# BACKD00RS\_02

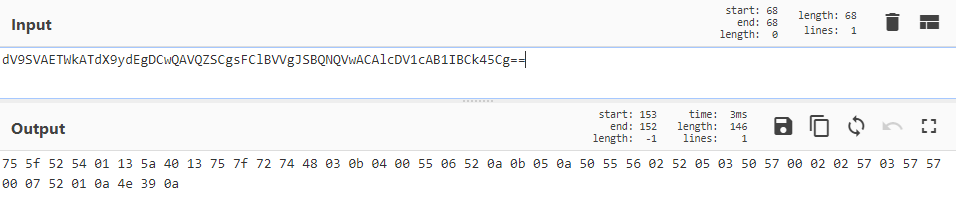
Buscando los archivos recientemente modificados en el sistema, nos damos cuenta de que se ha modificado el binario "ls".

Lo abrimos en un editor hexadecimal y vemos que se trata de un script en Bash que ejecuta otro binario localizado en "/usr/sbin/psl".

Decompilamos el binario con IDA y tratamos de entender la funcionalidad. Se trata de una Reverse shell que se conecta a una IP, lee en un buffer lo que recibe de ese equipo y lo ejecuta.

Abriendo el binario en un editor hexadecimal nos damos cuenta que hay un overlay en el fichero con el texto "Watch this: dV9SVAETWkATdX9ydEgDCwQAVQZSCgsFClBVVgJSBQNQVwACAlcDV1cAB1IBCk45Cg==.".

Cogemos la parte codificada y la metemos en la herramienta Cyberchef para decodear el Base64, eso nos devuelve un array de bytes.



Probamos a decodificar esos bytes con una XOR usando otra vez la herramienta Cyberchef y en la key 0x33 nos encontramos con la flag de este reto.

