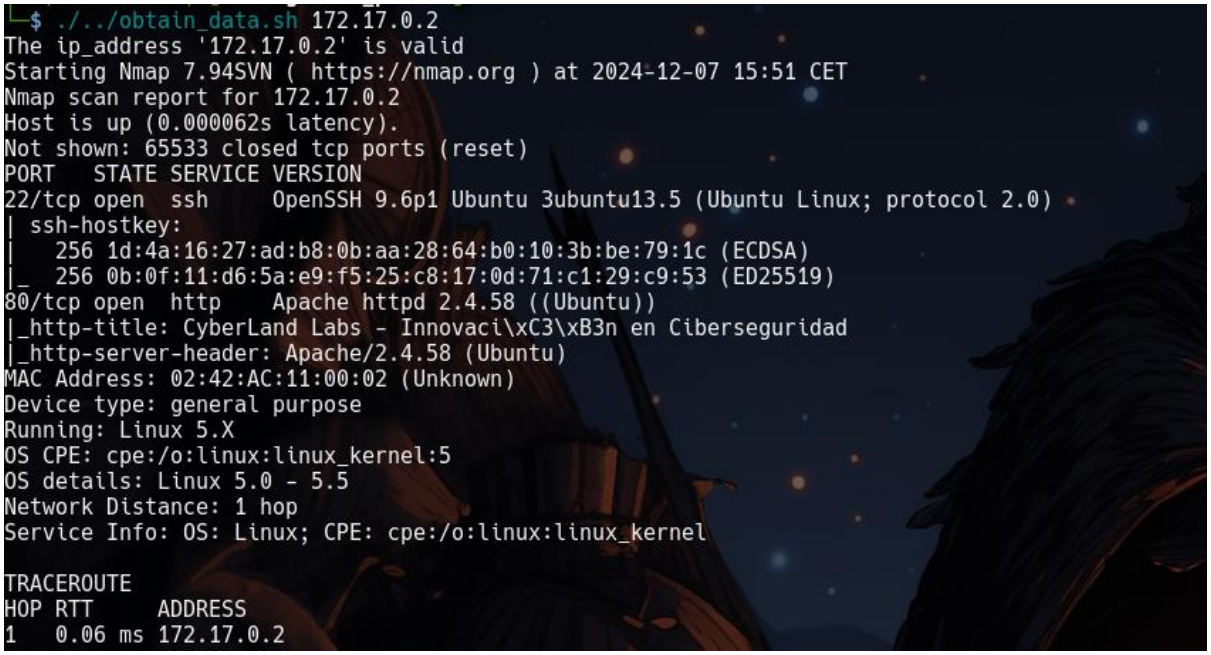
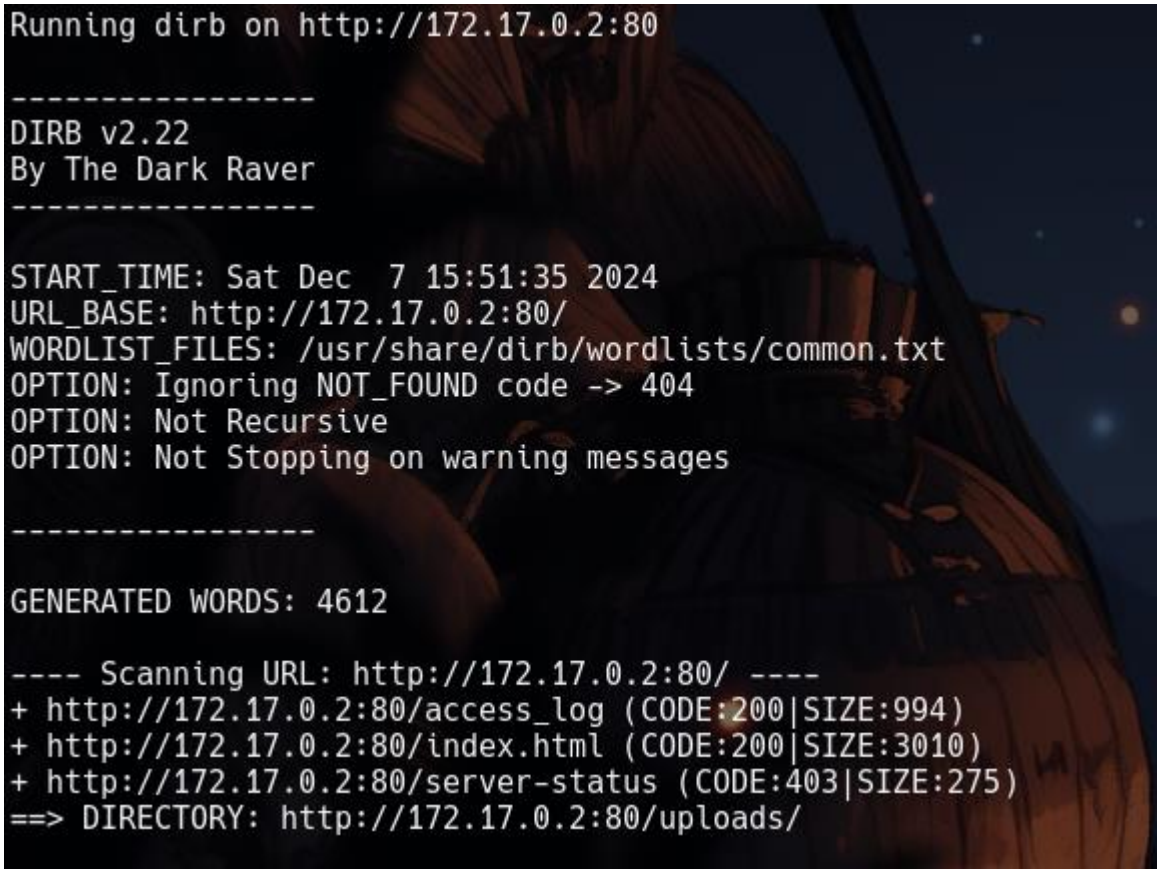
FORGOTTEN PORTAL

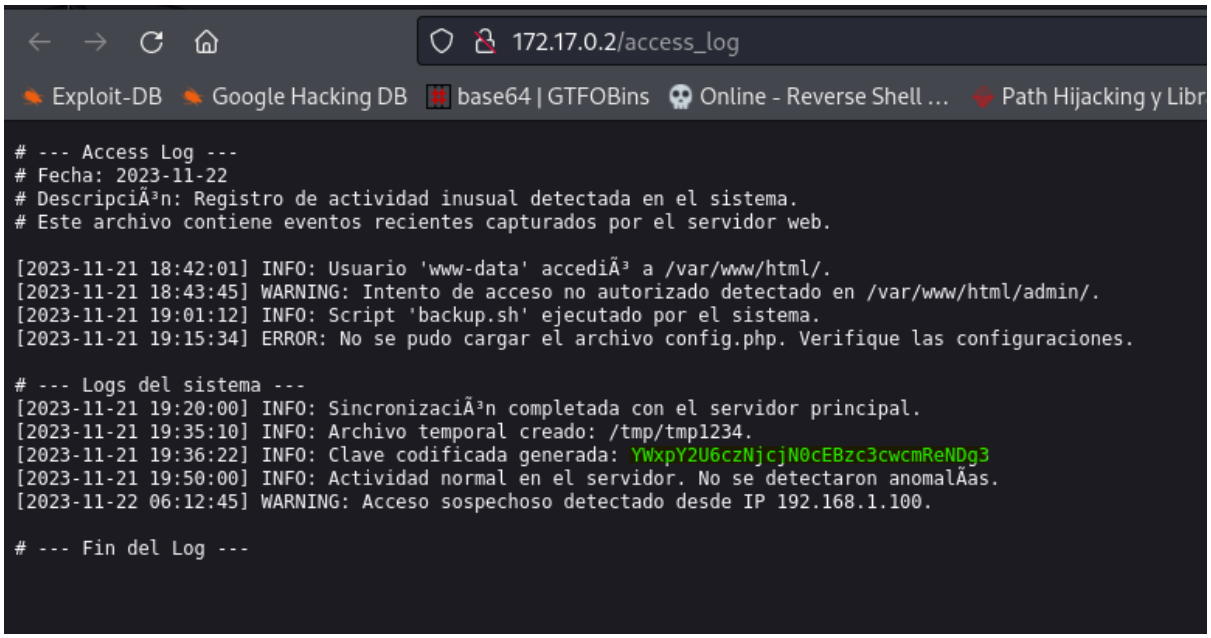
Realizamos escaneo nmap, detectamos el puerto 22 y 80 abiertos.



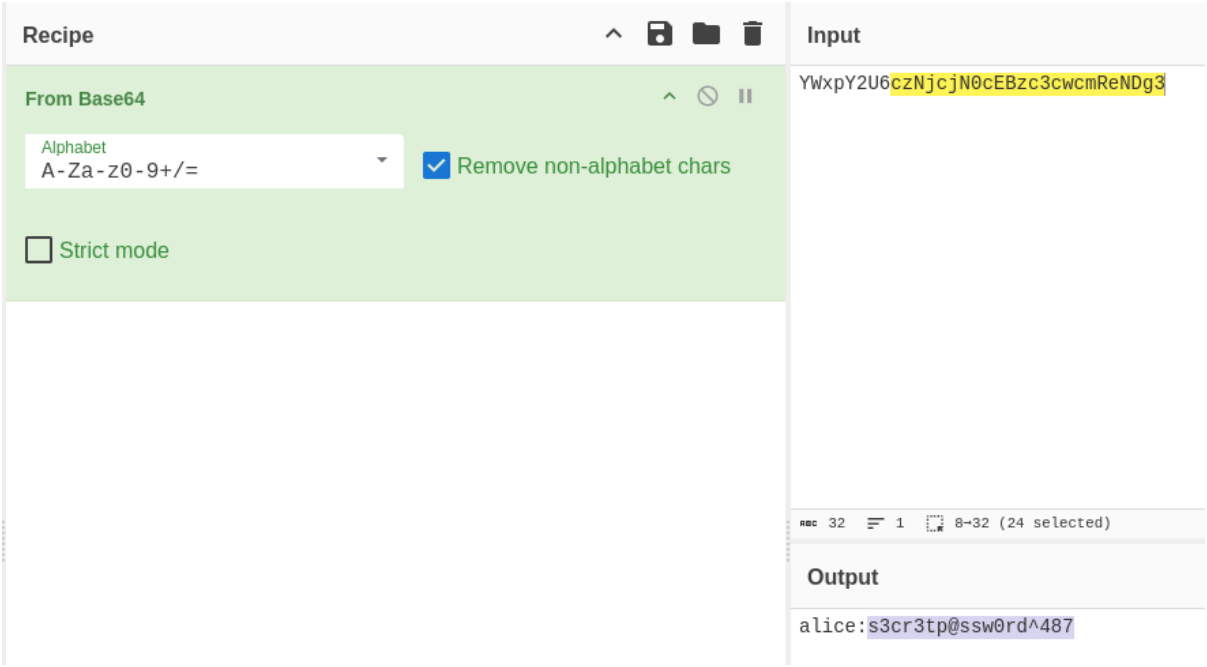
Realizando un escaneo con dirb con el diccionario por defecto nos devuelve las siguientes urls. Siendo la de access_log interesante.



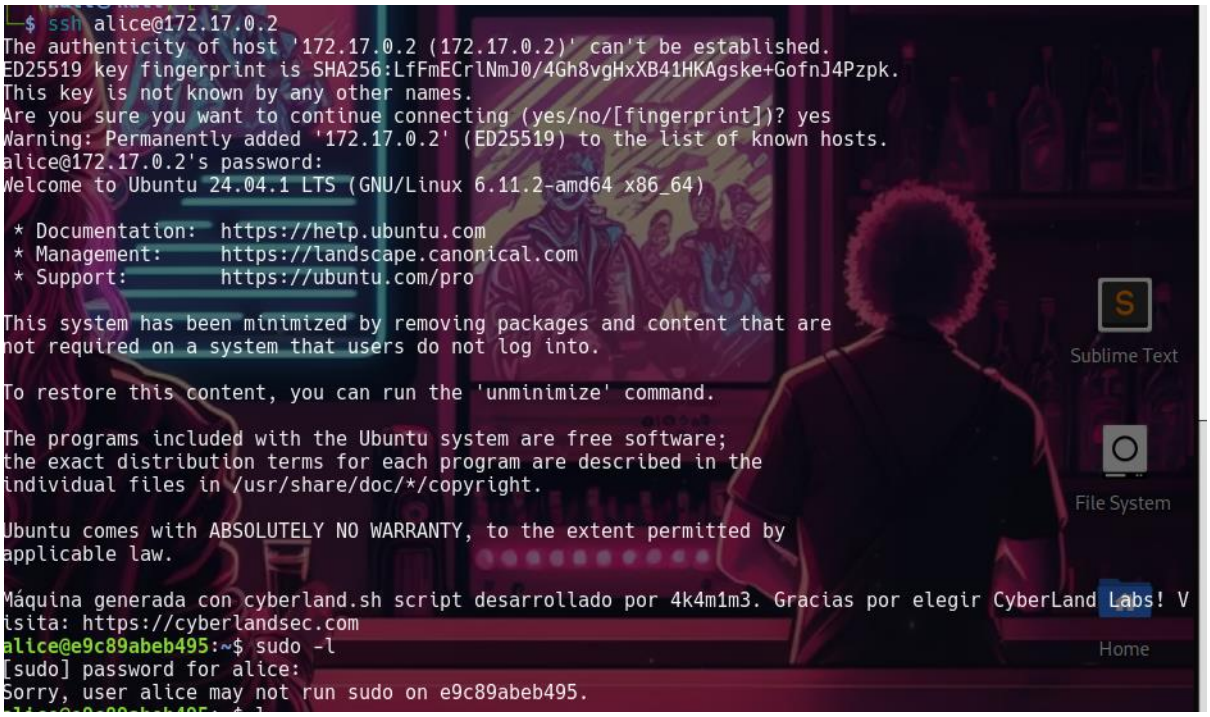
En el contenido de access log encontramos lo que indica ser la clave codificada, vamos a comprobar lo que es realmente.



Por lo visto está codificado en base64 y es login de la usuaria alice.

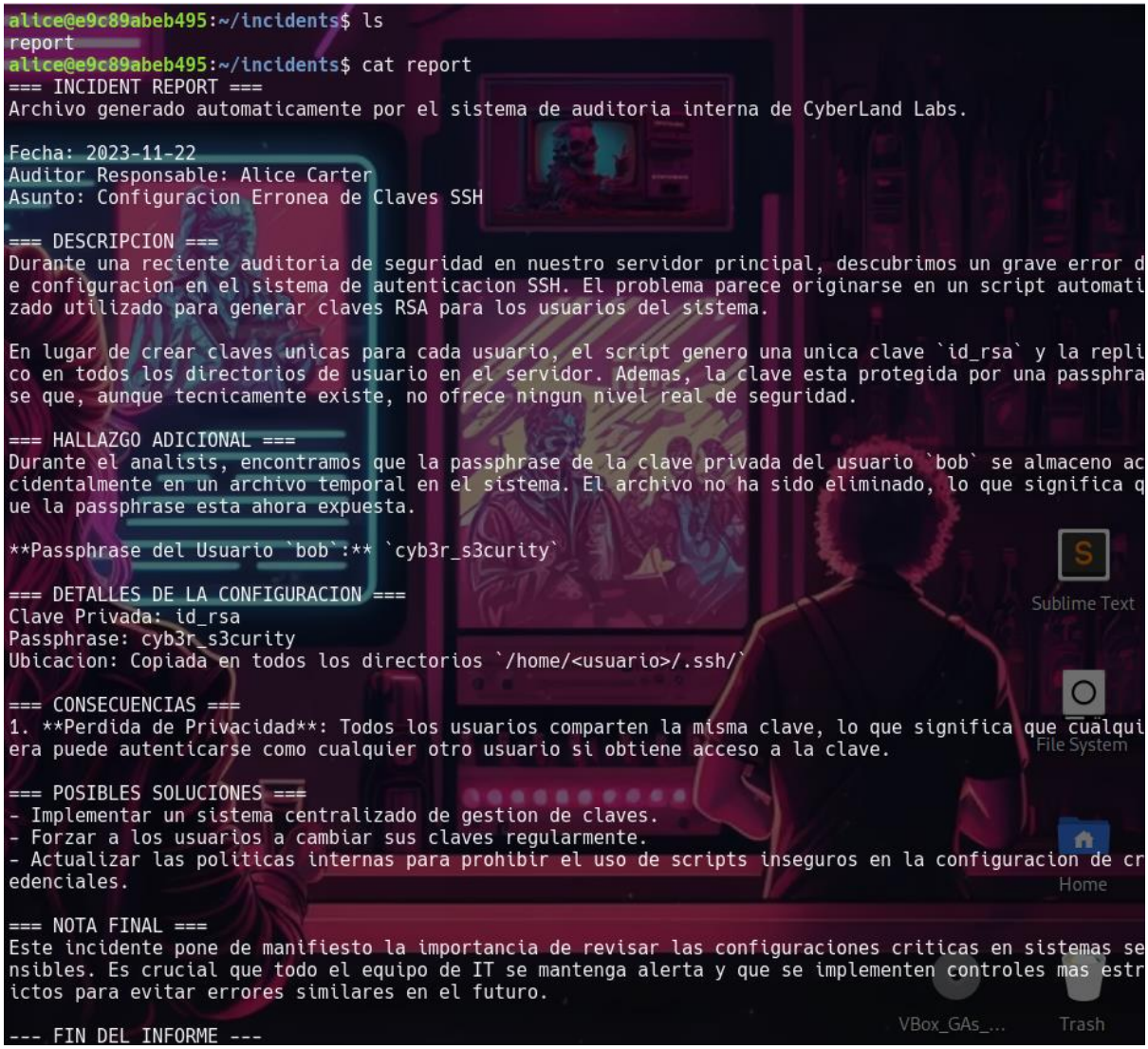


Accedemos mediante ssh con la usuaria alice la cual no está dentro del grupo sudoers.

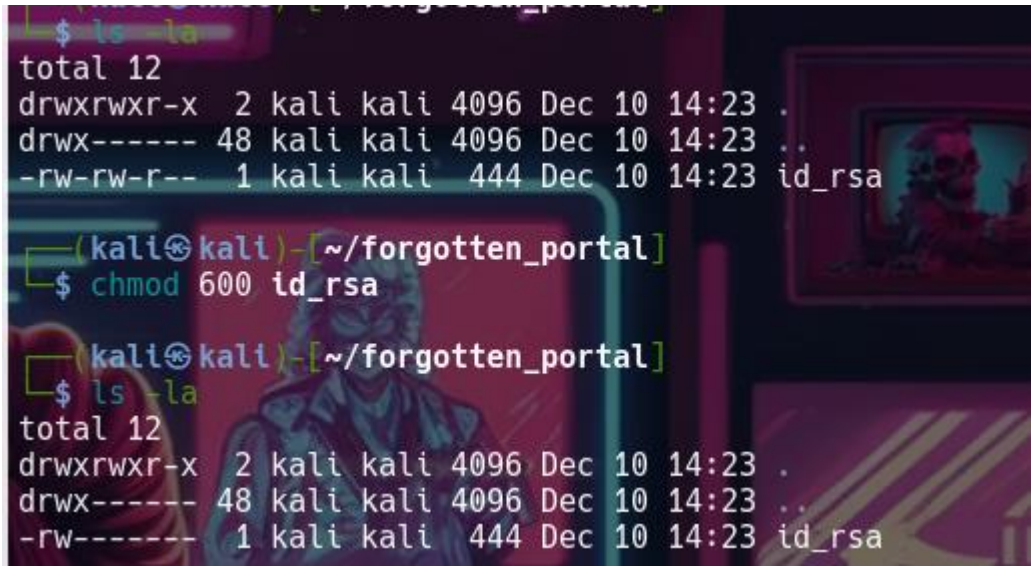


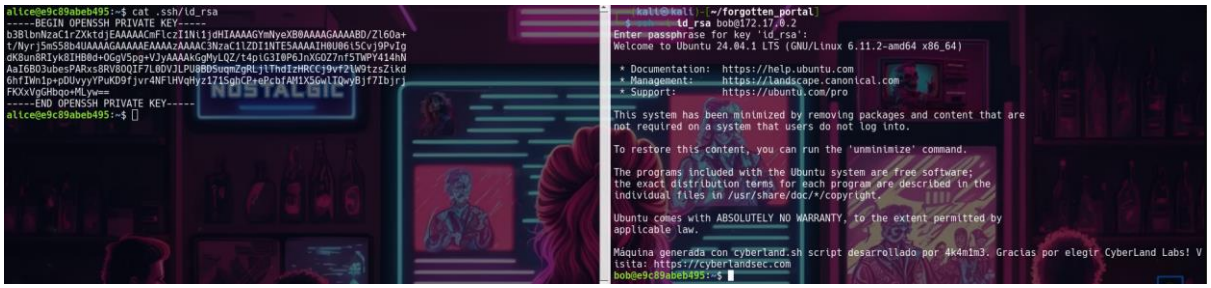
En su directorio encontramos la flag.

Dentro del mismo directorio de alice, en la carpeta incidents, encontramos un reporte en el cual tenemos alguna que otra pista.

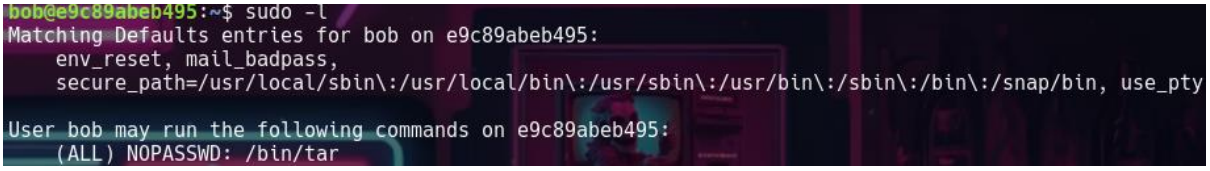


Si leemos detenidamente lo que pone en la nota anterior, vemos que todos los usuarios tienen la misma clave privada y que en caso del usuario bob tambíen se filtró la passphrase. Es por ello que vamos a ver la clave privada de la usuaria alice, copiarla y después de cambiarle los permisos vamos a probar a loguearnos con el usuario bob.





Una vez conseguimos el acceso de bob comprobamos si se puede ejecutar algo como sudo. En este caso se puede ejecutar el comando tar



Ahora, como siempre en estos casos, nos dirigimos a la página https://gtfobins.github.io/gtfobins/tar/#sudo donde podemos ver o guiarnos que comandos utilizar para aprovechar este privilegio mal configurado para lograr la escalada a root y obtener la deseada flag.