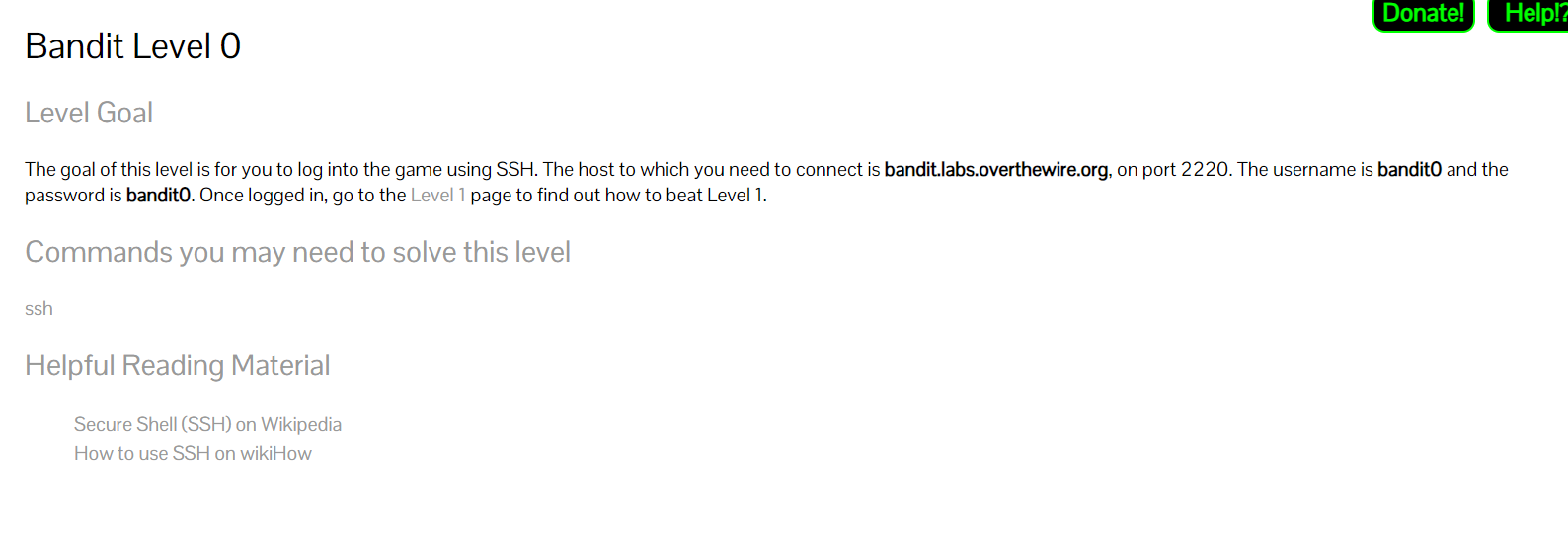
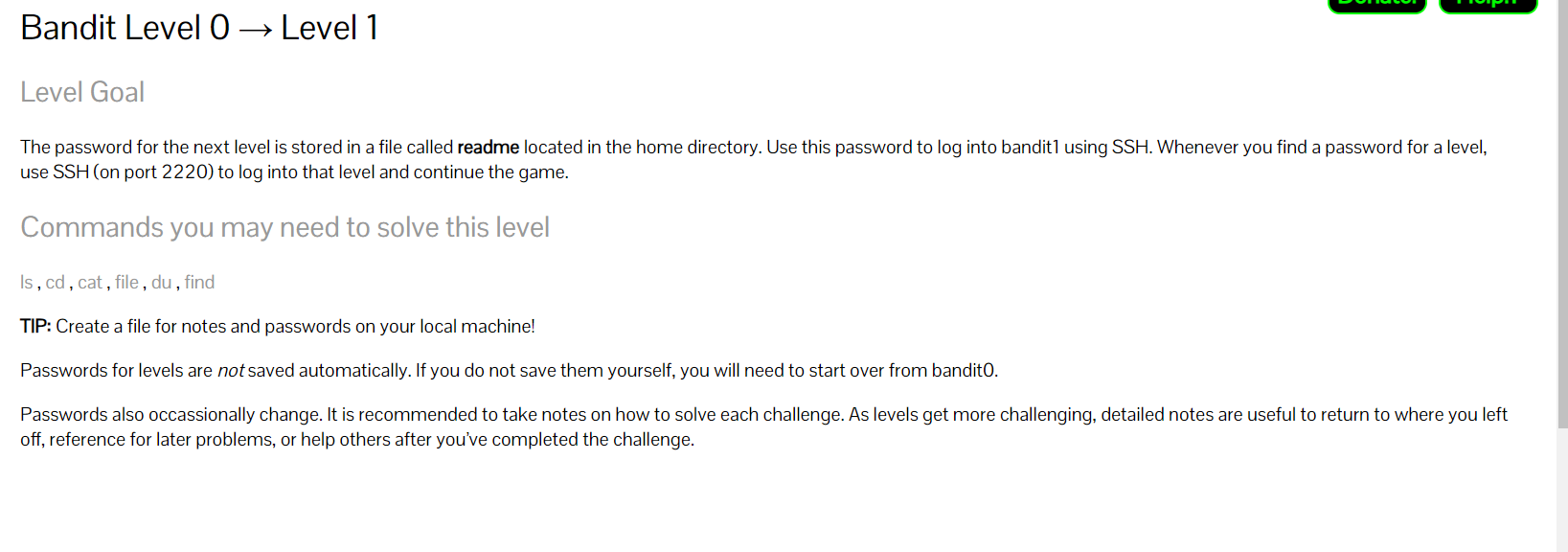
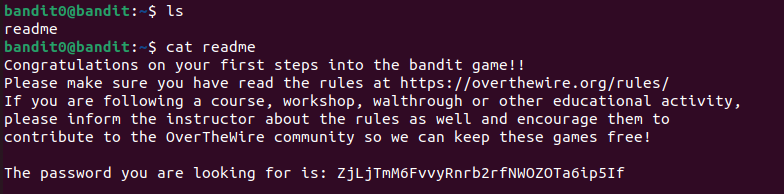
Nivel 0

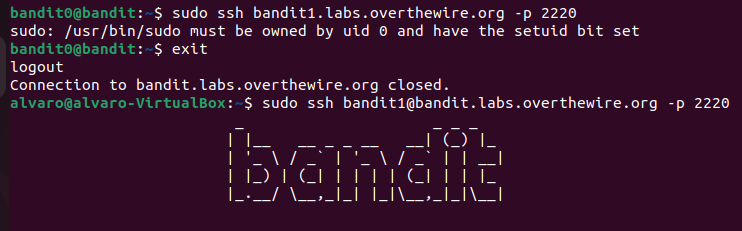




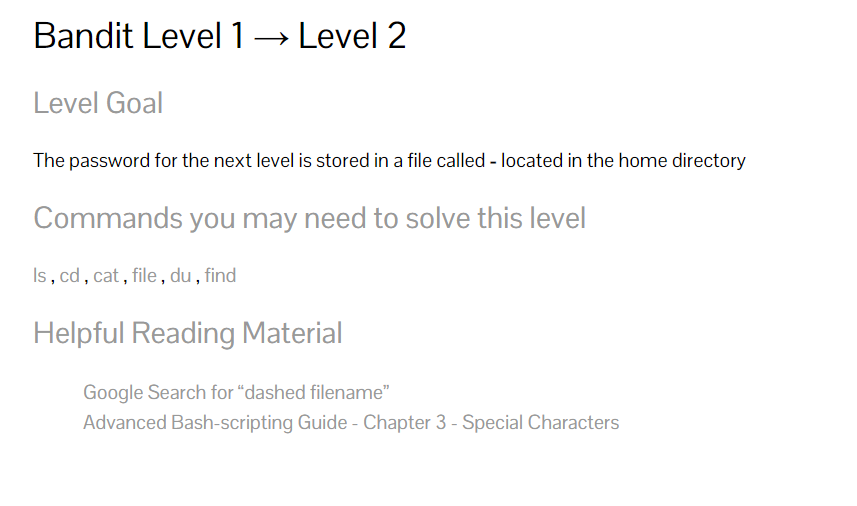
Nivel 0🡪1





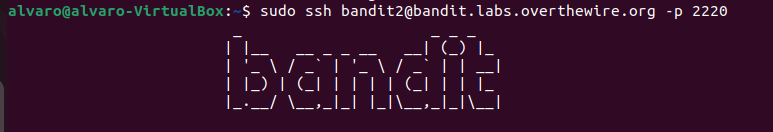


Nivel 1🡪2

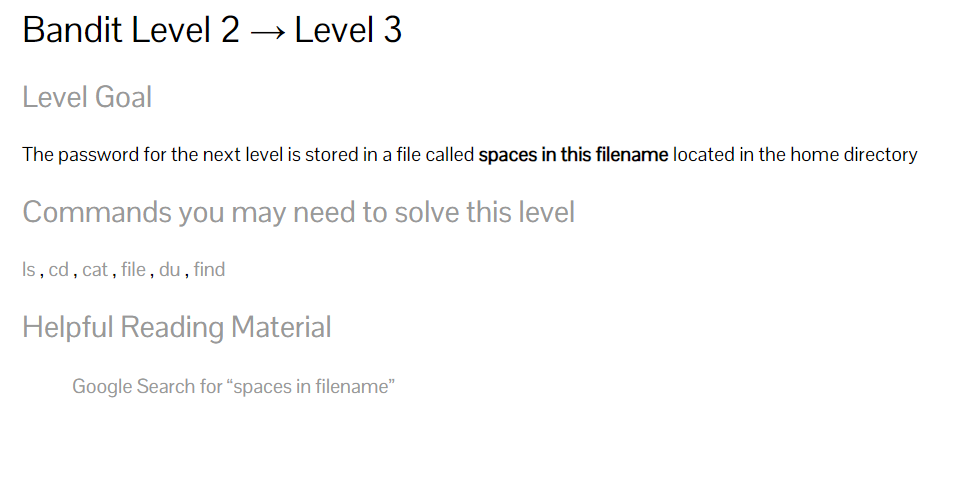


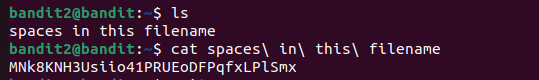


Aquí nos pide que busquemos la contraseña del siguiente nivel en un archivo llamado – y como en linux esto lo interpreta que es el inicio de una opcion de comando lo escapamos con ./



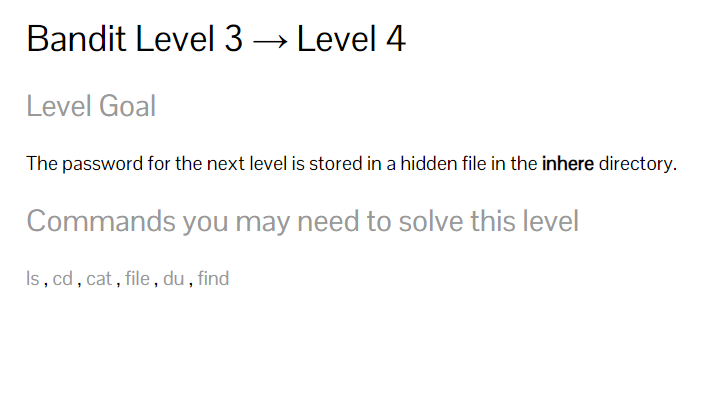
Nivel 2-🡪3

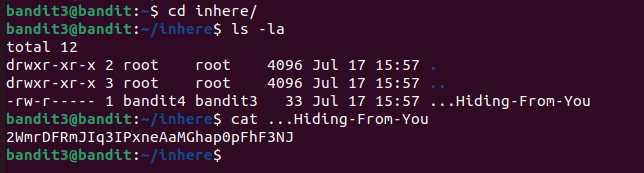




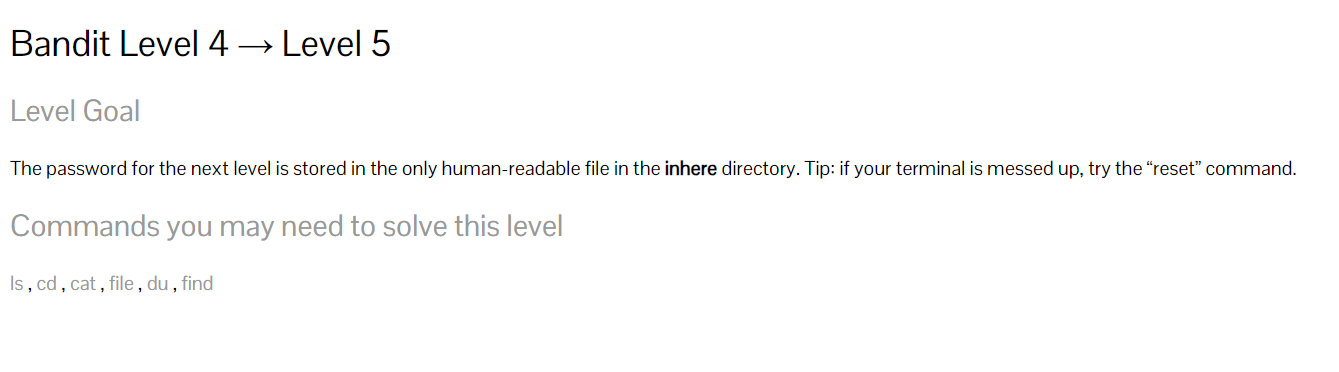
Tambien lo podriamos hacer cat “spaces in this filename”

Nivel 3🡪4





Nivel 4🡪5

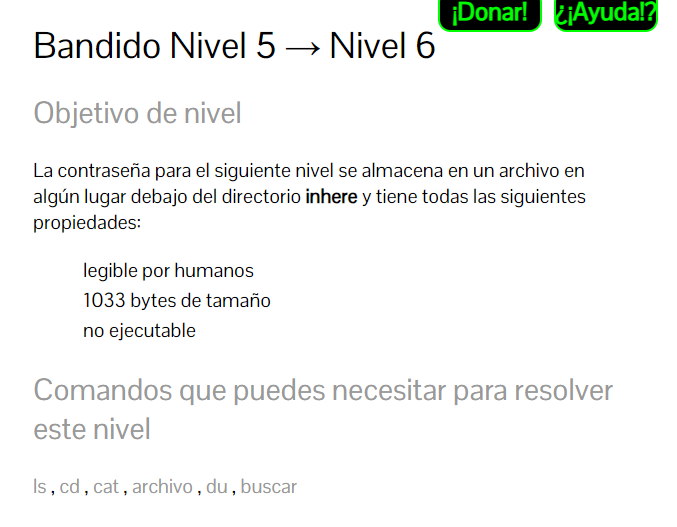








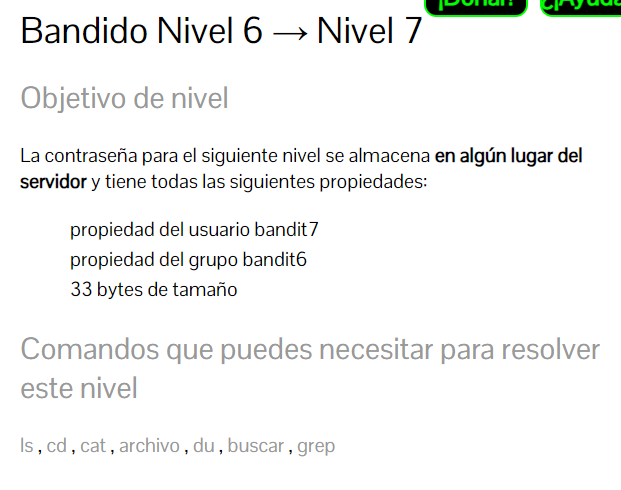
Nivel 5🡪6:







Nivel 6🡪7







/ busca en todo el sistema.

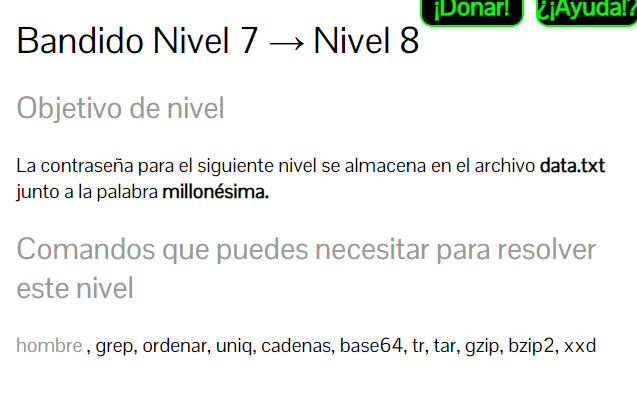
-user bandit7 busca archivos propiedad del usuario bandit7.

-group bandit6 busca archivos propiedad del grupo bandit6.

-size 33c busca archivos con un tamaño exacto de 33 bytes.

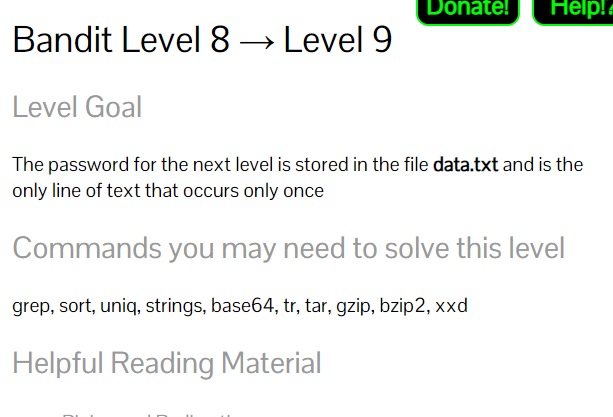
2>/dev/null oculta los mensajes de error por falta de permisos.

Nivel 7🡪8



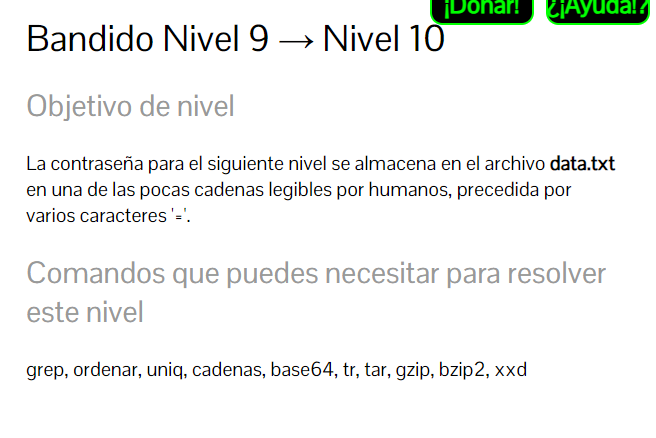


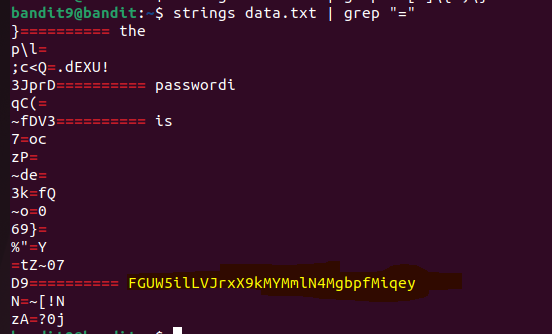
Nivel 8🡪9





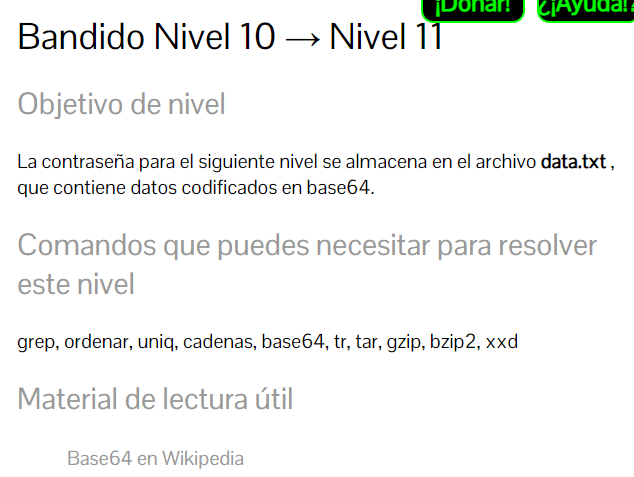
Nivel 9🡪10





FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Nivel 10🡪11

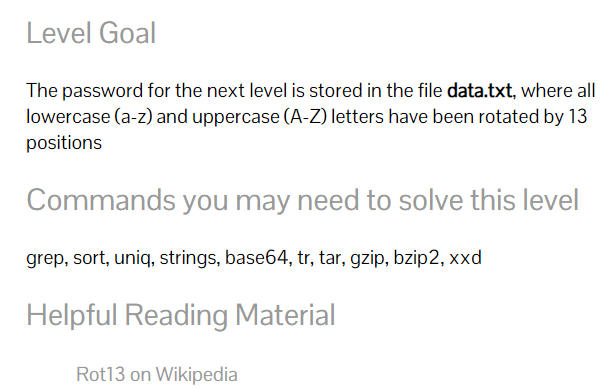






Aquí lo que he hecho es usar base64 –decode para descodificar el texto y poder tenerlo en texto normal

Nivel 11🡪12



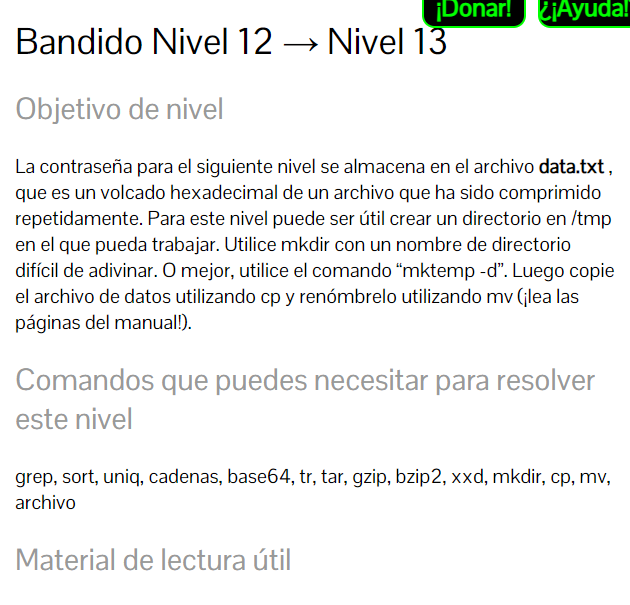


A-Za-z: corresponde al alfabeto normal (mayúsculas y minúsculas).

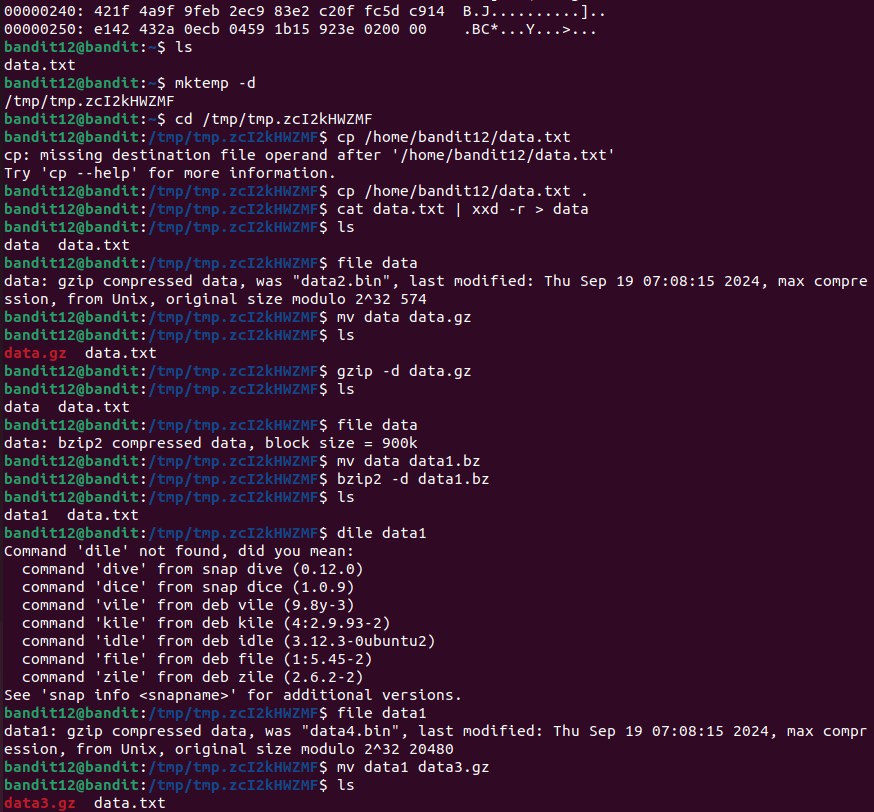
N-ZA-Mn-za-m: corresponde al alfabeto rotado 13 posiciones.

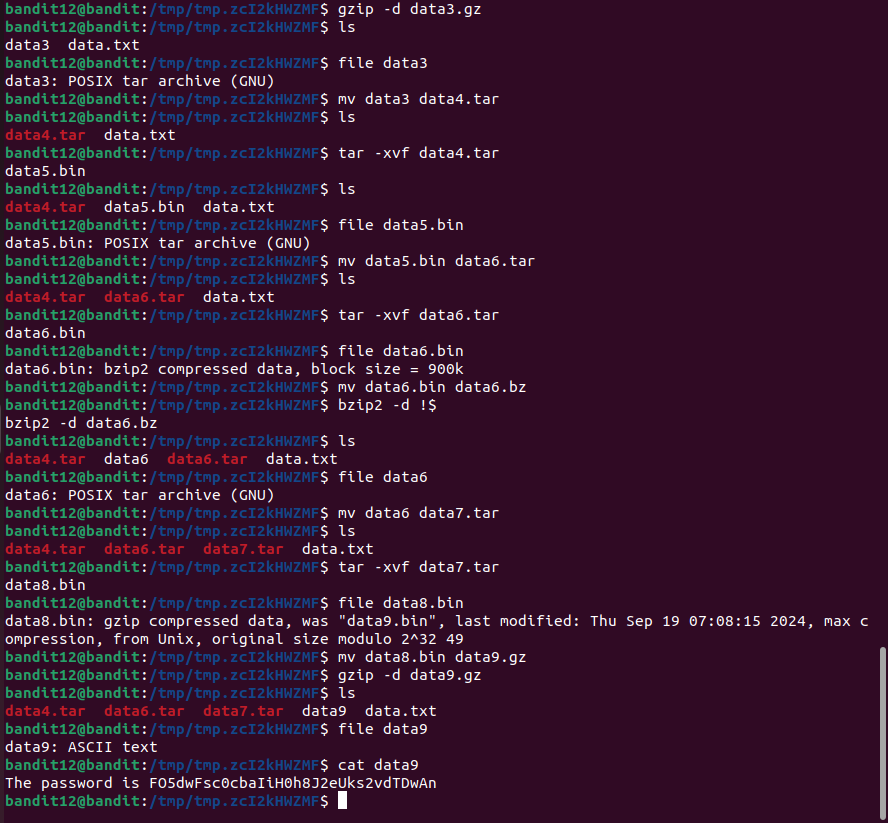
Y el tr es para desrotar y usamos el echo para que imprima lo que le metamos

Nivel 12🡪13



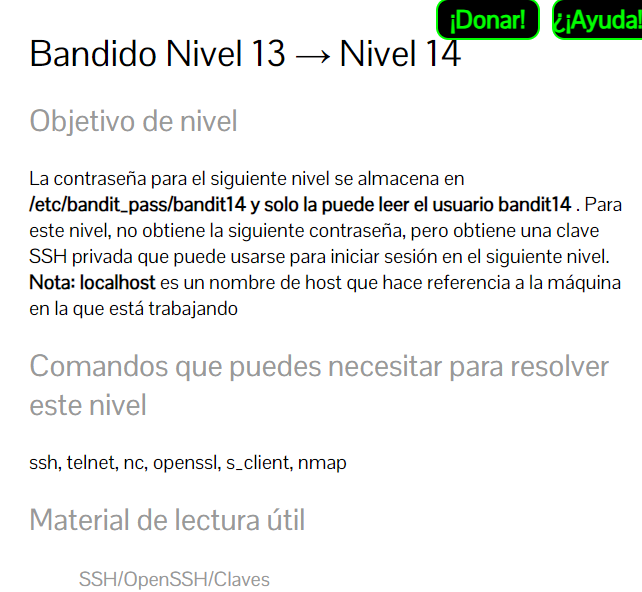
He seguido todos estos pasos uno a uno la vd que ha sido super fumada ☹





FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

Nivel 13 – 14



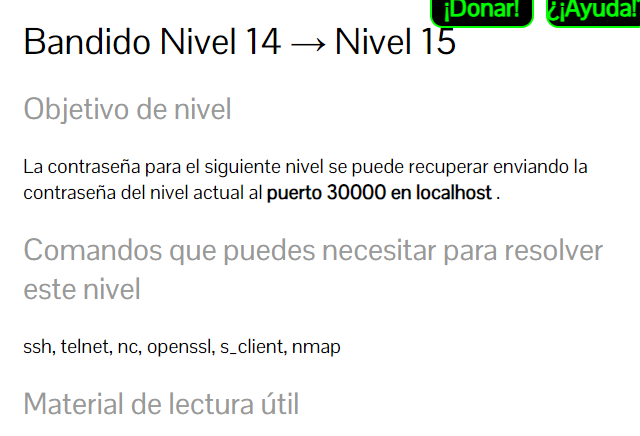


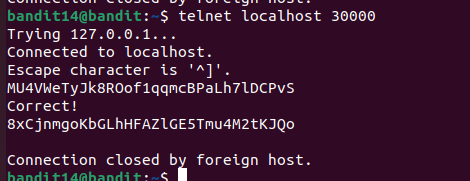


MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS

Aquí lo que hemos hecho es iniciar sesion en el nivel 14 con la clave ssh que teniamos en el 13 y nos ha mostrado la contraseña pero tampoco nos hace falta porque ya hemos iniicado por clave ssh

Nivel 14-15

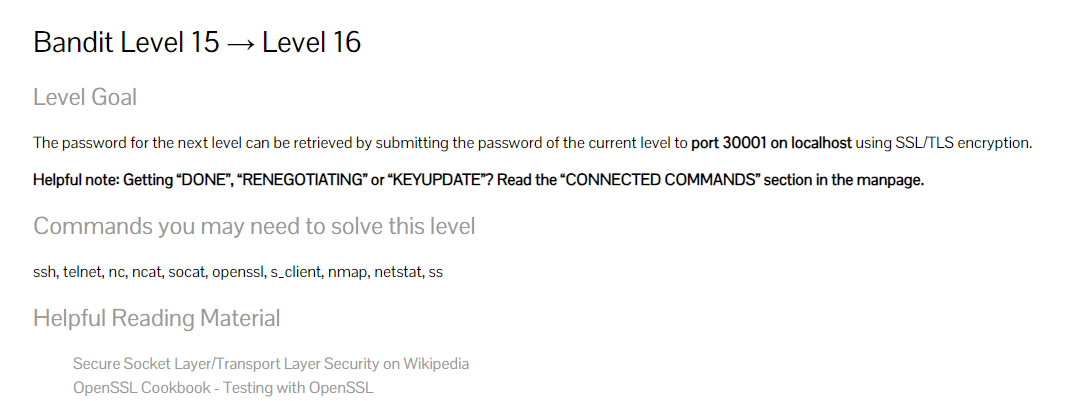




8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Con telnet nos conectamos a nuestra maquina que en vd seria la maquina del bandit porque nosotros estamos conectado a ellos por ssh que seria localhost y salfriamos por el puerto 30000 y ahí al meter la contraseña del nivel anterior nos devuelve la del nivel 15

Nivel 15-16

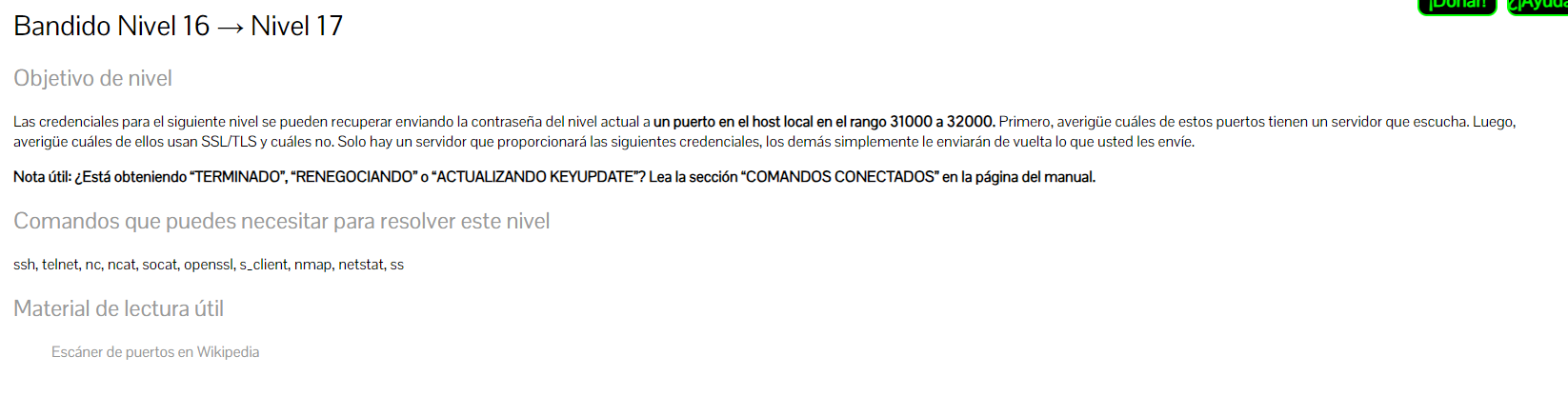


Aquí estamos utlizando en protocolo ssl del cliente y nos vamos a conectar a nuestra misma maquina por el puerto 30001 y cuando enviamos la contraseña del nivel anterior nos devolvera la del n

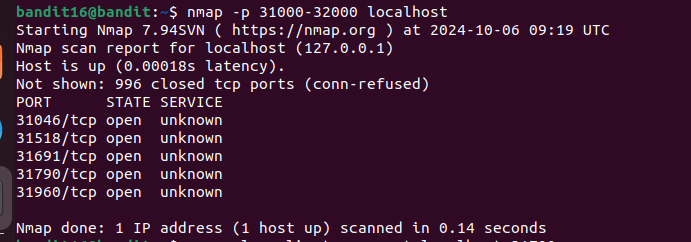


kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

nivel 16-17

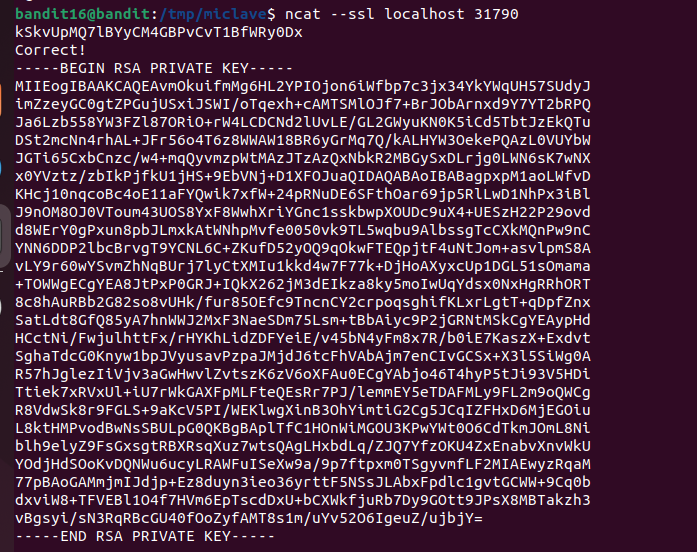


Escaneamos los puertos abiertos entre el 31000 y el 32000



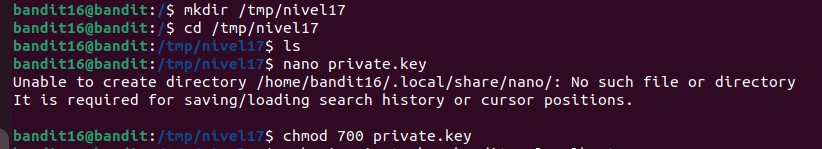
Con ncat nos permite hacer una conexión segura mediante ssl al host local por el puerto 31790

Y cuando ingresemos la contraseña del nivel anterior nos dara una clave privada



Luego nos tendremos que ir a tmp porque si no nos dejara crear ningun archivo

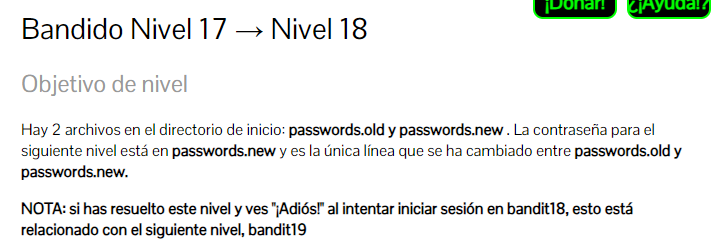
Y aquí creamos el archivo con la clave privada que nos ha dado y le damos permisos de ejecucion al archivo

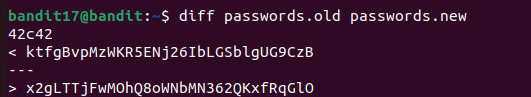


Y ya nos conectamos al nivel 17 con la clave privada



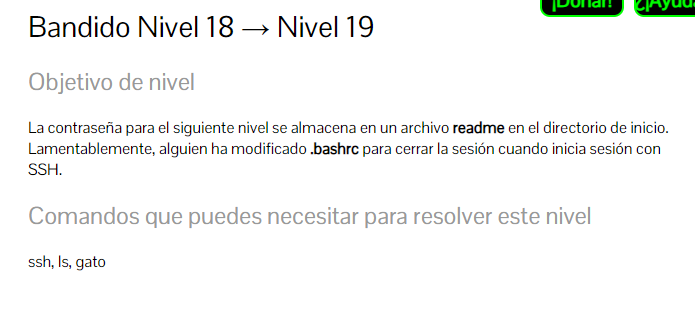
Nivel 17-18





x2gLTTjFwMOhQ8oWNbMN362QkxfRqGlO

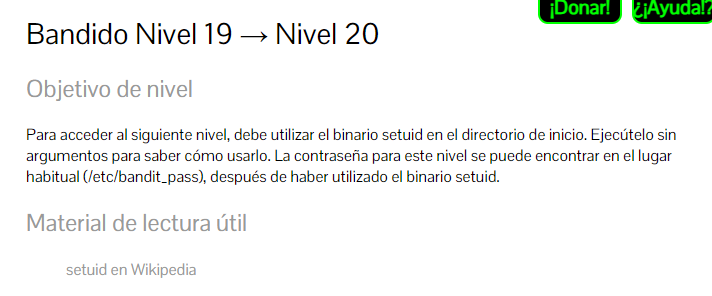
Nivel 18 - 19





Con cat ~/readme entre comillas lo que hacemos es inyectar ese codigo ya que hay algo que no nos deja iniciar normalmente en el nivel y entonces no podemos verlo de manera normal

Nivel 19-20



Aquí no nos deja ver lo que tiene dentro por que el archivo tiene el uid de bandit 20 y noostros somos bandit 19 asi que lo que voy a hacere es ejecutarlo como bandit 20







0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

Nivel 20-21

