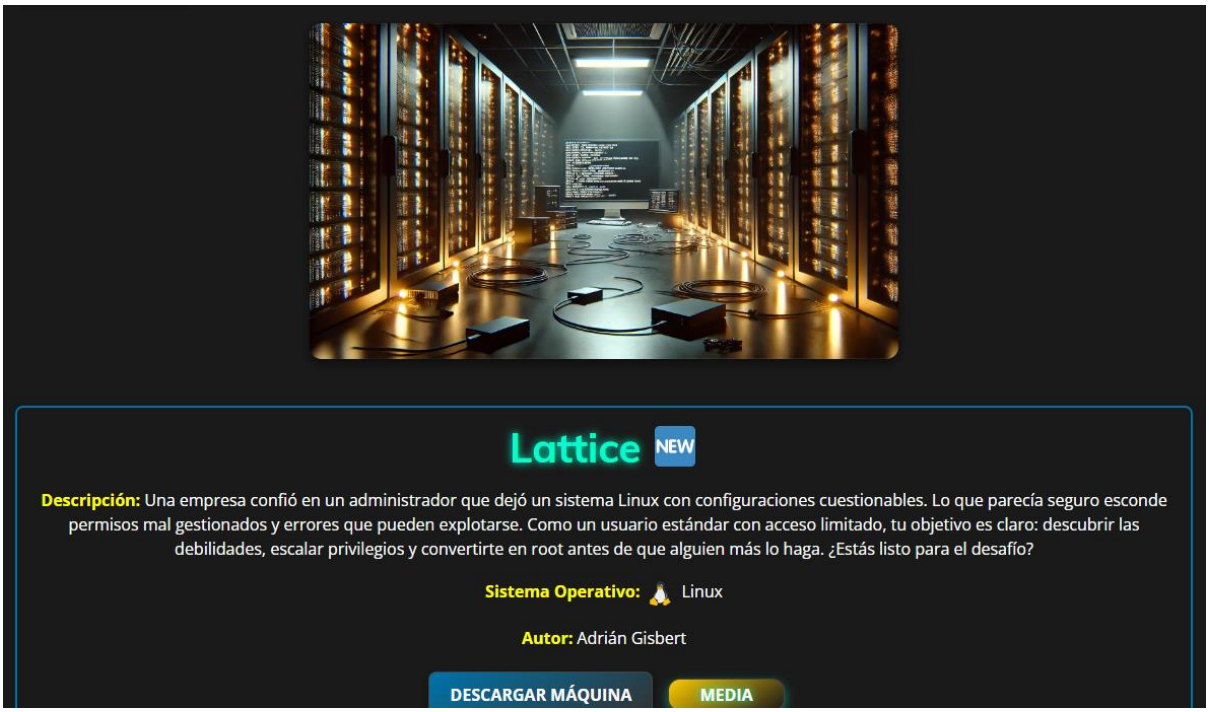
LATTICE



Lattice NEW

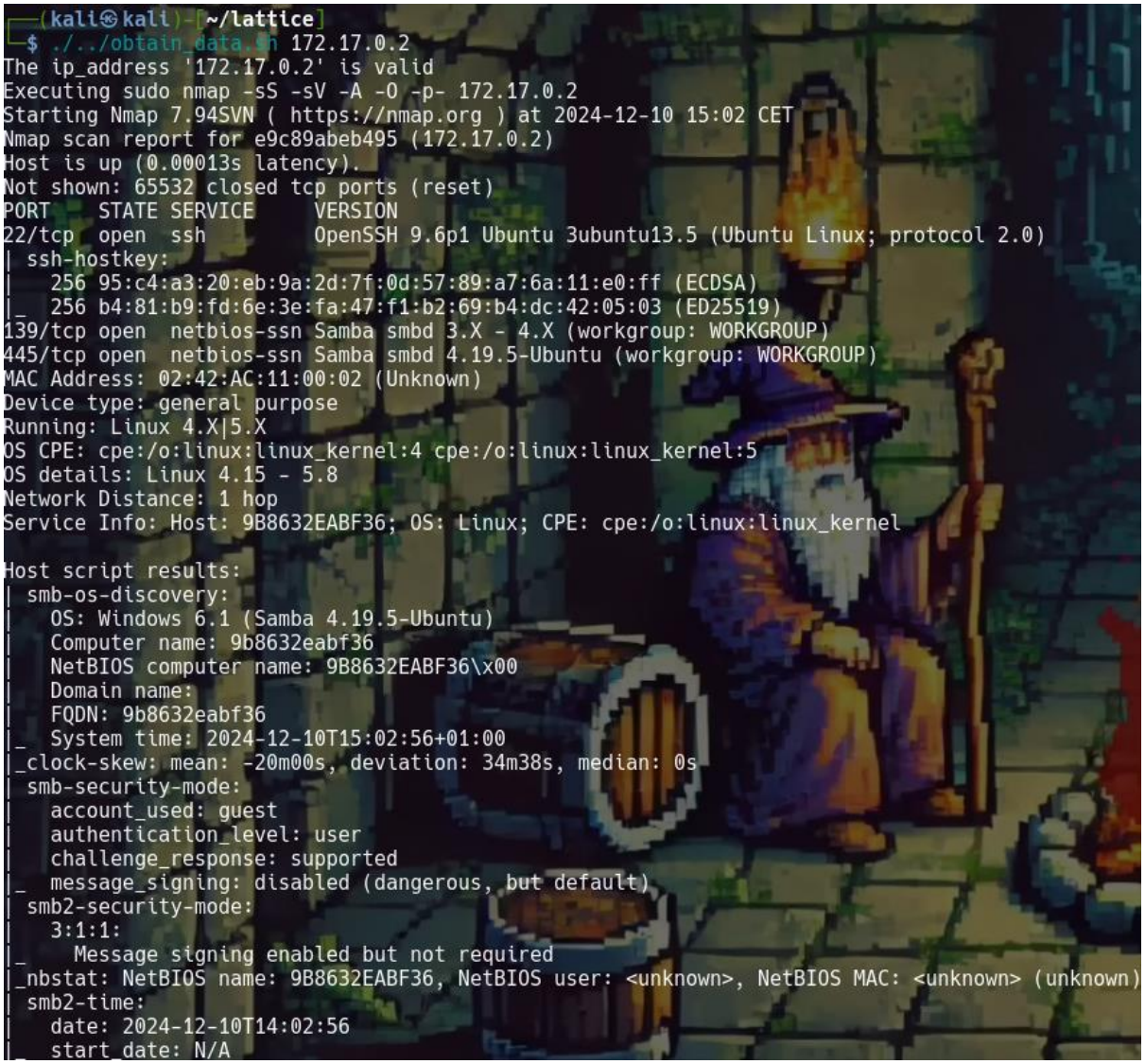
Descripción: Una empresa confió en un administrador que dejó un sistema Linux con configuraciones cuestionables. Lo que parecía seguro esconde permisos mal gestionados y errores que pueden explotarse. Como un usuario estándar con acceso limitado, tu objetivo es claro: descubrir las debilidades, escalar privilegios y convertirte en root antes de que alguien más lo haga. ¿Estás listo para el desafío?

Sistema Operativo: Linux

Autor: Adrián Gisbert

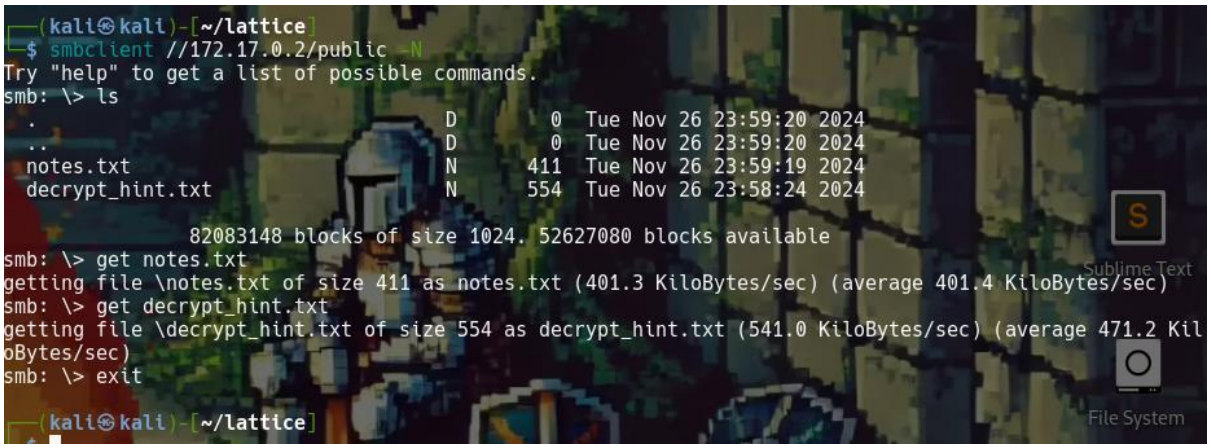
DESCARGAR MÁQUINA MEDIA

Ejecutamos nmap y observamos que existe el puerto 22 con ssh y el resto de puertos relacionados con el protocolo de smb.



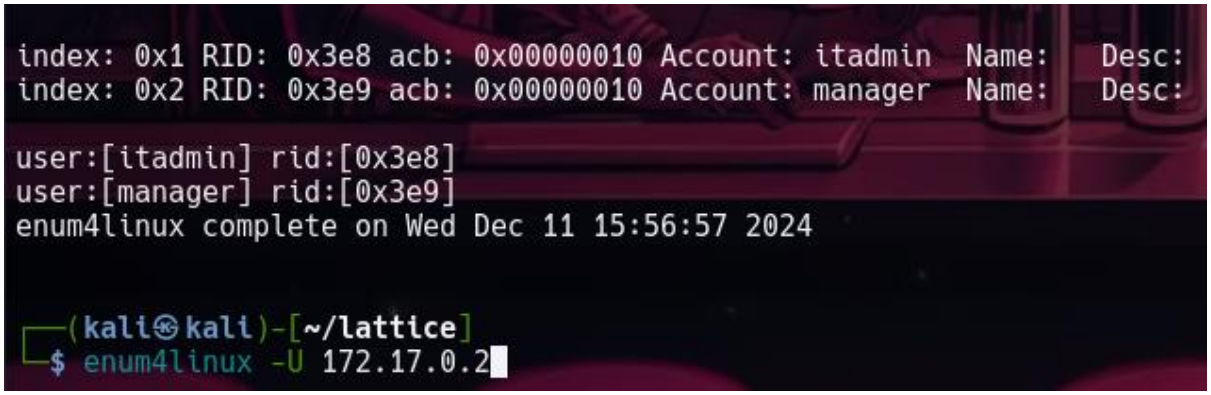
En samba, listamos los recursos visibles para anónimo.

Accedemos al recurso public y hay 2 ficheros .txt.



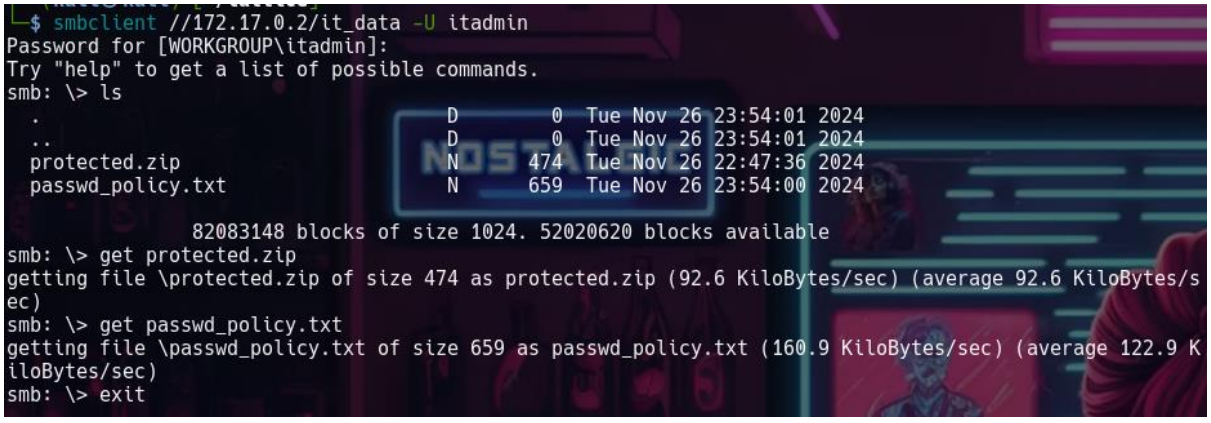
Si abrimos los ficheros descargados leemos lo siguiente.

Como el mensaje parece estar escrito por el usuario itadmin, vamos a comprobar si existe en samba o si existiese alguno más.

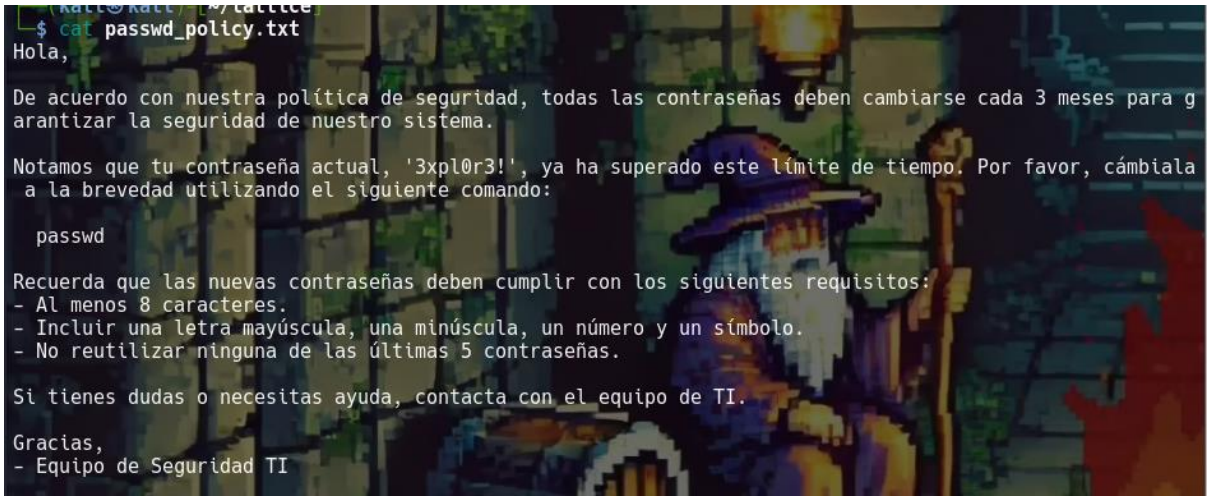


Al leer vemos que pone que no se acuerdan de la contraseña de itadmin y que esta es sencilla, vamos a realizar un ataque de fuerza bruta usando ese usuario.

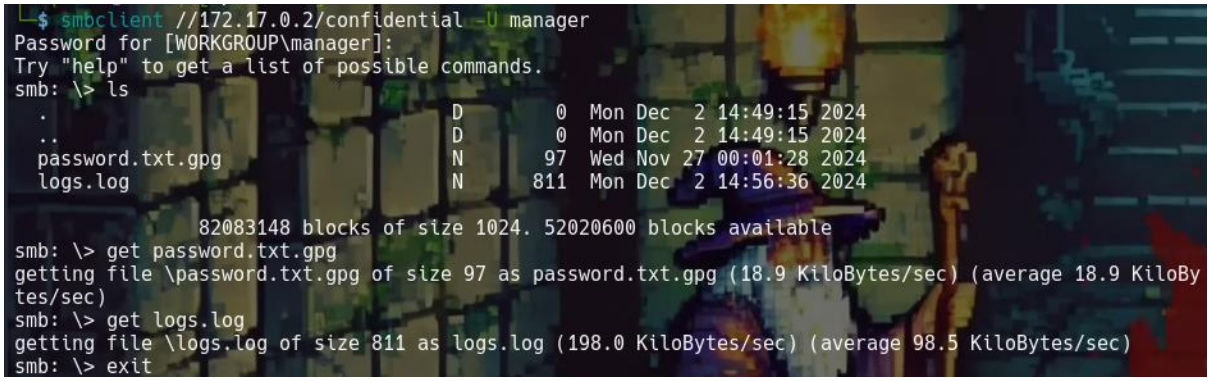
Accedemos al recurso it_data que se menciona en las notas con el usuario itadmin y descargamos en nuestra máquina todo lo que vemos.



Leemos el fichero puesto que todavía no tenemos la contraseña del zip.



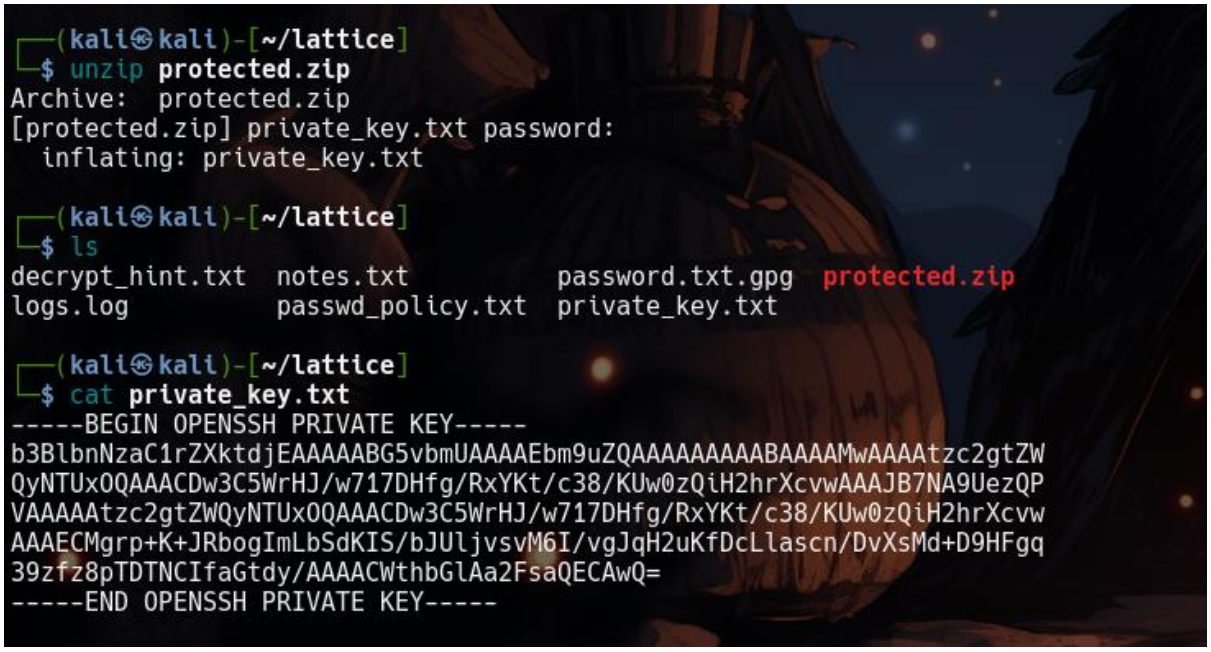
Realizando pruebas comprobamos que la contraseña citada en la nota anterior es del usuario manager. Accedemos al recurso /confidential y descargamos todo.



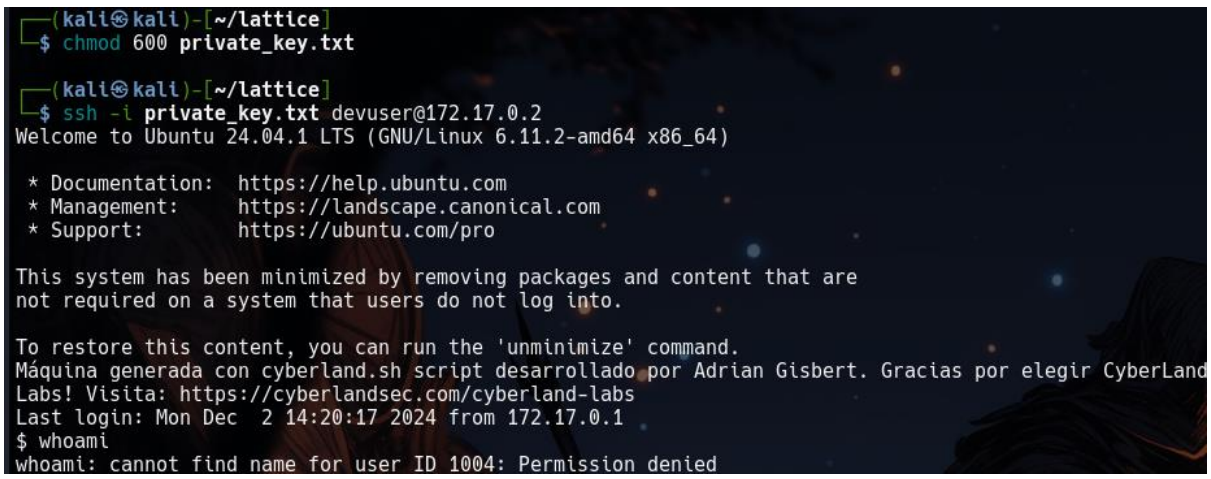
Leemos primero el fichero de log y sacamos en claro que existe en el sistema un usuario llamado devuser y que existe su clave privada.

Realizamos el decrypt al fichero .gpg que descargamos puesto que en notas anteriores nos dieron la clave: ExPl0r3.2024

A su vez esto nos da la contraseña que necesitamos para descomprimir el fichero .zip

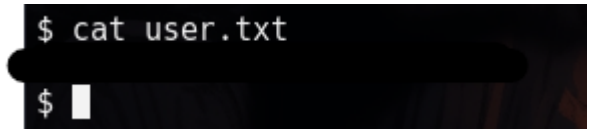


Damos permisos necesarios a la clave privada y usamos ssh para conectarnos con dicha clave.



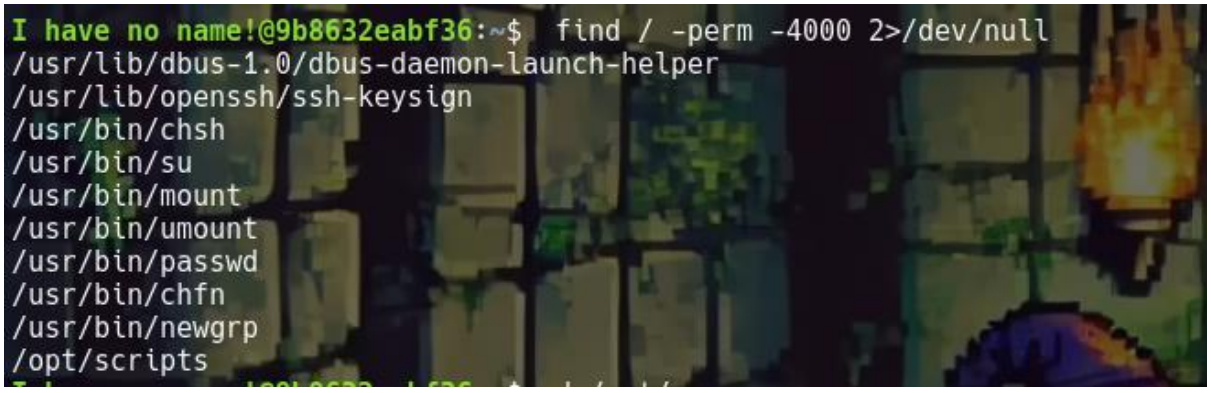
Si realizamos un listado del directorio home del usuario tenemos lo siguiente:

En el mismo directorio obtenemos la flag de user.

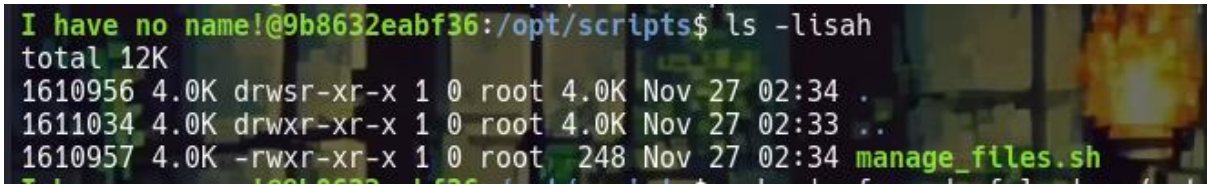


Para poder navegar mejor por el sistema cambiamos la shell.

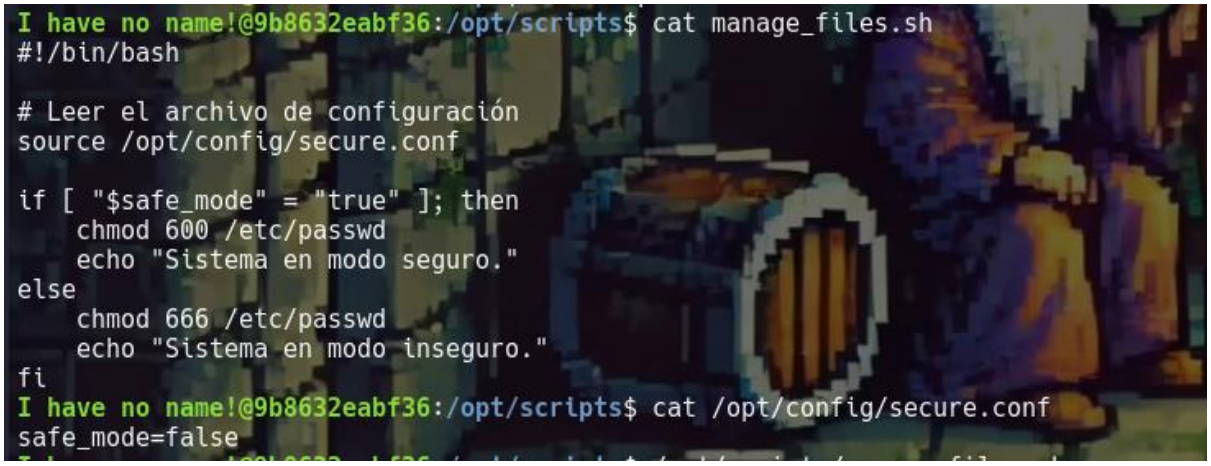
Buscando formas para realizar el escalado, encontramos un directorio un tanto fuera de lo común /opt/scripts en el que está activado el suid.



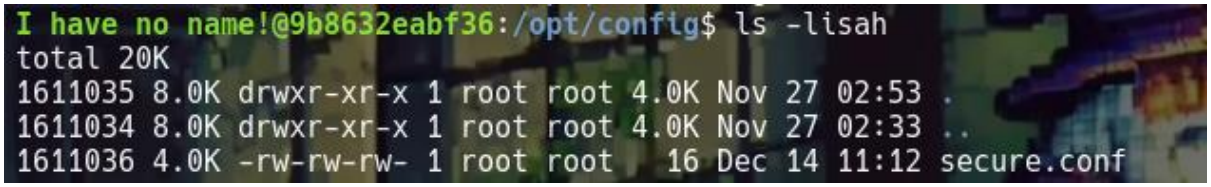
En el directorio de /opt/scripts encontramos un script en el que solo tenemos permisos de lectura y ejecución.



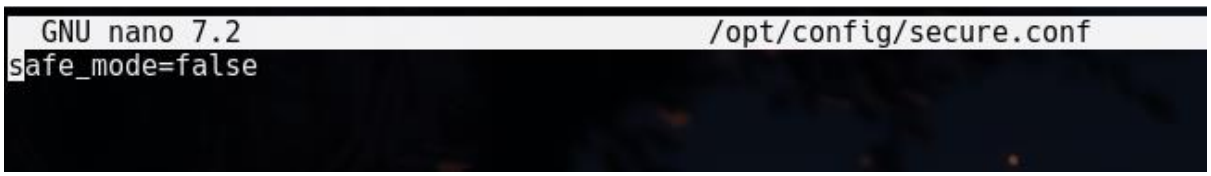
Echamos un vistazo al script donde hace referencia al fichero secure.conf el cual el contenido de este define el comportamiento de manage_files.sh.



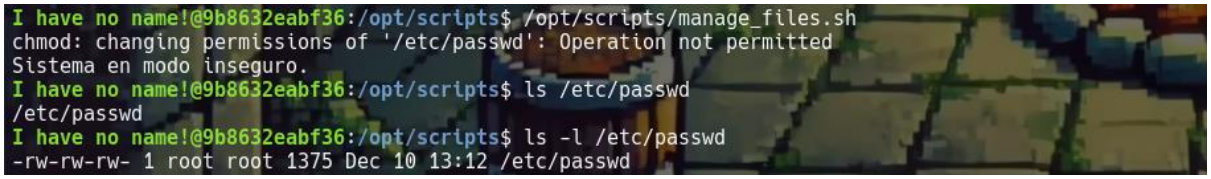
Ahora vamos a la ruta donde se ubica el fichero secure.conf (/opt/config) y vemos que tenemos permisos de escritura.



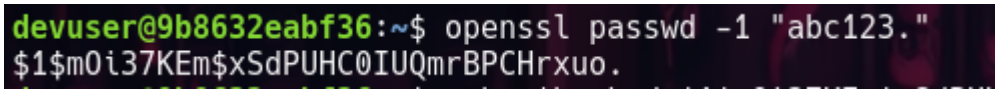
Editamos el fichero y ponemos el valor a false.



Una vez editado el fichero ejecutamos el script y aseguramos que tengamos permisos de escritura en el fichero passwd.



Para añadir un usuario en el fichero passwd es necesario que tenga una contraseña y que esta esté cifrada, es por ello que introducimos una contraseña y la ciframos, en este caso en md5.



Creamos un usario root llamado raat con la contraseña cifrada.

Accedemos como raat, vamos al directorio de root y adquirimos nuestra flag.