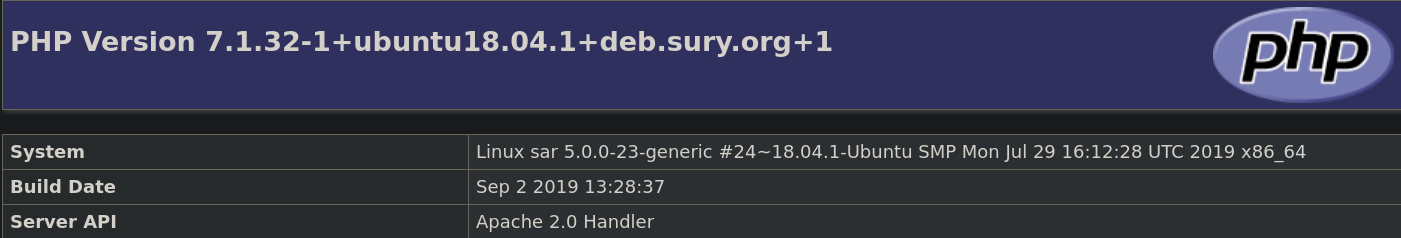


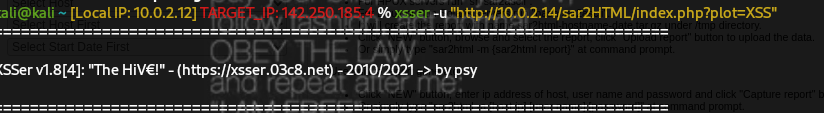
Entro en la web esta <http://10.0.2.14/sar2HTML/index.php>

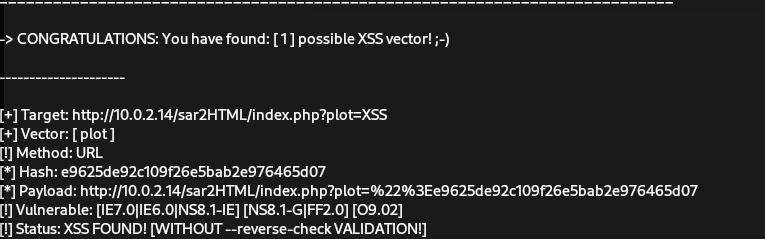
Ecuentro tb esta web <http://10.0.2.14/phpinfo.php>, que aporta mucha información sobre versiones y sistema operativo

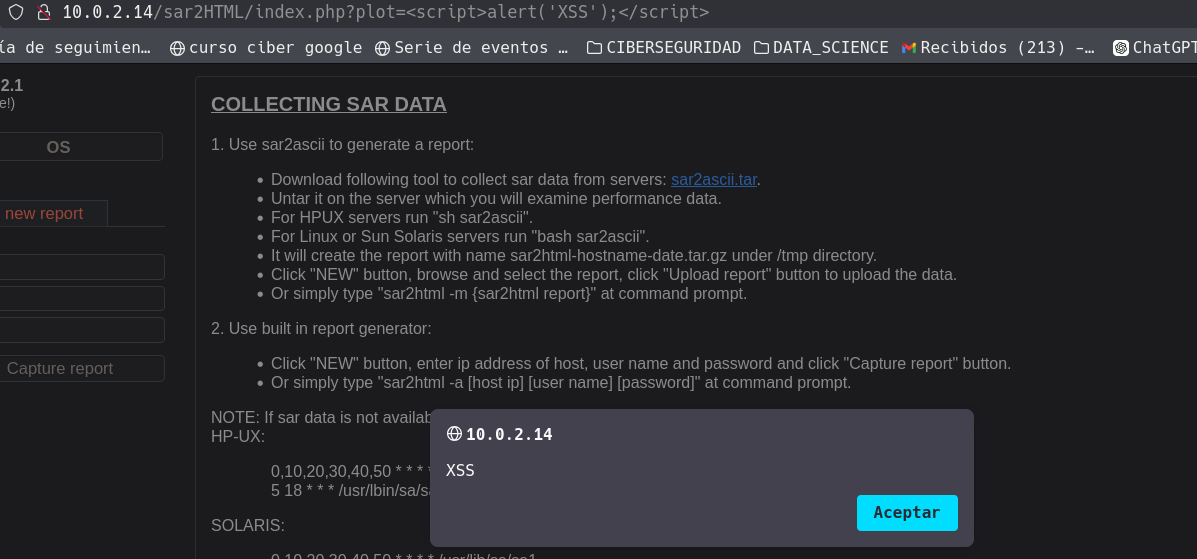


**SAR** en Linux significa **System Activity Reporter**. Es una herramienta del paquete **sysstat** que se utiliza para recopilar, informar y guardar estadísticas de rendimiento del sistema. **sar** puede proporcionar información detallada sobre el uso de los recursos del sistema, como CPU, memoria, disco, red, y otros.

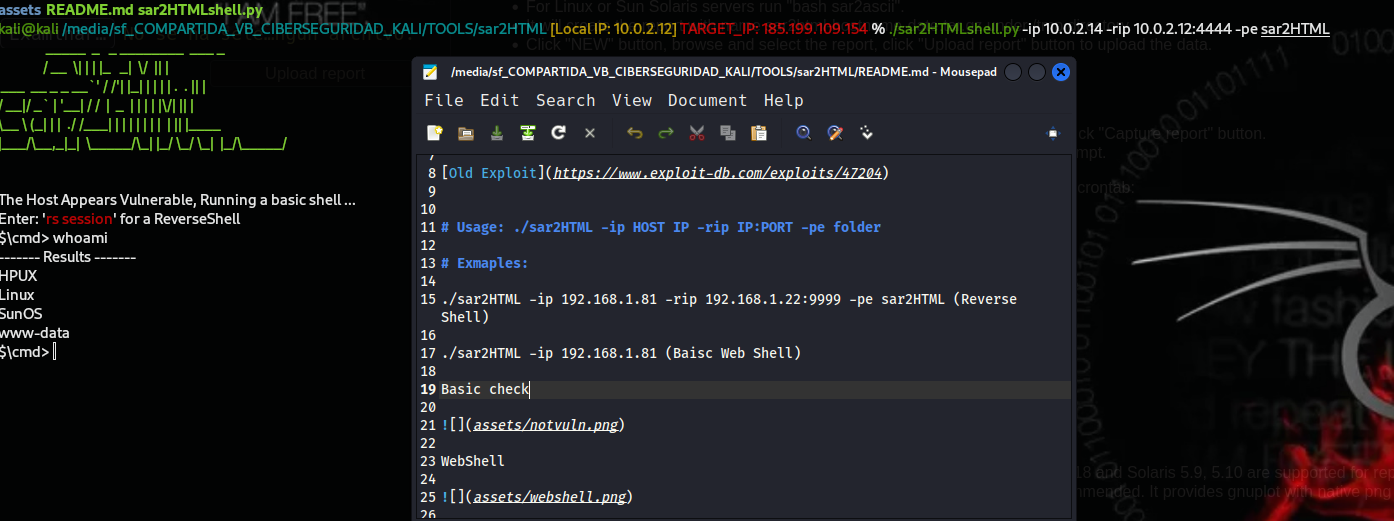
XSS



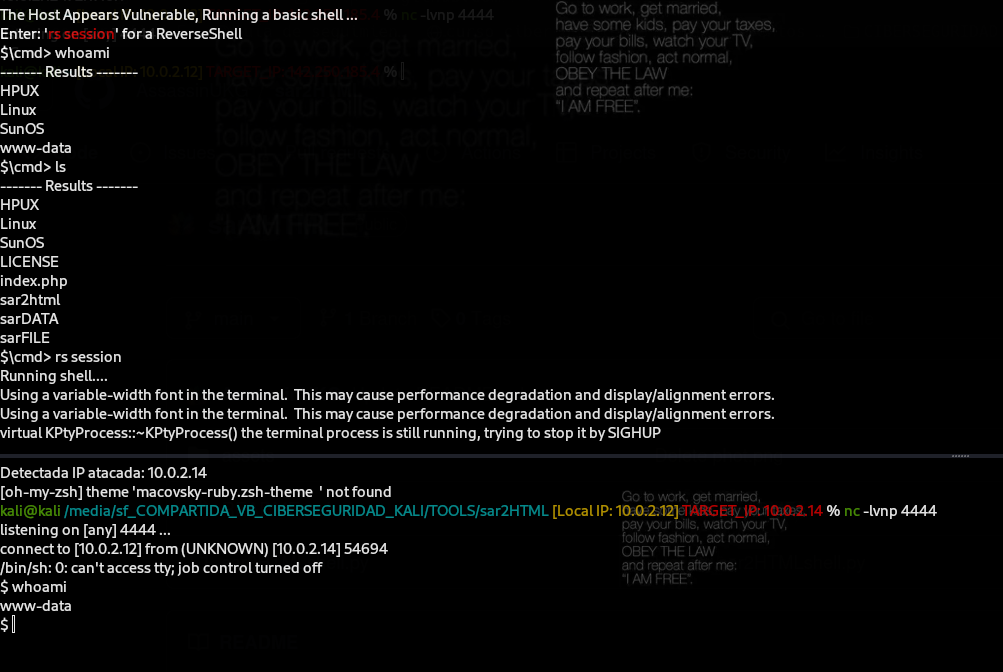




Consigo una shell con usuario limitado a través de ala aplicación <https://github.com/AssassinUKG/sar2HTML> .



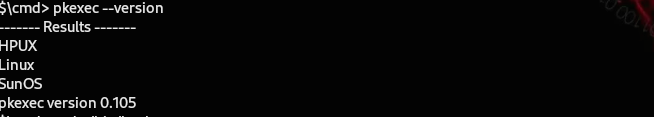
Y consigo la revserse shell



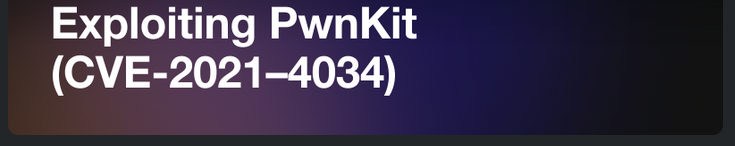
El bit SUID permite que un programa se ejecute con los privilegios del propietario del archivo, que muchas veces es **root**. Esto significa que si encuentras una vulnerabilidad o mal uso de estos archivos con el bit SUID, podrías escalar privilegios y obtener acceso como **root**.

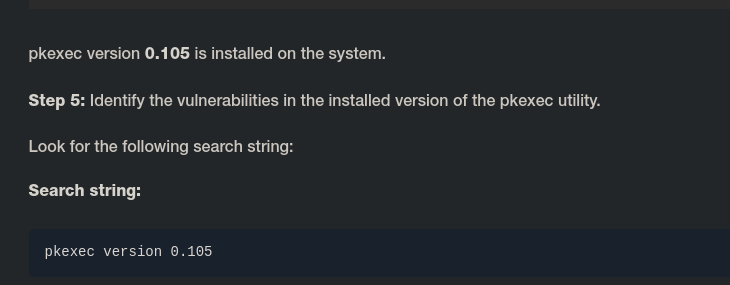


Buscamos información sobre la apliacion pkexec, la cual es una herramienta de **PolicyKit (Polkit)** que permite a un usuario ejecutar programas con los privilegios de otro usuario, típicamente **root**



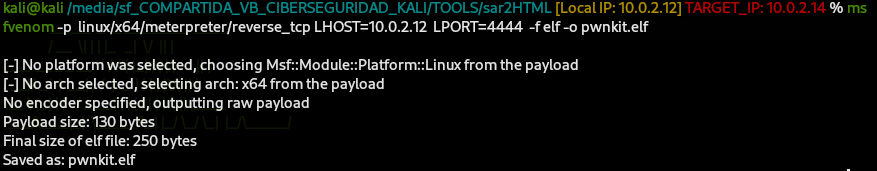
<https://ine.com/blog/exploiting-pwnkit-cve-20214034>



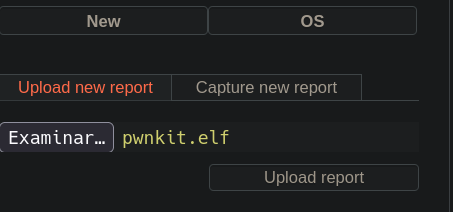


La versión que tiene instalada es vulnerable a ese exploit

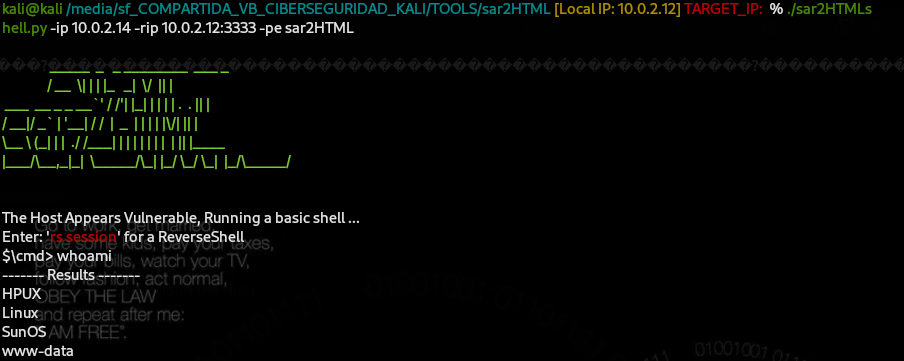
Hacemos el payload malicioso



Subo payload malicioso a través de la web <http://10.0.2.14/sar2HTML/index.php?plot=NEW> , y la damos a “upload report”

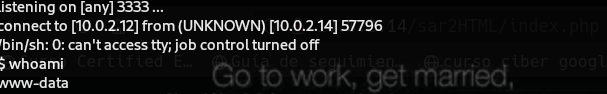


Abro nuevamente la shell básica con el exploit especifico para sar2HTML:



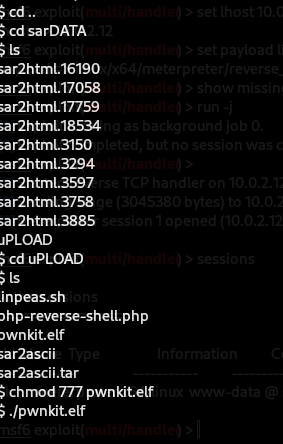
Paso con el comando re sesión a reverse shell, navegando hasta la carpeta upload donde esta el payload malicioso subido.



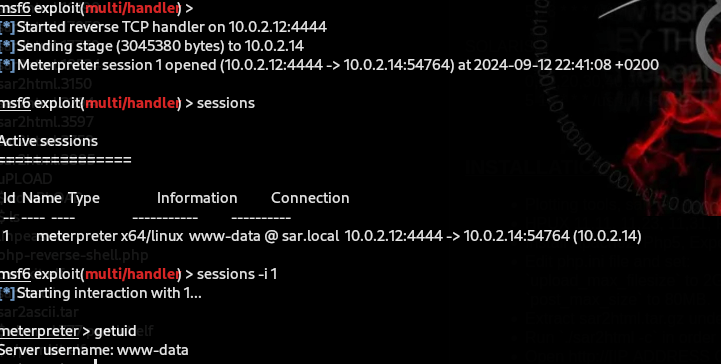


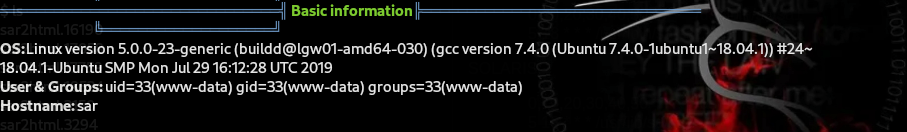
Le doy permisos al ahrchivo y lo ejecuto, no sin antes haber abierto una multi/handler en metasploit para recibir la conexión:



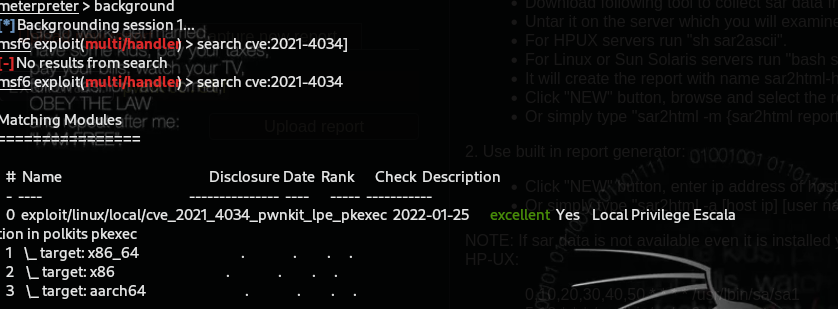


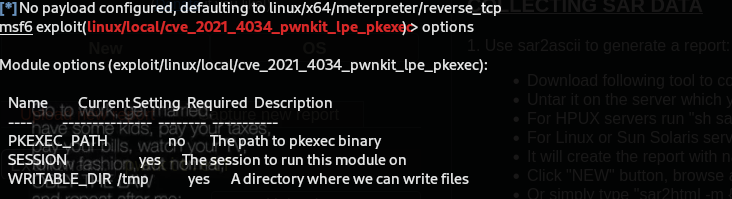
Una vez ejecuto el archivo ./pwnkit.elf, conseguimos una meterpreter a través de Metaesploit:

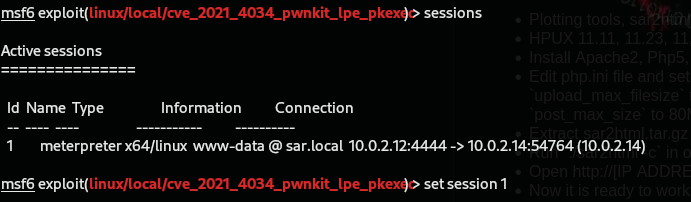




Ya tenemos una shelll mas comoda y mas interactiva para trabajar, pero los permisos de susuario son insuficientes para conseguir persitencia, por lo que con la vulnerabilidad CVE-2021-4034 anteriomente encontrada y aprovechando la sesión meterpreter actual, ejecutaremos el exploit, para conseguir una meterpreter con root.

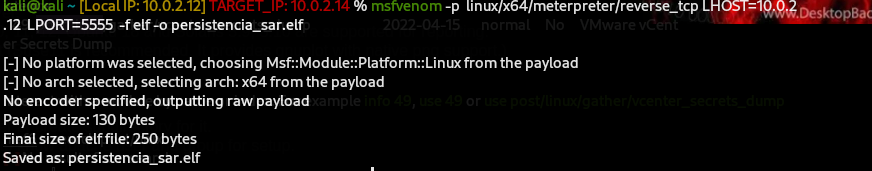




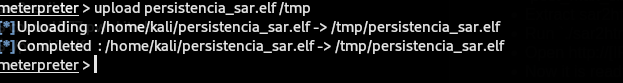




Ahora vamos a dejar un payload malicioso en el archivo de tareas programadas Crontab, archivo especial en sistemas operativos **Unix** y **Linux** que se utiliza para programar la ejecución automática de tareas en momentos específicos. gestionadas por el **daemon cron**, un proceso en segundo plano que se ejecuta en el sistema y verifica regularmente si hay tareas programadas que deben ejecutarse.



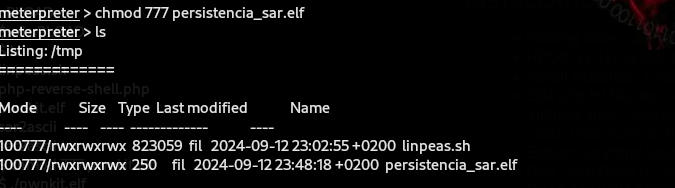
Subimos



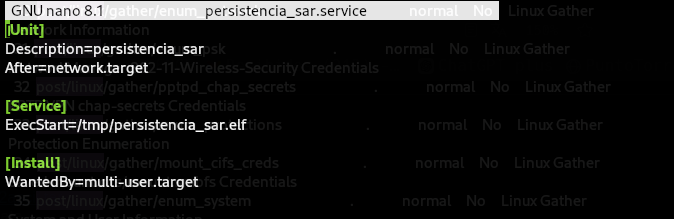
Abrimos un handler



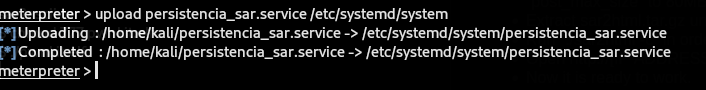
Continuamos con la sesión root



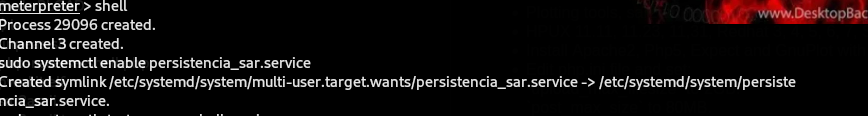
Vamos a ejecutar un servcio en System para q se inicie nuestro payload para ello, creamos un servicio:



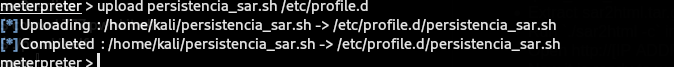
Lo subimos a la ruta del sistema



Y activamos el servicio



Probamos otros sitio, en profile.d





ESTA TODO HEHCO, FALTA CONSEGUIR USUARIO LOVE CONTRASEÑA O CUALQUIER OTROAPARA Q SE INCIE LA SHELL

