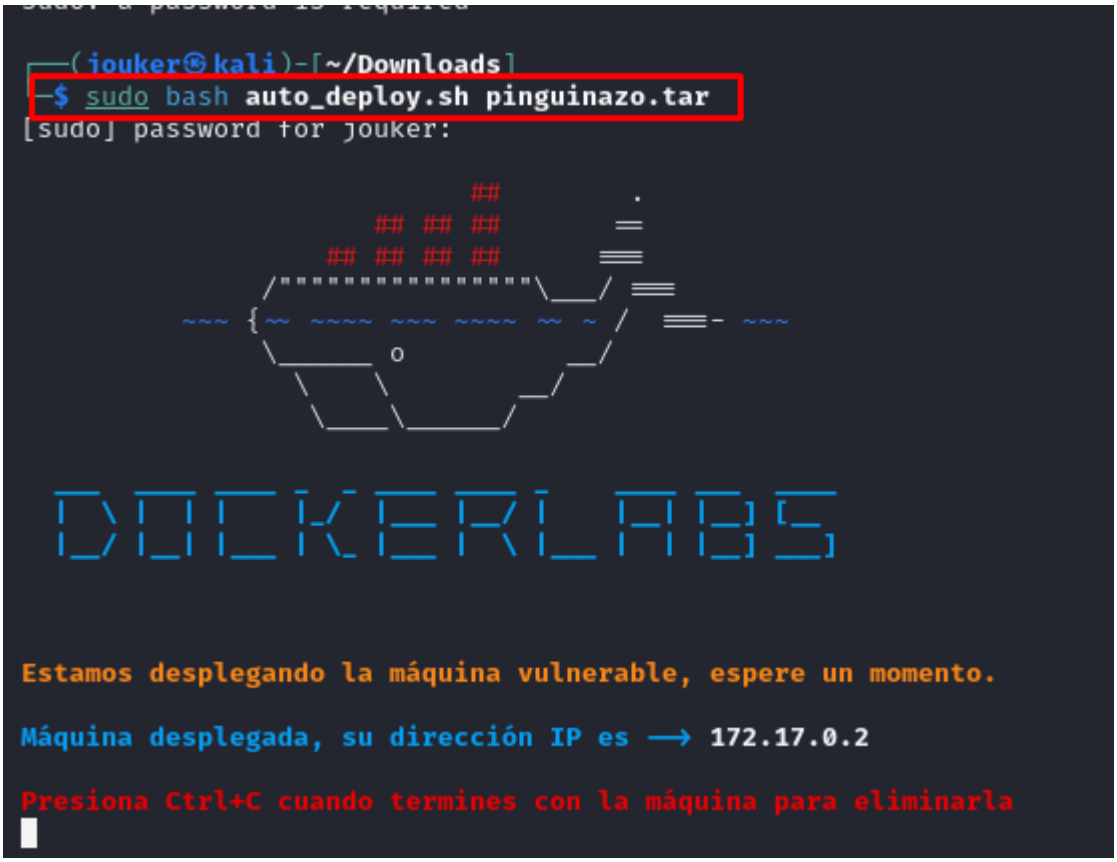
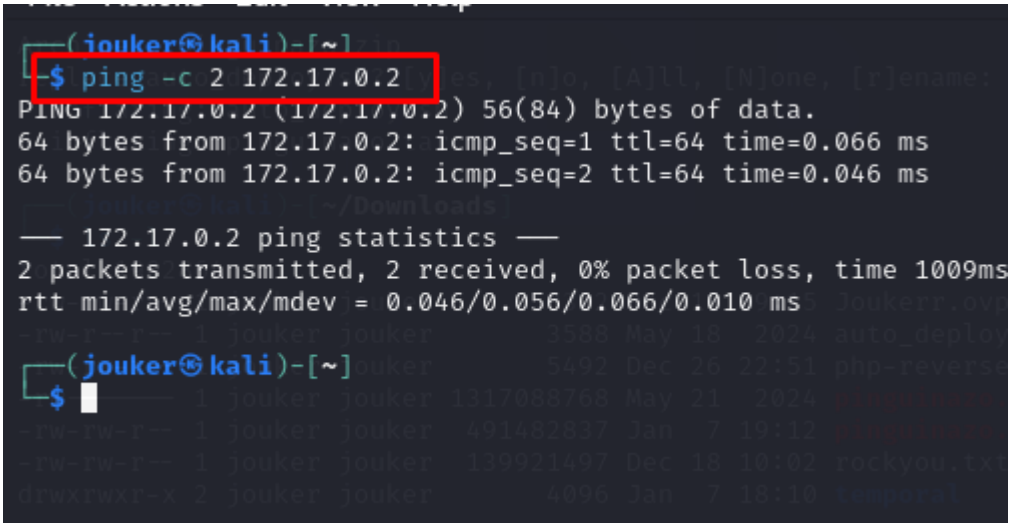
Abrimos Máquina

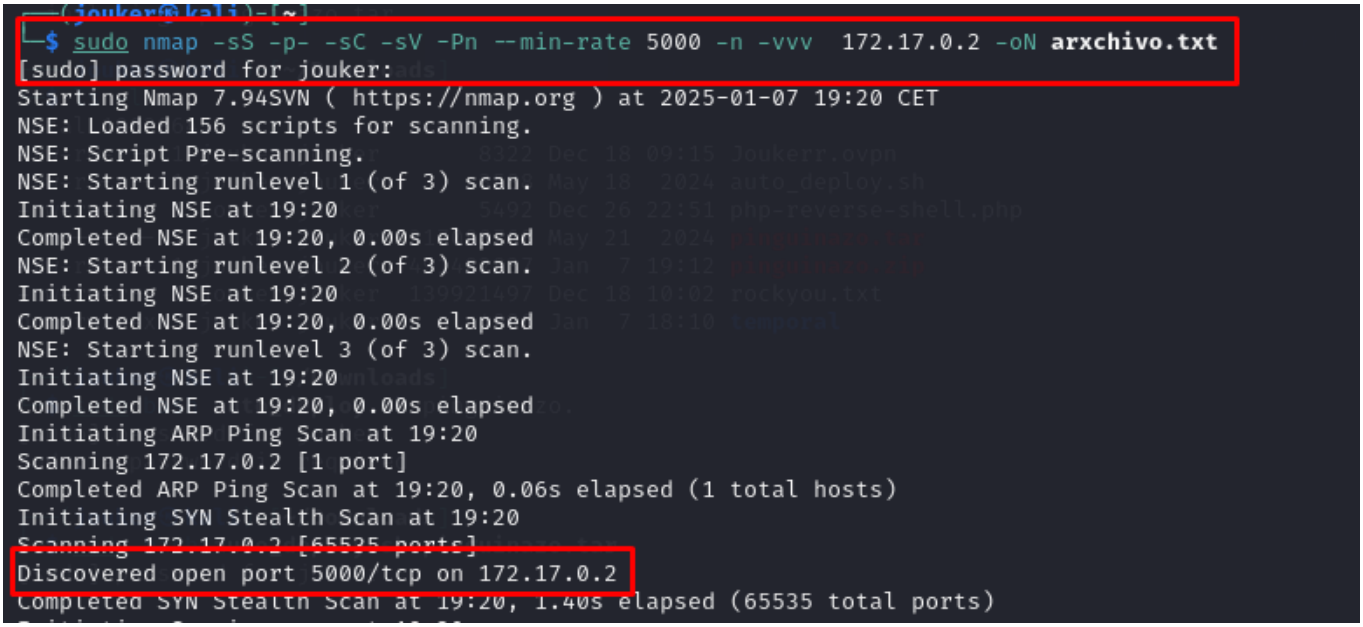



Ping de reconocimiento inicial

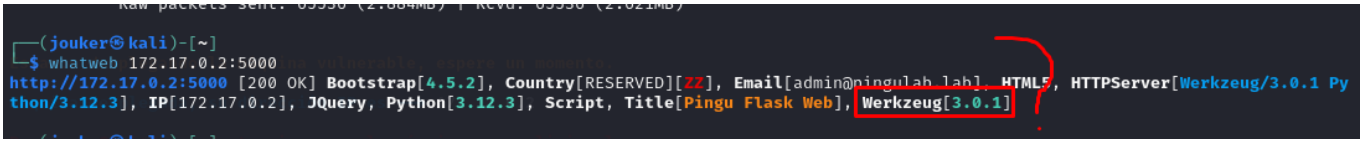



Nmap nos descubre que el puerto disponible en este caso es el puerto 5000, no nos encontramos el habitual 80 y 22, ni tampoco el 443, mirando con un poco más de detalle podemos ver como dicho

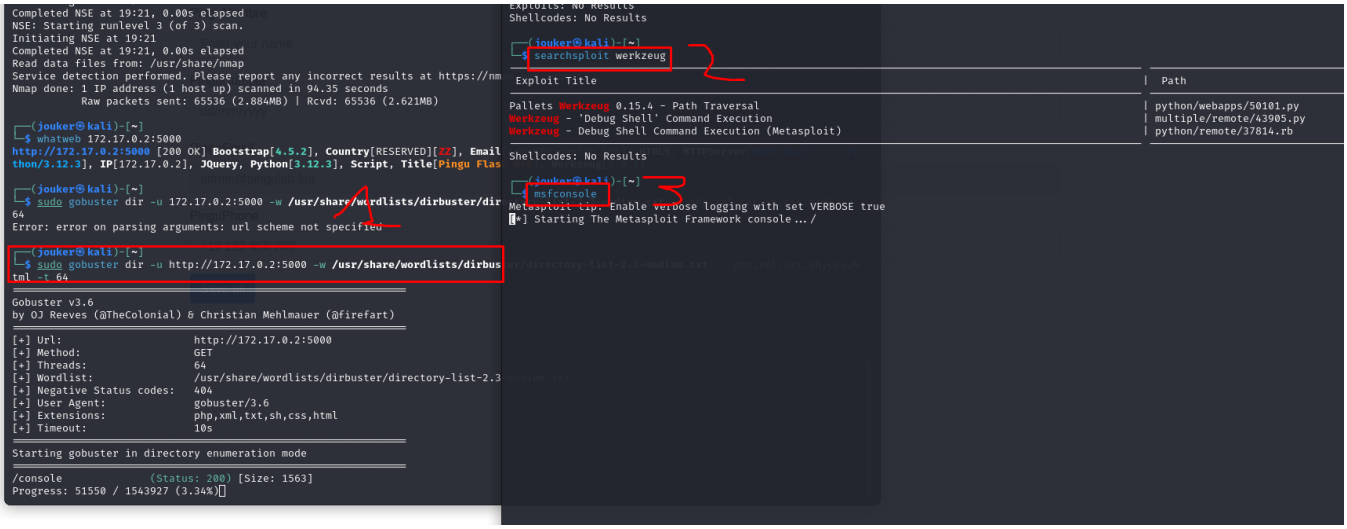
puerto 5000 también es un servidor web pero en un puerto diferente.



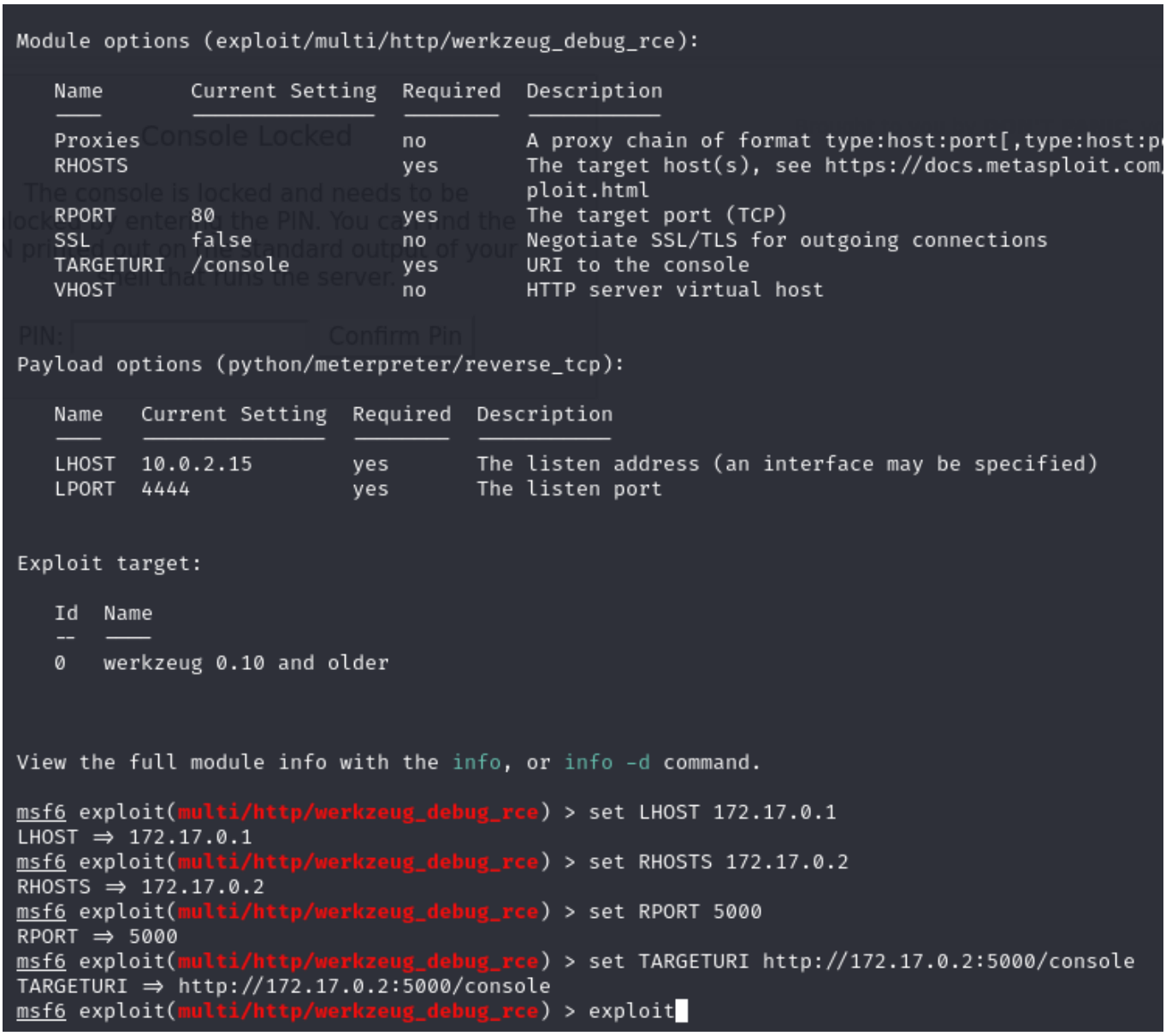

Fuera de lo habitual veo un WerkZeug, que no se que es, voy a mirar la página para ver si es vulnerable por alguna versión anterior



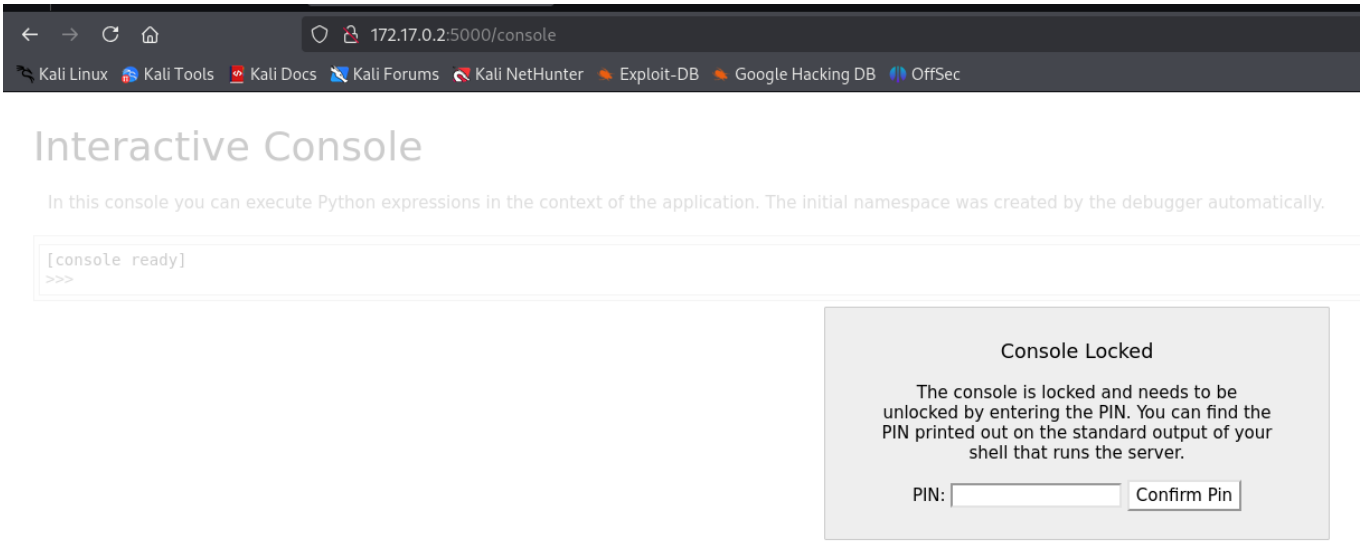

Aprovecho para realizar 2 tareas al mismo tiempo, buscar por metasploit lo de wekzeug, y al mismo tiempo realizo fuzzing de directorios.

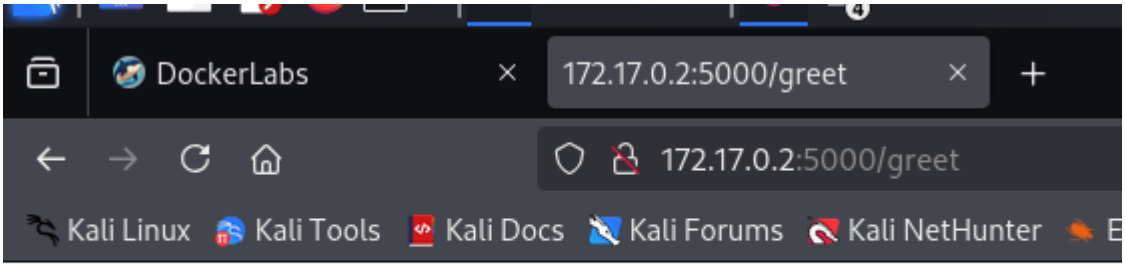


Al realizar el intento de intrusión en metasploit veo que he de indicar la existencia de un directorio console, que he listado antes con gobuster, como se ve en la captura anterior, al entrar un poco mas en detalle en dicha página me pide un PIN, pero no creo que sea relevante.



Esta es la página de la console




Hello sss!

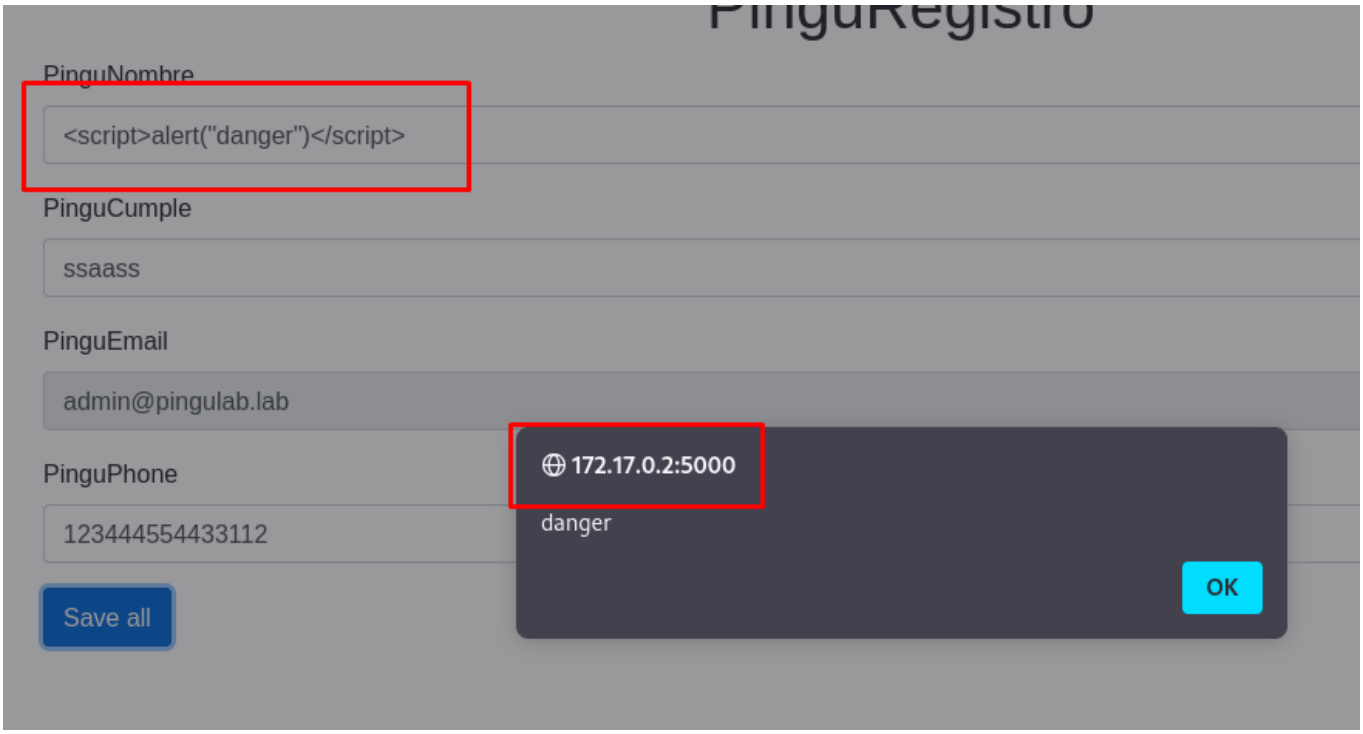
Hay algo curioso y es que si en el formulario tu pones etiquetas HTML puedes ver como SI se editan las cosas


Hello

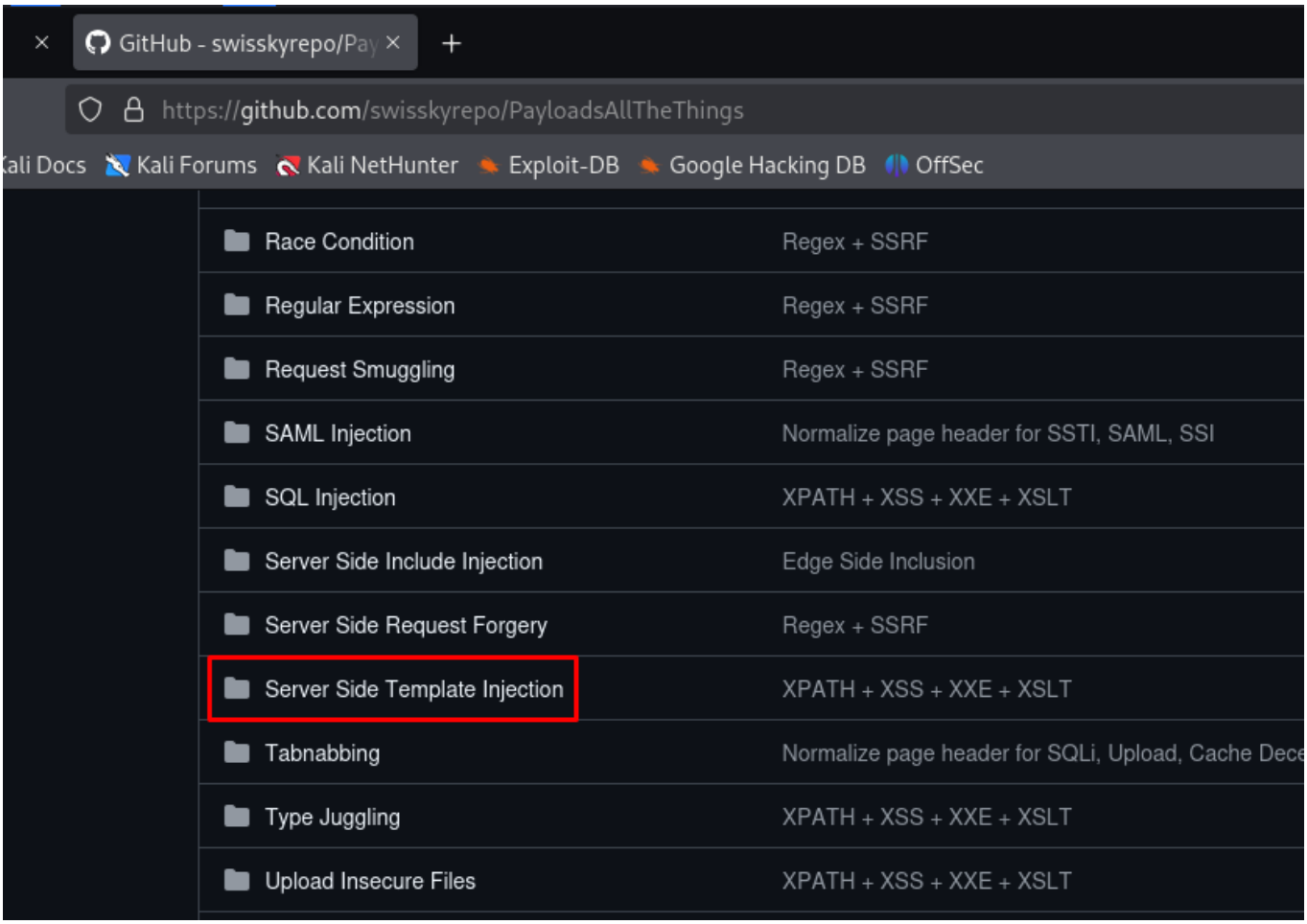
# Me interpretas los titulos o no?

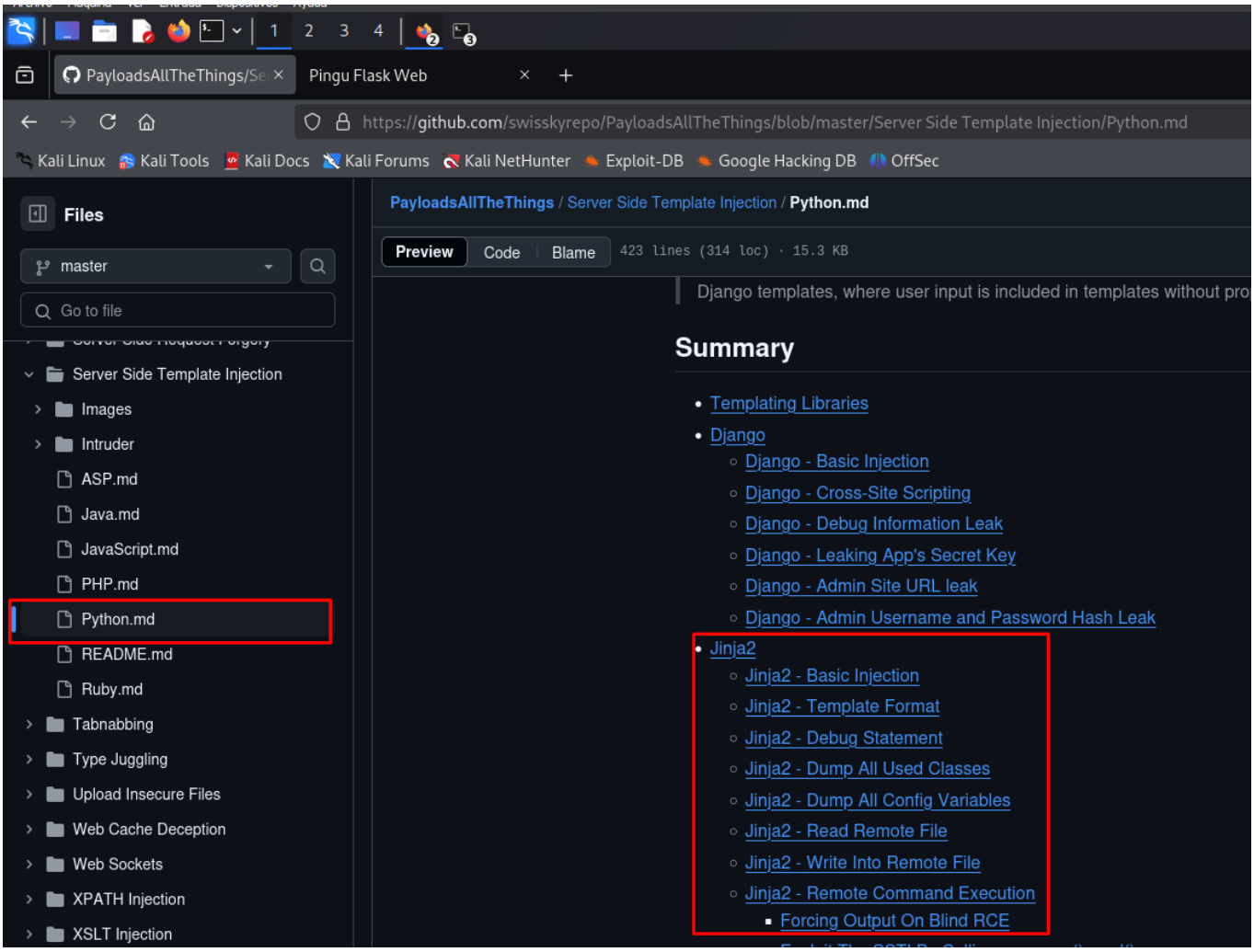
!

Ejemplo pero con crosssite scripting

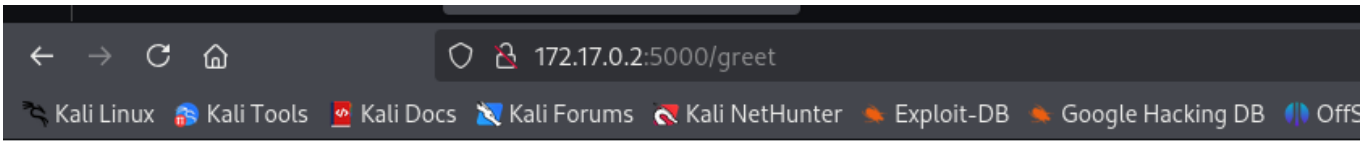


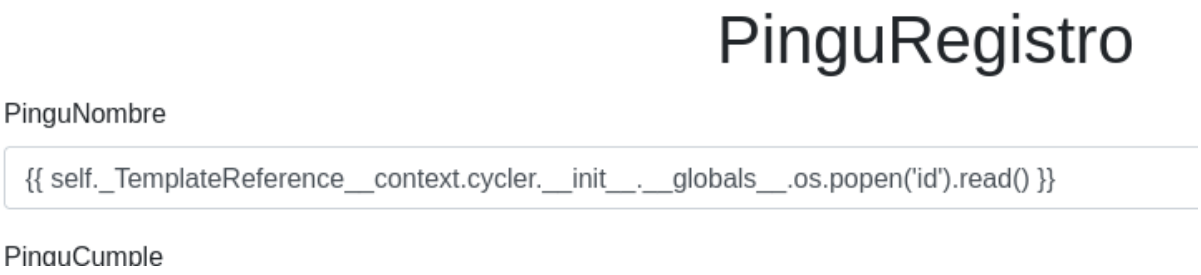

Parece ser que el error no tiene nada que ver con metasploit y hay que explorar un poco más en detalle que puedo encontrar con el XSS y mas bien parece un ataque SSTI de inyección de plantillas


GitHub - swisskyrepo/Pay
https://github.com/swisskyrepo/PayloadsAllTheThings
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Race Condition
Regex + SSRF
Regular Expression
Regex + SSRF
Request Smuggling
Regex + SSRF
SAML Injection
Normalize page header for SSTI, SAML, SSI
SQL Injection
XPATH + XSS + XXE + XSLT
Server Side Include Injection
Edge Side Inclusion
Server Side Request Forgery
Regex + SSRF
Server Side Template Injection
XPATH + XSS + XXE + XSLT
Tabnabbing
Normalize page header for SQLi, Upload, Cache Dece
Type Juggling
XPATH + XSS + XXE + XSLT
Upload Insecure Files
XPATH + XSS + XXE + XSLT



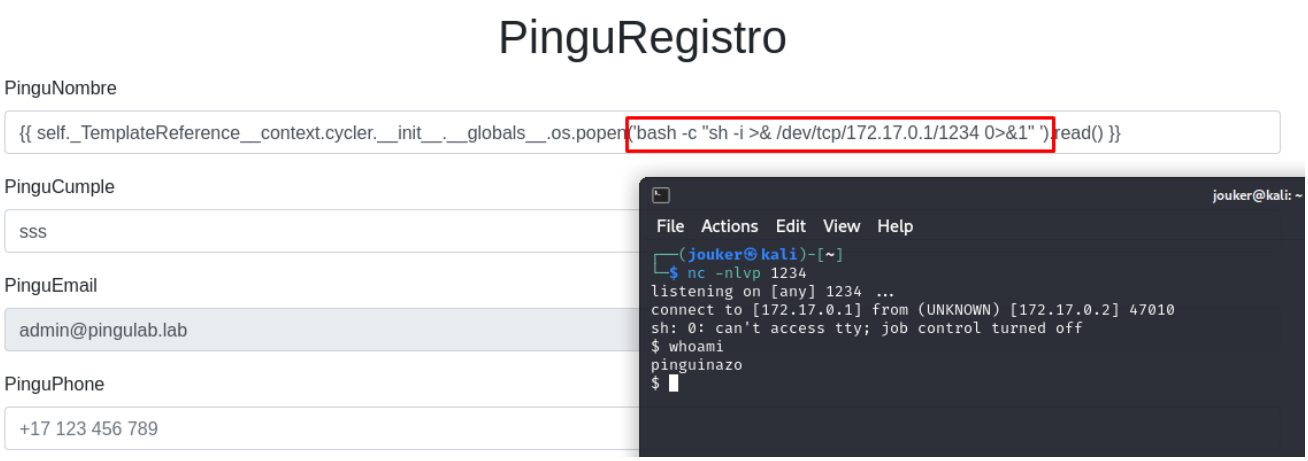

Al ejecutar la comanda correcta puedo ver los usuarios del sistema



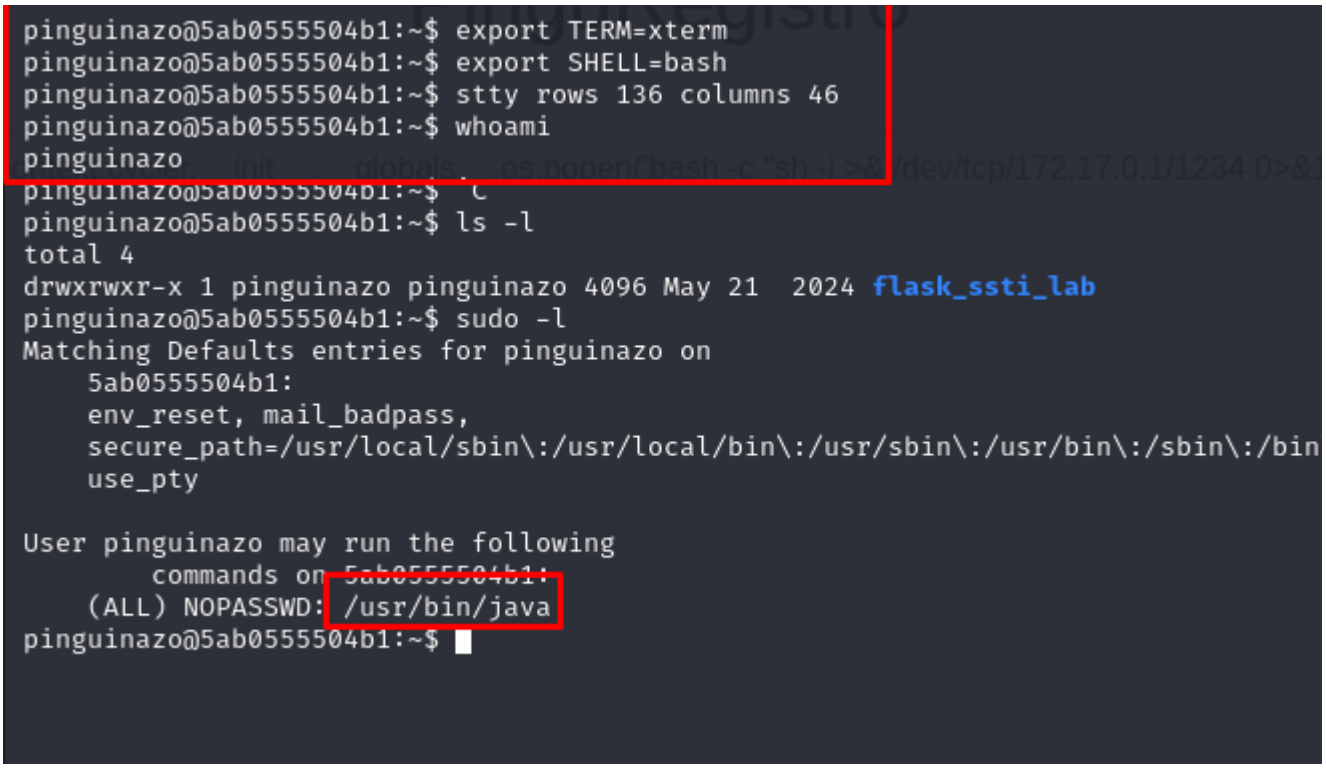




Colamos una shell reversa con bash -c y también con una reverse shell, sin bash -c no va a funcionar. Somos el usuario

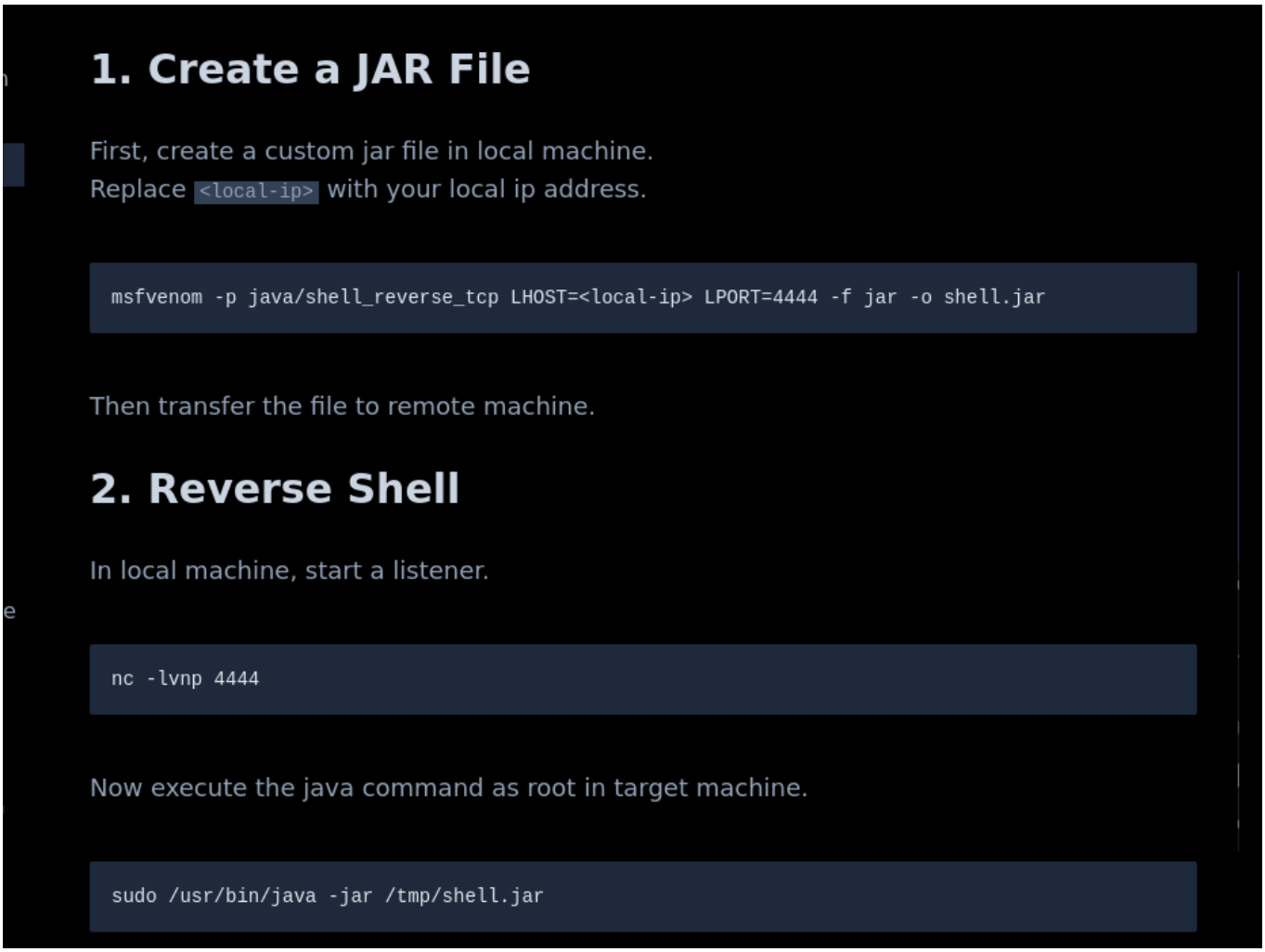
"Pingüinazo" en vez de "www-data"



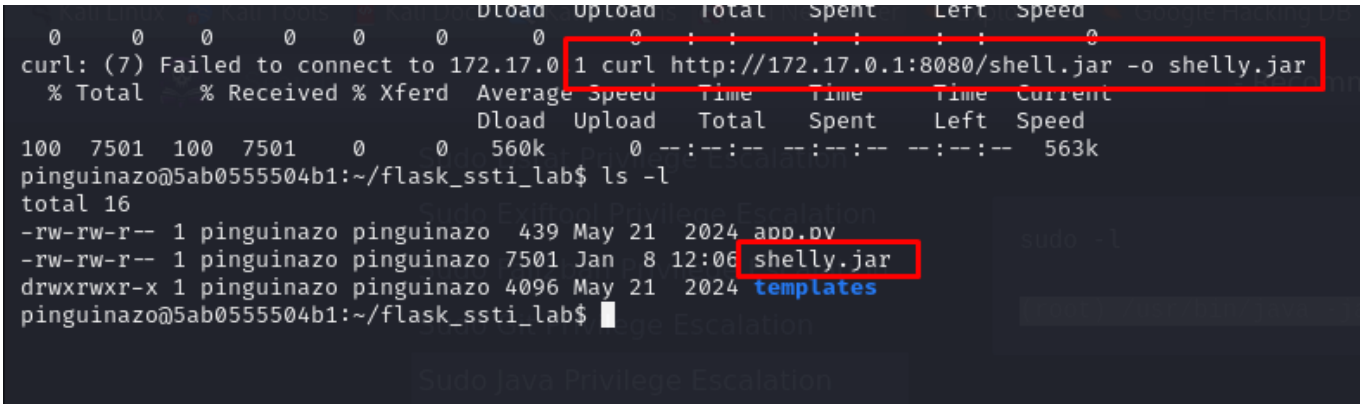

Realizamos tratamiento de la TTY y vemos la escalada de privilegios, veo que es vulnerable a traves de sudo -l /usr/bin/java, miramos en gtfobins para ver el binario vulnerable java, para ver como le hacemos el bypass.



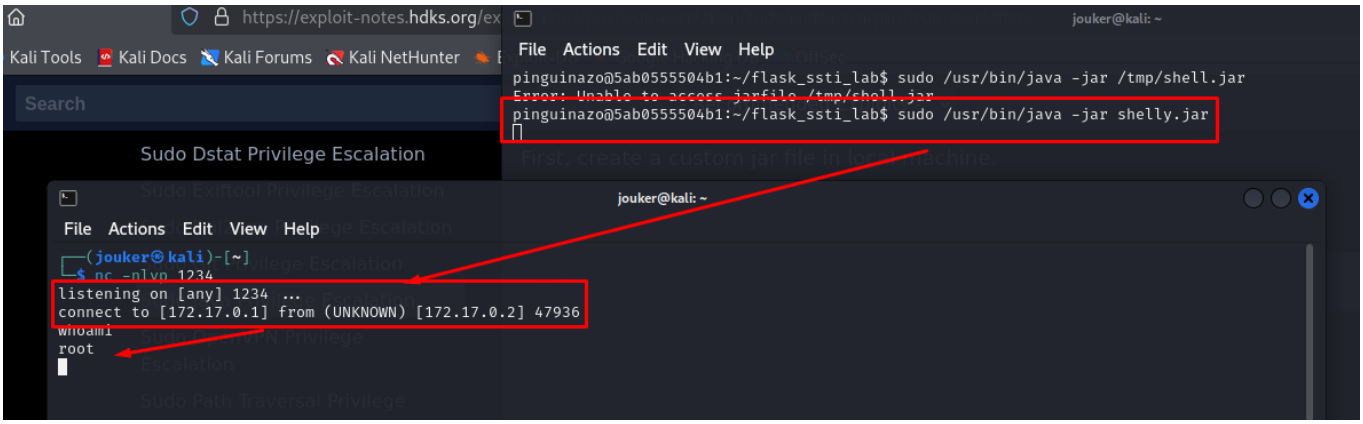

No se encuentra en GTFOBINS el bypass de java con sudo, yendo a una página vemos que hay que crear un exploit con msfvenom.




Tal como indica la comanda anterior hacemos un exploit de reverse shell con msfvenom apuntando a nuestra ip 172.17.0.1
una vez creado creamos un servidor pyhton con `python3 -m http.server 8080` con el servidor python creado en NUESTRA MÁQUINA local, nos dirigimos directamente a la máquina que hemos vulnerado previamente y ejecutamos la comanda de curl para obtener el archivo jar que hemos creado.
Creamos con netcat algo para ponernos a la escucha.




Finalmente somos root




Sinceramente bajo mi inexperiencia considero que esta máquina es más bien una medio-fácil más que una fácil.