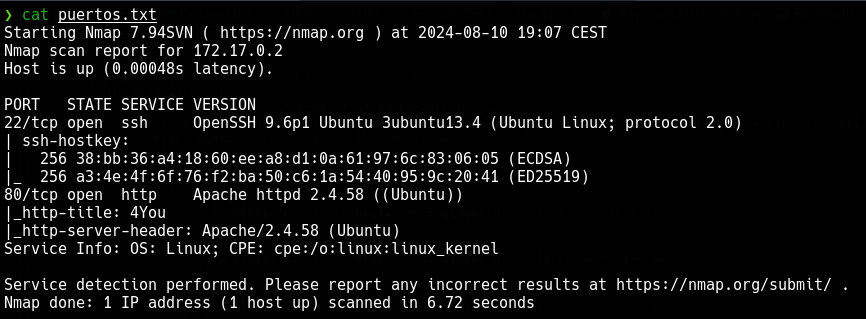
**Psycho**



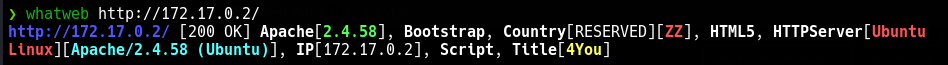
**Reconocimiento**:

Para comenzar, lo primero que haremos es realizar un escaneo de puertos con nmap, para ver que puertos y servicios tiene abiertos esta máquina.

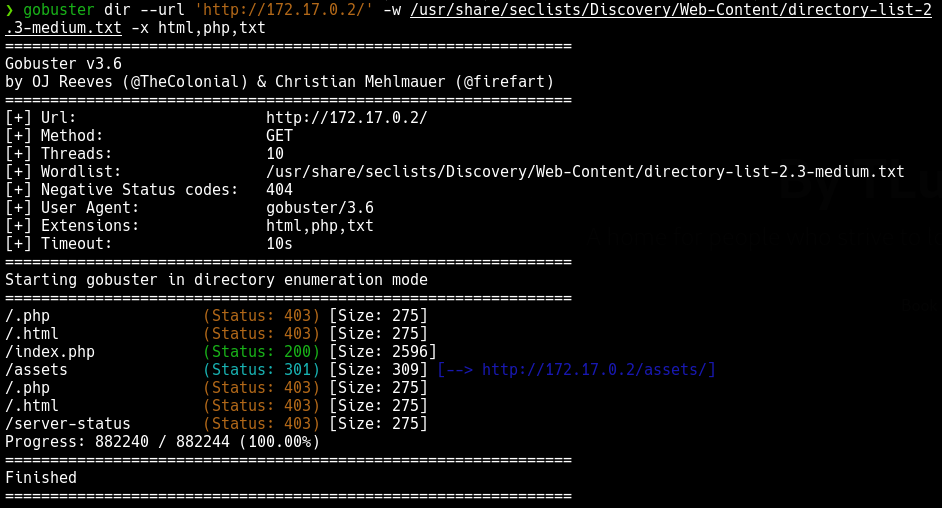


**Puerto 80**

Lo primero enumeramos las versiones de este servidor web para buscar posibles exploits, pero no es el caso



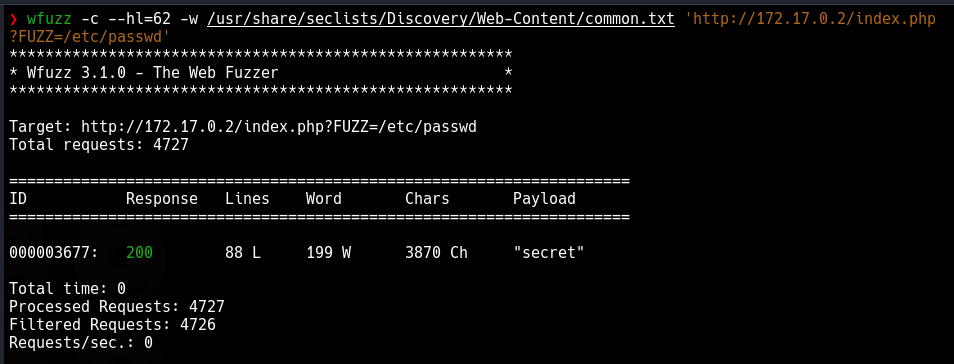
Lo siguiente es realizar un poco de Fuzzing Web para la enumeración de directorios del servidor web.



No encontramos gran cosa, pero me llama la atención el index.php, y en este .php aparece un error, lo que nos da a pensar que necesita un parámetro válido.

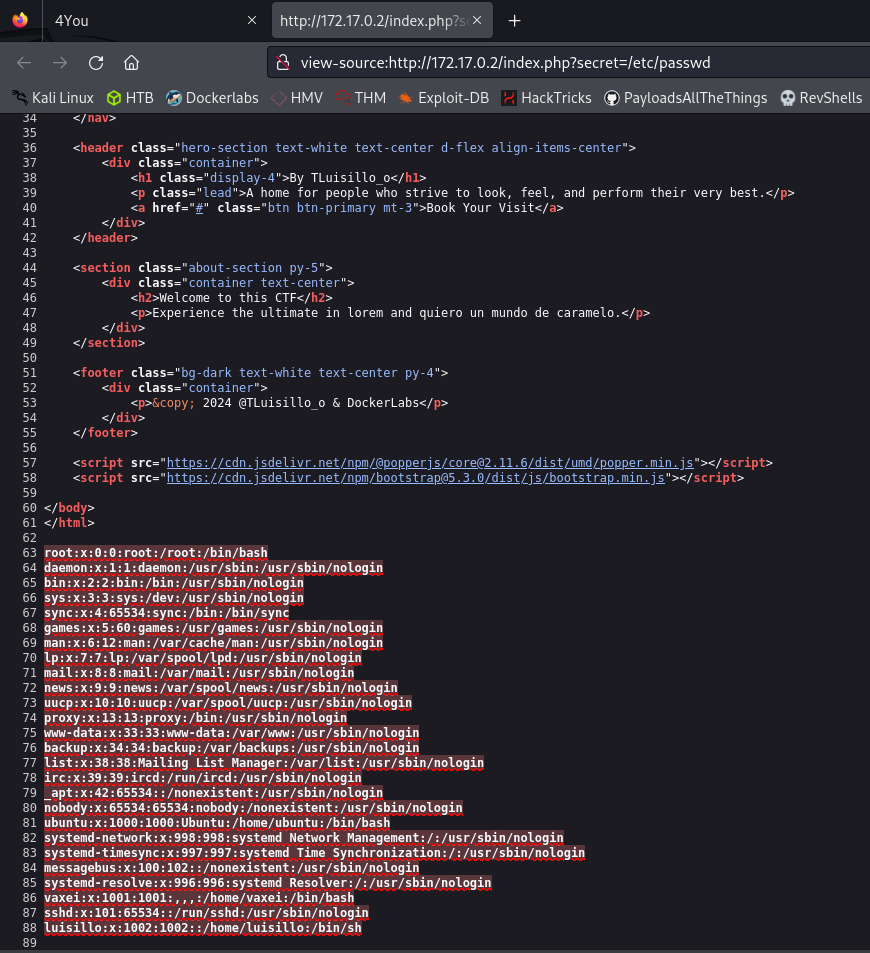


Realizamos un fuzzing a un posible parámetro para ver si es vulnerable a un LFI.



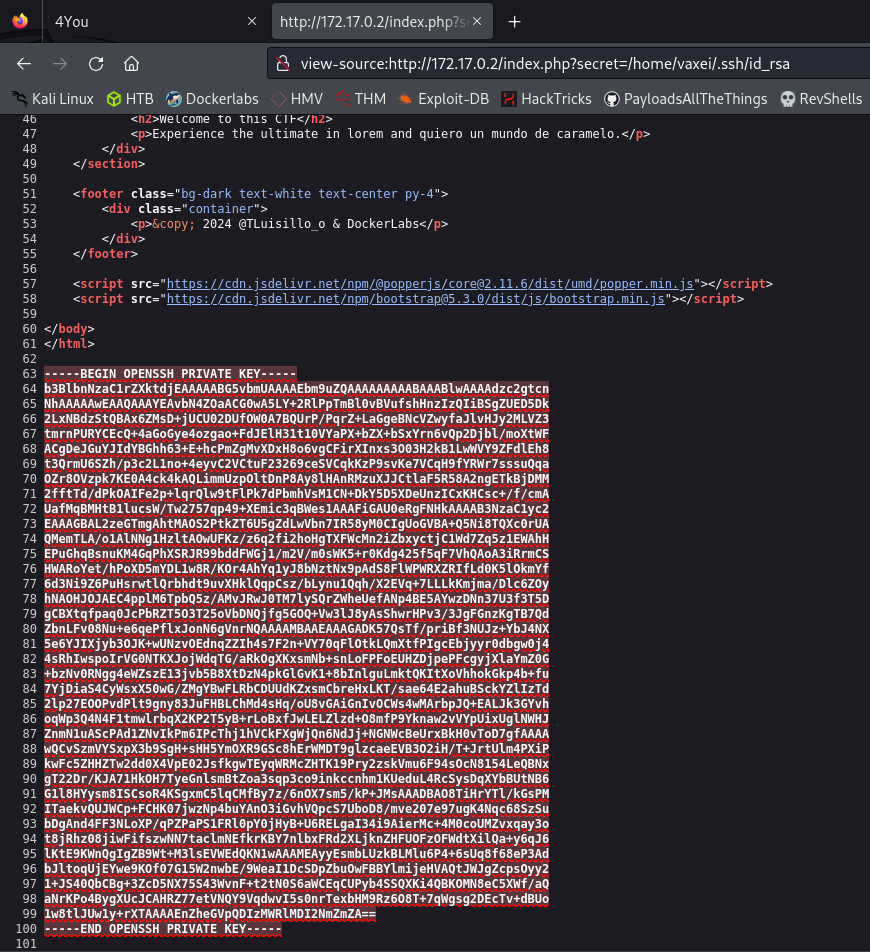
**Explotación**

Comprobamos que efectivamente, es vulnerable a un LFI si utilizamos el parámetro secret.

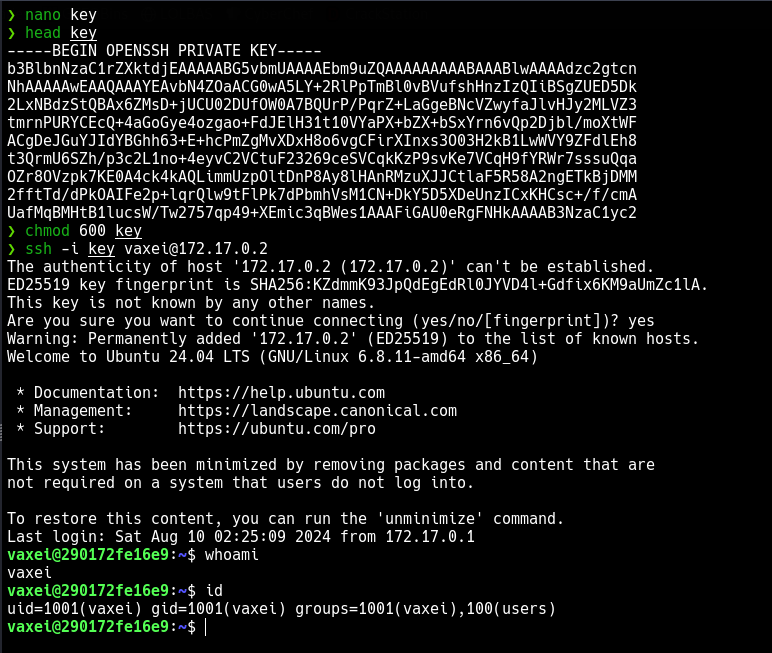


Podemos observar que hay 2 usuarios, luisillo y vaxei.

Recordando la enumeracion de puertos, tenemos el puerto 22 abierto, con el servicio ssh corriendo, por lo que vamos a ver si tenemos acceso a la clave id\_rsa de alguno de estos 2 usuarios.



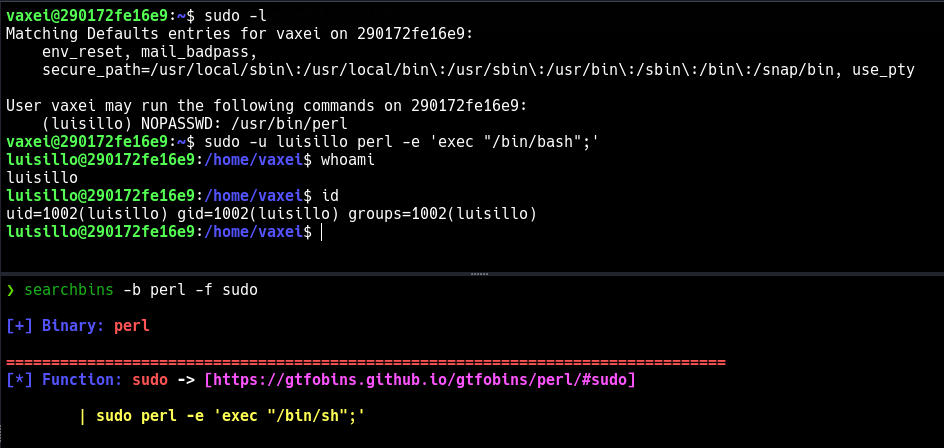
Tenemos la clave id\_rsa del usuario vaxei, nos la guardamos y le damos los permisos necesarios e intentamos conectarnos por ssh.



**Escalada de privilegios**

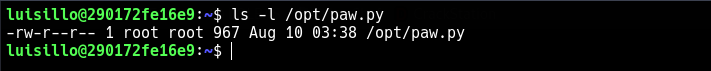
Ya tenemos acceso al servidor, ahora tenemos que escalar privilegios para comprometer por completo esta máquina.

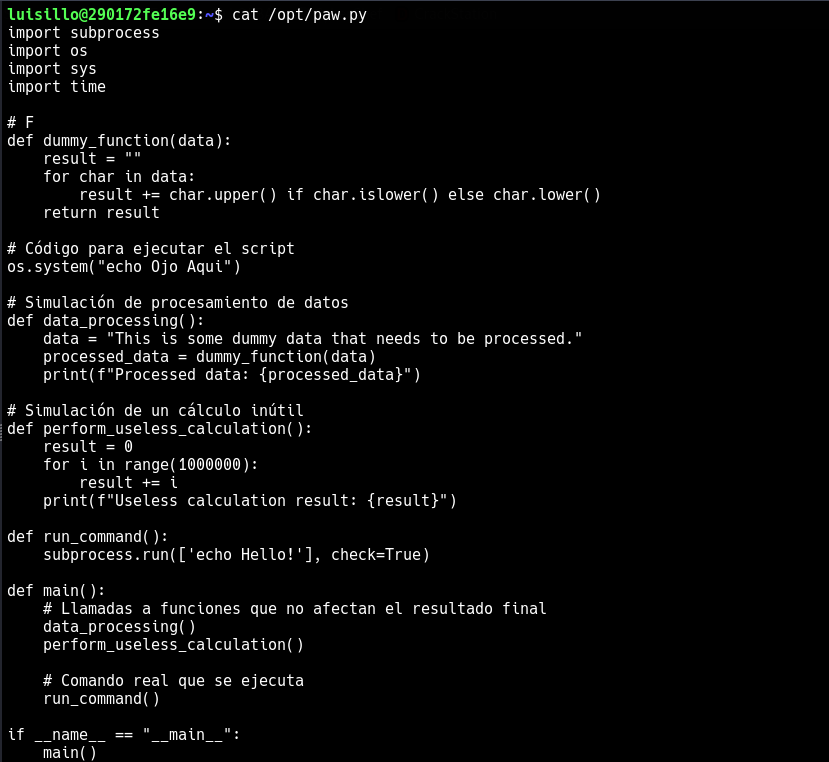
Podemos observar que podemos ejecutar el binario perl con privilegios del usuario luisillo.



Ya estamos como el usuario luisillo, y nuevamente con el comando sudo -l, vemos que puede ejecutar un script de python con privilegios de root.



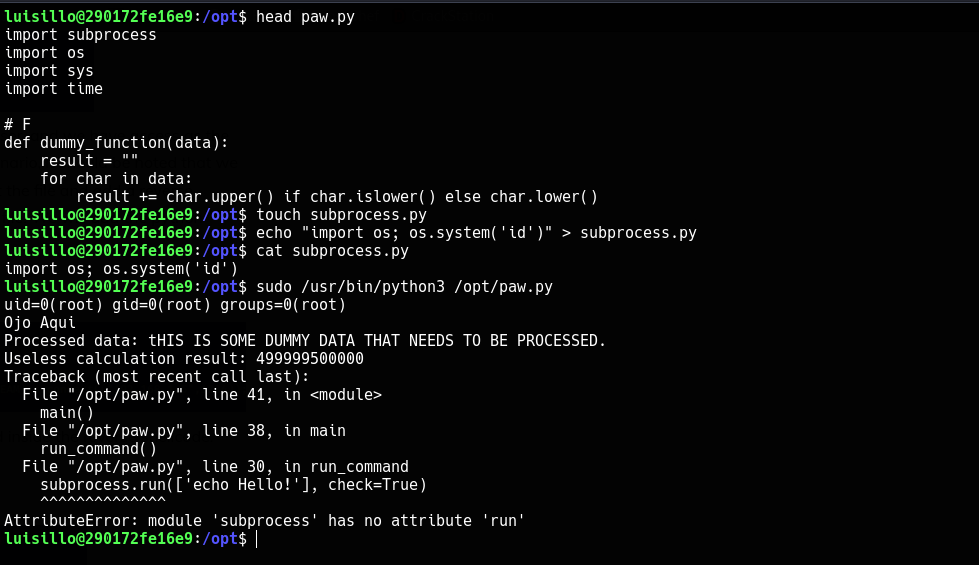




Podemos ver que el script utiliza varias librerías, pero al no tener permiso de escrituras sobre este script ni en las propias librerías almacenadas en /usr/lib/python3.12, no lo podemos modificar, por lo que vamos a intentar a ver si es posible realizan un Python Library Hijacking, para ello he utilizado una el siguiente artículo, centrándonos en el segundo método que enseña;

<https://www.hackingarticles.in/linux-privilege-escalation-python-library-hijacking/>

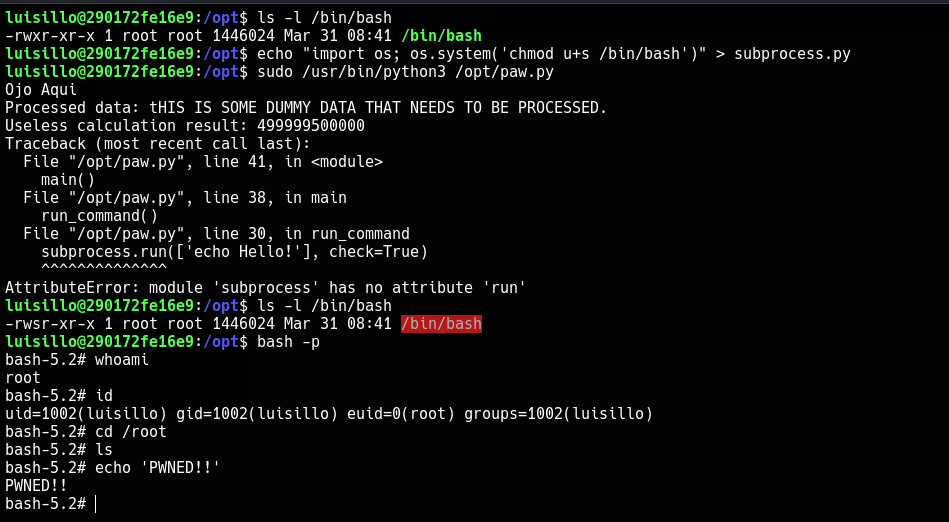
Lo primero es realizar un .py en la misma carpeta en la que se encuentra el script, /opt/, con el nombre de alguna de las librerías utilizadas en el script, en mi caso lo he hecho con subprocess.py



En el fichero que he creado, he importado la librería os y ejecuto el comando id. Ejecuto con sudo el script y vemos como nos muestra el comando que hemos puesto en nuestra "librería falsa".

Para escalar privilegios se puede hacer de varias formas, en mi caso le voy a dar permisos SUID a /bin/bash, y para ello, modificamos nuestro subprocess.py y le añadimos "chmod u+s /bin/bash"

Ejecutamos de nuevo el script, comprobamos que se le han asignado permisos SUID a la /bin/bash y con el comando bash -p obtenemos una shell de root



Con esto ya tendríamos la maquina comprometida, en la que hemos aprendido como detectar y explotar un LFI, como realizar movimiento lateral a otro usuario explotando sudo, y por ultimo como escalar privilegios realizando un Python Library Hijacking.