

hACKING éTICO

Unidad 1. Actividad 3



4 de octubre de 2023

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

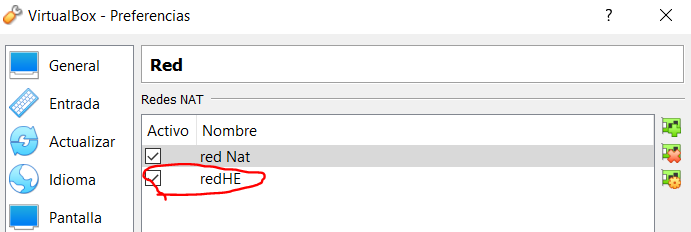
[Paso 1. 2](#_Toc147417585)

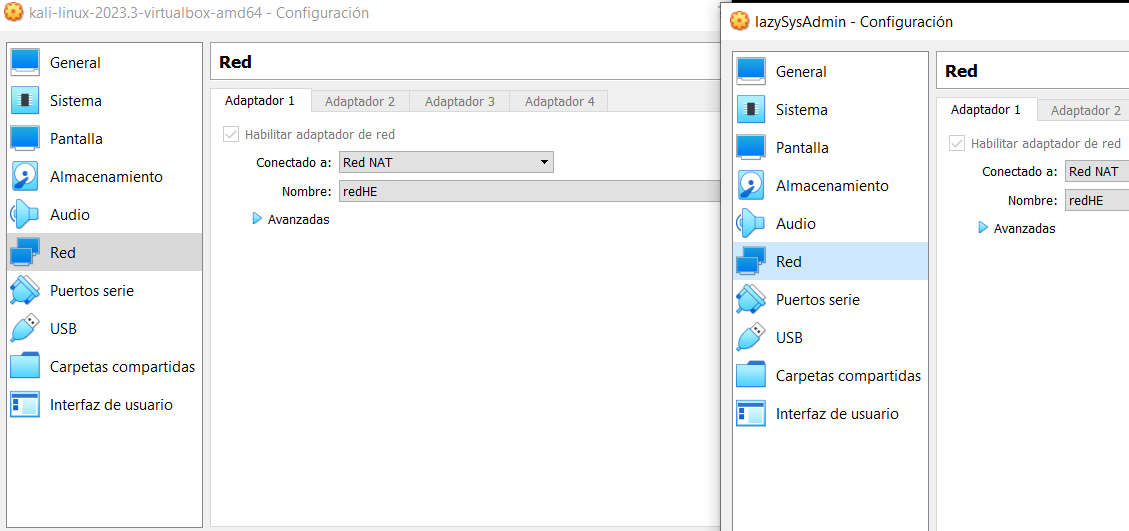
[Paso 2 3](#_Toc147417586)

[Extra 9](#_Toc147417587)

# Paso 1.

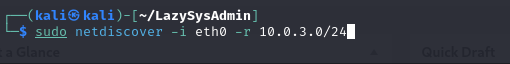
Lo primero que tenemos que hacer es crearnos una Red Nat donde vamos a poner nuestra ip con nuestro número de clase (en mi caso 10.0.3.0). Después se la hemos añadido a la maquina virtual Kali y también a la Ubuntu que nos ha pasado Pablo:

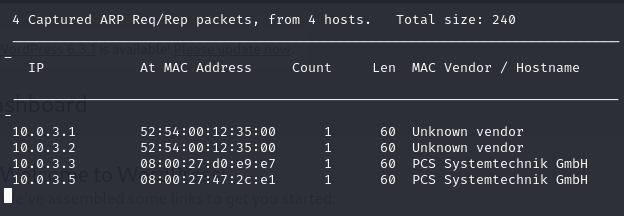




# Paso 2

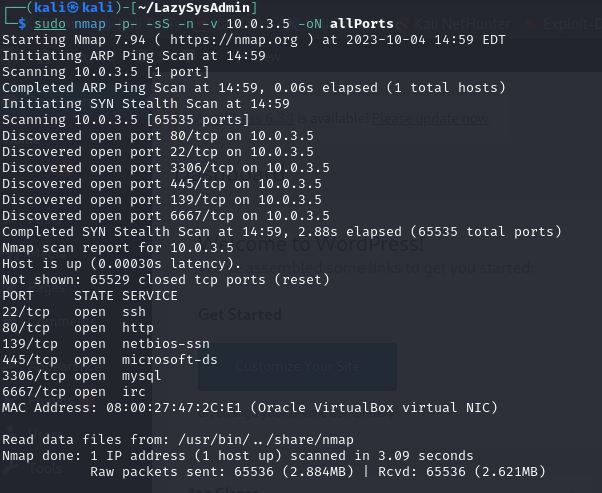
Ahora comprobamos la ip que tenemos y hacemos un scaner en la red:



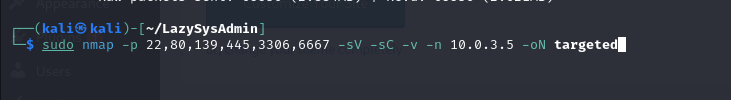


Como vemos nos ha detectado 4 ip, la que a nosotros nos interesa es la 10.0.3.5 ya que es la maquina Ubuntu que queremos explotar.

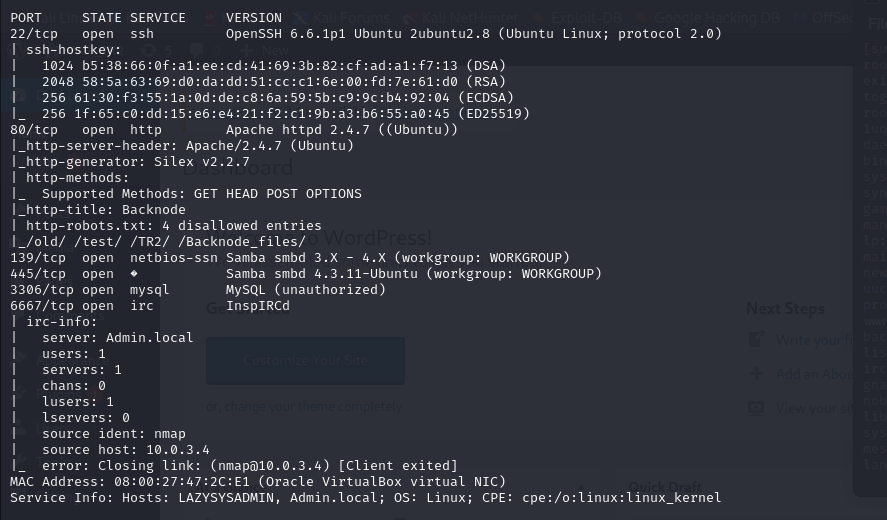
Ahora vamos a detectar todos los puertos que tenga abiertos esa ip:



Como vemos esta máquina tiene los puertos 80,22,3306,445,139 y 6667. Pues bien ahora vamos a escanear estos puertos que tiene abiertos:

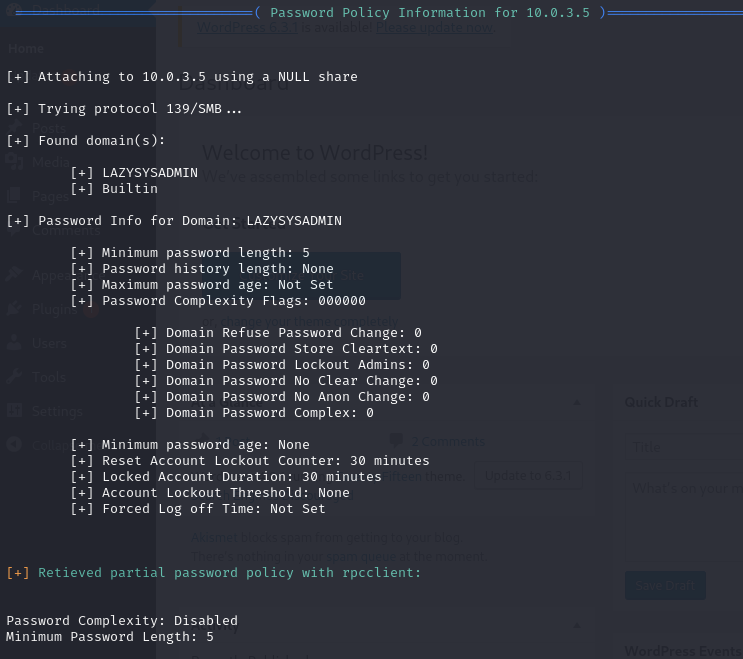


Aquí esta el resultado:

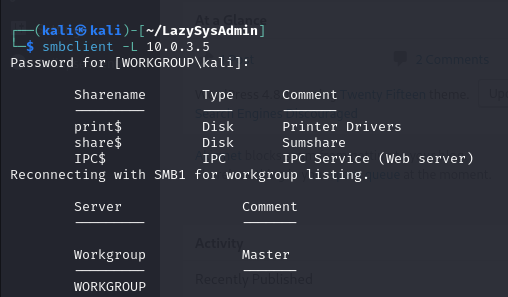


Ahora vamos a usar el comando emu3Linux para sacar información de usuarios, contraseñas etc…:

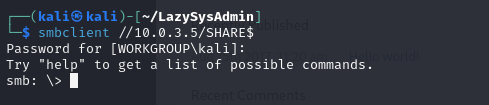


Aquí en el resultado de las contraseñas, podemos ver por ejemplo que la contraseña debe de tener un mínimo de 5 caracteres:  


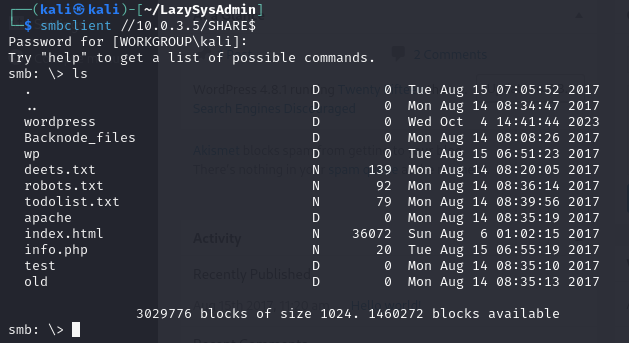
Ahora usamos el smbclient para que nos muestre las cosas que tiene publicas:



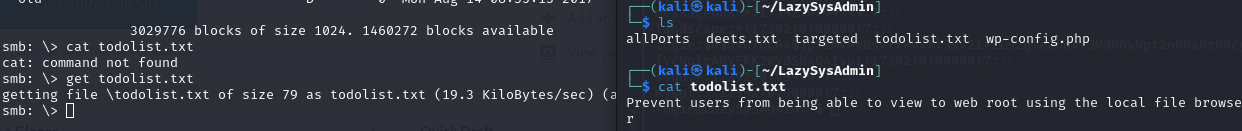
Aquí por ejemplo podemos ver que tiene impresora, una carpeta llamada share y un IPC que lo tienen todos los ordenadores. Nosotros nos vamos a centrar en la carpeta share:

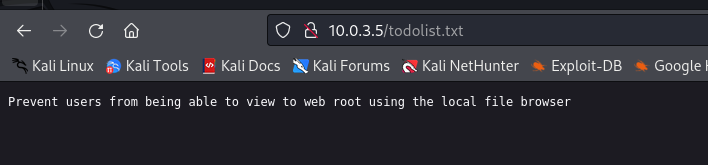


Ahora que esetamos dentro de la carpeta podemos investigar que es lo que tiene en esta:

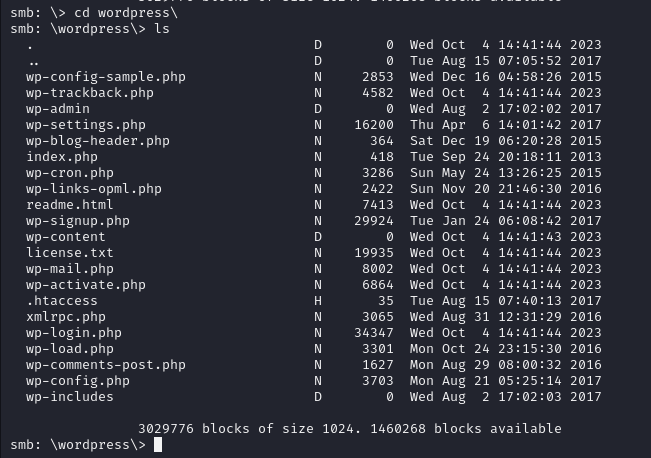


Nos vamos a centrar en los documentos txt y en la carpeta wordpress. Empezamos viendo el contenido de los documentos, para esto podemos hacerlo mediante descargarlo usando el comando “get” o mediante url:



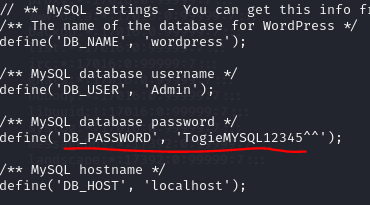


Ahora vamos a mirar wordpress, primero vamos a mirar el contenido que tiene la carpeta wordpress:

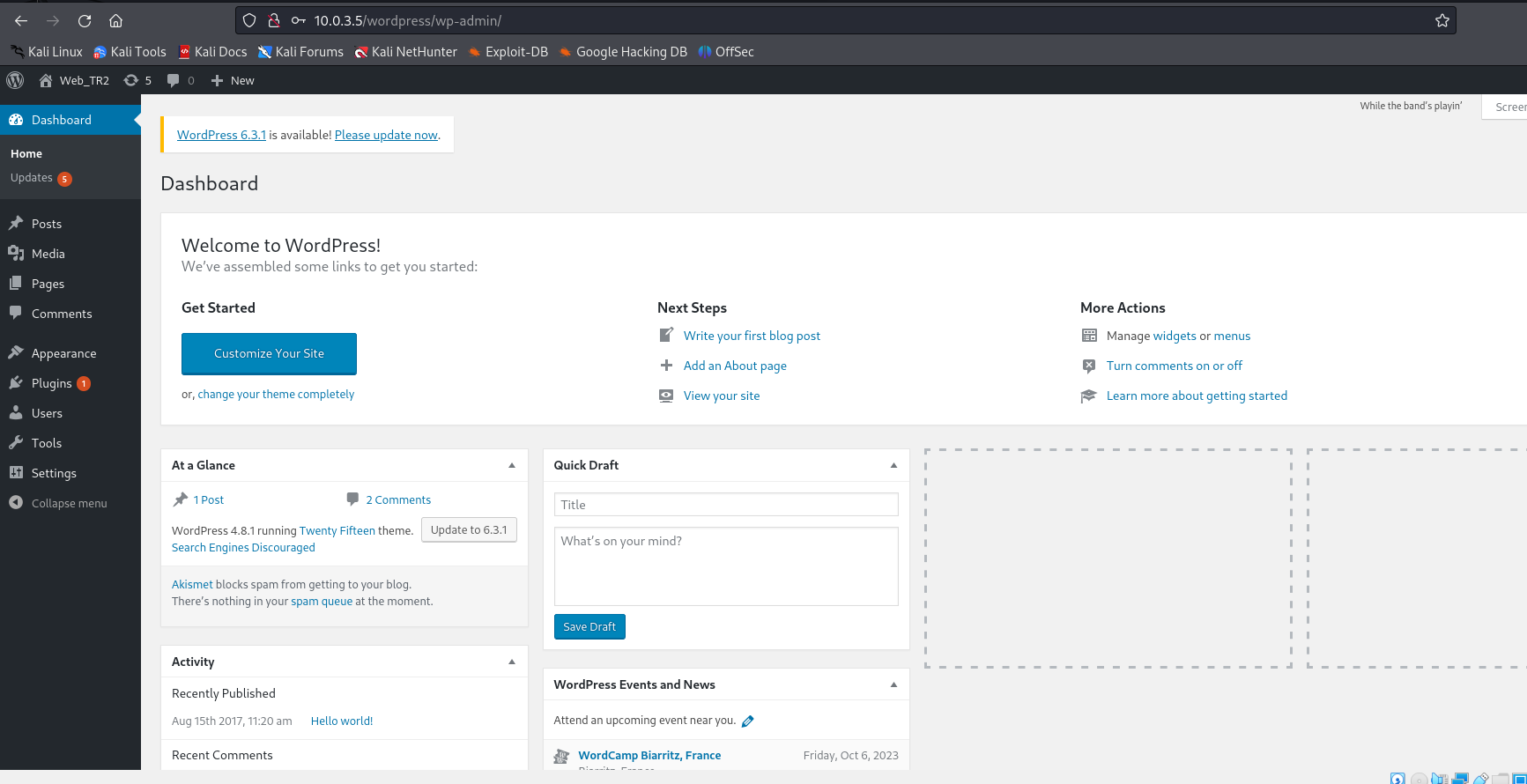


Vamos a fijarnos en el documento wp-config.php, ya que en ese archivo salen los usuarios y la contraseña de la base de datos y puede ser la misma que para entrar a la página de wordpress. Usamos el comando get para descargar el archivo:



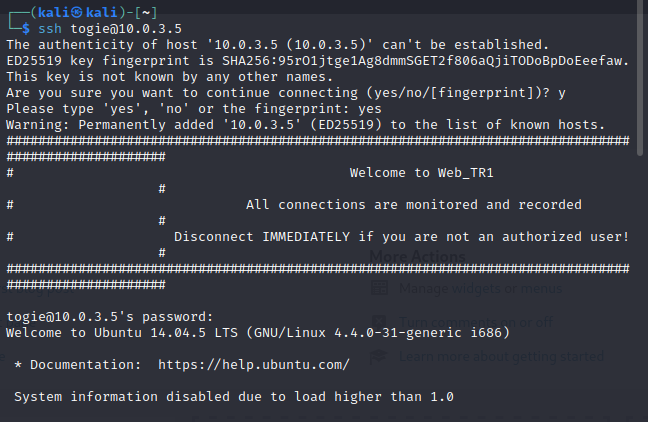


Ahora vamos a probar iniciar en su página de wordpress poniendo ese usuario y contraseña

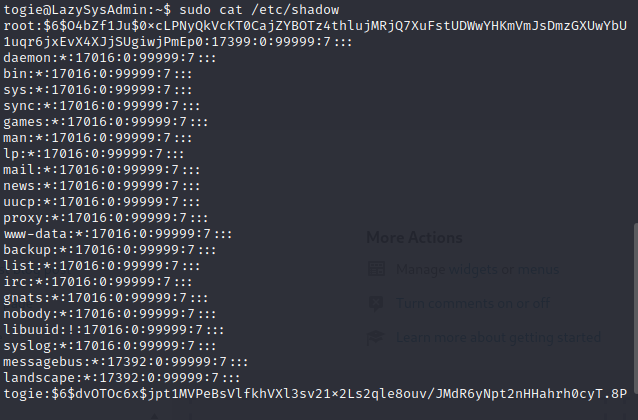


# Extra

Como extra podemos cambiar la contraseña del administrador, para esto nos conectamos mediante ssh a la maquina Ubuntu con los conocimientos previos que hemos obtenido:



Después podemos ver los usuarios y contraseñas en /etc/shadow:



Ahora simplemente usas el comando nano para cambiar la contraseña.