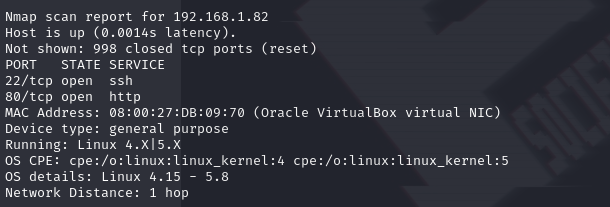
Juego Fsociety!

hago sudo nmap -O 192.168.1.0/24 para averiguar la IP de la máquina virtual

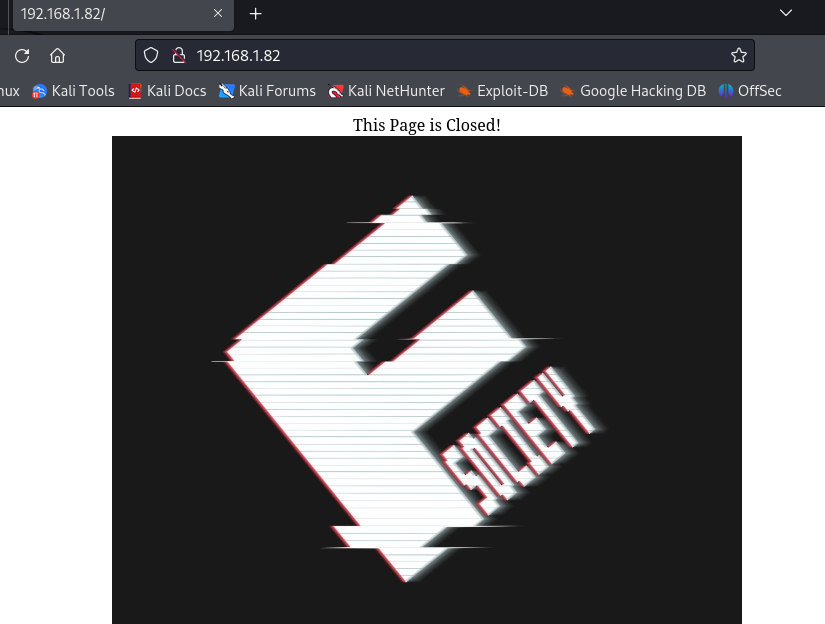
Este comando intentará detectar el sistema operativo de cada dispositivo activo. Nota que requiere privilegios de superusuario (sudo).

En los resultados hay una máquina que tiene como MAC Address un Oracle VirtualBox asi que supongo que es ese el IP correcto.



Abro un navegador web y navego a http://192.168.1.82.

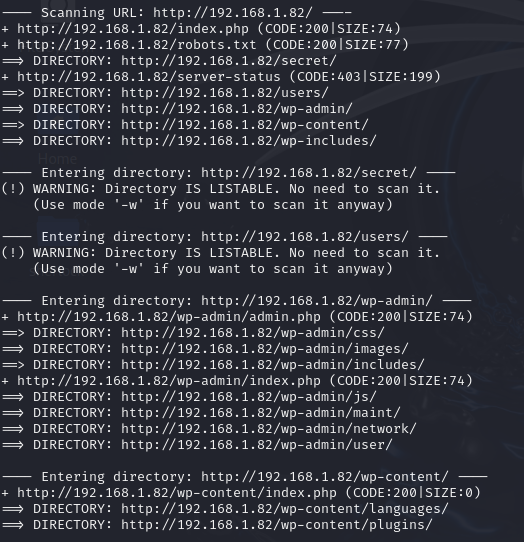
Observamos si hay una página de inicio de sesión, una aplicación web o cualquier otra cosa que pueda ofrecer pistas sobre cómo acceder.



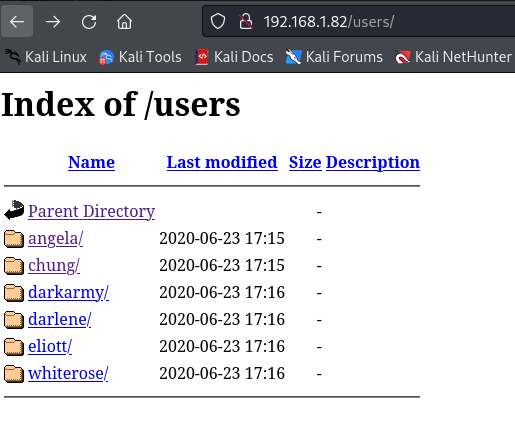
Vale, con esto confirmamos que es la IP correcta del objetivo.

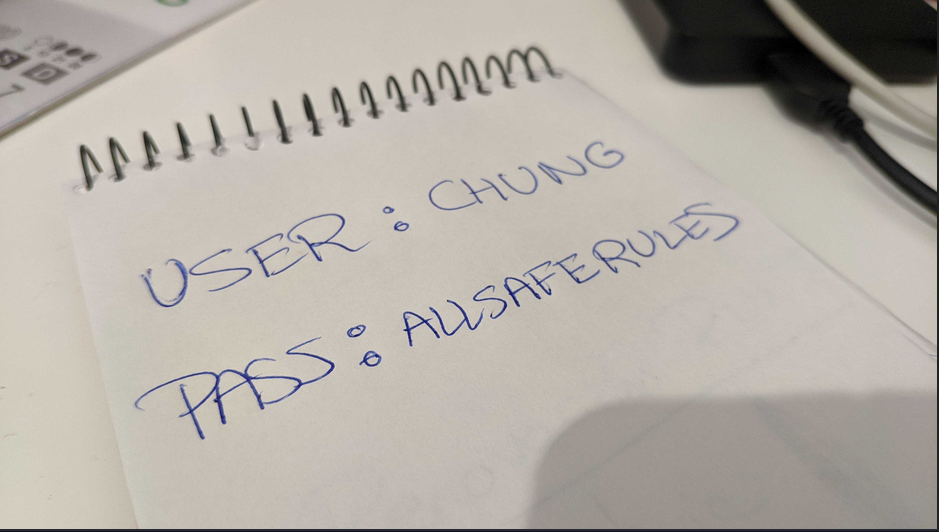
Vamos a usar herramientas como dirb para enumerar directorios y archivos en el servidor web.

dirb http://192.168.1.82



Navego a http://192.168.1.82/users/ para ver si hay listados de usuarios o información sobre usuarios del sistema.



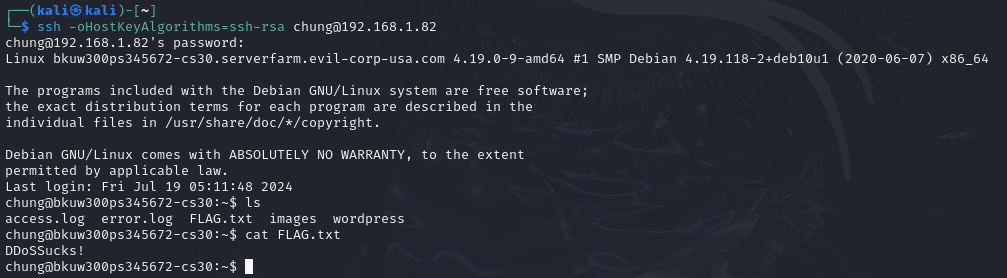


¡Tenemos credenciales!

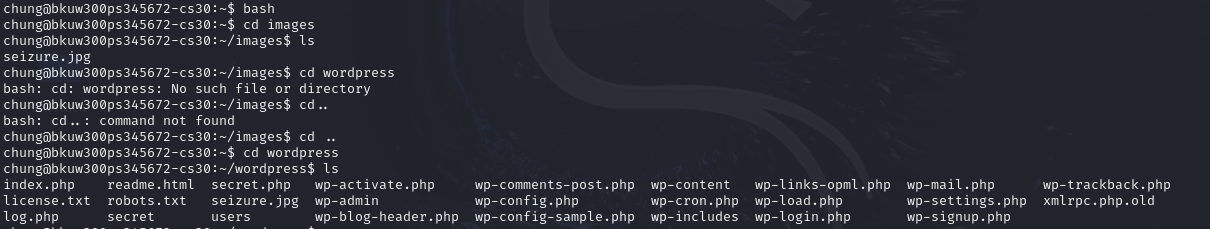


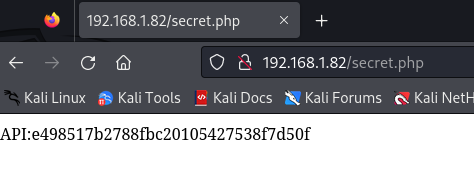
Estamos dentro

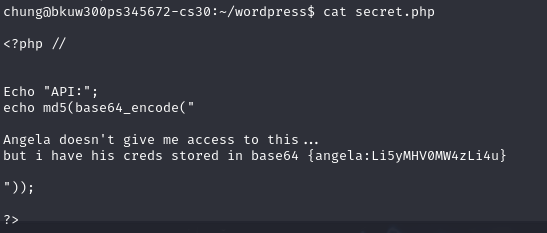
Entramos con ssh desde linux para más comodidad y trasteamos un poco

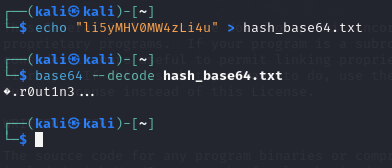


no me deja acceder a images ni a wordpress porque somos rbash asique dejamos de serlo



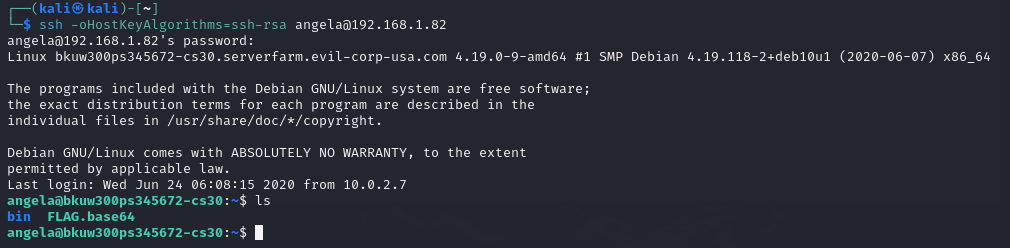






Parece que esa debe de ser la contraseña de Angela “..r0ut1n3…”

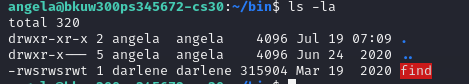
correcto, estoy dentro.



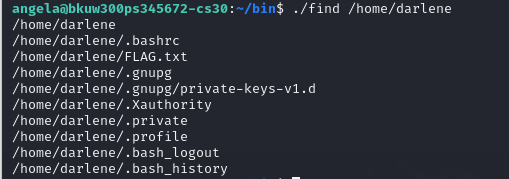
decodificamos la flag



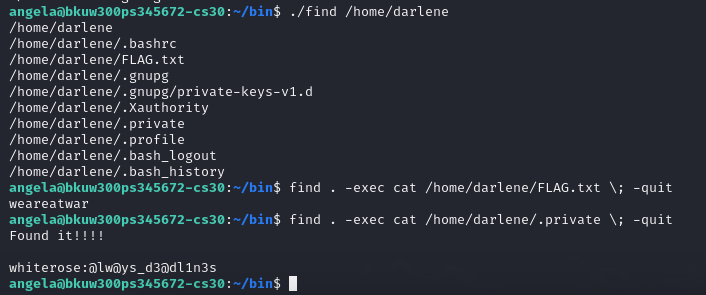
Vamos a ver los archivos y directorios que hay en la otra carpeta que se llama bin



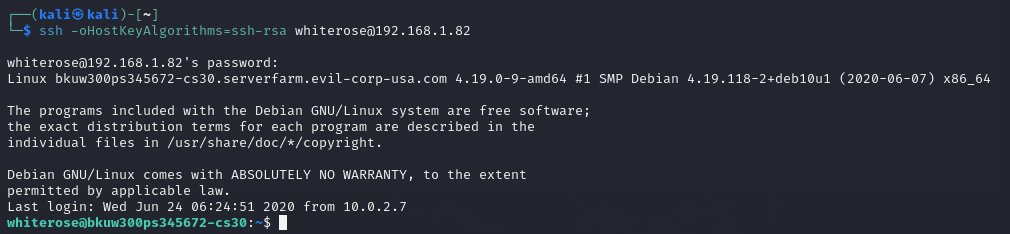
En este caso vemos find marcado en rojo justo en el apartado de Darlene que es otro usuario por lo tanto supongo que tendremos que usar el comando find para acceder a la carpeta del user Darlene



¡Correcto! veamos la siguiente flag

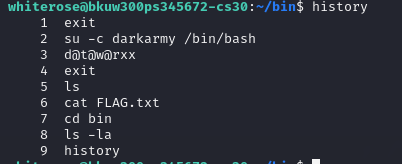


Tenemos las credenciales de whiterose!



Estamos dentro de whiterose.

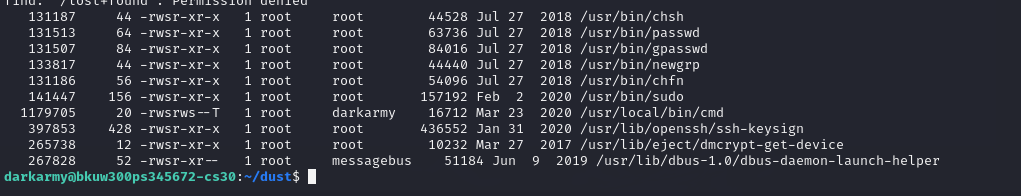
ponemos el comando history para ver los ultimos movimientos



La contraseña es d@t@w@rxx ??

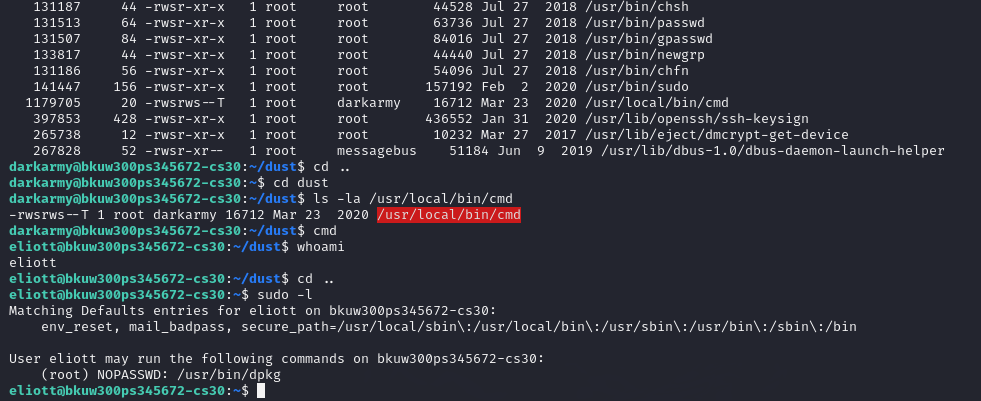
Vamos a probar

En darkarmy podemos buscar por archivos con el SUID activado de esta manera: **find / -perm -u=s -type f -ls**



Podemos ver que el archivo cmd tiene le bit SUID activado ejecutandose como root y lo podemos ejecutar siendo darkarmy

Por lo que ejecutamos cmd:



he ejecutado el comando sudo -l para ver lo programas que puede ejecutar el usuario eliott con permisos de root:

Podemos ejecutar dpkg con sudo y sin que nos pregunte la contraseña (NOPASSWD)

si miramos en la página GTFOBins podemos usar dpkg para abrir una shell

