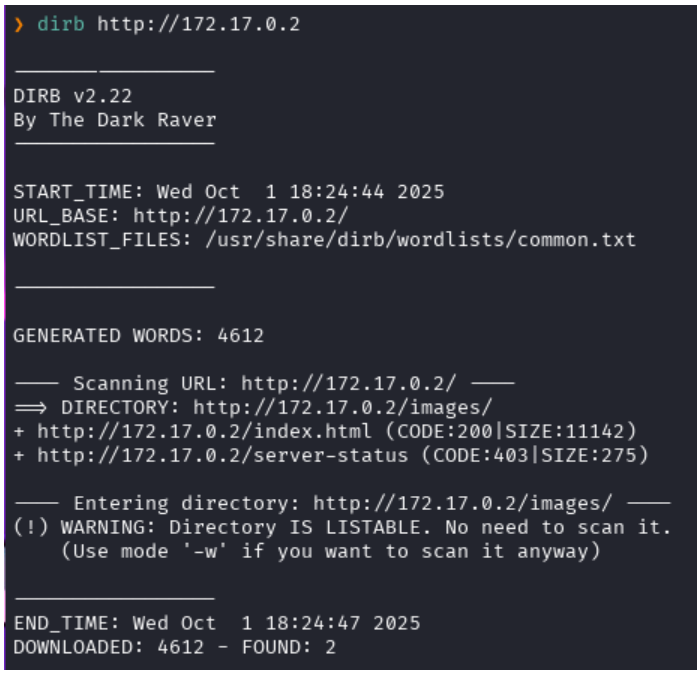
Vamos a desplegar la maquina vulnerable

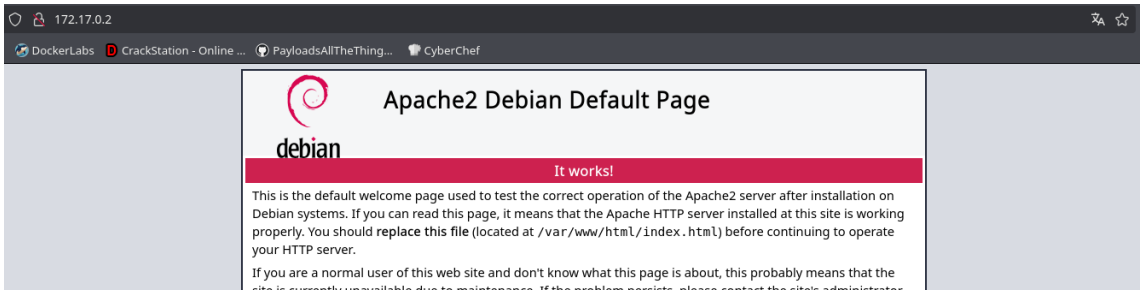


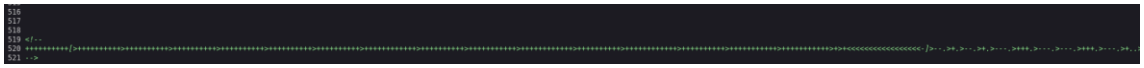
Haremos un escaneo profundo de los puertos abiertos de la maquina vulnerable.

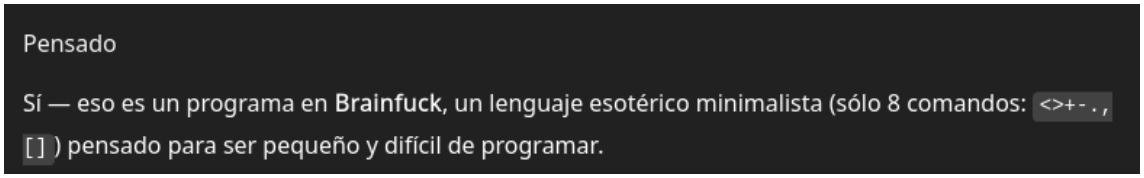
Como vemos que tiene un servidor web vamos a ver si cuenta con algún directorio oculto que podamos explorar con dirb



Vemos que en el código fuente de la pagina principal un comentario raro, así que le preguntaremos a chatgpt para que nos ayude a saber que es.

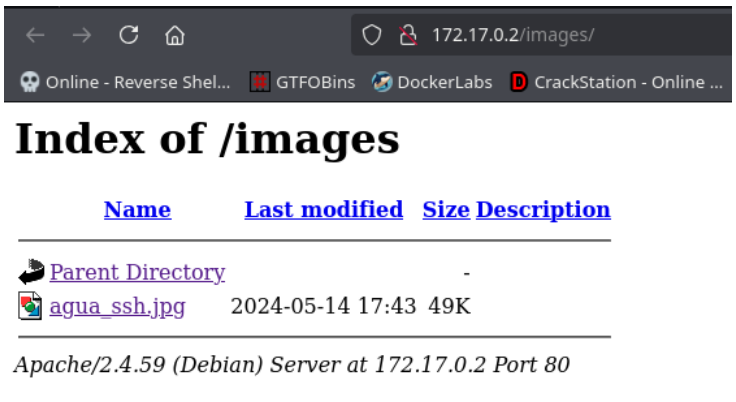




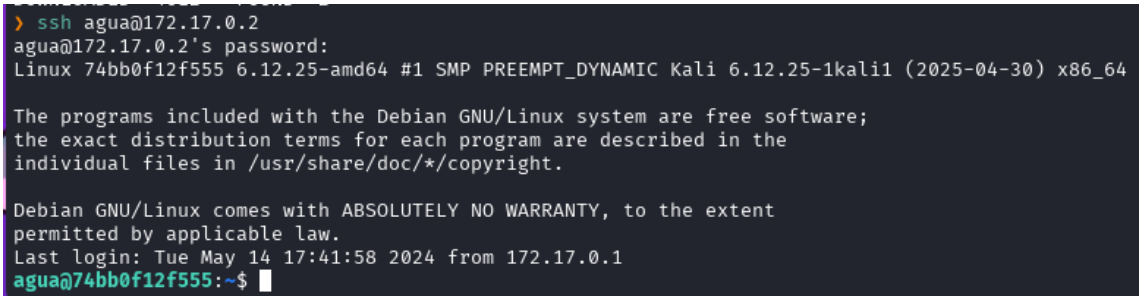


Ahora utilizaremos dcode.fr para descifrarlo.

Ahora en el otro directorio que encontramos es una imagen llamada agua_ssh, hice pruebas y no encontré nada, así que suponemos que es un usuario de ssh y la contraseña la que tenemos de antes.

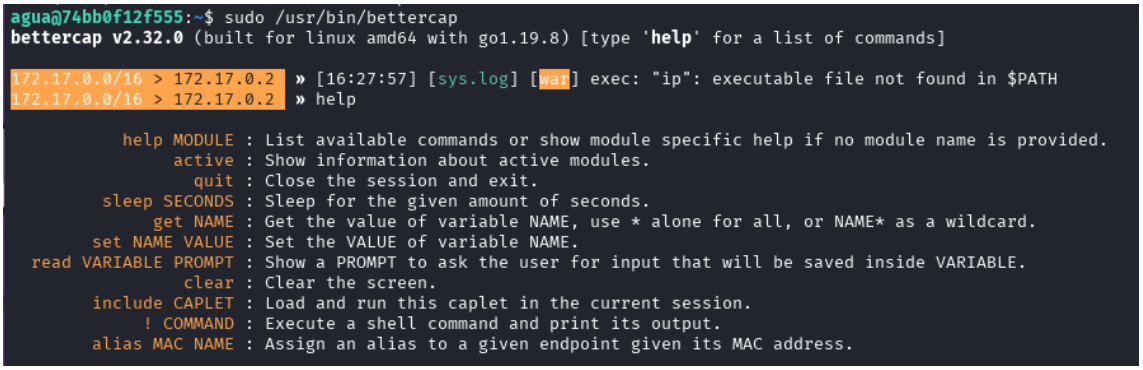


Nos conectamos por ssh y vemos que tenemos acceso al usuario.



Para ver el escalado de privilegios ejecutamos sudo -l y vemos que tenemos permisos, mirándolo es un ejecutable, así que lo ejecutamos.

Vemos que nos permite ejecutar help y ver de que trata, con la ayuda nos damos cuenta de que si escribimos ! y a continuación algún comando lo ejecuta como un Shell.



Ejecutamos el comando para poder tener luego una consola interactiva como root, aunque ya ejecutándolo antes éramos root.