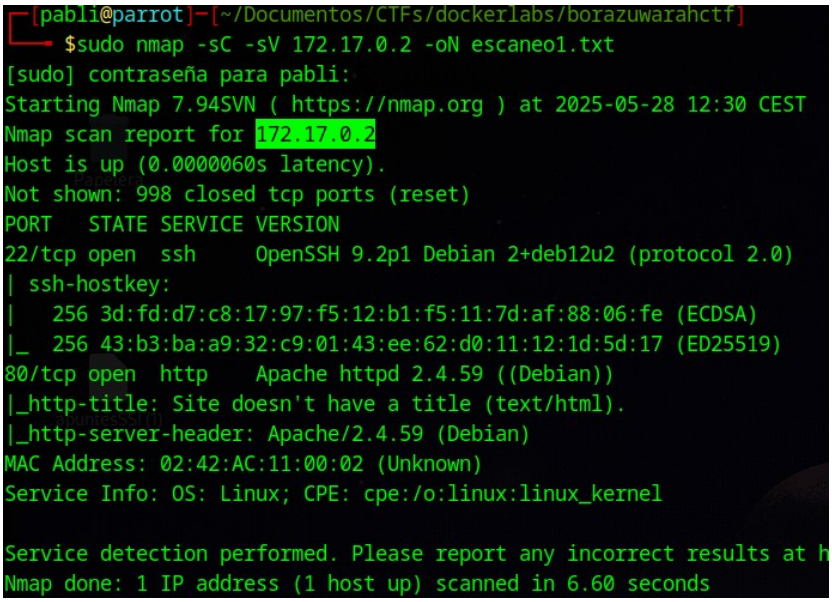
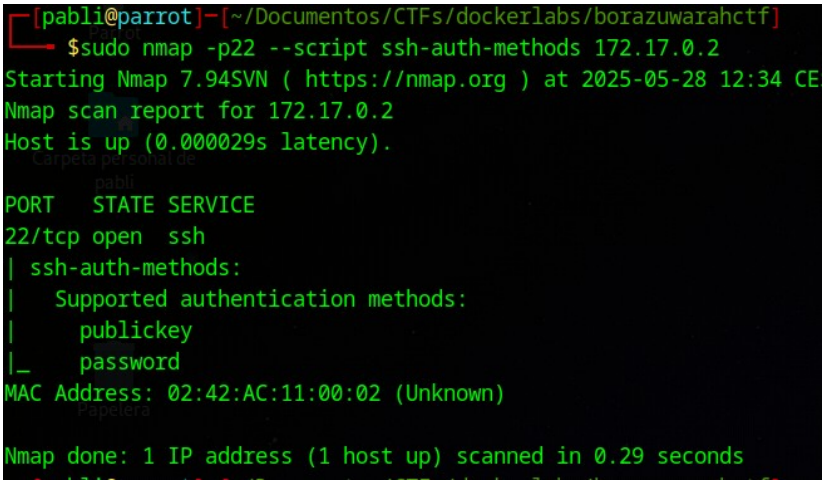
Dockerlabs

Máquina: borazuwarahctf
Pablo José Pérez Díez

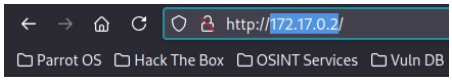
Enumeración:



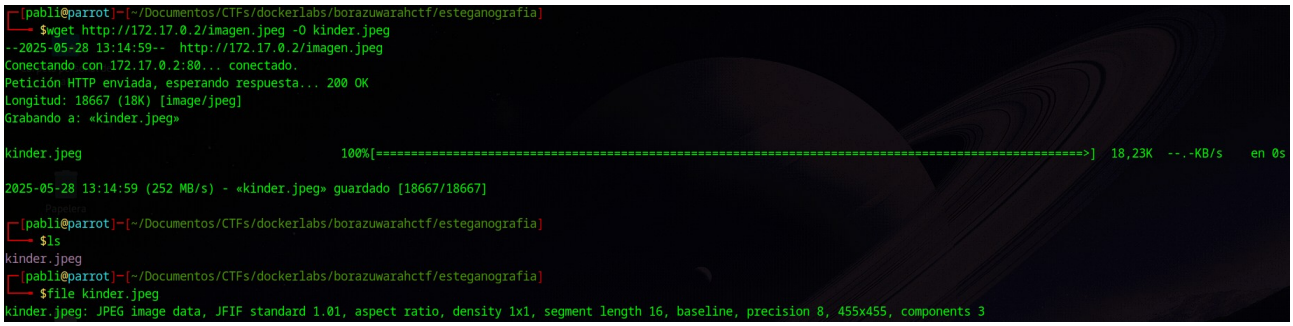


En un primer momento, se intentó, sin éxito, encontrar vulnerabilidades en las versiones de SSH y Apache.

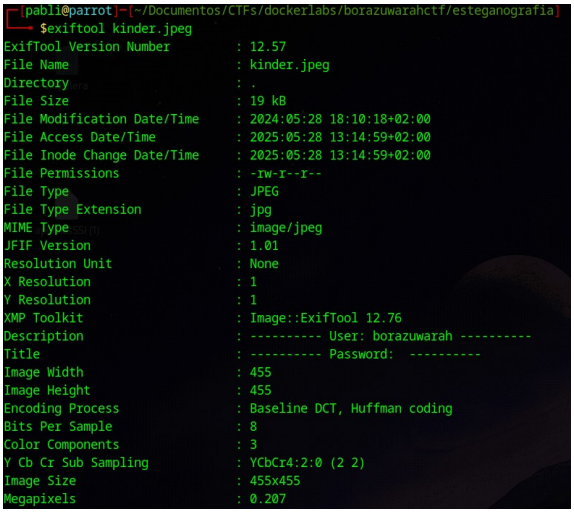
Comprobamos más a fondo el contenido de la web y nos fijamos en la imagen:



En este punto, y tras descartar los ataques y exploits a SSH y Apache, intentamos descubrir si se está usando esteganografía para guardar ciertas credenciales, así que nos bajamos la imagen:

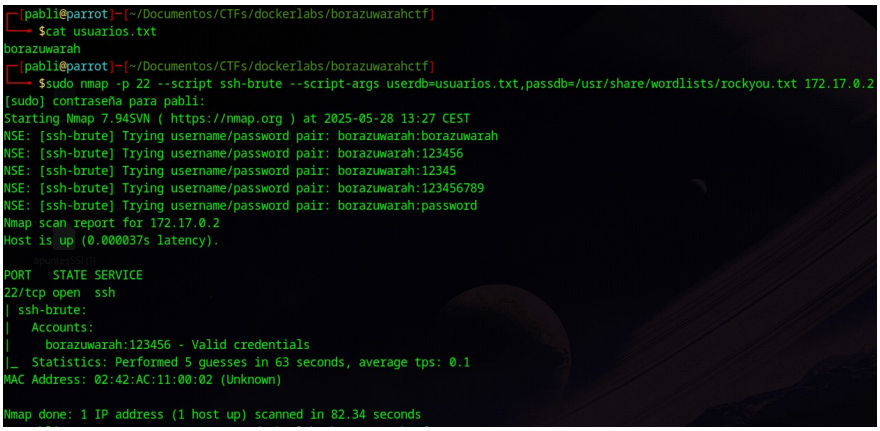


Antes de usar herramientas de esteganografía, observamos los metadatos de la imagen utilizando exiftool para ver si contienen algo interesante:

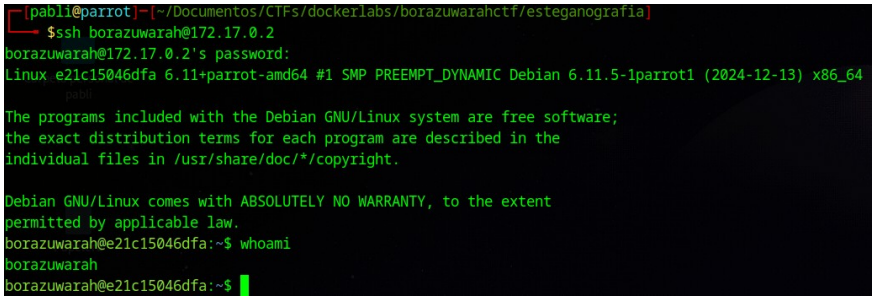


Como podemos observar obtenemos un nombre de usuario: **borazuwarah**

Utilizando fuerza bruta con un script NSE de Nmap y ese usuario en SSH conseguimos unas credenciales válidas:



Accedemos al sistema:



Al parecer, nuestro usuario ya tiene privilegios máximos en el sistema, por lo que habríamos terminado: