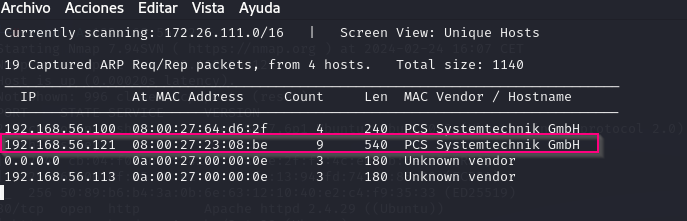
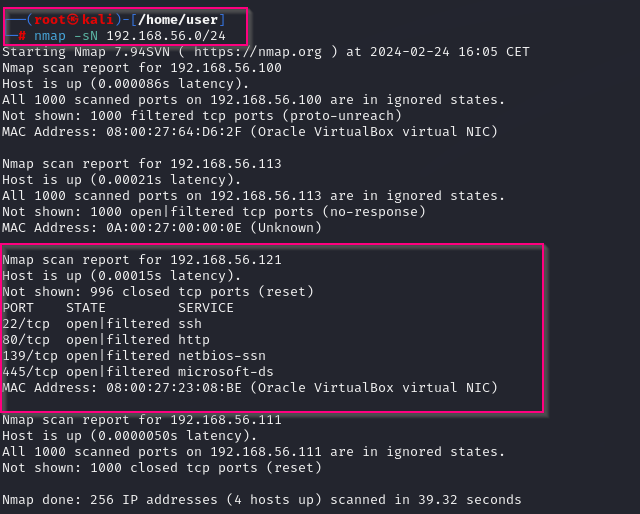
# **KB-Vuln: 3 Vulnhub Walkthrough**

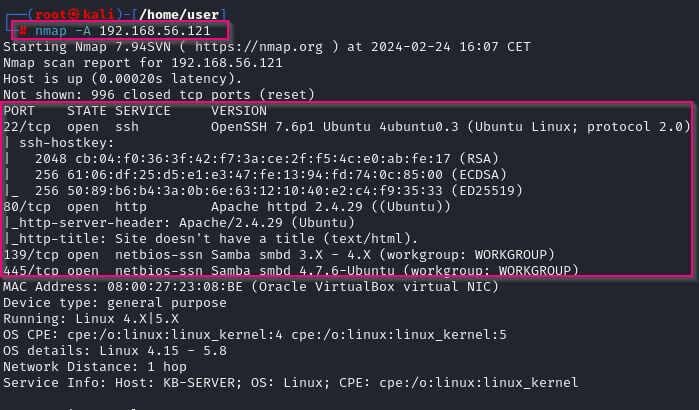
Para buscar la maquina vulnerables usaremos tanto netdiscover como nmap:



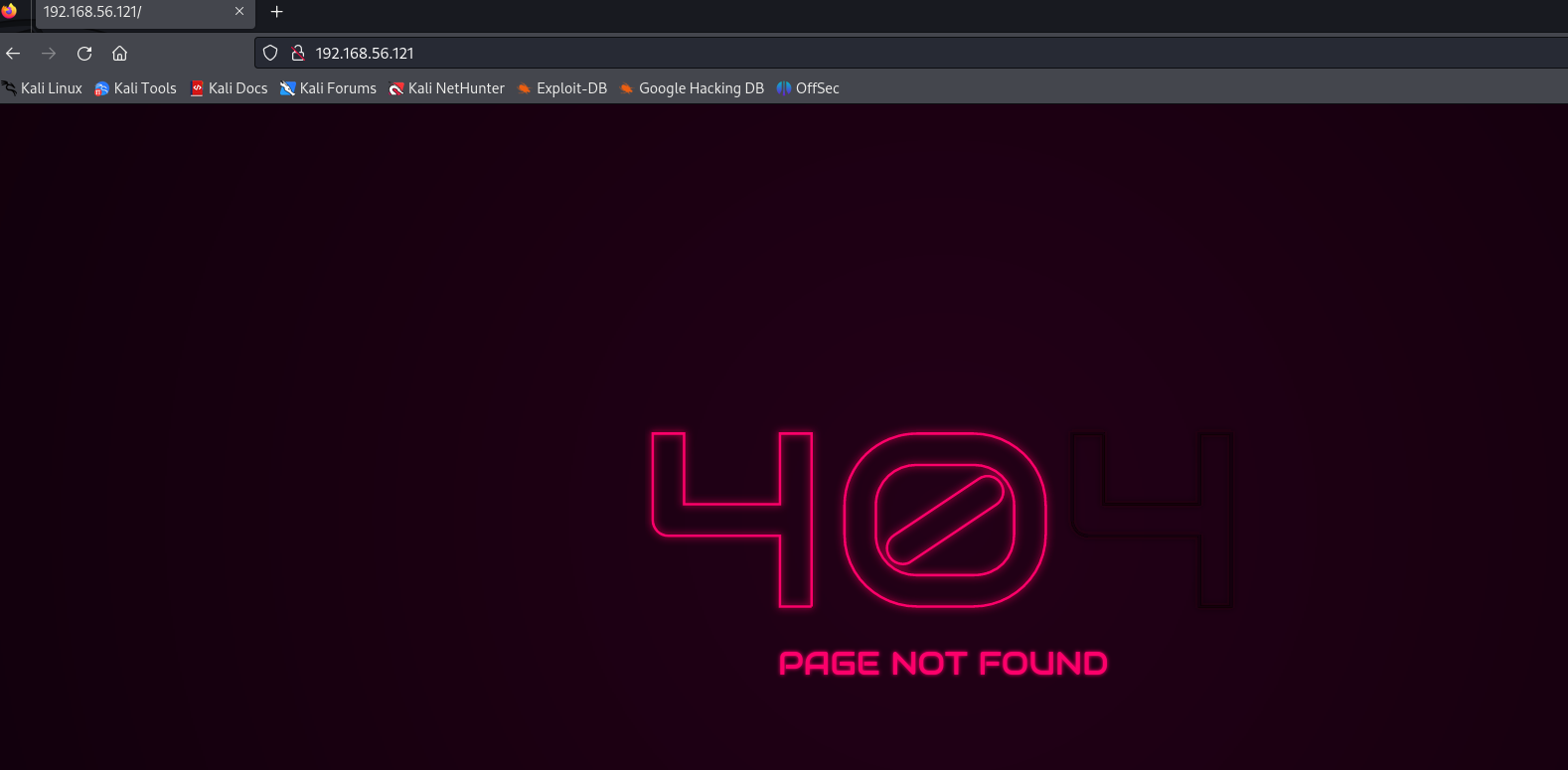
NMAP –sN 192.168.56.0/24



Cómo podemos ver la Ip que nos interesa en la 192.168.56.121 y vemos que tiene varios puertos abiertos. Haremos un escaneo más profundo con NMAP –A 192.168.56.121:



Nos meteremos en el puerto 80 pero podemos ver que da un error de 404:

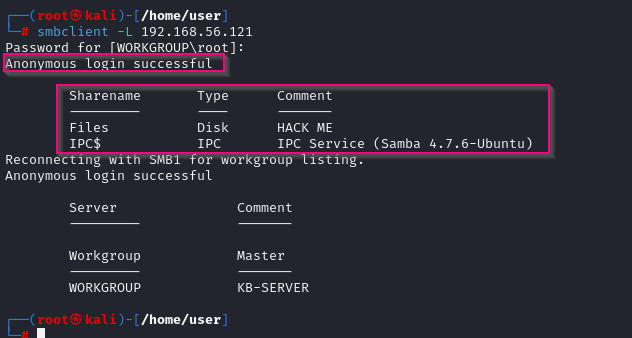


Intruduciremos el comando de NMAP –A –p- 192.168.56.121

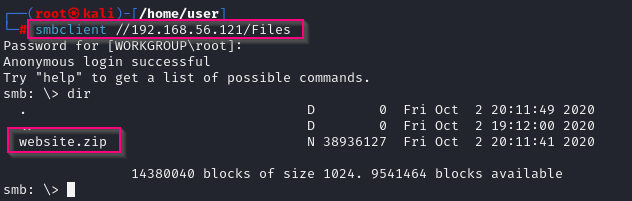
Así pues, ponemos la dirección IP en nuestro archivo "/etc/hosts" y empezamos ejecutando el mapa de todos los puertos con detección de sistema operativo, versiones de software, scripts y traceroute.



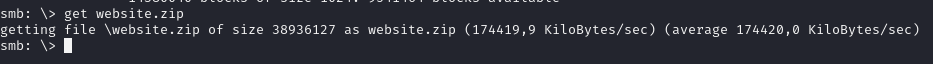
Comprobamos si el sitio es vulnerable a conexiones SMB nulas y listamos dos recursos compartidos. Uno de ellos nos llama la atención por tu comentario. Entramos sin contraseña.



Entramos en el recurso compartido "Archivos" y aparece una copia de seguridad de la web, la descargamos y la descomprimimos, pero está protegida por contraseña.

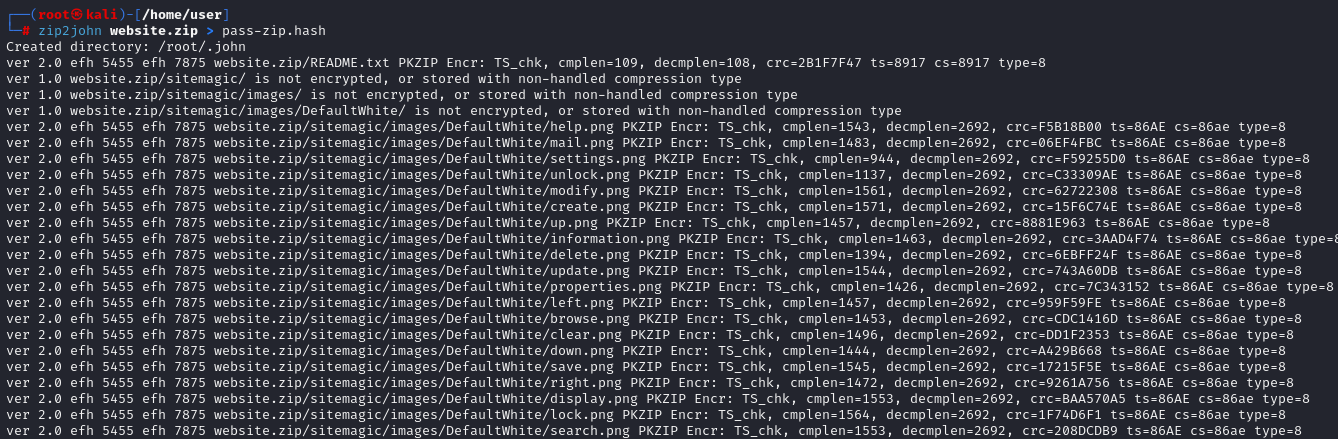


Obtenemos el archivo comprimido.



Exploiting

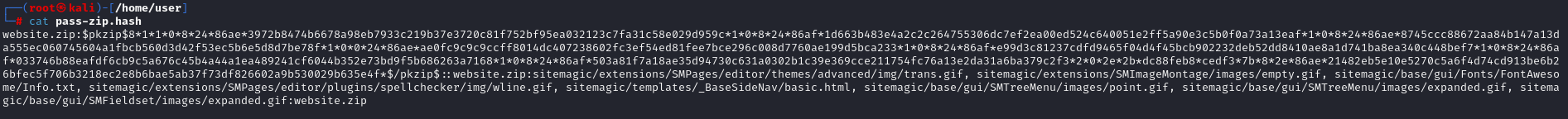
Usaremos zip2john para obtener el hash de la contraseña zip.



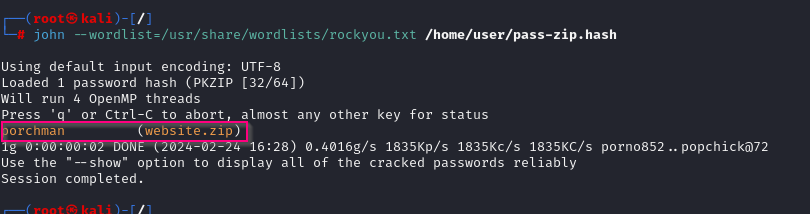
Comprobamos el contenido del fichero "pass-zip.hash" y lanzamos john con el diccionario rockyou.



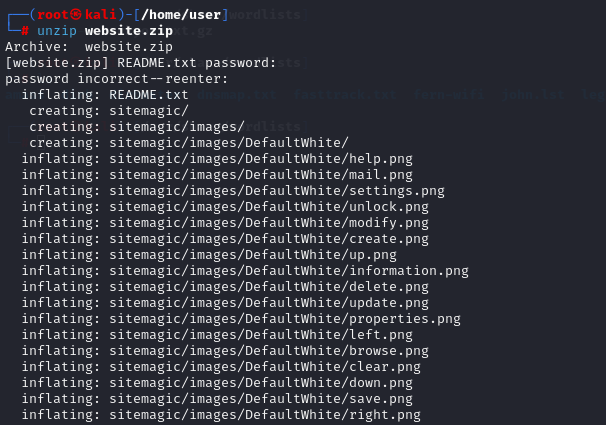
Contenido:



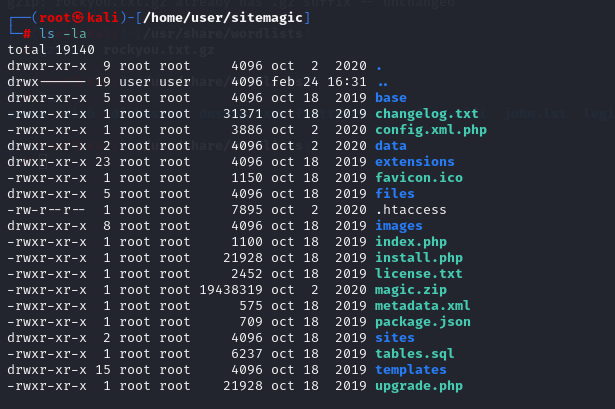
Esperamos un poco y obtenemos la contraseña del zip. porchman



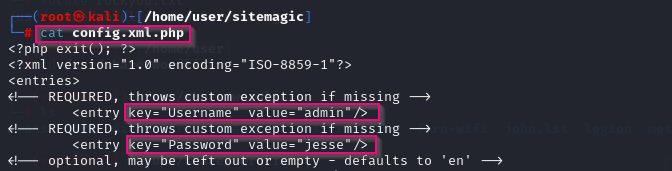
Descomprimimos el zip:



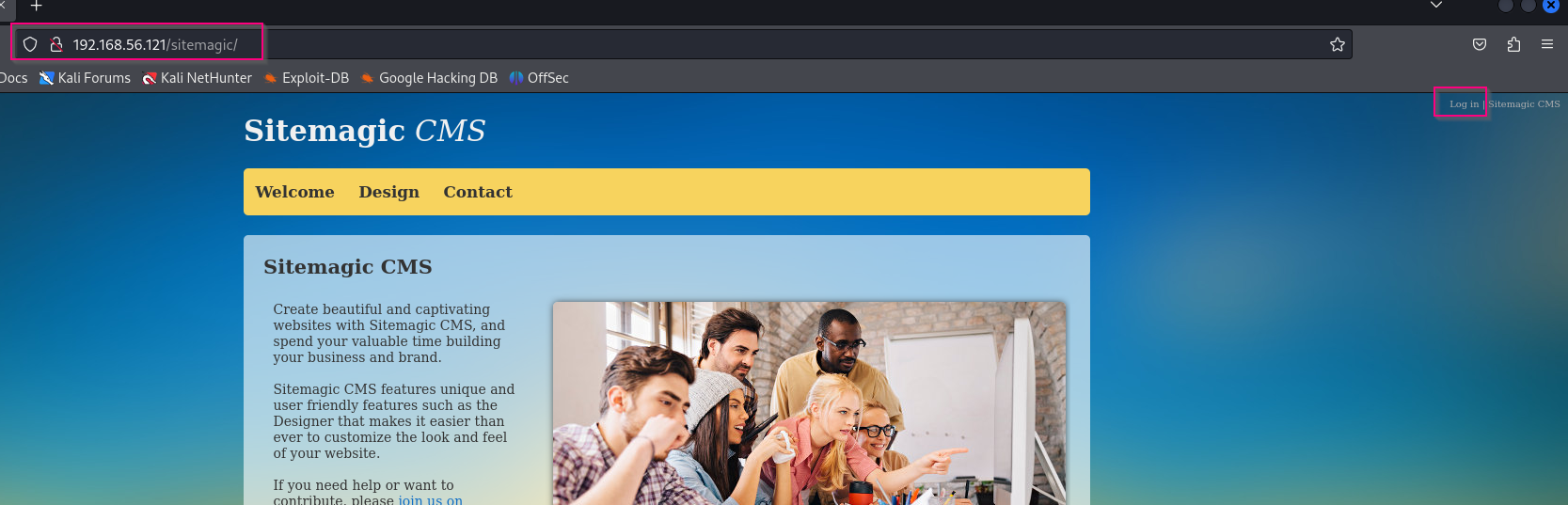
Y vemos que se ha creado un directorio llamado sitemagic:

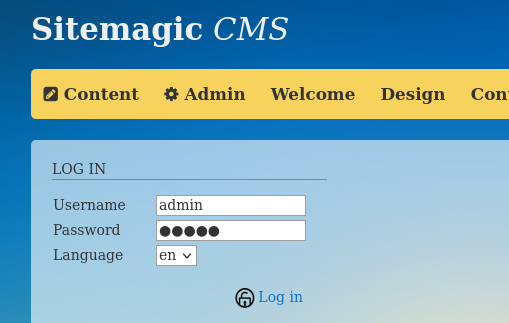


Revisamos el archivo de configuración "config.xml.php" y enumeramos las credenciales del administrador del CMS.

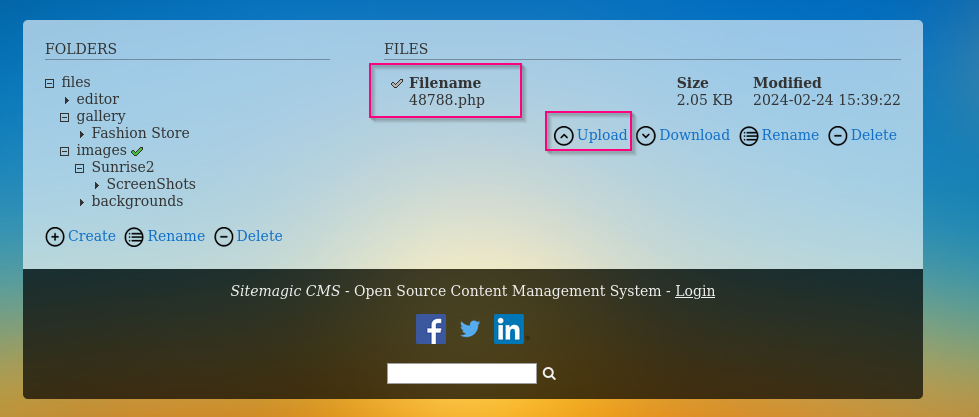


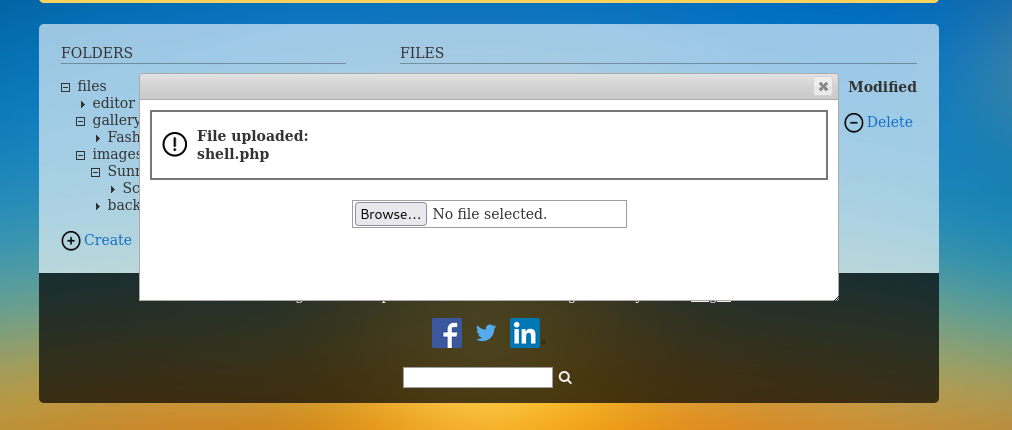
Entramos en la web, en sitemagic y nos logueamos con las credenciales de la imagen:



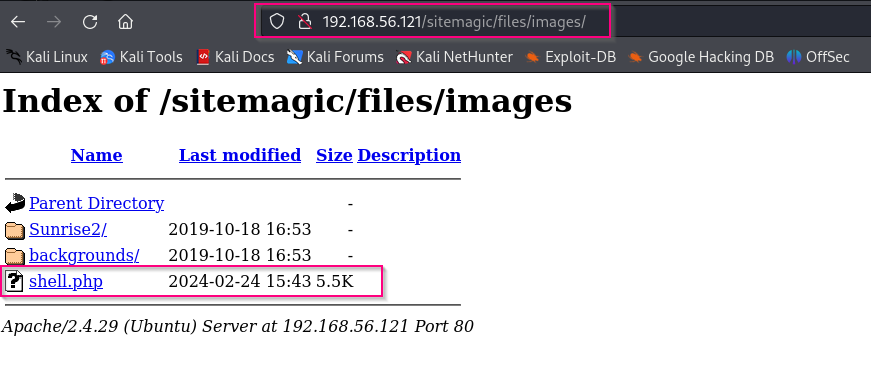


En la parte de Content/files subimos el archivo del exploit: pentestmonkey’s webshell

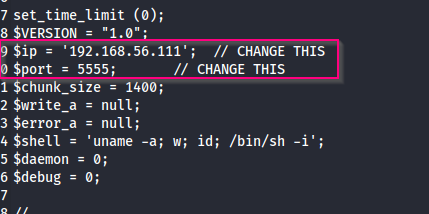
:



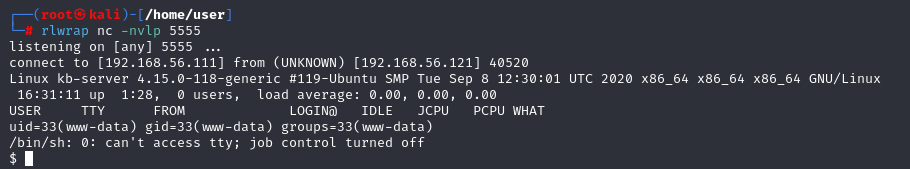
Y vemos que se haya subido:

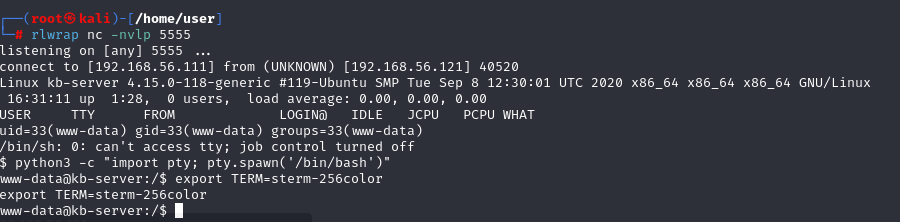


En el archivo de Shell tenemos que cambiar dos parámetros: la Ip es la de nuestro Kali y el puerto por donde ponemos el netcat.

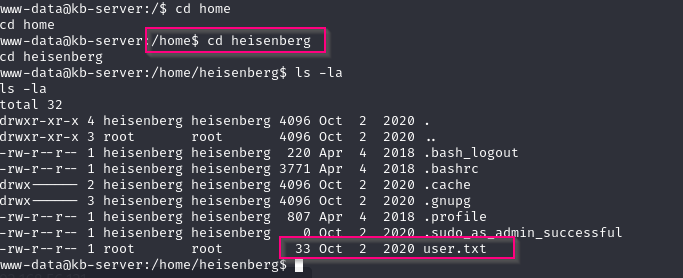


Y nos sale esto en el netcat cuando ejecutamos el shell.php

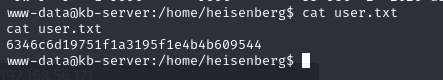




Accedemos a la página de inicio del usuario "heisenberg" y tenemos acceso a leer el fichero "usuario.txt".

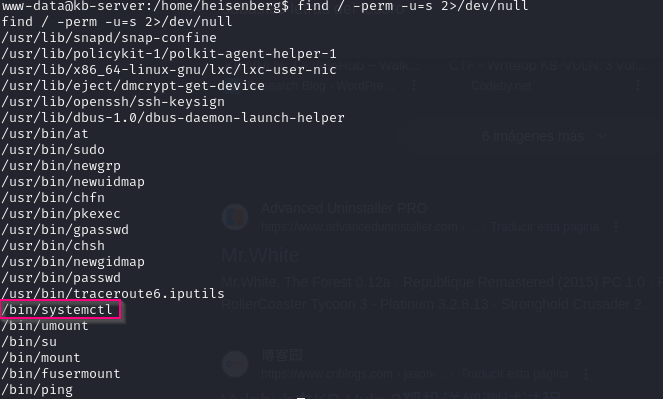


Hacemos un cat al archivo de texto:

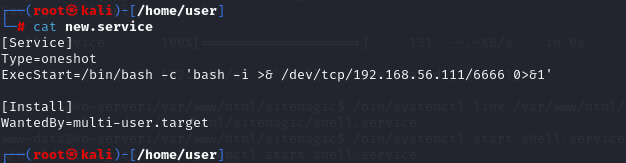


Nos da una serie de caracteres que no nos dicen nada.

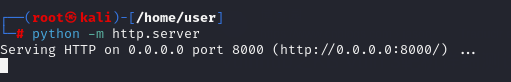
Asique usaremos el comando de find para obtener una lista de los archivos binarios que podemos ejecutar: y nos fijamos en el systemctl



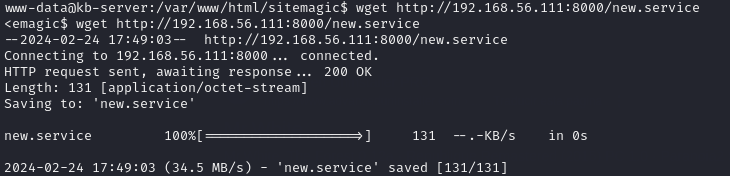
Y podemos utilizar métodos con esta información: creamos el siguiente archivo



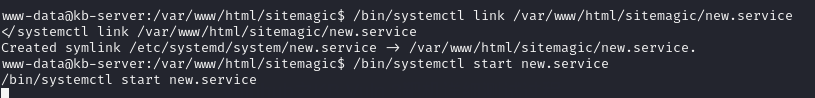
Abrimos el servidor de http 8000



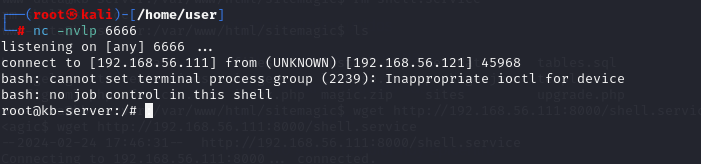
Y subimos el archivo nuestro de new.service a la maquina objetivo:



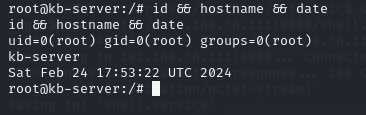
Y la linkeamos con systemctl:



Y activamos el servicio mientras hacemos un netcat al puerto 6666:



Y ya estaríamos en root:



Finalizamos:

